Contents

- Remote
  - MultiPoint Services
    - Planning a MultiPoint Services Deployment
      - Introducing MultiPoint Services
      - Getting started with MultiPoint Services
      - Common Usage Scenarios
      - MultiPoint Stations
      - Selecting Hardware for Your MultiPoint Services System
      - Hardware Requirements and Performance Recommendations
        - Variables Affecting MultiPoint Services System Performance
      - MultiPoint Services Site Planning
      - Network Considerations and User Accounts
      - Storing Files with MultiPoint Services
      - Protecting the System volume with Disk Protection
      - MultiPoint Services Virtualization Support
      - Application Considerations
      - Predeployment Checklist
      - Glossary
    - Migrate MultiPoint Services
      - Prepare to migrate to MultiPoint Services
      - Planning worksheet for your migration
      - Migrate to MultiPoint Services
      - Post-migration tasks
    - Deploying MultiPoint Services
      - Deploy a new MultiPoint Services System
        - Collect hardware and device drivers needed for the installation
        - Set up the physical computer and primary station
        - Install MultiPoint Services
        - Update and install device drivers if needed

- Set the date, time, and time zone
- Join the MultiPoint Server to a domain (optional)
- Install updates
- attach additional stations to your MultiPoint server
  - Set up a direct-video-connected station
  - Set up a USB zero client-connected station
  - Set up an RDP-over-LAN connected station
- Manage Client Access Licenses (CAL) with MultiPoint Services
- Install software on your MultiPoint Services System
- Optional configuration tasks for a MultiPoint Services deployment
  - Set up a split-screen station
  - Add printers
  - Create Windows 10 Enterprise virtual desktops for stations
- Prepare your MultiPoint Services System for users
  - Plan user accounts for your MultiPoint Services environment
  - Example scenarios: MultiPoint Services user accounts
  - Create local user accounts
  - Limit users' access to the MultiPoint server
  - Configure stations for automatic logon
  - Allow one account to have multiple sessions
  - Enable file sharing in MultiPoint Services
- System administration in MultiPoint Services
  - Configure Disk Protection in MultiPoint Services
  - Install Server Backup on your MultiPoint system
  - Configure group policies for a domain deployment
- Managing MultiPoint Services
  - Managing Your MultiPoint Services System
    - Privacy and Security Considerations
  - Manage Station Hardware
    - View Hardware Status
    - Work with USB Devices
    - Work with Video Devices

Set Up a Station
Manage System Tasks Using MultiPoint Manager
Edit Server Settings
Restart or Shut Down MultiPoint Systems
Switch Between modes
Enable or Disable Disk Protection
Manage Client Access Licenses
Remap All Stations
Save Connection Settings to File
Add or remove computers
Manage User Stations
View User Connection Status
Log off or Disconnect User Sessions
Suspend and Leave User Session active
End a User Session
Set up a Station for Automatic Logon
Split a User Station
Manage User Accounts
User Account Considerations
Create an Administrative User Account
Create a Standard User Account
Create a MultiPoint Dashboard User Account
Update or delete a User Account
Manage Virtual Desktops
Manage User Files
Keep Files Private
Share Files
Save and Share Files on a USB Flash Drive
Manage User Desktops Using MultiPoint Dashboard
Block or Unblock a Station
Limit Web Access
Block or Unblock USB Storage

Project a Station to Other Stations
Launch or Close Applications on a Station
Use IM
Take Control of a User Session
View Options for Session Thumbnails in MultiPoint Dashboard
Log Off User Sessions
Manage MultiPoint Systems Using MultiPoint Dashboard
Restart or Shut Down
Remap selected MultiPoint Systems
Remote Server Administration Tools
Remote Desktop Services
Remote Access
Overview
Tutorials
Always on VPN
Tutorial - Deploy Always On VPN
Step 1. Plan the Always On VPN Deployment
Step 2. Configure the Always On VPN Server Infrastructure
Step 3. Configure the Remote Access Server for Always On VPN
Step 4. Install and Configure the NPS Server
Step 5. Configure DNS and Firewall Settings
Step 6. Configure Windows 10 Client Always On VPN Connections
Step 7. Conditional access for VPN connectivity using Azure AD
Step 7.1. Configure EAP-TLS to ignore Certificate Revocation List (CRL) checking
Step 7.2. Create root certificates for VPN authentication with Azure AD
Step 7.3. Configure the Conditional Access policy
Step 7.4. Deploy Conditional Access root certificates to on-premises AD
Step 7.5. Create OMA-DM based VPNv2 Profiles to Windows 10 devices
DirectAccess
DirectAccess offline Domain Join
Deploy a Single DirectAccess Server Using the Getting started Wizard
Plan a Basic DirectAccess Deployment

Install and Configure Basic DirectAccess
Deploy a Single DirectAccess Server with Advanced Settings
Plan an Advanced DirectAccess Deployment
Install and Configure Advanced DirectAccess
Add DirectAccess to an Existing Remote Access (VPN) Deployment
Plan to Enable DirectAccess
Enable DirectAccess
Deploy DirectAccess Remote Client Management
Deploy Remote Access in an Enterprise
Deploy Remote Access in a Load Balancing Cluster
Plan a Remote Access Cluster Deployment
Configure a Remote Access Cluster
Deploy Multiple Remote Access Servers in a Multisite Deployment
Deploy Remote Access with OTP Authentication
Deploy Remote Access in a Multi-forest Environment
Use Remote Access Monitoring and Accounting
Monitor the existing load on the Remote Access server
Monitor the configuration distribution status of the Remote Access server
Monitor the operations status of the Remote Access server and its components
Identify and resolve Remote Access server operations problems
Monitor connected remote clients for activity and status
Generate a usage report for remote clients using historical data
Manage DirectAccess Clients Remotely
Plan Deployment for Remote Management of DirectAccess Clients
Install and Configure Deployment for remote Management of DirectAccess Clients
Publishing Applications using AD FS Preauthentication
Publishing Applications with SharePoint, Exchange and RDG
How-to Guides
Virtual Private Networking (VPN)
Configure VPN device tunneling
How to configure Diffie Hellman protocol over IKEv2 VPN connections
How to use single sign on (SSO) over VPN and Wi-Fi connections

- Concepts
  - Always On VPN
    - About Always On VPN
    - Always On VPN deployment infrastructure
    - Always On VPN features and functionalities
    - Always On VPN advanced features
  - DirectAccess
    - About DirectAccess
    - DirectAccess Unsupported configurations
    - Direct Access Capacity Planning
  - RAS Gateway
    - About RAS Gateway
    - GRE Tunneling in Windows Server
    - RAS Gateway GRE Tunnel Throughput and Performance
    - RAS Gateway for Software Defined Networking
  - Routing
    - Network Address Translation (NAT) routers
    - LAN routers running Border Gateway Protocol (BGP)
    - Routing Information Protocol (RIP)
    - Multicast-capable routers using Internet Group Management Protocol (IGMP)
    - Demand-dial routing
    - Unicast IP Routing
  - Web Application Proxy
- Troubleshooting
  - Always On VPN
  - DirectAccess
  - DirectAccess Known Issues
  - Troubleshooting Web Application Proxy
- Reference
  - BGP Windows PowerShell Command reference
  - Remote Access PowerShell Command reference
  - Windows VPN technical guide

Resources
DirectAccess Test Lab Guides
About DirectAccess Test Lab Guides
Test Lab Guide: Demonstrate DirectAccess in a Cluster with Windows NLB
Overview of the DirectAccess Cluster-NLB Test Lab Scenario
DirectAccess Cluster-NLB Test Lab Configuration Requirements
Steps for Configuring the DirectAccess Cluster-NLB Test Lab
Test Lab Guide: Demonstrate a DirectAccess Multisite Deployment
Overview of the Test Lab Scenario
Configuration Requirements
Steps for Configuring the Test Lab
Test Lab Guide: Demonstrate DirectAccess with OTP Authentication and RSA SecurID
Overview of the Test Lab Scenario
Configuration Requirements
Steps for Configuring the Test Lab
Routing and Remote Access Snap-In

MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint Services is a solution that allows multiple users, each with their own independent and familiar Windows experience, to simultaneously share one computer.

User stations, consisting of a monitor, keyboard, and mouse, are directly connected to the host computer through USB or video cables. Because MultiPoint Services is a genuine Microsoft published software product, when properly licensed, you are eligible to receive support by Microsoft or an authorized partner. This gives you the full capabilities of Windows, access to all the latest updates, and confidence that you are achieving the experience you expect.

Because MultiPoint Services enables multiple users to share one computer, it can provide a low-cost alternative to traditional computing scenarios where each user has their own computer. MultiPoint Services also provides an easy management solution for MultiPoint Services system administration known as MultiPoint Manager and an easy management solution for day-to-day administration, known as MultiPoint Dashboard.

Planning a MultiPoint Services Deployment

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint Services enables multiple stations to be connected to one computer. Multiple users can then share one computer at the same time. Each station consists of a station hub, monitor, keyboard, and mouse. MultiPoint Services includes the MultiPoint Manager application, which helps you, as an administrative user, to monitor and manage MultiPoint stations, and the MultiPoint Dashboard application, which provides day-to-day administrative functionality.

Use the following information to plan your deployment:

- Introducing MultiPoint Services
- Common Usage Scenarios
- MultiPoint Stations
- Selecting Hardware for Your MultiPoint Services System
- Hardware Requirements and Performance Recommendations
- MultiPoint Services Site Planning
- Network Considerations and User Accounts
- Storing Files with MultiPoint Services
- Protecting the System Volume with Disk Protection
- MultiPoint Services Virtualization Support
- Application Considerations
- Predeployment Checklist

You can also visit the MultiPoint Services.

Introducing MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint Services role in Windows Server 2016 allows multiple users, each with their own independent and familiar Windows experience, to simultaneously share one computer.There are several ways users can access their sessions. One way is by remoting into the server using the remote desktop apps with any device. Another way is through physical stations attached to the MultiPoint server:

- Directly to video ports on the computer
- Through specialized USB zero clients (also referred to as multifunction USB hubs), as well as through similar USB-over-Ethernet devices.
- Over the local area network (LAN)

Each of these methods is described in more detail in MultiPoint Services Stations later in this document.

This document addresses the following factors to consider when you are planning to deploy MultiPoint Services:

- What type of desktops to use with your MultiPoint Services system: Will you need sessions, virtual machines, or Windows PCs?
- Selecting Hardware for Your MultiPoint Services System: What hardware decisions should you make?
- Hardware Requirements and Performance Recommendations: What hardware is required for MultiPoint Services?
- MultiPoint Services Site Planning: Where will the computers that are running MultiPoint Services and their stations be located, and how will they be configured?
- Network Considerations and User Accounts: The networking environment into which the MultiPoint Services system is deployed can affect how user accounts are managed. What is your networking environment? How will user accounts be managed?
- Storing Files with MultiPoint Services: Where will user files be stored, and how will they be accessed?
- Predeployment Checklist

Getting Started with MultiPoint Services

12/9/2022 • 4 minutes to read • Edit Online

Your MultiPoint Services system allows many users to use multiple stations that are physically connected by using station hubs to only one computer. Each station typically consists of a station hub, mouse, keyboard, and video monitor. Each user at a MultiPoint Services station experiences a unique Windows computing session that you can manage using MultiPoint Manager.

The components of a MultiPoint Services system include the following:

- MultiPoint Services system software, which supports multiple monitors, keyboards, mouse devices, and other devices on the computer.
- The MultiPoint Manager application, which lets you monitor and take actions on MultiPoint Services stations.
- Maintenance and management tools.
- The MultiPoint Dashboard application, which lets you complete daily tasks, such as communicating with other users.

Information about how to manage MultiPoint Services stations with MultiPoint Manager and MultiPoint Dashboard is provided in this Help file.

Overview of MultiPoint Manager

MultiPoint Manager provides four tabs to use when you are managing the MultiPoint Services stations. Each tab, and the tasks that you can perform on them, is described in more detail in each Help topic.

The tabs are as follows:

- **Home tab:** Switch modes to perform administrative tasks, add or remove MultiPoint servers, restart or shut down the computer, enable disk protection, add client access licenses, remap stations, and get help or support. For more information, see the Manage System Tasks Using MultiPoint Manager topic.
- **Stations tab:** View users' *desktop* status and *end* or *suspend* user sessions. For more information, see the Manage User Stations topic.
- **Users tab:** Create and manage *standard user accounts* and *administrative user accounts*. For more information, see the Manage User Accounts topic.
- **Virtual Desktops tab:** Enable virtual desktop roles. For more information, see the Manage Virtual Desktops topic.

MultiPoint Server management and maintenance

After your MultiPoint Services system is set up, you can use MultiPoint Manager to manage MultiPoint Services.

Types of actions you can perform using MultiPoint Manager include the following:

- **Adding user accounts:** Use MultiPoint Manager to create standard and administrative user accounts.
- **Editing server settings:** You can configure your MultiPoint Services system to start in console mode, allow an account to have multiple sessions, assign a unique IP address to each station, and other tasks.

- **Switching to console mode:** You can change the MultiPoint Services system to console mode in order to install new software on your MultiPoint Services system. You can specify that all users can run the software, or that only you can use the software, depending on the installation and licensing options of the software.
- **Troubleshooting:** If you experience problems with MultiPoint Services, check the Troubleshooting section to find topics that can help you fix the problem.

Overview of MultiPoint Dashboard

MultiPoint Dashboard features a ribbon experience where you can choose between two tabs to access common daily tasks.

The tabs are as follows:

- **Home tab:** Block or unblock stations, set web limiting options, project desktops to other desktops, launch or close applications, communicate via instant messaging, assist other users through remote desktop control, adjust desktop thumbnail views, and enable or disable instant messaging and application auto-launch. For more information, see the Manage User Desktops Using MultiPoint Dashboard topic.
- **Systems tab:** Restart, shut down, or remap either all or selected systems. For more information, see the Manage MultiPoint Systems Using MultiPoint Dashboard topic.

Daily use of your MultiPoint Server system

As you begin to use MultiPoint Services daily, there is information about how to use MultiPoint Services that you might want to share with the users on your MultiPoint Services system. This information includes the following:

Sharing content and keeping content private:

- A user can save a file or document to a private folder that can be viewed only by that user.
- Users can also save documents to a public folder that is accessible to all users on the MultiPoint Services system.
- It is important for MultiPoint Services users to know that administrative users have access to all files and documents on the system, even if they are stored privately in a user's personal folder.

For more information about how to save and manage private and public content, see the Manage User Files topic.

Information about a user's MultiPoint Services session:

- Each user has a user name and password, and a unique desktop *session* on the MultiPoint Services system.
- A *standard user* is not an *administrative user* on the MultiPoint Services system. Standard users cannot install some types of software, but can save files and change desktop settings, except for the screen resolution. Any desktop changes the user makes are present when the user logs on again.
- Users can disconnect from one station and log back on to their session on a different station without losing their work. For more information, see the Suspend and Leave User Session Active topic.
- A standard user's session (or all user sessions) can be disconnected or logged off by the administrative user through MultiPoint Manager. For more information, see the Manage User Desktops topic.
- If a user forgets a password, you can reset the password from the **Users** tab, which uses standard Windows user account management functionality. For more information, see the Update or Delete a User

Account topic.

See Also

Managing Your MultiPoint Server System Important Information about Software License Compliance Manage System Tasks Using MultiPoint Manager Manage User Files Manage User Desktops Suspend and Leave User Session Active View User Connection Status Manage Station Hardware Set Up a Station Manage User Accounts Update or Delete a User Account Manage User Desktops Using MultiPoint Dashboard Manage MultiPoint Systems Using MultiPoint Dashboard Troubleshooting

Common Usage Scenarios

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint Services delivers individual user desktops with the most important elements of the Windows 10 desktop experience. It also offers a simple management tool, the MultiPoint Manager, that system administrators can use for discovery and control of multiple MultiPoint servers and clients. Additionally, MultiPoint Services includes the MultiPoint Dashboard for real-time visibility. Examples of what you can do with MultiPoint Services include the following:

- Give each user a personal computing experience and private folders without needing a separate computer for each person.
- Manage multiple MultiPoint systems in a computer lab, classroom, training center, or small business environment.
- Install a program once, and access it from any station.
- Monitor each user's desktop activity.
- Block screens with a customizable message to get the group's attention.
- Restrict the group to only accessing one or more websites.
- Project your screen to the other screens to demonstrate a particular task.
- Communicate privately with a standard user who is asking for help.
- Take control of a user's session to demonstrate a task.
- Do all of the above-listed items for a user who is using a traditional PC, laptop, or any other mobile device.

MultiPoint Stations

12/9/2022 • 6 minutes to read • Edit Online

In a MultiPoint Services system environment, *stations* are the user endpoints for connecting to the computer running MultiPoint Services. Each station provides the user with an independent Windows 10 experience. The following station types are supported:

- Direct-video-connected stations
- USB-zero-client-connected stations (including USB-over-Ethernet zero clients)
- RDP-over-LAN-connected stations (for rich client or thin client computers)

Full PCs that have the MultiPoint Connector installed can also be monitored and controlled using the MultiPoint Dashboard. On Windows 10 the MultiPoint Connector can be enabled through the control panel for Windows features.

Multipoint Services supports any combination of these station types, but it is recommended that one station be a direct-video-connected station, which can serve as the primary station. The reason for this recommendation is to be able to anticipate support scenarios. For example, to interact with the system's BIOS before MultiPoint Services is running.

Primary stations and standard stations

One direct-video-connected station is defined as the *primary station*. The remaining stations are referred to as *standard stations*.

The primary station displays the startup screens when the computer is turned on. It provides access to system configuration and troubleshooting information that is only available during startup. The primary station must be a direct-video-connected station. After startup, you can use the primary station like any other MultiPoint station.

Direct-video-connected stations

The computer running MultiPoint Services can contain multiple video cards, each of which can have one or more video ports. This allows you to plug monitors for multiple stations directly into the computer. Keyboards and mice are connected through USB hubs that are associated with each monitor. These hubs are referred to as *station hubs*. Other peripheral devices, such as speakers, headphones, or USB storage devices can also be connected to a station hub, and they are available only to the user of that station.

> **IMPORTANT**
>
> There should be at least one *direct-video-connected station* per server to act as the primary station to display the startup process when the computer is turned on.

Figure 1 MultiPoint services system with four direct-video-connected stations

PS/2 stations

With MultiPoint Services, you can map the PS/2 keyboard and mouse on the motherboard to a direct video connected monitor to create a PS/2 station. High-definition analog audio on the motherboard is the audio associated with this type of station. This does not apply to computers where there are no PS/2 jacks on the motherboard.

USB-zero-client-connected stations

USB-zero-client-connected stations utilize a *USB zero client* as a station hub. USB zero clients are sometimes referred to as a multifunction hub with video. They are a hub that connects to the computer through a USB cable, and these hubs typically support a video monitor, a mouse and keyboard (PS/2 or USB), audio, and additional USB devices. This guide refers to these specialized hubs as USB zero clients.

The following diagram shows a MultiPoint server system with a primary station (direct video connected station) and two additional USB zero client connected stations.

Figure 2 MultiPoint Services system with a primary station and two USB zero-client-connected stations

USB-over-Ethernet zero clients

USB-over-Ethernet zero clients are a variation of USB zero clients that send USB over LAN to the MultiPoint Services system. These types of USB zero clients function similarly to other USB zero clients, but are not limited by USB cable length maximums. USB-over-Ethernet zero clients are not traditional thin clients, and they appear as virtual USB devices on the MultiPoint Services system. When using these devices, refer to the device manufacturer for specific performance and site planning recommendations. Most devices have a third-party plugin for MultiPoint Manager that allows you to associate and connect devices to the MultiPoint Services system.

RDP-over-LAN connected stations

Thin clients and traditional desktop, laptop, or tablet computers, can connect to the computer running MultiPoint Services through the local area network (LAN) by using Remote Desktop Protocol (RDP) or a proprietary protocol and the Remote Desktop Protocol Provider. RDP connections provide an end-user experience that is very similar to any other MultiPoint station, but makes use of the local client computer's hardware. Learn more about our remote desktop applications available for Android, iOS, Mac and Windows in Remote Desktop clients.

Clients and devices that are running Microsoft RemoteFX can provide a rich multimedia experience by taking advantage of the processor and video hardware capabilities of the local thin client or computer to provide high-definition video over the network.

If you have existing LAN clients MultiPoint Services can provide a quick and cost effective way to simultaneously upgrade all of your users to a Windows 10 experience.

From a deployment and administration perspective, the following differences exist when you use RDP-over-LAN-connected stations:

- Not limited to physical USB connection distances
- Potential to reuse older computer hardware as stations
- Easier to scale to a higher number of stations. Any client on your network can potentially be used as a remote station
- No hardware troubleshooting through the MultiPoint Manager console
- No split-screen functionality.

  For more information, see Split-screen Stations later in this topic
- No station rename or configuring automatic logon through the MultiPoint Manager console

Figure 3 MultiPoint Services system with RDP-over-LAN-connected stations

Additional configuration options

Split-screen stations

MultiPoint Services offers a split screen option on computers with direct-video-connected stations or USB-zero-client-connected stations. A split screen provides the ability to create an additional station per monitor. Instead of requiring two monitors, you can use one monitor with two station hub setups to create two stations with one monitor. You can quickly increase the number of available stations without purchasing additional monitors, USB-zero clients, or video cards.

The benefits of using a split-screen station can include:

- Reducing cost and space by accommodating more users on a MultiPoint Services system.
- Allowing two users to collaborate side-by-side on a project.
- Allowing a teacher to demonstrate a procedure on one station while a student follows along on the other station.

Any MultiPoint Services station monitor that has a 1024x768 resolution or greater can be split into two station screens. For the best split screen user experience, a wide screen with a minimum 1600x900 resolution is recommended. A mini keyboard without a number pad is also recommended to allow the two keyboards to fit in front of the monitor.

To create split-screen stations, you set up one direct-video-connected or USB-zero-client-connected station. Then you add an additional station hub by plugging in a keyboard and mouse to a USB hub that is connected to the server. You can then convert the station into two stations by using MultiPoint Manager to split the screen and map the new hub to half of the monitor. The left half of the screen becomes one station and the right half becomes a second station.

After a station is split, one user can log on to the left station while another user logs on to the right station.

Figure 4 MultiPoint Services system with split screen stations

Station type comparison

DESCRIPTION	DIRECT VIDEO CONNECTED	USB ZERO CLIENT CONNECTED	RDP-OVER-LAN CONNECTED

DESCRIPTION	DIRECT VIDEO CONNECTED	USB ZERO CLIENT CONNECTED	RDP-OVER-LAN CONNECTED
Video performance	Recommended for best video performance		Use thin clients that support RemoteFX for improved video quality at lower network bandwidth
Physical limitations	Limited by video cable length and USB hub and cable length (Recommended 15 meter maximum length)	Limited by USB hub and cable length (Recommended 15 meter maximum length)	Limited by LAN distribution
Number of stations allowed	Limited by number of available PCIe slots on the motherboard times the video ports per video card	Total number may be limited by USB zero client manufacturer (For more information, see the Note that follows this table.)	Limited by available ports on network switch
Split-screen	Yes	Yes	No
MultiPoint Manager station peripheral status, auto-logon configuration, station renaming	Yes	Yes	No
Access to server startup menus	Yes	No	No

NOTE

The total number of USB zero clients that are connected to the server may be limited by the manufacturer or the hardware capability of the computer running MultiPoint Services.

Selecting Hardware for Your MultiPoint Services System

12/9/2022 • 12 minutes to read • Edit Online

When you build a MultiPoint Services system, you should select a computer that meets the Windows Server 2016 system requirements. If you are deciding which components to select, consider the following:

- The target price range of your complete solution.
- The types of usage scenarios that you might expect for the MultiPoint Services system, such as whether the users are running multimedia programs, using word processing or productivity programs, or browsing the Internet.
- Whether your scenario has large processing or memory demands.
- The number of users who could be using the system at the same time. If you plan to have many users on your system at the same time, or users who use system-intensive programs, you should plan for more computing power for your system.
- The type of stations. How many USB ports or video ports do you need?
- Future expansion plans. Do you plan to add stations to the MultiPoint Services system at a later date? Will you have enough video card slots, USB ports, or network taps? How many additional users will your hardware need to support?
- Physical layout. For more information, see MultiPoint Services Site Planning.

A MultiPoint Services system typically includes the following components:

- One computer that is running MultiPoint Services, which includes a CPU, RAM, hard disk drives, and video cards.
- A monitor, station hub, keyboard, and mouse for each station.
- Optional peripheral devices for the MultiPoint Services stations, including speakers, headphones, microphones, or storage devices that are available only to the user of the station.
- Optional peripheral devices that are available to all users of the MultiPoint Services system, connected directly to the host computer, such as printers, external hard disk drives, and USB storage devices.

Use the following information to make hardware decisions:

- Selecting a CPU
- Selecting hardware components

Selecting a CPU

A MultiPoint Services system is a multiple-user environment, with all users connected to a single host computer. This increases the CPU usage because all users share the same computer. Some tasks, such as multimedia programs (for example, media players or video-editing software), have larger processing demands. Therefore, make sure to select a CPU that can handle the processing requirements for the number of users and types of user scenarios that it will need to support.

MultiPoint Services requires an x64-based CPU, and must meet the system requirements for the computer as

described in Hardware Requirements and Performance Recommendations.

The following types of processors have been tested to be used on a MultiPoint Services system with high-demand processing programs, such as multimedia programs:

- **Dual-core processor:** Can support up to 8 stations.
- **Quad-core processor:** Can support up to 16 stations.
- **Quad-core processor with multithreading:** Can support up to 20 stations.
- **Six-core processor with multithreading:** Can support up to 24 stations.

With this information, select a CPU that meets the processing requirements for your MultiPoint Services system.

> **NOTE**
> If you are running video intensive applications the recommendation is at least one core per station.

Selecting hardware components

When you are building a MultiPoint Services system, consider the following hardware components that you may need:

- Video hardware
- MultiPoint Services station hardware
  - *USB hubs*
  - USB zero clients
  - Keyboards and mouse devices
  - Monitors
- Peripheral devices
  - Audio devices, such as speakers and headphones
  - Microphones
  - USB mass storage devices

When you have selected the hardware components for your MultiPoint Services system, make sure that you obtain current, 64-bit drivers for the components.

The following topics provide detailed information to help you select components for your MultiPoint Services system:

Selecting video hardware Selecting direct-video-connected or USB zero client station devices Selecting other station peripheral devices Selecting RDP-over-LAN-connected station hardware Selecting audio devices

Selecting video hardware

The video hardware that you select should support the number of monitors that you will require for the number of users you intend to have working at MultiPoint Services stations. In addition, different types of video hardware can provide a higher-performance solution for graphics-intensive programs, such as multimedia content.

Select the video hardware that can support the maximum number of monitors for the type of performance that your MultiPoint Services system requires. Make sure that you validate the performance of the video hardware

that you choose to ensure that it meets your performance requirements.

> **NOTE**
> You must install a video driver that supports extending your desktop across multiple monitors.

Video hardware options include:

- Internal video cards that use a PCI or a PCIe bus interface
- External video controllers connected by USB

The following sections describe the capabilities of each of these video hardware types. You can combine internal video cards and external video controllers to create the system that you want.

Internal video cards

An internal video card is plugged-in to the motherboard on the computer. The internal video card is a solution that can help the performance of graphics-intensive multimedia programs. However, an internal video card requires an available PCI or PCIe slot to plug-in to the motherboard. Many high-performance video cards require a PCIe slot, but there are a limited number of PCIe slots on a motherboard. You should know what kind of video card slots are available on your computer so that you can purchase the correct type of video cards.

The number of monitors that can connect to each video card depends on the GPU that is used on the card and the number of ports it supports, which typically ranges from 2 to 6.

When you are selecting internal video cards, select video cards that support the number of monitors required to create the desired number of direct video connected stations. The maximum number of monitors that can be supported is equal to the number of internal video cards that are plugged-in to the motherboard multiplied by the number of monitor ports on each of those video cards. For example, if you had two internal video cards and each card had two monitor ports, you could support up to four monitors.

External video controllers

USB zero clients contain an external video controller to connect a monitor to the client. The USB zero client might also include connections for headphones, speakers, a microphone, or other peripheral devices.

Select a USB zero client if you want to enable support for additional monitors without opening the computer, or if you want to support more stations than available video outputs. For example, if you previously had four monitors plugged-in to internal video cards, and you want to add two more monitors, you can plug-in two external video controllers to the computer and have room for two more monitors. In this manner, you can combine a USB zero client with the video controller and not use additional PCI or PCIe slots on the motherboard.

Selecting direct-video-connected or USB zero client station devices

A MultiPoint Services station consists of a station hub or USB zero client with a keyboard and mouse plugged-in, and a monitor that is plugged-in to the host computer or in to a USB zero client. Other peripheral devices can be plugged-in to the station hub or USB zero client, but they are not required to create MultiPoint station. These other peripheral devices are described in Selecting other station peripheral devices.

The devices that you select to create a MultiPoint Services station should meet minimum requirements to work with MultiPoint Services. Details about the requirements for the following MultiPoint Services station devices are provided in this topic:

- Selecting USB hubs
- Selecting USB zero clients
- Selecting keyboards and mouse devices
- Selecting monitors

Selecting USB hubs

The USB hubs that are used in a MultiPoint Services system can be a generic USB hub. Such hubs typically have four or more USB ports, and they allow multiple USB devices to be connected to a single USB port on the computer. Some other devices, such as keyboards and video monitors, may also incorporate a USB hub into their design.

An additional consideration is the use of an *externally powered* hub, instead of a *bus-powered* hub. With a bus-powered hub, the amount of current that is provided by the host computer must be sufficient to provide power to all the peripheral devices that are plugged-in to the hub, without degrading system performance. An externally powered hub allows you to connect more peripheral devices and provide sufficient power to all of them. The use of externally powered hubs can help prevent performance issues, port failures, and other intermittent issues.

When selecting a USB hub for your MultiPoint Services system, consider its use. The hub can be used as a *station hub*, an *intermediate hub*, or a *downstream hub*. Refer to the following table for descriptions about each hub type. We recommend all USB devices to be USB 2.0 or later.

DESCRIPTION	POWERED
Station Hub	Can be bus-powered unless high-powered devices will be plugged-in to it or a downstream hub will be connected to it
Intermediate Hub	Should be externally powered
Downstream Hub	Can be externally powered or bus powered depending on the devices that are plugged-in to the hub
Active USB Extender Cable	Active USB cables that include a USB hub are typically bus powered; therefore, they are not recommended for connecting station hubs to the computer.

Selecting USB zero clients

A USB zero client is a USB hub that contains a video output. Therefore, it allows a monitor to be connected to the computer through a USB connection. For more information about using USB zero clients for video, see Selecting video hardware in this document. A USB zero client can also enable the connection of a variety of USB and non-USB devices to the hub. USB zero clients are produced by specific hardware manufacturers, and they require installing a device-specific driver.

Selecting keyboards and mouse devices

The keyboard and mouse devices that you plug-in to the station will typically be USB devices. Some USB zero clients provide PS/2 ports, in which case, the keyboard and mouse should use PS/2 to connect to the station hub. You can also use a PS/2 keyboard and mouse if you are setting up a PS/2 direct-video-connected station.

A keyboard with an internal hub can be used as a station hub. However, all other station devices must connect to the internal hub by using ports on the keyboard. If such a keyboard is connected to the computer through another hub, that hub will be treated as an intermediate hub.

If you are using split-screen stations, you may want to consider using a mini keyboard that does not have a number pad so that the two keyboards can fit in front of the monitor.

Selecting monitors

There should be one monitor provided for each MultiPoint Services station, unless a split-screen is planned. Monitors are plugged into the video card on the computer, the USB zero client or the LAN-based client. Any type of monitor that is supported by the video card, USB zero client, or LAN-based client can be used, including CRT monitors.

Some special monitors include an internal LAN-based client or USB zero client. Such monitors will typically include audio input/output jacks and internal USB hubs for connecting keyboards and mice. They connect to the server through a USB or a LAN connection.

Display resolution

The minimum supported resolution for a station's display area is 512 x 768 pixels. If the MultiPoint Services system starts and finds that a station's display area is less than the minimum resolution, a blank screen will be displayed on that station and the station will not be usable.

If a display monitor is going to be shared by two stations as split-screen stations, the minimum requirement for the display is 1024 x 768, so that the resulting individual station screen areas are at least 512 x 768. For the best split-screen user experience, a wide screen with a minimum of resolution of 1600 x 900 is recommended.

Selecting other station peripheral devices

MultiPoint Services supports peripheral devices that are connected to a station hub, a USB zero client, or directly to the computer. Devices plugged into a station hub will be associated with that specific station. Other devices are available to every station when plugged directly into the computer. LAN clients can also support peripheral devices.

> **IMPORTANT**
>
> A keyboard cannot be connected to a downstream hub (for example, a hub that is plugged into a station hub). If you plug in a keyboard to a downstream hub, any peripherals that are plugged-in to the downstream hub will no longer be available to that station. This behavior allows the support of daisy-chained station hubs.

Available to all stations A USB device that is plugged into the computer (for example, not through a station hub) is available to all stations. Depending on the device, it can be used by multiple users at one time, or only one user can access it at a time. The following table explains how USB devices can be accessed.

> **NOTE**
>
> The "Connected to Host Computer" column in the table refers to the behavior when the computer running MultiPoint Services is running in station mode with stations. If you are running in console mode, the peripherals that are plugged anywhere behave in the same way as a standard server in a console session.

DESCRIPTION	CONNECTED TO HOST COMPUTER	CONNECTED TO STATION HUB OR DOWNSTREAM HUB
Keyboard	Not functional, unless it is part of a PS/2 station.	Available to individual station Cannot be connected to a downstream hub
Mouse	Not functional, unless it is part of a PS/2 station.	Available to individual station
Speaker/headphones	Not functional, unless it is part of a PS/2 station.	Available to individual station
USB storage device	Available to all stations	Available to individual station
HID Consumer Control	Not functional	Available to individual station

DESCRIPTION	CONNECTED TO HOST COMPUTER	CONNECTED TO STATION HUB OR DOWNSTREAM HUB
Other USB devices, such as cameras, document readers, and DVD drives	Available to all stations if supported by Windows Server 2012	Available to all stations if supported by Windows Server 2008 R2 Remote Desktop Services

Selecting RDP-over-LAN-connected station hardware

Any LAN client that can connect to Remote Desktop Services, by using Remote Desktop Protocol, can become a MultiPoint Services station.

If you want the LAN client to only be used as a MultiPoint station, you may want to "lock down" your LAN client. For example, configure your thin client so that it can only connect to a MultiPoint Services session, or configure your desktop computers so that access to desktop icons and Start Menu items such as a web browser is removed to prevent direct Internet access. You can make these configurations using your LAN client configuration tools or group or local policies.

Selecting audio devices

It is important to make sure that when you select audio devices, they can be plugged into the station hub, USB zero client or LAN client. Some USB hubs, USB zero clients, and LAN clients have an analog audio jack that can be used with traditional analog audio devices (such as headphones or earbuds). Station hubs that do not have analog jacks can use USB audio devices.

If you have configured a PS/2 direct-video-connected station by using PS/2 ports on the computer's motherboard for the keyboard and mouse, you must use the analog audio on the computer's motherboard in order for the audio device to be available to this station when the MultiPoint Services system is running in station mode.

If you do not have a PS/2 direct-video-connected station, the host audio device on the system's motherboard will be available only when the MultiPoint Services system is running in console mode.

Hardware Requirements and Performance Recommendations

12/9/2022 • 2 minutes to read • Edit Online

This topic describes the hardware that is required to run a MultiPoint Services system and support user application scenarios. The user scenario directly affects the CPU, RAM, and network bandwidth requirements.

Optimize MultiPoint Services system performance

The performance of your MultiPoint Services system will be directly affected by the capability of the CPU, the GPU, and the amount of RAM that is available on the computer that is running MultiPoint Services.

Applications and Internet content

Because MultiPoint Services is a shared resource computing solution, the type and number of applications that are running on the stations can impact the performance of your MultiPoint Services system. It is important to consider the types of programs that are used regularly when you are planning your system. For example, a graphics-intensive application requires a more powerful computer than an application such as a word processor. Overloading the computer with graphics-intensive applications will likely cause lag problems throughout the entire system.

The type of content that is accessed by applications also affects the system's performance. If multiple stations are using web browsers to access multimedia content, such as full-motion video, fewer stations can be connected before adversely affecting the system performance. Conversely, if the multiple stations are using web browsers to access static web content, more stations can be connected without a significant effect on performance.

Hardware recommendations

To achieve good performance with your MultiPoint Services system under various loads, use the guidelines in the following table when you are planning and testing your system. These are the basic requirements forMultiPoint Services . The actual configuration sizing depends on your system configuration, the workload you are running, and the hardware capability. You should always validate by testing your applications and hardware.

> **NOTE**
>
> 2C = 2 cores, 4C = 4 cores, 6C = 6 cores, MT = multithreading. Processor speed should be at least 2.0 gigahertz (GHz).

Minimum recommended hardware for running default MultiPoint Server stations

APPLICATION SCENARIO	UP TO 5 STATIONS	6-8 STATIONS	9-12 STATIONS	13-16 STATIONS	17-20 STATIONS	21-24 STATIONS
Productivity Office, web browsing, line-of-business applications	CPU: 2C RAM: 2 GB	CPU: 2C RAM: 4 GB	CPU: 4C RAM: 6 GB	CPU: 4C RAM: 8 GB	CPU: 4C+MT or 6C RAM: 10 GB	CPU: 6C+MT RAM: 12 GB

APPLICATION SCENARIO	UP TO 5 STATIONS	6-8 STATIONS	9-12 STATIONS	13-16 STATIONS	17-20 STATIONS	21-24 STATIONS
Mixed Office, web browsing, line-of-business applications, and occasional video use by some users	CPU: 2C RAM: 2 GB	CPU: 2C RAM: 4 GB	CPU: 4C RAM: 6 GB	CPU: 4C+MT or 6C RAM: 8 GB	CPU: 6C+MT RAM: 10 GB	CPU: 6C+MT RAM: 12 GB
Video intensive Office, web browsing, line-of-business applications, and frequent video use by all users **Note:** Video testing was performed using 360p H.264 video at native resolution.	CPU: 4C+MT RAM: 2 GB	CPU: 6C+MT RAM: 4 GB	CPU: 8C+MT RAM: 6 GB	CPU: 12C+MT RAM: 8 GB	CPU: 16C+MT RAM: 10 GB - Thin Client: RemoteFX - USB video not recommended	CPU: 20C+MT RAM: 12 GB - Thin Client: RemoteFX - USB video not recommended

Minimum recommended hardware for running full Windows 10 virtual desktops

Running a full virtual operating system instance for each station is more compute resource-intensive than running the default MultiPoint desktop sessions, so the host hardware requirements per station are higher:

1. CPU: 1 core or thread per station
2. Solid State Drive (SSD)
    a. Capacity >= 20GB per station + 40GB for the WMS host operating system
    b. Random Read/Write IOPS >= 3K per station
3. RAM >= 2GB per station + 2GB for the WMS host operating system

BIOS CPU setting has been configured to enable virtualization – Second Level Address Translation (SLAT)

For more information about choosing the best MultiPoint Services hardware for your needs, contact your hardware vendor.

Variables Affecting MultiPoint Services System Performance

12/9/2022 • 2 minutes to read • Edit Online

There are many variables that can affect the overall performance of your MultiPoint Services system. You may want to consider these when designing your system.

Usage

- **Applications** The type and number of applications running at the same time, especially graphic-heavy or memory intensive applications will affect the overall performance of your system. For more information, see Applications and Internet Content.
- **Internet use** Consider if your users will be viewing multimedia content or web pages that use full-motion videos. This type of content can overload the system if too many users are viewing concurrently.

  > **NOTE**
  > The projection feature in MultiPoint Services, which allows teachers to project their screens onto their student monitors, is not designed to project full-motion video. The projection feature is designed for demonstration purposes, such as showing a procedure.

- **High-speed devices** If too many users are concurrently using a high-speed device, like a web camera or DVD player, this affects the overall performance of the system.

Configuration

- **CPU, GPU, and RAM** See Optimize MultiPoint Services System Performance in this guide for CPU, GPU, and RAM recommendations.
- **Network bandwidth** For RDP-over-LAN connected stations, the network bandwidth and the capability of the client (for example, a thin client, desktop PC, or laptop) is important, particularly if video is running in the user's session. If you are using USB-over-Ethernet zero clients, network bandwidth should also be a consideration. Video data for all of the devices is sent over the same Ethernet connection, so you may want to consider setting up a separate Gigabit Ethernet network when using these devices.
- **RemoteFX** For RDP-over-LAN connected stations, you may be able to use RemoteFX to greatly improve the delivery of high-definition multimedia content.
- **Display resolution** If you have heavy full-screen video usage, you may want to consider reducing the monitor resolution to maximize performance.
- **Number of USB zero clients** The total number of USB zero clients on a single root hub on the server will directly affect video performance. For more information, see Layout for USB Zero Client Connected Stations. The number of USB-over-Ethernet zero client stations that are supported might be slightly less than the number of USB zero clients.
- **USB bandwidth** Consider the USB bandwidth when you are designing your system. This is especially important for USB zero clients, which send video data over the USB connection. To optimize bandwidth, minimize the number of devices that are connected to a single USB port on the server. This applies to daisy chained stations and intermediate hubs. For more information, see Station hubs and Intermediate

hubs.

- **USB type** Using USB 3.0 instead of USB 2.0 increases the available bandwidth between the server and the intermediate hub if you are connecting more than three USB zero clients to the hub or if you are using high-bandwidth USB devices.
- **Stations** The total number of stations affects the performance. If you have heavy graphics, processing, or video needs, you may want to limit the overall number of stations. For more information, see Optimize MultiPoint Services System performance.

MultiPoint Services Site Planning

12/9/2022 • 7 minutes to read • Edit Online

You should consider the location where one or more computers running MultiPoint Services and its associated stations will be deployed.

The computer that is running MultiPoint Services role should have convenient access to a power supply and to the peripheral devices that are connected directly to it, such as a printer. Additionally, the computer running MultiPoint Services must have convenient access to a network connection. A network connection is required for accessing the Internet, and where available, a LAN.

Additional factors to consider include the following:

- Will the MultiPoint Services system be set up in a specific room, or will it be set up on a rolling cart or table, so that it can be moved from place to place?

  > **NOTE**
  >
  > If you plan to use a mobile setup, you can *associate* the stations with MultiPoint Services every time you reconnect them to make sure that each keyboard and mouse is associated with the appropriate monitor.

- Will the primary station be located next to the other stations, or will it be separate? For example, if the MultiPoint Services system is set up in a classroom, will the primary station be on the teacher's desk and the standard stations positioned elsewhere in the room? When the computer running MultiPoint Services is restarted, the primary station will have access to the startup screens. If you are concerned about this level of access in a classroom setting, you may prefer to put the primary station at the teacher's desk.
- How many stations will fit in the room?
- Do you need a network? A single server solution that uses direct video connected or USB zero client connected stations does not need a network.
- Are there enough network connections in the room to support the required number of computers running MultiPoint Services
- Where are the power outlets located?
- Will you need an additional display device, such as a projector? If you plan to use a projector, will it hang from the ceiling, or will it be positioned on a table?
- What kind of cables will be required, and how many will be needed?
- Consider how you might want to expand in the future. Will you be adding more stations?

Station layout and configuration

The physical layout of your site may affect your choice of station type. For more details about the different station types, refer to MultiPoint Stations in this guide. Multiple station types are allowed on a single MultiPoint Services. This provides you with extra flexibility to meet your installation needs.

Layout for direct-video-connected stations

- For a direct-video-connected station, the distance between the monitors and computer is limited by the video cable length.

- Using intermediate hubs or daisy-chained station hubs is supported for ease-of-deployment, but the maximum recommended number of consecutive hubs is three. This means that the maximum distance from the computer to the station hub is 15 meters, because each USB 2.0 cable has the maximum length of five meters.

> **IMPORTANT**
>
> There should always be at least one direct video connected station per computer to act as the primary station.

Layout for USB zero client connected stations

- Using intermediate hubs or daisy-chained station hubs is supported for ease-of-deployment, but the maximum recommended number of consecutive hubs is three. This means that the maximum distance from the computer to the station hub is 15 meters, because each USB 2.0 cable has the maximum length of five meters.
- The maximum recommended number of USB zero clients connected to a single intermediate hub is three.

> **NOTE**
>
> Some computers come with a generic hub on the motherboard, which has the effect of adding an additional hub between the *root hub* of the computer and the station hubs.

- If video will be heavily used, it is recommended that you connect no more than two USB zero clients to a USB port on the server. For example, if an intermediate hub is used, only two USB zero clients should be connected to it. Or if you are daisy chaining USB zero clients, only two USB zero clients should be chained together. The addition of each USB zero client to the USB port on the server decreases the video bandwidth available.
- If you plan to connect more than three USB zero clients to a single USB port on the server, using USB 3.0 between the server and the intermediate hub is recommended.

> **NOTE**
>
> It is recommended that you verify the performance by using your applications and hardware to decide how many USB zero clients you can connect to a USB port on the server.

Figure 5 MultiPoint Services system with three USB zero clients connected to a single intermediate hub

Layout for RDP-over-LAN connected stations

There are no physical distance limitations for LAN clients. As long as they are on the LAN, they can connect to the MultiPoint Services system.

Using additional hubs

Additional hubs can be used to make installation easier. There are three types of hubs that are used on a MultiPoint Services system:

- Station hubs
- Intermediate hubs
- Downstream hubs

Station hubs

A station hub is an external hub that has been associated with a MultiPoint Services station. As a minimum, the station hub will have a keyboard plugged-in to it. It may also have additional peripherals attached. A station hub can be a generic USB hub that conforms to the USB 2.0 or later specification. Station hubs should be externally powered if high-powered devices will plugin to them.

Root hub A USB hub that is built-in to the host controller on a computer's motherboard is known as a *root hub*. Station hubs are generally plugged-in to the root hub on the computer running MultiPoint Services.

> **NOTE**
>
> Root hubs should not be used as station hubs. When USB ports are built-in to a computer, often it is not possible to determine which USB root hub they are internally connected to. As such, if you plugged-in a station keyboard and mouse directly to the USB ports of the computer, you may actually be plugging-in the keyboard and mouse to different USB root hubs. To guarantee that the keyboard and mouse are on the same hub, plug-in a station hub to the computer's USB port, and then plug-in the keyboard and mouse to that station hub.

Daisy chaining stations It may be easier to connect station hubs to another station hub rather than directly to the computer. This allows you to connect a USB hub to a station hub that is already plugged-in to the computer, so that you have a station hub attached to another station hub.

There should be no more than three USB zero clients or station hubs daisy chained consecutively. Care must be taken that the USB bandwidth is not exceeded when daisy chaining station hubs.

Figure 6 MultiPoint Services system with daisy-chained stations

Intermediate hubs

An intermediate hub is a hub that is between the server and a station hub. It is typically used to increase the number of ports that are available for station hubs or to extend the distance of the stations from the computer. It is recommended that no more than two intermediate hubs are used between a station hub and the server.

Intermediate hubs must be USB 2.0 or later, and they must be externally powered. USB 3.0 is recommended between the server and the intermediate hub if you are connecting more than three USB zero clients to an intermediate hub.

Downstream hubs

A downstream hub is connected to a station hub to add more available ports for station devices. A downstream hub can be externally powered or bus-powered, depending on the devices that are plugged-in to the hub.

Figure 7 MultiPoint Services system with an intermediate hub, a station hub, and a downstream hub

Users, stations, and computers

The number of stations you will need depends on the number of people who will have to access the computers running MultiPoint Services at the same time. Similarly, the number of computers running MultiPoint Services you will need depends on the total number of stations required. Direct-video-connected stations, USB-zero-client-connected stations, and RDP-over-LAN-connected stations are all considered stations. In addition, if the split-screen functionality is used, each half is considered a station.

Power considerations

The following components require access to a power strip or outlet:

- Server
- Monitors
- Intermediate hubs (if used)
- Some USB zero clients
- Powered USB devices, such as some external storage devices and DVD drives

Sample MultiPoint Services system layouts

Depending on the available furniture, the size of the room, the number of computers that are running MultiPoint Services, and the stations in the room, there are a variety of ways that the physical stations can be arranged. The following diagrams illustrate five possible alternatives.

> **NOTE**
>
> Some of these diagrams show a projector connected to the MultiPoint Services system. This is only an example; including a projector in a MultiPoint Services system is optional.

Computer lab In this setup, the stations are arranged around the walls of the room, with the students facing the walls.

Groups In this setup, there are three computers that are running MultiPoint Services, with stations clustered around each computer.

Lecture room In this setup, the stations are set up in rows. An advantage of this setup is that all of the students face the instructor.

Activity center This setup consists of a traditional lecture-room layout for the desks, and it has a separate area with a single computer that is running MultiPoint Services with its associated stations.

Small business office In this setup, the computer that is running MultiPoint Services is placed in a central location and users throughout the office connect to it by using a local area network (LAN).

Network Considerations and User Accounts

12/9/2022 • 5 minutes to read • Edit Online

MultiPoint Services can be deployed in a variety of network environments, and it can support local user accounts and domain user accounts. Generally, MultiPoint Services user accounts will be managed in one of the following network environments:

- A single computer running MultiPoint Services with local user accounts
- Multiple computers running MultiPoint Services, each with a local user account
- Multiple computers running MultiPoint Services and that are using domain user accounts

By definition, *local user accounts* can only be accessed from the computer on which they were created. Local user accounts are user accounts that are created on a specific computer that is running MultiPoint Services. In contrast, *domain user accounts* are user accounts that reside on a domain controller, and they can be accessed from any computer that is connected to the domain. When you are deciding which type of network environment to use, consider the following:

- Will resources be shared among servers?
- Will users be switching between servers?
- Will users access database servers that require authentication?
- Will users access internal web servers that require authentication?
- Is there an existing Active Directory domain infrastructure in place?
- Who will be using the MultiPoint Manager console to manage user desktops, view thumbnails, add users, limit websites, and so on? Will this person be managing more than one server? This person must have administrative privileges on the servers.

The following sections address user account management in these networking environments.

Single MultiPoint Server with local user accounts

In environments with a single computer that is running MultiPoint Services, there is no requirement to have a network. However, to take advantage of Internet resources, the networking requirements may be as basic as a router and a connection to an Internet service provider (ISP). Network connections that are associated with a network adapter on MultiPoint Services are configured, by default, to obtain an IP address and DNS server address automatically through DHCP. Internet routers are typically configured as DHCP servers, and they provide private IP addresses to computers that connect to them on the internal network. Therefore, a single computer running MultiPoint Services may be able to connect to the internal interface of the router, obtain automatic IP information, and connect to the Internet without significant effort or configuration by an administrator.

A common way to manage users in this kind of environment is to create a local user account for each person who will access the system. Anyone who has a local user account on that computer can log on to MultiPoint Services from any station that is associated with the system. Local user accounts can be created and managed from MultiPoint Manager.

Multiple MultiPoint Server systems with local user accounts

Given that local user accounts are only accessible from the computer on which they were created, when you deploy multiple MultiPoint Services systems in an environment, you can manage local user accounts in one of two ways:

- You can create user accounts for specific individuals on specific computers running MultiPoint Services.
- You can use MultiPoint Manager to create accounts for every user on every computer running MultiPoint Services.

For example, if you plan to assign users to a specific computer running MultiPoint Services, you might create four local user accounts on Computer A (user01, user02, user03, and user04) and four local user accounts on Computer B (user05, user06, user07, and user08). In this scenario, users 01-04 can log on to Computer A from any station that is connected to it; however, they cannot log on to Computer B. The same is true for users 05-08, who would be able to log on only to Computer B, but not to Computer A. Depending on the specific deployment environment, this can be acceptable or even desirable.

However, if every user must be able to log on to any of the computers running MultiPoint Services, a local user account must be created for each user on each computer that is running MultiPoint Services. Choosing to manage users in this manner introduces certain complexities. For example, if user01 logs on to Computer A on Monday and saves a file in the Documents folder, and then the user logs on to Computer B on Tuesday, the file that was saved in the Documents folder on Computer A will not be accessible on Computer B.

Additionally, if a user has accounts on Computer A and Computer B, there is no way to automatically synchronize the passwords for the accounts. This can result in users having difficulty logging on should the account password be changed on one computer, but not the other. You can simplify user account management in this kind of network environment by assigning each user to a single computer that is running MultiPoint Services. This way, the user can log on to any of the stations that are associated with that computer and access the appropriate files.

Multiple MultiPoint Services systems with domain accounts

Domain environments are common in large network environments that include multiple servers. For example, you might join one or more computers running the MultiPoint Services role to a domain, and then use Microsoft Active Directory to manage user accounts that can be accessed from any computer in the domain. This allows for individual domain user accounts to be created and accessed from any station in any MultiPoint Services system that is joined to the domain.

When you deploy MultiPoint Services in a domain environment, there are several factors to consider:

- If domain accounts are used, they cannot be managed from MultiPoint Manager.
- By default, MultiPoint Services is configured to give each user permission to log on to only one station at a time. If you decide to allow users to log on to multiple stations at the same time using a single account, you can use the **Edit Server Settings** option in MultiPoint Manager.
- The location of domain controllers may affect the speed and reliability with which users will be able to authenticate with the domain and locate resources.

Single user account for multiple stations

MultiPoint Services has the ability to log on to multiple stations on the same computer simultaneously using a single user account. This feature is useful in environments where users are not given unique user names, and where using a single user account can simplify the management of the MultiPoint Services system.

Storing Files with MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint Services supports storing user files in the following ways:

- **On the operating system partition of the hard disk drive.** By default, MultiPoint Services stores user files on the hard disk drive with the operating system.
- **On a separate partition of the hard disk drive.** When the MultiPoint Services system is set up for the first time, you can *partition* the hard disk drive. That is, you can configure a section of the drive so that it functions as if it were a separate drive. This makes it easier to restore or upgrade the operating system without affecting user files. For more information, see Create a partition or logical drive in the Windows Server Technical Library.
- **On an additional internal or external hard disk drive.** You can attach additional internal or external hard disk drives to MultiPoint Services for saving and backing up data.
- **In a shared network folder.** To make user files available from any station, you can create a shared folder on the network. This requires another computer or server in addition to the computer running MultiPoint Services. This is the recommended method for storing files if there is a file server available.

  For small systems of 2-3 computers running MultiPoint Services with no file server available, one of the MultiPoint Services computers can act as the file server for all of the MultiPoint Services computers. You would then create user accounts for all users on the MultiPoint Services that is acting as the file server.

Protecting the System Volume with Disk Protection

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint Services provides the option to instantly erase any changes to the system volume each time the computer is started. If you enable the Disk Protection feature, any modifications to the drive, such as configuration corruption or the introduction of malware, are undone the next time the computer restarts. This is a convenient feature for administrators who want to ensure that a known "good" or "golden" software image is loaded every time. Automatic updates or software patching can be scheduled, for example, in the middle of the night. The planning consideration is whether you want to have end users be able to make changes, such as installing software, from the Internet. With this feature enabled, if you want users to be able to store files, the file share will need to be outside of the system volume.

MultiPoint Services Virtualization Support

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint Services supports the Hyper-V role in two ways:

- MultiPoint Services can be deployed as a guest operating system on a server running Hyper-V.
- MultiPoint Services can be used as a virtualization server.

Running MultiPoint Services on a virtual machine provides the use of the Hyper-V tools to manage operating systems. These tools include checkpoint and rollback features, and they allow you to export and import virtual machines. For larger installations, you can consolidate servers by running multiple MultiPoint Services virtual computers on a single physical server. Possible scenarios include:

- A single classroom or lab has more than 20 seats. Rather than deploying multiple physical computers running MultiPoint Services, you can deploy multiple virtual machines on a single physical computer.

  > **NOTE**
  >
  > You can manage multiple MultiPoint servers, whether physical or virtual, through a single MultiPoint Manager console.

- The MultiPoint server is running on a virtual machine with another server infrastructure on the same physical computer. In that case this server infrastructure centralizes the domain, security, and data for the network. The MultiPoint server provides Remote Desktop Services and centralizes the desktops.

> **NOTE**
>
> When running MultiPoint Services on a virtual machine, USB-over-Ethernet and RDP client stations are supported. Direct video and USB zero client connected stations are not supported.

For more information about the Hyper-V role, see Hyper-V.

Application Considerations

12/9/2022 • 2 minutes to read • Edit Online

Application compatibility

Any application that you want to run on a MultiPoint Services system must fulfill the following requirements:

- It should install and run on Windows Server 2016
- It needs to be session aware so each user can run an instance of the app in a MultiPoint system.

If the application does specify this requirement we recommend to try installing the application and use it in a remote desktop session.

Addressing application compatibility problems

MultiPoint Services offers the option to associate stations with full instances of Windows 10 Enterprise editions running virtually on the same host computer. For critical applications that will not run multiple instances for multiple users, or will not install on a 64-bit operating system, this can be a solution. Deploying desktops this way requires using the Virtual Desktops tab in MultiPoint Manager to:

- Enable virtual desktops
- Create a desktop template
- Customize the template with the problem application
- Associate stations with the customized template

Each station starts from the same template, so any changes are erased each time the computer starts.

> **NOTE**
>
> It is important to verify the licensing requirements for the applications you want to run on a MultiPoint. Although you are installing one copy applications might require per-user licensing.

Predeployment Checklist

12/9/2022 • 2 minutes to read • Edit Online

Use the following checklist to help you plan your MultiPoint Services deployment.

STEP	ISSUE	HELP TOPIC
1.	Verify that your applications are compatible with MultiPoint Services.	Application Considerations
2.	Determine the number of users who are likely to access, at the same time, each computer that is running MultiPoint Services so that you can estimate the number of required computers that must run MultiPoint Services.	Users, stations, and computers
3.	Understand the software applications and the web content that will likely be accessed by users and the impact that will have on system performance.	Hardware Requirements and Performance Recommendations
4.	Determine the number and type of stations that will be connected to the system.	MultiPoint Stations
5.	Determine the hardware that is needed.	Selecting Hardware for Your MultiPoint Services System and Hardware Requirements and Performance Recommendations
6.	Determine where your MultiPoint Services system will be located. Will it be set up in a single room, or will it be set up so that it can be moved from one location to another?	MultiPoint Server Site Planning
7.	Determine how the stations will be arranged.	MultiPoint Services Site Planning
8.	Verify a proper power and network infrastructure.	MultiPoint Services Site Planning
9.	Determine how user accounts will be implemented and managed.	Network Considerations and User Accounts
10.	Determine how user files will be shared and stored.	Storing Files with MultiPoint Services

Glossary

12/9/2022 • 5 minutes to read • Edit Online

associate a station To specify which monitor is used with which station and peripheral devices, such as a keyboard and mouse. For direct video connected stations, this is done by pressing a specified key on the station's keyboard when prompted to do so. For USB zero client connected stations, this typically happens automatically.

bus-powered hub A hub that draws all of its power from the computer's USB interface. Bus-powered hubs do not need separate power connections. However, many devices do not work with this type of hub because they require more power than this type of hub provides.

console mode One of the two modes MultiPoint services can start. When the system is in console mode, no stations are available for use. Instead, all of the monitors are treated as a single extended desktop for the console session of the computer system. Console mode is typically used to install, update, or configure software, which cannot be done when the computer is in station mode. See also: *station mode*.

direct-video-connected station A MultiPoint station that consists of a monitor that is directly connected to a video output on the server, and at a minimum, it includes a keyboard and mouse that are connected to the server through a USB hub.

domain user account A user account that is hosted on a domain computer. Domain user accounts can be accessed from any computer that is connected to the domain, and they are not tied to any particular computer.

downstream hub A hub that is connected to a station hub to add more available ports for station devices. A downstream hub must not have a keyboard attached to it.

externally powered hub Also known as a self-powered hub, this hub takes its power from an external power supply unit; therefore, it can provide full power (up to 500 mA) to every port. Many hubs can operate as bus-powered or externally-powered hubs.

HID consumer control device A Human Interface Device (HID) is a computer device that interacts directly with humans. It may take input from or deliver output to humans. Examples are keyboard, mouse, trackball, touchpad, pointing stick, graphics table, joystick, fingerprint scanner, gamepad, webcam, headset, and driving simulator devices. A HID consumer control device is a particular class of HID devices that includes audio volume controls and multimedia and browser control keys.

intermediate hub A hub that is between a *root hub* on the server and a station hub. Intermediate hubs are typically used to increase the number of available ports for stations hubs or to extend the distance of the stations from the computer.

local user account A user account on a specific computer. A local user account is available only on the computer where the account is defined.

multifunction hub See *USB zero client*.

MultiPoint Services system A collection of hardware and software that consists of one computer that has Windows Server 2016 installed with the MultiPoint Services role enabled and at least one MultiPoint station. For more information about system layout options, see MultiPoint Services Site Planning

partition A section of space on a physical disk that functions as if it is a separate disk.

primary station The station that is the first to start up when MultiPoint Services is started. The primary station can be used by an administrator to access startup menus and settings. When it is not being used by the

administrator, it can be used as a normal station (it does not have to be reserved exclusively for administration). The primary station's monitor must always be connected directly to a video output on the computer that is running MultiPoint Services. See also: station.

RDP-over-LAN-connected station A station that is a thin client, traditional desktop, or laptop computer that connects to MultiPoint services by using Remote Desktop Protocol (RDP) through the local area network (LAN).

root hub A USB hub that is built-in to the host controller on a computer's motherboard.

split screen A station where a single monitor can be used to display two independent user desktops. Two sets of hubs, keyboards, and mice are associated with a single monitor. One set is associated with the left side of the monitor, and the other set is associated with the right side of the monitor.

standard station In contrast to the *primary station*, which can be used by an administrator to access startup menus, standard stations will not display startup menus, and they can only be used after MultiPoint Services has completed the startup process. See also: station.

station User endpoint for connecting to the computer running MultiPoint Services. Three station types are supported: direct-video-connected, USB-zero-client-connected, and RDP-over-LAN-connected stations. For more information about stations, see MultiPoint Stations.

station hub A USB hub that has been associated with a monitor to create a MultiPoint station. It connects peripheral USB devices to MultiPoint Services. See also: *USB zero client* and *USB hub*.

station mode One of the two modes MultiPoint services can start. Typically, the MultiPoint Services system is in station mode. When in station mode, the MultiPoint Services stations behave as if each station is a separate computer that is running the Windows operating system, and multiple users can use the system at the same time. See also: *console mode*.

USB hub A generic multiport USB expansion hub that complies with the universal serial bus (USB) 2.0 or later specifications. Such hubs typically have several USB ports, which allows multiple USB devices to be connected to a single USB port on the computer. USB hubs are typically separate devices that can be *externally powered* or *bus-powered*. Some other devices, such as some keyboards and video monitors, may incorporate a USB hub into their design. See also: *USB zero client*.

USB over Ethernet zero client A USB zero client that connects to the computer through a LAN connection rather than a USB port. This client appears to the server as a USB device even through the data is sent through the Ethernet connection.

USB zero client An expansion hub that connects to the computer through a USB port and enables the connection of a variety of non-USB devices to the hub. USB zero clients are produced by specific hardware manufacturers, and they require the installation of a device-specific driver. USB zero clients support connecting a video monitor (through VGA, DVI, and so on), and peripherals (through USB, sometimes PS/2, and analog audio). The USB zero client can be *externally powered* or *bus-powered*. See also, *USB hubs*.

USB zero client connected station A MultiPoint Services station that consists of (as a minimum) a monitor, keyboard, and mouse, which are connected to the server through a USB zero client.

MultiPoint Services migration in Windows Server 2016

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2016

You can migrate from a previous release of Windows Server 2016 MultiPoint Services to the RTM version of MultiPoint Services. The following information provides preparation information and migration and verification steps.

Migration documentation and tools ease the migration of server role settings and data from an existing server to a destination server that is running Windows Server 2016. By using the process described in this guide, you can simplify the migration process, reduce migration time, increase the accuracy of the migration process, and help eliminate possible conflicts that might otherwise occur during the migration process.

What to know before you begin

Before you begin the migration process, please note the following:

- The migration process does not automatically gather or record settings for applications on the MultiPoint Services role. You should create a customized migration plan for any applications that you want to migrate. This is also true when using the virtual desktops feature in MultiPoint Services.
- This guide does not provide guidance for moving data saved in user or shared folders on the MultiPoint server. This applies to regular stations and virtual desktop stations.
- This guide does not contain instructions on how to migrate when the source server is running multiple roles. If your server is running multiple roles, you need to design a custom migration procedure that is specific to your server environment, based on information provided in the role migration guides.
- This guide does not contain information for migrating Remote Desktop Services CALS. For this information, see Migrate Remote Desktop Services Client Access Licenses (RDS CALs).

Supported migration scenarios for MultiPoint Services in Windows Server 2016

The MultiPoint Service role services is available in Windows Server 2016 Standard and Datacenter. This migration guide describes how to migrate the Multipoint Services role services from a source server running Windows Server 2016 to a destination server running the same version.

Scenarios that are not supported

The following migration scenarios are not supported:

- Migrating or upgrading from Windows MultiPoint Server 2012 and 2011.
- Migrating from a source server to a destination server that is running on operating system with a different system UI language installed.
- Migrating the MultiPoint Services role service from physical servers to virtual machines.
- Migrating any applications or application settings from the MultiPoint Server.

The impact of migration on MultiPoint Services

Be aware that the MultiPoint Services role will not be available during the migration. Plan your data migration to occur during off-peak hours to minimize downtime and reduce impact to users. Notify users that the resources will be unavailable during that time.

Migration information and steps

Use the following information to plan and carry out your MultiPoint Services migration:

- Gather the information you need for the migration.
- Migrate the MultiPoint Services role service.
- Validate the migration and do any post-migration clean-up tasks

Prepare to migrate to MultiPoint Services in Windows Server 2016

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2016

Use the following information to gather the information you need to migrate the MultiPoint Services role service from a source server running an earlier release of Windows Server 2016 to a destination server running Windows Server 2016 RTM.

At a minimum, you must be a member of the Administrators group on the source server and the destination server to install, remove, or set up MultiPoint Services.

> **NOTE**
> The steps here do not provide guidance for migrating data saved to user folder or shared folders. Ensure that users back up their data before you begin the migration.

Use MultiPoint Manager to retrieve the information needed for migration. You will need server administrator permission to use MultiPoint Manager.

Record the MultiPoint server, user, and environment settings in the migration data collection worksheet. Use the following steps to gather that information.

MultiPoint Server settings for the local server

1. Start MultiPoint Manager.
2. On the **Home** tab, select the local server, and then click **Edit server settings**.
3. Record the settings in the data worksheet.
4. Close the settings window.

Managed servers and computers

You can find the names of the managed servers and computers on the **Home** tab in MultiPoint Manager.

Station settings

If auto-logon or display orientation are configured for the station, use the following steps to retrieve that information. Otherwise you can skip this step.

To retrieve the station settings:

1. Go to the **Stations** tab in MultiPoint Manager.
2. Find a station that has "yes" in the **Auto-logon** column.
3. Select that station, and then click **Configure station**.
4. Record the user that is used for auto-logon.

To retrieve the display orientation settings, view the **station settings** for each station.

List of users

1. Click the **Users** tab in MultiPoint Manager.
2. Record the **Administrator** and **MultiPoint Dashboard User** accoutns.
3. Record the standard users.

VDI template location

If you previously enabled the VDI template feature, record the location of the VDI template. As long as the source and destination servers are on the same network, you can import the template by using MultiPoint Manager.

Next step

You're now ready to migrate to MultiPoint Services in the RTM release of Windows Server 2016.

Planning worksheet for MultiPoint Services migration

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2016

Use the following lists and tables to gather the settings you need during MultiPoint Services migration.

Source server settings

You can find the server settings on the **Home** tab in MultiPoint Manager. Place a check-mark next to each setting in use on the source server.

- Allow one account to have multiple sessions.
- Allow this computer to be managed remotely.
- Allow monitoring of this computer's desktops.
- Always start in console mode.
- Do not show privacy notification at first user logon.
- Assign a unique IP to each station.
- Allow IM between the MultiPoint Dashboard and user sessions on this computer.
- Allow orchestration of administrator and MultiPoint Dashboard user sessions.
- Allow stations to use GPU hardware rendering.

Managed servers and computers

Record the names of the managed servers and computers. You can find this information on the **Home** tab in MultiPoint Manager.

COMPUTER	COMPUTER NAME
1	
2	
3	
4	
5	
6	
7	
8	
9	

COMPUTER	COMPUTER NAME
10	

Stations

Record the local stations and their settings. You can find this information on the **Stations** tab in MultiPoint Manager.

#	STATION NAME	AUTO-LOGON USER ACCOUNT	DISPLAY ORIENTATION
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Administrators and MultiPoint Dashboard Users

Copy the user names for the administrators and MultiPoint Dashboard users. You can find this information on the **Users** tab in MultiPoint Manager.

Administrators:

- User name:
- User name:
- User name:
- User name:
- User name:
- User name:

Dashboard users:

- User name:
- User name:
- User name:
- User name:
- User name:

VDI template and virtual desktops

Record the VDI template information and the names of virtual desktops in your MultiPoint Services deployment. You can find this information on the **Virtual Desktops** tab in MultiPoint Manager.

VDI template location:

#	VIRTUAL DESKTOP NAME
1	
2	
3	
4	
5	

Migrate to MultiPoint Services in Windows Server 2016

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2016

Use the following steps plus the information you gathered in the migration planning worksheet to migrate to MultiPoint Services in Windows Server 2016.

Transfer server settings

On the destination server, open MultiPoint Manager. Click **Edit server settings**. Apply the settings according to the migration planning worksheet.

> **NOTE**
>
> If you need to enable disk protection on the destination server, wait until after you configure MultiPoint Services.

Transfer station settings

Ensure that the stations are connected to the destination server and all mapped before you apply the station settings. The stations will be automatically detected. Follow the instructions on each station screen to define the server mapping of user stations and connected USB devices. Apply your preferred station settings as outlined in the migration planning worksheet.

Migrate the VDI template

Before you can import the VDI template from the source server, enabled virtual desktops on the destination server by using MultiPoint Manager:

1. Go to the **Virtual Desktops** tab in MultiPoint Manager.
2. Click **Enabled Virtual Desktops**. The server will install the Hyper-V role, and then restart.
3. Open MultiPoint Manager and navigate back to **Virtual Desktops**.
4. Click **Import virtual desktop template**. Follow the instructions to import the template from the source server.

> **NOTE**
>
> When you import a virtual desktop template, any customization applied to the template will be reset.

Next step

Validate your new MultiPoint Services deployment.

MultiPoint Services - post-migration tasks

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2016

After you migrate to MultiPoint Services in Windows Server 2016, use the following information to validate the migration and to perform clean-up steps.

Validate the migration by running a pilot program

You can validate your MultiPoint Services migration by creating a pilot project in the production environment. Run the pilot project on the servers before you put the migrated role services into production to verify that your deployment works as you expect. Consider limiting the number of connections at first, slowly increasing the number of users accessing MultiPoint Services.

> **NOTE**
>
> Always use test accounts to test the migration. Use an account with administrative privileges and an account for a valid user.

Retire the source server

After you validate your migration, you can shut down or disconnect the source server from your network. If the server was domain-joined, remove it from the domain before you disconnect it.

Deploying MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

This guide describes how to deploy a server running MultiPoint Services and set up MultiPoint stations, install and configure your system, set up user accounts, and perform some basic administration tasks, such as turning on Disk Protection and setting up backups, before you start using your system.

> **NOTE**
>
> For additional support, see the MultiPoint Services Help, which can be opened by clicking the Help icon or F1 on any MultiPoint Manager or MultiPoint Dashboard screen.

The deployment information is organized in the following way. At a minimum, you need to complete the tasks for deploying your system and preparing your environment for users. Other tasks might or might not apply to your environment.

- Deploy a new MultiPoint Services System

  Set up your MultiPoint Services computer and stations. Install and configure MultiPoint Services; set up your stations; install drivers, updates, and software; optionally join a domain; add client licenses (CALs) for each station.

- Optional configuration tasks for a MultiPoint Services deployment

  Perform optional configuration tasks. Set up a split-screen station; add printers; enable access over a wireless LAN; create virtual desktops for stations with the Windows 10, Windows 8, or Windows 7 operating system; change the display language for the system or for individual users.

- Prepare your MultiPoint Services system for users

  Plan and create user accounts; restrict users' access to the server; for open access, configure stations for automatic logon; allow multiple sessions for shared user accounts; implement file sharing for users.

- System administration in MultiPoint Services

  Perform some basic server administration tasks before you start using the server. Turn on Disk Protection; install Server Backup; to save power, configure sleep settings; configure group policies and the Registry for a domain deployment.

Additional References

- MultiPoint Services

Deploy a new Windows MultiPoint Services system

12/9/2022 • 2 minutes to read • Edit Online

The topics in this section explain how to set up your MultiPoint Services System. You will install and configure a MultiPoint server; set up your stations; install drivers, updates, and software; optionally join a domain; activate MultiPoint Server; and add client access licenses (CALs) for each station.

> **IMPORTANT**
>
> If you have not yet planned your MultiPoint Services deployment, see Planning a Windows MultiPoint Services Deployment.

In this section

For the initial installation, we recommend that you perform the tasks in the order in which they are presented.

1. Collect hardware and device drivers needed for the installation
2. Set up the physical computer and primary station
3. Install Windows Server 2016 and enroll MultiPoint Services
4. Update and install device drivers if needed
5. Set the date, time, and time zone
6. Join the MultiPoint Services system to a domain - optional
7. Install updates
8. Attach additional stations to your MultiPoint Services computer
9. Activate Windows Server 2016 and add Remote Desktop Services CALs
10. Install software on your MultiPoint Services system

Collect hardware and device drivers needed for the installation

12/9/2022 • 2 minutes to read • Edit Online

Before you start deploying your MultiPoint Services system, you will need:

- **Hardware components for the server** - Install any additional video cards or other system components at this time.
- **Hardware components for the stations** - For information about planning stations for your environment, see Selecting Hardware for Your MultiPoint Services System.
- **The latest drivers for your video cards** - If your OEM or device manufacturer did not supply these, you will need to download them from the device manufacturer's website.
- **The latest USB zero client drivers** - If you are using USB zero client stations, you must install the latest USB zero client drivers.

> **IMPORTANT**
>
> For a MultiPoint Services installation, you must install the 64-bit version of any drivers.

> **TIP**
>
> If you are installing MultiPoint Services on a computer with a different version of Windows already installed, you should find out the video card make and model in Device Manager before you start the Windows Server installation and ensure you can get drivers which are available for Windows Server 2016. Open Device Manager, open **Computer Management** from the **Start** screen. Then, in the console tree, click **Device Manager**.

Set up the physical computer and primary station

12/9/2022 • 2 minutes to read • Edit Online

Before you install MultiPoint Services, you need to set up the primary station for your MultiPoint Services system. If you will use a local area network (LAN) connect the computer to the LAN.

A *station* is an endpoint by which MultiPoint Services is accessed. The *primary station* is the first station to start when MultiPoint Services is started. Administrators can use it to access startup menus and settings. The primary station provides access to system configuration and troubleshooting information that is only available during startup and before the MultiPoint Services system is running. After startup, you can use the primary station as you would any other station.

The primary station must be a direct-video-connected station. The following procedure describes how to connect the needed hardware to your MultiPoint Services computer.

For more information about stations, see MultiPoint Stations. For help with making hardware selections, see Selecting Hardware for Your MultiPoint Services System. For information about connecting other stations types to MultiPoint Services, see Attach additional stations to your MultiPoint Services computer.

> **NOTE**
>
> To create a video-connected station, you must use a Latin keyboard (such as an English- or Spanish-language keyboard).

To set up your primary station

1. Ensure that the computer running MultiPoint Services is turned off and unplugged.
2. Connect the power cord of the monitor to a power outlet, and connect the monitor cable to the video display port on the computer, as shown below.

3. If the station will use a USB keyboard and mouse, complete the following steps:
   a. Connect an external USB hub to an open USB port on the computer, as shown below.

   b. Connect the USB keyboard and mouse to the USB hub.

NOTE

If your MultiPoint Services computer has PS/2 ports, you can, if needed, use a PS/2 keyboard and mouse plugged directly into the computer. However, this setup has significant limitations. Users cannot use audio devices, web cams, and flash drives on PS/2 stations.

c. If you are using an externally powered hub, connect the power cable of the hub to a power outlet.

IMPORTANT

We strongly recommend the use of a powered hub. Erratic system behavior can result from under-current conditions.

Users should not attach mice and keyboards directly to the USB ports of the computer. Doing so is likely to cause the incorrect association of multiple keyboards and mice to the same station, or to no station at all.

NOTE

The host audio device on the system's motherboard is only available while MultiPoint Services is in console mode. To ensure uninterrupted audio for a station that uses an external USB hub, you must use a USB audio device plugged into the hub.

To connect the computer to the LAN

- If you have a LAN, connect your computer to your network with a network cable.

Install MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

If you are installing a server from scratch follow these instructions to install MultiPoint Services.

After you have installed Windows Server 2016 successfully sign in as Administrator. Use the Server Manager where you can enable MultiPoint Services. The Server Manager opens automatically at start-up. On the Dashboard select **Add roles and features** to enable MultiPoint Services and follow the instructions in the wizard.

In the section for the installation type you might go either with the

- Role-based or feature-based installation or
- Remote Desktop Services installation

For standard MultiPoint Services deployments we recommend to select the Remote Desktop Services installation which allows you conveniently select the MultiPoint Services role under Deployment type. For the role-based installation you will need to select **MultiPoint Services** in the list of roles. The server will reboot after successful installation.

Configure your primary station

1. On the **Create a MultiPoint Server Station** page, type the specified letter from the keyboard for that monitor. The correct key entry associates the keyboard and mouse for that station.
2. Sign in as Administrator.

Update and install device drivers if needed

12/9/2022 • 2 minutes to read • Edit Online

If you are using USB zero clients or peripherals that require drivers, you should install the drivers at this time. It's a good idea also to check **Device Manager** for any driver alerts, and install drivers for those devices.

Generally, the most current drivers are required for following types of devices:

- USB zero clients
- USB-over-Ethernet zero clients
- Disk controllers
- Network adapters
- Sound controllers
- USB host controllers
- Graphic Cards

To check for driver alerts in Device Manager

1. Open the Start screen.
2. Type **computer management**, and then click **Computer Management** in the results.
3. In the Computer Management console tree, click **Device Manager**.
4. In the system devices on the right, check for driver alerts that might affect MultiPoint Server.

To install device drivers in MultiPoint Manager

1. To open MultiPoint Manager, search for "MultiPoint Manager," and then click **MultiPoint Manager** in the results.
2. In MultiPoint Manager, click the **Home** tab, and then click **Switch to console mode**.
3. To install a device driver, double click the driver file, and follow the instructions to install the driver.
4. Repeat the preceding step to install all required drivers.

> **NOTE**
>
> If an installation requires a computer restart, you will need to switch back to console mode before you install the next driver. MultiPoint server always starts in station mode. To switch to console mode go to the **Home** tab in the MultiPoint Manager and click **Switch to console mode**.

Set the date, time, and time zone

12/9/2022 • 2 minutes to read • Edit Online

After you finish installing device drivers, set the date, time, and time zone on the MultiPoint server.

1. From the **Start** screen of the MultiPoint server, open **Control Panel**.
2. Under **Clock, Language, and Region**, click **Set the time and date**.
3. On the **Date and Time** tab, verify the date and time. If they are not correct, click **Change date and time**, update the date and time, and then click **OK**.
4. Under **Time zone**, verify the time zone. If it is not correct, click **Change time zone**, select the correct time zone, and then click **OK**.
5. Click **OK** again to save your settings and close the dialog box.

Join the MultiPoint Services computer to a domain (optional)

12/9/2022 • 2 minutes to read • Edit Online

If you will access your MultiPoint Services computer over an Active Directory domain, your next step is to add the computer to the domain.

> **IMPORTANT**
>
> You must verify your time zone before you join the computer to a domain. For instructions, see Set the date, time, and time zone.

1. From the **Start** screen, open **Control Panel**. Click **System and Security**, and then click **System**.
2. Under **Computer name, domain, and workgroup settings**, click **Change settings**.
3. On the **Computer name** tab, click **Change**.
4. In the **Computer Name/Domain Changes** dialog box, select **Domain**, enter the name of the domain, and click **OK**, and then follow the steps in the wizard to complete the process.
5. After the computer restarts, log on as Administrator and wait for MultiPoint Manager to open.

> **IMPORTANT**
>
> To ensure that your MultiPoint Services domain deployment works correctly, you will need to configure a couple of group policies and update the Registry. For information, see Configure group policies for a domain deployment.

Install updates

12/9/2022 • 2 minutes to read • Edit Online

We recommend that you install updates if available. Installing updates requires an Internet connection.

1. From the **Start** screen, open **Control Panel**.
2. In Control Panel, type **updates**, and then click **Check for updates**.
3. If the Windows Update website lists any updates that are needed on your computer, install the updates.

Attach additional stations to MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

In your MultiPoint Services environment, your users use stations to connect to MultiPoint Services and do their work. The stations are the user endpoints for connecting to the computer running Multipoint Services.

MultiPoint services supports three types of station:

- Direct-video-connected stations
- USB zero client-connected stations (and USB over Ethernet zero client connected stations)
- RDP-over-LAN connected stations

The classifications are based on a station's hardware and the type of connection that it uses. You can mix and match connection types for your stations. The only requirement is that the primary station (which you installed earlier) must be a direct-video-connected station. For more information about station setups, see MultiPoint Stations.

For instructions that explain how to set up each type of station, see the following:

- Set up a direct-video-connected station
- Set up a USB zero client-connected station
- Set up an RDP-over-LAN connected station

For a detailed comparison of station types, see Station type comparison.

NOTE

- The procedures for attaching stations do not describe how to set up intermediate hubs or downstream hubs. For information about where to install these hubs, see MultiPoint Stations.
- In some cases, you might need to create station virtual desktops, which run in virtual machines. For example, you use applications that cannot be installed on Windows Server or applications that will not run multiple instances on the same host computer. For more information, see Create Windows 10 Enterprise virtual desktops for stations.

TIP

It is useful to create your stations in the order of their physical locations so that they are identified sequentially in MultiPoint Server. If you later want to change the name of a station, you can do that in MultiPoint Manager. For more information, see Remap all stations in MultiPoint Server Help and Support.

Set up a direct-video-connected station in MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

On a direct video-connected station, the monitor is connected directly to a video port on the MultiPoint Server computer. A keyboard and mouse are then connected to a USB hub, and are associated with the monitor.

The following illustration shows a MultiPoint Server environment that has a single MultiPoint Server computer and four direct-video-connected stations. For more information, see MultiPoint Server Stations.

MultiPoint Services system with four direct video connections

> **NOTE**
>
> To configure a direct-video-connected station, you must use a Latin keyboard (such as an English or Spanish language keyboard).

To set up a direct video-connected station

1. Connect the monitor cable to the video display port on the computer, as shown below.

2. Connect the power cord of the video monitor to a power outlet.

3. Connect a USB hub to an open USB port on the computer, as shown below.

4. Connect a keyboard and mouse to the USB station hub.

5. Connect any additional peripherals, such as headphones, to the USB hub.

6. If you are using an externally powered hub, connect the power cable of the hub to a power outlet.

> **IMPORTANT**
>
> We strongly recommend the use of a powered hub. Erratic system behavior can result from under-current conditions.
>
> Users should not attach mice and keyboards directly to the USB ports of the computer. Doing so is likely to cause the incorrect association of multiple keyboards and mice to the same station, or to no station at all.

7. Follow the instructions that appear on the monitor to create the station.

If you add more than one direct video-connected station to your MultiPoint Services environment, the primary station might change. You can easily find out which direct video connected station is your primary station.

To find out which direct video-connected station is the primary station

1. Turn on all monitors that are connected directly to the computer's display adapters (video cards).

2. Start (or restart) the MultiPoint Services computer, and see which monitor displays the startup screens. That station is the primary station.

> **NOTE**
>
> In some cases, BIOS startup information is displayed on multiple monitors simultaneously. In that case, any of the monitors can be considered the "primary station" for the purpose of accessing the BIOS.

Set up a USB zero client-connected station in MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

When you use USB zero clients to create MultiPoint Services stations, the monitor for each station is connected to the video port on the USB zero client, as shown in the following illustration. For more information about this and other station types, see MultiPoint Stations.

MultiPoint Services system with one direct-video-connected station and two USB zero client-connected stations

> **IMPORTANT**
>
> Before you set up USB zero client-connected stations, be sure to install the latest drivers for your video cards and the USB zero client. Outdated drivers can prevent the MultiPoint Services configuration from completing successfully. For instructions, see Update and install device drivers if needed.

> **IMPORTANT**
>
> If you are using a USB-over-Ethernet zero client, follow the instructions from your vendor, instead of this procedure, to use the Ethernet connection to set up the device on the network.

To set up a USB zero client-connected station

1. Connect the video monitor cable to the DVI or VGA video display port on the USB zero client, as shown in the following illustration.

2. Connect the USB zero client to an open USB port on the computer.

3. Connect a keyboard and mouse to the USB zero client.

4. If you are using an externally powered USB zero client, connect the power cord of the USB zero client to a power outlet.
5. Connect the power cord of the video monitor to a power outlet.
6. If you are prompted to associate devices with the station, follow the instructions on the monitor to complete the setup. (Generally, USB zero client-connected stations are associated with stations automatically as you add them to the server.)

Set up an RDP-over-LAN connected station in MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

An RDP-over-LAN connected station is a thin client, traditional desktop, or laptop computer that connects to MultiPoint Services on a local area network (LAN) by using the Remote Desktop Protocol (RDP). For more information about this and other station types, see MultiPoint Stations.

To set up a MultiPoint station using a computer or thin client on a LAN

1. Turn on the computer that is running MultiPoint Services.
2. Ensure that the MultiPoint Server computer is connected to the LAN by a switch, router, or other networking device and has a proper IP address. (An IP address that starts with 169.254 (an APIPA address) might indicate there is an issue with the LAN connection or that the DHCP server can't be reached or is not functioning correctly.)
3. Connect the client computer or thin client to the LAN.
4. Turn on the client computer or thin client.
5. On the client computer or thin client, start Remote Desktop Connection or an equivalent application, and enter the name or IP address of the computer running MultiPoint Services.

Set up a Windows 10 device for remote management by using Connector Services

Any PC or laptop running Windows 10 can be managed remotely as long as:

- the Connector Services have been enabled
- the machine has been added to managed computers on the MultiPoint server.

On the PC running Windows 10 follow these steps to enable MultiPoint Connector:

1. In the search box, type "Turn Windows features on or off" and select the proper search result.
2. In the list of features enable **MultiPoint Connector**. This will enable MultiPoint connector services which are needed to manage the device.

On the MultiPoint server:

1. Open MultiPoint Manager and select either **Add or remove personal computers** or **Add or remove MultiPoint Services**.
2. Select the remote computers you want to manage and click **OK**. You will be prompted for admin credentials on the remote machines. Once this is done, you will see the remote machines on the MultiPoint Manager home tab.

When successfully set up Dashboard Manager can monitor users working on the managed device.

IMPORTANT

When monitoring managed Windows 10 devices administratrive users cannot be monitored except the server settings have been changed accordingly. See Edit Server Settings

Manage Client Access Licenses

12/9/2022 • 2 minutes to read • Edit Online

Every station that connects to a MultiPoint Services system, including the computer running MultiPoint Services that is used as a station, must have a valid per-user Remote Desktop *client access license (CAL)*.

If you are using station virtual desktops instead of physical stations, you must install a CAL for each station virtual desktop.

1. Purchase a client license for each station that is connected to your MultiPoint Services computer or server. For more information about purchasing CALs, visit the documentation for Remote Desktop licensing.
2. From the **Start** screen, open **MultiPoint Manager**.
3. Click the **Home** tab, and then click **Add client access licenses**. This will open the management tool for CAL licensing.

Set the licensing mode manually

If not properly configured the MultiPoint Services set-up will prompt with a notification about the grace period being expired. Follow these steps to set the licensing mode:

1. Launch **Local Group Policy Editor** (gpedit.msc).
2. In the left pane, navigate to **Local Computer Policy->Computer Configuration->Administrative Templates->Windows Components->Remote Desktop Services->Remote Desktop Session Host->Licensing**.
3. In the right pane, right click **Use the specified Remote Desktop license servers** and select **Edit**:
   - In the group policy editor dialog, select **Enabled**
   - Enter the local computer name in the **License servers to use** field.
   - Select **OK**
4. In the right pane, right click **Set the Remote Desktop licensing mode** and select **Edit**
   - In the group policy editor dialog, select **Enabled**
   - Set the **Licensing mode** to Per Device/Per User
   - Select **OK**

See Also

Manage System Tasks Using MultiPoint Manager

Install software on your MultiPoint Services system

12/9/2022 • 2 minutes to read • Edit Online

When you are logged on as an administrative user, you can install new programs either in console mode or, from a station, in station mode. However, we recommend that you install programs in console mode.

You can install new software on the computer running MultiPoint Server so that all users can run the software, or so that only you can use the software, depending on the installation and licensing options of the software.

1. Log on to the MultiPoint Services computer as an administrator.
2. Open MultiPoint Manager.
3. Click the **Home** tab, and then click **Switch to console mode**.
4. Log on as an administrator, and install your applications.
5. After you finish installing applications, switch the computer back to station mode. To do this, on the **Home** tab, click **Switch to station mode**.

Optional configuration tasks for a MultiPoint Services deployment

12/9/2022 • 2 minutes to read • Edit Online

Topics in this section explain how to perform optional configuration tasks on your MultiPoint Services system.

Set up a split-screen station Add printers Create Windows 10 Enterprise virtual desktops for stations

Set up a split-screen station

12/9/2022 • 2 minutes to read • Edit Online

You can set up a split-screen station so two users can simultaneously use the system.

Any monitor that has a resolution of minimum 1200 x720, when connected to a station that supports the split-screen feature, can be split into two stations. After a station is split, the desktop that the monitor had displayed moves to the left half of the screen, and a new station is displayed on the right half of the screen. To finish creating the new station, you will need to map a keyboard, mouse, and USB hub to the station. After a station is split, a user can log on to the left station while another user logs on to the right station.

Split-screen stations have several benefits:

- You can reduce cost and space by accommodating more users on a MultiPoint Services system.
- Two users can collaborate together, side by side, on a project.
- A MultiPoint Dashboard user can demonstrate a procedure on one station while a student follows along on the other station.

The following illustration shows a MultiPoint Services system with a split screen station (on the right).

Requirements for a split screen station

To create a split-screen station, the monitor and station must meet these requirements:

- The monitor must have a resolution of 1200 x720 or higher.
- If you are using a USB-over-Ethernet zero client, check with your hardware vendor to find out whether split-screen stations are supported. Many USB-over-Ethernet zero client devices have limitations that prevent their configuration as split-screen stations.

Setting up a split-screen station

Use the following procedures to add a second hub for a split-screen station and then split the station in MultiPoint Services. The final procedure explains how to return a split-screen station to a single station.

> **NOTE**
> When you split a station, the active session on the station is suspended. The user must log on to the station again to resume work after the split occurs.

To add a second hub with keyboard and mouse:

1. Connect a USB hub to an open USB port on the computer, as shown in the following illustration.

2. Connect a keyboard and mouse to the USB hub.

3. Connect any additional peripherals, such as headphones to the USB hub.
4. If you are using an externally powered hub, connect the power cable of the hub to a power outlet.

To split a station:

1. In the MultiPoint Manager, click the **Stations** tab.
2. Under **Station**, click the name of the station you want to split.
3. Under **Selected Item Tasks**, click **Split station**.

   The original screen moves to the left half of the monitor, and a new station's screen is created on the right half of the same monitor.
4. Create the new station by pressing the specified letter on the newly added keyboard as indicated when the **Create a MultiPoint Server Station** screen appears on the right half of the monitor.

After a station is split, one user can log on to the left station while another user logs on to the right station.

To return a split station to a single station:

1. In the MultiPoint Manager, click the **Stations** tab.
2. Under **Station**, click the name of the station you want to unsplit.
3. Under **Selected Item Tasks**, click **Unsplit station**.

Add printers

12/9/2022 • 2 minutes to read • Edit Online

Use the procedures in this topic to make a local printer available to all users on a MultiPoint Services system.

> **NOTE**
>
> If you are using domain accounts with MultiPoint Services, users can use any network printer from their stations.

1. Connect the printer to the Multipoint server.
2. Configure the printer as a shared printer:
   a. Log on to the MultiPoint Server computer as an administrator.
   b. From the **Start** screen, open **Control Panel**.
   c. In Control Panel, click **Hardware**, and then click **Devices and Printers**.
   d. Under **Printers and Faxes**, right-click the printer, and then click **Printer Properties**.
   e. Click the **Sharing** tab.
   f. Click **Share this printer**, specify a share name for the printer, and then click **OK**.

Users logged on to any station that is connected to the Multipoint Services computer will be able to see and use the printer.

Create Windows 10 Enterprise virtual desktops for stations

12/9/2022 • 7 minutes to read • Edit Online

This optional configuration in MultiPoint Services is primarily intended for situations where an essential application requires its own instance of a client operating system for each user. Examples include applications that cannot be installed on Windows Server and applications that will not run multiple instances on the same host computer.

> **NOTE**
> These Virtual Desktops, also known as VDI, are much more resource intensive than the default MultiPoint Services desktop sessions, so we recommend that you use default MultiPoint Services sessions when possible.

Prerequisites

To prepare to create station virtual desktops, ensure that your MultiPoint Services system meets the following requirements:

HARDWARE	REQUIREMENTS
CPU (multimedia)	1 core or thread per virtual machine
Solid State Drive (SSD)	Capacity >= 20GB per station + 40GB for the MultiPoint Services host operating system Random Read/Write IOPS >= 3K per station
RAM	2GB per station + 2GB for the Windows MultiPoint Server host operating system
Graphics	DX11
BIOS	BIOS CPU setting configured to enable virtualization – Second Level Address Translation (SLAT)

- **Stations** - Set up the stations for your MultiPoint Services system. For more information, see Attach additional stations to MultiPoint Services.
- **Domain** - In a domain environment, the Windows MultiPoint Server computer has been added to the domain, and a domain user has been added to the local Administrators group on the MultiPoint Services host operating system.

Procedures

Use the following procedures to:

- Create a template for virtual desktops
- Create virtual desktops from the template

- Copy an existing virtual desktop template

Create a template for virtual desktops

Before you can create a template for your virtual desktops, you must enable the Virtual Desktop feature in MultiPoint Server.

To enable the Virtual Desktop feature

1. Log on to the MultiPoint Server host operating system with a local administrator account or, in a domain, with a domain account that is a member of the local Administrators group.
2. From the **Start** screen, open MultiPoint Manager.
3. Click the **Virtual Desktops** tab, click **Enable virtual desktops**, and then click **OK**, and wait for the system to restart.

Your next step is to create a Virtual Desktop template. You are literally creating a virtual hard disk (VHD) file that you can use as a template to create station virtual desktops for MultiPoint Manager. You can either use the physical installation media for Windows or an .ISO image file to as source for the template. You can also use a .VHD of the Windows installation. Note that to use a physical installation disc, you must insert the disc before you start the wizard.

To create a Virtual Desktop template

1. Log on to the MultiPoint Server host operating system with a local Administrator account or, in domain, a domain account that is a member of the local Administrators group.
2. From the **Start** screen, open MultiPoint Manager.
3. Click the **Virtual Desktops** tab.
4. Copy a Windows 10 Enterprise .iso file to the local SSD.
5. On the Virtual Desktops tab, click **Create virtual desktop template.**
6. In **Prefix**, enter a prefix to use to identify the template and the virtual desktops created with the template. The default prefix is the host computer name.

   The prefix is used to name the template and the virtual desktop stations. The template will be <*prefix*>-t. The virtual desktop stations will be named <*prefix*>-*n*, where *n* is the station identifier.
7. Enter a username and password to use for the local Administrator account for the template. In a domain, enter the credentials for a domain account that will be added to the local Administrators group. This account can be used to log on to the template and all virtual desktop stations created from the template.
8. Click **OK**, and wait for template creation to complete.
9. The new template will be listed on the **Virtual Desktops** tab. The template will be turned off.

Your next step is to configure the template with the software and setting that you want on the virtual desktops. You must do this before you create any virtual desktops from the template.

To customize a virtual desktop template

1. Log on to the MultiPoint server host operating system with a local administrator account or, in a domain, with a domain account in the local Administrators group.
2. From the **Start** screen, open MultiPoint Manager.
3. Click the **Virtual Desktops** tab.
4. Select the template that you want to customize, click **Customize template**, and then click **OK**.

> **NOTE**
> Only the templates that have not been used to create virtual desktop stations are available. If you want to update a template that is already in use, you must make a copy of the template by using the **Import template** task, described later, in Copy an existing virtual desktop template.

The template opens in a Hyper-V **VM Connect** window, and auto-logon is performed using the built-in Administrator account.

5. At this point you can install applications and software updates, change settings, and update the administrator profile. All changes made to the template's built-in administrator profile will be copied to the default user profile in the virtual desktop stations that are created from the template.

   If you are connecting your stations over a domain, we recommend that you create a local user account and add it to the local Administrators group during customization.

   > **NOTE**
   > If the system restarts while a template is being customized, auto-logon using the built-in Administrator account might fail after the system restarts. To get around this problem, manually log on using the local Administrator account that you created, change the password of the built-in Administrator account, log off, and then log back on using the built-in Administrator account and the new password. (You will need to delete the profile that was created when you logged on using the local Administrator account.)

6. After you finish configuring your system, double-click the **CompleteCustomization** shortcut on the administrator's desktop to run Sysprep and then shut down the template. During customization, the Sysprep tool removes all unique system information to prepare the Windows installation to be imaged.

Create virtual machine desktops from the template

With your virtual desktop template configured the way you want your desktops to be, you are ready to begin creating virtual desktops. A virtual desktop will be created for each station that is attached to the MultiPoint Server computer. The next time a user logs on to a station, they will see the virtual desktop instead of the session-based desktop that was displayed before.

> **NOTE**
> This procedure only works when MultiPoint Server is in *station mode*. If the system is in *console mode*, you can switch to station mode from MultiPoint Manager. If you are using default MultiPoint settings, you can also start station mode by restarting the computer. By default, the MultiPoint Server computer always starts in station mode

To create virtual desktops for your stations

1. Log on to the Windows MultiPoint server from a remote station (for example, from a Windows computer by using Remote Desktop Connection) using a local administrator account or, in a domain, a domain account in the local Administrators group.

   > **NOTE**
   > Alternatively, you can log on to the server using a local station. However, when you create a station virtual desktop, you will have to log off the station that you used to create the virtual desktop in order to connect the other station to the new virtual desktop.

2. From the **Start** screen, open MultiPoint Manager.

3. If the computer is in console mode, switch to station mode:

a. On the **Home** tab, click **Switch to station mode**.

b. When the computer restarts, log on as Administrator.

4. Click the **Virtual Desktops** tab.

5. Select the virtual desktop template that you want to use with the stations, click **Create virtual desktop stations**, and then click **OK**.

When the task completes, each local station will connect to a virtual machine-based virtual desktop.

> **NOTE**
>
> If a user account is logged on to any of the local stations, you will need to log out of the session to get the station to connect to one of the newly created station virtual desktops.

Copy an existing virtual desktop template

Use the following procedure to create a copy of an existing virtual desktop template that you can customize and use. This can be useful in the following situations:

- To copy a master template from a network share onto a MultiPoint Server host computer so that virtual desktop stations can be created from the master template.
- To create a copy of a template that is currently in use so that you can make additional customizations.

To import a virtual desktop template

1. Log on to the MultiPoint server as an administrator.

2. From the **Start** screen, open MultiPoint Manager.

3. Click the **Virtual Desktops** tab.

4. Click **Import virtual desktop template**, and use **Browse** to select the .vhd file (template) that you want to import. When you import a template, a copy is made of the original .vhd. By default, MultiPoint Services stores .vhd files in the C:\Users\Public\Documents\Hyper-V\Virtual hard disks\ folder.

5. Enter a prefix for the new template, and then click **OK**.

6. If you are making further customizations to a local template, you might change the prefix name by incrementing a version number at the end of the prefix. Or, if you are importing a master template, you might want to add the version of the master template to the end of the default prefix name.

7. When the task completes, you can customize the template or use it as it is to create stations.

Prepare your MultiPoint Services system for users

12/9/2022 • 2 minutes to read • Edit Online

After you install and configure MultiPoint Services, and perform any additional configuration and hardware setups, you are ready to give users access to the system. You will need to plan and create user accounts. In some environments, you also need to configure stations for auto-logon and allow multiple sessions for your shared user accounts. And you need to decide how to set up file sharing for your users. All of these topics are covered in this section.

> **NOTE**
>
> After you create your user accounts and make the other configuration updates to prepare for users, we recommend that you turn on Disk Protection so that no user can inadvertently make changes to system files and settings. For more information, see Configure Disk Protection.

Use the following information to prepare your system: Plan user accounts for your MultiPoint services environment Example scenarios for user accounts creation Create local user accounts in MultiPoint Services Limit users' access to the server Configure stations for automatic logon Allow one account to have multiple sessions Enable file sharing

Plan user accounts for your MultiPoint Services environment

12/9/2022 • 5 minutes to read • Edit Online

The best way to implement user accounts in MultiPoint Services depends on the size and complexity of your deployment:

- **Local user accounts** - For a small deployment with only a few computers running MultiPoind Services and few users, you might find it most convenient to use *local user accounts* that are created on MultiPoint Services. You can create an individual account for each person who will use the system, or create a generic account for each station, which anyone can use to log on. MultiPoint Services administrators create and manage local user accounts by using MultiPoint Manager. The local accounts can be administrators, have limited administrative rights, or be regular users with no access to the MultiPoint Services Desktop or MultiPoint Manager.
- **Domain accounts** - If your environment has many computers running MultiPoint Services and many users, you probably will find it more useful to set up an Active Directory Domain Services (AD DS) domain and use *domain user accounts*, which enable a user to access her own user profile and settings from any station in the domain. Domain user accounts must be created on the domain controller by a domain administrator.

> **NOTE**
>
> The following sections discuss scenarios that you might implement for local user accounts in MultiPoint Services. If you are using domain user accounts, see the "One or more MultiPoint servers in a domain network environment" scenario in Example scenarios: MultiPoint Services user accounts.

Planning local user accounts

The following sections consider the advantages, disadvantages, and requirements for several ways to implement individual or shared local user accounts in your Windows MultiPoint Services environment.

Use individual local user accounts

When creating local user accounts, you have the option two approaches. Assign each user to a particular server running MultiPoint Services and creating a single account for each user. Or create local user accounts for all user on every computer running Multipoint services. A key advantage of implementing individual user accounts is that each user has his or her own Windows desktop experience that includes private folders for storing data.

From a system management perspective, assigning users to a specific MultiPoint Services computer might be more convenient. For example, if you have two MultiPoint servers with five stations each, you might create local user accounts as illustrated in the following table.

Table 1: Assigning local user accounts to specific computers running MultiPoint Services

COMPUTER A	COMPUTER B
UserAccount_01	UserAccount_06
UserAccount_02	UserAccount_07

COMPUTER A	COMPUTER B
UserAccount_03	UserAccount_08
UserAccount_04	UserAccount_09
UserAccount_05	UserAccount_10

In this scenario, each user has a single account on a particular computer. Therefore, everyone who has a local account on Computer A can log on to her or his account from any station associated with Computer A. However, these users cannot access their accounts if they use a station associated with Computer B, and vice versa. An advantage to this approach is that, by always connecting to the same computer, users can always find and access their files.

In contrast, it is also possible to replicate individual user accounts on all computers running MultiPoint Services, as illustrated in the following table.

Table 2: Replicating user accounts on all computers running MultiPoint Services

COMPUTER A	COMPUTER B
UserAccount_01	UserAccount_01
UserAccount_02	UserAccount_02
UserAccount_03	UserAccount_03
UserAccount_04	UserAccount_04
UserAccount_05	UserAccount_05

An advantage of this approach is that users have a local user account on every available MultiPoint Services. However, the disadvantages might outweigh this advantage. For example, even if the user name and password for a particular person are the same on both computers, the accounts are not linked to each other. Therefore, if a user logs on to his or her account on Computer A on Monday, saves a file, and then logs on to his or her account on Computer B on Tuesday, he or she will not be able to access the file previously saved on Computer A. Additionally, replicating user accounts on multiple computers increases the administrative overhead and storage requirements.

Use generic local user accounts

If your MultiPoint Services system is not connected to a domain, and you do not want to create an individual account for each user, you can create generic accounts for each station. For example, if you have two computers running MultiPoint Services, and five stations are associated with each computer, you might decide to create user accounts similar to those shown in the following table.

Table 3: Creating generic user accounts, one account per station

COMPUTER A	COMPUTER B
Computer_A-Station_01	Computer_B-Station_01
Computer_A-Station_02	Computer_B-Station_02

COMPUTER A	COMPUTER B
Computer_A-Station_03	Computer_B-Station_03
Computer_A-Station_04	Computer_B-Station_04
Computer_A-Station_05	Computer_B-Station_05

In this scenario, every station account has the same password, and both the passwords and generic user account names are available to all users. An advantage to this approach is that the overhead of managing user accounts is likely to be less than if using individual accounts, because there typically are fewer stations than users. Additionally, the overhead caused by replicating user accounts on every server is eliminated.

Another option is to create generic accounts on each server. Every user logs on to a server as the same account. To allow this, you must enable multiple sessions per account. You can further simplify by using the same account name and password on all servers. This simplifies logon for the users, who need only know one account name and password to use any station on any server. It should be noted that in this scenario all users can see any change that any user makes. For example, if a file is saved to the desktop, all users can see the file.

IMPORTANT

It is important to understand that when users share a user account, either one per server or one per station, files saved on the server – even files saved in My Documents - are not private. Any user who logs on with the account has access to those files. When you use one account per station, if a user saves files to My Documents on one station, the user does not have access to those files on a different station. The same occurs when logging on to different MultiPoint Services computers.

To enable users to access their files from any station, you can use a file server, create a file share for each user account, or let users store their personal documents on a USB flash drive or other private storage device. Individual USB flash drives enable individual users to store private documents even if they are sharing a user account on a MultiPoint Services.

Example scenarios: MultiPoint Services user accounts

12/9/2022 • 4 minutes to read • Edit Online

What do you need to do to implement the user account scenario that you chose for your MultiPoint Services environment? The following tables describe each task to perform to configure user accounts and prepare stations for shared or individual user accounts on a stand-alone MultiPoint computer or on networked servers in a workgroup or an Active Directory domain. Choose the scenario that applies to your environment. Then follow the links in the table to complete each required configuration task.

> **NOTE**
>
> If you have not yet decided how to set up your user accounts, see Plan user accounts for your MultiPoint Services environment for more information about how each choice affects users.

Single MultiPoint Services computer in a stand-alone environment (no network)

SCENARIO	TASKS
My users do not need to log on. The stations can be available to anyone who walks up to them. They do not need an individual Windows desktop experience that includes private folders for storing data or personalized desktops.	1. Create a single local user account (For instructions, see Create local user accounts.) 2. Allow one account to have multiple sessions 3. Configure stations for automatic logon
My users can all share the same user logon. They do not need an individual Windows desktop experience that includes private folders for storing data or personalized desktops.	1. Create a single local user account (For instructions, see Create local user accounts.) 2. Allow one account to have multiple sessions
My users must have their own individual Windows desktop experience.	Create a local user account for each user (For instructions, see Create local user accounts.)

Multiple MultiPoint Services computers on a network, but with no domain

SCENARIO	TASKS
My users do not need to log on. The stations can be available to anyone who walks up to them. They do not need an individual Windows desktop experience that includes private folders for storing data or personalized desktops.	1. Create a single local user account on each server. (For instructions, see Create local user accounts.) 2. Allow one account to have multiple sessions on each server 3. Configure stations for automatic logon on each server
My users can all share the same user logon. They do not need an individual Windows desktop experience that includes private folders for storing data or personalized desktops.	1. Create a single local user account on each server. (For instructions, see Create local user accounts.) 2. Allow one account to have multiple sessions on each server.

SCENARIO	TASKS
My users must have their own individual Windows desktop experience. - **Option A** - My users will always use local stations connected to the same MultiPoint Services computer. - **Option B** - My users will use local stations on more than one MultiPoint Services computer. - **Option C** - My users will use remote clients on the LAN.	- **Option A** - Create a single local user account on each server for the users of that server. (For instructions, see Create local user accounts.) - **Option B** - Create local user accounts for every user on every server. **Note:** This means that each user will have a profile on each server. In other words, if they save a file in My Documents while logged onto Server A's station, they will not see the file when logging onto Server B's station. (For instructions, see Create local user accounts.) - **Option C** - Assign each user to a specific MultiPoint Services computer. Create local user accounts for the assigned users on each server. (For instructions, see Create local user accounts.)

One or more MultiPoint Services computers in a domain network environment

SCENARIO	TASKS
My users do not need to log on. The stations can be available to anyone who walks up to them. They do not need an individual Windows desktop experience that includes private folders for storing data or personalized desktops.	1. Create a domain account to log onto the servers. 2. Allow one account to have multiple sessions on each server. 3. Configure stations for automatic logon on each server.
My users can all share the same user logon. They do not need an individual Windows desktop experience that includes private folders for storing data or personalized desktops.	1. Create a domain account for a group or for each user. 2. Allow one account to have multiple sessions on each server.
My users must have their own individual Windows desktop experience. - **Option A** - Any user with a domain account can use the MultiPoint Services computer. - **Option B** - I want to limit which domain accounts can access the server.	- **Option A** - No setup is required. By default, all domain users have access to any MultiPoint Services computer on the network. - **Option B** - Limit the access of domain user accounts to the MultiPoint Services computer. For instructions, see Limit users access to the server.
I want to use local user accounts and manage them separately from my domain accounts. For example, you want someone to manage MultiPoint Services but not the domain or you do not want to give domain accounts to all MultiPoint Services users.	Create one or more local user accounts on each server. (For instructions, see Create local user accounts.) **Note:** This means that each user account will have a profile on each server. In other words, if they save a file in My Documents while logged onto Server A's station, they will not see the file when logging onto Server B's station.

Create local user accounts

12/9/2022 • 2 minutes to read • Edit Online

Three levels of local user accounts can be created in using the MultiPoint Manager: Standard User accounts; MultiPoint Dashboard users, who have limited administrative rights; and full Administrative User accounts.

Use the following procedure to create a local user account on a MultiPoint server. If your environment includes multiple MultiPoint servers, and you want the user to be able to log on to any station on any server, you need to create a local user account on each of your servers. That setup has some limitations. In a domain environment, you can also let users use their domain accounts. For an overview of your options, see Plan user accounts for your Windows MultiPoint Services environment.

1. Log on to the server as an administrator, and open MultiPoint Manager.
2. Click the **Users** tab, and then click **Add user account**.

   The Add User Account Wizard opens.
3. Enter an account name and password for the new user account, and then click **Next**.
4. Select the type of user account that you want to create:
   - **Standard User** - Can log on to a station and perform user tasks, but has no access to MultiPoint Manager or the MultiPoint Server Dashboard, and cannot shut down the system.
   - **MultiPoint Dashboard User** - Has limited administrative rights. A Dashboard user can open the Dashboard and perform tasks such as logging users off the system or shutting down the MultiPoint Server computer, but the user does not have access to MultiPoint Manager.
   - **Administrative User** Has full administrative rights in MultiPoint Server. For example, an administrative user can run MultiPoint Manager, add and delete users, modify system settings, and update drivers.
5. Click **Next**, and then click **Finish** to create the user account.

Limit users' access to the Multipoint server

12/9/2022 • 2 minutes to read • Edit Online

Whether you join MultiPoint server to an Active Directory domain or you use local user accounts, all users have access to MultiPoint server by default. Before you allow users to log on to stations in your MultiPoint Services environment, you should restrict access to the server.

Any user in the Remote Desktop Users group can log on to MultiPoint server. By default, the user group Everyone is a member of the Remote Desktop Users group, and therefore every local user and domain user can log on to the MultiPoint Server. To restrict access to MultiPoint Server, remove the Everyone user group from the Remote Desktop Users group, and then add specific users or groups to the Remote Desktop Users group.

Add or remove users or groups to the Remote Desktop Users group

1. From the **Start** screen, open **Computer Management**.
2. In the console tree, under **Local Users and Groups**, click **Groups**.
3. Double click **Remote Desktop Users**, and follow the instructions to add or remove users.
   - To restrict general access to the server, remove the Everyone group.
   - To give your MultiPoint server users access to stations, add each local account or each domain user or group account to the Remote Desktop Users group.

Configure stations for automatic logon

12/9/2022 • 2 minutes to read • Edit Online

If you want your stations to be available to anyone – and your users do not need private folders to store their personal data or personalized desktops – you can configure the stations for automatic logon. Auto-logon automatically logs on a user account that has been specified in the auto-logon settings when the MultiPoint Services starts.

1. From the **Start** screen, open **MultiPoint Manager**.
2. Click the **Stations** tab, and then click the name of the station that you want to configure for auto-logon.
3. In the right pane, click **Configure auto-logon**.

   The Configure Auto-Logon page opens.
4. Select the **Auto-logon using the following information** check box, and then enter the user account and password to use for auto-logon. Click **OK**.

   > **NOTE**
   >
   > The user account that you use for auto-logon must have a password.

> **NOTE**
>
> To temporarily log on to a station that is set up for automatic logon with a different user account, hover over the top right corner of the screen to display a vertical menu, click the Settings charm, click the Power icon, and then hold the SHIFT key and click **Disconnect**. Hold down the SHIFT key until a logon prompt appears.

Allow one account to have multiple sessions

12/9/2022 • 2 minutes to read • Edit Online

To enable a group of users use a shared account on multiple stations at the same time, configure the MultiPoint server to allow one account to be logged on to multiple stations simultaneously. By default, if a user logs on to a second station with a shared user account, the user account is logged off the first station.

1. From the **Start** screen, open **MultiPoint Manager**.
2. Click the **Home** tab.
3. In the **Computer** column, click the name of the MultiPoint Server computer, and then, in the right pane, click **Edit server settings**.
4. Select the **Allow one account to have multiple sessions** check box, and then click **OK**.

Enable file sharing in MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

You can allow users on your MultiPoint stations to share files in two ways:

- **If you have a file server on the network,** it is recommended that you create a shared folder on the file server.
- **If you have a small network of 2-3 MultiPoint servers, with no dedicated file server,** one of the MultiPoint servers can act as the file server for all the remaining computers running MultiPoint services. Create a shared folder on that server, and then create local user accounts for all users on that server. The shared folder can be on the original internal drive, or you can attach additional internal or external drives to the computer.

System administration in MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

Before you start using your MultiPoint Services system, it's a good idea to do some basic system administration.

Use the following information:

Configure Disk Protection Install Server Backup on your MultiPoint Services computer

Configure Disk Protection

12/9/2022 • 4 minutes to read • Edit Online

You can use Disk Protection in Multipoint Services to protect your system volume from unintended updates, to schedule Windows Updates to be retained while Disk Protection is active, to temporarily disable Disk Protection, and to uninstall Disk Protection.

By enabling Disk Protection in MultiPoint Services, you can protect the system volume (the drive where Windows is installed, usually C:) from unwanted changes. When Disk Protection is enabled, changes made to the system volume are stored in a temporary location so that simply restarting the computer discards them and automatically returns the system to the previous known-good state.

The administrator can easily install software or make configuration changes by temporarily disabling disk protection. In order to keep the system current with Windows Updates and anti-malware definitions, Disk Protection schedules a maintenance window to download and install updates. The administrator can also provide a custom script to run during the maintenance window to accommodate any maintenance needs beyond Windows Update.

Enable Disk Protection

Before you enable Disk Protection, make sure all applications and drivers are installed and up to date, and move your user profiles to a volume that will not be protected. If you need to make manual updates after you enable Disk Protection, you can temporarily disable Disk Protection. However, it's easiest to get the system into an ideal state before Disk Protection is turned on.

1. Log on to the server running MultiPoint Services as an administrator.
2. Before you enable Disk Protection:
   - Ensure the MultiPoint Services system is in exactly the state in which you want it to remain. For example, ensure that installed software, system settings, and updates are correct.
   - Move user profiles to a volume that is not protected, or set up a shared file location off the system volume as described in Enable file sharing in MultiPoint Services.
3. From the **Start** screen, open **MultiPoint Manager**.
4. Click the **Home** tab, click **Enable disk protection**, and then click **OK**.

When Disk Protection is enabled for the first time, the system is prepared by installing a driver and creating a cache file on the system volume. The cache file will temporarily store any changes made to the system volume while Disk Protection is active. Because system updates are stored in the cache file, they do not alter the protected contents of the volume outside the cache file. Each time the system starts, the cache file is reset, which discards any changes stored there since the previous system start. Thus, the system always starts in the same state as when Disk Protection was enabled.

Windows needs to update a few system files – including the system pagefile, crash dump location, and event logs. Those files are not discarded when Disk Protection is enabled. To accomplish this, a new volume named DpReserved is created when Disk Protection is enabled for the first time, and those files are moved to that volume. The DpReserved partition is not protected, so writes to those files persist through restarts, even when Disk Protection is enabled.

Schedule software updates

If Windows is configured to automatically install Windows Updates, Disk Protection allows these updates at the configured time, and does not discard the updates. For example, if Windows updates are scheduled for 3:00 a.m., Disk Protection checks for updates each day at 3:00 a.m. If any updates are found, MultiPoint Services temporarily disables Disk Protection, applies the updates, and then re-enables Disk Protection.

1. In MultiPoint Manager, display the **Home** tab, and then click **Schedule software updates**.
2. In the Schedule Software Updates dialog box, click **Update at**, and select a time for updates - for example, **3:00 AM**.
3. Select the **Run Windows Update** check box.
4. If your organization runs its own update script, select the **Run the following program** check box, and specify the location of your organization's update script.
5. Select a maximum time to allow updates to run.
6. Under **When finished**, choose whether to have the system return to its previous power state or shut down after applying updates.
7. Click **OK**.

Temporarily disable Disk Protection

If an administrator needs to install software, change system settings, or perform other maintenance tasks that involve system updates, they can temporarily disable Disk Protection. After the changes are made, re-enable Disk Protection. During system restarts, the system will retain its state when Disk Protection was enabled.

1. In MultiPoint Manager, click the **Home** tab.
2. On the Home tab, click **Disable disk protection**, and then click **OK**.

> **NOTE**
>
> Remember to re-enable Disk Protection after maintenance is complete. The system will not be protected again until the administrator explicitly re-enables Disk Protection.

Uninstall Disk Protection

Uninstalling Disk Protection removes the driver and the cache file, so you should only do this if you want to stop using Disk Protection long-term. If you simply want to perform maintenance or stop protection temporarily, use the Disable disk protection task instead.

You can uninstall Disk Protection whether it is enabled or disabled.

1. In MultiPoint Manager, click the **Home** tab.
2. On the Home tab, and click **Uninstall disk protection**, and then click **OK**.

   After you click **OK**, the computer restarts. The uninstallation process requires several restarts, during which the driver and cache file are removed. The DpReserved partition remains, and the pagefile, crash dump location, and event log files remain configured to use the DpReserved partition.

Install Server Backup on your MultiPoint server

12/9/2022 • 2 minutes to read • Edit Online

It is recommended that you consider a backup and recovery plan for your MultiPoint servers.

A good backup and recovery plan is important for any size environment. Windows Server Backup is a feature in Windows Server 2016 that provides a set of wizards and other tools for you to perform basic backup and recovery tasks for the server on which it is installed. You can use Windows Server Backup to back up a full server (all volumes), selected volumes, the system state, or specific files or folders, and to create a backup that you can use to rebuild your system.

You can recover volumes, folders, files, certain applications, and the system state. And, for disasters like hard disk failures, you can rebuild a system either from scratch or by using alternate hardware. To do this, you must have a backup of the full server or just the volumes that contain operating system files and the Windows Recovery Environment. This restores your complete system onto your old system or onto a new hard disk.

A key feature of Windows Server Backup is the ability to schedule backups to run automatically.

Use the following procedures to set up the type of backup you require.

Install backup and recovery tools

1. From the **Start** screen, open **Server Manager**.
2. Click **Add Roles and Features** to start the Add Roles Wizard. Then click **Next** after you review the **Before you begin** notes.
3. Select the **Role based or feature based installation** option, and then click **Next**.
4. Select the local computer that you are managing, and click **Next**.

   The Add Features Wizard opens.
5. On the **Select Features** page, expand Windows Server Backup Features, select the check boxes for **Windows Server Backup** and **Command-line Tools**, and then click **Next**.

   > **NOTE**
   >
   > Or, if you just want to install the snap-in and the Wbadmin command-line tool, expand **Windows Server Backup Features**, and then select the **Windows Server Backup** check box only—make sure the **Command-line Tools** check box is clear.
6. On the **Confirm Installation Selections** page, review your choices, and then click **Install**.

   If any errors occur during the installation, the **Installation Results** page will note the errors.
7. After the installation completes successfully, you should be able to access these backup and recovery tools:

   - To open the Windows Server Backup snap-in, on the **Start** screen, type **backup**, and then click **Windows Server Backup** in the results.
   - To start the Wbadmin tool and view syntax for its commands: On the **Start** screen, type **command**. In the results, right-click **Command Prompt**, click **Run as administrator** at the

bottom of the page, and then click **Yes** at the confirmation prompt. At the command prompt, type **wbadmin /?** and press ENTER. You should see command syntax and descriptions for the tool.

Configure backups using Windows Server Backup

- Follow the guidance in Backing Up Your Server.

Configure group policies for a domain deployment

12/9/2022 • 2 minutes to read • Edit Online

To ensure that your domain deployment of MultiPoint Services works properly, apply the following group policy settings to the WMSshell user account on a MultiPoint Services system.

> **IMPORTANT**
>
> Some group policy settings can prevent required configuration settings from being applied to MultiPoint Services. Be sure that you understand and define your group policy settings so that they work correctly on MultiPoint Services. For example, a Group Policy setting that prevents Autologon could present problems with MultiPoint Services logon behavior.

Update group policies for the WMSshell user account

The WMSshell user account is a system account which MultiPoint services uses to sign-in into the console, where the actual stations are created. This account is not meant to be managed by MultiPoint Manager.

> **NOTE**
>
> To find out how to update group policies, see Local Group Policy Editor.

POLICY: User Configuration > Administrative templates > Control Panel > **Personalization**

Assign the following values:

SETTING	VALUES
Enable screen saver	Disabled
Screen saver timeout	Disabled Seconds: xxx
Password protect the screen saver	Disabled

POLICY: Computer Configuration >Windows Settings >Security Settings >Local Policies >User Rights Assignment > **Allow log on locally**

SETTING	VALUES
Allow log on locally	Ensure that the list of accounts includes the WMSshell account. **Note:** By default, the WMSshell account is a member of the Users group. If the Users group is in the list, and WMSshell is a member of the Users group, you do not need to add the WMSshell account to the list.

> **IMPORTANT**
> When you set any group policies, make sure that the policies do not interfere with automatic updates and error Windows error reporting on the MultiPoint server. These are set by the **Install updates automatically** and **Automatic Windows Error Reporting** settings that were selected during Windows MultiPoint Server installation, configured in MultiPoint Manager using **Edit server settings**, or configured in scheduled updates for Disk Protection.

Update the Registry

For a domain deployment of MultiPoint Services, you should update the following registry subkeys.

> **IMPORTANT**
> Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

To update Registry subkeys for a domain deployment of MultiPoint Services

1. Open Registry editor. (At a command prompt, type **regedit.exe**, and press ENTER.)
2. In the left pane, locate and then select the following registry subkey:

   HKEY_USERS<SIDofWMSshell>\Software\Policies\Microsoft\Windows\Control Panel\Desktop

   where '<SIDofWMSshell>' is the security identifier (SID) for the WMSshell account. To identify the user, run the following PowerShell command.

   `Get-ADObject -Filter "objectSid -eq '<SID>'"` Learn more about Get-ADObject.
3. In the list on the right, update the following subkeys.

SUBKEY	VALUE NAME	VALUE DATA
ScreenSaveActive	REG_SZ	0 (zero)
ScreenSaveTimeout	REG_SZ	120
ScreenSaverIsSecure	REG_SZ	0 (zero)

   To update a Registry subkey:

   a. With the Registry key selected in the left pane, right-click the subkey in the right pane, and then click **Modify**.

   b. In the Edit String dialog box, type a new value in **Value data**, and then click **OK**.
4. After you finish updating Registry subkeys, restart the computer to activate the changes.

Managing MultiPoint Services

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint™ Services allows multiple users, each with their own independent Windows experience, to simultaneously share one computer. User stations, consisting of a monitor, keyboard, and mouse, are directly connected to the host computer through USB, video cables, or the network.

Use the following information to learn about the tasks that you can perform in MultiPoint Manager and MultiPoint Dashboard, such as how to manage MultiPoint Services stations by using MultiPoint Manager, and how to use MultiPoint Dashboard daily.

- Managing Your MultiPoint Services System
- Manage Station Hardware
- Manage System Tasks Using MultiPoint Manager
- Manage User Stations
- Manage User Accounts
- Manage Virtual Desktops
- Manage User Files
- Manage User Desktops Using MultiPoint Dashboard
- Manage MultiPoint Systems Using MultiPoint Dashboard

Additional References

- MultiPoint Services

Managing Your MultiPoint Services System

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint Services enables multiple stations to be connected to one computer. A traditional station consists of a *station hub* or zero client, monitor, keyboard, and mouse. Network-connected Remote Desktop Protocol (RDP) clients are also supported.

The following illustration shows an example layout of a MultiPoint Services system that contains four *stations*. Such a setup enables multiple users to use the computer at the same time, and to perform independent work or a group activity.

MultiPoint Services includes MultiPoint Manager, which helps you, as an administrative user, to monitor and manage your MultiPoint system, and MultiPoint Dashboard, which provides day-to-day administrative functionality. The topics included in this Help guide describe many of the tasks that you can perform in MultiPoint Manager and MultiPoint Dashboard.

See Also

Manage User Desktops Using MultiPoint Dashboard Privacy and Security Considerations

Privacy and Security Considerations

12/9/2022 • 2 minutes to read • Edit Online

Because your MultiPoint Services system is, by design, a shared computing environment, you should consider the following privacy and safe computing issues.

Privacy in a MultiPoint Services system

The capabilities of MultiPoint Services to share or keep private user documents may be new to you, other *administrative users*, *MultiPoint Dashboard users*, or *standard users* on your MultiPoint Services system. In MultiPoint Manager, you can see screen activity on all active standard user desktops. Standard users are notified when they log on to the MultiPoint Services system, and must accept this monitoring in order to proceed. For more information about how to share content or keep it private, see Manage User Files.

Security in a MultiPoint Services system

As an administrative user of your MultiPoint Services system, become familiar with the security and safe computing capabilities in Windows. These include Windows automatic updating and support for firewalls, virus protection, and spyware and other malware protection.

Shared computing resources, such as a MultiPoint Services system, may be prone to security threats due to the potentially large number of users of the system and the easy access to station hardware devices and wires. A malicious user may attempt to insert a keystroke logger or similar device at a MultiPoint Services station hub. If you see devices attached to any ports on your MultiPoint Services system that you do not recognize, consider it suspect and follow the security escalation guidelines of your organization.

See Also

Manage User Files Managing Your MultiPoint Services System

Manage Station Hardware

12/9/2022 • 2 minutes to read • Edit Online

A MultiPoint Services system consists of a single computer and at least one station. Station hardware typically consists of a station hub, mouse, keyboard, and video monitor. Stations are typically physically wired to the computer.

The following illustration shows an example of the layout of a MultiPoint Services system that has four stations. Each station is connected to the MultiPoint Services computer by using a USB hub and multi-monitor video cards. This illustration does not represent stations that are connected by using multifunction hubs.

The topics in this section describe how you can view the status of the hardware connected to your MultiPoint Services system, and provide detailed information about the types of USB devices and other peripheral hardware devices that you can use to set up a MultiPoint Services station. The following is a brief description of the topics in this section that can help you select hardware and set up your MultiPoint Services station.

View Hardware Status

In MultiPoint Manager, you can use the **Stations** tab to view the status of the stations and hardware devices that are connected to the MultiPoint Services computer. For more information about how to view the status of your MultiPoint Services computer and the hardware devices that are connected to it, see the View Hardware Status topic.

Work with USB Devices

When USB devices and other peripheral hardware devices are connected to the MultiPoint Services system, they function differently when they are connected to the MultiPoint Services computer than when they are connected to a MultiPoint Services station. The Work with USB Devices topic describes how different hardware devices might function in these scenarios and provides detailed information about how to work with station hubs.

Work with Video Devices

The Work with Video Devices topic discusses how video devices, such as a monitor or projector, function when they are connected to a computer in your MultiPoint Services system or to a MultiPoint Services station.

Set Up a Station

The Set Up a Station topic describes how to connect peripheral hardware devices to a MultiPoint Services station hub to create a MultiPoint Services station. MultiPoint Services supports two types of station hubs:

- An externally powered or bus-powered multi-port *USB hub* that can support a mouse, keyboard, and other USB peripheral devices
- A *multifunction hub* that can include an integrated video controller and ports for mouse, keyboard, and audio peripheral devices

Both types of station hubs connect to the computer by way of a USB cable. Procedures in the Set Up a Station topic describe how to connect hardware devices to each type of station hub.

See Also

View Hardware Status Work with USB Devices Work with Video Devices Set Up a Station

View Hardware Status

12/9/2022 • 2 minutes to read • Edit Online

In MultiPoint Manager, use the **Stations** tab to view *station* information, such as:

- Station name
- Required hardware to make each station usable (typically, hardware would include a video monitor, *station hub*, keyboard, and mouse)
- Additional peripheral hardware devices associated with a station
- Notification of required hardware that is missing or not working at a station is displayed in the relevant column
- Names of users who are currently connected to the MultiPoint Services system

> **TIP**
>
> If the stations in your MultiPoint Services system are physically arranged in a way that you intend to keep (for example, around a circular table), you may find it helpful to adhere station name or number labels, such as stickers or cards, to help identify the video monitor or hub of each station. That way, you and other users of the stations can more easily refer to and distinguish stations by their unique identifying name or number.

> **NOTE**
>
> The **Stations** tab is unavailable when the system is in console mode.

See Also

Manage Station Hardware Switch Between Modes

Work with USB Devices

12/9/2022 • 4 minutes to read • Edit Online

You can connect devices to either the computer in your MultiPoint Services system or to a MultiPoint station hub. The location where a device is connected, and the type of device, affects whether a device is available to all users on the system, only to individual users, or not available to any users. The following are examples of the different connection types:

- If you connect a device directly to the computer, such as a printer or USB mass storage device, the device can be accessed by all session users on the MultiPoint Services system. Virtual desktop station users will not be able to access the devices connected directly to the computer.
- If you connect a device to a station hub, such as a keyboard, mouse, *audio device*, or mass storage device, the device is available only to the user logged on to that MultiPoint Services station.
- If you connect certain types of devices to the computer, such as a keyboard or mouse, the devices are not available to any users on the system.

The following table shows a list of devices and how they behave, depending on where they are connected to the system. Information about how to connect station hubs is described in Working with station hubs. More information about how to connect video monitors to a station is described in Work with Video Devices.

DEVICE	BEHAVIOR WHEN IT IS CONNECTED DIRECTLY TO THE COMPUTER	BEHAVIOR WHEN IT IS CONNECTED TO A STATION	NOTES
Keyboard	We do not recommend connecting a keyboard directly to the computer.	Accessible only to the station user.	If the keyboard contains a USB port, then the USB hub inside the keyboard may be the station hub. Other USB devices attached to that port are available only to user who is using that keyboard. Some station hubs are equipped with a PS/2 mouse port that is converted into a USB connection inside the hub.
Mouse	We do not recommend connecting a mouse directly to the computer.	Accessible only to the station user.	Some station hubs are equipped with a PS/2 mouse port that is converted into a USB connection inside the hub.
USB hub	See Working with station hubs.	See Working with station hubs.	
Video monitor	See MultiPoint Services Video Devices.	See MultiPoint Services Video Devices.	

DEVICE	BEHAVIOR WHEN IT IS CONNECTED DIRECTLY TO THE COMPUTER	BEHAVIOR WHEN IT IS CONNECTED TO A STATION	NOTES
Audio output devices such as headphones	We do not recommend connecting an audio output device directly to the computer.	Accessible only to the station user.	Some station hubs are equipped with an analog audio port that is converted into a USB audio connection inside the hub.
Audio input devices such as microphones	We do not recommend connecting an audio input device directly to the computer.	Accessible only to the station user.	Some station hubs are equipped with an analog audio port that is converted into a USB audio connection inside the hub.
Printers	Accessible to all users on the system.*	Accessible only to the station user.	
USB mass storage device	Accessible to all users on the system.*	Accessible only to the station user.	These devices include USB flash drives, external hard disk drives, and digital cameras.
Web cameras	Accessible to all users on the system.*	Accessible only to the station user.	Only one user can connect to the camera at a time.

*Devices that are connected to the host computer are not visible to the users who are logged on to virtual desktop stations.

For more information about how to set up a station, see Set Up a Station.

Working with station hubs

There are four scenarios for how a USB hub can be used when it is connected to a MultiPoint Services system. Each of the following scenarios provides different access to the devices that are connected to it, depending on the type of hub and where it is connected to the system.

- A station hub connected to the computer in your MultiPoint Services system with a keyboard attached can be used to create a MultiPoint Services station. A keyboard and mouse are connected to the station hub using the ports that are available on the hub. A video monitor is connected to a video port on the computer or to a video adapter on the station hub, if available. The keyboard, mouse, and monitor are then *associated* with a MultiPoint Services station.
- A USB hub connected to the computer in your MultiPoint Services system with no keyboard attached can be used to connect additional devices to the computer when there are not enough ports on the computer for the required devices. All devices connected to this USB hub are available to all users of the MultiPoint Services system. This is not considered a MultiPoint Services station hub.
- A powered USB hub connected to the computer in your MultiPoint Services system, also known as an intermediate hub, can be used to connect additional USB hubs that are used to create MultiPoint stations.
- A USB hub connected to a station hub can be used to connect additional devices to the station hub. Keyboards must be connected directly to the station hub.

For more information about how to set up a MultiPoint Services station, see Set Up a Station.

See Also

Work with Video Devices

12/9/2022 • 2 minutes to read • Edit Online

Learn how video devices, such as a monitor or projector, function when they are connected to a computer in your MultiPoint Services system or to a MultiPoint Services *station*.

Working with video monitors

Depending on your MultiPoint Services system hardware, there are two ways to connect a video monitor:

- For *USB hub-based systems*, connect the video monitor cable to an open video port on the computer, as shown in the following illustration:

- For *multifunction hub-based systems* with built-in video support, connect the video monitor cable to the video port on the multifunction hub:

For more information, see the Set Up a Station topic.

Working with video projectors

You can connect a video projector to your MultiPoint Services system when you want to project a large image to be viewed by others; for example, in a lab setting. For both USB hub-based and multifunction hub-based stations, you have two options for connecting a projector to a station:

- Replace a monitor with a projector and use the projector as the display device for that station, as shown in the following illustration:

- Obtain a video splitter device to connect both a projector and monitor to the station's video port.

  MultiPoint Services will display the same image on both display devices. When not projecting, you can turn the projector off and use just the video monitor.

When using either option, note the following:

- Connecting a video display may require that you *associate the station* again so that MultiPoint Services can correctly recognize the new display. Follow the instructions that appear on the station's video display

device.

- You may need to obtain adapter or converter devices to convert between DVI and VGA plugs.
- Use of a "Y" splitter cable may decrease video quality on both video devices.
- When using both a projector and a monitor via a "Y" splitter cable, MultiPoint Services adjusts the screen resolution of both devices to the lowest maximum resolution of either device—most typically the projector.
- MultiPoint Services does not support extending a single station's display across multiple monitors.

See Also

Manage Station Hardware Set Up a Station

Set Up a Station

12/9/2022 • 2 minutes to read • Edit Online

A MultiPoint Services *station* typically consists of a *station hub*, mouse, keyboard, and video monitor. This topic describes how to connect the hardware devices to the station hub to create a MultiPoint Services station.

The station hub is a hardware device that connects peripheral devices to a computer in a MultiPoint Services system. MultiPoint Services supports two types of station hubs:

- **USB Hub:** A generic multiport USB expansion hub that complies with the universal serial bus 2.0 or later specifications. Such hubs typically have two, four, or more USB ports that allow for multiple USB devices to be connected to a single USB port on the computer. USB hubs are commonly separate devices that may be externally powered or bus-powered. When used as a station hub with MultiPoint Services, we recommend that you use a hub with four or more ports.

  > **IMPORTANT**
  >
  > If you plan to connect USB devices other than a keyboard and mouse to the hub, we recommend that you use an externally powered hub for best performance.

- **Multifunction Hub:** An expansion hub that connects to the computer via a USB port, and enables the connection of a variety of non-USB devices to the hub, including a video monitor. Multifunction hubs are produced by specific hardware manufacturers and may require the installation of a device-specific driver.

If you want to add a station to your MultiPoint Services system, first make sure that you have enough connection ports available for the station hardware that you want to use. In addition, you must secure the appropriate number of *client access licenses (CALs)* for your MultiPoint Services system.

Setting up station hardware

The procedures in this section describe how to connect MultiPoint Services station hardware to the different types of station hubs.

To set up a station with a USB hub

1. Before you can connect a new station, *end* all user *sessions*, and then shut down the computer and other powered devices in your MultiPoint Services system.

2. Connect the new video monitor cable to the video display port on the computer, as shown in the following illustration:

3. Connect the new USB hub to an open USB port on the computer:

4. Connect a keyboard and mouse to the USB hub:

5. Connect the power cord of the video monitor to a power outlet.
6. Turn on the computer.
7. MultiPoint Services starts. Follow the instructions that appear on the new station's video monitor to associate the devices to the new station.

To set up a station with a multifunction hub

1. Before you can connect a new station, end all user sessions, and then shut down the computer and other powered devices in your MultiPoint Services system.
2. Connect the new video monitor cable to the DVI or VGA video display port on the multifunction hub, as shown in the following illustration:

3. Connect the new multifunction hub to an open USB port on the computer:

4. Connect a keyboard and mouse to the PS2 or USB connectors on the multifunction hub:

5. Connect the power cord of the video monitor to a power outlet.
6. Turn on the computer.
7. MultiPoint Services starts. If prompted, follow the instructions that appear on the new station's video monitor to *associate* the devices to the new station.

See Also

Manage System Tasks Using MultiPoint Manager

12/9/2022 • 2 minutes to read • Edit Online

In MultiPoint Manager, you can use the **Home** tab to perform MultiPoint Services tasks and check the state of the system. Tasks that you can perform on the **Home** tab include:

- Editing the settings you selected when you installed MultiPoint Services, as described in the Edit Server Settings topic.
- Restarting or shutting down the computer, including user *sessions*, as described in the Restart or Shut Down topic.
- Switching modes to perform various administrative tasks, as described in the Switch Between Modes topic.
- Enabling or disabling disk protection, as described in the Enable or Disable Disk Protection topic.
- Remapping all stations, as described in the Remap All Stations topic.
- Adding or removing computers, as described in the Add or Remove Computers topic.

See Also

Edit Server Settings Restart or Shut Down Switch Between Modes Enable or Disable Disk Protection Remap All Stations Add or Remove Computers

Edit Server Settings

12/9/2022 • 3 minutes to read • Edit Online

When you installed MultiPoint Services, you configured settings for your system, including opting in to certain programs. This topic describes the settings you can set for your MultiPoint Services system, and explains how to edit the settings.

About MultiPoint Services settings

The following table describes the different settings that you can change for your MultiPoint Services system.

MULTIPOINT SERVICES SETTING	DESCRIPTION
Allow one account to have multiple sessions	Allows a single user account to be simultaneously logged on to multiple stations. This can be useful in cases such as a classroom where every student is using a shared, single account. Using this setting, any changes to the account resources, such as document folders or the desktop, are available to all users who are logged on using the same account.
Allow this computer to be managed remotely	Allows the computer that is running MultiPoint Services to be managed by other MultiPoint systems on your network. If this option is selected, and the managing computer is on the same subnet, this computer appears in the list of available servers to be managed. If this option is selected, and the managing computer is on a different subnet, the managing computer can still manage this computer, but you must specify the IP address of the computer.
Allow monitoring of this computer's desktops	Allows you to control whether desktops can be monitored on the MultiPoint Services system. If this setting is off (not selected), desktops of stations (both local and remote) that are connected to the computer that is running MultiPoint Services will not display in the Home tab of MultiPoint Manager (including on a different computer if the computer is being remotely managed).
Always start in console mode	Enables the RemoteFX technology, which is designed to allow faster and more efficient Remote Desktop sessions by offloading processing to the CPU and GPU. If you are connecting to MultiPoint Services using a RemoteFX-capable client, you may be able to achieve better performance using this option. The benefits depend on the capabilities of your server and network. For example, this depends in part on whether the time spent doing additional processing to compress the data stream is less than the time that is saved by transmitting less data.
Do not show privacy notification at first user logon	When a user logs on to a MultiPoint station for the first time, a notification displays to advise the user that their station activities may be monitored.

MULTIPOINT SERVICES SETTING	DESCRIPTION
Assign a unique IP to each station	Assigns a unique IP address to each station. By default, MultiPoint Services has one IP address, which is shared with all sessions that are running on the system. This configuration, however, can cause some application compatibility problems. For example, if an application requires a unique IP address, it may not run properly on MultiPoint Services. Selecting this option, also known as IP virtualization, can resolve this problem. IP virtualization is also useful for monitoring active sessions on MultiPoint Services. Some monitoring tools report usage according to the IP address. To enable session monitoring, you can use IP virtualization to assign a unique IP address to each session. Note that if you select this option, each new session receives a unique IP address. Any existing sessions continue to use the shared IP address until they are logged off and logged back on.
Allow IM between MultiPoint Dashboard and a user session on this computer	Enables chat between MultiPoint Manager and user session on this computer. For more information see Use IM.
Allow orchestration of administrator and MultiPoint Dashboard user sessions	When enabled, allows administrators to use the MultiPoint Dashboard for session orchestration. These sessions display as thumbnails.
Allow stations to use GPU hardware rendering	Controls whether stations can use the system's graphics processing unit (GPU).

Editing the computer settings

1. Open MultiPoint Manager in station mode, and then click the **Home** tab.
2. In the **Computer** column, click the computer name, and then, under the *computer name* **Tasks**, click **Edit computer settings**.
3. Select or clear the items you want to change, and then click **OK**.

See Also

Manage System Tasks Using MultiPoint Manager

Restart or Shut Down MultiPoint Systems

12/9/2022 • 2 minutes to read • Edit Online

You can restart or shut down one MultiPoint Services system or multiple MultiPoint Services systems in MultiPoint Dashboard.

Restart a MultiPoint Services system or multiple systems

1. Click **Systems**.
2. Click the thumbnail image of the server you want to restart, and then, on the **Hardware** tab, click **Restart**.

To shut down a MultiPoint Services system or multiple systems

1. Click the **Systems** tab.
2. Click the thumbnail image of the server you want to restart, and then, on the **Hardware** tab, click **Shut Down**.

Switch Between Modes

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint Manager includes the following modes to help you perform different types of MultiPoint Services system management:

- *Station mode*: By default, the MultiPoint Services system starts in station mode. While in station mode, the MultiPoint Services stations behave as if each station is a separate computer that is running Windows, and multiple users can use the system at the same time. You and your users can share files and perform the work that you must do.
- *Console mode*: When the MultiPoint Services system is in console mode, you can install and update software and drivers or perform other maintenance tasks. When the system is in console mode, no *stations* are available for use by other computer users. Such stations are not displayed in MultiPoint Manager. All monitors directly connected to the server are treated as displays of this computer system.

NOTE

You can enforce the system starting in Console mode by changing the default in the settings for the server.

To switch from station mode to console mode

1. Open MultiPoint Manager in station mode, and then click the **Home** tab.
2. In the **Computer** column, click the computer for which you want to change modes.
3. Under *computer name* **Tasks**, click **Switch to console mode**. The computer restarts and all stations become unavailable.

To switch from console mode to station mode

1. Open MultiPoint Manager in console mode, and then click the **Home** tab.
2. In the **Computer** column, click the computer for which you want to change modes.
3. Under *computer name* **Tasks**, click **Switch to station mode**. The computer restarts and all stations become available.

See Also

Manage System Tasks Using MultiPoint Manager

Enable or Disable Disk Protection

12/9/2022 • 2 minutes to read • Edit Online

The Disk Protection feature allows you to reset your MultiPoint Services system to a specified state each time you restart the system. Using Disk Protection, users can temporarily make changes to the MultiPoint Services system, and then those changes are discarded when the server is restarted. Examples of changes that will be discarded when the server is restarted include personalizing a user's profile, saving files, changing settings, or installing applications.

Enable Disk Protection

1. In MultiPoint Manager, click the **Home** tab, and then, under *computer name* **Tasks**, click **Enable Disk Protection**.
2. Review the information, and then click **OK**.

After the system restarts, any changes made to the system, including new applications that are installed, will be discarded on each subsequent restart.

Disable Disk Protection

1. In MultiPoint Manager, click the **Home** tab, and then, under *computer name* **Tasks**, click **Disable Disk Protection**.
2. Review the information, and then click **OK**.

After the system restarts, any changes made to the system, including applications that are installed on the server, are permanent and will not be discarded the next time the system is restarted.

Manage Client Access Licenses

12/9/2022 • 2 minutes to read • Edit Online

Every station that connects to a MultiPoint Services system, including the computer running MultiPoint Services that is used as a station, must have a valid per-user Remote Desktop *client access license (CAL)*.

If you are using station virtual desktops instead of physical stations, you must install a CAL for each station virtual desktop.

1. Purchase a client license for each station that is connected to your MultiPoint Services computer or server. For more information about purchasing CALs, visit the documentation for Remote Desktop licensing.
2. From the **Start** screen, open **MultiPoint Manager**.
3. Click the **Home** tab, and then click **Add client access licenses**. This will open the management tool for CAL licensing.

Set the licensing mode manually

If not properly configured the MultiPoint Services set-up will prompt with a notification about the grace period being expired. Follow these steps to set the licensing mode:

1. Launch **Local Group Policy Editor** (gpedit.msc).
2. In the left pane, navigate to **Local Computer Policy->Computer Configuration->Administrative Templates->Windows Components->Remote Desktop Services->Remote Desktop Session Host->Licensing**.
3. In the right pane, right click **Use the specified Remote Desktop license servers** and select **Edit**:
   - In the group policy editor dialog, select **Enabled**
   - Enter the local computer name in the **License servers to use** field.
   - Select **OK**
4. In the right pane, right click **Set the Remote Desktop licensing mode** and select **Edit**
   - In the group policy editor dialog, select **Enabled**
   - Set the **Licensing mode** to Per Device/Per User
   - Select **OK**

See Also

Manage System Tasks Using MultiPoint Manager

Remap All Stations

12/9/2022 • 2 minutes to read • Edit Online

Remapping stations allows you to associate keyboards and mice to monitors. When you remap all stations, the original settings, such as name and auto-logon information, are erased. All local user stations are suspended while the remapping takes place.

1. Open MultiPoint Manager in station mode, and then click the **Home** tab.
2. Under **Tasks**, click **Remap all stations**.
3. Follow the instructions on the station screens to associate the keyboards to the stations in your system.

Save Connection Settings to File

12/9/2022 • 2 minutes to read • Edit Online

Using Remote Desktop, you can connect to a MultiPoint Services system from another computer. If the remote computer supports Remote Desktop Protocol, the connection to the computer can be established automatically.

There are three types of connection files you can create:

- **MultiPoint Manager connection file**: Allows MultiPoint Manager to be run on another computer as a remote application.
- **MultiPoint Dashboard connection file**: Allows MultiPoint Dashboard to be run on another computer as a remote application.
- **Remote station connection file**: Allows another computer to connect to the MultiPoint Services system as a remote station.

To save system connection settings to a file

1. Open MultiPoint Manager in station mode, and then click the **Home** tab.
2. In the **Computer** column, click the name of the computer for which you want to save the connection settings to a file.
3. Under *computer name***Tasks**, click **Save connections to file**. The **Save Connection Settings to File** page is displayed.
4. Choose the type of connection file you want to create, and then click **OK**.
5. Choose the folder where you want to save the file, edit the **File name** if preferred, and then click **Save**.

Add or Remove Computers

12/9/2022 • 2 minutes to read • Edit Online

You can add other computers or remove computers from your MultiPoint Services system by using MultiPoint Manager. Adding other PCs to MultiPoint Manager allows the MultiPoint Dashboard to orchestrate any user's session when logged on to that PC in the same way it can for MultiPoint stations.

To add or remove servers in MultiPoint

1. Open MultiPoint Manager in station mode, and then click the **Home** tab.
2. Under *computer name* **Tasks**, click **Add or remove MultiPoint servers**. The **Add or Remove MultiPoint Servers** screen launches and begins discovering other servers on the local network subnet that can be managed with MultiPoint Manager.
3. Do one of the following:
   - **To add a server:** In the **Available** list, click a server that you want to manage with MultiPoint Manager, and then click **Add**. If the administrator user account and password for the server are different than the account you are currently logged on with, you are prompted to provide the account information.
   - **To add a server that is not on the subnet:** In the **MultiPoint Server name** field, type the name of the server you want to add, and then click **Manually Add**.
   - **To remove a server:** In the **Managed** list, click a server that you want to remove from management, and then click **Remove**.

To add or remove other computers

1. Open MultiPoint Manager in station mode, and then click the **Home** tab.
2. Under **Home Tasks**, click **Add or remove personal computers**. The **Add or Remove Personal Computers** screen launches and begins discovering other computers on the local network subnet that can be managed with MultiPoint Services.
3. Do one of the following:
   - **To add a computer:** In the **Available** list, click a computer that you want to manage with MultiPoint Services, and then click **Add**. When adding a computer, you are prompted to provide the account information.
   - **To add a computer that is not on the subnet:** In the **Personal Computer name** field, type the name of the computer you want to add, and then click **Manually Add**.
   - **To remove a computer:** In the **Managed** list, click a computer that you want to remove from management, and then click **Remove**.

See Also

Manage System Tasks Using MultiPoint Manager Edit Server Settings

Manage User Stations

12/9/2022 • 2 minutes to read • Edit Online

This section discusses managing the *stations* that make up the MultiPoint Services system. Managing a MultiPoint Services system includes both managing the hardware and software components of MultiPoint Manager. In a MultiPoint Services system, a desktop is the software user interface presented on the monitor for each user station.

Station status

You can view the following types of status for each desktop on the **Stations** tab. Status includes:

- Users who are logged on
- User sessions that are suspended, but are still active on the computer
- Which stations are being used and by which user

For more information about viewing desktop status, see the View User Connection Status topic.

> **TIP**
>
> You can assign friendly names to each station, which might help you identify the stations more easily. Use **Identify station**, which dipslays the station name on the assigned screen.

Different ways to log standard users off of the MultiPoint Services system

As an *administrative user*, you can log off Windows at any time, which will have no effect on active users in your MultiPoint Services system. *Standard users* can *disconnect* their session or *log off* the MultiPoint Services system too. In the care where disk protection is enabled, if a user is leaving for the day, they should make sure to save their work on the computer or an external storage device so that when the MultiPoint Services system is shut down, the user can still retrieve their saved work another day.

As an administrative user, you might need to end a standard user's *session*, rather than having the user log off. You can end a standard user's session in one of two ways:

- End the session and log the user off. For more information about ending a user's session, see the End a User Session topic.
- Suspend the user to temporarily end the user's session, but keep the session active in the MultiPoint Services system's computer memory. The suspended user can then reconnect to the session from the same station or a different station and continue his or her work. For more information about suspending a user's session, see the Suspend and Leave User Session Active topic.

Set a station to automatically log on

As an administrative user, you can set up one or more stations to automatically log on when the computer that is running MultiPoint Services starts. For more information about automatically logging on, see the Set Up a Station for Automatic Logon topic.

Split a station

Any station monitor that has a resolution greater than 1024x768 can be split into two stations. For more information about splitting a station, see the Split a User Station topic.

See Also

View User Connection Status Log off or Disconnect User Sessions Suspend and Leave User Session Active Set Up a Station for Automatic Logon End a User Session Split a User Station

View User Connection Status

12/9/2022 • 2 minutes to read • Edit Online

Use the **Stations** tab to determine the status of a standard or other administrative user's connection to a MultiPoint Services station.

Status values include the following:

- **Logged on**: A user session that is active on a station
- **Suspended**: A user session that is suspended, but is still active on the computer. The user's desktop session is preserved until the user logs on again
- **Logged off**: A user who is logged off is not displayed on the **Stations** tab

To view station status, open MultiPoint Manager in stations mode, and then click **Stations**.

See Also

Manage User Desktops Switch Between Modes

Log off or Disconnect User Sessions

12/9/2022 • 2 minutes to read • Edit Online

MultiPoint Services users can log on and log off of their desktop sessions as they would with any Windows session. Users can also disconnect or suspend their session so that the MultiPoint Services station is not being used, but their session remains active in the MultiPoint Services system's computer memory.

In addition, administrative users can end a user's session if the user has stepped away from their MultiPoint Services session or has forgotten to log off of the system.

Logging off or disconnecting a session

The following table describes the different options that you or any user can use to log off, suspend, or end a session.

ACTION	EFFECT
Click **Start**, click Settings, click the user name (top-right corner), and then click **Sign out**.	The session ends and the station is available for log on by any user.
Click **Start**, click **Settings**, click Power, and then click **Disconnect**.	Your session is disconnected and your session is preserved in computer memory. The station becomes available for log on by the same user or a different user.
Click **Start**, click Settings, click the user name (top-right corner), and then click **Lock**	The station is locked and your session is preserved in computer memory.

Suspending or ending a user's session

The following table describes the different options that you, as an administrative user, can use to disconnect or end a user's session.

ACTION	EFFECT
Suspend: In MultiPoint Manager, use the **Stations** tab to suspend the user's session. For more information, see the Suspend and Leave User Session Active topic.	The user's session ends and is preserved in computer memory. The station becomes available for log on by the same user or a different user. The user can log on to the same station or another station and continue with their work.
End: In MultiPoint Manager, use the **Stations** tab to end the user's session. You can also end all user sessions on the **Stations** tab. For more information, see the End a User Session topic.	The user's session ends and the station becomes available for log on by any user. The user's session no longer displays on the **Stations** tab, and it is not in computer memory.

See Also

Suspend and Leave User Session Active End a User Session Manage User Desktops Log Off User Sessions

Suspend and Leave User Session Active

12/9/2022 • 2 minutes to read • Edit Online

You can disconnect or suspend users from the MultiPoint Services system when you do not want to end the users' sessions. A user can also disconnect the session, rather than you disconnecting the session for them. While a user session is suspended, the session remains active in the MultiPoint Services system's computer memory until the computer is shut down or restarted. At that time, all suspended sessions are ended and any unsaved work is lost.

1. Open MultiPoint Manager in station mode, and then click the **Stations** tab.
2. In the **Computer** column, click name of the computer whose sessions you want to suspend.
3. Under **Stations Tasks**, click **Suspend all stations**.

After a user session has been suspended, the user can log on to the same or another station and continue to work in the original session.

See Also

Manage User Desktops Log off or Disconnect User Sessions

End a User Session

12/9/2022 • 2 minutes to read • Edit Online

You should end a user's session when you have to log the user off from the MultiPoint Services system to return the desktop to its default settings. The user receives a warning that the connection is about to end. You should end a user's connection when you want to:

- Restart the MultiPoint Services system computer
- Shut down the MultiPoint Services system computer
- Switch modes
- Log off a user who forgot to log off

To end user sessions:

1. Open MultiPoint Manager in station mode, and then click the **Stations** tab.
2. Do one of the following:
    - To end a single user session, in the **User** column, select the session you want to end, and then, under **Tasks**, click **Log off**.
    - To end all user sessions, under **Stations Tasks**, click **Log off all stations**.

See Also

Manage User Desktops Log off or Disconnect User Sessions

Set up a Station for Automatic Logon

12/9/2022 • 2 minutes to read • Edit Online

Auto-logon enables each station to be automatically logged on when the computer that is running MultiPoint Services starts, and display the desktop. An administrative user can set this feature for individual stations or for all stations.

1. Open MultiPoint Manager in station mode, and then click the **Stations** tab.
2. Click the name of the station you want to automatically log on.
3. Under **Tasks**, click **Configure station**. The **Configure Stations** page opens.
4. Select **Auto-logon using the following information**, and then enter a **User account** name.
5. Enter the password for the user account, and then re-enter the password to confirm it.
6. Click **OK**. The page closes. The account name is displayed in the **Auto-logon** column.

See Also

Manage User Stations

Split a User Station

12/9/2022 • 2 minutes to read • Edit Online

Any MultiPoint Services station monitor that has a resolution greater than 1024x768 can be split into two stations using the **Split station** task on the **Stations** tab. The desktop that is present on the monitor at the time that the split occurs moves to the left half of the monitor, and a new station is created on the right half of the same monitor. The new station must be mapped to a keyboard, mouse, and USB hub to complete its creation. After a station is split, a user can log on to the left station while another user logs on to the right station.

Benefits of using a split-screen station may include:

- Reducing cost and space by accommodating more students on a MultiPoint Services system
- Allowing two students to collaborate together, side-by-side on a project
- Allowing a teacher to demonstrate a procedure on one station while a student follows along on the other station

> **NOTE**
>
> When you split a station, the active session on the station is suspended. The user must log on to the station again to resume work after the split has occurred.

To split a station:

1. In MultiPoint Manager, in station mode, click the **Stations** tab.
2. In the **Station** column, click the name of the station you want to split.
3. Under **Stations Tasks**, click **Split station**.

To return a split station to a single station:

1. In MultiPoint Manager, in station mode, click the **Stations** tab.
2. In the **Station** column, click the name of the station for which you want to end a split.
3. Under **Stations Tasks**, click **Unsplit station**.

See Also

Manage User Stations

Manage User Accounts

12/9/2022 • 2 minutes to read • Edit Online

This section describes the different types of user accounts, how to create user accounts, and how to manage user accounts. In a MultiPoint Services system, there are two types of user accounts: *standard user accounts* and *administrative user accounts*, as described below.

> **TIP**
>
> The User Account Considerations topic provides guidelines that you should consider as you create and manage user accounts.

User Account Considerations

12/9/2022 • 2 minutes to read • Edit Online

This topic describes issues that you, as an administrative user, should consider as you create and manage user accounts. You manage user accounts in the Users tab in MultiPoint Manager. For more information, see the Manage User Accounts topic.

User account types

A user account is a collection of information that tells MultiPoint Services which files and folders a user can access, what changes they can make to the MultiPoint Services system, and each user's preferences, such as desktop background. Each person accesses their own user account by using a unique user name and password. MultiPoint Services supports three types of user accounts:

- **Administrative user accounts** are for individuals who will use MultiPoint Manager to use and manage the MultiPoint Services system. For more information, see Create an Administrative User Account.
- **Standard user accounts** are for individuals who will regularly access stations, but will not manage the system. Typically, you should create standard user accounts for most MultiPoint Services system users. For more information, see Create a Standard User Account.
- **MultiPoint Dashboard user accounts** are for individuals who use the MultiPoint Dashboard to manage standard user sessions and can log on from any station. For more information, see Create a MultiPoint Dashboard User Account.

User name and password considerations

Administrative users can perform tasks that affect all other users of the MultiPoint Services system, such as install software or change security settings. For this reason, administrative users should have unique user names and passwords that are known only to them.

One important consideration of user accounts is that each user account is allocated a unique **Documents** library in Windows Explorer that includes the **My Documents** folder. If the standard users on your MultiPoint Services system will store private documents in their **Documents** library in Windows Explorer, they too should log on to the MultiPoint Services system using a unique user name and password known only to them. For more information about storing documents in Windows Explorer, see the Manage User Files topic.

> **TIP**
>
> For stronger system security, all users' passwords should be strong passwords. A strong password is one that cannot be easily guessed or cracked, is at least eight characters long, does not contain all or part of the user's account name, and contains at least three of the four following categories of characters: uppercase characters, lowercase characters, numbers, and symbols found on a keyboard (such as !, @, #).

See Also

Create an Administrative User Account Create a Standard User Account Manage User Files Manage User Accounts

Create an Administrative User Account

12/9/2022 • 2 minutes to read • Edit Online

Create *administrative user accounts* for those individuals who will manage your MultiPoint Services system. To see who has administrative access, in MultiPoint Manager, click the **Users** tab. Administrative user accounts are displayed in the **Account Type** column as **Administrator**. *Administrative users* have access to all MultiPoint Manager tasks that change desktop and system settings, such as:

- Creating accounts
- Adding and removing programs
- Managing *desktops* and hardware
- Ending other user *sessions*

Administrative users can perform tasks that affect all other users of the MultiPoint Services system, such as install software or change security settings. For this reason, administrative users should have unique user names and passwords that are known only to them.

For more information about issues that you, as an administrative user, should consider as you create and manage user accounts, see the User Account Considerations topic.

> **NOTE**
>
> You might want to create a *standard user account* for you to use when you perform tasks on the MultiPoint Services system that are not related to MultiPoint Services system management. You would then only log on to your administrative user account when you need to perform system management tasks.

To create an administrative user account

1. In MultiPoint Manager, click the **Users** tab.
2. Under **User Tasks**, click **Add user account**. The **Add User Account** wizard opens.
3. In the **User account** field, type a logon name for the user. Typically, the logon user name is the first and last name written together without spaces, or the first initial and last name written together without a space.
4. In the **Full Name** field, type the name of the user in whatever format you prefer, such as given name, full name, or a nickname.
5. In the **Password** field, type a password for the user. The password should only be known to you and the user, and you should store this information in a secure location. The password can only be changed by an administrative user.
6. In the **Confirm password** field, retype the password, and then click **Next**.
7. On the level of access page, select **Administrative user**, and then click **Next**.
8. MultiPoint Services will check all of the information and display a message when the account has been set up. When you see the text, **A new user account was successfully created**, click **Finish**.

Create a Standard User Account

12/9/2022 • 2 minutes to read • Edit Online

Create *standard user accounts* for those users who will regularly access stations, but who will not manage your MultiPoint Services system. Users with standard user accounts can run most applications and save files, but cannot run MultiPoint Manager. To see who has standard user access, in MultiPoint Manager, click the **Users** tab. Standard user accounts are displayed in the **Account Type** column as **Standard**.

If your MultiPoint Services users will store private documents in Windows, each user should log on to the MultiPoint Services system using a unique user name and password.

> **NOTE**
>
> For more information about issues you, as an *administrative user*, should consider as you create and manage user accounts, see the User Account Considerations topic.

To create a standard user account

1. In MultiPoint Manager, click the **Users** tab.
2. Under **User Tasks**, click **Add user account**. The **Add User Account** wizard opens.
3. In the **User account** field, type a logon name for the user. Typically, the logon user name is the first and last name written together without spaces, or the first initial and last name written together without a space.
4. In the **Full name** field, type the name of the user in whatever format you prefer, such as given name, full name, or a nickname.
5. In the **Create password** field, type a password for the user. This password should only be known to you and the user, and you should store this information in a secure location. The password can only be changed by an administrative user.
6. In the **Confirm password** field, retype the password, and then click **Next**.
7. On the level of access page, select **Standard user**, and then click **Next**.
8. Click **Finish**.

Create a MultiPoint Dashboard User Account

12/9/2022 • 2 minutes to read • Edit Online

Create MultiPoint Dashboard user accounts for those users who will regularly access stations, but who will not manage your MultiPoint Services system. Users with MultiPoint Dashboard user accounts can run most applications and save files, but cannot run MultiPoint Manager. To see who has MultiPoint Dashboard user access, in MultiPoint Manager, click the **Users** tab. MultiPoint Dashboard user accounts are displayed in the **Account Type** column as **MultiPoint Dashboard User**.

If your MultiPoint Services users will store private documents in Windows, each user should log on to the MultiPoint Services system using a unique user name and password.

> **NOTE**
>
> For more information about issues you, as an *administrative user*, should consider as you create and manage user accounts, see the User Account Considerations topic.

To create a MultiPoint Dashboard user account

1. In MultiPoint Manager, click the **Users** tab.
2. Under **User Tasks**, click **Add user account**. The **Add User Account** wizard opens.
3. In the **User account** field, type a logon name for the user.
4. In the **Full name** field, type the name of the user in whatever format you prefer, such as given name, full name, or a nickname.
5. In the **Create password** field, type a password for the user. This password should only be known to you and the user, and you should store this information in a secure location. The password can only be changed by an administrative user.
6. In the **Confirm password** field, retype the password, and then click **Next**.
7. On the level of access page, select **MultiPoint Dashboard user**, and then click **Next**.
8. Click **Finish**.

See Also

User Account Considerations

Update or Delete a User Account

12/9/2022 • 2 minutes to read • Edit Online

If you are logged on as an administrative user on the MultiPoint Services system, you can modify any user account, including changing the level of access for an account, changing a full name and password, or deleting an account.

1. Open MultiPoint Manager in station mode, and then click the **Users** tab.
2. In the **User** column, click the account that you want to modify.
3. Under *user name* **Tasks**, click the appropriate task.

SELECTED ITEM TASK	DESCRIPTION
Change full name	Allows you to change the full name for the account.
Change password	Allows you to change the password for this account on to the MultiPoint Services system.
Change level of access	Allows you to change the account type to either administrative user or standard user.
Delete user account	Removes the user account from the MultiPoint Services system.

See Also

Create an Administrative User Account Create a Standard User Account Manage User Accounts

Manage Virtual Desktops

12/9/2022 • 3 minutes to read • Edit Online

Single computer VDI allows you to configure each *local* MultiPoint Services station to connect to a Windows 10 Enterprise guest operating system running in a Hyper-V virtual machine (VM) on the same MultiPoint Services computer as the station. These virtual desktop stations can be customized with application which cannot be installed on a Windows server version.

Enable the virtual desktop feature

1. Open MultiPoint Manager, and then click the **Virtual Desktops** tab.
2. Under **VDI Tasks**, click **Create virtual desktop**, and then browse your Windows 10 Enterprise .iso or VHD.

The system is restarted, which could take several minutes.

Create a virtual desktop template

1. Open MultiPoint Manager, and then click the **Virtual Desktops** tab.
2. Under **VDI Tasks**, click **Create virtual desktop**, and then browse to your Windows 10 Enterprise .iso or VHD.

   If using the DVD, the program automatically finds the Windows 10 Enterprise .wim file. Otherwise, click **Browse**, and then navigate to the Windows 10 Enterprise .iso or VHD.

   Modify the prefix if desired. It will default to the host computer name.

   > **NOTE**
   > The prefix is used to name the template and the virtual desktop stations. The template is named prefix -t. The virtual desktop stations will be named prefix -*n*, where *n* is the station ID.

3. Enter a name and password for the local administrator account that will be used to log on to all virtual station desktops that are created from the template, and then click **OK**.

   The template creation takes several minutes to complete.

   Next, learn how to customize the virtual desk template.

   > **NOTE**
   > If the MultiPoint server is domain-joined, the dialog populates an additional field which allows you to say whether the virtual machines that were created from the template should be joined to a domain.

Import a virtual desktop template

In the case where you have created a virtual desktop template on another MultiPoint server, you can import that template using the following steps.

1. Open MultiPoint Manager, and then click the **Virtual Desktops** tab.

2. Under the VDI tasks, click **Import Virtual desktop template**.

3. Locate the template and define path and prefix for the imported template.

Customize the virtual desktop template

After you have created the virtual desktop template, you can customize it with applications, software updates and configure system settings.

1. Open MultiPoint Manager, and then click the **Virtual Desktops** tab.
2. Choose the virtual desktop template, and then click **Customize virtual desktop template**. The template opens in a separate window, and additional instructions are presented that highlight the most important steps for customizing the virtual template. Carefully review those instructions.

Create virtual desktop stations

1. Open MultiPoint Manager in station mode, and then click the **Virtual Desktops** tab.

   > **NOTE**
   > If the MultiPoint Services system is not running in station mode, restart it before completing this procedure.

2. Select the virtual desktop template in the left-hand pane. It is named <prefix –t>.

3. Under template Tasks, click **Create virtual desktop stations**, and then click **OK**.

   The virtual desktop station creation process takes several minutes.

   > **NOTE**
   > If any of the local stations are currently connected to a session-based virtual desktop, you must log off of those stations in order for them to connect to one of the newly created virtual desktop stations.

Validate the newly created customized virtual station desktops

You can validate your customized virtual station desktops by logging on to one or more of the virtual desktop stations using either a local administrator account or a domain account, and then verify that the new VM-based virtual desktops are working properly.

Disable Virtual Desktops

When disabling virtual desktops the Hyper-V feature will be turned off. All users will be logged off and the system will be restarted. All virtual stations are assigned to MultiPoint local sessions after restart of the system.

1. Open MultiPoint Manager in station mode, and then click the **Virtual Desktops** tab.

2. Under the VDI Tasks click **Disable virtual desktops**.

Manage User Files

12/9/2022 • 2 minutes to read • Edit Online

Both standard users and administrative users at MultiPoint Services stations can save documents in Windows Explorer libraries and folders. A library is a collection of items, such as files and folders. Common libraries in Windows Explorer include **Documents**, **Music**, **Pictures**, and **Videos**. When working with libraries, there are two options for storing documents:

- Store documents privately so that they are accessible only to the user who stored them in a library or folder. Note that administrative users can access privately stored documents of standard users. However, standard users cannot access privately stored documents of administrative users. For more information about keeping content private, see the Keep Files Private topic.
- Store documents publicly so that they are accessible to all users on the MultiPoint Services system. For more information about sharing content with other users, see the Share Files topic.

The **Documents** library, by default, includes two folders: **My Documents** (which is private) and **Public Documents** (which is public). Other document libraries contain similar pairs of private and public folders. All administrative and standard users of a MultiPoint Services system should understand how the Windows Explorer location at which they put documents and other files can affect the privacy or public access of those files.

You can also share content with other users by using a USB storage device such as a USB flash drive or mass storage device (external hard disk). For more information about sharing content with storage devices, see the Save and Share Files on a USB Flash Drive topic.

Keep Files Private

12/9/2022 • 2 minutes to read • Edit Online

This topic applies to content, such as documents, that you (as an *administrative user*) and *standard users* do not want to share with other users in a MultiPoint Services system.

For more information about privacy in MultiPoint Services, see Privacy and Security Considerations.

To keep content private in Windows Explorer

To keep your documents and other content private, you should save your work in Windows Explorer in the **Documents** library in the **My Documents** folder. The **My Documents** folder is, by default, a private folder. Note, however, that administrative users have access to private folders in Windows Explorer.

> **WARNING**
>
> While an external storage device, such as a USB flash drive, is connected to a USB port on the host or on a USB hub that is not a station hub, it is viewable by any standard or administrative user logged onto the MultiPoint Services system. If you have privacy or security concerns about the content stored on an external storage device, connect it only to a station hub on the MultiPoint Services system. For information about how to use USB storage devices, see the Save and Share Files on a USB Flash Drive topic.

See Also

Manage User Files Save and Share Files on a USB Flash Drive

Share Files

12/9/2022 • 2 minutes to read • Edit Online

You can share content with other MultiPoint Services users by storing the content in a public folder in Windows Explorer. All content that is stored in public folders in Windows Explorer in a MultiPoint Services system is accessible to all users on the MultiPoint Services system.

You can also share content by storing it on removable storage devices, as described in Save and Share Files on a USB Flash Drive.

For information about keeping content private, see Keep Files Private.

To share content with other users by using Public folders

Share content with other users by storing it in the **Public Documents**, **Public Music**, and other public folders in Windows Explorer libraries.

You can also share files across multiple computers that are running MultiPoint Services on a network by creating a new folder, and then sharing it.

To share files across multiple computers in a MultiPoint Services network

1. Right-click on a desktop, and then click **New**.
2. Click **Folder**, and then type a name for the folder.
3. Double-click the folder to open it.
4. Click **Share with**, and then click **Specific people**.
5. Select specific users, or click **Everyone**.

See Also

Manage User Files Save and Share Files on a USB Flash Drive Keep Files Private

Save and Share Files on a USB Flash Drive

12/9/2022 • 2 minutes to read • Edit Online

In addition to being able to share content using Public folders in Windows Explorer, you can also share content using a USB storage device, such as a USB flash drive or mass storage device. When you attach a USB storage device directly to the host computer or to a USB hub that is not a station hub, that storage device will appear as a removable storage device to all users, *standard users* and *administrative users*, across the MultiPoint Services system.

You can also use a removable storage device to save and store private documents in a private folder in Windows Explorer, such as the **My Documents** folder in the **Documents** library.

> **NOTE**
>
> The Dashboard user can block the usage of USB storage. For more information, see Block or Unblock USB Storage.

To share content that is stored directly on a removable storage device

1. Connect the removable storage device to an open USB port on the host computer or a USB hub that is not a *station hub* in the MultiPoint Services system.
2. Instruct users at other *stations* to navigate to and open the removable storage device drive in Windows Explorer. Likewise, other users can share content with you from their own removable storage devices the same way.

To share content that is stored on a removable storage device by using Public folders

1. Connect the removable storage device to an open USB port on the host computer or a USB hub that is not a *station hub* in the MultiPoint Services system.
2. Copy the content you want to share to a public folder in Windows Explorer, such as **Public Documents** in the **Documents** library.

To privately work with content that is stored on a USB storage device

Connect the removable storage device to an open USB port on your station hub.

See Also

Keep Files Private Share Files Manage User Files

Manage User Desktops Using MultiPoint Dashboard

12/9/2022 • 2 minutes to read • Edit Online

In a MultiPoint Services system, a desktop is the software user interface presented on the monitor for each user *station*. The MultiPoint Dashboard is a tool which helps you manage those desktops.

In MultiPoint Dashboard, on the **Home** tab, you can do the following:

- View desktops You can view the thumbnail images for each active desktop. For information about viewing thumbnails, see the View Options for Session Thumbnails topic.
- Block or unblock stations You can block and unblock stations. You can also customize a message to display on blocked stations. For more information about blocking or unblocking stations, or creating a message to display on blocked stations, see the Block or Unblock a Station topic.
- Limit web use You can configure which websites users can visit. For information about setting websites, see the Limit Web Access topic.
- Block or unblock USB storage You can block and unblock USB storage either per station or for all station. When storage is blocked, users cannot use any USB storage devices on their stations. See the Block or Unblock USB Storage topic.
- Project a station to another station You can project your station to another station or stations. You can also project a different selected station to all other stations. For information about projecting a station, see the Project a Station to Other Stations topic.
- Launch or close applications on a station You can launch or close applications on a station. For information about launching or closing applications, see the Launch or Close Applications on a Station topic.
- Use IM You can chat with selected users. The chat message is only visible to the Dashboard user and the user of the selected session. See Use IM for more information.
- Change the size of thumbnail images You can change the size of the thumbnails that display in MultiPoint Dashboard. For information about changing the thumbnail size, see View Options for Session Thumbnails.
- Show all stations You can view all of the stations that are connected to your system, including stations that are not active. For information about viewing all stations, see the Show All Stations topic.
- Search and sort thumbnails You can define the order and grouping of thumbnails in the dashboard. Use search to filter the thumbnails.
- Log off all monitored stations You can log off all of the monitored stations on your MultiPoint Services system. For information about logging off monitored stations, see the Log Off User Sessions topic.

Block or Unblock a Station

12/9/2022 • 2 minutes to read • Edit Online

You can block a user or users from the MultiPoint Services system if you need to get their attention. While users are blocked, their sessions remains active in the MultiPoint Services system's computer memory until the stations are unblocked. You can customize a message to be displayed for a blocked user.

To block a station

1. In the MultiPoint Dashboard, select the thumbnail image of the station you want to block.
2. On the Blocking tab, click **Block**, and then click **Block Selected Desktop(s)** or **Block All Desktops**.

To unblock a station

1. In the MultiPoint Dashboard, select the thumbnail image of the station you want to unblock.
2. On the Blocking tab, click **Unblock**, and then click **Unblock Selected Desktop(s)**.

Create a message to display for blocked users

Before you block a user, you may want to create a message to display on the user's monitor when they are blocked. For example, "Please turn your attention to the speaker." **Station blocked** is the default text if you do not create your own message.

1. Click the **Block** drop-down menu, and then click **Set Message**. The **Set Message for Blocked Users** page opens.
2. Type the message you want to display on the blocked station(s), and then click **OK**.

Limit Web Access

12/9/2022 • 2 minutes to read • Edit Online

In addition to monitoring user activities on individual desktops, you, as an administrative user, can limit user access to specified websites by indicating permissible websites and websites to which you want to block user access.

To limit web access on a station

1. In MultiPoint Dashboard, on the **Web Limiting** tab, click **Configure**. The **Configure Web Limiting** page opens. Sites that the user can access are listed.
2. Click the thumbnail image of the user station on which you want to limit web access.
3. Under **Selected Item Tasks**, click **Limit web access on this station**. The **Configure Web Limiting** page opens. Sites that the user can access are listed.
4. To add an allowed site, type the web address, and then click **Add**.

   > **NOTE**
   >
   > For example, entering "Contoso.com" allows or blocks sites that are relative to www.contoso.com (for example, www.newpage.contoso.com). Entering "Contoso" will either allow or limit all Contoso-related sites (including contoso.com, contoso.uk, and so forth).

5. To remove a web address from the list of allowed sites, click the web address you want to remove access to, and then click **Remove**.

To limit web access on all stations

1. In MultiPoint Dashboard, on the **Web Limiting** tab, click the Start drop-down menu, and then click **Limit Web Access on All Desktops**.

   The **Configure Web Limiting** page opens. Sites that the user can access are listed. Do one of the following:

2. To add an allowed site, click **Allow only these sites**, type the allowed web address, and then click **Add**.

   To add a site you do not want users to visit, click **Disallow only these sites**, type the web address you don't want users to visit, and then click **Add**.

   > **NOTE**
   >
   > For example, entering "Contoso.com" allows or blocks sites that are relative to www.contoso.com (for example, www.newpage.contoso.com). Entering "Contoso" will either allow or limit all Contoso-related sites (including contoso.com, contoso.uk, and so forth).

3. To remove a web address from the list of allowed or disallowed sites, select the web address, and then click **Remove**.

See Also

Block or Unblock USB Storage

12/9/2022 • 2 minutes to read • Edit Online

You can prevent users for using USB storage on their user stations.

To block USB storage for selected stations

1. In the MultiPoint Dashboard, click the station you want to block.
2. Click **Block** > **Block Selected desktop(s)**.

To block USB Storage for all stations

Open MultiPoint Dashboard, and then from the drop-down menu, select **Block Storage on all stations**.

To unblock USB Storage for selected stations

Open MultiPoint Dashboard, choose the thumbnail image of the station you want to unblock, and then click **Unblock**.

Project a Station to Other Stations

12/9/2022 • 2 minutes to read • Edit Online

As a MultiPoint Dashboard User, you can project your desktop to a single user's station or all users' (non-administrator) stations. This feature is useful when you want to demonstrate a task to a user or set of users.

To project your desktop to a standard user's station

1. In MultiPoint Dashboard, click the thumbnail image of the desktop to which you want to project your station.
2. On the **Home** tab, click **Your Desktop**, and then click **Project Your Desktop to Selected Desktop(s)**.
3. To end the projection, click **Stop** (either on the **Projection** tab or in the right-hand corner below the ribbon).

To project your desktop to all stations

1. In MultiPoint Dashboard, on the **Home** tab, click **Your Desktop**, and then click **Project Your Desktop to All Desktop(s)**.
2. To end the projection, click **Stop** (either on the **Projection** tab or in the right-hand corner below the ribbon).

To project a different desktop to all desktops

1. Click the thumbnail image of the desktop you want to project to all desktops.
2. On the **Home** tab, click **Selected Desktop**, and then click **Selected Desktop**. The selected desktop is displayed on all desktops.
3. To end the projection, click **Stop** (either on the **Projection** tab or in the right-hand corner below the ribbon).

Launch or Close Applications on a Station

12/9/2022 • 2 minutes to read • Edit Online

As a MultiPoint Dashboard User, you can open or close an application on a user's desktop, selected desktops, or all desktops.

Launch an application on a user station

1. In MultiPoint Dashboard, click the thumbnail image of the user desktop on which you want to launch the application, and then click the drop–down menu for **Launch** in the ribbon under **Applications**.
2. Click **Launch an Application on Selected Desktops**. The **Launch Application** page opens.
3. Click the application you want to open, or in **Enter an application, folder, document, or Internet resource to open**, type the name of the resource you want to open, and then click **OK**.

Launch an application on all user stations

1. In MultiPoint Dashboard, click the drop–down menu for **Launch** (in the ribbon under **Applications**).
2. Click **Launch an Application on All Desktops**. The **Launch Application** page opens.
3. Click the application you want to open, or in **Enter an application, folder, document, or Internet resource to open**, type the name of the resource you want to open, and then click **OK**.

Close an application on a user station

1. In MultiPoint Dashboard, click the thumbnail image of the desktop on which you want to close an application.
2. Click **Close** in the ribbon under **Applications** to open the **Close Application** page.
3. Select the name of the application, folder, document, or Internet resource you want to close, and then click **Close Application**.

See Also

Manage User Desktops

Use IM

12/9/2022 • 2 minutes to read • Edit Online

If it has been enabled in the server settings, MultiPoint Dashboard users and station users can exchange private messages over IM.

To send a chat message from the MultiPoint Dashboard to a user

1. In MultiPoint Dashboard, click the thumbnail image or images of the user ypu want to send a message.
2. Click **Send** in the ribbon - an IM chat window opens.

> **NOTE**
>
> Users can IM the dashboard user by using the IM icon in the Windows taskbar. It is automatically pinned when IM is enabled in the server settings.

Take Control of a User Session

12/9/2022 • 2 minutes to read • Edit Online

As a MultiPoint Dashboard User, you can assist another user by remotely accessing his or her desktop using the Take Control feature.

1. In MultiPoint Dashboard, on the **Home** tab, click the thumbnail image of the desktop for the user you want to assist.
2. On the **Assist** tab, click **Take Control**. The user's desktop opens on your desktop, and then you can navigate their desktop using your keyboard and mouse.
3. When you are finished assisting the user, click **Stop**.

> **NOTE**
>
> You may need to minimize the user's desktop to see your MultiPoint Dashboard.

See Also

Manage User Desktops Using MultiPoint Dashboard

View Options for Session Thumbnails in MultiPoint Dashboard

12/9/2022 • 2 minutes to read • Edit Online

An easy way to monitor user activities on individual desktops is to view thumbnail images of each active desktop on your MultiPoint Services system. By default, images of desktops are displayed in MultiPoint Dashboard on the **Home** tab.

Using MultiPoint Dashboard, you can do the following:

- View a user's desktop more closely by enlarging its view in the dashboard.
- Change the size of the thumbnail images that are displayed in the dashboard. Three sizes are available for view: small, medium, or large. Medium is the default setting.
- View all desktops on the MultiPoint Services system, or choose a filtered view that shows active desktops.

To enlarge the view of a selected desktop in MultiPoint Dashboard

1. Click the **Home** tab, and then click the desktop you want to enlarge.
2. On the **Home** tab, click **Enlarge Selected**. The user's desktop opens in the dashboard.
3. When you are finished with the enlarged view, click Return to Desktops View.

To change the size of desktop thumbnails in MultiPoint Dashboard

1. Click the **Home** tab, and then select the desktop thumbnail you want to enlarge.
2. On the **Home** tab, click **Enlarge Selected**. The **Change Desktop Size** page opens.
3. Click the size you want (**Small**, **Medium**, or **Large**), and then click **OK**.

To show all desktops in MultiPoint Dashboard

1. Click the **Home** tab, and then click **Show** in the ribbon under **Desktops**..
2. Click **All**. All desktops are displayed in the dashboard.
3. To change back to the filtered view, click **Show**, and then click **Filtered View**.

> **NOTE**
>
> Right-click one or more thumbnails to get to additional actions you can take on active or inactive sessions, like **Log off Selected Users**. See Log Off User Sessions for more information.

See Also

Manage User Desktops Using MultiPoint Dashboard

Log Off User Sessions

12/9/2022 • 2 minutes to read • Edit Online

Standard users, MultiPoint Dashboard users, and administrative users can log on and log off of their desktop sessions as they would with any Windows session. In addition, administrative users and MultiPoint Dashboard users can end the user sessions on all of the monitored sessions on the MultiPoint Services system.

1. In MultiPoint Dashboard, click the **Home** tab.
2. Do one of the following:
   - To log off a single user session or selected sessions, click the thumbnail image of the session you want to end, and then click the top-left drop-down menu. Click **Log Off Users**, and then click **Log Off Selected Users**. You can also see this option by right-clicking the selected thumbnails.
   - To log off all user sessions, click the top-left drop-down menu, click **Log Off Users**, and then click **Log Off All Users**.

See Also

Manage User Desktops Log off or Disconnect User Sessions Suspend and Leave User Session Active

Manage MultiPoint Systems Using MultiPoint Dashboard

12/9/2022 • 2 minutes to read • Edit Online

In MultiPoint Dashboard, on the **Systems** tab, you can do the following:

- Restart or shut down selected systems You can restart or shut down selected MultiPoint Services systems. For information about restarting or shutting down selected systems, see the Restart or Shut Down MultiPoint Systems topic.
- Remap selected systems You can remap selected MultiPoint Services systems. For more information about remapping selected systems, see the Remap Selected MultiPoint Systems topic.

See Also

Restart or Shut Down MultiPoint Systems Remap Selected MultiPoint Systems

Restart or Shut Down

12/9/2022 • 2 minutes to read • Edit Online

You might have to restart the host computer and all of the *stations* in your MultiPoint Services system if instructed after you install hardware, software, and software updates. If you have added new hardware devices to a station, you might also want to associate the hardware devices to that station. For more information about how to *associate stations*, see the Switch Between Modes topic.

To turn off your MultiPoint Services system's computer safely, the computer must perform a shutdown process that closes any open programs, shuts down Windows, and turns off your computer and its associated *stations*. Do not just unplug or press the **Power** button to turn off your computer. You should shut down your computer at the end of the day and when you must install new hardware enclosed in the computer case. If you add other hardware to the system, you may also need to shut down or restart the server.

> **NOTE**
>
> Before you restart or shut down the computer that is running MultiPoint Services, all user *sessions* must have ended.

Restart the computer

1. End all user sessions. For more information about ending user sessions, see the End a User Session topic.
2. In MultiPoint Manager, click **Home**, and then click **Restart the computer**.

Shut down the computer

1. End all user sessions. For more information about ending user sessions, see the End a User Session topic.
2. In MultiPoint Manager, click the **Home** tab, and then click **Shut down the computer**.

See Also

End a User Session Manage System Tasks Using MultiPoint Manager Switch Between Modes Log off or Disconnect User Sessions

Remap Selected MultiPoint Systems

12/9/2022 • 2 minutes to read • Edit Online

Remapping stations in MultiPoint Dashboard allows you to associate keyboards and mice to monitors. Local user stations are suspended while a MultiPoint Services system is remapped.

Caution

Remapping is commonly used for troubleshooting purposes. Station settings, such as name and auto-logon information, are erased during the remapping process.

To remap a MultiPoint Services system

1. In MultiPoint Services, click the **Systems** tab.
2. Click the thumbnail image of the server you want to remap, and then, on the **Hardware** tab, click **Remap Selected System**.

Remote Server Administration Tools

12/9/2022 • 11 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic supports Remote Server Administration Tools for Windows 10.

> **IMPORTANT**
>
> Starting with Windows 10 October 2018 Update, RSAT is included as a set of **Features on Demand** in Windows 10 itself. See **When to use which RSAT version** below for installation instructions.

RSAT lets IT admins manage Windows Server roles and features from a Windows 10 PC.

Remote Server Administration Tools includes Server Manager, Microsoft Management Console (mmc) snap-ins, consoles, Windows PowerShell cmdlets and providers, and some command-line tools for managing roles and features that run on Windows Server.

Remote Server Administration Tools includes Windows PowerShell cmdlet modules that can be used to manage roles and features that are running on Remote servers. Although Windows PowerShell remote management is enabled by default on Windows Server 2016, it is not enabled by default on Windows 10. To run cmdlets that are part of Remote Server Administration Tools against a Remote server, run `Enable-PSremoting` in a Windows PowerShell session that has been opened with elevated user rights (that is, Run as Administrator) on your Windows client computer after installing Remote Server Administration Tools.

Remote Server Administration Tools for Windows 10

Use Remote Server Administration Tools for Windows 10 to manage specific technologies on computers that are running Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, and in limited cases, Windows Server 2012 , or Windows Server 2008 R2 .

Remote Server Administration Tools for Windows 10 includes support for remote management of computers that are running the Server Core installation option or the Minimal Server Interface configuration of Windows Server 2016, Windows Server 2012 R2 , and in limited cases, the Server Core installation options of Windows Server 2012. However, Remote Server Administration Tools for Windows 10 cannot be installed on any versions of the Windows Server operating system.

Tools available in this release

For a list of the tools available in Remote Server Administration Tools for Windows 10, see the table in Remote Server Administration Tools (RSAT) for Windows operating systems.

System requirements

Remote Server Administration Tools for Windows 10 can be installed only on computers that are running Windows 10. Remote Server Administration Tools cannot be installed on computers that are running Windows RT 8.1, or other system-on-chip devices.

Remote Server Administration Tools for Windows 10 runs on both x86-based and x64-based editions of Windows 10.

> **IMPORTANT**
> Remote Server Administration Tools for Windows 10 should not be installed on a computer that is running administration tools packs for Windows 8.1, Windows 8, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 or Windows 2000 Server. Remove all older versions of Administration Tools Pack or Remote Server Administration Tools, including earlier prerelease versions, and releases of the tools for different languages or locales from the computer before you install Remote Server Administration Tools for Windows 10.

To use this release of Server Manager to access and manage Remote servers that are running Windows Server 2012 R2 , Windows Server 2012 , or Windows Server 2008 R2 , you must install several updates to make the older Windows Server operating systems manageable by using Server Manager. For detailed information about how to prepare Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 for management by using Server Manager in Remote Server Administration Tools for Windows 10, see Manage Multiple, Remote Servers with Server Manager.

Windows PowerShell and Server Manager remote management must be enabled on remote servers to manage them by using tools that are part of Remote Server Administration Tools for Windows 10. Remote management is enabled by default on servers that are running Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012. For more information about how to enable remote management if it has been disabled, see Manage multiple, remote servers with Server Manager.

Install, uninstall and turn off/on RSAT tools

Use Features on Demand (FoD) to install specific RSAT tools on Windows 10 October 2018 Update, or later.

Starting with Windows 10 October 2018 Update, RSAT is included as a set of **Features on Demand** right from Windows 10. Now, instead of downloading an RSAT package you can just go to **Manage optional features** in **Settings** and click **Add a feature** to see the list of available RSAT tools. Select and install the specific RSAT tools you need. To see installation progress, click the **Back** button to view status on the **Manage optional features** page.

See the list of RSAT tools available via **Features on Demand**. In addition to installing via the graphical **Settings** app, you can also install specific RSAT tools via command line or automation using **DISM /Add-Capability**.

One benefit of Features on Demand is that installed features persist across Windows 10 version upgrades.

To uninstall specific RSAT tools on Windows 10 October 2018 Update or later (after installing with FoD)

On Windows 10, open the **Settings** app, go to **Manage optional features**, select and uninstall the specific RSAT tools you wish to remove. Note that in some cases, you will need to manually uninstall dependencies. Specifically, if RSAT tool A is needed by RSAT tool B, then choosing to uninstall RSAT tool A will fail if RSAT tool B is still installed. In this case, uninstall RSAT tool B first, and then uninstall RSAT tool A. Also note that in some cases, uninstalling an RSAT tool may appear to succeed even though the tool is still installed. In this case, restarting the PC will complete the removal of the tool.

See the list of RSAT tools including dependencies. In addition to uninstalling via the graphical Settings app, you can also uninstall specific RSAT tools via command line or automation using **DISM /Remove-Capability**.

When to use which RSAT version

If you have a version of Windows 10 prior to the October 2018 Update (1809), you will not be able to use **Features on Demand**. You will need to download and install the RSAT package.

- **Install RSAT FODs directly from Windows 10, as outlined above**: When installing on Windows 10 October 2018 Update (1809) or later, for managing Windows Server 2019 or previous versions.
- **Download and install WS_1803 RSAT package, as outlined below**: When installing on Windows

10 April 2018 Update (1803) or earlier, for managing Windows Server, version 1803 or Windows Server, version 1709.

- **Download and install WS2016 RSAT package, as outlined below**: When installing on Windows 10 April 2018 Update (1803) or earlier, for managing Windows Server 2016 or previous versions.

Download the RSAT package to install Remote Server Administration Tools for Windows 10

1. Download the Remote Server Administration Tools for Windows 10 package from the Microsoft Download Center. You can either run the installer from the Download Center website, or save the download package to a local computer or share.

   > **IMPORTANT**
   >
   > You can only install Remote Server Administration Tools for Windows 10 on computers that are running Windows 10. Remote Server Administration Tools cannot be installed on computers that are running Windows RT 8.1 or other system-on-chip devices.

2. If you save the download package to a local computer or share, double-click the installer program, **WindowsTH-KB2693643-x64.msu** or **WindowsTH-KB2693643-x86.msu**, depending on the architecture of the computer on which you want to install the tools.
3. When you are prompted by the **Windows Update Standalone Installer** dialog box to install the update, click **Yes**.
4. Read and accept the license terms. Click **I accept**.
5. Installation requires a few minutes to finish.

To uninstall Remote Server Administration Tools for Windows 10 after RSAT package install)

1. On the desktop, click **Start**, click **All Apps**, click **Windows System**, and then click **Control Panel**.
2. Under **Programs**, click **Uninstall a program**.
3. Click **View installed updates**.
4. Right-click **Update for Microsoft Windows (KB2693643)**, and then click **Uninstall**.
5. When you are asked if you are sure you want to uninstall the update, click **Yes**. S

To turn off specific tools (after RSAT package install)

6. On the desktop, click **Start**, click **All Apps**, click **Windows System**, and then click **Control Panel**.
7. Click **Programs**, and then in **Programs and Features** click **Turn Windows features on or off**.
8. In the **Windows Features** dialog box, expand **Remote Server Administration Tools**, and then expand either **Role Administration Tools** or **Feature Administration Tools**.
9. Clear the check boxes for any tools that you want to turn off.

   > **NOTE**
   >
   > If you turn off Server Manager, the computer must be restarted, and tools that were accessible from the **Tools** menu of Server Manager must be opened from the **Administrative Tools** folder.

10. When you are finished turning off tools that you do not want to use, click **OK**.

Run Remote Server Administration Tools

> **NOTE**
> After installing Remote Server Administration Tools for Windows 10, the **Administrative Tools** folder is displayed on the **Start** menu. You can access the tools from the following locations.
>
> - The **Tools** menu in the Server Manager console.
> - **Control Panel\System and Security\Administrative Tools**.
> - A shortcut saved to the desktop from the **Administrative Tools** folder (to do this, right click the **Control Panel\System and Security\Administrative Tools** link, and then click **Create Shortcut**).

The tools installed as part of Remote Server Administration Tools for Windows 10 cannot be used to manage the local client computer. Regardless of the tool you run, you must specify a remote server, or multiple remote servers, on which to run the tool. Because most tools are integrated with Server Manager, you add remote servers that you want to manage to the Server Manager server pool before managing the server by using the tools in the **Tools** menu. For more information about how to add servers to your server pool, and create custom groups of servers, see Add servers to Server Manager and Create and manage server groups.

In Remote Server Administration Tools for Windows 10, all GUI-based server management tools, such as mmc snap-ins and dialog boxes, are accessed from the **Tools** menu of the Server Manager console. Although the computer that runs Remote Server Administration Tools for Windows 10 runs a client-based operating system, after installing the tools, Server Manager, included with Remote Server Administration Tools for Windows 10, opens automatically by default on the client computer. Note that there is no **Local Server** page in the Server Manager console that runs on a client computer.

To start Server Manager on a client computer

1. On the **Start** menu, click **All Apps**, and then click **Administrative Tools**.
2. In the **Administrative Tools** folder, click **Server Manager**.

Although they are not listed in the Server Manager console **Tools** menu, Windows PowerShell cmdlets and Command prompt management tools are also installed for roles and features as part of Remote Server Administration Tools. For example, if you open a Windows PowerShell session with elevated user rights (Run as Administrator), and run the cmdlet `Get-Command -Module RDManagement`, the results include a list of remote Desktop Services cmdlets that are now available to run on the local computer after installing Remote Server Administration Tools, as long as the cmdlets are targeted at a remote server that is running all or part of the remote Desktop Services role.

To start Windows PowerShell with elevated user rights (Run as administrator)

1. On the **Start** menu, click **All Apps**, click **Windows System**, and then click **Windows PowerShell**.
2. To run Windows PowerShell as an administrator from the desktop, right-click the **Windows PowerShell** shortcut, and then click **Run as Administrator**.

> **NOTE**
> You can also start a Windows PowerShell session that is targeted at a specific server by right-clicking a managed server in a role or group page in Server Manager, and then clicking **Windows PowerShell**.

Known issues

Issue: RSAT FOD installation fails with error code 0x800f0954

> **Impact**: RSAT FODs on Windows 10 1809 (October 2018 Update) in WSUS/Configuration Manager environments
>
> **Resolution**: To install FODs on a domain-joined PC which receives updates through WSUS or Configuration

Manager, you will need to change a Group Policy setting to enable downloading FODs directly from Windows Update or a local share. For more details and instructions on how to change that setting, see How to make Features on Demand and language packs available when you're using WSUS/SCCM.

Issue: RSAT FOD installation via Settings app does not show status/progress

Impact: RSAT FODs on Windows 10 1809 (October 2018 Update)

Resolution: To see installation progress, click the **Back** button to view status on the **Manage optional features** page.

Issue: RSAT FOD uninstallation via Settings app may fail

Impact: RSAT FODs on Windows 10 1809 (October 2018 Update)

Resolution: In some cases, uninstallation failures are due to the need to manually uninstall dependencies. Specifically, if RSAT tool A is needed by RSAT tool B, then choosing to uninstall RSAT tool A will fail if RSAT tool B is still installed. In this case, uninstall RSAT tool B first, and then uninstall RSAT tool A. See the list of RSAT FODs including dependencies.

Issue: RSAT FOD uninstallation appears to succeed, but the tool is still installed

Impact: RSAT FODs on Windows 10 1809 (October 2018 Update)

Resolution: Restarting the PC will complete the removal of the tool.

Issue: RSAT missing after Windows 10 upgrade

Impact: Any RSAT .MSU package installation (prior to RSAT FODs) not automatically reinstalled

Resolution: An RSAT installation cannot be persisted across OS upgrades due to the RSAT .MSU being delivered as a Windows Update package. Please install RSAT again after upgrading Windows 10. Note that this limitation is one of the reasons why we've moved to FODs starting with Windows 10 1809. RSAT FODs which are installed will persist across future Windows 10 version upgrades.

See Also

- Remote Server Administration Tools for Windows 10
- Remote Server Administration Tools (RSAT) for Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 '

Welcome to Remote Desktop Services

12/9/2022 • 2 minutes to read • Edit Online

Remote Desktop Services (RDS) is the platform of choice for building virtualization solutions for every end customer need, including delivering individual virtualized applications, providing secure mobile and remote desktop access, and providing end users the ability to run their applications and desktops from the cloud.

RDS offers deployment flexibility, cost efficiency, and extensibility—all delivered through a variety of deployment options, including Windows Server 2016 for on-premises deployments, Microsoft Azure for cloud deployments, and a robust array of partner solutions.

Depending on your environment and preferences, you can set up the RDS solution for session-based virtualization, as a virtual desktop infrastructure (VDI), or as a combination of the two:

- **Session-based virtualization**: Leverage the compute power of Windows Server to provide a cost-effective multi-session environment to drive your users' everyday workloads.
- **VDI**: Leverage Windows client to provide the high performance, app compatibility, and familiarity that your users have come to expect of their Windows desktop experience.

Within these virtualization environments, you have additional flexibility in what you publish to your users:

- **Desktops**: Give your users a full desktop experience with a variety of applications that you install and manage. Ideal for users that rely on these computers as their primary workstations or that are coming from thin clients, such as with MultiPoint Services.
- **RemoteApps**: Specify individual applications that are hosted/run on the virtualized machine but appear as if they're running on the user's desktop like local applications. The apps have their own taskbar entry and can be resized and moved across monitors. Ideal for deploying and managing key applications in the secure, remote environment while allowing users to work from and customize their own desktops.

For environments where cost-effectiveness is crucial and you want to extend the benefits of deploying full desktops in a session-based virtualization environment, you can use MultiPoint Services to deliver the best value.

With these options and configurations, you have the flexibility to deploy the desktops and applications your users need in a remote, secure, and cost-effective fashion.

Next steps

Here are some next steps to help you get a better understanding of RDS and even start deploying your own environment:

- Understand the supported configurations for RDS with the various Windows and Windows Server versions
- Plan and design an RDS environment to accommodate various requirements, such as high availability and multi-factor authentication.
- Review the Remote Desktop Services architecture models that work best for your desired environment.
- Start to deploy your RDS environment with ARM and Azure Marketplace.

Remote access

12/9/2022 • 2 minutes to read • Edit Online

When you install the Remote Access Server Role with the *Add Roles and Features Wizard* or Windows PowerShell, you can choose to install one or more of the following three role services:

- Direct Access and VPN (RAS) service
- Routing service
- Web Application Proxy service

Anyone of these services can be installed either individually or on the same server.

> **IMPORTANT**
> Don't attempt to deploy Remote Access on a virtual machine (VM) in Microsoft Azure. Using Remote Access in Microsoft Azure is not supported. You can't use Remote Access in an Azure VM to deploy VPN, DirectAccess, or any other Remote Access feature in Windows Server. For more information, see Microsoft server software support for Microsoft Azure virtual machines.

DirectAccess and VPN service

VPN (RAS)

The VPN service uses the connectivity of the internet and a combination of tunneling and data encryption technologies to connect to remote clients and offices.

With VPN and Routing service, you can also choose to deploy Always On VPN. Always On VPN enables Windows 10 clients to securely access shared resources, intranet Web sites, and the applications on an internal network without having to manually connect. For more information, see Always On VPN

DirectAccess

DirectAccess allows connectivity for remote users to organization network resources without the need for traditional VPN connections. With DirectAccess connections, remote client computers are always connected to your organization. There's no need for remote users to start and stop connections, as is required with VPN connections. In addition, your IT administrators can manage DirectAccess client computers whenever they're' running and Internet connected.

> **IMPORTANT**
> For Windows 10 or later, it is recommended to connect using Always On VPN. DirectAccess should be used only for clients earlier than Windows 10.

Routing service

The Routing service allows you to route network traffic between subnets on your Local Area Network. Routing provides support for the following technologies:

- Network Address Translation (NAT) routers
- LAN routers running Border Gateway Protocol (BGP)
- Routing Information Protocol (RIP)

- Multicast-capable routers using Internet Group Management Protocol (IGMP)
- Demand-dial routing
- Unicast IP Routing

As a full-featured router, you can deploy RAS on either a physical computer or as a virtual machine (VM) on a computer that's running Hyper-V.

To install Remote Access as a LAN router, either use the *Add Roles and Features Wizard* in Server Manager and select the **Remote Access** server role and the **Routing** role service; or type the following command from an elevated Windows PowerShell prompt, and then press ENTER.

```
Install-RemoteAccess -VpnType RoutingOnly
```

Web Application Proxy service

Web Application Proxy service provides reverse proxy functionality for web applications inside your corporate network to allow users on any device to access them from outside the corporate network. Web Application Proxy pre-authenticates access to web applications using Active Directory Federation Services (AD FS), and also functions as an AD FS proxy.

To install Remote Access as a Web Application Proxy, either use the Add Roles and Features Wizard in Server Manager and select the **Remote Access** server role and the **Web Application Proxy** role service; or type the following command at a Windows PowerShell prompt, and then press ENTER.

```
Install-RemoteAccess -VpnType SstpProxy
```

For more information, see Web Application Proxy.

For more information about other networking technologies, see Networking in Windows Server.

Next Steps

Now you've learned about what the Remote Access role is, here are some articles that might help you during deployment:

- Always On VPN Deployment Guide
- Border Gateway Protocol (BGP)
- RAS Gateway
- Remote Access Server Role Documentation
- RAS Gateway for SDN
- Virtual Private Networking (VPN)

Deploy Always On VPN

12/9/2022 • 6 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows 11

In this tutorial, you'll learn how to deploy Always On VPN connections for remote domain-joined Windows client computers.

If you want to **configure conditional access** to fine-tune how VPN users access your resources, see Conditional access for VPN connectivity using Azure AD. To learn more about conditional access for VPN connectivity using Azure AD, see Conditional access in Azure Active Directory.

The following diagram illustrates the workflow process for the different scenarios when deploying Always On VPN:

Prerequisites

You most likely have the technologies deployed that you can use to deploy Always On VPN. Other than your DC/DNS servers, the Always On VPN deployment requires an NPS (RADIUS) server, a Certification Authority (CA) server, and a Remote Access (Routing/VPN) server. Once the infrastructure is set up, you must enroll clients and then connect the clients to your on-premises securely through several network changes.

- Active Directory domain infrastructure, including one or more Domain Name System (DNS) servers. Both internal and external Domain Name System (DNS) zones are required, which assumes that the internal zone is a delegated subdomain of the external zone (for example, corp.contoso.com and contoso.com).
- Active Directory-based public key infrastructure (PKI) and Active Directory Certificate Services (AD CS).
- Server, either virtual or physical, existing or new, to install Network Policy Server (NPS). If you already have NPS servers on your network, you can modify an existing NPS server configuration rather than add a new server.
- Remote Access as a RAS Gateway VPN server with a small subset of features supporting IKEv2 VPN connections and LAN routing.
- Perimeter network that includes two firewalls. Ensure that your firewalls allow the traffic that is necessary for both VPN and RADIUS communications to function properly. For more information, see Always On VPN Technology Overview.
- Physical server or virtual machine (VM) on your perimeter network with two physical Ethernet network adapters to install Remote Access as a RAS Gateway VPN server. VMs require virtual LAN (VLAN) for the host.
- Membership in Administrators, or equivalent, is the minimum required.
- Read the planning section of this guide to ensure that you are prepared for this deployment before you perform the deployment.
- Review the design and deployment guides for each of the technologies used. These guides can help you determine whether the deployment scenarios provide the services and configuration that you need for your

organization's network. For more information, see Always On VPN Technology Overview.

- Management platform of your choice for deploying the Always On VPN configuration because the CSP is not vendor-specific.

> **IMPORTANT**
>
> For this deployment, you can use all versions of Windows Server for the infrastructure servers and for the server that is running Remote Access.
>
> Don't attempt to deploy Remote Access on a virtual machine (VM) in Microsoft Azure. Using Remote Access in Microsoft Azure is not supported, including both Remote Access VPN and DirectAccess. For more information, see Microsoft server software support for Microsoft Azure virtual machines.

About this deployment

The instructions provided walk you through deploying Remote Access as a single tenant VPN RAS Gateway for point-to-site VPN connections, using any of the scenarios mentioned below, for remote client computers that are running Windows. You also find instructions for modifying some of your existing infrastructure for the deployment. Also throughout this deployment, you find links to help you learn more about the VPN connection process, servers to configure, ProfileXML VPNv2 CSP node, and other technologies to deploy Always On VPN.

Always On VPN deployment scenarios:

- Deploy Always On VPN only.
- Deploy Always On VPN with conditional access for VPN connectivity using Azure AD.

What isn't provided in this deployment

This deployment does not provide instructions for:

- Active Directory Domain Services (AD DS).
- Active Directory Certificate Services (AD CS) and a Public Key Infrastructure (PKI).
- Dynamic Host Configuration Protocol (DHCP).
- Network hardware, such as Ethernet cabling, firewalls, switches, and hubs.
- Additional network resources, such as application and file servers, that remote users can access over an Always On VPN connection.
- Internet connectivity or Conditional Access for Internet connectivity using Azure AD. For details, see Conditional access in Azure Active Directory.

Step 1. Plan the Always On VPN Deployment

In this step, you'll plan and prepare your Always On VPN deployment. Before you begin, you'll need to install the Remote Access server role on the computer you're planning on using as the VPN server. After proper planning, you can deploy Always On VPN, and optionally configure conditional access for VPN connectivity using Azure AD.

Step 2. Configure the Always On VPN Server Infrastructure

In this step, you install and configure the server-side components necessary to support the VPN. The server-side components include configuring PKI to distribute the certificates used by users, the VPN server, and the NPS server. You also configure RRAS to support IKEv2 connections and the NPS server to perform authorization for the VPN connections.

To configure the server infrastructure, you must perform the following tasks:

- **On a server configured with Active Directory Domain Services:** Enable certificate autoenrollment in Group Policy for both computers and users, create the VPN Users Group, the VPN Servers Group, and the NPS Servers Group, and add members to each group.
- **On an Active Directory Certificate Server CA:** Create the User Authentication, VPN Server Authentication, and NPS Server Authentication certificate templates.
- **On domain-joined Windows clients:** Enroll and validate user certificates.

Step 3. Configure the Remote Access Server for Always On VPN

In this step, you configure Remote Access VPN to allow IKEv2 VPN connections, deny connections from other VPN protocols, and assign a static IP address pool for the issuance of IP addresses to connecting authorized VPN clients.

To configure RAS, you must perform the following tasks:

- Enroll and validate the VPN server certificate
- Install and configure Remote Access VPN

Step 4. Install and Configure the NPS Server

In this step, you install Network Policy Server (NPS) by using either Windows PowerShell or the Server Manager Add Roles and Features Wizard. You also configure NPS to handle all authentication, authorization, and accounting duties for connection request that it receives from the VPN server.

To configure NPS, you must perform the following tasks:

- Register the NPS Server in Active Directory
- Configure RADIUS Accounting for your NPS Server
- Add the VPN Server as a RADIUS Client in NPS
- Configure Network Policy in NPS
- Autoenroll the NPS Server certificate

Step 5. Configure DNS and Firewall Settings for Always On VPN

In this step, you configure DNS and Firewall settings. When remote VPN clients connect, they use the same DNS servers that your internal clients use which allows them to resolve names in the same manner as the rest of your internal workstations.

Step 6. Configure Windows Client Always On VPN Connections

In this step, you configure the Windows client computers to communicate with that infrastructure with a VPN connection. You can use several technologies to configure Windows VPN clients, including Windows PowerShell, Microsoft Endpoint Configuration Manager, and Intune. All three require an XML VPN profile to configure the appropriate VPN settings.

Step 7. (Optional) Configure conditional access for VPN connectivity

In this optional step, you can fine-tune how authorized VPN users access your resources. With Azure AD conditional access for VPN connectivity, you can help protect the VPN connections. Conditional Access is a policy-based evaluation engine that lets you create access rules for any Azure AD connected application. For more information, see Azure Active Directory (Azure AD) conditional access.

Next step

Plan the Always On VPN deployment: This section will guide you on the next steps to take in preparing your Remote Access Server.

Step 1. Plan the Always On VPN deployment

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server, Windows Server 2012 R2, Windows 10

- **Next:** Step 2. Configure the Server Infrastructure

In this step of the tutorial, you'll learn how to plan and prepare your Always On VPN deployment.

Standard configuration considerations

Always On VPN has many standard configuration options. However, it is essential that you include the following information when creating your VPN configuration:

- **Connection type.** Virtual private networks (VPNs) are point-to-point connections across a private or public network, such as the Internet. A VPN client uses special TCP/IP or UDP-based protocols, called tunneling protocols, to connect to a VPN server. The connection type also determines which kind of authentication you will use. For details about the tunneling protocols available, see VPN connection types.
- **Routing.** In this context, routing rules determine whether users can use other network routes while connected to the VPN.
- **Triggering.** *Triggering* determines how and when a VPN connection is initiated (for example, when an app opens, when the device is turned on, manually by the user). For triggering options, see the VPN auto-triggered profile options.
- **Device or user authentication.** Always On VPN uses device certificates and device-initiated connection through a feature called Device Tunnel. A device tunnel can be initiated automatically and is persistent, resembling a DirectAccess infrastructure tunnel connection.

> **TIP**
> When migrating from DirectAccess to Always On VPN, consider starting with configuration options that are comparable to what you have, and then expand from there.

By using user certificates, the Always On VPN client connects automatically, but it does so at the user level (after user sign-in) instead of at the device level (before user sign-in). The experience is still seamless to the user, but it supports more advanced authentication mechanisms, like Windows Hello for Business.

Prepare the Remote Access Server

You must do the following on the computer used as a VPN server:

- **Make sure the VPN server software and hardware configuration is correct.** Install Windows Server on the computer that you plan to use as a Remote Access VPN server. This server must have two physical network adapters installed: one to connect to the external perimeter network, and one to connect to the internal perimeter network.
- **Identify which network adapter connects to the Internet and which network adapter connects to your private network.** Configure the network adapter facing the Internet with a public IP

address, while the adapter facing the intranet can use an IP address from the local network.

> **TIP**
> If you prefer not to use a public IP address on your perimeter network, you can configure the Edge Firewall with a public IP address, and then configure the firewall to forward VPN connection requests to the VPN server.

- **Connect the VPN server to the network**. Install the VPN server on a perimeter network, between the edge firewall and the perimeter firewall.

Plan Authentication Methods

IKEv2 is a VPN tunneling protocol described in Internet Engineering Task Force Request for Comments 7296. The primary advantage of IKEv2 is that it tolerates interruptions in the underlying network connection. For example, if a temporary loss in connection or if a user moves a client computer from one network to another, when reestablishing the network connection IKEv2 restores the VPN connection automatically — without user intervention.

> **TIP**
> You can configure the Remote Access VPN server to support IKEv2 connections while also disabling unused protocols, which reduces the server's security footprint.

Plan IP Addresses for Remote Clients

You can configure the VPN server to assign addresses to VPN clients from a static address pool that you configure or IP addresses from a DHCP server.

Prepare the Environment

- **Make sure that you have permissions to configure your external firewall and that you have a valid public IP address**. Open ports on the firewall to support IKEv2 VPN connections. You also need a public IP address to accept connections from external clients.
- **Choose a range of static IP addresses for VPN clients**. Determine the maximum number of simultaneous VPN clients that you want to support. Also, plan a range of static IP addresses on the internal perimeter network to meet that requirement, namely the *static address pool*. If you use DHCP to supply IP addresses on the internal DMZ, you might also need to create an exclusion for those static IP addresses in DHCP.
- **Make sure that you can edit your public DNS zone**. Add DNS records to your public DNS domain to support the VPN infrastructure.
- **Make sure that all VPN users have user accounts in Active Directory User (AD DS)**. Before users can connect to the network with VPN connections, they must have user accounts in AD DS.

Prepare Routing and Firewall

Install the VPN server inside the perimeter network, which partitions the perimeter network into internal and external perimeter networks. Depending on your network environment, you might need to make several routing modifications.

- **(Optional) Configure port forwarding.** Your edge firewall must open the ports and protocol IDs associated with an IKEv2 VPN and forward them to the VPN server. In most environments, doing so

requires you to configure port forwarding. Redirect Universal Datagram Protocol (UDP) ports 500 and 4500 to the VPN server.

- **Configure routing so that the DNS servers and VPN servers can reach the Internet**. This deployment uses IKEv2 and Network Address Translation (NAT). Make sure that the VPN server can reach all of the required internal networks and network resources. Any network or resource unreachable from the VPN server is also unreachable over VPN connections from remote locations.

In most environments, to reach the new internal perimeter network, adjust static routes on the edge firewall and the VPN server. In more complex environments, however, you may need to add static routes to internal routers or adjust internal firewall rules for the VPN server and the block of IP addresses associated with VPN clients.

Next steps

Step 2. Configure the Server Infrastructure: In this step, you install and configure the server-side components necessary to support the VPN. The server-side components include configuring PKI to distribute the certificates used by users, the VPN server, and the NPS server.

Step 2. Configure the server infrastructure

12/9/2022 • 14 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

- **Previous:** Step 1. Plan the Always On VPN Deployment
- **Next:** Step 3. Configure the Remote Access Server for Always On VPN

In this step, you'll install and configure the server-side components necessary to support the VPN. The server-side components include configuring PKI to distribute the certificates used by users, the VPN server, and the NPS server. You also configure RRAS to support IKEv2 connections and the NPS server to perform authorization for the VPN connections.

Configure certificate autoenrollment in Group Policy

In this procedure, you configure Group Policy on the domain controller so that domain members automatically request user and computer certificates. Doing so allows VPN users to request and retrieve user certificates that authenticate VPN connections automatically. Likewise, this policy allows NPS servers to request server authentication certificates automatically.

You manually enroll certificates on VPN servers.

> **TIP**
>
> For non-domained joined computers, see CA configuration for non-domain joined computers. Since the RRAS server is not domain joined, autoenrollment cannot be used to enroll the VPN gateway certificate. Therefore, use an offline certificate request procedure.

1. On a domain controller, open Group Policy Management.
2. In the navigation pane, right-click your domain (for example, corp.contoso.com), then select **Create a GPO in this domain, and Link it here**.
3. On the New GPO dialog box, enter **Autoenrollment Policy**, then select **OK**.
4. In the navigation pane, right-click **Autoenrollment Policy**, then select **Edit**.
5. In the Group Policy Management Editor, complete the following steps to configure computer certificate autoenrollment:
   a. In the navigation pane, go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**.
   b. In the details pane, right-click **Certificate Services Client – Auto-Enrollment**, then select **Properties**.
   c. On the Certificate Services Client – Auto-Enrollment Properties dialog box, in **Configuration Model**, select **Enabled**.
   d. Select **Renew expired certificates, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates**.

e. Select **OK**.

6. In the Group Policy Management Editor, complete the following steps to Configure user certificate autoenrollment:

   a. In the navigation pane, go to **User Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**.

   b. In the details pane, right-click **Certificate Services Client – Auto-Enrollment** and select **Properties**.

   c. On the Certificate Services Client – Auto-Enrollment Properties dialog box, in **Configuration Model**, select **Enabled**.

   d. Select **Renew expired certificates, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates**.

   e. Select **OK**.

   f. Close the Group Policy Management Editor.

7. Close Group Policy Management.

CA configuration for non-domain joined computers

Since the RRAS server is not domain joined, autoenrollment cannot be used to enroll the VPN gateway certificate. Therefore, use an offline certificate request procedure.

1. On the RRAS server, generate a file called **VPNGateway.inf** based upon the example certificate policy request provided in the example below and customize the following entries:

   - In the [NewRequest] section, replace vpn.contoso.com used for the Subject Name with the chosen [*Customer*] VPN endpoint FQDN.
   - In the [Extensions] section, replace vpn.contoso.com used for the Subject Alternate Name with the chosen [*Customer*] VPN endpoint FQDN.

2. Save or copy the **VPNGateway.inf** file to a chosen location.

3. From an elevated command prompt, navigate to the folder that contains the **VPNGateway.inf** file and type:

   ```
   certreq -new VPNGateway.inf VPNGateway.req
   ```

4. Copy the newly created **VPNGateway.req** output file to a Certification Authority server, or Privileged Access Workstation (PAW).

5. Save or copy the **VPNGateway.req** file to a chosen location on the Certification Authority server, or Privileged Access Workstation (PAW).

6. From an elevated command prompt, navigate to the folder that contains the VPNGateway.req file created in the previous step and type:

   ```
   certreq -attrib "CertificateTemplate:[Customer]VPNGateway" -submit VPNgateway.req VPNgateway.cer
   ```

7. If prompted by the Certification Authority List window, select the appropriate Enterprise CA to service the certificate request.

8. Copy the newly created **VPNGateway.cer** output file to the RRAS server.

9. Save or copy the **VPNGateway.cer** file to a chosen location on the RRAS server.
10. From an elevated command prompt, navigate to the folder that contains the VPNGateway.cer file created in the previous step and type:

    ```
    certreq -accept VPNGateway.cer
    ```

11. Run the Certificates MMC snap-in as described here selecting the **Computer account** option.
12. Ensure that a valid certificate exists for the RRAS server with the following properties:
    - **Intended Purposes:** Server Authentication, IP security IKE intermediate
    - **Certificate Template:** [*Customer*] VPN Server

Example: VPNGateway.inf script

Here you can see an example script of a certificate request policy used to request a VPN gateway certificate using an out-of-band process.

> **TIP**
> You can find a copy of the VPNGateway.inf script in the VPN Offering IP Kit under the Certificate Request Policies folder. Only update the 'Subject' and '_continue_' with customer-specific values.

```
[Version]

Signature="$Windows NT$"

[NewRequest]
Subject = "CN=vpn.contoso.com"
Exportable = FALSE
KeyLength = 2048
KeySpec = 1
KeyUsage = 0xA0
MachineKeySet = True
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
RequestType = PKCS10

[Extensions]
2.5.29.17 = "{text}"
_continue_ = "dns=vpn.contoso.com&"
```

Create the VPN Users, VPN Servers, and NPS Servers Groups

In this procedure, you can add a new Active Directory (AD) group that contains the users allowed to use the VPN to connect to your organization network.

This group serves two purposes:

- It defines which users are allowed to autoenroll for the user certificates the VPN requires.
- It defines which users the NPS authorizes for VPN access.

By using a custom group, if you ever want to revoke a user's VPN access, you can remove that user from the group.

You also add a group containing VPN servers and another group containing NPS servers. You use these groups to restrict certificate requests to their members.

> **NOTE**
> We recommend VPN servers that reside in the DMA/Perimeter not be domain-joined. However, if you prefer to have the VPN servers domain-joined for better manageability (Group Policies, Backup/Monitoring agent, no local users to manage, and so on), then add an AD group to the VPN server certificate template.

Configure the VPN Users group

1. On a domain controller, open Active Directory Users and Computers.
2. Right-click a container or organizational unit, select **New**, then select **Group**.
3. In **Group name**, enter **VPN Users**, then select **OK**.
4. Right-click **VPN Users** and select **Properties**.
5. On the **Members** tab of the VPN Users Properties dialog box, select **Add**.
6. On the Select Users dialog box, add all the users who need VPN access and select **OK**.
7. Close Active Directory Users and Computers.

Configure the VPN Servers and NPS Servers groups

1. On a domain controller, open Active Directory Users and Computers.
2. Right-click a container or organizational unit, select **New**, then select **Group**.
3. In **Group name**, enter **VPN Servers**, then select **OK**.
4. Right-click **VPN Servers** and select **Properties**.
5. On the **Members** tab of the VPN Servers Properties dialog box, select **Add**.
6. select **Object Types**, select the **Computers** check box, then select **OK**.
7. In **Enter the object names to select**, enter the names of your VPN servers, then select **OK**.
8. Select **OK** to close the VPN Servers Properties dialog box.
9. Repeat the previous steps for the NPS Servers group.
10. Close Active Directory Users and Computers.

Create the User Authentication template

In this procedure, you configure a custom client-server authentication template. This template is required because you want to improve the certificate's overall security by selecting upgraded compatibility levels and choosing the Microsoft Platform Crypto Provider. This last change lets you use the TPM on the client computers to secure the certificate. For an overview of the TPM, see Trusted Platform Module Technology Overview.

> **IMPORTANT**
> Microsoft Platform Crypto Provider" requires a TPM chip, in the case that you are running a VM and you get the following error: "Can not find a valid CSP in the local machine" when trying to manually enroll the certificate you need to check "Microsoft Software Key Storage Provider" and have it second in order after "Microsoft Platform Crypto Provider" in the Cryptography tab in certificate properties.

Procedure:

1. On the CA, open Certification Authority.

2. In the navigation pane, right-click **Certificate Templates** and select **Manage**.
3. In the Certificate Templates console, right-click **User** and select **Duplicate Template**.

> **WARNING**
> Do not select **Apply** or **OK** at any time prior to step 10. If you select these buttons before entering ALL parameters, many choices become fixed and no longer editable. For example, on the **Cryptography** tab, if *Legacy Cryptographic Storage Provider* shows in the Provider Category field, it becomes disabled, preventing any further change. The only alternative is to delete the template and recreate it.

4. On the Properties of New Template dialog box, on the **General** tab, complete the following steps:
   a. In **Template display name**, type **VPN User Authentication**.
   b. Clear the **Publish certificate in Active Directory** check box.
5. On the **Security** tab, complete the following steps:
   a. Select **Add**.
   b. On the Select Users, Computers, Service Accounts, or Groups dialog box, enter **VPN Users**, then select **OK**.
   c. In **Group or user names**, select **VPN Users**.
   d. In **Permissions for VPN Users**, select the **Enroll** and **Autoenroll** check boxes in the **Allow** column.

   > **TIP**
   > Make sure to keep the Read check box selected. In other words, you need the Read permissions for enrollment.

   e. In **Group or user names**, select **Domain Users**, then select **Remove**.
6. On the **Compatibility** tab, complete the following steps:
   a. In **Certification Authority**, select **Windows Server 2012 R2**.
   b. On the **Resulting changes** dialog box, select **OK**.
   c. In **Certificate recipient**, select **Windows 8.1/Windows Server 2012 R2**.
   d. On the **Resulting changes** dialog box, select **OK**.
7. On the **Request Handling** tab, clear the **Allow private key to be exported** check box.
8. On the **Cryptography** tab, complete the following steps:
   a. In **Provider Category**, select **Key Storage Provider**.
   b. Select **Requests must use one of the following providers**.
   c. Select the **Microsoft Platform Crypto Provider** check box.
9. On the **Subject Name** tab, if you don't have an email address listed on all user accounts, clear the **Include e-mail name in subject name** and **E-mail name** check boxes.
10. Select **OK** to save the VPN User Authentication certificate template.

11. Close the Certificate Templates console.
12. In the navigation pane of the Certification Authority snap-in, right-click **Certificate Templates**, select **New** and then select **Certificate Template to Issue**.
13. Select **VPN User Authentication**, then select **OK**.
14. Close the Certification Authority snap-in.

Create the VPN Server Authentication template

In this procedure, you can configure a new Server Authentication template for your VPN server. Adding the IP Security (IPsec) IKE Intermediate application policy allows the server to filter certificates if more than one certificate is available with the Server Authentication extended key usage.

> **IMPORTANT**
> Because VPN clients access this server from the public Internet, the subject and alternative names are different than the internal server name. As a result, you cannot autoenroll this certificate on VPN servers.

Prerequisites:

Domain-joined VPN servers

Procedure:

1. On the CA, open Certification Authority.
2. In the navigation pane, right-click **Certificate Templates** and select **Manage**.
3. In the Certificate Templates console, right-click **RAS and IAS Server** and select **Duplicate Template**.
4. On the Properties of New Template dialog box, on the **General** tab, in **Template display name**, enter a descriptive name for the VPN server, for example, **VPN Server Authentication** or **RADIUS Server**.
5. On the **Extensions** tab, complete the following steps:
   a. Select **Application Policies**, then select **Edit**.
   b. In the **Edit Application Policies Extension** dialog box, select **Add**.
   c. On the **Add Application Policy** dialog box, select **IP security IKE intermediate**, then select **OK**.

      Adding IP security IKE intermediate to the EKU helps in scenarios where more than one server authentication certificate exists on the VPN server. When IP security IKE intermediate is present, IPSec only uses the certificate with both EKU options. Without this, IKEv2 authentication could fail with Error 13801: IKE authentication credentials are unacceptable.

   d. Select **OK** to return to the **Properties of New Template** dialog box.
6. On the **Security** tab, complete the following steps:
   a. Select **Add**.
   b. On the **Select Users, Computers, Service Accounts, or Groups** dialog box, enter **VPN Servers**, then select **OK**.
   c. In **Group or user names**, select **VPN Servers**.
   d. In **Permissions for VPN Servers**, select the **Enroll** check box in the **Allow** column.

   e. In **Group or user names**, select **RAS and IAS Servers**, then select **Remove**.

7. On the **Subject Name** tab, complete the following steps:

   a. Select **Supply in the Request**.

   b. On the **Certificate Templates** warning dialog box, select **OK**.

8. (Optional) If you're configuring conditional access for VPN connectivity, select the **Request Handling** tab, then select **Allow private key to be exported**.

9. Select **OK** to save the VPN Server certificate template.

10. Close the Certificate Templates console.

11. Restart the Certificate Authority services.(*)

12. In the navigation pane of the Certification Authority snap-in, right-click **Certificate Templates**, select **New** and then select **Certificate Template to Issue**.

13. Select the name you chose in step 4 above, and click **OK**.

14. Close the Certification Authority snap-in.

- **You can stop/start the CA service by running the following command in CMD:**

```
net stop "certsvc"
net start "certsvc"
```

Create the NPS Server Authentication template

The third and last certificate template to create is the NPS Server Authentication template. The NPS Server Authentication template is a simple copy of the RAS and IAS Server template secured to the NPS Server group that you created earlier in this section.

You will configure this certificate for autoenrollment.

Procedure:

1. On the CA, open Certification Authority.

2. In the navigation pane, right-click **Certificate Templates** and select **Manage**.

3. In the Certificate Templates console, right-click **RAS and IAS Server**, and select **Duplicate Template**.

4. On the Properties of New Template dialog box, on the **General** tab, in **Template display name**, type **NPS Server Authentication**.

5. On the **Security** tab, complete the following steps:

   a. Select **Add**.

   b. On the **Select Users, Computers, Service Accounts, or Groups** dialog box, enter **NPS Servers**, then select **OK**.

   c. In **Group or user names**, select **NPS Servers**.

   d. In **Permissions for NPS Servers**, select the **Enroll** and **Autoenroll** check boxes in the **Allow** column.

   e. In **Group or user names**, select **RAS and IAS Servers**, then select **Remove**.

6. Select **OK** to save the NPS Server certificate template.
7. Close the Certificate Templates console.
8. In the navigation pane of the Certification Authority snap-in, right-click **Certificate Templates**, select **New** and then select **Certificate Template to Issue**.
9. Select **NPS Server Authentication**, and select **OK**.
10. Close the Certification Authority snap-in.

Enroll and validate the user certificate

Because you're using Group Policy to autoenroll user certificates, you need only update the policy, and Windows 10 will automatically enroll the user account for the correct certificate. You can then validate the certificate in the Certificates console.

Procedure:

1. Sign in to a domain-joined client computer as a member of the **VPN Users** group.
2. Press Windows key + R, type **gpupdate /force**, and press Enter.
3. On the Start menu, type **certmgr.msc**, and press Enter.
4. In the Certificates snap-in, under **Personal**, select **Certificates**. Your certificates appear in the details pane.
5. Right-click the certificate that has your current domain username, and then select **Open**.
6. On the **General** tab, confirm that the date listed under **Valid from** is today's date. If it isn't, you might have selected the wrong certificate.
7. Select **OK**, and close the Certificates snap-in.

Enroll and validate the server certificates

Unlike the user certificate, you must manually enroll the VPN server's certificate. After you've enrolled it, validate it by using the same process you used for the user certificate. Like the user certificate, the NPS server automatically enrolls its authentication certificate, so all you need to do is validate it.

> **NOTE**
> You might need to restart the VPN and NPS servers to allow them to update their group memberships before you can complete these steps.

Enroll and validate the VPN server certificate

1. On the VPN server's Start menu, type **certlm.msc**, and press Enter.
2. Right-click **Personal**, select **All Tasks** and then select **Request New Certificate** to start the Certificate Enrollment Wizard.
3. On the Before You Begin page, select **Next**.
4. On the Select Certificate Enrollment Policy page, select **Next**.
5. On the Request Certificates page, select the check box next to the VPN server to select it.
6. Under the VPN server check box, select **More information is required** to open the Certificate Properties dialog box and complete the following steps:

a. Select the **Subject** tab, select **Common Name** under **Subject name**, in **Type**.

b. Under **Subject name**, in **Value**, enter the name of the external domain clients used to connect to the VPN, for example, vpn.contoso.com, then select **Add**.

c. Under **Alternative Name**, in **Type**, select **DNS**.

d. Under **Alternative Name**, in **Value**, enter all of the server names clients use to connect to the VPN, for example, vpn.contoso.com, vpn, 132.64.86.2.

e. Select **Add** after entering each name.

f. Select **OK** when finished.

7. Select **Enroll**.

8. Select **Finish**.

9. In the Certificates snap-in, under **Personal**, select **Certificates**.

   Your listed certificates appear in the details pane.

10. Right-click the certificate that has your VPN server's name, and then select **Open**.

11. On the **General** tab, confirm that the date listed under **Valid from** is today's date. If it isn't, you might have selected the incorrect certificate.

12. On the **Details** tab, select **Enhanced Key Usage**, and verify that **IP security IKE intermediate** and **Server Authentication** display in the list.

13. Select **OK** to close the certificate.

14. Close the Certificates snap-in.

Validate the NPS server certificate

1. Restart the NPS server.

2. On the NPS server's Start menu, type **certlm.msc**, and press Enter.

3. In the Certificates snap-in, under **Personal**, select **Certificates**.

   Your listed certificates appear in the details pane.

4. Right-click the certificate that has your NPS server's name, and then select **Open**.

5. On the **General** tab, confirm that the date listed under **Valid from** is today's date. If it isn't, you might have selected the incorrect certificate.

6. Select **OK** to close the certificate.

7. Close the Certificates snap-in.

Next steps

Step 3. Configure the Remote Access Server for Always On VPN: In this step, you configure Remote Access VPN to allow IKEv2 VPN connections, deny connections from other VPN protocols, and assign a static IP address pool for issuance of IP addresses to connecting authorized VPN clients.

Step 3. Configure the Remote Access Server for Always On VPN

12/9/2022 • 8 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

- **Previous:** Step 2. Configure the Server Infrastructure
- **Previous:** Step 4. Install and configure the Network Policy Server (NPS)

RRAS is designed to perform well as both a router and a remote access server because it supports a wide array of features. For the purposes of this deployment, you require only a small subset of these features: support for IKEv2 VPN connections and LAN routing.

IKEv2 is a VPN tunneling protocol described in Internet Engineering Task Force Request for Comments 7296. The primary advantage of IKEv2 is that it tolerates interruptions in the underlying network connection. For example, if the connection is temporarily lost or if a user moves a client computer from one network to another, IKEv2 automatically restores the VPN connection when the network connection is reestablished—all without user intervention.

Configure the RRAS server to support IKEv2 connections while disabling unused protocols, which reduces the server's security footprint. Additionally, configure the server to assign addresses to VPN clients from a static address pool. You can feasibly assign addresses from either a pool or a DHCP server; however, using a DHCP server adds complexity to the design and delivers minimal benefits.

> **IMPORTANT**
>
> It is important to:
>
> - Install two Ethernet network adapters in the physical server. If you are installing the VPN server on a VM, you must create two External virtual switches, one for each physical network adapter; and then create two virtual network adapters for the VM, with each network adapter connected to one virtual switch.
> - Install the server on your perimeter network between your edge and internal firewalls, with one network adapter connected to the External Perimeter Network, and one network adapter connected to the Internal Perimeter Network.

> **WARNING**
>
> Before you get started, make sure to enable IPv6 on the VPN server. Otherwise, a connection cannot be established and an error message displays.

Install Remote Access as a RAS Gateway VPN Server

In this procedure, you install the Remote Access role as a single tenant RAS Gateway VPN server. For more information, see Remote Access.

Install the Remote Access role by using Windows PowerShell

1. Open Windows PowerShell as **Administrator**.

2. Enter and run the following cmdlet:

```
Install-WindowsFeature DirectAccess-VPN -IncludeManagementTools
```

After installation completes, the following message appears in Windows PowerShell.

```
| Success | Restart Needed | Exit Code |               Feature Result               |
|---------|----------------|-----------|--------------------------------------------|
|  True   |       No       |  Success  | {RAS Connection Manager Administration Kit |
```

Install the Remote Access role by using Server Manager

You can use the following procedure to install the Remote Access role using Server Manager.

1. On the VPN server, in Server Manager, select **Manage** and select **Add Roles and Features**.

   The Add Roles and Features Wizard opens.

2. On the Before you begin page, select **Next**.
3. On the Select Installation Type page, select the **Role-Based or feature-based installation** option and select **Next**.
4. On the Select destination server page, select the **Select a server from the server pool** option.
5. Under Server Pool, select the local computer and select **Next**.
6. On the Select server roles page, in **Roles**, select **Remote Access**, then **Next**.
7. On the Select features page, select **Next**.
8. On the Remote Access page, select **Next**.
9. On the Select role service page, in **Role services**, select **DirectAccess and VPN (RAS)**.

The **Add Roles and Features Wizard** dialog box opens.

11. On the Add Roles and Features dialog, select **Add Features** then select **Next**.
12. On the Web Server Role (IIS) page, select **Next**.
13. On the Select role services page, select **Next**.
14. On the Confirm installation selections page, review your choices, then select **Install**.
15. When the installation is complete, select **Close**.

Configure Remote Access as a VPN Server

In this section, you can configure Remote Access VPN to allow IKEv2 VPN connections, deny connections from other VPN protocols, and assign a static IP address pool for the issuance of IP addresses to connecting authorized VPN clients.

1. On the VPN server, in Server Manager, select the **Notifications** flag.
2. In the **Tasks** menu, select **Open the Getting Started Wizard**

   The Configure Remote Access wizard opens.

> **NOTE**
> The Configure Remote Access wizard might open behind Server Manager. If you think the wizard is taking too long to open, move or minimize Server Manager to find out whether the wizard is behind it. If not, wait for the wizard to initialize.

3. Select **Deploy VPN only**.

   The Routing and Remote Access Microsoft Management Console (MMC) opens.

4. Right-click the VPN server, then select **Configure and Enable Routing and Remote Access**.

   The Routing and Remote Access Server Setup Wizard opens.

5. In the Welcome to the Routing and Remote Access Server Setup Wizard, select **Next**.

6. In **Configuration**, select **Custom Configuration**, and then select **Next**.

7. In **Custom Configuration**, select **VPN access**, and then select **Next**.

   The Completing the Routing and Remote Access Server Setup Wizard opens.

8. Select **Finish** to close the wizard, then select **OK** to close the Routing and Remote Access dialog box.

9. Select **Start service** to start Remote Access.

10. In the Remote Access MMC, right-click the VPN server, then select **Properties**.

11. In Properties, select the **Security** tab and do:

    a. Select **Authentication provider** and select **RADIUS Authentication**.

    b. Select **Configure**.

    The RADIUS Authentication dialog box opens.

    c. Select **Add**.

    The Add RADIUS Server dialog box opens.

    d. In **Server name**, enter the Fully Qualified Domain Name (FQDN) of the NPS server on your Organization/Corporate network.

    For example, if the NetBIOS name of your NPS server is NPS1 and your domain name is corp.contoso.com, enter **NPS1.corp.contoso.com**.

    e. In **Shared secret**, select **Change**.

    The Change Secret dialog box opens.

    f. In **New secret**, enter a text string.

    g. In **Confirm new secret**, enter the same text string, then select **OK**.

    > **IMPORTANT**
    > Save this text string. When you configure the NPS Server on your Organization/Corporate network, you will add this VPN Server as a RADIUS Client. During that configuration, you will use this same shared secret so that the NPS and VPN Servers can communicate.

12. In **Add RADIUS Server**, review the default settings for:

- **Time-out**
- **Initial score**
- **Port**

13. If necessary, change the values to match the requirements for your environment and select **OK**.

    A NAS is a device that provides some level of access to a larger network. A NAS using a RADIUS infrastructure is also a RADIUS client, sending connection requests and accounting messages to a RADIUS server for authentication, authorization, and accounting.

14. Review the setting for **Accounting provider**:

IF YOU WANT THE...	THEN...
Remote Access activity logged on the Remote Access server	Make sure that **Windows Accounting** is selected.
NPS to perform accounting services for VPN	Change **Accounting provider** to **RADIUS Accounting** and then configure the NPS as the accounting provider.

15. Select the **IPv4** tab and do:

    a. Select **Static address pool**.

    b. Select **Add** to configure an IP address pool.

    The static address pool should contain addresses from the internal perimeter network. These addresses are on the internal-facing network connection on the VPN server, not the corporate network.

    c. In **Start IP address**, enter the starting IP address in the range you want to assign to VPN clients.

    d. In **End IP address**, enter the ending IP address in the range you want to assign to VPN clients, or in **Number of addresses**, enter the number of the address you want to make available. If you're using DHCP for this subnet, ensure that you configure a corresponding address exclusion on your DHCP servers.

    > **NOTE**
    > For optimal network performance, the VPN server itself should not have a network interface in the same IPv4 subnet that assigns IPv4 addresses to the clients. If the VPN server does have a network interface in that subnet, a broadcast or multicast that is sent to that subnet could cause a latency spike.

    e. (Optional) If you are using DHCP, select **Adapter**, and in the list of results, select the Ethernet adapter connected to your internal perimeter network.

16. (Optional) *If you are configuring conditional access for VPN connectivity*, from the **Certificate** drop-down list, under **SSL Certificate Binding**, select the VPN server authentication.

17. (Optional) *If you are configuring conditional access for VPN connectivity*, in the NPS MMC, expand **Policies\Network Policies** and do:

    a. Right-the **Connections to Microsoft Routing and Remote Access Server** network policy and select **Properties**.

    b. Select the **Grant access. Grant access if the connection request matches this policy** option.

c. Under Type of network access server, select **Remote Access Server (VPN-Dial up)** from the drop-down.

18. In the Routing and Remote Access MMC, right-click **Ports,** and then select **Properties**.

    The Ports Properties dialog box opens.

19. Select **WAN Miniport (SSTP)** and select **Configure**. The Configure Device - WAN Miniport (SSTP) dialog box opens.

    a. Clear the **Remote access connections (inbound only)** and **Demand-dial routing connections (inbound and outbound)** check boxes.

    b. Select **OK**.

20. Select **WAN Miniport (L2TP)** and select **Configure**. The Configure Device - WAN Miniport (L2TP) dialog box opens.

    a. In **Maximum ports**, enter the number of ports to match the maximum number of simultaneous VPN connections that you want to support.

    b. Select **OK**.

21. Select **WAN Miniport (PPTP)** and select **Configure**. The Configure Device - WAN Miniport (PPTP) dialog box opens.

    a. In **Maximum ports**, enter the number of ports to match the maximum number of simultaneous VPN connections that you want to support.

    b. Select **OK**.

22. Select **WAN Miniport (IKEv2)** and select **Configure**. The Configure Device - WAN Miniport (IKEv2) dialog box opens.

    a. In **Maximum ports**, enter the number of ports to match the maximum number of simultaneous VPN connections that you want to support.

    b. Select **OK**.

23. If prompted, select **Yes** to confirm restarting the server and select **Close** to restart the server.

Next step

Step 4. Install and configure the Network Policy Server (NPS): In this step, you install Network Policy Server (NPS) by using either Windows PowerShell or the Server Manager Add Roles and Features Wizard. You also configure NPS to handle all authentication, authorization, and accounting duties for connection requests that it receives from the VPN server.

Step 4. Install and configure the Network Policy Server (NPS)

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

- **Next:** Step 3. Configure the Remote Access Server for Always On VPN
- **Next:** Step 5. Configure DNS and Firewall Settings

In this step, you'll install Network Policy Server (NPS) for processing of connection requests that are sent by the VPN server:

- Perform authorization to verify that the user has permission to connect.
- Performing authentication to verify the user's identity.
- Performing accounting to log the aspects of the connection request that you chose when you configured RADIUS accounting in NPS.

The steps in this section allow you to complete the following items:

1. On the computer or VM that planned for the NPS server, and installed on your organization or corporate network, you can install NPS.

   > **TIP**
   > If you already have one or more NPS servers on your network, you do not need to perform NPS Server installation - instead, you can use this topic to update the configuration of an existing NPS server.

> **NOTE**
> You can not install the Network Policy Server service on Windows Server Core.

2. On the organization/corporate NPS server, you can configure NPS to perform as a RADIUS server that processes the connection requests received from the VPN server.

Install Network Policy Server

In this procedure, you install NPS by using either Windows PowerShell or the Server Manager Add Roles and Features Wizard. NPS is a role service of the Network Policy and Access Services server role.

> **TIP**
> By default, NPS listens for RADIUS traffic on ports 1812, 1813, 1645, and 1646 on all installed network adapters. When you install NPS, and you enable Windows Firewall with Advanced Security, firewall exceptions for these ports get created automatically for both IPv4 and IPv6 traffic. If your network access servers are configured to send RADIUS traffic over ports other than these defaults, remove the exceptions created in Windows Firewall with Advanced Security during NPS installation, and create exceptions for the ports that you do use for RADIUS traffic.

Procedure for Windows PowerShell:

To perform this procedure by using Windows PowerShell, run Windows PowerShell as Administrator, enter the following cmdlet:

```
Install-WindowsFeature NPAS -IncludeManagementTools
```

Procedure for Server Manager:

1. In Server Manager, select **Manage**, then select **Add Roles and Features**. The Add Roles and Features Wizard opens.
2. In Before You Begin, select **Next**.

   > **NOTE**
   > The **Before You Begin** page of the Add Roles and Features Wizard is not displayed if you had previously selected **Skip this page by default** when the Add Roles and Features Wizard ran.

3. In Select Installation Type, ensure that **Role-Based or feature-based installation** is selected, and select **Next**.
4. In Select destination server, ensure that **Select a server from the server pool** is selected.
5. In Server Pool, ensure that the local computer is selected and select **Next**.
6. In Select Server Roles, in **Roles**, select **Network Policy and Access Services**. A dialog box opens asking if it should add features required for Network Policy and Access Services.
7. Select **Add Features**, then select **Next**
8. In Select features, select **Next**, and in Network Policy and Access Services, review the information provided, then select **Next**.
9. In Select role services, select **Network Policy Server**.
10. For features required for Network Policy Server, select **Add Features**, then select **Next**.
11. In Confirm installation selections, select **Restart the destination server automatically if required**.
12. Select **Yes** to confirm the selected, and then select **Install**.

    The Installation progress page displays the status during the installation process. When the process completes, the message "Installation succeeded on *ComputerName*" is displayed, where *ComputerName* is the name of the computer upon which you installed Network Policy Server.

13. Select **Close**.

Configure NPS

After installing NPS, you configure NPS to handle all authentication, authorization, and accounting duties for connection request it receives from the VPN server.

Register the NPS Server in Active Directory

In this procedure, you register the server in Active Directory so that it has permission to access user account information while processing connection requests.

Procedure:

1. In Server Manager, select **Tools**, and then select **Network Policy Server**. The NPS console opens.
2. In the NPS console, right-click **NPS (Local)**, then select **Register server in Active Directory**.

   The Network Policy Server dialog box opens.
3. In the Network Policy Server dialog box, select **OK** twice.

For alternate methods of registering NPS, see Register an NPS Server in an Active Directory Domain.

Configure Network Policy Server Accounting

In this procedure, configure Network Policy Server Accounting using one of the following logging types:

- **Event logging**. Used primarily for auditing and troubleshooting connection attempts. You can configure NPS event logging by obtaining the NPS server properties in the NPS console.
- **Logging user authentication and accounting requests to a local file**. Used primarily for connection analysis and billing purposes. Also used as a security investigation tool because it provides you with a method of tracking the activity of a malicious user after an attack. You can configure local file logging using the Accounting Configuration wizard.
- **Logging user authentication and accounting requests to a Microsoft SQL Server XML-compliant database**. Used to allow multiple servers running NPS to have one data source. Also provides the advantages of using a relational database. You can configure SQL Server logging by using the Accounting Configuration wizard.

To configure Network Policy Server Accounting, see Configure Network Policy Server Accounting.

Add the VPN Server as a RADIUS Client

In the Configure the Remote Access Server for Always On VPN section, you installed and configured your VPN server. During VPN server configuration, you added a RADIUS shared secret on the VPN server.

In this procedure, you use the same shared secret text string to configure the VPN server as a RADIUS client in NPS. Use the same text string that you used on the VPN server, or communication between the NPS server and VPN server fails.

> **IMPORTANT**
> When you add a new network access server (VPN server, wireless access point, authenticating switch, or dial-up server) to your network, you must add the server as a RADIUS client in NPS so that NPS is aware of and can communicate with the network access server.

Procedure:

1. On the NPS server, in the NPS console, double-click **RADIUS Clients and Servers**.
2. Right-click **RADIUS Clients** and select **New**. The New RADIUS Client dialog box opens.
3. Verify that the **Enable this RADIUS client** check box is selected.
4. In **Friendly name**, enter a display name for the VPN server.
5. In **Address (IP or DNS)**, enter the NAS IP address or FQDN.

   If you enter the FQDN, select **Verify** if you want to verify that the name is correct and maps to a valid IP address.
6. In **Shared secret**, do:

   a. Ensure that **Manual** is selected.

b. Enter the strong text string that you also entered on the VPN server.

c. Reenter the shared secret in Confirm shared secret.

7. Select **OK**. The VPN Server appears in the list of RADIUS clients configured on the NPS server.

Configure NPS as a RADIUS for VPN Connections

In this procedure, you configure NPS as a RADIUS server on your organization network. On the NPS, you must define a policy that allows only users in a specific group to access the Organization/Corporate network through the VPN Server - and then only when using a valid user certificate in a PEAP authentication request.

Procedure:

1. In the NPS console, in Standard Configuration, ensure that **RADIUS server for Dial-Up or VPN Connections** is selected.

2. Select **Configure VPN or Dial-Up**.

   The Configure VPN or Dial-Up wizard opens.

3. Select **Virtual Private Network (VPN) Connections**, and select **Next**.

4. In Specify Dial-Up or VPN Server, in RADIUS clients, select the name of the VPN Server that you added in the previous step. For example, if your VPN server NetBIOS name is RAS1, select **RAS1**.

5. Select **Next**.

6. In Configure Authentication Methods, complete the following steps:

   a. Clear the **Microsoft Encrypted Authentication version 2 (MS-CHAPv2)** check box.

   b. Select the **Extensible Authentication Protocol** check box to select it.

   c. In Type (based on the method of access and network configuration), select **Microsoft: Protected EAP (PEAP)**, then select **Configure**.

      The Edit Protected EAP Properties dialog box opens.

   d. Select **Remove** to remove the Secured Password (EAP-MSCHAP v2) EAP type.

   e. Select **Add**. The Add EAP dialog box opens.

   f. Select **Smart Card or other certificate**, then select **OK**.

   g. Select **OK** to close Edit Protected EAP Properties.

7. Select **Next**.

8. In Specify User Groups, complete the following steps:

   a. Select **Add**. The Select Users, Computers, Service Accounts, or Groups dialog box opens.

   b. Enter **VPN Users**, then select **OK**.

   c. Select **Next**.

9. In Specify IP Filters, select **Next**.

10. In Specify Encryption Settings, select **Next**. Do not make any changes.

    These settings apply only to Microsoft Point-to-Point Encryption (MPPE) connections, which this scenario doesn't support.

11. In Specify a Realm Name, select **Next**.
12. Select **Finish** to close the wizard.

Autoenroll the NPS Server Certificate

In this procedure, you refresh Group Policy on the local NPS server manually. When Group Policy refreshes, if certificate autoenrollment is configured and functioning correctly, the local computer is auto-enrolled a certificate by the certification authority (CA).

> **NOTE**
> Group Policy refreshed automatically when you restart the domain member computer, or when a user logs on to a domain member computer. Also, Group Policy periodically refreshes. By default, this periodic refresh happens every 90 minutes with a randomized offset of up to 30 minutes.

Membership in **Administrators**, or equivalent, is the minimum required to complete this procedure.

Procedure:

1. On the NPS, open Windows PowerShell.
2. At the Windows PowerShell prompt, type **gpupdate**, and then press ENTER.

Next steps

Step 5. Configure DNS and firewall settings for Always On VPN: In this step, configure DNS and firewall settings for VPN connectivity.

Step 5. Configure DNS and firewall settings

12/9/2022 • 4 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

- **Previous:** Step 4. Install and Configure the NPS Server
- **Next:** Step 6. Configure Windows 10 Client Always On VPN Connections

In this step, you configure DNS and Firewall settings for VPN connectivity.

Configure DNS name resolution

When remote VPN clients connect, they use the same DNS servers that your internal clients use, which allows them to resolve names in the same manner as the rest of your internal workstations.

Because of this, you must ensure that the computer name that external clients use to connect to the VPN server matches the subject alternative name defined in certificates issued to the VPN server.

To ensure that remote clients can connect to your VPN server, you can create a DNS A (Host) record in your external DNS zone. The A record should use the certificate subject alternative name for the VPN server.

To add a host (A or AAAA) resource record to a zone

1. On a DNS server, in Server Manager, select **Tools**, and then select **DNS**. DNS Manager opens.
2. In the DNS Manager console tree, select the server that you want to manage.
3. In the details pane, in **Name**, double-click **Forward Lookup Zones** to expand the view.
4. In **Forward Lookup Zones** details, right-click the forward lookup zone to which you want to add a record, and then select **New Host (A or AAAA)**. The **New Host** dialog box opens.
5. In **New Host**, in **Name**, enter the certificate subject alternative name for the VPN server.
6. In IP address, enter the IP address for the VPN server. You can enter the address in IP version 4 (IPv4) format to add a host (A) resource record, or IP version 6 (IPv6) format to add a host (AAAA) resource record.
7. If you created a reverse lookup zone for a range of IP addresses, including the IP address that you entered, then select the **Create associated pointer (PTR) record** check box. Selecting this option creates an additional pointer (PTR) resource record in a reverse zone for this host, based on the information you entered in **Name** and **IP address**.
8. Select **Add Host**.

Configure the Edge Firewall

The Edge Firewall separates the External Perimeter Network from the Public Internet. For a visual representation of this separation, see the illustration in the topic Always On VPN Technology Overview.

Your Edge Firewall must allow and forward specific ports to your VPN server. If you use Network Address Translation (NAT) on your edge firewall, you might need to enable port forwarding for User Datagram Protocol (UDP) ports 500 and 4500. Forward these ports to the IP address that is assigned to the external interface of your VPN server.

If you're routing traffic inbound and performing NAT at or behind the VPN server, then you must open your firewall rules to allow UDP ports 500 and 4500 inbound to the external IP address applied to the public interface on the VPN server.

In either case, if your firewall supports deep packet inspection and you have difficulty establishing client connections, you should attempt to relax or disable deep packet inspection for IKE sessions.

For information on how to make these configuration changes, see your firewall documentation.

Configure the Internal Perimeter Network Firewall

The Internal Perimeter Network Firewall separates the Organization/Corporate Network from the Internal Perimeter Network. For a visual representation of this separation, see the illustration in the topic Always On VPN Technology Overview.

In this deployment, the Remote Access VPN server on the perimeter network is configured as a RADIUS client. The VPN server sends RADIUS traffic to the NPS on the corporate network and also receives RADIUS traffic from the NPS.

Configure the firewall to allow RADIUS traffic to flow in both directions.

> **NOTE**
> The NPS server on the Organization/Corporate network functions as a RADIUS Server for the VPN Server, which is a RADIUS Client. For more information about the RADIUS infrastructure, see Network Policy Server (NPS).

RADIUS Traffic Ports on the VPN Server and NPS Server

By default, NPS and VPN listen for RADIUS traffic on ports 1812, 1813, 1645, and 1646 on all installed network adapters. If you enable Windows Firewall with Advanced Security when installing NPS, firewall exceptions for these ports get created automatically during the installation process for both IPv6 and IPv4 traffic.

> **IMPORTANT**
> If your network access servers are configured to send RADIUS traffic over ports other than these defaults, remove the exceptions created in Windows Firewall with Advanced Security during NPS installation, and create exceptions for the ports that you do use for RADIUS traffic.

Use the Same RADIUS Ports for the Internal Perimeter Network Firewall Configuration

If you use the default RADIUS port configuration on the VPN Server and the NPS Server, make sure that you open the following ports on the Internal Perimeter Network Firewall:

- Ports UDP1812, UDP1813, UDP1645, and UDP1646

If you are not using the default RADIUS ports in your NPS deployment, you must configure the firewall to allow RADIUS traffic on the ports that you are using. For more information, see Configure Firewalls for RADIUS Traffic.

Next steps

Step 6. Configure Windows 10 Client Always On VPN Connections: In this step, you configure the Windows 10 client computers to communicate with that infrastructure with a VPN connection. You can use several technologies to configure Windows 10 VPN clients, including Windows PowerShell, Microsoft Endpoint Configuration Manager, and Intune. All three require an XML VPN profile to configure the appropriate VPN settings.

Step 6. Configure Windows 10 client Always On VPN connections

12/9/2022 • 26 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

- **Previous:** Step 5. Configure DNS and Firewall Settings
- **Next:** Step 7. (Optional) Conditional access for VPN connectivity using Azure AD

In this step, you'll learn about the ProfileXML options and schema, and configure the Windows 10 client computers to communicate with that infrastructure with a VPN connection.

You can configure the Always On VPN client through PowerShell, Microsoft Endpoint Configuration Manager, or Intune. All three require an XML VPN profile to configure the appropriate VPN settings. Automating PowerShell enrollment for organizations without Configuration Manager or Intune is possible.

> **NOTE**
>
> Group Policy does not include administrative templates to configure the Windows 10 Remote Access Always On VPN client. However, you can use logon scripts.

> **NOTE**
>
> Auto-triggered VPN connections will not work if folder redirection for %appdata% (C:\Users\username\AppData\Roaming) is enabled. Either folder redirection must be disabled for %appdata%, or the auto-triggered VPN profile must be deployed in system context, to change the path in which the rasphone.pbk file is stored.

ProfileXML overview

ProfileXML is a URI node within the VPNv2 CSP. Rather than configuring each VPNv2 CSP node individually—such as triggers, route lists, and authentication protocols—use this node to configure a Windows 10 VPN client by delivering all the settings as a single XML block to a single CSP node. The ProfileXML schema matches the schema of the VPNv2 CSP nodes almost identically, but some terms are slightly different.

You use ProfileXML in all the delivery methods this deployment describes, including Windows PowerShell, Microsoft Endpoint Configuration Manager, and Intune. There are two ways to configure the ProfileXML VPNv2 CSP node in this deployment:

- **OMA-DM**. One way is to use an MDM provider using OMA-DM, as discussed earlier in the section VPNv2 CSP nodes. Using this method, you can easily insert the VPN profile configuration XML markup into the ProfileXML CSP node when using Intune.
- **Windows Management Instrumentation (WMI)-to-CSP bridge**. The second method of configuring the ProfileXML CSP node is to use the WMI-to-CSP bridge—a WMI class called **MDM_VPNv2_01**—that can access the VPNv2 CSP and the ProfileXML node. When you create a new instance of that WMI class, WMI uses the CSP to create the VPN profile when using Windows PowerShell and Configuration Manager.

Even though these configuration methods differ, both require a properly formatted XML VPN profile. To use the ProfileXML VPNv2 CSP setting, you construct XML by using the ProfileXML schema to configure the tags necessary for the simple deployment scenario. For more information, see ProfileXML XSD.

Below you find each of the required settings and its corresponding ProfileXML tag. You configure each setting in a specific tag within the ProfileXML schema, and not all of them are found under the native profile. For additional tag placement, see the ProfileXML schema.

> **IMPORTANT**
>
> Any other combination of upper or lower case for 'true' in the following tags results in a partial configuration of the VPN profile:
>
> <AlwaysOn>**true**</AlwaysOn>
> <RememberCredentials>**true**</RememberCredentials>

Connection type: Native IKEv2

ProfileXML element:

```
<NativeProtocolType>IKEv2</NativeProtocolType>
```

Routing: Split tunneling

ProfileXML element:

```
<RoutingPolicyType>SplitTunnel</RoutingPolicyType>
```

Name resolution: Domain Name Information List and DNS suffix

ProfileXML elements:

```
<DomainNameInformation>
<DomainName>.corp.contoso.com</DomainName>
<DnsServers>10.10.1.10,10.10.1.50</DnsServers>
</DomainNameInformation>

<DnsSuffix>corp.contoso.com</DnsSuffix>
```

Triggering: Always On and Trusted Network Detection

ProfileXML elements:

```
<AlwaysOn>true</AlwaysOn>
<TrustedNetworkDetection>corp.contoso.com</TrustedNetworkDetection>
```

Authentication: PEAP-TLS with TPM-protected user certificates

ProfileXML elements:

```
<Authentication>
<UserMethod>Eap</UserMethod>
<Eap>
<Configuration>...</Configuration>
</Eap>
</Authentication>
```

You can use simple tags to configure some VPN authentication mechanisms. However, EAP and PEAP are more involved. The easiest way to create the XML markup is to configure a VPN client with its EAP settings, and then export that configuration to XML.

For more information about EAP settings, see EAP configuration.

Manually create a template connection profile

In this step, you use Protected Extensible Authentication Protocol (PEAP) to secure communication between the client and the server. Unlike a simple user name and password, this connection requires a unique EAPConfiguration section in the VPN profile to work.

Instead of describing how to create the XML markup from scratch, you use Settings in Windows to create a template VPN profile. After creating the template VPN profile, you use Windows PowerShell to consume the EAPConfiguration portion from that template to create the final ProfileXML that you deploy later in the deployment.

Record NPS certificate settings

Before creating the template, take note the hostname or fully qualified domain name (FQDN) of the NPS server from the server's certificate and the name of the CA that issued the certificate.

Procedure:

1. On your NPS server, open Network Policy Server.
2. In the NPS console, under Policies, click **Network Policies**.
3. Right-click **Virtual Private Network (VPN) Connections**, and click **Properties**.
4. Click the **Constraints** tab, and click **Authentication Methods**.
5. In EAP Types, click **Microsoft: Protected EAP (PEAP)**, and click **Edit**.
6. Record the values for **Certificate issued to** and **Issuer**.

   You use these values in the upcoming VPN template configuration. For example, if the server's FQDN is nps01.corp.contoso.com and the hostname is NPS01, the certificate name is based upon the FQDN or DNS name of the server—for example, nps01.corp.contoso.com.
7. Cancel the Edit Protected EAP Properties dialog box.
8. Cancel the Virtual Private Network (VPN) Connections Properties dialog box.
9. Close Network Policy Server.

> **NOTE**
> If you have multiple NPS servers, complete these steps on each one so that the VPN profile can verify each of them should they be used.

Configure the template VPN profile on a domain-joined client computer

Now that you have the necessary information configure the template VPN profile on a domain-joined client computer. The type of user account you use (that is, standard user or administrator) for this part of the process does not matter.

However, if you haven't restarted the computer since configuring certificate autoenrollment, do so before configuring the template VPN connection to ensure you have a usable certificate enrolled on it.

> **NOTE**
> There is no way to manually add any advanced properties of VPN, such as NRPT rules, Always On, Trusted network detection, etc. In the next step, you create a test VPN connection to verify the configuration of the VPN server and that you can establish a VPN connection to the server.

Manually create a single test VPN connection

1. Sign in to a domain-joined client computer as a member of the **VPN Users** group.
2. On the Start menu, type **VPN**, and press Enter.
3. In the details pane, click **Add a VPN connection**.
4. In the VPN Provider list, click **Windows (built-in)**.
5. In Connection Name, type **Template**.
6. In Server name or address, type the **external** FQDN of your VPN server (for example, **vpn.contoso.com**).
7. Click **Save**.
8. Under Related Settings, click **Change adapter options**.
9. Right-click **Template**, and click **Properties**.
10. On the **Security** tab, in **Type of VPN**, click **IKEv2**.
11. In Data encryption, click **Maximum strength encryption**.
12. Click **Use Extensible Authentication Protocol (EAP)**; then, in **Use Extensible Authentication Protocol (EAP)**, click **Microsoft: Protected EAP (PEAP) (encryption enabled)**.
13. Click **Properties** to open the Protected EAP Properties dialog box, and complete the following steps:

    a. In the **Connect to these servers** box, type the name of the NPS server that you retrieved from the NPS server authentication settings earlier in this section (for example, NPS01).

    > **NOTE**
    > The server name you type must match the name in the certificate. You recovered this name earlier in this section. If the name does not match, the connection will fail, stating that "The connection was prevented because of a policy configured on your RAS/VPN server."

    b. Under Trusted Root Certification Authorities, select the root CA that issued the NPS server's certificate (for example, contoso-CA).

    c. In Notifications before connecting, click **Don't ask user to authorize new servers or trusted CAs**.

    d. In Select Authentication Method, click **Smart Card or other certificate**, and click **Configure**. The Smart Card or other Certificate Properties dialog opens.

e. Click **Use a certificate on this computer**.

f. In the Connect to these servers box, enter the name of the NPS server you retrieved from the NPS server authentication settings in the previous steps.

g. Under Trusted Root Certification Authorities, select the root CA that issued the NPS server's certificate.

h. Select the **Don't prompt user to authorize new servers or trusted certification authorities** check box.

i. Click **OK** to close the Smart Card or other Certificate Properties dialog box.

j. Click **OK** to close the Protected EAP Properties dialog box.

14. Click **OK** to close the Template Properties dialog box.
15. Close the Network Connections window.
16. In Settings, test the VPN by clicking **Template**, and clicking **Connect**.

> **IMPORTANT**
> Make sure that the template VPN connection to your VPN server is successful. Doing so ensures that the EAP settings are correct before you use them in the next example. You must connect at least once before continuing; otherwise, the profile will not contain all the information necessary to connect to the VPN.

Create the ProfileXML configuration files

Before completing this section, make sure you have created and tested the template VPN connection that the section Manually create a template connection profile describes. Testing the VPN connection is necessary to ensure that the profile contains all the information required to connect to the VPN.

The Windows PowerShell script in Listing 1 creates two files on the desktop, both of which contain **EAPConfiguration** tags based on the template connection profile you created previously:

- **VPN_Profile.xml.** This file contains the XML markup required to configure the ProfileXML node in the VPNv2 CSP. Use this file with OMA-DM–compatible MDM services, such as Intune.
- **VPN_Profile.ps1.** This file is a Windows PowerShell script that you can run on client computers to configure the ProfileXML node in the VPNv2 CSP. You can also configure the CSP by deploying this script through Configuration Manager. You cannot run this script in a Remote Desktop session, including a Hyper-V enhanced session.

> **IMPORTANT**
> The example commands below require Windows 10 Build 1607 or later.

Create VPN_Profile.xml and VPN_Profile.ps1

1. Sign in to the domain-joined client computer containing the template VPN profile with the same user account that the section Manually create a template connection profile described.
2. Paste Listing 1 into Windows PowerShell integrated scripting environment (ISE), and customize the parameters described in the comments. These are $Template, $ProfileName, $Servers, $DnsSuffix, $DomainName, $TrustedNetwork, and $DNSServers. A full description of each setting is in the comments.
3. Run the script to generate **VPN_Profile.xml** and **VPN_Profile.ps1** on the desktop.

Listing 1. Understanding MakeProfile.ps1

This section explains the example code that you can use to gain an understanding of how to create a VPN Profile, specifically for configuring ProfileXML in the VPNv2 CSP.

After you assemble a script from this example code and run the script, the script generates two files: VPN_Profile.xml and VPN_Profile.ps1. Use VPN_Profile.xml to configure ProfileXML in OMA-DM compliant MDM services, such as Microsoft Intune.

Use the **VPN_Profile.ps1** script in Windows PowerShell or Microsoft Endpoint Configuration Manager to configure ProfileXML on the Windows 10 desktop.

> **NOTE**
>
> To view the full example script, see the section MakeProfile.ps1 Full Script.

Parameters

Configure the following parameters:

$Template. The name of the template from which to retrieve the EAP configuration.

$ProfileName. Unique alphanumeric identifier for the profile. The profile name must not include a forward slash (/). If the profile name has a space or other non-alphanumeric character, it must be properly escaped according to the URL encoding standard.

$Servers. Public or routable IP address or DNS name for the VPN gateway. It can point to the external IP of a gateway or a virtual IP for a server farm. Examples, 208.147.66.130 or vpn.contoso.com.

$DnsSuffix. Specifies one or more commas separated DNS suffixes. The first in the list is also used as the primary connection-specific DNS suffix for the VPN Interface. The entire list will also be added into the SuffixSearchList.

$DomainName. Used to indicate the namespace to which the policy applies. When a Name query is issued, the DNS client compares the name in the query to all of the namespaces under DomainNameInformationList to find a match. This parameter can be one of the following types:

- FQDN - Fully qualified domain name
- Suffix - A domain suffix that will be appended to the shortname query for DNS resolution. To specify a suffix, prepend a period (.) to the DNS suffix.

$DNSServers. List of comma-separated DNS Server IP addresses to use for the namespace.

$TrustedNetwork. Comma-separated string to identify the trusted network. VPN does not connect automatically when the user is on their corporate wireless network where protected resources are directly accessible to the device.

The following are example values for parameters used in the commands below. Ensure that you change these values for your environment.

```
$TemplateName = 'Template'
$ProfileName = 'Contoso%20AlwaysOn%20VPN'
$Servers = 'vpn.contoso.com'
$DnsSuffix = 'corp.contoso.com'
$DomainName = '.corp.contoso.com'
$DNSServers = '10.10.0.2,10.10.0.3'
$TrustedNetwork = 'corp.contoso.com'
```

Prepare and create the profile XML

The following example commands get EAP settings from the template profile:

```
$Connection = Get-VpnConnection -Name $TemplateName
if(!$Connection)
{
$Message = "Unable to get $TemplateName connection profile: $_"
Write-Host "$Message"
exit
}
$EAPSettings= $Connection.EapConfigXmlStream.InnerXml
```

Create the profile XML

> **IMPORTANT**
>
> Any other combination of upper or lower case for 'true' in the following tags results in a partial configuration of the VPN profile:
>
> <AlwaysOn>**true**</AlwaysOn>
> <RememberCredentials>**true**</RememberCredentials>

```
$ProfileXML = @("
<VPNProfile>
  <DnsSuffix>$DnsSuffix</DnsSuffix>
  <NativeProfile>
<Servers>$Servers</Servers>
<NativeProtocolType>IKEv2</NativeProtocolType>
<Authentication>
  <UserMethod>Eap</UserMethod>
  <Eap>
    <Configuration>
     $EAPSettings
    </Configuration>
  </Eap>
</Authentication>
<RoutingPolicyType>SplitTunnel</RoutingPolicyType>
  </NativeProfile>
  <AlwaysOn>true</AlwaysOn>
  <RememberCredentials>true</RememberCredentials>
  <TrustedNetworkDetection>$TrustedNetwork</TrustedNetworkDetection>
  <DomainNameInformation>
<DomainName>$DomainName</DomainName>
<DnsServers>$DNSServers</DnsServers>
</DomainNameInformation>
</VPNProfile>
")
```

Output VPN_Profile.xml for Intune

You can use the following example command to save the profile XML file:

```
$ProfileXML | Out-File -FilePath ($env:USERPROFILE + '\desktop\VPN_Profile.xml')
```

Output VPN_Profile.ps1 for the desktop and Configuration Manager

The following example code configures an AlwaysOn IKEv2 VPN Connection by using the ProfileXML node in the VPNv2 CSP.

You can use this script on the Windows 10 desktop or in Configuration Manager.

Define key VPN profile parameters

```
$Script = '$ProfileName = ''' + $ProfileName + ''''
$ProfileNameEscaped = $ProfileName -replace ' ', '%20'
```

Escape special characters in the profile

```
$ProfileXML = $ProfileXML -replace '<', '&lt;'
$ProfileXML = $ProfileXML -replace '>', '&gt;'
$ProfileXML = $ProfileXML -replace '"', '&quot;'
```

Define WMI-to-CSP Bridge properties

```
$nodeCSPURI = "./Vendor/MSFT/VPNv2"
$namespaceName = "root\cimv2\mdm\dmmap"
$className = "MDM_VPNv2_01"
```

Determine user SID for VPN profile:

```
try
{
$username = Gwmi -Class Win32_ComputerSystem | select username
$objuser = New-Object System.Security.Principal.NTAccount($username.username)
$sid = $objuser.Translate([System.Security.Principal.SecurityIdentifier])
$SidValue = $sid.Value
$Message = "User SID is $SidValue."
Write-Host "$Message"
}
catch [Exception]
{
$Message = "Unable to get user SID. User may be logged on over Remote Desktop: $_"
Write-Host "$Message"
exit
}
```

Define WMI session:

```
$session = New-CimSession
$options = New-Object Microsoft.Management.Infrastructure.Options.CimOperationOptions
$options.SetCustomOption("PolicyPlatformContext_PrincipalContext_Type", "PolicyPlatform_UserContext",
$false)
$options.SetCustomOption("PolicyPlatformContext_PrincipalContext_Id", "$SidValue", $false)
```

Detect and delete previous VPN profile:

```
try
{
  $deleteInstances = $session.EnumerateInstances($namespaceName, $className, $options)
  foreach ($deleteInstance in $deleteInstances)
  {
    $InstanceId = $deleteInstance.InstanceID
    if ("$InstanceId" -eq "$ProfileNameEscaped")
    {
        $session.DeleteInstance($namespaceName, $deleteInstance, $options)
        $Message = "Removed $ProfileName profile $InstanceId"
        Write-Host "$Message"
    } else {
        $Message = "Ignoring existing VPN profile $InstanceId"
        Write-Host "$Message"
    }
  }
}
catch [Exception]
{
  $Message = "Unable to remove existing outdated instance(s) of $ProfileName profile: $_"
  Write-Host "$Message"
  exit
}
```

Create the VPN profile:

```
try
{
  $newInstance = New-Object Microsoft.Management.Infrastructure.CimInstance $className, $namespaceName
  $property = [Microsoft.Management.Infrastructure.CimProperty]::Create("ParentID", "$nodeCSPURI", "String",
"Key")
  $newInstance.CimInstanceProperties.Add($property)
  $property = [Microsoft.Management.Infrastructure.CimProperty]::Create("InstanceID", "$ProfileNameEscaped",
"String", "Key")
  $newInstance.CimInstanceProperties.Add($property)
  $property = [Microsoft.Management.Infrastructure.CimProperty]::Create("ProfileXML", "$ProfileXML",
"String", "Property")
  $newInstance.CimInstanceProperties.Add($property)
  $session.CreateInstance($namespaceName, $newInstance, $options)
  $Message = "Created $ProfileName profile."


  Write-Host "$Message"
}
catch [Exception]
{
$Message = "Unable to create $ProfileName profile: $_"
Write-Host "$Message"
exit
}

$Message = "Script Complete"
Write-Host "$Message"
```

Save the profile XML file

```
$Script | Out-File -FilePath ($env:USERPROFILE + '\desktop\VPN_Profile.ps1')

$Message = "Successfully created VPN_Profile.xml and VPN_Profile.ps1 on the desktop."
Write-Host "$Message"
```

MakeProfile.ps1 Full Script

Most examples use the Set-WmiInstance Windows PowerShell cmdlet to insert ProfileXML into a new instance of the MDM_VPNv2_01 WMI class.

However, this does not work in Configuration Manager because you cannot run the package in the end users' context. Therefore, this script uses the Common Information Model to create a WMI session in the user's context, and then it creates a new instance of the MDM_VPNv2_01 WMI class in that session. This WMI class uses the WMI-to-CSP bridge to configure the VPNv2 CSP. Therefore, by adding the class instance, you configure the CSP.

> **IMPORTANT**
> WMI-to-CSP bridge requires local admin rights, by design. To deploy per user VPN profiles you should be using Configuration Manager or MDM.

> **NOTE**
> The script VPN_Profile.ps1 uses the current user's SID to identify the user's context. Because no SID is available in a Remote Desktop session, the script does not work in a Remote Desktop session. Likewise, it does not work in a Hyper-V enhanced session. If you're testing a Remote Access Always On VPN in virtual machines, disable enhanced session on your client VMs before running this script.

The following example script includes all of the code examples from previous sections. Ensure that you change example values to values that are appropriate for your environment.

```
$TemplateName = 'Template'
$ProfileName = 'Contoso AlwaysOn VPN'
$Servers = 'vpn.contoso.com'
$DnsSuffix = 'corp.contoso.com'
$DomainName = '.corp.contoso.com'
$DNSServers = '10.10.0.2,10.10.0.3'
$TrustedNetwork = 'corp.contoso.com'


$Connection = Get-VpnConnection -Name $TemplateName
if(!$Connection)
{
$Message = "Unable to get $TemplateName connection profile: $_"
Write-Host "$Message"
exit
}
$EAPSettings= $Connection.EapConfigXmlStream.InnerXml

$ProfileXML = @("
<VPNProfile>
  <DnsSuffix>$DnsSuffix</DnsSuffix>
  <NativeProfile>
<Servers>$Servers</Servers>
<NativeProtocolType>IKEv2</NativeProtocolType>
<Authentication>
  <UserMethod>Eap</UserMethod>
  <Eap>
   <Configuration>
    $EAPSettings
   </Configuration>
  </Eap>
</Authentication>
<RoutingPolicyType>SplitTunnel</RoutingPolicyType>
  </NativeProfile>
<AlwaysOn>true</AlwaysOn>
<RememberCredentials>true</RememberCredentials>
<TrustedNetworkDetection>$TrustedNetwork</TrustedNetworkDetection>
  <DomainNameInformation>
```

```
<DomainName>$DomainName</DomainName>
<DnsServers>$DNSServers</DnsServers>
</DomainNameInformation>
</VPNProfile>
")

$ProfileXML | Out-File -FilePath ($env:USERPROFILE + '\desktop\VPN_Profile.xml')

 $Script = @("
  `$ProfileName = '$ProfileName'
  `$ProfileNameEscaped = `$ProfileName -replace ' ', '%20'

  `$ProfileXML = '$ProfileXML'

  `$ProfileXML = `$ProfileXML -replace '<', '&lt;'
  `$ProfileXML = `$ProfileXML -replace '>', '&gt;'
  `$ProfileXML = `$ProfileXML -replace '`"', '&quot;'

  `$nodeCSPURI = `"./Vendor/MSFT/VPNv2`"
  `$namespaceName = `"root\cimv2\mdm\dmmap`"
  `$className = `"MDM_VPNv2_01`"

  try
  {
  `$username = Gwmi -Class Win32_ComputerSystem | select username
  `$objuser = New-Object System.Security.Principal.NTAccount(`$username.username)
  `$sid = `$objuser.Translate([System.Security.Principal.SecurityIdentifier])
  `$SidValue = `$sid.Value
  `$Message = `"User SID is `$SidValue.`"
  Write-Host `"`$Message`"
  }
  catch [Exception]
  {
  `$Message = `"Unable to get user SID. User may be logged on over Remote Desktop: `$_`"
  Write-Host `"`$Message`"
  exit
  }

  `$session = New-CimSession
  `$options = New-Object Microsoft.Management.Infrastructure.Options.CimOperationOptions
  `$options.SetCustomOption(`"PolicyPlatformContext_PrincipalContext_Type`",
`"PolicyPlatform_UserContext`", `$false)
  `$options.SetCustomOption(`"PolicyPlatformContext_PrincipalContext_Id`", `"`$SidValue`", `$false)

  try
  {
 `$deleteInstances = `$session.EnumerateInstances(`$namespaceName, `$className, `$options)
 foreach (`$deleteInstance in `$deleteInstances)
 {
     `$InstanceId = `$deleteInstance.InstanceID
     if (`"`$InstanceId`" -eq `"`$ProfileNameEscaped`")
     {
         `$session.DeleteInstance(`$namespaceName, `$deleteInstance, `$options)
         `$Message = `"Removed `$ProfileName profile `$InstanceId`"
         Write-Host `"`$Message`"
     } else {
         `$Message = `"Ignoring existing VPN profile `$InstanceId`"
         Write-Host `"`$Message`"
     }
 }
  }
  catch [Exception]
  {
 `$Message = `"Unable to remove existing outdated instance(s) of `$ProfileName profile: `$_`"
 Write-Host `"`$Message`"
 exit
  }

  try
```

```
    {
   `$newInstance = New-Object Microsoft.Management.Infrastructure.CimInstance `$className, `$namespaceName
   `$property = [Microsoft.Management.Infrastructure.CimProperty]::Create(`"ParentID`", `"`$nodeCSPURI`",
`"String`", `"Key`")
   `$newInstance.CimInstanceProperties.Add(`$property)
   `$property = [Microsoft.Management.Infrastructure.CimProperty]::Create(`"InstanceID`",
`"`$ProfileNameEscaped`", `"String`",      `"Key`")
   `$newInstance.CimInstanceProperties.Add(`$property)
   `$property = [Microsoft.Management.Infrastructure.CimProperty]::Create(`"ProfileXML`", `"`$ProfileXML`",
`"String`", `"Property`")
   `$newInstance.CimInstanceProperties.Add(`$property)
   `$session.CreateInstance(`$namespaceName, `$newInstance, `$options)
   `$Message = `"Created `$ProfileName profile.`"

   Write-Host `"`$Message`"
    }
    catch [Exception]
    {
   `$Message = `"Unable to create `$ProfileName profile: `$_`"
   Write-Host `"`$Message`"
   exit
    }

    `$Message = `"Script Complete`"
    Write-Host `"`$Message`"
    ")

    $Script | Out-File -FilePath ($env:USERPROFILE + '\desktop\VPN_Profile.ps1')

  $Message = "Successfully created VPN_Profile.xml and VPN_Profile.ps1 on the desktop."
  Write-Host "$Message"
```

Configure the VPN client by using Windows PowerShell

To configure the VPNv2 CSP on a Windows 10 client computer, run the VPN_Profile.ps1 Windows PowerShell script that you created in the Create the profile XML section. Open Windows PowerShell as an Administrator; otherwise, you'll receive an error saying, *Access denied*.

After running VPN_Profile.ps1 to configure the VPN profile, you can verify at any time that it was successful by running the following command in the Windows PowerShell ISE:

```
Get-WmiObject -Namespace root\cimv2\mdm\dmmap -Class MDM_VPNv2_01
```

Successful results from the Get-WmiObject cmdlet

```
__GENUS : 2
__CLASS : MDM_VPNv2_01
__SUPERCLASS:
__DYNASTY   : MDM_VPNv2_01
__RELPATH   : MDM_VPNv2_01.InstanceID="Contoso%20AlwaysOn%20VPN",ParentID
  ="./Vendor/MSFT/VPNv2"
__PROPERTY_COUNT: 10
__DERIVATION: {}
__SERVER: WIN01
__NAMESPACE : root\cimv2\mdm\dmmap
__PATH  : \\WIN01\root\cimv2\mdm\dmmap:MDM_VPNv2_01.InstanceID="Conto
  so%20AlwaysOn%20VPN",ParentID="./Vendor/MSFT/VPNv2"
AlwaysOn: True
ByPassForLocal  :
DnsSuffix   : corp.contoso.com
EdpModeId   :
InstanceID  : Contoso%20AlwaysOn%20VPN
LockDown:
```

```
ParentID: ./Vendor/MSFT/VPNv2
ProfileXML  : <VPNProfile><RememberCredentials>true</RememberCredentials>
  <AlwaysOn>true</AlwaysOn><DnsSuffix>corp.contoso.com</DnsSu
  ffix><TrustedNetworkDetection>corp.contoso.com</TrustedNetw
  orkDetection><NativeProfile><Servers>vpn.contoso.com;vpn.co
  ntoso.com</Servers><RoutingPolicyType>SplitTunnel</RoutingP
  olicyType><NativeProtocolType>Ikev2</NativeProtocolType><Au
  thentication><UserMethod>Eap</UserMethod><MachineMethod>Eap
  </MachineMethod><Eap><Configuration><EapHostConfig xmlns="h
  ttp://www.microsoft.com/provisioning/EapHostConfig"><EapMet
  hod><Type xmlns="https://www.microsoft.com/provisioning/EapC
  ommon">25</Type><VendorId xmlns="https://www.microsoft.com/p
  rovisioning/EapCommon">0</VendorId><VendorType xmlns="http:
  //www.microsoft.com/provisioning/EapCommon">0</VendorType><
  AuthorId xmlns="https://www.microsoft.com/provisioning/EapCo
  mmon">0</AuthorId></EapMethod><Config xmlns="https://www.mic
  rosoft.com/provisioning/EapHostConfig"><Eap xmlns="https://w
  ww.microsoft.com/provisioning/BaseEapConnectionPropertiesV1
  "><Type>25</Type><EapType xmlns="https://www.microsoft.com/p
  rovisioning/MsPeapConnectionPropertiesV1"><ServerValidation
  ><DisableUserPromptForServerValidation>true</DisableUserPro
  mptForServerValidation><ServerNames>NPS</ServerNames><Trust
  edRootCA>3f 07 88 e8 ac 00 32 e4 06 3f 30 f8 db 74 25 e1
  2e 5b 84 d1 </TrustedRootCA></ServerValidation><FastReconne
  ct>true</FastReconnect><InnerEapOptional>false</InnerEapOpt
  ional><Eap xmlns="https://www.microsoft.com/provisioning/Bas
  eEapConnectionPropertiesV1"><Type>13</Type><EapType xmlns="
  https://www.microsoft.com/provisioning/EapTlsConnectionPrope
  rtiesV1"><CredentialsSource><CertificateStore><SimpleCertSe
  lection>true</SimpleCertSelection></CertificateStore></Cred
  entialsSource><ServerValidation><DisableUserPromptForServer
  Validation>true</DisableUserPromptForServerValidation><Serv
  erNames>NPS</ServerNames><TrustedRootCA>3f 07 88 e8 ac 00
  32 e4 06 3f 30 f8 db 74 25 e1 2e 5b 84 d1 </TrustedRootCA><
  /ServerValidation><DifferentUsername>false</DifferentUserna
  me><PerformServerValidation xmlns="https://www.microsoft.com
  /provisioning/EapTlsConnectionPropertiesV2">true</PerformSe
  rverValidation><AcceptServerName xmlns="https://www.microsof
  t.com/provisioning/EapTlsConnectionPropertiesV2">true</Acce
  ptServerName></EapType></Eap><EnableQuarantineChecks>false<
  /EnableQuarantineChecks><RequireCryptoBinding>false</Requir
  eCryptoBinding><PeapExtensions><PerformServerValidation xml
  ns="https://www.microsoft.com/provisioning/MsPeapConnectionP
  ropertiesV2">true</PerformServerValidation><AcceptServerNam
  e xmlns="https://www.microsoft.com/provisioning/MsPeapConnec
  tionPropertiesV2">true</AcceptServerName></PeapExtensions><
  /EapType></Eap></Config></EapHostConfig></Configuration></E
  ap></Authentication></NativeProfile><DomainNameInformation>
  <DomainName>corp.contoso.com</DomainName><DnsServers>10.10.
      0.2,10.10.0.3</DnsServers><AutoTrigger>true</AutoTrigger></
  DomainNameInformation></VPNProfile>
RememberCredentials : True
TrustedNetworkDetection : corp.contoso.com
PSComputerName  : WIN01
```

The ProfileXML configuration must be correct in structure, spelling, configuration, and sometimes letter case. If you see something different in structure to Listing 1, the ProfileXML markup likely contains an error.

If you need to troubleshoot the markup, it is easier to put it in an XML editor than to troubleshoot it in the Windows PowerShell ISE. In either case, start with the simplest version of the profile, and add components back one at a time until the issue occurs again.

Configure the VPN client by using Configuration Manager

In Configuration Manager, you can deploy VPN profiles by using the ProfileXML CSP node, just like you did in

Windows PowerShell. Here, you use the VPN_Profile.ps1 Windows PowerShell script that you created in the section Create the ProfileXML configuration files.

To use Configuration Manager to deploy a Remote Access Always On VPN profile to Windows 10 client computers, you must start by creating a group of machines or users to whom you deploy the profile. In this scenario, create a user group to deploy the configuration script.

Create a user group

1. In the Configuration Manager console, open Assets and Compliance\User Collections.
2. On the **Home** ribbon, in the **Create** group, click **Create User Collection**.
3. On the General page, complete the following steps:

   a. In **Name**, type **VPN Users**.

   b. Click **Browse**, click **All Users** and click **OK**.

   c. Click **Next**.
4. On the Membership Rules page, complete the following steps:

   a. In **Membership rules**, click **Add Rule**, and click **Direct Rule**. In this example, you're adding individual users to the user collection. However, you might use a query rule to add users to this collection dynamically for a larger-scale deployment.

   b. On the **Welcome** page, click **Next**.

   c. On the Search for Resources page, in **Value**, type the name of the user you want to add. The resource name includes the user's domain. To include results based on a partial match, insert the **%** character at either end of your search criterion. For example, to find all users containing the string "lori," type **%lori%**. Click **Next**.

   d. On the Select Resources page, select the users you want to add to the group, and click **Next**.

   e. On the Summary page, click **Next**.

   f. On the Completion page, click **Close**.
5. Back on the Membership Rules page of the Create User Collection Wizard, click **Next**.
6. On the Summary page, click **Next**.
7. On the Completion page, click **Close**.

After you create the user group to receive the VPN profile, you can create a package and program to deploy the Windows PowerShell configuration script that you created in the section Create the ProfileXML configuration files.

Create a package containing the ProfileXML configuration script

1. Host the script VPN_Profile.ps1 on a network share that the site server computer account can access.
2. In the Configuration Manager console, open **Software Library\Application Management\Packages**.
3. On the **Home** ribbon, in the **Create** group, click **Create Package** to start the Create Package and Program Wizard.
4. On the Package page, complete the following steps:

   a. In **Name**, type **Windows 10 Always On VPN Profile**.

   b. Select the **This package contains source files** check box, and click **Browse**.

c. In the Set Source Folder dialog box, click **Browse**, select the file share containing VPN_Profile.ps1, and click **OK**. Make sure you select a network path, not a local path. In other words, the path should be something like *\fileserver\vpnscript*, not *c:\vpnscript*.

5. Click **Next**.
6. On the Program Type page, click **Next**.
7. On the Standard Program page, complete the following steps:

   a. In **Name**, type **VPN Profile Script**.

   b. In **Command line**, type **PowerShell.exe -ExecutionPolicy Bypass -File "VPN_Profile.ps1"**.

   c. In **Run mode**, click **Run with administrative rights**.

   d. Click **Next**.
8. On the Requirements page, complete the following steps:

   a. Select **This program can run only on specified platforms**.

   b. Select the **All Windows 10 (32-bit)** and **All Windows 10 (64-bit)** check boxes.

   c. In **Estimated disk space**, type **1**.

   d. In **Maximum allowed run time (minutes)**, type **15**.

   e. Click **Next**.
9. On the Summary page, click **Next**.
10. On the Completion page, click **Close**.

With the package and program created, you need to deploy it to the **VPN Users** group.

Deploy the ProfileXML configuration script

1. In the Configuration Manager console, open Software Library\Application Management\Packages.
2. In **Packages**, click **Windows 10 Always On VPN Profile**.
3. On the **Programs** tab, at the bottom of the details pane, right-click **VPN Profile Script**, click **Properties**, and complete the following steps:

   a. On the **Advanced** tab, in **When this program is assigned to a computer**, click **Once for every user who logs on**.

   b. Click **OK**.
4. Right-click **VPN Profile Script** and click **Deploy** to start the Deploy Software Wizard.
5. On the General page, complete the following steps:

   a. Beside **Collection**, click **Browse**.

   b. In the **Collection Types** list (top left), click **User Collections**.

   c. Click **VPN Users**, and click **OK**.

   d. Click **Next**.
6. On the Content page, complete the following steps:

   a. Click **Add**, and click **Distribution Point**.

b. In **Available distribution points**, select the distribution points to which you want to distribute the ProfileXML configuration script, and click **OK**.

c. Click **Next**.

7. On the Deployment settings page, click **Next**.
8. On the Scheduling page, complete the following steps:

   a. Click **New** to open the Assignment Schedule dialog box.

   b. Click **Assign immediately after this event**, and click **OK**.

   c. Click **Next**.

9. On the User Experience page, complete the following steps:

   a. Select the **Software Installation** check box.

   b. Click **Summary**.

10. On the Summary page, click **Next**.
11. On the Completion page, click **Close**.

With the ProfileXML configuration script deployed, sign in to a Windows 10 client computer with the user account you selected when you built the user collection. Verify the configuration of the VPN client.

> **NOTE**
> The script VPN_Profile.ps1 does not work in a Remote Desktop session. Likewise, it does not work in a Hyper-V enhanced session. If you're testing a Remote Access Always On VPN in virtual machines, disable enhanced session on your client VMs before continuing.

Verify the configuration of the VPN client

1. In Control Panel, under **System\Security**, click **Configuration Manager**.
2. In the Configuration Manager Properties dialog, on the **Actions** tab, complete the following steps:

   a. Click **Machine Policy Retrieval & Evaluation Cycle**, click **Run Now**, and click **OK**.

   b. Click **User Policy Retrieval & Evaluation Cycle**, click **Run Now**, and click **OK**.

   c. Click **OK**.

3. Close the Control Panel.

You should see the new VPN profile shortly.

Configure the VPN client by using Intune

To use Intune to deploy Windows 10 Remote Access Always On VPN profiles, you can configure the ProfileXML CSP node by using the VPN profile you created in the section Create the ProfileXML configuration files, or you can use the base EAP XML sample provided below.

> **NOTE**
> Intune now uses Azure AD groups. If Azure AD Connect synced the VPN Users group from on-premises to Azure AD, and users are assigned to the VPN Users group, you are ready to proceed.

Create the VPN device configuration policy to configure the Windows 10 client computers for all users added to the group. Since the Intune template provides VPN parameters, only copy the <EapHostConfig> </EapHostConfig> portion of the VPN_ProfileXML file.

Create the Always On VPN configuration policy

1. Sign into the Azure portal.
2. Go to **Intune** > **Device Configuration** > **Profiles**.
3. Click **Create Profile** to start the Create profile Wizard.
4. Enter a **Name** for the VPN profile and (optionally) a description.
5. Under **Platform**, select **Windows 10 or later**, and choose **VPN** from the Profile type drop-down.

> **TIP**
> If you are creating a custom VPN profileXML, see Apply ProfileXML using Intune for the instructions.

6. Under the **Base VPN** tab, verify or set the following settings:
   - **Connection name:** Enter the name of the VPN connection as it appears on the client computer in the **VPN** tab under **Settings**, for example, *Contoso AutoVPN*.
   - **Servers:** Add one or more VPN servers by clicking **Add.**
   - **Description** and **IP Address or FQDN:** Enter the description and IP Address or FQDN of the VPN server. These values must align with the Subject Name in the VPN server's authentication certificate.
   - **Default server:** If this is the default VPN server, set to **True**. Doing this enables this server as the default server that devices use to establish the connection.
   - **Connection type:** Set to **IKEv2**.
   - **Always On:** Set to **Enable** to connect to the VPN automatically at the sign-in and stay connected until the user manually disconnects.
   - **Remember credentials at each logon**: Boolean value (true or false) for caching credentials. If set to true, credentials are cached whenever possible.
7. Copy the following XML string to a text editor:

> **IMPORTANT**
> Any other combination of upper or lower case for 'true' in the following tags results in a partial configuration of the VPN profile:
>
> <AlwaysOn>**true**</AlwaysOn>
> <RememberCredentials>**true**</RememberCredentials>

```
<EapHostConfig xmlns="https://www.microsoft.com/provisioning/EapHostConfig"><EapMethod><Type
xmlns="https://www.microsoft.com/provisioning/EapCommon">25</Type><VendorId
xmlns="https://www.microsoft.com/provisioning/EapCommon">0</VendorId><VendorType
xmlns="https://www.microsoft.com/provisioning/EapCommon">0</VendorType><AuthorId
xmlns="https://www.microsoft.com/provisioning/EapCommon">0</AuthorId></EapMethod><Config
xmlns="https://www.microsoft.com/provisioning/EapHostConfig"><Eap
xmlns="https://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1"><Type>25</Type><EapType
xmlns="https://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV1"><ServerValidation>
<DisableUserPromptForServerValidation>true</DisableUserPromptForServerValidation>
<ServerNames>NPS.contoso.com</ServerNames><TrustedRootCA>5a 89 fe cb 5b 49 a7 0b 1a 52 63 b7 35 ee d7
1c c2 68 be 4b </TrustedRootCA></ServerValidation><FastReconnect>true</FastReconnect>
<InnerEapOptional>false</InnerEapOptional><Eap
xmlns="https://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1"><Type>13</Type><EapType
xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV1"><CredentialsSource>
<CertificateStore><SimpleCertSelection>true</SimpleCertSelection></CertificateStore>
</CredentialsSource><ServerValidation>
<DisableUserPromptForServerValidation>true</DisableUserPromptForServerValidation>
<ServerNames>NPS.contoso.com</ServerNames><TrustedRootCA>5a 89 fe cb 5b 49 a7 0b 1a 52 63 b7 35 ee d7
1c c2 68 be 4b </TrustedRootCA></ServerValidation><DifferentUsername>false</DifferentUsername>
<PerformServerValidation
xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2">true</PerformServerValida
tion><AcceptServerName
xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2">true</AcceptServerName>
</EapType></Eap><EnableQuarantineChecks>false</EnableQuarantineChecks>
<RequireCryptoBinding>false</RequireCryptoBinding><PeapExtensions><PerformServerValidation
xmlns="https://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV2">true</PerformServerValida
tion><AcceptServerName
xmlns="https://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV2">true</AcceptServerName>
</PeapExtensions></EapType></Eap></Config></EapHostConfig>
```

8. Replace the **<TrustedRootCA>5a 89 fe cb 5b 49 a7 0b 1a 52 63 b7 35 ee d7 1c c2 68 be 4b</TrustedRootCA>** in the sample with the certificate thumbprint of your on-premises root certificate authority in both places.

> **IMPORTANT**
> Do not use the sample thumbprint in the <TrustedRootCA></TrustedRootCA> section below. The TrustedRootCA must be the certificate thumbprint of the on-premises root certificate authority that issued the server-authentication certificate for RRAS and NPS servers. **This must not be the cloud root certificate, nor the intermediate issuing CA certificate thumbprint**.

9. Replace the **<ServerNames>NPS.contoso.com</ServerNames>** in the sample XML with the FQDN of the domain-joined NPS where authentication takes place.

10. Copy the revised XML string and paste into the **EAP Xml** box under the Base VPN tab and click **OK**. An Always On VPN Device Configuration policy using EAP is created in Intune.

Sync the Always On VPN configuration policy with Intune

To test the configuration policy, sign in to a Windows 10 client computer as the user you added to the **Always On VPN Users** group, and then sync with Intune.

1. On the Start menu, click **Settings**.

2. In Settings, click **Accounts**, and click **Access work or school**.

3. Click the MDM profile, and click **Info**.

4. Click **Sync** to force an Intune policy evaluation and retrieval.

5. Close Settings. After synchronization, you see the VPN profile available on the computer.

Next steps

You are done deploying Always On VPN. For other features you can configure, see the table below:

IF YOU WANT TO...	THEN SEE...
Configure Conditional Access for VPN	Step 7. (Optional) Configure conditional access for VPN connectivity using Azure AD: In this step, you can fine-tune how authorized VPN users access your resources using Azure Active Directory (Azure AD) conditional access. With Azure AD conditional access for virtual private network (VPN) connectivity, you can help protect the VPN connections. Conditional Access is a policy-based evaluation engine that lets you create access rules for any Azure Active Directory (Azure AD) connected application.
Learn more about the advanced VPN features	Advanced VPN Features: This page provides guidance on how to enable VPN Traffic Filters, how to configure Automatic VPN connections using App-Triggers, and how to configure NPS to only allow VPN Connections from clients using certificates issued by Azure AD.

Step 7. (Optional) Conditional access for VPN connectivity using Azure AD

12/9/2022 • 4 minutes to read • Edit Online

- **Previous:** Step 6. Configure Windows 10 Client Always On VPN Connections
- **Next:** Step 7.1. Configure EAP-TLS to ignore Certificate Revocation List (CRL) checking

In this optional step, you can fine-tune how VPN users access your resources using Azure Active Directory (Azure AD) conditional access. With Azure AD conditional access for virtual private network (VPN) connectivity, you can help protect the VPN connections. Conditional Access is a policy-based evaluation engine that lets you create access rules for any Azure Active Directory (Azure AD) connected application.

Prerequisites

You are familiar with the following topics:

- Conditional access in Azure Active Directory
- VPN and conditional access

To configure Azure Active Directory conditional access for VPN connectivity, you need to have the following configured:

- Server Infrastructure
- Remote Access Server for Always On VPN
- Network Policy Server
- DNS and Firewall Settings
- Windows 10 Client Always On VPN Connections

Step 7.1. Configure EAP-TLS to ignore Certificate Revocation List (CRL) checking

In this step, you can add **IgnoreNoRevocationCheck** and set it to allow authentication of clients when the certificate does not include CRL distribution points. By default, IgnoreNoRevocationCheck is set to 0 (disabled).

An EAP-TLS client cannot connect unless the NPS server completes a revocation check of the certificate chain (including the root certificate). Cloud certificates issued to the user by Azure AD do not have a CRL because they are short-lived certificates with a lifetime of one hour. EAP on NPS needs to be configured to ignore the absence of a CRL. Since the authentication method is EAP-TLS, this registry value is only needed under **EAP\13**. If other EAP authentication methods are used, then the registry value should be added under those as well.

Step 7.2. Create root certificates for VPN authentication with Azure AD

In this step, you configure root certificates for VPN authentication with Azure AD, which automatically creates a VPN server cloud app in the tenant.

To configure conditional access for VPN connectivity, you need to:

1. Create a VPN certificate in the Azure portal.
2. Download the VPN certificate.

3. Deploy the certificate to your VPN server.

> **IMPORTANT**
>
> Once a VPN certificate is created in the Azure portal, Azure AD will start using it immediately to issue short lived certificates to the VPN client. It is critical that the VPN certificate be deployed immediately to the VPN server to avoid any issues with credential validation of the VPN client.

> **NOTE**
>
> To create a VPN certificate in the Azure portal, you will need to sign in as Global Administrator. VPN certficate information such as certificatethumprint and certificate expiration information, is stored as a service principal named "VPN Server" in Azure AD. A user with least privileged role can view, but not modify service principal information. Only the following roles Global Administrator, Application Administrator, Cloud Application Administrator, Hybrid Identity Administrator, Directory Synchronization Accounts and Service Principal owners are premitted to update or delete service principal information including "VPN Server".

Step 7.3. Configure the Conditional Access policy

In this step, you configure the conditional access policy for VPN connectivity.

To configure the conditional access policy, you need to:

1. Create a Conditional Access policy that is assigned to VPN users.
2. Set the Cloud app to **VPN Server**.
3. Set the Grant (access control) to **Require multi-factor authentication**. You can use other controls as necessary.

Step 7.4. Deploy conditional access root certificates to on-premises AD

In this step, you deploy a trusted root certificate for VPN authentication to your on-premises AD.

To deploy the trusted root certificate, you need to:

1. Add the downloaded certificate as a *trusted root CA for VPN authentication*.
2. Import the root certificate to the VPN server and VPN client.
3. Verify that the certificates are present and show as trusted.

Step 7.5. Create OMA-DM based VPNv2 Profiles to Windows 10 devices

In this step, you can create OMA-DM based VPNv2 profiles using Intune to deploy a VPN Device Configuration policy. If you want to use Configuration Manager or PowerShell Script to create VPNv2 profiles, see VPNv2 CSP settings for more details.

Next steps

Step 7.1. Configure EAP-TLS to ignore Certificate Revocation List (CRL) checking: In this step, you must add **IgnoreNoRevocationCheck** and set it to allow authentication of clients when the certificate does not include CRL distribution points. By default, IgnoreNoRevocationCheck is set to 0 (disabled).

Related topics

- Configure VPNv2 Profiles: The VPN client is now able to integrate with the cloud-based Conditional Access Platform to provide a device compliance option for remote clients. In this step, you configure the VPNv2 profiles with `<DeviceCompliance> <Enabled>true</Enabled>`.
- Enhancing remote access in Windows 10 with an automatic VPN profile: Learn how Microsoft implements Conditional Access for VPN connectivity. VPN profiles contain all the information a device requires to connect to the corporate network, including the authentication methods that are supported and the VPN server that the device should connect to. Changes in Windows 10 Anniversary Update, including Conditional Access and single sign-on, made it possible for us to create our Always-On VPN connection profile.
- Conditional access in Azure Active Directory: Security is a top concern for organizations using the cloud. A key aspect of cloud security is identity and access when it comes to managing your cloud resources. In a mobile-first, cloud-first world, users can access your organization's resources using a variety of devices and apps from anywhere. As a result of this, just focusing on who can access a resource is not sufficient anymore. In order to master the balance between security and productivity, IT professionals also need to factor how a resource is being accessed into an access control decision.
- VPN and conditional access: The VPN client is now able to integrate with the cloud-based Conditional Access Platform to provide a device compliance option for remote clients. Conditional Access is a policy-based evaluation engine that lets you create access rules for any Azure Active Directory (Azure AD) connected application.

Step 7.1. Configure EAP-TLS to ignore Certificate Revocation List (CRL) checking

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

- **Previous:** Step 7. (Optional) Conditional access for VPN connectivity using Azure AD
- **Next:** Step 7.2. Create root certificates for VPN authentication with Azure AD

> **IMPORTANT**
> Failure to implement this registry change will cause IKEv2 connections using cloud certificates with PEAP to fail, but IKEv2 connections using Client Auth certificates issued from the on-premises CA would continue to work.

In this step, you can add **IgnoreNoRevocationCheck** and set it to allow authentication of clients when the certificate does not include CRL distribution points. By default, IgnoreNoRevocationCheck is set to 0 (disabled).

> **NOTE**
> If a Windows Routing and Remote Access Server (RRAS) uses NPS to proxy RADIUS calls to a second NPS, then you must set **IgnoreNoRevocationCheck=1** on both servers.

An EAP-TLS client cannot connect unless the NPS server completes a revocation check of the certificate chain (including the root certificate). Cloud certificates issued to the user by Azure AD do not have a CRL because they are short-lived certificates with a lifetime of one hour. EAP on NPS needs to be configured to ignore the absence of a CRL. By default, IgnoreNoRevocationCheck is set to 0 (disabled). Add IgnoreNoRevocationCheck and set it to 1 to allow authentication of clients when the certificate does not include CRL distribution points.

Since the authentication method is EAP-TLS, this registry value is only needed under EAP\13. If other EAP authentication methods are used, then the registry value should be added under those as well.

Procedure

1. Open **regedit.exe** on the NPS server.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13**.
3. Select **Edit > New** and select **DWORD (32-bit) Value** and enter **IgnoreNoRevocationCheck**.
4. Double-click **IgnoreNoRevocationCheck** and set the Value data to **1**.
5. Select **OK** and reboot the server. Restarting the RRAS and NPS services does not suffice.

REGISTRY PATH	EAP EXTENSION
HKLM\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13	EAP-TLS

REGISTRY PATH	EAP EXTENSION
HKLM\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\25	PEAP
HKLM\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\26	EAP-MSCHAP v2

Next steps

Step 7.2. Create root certificates for VPN authentication with Azure AD: In this step, you configure conditional access root certificates for VPN authentication with Azure AD, which automatically creates a VPN Server cloud app in the tenant.

Step 7.2. Create conditional access root certificates for VPN authentication with Azure AD

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

- **Previous:** Step 7.1. Configure EAP-TLS to ignore Certificate Revocation List (CRL) checking
- **Next:** Step 7.3. Configure the Conditional Access policy

In this step, you configure conditional access root certificates for VPN authentication with Azure AD, which automatically creates a Cloud app called VPN Server in the tenant. To configure conditional access for VPN connectivity, you need to:

1. Create a VPN certificate in the Azure portal.
2. Download the VPN certificate.
3. Deploy the certificate to your VPN and NPS servers.

> **IMPORTANT**
>
> Once a VPN certificate is created in the Azure portal, Azure AD will start using it immediately to issue short lived certificates to the VPN client. It is critical that the VPN certificate be deployed immediately to the VPN server to avoid any issues with credential validation of the VPN client.

When a user attempts a VPN connection, the VPN client makes a call into the Web Account Manager (WAM) on the Windows 10 client. WAM makes a call to the VPN Server cloud app. When the Conditions and Controls in the Conditional Access policy are satisfied, Azure AD issues a token in the form of a short-lived (1-hour) certificate to the WAM. The WAM places the certificate in the user's certificate store and passes off control to the VPN client.

The VPN client then sends the certificate issued by Azure AD to the VPN for credential validation.

> **NOTE**
>
> Azure AD uses the most recently created certificate in the VPN connectivity blade as the Issuer.

Procedure:

1. Sign in to your Azure portal as a global administrator.
2. On the left menu, click **Azure Active Directory**.
3. On the **Azure Active Directory** page, in the **Manage** section, click **Security**.
4. On the **Security** page, in the **Protect** section, click **Conditional Access**.
5. On the **Conditional Access | Policies** page, in the **Manage** section, click **VPN Connectivity**.
6. On the **VPN connectivity** page, click **New certificate**.
7. On the **New** page, perform the following steps: a. For **Select duration**, select either 1, 2 or 3 years. b. Select **Create**.

Next steps

Step 7.3. Configure the Conditional Access policy: In this step, you configure the conditional access policy for VPN connectivity.

Step 7.3. Configure the conditional access policy

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

- **Previous:** Step 7.2. Create root certificates for VPN authentication with Azure AD
- **Next:** Step 7.4. Deploy conditional access root certificates to on-premises AD

In this step, you configure the conditional access policy for VPN connectivity. When the first root certificate is created in the 'VPN connectivity' blade, it automatically creates a 'VPN Server' cloud application in the tenant.

Create a Conditional Access policy that is assigned to VPN users group and scope the **Cloud app** to **VPN Server**:

- **Users**: VPN Users
- **Cloud App**: VPN Server
- **Grant (access control)**: 'Require multi-factor authentication'. Other controls can be used if desired.

Procedure: This step covers creation of the most basic Conditional Access policy. If desired, additional Conditions and Controls can be used.

1. On the **Conditional Access** page, in the toolbar on the top, select **Add**.

2. On the **New** page, in the **Name** box, enter a name for your policy. For example, enter **VPN policy**.

3. In the **Assignment** section, select **Users and groups**.

4. On the **Users and groups** page, perform the following steps:

a. Select **Select users and groups**.

b. Select **Select**.

c. On the **Select** page, select the **VPN users** group, and then select **Select**.

d. On the **Users and groups** page, select **Done**.

5. On the **New** page, perform the following steps:

a. In the **Assignments** section, select **Cloud apps**.

b. On the **Cloud apps** page, select **Select apps**.

d. Select **VPN Server**.

6. On the **New** page, to open the **Grant** page, in the **Controls** section, select **Grant**.

7. On the **Grant** page, perform the following steps:

a. Select **Require multi-factor authentication**.

b. Select **Select**.

8. On the **New** page, under **Enable policy**, select **On**.

9. On the **New** page, select **Create**.

Next steps

Step 7.4. Deploy conditional access root certificates to on-premises AD: In this step, you deploy the conditional access root certificate as trusted root certificate for VPN authentication to your on-premises AD.

Step 7.4. Deploy conditional access root certificates to on-premises AD

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

In this step, you deploy the conditional access root certificate as trusted root certificate for VPN authentication to your on-premises AD.

- **Previous:** Step 7.3. Configure the Conditional Access policy
- **Next:** Step 7.5. Create OMA-DM based VPNv2 Profiles to Windows 10 devices

1. On the **VPN connectivity** page, select **Download certificate**.

> **NOTE**
>
> The **Download base64 certificate** option is available for some configurations that require base64 certificates for deployment.

2. Log on to a domain-joined computer with Enterprise Admin rights and run these commands from an Administrator command prompt to add the cloud root certificate(s) into the *Enterprise NTauth* store:

> **NOTE**
>
> For environments where the VPN server is not joined to the Active Directory domain, the cloud root certificates must be added to the *Trusted Root Certification Authorities* store manually.

COMMAND	DESCRIPTION
`certutil -dspublish -f VpnCert.cer RootCA`	Creates two **Microsoft VPN root CA gen 1** containers under the **CN=AIA** and **CN=Certification Authorities** containers, and publishes each root certificate as a value on the *cACertificate* attribute of both **Microsoft VPN root CA gen 1** containers.
`certutil -dspublish -f VpnCert.cer NTAuthCA`	Creates one **CN=NTAuthCertificates** container under the **CN=AIA** and **CN=Certification Authorities** containers, and publishes each root certificate as a value on the *cACertificate* attribute of the **CN=NTAuthCertificates** container.
`gpupdate /force`	Expedites adding the root certificates to the Windows server and client computers.

3. Verify that the root certificates are present in the Enterprise NTauth store and show as trusted:

   a. Log on to a server with Enterprise Admin rights that has the **Certificate Authority Management Tools** installed.

> **NOTE**
>
> By default the **Certificate Authority Management Tools** are installed Certificate Authority servers. They can be installed on other members servers as part of the **Role Administration Tools** in Server Manager.

a. On the VPN server, in the Start menu, enter **pkiview.msc** to open the Enterprise PKI dialog.
b. From the Start menu, enter **pkiview.msc** to open the Enterprise PKI dialog.
c. Right-click **Enterprise PKI** and select **Manage AD Containers**.
d. Verify that each Microsoft VPN root CA gen 1 certificate is present under:
   - NTAuthCertificates
   - AIA Container
   - Certificate Authorities Container

Next steps

Step 7.5. Create OMA-DM based VPNv2 Profiles to Windows 10 devices: In this step, you can create OMA-DM based VPNv2 profiles using Intune to deploy a VPN Device Configuration policy. If you want to use Microsoft Endpoint Configuration Manager or PowerShell Script to create VPNv2 profiles, see VPNv2 CSP settings for more details.

Step 7.5. Create OMA-DM based VPNv2 profiles to Windows 10 devices

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

- **Previous:** Step 7.4. Deploy conditional access root certificates to on-premises AD
- **Next:** Learn how conditional access for VPN works

In this step, you can create OMA-DM based VPNv2 profiles using Intune to deploy a VPN Device Configuration policy. If you want to use Microsoft Endpoint Configuration Manager or PowerShell script to create VPNv2 profiles, see VPNv2 CSP settings for more details.

Managed Deployment using Intune

Everything discussed in this section is the minimum needed to make VPN work with Conditional Access. It does not cover Split Tunneling, Using WIP, creating custom Intune device configuration profiles to get AutoVPN working, or SSO. Integrate the settings below into the VPN profile you created earlier under Step 5. Configure Windows 10 Client Always On VPN Connections. In this example, we are integrating them into the Configure the VPN client by using Intune policy.

Prerequisite:

Windows 10 client computer has already been configured with a VPN connection using Intune.

Procedure:

1. In the Azure portal, select **Intune** > **Device Configuration** > **Profiles** and select the VPN profile you created earlier in Configure the VPN client by using Intune.
2. In the policy editor, select **Properties** > **Settings** > **Base VPN**. Extend the existing **EAP Xml** to include a filter that gives the VPN client the logic it needs to retrieve the AAD Conditional Access certificate from the user's certificate store instead of leaving it to chance allowing it to use the first certificate discovered.

> **NOTE**
>
> Without this, the VPN client could retrieve the user certificate issued from the on-premises certificate authority, resulting in a failed VPN connection.

3. Locate the section that ends with **</AcceptServerName></EapType>** and insert the following string between these two values to provide the VPN client with the logic to select the AAD Conditional Access Certificate:

```
<TLSExtensions xmlns="http://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2">
<FilteringInfo xmlns="http://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV3">
<EKUMapping><EKUMap><EKUName>AAD Conditional Access</EKUName><EKUOID>1.3.6.1.4.1.311.87</EKUOID>
</EKUMap></EKUMapping><ClientAuthEKUList Enabled="true"><EKUMapInList><EKUName>AAD Conditional
Access</EKUName></EKUMapInList></ClientAuthEKUList></FilteringInfo></TLSExtensions>
```

4. Select the **Conditional Access** blade and toggle **Conditional access for this VPN connection** to **Enabled**.

   Enabling this setting changes the **<DeviceCompliance><Enabled>true</Enabled>** setting in the VPNv2 Profile XML.

5. Select **OK**.

6. Select **Assignments**, under Include, select **Select groups to include**.

7. Select the **VPN Users** group that receives this policy and select **Save**.

Force MDM Policy Sync on the Client

If the VPN profile does not show up on the client device, under Settings\Network & Internet\VPN, you can force MDM policy to sync.

1. Sign in to a domain-joined client computer as a member of the **VPN Users** group.
2. On the Start menu, enter **account**, and press Enter.
3. In the left navigation pane, select **Access work or school**.
4. Under Access work or school, select **Connected to <\domain> MDM**, then select **Info**.
5. Select **Sync** and verify the VPN profile appears under Settings\Network & Internet\VPN.

Next steps

You are done configuring the VPN profile to use Azure AD conditional access.

IF YOU WANT TO...	THEN SEE...
Learn more about how conditional access works with VPNs	VPN and conditional access: This page provides more information about how conditional access works with VPNs.
Learn more about the advanced VPN features	Advanced VPN Features: This page provides guidance on how to enable VPN Traffic Filters, how to configure Automatic VPN connections using App-Triggers, and how to configure NPS to only allow VPN Connections from clients using certificates issued by Azure AD.

Related topics

- VPNv2 CSP: This topic provides you with an overview of VPNv2 CSP. The VPNv2 configuration service provider allows the mobile device management (MDM) server to configure the VPN profile of the device.
- Configure Windows 10 Client Always On VPN Connections: This topic provides information about the ProfileXML options and schema, and how to create the ProfileXML VPN. After setting up the server infrastructure, you must configure the Windows 10 client computers to communicate with that infrastructure with a VPN connection.
- Configure the VPN client by using Intune: This topic provides information on how to deploy Windows 10

Remote Access Always On VPN profiles. Intune now uses Azure AD groups. If Azure AD Connect synced the VPN Users group from on-premises to Azure AD, then there is no need for configuring the VPN client using Intune.

DirectAccess Offline Domain Join

12/9/2022 • 6 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This guide explains the steps to perform an offline domain join with DirectAccess. During an offline domain join, a computer is configured to join a domain without physical or VPN connection.

This guide includes the following sections:

- Offline domain join overview
- Requirements for offline domain join
- Offline domain join process
- Steps for performing an offline domain join

Offline domain join overview

Introduced in Windows Server 2008 R2, domain controllers include a feature called Offline Domain Join. A command line utility named Djoin.exe lets you join a computer to a domain without physically contacting a domain controller while completing the domain join operation. The general steps for using Djoin.exe are:

1. Run **djoin /provision** to create the computer account metadata. The output of this command is a .txt file that includes a base-64 encoded blob.
2. Run **djoin /requestODJ** to insert the computer account metadata from the .txt file into the Windows directory of the destination computer.
3. Reboot the destination computer, and the computer will be joined to the domain.

Offline domain join with DirectAccess policies scenario overview

DirectAccess offline domain join is a process that computers running Windows Server 2016, Windows Server 2012, Windows 10 and Windows 8 can use to join a domain without being physically joined to the corporate network, or connected through VPN. This makes it possible to join computers to a domain from locations where there is no connectivity to a corporate network. Offline domain join for DirectAccess provides DirectAccess policies to clients to allow remote provisioning.

A domain join creates a computer account and establishes a trust relationship between a computer running a Windows operating system and an Active Directory domain.

Prepare for offline domain join

1. Create the machine account.
2. Inventory the membership of all security groups to which the machine account belongs.
3. Gather the required computer certificates, group policies, and group policy objects to be applied to the new client(s).

. The following sections explain operating system requirements and credential requirements for performing a DirectAccess offline domain join using Djoin.exe.

Operating system requirements

You can run Djoin.exe for DirectAccess only on computers that run Windows Server 2016, Windows Server 2012 or Windows 8. The computer on which you run Djoin.exe to provision computer account data into AD DS must be running Windows Server 2016, Windows 10, Windows Server 2012 or Windows 8. The computer that you want to join to the domain must also be running Windows Server 2016, Windows 10, Windows Server 2012 , or Windows 8.

Credential requirements

To perform an offline domain join, you must have the rights that are necessary to join workstations to the domain. Members of the Domain Admins group have these rights by default. If you are not a member of the Domain Admins group, a member of the Domain Admins group must complete one of the following actions to enable you to join workstations to the domain:

- Use Group Policy to grant the required user rights. This method allows you to create computers in the default Computers container and in any organizational unit (OU) that is created later (if no Deny access control entries (ACEs) are added).
- Edit the access control list (ACL) of the default Computers container for the domain to delegate the correct permissions to you.
- Create an OU and edit the ACL on that OU to grant you the **Create child - Allow** permission. Pass the **/machineOU** parameter to the **djoin /provision** command.

The following procedures show how to grant the user rights with Group Policy and how to delegate the correct permissions.

Granting user rights to join workstations to the domain

You can use the Group Policy Management Console (GPMC) to modify the domain policy or create a new policy that has settings that grant the user rights to add workstations to a domain.

Membership in **Domain Admins**, or equivalent, is the minimum required to grant user rights. Review details about using the appropriate accounts and group memberships at Local and Domain Default Groups (https://go.microsoft.com/fwlink/?LinkId=83477).

To grant rights to join workstations to a domain

1. Click **Start**, click **Administrative Tools**, and then click **Group Policy Management**.
2. Double-click the name of the forest, double-click **Domains**, double-click the name of the domain in which you want to join a computer, right-click **Default Domain Policy**, and then click **Edit**.
3. In the console tree, double-click **Computer Configuration**, double-click **Policies**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then double-click **User Rights Assignment**.
4. In the details pane, double-click **Add workstations to domain**.
5. Select the **Define these policy settings** check box, and then click **Add User or Group**.
6. Type the name of the account that you want to grant the user rights to, and then click **OK** twice.

Offline domain join process

Run Djoin.exe at an elevated command prompt to provision the computer account metadata. When you run the provisioning command, the computer account metadata is created in a binary file that you specify as part of the command.

For more information about the NetProvisionComputerAccount function that is used to provision the computer account during an offline domain join, see NetProvisionComputerAccount Function

(https://go.microsoft.com/fwlink/?LinkId=162426). For more information about the NetRequestOfflineDomainJoin function that runs locally on the destination computer, see NetRequestOfflineDomainJoin Function (https://go.microsoft.com/fwlink/?LinkId=162427).

Steps for performing a DirectAccess offline domain join

The offline domain join process includes the following steps:

1. Create a new computer account for each of the remote clients and generate a provisioning package using the Djoin.exe command from an already domain joined computer in the corporate network.
2. Add the client computer to the DirectAccessClients security group
3. Transfer the provisioning package securely to the remote computers(s) that will be joining the domain.
4. Apply the provisioning package and join the client to the domain.
5. Reboot the client to complete the domain join and establish connectivity.

There are two options to consider when creating the provisioning packet for the client. If you used the Getting Started Wizard to install DirectAccess without PKI, then you should use option 1 below. If you used the Advanced Setup Wizard to install DirectAccess with PKI, then you should use option 2 below.

Complete the following steps to perform the offline domain join:

Option1: Create a provisioning package for the client without PKI

1. At a command prompt of your Remote Access server, type the following command to provision the computer account:

```
Djoin /provision /domain <your domain name> /machine <remote machine name> /policynames DA Client GPO name /rootcacerts /savefile c:\files\provision.txt /reuse
```

Option2: Create a provisioning package for the client with PKI

1. At a command prompt of your Remote Access server, type the following command to provision the computer account:

```
Djoin /provision /machine <remote machine name> /domain <Your Domain name> /policynames <DA Client GPO name> /certtemplate <Name of client computer cert template> /savefile c:\files\provision.txt /reuse
```

Add the client computer to the DirectAccessClients security group

1. On your Domain Controller, from **Start** screen, type **Active** and select **Active Directory Users and Computers** from **Apps** screen.
2. Expand the tree under your domain, and select the **Users** container.
3. In the details pane, right-click **DirectAccessClients**, and click **Properties**.
4. On the **Members** tab, click **Add**.
5. Click **Object Types**, select **Computers**, and then click **OK**.
6. Type the client name to add, and then click **OK**.
7. Click **OK** to close the **DirectAccessClients** Properties dialog, and then close **Active Directory Users and Computers**.

Copy and then apply the provisioning package to the client computer

1. Copy the provisioning package from c:\files\provision.txt on the Remote Access Server, where it was saved, to c:\provision\provision.txt on the client computer.

2. On the client computer, open an elevated command prompt, and then type the following command to request the domain join:

```
Djoin /requestodj /loadfile C:\provision\provision.txt /windowspath %windir% /localos
```

3. Reboot the client computer. The computer will be joined to the domain. Following the reboot, the client will be joined to the domain and have connectivity to the corporate network with DirectAccess.

See Also

NetProvisionComputerAccount Function NetRequestOfflineDomainJoin Function

Deploy a Single DirectAccess Server Using the Getting Started Wizard

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic provides an introduction to the DirectAccess scenario that uses a single DirectAccess server, and allows you to deploy DirectAccess in a few easy steps.

Before you begin deploying, see the list of unsupported configurations, known issues, and prerequisites

You can use the following topics to review prerequisites and other information before you deploy DirectAccess.

- DirectAccess Unsupported Configurations
- Prerequisites for Deploying DirectAccess

Scenario description

In this scenario, a Windows Server computer is configured as a DirectAccess server with default settings. The configuration only requires a few easy wizard steps, without any need to configure infrastructure settings such as a certification authority (CA) or Active Directory security groups.

> **NOTE**
>
> If you want to configure an advanced deployment with custom settings, see Deploy a Single DirectAccess Server with Advanced Settings

In this scenario

To set up a basic DirectAccess server, several planning and deployment steps are required.

Prerequisites

Before you begin deploying this scenario, review this list for important requirements:

- Windows firewall must be enabled on all profiles
- This scenario is only supported when your client computers are running Windows 10, Windows 8.1 or Windows 8.
- ISATAP in the corporate network isn't supported. If you're using ISATAP, you should remove it and use native IPv6.
- A Public Key Infrastructure isn't required.
- Not supported for deploying two factor authentication. Domain credentials are required for authentication.
- Automatically deploys DirectAccess to all mobile computers in the current domain.

- Traffic to Internet doesn't go over the DirectAccess tunnel. Force tunnel configuration isn't supported.
- DirectAccess server is the Network Location Server.
- Network Access Protection (NAP) isn't supported.
- Changing policies outside of the DirectAccess management console or PowerShell cmdlets isn't supported.
- To deploy multisite, now or in the future, first Deploy a Single DirectAccess Server with Advanced Settings.

Planning steps

Planning is divided into two phases:

1. Planning for the DirectAccess infrastructure. This phase describes the planning that's required to set up the network infrastructure before beginning the DirectAccess deployment. Planning includes the design of the network and server topology, and the DirectAccess network location server.
2. Planning for the DirectAccess deployment. This phase describes the planning steps required to prepare for the DirectAccess deployment. It includes planning for DirectAccess client computers, server and client authentication requirements, VPN settings, infrastructure servers, and management and application servers.

For detailed planning steps, see Plan an Advanced DirectAccess Deployment.

Deployment steps

Deployment is divided into three phases:

1. Configuring the DirectAccess infrastructure. This phase includes configuring the following components:

- Network and routing
- Firewall settings (if required)
- Certificates
- DNS servers
- Active Directory and GPO settings
- DirectAccess network location server

2. Configuring DirectAccess server settings. This phase includes steps for configuring DirectAccess client computers, the DirectAccess server, infrastructure servers, management and application servers.
3. Verifying the deployment. This phase includes steps to verify that the deployment is working as required.

For detailed deployment steps, see Install and Configure Basic DirectAccess.

Practical applications

Deploying a single Remote Access server provides the following benefits:

- Ease-of-access. You can configure managed client computers running Windows 10, Windows 8.1, Windows 8, or Windows 7, as DirectAccess clients. These clients can access internal network resources via DirectAccess anytime they're located on the Internet without needing to log in to a VPN connection. Client computers that aren't running one of these operating systems can connect to the internal network by using traditional VPN connections.
- Ease-of-management. DirectAccess client computers located on the Internet can be remotely managed by Remote Access administrators over DirectAccess, even when the client computers aren't located in the internal corporate network. Client computers that don't meet corporate requirements can be remediated

automatically by management servers. Both DirectAccess and VPN are managed in the same console and with the same set of wizards. Additionally, one or more Remote Access servers can be managed from a single Remote Access Management console

Roles and features included in this scenario

The following table lists the roles and features required for the scenario:

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access role	The role is installed and uninstalled using the Server Manager console or Windows PowerShell. This role encompasses both DirectAccess, Routing, and Remote Access Services. The Remote Access role consists of two components: 1. DirectAccess and Routing and Remote Access Services (RRAS) VPN. DirectAccess and VPN are managed together in the Remote Access Management console. 2. RRAS Routing. RRAS routing features are managed in the legacy Routing and Remote Access console. The Remote Access Server Role is dependent on the following server roles/features: - Internet Information Services (IIS) Web Server - This feature is required to configure the network location server on the Remote Access server, and the default web probe. - Windows Internal Database. Used for local accounting on the Remote Access server.
Remote Access Management Tools feature	This feature is installed as follows: - It's installed by default on a Remote Access server when the Remote Access role is installed, and supports the Remote Management console user interface and Windows PowerShell cmdlets. - It can be optionally installed on a server not running the Remote Access server role. In this case, it's used for remote management of a Remote Access computer running DirectAccess and VPN. The Remote Access Management Tools feature consists of the following components: - Remote Access GUI - Remote Access module for Windows PowerShell Dependencies include: - Group Policy Management Console - RAS Connection Manager Administration Kit (CMAK) - Windows PowerShell 3.0 - Graphical Management Tools and Infrastructure

Hardware requirements

Hardware requirements for this scenario include the following:

- Server requirements:
  - A computer that meets the hardware requirements for Windows Server 2016, Windows Server 2012 R2 , or Windows Server 2012 .

- The server must have at least one network adapter installed, enabled, and connected to the internal network. When two adapters are used, there should be one adapter connected to the internal corporate network, and one connected to the external network (Internet, or private network).
- At least one domain controller. The Remote Access server and DirectAccess clients must be domain members.

- Client requirements:
  - A client computer must be running Windows 10, Windows 8.1 or Windows 8.

    > **IMPORTANT**
    > If some or all of your client computers are running Windows 7, you must use the Advanced Setup Wizard. The Getting Started Setup Wizard described in this document doesn't support client computers that are running Windows 7. See Deploy a Single DirectAccess Server with Advanced Settings for instructions on how to use Windows 7 clients with DirectAccess.

    > **NOTE**
    > Only the following operating systems can be used as DirectAccess clients: Windows 10 Enterprise, Windows 8.1 Enterprise, Windows Server 2016, Windows Server 2012 R2 , Windows Server 2012 , Windows 8 Enterprise, Windows Server 2008 R2, Windows 7 Enterprise, and Windows 7 Ultimate.

- Infrastructure and management server requirements:
  - If VPN is enabled and a static IP address pool isn't configured, you must deploy a DHCP server to allocate IP addresses automatically to VPN clients.
- A DNS server running Windows Server 2016, Windows Server 2012 R2 , Windows Server 2012 , Windows Server 2008 SP2, or Windows Server 2008 R2 is required.

Software requirements

Below are the requirements for this scenario:

- Server requirements:
  - The Remote Access server must be a domain member. The server can be deployed at the edge of the internal network, or behind an edge firewall or other device.
  - If the Remote Access server is located behind an edge firewall or NAT device, the device must be configured to allow traffic to and from the Remote Access server.
  - The person deploying remote access on the server requires local administrator permissions on the server, and domain user permissions. In addition, the administrator requires permissions for the GPOs used in DirectAccess deployment. To take advantage of the features that restricts DirectAccess deployment to mobile computers only, permissions to create a WMI filter on the domain controller are required.

- Remote Access client requirements:
  - DirectAccess clients must be domain members. Domains containing clients can belong to the same forest as the Remote Access server, or have a two-way trust with the Remote Access server forest.
  - An Active Directory security group is required to contain the computers that will be configured as

DirectAccess clients. If a security group isn't specified when configuring DirectAccess client settings, by default the client GPO is applied on all laptop computers in the Domain Computers security group. Only the following operating systems can be used as DirectAccess clients: Windows Server 2016, Windows Server 2012 R2 , Windows Server 2012 , Windows Server 2008 R2, Windows 8 Enterprise, Windows 7 Enterprise, and Windows 7 Ultimate.

See also

The following table provides links to additional resources.

CONTENT TYPE	REFERENCES
Remote Access on TechNet	Remote Access TechCenter
Tools and settings	Remote Access PowerShell cmdlets
Community resources	DirectAccess Wiki entries
Related technologies	How IPv6 works

Plan a Basic DirectAccess Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes the planning steps required to deploy a single DirectAccess server running Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012 with basic features:

1. Step 1: Plan the Basic DirectAccess Infrastructure-Plan network and server topology, firewall settings, certificate requirements, DNS and Active Directory.
2. Step 2: Plan the Basic DirectAccess Deployment-Plan client and server deployment.

Next step

After you have completed these planning steps, you can begin the server deployment. For instructions, see Install and Configure Basic DirectAccess.

Step 1 Plan the Basic DirectAccess Infrastructure

12/9/2022 • 18 minutes to read • Edit Online

The first step for a basic DirectAccess deployment on a single server is to perform planning for the infrastructure required for the deployment. This topic describes the infrastructure planning steps:

TASK	DESCRIPTION
Plan network topology and settings	Decide where to place the DirectAccess server (at the edge, or behind a Network Address Translation (NAT) device or firewall), and plan IP addressing and routing.
Plan firewall requirements	Plan for allowing DirectAccess through edge firewalls.
Plan certificate requirements	DirectAccess can use Kerberos or certificates for client authentication. In this basic DirectAccess deployment a Kerberos Proxy is automatically configured and authentication is accomplished using Active Directory credentials.
Plan DNS requirements	Plan DNS settings for the DirectAccess server, infrastructure servers, and client connectivity.
Plan Active Directory	Plan your domain controllers and Active Directory requirements.
Plan Group Policy Objects	Decide what GPOs are required in your organization and how to create or edit the GPOs.

The planning tasks do not need to be done in a specific order.

Plan network topology and settings

Plan network adapters and IP addressing

1. Identify the network adapter topology you want to use. DirectAccess can be set up with either of the following:

   - With two network adapters - Either at the edge with one network adapter connected to the Internet and the other to the internal network, or behind a NAT, firewall, or router device, with one network adapter connected to a perimeter network and the other to the internal network.

   - Behind a NAT device with one network adapter - The DirectAccess server is installed behind a NAT device, and the single network adapter is connected to the internal network.

2. Identity your IP addressing requirements:

   DirectAccess uses IPv6 with IPsec to create a secure connection between DirectAccess client computers and the internal corporate network. However, DirectAccess does not necessarily require connectivity to the IPv6 Internet or native IPv6 support on internal networks. Instead, it automatically configures and uses IPv6 transition technologies to tunnel IPv6 traffic across the IPv4 Internet (6to4, Teredo, IP-HTTPS) and across your IPv4-only intranet (NAT64 or ISATAP). For an overview of these transition technologies, see the following resources:

- IPv6 Transition Technologies
- IP-HTTPS Tunneling Protocol Specification

3. Configure required adapters and addressing according to the following table. For deployments behind a NAT device using a single network adapter, configure your IP addresses using only the **Internal network adapter** column.

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER[1]	ROUTING REQUIREMENTS
IPv4 intranet and IPv4 Internet	Configure the following: - One static public IPv4 address with the appropriate subnet mask. - A default gateway IPv4 address of your Internet firewall or local Internet service provider (ISP) router.	Configure the following: - An IPv4 intranet address with the appropriate subnet mask. - A connection-specific DNS suffix of your intranet namespace. A DNS server must also be configured on the internal interface. - Do not configure a default gateway on any intranet interfaces.	To configure the DirectAccess server to reach all subnets on the internal IPv4 network do the following: 1. List the IPv4 address spaces for all the locations on your intranet. 2. Use the **route add -p** or **netsh interface ipv4 add route** commands to add the IPv4 address spaces as static routes in the IPv4 routing table of the DirectAccess server.

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv6 Internet and IPv6 intranet	Configure the following: - Use the autoconfigured address configuration provided by your ISP. - Use the **route print** command to ensure that a default IPv6 route pointing to the ISP router exists in the IPv6 routing table. - Determine whether the ISP and intranet routers are using default router preferences described in RFC 4191, and using a higher default preference than your local intranet routers. If both of these are true, no other configuration for the default route is required. The higher preference for the ISP router ensures that the active default IPv6 route of the DirectAccess server points to the IPv6 Internet. Because the DirectAccess server is an IPv6 router, if you have a native IPv6 infrastructure, the Internet interface can also reach the domain controllers on the intranet. In this case, add packet filters to the domain controller in the perimeter network that prevent connectivity to the IPv6 address of the Internet-facing interface of the DirectAccess server.	Configure the following: - If you are not using default preference levels, configure your intranet interfaces with the **netsh interface ipv6 set InterfaceIndex ignoredefaultroutes=enabled** command. This command ensures that additional default routes pointing to intranet routers will not be added to the IPv6 routing table. You can obtain the InterfaceIndex of your intranet interfaces from the display of the netsh interface show interface command.	If you have an IPv6 intranet, to configure the DirectAccess server to reach all of the IPv6 locations, do the following: 1. List the IPv6 address spaces for all the locations on your intranet. 2. Use the **netsh interface ipv6 add route** command to add the IPv6 address spaces as static routes in the IPv6 routing table of the DirectAccess server.

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv4 Internet and IPv6 intranet	The DirectAccess server forwards default IPv6 route traffic using the Microsoft 6to4 Adapter interface to a 6to4 relay on the IPv4 Internet. You can configure a DirectAccess server for the IPv4 address of the Microsoft 6to4 relay on the IPv4 Internet (used when native IPv6 is not deployed in the corporate network) with the following command : netsh interface ipv6 6to4 set relay name=192.88.99.1 state=enabled command.		

> **NOTE**
>
> Note the following:
>
> 1. If the DirectAccess client has been assigned a public IPv4 address, it will use the 6to4 transition technology to connect to the intranet. If the DirectAccess client cannot connect to the DirectAccess server with 6to4, it will use IP-HTTPS.
> 2. Native IPv6 client computers can connect to the DirectAccess server over native IPv6, and no transition technology is required.

Plan firewall requirements

If the DirectAccess server is behind an edge firewall, the following exceptions will be required for DirectAccess traffic when the DirectAccess server is on the IPv4 Internet:

- 6to4 traffic - IP Protocol 41 inbound and outbound.
- IP-HTTPS-Transmission Control Protocol (TCP) destination port 443, and TCP source port 443 outbound.
- If you are deploying DirectAccess with a single network adapter, and installing the network location server on the DirectAccess server, TCP port 62000 should also be exempted.

> **NOTE**
>
> This exemption is on the DirectAccess server. All the other exceptions are on the edge firewall.

The following exceptions will be required for DirectAccess traffic when the DirectAccess server is on the IPv6 Internet:

- IP Protocol 50
- UDP destination port 500 inbound, and UDP source port 500 outbound.

When using additional firewalls, apply the following internal network firewall exceptions for DirectAccess traffic:

- ISATAP - Protocol 41 inbound and outbound
- TCP/UDP for all IPv4/IPv6 traffic

Plan certificate requirements

Certificate requirements for IPsec include a computer certificate used by DirectAccess client computers when establishing the IPsec connection between the client and the DirectAccess server, and a computer certificate used by DirectAccess servers to establish IPsec connections with DirectAccess clients. For DirectAccess in Windows Server 2012 R2 and Windows Server 2012, the use of these IPsec certificates is not mandatory. The Getting Started Wizard configures the DirectAccess server to act as a Kerberos proxy to perform IPsec authentication without requiring certificates.

1. **IP-HTTPS server**. When you configure DirectAccess, the DirectAccess server is automatically configured to act as the IP-HTTPS web listener. The IP-HTTPS site requires a website certificate, and client computers must be able to contact the certificate revocation list (CRL) site for the certificate. The Enable DirectAccess wizard tries to use the SSTP VPN certificate. If SSTP is not configured, it checks if a certificate for IP-HTTPS is present in the machine personal store. If none is available, it automatically creates a self-signed certificate.

2. **Network location server**. The network location server is a website used to detect whether client computers are located in the corporate network. The network location server requires a web site certificate. DirectAccess clients must be able to contact the CRL site for the certificate. The Enable Remote Access wizard checks if a certificate for Network Location Server is present in the machine personal store. If not present, it automatically creates a self-signed certificate.

The certification requirements for each of these are summarized in the following table:

IPSEC AUTHENTICATION	IP-HTTPS SERVER	NETWORK LOCATION SERVER
An internal CA is required to issue computer certificates to the DirectAccess server and clients for IPsec authentication when you don't use the Kerberos proxy for authentication	Public CA - It is recommended to use a public CA to issue the IP-HTTPS certificate, this ensures that the CRL distribution point is available externally.	Internal CA - You can use an internal CA to issue the network location server website certificate. Make sure that the CRL distribution point is highly available from the internal network.
	Internal CA - You can use an internal CA to issue the IP-HTTPS certificate; however, you must make sure that the CRL distribution point is available externally.	Self-signed certificate - You can use a self-signed certificate for the network location server website; however, you cannot use a self-signed certificate in multisite deployments.
	Self-signed certificate - You can use a self-signed certificate for the IP-HTTPS server; however, you must make sure that the CRL distribution point is available externally. A self-signed certificate cannot be used in a multisite deployment.	

Plan certificates for IP-HTTPS and network location server

If you want to provision a certificate for these purposes, refer to Deploy a Single DirectAccess Server with Advanced Settings. If no certificates are available, the Getting Started wizard automatically creates self-signed certificates for these purposes.

> **NOTE**
> If you provision certificates for IP-HTTPS and the network location server manually, ensure that the certificates have a subject name. If the certificate does not have a subject name, but does have an alternative name, it will not be accepted by the DirectAccess wizard.

Plan DNS requirements

In a DirectAccess deployment, DNS is required for the following:

- **DirectAccess client requests**. DNS is used to resolve requests from DirectAccess client computers that are not located on the internal network. DirectAccess clients attempt to connect to the DirectAccess network location server in order to determine whether they are located on the Internet, or on the corporate network: If the connection is successful, then clients are determined to be on the intranet and DirectAccess is not used, and client requests are resolved using the DNS server configured on the network adapter of the client computer. If the connection does not succeed, clients are assumed to be on the Internet. DirectAccess clients will use the name resolution policy table (NRPT) to determine which DNS server to use when resolving name requests. You can specify that clients should use DirectAccess DNS64 to resolve names, or an alternative internal DNS server. When performing name resolution, the NRPT is used by DirectAccess clients to identify how to handle a request. Clients request an FQDN or single-label name such as http://internal. If a single-label name is requests, a DNS suffix is appended to make an FQDN. If the DNS query matches an entry in the NRPT, and DNS4 or an intranet DNS server is specified for the entry, then the query is sent for name resolution using the specified server. If a match exists but no DNS server is specified, then this indicates an exemption rule and normal name resolution is applied.

  When a new suffix is added to the NRPT in the DirectAccess Management console, the default DNS servers for the suffix can be automatically discovered by clicking the **Detect** button. Auto detection works as follows:

  1. If the corporate network is IPv4-based, or IPv4 and IPv6, the default address is the DNS64 address of the internal adapter on the DirectAccess server.
  2. If the corporate network is IPv6-based, the default address is the IPv6 address of DNS servers in the corporate network.

> **NOTE**
> Starting with the Windows 10 May 2020 Update, a client no longer registers its IP addresses on DNS servers configured in a Name Resolution Policy Table (NRPT). If DNS registration is needed, for example **Manage Out**, it can be explicitly enabled with this registry key on the client:
>
> Path: `HKLM\System\CurrentControlSet\Services\Dnscache\Parameters`
> Type: `DWORD`
> Value name: `DisableNRPTForAdapterRegistration`
> Values:
> `1` - DNS Registration disabled (default since the Windows 10 May 2020 Update)
> `0` - DNS Registration enabled

- **Infrastructure servers**

  1. **Network location server**. DirectAccess clients attempt to reach the network location server to determine if they are on the internal network. Clients on the internal network must be able to resolve the name of the network location server, but must be prevented from resolving the name when they are located on the Internet. To ensure this occurs, by default, the FQDN of the network location server is added as an exemption rule to the NRPT. In addition, when you configure

DirectAccess, the following rules are created automatically:

a. A DNS suffix rule for root domain or the domain name of the DirectAccess server, and the IPv6 addresses corresponding to the intranet DNS servers configured on the DirectAccess server. For example, if the DirectAccess server is a member of the corp.contoso.com domain, a rule is created for the corp.contoso.com DNS suffix.

b. An exemption rule for the FQDN of the network location server. For example, if the network location server URL is https://nls.corp.contoso.com, an exemption rule is created for the FQDN nls.corp.contoso.com.

IP-HTTPS server. The DirectAccess server acts as an IP-HTTPS listener and uses its server certificate to authenticate to IP-HTTPS clients. The IP-HTTPS name must be resolvable by DirectAccess clients using public DNS servers.

Connectivity verifiers. DirectAccess creates a default web probe that is used by DirectAccess client computers use to verify connectivity to the internal network. To ensure the probe works as expected the following names must be registered manually in DNS:

a. directaccess-webprobehost - should resolve to the internal IPv4 address of the DirectAccess server, or to the IPv6 address in an IPv6-only environment.

b. directaccess-corpconnectivityhost - should resolve to localhost (loopback) address. A and AAAA record should be created, A record with value 127.0.0.1 and AAAA record with value constructed out of NAT64 prefix with the last 32 bits as 127.0.0.1. The NAT64 prefix can be retrieved by running the cmdlet get-netnattransitionconfiguration.

You can create additional connectivity verifiers using other web addresses over HTTP or PING. For each connectivity verifier, a DNS entry must exist.

DNS server requirements

- For DirectAccess clients, you must use a DNS server that is running Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, or any DNS server that supports IPv6.

> **NOTE**
> It is not recommended that you use DNS servers that are running Windows Server 2003 when you are deploying DirectAccess. Although Windows Server 2003 DNS servers do support IPv6 records, Windows Server 2003 is no longer supported by Microsoft. In addition, you should not deploy DirectAccess if your domain controllers are running Windows Server 2003 due to an issue with the File Replication Service. For more information, see DirectAccess Unsupported Configurations.

Plan the network location server

The network location server is a website used to detect whether DirectAccess clients are located in the corporate network. Clients in the corporate network do not use DirectAccess to reach internal resources, but instead connect directly.

The Getting Started Wizard automatically sets up network location server on the DirectAccess server and the website is created automatically when you deploy DirectAccess. This allows for a simple installation without the use of a certificate infrastructure.

If you want to deploy a Network Location Server and not use self-signed certificates, refer to Deploy a Single DirectAccess Server with Advanced Settings.

Plan Active Directory

DirectAccess uses Active Directory and Active Directory Group policy objects as follows:

- **Authentication**. Active Directory is used for authentication. The DirectAccess tunnel uses Kerberos authentication for the user to access internal resources.
- **Group policy objects**. DirectAccess gathers configuration settings into group policy objects that are applied to DirectAccess servers, and clients.
- **Security groups**. DirectAccess uses security groups to gather together and identify DirectAccess client computers, and DirectAccess servers. The group policies are applied to the required security group.

Active Directory Requirements

When planning Active Directory for a DirectAccess deployment, the following is required:

- At least one domain controller installed on Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008.

  If the domain controller is on a perimeter network (and therefore reachable from the Internet-facing network adapter of DirectAccess server) prevent the DirectAccess server from reaching it by adding packet filters on the domain controller, to prevent connectivity to the IP address of the Internet adapter.
- The DirectAccess server must be a domain member.
- DirectAccess clients must be domain members. Clients can belong to:
  - Any domain in the same forest as the DirectAccess server.
  - Any domain that has a two-way trust with the DirectAccess server domain.
  - Any domain in a forest that has a two-way trust with the forest to which the DirectAccess domain belongs.

> **NOTE**
> - The DirectAccess server cannot be a domain controller.
> - The Active Directory domain controller used for DirectAccess must not be reachable from the external Internet adapter of the DirectAccess server (the adapter must not be in the domain profile of Windows Firewall).

Plan Group Policy Objects

DirectAccess settings configured when you configure DirectAccess are collected into Group policy objects (GPO). Two different GPOs are populated with DirectAccess settings, and distributed as follows:

- **DirectAccess client GPO**. This GPO contains client settings, including IPv6 transition technology settings, NRPT entries, and Windows Firewall with Advanced Security connection security rules. The GPO is applied to the security groups specified for the client computers.
- **DirectAccess server GPO**. This GPO contains the DirectAccess configuration settings that are applied to any server configured as a DirectAccess server in your deployment. It also contains Windows Firewall with Advanced Security connection security rules.

GPOs can be configured in two ways:

1. **Automatically**. You can specify that they are created automatically. A default name is specified for each GPO. GPOs are created automatically by the Getting Started Wizard.
2. **Manually**. You can use GPOs that have been predefined by the Active Directory administrator.

Note that once DirectAccess is configured to use specific GPOs, it cannot be configured to use different GPOs.

> **IMPORTANT**
> Whether you are using automatically or manually configured GPOs, you will need to add a policy for slow link detection if your clients will use 3G. The Group Policy path for **Policy: Configure Group Policy slow link detection** is: **Computer configuration / Polices / Administrative Templates / System / Group Policy**.

Caution

Use the following procedure to backup all DirectAccess Group Policy Objects before executing DirectAccess cmdlets: Back up and Restore DirectAccess Configuration

Automatically-created GPOs

Note the following when using automatically-created GPOs:

Automatically created GPOS are applied according to the location and link target parameter, as follows:

- For the DirectAccess server GPO, both the location and link parameters point to the domain containing the DirectAccess server.
- When client GPOs are created, the location is set to a single domain in which the GPO will be created. The GPO name is looked up in each domain, and filled with DirectAccess settings if it exists. The link target is set to the root of the domain in which the GPO was created. A GPO is created for each domain that contains client computers, and the GPO is linked to the root of its respective domain.

When using automatically created GPOs, to apply DirectAccess settings, the DirectAccess server administrator requires the following permissions:

- GPO create permissions for each domain.
- Link permissions for all the selected client domain roots.
- Link permissions for the server GPO domain roots.
- Create, edit, delete, and modify security permissions are required for the GPOs.
- It is recommended that the DirectAccess administrator has GPO read permissions for each required domain. This enables DirectAccess to verify that GPOs with duplicate names do not exist when creating GPOs.

Note that if the correct permissions for linking GPOs do not exist, a warning is issued. The DirectAccess operation will continue but linking will not occur. If this warning is issued links will not be created automatically, even after the permissions are added later. Instead the administrator will need to create the links manually.

Manually-created GPOs

Note the following when using manually-created GPOs:

- The GPOs should exist before running the Remote Access Getting Started wizard.
- When using manually-created GPOs, to apply DirectAccess settings the DirectAccess administrator requires full GPO permissions (Edit, Delete, Modify security) on the manually-created GPOs.
- When using manually created GPOs a search is made for a link to the GPO in the entire domain. If the GPO is not linked in the domain then a link is automatically created in the domain root. If the required permissions to create the link are not available a warning is issued.

Note that if the correct permissions for linking GPOs do not exist, a warning is issued. The DirectAccess operation will continue but linking will not occur. If this warning is issued links will not be created automatically, even when the permissions are added later. Instead the administrator will need to create the links manually.

Recovering from a deleted GPO

If a DirectAccess server, client, or application server GPO has been deleted by accident and there is no backup available, you must remove the configuration settings and re-configure again. If a backup is available, you can restore the GPO from the backup.

DirectAccess Management will display the following error message: **GPO <GPO name> cannot be found**. To remove the configuration settings, take the following steps:

1. Run the PowerShell cmdlet **Uninstall-remoteaccess**.
2. Re-open **DirectAccess Management**.
3. You will see an error message that the GPO is not found. Click **Remove configuration settings**. After completion, the server will be restored to an un-configured state.

Next step

- Step 2: Plan the Basic DirectAccess Deployment

Step 2 Plan the Basic DirectAccess Deployment

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After planning the DirectAccess infrastructure, the next step in deploying DirectAccess on a single server with basic settings is to plan the settings for the Getting Started Wizard.

TASK	DESCRIPTION
Planning for client deployment	By default, the Getting Started Wizard deploys DirectAccess to all laptops and notebook computers in the domain by applying a WMI filter to the client settings GPO
Planning for DirectAccess server deployment	Plan how to deploy the DirectAccess server.

Planning for client deployment

There are two decisions to make when planning your client deployment:

1. Will DirectAccess be available to mobile computers only, or to any computer?

   When you configure DirectAccess clients in the Getting Started Wizard, you can choose to allow only mobile computers in the specified security groups to connect using DirectAccess. If you restrict access to mobile computers, DirectAccess automatically configures a WMI filter to ensure that the DirectAccess client GPO is applied only to mobile computers in the specified security groups. The DirectAccess administrator requires permissions to create or modify group policy WMI filters to enable this setting.

2. What security groups will contain the DirectAccess client computers?

   DirectAccess settings are contained in the DirectAccess client GPO. The GPO is applied to computers that are part of the security groups that you specify in the Getting Started wizard. You can specify security groups contained in any supported domain. Before you configure DirectAccess, the security groups should be created. You can add computers to the security group after completing the DirectAccess deployment, but note that if you add client computers that reside in a different domain to the security group, the client GPO will not be applied to these clients. For example, if you created SG1 in domain A for DirectAccess clients, and later add clients from domain B to this group, the client GPO will not be applied to clients in domain B. To avoid this issue, create a new client security group for each domain that contains client computers. Alternatively, if you do not want to create a new security group, run the Add-DAClient cmdlet with the name of the new GPO for the new domain.

Planning for DirectAccess server deployment

There are a number of decisions to make when planning to deploy your DirectAccess server:

- **Network topology** -There are two topologies available when deploying a DirectAccess server:
  - **Two adapters** -With two network adapters, DirectAccess can be configured with one network adapter connected directly to the Internet, and the other is connected to the internal network. Or alternatively the server is installed behind an edge device such as a firewall or a router. In this configuration one network adapter is connected to the perimeter network, the other is connected

to the internal network.

  - **Single network adapter** -In this configuration the DirectAccess server is installed behind an edge device such as a firewall or a router. The network adapter is connected to the internal network.

- **Network adapters** -The DirectAccess wizard automatically detects the network adapters configured on the DirectAccess server. You can make sure that the correct adapters are selected from the **Review** page.
- **IP-HTTPS certificate** -Since there is no PKI required in this deployment, the wizard automatically provisions self-signed certificates for IP-HTTPS and the Network Location Server (if no certificates are present), and automatically enables Kerberos proxy. The wizard also enables NAT64 and DNS64 for protocol translation in the IPv4-only environment. After the wizard successfully completes applying the configuration, click **Close**.
- **Windows 7 clients** -You cannot enable support for Windows 7 clients from the Getting Started wizard. This can be enabled from the Advanced Setup Wizard. For more details, see Deploy a Single DirectAccess Server with Advanced Settings.
- **VPN configuration** -Before you configure DirectAccess, decide if you are going to provide VPN access to remote clients. You should provide VPN access if you have client computers in your organization that do not support DirectAccess connectivity (either because they are unmanaged or run an operating system for which DirectAccess is not supported). The Getting Started Wizard configures VPN IP address assignment using DHCP and configures VPN clients to be authenticated using Active Directory.
- **Force Tunneling** -If you plan to use Force Tunneling, or might add it in the future, you should use Deploy a Single DirectAccess Server with Advanced Settings to deploy a two tunnel configuration. Because of security considerations, Force Tunneling in a single tunnel configuration is not supported.

Previous step

- Step 1: Plan the Basic DirectAccess Infrastructure

Install and Configure Basic DirectAccess

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This overview provides an introduction to the configuration steps required to deploy a single DirectAccess server running Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012 with basic settings.

- Step 1: Configure the Basic DirectAccess Infrastructure. This step includes configuring network and server settings, DNS settings and Active Directory settings.
- Step 2: Configure the Basic DirectAccess Server. This step includes configuring DirectAccess client computers and server settings.
- Step 3: Verify Deployments. This includes steps for verifying your deployment.

Before starting your deployment, verify the planning steps described in Plan a Basic DirectAccess Deployment.

Step 1 Configure the Basic DirectAccess Infrastructure

12/9/2022 • 10 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to configure the infrastructure required for a basic DirectAccess deployment using a single DirectAccess server in a mixed IPv4 and IPv6 environment. Before beginning the deployment steps, ensure that you have completed the planning steps described in Plan a Basic DirectAccess Deployment.

TASK	DESCRIPTION
Configure server network settings	Configure the server network settings on the DirectAccess server.
Configure routing in the corporate network	Configure routing in the corporate network to make sure traffic is appropriately routed.
Configure firewalls	Configure additional firewalls, if required.
Configure the DNS server	Configure DNS settings for the DirectAccess server.
Configure Active Directory	Join client computers and the DirectAccess server to the Active Directory domain.
Configure GPOs	Configure GPOs for the deployment, if required.
Configure security groups	Configure security groups that will contain DirectAccess client computers, and any other security groups required in the deployment.

NOTE

This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

Configure server network settings

The following network interface settings are required for a single server deployment in an environment with IPv4 and IPv6. All IP addresses are configured by using **Change adapter settings** in the **Windows Networking and Sharing Center**.

- Edge topology
  - One Internet-facing public static IPv4 or IPv6 addresses.

> **NOTE**
> Two consecutive public IPv4 addresses are required for Teredo. If you are not using Teredo, you can configure a single public static IPv4 address.

  - A single internal static IPv4 or IPv6 address.

- Behind NAT device (two network adapters)
  - A single internal network-facing static IPv4 or IPv6 address.
  - A single perimeter network-facing static IPv4 or IPv6 address.
- Behind NAT device (one network adapter)
  - A single static IPv4 or IPv6 address.

> **NOTE**
> If the DirectAccess server has two or more network adapters (one classified in the domain profile and the other in a public/private profile), but you want to use a single NIC topology, then the recommendations are:
>
> 1. Ensure that the second NIC, and any additional NICs, are also classified in the domain profile.
> 2. If the second NIC cannot be configured for the domain profile for any reason, then the DirectAccess IPsec policy must be manually scoped to all profiles using the following Windows PowerShell commands:
>
>  ```
>  $gposession = Open-NetGPO -PolicyStore <Name of the server GPO>
>  Set-NetIPsecRule -DisplayName <Name of the IPsec policy> -GPOSession $gposession -Profile Any
>  Save-NetGPO -GPOSession $gposession
>  ```
>
> The names of the IPsec policies are DirectAccess-DaServerToInfra and DirectAccess-DaServerToCorp.

Configure routing in the corporate network

Configure routing in the corporate network as follows:

- When native IPv6 is deployed in the organization, add a route so that the routers on the internal network route IPv6 traffic back through the Remote Access server.
- Manually configure organization IPv4 and IPv6 routes on the Remote Access servers. Add a published route so that all traffic with an organization (/48) IPv6 prefix is forwarded to the internal network. In addition, for IPv4 traffic, add explicit routes so that IPv4 traffic is forwarded to the internal network.

Configure firewalls

When using additional firewalls in your deployment, apply the following Internet-facing firewall exceptions for Remote Access traffic when the Remote Access server is on the IPv4 Internet:

- 6to4 traffic -IP Protocol 41 inbound and outbound.
- IP-HTTPS -Transmission Control Protocol (TCP) destination port 443, and TCP source port 443 outbound. When the Remote Access server has a single network adapter, and the network location server is on the Remote Access server, then TCP port 62000 is also required.

> **NOTE**
> This exemption has to be configured on the remote access server. All the other exemptions have to be configured on the edge firewall.

> **NOTE**
> For Teredo and 6to4 traffic, these exceptions should be applied for both of the Internet-facing consecutive public IPv4 addresses on the Remote Access server. For IP-HTTPS the exceptions need only be applied for the address to which the external name of the server resolves.

When using additional firewalls, apply the following Internet-facing firewall exceptions for Remote Access traffic when the Remote Access server is on the IPv6 Internet:

- IP Protocol 50
- UDP destination port 500 inbound, and UDP source port 500 outbound.

When using additional firewalls, apply the following internal network firewall exceptions for Remote Access traffic:

- ISATAP -Protocol 41 inbound and outbound
- TCP/UDP for all IPv4/IPv6 traffic

Configure the DNS server

You must manually configure a DNS entry for the network location server website for the internal network in your deployment.

To create the network location server and NCSI probe DNS records

1. On the internal network DNS server, run **dnsmgmt.msc** and then press ENTER.
2. In the left pane of the **DNS Manager** console, expand the forward lookup zone for your domain. Right click the domain and click **New Host (A or AAAA)**.
3. On the **New Host** dialog box, in the **Name (uses parent domain name if blank)** box, enter the DNS name for the network location server website (this is the name the DirectAccess clients use to connect to the network location server). In the **IP address** box, enter the IPv4 address of the network location server, and then click **Add Host**. On the **DNS** dialog box, click **OK**.
4. On the **New Host** dialog box, in the **Name (uses parent domain name if blank)** box, enter the DNS name for the web probe (the name for the default web probe is directaccess-webprobehost). In the **IP address** box, enter the IPv4 address of the web probe, and then click **Add Host**. Repeat this process for directaccess-corpconnectivityhost and any manually created connectivity verifiers. On the **DNS** dialog box, click **OK**.
5. Click **Done**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Add-DnsServerResourceRecordA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv4Address
<network_location_server_IPv4_address>
Add-DnsServerResourceRecordAAAA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv6Address
<network_location_server_IPv6_address>
```

You must also configure DNS entries for the following:

- **The IP-HTTPS server** -DirectAccess clients must be able to resolve the DNS name of the Remote Access server from the Internet.
- **CRL revocation checking** -DirectAccess uses certificate revocation checking for the IP-HTTPS connection between DirectAccess clients and the Remote Access server, and for the HTTPS-based connection between the DirectAccess client and the network location server. In both cases, DirectAccess clients must be able to resolve and access the CRL distribution point location.

Configure Active Directory

The Remote Access server and all DirectAccess client computers must be joined to an Active Directory domain. DirectAccess client computers must be a member of one of the following domain types:

- Domains that belong to the same forest as the Remote Access server.
- Domains that belong to forests with a two-way trust with the Remote Access server forest.
- Domains that have a two-way domain trust to the Remote Access server domain.

To join the Remote Access server to a domain

1. In Server Manager, click **Local Server**. In the details pane, click the link next to **Computer name**.
2. On the **System Properties** dialog box, click the **Computer Name** tab. On the **Computer Name** tab, click **Change**.
3. In **Computer Name**, type the name of the computer if you are also changing the computer name when joining the server to the domain. Under **Member of**, click **Domain**, and then type the name of the domain to which you want to join the server; for example, corp.contoso.com, and then click **OK**.
4. When you are prompted for a user name and password, enter the user name and password of a user with rights to join computers to the domain, and then click **OK**.
5. When you see a dialog box welcoming you to the domain, click **OK**.
6. When you are prompted that you must restart the computer, click **OK**.
7. On the **System Properties** dialog box, click **Close**.
8. When you are prompted to restart the computer, click **Restart Now**.

To join client computers to the domain

1. Run **explorer.exe**.
2. Right-click the Computer icon, and then click **Properties**.
3. On the **System** page, click **Advanced system settings**.
4. On the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
5. In **Computer name**, type the name of the computer if you are also changing the computer name when joining the server to the domain. Under **Member of**, click **Domain**, and then type the name of the domain to which you want to join the server; for example, corp.contoso.com, and then click **OK**.

6. When you are prompted for a user name and password, enter the user name and password of a user with rights to join computers to the domain, and then click **OK**.
7. When you see a dialog box welcoming you to the domain, click **OK**.
8. When you are prompted that you must restart the computer, click **OK**.
9. On the **System Properties** dialog box, click Close. Click **Restart Now** when prompted.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

Note that you must supply domain credentials after entering the Add-Computer command below.

```
Add-Computer -DomainName <domain_name>
Restart-Computer
```

Configure GPOs

To deploy Remote Access, you require a minimum of two Group policy objects: one Group policy object contains settings for the Remote Access server and one contains settings for DirectAccess client computers. When you configure Remote Access, the wizard automatically creates the required Group policy object. However, if your organization enforces a naming convention, or you do not have the required permissions to create or edit Group policy objects, they must be created prior to configuring Remote Access.

To create a Group policy object, see Create and Edit a Group Policy Object.

IMPORTANT

The administrator can manually link the DirectAccess Group policy object to an Organizational Unit using these steps:

1. Before configuring DirectAccess, link the created GPOs to the respective Organizational Units.
2. Configure DirectAccess, specifying a security group for the client computers.
3. The administrator may or may not have permissions to link the Group Policy Objects to the domain. In either case, the Group Policy Objects will be configured automatically. If the GPOs are already linked to an OU, the links will not be removed. Nor will the GPOs be linked to the domain. For server GPO, the OU must contain the server computer object, else the GPO will be linked to the root of the domain.
4. If the linking to OU has not been done before running the DirectAccess wizard, after the configuration is complete, the administrator can link the DirectAccess Group Policy Objects to the required Organizational Units. The link to the domain can be removed. Steps for linking a Group policy object to an Organization Unit can be found here

NOTE

If a Group policy object was created manually, it is possible during the DirectAccess configuration that the Group policy object will not be available. The Group policy object may not have been replicated to the closest Domain Controller to the management computer. In this event, the administrator can wait for replication to complete, or force the replication.

WARNING

Using any means other than the DirectAccess Setup Wizard to configure DirectAccess, such as modifying DirectAccess Group Policy Objects directly or manually modifying the default policy settings on the server or client, is not supported.

Configure security groups

The DirectAccess settings contained in the client computer Group policy objects are applied only to computers that are members of the security groups that you specify when configuring Remote Access.

To create a security group for DirectAccess clients

1. Run **dsa.msc**. In the **Active Directory Users and Computers** console, in the left pane, expand the domain that will contain the security group, right-click **Users**, point to **New**, and then click **Group**.
2. On the **New Object - Group** dialog box, under **Group name**, enter the name for the security group.
3. Under **Group scope**, click **Global**, under **Group type**, click **Security**, and then click **OK**.
4. Double-click the DirectAccess client computers security group, and on the properties dialog box, click the **Members** tab.
5. On the **Members** tab, click **Add**.
6. On the **Select Users, Contacts, Computers, or Service Accounts** dialog box, select the client computers that you want to enable for DirectAccess, and then click **OK**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
New-ADGroup -GroupScope global -Name <DirectAccess_clients_group_name>
Add-ADGroupMember -Identity DirectAccess_clients_group_name -Members <computer_name>
```

Next step

- Step 2: Configure the Basic DirectAccess Server

Step 2 Configure the Basic DirectAccess Server

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to configure the client and server settings required for a basic DirectAccess deployment. Before beginning the deployment steps, ensure that you have completed the planning steps described in Plan a Basic DirectAccess Deployment.

TASK	DESCRIPTION
Install the Remote Access role	Install the Remote Access role.
Configure DirectAccess Using the Getting Started Wizard	The new Getting Started Wizard presents a greatly simplified configuration experience. The wizard masks the complexity of DirectAccess, and allows for an automated setup in a few simple steps. The wizard provides a seamless experience for the administrator by configuring Kerberos proxy automatically to eliminate the need for an internal PKI deployment.
Update clients with the DirectAccess configuration	To receive the DirectAccess settings, clients must update group policy while connected to the intranet.

NOTE

This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

Install the Remote Access role

To deploy Remote Access, you must install the Remote Access role on a server in your organization that will act as the Remote Access server.

To install the Remote Access role

1. On the Remote Access server, in the Server Manager console, in the **Dashboard**, click **Add roles and features**.
2. Click **Next** three times to get to the server role selection screen.
3. On the **Select server roles** dialog, select **Remote Access**, and then click **Next**.
4. On the **Select features** dialog, click **Next**.
5. Click **Next**, and then on the **Select role services** dialog, click the **DirectAccess and VPN (RAS)** check box.
6. Click **Add Features**, click **Next**, and then click **Install**.
7. On the **Installation progress** dialog, verify that the installation was successful, and then click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets install the Remote Access role:

1. Open PowerShell as administrator.
2. Install Remote Access feature:

```
Install-WindowsFeature RemoteAccess
```

3. Restart the computer:

```
Restart-Computer
```

4. Install Remote Access PowerShell:

```
Install-WindowsFeature RSAT-RemoteAccess-PowerShell
```

Configure DirectAccess with the Getting Started Wizard

To configure DirectAccess using the Getting Started Wizard

1. In Server Manager click **Tools**, and then click **Remote Access Management**.
2. In the Remote Access Management console, select the role service to configure in the left navigation pane, and then click **Run the Getting Started Wizard**.
3. Click **Deploy DirectAccess only**.
4. Select the topology of your network configuration and type the public name to which remote access clients will connect. Click **Next**.

> **NOTE**
> By default, the Getting Started Wizard deploys DirectAccess to all laptops and notebook computers in the domain by applying a WMI filter to the client settings GPO.

5. Click **Finish**.
6. Since there is no PKI used in this deployment, if certificates are not found, the wizard will automatically provision self-signed certificates for IP-HTTPS and the Network Location Server, and will automatically enable Kerberos proxy. The wizard will also enable NAT64 and DNS64 for protocol translation in the IPv4-only environment. After the wizard successfully completes applying the configuration, click **Close**.
7. In the console tree of the Remote Access Management console, select **Operations Status**. Wait until the status of all monitors display as "Working". In the Tasks pane under Monitoring, click **Refresh** periodically to update the display.

Update clients with the DirectAccess configuration

To update DirectAccess clients

1. Open PowerShell as an administrator.
2. In the PowerShell window, type **gpupdate** and then press **ENTER**.
3. Wait for the computer policy update to complete successfully.
4. Type **Get-DnsClientNrptPolicy** and then press **ENTER**

The Name Resolution Policy Table (NRPT) entries for DirectAccess are displayed. Note that the NLS server exemption is displayed. The Getting Started wizard automatically created this DNS entry for the DirectAccess server, and provisioned an associated self-signed certificate so that the DirectAccess server can function as the Network Location Server.

5. Type **Get-NCSIPolicyConfiguration** and then press **ENTER**. The network connectivity status indicator settings deployed by the wizard are displayed. Note the value of DomainLocationDeterminationURL. Whenever this network location server URL is accessible, the client will determine that it is inside the corporate network, and NRPT settings will not be applied.

6. Type **Get-DAConnectionStatus** and then press **ENTER**. Since the client can reach the network location server URL, the status will display as **ConnectedLocally**.

Previous step

- Step 1: Configure the DirectAccess Infrastructure

Next step

- Step 3 Verify Basic DirectAccess Deployments

Step 3 Verify Deployments

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to verify that you have correctly configured your basic DirectAccess deployment.

To verify access to internal resources through DirectAccess

1. Connect a DirectAccess client computer to the corporate network and obtain the group policy.
2. Click the **Network connections** icon in the notification area to access the DA Media Manager.
3. Click the **DirectAccess Connection**, and you will see that the status is **Connected Locally**.
4. Connect the client computer to the external network and attempt to access internal resources.

   You should be able to access all corporate resources.

Previous step

- Step 2: Configure the DirectAccess Server

Deploy a Single DirectAccess Server with Advanced Settings

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic provides an introduction to the DirectAccess scenario that uses a single DirectAccess server, and allows you to deploy DirectAccess with advanced settings.

Before you begin deploying, see the list of unsupported configurations, known issues, and prerequisites

You can use the following topics to review prerequisites and other information before you deploy DirectAccess.

- DirectAccess Unsupported Configurations
- Prerequisites for Deploying DirectAccess

Scenario description

In this scenario, a single computer running either Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012, is configured as a DirectAccess server with advanced settings.

> **NOTE**
>
> If you want to configure a basic deployment with simple settings only, see Deploy a Single DirectAccess Server Using the Getting Started Wizard. In the simple scenario, DirectAccess is configured with default settings by using a wizard, without any need to configure infrastructure settings such as a certification authority (CA) or Active Directory security groups.

In this scenario

To set up a single DirectAccess server with advanced settings, you must complete several planning and deployment steps.

Prerequisites

Before you begin, you can review the following requirements.

- Windows Firewall must be enabled on all profiles.
- The DirectAccess server is the network location server.
- You want all wireless computers in the domain where you install the DirectAccess server to be DirectAccess-enabled. When you deploy DirectAccess, it is automatically enabled on all mobile computers in the current domain.

> **IMPORTANT**
>
> Some technologies and configurations are not supported when you deploy DirectAccess.
>
> - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) in the corporate network is not supported. If you are using ISATAP, you must remove it and use native IPv6.

Planning steps

Planning is divided into two phases:

1. **Planning for the DirectAccess infrastructure**. This phase describes the planning required to set up the network infrastructure before beginning the DirectAccess deployment. It includes planning the network and server topology, certificate planning, DNS, Active Directory and Group Policy object (GPO) configuration, and the DirectAccess network location server.
2. **Planning for the DirectAccess deployment**. This phase describes the planning steps required to prepare for the DirectAccess deployment. It includes planning for DirectAccess client computers, server and client authentication requirements, VPN settings, infrastructure servers, and management and application servers.

Deployment steps

Deployment is divided into three phases:

1. **Configuring the DirectAccess infrastructure**. This phase includes configuring network and routing, configuring firewall settings if required, configuring certificates, DNS servers, Active Directory and GPO settings, and the DirectAccess network location server.
2. **Configuring DirectAccess server settings**. This phase includes steps for configuring DirectAccess client computers, the DirectAccess server, infrastructure servers, management and application servers.
3. **Verifying the deployment**. This phase includes steps to verify the DirectAccess deployment.

For detailed deployment steps, see Install and Configure Advanced DirectAccess.

Practical applications

Deploying a single DirectAccess server provides the following:

- **Ease of access**. Managed client computers running Windows 10, Windows 8.1, Windows 8, and Windows 7 can be configured as DirectAccess client computers. These clients can access internal network resources via DirectAccess any time they are located on the Internet without needing to log in to a VPN connection. Client computers not running one of these operating systems can connect to the internal network via VPN.
- **Ease of management**. DirectAccess client computers located on the Internet can be remotely managed by Remote Access administrators over DirectAccess, even when the client computers are not located in the internal corporate network. Client computers that do not meet corporate requirements can be remediated automatically by management servers. Both DirectAccess and VPN are managed in the same console and with the same set of wizards. Additionally, one or more DirectAccess servers can be managed from a single Remote Access Management console

Roles and features required for this scenario

The following table lists the roles and features that are required for this scenario:

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access role	The role is installed and uninstalled using the Server Manager console or Windows PowerShell. This role encompasses both DirectAccess and Routing and Remote Access Services (RRAS). The Remote Access role consists of two components: 1. DirectAccess and RRAS VPN. DirectAccess and VPN are managed together in the Remote Access Management console. 2. RRAS Routing. RRAS routing features are managed in the legacy Routing and Remote Access console. The Remote Access server role is dependent on the following server roles/features: - Internet Information Services (IIS) Web Server - This feature is required to configure the network location server on the DirectAccess server, and the default web probe. - Windows Internal Database. Used for local accounting on the DirectAccess server.
Remote Access Management Tools feature	This feature is installed as follows: - It is installed by default on a DirectAccess server when the Remote Access role is installed, and supports the Remote Management console user interface and Windows PowerShell cmdlets. - It can be optionally installed on a server not running the DirectAccess server role. In this case it is used for remote management of a Remote Access computer running DirectAccess and VPN. The Remote Access Management Tools feature consists of the following: - Remote Access graphical user interface (GUI) - Remote Access module for Windows PowerShell Dependencies include: - Group Policy Management Console - RAS Connection Manager Administration Kit (CMAK) - Windows PowerShell 3.0 - Graphical Management Tools and Infrastructure

Hardware requirements

Hardware requirements for this scenario include the following:

- Server requirements:
  - A computer that meets the hardware requirements for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 .
  - The server must have at least one network adapter installed, enabled, and connected to the internal network. When two adapters are used, there should be one adapter connected to the internal corporate network, and one connected to the external network (Internet, or private network).
  - If Teredo is required as an IPv4 to IPv6 transition protocol, the external adapter of the server

requires two consecutive public IPv4 addresses. If a single IP address is available, then only IP-HTTPS can be used as the transition protocol.

  - At least one domain controller. The DirectAccess server and DirectAccess clients must be domain members.
  - A certification authority (CA) is required if you do not want to use self-signed certificates for IP-HTTPS or the network location server, or if you want to use client certificates for client IPsec authentication. Alternatively, you can request certificates from a public CA.
  - If the network location server is not located on the DirectAccess server, a separate web server is required to run it.
- Client requirements:
  - A client computer must be running Windows 10, Windows 8, or Windows 7.

    > **NOTE**
    > The following operating systems can be used as DirectAccess clients: Windows 10, Windows Server 2012 R2 , Windows Server 2012 , Windows 8 Enterprise, Windows 7 Enterprise, or Windows 7 Ultimate.

- Infrastructure and management server requirements:
  - During remote management of DirectAccess client computers, clients initiate communications with management servers such as domain controllers, System Center Configuration Servers, and Health Registration Authority (HRA) servers for services that include Windows and antivirus updates and Network Access Protection (NAP) client compliance. The required servers should be deployed before beginning the Remote Access deployment.
  - If Remote Access requires client NAP compliance, NPS and HRS servers should be deployed before beginning remote access deployment
  - If VPN is enabled, a DHCP server is required to allocate IP addresses automatically to VPN clients, if a static address pool is not used.

Software requirements

There are a number of requirements for this scenario:

- Server requirements:
  - The DirectAccess server must be a domain member. The server can be deployed at the edge of the internal network, or behind an edge firewall or other device.
  - If the DirectAccess server is located behind an edge firewall or NAT device, the device must be configured to allow traffic to and from the DirectAccess server.
  - The person deploying remote access on the server requires local administrator permissions on the server, and domain user permissions. In addition, the administrator requires permissions for the GPOs used in DirectAccess deployment. To take advantage of the features that restricts DirectAccess deployment to mobile computers only, permissions to create a WMI filter on the domain controller are required.
- Remote Access client requirements:
  - DirectAccess clients must be domain members. Domains containing clients can belong to the same forest as the DirectAccess server, or have a two-way trust with the DirectAccess server forest or

domain.

- An Active Directory security group is required to contain the computers that will be configured as DirectAccess clients. If a security group is not specified when configuring DirectAccess client settings, by default the client GPO is applied on all laptop computers in the Domain Computers security group.

> **NOTE**
> It is recommended that you create a security group for each domain that contains DirectAccess client computers.

> **IMPORTANT**
> If you have enabled Teredo in your DirectAccess deployment, and you want to provide access to Windows 7 clients, ensure that the clients are upgraded to Windows 7 with SP1. Clients using Windows 7 RTM will not be able to connect over Teredo. However, these clients will still be able to connect to the corporate network over IP-HTTPS.

See also

The following table provides links to additional resources.

CONTENT TYPE	REFERENCES
Deployment	DirectAccess Deployment Paths in Windows Server Deploy a Single DirectAccess Server Using the Getting Started Wizard
Tools and settings	Remote Access PowerShell cmdlets
Community resources	DirectAccess Survival Guide DirectAccess Wiki entries
Related technologies	How IPv6 works

Plan an Advanced DirectAccess Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic lists the planning steps that are required to deploy a single DirectAccess server running Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012 with a full range of basic and advanced features. The planning phase includes the following topics.

- Step 1: Plan the Advanced DirectAccess Infrastructure

  In this phase, you plan your network and server topology, firewall settings, certificate requirements, the Domain Name System (DNS), Active Directory, DirectAccess management servers, and the DirectAccess network location server.

- Step 2: Plan Advanced DirectAccess Deployments

  In this phase, you plan for the client and server deployment, including the DirectAccess infrastructure and the application servers.

Next step

After you have completed these planning steps, you can begin the server deployment. For instructions, see Install and Configure Advanced DirectAccess.

Step 1 Plan the Advanced DirectAccess Infrastructure

12/9/2022 • 45 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first step of planning for an advanced DirectAccess deployment on a single server is to plan the infrastructure that is required for the deployment. This topic describes the infrastructure planning steps. These planning tasks do not need to be completed in a specific order.

TASK	DESCRIPTION
1.1 Plan network topology and settings	Decide where to place the DirectAccess server (at the edge, or behind a Network Address Translation (NAT) device or firewall), and plan IP addressing, routing, and force tunneling.
1.2 Plan firewall requirements	Plan for allowing DirectAccess traffic through edge firewalls.
1.3 Plan certificate requirements	Decide whether you want to use Kerberos or certificates for client authentication, and plan your website certificates. IP-HTTPS is a transition protocol that is used by DirectAccess clients to tunnel IPv6 traffic over IPv4 networks. Decide whether to authenticate to the IP-HTTPS server by using a certificate that is issued by a certification authority (CA), or by using a self-signed certificate that is issued automatically by the DirectAccess server.
1.4 Plan DNS requirements	Plan Domain Name System (DNS) settings for the DirectAccess server, infrastructure servers, local name resolution options, and client connectivity.
1.5 Plan the network location server	The network location server is used by DirectAccess clients to determine whether they are located on the internal network. Decide where to place the network location server website in your organization (on the DirectAccess server or an alternate server), and plan the certificate requirements if the network location server is located on the DirectAccess server.
1.6 Plan management servers	You can remotely manage DirectAccess client computers that are located outside the corporate network on the Internet. Plan for management servers (such as update servers) that are used during remote client management.
1.7 Plan Active Directory Domain Services	Plan for your domain controllers, your Active Directory requirements, client authentication, and multiple domains.
1.8 Plan Group Policy Objects	Decide what GPOs are required in your organization and how to create or edit the GPOs.

1.1 Plan network topology and settings

This section explains how to plan for your network, including:

- 1.1.1 Plan network adapters and IP addressing
- 1.1.2 Plan IPv6 intranet connectivity
- 1.1.3 Plan for force tunneling

1.1.1 Plan network adapters and IP addressing

1. Identify the network adapter topology you want to use. DirectAccess can be set up by using either of the following topologies:

   - **Two network adapters**. The DirectAccess server can be installed at the edge with one network adapter that is connected to the Internet and the other to the internal network, or it can be installed behind a NAT, firewall, or router device, with one network adapter connected to a perimeter network and the other to the internal network.

   - **One network adapter**. The DirectAccess server is installed behind a NAT device, and the single network adapter is connected to the internal network.

2. Identify your IP addressing requirements:

   DirectAccess uses IPv6 with IPsec to create a secure connection between DirectAccess client computers and the internal corporate network. However, DirectAccess does not necessarily require connectivity to the IPv6 Internet or native IPv6 support on internal networks. Instead, it automatically configures and uses IPv6 transition technologies to tunnel IPv6 traffic across the IPv4 Internet (by using 6to4, Teredo, or IP-HTTPS) and across your IPv4-only intranet (by using NAT64 or ISATAP). For an overview of these transition technologies, see the following resources:

   - IPv6 Transition Technologies
   - IP-HTTPS Tunneling Protocol Specification

3. Configure required adapters and addresses according to the following table. For deployments that use a single network adapter and are set up behind a NAT device, configure your IP addresses by using only the **Internal network adapter** column.

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv4 Internet and IPv4 intranet	Configure two static consecutive public IPv4 addresses with the appropriate subnet masks (required for Teredo only). Also configure the default gateway IPv4 address of your Internet firewall or local Internet service provider (ISP) router. **Note:** The DirectAccess server requires two consecutive public IPv4 addresses so that it can act as a Teredo server and Windows-based clients can use the DirectAccess server to detect the type of NAT device that they are behind.	Configure the following: - An IPv4 intranet address with the appropriate subnet mask. - The connection-specific DNS suffix of your intranet namespace. A DNS server should also be configured on the internal interface. **Caution:** Do not configure a default gateway on any intranet interfaces.	To configure the DirectAccess server to reach all subnets on the internal IPv4 network, do the following: - List the IPv4 address spaces for all the locations on your intranet. - Use the **route add -p** or the **netsh interface ipv4 add route** command to add the IPv4 address spaces as static routes in the IPv4 routing table of the DirectAccess server.

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv6 Internet and IPv6 intranet	Configure the following: - Use the address configuration that is provided by your ISP. - Use the **Route Print** command to ensure that a default IPv6 route exists, and it is pointing to the ISP router in the IPv6 routing table. - Determine whether the ISP and intranet routers are using the default router preferences described in RFC 4191, and using a higher default preference than your local intranet routers. If both of these are true, no other configuration for the default route is required. The higher preference for the ISP router ensures that the active default IPv6 route of the DirectAccess server points to the IPv6 Internet. Because the DirectAccess server is an IPv6 router, if you have a native IPv6 infrastructure, the Internet interface can also reach the domain controllers on the intranet. In this case, add packet filters to the domain controller in the perimeter network that prevent connectivity to the IPv6 address of the Internet-facing interface of the DirectAccess server.	Configure the following: - If you are not using the default preference levels, you can configure your intranet interfaces by using the following command**netsh interface ipv6 set InterfaceIndex ignoredefaultroutes=enabled**. This command ensures that additional default routes that point to intranet routers will not be added to the IPv6 routing table. You can obtain the interface index of your intranet interfaces by using the following command: **netsh interface ipv6 show interface**.	If you have an IPv6 intranet, to configure the DirectAccess server to reach all of the IPv6 locations, do the following: - List the IPv6 address spaces for all the locations on your intranet. - Use the **netsh interface ipv6 add route** command to add the IPv6 address spaces as static routes in the IPv6 routing table of the DirectAccess server.

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv4 Internet and IPv6 intranet	The DirectAccess server forwards default IPv6 route traffic through the Microsoft 6to4 adapter to a 6to4 relay on the IPv4 Internet. You can configure a DirectAccess server for the IPv4 address of the Microsoft 6to4 adapter by using the following command: `netsh interface ipv6 6to4 set relay name= <ipaddress> state=enabled` .		

NOTE

- If the DirectAccess client has been assigned a public IPv4 address, it will use the 6to4 transition technology to connect to the intranet. If it is assigned a private IPv4 address, it will use Teredo. If the DirectAccess client cannot connect to the DirectAccess server with 6to4 or Teredo, it will use IP-HTTPS.
- To use Teredo, you must configure two consecutive IP addresses on the external facing network adapter.
- You cannot use Teredo if the DirectAccess server has only one network adapter.
- Native IPv6 client computers can connect to the DirectAccess server over native IPv6, and no transition technology is required.

1.1.2 Plan IPv6 intranet connectivity

To manage remote DirectAccess clients, IPv6 is required. IPv6 allows DirectAccess management servers to connect to DirectAccess clients that are located on the Internet for the purpose of remote management.

NOTE

- Using IPv6 on your network is not required to support connections that are initiated by DirectAccess client computers to IPv4 resources on your organization network. NAT64/DNS64 is used for this purpose.
- If you are not managing remote DirectAccess clients, you do not need to deploy IPv6.
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is not supported in DirectAccess deployments.
- When you use IPv6, you can enable IPv6 host (AAAA) resource record queries for DNS64 by using the following Windows PowerShell command: **`Set-NetDnsTransitionConfiguration -OnlySendAQuery $false`**.

1.1.3 Plan for force tunneling

With IPv6 and the Name Resolution Policy Table (NRPT), by default, DirectAccess clients separate their intranet and Internet traffic as follows:

- DNS name queries for intranet fully qualified domain names (FQDNs) and all intranet traffic is exchanged over the tunnels that are created with the DirectAccess server or directly with intranet servers. Intranet traffic from DirectAccess clients is IPv6 traffic.

- DNS name queries for FQDNs that correspond to exemption rules or do not match the intranet namespace, and all traffic to Internet servers, is exchanged over the physical interface that is connected to the Internet. Internet traffic from DirectAccess clients is typically IPv4 traffic.

In contrast, by default, some remote access virtual private network (VPN) implementations, including the VPN

client, send all intranet and Internet traffic over the remote access VPN connection. Internet-bound traffic is routed by the VPN server to intranet IPv4 web proxy servers for access to IPv4 Internet resources. It is possible to separate the intranet and Internet traffic for remote access VPN clients by using split tunneling. This involves configuring the Internet Protocol (IP) routing table on VPN clients so that traffic to intranet locations is sent over the VPN connection, and traffic to all other locations is sent by using the physical interface that is connected to the Internet.

You can configure DirectAccess clients to send all of their traffic through the tunnels to the DirectAccess server with force tunneling. When force tunneling is configured, DirectAccess clients detect that they are on the Internet, and they remove their IPv4 default route. With the exception of local subnet traffic, all traffic sent by the DirectAccess client is IPv6 traffic that goes through tunnels to the DirectAccess server.

> **IMPORTANT**
>
> If you plan to use force tunneling, or you might add it in the future, you should deploy a two tunnel configuration. Because of security considerations, force tunneling in a single tunnel configuration is not supported.

Enabling force tunneling has the following consequences:

- DirectAccess clients use only Internet Protocol over Secure Hypertext Transfer Protocol (IP-HTTPS) to obtain IPv6 connectivity to the DirectAccess server over the IPv4 Internet.
- The only locations that a DirectAccess client can reach by default with IPv4 traffic are those on its local subnet. All other traffic that is sent by applications and services running on the DirectAccess client is IPv6 traffic, which is sent over the DirectAccess connection. Therefore, IPv4-only applications on the DirectAccess client cannot be used to reach Internet resources, except those on the local subnet.

> **IMPORTANT**
>
> For force tunneling through DNS64 and NAT64, IPv6 Internet connectivity must be implemented. One way to achieve this is by making the IP-HTTPS prefix globally routable, so that ipv6.msftncsi.com will be reachable over IPv6, and the response from the Internet server to the IP-HTTPS clients is able to return through the DirectAccess server.
>
> Because this is not feasible in most cases, the best option is to create virtual NCSI servers inside the corporate network as follows:
>
> 1. Add an NRPT entry for ipv6.msftncsi.com and resolve it against DNS64 to an internal website (this can be IPv4 website).
> 2. Add an NRPT entry for dns.msftncsi.com and resolve it against a corporate DNS server to return the IPv6 host (AAAA) resource record fd3e:4f5a:5b81::1. (Using DNS64 to only send host (A) resource record queries for this FQDN may not work because it is configured in IPv4 only deployments, so you should configure it to resolve against corporate DNS directly.)

1.2 Plan firewall requirements

If the DirectAccess server is behind an edge firewall, the following exceptions are required for Remote Access traffic when the DirectAccess server is on the IPv4 Internet:

- Teredo traffic-User Datagram Protocol (UDP) destination port 3544 inbound, and UDP source port 3544 outbound.
- 6to4 traffic-IP Protocol 41 inbound and outbound.
- IP-HTTPS-Transmission Control Protocol (TCP) destination port 443, and TCP source port 443 outbound.
- If you are deploying Remote Access with a single network adapter, and installing the network location

server on the DirectAccess server, TCP port 62000 should also be exempted.

> **NOTE**
> This exemption is on the DirectAccess server, and all other exemptions are on the edge firewall.

For Teredo and 6to4 traffic, these exceptions should be applied for both of the Internet-facing consecutive public IPv4 addresses on the DirectAccess server. For IP-HTTPS, the exceptions need to be applied on the address that is registered on the public DNS server.

The following exceptions are required for Remote Access traffic when the DirectAccess server is on the IPv6 Internet:

- IP Protocol ID 50
- UDP destination port 500 inbound, and UDP source port 500 outbound
- ICMPv6 traffic inbound and outbound (when using Teredo only)

When you use additional firewalls, apply the following internal network firewall exceptions for Remote Access traffic:

- ISATAP-Protocol 41 inbound and outbound
- TCP/UDP for all IPv4 and IPv6 traffic
- ICMP for all IPv4 and IPv6 traffic (when using Teredo only)

1.3 Plan certificate requirements

There are three scenarios that require certificates when you deploy a single DirectAccess server:

- 1.3.1 Plan computer certificates for IPsec authentication

  Certificate requirements for IPsec include a computer certificate that is used by DirectAccess client computers when they establish the IPsec connection between the client and the DirectAccess server, and a computer certificate that is used by DirectAccess servers to establish IPsec connections with DirectAccess clients.

  For DirectAccess in Windows Server 2012 the use of these IPsec certificates is not mandatory. As an alternative the DirectAccess server can act as a Kerberos proxy to perform IPsec authentication without requiring certificates. If Kerberos protocol is used, it works over SSL, and the Kerberos proxy uses the certificate that is configured for IP-HTTPS for this purpose. Some enterprise scenarios (including multisite deployment and one-time password (OTP) client authentication) require the use of certificate authentication, and not the Kerberos protocol.

- 1.3.2 Plan certificates for IP-HTTPS

  When you configure Remote Access, the DirectAccess server is automatically configured to act as the IP-HTTPS listener. The IP-HTTPS site requires a website certificate, and client computers must be able to contact the certificate revocation list (CRL) site for the certificate.

- 1.3.3 Plan website certificates for the network location server

  The network location server is a website that is used to detect whether client computers are located in the corporate network. The network location server requires a website certificate. DirectAccess clients must be able to contact the CRL site for the certificate.

The certification authority (CA) requirements for each scenario are summarized in the following table.

IPSEC AUTHENTICATION	IP-HTTPS SERVER	NETWORK LOCATION SERVER
An internal CA is required to issue computer certificates to the DirectAccess server and clients for IPsec authentication when you don't use the Kerberos proxy for authentication	Internal CA: You can use an internal CA to issue the IP-HTTPS certificate; however, you must make sure that the CRL distribution point is available externally.	Internal CA: You can use an internal CA to issue the network location server website certificate. Make sure that the CRL distribution point has high availability from the internal network.
	Self-signed certificate: You can use a self-signed certificate for the IP-HTTPS server; however, you must make sure that the CRL distribution point is available externally. A self-signed certificate cannot be used in multisite deployments.	Self-signed certificate: You can use a self-signed certificate for the network location server website. A self-signed certificate cannot be used in multisite deployments.
	Recommended Public CA: It is recommended to use a public CA to issue the IP-HTTPS certificate. This ensures that the CRL distribution point is available externally.	

1.3.1 Plan computer certificates for IPsec authentication

If you are using certificate-based IPsec authentication, the DirectAccess server and clients are required to obtain a computer certificate. The simplest way to install the certificates is to configure Group Policy-based automatic enrollment for computer certificates. This ensures that all domain members obtain a certificate from an enterprise CA. If you do not have an enterprise CA set up in your organization, see Active Directory Certificate Services.

This certificate has the following requirements:

- The certificate should have a Client Authentication extended key usage (EKU).
- The client certificate and the server certificate should chain to the same root certificate. This root certificate must be selected in the DirectAccess configuration settings.

1.3.2 Plan certificates for IP-HTTPS

The DirectAccess server acts as an IP-HTTPS listener, and you must manually install an HTTPS website certificate on the server. Consider the following when you are planning:

- Using a public CA is recommended, so that certificate revocation lists (CRLs) are readily available.
- In the **Subject** field, specify the IPv4 address of the Internet adapter of DirectAccess server or the FQDN of the IP-HTTPS URL (the ConnectTo address). If the DirectAccess server is located behind a NAT device, the public name or address of the NAT device should be specified.
- The common name of the certificate should match the name of the IP-HTTPS site.
- For the **Enhanced Key Usage** field, use the server authentication object identifier (OID).
- For the **CRL Distribution Points** field, specify a CRL distribution point that is accessible by DirectAccess clients that are connected to the Internet.

- The IP-HTTPS certificate must have a private key.
- The IP-HTTPS certificate must be imported directly into the personal store.
- IP-HTTPS certificates can have wildcard characters in the name.

If you plan to use IP-HTTPS on a non-standard port, perform the following steps on the DirectAccess server:

1. Remove the existing certificate binding for 0.0.0.0:443, and replace it with a certificate binding for your chosen port. For purposes of this example, port 44500 is used. Prior to deleting the certificate binding, show and copy the **appid**.

   a. To delete the certificate binding, enter:

   ```
   netsh http delete ssl ipport=0.0.0.0:443
   ```

   b. To add the new certificate binding, enter:

   ```
   netsh http add ssl ipport=0.0.0.0:44500 certhash=<use the thumbprint from the DirectAccess
   server SSL cert> appid=<use the appid from the binding that was deleted>
   ```

2. To modify the IP-HTTPS URL on the server, enter:

   ```
   Netsh int http set int url=https://<DirectAccess server name (for example
   server.contoso.com)>:44500/IPHTTPS
   ```

   ```
   Net stop iphlpsvc & net start iphlpsvc
   ```

3. Change the URL reservation for kdcproxy.

   a. To delete the existing URL reservation, enter:

   ```
   netsh http del urlacl url=https://+:443/KdcProxy/
   ```

   b. To add a new URL reservation, enter:

   ```
   netsh http add urlacl url=https://+:44500/KdcProxy/ sddl=D:(A;;GX;;;NS)
   ```

4. Add the setting to make kppsvc listen on the non-standard port. To add the registry entry, enter:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KPSSVC\Settings /v HttpsUrlGroup /t REG_MULTI_SZ
   /d +:44500 /f
   ```

5. To restart the kdcproxy service on the domain controller, enter:

   ```
   net stop kpssvc & net start kpssvc
   ```

To use IP-HTTPS on a non-standard port, perform the following steps on the domain controller:

1. Modify the IP-HTTPS setting in the client GPO.

   a. Open the Group Policy editor.

b. Navigate to Computer configuration=>Policies=>Administrative Templates=> Network=>TCPIP settings =>IPv6 transition technologies.

c. Open the IP-HTTPS state setting and change the URL to **https://<DirectAccess server name (for example server.contoso.com)>:44500/IPHTTPS**.

d. Click **Apply**.

2. Modify the Kerberos proxy client settings in the client GPO.

a. In the Group Policy editor, navigate to Computer configuration=>Policies=>Administrative Templates=> System=>Kerberos => Specify the KDC proxy servers for Kerberos clients.

b. Open the IPHTTPS state setting and change the URL to **https://<DirectAccess server name (for example server.contoso.com)>:44500/IPHTTPS**.

c. Click **Apply**.

3. Modify the client IPsec policy settings to use ComputerKerb and UserKerb.

a. In the Group Policy editor, navigate to Computer configuration=>Policies=> Windows Settings=> Security Settings=> Windows Firewall with Advanced security.

b. Click **Connection security rules**, and then double-click **IPsec rule**.

c. On the **Authentication** tab, click **Advanced**.

d. For Auth1: rRmove the existing authentication method, and replace it with ComputerKerb. For Auth2: Remove the existing authentication method, and replace it with UserKerb.

e. Click **Apply**, and then **OK**.

To complete the manual process for using an IP-HTTPS non-standard port, run **gpupdate /force** on the client computers and the DirectAccess server.

1.3.3 Plan website certificates for the network location server

When you plan for the network location server website, consider the following:

- In the **Subject** field, specify the IP address of the intranet interface of the network location server or the FQDN of the network location URL.
- In the **Enhanced Key Usage** field, use the Server Authentication OID.
- In the **CRL Distribution Points** field, use a CRL distribution point that is accessible by DirectAccess clients that are connected to the intranet. This CRL distribution point should not be accessible from outside the internal network.
- If you are later planning to configure a multisite or cluster deployment, the name of the certificate should not match the internal name of any DirectAccess server that will be added to the deployment.

> **NOTE**
>
> Ensure that the certificates for IP-HTTPS and the network location server have a **Subject Name**. If the certificate does not have a **Subject Name**, but it has an **Alternative Name**, it will not be accepted by the Remote Access Wizard.

1.4 Plan DNS requirements

This section explains the DNS requirements for DirectAccess client requests and infrastructure servers in a

Remote Access deployment. It includes the following subsections:

- 1.4.1 Plan for DNS server requirements
- 1.4.2 Plan for local name resolution

DirectAccess client requests

DNS is used to resolve requests from DirectAccess client computers that are not located on the internal (or corporate) network. DirectAccess clients attempt to connect to the DirectAccess network location server to determine whether they are located on the Internet, or on the internal network.

- If the connection is successful, clients are identified as being located on the internal network, DirectAccess is not used, and client requests are resolved by using the DNS server that is configured on the network adapter of the client computer.
- If the connection does not succeed, clients are assumed to be located on the Internet, and DirectAccess clients will use the name resolution policy table (NRPT) to determine which DNS server to use when resolving name requests.

You can specify that clients use DirectAccess DNS64 to resolve names, or an alternative internal DNS server. When performing name resolution, the NRPT is used by DirectAccess clients to identify how to handle a request. Clients request an FQDN or single-label name such as https://internal. If a single-label name is requested, a DNS suffix is appended to make an FQDN. If the DNS query matches an entry in the NRPT, and DNS64 or a DNS server on the internal network is specified for the entry, the query is sent for name resolution using the specified server. If a match exists, but no DNS server is specified, this indicates an exemption rule, and normal name resolution is applied.

> **NOTE**
> Note that when a new suffix is added to the NRPT in the Remote Access Management Console, the default DNS servers for the suffix can be automatically discovered by clicking **Detect**.

Auto detection works as follows:

- If the corporate network is IPv4-based, or it uses IPv4 and IPv6, the default address is the DNS64 address of the internal adapter on the DirectAccess server.
- If the corporate network is IPv6-based, the default address is the IPv6 address of DNS servers in the corporate network.

> **NOTE**
> Starting with the Windows 10 May 2020 Update, a client no longer registers its IP addresses on DNS servers configured in a Name Resolution Policy Table (NRPT). If DNS registration is needed, for example **Manage Out**, it can be explicitly enabled with this registry key on the client:
>
> Path: `HKLM\System\CurrentControlSet\Services\Dnscache\Parameters`
> Type: `DWORD`
> Value name: `DisableNRPTForAdapterRegistration`
> Values:
> `1` - DNS Registration disabled (default since the Windows 10 May 2020 Update)
> `0` - DNS Registration enabled

Infrastructure servers

- **Network location server**

DirectAccess clients attempt to reach the network location server to determine if they are on the internal network. Clients on the internal network must be able to resolve the name of the network location server, but they must be prevented from resolving the name when they are located on the Internet. To ensure that this occurs, by default, the FQDN of the network location server is added as an exemption rule to the NRPT. In addition, when you configure Remote Access, the following rules are created automatically:

- A DNS suffix rule for the root domain or the domain name of the DirectAccess server, and the IPv6 addresses that correspond to the DNS64 address. In IPv6-only corporate networks, the intranet DNS servers are configured on the DirectAccess server. For example, if the DirectAccess server is a member of the corp.contoso.com domain, a rule is created for the corp.contoso.com DNS suffix.
- An exemption rule for the FQDN of the network location server. For example, if the network location server URL is https://nls.corp.contoso.com, an exemption rule is created for the FQDN nls.corp.contoso.com.

- **IP-HTTPS server**

  The DirectAccess server acts as an IP-HTTPS listener, and it uses its server certificate to authenticate to IP-HTTPS clients. The IP-HTTPS name must be resolvable by DirectAccess clients that are using public DNS servers.

- **CRL revocation checking**

  DirectAccess uses certificate revocation checking for the IP-HTTPS connection between DirectAccess clients and the DirectAccess server, and for the HTTPS-based connection between the DirectAccess client and the network location server. In both cases, DirectAccess clients must be able to resolve and access the CRL distribution point location.

- **ISATAP**

  ISATAP enables corporate computers to acquire an IPv6 address, and it encapsulates IPv6 packets within an IPv4 header. It is used by the DirectAccess server to provide IPv6 connectivity to ISATAP hosts across an intranet. In a non-native IPv6 network environment, the DirectAccess server configures itself automatically as an ISATAP router.

  Because ISATAP is no longer supported in DirectAccess, you must ensure that your DNS servers are configured not to respond to ISATAP queries. By default, the DNS Server service blocks name resolution for the ISATAP name through the DNS Global Query Block List. Do not remove the ISATAP name from the Global Query Block List.

- **Connectivity verifiers**

  Remote Access creates a default web probe that is used by DirectAccess client computers to verify connectivity to the internal network. To ensure that the probe works as expected, the following names must be registered manually in DNS:

  - **directaccess-webprobehost**-Should resolve to the internal IPv4 address of the DirectAccess server, or to the IPv6 address in an IPv6-only environment.
  - **directaccess-corpconnectivityhost**-Should resolve to the local host (loopback) address. The following host (A) and (AAAA) resource records should be created: a host (A) resource record with value 127.0.0.1, and a host (AAAA) resource record with value constructed out of NAT64 prefix with the last 32 bits as 127.0.0.1. The NAT64 prefix can be retrieved by running the Windows PowerShell command **get-netnattransitionconfiguration**.

> **NOTE**
> This is valid only in an IPv4-only environment. In an IPv4 plus IPv6, or an IPv6-only environment, only a host (AAAA) resource record should be created with the loopback IP address ::1.

You can create additional connectivity verifiers by using other web addresses over HTTP or by using **ping**. For each connectivity verifier, a DNS entry must exist.

1.4.1 Plan for DNS server requirements

Following are the requirements for DNS when you deploy DirectAccess.

- For DirectAccess clients, you must use a DNS server that is running Windows Server 2012 R2 , Windows Server 2012 , Windows Server 2008 R2 , Windows Server 2008 , or any other DNS server that supports IPv6.

  > **NOTE**
  > It is not recommended that you use DNS servers that are running Windows Server 2003 when you are deploying DirectAccess. Although Windows Server 2003 DNS servers do support IPv6 records, Windows Server 2003 is no longer supported by Microsoft. In addition, you should not deploy DirectAccess if your domain controllers are running Windows Server 2003 due to an issue with the File Replication Service. For more information, see DirectAccess Unsupported Configurations.

- Use a DNS server that supports dynamic updates. You can use DNS servers that do not support dynamic updates, but you must manually update entries on these servers.
- The FQDN for your Internet-accessible CRL distribution points must be resolvable by using Internet DNS servers. For example, if URL https://crl.contoso.com/crld/corp-DC1-CA.crl is in the **CRL Distribution Points** field of the IP-HTTPS certificate of the DirectAccess server, you must ensure that the FQDN crld.contoso.com is resolvable by using Internet DNS servers.

1.4.2 Plan for local name resolution

When you plan for local name resolution, consider the following issues:

NRPT

You may need to create additional NRPT rules in the following cases:

- If you need to add more DNS suffixes for your intranet namespace.
- If the fully qualified domain name (FQDN) of your CRL distribution points are based on your intranet namespace, you must add exemption rules for the FQDNs of the CRL distribution points.
- If you have a split-brain DNS environment, you must add exemption rules for the names of resources for which you want DirectAccess clients located on the Internet to access the Internet version, rather than the intranet version.
- If you are redirecting traffic to an external website through your intranet web proxy servers, the external website is available only from the intranet, and it uses the addresses of your web proxy servers to permit the inbound requests. In this case, add an exemption rule for the FQDN of the external website, and specify that the rule use your intranet web proxy server rather than the IPv6 addresses of intranet DNS servers.

  For example, if you are testing an external website named test.contoso.com, this name is not resolvable through Internet DNS servers, but the Contoso web proxy server knows how to resolve the name and to direct requests for the website to the external web server. To prevent users who are not on the Contoso

intranet from accessing the site, the external website allows requests only from the IPv4 Internet address of the Contoso web proxy. Thus, intranet users can access the website because they are using the Contoso web proxy, but DirectAccess users cannot access it because they are not using the Contoso web proxy. By configuring an NRPT exemption rule for test.contoso.com that uses the Contoso web proxy, webpage requests for test.contoso.com are routed to the intranet web proxy server over the IPv4 Internet.

Single label names

Single label names, such as https://paycheck, are sometimes used for intranet servers. If a single label name is requested, and a DNS suffix search list is configured, the DNS suffixes in the list will be appended to the single label name. For example, when a user on a computer that is a member of the corp.contoso.com domain types https://paycheck in the web browser, the FQDN that is constructed as the name is paycheck.corp.contoso.com. By default the appended suffix is based on the primary DNS suffix of the client computer.

> **NOTE**
>
> In a disjoint name space scenario (where one or more domain computers has a DNS suffix that does not match the Active Directory domain to which the computers belong), you should ensure that the search list is customized to include all the required suffixes. By default, the Remote Access Wizard will configure the Active Directory DNS name as the primary DNS suffix on the client. Make sure to add the DNS suffix that is used by clients for name resolution.

If multiple domains and Windows Internet Name Service (WINS) are deployed in your organization and you are connecting remotely, single-names can be resolved as follows:

- Deploy a WINS forward lookup zone in the DNS. When trying to resolve computername.dns.zone1.corp.contoso.com, the request is directed to the WINS server that is using only computername. The client thinks it is issuing a regular DNS host (A) resource record, but it is actually a NetBIOS request. For more information, see Managing a Forward Lookup Zone.
- Add a DNS suffix, for example dns.zone1.corp.contoso.com, to the default domain policy GPO.

Split-brain DNS

Split-brain DNS is the use of the same DNS domain for Internet and intranet name resolution.

For split-brain DNS deployments, you must list the FQDNs that are duplicated on the Internet and intranet, and decide which resources the DirectAccess client should reach-the intranet or the Internet version. For each name that corresponds to a resource for which you want DirectAccess clients to reach the Internet version, you must add the corresponding FQDN as an exemption rule to the NRPT for your DirectAccess clients.

In a split-brain DNS environment, if you want both versions of the resource to be available, configure your intranet resources with alternate names, that are not duplicates of the names used on the Internet, and instruct your users to use the alternate name when on the Intranet. For example, configure the alternate name www.internal.contoso.com for the internal name www.contoso.com.

In a non-split-brain DNS environment, the Internet namespace is different from the intranet namespace. For example, the Contoso Corporation uses contoso.com on the Internet and corp.contoso.com on the intranet. Because all intranet resources use the corp.contoso.com DNS suffix, the NRPT rule for corp.contoso.com routes all DNS name queries for intranet resources to intranet DNS servers. DNS name queries for names with the contoso.com suffix do not match the corp.contoso.com intranet namespace rule in the NRPT, and are sent to Internet DNS servers. With a non-split-brain DNS deployment, because there is no duplication of FQDNs for intranet and Internet resources, there is no additional configuration needed for the NRPT. DirectAccess clients can access both Internet and intranet resources for the organization.

Local name resolution behavior for DirectAccess clients

If a name cannot be resolved with DNS, to resolve the name on the local subnet, the DNS Client service in

Windows Server 2012 R2 , Windows Server 2012 , Windows Server 2008 R2 , Windows 8, and Windows 7 can use local name resolution, with the Link-Local Multicast Name Resolution (LLMNR) and NetBIOS over TCP/IP protocols.

Local name resolution is typically needed for peer-to-peer connectivity when the computer is located on private networks, such as single subnet home networks. When the DNS Client service performs local name resolution for intranet server names and the computer is connected to a shared subnet on the Internet, malicious users can capture LLMNR and NetBIOS over TCP/IP messages to determine intranet server names. On the DNS page of the Infrastructure Server Setup Wizard, you configure the local name resolution behavior based on the types of responses received from intranet DNS servers. The following options are available:

- **Use local name resolution if the name does not exist in DNS**. This option is the most secure because the DirectAccess client performs local name resolution only for server names that cannot be resolved by intranet DNS servers. If the intranet DNS servers can be reached, the names of intranet servers are resolved. If the intranet DNS servers cannot be reached, or if there are other types of DNS errors, the intranet server names are not leaked to the subnet through local name resolution.
- **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)**. This option is recommended because it allows the use of local name resolution on a private network only when the intranet DNS servers are unreachable.
- **Use local name resolution for any kind of DNS resolution error (least secure)**. This is the least secure option because the names of intranet network servers can be leaked to the local subnet through local name resolution.

1.5 Plan the network location server

The network location server is a website that is used to detect whether DirectAccess clients are located in the corporate network. Clients in the corporate network do not use DirectAccess to reach internal resources, but instead, they connect directly.

The network location server website can be hosted on the DirectAccess server or on another server in your organization. If you host the network location server on the DirectAccess server, the website is created automatically when you install the Remote Access server role. If you host the network location server on another server in your organization running a Windows operating system, you must make sure that Internet Information Services (IIS) is installed on that server, and that the website is created. DirectAccess does not configure settings on a remote network location server.

Ensure that the network location server website meets the following requirements:

- It is a website with an HTTPS server certificate.
- DirectAccess client computers must trust the CA that issued the server certificate to the network location server website.
- DirectAccess client computers on the internal network must be able to resolve the name of the network location server site.
- The network location server site must have high availability to computers on the internal network.
- The network location server must not be accessible to DirectAccess client computers on the Internet.
- The server certificate must be checked against a CRL.

1.5.1 Plan certificates for the network location server

When you are obtaining the website certificate to use for the network location server, consider the following:

1. In the **Subject** field, specify an IP address of the intranet interface of the network location server or the FQDN of the network location URL.
2. In the **Enhanced Key Usage** field, use the Server Authentication OID.
3. In the **CRL Distribution Points** field, use a CRL distribution point that is accessible by DirectAccess clients that are connected to the intranet. This CRL distribution point should not be accessible from outside the internal network.

1.5.2 Plan DNS for the network location server

DirectAccess clients attempt to reach the network location server to determine if they are on the internal network. Clients on the internal network must be able to resolve the name of the network location server, but they must be prevented from resolving the name when they are located on the Internet. To ensure that this occurs, by default, the FQDN of the network location server is added as an exemption rule to the NRPT.

1.6 Plan management servers

DirectAccess clients initiate communications with management servers that provide services such as Windows Update and antivirus updates. DirectAccess clients also use the Kerberos protocol to contact domain controllers to authenticate before they access the internal network. During remote management of DirectAccess clients, management servers communicate with client computers to perform management functions such as software or hardware inventory assessments. Remote Access can automatically discover some management servers, including:

- Domain controllers-Auto-discovery of domain controllers is performed for all domains in the same forest as the DirectAccess server and client computers.
- Microsoft Endpoint Configuration Manager servers-Auto-discovery of Configuration Manager servers is performed for all domains in the same forest as the DirectAccess server and client computers.

Domain controllers and Configuration Manager servers are automatically detected the first time that DirectAccess is configured. Detected domain controllers are not displayed in the console, but settings can be retrieved by using the Windows PowerShell cmdlet **Get-DAMgmtServer -Type All**. If domain controller or Configuration Manager servers are modified, clicking **Refresh Management Servers** in the Remote Access Management console refreshes the management server list.

Management server requirements

- Management servers must be accessible over the first (infrastructure) tunnel. When you configure Remote Access, adding servers to the management servers list automatically makes them accessible over this tunnel.
- Management servers that initiate connections to DirectAccess clients must fully support IPv6, by means of a native IPv6 address or by using one that is assigned by ISATAP.

1.7 Plan Active Directory Domain Services

This section explains how DirectAccess uses Active Directory Domain Services (AD DS), and it includes the following subsections:

- 1.7.1 Plan client authentication
- 1.7.2 Plan multiple domains

DirectAccess uses AD DS and Active Directory Group policy objects (GPOs) as follows:

- **Authentication**

AD DS is used for authentication. The infrastructure tunnel uses NTLMv2 authentication for the computer account that is connecting to the DirectAccess server, and the account must be listed in an Active Directory domain. The intranet tunnel uses Kerberos authentication for the user to create the second tunnel.

- **Group Policy Objects**

  DirectAccess gathers configuration settings into GPOs that are applied to DirectAccess servers, clients, and internal application servers.

- **Security groups**

  DirectAccess uses security groups to gather and identify DirectAccess client computers. The GPOs are applied to the required security group.

- **Extended IPsec policies**

  DirectAccess can use IPsec authentication and encryption between clients and the DirectAccess server. You can extend IPsec authentication and encryption from the client to the specified internal application servers. To do this, add the required application servers into a security group.

AD DS requirements

When you plan AD DS for a DirectAccess deployment, consider the following requirements:

- At least one domain controller must be installed with the Windows Server 2016, Windows Server 2012 R2 , Windows Server 2012 , Windows Server 2008 R2 , or Windows Server 2008 operating system.

  If the domain controller is on a perimeter network (and therefore reachable from the Internet-facing network adapter of the DirectAccess server), you must prevent the DirectAccess server from reaching it by adding packet filters on the domain controller to prevent connectivity to the IP address of the Internet adapter.

- The DirectAccess server must be a domain member.
- DirectAccess clients must be domain members. Clients can belong to:
  - Any domain in the same forest as the DirectAccess server.
  - Any domain that has a two-way trust with the DirectAccess server domain.
  - Any domain in a forest that has a two-way trust with the forest to which the DirectAccess domain belongs.

> **NOTE**
> - The DirectAccess server cannot be a domain controller.
> - The AD DS domain controller that is used for DirectAccess must not be reachable from the external Internet adapter of the DirectAccess server (that is, the adapter must not be in the domain profile of Windows Firewall).

1.7.1 Plan client authentication

DirectAccess allows you to choose between using certificates for IPsec computer authentication or using a built-in Kerberos proxy that authenticates by using user names and passwords.

When choosing to use Ad DS credentials for authentication, DirectAccess uses one security tunnel that uses Computer Kerberos for the first authentication and User Kerberos for the second authentication. When using this mode for authentication, DirectAccess uses a single security tunnel that provides access to the DNS server, the domain controller, and to other servers on the internal network.

When choosing to use two-factor authentication or Network Access Protection, DirectAccess uses two security tunnels. The Remote Access Setup Wizard configures Windows Firewall with Advanced Security connection security rules that specify the use of the following types of credentials when negotiating the IPsec security associations for the tunnels to the DirectAccess server:

- The infrastructure tunnel uses Computer Kerberos credentials for the first authentication and User Kerberos for the second authentication.
- The intranet tunnel uses computer certificate credentials for the first authentication and User Kerberos for the second authentication.

When DirectAccess is choosing to allow access to clients running Windows 7 or in a multisite deployment, it uses two security tunnels. The Remote Access Setup Wizard configures Windows Firewall with Advanced Security connection security rules that specify the use of the following types of credentials when negotiating the IPsec security associations for the tunnels to the DirectAccess server:

- The infrastructure tunnel uses computer certificate credentials for the first authentication and NTLMv2 for the second authentication. NTLMv2 credentials force the use of Authenticated Internet Protocol (AuthIP), and they provide access to a DNS server and domain controller before the DirectAccess client can use Kerberos credentials for the intranet tunnel.
- The intranet tunnel uses computer certificate credentials for the first authentication and User Kerberos for the second authentication.

1.7.2 Plan multiple domains

The management servers list should include domain controllers from all domains that contain security groups that include DirectAccess client computers. It should contain all domains that contain user accounts that might use computers that are configured as DirectAccess clients. This ensures that users who are not located in the same domain as the client computer they are using are authenticated with a domain controller in the user domain. This is done automatically if domains are in the same forest.

> **NOTE**
>
> If there are computers in the security groups that are used for client computers or application servers in different forests, the domain controllers of those forests are not detected automatically. You can run the task **Refresh Management Servers** in the Remote Access Management console to detect these domain controllers.

Where possible, common domain name suffixes should be added to the Name Resolution Policy Table (NRPT) during the Remote Access deployment. For example, if you have two domains, domain1.corp.contoso.com and domain2.corp.contoso.com, instead of adding two entries into the NRPT, you can add a common DNS suffix entry, where the domain name suffix is corp.contoso.com. This happens automatically for domains in the same root, but domains that are not in the same root must be added manually.

If Windows Internet Name Service (WINS) is deployed in a multiple domain environment, you must deploy a WINS forward lookup zone in DNS. For more information, see **Single label names** in the 1.4.2 Plan for local name resolution section earlier in this document.

1.8 Plan Group Policy Objects

This section explains the role of Group Policy Objects (GPOs) in your Remote Access infrastructure, and it includes the following subsections:

- 1.8.1 Configure automatically created GPOs
- 1.8.2 Configure manually created GPOs

- 1.8.3 Manage GPOs in a multi-domain controller environment
- 1.8.4 Manage Remote Access GPOs with limited permissions
- 1.8.5 Recover from a deleted GPO

DirectAccess settings that are configured when you configure Remote Access are collected into GPOs. The following types of GPOs are populated with DirectAccess settings, and they are distributed as follows:

- **DirectAccess client GPO**

  This GPO contains client settings, including IPv6 transition technology settings, NRPT entries, and Windows Firewall with Advanced Security connection security rules. The GPO is applied to the security groups that are specified for the client computers.

- **DirectAccess server GPO**

  This GPO contains the DirectAccess configuration settings that are applied to any server that is configured as a DirectAccess server in your deployment. It also contains Windows Firewall with Advanced Security connection security rules.

- **Application servers GPO**

  This GPO contains settings for selected application servers to which you optionally extend authentication and encryption from DirectAccess clients. If authentication and encryption are not extended, this GPO is not used.

GPOs can be configured in two ways:

- **Automatically**-You can specify that they are created automatically. A default name is specified for each GPO.
- **Manually**-You can use GPOs that have been predefined by the Active Directory administrator.

> **NOTE**
> After DirectAccess is configured to use specific GPOs, it cannot be configured to use different GPOs.

Whether you are using automatically or manually configured GPOs, you need to add a policy for slow link detection if your clients will use 3G networks. The path for **Policy: Configure Group Policy slow link detection** is: **Computer configuration/Polices/Administrative Templates/System/Group Policy**.

Caution

Use the following procedure to back up all Remote Access GPOs before you run DirectAccess cmdlets: Back up and Restore Remote Access Configuration.

If the correct permissions (which are listed in the following sections) for linking GPOs do not exist, a warning is issued. The Remote Access operation will continue but linking will not occur. If this warning is issued, links will not be created automatically, even when the permissions are added later. Instead the administrator needs to create the links manually.

1.8.1 Configure automatically created GPOs

Consider the following when you use automatically-created GPOs.

Automatically created GPOs are applied according to the location and link target parameter, as follows:

- For the DirectAccess server GPO, the location parameter and the link parameter point to the domain that contains the DirectAccess server.
- When client and application server GPOs are created, the location is set to a single domain in which the

GPO will be created. The GPO name is looked up in each domain, and it is filled with DirectAccess settings if it exists. The link target is set to the root of the domain in which the GPO was created. A GPO is created for each domain that contains client computers or application servers, and the GPO is linked to the root of its respective domain.

When you use automatically created GPOs to apply DirectAccess settings, the Remote Access administrator requires the following permissions:

- GPO create permissions for each domain
- Link permissions for all the selected client domain roots
- Link permissions for the server GPO domain roots

In addition, the following permissions are needed:

- Create, Edit, Delete, and Modify security permissions are required for the GPOs.
- We recommend that the Remote Access administrator has GPO Read permissions for each required domain. This enables Remote Access to verify that GPOs with duplicate names do not exist when creating GPOs.

1.8.2 Configure manually created GPOs

Consider the following when using manually created GPOs:

- The GPOs should exist before running the Remote Access Setup Wizard.
- To apply DirectAccess settings, the Remote Access administrator requires full GPO permissions (Edit, Delete, Modify security permissions) on the manually created GPOs.
- A search is made in the entire domain for a link to the GPO. If the GPO is not linked in the domain, a link is automatically created in the domain root. If the required permissions to create the link are not available, a warning is issued.

1.8.3 Manage GPOs in a multi-domain controller environment

Each GPO is managed by a specific domain controller, as follows:

- The server GPO is managed by one of the domain controllers in the Active Directory site that is associated with the server. If domain controllers in that site are Read-only, the server GPO is managed by the Write-enabled domain controller that is closest to the DirectAccess server.
- Client and application server GPOs are managed by the domain controller that is running as the primary domain controller (PDC).

If you want to manually modify GPO settings, consider the following:

- For the server GPO, to identify which domain controller is associated with the DirectAccess server, from an elevated command prompt on the DirectAccess server, run **nltest /dsgetdc: /writable**.
- By default, when you make changes with networking Windows PowerShell cmdlets or you make changes from the Group Policy Management console, the domain controller that is acting as the PDC is used.

In addition, if you modify settings on a domain controller that is not the domain controller associated with the DirectAccess server (for the server GPO) or the PDC (for client and application server GPOs), consider the following:

- Before you modify the settings, ensure that the domain controller is replicated with an up-to-date GPO, and back up your GPO settings. For more information, see Back up and Restore Remote Access Configuration. If the GPO is not updated, merge conflicts during replication might occur, which can result in a corrupt Remote Access configuration.

- After you modify the settings, you must wait for changes to replicate to the domain controllers that are associated with the GPOs. Do not make additional changes by using the Remote Access Management console or Remote Access PowerShell cmdlets until replication is complete. If a GPO is edited on two domain controllers before replication is complete, merge conflicts might occur, which can result in a corrupt Remote Access configuration.

Alternatively, you can change the default setting by using the **Change Domain Controller** dialog box in the Group Policy Management console, or by using the Windows PowerShell cmdlet **Open-NetGPO**, so that the changes use the domain controller you specify.

- To do this in the Group Policy Management console, right-click the domain or sites container, and click **Change Domain Controller**.
- To do this in Windows PowerShell, specify the **DomainController** parameter for the **Open-NetGPO** cmdlet. For example, to enable the private and public profiles in Windows Firewall on a GPO named domain1\DA_Server_GPO _Europe by using a domain controller named europe-dc.corp.contoso.com, enter the following:

```
$gpoSession = Open-NetGPO -PolicyStore "domain1\DA_Server_GPO _Europe" -DomainController "europe-
dc.corp.contoso.com"
Set-NetFirewallProfile -GpoSession $gpoSession -Name @("Private","Public") -Enabled True
Save-NetGPO -GpoSession $gpoSession
```

1.8.4 Manage Remote Access GPOs with limited permissions

To manage a Remote Access deployment, the Remote Access administrator requires full GPO permissions (Read, Edit, Delete, and Modify security permissions) on the GPOs that are used in the deployment. This is because the Remote Access Management console and the Remote Access PowerShell modules read the configuration from and write it to the Remote Access GPOs (that is, client, server, and application server GPOs).

In many organizations, the domain administrator who is in charge of GPO operations is not the same person as the Remote Access administrator who is in charge of the Remote Access configuration. These organizations may have policies that restrict the Remote Access administrator from having full permissions on GPOs in the domain. The domain administrator may be also required to review the policy configuration before applying it to any computer in the domain.

To accommodate these requirements, the domain administrator should create two copies of each GPO: staging and production. The Remote Access administrator is given full permissions on the staging GPOs. The Remote Access administrator specifies the staging GPOs in the Remote Access Management console and in Windows PowerShell cmdlets as the GPOs used for the Remote Access deployment. This enables the Remote Access administrator to read and modify the Remote Access configuration as and when required.

The domain administrator must make sure that the staging GPOs are not linked to any scope-of-management in the domain and that the Remote Access administrator does not have GPO link permissions in the domain. This ensures that changes made by the Remote Access administrator to the staging GPOs do not have any effect on computers in the domain.

The domain administrator links the production GPOs to the required scope-of-management and applies the appropriate security filtering. This ensures that changes to these GPOs are applied to the computers in the domain (client computers, DirectAccess servers, and application servers). The Remote Access administrator has no permissions on the production GPOs.

When changes are made to the staging GPOs, the domain administrator can review the policy configuration in these GPOs to make sure that it satisfies the security requirements in the organization. The domain administrator then exports the settings from the staging GPOs by using the backup feature, and imports the settings to the corresponding production GPOs, which will be applied to the computers in the domain.

The following diagram shows this configuration.

1.8.5 Recover from a deleted GPO

If a client, DirectAccess server, or application server GPO has been deleted accidentally and there is no backup available, you must remove the configuration settings and reconfigure them. If a backup is available, you can restore the GPO from the backup.

The Remote Access Management console will display the following error message: **GPO (GPO name) cannot be found**. To remove the configuration settings, take the following steps:

1. Run the Windows PowerShell cmdlet **Uninstall-remoteaccess**.
2. Open the Remote Access Management console.
3. You will see an error message that the GPO is not found. Click **Remove configuration settings**. After completion, the server will be restored to an unconfigured state.

Next steps

- Step 2: Plan DirectAccess Deployments

Step 2 Plan Advanced DirectAccess Deployments

12/9/2022 • 9 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After you plan the DirectAccess infrastructure, the next step in deploying advanced DirectAccess on a single server with IPv4 and IPv6 is to plan the settings for the Remote Access Setup Wizard.

TASK	DESCRIPTION
2.1 Plan for client deployment	Plan how to allow client computers to connect by using DirectAccess. Decide which managed computers will be configured as DirectAccess clients, and plan to deploy the Network Connectivity Assistant or DirectAccess Connectivity Assistant on client computers.
2.2 Plan for DirectAccess server deployment	Plan how to deploy the DirectAccess server.
2.3 Plan infrastructure servers	Plan the infrastructure servers for your DirectAccess deployment, including the DirectAccess network location server, Domain Name System (DNS) servers, and DirectAccess management servers.
2.4 Plan application servers	Plan for IPv4 and IPv6 application servers, and optionally consider whether end-to-end authentication between DirectAccess client computers and internal application servers is required.
2.5 Plan DirectAccess and third-party VPN clients	When deploying DirectAccess with third-party VPN clients, it might be necessary to set a registry value to enable a seamless coexistence of the two remote access solutions.

2.1 Plan for client deployment

There are three decisions to make when you are planning your client deployment:

1. Will DirectAccess be available to mobile computers only, or to any computer?

   When you configure DirectAccess clients in the DirectAccess Client Setup Wizard, you can choose to allow only mobile computers in the specified security groups to connect by using DirectAccess. If you restrict access to mobile computers, Remote Access automatically configures a WMI filter to ensure that the DirectAccess client GPO is applied only to mobile computers in the specified security groups. The Remote Access administrator requires Create or Modify security permissions to create or modify Group Policy Object (GPO) WMI filters to enable this setting.

2. What security groups will contain the DirectAccess client computers?

   DirectAccess client settings are contained in the DirectAccess client GPO. The GPO is applied to computers that are part of the security groups that you specify in the DirectAccess Client Setup Wizard. You can specify that security groups be contained in any supported domain. For more information, see section 1.7 Plan Active Directory Domain Services.

   Before you configure DirectAccess, you should create the security groups. You can add computers to the

security group after you complete the DirectAccess deployment, but if you add client computers that reside in a different domain than the security group, the client GPO will not be applied to those clients. For example, if you created SG1 in domain A for DirectAccess clients, and later add clients from domain B to this group, the client GPO will not be applied to clients from domain B. To avoid this issue, create a new client security group for each domain that contains DirectAccess client computers. Alternatively, if you do not want to create a new security group, run the Windows PowerShell cmdlet **Add-DAClient** with the name of the new GPO for the new domain.

3. What settings will you configure for the network connectivity assistant?

   The network connectivity assistant runs on client computers, and it provides additional information about the DirectAccess connection to end users. In the DirectAccess Client Setup Wizard, you can configure the following:

   - **Connectivity verifiers**

     A default web probe is created that clients use to validate connectivity to the internal network. The default name is:

     https://directaccess-WebProbeHost.<domain_name>

     The name should be registered manually in DNS. You can create other connectivity verifiers by using other web addresses over HTTP or **ping**. For each connectivity verifier, a DNS entry must exist.

   - **A Help Desk email address**

     If end users experience DirectAccess connectivity issues, they can send an email that contains diagnostic information to the DirectAccess administrator to troubleshoot the issue.

   - **A DirectAccess connection name**

     Specify a DirectAccess connection name to help end users identify the DirectAccess connection on their computer.

   - **Allow DirectAccess clients to use local name resolution**

     Clients require a way to resolve names locally. If you allow DirectAccess clients to use local name resolution, end users can use local DNS servers to resolve names. When end users select to use local DNS servers for name resolutions, DirectAccess does not send resolution requests for single label names to the internal corporate DNS server. It uses local name resolution instead (by using the Link-Local Multicast Name Resolution (LLMNR) and NetBIOS over TCP/IP protocols).

2.2 Plan for DirectAccess server deployment

Consider the following decisions when you are planning to deploy your DirectAccess server:

- **Network topology**

  There are a couple of topologies available when deploying a DirectAccess server:

  - **Two network adapters**. With two network adapters, DirectAccess can be configured with one network adapter connected directly to the Internet, and the other connected to the internal network. Alternately, the server is installed behind an edge device such as a firewall or a router. In this configuration, one network adapter is connected to the perimeter network, and the other is connected to the internal network.

  - **One network adapter**. In this configuration, the DirectAccess server is installed behind an edge device such as a firewall or a router. The network adapter is connected to the internal network.

For more information about selecting the topology for your deployment, see 1.1 Plan network topology and settings.

- **ConnectTo address**

  Client computers use the ConnectTo address to connect to the DirectAccess server. The address that you choose must match the subject name of the IP-HTTPS certificate that you deploy for the IP-HTTPS connection, and it must be available in the public DNS.

- **Network adapters**

  The Remote Access Server Setup Wizard automatically detects the network adapters that are configured on the DirectAccess server. You must make sure that the correct adapters are selected.

- **IP-HTTPS certificate**

  The Remote Access Server Setup Wizard automatically detects a certificate that is suitable for the IP-HTTPS connection. The subject name of the certificate that you select must match the ConnectTo address. If you are using self-signed certificates, you can select to use a certificate that is created automatically by the Remote Access server.

- **IPv6 prefixes**

  If the Remote Access Server Setup Wizard detects that IPv6 has been deployed on the network adapters, it automatically populates IPv6 prefixes for the internal network, an IPv6 prefix to assign to DirectAccess client computers, and an IPv6 prefix to assign to VPN client computers. If the automatically generated prefixes are not correct for your native IPv6 infrastructure, you must manually change them. For more information, see 1.1 Plan network topology and settings.

- **Authentication**

  Decide how DirectAccess clients will authenticate to the DirectAccess server:

  - **User authentication**. You can enable users to authenticate with Active Directory credentials or with two-factor authentication. For more information about authenticating with two-factor authentication, see Deploy Remote Access with OTP authentication.
  - **Computer authentication**. You can configure computer authentication to use certificates or to use the DirectAccess server as a Kerberos proxy on behalf of the client. For more information, see 1.3 Plan certificate requirements.
  - **Windows 7 clients**. By default, client computers that are running Windows 7 cannot connect to a Windows Server 2012 R2 or Windows Server 2012 DirectAccess deployment. If you have clients in your organization that are running Windows 7, and they require remote access to internal resources, you can allow them to connect. Any client computers that you want to allow to access internal resources must be a member of a security group that you specify in the DirectAccess Client Setup Wizard.

    > **NOTE**
    >
    > Allowing clients running Windows 7 to connect by using DirectAccess requires that you use computer certificate authentication.

- **VPN configuration**

  Before you configure DirectAccess, decide whether you are going to provide VPN access to non-DirectAccess capable remote clients. You should provide VPN access if you have client computers in your organization that do not support DirectAccess connectivity (because they are unmanaged or because

they run an operating system for which DirectAccess is not supported). The Remote Access Server Setup Wizard allows you to configure how IP addresses are assigned (by using DHCP or from a static address pool) and how VPN clients are authenticated - by using Active Directory or a Remote Authentication Dial-Up Service (RADIUS) server.

2.3 Plan infrastructure servers

DirectAccess requires three types of infrastructure servers:

- **DNS servers**. For more information, see 1.4 Plan DNS requirements
- **Network location server**. For more information, see 1.5 Plan the network location server
- **Management servers**. For more information, see 1.6 Plan management servers

2.4 Plan application servers

Application servers are the servers on the corporate network that are accessible by client computers over a DirectAccess connection. Application servers are identified by adding them into a security group. The application server GPO is then applied to servers in that group.

> **NOTE**
> Adding the application servers to a security group is required only if you require end-to-end authentication and encryption.

You can optionally require end-to-end authentication and encryption between DirectAccess client and selected internal application servers. If you configure end-to-end authentication, DirectAccess clients use an IPsec transport policy. This policy requires that the authentication and traffic protection of IPsec sessions is terminated at the specified application servers. In this case, the Remote Access server forwards the authenticated and protected IPsec sessions to the application servers.

By default, when you extend authentication to application servers, the data payload is encrypted between the DirectAccess client and the application server. You can choose to not encrypt traffic, and use authentication only. However, this is less secure than using authentication and encryption, and it is supported only for application servers running the Windows Server 2008 R2 , or Windows Server 2012 operating systems.

2.5 Plan DirectAccess and third-party VPN clients

Some third-party VPN clients do not create connections in the Network Connections folder. This can cause DirectAccess to determine that it has no intranet connectivity when the VPN connection is established and connectivity to the intranet exists. This occurs when third-party VPN clients register their interfaces by defining them as Network Device Interface Specification (NDIS) endpoint types. You can enable coexistence with these types of VPN clients by setting the following registry value to 1 on DirectAccess clients:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NlaSvc\Parameters\ShowDomainEndpointInterfaces (REG_DWORD)

Some third-party VPN clients use a split-tunneling configuration, which allows the VPN client computer to access the Internet directly, without the need to send the traffic through the VPN connection to the intranet.

Split-tunnel configurations typically leave the default gateway setting on the VPN client as not configured or as all zeros (0.0.0.0). You can confirm this by establishing a successful VPN connection to your intranet and using the Ipconfig.exe command line tool to view the resulting configuration.

If the VPN connection lists its default gateway as empty or all zeros (0.0.0.0), your VPN client is configured in

this way. By default, the DirectAccess client does not identify split-tunnelf configurations. To configure DirectAccess clients to detect these types of VPN client configurations and coexist with them, set the following registry value to 1:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NlaSvc\Parameters\Internet\EnableNoGatewayLocationDetection (REG_DWORD)

Previous step

- Step 1: Plan the DirectAccess Infrastructure

Install and Configure Advanced DirectAccess

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This overview lists the configuration steps required to deploy a single DirectAccess server running Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012 with IPv4 and IPv6.

- Step 1: Configure Advanced DirectAccess Infrastructure.

  In this phase, you configure network and server settings, certificate requirements, Domain Name System (DNS) settings, the network location server deployment, DirectAccess management servers, Active Directory settings, and Group Policy Objects (GPOs).

- Step 2: Configure Advanced DirectAccess Servers.

  In this phase, you configure the DirectAccess client computers, server settings, infrastructure servers, and application servers.

- Step 3: Verify the Advanced DirectAccess Deployment.

  This step describes steps for verifying the deployment.

Before you start your deployment, verify the planning steps that are described in Plan an Advanced DirectAccess Deployment.

Step 1 Configure Advanced DirectAccess Infrastructure

12/9/2022 • 24 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2, Windows Server 2012

This topic describes how to configure the infrastructure that is required for an advanced Remote Access deployment that uses a single DirectAccess server in a mixed IPv4 and IPv6 environment. Before you begin the deployment steps, ensure that you have completed the planning steps that are described in Plan an Advanced DirectAccess Deployment.

TASK	DESCRIPTION
1.1 Configure server network settings	Configure the server network settings on the DirectAccess server.
1.2 Configure force tunneling	Configure force tunneling.
1.3 Configure routing in the corporate network	Configure routing in the corporate network.
1.4 Configure firewalls	Configure additional firewalls, if required.
1.5 Configure CAs and certificates	Configure a certification authority (CA), if required, and any other certificate templates that are required in the deployment.
1.6 Configure the DNS server	Configure the Domain Name System (DNS) settings for the DirectAccess server.
1.7 Configure Active Directory	Join client computers and the DirectAccess server to the Active Directory domain.
1.8 Configure GPOs	Configure GPOs for the deployment, if required.
1.9 Configure security groups	Configure security groups that will contain DirectAccess client computers, and any other security groups that are required in the deployment.
1.10 Configure the network location server	Configure the network location server, including installing the network location server website certificate.

NOTE

This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

1.1 Configure server network settings

The following network interface settings are required for a single server deployment in an environment that is

using IPv4 and IPv6. All IP addresses are configured by using **Change adapter settings** in the **Windows Networking and Sharing Center**.

Edge topology

- Two Internet-facing consecutive public static IPv4 or IPv6 addresses

> **NOTE**
> Two public addresses are required for Teredo. If you are not using Teredo, you can configure a single public static IPv4 address.

- A single internal static IPv4 or IPv6 address

Behind NAT device (with two network adapters)

- A single Internet-facing static IPv4 or IPv6 address
- A single internal network-facing static IPv4 or IPv6 address

Behind NAT device (with one network adapter)

- A single internal network-facing static IPv4 or IPv6 address

> **NOTE**
> If a DirectAccess server with two or more network adapters (one classified in the domain profile and the other in a public or private profile) is configured with a single network adapter topology, we recommend the following:
>
> - Ensure that the second network adapter and any additional network adapters are classified in the domain profile.
> - If the second network adapter cannot be configured for the domain profile, the DirectAccess IPsec policy must be manually scoped to all profiles by using the following Windows PowerShell command after DirectAccess is configured:
>
> ```
> $gposession = Open-NetGPO "PolicyStore <Name of the server GPO>
> Set-NetIPsecRule "DisplayName <Name of the IPsec policy> "GPOSession $gposession "Profile Any
> Save-NetGPO "GPOSession $gposession
> ```

1.2 Configure force tunneling

Force tunneling can be configured through the Remote Access Setup Wizard. It is presented as a check box in the Configure Remote Clients Wizard. This setting only affects DirectAccess clients. If VPN is enabled, VPN clients will by default use force tunneling. Administrators can change the setting for VPN clients from the client profile.

Selecting the check box for force tunneling does the following:

- Enables force tunneling on DirectAccess clients
- Adds an **Any** entry in the Name Resolution Policy Table (NRPT) for DirectAccess clients, which means that all DNS traffic will go to the internal network DNS servers
- Configures DirectAccess clients to always use the IP-HTTPS transition technology

To make Internet resources available to DirectAccess clients that use force tunneling, you can use a proxy server, which can receive IPv6-based requests for Internet resources and translate them to requests for IPv4-based Internet resources. To configure a proxy server for Internet resources, you need to modify the default entry in NRPT to add the proxy server. You can accomplish this by using the Remote Access PowerShell cmdlets or the

DNS PowerShell cmdlets. For example, use the Remote Access PowerShell cmdlet as follows:

```
Set-DAClientDNSConfiguration "DNSSuffix "." "ProxyServer <Name of the proxy server:port>
```

> **NOTE**
> If DirectAccess and VPN are enabled on the same server, and VPN is in force-tunnel mode, and the server is deployed in an edge topology or a behind NAT topology (with two network adapters, one connected to the domain and one to a private network), VPN Internet traffic cannot be forwarded through the external interface of the DirectAccess server. To enable this scenario, organizations must deploy Remote Access on the server behind a firewall in single network adapter topology. Alternatively, organizations can use a separate proxy server in the internal network to forward the Internet traffic from VPN clients.

> **NOTE**
> If an organization is using a web proxy for DirectAccess clients to access Internet resources, and the corporate proxy is not capable of handling internal network resources, DirectAccess clients will not be able to access internal resources if they are outside the intranet. In such a scenario, to enable DirectAccess clients to access internal resources, manually create NRPT entries for the internal network suffixes by using the DNS page of the infrastructure wizard. Do not apply proxy settings on these NRPT suffixes. The suffixes should be populated with default DNS server entries.

1.3 Configure routing in the corporate network

Configure routing in the corporate network as follows:

- When native IPv6 is deployed in the organization, add a route so that the routers on the internal network route IPv6 traffic back through the DirectAccess server.
- Manually configure the organization"s IPv4 and IPv6 routes on the DirectAccess servers. Add a published route so that all traffic with an organization (/48) IPv6 prefix is forwarded to the internal network. For IPv4 traffic, add explicit routes so that IPv4 traffic is forwarded to the internal network.

1.4 Configure firewalls

When using additional firewalls in your deployment, apply the following Internet-facing firewall exceptions for Remote Access traffic when the DirectAccess server is on the IPv4 Internet:

- Teredo traffic"User Datagram Protocol (UDP) destination port 3544 inbound, and UDP source port 3544 outbound.
- 6to4 traffic"IP Protocol 41 inbound and outbound.
- IP-HTTPS"Transmission Control Protocol (TCP) destination port 443, and TCP source port 443 outbound. When the DirectAccess server has a single network adapter, and the network location server is on the DirectAccess server, then TCP port 62000 is also required.

  > **NOTE**
  > This exemption must be configured on the DirectAccess server, while all the other exemptions have to be configured on the edge firewall.

> **NOTE**
> For Teredo and 6to4 traffic, these exceptions should be applied for both of the Internet-facing consecutive public IPv4 addresses on the DirectAccess server. For IP-HTTPS the exceptions need only be applied to the address where the public name of the server resolves.

When using additional firewalls, apply the following Internet-facing firewall exceptions for Remote Access traffic when the DirectAccess server is on the IPv6 Internet:

- IP Protocol 50
- UDP destination port 500 inbound, and UDP source port 500 outbound.
- Internet Control Message Protocol for IPv6 (ICMPv6) traffic inbound and outbound " for Teredo implementations only.

When using additional firewalls, apply the following internal network firewall exceptions for Remote Access traffic:

- ISATAP"Protocol 41 inbound and outbound
- TCP/UDP for all IPv4/IPv6 traffic
- ICMP for all IPv4/IPv6 traffic

1.5 Configure CAs and certificates

Remote Access in Windows Server 2012 allows you to choose between using certificates for computer authentication or using a built in Kerberos proxy that authenticates using user names and passwords. You must also configure an IP-HTTPS certificate on the DirectAccess server.

For more information, see Active Directory Certificate Services.

1.5.1 Configure IPsec authentication

A computer certificate is required on the DirectAccess server and on all DirectAccess clients to use IPsec authentication. The certificate must be issued by an internal certification authority (CA), and DirectAccess servers and DirectAccess clients must trust the CA chain that issues root and intermediate certificates.

To configure IPsec authentication

1. In the internal CA, decide if you will use the **Computer** certificate template, or if you will create a new certificate template as described in Creating Certificate Templates.

   > **NOTE**
   > If you create a new template, it must be configured for Client Authentication.

2. Deploy the certificate template, if required. For more information, see Deploying Certificate Templates.
3. Configure the certificate template for autoenrollment, if required. For more information, see Configure Certificate Autoenrollment.

1.5.2 Configure certificate templates

When you use an internal CA to issue certificates, you must configure a certificate template for the IP-HTTPS certificate and the network location server website certificate.

To configure a certificate template

1. In the internal CA, create a certificate template as described in Creating Certificate Templates.

2. Deploy the certificate template as described in Deploying Certificate Templates.

1.5.3 Configure the IP-HTTPS certificate

Remote Access requires an IP-HTTPS certificate to authenticate IP-HTTPS connections to the DirectAccess server. There are three certificate options that are available for IP-HTTPS authentication:

Public certificate

A public certificate is supplied by a third party. If the certificate subject name does not contain wildcard characters, it must be the externally resolvable fully qualified domain name (FQDN) URL that is used only for the DirectAccess server IP-HTTPS connections.

Private certificate

If you use a private certificate, the following are required, if they do not already exist:

- A website certificate that is used for IP-HTTPS authentication. The certificate subject should be an externally resolvable FQDN that is reachable from the Internet. The certificate is based on the certificate template that you created by following the instructions in 1.5.2 Configure certificate templates.
- A certificate revocation list (CRL) distribution point that is reachable from a publicly resolvable FQDN.

Self-signed certificate

If you use a self-signed certificate, the following are required, if they do not already exist:

- A website certificate that is used for IP-HTTPS authentication. The certificate subject should be an externally resolvable FQDN that is reachable from the Internet.
- A CRL distribution point that is reachable from a publicly resolvable FQDN.

> **NOTE**
> Self-signed certificates cannot be used in multisite deployments.

Make sure that the website certificate that is used for IP-HTTPS authentication meets the following requirements:

- The common name of the certificate should match the name of the IP-HTTPS site.
- In the **Subject** field, specify the FQDN of the IP-HTTPS URL.
- For the **Enhanced Key Usage** field, use the server authentication object identifier (OID).
- For the **CRL Distribution Points** field, specify a CRL distribution point that is accessible by DirectAccess clients that are connected to the Internet.
- The IP-HTTPS certificate must have a private key.
- The IP-HTTPS certificate must be imported directly into the personal store.
- IP-HTTPS certificates can have wildcard characters in the name.

To install the IP-HTTPS certificate from an internal CA

1. On the DirectAccess server: On the **Start** screen, type **mmc.exe**, and then press ENTER.
2. In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Local computer**, click **Finish**, and then click **OK**.

4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
6. Click **Next** twice.
7. On the **Request Certificates** page, select the check box for the certificate template that you previously created (for more information, see 1.5.2 Configure certificate templates). If required, click **More information is required to enroll for this certificate**.
8. In the **Certificate Properties** dialog box, on the **Subject** tab, in the **Subject name** area, in **Type**, select **Common Name**.
9. In **Value**, specify the IPv4 address of the external facing adapter of the DirectAccess server or the FQDN of the IP-HTTPS URL, and then click **Add**.
10. In the **Alternative name** area, in **Type**, select **DNS**.
11. In **Value**, specify the IPv4 address of the external facing adapter of the DirectAccess server or the FQDN of the IP-HTTPS URL, and then click **Add**.
12. On the **General** tab, in **Friendly name**, you can enter a name that will help you identify the certificate.
13. On the **Extensions** tab, click the arrow next to **Extended Key Usage**, and make sure that **Server Authentication** appears in the **Selected options** list.
14. Click **OK**, click **Enroll**, and then click **Finish**.
15. In the details pane of the Certificates snap-in, verify that the new certificate was enrolled with Intended Purposes of Server Authentication.

1.6 Configure the DNS server

You must manually configure a DNS entry for the network location server website for the internal network in your deployment.

To create the network location server

1. On the internal network DNS server: On the **Start** screen, type**dnsmgmt.msc**, and then press ENTER.
2. In the left pane of the **DNS Manager** console, expand the forward lookup zone for your domain. Right click the domain, and click **New Host (A or AAAA)**.
3. In the **New Host** dialog box, In the **IP address** box:
   - In the **Name (uses parent domain name if blank)** box, enter the DNS name for the network location server website (this is the name that the DirectAccess clients use to connect to the network location server).
   - Enter the IPv4 or IPv6 address of the network location server, and then click **Add Host**, and then click **OK**.
4. In the **New Host** dialog box:
   - In the **Name (uses parent domain name if blank)** box, enter the DNS name for the web probe (the name for the default web probe is **directaccess-webprobehost**).
   - In the **IP address** box, enter the IPv4 or IPv6 address of the web probe, and then click **Add Host**.
   - Repeat this process for **directaccess-corpconnectivityhost** and any manually created connectivity verifiers.

5. In the **DNS** dialog box, click **OK**, and then click **Done**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Add-DnsServerResourceRecordA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv4Address
<network_location_server_IPv4_address>
Add-DnsServerResourceRecordAAAA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv6Address
<network_location_server_IPv6_address>
```

You must also configure DNS entries for the following:

- **The IP-HTTPS server**

  DirectAccess clients must be able to resolve the DNS name of the DirectAccess server from the Internet.

- **CRL revocation checking**

  DirectAccess uses certificate revocation checking for the IP-HTTPS connection between DirectAccess clients and the DirectAccess server, and for the HTTPS-based connection between the DirectAccess client and the network location server. In both cases, DirectAccess clients must be able to resolve and access the CRL distribution point location.

- **ISATAP**

  Intrasite Automatic Tunnel Addressing Protocol (ISATAP) uses tunneling to enable DirectAccess clients to connect to the DirectAccess server over the IPv4 Internet, encapsulating IPv6 packets within an IPv4 header. It is used by Remote Access to provide IPv6 connectivity to ISATAP hosts across an intranet. In a non-native IPv6 network environment, the DirectAccess server configures itself automatically as an ISATAP router. Resolution support for the ISATAP name is required.

1.7 Configure Active Directory

The DirectAccess server and all DirectAccess client computers must be joined to an Active Directory domain. DirectAccess client computers must be a member of one of the following domain types:

- Domains that belong in the same forest as the DirectAccess server.
- Domains that belong to forests with a two-way trust with the DirectAccess server forest.
- Domains that have a two-way domain trust to the DirectAccess server domain.

To join the DirectAccess server to a domain

1. In Server Manager, click **Local Server**. In the details pane, click the link next to **Computer name**.
2. In the **System Properties** dialog box, click the **Computer Name** tab, and then click **Change**.
3. In **Computer Name**, type the name of the computer if you are also changing the computer name when joining the server to the domain. Under **Member of**, click **Domain**, and then type the name of the domain to which you want to join the server (for example, corp.contoso.com), and then click **OK**.
4. When you are prompted for a user name and password, enter the user name and password of a user with rights to join computers to the domain, and then click **OK**.
5. When you see a dialog box that welcomes you to the domain, click **OK**.
6. When you are prompted that you must restart the computer, click **OK**.

7. In the **System Properties** dialog box, click **Close**.
8. When you are prompted to restart the computer, click **Restart Now**.

To join client computers to the domain

1. On the **Start** screen, type**explorer.exe**, and then press ENTER.
2. Right-click the Computer icon, and then click **Properties**.
3. On the **System** page, click **Advanced system settings**.
4. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
5. In **Computer name**, type the name of the computer if you are also changing the computer name when joining the server to the domain. Under **Member of**, click **Domain**, and then type the name of the domain to which you want to join the server (for example, corp.contoso.com), and then click **OK**.
6. When you are prompted for a user name and password, enter the user name and password of a user with rights to join computers to the domain, and then click **OK**.
7. When you see a dialog box that welcomes you to the domain, click **OK**.
8. When you are prompted that you must restart the computer, click **OK**.
9. In the **System Properties** dialog box, click **Close**.
10. When you are prompted to restart the computer, click **Restart Now**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

> **NOTE**
> You must supply domain credentials when you enter the following **Add-Computer** command.

```
Add-Computer -DomainName <domain_name>
Restart-Computer
```

1.8 Configure GPOs

A minimum of two Group Policy Objects are required to deploy Remote Access:

- One contains settings for the DirectAccess server
- One contains settings for DirectAccess client computers

When you configure Remote Access, the wizard automatically creates the required Group Policy Objects. However, if your organization enforces a naming convention, you can type a name in the GPO dialog box in the Remote Access Management console. For more information, see 2.7. Configuration summary and alternate GPOs. If you have created permissions, the GPO will be created. If you do not have the required permissions to create GPOs, they must be created prior to configuring Remote Access.

To create Group Policy Objects, see Create and Edit a Group Policy Object.

IMPORTANT

Administrators can manually link the DirectAccess Group Policy Objects to an organizational unit (OU) by following these steps:

1. Before you configure DirectAccess, link the created GPOs to the respective OUs.
2. When you configure DirectAccess, specify a security group for the client computers.
3. The Remote Access administrator may or may not have permissions to link the Group Policy Objects to the domain. In either case, the Group Policy Objects will be configured automatically. If the GPOs are already linked to an OU, the links will not be removed, and the GPOs will not be linked to the domain. For a server GPO, the OU must contain the server computer object, or the GPO will be linked to the root of the domain.
4. If you did not link to the OU before running the DirectAccess Wizard, after the configuration is complete, the domain administrator can link the DirectAccess Group Policy Objects to the required OUs. The link to the domain can be removed. For more information, see Link a Group Policy Object.

NOTE

If a Group Policy Object was created manually, it is possible that the Group Policy Object will not be available during the DirectAccess configuration. The Group Policy Object may not have been replicated to the closest domain controller to the management computer. In this event, the administrator can wait for replication to complete, or force the replication.

1.8.1 Configure Remote Access GPOs with limited permissions

In a deployment that uses staging and production GPOs, the domain administrator should do the following:

1. Obtain the list of required GPOs for the Remote Access deployment from the Remote Access administrator. For more information, see 1.8 Plan Group Policy Objects.

2. For each GPO that is requested by the Remote Access administrator, create a pair of GPOs with different names. The first will be used as the staging GPO, and the second as the production GPO.

   To create Group Policy Objects, see Create and Edit a Group Policy Object.

3. To link the production GPOs, see Link a Group Policy Object.

4. Grant the Remote Access administrator **Edit settings, delete and modify security** permissions on all of the staging GPOs. For more information, see Delegate Permissions for a Group or User on a Group Policy Object.

5. Deny the Remote Access administrator permissions to link GPOs in all domains (or verify that the Remote Access administrator doesn't have such permissions). For more information, see Delegate Permissions to Link Group Policy Objects.

When Remote Access administrators configure Remote Access, they should always specify only the staging GPOs (not the production GPOs). This is true in the initial configuration of Remote Access and when performing additional configuration operations where additional GPOs are required; for example, when adding entry points in a multisite deployment or enabling client computers in additional domains.

After the Remote Access administrator completes any changes to the Remote Access configuration, the domain administrator should review the settings in the staging GPOs, and use the following procedure to copy the settings to the production GPOs.

TIP

Perform the following procedure after each change of the Remote Access configuration.

To copy settings to the production GPOs

1. Verify that all of the staging GPOs in the Remote Access deployment have been replicated to all of the domain controllers in the domain. This is required to ensure the most up-to-date configuration is imported to the production GPOs. For more information, see Check Group Policy Infrastructure Status.

2. Export the settings by backing up all of the staging GPOs in the Remote Access deployment. For more information, see Back Up a Group Policy Object.

3. For each production GPO, change the security filters to match the security filters of the corresponding staging GPO. For more information, see Filter Using Security Groups.

   > **NOTE**
   >
   > This is required because **Import Settings** does not copy the security filter of the source GPO.

4. For each production GPO, import the settings from the backup of the corresponding staging GPO as follows:

   a. In the Group Policy Management Console (GPMC), expand the Group Policy Objects node in the forest and domain that contains the production Group Policy Object into which the settings will be imported.

   b. Right-click the GPO, and click **Import Settings**.

   c. In the **Import Settings Wizard**, on the **Welcome** page, click **Next**.

   d. On the **Backup GPO** page, click **Backup**.

   e. In the **Back up Group Policy Object** dialog box, in the **Location** box, enter the path for the location where you want to store the GPO backups, or click **Browse** to locate the folder.

   f. In the **Description** box, type a description for the production GPO, and then click **Back Up**.

   g. When the backup completes, click **OK**, and then on the **Backup GPO** page, click **Next**.

   h. On the **Backup location** page, in the **Backup folder** box, enter the path for the location in which the backup of the corresponding staging GPO was stored in Step 2, or click **Browse** to locate the folder, and then click **Next**.

   i. On the **Source GPO** page, select the **Show only the latest version of each GPO** check box to hide older backups, and select the corresponding staging GPO. Click **View Settings** to review the Remote Access settings before applying them to the production GPO, and then click **Next**.

   j. On the **Scanning Backup** page, click **Next**, and then click **Finish**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

- To back up the staging client GPO "DirectAccess Client Settings - Staging" in domain "corp.contoso.com" to the backup folder "C:\Backups":

  ```
  $backup = Backup-GPO "Name 'DirectAccess Client Settings - Staging' "Domain 'corp.contoso.com' "Path
  'C:\Backups\'
  ```

- To see the security filtering of the staging client GPO "DirectAccess Client Settings - Staging" in domain

"corp.contoso.com":

```
Get-GPPermission "Name 'DirectAccess Client Settings - Staging' "Domain 'corp.contoso.com' "All | ?{
$_.Permission "eq 'GpoApply'}
```

- To add the security group "corp.contoso.com\DirectAccess clients" to the security filter of the production client GPO "DirectAccess Client Settings " Production" in domain "corp.contoso.com":

```
Set-GPPermission "Name 'DirectAccess Client Settings - Production' "Domain 'corp.contoso.com'
"PermissionLevel GpoApply "TargetName 'corp.contoso.com\DirectAccess clients' "TargetType Group
```

- To import settings from the backup to the production client GPO "DirectAccess Client Settings " Production" in domain "corp.contoso.com":

```
Import-GPO "BackupId $backup.Id "Path $backup.BackupDirectory "TargetName 'DirectAccess Client
Settings - Production' "Domain 'corp.contoso.com'
```

1.9 Configure security groups

The DirectAccess settings that are contained in the client computer Group Policy Object are applied only to computers that are members of the security groups that you specify when you configure Remote Access. In addition, if you are using security groups to manage your application servers, create a security group for these servers.

To create a security group for DirectAccess clients

1. On the **Start** screen, type**dsa.msc**, and then press ENTER. In the **Active Directory Users and Computers** console, in the left pane, expand the domain that will contain the security group, right-click **Users**, point to **New**, and then click **Group**.
2. In the **New Object - Group** dialog box, under **Group name**, enter the name for the security group.
3. Under **Group scope**, click **Global**, and under **Group type**, click **Security**, and then click **OK**.
4. Double-click the DirectAccess client computers security group, and in the properties dialog box, click the **Members** tab.
5. On the **Members** tab, click **Add**.
6. In the **Select Users, Contacts, Computers, or Service Accounts** dialog box, select the client computers that you want to enable for DirectAccess, and then click **OK**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
New-ADGroup -GroupScope global -Name <DirectAccess_clients_group_name>
Add-ADGroupMember -Identity DirectAccess_clients_group_name -Members <computer_name>
```

1.10 Configure the network location server

The network location server should be a server with high availability, and it should have a valid SSL certificate that is trusted by the DirectAccess clients. There are two certificate options for the network location server

certificate:

- **Private certificate**

  This certificate is based on the certificate template that you created by following the instructions in 1.5.2 Configure certificate templates.

- **Self-signed certificate**

> **NOTE**
> Self-signed certificates cannot be used in multisite deployments.

The following are required for either type of certificate, if they do not already exist:

- A website certificate that is used for the network location server. The certificate subject should be the URL of the network location server.
- A CRL distribution point that has high availability from the internal network.

> **NOTE**
> If the network location server website is located on the DirectAccess server, a website is created automatically when you configure Remote Access. This site is bound to the server certificate that you provide.

To install the network location server certificate from an internal CA

1. On the server that will host the network location server website: On the **Start** screen, type**mmc.exe**, and then press ENTER.
2. In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
6. Click **Next** twice.
7. On the **Request Certificates** page, select the check box for the certificate template that you created by following the instructions in 1.5.2 Configure certificate templates. If required, click **More information is required to enroll for this certificate**.
8. In the **Certificate Properties** dialog box, on the **Subject** tab, in the **Subject name** area, in **Type**, select **Common Name**.
9. In **Value**, enter the FQDN of the network location server website, and then click **Add**.
10. In the **Alternative name** area, in **Type**, select **DNS**.
11. In **Value**, enter the FQDN of the network location server website, and then click **Add**.
12. On the **General** tab, in **Friendly name**, you can enter a name that will help you identify the certificate.
13. Click **OK**, click **Enroll**, and then click **Finish**.
14. In the details pane of the Certificates snap-in, verify that new certificate was enrolled with Intended Purposes of Server Authentication.

To configure the network location server

1. Set up a website on a high availability server. The website does not require any content, but when you test it, you might define a default page that provides a message when clients connect.

   > **NOTE**
   >
   > This step is not required if the network location server website is hosted on the DirectAccess server.

2. Bind an HTTPS server certificate to the website. The common name of the certificate should match the name of the network location server site. Ensure that DirectAccess clients trust the issuing CA.

   > **NOTE**
   >
   > This step is not required if the network location server website is hosted on the DirectAccess server.

3. Set up a CRL site that has high availability from the internal network.

   CRL distribution points can be accessed through:

   - Web servers by using an HTTP-based URL, such as: https://crl.corp.contoso.com/crld/corp-APP1-CA.crl
   - File servers that are accessed through a universal naming convention (UNC) path, such as \\crl.corp.contoso.com\crld\corp-APP1-CA.crl

   If the internal CRL distribution point is reachable only over IPv6, you must configure a Windows Firewall with Advanced Security connection security rule to exempt IPsec protection from the IPv6 address of your intranet to the IPv6 addresses of your CRL distribution points.

4. Ensure that DirectAccess clients on the internal network can resolve the name of the network location server. Ensure that the name is not resolvable by DirectAccess clients on the Internet.

Next step

- Step 2: Configure Advanced DirectAccess Servers

Step 2 Configure Advanced DirectAccess Servers

12/9/2022 • 11 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to configure the client and server settings that are required for an advanced Remote Access deployment that uses a single Remote Access server in a mixed IPv4 and IPv6 environment. Before you begin the deployment steps, ensure that you have completed the planning steps that are described in Plan an Advanced DirectAccess Deployment.

TASK	DESCRIPTION
2.1. Install the Remote Access role	Install the Remote Access role.
2.2. Configure the deployment type	Configure the deployment type as DirectAccess and VPN, DirectAccess only, or VPN only.
Plan an Advanced DirectAccess Deployment	Configure the Remote Access server with the security groups that contain DirectAccess clients.
2.4. Configure the Remote Access server	Configure Remote Access server settings.
2.5. Configure the infrastructure servers	Configure the infrastructure servers that are used in the organization.
2.6. Configure application servers	Configure application servers so that they require authentication and encryption.
2.7. Configuration summary and alternate GPOs	View the Remote Access configuration summary, and modify the GPOs if desired.
2.8. How to configure the Remote Access server using Windows PowerShell	Configure Remote Access by using Windows PowerShell.

NOTE

This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

2.1. Install the Remote Access role

To deploy Remote Access, you must install the Remote Access role on a server in your organization that will act as the Remote Access server.

To install the Remote Access role

1. On the Remote Access server, in the Server Manager console, in the **Dashboard**, click **Add roles and features**.
2. Click **Next** three times to get to the **Select server roles** screen.
3. On the **Select server roles** page, select **Remote Access**, click **Add Features**, and then click **Next**.

4. Click **Next** five times.

5. On the **Confirm installation selections** page, click **Install**.

6. On the **Installation progress** page, verify that the installation was successful, and then click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

2.2. Configure the deployment type

Remote Access can be deployed by using the Remote Access Management console in three ways:

- DirectAccess and VPN
- DirectAccess only
- VPN only

This guide uses a DirectAccess-only deployment in the example procedures.

To configure the deployment type

1. On the Remote Access server, open the Remote Access Management console: On the **Start** screen, type**RAMgmtUI.exe**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.

2. In the Remote Access Management Console, in the middle pane, click **Run the Remote Access Setup Wizard**.

3. In the **Configure Remote Access** dialog box, click the whether to deploy DirectAccess and VPN, DirectAccess only, or VPN only.

2.3. Configure DirectAccess clients

For a client computer to be provisioned to use DirectAccess, it must belong to the selected security group. After DirectAccess is configured, client computers in the security group are provisioned to receive the DirectAccess Group Policy Object (GPO). You can also configure the deployment scenario, which allows you to configure DirectAccess for client access and remote management, or for remote management only.

To configure DirectAccess clients

1. In the middle pane of the Remote Access Management console, in the **Step 1 Remote Clients** area, click **Configure**.

2. In the DirectAccess Client Setup Wizard, on the **Deployment Scenario** page, click the deployment scenario that you want to use in your organization (**Full DirectAccess** or **Remote management only**) , and then click **Next**.

3. On the **Select Groups** page, click **Add**.

4. In the **Select Groups** dialog box, select the security groups that contain your DirectAccess client computers.

> **NOTE**
> If the security group is located in a different forest than the Remote Access server, after you complete the Remote Access Setup Wizard, click **Refresh Management Servers** in the **Tasks** pane to discover the domain controllers and Configuration Manager servers in the new forest.

5. Select the **Enable DirectAccess for mobile computers only** check box to allow only mobile computers to access the internal network, if required.
6. Select the **Use force tunneling** check box to route all client traffic (to the internal network and to the Internet) through the Remote Access server, if required.
7. Click **Next**.
8. On the **Network Connectivity Assistant** page:
   - In the table, add resources that will be used to determine connectivity to the internal network. A default web probe is created automatically if no other resources are configured.

     > **Caution**
     > When you configure the web probe locations for determining connectivity to the Enterprise network, ensure that you have at least one HTTP-based probe configured. Configuring a **ping** probe only is not sufficient, and this could lead to inaccurate determination of connectivity status. This is because **ping** is exempt from IPsec, and as a result, it does not ensure that the IPsec tunnels are properly established.

   - Add a Help Desk email address to allow users to send information if they experience connectivity issues.
   - Provide a friendly name for the DirectAccess connection. This name appears in the network list when users click the network icon in the notification area.
   - Select the **Allow DirectAccess clients to use local name resolution** check box, if required.

     > **NOTE**
     > When local name resolution is enabled, users who run the Network Connectivity Assistant can select to resolve names by using DNS servers that are configured on the DirectAccess client computer.

9. Click **Finish**.

2.4. Configure the Remote Access server

To deploy Remote Access, you need to configure the Remote Access server with the correct network adapters, a public URL for the Remote Access server to which client computers can connect (the ConnectTo address), an IP-HTTPS certificate with a subject that matches the ConnectTo address, IPv6 settings, and client computer authentication.

To configure the Remote Access server

1. In the middle pane of the Remote Access Management console, in the **Step 2 Remote Access Server** area, click **Configure**.
2. In the Remote Access Server Setup Wizard, on the **Network Topology** page, click the deployment topology that will be used in your organization. In **Type the public name or IPv4 address used by clients to connect to the Remote Access server**, enter the public name for the deployment (this name matches the subject name of the IP-HTTPS certificate, for example, edge1.contoso.com), and then

click **Next**.

3. On the **Network Adapters** page, the wizard automatically detects the network adapters for the networks in your deployment. If the wizard does not detect the correct network adapters, manually select the correct adapters. The wizard also automatically detects the IP-HTTPS certificate, based on the public name for the deployment set in the previous step of the wizard. If the wizard does not detect the correct IP-HTTPS certificate, click **Browse** to manually select the correct certificate, and then click **Next**.

4. On the **Prefix Configuration** page (this appears only if IPv6 is deployed in the internal network), the wizard automatically detects the IPv6 settings that are used in the internal network. If your deployment requires additional prefixes, configure the IPv6 prefixes for the internal network, an IPv6 prefix to assign to DirectAccess client computers, and an IPv6 prefix to assign to VPN client computers.

   > **NOTE**
   > You can specify multiple internal IPv6 prefixes by using a semicolon delimited list, for example, 2001:db8:1::/48;2001:db8:2::/48.

5. On the **Authentication** page:

   - In **User Authentication**, click **Active Directory credentials**. To configure a deployment by using two-factor authentication, click **Two-factor authentication**. For more information, see Deploy Remote Access with OTP authentication.
   - For multisite and two-factor authentication deployments, you must use computer certificate authentication. Select the **Use computer certificates** check box to use computer certificate authentication, and select the IPsec root certificate.
   - To enable Windows 7 client computers to connect through DirectAccess, select the **Enable Windows 7 client computers to connect via DirectAccess** check box.

     > **NOTE**
     > You must also use computer certificate authentication in this type of deployment.

6. Click **Finish**.

2.5. Configure the infrastructure servers

To configure the infrastructure servers in a Remote Access deployment, you must configure the network location server, DNS settings (including the DNS suffix search list), and management servers that are not automatically detected by Remote Access.

To configure the infrastructure servers

1. In the middle pane of the Remote Access Management console, in the **Step 3 Infrastructure Servers** area, click **Configure**.

2. In the Infrastructure Server Setup Wizard, on the **Network Location Server** page, click the option that corresponds to the location of the network location server in your deployment. If the network location server is on a remote web server, enter the URL and click **Validate** before you continue. If the network location server is on the Remote Access server, click **Browse** to locate the relevant certificate, and then click **Next**.

3. On the **DNS** page, in the table, enter any additional name suffixes that will be applied as Name Resolution Policy Table (NRPT) exemptions. Select a local name resolution option, and then click **Next**.

4. On the **DNS Suffix Search List** page, the Remote Access server automatically detects any domain suffixes in the deployment. Use the **Add** and **Remove** buttons to add and remove domain suffixes from the list of domain suffixes to use. To add a new domain suffix, in **New Suffix**, enter the suffix, and then click **Add**. Click **Next**.

5. On the **Management** page, add any management servers that are not detected automatically, and then click **Next**. Remote Access automatically adds domain controllers and Configuration Manager servers.

   > **NOTE**
   > Although the servers are added automatically, they don't appear in the list. After you apply the configuration the first time, the Configuration Manager servers appear in the list.

6. Click **Finish**.

2.6. Configure application servers

In a Remote Access deployment, configuring application servers is an optional task. Remote Access enables you to require authentication for selected application servers, which is determined by their inclusion in an application servers security group. By default, traffic to application servers that require authentication is also encrypted; however, you can choose to not encrypt traffic to application servers and use authentication only.

> **NOTE**
> Authentication without encryption is supported only on application servers running Windows Server 2012 R2 , Windows Server 2012 , or Windows Server 2008 R2 .

To configure application servers

1. In the middle pane of the Remote Access Management console, in the **Step 4 Application Servers** area, click **Configure**.

2. In the DirectAccess Application Server Setup Wizard, to require authentication to selected application servers, click **Extend authentication to selected application servers**. Click **Add** to select the application server security group.

3. To limit access to only the servers in the application server security group, select the **Allow access only to servers included in the security groups** check box.

4. To use authentication without encryption, select the **Do not encrypt traffic. Use authentication only** check box.

5. Click **Finish**.

2.7. Configuration summary and alternate GPOs

When the Remote Access configuration is complete, the **Remote Access Review** is displayed. You can review all of the settings that you previously selected, including:

1. **GPO Settings**: The DirectAccess server GPO name and client GPO name are listed. Additionally, you can click the **Change** link next to the **GPO Settings** heading to modify the GPO settings.

2. **Remote Clients**: The DirectAccess client configuration is displayed, including the security group, force tunneling status, connectivity verifiers, and DirectAccess connection name.

3. **Remote Access Server**: The DirectAccess configuration is displayed including the public name/address, network adapter configuration, certificate information, and OTP information if configured.

4. **Infrastructure Servers**: This list includes the network location server URL, DNS suffixes that are used by DirectAccess clients, and management server information.

5. **Application Servers**: The DirectAccess remote management status is displayed, in addition to the status of the end-to-end authentication to specific application servers.

2.8. How to configure the Remote Access server by using Windows PowerShell

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

To perform a full installation in an edge topology of Remote Access for DirectAccess only in a domain with the root **corp.contoso.com** and using the following parameters: server GPO: **DirectAccess Server Settings**, client GPO: DirectAccess Client Settings, internal network adapter: **Corpnet**, external network adapter: **Internet**, ConnectTto address: **edge1.contoso.com**, and network location server: **nls.corp.contoso.com**:

```
Install-RemoteAccess -Force -PassThru -ServerGpoName 'corp.contoso.com\DirectAccess Server Settings' -
ClientGpoName 'corp.contoso.com\DirectAccess Client Settings' -DAInstallType 'FullInstall' -
InternetInterface 'Internet' -InternalInterface 'Corpnet' -ConnectToAddress 'edge1.contoso.com' -NlsUrl
'https://nls.corp.contoso.com/'
```

To configure the Remote Access server to use computer certificate authentication, with an IPsec root certificate that is issued by the certification authority named CORP-APP1-CA:

```
$certs = Get-ChildItem Cert:\LocalMachine\Root
$IPsecRootCert = $certs | Where-Object {$_.Subject -Match "corp-APP1-CA"}
Set-DAServer -IPsecRootCertificate $IPsecRootCert
```

To add the security group that contains DirectAccess clients named **DirectAccessClients**, and to remove the default Domain Computers security group:

```
Add-DAClient -SecurityGroupNameList @('corp.contoso.com\DirectAccessClients')
Remove-DAClient -SecurityGroupNameList @('corp.contoso.com\Domain Computers')
```

To enable Remote Access for all computers (not only notebooks and laptops), and to enable Remote Access for Windows 7 clients:

```
Set-DAClient -OnlyRemoteComputers 'Disabled' -Downlevel 'Enabled'
```

To configure the DirectAccess client experience, including the friendly connection name and the web probe URL:

```
Set-DAClientExperienceConfiguration -FriendlyName 'Contoso DirectAccess Connection' -PreferLocalNamesAllowed
$False -PolicyStore 'corp.contoso.com\DirectAccess Client Settings' -CorporateResources
@('HTTP:https://directaccess-WebProbeHost.corp.contoso.com')
```

Previous step

- Step 1: Configure Advanced DirectAccess Infrastructure

Next step

- Step 3: Verify the Deployment

Step 3 Verify the Advanced DirectAccess Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to verify that you have correctly configured your DirectAccess deployment.

To verify access to internal resources through DirectAccess

1. Connect a DirectAccess client computer to the corporate network and obtain the Group Policy Object.
2. Click the **Network connections** icon in the notification area to access the DirectAccess Media Manager.
3. Click **DirectAccess Connection**, and you will see that the status is **Connected Locally**.
4. Connect the client computer to the external network and attempt to access internal resources.

   You should be able to access all corporate resources.

Previous step

- Step 2: Configuring DirectAccess Servers

Add DirectAccess to an Existing Remote Access (VPN) Deployment

12/9/2022 • 6 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Scenario description

In this scenario, a single computer running Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 is configured as a DirectAccess server with recommended settings after you have already installed and configured VPN. If you want to configure DirectAccess with enterprise features, such as a load-balanced cluster, multisite deployment, or two-factor client authentication, complete the scenario described in this topic to set up a single server, and then set up the enterprise scenario as described in Deploy Remote Access in an enterprise.

In this scenario

To set up a single Remote Access server, a number of planning and deployment steps are required.

Planning steps

Planning is divided into two phases:

1. **Plan the Remote Access infrastructure**

   In this phase, you describe the planning that is required to set up the network infrastructure before you begin the Remote Access deployment. It includes planning for the network and server topology, certificates, Domain Name System (DNS), Active Directory and Group Policy Object (GPO) configuration, and the DirectAccess network location server.

2. **Plan the Remote Access deployment**

   In this phase, you describe the planning steps that are required to prepare for the Remote Access deployment. It includes planning for Remote Access client computers, server and client authentication requirements, and infrastructure servers.

Deployment steps

Deployment is divided into three phases:

1. **Configure the Remote Access infrastructure**

   In this phase, you configure the network and routing, firewall settings (if required), certificates, DNS servers, Active Directory and GPO settings, and the DirectAccess network location server.

2. **Configure Remote Access server settings**

   In this phase, you configure the Remote Access client computers, the Remote Access server, and the infrastructure servers.

3. **Verify the deployment**

   In this phase, you verify that the deployment is working as required.

Practical applications

Deploying a single Remote Access server provides the following:

- **Ease of access**

  Managed client computers running Windows 8 and Windows 7 can be configured as DirectAccess client computers. These clients can access internal network resources through DirectAccess any time they are located on the Internet, without the need to sign in to a VPN connection. Client computers that are not running one of these operating systems can connect to the internal network through a VPN. DirectAccess and VPN are managed in the same console and with the same set of wizards.

- **Ease of management**

  DirectAccess client computers that have access to the Internet can be remotely managed by remote access administrators by using DirectAccess, even when the client computers are not located on the internal corporate network. Client computers that do not meet corporate requirements can be remediated automatically by management servers.

Roles and features required for this scenario

The following table lists the roles and features that are required for this scenario:

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access role	The role is installed and uninstalled by using the Server Manager console or Windows PowerShell. This role encompasses DirectAccess, which was previously a feature in Windows Server 2008 R2, and Routing and Remote Access Services, which was previously a role service under the Network Policy and Access Services (NPAS) server role. The Remote Access role consists of two components: 1. DirectAccess and Routing and Remote Access Services (RRAS) VPN: Managed in the Remote Access Management console. 2. RRAS Routing: Managed in the Routing and Remote Access console. The Remote Access Server role is dependent on the following server features: - Internet Information Services (IIS) Web Server:Required to configure the network location server on the Remote Access server, and the default web probe. - Windows Internal Database: Used for local accounting on the Remote Access server.

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access Management Tools feature	This feature is installed as follows: - By default on a Remote Access server when the Remote Access role is installed. Supports the Remote Management console user interface and the Windows PowerShell cmdlets. - Optionally installed on a server not running the Remote Access server role. In this case, it is used for remote management of a Remote Access computer running DirectAccess and VPN. The Remote Access Management Tools feature consists of the following: - Remote Access GUI - Remote Access module for Windows PowerShell Dependencies include: - Group Policy Management Console - RAS Connection Manager Administration Kit (CMAK) - Windows PowerShell 3.0 - Graphical Management Tools and Infrastructure

Hardware requirements

Hardware requirements for this scenario include the following:

Server requirements

- A computer that meets the hardware requirements for Windows Server 2012 .
- The server must have at least one network adapter installed, enabled, and joined to the internal network. When two adapters are used, there should be one adapter connected to the internal corporate network, and one connected to the external network (Internet).
- If Teredo is required as an IPv4 to IPv6 transition protocol, the external adapter of the server requires two consecutive public IPv4 addresses. The Enable DirectAccess Wizard does not enable Teredo, even if two consecutive IP addresses are present. If a single IP address is available, only IP-HTTPS can be used as the transition protocol.
- At least one domain controller. The Remote Access server and DirectAccess clients must be domain members.
- The Enable DirectAccess Wizard requires certificates for IP-HTTPS and the network location server. If the SSTP VPN is already using a certificate, it is reused for IP-HTTPS. If the SSTP VPN is not configured, you can configure a certificate for IP-HTTPS or use an automatically created self-signed certificate. For the network location server, you can configure a certificate or use an automatically created self-signed certificate.

Client requirements

- A client computer must be running Windows 8 or Windows 7.

> **NOTE**
>
> Only the following operating systems can be used as DirectAccess clients: Windows Server 2012, Windows Server 2008 R2, Windows 8 Enterprise, Windows 7 Enterprise, and Windows 7 Ultimate.

Infrastructure and management server requirements

- During the remote management of DirectAccess client computers, clients initiate communication with management servers, such as domain controllers, System Center configuration servers, and Health Registration Authority (HRA) servers for services that include Windows and antivirus updates and Network Access Protection (NAP) client compliance. The required servers should be deployed before you begin the Remote Access deployment.
- If remote access requires client NAP compliance, the Network Policy Server (NPS) and the HRA should be deployed before you begin the Remote Access deployment.
- A DNS server running Windows Server 2012 , Windows Server 2008 R2, or Windows Server 2008 with SP2 is required.

Software requirements

Software requirements for this scenario include the following:

Server requirements

- The Remote Access server must be a domain member. The server can be deployed at the edge of the internal network, or behind an edge firewall or other device.
- If the Remote Access server is located behind an edge firewall or network address translation (NAT) device, the device must be configured to allow traffic to and from the Remote Access server.
- The person who deploys remote access on the server requires local administrator permissions on the server, and domain user permissions. In addition, the administrator requires permissions for the GPOs that are used in DirectAccess deployment. To take advantage of the features that restrict a DirectAccess deployment to mobile computers only, permissions to create a WMI filter on the domain controller are required.

Remote access client requirements

- DirectAccess clients must be domain members. Domains that contain clients can belong to the same forest as the Remote Access server, or they can have a two-way trust with the Remote Access server forest or domain.
- An Active Directory security group is required to contain the computers that will be configured as DirectAccess clients. If a security group is not specified when you configure DirectAccess client settings, by default, the client GPO is applied on all laptop computers (that are DirectAccess capable) in the Domain Computers security group. Only the following operating systems can be used as DirectAccess clients: Windows Server 2012 , Windows Server 2008 R2 , Windows 8 Enterprise, Windows 7 Enterprise, and Windows 7 Ultimate.

> **NOTE**
>
> We recommend that you create a security group for each domain that contains computers that will be configured as DirectAccess clients.

Plan to Enable DirectAccess

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Note: Windows Server 2012 combines DirectAccess and Remote Access Service (RAS) into a single Remote Access role. This section describes the planning steps that are required to deploy a single Remote Access server running Windows Server 2016 with basic features.

The planning phase includes the following steps:

- Step 1: Plan DirectAccess infrastructure

  In this phase, you describe the planning that is required to set up the network infrastructure before you begin the Remote Access deployment. It includes planning for the network and server topology, certificates, Domain Name System (DNS), Active Directory and Group Policy Object (GPO) configuration, and the DirectAccess network location server.

- Step 2: Plan DirectAccess deployment

  In this phase, you describe the planning steps that are required to prepare for the Remote Access deployment. It includes planning for Remote Access client computers, server and client authentication requirements, and infrastructure servers.

Step 1 Plan DirectAccess Infrastructure

12/9/2022 • 18 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first step of planning for a basic Remote Access deployment on a single server is to perform planning for the infrastructure required for the deployment. This topic describes the infrastructure planning steps:

TASK	DESCRIPTION
Plan network topology and settings	Decide where to place the Remote Access server (at the edge, or behind a Network Address Translation (NAT) device or firewall), and plan IP addressing and routing.
Plan firewall requirements	Plan for allowing Remote Access through edge firewalls.
Plan certificate requirements	Remote Access can use Kerberos or certificates for client authentication. In this basic Remote Access deployment, Kerberos is automatically configured and authentication is accomplished using a self-signed certificate issued automatically by the Remote Access server.
Plan DNS requirements	Plan DNS settings for the Remote Access server, infrastructure servers, local name resolution options, and client connectivity.
Plan Active Directory	Plan your domain controllers and Active Directory requirements.
Plan Group Policy Objects	Decide what GPOs are required in your organization and how to create or edit the GPOs.

The planning tasks do not need to be done in a specific order.

Plan network topology and settings

Plan network adapters and IP addressing

1. Identify the network adapter topology you want to use. Remote Access can be set up with either of the following:

   - With two network adapters: Either at the edge with one network adapter connected to the Internet and the other to the internal network, or behind a NAT, firewall, or router device, with one network adapter connected to a perimeter network and the other to the internal network.

   - Behind a NAT device with one network adapter: The Remote Access server is installed behind a NAT device, and the single network adapter is connected to the internal network.

2. Identity your IP addressing requirements:

   DirectAccess uses IPv6 with IPsec to create a secure connection between DirectAccess client computers and the internal corporate network. However, DirectAccess does not necessarily require connectivity to the IPv6 Internet or native IPv6 support on internal networks. Instead, it automatically configures and

uses IPv6 transition technologies to tunnel IPv6 traffic across the IPv4 Internet (6to4, Teredo, IP-HTTPS) and across your IPv4-only intranet (NAT64 or ISATAP). For an overview of these transition technologies, see the following resources:

- IPv6 Transition Technologies
- IP-HTTPS Tunneling Protocol Specification

3. Configure required adapters and addressing according to the following table. For deployments behind a NAT device using a single network adapter, configure your IP addresses using only the 'Internal network adapter' column.

IP ADDRESS TYPE	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv4 intranet and IPv4 Internet	Configure the following: - One static public IPv4 address with the appropriate subnet masks. - A default gateway IPv4 address of your Internet firewall or local Internet service provider (ISP) router.	Configure the following: - An IPv4 intranet address with the appropriate subnet mask. - A connection-specific DNS suffix of your intranet namespace. The DNS Server must also be configured on the Internal interface. - Do not configure a default gateway on any intranet interfaces.	To configure the Remote Access server to reach all subnets on the internal IPv4 network do the following: 1. List the IPv4 address spaces for all the locations on your intranet. 2. Use the **route add -p** or **netsh interface ipv4 add route** commands to add the IPv4 address spaces as static routes in the IPv4 routing table of the Remote Access server.

IP ADDRESS TYPE	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv6 Internet and IPv6 intranet	Configure the following: - Use the autoconfigured address configuration provided by your ISP. - Use the **route print** command to ensure that a default IPv6 route pointing to the ISP router exists in the IPv6 routing table. - Determine whether the ISP and intranet routers are using default router preferences described in RFC 4191, and using a higher default preference than your local intranet routers. If both of these are true, no other configuration for the default route is required. The higher preference for the ISP router ensures that the active default IPv6 route of the Remote Access server points to the IPv6 Internet. Because the Remote Access server is an IPv6 router, if you have a native IPv6 infrastructure, the Internet interface can also reach the domain controllers on the intranet. In this case, add packet filters to the domain controller in the perimeter network that prevent connectivity to the IPv6 address of the Internet-facing interface of the Remote Access server.	Configure the following: - If you are not using default preference levels, configure your intranet interfaces with the **netsh interface ipv6 set InterfaceIndex ignoredefaultroutes=enabled** command. This command ensures that additional default routes pointing to intranet routers will not be added to the IPv6 routing table. You can obtain the InterfaceIndex of your intranet interfaces from the display of the netsh interface show interface command.	If you have an IPv6 intranet, to configure the Remote Access server to reach all of the IPv6 locations, do the following: 1. List the IPv6 address spaces for all the locations on your intranet. 2. Use the **netsh interface ipv6 add route** command to add the IPv6 address spaces as static routes in the IPv6 routing table of the Remote Access server.

IP ADDRESS TYPE	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv6 Internet and IPv4 intranet	The Remote Access server forwards default IPv6 route traffic using the Microsoft 6to4 Adapter interface to a 6to4 relay on the IPv4 Internet. You can configure a Remote Access server for the IPv4 address of the Microsoft 6to4 relay on the IPv4 Internet (used when native IPv6 is not deployed in the corporate network) with the following command : netsh interface ipv6 6to4 set relay name=192.88.99.1 state=enabled command.		

NOTE

1. If the DirectAccess client has been assigned a public IPv4 address, it will use the 6to4 transition technology to connect to the intranet. If the DirectAccess client cannot connect to the DirectAccess server with 6to4, it will use IP-HTTPS.
2. Native IPv6 client computers can connect to the Remote Access server over native IPv6, and no transition technology is required.

Plan firewall requirements

If the Remote Access server is behind an edge firewall, the following exceptions will be required for Remote Access traffic when the Remote Access server is on the IPv4 Internet:

- 6to4 traffic -IP Protocol 41 inbound and outbound.
- IP-HTTPS -Transmission Control Protocol (TCP) destination port 443, and TCP source port 443 outbound.
- If you are deploying Remote Access with a single network adapter, and installing the network location server on the Remote Access server, TCP port 62000 should also be exempted.

The following exceptions will be required for Remote Access traffic when the Remote Access server is on the IPv6 Internet:

- IP Protocol 50
- UDP destination port 500 inbound, and UDP source port 500 outbound.

When using additional firewalls, apply the following internal network firewall exceptions for Remote Access traffic:

- ISATAP -Protocol 41 inbound and outbound
- TCP/UDP for all IPv4/IPv6 traffic

Plan certificate requirements

Certificate requirements for IPsec include a computer certificate used by DirectAccess client computers when establishing the IPsec connection between the client and the Remote Access server, and a computer certificate used by Remote Access servers to establish IPsec connections with DirectAccess clients. For DirectAccess in

Windows Server 2012 the use of these IPsec certificates is not mandatory. The Enable DirectAccess Wizard configures the Remote Access server to act as a Kerberos proxy to perform IPsec authentication without requiring certificates.

1. **IP-HTTPS server**: When you configure Remote Access, the Remote Access server is automatically configured to act as the IP-HTTPS web listener. The IP-HTTPS site requires a website certificate, and client computers must be able to contact the certificate revocation list (CRL) site for the certificate. The Enable DirectAccess wizard tries to use the SSTP VPN certificate. If SSTP is not configured, it checks if a certificate for IP-HTTPS is present in the machine personal store. If none is available, it automatically creates a self-signed certificate.
2. **Network location server**: The network location server is a website used to detect whether client computers are located in the corporate network. The network location server requires a website certificate. DirectAccess clients must be able to contact the CRL site for the certificate. The Enable DirectAccess wizard checks if a certificate for Network Location Server is present in the machine personal store. If not present, it automatically creates a self-signed certificate.

The certification requirements for each of these are summarized in the following table:

IPSEC AUTHENTICATION	IP-HTTPS SERVER	NETWORK LOCATION SERVER
An internal CA is required to issue computer certificates to the Remote Access server and clients for IPsec authentication when you don't use the Kerberos proxy for authentication	Public CA: We recommend using a public CA to issue the IP-HTTPS certificate, this ensures that the CRL distribution point is available externally.	Internal CA: You can use an internal CA to issue the network location server website certificate. Make sure that the CRL distribution point is highly available from the internal network.
	Internal CA: You can use an internal CA to issue the IP-HTTPS certificate; however, you must make sure that the CRL distribution point is available externally.	Self-signed certificate: You can use a self-signed certificate for the network location server website; however, you cannot use a self-signed certificate in multisite deployments.
	Self-signed certificate: You can use a self-signed certificate for the IP-HTTPS server; however, you must make sure that the CRL distribution point is available externally. A self-signed certificate cannot be used in a multisite deployment.	

Plan certificates for IP-HTTPS

The Remote Access server acts as an IP-HTTPS listener, and you must manually install an HTTPS website certificate on the server. Note the following when planning:

- Using a public CA is recommended, so that CRLs are readily available.
- In the subject field, specify either the IPv4 address of the Internet adapter of Remote Access server, or the FQDN of the IP-HTTPS URL (the ConnectTo address). If the Remote Access server is located behind a NAT device, the public name or address of the NAT device should be specified.
- The common name of the certificate should match the name of the IP-HTTPS site.
- For the Enhanced Key Usage field, use the Server Authentication object identifier (OID).
- For the CRL Distribution Points field, specify a CRL distribution point that is accessible by DirectAccess clients that are connected to the Internet.
- The IP-HTTPS certificate must have a private key.

- The IP-HTTPS certificate must be imported directly into the personal store.
- IP-HTTPS certificates can have wildcards in the name.

Plan website certificates for the network location server

When planning for the network location server website, note the following:

- In the Subject field, specify either an IP address of the intranet interface of the network location server or the FQDN of the network location URL.
- For the Enhanced Key Usage field, use the Server Authentication OID.
- For the CRL Distribution Points field, a CRL distribution point that is accessible by DirectAccess clients that are connected to the intranet. This CRL distribution point should not be accessible from outside the internal network.
- If you are later planning to configure a multisite or cluster deployment, the name of the certificate should not match the internal name of the Remote Access server.

> **NOTE**
>
> Ensure that the certificates for IP-HTTPS and network location server have a **Subject Name**. If the certificate does not have a **Subject Name** but has an **Alternative Name**, then it will not be accepted by the Remote Access wizard.

Plan DNS requirements

In a Remote Access deployment, DNS is required for the following:

- **DirectAccess client requests**: DNS is used to resolve requests from DirectAccess client computers that are not located on the internal network. DirectAccess clients attempt to connect to the DirectAccess network location server in order to determine whether they are located on the Internet, or on the corporate network: If the connection is successful, then clients are determined to be on the intranet and DirectAccess is not used, and client requests are resolved using the DNS server configured on the network adapter of the client computer. If the connection does not succeed, clients are assumed to be on the Internet. DirectAccess clients will use the name resolution policy table (NRPT) to determine which DNS server to use when resolving name requests. You can specify that clients should use DirectAccess DNS64 to resolve names, or an alternative internal DNS server. When performing name resolution, the NRPT is used by DirectAccess clients to identify how to handle a request. Clients request an FQDN or single-label name such as https://internal. If a single-label name is requests, a DNS suffix is appended to make an FQDN. If the DNS query matches an entry in the NRPT, and DNS4 or an intranet DNS server is specified for the entry, then the query is sent for name resolution using the specified server. If a match exists but no DNS server is specified, then this indicates an exemption rule and normal name resolution is applied.

  Note that when a new suffix is added to the NRPT in the Remote Access Management console, the default DNS servers for the suffix can be automatically discovered by clicking the **Detect** button. Auto detection works as follows:

  1. If the corporate network is IPv4-based, or IPv4 and IPv6, the default address is the DNS64 address of the internal adapter on the Remote Access server.
  2. If the corporate network is IPv6-based, the default address is the IPv6 address of DNS servers in the corporate network.

- **Infrastructure servers**

  1. **Network location server**: DirectAccess clients attempt to reach the network location server to

determine if they are on the internal network. Clients on the internal network must be able to resolve the name of the network location server, but must be prevented from resolving the name when they are located on the Internet. To ensure this occurs, by default, the FQDN of the network location server is added as an exemption rule to the NRPT. In addition, when you configure Remote Access, the following rules are created automatically:

a. A DNS suffix rule for root domain or the domain name of the Remote Access server, and the IPv6 addresses corresponding to the intranet DNS servers configured on the Remote Access server. For example, if the Remote Access server is a member of the corp.contoso.com domain, a rule is created for the corp.contoso.com DNS suffix.

b. An exemption rule for the FQDN of the network location server. For example, if the network location server URL is https://nls.corp.contoso.com, an exemption rule is created for the FQDN nls.corp.contoso.com.

IP-HTTPS server: The Remote Access server acts as an IP-HTTPS listener and uses its server certificate to authenticate to IP-HTTPS clients. The IP-HTTPS name must be resolvable by DirectAccess clients using public DNS servers.

Connectivity verifiers: Remote Access creates a default web probe that is used by DirectAccess client computers use to verify connectivity to the internal network. To ensure the probe works as expected the following names must be registered manually in DNS:

a. directaccess-webprobehost should resolve to the internal IPv4 address of the Remote Access server, or to the IPv6 address in an IPv6-only environment.

b. directaccess-corpconnectivityhost should resolve to localhost (loopback) address. A and AAAA record should be created, A record with value 127.0.0.1 and AAAA record with value constructed out of NAT64 prefix with the last 32 bits as 127.0.0.1. The NAT64 prefix can be retrieved by running the cmdlet get-netnattransitionconfiguration.

> **NOTE**
> This is valid only in an IPv4-only environment. In an IPv4+IPv6, or IPv6-only environment, only a AAAA record should be created with the loopback IP address ::1.

You can create additional connectivity verifiers using other web addresses over HTTP or PING. For each connectivity verifier, a DNS entry must exist.

DNS server requirements

- For DirectAccess clients, you must use either a DNS server running Windows Server 2003, Windows Server 2008 , Windows Server 2008 R2 , Windows Server 2012 , or any DNS server that supports IPv6.

Plan Active Directory

Remote Access uses Active Directory and Active Directory Group Policy Objects as follows:

- **Authentication**: Active Directory is used for authentication. The intranet tunnel uses Kerberos authentication for the user to access internal resources.
- **Group policy objects**: Remote Access gathers configuration settings into group policy objects that are applied to Remote Access servers, clients, and internal application servers.
- **Security groups**: Remote Access uses security groups to gather together and identify DirectAccess client computers, and Remote Access servers. The group policies are applied to the required security group.
- **Extended IPsec policies**: Remote Access can use IPsec authentication and encryption between clients and the Remote Access server. You can extend IPsec authentication and encryption through to specified

internal application servers.

Active Directory Requirements

When planning Active Directory for a Remote Access deployment, the following is required:

- At least one domain controller installed on the Windows Server 2012 , Windows Server 2008 R2 Windows Server 2008 , or Windows Server 2003 operating systems.

  If the domain controller is on a perimeter network (and therefore reachable from the Internet-facing network adapter of Remote Access server) prevent the Remote Access server from reaching it by adding packet filters on the domain controller, to prevent connectivity to the IP address of the Internet adapter.

- The Remote Access server must be a domain member.
- DirectAccess clients must be domain members. Clients can belong to:
  - Any domain in the same forest as the Remote Access server.
  - Any domain that has a two-way trust with the Remote Access server domain.
  - Any domain in a forest that has a two-way trust with the forest to which the Remote Access domain belongs.

> **NOTE**
>
> - The Remote Access server cannot be a domain controller.
> - The Active Directory domain controller used for Remote Access must not be reachable from the external Internet adapter of the Remote Access server (the adapter must not be in the domain profile of Windows Firewall).

Plan Group Policy Objects

DirectAccess settings configured when you configure Remote Access are collected into Group Policy Objects (GPO). Three different GPOs are populated with DirectAccess settings, and distributed as follows:

- **DirectAccess client GPO**: This GPO contains client settings, including IPv6 transition technology settings, NRPT entries, and Windows Firewall with Advanced Security connection security rules. The GPO is applied to the security groups specified for the client computers.
- **DirectAccess server GPO**: This GPO contains the DirectAccess configuration settings that are applied to any server configured as a Remote Access server in your deployment. It also contains Windows Firewall with Advanced Security connection security rules.
- **Application servers GPO**: This GPO contains settings for selected application servers to which you optionally extend authentication and encryption from DirectAccess clients. If authentication and encryption are not extended then this GPO is not used.

GPOs are created automatically by the Enable DirectAccess Wizard and a default name is specified for each GPO.

Caution

Use the following procedure to backup all Remote Access Group Policy Objects before executing DirectAccess cmdlets: Back up and Restore Remote Access Configuration

GPOs can be configured in two ways:

1. **Automatically**: You can specify that they are created automatically. A default name is specified for each GPO.
2. **Manually**: You can use GPOs that have been predefined by the Active Directory administrator.

Note that once DirectAccess is configured to use specific GPOs, it cannot be configured to use different GPOs.

Automatically-created GPOs

Note the following when using automatically-created GPOs:

Automatically created GPOS are applied according to the location and link target parameter, as follows:

- For the DirectAccess server GPO, both the location and link parameters point to the domain containing the Remote Access server.
- When client GPOs are created, the location is set to a single domain in which the GPO will be created. The GPO name is looked up in each domain, and filled with DirectAccess settings if it exists. The link target is set to the root of the domain in which the GPO was created. A GPO is created for each domain that contains client computers or application servers, and the GPO is linked to the root of its respective domain.

When using automatically created GPOs, to apply DirectAccess settings, the Remote Access server administrator requires the following permissions:

- GPO create permissions for each domain.
- Link permissions for all the selected client domain roots.
- Link permissions for the server GPO domain roots.
- Create, edit, delete, and modify security permissions are required for the GPOs.
- It is recommended that the Remote Access administrator has GPO read permissions for each required domain. This enables Remote Access to verify that GPOs with duplicate names do not exist when creating GPOs.

Note that if the correct permissions for linking GPOs do not exist, a warning is issued. The Remote Access operation will continue but linking will not occur. If this warning is issued links will not be created automatically, even after the permissions are in place. Instead the administrator will need to create the links manually.

Manually-created GPOs

Note the following when using manually-created GPOs:

- The GPOs should exist before running the Remote Access Setup wizard.
- When using manually-created GPOs, to apply DirectAccess settings the Remote Access administrator requires full GPO permissions (Edit, Delete, Modify security) on the manually-created GPOs.
- When using manually created GPOs a search is made for a link to the GPO in the entire domain. If the GPO is not linked in the domain then a link is automatically created in the domain root. If the required permissions to create the link are not available a warning is issued.

Note that if the correct permissions for linking GPOs do not exist, a warning is issued. The Remote Access operation will continue but linking will not occur. If this warning is issued links will not be created automatically, even when the permissions are added later. Instead the administrator will need to create the links manually.

Recovering from a deleted GPO

If a Remote Access server, client, or application server GPO has been deleted by accident and there is no backup available, you must remove the configuration settings and re-configure again. If a backup is available, you can restore the GPO from the backup.

Remote Access Management will display the following error message: **GPO (GPO name) cannot be found**. To remove the configuration settings, take the following steps:

1. Run the PowerShell cmdlet **Uninstall-remoteaccess**.
2. Reopen **Remote Access Management**.

3. You will see an error message that the GPO is not found. Click **Remove configuration settings**. After completion, the server will be restored to an un-configured state.

Step 2 Plan the DirectAccess Deployment

12/9/2022 • 4 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After planning the Remote Access infrastructure, the next step in enabling DirectAccess is to plan the settings for the Enable DirectAccesss Wizard.

TASK	DESCRIPTION
Planning for client deployment	Plan how to allow client computers to connect using DirectAccess. Decide which managed computers will be configured as DirectAccess clients.
Planning for Remote Access server deployment	Plan how to deploy the Remote Access server.

Planning for client deployment

There are two decisions to make when planning your client deployment:

- Will DirectAccess be available to mobile computers only, or to any computer?

  When you configure DirectAccess clients in the Enable DirectAccess wizard, you can choose to allow only mobile computers in the specified security groups to connect using DirectAccess. If you restrict access to mobile computers, Remote Access automatically configures a WMI filter to ensure that the DirectAccess client GPO is applied only to mobile computers in the specified security groups. The Remote Access administrator requires permissions to create or modify group policy WMI filters to enable this setting.

- What security groups will contain the DirectAccess client computers?

  DirectAccess settings are contained in the DirectAccess client GPO. The GPO is applied to computers that are part of the security groups that you specify in the Enable DirectAccess wizard. You can specify security groups contained in any supported domain. Before you configure Remote Access, the security groups should be created. You can add computers to the security group after completing the Remote Access deployment, but note that if you add client computers that reside in a different domain to the security group, the client GPO will not be applied to these clients. For example, if you created SG1 in domain A for DirectAccess clients, and later add clients from domain B to this group, the client GPO will not be applied to clients in domain B. To avoid this issue, create a new client security group for each domain that contains client computers. Alternatively, if you do not want to create a new security group, run the Add-DAClient cmdlet with the name of the new GPO for the new domain.

Planning for Remote Access server deployment

There are a number of decisions to make when planning to deploy your Remote Access server:

- **Network topology**-There are two topologies available when deploying a Remote Access server:
  - **Two adapters**-With two network adapters, Remote Access can be configured with one network adapter connected directly to the Internet, and the other is connected to the internal network. Or alternatively the server is installed behind an edge device such as a firewall or a router. In this configuration one network adapter is connected to the perimeter network, the other is connected

to the internal network.

  - **Single network adapter**-In this configuration the Remote Access server is installed behind an edge device such as a firewall or a router. The network adapter is connected to the internal network.

- **Network adapters**-The Enable DirectAccess wizard automatically detects the network adapters configured on the Remote Access server, based on the interfaces used by VPN. You must make sure that the correct adapters are selected.

- **ConnectTo address**-Client computers use the ConnectTo address in order to connect to the Remote Access server. The address that you choose must match the subject name of the IP-HTTPS certificate that you deploy for the IP-HTTPS connection and must be available in the public DNS. See Planning website certificates for IP-HTTPS.

- **IP-HTTPS certificate**-If SSTP VPN is configured, the Enable DirectAccess wizard picks up the certificate used by SSTP for IP-HTTPS. If SSTP VPN is not configured, the wizard will try to see if a certificate for IP-HTTPS has been configured. If not, it will automatically provision self-signed certificates for IP-HTTPS.The wizard automatically enables Kerberos authentication. The wizard will also enable NAT64 and DNS64 for protocol translation in the IPv4-only environment.

- **IPv6 prefixes**-If the wizard detects that IPv6 has been deployed on the network adapters, it automatically creates IPv6 prefixes for the internal network, an IPv6 prefix to assign to DirectAccess client computers, and an IPv6 prefix to assign to VPN client computers. If the automatically generated prefixes are not correct for your native IPv6 or ISATAP infrastructure, you must manually change them. See 1.1 Planning network and server topology and settings.

- **Windows 7 clients**-By default, Windows 7 client computers cannot connect to a Windows Server 2012 Remote Access deployment. If you have Windows 7 client computers in your organization that require remote access to internal resources, you can allow them to connect. Any client computers that you want to allow to access internal resources must be a member of a security group that you specify in the Enable DirectAccess wizard.

  > **NOTE**
  > Allowing Windows 7 client computers to connect using DirectAccess requires you to use computer certificate authentication.

- **Authentication**-The Enable DirectAccess wizard uses Active Directory to authenticate the user credentials. To deploy two-factor authentication, see Deploy Remote Access with OTP authentication.

Enable DirectAccess

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016 and Windows Server 2012 combine DirectAccess and Remote Access Service (RAS) VPN into a single Remote Access role. This overview provides an introduction to the configuration steps required in order to deploy a single Windows Server 2016 or Windows Server 2012 Remote Access server with basic settings.

- Step 1: Configure the DirectAccess infrastructure. This step includes configuring network and server settings, DNS settings and Active Directory settings.
- Step 2: Configure the DirectAccess-VPN Server. This step includes configuring DirectAccess client computers, server settings.
- Step 3: Verify the deployment. This step includes steps for verifying the deployment.

Before starting the deployment, verify the planning steps described in Plan to Enable DirectAccess.

Step 1 Configure the DirectAccess Infrastructure

12/9/2022 • 14 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to configure the infrastructure required for enabling DirectAccess in an existing VPN deployment. Before beginning the deployment steps, ensure that you have completed the planning steps described in Step 1: Plan DirectAccess Infrastructure.

TASK	DESCRIPTION
Configure server network settings	Configure the server network settings on the Remote Access server.
Configure routing in the corporate network	Configure routing in the corporate network to make sure traffic is appropriately routed.
Configure firewalls	Configure additional firewalls, if required.
Configure CAs and certificates	The Enable DirectAccess Wizard configures a built in Kerberos proxy that authenticates using user names and passwords. It also configures an IP-HTTPS certificate on the Remote Access server.
Configure the DNS server	Configure DNS settings for the Remote Access server.
Configure Active Directory	Join client computers to the Active Directory domain.
Configure GPOs	Configure GPOs for the deployment, if required.
Configure security groups	Configure security groups that will contain DirectAccess client computers, and any other security groups required in the deployment.
Configure the network location server	The Enable DirectAccess Wizard configures the network location server on the DirectAccess server.

Configure server network settings

The following network interface settings are required for a single server deployment in an environment with IPv4 and IPv6. All IP addresses are configured by using **Change adapter settings** in the **Windows Networking and Sharing Center**.

- Edge topology
  - One Internet-facing public static IPv4 or IPv6 address.
  - A single internal static IPv4 or IPv6 address.
- Behind NAT device (two network adapters)
  - A single internal network-facing static IPv4 or IPv6 address.

- Behind NAT device (one network adapter)
  - A single static IPv4 or IPv6 address.

> **NOTE**
>
> In the event that the Remote Access server has two network adapters (one classified in the domain profile and the other in a public/private profile), but a single NIC topology will be used, then the recommendation is as follows:
>
> 1. Ensure that the 2nd NIC is also classified in the domain profile - Recommended.
> 2. If the 2nd NIC cannot be configured for the domain profile for any reason, then the DirectAccess IPsec policy must be manually scoped to all profiles using the following Windows PowerShell commands:
>
> ```
> $gposession = Open-NetGPO -PolicyStore <Name of the server GPO>
> Set-NetIPsecRule -DisplayName <Name of the IPsec policy> -GPOSession $gposession -Profile Any
> Save-NetGPO -GPOSession $gposession
> ```

Configure routing in the corporate network

Configure routing in the corporate network as follows:

- When native IPv6 is deployed in the organization, add a route so that the routers on the internal network route IPv6 traffic back through the Remote Access server.
- Manually configure organization IPv4 and IPv6 routes on the Remote Access servers. Add a published route so that all traffic with an organization (/48) IPv6 prefix is forwarded to the internal network. In addition, for IPv4 traffic, add explicit routes so that IPv4 traffic is forwarded to the internal network.

Configure firewalls

When using additional firewalls in your deployment, apply the following Internet-facing firewall exceptions for Remote Access traffic when the Remote Access server is on the IPv4 Internet:

- 6to4 traffic-IP Protocol 41 inbound and outbound.
- IP-HTTPS-Transmission Control Protocol (TCP) destination port 443, and TCP source port 443 outbound. When the Remote Access server has a single network adapter, and the network location server is on the Remote Access server, then TCP port 62000 is also required.

When using additional firewalls, apply the following Internet-facing firewall exceptions for Remote Access traffic when the Remote Access server is on the IPv6 Internet:

- IP Protocol 50
- UDP destination port 500 inbound, and UDP source port 500 outbound.

When using additional firewalls, apply the following internal network firewall exceptions for Remote Access traffic:

- ISATAP-Protocol 41 inbound and outbound
- TCP/UDP for all IPv4/IPv6 traffic

Configure CAs and certificates

The Enable DirectAccess Wizard configures a built in Kerberos proxy that authenticates using user names and passwords. It also configures an IP-HTTPS certificate on the Remote Access server.

Configure certificate templates

When you use an internal CA to issue certificates, you must configure a certificate template for the IP-HTTPS certificate and the network location server website certificate.

To configure a certificate template

1. On the internal CA, create a certificate template as described in Creating Certificate Templates.
2. Deploy the certificate template as described in Deploying Certificate Templates.

Configure the IP-HTTPS certificate

Remote Access requires an IP-HTTPS certificate to authenticate IP-HTTPS connections to the Remote Access server. There are three certificate options for the IP-HTTPS certificate:

- **Public**-Supplied by a 3rd party.

  A certificate used for IP-HTTPS authentication. In the case that the certificate subject name is not a wild card, then it must be the externally resolvable FQDN URL used only for the Remote Access server IP-HTTPS connections.

- **Private**-The following are required, if they do not already exist:
  - A website certificate used for IP-HTTPS authentication. The certificate subject should be an externally resolvable fully qualified domain name (FQDN) reachable from the Internet.
  - A certificate revocation list (CRL) distribution point that is reachable from a publicly resolvable FQDN.

- **Self-signed**-The following are required, if they do not already exist:

  > **NOTE**
  > Self-signed certificates cannot be used in multisite deployments.

  - A website certificate used for IP-HTTPS authentication. The certificate subject should be an externally resolvable FQDN reachable from the Internet.
  - A CRL distribution point that is reachable from a publicly resolvable fully qualified domain name (FQDN).

Make sure that the website certificate used for IP-HTTPS authentication meets the following requirements:

- The common name of the certificate should match the name of the IP-HTTPS site.
- In the subject field, specify either the IPv4 address of the external-facing adapter of the Remote Access server, or the FQDN of the IP-HTTPS URL.
- For the Enhanced Key Usage field, use the Server Authentication object identifier (OID).
- For the CRL Distribution Points field, specify a CRL distribution point that is accessible by DirectAccess clients that are connected to the Internet.
- The IP-HTTPS certificate must have a private key.
- The IP-HTTPS certificate must be imported directly into the personal store.
- IP-HTTPS certificates can have wildcards in the name.

To install the IP-HTTPS certificate from an internal CA

1. On the Remote Access server: On the **Start** screen, type**mmc.exe**, and then press ENTER.
2. In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.

3. On the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
6. Click **Next** twice.
7. On the **Request Certificates** page, select the check box for the certificate template, and if required, click **More information is required to enroll for this certificate**.
8. On the **Certificate Properties** dialog box, on the **Subject** tab, in the **Subject name** area, in **Type**, select **Common Name**.
9. In **Value**, specify either the IPv4 address of the external-facing adapter of the Remote Access server, or the FQDN of the IP-HTTPS URL, and then click **Add**.
10. In the **Alternative name** area, in **Type**, select **DNS**.
11. In **Value**, specify either the IPv4 address of the external-facing adapter of the Remote Access server, or the FQDN of the IP-HTTPS URL, and then click **Add**.
12. On the **General** tab, in **Friendly name**, you can enter a name that will help you identify the certificate.
13. On the **Extensions** tab, next to **Extended Key Usage**, click the arrow, and make sure that Server Authentication is in the **Selected options** list.
14. Click **OK**, click **Enroll**, and then click **Finish**.
15. In the details pane of the Certificates snap-in, verify that new certificate was enrolled with Intended Purposes of Server Authentication.

Configure the DNS server

You must manually configure a DNS entry for the network location server website for the internal network in your deployment.

To create the network location server and web probe DNS records

1. On the internal network DNS server: On the **Start** screen, type** dnsmgmt.msc**, and then press ENTER.
2. In the left pane of the **DNS Manager** console, expand the forward lookup zone for your domain. Right click the domain and click **New Host (A or AAAA)**.
3. On the **New Host** dialog box, in the **Name (uses parent domain name if blank)** box, enter the DNS name for the network location server website (this is the name the DirectAccess clients use to connect to the network location server). In the **IP address** box, enter the IPv4 address of the network location server, and then click **Add Host**. On the **DNS** dialog box, click **OK**.
4. On the **New Host** dialog box, in the **Name (uses parent domain name if blank)** box, enter the DNS name for the web probe (the name for the default web probe is directaccess-webprobehost). In the **IP address** box, enter the IPv4 address of the web probe, and then click **Add Host**. Repeat this process for directaccess-corpconnectivityhost and any manually created connectivity verifiers. On the **DNS** dialog box, click **OK**.
5. Click **Done**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Add-DnsServerResourceRecordA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv4Address
<network_location_server_IPv4_address>
Add-DnsServerResourceRecordAAAA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv6Address
<network_location_server_IPv6_address>
```

You must also configure DNS entries for the following:

- **The IP-HTTPS server**-DirectAccess clients must be able to resolve the DNS name of the Remote Access server from the Internet.
- **CRL revocation checking**-DirectAccess uses certificate revocation checking for the IP-HTTPS connection between DirectAccess clients and the Remote Access server, and for the HTTPS-based connection between the DirectAccess client and the network location server. In both cases, DirectAccess clients must be able to resolve and access the CRL distribution point location.

Configure Active Directory

The Remote Access server and all DirectAccess client computers must be joined to an Active Directory domain. DirectAccess client computers must be a member of one of the following domain types:

- Domains that belong in the same forest as the Remote Access server.
- Domains that belong to forests with a two-way trust with the Remote Access server forest.
- Domains that have a two-way domain trust to the Remote Access server domain.

To join client computers to the domain

1. On the **Start** screen, type **explorer.exe**, and then press ENTER.
2. Right-click the Computer icon, and then click **Properties**.
3. On the **System** page, click **Advanced system settings**.
4. On the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
5. In **Computer name**, type the name of the computer if you are also changing the computer name when joining the server to the domain. Under **Member of**, click **Domain**, and then type the name of the domain to which you want to join the server; for example, corp.contoso.com, and then click **OK**.
6. When you are prompted for a user name and password, enter the user name and password of a user with rights to join computers to the domain, and then click **OK**.
7. When you see a dialog box welcoming you to the domain, click **OK**.
8. When you are prompted that you must restart the computer, click **OK**.
9. On the **System Properties** dialog box, click Close. Click **Restart Now** when prompted.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

Note that you must supply domain credentials after entering the Add-Computer command below.

```
Add-Computer -DomainName <domain_name>
Restart-Computer
```

Configure GPOs

To deploy Remote Access, you require a minimum of two Group Policy Objects: one Group Policy Object contains settings for the Remote Access server and one contains settings for DirectAccess client computers. When you configure Remote Access, the wizard automatically creates the required Group Policy Objects. However, if your organization enforces a naming convention, or you do not have the required permissions to create or edit Group Policy Objects, they must be created prior to configuring Remote Access.

To create Group Policy Objects, see Create and Edit a Group Policy Object.

> **IMPORTANT**
>
> The administrator can manually link the DirectAccess Group Policy Objects to an Organizational Unit using these steps:
>
> 1. Before configuring DirectAccess, link the created GPOs to the respective Organizational Units.
> 2. Configure DirectAccess, specifying a security group for the client computers.
> 3. The Remote Access administrator may or may not have permissions to link the Group Policy Objects to the domain. In either case, the Group Policy Objects will be configured automatically. If the GPOs are already linked to an OU, the links will not be removed, and the GPOs will not be linked to the domain. For a server GPO, the OU must contain the server computer object, or the GPO will be linked to the root of the domain.
> 4. If the linking to the OU has not been done before running the DirectAccess wizard, then after the configuration is complete, the domain administrator can link the DirectAccess Group Policy Objects to the required Organizational Units. The link to the domain can be removed. Steps for linking a Group Policy Object to an Organization Unit can be found here.

> **NOTE**
>
> If a Group Policy Object was created manually, it is possible during the DirectAccess configuration that the Group Policy Object will not be available. The Group Policy Object may not have been replicated to the closest Domain Controller to the management computer. In this event, the administrator can wait for replication to complete, or force the replication.

Configure security groups

The DirectAccess settings contained in the client computer Group Policy Object are applied only to computers that are members of the security groups that you specify when configuring Remote Access. In addition, if you are using security groups to manage your application servers, create a security group for these servers.

To create a security group for DirectAccess clients

1. On the **Start** screen, type**dsa.msc**, and then press ENTER. In the **Active Directory Users and Computers** console, in the left pane, expand the domain that will contain the security group, right-click **Users**, point to **New**, and then click **Group**.

2. On the **New Object - Group** dialog box, under **Group name**, enter the name for the security group.

3. Under **Group scope**, click **Global**, under **Group type**, click **Security**, and then click **OK**.

4. Double-click the DirectAccess client computers security group, and on the properties dialog box, click the **Members** tab.

5. On the **Members** tab, click **Add**.

6. On the **Select Users, Contacts, Computers, or Service Accounts** dialog box, select the client computers that you want to enable for DirectAccess, and then click **OK**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
New-ADGroup -GroupScope global -Name <DirectAccess_clients_group_name>
Add-ADGroupMember -Identity DirectAccess_clients_group_name -Members <computer_name>
```

Configure the network location server

The network location server should be on a server with high availability, and a valid SSL certificate trusted by the DirectAccess clients. There are two certificate options for the network location server certificate:

- **Private**-The following are required, if they do not already exist:
  - A website certificate used for the network location server. The certificate subject should be the URL of the network location server.
  - A CRL distribution point that is highly available from the internal network.
- **Self-signed**-The following are required, if they do not already exist:

  > **NOTE**
  > Self-signed certificates cannot be used in multisite deployments.

  - A website certificate used for the network location server. The certificate subject should be the URL of the network location server.

> **NOTE**
> If the network location server website is located on the Remote Access server, a website will be created automatically when configuring Remote Access that is bound to the server certificate that you provide.

To install the network location server certificate from an internal CA

1. On the server that will host the network location server website: On the **Start** screen, type**mmc.exe**, and then press ENTER.
2. In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.
3. On the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
6. Click **Next** twice.
7. On the **Request Certificates** page, select the check box for the certificate template, and if required, click **More information is required to enroll for this certificate**.

8. On the **Certificate Properties** dialog box, on the **Subject** tab, in the **Subject name** area, in **Type**, select **Common Name**.
9. In **Value**, enter the FQDN of the network location server website, and then click **Add**.
10. In the **Alternative name** area, in **Type**, select **DNS**.
11. In **Value**, enter the FQDN of the network location server website, and then click **Add**.
12. On the **General** tab, in **Friendly name**, you can enter a name that will help you identify the certificate.
13. Click **OK**, click **Enroll**, and then click **Finish**.
14. In the details pane of the Certificates snap-in, verify that new certificate was enrolled with Intended Purposes of Server Authentication.

Step 2 Configure the DirectAccess-VPN Server

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to configure the client and server settings required for a basic Remote Access deployment using the Enable DirectAccess Wizard.

The following table provides an overview of the steps you can complete by using this topic.

TASK	DESCRIPTION
Configure DirectAccess clients	Configure the Remote Access server with the security groups containing DirectAccess clients.
Configure the Network Topology	Configure Remote Access server settings.
Configure the DNS Suffix Search List	Modify the Suffix search list if desired.
GPO Configuration	Modify the GPOs if desired.

To Start the Enable DirectAcces Wizard

1. In Server Manager, click **Tools**, and then click **Remote Access**.The Enable DirectAccess Wizard starts automatically unless you have selected **Do not show this screen again**.
2. If the wizard does not start automatically, right-click the server node in the Routing and Remote Access tree, and then click **Enable DirectAccess**.
3. Click **Next**.

Configure DirectAccess clients

For a client computer to be provisioned to use DirectAccess it must belong to the selected security group. After DirectAccess is configured, client computers in the security group are provisioned to receive the DirectAccess group policy.

1. On the **Select Groups** page, click **Add**.
2. On the **Select Groups** dialog box, select the security groups containing DirectAccess client computers.
3. Select the **Enable DirectAccess for mobile computers only** check box to allow only mobile computers to access the internal network.
4. Select the **Use force tunneling** check box to route all client traffic (to the internal network and to the Internet) through the Remote Access server.
5. Click **Next**.

Configure the Network Topology

To deploy Remote Access, you need to configure the Remote Access server with the correct network adapters, a

public URL for the Remote Access server to which client computers can connect (the connect to address), and an IP-HTTPS certificate whose subject matches the connect to address.

1. On the **Network Topology** page, click the deployment topology that will be used in your organization. In **Type the public name or IPv4 address used by clients to connect to the Remote Access server**, enter the public name for the deployment (this name matches the subject name of the IP-HTTPS certificate, for example, edge1.contoso.com), and then click **Next**.

Configure the DNS Suffix Search List

For DNS clients, you can configure a DNS domain suffix search list that extends or revises their DNS search capabilities. By adding additional suffixes to the list, you can search for short, unqualified computer names in more than one specified DNS domain. Then, if a DNS query fails, the DNS Client service can use this list to append other name suffix endings to your original name and repeat DNS queries to the DNS server for these alternate FQDNs.

1. Select **Configure DirectAccess Clients with DNS client suffix search list** to specify additional suffixes for client name searches.

2. Type a new suffix name in **New Suffix** and then click **Add**. Additionally, you can change the search order and remove suffixes from **Domain Suffixes to use**.

> [NOTE] In a disjoint name space scenario (where one or more domain computers has an DNS suffix that does not match the Active Directory domain to which the computers belong), you should ensure that the search list is customized to include all the required suffixes. The Remote Access wizard will by default configure the Active Directory DNS name as the primary DNS suffix on the client. Admin should ensure that he adds the DNS suffix used by clients for name resolution.

For computers and servers, the following default DNS search behavior is predetermined and used when completing and resolving short, unqualified names.When the suffix search list is empty or unspecified, the primary DNS suffix of the computer is appended to short unqualified names, and a DNS query is used to resolve the resultant FQDN.

If this query fails, the computer can try additional queries for alternate FQDNs by appending any connection-specific DNS suffix configured for network connections.If no connection-specific suffixes are configured or queries for these resultant connection-specific FQDNs fail, then the client can then begin to retry queries based on systematic reduction of the primary suffix (also known as devolution).

For example, if the primary suffix is "example.microsoft.com," the devolution process can retry queries for the short name by searching for it in the "microsoft.com" and "com" domains.

When the suffix search list is not empty and has at least one DNS suffix specified, attempts to qualify and resolve short DNS names is limited to searching only those FQDNs made possible by the specified suffix list.

If queries for all FQDNs formed as a result of appending and trying each suffix in the list are not resolved, the query process fails, producing a "name not found" result.

> **WARNING**
>
> If the domain suffix list is used, clients continue to send additional alternate queries based on different DNS domain names when a query is not answered or resolved. Once a name is resolved using an entry in the suffix list, unused list entries are not tried. For this reason, it is most efficient to order the list with the most used domain suffixes first.
>
> Domain name suffix searches are used only when a DNS name entry is not fully qualified. To fully qualify a DNS name, a trailing period (.) is entered at the end of the name.

GPO Configuration

When you configure Remote Access, DirectAccess settings are collected into Group Policy Objects (GPO).

In **GPO Settings**, the DirectAccess server GPO name and Client GPO name are listed. Additionally, you can modify the GPO selection settings.

Two GPOs are populated automatically with DirectAccess settings, and distributed in this way:

1. **DirectAccess client GPO**. This GPO contains client settings, including IPv6 transition technology settings, NRPT entries, and Windows Firewall with Advanced Security connection security rules. The GPO is applied to the security groups specified for the client computers.
2. **DirectAccess server GPO**. This GPO contains the DirectAccess configuration settings that are applied to any server configured as a Remote Access server in your deployment. It also contains Windows Firewall with Advanced Security connection security rules.

Summary

Once the Remote Access configuration is complete the **Summary** is displayed. You can change the configured settings or click **Finish** to apply the configuration.

Step 3 Verify the Remote Access (VPN) Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to verify that you have correctly configured your DirectAccess deployment.

To verify access to internal resources through DirectAccess

1. Connect a DirectAccess client computer to the corporate network and obtain the group policy.
2. Click the **Network connections** icon in the notification area to access the DA Media Manager.
3. Click the **DirectAccess Connection**, and you will see that the status is **Connected Locally**.
4. Connect the client computer to the external network and attempt to access internal resources.

   You should be able to access all corporate resources.

Manage Remote Access

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The DirectAccess Remote Client Management deployment scenario uses DirectAccess to maintain clients over the Internet. This section explains the scenario, including its phases, roles, features, and links to additional resources.

Windows Server 2016 and Windows Server 2012 combine DirectAccess and Routing and Remote Access Service (RRAS) VPN into a single Remote Access role.

> **NOTE**
>
> In addition to this topic, the following Remote Access management topics are available.
>
> - Use Remote Access Monitoring and Accounting
> - Manage DirectAccess Clients Remotely

Scenario description

DirectAccess client computers are connected to the intranet whenever they are connected to the Internet, regardless of whether the user has signed in to the computer. They can be managed as intranet resources and kept current with Group Policy changes, operating system updates, antimalware updates, and other organizational changes.

In some cases, intranet servers or computers must initiate connections to DirectAccess clients. For example, Help Dtechnicians can use remote desktop connections to connect to and troubleshoot remote DirectAccess clients. This scenario lets you keep your existing remote access solution in place for user connectivity, while using DirectAccess for remote management.

DirectAccess provides a configuration that supports remote management of DirectAccess clients. You can use a deployment wizard option that limits the creation of policies to only those needed for remote management of client computers.

> **NOTE**
>
> In this deployment, user-level configuration options such as force tunneling, Network Access Protection (NAP) integration, and two-factor authentication are not available.

In this scenario

The DirectAccess Remote Client Management deployment scenario includes the following steps for planning and configuring.

Plan the deployment

There are only a few computer and network requirements for planning this scenario. They include:

- **Network and server topology**: With DirectAccess, you can place your Remote Access server at the edge of your intranet or behind a network address translation (NAT) device or a firewall.

- **DirectAccess network location server**: The network location server is used by DirectAccess clients to determine whether they are located on the internal network. The network location server can be installed on the DirectAccess server or on another server.
- **DirectAccess clients**: Decide which managed computers will be configured as DirectAccess clients.

Configure the deployment

Configuring your deployment consists of a number of steps. These include:

1. **Configure the infrastructure**: Configure DNS settings, join the server and client computers to a domain if required, and configure Active Directory security groups.

   In this deployment scenario, Group Policy Objects (GPOs) are created automatically by Remote Access. For advanced certificate GPO options, see Deploying advanced Remote Access.

2. **Configure Remote Access server and network settings**: Configure network adapters, IP addresses, and routing.
3. **Configure certificate settings**: In this deployment scenario, the Getting Started Wizard creates self-signed certificates, so there is no need to configure the more advanced certificate infrastructure.
4. **Configure the network location server**: In this scenario, the network location server is installed on the Remote Access server.
5. **Plan DirectAccess management servers**: Administrators can remotely manage DirectAccess client computers that are located outside the corporate network by using the Internet. Management servers include computers that are used during remote client management (such as update servers).
6. **Configure the Remote Access server**: Install the Remote Access role and run the DirectAccess Getting Started Wizard to configure DirectAccess.
7. **Verify the deployment**: Test a client to make sure it is able to connect to the internal network and the Internet by using DirectAccess.

Practical applications

Deploying a single Remote Access server for managing DirectAccess clients provides the following:

- **Ease-of-access**: Managed client computers running Windows 8 or Windows 7 can be configured as DirectAccess client computers. These clients can access internal network resources through DirectAccess any time they are connected to the Internet without needing to sign in to a VPN connection. Client computers not running one of these operating systems can connect to the internal network through VPN. DirectAccess and VPN are managed in the same console and with the same set of wizards.
- **Ease-of-management**: DirectAccess client computers that are connected to the Internet can be remotely managed by remote access administrators by using DirectAccess, even when the client computers are not located in the internal corporate network. Client computers that do not meet corporate requirements can be remediated automatically by management servers. One or more Remote Access servers can be managed from a single Remote Access Management console.

Roles and features included in this scenario

The following table lists the roles and features required for the scenario:

ROLE OR FEATURE	HOW IT SUPPORTS THIS SCENARIO

ROLE OR FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access role	This role is installed and uninstalled by using the Server Manager console or Windows PowerShell. This role encompasses DirectAccess, which was previously a feature in Windows Server 2008 R2, and Routing and Remote Access Services, which was previously a role service under the Network Policy and Access Services (NPAS) server role. The Remote Access role consists of two components: 1. DirectAccess and Routing and Remote Access Services (RRAS) VPN: DirectAccess and VPN are managed in the Remote Access Management console. 2. RRAS: Features are managed in the Routing and Remote Access console. The Remote Access server role is dependent on the following features: - Web Server (IIS): Required to configure the network location server and default web probe. - Windows internal database: Used for local accounting on the Remote Access server.
Remote Access Management Tools feature	This feature is installed as follows: - By default on a Remote Access server when the Remote Access role is installed and supports the Remote Management console user interface. - As an option on a server that is not running the Remote Access server role. In this case, it is used for remote management of a Remote Access server. This feature consists of the following: - Remote Access GUI and command-line tools - Remote Access module for Windows PowerShell Dependencies include: - Group Policy Management Console - RAS Connection Manager Administration Kit (CMAK) - Windows PowerShell 3.0 - Graphical Management Tools and Infrastructure

Hardware requirements

Hardware requirements for this scenario include the following:

Server requirements

- A computer that meets the hardware requirements for Windows Server 2016. For more information, see Windows Server 2016 System Requirements.
- The server must have at least one network adapter installed and enabled. There should be only one adapter connected to the corporate internal network, and only one connected to the external network (Internet).
- If Teredo is required as an IPv6 to IPv4 transition protocol, the external adapter of the server requires two consecutive public IPv4 addresses. If a single network adapter is available, only IP-HTTPS can be used as the transition protocol.
- At least one domain controller. The Remote Access servers and DirectAccess clients must be domain members.

- A certification authority is required on the server if you do not want to use self-signed certificates for IP-HTTPS or the network location server, or if you want to use client certificates for client IPsec authentication.

Client requirements

- A client computer must be running Windows 10 or Windows 8 or Windows 7.

Infrastructure and management server requirements

- During remote management of DirectAccess client computers, clients initiate communications with management servers, such as domain controllers, System Center Configuration Servers, and Health Registration Authority (HRA) servers. These servers provide services that include Windows and antivirus updates and Network Access Protection (NAP) client compliance. You should deploy the required servers before you begin the Remote Access deployment.

- A DNS server running Windows Server 2016, Windows Server 2012 R2 , Windows Server 2012 , Windows Server 2008 R2, or Windows Server 2008 with SP2 is required.

Software requirements

Software requirements for this scenario include the following:

Server requirements

- The Remote Access server must be a domain member. The server can be deployed at the edge of the internal network, or behind an edge firewall or other device.

- If the Remote Access server is located behind an edge firewall or NAT device, the device must be configured to allow traffic to and from the Remote Access server.

- Admins who deploy a Remote Access server require local administrator permissions on the server and domain user permissions. In addition, the administrator requires permissions for the GPOs that are used for DirectAccess deployment. To take advantage of the features that restrict DirectAccess deployment to only mobile computers, Domain Admin permissions are required on the domain controller to create a WMI filter.

- If the network location server is not located on the Remote Access server, a separate server to run it is required.

Remote access client requirements

- DirectAccess clients must be domain members. Domains that contain clients can belong to the same forest as the Remote Access server, or they can have a two-way trust with the Remote Access server forest or domain.

- An Active Directory security group is required to contain the computers that will be configured as DirectAccess clients. Computers should not be included in more than one security group that includes DirectAccess clients. If clients are included in multiple groups, name resolution for client requests will not work as expected.

Deploy Remote Access in an Enterprise

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic provides an introduction to the DirectAccess scenario for the Enterprise.

> **IMPORTANT**
>
> To deploy DirectAccess using this guide, you must use a DirectAccess server that is running Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012.

Before you begin deploying, see the list of unsupported configurations, known issues, and prerequisites

- DirectAccess Unsupported Configurations
- DirectAccess Known Issues
- Prerequisites for Deploying DirectAccess) Prerequisites

Scenario description

Remote access includes a number of enterprise features, including deploying multiple Remote Access servers in a cluster load balanced with Windows Network Load Balancing (NLB) or an external load balancer, setting up a multisite deployment with Remote Access servers situated in dispersed geographical locations, and deploying DirectAccess with two-factor client authentication using a one-time password (OTP).

In this scenario

Each enterprise scenario is described in a document that includes planning and deployment instructions. For more information, see:

- Deploy Remote Access in a cluster
- Deploy Multiple Remote Access Servers in a Multisite Deployment
- Deploy Remote Access with OTP Authentication
- Deploy Remote Access in a Multi-Forest Environment

Practical applications

Remote access enterprise scenarios provide the following:

- **Increased availability**. Deploying multiple Remote Access servers in a cluster provides scalability and increases the capacity for throughput and number of users. Load balancing the cluster provides high availability. If a server in the cluster fails, remote users can continue to access the internal corporate network via a different server in the cluster. Failover is transparent as clients connect to the cluster using a virtual IP (VIP) address.
- **Ease-of-management**. A cluster or multisite deployment can be configured and managed as a single

entity using the Remote Access Management console running on one of the cluster servers. In addition, a multisite deployment allows administrators to align Remote Access deployment to Active Directory sites, providing a simplified architecture. Shared settings can easily be set across cluster servers or on all multisite entry point servers. Remote Access settings can be managed from any of the servers in the cluster or deployment, or remotely using Remote Server Administration Tools (RSAT). In addition, the entire cluster or multisite deployment can be monitored from a single Remote Access Management console.

- **Cost efficiency**. A Remote Access multisite deployment allows enterprises to deploy Remote Access servers in multiple sites corresponding to client locations. This provides a predictable access experience for remote clients regardless of location, and reduces costs and intranet bandwidth by routing client traffic over the Internet to the closest Remote Access server.
- **Security**. Deploying strong client authentication with a one-time password (OTP) instead of standard Active Directory password increases security.

Roles and features included in this scenario

The following table lists the roles and features used in the enterprise scenario.

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access server role	The role is installed and uninstalled using the Server Manager console. This role encompasses both DirectAccess, which was previously a feature in Windows Server 2008 R2, and Routing and Remote Access Services which was previously a role service under the Network Policy and Access Services (NPAS) server role. The Remote Access role consists of two components: 1. DirectAccess and Routing and Remote Access Services (RRAS) VPN-DirectAccess and VPN are managed together in the Remote Access Management console. 2. RRAS Routing-RRAS routing features are managed in the legacy Routing and Remote Access console. The Remote Access Server Role is dependent on the following server features: - Internet Information Services (IIS) - This feature is required to configure the network location server and default web probe. - Group Policy Management Console feature - feature is required by DirectAccess to create and manage the Group Policy Objects (GPOs) in Active Directory and must be installed as a required feature for the server role.

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access Management Tools feature	This feature is installed as follows: - It is installed by default on a Remote Access server when the Remote Access role is installed, and supports the Remote Management console user interface. - It can be optionally installed on a server not running the Remote Access server role. In this case it is used for remote management of a Remote Access computer running DirectAccess and VPN. The Remote Access Management Tools feature consists of the following: 1. Remote Access GUI and Command Line Tools 2. Remote Access module for Windows PowerShell Dependencies include: 1. Group Policy Management Console 2. RAS Connection Manager Administration Kit (CMAK) 3. Windows PowerShell 3.0 4. Graphical Management Tools and Infrastructure
Windows NLB	This feature allows the load balancing of multiple Remote Access servers.

Deploy Remote Access in a Cluster

12/9/2022 • 6 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016 and Windows Server 2012 combine DirectAccess and Remote Access Service (RAS) VPN into a single Remote Access role. You can deploy Remote Access in a number of enterprise scenarios. This overview provides an introduction to the enterprise scenario for deploying multiple Remote Access servers in a cluster load balanced with Windows Network Load Balancing (NLB) or with an external load balancer (ELB), such as F5 Big-IP.

Scenario description

A cluster deployment gathers multiple Remote Access servers into a single unit, which then acts as a single point of contact for remote client computers connecting over DirectAccess or VPN to the internal corporate network using the external virtual IP (VIP) address of the Remote Access cluster. Traffic to the cluster is load balanced using Windows NLB or with an external load balancer (such as F5 Big-IP).

Prerequisites

Before you begin deploying this scenario, review this list for important requirements:

- Default load balancing through Windows NLB.
- External load balancers are supported.
- Unicast mode is the default and recommended mode for NLB.
- Changing policies outside of the DirectAccess management console or PowerShell cmdlets is not supported.
- When NLB or an external load balancer is used, the IPHTTPS prefix cannot be changed to anything other than /59.
- The load balanced nodes must be in the same IPv4 subnet.
- In ELB deployments, if manage out is needed, then DirectAccess clients cannot use Teredo. Only IPHTTPS can be used for end-to-end communication.
- Ensure all known NLB/ELB hotfixes are installed.
- ISATAP in the corporate network is not supported. If you are using ISATAP, you should remove it and use native IPv6.

In this scenario

The cluster deployment scenario includes a number of steps:

1. Deploy an Always on VPN server with Advanced options. A single Remote Access server with advanced settings must be deployed before setting up a cluster deployment.
2. Plan a Remote Access Cluster Deployment. To build a cluster from a single server deployment a number of additional steps are required, including preparing certificates for the cluster deployment.

3. Configure a Remote Access Cluster. This consists of a number of configuration steps, including preparing the single server for Windows NLB or the external load balancer, preparing additional servers to join the cluster, and enabling load balancing.

Practical applications

Gathering multiple servers into a server cluster provides the following:

- Scalability. A single Remote Access server provides a limited level of server reliability and scalable performance. By grouping the resources of two or more servers into a single cluster, you increase the capacity for number of users and throughput.
- High availability. A cluster provides high availability for always-on access. If one server in the cluster fails, remote users can continue to access the corporate network via a different server in the cluster. All servers in the cluster have the same set of cluster virtual IP (VIP) addresses, while still maintaining a unique, dedicated IP addresses for each server.
- Ease-of-management. A cluster allows management of multiple servers as a single entity. Shared settings can easily be set across cluster server. Remote Access settings can be managed from any of the servers in the cluster, or remotely using Remote Server Administration Tools (RSAT). In addition, the entire cluster can be monitored from a single Remote Access Management console.

Roles and features included in this scenario

The following table lists the roles and features required for the scenario:

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access role	The role is installed and uninstalled using the Server Manager console. It encompasses both DirectAccess, which was previously a feature in Windows Server 2008 R2, and Routing and Remote Access Services (RRAS), which was previously a role service under the Network Policy and Access Services (NPAS) server role. The Remote Access role consists of two components: - Always On VPN and Routing and Remote Access Services (RRAS) VPN-DirectAccess and VPN are managed together in the Remote Access Management console. - RRAS Routing-RRAS routing features are managed in the legacy Routing and Remote Access console. Dependencies are as follows: - Internet Information Services (IIS) Web Server - This feature is required to configure the network location server and default web probe. - Windows Internal Database-Used for local accounting on the Remote Access server.

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access Management Tools feature	This feature is installed as follows: - It is installed by default on a Remote Access server when the Remote Access role is installed, and supports the Remote Management console user interface. - It can be optionally installed on a server not running the Remote Access server role. In this case it is used for remote management of a Remote Access computer running DirectAccess and VPN. The Remote Access Management Tools feature consists of the following: - Remote Access GUI and Command Line Tools - Remote Access module for Windows PowerShell Dependencies include: - Group Policy Management Console - RAS Connection Manager Administration Kit (CMAK) - Windows PowerShell 3.0 - Graphical Management Tools and Infrastructure
Network Load Balancing	This feature provides load balancing in a cluster using Windows NLB.

Hardware requirements

Hardware requirements for this scenario include the following:

- At least two computers that meet the hardware requirements for Windows Server 2012.
- For the External Load Balancer scenario, dedicated hardware is required (i.e. F5 BigIP).
- In order to test the scenario, you must have at least one computer running Windows 10 configured as an Always On VPN client.

Software requirements

There are a number of requirements for this scenario:

- Software requirements for single server deployment. For more information see Deploy a Single DirectAccess Server with Advanced Settings. A single Remote Access).
- In addition to software requirements for a single server there are a number of cluster-specific requirements:
  - On each cluster server the IP-HTTPS certificate subject name must match the ConnectTo address. A cluster deployment supports a mix of wildcard and non-wildcard certificates on cluster servers.
  - If the network location server is installed on the Remote Access server, on each cluster server the network location server certificate must have the same subject name. In addition, the name of the network location server certificate must not have the same name as any server in the DirectAccess deployment.
  - IP-HTTPS and network location server certificates must be issued using the same method with which the certificate to the single server was issued. For example, if the single server uses a public certification authority (CA) then all servers in the cluster must have a certificate issued by a public CA. Or if the single server uses a self-signed certificate for IP-HTTPS then all servers in the cluster

must do likewise.

- The IPv6 prefix assigned to DirectAccess client computers on server clusters must be 59 bits. If VPN is enabled, the VPN prefix must also be 59 bits.

Known issues

The following are known issues when configuring a cluster scenario:

- After configuring DirectAccess in an IPv4-only deployment with a single network adapter, and after the default DNS64 (the IPv6 address which contains ":3333::") is automatically configured on the network adapter, attempting to enable load-balancing via the Remote Access Management console causes a prompt for the user to supply an IPv6 DIP. If an IPv6 DIP is supplied, the configuration fails after clicking **Commit** with the error: The parameter is incorrect.

  To resolve this issue:

  1. Download the backup and restore scripts from Back up and Restore Remote Access Configuration.
  2. Back up your Remote Access GPOs using the downloaded script Backup-RemoteAccess.ps1
  3. Attempt to enable load balancing until the step at which it fails. On the Enable Load Balancing dialog box, expand the details area, right-click in the details area, and then click **Copy Script**.
  4. Open Notepad, and paste the contents of the clipboard. For example:

     ```
     Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress @('10.244.4.19
     /255.255.255.0','fdc4:29bd:abde:3333::2/128') -InternetVirtualIPAddress
     @('fdc4:29bd:abde:3333::1/128', '10.244.4.21 /255.255.255.0') -ComputerName
     'DA1.domain1.corp.contoso.com' -Verbose
     ```

  5. Close any open Remote Access dialog boxes and close the Remote Access Management console.
  6. Edit the pasted text and remove the IPv6 addresses. For example:

     ```
     Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress @('10.244.4.19 /255.255.255.0') -
     InternetVirtualIPAddress @('10.244.4.21 /255.255.255.0') -ComputerName
     'DA1.domain1.corp.contoso.com' -Verbose
     ```

  7. In an elevated PowerShell window, run the command from the previous step.
  8. If the cmdlet fails while it is running (not due to incorrect input values), run the command Restore-RemoteAccess.ps1 and follow instructions to make sure that the integrity of your original configuration is maintained.
  9. You can now open the Remote Access Management console again.

Plan a Remote Access Cluster Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016 and Windows Server 2012 combine DirectAccess and Remote Access Service (RAS) VPN into a single Remote Access role. This overview provides an introduction to the planning steps required in order to deploy a cluster of Windows Server 2016 or Windows Server 2012 Remote Access servers.

- Plan an Advanced DirectAccess Deployment. This step includes planning for the infrastructure required to deploy a single server. It includes planning for network and server settings, certificate requirements, DNS settings, network location server deployment, DirectAccess management servers, Active Directory settings, and Group Policy Objects (GPOs).
- Step 2 Plan Cluster Servers .
- Step 3 Plan a Load-Balanced Cluster Deployment.
- Step 4: Record your planning decisions for Remote Access advanced deployment. This record can be used as a job aid for everyone involved in completing the deployment steps.

After you have completed these planning steps, see Configure a Remote Access cluster.

For instructions on configuring a cluster deployment as a proof of concept in a lab environment, see Test Lab Guide - Demonstrate DirectAccess in a Cluster with Windows NLB.

Step 1 Plan an Advanced Single Server Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first step in planning a Remote Access with one-time password (OTP) client authentication deployment is to plan and configure an advanced single server deployment.

Plan a single server deployment

Before you deploy Remote Access with OTP, make sure that you have completed all the steps to deploy a single Remote Access server. See Deploy a Single DirectAccess Server with Advanced Settings.

Step 2 Plan Cluster Servers

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After deploying a single Remote Access server, plan to add additional servers to the cluster.

TASK	DESCRIPTION
2.1 Installing roles and features.	For each server that will be added to the cluster, plan for installation of the Remote Access role and the Windows NLB feature (if needed), plan the topology, IP addressing, routing and forwarding.
2.2 Configure server settings	Configure settings for each server that will be added to the cluster. Note that you can configure a load balanced cluster of servers using virtual machines. In order for routing and connectivity to work correctly, you must configure the virtual machines to use MAC address spoofing.

2.1 Installing roles and features

For each server you want to join to the cluster, plan to install the Remote Access role. In addition plan to install the Network Load Balancing (NLB) feature if you want to load balance traffic to the cluster using Windows NLB. For more information see Network Load Balancing.

2.2 Configure server settings

For each server that will be added to the cluster, plan IP address and domain settings. Note the following:

1. Servers in the cluster must all belong to the same domain.
2. Servers in the cluster must be located on the same subnet.
3. Each server in the cluster should have the same number of network adapters in use for the DirectAccess deployment.

When you load balance the cluster using Windows NLB the following Windows NLB settings are applied:

1. Operation mode-Unicast. This can be changed to multicast using NLB Manager. This setting cannot be modified in the Remote Access Management console.
2. Load weight factor-Defined as Equal, where all cluster servers have equal load.
3. Filtering mode-Traffic will be load balanced across multiple hosts.
4. Affinity-Single affinity is defined.
5. Protocols-Both

Step 3 Plan a Load-Balanced Cluster Deployment

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The next step is to plan the load-balancing configuration and cluster deployment.

TASK	DESCRIPTION
3.1 Plan load balancing	Decide whether to use Windows Network Load Balancing (NLB), or an external load balancer (ELB).
3.2 Plan IP-HTTPS	If a self-signed certificate is not used, the Remote Access server needs an SSL certificate on each server in the cluster, in order to authenticate IP-HTTPS connections.
3.3 Plan for VPN client connections	Note the requirements for VPN client connections.
3.4 Plan the network location server	If the network location server website is hosted on the Remote Access server, and a self-signed certificate is not used, ensure that each server in the cluster has a server certificate to authenticate the connection to the website.

3.1 Plan load balancing

Remote Access can be deployed on a single server, or on a cluster of Remote Access servers. Traffic to the cluster can be load balanced to provide high availability and scalability for DirectAccess clients. There are two load balancing options:

- **Windows NLB**-Windows NLB is a Windows server feature. To use it, you do not require additional hardware because all the servers in the cluster are responsible for managing the traffic load. Windows NLB supports a maximum of eight servers in a Remote Access cluster.
- **External load balancer**-Using an external load balancer requires external hardware to manage the traffic load between the Remote Access cluster servers. In addition, using an external load balancer supports a maximum of 32 Remote Access servers in a cluster. Some points to keep in mind when configuring external load balancing are:
  - The administrator must ensure that the Virtual IPs configured through the Remote Access load balancing wizard are used on the external load balancers (like F5 Big-Ip Local Traffic Manager system). When external load balancing is enabled, the IP addresses on the external and internal interfaces will be promoted to Virtual IP addresses, and have to be plumbed on the load balancers. This is done so that the administrator does not have to change the DNS entry for the public name of the cluster deployment. Also, the IPsec tunnel endpoints are derived from the server IPs. If the administrator provides separate Virtual IPs, then the client will not be able to connect to the server. See example for configuring DirectAccess with External Load Balancing in 3.1.1 External Load Balancer configuration example.
  - Many external load balancers (including F5) do not support load balancing of 6to4 and ISATAP. If the Remote Access server is an ISATAP router, the ISATAP function should be moved to a different computer. Also, when ISATAP function is on a different computer, the DirectAccess servers must

have native IPv6 connectivity with the ISATAP router. Note that this connectivity should be present before configuring DirectAccess.

- For external load balancing, if Teredo has to be used, all the Remote Access servers must have two consecutive public IPv4 addresses as dedicated IP addresses. The Virtual IPs of the cluster also must have two consecutive public IPv4 addresses. This is not true for Windows NLB where only the Virtual IPs of the cluster must have two consecutive public IPv4 addresses. If Teredo is not used, two consecutive IP addresses are not required.
- The administrator can switch from Windows NLB to external load balancer and vice versa. Note that the administrator cannot switch from external load balancer to Windows NLB if he has more than 8 servers in the external load balancer deployment.

3.1.1 External Load Balancer configuration example

This section describes the configuration steps for enabling an external load balancer on a new Remote Access deployment. When using an external load balancer, the Remote Access cluster may look like the figure below, where the Remote Access servers are connected to the corporate network through a load balancer on the internal network, and to the Internet through a load balancer connected to the external network:

Planning information

1. External VIPs (IPs that the client will use to connect to Remote Access) were decided to be 131.107.0.102, 131.107.0.103
2. Load balancer on external network self-IPs - 131.107.0.245 (Internet), 131.107.1.245

   The perimeter network (also known as demilitarized zone and DMZ) is between the load balancer on the external network and the Remote Access server.
3. IP addresses for the Remote Access server on the perimeter network - 131.107.1.102, 131.107.1.103
4. IP addresses for the Remote Access server on the ELB network (i.e. between the Remote Access server and the load balancer on the internal network) - 30.11.1.101, 2006:2005:11:1::101
5. Load balancer on internal network self-IPs - 30.11.1.245 2006:2005:11:1::245 (ELB), 30.1.1.245 2006:2005:1:1::245 (Corpnet)
6. Internal VIPs (IP addresses used for client web-probe and for network location server, if installed on the Remote Access servers) were decided to be 30.1.1.10, 2006:2005:1:1::10

Steps

1. Configure the Remote Access server's external network adapter (that is connected to the perimeter network) with addresses 131.107.0.102, 131.107.0.103. This step is required for the DirectAccess configuration to detect the correct IPsec tunnel endpoints.

2. Configure the Remote Access server's internal network adapter (that is connected to the ELB network) with the web-probe/network location server IP addresses (30.1.1.10, 2006:2005:1:1::10). This step is required for allowing clients to access the web-probe IP, so the network connectivity assistant correctly indicates the connection status to DirectAccess. This step also allows access to the network location server, if it is configured on the DirectAccess server.

   > **NOTE**
   >
   > Make sure that the domain controller is reachable from the Remote Access server with this configuration.

3. Configure DirectAccess single server on the Remote Access server.

4. Enable external load balancing in the DirectAccess configuration. Use 131.107.1.102 as the external dedicated IP address (DIP) (131.107.1.103 will be selected automatically), use 30.11.1.101, 2006:2005:11:1::101 as the internal DIPs.

5. Configure the external virtual IPs (VIP) on the external load balancer with addresses 131.107.0.102 and 131.107.0.103. Also, configure the internal VIPs on the external load balancer with addresses 30.1.1.10 and 2006:2005:1:1::10.

6. The Remote Access server will now be configured with the planned IP addresses, and the external and internal IP addresses for the cluster will be configured according to the planned IP addresses.

3.2 Plan IP-HTTPS

1. **Certificate requirements**-During deployment of the single Remote Access server you selected to use either an IP-HTTPS certificate issued by a public or internal certification authority (CA), or a self-signed certificate. For the cluster deployment, you must use identical type of certificate on each member of the Remote Access cluster. That is, if you used a certificate issued by a public CA (recommended), you must install a certificate issued by a public CA on each member of the cluster. The subject name of the new certificate should be identical to the subject name of the IP-HTTPS certificate currently used in your deployment. Note that if you are using self-signed certificates these will be configured automatically on each server during cluster deployment.

2. **Prefix requirements**-Remote Access enables load balancing of both SSL-based traffic and DirectAccess traffic. To load balance all IPv6 based DirectAccess traffic, Remote Access must examine the IPv4 tunneling for all transition technologies. Because IP-HTTPS traffic is encrypted, examining the content of the IPv4 tunnel is not possible. To enable IP-HTTPS traffic to be load balanced, you must allocate a wide enough IPv6 prefix so that a different IPv6 /64 prefix can be assigned to every cluster member. You can configure a maximum of 32 servers in a load balanced cluster; therefore, you must specify a /59 prefix. This prefix must be routable to the internal IPv6 address of the Remote Access cluster, and is configured in the Remote Access Server Setup wizard.

   > **NOTE**
   >
   > The prefix requirements are relevant only in an IPv6 enabled internal network (IPv6-only, or IPV4+IPv6). In an IPv4 only corporate network, the client prefix is automatically configured and the administrator cannot change it.

3.3 Plan for VPN client connections

There are a number of considerations for VPN client connections:

- VPN client traffic cannot be load balanced if VPN client addresses are allocated using DHCP. A static address pool is required.
- RRAS can be enabled on a load-balanced cluster that has been deployed for DirectAccess only, using **Enable VPN** on the Tasks pane of the Remote Access Management console.
- Any VPN changes completed in the Routing and Remote Access Management console (rrasmgmt.msc) will have to be replicated manually on all Remote Access servers in the cluster.
- To enable VPN IPv6 client traffic to be load balanced, you must specify a 59-bit IPv6 prefix.

3.4 Plan the network location server

If you are running the network location server website on the single Remote Access server, during deployment you selected to use either a certificate issued by an internal certification authority (CA), or a self-signed certificate. Note the following:

1. Each member of the Remote Access cluster must have a certificate for the network location server that corresponds to the DNS entry for the network location server website.
2. The certificate for each cluster server must be issued in the same way as the certificate on the single Remote Access server current network location server certificate. For example, if you used a certificate issued by an internal CA, you must install a certificate issued by the internal CA on each member of the cluster.
3. If you used a self-signed certificate, a self-signed certificate will be configured automatically for each server during cluster deployment.
4. The subject name of the certificate must not be identical to the name of any of the servers in the Remote Access deployment.

Configure a Remote Access Cluster

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016 and Windows Server 2012 combine Always On VPN and Routing and Remote Access Service (RRAS) VPN into a single Remote Access role. This overview provides an introduction to the configuration steps required to deploy a single Windows Server 2016 or Windows Server 2012 Remote Access server in a load-balanced cluster.

- Step 1: Deploy an Always on VPN server with Advanced options.
- Step 2: Prepare cluster servers.
- Step 3: Configure a load-balanced cluster.
- Step 4: Verify the cluster.

Step 1 Implement a Single Server Remote Access Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first configuration step to deploy Remote Access in a multisite topology is to implement an advanced single server deployment and then plan to add servers to each multisite entry point.

Implement a single server deployment

Before you can configure a multisite deployment, you must configure an advanced single server Remote Access deployment as described in Deploy a Single DirectAccess Server with Advanced Settings.

See also

- Step 2: Configure the multisite infrastructure

Step 2 Prepare Cluster Servers

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Before you can configure a cluster deployment, you prepare additional servers to add to the cluster.

TASK	DESCRIPTION
2.1 Configure the Remote Access infrastructure	On each server you want to add to the cluster, configure the server topology, IP addressing, routing, and forwarding. If you configure a load balanced cluster of virtual machines, you must configure the virtual machines to use MAC address spoofing. In addition, join each server to the same domain, and connect all the servers to the same subnet.
2.2 Install the Remote Access role	On each additional server you want to add to the cluster, install the Remote Access role
2.3 Install NLB	On the deployed Remote Access server and on each additional server you want to add to the cluster, install the NLB feature. Note that this step is not required when using an External Load Balancer.

2.1 Configure the Remote Access infrastructure

To configure a Remote Access cluster, you must configure the server topology, IP addressing, routing, and forwarding on every server that will form part of the cluster.

To configure the Remote Access infrastructure

1. Configure each of the servers that will be in the cluster with the same topology as the first Remote Access server.
2. Configure each of the servers that will be in the cluster with appropriate IP addressing, routing, and forwarding based on the configuration of the first Remote Access server. Note that all the servers in the cluster must be connected to the same subnet.
3. Join each of the servers that will be in the cluster to the same domain as the first Remote Access server.

2.2 Install the Remote Access role

To configure a Remote Access cluster, you must install the Remote Access role on every server that will form a part of the cluster.

To install the Remote Access role on Always On VPN servers

1. On the DirectAccess server, in the Server Manager console, in the **Dashboard**, click **Add roles and features**.
2. Click **Next** three times to get to the server role selection screen.
3. On the **Select Server Roles** dialog, select **Remote Access**, and then click **Next**.

4. Click **Next** three times.
5. On the **Select role services** dialog, select **DirectAccess and VPN (RAS)** and then click **Add Features**.
6. Select **Routing**, select **Web Application Proxy**, click **Add Features**, and then click **Next**.
7. Click **Next**, and then click **Install**.
8. On the **Installation progress** dialog, verify that the installation was successful, and then click **Close**.
9. Repeat this procedure on all servers that you want to be cluster members.

2.3 Install NLB

To configure a Remote Access cluster, you must install the Network Load Balancing feature on every server that will form a part of the cluster.

> **NOTE**
> This step is not required if an external load balancer is used.

To install the NLB role

1. On the DirectAccess server, in the Server Manager console, in the **Dashboard**, click **Add roles and features**.
2. Click **Next** four times to get to the server feature selection screen.
3. On the **Select features** dialog, select **Network Load Balancing**, click **Add Features**, click **Next**, and then click **Install**.
4. On the **Installation progress** dialog, verify that the installation was successful, and then click **Close**.
5. Repeat this procedure on all servers that you want to be cluster members.

See also

- Step 3: Configure a load-balanced cluster

Step 3 Configure a Load-Balanced Cluster

12/9/2022 • 14 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After preparing servers for the cluster, configure load-balancing on the single server, configure the required certificates, and deploy the cluster.

TASK	DESCRIPTION
3.1 Configure the IPv6 prefix	If the corporate environment is IPv4+IPv6, or IPv6-only, then on the single Remote Access server, ensure that the IPv6 prefix assigned to DirectAccess client computers is large enough to cover all of the servers in your cluster.
3.2 Enable load balancing	Enable load balancing on the single Remote Access server.
3.3 Install the IP-HTTPS certificate	Each server in the cluster requires a server certificate to authenticate IP-HTTPS connection. Export the IP-HTTPS certificate from the single Remote Access server and deploy it on each server you will add to the cluster. This is required only if using non-self-signed certificates.
3.4 Install the network location server certificate	If the single server has the network location server deployed locally, then you will need to deploy the network location server certificate on each server in the cluster. If the network location server is hosted on an external server, a certificate on each server is not required. This is required only if using non-self-signed certificates.
3.5 Add servers to the cluster	Add all servers to the cluster. Remote Access must not be configured on the servers to be added.
3.6 Remove a server from the cluster	Instructions for removing a server from the cluster.
3.7 Disable load balancing	Instructions for disabling load balancing.

NOTE

The IP address that is selected for the DIP must not be in use on the network adapters of the first Remote Access server in the cluster. Beginning the DirectAccess deployment with both VIP and DIP added to the network adapter will result in failure.

NOTE

Make sure not to use a DIP that is already present on another machine on the network.

3.1 Configure the IPv6 prefix

To configure the prefix

1. On the Remote Access server, click **Start**, and then click **Remote Access Management**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the Remote Access Management Console, click **Configuration**.
3. In the middle pane of the console, in the **Step 2 DirectAccess Server** area, click **Edit**.
4. Click **Prefix Configuration**. On the **Prefix Configuration** page, in **IPv6 prefix assigned to DirectAccess client computers**, enter the IPv6 prefix used for DirectAccess client computers with a subnet length of 59, for example, **2001:db8:1:1000::/59**. If VPN were also enabled with IPv6, then an IPv6 prefix would be displayed, and the subnet length would need to be changed to 59. Click **Next**.
5. In the middle pane of the console, click **Finish**.
6. On the **Remote Access Review** dialog box, review the configuration settings, and then click **Apply**. On the **Applying Remote Access Setup Wizard Settings** dialog box, click **Close**.

3.2 Enable load balancing

To enable load balancing

1. On the configured DirectAccess server, click **Start**, and then click **Remote Access Management**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the Remote Access Management console, in the left pane, click **Configuration**, and then in the **Tasks** pane, click **Enable Load Balancing**.
3. In the Enable Load Balancing Wizard, click **Next**.
4. Depending on what you chose in planning steps:
   a. Windows NLB: On the **Load Balancing Method** page, click **Use Windows Network Load Balancing (NLB)**, and then click **Next**.
   b. External load balancer: On the **Load Balancing Method** page, click **Use an external load balancer**, and then click **Next**.
5. In a single network adapter deployment, on the **Dedicated IP Addresses** page, do the following, and then click **Next**:
   a. In the **IPv4 address** box, enter the new IPv4 address for this Remote Access server; the current IPv4 address will be the virtual IP address (VIP) of the load-balanced cluster. In the **Subnet mask** box, enter the subnet mask.
   b. If the corporate environment is native IPv6, then in the **IPv6 address** box, enter the new IPv6 address for this Remote Access server; the current IPv6 address will be the VIP of the load-balanced cluster. In the **Subnet prefix length** box, enter the subnet prefix length.
6. In a two network adapter deployment, on the **External Dedicated IP Addresses** page, do the following, and then click **Next**:
   a. In the **IPv4 address** box, enter the new external IPv4 address for this Remote Access server; the current IPv4 address will be the virtual IP address (VIP) of the load balancing cluster. In the **Subnet mask** box, enter the subnet mask.
   b. If there are currently native IPv6 addresses configured on the internet-facing network adapter of the Remote Access server, in the **IPv6 address** box, enter the new external IPv6 address for this Remote Access server; the current IPv6 address will be the VIP of the load balancing cluster. In the

Subnet prefix length box, enter the subnet prefix length.

7. In a two network adapter deployment, on the **Internal Dedicated IP Addresses** page, do the following, and then click **Next**:

   a. In the **IPv4 address** box, enter the new internal IPv4 address for this Remote Access server; the current IPv4 address will be the VIP of the load balancing cluster. In the **Subnet mask** box, enter the subnet mask.

   b. If the corporate environment is native IPv6, then in the **IPv6 address** box, enter the new internal IPv6 address for this Remote Access server; the current IPv6 address will be the VIP of the load balancing cluster. In the **Subnet prefix length** box, enter the subnet prefix length.

8. On the **Summary** page, click **Commit**.

9. On the **Enable Load Balancing** dialog box, click **Close**.

10. In the Enable Load Balancing Wizard, click **Close**.

> **NOTE**
>
> If external load balancing is being used, note the Virtual IPs and provide them as on the external load balancers.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

If you chose to use Windows NLB in the planning steps, then execute the following:

```
Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress "2.1.1.20/255.255.255.0" -
InternalDedicatedIPAddress @("10.1.1.30/255.255.255.0","3ffe::20/64") -InternetVirtualIPAddress
@("2.1.1.1/255.255.255.0","2.1.1.2/255.255.255.0") -InternalVirtualIPAddress
@("10.1.1.2/255.255.255.0","3ffe::2/64")
```

If you chose to use an external load balancer in the planning steps: then execute the following:

```
Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress "2.1.1.20/255.255.255.0" -
InternalDedicatedIPAddress @("10.1.1.30/255.255.255.0","3ffe::20/64") -UseThirdPrtyLoadBalancer
```

> **NOTE**
>
> It is recommended to not include changes to load-balancer settings with changes to any other settings, if you are using staging GPOs. Any changes to load-balancer settings must be applied first and then other configuration changes should be made. Also, after configuring load-balancer on a new DirectAccess server, please allow some time for the IP changes to be applied and replicated across the DNS servers in the enterprise, before you change other DirectAccess settings related to the new cluster.

3.3 Install the IP-HTTPS certificate

Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure.

To install the IP-HTTPS certificate

1. On the configured Remote Access server, click **Start**, type **mmc** and press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.
3. On the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Finish**, and then click **OK**.
4. In the left pane of the console, navigate to **Certificates (Local Computer)\Personal\Certificates**. Right-click the IP-HTTPS certificate, point to **All Tasks** and click **Export**.
5. On the **Welcome to the Certificate Export Wizard** page, click **Next**.
6. On the **Export Private Key** page, click **Yes, export the private key**, and then click **Next**.
7. On the **Export File Format** page, click **Personal Information Exchange - PKCS #12 (.PFX)**, and then click **Next**.
8. On the **Security** page, select the **Password** check box, enter a password in the **Password** box and confirm the password, and then click **Next**.
9. On the **File to Export** page, enter a name for the certificate file and save it to the desktop, and then click **Next**.
10. On the **Completing the Certificate Export Wizard** page, click **Finish**.
11. On the **Certificate Export Wizard** dialog box, click **OK**.
12. Copy the certificate to all servers that you want to be cluster members.
13. On the new DirectAccess server, click **Start**, type **mmc** and press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
14. In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.
15. On the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Finish**, and then click **OK**.
16. In the left pane of the console, navigate to **Certificates (Local Computer)\Personal\Certificates**. Right click the **Certificates** node, point to **All Tasks**, and then click **Import**.
17. On the **Welcome to the Certificate Import Wizard** page, click **Next**.
18. On the **File to Import** page, click **Browse** to locate the certificate. Select the certificate and then click **Next**.
19. On the **Private key protection** page, in the **Password** box, type the password, and then click **Next**.
20. On the **Certificate Store** page, click **Next**.
21. On the **Completing the Certificate Import Wizard** page, click **Finish**.
22. On the **Certificate Import Wizard** dialog box, click **OK**.
23. Repeat steps 13-22 on all servers that you want to be cluster members.

3.4 Install the network location server certificate

Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure.

To install a certificate for network location

1. On the Remote Access server, click **Start**, type **mmc**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. Click **File**, and then click **Add/Remove Snap-ins**.
3. Click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
6. Click **Next** twice.
7. On the **Request Certificates** page, click the Web Server certificate template, and then click **More information is required to enroll for this certificate**.

   If the Web Server certificate template does not appear, ensure that the Remote Access server computer account has enroll permissions for the Web Server certificate template. For more information, see Configure Permissions on the Web Server Certificate Template.
8. On the **Subject** tab of the **Certificate Properties** dialog box, in **Subject name**, for **Type**, select **Common name**.
9. In **Value**, type the fully qualified domain name (FQDN) for the intranet name of the network location server website (for example, nls.corp.contoso.com), and then click **Add**.
10. Click **OK**, click **Enroll**, and then click **Finish**.
11. In the details pane of the Certificates snap-in, verify that a new certificate with the FQDN was enrolled with **Intended Purposes** of **Server Authentication**.
12. Right-click the certificate, and then click **Properties**.
13. In **Friendly Name**, type **Network Location Certificate**, and then click **OK**.

    > **TIP**
    > Steps 12 and 13 are optional, but make it easier for you to select the certificate for network location when configuring Remote Access.

14. Repeat this procedure on all servers that you want to be cluster members.

3.5 Add servers to the cluster

To add servers to the cluster

1. On the configured DirectAccess server, click **Start**, and then click **Remote Access Management**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the Remote Access Management Console, click **Configuration**. In the **Tasks** pane, under **Load Balanced Cluster**, click **Add or Remove Servers**.
3. On the **Add or Remove Servers** dialog box, click **Add Server**.
4. On the **Add a Server** dialog box, on the **Select Server** page, enter the name of the additional Remote Access server, and then click **Next**.
5. On the **Network Adapters** page, do one the following:

- If you are deploying a topology with two network adapters, in **External adapter**, select the adapter that is connected to the external network. In **Internal adapter**, select the adapter that is connected to the internal network.
- If you are deploying a topology with one network adapter, in **Network adapter**, select the adapter that is connected to the internal network.

6. On the **Network Adapters** page, in **Select the certificate used to authenticate IP-HTTPS connections**, click **Browse** to locate and select the IP-HTTPS certificate, and then click **Next**.
7. On the **Network Location Server** page, click **Browse** to select the certificate for the network location server website running on the Remote Access server, and then click **Next**.

> **NOTE**
> The **Network Location Server** page appears only when the network location server website is running on the Remote Access server.

> **NOTE**
> If VPN were also configured on the Remote Access server, then you would be asked to add the VPN IP address pool information at this point.

8. On the **Summary** page, click **Add**.
9. On the **Completion** page, click **Close**.
10. Repeat this procedure for all Remote Access servers to be added to the cluster.
11. On the **Add or Remove Servers** dialog box, click **Commit**.
12. On the **Adding and Removing Servers** dialog box, click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Add-RemoteAccessLoadBalancerNode -RemoteAccessServer <server name>
```

> **NOTE**
> If VPN has not been enabled in a load balanced cluster, you should not provide any VPN address ranges when adding a new server to the cluster using Windows PowerShell cmdlets. If you have done so by mistake, remove the server from the cluster, and add it again to the cluster without specifying the VPN address ranges.

3.6 Remove a server from the cluster

To remove a server from the cluster

1. On the configured Remote Access server, click **Start**, and then click **Remote Access Management**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the Remote Access Management Console, click **Configuration**. In the **Tasks** pane, under **Load**

Balanced Cluster, click **Add or Remove Servers**.

3. On the **Add or Remove Servers** dialog box, select the Remote Access server you want to remove, and then click **Remove Server**.

4. On the **Remove Server Warning** dialog box, make sure you chose the right server, and then click **OK**.

5. Repeat this procedure for all Remote Access servers to be removed from the cluster.

6. On the **Add or Remove Servers** dialog box, click **Commit**.

7. On the **Adding and Removing Servers** dialog box, click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Remove-RemoteAccessLoadBalancerNode -RemoteAccessServer <server name>
```

3.7 Disable load balancing

Do this step using Windows PowerShell

To disable load balancing

1. On the configured DirectAccess server, click **Start**, and then click **Remote Access Management**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.

2. In the Remote Access Management Console, click **Configuration**. In the **Tasks** pane, under **Load Balanced Cluster**, click **Disable Load Balancing**.

3. On the **Disable Load Balancing** dialog box, click **Ok**.

4. On the **Disable Load Balancing** dialog box, click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
set-RemoteAccessLoadBalancer -disable
```

Disabling load balancing will remove Remote Access settings and NLB settings (if configured) from all servers except the server from which it is being executed. On this Remote Access server, NLB settings will be removed (if it was configured) but Remote Access settings will remain.

Clicking **Remove configuration settings** will remove Remote Access and NLB (if configured) from all servers in the deployment.

NOTE

- If Remote Access is uninstalled when load balancing is deployed, all the servers are left with DIPs. The VIPs are removed. This causes all routes in the corporate network that are targeted to the VIPs addresses to fail. This also affects DNS entries which were resolved to the VIPs, such as the network location server certificate subject name. To avoid this issue, disable load balancing, which leaves the VIPs on the last Remote Access server, and then uninstall Remote Access.
- After using the **Set-RemoteAccessLoadBalancer** cmdlet to disable load balancing, wait for 2 minutes before running any other cmdlet. This should also be done in any scripts that run another cmdlet after the **Set-RemoteAccessLoadBalancer -disable** cmdlet.
- Disabling load balancing changes the virtual IP address of the cluster into a dedicated IP address. As a result, any operation that queries for the name of the server will fail until the cached DNS entry on the server expires. Make sure that you do not run any Remote Access PowerShell cmdlets after disabling load balancing until the cache on the server has expired. This problem is more common if you try to disable load balancing on a machine from another machine that is in another domain. This also occurs if you disable load balancing from the Remote Access Management console and may prevent the configuration from loading. The configuration will load after the cache has expired or has been flushed.

See also

- Step 4: Verifying the cluster

Step 4 Verify the Cluster

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to verify that you have correctly configured your DirectAccess cluster deployment.

To verify access to internal resources through the cluster

1. Connect a DirectAccess client computer to the corporate network and obtain the group policy.
2. Connect the client computer to the external network and attempt to access internal resources.

   You should be able to access all corporate resources.
3. Test connectivity through each server in the cluster by turning off, or disconnecting from the external network, all but one of the cluster servers. On the client computer, attempt to access corporate resources. Repeat the test on a different cluster server.

   You should be able to access all corporate resources through each cluster server.

Deploy Multiple Remote Access Servers in a Multisite Deployment

12/9/2022 • 9 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016 and Windows Server 2012 combine DirectAccess and Remote Access Service (RAS) VPN into a single Remote Access role. Remote Access can be deployed in a number of enterprise scenarios. This overview provides an introduction to the enterprise scenario for deploying Remote Access servers in a multisite configuration.

Scenario description

In a multisite deployment two or more Remote Access servers or server clusters are deployed and configured as different entry points in a single location, or in dispersed geographical locations. Deploying multiple entry points in a single location allows for server redundancy, or for the alignment of Remote Access servers with existing network architecture. Deployment by geographical location ensures efficient use of resources, as remote client computers can connect to internal network resources using an entry point closest to them. Traffic across a multisite deployment can be distributed and balanced with an external global load balancer.

A multisite deployment supports client computers running Windows 10, Windows 8 or Windows 7 . Client computers running Windows 10 or Windows 8 automatically identify an entry point, or the user can manually select an entry point. Automatic assignment occurs in the following priority order:

1. Use an entry point selected manually by the user.
2. Use an entry point identified by an external global load balancer if one is deployed.
3. Use the closest entry point identified by the client computer using an automatic probe mechanism.

Support for clients running Windows 7 must be manually enabled on each entry point, and selection of an entry point by these clients is not supported.

Prerequisites

Before you begin deploying this scenario, review this list for important requirements:

- Deploy a Single DirectAccess Server with Advanced Settings must be deployed before a multisite deployment.
- Windows 7 clients will always connect to a specific site. They will not be able to connect to the closest site based on location of the client (unlike Windows 10, 8, or 8.1 clients).
- Changing policies outside of the DirectAccess management console or PowerShell cmdlets is not supported.
- A Public Key Infrastructure must be deployed.

  For more information see: Test Lab Guide Mini-Module: Basic PKI for Windows Server 2012.
- The corporate network must be IPv6 enabled. If you are using ISATAP, you should remove it and use native IPv6.

In this scenario

The multisite deployment scenario includes a number of steps:

1. Deploy a single DirectAccess server with advanced settings. A single Remote Access server with advanced settings must be deployed before setting up a multisite deployment.
2. Plan a Multisite Deployment. To build a multisite deployment from a single server a number of additional planning steps are required, including compliance with multisite prerequisites, and planning for Active Directory security groups, Group Policy Objects (GPOs), DNS, and client settings.
3. Configure a Multisite Deployment. This consists of a number of configuration steps, including preparation of the Active Directory infrastructure, configuration of the existing Remote Access server, and the addition of multiple Remote Access servers as entry points to the multisite deployment.
4. Troubleshoot a Multisite Deployment. This troubleshooting section describes a number of the most common errors that can occur when deploying Remote Access in a multisite deployment.

Practical applications

A multisite deployment provides the following:

- Improved performance-A multisite deployment allows client computers accessing internal resources using Remote Access to connect using the closest and most suitable entry point. Client access internal resources efficiently, and the speed of client Internet requests routed via DirectAccess is improved. Traffic across entry points can be balanced using an external global load balancer.
- Ease-of-management-Multisite allows administrators to align the Remote Access deployment to an Active Directory sites deployment, providing a simplified architecture. Shared settings can easily be set across entry point servers or clusters. Remote Access settings can be managed from any of the servers in the deployment, or remotely using Remote Server Administration Tools (RSAT). In addition, the entire multisite deployment can be monitored from a single Remote Access Management console.

Roles and features included in this scenario

The following table lists the roles and features used in this scenario.

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access role	The role is installed and uninstalled using the Server Manager console. It encompasses both DirectAccess, which was previously a feature in Windows Server 2008 R2, and Routing and Remote Access Services (RRAS), which was previously a role service under the Network Policy and Access Services (NPAS) server role. The Remote Access role consists of two components: - DirectAccess and Routing and Remote Access Services (RRAS) VPN-DirectAccess and VPN are managed together in the Remote Access Management console. - RRAS Routing-RRAS routing features are managed in the legacy Routing and Remote Access console. Dependencies are as follows: - Internet Information Services (IIS) Web Server - This feature is required to configure the network location server and default web probe. - Windows Internal Database-Used for local accounting on the Remote Access server.

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access Management Tools feature	This feature is installed as follows: - It is installed by default on a Remote Access server when the Remote Access role is installed, and supports the Remote Management console user interface. - It can be optionally installed on a server not running the Remote Access server role. In this case it is used for remote management of a Remote Access computer running DirectAccess and VPN. The Remote Access Management Tools feature consists of the following: - Remote Access GUI and Command Line Tools - Remote Access module for Windows PowerShell Dependencies include: - Group Policy Management Console - RAS Connection Manager Administration Kit (CMAK) - Windows PowerShell 3.0 - Graphical Management Tools and Infrastructure

Hardware requirements

Hardware requirements for this scenario include the following:

- At least two Remote Access computers to be gathered into a multisite deployment.
- In order to test the scenario, at least one computer running Windows 8 and configured as a DirectAccess client is required. To test the scenario for clients running Windows 7 at least one computer running Windows 7 is required.
- To load balance traffic across entry point servers, a third-party external global load balancer is required.

Software requirements

Software requirements for this scenario include the following:

- Software requirements for single server deployment.
- In addition to software requirements for a single server there are a number of multisite-specific requirements:
    - IPsec authentication requirements-In a multisite deployment DirectAccess must be deployed using IPsec machine certificate authentication. The option to perform IPsec authentication using the Remote Access server as a Kerberos proxy is not supported. An internal CA is required to deploy the IPsec certificates.
    - IP-HTTPS and network location server requirements-Certificates required for IP-HTTPS and the network location server must be issued by a CA. The option to use certificates that are automatically issued and self-signed by the Remote Access server is not supported. Certificates can be issued by an internal CA or by a third-party external CA.
    - Active Directory requirements-At least one Active Directory site is required. The Remote Access server should be located in the site. For faster update times, it is recommended that each site has a writeable domain controller, though this is not mandatory.
    - Security group requirements-Requirements are as follows:

    - A single security group is required for all Windows 8 client computers from all domains. It is recommended to create a unique security group of these clients for each domain.
    - A unique security group containing Windows 7 computers is required for each entry point configured to support Windows 7 clients. It is recommended to have a unique security group for each entry point in each domain.
    - Computers should not be included in more than one security group that includes DirectAccess clients. If clients are included in multiple groups, name resolution for client requests will not work as expected.
  - GPO requirements-GPOs can be manually created before configuring Remote Access, or automatically created during Remote Access deployment. Requirements are as follows:
    - A unique client GPO is required for each domain.
    - A server GPO is required for each entry point, in the domain in which the entry point is located. So if multiple entry points are located in the same domain, there will be multiple server GPOs (one for each entry point) in the domain.
    - A unique Windows 7 client GPO is required for each entry point enabled for Windows 7 client support, for each domain.

Known issues

The following are known issues when configuring a multisite scenario:

- **Multiple entry points in the same IPv4 subnet**. Adding multiple entry points in the same IPv4 subnet will result in an IP address conflict message, and the DNS64 address for the entry point will not be configured as expected. This issue occurs when IPv6 has not been deployed on the internal interfaces of the servers on the corporate network. To prevent this problem run the following Windows PowerShell command on all current and future Remote Access servers:

  ```
  Set-NetIPInterface -InterfaceAlias <InternalInterfaceName> -AddressFamily IPv6 -DadTransmits 0
  ```

- If the public address specified for DirectAccess clients to connect to the Remote Access server has a suffix included in NRPT, DirectAccess might not work as expected. Ensure that the NRPT has an exemption for the public name. In a multisite deployment, exemptions should be added for the public names of all entry points. Note that if force tunneling is enabled these exemptions are added automatically. They are removed if force tunneling is disabled.

- When using the Windows PowerShell cmdlet **Disable-DAMultiSite**, the WhatIf and Confirm parameters have no effect, and Multisite will be disabled and Windows 7 GPOs will be removed.

- When Windows 7 clients using DCA in a Multisite deployment are upgraded to Windows 8, the Network Connectivity Assistant will not function. This issue can be resolved in advance of the client upgrade by modifying the Windows 7 GPOs using the following Windows PowerShell cmdlets:

  ```
  Set-GPRegistryValue -Name <Windows7GpoName> -Domain <DomainName> -Key
  "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkConnectivityAssistant" -ValueName
  "TemporaryValue" -Type Dword -Value 1
  Remove-GPRegistryValue -Name <Windows7GpoName> -Domain <DomainName> -Key
  "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkConnectivityAssistant"
  ```

  In the event that the client has already been upgraded, then move the client computer to the Windows 8 security group.

- When modifying domain controller settings using the Windows PowerShell cmdlet **Set-DAEntryPointDC**, if the ComputerName parameter specified is a Remote Access server in an entry point other than the last one added to the Multisite deployment, a warning will be displayed indicating that the server specified will not be updated until the next policy refresh. The actual server(s) that was not updated can be seen using the **Configuration Status** in the **DASHBOARD** of the **Remote Access Management Console**. This will not cause any functional problems, however, you can run **gpupdate /force** on the server(s) that was not updated to get the configuration status updated immediately.

- When multisite is deployed in an IPv4-only corporate network, changing the internal network IPv6 prefix also changes the DNS64 address, but does not update the address on firewall rules that allow DNS queries to the DNS64 service. To resolve this issue, run the following Windows PowerShell commands after changing the internal network IPv6 prefix:

```
$dns64Address = (Get-DAClientDnsConfiguration).NrptEntry | ?{ $_.DirectAccessDnsServers -match
':3333::1' } | Select-Object -First 1 -ExpandProperty DirectAccessDnsServers

$serverGpoName = (Get-RemoteAccess).ServerGpoName

$serverGpoDc = (Get-DAEntryPointDC).DomainControllerName

$gpoSession = Open-NetGPO -PolicyStore $serverGpoName -DomainController $serverGpoDc

Get-NetFirewallRule -GPOSession $gpoSession | ? {$_.Name -in @('0FDEEC95-1EA6-4042-8BA6-
6EF5336DE91A', '24FD98AA-178E-4B01-9220-D0DADA9C8503')} |  Set-NetFirewallRule -LocalAddress
$dns64Address

Save-NetGPO -GPOSession $gpoSession
```

- If DirectAccess was deployed when an existing ISATAP infrastructure was present, when removing an entry point that was an ISATAP host, the IPv6 address of the DNS64 service will be removed from the DNS server addresses of all DNS suffixes in the NRPT.

  To resolve this issue, in the **Infrastructure Server Setup** wizard, on the **DNS** page, remove the DNS suffixes that were modified and add them again with the correct DNS server addresses, by clicking **Detect** on the **DNS Server Addresses** dialog box.

Plan a Multisite Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016, Windows Server 2012 combine DirectAccess and Routing and Remote Access Service (RRAS) VPN into a single Remote Access role. This overview provides an introduction to the planning steps required in order to deploy Windows Server 2016 or Windows Server 2012 Remote Access in a multisite configuration.

1. Deploy a Single DirectAccess Server with Advanced Settings. This step includes planning for the infrastructure required to deploy a single server. It includes planning for network and server settings, certificate requirements, DNS settings, network location server deployment, DirectAccess management servers, Active Directory settings, and Group Policy objects (GPOs).
2. Step 2 Plan the multisite infrastructure. This step includes Active Directory and GPO planning, and DNS configuration.
3. Step 3 Plan the Multisite Deployment. This step includes planning certificate settings, network location server configuration, client entry point settings, IPv6 prefix settings, and optionally global load balancing settings.

> **NOTE**
>
> Record your planning decisions for Remote Access advanced deployment. This record can be used as a job aid for everyone involved in completing the deployment steps.

After you have completed these planning steps, see Configuring a multisite deployment.

Step 1 Plan an Advanced Single Server Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first step in planning a Remote Access with one-time password (OTP) client authentication deployment is to plan and configure an advanced single server deployment.

Plan a single server deployment

Before you deploy Remote Access with OTP, make sure that you have completed all the steps to deploy a single Remote Access server. See Deploy a Single DirectAccess Server with Advanced Settings.

Step 2 Plan the Multisite Infrastructure

12/9/2022 • 12 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The next step in deploying Remote Access in a multisite topology is to complete the multisite infrastructure planning; including, Active Directory, security groups, and Group Policy Objects.

2.1 Plan Active Directory

A Remote Access multisite deployment can be configured in a number of topologies:

- **Single Active Directory site, multiple entry points**-In this topology, you have a single Active Directory site for your entire organization with fast intranet links throughout the site, but you have multiple Remote Access servers deployed throughout your organization, each acting as an entry point. A geographical example of this topology is to have a single Active Directory site for the United States with entry points on the East coast and the West coast.

- **Multiple Active Directory sites, multiple entry points**-In this topology, you have two or more Active Directory sites with a Remote Access server deployed as an entry point for each site. Each Remote Access server is associated with the Active Directory domain controller for the site. A geographical example of this topology is to have an Active Directory site for the United States and one for Europe with a single entry point for each site. Note that if you have multiple Active Directory sites you do not need to have an entry point associated with each site. In addition, some Active Directory sites can have more than one entry point associated with it.

In a multisite entry point, you can configure a single Remote Access server, multiple Remote Access servers, or a Remote Access server clusters.

Active Directory best practices and recommendations

Note the following recommendations and constraints for Active Directory deployment in a multisite scenario:

1. Each Active Directory site can contain one or more Remote Access servers, or a server cluster, functioning as multisite entry points for client computers. However an Active Directory site is not required to have an entry point.

2. A multisite entry point can only be associated with a single Active Directory site. When client computers running Windows 8 connect to a specific entry point, they are considered as belonging to the Active Directory site associated with that entry point.

3. It is recommended that each Active Directory site has a domain controller. The domain controller can be read-only.

4. If each Active Directory site contains a domain controller, The GPO for a server in the entry point is managed by one of the domain controllers in the Active Directory site associated with the endpoint. If there are no write-enabled domain controllers in that site, then the GPO for a server is managed on a write-enabled domain controller that is found closest to the first Remote Access server that is configured in the entry point. Closest is determined by a link cost calculation. Note that in this scenario, after making configuration changes there might be a delay when replicating between the domain controller managing the GPO and the read-only domain controller in the server's Active Directory site.

5. Client GPOs and optional application server GPOs are managed on the domain controller running as the Primary Domain Controller (PDC) emulator. This means that client GPOs are not necessarily managed in the Active Directory site containing the entry point to which clients connect.

6. If the domain controller for an Active Directory site is unreachable, the Remote Access server will connect to an alternate domain controller in the site (if available). If not, it connects to the domain controller for another site to retrieve an updated GPO and to authenticate clients. In both cases, the Remote Access Management console and PowerShell cmdlets cannot be used to retrieve or modify configuration settings until the domain controller is available. Note the following:

a. If the server running as the PDC emulator is unavailable, you must designate an available domain controller that has updated GPOs as the PDC emulator.

b. If the domain controller that manages a server GPO is unavailable, use the Set-DAEntryPointDC PowerShell cmdlet to associate a new domain controller with the entry point. The new domain controller should have up-to-date GPOs before running the cmdlet.

2.2 Plan security groups

During deployment of a single server with advanced settings, all client computers accessing the internal network via DirectAccess were gathered into a security group. In a multisite deployment, this security group is used for Windows 8 client computers only. For a multisite deployment, Windows 7 client computers will be gathered into separate security groups for each entry point in the multisite deployment. For example, if you previously grouped all client computers in the group DA_Clients, you must now remove any Windows 7 computers from that group and put them in a different security group. For example, in the multiple Active Directory sites, multiple entry points topology, you create a security group for the United States entry point (DA_Clients_US) and one for the Europe entry point (DA_Clients_Europe). Place any Windows 7 client computers located in the United States in the DA_Clients_US group and any located in Europe in the DA_Clients_Europe group. If you do not have any Windows 7 client computers, you do not need to plan security groups for Windows 7 computers.

Required security groups are as follows:

- One security group for all Windows 8 client computers. It is recommended to create a unique security group for these clients for each domain.
- A unique security group containing Windows 7 client computers for each entry point. It is recommended to create a unique group for each domain. For example: Domain1\DA_Clients_Europe; Domain2\DA_Clients_Europe; Domain1\DA_Clients_US; Domain2\DA_Clients_US.

2.3 Plan Group Policy Objects

DirectAccess settings configured during Remote Access deployment are collected into GPOs. Your single server deployment already uses GPOs for DirectAccess clients, the Remote Access server, and optionally for application servers. A multisite deployment requires the following GPOs:

- A server GPO for each entry point.
- A GPO for each domain containing client computers running Windows 8.
- A GPO for each entry point and each domain containing Windows 7 client computers.

GPOs can be configured as follows:

- **Automatically**-You can specify that GPOs are created automatically by Remote Access. A default name is specified for each GPO, and can be modified.
- **Manually**-You can use GPOs that have been created manually by the Active Directory administrator.

> **NOTE**
> Once DirectAccess is configured to use specific GPOs, it cannot be configured to use different GPOs.

2.3.1 Automatically-created GPOs

Note the following when using automatically-created GPOs:

- Automatically created GPOs are applied according to the location and link target parameter, as follows:

  - For the server GPO, both the location and link parameters point to the domain containing the Remote Access server.
  - For client GPOs, the link target is set to the root of the domain in which the GPO was created. A GPO is created for each domain that contains client computers, and the GPO will be linked to the root of each domain. .
- For automatically-created GPOs, to apply DirectAccess settings the Remote Access server administrator requires the following permissions:
  - GPO create permissions for required domains.
  - Link permissions for all the selected client domain roots.
  - Permission to create the WMI filter for GPOs is required if DirectAccess was configured to work on mobile computers only.
  - Link permissions for the roots of domains associated with the entry points (the server GPO domains)
  - It is recommended that the Remote Access administrator has GPO read permissions for each required domain. This enables Remote Access to verify that GPOs with duplicate names do not exist when creating GPOs for the multisite deployment.
  - Active Directory replication permissions on domains associated with entry points. This is because when initially adding entry points, the server GPO for the entry point is created on the domain controller closest to that entry point. However, since link creation is supported on the PDC emulator only, the GPO must be replicated from the domain controller on which it was created to the domain controller running as the PDC emulator before creating the link.

Note that if the correct permissions for replication and linking GPOs do not exist, a warning is issued. The Remote Access operation will continue but replication and linking will not occur. If a link warning is issued links will not be created automatically, even after the permissions are in place. Instead the administrator will need to create the links manually.

2.3.2 Manually created GPOs

Note the following when using manually-created GPOs:

- The following GPOs should be created manually for the multisite deployment:
  - **Server GPO**-A server GPO for each entry point (in the domain in which the entry point is located). This GPO will be applied on each Remote Access server in the entry point.
  - **Client GPO (Windows 7)**-A GPO for each entry point and each domain containing Windows 7 client computers that will connect to entry points in the multisite deployment. For example Domain1\DA_W7_Clients_GPO_Europe; Domain2\DA_W7_Clients_GPO_Europe; Domain1\DA_W7_Clients_GPO_US; Domain2\DA_W7_Clients_GPO_US. If no Windows 7 client computers will connect to entry points, GPOs are not required.
- There is no requirement to create additional GPOs for Windows 8 client computers. A GPO for each domain containing client computers was already created when the single Remote Access server was deployed. In a multisite deployment these client GPOs will function as the GPOs for Windows 8 clients.
- The GPOs should exist before clicking the Commit button in the multisite deployment wizards.
- When using manually created GPOs a search is made for a link to the GPO in the entire domain. If the GPO is not linked in the domain then a link is automatically created in the domain root. If the required permissions to create the link are not available a warning is issued.

- When using manually-created GPOs, to apply DirectAccess settings the Remote Access server administrator requires full GPO permissions (Edit, Delete, Modify security) on the manually-created GPOs.

Note that if the correct permissions for replication and linking GPOs do not exist, a warning is issued. The Remote Access operation will continue but replication and linking will not occur. If a link warning is issued links will not be created automatically, even after the permissions are in place. Instead the administrator will need to create the links manually.

2.3.3 Managing GPOs in a multi-domain controller environment

Each GPO will be managed by a specific domain controller, as follows:

- The server GPO is managed by one of the domain controllers in the Active Directory site associated with the server, or if domain controllers in that site are read-only, by a write-enabled domain controller closest to the first server in the entry point.
- Client GPOs will be managed by the domain controller running as the PDC emulator.

If you want to manually modify GPO settings note the following:

- For server GPOs, in order to identify which domain controller is associated with a specific entry point, run the PowerShell cmdlet `Get-DAEntryPointDC -EntryPointName <name of entry point>`.
- By default, when you make changes with networking PowerShell cmdlets or the Group Policy Management console, the domain controller acting as the PDC emulator is used.
- If you modify settings on a domain controller that is not the domain controller associated with the entry point (for server GPOs) or the PDC emulator (for client GPOs), note the following:
  1. Before modifying the settings, ensure that the domain controller is replicated with an up-to-date GPO, and back up GPO settings, before making changes. If the GPO is not updated, merge conflicts during replication might occur, resulting in a corrupt Remote Access configuration.
  2. After modifying the settings, you must wait for changes to replicate to the domain controller that is associated with the GPOs. Do not make additional changes using the Remote Access Management console or Remote Access PowerShell cmdlets until replication is complete. If a GPO is edited on two different domain controllers before replication is complete, merge conflicts might occur, resulting in a corrupt configuration
- Alternatively you can change the default setting using the **Change Domain Controller** dialog box in the Group Policy Management console, or using the **Open-NetGPO** PowerShell cmdlet, so that changes made using the console or the networking cmdlets use the domain controller you specify.
  1. To do this in the Group Policy Management console, right-click the domain or sites container and click **Change Domain Controller**.
  2. To do this in PowerShell, specify the DomainController parameter for the Open-NetGPO cmdlet. For example, to enable the private and public profiles in Windows Firewall on a GPO named domain1\DA_Server_GPO _Europe using a domain controller named europe-dc.corp.contoso.com, do the following:

```
$gpoSession = Open-NetGPO -PolicyStore "domain1\DA_Server_GPO _Europe" -DomainController
"europe-dc.corp.contoso.com"
Set-NetFirewallProfile -GpoSession $gpoSession -Name @("Private","Public") -Enabled True
Save-NetGPO -GpoSession $gpoSession
```

Modifying domain controller association

To maintain the configuration consistency in a multisite deployment, it is important to make sure that each GPO

is managed by a single domain controller. In some scenarios, it may be required to assign a different domain controller for a GPO:

- **Domain controller maintenance and downtime**-When the domain controller that manages a GPO is not available, it may be required to manage the GPO on a different domain controller.
- **Optimization of configuration distribution**-After network infrastructure changes, it may be required to manage the server GPO of an entry point on a domain controller in the same Active Directory site as the entry point.

2.4 Plan DNS

Note the following when planning DNS for a multisite deployment:

1. Client computers use the ConnectTo address in order to connect to the Remote Access server. Each entry point in your deployment requires a different ConnectTo address. Each entry point ConnectTo address must be available in the public DNS and the address that you choose must match the subject name of the IP-HTTPS certificate that you deploy for the IP-HTTPS connection.
2. In addition, Remote Access enforces symmetric routing; therefore, only Teredo and IP-HTTPS clients can connect when a multisite deployment is enabled. To allow native IPv6 clients to connect, the ConnectTo address (the IP-HTTPS URL) must resolve to both the external (Internet-facing) IPv6 and IPv4 addresses on the Remote Access server.
3. Remote Access creates a default web probe that is used by DirectAccess client computers to verify connectivity to the internal network. During configuration of the single server the following names should have been registered in DNS:

   a. directaccess-WebProbeHost-should resolve to the internal IPv4 address of the Remote Access server, or to the IPv6 address in an IPv6-only environment.

   b. directaccess-CorpConnectivityHost-should resolve to a localhost (loopback) address (either ::1 or 127.0.0.1, depending on whether IPv6 is deployed in the corporate network).

   In a multisite deployment an additional DNS entry for directaccess-WebProbeHost must be created for each entry point. When adding an entry point, Remote Access tries to automatically create this additional directaccess-WebProbeHost entry. However, if it fails a warning will be shown and you must create the entry manually.

   > **NOTE**
   >
   > When DNS scavenging is enabled in your DNS infrastructure, it is recommended to disable scavenging on the DNS entries created automatically by Remote Access.

Step 3 Plan the Multisite Deployment

12/9/2022 • 17 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After planning the multisite infrastructure, plan any additional certificate requirements, how client computers select entry points, and IPv6 addresses assigned in your deployment.

The following sections provide detailed planning information.

3.1 Plan IP-HTTPS certificates

When you configure the entry points, you configure each entry point with a specific ConnectTo address. The IP-HTTPS certificate for each entry point must match the ConnectTo address. Note the following when obtaining the certificate:

- You cannot use self-signed certificates in a multisite deployment.
- Using a public CA is recommended, so that CRLs are readily available.
- In the subject field, specify either the IPv4 address of the external adapter of Remote Access server (if the ConnectTo address has been specified as an IP address and not a DNS name), or the FQDN of the IP-HTTPS URL.
- The common name of the certificate should match the name of the IP-HTTPS website. Use of a wildcard URL that matches the ConnectTo DNS name is also supported.
- IP-HTTPS certificates can use wildcards in the subject name. The same wildcard certificate can be used for all entry points.
- For the Enhanced Key Usage field, use the Server Authentication object identifier (OID).
- If you are supporting client computers running Windows 7 in the multisite deployment, in the CRL Distribution Points field, specify a CRL distribution point that is accessible by DirectAccess clients that are connected to the Internet. This is not required for clients running Windows 8 (by default the CRL revocation check is disabled for IP-HTTPS on these clients).
- The IP-HTTPS certificate must have a private key.
- The IP-HTTPS certificate must be imported directly into the personal store of the computer, and not of the user.

3.2 Plan the network location server

The network location server website can be hosted on the Remote Access server or on another server in your organization. If you host the network location server on the Remote Access server, the website is created automatically when you deploy Remote Access. If you host the network location server on another server running a Windows operating system in your organization, you must make sure that Internet Information Services (IIS) is installed to create the website.

3.2.1 Certificate requirements for the network location server

Make sure that the network location server website meets the following requirements for certificate deployment:

- It requires an HTTPS server certificate.
- If the network location server is located on the Remote Access server, and you selected to use a self-signed certificate when you deployed the single Remote Access server, you must reconfigure the single server deployment to use a certificate issued by an internal CA.
- DirectAccess client computers must trust the CA that issued the server certificate to the network location server website.
- DirectAccess client computers on the internal network must be able to resolve the name of the network location server website.
- The network location server website must be highly available to computers on the internal network.
- The network location server must not be accessible to DirectAccess client computers on the Internet.
- The server certificate must be checked against a Certificate Revocation List (CRL).
- Wildcard certificates are not supported when the network location server is hosted on the Remote Access server.

When obtaining the website certificate to use for the network location server, note the following:

1. In the Subject field, specify either an IP address of the intranet interface of the network location server or the FQDN of the network location URL. Note that you should not specify an IP address if the network location server is hosted on the Remote Access server. This is because the network location server must use the same subject name for all entry points, and not all entry points have the same IP address.
2. For the Enhanced Key Usage field, use the Server Authentication OID.
3. For the CRL Distribution Points field, use a CRL distribution point that is accessible by DirectAccess clients that are connected to the intranet.

3.2.2DNS for the network location server

If you host the network location server on the Remote Access server, you must add a DNS entry for the network location server website for every entry point in your deployment. Note the following:

- The subject name of the first network location server certificate in the multisite deployment is used as the network location server URL for all entry points, therefore the subject name and the network location server URL cannot be the same as the computer name of the first Remote Access server in the deployment. It must be an FQDN dedicated for the network location server.
- The service provided by the network location server traffic is balanced across entry points using DNS, and therefore there should be a DNS entry with the same URL for each entry point, configured with the internal IP address of the entry point.
- All entry points must be configured with a network location server certificate with the same subject name (that matches the network location server URL).
- The network location server infrastructure (DNS and certificate settings) for an entry point must be created before adding the entry point.

3.3 Plan the IPsec root certificate for all Remote Access servers

Note the following when planning for IPsec client authentication in a multisite deployment:

1. If you opted to use the built-in Kerberos proxy for computer authentication when you set up the single Remote Access server, you must change the setting to use computer certificates issued by an internal CA, since Kerberos proxy is not supported for a multisite deployment.

2. If you used a self-signed certificate, you must reconfigure the single server deployment to use a certificate issued by an internal CA.
3. For IPsec authentication to succeed during client authentication, all Remote Access servers must have a certificate issued by the IPsec root or intermediate CA, and with the Client Authentication OID for Enhanced Key Usage.
4. The same IPsec root or intermediate certificate must be installed on all of the Remote Access servers in the multisite deployment.

3.4 Plan global server load balancing

In a multisite deployment, you can additionally configure a global server load balancer. A global server load balancer can be useful to your organization if your deployment covers a large geographical distribution because it can distribute traffic load between the entry points. The global server load balancer can be configured to provide DirectAccess clients with the entry point information of the closest entry point. The process works as follows:

1. Client computers running Windows 10 or Windows 8 have a list of global server load balancer IP addresses, each associated with an entry point.
2. The Windows 10 or Windows 8 client computer attempts to resolve the FQDN of the global server load balancer in the public DNS to an IP address. If the resolved IP address is listed as the global server load balancer IP address of an entry point, the client computer automatically selects that entry point and connects to its IP-HTTPS URL (ConnectTo address), or to its Teredo server IP address. Note that the IP address of the global server load balancer does not need to be identical to the ConnectTo address or to the Teredo server address of the entry point, since the client computers never try to connect to the global server load balancer IP address.
3. If the client computer is behind a web proxy (and cannot use DNS resolution), or if the global server load balancer FQDN does not resolve to any configured global server load balancer IP address, then an entry point will be selected automatically using an HTTPS probe to the IP-HTTPS URLs of all entry points. The client will connect to server that responds first.

For a list of global server load balancing devices that support Remote Access, go to the Find a Partner page at Microsoft Server and Cloud Platform.

3.5 Plan DirectAccess client entry point selection

When you configure a multisite deployment, by default, Windows 10 and Windows 8 client computers are configured with the information required to connect to all entry points in the deployment and to automatically connect to a single entry point based on a selection algorithm. You can also configure your deployment to allow Windows 10 and Windows 8 client computers to manually select the entry point to which they will connect. If a Windows 10 or Windows 8 client computer is currently connected to the United States entry point and automatic entry point selection is enabled, if the United States entry point becomes unreachable, after a few minutes the client computer will attempt to connect through the Europe entry point. Using automatic entry point selection is recommended; however, allowing manual entry point selection enables end users to connect to a different entry point based on current network conditions. For example, if a computer is connected to the United States entry point and the connection to the internal network becomes much slower than expected. In this situation, the end user can manually select to connect to the Europe entry point to improve the connection to the internal network.

> **NOTE**
> After an end user selects an entry point manually, the client computer will not revert to automatic entry point selection. That is, if the manually selected entry point becomes unreachable, the end user must either revert to automatic entry point selection, or manually select another entry point.

Windows 7 client computers are configured with the information required to connect to a single entry point in the multisite deployment. They cannot store the information for multiple entry points simultaneously. For example, a Windows 7 client computer can be configured to connect to the United States entry point, but not the Europe entry point. If the United States entry point is unreachable, the Windows 7 client computer will lose connectivity to the internal network until the entry point is reachable. The end user cannot make any changes to attempt to connect to the Europe entry point.

3.6 Plan prefixes and routing

Internal IPv6 prefix

During deployment of the single Remote Access server you planned the internal network IPv6 prefixes Note the following in a multisite deployment:

1. If you included all of your Active Directory sites when you configured your single server Remote Access deployment, the internal network IPv6 prefixes will already be defined in the Remote Access Management console.
2. If you create additional Active Directory sites for multisite deployment, you must plan new IPv6 prefixes for the additional sites and define them in Remote Access. Note that IPv6 prefixes can only be configured using the Remote Access Management console or PowerShell cmdlets if IPv6 is deployed in the internal corporate network.

IPv6 prefix for DirectAccess client computers (IP-HTTPS prefix)

1. If IPv6 is deployed in the internal corporate network, you must plan an IPv6 prefix to assign to DirectAccess client computers in any additional entry points in your deployment.
2. Ensure that the IPv6 prefixes to assign to DirectAccess client computers in each entry point are distinct and that there is no overlap in the IPv6 prefixes.
3. If IPv6 is not deployed in the corporate network, an IP-HTTPS prefix for each entry point will be automatically selected when adding the entry point.

IPv6 prefix for VPN clients

If you deployed VPN on the single Remote Access server, note the following:

1. Adding an IPv6 VPN prefix to an entry point is only required if you want to allow VPN client IPv6 connectivity to the corporate network.
2. The VPN prefix can only be configured on an entry point using the Remote Access Management console or PowerShell cmdlet if IPv6 is deployed in the internal corporate network, and if VPN is enabled on the entry point.
3. The VPN prefix should be unique in each entry point and should not overlap with other VPN or IP-HTTPS prefixes.
4. If IPv6 is not deployed in the corporate network, VPN clients connecting to the entry point will not be assigned an IPv6 address.

Routing

In a multisite deployment symmetric routing is enforced using Teredo and IP-HTTPS. When IPv6 is deployed in

the corporate network note the following:

1. The Teredo and IP-HTTPS prefixes of each entry point must be routable across the corporate network to their associated Remote Access server.
2. The routes must be configured in the corporate network routing infrastructure.
3. For each entry point there should be one to three routes in the internal network:
   a. IP-HTTPS prefix-This prefix is chosen by the administrator in the Add an Entry Point wizard.
   b. VPN IPv6 prefix (optional). This prefix can be chosen after enabling VPN for an entry point
   c. Teredo prefix (optional). This prefix is relevant only if the Remote Access server is configured with two consecutive public IPv4 addresses on the external adapter. The prefix is based on the first public IPv4 address of the address pair. For example if the external addresses are:
      a. www.xxx.yyy.zzz
      b. www.xxx.yyy.zzz+1

      Then the Teredo prefix to configure is 2001:0:WWXX:YYZZ::/64, where WWXX:YYZZ is the hexadecimal representation of the IPv4 address www.xxx.yyy.zzz.

      Note that you can use the following script to calculate the Teredo prefix:

```
$TeredoIPv4 = (Get-NetTeredoConfiguration).ServerName # Use for a Remote Access server that is
already configured
$TeredoIPv4 = "20.0.0.1" # Use for an IPv4 address

    [Byte[]] $TeredoServerAddressBytes = `
    [System.Net.IPAddress]::Parse("2001::").GetAddressBytes()[0..3] + `
    [System.Net.IPAddress]::Parse($TeredoIPv4).GetAddressBytes() + `
    [System.Net.IPAddress]::Parse("::").GetAddressBytes()[0..7]

Write-Host "The server's Teredo prefix is
$([System.Net.IPAddress]$TeredoServerAddressBytes)/64"
```

   d. All of the above routes must be routed to the IPv6 address on the internal adapter of the Remote Access server (or to the internal virtual IP (VIP) address for a load balanced entry point).

> **NOTE**
> When IPv6 is deployed in the corporate network and Remote Access server administration is performed remotely over DirectAccess, routes for the Teredo and IP-HTTPS prefixes of all other entry points must be added to each Remote Access server so that the traffic will be forwarded to the internal network.

Active Directory site-specific IPv6 prefixes

When a client computer running Windows 10 or Windows 8 is connected to an entry point, the client computer is immediately associated with the Active Directory site of the entry point, and is configured with IPv6 prefixes associated with the entry point. The preference is for client computers to connect to resources using these IPv6 prefixes, since they are configured dynamically in the IPv6 prefix policy table with higher precedence when connecting to an entry point.

If your organization uses an Active Directory topology with site-specific IPv6 prefixes (for example an internal resource FQDN app.corp.com is hosted in both North America and Europe with a site-specific IP address in each location) this is not configured by default using the Remote Access console, and site-specific IPv6 prefixes are not configured for each entry point. If you do want to enable this optional scenario, you need to configure each entry point with the specific IPv6 prefixes that should be preferred by client computers connecting to a specific

entry point. Do this as follows:

1. For each GPO used for Windows 10 or Windows 8 client computers, run the Set-DAEntryPointTableItem PowerShell cmdlet
2. Set the EntryPointRange parameter for the cmdlet with the site-specific IPv6 prefixes. For example, to add the site-specific prefixes 2001:db8:1:1::/64 and 2001:db:1:2::/64 to an entry point called Europe, run the following

```
$entryPointName = "Europe"
$prefixesToAdd = @("2001:db8:1:1::/64", "2001:db8:1:2::/64")
$clientGpos = (Get-DAClient).GpoName
$clientGpos | % { Get-DAEntryPointTableItem -EntryPointName $entryPointName -PolicyStore $_ | %{ Set-
DAEntryPointTableItem -PolicyStore $_.PolicyStore -EntryPointName $_.EntryPointName -EntryPointRange
($_.EntryPointRange) + $prefixesToAdd}}
```

3. When modifying the EntryPointRange parameter, ensure that you do not remove the existing 128-bit prefixes which belong to the IPsec tunnel endpoints and the DNS64 address.

3.7 Plan the transition to IPv6 when multisite Remote Access is deployed

Many organizations use the IPv4 protocol on the corporate network. With the exhaustion of available IPv4 prefixes, many organizations are making the transition from IPv4-only to IPv6-only networks.

This transition is most likely to take place in two stages:

1. From an IPv4-only to an IPv6+IPv4 corporate network.
2. From an IPv6+IPv4 to an IPv6-only corporate network.

In each part, the transition may be performed in stages. In each stage only one subnet of the network may be changed to the new network configuration. Therefore, a DirectAccess multisite deployment is required to support a hybrid deployment where, for example, some of the entry points belong to an IPv4-only subnet and others belong to an IPv6+IPv4 subnet. In addition, configuration changes during the transition processes must not break client connectivity via DirectAccess.

Transition from an IPv4-only to an IPv6+IPv4 corporate network

When adding IPv6 addresses to an IPv4-only corporate network, you may want to add an IPv6 address to an already deployed DirectAccess server. In addition, you may want to add an entry point or a node to a load balanced cluster with both IPv4 and IPv6 addresses to the DirectAccess deployment.

Remote Access allows you to add servers with both IPv4 and IPv6 addresses to a deployment that was originally configured with only IPv4 addresses. These servers are added as IPv4-only servers and their IPv6 addresses are ignored by DirectAccess; consequently, your organization cannot take advantage of the benefits of native IPv6 connectivity on these new servers.

To transform the deployment to an IPv6+IPv4 deployment and take advantage of the native IPv6 capabilities, you must reinstall DirectAccess. To maintain client connectivity throughout the reinstallation see Transition from an IPv4-only to an IPv6-only deployment using dual DirectAccess deployments.

> **NOTE**
> As with an IPv4-only network, in a mixed IPv4+IPv6 network, the address of the DNS server that is used to resolve client DNS requests must be configured with the DNS64 that is deployed on Remote Access servers themselves, and not with a corporate DNS.

Transition from an IPv6+IPv4 to an IPv6-only corporate network

DirectAccess enables you to add IPv6-only entry points only if the first Remote Access server in the deployment originally had either both IPv4 and IPv6 addresses or only an IPv6 address. That is, you cannot transition from an IPv4-only network to an IPv6-only network in a single step without reinstalling DirectAccess. To transition directly from an IPv4-only network to an IPv6-only network, see Transition from an IPv4-only to an IPv6-only deployment using dual DirectAccess deployments.

After you have completed the transition from an IPv4-only deployment to an IPv6+IPv4 deployment, you can transition to an IPv6-only network. During, and after the transition, note the following:

- If any IPv4-only backend servers remain in the corporate network, they will not be reachable to clients that connect through the IPv6-only entry points.
- When adding IPv6-only entry points to an IPv4+IPv6 deployment, DNS64 and NAT64 will not be enabled on the new servers. Clients that connect to these entry points will be automatically configured to use the corporate DNS servers.
- If you need to delete IPv4 addresses from a deployed server, you must remove the server from the DirectAccess deployment, remove its IPv4 corporate network address, and add it again to the deployment.

To support client connectivity to the corporate network, you must ensure that the network location server can be resolved by the corporate DNS to its IPv6 address. An additional IPv4 address can be set as well, but isn't required.

Transition from an IPv4-only to an IPv6-only deployment using dual DirectAccess deployments

The transition from an IPv4-only to an IPv6-only corporate network cannot be done without reinstalling the DirectAccess deployment. To maintain client connectivity during the transition, you can use another DirectAccess deployment. Dual deployment is required when the first transition stage finishes (IPv4-only network upgraded to IPv4+IPv6) and you intend to prepare for a future transition to an IPv6-only corporate network orto take advantage of the native IPv6 connectivity benefits. The dual deployment is described in the following general steps:

1. Install a second DirectAccess deployment. You can install DirectAccess on new servers, or remove servers from the first deployment and use them for the second deployment.

   > **NOTE**
   >
   > When installing an additional DirectAccess deployment alongside a current one, make sure that no two entry points share the same client prefix.
   >
   > If you install DirectAccess using the Getting Started Wizard or with the cmdlet `Install-RemoteAccess`, Remote Access automatically sets the client prefix of the first entry point in the deployment to a default value of <IPv6 subnet_prefix>:1000::/64. If needed, you must change the prefix.

2. Remove the chosen client security groups from the first deployment.
3. Add the client security groups to the second deployment.

   > **IMPORTANT**
   >
   > To maintain client connectivity throughout the process, you must add the security groups to the second deployment immediately after removing them from the first. This ensures that clients will not be updated with either two or zero DirectAccess GPOs. Clients will start using the second deployment once they retrieve and update their client GPO.

4. Optional: Remove the DirectAccess entry points from the first deployment and add those servers as new entry points in the second.

When you have completed the transition, you can uninstall the first DirectAccess deployment. When uninstalling, the following issues may occur:

- If the deployment was configured to support only clients on mobile computers, the WMI filter will be deleted. If the client security groups of the second deployment include desktop computers, the DirectAccess client GPO will not filter desktop computers and may cause issues on them. If a mobile computers filter is needed, recreate it by following the instructions on Create WMI Filters for the GPO.
- If both deployments were originally created on the same Active Directory domain, the DNS probe entry which points to localhost will be deleted and may cause client connectivity issues. For example, clients may connect using IP-HTTPS rather than Teredo, or switch between DirectAccess multisite entry points. In this case, you must add the following DNS entry to the corporate DNS:
  - Zone: domain name
  - Name: directaccess-corpConnectivityHost
  - IP address: ::1
  - Type: AAAA

Configure a Multisite Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016 combines DirectAccess and Remote Access Service (RAS) VPN into a single Remote Access role. This overview provides an introduction to the configuration steps required in order to deploy a single Windows Server 2016 or Windows Server 2012 Remote Access multisite deployment.

- Step 1: Deploy a Single DirectAccess Server with Advanced Settings. Install and configure a single Remote Access server. The multisite deployment requires you to install a single server before configuring a multisite deployment.
- Step 2: Configure the multisite infrastructure. For a multisite deployment you must configure additional Active Directory sites and domain controllers. Additional security groups and Group Policy Objects (GPOs) are also required if you are not using automatically configured GPOs.
- Step 3: Configure the multisite deployment-Install the Remote Access role on additional Remote Access servers, enable the multisite deployment, and configure the additional servers as entry points for the deployment.
- Step 4: Verify the multisite deployment

Step 1 Implement a Single Server Remote Access Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first configuration step to deploy Remote Access in a multisite topology is to implement an advanced single server deployment and then plan to add servers to each multisite entry point.

Implement a single server deployment

Before you can configure a multisite deployment, you must configure an advanced single server Remote Access deployment as described in Deploy a Single DirectAccess Server with Advanced Settings.

See also

- Step 2: Configure the multisite infrastructure

Step 2 Configure the Multisite Infrastructure

12/9/2022 • 15 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2, Windows Server 2012

To configure a multisite deployment, there are a number of steps required to modify network infrastructure settings including: configuring additional Active Directory sites and domain controllers, configuring additional security groups, and configuring Group Policy Objects (GPOs) if you are not using automatically configured GPOs.

TASK	DESCRIPTION
2.1. Configure additional Active Directory sites	Configure additional Active Directory sites for the deployment.
2.2. Configure additional domain controllers	Configure additional Active Directory domain controllers as required.
2.3. Configure security groups	Configure security groups for any Windows 7 client computers.
2.4. Configure GPOs	Configure additional Group Policy Objects as required.

NOTE

This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

2.1. Configure additional Active Directory sites

All entry points can reside in a single Active Directory site. Therefore, at least one Active Directory site is required for the implementation of Remote Access servers in a multisite configuration. Use this procedure if you need to create the first Active Directory site, or if you desire to use additional Active Directory sites for the multisite deployment. Use the Active Directory Sites and Services snap-in to create new sites in your organization"s network.

Membership in the **Enterprise Admins** group in the forest or the **Domain Admins** group in the forest root domain, or equivalent, at a minimum is required to complete this procedure. Review details about using the appropriate accounts and group memberships at Local and Domain Default Groups.

For more information, see Adding a Site to the Forest.

To configure additional Active Directory sites

1. On the primary domain controller, click **Start**, and then click **Active Directory Sites and Services**.
2. In the Active Directory Sites and Services console, in the console tree, right-click **Sites**, and then click **New Site**.
3. On the **New Object - Site** dialog box, in the **Name** box, enter a name for the new site.
4. In **Link Name**, click a site link object, and then click **OK** twice.

5. In the console tree, expand **Sites**, right-click **Subnets**, and then click **New Subnet**.
6. On the **New Object - Subnet** dialog box, under **Prefix**, type the IPv4 or IPv6 subnet prefix, in the **Select a site object for this prefix** list, click the site to associate with this subnet, and then click **OK**.
7. Repeat steps 5 and 6 until you have created all the subnets required in your deployment.
8. Close Active Directory Sites and Services.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

To install the Windows Feature "Active Directory module for Windows PowerShell":

```
Install-WindowsFeature "Name RSAT-AD-PowerShell
```

or add the "Active Directory PowerShell Snap-In" via OptionalFeatures.

If running the following cmdlets on Windows 7" or Windows Server 2008 R2 , then the Active Directory PowerShell module must be imported:

```
Import-Module ActiveDirectory
```

To configure an Active Directory site named "Second-Site" using the built-in DEFAULTIPSITELINK:

```
New-ADReplicationSite -Name "Second-Site"
Set-ADReplicationSiteLink -Identity "DEFAULTIPSITELINK" -sitesIncluded @{Add="Second-Site"}
```

To configure IPv4 and IPv6 subnets for the Second-Site:

```
New-ADReplicationSubnet -Name "10.2.0.0/24" -Site "Second-Site"
New-ADReplicationSubnet -Name "2001:db8:2::/64" -Site "Second-Site"
```

2.2. Configure additional domain controllers

To configure a multisite deployment in a single domain, it is recommended that you have at least one writeable domain controller for each site in your deployment.

To perform this procedure, at a minimum you must be a member of the Domain Admins group in the domain in which the domain controller is being installed.

For more information, see Installing an Additional Domain Controller.

To configure additional domain controllers

1. On the server that will act as a domain controller, in **Server Manager**, on the **Dashboard**, click **add roles and features**.
2. Click **Next** three times to get to the server role selection screen
3. On the **Select Server Roles** page, select **Active Directory Domain Services**. Click **Add Features** when prompted, and then click **Next** three times.
4. On the **Confirmation** page, click **Install**.

5. When the installation completes successfully, click **Promote this server to a domain controller**.
6. In the Active Directory Domain Services Configuration Wizard, on the **Deployment Configuration** page, click **Add a domain controller to an existing domain**.
7. In **Domain**, enter the domain name; for example, corp.contoso.com.
8. Under **Supply the credentials to perform this operation**, click **Change**. On the **Windows Security** dialog box, provide the user name and password for an account that can install the additional domain controller. To install an additional domain controller, you must be a member of the Enterprise Admins group or the Domain Admins group. When you are finished providing credentials, click **Next**.
9. On the **Domain Controller Options** page, do the following:
   a. Make the following selections:
      - **Domain Name System (DNS) server**"This option is selected by default so that your domain controller can function as a Domain Name System (DNS) server. If you do not want the domain controller to be a DNS server, clear this option.

        If the DNS server role is not installed on the Primary Domain Controller (PDC) emulator in the forest root domain, then the option to install DNS server on an additional domain controller is not available. As a workaround in this situation, you can install the DNS server role before or after the AD DS installation.

        > **NOTE**
        > If you select the option to install DNS server, you might receive a message that indicates that a DNS delegation for the DNS server could not be created and that you should manually create a DNS delegation to the DNS server to ensure reliable name resolution. If you are installing an additional domain controller in either the forest root domain or a tree root domain, you do not have to create the DNS delegation. In this case, click **Yes** and disregard the message.

      - **Global Catalog (GC)**"This option is selected by default. It adds the global catalog, read-only directory partitions to the domain controller, and it enables global catalog search functionality.
      - **Read-only domain controller (RODC)**"This option is not selected by default. It makes the additional domain controller read only; that is, it makes the domain controller an RODC.

   b. In **Site name**, select a site from the list.
   c. Under **Type the Directory Services Restore Mode (DSRM) password**, in **Password** and **Confirm password**, type a strong password twice, and then click **Next**. This password must be used to start AD DS in DSRM for tasks that must be performed offline.
10. On the **DNS Options** page, select the **Update DNS delegation** check box if you want to update DNS delegation during role installation, and then click **Next**.
11. On the **Additional Options** page, type or browse to the volume and folder locations for the database file, the directory service log files, and the system volume (SYSVOL) files. Specify replication options as required, and then click **Next**.
12. On the **Review Options** page, review the installation options, and then click **Next**.
13. On the **Prerequisites Check** page, after the prerequisites are validated, click **Install**.
14. Wait until the wizard completes the configuration, and then click **Close**.

15. Restart the computer if it did not restart automatically.

2.3. Configure security groups

A multisite deployment requires an additional security group for Windows 7 client computers for every entry point in the deployment that allows access to Windows 7 client computers. If there are multiple domains containing Windows 7 client computers, then it is recommended to create a security group in each domain for the same entry point. Alternatively, one universal security group containing the client computers from both domains can be used. For example, in an environment with two domains, if you want to allow access to Windows 7 client computers in entry points 1 and 3, but not in entry point 2, then create two new security groups to contain the Windows 7 client computers for each entry point in each of the domains.

To configure additional security groups

1. On the primary domain controller, click **Start**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click the folder in which you want to add a new group, for example, corp.contoso.com/Users. Point to **New**, and then click **Group**.
3. On the **New Object - Group** dialog box, under **Group name**, type the name of the new group, for example, Win7_Clients_Entrypoint1.
4. Under **Group scope**, click **Universal**, under **Group type**, click **Security**, and then click **OK**.
5. To add computers to the new security group, double-click the security group, and on the **<Group_Name> Properties** dialog box, click the **Members** tab.
6. On the **Members** tab, click **Add**.
7. Select the Windows 7 computers to add to this security group, and then click **OK**.
8. Repeat this procedure to create a security group for every entry point as required.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

To install the Windows Feature "Active Directory module for Windows PowerShell":

```
Install-WindowsFeature "Name RSAT-AD-PowerShell
```

or add the "Active Directory PowerShell Snap-In" via OptionalFeatures.

If running the following cmdlets on Windows 7" or Windows Server 2008 R2 , then the Active Directory PowerShell module must be imported:

```
Import-Module ActiveDirectory
```

To configure a security group named Win7_Clients_Entrypoint1 and to add a client computer named CLIENT2:

```
New-ADGroup -GroupScope universal -Name Win7_Clients_Entrypoint1
Add-ADGroupMember -Identity Win7_Clients_Entrypoint1 -Members CLIENT2$
```

2.4. Configure GPOs

A multisite Remote Access deployment requires the following Group Policy Objects:

- A GPO for every entry point for the Remote Access server.
- A GPO for any Windows 8 client computers for each domain.
- A GPO in each domain that contains Windows 7 client computers for each entry point configured to support Windows 7 clients.

> **NOTE**
> If you do not have any Windows 7 client computers, you do not need to create GPOs for Windows 7 computers.

When you configure Remote Access, the wizard automatically creates the required Group Policy Objects if they don"t already exist. If you do not have the required permissions to create Group Policy Objects, they must be created prior to configuring Remote Access. The DirectAccess administrator must have full permissions on the GPOs (Edit + modify security + delete).

> **IMPORTANT**
> After manually creating the GPOs for Remote Access you must allow sufficient time for Active Directory and DFS replication to the domain controller in the Active Directory site that is associated with the Remote Access server. If Remote Access automatically created the Group Policy Objects, then no wait time is required.

To create Group Policy Objects, see Create and Edit a Group Policy Object.

Domain controller maintenance and downtime

When a domain controller running as the PDC emulator, or domain controllers managing server GPOs experience downtime, it is not possible to load or modify the Remote Access configuration. This does not affect client connectivity if other domain controllers are available.

To load or modify the Remote Access configuration, you can transfer the PDC emulator role to a different domain controller for the client or application server GPOs; for server GPOs, change the domain controllers that manage the server GPOs.

> **IMPORTANT**
> This operation can be performed only by a domain administrator. The impact of changing the primary domain controller is not confined to Remote Access; therefore, use caution when transferring the PDC emulator role.

> **NOTE**
> Before modifying domain controller association, make sure that all of the GPOs in the Remote Access deployment have been replicated to all of the domain controllers in the domain. If the GPO is not synchronized, recent configuration changes may be lost after modifying domain controller association, which may lead to a corrupt configuration. To verify GPO synchronization, see Check Group Policy Infrastructure Status.

To transfer the PDC emulator role

1. On the **Start** screen, type**dsa.msc**, and then press ENTER.
2. In the left pane of the Active Directory Users and Computers console, right-click **Active Directory Users and Computers**, and then click **Change Domain Controller**. On the Change Directory Server dialog box, click **This Domain Controller or AD LDS instance**, in the list click the domain controller that will be the new role holder, and then click **OK**.

> **NOTE**
> You must perform this step if you are not on the domain controller to which you want to transfer the role. Do not perform this step if you are already connected to the domain controller to which you want to transfer the role.

3. In the console tree, right-click **Active Directory Users and Computers**, point to **All Tasks**, and then click **Operations Masters**.
4. On the Operations Masters dialog box, click the **PDC** tab, and then click **Change**.
5. Click **Yes** to confirm that you want to transfer the role, and then click **Close**.

To change the domain controller that manages server GPOs

- Run the Windows PowerShell cmdlet Set-DAEntryPointDC on the Remote Access server and specify the unreachable domain controller name for the *ExistingDC* parameter. This command modifies the domain controller association for the server GPOs of the entry points that are currently managed by that domain controller.
  - To replace the unreachable domain controller "dc1.corp.contoso.com" with the domain controller "dc2.corp.contoso.com", do the following:

    ```
    Set-DAEntryPointDC "ExistingDC 'dc1.corp.contoso.com' "NewDC 'dc2.corp.contoso.com'
    "ErrorAction Inquire
    ```

  - To replace the unreachable domain controller "dc1.corp.contoso.com" with a domain controller in the closest Active Directory site to the Remote Access server "DA1.corp.contoso.com", do the following:

    ```
    Set-DAEntryPointDC "ExistingDC 'dc1.corp.contoso.com' "ComputerName 'DA1.corp.contoso.com'
    "ErrorAction Inquire
    ```

Change two or more domain controllers that manage server GPOs

In a minimal number of cases, two or more domain controllers that manage server GPOs are unavailable. If this occurs, more steps are required to change the domain controller association for the server GPOs.

Domain controller association information is stored both in the registry of the Remote Access servers and in all server GPOs. In the following example, there are two entry points with two Remote Access servers, "DA1" in "Entry point 1" and "DA2" in "Entry point 2". The server GPO of "Entry point 1" is managed in the domain controller "DC1", while the server GPO of "Entry point 2" is managed in the domain controller "DC2". Both "DC1" and "DC2" are unavailable. A third domain controller is still available in the domain, "DC3", and the data from "DC1" and "DC2" was already replicated to "DC3".

To change two or more domain controllers that manage server GPOs

1. To replace the unavailable domain controller "DC2" with the domain controller "DC3", run the following command:

```
Set-DAEntryPointDC "ExistingDC 'DC2' "NewDC 'DC3' "ComputerName 'DA2' "ErrorAction Continue
```

   This command updates the domain controller association for the "Entry point 2" server GPO in the registry of DA2 and in the "Entry point 2" server GPO itself; however, it does not update the "Entry point 1" server GPO because the domain controller that manages it is unavailable.

   > **TIP**
   > This command uses the Continue value for the *ErrorAction* parameter, which updates the "Entry point 2" server GPO despite the failure to update "Entry point 1" server GPO.

   The resulting configuration is shown in the following diagram.

2. To replace the unavailable domain controller "DC1" with the domain controller "DC3", run the following command:

```
Set-DAEntryPointDC "ExistingDC 'DC1' "NewDC 'DC3' "ComputerName 'DA2' "ErrorAction Continue
```

   This command updates the domain controller association for the "Entry point 1" server GPO in the registry of DA1 and in the "Entry point 1" and "Entry point 2" server GPOs. The resulting configuration is shown in the following diagram.

3. To synchronize the domain controller association for the "Entry point 2" server GPO in the "Entry point 1" server GPO, run the command to replace "DC2" with "DC3", and specify the Remote Access server whose

server GPO is not synchronized, in this case "DA1", for the *ComputerName* parameter.

```
Set-DAEntryPointDC "ExistingDC 'DC2' "NewDC 'DC3' "ComputerName 'DA1' "ErrorAction Continue
```

The final configuration is shown in the following diagram.

Optimization of configuration distribution

When making configuration changes, the changes are applied only after the server GPOs propagate to the Remote Access servers. To reduce the configuration distribution time, Remote Access automatically selects a writable domain controller which is closest to the Remote Access server when creating its server GPO.

In some scenarios, it may be required to manually modify the domain controller that manages a server GPO in order to optimize configuration distribution time:

- There were no writable domain controllers in the Active Directory site of a Remote Access server at the time of adding it as an entry point. A writable domain controller is now being added to the Active Directory site of the Remote Access server.
- An IP address change, or an Active Directory Sites and Subnets change may have moved the Remote Access server to a different Active Directory site.
- The domain controller association for an entry point was manually modified due to maintenance work on a domain controller, and now the domain controller is back online.

In these scenarios, run the PowerShell cmdlet `Set-DAEntryPointDC` on the Remote Access server and specify the name of the entry point you want to optimize using the parameter *EntryPointName*. You should do this only after the GPO data from the domain controller currently storing the server GPO was already fully replicated to the desired new domain controller.

> **NOTE**
> Before modifying domain controller association, make sure that all of the GPOs in the Remote Access deployment have been replicated to all of the domain controllers in the domain. If the GPO is not synchronized, recent configuration changes may be lost after modifying domain controller association, which may lead to a corrupt configuration. To verify GPO synchronization, see Check Group Policy Infrastructure Status.

To optimize the configuration distribution time, do one of the following:

- To manage the server GPO of entry point "Entry point 1" on a domain controller in the closest Active Directory site to the Remote Access server "DA1.corp.contoso.com", run the following command:

```
Set-DAEntryPointDC "EntryPointName 'Entry point 1' "ComputerName 'DA1.corp.contoso.com' "ErrorAction
Inquire
```

- To manage the server GPO of entry point "Entry point 1" on the domain controller "dc2.corp.contoso.com", run the following command:

```
Set-DAEntryPointDC "EntryPointName 'Entry point 1' "NewDC 'dc2.corp.contoso.com' "ComputerName
'DA1.corp.contoso.com' "ErrorAction Inquire
```

> **NOTE**
>
> When modifying the domain controller associated with a specific entry point, you must specify a Remote Access server that is a member of that entry point for the *ComputerName* parameter.

See also

- Step 3: Configure the multisite deployment
- Step 1: Implement a single server Remote Access deployment

Step 3 Configure the Multisite Deployment

12/9/2022 • 18 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After configuring the multisite infrastructure follow these steps to set up the Remote Access multisite deployment.

TASK	DESCRIPTION
3.1. Configure Remote Access servers	Configure additional Remote Access servers by setting up IP addresses, joining them to the domain, and installing the Remote Access role.
3.2. Grant administrator access	Grant privileges on the additional Remote Access servers to the DirectAccess administrator.
3.3. Configure IP-HTTPS for a multisite deployment	Configure the IP-HTTPS certificate used in a multisite deployment.
3.4. Configure the network location server for a multisite deployment	Configure the network location server certificate used in a multisite deployment.
3.5. Configure DirectAccess clients for a multisite deployment	Remove Windows 7 client computers from Windows 8 security groups.
3.6. Enable the multisite deployment	Enable the multisite deployment on the first Remote Access server.
3.7. Add entry points to the multisite deployment	Add additional entry points to the multisite deployment.

NOTE

This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

3.1. Configure Remote Access servers

To install the Remote Access role

1. Make sure that each Remote Access server is configured with the proper deployment topology (Edge, behind a NAT, single network interface), and corresponding routes.
2. Configure the IP addresses on each Remote Access server according to the site topology and your organization's IP addressing scheme.
3. Join each Remote Access server to an Active Directory domain.
4. In the Server Manager console, in the **Dashboard**, click **Add roles and features**.
5. Click **Next** three times to get to the server role selection screen.

6. On the **Select Server Roles** dialog, select **Remote Access**, and then click **Next**.
7. Click **Next** three times.
8. On the **Select role services** dialog, select **DirectAccess and VPN (RAS)** and then click **Add Features**.
9. Select **Routing**, select **Web Application Proxy**, click **Add Features**, and then click **Next**.
10. Click **Next**, and then click **Install**.
11. On the **Installation progress** dialog, verify that the installation was successful, and then click **Close**.

Windows PowerShell equivalent commands

Steps 1 - 3 must be performed manually, and are not accomplished using this Windows PowerShell cmdlet.

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

3.2. Grant administrator access

To grant administrator permissions

1. On the Remote Access server in the additional entry point: On the **Start** screen, type **Computer Management**, and then press ENTER.
2. In the left pane, click **Local Users and Groups**.
3. Double-click **Groups**, and then double-click **Administrators**.
4. On the **Administrators Properties** dialog box, click **Add**, and on the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Locations**.
5. On the **Locations** dialog box, in the **Location** tree, click the location that contains the user account of the DirectAccess administrator, and then click **OK**.
6. In the **Enter the object names to select**, enter the user name of the DirectAccess administrator, and then click **OK** twice.
7. On the **Administrators Properties** dialog box, click **OK**.
8. Close the Computer Management window.
9. Repeat this procedure on all Remote Access servers that will be part of the multisite deployment.

3.3. Configure IP-HTTPS for a multisite deployment

On each Remote Access server that will be added to the multisite deployment, an SSL certificate is required to verify the HTTPS connection to the IP-HTTPS web server. Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure.

To obtain an IP-HTTPS certificate

1. On each Remote Access server: On the **Start** screen, type **mmc**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.

2. Click **File**, and then click **Add/Remove Snap-ins**.
3. Click **Certificates**, click **Add**, click **Computer account**, click **Next**, select **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.
6. Click **Next** twice.
7. On the **Request Certificates** page, click the Web Server certificate template, and then click **More information is required to enroll for this certificate**.

   If the Web Server certificate template does not appear, ensure that the Remote Access server computer account has enroll permissions for the Web Server certificate template. For more information, see Configure Permissions on the Web Server Certificate Template.
8. On the **Subject** tab of the **Certificate Properties** dialog box, in **Subject name**, for **Type**, select **Common name**.
9. In **Value**, type the fully qualified domain name (FQDN) of the Internet name of the Remote Access server (for example, Europe.contoso.com), and then click **Add**.
10. Click **OK**, click **Enroll**, and then click **Finish**.
11. In the details pane of the Certificates snap-in, verify that a new certificate with the FQDN was enrolled with **Intended Purposes** of **Server Authentication**.
12. Right-click the certificate, and then click **Properties**.
13. In **Friendly Name**, type **IP-HTTPS Certificate**, and then click **OK**.

> **TIP**
> Steps 12 and 13 are optional, but make it easier for you to select the certificate for IP-HTTPS when configuring Remote Access.

14. Repeat this procedure on all Remote Access servers in your deployment.

3.4. Configure the network location server for a multisite deployment

If you selected to set up the network location server website on the Remote Access server when you set up your first server, each new Remote Access server that you add needs to be configured with a Web Server certificate that has the same subject name that was selected for the network location server for the first server. Each server requires a certificate to authenticate the connection to the network location server, and client computers located in the internal network must be able to resolve the name of the website in DNS.

To install a certificate for network location

1. On the Remote Access server: On the **Start** screen, type **mmc**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. Click **File**, and then click **Add/Remove Snap-ins**.
3. Click **Certificates**, click **Add**, click **Computer account**, click **Next**, select **Local computer**, click **Finish**, and then click **OK**.

4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.

5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**.

> **NOTE**
> You may also import the same certificate that was used for the network location server for the first Remote Access server.

6. Click **Next** twice.

7. On the **Request Certificates** page, click the Web Server certificate template, and then click **More information is required to enroll for this certificate**.

   If the Web Server certificate template does not appear, ensure that the Remote Access server computer account has enroll permissions for the Web Server certificate template. For more information, see Configure Permissions on the Web Server Certificate Template.

8. On the **Subject** tab of the **Certificate Properties** dialog box, in **Subject name**, for **Type**, select **Common name**.

9. In **Value**, type the fully qualified domain name (FQDN) that was configured for the network location server certificate of the first Remote Access server (for example, nls.corp.contoso.com), and then click **Add**.

10. Click **OK**, click **Enroll**, and then click **Finish**.

11. In the details pane of the Certificates snap-in, verify that a new certificate with the FQDN was enrolled with **Intended Purposes** of **Server Authentication**.

12. Right-click the certificate, and then click **Properties**.

13. In **Friendly Name**, type **Network Location Certificate**, and then click **OK**.

> **TIP**
> Steps 12 and 13 are optional, but make it easier for you to select the certificate for network location when configuring Remote Access.

14. Repeat this procedure on all Remote Access servers in your deployment.

To create the network location server DNS records

1. On the DNS server: On the **Start** screen, type **dnsmgmt.msc**, and then press ENTER.

2. In the left pane of the **DNS Manager** console, open the forward lookup zone for the internal network. Right click the relevant zone and click **New Host (A or AAAA)**.

3. On the **New Host** dialog box, in the **Name (uses parent domain name if blank)** box, enter the name that was used for the network location server for the first Remote Access server. In the **IP address** box, enter the intranet-facing IPv4 address of the Remote Access server, and then click **Add Host**. On the **DNS** dialog box, click **OK**.

4. On the **New Host** dialog box, in the **Name (uses parent domain name if blank)** box, enter the name that was used for the network location server for the first Remote Access server. In the **IP address** box, enter the intranet-facing IPv6 address of the Remote Access server, and then click **Add Host**. On the **DNS** dialog box, click **OK**.

5. Repeat steps 3 and 4 for every Remote Access server in your deployment.

6. Click **Done**.

7. Repeat this procedure before adding servers as additional entry points in the deployment.

3.5. Configure DirectAccess clients for a multisite deployment

DirectAccess Windows client computers must be members of security group(s) which define their DirectAccess association. Before multisite is enabled, these security group(s) can contain both Windows 8 clients and Windows 7 clients (if the appropriate "downlevel" mode was selected). Once multisite is enabled, existing client security group(s), in single server mode, are converted to security group(s) for Windows 8 only. After multisite is enabled, DirectAccess Windows 7 client computers must be moved to corresponding dedicated Windows 7 client security groups (which are associated with specific entry-points), or they will not be able to connect over DirectAccess. The Windows 7 clients must first be removed from the existing security groups which are now Windows 8 security groups. Caution: Windows 7 client computers that are members of both Windows 7 and Windows 8 client security groups will lose remote connectivity, and Windows 7 clients without SP1 installed will lose corporate connectivity as well. Therefore, all Windows 7 client computers must be removed from Windows 8 security groups.

Remove Windows 7 clients from Windows 8 security groups

1. On the primary domain controller, click **Start**, and then click **Active Directory Users and Computers**.

2. To remove computers from the security group, double-click the security group, and on the **<Group_Name> Properties** dialog box, click the **Members** tab.

3. Select the Windows 7 client computer, and click **Remove**.

4. Repeat this procedure to remove the Windows 7 client computers from the Windows 8 security groups.

> **IMPORTANT**
>
> When enabling a Remote Access multisite configuration all client computers (Windows 7 and Windows 8) will lose remote connectivity until they are able to connect to the corporate network directly or by VPN to update their group policies. This is true when enabling multisite functionality for the first time, and also when disabling multisite.

3.6. Enable the multisite deployment

To configure a multisite deployment, enable the multisite feature on your existing Remote Access server. Before enabling multisite in your deployment, make sure you have the following information:

1. Global load balancer settings and IP addresses if you want to load balance DirectAccess client connections across all entry-points in your deployment.

2. The security group(s) containing Windows 7 client computers for the first entry point in your deployment, if you want to enable Remote Access for Windows 7 client computers.

3. Group Policy Object names, if you are required to use non-default Group Policy Objects, which are applied on Windows 7 client computers for the first entry point in your deployment, if you require support for Windows 7 client computers.

To enable a multisite configuration

1. On your existing Remote Access server: On the **Start** screen, type **RAMgmtUI.exe**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.

2. In the Remote Access Management Console, click **Configuration**, and then in the **Tasks** pane, click

Enable Multisite.

3. In the **Enable Multisite Deployment** wizard, on the **Before You Begin** page, click **Next**.

4. On the **Deployment Name** page, in **Multisite deployment name**, enter a name for your deployment. In **First entry point name**, enter a name to identify the first entry point which is the current Remote Access server, and then click **Next**.

5. On the **Entry Point Selection** page, do one of the following:

   - Click **Assign entry points automatically, and allow clients to select manually** to automatically route client computers to the most suitable entry point, while also allowing client computers to select an entry point manually. Manual entry point selection is available only for Windows 8 computers. Click **Next**.

   - Click **Assign entry points automatically** to automatically route client computers to the most suitable entry point, and then click **Next**.

6. On the **Global Load Balancing** page, do one of the following:

   - Click **No, do not use global load balancing** if you do not want to use a global load balancing, and then click **Next**.

     > **NOTE**
     >
     > When selecting this option client computers connect to their closest entry point automatically.

   - Click **Yes, use global load balancing** if you want to load balance the traffic globally between all entry points. In **Type the global load balancing FQDN to be used by all entry points**, enter the global load balancing FQDN, and in **Type the global load balancing IP address for this entry point** that contains the first Remote Access server, enter the global load balancing IP address for this entry point, and then click **Next**.

7. On the **Client Support** page, do one of the following:

   - To limit access to client computers running Windows 8 or later operating systems, click **Limit access to client computers running Windows 8 or a later operating system**, and then click **Next**.

   - To allow client computers running Windows 7 to access this entry point, click **Allow client computers running Windows 7 to access this entry point**, and click **Add**. On the **Select Groups** dialog box, select the security group(s) that contains the Windows 7 client computers, click **OK**, and then click **Next**.

8. On the **Client GPO Settings** page, accept the default GPO for Windows 7 client computers for this entry point, type the name of the GPO that want Remote Access to create automatically, or click **Browse** to locate the GPO for Windows 7 client computers, and then click **Next**.

   > **NOTE**
   >
   > - The **Client GPO Settings** page appears only when you configure the entry point to allow Windows 7 client computers to access the entry point.
   > - You can optionally click **Validate GPOs** to ensure that you have the proper permissions for the selected GPO or GPOs for this entry point. If the GPO does not exist and will be automatically created, then create and link permissions are required. In the case where the GPOs were created manually, then edit, modify security, and delete permissions are required.

9. On the **Summary** page, click **Commit**.
10. On the **Enabling Multisite Deployment** dialog box, click **Close** and then on the Enable Multisite Deployment wizard, click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

To enable a multisite deployment named 'Contoso' on the first entry point named 'Edge1-US'. The deployment allows clients to manually select the entry point, and does not use a global load balancer.

```
Enable-DAMultiSite -Name 'Contoso' -EntryPointName 'Edge1-US' -ManualEntryPointSelectionAllowed 'Enabled'
```

To allow Windows 7 client computers access through the first entry point through the security group DA_Clients_US and using the GPO DA_W7_Clients_GPO_US.

```
Add-DAClient -EntrypointName 'Edge1-US' -DownlevelSecurityGroupNameList @('corp.contoso.com\DA_Clients_US')
-DownlevelGpoName @('corp.contoso.com\DA_W7_Clients_GPO_US)
```

3.7. Add entry points to the multisite deployment

After enabling multisite in your deployment, you can add additional entry points using the Add an Entry Point wizard. Before adding entry points, make sure you have the following information:

- Global load balancer IP addresses for each new entry point if you are using global load balancing.
- The security group(s) containing Windows 7 client computers for each entry point that will be added if you want to enable Remote Access for Windows 7 client computers.
- Group Policy Object names, if you are required to use non-default Group Policy Objects, which are applied on Windows 7 client computers for each entry point that will be added, if you require support for Windows 7 client computers.
- In the case where IPv6 is deployed in the organization's network you will need to prepare the IP-HTTPS prefix for the new entry point.

To add entry-points to your multisite deployment

1. On your existing Remote Access server: On the **Start** screen, type **RAMgmtUI.exe**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the Remote Access Management Console, click **Configuration**, and then in the **Tasks** pane, click **Add an Entry Point**.
3. In the Add an Entry Point Wizard, on the **Entry Point Details** page, in **Remote Access server**, enter the fully qualified domain name (FQDN) of the server to add. In **Entry point name**, enter the name of the entry point, and then click **Next**.
4. On the **Global Load Balancing Settings** page, enter the global load balancing IP address of this entry point, and then click **Next**.

> **NOTE**
> The **Global Load Balancing Settings** page appears only when the multisite configuration uses a global load balancer.

5. On the **Network Topology** page, click the topology that corresponds with the network topology of the Remote Access server that you are adding, and then click **Next**.
6. On the **Network Name or IP Address** page, in **Type in the public name or IP address used by clients to connect to the remote access server**, enter the public name or IP address used by clients to connect to the Remote Access server. The public name corresponds with the subject name of the IP-HTTPS certificate. In the case where Edge network topology was implemented, the IP address is that of the external adapter of the Remote Access server. Click **Next**.
7. On the **Network Adapters** page, do one the following:
   - If you are deploying a topology with two network adapters, in **External adapter**, select the adapter that is connected to the external network. In **Internal adapter**, select the adapter that is connected to the internal network.
   - If you are deploying a topology with one network adapter, in **Network adapter**, select the adapter that is connected to the internal network.
8. On the **Network Adapters** page, in **Select the certificate used to authenticate IP-HTTPS connections**, click **Browse** to locate and select the IP-HTTPS certificate. Click **Next**.
9. If IPv6 is configured on the corporate network, on the **Prefix Configuration** page, in **IPv6 prefix assigned to client computers**, enter an IP-HTTPS prefix to assign IPv6 addresses to DirectAccess client computers, and click **Next**.
10. On the **Client Support** page, do one of the following:
    - To limit access to client computers running Windows 8 or later operating systems, click **Limit access to client computers running Windows 8 or a later operating system**, and then click **Next**.
    - To allow client computers running Windows 7 to access this entry point, click **Allow client computers running Windows 7 to access this entry point**, and click **Add**. On the **Select Groups** dialog box, select the security group(s) that contain the Windows 7 client computers that will connect to this entry point, click **OK**, and click **Next**.
11. On the **Client GPO Settings** page, accept the default GPO for Windows 7 client computers for this entry point, type the name of the GPO that you want Remote Access to create automatically, or click **Browse** to locate the GPO for Windows 7 client computers, and click **Next**.

> **NOTE**
> - The **Client GPO Settings** page appears only when you configure the entry point to allow Windows 7 client computers to access the entry point.
> - You can optionally click **Validate GPOs** to ensure that you have the proper permissions for the selected GPO or GPOs for this entry point. If the GPO does not exist and will be automatically created, then create and link permissions are required. In the case where the GPOs were created manually, then edit, modify security, and delete permissions are required.

12. On the **Server GPO Settings** page, accept the default GPO for this Remote Access server, type the name of the GPO that you want Remote Access to create automatically, or click **Browse** to locate the GPO for

this server, and then click **Next**.

13. On the **Network Location Server** page, click **Browse** to select the certificate for the network location server website running on the Remote Access server, and then click **Next**.

> **NOTE**
>
> The **Network Location Server** page appears only when the network location server website is running on the Remote Access server.

14. On the **Summary** page, review the entry point settings, and then click **Commit**.

15. On the **Adding Entry Point** dialog box, click **Close** and then on the Add an Entry Point Wizard, click **Close**.

> **NOTE**
>
> If the entry point that was added is in a different forest than the existing entry points or client computers, then it is required to click **Refresh Management Servers** in the **Tasks** pane to discover the domain controllers and Configuration Manager in the new forest.

16. Repeat this procedure from step 2 for every entry point that you want to add to your multisite deployment.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

To add the computer edge2 from the corp2 domain as a second entry point named Edge2-Europe. The entry point configuration is: a client IPv6 prefix '2001:db8:2:2000::/64', a connect to address (the IP-HTTPS certificate on the edge2 computer) 'edge2.contoso.com', a server GPO named "DirectAccess Server Settings - Edge2-Europe", and the internal and external interfaces named Internet and Corpnet2 respectively:

```
Add-DAEntryPoint -RemoteAccessServer 'edge2.corp2.corp.contoso.com' -Name 'Edge2-Europe' -ClientIPv6Prefix
'2001:db8:2:2000::/64' -ConnectToAddress 'Europe.contoso.com' -ServerGpoName
'corp2.corp.contoso.com\DirectAccess Server Settings - Edge2-Europe' -InternetInterface 'Internet' -
InternalInterface 'Corpnet2'
```

To allow Windows 7 client computers access through the second entry point through the security group DA_Clients_Europe and using the GPO DA_W7_Clients_GPO_Europe.

```
Add-DAClient -EntrypointName 'Edge2-Europe' -DownlevelGpoName @('corp.contoso.com\
DA_W7_Clients_GPO_Europe') -DownlevelSecurityGroupNameList @('corp.contoso.com\DA_Clients_Europe')
```

See also

- Step 2: Configure the multisite infrastructure

Step 4 Verify the Multisite Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to verify that you have correctly configured your Remote Access multisite deployment.

To verify access to internal resources through the multisite deployment

1. Connect a DirectAccess client computer to the corporate network and obtain the group policy.
2. Connect the client computer to the external network and attempt to access internal resources.

   You should be able to access all corporate resources.
3. Test connectivity through each server in the multisite deployment by turning off, or disconnecting from the external network, all but one of the Remote Access servers. On the client computer, attempt to access corporate resources. Repeat the test on a different multisite server. It may take up to 10 minutes for the client computer to connect to the new entry point. This is because probing is turned off for 10 minutes for an entry point after it is deemed unreachable, in order to optimize bandwidth and battery life. Alternatively, you can switch between the various entry-points manually by choosing the desired entry-point from the combo-box shown when executing **daprop.exe**.

   You should be able to access all corporate resources through each multisite server.
4. Connect a Windows 7® client computer to the corporate network and obtain the group policy.
5. Connect the Windows 7 client computer to the external network and attempt to access internal resources.

   You should be able to access all corporate resources.
6. Test connectivity for Windows 7 clients through each server in the multisite deployment by accessing the Active Directory Users and Computers console, and moving the client computer to the security group that corresponds to each server. After the changes have replicated throughout the domain, restart the client computer while connected to the corporate network to obtain the new group policy. Attempt to access corporate resources. Repeat the test on a different multisite server.

   You should be able to access all corporate resources through each multisite server.

   In a production environment this method may not be feasible due to the amount of time required for changes to replicate throughout the domain. You may want to force replication where possible. Testing can also be done from multiple different Windows 7 client computers that are already members of the different Windows 7 security groups in the multisite deployment.

Troubleshoot a Multisite Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to troubleshoot the most common errors that may occur when configuring a multisite Remote Access deployment.

- Troubleshooting enabling multisite
- Troubleshooting adding entry points
- Troubleshooting setting the entry point domain controller
- Troubleshooting web probe URLs
- Troubleshooting general issues

Troubleshooting Enabling Multisite

12/9/2022 • 6 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic contains troubleshooting information for issues related to the `Enable-DAMultisite` command. To confirm that the error you received is related to enabling multisite, check in the Windows Event log for the event ID 10051.

User connectivity issues

Users may experience connectivity issues when you enable multisite if the configuration is not correct.

Cause

In a multisite deployment, Windows 10 and Windows 8 client computers are able to roam between different entry points. Windows 7 client computers must be associated with a specific entry point in the multisite deployment. If client computers are not in the correct security group, they may receive the wrong group policy settings.

Solution

DirectAccess requires at least one security group for all Windows 10 and Windows 8 client computers; we recommend using one security group for all Windows 10 and Windows 8 computers per domain. DirectAccess also requires a security group for Windows 7 client computers for each entry point. Each client computer should be included in only one security group. Therefore, you should make sure that the security groups for Windows 10 and Windows 8 clients contain only computers running Windows 10 or Windows 8, and that each Windows 7 client computer belongs to a single dedicated security group for the relevant entry point and that no Windows 10 or Windows 8 clients belong to the Windows 7 security groups.

Configure the Windows 8 security groups on the **Select Groups** page of the **DirectAccess Client Setup** wizard. Configure Windows 7 security groups on the **Client Support** page of the **Enable Multisite Deployment** wizard, or on the **Client Support** page of the **Add an Entry Point** wizard.

Kerberos proxy authentication

Error received. Kerberos proxy authentication is not supported in a multisite deployment. You must enable the use of computer certificates for IPsec user authentication.

Cause

Computer certificate authentication must be enabled before enabling multisite.

Solution

To enable computer certificate authentication:

1. In the Remote Access Management console, in the details pane, under **Step 2 Remote Access Server**, click **Edit**.
2. In the **Remote Access Server Setup** wizard, on the **Authentication** page, select the **Use computer certificates** check box, and select the root or intermediate certification authority that issues certificates in your deployment.

To enable computer certificate authentication using Windows PowerShell, use the `Set-DAServer` cmdlet and specify the *IPsecRootCertificate* parameter.

IP-HTTPS certificates

Error received. The DirectAccess server uses a self-signed IP-HTTPS certificate. Configure IP-HTTPS to use a signed certificate from a known CA.

Cause

The IP-HTTPS certificate is self-signed. You cannot use self-signed certificates in a multisite deployment.

Solution

To select an IP-HTTPS certificate:

1. In the Remote Access Management console, in the details pane, under **Step 2 Remote Access Server**, click **Edit**.
2. In the **Remote Access Server Setup** wizard, on the **Network Adapters** page, under **Select the certificate used to authenticate IP-HTTPS connections**, make sure the **Use a self-signed certificate created automatically by DirectAccess** check box is cleared, and click **Browse** to select a certificate issued by a trusted CA.

Network location server

- **Issue 1**

  Error received. DirectAccess is configured to use a self-signed certificate for the network location server. Configure the network location server to use a signed certificate from a CA.

  Cause

  The network location server is deployed on the Remote Access server and uses a self-signed certificate. You cannot use self-signed certificates in a multisite deployment.

  Solution

  To select a network location server certificate:

  1. In the Remote Access Management console, in the details pane, under **Step 3 Infrastructure Servers**, click **Edit**.
  2. In the **Infrastructure Server Setup** wizard, on the **Network Location Server** page, under **The network location server is deployed on the Remote Access server**, make sure the **Use a self-signed certificate** check box is cleared, and click **Browse** to select a certificate issued by an Enterprise CA.

- **Issue 2**

  Error received. To deploy a network load balanced cluster or multisite deployment, obtain a certificate for the network location server with a subject name that is different from the internal name of the Remote Access server.

  Cause

  The subject name of the certificate used for the network location server website is the same as the internal name of the Remote Access server. This will cause name resolution issues.

  Solution

Obtain a certificate with a subject name that is not the same as the internal name of the Remote Access server.

To configure the network location server:

1. In the Remote Access Management console, in the details pane, under **Step 3 Infrastructure Servers**, click **Edit**.
2. In the **Infrastructure Server Setup** wizard, on the **Network Location Server** page, under **The network location server is deployed on the Remote Access server**, click **Browse** to select the certificate you previously obtained. The certificate must have a subject name that is different from the internal name of the Remote Access server.

Windows 7 client computers

Warning received. When enabling multisite, the security groups configured for DirectAccess clients must not contain Windows 7 computers. To support Windows 7 client computers in a multisite deployment, select a security group containing the clients for each entry point.

Cause

In the existing DirectAccess deployment, Windows 7 client support was enabled.

Solution

DirectAccess requires at least one security group for all Windows 8 client computers and a security group for Windows 7 client computers for each entry point. Each client computer should be included in only one security group. Therefore, you should make sure that the security group for Windows 8 clients contains only computers running Windows 8, and that each Windows 7 client computer belongs to a single dedicated security group for the relevant entry point and that no Windows 8 clients belong to the Windows 7 security groups.

Active Directory site

Error received. The server <server_name> is not associated with an Active Directory Site.

Cause

DirectAccess could not determine the Active Directory site. In the Active Directory Sites and Services console you can configure the different subnets for your network and associate each subnet with the relevant Active Directory site. This error may occur if the IP address of the Remote Access server does not belong to any of the subnets, or that the subnet to which the IP address belongs is not defined with an Active Directory site.

Solution

Confirm that this is the issue by running the command `nltest /dsgetsite` on your Remote Access server. If this is the issue, the command will return ERROR_NO_SITENAME. To solve this issue, on your domain controller, make sure that a subnet which contains the internal server IP address exists and that it is defined with an Active Directory site.

Saving server GPO settings

Error received. An error occurred while saving Remote Access settings to GPO <GPO_name>.

Cause

Changes to the server GPO couldn't be saved either due to connectivity issues or if there is a sharing violation on the registry.pol file, for example, another user has locked the file.

Solution

Make sure that there is connectivity between the Remote Access server and the domain controller. If there is connectivity, check on the domain controller if the registry.pol file is locked to another user, and if necessary, end that user session to unlock the file.

Internal error occurred

Error received. An internal error occurred.

Cause

This may be caused by an unexpected entry point table configuration in the client GPO. This can occur if the administrator uses DirectAccess client cmdlets to edit the entry point table in the client GPO.

Solution

Review the entry point table configuration in all client GPOs and fix any inconsistencies in the multisite configuration between the different instances of the client GPOs and the DirectAccess configuration. Use the `Get-DaEntryPointTableItem` cmdlet with the name of the client GPO to get the entry point table on the client. Use the `Get-NetIPHttpsConfiguration` cmdlet to get all the IP-HTTPS profiles for all the entry points.

For further information, see DirectAccess Client Cmdlets in Windows PowerShell.

Troubleshooting Adding Entry Points

12/9/2022 • 9 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic contains troubleshooting information for issues related to the `Add-DAEntryPoint` command. To confirm that the error you received is related to adding an entry point, check in the Windows Event log for the event ID 10067.

Missing RemoteAccessServer parameter

Error received. You must supply a value for the parameter RemoteAccessServer.

Cause

When adding a new entry point to a multisite deployment, you must specify the parameter *RemoteAccessServer*, which is the name of the server which you want to add as the new entry point.

Solution

Run the command and make sure to specify the *RemoteAccessServer* parameter with the name of the server to be added as an entry point.

Remote Access is not configured

Error received. Remote Access is not configured on <server_name>. Specify the name of a server that belongs to a multisite deployment.

Cause

Remote Access is not configured on the computer specified by the *ComputerName* parameter, or on the computer on which you run the command.

When adding a new entry point to a multisite deployment, you must specify two parameters: *ComputerName* and *RemoteAccessServer*. The *ComputerName* is the name of a server which is already part of the multisite deployment, the *RemoteAccessServer* is the name of the server which you want to add as the new entry point. If you run from a computer that is part of the multisite deployment, the ComputerName parameter is not required.

Solution

Run the command and make sure to specify the *ComputerName* parameter with the name of the server that is already configured as part of the multisite deployment, or run the command from a computer that is part of the multisite deployment.

Multisite not enabled

Error received. You must enable a multisite deployment before performing this operation. Use the `Enable-DAMultiSite` cmdlet to do this.

Cause

Multisite is not enabled on the server specified by the *ComputerName* parameter. To add a new entry point to a

Remote Access deployment, you must first enable multisite.

Solution

Enable multisite using the `Enable-DaMultiSite` cmdlet. For more information, see Deploy multisite Remote Access.

IPv6 prefix issues

- **Issue 1**

  Error received. IPv6 is deployed in the internal network, but you have not specified a client IPv6 prefix.

  Cause

  IPv6 is deployed on the corporate network, and an IP-HTTPS prefix is required. However, a prefix was not specified in the *ClientIPv6Prefix* parameter for the new entry point.

  Solution

  1. Assign a unique IP-HTTPS prefix to the new entry point and ensure that packets targeted to an IP address under this prefix will be routed to the server you are adding.
  2. Run the `Add-DAEntryPoint` cmdlet and specify the IP-HTTPS prefix in the *ClientIPv6Prefix* parameter.

- **Issue 2**

  Error received. The client IPv6 prefix is already in use by another entry point. Specify an alternate value.

  Cause

  The IP-HTTPS prefix specified in the *ClientIPv6Prefix* parameter is already used by a different entry point

  Solution

  1. Assign a unique IP-HTTPS prefix to the new entry point and ensure that packets targeted to an IP address under this prefix will be routed to the server you are adding.
  2. Run the `Add-DAEntryPoint` cmdlet and specify the IP-HTTPS prefix in the *ClientIPv6Prefix* parameter.

ConnectTo address

Error received. The address (<connect_to_address>) to which DirectAccess clients connect on the RemoteAccess server is the same as the network location server address. Specify an alternate value.

Cause

The ConnectTo address and the network location server address are the same.

Solution

The ConnectTo address should be resolvable over the Internet to allow client machines to connect over IP-HTTPS. The network location server address should be resolvable over the corporate network but should not be resolvable over the Internet. Make sure that the network location server and the ConnectTo addresses are not the same. Select different addresses and try again.

DirectAccess or VPN already installed

Error received. A VPN installation was detected on the server <server_name>. Specify an alternate server that

does not have Remote Access installed, or remove the VPN configuration from the server.

Or

Remote Access is already installed on server <server_name>. Specify an alternate server not running DirectAccess, or remove the existing DirectAccess configuration from the server.

Cause

DirectAccess or VPN is already configured on the new entry point. You cannot add a configured entry point to a multisite deployment.

Solution

To add a server to a multisite deployment, you must install the Remote Access role on the server but DirectAccess and VPN should not be configured.

Run the command and make sure that the server you specify in the *RemoteAccessServer* parameter does not have DirectAccess or VPN configured.

IPsec root certificate

Error received. The configured IPsec root certificate cannot be located on server <server_name>.

Cause

The certificate of the root or intermediate certification authority (CA) that issues computer certificates could not be found on the server you are trying to add to the deployment.

Solution

In the Remote Access Management console, in **Step 2 Remote Access Server**, click **Edit**, and on the **Authentication** page, under **Use computer certificates**, make sure that the certificate selected is valid. If the certificate is valid, make sure that it is located under the trusted root CA on the server you want to add and try again.

> **NOTE**
> The certificate must be the same certificate with the same Thumbprint.

If the certificate is not valid, select a valid certificate which is configured as the trusted root CA on all the Remote Access servers.

Mixing IPv6 and IPv4 entry points

When DirectAccess is installed for the first time, the internal network adapter is inspected to determine if the network contains IPv4 addresses only (IPv4-only network), IPv6 and IPv4 addresses, or IPv6 addresses only (IPv6-only network). The information is used to determine the deployment type (IPv4 only, IPv6+IPv4, or IPv6 only).

- **Issue 1**

  Warning received. The Remote Access server being added is configured with both IPv4 and IPv6 addresses. This is an IPv4 only deployment, and Remote Access will ignore the IPv6 addresses.

  #### Cause

  When this deployment was first installed, the internal network was detected as an IPv4 only network. In a multisite deployment, different entry points are assumed to be located in different subnets with different

characteristics. Therefore, although the deployment is configured as an IPv4 only deployment, it can contain an entry point located in an IPv6+IPv4 subnet. However, although the entry point will be added to the deployment, DirectAccess will ignore the IPv6 addresses configured on the new entry point's internal interface.

Solution

If the entire internal network is configured with IPv6 and IPv4 addresses, consider moving to an IPv6+IPv4 deployment to benefit from IPv6 technologies. See "Transitioning from a pure IPv4 to an IPv6+IPv4 corporate network" in Step 3: Plan the multisite deployment.

- **Issue 2**

  Error received. The internal network adapters of the Remote Accces servers in this multisite deployment are configured with IPv4 addresses. The entry point you are adding must also be configured with an IPv4 address on the internal network adapter.

  Cause

  When this deployment was first installed, the internal network was detected as an IPv4 only network. Remote Access detected that the entry point that you are trying to add is configured with only IPv6 addresses on its internal network. This is not allowed in an IPv4 only deployment.

  Solution

  If the entire network is already configured with IPv6 addresses, you should move to an IPv6+IPv4 or IPv6-only deployment. See "Plan the transition to IPv6 when multisite Remote Access is deployed".

- **Issue 3**

  Error received. This entry point is located in an IPv4 network, but previous entry points are located in an IPv6 network. Connect this entry point to the IPv6 network before adding it to the same multisite deployment.

  Cause

  When this deployment was first installed, it was detected that the internal network is IPv6+IPv4 or IPv6-only. It was detected that only IPv4 addresses are configured on the internal network on the new entry point you are trying to add. This is not allowed in IPv6+IPv4, or IPv6-only deployments.

  Solution

  Configure the new entry point with IPv6 addresses and then add the entry point to the multisite deployment.

- **Issue 4**

  Warning received. The internal network adapter on the Remote Access server is not configured with an IPv4 address. DNS64 and NAT64 will not be configured on this server. DirectAccess clients can access IPv6 internal servers only.

  Cause

  When this deployment was first installed, it was detected that the internal network is IPv6+IPv4. In this deployment mode, DNS64 and NAT64 are enabled to allow client computers to access machines on the internal network that are configured with only IPv4 addresses.

  When adding the new entry point, Remote Access detected that the internal interface on the new computer has only IPv6 addresses. To configure DNS64 and NAT64, an IPv4 address is required in order to route packets from the Remote Access server to the IPv4 only computer. Since no such IP exists on the

new computer, NAT64 and DNS64 won't be configured on the Remote Access server. Therefore, client machines accessing the corporate network over DirectAccess using this entry point won't be able to access IPv4 only servers on the internal network. For information on how to transition to an IPv6+IPv4 network, or an IPv6-only network, see "Plan the transition to IPv6 when multisite Remote Access is deployed".

Solution

Add an IPv4 address to the new Remote Access server to ensure that DNS64 and NAT64 work correctly.

Domain issues with the ServerGpoName

- **Issue 1**

  Error received. The domain specified in the ServerGpoName parameter <server_GPO> does not exist. Specify the domain <domain_name> instead.

  Cause

  The domain name part of the server GPO name which was sent by the administrator was not found.

  Solution

  Make sure that you typed the domain name correctly. If the domain name is spelled correctly, try again using the fully qualified domain name (FQDN).

- **Issue 2**

  Error received. The server GPO must be located in the Remote Access server domain. Specify the domain <domain_name> in the ServerGpoName parameter.

  Cause

  The domain of the server GPO is not the same as the one to which the Remote Access server belongs.

  Solution

  The server GPO should be located in the same domain as the Remote Access server. Use the server's domain name for the server GPO and try again.

Split-brain DNS

Warning received. The NRPT entry for the DNS suffix <DNS_suffix> contains the public name used by client computers to connect to the Remote Access server. Add the name <connect_to_address> as an exemption in the NRPT.

Cause

You are using split brain DNS. To allow clients to connect using IP-HTTPS, you should make sure that the ConnectTo address selected is exempt in the NRPT rules.

Solution

If you have a multisite deployment, make sure that all connect to addresses of the different entry points are exempt from the NRPT rules.

To exempt an address in the NRPT rules:

1. In the Remote Access Management console, under **Step 3 Infrastructure Servers**, click **Edit**.
2. In the **Infrastructure Server Setup** wizard, on the **DNS** page, double-click the table to enter a new

name suffix.

3. On the **DNS Server Addresses** dialog box, in DNS suffix, enter the ConnectTo address of the entry point, and then click **Apply**.

When you add name suffixes without specifying a server address, the suffix is treated as an NRPT exemption.

Saving server GPO settings

Error received. An error occurred while saving Remote Access settings to GPO <GPO_name>.

To troubleshoot this error, see Saving server GPO settings in Troubleshooting Enabling Multisite.

GPO updates cannot be applied

Warning received. GPO updates cannot be applied on <server_name>. Changes will not take effect until the next policy refresh.

Cause

An error occurred while trying to refresh policies on the specified computer. Therefore, changes made will not take effect until the next policy refresh.

Solution

To force a policy refresh, run `gpupdate /force` on the specified computer.

Troubleshooting Setting the Entry Point Domain Controller

12/9/2022 • 8 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic contains troubleshooting information for issues related to the `Set-DAEntryPointDC` command. To confirm that the error you received is related to setting the entry point domain controller, check in the Windows Event log for the event ID 10065.

Saving server GPO settings

Error received. An error occurred while saving Remote Access settings to GPO <GPO_name>.

To troubleshoot this error, see Saving server GPO settings.

Remote Access is not configured

Error received. Remote Access is not configured on <server_name>. Specify the name of a server that belongs to a multisite deployment.

Or

Remote Access is not configured on the server <server_name>. Specify a computer with DirectAccess enabled.

Cause

Remote Access is not configured on the computer specified by the *ComputerName* parameter.

The `Set-DaEntryPointDC` cmdlet is available only on servers that are part of a configured multisite deployment.

Solution

Run the command and make sure to specify the *ComputerName* parameter with the name of the server that is already configured as part of the multisite deployment.

Multisite is not enabled

Error received. You must enable a multisite deployment before performing this operation. Use the `Enable-DAMultiSite` cmdlet to do this.

Cause

Multisite is not enabled on the server specified by the *ComputerName* parameter.

The `Set-DaEntryPointDC` cmdlet is available only on servers that are part of a configured multisite deployment.

Solution

Run the command and make sure to specify the *ComputerName* parameter with the name of the server that is already configured as part of the multisite deployment.

Entry point and domain controller not provided in cmdlet

The `Set-DaEntryPointDC` cmdlet enables you to change the domain controller that is associated with different entry points, for example, if a particular domain controller is no longer available. You can update a specific entry point to use a different domain controller, or you can update all entry points which use a specific domain controller to use a new domain controller. In the first case, you should use the *EntryPointName* parameter to specify which entry point should be updated. In the second case, you should use the *ExistingDC* parameter to specify which domain controller should be replaced. You can specify only one of these parameters.

Error received. No required parameters were specified. Provide the name of an entry point or an existing domain controller.

Or

Cmdlet `Set-DaEntryPointDC` is missing all required parameters.

Cause

The *EntryPointName* or *ExistingDC* parameters were not specified, or both parameters were specified, for the `Set-DaEntryPointDC` cmdlet.

Solution

Run the command and make sure to specify either the *EntryPointName* parameter or the *ExistingDC* parameter.

Could not locate domain controller

Error received. Unable to locate a new domain controller automatically. Retry later or verify domain controller settings.

Cause

The computer specified with the *ComputerName* parameter is not reachable over RPC or the domain does not contain any available writable domain controllers.

Solution

Make sure that the remote computer is accessible over RPC and that there is a writable domain controller available for the domain. If a writable domain controller is available for the domain, you can also specify its name explicitly using the *NewDC* parameter.

Could not connect to domain controller

- **Issue 1**

  Error received. The domain controller <domain_controller> cannot be reached. Check network connectivity and server availability.

  Cause

  The domain controller cannot be reached. This occurs only when the administrator specifies a domain controller in the *NewDC* or *ExistingDC* parameters.

  Solution

  Make sure that the domain controller's name is spelled correctly. If you used a short name to specify the name, use the FQDN and try again.

- **Issue 2**

  Error received. The domain controller <domain_controller> cannot be contacted.

  Cause

There may be a network issue that means the domain controller specified in the *NewDC* parameter, or any other existing domain controller in the configuration cannot be reached.

Solution

Make sure that the domain controller's name is spelled correctly, make sure it exists, is running, is writable, and that there is a trust relationship between the domain controller and the domain.

- **Issue 3**

  Error received. Domain controller <domain_controller> cannot be reached for %2!s!.

  Cause

  To maintain the configuration consistency in a multisite deployment, it is important to make sure that each GPO is managed by a single domain controller. When the domain controller that manages an entry point's server GPO is not available, Remote Access configuration settings cannot be read or modified.

  Solution

  Follow the procedure "To change the domain controller that manages server GPOs" described in 2.4. Configure GPOs.

- **Issue 4**

  Error received. The primary domain controller in domain <domain_name> cannot be reached.

  Cause

  To maintain the configuration consistency in a multisite deployment, it is important to make sure that each GPO is managed by a single domain controller. Client GPOs are managed on the primary domain controller. If the primary domain controller is not available, Remote Access configuration settings cannot be read or modified.

  Solution

  Follow the procedure "To transfer the PDC emulator role" described in 2.4. Configure GPOs.

Read-only domain controller

Error received. The domain controller <domain_controller> is read-only. Specify a domain controller that is not read-only.

Cause

The domain controller specified with the *NewDC* parameter is read-only.

Solution

When using the `Set-DAEntryPointDC`, the *NewDC* parameter is used to update the domain controller associated with a particular entry point, or to update all entry points associated with a domain controller. Therefore, the new domain controller must be writable. Specify a writable domain controller in the *NewDC* parameter and try again.

Cannot retrieve GPO

- **Issue 1**

  Error received. GPO <GPO_name> on domain controller <previous_domain_controller> cannot be retrieved from domain controller <replacement_domain_controller> because they are not in the same domain.

Cause

The Remote Access server and the domain controller are not in the same domain; therefore, the GPO cannot be retrieved.

Solution

If you tried to update a specific entry point, make sure that the new domain controller is in the same domain as the entry point server. If you tried to update a specific domain controller, make sure that the new domain controller is in the same domain as the one you are trying to replace.

- **Issue 2**

  Error received. GPO <GPO_name> on domain controller <previous_domain_controller> cannot be retrieved from domain controller <replacement_domain_controller>. Wait until domain replication completes and then try again.

  Cause

  When trying to update an entry point domain controller, the cmdlet tries to read the server GPO from the new domain controller; however, the GPO cannot be found on the new domain controller because it has not yet replicated.

  Solution

  The server GPO does not exist on the new domain controller. Make sure that the GPOs have replicated successfully to the new domain controller and try again.

- **Issue 3**

  Error received. You do not have permissions to access GPO <GPO_name>.

  Cause

  When trying to update an entry point domain controller, the cmdlet tries to read the server GPO from the new domain controller; however, the GPO cannot be read on the new domain controller because you do not have the correct permissions.

  Solution

  The GPO exists on the domain controller, but it cannot be read. Make sure that you have the required permissions and try again.

Entry point not part of multisite deployment

Error received. Entry point <entry_point_name> is not part of the multisite deployment. Specify an alternate value.

Cause

The entry point name you specified was not found.

Solution

Make sure that the entry point name is spelled correctly and that GPOs are replicated to the required domain controllers, and then try again. To view the assigned domain controller for each entry point, use `Get-DAEntryPointDC`.

Remote Access server settings

- **Issue 1**

Error received. Server <server_name> in entry point <entry_point_name> cannot be accessed.

Cause

When trying to update an entry point domain controller, the cmdlet tries to read and write the entry point domain controller from all relevant Remote Access servers. The cmdlet was not able to read the data from one or more Remote Access servers.

Solution

Make sure that all relevant Remote Access servers are running and that you have local administrator permissions on all of them and then try again.

- **Issue 2**

  Error received. Settings cannot be saved to the registry on server <server_name> in entry point <entry_point_name>.

  Cause

  When trying to update an entry point domain controller, the cmdlet tries to read and write the entry point domain controller from all relevant Remote Access servers. The cmdlet was not able to write the data to one or more Remote Access servers.

  Solution

  Make sure that all relevant Remote Access servers are running and that you have local administrator permissions on all of them and then try again.

- **Issue 3**

  Error received. GPO updates cannot be applied on <server_name>. Changes will not take effect until the next policy refresh.

  Cause

  When using the cmdlet `Set-DAEntryPointDC`, the *ComputerName* parameter specified is a Remote Access server in an entry point other than the last one added to the Multisite deployment.

  Solution

  Any servers that were not updated can be seen using the **Configuration Status** in the **DASHBOARD** of the Remote Access Management Console. This does not cause any functional problems; however, you can run `gpupdate /force` on any servers that were not updated to get the configuration status updated immediately.

Problem resolving FQDN

Error received. Server <server_name> in entry point <entry_point_name> cannot be accessed.

Cause

While getting the list of DirectAccess servers to modify, the cmdlet was not able to resolve the fully qualified domain name (FQDN) of one of the servers from its computer SID.

Solution

The entry point specified in the error message is associated with a domain controller. Make sure that the domain controller is available for the entry point. If the computer to which the specified SID belongs was removed from the domain, ignore this message and then remove the server from the multisite deployment.

No entry points to update

Warning received. Domain controller settings were not modified. If you think changes are required, ensure that cmdlet parameters are configured correctly, and that GPOs are replicated to the required domain controllers.

Cause

When calling the `Set-DaEntryPointDC` cmdlet with the *ExistingDC* parameter, DirectAccess checks all the entry points and updates the entry points that are associated with the specified domain controller. However, no entry point uses the specified *ExistingDC*.

Solution

To see the list of entry points and their associated domain controllers, use the `Get-DAEntryPointDC` cmdlet. If changes should have been made, make sure that the cmdlet parameters are spelled correctly, and that the GPOs are replicated to the required domain controllers, and then try again.

Troubleshooting General Issues

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic contains troubleshooting information for general issues related to Remote Access.

GPO retrieval error

Error received. DirectAccess server GPO settings cannot be retrieved. Ensure you have edit permissions for the GPO.

The Remote Access management console is unresponsive after receiving this error.

Cause

DirectAccess cannot access the GPO of one of the entry points in the deployment and as a result the configuration fails to load.

Solution

Make sure that each entry point in the deployment has a corresponding GPO on its domain controller and verify that the logged on user has read and write permissions for all GPOs configured in the Remote Access deployment.

As a workaround, use the configuration cmdlets instead of using the Remote Access management console; for example, using `Get-RemoteAccess` and `Get-DAEntryPoint`.

> **NOTE**
> This scenario does not occur when the server GPO of the current entry point isn't available.

You can use the `Get-DAEntryPointDC` cmdlet to list all domain controllers that store server GPOs and `Get-DAMultiSite` in conjunction with `Get-RemoteAccess` to retrieve a complete list of the server GPOs in the deployment. For example:

```
$ServerGpos = Get-DAEntryPointDC | ForEach-Object {
   @{
       GpoName = (Get-RemoteAccess -EntryPoint $_.EntryPointName).ServerGpoName;
        DC = $_.DomainControllerName }
}
$ServerGpos | ForEach-Object { $GpoName = $_['GpoName'] ; $DC = $_['DC'] ; Write-Host "Server GPO '$GpoName'
on DC '$DC'" }
```

Windows 7 to Windows 8 or 10 client upgrade

Symptom. After a Windows 7 client upgrades to Windows 10 or Windows 8 in a multisite deployment, the DirectAccess connection is not visible in the Networks list.

Cause

The Windows 7 GPOs in a multisite deployment do not contain the Windows 8 Network Connectivity Assistant

configuration.

Windows 7 clients should use DirectAccess Connectivity Assistant to monitor their DirectAccess connectivity status which requires a separate manual configuration in the Windows 7 client GPOs. When Windows 7 clients are upgraded to Windows 10 or Windows 8, the Network Connectivity Assistant will not function if the Windows 7 client GPO is still applied.

Solution

If DirectAccess Connectivity Assistant settings are configured in the Windows 7 GPOs, you can resolve this issue before upgrading client computers by modifying the Windows 7 GPOs using the following PowerShell cmdlets:

```
Set-GPRegistryValue -Name <Windows7GpoName> -Domain <DomainName> -Key
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkConnectivityAssistant" -ValueName
"TemporaryValue" -Type Dword -Value 1
Remove-GPRegistryValue -Name <Windows7GpoName> -Domain <DomainName> -Key
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkConnectivityAssistant"
```

If a client has already been upgraded or the DCA is not configured, move the client computer to the Windows 10 or Windows 8 security group.

General cmdlet errors

- **Issue 1**

  Error received. Domain controller <domain_controller> cannot be reached for <server_name or entry_point_name>.

  Cause

  To maintain the configuration consistency in a multisite deployment, it is important to make sure that each GPO is managed by a single domain controller. When the domain controller that manages an entry point's server GPO is not available, Remote Access configuration settings cannot be read or modified.

  Solution

  Follow the procedure "To change the domain controller that manages server GPOs" described in 2.4. Configure GPOs.

- **Issue 2**

  Error received. The primary domain controller in domain <domain_name> cannot be reached.

  Cause

  To maintain the configuration consistency in a multisite deployment, it is important to make sure that each GPO is managed by a single domain controller. Client GPOs are managed on the primary domain controller. If the primary domain controller is not available, Remote Access configuration settings cannot be read or modified.

  Solution

  Follow the procedure "To transfer the PDC emulator role" described in 2.4. Configure GPOs.

Deploy Remote Access with OTP Authentication

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016 and Windows Server 2012 combine DirectAccess and Routing and Remote Access Service (RRAS) VPN into a single Remote Access role.

Scenario description

In this scenario a Remote Access server with DirectAccess enabled is configured to authenticate DirectAccess client users with two-factor one-time password (OTP) authentication, in addition to standard Active Directory credentials.

Prerequisites

Before you begin deploying this scenario, review this list for important requirements:

- Deploy a Single DirectAccess Server with Advanced Settings must be deployed before you deploy OTP.
- Windows 7 Clients must use DCA 2.0 to support OTP.
- OTP does not support PIN change.
- A Public Key Infrastructure must be deployed.

  For more information see: Test Lab Guide Mini-Module: Basic PKI for Windows Server 2012.
- Changing policies outside of the DirectAccess management console or Windows PowerShell cmdlets is not supported.

In this scenario

The OTP authentication scenario includes a number of steps:

1. Deploy a Single DirectAccess Server with Advanced Settings. A single Remote Access server must be deployed before configuring OTP. Planning and deploying a single server includes designing and configuring a network topology, planning and deploying certificates, setting up DNS and Active Directory, configuring Remote Access server settings, deploying DirectAccess clients, and preparing intranet servers.
2. Plan Remote Access with OTP Authentication. In addition to the planning required for a single server, OTP requires planning for a Microsoft certification authority (CA) and certificate templates for OTP; and a RADIUS-enabled OTP server. Planning might also include a requirement for security groups to exempt specific users from strong (OTP or smart card) authentication. For information regarding the configuration of OTP in a multi-forest environment, see Configure a Multi-Forest Deployment.
3. Configure DirectAccess with OTP Authentication. OTP deployment consists of a number of configuration steps, including preparing the infrastructure for OTP authentication, configuring the OTP server, configuring OTP settings on the Remote Access server, and updating DirectAccess client settings.
4. Troubleshoot an OTP Deployment. This troubleshooting section describes a number of the most common errors that can occur when deploying Remote Access with OTP authentication.

Practical applications

Increase security-Using OTP increases the security of your DirectAccess deployment. A user requires OTP credentials in order to gain access to the internal network. A user supplies OTP credentials via the Workplace Connections available in the network connections on the Windows 10 or Windows 8 client computer, or by using DirectAccess Connectivity Assistant (DCA) on client computers running Windows 7. The OTP authentication process works as follows:

1. The DirectAccess client enters domain credentials to access DirectAccess infrastructure servers (over the infrastructure tunnel). If no connection to the internal network is available, due to a specific IKE failure, Workplace Connection on the client computer notifies the user that credentials are required. On client computers running Windows 7, a pop-up requesting smart card credentials appears.
2. After the OTP credentials have been entered, they are sent over SSL to the Remote Access server, together with a request for a short-term smart card logon certificate.
3. The Remote Access server initiates validation of the OTP credentials with the RADIUS-based OTP server.
4. If successful, the Remote Access server signs the certificate request using its registration authority certificate, and sends it back to the DirectAccess client computer
5. The DirectAccess client computer forwards the signed certificate request to the CA and stores the enrolled certificate for use by the Kerberos SSP/AP.
6. Using this certificate the client computer transparently performs standard smart card Kerberos authentication.

Roles and features included in this scenario

The following table lists the roles and features required for the scenario:

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access Management role	The role is installed and uninstalled using the Server Manager console. This role encompasses both DirectAccess, which was previously a feature in Windows Server 2008 R2, and Routing and Remote Access Services which was previously a role service under the Network Policy and Access Services (NPAS) server role. The Remote Access role consists of two components: 1. DirectAccess and Routing and Remote Access Services (RRAS) VPN-DirectAccess and VPN are managed together in the Remote Access Management console. 2. RRAS Routing-RRAS routing features are managed in the legacy Routing and Remote Access console. The Remote Access role is dependent on the following server features: - Internet Information Services (IIS) Web Server - This feature is required to configure the network location server, utilize OTP authentication, and configure the default web probe. - Windows Internal Database-Used for local accounting on the Remote Access server.

ROLE/FEATURE	HOW IT SUPPORTS THIS SCENARIO
Remote Access Management Tools feature	This feature is installed as follows: - It is installed by default on a Remote Access server when the Remote Access role is installed, and supports the Remote Management console user interface. - It can be optionally installed on a server not running the Remote Access server role. In this case it is used for remote management of a Remote Access computer running DirectAccess and VPN. The Remote Access Management Tools feature consists of the following: - Remote Access GUI and Command Line Tools - Remote Access module for Windows PowerShell Dependencies include: - Group Policy Management Console - RAS Connection Manager Administration Kit (CMAK) - Windows PowerShell 3.0 - Graphical Management Tools and Infrastructure

Hardware requirements

Hardware requirements for this scenario include the following:

- A computer that meets the hardware requirements for Windows Server 2016 or Windows Server 2012.
- In order to test the scenario, at least one computer running Windows 10, Windows 8, or Windows 7 configured as a DirectAccess client is required.
- An OTP server that supports PAP over RADIUS.
- An OTP hardware or software token.

Software requirements

There are a number of requirements for this scenario:

1. Software requirements for single server deployment. For more information, see Deploy a Single DirectAccess Server with Advanced Settings.
2. In addition to software requirements for a single server there are a number of OTP-specific requirements:
    a. CA for IPsec authentication-In an OTP deployment DirectAccess must be deployed using IPsec machines certificates issued by a CA. IPsec authentication using the Remote Access server as a Kerberos proxy is not supported in an OTP deployment. An internal CA is required.
    b. CA for OTP authentication-A Microsoft Enterprise CA (running on Windows 2003 Server or later) is required to issue the OTP client certificate. The same CA used for issuing certificates for IPsec authentication can be used. The CA server must be available over the first infrastructure tunnel.
    c. Security group-To exempt users from strong authentication, an Active Directory security group containing these users is required.
    d. Client-side requirements-For Windows 10 and Windows 8 client computers, the Network Connectivity Assistant (NCA) service is used to detect whether OTP credentials are required. If they are, the DirectAccess Media Manager prompts for credentials. NCA is included in the operating

system, and no installation or deployment is required. For Windows 7 client computers, DirectAccess Connectivity Assistant (DCA) 2.0 is required. Learn how to Install and Configure Advanced DirectAccess.

e. Note the following:

   a. OTP authentication can be used in parallel with smart card and Trusted Platform Module (TPM)-based authentication. Enabling OTP authentication in the Remote Access Management console also enables use of smartcard authentication.

   b. During Remote Access configuration users in a specified security group can be exempt from two-factor authentication, and thus authenticate with username/password only.

   c. OTP new PIN and next tokencode modes are not supported

   d. In a Remote Access multisite deployment, OTP settings are global and identify for all entry points. If multiple RADIUS or CA servers are configured for OTP, they are sorted by each Remote Access server according to availability and proximity.

   e. When configuring OTP in a Remote Access multi-forest environment, OTP CAs should be from the resource forest only, and certificate enrollment should be configured across forest trusts. For more information, see AD CS: Cross-forest Certificate Enrollment with Windows Server 2008 R2.

   f. Users who are using a KEY FOB OTP token should insert the PIN followed by the tokencode (without any separators) in the DirectAccess OTP dialog. Users who are using PIN PAD OTP token should insert only the tokencode in the dialog.

   g. When the WEBDAV is enabled then OTP should not be enabled.

Known Issues

The following are known issues when configuring an OTP scenario:

- Remote Access uses a probe mechanism to verify connectivity to RADIUS-based OTP servers. In some cases this might cause an error to be issued on the OTP server. To avoid this issue, do the following on the OTP server:

  - Create a user account that matches the username and password configured on the Remote Access server for the probe mechanism. The username should not define an Active Directory user.

    By default the username on the Remote Access server is DAProbeUser and the password is DAProbePass. These default settings can be modified using the following values in the registry on the Remote Access server:

    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectAccess\OTP\RadiusProbeUser

    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DirectAccess\OTP\ RadiusProbePass

- If you change the IPsec root certificate in a configured and running DirectAccess deployment, OTP stops working. To resolve this issue, on each DirectAccess server, at a Windows PowerShell prompt, run the command: `iisreset`

Plan Remote Access with OTP Authentication

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016 and Windows Server 2012 combine DirectAccess and Routing and Remote Access Service (RRAS) VPN into a single Remote Access role. This overview provides an introduction to the configuration steps required in order to deploy a single Windows Server 2016 or Windows Server 2012 Remote Access multisite deployment.

- Step 1: Deploy a Single DirectAccess Server with Advanced Settings. This step includes planning for the infrastructure required to deploy a single server. It includes planning for network and server settings, certificate requirements, DNS settings, network location server deployment, DirectAccess management servers, Active Directory settings, and Group Policy objects (GPOs).
- Step 2: Plan the RADIUS server deployment
- Step 3: Plan OTP certificate deployment
- Step 4: Plan for OTP on the Remote Access server

After you have completed these planning steps, see Configure Remote Access with OTP Authentication. For information on configuring a multisite deployment as a proof of concept in a lab environment, see Test Lab Guide: Demonstrate DirectAccess with OTP Authentication and RSA SecurID.

Step 1 Plan an Advanced Single Server Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first step in planning a Remote Access with one-time password (OTP) client authentication deployment is to plan and configure an advanced single server deployment.

Plan a single server deployment

Before you deploy Remote Access with OTP, make sure that you have completed all the steps to deploy a single Remote Access server. See Deploy a Single DirectAccess Server with Advanced Settings.

Step 2 Plan the RADIUS Server Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After deploying a single Remote Access server, plan for the one-time password (OTP) authentication server.

TASK	DESCRIPTION
2.1 Plan the RADIUS server	For the OTP authentication server, Remote Access in Windows Server 2016 and Windows Server 2012 supports any RADIUS-enabled OTP server that supports the password authentication protocol (PAP).

2.1 Plan the RADIUS server

Note the following when planning a RADIUS server for OTP authentication:

- For most types of OTP deployments, you must configure the Remote Access server as a RADIUS agent. For more information, see the OTP vendor documentation.
- For all OTP deployments, you must synchronize your Active Directory users with your RADIUS server.
- The RADIUS server does not need to be a domain member.
- When you deploy the RADIUS server, you configure a shared secret and the port number for RADIUS traffic. Make a note of these details; they are required when you configure the Remote Access server.

You can view an example test lab guide that sets up OTP authentication with an RSA SecurID server in Test Lab Guide: Demonstrate DirectAccess with OTP authentication and RSA SecurID.

Step 3 Plan OTP Certificate Deployment

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After planning the RADIUS server, you must plan for certification authority (CA) requirements, including the CA that will issue one-time password (OTP) certificates, the OTP certificate template, and the registration authority certificate used by the Remote Access server to sign all DirectAccess client OTP certificate requests. These certificates are used as follows:

1. The DirectAccess client requests an OTP certificate, and the Remote Access server receives the request.
2. The Remote access server verifies the OTP credentials and if they are valid, the server acts as a registration authority, and signs the OTP certificate enrollment request using a short-lived signing certificate.
3. The Remote Access server sends the signed certificate enrollment request back to the DirectAccess client
4. The client then enrolls the OTP certificate from the CA using the certificate enrollment requests signed by the server.
5. The CA verifies the credentials and the request.

TASK	DESCRIPTION
3.1 Plan the OTP CA	Plan the certification authority (CA) to use to issue certificates to DirectAccess clients for OTP authentication.
3.2 Plan the OTP certificate template	Plan the OTP certificate template.
3.3 Plan the registration authority certificate	Plan the registration authority certificate to sign all OTP authentication certificate requests.

3.1 Plan the OTP CA

To deploy DirectAccess using one-time password authentication (OTP), you require an internal CA to issue the OTP authentication certificates to DirectAccess client computers. For this purpose, you can use the same internal CA that you use to issue the certificates that are used for regular IPsec computer authentication.

3.2 Plan the OTP certificate template

Each DirectAccess client requires an OTP authentication certificate in order to gain access to the internal network. You must configure a template on your internal CA for the OTP certificate. Note the following when configuring the OTP certificate template:

- All users who need to perform OTP authentication must have read and enroll permissions for this template.
- The subject name should be built from Active Directory information, to ensure that the subject name matches the OTP user name, and not the name of the Remote Access server that performs the certificate request. The subject name must be in the fully distinguished name format, and the subject alternative name must be in UPN format. This ensures that the enrolled OTP certificate is valid for Smartcard

Kerberos authentication.

- The intended purpose of the certificate must be Smart Card Logon
- Issuance must require one authorized signature. The signature must be configured with the predefined DirectAccess OTP Application Policy set in the registration authority signing certificate template.
- The validity period should be set to one hour.

> **NOTE**
>
> In situations where the CA server is a Windows Server 2003 computer, then the template must be configured on a different computer. This is due to the fact that setting the **Validity period** in hours is not possible when running Windows versions prior to 2008/Vista. If the computer that you use to configure the template does not have the Certification Service role installed, or it is a client computer, then you may need to install the Certificate Templates snap-in. For more information on this subject click here.

- The renewal period should be set to 0.
- (Optional) Certificates and requests should not be stored in the CA database.
- The certificate Enhanced Key Usage parameter must be set correctly, as follows:
  - For the DirectAccess registration signing certificate template use the key 1.3.6.1.4.1.311.81.1.1.
  - For the OTP authentication certificate template use the key 1.3.6.1.4.1.311.20.2.2 key.

3.3 Plan the registration authority certificate

When DirectAccess clients request an OTP certificate, the Remote Access server receives the request from the client. The Remote Access server signs all OTP certificate requests from clients using the registration authority certificate. The CA issues certificates only if the request is signed by the registration authority certificate on the Remote Access server. The certificate must be issued by an internal CA, the certificate cannot be self-signed. It does not have to be issued by the CA that issued the OTP certificates but the CA that issues the OTP certificates must trust the CA that issues the registration authority signing certificate.

See also

- Step 4: Plan OTP for the Remote Access server

Step 4 Plan for OTP on the Remote Access Server

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After planning for the one-time password (OTP) RADIUS server and certificate settings, the final step in planning a Remote Access OTP deployment is to plan for client OTP settings on the Remote Access server.

TASK	DESCRIPTION
4.1 Plan for OTP client exemptions	Plan for exemptions for users that you do not require to authentication using OTP.
4.2 Plan for Windows 7 clients	Plan to deploy the DirectAccess Connectivity Assistant (DCA) 2.0 to Windows 7 client computers.
4.3 Plan for smart cards	Plan for the use of smart cards for additional authorization.

4.1 Plan for OTP client exemptions

When OTP authentication is enabled, by default all users are required to authenticate using a combination of user name and password, and OTP credentials. However, you can allow selected users to authenticate using a user name and password only, without OTP. To do this, create a security group and add any users that you want to exempt from OTP authentication.

> **NOTE**
>
> Only client computers from a single forest may be exempted due to the fact that only one security group can be selected for client exemptions.

4.2 Plan for Windows 7 clients

By default, Windows 7 client computers cannot authenticate using OTP. Windows 7 client computers require DCA 2.0 to authenticate using OTP in a Windows Server 2012 Remote Access deployment. For more information about DCA 2.0, see DirectAccess Connectivity Assistant 2.0 on the Microsoft Download Center.

4.3 Plan for smart cards

When OTP authentication is enabled, the option to enable the use of smart cards for additional authorization is available. Create a security group to allow temporary access in the event that a user's smart card is not functional.

See also

- Configure DirectAccess with OTP authentication

Configure Remote Access with OTP Authentication

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016 and Windows Server 2012 combine DirectAccess and Routing and Remote Access Service (RRAS) VPN into a single Remote Access role. This overview provides an introduction to the configuration steps required in order to deploy a single Windows Server 2016 or Windows Server 2012 Remote Access multisite deployment.

- Step 1: Implement a Single Server Remote Access Deployment. Install and configure a single Remote Access server. For instructions, see Deploy a Single DirectAccess Server with Advanced Settings.
- Step 2: Configure the RADIUS Server.
- Step 3: Configure the Remote Access Server for OTP.
- Step 4: Verify DirectAccess with OTP.

Step 1 Implement a Single Server Remote Access Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first configuration step to deploy Remote Access in a multisite topology is to implement an advanced single server deployment and then plan to add servers to each multisite entry point.

Implement a single server deployment

Before you can configure a multisite deployment, you must configure an advanced single server Remote Access deployment as described in Deploy a Single DirectAccess Server with Advanced Settings.

See also

- Step 2: Configure the multisite infrastructure

Step 2 Configure the RADIUS Server

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Before you configure the Remote Access server to support DirectAccess with OTP support, you configure the RADIUS server.

TASK	DESCRIPTION
2.1. Configure the RADIUS software distribution tokens	On the RADIUS server configure software distribution tokens.
2.2. Configure the RADIUS security information	On the RADIUS server configure the ports and shared secret to be used.
2.3 Adding user account for OTP probing	On the RADIUS server create a new user account for OTP probing.
2.4 Synchronize with Active Directory	On the RADIUS server create user accounts synchronized with Active Directory accounts.
2.5 Configure the RADIUS authentication agent	Configure the Remote Access server as a RADIUS authentication agent.

2.1 Configure the RADIUS software distribution tokens

The RADIUS server must be configured with the necessary license and software and/or hardware distribution tokens to be used by DirectAccess with OTP. This process will be specific to each RADIUS vendor implementation.

2.2 Configure the RADIUS security information

The RADIUS server uses UDP ports for communication purposes, and each RADIUS vendor has its own default UDP ports for incoming and outgoing communication. For the RADIUS server to work with the Remote Access server, make sure that all firewalls in the environment are configured to allow UDP traffic between the DirectAccess and OTP servers over the required ports as needed.

The RADIUS server uses a shared secret for authentication purposes. Configure the RADIUS server with a strong password for the shared secret, and note that this will be used when configuring the DirectAccess server's client computer configuration for use with DirectAccess with OTP.

2.3 Adding user account for OTP probing

On the RADIUS server create a new user account called **DAProbeUser** and give it the password **DAProbePass**.

2.4 Synchronize with Active Directory

The RADIUS server must have user accounts that correspond to the users in Active Directory that will be using DirectAccess with OTP.

To synchronize the RADIUS and Active Directory users

1. Record the user information from Active Directory for all DirectAccess with OTP users.
2. Use the vendor specific procedure to create identical user **domain\username** accounts in the RADIUS server that were recorded.

2.5 Configure the RADIUS authentication agent

The Remote Access server must be configured as a RADIUS authentication agent for the DirectAccess with OTP implementation. Follow the RADIUS vendor instructions to configure the Remote Access server as a RADIUS authentication agent.

Step 3 Configure the Remote Access Server for OTP

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Once the RADIUS server has been configured with software distribution tokens, communication ports are open, a shared secret has been created, user accounts corresponding to Active Directory have been created on the RADIUS server, and the Remote Access server has been configured as a RADIUS authentication agent, then the Remote Access server needs to be configured to support OTP.

TASK	DESCRIPTION
3.1 Exempt users from OTP authentication (optional)	If specific users will be exempted from DirectAccess with OTP authentication, then follow these preliminary steps.
3.2 Configure the Remote Access server to support OTP	On the Remote Access server update the Remote Access configuration to support OTP two-factor authentication.
3.3 Smart cards for additional authorization	Additional information regarding the use of smart cards.

> **NOTE**
> This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

3.1 Exempt users from OTP authentication (optional)

If specific users are to be exempted from OTP authentication, then these steps must be taken prior to the Remote Access configuration:

> **NOTE**
> You must wait for replication between domains to complete when configuring the OTP exemption group.

Create user exemption security group

1. Create a security group in Active Directory for the purpose OTP exemption.
2. Add all users to be exempted from OTP authentication to the security group.

> **NOTE**
> Make sure to include only user accounts, and not computer accounts, in the OTP exemption security group.

3.2 Configure the Remote Access server to support OTP

To configure Remote Access to use two-factor authentication and OTP with the RADIUS server and certificate deployment from the previous sections, use the following steps:

Configure Remote Access for OTP

1. Open **Remote Access Management** and click **Configuration**.
2. In the **DirectAccess Setup** window, under **Step 2 - Remote Access Server**, click **Edit**.
3. Click **Next** three times, and in the **Authentication** section select both **Two factor authentication** and **Use OTP**, and ensure that **Use computer certificates** is checked.

   > **NOTE**
   > After OTP has been enabled on the Remote Access server, if you disable OTP by deselecting **Use OTP**, the ISAPI and CGI extensions will be uninstalled on the server.

4. If Windows 7 support is required, select the **Enable Windows 7 client computers to connect via DirectAccess** check box. Note: As discussed in the planning section, Windows 7 clients must have DCA 2.0 installed to support DirectAccess with OTP.
5. Click **Next**.
6. In the **OTP RADIUS Server** section, double-click the blank **Server Name** field.
7. In the **Add a RADIUS Server** dialog, type the name of the RADIUS server in the **Server name** field. Click **Change** next to the **Shared secret** field, and type the same password that you used when configuring the RADIUS server in the **New secret** and **Confirm new secret** fields. Click **OK** twice, and click **Next**.

   > **NOTE**
   > If the RADIUS server is in a domain that is different than the Remote Access server, then the **Server Name** field must specify the FQDN of the RADIUS server.

8. In the **OTP CA Servers** section select the CA servers to be used for the enrollment of OTP client authentication certificates, and click **Add**. Click **Next**.
9. In the **OTP Certificate Templates** section click **Browse** to select the certificate template used for the enrollment of certificates that are issued for OTP authentication.

   > **NOTE**
   > The certificate template for OTP certificates issued by the corporate CA must be configured without the "Do not include revocation information in issued certificates" option. If this option is selected during the certificate template creation, then OTP client computers will fail to logon properly.

   Click **Browse** to select a certificate template used to enroll the certificate used by the Remote Access server to sign OTP certificate enrollment requests. Click **OK**. Click **Next**.

10. If exempting specific users from DirectAccess with OTP is required, then in the **OTP Exemptions** section select **Do not require users in the specified security group to authenticate using two-factor authentication**. Click **Security Group** and select the security group that was created for OTP exemptions.
11. On the **Remote Access Server Setup** page click **Finish**.
12. In the **DirectAccess Setup** window, under **Step 3 - Infrastructure Servers**, click **Edit**.
13. Click **Next** two times, and in the **Management** section double-click the **Management Servers** field.
14. Enter the **Computer name** or **Address** of the CA server that is configured to issue OTP certificates, and

click **OK**.

15. In the **Remote Access Setup** windows click **Finish**.
16. Click **Finish** on the **DirectAccess Expert Wizard**.
17. On the **Remote Access Review** dialog box click **Apply**, wait for the DirectAccess policy to be updated, and click **Close**.
18. On the **Start** screen, type**powershell.exe**, right-click **powershell**, click **Advanced**, and click **Run as administrator**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
19. In the Windows PowerShell window, type **gpupdate /force** and press ENTER.

To configure Remote Access for OTP using PowerShell commands:

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

To configure Remote Access to use two-factor authentication on a deployment that currently uses computer certificate authentication:

```
Set-DAServer -UserAuthentication TwoFactor
```

To configure Remote Access to use OTP authentication using the following settings:

- An OTP server named OTP.corp.contoso.com.
- A CA server named APP1.corp.contoso.com\corp-APP1-CA1.
- A certificate template named DAOTPLogon used for the enrollment of certificates that are issued for OTP authentication.
- A certificate template named DAOTPRA used to enroll the Registration Authority certificate used by the Remote Access server to sign OTP certificate enrollment requests.

```
Enable-DAOtpAuthentication -CertificateTemplateName 'DAOTPLogon' -SigningCertificateTemplateName 'DAOTPRA' -
CAServer @('APP1.corp.contoso.com\corp-APP1-CA1') -RadiusServer OTP.corp.contoso.com -SharedSecret Abcd123$
```

After executing the PowerShell commands complete steps 12-19 from the previous procedure to configure the Remote Access server to support OTP.

> **NOTE**
> Make sure to verify that you have applied the OTP settings on the Remote Access server before you add an entry point.

3.3 Smart cards for additional authorization

On the Authentication page of Step 2 in the Remote Access Setup Wizard, you can require the use of smart cards for access to the internal network. When this option is selected, the Remote Access Setup Wizard configures the IPsec connection security rule for the intranet tunnel on the DirectAccess server to require tunnel mode authorization with smart cards. Tunnel mode authorization allows you to specify that only authorized computers or users can establish an inbound tunnel.

To use smart cards with IPsec tunnel mode authorization for the intranet tunnel, you must deploy a public key infrastructure (PKI) with smart cards infrastructure.

Because your DirectAccess clients are using smart cards for access to the intranet, you can also use authentication mechanism assurance, a feature of Windows Server 2008 R2, to control access to resources, such as files, folders, and printers, based on whether the user logged on with a smart card-based certificate. Authentication mechanism assurance requires a domain functional level of Windows Server 2008 R2.

Allowing access for users with unusable smart cards

To allow temporary access for users with smart cards that are unusable, do the following:

1. Create an Active Directory security group to contain the user accounts of users who temporarily cannot use their smart cards.
2. For the DirectAccess server Group Policy Object, configure global IPsec settings for IPsec tunnel authorization and add the Active Directory security group to the list of authorized users.

To grant access to a user that cannot use their smart card, temporarily add their user account to the Active Directory security group. Remove the user account from the group when the smart card is usable.

Under the covers: Smart card authorization

Smart card authorization works by enabling tunnel mode authorization on the intranet tunnel connection security rule of the DirectAccess server for a specific Kerberos-based security identifier (SID). For smart card authorization, this is the well-known SID (S-1-5-65-1), which maps to smart card-based logons. This SID is present in a DirectAccess client's Kerberos token and is referred to as "This Organization Certificate" when configured in the global IPsec tunnel mode authorization settings.

When you enable smart card authorization in Step 2 of the DirectAccess Setup Wizard, the DirectAccess Setup Wizard configures the global IPsec tunnel mode authorization setting with this SID for the DirectAccess server Group Policy Object. To view this configuration in the Windows Firewall with Advanced Security snap-in for the DirectAccess server Group Policy Object, do the following:

1. Right click Windows Firewall with Advanced Security, and then click Properties.
2. On the IPsec Settings tab, in IPsec tunnel authorization, click Customize.
3. Click the Users tab. You should see the "NT AUTHORITY\This Organization Certificate" as an authorized user.

Step 4 Verify DirectAccess with OTP

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to verify that you have correctly configured your DirectAccess with OTP deployment.

To verify OTP health on the Remote Access server

1. On the Remote Access server open the **Remote Access Management** console.
2. Under **Remote Access Servers** click the Remote Access server that has been configured for OTP support.
3. Click **Operations Status**.
4. Verify that the status of OTP displays the green icon and is Working.

> **NOTE**
>
> The health status update interval will be a maximum of the sum of the values from the registry key HKLM\SYSTEM\CCS\Services\Ramgmtsvc\parameters\HealthRefreshTimeout and the **Time interval for server activity** that was set in the Remote Access configuration.

To verify access to internal resources using OTP authentication

1. Connect a DirectAccess client computer to the corporate network and run **gpupdate /force** from the command prompt to obtain the group policy.
2. Disconnect the client computer from the corporate network, connect to the external network, and attempt to access internal resources. You should not have access to the internal resources.
3. In the case of a software token, access the OTP client token using the vendor instructions, and note the current token code. When a hardware token is used, follow the vendor instructions for authentication.
4. Click the **Network connections** icon in the notification area to access the DA Media Manager.
5. Click the **DirectAccess Connection**, and click **Continue**.
6. Enter the token code noted previously, and click **OK**. Wait for authentication to complete. The DirectAccess Workplace Connection status will now be **Connected**.
7. Attempt to access internal resources. You should be able to access all corporate resources.

Troubleshoot an OTP Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to troubleshoot the most common errors that may occur when configuring a Remote Access deployment using OTP authentication.

- Troubleshooting authentication issues
- Troubleshooting enabling OTP

Troubleshooting Authentication Issues

12/9/2022 • 10 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic contains troubleshooting information for issues related to problems users may have when attempting to connect to DirectAccess using OTP authentication. DirectAccerss OTP related events are logged on the client computer in Event Viewer under **Applications and Services Logs/Microsoft/Windows/OtpCredentialProvider**. Make sure that this log is enabled when troubleshooting issues with DirectAccess OTP.

Failed to access the CA that issues OTP certificates

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log). OTP certificate enrollment for user <username> failed on CA server <CA_name>, request failed, possible reasons for failure: CA server name cannot be resolved, CA server cannot be accessed over the first DirectAccess tunnel or the connection to the CA server cannot be established.

Cause

The user provided a valid one-time password and the DirectAccess server signed the certificate request; however, the client computer cannot contact the CA that issues OTP certificates to finish the enrollment process.

Solution

On the DirectAccess server, run the following Windows PowerShell commands:

1. Get the list of configured OTP issuing CAs and check the value of 'CAServer': `Get-DAOtpAuthentication`
2. Make sure that the CAs are configured as a management servers: `Get-DAMgmtServer -Type All`
3. Make sure that the client computer has established the infrastructure tunnel: In the Windows Firewall with Advanced Security console, expand **Monitoring/Security Associations**, click **Main Mode**, and make sure that the IPsec security associations appear with the correct remote addresses for your DirectAccess configuration.

DirectAccess server connectivity issues

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log)

One of the following errors:

- A connection cannot be established to Remote Access server <DirectAccess_server_hostname> using base path <OTP_authentication_path> and port <OTP_authentication_port>. Error code: <internal_error_code>.
- User credentials cannot be sent to Remote Access server <DirectAccess_server_hostname> using base path <OTP_authentication_path> and port <OTP_authentication_port>. Error code: <internal_error_code>.
- A response was not received from Remote Access server <DirectAccess_server_hostname> using base

path <OTP_authentication_path> and port <OTP_authentication_port>. Error code: <internal_error_code>.

Cause

The client computer cannot access the DirectAccess server over the Internet, due to either network issues or to a misconfigured IIS server on the DirectAccess server.

Solution

Make sure that the Internet connection on the client computer is working, and make sure that the DirectAccess service is running and accessible over the Internet.

Failed to enroll for the DirectAccess OTP logon certificate

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log). Certificate enrollment from CA <CA_name> failed. The request was not signed as expected by the OTP signing certificate, or the user does not have permission to enroll.

Cause

The one-time password provided by the user was correct, but the issuing certification authority (CA) refused to issue the OTP logon certificate. The certificate request may not be properly signed with the correct EKU (OTP registration authority application policy), or the user does not have the "Enroll" permission on the DA OTP template.

Solution

Make sure that DirectAccess OTP users have permission to enroll for the DirectAccess OTP logon certificate and that the proper "Application Policy" is included in the DA OTP registration authority signing template. Also make sure that the DirectAccess registration authority certificate on the Remote Access server is valid. See 3.2 Plan the OTP certificate template and 3.3 Plan the registration authority certificate.

Missing or invalid computer account certificate

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log). OTP authentication cannot be completed because the computer certificate required for OTP cannot be found in local machine certificate store.

Cause

DirectAccess OTP authentication requires a client computer certificate to establish an SSL connection with the DirectAccess server; however, the client computer certificate was not found or is not valid, for example, if the certificate expired.

Solution

Make sure that the computer certificate exists and is valid:

1. On the client computer, in the MMC certificates console, for the Local Computer account, open **Personal/Certificates**.
2. Make sure that there is a certificate issued that matches the computer name and double-click the certificate.
3. On the **Certificate** dialog box, on the **Certificate Path** tab, under **Certificate status**, make sure that it says "This certificate is OK."

If a valid certificate is not found, delete the invalid certificate (if it exists) and re-enroll for the computer certificate by either running `gpupdate /Force` from an elevated command prompt or restarting the client computer.

Missing CA that issues OTP certificates

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log). OTP authentication cannot be completed because the DA server did not return an address of an issuing CA.

Cause

Either there are no CAs that issue OTP certificates configured, or all of the configured CAs that issue OTP certificates are unresponsive.

Solution

1. Use the following command to get the list of CAs that issue OTP certificates (the CA name is shown in CAServer): `Get-DAOtpAuthentication`.
2. If no CAs are configured:
   a. Use either the command `Set-DAOtpAuthentication` or the Remote Access Management console to configure the CAs that issue the DirectAccess OTP logon certificate.
   b. Apply the new configuration and force the clients to refresh the DirectAccess GPO settings by running `gpupdate /Force` from an elevated command prompt or restarting the client machine.
3. If there are CAs configured, make sure they're online and responding to enrollment requests.

Misconfigured DirectAccess server address

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log). OTP authentication cannot complete as expected. The name or address of the Remote Access server cannot be determined. Error code: <error_code>. DirectAccess settings should be validated by the server administrator.

Cause

The address of the DirectAccess server is not configured properly.

Solution

Check the configured DirectAccess server address using `Get-DirectAccess` and correct the address if it is misconfigured.

Make sure the latest settings are deployed on the client computer by running `gpupdate /force` from an elevated command prompt or restart the client machine.

Failed to generate the OTP logon certificate request

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log). The certificate request for OTP authentication cannot be initialized. Either a private key cannot be generated, or user <username> cannot access certificate template <OTP_template_name> on the domain controller.

Cause

There are two possible causes for this error:

- The user doesn't have permission to read the OTP logon template.
- The user's computer can't access the domain controller because of network issues.

Solution

- Review the permissions setting on the OTP logon template and make sure that all users provisioned for DirectAccess OTP have 'Read' permission.
- Make sure that the domain controller is configured as a management server and that the client machine can reach the domain controller over the infrastructure tunnel. See 3.2 Plan the OTP certificate template.

No connection to the domain controller

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log). A connection with the domain controller for the purpose of OTP authentication cannot be established. Error code: <error_code>.

Cause

There are two possible causes for this error:

- The user's computer has no network connectivity.
- The domain controller isn't accessible over the infrastructure tunnel.

Solution

- Make sure that the domain controller is configured as a management server by running the following command from a PowerShell prompt: `Get-DAMgmtServer -Type All`.
- Make sure that the client computer can reach the domain controller over the infrastructure tunnel.

OTP provider requires challenge/response

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log). OTP authentication with Remote Access server (<DirectAccess_server_name>) for user (<username>) required a challenge from the user.

Cause

The OTP provider used requires the user to provide additional credentials in the form of a RADIUS challenge/response exchange, which is not supported by Windows Server 2012 DirectAccess OTP.

Solution

Configure the OTP provider to not require challenge/response in any scenario.

Incorrect OTP logon template used

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log). The CA template from which user <username> requested a certificate is not configured to issue OTP certificates.

Cause

The DirectAccess OTP logon template was replaced and the client computer is attempting to authenticate using

an older template.

Solution

Make sure the client computer is using the latest OTP configuration by performing one of the following:

- Force a Group Policy update by running the following command from an elevated command prompt: `gpupdate /Force`.
- Restart the client machine.

Missing OTP signing certificate

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log). An OTP signing certificate cannot be found. The OTP certificate enrollment request cannot be signed.

Cause

The DirectAccess OTP signing certificate cannot be found on the Remote Access server; therefore, the user certificate request can't be signed by the Remote Access server. Either there is no signing certificate, or the signing certificate has expired and was not renewed.

Solution

Perform these steps on the Remote Access server.

1. Check the configured OTP signing certificate template name by running the PowerShell cmdlet `Get-DAOtpAuthentication` and inspect the value of `SigningCertificateTemplateName`.
2. Use the Certificates MMC snap-in to make sure that a valid certificate enrolled from this template exists on the computer.
3. If no such certificate exists, delete the expired certificate (if one exists) and enroll for a new certificate based on this template.

To create the OTP signing certificate template see 3.3 Plan the registration authority certificate.

Missing or incorrect UPN/DN for the user

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (client event log)

One of the following errors:

- User <username> cannot be authenticated with OTP. Ensure that a UPN is defined for the user name in Active Directory. Error code: <error_code>.
- User <username> cannot be authenticated with OTP. Ensure that a DN is defined for the user name in Active Directory. Error code: <error_code>.

Error received (server event log)

The user name <username> specified for OTP authentication does not exist.

Cause

The user does not have the User Principal Name (UPN) or Distinguished Name (DN) attributes properly set in the user account, these properties are required for proper functioning of DirectAccess OTP.

Solution

Use the Active Directory Users and Computers console on the domain controller to verify that both of these attributes are properly set for the authenticating user.

OTP certificate is not trusted for login

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Cause

The CA that issues OTP certificates is not in the enterprise NTAuth store; therefore, enrolled certificates can't be used for logon. This can occur in multi domain and multiforest environments where cross domain CA trust is not established.

Solution

Make sure that the certificate of the root of the CA hierarchy that issues OTP certificates is installed in the enterprise NTAuth Certificate store of the domain to which the user is attempting to authenticate.

Windows could not verify user credentials

Scenario. User fails to authenticate using OTP with the error: "Authentication failed due to an internal error"

Error received (Client computer). Something went wrong while Windows was verifying your credentials. Try again, or ask your administrator for help.

Cause

The Kerberos authentication protocol does not work when the DirectAccess OTP logon certificate does not include a CRL. The DirectAccess OTP logon certificate does not include a CRL because either:

- The DirectAccess OTP logon template was configured with the option **Do not include revocation information in issued certificates**.
- The CA is configured not to publish CRLs.

Solution

1. To confirm the cause for this error, in the Remote Access Management console, in **Step 2 Remote Access Server**, click **Edit**, and then in the **Remote Access Server Setup** wizard, click **OTP Certificate Templates**. Make a note of the certificate template used for the enrollment of certificates that are issued for OTP authentication. Open the Certification Authority console, in the left pane, click **Certificate Templates**, double-click the OTP logon certificate to view the certificate template properties.

   To solve this issue, configure a certificate for the OTP logon certificate and do not select the **Do not include revocation information in issued certificates** check box on the **Server** tab of the template properties dialog box.

2. On the CA server, open the Certification Authority MMC, right click the issuing CA and click **Properties**. On the **Extensions** tab make sure that CRL publishing is correctly configured.

Troubleshooting Enabling OTP

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic contains troubleshooting information for issues related to enabling DirectAccess OTP authentication using either the **Enable-DAOtpAuthentication** PowerShell cmdlet or the Remote Access Management console.

Failed to enroll the OTP signing certificate

Error received (server event log). An OTP signing certificate cannot be enrolled using certificate template <OTP_signing_template_name>

Cause

There are three possible causes for this error:

- The template doesn't exist.
- The permissions set on the template do not allow the DirectAccess server to enroll.
- There is no network connectivity to the issuing certification authority (CA).

Solution

1. Make sure that the OTP signing certificate template with the given name:
   a. Exists and has the proper permissions.
   b. Is set to be issued by at least one CA that can issue certificates to the DirectAccess server.
2. If the template doesn't exist, create it as described in 3.3 Plan the registration authority certificate, or if another matching template exists reconfigure DirectAccess OTP with the new template name.

Failed to enable DirectAccess OTP when WebDAV is installed

Scenario. While attempting to apply the DirectAccess OTP configuration in the Remote Access Management console or by using the `Enable-DAOtpAuthentication` PowerShell cmdlet, the operation fails.

Error received (server event log). DirectAccess OTP settings cannot be applied because the WebDAV IIS extension is running on the server. Remove WebDAV and apply the settings again.

Cause

The DirectAccess OTP service is incompatible with the WebDAV Publishing feature and cannot be enabled while WebDAV is installed.

Solution

Uninstall the WebDAV role:

1. In the Server Manager console, in the left-pane, click **IIS**.
2. In the main pane, scroll to **ROLES AND FEATURES**.

3. Right-click **WebDAV Publishing**, and then click **Remove Role or Feature**.
4. Complete the Remove Roles and Features Wizard.
5. Re-apply the DirectAccess OTP configuration.

No templates available in the Remote Access Management console

Scenario. While configuring OTP or registration authority certificate templates using the Remote Access Management console, some, or all of the templates are missing from the selection windows.

Cause

There are two possible causes for this error:

- The template is not configured according to the DirectAccess OTP requirements and so it cannot be selected.
- The selected CAs under **OTP CA Servers** are not configured to issue the required templates.

Solution

1. Make sure that the OTP logon template and the OTP signing certificate template are configured properly as described in 3.2 Plan the OTP certificate template and 3.3 Plan the registration authority certificate.
2. Make sure that the configured CAs in the **OTP CA Servers** list are configured to issues the relevant templates:
   a. On the CA server, open the Certification Authority console.
   b. In the left pane, expand the chosen CA server.
   c. Click **Certificate Templates** and make sure the required templates are enabled. If not, right-click **Certificate Templates**, click **New**, click **Certificate Template to issue**, and then select the templates you want to enable.

Cannot set renewal period of OTP template to 1 hour

Scenario. When configuring the DirectAccess OTP logon template using Windows 2003 CA, it is not possible to set the renewal period of the template to 1 hour.

Cause

The Certificate Templates MMC snap-in in Windows Server 2003 doesn't allow you to set the renewal period of a template to 1 hour.

Solution

Install Certificate Templates snap-in on a post-Windows Server 2003 server and use it to configure the OTP logon template, see Install the Certificate Templates Snap-In.

Deploy Remote Access in a Multi-Forest Environment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The Remote Access configuration tools (the Remote Access Management console and the Windows PowerShell cmdlets) are designed to work well in a single forest environment containing one or more domains. However, when Remote Access is deployed in a multi-forest environment, the Remote Access administrator must perform some manual configuration for a successful deployment. This guide describes the planning and configuration steps for a multi-forest deployment; including when one-time password (OTP) authentication is used.

- Plan a multiforest deployment
- Configure a multiforest deployment

Plan a Multi-Forest Deployment

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes the planning steps required when configuring Remote Access in a multi-forest deployment.

Prerequisites

Before you begin deploying this scenario, review this list for important requirements:

- Two-way trust is required.

Plan trust between forests

When you decide to enable access to resources from a new forest, allow clients from the new forest to use DirectAccess, or add Remote Access servers from the new forest as entry points to the Remote Access deployment, you must make sure that a full trust; that is, a two-way transitive trust, is configured between the two forests, see Trust types. Full trust between forests is a prerequisite for a multi-forest deployment to allow administrators to perform operations such as editing GPOs in the new forest, using security groups from new forest as the client security group, performing remote calls (WinRM, RPC) to computers in the new forest, and authenticating remote clients from the new forest.

Plan Remote Access administrator permissions

When you configure Remote Access it updates and sometimes creates GPOs in each of the domains that contain Remote Access servers or clients. In a multi-forest environment, as in single-forest environments, the Remote Access administrator must have permissions to write and modify DirectAccess GPOs and their security filters and optionally have permissions to create links for the DirectAccess GPOs in all involved forests. These permissions are required regardless of the forest to which the Remote Access administrator belongs.

In addition, the Remote Access administrator must be a local administrator on all Remote Access servers including on the Remote Access servers from the new forest that are added as entry points to the original Remote Access deployment.

Plan client security groups

You must configure at least one security group in the new forest for DirectAccess client machines in the new forest. This is because a single security group cannot contain accounts from several forests.

NOTE

- DirectAccess requires at least one Windows 10® or Windows® 8 client security group for each forest. However, it is recommended to have one Windows 10 or Windows 8 client security group for each domain that contains Windows 10 or Windows 8 clients.
- When multisite is enabled, DirectAccess requires at least one Windows 7® client security group per forest for each DirectAccess entry point in which Windows 7 client computers are supported. However, it is recommended to have a separate Windows 7 client security group for each entry point for each domain that contains Windows 7 clients.

For DirectAccess to be applied on client computers in additional domains, client GPOs must be created in those domains. Adding security groups triggers writing new client GPOs for the new domains; therefore, if you add a new security group from a new domain to the list of DirectAccess client security groups, a client GPO will be automatically created on the new domain and client computers from the new domain will get the DirectAccess settings via the client GPO.

Note that if you add a client from a new domain to an existing security group that is already configured as a DirectAccess client security group, the client GPO will not be created automatically by DirectAccess on the new domain. The client in the new domain will not receive the DirectAccess settings and will not be able to connect using DirectAcecss.

Plan certification authorities

If the DirectAccess deployment is configured to use One-Time Password (OTP) authentication, each forest contains the same signing certificate templates but with different Oid values. This results in the forests not being able to be configured as a single configuration unit. To resolve this issue and configure OTP in a multi-forest environment, see the section " Configure OTP in a multi-forest deployment" in the topic Configure a Multi-Forest Deployment.

When using IPsec machine certificate authentication, all client and server computers must have a computer certificate issued by the same root or intermediate certification authority, regardless of the forest to which they belong.

Plan OTP exemptions

If you are using DirectAccess OTP authentication, note that the OTP exemption security group is limited to users of a single forest. This is because each security group can contain only users from a single forest and only one such security group can be configured.

Configure a Multi-Forest Deployment

12/9/2022 • 9 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to configure a Remote Access multi-forest deployment in several possible scenarios. All of the scenarios assume that DirectAccess is currently deployed on a single forest called Forest1, and that you are configuring DirectAccess to work with a new forest called Forest2.

Access resources from Forest2

In this scenario, DirectAccess is already deployed on Forest1, and is configured to allow clients from Forest1 to access the corporate network. By default, clients connected via DirectAccess can access only resources in Forest1 and cannot access any servers in Forest2.

To enable DirectAccess clients to access resources from Forest2

1. If the DNS suffix of Forest2 is not part of the DNS suffix of Forest1, add NRPT rules with the suffixes of the domains in Forest2, and optionally, add the suffixes of the domains in Forest2 to the DNS suffix search list.
2. Add the relevant internal IPv6 prefixes in Forest2 if IPv6 is deployed on the internal network.

Enable clients from Forest2 to connect via DirectAccess

In this scenario, you configure the Remote Access deployment to allow clients from Forest2 to access the corporate network. It is assumed that you have created the required security groups for client computers in Forest2.

To allow clients from Forest2 to access the corporate network

1. Add the security group of the clients from Forest2.
2. If the DNS suffix of Forest2 is not part of the DNS suffix of Forest1, add NRPT rules with the suffixes of the clients' domain in Forest2 to enable access to the domain controllers for authentication, and optionally, add the suffixes of the domains in Forest2 to the DNS suffix search list.
3. Add the internal IPv6 prefixes in Forest2 to enable DirectAccess to create the IPsec tunnel to the domain controllers for authentication.
4. Refresh the management servers list.

Add entry points from Forest2

In this scenario, DirectAccess is deployed in a multisite configuration on Forest1, and you want to add a Remote Access server, named DA2, from Forest2 as an entry point to the existing DirectAccess multisite deployment.

To add a Remote Access server from Forest2 as an entry point

1. Make sure that the Remote Access administrator has sufficient permissions to write GPOs on the domain of DA2, and that the Remote Access administrator is a local administrator on DA2.
2. Add DA2 as an entry point.
3. Add NRPT rules with the suffixes of the domains in Forest2 to enable access to the domain controllers for authentication, and optionally, add the suffixes of the domains in Forest2 to the DNS suffix search list.

4. Add the relevant internal IPv6 prefixes in Forest2, if required, to enable Remote Access to establish the IPsec tunnel to the corporate resources and to make sure that NCSI probes work correctly.

5. Refresh the management servers list.

Configure OTP in a multi-forest deployment

Note the following terms when configuring OTP in a multi-forest deployment:

- Root CA-The forest(s) main PKI tree CA.
- Enterprise CA-All other CAs.
- Resource Forest-The forest that contains the Root CA, and is considered to be the 'Managing forest\domain'.
- Account Forest-All other forests in the topology.

The PowerShell script, PKISync.ps1, is required for this procedure. See AD CS: PKISync.ps1 Script for Cross-forest Certificate Enrollment.

> **NOTE**
> This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

Configure CAs as certificate publishers

1. Enable LDAP referral support on all of the enterprise CAs in all of the forests by running the following command from an elevated command prompt:

```
certutil -setreg Policy\EditFlags +EDITF_ENABLELDAPREFERRALS
```

2. Add all enterprise CA computer accounts to the Active Directory Cert Publishers security groups in each of the account forests.

3. Restart all of the certsvc services on all of the CA computers in all of the forests by running the following command from an elevated command prompt:

```
net stop certsvc && net start certsvc
```

4. Extract the root CA certificate by running the following command from an elevated command prompt:

```
certutil -config <Computer-Name>\<Root-CA-Name> -ca.cert <root-ca-cert-filename.cer>
```

   (If you run the command on the root CA you can omit the connection information, -config <Computer-Name>\<Root-CA-Name>)

   a. Import the Root CA certificate from the previous step on the Account Forest CA by running the following command from an elevated command prompt:

```
certutil -dspublish -f <root-ca-cert-filename.cer> RootCA
```

   b. Grant Resource Forest certificate templates Read/Write permissions to the <Account Forest>\<Administrator account>.

c. Extract all resource forest enterprise CA certificates by running the following command from an elevated command prompt:

```
certutil -config <Computer-Name>\<Enterprise-CA-Name> -ca.cert <enterprise-ca-cert-filename.cer>
```

(If you run the command on the root CA you can omit the connection information, -config <Computer-Name>\<Root-CA-Name>)

d. Import the Enterprise CA certificates from the previous step on the Account Forest CA by running the following commands from an elevated command prompt:

```
certutil -dspublish -f <enterprise-ca-cert-filename.cer> NTAuthCA
certutil -dspublish -f <enterprise-ca-cert-filename.cer> SubCA
```

e. Remove account forest OTP certificate templates from the list of issued Certificate Templates.

Delete and import OTP certificate templates

1. Delete OTP certificate templates from the Account Forest; that is, Forest2.

2. Copy certificate templates and Oid objects from the Resource Forest to each of the Account Forests using the following PowerShell commands:

```
.\PKISync.ps1 -sourceforest <resource forest DNS> -targetforest <account forest DNS> -type Template -cn <DA OTP registration authority template common name>.
.\PKISync.ps1 -sourceforest <resource forest DNS> -targetforest <account forest DNS> -type Template -cn <Secure DA OTP logon certificate template common name>.
.\PKISync.ps1 -sourceforest <resource forest DNS> -targetforest <account forest DNS> -type Oid -f
```

Publish OTP certificate templates

- Issue the newly imported certificate templates on all Account Forests CAs.

Extract and Synchronize the CA

1. Extract all Enterprise CA certificates from the Account Forests by running the following commands from an elevated command prompt:

```
certutil -config <Computer-Name>\<Enterprise-CA-Name> -ca.cert <enterprise-ca-cert-filename.cer>
```

2. Synchronize CAs across forests from the Account Forests to the Resource Forest using the following PowerShell command:

```
.\PKISync.ps1 -sourceforest <account forest DNS> -targetforest <resource forest DNS> -type CA -cn <enterprise CA sanitized name> -f
```

3. Synchronize CAs across forests from the Resource Forest to the Account Forests using the following PowerShell command:

```
.\PKISync.ps1 -sourceforest <resource forest DNS> -targetforest <account forest DNS> -type CA -cn <enterprise CA sanitized name> -f
```

Configuration procedures

The following sections contain the configuration procedures for the above scenario deployments. After completing a procedure, return to the scenario to continue.

Add NRPT rules and DNS suffixes

Clients that connect via DirectAccess to the corporate network use the Name Resolution Policy Table (NRPT) to determine which DNS server should be used to resolve the address of different resources. This allows the client to resolve corporate resource addresses and helps the client maintain a proper inside-corporate/outside-corporate classification, which is required to keep DirectAccess working. The DirectAccess configuration tools automatically detect the root DNS suffix of Forest1 and add it to the NRPT table. However, the FQDN suffixes of Forest2 are not added automatically to the NRPT table, and the Remote Access administrator must add them manually.

The DNS suffix search list allows the clients to use short label names instead of FQDNs. The Remote Access configuration tools automatically add all the domains in Forest1 to the DNS suffix search list. If you want to enable clients to use short label names for resources in Forest2, you need to add them manually.

To add a DNS suffix to the NRPT table and domain suffixes to the DNS suffix search list

1. In the middle pane of the Remote Access Management console, in the **Step 3 Infrastructure Servers** area, click **Edit**.
2. On the **Network Location Server** page, click **Next**.
3. On the **DNS** page, in the table, enter any additional name suffixes that are part of the corporate network in Forest 2. In **DNS Server Address**, enter the DNS server address manually, or by clicking **Detect**. If you don't enter the address, the new entries are applied as NRPT exemptions. Then click **Next**.
4. Optional: On the **DNS Suffix Search List** page, add any DNS suffixes by entering the suffix in the **New Suffix** box, and then clicking **Add**. Then click **Next**.
5. On the **Management** page, click **Finish**.
6. In middle pane of the Remote Access Management console, click **Finish**.
7. On the **Remote Access Review** dialog box, click **Apply**.
8. On the **Applying Remote Access Setup Wizard Settings** dialog box, click **Close**.

Add internal IPv6 prefix

> **NOTE**
> Adding an internal IPv6 prefix is relevant only when IPv6 is deployed on the internal network.

Remote Access manages a list of IPv6 prefixes for corporate resources. Only resources with these IPv6 prefixes may be accessed by clients that are connected via DirectAccess. Because the Remote Access Management console and Windows PowerShell commands automatically add the IPv6 prefixes of Forest1, and might not add the prefixes of other forests, you must add any missing prefixes of Forest2 manually.

To add an IPv6 prefix

1. In the middle pane of the Remote Access Management console, in the **Step 2 Remote Access Server** area, click **Edit**.
2. In the Remote Access Server Setup wizard, click **Prefix Configuration**.
3. On the **Prefix Configuration** page, in **Internal network IPv6 prefixes**, add any additional IPv6 prefixes separated by semicolons, for example, 2001:db8:1::/64;2001:db8:2::/64. Then click **Next**.
4. On the **Authentication** page, click **Finish**.
5. In middle pane of the Remote Access Management console, click **Finish**.

6. On the **Remote Access Review** dialog box, click **Apply**.

7. On the **Applying Remote Access Setup Wizard Settings** dialog box, click **Close**.

Add client security groups

To enable Windows 8 client computers from Forest2 to access resources through DirectAccess, you must add the security group from Forest2 to the Remote Access deployment.

To add Windows 8 client security groups

1. In the middle pane of the Remote Access Management console, in the **Step 1 Remote Clients** area, click **Edit**.

2. In the DirectAccess Client Setup wizard, click **Select Groups**, and then on the **Select Groups** page, click **Add**.

3. On the **Select Groups** dialog box, select the security groups containing DirectAccess client computers. Then click **Next**.

4. On the **Network Connectivity Assistant** page, click **Finish**.

5. In middle pane of the Remote Access Management console, click **Finish**.

6. On the **Remote Access Review** dialog box, click **Apply**.

7. On the **Applying Remote Access Setup Wizard Settings** dialog box, click **Close**.

To enable Windows 7 client computers from Forest2 to access resources through DirectAccess when multisite is enabled, you must add the security group from Forest2 to the Remote Access deployment for each entry point. For information about adding Windows 7 security groups, see the description of the **Client Support** page in 3.6. Enable the multisite deployment.

Refresh the management servers list

Remote Access automatically discovers the infrastructure servers in all the forests that contain DirectAccess configuration GPOs. If DirectAccess was deployed on a server from Forest1, the server GPO will be written to its domain in Forest1. If you enabled access to DirectAccess for clients from Forest2, the client GPO will be written to a domain in Forest2.

The automatic discovery process of infrastructure servers is required to allow access through DirectAccess to the domain controllers and Microsoft Endpoint Configuration Manager. You must manually start the discovery process.

To refresh the management servers list

1. In the Remote Access Management console, click **Configuration**, and then in the **Tasks** pane, click **Refresh Management Servers**.

2. On the **Refreshing Management Servers** dialog box, click **Close**.

Use Remote Access Monitoring and Accounting

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Remote Access monitoring reports remote user activity and status for DirectAccess and VPN connections. It tracks the number and duration of client connections (among other statistics), and monitors the operations status of the server. An easy-to-use monitoring console provides a view of your entire Remote Access infrastructure. Monitoring views are available for single server, cluster, and multisite configurations.

Note: Windows Server 2012 combines DirectAccess and Routing and Remote Access Service (RRAS) into a single Remote Access role.

> **NOTE**
>
> In addition to this topic, the following topics on monitoring Remote Access are available.
>
> - Monitor the existing load on the Remote Access server
> - Monitor the configuration distribution status of the Remote Access server
> - Monitor the Operations Status of the Remote Access server and its components
> - Identify and resolve Remote Access server operations problems
> - Monitor connected remote clients for activity and status
> - Generate a usage report for remote clients using historical data

In this guide

This document contains instructions for leveraging the monitoring capabilities of Remote Access by using the DirectAccess management console and the corresponding Windows PowerShell cmdlets, which are provided as part of the Remote Access server role.

The following monitoring and accounting scenarios are explained:

1. Monitor the existing load on the Remote Access server
2. Monitor the configuration distribution status of the Remote Access server
3. Monitor the operations status of the Remote Access server and its components
4. Identify and resolve Remote Access server operations issues
5. Monitor connected remote clients for activity and status
6. Generate a usage report for remote clients by using historical data

Understand monitoring and accounting

Before you begin monitoring and accounting tasks for remote clients, you need to understand the difference between the two.

- **Monitoring** shows actively connected users at a given point in time.
- **Accounting** keeps a history of users who have connected to the corporate network, and their usage details (for compliance and auditing purposes).

Remote client monitoring is based on connections. There are two types of tunnel connections that are established by DirectAccess clients:

- **Machine tunnel traffic connections**: This tunnel is established by the computer, in system context, to access servers that are required for name resolution, authentication, remediation updating, and so on.
- **User tunnel traffic connections**: This tunnel is established by the user account on the computer, in a user context, when the user tries to access a resource on the corporate network. Depending on the deployment requirements, a user might have to provide strong credentials (for example, by using a smart card or providing a one-time password) to access the corporate network resources.

For DirectAccess, a connection is uniquely identified by the IP address of the remote client. For example, if a machine tunnel is open for a client computer, and a user is connected from that computer, these would be using the same connection. In a situation where the user disconnects and connects again while the machine tunnel is still active, it is a single connection.

Monitor the existing load on the Remote Access server

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Note: Windows Server 2012 combines DirectAccess and Routing and Remote Access Service (RRAS) into a single Remote Access role.

The term **Load** refers to the statistics that relate to the number of connections on the Remote Access server. Following are the steps required to track the load on the Remote Access server.

You can use the monitoring dashboard that is available in the management console on the Remote Access server to view the load statistics for the server, or you can use Performance Monitor counters to track the statistics.

> **NOTE**
>
> You must be signed in as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this topic. If you cannot complete a task while you are signed in with an account that is a member of the Administrators group, try performing the task while you are signed in with an account that is a member of the Domain Admins group.

To use the monitoring dashboard to monitor the Remote Access server load

1. In **Server Manager**, click **Tools**, and then click **Remote Access Management**.
2. Click **DASHBOARD** to navigate to **Remote Access Dashboard** in the **Remote Access Management Console**.
3. On the monitoring dashboard, notice the **Remote Client Status** tile within the **Server Status** tile. This tile lists statistics such as the total number of remote clients that are connected, the total number of DirectAccess clients that are connected, and the maximum number of users who connected in last 24 hours.
4. You can click **Refresh** under **Tasks** in the right pane to reload the health status. To change the default refresh interval, click **Configure Refresh Interval** under **Tasks**.

To use the Performance Monitor tool to monitor performance counters on the Remote Access server

1. Click **Start**, click **Administrative Tools**, and then double-click **Performance Monitor**.
2. Under **Performance**, click **Performance Monitor**.
3. Click the **Add** button (denoted by a green cross icon) in the **Performance Monitor** toolbar.
4. From the list of **Available Counters**, select all the counters in the **RAS** and **RAmgmtsvc** categories, and then click **Add>>**.
5. Again, from the list of **Available Counters**, select all the counters in the **IPsec Connections** category, and then click **Add>>.**
6. Click **OK** to add the selected counters in the **Performance Monitor** console for tracking.

Performance Monitor will now graphically show the selected server load statistics.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
PS> Get-RemoteAccessConnectionStatisticsSummary
```

Monitor the configuration distribution status of the Remote Access server

12/9/2022 • 4 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Note: Windows Server 2012 combines DirectAccess and Remote Access Service (RAS) into a single Remote Access role.

The Remote Access Management Console compares the configuration versions from all the monitored servers to verify that they match and are using the latest configuration version. This shows whether the latest configuration version (which is specified in the Group Policy Objects or GPOs) was distributed to all of the servers and whether it was successfully applied on the servers.

To use the monitoring dashboard to monitor the configuration distribution

1. In **Server Manager**, click **Tools**, and then click **Remote Access Management**.
2. Click **DASHBOARD** to navigate to **Remote Access Dashboard** in the **Remote Access Management Console**.
3. On the monitoring dashboard, notice the **Configuration Status** tile at the top center. This tile shows the current status of the configuration distribution.

The following table shows the messages that are generated by the **Configuration Status** tile, their meanings, and the necessary administrative action (if any).

SEVERITY	MESSAGE	MEANING	WHAT TO DO?
Success	The configuration was distributed successfully.	The configuration in the GPO was successfully applied on the server.	No action needed.
Warning	Configuration for server [*server name*] not retrieved from the domain controller. The GPO is not linked.	The configuration in the GPO did not yet reach the server. This could be because the GPO is not linked to the server.	Link the GPO to a scope of management that is applied to the server, or in a staging GPO scenario, manually export the settings from the staging GPO and import them to the production GPO. For more information about staging GPOs, see **Managing Remote Access GPOs with limited permissions** in Step-1-Plan-the-DirectAccess-Infrastructure. For GPO staging steps, see **Configuring Remote Access GPOs with limited permissions** in Step 1: Configure the DirectAccess Infrastructure.

SEVERITY	MESSAGE	MEANING	WHAT TO DO?
Warning	Configuration for server [*server name*] not yet retrieved from the domain controller.	The configuration in the GPO did not yet reach the server. It can take up to 10 minutes to propagate a new configuration.	Allow more time for the policies to update on the server.
Error	Configuration for server [*server name*] cannot be retrieved from the domain controller.	The configuration in the GPO did not reach the server, and more than 10 minutes have passed since the configuration was changed.	This could happen in one of the following scenarios: - The server has no connectivity to the domain to update the policies. You can run "gpupdate /force" on the server to force a policy update. - GPO replication might be required to retrieve the updated configuration. - There is no writable domain controller in the Active Directory site of the Remote Access server. Wait for GPOs to replicate to all domain controllers, and then use the Windows PowerShell cmdlet **Set-DAEntryPointDC** to associate the entry point with a writable domain controller in Active Directory in the Remote Access server.
Warning	Configuration for server [*server name*] retrieved from the domain controller, but not yet applied.	The configuration in the GPO reached the server but is not yet applied. It can take up to 15 minutes before the configuration is applied.	Allow more time for the configuration to be fully applied to the server.

SEVERITY	MESSAGE	MEANING	WHAT TO DO?
Error	Configuration for server [*server name*] retrieved from the domain controller cannot be applied.	The configuration in the GPO reached the server but is not successfully applied, and more than 15 minutes have passed since the configuration was changed.	This could happen in one of the following scenarios: 1. The configuration is currently in the process of being applied. This is shown as an error because it may have taken a long time to retrieve the configuration from the GPO. To verify whether this is the reason, use **Task Scheduler** and navigate to Microsoft\Windows\RemoteAccess to verify that **RAConfigTask** is currently running. 2. If **RAConfigTask** is not currently running, it may have failed to apply the configuration on the server. Check for errors in **Event Viewer** under the Remote Access server operations channel, which is located at \Applications and Services Logs\Microsoft\Windows\RemoteAccess-RemoteAccessServer. Check for errors in **OPERATIONS STATUS** in the Remote Access Management Console. For more information, see Monitor the Operations Status of the Remote Access server and its components.
Error	Configuration for multisite servers retrieved from the domain controller. The configuration does not match on all servers.	There is an inconsistency between the configuration versions of the server GPOs in the multisite deployment. Ideally, all the server GPOs for all entry points will have the same global configuration, but for some reason, they are out of sync.	This can happen when a configuration change failed and was not rolled back successfully. You should restore the GPOs from a backup state where all server GPOs were synchronized. For information about a script that you can use, see Back up and Restore Remote Access Configuration.

Monitor the operations status of the Remote Access server and its components

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Note: Windows Server 2012 combines DirectAccess and Routing and Remote Access Service (RRAS) into a single Remote Access role.

The management console in the Remote Access server can be used to monitor its operations status.

> **NOTE**
> You must be signed in as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the task described in this topic. If you cannot complete a task while you are signed in with an account that is a member of the Administrators group, try performing the task while you are signed in with an account that is a member of the Domain Admins group.

To monitor the Remote Access server operations status

1. In **Server Manager**, click **Tools**, and then click **Remote Access Management**.
2. Click **DASHBOARD** to navigate to **Remote Access Reporting** in the **Remote Access Management Console**.
3. On the monitoring dashboard, notice the **Operations Status** tile within the **Server Status** tile. This tile lists the server operations status and the status of all the server's components.
4. Click **Refresh** under **Tasks** in the right pane to reload the operations status. The operations status is automatically refreshed every five minutes, which is the default refresh interval. To change the default refresh interval, click **Configure Refresh Interval**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

> **NOTE**
> The command for operations status of a cluster is included for reference.

```
PS> Get-RemoteAccessHealth
PS> Get-RemoteAccessHealth -Cluster
```

Identify and resolve Remote Access server operations problems

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Note: Windows Server 2012 combines DirectAccess and Routing and Remote Access Service (RRAS) into a single Remote Access role.

You can using the following procedures to identify Remote Access server operations issues, their root causes, and the resolution required to fix the issues.

> **NOTE**
>
> You must be signed in as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this topic. If you cannot complete a task while you are signed in with an account that is a member of the Administrators group, try performing the task while you are signed in with an account that is a member of the Domain Admins group.

This topic includes information about performing the following tasks:

- Simulate an operations issue
- Identify the operations issue and take corrective action
- Restore the IP Helper service

Simulate an operations issue

Caution

Because your Remote Access server is probably configured properly and not experiencing any issues, you can use the following procedure to simulate an operations issue. If your server is currently servicing clients in a production environment, you may not want to take these actions at this time. Rather, you can read through the steps to understand how to address issues that might arise on your Remote Access server in the future.

The IP Helper service (IPHlpSvc) hosts IPv6 transitioning technologies (such as IP-HTTPS, 6to4, or Teredo), and it is required for the DirectAccess server to function properly. To demonstrate a simulated operations issue on the Remote Access server, you must stop the (IPHlpSvc) network service.

To stop the IP Helper service

1. On the **Start** screen of the Remote Access server, click **Administrative Tools**, and then double-click **Services**.
2. In the list of **Services**, scroll down and right-click **IP Helper**, and then click **Stop**.

Identify the operations issue and take corrective action

Turning off the IP Helper service will cause a serious error on the Remote Access server. The monitoring dashboard will show the operations status of the server and the details of the issue.

To identify the details and take corrective action

1. In **Server Manager**, click **Tools**, and then click **Remote Access Management**.
2. Click **DASHBOARD** to navigate to **Remote Access Dashboard** in the **Remote Access Management Console**.

3. Make sure your Remote Access server is selected in the left pane, and then in the middle pane, click **Operations Status**.

4. You will see the list of components with green or red icons, which indicate their operational status. Click the **IP-HTTPS** row in the list. When you selected a row, the details for the operation are shown in the **Details** pane as follows:

   Error

   The IP Helper service (IPHlpSvc) has stopped. DirectAccess might not function as expected. The IP Helper service provides tunnel connectivity by using the connectivity platform, IPv6 transition technologies, and IP-HTTPS.

   Causes

   a. The IP Helper service has stopped.

   b. The IP Helper service is not responding.

   Resolution

   a. To ensure that the service is running, type **Get-Service iphlpsvc** at a Windows PowerShell prompt.

   b. To enable the service, type **Start-Service iphlpsvc** from an elevated Windows PowerShell prompt.

   c. To restart the service, type **Restart-Service iphlpsvc** from an elevated Windows PowerShell prompt.

Restore the IP Helper service

To restore the IP Helper service on your Remote Access server, you can follow the Resolution steps above to start or restart the service, or you can use the following procedure to reverse the procedure that you used to simulate the IP Helper service failure.

To restart the IP Helper service on the Remote Access server

1. On the **Start** screen, click **Administrative Tools**, and then double-click **Services**.

2. In the list of **Services**, scroll down and right-click **IP Helper**, and then click **Start**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
PS> Get-RemoteAccessHealth | Where-Object {$_.Component -eq "IP-HTTPS"} | Format-List -Property *
```

Monitor connected remote clients for activity and status

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Note: Windows Server 2012 combines DirectAccess and Remote Access Service (RAS) into a single Remote Access role.

You can use the management console on the Remote Access server to monitor remote client activity and status.

> **NOTE**
> You must be signed in as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this topic. If you cannot complete a task while you are signed in with an account that is a member of the Administrators group, try performing the task while you are signed in with an account that is a member of the Domain Admins group.

To monitor remote client activity and status

1. In **Server Manager**, click **Tools**, and then click **Remote Access Management**.
2. Click **REPORTING** to navigate to **Remote Access Reporting** in the **Remote Access Management Console**.
3. Click **Remote Client Status** to navigate to the remote client activity and status user interface in the **Remote Access Management Console**.
4. You will see the list of users who are connected to the Remote Access server and detailed statistics about them. Click the first row in the list that corresponds to a client. When you select a row, the remote user activity is shown in the preview pane.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
PS> Get-RemoteAccessConnectionStatistics
```

The user statistics can be filtered, based on criteria selections, by using the fields in the following table.

FIELD NAME	VALUE
Username	The user name or alias of the remote user. Wildcard characters can be used to select a group of users, such as contoso* or *\administrator.
Hostname	The computer account name of the remote user. An IPv4 or IPv6 address also can be specified.

FIELD NAME	VALUE
Type	DirectAccess or VPN. If DirectAccess is selected, all remote users who are connected by using DirectAccess are listed. If VPN is selected, all remote users who are connected by using VPN are listed.
ISP address	The IPv4 or IPv6 address of the remote user.
IPv4 address	The inner IPv4 address of the tunnel that connect the remote user to the corporate network.
IPv6 address	The inner IPv6 address of the tunnel that connects the remote user to the corporate network.
Protocol/Tunnel	The transitioning technology that is used by the remote client. This is Teredo, 6to4, or IP-HTTPS for DirectAccess users, and it is PPTP, L2TP, SSTP, or IKEv2 for VPN users.
Resource Accessed	All users who are accessing a particular corporate resource or an endpoint. The value that corresponds to this field is the hostname/IP address of the server.
Server	The Remote Access server to which clients are connected. This is relevant only for cluster and multisite deployments.

Generate a usage report for remote clients using historical data

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Note: Windows Server 2012 combines DirectAccess and Routing and Remote Access Service (RRAS) into a single Remote Access role.

The management console on the Remote Access server can be used to generate a usage report for the remote clients that are accessing the server. To generate a usage report for remote clients, you first enable accounting on the Remote Access server. After you generate the report, you can use the monitoring dashboard that is available in the management console on the Remote Access server to view the load statistics on the server.

> **NOTE**
>
> You must be signed in as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this topic. If you cannot complete a task while you are signed in with an account that is a member of the Administrators group, try performing the task while you are signed in with an account that is a member of the Domain Admins group.

To enable accounting on the Remote Access Server

1. In **Server Manager**, click **Tools**, and then click **Remote Access Management**.
2. Click **REPORTING** to navigate to **Remote Access Reporting** in the **Remote Access Management Console**.
3. Click **Configure Accounting** in the **Remote Access Reporting** task pane.
4. Select the **Use inbox accounting** check box to enable accounting on the Remote Access server.
5. Click **Apply** to enable the accounting configuration on the server, and then click **Close** after the server has applied the configuration successfully.

To generate the usage report

1. In **Server Manager**, click **Tools**, and then click **Remote Access Management**.
2. Click **REPORTING** to navigate to **Remote Access Reporting** in the **Remote Access Management Console**.
3. In the middle pane, click dates in the calendar to select the report duration **Start date:** and **End date:**, and then click **Generate Report**.
4. You will see the list of users that have connected to the Remote Access server within the selected time and detailed statistics about them. Click the first row in the list. When you select a row, the remote user activity is shown in the preview pane. Now select the **Server Load Statistics** tab in the preview pane to see the historical load on the server.

   Click the **Server Load Statistics** tab in the preview pane to see the historical load on the server.

NOTE

Understanding sessions

Remote Access accounting is based on the concept of **sessions**. In contrast to a **connection**, a **session** is uniquely identified by a combination of remote client IP address and user name. For example, if a machine tunnel is formed from the remote client, named Client1, a session will be created and stored in the accounting database. When a user named User1 connects from that client after some time passes (but the machine tunnel is still active), the session is recorded as a separate session. The distinction of sessions is to retain the distinction between machine tunnel and user tunnel.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

In the following script, change the date range for which you want a report in the **-StartDateTime** and **-EndDateTime** parameters.

```
PS> Get-RemoteAccessConnectionStatisticsSummary -StartDateTime "1 October 2010 00:00:00" -EndDateTime "14
October 2010 00:00:00"
Shows server load statistics.
PS> Get-RemoteAccessUserActivity -HostIPAddress 10.0.0.1 -StartDateTime "1 October 2010 00:00:00" -
EndDateTime "14 October 2010 00:00:00"
```

Manage DirectAccess Clients Remotely

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Remote Access monitoring reports remote user activity and status for DirectAccess and VPN connections. It tracks the number and duration of client connections (among other statistics), and monitors the operations status of the server. An easy-to-use monitoring console provides a view of your entire Remote Access infrastructure. Monitoring views are available for single server, cluster, and multisite configurations.

Note: Windows Server 2016 combines DirectAccess and Remote Access Service (RAS) into a single Remote Access role.

In this guide

This document contains instructions for leveraging the monitoring capabilities of Remote Access by using the DirectAccess management console and the corresponding Windows PowerShell cmdlets, which are provided as part of the Remote Access server role.

The following monitoring and accounting scenarios are explained:

1. Monitor the existing load on the Remote Access server
2. Monitor the configuration distribution status of the Remote Access server
3. Monitor the operations status of the Remote Access server and its components
4. Identify and resolve Remote Access server operations issues
5. Monitor connected remote clients for activity and status
6. Generate a usage report for remote clients by using historical data

Understand monitoring and accounting

Before you begin monitoring and accounting tasks for remote clients, you need to understand the difference between the two.

- **Monitoring** shows actively connected users at a given point in time.
- **Accounting** keeps a history of users who have connected to the corporate network, and their usage details (for compliance and auditing purposes).

Remote client monitoring is based on connections. There are two types of tunnel connections that are established by DirectAccess clients:

- **Machine tunnel traffic connections**: This tunnel is established by the computer, in system context, to access servers that are required for name resolution, authentication, remediation updating, and so on.
- **User tunnel traffic connections**: This tunnel is established by the user account on the computer, in a user context, when the user tries to access a resource on the corporate network. Depending on the deployment requirements, a user might have to provide strong credentials (for example, by using a smart card or providing a one-time password) to access the corporate network resources.

For DirectAccess, a connection is uniquely identified by the IP address of the remote client. For example, if a machine tunnel is open for a client computer, and a user is connected from that computer, these would be using

the same connection. In a situation where the user disconnects and connects again while the machine tunnel is still active, it is a single connection.

Plan Deployment for Remote Management of DirectAccess Clients

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The following topics provide planning steps for deploying a single Remote Access server running that can be used for remote management of DirectAccess clients.

Step 1: Plan the Remote Access Infrastructure: This topic helps you plan the network topology and server settings, firewall requirements, certificate requirements, Domain Name System requirements, DirectAccess network location server and management servers' configuration, Active Directory requirements, and Group Policy Object creation.

Step 2: Plan the Remote Access Deployment: Plan client and server deployment strategies and infrastructure servers' configurations.

Step 1 Plan the Remote Access Infrastructure

12/9/2022 • 37 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

NOTE

Windows Server 2016 combines DirectAccess and Routing and Remote Access Service (RRAS) into a single Remote Access role.

This topic describes the steps for planning an infrastructure that you can use to set up a single Remote Access server for remote management of DirectAccess clients. The following table lists the steps, but these planning tasks do not need to be done in a specific order.

TASK	DESCRIPTION
Plan network topology and server settings	Decide where to place the Remote Access server (at the edge or behind a Network Address Translation (NAT) device or firewall), and plan IP addressing and routing.
Plan firewall requirements	Plan for allowing Remote Access through edge firewalls.
Plan certificate requirements	Decide if you will use Kerberos protocol or certificates for client authentication, and plan your website certificates. IP-HTTPS is a transition protocol that is used by DirectAccess clients to tunnel IPv6 traffic over IPv4 networks. Decide whether to authenticate IP-HTTPS for the server by using a certificate that is issued by a certification authority (CA), or by using a self-signed certificate that is issued automatically by the Remote Access server.
Plan DNS requirements	Plan the Domain Name System (DNS) settings for the Remote Access server, infrastructure servers, local name resolution options, and client connectivity.
Plan the network location server configuration	Decide where to place the network location server website in your organization (on the Remote Access server or an alternative server), and plan the certificate requirements if the network location server will be located on the Remote Access server. **Note:** The network location server is used by DirectAccess clients to determine whether they are located on the internal network.
Plan management servers' configurations	Plan for management servers (such as update servers) that are used during remote client management. **Note:** Administrators can remotely manage DirectAccess client computers that are located outside the corporate network by using the Internet.

TASK	DESCRIPTION
Plan Active Directory requirements	Plan your domain controllers, your Active Directory requirements, client authentication, and multiple domain structure.
Plan Group Policy Object creation	Decide what GPOs are required in your organization and how to create and edit the GPOs.

Plan network topology and settings

When you plan your network, you need to consider the network adapter topology, settings for IP addressing, and requirements for ISATAP.

Plan network adapters and IP addressing

1. Identify the network adapter topology that you want to use. Remote Access can be set up with any of the following topologies:

   - With two network adapters: The Remote Access server is installed at the edge with one network adapter connected to the Internet and the other to the internal network.
   - With two network adapters: The Remote Access server is installed behind a NAT device, firewall, or router, with one network adapter connected to a perimeter network and the other to the internal network.
   - With one network adapter: The Remote Access server is installed behind a NAT device, and the single network adapter is connected to the internal network.

2. Identify your IP addressing requirements:

   DirectAccess uses IPv6 with IPsec to create a secure connection between DirectAccess client computers and the internal corporate network. However, DirectAccess does not necessarily require connectivity to the IPv6 Internet or native IPv6 support on internal networks. Instead, it automatically configures and uses IPv6 transition technologies to tunnel IPv6 traffic across the IPv4 Internet (6to4, Teredo, or IP-HTTPS) and across your IPv4-only intranet (NAT64 or ISATAP). For an overview of these transition technologies, see the following resources:

   - IPv6 Transition Technologies
   - IP-HTTPS Tunneling Protocol Specification

3. Configure required adapters and addressing according to the following table. For deployments that are behind a NAT device using a single network adapter, configure your IP addresses by using only the **Internal network adapter** column.

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER[1, ABOVE]	ROUTING REQUIREMENTS

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv4 Internet and IPv4 intranet	Configure the following: - Two static consecutive public IPv4 addresses with the appropriate subnet masks (required for Teredo only). - A default gateway IPv4 address for your Internet firewall or local Internet service provider (ISP) router. **Note:** The Remote Access server requires two consecutive public IPv4 addresses so that it can act as a Teredo server and Windows-based Teredo clients can use the Remote Access server to detect the type of NAT device.	Configure the following: - An IPv4 intranet address with the appropriate subnet mask. - A connection-specific DNS suffix for your intranet namespace. A DNS server should also be configured on the internal interface. **Caution:** Do not configure a default gateway on any intranet interfaces.	To configure the Remote Access server to reach all subnets on the internal IPv4 network, do the following: - List the IPv4 address spaces for all the locations on your intranet. - Use the `route add -p` or `netsh interface ipv4 add route` commands to add the IPv4 address spaces as static routes in the IPv4 routing table of the Remote Access server.

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv6 Internet and IPv6 intranet	Configure the following: - Use the autoconfigured address configuration provided by your ISP. - Use the `route print` command to ensure that a default IPv6 route that points to the ISP router exists in the IPv6 routing table. - Determine if the ISP and intranet routers are using default router preferences as described in RFC 4191, and if they are use a higher default preference than your local intranet routers. If both of these are true, no other configuration for the default route is required. The higher preference for the ISP router ensures that the active default IPv6 route of the Remote Access server points to the IPv6 Internet. Because the Remote Access server is an IPv6 router, if you have a native IPv6 infrastructure, the Internet interface can also reach the domain controllers on the intranet. In this case, add packet filters to the domain controller in the perimeter network that prevent connectivity to the IPv6 address of the Internet interface of the Remote Access server.	Configure the following: If you are not using default preference levels, configure your intranet interfaces by using the `netsh interface ipv6 set InterfaceIndex ignoredefaultroutes=enabled` command. This command ensures that additional default routes that point to intranet routers will not be added to the IPv6 routing table. You can obtain the InterfaceIndex of your intranet interfaces from the display of the `netsh interface show interface` command.	If you have an IPv6 intranet, to configure the Remote Access server to reach all of the IPv6 locations, do the following: - List the IPv6 address spaces for all the locations on your intranet. - Use the `netsh interface ipv6 add route` command to add the IPv6 address spaces as static routes in the IPv6 routing table of the Remote Access server.

DESCRIPTION	EXTERNAL NETWORK ADAPTER	INTERNAL NETWORK ADAPTER	ROUTING REQUIREMENTS
IPv4 Internet and IPv6 intranet	The Remote Access server forwards default IPv6 route traffic by using the Microsoft 6to4 adapter interface to a 6to4 relay on the IPv4 Internet. When native IPv6 is not deployed in the corporate network, you can use the following command to configure a Remote Access server for the IPv4 address of the Microsoft 6to4 relay on the IPv4 Internet: `netsh interface ipv6 6to4 set relay name= <ipaddress> state=enabled` .		

NOTE

- If the DirectAccess client has been assigned a public IPv4 address, it will use the 6to4 relay technology to connect to the intranet. If the client is assigned a private IPv4 address, it will use Teredo. If the DirectAccess client cannot connect to the DirectAccess server with 6to4 or Teredo, it will use IP-HTTPS.
- To use Teredo, you must configure two consecutive IP addresses on the external facing network adapter.
- You cannot use Teredo if the Remote Access server has only one network adapter.
- Native IPv6 client computers can connect to the Remote Access server over native IPv6, and no transition technology is required.

Plan ISATAP requirements

ISATAP is required for remote management of DirectAccessclients, so that DirectAccess management servers can connect to DirectAccess clients located on the Internet. ISATAP is not required to support connections that are initiated by DirectAccess client computers to IPv4 resources on the corporate network. NAT64/DNS64 is used for this purpose. If your deployment requires ISATAP, use the following table to identify your requirements.

ISATAP DEPLOYMENT SCENARIO	REQUIREMENTS
Existing native IPv6 intranet (no ISATAP is required)	With an existing native IPv6 infrastructure, you specify the prefix of the organization during Remote Access deployment, and the Remote Access server does not configure itself as an ISATAP router. Do the following: 1. To ensure that DirectAccess clients are reachable from the intranet, you must modify your IPv6 routing so that default route traffic is forwarded to the Remote Access server. If your intranet IPv6 address space uses an address other than a single 48-bit IPv6 address prefix, you must specify the relevant organization IPv6 prefix during deployment. 2. If you are currently connected to the IPv6 Internet, you must configure your default route traffic so that it is forwarded to the Remote Access server, and then configure the appropriate connections and routes on the Remote Access server, so that the default route traffic is forwarded to the device that is connected to the IPv6 Internet.

ISATAP DEPLOYMENT SCENARIO	REQUIREMENTS
Existing ISATAP deployment	If you have an existing ISATAP infrastructure, during deployment you are prompted for the 48-bit prefix of the organization, and the Remote Access server does not configure itself as an ISATAP router. To ensure that DirectAccess clients are reachable from the intranet, you must modify your IPv6 routing infrastructure so that default route traffic is forwarded to the Remote Access server. This change needs to be done on the existing ISATAP router to which the intranet clients must already be forwarding the default traffic.
No existing IPv6 connectivity	When the Remote Access setup wizard detects that the server has no native or ISATAP-based IPv6 connectivity, it automatically derives a 6to4-based 48-bit prefix for the intranet, and configures the Remote Access server as an ISATAP router to provide IPv6 connectivity to ISATAP hosts across your intranet. (A 6to4-based prefix is used only if the server has public addresses, otherwise the prefix is automatically generated from a unique local address range.) To use ISATAP do the following: 1. Register the ISATAP name on a DNS server for each domain on which you want to enable ISATAP-based connectivity, so that the ISATAP name is resolvable by the internal DNS server to the internal IPv4 address of the Remote Access server. 2. By default, DNS servers running Windows Server 2012 , Windows Server 2008 R2 , Windows Server 2008 , or Windows Server 2003 block resolution of the ISATAP name by using the global query block list. To enable ISATAP, you must remove the ISATAP name from the block list. For more information, see Remove ISATAP from the DNS Global Query Block List. Windows-based ISATAP hosts that can resolve the ISATAP name automatically configure an address with the Remote Access server as following: 1. An ISATAP-based IPv6 address on an ISATAP tunneling interface 2. A 64-bit route that provides connectivity to the other ISATAP hosts on the intranet 3. A default IPv6 route that points to the Remote Access server. The default route ensures that intranet ISATAP hosts can reach DirectAccess clients When your Windows-based ISATAP hosts obtain an ISATAP-based IPv6 address, they begin to use ISATAP-encapsulated traffic to communicate if the destination is also an ISATAP host. Because ISATAP uses a single 64-bit subnet for the entire intranet, your communication goes from a segmented IPv4 model of communication, to a single subnet communication model with IPv6. This can affect the behavior of some Active Directory Domain Services (AD DS) and applications that rely on your Active Directory Sites and Services configuration. For example, if you used the Active Directory Sites and Services snap-in to configure sites, IPv4-based subnets, and intersite transports for forwarding requests to servers within sites, this configuration is not used by ISATAP hosts.

ISATAP DEPLOYMENT SCENARIO	REQUIREMENTS
	1. To configure Active Directory Sites and Services for forwarding within sites for ISATAP hosts, for each IPv4 subnet object, you must configure an equivalent IPv6 subnet object, in which the IPv6 address prefix for the subnet expresses the same range of ISATAP host addresses as the IPv4 subnet. For example, for the IPv4 subnet 192.168.99.0/24 and the 64-bit ISATAP address prefix 2002:836b:1:8000::/64, the equivalent IPv6 address prefix for the IPv6 subnet object is 2002:836b:1:8000:0:5efe:192.168.99.0/120. For an arbitrary IPv4 prefix length (set to 24 in the example), you can determine the corresponding IPv6 prefix length from the formula 96 + IPv4PrefixLength. 2. For the IPv6 addresses of DirectAccess clients, add the following: • For Teredo-based DirectAccess clients: An IPv6 subnet for the range 2001:0:WWXX:YYZZ::/64, in which WWXX:YYZZ is the colon-hexadecimal version of the first Internet-facing IPv4 address of the Remote Access server. . • For IP-HTTPS-based DirectAccess clients: An IPv6 subnet for the range 2002:WWXX:YYZZ:8100::/56, in which WWXX:YYZZ is the colon-hexadecimal version of the first Internet-facing IPv4 address (w.x.y.z) of the Remote Access server. . • For 6to4-based DirectAccess clients: A series of 6to4-based IPv6 prefixes that begin with 2002: and represent the regional, public IPv4 address prefixes that are administered by Internet Assigned Numbers Authority (IANA) and regional registries. The 6to4-based prefix for a public IPv4 address prefix w.x.y.z/n is 2002:WWXX:YYZZ::/[16+n], in which WWXX:YYZZ is the colon-hexadecimal version of w.x.y.z. For example, the 7.0.0.0/8 range is administered by American Registry for Internet Numbers (ARIN) for North America. The corresponding 6to4-based prefix for this public IPv6 address range is 2002:700::/24. For information about the IPv4 public address space, see IANA IPv4 Address Space Registry. .

> **IMPORTANT**
>
> Ensure that you do not have public IP addresses on the internal interface of the DirectAccess server. If you have public IP address on the internal interface, connectivity through ISATAP may fail.

Plan firewall requirements

If the Remote Access server is behind an edge firewall, the following exceptions will be required for Remote Access traffic when the Remote Access server is on the IPv4 Internet:

- For IP-HTTPS: Transmission Control Protocol (TCP) destination port 443, and TCP source port 443 outbound.

- For Teredo traffic: User Datagram Protocol (UDP) destination port 3544 inbound, and UDP source port 3544 outbound.
- For 6to4 traffic: IP Protocol 41 inbound and outbound.

> **NOTE**
>
> For Teredo and 6to4 traffic, these exceptions should be applied for both of the Internet-facing consecutive public IPv4 addresses on the Remote Access server.
>
> For IP-HTTPS the exceptions need to be applied on the address that is registered on the public DNS server.

- If you are deploying Remote Access with a single network adapter and installing the network location server on the Remote Access server, TCP port 62000.

> **NOTE**
>
> This exemption is on the Remote Access server, and the previous exemptions are on the edge firewall.

The following exceptions are required for Remote Access traffic when the Remote Access server is on the IPv6 Internet:

- IP Protocol 50
- UDP destination port 500 inbound, and UDP source port 500 outbound.
- ICMPv6 traffic inbound and outbound (only when using Teredo).

When you are using additional firewalls, apply the following internal network firewall exceptions for Remote Access traffic:

- For ISATAP: Protocol 41 inbound and outbound
- For all IPv4/IPv6 traffic: TCP/UD
- For Teredo: ICMP for all IPv4/IPv6 traffic

Plan certificate requirements

There are three scenarios that require certificates when you deploy a single Remote Access server.

- **IPsec authentication**: Certificate requirements for IPsec include a computer certificate that is used by DirectAccess client computers when they establish the IPsec connection with the Remote Access server, and a computer certificate that is used by Remote Access servers to establish IPsec connections with DirectAccess clients.

  For DirectAccess in Windows Server 2012 , the use of these IPsec certificates is not mandatory. As an alternative, the Remote Access server can act as a proxy for Kerberos authentication without requiring certificates. If Kerberos authentication is used, it works over SSL, and the Kerberos protocol uses the certificate that was configured for IP-HTTPS. Some enterprise scenarios (including multisite deployment and one-time password client authentication) require the use of certificate authentication, and not Kerberos authentication.

- **IP-HTTPS server**: When you configure Remote Access, the Remote Access server is automatically configured to act as the IP-HTTPS web listener. The IP-HTTPS site requires a website certificate, and client computers must be able to contact the certificate revocation list (CRL) site for the certificate.
- **Network location server**: The network location server is a website that is used to detect whether client computers are located in the corporate network. The network location server requires a website

certificate. DirectAccess clients must be able to contact the CRL site for the certificate.

The certification authority (CA) requirements for each of these scenarios is summarized in the following table.

IPSEC AUTHENTICATION	IP-HTTPS SERVER	NETWORK LOCATION SERVER
An internal CA is required to issue computer certificates to the Remote Access server and clients for IPsec authentication when you don't use the Kerberos protocol for authentication.	Internal CA: You can use an internal CA to issue the IP-HTTPS certificate; however, you must make sure that the CRL distribution point is available externally.	Internal CA: You can use an internal CA to issue the network location server website certificate. Make sure that the CRL distribution point is highly available from the internal network.
	Self-signed certificate: You can use a self-signed certificate for the IP-HTTPS server. A self-signed certificate cannot be used in a multisite deployment.	Self-signed certificate: You can use a self-signed certificate for the network location server website; however, you cannot use a self-signed certificate in multisite deployments.
	Public CA: We recommend that you use a public CA to issue the IP-HTTPS certificate, this ensures that the CRL distribution point is available externally.	

Plan computer certificates for IPsec authentication

If you are using certificate-based IPsec authentication, the Remote Access server and clients are required to obtain a computer certificate. The simplest way to install the certificates is to use Group Policy to configure automatic enrollment for computer certificates. This ensures that all domain members obtain a certificate from an enterprise CA. If you do not have an enterprise CA set up in your organization, see Active Directory Certificate Services.

This certificate has the following requirements:

- The certificate should have client authentication extended key usage (EKU).
- The client and the server certificates should relate to the same root certificate. This root certificate must be selected in the DirectAccess configuration settings.

Plan certificates for IP-HTTPS

The Remote Access server acts as an IP-HTTPS listener, and you must manually install an HTTPS website certificate on the server. Consider the following when you are planning:

- Using a public CA is recommended, so that CRLs are readily available.
- In the subject field, specify the IPv4 address of the Internet adapter of Remote Access server or the FQDN of the IP-HTTPS URL (the ConnectTo address). If the Remote Access server is located behind a NAT device, the public name or address of the NAT device should be specified.
- The common name of the certificate should match the name of the IP-HTTPS site.
- For the **Enhanced Key Usage** field, use the Server Authentication object identifier (OID).
- For the **CRL Distribution Points** field, specify a CRL distribution point that is accessible by DirectAccess clients that are connected to the Internet.

  > **NOTE**
  >
  > This is only required for clients running Windows 7.

- The IP-HTTPS certificate must have a private key.

- The IP-HTTPS certificate must be imported directly into the personal store.
- IP-HTTPS certificates can have wildcard characters in the name.

Plan website certificates for the network location server

Consider the following when you are planning the network location server website:

- In the **Subject** field, specify an IP address of the intranet interface of the network location server or the FQDN of the network location URL.
- For the **Enhanced Key Usage** field, use the Server Authentication OID.
- For the **CRL Distribution Points** field, use a CRL distribution point that is accessible by DirectAccess clients that are connected to the intranet. This CRL distribution point should not be accessible from outside the internal network.

> **NOTE**
> Ensure that the certificates for IP-HTTPS and network location server have a subject name. If the certificate uses an alternative name, it will not be accepted by the Remote Access Wizard.

Plan DNS requirements

This section explains the DNS requirements for clients and servers in a Remote Access deployment.

DirectAccess client requests

DNS is used to resolve requests from DirectAccess client computers that are not located on the internal network. DirectAccess clients attempt to connect to the DirectAccess network location server to determine whether they are located on the Internet or on the corporate network.

- If the connection is successful, clients are determined to be on the intranet, DirectAccess is not used, and client requests are resolved by using the DNS server that is configured on the network adapter of the client computer.
- If the connection does not succeed, clients are assumed to be on the Internet. DirectAccess clients will use the name resolution policy table (NRPT) to determine which DNS server to use when resolving name requests. You can specify that clients should use DirectAccess DNS64 to resolve names, or an alternative internal DNS server.

When performing name resolution, the NRPT is used by DirectAccess clients to identify how to handle a request. Clients request an FQDN or single-label name such as `<https://internal>`. If a single-label name is requested, a DNS suffix is appended to make an FQDN. If the DNS query matches an entry in the NRPT and DNS4 or an intranet DNS server is specified for the entry, the query is sent for name resolution by using the specified server. If a match exists but no DNS server is specified, an exemption rule and normal name resolution is applied.

When a new suffix is added to the NRPT in the Remote Access Management console, the default DNS servers for the suffix can be automatically discovered by clicking the **Detect** button. Automatic detection works as follows:

- If the corporate network is IPv4-based, or it uses IPv4 and IPv6, the default address is the DNS64 address of the internal adapter on the Remote Access server.
- If the corporate network is IPv6-based, the default address is the IPv6 address of DNS servers in the corporate network.

Infrastructure servers

- **Network location server**

  DirectAccess clients attempt to reach the network location server to determine if they are on the internal network. Clients on the internal network must be able to resolve the name of the network location server, and they must be prevented from resolving the name when they are located on the Internet. To ensure

that this occurs, by default, the FQDN of the network location server is added as an exemption rule to the NRPT. In addition, when you configure Remote Access, the following rules are created automatically:

  - A DNS suffix rule for root domain or the domain name of the Remote Access server, and the IPv6 addresses that correspond to the intranet DNS servers that are configured on the Remote Access server. For example, if the Remote Access server is a member of the corp.contoso.com domain, a rule is created for the corp.contoso.com DNS suffix.
  - An exemption rule for the FQDN of the network location server. For example, if the network location server URL is https://nls.corp.contoso.com, an exemption rule is created for the FQDN nls.corp.contoso.com.

- **IP-HTTPS server**

  The Remote Access server acts as an IP-HTTPS listener and uses its server certificate to authenticate to IP-HTTPS clients. The IP-HTTPS name must be resolvable by DirectAccess clients that use public DNS servers.

Connectivity verifiers

Remote Access creates a default web probe that is used by DirectAccess client computers to verify connectivity to the internal network. To ensure that the probe works as expected, the following names must be registered manually in DNS:

- **directaccess-webprobehost** should resolve to the internal IPv4 address of the Remote Access server, or to the IPv6 address in an IPv6-only environment.
- **directaccess-corpconnectivityhost** should resolve to the local host (loopback) address. You should create A and AAAA records. The value of the A record is 127.0.0.1, and the value of the AAAA record is constructed from the NAT64 prefix with the last 32 bits as 127.0.0.1. The NAT64 prefix can be retrieved by running the **Get-netnatTransitionConfiguration** Windows PowerShell cmdlet.

  > **NOTE**
  > This is valid only in IPv4-only environments. In an IPv4 plus IPv6 or an IPv6-only environment, create only a AAAA record with the loopback IP address ::1.

You can create additional connectivity verifiers by using other web addresses over HTTP or PING. For each connectivity verifier, a DNS entry must exist.

DNS server requirements

- For DirectAccess clients, you must use a DNS server running Windows Server 2012 , Windows Server 2008 R2 , Windows Server 2008 , Windows Server 2003, or any DNS server that supports IPv6.
- You should use a DNS server that supports dynamic updates. You can use DNS servers that do not support dynamic updates, but then entries must be manually updated.
- The FQDN for your CRL distribution points must be resolvable by using Internet DNS servers. For example, if URL https://crl.contoso.com/crld/corp-DC1-CA.crl is in the **CRL Distribution Points** field of the IP-HTTPS certificate of the Remote Access server, you must ensure that the FQDN crld.contoso.com is resolvable by using Internet DNS servers.

Plan for local name resolution

Consider the following when you are planning for local name resolution:

NRPT

You may need to create additional name resolution policy table (NRPT) rules in the following situations:

- You need to add more DNS suffixes for your intranet namespace.

- If the FQDNs of your CRL distribution points are based on your intranet namespace, you must add exemption rules for the FQDNs of the CRL distribution points.
- If you have a split-brain DNS environment, you must add exemption rules for the names of resources for which you want DirectAccess clients that are located on the Internet to access the Internet version, rather than the intranet version.
- If you are redirecting traffic to an external website through your intranet web proxy servers, the external website is available only from the intranet. It uses the addresses of your web proxy servers to permit the inbound requests. In this situation, add an exemption rule for the FQDN of the external website, and specify that the rule uses your intranet web proxy server rather than the IPv6 addresses of intranet DNS servers.

  For example, let's say that you are testing an external website named test.contoso.com. This name is not resolvable through Internet DNS servers, but the Contoso web proxy server knows how to resolve the name and how to direct requests for the website to the external web server. To prevent users who are not on the Contoso intranet from accessing the site, the external website allows requests only from the IPv4 Internet address of the Contoso web proxy. Thus, intranet users can access the website because they are using the Contoso web proxy, but DirectAccess users cannot because they are not using the Contoso web proxy. By configuring an NRPT exemption rule for test.contoso.com that uses the Contoso web proxy, webpage requests for test.contoso.com are routed to the intranet web proxy server over the IPv4 Internet.

Single label names

Single label names, such as `<https://paycheck>`, are sometimes used for intranet servers. If a single label name is requested and a DNS suffix search list is configured, the DNS suffixes in the list will be appended to the single label name. For example, when a user on a computer that is a member of the corp.contoso.com domain types `<https://paycheck>` in the web browser, the FQDN that is constructed as the name is paycheck.corp.contoso.com. By default, the appended suffix is based on the primary DNS suffix of the client computer.

> **NOTE**
>
> In a disjointed name space scenario (where one or more domain computers has a DNS suffix that does not match the Active Directory domain to which the computers are members), you should ensure that the search list is customized to include all the required suffixes. By default, the Remote Access Wizard, configures the Active Directory DNS name as the primary DNS suffix on the client. Make sure to add the DNS suffix that is used by clients for name resolution.

If multiple domains and Windows Internet Name Service (WINS) are deployed in your organization, and you are connecting remotely, single-names can be resolved as follows:

- By deploying a WINS forward lookup zone in the DNS. When trying to resolve computername.dns.zone1.corp.contoso.com, the request is directed to the WINS server that is only using the computer name. The client thinks it is issuing a regular DNS A records request, but it is actually a NetBIOS request.

  For more information, see Managing a Forward Lookup Zone.
- By adding a DNS suffix (for example, dns.zone1.corp.contoso.com) to the default domain GPO.

Split-brain DNS

Split-brain DNS refers to the use of the same DNS domain for Internet and intranet name resolution.

For split-brain DNS deployments, you must list the FQDNs that are duplicated on the Internet and intranet, and decide which resources the DirectAccess client should reach-the intranet or the Internet version. When you want DirectAccess clients to reach the Internet version, you must add the corresponding FQDN as an exemption rule to the NRPT for each resource.

In a split-brain DNS environment, if you want both versions of the resource to be available, configure your intranet resources with names that do not duplicate the names that are used on the Internet. Then instruct your users to use the alternate name when they access the resource on the intranet. For example, configure www.internal.contoso.com for the internal name of www.contoso.com.

In a non-split-brain DNS environment, the Internet namespace is different from the intranet namespace. For example, the Contoso Corporation uses contoso.com on the Internet and corp.contoso.com on the intranet. Because all intranet resources use the corp.contoso.com DNS suffix, the NRPT rule for corp.contoso.com routes all DNS name queries for intranet resources to intranet DNS servers. DNS queries for names with the contoso.com suffix do not match the corp.contoso.com intranet namespace rule in the NRPT, and they are sent to Internet DNS servers. With a non-split-brain DNS deployment, because there is no duplication of FQDNs for intranet and Internet resources, there is no additional configuration needed for the NRPT. DirectAccess clients can access both Internet and intranet resources for their organization.

Plan local name resolution behavior for DirectAccess clients

If a name cannot be resolved with DNS, the DNS Client service in Windows Server 2012 , Windows 8, Windows Server 2008 R2 , and Windows 7 can use local name resolution, with the Link-Local Multicast Name Resolution (LLMNR) and NetBIOS over TCP/IP protocols, to resolve the name on the local subnet. Local name resolution is typically needed for peer-to-peer connectivity when the computer is located on private networks, such as single subnet home networks.

When the DNS Client service performs local name resolution for intranet server names, and the computer is connected to a shared subnet on the Internet, malicious users can capture LLMNR and NetBIOS over TCP/IP messages to determine intranet server names. On the DNS page of the Infrastructure Server Setup Wizard, you can configure the local name resolution behavior based on the types of responses received from intranet DNS servers. The following options are available:

- **Use local name resolution if the name does not exist in DNS**: This option is the most secure because the DirectAccess client performs local name resolution only for server names that cannot be resolved by intranet DNS servers. If the intranet DNS servers can be reached, the names of intranet servers are resolved. If the intranet DNS servers cannot be reached, or if there are other types of DNS errors, the intranet server names are not leaked to the subnet through local name resolution.
- **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)**: This option is recommended because it allows the use of local name resolution on a private network only when the intranet DNS servers are unreachable.
- **Use local name resolution for any kind of DNS resolution error (least secure)**: This is the least secure option because the names of intranet network servers can be leaked to the local subnet through local name resolution.

Plan the network location server configuration

The network location server is a website that is used to detect whether DirectAccess clients are located in the corporate network. Clients in the corporate network do not use DirectAccess to reach internal resources; but instead, they connect directly.

The network location server website can be hosted on the Remote Access server or on another server in your organization. If you host the network location server on the Remote Access server, the website is created automatically when you deploy Remote Access. If you host the network location server on another server running a Windows operating system, you must make sure that Internet Information Services (IIS) is installed on that server, and that the website is created. Remote Access does not configure settings on the network location server.

Make sure that the network location server website meets the following requirements:

- Has an HTTPS server certificate.

- Has high availability to computers on the internal network.
- Is not accessible to DirectAccess client computers on the Internet.
-

In addition, consider the following requirements for clients when you are setting up your network location server website:

- DirectAccess client computers must trust the CA that issued the server certificate to the network location server website.
- DirectAccess client computers on the internal network must be able to resolve the name of the network location server site.

Plan certificates for the network location server

When you obtain the website certificate to use for the network location server, consider the following:

- In the **Subject** field, specify the IP address of the intranet interface of the network location server or the FQDN of the network location URL.
- For the **Enhanced Key Usage** field, use the Server Authentication OID.
- The network location server certificate must be checked against a certificate revocation list (CRL). For the **CRL Distribution Points** field, use a CRL distribution point that is accessible by DirectAccess clients that are connected to the intranet. This CRL distribution point should not be accessible from outside the internal network.

Plan DNS for the network location server

DirectAccess clients attempt to reach the network location server to determine if they are on the internal network. Clients on the internal network must be able to resolve the name of the network location server, but must be prevented from resolving the name when they are located on the Internet. To ensure this occurs, by default, the FQDN of the network location server is added as an exemption rule to the NRPT.

Plan management servers' configuration

DirectAccess clients initiate communication with management servers that provide services such as Windows Update and antivirus updates. DirectAccess clients also use the Kerberos protocol to authenticate to domain controllers before they access the internal network. During remote management of DirectAccess clients, management servers communicate with client computers to perform management functions such as software or hardware inventory assessments. Remote Access can automatically discover some management servers, including:

- Domain controllers: Automatic discovery of domain controllers is performed for the domains that contain client computers and for all domains in the same forest as the Remote Access server.
- Microsoft Endpoint Configuration Manager servers

Domain controllers and Configuration Manager servers are automatically detected the first time DirectAccess is configured. The detected domain controllers are not displayed in the console, but settings can be retrieved using Windows PowerShell cmdlets. If domain controller or Configuration Manager servers are modified, clicking **Update Management Servers** in the console refreshes the management server list.

Management server requirements

- Management servers must be accessible over the infrastructure tunnel. When you configure Remote Access, adding servers to the management servers list automatically makes them accessible over this tunnel.
- Management servers that initiate connections to DirectAccess clients must fully support IPv6, by means of a native IPv6 address or by using an address that is assigned by ISATAP.

Plan Active Directory requirements

Remote Access uses Active Directory as follows:

- **Authentication**: The infrastructure tunnel uses NTLMv2 authentication for the computer account that is connecting to the Remote Access server, and the account must be in an Active Directory domain. The intranet tunnel uses Kerberos authentication for the user to create the intranet tunnel.
- **Group Policy Objects**: Remote Access gathers configuration settings into Group Policy Objects (GPOs), which are applied to Remote Access servers, clients, and internal application servers.
- **Security groups**: Remote Access uses security groups to gather and identify DirectAccess client computers. GPOs are applied to the required security groups.

When you plan an Active Directory environment for a Remote Access deployment, consider the following requirements:

- At least one domain controller is installed on the Windows Server 2012 , Windows Server 2008 R2 Windows Server 2008 , or Windows Server 2003 operating system.

  If the domain controller is on a perimeter network (and therefore reachable from the Internet-facing network adapter of Remote Access server), prevent the Remote Access server from reaching it. You need to add packet filters on the domain controller to prevent connectivity to the IP address of the Internet adapter.
- The Remote Access server must be a domain member.
- DirectAccess clients must be domain members. Clients can belong to:
  - Any domain in the same forest as the Remote Access server.
  - Any domain that has a two-way trust with the Remote Access server domain.
  - Any domain in a forest that has a two-way trust with the forest of the Remote Access server domain.

> **NOTE**
> - The Remote Access server cannot be a domain controller.
> - The Active Directory domain controller that is used for Remote Access must not be reachable from the external Internet adapter of the Remote Access server (the adapter must not be in the domain profile of Windows Firewall).

Plan client authentication

In Remote Access in Windows Server 2012 , you can choose between using built-in Kerberos authentication, which uses user names and passwords, or using certificates for IPsec computer authentication.

Kerberos authentication: When you choose to use Active Directory credentials for authentication, DirectAccess first uses Kerberos authentication for the computer, and then it uses Kerberos authentication for the user. When using this mode of authentication, DirectAccess uses a single security tunnel that provides access to the DNS server, the domain controller, and any other server on the internal network

IPsec authentication: When you choose to use two-factor authentication or Network Access Protection, DirectAccess uses two security tunnels. The Remote Access Setup Wizard configures connection security rules in Windows Firewall with Advanced Security. These rules specify the following credentials when negotiating IPsec security to the Remote Access server:

- The infrastructure tunnel uses computer certificate credentials for the first authentication and user (NTLMv2) credentials for the second authentication. User credentials force the use of Authenticated Internet Protocol (AuthIP), and they provide access to a DNS server and domain controller before the

DirectAccess client can use Kerberos credentials for the intranet tunnel.

- The intranet tunnel uses computer certificate credentials for the first authentication and user (Kerberos V5) credentials for the second authentication.

Plan multiple domains

The management servers list should include domain controllers from all domains that contain security groups that include DirectAccess client computers. It should contain all domains that contain user accounts that might use computers configured as DirectAccess clients. This ensures that users who are not located in the same domain as the client computer they are using are authenticated with a domain controller in the user domain.

This authentication is automatic if the domains are in the same forest. If there is a security group with client computers or application servers that are in different forests, the domain controllers of those forests are not detected automatically. Forests are also not detected automatically. You can run the task **Update Management Servers** in the **Remote Access Management** to detect these domain controllers.

Where possible, common domain name suffixes should be added to the NRPT during Remote Access deployment. For example, if you have two domains, domain1.corp.contoso.com and domain2.corp.contoso.com, instead of adding two entries into the NRPT, you can add a common DNS suffix entry, where the domain name suffix is corp.contoso.com. This happens automatically for domains in the same root. Domains that are not in the same root must be added manually.

Plan Group Policy Object creation

When you configure Remote Access, DirectAccess settings are collected into Group Policy Objects (GPOs). Two GPOs are populated with DirectAccess settings, and they are distributed as follows:

- **DirectAccess client GPO**: This GPO contains client settings, including IPv6 transition technology settings, NRPT entries, and connection security rules for Windows Firewall with Advanced Security. The GPO is applied to the security groups that are specified for the client computers.
- **DirectAccess server GPO**: This GPO contains the DirectAccess configuration settings that are applied to any server that you configured as a Remote Access server in your deployment. It also contains connection security rules for Windows Firewall with Advanced Security.

> **NOTE**
> Configuration of application servers is not supported in remote management of DirectAccess clients because clients cannot access the internal network of the DirectAccess server where the application servers reside. Step 4 in the Remote Access Setup configuration screen is unavailable for this type of configuration.

You can configure GPOs automatically or manually.

Automatically: When you specify that GPOs are created automatically, a default name is specified for each GPO.

Manually: You can use GPOs that have been predefined by the Active Directory administrator.

When you configure your GPOs, consider the following warnings:

- After DirectAccess is configured to use specific GPOs, it cannot be configured to use different GPOs.
- Use the following procedure to back up all Remote Access Group Policy Objects before you run DirectAccess cmdlets:

  Back up and Restore Remote Access Configuration.

- Whether you are using automatically or manually configured GPOs, you need to add a policy for slow link detection if your clients will use 3G. The path for **Policy: Configure Group Policy slow link**

detection is:

Computer configuration/Polices/Administrative Templates/System/Group Policy.

- If the correct permissions for linking GPOs do not exist, a warning is issued. The Remote Access operation will continue, but linking will not occur. If this warning is issued, links will not be created automatically, even if the permissions are added later. Instead the administrator needs to create the links manually.

Automatically created GPOs

Consider the following when using automatically created GPOs:

Automatically created GPOS are applied according to the location and link target, as follows:

- For the DirectAccess server GPO, the location and link target point to the domain that contains the Remote Access server.
- When client and application server GPOs are created, the location is set to a single domain. The GPO name is looked up in each domain, and the domain is filled with DirectAccess settings if it exists.
- The link target is set to the root of the domain in which the GPO was created. A GPO is created for each domain that contains client computers or application servers, and the GPO is linked to the root of its respective domain.

When using automatically created GPOs to apply DirectAccess settings, the Remote Access server administrator requires the following permissions:

- Permissions to create GPOs for each domain.
- Permissions to link to all the selected client domain roots.
- Permissions to link to the server GPO domain roots.
- Security permissions to create, edit, delete, and modify the GPOs.
- GPO read permissions for each required domain. This permission is not required, but it is recommended because it enables Remote Access to verify that GPOs with duplicate names do not exist when GPOs are being created.

Manually created GPOs

Consider the following when using manually created GPOs:

- The GPOs should exist before running the Remote Access Setup Wizard.
- To apply DirectAccess settings, the Remote Access server administrator requires full security permissions to create, edit, delete, and modify the manually created GPOs.
- A search is made for a link to the GPO in the entire domain. If the GPO is not linked in the domain, a link is automatically created in the domain root. If the required permissions to create the link are not available, a warning is issued.

Recovering from a deleted GPO

If a GPO on a Remote Access server, client, or application server has been deleted by accident, the following error message will appear: **GPO (GPO name) cannot be found**.

If a backup is available, you can restore the GPO from the backup. If there is no backup available, you must remove the configuration settings and configure them again.

To remove configuration settings

1. Run the Windows PowerShell cmdlet **Uninstall-RemoteAccess**.
2. Open **Remote Access Management**.

3. You will see an error message that the GPO is not found. Click **Remove configuration settings**. After completion, the server will be restored to an unconfigured state, and you can reconfigure the settings.

Step 2 Plan the Remote Access Deployment

12/9/2022 • 6 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

After you plan for the infrastructure that you intend to use to set up your single Remote Access server for remote management of DirectAccess clients, you are ready to plan the settings that the Remote Access Setup Wizard will use.

> **NOTE**
>
> Before you continue with these tasks, see Step 1: Plan the Remote Access Infrastructure.

TASK	DESCRIPTION
Plan a client deployment strategy	Decide which managed computers will be configured as DirectAccess clients.
Plan a Remote Access server deployment strategy	Plan how to deploy the Remote Access server.
Plan the infrastructure servers' configurations	Plan the infrastructure servers in your Remote Access deployment, including the DirectAccess network location server, DNS servers, and DirectAccess management servers.

Plan a client deployment strategy

There are three decisions to make when you are planning your client deployment:

1. Will DirectAccess be available to mobile computers only, or to every computer in a specified security group?

   When you configure DirectAccess clients in the DirectAccess Client Setup Wizard, you can choose to allow only mobile computers in specified security groups to connect to the server by using DirectAccess. If you restrict access to mobile computers, Remote Access automatically configures a WMI filter to ensure that the DirectAccess client GPO is applied only to mobile computers in the specified security groups. The Remote Access administrator requires permissions to create or modify group policy WMI filters to enable this setting.

2. What security groups will contain the DirectAccess client computers?

   DirectAccess settings are contained in the DirectAccess client Group Policy Object (GPO). The GPO is applied to computers that are part of the security groups that you specify in the DirectAccess Client Setup Wizard. You can specify security groups that are contained in any supported domain.

   Before you configure Remote Access, you need to create the security groups. You can add computers to the security group after you complete the Remote Access deployment. However, if you add client computers that reside in a different domain than the security group, the client GPO will not be applied to those clients. For example, if you created SG1 in domain A for DirectAccess clients, and you later add clients from domain B to this group, the client GPO will not be applied to clients in domain B.

   To avoid this issue, create a new client security group for each domain that contains client computers.

Alternatively, if you do not want to create a new security group, run the **Add-DAClient** Windows PowerShell cmdlet with the name of the new GPO for the new domain.

3. What settings will you configure for the DirectAccess Network Connectivity Assistant?

   The DirectAccess Network Connectivity Assistant runs on client computers and provides additional information about the DirectAccess connection to end users. In the DirectAccess Client Setup Wizard, you can configure the following:

   - **Connectivity verifiers**

     A default web probe is created that clients use to validate connectivity to the internal network. The default name is `https://directaccess-WebProbeHost.<domain_name>`. The name should be registered manually in DNS. You can create other connectivity verifiers that use other web addresses over HTTP or PING. For each connectivity verifier, a DNS entry must exist.

   - **Help Desk email address**

     If end users experience DirectAccess connectivity issues, they can send an email that contains diagnostic information to the Remote Access administrator, who can troubleshoot the issue.

   - **DirectAccess connection name**

     You can specify a DirectAccess connection name to help end users identify the DirectAccess connection on their computer.

   - **Allow DirectAccess clients to use local name resolution**

     Clients require a means of resolving names locally. If you allow DirectAccess clients to use local name resolution, end users can use local DNS servers to resolve names. When end users choose to use local DNS servers for name resolution, DirectAccess does not send resolution requests for single label names to the internal corporate DNS server. It uses local name resolution instead (by using the Link-Local Multicast Name Resolution (LLMNR) and NetBios over TCP/IP protocols).

Plan a Remote Access server deployment strategy

Decisions that you need to make when you are planning to deploy your Remote Access server include:

- **Network topology**

  There are two topologies available when deploying a Remote Access server:

  - **Two adapters**: With two network adapters, Remote Access can be configured with one network adapter connected directly to the Internet and the other connected to the internal network. Or alternatively, the server is installed behind an edge device, such as a firewall or a router. In this configuration one network adapter is connected to the perimeter network, and the other is connected to the internal network.

  - **Single network adapter**: In this configuration the Remote Access server is installed behind an edge device, such as a firewall or a router. The network adapter is connected to the internal network.

- **Network adapters**

  The Remote Access Server Setup Wizard automatically detects the network adapters that are configured on the Remote Access server. You must make sure that the correct adapters are selected.

- **IP-HTTPS certificate**

  The Remote Access Server Setup Wizard automatically detects a certificate that is suitable for the IP-

HTTPS connection. The subject name of the certificate that you select must match the ConnectTo address. If you are using self-signed certificates, you can choose to use a certificate that is created automatically by the Remote Access server.

- **IPv6 prefixes**

  If the Remote Access Server Setup Wizard detects that IPv6 has been deployed on the network adapters, it automatically populates IPv6 prefixes for the internal network, an IPv6 prefix to assign to DirectAccess client computers, and an IPv6 prefix to assign to VPN client computers. If the automatically generated prefixes are not correct for your native IPv6 or ISATAP infrastructure, you must manually change them.

- **Authentication**

  You can choose one of the following methods for authenticating DirectAccess clients to the Remote Access server:

  - **User authentication**: You can enable users to authenticate with Active Directory credentials or with two-factor authentication.
  - **Computer authentication**: You can configure computer authentication to use certificates. Or the Remote Access server can act as a proxy for Kerberos authentication without requiring certificates.
  - **Windows 7 clients** By default, client computers running Windows 7 cannot connect to a Remote Access deployment running Windows Server 2012 . If you have clients running Windows 7 in your organization that require remote access to internal resources, you can allow them to connect. Any client computers that you want to allow to access internal resources must be a member of a security group that you specify in the DirectAccess Client Setup Wizard.

    > **NOTE**
    > Allowing clients running Windows 7 to connect by using DirectAccess requires you to use computer certificate authentication.

- **VPN configuration**

  Before you configure Remote Access, decide if you are going to provide VPN access to remote clients. You should provide VPN access if you have client computers in your organization that do not support DirectAccess connectivity (for example, they are unmanaged or they run an operating system for which DirectAccess is not supported). The Remote Access Server Setup Wizard allows you to configure how IP addresses are assigned (by using DHCP or from a static address pool) and how VPN clients are authenticated (by using Active Directory or a RADIUS server).

Plan the infrastructure servers' configurations

Remote Access requires three types of infrastructure servers:

- **Network location server**
- **DNS servers**
- **Management servers**

Additional References

- Step 1: Plan the Remote Access Infrastructure

Install and Configure Deployment for Remote Management of DirectAccess Clients

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic introduces the configuration steps that are required to deploy a single Remote Access server that can be used for remote management of DirectAccess clients.

- Step 1: Configure the Remote Access Infrastructure: This topic describes how to configure network and server settings, certificate requirements, DNS settings, network location server deployment, DirectAccess management servers, Active Directory settings, and Group Policy Objects.
- Step 2: Configure the Remote Access Server: This topic describes how to configure DirectAccess client computers, server settings, and infrastructure and application servers.
- Step 3: Verify the Deployment: This topic describes how to verify the deployment.

Step 1 Configure the Remote Access Infrastructure

12/9/2022 • 18 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Note: Windows Server 2012 combines DirectAccess and Routing and Remote Access Service (RRAS) into a single Remote Access role.

This topic describes how to configure the infrastructure that is required for an advanced Remote Access deployment using a single Remote Access server in a mixed IPv4 and IPv6 environment. Before beginning the deployment steps, ensure that you have completed the planning steps described in Step 1: Plan the Remote Access Infrastructure.

TASK	DESCRIPTION
Configure server network settings	Configure the server network settings on the Remote Access server.
Configure routing in the corporate network	Configure routing in the corporate network to make sure traffic is appropriately routed.
Configure firewalls	Configure additional firewalls, if required.
Configure CAs and certificates	Configure a certification authority (CA), if required, and any other certificate templates required in the deployment.
Configure the DNS server	Configure DNS settings for the Remote Access server.
Configure Active Directory	Join client computers and the Remote Access server to the Active Directory domain.
Configure GPOs	Configure Group Policy Objects (GPOs) for the deployment, if required.
Configure security groups	Configure security groups that will contain DirectAccess client computers, and any other security groups that are required in the deployment.
Configure the network location server	Configure the network location server, including installing the network location server website certificate.

NOTE

This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

Configure server network settings

Depending on if you decide to place the Remote Access server at the edge or behind a Network Address Translation (NAT) device, the following network interface address settings are required for a single server

deployment in an environment with IPv4 and IPv6. All IP addresses are configured by using **Change adapter settings** in the **Windows Networking and Sharing Center**.

Edge topology:

Requires the following:

- Two Internet-facing consecutive public static IPv4 or IPv6 addresses.

> **NOTE**
>
> Two consecutive public IPv4 addresses are required for Teredo. If you are not using Teredo, you can configure a single public static IPv4 address.

- A single internal static IPv4 or IPv6 address.

Behind NAT device (two network adapters):

Requires a single internal network-facing static IPv4 or IPv6 address.

Behind NAT device (one network adapter):

Requires a single static IPv4 or IPv6 address.

If the Remote Access server has two network adapters (one for the domain profile and the other for a public or private profile), but you are using a single network adapter topology, the recommendation is as follows:

1. Ensure that the second network adapter is also classified in the domain profile.
2. If the second network adapter cannot be configured for the domain profile for any reason, the DirectAccess IPsec policy must be manually scoped to all profiles by using the following Windows PowerShell command:

   ```
   $gposession = Open-NetGPO -PolicyStore <Name of the server GPO>
   Set-NetIPsecRule -DisplayName <Name of the IPsec policy> -GPOSession $gposession -Profile Any
   Save-NetGPO -GPOSession $gposession
   ```

   The names of the IPsec policies to use in this command are **DirectAccess-DaServerToInfra** and **DirectAccess-DaServerToCorp**.

Configure routing in the corporate network

Configure routing in the corporate network as follows:

- When native IPv6 is deployed in the organization, add a route so that the routers on the internal network route IPv6 traffic back through the Remote Access server.
- Manually configure organization IPv4 and IPv6 routes on the Remote Access servers. Add a published route so that all traffic with an (/48) IPv6 prefix is forwarded to the internal network. In addition, for IPv4 traffic, add explicit routes so that IPv4 traffic is forwarded to the internal network.

Configure firewalls

Depending on the network settings you chose, when you use additional firewalls in your deployment, apply the following firewall exceptions for Remote Access traffic:

Remote Access server on IPv4 Internet

Apply the following Internet-facing firewall exceptions for Remote Access traffic when the Remote Access server

is on the IPv4 Internet:

- **Teredo traffic**

  User Datagram Protocol (UDP) destination port 3544 inbound, and UDP source port 3544 outbound. Apply this exemption for both of the Internet-facing consecutive public IPv4 addresses on the Remote Access server.

- **6to4 traffic**

  IP Protocol 41 inbound and outbound. Apply this exemption for both of the Internet-facing consecutive public IPv4 addresses on the Remote Access server.

- **IP-HTTPS traffic**

  Transmission Control Protocol (TCP) destination port 443, and TCP source port 443 outbound. When the Remote Access server has a single network adapter, and the network location server is on the Remote Access server, then TCP port 62000 is also required. Apply these exemptions only for the address to which the external name of the server resolves.

  > **NOTE**
  > This exemption is configured on the Remote Access server. All the other exemptions are configured on the edge firewall.

Remote Access server on IPv6 Internet

Apply the following Internet-facing firewall exceptions for Remote Access traffic when the Remote Access server is on the IPv6 Internet:

- IP Protocol 50
- UDP destination port 500 inbound, and UDP source port 500 outbound.
- Internet Control Message Protocol for IPv6 (ICMPv6) traffic inbound and outbound - for Teredo implementations only.

Remote Access traffic

Apply the following internal network firewall exceptions for Remote Access traffic:

- ISATAP: Protocol 41 inbound and outbound
- TCP/UDP for all IPv4 or IPv6 traffic
- ICMP for all IPv4 or IPv6 traffic

Configure CAs and certificates

With Remote Access in Windows Server 2012 , you to choose between using certificates for computer authentication or using a built-in Kerberos authentication that uses user names and passwords. You must also configure an IP-HTTPS certificate on the Remote Access server. This section explains how to configure these certificates.

For information about setting up a public key infrastructure (PKI), see Active Directory Certificate Services.

Configure IPsec authentication

A certificate is required on the Remote Access server and all DirectAccess clients so that they can use IPsec authentication. The certificate must be issued by an internal certification authority (CA). Remote Access servers and DirectAccess clients must trust the CA that issues the root and intermediate certificates.

To configure IPsec authentication

1. On the internal CA, decide if you will use the default computer certificate template, or if you will create a new certificate template as described in Creating Certificate Templates.

   > **NOTE**
   > If you create a new template, it must be configured for client authentication.

2. Deploy the certificate template if required. For more information, see Deploying Certificate Templates.
3. Configure the template for autoenrollment if required.
4. Configure certificate autoenrollment if required. For more information, see Configure Certificate Autoenrollment.

Configure certificate templates

When you use an internal CA to issue certificates, you must configure certificate templates for the IP-HTTPS certificate and the network location server website certificate.

To configure a certificate template

1. On the internal CA, create a certificate template as described in Creating Certificate Templates.
2. Deploy the certificate template as described in Deploying Certificate Templates.

After you prepare your templates, you can use them to configure the certificates. See the following procedures for details:

- Configure the IP-HTTPS certificate
- Configure the network location server

Configure the IP-HTTPS certificate

Remote Access requires an IP-HTTPS certificate to authenticate IP-HTTPS connections to the Remote Access server. There are three certificate options for the IP-HTTPS certificate:

- **Public**

  Supplied by a third party.

- **Private**

  The certificate is based on the certificate template that you created in Configuring certificate templates. It requires, a certificate revocation list (CRL) distribution point that is reachable from a publicly resolvable FQDN.

- **Self-signed**

  This certificate requires a CRL distribution point that is reachable from a publicly resolvable FQDN.

  > **NOTE**
  > Self-signed certificates cannot be used in multisite deployments.

Make sure that the website certificate used for IP-HTTPS authentication meets the following requirements:

- The certificate subject name should be the externally resolvable fully qualified domain name (FQDN) of the IP-HTTPS URL (the ConnectTo address) that is used only for the Remote Access server IP-HTTPS connections.

- The common name of the certificate should match the name of the IP-HTTPS site.
- In the subject field, specify the IPv4 address of the external-facing adapter of the Remote Access server or the FQDN of the IP-HTTPS URL.
- For the **Enhanced Key Usage** field, use the Server Authentication object identifier (OID).
- For the **CRL Distribution Points** field, specify a CRL distribution point that is accessible by DirectAccess clients that are connected to the Internet.
- The IP-HTTPS certificate must have a private key.
- The IP-HTTPS certificate must be imported directly into the personal store.
- IP-HTTPS certificates can have wildcard characters in the name.

To install the IP-HTTPS certificate from an internal CA

1. On the Remote Access server: On the **Start** screen, type**mmc.exe**, and then press ENTER.
2. In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
5. Right-click **Certificates**, point to **All Tasks**, click **Request New Certificate**, and then click **Next** twice..
6. On the **Request Certificates** page, select the check box for the certificate template that you created in Configuring certificate templates, and if required, click **More information is required to enroll for this certificate**.
7. In the **Certificate Properties** dialog box, on the **Subject** tab, in the **Subject name** area, in **Type**, select **Common Name**.
8. In **Value**, specify the IPv4 address of the external-facing adapter of the Remote Access server, or the FQDN of the IP-HTTPS URL, and then click **Add**.
9. In the **Alternative name** area, in **Type**, select **DNS**.
10. In **Value**, specify the IPv4 address of the external-facing adapter of the Remote Access server, or the FQDN of the IP-HTTPS URL, and then click **Add**.
11. On the **General** tab, in **Friendly name**, you can enter a name that will help you identify the certificate.
12. On the **Extensions** tab, next to **Extended Key Usage**, click the arrow, and make sure that Server Authentication is in the **Selected options** list.
13. Click **OK**, click **Enroll**, and then click **Finish**.
14. In the details pane of the Certificates snap-in, verify that the new certificate was enrolled with the intended purpose of server authentication.

Configure the DNS server

You must manually configure a DNS entry for the network location server website for the internal network in your deployment.

To add the network location server and web probe

1. On the internal network DNS server: On the **Start** screen, type**dnsmgmt.msc**, and then press ENTER.

2. In the left pane of the **DNS Manager** console, expand the forward lookup zone for your domain. Right-click the domain, and click **New Host (A or AAAA)**.
3. In the **New Host** dialog box, in the **Name (uses parent domain name if blank)** box, enter the DNS name for the network location server website (this is the name the DirectAccess clients use to connect to the network location server). In the **IP address** box, enter the IPv4 address of the network location server, and click **Add Host**, and then click **OK**.
4. In the **New Host** dialog box, in the **Name (uses parent domain name if blank)** box, enter the DNS name for the web probe (the name for the default web probe is directaccess-webprobehost). In the **IP address** box, enter the IPv4 address of the web probe, and then click **Add Host**.
5. Repeat this process for directaccess-corpconnectivityhost and any manually created connectivity verifiers. In the **DNS** dialog box, click **OK**.
6. Click **Done**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Add-DnsServerResourceRecordA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv4Address
<network_location_server_IPv4_address>
Add-DnsServerResourceRecordAAAA -Name <network_location_server_name> -ZoneName <DNS_zone_name> -IPv6Address
<network_location_server_IPv6_address>
```

You must also configure DNS entries for the following:

- **The IP-HTTPS server**

  DirectAccess clients must be able to resolve the DNS name of the Remote Access server from the Internet.

- **CRL revocation checking**

  DirectAccess uses certificate revocation checking for the IP-HTTPS connection between DirectAccess clients and the Remote Access server, and for the HTTPS-based connection between the DirectAccess client and the network location server. In both cases, DirectAccess clients must be able to resolve and access the CRL distribution point location.

- **ISATAP**

  Intrasite Automatic Tunnel Addressing Protocol (ISATAP) uses tunnels to enable DirectAccess clients to connect to the Remote Access server over the IPv4 Internet, encapsulating IPv6 packets within an IPv4 header. It is used by Remote Access to provide IPv6 connectivity to ISATAP hosts across an intranet. In a non-native IPv6 network environment, the Remote Access server configures itself automatically as an ISATAP router. Resolution support for the ISATAP name is required.

Configure Active Directory

The Remote Access server and all DirectAccess client computers must be joined to an Active Directory domain. DirectAccess client computers must be a member of one of the following domain types:

- Domains that belong in the same forest as the Remote Access server.
- Domains that belong to forests with a two-way trust with the Remote Access server forest.

- Domains that have a two-way domain trust to the Remote Access server domain.

To join the Remote Access server to a domain

1. In Server Manager, click **Local Server**. In the details pane, click the link next to **Computer name**.
2. In the **System Properties** dialog box, click the **Computer Name** tab, and then click **Change**.
3. In the **Computer Name** box, type the name of the computer if you are also changing the computer name when joining the server to the domain. Under **Member of**, click **Domain**, and then type the name of the domain to which you want to join the server, (for example, corp.contoso.com), and then click **OK**.
4. When you are prompted for a user name and password, enter the user name and password of a user with permissions to join computers to the domain, and then click **OK**.
5. When you see a dialog box welcoming you to the domain, click **OK**.
6. When you are prompted that you must restart the computer, click **OK**.
7. In the **System Properties** dialog box, click **Close**.
8. When you are prompted to restart the computer, click **Restart Now**.

To join client computers to the domain

1. On the **Start** screen, type**explorer.exe**, and then press ENTER.
2. Right-click the Computer icon, and then click **Properties**.
3. On the **System** page, click **Advanced system settings**.
4. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
5. In the **Computer name** box, type the name of the computer if you are also changing the computer name when joining the server to the domain. Under **Member of**, click **Domain**, and then type the name of the domain to which you want to join the server (for example, corp.contoso.com), and then click **OK**.
6. When you are prompted for a user name and password, enter the user name and password of a user with permissions to join computers to the domain, and then click **OK**.
7. When you see a dialog box welcoming you to the domain, click **OK**.
8. When you are prompted that you must restart the computer, click **OK**.
9. In the **System Properties** dialog box, click Close.
10. Click **Restart Now** when prompted.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

> **NOTE**
>
> You must supply domain credentials after you enter the following command.

```
Add-Computer -DomainName <domain_name>
Restart-Computer
```

Configure GPOs

To deploy Remote Access, you require a minimum of two Group Policy Objects. One Group Policy Object contains settings for the Remote Access server, and one contains settings for DirectAccess client computers. When you configure Remote Access, the wizard automatically creates the required Group Policy Objects. However, if your organization enforces a naming convention, or you do not have the required permissions to create or edit Group Policy Objects, they must be created prior to configuring Remote Access.

To create Group Policy Objects, see Create and Edit a Group Policy Object.

An administrator can manually link the DirectAccess Group Policy Objects to an organizational unit (OU). Consider the following:

1. Link the created GPOs to the respective OUs before you configure DirectAccess.
2. When you configure DirectAccess, specify a security group for the client computers.
3. The GPOs are configured automatically, regardless of if the administrator has permissions to link the GPOs to the domain.
4. If the GPOs are already linked to an OU, the links will not be removed, but they are not linked to the domain.
5. For server GPOs, the OU must contain the server computer object-otherwise, the GPO will be linked to the root of the domain.
6. If the OU has not been linked previously by running the DirectAccess Setup Wizard, after the configuration is complete, the administrator can link the DirectAccess GPOs to the required OUs, and remove the link to the domain.

   For more information, see Link a Group Policy Object.

> **NOTE**
>
> If a Group Policy Object was created manually, it is possible that the Group Policy Object will not be available during the DirectAccess configuration. The Group Policy Object may not have been replicated to the domain controller closest to the management computer. The administrator can wait for replication to complete or force the replication.

Configure security groups

The DirectAccess settings that are contained in the client computer Group Policy Object are applied only to computers that are members of the security groups that you specify when configuring Remote Access.

To create a security group for DirectAccess clients

1. On the **Start** screen, type**dsa.msc**, and then press ENTER.
2. In the **Active Directory Users and Computers** console, in the left pane, expand the domain that will contain the security group, right-click **Users**, point to **New**, and then click **Group**.
3. In the **New Object - Group** dialog box, under **Group name**, enter the name for the security group.
4. Under **Group scope**, click **Global**, and under **Group type**, click **Security**, and then click **OK**.
5. Double-click the DirectAccess client computers security group, and in the **Properties** dialog box, click the **Members** tab.
6. On the **Members** tab, click **Add**.
7. In the **Select Users, Contacts, Computers, or Service Accounts** dialog box, select the client

computers that you want to enable for DirectAccess, and then click **OK**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
New-ADGroup -GroupScope global -Name <DirectAccess_clients_group_name>
Add-ADGroupMember -Identity DirectAccess_clients_group_name -Members <computer_name>
```

Configure the network location server

The network location server should be on a server with high availability, and it needs a valid Secure Sockets Layer (SSL) certificate that is trusted by the DirectAccess clients.

> **NOTE**
> If the network location server website is located on the Remote Access server, a website will be created automatically when you configure Remote Access and it is bound to the server certificate that you provide.

There are two certificate options for the network location server certificate:

- **Private**

  > **NOTE**
  > The certificate is based on the certificate template that you created in Configuring certificate templates.

- **Self-signed**

  > **NOTE**
  > Self-signed certificates cannot be used in multisite deployments.

Whether you use a private certificate or a self-signed certificate, they require the following:

- A website certificate that is used for the network location server. The certificate subject should be the URL of the network location server.
- A CRL distribution point that has high availability on the internal network.

To install the network location server certificate from an internal CA

1. On the server that will host the network location server website: On the **Start** screen, type**mmc.exe**, and then press ENTER.
2. In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**.
5. Right-click **Certificates**, point to **All Tasks**, click **Request New Certificate**, and then click **Next** twice.

6. On the **Request Certificates** page, select the check box for the certificate template that you created in Configuring certificate templates, and if required, click **More information is required to enroll for this certificate**.
7. In the **Certificate Properties** dialog box, on the **Subject** tab, in the **Subject name** area, in **Type**, select **Common Name**.
8. In **Value**, enter the FQDN of the network location server website, and then click **Add**.
9. In the **Alternative name** area, in **Type**, select **DNS**.
10. In **Value**, enter the FQDN of the network location server website, and then click **Add**.
11. On the **General** tab, in **Friendly name**, you can enter a name that will help you identify the certificate.
12. Click **OK**, click **Enroll**, and then click **Finish**.
13. In the details pane of the Certificates snap-in, verify that new certificate was enrolled with the intended purpose of server authentication.

To configure the network location server

1. Set up a website on a high availability server. The website does not require any content, but when you test it, you might define a default page that provides a message when clients connect.

   This step is not required if the network location server website is hosted on the Remote Access server.

2. Bind an HTTPS server certificate to the website. The common name of the certificate should match the name of the network location server site. Ensure that DirectAccess clients trust the issuing CA.

   This step is not required if the network location server website is hosted on the Remote Access server.

3. Set up a CRL site that has high availability on the internal network.

   CRL distribution points can be accessed through:

   - Web servers that use an HTTP-based URL, such as: https://crl.corp.contoso.com/crld/corp-APP1-CA.crl
   - File servers that are accessed through a universal naming convention (UNC) path, such as \\crl.corp.contoso.com\crld\corp-APP1-CA.crl

   If the internal CRL distribution point is reachable only over IPv6, you must configure a Windows Firewall with Advanced Security connection security rule. This exempts IPsec protection from the IPv6 address space of your intranet to the IPv6 addresses of your CRL distribution points.

4. Ensure that DirectAccess clients on the internal network can resolve the name of the network location server, and that DirectAccess clients on the Internet cannot resolve the name.

See also

- Step 2: Configure the Remote Access Server

Step 2 Configure the Remote Access Server

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to configure the client and server settings that are required for remote management of DirectAccess clients. Before you begin the deployment steps, ensure that you have completed the planning steps that are described in Step 2 Plan the Remote Access Deployment.

TASK	DESCRIPTION
Install the Remote Access role	Install the Remote Access role.
Configure the deployment type	Configure the deployment type as DirectAccess and VPN, DirectAccess only, or VPN only.
Configure DirectAccess clients	Configure the Remote Access server with the security groups that contain DirectAccess clients.
Configure the Remote Access server	Configure the Remote Access server settings.
Configure the infrastructure servers	Configure the infrastructure servers that are used in the organization.
Configure application servers	Configure the application servers to require authentication and encryption.
Configuration summary and alternate GPOs	View the Remote Access configuration summary, and modify the GPOs if desired.

NOTE

This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

Install the Remote Access role

You must install the Remote Access role on a server in your organization that will act as the Remote Access server.

To install the Remote Access role

To install the Remote Access role on DirectAccess servers

1. On the DirectAccess server, in the Server Manager console, in the **Dashboard**, click **Add roles and features**.
2. Click **Next** three times to get to the server role selection screen.
3. On the **Select Server Roles** dialog, select **Remote Access**, and then click **Next**.
4. Click **Next** three times.

5. On the **Select role services** dialog, select **DirectAccess and VPN (RAS)** and then click **Add Features**.

6. Select **Routing**, select **Web Application Proxy**, click **Add Features**, and then click **Next**.

7. Click **Next**, and then click **Install**.

8. On the **Installation progress** dialog, verify that the installation was successful, and then click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

Configure the deployment type

There are three options that you can use to deploy Remote Access from the Remote Access Management console:

- DirectAccess and VPN
- DirectAccess only
- VPN only

> **NOTE**
> This guide uses the DirectAccess only method of deployment in the example procedures.

To configure the deployment type

1. On the Remote Access server, open the Remote Access Management console: On the **Start** screen, type, type **Remote Access Management Console**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.

2. In the Remote Access Management Console, in the middle pane, click **Run the Remote Access Setup Wizard**.

3. In the **Configure Remote Access** dialog box, select DirectAccess and VPN, DirectAccess only, or VPN only.

Configure DirectAccess clients

For a client computer to be provisioned to use DirectAccess, it must belong to the selected security group. After DirectAccess is configured, client computers in the security group are provisioned to receive the DirectAccess Group Policy Objects (GPOs) for remote management.

To configure DirectAccess clients

1. In the middle pane of the Remote Access Management console, in the **Step 1 Remote Clients** area, click **Configure**.

2. In the DirectAccess Client Setup Wizard, on the **Deployment Scenario** page, click **Deploy DirectAccess for remote management only**, and then click **Next**.

3. On the **Select Groups** page, click **Add**.

4. In the **Select Groups** dialog box, select the security groups that contain the DirectAccess client computers, and then click **Next**.

5. On the **Network Connectivity Assistant** page:

   - In the table, add the resources that will be used to determine connectivity to the internal network. A default web probe is created automatically if no other resources are configured. When configuring the web probe locations for determining connectivity to the enterprise network, ensure that you have at least one HTTP based probe configured. Configuring only a ping probe is not sufficient, and it could lead to an inaccurate determination of connectivity status. This is because ping is exempted from IPsec. As a result, ping does not ensure that the IPsec tunnels are properly established.

   - Add a Help Desk email address to allow users to send information if they experience connectivity issues.

   - Provide a friendly name for the DirectAccess connection.

   - Select the **Allow DirectAccess clients to use local name resolution** check box, if required.

     > **NOTE**
     > When local name resolution is enabled, users who are running the NCA can resolve names by using DNS servers that are configured on the DirectAccess client computer.

6. Click **Finish**.

Configure the Remote Access server

To deploy Remote Access, you need to configure the server that will act as the Remote Access server with the following:

1. Correct network adapters
2. A public URL for the Remote Access server to which client computers can connect (the ConnectTo address)
3. An IP-HTTPS certificate with a subject that matches the ConnectTo address
4. IPv6 settings
5. Client computer authentication

To configure the Remote Access server

1. In the middle pane of the Remote Access Management console, in the **Step 2 Remote Access Server** area, click **Configure**.

2. In the Remote Access Server Setup Wizard, on the **Network Topology** page, click the deployment topology that will be used in your organization. In **Type the public name or IPv4 address used by clients to connect to the Remote Access server**, enter the public name for the deployment (this name matches the subject name of the IP-HTTPS certificate, for example, edge1.contoso.com), and then click **Next**.

3. On the **Network Adapters** page, the wizard automatically detects:

   - Network adapters for the networks in your deployment. If the wizard does not detect the correct network adapters, manually select the correct adapters.

   - IP-HTTPS certificate. This is based on the public name for the deployment that you set during the

previous step of the wizard. If the wizard does not detect the correct IP-HTTPS certificate, click **Browse** to manually select the correct certificate.

4. Click **Next**.

5. On the **Prefix Configuration** page (this page is only visible if IPv6 is detected in the internal network), the wizard automatically detects the IPv6 settings that are used on the internal network. If your deployment requires additional prefixes, configure the IPv6 prefixes for the internal network, an IPv6 prefix to assign to DirectAccess client computers, and an IPv6 prefix to assign to VPN client computers.

6. On the **Authentication** page:

   - For multisite and two-factor authentication deployments, you must use computer certificate authentication. Select the **Use computer certificates** check box to use computer certificate authentication and select the IPsec root certificate.

   - To enable client computers running Windows 7 to connect via DirectAccess, select the **Enable Windows 7 client computers to connect via DirectAccess** check box. You must also use computer certificate authentication in this type of deployment.

7. Click **Finish**.

Configure the infrastructure servers

To configure the infrastructure servers in a Remote Access deployment, you must configure the following:

- Network location server
- DNS settings, including the DNS suffix search list
- Any management servers that are not automatically detected by Remote Access

To configure the infrastructure servers

1. In the middle pane of the Remote Access Management console, in the **Step 3 Infrastructure Servers** area, click **Configure**.

2. In the Infrastructure Server Setup Wizard, on the **Network Location Server** page, click the option that corresponds to the location of the network location server in your deployment.

   - If the network location server is on a remote web server, enter the URL, and then click **Validate** before you continue.

   - If the network location server is on the Remote Access server, click **Browse** to locate the relevant certificate, and then click **Next**.

3. On the **DNS** page, in the table, enter additional name suffixes that will be applied as Name Resolution Policy Table (NRPT) exemptions. Select a local name resolution option, and then click **Next**.

4. On the **DNS Suffix Search List** page, the Remote Access server automatically detects domain suffixes in the deployment. Use the **Add** and **Remove** buttons to create the list of domain suffixes that you want to use. To add a new domain suffix, in **New Suffix**, enter the suffix, and then click **Add**. Click **Next**.

5. On the **Management** page, add management servers that are not detected automatically, and then click **Next**. Remote Access automatically adds domain controllers and Configuration Manager servers.

6. Click **Finish**.

Configure application servers

In a full Remote Access deployment, configuring application servers is an optional task. In this scenario for

remote management of DirectAccess clients, application servers are not utilized and this step is greyed out to indicate that it is not active. Click **Finish** to apply the configuration.

Configuration summary and alternate GPOs

When the Remote Access configuration is complete, the **Remote Access Review** is displayed. You can review all of the settings that you previously selected, including:

- **GPO Settings**

  The DirectAccess server GPO name and Client GPO name are listed. You can click the **Change** link next to the **GPO Settings** heading to modify the GPO settings.

- **Remote Clients**

  The DirectAccess client configuration is displayed, including the security group, connectivity verifiers, and DirectAccess connection name.

- **Remote Access Server**

  The DirectAccess configuration is displayed, including the public name and address, network adapter configuration, and certificate information.

- **Infrastructure Servers**

  This list includes the network location server URL, DNS suffixes that are used by DirectAccess clients, and management server information.

See also

- Step 3: Verify the Deployment

Step 3 Verify the Advanced DirectAccess Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This topic describes how to verify that you have correctly configured your DirectAccess deployment.

To verify access to internal resources through DirectAccess

1. Connect a DirectAccess client computer to the corporate network and obtain the Group Policy Object.
2. Click the **Network connections** icon in the notification area to access the DirectAccess Media Manager.
3. Click **DirectAccess Connection**, and you will see that the status is **Connected Locally**.
4. Connect the client computer to the external network and attempt to access internal resources.

   You should be able to access all corporate resources.

Previous step

- Step 2: Configuring DirectAccess Servers

Publishing Applications using AD FS Preauthentication

12/9/2022 • 21 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This content is relevant for the on-premises version of Web Application Proxy. To enable secure access to on-premises applications over the cloud, see the Azure AD Application Proxy content.

This topic describes how to publish applications through Web Application Proxy using Active Directory Federation Services (AD FS) preauthentication.

For all types of application that you can publish using AD FS preauthentication, you must add a AD FS relying party trust to the Federation Service.

The general AD FS preauthentication flow is as follows:

> **NOTE**
>
> This authentication flow is not applicable for clients that use Microsoft Store apps.

1. The client device attempts to access a published web application on a particular resource URL; for example https://app1.contoso.com/.

   The resource URL is a public address on which Web Application Proxy listens for incoming HTTPS requests.

   If HTTP to HTTPS redirection is enabled, Web Application Proxy will also listen for incoming HTTP requests.

2. Web Application Proxy redirects the HTTPS request to the AD FS server with URL encoded parameters, including the resource URL and the appRealm (a relying party identifier).

   The user authenticates using the authentication method required by the AD FS server; for example, user name and password, two-factor authentication with a one-time password, and so on.

3. After the user is authenticated, the AD FS server issues a security token, the 'edge token', containing the following information and redirects the HTTPS request back to the Web Application Proxy server:

   - The resource identifier that the user attempted to access.
   - The user's identity as a user principal name (UPN).
   - The expiry of the access grant approval; that is, the user is granted access for a limited period of time, after which they are required to authenticate again.
   - Signature of the information in the edge token.

4. Web Application Proxy receives the redirected HTTPS request from the AD FS server with the edge token and validates and uses the token as follows:

   - Validates that the edge token signature is from the federation service that is configured in the Web Application Proxy configuration.

- Validates that the token was issued for the correct application.
- Validates that the token has not expired.
- Uses the user identity when required; for example to obtain a Kerberos ticket if the backend server is configured to use Integrated Windows authentication.

5. If the edge token is valid, Web Application Proxy forwards the HTTPS request to the published web application using either HTTP or HTTPS.
6. The client now has access to the published web application; however, the published application may be configured to require the user to perform additional authentication. If, for example, the published web application is a SharePoint site and does not require additional authentication, the user will see the SharePoint site in the browser.
7. Web Application Proxy saves a cookie on the client device. The cookie is used by Web Application Proxy to identify that this session has already been preauthenticated and that no further preauthentication is required.

> **IMPORTANT**
> When configuring the external URL and the backend server URL, make sure you include the fully qualified domain name (FQDN), and not an IP address.

> **NOTE**
> This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see Using Cmdlets.

Publish a Claims-based Application for Web Browser Clients

To publish an application that uses claims for authentication, you must add a relying party trust for the application to the Federation Service.

When publishing claims-based applications and accessing the application from a browser, the general authentication flow is as follows:

1. The client attempts to access a claims-based application using a web browser; for example, https://appserver.contoso.com/claimapp/.
2. The web browser sends an HTTPS request to the Web Application Proxy server which redirects the request to the AD FS server.
3. The AD FS server authenticates the user and the device and redirects the request back to Web Application Proxy. The request now contains the edge token. The AD FS server adds a single sign-on (SSO) cookie to the request because the user has already performed authentication against the AD FS server.
4. Web Application Proxy validates the token, adds its own cookie, and forwards the request to the backend server.
5. The backend server redirects the request to the AD FS server to get the application security token.
6. The request is redirected to the backend server by the AD FS server. The request now contains the application token and the SSO cookie. The user is granted access to the application and is not required to enter a user name or password.

This procedure describes how to publish a claims-based application, such as a SharePoint site, that will be

accessed by web browser clients. Before you begin, make sure that you have done the following:

- Created a relying party trust for the application in the AD FS Management console.
- Verified that a certificate on the Web Application Proxy server is suitable for the application you want to publish.

To publish a claims-based application

1. On the Web Application Proxy server, in the Remote Access Management console, in the **Navigation** pane, click **Web Application Proxy**, and then in the **Tasks** pane, click **Publish**.
2. On the **Publish New Application Wizard**, on the **Welcome** page, click **Next**.
3. On the **Preauthentication** page, click **Active Directory Federation Services (AD FS)**, and then click **Next**.
4. On the **Supported Clients** page, select **Web and MSOFBA**, and then click **Next**.
5. On the **Relying Party** page, in the list of relying parties select the relying party for the application that you want to publish, and then click **Next**.
6. On the **Publishing Settings** page, do the following, and then click **Next**:
   - In the **Name** box, enter a friendly name for the application.

     This name is used only in the list of published applications in the Remote Access Management console.
   - In the **External URL** box, enter the external URL for this application; for example, https://sp.contoso.com/app1/.
   - In the **External certificate** list, select a certificate whose subject covers the external URL.
   - In the **Backend server URL** box, enter the URL of the backend server. Note that this value is automatically entered when you enter the external URL and you should change it only if the backend server URL is different; for example, https://sp/app1/.

     > **NOTE**
     > Web Application Proxy can translate host names in URLs, but cannot translate path names. Therefore, you can enter different host names, but you must enter the same path name. For example, you can enter an external URL of https://apps.contoso.com/app1/ and a backend server URL of https://app-server/app1/. However, you cannot enter an external URL of https://apps.contoso.com/app1/ and a backend server URL of https://apps.contoso.com/internal-app1/.
7. On the **Confirmation** page, review the settings, and then click **Publish**. You can copy the PowerShell command to set up additional published applications.
8. On the **Results** page, make sure that the application published successfully, and then click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Add-WebApplicationProxyApplication
    -BackendServerURL 'https://sp.contoso.com/app1/'
    -ExternalCertificateThumbprint '1a2b3c4d5e6f1a2b3c4d5e6f1a2b3c4d5e6f1a2b'
    -ExternalURL 'https://sp.contoso.com/app1/'
    -Name 'SP'
    -ExternalPreAuthentication ADFS
    -ADFSRelyingPartyName 'SP_Relying_Party'
```

Publish an Integrated Windows authenticated-based Application for Web Browser Clients

Web Application Proxy can be used to publish applications that uses Integrated Windows authentication; that is, Web Application Proxy performs preauthentication as required, and can then perform SSO to the published application that uses Integrated Windows authentication. To publish an application that uses Integrated Windows authentication you must add a non-claims-aware relying party trust for the application to the Federation Service.

To allow Web Application Proxy to perform single sign-on (SSO) and to perform credentials delegation using Kerberos constrained delegation, the Web Application Proxy server must be joined to a domain. See Plan Active Directory.

To allow users to access applications that use Integrated Windows authentication, the Web Application Proxy server must be able to provide delegation for users to the published application. You can do this on the domain controller for any application. You can also do this on the backend server if it is running on Windows Server 2012 R2 or Windows Server 2012 . For more information, see What's New in Kerberos Authentication.

For a walkthrough of how to configure Web Application Proxy to publish an application using Integrated Windows authentication, see Configure a site to use Integrated Windows authentication.

When using Integrated Windows authentication to backend servers, the authentication between Web Application Proxy and the published application is not claims-based, instead it uses Kerberos constrained delegation to authenticate end users to the application. The general flow is described below:

1. The client attempts to access a non-claims-based application using a web browser; for example, https://appserver.contoso.com/nonclaimapp/.
2. The web browser sends an HTTPS request to the Web Application Proxy server which redirects the request to the AD FS server.
3. The AD FS server authenticates the user and redirects the request back to Web Application Proxy. The request now contains the edge token.
4. Web Application Proxy validates the token.
5. If the token is valid, Web Application Proxy obtains a Kerberos ticket from the domain controller on behalf of the user.
6. Web Application Proxy adds the Kerberos ticket to the request as part of the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) token, and forwards the request to the backend server. The request contains the Kerberos ticket; therefore, the user is granted access to the application without the need for further authentication.

This procedure describes how to publish an application that uses Integrated Windows authentication, such as Outlook Web App, that will be accessed by web browser clients. Before you begin, make sure that you have done the following:

- Created a non-claims-aware relying party trust for the application in the AD FS Management console.

- Configured the backend server to support Kerberos constrained delegation on the domain controller or by using the Set-ADUser cmdlet with the -PrincipalsAllowedToDelegateToAccount parameter. Note that if the backend server is running on Windows Server 2012 R2 or Windows Server 2012 , you can also run this PowerShell command on the backend server.
- Made sure that the Web Application Proxy servers are configured for delegation to the service principal names of the backend servers.
- Verified that a certificate on the Web Application Proxy server is suitable for the application you want to publish.

To publish a non-claims-based application

1. On the Web Application Proxy server, in the Remote Access Management console, in the **Navigation** pane, click **Web Application Proxy**, and then in the **Tasks** pane, click **Publish**.
2. On the **Publish New Application Wizard**, on the **Welcome** page, click **Next**.
3. On the **Preauthentication** page, click **Active Directory Federation Services (AD FS)**, and then click **Next**.
4. On the **Supported Clients** page, select **Web and MSOFBA**, and then click **Next**.
5. On the **Relying Party** page, in the list of relying parties select the relying party for the application that you want to publish, and then click **Next**.
6. On the **Publishing Settings** page, do the following, and then click **Next**:
   - In the **Name** box, enter a friendly name for the application.

     This name is used only in the list of published applications in the Remote Access Management console.
   - In the **External URL** box, enter the external URL for this application; for example, https://owa.contoso.com/.
   - In the **External certificate** list, select a certificate whose subject covers the external URL.
   - In the **Backend server URL** box, enter the URL of the backend server. Note that this value is automatically entered when you enter the external URL and you should change it only if the backend server URL is different; for example, https://owa/.

     > **NOTE**
     > Web Application Proxy can translate host names in URLs, but cannot translate path names. Therefore, you can enter different host names, but you must enter the same path name. For example, you can enter an external URL of https://apps.contoso.com/app1/ and a backend server URL of https://app-server/app1/. However, you cannot enter an external URL of https://apps.contoso.com/app1/ and a backend server URL of https://apps.contoso.com/internal-app1/.

   - In the **Backend server SPN** box, enter the service principal name for the backend server; for example, HTTP/owa.contoso.com.
7. On the **Confirmation** page, review the settings, and then click **Publish**. You can copy the PowerShell command to set up additional published applications.
8. On the **Results** page, make sure that the application published successfully, and then click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure.

Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Add-WebApplicationProxyApplication
    -BackendServerAuthenticationSpn 'HTTP/owa.contoso.com'
    -BackendServerURL 'https://owa.contoso.com/'
    -ExternalCertificateThumbprint '1a2b3c4d5e6f1a2b3c4d5e6f1a2b3c4d5e6f1a2b'
    -ExternalURL 'https://owa.contoso.com/'
    -Name 'OWA'
    -ExternalPreAuthentication ADFS
    -ADFSRelyingPartyName 'Non-Claims_Relying_Party'
```

Publish an Application that uses MS-OFBA

Web Application Proxy supports access from Microsoft Office clients such as Microsoft Word that access documents and data on backend servers. The only difference between these applications and a standard browser is that the redirection to the STS is done not via regular HTTP redirection but with special MS-OFBA headers as specified in: https://msdn.microsoft.com/library/dd773463(v=office.12).aspx. Backend application may be claims or IWA. To publish an application for clients that use MS-OFBA, you must add a relying party trust for the application to the Federation Service. Depending on the application, you can use claims-based authentication or Integrated Windows authentication. Therefore, you must add the relevant relying party trust depending on the application.

To allow Web Application Proxy to perform single sign-on (SSO) and to perform credentials delegation using Kerberos constrained delegation, the Web Application Proxy server must be joined to a domain. See Plan Active Directory.

There are no additional planning steps if the application uses claims-based authentication. If the application used Integrated Windows authentication, see Publish an Integrated Windows authenticated-based Application for Web Browser Clients.

The authentication flow for clients that use the MS-OFBA protocol using claims-based authentication is described below. The authentication for this scenario can either use the application token in the URL, or in the body.

1. The user is working in an Office program, and from the **Recent Documents** list, opens a file on a SharePoint site.
2. The Office program shows a window with a browser control that requires the user to enter credentials.

   > **NOTE**
   > In some cases, the window may not appear because the client is already authenticated.

3. Web Application Proxy redirects the request to the AD FS server, which performs the authentication.
4. The AD FS server redirects the request back to Web Application Proxy. The request now contains the edge token.
5. The AD FS server adds a single sign-on (SSO) cookie to the request because the user has already performed authentication against the AD FS server.
6. Web Application Proxy validates the token and forwards the request to the backend server.
7. The backend server redirects the request to the AD FS server to get the application security token.
8. The request is redirected to the backend server. The request now contains the application token and the

SSO cookie. The user is granted access to the SharePoint site and is not required to enter a user name or password to view the file.

The steps to publish an application that uses MS-OFBA are identical to the steps for a claims-based application or a non-claims-based application. For claims-based applications, see Publish a Claims-based Application for Web Browser Clients, for non-claims-based applications, see Publish an Integrated Windows authenticated-based Application for Web Browser Clients. Web Application Proxy automatically detects the client and will authenticate the user as required.

Publish an Application that uses HTTP Basic

HTTP Basic is the authorization protocol used by many protocols, to connect rich clients, including smartphones, with your Exchange mailbox. For more information on HTTP Basic, see RFC 2617. Web Application Proxy traditionally interacts with AD FS using redirections; most rich clients don't support cookies or state management. In this way Web Application Proxy enables the HTTP app to receive a non-claims relying party trust for the application to the Federation Service. See Plan Active Directory.

The authentication flow for clients that use HTTP Basic is described below and in this diagram:

1. The user attempts to access a published web application a telephone client.
2. The app sends an HTTPS request to the URL published by Web Application Proxy.
3. If the request does not contain credentials, Web Application Proxy returns an HTTP 401 response to the app containing the URL of the authenticating AD FS server.
4. The user sends the HTTPS request to the app again with authorization set to Basic and user name and Base 64 encrypted password of the user in the www-authenticate request header.
5. Because the device cannot be redirected to AD FS, the Web Application Proxy sends an authentication request to AD FS with the credentials that it has including username and password. The token is acquired on behalf of the device.
6. In order to minimize the number of requests sent to the AD FS, Web Application Proxy, validates subsequent client requests using cached tokens for as long as the token is valid. Web Application Proxy periodically cleans the cache. You can view the size of the cache using the performance counter.
7. If the token is valid, Web Application Proxy forwards the request to the backend server and the user is granted access to the published web application.

The following procedure explains how to publish HTTP basic applications.

To publish an HTTP Basic application

1. On the Web Application Proxy server, in the Remote Access Management console, in the **Navigation** pane, click **Web Application Proxy**, and then in the **Tasks** pane, click **Publish**.
2. On the **Publish New Application Wizard**, on the **Welcome** page, click **Next**.
3. On the **Preauthentication** page, click **Active Directory Federation Services (AD FS)**, and then click **Next**.

4. On the **Supported Clients** page, select **HTTP Basic** and then click **Next**.

   If you wish to enable access to the Exchange only from workplace joined devices, select the **Enable access only for workplace joined devices** box. For more information see Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications.

5. On the **Relying Party** page, in the list of relying parties select the relying party for the application that you want to publish, and then click **Next**. Note that this list contains only on-claims relying parties.

6. On the **Publishing Settings** page, do the following, and then click **Next**:

   - In the **Name** box, enter a friendly name for the application.

     This name is used only in the list of published applications in the Remote Access Management console.

   - In the **External URL** box, enter the external URL for this application; for example, mail.contoso.com

   - In the **External certificate** list, select a certificate whose subject covers the external URL.

   - In the **Backend server URL** box, enter the URL of the backend server. Note that this value is automatically entered when you enter the external URL and you should change it only if the backend server URL is different; for example, mail.contoso.com.

7. On the **Confirmation** page, review the settings, and then click **Publish**. You can copy the PowerShell command to set up additional published applications.

8. On the **Results** page, make sure that the application published successfully, and then click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

This Windows PowerShell script enables preauthentication for all devices, not just workplace joined devices.

```
Add-WebApplicationProxyApplication
     -BackendServerUrl 'https://mail.contoso.com'
     -ExternalCertificateThumbprint '697F4FF0B9947BB8203A96ED05A3021830638E50'
     -ExternalUrl 'https://mail.contoso.com'
     -Name 'Exchange'
     -ExternalPreAuthentication ADFSforRichClients
     -ADFSRelyingPartyName 'EAS_Relying_Party'
```

The following preauthenticates only workplace joined devices:

```
Add-WebApplicationProxyApplication
     -BackendServerUrl 'https://mail.contoso.com'
     -ExternalCertificateThumbprint '697F4FF0B9947BB8203A96ED05A3021830638E50'
     -EnableHTTPRedirect:$true
     -ExternalUrl 'https://mail.contoso.com'
     -Name 'Exchange'
     -ExternalPreAuthentication ADFSforRichClients
     -ADFSRelyingPartyName 'EAS_Relying_Party'
```

Publish an Application that uses OAuth2 such as a Microsoft Store App

To publish an application for Microsoft Store apps, you must add a relying party trust for the application to the Federation Service.

To allow Web Application Proxy to perform single sign-on (SSO) and to perform credentials delegation using Kerberos constrained delegation, the Web Application Proxy server must be joined to a domain. See Plan Active Directory.

> **NOTE**
> Web Application Proxy supports publishing only for Microsoft Store apps that use the OAuth 2.0 protocol.

In the AD FS Management console, you must make sure that the OAuth endpoint is proxy enabled. To check if the OAuth endpoint is proxy enabled, open the AD FS Management console, expand **Service**, click **Endpoints**, in the **Endpoints** list, locate the OAuth endpoint and make sure that the value in the **Proxy Enabled** column is **Yes**.

The authentication flow for clients that use Microsoft Store apps is described below:

> **NOTE**
> The Web Application Proxy redirects to the AD FS server for authentication. Because Microsoft Store apps do not support redirects, if you use Microsoft Store apps, it is necessary to set the URL of the AD FS server using the Set-WebApplicationProxyConfiguration cmdlet and the OAuthAuthenticationURL parameter.
>
> Microsoft Store apps can be published only using Windows PowerShell.

1. The client attempts to access a published web application using a Microsoft Store app.
2. The app sends an HTTPS request to the URL published by Web Application Proxy.
3. Web Application Proxy returns an HTTP 401 response to the app containing the URL of the authenticating AD FS server. This process is known as 'discovery'.

   > **NOTE**
   > If the app knows the URL of the authenticating AD FS server and already has a combo token containing the OAuth token and the edge token, steps 2 and 3 are skipped in this authentication flow.

4. The app sends an HTTPS request to the AD FS server.
5. The app uses the web authentication broker to generate a dialog box in which the user enters credentials to authenticate to the AD FS server. For information about web authentication broker, see Web authentication broker.
6. After successful authentication, the AD FS server creates a combo token that contains the OAuth token and the edge token and sends the token to the app.
7. The app sends an HTTPS request containing the combo token to the URL published by Web Application Proxy.
8. Web Application Proxy splits the combo token into its two parts and validates the edge token.
9. If the edge token is valid, Web Application Proxy forwards the request to the backend server with only the OAuth token. The user is granted access to the published web application.

This procedure describes how to publish an application for OAuth2. This type of application can be published only using Windows PowerShell. Before you begin, make sure that you have done the following:

- Created a relying party trust for the application in the AD FS Management console.
- Made sure that the OAuth endpoint is proxy enabled in the AD FS Management console and make a note of the URL Path.
- Verified that a certificate on the Web Application Proxy server is suitable for the application you want to publish.

To publish an OAuth2 app

1. On the Web Application Proxy server, in the Remote Access Management console, in the **Navigation** pane, click **Web Application Proxy**, and then in the **Tasks** pane, click **Publish**.
2. On the **Publish New Application Wizard**, on the **Welcome** page, click **Next**.
3. On the **Preauthentication** page, click **Active Directory Federation Services (AD FS)**, and then click **Next**.
4. On the **Supported Clients** page, select **OAuth2** and then click **Next**.
5. On the **Relying Party** page, in the list of relying parties select the relying party for the application that you want to publish, and then click **Next**.
6. On the **Publishing Settings** page, do the following, and then click **Next**:
   - In the **Name** box, enter a friendly name for the application.

     This name is used only in the list of published applications in the Remote Access Management console.
   - In the **External URL** box, enter the external URL for this application; for example, https://server1.contoso.com/app1/.
   - In the **External certificate** list, select a certificate whose subject covers the external URL.

     In order to make sure your users can access your app, even if they neglect to type HTTPS in the URL, select the **Enable HTTP to HTTPS Redirection** box.
   - In the **Backend server URL** box, enter the URL of the backend server. Note that this value is automatically entered when you enter the external URL and you should change it only if the backend server URL is different; for example, https://sp/app1/.

     > **NOTE**
     > Web Application Proxy can translate host names in URLs, but cannot translate path names. Therefore, you can enter different host names, but you must enter the same path name. For example, you can enter an external URL of https://apps.contoso.com/app1/ and a backend server URL of https://app-server/app1/. However, you cannot enter an external URL of https://apps.contoso.com/app1/ and a backend server URL of https://apps.contoso.com/internal-app1/.
7. On the **Confirmation** page, review the settings, and then click **Publish**. You can copy the PowerShell command to set up additional published applications.
8. On the **Results** page, make sure that the application published successfully, and then click **Close**.

Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

To set the OAuth authentication URL for a federation server address of fs.contoso.com and a URL path of /adfs/oauth2/:

```
Set-WebApplicationProxyConfiguration -OAuthAuthenticationURL 'https://fs.contoso.com/adfs/oauth2/'
```

To publish the application:

```
Add-WebApplicationProxyApplication
    -BackendServerURL 'https://storeapp.contoso.com/'
    -ExternalCertificateThumbprint '1a2b3c4d5e6f1a2b3c4d5e6f1a2b3c4d5e6f1a2b'
    -ExternalURL 'https://storeapp.contoso.com/'
    -Name 'Microsoft Store app Server'
    -ExternalPreAuthentication ADFS
    -ADFSRelyingPartyName 'Store_app_Relying_Party'
    -UseOAuthAuthentication
```

See also

- Troubleshooting Web Application Proxy
- Publish Applications through Web Application Proxy
- Planning to Publish Applications Using Web Application Proxy
- Web Application Proxy Walkthrough Guide
- Web Application Proxy Cmdlets in Windows PowerShell
- Add-WebApplicationProxyApplication
- Set-WebApplicationProxyConfiguration

Publishing Applications with SharePoint, Exchange and RDG

12/9/2022 • 9 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This content is relevant for the on-premises version of Web Application Proxy. To enable secure access to on-premises applications over the cloud, see the Azure AD Application Proxy content.

This topic describes the tasks necessary to publish SharePoint Server, Exchange Server or Remote Desktop Gateway (RDP) through Web Application Proxy.

> **NOTE**
> This information is provided as-is. Remote Desktop Services supports and recommends using Azure App Proxy to provide secure remote access to on-premises applications.

Publish SharePoint Server

You can publish a SharePoint site through Web Application Proxy when the SharePoint site is configured for claims-based authentication or Integrated Windows authentication. If you want to use Active Directory Federation Services (AD FS) for pre-authentication, you must configure a relying party using one of the wizards.

- If the SharePoint site uses claims-based authentication, you must use the Add Relying Party Trust Wizard to configure the relying party trust for the application.
- If the SharePoint site uses Integrated Windows authentication, you must use the Add Non-Claims-Based Relying Party Trust Wizard to configure the relying party trust for the application. You can use IWA with a claims-based web application provided that you configure KDC.

  To allow users to authenticate using Integrated Windows authentication, the Web Application Proxy server must be joined to a domain.

  You must configure the application to support Kerberos constrained delegation. You can do this on the domain controller for any application. You can also configure the application directly on the backend server if it is running on Windows Server 2012 R2 or Windows Server 2012 . For more information, see What's New in Kerberos Authentication. You must also make sure that the Web Application Proxy servers are configured for delegation to the service principal names of the backend servers. For a walkthrough of how to configure Web Application Proxy to publish an application using Integrated Windows authentication, see Configure a site to use Integrated Windows authentication.

If your SharePoint site is configured using either alternate access mappings (AAM) or host-named site collections, you can use different external and backend server URLs to publish your application. However, if you do not configure your SharePoint site using AAM or host-named site collections, you must use the same external and backend server URLs.

Publish Exchange Server

The following table describes the Exchange services that you can publish through Web Application Proxy and the supported pre-authentication for these services:

EXCHANGE SERVICE	PRE-AUTHENTICATION	NOTES
Outlook Web App	- AD FS using non-claims-based authentication - Pass-through - AD FS using claims-based authentication for on-premises Exchange 2013 Service Pak 1 (SP1)	For more information see: Using AD FS claims-based authentication with Outlook Web App and EAC
Exchange Control Panel	Pass-through	
Outlook Anywhere	Pass-through	You must publish additional URLs for Outlook Anywhere to work correctly: - The autodiscover, EWS, and OAB (in case of Outlook cache mode) URL. - The external host name of the Exchange Server; that is, the URL that is configured for clients to connect to. - The internal FQDN of the Exchange Server.
Exchange ActiveSync	Pass-through AD FS using HTTP Basic authorization protocol	
Exchange Web Services	Pass-through	
Autodiscover	Pass-through	
Offline Address Book	Pass-through	

To publish Outlook Web App using Integrated Windows authentication, you must use the Add Non-Claims-Based Relying Party Trust Wizard to configure the relying party trust for the application.

To allow users to authenticate using Kerberos constrained delegation the Web Application Proxy server must be joined to a domain.

You must configure the application to support Kerberos authentication. Additionally you need to register a service principal name (SPN) to the account that the web service is running under. You can do this on the domain controller or on the backend servers. In a load balanced Exchange environment this would require using the Alternate Service Account, see Configuring Kerberos authentication for load-balanced Client Access servers

You can also configure the application directly on the backend server if it is running on Windows Server 2012 R2 or Windows Server 2012. For more information, see What's New in Kerberos Authentication. You must also make sure that the Web Application Proxy servers are configured for delegation to the service principal names of the backend servers.

Publishing Remote Desktop Gateway through Web Application Proxy

If you want to restrict access to your Remote Access Gateway and add pre-authentication for remote access, you can roll it out through Web Application Proxy. This is a really good way to make sure you have rich pre-authentication for RDG including MFA. Publishing without pre-authentication is also an option and provides a single point of entry into your systems.

How to publish an application in RDG using Web Application Proxy pass-through authentication

1. Installation will be different depending on whether your RD Web Access (/rdweb) and RD Gateway (rpc) roles are on the same server or on different servers.

2. If the RD Web Access and RD Gateway roles are hosted on the same RDG server, you can simply publish the root FQDN in Web Application Proxy such as, https://rdg.contoso.com/.

   You can also publish the two virtual directories individually e.g.https://rdg.contoso.com/rdweb/ and https://rdg.contoso.com/rpc/.

3. If the RD Web Access and the RD Gateway are hosted on separate RDG servers, you have to publish the two virtual directories individually. You can use the same or different external FQDN's e.g. https://rdweb.contoso.com/rdweb/ and https://gateway.contoso.com/rpc/.

4. If the External and Internal FQDN's are different you should not disable request header translation on the RDWeb publishing rule. This can be done by running the following PowerShell script on the Web Application Proxy server but it should be enabled by default.

   ```
   Get-WebApplicationProxyApplication applicationname | Set-WebApplicationProxyApplication -
   DisableTranslateUrlInRequestHeaders:$false
   ```

   > **NOTE**
   >
   > If you need to support rich clients such as RemoteApp and Desktop Connections or iOS Remote Desktop connections, these do not support pre-authentication so you have to publish RDG using pass-through authentication.

How to publish an application in RDG using Web Application Proxy with pre-authentication

1. Web Application Proxy pre-authentication with RDG works by passing the pre-authentication cookie obtained by Internet Explorer being passed into the Remote Desktop Connection client (mstsc.exe). This is then used by the Remote Desktop Connection client (mstsc.exe). This is then used by Remote Desktop Connection client as proof of authentication.

   The following procedure tells the Collection server to include the necessary custom RDP properties in the Remote App RDP files that are sent to clients. These tell the client that pre-authentication is required and to pass the cookies for the pre-authentication server address to Remote Desktop Connection client (mstsc.exe) . In conjunction with disabling the HttpOnly feature on the Web Application Proxy application, this allows the Remote Desktop Connection client (mstsc.exe) to utilize the Web Application Proxy cookie obtained through the browser.

   Authentication to the RD Web Access server will still use the RD Web Access form logon. This provides the least number of user authentication prompts as the RD Web Access logon form creates a client-side credential store that can then be used by Remote Desktop Connection client (mstsc.exe) for any subsequent Remote App launch.

2. First, create a manual Relying Party Trust in AD FS as if you were publishing a claims aware app. This means that you have to create a dummy relying party trust that is there to enforce pre-authentication, so that you get pre-authentication without Kerberos Constrained Delegation to the published server. Once a user has authenticated, everything else is passed through.

   > **WARNING**
   >
   > It might seem that using delegation is preferable but it does not fully solve mstsc SSO requirements and there are issues when delegating to the /rpc directory because the client expects to handle the RD Gateway authentication itself.

3. To create a manual Relying Party Trust, follow the steps in the AD FS Management Console:

   a. Use the **Add Relying Party Trust** wizard

   b. Select **Enter data about the relying party manually**.

   c. Accept all default settings.

   d. For the Relying Party Trust identifier, enter the external FQDN you will use for RDG access, for example https://rdg.contoso.com/.

   This is the relying party trust you will use when publishing the app in Web Application Proxy.

4. Publish the root of the site (for example, https://rdg.contoso.com/) in Web Application Proxy. Set the pre-authentication to AD FS and use the relying party trust you created above. This will enable /rdweb and /rpc to use the same Web Application Proxy authentication cookie.

   It is possible to publish /rdweb and /rpc as separate applications and even to use different published servers. You just need to ensure that you publish both using the same Relying Party Trust as the Web Application Proxy token is issued for the Relying Party Trust and is therefore valid across applications published with the same Relying Party Trust.

5. If the External and Internal FQDN's are different you should not disable request header translation on the RDWeb publishing rule. This can be done by running the following PowerShell script on the Web Application Proxy server but it should be enabled by default:

   ```
   Get-WebApplicationProxyApplication applicationname | Set-WebApplicationProxyApplication -
   DisableTranslateUrlInRequestHeaders:$true
   ```

6. Disable the HttpOnly cookie property in Web Application Proxy on the RDG published application. To allow the RDG ActiveX control access to the Web Application Proxy authentication cookie, you have to disable the HttpOnly property on the Web Application Proxy cookie.

   This requires you to install the November 2014 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 (KB3000850).

   After installing the hotfix, run the following PowerShell script on the Web Application Proxy server specifying the relevant application name:

   ```
   Get-WebApplicationProxyApplication applicationname | Set-WebApplicationProxyApplication -
   DisableHttpOnlyCookieProtection:$true
   ```

   Disabling HttpOnly allows the RDG ActiveX control access to the Web Application Proxy authentication cookie.

7. Configure the relevant RDG collection on the Collection server to let the Remote Desktop Connection client (mstsc.exe) know that pre-authentication is required in the rdp file.

   - In Windows Server 2012 and Windows Server 2012 R2 this can be accomplished by running the following PowerShell cmdlet on the RDG Collection server:

     ```
     Set-RDSessionCollectionConfiguration -CollectionName "<yourcollectionname>" -CustomRdpProperty
     "pre-authentication server address:s: <https://externalfqdn/rdweb/>`nrequire pre-
     authentication:i:1"
     ```

     Make sure you remove the < and > brackets when you replace with your own values, for example:

```
Set-RDSessionCollectionConfiguration -CollectionName "MyAppCollection" -CustomRdpProperty
"pre-authentication server address:s: https://rdg.contoso.com/rdweb/`nrequire pre-
authentication:i:1"
```

- In Windows Server 2008 R2:

  a. Log onto the Terminal Server with an account that has Administrator privileges.

  b. Go to **Start** >**Administrative Tools** > **Terminal Services** > **TS RemoteApp Manager.**

  c. In the **Overview** pane of TS RemoteApp Manager, next to RDP Settings, click **Change**.

  d. On the **Custom RDP Settings** tab, type the following RDP settings into the Custom RDP settings box:

  `pre-authentication server address: s: https://externalfqdn/rdweb/`

  `require pre-authentication:i:1`

  e. When you are done, click **Apply**.

  This tells the Collection server to include the custom RDP properties in the RDP files that are sent to clients. These tell the client that pre-authentication is required and to pass the cookies for the pre-authentication server address to the Remote Desktop Connection client (mstsc.exe) . This, in conjunction with disabling HttpOnly on the Web Application Proxy application, allows the Remote Desktop Connection client (mstsc.exe) to utilize the Web Application Proxy authentication cookie obtained through the browser.

  For more information on RDP, see Configuring the TS Gateway OTP Scenario.

See also

- Planning to Publish Applications Using Web Application Proxy
- Troubleshooting Web Application Proxy
- Web Application Proxy Walkthrough Guide

Configure VPN device tunnels in Windows 10

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows 10 version 1709

Always On VPN gives you the ability to create a dedicated VPN profile for device or machine. Always On VPN connections include two types of tunnels:

- *Device tunnel* connects to specified VPN servers before users log on to the device. Pre-login connectivity scenarios and device management purposes use device tunnel.
- *User tunnel* connects only after a user logs on to the device. User tunnel allows users to access organization resources through VPN servers.

Unlike *user tunnel*, which only connects after a user logs on to the device or machine, *device tunnel* allows the VPN to establish connectivity before the user logs on. Both *device tunnel* and *user tunnel* operate independently with their VPN profiles, can be connected at the same time, and can use different authentication methods and other VPN configuration settings as appropriate. User tunnel supports SSTP and IKEv2, and device tunnel supports IKEv2 only with no support for SSTP fallback.

User tunnel is supported on domain-joined, nondomain-joined (workgroup), or Azure AD–joined devices to allow for both enterprise and BYOD scenarios. It is available in all Windows editions, and the platform features are available to third parties by way of UWP VPN plug-in support.

Device tunnel can only be configured on domain-joined devices running Windows 10 Enterprise or Education version 1709 or later. There is no support for third-party control of the device tunnel. Device tunnel does not support using the Name Resolution Policy table (NRPT). Device tunnel does not support Force tunnel. You must configure it as Split tunnel. |

Prerequisites

You must enable machine certificate authentication for VPN connections and define a root certification authority for authenticating incoming VPN connections.

```
$VPNRootCertAuthority = "Common Name of trusted root certification authority"
$RootCACert = (Get-ChildItem -Path cert:LocalMachine\root | Where-Object {$_.Subject -Like
"*$VPNRootCertAuthority*" })
Set-VpnAuthProtocol -UserAuthProtocolAccepted Certificate, EAP -RootCertificateNameToAccept $RootCACert -
PassThru
```

FEATURES	REQUIREMENTS
• Always connected (as long as there is network connectivity and the computer is not in a low power state) • Connects to your organization VPN servers before user logon • Can coexist with one active user tunnel • Transparent to the user	• The device must be a domain joined computer running Windows 10 Enterprise or Education version 1709 or later. • The tunnel is only configurable for the Windows built-in VPN solution and is established using IKEv2 with computer certificate authentication. • Only one device tunnel can be configured per device.

VPN Device Tunnel Configuration

The sample profile XML below provides good guidance for scenarios where only client initiated pulls are required over the device tunnel. Traffic filters are leveraged to restrict the device tunnel to management traffic only. This configuration works well for Windows Update, typical Group Policy (GP) and Microsoft Endpoint Configuration Manager update scenarios, as well as VPN connectivity for first logon without cached credentials, or password reset scenarios.

For server-initiated push cases, like Windows Remote Management (WinRM), Remote GPUpdate, and remote Configuration Manager update scenarios – you must allow inbound traffic on the device tunnel, so traffic filters cannot be used. If in the device tunnel profile you turn on traffic filters, then the Device Tunnel denies inbound traffic. This limitation is going to be removed in future releases.

Sample VPN profileXML

Following is the sample VPN profileXML.

```
<VPNProfile>
  <NativeProfile>
<Servers>vpn.contoso.com</Servers>
<NativeProtocolType>IKEv2</NativeProtocolType>
<Authentication>
  <MachineMethod>Certificate</MachineMethod>
</Authentication>
<RoutingPolicyType>SplitTunnel</RoutingPolicyType>
 <!-- disable the addition of a class based route for the assigned IP address on the VPN interface -->
<DisableClassBasedDefaultRoute>true</DisableClassBasedDefaultRoute>
  </NativeProfile>
  <!-- use host routes(/32) to prevent routing conflicts -->
  <Route>
<Address>10.10.0.2</Address>
<PrefixSize>32</PrefixSize>
  </Route>
  <Route>
<Address>10.10.0.3</Address>
<PrefixSize>32</PrefixSize>
  </Route>
<!-- traffic filters for the routes specified above so that only this traffic can go over the device tunnel
-->
  <TrafficFilter>
<RemoteAddressRanges>10.10.0.2, 10.10.0.3</RemoteAddressRanges>
  </TrafficFilter>
<!-- need to specify always on = true -->
  <AlwaysOn>true</AlwaysOn>
<!-- new node to specify that this is a device tunnel -->
 <DeviceTunnel>true</DeviceTunnel>
<!--new node to register client IP address in DNS to enable manage out -->
<RegisterDNS>true</RegisterDNS>
</VPNProfile>
```

Depending on the needs of each particular deployment scenario, another VPN feature that can be configured with the device tunnel is Trusted Network Detection.

```
 <!-- inside/outside detection -->
  <TrustedNetworkDetection>corp.contoso.com</TrustedNetworkDetection>
```

Deployment and Testing

You can configure device tunnels by using a Windows PowerShell script and using the Windows Management Instrumentation (WMI) bridge. The Always On VPN device tunnel must be configured in the context of the **LOCAL SYSTEM** account. To accomplish this, it will be necessary to use PsExec, one of the PsTools included in the Sysinternals suite of utilities.

For guidelines on how to deploy a per device `(.\Device)` vs. a per user `(.\User)` profile, see Using PowerShell scripting with the WMI Bridge Provider.

Run the following Windows PowerShell command to verify that you have successfully deployed a device profile:

```
Get-VpnConnection -AllUserConnection
```

The output displays a list of the device-wide VPN profiles that are deployed on the device.

Example Windows PowerShell Script

You can use the following Windows PowerShell script to assist in creating your own script for profile creation.

```
Param(
[string]$xmlFilePath,
[string]$ProfileName
)

$a = Test-Path $xmlFilePath
echo $a

$ProfileXML = Get-Content $xmlFilePath

echo $XML

$ProfileNameEscaped = $ProfileName -replace ' ', '%20'

$Version = 201606090004

$ProfileXML = $ProfileXML -replace '<', '&lt;'
$ProfileXML = $ProfileXML -replace '>', '&gt;'
$ProfileXML = $ProfileXML -replace '"', '&quot;'

$nodeCSPURI = './Vendor/MSFT/VPNv2'
$namespaceName = "root\cimv2\mdm\dmmap"
$className = "MDM_VPNv2_01"

$session = New-CimSession

try
{
$newInstance = New-Object Microsoft.Management.Infrastructure.CimInstance $className, $namespaceName
$property = [Microsoft.Management.Infrastructure.CimProperty]::Create("ParentID", "$nodeCSPURI", 'String',
'Key')
$newInstance.CimInstanceProperties.Add($property)
$property = [Microsoft.Management.Infrastructure.CimProperty]::Create("InstanceID", "$ProfileNameEscaped",
'String', 'Key')
$newInstance.CimInstanceProperties.Add($property)
$property = [Microsoft.Management.Infrastructure.CimProperty]::Create("ProfileXML", "$ProfileXML", 'String',
'Property')
$newInstance.CimInstanceProperties.Add($property)

$session.CreateInstance($namespaceName, $newInstance)
$Message = "Created $ProfileName profile."
Write-Host "$Message"
}
catch [Exception]
{
$Message = "Unable to create $ProfileName profile: $_"
Write-Host "$Message"
exit
}
$Message = "Complete."
Write-Host "$Message"
```

Additional Resources

The following are additional resources to assist with your VPN deployment.

VPN client configuration resources

The following are VPN client configuration resources.

- How to Create VPN profiles in Configuration Manager
- Configure Windows 10 Client Always On VPN Connections
- VPN profile options

Remote Access Server Gateway resources

The following are Remote Access Server (RAS) Gateway resources.

- Configure RRAS with a Computer Authentication Certificate
- Troubleshooting IKEv2 VPN Connections
- Configure IKEv2-based Remote Access

> **IMPORTANT**
>
> When using Device Tunnel with a Microsoft RAS gateway, you will need to configure the RRAS server to support IKEv2 machine certificate authentication by enabling the **Allow machine certificate authentication for IKEv2** authentication method as described here. Once this setting is enabled, it is strongly recommended that the **Set-VpnAuthProtocol** PowerShell cmdlet, along with the **RootCertificateNameToAccept** optional parameter, is used to ensure that RRAS IKEv2 connections are only permitted for VPN client certificates that chain to an explicitly defined internal/private Root Certification Authority. Alternatively, the **Trusted Root Certification Authorities** store on the RRAS server should be amended to ensure that it does not contain public certification authorities as discussed here. Similar methods may also need to be considered for other VPN gateways.

About Always On VPN

12/9/2022 • 8 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows 11

Always On VPN has many benefits over the Windows VPN solutions of the past. The following key improvements align Always On VPN with Microsoft's cloud-first, mobile-first vision:

- **Platform Integration:** Always On VPN has improved integration with the Windows operating system and third-party solutions to provide a robust platform for countless advanced connection scenarios.
- **Security:** Always On VPN has new, advanced security capabilities to restrict the type of traffic, which applications can use the VPN connection, and which authentication methods you can use to initiate the connection. When the connection is active most of the time, it is especially important to secure the connection. For more details, see VPN authentication options.
- **VPN Connectivity:** Always On VPN, with or without Device Tunnel provides auto-trigger capability. Before Always On VPN, the ability to trigger an automatic connection through either user or device authentication was not possible.
- **Networking control:** Always On VPN allows administrators to specify routing policies at a more granular level—even down to the individual application—which is perfect for line-of-business (LOB) apps that require special remote access. Always On VPN is also fully compatible with both Internet Protocol version 4 (IPv4) and version 6 (IPv6). Unlike DirectAccess, there is no specific dependency on IPv6.

  > **NOTE**
  >
  > Before you get started, make sure to enable IPv6 on the VPN server. Otherwise, a connection cannot be established and an error message displays.

- **Configuration and compatibility:** Always On VPN can be deployed and managed several ways, which gives Always On VPN several advantages over the other VPN client software.

Platform integration

Microsoft has introduced or improved the following integration capabilities in Always On VPN:

KEY IMPROVEMENT	DESCRIPTION
Windows Information Protection (WIP)	Integration with WIP allows network policy enforcement to determine whether traffic is permitted to go over the VPN. If the user profile is active and WIP policies are applied, Always On VPN is automatically triggered to connect. Also, when you use WIP, there's no need to specify AppTriggerList and TrafficFilterList rules separately in the VPN profile (unless you want more advanced configuration) because the WIP policies and application lists automatically take effect.

KEY IMPROVEMENT	DESCRIPTION
Windows Hello for Business	Always On VPN natively supports Windows Hello for Business (in certificate-based authentication mode) to provide a seamless single sign-on experience for both sign-in to the machine and connection to the VPN. Therefore, no secondary authentication (user credentials) is needed for the VPN connection, making it possible to use an Always On connection with Windows Hello for Business authentication.
Microsoft Azure conditional access	The Always On VPN client can integrate with the Azure conditional access platform to enforce multifactor authentication (MFA), device compliance, or a combination of the two. When compliant with conditional access policies, Azure Active Directory (Azure AD) issues a short-lived (by default, 60 minutes) IP Security (IPsec) authentication certificate that can then be used to authenticate to the VPN gateway. Device compliance uses Configuration Manager/Intune compliance policies, which can include the device health attestation state as part of the connection compliance check.
Azure AD Multi-Factor Authentication	When combined with Remote Authentication Dial-In User Service (RADIUS) services and the Network Policy Server (NPS) extension for Azure AD Multi-Factor Authentication, VPN authentication can use strong MFA.
Third-party VPN plug-in	With the Universal Windows Platform (UWP), third-party VPN providers can create a single application for the full range of Windows devices. The UWP provides a guaranteed core API layer across devices, eliminating the complexity of and problems often associated with writing kernel-level drivers. Currently, Windows UWP VPN plug-ins exist for Pulse Secure, F5 Access, Check Point Capsule VPN, FortiClient, SonicWall Mobile Connect, and GlobalProtect; no doubt, others will appear in the future.

Security

The primary improvements in security are in the following areas:

KEY IMPROVEMENT	DESCRIPTION

KEY IMPROVEMENT	DESCRIPTION
Traffic filters	Through traffic filters, you can specify client-side policies that determine which traffic is allowed into the corporate network. In this way, administrators can apply app or traffic restrictions on the VPN interface, limiting its use to specific sources, destination ports, and IP addresses. Two types of filtering rules are available: • **App-based rules.** App-based firewall rules are based on a list of specified applications so that only traffic originating from these apps are permitted to go over the VPN interface. • **Traffic-based rules.** Traffic-based firewall rules are based on network requirements like ports, addresses, and protocols. Use these rules only for traffic that matches these specific conditions are permitted to go over the VPN interface. ***Note:*** These rules apply only to traffic outbound from the device. Use of Traffic filters blocks inbound traffic from the corporate network to the client.
Per-App VPN	Per-App VPN is like having an app-based traffic filter, but it goes farther to combine application triggers with an app-based traffic filter so that VPN connectivity is constrained to a specific application as opposed to all applications on the VPN client. The feature automatically initiates when the app starts.
Support for customized IPsec cryptography algorithms	Always On VPN supports the use of both RSA and elliptic curve cryptography–based custom cryptographic algorithms to meet stringent government or organizational security policies.
Native Extensible Authentication Protocol (EAP) support	Always On VPN natively supports EAP, which allows you to use a diverse set of Microsoft and third-party EAP types as part of the authentication workflow. EAP provides secure authentication based on the following authentication types: • Username and password • Smart card (both physical and virtual) • User certificates • Windows Hello for Business • MFA support by way of EAP RADIUS integration The application vendor controls third-party UWP VPN plug-in authentication methods, although they have an array of available options, including custom credential types and OTP support.

VPN connectivity

The following are the primary improvements in Always On VPN connectivity:

KEY IMPROVEMENT	DESCRIPTION

KEY IMPROVEMENT	DESCRIPTION
Always On	Always On is a Windows feature that enables the active VPN profile to connect automatically and remain connected based on triggers—namely, user sign-in, network state change, or device screen active. Always On is also integrated into the connected standby experience to maximize battery life.
Application triggering	You can configure VPN profiles in Windows to connect automatically on the launch of a specified set of applications. You can configure both desktop and UWP applications to trigger a VPN connection.
Name-based triggering	With Always On VPN, you can define rules so that specific domain name queries trigger the VPN connection. Windows devices support name-based triggering for domain-joined and nondomain-joined machines (previously, only nondomain-joined machines were supported).
Trusted network detection	Always On VPN includes this feature to ensure that VPN connectivity is not triggered if a user is connected to a trusted network within the corporate boundary. You can combine this feature with any of the triggering methods mentioned earlier to provide a seamless "only connect when needed" user experience.
Device Tunnel	Always On VPN gives you the ability to create a dedicated VPN profile for device or machine. Unlike *User Tunnel*, which only connects after a user logs on to the device or machine, *Device Tunnel* allows the VPN to establish connectivity before user sign-in. Both Device Tunnel and User Tunnel operate independently with their VPN profiles, can be connected at the same time, and can use different authentication methods and other VPN configuration settings as appropriate.

Networking

The following are some of the networking improvements in Always On VPN:

KEY IMPROVEMENT	DESCRIPTION
Dual-stack support for IPv4 and IPv6	Always On VPN natively supports the use of both IPv4 and IPv6 in a dual-stack approach. It has no specific dependency on one protocol over the other, which allows for maximum IPv4/IPv6 application compatibility combined with support for future IPv6 networking needs. ***Note:*** Before you get started, make sure to enable IPv6 on the VPN server. Otherwise, a connection cannot be established and an error message displays.
Application-specific routing policies	In addition to defining global VPN connection routing policies for internet and intranet traffic separation, it is possible to add routing policies to control the use of split tunnel or force tunnel configurations on a per-application basis. This option gives you more granular control over which apps are allowed to interact with which resources through the VPN tunnel.

KEY IMPROVEMENT	DESCRIPTION
Exclusion routes	Always On VPN supports the ability to specify exclusion routes that specifically control routing behavior to define which traffic should traverse the VPN only and not go over the physical network interface. ***Notes:*** - Exclusion routes currently work for traffic within the same subnet as the client, for example, LinkLocal. - Exclusion routes only work in a Split Tunnel setup.

Configuration and compatibility

The following are some of the configuration and compatibility improvements in Always On VPN:

KEY IMPROVEMENT	DESCRIPTION
Third-party VPN gateway compatibility	The Always On VPN client does not require the use of a Microsoft-based VPN gateway to operate. Through the support of the IKEv2 protocol, the client facilitates interoperability with third-party VPN gateways that support this industry-standard tunneling type. You can also achieve interoperability with third-party VPN gateways by using a UWP VPN plug-in combined with a custom tunneling type without sacrificing Always On VPN platform features and benefits. ***Note:*** Consult with your gateway or third-party back-end appliance vendor on configurations and compatibility with Always On VPN and Device Tunnel using IKEv2.
Industry-standard IKEv2 VPN protocol support	The Always On VPN client supports IKEv2, one of today's most widely used industry-standard tunneling protocols. This compatibility maximizes interoperability with third-party VPN gateways.
Platform support	Always On VPN supports domain-joined, nondomain-joined (workgroup), or Azure AD–joined devices to allow for both enterprises and bring your own device (BYOD) scenarios. Also, Always On VPN is available in all Windows editions.
Diverse management and deployment mechanisms	You can use many management and deployment mechanisms to manage VPN settings (called a *VPN profile*), including Windows PowerShell, Microsoft Endpoint Configuration Manager, Intune or third-party mobile device management (MDM) tool, and Windows Configuration Designer. These options simplify the configuration of Always On VPN regardless of the client management tools you use.
Standardized VPN profile definition	Always On VPN supports configuration using a standard XML profile (ProfileXML), providing a standard configuration template format that most management and deployment toolsets use.

Next steps

- Learn about some of the advanced Always On VPN features
- Learn more about the Always On VPN technology
- Start planning your Always On VPN deployment

Always On VPN deployment infrastructure

12/9/2022 • 11 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows 11

The following illustration shows the infrastructure that is required to deploy Always On VPN.

The connection process depicted in this illustration is composed of the following steps:

1. The Windows VPN client uses public DNS servers to perform a name resolution query for the IP address of the VPN gateway.
2. The VPN client uses the IP address returned by DNS to send a connection request to the VPN gateway.
3. The VPN gateway is also configured as a Remote Authentication Dial-In User Service (RADIUS) Client; the VPN RADIUS Client sends the connection request to the organization/corporate NPS server for connection request processing.
4. The NPS server processes the connection request, including performing authorization and authentication, and determines whether to allow or deny the connection request.
5. The NPS server forwards an Access-Accept or Access-Deny response to the VPN gateway.

6. The connection is initiated or terminated based on the response that the VPN server received from the NPS server.

For more information on each infrastructure component depicted in the illustration above, see the following sections.

> **NOTE**
> If you already have some of these technologies deployed on your network, you can use the instructions in this deployment guidance to perform additional configuration of the technologies for this deployment purpose.

Domain Name System (DNS)

Both internal and external Domain Name System (DNS) zones are required, which assumes that the internal zone is a delegated subdomain of the external zone (for example, corp.contoso.com and contoso.com).

Learn more about Domain Name System (DNS) or Core Network Guide.

> **NOTE**
> Other DNS designs, such as split-brain DNS (using the same domain name internally and externally in separate DNS zones) or unrelated internal and external domains (e.g., contoso.local and contoso.com) are also possible. For more information about deploying split-brain DNS, see Use DNS Policy for Split-Brain DNS Deployment.

Firewalls

Make sure that your firewalls allow the traffic that is necessary for both VPN and RADIUS communications to function correctly.

For more information, see Configure Firewalls for RADIUS Traffic.

Remote Access as a RAS Gateway VPN Server

In Windows Server 2016, the Remote Access server role is designed to perform well as both a router and a remote access server; therefore, it supports a wide array of features. For this deployment guidance, you require only a small subset of these features: support for IKEv2 VPN connections and LAN routing.

IKEv2 is a VPN tunneling protocol described in Internet Engineering Task Force Request for Comments 7296. The primary advantage of IKEv2 is that it tolerates interruptions in the underlying network connection. For example, if the connection is temporarily lost or if a user moves a client computer from one network to another, IKEv2 automatically restores the VPN connection when the network connection is reestablished—all without user intervention.

By using RAS Gateway, you can deploy VPN connections to provide end users with remote access to your organization's network and resources. Deploying Always On VPN maintains a persistent connection between clients and your organization network whenever remote computers are connected to the Internet. With RAS Gateway, you can also create a site-to-site VPN connection between two servers at different locations, such as between your primary office and a branch office, and use Network Address Translation (NAT) so that users inside the network can access external resources, such as the Internet. Also, RAS Gateway supports Border Gateway Protocol (BGP), which provides dynamic routing services when your remote office locations also have edge gateways that support BGP.

You can manage Remote Access Service (RAS) Gateways by using Windows PowerShell commands and the Remote Access Microsoft Management Console (MMC).

Network Policy Server (NPS)

NPS allows you to create and enforce organization-wide network access policies for connection request authentication and authorization. When you use NPS as a Remote Authentication Dial-In User Service (RADIUS) server, you configure network access servers, such as VPN servers, as RADIUS clients in NPS.

You also configure network policies that NPS uses to authorize connection requests, and you can configure RADIUS accounting so that NPS logs accounting information to log files on the local hard disk or in a Microsoft SQL Server database.

For more information, see Network Policy Server (NPS).

Active Directory Certificate Services

The Certification Authority (CA) Server is a certification authority that is running Active Directory Certificate Services. The VPN configuration requires an Active Directory-based public key infrastructure (PKI).

Organizations can use AD CS to enhance security by binding the identity of a person, device, or service to a corresponding public key. AD CS also includes features that allow you to manage certificate enrollment and revocation in a variety of scalable environments. For more information, see Active Directory Certificate Services Overview and Public Key Infrastructure Design Guidance.

During completion of the deployment, you will configure the following certificate templates on the CA.

- The User Authentication certificate template
- The VPN Server Authentication certificate template
- The NPS Server Authentication certificate template

Certificate Templates

Certificate templates can greatly simplify the task of administering a certification authority (CA) by allowing you to issue certificates that are preconfigured for selected tasks. The Certificate Templates MMC snap-in allows you to perform the following tasks.

- View properties for each certificate template.
- Copy and modify certificate templates.
- Control which users and computers can read templates and enroll for certificates.
- Perform other administrative tasks relating to certificate templates.

Certificate templates are an integral part of an enterprise certification authority (CA). They are an important element of the certificate policy for an environment, which is the set of rules and formats for certificate enrollment, use, and management.

For more information, see Certificate Templates.

Digital Server Certificates

This deployment guidance provides instructions for using Active Directory Certificate Services (AD CS) to both enroll and automatically enroll certificates to Remote Access and NPS infrastructure servers. AD CS allows you to build a public key infrastructure (PKI) and provide public key cryptography, digital certificates, and digital signature capabilities for your organization.

When you use digital server certificates for authentication between computers on your network, the certificates provide:

1. Confidentiality through encryption.

2. Integrity through digital signatures.
3. Authentication by associating certificate keys with a computer, user, or device accounts on a computer network.

For more information, see Active Directory Certificate Services Overview.

Active Directory Domain Services (AD DS)

AD DS provides a distributed database that stores and manages information about network resources and application-specific data from directory-enabled applications. Administrators can use AD DS to organize elements of a network, such as users, computers, and other devices, into a hierarchical containment structure. The hierarchical containment structure includes the Active Directory forest, domains in the forest, and organizational units (OUs) in each domain. A server that is running AD DS is called a domain controller.

AD DS contains the user accounts, computer accounts, and account properties that are required by Protected Extensible Authentication Protocol (PEAP) to authenticate user credentials and to evaluate authorization for VPN connection requests. For information about deploying AD DS, see the Windows Server Core Network Guide.

During completion of the steps in this deployment, you will configure the following items on the domain controller.

- Enable certificate autoenrollment in Group Policy for computers and users
- Create the VPN Users Group
- Create the VPN Servers Group
- Create the NPS Servers Group

Active Directory Users and Computers

Active Directory Users and Computers is a component of AD DS that contains accounts that represent physical entities, such as a computer, a person, or a security group. A security group is a collection of user or computer accounts that administrators can manage as a single unit. User and computer accounts that belong to a particular group are referred to as group members.

User accounts in Active Directory Users and Computers have dial-in properties that NPS evaluates during the authorization process - unless the **Network Access Permission** property of the user account is set to **Control access through NPS Network Policy**. This is the default setting for all user accounts. In some cases, however, this setting might have a different configuration that blocks the user from connecting using VPN. To protect against this possibility, you can configure the NPS server to ignore user account dial-in properties.

For more information, see Configure NPS to Ignore User Account Dial-in Properties.

Group Policy Management

Group Policy Management enables directory-based change and configuration management of user and computer settings, including security and user information. You use Group Policy to define configurations for groups of users and computers.

With Group Policy, you can specify settings for registry entries, security, software installation, scripts, folder redirection, remote installation services, and Internet Explorer maintenance. The Group Policy settings that you create are contained in a Group Policy object (GPO). You can associate a GPO with selected Active Directory system containers (sites, domains, and OUs) to apply the GPO's settings to the users and computers in those Active Directory containers. To manage Group Policy objects across an enterprise, you can use the Group Policy Management Editor Microsoft Management Console (MMC).

Windows VPN Clients

In addition to the server components, ensure that the client computers you configure to use VPN are running Windows 10 Anniversary Update (version 1607) or later. The Windows VPN clients must be domain-joined to your Active Directory domain.

The Windows VPN client is highly configurable and offers many options. To better illustrate the specific features this scenario uses, Table 1 identifies the VPN feature categories and specific configurations that this deployment references. You'll configure the individual settings for these features by using the VPNv2 configuration service provider (CSP) discussed later in this deployment.

Table 1. VPN Features and Configurations Discussed in this Deployment

VPN FEATURE	DEPLOYMENT SCENARIO CONFIGURATION
Connection type	Native IKEv2
Routing	Split tunneling
Name resolution	Domain Name Information List and DNS suffix
Triggering	Always On and Trusted Network Detection
Authentication	PEAP-TLS with TPM–protected user certificates

NOTE

PEAP-TLS and TPM are "Protected Extensible Authentication Protocol with Transport Layer Security" and "Trusted Platform Module," respectively.

VPNv2 CSP Nodes

In this deployment, you use the ProfileXML VPNv2 CSP node to create the VPN profile that is delivered to Windows client computers. Configuration Service Providers (CSPs) are interfaces that expose various management capabilities within the Windows client; conceptually, CSPs work similar to how Group Policy works. Each CSP has configuration nodes that represent individual settings. Also like Group Policy settings, you can tie CSP settings to registry keys, files, permissions, and so on. Similar to how you use the Group Policy Management Editor to configure Group Policy objects (GPOs), you configure CSP nodes by using a mobile device management (MDM) solution such as Microsoft Intune. MDM products like Intune offer a user-friendly configuration option that configures the CSP in the operating system.

However, you can't configure some CSP nodes directly through a user interface (UI) like the Intune Admin Console. In these cases, you must configure the Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings manually. You configure OMA-URIs by using the OMA Device Management protocol (OMA-DM), a universal device management specification that most modern Apple, Android, and Windows devices support. As long as they adhere to the OMA-DM specification, all MDM products should interact with these operating systems in the same way.

Windows offers many CSPs, but this deployment focuses on using the VPNv2 CSP to configure the VPN client. The VPNv2 CSP allows configuration of each VPN profile setting in Windows through a unique CSP node. Also contained in the VPNv2 CSP is a node called *ProfileXML*, which allows you to configure all the settings in one node rather than individually. For more information about ProfileXML, see the section "ProfileXML overview" later in this deployment. For details about each VPNv2 CSP node, see the VPNv2 CSP.

Next steps

- Learn about some of the advanced Always On VPN features
- Start planning your Always On VPN deployment

Related topics

- Microsoft server software support for Microsoft Azure virtual machines: This article discusses the support policy for running Microsoft server software in the Microsoft Azure virtual machine environment (infrastructure-as-a-service).
- Remote Access: This topic provides an overview of the Remote Access server role in Windows Server.
- Windows VPN Client Technical Guide: This guide walks you through the decisions you will make for

Windows clients in your enterprise VPN solution and how to configure your deployment. This guide references the VPNv2 Configuration Service Provider (CSP) and provides mobile device management (MDM) configuration instructions using Microsoft Intune and the VPN Profile template for Windows clients.

- Core Network Guide: This guide provides instructions on how to plan and deploy the core components required for a fully functioning network and a new Active Directory domain in a new forest.
- Domain Name System (DNS): This topic provides an overview of Domain Name Systems (DNS). In Windows Server, DNS is a server role that you can install by using Server Manager or Windows PowerShell commands. If you are installing a new Active Directory forest and domain, DNS is automatically installed with Active Directory as the Global Catalogue server for the forest and domain.
- Active Directory Certificate Services Overview: This document provides an overview of Active Directory Certificate Services (AD CS) in Windows Server® 2012. AD CS is the Server Role that allows you to build a public key infrastructure (PKI) and provide public key cryptography, digital certificates, and digital signature capabilities for your organization.
- Public Key Infrastructure Design Guidance: This forum provides guidance on designing Public Key Infrastructures (PKIs). Before you configure a PKI and certification authority (CA) hierarchy, you should be aware of your organization's security policy and certificate practice statement (CPS).
- Active Directory Certificate Services Overview: This step-by-step guide describes the steps needed to set up a basic configuration of Active Directory® Certificate Services (AD CS) in a lab environment. AD CS in Windows Server® 2008 R2 provides customizable services for creating and managing public key certificates used in software security systems employing public key technologies.
- Network Policy Server (NPS): This topic provides an overview of Network Policy Server in Windows Server. Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication and authorization.

Always On VPN features and functionalities

12/9/2022 • 6 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10

In this topic, you learn about the features and functionalities of Always On VPN. The following table is not an exhaustive list, however, it does include some of the most common features and functionalities used in remote access solutions.

> **TIP**
> If you currently use DirectAccess, we recommend that you investigate the Always On VPN functionality carefully to determine if it addresses all of your remote access needs before migrating from DirectAccess to Always On VPN.

FUNCTIONAL AREA	ALWAYS ON VPN
Seamless, transparent connectivity to the corporate network.	You can configure Always On VPN to support auto-triggering based on application launch or namespace resolution requests. Define using: **VPNv2/ProfileName/AlwaysOn** **VPNv2/ProfileName/AppTriggerList** **VPNv2/ProfileName/DomainNameInformationList/AutoTrigger**
Use of a dedicated Infrastructure Tunnel to provide connectivity for users not signed into the corporate network.	You can achieve this functionality by using the Device Tunnel feature in the VPN profile. ***Note:*** Device Tunnel can only be configured on domain-joined devices using IKEv2 with computer certificate authentication. Define using: **VPNv2/ProfileName/DeviceTunnel**
Use of manage-out to allow remote connectivity to clients from management systems located on the corporate network.	You can achieve this functionality by using the Device Tunnel feature in the VPN profile combined with configuring the VPN connection to dynamically register the IP addresses assigned to the VPN interface with internal DNS services. ***Note:*** If you turn on traffic filters in the Device Tunnel profile, then the Device Tunnel denies inbound traffic (from the corporate network to the client). Define using: **VPNv2/ProfileName/DeviceTunnel** **VPNv2/ProfileName/RegisterDNS**

FUNCTIONAL AREA	ALWAYS ON VPN
Fall back when clients are behind firewalls or proxy servers.	You can configure to fall back to SSTP (from IKEv2) by using the automatic tunnel/protocol type within the VPN profile. ***Note:*** User Tunnel supports SSTP and IKEv2, and Device Tunnel supports IKEv2 only with no support for SSTP fallback. Define using: **VPNv2/ProfileName/NativeProfile/NativeProtocolType**
Support for end-to-edge access mode.	Always On VPN provides connectivity to corporate resources by using tunnel policies that require authentication and encryption until they reach the VPN gateway. By default, the tunnel sessions terminate at the VPN gateway, which also functions as the IKEv2 gateway, providing end-to-edge security.
Support for machine certificate authentication.	The IKEv2 protocol type available as part of the Always On VPN platform specifically supports the use of machine or computer certificates for VPN authentication. ***Note:*** IKEv2 is the only supported protocol for Device Tunnel and there is no support option for SSTP fallback. Define using: **VPNv2/ProfileName/NativeProfile/Authentication/MachineMethod**
Use security groups to limit remote access functionality to specific clients.	You can configure Always On VPN to support granular authorization when using RADIUS, which includes the use of security groups to control VPN access.
Support for servers behind an edge firewall or NAT device.	Always On VPN gives you the ability to use protocols like IKEv2 and SSTP that fully support the use of a VPN gateway that is behind a NAT device or edge firewall. ***Note:*** User Tunnel supports SSTP and IKEv2, and Device Tunnel supports IKEv2 only with no support for SSTP fallback.
Ability to determine intranet connectivity when connected to the corporate network.	Trusted network detection provides the capability to detect corporate network connections, and it is based on an assessment of the connection-specific DNS suffix assigned to network interfaces and network profile. Define using: **VPNv2/ProfileName/TrustedNetworkDetection**

FUNCTIONAL AREA	ALWAYS ON VPN
Compliance using Network Access Protection (NAP).	The Always On VPN client can integrate with Azure conditional access to enforce MFA, device compliance, or a combination of both. When compliant with conditional access policies, Azure AD issues a short-lived (by default, 60 minutes) IPsec authentication certificate that the client can then use to authenticate to the VPN gateway. Device compliance takes advantage of Configuration Manager/Intune compliance policies, which can include the device health attestation state. At this time, Azure VPN conditional access provides the closest replacement to the existing NAP solution, although there is no form of remediation service or quarantine network capabilities. For more details, see VPN and conditional access. Define using: **VPNv2/ProfileName/DeviceCompliance**
Ability to define which management servers are accessible before user sign-in.	You can achieve this functionality in Always On VPN by using the Device Tunnel feature (available in version 1709 – for IKEv2 only) in the VPN profile combined with traffic filters to control which management systems on the corporate network are accessible through the Device Tunnel. ***Note:*** If you turn on traffic filters in the Device Tunnel profile, then the Device Tunnel denies inbound traffic (from the corporate network to the client). Define using: **VPNv2/ProfileName/DeviceTunnel** **VPNv2/ProfileName/TrafficFilterList**

Other functionalities

Each item in this section is a use case scenario or commonly used remote access functionality for which Always On VPN has improved functionality—either through an expansion of functionality or elimination of a previous limitation.

FUNCTIONAL AREA	ALWAYS ON VPN
Domain-joined devices with Enterprise SKUs requirement.	Always On VPN supports domain-joined, nondomain-joined (workgroup), or Azure AD–joined devices to allow for both enterprise and BYOD scenarios. Always On VPN is available in all Windows editions, and the platform features are available to third parties by way of UWP VPN plug-in support. ***Note:*** Device Tunnel can only be configured on domain-joined devices running Windows 10 Enterprise or Education version 1709 or later. There is no support for third-party control of the Device Tunnel.
Support for both IPv4 and IPv6.	With Always On VPN, users can access both IPv4 and IPv6 resources on the corporate network. The Always On VPN client uses a dual-stack approach that doesn't specifically depend on IPv6 or the need for the VPN gateway to provide NAT64 or DNS64 translation services.

FUNCTIONAL AREA	ALWAYS ON VPN
Support for two-factor or OTP authentication.	The Always On VPN platform natively supports EAP, which allows for the use of diverse Microsoft and third-party EAP types as part of the authentication workflow. Always On VPN specifically supports smart card (both physical and virtual) and Windows Hello for Business certificates to satisfy two-factor authentication requirements. Also, Always On VPN supports OTP through MFA (not supported natively, only supported on third-party plugins) by way of EAP RADIUS integration. Define using: **VPNv2/ProfileName/NativeProfile/Authentication**
Support for multiple domains and forests.	The Always On VPN platform has no dependency on Active Directory Domain Services (AD DS) forests or domain topology (or associated functional/schema levels) because it doesn't require the VPN client to be domain joined to function. Group Policy is therefore not a dependency to define VPN profile settings because you do not use it during client configuration. Where Active Directory authorization integration is required, you can achieve it through RADIUS as part of the EAP authentication and authorization process.
Support for both split and force tunnel for internet/intranet traffic separation.	You can configure Always On VPN to support both force tunnel (the default operating mode) and split tunnel natively. Always On VPN provides Other granularity for application-specific routing policies. ***Note:*** Force Tunnel is supported by User Tunnel only. No other VPN Tunnels can be active in parallel to a Force Tunnel User Tunnel. Define using: **VPNv2/ProfileName/NativeProfile/RoutingPolicyType** **VPNv2/ProfileName/TrafficFilterList/App/RoutingPolicyType**
Multiple protocol support.	Always On VPN can be configured to support SSTP natively if Secure Sockets Layer fallback from IKEv2 is required. ***Note:*** User Tunnel supports SSTP and IKEv2, and Device Tunnel supports IKEv2 only with no support for SSTP fallback.
Connectivity Assistant to provide corporate connectivity status.	Always On VPN is fully integrated with the native Network Connectivity Assistant and provides connectivity status from the View All Networks interface. With the advent of Windows 10 Creators Update (version 1703), VPN connection status and VPN connection control for User Tunnel are now available through the Network flyout (for the Windows built-in VPN client), as well.

FUNCTIONAL AREA	ALWAYS ON VPN
Name resolution of corporate resources using short-name, fully qualified domain name (FQDN), and DNS suffix.	Always On VPN can natively define one or more DNS suffixes as part of the VPN connection and IP address assignment process, including corporate resource name resolution for short names, FQDNs, or entire DNS namespaces. Always On VPN also supports the use of Name Resolution Policy Tables to provide namespace-specific resolution granularity. ***Note:*** Avoid the use of Global Suffixes as they interfere with shortname resolution when using Name Resolution Policy tables. Define using: **VPNv2/ProfileName/DnsSuffix** **VPNv2/ProfileName/DomainNameInformationList**

Next steps

- Learn more about the Always On VPN enhancements
- Learn about some of the advanced Always On VPN features
- Learn more about the Always On VPN technology
- Start planning your Always On VPN deployment

Advanced features of Always On VPN

12/9/2022 • 7 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

Beyond a standard deployment, you can add other advanced VPN features to improve the security and availability of your VPN connection. For example, the VPN server can use these features to help make sure that the connecting client is healthy before it allows a connection.

High Availability

The following are more options for high availability.

OPTION	DESCRIPTION
Server resilience and load balancing	In environments that require high availability or that support large numbers of requests, you can increase the performance and resiliency of Remote Access. Use can load balancing between multiple servers that are running Network Policy Server (NPS) and enable Remote Access server clustering. Related documents: • NPS Proxy Server Load Balancing • Deploy Remote Access in a Cluster
Geographic site resilience	For IP-based geolocation, you can use Global Traffic Manager with DNS in Windows Server 2016. For more robust geographic load balancing, you can use Global Server Load Balancing solutions, such as Microsoft Azure Traffic Manager. Related documents: • Overview of Traffic Manager • Microsoft Azure Traffic Manager

Advanced Authentication

The following are more options for authentication.

OPTION	DESCRIPTION

OPTION	DESCRIPTION
Windows Hello for Business	In Windows 10, Windows Hello for Business replaces passwords by providing strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or Personal Identification Number (PIN). The Windows 10 VPN client is compatible with Windows Hello for Business. After the user logs in by using a gesture, the VPN connection uses the Windows Hello for Business certificate for certificate-based authentication. Related documents: • Windows Hello for Business • Technical Case Study: Enabling Remote Access with Windows Hello for Business in Windows 10
Azure Multifactor Authentication (MFA)	Azure AD Multi-Factor Authentication has cloud and on-premises versions that you can integrate with the Windows VPN authentication mechanism. For more information about how this mechanism works, see Integrate RADIUS authentication with Azure AD Multi-Factor Authentication Server.

Advanced VPN Features

The following are more options for advanced features.

OPTION	DESCRIPTION
Traffic filtering	If you have to enforce the choice of which applications VPN clients can access, you can enable VPN Traffic Filters. For more information, see VPN security features.
App-triggered VPN	You can configure VPN profiles to connect automatically when certain applications or types of applications start. For more information about this and other triggering options, see VPN auto-triggered profile options.

OPTION	DESCRIPTION
VPN conditional access	Conditional access and device compliance can require managed devices to meet standards before they can connect to the VPN. One of the advanced features for VPN conditional access allows you to restrict the VPN connections to only the devices whose client authentication certificate contains the "AAD Conditional Access" OID of **1.3.6.1.4.1.311.87**. To restrict the VPN connections, you must do the following: 1. On the NPS server, open the **Network Policy Server** snap-in. 2. Expand **Policies** > **Network Policies**. 3. Right-click the **Virtual Private Network (VPN) Connections** Network Policy and select **Properties**. 4. Select the **Settings** tab. 5. Select **Vendor Specific**, and then select **Add**. 6. Select the **Allowed-Certificate-OID** option, and then select **Add**. 7. Paste the AAD Conditional Access OID of **1.3.6.1.4.1.311.87** as the attribute value, and then select **OK** two times. 8. Select **Close**, and then select **Apply**. After you follow these steps, when VPN clients try to connect by using any certificate other than the short-lived cloud certificate, the connection fails. For more information about conditional access, see VPN and conditional access.

Blocking VPN Clients that Use Revoked Certificates

After you install updates, the RRAS server can enforce certificate revocation for VPNs that use IKEv2 and machine certificates for authentication, such as device tunnel Always-on VPNs. This means that for such VPNs, the RRAS server can deny VPN connections to clients that try to use a revoked certificate.

Availability

The following table lists the releases that contain the fixes for each version of Windows.

OPERATING SYSTEM VERSION	RELEASE
Windows Server, version 1903	KB4501375
Windows Server 2019 Windows Server, version 1809	KB4505658
Windows Server, version 1803	KB4507466
Windows Server, version 1709	KB4507465
Windows Server 2016, version 1607	KB4503294

How to configure prerequisites

1. Install the Windows updates as they become available.
2. Make sure that all the VPN client and RRAS server certificates that you use have CDP entries, and that the RRAS server can reach the respective CRLs.
3. On the RRAS server, use the **Set-VpnAuthProtocol** PowerShell cmdlet to configure the **RootCertificateNameToAccept** parameter.

   The following example lists the commands to do this. In the example, **CN=Contoso Root Certification Authority** represents the distinguished name of the Root Certification Authority.

   ```
   $cert1 = ( Get-ChildItem -Path cert:LocalMachine\root | Where-Object -FilterScript { $_.Subject -Like "*CN=Contoso Root Certification Authority*" } )
   Set-VpnAuthProtocol -RootCertificateNameToAccept $cert1 -PassThru
   ```

How to configure the RRAS server to enforce certificate revocation for VPN connections that are based on IKEv2 machine certificates

1. In a Command Prompt window, run the following command:

   ```
   reg add HKLM\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\Ikev2 /f /v CertAuthFlags /t REG_DWORD /d "4"
   ```

2. Restart the **Routing and Remote Access** service.

To disable certificate revocation for these VPN connections, set **CertAuthFlags = 2** or remove the **CertAuthFlags** value, and then restart the **Routing and Remote Access** service.

How to revoke a VPN client certificate for a VPN connection that is based on an IKEv2 machine certificate

1. Revoke the VPN client certificate from the Certification Authority.
2. Publish a new CRL from the Certification Authority.
3. On the RRAS server, open an administrative Command Prompt window, and then run the following commands:

   ```
   certutil -urlcache * delete
   certutil -setreg chain\ChainCacheResyncFiletime @now
   ```

How to verify that certificate revocation for IKEv2 machine certificate-based VPN connections is working

> **NOTE**
> Before you use this procedure, make sure that you enable the CAPI2 operational event log.

1. Follow the previous steps to revoke a VPN client certificate.
2. Try to connect to the VPN by using a client that has the revoked certificate. The RRAS server should refuse the connection and display a message such as "IKE authentication credentials are unacceptable."
3. On the RRAS server, open Event Viewer, and navigate to **Applications and Services Logs/Microsoft/Windows/CAPI2**.
4. Search for an event that has the following information:
   - Log Name: **Microsoft-Windows-CAPI2/Operational Microsoft-Windows-CAPI2/Operational**

- Event ID: **41**
- The event contains the following text: **subject="*Client FQDN*"** (*Client FQDN* represents the fully qualified domain name of the client that has the revoked certificate.)

The **<Result>** field of the event data should include **The certificate is revoked**. For example, see the following excerpts from an event:

```
Log Name:      Microsoft-Windows-CAPI2/Operational Microsoft-Windows-CAPI2/Operational
Source:        Microsoft-Windows-CAPI2
Date:          5/20/2019 1:33:24 PM
Event ID:      41
...
Event Xml:
<Event xmlns="https://schemas.microsoft.com/win/2004/08/events/event">
 <UserData>
  <CertVerifyRevocation>
   <Certificate fileRef="C97AE73E9823E8179903E81107E089497C77A720.cer"
subjectName="client01.corp.contoso.com" />
   <IssuerCertificate fileRef="34B1AE2BD868FE4F8BFDCA96E47C87C12BC01E3A.cer" subjectName="Contoso
Root Certification Authority" />
   ...
   <Result value="80092010">The certificate is revoked.</Result>
  </CertVerifyRevocation>
 </UserData>
</Event>
```

Trusted Platform Module (TPM) Key Attestation

A user certificate that has a TPM-attested key provides higher security assurance, backed up by non-exportability, anti-hammering, and isolation of keys provided by the TPM.

For more information about TPM key attestation in Windows 10, see TPM Key Attestation.

Next step

Start planning the Always On VPN deployment: Before you install the Remote Access server role on the computer that you plan to use as a VPN server, do the following tasks. After appropriate planning, you can deploy Always On VPN, and optionally configure conditional access for VPN connectivity using Azure AD.

Related topics

- NPS Proxy Server Load Balancing: Remote Authentication Dial-In User Service (RADIUS) clients, which are network access servers such as virtual private network (VPN) servers and wireless access points, create connection requests and send them to RADIUS servers such as NPS. In some cases, an NPS server might receive too many connection requests at one time, resulting in degraded performance or an overload.
- Overview of Traffic Manager: This topic provides an overview of Azure Traffic Manager, which allows you to control the distribution of user traffic for service endpoints. Traffic Manager uses the Domain Name System (DNS) to direct client requests to the most appropriate endpoint based on a traffic-routing method and the health of the endpoints.
- Windows Hello for Business: This topic provides an overview of the prerequisites, such as cloud only deployments and hybrid deployments. This topic also lists frequently asked questions about Windows Hello for Business.
- Technical case study: Enabling Remote Access with Windows Hello for Business in Windows 10: In this

technical case study, learn how Microsoft implements remote access with Windows Hello for Business. Windows Hello for Business is a private/public key or certificate-based authentication approach for organizations and consumers that goes beyond passwords. This form of authentication relies on key pair credentials that can replace passwords and are resistant to breaches, thefts, and phishing.

- Integrate RADIUS authentication with Azure AD Multi-Factor Authentication: This topic walks you through adding and configuring a RADIUS client authentication with Azure AD Multi-Factor Authentication Server. RADIUS is a standard protocol to accept authentication requests and to process those requests. The Azure AD Multi-Factor Authentication Server can act as a RADIUS server.
- VPN security features: This topic provides an overview of VPN security guidelines for LockDown VPN, Windows Information Protection (WIP) integration with VPN, and traffic filters.
- VPN auto-triggered profile options: This topic provides an overview of VPN auto-triggered profile options, such as app trigger, name-based trigger, and Always On.
- VPN and conditional access: This topic provides an overview of cloud-based Conditional Access Platform to provide a device compliance option for remote clients. Conditional Access is a policy-based evaluation engine that lets you create access rules for any Azure Active Directory (Azure AD) connected application.
- TPM Key Attestation: This topic provides an overview of Trusted Platform Module (TPM) and steps to deploy TPM key attestation. You can also find troubleshooting information and steps to resolve issues.

DirectAccess

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

You can use this topic for a brief overview of DirectAccess, including the server and client operating systems that support DirectAccess, and for links to additional DirectAccess documentation for Windows Server.

> **NOTE**
>
> In addition to this topic, the following DirectAccess documentation is available.
>
> - DirectAccess Deployment Paths in Windows Server
> - Prerequisites for Deploying DirectAccess
> - DirectAccess Unsupported Configurations
> - DirectAccess Test Lab Guides
> - DirectAccess Known Issues
> - DirectAccess Capacity Planning
> - DirectAccess Offline Domain Join
> - Troubleshooting DirectAccess
> - Deploy a Single DirectAccess Server Using the Getting Started Wizard
> - Deploy a Single DirectAccess Server with Advanced Settings
> - Add DirectAccess to an Existing Remote Access (VPN) Deployment

DirectAccess allows connectivity for remote users to organization network resources without the need for traditional Virtual Private Network (VPN) connections. With DirectAccess connections, remote client computers are always connected to your organization - there is no need for remote users to start and stop connections, as is required with VPN connections. In addition, your IT administrators can manage DirectAccess client computers whenever they are running and Internet connected.

> **IMPORTANT**
>
> Do not attempt to deploy Remote Access on a virtual machine (VM) in Microsoft Azure. Using Remote Access in Microsoft Azure is not supported. You cannot use Remote Access in an Azure VM to deploy VPN, DirectAccess, or any other Remote Access feature in Windows Server 2016 or earlier versions of Windows Server. For more information, see Microsoft server software support for Microsoft Azure virtual machines.

DirectAccess provides support only for domain-joined clients that include operating system support for DirectAccess.

The following client operating systems support DirectAccess.

- Windows 11 Enterprise
- Windows 10 Enterprise
- Windows 10 Enterprise 2015 Long Term Servicing Branch (LTSB)
- Windows 8.1 Enterprise

DirectAccess Unsupported Configurations

12/9/2022 • 4 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Review the following list of unsupported DirectAccess configurations before you start your deployment to avoid having to start your deployment again.

File Replication Service (FRS) distribution of Group Policy objects (SYSVOL replications)

Do not deploy DirectAccess in environments where your domain controllers are running the File Replication Service (FRS) for distribution of Group Policy objects (SYSVOL replications). Deployment of DirectAccess is not supported when you use FRS.

You are using FRS if you have domain controllers that are running Windows Server 2003 or Windows Server 2003 R2. In addition, you might be using FRS if you previously used Windows 2000 Server or Windows Server 2003 domain controllers and you never migrated SYSVOL replication from FRS to Distributed File System Replication (DFS-R).

If you deploy DirectAccess with FRS SYSVOL replication, you risk the unintentional deletion of DirectAccess Group Policy objects that contain the DirectAccess server and client configuration information. If these objects are deleted, your DirectAccess deployment will suffer an outage, and client computers that use DirectAccess will not be able to connect to your network.

If you are planning to deploy DirectAccess, you must use domain controllers that are running operating systems later than Windows Server 2003 R2, and you must use DFS-R.

For information on migrating from FRS to DFS-R, see the SYSVOL Replication Migration Guide: FRS to DFS Replication.

Network Access Protection for DirectAccess clients

Network Access Protection (NAP) is used to determine whether remote client computers meet IT policies before they are granted access to the corporate network. NAP was deprecated in Windows Server 2012 R2 and is not included in Windows Server 2016. For this reason, starting a new deployment of DirectAccess with NAP is not recommended. A different method of end point control for the security of DirectAccess clients is recommended.

Multisite support for Windows 7 clients

When DirectAccess is configured in a multisite deployment, Windows 10®, Windows® 8.1, and Windows® 8 clients have the capability of connecting to the nearest site. Windows 7® client computers do not have the same capability. Site selection for Windows 7 clients is set to a particular site at the time of policy configuration, and these clients will always connect to that designated site, regardless of their location.

User-based access control

DirectAccess policies are computer based, not user based. Specifying DirectAccess user policies to control access to the corporate network is not supported.

Customizing DirectAccess policy

DirectAccess can be configured by using the DirectAccess Setup Wizard, the Remote Access Management console, or the Remote Access Windows PowerShell cmdlets. Using any means other than the DirectAccess Setup Wizard to configure DirectAccess, such as modifying DirectAccess Group Policy Objects directly or manually modifying the default policy settings on the server or client, is not supported. These modifications may result in an unusable configuration.

KerbProxy authentication

When you configure a DirectAccess server with the Getting Started Wizard, the DirectAccess server is automatically configured to use KerbProxy authentication for computer and user authentication. Because of this, you should only use the Getting Started Wizard for single-site deployments where only Windows 10®, Windows 8.1, or Windows 8 clients are deployed.

In addition, the following features should not be used with KerbProxy authentication:

- Load balancing by using either an external load balancer or Windows Load Balancer
- Two-factor authentication where smart cards or a one-time password (OTP) are required

The following deployment plans are not supported if you enable KerbProxy authentication:

- Multisite.
- DirectAccess support for Windows 7 clients.
- Force tunneling. To ensure that KerbProxy authentication is not enabled when you use force tunneling, configure the following items while running the wizard:
  - Enable force tunneling
  - Enable DirectAccess for Windows 7 clients

> **NOTE**
> For the previous deployments, you should use the Advanced Configuration Wizard, which uses a two-tunnel configuration with a certificate-based computer and user authentication. For more information, see Deploy a Single DirectAccess Server with Advanced Settings.

Using ISATAP

ISATAP is a transition technology that provides IPv6 connectivity in IPv4-only corporate networks. It is limited to small- and medium-sized organizations with a single DirectAccess server deployment, and it allows remote management of DirectAccess clients. If ISATAP is deployedin a multisite, load balancing, or multidomain environment, you must remove it or move it to a native IPv6 deployment before you configure DirectAccess.

IPHTTPS and one-time password (OTP) endpoint configuration

When you use IPHTTPS, the IPHTTPS connection must terminate on the DirectAccess server, not on any other device, such as a load balancer. Similarly, the out-of-band Secure Sockets Layer (SSL) connection that is created during one-time password (OTP) authentication must terminate on the DirectAccess server. All devices between the endpoints of these connections must be configured in pass-through mode.

Force Tunnel with OTP authentication

Do not deploy a DirectAccess server with two-factor authentication with OTP and Force Tunneling, or OTP authentication will fail. An out-of-band Secure Sockets Layer (SSL) connection is required between the DirectAccess server and the DirectAccess client. This connection requires an exemption to send the traffic outside of the DirectAccess tunnel. In a Force Tunnel configuration, all traffic must flow through a DirectAccess tunnel, and no exemption is allowed after the tunnel is established. Because of this, it is not supported to have OTP authentication in a Forced Tunnel configuration.

Deploying DirectAccess with a Read-Only Domain Controller

DirectAccess servers must have access to a read-write domain controller, and do not function correctly with a Read-Only Domain Controller (RODC).

A read-write domain controller is required for many reasons, including the following:

- On the DirectAccess server, a read-write domain controller is required to open the Remote Access Microsoft Management Console (MMC).
- The DirectAccess server must both read and write to the DirectAccess client and DirectAccess server Group Policy Objects (GPOs).
- The DirectAccess server reads and writes to the client GPO specifically from the Primary Domain Controller emulator (PDCe).

Because of these requirements, do not deploy DirectAccess with an RODC.

DirectAccess Capacity Planning

12/9/2022 • 6 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This document is a report on Windows Server 2012 DirectAccess server performance. Testing was performed to determine throughput capacity using high-end computer hardware and low-end computer hardware. High and low-end CPU performance was dependent on the network traffic throughput and the types of clients used. A typical DirectAccess deployment (and the basis for these tests) consists of 1/3 (30%) IPHTTPS clients, and 2/3 (70%) Teredo clients. Teredo clients outperform IPHTTPS clients in part because Windows Server 2012 utilizes Receive Side Scaling (RSS) which allows use of all CPU cores. In these tests, since RSS is enabled, Hyper threading is disabled. In addition, TCP/IP in Windows Server 2012 supports UDP traffic allowing Teredo clients to load balance across CPUs.

Data was collected from both a low-end (4 core, 4 Gig) server, and from hardware which is expected to be a more typical in a high-end (8 core, 8 Gig) server. Below is a screen shot of the new Windows 8 task manager on low-end hardware with 750 clients (562 Teredo, 188 IPHTTPS) running ~77 Mbits/sec. This is to simulate users who do not present smart card credentials.

These test results indicate that Teredo performs better than IPHTTPS in Windows 8, but that both Teredo and IPHTTPS bandwidth usage has improved when compared to Windows 7.

High-end hardware test environment

The following chart shows the results of the high-end hardware performance test environment. All test results and analysis are detailed in this document.

CONFIGURATION - HARDWARE	LOW-END HARDWARE (4GB RAM, 4 CORE)	HIGH-END HARDWARE (8 GB, 8 CORE)
Double Tunnel - PKI - Including DNS64/NAT64	750 concurrent connections at 50% CPU, 50 % Memory with Corpnet NIC throughput 75 Mbps. Stretch target is 1000 users @ 50% CPU.	1500 concurrent connections at 50% CPU, 50 % Memory with Corpnet NIC throughput 150 Mbps.

Test Environment

Perf Bench Topology

The performance test environment is a 5 machine bench. For the low-end test, one 4-core 4 Gig DirectAccess server was used and for the high-end hardware test, one 8-core, 16 Gig DirectAccess server was used. For low-end and high-end test environments the following was used: one Back end Server (the sender), and two client computers (the receivers). Receivers are split among the two client computers. Otherwise, the receivers would be CPU bound and limit the number of clients and bandwidth. On the receiving side a simulator to simulate hundreds of clients (either HTTPS or Teredo clients are simulated). IPsec, DOSp are both configured. RSS is enabled on the DirectAccess server. RSS queue size is set to 8. Without configuring RSS, a single processor will get pegged at a high utilization while the other cores are underutilized. Also of note is that the DirectAccess server is a 4 core machine with hyper threading turned off. Hyper threading is off because RSS only works on physical cores and use of hyper threading produces skewed results. (This means that not all the cores will be uniformly loaded).

Testing results for low-end hardware:

Testing was performed both with 1000 & with 750 clients. In all cases traffic split was 70% Teredo and 30% IPHTTPS. All tests involved TCP traffic over Nat64 using 2 IPsec tunnels per client. In all tests, memory utilization was light and CPU utilization was acceptable.

Individual Test Results:

The following sections describe individual tests. Each section title highlights the key elements of each test followed by a summary description of the results and then a chart showing the detailed results data.

Low-end Perf: 750 clients, 70/30 split, 84.17 Mbits/sec throughput:

The following three tests represent low-end hardware. In the below test runs, there were 750 clients with a throughput of 84.17 Mbits/sec and a traffic split of 562 Teredo and 188 IPHTTPS. Teredo MTU was set to 1472, and Teredo Shunt was enabled. CPU utilization averaged 46.42% across the three tests, and average memory utilization, expressed as a percentage of committed bytes of the total available memory of 4Gb, was 25.95%.

SCENARIO	CPUAVG (FROM COUNTER)	MBIT/S (CORP SIDE)	MBIT/S (INTERNET SIDE)	ACTIVE QMSA	ACTIVE MMSA	MEM UTILIZATION (4 GIG SYSTEM)
Low-end HW. 562 Teredo clients. 188 IPHTTPS clients.	47.7472542	84.3	119.13	1502.05	1502.1	26.27%
Low-end HW. 562 Teredo clients. 188 IPHTTPS clients.	46.3889778	84.146	118.73	1501.25	1501.2	25.90%
Low-end HW. 562 Teredo clients. 188 IPHTTPS clients.	45.113082	84.0494	118.43	1546.14	1546.1	25.68%

1000 clients, 70/30 split, 78 Mbits/sec throughput:

The following three tests represent performance on low-end hardware. In the test runs below, there were 1000 clients with an average throughput of ~78.64 Mbits/sec and a traffic split of 700 Teredo and 300 IPHTTPS. Teredo MTU was set to 1472 and Teredo Shunt was enabled. CPU utilization averaged ~50.7%, and average memory utilization, expressed as a percentage of committed bytes of the total available memory of 4Gb, was ~28.7%.

SCENARIO	CPUAVG (FROM COUNTER)	MBIT/S (CORP SIDE)	MBIT/S (INTERNET SIDE)	ACTIVE QMSA	ACTIVE MMSA	MEM UTILIZATION (4 GIG SYSTEM)
Low-end HW. 700 Teredo clients. 300 IPHTTPS clients.	51.28406247	78.6432	113.19	2002.42	1502.1	25.59%
Low-end HW. 700 Teredo clients. 300 IPHTTPS clients.	51.06993128	78.6402	113.22	2001.4	1501.2	30.87%

SCENARIO	CPUAVG (FROM COUNTER)	MBIT/S (CORP SIDE)	MBIT/S (INTERNET SIDE)	ACTIVE QMSA	ACTIVE MMSA	MEM UTILIZATION (4 GIG SYSTEM)
Low-end HW. 700 Teredo clients. 300 IPHTTPS clients.	49.75235617	78.6387	113.2	2002.6	1546.1	30.66%

1000 clients, 70/30 split, 109 Mbits/sec throughput:

In the following three test runs there were 1000 clients with an average throughput of ~109.2 Mbits/sec and a traffic split of 700 Teredo and 300 IPHTTPS. Teredo MTU was set to 1472 and Teredo Shunt was enabled. CPU utilization averaged ~59.06% across the three tests, and average memory utilization, expressed as a percentage of committed bytes of the total available memory of 4Gb, was ~27.34%.

SCENARIO	CPUAVG (FROM COUNTER)	MBIT/S (CORP SIDE)	MBIT/S (INTERNET SIDE)	ACTIVE QMSA	ACTIVE MMSA	MEM UTILIZATION (4 GIG SYSTEM)
Low-end HW. 700 Teredo clients. 300 IPHTTPS clients.	59.81640675	108.305	153.14	2001.64	2001.6	24.38%
Low-end HW. 700 Teredo clients. 300 IPHTTPS clients.	59.46473798	110.969	157.53	2005.22	2005.2	28.72%
Low-end HW. 700 Teredo clients. 300 IPHTTPS clients.	57.89089768	108.305	153.14	1999.53	2018.3	24.38%

Testing results for high-end hardware:

Testing was performed with 1500 clients. Traffic split was 70% Teredo and 30% IPHTTPS. All tests involved TCP traffic over Nat64 using 2 IPsec tunnels per client. In all tests, memory utilization was light and CPU utilization was acceptable.

Individual Test Results:

The following sections describe individual tests. Each section title highlights the key elements of each test followed by a summary description of the results and then a chart containing the detailed results data.

1500 clients, 70/30 split, 153.2 Mbits/sec throughput

The following five tests represent high-end hardware. In the below test runs there were 1500 clients with an average throughput of 153.2 Mbits/sec and a traffic split of 1050 Teredo and 450 IPHTTPS. CPU utilization

averaged 50.68% across the five tests, and average memory utilization, expressed as a percentage of committed bytes of the total available memory of 8Gb, was 22.25%.

SCENARIO	CPUAVG (FROM COUNTER)	MBIT/S (CORP SIDE)	MBIT/S (INTERNET SIDE)	ACTIVE QMSA	ACTIVE MMSA	MEM UTILIZATION (4 GIG SYSTEM)
High-end HW. 1050 Teredo clients. 450 IPHTTPS clients.	51.712437	157.029	216.29	3000.31	3046	21.58%
High-end HW. 1050 Teredo clients. 450 IPHTTPS clients.	48.86020205	151.012	206.53	3002.86	3045.3	21.15%
High-end HW. 1050 Teredo clients. 450 IPHTTPS clients.	52.23979519	155.511	213.45	3001.15	3002.9	22.90%
High-end HW. 1050 Teredo clients. 450 IPHTTPS clients.	51.26269767	155.09	212.92	3000.74	3002.4	22.91%
High-end HW. 1050 Teredo clients. 450 IPHTTPS clients.	50.15751307	154.772	211.92	3000.9	3002.1	22.93%
High-end HW. 1050 Teredo clients. 450 IPHTTPS clients.	49.83665607	145.994	201.92	3000.51	3006	22.03%

Performance Monitor
File Action View Window Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
User Defined
IPHTTPS-perf-test
Server Manager Per
System
Event Trace Sessions
Startup Event Trace Ses
Reports
IPHTTPS Global
Default
Sessions - Total sessions
450.000
IPsec AuthIP IPv6
Active Extended Mode SAs
3,004.000
Active Main Mode SAs
3,005.000
Active Quick Mode SAs
3,004.000
Failed Extended Mode Negotiations/sec
27.001
Task Manager
File Options View
Processes Performance Users Details Services
CPU
49% 2.22 GHz
Memory
1.7/16.0 GB (11%)
Ethernet
S: 56.0 Kbps R: 16.0 Kbps
Ethernet
Not connected
Ethernet
S: 8.9 Mbps R: 149 Mbps
Ethernet
S: 185 Mbps R: 30.9 Mbps
CPU
Intel(R) Xeon(R) CPU L5630 @ 2.13GHz
% Utilization over 60 seconds
100%
Utilization
49%
Speed
2.22 GHz
Processes
37
Threads
824
Handles
33810
Up time
1:05:27:24
Maximum speed: 2.13 GHz
Sockets: 2
Cores: 8
Logical processors: 8
Virtualization: Enabled
L1 cache: 512 KB
L2 cache: 2.0 MB
L3 cache: 24.0 MB
Fewer details
Open Resource Monitor

RAS Gateway

12/9/2022 • 9 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

With RAS Gateway, Cloud Service Providers (CSPs) and Enterprises can enable datacenter and cloud network traffic routing between both virtual and physical networks, including the Internet.

> **NOTE**
> RAS Gateway supports IPv4 and IPv6, including IPv4 and IPv6 forwarding. When you configure RAS Gateway with Network Address Translation (NAT), only NAT44 is supported.

Who will be interested in the RAS Gateway?

If you're a system administrator, network architect, or other IT professional, RAS Gateway may interest you under one or more of the following circumstances:

- You design or support IT infrastructure for an organization that is using or planning to use Hyper-V to deploy virtual machines (VMs) on virtual networks.
- You design or support IT infrastructure for an organization that has deployed or is planning to deploy cloud technologies.
- You want to provide full network connectivity between physical networks and virtual networks.
- You want to provide your organization's customers with access to their virtual networks over the Internet.
- You want to connect offices at different physical locations across the Internet.

This topic, which is intended for Information Technology (IT) professionals, provides information about the RAS Gateway, including RAS Gateway deployment modes and features.

This topic contains the following sections:

- RAS Gateway Deployment Modes
- Clustering RAS Gateway for high availability
- RAS Gateway Features
- RAS Gateway Deployment Scenarios
- RAS Gateway Management Tools

RAS Gateway Deployment Modes

RAS Gateway includes the following deployment modes:

Single tenant mode

It's recommended that you don't deploy RAS Gateway in single tenant mode. For single tenant mode scenarios, see Single Tenant.

Multitenant mode

If your organization is a CSP or an Enterprise with multiple tenants, you can deploy RAS Gateway in multitenant mode to provide network traffic routing to and from virtual and physical networks.

Multitenancy is the ability of a cloud infrastructure to support the virtual machine workloads of multiple tenants, yet isolate them from each other, while all of the workloads run on the same infrastructure. The multiple workloads of an individual tenant can interconnect and be managed remotely, but these systems do not interconnect with the workloads of other tenants, nor can other tenants remotely manage them.

For example, an Enterprise might have many different virtual subnets, each of which is dedicated to servicing a specific department, such as Research and Development or Accounting. In another example, a CSP has many tenants with isolated virtual subnets existing in the same physical datacenter. In both cases, RAS Gateway can route traffic to and from each tenant while maintaining the designed isolation of each tenant. This capability makes the RAS Gateway multitenant-aware.

Virtual networks are created by using Hyper-V Network Virtualization. RAS Gateway is integrated with Hyper-V Network Virtualization, and is able to route network traffic effectively in circumstances where there are many different customers - or tenants - who have isolated virtual networks in the same datacenter.

Hyper-V Network Virtualization provides you with the ability to deploy a virtual machine (VM) network that is independent of the underlying physical network. With VM networks, which are composed of one or more virtual subnets, the exact physical location of an IP subnet is decoupled from the virtual network topology. As a result, you can easily move your on premises subnets to the cloud - while preserving your existing IP addresses and topology in the cloud. This ability to preserve infrastructure allows existing services to continue to work, unaware of the physical location of the subnets. That is, Hyper-V Network Virtualization enables a seamless hybrid cloud.

> **NOTE**
>
> Hyper-V Network Virtualization is a network overlay technology using Network Virtualization Generic Routing Encapsulation (NVGRE), which allows tenants to bring their own address space and allows CSPs better scalability than is possible by using VLANs for tenant isolation.

In Windows Server, RAS Gateway routes network traffic between the physical network and VM network resources, regardless of where the resources are located. You can use RAS Gateway to route network traffic between physical and virtual networks at the same physical location or at many different physical locations.

For example, if you have both a physical network and a virtual network at the same physical location, you can deploy a computer running Hyper-V that is configured with an RAS Gateway VM to act as a forwarding gateway and route traffic between the virtual and physical networks.

In another example, if your virtual networks exist in the cloud, your CSP can deploy an RAS Gateway so that you can create a virtual private network (VPN) site-to-site connection between your VPN server and the CSP's RAS Gateway; when this link is established you can connect to your virtual resources in the cloud over the VPN connection.

For more information, see RAS Gateway High Availability.

Clustering RAS Gateway for high availability

RAS Gateway is deployed on a dedicated computer that is running Hyper-V and that is configured with one VM. The VM is then configured as a RAS Gateway.

For high availability of network resources, you can deploy RAS Gateway with failover by using two physical host servers running Hyper-V that are each also running a virtual machine (VM) that is configured as a gateway. The gateway VMs are then configured as a cluster to provide failover protection against network outages and hardware failure.

For example, if your organization is an Enterprise with a private cloud deployment, you might need only two RAS Gateway VMs, each of which is installed on a different computer running Hyper-V. In this scenario, the RAS Gateway VMs are added to a cluster to provide high availability.

In another example, if your organization is a Cloud Service Provider (CSP) with two hundred tenants in your datacenter, you can use eight RAS Gateway VMs, with each pair of clustered RAS Gateway VMs providing routing services for fifty tenants. In this scenario, two computers that are running Hyper-V each have four VMs that are configured as RAS Gateways. You then configure four RAS Gateway VM clusters, each cluster containing one VM from each computer running Hyper-V.

When you deploy RAS Gateway, the host servers running Hyper-V and the VMs that you configure as gateways must be running Windows Server.

RAS Gateway Features

RAS Gateway includes the following capabilities:

- **Site-to-site VPN**. This RAS Gateway feature allows you to connect two networks at different physical locations across the Internet by using a site-to-site VPN connection. If you have a main office and multiple branch offices, you can deploy an edge RAS Gateway at each location and create site-to-site connections to provide network traffic flow between the locations. For CSPs that host many tenants in their datacenter, RAS Gateway provides a multitenant gateway solution that allows your tenants to access and manage their resources over site-to-site VPN connections from remote sites, and that allows network traffic flow between virtual resources in your datacenter and their physical network.

- **Point-to-site VPN**. This RAS Gateway feature allows organization employees or administrators to connect to your organization's network from remote locations. For single tenant deployments of RAS Gateway, remote employees can connect to your organization network by using a VPN connection. This connection allows them to use internal network resources, such as intranet web sites and file servers. For multitenant deployments, tenant network administrators can use point-to-site VPN connections to access virtual network resources at the CSP datacenter.

- **Dynamic routing with Border Gateway Protocol (BGP)**. BGP reduces the need for manual route configuration on routers because it is a dynamic routing protocol, and automatically learns routes between sites that are connected by using site-to-site VPN connections. If your organization has multiple sites that are connected by using BGP-enabled routers such as RAS Gateway, BGP allows the routers to automatically calculate and use valid routes to each other in the event of network disruption or failure. For more information, see RFC 4271.

- **Network Address Translation (NAT)**. Network address translation (NAT) allows you to share a connection to the public Internet through a single interface with a single public IP address. The computers on the private network use private, non-routable addresses. NAT maps the private addresses to the public address. This RAS Gateway feature allows organization employees with single tenant deployments to access Internet resources from behind the gateway. For CSPs, this feature allows applications that are running on tenant VMs to access the Internet. For example, a tenant VM that is configured as a Web server can contact external financial resources to process credit card transactions.

RAS Gateway Deployment Scenarios

The following are the recommended deployment scenarios for RAS Gateway:

- **Enterprise Edge - Single Tenant deployment**. With the single tenant Enterprise deployment, you can connect one physical to multiple other physical locations across the Internet by using the site-to-site VPN feature - and Border Gateway Protocol (BGP) allows you to use dynamic routing. You can also provide remote employees access to your organization network with both point-to-site VPN connections and

DirectAccess connections. (DirectAccess connections are always on, and also provide the advantage that you can easily manage computers that are connected using DirectAccess, because they are connected whenever they are on and Internet-connected.) You can also configure single tenant Enterprise RAS Gateways with NAT, so that computers on your Intranet can easily communicate with the Internet.

- **Cloud Service Provider Edge - Multitenant deployment**. RAS Gateway multitenant deployment for CSPs allows you to offer your tenants all of the features that are available with the Enterprise Edge single tenant deployment. Site-to-site VPN connections between tenant virtual networks in your datacenter and the tenant network locations across the Internet mean that tenants have seamless access to their cloud resources all the time. Point-to-site VPN access for tenants means that tenant administrators can always connect to their virtual networks in your datacenter to manage their resources. BGP provides dynamic routing and keeps tenants connected to their assets even when network problems occur on the Internet or elsewhere. And NAT allows tenant VMs to connect to resources on the Internet, such as credit card processing resources.

RAS Gateway Management Tools

The following are the management tools for RAS Gateway:

- In Windows Server 2016, to deploy an RAS Gateway router, you must use Windows PowerShell commands. For more information, see Remote Access Cmdlets for Windows Server and Windows 11.
- In System Center Virtual Machine Manager (VMM), the RAS Gateway is named Windows Server Gateway. A limited set of Border Gateway Protocol (BGP) configuration options are available in the VMM software interface, including **Local BGP IP Address** and **Autonomous System Numbers (ASN)**, **List of BGP Peer IP Addresses**, and **ASN values**. You can, however, use Remote Access Windows PowerShell BGP commands to configure all other features of Windows Server Gateway. For more information, see Virtual Machine Manager (VMM) and Remote Access Cmdlets for Windows Server and the Windows client.

Related topics

- RAS Gateway High Availability
- GRE Tunneling in Windows Server
- RAS Gateway GRE Tunnel Throughput and Performance

GRE Tunneling in Windows Server 2016

12/9/2022 • 4 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016 provides updates to Generic Routing Encapsulation (GRE) tunnel capability for the RAS Gateway.

GRE is a lightweight tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork. The Microsoft GRE implementation can encapsulate IPv4 and IPv6.

GRE tunnels are useful in many scenarios because:

- They are lightweight and RFC 2890 compliant, making it interoperable with various vendor devices
- You can use Border Gateway Protocol (BGP) for dynamic routing
- You can configure GRE multitenant RAS Gateways for use with Software Defined Networking (SDN)
- You can use System Center Virtual Machine Manager to manage GRE-based RAS Gateways
- You can achieve up to 2.0 Gbps throughput on a 6 core virtual machine that is configured as a GRE RAS Gateway
- A single gateway supports multiple connection modes

GRE based tunnels enable connectivity between tenant virtual networks and external networks. Since the GRE protocol is lightweight and support for GRE is available on most of network devices it becomes an ideal choice for tunneling where the encryption of data is not required.

GRE support in Site to Site (S2S) tunnels solves the problem of forwarding between tenant virtual networks and tenant external networks using a multi-tenant gateway, as described later in this topic.

The GRE tunnel feature is designed to address the following requirements:

- A hosting provider must be able to create virtual networks for forwarding without modifying the physical switch configuration.
- A hosting provider must be able to add subnets to their externally facing networks without modifying the configuration of the physical switches within their infrastructure. The GRE tunnel feature enables or enhances several key scenarios for hosting service providers using Microsoft technologies to implement Software Defined Networking in their service offerings.

The following are some example scenarios:

- Access from tenant virtual networks to tenant physical networks
- High speed connectivity
- Integration with VLAN based isolation
- Access shared resources
- Services of third party devices to tenants

Key scenarios

The following are key scenarios that the GRE tunnel feature addresses.

Access from tenant virtual networks to tenant physical networks

This scenario enables a scalable way to provide access from tenant virtual networks to tenant physical networks located on the hosting service provider premises. A GRE tunnel endpoint is established on the multitenant gateway, the other GRE tunnel endpoint is established on a third-party device on the physical network. Layer-3 traffic is routed between the virtual machines in the virtual network and the third-party device on the physical network.

High speed connectivity

This scenario enables a scalable way to provide high speed connectivity from the tenant on-premises network to their virtual network located in the hosting service provider network. A tenant connects to the service provider network via multiprotocol label switching (MPLS), where a GRE tunnel is established between the hosting service provider's edge router and the multitenant gateway to the tenant's virtual network.

Integration with VLAN based isolation

This scenario allows you to integrate VLAN based isolation with Hyper-V Network Virtualization. A physical network on the hosting provider network contains a load balancer using VLAN-based isolation. A multitenant gateway establishes GRE tunnels between the load balancer on the physical network and the multitenant gateway on the virtual network.

Multiple tunnels can be established between the source and destination, and the GRE key is used to discriminate between the tunnels.

Access shared resources

This scenario allows you to access shared resources on a physical network located on the hosting provider

network.

You may have a shared service located on a server on a physical network located in the hosting provider network that you want to share with multiple tenant virtual networks.

The tenant networks with non-overlapping subnets access the common network over a GRE tunnel. A single tenant gateway routes between the GRE tunnels, thus routing packets to the appropriate tenant networks.

In this scenario, the single tenant gateway can be replaced by third-party hardware appliances.

Services of third party devices to tenants

This scenario can be used to integrate third party devices (such as hardware load balancers) into the tenant virtual network traffic flow. For example, traffic originating from an enterprise site passes through a S2S tunnel to the multitenant gateway. The traffic is routed to the load balancer over a GRE tunnel. The load balancer routes traffic to multiple virtual machines on the enterprise's virtual network. The same thing happens for another tenant with potentially overlapping IP addresses in the virtual networks. The network traffic is isolated on the load balancer using VLANs, and is applicable to all layer 3 devices that support VLANs.

Configuration and deployment

A GRE tunnel is exposed as an additional protocol within a S2S interface. It is implemented in a similar fashion as an IPSec S2S tunnel described in the following Networking Blog: Multi-tenant Site-to-Site (S2S) VPN Gateway with Windows Server 2012 R2

See the following topic for an example that deploys gateways, including GRE tunnel gateways:

Deploy a Software Defined Network infrastructure using scripts

More information

For more information about deploying S2S gateways, see the following topics:

- RAS Gateway
- Border Gateway Protocol (BGP)

- New! Windows Server 2012 R2 RAS Multitenant Gateway Deployment Guide
- Deploy Border Gateway Protocol (BGP) with the RAS Multitenant Gateway

RAS Gateway GRE Tunnel Throughput and Performance

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server (Semi-Annual Channel)

You can use this topic to learn about Remote Access Server (RAS) Gateway Generic Routing Encapsulation (GRE) Tunnel performance on Windows Server, version 1709, in a non-Software Defined Networking (SDN) based test environment.

RAS Gateway is a software router and gateway that you can use in either single tenant mode or multitenant mode. This topic discusses a single tenant mode, high availability configuration with Failover Clustering. The GRE tunnel performance statistics that are presented in this topic are valid for RAS Gateway in both single tenant and multitenant modes.

> **NOTE**
>
> Failover Clustering is a Windows Server feature that enables you to group multiple servers together into a fault-tolerant cluster. For more information, see Failover Clustering

Single tenant mode allows organizations of any size to deploy the gateway as an exterior, or Internet-facing edge virtual private network (VPN) server. In single tenant mode, you can deploy RAS Gateway on a physical server or virtual machine (VM). This topic describes RAS Gateway deployment on two Virtual Machines (VMs) that are configured in a failover cluster.

> **IMPORTANT**
>
> Because GRE tunnels provide encapsulation but not encryption, you should not use RAS Gateway configured with GRE as an Internet edge gateway. To learn about the best uses for RAS Gateway with GRE tunnels, see GRE Tunneling in Windows Server.

GRE is a lightweight tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork. The Microsoft GRE implementation encapsulates both IPv4 and IPv6.

For more information, see the section **RAS Gateway Deployment Scenarios** in the topic RAS Gateway.

In this test scenario, which is depicted in the following illustration, the traffic flow that is measured moves from the Organization Intranet 2 out to the Organization Intranet 1. Tenant Workload VMs send network traffic from Intranet 2 to Intranet 1 by using RAS Gateway.

Test Environment Configuration

This section provides information about the test environment and RAS Gateway configuration.

In the test environment, RAS Gateway VMs are deployed on Hyper-V hosts in a failover cluster for high availability.

Hyper-V Host Configuration

Two Hyper-V hosts are configured to support the test scenario in the following manner.

- Two dual-homed physical computers are configured with Windows Server, version 1709
- The two physical network adapters in each of the two servers are connected to different subnetworks - both of which represent subnets of an Organization Intranet. Both networks and supporting hardware have a capacity of 10 GBps.
- Hyperthreading on the physical servers is disabled. This provides the maximum throughput from the physical NICs.
- The Hyper-V server role is installed on both servers and configured with two External Hyper-V Virtual Switches, one for each physical network adapter.
- Because both servers are connected to the same intranet, the servers can communicate with each other.
- The Hyper-V hosts are configured in a failover cluster over the intranet network.

> **NOTE**
>
> For more information, see Hyper-V Virtual Switch.

VM Configuration

Two VMs are configured to support the test scenario in the following manner.

- On each server a VM is installed that is running Windows Server, version 1709. Each VM is configured with 10 Cores and 8 GB RAM.
- Each VM is also configured with two virtual network adapters. One virtual network adapter is connected to the Intranet 1 virtual switch, and the other virtual network adapter is connected to the Intranet 2 virtual switch.
- Each VM has RAS Gateway installed and configured as a GRE-based VPN server.
- The gateway VMs are configured in a failover cluster. When clustered, one VM is active and the other VM is passive.

Workload Hyper-V Hosts and VMs

For this test, two Workload Hyper-V hosts are installed on the intranet, and each host has one VM installed. If you are duplicating this test in your own test environment, you can install as many workload servers and VMs as is appropriate for your purposes.

- Workload Hyper-V hosts have one physical network adapter installed that is connected to the Organization Intranet.
- In Hyper-V Virtual Switch, one virtual switch is created on each host. The switch is External and is bound to the one network adapter connected to the intranet.
- The workload VMs are configured with 2 GB RAM and 2 Cores.
- The Workload VMs each have one virtual network adapter that is connected to the intranet virtual switch.

Traffic Generator Tool

The traffic generator tool that is used in this test is the ctsTraffic tool. The Git repository for this tool is located at https://github.com/Microsoft/ctsTraffic.

RAS Gateway Performance

The illustrations in this section depict Task Manager displays of GRE tunnel throughput with multiple TCP connections.

You can achieve up to 2.0 Gbps throughput on multi-core VMs that are configured as GRE RAS Gateways.

GRE Tunnel Performance with Multiple TCP Sessions

With multiple TCP sessions, the CPU utilization reaches 100% and the maximum throughput on the GRE tunnel is 2.0 Gbps.

The following illustration depicts CPU Utilization on both of the RAS Gateway VMs. The active VM, RAS Gateway VM #1, is on the left, while the passive VM, RAS Gateway VM #2, is on the right.

The following illustration depicts Ethernet network throughput on the RAS Gateway VMs. The active VM, RAS Gateway VM #1, is on the left, while the passive VM, RAS Gateway VM #2, is on the right.

GRE Tunnel Performance with One TCP Connection

With the test configuration changed from multiple TCP sessions to a single TCP session, only one CPU core reaches maximum capacity on the RAS Gateway VMs.

The maximum throughput on the GRE tunnel is between 400-500 Mbps.

The following illustration depicts CPU Utilization on both of the RAS Gateway VMs. The active VM, RAS Gateway VM #1, is on the left, while the passive VM, RAS Gateway VM #2, is on the right.

The following illustration depicts Ethernet network throughput on the RAS Gateway VMs. The active VM, RAS Gateway VM #1, is on the left, while the passive VM, RAS Gateway VM #2, is on the right.

For more information about RAS Gateway performance, see HNV Gateway Performance Tuning in Software Defined Networks.

Border Gateway Protocol (BGP)

12/9/2022 • 11 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

You can use this topic to gain an understanding of Border Gateway Protocol (BGP), including BGP supported deployment topologies and BGP features and capabilities.

> **NOTE**
>
> In addition to this topic, the following BGP documentation is available.
>
> - BGP Windows PowerShell Command Reference

This topic contains the following sections.

- BGP Supported Deployment Topologies
- BGP Features

When configured on a Windows Server 2016 Remote Access Service (RAS) Gateway in multitenant mode, Border Gateway Protocol (BGP) provides you with the ability to manage the routing of network traffic between your tenants' VM networks and their remote sites. You can also use BGP for single tenant RAS Gateway deployments, and when you deploy Remote Access as a Local Area Network (LAN) router.

BGP reduces the need for manual route configuration on routers because it is a dynamic routing protocol, and automatically learns routes between sites that are connected by using site-to-site VPN connections.

To use BGP routing, you must install the **Remote Access Service (RAS)** and/or the **Routing** role service of the Remote Access server role on a computer or virtual machine (VM) - the type of system you use depends on whether or not you have a multitenant deployment:

- For a multitenant deployment, it is recommended that you install the RAS Gateway on one or more VMs. Use of multiple VMs provides high availability. The RAS Gateway is capable of handling multiple connections from multiple tenants, and consists of a Hyper-V host and a VM that is actually configured as the gateway. This gateway is configured with site-to-site VPN connections as a multitenant BGP router to exchange tenant and Cloud Service Provider (CSP) subnet routes.
- For a single tenant edge gateway deployment or a LAN router deployment, you can install the RAS Gateway on either a physical computer or a VM.

> **IMPORTANT**
>
> When you install a RAS Gateway, you must specify whether BGP is enabled for each tenant by using the **Enable-RemoteAccessRoutingDomain** Windows PowerShell command with the **Type** parameter value of **All**. To install Remote Access as a BGP-enabled LAN router without multitenant capabilities, you can use the command **Install-RemoteAccess -VpnType RoutingOnly**.
>
> The following example code illustrates how to install RAS in Multitenancy mode with all RAS features (point-to-site VPN, site-to-site VPN, and BGP routing) enabled for two tenants, Contoso and Fabrikam.

```
$Contoso_RoutingDomain = "ContosoTenant"
$Fabrikam_RoutingDomain = "FabrikamTenant"

Install-RemoteAccess -MultiTenancy

Enable-RemoteAccessRoutingDomain -Name $Contoso_RoutingDomain -Type All -PassThru
Enable-RemoteAccessRoutingDomain -Name $Fabrikam_RoutingDomain -Type All -PassThru
```

BGP Supported Deployment Topologies

Listed below are the supported deployment topologies where Enterprise sites are connected to a Cloud Service Provider (CSP) datacenter.

In all scenarios, the CSP gateway is a Windows Server 2016 RAS Gateway at the edge. The RAS Gateway, which is capable of handling multiple connections from multiple tenants, consists of a Hyper-V host and a VM that is actually configured as the gateway. This edge gateway is configured with site-to-site VPN connections as a multitenant BGP router to exchange Enterprise and CSP subnet routes.

Tenants connect to their resources at the CSP datacenter by using a site-to-site (S2S) VPN connection. In addition, the BGP routing protocol is deployed for dynamic routing information exchange between the Enterprise and CSP gateways.

The following deployment topologies are supported.

- RAS VPN Site-to-Site Gateway with BGP at Enterprise site edge
- Third party Gateway with BGP at Enterprise site edge
- Multiple Enterprise sites with third party gateways
- Separate termination points for BGP and VPN

The following sections contain additional information on each supported BGP topology.

RAS VPN Site-to-Site Gateway with BGP at Enterprise site edge

This topology depicts an Enterprise site connected to a CSP. The Enterprise routing topology includes an internal router, a Windows Server 2016 RAS Gateway configured for VPN site-to-site connections with the CSP, and an edge firewall device. The RAS Gateway terminates the S2S VPN and BGP connections.

Both sites are connected using External Border Gateway Protocol (eBGP), which can transmit information between BGP-enabled routers in separate autonomous systems (AS). This requires that both the Enterprise and the CSP have distinct Autonomous System Numbers (ASN), which is a parameter that is integral to the BGP protocol.

In this scenario, BGP works in the following way.

- The Enterprise site edge device learns the virtualized subnet routes (10.2.1.0/24) hosted in the cloud by using BGP. This device also advertises the on-premises subnet routes (10.1.1.0/24) to the CSP RAS Multitenant Gateway.

- The customer edge router learns on-premises internal routes through one of the following mechanisms:
  - The edge device runs BGP with an internal router and learns internal routes (in this example, 10.1.1.0/24). Meanwhile, the internal router learns external routes (such as 10.2.1.0/24) from the edge device, and the internal router must distribute these routes to other on-premises routers using an Interior Gateway Protocol (IGP) such as Open Shortest Path First (OSPF) or Routing Information Protocol (RIP).
  - The edge device can be configured with static routes or interfaces to select routes for advertisement by using BGP. The edge device also distributes the external routes to other on-premises routers using an IGP.

Third party Gateway with BGP at Enterprise site edge

This topology depicts an Enterprise site using a third party edge router to connect to a CSP. The edge router also serves as a site-to-site VPN gateway.

The Enterprise edge router learns on-premises internal routes through one of the following mechanisms:

- The edge device runs BGP with an internal router and learns internal routes (in this case, 10.1.1.0/24)
- The edge device implements an Interior Gateway Protocol (IGP) and participates directly in internal routing.

Multiple Enterprise sites connecting to CSP cloud datacenter

This topology depicts multiple Enterprise sites that use third party gateways to connect to a CSP. The third party edge devices serve as site-to-site VPN gateways and as BGP routers.

The customer edge routers learn on-premises internal routes through one of the following mechanisms:

- The edge device runs BGP with an internal router and learns internal routes (in this case, 10.1.1.0/24)
- The edge device implements an Interior Gateway Protocol (IGP) and participates directly in internal routing.

Each Enterprise site learns the routes from the other site over the direct eBGP connectivity.

Each Enterprise site learns the hosted network routes directly and by using the other Enterprise site, but selects

the best route based on the cost of the route.

If the BGP router at Enterprise Site 1 cannot connect with the Enterprise Site 2 BGP router because connectivity has failed, the Site 1 BGP router dynamically begins to learn the routes to Enterprise Site 2 network from the CSP BGP Router, and the traffic is seamlessly rerouted from Site 1 to Site 2 via the Windows Server BGP Router at the CSP.

Separate termination points for BGP and VPN

This topology depicts an Enterprise that uses two different routers as the BGP and site-to-site VPN endpoints. Site-to-site VPN is terminated on the Windows Server 2016 RAS Gateway, while BGP is terminated on an internal router. At the CSP side of the connections, the CSP terminates both the VPN and BGP connections with the RAS Gateway. With this configuration, the internal third party router hardware must support redistribution of IGP routes to BGP, as well as redistributing BGP routes to IGP.

The internal router learns Enterprise routes through one of the following mechanisms:

- BGP
- An Interior Gateway Protocol (IGP) such as OSPF or RIP.
- Static route configuration

When any IGP is used at the Enterprise site, the internal router must redistribute IGP routes into BGP - as well as redistribute BGP routes into IGP routes - for maintaining the subnet connectivity between CSP virtual networks and local Enterprise subnets.

With this deployment, the Enterprise RAS Gateway has a site-to-site VPN connection with the CSP RAS Gateway, which provides the Enterprise RAS Gateway with the routes to the CSP gateway. The Enterprise internal router then learns this route to the CSP gateway by using iBGP with the Enterprise RAS Gateway. Because of this, the Enterprise internal router is then able to establish a peering session with the CSP RAS Gateway BGP Router.

From this point forward, the Enterprise internal router and the CSP RAS Gateway exchange routing information. And the Enterprise RAS BGP router learns the CSP routes and Enterprise routes to physically route packets between the networks.

BGP Features

Following are the features of the RAS Gateway BGP Router.

BGP Routing as a role service of Remote Access. You can now install the **Routing** role service of the Remote Access server role without installing the **Remote Access Service (RAS)** role service when you want to use Remote Access as a BGP LAN router. This reduces the BGP router memory footprint and only installs the components required for dynamic BGP routing. The Routing role service is useful when only a BGP Router VM is required, and you don't require use of DirectAccess or VPN. In addition, using Remote Access as a LAN router with BGP provides you with the dynamic routing advantages of BGP on your internal network.

BGP Statistics (Message counters, Route counters). The BGP Router supports displaying the message and route statistics, if required, by using the **Get-BgpStatistics** Windows PowerShell command.

Equal Cost Multi Path Routing (ECMP) support. The BGP Router supports ECMP and can have more than

one equal cost routes plumbed into the BGP routing table and stack. The BGP router selection of the route for transmitting data packets is random with ECMP enabled.

HoldTime configuration. The BGP Router supports configuration of the HoldTimer value according to your network requirements. This timer can be dynamically changed to accommodate interoperability with third party devices or to maintain a specific maximum time for BGP peering session timeout.

Internal BGP and External BGP support. The BGP router supports both iBGP and eBGP peering. To configure either, you must ensure that the appropriate ASNs are assigned to the local and remote BGP Routers. All four BGP deployment topologies employ the use of eBGP peering, and the fourth topology uses iBGP peering as well.

Interoperability with 3rd party solutions. The BGP Router is based on the latest BGP version 4 specification, and has been tested for interoperability with most of the major third party BGP routing devices. For more information, see Request for Comments (RFC) 4271, A Border Gateway Protocol 4 (BGP-4).

IPv4 and IPv6 transport peering support. The BGP Router supports both IPv4 and IPv6 peering. However, you must configure the BGP Identifier as the IPv4 address of the BGP Router. For all of the BGP router deployment topologies, either of the two peering types (IPV4 / IPv6) can be used.

IPv4 and IPv6 unicast route learning and advertisement capability (Multiprotocol Network Layer Reachability Information [NLRI]). No matter what transport you use, the BGP Router can exchange IPv4 and IPv6 routes if the appropriate capability is announced by other BGP routers while establishing the session. To configure IPv6 routing, parameter IPv6Routing must be enabled, and a Local Global IPv6 address must be configured at the router level.

Mixed mode and Passive mode peering. You can configure BGP peering sessions in either mixed mode - where the BGP router acts as both initiator and responder - or passive mode, where the BGP router does not initiate peering, but does respond to incoming requests. Mixed mode is the default, and is recommended for BGP peering. This is true unless you want to use passive mode for debugging or diagnostic purposes. For all of the BGP router deployment topologies, mixed mode peering is required to enable automatic restarts in case of failure events.

Route Attribute rewrite capability. You can add, modify, or remove the following attributes from the BGP router ingress and egress route advertisements by using the BGP Routing policies Next-Hop, MED, Local-Pref, and Community.

Route filtering. The BGP router supports filtering ingress or egress route advertisements based on multiple route attributes such as Prefix, ASN-Range, Community, and Next-Hop.

Route-Reflector (RR) and RR client. The BGP Router can act as a Route-Reflector and an RR client. This is useful in complex topologies where RR can simplify the network by forming RR Clusters.

Route-Refresh support. The BGP Router supports Route-Refresh and advertises this capability on peering by default. It is capable of sending a fresh set of route updates when requested by a peer via route-refresh message, as well as sending a Route-Refresh to update its Routing table in the events like Routing policy changes for a peer. This enables the scenario of changing or updating the BGP Routing policies in Windows Server 2016 without needing to restart the peering.

Static route configuration support. You can configure static routes or interfaces on the BGP Router by using the **Add-BgpCustomRoute** Windows PowerShell command. The static routes that you configure can be the prefixes or the name of the interfaces from which the routes must be chosen. However, only the routes with resolvable next-hops are plumbed into the BGP routing tables and advertised to peers.

Transit routing support. The BGP Router supports transit routing for iBGP to iBGP connections, iBGP to eBGP connections as well as eBGP to eBGP connections.

Route Flap Dampening. Route Flap Dampening to BGP Routing in Windows Server 2016 provides support for Route flap dampening. For example, when a route is constantly being advertised and withdrawn, making the

routing table unstable, you can configure the BGP Router to assign a dampening weight to the route and monitor it for flaps - and accordingly suppress or un-suppress it as required. This helps with maintaining a stable routing table and less processing by the BGP Router.

Route Aggregation. Route Aggregation to the BGP Router provides you with the ability to configure Aggregate Routes and to replace the more granular route advertisements with summary or aggregate routes to peers. This results in a fewer number of route advertisement messages transmitted on the network.

> **NOTE**
>
> In System Center, the RAS Gateway is named Windows Server Gateway.

Web Application Proxy in Windows Server

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This content is relevant for the on-premises version of Web Application Proxy. To enable secure access to on-premises applications over the cloud, see the Azure AD Application Proxy content.

The content in this section describes what's new and changed in the Web Application Proxy for Windows Server. The new features and changes listed here are the ones most likely to have the greatest impact as you work with the Preview.

Web Application Proxy features

- Preauthentication for HTTP Basic application publishing

  HTTP Basic is the authorization protocol used by many protocols, including ActiveSync, to connect rich clients, including smartphones, with your Exchange mailbox. Web Application Proxy traditionally interacts with AD FS using redirections which is not supported on ActiveSync clients. This new version of Web Application Proxy provides support to publish an app using HTTP basic by enabling the HTTP app to receive a non-claims relying party trust for the application to the Federation Service.

  For more information on HTTP basic publishing, see Publishing Applications using AD FS Preauthentication

- Wildcard domain publishing of applications

  To support scenarios such as SharePoint 2013, the external URL for the application can now include a wildcard to enable you to publish multiple applications from within a specific domain, for example, https://*.sp-apps.contoso.com. This will simplify publishing of SharePoint apps.

- HTTP to HTTPS redirection

  In order to make sure your users can access your app, even if they neglect to type HTTPS in the URL, Web Application Proxy now supports HTTP to HTTPS redirection.

- HTTP Publishing

  It is now possible to publish HTTP applications using pass-through preauthentication

- Publishing of Remote Desktop Gateway apps

  For more information on RDG in Web Application Proxy, see Publishing Applications with SharePoint, Exchange and RDG

- New debug log for better troubleshooting and improved service log for complete audit trail and improved error handling

  For more information on troubleshooting, see Troubleshooting Web Application Proxy

- Administrator Console UI improvements

- Propagation of client IP address to backend applications

See Also

- What's New in Windows Server
- Publishing Applications using AD FS Preauthentication
- Troubleshooting Web Application Proxy

Troubleshoot Always On VPN

12/9/2022 • 11 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10

If your Always On VPN setup is failing to connect clients to your internal network, the cause is likely an invalid VPN certificate, incorrect NPS policies, or issues with the client deployment scripts or in Routing and Remote Access. The first step in troubleshooting and testing your VPN connection is understanding the core components of the Always On VPN infrastructure.

You can troubleshoot connection issues in several ways. For client-side issues and general troubleshooting, the application logs on client computers are invaluable. For authentication-specific issues, the NPS log on the NPS server can help you determine the source of the problem.

Error codes

Error code: 800

- **Error description.** The remote connection was not made because the attempted VPN tunnels failed. The VPN server might be unreachable. If this connection is attempting to use an L2TP/IPsec tunnel, the security parameters required for IPsec negotiation might not be configured properly.
- **Possible cause.** This error occurs when the VPN tunnel type is **Automatic** and the connection attempt fails for all VPN tunnels.
- **Possible solutions:**
  - If you know which tunnel to use for your deployment, set the type of VPN to that particular tunnel type on the VPN client side.
  - By making a VPN connection with a particular tunnel type, your connection will still fail, but it will result in a more tunnel-specific error (for example, "GRE blocked for PPTP").
  - This error also occurs when the VPN server cannot be reached or the tunnel connection fails.
- **Make sure:**
  - IKE ports (UDP ports 500 and 4500) aren't blocked.
  - The correct certificates for IKE are present on both the client and the server.

Error code: 809

- **Error description.** The network connection between your computer and the VPN server could not be established because the remote server is not responding. This could be because one of the network devices (e.g., firewalls, NAT, routers) between your computer and the remote server is not configured to allow VPN connections. Please contact your administrator or your service provider to determine which device may be causing the problem.
- **Possible cause.** This error is caused by blocked UDP 500 or 4500 ports on the VPN server or the firewall.
- **Possible solution.** Ensure that UDP ports 500 and 4500 are allowed through all firewalls between the client and the RRAS server.

Error code: 812

- **Error description.** Can't connect to Always On VPN. The connection was prevented because of a policy configured on your RAS/VPN server. Specifically, the authentication method the server used to verify your user name and password may not match the authentication method configured in your connection profile. Please contact the administrator of the RAS server and notify him or her of this error.
- **Possible causes:**
  - The typical cause of this error is that the NPS has specified an authentication condition that the client cannot meet. For example, the NPS may specify the use of a certificate to secure the PEAP connection, but the client is attempting to use EAP-MSCHAPv2.
  - Event log 20276 is logged to the event viewer when the RRAS-based VPN server authentication protocol setting doesn't match that of the VPN client computer.
- **Possible solution.** Ensure that your client configuration matches the conditions that are specified on the NPS server.

Error code: 13806

- **Error description.** IKE failed to find a valid machine certificate. Contact your network security administrator about installing a valid certificate in the appropriate certificate store.
- **Possible cause.** This error typically occurs when no machine certificate or root machine certificate is present on the VPN server.
- **Possible solution.** Ensure that the certificates outlined in this deployment are installed on both the client computer and the VPN server.

Error code: 13801

- **Error description.** IKE authentication credentials are unacceptable.
- **Possible causes.** This error typically occurs in one of the following cases:
  - The machine certificate used for IKEv2 validation on the RAS server doesn't have **Server Authentication** under **Enhanced Key Usage**.
  - The machine certificate on the RAS server has expired.
  - The root certificate to validate the RAS server certificate isn't present on the client computer.
  - The VPN server name used on the client computer doesn't match the **subjectName** of the server certificate.
- **Possible solution.** Verify that the server certificate includes **Server Authentication** under **Enhanced Key Usage**. Verify that the server certificate is still valid. Verify that the CA used is listed under **Trusted Root Certification Authorities** on the RRAS server. Verify that the VPN client connects by using the FQDN of the VPN server as presented on the VPN server's certificate.

Error code: 0x80070040

- **Error description.** The server certificate does not have **Server Authentication** as one of its certificate usage entries.
- **Possible cause.** This error may occur if no server authentication certificate is installed on the RAS server.
- **Possible solution.** Make sure that the machine certificate the RAS server uses for **IKEv2** has **Server Authentication** as one of the certificate usage entries.

Error code: 0x800B0109

Generally, the VPN client machine is joined to the Active Directory–based domain. If you use domain credentials to log on to the VPN server, the certificate is automatically installed in the Trusted Root Certification Authorities store. However, if the computer is not joined to the domain or if you use an alternative certificate chain, you may experience this issue.

- **Error description.** A certificate chain processed but terminated in a root certificate that the trust provider does not trust.
- **Possible cause.** This error may occur if the appropriate trusted root CA certificate is not installed in the Trusted Root Certification Authorities store on the client computer.
- **Possible solution.** Make sure that the root certificate is installed on the client computer in the Trusted Root Certification Authorities store.

Logs

Application logs

The application logs on client computers record most of the higher-level details of VPN connection events.

Look for events from source RasClient. All error messages return the error code at the end of the message. Some of the more common error codes are detailed below, but a full list is available in Routing and Remote Access Error Codes.

NPS logs

NPS creates and stores the NPS accounting logs. By default, these are stored in %SYSTEMROOT%\System32\Logfiles\ in a file named IN*XXXX*.txt, where *XXXX* is the date the file was created.

By default, these logs are in comma-separated values format, but they don't include a heading row. The heading row is:

```
ComputerName,ServiceName,Record-Date,Record-Time,Packet-Type,User-Name,Fully-Qualified-Distinguished-
Name,Called-Station-ID,Calling-Station-ID,Callback-Number,Framed-IP-Address,NAS-Identifier,NAS-IP-
Address,NAS-Port,Client-Vendor,Client-IP-Address,Client-Friendly-Name,Event-Timestamp,Port-Limit,NAS-Port-
Type,Connect-Info,Framed-Protocol,Service-Type,Authentication-Type,Policy-Name,Reason-Code,Class,Session-
Timeout,Idle-Timeout,Termination-Action,EAP-Friendly-Name,Acct-Status-Type,Acct-Delay-Time,Acct-Input-
Octets,Acct-Output-Octets,Acct-Session-Id,Acct-Authentic,Acct-Session-Time,Acct-Input-Packets,Acct-Output-
Packets,Acct-Terminate-Cause,Acct-Multi-Ssn-ID,Acct-Link-Count,Acct-Interim-Interval,Tunnel-Type,Tunnel-
Medium-Type,Tunnel-Client-Endpt,Tunnel-Server-Endpt,Acct-Tunnel-Conn,Tunnel-Pvt-Group-ID,Tunnel-Assignment-
ID,Tunnel-Preference,MS-Acct-Auth-Type,MS-Acct-EAP-Type,MS-RAS-Version,MS-RAS-Vendor,MS-CHAP-Error,MS-CHAP-
Domain,MS-MPPE-Encryption-Types,MS-MPPE-Encryption-Policy,Proxy-Policy-Name,Provider-Type,Provider-
Name,Remote-Server-Address,MS-RAS-Client-Name,MS-RAS-Client-Version
```

If you paste this heading row as the first line of the log file, then import the file into Microsoft Excel, the columns will be properly labeled.

The NPS logs can be helpful in diagnosing policy-related issues. For more information about NPS logs, see Interpret NPS Database Format Log Files.

VPN_Profile.ps1 script issues

The most common issues when manually running the VPN_ Profile.ps1 script include:

- Do you use a remote connection tool? Make sure not to use RDP or another remote connection method as it messes with user login detection.
- Is the user an administrator of that local machine? Make sure that while running the VPN_Profile.ps1 script that the user has administrator privileges.

- Do you have additional PowerShell security features enabled? Make sure that the PowerShell execution policy is not blocking the script. You might consider turning off Constrained Language mode, if enabled, before running the script. You can activate Constrained Language mode after the script completes successfully.

Always On VPN client connection issues

A small misconfiguration can cause the client connection to fail and can be challenging to find the cause. An Always On VPN client goes through several steps before establishing a connection. When troubleshooting client connection issues, go through the process of elimination with the following:

1. Is the template machine externally connected? A **whatismyip** scan should show a public IP address that does not belong to you.
2. Can you resolve the Remote Access/VPN server name to an IP address? In **Control Panel** > **Network** and **Internet** > **Network Connections**, open the properties for your VPN Profile. The value in the **General** tab should be publicly resolvable through DNS.
3. Can you access the VPN server from an external network? Consider opening Internet Control Message Protocol (ICMP) to the external interface and pinging the name from the remote client. After a ping is successful, you can remove the ICMP allow rule.
4. Do you have the internal and external NICs on the VPN server configured correctly? Are they in different subnets? Does the external NIC connect to the correct interface on your firewall?
5. Are UDP 500 and 4500 ports open from the client to the VPN server's external interface? Check the client firewall, server firewall, and any hardware firewalls. IPSEC uses UDP port 500, so make sure that you do not have IPEC disabled or blocked anywhere.
6. Is certificate validation failing? Verify the NPS server has a Server Authentication certificate that can service IKE requests. Make sure that you have the correct VPN server IP specified as an NPS client. Make sure that you are authenticating with PEAP, and the Protected EAP properties should only allow authentication with a certificate. You can check the NPS event logs for authentication failures. For more details, see Install and Configure the NPS Server
7. Are you connecting but do not have Internet/local network access? Check your DHCP/VPN server IP pools for configuration issues.
8. Are you connecting and have a valid internal IP but do not have access to local resources? Verify that clients know how to get to those resources. You can use the VPN server to route requests.

Azure AD Conditional Access connection issues

Oops - You can't get to this yet

- **Error description.** When the Conditional Access policy is not satisfied, blocking the VPN connection, but connects after the user selects **X** to close the message. Selecting **OK** causes another authentication attempt, which ends in another "Oops" message. These events are recorded in the AAD Operational Event log of the client.
- **Possible cause**
  - The user has a valid client authentication certificate in their Personal Certificate store that was not issued by Azure AD.
  - The VPN profile <TLSExtensions> section is either missing or does not contain the **<EKUName>AAD Conditional Access</EKUName> <EKUOID>1.3.6.1.4.1.311.87</EKUOID><EKUName>AAD Conditional**

Access</EKUName><EKUOID>1.3.6.1.4.1.311.87</EKUOID> entries. The <EKUName> and <EKUOID> entries tell the VPN client which certificate to retrieve from the user's certificate store when passing the certificate to the VPN server. Without this, the VPN client uses whatever valid Client Authentication certificate is in the user's certificate store and authentication succeeds.

- The RADIUS server (NPS) has not been configured to only accept client certificates that contain the **AAD Conditional Access** OID.

- **Possible solution.** To escape this loop, do the following:

  1. In Windows PowerShell, run the **Get-WmiObject** cmdlet to dump the VPN profile configuration.
  2. Verify that the **<TLSExtensions>**, **<EKUName>**, and **<EKUOID>** sections exist and shows the correct name and OID.

```
PS C:\> Get-WmiObject -Class MDM_VPNv2_01 -Namespace root\cimv2\mdm\dmmap

__GENUS                 : 2
__CLASS                 : MDM_VPNv2_01
__SUPERCLASS            :
__DYNASTY               : MDM_VPNv2_01
__RELPATH               : MDM_VPNv2_01.InstanceID="AlwaysOnVPN",ParentID="./Vendor/MSFT/VPNv2"
__PROPERTY_COUNT        : 10
__DERIVATION            : {}
__SERVER                : DERS2
__NAMESPACE             : root\cimv2\mdm\dmmap
__PATH                  :
\\DERS2\root\cimv2\mdm\dmmap:MDM_VPNv2_01.InstanceID="AlwaysOnVPN",ParentID="./Vendor/MSFT/VP
                            Nv2"
AlwaysOn                :
ByPassForLocal          :
DnsSuffix               :
EdpModeId               :
InstanceID              : AlwaysOnVPN
LockDown                :
ParentID                : ./Vendor/MSFT/VPNv2
ProfileXML              : <VPNProfile><RememberCredentials>false</RememberCredentials>
<DeviceCompliance><Enabled>true</
                            Enabled><Sso><Enabled>true</Enabled></Sso></DeviceCompliance>
<NativeProfile><Servers>derras2.
                            corp.deverett.info;derras2.corp.deverett.info</Servers>
<RoutingPolicyType>ForceTunnel</Routin
                            gPolicyType><NativeProtocolType>Ikev2</NativeProtocolType>
<Authentication><UserMethod>Eap</Us
                            erMethod><MachineMethod>Eap</MachineMethod><Eap><Configuration>
<EapHostConfig
                            xmlns="https://www.microsoft.com/provisioning/EapHostConfig">
<EapMethod><Type
                            xmlns="https://www.microsoft.com/provisioning/EapCommon">25</Type>
<VendorId

xmlns="https://www.microsoft.com/provisioning/EapCommon">0</VendorId><VendorType

xmlns="https://www.microsoft.com/provisioning/EapCommon">0</VendorType><AuthorId

xmlns="https://www.microsoft.com/provisioning/EapCommon">0</AuthorId></EapMethod><Config
                            xmlns="https://www.microsoft.com/provisioning/EapHostConfig"><Eap
xmlns="https://www.microsoft.
                            com/provisioning/BaseEapConnectionPropertiesV1"><Type>25</Type>
<EapType xmlns="https://www.mic
                            rosoft.com/provisioning/MsPeapConnectionPropertiesV1">
<ServerValidation><DisableUserPromptFor
                            ServerValidation>true</DisableUserPromptForServerValidation>
<ServerNames></ServerNames></Serv
                            erValidation><FastReconnect>true</FastReconnect>
<InnerEapOptional>false</InnerEapOptional><Ea
```

```
                            p
xmlns="https://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1"><Type>13</Type>
                            <EapType
xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV1"><Credenti
                            alsSource><CertificateStore>
<SimpleCertSelection>true</SimpleCertSelection></CertificateStore
                            ></CredentialsSource><ServerValidation>
<DisableUserPromptForServerValidation>true</DisableUse
                            rPromptForServerValidation><ServerNames></ServerNames>
<TrustedRootCA>5a 89 fe cb 5b 49 a7 0b
                            1a 52 63 b7 35 ee d7 1c c2 68 be 4b </TrustedRootCA>
</ServerValidation><DifferentUsername>fal
                            se</DifferentUsername><PerformServerValidation
xmlns="https://www.microsoft.com/provisioning/E
                            apTlsConnectionPropertiesV2">true</PerformServerValidation>
<AcceptServerName xmlns="https://ww

w.microsoft.com/provisioning/EapTlsConnectionPropertiesV2">false</AcceptServerName><TLSExtens
                            ions

xmlns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2"><FilteringInfo xml

ns="https://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV3"><EKUMapping><EKUMap><
                            EKUName>AAD Conditional
                            Access</EKUName><EKUOID>1.3.6.1.4.1.311.87</EKUOID></EKUMap>
</EKUMapping><ClientAuthEKUList
                            Enabled="true"><EKUMapInList><EKUName>AAD Conditional
Access</EKUName></EKUMapInList></Client
                            AuthEKUList></FilteringInfo></TLSExtensions></EapType></Eap>
<EnableQuarantineChecks>false</En
                            ableQuarantineChecks>
<RequireCryptoBinding>false</RequireCryptoBinding><PeapExtensions><Perfo
                            rmServerValidation
xmlns="https://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV2"
                            >false</PerformServerValidation><AcceptServerName
xmlns="https://www.microsoft.com/provisionin
                            g/MsPeapConnectionPropertiesV2">false</AcceptServerName>
</PeapExtensions></EapType></Eap></Co
                            nfig></EapHostConfig></Configuration></Eap></Authentication>
</NativeProfile></VPNProfile>
RememberCredentials     : False
TrustedNetworkDetection :
PSComputerName          : DERS2
```

3. To determine if there are valid certificates in the user's certificate store, run the **Certutil** command:

```
C:\>certutil -store -user My

 My "Personal"
 ================ Certificate 0 ================
 Serial Number: 32000000265259d0069fa6f205000000000026
 Issuer: CN=corp-DEDC0-CA, DC=corp, DC=deverett, DC=info
  NotBefore: 12/8/2017 8:07 PM
  NotAfter: 12/8/2018 8:07 PM
 Subject: E=winfed@deverett.info, CN=WinFed, OU=Users, OU=Corp, DC=corp, DC=deverett, DC=info
 Certificate Template Name (Certificate Type): User
 Non-root Certificate
 Template: User
 Cert Hash(sha1): a50337ab015d5612b7dc4c1e759d201e74cc2a93
   Key Container = a890fd7fbbfc072f8fe045e680c501cf_5834bfa9-1c4a-44a8-a128-c2267f712336
   Simple container name: te-User-c7bcc4bd-0498-4411-af44-da2257f54387
   Provider = Microsoft Enhanced Cryptographic Provider v1.0
 Encryption test passed

 ================ Certificate 1 ================
 Serial Number: 367fbdd7e6e4103dec9b91f93959ac56
 Issuer: CN=Microsoft VPN root CA gen 1
  NotBefore: 12/8/2017 6:24 PM
  NotAfter: 12/8/2017 7:29 PM
 Subject: CN=WinFed@deverett.info
 Non-root Certificate
 Cert Hash(sha1): 37378a1b06dcef1b4d4753f7d21e4f20b18fbfec
   Key Container = 31685cae-af6f-48fb-ac37-845c69b4c097
   Unique container name: bf4097e20d4480b8d6ebc139c9360f02_5834bfa9-1c4a-44a8-a128-
c2267f712336
   Provider = Microsoft Software Key Storage Provider
 Private key is NOT exportable
 Encryption test passed
```

> **NOTE**
>
> If a certificate from Issuer **CN=Microsoft VPN root CA gen 1** is present in the user's Personal store, but the user gained access by selecting **X** to close the Oops message, collect CAPI2 event logs to verify the certificate used to authenticate was a valid Client Authentication certificate that was not issued from the Microsoft VPN root CA.

4. If a valid Client Authentication certificate exists in the user's Personal store, the connection fails (as it should) after the user selects the **X** and if the **<TLSExtensions>**, **<EKUName>**, and **<EKUOID>** sections exist and contain the correct information.

   An error message that says "A certificate could not be found that can be used with the Extensible Authenticate Protocol" appears.

Unable to delete the certificate from the VPN connectivity blade

- **Error description.** Certificates on the VPN connectivity blade cannot be deleted.
- **Possible cause.** The certificate is set to **Primary**.
- **Possible solution.**
  1. In the VPN connectivity blade, select the certificate.
  2. Under **Primary**, select **No**, then select **Save**.
  3. In the VPN connectivity blade, select the certificate again.
  4. Select **Delete**.

Troubleshooting DirectAccess

12/9/2022 • 4 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Follow these steps to troubleshoot Remote Access (DirectAccess) issues.

ISSUE	RESOLUTION

Remote Access management console is unable to show the DirectAccess configuration	**To restore missing configuration information**
	- If you are troubleshooting a multisite deployment, ensure that the domain controller closest to the entry point is available.
	- Use the **Get-DAEntrypointDC** cmdlet to retrieve the name of the domain controller closest to the entry point. If the domain controller is not running, use the **Set-DAEntryPointDC** cmdlet to point to another domain controller.
	- Run **gpresult** from an elevated command prompt on the server to ensure the server is getting the DirectAccess Group Policy Objects.
	- Enable user interface (UI) logging.
	- Use the following command to start Windows PowerShell logging:
	`logman create trace ETWTrace -ow -o c:\ETWTrace.etl -p {AAD4C46D-56DE-4F98-BDA2-B5EAEBDD2B04} 0xffffffffffffffff 0xff -nb 16 16 -bs 1024 -mode 0x2 -max 2048 -ets`
	`logman update trace ETWTrace -p {62DFF3DA-7513-4FCA-BC73-25B111FBB1DB} 0xffffffffffffffff 0xff -ets`
	
	<repro>- Close and reopen the user interface.
	- Disable Windows Powershell logging. Collect the Event Trace Log files. Also, collect all the logs from the **%windir%/tracing** folder.

ISSUE	RESOLUTION

Applying the DirectAccess configuration fails	**To refresh the DirectAccess configuration**
	- If you are troubleshooting a multisite deployment, ensure that the domain controller closest to the entry point is available.
	- Use the **Get-DAEntrypointDC** cmdlet to retrieve the name of the domain controller closest to the entry point. If the domain controller is not running, use the **Set-DAEntryPointDC** cmdlet to point to another domain controller.
	- Use the following command to start Windows Powershell logging:
	`logman create trace ETWTrace -ow -o c:\ETWTrace.etl -p {AAD4C46D-56DE-4F98-BDA2-B5EAEBDD2B04} 0xffffffffffffffff 0xff -nb 16 16 -bs 1024 -mode 0x2 -max 2048 -ets`
	`logman update trace ETWTrace -p {62DFF3DA-7513-4FCA-BC73-25B111FBB1DB} 0xffffffffffffffff 0xff -ets`
	<repro>
	- Click **Apply**.
	- After the failure occurs, disable Windows Powershell logging, and collect the Event Trace Log.

DirectAccess is configured, but clients are not able to connect to internal resources	**To troubleshoot client connection issues** - Click the **Operations Status** tab in the Remote Access Management console, and ensure that all the components show a green icon. If not, check the error details and follow the resolution steps. - Run the Remote Access Server Best Practices Analyzer (BPA). If there are any warnings or errors, follow the resolution steps to resolve the issue.
Encountering issues related to a multisite configuration (for example, enabling a multisite, adding entry points, or setting the domain controller for an entry point)	Follow the steps in Troubleshoot a Multisite Deployment.
Configuration status tile on the dashboard shows a warning or error	Follow the steps in Monitor the configuration distribution status of the Remote Access server.
Encountering issues related to configuring load balancing (for example, the configuration fails when you enable load balancing, or there are issues when you add or remove servers from a cluster)	If you were enabling load balancing or adding a node, and the configuration refreshed when you clicked **Apply**, but the cluster didn't form correctly on the server, run the following command: **cmd.exe /c "reg add HKLM\SYSTEM\CurrentControlSet\Services\RaMgmtSvc\Parameters /f /v DebugFlag /t REG_DWORD /d ""0xffffffff"" "** to collect the user interface logs on the new server.
Operations status shows an error or warning after following steps to correct the situation	If the operations status is showing incorrect information (such as errors-even after you fix them): - Enable the registry key **cmd.exe /c "reg add HKLM\SYSTEM\CurrentControlSet\Services\RaMgmtSvc\Parameters /f /v EnableTracing /t REG_DWORD /d ""5"" "**. - Refresh the operations status and collect the logs from **%windir%/tracing**.

ISSUE	RESOLUTION

Windows 8 and later DirectAccess client computers report "No Internet" as status for the DirectAccess connection, and Network Connectivity Status Indicator (NCSI) reports limited connectivity.	This can occur when Force Tunneling is enabled in the DirectAccess configuration and, because of this, only IPHTTPS is being used. To resolve this issue, you can create and configure a proxy server. NCSI then uses the proxy server to perform Internet connectivity checks. It is recommended that you add a static proxy to the Name Resolution Policy Table (NRPT) by using the following procedure.
	Before you run the commands in this procedure, ensure that you replace all domain names, computer names, and other Windows PowerShell command variables with values that are appropriate for your deployment.
	Configure a static proxy for an NRPT rule
	1. Display the "." NRPT rule:
	`Get-DnsClientNrptRule -GpoName "corp.example.com\DirectAccess Client Settings" -Server <DomainControllerNetBIOSName>`
	2. Note the name (GUID) of the "." NRPT rule. The name (GUID) should start with **DA-{..}**
	3. Set the proxy for the "." NRPT rule to **proxy.corp.example.com:8080**:
	`Set-DnsClientNrptRule -Name "DA-{..}" -Server <DomainControllerNetBIOSName> -GPOName "corp.example.com\DirectAccess Client Settings" -DAProxyServerName "proxy.corp.example.com:8080" -DAProxyType "UseProxyName"`
	4. Display the "." NRPT rule again by running `Get-DnsClientNrptRule`, and verify that **ProxyFQDN:port** is now correctly configured.
	5. Refresh Group Policy by running `gpupdate /force` on a DirectAccess client when the client is connected internally, then display the NRPT using `Get-DnsClientNrptPolicy` and verify that the "." rule shows **ProxyFQDN:port**.

DirectAccess Known Issues

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2016, Windows Server 2019

DNS registration of DirectAccess client IPv6 addresses

Starting with the Windows 10 May 2020 Update, a client no longer registers its IP addresses on DNS servers configured in a Name Resolution Policy Table (NRPT). If DNS registration is needed, for example **Manage Out**, it can be explicitly enabled with this registry key on the client:

Path: `HKLM\System\CurrentControlSet\Services\Dnscache\Parameters`
Type: `DWORD`
Value name: `DisableNRPTForAdapterRegistration`
Values:
`1` - DNS Registration disabled (default since the Windows 10 May 2020 Update)
`0` - DNS Registration enabled

Recommended hotfixes and updates for Windows Server 2012 DirectAccess

The following link lists Microsoft Technical Support documents for DirectAccess that you should review and apply before you start your deployment to avoid an unusable configuration.

- Recommended hotfixes and updates for Windows Server 2012 DirectAccess

Troubleshooting Web Application Proxy

12/9/2022 • 13 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This content is relevant for the on-premises version of Web Application Proxy. To enable secure access to on-premises applications over the cloud, see the Azure AD Application Proxy content.

This section provides troubleshooting procedures for Web Application Proxy including event explanations and solutions. There are three places where errors are displayed:

- In the Web Application Proxy administrator console

  Each event ID listed in the administrator console can be viewed in the Windows Event Viewer and corresponding descriptions and solutions are found below.

  Open Event Viewer and look for events related to Web Application Proxy under **Applications and Services Logs** > **Microsoft** > **Windows** > **Web Application Proxy** > **Admin**

  If needed, detailed logs are available by turning on analytics and debugging logs and turning on the Web Application Proxy session log, found in the Windows Event Viewer under \ Microsoft \ Windows \ Web Application Proxy \ Admin.

- In PowerShell errors

  Events for issues encountered during configuration are displayed in PowerShell.

  All errors are presented to the PowerShell user using standard PowerShell error prompts. All PowerShell commands are logged as events. All events that occur in PowerShell are listed in the Windows Event Viewer with the ID number 12016, and are defined below in the PowerShell section.

- In the Best Practices Analyzer

  These events are described in the Best Practices Analyzer for Web Application Proxy

PowerShell Messages

EVENT OR SYMPTOM	POSSIBLE CAUSE	RESOLUTION
The trust certificate ("ADFS ProxyTrust - <WAP machine name>") is not valid	This could be caused by any of the following: - The Application Proxy machine was down for too long. - Disconnections between the Web Application Proxy and AD FS - Certificate infrastructure issues - Changes on the AD FS machine, or the renew process between the Web Application Proxy and the AD FS did not run as planned every 8 hours, then they need to renew trust - The clock of the Web Application Proxy machine and the AD FS are not synchronized.	Make sure the clocks are synchronized. Run the Install-WebApplicationProxy cmdlet.
Configuration data was not found in AD FS	This may be because Web Application Proxy was not fully installed yet or because of changes in the AD FS database or corruption of the database.	Run the Install-WebApplicationProxy Cmdlet
An error occurred when Web Application Proxy tried to read configuration from AD FS.	This may indicate that AD FS is not reachable, or that AD FS encountered an internal problem trying to read configuration from the AD FS database.	Verify that AD FS is reachable and working properly.
The configuration data stored in AD FS is corrupted or Web Application Proxy was unable to parse it. OR Web Application Proxy was unable to retrieve the list of Relying Parties from AD FS.	This may occur if the configuration data was modified in AD FS.	Restart the Web Application Proxy service. If the problem persists, run the Install-WebApplicationProxy Cmdlet.

Administrator Console Events

The following administrator console events are generally indicative of authentication errors, invalid tokens or expired cookies.

EVENT OR SYMPTOM	POSSIBLE CAUSE	RESOLUTION
11005 Web Application Proxy could not create the cookie encryption key using the secret from the configuration.	The global configuration "AccessCookiesEncryptionKey" parameter was changed by the PowerShell command: Set-WebApplicationProxyConfiguration -RegenerateAccessCookiesEncryptionKey	No action is required. The problematic cookie was removed and the user was redirected to STS for authentication.

EVENT OR SYMPTOM	POSSIBLE CAUSE	RESOLUTION
12000 Web Application Proxy could not check for configuration changes for at least 60 minutes	Web Application Proxy can't access the Web Application Proxy configuration using the command Get-WebApplicationProxyConfiguration/Application. This is usually caused by lack of connectivity with AD FS or the need to renew trust with AD FS.	Check connectivity with AD FS. You can do this using the link https://<FQDN_AD_FS_Proxy>/FederationMetadata/2007-06/FederationMetadata.xmlMake sure there is trust established between the AD FS and the Web Application Proxy. If these solutions don't work, run the Install-WebApplicationProxy Cmdlet.
12003 Web Application Proxy could not parse the access cookie.	This may indicate that the Web Application Proxy and the AD FS are not connected or that they don't receive the same configuration.	Check connectivity with AD FS. You can do this using the link https://<FQDN_AD_FS_Proxy>/FederationMetadata/2007-06/FederationMetadata.xmlMake sure there is trust established between the AD FS and the Web Application Proxy. If these solutions don't work, run the Install-WebApplicationProxy Cmdlet.
12004 Web Application Proxy received a request with a nonvalid access cookie.	This event may indicate that the Web Application Proxy and the AD FS are not connected or that they don't receive the same configuration. If you ran the "AccessCookiesEncryptionKey" parameter was changed by Set-WebApplicationProxyConfiguration -RegenerateAccessCookiesEncryptionKey PowerShell command, this event is normal and requires no resolution steps.	Check connectivity with AD FS. You can do this using the link https://<FQDN_AD_FS_Proxy>/FederationMetadata/2007-06/FederationMetadata.xmlMake sure there is trust established between the AD FS and the Web Application Proxy. If these solutions don't work, run the Install-WebApplicationProxy Cmdlet.
12008 Web Application Proxy exceeded the maximum number of permitted Kerberos authentication attempts to the backend server.	This event may indicate incorrect configuration between Web Application Proxy and the backend application server, or a problem in time and date configuration on both machines.	The backend server declined the Kerberos ticket created by Web Application Proxy. Verify that the configuration of the Web Application Proxy and the backend application server are configured correctly. Make sure that the time and date configuration on the Web Application Proxy and the backend application server are synchronized.
12011 Web Application Proxy received a request with a non-valid access cookie signature.	This event may indicate that the Web Application Proxy and the AD FS are not connected or that they don't receive the same configuration. If you ran the "AccessCookiesEncryptionKey" parameter was changed by Set-WebApplicationProxyConfiguration -RegenerateAccessCookiesEncryptionKey PowerShell command, this event is normal and requires no resolution steps.	Check connectivity with AD FS. You can do this using the link https://<FQDN_AD_FS_Proxy>/FederationMetadata/2007-06/FederationMetadata.xmlMake sure there is trust established between the AD FS and the Web Application Proxy. If these solutions don't work, run the Install-WebApplicationProxy Cmdlet.

EVENT OR SYMPTOM	POSSIBLE CAUSE	RESOLUTION
12027 Proxy encountered an unexpected error while processing the request. The name provided is not a properly formed account name.	This event may indicate incorrect configuration between Web Application Proxy and the domain controller server, or a problem in time and date configuration on both machines.	The domain controller declined the Kerberos ticket created by Web Application Proxy. Verify that the configuration of the Web Application Proxy and the backend application server are configured correctly, especially the SPN configuration. Make sure the Web Application Proxy is domain joined to the same domain as the domain controller to ensure that the domain controller establishes trust with Web Application Proxy. Make sure that the time and date configuration on the Web Application Proxy and the domain controller are synchronized.
13012 Web Application Proxy received a nonvalid edge token signature		Make sure you updated Web Application Proxy with KB 2955164.
13013 Web Application Proxy received a request that contained an expired edge token.	Web Application Proxy and AD FS do not have synchronized clocks.	Synchronize the clocks between Web Application Proxy and AD FS.
13014 Web Application Proxy received a request with a nonvalid edge token. The token is not valid because it could not be parsed.	This may indicate an issue with the AD FS configuration.	Check your AD FS configuration and, if necessary, restore the default configuration.
13015 Web Application Proxy received a request with an expired access cookie.	This could indicate clocks that are not synchronized.	If you are working with a cluster of Web Application Proxy machines, make sure that the time and date of the machines is synchronized.
13016 Web Application Proxy cannot retrieve a Kerberos ticket on behalf of the user because there is no UPN in the edge token or in the access cookie.	There is a problem with the STS configuration.	Fix the UPN claim configuration in the STS.

EVENT OR SYMPTOM	POSSIBLE CAUSE	RESOLUTION
13019 Web Application Proxy cannot retrieve a Kerberos ticket on behalf of the user because of the following general API error	This event may indicate incorrect configuration between Web Application Proxy and the domain controller server, or a problem in time and date configuration on both machines.	The domain controller declined the Kerberos ticket created by Web Application Proxy. Verify that the configuration of the Web Application Proxy and the backend application server are configured correctly, especially the SPN configuration. Make sure the Web Application Proxy is domain joined to the same domain as the domain controller to ensure that the domain controller establishes trust with Web Application Proxy. Make sure that the time and date configuration on the Web Application Proxy and the domain controller are synchronized.
13020 Web Application Proxy cannot retrieve a Kerberos ticket on behalf of the user because the backend server SPN is not defined.	This event may indicate incorrect configuration between Web Application Proxy and the domain controller server, or a problem in time and date configuration on both machines.	The domain controller declined the Kerberos ticket created by Web Application Proxy. Verify that the configuration of the Web Application Proxy and the backend application server are configured correctly, especially the SPN configuration. Make sure the Web Application Proxy is domain joined to the same domain as the domain controller to ensure that the domain controller establishes trust with Web Application Proxy. Make sure that the time and date configuration on the Web Application Proxy and the domain controller are synchronized.
13022 Web Application Proxy cannot authenticate the user because the backend server responds to Kerberos authentication attempts with an HTTP 401 error.	This event may indicate incorrect configuration between Web Application Proxy and the backend application server, or a problem in time and date configuration on both machines.	The backend server declined the Kerberos ticket created by Web Application Proxy. Verify that the configuration of the Web Application Proxy and the backend application server are configured correctly. Make sure that the time and date configuration on the Web Application Proxy and the backend application server are synchronized.
13025 The client did not present an SSL certificate to Web Application Proxy.	This event may indicate a problem in time and date configuration.	Make sure that the certificate infrastructure is valid and that the time and date of the Web Application Proxy and the AD FS are synchronized. Make sure that the thumbprint configured for the Web Application Proxy is the correct one.
13026 The client presented an SSL certificate to Web Application Proxy, but the certificate is not valid: the certificate does not match the thumbprint.	This event may indicate a problem in time and date configuration.	Make sure that the certificate infrastructure is valid and that the time and date of the Web Application Proxy and the AD FS are synchronized. Make sure that the thumbprint configured for the Web Application Proxy is the correct one.

EVENT OR SYMPTOM	POSSIBLE CAUSE	RESOLUTION
13028 Web Application Proxy received a request that contained an edge token that is not yet valid.	This event may indicate a problem in time and date configuration.	Make sure that the certificate infrastructure is valid and that the time and date of the Web Application Proxy and the AD FS are synchronized.
13030 The client presented an SSL certificate to Web Application Proxy, but the trust provider does not trust the certificate authority that issued the client certificate.	This event may indicate a problem in time and date configuration.	Make sure that the certificate infrastructure is valid and that the time and date of the Web Application Proxy and the AD FS are synchronized. Make sure that the thumbprint configured for the Web Application Proxy is the correct one.
13031 The client presented an SSL certificate to Web Application Proxy, but the certificate chain terminated in a root certificate that is not trusted by the trust provider.	This event may indicate a problem in time and date configuration.	Make sure that the certificate infrastructure is valid and that the time and date of the Web Application Proxy and the AD FS are synchronized. Make sure that the thumbprint configured for the Web Application Proxy is the correct one.
13032 The client presented an SSL certificate to Web Application Proxy, but the certificate was not valid for the requested usage.	This event may indicate a problem in time and date configuration.	Make sure that the certificate infrastructure is valid and that the time and date of the Web Application Proxy and the AD FS are synchronized. Make sure that the thumbprint configured for the Web Application Proxy is the correct one.
13033 The client presented an SSL certificate to Web Application Proxy, but the certificate was not within its validity period when verifying against the current system clock or the timestamp in the signed file.	This event may indicate a problem in time and date configuration.	Make sure that the certificate infrastructure is valid and that the time and date of the Web Application Proxy and the AD FS are synchronized. Make sure that the thumbprint configured for the Web Application Proxy is the correct one.
13034 The client presented an SSL certificate to Web Application Proxy, but the certificate was not valid.	This event may indicate a problem in time and date configuration.	Make sure that the certificate infrastructure is valid and that the time and date of the Web Application Proxy and the AD FS are synchronized. Make sure that the thumbprint configured for the Web Application Proxy is the correct one.

The following administrator console events are usually indicative of problems having to do with configuration such as provisioning, requests that are not successful, backend servers that are unreachable and buffer overflows.

EVENT OR SYMPTOM	POSSIBLE CAUSE	RESOLUTION
12019 Web Application Proxy could not create a listener for the following URL.	A possible cause for the event is that another service is listening to the same URL.	The admin must make sure that no one listens or binds to the same URLs. To check this, run the command: netsh http show urlacl. If this URL is used by another component running on the Web Application Proxy machine, either remove it, or use a different URL to publish the applications through Web Application Proxy.
12020 Web Application Proxy could not create a reservation for the following URL.	A possible cause for the event is that another service has a reservation on the same URL.	The admin must make sure that no one binds to the same URLs. To check this, run the command: netsh http show urlacl. If this URL is used by another component running on the Web Application Proxy machine, either remove it, or use a different URL to publish the applications through Web Application Proxy.
12021 Web Application Proxy could not bind the SSL server certificate. All other configuration settings were applied.	Unable to create and set a configuration record of SSL certificate data.	Make sure that the certificate thumbprints that are configured for Web Application Proxy applications are installed on all the Web Application Proxy machines with a private key in the local computer store.
13001 The SSL server certificate presented to Web Application Proxy by the backend server is not valid; the certificate is not trusted.	One or more errors were found in the Secure Sockets Layer (SSL) certificate sent by the server. This could indicate that the backend server provided an SSL that was not valid or that there is no trust between the Web Application Proxy and the backend server.	Validate a backend server SSL certificate. Make sure that the Web Application Proxy machine is configured with the right root CAs to trust the backend server certificate.
13006	When the error code is 0x80072ee7, the failure is caused by the inability to resolve the backend server URL. Other error codes are described in https://msdn.microsoft.com/library/windows/desktop/aa384110(v=vs.85)	Check that the backend server URL is correct and that its name can be resolved correctly from the Web Application Proxy machine.
13007 The HTTP response from the backend server was not received within the expected interval.	The back-end server request timed out or is slow or unresponsive.	Check the backend server configuration. If it's very slow, check the connectivity to the backend server and also consider changing the Web Application Proxy global configuration parameter cmdlet for InactiveTransactionsTimeoutSec.

See Also

What's New in Web Application Proxy in Windows Server 2016

Working with Web Application Proxy

BGP Windows PowerShell Command Reference

12/9/2022 • 9 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

You can use this topic as a reference, when writing Windows PowerShell scripts, to add, configure, and remove BGP capabilities from RAS Gateway and Remote Access Local Area Network (LAN) routers.

These BGP commands are part of the Remote Access Windows PowerShell command set for Windows Server 2016. This topic helps you quickly locate the BGP commands that you want to use in scripts.

For more information on all Remote Access commands, see Remote Access Cmdlets.

BGP Command Reference

The following sections provide command name, purpose, and syntax for each BGP command, as well as a link to the command in the Remote Access reference, which contains more detailed information about each command.

This reference contains the following sections.

- Add commands
- Clear commands
- Disable and Enable commands
- Get commands
- Install commands
- Remove commands
- Set commands
- Start and Stop commands
- Uninstall commands

Add commands

Following are the BGP Add commands.

Add-BgpCustomRoute

Adds custom routes to the BGP routing table.

```
Add-BgpCustomRoute [-CimSession <CimSession[]> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-Interface <String[]> ] [-Network <String[]> ] [-
PassThru] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [ <CommonParameters>] [ <WorkflowParameters>]
```

Add-BgpPeer

Adds a new BGP peer.

```
Add-BgpPeer [-Name] <String> -LocalIPAddress <IPAddress> -PeerASN <UInt32> -PeerIPAddress <IPAddress> [-
CimSession <CimSession[]> ] [-HoldTimeSec <UInt16> ] [-IdleHoldTimeSec <UInt16> ] [-InformationAction
<ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable
<String> ] [-LocalASN <UInt32> ] [-MaxAllowedPrefix <UInt32> ] [-OperationMode <OperationMode> {Mixed |
Server} ] [-PassThru] [-PeeringMode <PeeringMode> {Automatic | Manual} ] [-RouteReflectorClient <Boolean> ]
[-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Weight <UInt16> ] [ <CommonParameters>] [
<WorkflowParameters>]
```

Add-BgpRouteAggregate

Adds a new aggregate route for specific BGP routes.

```
Add-BgpRouteAggregate -Prefix <String> [-AttributePolicy <String[]> ] [-CimSession <CimSession[]> ] [-Force]
[-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ]
[-InformationVariable <String> ] [-PassThru] [-PreserveASPath <PreserveASPath> ] [-RoutingDomain <String> ]
[-SummaryOnly <SummaryOnly> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [
<WorkflowParameters>]
```

Add-BgpRouter

Adds a BGP router for the specified Tenant ID.

```
Add-BgpRouter -BgpIdentifier <IPAddress> -LocalASN <UInt32> [-CimSession <CimSession[]> ] [-
ClientToClientReflection <ClientToClientReflection> ] [-ClusterId <UInt32> ] [-CompareMEDAcrossASN <Boolean>
] [-DefaultGatewayRouting <Boolean> ] [-Force] [-InformationAction <ActionPreference> {SilentlyContinue |
Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-IPv6Routing
<IPv6RoutingState> {Disabled | Enabled} ] [-LocalIPv6Address <IPAddress> ] [-PassThru] [-RouteReflector
<RouteReflector> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-TransitRouting <TransitRouting> ]
[ <CommonParameters>] [ <WorkflowParameters>]
```

Add-BgpRoutingPolicy

Adds a BGP routing policy to the policy store.

```
Add-BgpRoutingPolicy [-Name] <String> [-PolicyType] <PolicyType> {Deny | Allow | ModifyAttribute} [-
AddCommunity <String[]> ] [-CimSession <CimSession[]> ] [-ClearMED] [-Force] [-IgnorePrefix <String[]> ] [-
InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue |
Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-MatchASNRange <UInt32[]> ] [-
MatchCommunity <String[]> ] [-MatchNextHop <IPAddress[]> ] [-MatchPrefix <String[]> ] [-NewLocalPref
<UInt32]> ] [-NewMED <UInt32]> ] [-NewNextHop <IPAddress> ] [-PassThru] [-RemoveAllCommunities] [-
RemoveCommunity <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [ <CommonParameters>] [
<WorkflowParameters>]
```

Add-BgpRoutingPolicyForPeer

Adds BGP routing policies to BGP peers.

```
Add-BgpRoutingPolicyForPeer -Direction <PolicyDirection> {Ingress | Egress} -PolicyName <String[]> [-
CimSession <CimSession[]> ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ]
[-PeerName <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [
<CommonParameters>] [ <WorkflowParameters>]
```

Clear commands

Following are the Clear commands for BGP

Clear-BgpRouteFlapDampening

Clears the route flap dampening information for the specified set of BGP routes.

```
Clear-BgpRouteFlapDampening [-CimSession <CimSession[]> ] [-Force] [-InformationAction <ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-
Prefix <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [
<CommonParameters>] [ <WorkflowParameters>]
```

Disable and Enable commands

Following are the Disable and Enable commands for BGP

Disable-BgpRouteFlapDampening

Disables route dampening for the flapping BGP routes.

```
Disable-BgpRouteFlapDampening [-CimSession <CimSession[]> ] [-Force] [-InformationAction <ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-
RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [
<WorkflowParameters>]
```

Enable-BgpRouteFlapDampening

Enables route dampening for the flapping BGP routes.

```
Enable-BgpRouteFlapDampening [-CimSession <CimSession[]> ] [-Force] [-InformationAction <ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-
PassThru] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [
<WorkflowParameters>]
```

Get commands

Following are the Get commands for BGP.

Get-BgpCustomRoute

Gets custom route information from the BGP router.

```
Get-BgpCustomRoute [-CimSession <CimSession[]> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [
<CommonParameters>] [ <WorkflowParameters>]
```

Get-BgpPeer

Gets configuration information for BGP peers.

```
Get-BgpPeer [[-Name] <String[]> ] [-CimSession <CimSession[]> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [
<CommonParameters>] [ <WorkflowParameters>]
```

Get-BgpRouteAggregate

Gets all the aggregate BGP routes configured by the administrator.

```
Get-BgpRouteAggregate [-CimSession <CimSession[]> ] [-InformationAction <ActionPreference> {SilentlyContinue
| Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-Prefix <String[]> ] [-
RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [
<WorkflowParameters>]
```

Get-BgpRouteFlapDampening

Retrieves the configuration of a BGP route dampening engine.

```
Get-BgpRouteFlapDampening [-CimSession <CimSession[]> ] [-InformationAction <ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-
RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [
<WorkflowParameters>]
```

Get-BgpRouteInformation

Retrieves BGP route information for one or more network prefixes from the BGP routing table.

```
Get-BgpRouteInformation [-CimSession <CimSession[]> ] [-InformationAction <ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-
Network <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Type <RouteType> ] [
<CommonParameters>] [ <WorkflowParameters>]
```

Get-BgpRouter

Gets configuration information for BGP routers.

```
Get-BgpRouter [-CimSession <CimSession[]> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String[]> ] [-ThrottleLimit <Int32> ] [
<CommonParameters>] [ <WorkflowParameters>]
```

Get-BgpRoutingPolicy

Gets configuration information of BGP routing policies.

```
Get-BgpRoutingPolicy [[-Name] <String[]> ] [-CimSession <CimSession[]> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-PolicyType <PolicyType> {Deny | Allow |
ModifyAttribute} ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [ <CommonParameters>] [
<WorkflowParameters>]
```

Get-BgpStatistics

Retrieves BGP peering-related message and route advertisement statistics.

```
Get-BgpStatistics [-CimSession <CimSession[]> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-PeerName <String[]> ] [-RoutingDomain <String> ] [-
ThrottleLimit <Int32> ] [ <CommonParameters>] [ <WorkflowParameters>]
```

Install commands

Following are the Install commands for RAS Gateway and BGP.

Install-RemoteAccess

Performs prerequisite checks for DirectAccess (DA) to ensure that it can be installed, installs DA for remote access (RA) (includes management of remote clients) or for management of remote clients only, installs VPN (both Remote Access VPN and site-to-site VPN), and installs BGP Routing.

```
Parameter Set: MultiTenant
Install-RemoteAccess [-MultiTenancy] [-CapacityKbps <UInt64> ] [-CimSession <CimSession[]> ] [-ComputerName
<String> ] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop |
Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-MsgAuthenticator <String>
{Enabled | Disabled} ] [-PassThru] [-RadiusPort <UInt16> ] [-RadiusScore <Byte> ] [-RadiusServer <String> ]
[-RadiusTimeout <UInt32> ] [-SharedSecret <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [
<CommonParameters>] [ <WorkflowParameters>]

Parameter Set: Vpn
Install-RemoteAccess [-VpnType] <String> {Vpn | VpnS2S | SstpProxy | RoutingOnly} [-CimSession
<CimSession[]> ] [-ComputerName <String> ] [-EntrypointName <String> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-IPAddressRange <String[]> ] [-IPv6Prefix <String> ] [-
Legacy] [-MsgAuthenticator <String> {Enabled | Disabled} ] [-PassThru] [-RadiusPort <UInt16> ] [-RadiusScore
<Byte> ] [-RadiusServer <String> ] [-RadiusTimeout <UInt32> ] [-SharedSecret <String> ] [-ThrottleLimit
<Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

IMPORTANT

When you install RAS Gateway in Multitenant mode, you must specify whether BGP is enabled for each tenant by using the **Enable-RemoteAccessRoutingDomain** Windows PowerShell command with the **-Type** parameter value of **All**. The following example code illustrates how to install RAS in Multitenancy mode with all RAS features (point-to-site VPN, site-to-site VPN, and BGP routing) enabled for two tenants, Contoso and Fabrikam.

```
$Contoso_RoutingDomain = "ContosoTenant"
$Fabrikam_RoutingDomain = "FabrikamTenant"

Install-RemoteAccess -MultiTenancy

Enable-RemoteAccessRoutingDomain -Name $Contoso_RoutingDomain -Type All -PassThru
Enable-RemoteAccessRoutingDomain -Name $Fabrikam_RoutingDomain -Type All -PassThru
```

If you are using Remote Access as a LAN router instead of as a gateway, you can still use BGP, which provides the advantage of having dynamic routing on your intranet. To install Remote Access as a BGP LAN router, type the following command in a Windows PowerShell prompt, and then press ENTER.

```
Install-RemoteAccess -VpnType RoutingOnly
```

Remove commands

Following are the Remove commands for BGP.

Remove-BgpCustomRoute

Removes custom routes from the BGP router.

```
Remove-BgpCustomRoute [-CimSession <CimSession[]> ] [-Force] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-Interface <String[]> ] [-Network <String[]> ] [-
RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [
<WorkflowParameters>]
```

Remove-BgpPeer

Removes BGP peers from a router.

```
Remove-BgpPeer [-Name] <String[]> [-CimSession <CimSession[]> ] [-Force] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-
Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Remove-BgpRouteAggregate

Removes the set of specified aggregate BGP routes.

```
Remove-BgpRouteAggregate [-CimSession <CimSession[]> ] [-Force] [-InformationAction <ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-
Prefix <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [
<CommonParameters>] [ <WorkflowParameters>]
```

Remove-BgpRouter

Removes a BGP router.

```
Remove-BgpRouter [-CimSession <CimSession[]> ] [-Force] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String[]> ] [-ThrottleLimit <Int32> ] [-
Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Remove-BgpRoutingPolicy

Removes routing policies from the policy store.

```
Remove-BgpRoutingPolicy [-Name] <String[]> [-CimSession <CimSession[]> ] [-Force] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-
Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Remove-BgpRoutingPolicyForPeer

Removes routing policies from BGP peers.

```
Parameter Set: Remove1
Remove-BgpRoutingPolicyForPeer [-CimSession <CimSession[]> ] [-Direction <PolicyDirection> {Ingress |
Egress} ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue |
Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-PeerName
<String[]> ] [-PolicyName <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-
WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Set commands

Following are the Set commands for BGP.

Set-BgpPeer

Updates the configuration of the specified BGP peer.

```
Set-BgpPeer [-Name] <String> [-CimSession <CimSession[]> ] [-ClearPrefixLimit] [-Force] [-HoldTimeSec
<UInt16> ] [-IdleHoldTimeSec <UInt16> ] [-InformationAction <ActionPreference> {SilentlyContinue | Stop |
Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-LocalASN <UInt32> ] [-
LocalIPAddress <IPAddress> ] [-MaxAllowedPrefix <UInt32> ] [-OperationMode <OperationMode> {Mixed | Server}
] [-PassThru] [-PeerASN <UInt32> ] [-PeeringMode <PeeringMode> {Automatic | Manual} ] [-PeerIPAddress
<IPAddress> ] [-RouteReflectorClient <Boolean> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-
Weight <UInt16> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Set-BgpRouteAggregate

Updates the properties of specified aggregate BGP route.

```
Set-BgpRouteAggregate -Prefix <String> [-AttributePolicy <String[]> ] [-CimSession <CimSession[]> ] [-Force]
[-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ]
[-InformationVariable <String> ] [-PassThru] [-PreserveASPath <PreserveASPath> ] [-RoutingDomain <String> ]
[-SummaryOnly <SummaryOnly> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [ <CommonParameters>] [
<WorkflowParameters>]
```

Set-BgpRouteFlapDampening

Configures the BGP route dampening engine.

```
Set-BgpRouteFlapDampening [-CimSession <CimSession[]> ] [-Force] [-HalfLife <UInt32> ] [-HalfLifeUnreachable
<UInt32> ] [-InformationAction <ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <String> ] [-MaxSuppressTime <UInt32> ] [-PassThru] [-ReuseThreshold
<UInt32> ] [-RoutingDomain <String> ] [-SuppressThreshold <UInt32> ] [-ThrottleLimit <Int32> ] [-Confirm] [-
WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Set-BgpRouter

Updates the configuration of the local BGP router for the specified tenant ID.

```
Set-BgpRouter [-BgpIdentifier <IPAddress> ] [-CimSession <CimSession[]> ] [-ClientToClientReflection
<ClientToClientReflection> ] [-ClusterId <UInt32> ] [-CompareMEDAcrossASN <Boolean> ] [-
DefaultGatewayRouting <Boolean> ] [-Force] [-InformationAction <ActionPreference> {SilentlyContinue | Stop |
Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <String> ] [-IPv6Routing <IPv6RoutingState>
{Disabled | Enabled} ] [-LocalASN <UInt32> ] [-LocalIPv6Address <IPAddress> ] [-PassThru] [-RouteReflector
<RouteReflector> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-TransitRouting <TransitRouting> ]
[-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Set-BgpRoutingPolicy

Modifies a routing policy configuration.

```
Set-BgpRoutingPolicy [-Name] <String> [-AddCommunity <String[]> ] [-CimSession <CimSession[]> ] [-ClearMED]
[-Force] [-IgnorePrefix <String[]> ] [-InformationAction <System.Management.Automation.ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ]
[-MatchASNRange <UInt32[]> ] [-MatchCommunity <String[]> ] [-MatchNextHop <IPAddress[]> ] [-MatchPrefix
<String[]> ] [-NewLocalPref <UInt32]> ] [-NewMED <UInt32]> ] [-NewNextHop <IPAddress> ] [-PassThru] [-
PolicyType <PolicyType> {Deny | Allow | ModifyAttribute} ] [-RemoveAllCommunities] [-RemoveCommunity
<String[]> ] [-RemovePolicyClause <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-
Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Set-BgpRoutingPolicyForPeer

Modifies BGP routing policies for BGP peers.

```
Set-BgpRoutingPolicyForPeer -Direction <PolicyDirection> {Ingress | Egress} -PolicyName <String[]> [-
CimSession <CimSession[]> ] [-Force] [-InformationAction <System.Management.Automation.ActionPreference>
{SilentlyContinue | Stop | Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ]
[-PeerName <String[]> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-Confirm] [-WhatIf] [
<CommonParameters>] [ <WorkflowParameters>]
```

Start and Stop commands

Following are the Start and Stop commands for BGP.

Start-BgpPeer

Starts routing sessions for BGP peers.

```
Start-BgpPeer [-Name] <String[]> [-CimSession <CimSession[]> ] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [
<CommonParameters>] [ <WorkflowParameters>]
```

Stop-BgpPeer

Stops routing sessions for BGP peers.

```
Stop-BgpPeer [-Name] <String[]> [-CimSession <CimSession[]> ] [-Force] [-InformationAction
<System.Management.Automation.ActionPreference> {SilentlyContinue | Stop | Continue | Inquire | Ignore |
Suspend} ] [-InformationVariable <System.String> ] [-RoutingDomain <String> ] [-ThrottleLimit <Int32> ] [-
Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

Uninstall commands

Following are the Uninstall commands for RAS Gateway and BGP.

Uninstall-RemoteAccess

Uninstalls Remote Access from the computer, including all Remote Access features and functionality (RAS Gateway, BGP, etc).

```
Uninstall-RemoteAccess [-CimSession <CimSession[]> ] [-ComputerName <String> ] [-EntrypointName <String> ]
[-Force] [-InformationAction <System.Management.Automation.ActionPreference> {SilentlyContinue | Stop |
Continue | Inquire | Ignore | Suspend} ] [-InformationVariable <System.String> ] [-ThrottleLimit <Int32> ]
[-VpnType <String> {Vpn | VpnS2S} ] [-Confirm] [-WhatIf] [ <CommonParameters>] [ <WorkflowParameters>]
```

DirectAccess Test Lab Guides

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Following are links to the test lab guides for DirectAccess in Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012.

- Test Lab Guide: Demonstrate DirectAccess in a cluster with Windows NLB
- Test Lab Guide: Demonstrate a DirectAccess multisite deployment
- Test Lab Guide: Demonstrate DirectAccess with OTP authentication and RSA SecurID

Test Lab Guide: Demonstrate DirectAccess in a Cluster with Windows NLB

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Remote Access is a server role in the Windows Server 2016, Windows Server 2012 R2 andWindows Server 2012 operating systems that enables remote users to securely access internal network resources using DirectAccess or RRAS VPN. This guide contains step-by-step instructions for extending the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6 to demonstrate DirectAccess Network Load Balancing and cluster configuration.

About this guide

This guide contains instructions for configuring and demonstrating Remote Access using six servers and two client computers. The completed Remote Access test lab with NLB simulates an intranet, the Internet, and a home network and demonstrates Remote Access functionality in different Internet connection scenarios.

> **IMPORTANT**
>
> This lab is a proof of concept using the minimum number of computers. The configuration detailed in this guide is for test lab purposes only, and is not to be used in a production environment.

Known issues

The following are known issues when configuring a cluster scenario:

- After configuring DirectAccess in an IPv4-only deployment with a single network adapter, and after the default DNS64 (the IPv6 address which contains ":3333::") is automatically configured on the network adapter, attempting to enable load-balancing via the Remote Access Management console causes a prompt for the user to supply an IPv6 DIP. If an IPv6 DIP is supplied, the configuration fails after clicking **Commit** with the error: The parameter is incorrect.

  To resolve this issue:

  1. Download the backup and restore scripts from Back up and Restore Remote Access Configuration.
  2. Back up your Remote Access GPOs using the downloaded script Backup-RemoteAccess.ps1
  3. Attempt to enable load balancing until the step at which it fails. On the Enable Load Balancing dialog box, expand the details area, right-click in the details area, and then click **Copy Script**.
  4. Open Notepad, and paste the contents of the clipboard. For example:

     ```
     Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress
     @('10.244.4.19/255.255.255.0','fdc4:29bd:abde:3333::2/128') -InternetVirtualIPAddress
     @('fdc4:29bd:abde:3333::1/128', '10.244.4.21/255.255.255.0') -ComputerName
     'DA1.domain1.corp.contoso.com' -Verbose
     ```

  5. Close any open Remote Access dialog boxes and close the Remote Access Management console.

6. Edit the pasted text and remove the IPv6 addresses. For example:

```
Set-RemoteAccessLoadBalancer -InternetDedicatedIPAddress @('10.244.4.19/255.255.255.0') -
InternetVirtualIPAddress @('10.244.4.21/255.255.255.0') -ComputerName
'DA1.domain1.corp.contoso.com' -Verbose
```

7. In an elevated PowerShell window, run the command from the previous step.

8. If the cmdlet fails while it is running (not due to incorrect input values), run the command Restore-RemoteAccess.ps1 and follow instructions to make sure that the integrity of your original configuration is maintained.

9. You can now open the Remote Access Management console again.

Overview of the DirectAccess Cluster-NLB Test Lab Scenario

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

In this test lab scenario, DirectAccess is deployed with:

- **DC1** -A server that is configured as a domain controller, Domain Name System (DNS) server, and Dynamic Host Configuration Protocol (DHCP) server.
- **EDGE1** -A server on the internal network that is configured as the first Remote Access server in a Remote Access server cluster. This server has two network adapters; one connected to the internal network, and the other connected to the external network.
- **EDGE2** -A server on the internal network that is configured as the second Remote Access server in a Remote Access server cluster. This server has two network adapters; one connected to the internal network, and the other connected to the external network.
- **APP1** -A server on the internal network that is configured as a web and file server, and as an enterprise root certification authority (CA)
- **APP2** -A computer on the internal network that is configured as an IPv4 only web and file server. This computer is used to highlight the NAT64/DNS64 capabilities.
- **INET1** -A server that is configured as an Internet DNS and DHCP server.
- **NAT1** -A client computer that is configured as a network address translator (NAT) device using Internet Connection Sharing.
- **CLIENT1** -A client computer that is configured as a DirectAccess client that will be used to test DirectAccess connectivity when moving between the internal network, the simulated Internet, and a home network.

The test lab consists of three subnets that simulate the following:

- A home network named Homenet (192.168.137.0/24) connected to the Internet by a NAT.
- The external network represented by the Internet subnet (131.107.0.0/24).
- An internal network named Corpnet (10.0.0.0/24; 2001:db8:1::/64) separated from the Internet by the Remote Access server.

Computers on each subnet connect using either a physical or virtual hub or switch, as shown in the following figure.

INET1
DC1
EDGE1
NAT1
Internet
131.107.0.0/24
Corpnet
10.0.0.0/24
2001:db8:1::/64
APP1
EDGE2
Homenet
192.168.137.0/24
APP2
CLIENT1

DirectAccess Cluster-NLB Test Lab Configuration Requirements

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The following components are required for configuring DirectAccess in the test lab:

- The product disc or files for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012.
- Six computers or virtual machines that meet the minimum hardware requirements for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 ; two of these computers have two network adapters installed.
- The product disc or files for Windows 10® or Windows® 8.
- Two computers or virtual machines that meet the minimum hardware requirements for Windows 10® or Windows® 8; one of these computers has two network adapters installed.

Steps for Configuring the DirectAccess Cluster-NLB Test Lab

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The following steps describe how to configure the Remote Access infrastructure, configure the Remote Access servers and clients, and test DirectAccess connectivity from the Internet and Homenet subnets.

In this test lab guide you will build a Network Load Balancing (NLB) enabled Remote Access cluster by performing the following steps:

- STEP 1 Complete the DirectAccess Configuration. Complete all the steps in the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6.
- STEP 2: Configure EDGE1. Configure the Remote Access role on EDGE1 for load balancing.
- STEP 3: Install and configure EDGE2. EDGE2 acts as the second Remote Access server in a Remote Access cluster.
- STEP 4: Create the network load balanced Remote Access cluster-EDGE1 is configured as the first server in a Remote Access cluster. EDGE2 is joined to the cluster and NLB is configured for the cluster.
- STEP 5: Test DirectAccess connectivity from the Internet and through the cluster. After NLB and cluster configuration is complete you can test DirectAccess client connectivity through the load balanced cluster.
- STEP 6: Test DirectAccess client connectivity from behind a NAT device. Move the client computer behind a NAT device to simulate testing DirectAccess client connectivity from behind a home router.
- STEP 7: Test connectivity when returning to the Corpnet. Make sure that the client computer can still access corporate resources when returning to Corpnet.
- STEP 8: Snapshot the configuration. After completing the test lab, take a snapshot of the working Remote Access NLB cluster so that you can return to it later to test additional scenarios.

STEP 1 Complete the DirectAccess in a Cluster with Windows NLB Configuration

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first step is to complete all the steps in the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6. If you have already completed the steps in this test lab guides and saved a snapshot or disk image of the test lab, you can restore the snapshot or image and begin with the next step.

STEP 2 Configure EDGE1

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The following procedure is performed on the DirectAccess server:

To configure DirectAccess on EDGE1

1. On the **Start** screen, type**RAMgmtUI.exe**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the Remote Access Management console, in the left pane, click **Configuration**.
3. In the middle pane of the console, in the **Step 2 Remote Access Server** area, click **Edit**.
4. In the **Remote Access Server Setup** wizard, click **Prefix Configuration**. On the **Prefix Configuration** page, in **IPv6 prefix assigned to DirectAccess client computers**, enter **2001:db8:1:1000::/59**, and then click **Next**.
5. Click **Finish**.
6. In the middle pane of the console, click **Finish**.
7. On the **Remote Access Review** dialog box, review the configuration settings, and then click **Apply**. On the **Applying Remote Access Setup Wizard Settings** dialog box, click **Close**.

STEP 3 Install and Configure EDGE2

12/9/2022 • 4 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

EDGE2 is the second member of a Remote Access cluster. EDGE2 is installed and configured before enabling the cluster configuration.

Perform the following steps to configure EDGE2:

Install the operating system on EDGE2

1. On EDGE2, start the installation of Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 .
2. Follow the instructions to complete the installation, specifying Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 (full installation) and a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect EDGE2 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 , and then disconnect from the Internet.
4. Connect one network adapter to the Corpnet subnet or the virtual switch representing the corpnet subnet and the other to the Internet subnet or virtual switch representing the Internet subnet.

Configure TCP/IP properties

1. In the Server Manager console, click **Local Server**, and then in the **Properties** area, next to **Wired Ethernet Connection**, click the link.
2. In the **Network Connections** window, right-click the network connection that is connected to the Corpnet subnet or virtual switch, and then click **Rename**.
3. Type **Corpnet**, and then press ENTER.
4. Right-click **Corpnet**, and then click **Properties**.
5. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
6. Click **Use the following IP address**. In **IP address**, type **10.0.0.8**. In **Subnet mask**, type **255.255.255.0**.
7. Click **Use the following DNS server addresses**. In **Preferred DNS server**, type **10.0.0.1**.
8. Click **Advanced**, and then click the **DNS** tab.
9. In **DNS suffix for this connection**, type **corp.contoso.com**, click **OK** twice.
10. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
11. Click **Use the following IPv6 address**. In **IPv6 address**, type **2001:db8:1::8**. In **Subnet prefix length**, type **64**.
12. Click **Use the following DNS server addresses**. In **Preferred DNS server**, type **2001:db8:1::1**.

13. Click **Advanced**, and then click the **DNS** tab.
14. In **DNS suffix for this connection**, type **corp.contoso.com**, click **OK** twice, and then click **Close**.
15. In the **Network Connections** window, right-click the network connection that is connected to the Internet subnet, and then click **Rename**.
16. Type **Internet**, and then press ENTER.
17. Right-click **Internet**, and then click **Properties**.
18. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
19. Click **Use the following IP address**. In **IP address**, enter **131.107.0.8**. In **Subnet mask**, enter **255.255.255.0**.
20. Click the **DNS** tab
21. In **DNS suffix for this connection**, type **isp.example.com**, and then click **OK** twice, and then click **Close**.
22. Close the **Network Connections** window.
23. To check network communication between EDGE2 and DC1, click **Start**, type **cmd**, and then press ENTER.
24. In the Command Prompt window, type **ping dc1.corp.contoso.com** and press ENTER. Verify that there are four responses from 10.0.0.1 or the IPv6 address 2001:db8:1::1
25. Close the Command Prompt window.

Rename EDGE2 and join it to the domain

1. In the Server Manager console, in **Local Server**, in the **Properties** area, next to **Computer name**, click the link.
2. On the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
3. On the **Computer Name/Domain Changes** dialog box, in the **Computer name** box, type **EDGE2**. In the **Member of** area, click **Domain**, and in the text box, enter **corp.contoso.com**, and then click **OK**.
4. When you are prompted for a user name and password, type **User1** and its password, and then click **OK**.
5. When you see a dialog box welcoming you to the corp.contoso.com domain, click **OK**.
6. When you are prompted that you must restart the computer, click **OK**.
7. On the **System Properties** dialog box, click **Close**.
8. When you are prompted to restart the computer, click **Restart Now**.
9. After restarting, login as CORP\User1.

Install the IP-HTTPS certificate

1. On the **Start** screen, type**mmc.exe**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.
3. On the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Finish**, and then click **OK**.

4. In the left pane of the console, navigate to **Certificates (Local Computer)\Personal\Certificates**. Right click the **Certificates** node, point to **All Tasks**, and then click **Request New Certificate**.
5. On the Certificate Enrollment wizard, click **Next** twice.
6. On the **Request Certificates** page, select the **Web Server** check box, and then click **More information is required to enroll for this certificate**.
7. On the **Certificate Properties** dialog box, on the **Subject** tab, in the **Subject name** area, in the **Type** list, click **Common Name**.
8. In **Value**, type **edge1.contoso.com**, and then click **Add**.
9. In the **Alternative name** area, in the **Type** list, click **DNS**.
10. In **Value**, type **edge1.contoso.com**, and then click **Add**.
11. On the **General** tab, in **Friendly name**, type **IP-HTTPS Certificate**.
12. Click **OK**, click **Enroll**, and then click **Finish**.
13. In the details pane of the Certificates snap-in, verify that a new certificate with the name edge1.contoso.com was enrolled with Intended Purposes of Server Authentication.
14. Close the console window. If you are prompted to save settings, click **No**.

Install the Remote Access role on EDGE2

1. In the Server Manager console, in the **Dashboard**, click **Add roles and features**.
2. Click **Next** three times to get to the server role selection screen.
3. On the **Select server roles** dialog, select **Remote Access**, click **Add Features**, and then click **Next**.
4. Click **Next** five times.
5. On the **Confirm installation selections** dialog, click **Install**.
6. On the **Installation progress** dialog, verify that the installation was successful, and then click **Close**.

STEP 4 Create the Network Load Balanced Remote Access Cluster

12/9/2022 • 4 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012 enable you to create clusters of Remote Access servers. A cluster acts as a single logical server and provides centralized configuration and management for the servers in the cluster. When using Network Load Balancing (NLB) there is support for up to 8 Remote Access members in a single cluster. Remote Access clusters provide high availability and load balancing of connections from DirectAccess clients to the internal network.

The following procedures enable you to create and test a Remote Access cluster:

1. Install the Network Load Balancing feature on EDGE1 and EDGE2. Before enabling load balancing, you must install the Network Load Balancing feature on both EDGE1 and EDGE2.
2. Enable load balancing on EDGE1. EDGE1 was originally installed in single server mode. To enable load balancing, you configure new external and internal dedicated IP addresses (DIPs) for EDGE1. The previous DIPs on EDGE1 are automatically configured as virtual IP addresses (VIPs) for the cluster. The new external DIP is 131.107.0.10, the new internal IPv4 DIP is 10.0.0.10, the new internal IPv6 DIP is 2001:db8:1::10. The cluster VIPs are 131.107.0.2 and 131.107.0.3 (external), and 10.0.0.2 and 2001:db8:1::2 (internal).
3. Add EDGE2 to the load balanced cluster. After enabling load balancing, you can now add EDGE2 to the cluster to provide load balancing and high availability for DirectAccess client connections.

Prerequisites

If you are creating this test lab on virtual machines, you must enable MAC address spoofing on EDGE1 and EDGE2.

Enable MAC address spoofing on EDGE1 and EDGE2

1. Perform a graceful shutdown on EDGE1 and EDGE2.
2. On the machine hosting your virtual machines, in **Hyper-V Manager**, right-click EDGE1, and then click **Settings**.
3. On the **Settings** dialog box, in the **Hardware** list, click the network adapter connected to the corpnet network, and then in the details pane, select the **Enable spoofing of MAC addresses** check box.
4. In the **Hardware** list, click the network adapter connected to the Internet network, and then in the details pane, select the **Enable spoofing of MAC addresses** check box.
5. On the **Settings** dialog box, click **OK**.
6. Repeat this procedure from step 2 on EDGE2.

Install the Network Load Balancing feature on EDGE1 and EDGE2

To configure EDGE1 and EDGE2 in a cluster, you must install the Network Load Balancing feature on both EDGE1 and EDGE2.

To install Network Load Balancing

1. On EDGE1, in the Server Manager console, in the **Dashboard**, click **Add roles and features**.
2. Click **Next** four times to get to the server feature selection screen.
3. On the **Select features** dialog, select **Network Load Balancing**, click **Add Features**, click **Next**, and then click **Install**.
4. On the **Installation progress** dialog, verify that the installation was successful, and then click **Close**.
5. Repeat this procedure on EDGE2.

Enable load balancing on EDGE1

Use this procedure to enable load balancing and configure the new DIPs on EDGE1.

Enable load balancing

1. On EDGE1, click **Start**, type **RAMgmtUI.exe**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the Remote Access Management console, in the left pane, click **Configuration**, and then in the **Tasks** pane, click **Enable Load Balancing**.
3. In the Enable Load Balancing Wizard, click **Next**.
4. On the **Load Balancing Method** page, click **Use Windows Network Load Balancing (NLB)**, and then click **Next**.
5. On the **External Dedicated IP Addresses** page, in the **IPv4 address** box, type **131.107.0.10**, in the **Subnet mask** box, verify the subnet prefix is **255.255.255.0**, and then click **Next**.
6. On the **Internal Dedicated IP Addresses** page, do the following, and then click **Next**:
   a. In the **IPv4 address** box, type **10.0.0.10** and in the **Subnet mask** box, verify the subnet prefix is **255.255.255.0**.
   b. In the **IPv6 address** box, type **2001:db8:1::10** and in the Subnet prefix length, verify the value is **64**.
7. On the **Summary** page, click **Commit**.
8. On the **Enable Load Balancing** dialog box, click **Close**.
9. In the Enable Load Balancing Wizard, click **Close**.

Add EDGE2 to the load balanced cluster

Use this procedure to add EDGE2 to the NLB cluster.

> **NOTE**
> You should wait two minutes after completing the previous steps before proceeding. After enabling NLB, the RAConfigTask runs and configures the machine with NLB settings. This might take a few minutes to complete, and if the administrator runs another NLB related configuration before the task ends, that configuration will fail.

Add EDGE2 to the cluster

1. On the EDGE1 computer or virtual machine, in the Remote Access Management Console, in the **Tasks** pane, under **Load Balanced Cluster**, click **Add or Remove Servers**.

2. On the **Add or Remove Servers** dialog box, click **Add Server**.
3. On the **Add a Server** wizard, on the **Select Server** page, type **EDGE2**, and then click **Next**.
4. On the **Network Adapters** page, in **External adapter**, make sure that **Internet** is selected, and in **Internal adapter**, make sure that **Corpnet** is selected. Click **Browse**, on the **Windows Security** dialog box, make sure that **IP-HTTPS Certificate** is selected, click **OK**, and then click **Next**.
5. On the **Summary** page, click **Add**.
6. On the **Completion** page, click **Close**.
7. On the **Add or Remove Servers** dialog box, click **Commit**.
8. On the **Adding and Removing Servers** dialog box, click **Close**.
9. On the **Start** screen, type**nlbmgr.exe**, and the press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
10. In the **Network Load Balancing Manager**, click **Internal DA cluster**. In the details pane, make sure that both **EDGE1(Corpnet)** and **EDGE2(Corpnet)** have the status **Converged**.
11. If a server is not **Converged**, in the console tree, right-click the server, point to **Control Host**, and then click **Start**.
12. In the **Network Load Balancing Manager**, click **Internet DA cluster**. Make sure that in the details pane, both **EDGE1(Internet)** and **EDGE2(Internet)** have the status **Converged**.
13. If a server is not **Converged**, in the console tree, right-click the server, point to **Control Host**, and then click **Start**.

STEP 5 Test DirectAccess Connectivity from the Internet and Through the Cluster

12/9/2022 • 4 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

CLIENT1 is now ready for DirectAccess testing.

- Test DirectAccess connectivity from the Internet. Connect CLIENT1 to the simulated Internet. When connected to the simulated Internet, the client is assigned public IPv4 addresses. When a DirectAccess client is assigned a public IPv4 address, it tries to establish a connection to the Remote Access server using an IPv6 transition technology.
- Test DirectAccess client connectivity through the cluster. Test cluster functionality. Before you begin testing, we recommend that you shut down both EDGE1 and EDGE2 for at least five minutes. There are a number of reasons for this, which include ARP cache timeouts and changes related to NLB. When validating NLB configuration in a test lab, you will need to be patient as changes in configuration will not be immediately reflected in connectivity until after a period of time has elapsed. This is important to keep in mind when you carry out the following tasks.

> **TIP**
> We recommend that you clear the Internet Explorer cache before performing this procedure and each time you test the connection through a different Remote Access server to make sure that you are testing the connection and not retrieving the webpages from the cache.

Test DirectAccess connectivity from the Internet

1. Unplug CLIENT1 from the corpnet switch and connect it to the Internet switch. Wait for 30 seconds.
2. In an elevated Windows PowerShell window, type **ipconfig /flushdns** and press ENTER. This flushes name resolution entries that may still exist in the client DNS cache from when the client computer was connected to the corpnet.
3. In the Windows PowerShell window, type **Get-DnsClientNrptPolicy** and press ENTER.

   The output shows the current settings for the Name Resolution Policy Table (NRPT). These settings indicate that all connections to .corp.contoso.com should be resolved by the Remote Access DNS server, with the IPv6 address 2001:db8:1::2. Also, note the NRPT entry indicating that there is an exemption for the name nls.corp.contoso.com; names on the exemption list are not answered by the Remote Access DNS server. You can ping the Remote Access DNS server IP address to confirm connectivity to the Remote Access server; for example, you can ping 2001:db8:1::2.
4. In the Windows PowerShell window, type **ping app1** and press ENTER. You should see replies from the IPv6 address for APP1, which in this case is 2001:db8:1::3.
5. In the Windows PowerShell window, type **ping app2** and press ENTER. You should see replies from the NAT64 address assigned by EDGE1 to APP2, which in this case is fdc9:9f4e:eb1b:7777::a00:4.

   The ability to ping APP2 is important, because success indicates that you were able to establish a connection using NAT64/DNS64, as APP2 is an IPv4 only resource.

6. Leave the Windows PowerShell window open for the next procedure.
7. Open Internet Explorer, in the Internet Explorer address bar, enter **https://app1/** and press ENTER. You will see the default IIS website on APP1.
8. In the Internet Explorer address bar, enter **https://app2/** and press ENTER. You will see the default website on APP2.
9. On the **Start** screen, type**\\App2\Files**, and then press ENTER. Double-click the New Text Document file.

   This demonstrates that you were able to connect to an IPv4 only server using SMB to obtain a resource in the resource domain.
10. On the **Start** screen, type**wf.msc**, and then press ENTER.
11. In the **Windows Firewall with Advanced Security** console, notice that only the **Private** or **Public Profile** is active. The Windows Firewall must be enabled for DirectAccess to work correctly. If the Windows Firewall is disabled, DirectAccess connectivity does not work.
12. In the left pane of the console, expand the **Monitoring** node, and click the **Connection Security Rules** node. You should see the active connection security rules: **DirectAccess Policy-ClientToCorp**, **DirectAccess Policy-ClientToDNS64NAT64PrefixExemption**, **DirectAccess Policy-ClientToInfra**, and **DirectAccess Policy-ClientToNlaExempt**. Scroll the middle pane to the right to show the **1st Authentication Methods** and **2nd Authentication Methods** columns. Notice that the first rule (ClientToCorp) uses Kerberos V5 to establish the intranet tunnel and the third rule (ClientToInfra) uses NTLMv2 to establish the infrastructure tunnel.
13. In the left pane of the console, expand the **Security Associations** node, and click the **Main Mode** node. Notice the infrastructure tunnel security associations using NTLMv2 and the intranet tunnel security association using Kerberos V5. Right-click the entry that shows **User (Kerberos V5)** as the **2nd Authentication Method** and click **Properties**. On the **General** tab, notice the **Second authentication Local ID** is **CORP\User1**, indicating that User1 was able to successfully authenticate to the CORP domain using Kerberos.

Test DirectAccess client connectivity through the cluster

1. Perform a graceful shutdown on EDGE2.

   You can use the Network Load Balancing Manager to view the status of the servers when running these tests.
2. On CLIENT1, in the Windows PowerShell window, type **ipconfig /flushdns** and press ENTER. This flushes name resolution entries that may still exist in the client DNS cache.
3. In the Windows PowerShell window, ping APP1, and APP2. You should receive replies from both of these resources.
4. On the **Start** screen, type**\\app2\files**. You should see the shared folder on the APP2 computer. The ability to open the file share on APP2 indicates that the second tunnel, which requires Kerberos authentication for the user, is working correctly.
5. Open Internet Explorer, and then open the websites https://app1/ and https://app2/. The ability to open both websites confirms that both the first and second tunnels are up and functioning. Close Internet Explorer.
6. Start the EDGE2 computer.
7. On EDGE1 perform a graceful shutdown.

8. Wait for 5 minutes, and then return to CLIENT1. Perform steps 2-5. This confirms that CLIENT1 was able to transparently fail over to EDGE2 after EDGE1 became unavailable.

STEP 6 Test DirectAccess Client Connectivity from Behind a NAT Device

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

When a DirectAccess client is connected to the Internet from behind a NAT device or a web proxy server, the DirectAccess client uses either Teredo or IP-HTTPS to connect to the Remote Access server.

If the NAT device enables outbound UDP port 3544 to the Remote Access server's public IP address, then Teredo is used. If Teredo access is not available, the DirectAccess client falls back to IP-HTTPS over outbound TCP port 443, which enables access through firewalls or web proxy servers over the traditional SSL port.

If the web proxy requires authentication, the IP-HTTPS connection will fail. IP-HTTPS connections also fail if the web proxy performs outbound SSL inspection, due to the fact that the HTTPS session is terminated at the web proxy instead of the Remote Access server. In this section you will perform the same tests performed when connecting using a 6to4 connection in the previous section.

The following procedures are performed on both client computers:

1. Test Teredo connectivity. The first set of tests are performed when the DirectAccess client is configured to use Teredo. This is the automatic setting when the NAT device allows outbound access to UDP port 3544.
2. Test IP-HTTPS connectivity. The second set of tests are performed when the DirectAccess client is configured to use IP-HTTPS. In order to demonstrate IP-HTTPS connectivity, Teredo is disabled on the client computers.

> **TIP**
> It is recommended that you clear the Internet Explorer cache before performing these procedures to ensure that you are testing the connection and not retrieving the website pages from the cache.

Prerequisites

Before performing these tests, unplug CLIENT1 from the Internet switch and connect it to the Homenet switch. If asked what type of network you want to define the current network, select **Home Network**.

Start EDGE1 and EDGE2 if they are not already running.

Test Teredo connectivity

1. On CLIENT1, open an elevated Windows PowerShell window, type **ipconfig /all** and press ENTER.
2. Examine the output of the ipconfig command.

   CLIENT1 is now connected to the Internet from behind a NAT device and is assigned a private IPv4 address. When the DirectAccess client is behind a NAT device and assigned a private IPv4 address, the preferred IPv6 transition technology is Teredo. If you look at the output of the ipconfig command, you should see a section for Tunnel adapter Teredo Tunneling Pseudo-Interface and then a description Microsoft Teredo Tunneling Adapter, with an IP address that starts with 2001: consistent with being a Teredo address. If you do not see the Teredo section, enable Teredo with the following command: **netsh**

interface Teredo set state enterpriseclient and then rerun the ipconfig command. You will not see a default gateway listed for the Teredo tunnel adapter.

3. In the Windows PowerShell window, type **ipconfig /flushdns** and press ENTER.

   This will flush name resolution entries that may still exist in the client DNS cache from when the client computer was connected to the Internet.

4. In the Windows PowerShell window, type **Get-DnsClientNrptPolicy** and press ENTER.

   The output shows the current settings for the Name Resolution Policy Table (NRPT). These settings indicate that all connections to .corp.contoso.com should be resolved by the Remote Access DNS server, with the IPv6 address of 2001:db8:1::2. Also, note the NRPT entry indicating that there is an exemption for the name nls.corp.contoso.com; names on the exemption list are not answered by the Remote Access DNS server. You can ping the Remote Access DNS server IP address to confirm connectivity to the Remote Access server; for example, you can ping 2001:db8:1::2 in this example.

5. In the Windows PowerShell window, type **ping app1** and press ENTER. You should see replies from the IPv6 address of APP1, 2001:db8:1::3.

6. In the Windows PowerShell window, type **ping app2** and press ENTER. You should see replies from the NAT64 address assigned by EDGE1 to APP2, which in this case is fdc9:9f4e:eb1b:7777::a00:4.

7. Leave the Windows PowerShell window open for the next procedure.

8. Open Internet Explorer, in the Internet Explorer address bar, enter **https://app1/** and press ENTER. You will see the default IIS website on APP1.

9. In the Internet Explorer address bar, enter **https://app2/** and press ENTER. You will see the default website on APP2.

10. On the **Start** screen, type**\\App2\Files**, and then press ENTER. Double-click the New Text Document file. This demonstrates that you were able to connect to an IPv4 only server using SMB to obtain a resource on an IPv4 only host.

Test IP-HTTPS connectivity

1. Open an elevated Windows PowerShell window, type **netsh interface teredo set state disabled** and press ENTER. This disables Teredo on the client computer and enables the client computer to configure itself to use IP-HTTPS. An **Ok** response appears when the command completes.

2. In the Windows PowerShell window, type **ipconfig /all** and press ENTER.

3. Examine the output of the ipconfig command. This computer is now connected to the Internet from behind a NAT device and is assigned a private IPv4 address. Teredo is disabled and the DirectAccess client falls back to IP-HTTPS. When you look at the output of the ipconfig command, you see a section for Tunnel adapter iphttpsinterface with an IP address that starts with 2001:db8:1:100 consistent with this being an IP-HTTPS address based on the prefix that was configured when setting up DirectAccess. You will not see a default gateway listed for the IP-HTTPS tunnel adapter.

4. In the Windows PowerShell window, type **ipconfig /flushdns** and press ENTER. This will flush name resolution entries that may still exist in the client DNS cache from when the client computer was connected to the corpnet.

5. In the Windows PowerShell window, type **ping app1** and press ENTER. You should see replies from the IPv6 address of APP1, 2001:db8:1::3.

6. In the Windows PowerShell window, type **ping app2** and press ENTER. You should see replies from the NAT64 address assigned by EDGE1 to APP2, which in this case is fdc9:9f4e:eb1b:7777::a00:4.

7. Open Internet Explorer, in the Internet Explorer address bar, enter **https://app1/** and press ENTER. You will see the default IIS site on APP1.

8. In the Internet Explorer address bar, enter **https://app2/** and press ENTER. You will see the default website on APP2.

9. On the **Start** screen, type**\\App2\Files**, and then press ENTER. Double-click the New Text Document file. This demonstrates that you were able to connect to an IPv4 only server using SMB to obtain a resource on an IPv4 only host.

STEP 7 Test Connectivity When Returning to the Corpnet

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Many of your users will move between remote locations and the corpnet, so it's important that when they return to the corpnet that they are able to access resources without having to make any configuration changes. Remote Access makes this possible because when the DirectAccess client returns to the corpnet, it is able to make a connection to the network location server. Once the HTTPS connection is successfully established to the network location server, the DirectAccess client disables the DirectAccess client configuration and uses a direct connection to corpnet.

Test connectivity on CLIENT1

1. Shut down CLIENT1 and then unplug CLIENT1 from the Homenet subnet or virtual switch and connect it to the Corpnet subnet or virtual switch. Turn on CLIENT1, and log on as CORP\User1.
2. Open an elevated Windows PowerShell window, type **ipconfig /all**, and press ENTER. The output will indicate that CLIENT1 has a local IP address, and that there is no active 6to4, Teredo, or IP-HTTPS tunnel.
3. Test connectivity to the network share on APP2. On the **Start** screen, type **\\APP2\Files**, and then press ENTER. You will be able to open the file in that folder.

STEP 8 Snapshot the DirectAccess Cluster-NLB Configuration

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This completes the DirectAccess test lab. To save this configuration so that you can quickly return to a working DirectAccess with NLB cluster configuration from which you can test other DirectAccess modular test lab guides, test lab guide extensions, or for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots DirectAccess cluster and NLB. If your lab uses physical computers, create disk images to save the DirectAccess test lab configuration.

Test Lab Guide: Demonstrate a DirectAccess Multisite Deployment

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Remote Access is a server role in the Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012 operating systems that enables remote users to securely access internal network resources using DirectAccess or RRAS VPN. This guide contains step-by-step instructions for extending the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6 to demonstrate Remote Access in a multisite scenario.

Deploying Remote Access in a multisite scenario enables you to configure Remote Access servers in geographically diverse locations. Previously, remote users were required to always connect to the corporate network through a particular DirectAccess server. With Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 and Windows 10 or Windows 8, you can configure entry points for each geographic location in your deployment. Each entry point can be a single Remote Access server or a cluster of Remote Access servers. Remote users have the option to connect to any of the organization's Remote Access entry points. For example, if a remote user usually connects to the Remote Access entry point located in Asia, but then goes on a business trip to Europe, the client computer automatically connects to the closest Remote Access entry point.

About this guide

This guide contains instructions for configuring and demonstrating Remote Access using nine servers and three client computers. The completed Remote Access multisite test lab simulates an intranet, the Internet, and a home network and demonstrates Remote Access functionality in different Internet connection scenarios.

> **IMPORTANT**
>
> This lab is a proof of concept using the minimum number of computers. The configuration detailed in this guide is for test lab purposes only, and is not to be used in a production environment.

Overview of the Test Lab Scenario OTP Authentication and RSA SecurID

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Remote Access is a server role in the Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012 operating systems that enables remote users to securely access internal network resources using DirectAccess or virtual private networks (VPNs) with the Routing and Remote Access Service (RRAS). This guide contains step-by-step instructions for extending the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6 to demonstrate a Remote Access one-time password (OTP) configuration.

> **WARNING**
>
> The design of this test lab guide includes infrastructure servers, such as a domain controller and a certification authority (CA) that are running either Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 . Using this test lab guide to configure infrastructure servers that are running other operating systems has not been tested, and instructions for configuring other operating systems are not included in this guide.

About this guide

Remote Access in Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012 adds support for client authentication with OTP. For the purposes of this test lab only RSA SecurID is used to demonstrate OTP functionality with Remote Access. Other RADIUS based OTP solutions are supported as well, but are outside the scope of this test lab. This guide contains instructions for configuring and demonstrating Remote Access using six servers and two client computers. The completed Remote Access with OTP test lab simulates an intranet, the Internet, and a home network, and demonstrates Remote Access functionality in different Internet connection scenarios.

> **IMPORTANT**
>
> This lab is a proof of concept using the minimum number of computers. The configuration detailed in this guide is for test lab purposes only, and is not to be used in a production environment.

Configuration Requirements

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The following components are required to configure Remote Access in the test lab:

- The product disc or files for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012.
- Nine computers or virtual machines that meet the minimum hardware requirements for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 ; three of these computers have two network adapters installed.
- The product disc or files for Windows 10® or Windows® 8 .
- The product disc or files for Windows 7 Ultimate.
- Three computers or virtual machines that meet the minimum hardware requirements for Windows 10®, Windows 8 or Windows 7 ; one of these computers has two network adapters installed.

Steps for Configuring the Test Lab

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The following steps describe how to configure the Remote Access infrastructure, configure the Remote Access servers and clients and test DirectAccess connectivity from the Internet and Homenet subnets.

In this test lab guide you will build a multisite Remote Access deployment by performing the following steps:

- STEP 1: Complete the Base Configuration. Complete all the steps in the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6.
- STEP 2: Install and configure ROUTER1. ROUTER1 provides routing and forwarding functionality between the Corpnet and 2-Corpnet subnets.
- STEP 3: Install and configure CLIENT2. CLIENT2 is a Windows 7 client computer that is used to demonstrate the backwards compatibility of a Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 Remote Access deployment.
- STEP 4: Configure APP1. Configure APP1 with ROUTER1 as the default gateway and 2-DC1 as the alternate DNS server.
- STEP 5: Configure DC1. Configure DC1 with an additional Active Directory site and additional security groups for Windows 7 client computers.
- STEP 6: Install and configure 2-DC1. In a multisite deployment, you have two or more domains and sites. 2-DC1 provides domain controller and DNS services for the corp2.corp.contoso.com domain.
- STEP 7: Install and configure 2-APP1. 2-APP1 is a web and file server in the 2-Corpnet network.
- STEP 8: Configure INET1. INET1 simulates the Internet in this test lab guide. You must configure a DNS entry that resolves to the public IP address of 2-EDGE1.
- STEP 9: Configure EDGE1. Configure the 2-Corpnet DNS server and routing on EDGE1.
- STEP 10: Install and configure 2-EDGE1. Two Remote Access servers are required in a multisite deployment. 2-EDGE1 provides Remote Access services for the second domain.
- STEP 11: Configure multisite deployment. After configuring both Remote Access servers, you can configure your multisite deployment.
- STEP 12: Test DirectAccess connectivity. Test DirectAccess connectivity from both client computers from the Internet subnet through EDGE1 and 2-EDGE1.
- STEP 13: Test DirectAccess connectivity from behind a NAT device. Test DirectAccess connectivity from behind a NAT device.
- STEP 14: Snapshot the configuration. After completing the test lab, take a snapshot of the working Remote Access multisite deployment so that you can return to it later to test additional scenarios.

Step 1 Complete the DirectAccess Configuration

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first step is to complete all the steps in the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6. If you have already completed the steps in this test lab guides and saved a snapshot or disk image of the test lab, you can restore the snapshot or image and begin with the next step.

STEP 2 Install and Configure ROUTER1

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

In this multisite test lab guide, the router computer provides an IPv4 and IPv6 bridge between the Corpnet and 2-Corpnet subnets, and acts as a router for IP-HTTPS and Teredo traffic.

- Install the operating system on ROUTER1
- Configure TCP/IP properties and rename the computer
- Turn off the firewall
- Configure routing and forwarding

Install the operating system on ROUTER1

First, install Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012.

To install the operating system on ROUTER1

1. Start the installation of Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 (full installation).
2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect ROUTER1 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 , and then disconnect from the Internet.
4. Connect ROUTER1 to the Corpnet and 2-Corpnet subnets.

Configure TCP/IP properties and rename the computer

Configure TCP/IP settings on the router and rename the computer to ROUTER1.

To configure TCP/IP properties and rename the computer

1. In the Server Manager console, click **Local Server**, and then in the **Properties** area, next to **Wired Ethernet Connection**, click the link.
2. In the **Network Connections** window, right-click the network adapter that is connected to Corpnet, click **Rename**, type **Corpnet**, and press ENTER.
3. Right-click **Corpnet**, and then click **Properties**.
4. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
5. Click **Use the following IP address**. In **IP address**, type **10.0.0.254**. In **Subnet mask**, type **255.255.255.0**, and then click **OK**.
6. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
7. Click **Use the following IPv6 address**. In **IPv6 address**, type **2001:db8:1::fe**. In **Subnet prefix length**, type **64**, and then click **OK**.

8. On the **Corpnet Properties** dialog box click **Close**.
9. In the **Network Connections** window, right-click the network adapter that is connected to 2-Corpnet, click **Rename**, type **2-Corpnet**, and press ENTER.
10. Right-click **2-Corpnet**, and then click **Properties**.
11. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
12. Click **Use the following IP address**. In **IP address**, type **10.2.0.254**. In **Subnet mask**, type **255.255.255.0**, and then click **OK**.
13. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
14. Click **Use the following IPv6 address**. In **IPv6 address**, type **2001:db8:2::fe**. In **Subnet prefix length**, type **64**, and then click **OK**.
15. On the **2-Corpnet Properties** dialog box click **Close**.
16. Close the **Network Connections** window.
17. In the Server Manager console, in **Local Server**, in the **Properties** area, next to **Computer name**, click the link.
18. On the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
19. On the **Computer Name/Domain Changes** dialog box, in **Computer name**, type **ROUTER1**, and then click **OK**.
20. When you are prompted that you must restart the computer, click **OK**.
21. On the **System Properties** dialog box, click **Close**.
22. When you are prompted to restart the computer, click **Restart Now**.
23. After the computer has restarted, log on with the local Administrator account.

Turn off the firewall

This computer is configured only to provide routing between the Corpnet and 2-Corpnet subnets; therefore, the firewall must be turned off.

To turn off the firewall

1. On the **Start** screen, type**wf.msc**, and then press ENTER.
2. In Windows Firewall with Advanced Security, in the **Actions** pane, click **Properties**.
3. On the **Windows Firewall with Advanced Security** dialog box, on the **Domain Profile** tab, in **Firewall state**, click **Off**.
4. On the **Windows Firewall with Advanced Security** dialog box, on the **Private Profile** tab, in **Firewall state**, click **Off**.
5. On the **Windows Firewall with Advanced Security** dialog box, on the **Public Profile** tab, in **Firewall state**, click **Off**, and then click **OK**.
6. Close Windows Firewall with Advanced Security.

Configure routing and forwarding

To provide routing and forwarding services between the Corpnet and 2-Corpnet subnets, you must enable

forwarding on the network interfaces and configure static routes between the subnets.

To configure static routes

1. On the **Start** screen, type **cmd.exe**, and then press ENTER.
2. Enable forwarding on both the IPv4 and IPv6 interfaces of both network adapters using the following commands. After entering each command, press ENTER.

```
netsh interface IPv4 set interface Corpnet forwarding=enabled
netsh interface IPv4 set interface 2-Corpnet forwarding=enabled
netsh interface IPv6 set interface Corpnet forwarding=enabled
netsh interface IPv6 set interface 2-Corpnet forwarding=enabled
```

3. Enable IP-HTTPS routing between the Corpnet and 2-Corpnet subnets.

```
netsh interface IPv6 add route 2001:db8:1:1000::/59 Corpnet 2001:db8:1::2
netsh interface IPv6 add route 2001:db8:2:2000::/59 2-Corpnet 2001:db8:2::20
```

4. Enable Teredo routing between the Corpnet and 2-Corpnet subnets.

```
netsh interface IPv6 add route 2001:0:836b:2::/64 Corpnet 2001:db8:1::2
netsh interface IPv6 add route 2001:0:836b:14::/64 2-Corpnet 2001:db8:2::20
```

5. Close the Command Prompt window.

STEP 3 Install and Configure CLIENT2

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

CLIENT2 is a Windows 7® computer that is used to demonstrate the backwards compatibility of Remote Access running on Windows Server 2016 servers.

1. To install the operating system on CLIENT2. Install Windows® 7 Enterprise or Windows® 7 Ultimate on CLIENT2.
2. To join CLIENT2 to the CORP domain. Join CLIENT2 to the corp.contoso.com domain.

To install the operating system on CLIENT2

1. Start the installation of Windows 7.
2. When you are prompted for a user name, type **User1**. When you are prompted for a computer name, type **CLIENT2**.
3. When you are prompted for a password, type a strong password twice.
4. When you are prompted for protection settings, click **Use recommended settings**.
5. When you are prompted for your computer's current location, click **Work network**.
6. Connect CLIENT2 to a network that has Internet access and run Windows Update to install the latest updates for Windows 7 , and then disconnect from the Internet.
7. Connect CLIENT2 to the Corpnet subnet.

User account control

When you configure the Windows 7 operating system, you are required to click **Continue** on the **User Account Control** (UAC) dialog box for some tasks. Several of the configuration tasks require UAC approval. When you are prompted, always click **Continue** to authorize these changes.

To join CLIENT2 to the CORP domain

1. Click **Start**, right-click **Computer**, and then click **Properties**.
2. On the **System** page, in the **Computer name, domain, and workgroup settings** area, click **Change settings**.
3. On the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
4. On the **Computer Name/Domain Changes** dialog box, click **Domain**, type **corp.contoso.com**, and then click **OK**.
5. When you are prompted for a user name and password, type the user name and password for the User1 domain account, and then click **OK**.
6. When you see a dialog box that welcomes you to the corp.contoso.com domain, click **OK**.
7. When you see a dialog box that prompts you to restart the computer, click **OK**.

8. On the **System Properties** dialog box, click **Close**, and when you see a dialog that prompts you to restart the computer, click **Restart Now**.

9. After the computer restarts, log on as CORP\User1.

STEP 4 Configure APP1

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Configure static IPv6 addressing and gateway settings to enable APP1 access to the 2-Corpnet subnet.

- To configure the default gateway and DNS server. The multisite configuration uses the ROUTER1 computer as a default gateway. Configure the default gateway on APP1.

To configure the default gateway and DNS server

1. In the Server Manager console, click **Local Server**, and then in the **Properties** area, next to **Wired Ethernet Connection**, click the link.
2. In the **Network Connections** window, right-click **Wired Ethernet Connection**, and then click **Properties**.
3. On the **Wired Ethernet Connection Properties** dialog box, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4. In **Default gateway**, type **10.0.0.254**, and in **Alternate DNS server**, type **10.2.0.1**, and then click **OK**.
5. On the **Wired Ethernet Connection Properties** dialog box, click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
6. In **Default gateway**, type **2001:db8:1::fe**. In **Alternate DNS server**, type **2001:db8:2::1**, and then click **OK**.
7. On the **Wired Ethernet Connection Properties** dialog box, click **Close**, and then close the **Network Connections** window.

STEP 5 Configure DC1

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

DC1 acts as a domain controller, DNS server, and DHCP server for the corp.contoso.com domain.

To configure Remote Access to use a multisite topology, it is necessary to add an additional Active Directory Domain Services (AD DS) site for the second domain controller 2-DC1, and to configure routing between the subnets.

1. To configure the default gateway on the domain controller. Configure the default gateway on DC1.
2. Create security groups for Windows 7 DirectAccess clients on DC1. When DirectAccess is configured, it automatically creates Group Policy Objects (GPOs) and GPO settings that are applied to DirectAccess clients and servers. The DirectAccess client GPO is applied to specific Active Directory security groups.
3. To add a new AD DS site. Create a second AD DS site.

To configure the default gateway on the domain controller

1. In the Server Manager console, click **Local Server**, and then in the **Properties** area, next to **Wired Ethernet Connection**, click the link.
2. In the Network Connections window, right-click **Wired Ethernet Connection**, and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4. In **Default gateway**, type **10.0.0.254**, and in **Alternate DNS server**, type **10.2.0.1**, and then click **OK**.
5. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
6. In **Default gateway**, type **2001:db8:1::fe**, and in **Alternate DNS server**, type **2001:db8:2::1**, and then click **OK**.
7. On the **Wired Ethernet Connection Properties** dialog box, click **Close**.
8. Close the **Network Connections** window.

Create security groups for Windows 7 DirectAccess clients on DC1

Create the DirectAccess security groups for Windows 7 with the following procedure.

Windows 7 client computers must be members of separate security groups because they are able to connect to internal resources through a single entry point only. When enabling Multisite support or adding entry points, if Windows 7 support is requested, then a separate GPO will be automatically created by DirectAccess for Windows 7 clients for each entry point.

Create security groups

1. On the **Start** screen, type**dsa.msc**, and then press ENTER.
2. In the left pane, expand **corp.contoso.com**, click **Users**, then right-click **Users**, point to **New**, and then click **Group**.

3. On the **New Object - Group** dialog box, under **Group name**, enter **Win7_Clients_Site1**.
4. Under **Group scope**, click **Global**, under **Group type**, click **Security**, and then click **OK**.
5. Double-click the **Win7_Clients_Site1** security group, and on the **Win7_Clients_Site1 Properties** dialog box, click the **Members** tab.
6. On the **Members** tab, click **Add**.
7. On the **Select Users, Contacts, Computers, or Service Accounts** dialog box, click **Object Types**. On the **Object Types** dialog box, select **Computers**, and then click **OK**.
8. In **Enter the object names to select**, type **client2**, and then click **OK**, and then on the **Win7_Clients_Site1 Properties** dialog box click **OK**.
9. In the **Active Directory Users and Computers** console, in the left pane, right-click **Users**, point to **New**, and then click **Group**.
10. On the **New Object - Group** dialog box, under **Group name**, enter **Win7_Clients_Site2**.
11. Under **Group scope**, click **Global**, under **Group type**, click **Security**, and then click **OK**.
12. Close the **Active Directory Users and Computers** console.

To add a new AD DS site

1. On the **Start** screen, type**dssite.msc**, and then press ENTER.
2. In the Active Directory Sites and Services console, in the console tree, right-click **Sites**, and then click **New Site**.
3. On the **New Object - Site** dialog box, in the **Name** box, type **Second-Site**.
4. In the list box, click **DEFAULTIPSITELINK**, and then click **OK** twice.
5. In the console tree, expand **Sites**, right-click **Subnets**, and then click **New Subnet**.
6. On the **New Object - Subnet** dialog box, under **Prefix**, type **10.0.0.0/24**, in the **Select a site object for this prefix** list, click **Default-First-Site-Name**, and then click **OK**.
7. In the console tree, right-click **Subnets**, and then click **New Subnet**.
8. On the **New Object - Subnet** dialog box, under **Prefix**, type **2001:db8:1::/64**, in the **Select a site object for this prefix** list, click **Default-First-Site-Name**, and then click **OK**.
9. In the console tree, right-click **Subnets**, and then click **New Subnet**.
10. On the **New Object - Subnet** dialog box, under **Prefix**, type **10.2.0.0/24**, in the **Select a site object for this prefix** list, click **Second-Site**, and then click **OK**.
11. In the console tree, right-click **Subnets**, and then click **New Subnet**.
12. On the **New Object - Subnet** dialog box, under **Prefix**, type **2001:db8:2::/64**, in the **Select a site object for this prefix** list, click **Second-Site**, and then click **OK**.
13. Close Active Directory Sites and Services.

STEP 6 Install and Configure 2-DC1

12/9/2022 • 6 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

2-DC1 provides the following services:

- A domain controller for the corp2.corp.contoso.com Active Directory Domain Services (AD DS) domain.
- A DNS server for the corp2.corp.contoso.com DNS domain.

2-DC1 configuration consists of the following:

- Install the operating system on 2-DC1
- Configure TCP/IP properties
- Configure 2-DC1 as a domain controller and DNS server
- Provide Group Policy permissions to CORP\User1
- Allow CORP2 computers to obtain computer certificates
- Force replication between DC1 and 2-DC1

Install the operating system on 2-DC1

First, install Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012.

To install the operating system on 2-DC1

1. Start the installation of Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 .
2. Follow the instructions to complete the installation, specifying Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 (full installation) and a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect 2-DC1 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 , and then disconnect from the Internet.
4. Connect 2-DC1 to the 2-Corpnet subnet.

Configure TCP/IP properties

Configure the TCP/IP protocol with static IP addresses.

To configure TCP/IP on 2-DC1

1. In the Server Manager console, click **Local Server**, and then in the **Properties** area, next to **Wired Ethernet Connection**, click the link.
2. In **Network Connections**, right-click **Wired Ethernet Connection**, and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4. Click **Use the following IP address**. In **IP address**, type **10.2.0.1**. In **Subnet mask**, type **255.255.255.0**. In **Default gateway**, type **10.2.0.254**. Click **Use the following DNS server**

addresses, in **Preferred DNS server**, type **10.2.0.1**, and in **Alternate DNS server**, type **10.0.0.1**.

5. Click **Advanced**, and then click the **DNS** tab.
6. In **DNS suffix for this connection**, type **corp2.corp.contoso.com**, and then click **OK** twice.
7. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
8. Click **Use the following IPv6 address**. In **IPv6 address**, type **2001:db8:2::1**. In **Subnet prefix length**, type **64**. In **Default gateway**, type **2001:db8:2::fe**. Click **Use the following DNS server addresses**, in **Preferred DNS server**, type **2001:db8:2::1**, and in **Alternate DNS server**, type **2001:db8:1::1**.
9. Click **Advanced**, and then click the **DNS** tab.
10. In **DNS suffix for this connection**, type **corp2.corp.contoso.com**, and then click **OK** twice.
11. On the **Wired Ethernet Connection Properties** dialog box, click **Close**.
12. Close the **Network Connections** window.
13. In the Server Manager console, in **Local Server**, in the **Properties** area, next to **Computer name**, click the link.
14. On the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
15. On the **Computer Name/Domain Changes** dialog box, in **Computer name**, type **2-DC1**, and then click **OK**.
16. When you are prompted that you must restart the computer, click **OK**.
17. On the **System Properties** dialog box, click **Close**.
18. When you are prompted to restart the computer, click **Restart Now**.
19. After restarting, login using the local administrator account.

Configure 2-DC1 as a domain controller and DNS server

Configure 2-DC1 as a domain controller for the corp2.corp.contoso.com domain and as a DNS server for the corp2.corp.contoso.com DNS domain.

To configure 2-DC1 as a domain controller and DNS server

1. In the Server Manager console, on the **Dashboard**, click **Add roles and features**.
2. Click **Next** three times to get to the server role selection screen
3. On the **Select server roles** page, select **Active Directory Domain Services**. Click **Add Features** when prompted, and then click **Next** three times.
4. On the **Confirm installation selections** page, click **Install**.
5. When the installation completes successfully, click **Promote this server to a domain controller**.
6. In the Active Directory Domain Services Configuration Wizard, on the **Deployment Configuration** page, click **Add a new domain to an existing forest**.
7. In **Parent domain name**, type **corp.contoso.com**, in **New domain name**, type **corp2**.
8. Under **Supply the credentials to perform this operation**, click **Change**. On the **Windows Security** dialog box, in **User name**, type **corp.contoso.com\Administrator**, and in **Password**, enter the corp\Administrator password, click **OK**, and then click **Next**.

9. On the **Domain Controller Options** page, make sure that the **Site name** is **Second-Site**. Under **Type the Directory Services Restore Mode (DSRM) password**, in **Password** and **Confirm password**, type a strong password twice, and then click **Next** five times.
10. On the **Prerequisites Check** page, after the prerequisites are validated, click **Install**.
11. Wait until the wizard completes the configuration of Active Directory and DNS services, and then click **Close**.
12. After the computer restarts, log in to the CORP2 domain using the Administrator account.

Provide Group Policy permissions to CORP\User1

Use this procedure to provide the CORP\User1 user with full permissions to create and change corp2 Group Policy Objects.

To provide Group Policy permissions

1. On the **Start** screen, type**gpmc.msc**, and then press ENTER.
2. In the Group Policy Management console, open **Forest: corp.contoso.com/Domains/corp2.corp.contoso.com**.
3. In the details pane, click the **Delegation** tab. In the **Permission** drop-down list, click **Link GPOs**.
4. Click **Add**, and on the new **Select User, Computer, or Group** dialog box, click **Locations**.
5. On the **Locations** dialog box, in the **Location** tree, click **corp.contoso.com**, and click **OK**.
6. In **Enter the object name to select** type **User1**, click **OK**, and on the **Add Group or User** dialog box, click **OK**.
7. In the Group Policy Management console, in the tree, click **Group Policy Objects**, and in the details pane click the **Delegation** tab.
8. Click **Add**, and on the new **Select User, Computer, or Group** dialog box, click **Locations**.
9. On the **Locations** dialog box, in the **Location** tree, click **corp.contoso.com**, and click **OK**.
10. In **Enter the object name to select** type **User1**, click **OK**.
11. In the Group Policy Management console, in the tree, click **WMI Filters**, and in the details pane click the **Delegation** tab.
12. Click **Add**, and on the new **Select User, Computer, or Group** dialog box, click **Locations**.
13. On the **Locations** dialog box, in the **Location** tree, click **corp.contoso.com**, and click **OK**.
14. In **Enter the object name to select** type **User1**, click **OK**. On the **Add Group or User** dialog box, make sure that **Permissions** are set to **Full control**, and then click **OK**.
15. Close the Group Policy Management console.

Allow CORP2 computers to obtain computer certificates

Computers in the CORP2 domain must obtain computer certificates from the certification authority on APP1. Perform this procedure on APP1.

To allow CORP2 computers to automatically obtain computer certificates

1. On APP1, click **Start**, type **certtmpl.msc**, and then press ENTER.
2. In the **Certificates Template Console**, in the middle pane, double-click **Client-Server**

Authentication.

3. On the **Client-Server Authentication Properties** dialog box, click the **Security** tab.
4. Click **Add**, and on the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Locations**.
5. On the **Locations** dialog box, in **Location**, expand **corp.contoso.com**, click **corp2.corp.contoso.com**, and then click **OK**.
6. In **Enter the object names to select**, type **Domain Admins; Domain Computers** and then click **OK**.
7. On the **Client-Server Authentication Properties** dialog box, in **Group or user names**, click **Domain Admins (CORP2\Domain Admins)**, and in **Permissions for Domain Admins**, in the **Allow** column, select **Write** and **Enroll**.
8. In **Group or user names**, click **Domain Computers (CORP2\Domain Computers)**, and in **Permissions for Domain Computers**, in the **Allow** column, select **Enroll** and **Autoenroll**, and then click **OK**.
9. Close the Certificate Templates Console.

Force replication between DC1 and 2-DC1

Before you can enroll for certificates on 2-EDGE1, you must force the replication of settings from DC1 to 2-DC1. This operation should be done on DC1.

To force replication

1. On DC1, click **Start**, and then click **Active Directory Sites and Services**.
2. In the Active Directory Sites and Services console, in the tree, expand **Inter-Site Transports**, and then click **IP**.
3. In the details pane, double-click **DEFAULTIPSITELINK**.
4. On the **DEFAULTIPSITELINK Properties** dialog box, in **Cost**, type **1**, in **Replicate every**, type **15**, and then click **OK**. Wait for 15 minutes for replication to complete.
5. To force replication now in the console tree, expand **Sites\Default-First-Site-name\Servers\DC1\NTDS Settings**, in the details pane, right-click **<automatically generated>**, click **Replicate Now**, and then on the **Replicate Now** dialog box, click **OK**.
6. To ensure replication has completed successfully do the following:
   a. On the **Start** screen, type**cmd.exe**, and then press ENTER.
   b. Type the following command, and then press ENTER.

      ```
      repadmin /syncall /e /A /P /d /q
      ```

   c. Make sure that all partitions are synchronized with no errors. If not, then rerun the command until no errors are reported before proceeding.
7. Close the Command Prompt window.

STEP 7 Install and Configure 2-APP1

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

2-APP1 provides web and file sharing services. 2-APP1 configuration consists of the following:

- Install the operating system on 2-APP1
- Configure TCP/IP properties
- Join 2-APP1 to the CORP2 domain
- Install the Web Server (IIS) role on 2-APP1
- Create a shared folder on 2-APP1

Install the operating system on 2-APP1

First, install Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012.

To install the operating system on 2-APP1

1. Start the installation of Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 (full installation).
2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect 2-APP1 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 , and then disconnect from the Internet.
4. Connect 2-APP1 to the 2-Corpnet subnet.

Configure TCP/IP properties

Configure TCP/IP properties on 2-APP1.

To configure TCP/IP properties

1. In the Server Manager console, click **Local Server**, and then in the **Properties** area, next to **Wired Ethernet Connection**, click the link.
2. In the **Network Connections** window, right-click **Wired Ethernet Connection**, and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4. Click **Use the following IP address**. In **IP address**, type **10.2.0.3**. In **Subnet mask**, type **255.255.255.0**. In **Default gateway**, type **10.2.0.254**.
5. Click **Use the following DNS server addresses**. In **Preferred DNS server**, type **10.2.0.1**.
6. Click **Advanced**, and then click the **DNS** tab. In **DNS suffix for this connection**, type **corp2.corp.contoso.com**, and click **OK** twice.
7. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.

8. Click **Use the following IPv6 address**. In **IPv6 address**, type **2001:db8:2::3**. In **Subnet prefix length**, type **64**. In **Default gateway**, type **2001:db8:2::fe**. Click **Use the following DNS server addresses**, and in **Preferred DNS server**, type **2001:db8:2::1**.
9. Click **Advanced**, and then click the **DNS** tab.
10. In **DNS suffix for this connection**, type **corp2.corp.contoso.com**, and then click **OK** twice.
11. On the **Wired Ethernet Connection Properties** dialog box click **Close**.
12. Close the **Network Connections** window.

Join 2-APP1 to the CORP2 domain

Join 2-APP1 to the corp2.corp.contoso.com domain.

To join 2-APP1 to the CORP2 domain

1. In the Server Manager console, in **Local Server**, in the **Properties** area, next to **Computer name**, click the link.
2. On the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
3. In **Computer name**, type **2-APP1**. In **Member of**, click **Domain**, type **corp2.corp.contoso.com**, and then click **OK**.
4. When you are prompted for a user name and password, type **Administrator** and its password, and then click **OK**.
5. When you see a dialog box welcoming you to the corp2.corp.contoso.com domain, click **OK**.
6. When you are prompted that you must restart the computer, click **OK**.
7. On the **System Properties** dialog box, click **Close**.
8. When you are prompted to restart the computer, click **Restart Now**.
9. After the computer restarts, click **Switch User**, and then click **Other User** and log on to the CORP2 domain with the Administrator account.

Install the Web Server (IIS) role on 2-APP1

Install the Web Server (IIS) role to make 2-APP1 a web server.

To install the Web Server (IIS) role

1. In the Server Manager console, on the **Dashboard**, click **Add roles and features**.
2. Click **Next** three times to get to the server role selection screen
3. On the **Select server roles** page, select **Web Server (IIS)**, and then click **Next** four times.
4. On the **Confirm installation selections** page, click **Install**.
5. Verify that the installation was successful, and then click **Close**.

Create a shared folder on 2-APP1

Create a shared folder and a text file within the folder on 2-APP1.

To create a shared folder

1. On the **Start** screen, type**explorer.exe**, and then press ENTER.
2. Click **Computer**, then double-click **Local Disk (C:)**.

3. Click **New Folder**, type **Files**, and then press ENTER. Leave the **Local Disk** window open.
4. On the **Start** screen, type**notepad.exe**, right-click **Notepad**, click **Advanced**, and then click **Run as administrator**.
5. In the **Untitled - Notepad** window, type **This is a shared file on 2-APP1**.
6. Click **File**, click **Save**, click **Computer**, double-click **Local Disk (C:)**, and then double-click the **Files** folder.
7. In **File name**, type **example.txt**, and then click **Save**. Close Notepad.
8. In the **Local Disk** window, right-click the **Files** folder, point to **Share with**, and then click **Specific people**.
9. On the **File Sharing** dialog box, in the drop-down list, click **Everyone**, and then click **Add**. In **Permission Level** for **Everyone**, click **Read/Write**.
10. Click **Share**, and then click **Done**.
11. Close the **Local Disk** window.

STEP 8: Configure INET1

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

To enable client computers to connect to Remote Access servers over the Internet, you must configure a DNS entry for 2-EDGE1 on INET1.

To create the 2-EDGE1 DNS entry

1. On the **Start** screen, type **dnsmgmt.msc**, and then press ENTER.
2. In the console tree, open **Forward Lookup Zones**, click **contoso.com**, then right-click **contoso.com**, and then click **New Host (A or AAAA)**.
3. In **Name**, type **2-EDGE1**. In **IP address**, type **131.107.0.20**. Click **Add Host**, click **OK**, and then click **Done**.

STEP 9 Configure EDGE1

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The following procedures are performed on the EDGE1 server:

1. Configure the DNS servers on EDGE1. It is necessary to configure the DNS server from the corp2.corp.contoso.com domain on EDGE1.
2. Configure routing between subnets. Configure routing on EDGE1 to enable communication between the Corpnet and 2-Corpnet subnets.

Configure the DNS servers on EDGE1

1. In the Server Manager console, click **Local Server**, and then in the **Properties** area, next to **Corpnet**, click the link.
2. In the Network Connections window, right-click **Corpnet**, and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4. In **Alternate DNS server**, type **10.2.0.1**. and then click **OK**.
5. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
6. In **Alternate DNS server**, type **2001:db8:2::1** and then click **OK**.
7. On the **Corpnet Properties** dialog box, click **Close**.
8. Close the **Network Connections** window.

Configure routing between subnets

1. On the **Start** screen, type**cmd.exe**, right-click **cmd**, click **Advanced**, and then click **Run as administrator**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the Command Prompt window, enter the following commands. After entering each command, press ENTER.

```
netsh interface IPv4 add route 10.2.0.0/24 Corpnet 10.0.0.254
netsh interface IPv6 add route 2001:db8:2::/64 Corpnet 2001:db8:1::fe
```

3. Close the Command Prompt window.

STEP 10 Install and Configure 2-EDGE1

12/9/2022 • 6 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

2-EDGE1 configuration consists of the following:

- Install the operating system on 2-EDGE1. Install Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 on 2-EDGE1.
- Configure TCP/IP properties. Configure 2-EDGE1 with static addresses on both network interfaces.
- Configure routing between subnets. To enable communication between the Corpnet and 2-Corpnet subnets, you must configure routing.
- Join 2-EDGE1 to the CORP2 domain. Join 2-EDGE1 to the corp2.corp.contoso.com domain.
- Obtain certificates on 2-EDGE1. Certificates are required for the IPsec connection between DirectAccess clients and the Remote Access server, and to authenticate the IP-HTTPS listener when clients connect over HTTPS.
- Provide access to CORP\User1. The user CORP\User1 is the Remote Access administrator. To enable this user to make changes to 2-EDGE1 from EDGE1, you must grant access to the user.
- Install the Remote Access role on 2-EDGE1. To enable a multisite deployment, you must install the Remote Access role on 2-EDGE1.

2-EDGE1 must have two network adapters installed.

Install the operating system on 2-EDGE1

1. Start the installation of Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 .
2. Follow the instructions to complete the installation, specifying Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 (full installation) and a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect 2-EDGE1 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 , and then disconnect from the Internet.
4. Connect one network adapter to the 2-Corpnet subnet and the other to the simulated Internet.

Configure TCP/IP properties

1. In the Server Manager console, click **Local Server**, and then in the **Properties** area, next to **Wired Ethernet Connection**, click the link.
2. In **Network Connections**, right-click the network connection that is connected to the 2-Corpnet subnet, click **Rename**, type **2-Corpnet**, and then press ENTER.
3. Right-click **2-Corpnet**, and then click **Properties**.
4. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

5. Click **Use the following IP address**. In **IP address**, type **10.2.0.20**, in **Subnet mask**, type **255.255.255.0**.
6. Click **Use the following DNS server addresses**. In **Preferred DNS server**, type **10.2.0.1**, and in **Alternate DNS server**, type **10.0.0.1**.
7. Click **Advanced**, and then click the **DNS** tab.
8. In **DNS suffix for this connection**, type **corp2.corp.contoso.com**, and then click **OK** twice.
9. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
10. Click **Use the following IPv6 address**. In **IPv6 address**, type **2001:db8:2::20**, in **Subnet prefix length**, type **64**. Click **Use the following DNS server addresses**, and in **Preferred DNS server**, type **2001:db8:2::1**, in **Alternate DNS server**, type **2001:db8:1::1**.
11. Click **Advanced**, and then click the **DNS** tab.
12. In **DNS suffix for this connection**, type **corp2.corp.contoso.com**, and then click **OK** twice.
13. On the **2-Corpnet Properties** dialog box, click **Close**.
14. In the **Network Connections** window, right-click the network connection that is connected to the Internet subnet, click **Rename**, type **Internet**, and then press ENTER.
15. Right-click **Internet**, and then click **Properties**.
16. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
17. Click **Use the following IP address**. In **IP address**, type **131.107.0.20**. In **Subnet mask**, type **255.255.255.0**.
18. Click **Advanced**. On the **IP Settings** tab, in the **IP addresses** area, click **Add**. On the **TCP/IP Address** dialog box, in **IP address** type **131.107.0.21**, in **Subnet mask** type **255.255.255.0**, and then click **Add**.
19. Click the **DNS** tab.
20. In **DNS suffix for this connection**, type **isp.example.com**, click **OK** twice, and then click **Close**.
21. Close the **Network Connections** window.

Configure routing between subnets

1. On the **Start** screen, type**cmd.exe**, and then press ENTER.
2. In the Command Prompt window, enter the following commands. After entering each command, press ENTER.

```
netsh interface IPv4 add route 10.0.0.0/24 2-Corpnet 10.2.0.254
netsh interface IPv6 add route 2001:db8:1::/64 2-Corpnet 2001:db8:2::fe
```

3. To check network communication between 2-EDGE1 and DC1, type **ping dc1.corp.contoso.com**.
4. Verify that there are four responses from either the IPv4 address, 10.0.0.1, or from the IPv6 address, 2001:db8:1::1.
5. Close the Command Prompt window.

Join 2-EDGE1 to the CORP2 domain

1. In the Server Manager console, in **Local Server**, in the **Properties** area, next to **Computer name**, click the link.
2. On the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
3. On the **Computer Name/Domain Changes** dialog box, in **Computer name**, type **2-EDGE1**. In **Member of**, click **Domain**, type **corp2.corp.contoso.com**, and then click **OK**.
4. If you are prompted for a user name and password, type **Administrator** and its password, and then click **OK**.
5. When you see a dialog box welcoming you to the corp2.corp.contoso.com domain, click **OK**.
6. When you are prompted that you must restart the computer, click **OK**.
7. On the **System Properties** dialog box, click **Close**.
8. When you are prompted to restart the computer, click **Restart Now**.
9. After the computer has restarted, click **Switch User**, and then click **Other User** and log on to the CORP2 domain with the Administrator account.

Obtain certificates on 2-EDGE1

1. On the **Start** screen, type**mmc.exe**, and then press ENTER.
2. In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.
3. On the **Add or Remove Snap-ins** dialog box, click **Certificates**, click **Add**, click **Computer account**, click **Next**, click **Local computer**, click **Finish**, and then click **OK**.
4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal**.
5. Right-click **Personal**, point to **All Tasks**, and then click **Request New Certificate**.
6. Click **Next** twice.
7. On the **Request Certificates** page, select the **Client-Server Authentication** and the **Web Server** check boxes, and then click **More information is required to enroll for this certificate**.
8. On the **Certificate Properties** dialog box, on the **Subject** tab, in the **Subject name** area, in **Type**, select **Common name**.
9. In **Value**, type **2-edge1.contoso.com**, and then click **Add**.
10. In the **Alternative name** area, in **Type**, select **DNS**.
11. In **Value**, enter **2-edge1.contoso.com**, and then click **Add**.
12. On the **General** tab, in **Friendly name**, type **IP-HTTPS Certificate**.
13. Click **OK**, click **Enroll**, and then click **Finish**.
14. In the details pane of the Certificates snap-in, verify that a new certificate with the name 2-edge1.contoso.com was enrolled with Intended Purposes of Server Authentication, and a new certificate with the name 2-edge1.corp2.corp.contoso.com was enrolled with Intended Purposes of Client Authentication and Server Authentication.
15. Close the console window. If you are prompted to save settings, click **No**.

Provide access to CORP\User1

1. On the **Start** screen, type**compmgmt.msc**, and then press ENTER.
2. In the left pane, click **Local Users and Groups**.
3. Double-click **Groups**, and then double-click **Administrators**.
4. On the **Administrators Properties** dialog box, click **Add**, and on the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Locations**.
5. On the **Locations** dialog box, in the **Location** tree, click **corp.contoso.com**, and then click **OK**.
6. In the **Enter the object names to select** type **User1**, and then click **OK**.
7. On the **Administrators Properties** dialog box, click **OK**.
8. Close the Computer Management window.

Install the Remote Access role on 2-EDGE1

1. In the Server Manager console, in the **Dashboard**, click **Add roles and features**.
2. Click **Next** three times to get to the server role selection screen.
3. On the **Select server roles** dialog, select **Remote Access**, click **Add Features**, and then click **Next**.
4. Click **Next** five times.
5. On the **Confirm installation selections** dialog, click **Install**.
6. On the **Installation progress** dialog, verify that the installation was successful, and then click **Close**.

STEP 11 Configure the Multisite Deployment

12/9/2022 • 3 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

To configure a multisite deployment, make changes to the current Remote Access configuration wizard on EDGE1, enable the multisite feature, and then add 2-EDGE1 as a second entry point.

- Configure Remote Access on EDGE1
- Enable multisite configuration on EDGE1
- Add 2-EDGE1 as a second entry-point

Configure Remote Access on EDGE1

1. On the **Start** screen, type**RAMgmtUI.exe**, and then press ENTER. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the Remote Access Management Console, click **Configuration**.
3. In the middle pane of the console, in the **Step 2 Remote Access Server** area, click **Edit**.
4. Click **Prefix Configuration**. On the **Prefix Configuration** page, in **Internal network IPv6 prefixes**, enter **2001:db8:1::/64; 2001:db8:2::/64**. In **IPv6 prefix assigned to DirectAccess client computers**, enter **2001:db8:1:1000::/64**, click **Next**, and then click **Finish**.
5. In the middle pane of the console, in the **Step 3 Infrastructure Servers** area, click **Edit**.
6. Click **DNS Suffix Search List**. On the **DNS Suffix Search List** page, make sure that the **Configure DirectAccess clients with DNS client suffix search list** check box is selected and that the **corp.contoso.com** and **corp2.corp.contoso.com** domain suffixes appear in the **Domain suffixes to use** list, click **Next**, and then click Finish.
7. In the middle pane of the console, click **Finish**.
8. On the **Remote Access Review** dialog box, review the configuration settings, and then click **Apply**. On the **Applying Remote Access Setup Wizard Settings** dialog box, click **Close**.
9. In the **Tasks** pane, click **Refresh Management Servers**, and click **Close** when finished.

Enable multisite configuration on EDGE1

1. In the Remote Access Management Console, in the **Tasks** pane, click **Enable Multisite**.
2. In the Enable Multisite Deployment wizard, on the **Before You Begin** page, click **Next**.
3. On the **Deployment Name** page, in **Multisite deployment name**, type **Contoso**, in **First entry point name**, type **Edge1-Site**, and then click **Next**.
4. On the **Entry Point Selection** page, click **Assign entry points automatically, and allow clients to select manually**, and then click **Next**.
5. On the **Global Load Balancing** page, click **No, do not use global load balancing**, and then click **Next**.

6. On the **Client Support** page, click **Allow client computers running Windows 7 to access this entry point**, and click **Add**.
7. On the **Select Groups** dialog box, in **Enter the object names to select**, type **Win7_Clients_Site1**, click **OK**, and then click **Next**.
8. On the **Client GPO Settings** page, click **Next**.
9. On the **Summary** page, click **Commit**.
10. On the **Enabling Multisite Deployment** dialog box, click **Close** and then on the Enable Multisite Deployment wizard, click **Close**.

Add 2-EDGE1 as a second entry-point

1. In the Remote Access Management Console, in the **Tasks** pane, click **Add an Entry Point**.
2. In the Add an Entry Point Wizard, on the **Entry Point Details** page, in **Remote Access server**, type **2-edge1.corp2.corp.contoso.com**, in **Entry point name**, type **2-Edge1-Site**, and then click **Next**.
3. On the **Network Topology** page, click **Edge**, and then click **Next**.
4. On the **Network Name or IP Address** page, in **Type in the public name or IP address used by clients to connect to the Remote Access server**, type **2-edge1.contoso.com**, and then click **Next**.
5. On the **Network Adapters** page, make sure that the **External adapter** is **Internet**, the **Internal adapter** is **2-Corpnet**, the certificate is **CN=2-edge1.contoso.com**, and then click **Next**.
6. On the **Prefix Configuration** page, in **IPv6 prefix assigned to DirectAccess client computers**, type **2001:db8:2:2000::/64**, and then click **Next**.
7. On the **Client Support** page, click **Allow client computers running Windows 7 to access this entry point**, and click **Add**.
8. On the **Select Groups** dialog box, in **Enter the object names to select**, type **Win7_Clients_Site2**, click **OK**, and then click **Next**.
9. On the **Client GPO Settings** page, click **Next**.
10. On the **Server GPO Settings** page, click **Next**.
11. On the **Summary** page click **Commit**.
12. On the **Adding Entry Point** dialog box, click **Close** and then on the Add an Entry Point wizard, click **Close**.

STEP 12 Test DirectAccess Connectivity

12/9/2022 • 8 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Before you can test connectivity from the client computers when they are located on the Internet or Homenet networks, you must make sure they have the correct group policy settings.

- To verify clients have the correct group policy
- Test DirectAccess connectivity from the Internet through EDGE1
- Move CLIENT2 to the Win7_Clients_Site2 security group
- Test DirectAccess connectivity from the Internet through 2-EDGE1

Prerequisites

Connect both client computers to the Corpnet network, and then restart both client computers.

Verify clients have the correct group policy

1. On CLIENT1, click **Start**, type **powershell.exe**, right-click **powershell**, click **Advanced**, and then click **Run as administrator**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
2. In the Windows PowerShell window, type **ipconfig** and press ENTER.

   Make sure that the Corpnet adapter IPv4 address starts with 10.0.0.
3. In the Windows PowerShell window type **Get-DnsClientNrptPolicy** and press ENTER. The Name Resolution Policy Table (NRPT) entries for DirectAccess are displayed.
   - .corp.contoso.com-These settings indicate that all connections to corp.contoso.com should be resolved by one of the DirectAccess DNS servers, with the IPv6 address 2001:db8:1::2 or 2001:db8:2::20.
   - nls.corp.contoso.com-These settings indicate that there is an exemption for the name nls.corp.contoso.com.
4. Leave the Windows PowerShell window open for the next procedure.
5. On CLIENT2, click **Start**, click **All Programs**, click **Accessories**, click **Windows PowerShell**, right-click **Windows PowerShell**, and then click **Run as administrator**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
6. In the Windows PowerShell window, type **ipconfig** and press ENTER.

   Make sure that the Corpnet adapter IPv4 address starts with 10.0.0.
7. In the Windows PowerShell window, type **netsh namespace show policy** and press ENTER.

   In the output, there should be two sections:
   - .corp.contoso.com-These settings indicate that all connections to corp.contoso.com should be resolved by the DirectAccess DNS server, with the IPv6 address 2001:db8:1::2.

- nls.corp.contoso.com-These settings indicate that there is an exemption for the name nls.corp.contoso.com.

8. Leave the Windows PowerShell window open for the next procedure.

Test DirectAccess connectivity from the Internet through EDGE1

1. Unplug 2-EDGE1 from the Internet network.
2. Unplug CLIENT1 and CLIENT2 from the corpnet switch and connect them to the Internet switch. Wait for 30 seconds.
3. On CLIENT1, in the Windows PowerShell window, type **ipconfig /all** and press ENTER.
4. Examine the output from the ipconfig command.

   The client computer is now connected to the Internet and has a public IPv4 address. When the DirectAccess client has a public IPv4 address, it uses the Teredo or IP-HTTPS IPv6 transition technologies to tunnel the IPv6 messages over an IPv4 Internet between the DirectAccess client and Remote Access server. Note that Teredo is the preferred transition technology.

5. In the Windows PowerShell window, type **ipconfig /flushdns** and press ENTER. This flushes name resolution entries that may still exist in the client DNS cache from when the client computer was connected to the corpnet.
6. Disable the Teredo interface to ensure that the client computer uses IP-HTTPS to connect to corpnet with the following command:

   ```
   netsh interface teredo set state disable
   ```

7. Ensure you are connected through EDGE1. Type **netsh interface httpstunnel show interfaces** and press ENTER.

   The output should contain URL : https://edge1.contoso.com:443/IPHTTPS.

   > **TIP**
   > On CLIENT1, you can also run the following Windows PowerShell command: **Get-NetIPHTTPSConfiguration**. The output shows the available server URL connections and the currently active profile.

8. In the Windows PowerShell window, type **ping app1** and press ENTER. You should see replies from the IPv6 address assigned to APP1, which in this case is 2001:db8:1::3.
9. In the Windows PowerShell window, type **ping 2-app1** and press ENTER. You should see replies from the IPv6 address assigned to 2-APP1, which in this case is 2001:db8:2::3.
10. In the Windows PowerShell window, type **ping app2** and press ENTER. You should see replies from the NAT64 address assigned by EDGE1 to APP2, which in this case is fd**c9:9f4e:eb1b**:7777::a00:4. Note that the bold values will vary due to how the address is generated.

    The ability to ping APP2 is important, because success indicates that you were able to establish a connection using NAT64/DNS64, as APP2 is an IPv4 only resource.

11. Open Internet Explorer, in the Internet Explorer address bar, enter **https://app1/** and press ENTER. You will see the default IIS website on APP1.
12. In the Internet Explorer address bar, enter **https://2-app1/** and press ENTER. You will see the default

website on 2-APP1.

13. In the Internet Explorer address bar, enter **https://app2/** and press ENTER. You will see the default website on APP2.

14. On the **Start** screen, type**\\2-App1\Files**, and then press ENTER. Double-click the example text file.

    This demonstrates that you were able to connect to the file server in the corp2.corp.contoso.com domain when connected through EDGE1.

15. On the **Start** screen, type**\\App2\Files**, and then press ENTER. Double-click the New Text Document file.

    This demonstrates that you were able to connect to an IPv4 only server using SMB to obtain a resource in the resource domain.

16. On the **Start** screen, type**wf.msc**, and then press ENTER.

17. In the **Windows Firewall with Advanced Security** console, notice that only the **Public Profile** is active. The Windows Firewall must be enabled for DirectAccess to work correctly. If the Windows Firewall is disabled, DirectAccess connectivity does not work.

18. In the left pane of the console, expand the **Monitoring** node, and click the **Connection Security Rules** node. You should see the active connection security rules: **DirectAccess Policy-ClientToCorp**, **DirectAccess Policy-ClientToDNS64NAT64PrefixExemption**, **DirectAccess Policy-ClientToInfra**, and **DirectAccess Policy-ClientToNlaExempt**. Scroll the middle pane to the right to show the **1st Authentication Methods** and **2nd Authentication Methods** columns. Notice that the first rule (ClientToCorp) uses Kerberos V5 to establish the intranet tunnel and the third rule (ClientToInfra) uses NTLMv2 to establish the infrastructure tunnel.

19. In the left pane of the console, expand the **Security Associations** node, and click the **Main Mode** node. Notice the infrastructure tunnel security associations using NTLMv2 and the intranet tunnel security association using Kerberos V5. Right-click the entry that shows **User (Kerberos V5)** as the **2nd Authentication Method** and click **Properties**. On the **General** tab, notice the **Second authentication Local ID** is **CORP\User1**, indicating that User1 was able to successfully authenticate to the CORP domain using Kerberos.

20. Repeat this procedure from step 3 on CLIENT2.

Move CLIENT2 to the Win7_Clients_Site2 security group

1. On DC1, click **Start**, type **dsa.msc**, and then press ENTER.

2. In the Active Directory Users and Computers console, open **corp.contoso.com/Users** and double-click **Win7_Clients_Site1**.

3. On the **Win7_Clients_Site1 Properties** dialog box, click the **Members** tab, click **CLIENT2**, click **Remove**, click **Yes**, and then click **OK**.

4. Double-click **Win7_Clients_Site2**, and then on the **Win7_Clients_Site2 Properties** dialog box, click the **Members** tab.

5. Click **Add**, and on the **Select Users, Contacts, Computers, or Service Accounts** dialog box, click **Object Types**, select **Computers**, and then click **OK**.

6. In **Enter the object names to select**, type **CLIENT2**, and then click **OK**.

7. Restart CLIENT2 and log on using the corp/User1 account.

8. On CLIENT2, open an elevated Windows PowerShell window, type **netsh namespace show policy** and press ENTER.

In the output, there should be two sections:

- .corp.contoso.com-These settings indicate that all connections to corp.contoso.com should be resolved by the DirectAccess DNS server, with the IPv6 address 2001:db8:2::20.
- nls.corp.contoso.com-These settings indicate that there is an exemption for the name nls.corp.contoso.com.

Test DirectAccess connectivity from the Internet through 2-EDGE1

1. Connect 2-EDGE1 to the Internet network.
2. Unplug EDGE1 from the Internet network.
3. On CLIENT1, open an elevated Windows PowerShell window.
4. In the Windows PowerShell window, type **ipconfig /flushdns** and press ENTER. This flushes name resolution entries that may still exist in the client DNS cache from when the client computer was connected to the corpnet.
5. Ensure you are connected through 2-EDGE1. Type **netsh interface httpstunnel show interfaces** and press ENTER.

   The output should contain URL : https://2-edge1.contoso.com:443/IPHTTPS.

   > **TIP**
   > On CLIENT1, you can also run the following command: **Get-NetIPHTTPSConfiguration**. The output shows the available server URL connections and the currently active profile.

   > **NOTE**
   > CLIENT1 automatically changes the server through which it connects to corporate resources. If the output of the command shows a connection to EDGE1, wait for approximately five minutes and then try again.

6. In the Windows PowerShell window, type **ping app1** and press ENTER. You should see replies from the IPv6 address assigned to APP1, which in this case is 2001:db8:1::3.
7. In the Windows PowerShell window, type **ping 2-app1** and press ENTER. You should see replies from the IPv6 address assigned to 2-APP1, which in this case is 2001:db8:2::3.
8. In the Windows PowerShell window, type **ping app2** and press ENTER. You should see replies from the NAT64 address assigned by EDGE1 to APP2, which in this case is fd**c9:9f4e:eb1b**:7777::a00:4. Note that the bold values will vary due to how the address is generated.

   The ability to ping APP2 is important, because success indicates that you were able to establish a connection using NAT64/DNS64, as APP2 is an IPv4 only resource.

9. Open Internet Explorer, in the Internet Explorer address bar, enter **https://app1/** and press ENTER. You will see the default IIS website on APP1.
10. In the Internet Explorer address bar, enter **https://2-app1/** and press ENTER. You will see the default website on APP2.
11. In the Internet Explorer address bar, enter **https://app2/** and press ENTER. You will see the default website on APP3.
12. On the **Start** screen, type**\\App1\Files**, and then press ENTER. Double-click the example text file.

This demonstrates that you were able to connect to the file server in the corp.contoso.com domain when connected through 2-EDGE1.

13. On the **Start** screen, type**\\App2\Files**, and then press ENTER. Double-click the New Text Document file.

    This demonstrates that you were able to connect to an IPv4 only server using SMB to obtain a resource in the resource domain.

14. Repeat this procedure on CLIENT2 from step 3.

STEP 13 Test DirectAccess Connectivity from Behind a NAT Device

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

When a DirectAccess client is connected to the Internet from behind a NAT device or a web proxy server, the DirectAccess client uses either Teredo or IP-HTTPS to connect to the Remote Access server. If the NAT device enables outbound UDP port 3544 to the Remote Access server's public IP address, then Teredo is used. If Teredo access is not available, the DirectAccess client falls back to IP-HTTPS over outbound TCP port 443, which enables access through firewalls or web proxy servers over the traditional SSL port. If the web proxy requires authentication, the IP-HTTPS connection will fail. IP-HTTPS connections also fail if the web proxy performs outbound SSL inspection, due to the fact that the HTTPS session is terminated at the web proxy instead of the Remote Access server.

The following procedures are performed on both client computers:

1. Test Teredo connectivity. The first set of tests are performed when the DirectAccess client is configured to use Teredo. This is the automatic setting when the NAT device allows outbound access to UDP port 3544. First run the tests on CLIENT1 and then run the tests on CLIENT2.
2. Test IP-HTTPS connectivity. The second set of tests are performed when the DirectAccess client is configured to use IP-HTTPS. In order to demonstrate IP-HTTPS connectivity, Teredo is disabled on the client computers. First run the tests on CLIENT1 and then run the tests on CLIENT2.

Prerequisites

Start EDGE1 and 2-EDGE1 if they are not already running, and make sure they are connected to the Internet subnet.

Before performing these tests, unplug CLIENT1 and CLIENT2 from the Internet switch and connect them to the Homenet switch. If asked what type of network you want to define the current network, select **Home network**.

Test Teredo connectivity

1. On CLIENT1, open an elevated Windows PowerShell window.
2. Enable the Teredo adapter, type **netsh interface teredo set state enterpriseclient**, and then press ENTER.
3. In the Windows PowerShell window, type **ipconfig /all** and press ENTER.
4. Examine the output of the ipconfig command.

   This computer is now connected to the Internet from behind a NAT device and is assigned a private IPv4 address. When the DirectAccess client is behind a NAT device and assigned a private IPv4 address, the preferred IPv6 transition technology is Teredo. If you look at the output of the ipconfig command, you should see a section for Tunnel adapter Teredo Tunneling Pseudo-Interface and then a description Microsoft Teredo Tunneling Adapter, with an IP address that starts with 2001:0 consistent with being a Teredo address. You should see the default gateway listed for the Teredo tunnel adapter as '::'.
5. In the Windows PowerShell window, type **ipconfig /flushdns** and press ENTER.

This will flush name resolution entries that may still exist in the client DNS cache from when the client computer was connected to the Internet.

6. In the Windows PowerShell window, type **ping app1** and press ENTER. You should see replies from the IPv6 address of APP1, 2001:db8:1::3.

7. In the Windows PowerShell window, type **ping app2** and press ENTER. You should see replies from the NAT64 address assigned by EDGE1 to APP2, which in this case is fd**c9:9f4e:eb1b**:7777::a00:4. Note that the bold values will vary due to how the address is generated.

8. In the Windows PowerShell window, type **ping 2-app1** and press ENTER. You should see replies from the IPv6 address of 2-APP1, 2001:db8:2::3.

9. Open Internet Explorer, in the Internet Explorer address bar, enter **https://2-app1/** and press ENTER. You will see the default IIS website on 2-APP1.

10. In the Internet Explorer address bar, enter **https://app2/** and press ENTER. You will see the default website on APP2.

11. On the **Start** screen, type**\\App2\Files**, and then press ENTER. Double-click the New Text Document file. This demonstrates that you were able to connect to an IPv4 only server using SMB to obtain a resource on an IPv4 only host.

12. Repeat this procedure on CLIENT2.

Test IP-HTTPS connectivity

1. On CLIENT1, open an elevated Windows PowerShell window, and type **netsh interface teredo set state disabled** and press ENTER. This disables Teredo on the client computer and enables the client computer to configure itself to use IP-HTTPS. An **Ok** response appears when the command completes.

2. In the Windows PowerShell window, type **ipconfig /all** and press ENTER.

3. Examine the output of the ipconfig command. This computer is now connected to the Internet from behind a NAT device and is assigned a private IPv4 address. Teredo is disabled and the DirectAccess client falls back to IP-HTTPS. When you look at the output of the ipconfig command, you see a section for Tunnel adapter iphttpsinterface with an IP address that starts with 2001:db8:1:1000 or 2001:db8:2:2000 consistent with this being an IP-HTTPS address based on the prefixes that were configured when setting up DirectAccess. You will not see a default gateway listed for the IPHTTPSInterface tunnel adapter.

4. In the Windows PowerShell window, type **ipconfig /flushdns** and press ENTER. This will flush name resolution entries that may still exist in the client DNS cache from when the client computer was connected to the corpnet.

5. In the Windows PowerShell window, type **ping app1** and press ENTER. You should see replies from the IPv6 address of APP1, 2001:db8:1::3.

6. In the Windows PowerShell window, type **ping app2** and press ENTER. You should see replies from the NAT64 address assigned by EDGE1 to APP2, which in this case is fd**c9:9f4e:eb1b**:7777::a00:4. Note that the bold values will vary due to how the address is generated.

7. In the Windows PowerShell window, type **ping 2-app1** and press ENTER. You should see replies from the IPv6 address of 2-APP1, 2001:db8:2::3.

8. Open Internet Explorer, in the Internet Explorer address bar, enter **https://2-app1/** and press ENTER. You will see the default IIS website on 2-APP1.

9. In the Internet Explorer address bar, enter **https://app2/** and press ENTER. You will see the default website on APP2.

10. On the **Start** screen, type **\\App2\Files**, and then press ENTER. Double-click the New Text Document file. This demonstrates that you were able to connect to an IPv4 only server using SMB to obtain a resource on an IPv4 only host.

11. Repeat this procedure on CLIENT2.

STEP 14 Snapshot the Configuration

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This completes the DirectAccess multisite test lab. To save this configuration so that you can quickly return to a working DirectAccess multisite configuration from which you can test other DirectAccess modular test lab guides, test lab guide extensions, or for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots TLG DirectAccess Multisite. If your lab uses physical computers, create disk images to save the DirectAccess test lab configuration.

Test Lab Guide: Demonstrate DirectAccess with OTP Authentication and RSA SecurID

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Remote Access is a server role in the Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012 operating system that enables remote users to securely access internal network resources using DirectAccess or virtual private networks (VPNs) with the Routing and Remote Access Service (RRAS). This guide contains step-by-step instructions for extending the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6 to demonstrate a Remote Access one-time password (OTP) configuration.

> **WARNING**
>
> The design of this test lab guide includes infrastructure servers, such as a domain controller and a certification authority (CA) that are running either Windows Server 2012 R2 or Windows Server 2012. Using this test lab guide to configure infrastructure servers that are running other operating systems has not been tested, and instructions for configuring other operating systems are not included in this guide.

About this guide

Remote Access in Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012 adds support for client authentication with OTP. For the purposes of this test lab only RSA SecurID is used to demonstrate OTP functionality with Remote Access. Other RADIUS based OTP solutions are supported as well, but are outside the scope of this test lab. This guide contains instructions for configuring and demonstrating Remote Access using six servers and two client computers. The completed Remote Access with OTP test lab simulates an intranet, the Internet, and a home network, and demonstrates Remote Access functionality in different Internet connection scenarios.

> **IMPORTANT**
>
> This lab is a proof of concept using the minimum number of computers. The configuration detailed in this guide is for test lab purposes only, and is not to be used in a production environment.

Overview of the Test Lab Scenario OTP Authentication and RSA SecurID

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Remote Access is a server role in the Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012 operating systems that enables remote users to securely access internal network resources using DirectAccess or virtual private networks (VPNs) with the Routing and Remote Access Service (RRAS). This guide contains step-by-step instructions for extending the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6 to demonstrate a Remote Access one-time password (OTP) configuration.

> **WARNING**
>
> The design of this test lab guide includes infrastructure servers, such as a domain controller and a certification authority (CA) that are running either Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 . Using this test lab guide to configure infrastructure servers that are running other operating systems has not been tested, and instructions for configuring other operating systems are not included in this guide.

About this guide

Remote Access in Windows Server 2016, Windows Server 2012 R2 and Windows Server 2012 adds support for client authentication with OTP. For the purposes of this test lab only RSA SecurID is used to demonstrate OTP functionality with Remote Access. Other RADIUS based OTP solutions are supported as well, but are outside the scope of this test lab. This guide contains instructions for configuring and demonstrating Remote Access using six servers and two client computers. The completed Remote Access with OTP test lab simulates an intranet, the Internet, and a home network, and demonstrates Remote Access functionality in different Internet connection scenarios.

> **IMPORTANT**
>
> This lab is a proof of concept using the minimum number of computers. The configuration detailed in this guide is for test lab purposes only, and is not to be used in a production environment.

Configuration Requirements

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The following components are required to configure Remote Access in the test lab:

- The product disc or files for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012.
- Nine computers or virtual machines that meet the minimum hardware requirements for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 ; three of these computers have two network adapters installed.
- The product disc or files for Windows 10® or Windows® 8 .
- The product disc or files for Windows 7 Ultimate.
- Three computers or virtual machines that meet the minimum hardware requirements for Windows 10®, Windows 8 or Windows 7 ; one of these computers has two network adapters installed.

Steps for Configuring the DirectAccess Cluster-NLB Test Lab

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The following steps describe how to configure the Remote Access infrastructure, configure the Remote Access servers and clients, and test DirectAccess connectivity from the Internet and Homenet subnets.

In this test lab guide you will build a Network Load Balancing (NLB) enabled Remote Access cluster by performing the following steps:

- STEP 1 Complete the DirectAccess Configuration. Complete all the steps in the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6.
- STEP 2: Configure EDGE1. Configure the Remote Access role on EDGE1 for load balancing.
- STEP 3: Install and configure EDGE2. EDGE2 acts as the second Remote Access server in a Remote Access cluster.
- STEP 4: Create the network load balanced Remote Access cluster-EDGE1 is configured as the first server in a Remote Access cluster. EDGE2 is joined to the cluster and NLB is configured for the cluster.
- STEP 5: Test DirectAccess connectivity from the Internet and through the cluster. After NLB and cluster configuration is complete you can test DirectAccess client connectivity through the load balanced cluster.
- STEP 6: Test DirectAccess client connectivity from behind a NAT device. Move the client computer behind a NAT device to simulate testing DirectAccess client connectivity from behind a home router.
- STEP 7: Test connectivity when returning to the Corpnet. Make sure that the client computer can still access corporate resources when returning to Corpnet.
- STEP 8: Snapshot the configuration. After completing the test lab, take a snapshot of the working Remote Access NLB cluster so that you can return to it later to test additional scenarios.

STEP 1 Complete the DirectAccess in a Cluster with Windows NLB Configuration

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The first step is to complete all the steps in the Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6. If you have already completed the steps in this test lab guides and saved a snapshot or disk image of the test lab, you can restore the snapshot or image and begin with the next step.

STEP 2 Configure APP1

12/9/2022 • 5 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Use the following steps to prepare APP1 for OTP support:

1. To create and deploy a certificate template used to sign OTP certificate requests. Configure a certificate template used to sign OTP certificate requests.
2. To create and deploy a certificate template for OTP certificates issued by the corporate CA. Configure a certificate template for OTP certificates issued by the corporate CA.

> **WARNING**
> The design of this test lab guide includes infrastructure servers, such as a domain controller and a certification authority (CA) that are running either Windows Server 2012 R2 or Windows Server 2012. Using this test lab guide to configure infrastructure servers that are running other operating systems has not been tested, and instructions for configuring other operating systems are not included in this guide.

To create and deploy a certificate template used to sign OTP certificate requests

1. Run **certtmpl.msc**, and then press ENTER.
2. In the Certificate Templates Console, in the details pane, right-click the **Computer** template, and click **Duplicate Template**.
3. On the **Properties of New Template** dialog box, on the **Compatibility** tab, in the **Certification Authority** list, select the operating system you want, and in the **Resulting changes** dialog box click **OK**. In the **Certificate recipient** list select the operating system you want, and in the **Resulting changes** dialog box click **OK**.
4. On the **Properties of New Template** dialog box, click the **General** tab.
5. On the **General** tab, in **Template display name**, type **DAOTPRA**. Set the **Validity period** to 2 days, and set the **Renewal Period** to 1 day. If the **Certificate Templates** warning is displayed, click **OK**.
6. Click the **Security** tab, and then click **Add**.
7. On the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Object Types**. On the **Object Types** dialog box, select **Computers**, and then click **OK**. In the **Enter the object names to select** box, type **EDGE1**, click **OK**, and in the **Allow** column, select the **Read**, **Enroll**, and **Autoenroll** check boxes. Click **Authenticated Users**, select the **Read** check box under the **Allow** column, and clear all other check boxes. Click **Domain Computers**, and uncheck **Enroll** under the **Allow** column. Click **Domain Admins** and **Enterprise Admins** and click **Full Control** under the **Allow** column for both. Click **Apply**.
8. Click the **Subject Name** tab, and then click **Build from this Active Directory information**. In the **Subject name format:** list select **DNS name**, make sure that the **DNS name** box is checked, and click **Apply**.

9. Click the **Extensions** tab, select **Application Policies** and then click **Edit**. Remove all existing application policies. Click **Add**, and on the **Add Application Policy** dialog box, click **New**, enter **DA OTP RA** in the **Name:** field and **1.3.6.1.4.1.311.81.1.1** in the **Object identifier:** field, and click **OK**. On the **Add Application Policy** dialog box, click **OK**. On the **Edit Application Policies Extension**, click **OK**. On the **Properties of New Template** dialog box, click **OK**.

To create and deploy a certificate template for OTP certificates issued by the corporate CA

1. In the Certificate Templates Console, in the details pane, right-click the **Smartcard Logon** template, and click **Duplicate Template**.

2. On the **Properties of New Template** dialog box, on the **Compatibility** tab in the **Certification Authority** list, click the operating system you want to use, and in the **Resulting changes** dialog box, click **OK**. In the **Certificate recipient** list select the operating system you want to use, and in the **Resulting changes** dialog box click **OK**.

3. On the **Properties of New Template** dialog box, click the **General** tab.

4. On the **General** tab, in **Template display name**, type **DAOTPLogon**. In **Validity period**, in the drop-down list, click **hours**, on the **Certificate Templates** dialog box, click **OK**, and make sure that the number of hours is set to 1. In **Renewal period**, type **0**.

> **IMPORTANT**
>
> **Windows Server 2003 CA**. In situations where the certification authority (CA) is on a computer that is running Windows Server 2003, then the certificate template must be configured on a different computer. This is required because setting the **Validity period** in hours is not possible when running Windows versions prior to Windows Server 2008 and Windows Vista. If the computer that you use to configure the template does not have the Active Directory Certificate Services server role installed, or if it is a client computer, then you may need to install the Certificate Templates snap-in. For more information, see Install the Certificate Templates Snap-In.
>
> **Windows Server 2008 R2 CA**. If you have already deployed a certification authority (CA) that is running Windows Server 2008 R2 , you must configure the certificate template **Renewal Period** to 1 or 2 hours, and the **Validity Period** to be longer than the **Renewal Period**, but not more than 4 hours. If you configure a certificate template **Validity Period** of longer than 4 hours with a CA that is running Windows Server 2008 R2 , the DirectAccess installation wizard cannot detect the certificate template, and DirectAccess installation fails.

5. Click the **Security** tab, select **Authenticated Users**, in the **Allow** column, and select the **Read** and **Enroll** check boxes. Click **OK**. Click **Domain Admins** and **Enterprise Admins**, and click **Full Control** under the **Allow** column for both. Click **Apply**.

6. Click the **Subject Name** tab, and then click **Build from this Active Directory information**. In the **Subject name format:** list select **Fully distinguished name**, make sure that the **User principal name (UPN)** box is checked, and click **Apply**.

7. Click the **Server** tab, select the **Do not store certificates and requests in the CA database** check box, clear the **Do not include revocation information in issued certificates** check box, and then on the **Properties of New Template** dialog box, click **Apply**.

8. Click the **Issuance Requirements** tab, select the **This number of authorized signatures:** check box, set the value to 1. In the **Policy type required in signature:** list select **Application policy**, and in the **Application policy** list select **DA OTP RA**. On the **Properties of New Template** dialog box, click **OK**.

9. Click the **Extensions** tab, and on **Application Policies** click **Edit**. Delete **Client Authentication**, keep **SmartCardLogon**, and click **OK** twice.

10. Close the Certificate Templates Console.
11. On the **Start** screen, type**certsrv.msc**, and then press ENTER.
12. In the Certification Authority console tree, expand **corp-APP1-CA-1**, click **Certificate Templates**, right-click **Certificate Templates**, point to **New**, and click **Certificate Template to Issue**.
13. In the list of certificate templates, click **DAOTPRA** and **DAOTPLogon**, and click **OK**.
14. In the details pane of the console you should see the **DAOTPRA** certificate template with an **Intended purpose** of **DA OTP RA** and the **DAOTPLogon** certificate template with an **Intended Purpose** of **Smart Card Logon**.
15. Restart the services.
16. Close the Certification Authority console.
17. Open an elevated command prompt. Type **CertUtil.exe -SetReg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS**, and press ENTER.
18. Leave the Command Prompt window open for the next step.

STEP 3 Configure DC1

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

DC1 acts as a domain controller, DNS server, and DHCP server for the corp.contoso.com domain. Configure DC1 as follows:

Verify User1 has a User Principal Name defined on DC1

1. On DC1, open Server Manager, and click **AD DS** in the left pane. Right-click **DC1** and select **Active Directory Users and Computers**. In the left pane expand **corp.contoso.com\Users**, and double-click User1.
2. On the **Account** tab verify that **User logon name** is set to User1. If not, then enter **User1** in the **User logon name** field.
3. Click **OK**. Close the **Active Directory Users and Computers** console.

STEP 4 Install and Configure RSA and EDGE1

12/9/2022 • 11 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

RSA is the RADIUS and OTP server, and is installed prior to configuring RADIUS and OTP.

You will perform the following steps to configure the RSA deployment:

1. Install the operating system on the RSA server. Install Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 on the RSA server.
2. Configure TCP/IP on RSA. Configure TCP/IP settings on the RSA server.
3. Copy Authentication Manager installation files to the RSA server. After installing the operating system on RSA, copy the Authentication Manager files to the RSA computer.
4. Join the RSA server to the CORP domain. Join RSA to the CORP domain.
5. Disable Windows Firewall on RSA. Disable the Windows Firewall on the RSA server.
6. Install RSA Authentication Manager on the RSA server. Install RSA Authentication Manager.
7. Configure RSA Authentication Manager. Configure Authentication Manager.
8. Create DAProbeUser. Create a user account for probing purposes.
9. Install RSA SecurID software token on CLIENT1. Install RSA SecurID software token on CLIENT1.
10. Configure EDGE1 as an RSA Authentication Agent. Configure RSA Authentication Agent on EDGE1.
11. Configure EDGE1 to support OTP authentication. Configure OTP for DirectAccess, and verify the configuration.

Install the operating system on the RSA server

1. On RSA, start the installation of Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 .
2. Follow the instructions to complete the installation, specifying Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 (Full Installation) and a strong password for the local Administrator account. Log on using the local Administrator account.
3. Connect RSA to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2016, Windows Server 2012 R2 or Windows Server 2012 , and then disconnect from the Internet.
4. Connect RSA to the Corpnet subnet.

Configure TCP/IP on RSA

1. In Initial Configuration Tasks, click **Configure networking**.
2. In **Network Connections**, right-click **Local Area Connection**, and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

4. Click **Use the following IP address**. In **IP address**, type **10.0.0.5**. In **Subnet mask**, type **255.255.255.0**. In **Default Gateway**, type **10.0.0.2**. Click **Use the following DNS server addresses**, in **Preferred DNS server**, type **10.0.0.1**.
5. Click **Advanced**, and then click the **DNS** tab.
6. In **DNS suffix for this connection**, type **corp.contoso.com**, and then click **OK** twice.
7. On the **Local Area Connection Properties** dialog box, click **Close**.
8. Close the **Network Connections** window.

Copy Authentication Manager installation files to the RSA server

1. On the RSA server create the folder C:\RSA Installation.
2. Copy the contents of the RSA Authentication Manager 7.1 SP4 media to the C:\RSA Installation folder.
3. Create the subfolder C:\RSA Installation\License and Token.
4. Copy the RSA license files to C:\RSA Installation\License and Token.

Join the RSA server to the CORP domain

1. Right-click **My Computer**, and click **Properties**.
2. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
3. In **Computer Name**, type **RSA**. In **Member of**, click **Domain**, type **corp.contoso.com**, and click **OK**.
4. When you are prompted for a user name and password, type **User1** and its password, and click **OK**.
5. On the domain welcoming dialog box click **OK**.
6. When you are prompted that you must restart the computer, click **OK**.
7. On the **System Properties** dialog box, click **Close**.
8. When you are prompted to restart the computer, click **Restart Now**.
9. After the computer has restarted, type **User1** and the password, select CORP in the **Log on to:** drop down list, and click **OK**.

Disable Windows Firewall on RSA

1. Click **Start**, click **Control Panel**, click **System and Security**, and click **Windows Firewall**.
2. Click **Turn Windows Firewall on or off**.
3. **Turn off Windows Firewall** for all settings.
4. Click **OK** and close Windows Firewall.

Install RSA Authentication Manager on the RSA server

1. If the Security Warning message appears at any time during this process, click **Run** to continue.
2. Open the C:\RSA Installation folder and double-click **autorun.exe**.
3. Click **Install Now**, click **Next**, select the top option for the Americas, and click **Next**.
4. Select **I accept the terms of the license agreement**, and click **Next**.

5. Select **Primary Instance**, and click **Next**.
6. In the **Directory Name:** field type **C:\RSA**, and click **Next**.
7. Verify that the server name (RSA.corp.contoso.com) and IP address are correct, and click **Next**.
8. Browse to C:\RSA Installation\License and Token, and click **Next**.
9. On the **Verify license file** page, click **Next**.
10. In the **User ID** field type **Administrator**, and in the **Password** and **Confirm Password** fields type a strong password. Click **Next**.
11. On the log selection screen, accept the defaults and click **Next**.
12. On the summary screen, click **Install**.
13. After installation is complete, click **Finish**.

Configure RSA Authentication Manager

1. If the RSA Security Console does not open automatically, then on the RSA computer desktop double-click "RSA Security Console".
2. If the security certificate warning / security alert appears, click **Continue to this website** or click **Yes** to proceed, and add this site to trusted sites, if requested.
3. In the **User ID** field type **Administrator** and click **OK**.
4. In the **Password** field type the password for the Administrator account and click **Log On**.
5. Insert Token information.
   a. In the **RSA Security Console** click **Authentication** and click **SecurID Tokens**.
   b. Click **Import Tokens Job**, and then click **Add New**.
   c. In the **Import Options** section click **Browse**. Browse to and select the tokens XML file in the C:\RSA Installation\License and Token folder and click **Open**.
   d. Click **Submit Job** on the bottom of the page.
6. Create OTP new user.
   a. In the **RSA Security Console** click the **Identity** tab, click **Users**, and click **Add New**.
   b. In the **Last Name:** section type **User**, and in the **User ID:** section type **User1** (UserID must be the same as the AD username used for this lab). In the **Password:** and **Confirm Password:** sections type a strong password. Clear the **'Require user to change password at next logon'** check box and click **Save**.
7. Assign User1 to one of the imported tokens.
   a. On the **Users** page click **User1** and click **SecurID Tokens**.
   b. Click **SecurID Tokens** and click **Assign Token**.
   c. Under the **Serial Number** heading click the first number listed, and click **Assign**.
   d. Click the assigned token, and click **Edit**. In the **SecurID PIN Management** section for **User Authentication Requirement**, select **Do not require PIN (only tokencode)**.
   e. Click **Save and Distribute Token**.

f. On the **Distribute Software Token** page in the **Basics** section, click **Issue Token File (SDTID)**.

g. On the **Distribute Software Token** page in the **Token File Options** section, clear the **Enable copy protection** check box. Click **No Password** and **Next**.

h. On the **Distribute Software Token** page in the **Download File** section, click **Download Now**. Click **Save**. Browse to C:\RSA Installation and click **Save** and **Close**.

i. Minimize the **RSA Security Console** for use later.

8. Configure Authentication Manager as RADIUS server.

   a. On the RSA computer desktop double-click **"RSA Security Operations Console"**.

   b. If the security certificate warning / security alert appears, click **Continue to this website** or click **Yes** to proceed, and add this site to trusted sites if requested.

   c. Enter the User ID and Password and click **Log On**.

   d. Click **Deployment Configuration - RADIUS - Configure Server**.

   e. On the **Additional Credentials Required** page enter the administrator User ID and Password and click **OK**.

   f. On the **Configure RADIUS Server** page enter the same password used for the administrator user for the **Secrets** and **Master Password**. Enter the Administrator User ID and Password, and click **Configure**.

   g. Verify that the message **'Successfully configured RADIUS server'** is displayed. Click **Done**. Close the **RSA Operations Console**.

   h. Switch back to the **"RSA Security Console"**.

   i. On the **RADIUS** tab click **RADIUS Servers**. Verify that rsa.corp.contoso.com is listed.

9. Configure RSA server as RSA Authentication Client.

   a. On the **RADIUS** tab, click **RADIUS Clients** and **Add New**.

   b. Click the **ANY RADIUS Client** check box.

   c. Type a strong password of your choice in the **Shared Secret** field. You will use this same password later when configuring EDGE1 for OTP.

   d. Leave the **IP Address** field blank, and the **Make / Model** entry as **Standard RADIUS**.

   e. Click **Save without RSA Agent**.

10. Create files required for configuring EDGE1 as a RSA Authentication Agent.

    a. On the **Access** tab, highlight **Authentication Agents**, and click **Add New**.

    b. Type **EDGE1** in the **Hostname** field, and click **Resolve IP**.

    c. Notice that the IP address for EDGE1 is now displayed in the **IP Address** field. Click **Save**.

11. Generate a configuration file for the EDGE1 server (AM_Config.zip).

    a. On the **Access** tab, highlight **Authentication Agents**, and click **Generate Configuration File**.

    b. On the **Generate Configuration File** page click **Generate Config File**, and then click **Download Now**.

    c. Click **Save**, browse to C:\ RSA Installation, and click **Save**.

d. Click **Close** on the **Download Complete** dialog.

12. Generate a node secret file for the EDGE1 server (EDGE1_NodeSecret.zip).

    a. On the **Access** tab, highlight **Authentication Agents**, and click **Manage Existing**.

    b. Click the current configured node EDGE1, and click **Manage Node Secret**.

    c. Check the **Create a new random node secret, and export the node secret to a file** check box.

    d. Enter the same password used for the administrator user in the **Encryption Password** and **Confirm Encryption Password** fields, and click **Save**.

    e. On the **Node Secret File Generated** page click **Download Now**.

    f. On the **File Download** dialog click **Save**, browse to C:\RSA Installation, and click **Save**. Click **Close** on the **Download Complete** dialog.

    g. From the RSA Authentication Manager media copy \auth_mgr\windows-x86_64\am\rsa-ace_nsload\win32-5.0-x86\agent_nsload.exe to C:\RSA Installation.

Create DAProbeUser

1. In the **RSA Security Console** click the **Identity** tab, click **Users**, and click **Add New**.

2. In the **Last Name:** section type **Probe**, and in the **User ID:** section type **DAProbeUser**. In the **Password:** and **Confirm Password:** sections type a strong password. Clear the **'Require user to change password at next logon'** check box and click **Save**.

Install RSA SecurID software token on CLIENT1

Use this procedure to install SecurID software token on CLIENT1.

Install SecurID software token

1. On the CLIENT1 computer, create the folder C:\RSA Files. Copy the file Software_Tokens.zip from C:\RSA Installation on the RSA computer to C:\RSA Files. Extract the file User1_000031701832.SDTID to C:\RSA Files on CLIENT1.

2. Access the RSA SecurID software token media source, and double-click RSASECURIDTOKEN410 in the **SecurID SoftwareToken client app** folder to start the RSA SecurID installation. If the **Open File - Security Warning** message appears, then click **Run**.

3. On the **RSA SecurID Software Token - InstallShield Wizard** dialog click **Next** twice.

4. Accept the license agreement, and click **Next**.

5. On the **Setup Type** dialog select **Typical**, click **Next**, and click **Install**.

6. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.

7. Select the **Launch RSA SecurID Software Token** check box, and click **Finish**.

8. Click **Import from File**.

9. Click **Browse**, select C:\RSA Files\User1_000031701832.SDTID, and click **Open**.

10. Click **OK** twice.

Configure EDGE1 as an RSA Authentication Agent

Use this procedure to configure EDGE1 to perform RSA authentication.

Configure the RSA Authentication Agent

1. On EDGE1 open Windows Explorer and create the folder C:\RSA Files. Browse to the RSA ACE Installation media.
2. Copy the files agent_nsload.exe, AM_Config.zip and EDGE1_NodeSecret.zip from the RSA media to C:\RSA Files.
3. Extract the contents of both zip files to the following locations:
   a. C:\Windows\system32\
   b. C:\Windows\SysWOW64\
4. Copy agent_nsload.exe to C:\Windows\SysWOW64\.
5. Open an elevated command prompt and navigate to C:\Windows\SysWOW64.
6. Type **agent_nsload.exe -f nodesecret.rec -p <password>** where <password> is the strong password that you created during the initial RSA configuration. Press Enter.
7. Copy C:\Windows\SysWOW64\securid to C:\Windows\System32.

Configure EDGE1 to support OTP authentication

Use this procedure to configure OTP for DirectAccess, and verify the configuration.

Configure OTP for DirectAccess

1. On EDGE1, open Server Manager, and click **REMOTE ACCESS** in the left pane.
2. Right-click **EDGE1** in the SERVERS pane, and select **Remote Access Management**.
3. Click **Configuration**.
4. In the **DirectAccess Setup** window, under **Step 2 - Remote Access Server**, click **Edit**.
5. Click **Next** three times, and in the **Authentication** section select **Two factor authentication** and **Use OTP**, and ensure that **Use computer certificates** is checked. Verify that the root CA is set to **CN=corp-APP1-CA**. Click **Next**.
6. In the **OTP RADIUS Server** section, double-click the blank **Server Name** field.
7. In the **Add a RADIUS Server** dialog, type **RSA** in the **Server name** field. Click **Change** next to the **Shared secret** field, and type the same password that you used when configuring the RADIUS clients on the RSA server in the **New secret** and **Confirm new secret** fields. Click **OK** twice, and click **Next**.

   > **NOTE**
   > If the RADIUS server is in a domain that is different than the Remote Access server, then the **Server Name** field must specify the FQDN of the RADIUS server.

8. In the **OTP CA Servers** section select APP1.corp.contoso.com, and click **Add**. Click **Next**.
9. On the **OTP Certificate Templates** page click **Browse** to select a certificate template used for the enrollment of certificates that are issued for OTP authentication, and on the **Certificate Templates** dialog box select **DAOTPLogon**. Click **OK**. Click **Browse** to select a certificate template used to enroll the certificate used by the Remote Access server to sign OTP certificate enrollment requests, and on the

Certificate Templates dialog box select **DAOTPRA**. Click **Ok**. Click **Next**.

10. On the **Remote Access Server Setup** page click **Finish**, and click **Finish** on the **DirectAccess Expert Wizard**.

11. On the **Remote Access Review** dialog box click **Apply**, wait for the DirectAccess policy to be updated, and click **Close**.

12. On the **Start** screen, type**powershell.exe**, right-click **powershell**, click **Advanced**, and click **Run as administrator**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.

13. In the Windows PowerShell window, type **gpupdate /force** and press ENTER.

14. Close and reopen the Remote Access Management Console and verify that all OTP settings are correct.

STEP 5 Verify OTP Health on EDGE1

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The following procedures verify that OTP is configured and functioning correctly using DirectAccess Server Health Monitoring on EDGE1.

Verify OTP Health on EDGE1 using DirectAccess Server Health Monitoring

1. On EDGE1, open the **Remote Access Management** console.
2. Click **Operations Status**.
3. Verify that the status of OTP is **Working**.

STEP 6 Test DirectAccess Connectivity from the Homenet Subnet

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The DirectAccess one-time password (OTP) deployment is now complete and you can start to test connectivity from the Homenet subnet.

To test OTP functionality from the Homenet subnet on CLIENT1

1. On CLIENT1, make sure that you are logged on as **User1**.
2. On the **Start** screen, type**powershell.exe**, right-click **powershell**, click **Advanced**, and then click **Run as administrator**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
3. In the Windows PowerShell window, type **gpupdate /force**, and press ENTER.
4. Unplug CLIENT1 from the Corpnet subnet and connect it to the Homenet subnet.
5. On CLIENT1, open Internet Explorer, and in the address bar, type **https://app1.corp.contoso.com/** and press ENTER. Press F5.

   The site should not open.
6. On the **Start** screen, type**RSA**, and click **RSA SecurID Token**.
7. Wait until the RSA SecurID token changes the One-time password, and then click **Copy**.
8. Click the **Network connections** icon in the notification area to access the DA Media Manager.
9. Click **Contoso DirectAccess Connection**, and click **Continue**.
10. Press Control+Alt+Delete, and click the **One-time password (OTP)** tile.
11. Paste the previously copied eight digit tokencode, and click **OK**. Wait for authentication to complete. The DirectAccess Workplace Connection status will now be **Connected**.
12. In Internet Explorer, in the address bar, type **https://app1.corp.contoso.com/** and press ENTER. Press F5. You will see the default IIS website on APP1.
13. In the Internet Explorer address bar, type **https://app2.corp.contoso.com/** and press ENTER. Press F5. You will see the default IIS website on APP2.
14. On the **Start** screen, type**\\app1\files**, and press ENTER.
15. In the **Files** shared folder window, double-click the **Example.txt** file. You will see the contents of the Example.txt file.
16. On the **Start** screen, type**\\app2\files**, and press ENTER.
17. In the **Files** shared folder window, double-click the **New Text Document.txt** file. You will see the contents of the New Text Document.txt file.

STEP 7 Test DirectAccess Connectivity from the Internet

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The DirectAccess one-time password (OTP) deployment has been tested from the Homenet subnet, and can now be tested from the Internet.

To test OTP functionality from the Internet on CLIENT1

1. On CLIENT1 make sure that you are logged on as **User1**. Connect CLIENT1 to the Corpnet subnet.
2. On the **Start** screen, type**powershell.exe**, right-click **powershell**, click **Advanced**, and then click **Run as administrator**. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
3. In the Windows PowerShell window, type **gpupdate /force** and press ENTER.
4. Unplug CLIENT1 from the Homenet subnet, connect it to the Internet, and restart the computer.
5. On CLIENT1, open Internet Explorer, and in the address bar, type **https://app1.corp.contoso.com/** and press ENTER. Press F5.

   The site should not open.
6. On the **Start** screen, type**RSA**, and click **RSA SecurID Token**.
7. Wait until the RSA SecurID token changes the One-time password, and then click **Copy**.
8. Click the **Network connections** icon in the notification area to access the DA Media Manager.
9. Click **Workplace Connection**, and click **Continue**.
10. Press Control+Alt+Delete, and click the **One-time password (OTP)** tile.
11. Paste the previously copied eight digit tokencode, and click **OK**. Wait for authentication to complete. The DirectAccess Workplace Connection status will now be **Connected**.
12. In Internet Explorer, in the address bar, type **https://app1.corp.contoso.com/** and press ENTER. Press F5. You will see the default IIS website on APP1.
13. In the Internet Explorer address bar, type **https://app2.corp.contoso.com/** and press ENTER. Press F5. You will see the default IIS website on APP2.
14. On the **Start** screen, type**\\app1\files**, and press ENTER.
15. In the **Files** shared folder window, double-click the **Example.txt** file. You will see the contents of the Example.txt file.
16. On the **Start** screen, type**\\app2\files**, and press ENTER.
17. In the **Files** shared folder window, double-click the **New Text Document.txt** file. You will see the contents of the New Text Document.txt file.

STEP 8 Snapshot the DirectAccess Cluster-NLB Configuration

12/9/2022 • 2 minutes to read • Edit Online

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

This completes the DirectAccess test lab. To save this configuration so that you can quickly return to a working DirectAccess with NLB cluster configuration from which you can test other DirectAccess modular test lab guides, test lab guide extensions, or for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots DirectAccess cluster and NLB. If your lab uses physical computers, create disk images to save the DirectAccess test lab configuration.