This document explains the required steps to configure the Offline Assessment for Active Directory Security.

Important: Internet connectivity is needed to

- Access the **Services Hub** portal using your corporate credentials.
- Download the toolset
- Download the latest **wsusscn2.cab** file

All data collection and analysis is done locally on the tools machine.
No data is transported outside your environment without your agreement, in order to keep your data protected. Data is analyzed locally using our RAP expert system that is part of the Offline Assessment client.

How to prepare for your Offline Assessment for Active Directory Security

A data collection machine is used to connect to each of the servers in your environment and retrieves information from them, communicating over Remote Procedure Call (RPC), Server Message Block (SMB), PowerShell Remoting, and Lightweight Directory Access Protocol (LDAP). Once the data is collected and the operational interview is completed, the Offline Assessment tool will analyze the data locally.

A checklist of prerequisite actions follows. Each item links to any additional software required for the tools machine, and detailed steps included later in this document.

At a high level, your steps to success are:

- Install prerequisites on your tools machine and configure your environment.
- Collect data from your Devices.
- Complete the operational survey.

The Offline Assessment for Active Directory Security is available for Domain Controllers running on Windows Server 2016, Windows Server 2019, Windows Server 2022 or Windows Server 2025.

Although there are no limitations to the number of target machines, an engineer can efficiently cover up to 150 targets during the engagement.

This document was last updated on February 20, 2026. To ensure you have the latest version of this document, check here: https://go.microsoft.com/fwlink/?LinkId=619023

Table of Contents

System Requirements and Configuration at Glance

Review the following details to ensure that you meet the necessary requirements.

Supported Target Operating System Versions

Your Active Directory domain controllers must run Windows Server 2016, Windows Server 2019, Windows Server 2022 or Windows Server 2025.

Environment Permissions

A domain account with the following rights:

- Enterprise Administrator.
- Administrative access to every domain controller in the forest.
- Administrative access to all Microsoft Domain Name System (DNS) servers that the domain controllers participate with.
- Administrative access on the data collection machine
- Log on locally privileges on the data collection machine.

Data Collection machine

- The data collection machine must be joined to one of the domains in the forest to be assessed.
- Data collection machine hardware**:** Minimum 16 gigabytes (GB) of RAM, 2 gigahertz (GHz dual-core processor, minimum 10 GB of free disk space.
- Depending on the size and complexity of your environment, you will need to increase the total amount of RAM to ensure that the data collection is successful and completes in a timely manner.
- The data collection machine is used to connect to all domain controllers in the forest and retrieve information from it. The machine is communicating over Remote Procedure Call (RPC), Server Message Block (SMB), WMI, remote registry, Lightweight Directory Access Protocol (LDAP) and Distributed Component Object Model (DCOM).
- Short name resolution must work from the data collection machine. This typically means making sure DNS suffixes for all domains in the forest are added on the Tools machine.
- Microsoft .NET Framework 4.8 or newer installed and running on Windows Server 2016 or newer.
- Networked “Documents” or redirected “Documents” folders are not supported. Local “Documents” folder on the data collection machine is required.
- Antivirus and any other type of Security software need to be configured to exclude Assessment related files, file types, working directory folders and process (OfflineAssessmentClient.exe) to avoid process termination, blockage and alerts. Add an exclusion to Windows Security

Scanning Security Updates with Windows PowerShell V5 Using wsusscn2.cab File

- PowerShell V5 is used to scan the servers for installed and missing security patches.
- Download the Windows Update offline scan file (Wsusscn2.cab) and place the file at the root of the system drive C:\wsusscn2.cab on the collection machine.
- The latest cab files can be downloaded from the following link: http://go.microsoft.com/fwlink/?LinkId=76054.
- Windows Update Agent must be running on all domain controllers.

Running the Offline Assessment

- Do not use the Run As feature to start the Offline Assessment Client, as this may cause some collectors to fail.
- An account with Enterprise Administrator privileges must log on interactively to the collection machine and start the Offline Assessment Client with administrative elevation ("Run as Administrator").

PowerShell Remoting

To complete the assessment with the accurate results, you will need to configure all Doman Controllers in the Forest for PowerShell remoting.

PowerShell on the tools machine is used to scan the servers for installed security patches as well as audit policy configuration.

- PowerShell version 2 or greater is required on target domain controllers and comes installed by default starting with Windows Server 2008 R2.

Additional requirements for Target Machines when defaults are modified.

The following three items must be configured on target Doman Controllers to support data collection: PowerShell Remoting, WinRM service and Listener, and Inbound Allow Firewall Rules.

Note: Windows Server 2016 and later have WinRM and PowerShell remoting enabled by default. The following configuration steps detailed below will only need to be implemented if the default configuration for target machines has been altered. The following settings will need to be configured to support PowerShell Remoting

- Execute Enable-PSRemoting Powershell cmdlet on each target machine within the scope of the assessment. This one command will configure PS-Remoting, WinRM service and listener, and enable required Inbound FW rules. A detailed description of everything Enable-PSRemoting does is documented here

OR

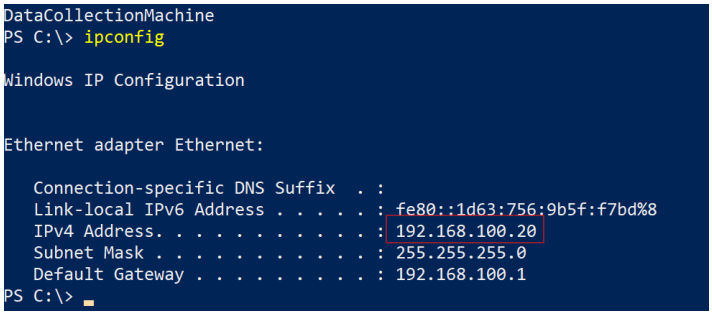
- Configure WinRM / PowerShell remoting via Group Policy
  - Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service
  - **Allow remote server management through WinRM**
  - Click on Enabled and specify allowed IP addresses / ranges or "*" to allow messages from any IP address
- Configure WinRM service for automatic start via Group Policy
  - Computer Configuration > Policies > Windows Settings > Security Settings > System Services.
  - Define **Windows Remote Management (WS-Management)** service for Automatic startup mode
- Configure Inbound allow Firewall Rules: This can be done individually in the local firewall policy of every target domain controller or via a group policy which allow communication from the tools machine.

Two steps are involved to configure a group policy to enable both WinRM listener and the required inbound allow firewall rules:

- Identify the IP address of the source computer where data collection will occur from.
- Create a new GPO linked to the domain controller organizational unit, and define an inbound rule for the tools machine

Step 1: Log into the chosen data collection machine to identify its current IP address using IPConfig.exe from the command prompt.

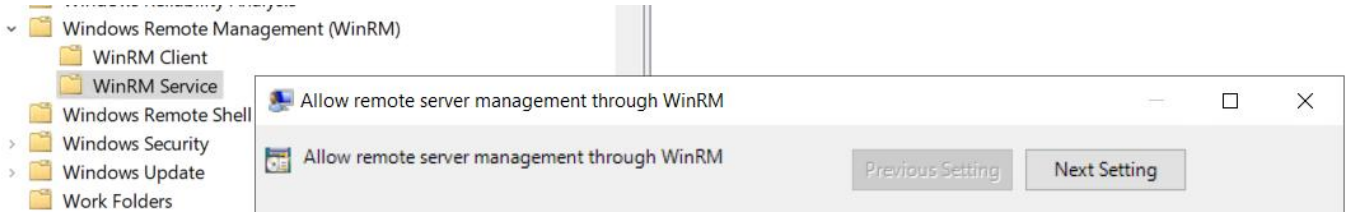
- Make a note of the IPv4 address of your machine. The final step in the configuration will use this address to ensure only the data collection machine can communicate with the Windows Update Agent on the domain controllers.



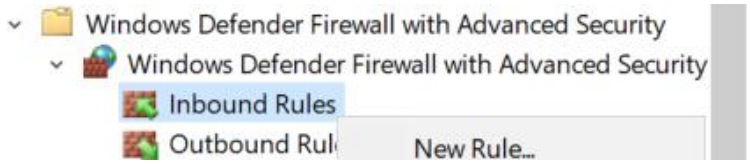
Step 2: Create, configure, and link a group policy object to the domain controllers OU in each domain in the forest.

- Create a new GPO. Make sure the GPO applies to the Domain Controllers organizational unit. Give the new group policy a name based on your group policy naming convention or something that identifies its purpose similar to "AD Security Assessment"

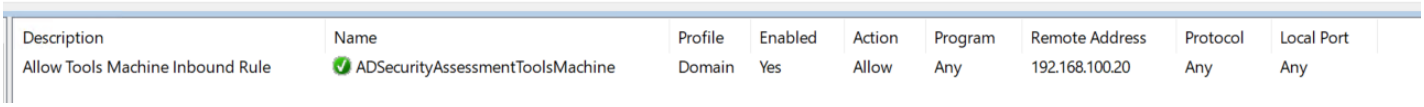
- Within the GPO open:
  - Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service
  - Enable "Allow remote server management through WinRM"
  - Specify allowed IP addresses / ranges or "*" to allow messages from any IP address



- Create an advanced Inbound Firewall Rule to allow all network traffic between the data collection machine and the Domain Controllers. This can be the applied to the same GPO that was used above.
- Navigate to:
    - Computer > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Inbound Rules.
- To create the new rule, Right Click on “Inbound Rules” and select “New”.



- On the Rule Type page select Custom rule and choose “Next”
- On the Program page select “All programs” from the tools machine and click “Next”.
- On the Protocols and Ports page, ensure Any protocol and All ports are selected, then click “Next”.
- On the Scope page specify the IP address of the data collection machine under the “Which remote IP addresses does this rule apply to” portion of the scope page, then select “Next”.
- On the Action page, choose to “Allow the connection” and click “Next”.
- On the Profile page, choose to select network profile “Domain” and click “Next”.
- Choose a name for the rule (Example: ADSecurityAssessmentToolsMachine) and complete the wizard.



Description	Name	Profile	Enabled	Action	Program	Remote Address	Protocol	Local Port
Allow Tools Machine Inbound Rule	ADSecurityAssessmentToolsMachine	Domain	Yes	Allow	Any	192.168.100.20	Any	Any

Appendix

Data Collection Methods

The **Active Directory Security Assessment** uses multiple data collection methods to collect information from your environment. This section describes the methods used to collect data from an Active Directory environment. The collectors are:

- Registry Collectors
- LDAP Collectors
- .NET Framework
- Windows PowerShell
- File Data Collector
- Windows Management Instrumentation (WMI)
- Custom C# Code

Registry Collectors

Registry keys and values are read from the data collection machine and all Domain Controllers. They include items such as:

- Service information from HKLM\SYSTEM\CurrentControlSet\Services.
  This allows determination of where the AD Database and log files are located on each DC, and gets detailed information on each service relevant to the proper function of AD.
- Operating System information from HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
  This allows one to determine Operation System information such as Windows Server 2019 or Windows Server 2022.

LDAP Collectors

LDAP queries are used to collect data for the Domain, Domain Controllers, Forest Partitions, Group Memberships, Account Names and their properties, Object permissions, and other components from AD itself.

.NET Framework

The assessment leverages the System.DirectoryServices.ActiveDirectory .NET Framework Namespace and uses several methods to determine and collect architectural information about the directory service.

Windows PowerShell

Collects various information, such as:

- ACL information on organizational unit objects in Active Directory
- Auditing Policy Configuration
- Installed Security Updates
- Scheduled Tasks

File Data Collector

Enumerates files in a folder on a remote machine, and optionally retrieves those files. Examples include:

- Scripts in SYSVOL
- Group Policy Preference configuration files

Windows Management Instrumentation (WMI)

WMI is used to collect various information such as:

- WIN32_Volume
  WMI collects information on Volume Settings for each DC in the forest. The information is used for instance to determine the system volume and drive letter which allows the client to collect information on files located on the system drive.

- Win32_Process
  Collect information on the processes running on each DC in the forest. The information provides insight in processes that consume a large amount of threads, memory or have a large page file usage.

- Win32_LogicalDisk
  Used to collect information on the logical disks. We use the information to determine the amount of free space on the disk where the database or log files are located.

Custom C# Code

Collects information not captured using other collectors. The primary example here is the collection of effective user rights on the domain controllers.

Validation

Check computer WMI access against every target machine.

- get-wmiobject Win32_ComputerSystem -computer <computername> | fl Name,Domain
    - Name : <computername>
    - Domain : <domain name>

Check if administrative shares are available against every target machine

- get-wmiobject WIN32_Share -computer<computername> | Where-Object Name -eq "c$" | fl name
    - name : C$

Check Scheduled Tasks access against every target machine

- $([xml](schtasks /query /XML ONE /S <computername>)).Tasks.Task.Count
    - <Number of Tasks>

Check PowerShell Remoting

- Enter-PSSession -ComputerName localhost
    - [<computername>]: PS C:\Users\<username>\Documents>