Defender for Identity deployment

See staging:

# Quick installation

This article outlines the steps to install Microsoft Defender for Identity on Active Directory or Active Directory Federation Services (AD FS) servers.

[!VIDEO https://www.microsoft.com/en-us/videoplayer/embed/RW16oLB]

In this short video, we show a step-by-step guide on how to install the Microsoft Defender for Identity sensor. The video begins by explaining the importance of having the sensors installed to protect your organization against identity-based attacks. It then goes on to show the user how to download and install the sensor, as well as how to find the potential health issues, and how to see your secure score Identity related posture assessments.

## Prerequisites

### Licensing requirements

Acquire a license for Enterprise Mobility + Security E5 (EMS E5/A5), Microsoft 365 E5 (M365 E5/A5/G5) or Microsoft 365 E5/A5/G5 Security directly via the [Microsoft 365 portal](https://www.microsoft.com/cloud-platform/enterprise-mobility-security-pricing) or use the Cloud Solution Partner (CSP) licensing model.

Standalone Defender for Identity licenses are also available.

For more information, see [Licensing and privacy](/defender-for-identity/technical-faq#licensing-and-privacy).

### Required permissions

* To create your Defender for Identity instance, you’ll need an Azure AD tenant with at least one global/security administrator. Each Defender for Identity instance supports a multiple Active Directory forest boundary and Forest Functional Level (FFL) of Windows 2003 and above.
* You need to be a [global administrator or security administrator on the tenant](/azure/active-directory/users-groups-roles/directory-assign-admin-roles#available-roles) to access the Identity section on the Microsoft 365 Defender portal and be able to create the workspace.

For more information, see [Role groups](role-groups.md).

### Minimum system requirements

The Defender for Identity sensor supports installation on the different operating system versions, as described in the following table. It requires a minimum of 2 cores, 6 GB of RAM, and 6 GB of disk space installed on the domain controller.

For accurate calculations of the resources required by your server according to your specific load, refer to [Plan capacity for Microsoft Defender for Identity deployment](capacity-planning.md).

| **Operating system version** | **Server with Desktop** **Experience** | **Server** **Core** | **Nano** **Server** | **Supported** **installations** |
| --- | --- | --- | --- | --- |
| Windows Server 2012\* | ✔ | ✔ | Not applicable | Domain controller |
| Windows Server 2012 R2\* | ✔ | ✔ | Not applicable | Domain controller |
| Windows Server 2016 | ✔ | ✔ | ❌ | Domain controller, AD FS |
| Windows Server 2019\*\* | ✔ | ✔ | ❌ | Domain controller, AD FS |
| Windows Server 2022 | ✔ | ✔ | ❌ | Domain controller, AD FS |

\* Windows Server 2012 and Windows Server 2012 R2 will reach extended end of support on October 10, 2023. You should plan to upgrade those servers as Microsoft will no longer support the Defender for Identity sensor on devices running Windows Server 2012 and Windows Server 2012 R2.

\*\* Requires [KB4487044](https://support.microsoft.com/topic/february-12-2019-kb4487044-os-build-17763-316-6502eb5d-dde8-6902-e149-27ef359ed616) or a newer cumulative update. Sensors installed on Server 2019 without this update will be automatically stopped if the file version of the *ntdsai.dll* file in the system directory is older than *10.0.17763.316*.

## Install Defender for Identity

Make sure to install Defender for Identity on Windows 2012 and higher on a server with minimum of 2 cores, 6 GB of RAM, and 6 GB of disk space. For more information, see [Minimum system requirements](#minimum-system-requirements).

1. Download the Defender for Identity sensor from the [Microsoft 365 Defender portal](https://security.microsoft.com) in the **Settings** -> **Identities** -> **Sensors** page.
   * Copy the **Access key**. You’ll need it for the installation.
   * You only need to download the installer once, as it can be used for every server in the tenant.
2. Verify that the servers you intend to install Defender for Identity sensors on can reach the Defender for Identity cloud service, by accessing https://\*your-instance-name\*sensorapi.atp.azure.com.
   * To get your instance name, see the [About page](https://security.microsoft.com/settings/identities) in the portal.
   * For proxy configuration, see [Configure proxy settings for your sensor](configure-proxy.md).
3. From the domain controller, run the installer downloaded in step 1 and follow the instructions on the screen.
   * For deployment on multiple domain controllers, use the silent installation.

### Notes

* For optimal performance, set the **Power Option** of the machine running the Defender for Identity sensor to **High Performance**.
* The domain controller can be a read-only domain controller (RODC).
* If you’re installing on an AD FS farm, we recommend installing the sensor on each AD FS server, or at least on the primary node.
* During installation, if .NET Framework 4.7 or later isn’t installed, the .NET Framework 4.7 will be installed and might require a reboot of the server. A reboot might also be required if there’s a restart already pending. So when installing the sensors, consider scheduling a maintenance window for the domain controllers.
* For Windows Server 2012, the Defender for Identity sensor isn’t supported in [Multiple Processor Group mode](/windows/win32/procthread/processor-groups). For more information about multi-processor group mode, see the [troubleshooting article](../troubleshooting-known-issues.md#multi-processor-group-mode).
* When running as a virtual machine, all memory is required to be allocated to the virtual machine at all times.

## Next steps

For more detailed installation instructions, see the links in [Deploy Microsoft Defender for Identity with Microsoft 365 Defender](deploy-defender-identity.md).

# Deploy Microsoft Defender for Identity with Microsoft 365 Defender

This article describes how to deploy Microsoft Defender for Identity with Microsoft 365 Defender.

## Start using Microsoft 365 Defender

1. Sign in to [Microsoft 365 Defender](https://security.microsoft.com).

2. From the navigation menu, select any item, such as **Incidents & alerts**, **Hunting**, **Action center**, or **Threat analytics** to initiate the onboarding process.

You’ll then be given the option to deploy supported services, including Microsoft Defender for Identity. When you go to the Defender for Identity settings, the required cloud components will be auto-provisioned.

For more information about these steps, see the following articles:

* [Microsoft Defender for Identity in Microsoft 365 Defender](/microsoft-365/security/defender/microsoft-365-security-center-mdi?bc=/defender-for-identity/breadcrumb/toc.json&toc=/defender-for-identity/TOC.json)
* [Get started with Microsoft 365 Defender](/microsoft-365/security/defender/get-started)
* [Turn on Microsoft 365 Defender](/microsoft-365/security/defender/m365d-enable)
* [Deploy supported services](/microsoft-365/security/defender/deploy-supported-services)
* [Frequently asked questions when turning on Microsoft 365 Defender](/microsoft-365/security/defender/m365d-enable-faq)

[!IMPORTANT] Currently, Defender for Identity data centers are deployed in Europe, UK, North America/Central America/Caribbean, Australia East, and Asia. Your instance is created automatically in the Azure region closest to the geographical location of your Azure Active Directory tenant. Once created, Defender for Identity instances aren’t movable.

## Prepare

Use the following articles to prepare for your Defender for Identity deployment:

1. [Defender for Identity prerequisites](prerequisites.md).
2. [Plan your Defender for Identity capacity](capacity-planning.md).
3. [Configure Windows Event collection](configure-windows-event-collection.md).
4. [Directory Service accounts](directory-service-accounts.md).
5. [Role groups](role-groups.md).
6. [Configure remote calls to SAM](remote-calls-sam.md).

[!NOTE] To test and see if your environment has the necessary prerequisites, you can run the Test-MdiReadiness.ps1 script. For more information, see [the script’s page](https://github.com/microsoft/Microsoft-Defender-for-Identity/tree/main/Test-MdiReadiness).

## Deploy

Use the following articles to deploy and configure your Defender for Identity sensor:

1. [Download the Defender for Identity sensor](download-sensor.md).
2. [Proxy configuration](configure-proxy.md).
3. [Install the Defender for Identity sensor](install-sensor.md).
4. [Manage action accounts](manage-action-accounts.md).
5. [Configure the Defender for Identity sensor](configure-sensor-settings.md) to start receiving data.

The following articles provide extra guidance for specific scenarios:

* [Installing on Active Directory Federation Services](active-directory-federation-services.md)
* [Multi-forest support](multi-forest.md)
* [Migrate from Advanced Threat Analytics (ATA)](migrate-from-ata-overview.md)

### Standalone sensor

If you deploy Defender for Identity standalone sensors, you’ll need to do the following steps:

1. [Configure port mirroring](configure-port-mirroring.md)
2. [Validate port mirroring](configure-port-mirroring.md#validate-port-mirroring)
3. [Listen for SIEM events on your Defender for Identity standalone sensor](configure-event-collection.md)
4. [Configure Windows event forwarding to your Defender for Identity standalone sensor](configure-event-forwarding.md)

For more information, see [Windows event collection overview](event-collection-overview.md).

## Next steps

[!div class=“step-by-step”] [Defender for Identity prerequisites »](prerequisites.md)

# Plan and prepare

## Microsoft Defender for Identity prerequisites

This article describes the requirements for a successful Microsoft Defender for Identity deployment.

### Licensing requirements

Before deploying Defender for Identity, make sure to acquire one of the following Microsoft 365 licenses:

* Enterprise Mobility + Security E5 (EMS E5/A5)
* Microsoft 365 E5 (M365 E5/A5/G5)
* Microsoft 365 E5/A5/G5 Security

Acquire your licenses directly via the [Microsoft 365 portal](https://www.microsoft.com/cloud-platform/enterprise-mobility-security-pricing) or use the Cloud Solution Partner (CSP) licensing model

Defender for Identity also supports standalone licenses.

For more information, see [Licensing and privacy](/defender-for-identity/technical-faq#licensing-and-privacy).

### Required permissions

To create your Defender for Identity instance, you’ll need an Azure Active Directory (Azure AD) tenant with at least one Global or Security administrator.

Each Defender for Identity instance supports multiple Active Directory forest boundaries and Forest Functional Levels (FFL), for Windows 2003 and higher.

You’ll need Global or Security administrator access on your tenant to access the **Identity** section of the Microsoft 365 Defender **Settings** area and create the workspace.

For more information, see [Microsoft Defender for Identity role groups](role-groups.md).

### Defender for Identity firewall requirements

Use the **AzureAdvancedThreatProtection** Azure service tag to enable access to Defender for Identity.

For more information about service tags, see [Virtual network service tags](/azure/virtual-network/service-tags-overview) or [download the service tags](https://www.microsoft.com/download/details.aspx?id=56519) file.

### Required network adapters

The Defender for Identity sensor monitors local traffic on all of the domain controller’s network adapters.

After deployment, you’ll use the Microsoft 365 Defender portal to modify which network adapters are monitored.

When you install the Defender for Identity sensor on a machine configured with a NIC teaming adapter and the Winpcap driver, you’ll receive an installation error.

To install the Defender for Identity sensor on a machine configured with NIC teaming, make sure you replace the Winpcap driver with Npcap. For more information, see [How do I download and install or upgrade the Npcap driver?](../technical-faq.yml#how-do-i-download-and-install-or-upgrade-the-npcap-driver)

### Sensor requirements

The following table summarizes requirements for the domain controller server where you’ll install the Defender for Identity sensor.

| Prerequisite / Recommendation | Description |
| --- | --- |
| **Specifications** | Make sure to install Defender for Identity on Windows version 2012 or higher, on a domain controller server with a minimum of:- 2 cores- 6 GB of RAM- 6 GB of disk space required, 10 GB recommended, including space for Defender for Identity binaries and logs Defender for Identity supports read-only domain controllers (RODC). |
| **Performance** | For optimal performance, set the **Power Option** of the machine running the Defender for Identity sensor to **High Performance**. |
| **Maintenance window** | We recommend scheduling a maintenance window for your domain controllers, as a restart might be required if the installation runs and a restart is already pending, or if .NET Framework needs to be installed. If .NET Framework version 4.7 or later isn’t already found on the system, .NET Framework version 4.7 is installed, and may require a restart. |

#### Minimum operating system requirements

The following table lists installation support across several operating system versions:

| Operating system version | Server with Desktop Experience | Server Core | Nano Server | Supported installations |
| --- | --- | --- | --- | --- |
| Windows Server 2012 [1](#eos) [2](#mpg) | ✔ | ✔ | Not applicable | Domain controller |
| Windows Server 2012 R2 [1](#eos) | ✔ | ✔ | Not applicable | Domain controller |
| Windows Server 2016 | ✔ | ✔ | Not supported | Domain controller, AD FS |
| Windows Server 2019 [3](#kb) | ✔ | ✔ | Not supported | Domain controller, AD FS |
| Windows Server 2022 | ✔ | ✔ | Not supported | Domain controller, AD FS |

1 Windows Server 2012 and Windows Server 2012 R2 will reach extended end of support on **October 10, 2023**. We recommend that you plan to upgrade those servers by that point, as Microsoft will no longer support the Defender for Identity sensor on devices running Windows Server 2012 and Windows Server 2012 R2.

2 For Windows Server 2012, the Defender for Identity sensor isn’t supported in a [Multi Processor Group mode](/windows/win32/procthread/processor-groups). For more information, see [Multi Processor Group mode troubleshooting](../troubleshooting-known-issues.md#multi-processor-group-mode).

3 Requires [KB4487044](https://support.microsoft.com/topic/february-12-2019-kb4487044-os-build-17763-316-6502eb5d-dde8-6902-e149-27ef359ed616) or a newer cumulative update. Sensors installed on Server 2019 without this update will be automatically stopped if the *ntdsai.dll* file version found in the system directory is older than *10.0.17763.316*.

#### Required ports

| **Protocol** | **Transport** | **Port** | **From** | **To** |
| --- | --- | --- | --- | --- |
| **Internet ports** |  |  |  |  |
| **SSL** (\*.atp.azure.com) | TCP | 443 | Defender for Identity sensor | Defender for Identity cloud service |
| **Internal ports** |  |  |  |  |
| **DNS** | TCP and UDP | 53 | Defender for Identity sensor | DNS Servers |
| **Netlogon** (SMB, CIFS, SAM-R) | TCP/UDP | 445 | Defender for Identity sensor | All devices on the network |
| **RADIUS** | UDP | 1813 | RADIUS | Defender for |
| Identity sensor |  |  |  |  |
| **Localhost ports** [1](#localhost) Required for the sensor service updater |  |  |  |  |
| **SSL** (localhost) | TCP | 444 | Sensor service | Sensor updater service |
| **NNR ports** [2](#nnr) |  |  |  |  |
| **NTLM over RPC** | TCP | Port 135 | Defender for Identity sensor | All devices on network |
| **NetBIOS** | UDP | 137 | Defender for Identity sensor | All devices on network |
| **RDP** | TCP | 3389, only the first packet of Client hello | Defender for Identity sensor | All devices on network |

1 By default, localhost to localhost traffic is allowed unless a custom firewall policy blocks it.

2 While only one of the listed ports is required, we recommend opening all of them.

#### Dynamic memory requirements

The following table describes memory requirements on the server used for the Defender for Identity sensor, depending on the type of virtualization you’re using:

| VM running on | Description |
| --- | --- |
| **Hyper-V** | Ensure that **Enable Dynamic Memory** isn’t enabled for the VM. |
| **VMware** | Ensure that the amount of memory configured and the reserved memory are the same, or select the **Reserve all guest memory (All locked)** option in the VM settings. |
| **Other virtualization host** | Refer to the vendor supplied documentation on how to ensure that memory is fully allocated to the VM at all times. |

[!IMPORTANT] When running as a virtual machine, all memory must be allocated to the virtual machine at all times.

### More resources

For more information, see [Defender for Identity architecture](../architecture.md)

### Next steps

[!div class=“step-by-step”] [Plan capacity for Microsoft Defender for Identity »](capacity-planning.md)

## Plan capacity for Microsoft Defender for Identity deployment

In this article, you’ll learn how to determine what resources you need for your Microsoft Defender for Identity sensors.

### Prerequisites

* Download the [Defender for Identity Sizing Tool](https://aka.ms/mdi/sizingtool).
* Review the [Defender for Identity architecture](../architecture.md) article.
* Review the [Defender for Identity prerequisites](prerequisites.md) article.

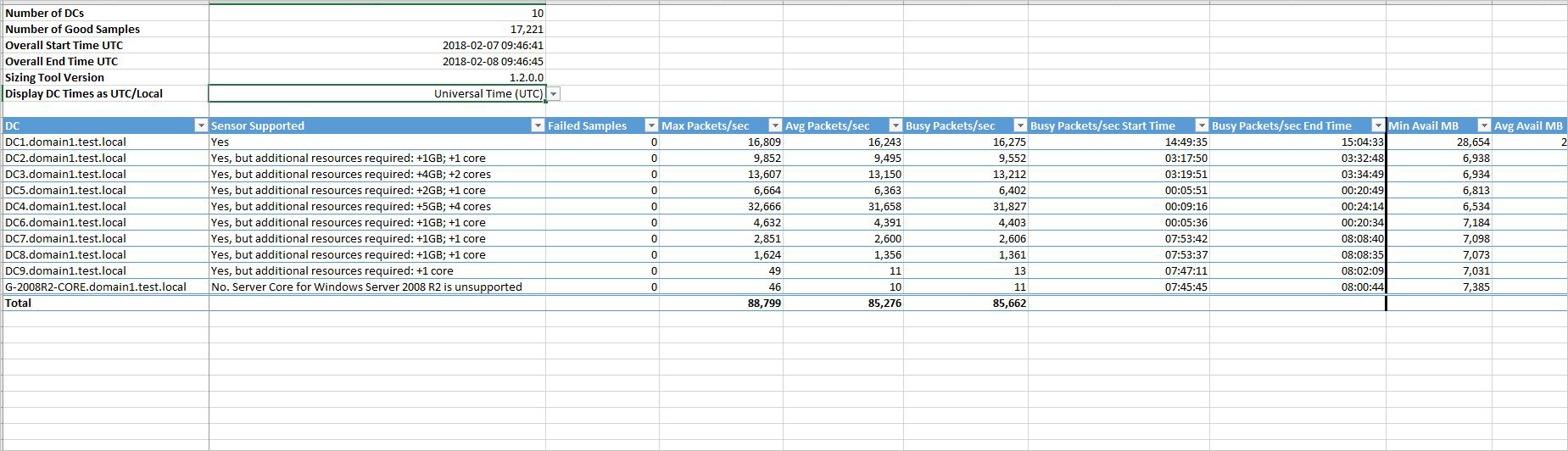
### Use the sizing tool

The recommended and simplest way to determine capacity for your Defender for Identity deployment is to use the Defender for Identity Sizing Tool.

[!TIP] If you’re unable to use the tool, you can manually gather traffic information instead. For more information, see [Domain controller traffic estimator](#manual-sizing).

**To determine capacity with the sizing tool**:

1. Run the Defender for Identity Sizing Tool, **TriSizingTool.exe**, from the zip file you downloaded.
2. When the tool finishes running, open the Excel file results.
3. In the Excel file, locate and select the **Azure ATP Summary** sheet.

* For example:
* 
* Screenshot of a sample capacity planning tool.
* The other sheet isn’t needed since it’s for ATA planning.

1. Locate the **Busy Packets/sec** field in the Azure ATP sensor table in the results Excel file and make a note of it.
2. Match your **Busy Packets/sec** field to the **PACKETS PER SECOND** field in the [Defender for Identity sensor table](#sizing) section of this article. Use the fields to determine the memory and CPU that will be used by the sensor.

[!NOTE] To ensure accurate results, only run the sizing tool before you’ve installed any Defender for Identity sensors in your environment.

### Defender for Identity sensor sizing

A Defender for Identity sensor can support the monitoring of a domain controller based on the amount of network traffic the domain controller generates. The following table is an estimate. The final amount that the sensor parses is dependent on the amount of traffic and the distribution of traffic.

The following CPU and Random Access Memory (RAM) capacity refers to the **sensor’s own consumption**, not the domain controller capacity.

| Packets per second | CPU (physical cores) [1](#phys) | RAM (GB) |
| --- | --- | --- |
| 0-1k | 0.25 | 2.50 |
| 1k-5k | 0.75 | 6.00 |
| 5k-10k | 1.00 | 6.50 |
| 10k-20k | 2.00 | 9.00 |
| 20k-50k | 3.50 | 9.50 |
| 50k-75k | 5.50 | 11.50 |
| 75k-100k | 7.50 | 13.50 |

1 CPU capacity doesn’t include hyper-threaded cores. We recommend that you don’t work with hyper-threaded cores, which can result in health issues in the Defender for Identity sensor.

When determining sizing, keep in mind the total number of cores and total amount of memory that will be used by the sensor service.

[!IMPORTANT] While domain controller performance may not be affected if the server doesn’t have required resources, the Defender for Identity sensor may not operate as expected.

For more information, see [Microsoft Defender for Identity prerequisites](prerequisites.md).

### Domain controller traffic estimation

If for some reason you can’t use the Defender for Identity Sizing Tool, manually gather the packet/sec counter information from each of your domain controllers instead.

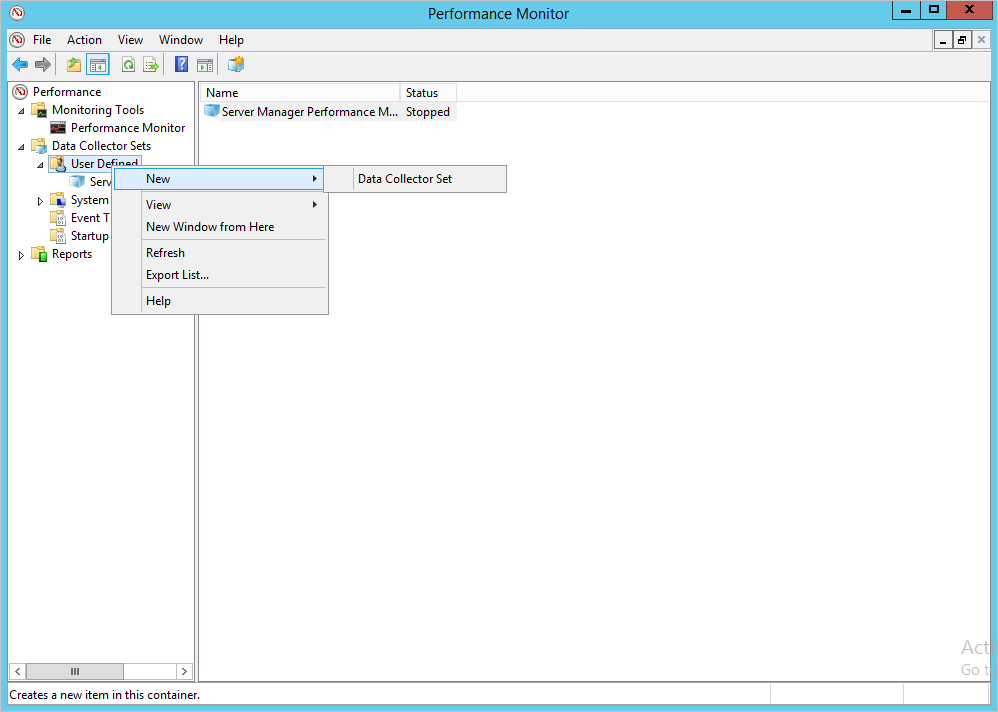
Gather the information for 24 hours with a low collection interval, of approximately 5 seconds each. Then, for each domain controller, calculate the total daily average and the average busiest period of 15 minutes.

This section describes how to collect the packets/sec counter from a domain controller.

[!TIP] There are various tools that you can use to discover the average packets per second of your domain controllers. If you don’t have any tools that track this counter, you can use the Windows Performance Monitor to gather the required information.

**On each domain controller**:

1. Open Performance Monitor and select **Data Collector Sets**. Then right-click **User Defined > New > Data Collector Set**. For example:

* 
* Screenshot of the Performance Monitor with the Data Collector Sets node selected.

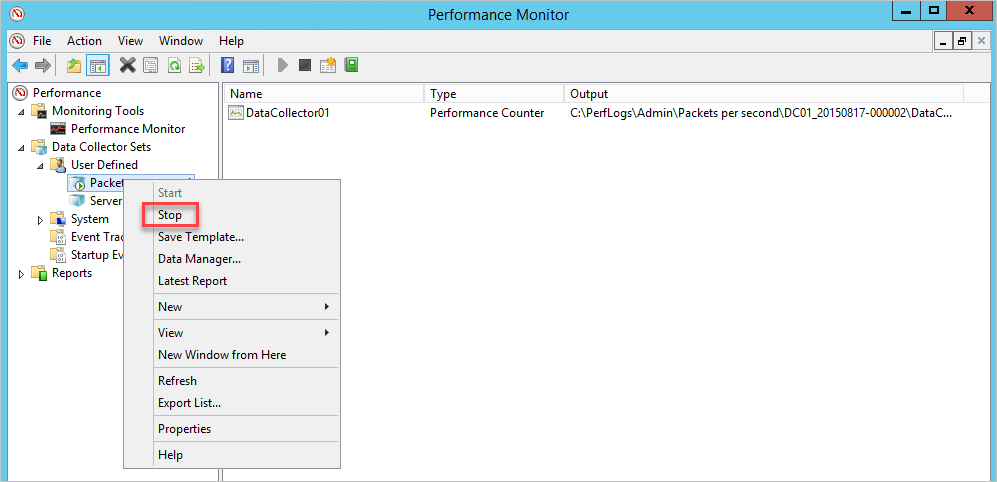
1. Enter a name for the collector set and select **Create Manually (Advanced) > Next**.
2. On the **What type of data do you want to include?** dialog, select **Create data logs** > **Performance counter**.
3. On the **Which performance counters would you like to log** dialog, select **Add** > **Network Adapter** > **Packets/sec**. Select the relevant instance, and then select **Add > OK**.

* If you aren’t sure which instance to select, select **<All instances>**.
* [!NOTE] To perform this operation in a command line, run ipconfig /all to see the name of the adapter it’s and configuration.

1. Change the **Sample interval** to **five seconds**, and then define the location where you want the data to be saved.
2. On the **Create the data collector set** dialog, select **Start this data collector set now**, and then select **Finish**.

* The data collector set you created is now shown with a green triangle, indicating that it’s working as expected.

1. After 24 hours, stop the data collector set. Right-click the data collector set and select **Stop**. For example:

* 
* Screenshot of the Performance Monitor dialog showing the Stop option.

1. In the File Explorer, browse to the folder where the **.blg** file was saved. Double-click the **.blg** file to open it in Performance Monitor.
2. Select the **Packets/sec** counter, and record the average and maximum values. For example:

* 
* Screenshot of the Performance Monitor dialog with the Packets/sec counter selected.

[!NOTE] By default, Defender for Identity supports up to 350 sensors. To install more sensors, contact Defender for Identity support.

### Next steps

[!div class=“step-by-step”] [« Prerequisites](prerequisites.md) [Microsoft Defender for Identity Directory Service account recommendations »](directory-service-accounts.md)

## Configure a Directory Service account for Microsoft Defender for Identity

Defender for Identity’s Directory Service account (DSA) is used by the sensor to do the following:

* Connect to the domain controller at startup using the configured DSA option
* Query the domain controller for data on entities seen in network traffic, monitored events, and monitored ETW activities

One sensor in each domain is defined as the *domain synchronizer*, and is responsible for tracking changes to the entities in the domain, like objects created, entity attributes tracked by Defender for Identity and so on.

If a sensor detects activities in other domains, it queries the other domain via LDAP for more details.

Defender for Identity requests the member list for the local administrator group from devices seen in network traffic, events, and ETQ activities via an [SAM-R call](remote-calls-sam.md) made to the device. Collected data is used to calculate potential lateral movement paths.

This article describes how to create and configure a Defender for Identity DSA.

[!NOTE] By default, Defender for Identity supports up to 30 credentials. To add more credentials, contact Defender for Identity support.

### Supported DSA account options

Defender for Identity supports the following DSA options:

* **gMSA** (Recommended). Provides a more secure deployment and password management. Active Directory manages the creation and rotation of the account’s password, just like a computer account’s password, and you can control how often the account’s password is changed.
* gMSA requires extra setup steps.
* **Regular user account**. Easy to use when getting started, and simpler to configure read permissions between trusted forests, but requires extra overhead for password management.
* A regular user account is less secure, as it requires you to create and manage passwords, and can lead to downtime if the password expires and isn’t updated for both the user and the DSA.

### DSA entry usage

This section describes how to understand how many DSA entries are used and how the sensor selects the DSA entry to use in any given scenario.

Defender for Identity requires at least one DSA entry, with read permissions to all the domains in the forests. In an untrusted, multi-forest environment, a DSA account is required for each forest.

Defender for IoT gets a list of DSA entries configured for Defender for Identity, and selects an entry to use.

#### Single DSA entry

When only one DSA entry is configured, the sensor attempts to use the configured DSA entry in the following scenarios:

* At start up, as a reaction to a new domain contacting the domain controller
* Each time a SAM-R query is made
* Whenever a connection needs to be recreated

Sensor attempts differ, depending on the type of DSA entry:

| Type | Description |
| --- | --- |
| **gMSA account** | The sensor attempts to retrieve the gMSA account password from Active Directory, and then sign into the domain. |
| **Regular user account** | The sensor attempts to sign into the domain controller using the configured username and password. |

#### Multiple DSA entries

When there are multiple DSA entries configured, the following logic is applied:

1. The sensor looks for an entry with an exact match of the domain name for the target domain. If an exact match is found, the sensor attempts to authenticate using the credentials in that entry.
2. If there isn’t an exact match, or if the authentication failed, the sensor searches the list for an entry to the parent domain using DNS FQDN, and attempts to authenticate using the credentials in the parent entry instead.
3. If there isn’t an entry for the parent domain, or if the authentication failed, the sensor searches the list for an sibling domain entry, using the DNS FQDN, and attempts to authenticate using the credentials in the sibling entry instead.
4. If there isn’t an entry for the sibling domain, or if the authentication failed, the sensor reviews the list again and tries to authenticate again with each entry until it succeeds. DSA gMSA entries have higher priority than regular DSA entries.

For example, the sensor tries the DSA entries in the following order:

1. The sensor looks for a match between the DNS domain name of the target domain, such as emea.contoso.com and the DSA gMSA entry, such as emea.contoso.com.
2. The sensor looks for a match between the DNS domain name of the target domain, such as emea.contoso.com and the DSA regular entry DSA, such as emea.contoso.com
3. The sensor looks for a match in the root DNS name of the target domain, such as emea.contoso.com and the DSA gMSA entry domain name, such as contoso.com.
4. The sensor looks for a match in the root DNS name of the target domain, such as emea.contoso.com and the DSA regular entry domain name, such as contoso.com.
5. The sensor looks for the target domain name for a sibling domain, such as emea.contoso.com and the DSA gMSA entry domain name, such as apac.contoso.com.
6. The sensor looks for the target domain name for a sibling domain, such as emea.contoso.com and the DSA regular entry domain name, such as apac.contoso.com.
7. The sensor runs a round robin of all DSA gMSA entries.
8. The sensor runs a round robin of all DSA regular entries.

For another example, if the DSA entires configured are as follows:

* DSA1.northamerica.contoso.com
* DSA2.EMEA.contoso.com DSA3.fabrikam.com

Then the following table lists the sensors and the DSA entry that’s used first:

| Domain controller FQDN | DSA entry used |
| --- | --- |
| DC01.contoso.com | Round robin |
| DC02.fabrikam.com | DSA3.fabrikam.com |
| DC03.emea.contoso.com | DSA2.emea.contoso.com |
| DC04.contoso.com | Round robin |

[!NOTE]

* In a multi-domain forest, we recommend that you create the DSA account in the domain with the largest number of domain controllers.
* In multi-forest, multi-domain environment, consider creating a DSA entry for each domain in the environment to avoid failed authentications from being recorded due to the round robin method.

[!IMPORTANT] If a sensor isn’t able to successfully authenticate via LDAP to the Active Directory domain at startup, the sensor won’t enter a running state and a health issue is generated. For more information, see [Defender for Identity health issues](../health-alerts.md).

### Create a gMSA account for use with Defender for Identity

This section describes how to create a gMSA account for use as a Defender for Identity DSA entry. For more information, see [Getting started with Group Managed Service Accounts](/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts).

[!TIP] In multi-forest, multi-domain environments, we recommend creating the gMSAs with a unique name for each forest or domain. Also, create a universal group in each domain, containing all sensors’ computer accounts so that all sensors can retrieve the gMSAs’ passwords, and perform the cross-domain authentications.

#### Grant permissions to retrieve the gMSA account’s password

Before you create the gMSA account, consider how to assign permissions to retrieve the account’s password.

When using a gMSA entry, the sensor needs to retrieve the gMSA’s password from Active Directory. This can be done either by assigning to each of the sensors or by using a group.

* **In a single-forest, single-domain deployment**, if you aren’t planning to install the sensor on any AD FS servers, you can use the built-in Domain Controllers security group.
* **In a forest with multiple domains**, when using a single DSA account, we recommend creating a universal group and adding each of the domain controllers and AD FS servers to the universal group.

If you add a computer account to the universal group after the computer received its Kerberos ticket, it won’t be able to retrieve the gMSA’s password until it receives a new Kerberos ticket. The Kerberos ticket has a list of groups that an entity is a member of when the ticket is issued.

In such scenarios, do one of the following:

1. Wait for new Kerberos ticket to be issued. Kerberos tickets are normally valid for 10 hours.

1.Reboot the server. When the server is rebooted, a new Kerberos ticket is requested with the new group membership.

1. Purge the existing Kerberos tickets. This forces the domain controller to request a new Kerberos ticket.

* To purge the tickets, from an administrator command prompt on the domain controller, run the following command: klist purge -li 0x3e7

#### Create the gMSA account

This section describes how to create a specific group that can retrieve the account’s password, create a gMSA account, and then test that the account is ready to use.

Run the following PowerShell commands as an administrator:

# Set the variables:   
$gMSA\_AccountName = 'mdiSvc01'   
$gMSA\_HostsGroupName = 'mdiSvc01Group'   
$gMSA\_HostNames = 'DC1', 'DC2', 'DC3', 'DC4', 'DC5', 'DC6', 'ADFS1', 'ADFS2'   
# Import the required PowerShell module:   
Import-Module ActiveDirectory   
# Create the group and add the members   
$gMSA\_HostsGroup = New-ADGroup -Name $gMSA\_HostsGroupName -GroupScope Global -PassThru   
$gMSA\_HostNames | ForEach-Object { Get-ADComputer -Identity $\_ } |   
 ForEach-Object { Add-ADGroupMember -Identity $gMSA\_HostsGroupName Members $\_ }   
# Or, use the built-in 'Domain Controllers' group if the environment is a single forest, and will contain only domain controller sensors   
# $gMSA\_HostsGroup = Get-ADGroup -Identity 'Domain Controllers'   
# Create the gMSA:   
New-ADServiceAccount -Name $gMSA\_AccountName -DNSHostName   
"$gMSA\_AccountName.$env:USERDNSDOMAIN" `   
-PrincipalsAllowedToRetrieveManagedPassword $gMSA\_HostsGroupName

#### Grant required DSA permissions

The DSA requires read permissions on all objects in Active Directory, including the **Deleted Objects** container.

The read-only permissions on the **Deleted Objects** container allows Defender for Identity to detect user deletions from your Active Directory.

Use the following code sample to help you grant the required read permissions on the **Deleted Objects** container:

# Declare the \*user\* or \*group\* that needs to have read access to the deleted objects container   
# Note that if the identity you want to grant the permissions to is a Group   
Managed Service Account (gMSA),   
# you need first to create a security group, add the gMSA as a member and list that group as the identity below $Identity = 'CONTOSO\mdisvc'   
# Get the deleted objects container's distinguished name:   
$distinguishedName = ([adsi]'').distinguishedName.Value   
$deletedObjectsDN = 'CN=Deleted Objects,{0}' -f $distinguishedName   
# Take ownership on the deleted objects container: $params = @("$deletedObjectsDN", '/takeOwnership')   
C:\Windows\System32\dsacls.exe $params   
# Grant the 'List Contents' and 'Read Property' permissions to the user or group:   
$params = @("$deletedObjectsDN", '/G', "$($Identity):LCRP")   
C:\Windows\System32\dsacls.exe $params   
# To remove the permissions, uncomment the next 2 lines and run them instead of the two prior ones:  
# $params = @("$deletedObjectsDN", '/R', $Identity)  
# C:\Windows\System32\dsacls.exe $params

For more information, see [Changing permissions on a deleted object container](/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc816824(v=ws.10)).

#### Install the gMSA account

To install the gMSA account, run the following commands as an administrator, locally on each of the servers:

# Import the required PowerShell module:  
Import-Module ActiveDirectory  
  
# Install the gMSA account  
Install-ADServiceAccount -Identity 'mdiSvc01'

#### Validate that the domain controller can retrieve the gMSA’s password

To validate that the server has the required permissions to retrieve the gMSA’s password, run the following PowerShell command:

Test-ADServiceAccount -Identity 'mdiSvc01'

If it has the permissions, the command will return a **True** message.

[!NOTE] If you get an error message when running Test-ADServiceAccount, either restart the server or run klist purge -li 0x3e7 and try again.

#### Verify that the gMSA account has the required rights

The Defender for Identity sensor service, *Azure Advanced Threat Protection Sensor*, runs as a *LocalService* and performs impersonation of the DSA account. The impersonation will fail if the *Log on as a service* policy is configured but the permission hasn’t been granted to the gMSA account. In such cases, you’ll see the following health issue: **Directory services user credentials are incorrect.**

If you see this alert, we recommend checking to see if the *Log on as a service policy* is configured. If you need to configure the *Log on as a service* policy, do so either in a Group Policy setting or in a Local Security Policy.

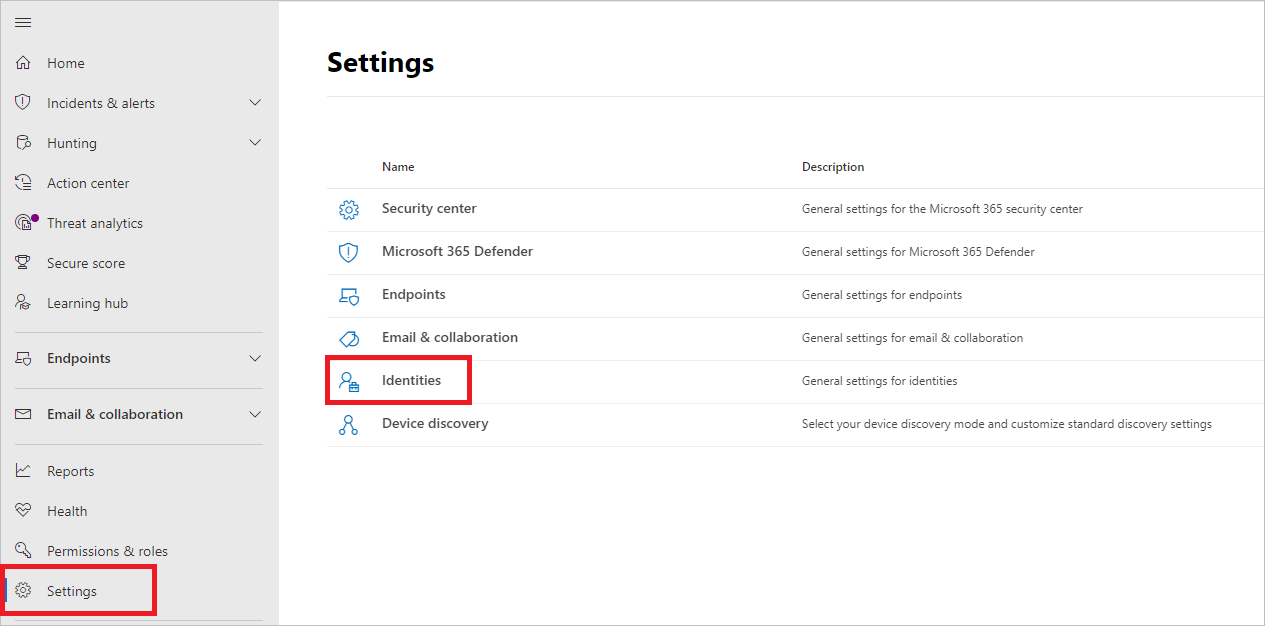
* **To check the Local Policy**, run secpol.msc and select **Local Policies**. Under **User Rights Assignment**, go to the **Log on as a service policy** setting. For example:
* :::image type=“content” source=“../media/log-on-as-a-service.png” alt-text=“Screenshot of the log on as a service properties.”:::
* If the policy is enabled, add the gMSA account to the list of accounts that can log on as a service.
* **To check if the setting is configured in a Group Policy**: Run rsop.msc and see if the **Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> Log on as a service** policy is selected. For example:
* :::image type=“content” source=“../media/log-on-as-a-service-gpmc.png” alt-text=“Screenshot of the Log on as a service policy in the Group Policy Management Editor.” lightbox=“../media/log-on-as-a-service-gpmc.png”:::
* If the setting is configured, add the gMSA account to the list of accounts that can log on as a service in the Group Policy Management Editor.

[!NOTE] If you use the Group Policy Management Editor to configure the **Log on as a service** setting, make sure you add both **NT ServiceServices** and the gMSA account you created.

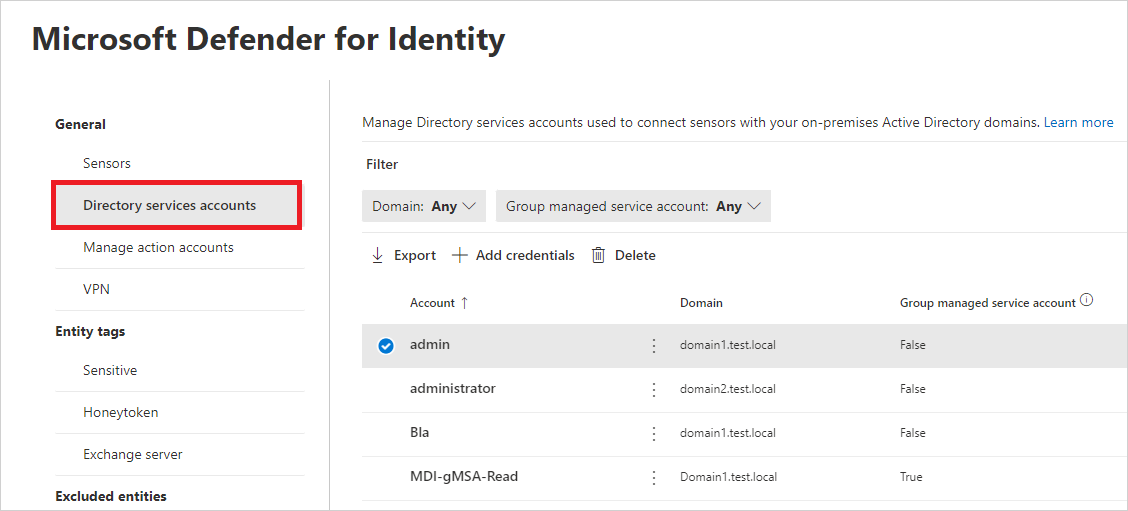
### Configure a Directory Service account in Microsoft 365 Defender

To connect your sensors with your Active Directory domains, you’ll need to configure Directory Service accounts in Microsoft 365 Defender.

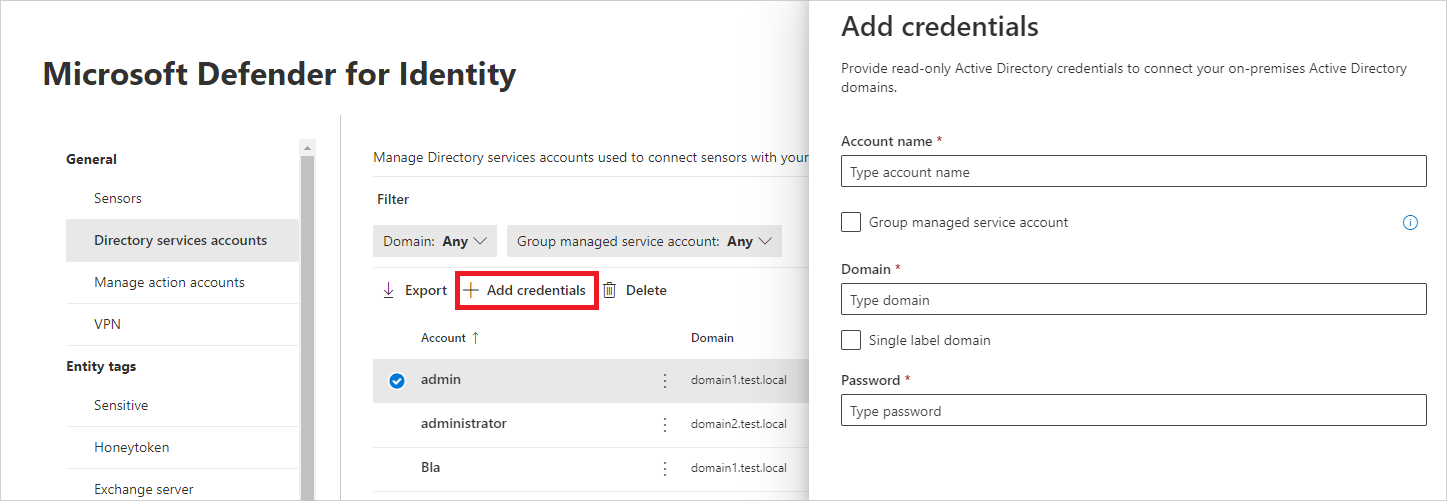
1. In [Microsoft 365 Defender](https://security.microsoft.com/), go to **Settings > Identities**. For example:

* [](../media/settings-identities.png#lightbox)

1. Select **Directory Service accounts**. You’ll see which accounts are associated with which domains. For example:

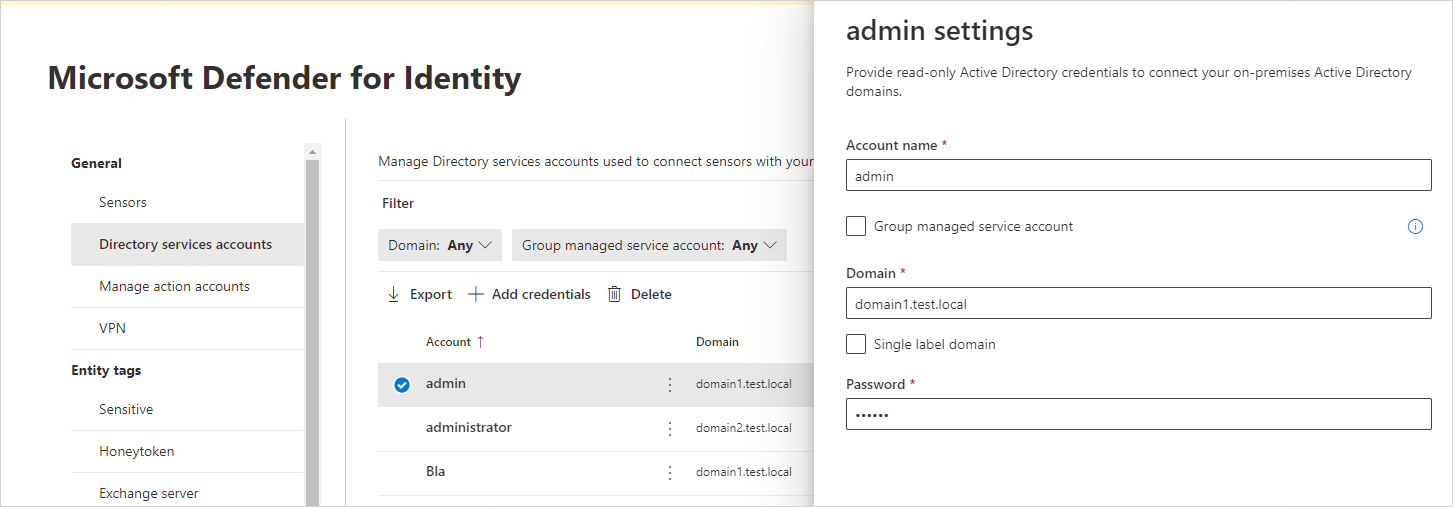
* [](../media/directory-service-accounts.png#lightbox)

1. To add Directory Service account credentials, select **Add credentials** and enter the **Account name**, **Domain**, and **Password** of the account you created earlier. You can also choose if it’s a **Group managed service account** (gMSA), and if it belongs to a **Single label domain**. For example:

* [](../media/new-directory-service-account.png#lightbox)

| Field | Comments |
| --- | --- |
| **Account name** (required) | Enter the read-only AD username. For example: **DefenderForIdentityUser**. - You must use a **standard** AD user or gMSA account. - **Don’t** use the UPN format for your username. - When using a gMSA, the user string should end with the $ sign. For example: mdisvc$**NOTE:** We recommend that you avoid using accounts assigned to specific users. |
| **Password** (required for standard AD user accounts) | For AD user accounts only, generate a strong password for the read-only user. For example: PePR!BZ&}Y54UpC3aB. |
| **Group managed service account** (required for gMSA accounts) | For gMSA accounts only, select **Group managed service account**. |
| **Domain** (required) | Enter the domain for the read-only user. For example: **contoso.com**. It’s important that you enter the complete FQDN of the domain where the user is located. For example, if the user’s account is in domain corp.contoso.com, you need to enter corp.contoso.com not contoso.com. For more information, see [Microsoft support for Single Label Domains](/troubleshoot/windows-server/networking/single-label-domains-support-policy). |

1. Select **Save**.
2. (Optional) If you select an account, a details pane will open with the settings for that account. For example:

* [](../media/account-settings.png#lightbox)

[!NOTE] You can use this same procedure to change the password for standard Active Directory user accounts. There is no password set for gMSA accounts.

#### Troubleshooting

For more information, see [Sensor failed to retrieve the gMSA credentials](../troubleshooting-known-issues.md#sensor-failed-to-retrieve-group-managed-service-account-gmsa-credentials).

### Next steps

[!div class=“step-by-step”] [« Plan capacity for Microsoft Defender for Identity deployment](capacity-planning.md) [Role groups »](role-groups.md)

## Microsoft Defender for Identity roles and permissions

Microsoft Defender for Identity uses Microsoft 365’s role-based access control (RBAC) to manage your user access, so that you can safeguard your data according to your organization’s specific security and compliance needs.

Defender for Identity also supports built-in security groups to define user roles with your tenant’s Azure Active Directory.

This article describes Defender for Identities access management and role authorization, helping you segregate duties within your security team, and granting only the amount of access that users need to do their jobs.

[!INCLUDE [gdpr-intro-sentence](../../includes/gdpr-intro-sentence.md)]

### Permissions required for Defender for Identity in Microsoft 365 Defender

The following table lists the permissions required to access [Defender for Identity in Microsoft 365 Defender](/microsoft-365/security/defender/microsoft-365-security-center-mdi), using either built-in Azure Active Directory role groups or Microsoft 365’s RBAC.

| Actions in Microsoft 365 Defender | Required permissions |
| --- | --- |
| **Create a Defender for Identity workspace** | One of the following Azure AD roles: - Global Administrator - Security Administrator |
| **Configure Defender for Identity settings** | One of the following Azure AD roles:- Global Administrator- Security Administrator **Or** the following [unified RBAC permissions](#Xb8ba7292d693aee6b458b943ee9e7971a0d8812):- Authorization and settings/Security settings/Read- Authorization and settings/Security settings/All permissions- Authorization and settings/System settings/Read- Authorization and settings/System settings/All permissions |
| **View Defender for Identity security alerts and activities** | One of the Azure AD roles required by [Microsoft 365 Defender](/microsoft-365/security/defender/m365d-permissions) **Or** the following [unified RBAC permissions](#Xb8ba7292d693aee6b458b943ee9e7971a0d8812):- Security operations/Security data/Alerts (Manage)- Security operations/Security data/Security data basics (Read) |
| **View Defender for Identity security assessments in Microsoft Secure Score** | - [Permissions to access Microsoft Secure Score](/microsoft-365/security/defender/microsoft-secure-score#required-permissions) - The following [unified RBAC permissions](#Xb8ba7292d693aee6b458b943ee9e7971a0d8812): Security operations/Security data/Security data basics (Read) |
| **View Defender for Identity details in the Assets > Identities page** | One of the following:- [Permissions to access Defender for Cloud Apps](/azure/defender-for-cloud/permissions) One of the Azure AD roles as required by [Microsoft 365 Defender](/microsoft-365/security/defender/m365d-permissions) |

### Defender for Identity built-in security groups

Defender for Identity uses Azure AD security groups as a basis for role groups. Defender for Identity provides the following built-in security groups for your user roles:

* Azure ATP *(Workspace name)* Administrators
* Azure ATP *(Workspace name)* Users
* Azure ATP *(Workspace name)* Viewers

The following table describes the type of access in Defender for Identity available for each role:

| Activity | Azure ATP *(Workspace name)* Administrators | Azure ATP *(Workspace name)* Users | Azure ATP *(Workspace name)* Viewers |
| --- | --- | --- | --- |
| **Change health alert statuses** | ✔ | - | - |
| **Change security alert statuses** (reopen, close, exclude, suppress) | ✔ | ✔ | - |
| **Delete workspace** | ✔ | - | - |
| **Download a report** | ✔ | ✔ | ✔ |
| **Login** | ✔ | ✔ | ✔ |
| **Share/Export security alerts** (via email, get link, download details) | ✔ | ✔ | ✔ |
| **Update Defender for Identity configuration - Updates** | ✔ | - | - |
| **Update Defender for Identity configuration - Entity tags** (sensitive and honeytoken) | ✔ | ✔ | - |
| **Update Defender for Identity configuration - Exclusions** | ✔ | ✔ | - |
| **Update Defender for Identity configuration - Language** | ✔ | ✔ | - |
| **Update Defender for Identity configuration - Notifications** (email and syslog) | ✔ | ✔ | - |
| **Update Defender for Identity configuration - Preview detections** | ✔ | ✔ | - |
| **Update Defender for Identity configuration - Scheduled reports** | ✔ | ✔ | - |
| **Update Defender for Identity configuration - Data sources** (directory services, SIEM, VPN, Defender for Endpoint) | ✔ | - | - |
| **Update Defender for Identity configuration - Sensors** (download, regenerate key, configure, delete) | ✔ | - | - |
| **View entity profiles and security alerts** | ✔ | ✔ | ✔ |

Manage your role groups from the Azure Active Directory [Groups management page](https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/GroupsManagementMenuBlade/AllGroups). Only Azure AD users can be added or removed from security groups.

#### Azure Active Directory mapping

The following table maps Azure Active Directory roles to their Defender for Identity roles.

| Azure Active Directory roles …. | Are automatically mapped to the following Defender for Identity roles |
| --- | --- |
| - Global administrator - Security administrator | Administrator |
| - Security operator | User |
| - Global reader- Security reader | Viewer |

### Mapping built-in role groups to Microsoft 365’s unified RBAC

Microsoft 365’s unified RBAC provides more granular options for defining user access than Defender for Identity’s build-in security groups. Define unified RBAC in Microsoft 365 Defender. For example:

:::image type=“content” source=“../media/choose-permissions.png” alt-text=“Screenshot of the Permissions page in Microsoft 365 Defender.” lightbox=“../media/choose-permissions.png”:::

The following table maps the built-in Defender for Identity role to require permissions in Microsoft 365 Defender:

| Built-in Defender for Identity role | Minimum required Microsoft 365 unified RBAC permissions |
| --- | --- |
| **Administrator** | - Authorization and settings/Security settings/Read- Authorization and settings/Security settings/All permissions-Authorization and settings/System settings/Read-Authorization and settings/System settings/All permissions- Security operations/Security data/Alerts (manage)- Security operations/Security data/Security data basics (Read)- Authorization and settings/Authorization/All permissions - Authorization and settings/Authorization/Read |
| **User** | - Security operations/Security data/Security data basics (Read)- Authorization and settings/System settings/Read- Authorization and settings/Security settings/Read- Security operations/Security data/Alerts (manage)- microsoft.xdr/configuration/security/manage |
| **Viewer** | - Security operations/Security data/Security data basics (Read)- Authorization and settings/System settings/Read- Authorization and settings/Security settings/Read` |

For more information, see [Custom roles in role-based access control for Microsoft 365 Defender](/microsoft-365/security/defender/custom-roles).

#### Migrating from built-in role groups

Legacy customers can migrate any Defender for Identity role groups to Microsoft 365 Defender.

Information included from the [Defender for Cloud Apps activity log](../classic-mcas-integration.md#activities) may still contain Defender for Identity data, which adheres to existing Defender for Cloud Apps permissions.

### Next steps

[!div class=“step-by-step”] [« Directory Service accounts](directory-service-accounts.md) [Configure remote calls to SAM »](remote-calls-sam.md)

## Configure SAM-R to enable lateral movement path detection in Microsoft Defender for Identity

Microsoft Defender for Identity [lateral movement path](/defender-for-identity/understand-lateral-movement-paths) detection relies on queries that identify local admins on specific machines. These queries are performed with the SAM-R protocol, using the Defender for Identity [Directory Service account](directory-service-accounts.md) you configured.

This article describes how to configure required permissions for using the SAM-R protocol.

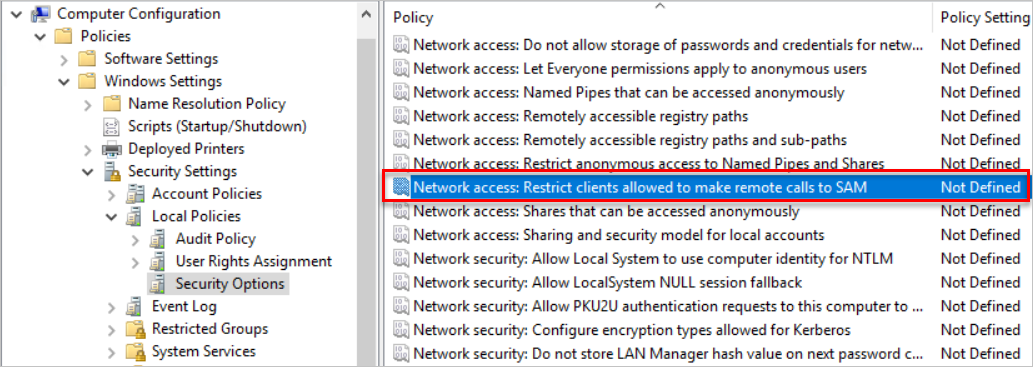
### Configure SAM-R required permissions

To ensure that Windows clients and servers allow your Defender for Identity Directory Service account to perform SAM-R, you must modify the **Group Policy** and add the Defender for Identity Directory Service account, in addition to the configured accounts listed in the **Network access** policy. Make sure to apply group policies to all computers **except domain controllers**.

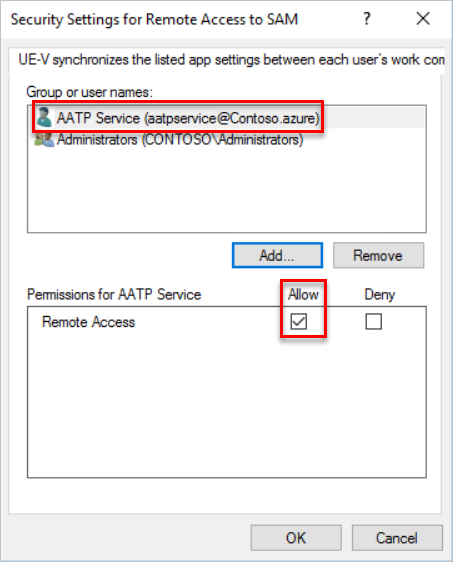
[!NOTE] Perform this procedure in *audit mode* first, verifying the compatibility of the proposed changes before making changes to your production environment.

Testing in audit mode is critical in ensuring that your environment remains secure, and any changes will not impact your application compatibility. You may observe increased SAM-R traffic, generated by the Defender for Identity sensors.

1. Locate the policy. In your **Computer configuration > Windows settings > Security settings > Local policies > Security options**, select the **Network access - Restrict clients allowed to make remote calls to SAM** policy. For example:

* 
* Screenshot of the Network access policy selected.

1. Add the Defender for Identity Directory Service account to the list of approved accounts able to perform this action on your modern Windows systems. For example:

* 
* Screenshot of the Security Settings for Remote Access to SAM dialog.

The Defender for Identity Directory Service account now has the privileges needed to perform SAM-R in the environment.

For more information, see [Network access: Restrict clients allowed to make remote calls to SAM](/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls).

### Add the service account to the list of allowed accounts

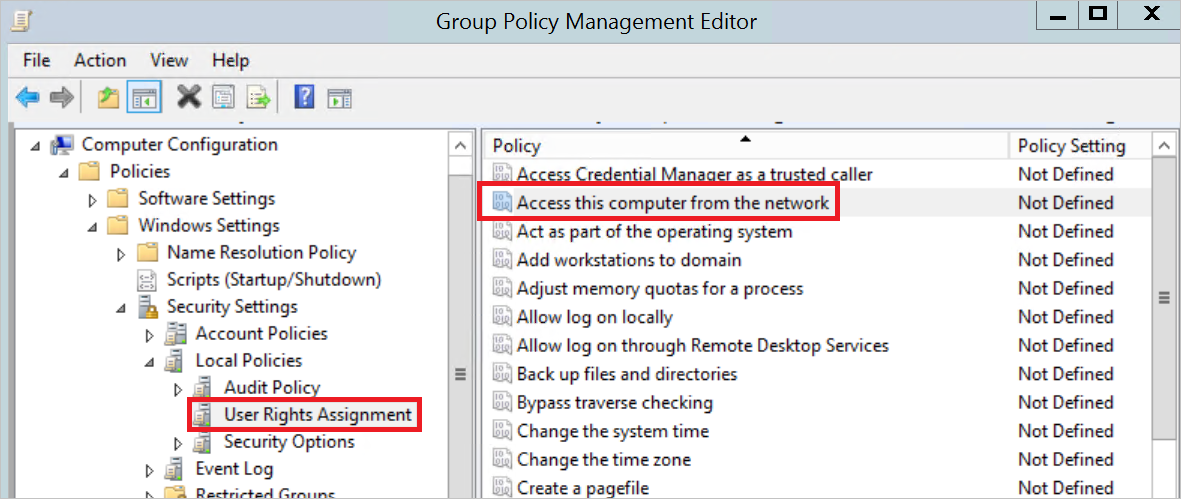
After defining the [*Access this computer from the network*](/windows/security/threat-protection/security-policy-settings/access-this-computer-from-the-network) setting in any GPO that applies to computers in your domain, add the Defender for Identity Directory Service account to the list of allowed accounts for that setting.

This procedure is only required if you’ve previously enabled the [Access this computer from the network](/windows/security/threat-protection/security-policy-settings/access-this-computer-from-the-network) setting. The [Access this computer from the network](/windows/security/threat-protection/security-policy-settings/access-this-computer-from-the-network) setting isn’t enabled by default.

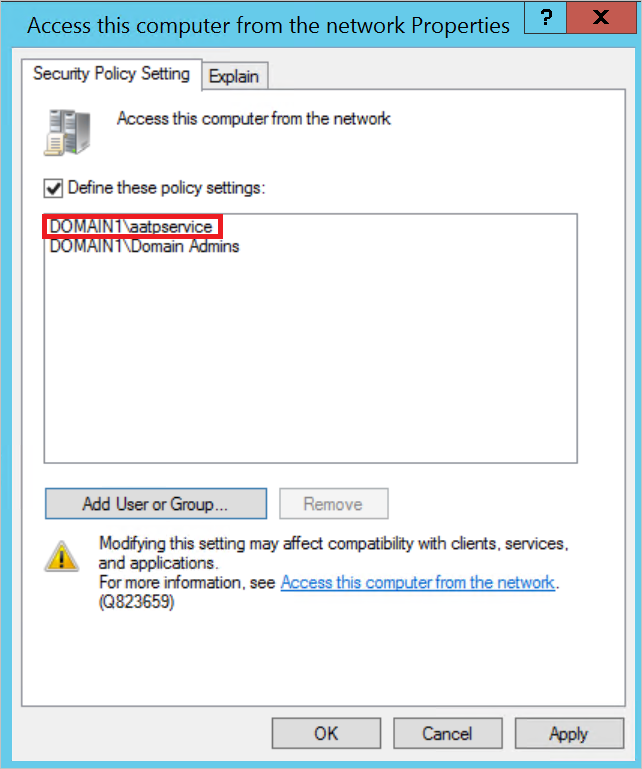
[!NOTE] The [Microsoft Security Compliance Toolkit](https://www.microsoft.com/download/details.aspx?id=55319) recommends replacing the default *Everyone* with *Authenticated Users* to prevent anonymous connections from performing network sign-ins. Review your local policy settings before managing the [Access this computer from the network](/windows/security/threat-protection/security-policy-settings/access-this-computer-from-the-network) setting from a GPO, and consider including *Authenticated Users* in the GPO if needed.

**To add the Defender for Identity service account to the list of allowed accounts**:

1. Go to the policy and navigate to **Computer Configuration** -> **Policies** -> **Windows Settings** -> **Local Policies** -> **User Right Assignment**, and select the **Access this computer from the network** setting. For example:

* 
* Screenshot of the Group Policy Management Editor.

1. Add the Defender for Identity Directory Service account to the list of approved accounts. For example:

* 
* Screenshot of the Access this computer from the network Properties dialog

### Next steps

[!div class=“step-by-step”] [« Role groups](role-groups.md) [Download the Defender for Identity sensor »](download-sensor.md)

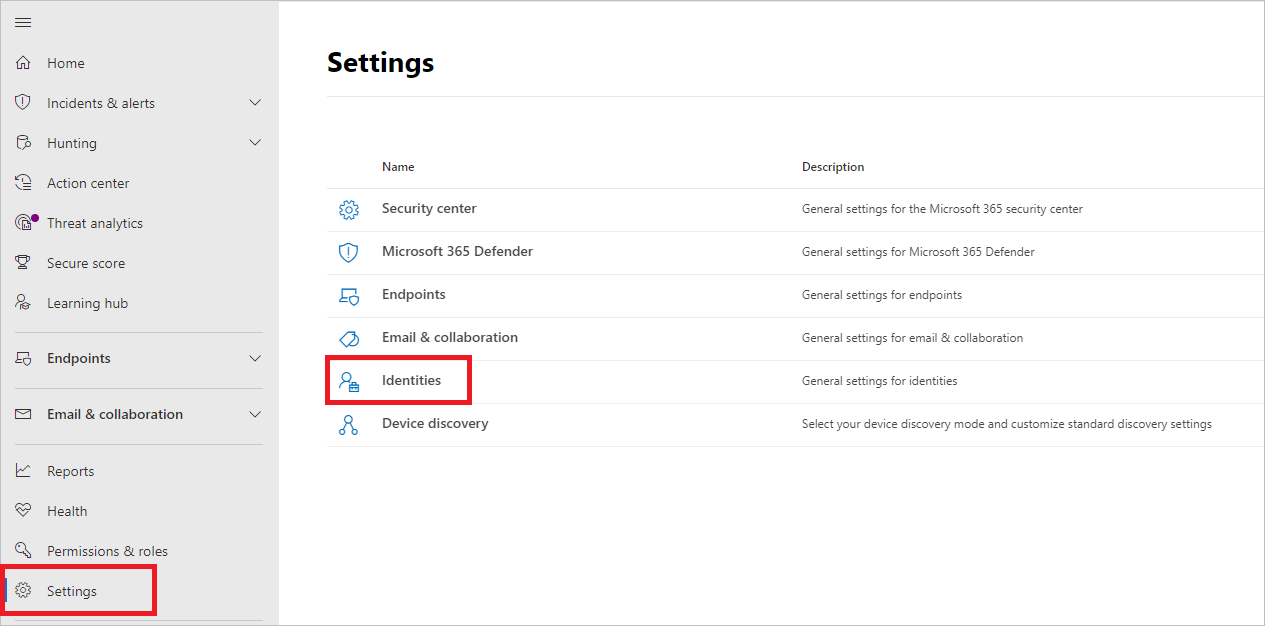
# Deploy Defender for Identity

## Download the Microsoft Defender for Identity sensor

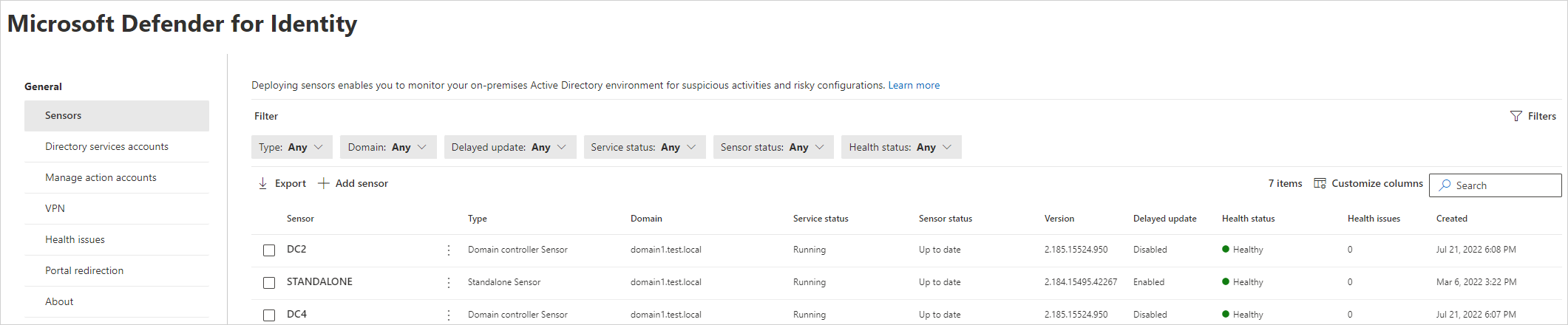
This article describes how to download the Microsoft Defender for Identity sensor for your domain controllers.

### Add and download a sensor

1. In [Microsoft 365 Defender](https://security.microsoft.com), go to **Settings** and then **Identities**. For example:

* 
* Screenshot of the Settings page.

1. Select the **Sensors** tab, which displays all of your Defender for Identity sensors. For example:

* [](../media/sensor-page.png#lightbox)

1. Select **Add sensor**. Then, in the **Add a new sensor** pane, select **Download installer** and save the installation package locally. The downloaded zip file includes the following files:
   * The Defender for Identity sensor installer
   * The configuration setting file with the required information to connect to the Defender for Identity cloud service
2. In the **Add a new sensor** pane, copy the **Access key** value and save it to a secured location. This access key is a one-time password for use when deploying the sensor, after which communication is performed using certificates for authentication and TLS encryption.

* [!TIP] Use the **Regenerate key** button if you ever need to regenerate the new access key. It won’t affect any previously deployed sensors, because it’s only used for initial registration of the sensor.

1. Copy the downloaded installation package to the dedicated server or domain controller where you’re installing the Defender for Identity sensor.

### Next steps

[!div class=“step-by-step”] [« Configure remote calls to SAM](remote-calls-sam.md) [Proxy configuration »](configure-proxy.md)

## Configure endpoint proxy and internet connectivity settings for your Microsoft Defender for Identity sensor

Each Microsoft Defender for Identity sensor requires internet connectivity to the Defender for Identity cloud service to report sensor data and operate successfully.

In some organizations, the domain controllers aren’t directly connected to the internet, but are connected through a web proxy connection, and SSL inspection and intercepting proxies are not supported for security reasons.

In such cases, your proxy server must allow the data to directly pass from the Defender for Identity sensors to the relevant URLs without interception.

Use the command line, Microsoft Windows Internet (WinINet), or the registry to configure your proxy server.

We recommend using the command line to ensure that only the Defender for Identity sensor services communicate through the proxy. When you use WinINet or the registry to configure your proxy, other services running in the context as Local System or Local Service will also direct traffic through the proxy.

[!NOTE] Microsoft does not provide a proxy server. This article describes how to ensure that the required URLs are accessible via a proxy server that you configure.

### Configure a proxy server using the command line

Configure your proxy server during sensor installation using the following command-line switches.

#### Syntax

"Azure ATP sensor Setup.exe" [/quiet] [/Help] [ProxyUrl="http://proxy.internal.com"] [ProxyUserName="domain\proxyuser"] [ProxyUserPassword="ProxyPassword"]

#### Switch descriptions

| Name | Syntax | Mandatory for silent installation? | Description |
| --- | --- | --- | --- |
| **ProxyUrl** | ProxyUrl="http\://proxy.contoso.com:8080" | No | Specifies the proxy URL and port number for the Defender for Identity sensor. |
| **ProxyUserName** | ProxyUserName="Contoso\ProxyUser" | No | If your proxy service requires authentication, define a user name in the DOMAIN\user format. |
| **ProxyUserPassword** | ProxyUserPassword="P@ssw0rd" | No | Specifies the password for your proxy user name. Credentials are encrypted and stored locally by the Defender for Identity sensor. |

[!TIP] If you’ve configured a proxy during installation, changing the proxy configuration requires you to remove and install the sensor. Therefore, we recommend creating and using a custom DNS A record for the proxy server, which you can use to change the proxy server’s address when needed.

We also recommend using the *hosts* file for testing.

### Configure a proxy server using WinINet

When configuring the proxy using WinINet, keep in mind that the embedded Defender for Identity sensor service runs in system context using the **LocalService** account, and that the Defender for Identity Sensor updater service runs in the system context using **LocalSystem** account.

* If you use WinHTTP for proxy configuration, you still need to configure Windows Internet (WinINet) browser proxy settings for communication between the sensor and the Defender for Identity cloud service.
* If you’re using Transparent proxy or WPAD in your network topology, you don’t need to configure WinINet for your proxy.

### Configure a proxy server using the registry

This section describes how to configure a static proxy server manually using a registry-based static proxy.

[!IMPORTANT] Configuring a proxy via the registry affects all applications that use WinINet with the **LocalService** and **LocalSystem** accounts, including Windows services.

Apply registry changes only to the **LocalService** and **LocalSystem** accounts.

To configure your proxy, copy your proxy configuration in user context to the **LocalSystem** and **LocalService** accounts as follows:

1. Back up your registry keys.
2. In the registry, search for the DefaultConnectionSettings value as REG\_BINARY, under the HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings registry key, and copy it.
3. If the LocalSystem doesn’t have the correct proxy settings, copy the proxy setting from the Current\_User to the LocalSystem, under the HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings registry key.

* Make sure to paste the value from the Current\_User’s DefaultConnectionSettings registry key as REG\_BINARY.
* This may happen if your proxy settings aren’t configured, or if they’re different from the Current\_User.

1. If the LocalService doesn’t have the correct proxy settings, then copy the proxy setting from the Current\_User to the LocalService, under the HKU\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings registry key.

* Make sure to paste the value from the Current\_User’s DefaultConnectionSettings registry key as REG\_BINARY.

### Enable access to Defender for Identity service URLs in the proxy server

To ensure maximal security and data privacy, Defender for Identity uses certificate-based, mutual authentication between each Defender for Identity sensor and the Defender for Identity cloud back-end. SSL inspection and interception are not supported, as they interfere in the authentication process.

To enable access to Defender for Identity, make sure to allow traffic to the following URLs:

| URL | Description | Example |
| --- | --- | --- |
| <your-instance-name>.atp.azure.com | Console connectivity | contoso-corp.atp.azure.com |
| <your-instance-name>sensorapi.atp.azure.com | Sensor connectivity | contoso-corpsensorapi.atp.azure.com |

The URL syntaxes listed in the table above automatically map to the correct service location for your Defender for Identity instance.

[!TIP] Occasionally, the Defender for Identity service IP addresses may change.

If you manually configure IP addresses, or if your proxy automatically resolves DNS names to their IP address and uses them, we recommend that you periodically check that the configured IP addresses are still up-to-date.

#### Enable access with a service tag

Alternately, use the IP address ranges in our **AzureAdvancedThreatProtection** Azure service tag to enable access to Defender for Identity. For more information, see [Virtual network service tags](/azure/virtual-network/service-tags-overview).

To download the *Azure IP Ranges and Service Tags - Public Cloud* file, select <https://www.microsoft.com/download/details.aspx?id=56519>.

For US Government offerings, see [Get started with US Government offerings](../us-govt-gcc-high.md).

### Test proxy connectivity

The Defender for Identity sensor requires network connectivity to the Defender for Identity service running in Azure. Most organizations control access to the internet via firewall or proxies. When using a proxy, you can allow access port 443 via a single URL. For more information, see [Required ports](prerequisites.md#required-ports)

After the proxy has been configured to allow the sensor access to the Defender for Identity service, do the following steps to confirm that everything is working as expected. Perform this procedure either before you deploy the sensor, or if the sensor experiences connectivity issues after being installed.

1. Open a browser using the same proxy settings being used by the sensor.

* [!NOTE] If the proxy settings are defined for **Local System**, you’ll need to use PSExec to open a session as **Local System** and open the browser from that session.

1. Go to: https://<your\_workspace\_name>sensorapi.atp.azure.com, where <your\_workspace\_name> is the name of your Defender for Identity workspace.

* [!IMPORTANT] You *must* specify HTTPS, not HTTP, to properly test connectivity.

You should get an *Error 503 The service is unavailable* message, which indicates you were successfully able to route to the Defender for Identity HTTPS endpoint. This is the desired result.

If you don’t get an *Error 503 The service is unavailable* message, you may have a problem with your proxy configuration. Check your network and proxy settings.

If you get a certificate error, ensure that you have the required trusted root certificates installed before continuing. For more information, see [Proxy authentication problem presents as a connection error](../troubleshooting-known-issues.md#proxy-authentication-problem-presents-as-a-connection-error).

Certificate details should look similar to the following: **DigiCert Global Root G2** > **Microsoft Azure TLS Issuing CA 01** > \***.atp.azure.com**.

### Next steps

[!div class=“step-by-step”] [« Download the Defender for Identity sensor](download-sensor.md) [Install the Defender for Identity sensor »](install-sensor.md)

## Install the Microsoft Defender for Identity sensor

Learn how to install the Microsoft Defender for Identity sensor on domain controllers.

[!NOTE] When installing the sensor on Windows Server Core, or to deploy the sensor via a software deployment system, follow the steps for [silent installation](#Xc26f3ebdeb6454a7339fec0ca727bf0942535f9) instead.

### Prerequisites

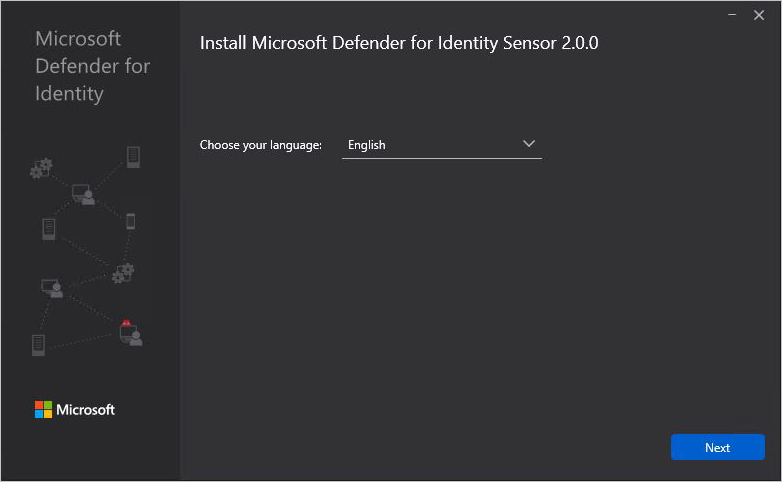
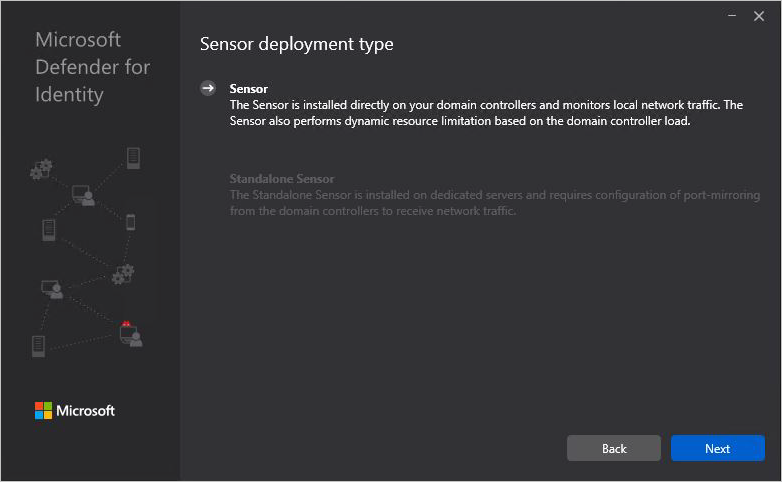
Before you start, make sure that you have:

* A downloaded copy of your [Defender for Identity sensor setup package](download-sensor.md) and the access key.
* Microsoft .NET Framework 4.7 or later is installed on the machine. If Microsoft .NET Framework 4.7 or later isn’t installed, the Defender for Identity sensor setup package installs it, which may require a reboot of the server.
* Relevant server specifications and network requirements, if you’re installing the sensor on an Active Directory Federation Service (AD FS) server. For more information, see [Microsoft Defender for Identity on Active Directory Federation Services (AD FS)](active-directory-federation-services.md).

### Install the sensor

Perform the following steps on the domain controller or AD FS server.

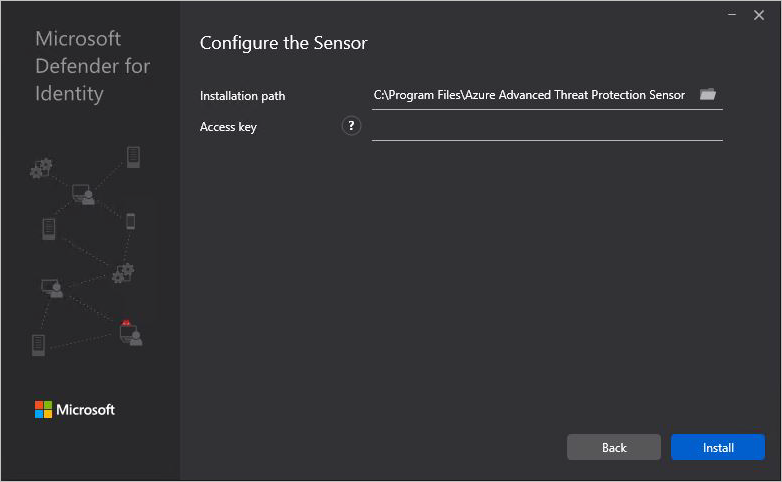
1. Verify the machine has connectivity to the relevant [Defender for Identity cloud service endpoint(s)](configure-proxy.md#enable-access-to-defender-for-identity-service-urls-in-the-proxy-server).
2. Extract the installation files from the zip file. Installing directly from the zip file will fail.
3. Run **Azure ATP sensor setup.exe** with elevated privileges (**Run as administrator**) and follow the setup wizard.
4. On the **Welcome** page, select your language and select **Next**. For example:

* 
* Screenshot of the Defender for Identity standalone sensor installation language selection.
* The installation wizard automatically checks if the server is a domain controller/ AD FS server or a dedicated server.
  + If it’s a domain controller / AD FS server, the Defender for Identity sensor is installed.
  + If it’s a dedicated server, the Defender for Identity standalone sensor is installed.
* For example, for a Defender for Identity sensor, the following screen is displayed to let you know that a Defender for Identity sensor is installed on your dedicated server:
* 
* Screenshot of the Defender for Identity sensor installation.

1. Select **Next**.

* A warning is issued if the domain controller / AD FS server or dedicated server does not meet the minimum hardware requirements for the installation. The warning doesn’t prevent you from selecting **Next**, and proceeding with the installation. It can still be the right option for the installation of Defender for Identity in a small lab test environment where less room for data storage is required.
* For production environments, we highly recommend working with Defender for Identity’s [capacity planning](capacity-planning.md) guide to make sure your domain controllers or dedicated servers meet the necessary requirements.

1. Under **Configure the sensor**, enter the installation path and the setup package access key. For example:

* 
* Screenshot of the Defender for Identity sensor configuration screen.
* Enter the following details:
  + **Installation path**: The location where the Defender for Identity sensor is installed. By default the path is %programfiles%\Azure Advanced Threat Protection sensor. Leave the default value.
  + **Access key**: Retrieved from the Microsoft 365 Defender portal in a [previous step](download-sensor.md).

1. Select **Install**. The following components are installed and configured during the installation of the Defender for Identity sensor:
   * **KB 3047154** (for Windows Server 2012 R2 only)
   * [!IMPORTANT]
     + Don’t install KB 3047154 on a virtualization host, which is the host that is running the virtualization. This may cause port mirroring to stop working properly. It’s fine to run KB 3047154 on a virtual machine.
     + If Wireshark is installed on the Defender for Identity sensor machine, you’ll need to restart the Defender for Identity sensor after running Wireshark because they use the same drivers.
   * **Defender for Identity sensor service** and **Defender for Identity sensor updater service** -\*\* Microsoft Visual C++ 2013 Redistributable\*\*

#### Viewing sensor versions

Beginning with version 2.176, when installing the sensor from a new package, the sensor’s version under **Add/Remove Programs** will appear with the full version number, such as **2.176.x.y**, instead of the static **2.0.0.0** that was previously shown.

The installed version continues to show even after automatic updates are run from the Defender for Identity cloud services.

View the sensor’s real version in the Microsoft 365 Defender [sensor settings page](https://security.microsoft.com/settings/identities?tabid=sensor), in the executable path or in the file version.

### Defender for Identity sensor silent installation

The Defender for Identity silent installation is configured to automatically restart the server at the end of the installation if necessary.

Make sure to schedule a silent installation only during a maintenance window. Because of a Windows Installer bug, the *norestart* flag cannot be reliably used to make sure the server does not restart.

To track your deployment progress, monitor the Defender for Identity installer logs, which are located in %AppData%\Local\Temp.

#### Silent installation via a deployment system

When silently deploying the Defender for Identity sensor via System Center Configuration Manager or other software deployment system, we recommend creating two deployment packages:

* Net Framework 4.7 or later, which may include rebooting the domain controller
* The Defender for Identity sensor

Make the Defender for Identity sensor package dependent on the deployment of the .Net Framework package deployment. If needed, get the [.Net Framework 4.7 offline deployment package](https://support.microsoft.com/topic/the-net-framework-4-7-offline-installer-for-windows-f32bcb33-5f94-57ce-6120-62c9526a91f2).

#### Run a silent installation

Use the following commands to perform a fully silent install of the Defender for Identity sensor, using the access key copied in a [previous step](download-sensor.md).

**cmd.exe syntax**:

"Azure ATP sensor Setup.exe" /quiet NetFrameworkCommandLineArguments="/q" AccessKey="<Access Key>"

**Powershell syntax**:

.\"Azure ATP sensor Setup.exe" /quiet NetFrameworkCommandLineArguments="/q" AccessKey="<Access Key>"

[!NOTE] When using the Powershell syntax, omitting the .\ preface results in an error that prevents silent installation.

**Installation options**:

| Name | Syntax | Mandatory for silent installation? | Description |
| --- | --- | --- | --- |
| Quiet | /quiet | Yes | Runs the installer displaying no UI and no prompts. |
| Help | /help | No | Provides help and quick reference. Displays the correct use of the setup command including a list of all options and behaviors. |
| NetFrameworkCommandLineArguments="/q" | NetFrameworkCommandLineArguments="/q" | Yes | Specifies the parameters for the .Net Framework installation. Must be set to enforce the silent installation of .Net Framework. |

**Installation parameters**:

| Name | Syntax | Mandatory for silent installation? | Description |
| --- | --- | --- | --- |
| InstallationPath | InstallationPath="" | No | Sets the path for the installation of Defender for Identity Sensor binaries. Default path: %programfiles%\Azure Advanced Threat Protection Sensor |
| AccessKey | AccessKey="\\*\\*" | Yes | Sets the access key that is used to register the Defender for Identity sensor with the Defender for Identity instance. |
| AccessKeyFile | AccessKeyFile="" | No | Sets the workspace Access Key from the provided text file path. |
| DelayedUpdate | DelayedUpdate=true | No | Sets the sensor’s update mechanism to delay the update for 72 hours from the official release of each service update. For more information, see [Delayed sensor update](../sensor-settings.md#delayed-sensor-update). |
| LogsPath | LogsPath="" | No | Sets the path for the Defender for Identity Sensor logs. Default path: %programfiles%\Azure Advanced Threat Protection Sensor |

**Examples**:

Use the following commands to silently install the Defender for Identity sensor:

"Azure ATP sensor Setup.exe" /quiet NetFrameworkCommandLineArguments="/q" AccessKey="mmAOkLYCzfH8L/zUIsH24BIJBevlAWu7wUcSfIkRJufpuEojaDHYdjrNs0P3zpD+/bObKfLS0puD7biT5KDf3g=="

"Azure ATP sensor Setup.exe" /quiet NetFrameworkCommandLineArguments="/q" AccessKeyFile="C:\Path\myAccessKeyFile.txt"

### Installing on AD FS servers

If you installed the sensor on AD FS servers, follow the steps in [Post-installation steps for AD FS servers](active-directory-federation-services.md#post-installation-steps-for-ad-fs-servers) to complete the setup.

These steps are required, or the sensor services will not start.

### Next steps

[!div class=“step-by-step”] [« Proxy configuration](configure-proxy.md) [Manage action accounts »](manage-action-accounts.md)

## Microsoft Defender for Identity action accounts

Defender for Identity allows you to take [remediation actions](../remediation-actions.md) targeting on-premises Active Directory accounts in the event that an identity is compromised. To take these actions, Microsoft Defender for Identity needs to have the required permissions to do so.

By default, the Microsoft Defender for Identity sensor installed on a domain controller will impersonate the LocalSystem account of the domain controller and perform the actions. However, you can change this default behavior by setting up a gMSA account and scope the permissions as you need. For example:

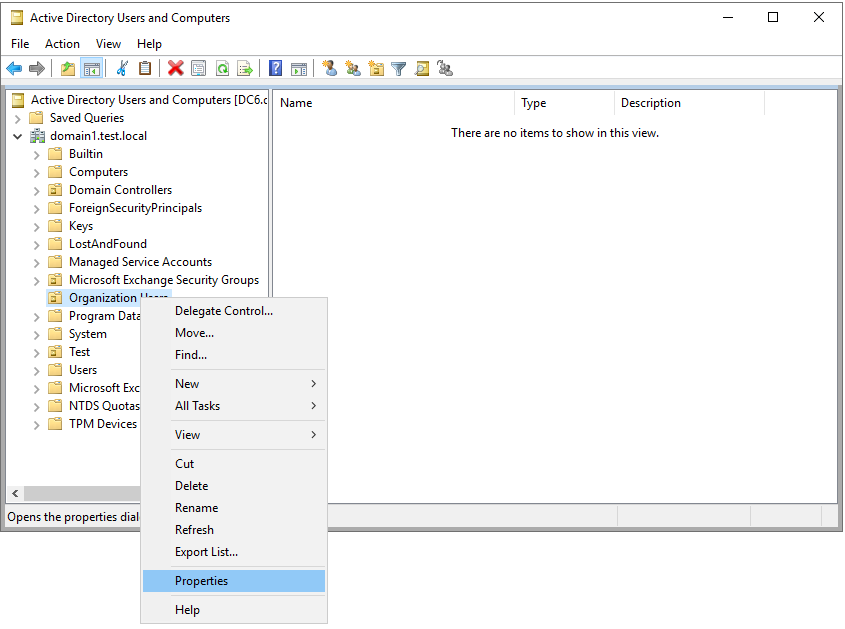
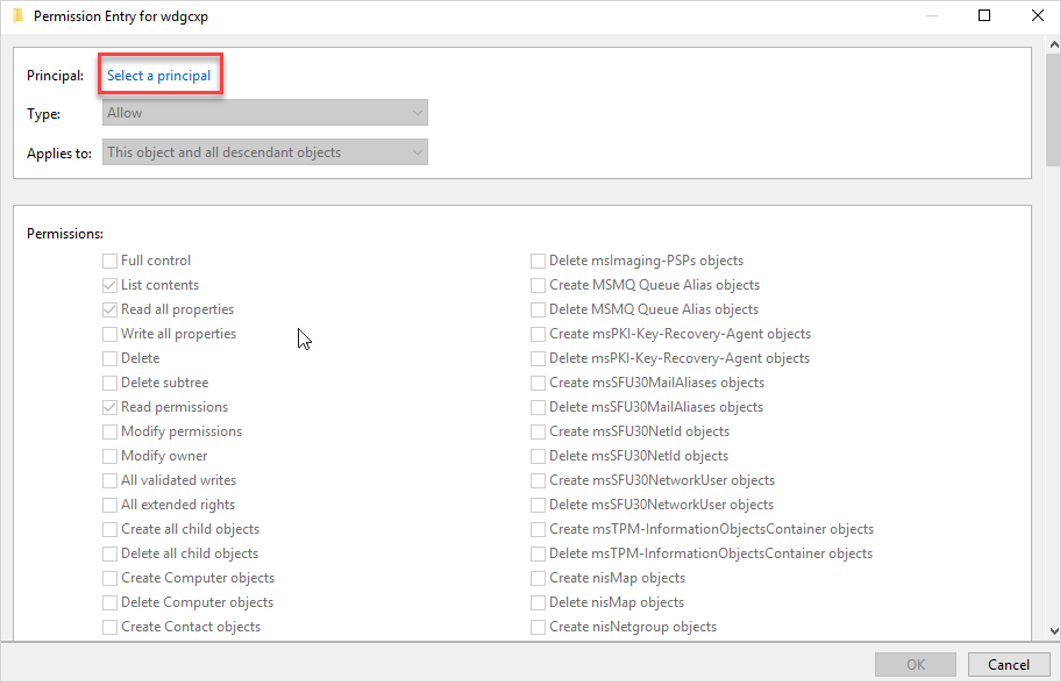
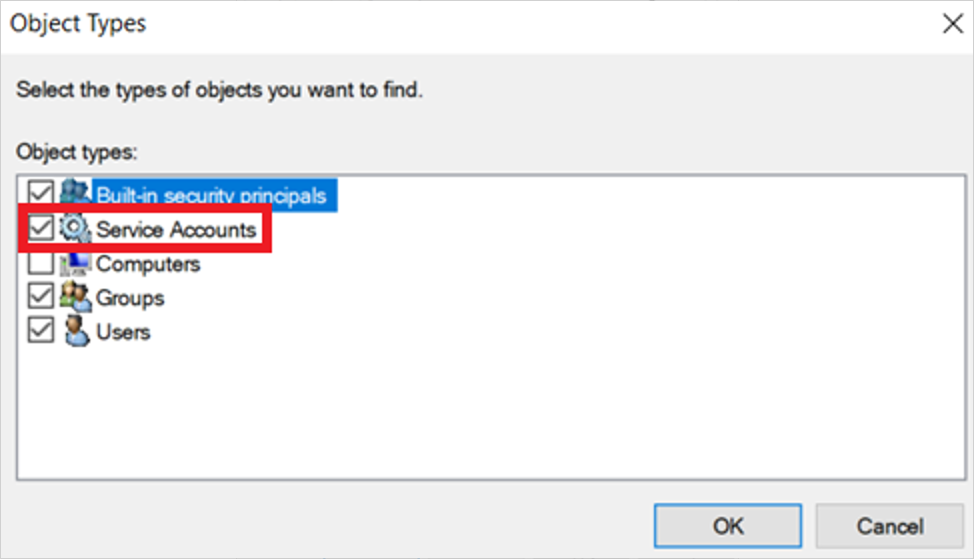
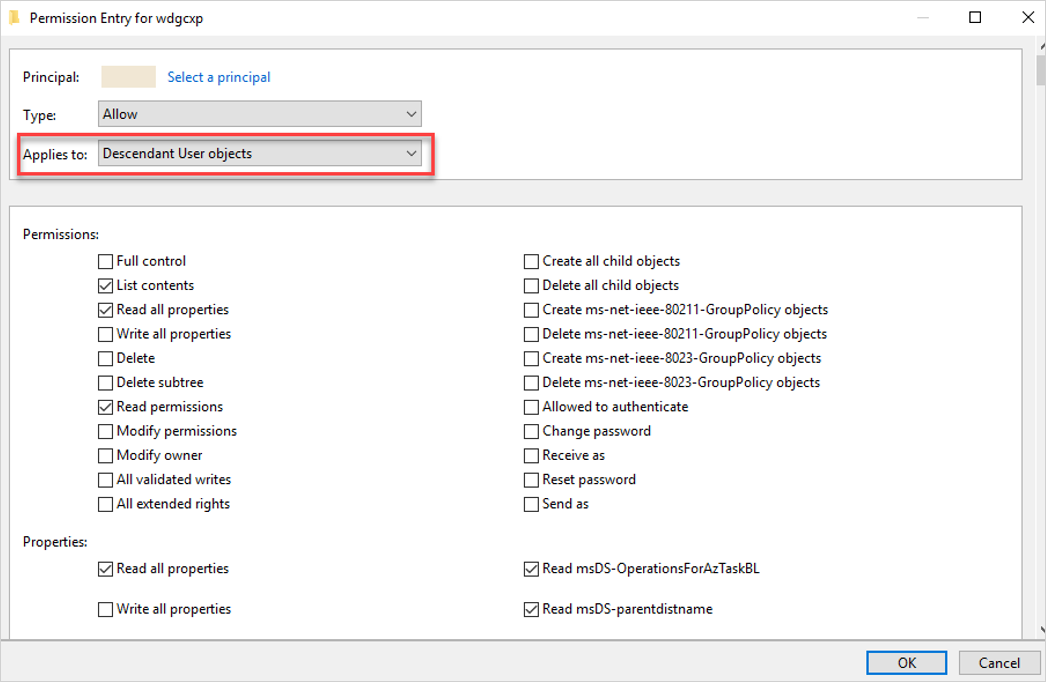
:::image type=“content” source=“../media/management-accounts.png” alt-text=“Screenshot of the Manage action accounts tab.”:::

### Best practices for action accounts

We recommend that you avoid using the same gMSA account you configured for Defender for Identity managed actions on servers other than domain controllers. If you use the same account and the server is compromised, an attacker could retrieve the password for the account and gain the ability to change passwords and disable accounts.

We also recommend that you avoid using the same account as both the Directory Service account and the Manage Action account. This is because the Directory Service account requires only read-only permissions to Active Directory, and the Manage Action accounts needs write permissions on user accounts.

### Create and configure a specific action account

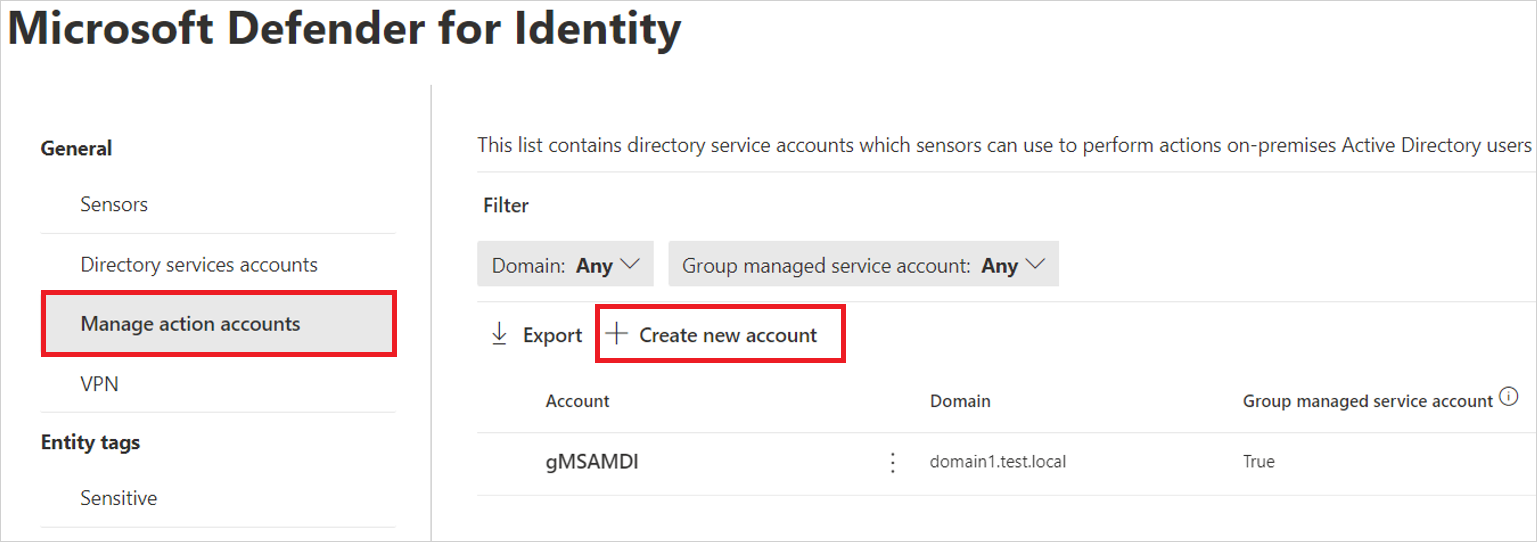
1. Create a new gMSA account. For more information, see [Getting started with Group Managed Service Accounts](/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts).
2. Assign the **Log on as a service** right to the gMSA account on each domain controller running the Defender for Identity sensor.
3. Grant the required permissions to the gMSA account as follows:
   1. Open **Active Directory Users and Computers**.
   2. Right-click the relevant domain or OU and select **Properties**. For example:
   * 
   * Screenshot of selecting domain or OU properties.
   1. Go the **Security** tab and select **Advanced**. For example:
   * 
   * Screenshot of the advanced security settings.
   1. Select **Add** > **Select a principal**. For example:
   * 
   * Screenshot of selecting a principal.
   1. Make sure **Service accounts** is marked in **Object types**. For example:
   * 
   * Screenshot oof selecting service accounts as object types.
   1. In the **Enter the object name to select** box, enter the name of the gMSA account and select **OK**.
   2. In the **Applies to** field, select **Descendant User objects**, leave the existing settings, and add the permissions and properties shown in the following example:
   * 
   * Screenshot of setting permissions and properties.
   * Required permissions include:

| Action | Permissions | Properties |
| --- | --- | --- |
| **Enable force password reset** | Reset password | - Read pwdLastSet - Write pwdLastSet |
| **To disable user** | - | - Read userAccountControl - Write userAccountControl |

* 1. In the **Applies to** field, select **Descendant Group objects** and set the following properties:
     + Read members
     + Write members
  2. Select **OK**.

### Add the gMSA account in the Microsoft 365 Defender portal

1. Go to the [Microsoft 365 Defender portal](https://security.microsoft.com) and select **Settings** -> **Identities** > **Microsoft Defender for Identity** > **Manage action accounts** > **+Create new account**. For exmaple:

* 
* Screenshot of the Create new account button.

1. Enter the account name and domain and select **Save**.

Your action account is listed on the **Manage action accounts** page.

### Related videos

[Remediation actions in Defender for Identity](https://www.microsoft.com/videoplayer/embed/RE4U7Pe)

### Next steps

[!div class=“step-by-step”] [« Install the Defender for Identity sensor](install-sensor.md) [Configure the Defender for Identity sensor »](configure-sensor-settings.md)

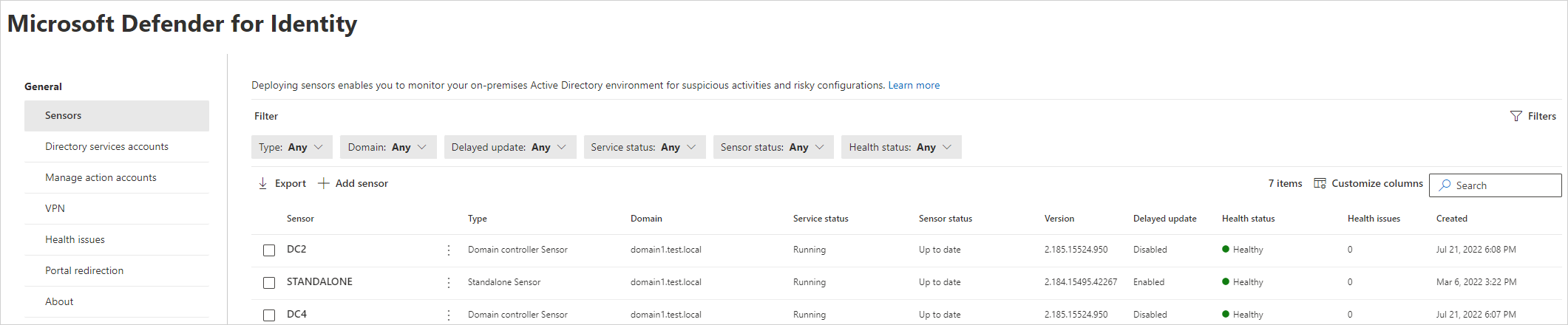
## Configure Microsoft Defender for Identity sensor settings

In this article, you’ll learn how to correctly configure Microsoft Defender for Identity sensor settings to start seeing data. You’ll need to do additional configuration and integration to take advantage of Defender for Identity’s full capabilities.

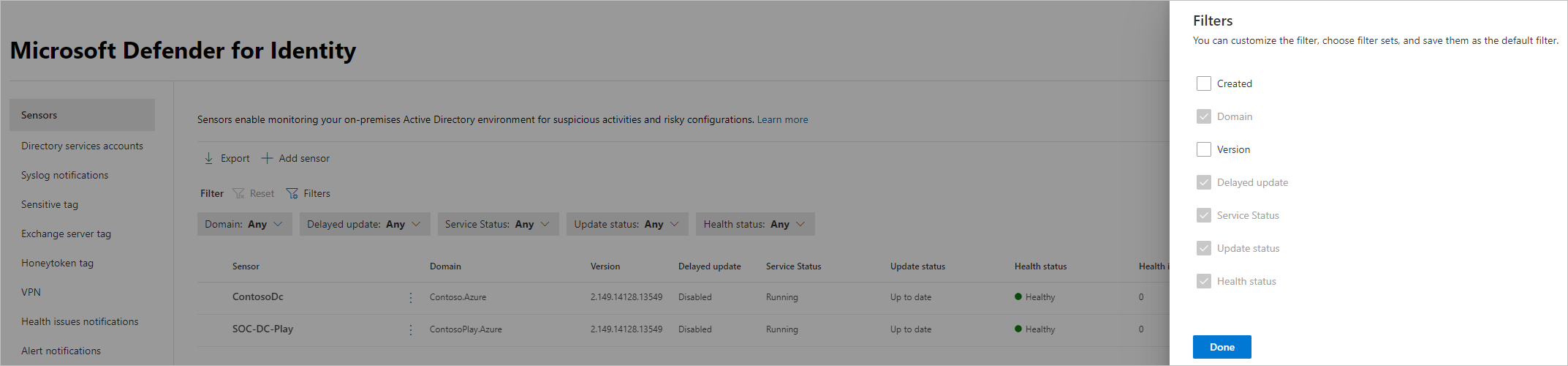
### View and configure sensor settings

After the Defender for Identity sensor is installed, do the following to view and configure Defender for Identity sensor settings:

1. In [Microsoft 365 Defender](https://security.microsoft.com), go to **Settings** > **Identities** **Sensors**. For example:

* [](../media/sensor-page.png#lightbox)
* The **Sensors** page displays all of your Defender for Identity sensors, listing the following details per sensor:
  + Sensor name
  + Sensor domain membership
  + Sensor version number
  + Whether updates should be [delayed](../sensor-settings.md#delayed-sensor-update).
  + Sensor service status
  + Sensor status
  + Sensor health status
  + The number of health issues
  + When the sensor was created.
* For more information, see [Sensor details](../sensor-settings.md#sensor-details).

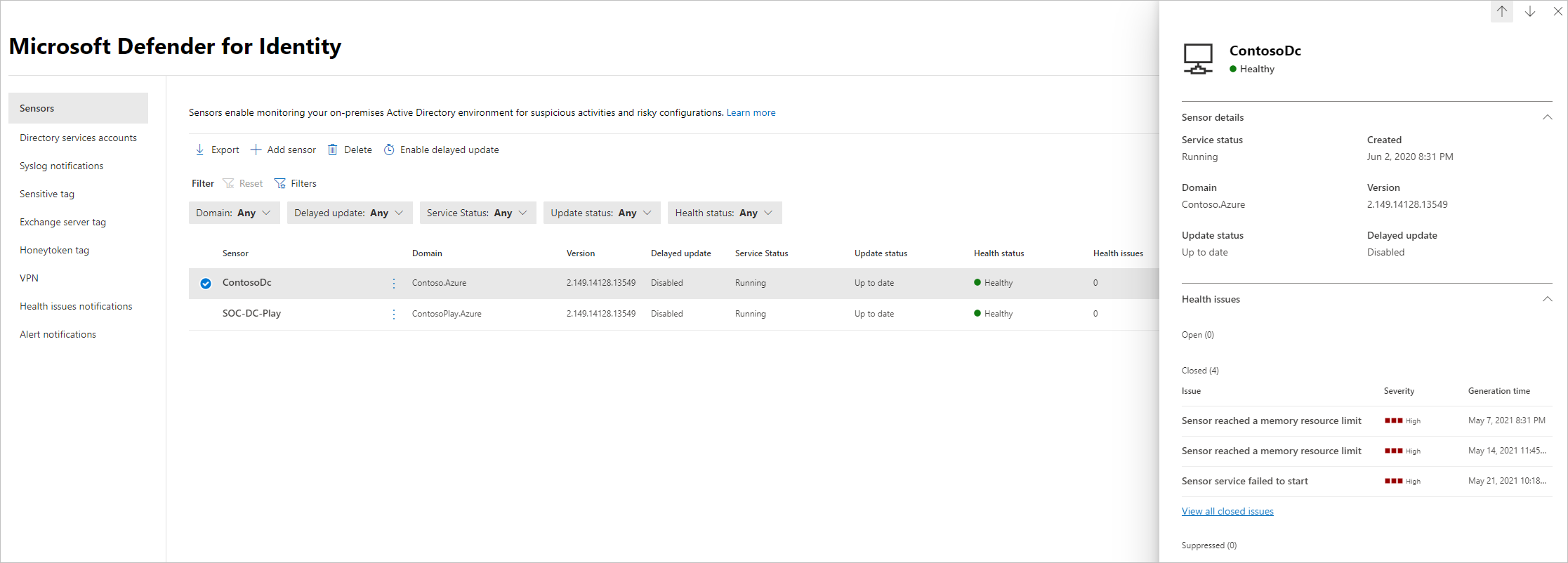
1. Select **Filters** to select the filters you want visible. For example:

* [](../media/sensor-filters.png#lightbox)

1. Use the dispalyed filters to determine which sensors to display. For example:

* :::image type=“content” source=“../media/filtered-sensor.png” alt-text=“Screenshot of a filtered list of sensors.” lightbox=“../media/filtered-sensor.png”:::

1. Select a sensor to show a details pane with more information about the sensor and its health status. For example:

* [](../media/sensor-details.png#lightbox)

1. Select **Manage sensor** to show a pane where you can configure sensor details. For example:

* :::image type=“content” source=“../media/manage-sensor.png” alt-text=“Screenshot of the Manage sensor option.” lightbox=“../media/manage-sensor.png”:::

1. Configure the following sensor details:
   * **Description** (optional): Enter a description for the Defender for Identity sensor.
   * **Domain Controllers (FQDN)**: This is required for the Defender for Identity standalone and AD FS sensors, and cannot be modified for the Defender for Identity sensor.
   * Enter the complete FQDN of your domain controller and select the plus sign to add it to the list. For example, **DC1.domain1.test.local**.
   * For any servers you define in the **Domain Controllers** list:
     + All domain controllers whose traffic is being monitored via port mirroring by the Defender for Identity standalone sensor must be listed in the **Domain Controllers** list. If a domain controller isn’t listed in the **Domain Controllers** list, detection of suspicious activities might not function as expected.
     + At least one domain controller in the list should be a global catalog. This enables Defender for Identity to resolve computer and user objects in other domains in the forest.
   * **Capture Network adapters** (required):
     + For Defender for Identity sensors, all network adapters that are used for communication with other computers in your organization.
     + For Defender for Identity standalone sensor on a dedicated server, select the network adapters that are configured as the destination mirror port. These network adapters receive the mirrored domain controller traffic.
2. On the **Sensors** page, select **Export** to export a list of your sensors to a **.csv** file. For example:

* :::image type=“content” source=“../media/export-sensors.png” alt-text=“Screenshot of exporting a list of sensors.” lightbox=“../media/export-sensors.png”:::

### Validate installations

#### Verify latest available sensor version

The Defender for Identity version is updated frequently. Check for the latest version in the Microsoft 365 Defender **Settings** > **Identities** > **About** page.

#### Validate successful deployment

To validate that the Defender for Identity sensor has been successfully deployed:

1. Check that the **Azure Advanced Threat Protection sensor** service is running on your sensor machine. After you save the Defender for Identity sensor settings, it might take a few seconds for the service to start.
2. If the service doesn’t start, review the **Microsoft.Tri.sensor-Errors.log** file, located by default at %programfiles%\Azure Advanced Threat Protection sensor\<sensor version>\Logs, where <sensor version> is the version you deployed.

#### Validate connectivity

Verify Defender for Identity connectivity on any domain device using the following steps.

When using the examples in the following steps, make sure to replace contosodc.contoso.azure and contoso.azure with the FQDN of your Defender for Identity sensor and domain name respectively.

1. Open a command prompt and enter nslookup
2. Enter server and the FQDN or IP address of the domain controller where the Defender for Identity sensor is installed. For example: server contosodc.contoso.azure
3. Enter ls -d contoso.azure
4. Repeat the previous two steps for each sensor you want to test.
5. From the Defender for Identity console, open the entity profile for the computer you ran the connectivity test from.
6. In Microsoft 365 Defender, search for the name of the user you used to run the commands in the previous steps. Select the name in the results, and view the user details page and all related activities and alerts.

If the domain controller that you’re testing is the first sensor you’ve deployed, wait at least 15 minutes before verifying any logical activity for that domain controller, allowing the database backend to complete the initial microservice deployments.

#### Validate successful deployment on an AD FS server

To validate that the Defender for Identity sensor has been successfully deployed on an AD FS server:

1. Check that the **Azure Advanced Threat Protection sensor** service is running. After you save the Defender for Identity sensor settings, it might take a few seconds for the service to start.
2. If the service doesn’t start, review the Microsoft.Tri.sensor-Errors.log file, located by default at: %programfiles%\Azure Advanced Threat Protection sensor\Version X\Logs
3. Use AD FS to authenticate a user to any application, and then verify that the AD FS authentication was observed by Defender for Identity:

* From Microsoft 365 Defender, select **Hunting** > **Advanced Hunting**. In the **Query** pane, enter and run the following query:
* IdentityLogonEvents | where Protocol contains 'Adfs'
* The results pane should include a list of events with a **LogonType** of **Logon with ADFS authentication**. Select a specific row to see additional details in the **Inspect Record** left pane. For example:
* :::image type=“content” source=“../media/adfs-logon-advanced-hunting.png” alt-text=“Screenshot of the results of an AD FS logon advanced hunting query.” lightbox=“../media/adfs-logon-advanced-hunting.png”:::

### Related videos

* [Microsoft Defender for Identity settings](https://www.microsoft.com/videoplayer/embed/RWFVEX)

### Next steps

Now that you’ve configured the initial configuration steps, you can configure more settings. Go to any of the pages below for more information:

* [Updating your sensors](../sensor-settings.md#updating-your-sensors)
* [Set entity tags: sensitive, honeytoken, and Exchange server](../entity-tags.md)
* [Configure detection exclusions](../exclusions.md)
* [Configure notifications: health issues, alerts, and Syslog](../notifications.md)

# Zero Trust with Defender for Identity

[Zero Trust](/security/zero-trust/zero-trust-overview) is a security strategy for designing and implementing the following sets of security principles:

| Verify explicitly | Use least privilege access | Assume breach |
| --- | --- | --- |
| Always authenticate and authorize based on all available data points. | Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection. | Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses. |

Defender for Identity is a primary component of a Zero Trust strategy and your XDR deployment with Microsoft 365 Defender. Defender for Identity uses Active Directory signals to detect sudden account changes like privilege escalation or high-risk lateral movement, and reports on easily exploited identity issues like unconstrained Kerberos delegation, for correction by the security team.

## Monitoring for Zero Trust

When monitoring for Zero Trust, make sure review and mitigate open alerts from Defender for Identity together with your other security operations. You may also want to use [advanced hunting queries in Microsoft 365 Defender](/microsoft-365/security/defender/advanced-hunting-overview) to look for threats across identities, devices, and cloud apps.

For example, you can use advanced hunting to discover an attacker’s [lateral movement paths](../understand-lateral-movement-paths.md), and then see if the same identity has been involved in other detections.

[!TIP] Ingest your alerts into [Microsoft Sentinel with Microsoft 365 Defender](/azure/sentinel/microsoft-365-defender-sentinel-integration), a cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution to provide your Security Operations Center (SOC) with a single pane of glass for monitoring security events across your enterprise.

## Next steps

Learn more about Zero Trust and how to build an enterprise-scale strategy and architecture with the [Zero Trust Guidance Center](/security/zero-trust).

For more information, see:

* [Securing identity with Zero Trust](/security/zero-trust/deploy/identity)
* [Deploy your identity infrastructure for Microsoft 365](/microsoft-365/enterprise/deploy-identity-solution-overview)
* [Zero Trust deployment plan with Microsoft 365](/microsoft-365/security/microsoft-365-zero-trust)
* [Zero Trust with Microsoft 365 Defender](/microsoft-365/security/defender/zero-trust-with-microsoft-365-defender)

# Microsoft Defender for Identity on Active Directory Federation Services (AD FS)

Defender for Identity protects the Active Directory Federation Services (AD FS) in your environment by detecting on-premises attacks against AD FS servers.

This article describes the additional prerequisites and post-installation steps required when installing Defender for Identity sensors on AD FS servers.

For more information, see:

* [Microsoft Defender for Identity prerequisites](prerequisites.md)
* [Install the Microsoft Defender for Identity sensor](install-sensor.md) For more information, see [Microsoft Defender for Identity prerequisites](prerequisites.md).

[!NOTE] If you use both Defender for Identity and Defender for Endpoint, you must install both sensors on domain controllers or AD FS servers to protect both the server and Active Directory.

## Server specifications

The Defender for Identity sensor supports the following AD FS servers:

| Operating system | Server with desktop experience | Server core | Nano server |
| --- | --- | --- | --- |
| Windows Server 2016 | ✔ | ✔ | ❌ |
| Windows Server 2019 | ✔ | ✔ | ❌ |
| Windows Server 2022 | ✔ | ✔ | ❌ |

[!NOTE] The Defender for Identity sensor is supported only on the federation servers. It is not required on the Web Application Proxy (WAP) servers.

For more information, see [Sensor requirements](prerequisites.md#sensor-requirements).

## Network requirements

For sensors running on AD FS servers to be able to communicate with the Defender for Identity cloud service, you must open port 443 on your firewalls and proxies to the following endpoint: <your-instance-name>sensorapi.atp.azure.com

For example: *contoso-corpsensorapi.atp.azure.com*

For more information see [Configure endpoint proxy and Internet connectivity settings for your Microsoft Defender for Identity sensor](configure-proxy.md).

## Verbose logging for AD FS Windows event logs

Sensors running on AD FS servers must have the auditing level set to **Verbose**, tracking the following events:

* 1202 - The Federation Service validated a new credential
* 1203 - The Federation Service failed to validate a new credential
* 4624 - An account was successfully logged on
* 4625 - An account failed to log on

Configure the auditing level to **Verbose** using the following command:

Set-AdfsProperties -AuditLevel Verbose

For more information, see [Event auditing information for AD FS](/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-logging#event-auditing-information-for-ad-fs-on-windows-server-2016).

## Read permissions for the AD FS database

For sensors running on AD FS servers to have access to the AD FS database, you need to grant read (*db\_datareader*) permissions for the relevant [Directory Services Account](directory-service-accounts.md) configured.

If you have more than one AD FS server, make sure to grant this permission across all of them since database permissions are not replicated across servers.

[!NOTE] If the AD FS database runs on a dedicated SQL server instead of the local AD FS server, and you’re using a group-managed service account (gMSA) as the [Directory Services Account (DSA)](directory-service-accounts.md), make sure that you grant the SQL server the [required permissions](directory-service-accounts.md#grant-permissions-to-retrieve-the-gmsa-accounts-password) to retrieve the gMSA’s password.

### Grant access to the AD FS database

Grant access to the database using SQL Server Management Studio, TSQL, or PowerShell.

For example, the commands listed below might be helpful if you’re using the Windows Internal Database (WID) or an external SQL server.

In these sample codes:

* **[DOMAIN1]** is the directory services user of the workspace
* **AdfsConfigurationV4** is an example of an AD FS database name, and may vary
* \*\*server=.##WID\* - is the connection string to the database if you are using WID

[!TIP] If you don’t know your connection string, follow the steps in the [Windows server documentation](/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-sql#to-acquire-the-sql-connection-string).

**To grant the sensor access to the AD FS database using TSQL**:

USE [master]  
CREATE LOGIN [DOMAIN1\triservice] FROM WINDOWS WITH DEFAULT\_DATABASE=[master]  
USE [AdfsConfigurationV4]  
CREATE USER [DOMAIN1\triservice] FOR LOGIN [DOMAIN1\triservice]  
ALTER ROLE [db\_datareader] ADD MEMBER [DOMAIN1\triservice]  
GRANT CONNECT TO [DOMAIN1\triservice]  
GRANT SELECT TO [DOMAIN1\triservice]  
GO

**To grant the sensor access to the AD FS database using PowerShell**:

$ConnectionString = 'server=\\.\pipe\MICROSOFT##WID\tsql\querydatabase=AdfsConfigurationV4;trusted\_connection=true;'  
$SQLConnection= New-Object System.Data.SQLClient.SQLConnection($ConnectionString)  
$SQLConnection.Open()  
$SQLCommand = $SQLConnection.CreateCommand()  
$SQLCommand.CommandText = @"  
USE [master];   
CREATE LOGIN [DOMAIN1\triservice] FROM WINDOWS WITH DEFAULT\_DATABASE=[master];  
USE [AdfsConfigurationV4];   
CREATE USER [DOMAIN1\triservice] FOR LOGIN [DOMAIN1\triservice];   
ALTER ROLE [db\_datareader] ADD MEMBER [DOMAIN1\triservice];   
GRANT CONNECT TO [DOMAIN1\triservice];   
GRANT SELECT TO [DOMAIN1\triservice];  
"@  
$SqlDataReader = $SQLCommand.ExecuteReader()  
$SQLConnection.Close()

## SQL server permissions

For sensor installations on AD FS servers, configure the SQL server to allow *Directory service* account with the following permissions to the **AdfsConfiguration** database:

* *connect*
* *log in*
* *read*
* *select*

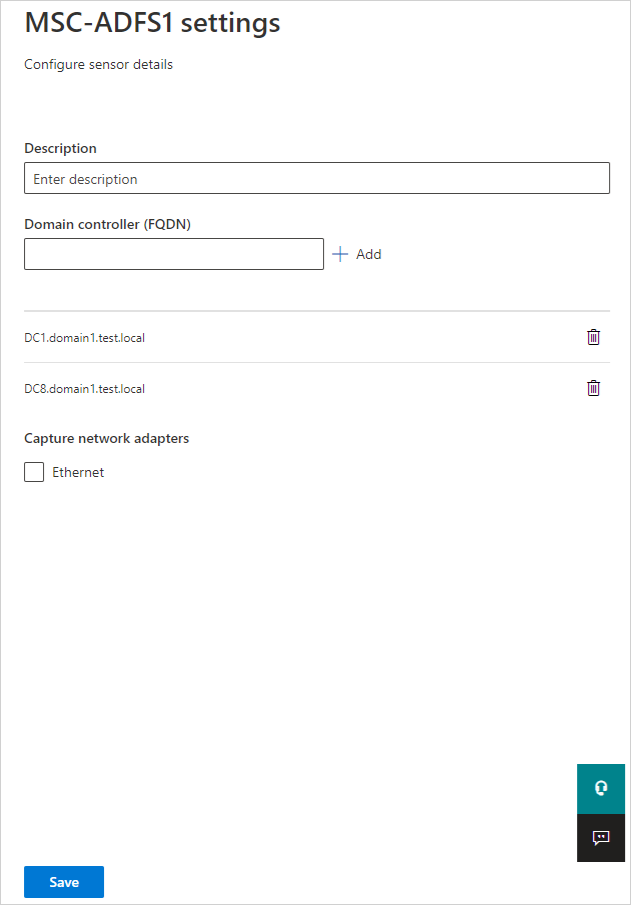
## Install the Microsoft Defender for Identity sensor on an AD FS server

For more information, see [Install the Defender for Identity sensor](install-sensor.md).

## Post-installation steps for AD FS servers

Installing the sensor on an AD FS server automatically selects the closest domain controller. Use the following steps to check or modify the selected domain controller.

1. In [Microsoft 365 Defender](https://security.microsoft.com), go to **Settings** > **Identities** > **Sensors** to view all of your Defender for Identity sensors.
2. Locate and select the sensor you installed on an AD FS server.
3. In the pane that opens, in the **Domain Controller (FQDN)** field, enter the FQDN of the resolver domain controllers. Select the plus icon **(+)**, and then select **Save**. For example:

* 
* Defender for Identity configure AD FS sensor resolver

Initializing the sensor may take a couple of minutes, at which time the AD FS sensor service status should change from **stopped** to **running**.

## Next steps

For more information, see:

* [Directory Service account recommendations](/defender-for-identity/directory-service-accounts)
* [Microsoft Defender for Identity Directory Service account recommendations](directory-service-accounts.md)

# Microsoft Defender for Identity multi-forest support

Microsoft Defender for Identity supports organizations with multiple Active Directory forests, giving you the ability to easily monitor activity and profile users across forests.

Enterprise organizations typically have several Active Directory forests - often used for different purposes, including legacy infrastructure from corporate mergers and acquisitions, geographical distribution, and security boundaries (red-forests).

Securing your multiple Active Directory forests with Defender for Identity provides the following advantages:

* View and investigate activities performed by users across multiple forests from a single location
* Gain improved detection and reduce false positives with advanced Active Directory integration and account resolution
* Gain greater control and easier deployment, with an improved set of health issues and reporting for cross-org coverage when your domain controllers are all monitored from a single Defender for Identity server

## Prerequisites

Defender for Identity requires the following to support multiple Active Directory forests:

* **A Directory Service account**: The Directory Service account you configure for each forest must:
  + Be trusted in all the other forests
  + Have at least read-only permission to perform LDAP queries on the domain controllers.
* If Defender for Identity standalone sensors are installed on standalone machines, rather than directly on the domain controllers, the machines must be allowed to communicate with all of remote forest domain controllers using LDAP.
* **Required ports**: In order for Defender for Identity to communicate with the Defender for Identity sensors, including standalone sensors, make sure the following ports are opened on any machine where a Defender for Identity sensor is installed:

| Protocol | Transport | Port | To/From | Direction |
| --- | --- | --- | --- | --- |
| **Internet ports** |  |  |  |  |
| SSL (\*.atp.azure.com) | TCP | 443 | Defender for Identity cloud service | Outbound |
| **Internal ports** |  |  |  |  |
| LDAP | TCP and UDP | 389 | Domain controllers | Outbound |
| Secure LDAP (LDAPS) | TCP | 636 | Domain controllers | Outbound |
| LDAP to Global Catalog | TCP | 3268 | Domain controllers | Outbound |
| LDAPS to Global Catalog | TCP | 3269 | Domain controllers | Outbound |

<!–> > [!NOTE] > Each Defender for Identity sensor can only report to a single Defender for Identity workspace.

## Detection activity across multiple forests

To detect cross-forest activities, Defender for Identity sensors query domain controllers in remote forests to create profiles for all entities involved, including users and computers from remote forests.

* Defender for Identity sensors can be installed on domain controllers in all forests, even forests with no trust.
* [Add additional credentials](directory-service-accounts.md#configure-a-directory-service-account-in-microsoft-365-defender) on the **Directory Service accounts** page to support any untrusted forests in your environment.
  + Only one credential is required to support all forests with a two-way trust.
  + Additional credentials are only required for each forest with non-Kerberos trust or no trust.
  + There’s a default limit of 30 untrusted forests per Defender for Identity instance. Contact support if your organization has more than 30 forests.

For more information, see [Microsoft Defender for Identity Directory Service account recommendations](directory-service-accounts.md).

## Multi-forest mapping process

When Defender for Identity maps your forests, it uses the following process:

1. After the Defender for Identity sensor starts running, the sensor queries the remote Active Directory forests and retrieves a list of users and machine data for profile creation.
2. Every 5 minutes, each Defender for Identity sensor queries one domain controller from each domain, from each forest, to map all the forests in the network.

* The Defender for Identity sensors map the forests using the trustedDomain Active Directory object, by signing in and checking the trust type.

You may see ad-hoc traffic when the Defender for Identity sensor detects cross forest activity. When this occurs, the Defender for Identity sensors will send an LDAP query to the relevant domain controllers to retrieve entity information.

[!NOTE] Interactive sign-ins performed by users in one forest to access resources in another forest aren’t displayed in the Defender for Identity dashboard.

## Next steps

* [Defender for Identity sizing tool](https://aka.ms/aatpsizingtool)
* [Defender for Identity architecture](../architecture.md)
* [Install Defender for Identity](/defender-for-identity/classic-install-step1)
* [Check out the Defender for Identity forum!](https://aka.ms/MDIcommunity)

# Advanced Threat Analytics (ATA) to Microsoft Defender for Identity

[!NOTE] The final release of ATA is [generally available](https://support.microsoft.com/help/4568997/update-3-for-microsoft-advanced-threat-analytics-1-9). ATA ended Mainstream Support on January 12, 2021. Extended Support will continue until January 2026. For more information, read [our blog](https://techcommunity.microsoft.com/t5/microsoft-security-and/end-of-mainstream-support-for-advanced-threat-analytics-january/ba-p/1539181).

This article describes how to migrate from an existing ATA installation to Microsoft Defender for Identity:

[!div class=“checklist”]

* Review and confirm Defender for Identity service prerequisites
* Document your existing ATA configuration
* Plan your migration
* Set up and configure your Defender for Identity service
* Perform post-migration checks and verifications
* Decommission ATA

[!NOTE] While you can migrate to Defender for Identity from any ATA version, your ATA data isn’t migrated. Therefore, we recommend that you plan to retain your ATA Data Center and any alerts required for ongoing investigations until all ATA alerts are closed or remediated.

[!IMPORTANT] This migration guide is designed for Defender for Identity sensors only, and not standalone sensors.

## Prerequisites

To migrate from ATA to Defender for Identity, you must have:

* An Azure Active Directory tenant with at least one global/security administrator, so that you can create a Defender for Identity instance. Each Defender for Identity instance supports a multiple Active Directory forest boundary and Forest Functional Level (FFL) of Windows 2003 and above.
* .Net Framework version 4.7 or later. You may also need to restart your domain controller if your current .Net Framework version is not 4.7 or later.
* An environment and domain controllers that meet Defender for Identity sensor requirements. For more information, see [Microsoft Defender for Identity prerequisites](prerequisites.md).
* Verification that all domain controllers you plan to use have sufficient internet access to the Defender for Identity service. For more information, see [Defender for Identity proxy configuration requirements](configure-proxy.md).

## Plan your migration

Before starting the migration, gather all of the following information:

* Account details for your [Directory Services](directory-service-accounts.md) account.
* Syslog notification [settings](/defender-for-identity/notifications).
* Email [notification details](../notifications.md).
* All [ATA role group memberships](/advanced-threat-analytics/ata-role-groups)
* [VPN integration details](../vpn-integration.md)
* Alert exclusions. Exclusions are not transferable from ATA to Defender for Identity, so details of each exclusion are required to [replicate the exclusions in Defender for Identity](../exclusions.md).
* Account details for entity tags. If you don’t already have dedicated entity tags, create new ones for use with Defender for Identity. For more information, see [Defender for Identity identity tags in Microsoft 365 Defender](/microsoft-365/security/defender-identity/entity-tags).
* A complete list of all entities, such as computers, groups, or users, that you want to manually tag as Sensitive entities. For more information, see [Defender for Identity entity tags in Microsoft 365 Defender](../entity-tags.md).
* Report scheduling [details](/defender-for-identity/classic-reports), including a list of all reports and scheduled timing.

[!CAUTION] Do not uninstall the ATA Center until all ATA Gateways are removed. Uninstalling the ATA Center with ATA Gateways still running leaves your organization exposed with no threat protection.

## Move to Defender for Identity

Use the following steps to migrate to Defender for Identity:

1. [Create your new Defender for Identity instance](deploy-defender-identity.md#start-using-microsoft-365-defender).
2. Uninstall the ATA Lightweight Gateway on all domain controllers.
3. Install the Defender for Identity Sensor on all domain controllers:
   1. [Download the Defender for Identity sensor files](download-sensor.md) and retrieve the access key.
   2. [Install Defender for Identity sensors on your domain controllers](install-sensor.md).
4. [Configure the your Defender for Identity sensor](configure-sensor-settings.md).

After the migration is complete, allow two hours for the initial sync to be completed before moving on with validation tasks.

## Validate your migration

In Microsoft 365 Defender, check the following areas to validate your migration:

Review any [health issues](../health-alerts.md) for signs of service issues - Review Defender for Identity [sensor error logs](../troubleshooting-using-logs.md) for any unusual errors.

## Post-migration activities

After completing your migration to Defender for Identity, do the following to clean up your legacy ATA resources:

1. Make sure that you’ve recorded or remediated all existing ATA alerts. Existing ATA security alerts aren’t imported to Defender for Identity with the migration.
2. Do one or both of the following:
   * **Decommission the ATA Center**. We recommend keeping ATA data online for a period of time.
   * **Back up Mongo DB** if you want to keep the ATA data indefinitely. For more information, see [Backing up the ATA database](/advanced-threat-analytics/ata-database-management#backing-up-the-ata-database).

## Next steps

For more information, see:

* [What is Microsoft Defender for Identity?](../what-is.md)
* [Understanding security alerts](../understanding-security-alerts.md)
* [What’s new in Microsoft Defender for Identity](../whats-new.md)
* [Defender for Identity frequently asked questions](../technical-faq.yml).

Do you have more questions, or an interest in discussing Defender for Identity and related security with others? Join the [Defender for Identity Community](https://techcommunity.microsoft.com/t5/Azure-Advanced-Threat-Protection/bd-p/AzureAdvancedThreatProtection) today!

# Configure a standalone sensor

## Configure port mirroring

This article describes port mirroring options for Microsoft Defender for Identity, and is relevant only for standalone sensors. Defender for Identity mainly uses deep packet inspection over network traffic to and from your domain controllers. For Defender for Identity standalone sensors to see network traffic, you must either configure port mirroring, or use a Network TAP. Port mirroring copies the traffic from one port (the source port) to another port (the destination port).

When using port mirroring, configure port mirroring for each domain controller that you’re monitoring as the source of your network traffic. We recommend working with your networking or virtualization team to configure port mirroring.

[!IMPORTANT] Defender for Identity standalone sensors do not support the collection of Event Tracing for Windows (ETW) log entries that provide the data for multiple detections. For full coverage of your environment, we recommend deploying the Defender for Identity sensor.

### Choose a port mirroring method

Your domain controllers and Defender for Identity standalone sensor can be either physical or virtual. The following are common methods for port mirroring and some considerations. For more information, see your switch or virtualization server product documentation. Your switch manufacturer might use different terminology.

* **Switched Port Analyzer (SPAN)** – Copies network traffic from one or more switch ports to another switch port on the same switch. Both the Defender for Identity standalone sensor and domain controllers must be connected to the same physical switch.
* **Remote Switch Port Analyzer (RSPAN)** – Allows you to monitor network traffic from source ports distributed over multiple physical switches. RSPAN copies the source traffic into a special RSPAN configured VLAN. This VLAN needs to be trunked to the other switches involved. RSPAN works at Layer 2.
* **Encapsulated Remote Switch Port Analyzer (ERSPAN)** – A Cisco proprietary technology working at Layer 3. ERSPAN allows you to monitor traffic across switches without the need for VLAN trunks and uses generic routing encapsulation (GRE) to copy monitored network traffic.
* Defender for Identity currently cannot directly receive ERSPAN traffic. Instead:
  1. Configure the ERSPAN destination where the traffic is decapsulated as a switch or router that can decapsulate the traffic.
  2. Configure the switch or router to forward the decapsulated traffic to the Defender for Identity standalone sensor using either SPAN or RSPAN.

[!NOTE] - If the domain controller being port mirrored is connected over a WAN link, make sure the WAN link can handle the additional load of the ERSPAN traffic.

* Defender for Identity only supports traffic monitoring when the traffic reaches the NIC and the domain controller in the same manner. Defender for Identity does not support traffic monitoring when the traffic is broken out to different ports.

### Supported port mirroring options

The following table describes Defender for Identity’s support for port mirroring configurations:

| Defender for Identity standalone sensor | Domain controller | Considerations |
| --- | --- | --- |
| Virtual | Virtual on same host | The virtual switch needs to support port mirroring.Moving one of the virtual machines to another host by itself may break the port mirroring. |
| Virtual | Virtual on different hosts | Make sure your virtual switch supports this scenario. |
| Virtual | Physical | Requires a dedicated network adapter otherwise Defender for Identity sees all of the traffic coming in and out of the host, even the traffic it sends to the Defender for Identity cloud service. |
| Physical | Virtual | Make sure your virtual switch supports this scenario - and port mirroring configuration on your physical switches based on the scenario:If the virtual host is on the same physical switch, you need to configure a switch level span.If the virtual host is on a different switch, you need to configure RSPAN or ERSPAN\*. |
| Physical | Physical on the same switch | Physical switch must support SPAN/Port Mirroring. |
| Physical | Physical on a different switch | Requires physical switches to support RSPAN or ERSPAN ERSPAN is only supported when decapsulation is performed before the traffic is analyzed by Defender for Identity. |

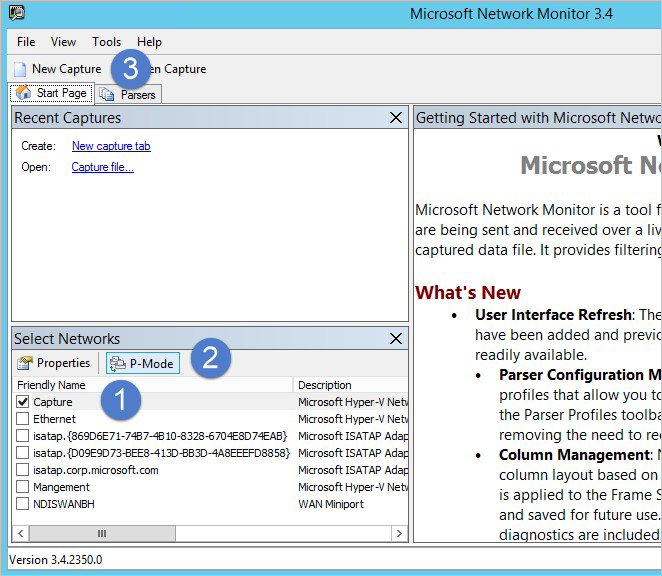
[!NOTE] - The time on your domain controllers and the connected Defender for Identity sensor must be synchronized to within 5 minutes of eachother.

### Validate port mirroring

After configuring port mirroring, validate that port mirroring is working before installing the Defender for Identity standalone sensor. The Defender for Identity standalone sensor must be able to see the traffic to and from the domain controller.

[!IMPORTANT] This procedure uses Microsoft Network Monitor to validate port mirroring. If you choose to validate with Wireshark, restart the Defender for Identity standalone sensor service after you finish validating.

**To validate port mirroring**:

1. Install [Microsoft Network Monitor 3.4](https://www.microsoft.com/download/details.aspx?id=4865) on the Defender for Identity standalone sensor that you want to validate.
2. Open Network Monitor and create a new capture tab.
   1. Select only the **Capture** network adapter or the network adapter that is connected to the switch port that is configured as the port mirroring destination.
   2. Ensure that P-Mode is enabled.
   3. Select **New Capture**. For example:
   * 
   * Screenshot of the Microsoft Network Monitor dialog highlighting the New Capture button.
3. In your new tab’s **Display Filter** area, enter the following filter: **KerberosV5 OR LDAP** and then select **Apply**.
4. Select **Start** to start the capture session. If you do not see traffic to and from the domain controller listed in the **Frame summary** area, review your port mirroring configuration.

* [!NOTE] It is important to make sure you see traffic to and from the domain controllers.

1. If you only see traffic in one direction, work with your networking or virtualization teams to help troubleshoot your port mirroring configuration.

### Working with virtualization clusters

If you are working with virtualization clusters:

* **Configure affinity between the domain controller and the Defender for Identity standalone sensor**. Configure affinity for each domain controller running on the virtualization cluster in a virtual machine with the Defender for Identity standalone sensor. When the domain controller moves to another host in the cluster, the Defender for Identity standalone sensor follows it. This works well when there are a few domain controllers.
* [!NOTE] This step is irrelevant if your environment supports Virtual to Virtual on different hosts (RSPAN).
* **Ensure proper sensor sizing**. Make sure that the Defender for Identity standalone sensor is properly sized to handle monitoring all of the DCs by themselves:
  1. Install a virtual machine on each virtualization host.
  2. Install a Defender for Identity standalone sensor on each host.
  3. Configure each Defender for Identity standalone sensor to monitor all of the domain controllers that run on the cluster.
* Any host the domain controllers run on is monitored.

### Next steps

* [Configure event forwarding](configure-event-forwarding.md)
* [Check out the Defender for Identity forum!](https://aka.ms/MDIcommunity)

## Configure event collection

### Windows event collection overview

We recommend that you enhance Microsoft Defender for Identity’s detection capabilities with extra Windows events that aren’t available via the domain controller network traffic.

While the Defender for Identity sensor is configured to automatically collect syslog events, if you’re working with a standalone Defender for Identity sensor, you’ll need to configure this manually. Using one of the following options:

* [Listen for SIEM events on your Defender for Identity standalone sensor](configure-event-collection.md)
* [Configure Windows event forwarding to your Defender for Identity standalone sensor](configure-event-forwarding.md)

When you’re finished, make sure to also configure audit policies as needed. For more information, see [Configure audit policies for Windows event logs](configure-windows-event-collection.md).

[!IMPORTANT] Defender for Identity standalone sensors do not support the collection of Event Tracing for Windows (ETW) log entries that provide the data for multiple detections. For full coverage of your environment, we recommend deploying the Defender for Identity sensor.

#### SIEM/syslog data support

Defender for Identity supports UDP traffic from your SIEM or syslog server. If you don’t use a SIEM or syslog server, configure your Windows domain controllers to forward all required events the the Defender for Identity sensor for analysis. For more information, see your SIEM or syslog server’s product documentation.

[!CAUTION] When forwarding syslog data to a standalone sensor, make sure not to forward *all* syslog data to your sensor.

#### NNR requirements

Network Name Resolution (NNR) is a main component of Defender for Identity functionality. To resolve IP addresses to computer names, Defender for Identity sensors look up the IP addresses using the following methods:

* NTLM over RPC (TCP Port 135).
* NetBIOS (UDP port 137).
* RDP (TCP port 3389). Only the first packet of **Client hello** queries the DNS server using reverse DNS lookup of the IP address (UDP 53)

For the first three methods to work, the relevant ports must be opened inbound from the Defender for Identity sensors to devices on the network.

#### Windows Event logs

Defender for Identity detection relies on specific Windows Event logs that the sensor parses from your domain controllers. For the correct events to be audited and included in the Windows Event log, your domain controllers require accurate Advanced Audit Policy settings. For more information, see [Configure Advanced Audit Policy settings](configure-windows-event-collection.md#configure-advanced-audit-policy-settings).

To make sure Windows Event 8004 is audited as needed by the service, review your NTLM audit settings. For sensors running on AD FS servers, configure the auditing level to **Verbose**. For more information, see [Enable auditing on an ADFS object](configure-windows-event-collection.md#enable-auditing-on-an-adfs-object).

#### Supported Windows events

The following Windows events are supported for the Defender for Identity sensor to collect and enhance your system’s detection abilities:

* **For Active Directory Federation Services (AD FS) events**:
  + 1202 - The Federation Service validated a new credential
  + 1203 - The Federation Service failed to validate a new credential
  + 4624 - An account was successfully logged on
  + 4625 - An account failed to log on
* **For other events**:
  + 1644 - LDAP search
  + 4662 - An operation was performed on an object
  + 4726 - User Account Deleted
  + 4728 - Member Added to Global Security Group
  + 4729 - Member Removed from Global Security Group
  + 4730 - Global Security Group Deleted
  + 4732 - Member Added to Local Security Group
  + 4733 - Member Removed from Local Security Group
  + 4741 - Computer Account Added
  + 4743 - Computer Account Deleted
  + 4753 - Global Distribution Group Deleted
  + 4756 - Member Added to Universal Security Group
  + 4757 - Member Removed from Universal Security Group
  + 4758 - Universal Security Group Deleted
  + 4763 - Universal Distribution Group Deleted
  + 4776 - Domain Controller Attempted to Validate Credentials for an Account (NTLM)
  + 5136 - A directory service object was modified
  + 7045 - New Service Installed
  + 8004 - NTLM Authentication

#### Next steps

For more information, see:

* [Listen for SIEM events on your Defender for Identity sensor](configure-event-collection.md)
* [Configure Windows event forwarding](configure-event-forwarding.md)
* [Configure audit policies for Windows event logs](configure-windows-event-collection.md).

### Listen for SIEM events on your Defender for Identity standalone sensor

This article describes the required message syntax when configuring a Defender for Identity standalone sensor to listen for supported SIEM event types. Listening for SIEM events is one method for enhancing your detection abilities with extra Windows events that aren’t available from the domain controller network.

For more information, see [Windows event collection overview](event-collection-overview.md).

[!IMPORTANT] Defender for Identity standalone sensors do not support the collection of Event Tracing for Windows (ETW) log entries that provide the data for multiple detections. For full coverage of your environment, we recommend deploying the Defender for Identity sensor.

##### RSA Security Analytics

Use the following message syntax to configure your standalone sensor to listen for RSA Security Analytics events:

<Syslog Header>RsaSA\n2015-May-19 09:07:09\n4776\nMicrosoft-Windows-Security-Auditing\nSecurity\XXXXX.subDomain.domain.org.il\nYYYYY$\nMMMMM \n0x0

In this syntax:

* The syslog header is optional.
* The ``` character separator is required between all fields.
* The fields, in order, are:
  1. (Required) RsaSA constant
  2. The timestamp of the actual event. Make sure that it’s not the timestamp of the *arrival* to the SIEM, or when it’s sent to Defender for Identity. We highly recommend using an accuracy of milliseconds.
  3. The Windows event ID
  4. The Windows event provider name
  5. The Windows event log name
  6. The name of the computer receiving the event, such as the domain controller
  7. The name of the user authenticating
  8. The name of the source host name
  9. The result code of the NTLM

[!IMPORTANT] The order of the fields is important and nothing else should be included in the message.

##### MicroFocus ArcSight

Use the following message syntax to configure your standalone sensor to listen for MicroFocus ArcSight events:

CEF:0|Microsoft|Microsoft Windows||Microsoft-Windows-Security-Auditing:4776|The domain controller attempted to validate the credentials for an account.|Low| externalId=4776 cat=Security rt=1426218619000 shost=KKKKKK dhost=YYYYYY.subDomain.domain.com duser=XXXXXX cs2=Security cs3=Microsoft-Windows-Security-Auditing cs4=0x0 cs3Label=EventSource cs4Label=Reason or Error Code

In this syntax:

* Your message must comply with the protocol definition.
* No syslog header is included.
* The header part, separated by a *pipe* (**|**) must be included, as stated in the protocol
* The following keys in the *Extension* part must be present in the event:

| Key | Description |
| --- | --- |
| **externalId** | The Windows event ID |
| **rt** | The timestamp of the actual event. Make sure that the value isn’t the timestamp of the *arrival* to the SIEM, or when it’s sent to Defender for Identity. Also make sure sure to use an accuracy of milliseconds. |
| **cat** | The Windows event log name |
| **shost** | The source host name |
| **dhost** | The computer receiving the event, such as the domain controller |
| **duser** | The user authenticating |

* The order isn’t important for the *Extension* part
* You must have a custom key and **keyLable** for the following fields:
  + EventSource
  + `Reason or Error Code`` = The result code of the NTLM

##### Splunk

Use the following message syntax to configure your standalone sensor to listen for Splunk events:

<Syslog Header>\r\nEventCode=4776\r\nLogfile=Security\r\nSourceName=Microsoft-Windows-Security-Auditing\r\nTimeGenerated=20150310132717.784882-000\r\ComputerName=YYYYY\r\nMessage=

In this syntax:

* The syslog header is optional.
* There’s a \r\n character separator between all required fields. These are CRLF control characters, (0D0A in hex), and not literal characters.
* The fields are in key=value format.
* The following keys must exist and have a value:

| Name | Description |
| --- | --- |
| **EventCode** | The Windows event ID |
| **Logfile** | The Windows event log name |
| **SourceName** | The Windows event provider name |
| **TimeGenerated** | The timestamp of the actual event. Make sure that the value isn’t the timestamp of the *arrival* to the SIEM, or when it’s sent to Defender for Identity. The timestamp format must be The format should match yyyyMMddHHmmss.FFFFFF, and you must use an accuracy of milliseconds. |
| **ComputerName** | The source host name |
| **Message** | The original event text from the Windows event |

* The *Message Key* and value must be last.
* The order isn’t important for the key=value pairs.

A message similar to the following appears:

The computer attempted to validate the credentials for an account.  
  
Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
  
Logon Account: Administrator  
  
Source Workstation: SIEM  
  
Error Code: 0x0

##### QRadar

QRadar enables event collection via an agent. If the data is gathered using an agent, the time format is gathered without millisecond data.

Because Defender for Identity needs millisecond data, you must first configure QRadar to use agentless Windows event collection. For more information, see [QRadar: Agentless Windows Events Collection using the MSRPC Protocol](https://www.ibm.com/support/pages/qradar-agentless-windows-events-collection-using-msrpc-protocol-msrpc-faq).

Use the following message syntax to configure your standalone sensor to listen for QRadar events:

<13>Feb 11 00:00:00 %IPADDRESS% AgentDevice=WindowsLog AgentLogFile=Security Source=Microsoft-Windows-Security-Auditing Computer=%FQDN% User= Domain= EventID=4776 EventIDCode=4776 EventType=8 EventCategory=14336 RecordNumber=1961417 TimeGenerated=1456144380009 TimeWritten=1456144380009 Message=The computer attempted to validate the credentials for an account. Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0 Logon Account: Administrator Source Workstation: HOSTNAME Error Code: 0x0

In this syntax, you must include the following fields:

* The agent type for the collection
* The Windows event log provider name
* The Windows event log source
* The DC fully qualified domain name
* The Windows event ID
* TimeGenerated, which is the timestamp of the actual event. Make sure that the value isn’t the timestamp of the *arrival* to the SIEM, or when it’s sent to Defender for Identity. The timestamp format must be The format should match yyyyMMddHHmmss.FFFFFF, and must have an accuracy of milliseconds.

Make sure that the message includes the original event text from the Windows event, and that you have `` between the key=value pairs.

[!NOTE] Using WinCollect for Windows event collection is not supported.

#### Next steps

* [Defender for Identity sizing tool](https://aka.ms/mdi/sizingtool)
* [Defender for Identity SIEM log reference](../cef-format-sa.md)
* [Defender for Identity prerequisites](prerequisites.md)
* [Check out the Defender for Identity forum!](https://aka.ms/MDIcommunity)

## Configure audit policies for Windows event logs

Microsoft Defender for Identity detection relies on specific Windows Event log entries to enhance detections and provide extra information on the users who performed specific actions, such as NTLM logons and security group modifications.

For the correct events to be audited and included in the Windows Even Log, your domain controllers require specific Advanced Audit Policy settings. Misconfigured Advanced Audit Policy settings can cause gaps in the Event Log and incomplete Defender for Identity coverage.

This article describes how to configure your Advanced Audit Policy settings as needed and other configurations for specific event types.

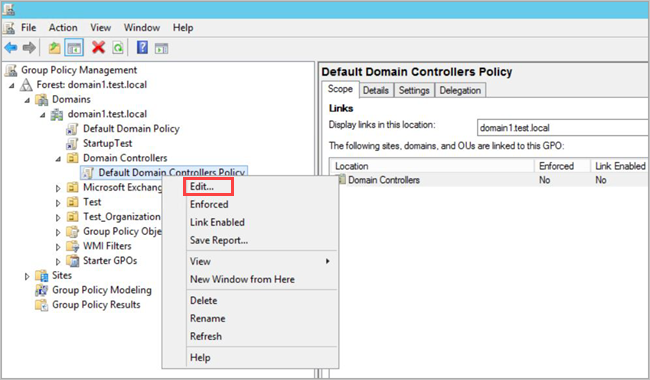
[!TIP] Some events that are collected by the Defender for Identity sensor aren’t collected by default by the Defender for Identity standalone sensor. If you’re working with the standalone Defender for Identity sensor, forward events using the following methods:

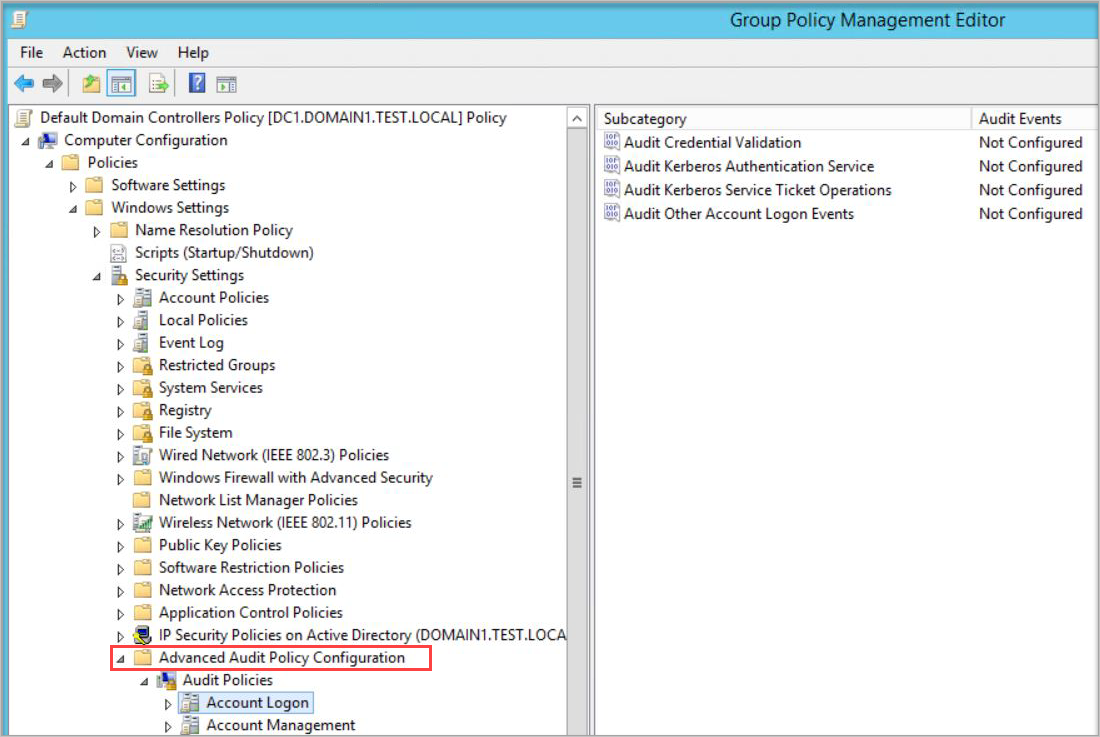
* [Configure the Defender for Identity standalone sensor](configure-event-forwarding.md) to listen for SIEM events
* [Configure Windows Event Forwarding](configure-event-forwarding.md)

### Configure Advanced Audit Policy settings

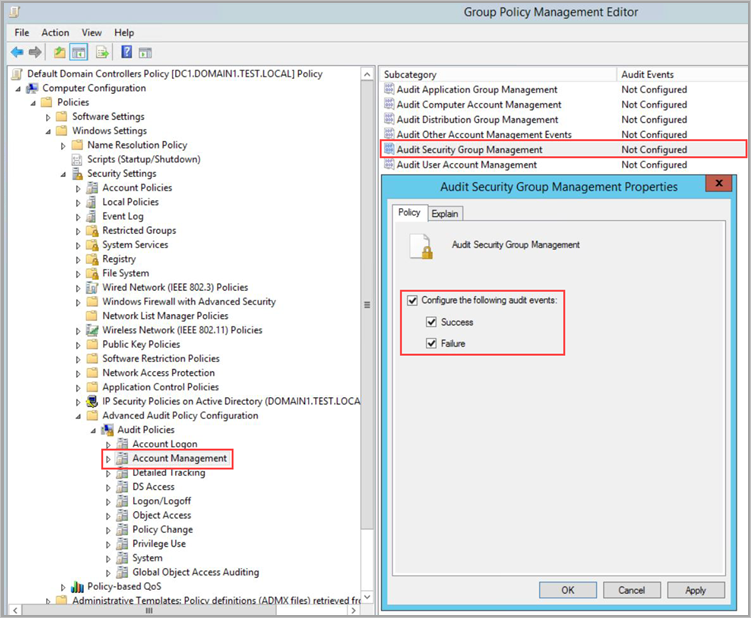
This procedure describes how to modify your domain controller’s Advanced Audit Policies as needed for Defender for Identity.

1. Log in to the server as **Domain Administrator**.
2. Open the Group Policy Management Editor from **Server Manager** > **Tools** > **Group Policy Management**.
3. Expand the **Domain Controllers Organizational Units**, right-click **Default Domain Controllers Policy**, and then select **Edit**. For example:

* 
* Screenshot of the Edit domain controller policy dialog.
* [!NOTE] Use the Default Domain Controllers Policy or a dedicated GPO to set these policies.

1. From the window that opens, go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** and depending on the policy you want to enable, do the following:
   1. Go to **Advanced Audit Policy Configuration** > **Audit Policies**. For example:
   * 
   * Screenshot of the Advanced Audit Policy Configuration dialog.
   1. Under **Audit Policies**, edit each of the following policies and select **Configure the following audit events** for both **Success** and **Failure** events.

| Audit policy | Subcategory | Triggers event IDs |
| --- | --- | --- |
| **Account Logon** | Audit Credential Validation | 4776 |
| **Account Management** | Audit Computer Account Management | 4741, 4743 |
| **Account Management** | Audit Distribution Group Management | 4753, 4763 |
| **Account Management** | Audit Security Group Management | 4728, 4729, 4730, 4732, 4733, 4756, 4757, 4758 |
| **Account Management** | Audit User Account Management | 4726 |
| **DS Access** | Audit Directory Service Access | 4662 - For this event, it’s also necessary to [Configure object auditing](#configure-object-auditing). |
| **DS Access** | Audit Directory Service Changes | 5136 |
| **System** | Audit Security System Extension | 7045 |

* + For example, to configure **Audit Security Group Management**, under **Account Management**, double-click **Audit Security Group Management**, and then select **Configure the following audit events** for both **Success** and **Failure** events:
  + 
  + Screenshot of the Audit Security Group Management dialog.

1. From an elevated command prompt type gpupdate.
2. After applying via GPO, the new events are visible in the Event Viewer, under **Windows Logs** -> **Security**.

### Event ID 8004

This section describes the extra configuration steps needed to audit Event ID 8004.

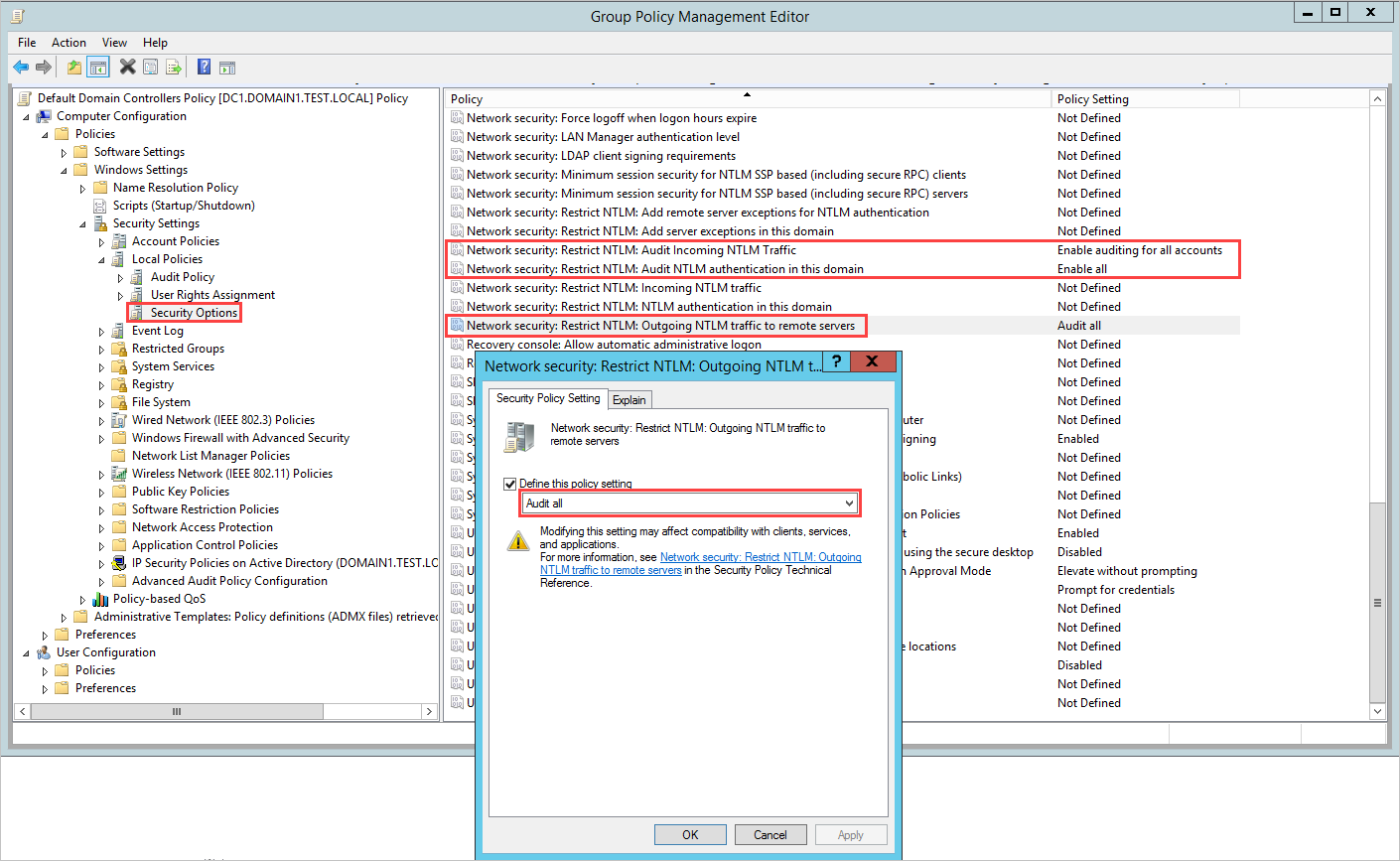
[!NOTE]

* Domain group policies to collect Windows Event 8004 should **only** be applied to domain controllers.
* When Windows Event 8004 is parsed by Defender for Identity Sensor, Defender for Identity NTLM authentications activities are enriched with the server accessed data.

1. Following the [initial steps](#configure-advanced-audit-policy-settings), open **Group Policy Management** and go to the **Default Domain Controllers Policy** > **Local Policies** > **Security Options**.
2. Under **Security Options**, configure the specified security policies as follows:

| Security policy setting | Value |
| --- | --- |
| **Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers** | Audit all |
| **Network security: Restrict NTLM: Audit NTLM authentication in this domain** | Enable all |
| **Network security: Restrict NTLM: Audit Incoming NTLM Traffic** | Enable auditing for all accounts |

For example, to configure **Outgoing NTLM traffic to remote servers**, under **Security Options**, double-click **Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers**, and then select **Audit all**:



Screenshot of the Audit Outgoing NTLM traffic to remote servers configuration.

### Configure auditing for extra LDAP queries

Microsoft Defender for Identity can monitor extra LDAP queries in your network, which are sent over the Active Directory Web Service protocol and act like normal LDAP queries. To have visibility into these activities, you need to enable **event 1644** on your domain controllers.

Event 1644 covers LDAP activities in your domain and is primarily used to identify expensive, inefficient, or slow Lightweight Directory Access Protocol (LDAP) searches that are serviced by Active Directory domain controllers.

[!IMPORTANT] Logging the 1644 events may impact server performance. While the resource limitation feature can stop the Defender for Identity service if the server is running out of resources, it does not stop the event auditing at the operating system level. Therefore, to avoid performance issues, make sure your servers have sufficient memory, CPU, and disk resources.

Windows event 1644 isn’t collected by default on domain controllers and needs to be manually activated to support this feature. Create registry keys with the following values:

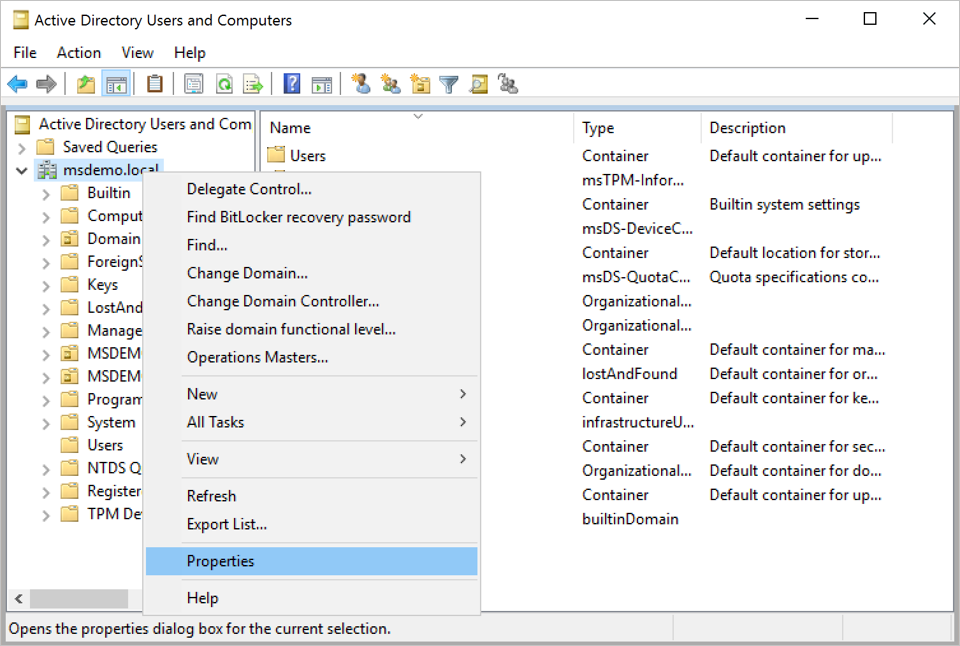
Windows Registry Editor Version 5.00   
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics]   
"15 Field Engineering"=dword:00000005   
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters]   
"Expensive Search Results Threshold"=dword:00000001   
"Inefficient Search Results Threshold"=dword:00000001 "Search Time Threshold (msecs)"=dword:00000001

### Configure object auditing

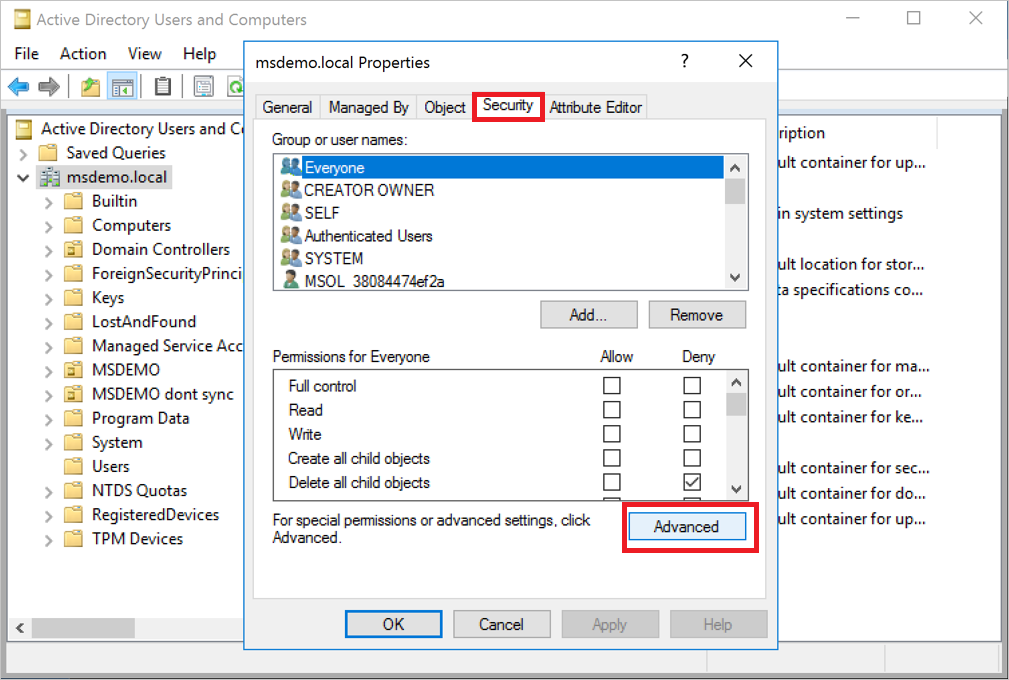
To collect 4662 events, you must also configure object auditing on the user, group and computer objects. This procedure describes how to enable auditing on all users, groups, and computers in the Active Directory domain.

[!IMPORTANT] Make sure to [review and verify your audit policies](#configure-advanced-audit-policy-settings) before enabling event collection to ensure that the domain controllers are properly configured to record the necessary events. If configured properly, this auditing should have minimal effect on server performance.

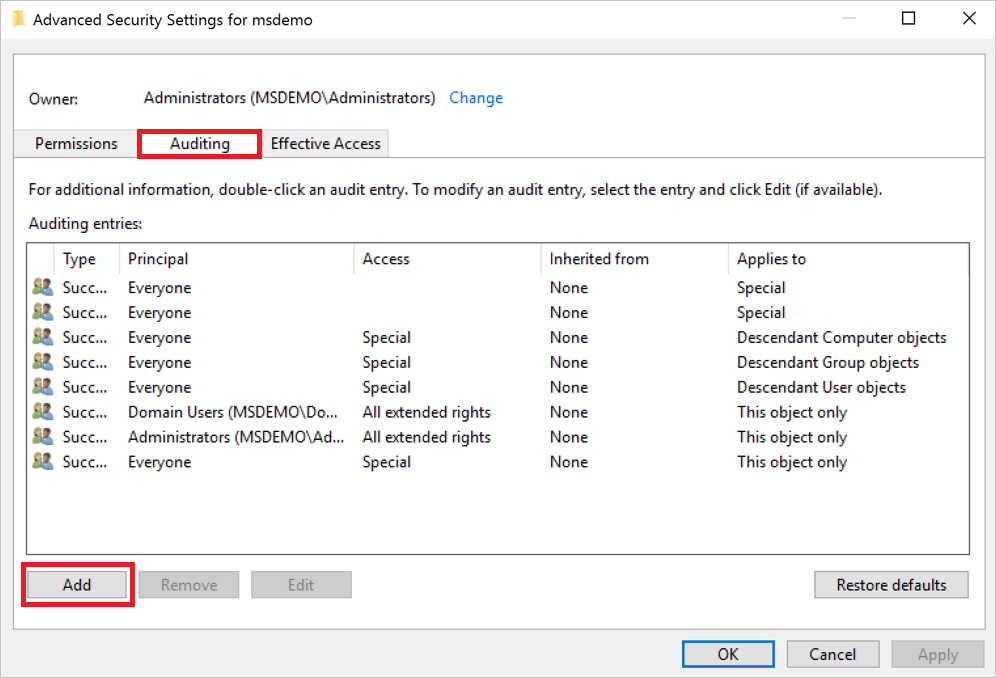
1. Go to the **Active Directory Users and Computers** console.
2. Select the domain you want to audit.
3. Select the **View** menu and select **Advanced Features**.
4. Right-click the domain and select **Properties**. For example:

* 
* Screenshot of the container properties option.

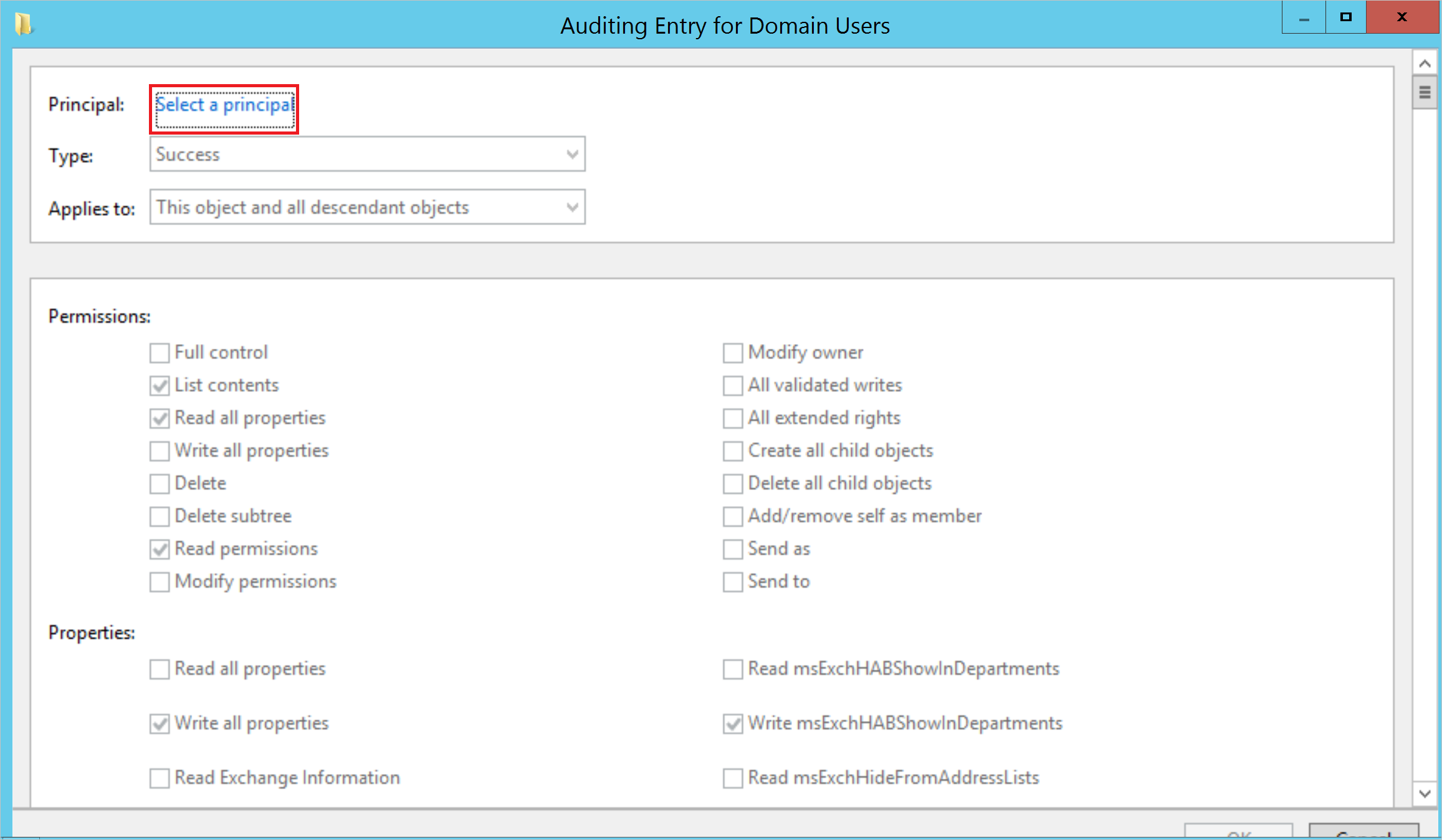
1. Go to the **Security** tab, and select **Advanced**. For example:

* 
* Screenshot of the advanced security properties dialog.

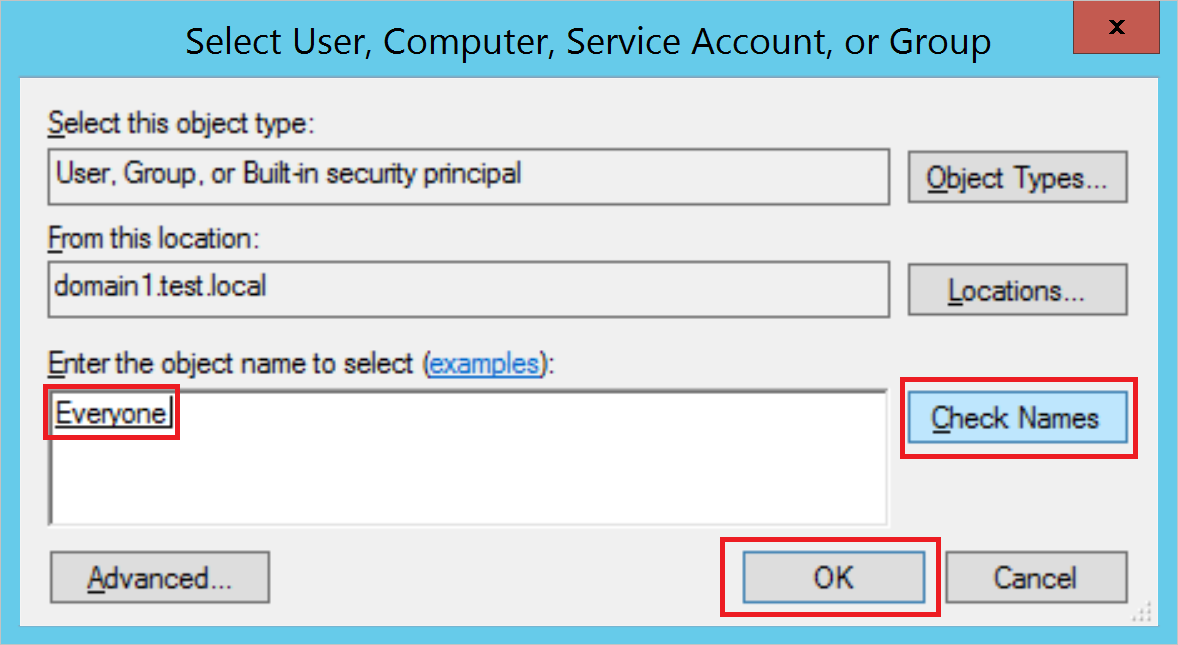
1. In **Advanced Security Settings**, select the **Auditing** tab and then select **Add**. For example:

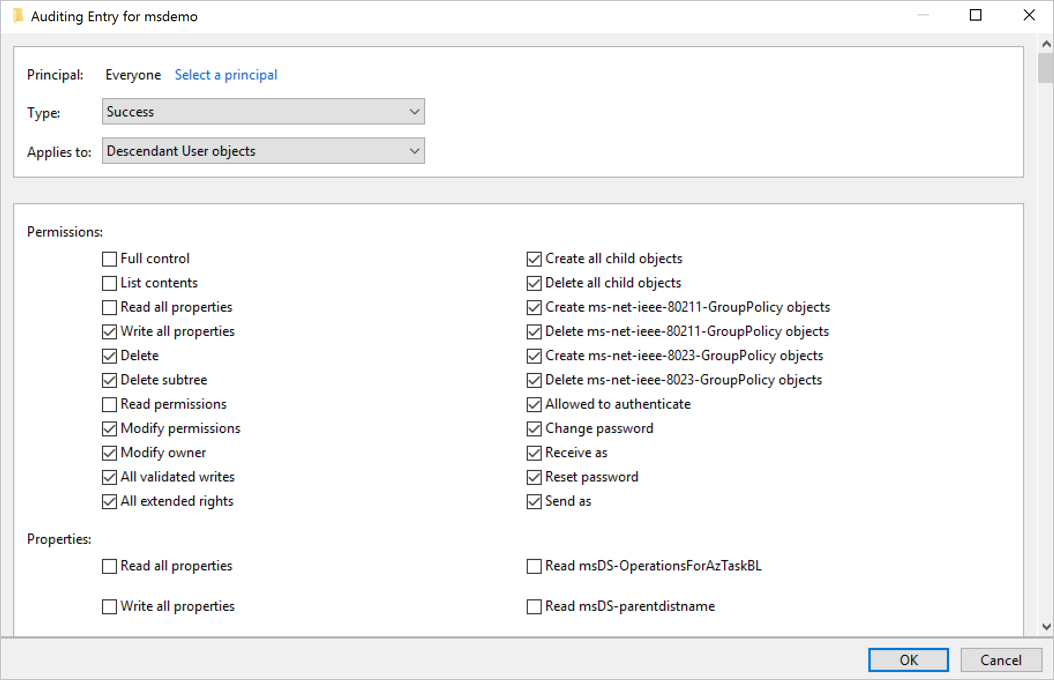
* 
* Screenshot of the Auditing tab.

1. Select **Select a principal**. For example:

* 
* Screenshot of the Select a principal option.

1. Under **Enter the object name to select**, enter **Everyone** and select **Check Names** > **OK**. For example:

* 
* Screenshot of the Select everyone settings.

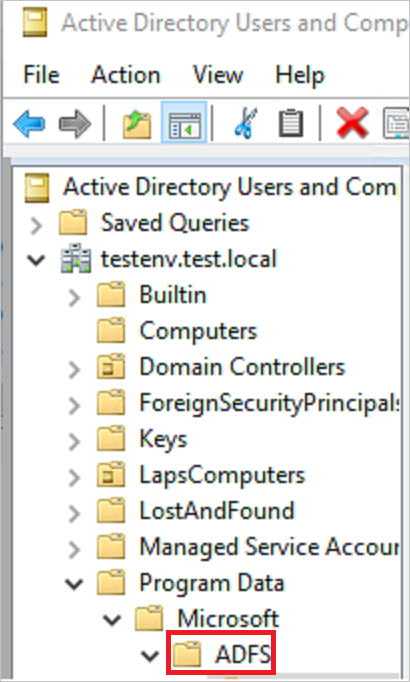
1. You’ll then return to **Auditing Entry**. Make the following selections:
   1. For **Type** select **Success**.
   2. For **Applies to** select **Descendant User objects.**
   3. Under **Permissions**, scroll down and select the **Clear all** button. For example:
   * :::image type=“content” source=“../media/clear-all.png” alt-text=“Screenshot of selecting Clear all.”:::
   1. Scroll back up and select **Full Control**. All the permissions are selected.
   2. Clear the selection for the **List contents**, **Read all properties**, and **Read permissions** permissions, and select **OK**. This sets all the **Properties** settings to **Write**. For example:
   * 
   * Screenshot of selecting permissions.
   * Now, when triggered, all relevant changes to directory services will appear as 4662 events.
2. Repeat the steps in this procedure, but for **Applies to**, select the following object types:
   * **Descendant Group Objects**
   * **Descendant Computer Objects**
   * **Descendant msDS-GroupManagedServiceAccount Objects**
   * **Descendant msDS-ManagedServiceAccount Objects**

[!NOTE] Assigning the auditing permissions on the **All descendant objects** would work as well, but we only require the object types as detailed above.

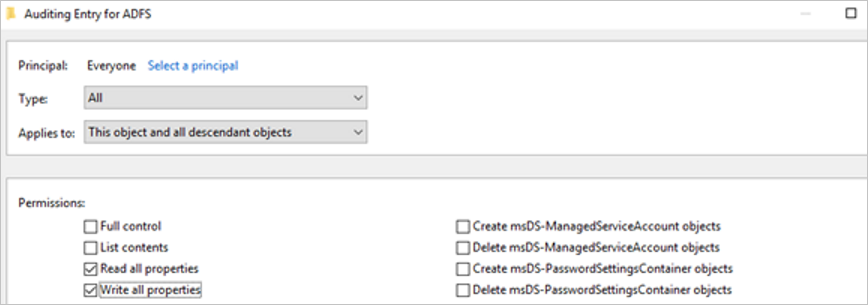
Some detections require auditing specific Active Directory objects. To do so, follow the steps in this procedure, with the changes noted as follows regarding the objects to audit and permissions to include.

#### Enable auditing on an ADFS object

1. Go to the **Active Directory Users and Computers** console, and select the domain you want to enable the logs on.
2. Go to to **Program Data** > **Microsoft** > **ADFS**. For example:

* 
* Screenshot of an ADFS container.

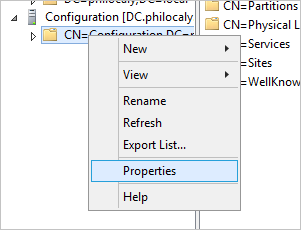
1. Right-click **ADFS** and select **Properties**.
2. Go to the **Security** tab and select **Advanced** > **Advanced Security Settings** > **Auditing** tab > **Add** > **Select a principal**.
3. Under **Enter the object name to select**, enter **Everyone**.
4. Select **Check Names** > **OK**.
5. You’ll then return to **Auditing Entry**. Make the following selections:
   * For **Type** select **All**.
   * For **Applies to** select **This object and all descendant objects**.
   * Under **Permissions**, scroll down and select **Clear all**. Scroll up and select **Read all properties** and **Write all properties**.

* For example:
* 
* Screenshot of the auditing settings for ADFS.

1. Select **OK**.

#### Enable auditing on an Exchange object

1. Open ADSI Edit by selecting **Start** > **Run**. Enter *ADSIEdit.msc* and select **OK**.
2. On the **Action** menu, select **Connect to**.
3. In the **Connection Settings** dialog boxm under **Select a well known Naming Context**, select **Configuration** > **OK**.
4. Expand the **Configuration** container to show the **Configuration** node, beginning with *“CN=Configuration,DC=…”*
5. Right-click the **Configuration** node and select **Properties**. For example:

* 
* Screenshot of the Configuration node properties.

1. Select the **Security** tab > **Advanced**.
2. In the **Advanced Security Settings**, select the **Auditing** tab > **Add**.
3. Select **Select a principal**.
4. Under **Enter the object name to select**, enter **Everyone** and select **Check Names** > **OK**.
5. You’ll then return to **Auditing Entry**. Make the following selections:
   * For **Type** select **All**.
   * For **Applies to** select **This object and all descendant objects**.
   * Under **Permissions**, scroll down and select **Clear all**. Scroll up and select **Write all properties**.

* For example:
* 
* Screenshot of the auditing settings for the Configuration container.

1. Select **OK**.

### Next steps

[!div class=“step-by-step”] [« Plan capacity for Microsoft Defender for Identity](capacity-planning.md) [Directory Service accounts »](directory-service-accounts.md)

## Configure Windows event forwarding to your Defender for Identity standalone sensor

This article describes an example of how to configure Windows event forwarding to your Microsoft Defender for Identity standalone sensor. Event forwarding is one method for enhancing your detection abilities with extra Windows events that aren’t available from the domain controller network. For more information, see [Windows event collection overview](event-collection-overview.md).

[!IMPORTANT] Defender for Identity standalone sensors do not support the collection of Event Tracing for Windows (ETW) log entries that provide the data for multiple detections. For full coverage of your environment, we recommend deploying the Defender for Identity sensor.

### Prerequisites

Before you start:

* Make sure that the domain controller is properly configured to capture the required events.
* [Configure port mirroring](configure-port-mirroring.md)

### Step 1: Add the network service account to the domain

This procedure describes how to add the network service account to the **Event Log Readers Group** domain. For this scenario, assume that the Defender for Identity standalone sensor is a member of the domain.

1. In Active Directory’s Users and Computers, go to the **Built-in** folder and double-click **Event Log Readers**.
2. Select **Members**.
3. If **Network Service** is not listed, select **Add**, and then enter **Network Service** in the **Enter the object names to select** field.
4. Select **Check Names** and select **OK** twice.

After adding the **Network Service** to the **Event Log Readers** group, reboot the domain controllers for the change to take effect.

For more information, see [Active Directory accounts](/windows-server/identity/ad-ds/manage/understand-default-user-accounts).

### Step 2: Create a policy that sets the Configure target setting

This procedure describes how to create a policy on the domain controllers to set the **Configure target** Subscription Manager setting

[!TIP] You can create a group policy for these settings and apply the group policy to each domain controller monitored by the Defender for Identity standalone sensor. The following steps modify the local policy of the domain controller.

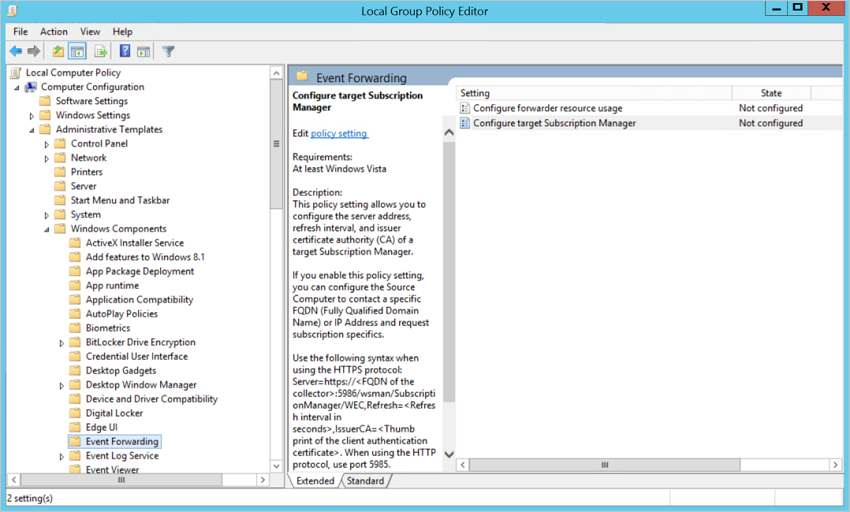
1. On each domain controller, run:

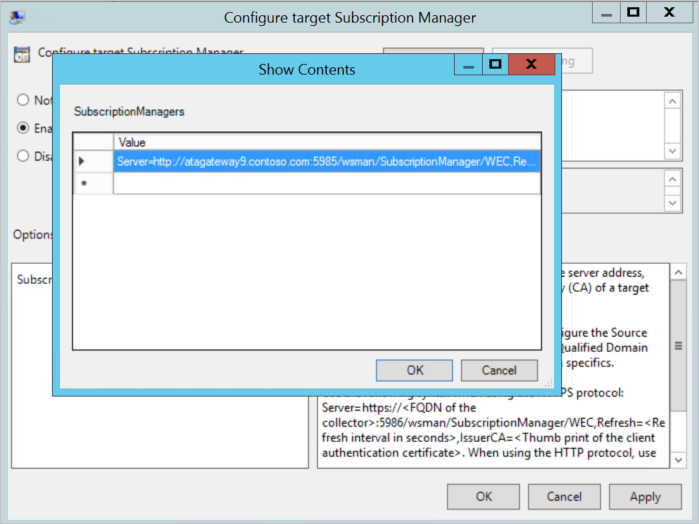
* ninrm quick config

1. From a command prompt, enter

* gpedit.msc

1. Expand **Computer Configuration > Administrative Templates > Windows Components > Event Forwarding**. For example:

* 
* Screenshot of the Local policy group editor dialog.

1. Double-click **Configure target Subscription Manager** and then:
   1. Select **Enabled**.
   2. Under **Options**, select **Show**.
   3. Under **SubscriptionManagers**, enter the following value and select **OK**:
   * **Server=http://<fqdnMicrosoftDefenderForIdentitySensor>:5985/wsman/SubscriptionManager/WEC,Refresh=10**
   * For example, using **Server=http://atpsensor9.contoso.com:5985/wsman/SubscriptionManager/WEC,Refresh=10**:
   * 
   * Screenshot of the Configure target subscription dialog.
2. Select **OK**.
3. From an elevated command prompt, enter:

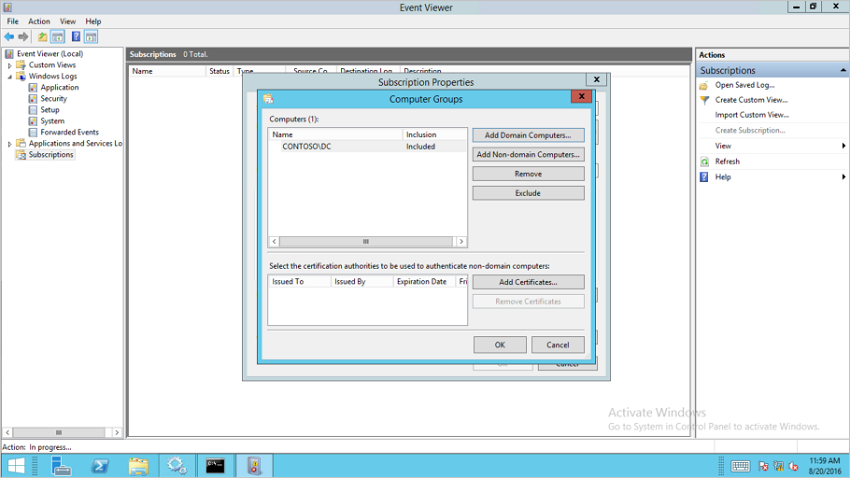
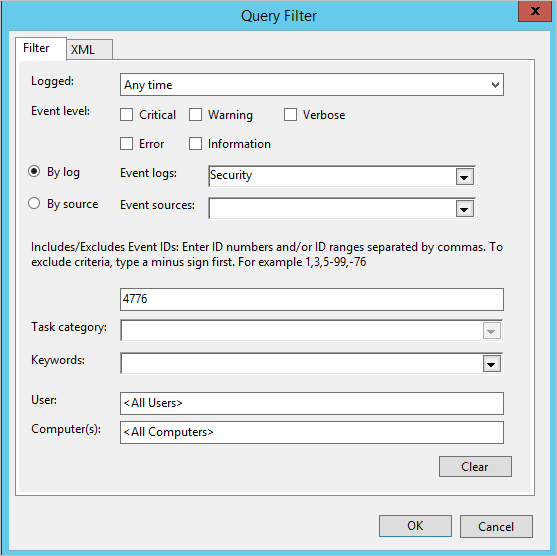
* gpupdate /force

#### Step 3: Create and select a subscription on your sensor

This procedure describes how to create a subscription for use with Defender for Identity and then select it from your standalone sensor.

1. Open an elevated command prompt and enter

* wecutil qc

1. Open **Event Viewer**.
2. Right-click **Subscriptions** and select **Create Subscription**.
   1. Enter a name and description for the subscription.
   2. For **Destination Log**, confirm that **Forwarded Events** is selected. For Defender for Identity to read the events, the destination log must be **Forwarded Events**.
   3. Select **Source computer initiated** > **Select Computers Groups** > **Add Domain Computer**.
      1. Enter the name of the domain controller in the **Enter the object name to select** field.
      2. Select **Check Names** > **OK** > **OK**.
      3. Select **OK**. For example:
      * 
      * Screenshot of the Event Viewer dialog.
   4. Select **Select Events** > **By log** > **Security**.
   5. In the **Includes/Excludes Event ID** field type the event number and select **OK**. For example, enter **4776**:
   * 
   * Screenshot of the Query dialog.
   1. Return to the command window opened in the first step. Run the following commands, replacing *SubscriptionName* with the name you created for the subscription.
   * wecutil ss "SubscriptionName" /cm:"Custom"  
     wecutil ss "SubscriptionName" /HeartbeatInterval:5000
   1. Return to the **Event Viewer** console. Right-click the created subscription and select **Runtime Status** to see if there are any issues with the status.
   2. After a few minutes, check to see that the events you set to be forwarded is showing up in the Forwarded Events on the Defender for Identity standalone sensor.

For more information, see: [Configure the computers to forward and collect events](/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc748890(v=ws.11))

### Next steps

* [Install Defender for Identity](/defender-for-identity/classic-install-step1)
* [Check out the Defender for Identity forum!](https://aka.ms/MDIcommunity)