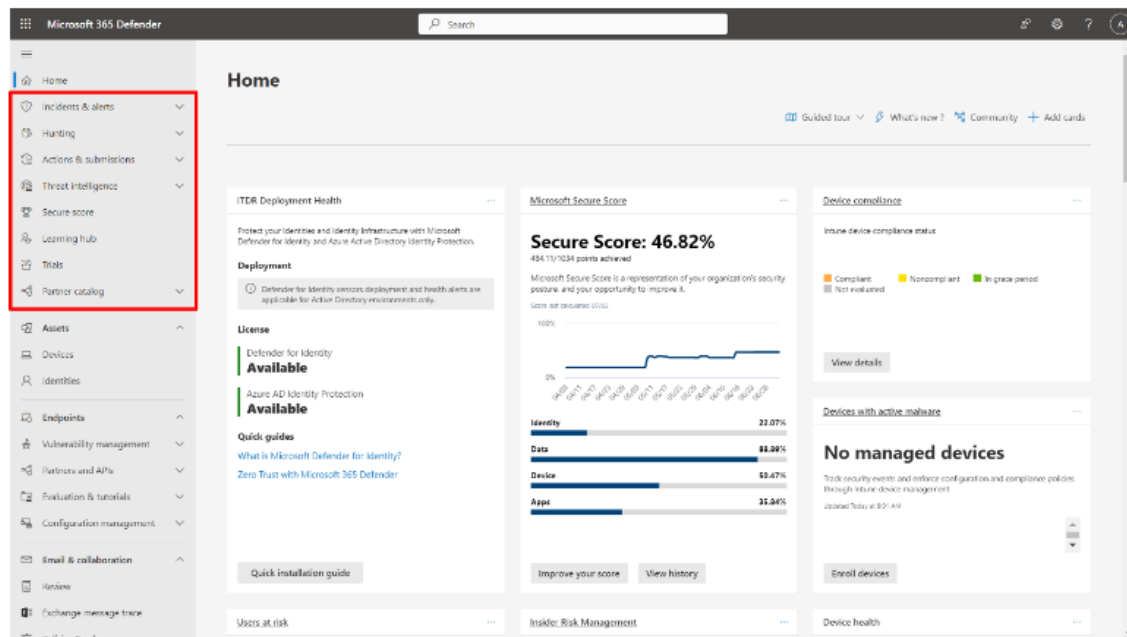


## Sign in

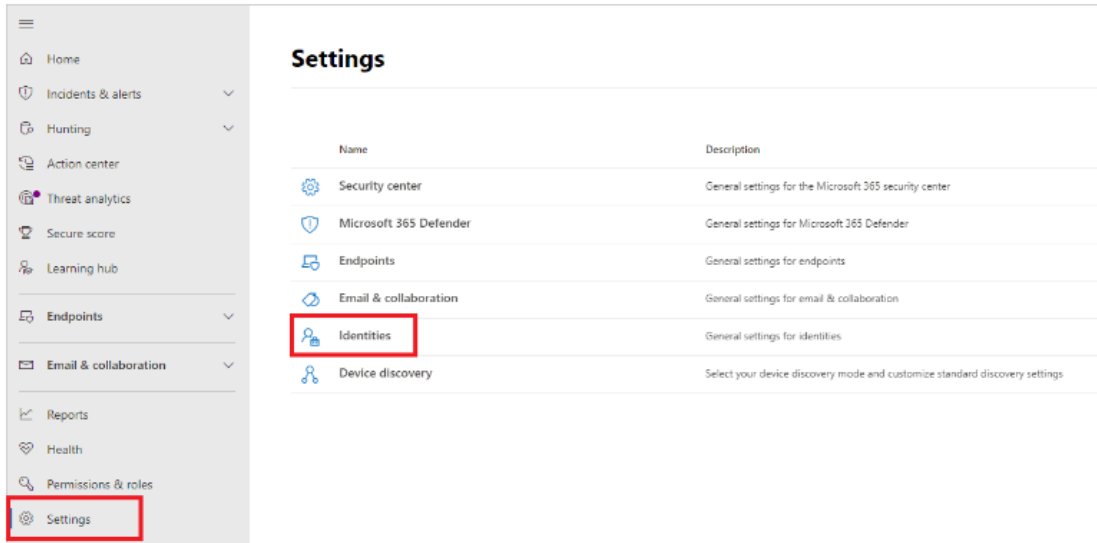
To begin the deployment, sign in to the [Microsoft 365 Defender portal](#). From the navigation menu, select any item, such as **Incidents & alerts**, **Hunting**, **Actions & submissions**, or **Threat intelligence** to initiate the onboarding process.



You'll then get the option to deploy supported services, including MDI. When you go to the MDI settings, the required cloud components will be auto-provisioned.

## Step 1: Download the Microsoft Defender for Identity sensor

1. In the [portal](#), go to **Settings** and then **Identities**.



The screenshot displays the Microsoft Defender for Identity portal interface. On the left is a navigation sidebar with various menu items. The 'Settings' item at the bottom of this sidebar is highlighted with a red rectangle. The main content area on the right is titled 'Settings' and contains a table with two columns: 'Name' and 'Description'. The table lists several configuration categories. The 'Identities' row in this table is also highlighted with a red rectangle.

Name	Description
Security center	General settings for the Microsoft 365 security center
Microsoft 365 Defender	General settings for Microsoft 365 Defender
Endpoints	General settings for endpoints
Email & collaboration	General settings for email & collaboration
<b>Identities</b>	General settings for identities
Device discovery	Select your device discovery mode and customize standard discovery settings

2. Select the **Sensors** page, which displays all of your MDI sensors.

**Microsoft Defender for Identity**

Deploying sensors enables you to monitor your on-premises Active Directory environment for suspicious activities and risky configurations. [Learn more](#)

Filter: Type: Any Domain: Any Delayed update: Any Service status: Any Sensor status: Any Health status: Any

Export Add sensor

Sensor	Type	Domain	Service status	Sensor status	Version	Delayed update	Health status	Health issues	Created
<input type="checkbox"/> DC2	Domain controller Sensor	domain1.test.local	Running	Up to date	2.101.1552.8750	Disabled	Healthy	0	Jul 21, 2022 9:00 PM
<input type="checkbox"/> STANDALONE	Standalone Sensor	domain1.test.local	Running	Up to date	2.104.1595.42207	Enabled	Healthy	0	Nov 6, 2022 5:02 PM
<input type="checkbox"/> DC4	Domain controller Sensor	domain1.test.local	Running	Up to date	2.101.1552.8750	Disabled	Healthy	0	Jul 21, 2022 9:07 PM

3. Select **Add sensor**.

**Microsoft Defender for Identity**

Sensors enable monitoring your on-premises Active Directory environment for suspicious activities and risky configurations. [Learn more](#)

Sensors

Directory services accounts

Syslog notifications

Sensitive tag

Exchange server tag

Honeytoken tag

Export + Add sensor Delete

Filter Reset Filters

Domain: Any Delayed update: Any

Sensor

4. A pane will open, providing you with a button to download the sensor installer and a generated access key.

✕

## Add a new sensor

Install and configure the sensor using the generated access key. Once installed, the new sensor will appear in the sensor list. [How?](#)

**Download installer**

Access key

QC7kADzYrEj6Q5GZe/EtlprvfXpq/Sr4o1PSh6KlIzrnMQRKaCriPAMZgaGh4...

Access key is only used during sensor deployment, Re-generating the key will invalidate all previous keys, for all sensors.

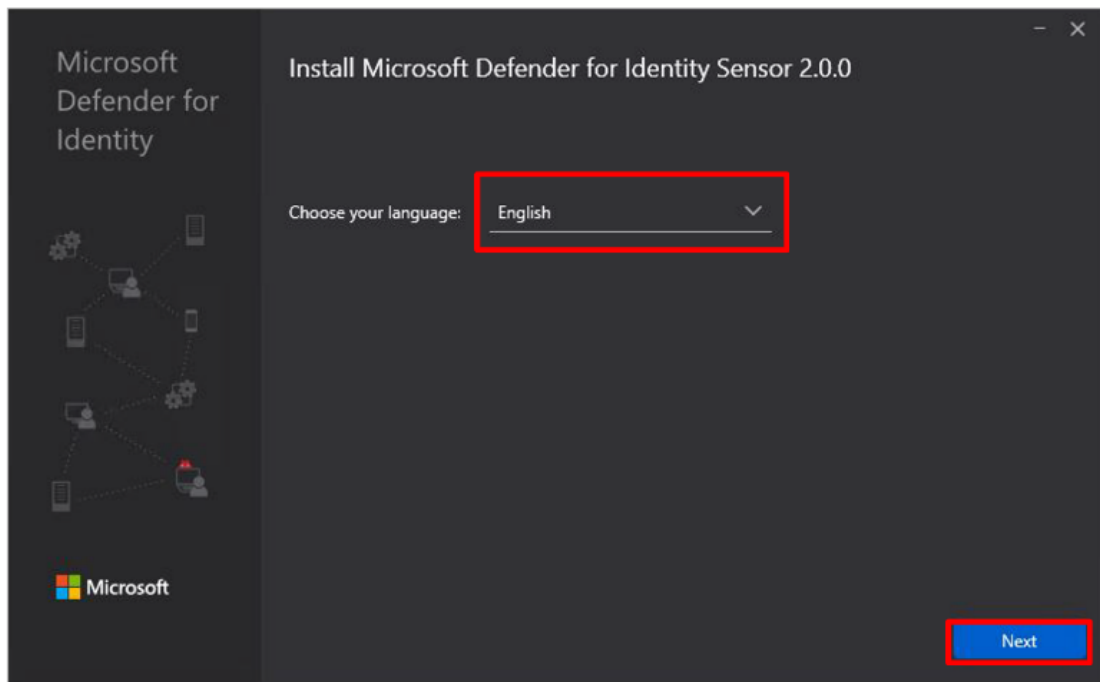
**Regenerate key**

5. Select **Download installer** to save the package locally. The zip file includes the following files:
  - MDI sensor installer
  - Configuration setting file with the required information to connect to the MDI cloud service.
6. Also copy the **Access key**. The access key is required for the MDI sensor to connect to your MDI instance and you will use it in a later step. The access key is a one-time password for sensor deployment, after which all communication is performed using certificates for authentication and TLS encryption.
7. 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.
8. Next, copy the package to the dedicated server or domain controller onto which you're installing the MDI sensor.

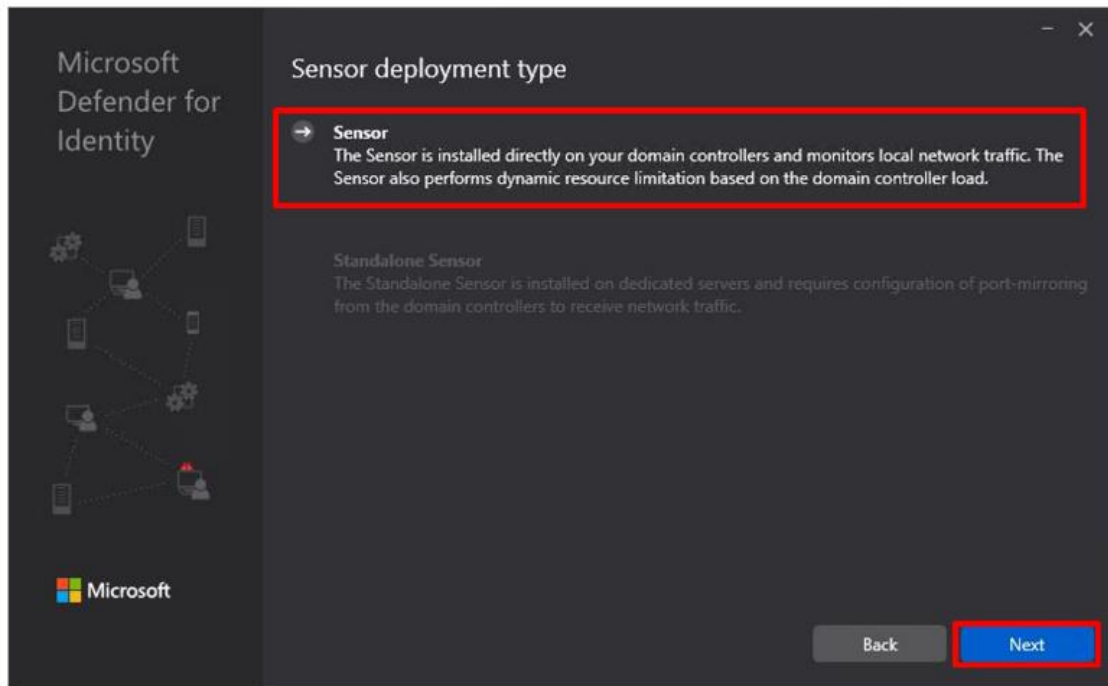
## Step 2: Install the Microsoft Defender for Identity sensor

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

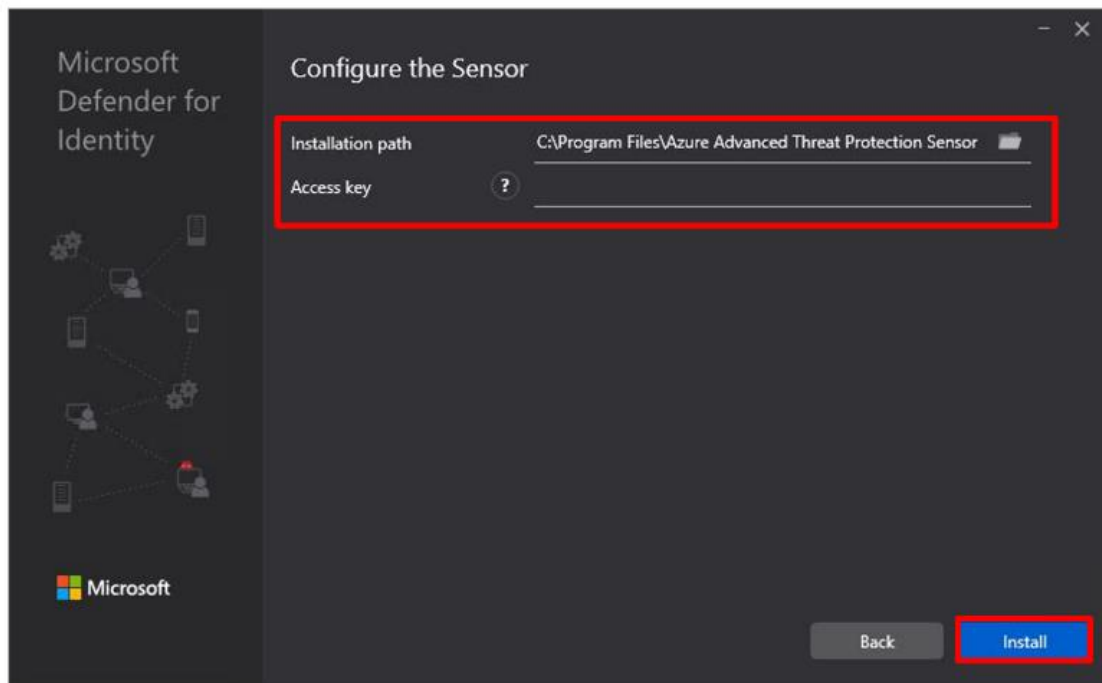
1. Verify that the machine has connectivity to the relevant [MDI cloud service](#) endpoints.
2. Extract the installation files from the zip file. Take note that installing directly from the zip file will fail.
3. Run *Azure ATP sensor setup.exe* with elevated privileges with other words, run as administrator and follow the setup wizard.
4. On the **Welcome** page, select your language and select **Next**.



5. The installation wizard automatically checks if the server is a domain controller, an AD FS server or a dedicated server. If it's a domain controller or AD FS server, the MDI sensor will install. If it's a dedicated server, the MDI standalone sensor will install. For example, for an MDI sensor, the following screen will display to let you know that an MDI sensor is installed on your dedicated server. Select **Next** on this screen.



- Under **Configure the sensor**, enter the installation path and the access key that you copied from the previous step, based on your environment. The installation path is the location where the MDI sensor is installed. By default the path is **%programfiles%\Azure Advanced Threat Protection sensor**. Leave the default value. The access key was retrieved from the Microsoft 365 Defender portal in the previous step. Select **Install**.



Microsoft Defender for Identity

Configure the Sensor


Installation path C:\Program Files\Azure Advanced Threat Protection Sensor

Access key ?

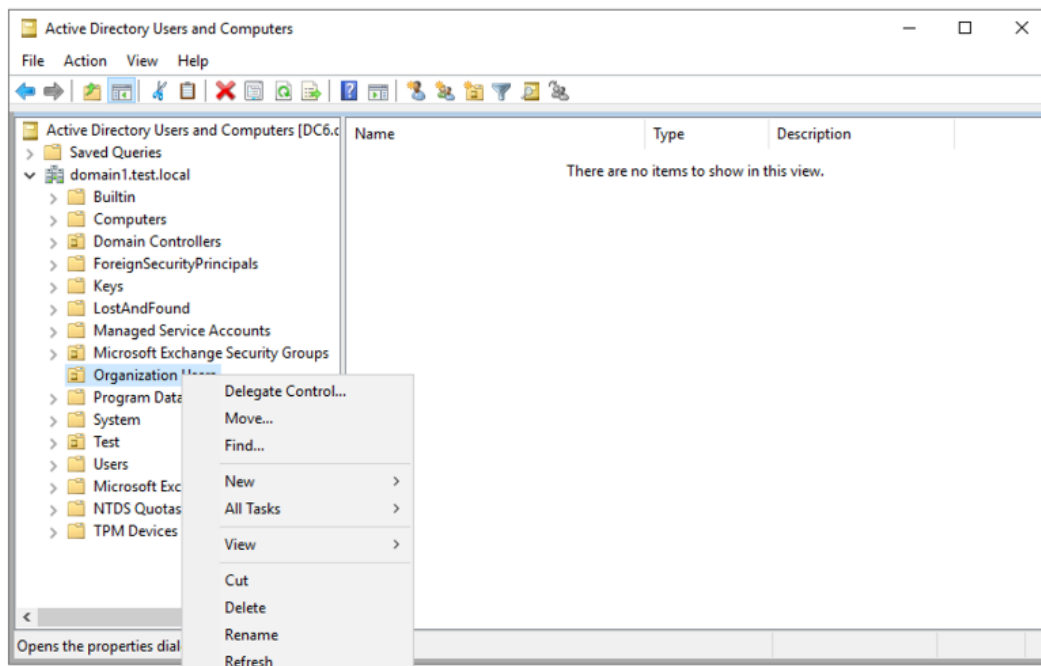
Back Install

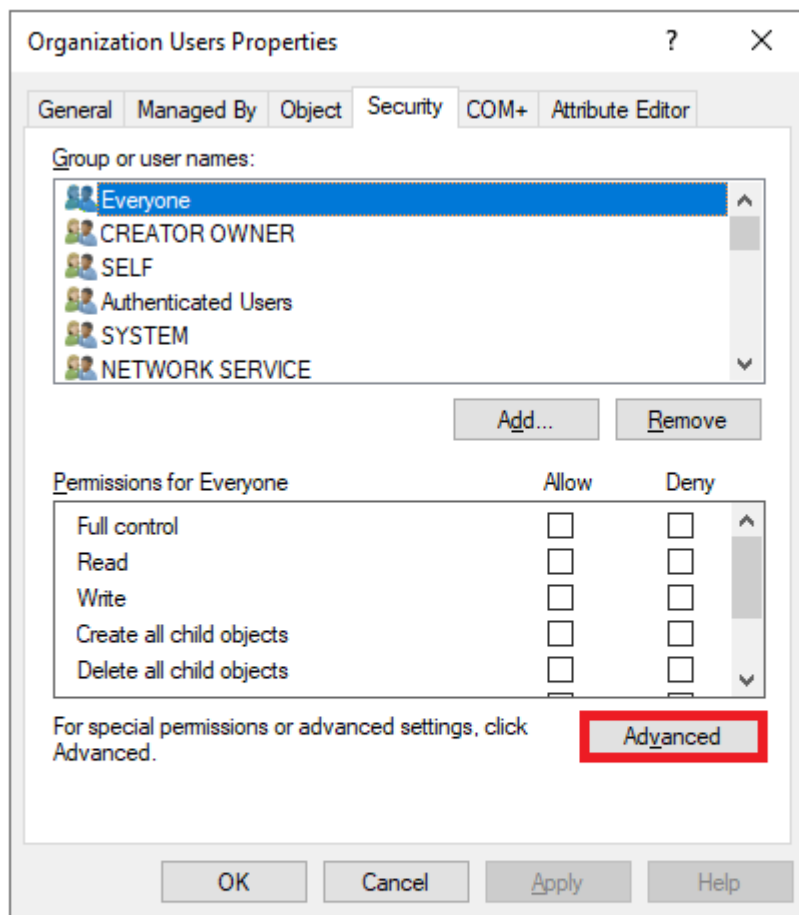


### Step 3: Manage Action accounts

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

1. On a domain controller in your domain, create a new gMSA account.
2. Assign the **Log on as a service** right to the gMSA account on each domain controller that runs the MDI sensor.
3. Grant the required permissions to the gMSA account.
4. Open **Active Directory Users and Computers**.
5. Right-click the relevant domain or OU, and select **Properties**.





6. Go the **Security** tab and select **Advanced**.
7. Select **Add**.
8. Choose **Select principal**.

Permission Entry for wdgexp

Principal: Select a principal

Type: Allow

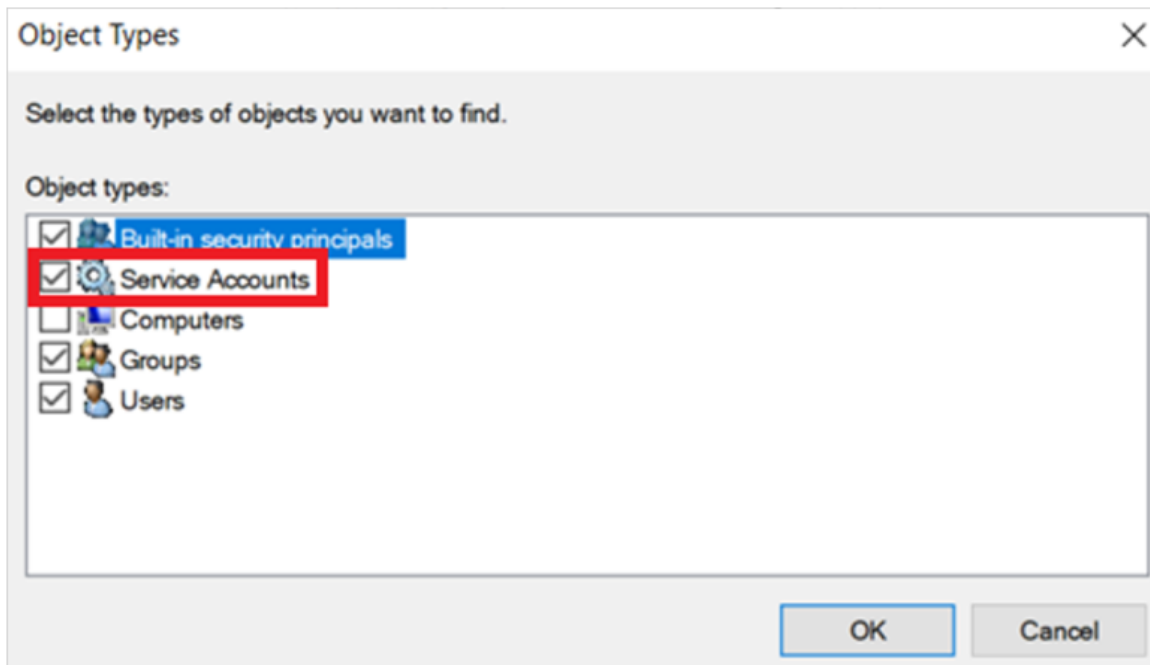
Applies to: This object and all descendant objects

Permissions:

<input type="checkbox"/> Full control	<input type="checkbox"/> Delete msImaging-PSPs objects
<input checked="" type="checkbox"/> List contents	<input type="checkbox"/> Create MSMQ Queue Alias objects
<input checked="" type="checkbox"/> Read all properties	<input type="checkbox"/> Delete MSMQ Queue Alias objects
<input type="checkbox"/> Write all properties	<input type="checkbox"/> Create msPKI-Key-Recovery-Agent objects
<input type="checkbox"/> Delete	<input type="checkbox"/> Delete msPKI-Key-Recovery-Agent objects
<input type="checkbox"/> Delete subtree	<input type="checkbox"/> Create msSFU30MailAliases objects
<input checked="" type="checkbox"/> Read permissions	<input type="checkbox"/> Delete msSFU30MailAliases objects
<input type="checkbox"/> Modify permissions	<input type="checkbox"/> Create msSFU30NetId objects
<input type="checkbox"/> Modify owner	<input type="checkbox"/> Delete msSFU30NetId objects
<input type="checkbox"/> All validated writes	<input type="checkbox"/> Create msSFU30NetworkUser objects
<input type="checkbox"/> All extended rights	<input type="checkbox"/> Delete msSFU30NetworkUser objects
<input type="checkbox"/> Create all child objects	<input type="checkbox"/> Create msTPM-InformationObjectsContainer objects
<input type="checkbox"/> Delete all child objects	<input type="checkbox"/> Delete msTPM-InformationObjectsContainer objects
<input type="checkbox"/> Create Computer objects	<input type="checkbox"/> Create nisMap objects
<input type="checkbox"/> Delete Computer objects	<input type="checkbox"/> Delete nisMap objects
<input type="checkbox"/> Create Contact objects	<input type="checkbox"/> Create nisNetgroup objects

OK Cancel

9. Make sure **Service Accounts** is marked in **Object Types**.



10. Enter the name of the gMSA account in the **Enter the object name to select** box and select **OK**.
11. Select **Descendant User objects** in the **Applies to** field, leave the existing settings, and add the following permissions and properties:

Permission Entry for wdgexp

Principal:  [Select a principal](#)

Type:

Applies to:

Permissions:

<input type="checkbox"/> Full control	<input type="checkbox"/> Create all child objects
<input checked="" type="checkbox"/> List contents	<input type="checkbox"/> Delete all child objects
<input checked="" type="checkbox"/> Read all properties	<input type="checkbox"/> Create ms-net-ieee-80211-GroupPolicy objects
<input type="checkbox"/> Write all properties	<input type="checkbox"/> Delete ms-net-ieee-80211-GroupPolicy objects
<input type="checkbox"/> Delete	<input type="checkbox"/> Create ms-net-ieee-8023-GroupPolicy objects
<input type="checkbox"/> Delete subtree	<input type="checkbox"/> Delete ms-net-ieee-8023-GroupPolicy objects
<input checked="" type="checkbox"/> Read permissions	<input type="checkbox"/> Allowed to authenticate
<input type="checkbox"/> Modify permissions	<input type="checkbox"/> Change password
<input type="checkbox"/> Modify owner	<input type="checkbox"/> Receive as
<input type="checkbox"/> All validated writes	<input type="checkbox"/> Reset password
<input type="checkbox"/> All extended rights	<input type="checkbox"/> Send as

Properties:

<input checked="" type="checkbox"/> Read all properties	<input checked="" type="checkbox"/> Read msDS-OperationsForAzTaskBL
<input type="checkbox"/> Write all properties	<input checked="" type="checkbox"/> Read msDS-parentdistname

OK Cancel

Permissions to enable force password reset:

- **Reset password**

Properties:

- **Read pwdLastSet**
- **Write pwdLastSet**

Properties to disable user:

- **Read userAccountControl**
- **Write userAccountControl**

12. Select **Descendant Group objects** in the **Applies to** field and set the following properties:

- **Read members**
- **Write members**

13. Select **OK**.

#### Step 4: Add the gMSA account in the Microsoft 365 Defender portal

1. Go to the [Microsoft 365 Defender portal](#).
2. Go to **Settings** and then **Identities**.
3. Under **Microsoft Defender for Identity**, select **Manage action accounts**.
4. Select **+ Create new account** to add your gMSA account.
5. Provide the account name and domain, and select **Save**.
6. Your action account will be listed on the **Manage action accounts** page.

### Microsoft Defender for Identity

**General**

- Sensors
- Directory services accounts
- Manage action accounts**
- VPN

**Entity tags**

- Sensitive

This list contains directory service accounts which sensors can use to perform actions on-premises Active Directory users

Filter

Domain: **Any** Group managed service account: **Any**

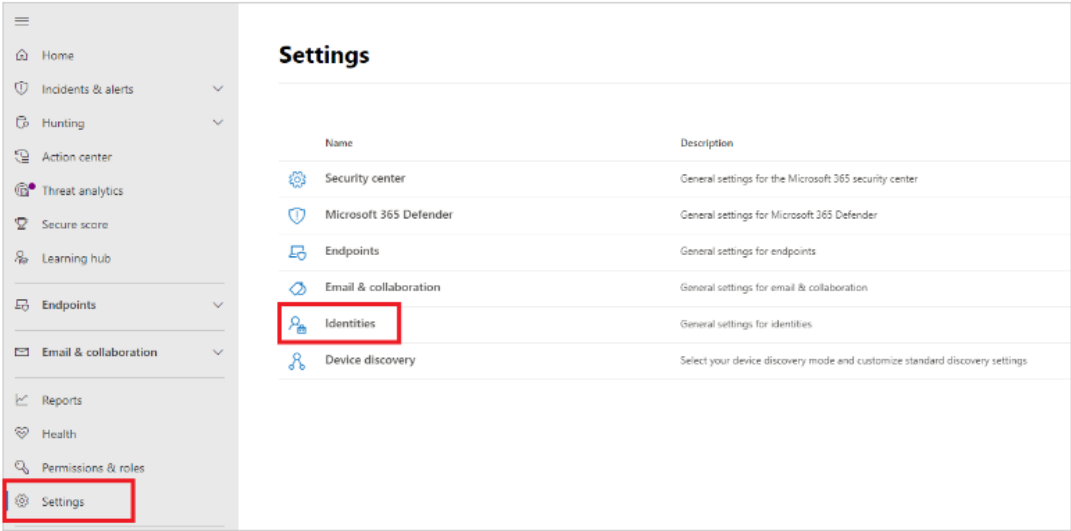
⌵ Export **+ Create new account**

Account	Domain	Group managed service account ⓘ
gMSAMDI	domain1.test.local	True

Step 5: View and configure sensor settings

After the MDI sensor is installed, do the following to view and configure MDI sensor settings.

- 1. In [Microsoft 365 Defender](#), go to **Settings** and then **Identities**.





- Sensor name
- Domain membership
- Version number
- If updates should be delayed
- Service status
- Sensor status
- Health status
- The number of health issues
- When the sensor was created

Microsoft Defender for Identity

General

Sensors

Directory services accounts

Management action accounts

VPN

Health issues

Portal redirection

About

Deploying sensors enables you to monitor your on-premises Active Directory environment for suspicious activities and risky configurations. [Learn more](#)

Filter

Type: Any

Domain: Any

Delayed update: Any

Service status: Any

Sensor status: Any

Health status: Any

Export

Add sensor

7 items

Customize columns

Search

Sensor	Type	Example	Service status	Sensor status	Version	Delayed update	Health status	Health issues	Created
<input type="checkbox"/> DC2	Domain controller Sensor	domain1-test.local	Running	Up to date	1.185.1024.878	Enabled	<span>Healthy</span>	0	Sat 21, 2023 5:08 PM
<input type="checkbox"/> STANDALONE	Standalone Sensor	domain1-test.local	Running	Up to date	2.184.1045.4207	Enabled	<span>Healthy</span>	0	Mon 6, 2022 3:22 PM
<input type="checkbox"/> DC4	Domain controller Sensor	domain1-test.local	Running	Up to date	1.185.1024.878	Enabled	<span>Healthy</span>	0	Sat 21, 2023 5:07 PM

- If you select **Filters**, you can choose which filters will be available. Then with each filter, you can choose which sensors to display.

The screenshot shows the 'Sensors' page in the Microsoft Defender for Identity console. On the left is a sidebar with navigation links: Sensors, Directory services accounts, Spring notifications, Service logs, Exchange server logs, Home mailbox logs, MFA, Health issues notifications, and Alert notifications. The main area has a header 'Sensors enable monitoring your on-premises Active Directory environment for suspicious activities and policy configurations. Learn more.' Below this are buttons for 'Export', '+ Add sensor', and 'Delete'. A 'Filter' dropdown is set to 'Focus', and a 'Filters' button is visible. Below the filters are tabs for 'Domains: Any', 'Delayed updates: Any', 'Service Status: Any', 'Update status: Any', and 'Health status: Any'. A table lists two sensors:

Sensor	Domain	Version	Delayed updates	Service Status	Update status	Health status	Health issues
Samscoops Dc	Samscoops.Azure	2.145.14125.1048	Disabled	Running	Up to date	Healthy	0
SDDC-DC-Play	SamscoopsPlay.Azure	2.145.14125.1048	Disabled	Running	Up to date	Healthy	0

On the right, a 'Filters' sidebar allows customizing the filter. It includes checkboxes for 'Created', 'Domains', 'Version', 'Delayed updates', 'Service Status', 'Update status', and 'Health status'. A 'Done' button is at the bottom.


- If you select one of the sensors, a pane will display with information about the sensor and its health status.

The screenshot shows the detailed view for the 'Samscoops Dc' sensor. The left sidebar is the same as in the previous screenshot. The main area has the same header and buttons. The 'Filter' dropdown is now set to 'Filters'. The tabs for filters are the same. The table below shows the sensor details:

Sensor	Domain	Version	Delayed updates	Service Status	Update status	Health status	Health issues
Samscoops Dc	Samscoops.Azure	2.145.14125.1048	Disabled	Running	Up to date	Healthy	0
SDDC-DC-Play	SamscoopsPlay.Azure	2.145.14125.1048	Disabled	Running	Up to date	Healthy	0

On the right, a pane titled 'Samscoops Dc' shows the sensor's health status as 'Healthy'. It includes sections for 'Sensor details' (Created: Jun 2, 2020 8:51 PM, Running), 'Console' (Version: 2.145.14125.1048, Console: Console.Azure), 'Update status' (Up to date, Delayed updates: Disabled), and 'Health issues' (Clean [0]). Below this is a table of 'Clean [0]' items, showing 'Sensor reached a memory resource limit' with a severity of 'High' and a timestamp of 'May 11, 2021 1:27 PM'.

5. If you select **Manage sensor**, a pane will open where you can configure the sensor details.



## SamscoopsDc

● Healthy

---

**Sensor details**

**Service status**  
Running

**Domain**  
Contoso.Azure

**Update status**  
Up to date

**Created**  
Jun 2, 2020 8:31 PM

**Version**  
2.149.14128.13549

**Delayed update**  
Disabled

---

**Health issues**

×

# SamscoopsDc settings

Configure sensor details

Description

Enter description

Domain controller (FQDN)

SamscoopsDc.Samscoops.Azure

Capture network adapters

☒ Ethernet

6. On the **Sensors** page, you can export your list of sensors to a .csv file by selecting **Export**.

The screenshot shows the Microsoft Defender for Identity console. At the top, a 'Downloads' bar contains a button labeled 'Sensors.csv' with a download icon, which is highlighted by a red rectangle. Below this, the 'Sensors' page is displayed. On the left, a sidebar menu includes 'General' (with 'Sensors' selected), 'Directory services accounts', 'Manage action accounts', 'VPN', 'Entity tags' (with 'Sensitive', 'Honeytoken', and 'Exchange server'), and 'Excluded entities'. The main content area has a heading 'Deploying sensors enables you to monitor your on-premises Active Directory environment for suspicious activities and risky configurations. [Learn more](#)'. Below this is a 'Filter' section with dropdowns for 'Type: Any', 'Domain: Any', 'Delayed update: Any', 'Service status: Any', 'Update status: Any', and 'Health status: Any'. A red box highlights the 'Export' button (with a download icon) and the '+ Add sensor' button. To the right of the buttons, it says '4 items' and 'Customize columns'. A search bar is also present. Below the filters is a table with the following data:

Sensor	Type	Domain	Version	Delayed update	Service status
MSC-ADFS1	AD FS Sensor	domain1.test.local	2.177.15156.22652	Disabled	Running
DC5	Domain controller Sensor	domain2.test.local	2.177.15156.22652	Disabled	Running
DC1	Domain controller Sensor	domain1.test.local	2.177.15156.22652	Disabled	Running
STANDALONE	Standalone Sensor	domain1.test.local	2.177.15156.22652	Disabled	Running