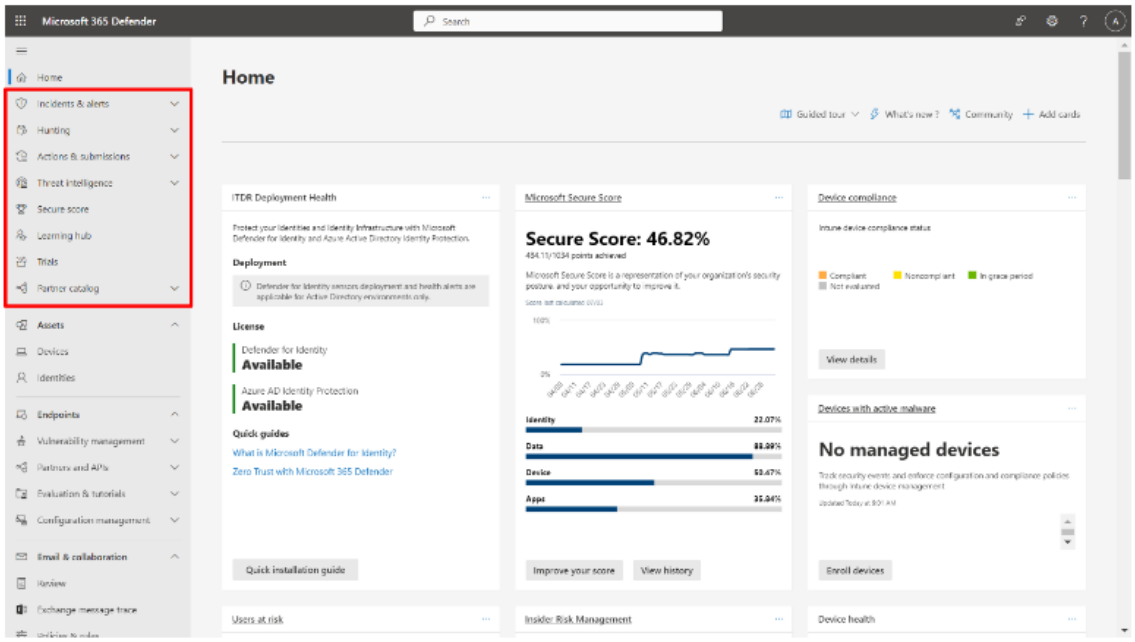
Sign in

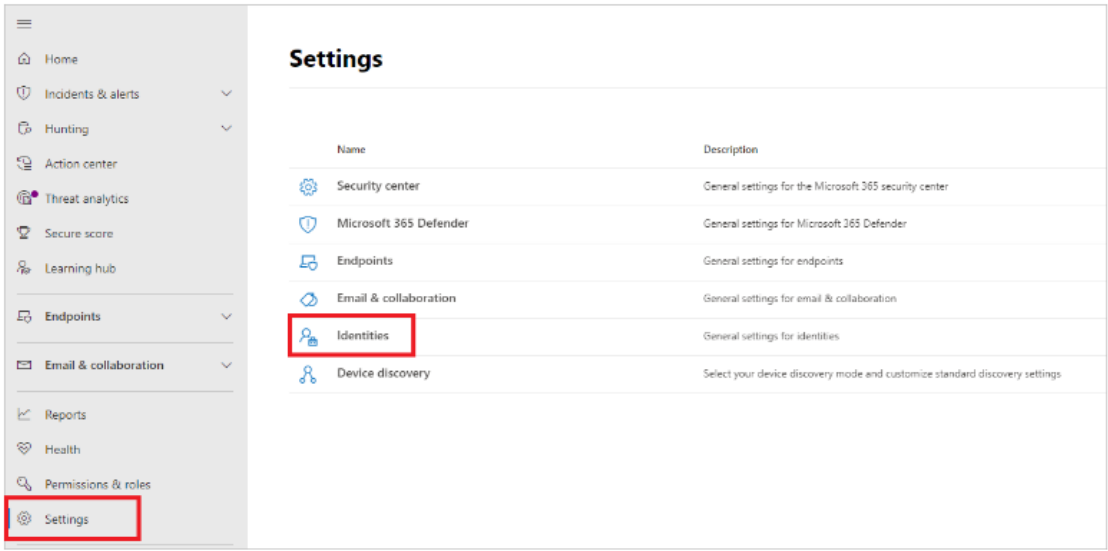
To begin the deployment, sign in to the Microsoft 365 Defender portal. From the navigation menu, select any item, such as **Incidents & alerts**, **Hunting**, **Actions & submissions**, or **Threat intelligence** to initiate the onboarding process.



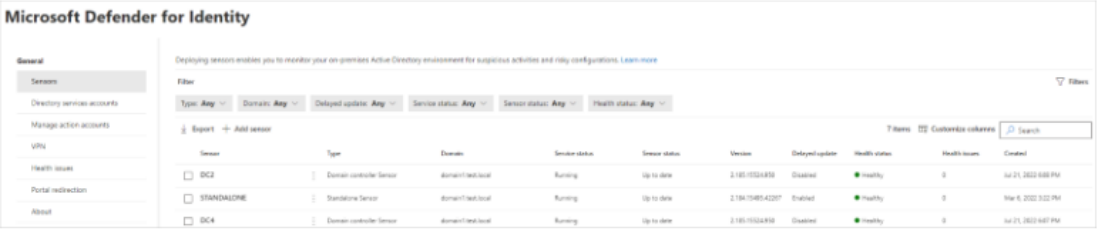
You'll then get the option to deploy supported services, including MDI. When you go to the MDI settings, the required cloud components will be auto-provisioned.

Step 1: Download the Microsoft Defender for Identity sensor

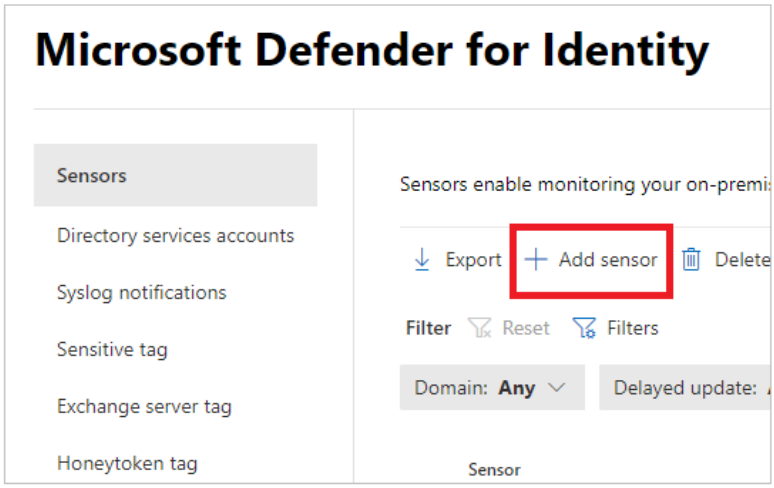
1. In the portal, go to **Settings** and then **Identities**.



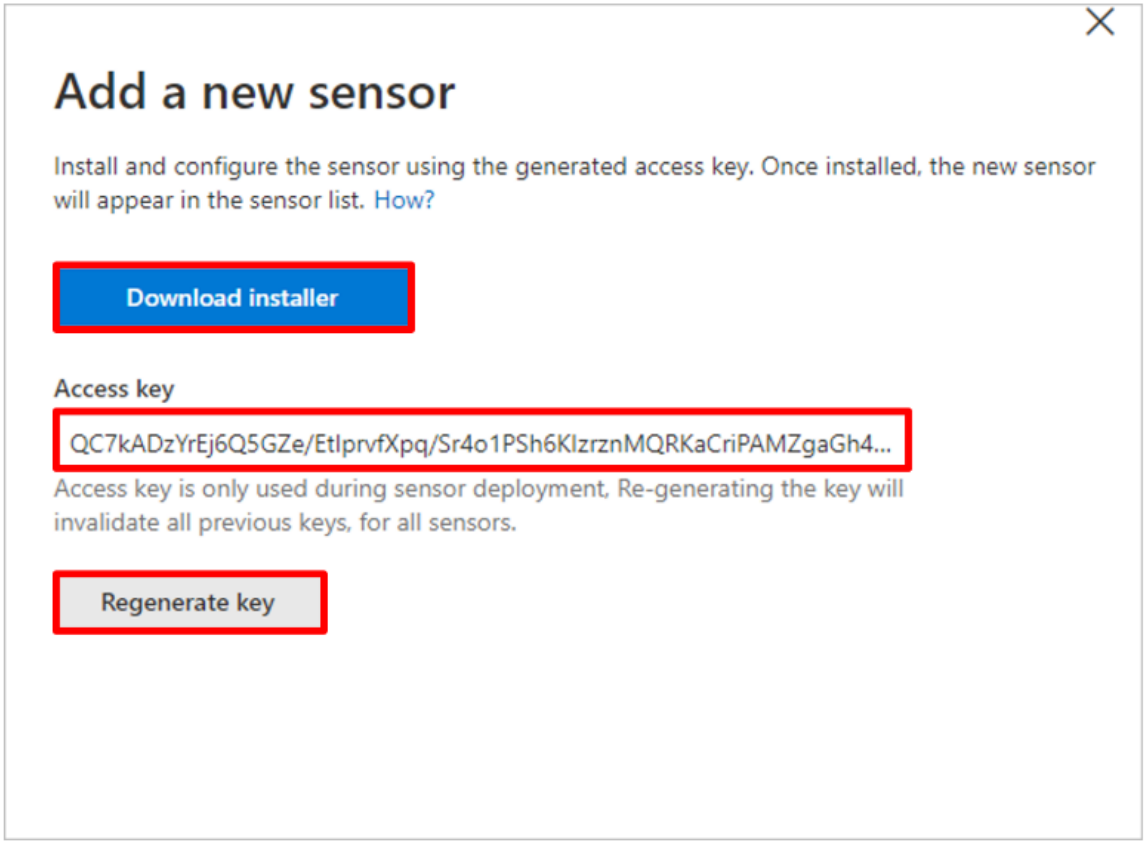
2. Select the **Sensors** page, which displays all of your MDI sensors.



3. Select **Add sensor**.



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

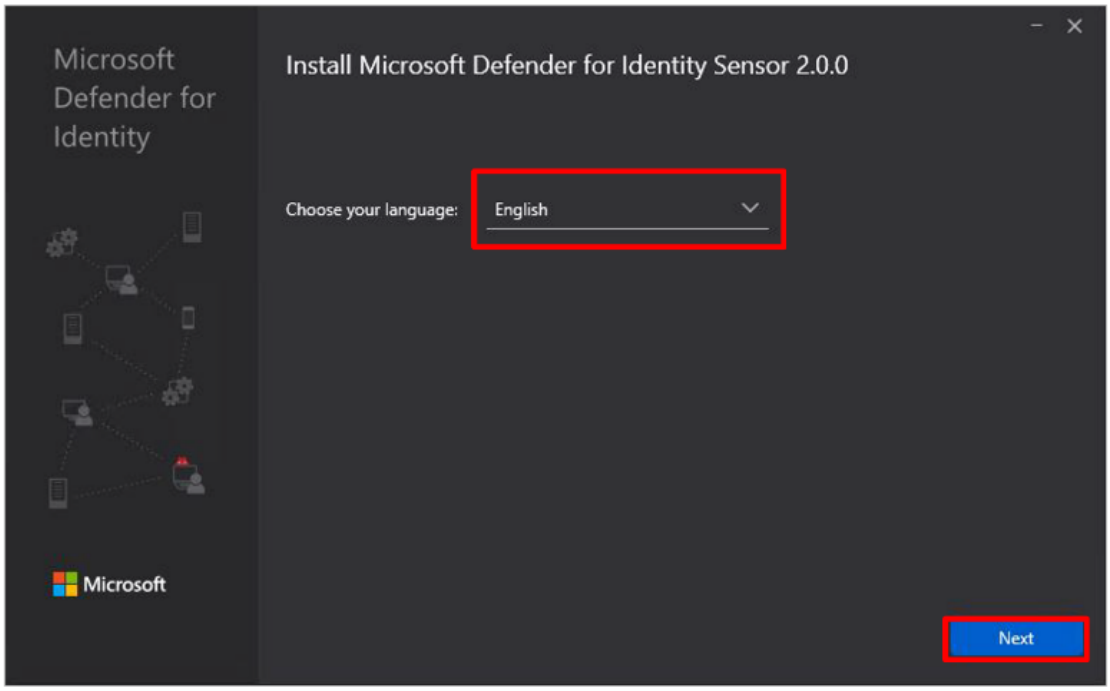
7. Use the **Regenerate key** button if you ever need to regenerate the new access key. It won't affect any previously deployed sensors because it's only used for initial registration of the sensor.

8. Next, copy the package to the dedicated server or domain controller onto which you're installing the MDI sensor.

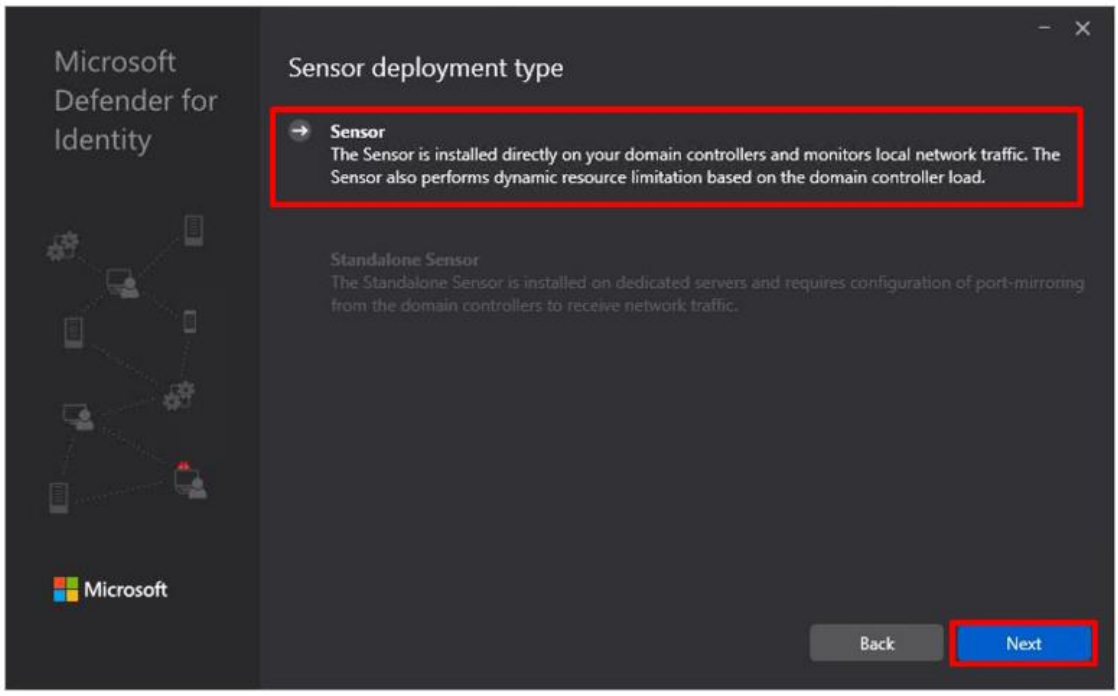
Step 2: Install the Microsoft Defender for Identity sensor

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

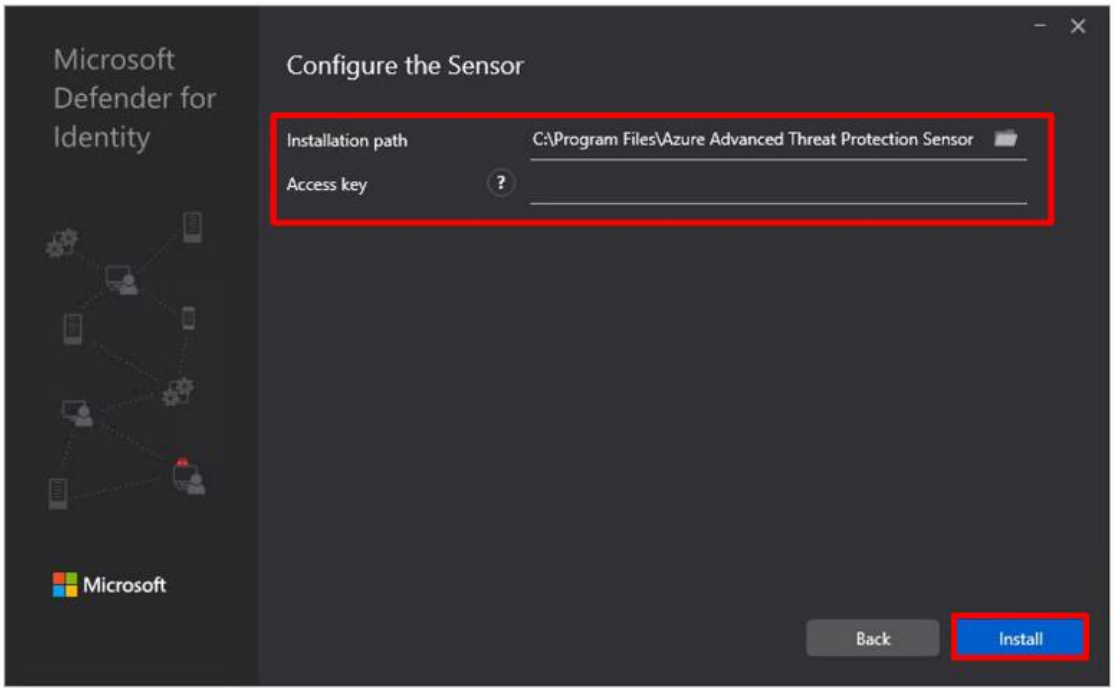
1. Verify that the machine has connectivity to the relevant MDI cloud service endpoints.
2. Extract the installation files from the zip file. Take note that installing directly from the zip file will fail.
3. Run *Azure ATP sensor setup.exe* with elevated privileges with other words, run as administrator 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.



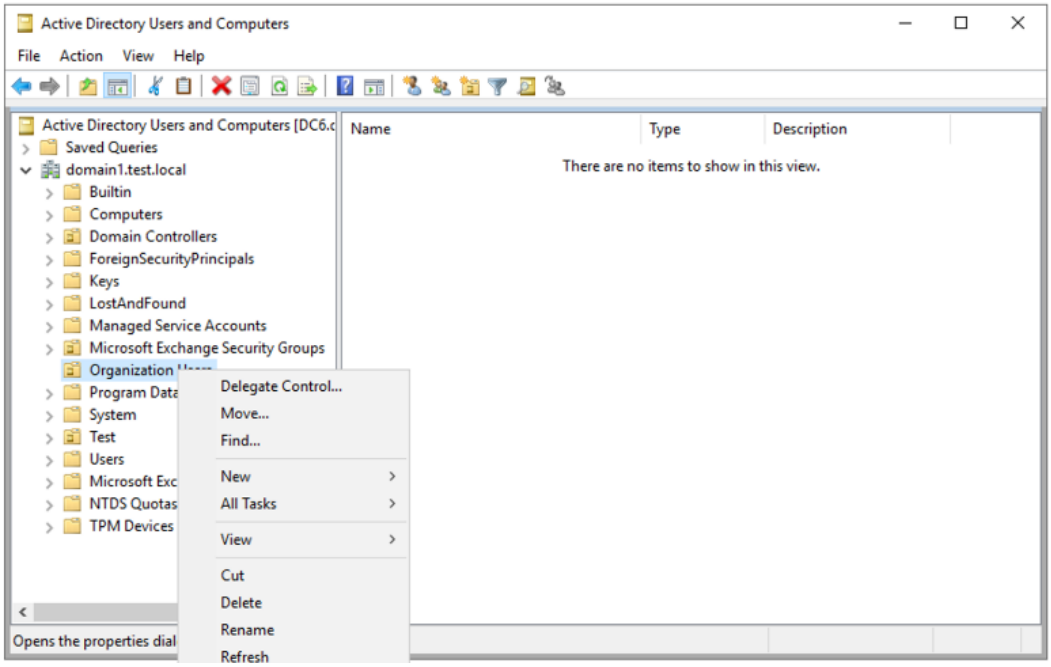
6. Under **Configure the sensor**, enter the installation path and the access key that you copied from the previous step, based on your environment. The installation path is the location where the MDI sensor is installed. By default the path is **%programfiles%\Azure Advanced Threat Protection sensor**.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

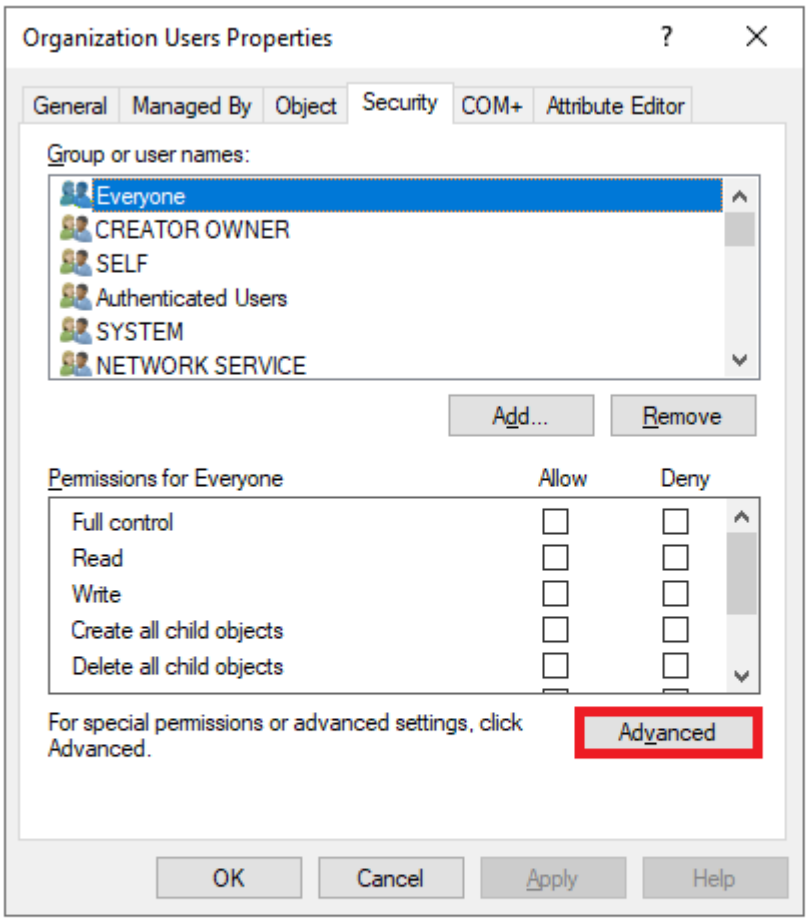


Step 3: Manage Action accounts

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**.

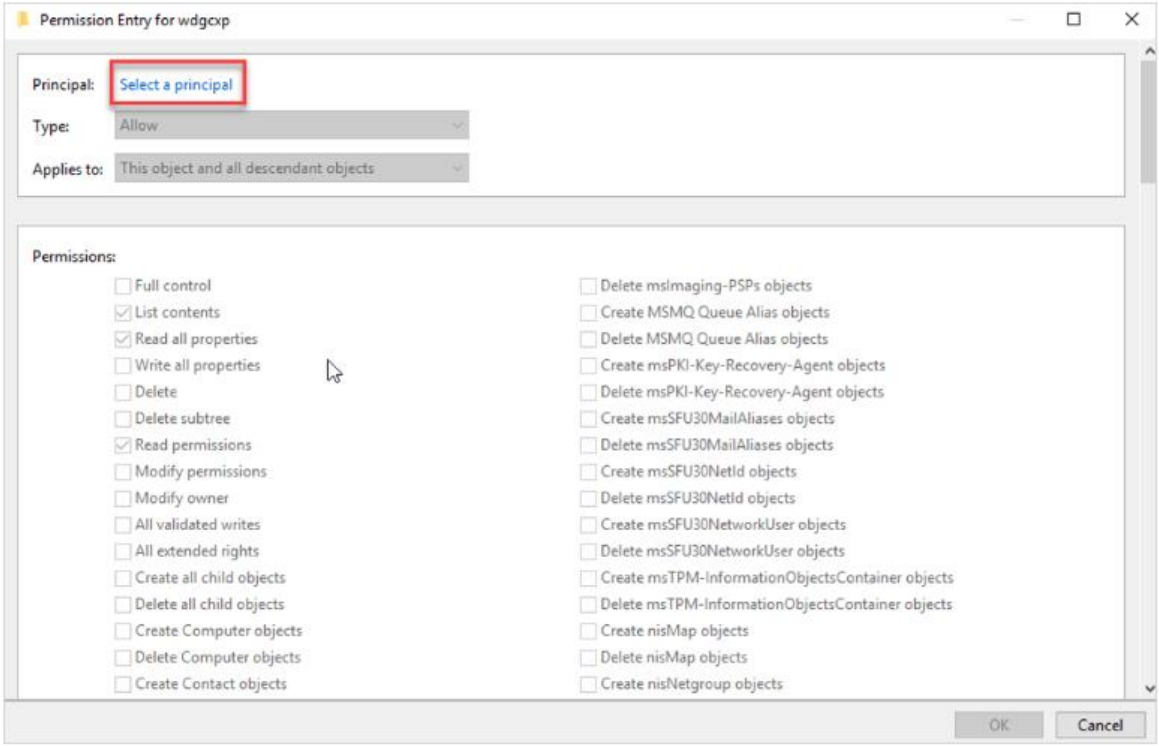




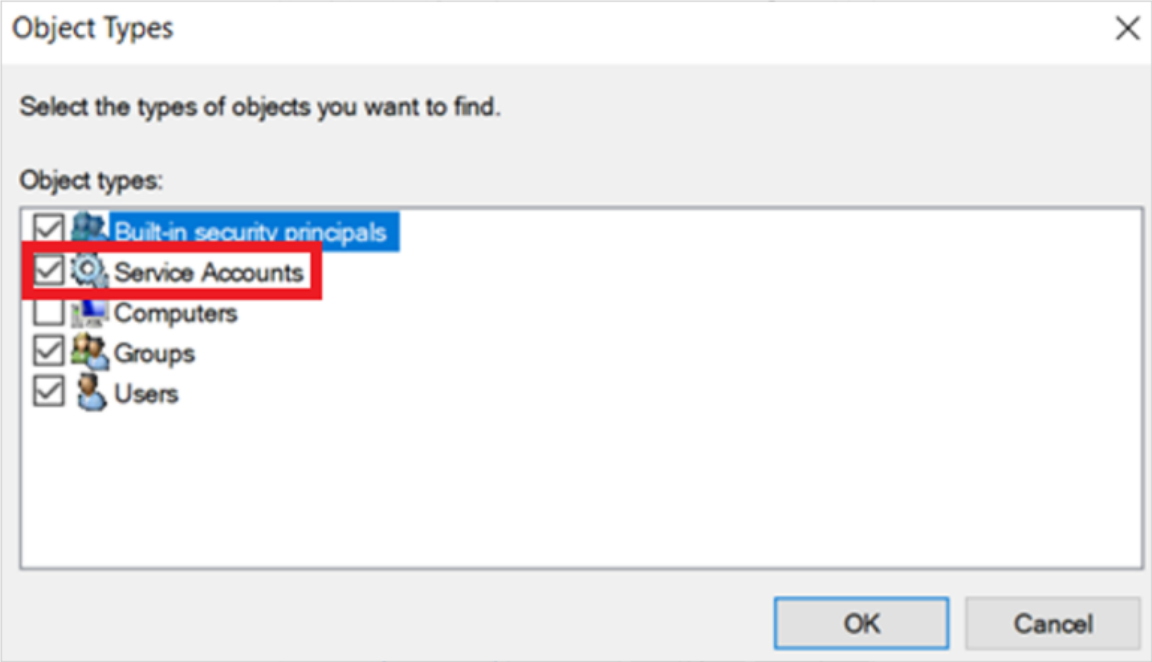
6. Go the **Security** tab and select **Advanced**.

7. Select **Add**.

8. Choose **Select principal.**

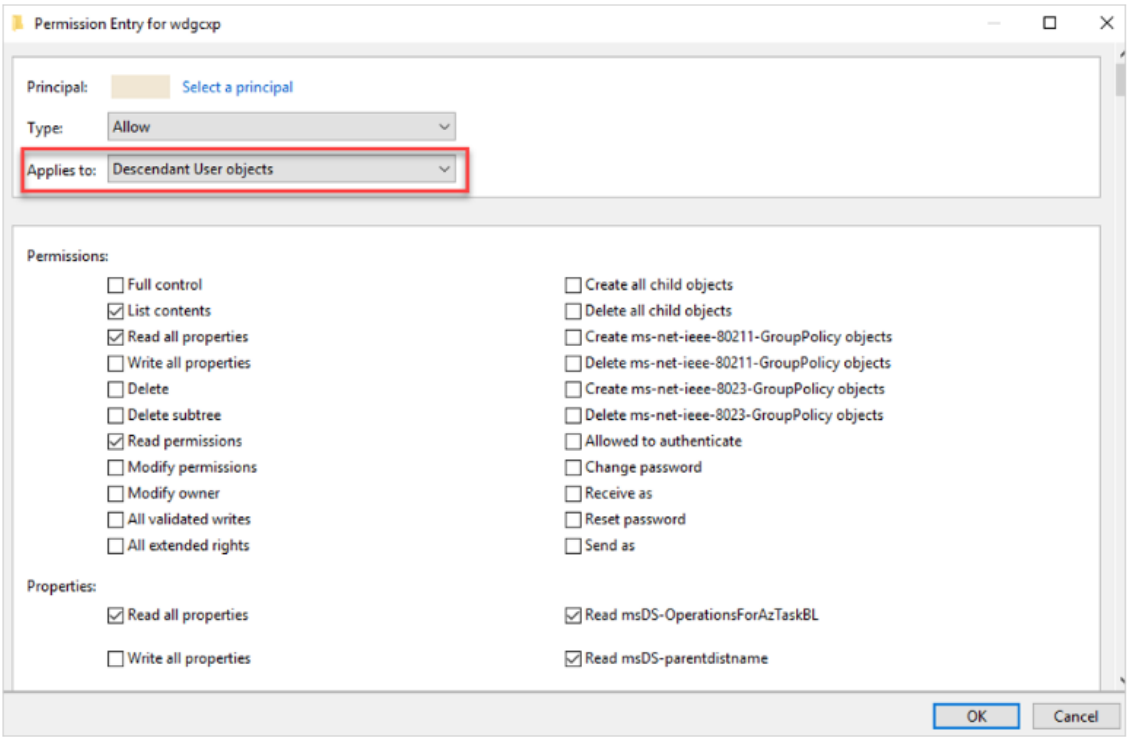

Permission Entry for wdgcxp
Principal:
Select a principal
Type:
Allow
Applies to:
This object and all descendant objects
Permissions:
Full control
List contents
Read all properties
Write all properties
Delete
Delete subtree
Read permissions
Modify permissions
Modify owner
All validated writes
All extended rights
Create all child objects
Delete all child objects
Create Computer objects
Delete Computer objects
Create Contact objects
Delete msImaging-PSPs objects
Create MSMQ Queue Alias objects
Delete MSMQ Queue Alias objects
Create msPKI-Key-Recovery-Agent objects
Delete msPKI-Key-Recovery-Agent objects
Create msSFU30MailAliases objects
Delete msSFU30MailAliases objects
Create msSFU30NetId objects
Delete msSFU30NetId objects
Create msSFU30NetworkUser objects
Delete msSFU30NetworkUser objects
Create msTPM-InformationObjectsContainer objects
Delete msTPM-InformationObjectsContainer objects
Create nisMap objects
Delete nisMap objects
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:



Permissions to enable force password reset:

- **Reset password**

Properties:

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

Properties to disable user:

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

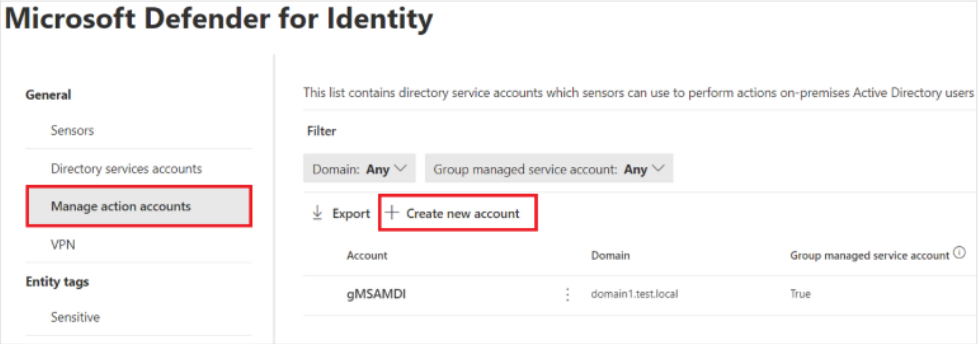
12. Select **Descendant Group objects** in the **Applies to** field and set the following properties:

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

13. Select **OK**.

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

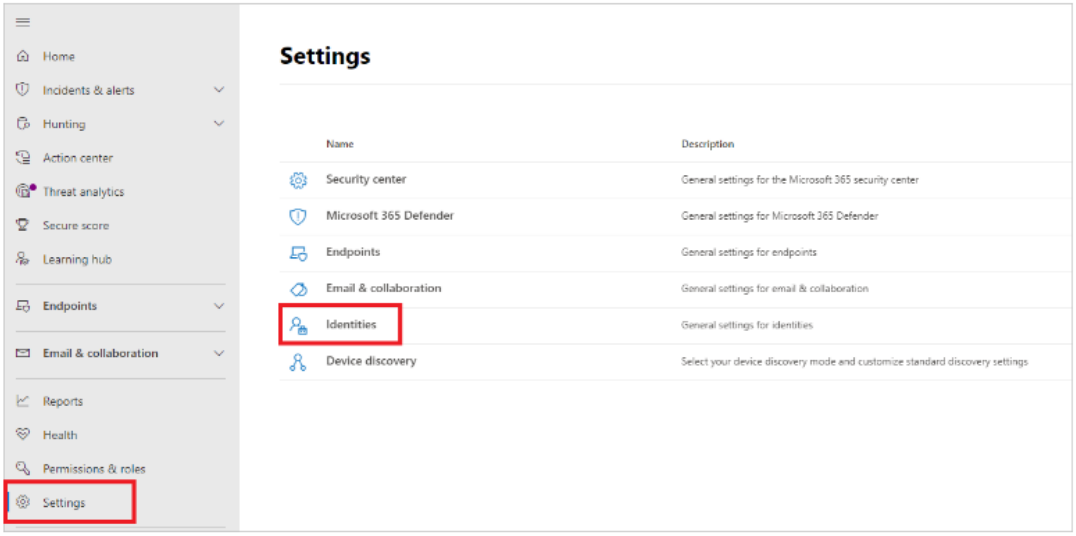
1. Go to the Microsoft 365 Defender portal.
2. Go to **Settings** and then **Identities**.
3. Under **Microsoft Defender for Identity**, select **Manage action accounts**.
4. Select **+ Create new account** to add your gMSA account.
5. Provide the account name and domain, and select **Save**.
6. Your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



Step 5: View and configure sensor settings

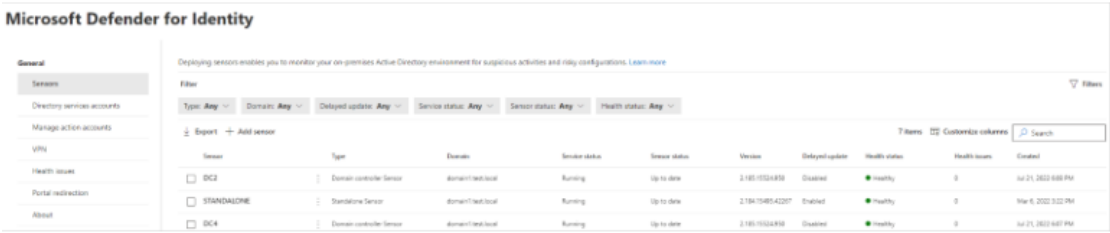
After the MDI sensor is installed, do the following to view and configure MDI sensor settings.

1. In Microsoft 365 Defender, go to **Settings** and then **Identities**.

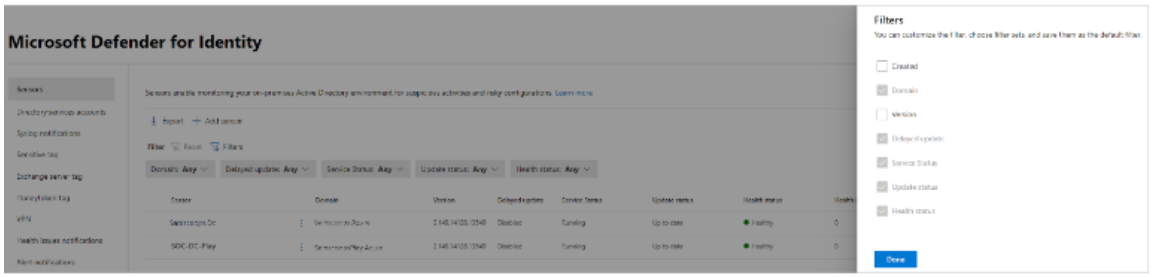


2. Select the **Sensors** page, which displays all your MDI sensors. For each sensor, it will list:

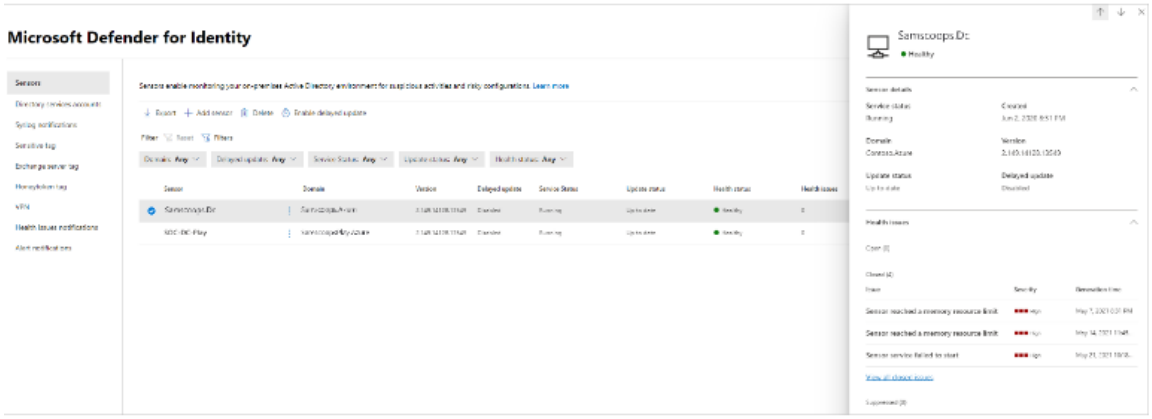
- Sensor name
- Domain membership
- Version number
- If updates should be delayed
- Service status
- Sensor status
- Health status
- The number of health issues
- When the sensor was created



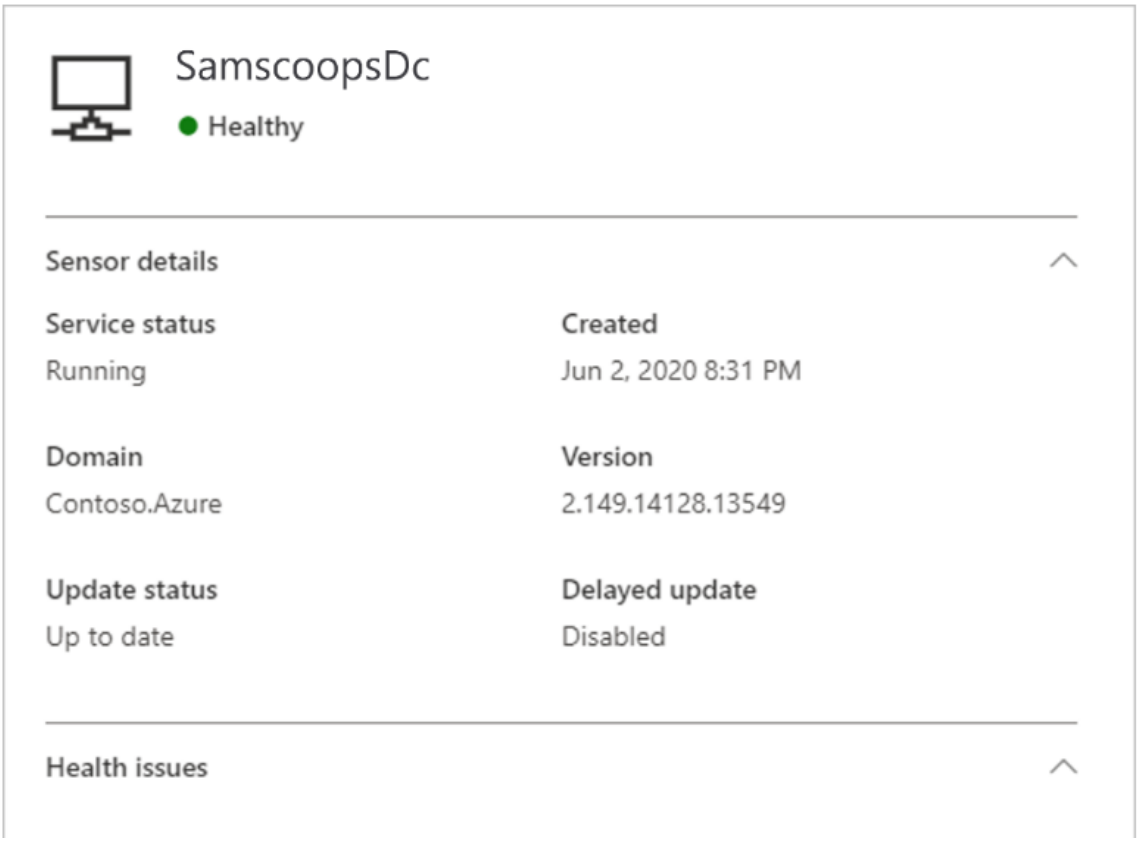
3. If you select **Filters**, you can choose which filters will be available. Then with each filter, you can choose which sensors to display.

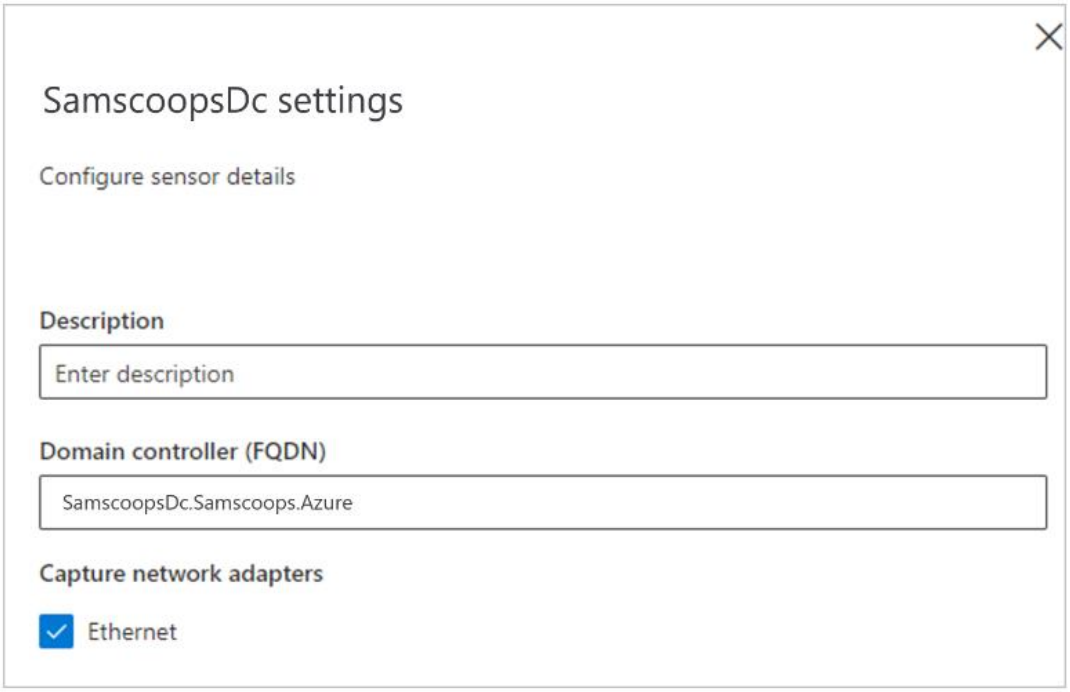


4. If you select one of the sensors, a pane will display with information about the sensor and its health status.



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




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**.