Microsoft

Ready to deploy
Microsoft Defender for Identity?

Use this guide to help you meet the pre-requisites to successfully deploy Defender for Identity!

Server requirements

- ✔ Domain controllers – Windows Server 2008 R2 and above
- ✔ Active Directory Federated Services – Windows Server 2016 and above
- ✔ Memory – 6 GB (sensor minimum requirement)
- ✔ CPU – 2 cores (sensor minimum requirement)
- ✔ 5 GB free disk space (10 GB recommended)
- ✔ .NET Framework 4.7 or later
- ✔ Set power option on domain controller to high performance

NOTE: For virtual machines, dynamic memory and any other memory ballooning should be disabled

Verify network settings

- ✔ Sensor to MDI Service – SSL 443 (outbound only). See the following guidance on ports for how to limit the connectivity to only the MDI service.*
- ✔ Network Name Resolution – 135, 137, 3389 (from the sensor to all devices on the network)**
- ✔ Lateral Movement Paths – 445 (from the sensor to all the devices on the network)

* *Required for the successful deployment of the sensor*

** *If these ports are not opened, this can cause an increase in the number of false positive alerts*

Create a directory service account

- ✔ Group managed service account (recommended for Windows Server 2012 and above)
- ✔ Standard Active Directory account

Note: Accounts need read only access to all Active Directory objects (including deleted objects container)

Windows events

- ✔ Domain controller – 4726, 4728 – 4730, 4732, 4733, 4743, 4753, 4756, 4757, 4758, 4763, 4776, 7045, 8004
- ✔ Active Directory Federated Services – 1202, 1203, 4624, 4625

NOTE: All listed events should be enabled in order to gain the maximum level of protection from the product
To learn more about Windows events, click here

Ready to deploy!

Congratulations! You have completed the initial pre-requisites.
Head over to our QuickStart Guide to enable your Defender for Identity instance and deploy the sensors.