Microsoft Defender for Identity

Deployment Guide

# Pre-requisites

* **Networking**
  + Internet - Sensors should reach \*.atp.azure.com on outbound TCP 443
  + Intranet – Network name resolution to domain members to correlate between raw activities (containing IP addresses), and the relevant computers involved in each activity
    - NTLM over RPC: TCP Port 135 is open for inbound communication from Defender for Identity Sensors, on all computers in the environment.
    - NetBIOS: UDP Port 137 is open for inbound communication from Defender for Identity Sensors, on all computers in the environment.
    - RDP: TCP Port 3389 is open for inbound communication from Defender for Identity Sensors, on all computers in the environment.
    - Reverse DNS: UDP Port 53 so sensor can reach the DNS server and that Reverse Lookup Zones are enabled.
  + Ports (DC sensor): [Ports for DC sensors](https://learn.microsoft.com/en-us/defender-for-identity/prerequisites#ports)
  + Ports (Standalone sensor): [Ports for standalone sensors](https://learn.microsoft.com/en-us/defender-for-identity/prerequisites#ports-for-standalone-sensors)
* **Operating System**
  + DC sensor – 2012+ (incl. RODC)
    - KB 3047154 (for Windows Server 2012 R2 only but ***not*** on virtualization ***host*** or port mirroring will not work)
  + AD FS sensor – 2016+ (2019 requires KB4487044 or new)
* **.Net Framework** - .NET Framework 4.7+
* **Hardware**
  + Minimum - 2 cores / 6 GB RAM / 6-10 GB disk space
  + High Perf Power Option
  + No dynamic memory for VMs
  + Use Ncap driver instead of WinPcap (NIC teaming + WinPcap will result in error)
    - MDI 2.184+ installs Npcap 1.0 OEM
* **Auditing**
  + Advanced audit policy
  + NTLM auditing (group policy)
  + AD FS verbose logging
  + Active directory object auditing
* **Accounts**
  + Service account - Sensor service runs as LocalService.
  + DSA – local service account, user account or gMSA used to query DC, tracking changes, SAM-R calls to devices
  + Action Accounts - remediation actions targeting on-premises Active Directory accounts in the event that an identity is compromised.
* **Active Directory permissions**
  + SAM-R permissions on all domain members assigned to MDI DSA (in addition to Built-in\Administrators) used to identify local admins on specific machines.
* **Standalone sensor specific**
  + Port mirroring
  + NICs
    - Management - (query DC, clients) static IP, gateway / preferred and alternate DNS servers / DNS suffix for this connection (if workgroup)
    - Capture – (mirroring) static non-routable IP address (with /32 mask) / no default sensor gateway / no DNS server addresses.
  + Forwarding of windows event logs from DCs or from SIEM - 4662, 4726, 4728, 4729, 4730, 4732, 4733, 4741, 4743, 4753, 4756, 4757, 4758, 4763, 4776, 5136, 7045

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 on all your domain controllers.

# Deployment

## Capacity planning

1. Dowload tool from [Defender for Identity Sizing Tool](https://aka.ms/mdi/sizingtool).
2. Run the Defender for Identity Sizing Tool, **TriSizingTool.exe**, from the zip file you downloaded.
3. When the tool finishes running, open the Excel file results.
4. In the Excel file, locate and select the **Azure ATP Summary** sheet. The other sheet isn't needed since it's for ATA planning.
5. Locate the **Busy Packets/sec** field in the Azure ATP sensor table in the results Excel file and make a note of it.
6. Match your **Busy Packets/sec** field to the **PACKETS PER SECOND** field in the table below. Use the fields to determine the memory and CPU *that will be used by the sensor*.

|  |  |  |
| --- | --- | --- |
| **Packets per second** | **CPU (cores)\*** | **Memory\*\* (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 |

A minimum of 2 cores is required.

A minimum of 6 GB of hard drive space is required, 10 GB is recommended, including space needed for the Defender for Identity binaries and logs.

Details at [Use the sizing tool](https://learn.microsoft.com/en-us/defender-for-identity/capacity-planning#use-the-sizing-tool)

## Server Configuration

* A minimum of 2 cores is required.
* A minimum of 6 GB of hard drive space is required, 10 GB is recommended, including space needed for the Defender for Identity binaries and logs.
* It's recommended that you don't work with hyper-threaded cores. Working with hyper-threaded cores can result in Defender for Identity sensor health issues.
* Set the Power Option of the Defender for Identity sensor to High Performance.
* Dynamic memory
  + **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 following option in the VM setting – **Reserve all guest memory (All locked)**.
  + **Other virtualization host** - Refer to the vendor supplied documentation on how to ensure that memory is fully allocated to the VM at all times.

## Configure audit policies

1. [Advanced audit policy on domain controllers](https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#configure-audit-policies):

|  |  |  |
| --- | --- | --- |
| **Audit policy** | **Subcategory** | **Triggers event IDs** |
| Account Logon | Audit Credential Validation | 4776 |
| Account Management | Audit Computer Account Management | 4741, 4743 |
| Audit Distribution Group Management | 4753, 4763 |
| Audit Security Group Management | 4728, 4729, 4730, 4732, 4733, 4756, 4757, 4758 |
| Audit User Account Management | 4726 |
| DS Access | Audit Directory Service Access | 4662 |
| Audit Directory Service Changes | 5136 |
| System | Audit Security System Extension | 7045 |

1. [NTLM Auditing on domain controllers](https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#event-id-8004):

* 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

1. [Set AD FS auditing level to Verbose](https://learn.microsoft.com/en-us/defender-for-identity/active-directory-federation-services#ad-fs-windows-event-logs):

Set-AdfsProperties -AuditLevel Verbose

## Active Directory object auditing

1. [Set System ACL at domain root for](https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#configure-object-auditing):
   * Descendant User Objects
   * Descendant Group Objects
   * Descendant Computer Objects
   * Descendant msDS-GroupManagedServiceAccount Objects
   * Descendant msDS-ManagedServiceAccount Objects
2. [Enable auditing on ADFS object](https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#enable-auditing-on-an-adfs-object).
3. [Enable auditing on Exchange object](https://learn.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection#enable-auditing-on-an-exchange-object).

## Standalone sensor Configuration

[Network adapters for standalone sensors](https://learn.microsoft.com/en-us/defender-for-identity/prerequisites#network-adapters-for-standalone-sensors)

[Configure event forwarding](https://learn.microsoft.com/en-us/defender-for-identity/configure-event-forwarding)

[Port mirroring](https://learn.microsoft.com/en-us/defender-for-identity/configure-port-mirroring)

## MDI Directory Service Account (gMSA)

For details see [Directory Service account recommendations](https://learn.microsoft.com/en-us/defender-for-identity/directory-service-accounts)

### Create and install DSA

1. Launch an elevated PowerShell console, and import the active directory module by running the command:

Import-Module ActiveDirectory

1. To create the KDS root key using the New-KdsRootKey cmdlet run the following command:

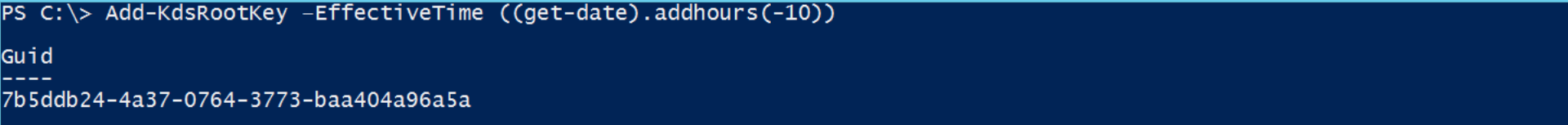
Add-KdsRootKey –EffectiveImmediately

The domain controllers will **wait up to 10 hours** from time of creation to allow all domain controllers to converge their AD replication before allowing the creation of a gMSA. The 10 hours is a safety measure to prevent password generation from occurring before all DCs in the environment can answer gMSA requests.

**For test environments alone**, you can create a KDS root key and set the start time in the past to avoid the interval wait for key generation by using the following command:

Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))

Validate that a 4004 event has been logged in the kds event log



Log Name: Microsoft-Windows-KdsSvc/Operational

Source: Microsoft-Windows-KdsSvc

Date: 5/29/2023 9:30:47 AM

Event ID: 4004

Task Category: None

Level: Information

Keywords:

User: SFS\PParker

Computer: SFSDC01.SFS.com

Description:

Group Key Distribution Service created the first master root key in AD. The key ID is b80f4c81-1fd3-2b2d-ecc6-7a02d99c73d8.

1. To create a gMSA using the New-ADServiceAccount cmdlet run the following command:

New-ADServiceAccount -Name *<MSA\_Name>* –DNSHostName *<dNSHostName\_of\_gMSA>* -PrincipalsAllowedToRetrieveManagedPassword *<security\_group>*

Where,

**DNSHostName** specifies the DNS host name of service, and

**PrincipalsAllowedToRetrieveManagedPassword** specifies the computer accounts of the member hosts or the security group that the member hosts are a member of

PS C:\> New-ADServiceAccount -Name svc\_mdi\_dsa\_sfs –DNSHostName svc\_mdi\_dsa\_sfs -PrincipalsAllowedToRetrieveManagedPassword "CN=Domain Controllers,CN=Users,DC=SFS,DC=com"

A screenshot of a computer

Description automatically generated

1. On each of the domain controllers, configure the gMSA by running the command:

Install-ADServiceAccount -Identity *<MSA\_Name>*

PS C:\> Install-ADServiceAccount -Identity "svc\_mdi\_dsa\_sfs"

This can also be run remotely using the command Invoke-Command -ComputerName COMPUTER -ScriptBlock { COMMAND }

1. Test the managed service account on each of the domain controllers by running the command:

Test-ADServiceAccount -Identity *<MSA\_Name>*

PS C:\> Test-ADServiceAccount -Identity "svc\_mdi\_dsa\_sfs"

True

This can also be run remotely using the command Invoke-Command -ComputerName COMPUTER -ScriptBlock { COMMAND }

### Grant DSA read permissions on 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

$mdiDSA = 'SFS\svc\_mdi\_dsa\_sfs$'

# 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', "$($mdiDSA):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', $mdiDSA)

# C:\Windows\System32\dsacls.exe $params

Owner: SFS\Domain Admins

Group: NT AUTHORITY\SYSTEM

Access list:

{This object is protected from inheriting permissions from the parent}

Allow BUILTIN\Administrators SPECIAL ACCESS

LIST CONTENTS

READ PROPERTY

Allow NT AUTHORITY\SYSTEM SPECIAL ACCESS

DELETE

READ PERMISSONS

WRITE PERMISSIONS

CHANGE OWNERSHIP

CREATE CHILD

DELETE CHILD

LIST CONTENTS

WRITE SELF

WRITE PROPERTY

READ PROPERTY

The command completed successfully

Owner: SFS\Domain Admins

Group: NT AUTHORITY\SYSTEM

Access list:

{This object is protected from inheriting permissions from the parent}

Allow SFS\svc\_mdi\_dsa\_sfs$ SPECIAL ACCESS

LIST CONTENTS

READ PROPERTY

Allow BUILTIN\Administrators SPECIAL ACCESS

LIST CONTENTS

READ PROPERTY

Allow NT AUTHORITY\SYSTEM SPECIAL ACCESS

DELETE

READ PERMISSONS

WRITE PERMISSIONS

CHANGE OWNERSHIP

CREATE CHILD

DELETE CHILD

LIST CONTENTS

WRITE SELF

WRITE PROPERTY

READ PROPERTY

The command completed successfully

PS C:\>

### Grant DSA Log on as a service right on DCs

For details see [Verify that the gMSA account has the required rights](https://learn.microsoft.com/en-us/defender-for-identity/directory-service-accounts#verify-that-the-gmsa-account-has-the-required-rights-if-needed)

If you use Group Policy to configure the **Log on as a service** setting, make sure you add both **NT Service\All Services** and the gMSA account you created.

A screenshot of a computer

Description automatically generated with medium confidence

### Grant DSA SAM-R permissions on domain members

Make sure to apply group policies to all computers **except domain controllers**.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

A picture containing text, screenshot, display, number

Description automatically generated

### Grant DSA Access this computer from the network right on domain members

The setting is not enabled by default. If you have not enabled it previously, you don't need to modify it to allow Defender for Identity to make remote calls to SAM.

A screenshot of a computer security setting

Description automatically generated with low confidence

**Notes:**

* In a multi-domain forest, it's recommended that the DSA account be created in the domain with the largest number of domain controllers.
* In multi-forest multi-domain environments, consider creating a DSA entry for each domain in the environment to avoid failed authentications from being recorded due to the round robin method.
* In multi-forest multi-domain environments, we recommend creating the gMSAs with a unique name for each forest or domain, and creating a universal group in each domain, containing all sensors' computer accounts to enable all sensors to retrieve the gMSAs' passwords and perform the cross-domain authentications.
* 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, it's recommended to create a universal group and add 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 has received it’s Kerberos ticket, it will not be able to retrieve the gMSA’s password, until it requests a new Kerberos ticket.

## MDI Action Account (gMSA)

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.

### Create and install action account

Use the steps in the [Create and install DSA](#_Create_and_install) section to create the action account. Example commands provided below:

New-ADServiceAccount -Name svc\_mdi\_aa\_sfs –DNSHostName svc\_mdi\_aa\_sfs -PrincipalsAllowedToRetrieveManagedPassword "CN=Domain Controllers,CN=Users,DC=SFS,DC=com"

Install-ADServiceAccount -Identity "svc\_mdi\_aa\_sfs"

Test-ADServiceAccount -Identity "svc\_mdi\_aa\_sfs"

### Grant Log on as a service right on DCs

A screenshot of a service setting

Description automatically generated with low confidence

### Grant action account permissions on AD objects

For details see [Create and configure a specific action account](https://learn.microsoft.com/en-us/defender-for-identity/manage-action-accounts#create-and-configure-a-specific-action-account)

At the domain root, grant the following permissions:

* Descendant User objects
  + Reset password
  + Read pwdLastSet
  + Write pwdLastSet
  + Read userAccountControl
  + Write userAccountControl
* Descendant Group objects
  + Read members
  + Write members

**Notes**

* It's not recommended to use the same gMSA account you configured for Defender for Identity managed actions on servers other than domain controllers. If the server is compromised, an attacker could retrieve the password for the account and gain the ability to change passwords and disable accounts.
* We don't recommend using the same account as 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.

# Deploy MDI Sensor

[MDI Sensor deployment](https://learn.microsoft.com/en-us/defender-for-identity/install-sensor)

[Proxy Configuration](https://learn.microsoft.com/en-us/defender-for-identity/configure-proxy)

[AD FS sensor deployment](https://learn.microsoft.com/en-us/defender-for-identity/active-directory-federation-services)

# Standalone Sensor Configuration

[Network adapters for standalone sensors](https://learn.microsoft.com/en-us/defender-for-identity/prerequisites#network-adapters-for-standalone-sensors)

[Configure event forwarding](https://learn.microsoft.com/en-us/defender-for-identity/configure-event-forwarding)

[Port mirroring](https://learn.microsoft.com/en-us/defender-for-identity/configure-port-mirroring)

# D365 Portal Configuration

## [Ensure sensors are showing up healthy](https://learn.microsoft.com/en-us/defender-for-identity/sensor-settings).

[Manage health issues](https://learn.microsoft.com/en-us/defender-for-identity/health-alerts)

## [Add Directory Services Accounts](https://learn.microsoft.com/en-us/defender-for-identity/directory-service-accounts#configure-directory-service-account-in-microsoft-365-defender)

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

## [Add Action Accounts](https://learn.microsoft.com/en-us/defender-for-identity/manage-action-accounts#add-the-gmsa-account-in-the-microsoft-365-defender-portal)

## [Enable RADIUS accounting](https://learn.microsoft.com/en-us/defender-for-identity/vpn-integration)

## [Remove learning period](https://learn.microsoft.com/en-us/defender-for-identity/advanced-settings#removing-the-learning-period-for-alerts)

For testing or proof-of-concept scenarios

## [Entity Tags](https://learn.microsoft.com/en-us/defender-for-identity/entity-tags)

Sensitive Accounts

Honeytoken accounts

Exchange accounts

## [Notifications](https://learn.microsoft.com/en-us/defender-for-identity/notifications)

Health issues

Alert notifications

Syslog notifications