8

Managing Additional Capabilities for Windows

This chapter focuses on implementing the remaining MDE security capabilities for Windows. So far, you have learned how to manage **Microsoft Defender Antivirus** (**MDAV**) and ASR capabilities. Now, you will learn about the other key features of any MDE environment:

- **Device discovery**, which lets you understand your estate and build Microsoft Defender Vulnerability Management data
- **Device control**, which lets you protect endpoints from threats or non-compliance from attached devices, including printers
- **Windows Defender Firewall with Advanced Security** (**WFAS**), which is the client firewall built into Windows and Windows Server for network control

By the end of this chapter, you will understand the use cases for these and how to implement them in line with good practices.

Device discovery

Some of the devices you should be most worried about compromising your environment are those you don't control, can't control, or don't even know about. The objective of MDE's **device discovery** capability is to uncover these risks, be they traditional unmanaged endpoints such as laptops and desktops, or other platforms such as network devices and printers.

Discovery can be approached in two ways:

- Unmanaged devices can be discovered using MDE-onboarded devices. This means no additional agent or software to manage. This is sometimes referred to as the **distributed sensor architecture**. It is distributed insofar as all your onboarded devices can work together to build the data of discovered devices.
- Managed network devices can be discovered using targeted assessment with a dedicated scanning device with an agent. Microsoft calls this **network device discovery** or **authenticated scan**. It is also sometimes referred to as **targeted assessment**. It is targeted insofar as you must specify options such as an IP range to assess.

Only clients running Windows 10 1809 or later (including Windows 11) and servers running Windows Server 2019 or later (including Windows Server 2022) can be used for discovery. It is assisted by **Packet Monitor** (**Pktmon**), which is a Microsoft tool for network capture and diagnostics.

We'll start our exploration of device discovery with the distributed approach before diving into network device discovery.

Distributed device discovery

Distributed device discovery can operate in two different modes:

- **Basic discovery**, in which information is gathered only passively
- **Standard discovery**, in which information is gathered actively

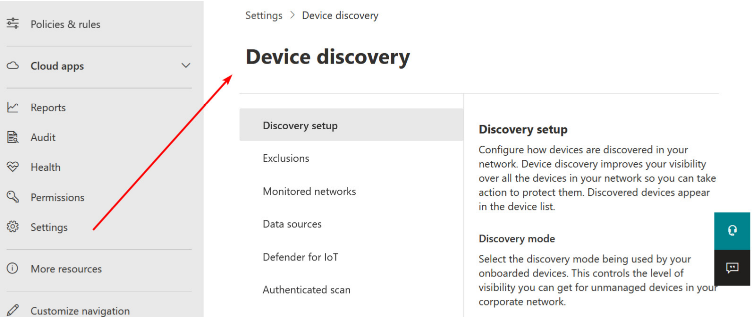
Devices configured to conduct basic discovery gather the information passively. Device information and events are extracted from standard network traffic the device sees, such as broadcasts, and it does not initiate any discovery traffic. The information discovered is, consequently, limited. For example, basic discovery may ascertain a discovered device runs Windows, but it won't know which version. A background process called `SenseNDR.exe` runs on the devices and constantly assesses traffic, sending telemetry to MDE cloud services.

Standard/active mode is the default configuration and performs unicast and multicast probing. Unlike basic discovery, this mode can present information such as hostnames and which version of Windows the device is running. Active scans supplement the data discovered in basic/passive discovery. Standard discovery uses `SenseIR.exe` and runs in addition to basic discovery; think of it as an additional layer of benefit. The additional scanning of standard mode occurs at approximately a 3-week interval, depending on variables, such as changes to the scanning device. Active scanning consumes as little as 5 KB of network bandwidth for each device being discovered. For a peek under the hood at how active scanning operates, you can see the Microsoft-signed PowerShell scripts that power it, which are downloaded to `C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads`.

You may be wondering about the detection of devices on networks you aren't concerned with, such as home networks, airport Wi-Fi, and so on. Public and private networks are distinguished from corporate networks and are not included in discovery to avoid increasing the noise of discovered data in Microsoft 365 Defender. One way this is achieved is by comparing the network to networks seen by other onboarded devices and using pattern matching: if multiple devices share a network name, gateway, and DHCP server, it's reasonable to assume it's corporate. These are regarded as **monitored networks**. This should also ease any privacy concerns home-based workers may have.

An administrator can *ignore* a network falsely marked as monitored and vice versa. Alternatively, IP address ranges can be excluded, which is particularly useful if you manage honeypots. Device discovery can also be disabled in its entirety from the **Advanced Settings** page.

Now that you know what distributed device discovery is, we'll get into how you can customize it for your environment. Let's go to **Microsoft 365 Defender** | **Settings** | **Device discovery**:



Discovery setup

Configure how devices are discovered in your network. Device discovery improves your visibility over all the devices in your network so you can take action to protect them. Discovered devices appear in the device list.

Discovery mode

Select the discovery mode being used by your onboarded devices. This controls the level of visibility you can get for unmanaged devices in your corporate network.

Figure 8.1 – Configuring Device discovery in the Microsoft 365 Defender portal

On the **Discovery setup** page, you will find the **Discovery mode** section, with the choice for a tenant default of **basic** or **standard discovery** modes. The latter is the default, and unless you have a specific reason not to use this, my advice is to keep it this way.

If you do choose to limit the use of standard discovery, you'll also find the **Select which devices to use for Standard discovery** option. This lets you have a default of basic, but apply standard discovery to devices that have the tags you select. An important point to note here is that only tags defined in the portal or by an API are respected: if the tag exists are a result of an endpoint policy, such as a registry key, it won't work.

Other device discovery settings include the ability to specify **exclusions** by IP range or specific IP, which you may wish to use to avoid interference with honeypots. The **Monitored networks** page lists the networks that device discovery has found, including **Ignored**, though you will need to amend the default filter to see these. Within here, you can switch networks between monitor states, though you'll only have the network name to do so: details such as IP ranges are not presented. If you move from **monitored** to **ignored**, discovered devices are not removed as a result, but will be purged at the end of your MDE retention period.

JUST BECAUSE YOU DON'T SEE IT IN THE UI...

...doesn't mean it's not there! Although in the list of networks in the device discovery settings, you only see the network name, there is more raw data available. You can use advanced hunting with KQL to query this using the **DeviceNetworkInfo** *table.*

With our review of how to configure distributed device scanning complete, we can move on to the next option: a dedicated scanner.

Network device discovery

The network device discovery capability uses a *dedicated* MDE-onboarded device as a scanner, rather than a *distributed* approach.

The kind of scenario this method is useful for is devices that *cannot* be managed by MDE, or maybe any other endpoint protection platform – for example, network routers and switches. These devices are just as capable of having dangerously outdated software and being breached, so you will want to know whether patches are available. Network device discovery informs you about such out-of-date platforms.

Network device discovery should also be considered an approach to scanning managed devices, rather than unmanaged ones. This is because it uses authenticated SNMP, so you must have a means of authenticating to scanned devices and ensuring they are configured with SNMP.

The target network devices and operating systems supported are noted in the following list, which is expected to continue growing:

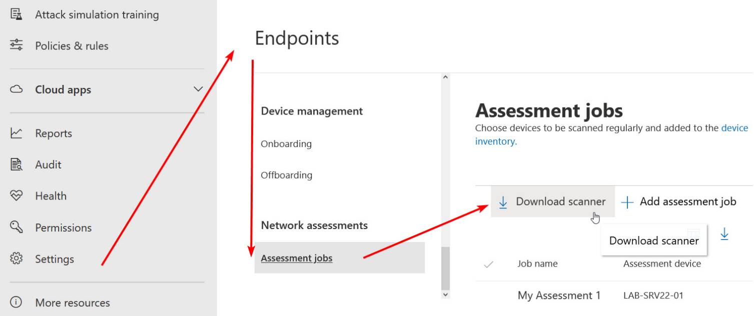
- Cisco IOS, IOS-XE, and NX-OS
- HPE ArubaOS and Procurve switches
- Juniper Junos
- Palo Alto Networks PAN-OS

Scanning software is installed on a Windows 10 or Windows Server 2019 device (or later) that runs the `MdatpNetworkScanAgent.exe` process. This is called the **assessment device**. An administrator specifies an IP address range and the SNMP credentials, which are used to gather SNMP **object identifiers** (**OIDs**) from scanned devices. One assessment device is limited to 1,500 IP addresses that can be successfully scanned, so in larger environments, you may need to consider multiple assessment devices.

The assessment device must be able to perform read-only operations on the network devices you wish to scan, so watch out for firewall rules and other controls that may limit its access. Authentication uses a community string, or the user-based security model options of *NoAuthNoPriv*, *AuthProv*, and *AuthNoPriv*. Additionally, the network scanner must have access to Microsoft's cloud resources, such as authentication URLs and `*.blob.core.windows.net/networkscannerstable/*`.

Scanning occurs hourly, though results aren't necessarily sent to the cloud service for vulnerability analysis each time: there is an 8-hour update cycle to the cloud if no changes have been identified by the scanning software. As the cloud service obtains the data, such as the operating system and version, it assesses what known vulnerabilities there are in terms of **Common Vulnerabilities and Exposures** (**CVEs**), and this informs security recommendations in Microsoft 365 Defender.

You can download the assessment device network scanner software, `MdatpScanAgentSetup.msi`, from **Microsoft 365 Defender** | **Settings** | **Endpoints** | **Assessment jobs** | **Download scanner**, then initiate the installation on the endpoint you've chosen to be the assessment device:



Assessment jobs

Choose devices to be scanned regularly and added to the device inventory.

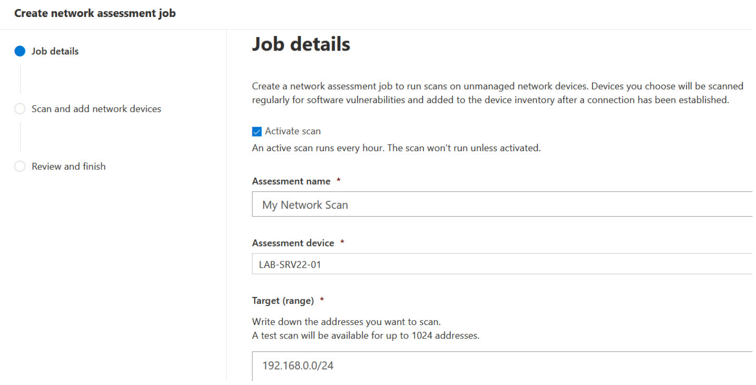
Job name	Assessment device
My Assessment 1	LAB-SRV22-01

Figure 8.2 – Downloading the network device scanner from the Microsoft 365 Defender portal

Installation is your usual simple process with one notable step: to register your assessment device to your MDE, Azure AD device login authentication is used. As the installation wizard runs, it confirms the device has been onboarded to MDE before allowing you to continue. A command prompt window will appear with a URL and a security code. Visit this URL in a web browser, enter the security code, and authenticate to allow the installation to proceed. The authenticating user must have the **Manage security settings** role permission in MDE. You do not need to perform the reinstallation for scanner software updates: a Task Scheduler entry is created that uses a script, `MDATPNetworkScannerUpdater.ps1`, to check for and install updates every hour.

Once the assessment device has been provisioned, you can jump back to **Microsoft 365 Defender** | **Settings** | **Endpoints** | **Assessment jobs** | **Add network assessment job** to configure scanning.

On the **Job details** page, you'll have to give the assessment a name and choose which of your assessment devices will perform it. Each job must have targets specified too. This can be one or more IPv4 ranges in CIDR format (for example, `172.16.10.0/24`) or individual addresses. You will also need to specify the SNMP authentication protocol, which will largely be dependent on what your network devices support. To confirm you have configured a job appropriately, you will have the opportunity to run a test scan against up to 1,024 addresses, though this is not mandatory. The advantage of doing a test scan is that it will assess which devices can be scanned successfully and allow you to limit it to those. Otherwise, it will attempt to scan every IP you specified, even if it won't be successful:



Job details

Create a network assessment job to run scans on unmanaged network devices. Devices you choose will be scanned regularly for software vulnerabilities and added to the device inventory after a connection has been established.

☑ Activate scan

An active scan runs every hour. The scan won't run unless activated.

Assessment name *
My Network Scan

Assessment device *
LAB-SRV22-01

Target (range) *
Write down the addresses you want to scan.
A test scan will be available for up to 1024 addresses.
192.168.0.0/24

Figure 8.3 – Creating a network assessment job in the Microsoft 365 Defender portal

When the assessment device finds network devices and sends data on them to the cloud, they will be presented in **Microsoft 365 Defender** | **Device inventory** | **Network devices**. You'll find information such as the make and mode, as well as risk/exposure ratings. This also feeds into **security recommends**, which you'll learn more about in ***Chapter 16***.

In this section, you've learned about two of the capabilities MDE provides for you to stay on top of securing your devices that aren't onboarded to it. This contributes to your proactive security defenses and leads us to another proactive capability we can leverage: ASR rules.

Device control

Device control is all about protecting your endpoints from devices attached to them. USB attacks continue to be a problem, and you may also have governance needs to restrict access to external storage. We know we need some level of access to devices for productivity and business processes, but that must be balanced with security. In the era of remote work, this is particularly relevant because you are limited in your ability to *physically* monitor what users are connecting. Device control contributes to endpoint security by giving administrators the ability to control what types of hardware are permitted.

BitLocker and Endpoint DLP can be regarded as device control capabilities but are quite separate from MDE's scope and aren't covered in this book. Due to the nature of their access, device control is targeted at client operating systems rather than server operating systems.

Device control is divided into three capabilities:

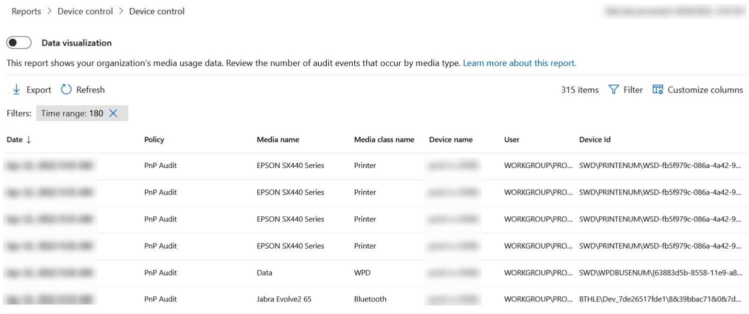
- Removable storage access control
- Device installation
- Device control printer protection

The manageability of these varies. None are controllable with Configuration Manager. All can be configured with Intune, but only device installation has a proper UI: the others are custom OMA-URIs. Group Policy remains an option for all three. In the case of removable storage access controls, you will be diving into some intricate XML editing. Consequently, this section of this book attempts to balance what you need to know to get started without overwhelming you in the detail.

Before you start

Let's address *monitoring* device control with Microsoft 365 Defender before we discuss *configuring* it. The capabilities you'll learn about allow you to control device authorization and installation, but before doing so, you can lean into the data to see what the use is currently like. This gives you a starting point for taking control of the situation so that you understand the consequences of rolling out block policies.

Using Microsoft 365 Defender, you can get data for the length of your retention period on device usage: printers, Bluetooth devices, removable storage, and so on. You can find this in **Reports** | **Device control**:



Reports > Device control > Device control [redacted]

○ Data visualization

This report shows your organization's media usage data. Review the number of audit events that occur by media type. Learn more about this report.

Filters: Time range: 180 ✕

Date ↓	Policy	Media name	Media class name	Device name	User	Device Id
[redacted]	PnP Audit	EPSON SX440 Series	Printer	[redacted]	WORKGROUP\PRO...	SWD\PRINTENUM\WSD-fb5f979c-086a-4a42-9...
[redacted]	PnP Audit	EPSON SX440 Series	Printer	[redacted]	WORKGROUP\PRO...	SWD\PRINTENUM\WSD-fb5f979c-086a-4a42-9...
[redacted]	PnP Audit	EPSON SX440 Series	Printer	[redacted]	WORKGROUP\PRO...	SWD\PRINTENUM\WSD-fb5f979c-086a-4a42-9...
[redacted]	PnP Audit	EPSON SX440 Series	Printer	[redacted]	WORKGROUP\PRO...	SWD\PRINTENUM\WSD-fb5f979c-086a-4a42-9...
[redacted]	PnP Audit	Data	WPD	[redacted]	WORKGROUP\PRO...	SWD\WPDBUSENUM\{63883d5b-8558-11e9-a8...
[redacted]	PnP Audit	Jabra Evolve2 65	Bluetooth	[redacted]	WORKGROUP\PRO...	BTHLE\Dev_7de26517fde1\8&39bbac71&0&7d...

Figure 8.4 – Using the Device control report in Microsoft 365 Defender

The report is populated by onboarded device telemetry data. It can be filtered by device and media class so that you can dig into the weeds and understand *if I configure control A, what will the effects be on device B?*

Now that you know how to review device usage before taking control of it, we'll have a look at each device control type: what they are, and how to set them up. We'll do this using Intune and Group Policy.

Removable storage access control

It is common for removable storage to either be forbidden entirely and enforced by policy or allowed but only for BitLocker-encrypted devices. What if we want more granular control? For example, allowing removable storage but only for devices we authorize?

Removable storage access control for Windows 10 and 11 lets you control the storage operations available for users and/or devices based on device properties. For example, you can set storage to read-only unless the storage matches an instance ID you trust. Even if trusted, you can continue to audit the access operations for that storage.

As with most of the ASR capabilities, you can run removable storage access control in different action modes. Audit mode can be used to gather data, with allow and prevent modes used for enforcement. MDAV does not have to be in active mode for removable storage access control to function.

You can control permissions for **read, write, and execute** (**RWX**) based on the following device properties:

- Device class
- Device, hardware, instance, primary, product, serial number, or vendor IDs
- Friendly name

You will need the GUID for these, which can be found in either the **Details** tab of a device in **Device Manager** or reference guides such as the documentation available at **learn.microsoft.com/en-us/windows-hardware/drivers/install/system-defined-device-setup-classes-available-to-vendors** and **learn.microsoft.com/en-us/windows-hardware/drivers/install/system-defined-device-setup-classes-reserved-for-system-use**. These provide GUIDs for devices that are typically external or part of the computer, respectively.

When we start to roll out removable storage access control, there are four stages of the process to consider:

1. Create a removable media group.
2. Create an enforcement policy for each removable media group.
3. Choose a default rule for media that falls outside the policies.
4. Deploy and monitor.

An Intune endpoint security profile and Group Policy are central deployment options for removable storage access control. XML files are used for configuration when using Group Policy. The XML configuration process is intricate and requires a level of detail that is outside the scope of this book; you can refer to the official documentation available at **learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-control-removable-storage-access-control**.

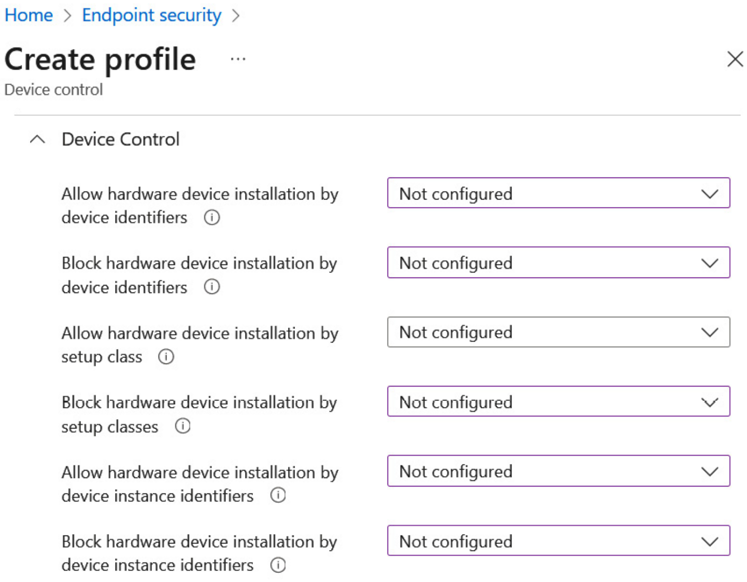
Device installation

In addition to storage access rights, we can also use device control to manage device installation – for example, we can block entire categories.

An Intune endpoint security profile and Group Policy are central deployment options for removable storage access control. XML files are used for configuration when using Group Policy, or you optionally can use them for custom OMA-URI-based profiles in Intune.

We'll demonstrate Intune with the following two steps:

1. In Intune, navigate to **Endpoint security** | **Attack surface reduction** | + **Create Policy** (or choose an existing policy). For **Platform**, choose **Windows 10 and later**, and for **Profile**, choose **Device control**.
2. Within the profile, you have options to allow or block hardware device installation by device identifiers, setup classes, or instance identifiers. You must then specify a list for each. When you choose the block option, you will also have an option called **Remove matching hardware devices**, which will block and remove existing installations:


Home > Endpoint security >

Create profile

Device control

Device Control

Allow hardware device installation by device identifiers ⓘ	Not configured
Block hardware device installation by device identifiers ⓘ	Not configured
Allow hardware device installation by setup class ⓘ	Not configured
Block hardware device installation by setup classes ⓘ	Not configured
Allow hardware device installation by device instance identifiers ⓘ	Not configured
Block hardware device installation by device instance identifiers ⓘ	Not configured

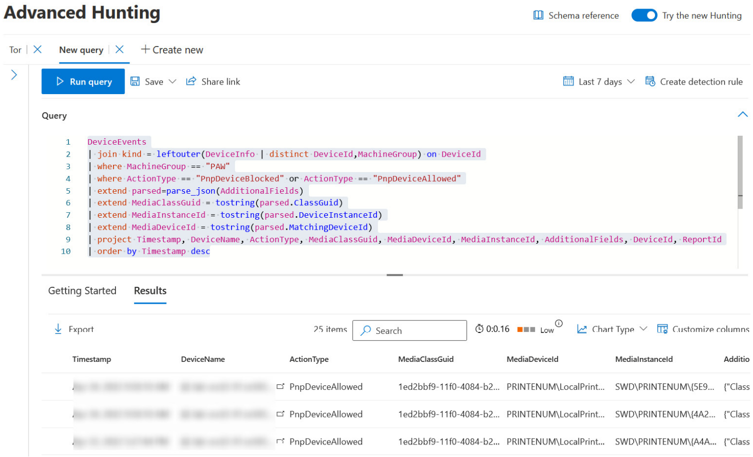
Figure 8.5 – Configuring a device control profile in Intune

You can audit device installation in Microsoft 365 Defender with advanced hunting. The **DeviceEvents** table's **ActionType** value should be queried for **PnpDeviceBlocked** or **PnpDeviceAllowed**.

In the example that follows, which is of a variation of a Microsoft-provided query, we can see the results when limited to a machine group called **privileged access workstation** (**PAW**). You can then take queries such as this and create automatic detection rules for alerts. You'll learn more about this capability in *Chapter 18*:

```
DeviceEvents
| join kind = leftouter(DeviceInfo | distinct DeviceId,MachineGroup) on DeviceId
| where MachineGroup == "PAW"
| where ActionType == "PnpDeviceBlocked" or ActionType == "PnpDeviceAllowed"
| extend parsed=parse_json(AdditionalFields)
| extend MediaClassGuid = tostring(parsed.ClassGuid)
| extend MediaInstanceId = tostring(parsed.DeviceInstanceId)
| extend MediaDeviceId = tostring(parsed.MatchingDeviceId)
| project Timestamp, DeviceName, ActionType, MediaClassGuid, MediaDeviceId, MediaInstanceId, Add
| order by Timestamp desc
```

In *Figure 8.6*, we can see the query in action, as well as the results:



```
DeviceEvents
| join kind = leftouter(DeviceInfo | distinct DeviceId,MachineGroup) on DeviceId
| where MachineGroup == "PAW"
| where ActionType == "PnpDeviceBlocked" or ActionType == "PnpDeviceAllowed"
| extend parsed=parse_json(AdditionalFields)
| extend MediaClassGuid = tostring(parsed.ClassGuid)
| extend MediaInstanceId = tostring(parsed.DeviceInstanceId)
| extend MediaDeviceId = tostring(parsed.MatchingDeviceId)
| project Timestamp, DeviceName, ActionType, MediaClassGuid, MediaDeviceId, MediaInstanceId, AdditionalFields, DeviceId, ReportId
| order by Timestamp desc
```

Timestamp	DeviceName	ActionType	MediaClassGuid	MediaDeviceId	MediaInstanceId	Additio
[redacted]	[redacted]	PnpDeviceAllowed	1ed2bbf9-11f0-4084-b2...	PRINTENUM\LocalPrint...	SWD\PRINTENUM\{5E9...	{"Class
[redacted]	[redacted]	PnpDeviceAllowed	1ed2bbf9-11f0-4084-b2...	PRINTENUM\LocalPrint...	SWD\PRINTENUM\{4A2...	{"Class
[redacted]	[redacted]	PnpDeviceAllowed	1ed2bbf9-11f0-4084-b2...	PRINTENUM\LocalPrint...	SWD\PRINTENUM\{A4A...	{"Class

Figure 8.6 – Running an advanced hunting query to see device installation events

You can extend device control capabilities to printers with **printer protection**, which we will cover in the next section.

Printer protection

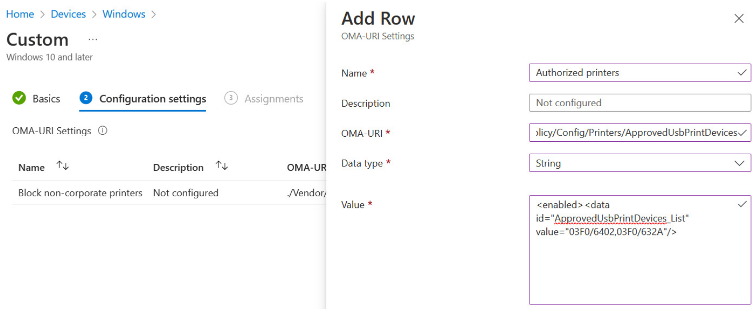
Available for Windows 10 1809 or later, printer protection lets you specify allowed USB print devices and restrict printing from unauthorized printers.

Printer protection can be deployed to your devices using a custom OMA-URI profile with Intune or Group Policy. You can scope it at the user or device level. It is a two-step process for either approach. First, a setting is configured to restrict printing from unauthorized printers. Secondly, a setting is configured that lists authorized printers based on the **vendor ID** (**VID**) and **product ID** (**PID**). These can be found in the **Details** tab | **Hardware IDs properties** section of a device in **Device Manager**.

Follow these steps in the Intune admin center to start managing printer protection with Intune:

1. Create a custom OMA-URI profile by going to **Devices** | **Windows** | + **Create profile** | **Templates** | **Custom**.
2. In the **Configuration settings** tab, add a row to block unauthorized printers. The configuration should be like this:
    1. **OMA-URI**:
        1. `./Vendor/MSFT/Policy/Config/Printers/EnableDeviceControl` if applying to devices
        2. `./Vendor/MSFT/Policy/Config/Printers/EnableDeviceControlUser` if applying to users
    2. **Data type**: `String`
    3. **Value**: `<enabled/>`
3. Now, add another row that will list the authorized printers. In the text that follows, replace `VID`/`PID` with the values of your printer. You need both, and you can keep them separated with a slash (`/`). You can list multiple printers by separating the VID and PID with a comma (`,`):
    1. **OMA-URI**:

    1. `/Vendor/MSFT/Policy/Config/Printers/ApprovedUsbPrintDevices` if applying to devices
    2. `./Vendor/MSFT/Policy/Config/Printers/ApprovedUsbPrintDevicesUser` if applying to users
2. **Data type**: `String`
3. **Value**: `<enabled><data id="ApprovedUsbPrintDevices_List" value="VID/PID,VID/PID"/>`:



Name	Description	OMA-UR
Block non-corporate printers	Not configured	./Vendor/

Name * Authorized printers

Description Not configured

OMA-URI * ɔlicy/Config/Printers/ApprovedUsbPrintDevices

Data type * String

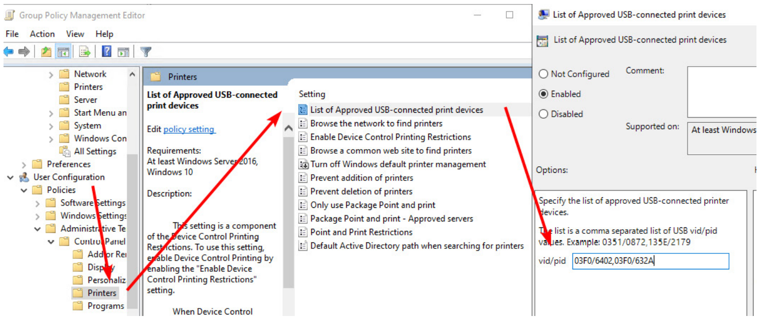
Value * <enabled><data id="ApprovedUsbPrintDevices_List" value="03F0/6402,03F0/632A"/>

Figure 8.7 – Creating a custom OMA-URI for printer protection in Intune

4. Proceed to assign your Intune policy to the appropriate user or device Azure AD groups.

That's how the job's done for Intune devices, but what if you don't have Intune? In Group Policy environments, follow the same principles of prohibiting printers and then allow-listing authorized ones:

1. In your GPO, navigate to **Computer Configuration** | **Policies** | **Administrative Templates** | **Printers** | **Enable Device Control Printing Restrictions** and select **Enable** for it for computer-level configuration.
2. For user-level configuration, instead, navigate to **User Configuration** | **Policies** | **Administrative Templates** | **Control Panel** | **Printers** | **Enable Device Control Printing Restrictions** and enable this setting.
3. On the same pages for either user or computer-level printer protection, go to the **List of Approved USB-connected print devices** setting and enter a comma-separated list of the approved printers:


Group Policy Management Editor
File
Action
View
Help
Network
Printers
Server
Start Menu an
System
Windows Con
All Settings
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Te
Control Panel
Add or Re
Display
Personaliz
Printers
Programs
Printers
Setting
List of Approved USB-connected print devices
Browse the network to find printers
Enable Device Control Printing Restrictions
Browse a common web site to find printers
Turn off Windows default printer management
Prevent addition of printers
Prevent deletion of printers
Only use Package Point and print
Package Point and print - Approved servers
Point and Print Restrictions
Default Active Directory path when searching for printers
List of Approved USB-connected print devices
List of Approved USB-connected print devices
Comment:
Supported on:
Options:

List of Approved USB-connected print devices

Edit policy setting

Requirements:
At least Windows Server 2016, Windows 10

Description:

This setting is a component of the Device Control Printing Restrictions. To use this setting, enable Device Control Printing by enabling the "Enable Device Control Printing Restrictions" setting.

When Device Control

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows

Specify the list of approved USB-connected printer devices.

The list is a comma separated list of USB vid/pid values. Example: 0351/0872,135E/2179

vid/pid 03F0/6402,03F0/632A

Figure 8.8 – User-level configuration of printer protection with Group Policy

4. Proceed to link your GPO to either a user or computer OU.

Hopefully, you can take what you've learned in this section and use printer protection in your environment to help with every system administrator's least favorite part of the job: printers! This brings us to the end of device control. In the next section, we'll move away from controlling devices and onto controlling the network as we explore firewall options.

WFAS

Built into Windows 7 onward, including Windows Server equivalents, WFAS is the host firewall that can be used to control network traffic. WFAS is stateful, without being dependent on MDAV's active mode, and comes preloaded with rules to protect systems out of the box, though it can also be managed centrally with the usual administrator tools for additional control and customization.

A key part of WFAS to understand is the concept of **profiles**, which are containers for rules depending on the connection determined by **Network Location Awareness** (**NLA**) (the `NlaSvc` service). There are three profiles, corresponding to NLA's three location types:

- **Public**, which is the most restrictive, and for areas such as public Wi-Fi, but also the default network
- **Private**, which is behind a NAT and, most commonly now, the end user's home or non-Active Directory Domain Services network
- **Domain**, which is an on-premises Active Directory Domain Services network, determined by the line of sight to a domain controller for the device's domain

A full *internals* style of WFAS falls beyond the scope of this book, but in this section, you will learn about the recommended practices for managing it, and how to navigate the administrative consoles to do so.

Recommended practices

The following are approaches to WFAS management that will steer you in the right direction. Every organization's firewall rules requirements will be unique, but there are patterns that secure implementations have. We'll start by explaining the recommendations, and then follow them by exploring how to control them with administrative tools. So, let's start with the main points to consider:

- Microsoft packaged WFAS with inbound and outbound rules from the get-go that are suitable for general scenarios. By default, outbound traffic is allowed, and inbound is not. Some inbound traffic is allowed by rules that open management services and protocols. An exception to this being generally suitable is servers, which you should harden with additional rules to also block unnecessary outbound traffic, and a review of the inbound rules to confirm they are required. For clients, you may still want to consider implementing some outbound rules in secure environments.

IF YOU WANT TO TURN UP THE DIAL…

WFAS can further harden your client's network defenses by implementing IPsec controls to protect against lateral movement. In the Further reading section of this chapter, you will find a reference to an excellent series of blogs on this.

- Although WFAS is on by default, you should use your administrative tool of choice to force-enable it, effectively overruling a local administrator disabling it. This is a setting that is off by default, but this book recommends (just as it did for similar MDAV settings) disabling local rule merge. WFAS rules can be managed centrally or locally, and are, by default, combined. Local merge allows a user with administrative rights to potentially violate your intended security rules and should be disabled.
- Important as it is, you shouldn't rush into disabling local rule merge. When apps are installed on Windows, they will often add firewall rules, usually without you realizing it. If you manage a complex estate of devices with various apps, or users installing their own, you need to consider that restricting their ability to create rules may break functionality. One way of approaching this is to install software on reference devices, monitor the required firewall rules, and then control these with your central administrative tools.
- As you create rules, there are important design considerations to note. Unlike many third-party firewalls, there is no priority or weighting system. So, how are conflicts resolved?
    - When you allow something, such as inbound traffic, this wins over the default block
    - If another block rule conflicts with this, that wins because explicit blocks always win
    - This includes against the last design point, which is that as a rule increases in specificity, the higher its ranking

Consider the following example of the rules:

- Rule 1 allows inbound TCP traffic on port `135` from `172.16.0.1/16`
- Rule 2 allows inbound TCP traffic on port `135` from `172.16.0.1`
- Rule 3 blocks inbound TCP traffic on port `135`

In this case, rule 2 supersedes rule 1 as it is more specific. However, rule 3 wins overall as it is an explicit block. The takeaway? Be as specific as you can in your definition of rules, not only because it's good for security but also because it is functionally important for WFAS. When specifying applications in rules, you are forced to be specific: wildcards are not supported; only full paths are (though variables can be used).

- The last recommendation we'll cover is enabling auditing of **Windows Filtering Platform** (**WFP**) blocked connections and packet drops. These won't increase its protective capabilities but do power reporting capabilities in the Microsoft 365 Defender portal.

Now that you're aware of the recommendations for a solid WFAS foundation, we can get into how to set it up.

Configuring WFAS

Locally, WFAS and its rules can be controlled using **WFAS MMC** (`wf.msc`). The **Windows Defender Firewall** control panel (`firewall.cpl`) is also available, which is a simplified page that cannot report rules but can be used for enabling and disabling the firewall. The MMC is a useful source for seeing existing firewall rules, such as referring to rules created during app installation.

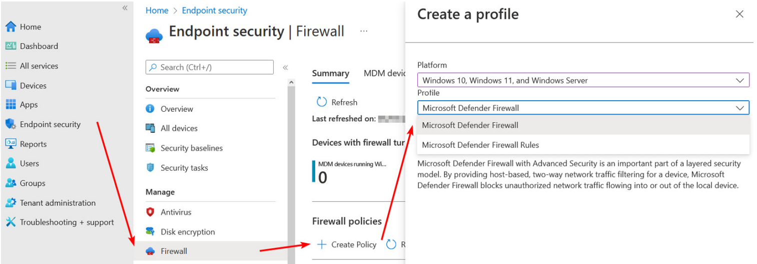
At the command line, **`netsh advfirewall`** is also available. So too is PowerShell's built-in **`NetSecurity`** module, with cmdlets such as **`Get-NetFirewallRule`**, **`Set-NetFirewallSetting`**, and **`Remove-NetFirewallRule`**. These GUI and CLI options don't scale well, though you may need them for troubleshooting or configuring individual devices.

As we've done throughout this chapter, we'll focus on using Intune, Configuration Manager, and Group Policy to configure things. You can use the steps here to learn how to navigate WFAS management, and then implement your own rules and customizations as required.

Intune-enrolled or Security Management devices can be configured in the **Intune admin center** | **Endpoint security** | **Firewall**. You have the option of two profile types:

- **Microsoft Defender Firewall**, which controls global firewall and profile-specific settings
- **Microsoft Defender Firewall Rules**, which controls firewall rules for each type of profile

In *Figure 8.9*, you can follow the arrows to get started with using Intune to configure WFAS:



Last refreshed on: [redacted]

Platform: Windows 10, Windows 11, and Windows Server

Profile: Microsoft Defender Firewall

Microsoft Defender Firewall

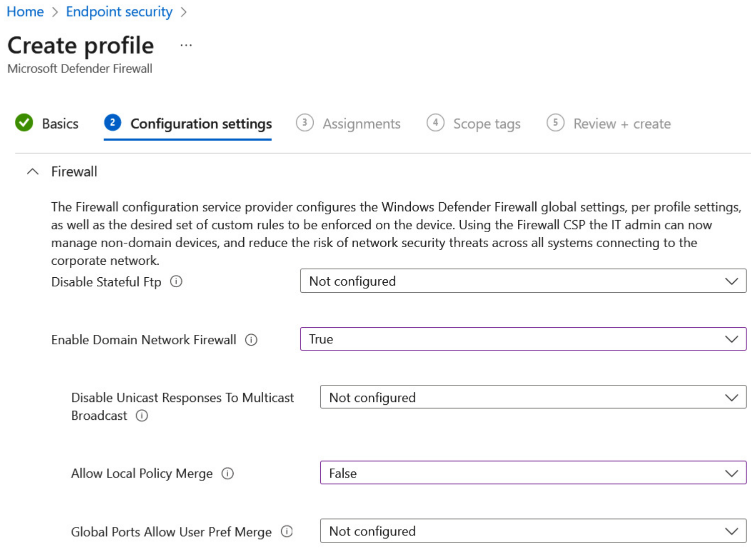
Microsoft Defender Firewall Rules

Microsoft Defender Firewall with Advanced Security is an important part of a layered security model. By providing host-based, two-way network traffic filtering for a device, Microsoft Defender Firewall blocks unauthorized network traffic flowing into or out of the local device.

Figure 8.9 – Creating a WFAS profile in Intune

For a **Microsoft Defender Firewall** profile, at the very least, you should consider changing the following settings, based on your environment's specific requirements:

- Set **Enable Domain Network Firewall**, **Enable Private Network Firewall**, and **Enable Public Network Firewall** to **True**
- Set each profile's **Allow Local Policy Merge** to **False**
- Set each profile's **Allow Local Ipsec Policy Merge** to **False**
- Set each profile's **Default Inbound Action** to **Block**
- Set each profile's **Disable Inbound Notifications** to **True**:



The Firewall configuration service provider configures the Windows Defender Firewall global settings, per profile settings, as well as the desired set of custom rules to be enforced on the device. Using the Firewall CSP the IT admin can now manage non-domain devices, and reduce the risk of network security threats across all systems connecting to the corporate network.

Disable Stateful Ftp: Not configured

Enable Domain Network Firewall: True

Disable Unicast Responses To Multicast Broadcast: Not configured

Allow Local Policy Merge: False

Global Ports Allow User Pref Merge: Not configured

Figure 8.10 – Configuring a WFAS profile with Intune

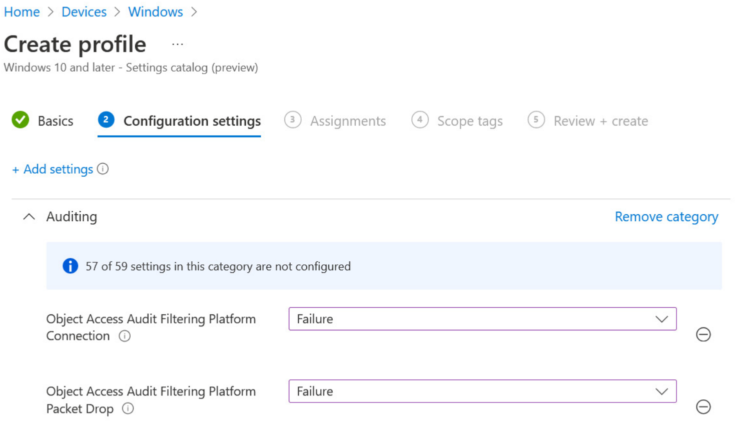
When you configure a **Microsoft Defender Firewall Rules** profile, you can specify up to 150 rules. If you need more, additional profiles can be used and merged on the device (this is only true of rules, not firewall settings). In the profile settings, use the + **Add** button and enter your configuration. Here are some points to note when editing rules:

- If a value isn't entered in a field, it defaults to **`Any`** when applied on the device
- Port values support single ports or ranges (such as **`21-22`**)
- Addresses support individual IPv4/6 addresses or ranges (**`192.168.0.0`**- **`192.168.0.255`**)/prefixes; or, for remote addresses, values such as **`Defaultgateway`**, **`Internet`**, or **`Localsubnet`**

Firewall rules are not *tattooed* to devices like some Intune settings. Therefore, if the assignment scope of the policy or device changes, the rule may be lost.

In the recommendations, you learned that two audits should be enabled to allow WFAS reporting in Microsoft 365 Defender. You can configure these with the Intune settings catalog by following these steps:

1. In Intune, head to **Devices** | **Windows** | **Configuration profiles** | + **Create profile**.
2. Choose **Windows 10 and later** as the platform and **Settings catalog** as the profile type.
3. Navigate through the wizard by giving the profile a name, and in **Configuration settings**, choose + **Add settings**.
4. Under the **Auditing** category, choose **Object Access Audit Filtering Platform Connection** and **Object Access Audit Filtering Platform Packet Drop**. Choose to audit **Failure** for both.
5. Proceed to assign the profile to the devices you're targeting:



57 of 59 settings in this category are not configured

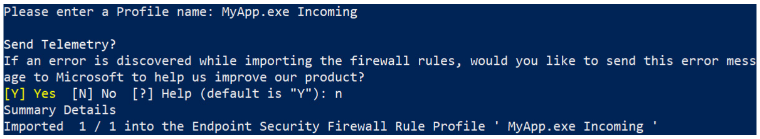
Object Access Audit Filtering Platform Connection: Failure

Object Access Audit Filtering Platform Packet Drop: Failure

Figure 8.11 – Configuring audits to power firewall reporting in Intune

If you're moving from Group Policy management of WFAS to Intune, Microsoft provides a script to import rules, known as the **Endpoint security firewall rule migration tool**. You can download this PowerShell script from aka.ms/EndpointSecurityFWRuleMigrationTool.

On a reference device with the rules that you want to migrate, run **Export-FirewallRules.ps1** with elevated rights. Prerequisites will be installed if needed (the Intune PowerShell SDK and the **ImportExcel** module), and you'll have to authenticate to Azure AD with an account that has (at least) **Endpoint security manager** permissions. OAuth permissions are then requested for Microsoft Intune PowerShell, which lets the script communicate with the service to post the imports. To perform the import, confirm the Intune firewall rule profile name when prompted, and let the script run:



```
Please enter a Profile name: MyApp.exe Incoming

Send Telemetry?
If an error is discovered while importing the firewall rules, would you like to send this error mess
age to Microsoft to help us improve our product?
[Y] Yes  [N] No  [?] Help (default is "Y"): n
Summary Details
Imported  1 / 1 into the Endpoint Security Firewall Rule Profile ' MyApp.exe Incoming '
```

Figure 8.12 – Importing firewall rules into Intune with the migration tool

The 150 rules-per-profile limitation applies, with extra profiles created automatically if needed. Optionally, you can use the **-IncludeLocalRules** parameter to include rules created locally on the device, and **-IncludeDisabledRules** to also import disabled ones. The profiles created in Intune will not have any assignments, so jump into Intune and scope them to your targets.

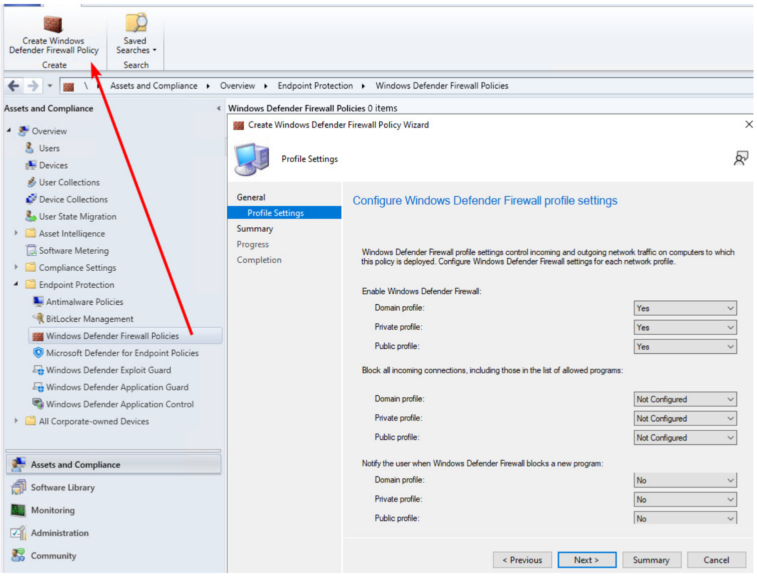
Management options in Configuration Manager for WFAS are limited to only three controls for each policy:

- Enable the firewall
- Block all incoming connections
- Control user notifications on blocks

You cannot control additional settings including, importantly, rules. Therefore, Intune or Group Policy should be used.

To manage these limited WFAS settings with Configuration Manager, you can create policies by going to **Assets and Compliance** | **Endpoint**

Protection | **Windows Defender Firewall Policies** | **Create Windows Defender Firewall Policy**:


Create Windows Defender Firewall Policy
Create
Saved Searches
Search
Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Windows Defender Firewall Policies
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
BitLocker Management
Windows Defender Firewall Policies
Microsoft Defender for Endpoint Policies
Windows Defender Exploit Guard
Windows Defender Application Guard
Windows Defender Application Control
All Corporate-owned Devices
Assets and Compliance
Software Library
Monitoring
Administration
Community
Windows Defender Firewall Policies 0 items
Create Windows Defender Firewall Policy Wizard
Profile Settings
General
Profile Settings
Summary
Progress
Completion
< Previous
Next >
Summary
Cancel

Configure Windows Defender Firewall profile settings

Windows Defender Firewall profile settings control incoming and outgoing network traffic on computers to which this policy is deployed. Configure Windows Defender Firewall settings for each network profile.

Enable Windows Defender Firewall:

Domain profile: Yes

Private profile: Yes

Public profile: Yes

Block all incoming connections, including those in the list of allowed programs:

Domain profile: Not Configured

Private profile: Not Configured

Public profile: Not Configured

Notify the user when Windows Defender Firewall blocks a new program:

Domain profile: No

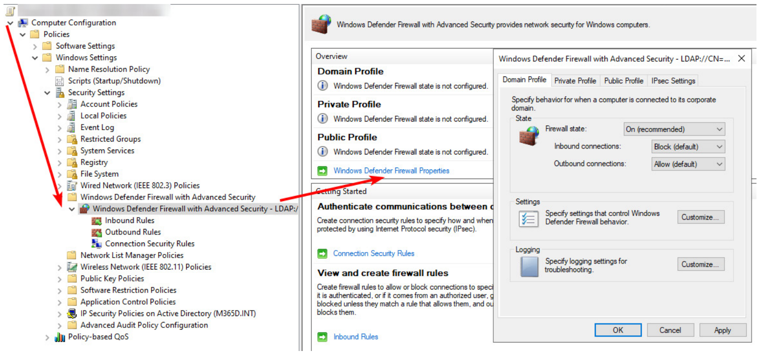
Private profile: No

Public profile: No

Figure 8.13 – Managing WFAS with Configuration Manager's limited options

Group Policy allows you to configure system-level settings for WFAS as well as rules. In your GPO, head to **Computer Configuration** | **Policies** | **Windows Settings** | **Security Settings** | **Windows Defender with Advanced Security** | **Windows Defender Firewall with Advanced Security - <LDAP string>**.

In the **Windows Defender Firewall with Advanced Security - <LDAP string>** section, click into **Windows Defender Firewall Properties** to configure the settings per profile, such as enforcing the firewall to be enabled, default inbound/outbound connection rules, and notifications:


Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Windows Defender Firewall with Advanced Security - LDAP:/
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (M365D.INT)
Advanced Audit Policy Configuration
Policy-based QoS
Overview
Windows Defender Firewall Properties
Getting Started
Connection Security Rules
Inbound Rules
Windows Defender Firewall with Advanced Security - LDAP://CN=...
Domain Profile
Private Profile
Public Profile
IPsec Settings
State
Settings
Customize...
Logging
Customize...
OK
Cancel
Apply

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Domain Profile: Windows Defender Firewall state is not configured.

Private Profile: Windows Defender Firewall state is not configured.

Public Profile: Windows Defender Firewall state is not configured.

Authenticate communications between c

Create connection security rules to specify how and when protected by using Internet Protocol security (IPsec).

View and create firewall rules

Create firewall rules to allow or block connections to speci it is authenticated, or if it comes from an authorized user, g blocked unless they match a rule that allows them, and ou blocks them.

Specify behavior for when a computer is connected to its corporate domain.

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Specify settings that control Windows Defender Firewall behavior.

Specify logging settings for troubleshooting.

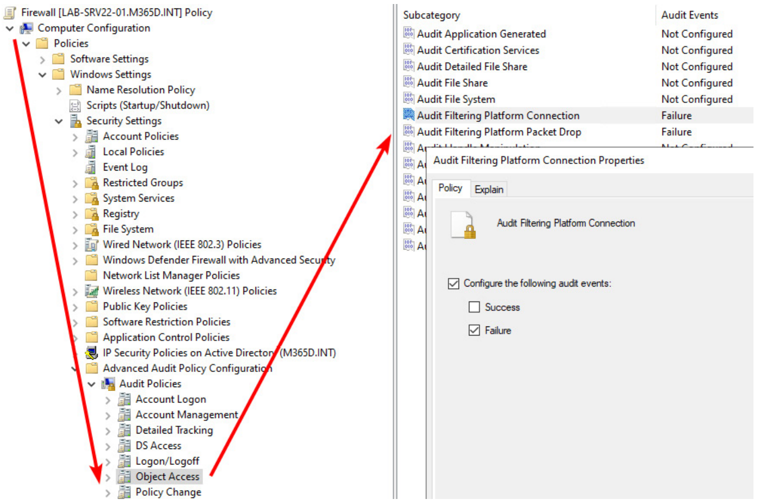
Figure 8.14 – Configuring profile settings for WFAS using Group Policy

You can also use the **Inbound Rules** and **Outbound Pules** sections to configure rules using the **Rule Wizard** area. This is the same GUI experience as for configuring the rules on the client itself. Lastly, you can use the **Connection Security Rules** section to configure IPsec authentication settings.

In Group Policy, you should also enable the appropriate auditing for Microsoft 365 Defender to report on WFAS. In a GPO, navigate to **Computer Configuration**| **Policies** | **Windows Settings** | **Security**

Settings | **Advanced Audit Policy Configuration** | **Audit Policies** | **Object Access**. Then, enable the following options with the **Failure** option:

- **Audit Filtering Platform Connection**
- **Audit Filtering Platform Packet Drop**


Firewall [LAB-SRV22-01.M365D.INT] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (M365D.INT)
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change

Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Not Configured
Audit Detailed File Share	Not Configured
Audit File Share	Not Configured
Audit File System	Not Configured
Audit Filtering Platform Connection	Failure
Audit Filtering Platform Packet Drop	Failure

Audit Filtering Platform Connection Properties

Audit Filtering Platform Connection

☑ Configure the following audit events:

☐ Success

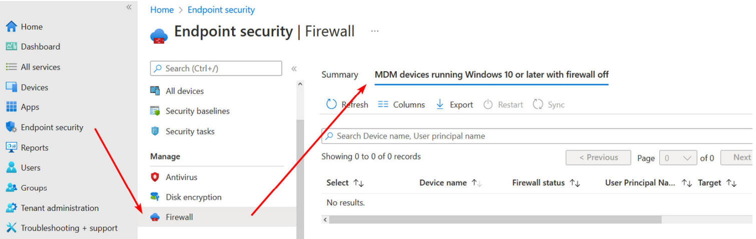
☑ Failure

Figure 8.15 – Audit Filtering Platform options in Group Policy

With your introduction to configuring and deploying WFAS using the main three management tools now complete, let's move on to how you can keep an eye on it across your estate.

Monitoring WFAS

Intune's **MDM devices running Windows 10 or later with firewall off** applies to Windows 10 and 11 and tells you exactly what it sounds like it does. You can find it in **Endpoint security** | **Firewall** | **MDM devices running Windows 10 or later with firewall off**. This page gives you an exportable list of devices, along with firewall status information:



Showing 0 to 0 of 0 records

Select	Device name	Firewall status	User Principal Na...	Target
No results.				

Figure 8.16 – Using the MDM admin center to see devices with WFAS off

You can also use **Reports** | **Firewall** | **MDM Firewall status for Windows 10 and later** in Intune. When you click **Generate report**, it will start to populate a line-level report of devices and their statuses, which can be exported too.

Moving from Intune to Microsoft 365 Defender, we can get more data about WFAS. Head to **Microsoft 365 Defender** | **Reports** | **Firewall** to view reports on inbound and outbound connections, as well as a tab about connections based on apps and processes.

Lastly, advanced hunting makes firewall analysis possible with the `DeviceEvents` table. Blocked connections can be found by querying `ActionType` for values such as `FirewallInboundConnectionBlocked`, `FirewallOutboundConnectionBlocked`, and `FirewallInboundConnectionToAppBlocked`.

This section on WFAS brings us to the end of exploring the features across MDE for securing Windows clients and servers.

Summary

This chapter concluded a series of chapters on managing MDE capabilities for Windows. In this one, you learned about key features in completing the MDE management options. This started with device discovery for discovering unmanaged devices or network devices using the authenticated scanner. Then, you learned about device control, which can be configured to protect your managed devices from unsanctioned or potentially malicious attached devices. Lastly, we explored WFAS, the built-in firewall capability for Windows that, although enabled out of the box, should be tuned for optimum protection.

In the chapters that follow, you will learn about how protection does not stop at Windows devices as we cover MDE across other operating systems.

Questions

To test your knowledge of protecting Windows clients and servers with MDE, try answering the following questions. The answers can be found toward the end of this book:

1. Which of the following firewall profiles should be applicable in an office network for Active Directory-joined devices with line of sight to a domain controller?
   1. Domain
   2. Public
   3. Private
2. You want to monitor Cisco switches in your network for known vulnerabilities. Which of the following MDE capabilities should you consider?
   1. Device control
   2. Network protection
   3. Cloud-delivered protection
   4. Network device discovery
3. There is only one type of USB printer you want to support in your organization. You are reviewing printer protection to enforce this. Which of the following pieces of information do you need about the supported printer? Choose all that apply.
   1. VID
   2. Serial ID
   3. Product ID

   4. Friendly name
4. You find that a corporate network is not being scanned as part of distributed device discovery. Where can you confirm whether it is being treated as a personal network?
   1. Device compliance in Intune
   2. Monitored networks in Microsoft 365 Defender
   3. Discovery setup in Microsoft 365 Defender
   4. Device configuration in Intune
5. True or false: if you remove an Intune device from the assignment scope of a firewall rule policy in Intune, the firewall rule requires an additional policy to remove it?
   1. True
   2. False

Further reading

To go into even further detail about some of the topics in this chapter, you can refer to the following online material:

- Microsoft maintains an official GitHub repository for device control with sample XML files that you may find useful for your learning and deployments: **github.com/microsoft/mdatp-devicecontrol**.
- In the *WFAS* section, it was mentioned you can implement IPsec controls, which require authentication to allow communication. Anthony Fontanez has an excellent series of blogs on this, and more: **anthonyfontanez.com/index.php/2021/09/16/windows-firewall-the-series**.
- There is a useful guide and script tool for troubleshooting WFAS deployment using Intune available on Microsoft TechCommunity: **techcommunity.microsoft.com/t5/intune-customer-success/how-to-trace-and-troubleshoot-the-intune-endpoint-security/ba-p/3261452?WT.mc_id=EM-MVP-5003580**.