

# Considerations for Deployment and Configuration

As we touched on in the previous chapter, **Microsoft Defender for Endpoint's (MDE's)** deployment and configuration choices typically depend on the tools you are already using in your environment. Depending on your current management strategy, this can be beneficial – or require you to rethink your approach.

For a long time, Microsoft held on to the strategy of introducing new features alongside Windows operating system development. Later, coverage was expanded to both down-level as well as non-Windows operating systems; this expanded coverage resulted in a more fragmented feature set and a dependence on Microsoft's first-party management solutions. Unfortunately, this first-party management also needed to catch up to support this expanded coverage and evolving feature set.

In this chapter, you will augment your planning with deeper technical explanations of different operating systems requirements, deployment methodologies, and configuration management tools. You'll also take a step-by-step look at the options within the unified portal. As you do, some aspects of this chapter may seem a little redundant regarding ideas from ***Chapter 5, Planning and Preparing for Deployment***. This is to be expected, as a high-level understanding of these same technologies is required to properly plan. However, in this chapter, the goal is to ensure you have all the information you need to click the buttons once the plan is executed.

Aimed more at the IT and security professionals than the project manager, this chapter will get into the weeds and hopefully answer any out-

standing questions you may have. Note that this chapter is heavily subject to change due to granularity (especially with things such as what operating systems are supported) but should remain a solid guidepost for the near future. Just be aware that you may need to do additional research if you get stuck on a deep technical issue and it seems to conflict with the text. Due to the rapidity of changes, we will also make no distinction between what is currently still in the public preview stage, versus those capabilities that are generally available.

To help you to make informed decisions on which tools and portal settings to use and how to implement them, we're going to cover the following topics:

- Operating system specifics and prerequisites
- Portal configuration
- Deployment methodologies
- Configuration management considerations

## Operating system specifics and prerequisites

To ensure a smooth onboarding experience, it pays to ensure prerequisites have been met before attempting a large-scale rollout. That said, there are some common pitfalls to avoid in this area, often driven by older operating systems and non-Windows machines requiring a different approach. Let's look at what some of those are.

## Understanding monitoring agents

At the end of 2020, as a reaction to a spike in human-operated ransomware incidents across many organizations, from health care to (local) government during a global pandemic, Microsoft set out to create a completely revamped version of the MDE product for Windows Server 2012 R2 and 2016. The intent was to shore up defenses and offer a level of par-

ity, including advanced tamper protection and response capabilities, against increasingly common ransomware tactics and techniques.

Aside from offering a solution stack that was no longer just *detection*, but a greatly improved **endpoint detection and response (EDR)** sensor with rich response capabilities, it also provided a full, next-generation antimalware solution in the form of **Microsoft Defender Antivirus (Defender Antivirus)** (even on Windows Server 2012 R2, where Windows Defender Antivirus was never included). It also signaled a move away from the dependency on Microsoft Monitoring Agent by providing a unified installation package and using the same cloud infrastructure as modern MDE platforms such as Windows Server 2019.

**Microsoft Monitoring Agent (MMA)** provided an agent for **System Center Operations Manager (SCOM)** and its cloud-based successor **Operations Management Suite (OMS)**, later to be renamed to **Log Analytics/Azure Monitor**. In the case of MDE, upon launching the product in 2016 for Windows 10, the team released a sensor specifically for servers – called **MsSenseS**. This sensor was then delivered using a **Management Pack**, a concept used in SCOM to provide health monitoring scripts.

With this modern, unified solution, there was no longer a dependency on MMA or its infrastructure, so the scope and security value of the solution increased dramatically. This also meant that customers were set on a migration path, new prerequisites were established, and deployment and configuration options became much more like those for more recent Windows versions.

### *COLD SNACK*

*A few years ago, the lead author of this book delivered a presentation to the MDE product group. In it, he told a story about a customer conversation covering all the amazing features in what was then known as **Windows Defender Advanced Threat Protection... on Windows 10. Successfully***

*pointing out the fragmented MDE feature coverage on server operating systems, he has since joined the team and delivered the modern, unified solution that addressed a large part of this fragmentation.*

## Supported operating systems

As of August 2022, the following operating systems are supported for use with MDE. Always check the online documentation to verify the currently supported ones.

### Windows

In general, MDE for Windows support closely follows the operating system life cycle, particularly for those where the features are built in. Key exceptions exist for older operating systems, where support is currently loosely coupled (the timelines correspond) with the **Extended Security Updates (ESU)** program. See the following table for a quick breakdown:

Version	SKUs	Notes
Windows 7 Service Pack 1	Pro, Enterprise	Limited functionality, OS in Extended Security Updates phase
Windows 8.1	Pro, Enterprise	Limited functionality
Windows 10	Pro, Pro Education, Enterprise, Enterprise IoT, Windows 365	Requires a supported version of Windows 10, which is on the modern life cycle
Windows 10	Enterprise LTSC 2016	This is the fixed life cycle version and does not receive new features

Windows 10	Enterprise Multi-Session	This SKU is only available for use in the Azure Virtual Desktop service
Windows 11	Pro, Pro Education, Enterprise, Enterprise IoT, Windows 365	Requires a supported version of Windows 11, which is on the modern life cycle
Windows Server 2008 R2 Service Pack 1	Standard, Datacenter, Enterprise	Limited functionality, OS in Extended Security Updates phase
Windows Server 2012 R2, 2016, 2019, 2022	Standard, Datacenter	For Windows Server 2012 R2 and 2016, upgrade to the unified agent

Table 6.1 – MDE-supported Windows operating systems

## macOS

For macOS, Microsoft maintains an  $n - 2$  strategy of supporting major operating system releases (written out as *n minus two*, where *n* is the most recent production version). This means that if your devices are running the latest or previous two versions of macOS, you are in a supported state. New versions are supported regarding the general availability of the operating system.

New product versions have an expiration date. Fortunately, the user interface will alert you.

## Linux

For Linux, support is tied to the distribution version, but in the case of Red Hat and CentOS 6.7 to 6.10, they are also tied to the kernel version. Currently, only x64 (AMD64/EMT64) and x86\_64 architectures are supported. See the following table for a quick breakdown:

Distribution	Versions
Red Hat Enterprise Linux	6.7 to 6.10, 7.2 or higher (including 8.x)*
CentOS	6.7 to 6.10, 7.2 or higher*
Ubuntu	16.04 LTS or higher
Debian	9 or higher
SUSE Linux Enterprise Server	12 or higher
Oracle Linux	7.2-7.9, 8.x
Amazon Linux	2
Fedora	33

Table 6.2 – MDE-supported Linux operating systems

\*

*For versions 6.7 to 6.10, only specific kernel versions are supported.*

Like on macOS, each version of the product is tied to an expiration date.

## Mobile operating systems

Currently, MDE supports the following mobile operating systems and versions:

- Smartphone devices running Android version 6.0 and above are supported
- For Apple, devices must be on iOS 13.0 or higher

## Operating system specifics

In this section, you will find an overview of what categories of features are available at the time of writing on each operating system family. In some cases, these features also have different capabilities, depending on the specific platform.

### Feature availability for desktop and server operating systems

Despite a large push from the MDE team to create parity and deliver security value across a broad set of operating systems, not all capabilities are available on all operating systems – or do not apply universally due to operating system specifics. See the following table for a quick breakdown of those capabilities:

Operating System	Windows 10 and later	Windows Server 2012 R2 and later	macOS	Linux
<b>Prevention</b>				
<b>Attack Surface Reduction (ASR) rules</b>	Y	Y	N	N

Operating System	Windows 10 and later	Windows Server 2012 R2 and later	macOS	Linux
Device Control	Y	N	Y	N
Controlled Folder Access	Y	Y	N	N
Firewall	Y	Y	N	N
Network Protection	Y	Y	Y	Y
Next-Generation protection	Y	Y	Y	Y
Tamper Protection	Y	Y	Y	N
Web Protection	Y	Y	Y	Y
<b>Detection</b>				
Advanced Hunting	Y	Y	Y	Y
Custom file indicators	Y	Y	Y	Y
Custom network indicators	Y	Y	Y	Y
EDR Block	Y	Y	N	N



<b>Operating System</b>	<b>Windows 10 and later</b>	<b>Windows Server 2012 R2 and later</b>	<b>macOS</b>	<b>Linux</b>
Passive Mode	Y	Y	Y	Y
Sense detection sensor	Y	Y	Y	Y
Endpoint and net- work device discovery	Y	N	N	N
Vulnerability management	Y	Y	Y	Y
<b>Response</b>				
<b>Automated Investigation and Response (AIR)</b>	Y	Y	N	N
Device response ca- pabilities: collect an investigation package, run Defender Antivirus scan	Y	Y	Y	Y
Device isolation	Y	Y	Y	N
File response capa- bilities: collect a	Y	Y	N	N

Operating System	Windows 10 and later	Windows Server 2012 R2 and later	macOS	Linux
file, trigger deep analysis, block the file, stop and quar- antine processes				
Live Response	Y	Y	Y	Y

Table 6.3 – Feature availability for desktop and server operating systems

*COLD SNACK*

*For Windows Server 2008 R2, Windows 7, and Windows 8.1 only core anti-malware and detection sensor features are available; however, all endpoints are represented in the same cross-entity portal experiences.*

**Next-generation protection**

MDE provides antimalware coverage for all supported operating systems.

For Windows 7 SP1, 8.1, and Windows Server 2008 R2, MDE offers the **System Center Endpoint Protection (SCEP)** agent. This basic antimalware solution is also available integrated with **Microsoft Configuration Manager (ConfigMgr)** (though note that no version of ConfigMgr formally supports Windows 7 SP1 nor Windows Server 2008 R2 anymore) but can be downloaded, installed, and managed without.

For Windows Server 2012 R2, the modern unified solution introduced in 2022 brought Defender Antivirus to replace SCEP. On Windows Server 2016 and later, Defender Antivirus shipped as a built-in component.

For macOS and Linux, the antimalware engine that shipped on launch was replaced in 2022 with a version that is much more like the Windows one, offering a higher level of cloud-delivered protection and opening cross-development opportunities for new protections and capabilities.

Granular device control capabilities and policies are currently only available on recent Windows 10 and later client operating systems.

## **Attack surface reduction**

The ASR category was introduced alongside Windows 10. Most features are available from Windows Server 2012 R2 and later (requiring the modern, unified solution), but there are some differences to observe due to dependencies on operating system capabilities that were introduced in newer versions of Windows.

There are a few ASR rules not available on Windows Server 2012 R2 and 2016:

- Block JavaScript or VBScript from launching downloaded executable content
- Block Win32 API calls from Office macros
- Block persistence through a WMI event subscription

Some other rules require a specific minimum Windows 10 version: At the time of writing, the most recent minimum requirement is version 1903. For a full overview of supported rules per operating system, please refer to ***Chapter 10, Reference Guide, Tips, and Tricks***.

For macOS and Linux, there is currently no equivalent capability to ASR rules or Windows Firewall on macOS and Linux. However, Network Protection and Web Content Filtering were the first features in this category to be released in 2022.

## **Endpoint detection and response**

MDE's EDR sensor (then called Windows Defender Advanced Threat Protection) was initially launched in 2016 built into Windows 10, version 1607 (known as the **Anniversary Update**), and with support for Windows Server 2016, where it had to be installed. Since then, the EDR sensor comes built into every new Windows release and no installation is required.

In 2018, EDR support for Windows 7 and Windows 8.1 was added that leveraged the same EDR sensor, MsSenseS (which was released for Windows Server 2016). The sensor was delivered via Microsoft Monitoring Agent.

In 2019, support was expanded to Windows Server 2008 R2 SP1.

In a nutshell, MsSenseS only offers detection capability, whereas MsSense offers not just an improved detection capability but also a large set of response capabilities.

On Linux and macOS, the agent is monolithic in that it combines EDR and next-generation protection.

## Mobile threat defense

The following table lists what capabilities are available for devices running Android or iOS:

Capability	Description
Web Protection	Provides anti-phishing and protection against unsafe network connections. Supports custom (URL/IP) indicators.
Malware Protection (Android-only)	Scans for malicious apps.

Jailbreak Detection (iOS-only)	Detects whether a device was jailbroken.
Vulnerability Management	Integration with threat vulnerability management.
Network Protection	Protects against rogue Wi-Fi-related threats as well as compromised certificates. Allows you to allowlist the root CA and private root CA certificates in Intune.
Unified Alerting	Ensures alerts on mobile devices (and their timelines) end up in the Microsoft 365 security console.
Conditional Access and Conditional Launch	Blocks risky devices from accessing corporate resources. Integration with app protection policies via <b>Mobile Application Management (MAM)</b> in Intune.
Privacy Controls	Can configure privacy in threat reports by controlling the data that is sent to your tenant.
Integration with Microsoft Tunnel	Integration with <b>Microsoft Tunnel</b> .

Table 6.4 – Mobile threat defense (MTD) capabilities

## Prerequisites

Now that you are aware of feature availability and operating system coverage, you will want to make sure that the minimum system requirements have been met. Sometimes, this may lead to resizing your environment (adding more resources to your virtual machines). Particularly on

Linux, sometimes, sizing had only been performed on the running workload and security solutions were not accounted for.

Then, particularly on older operating systems, you will want to ensure that you have applied the appropriate patches – not just to secure the operating system itself, but to meet the requirements for MDE.

In general, for Windows operating systems, if you have updated to a recent cumulative update package, you are in good shape. The documentation calls out exactly which pieces are needed for the product to operate as expected.

### *COLD SNACK*

*A (any!) security solution is not a substitute for security hygiene no matter what. If you wish to stand a chance of defending against advanced attacks, know that older operating systems are extremely vulnerable! If you cannot isolate machines that are running these legacy operating systems, patch them – but better yet, decommission or replace them with a more modern platform.*

## **Windows**

For most modern Windows operating systems, if you are running a version that is in mainstream or extended support and is up to date, all components are built in. You should be in decent shape and onboarding should not pose any major challenges. For older operating systems such as Windows 7 SP1, 2008 R2, Windows 8.1, 2012 R2, and 2016, you will need additional steps, especially if you have not regularly applied operating system updates.

System requirements follow those of the Windows version that is installed except for those that require MMA to be installed.

### **Windows 7 SP1 (Service Pack 1), Windows 8.1, and Windows Server 2008 R2**

For these older operating systems, there are two separate components to install:

- **Antimalware: System Center Endpoint Protection (SCEP):**
  - Service Pack 1 for Windows 7 and 2008 R2
  - January 2017 antimalware platform update (4.10.209) for clients already running older (4.7) versions of SCEP (you can obtain the latest installer from Microsoft's volume licensing center)
  - The SCEP client Cloud Protection Service (MAPS) membership setting should be configured to **Advanced** to ensure malware events get captured in the machine timeline
- **EDR: MsSenseS.exe** delivered through MMA is the detection component. The dependency on MMA provides additional requirements:
  - Core prerequisites:
    - C++ Redistributable 2015
    - .NET Framework 4.5.2 or higher
    - Update for customer experience and diagnostic telemetry
  - Windows 7 and 2008 R2 SP1:
    - February 2018 or newer monthly *update rollup*
    - March 12, 2019 or newer servicing stack update
    - SHA-2 code signing support update

## Windows Server 2012 R2

With the modern, unified solution, the prerequisites were simplified to such a point that only operating system updates were required.

The installer will tell you if you have not met the core requirements; if so, please realize that you may be encountering a machine that has not received any updates for a very long time. **Microsoft Detection and Response Team (DART)**, a customer-facing incident response team, regularly encounters this situation in organizations that have been heavily compromised.

The core prerequisites are as follows:

- October 12, 2021, monthly rollup (KB5006714) or later

After installation, feature updates and bug fixes will be delivered through KB5005292 (EDR sensor update) and KB405263 (antimalware platform update).

## Windows Server 2016

Since the modern, unified solution has a dependency on Defender Antivirus for its response capabilities (EDR Block, AV scan, and Auto IR to name a few) the dependency here, aside from regular OS updates, is the Windows Defender Antivirus feature, which shipped with the operating system. This is likely where most of the complexity lies as very few organizations go back to their servers and decide to add a feature; in addition, third-party antimalware solutions have historically attempted to remove or disable Windows Defender Antivirus to avoid conflicts.

Core prerequisites:

- **Servicing Stack Update (SSU)** from September 14, 2021 or later
- **Latest Cumulative Update (LCU)** from September 20, 2018 or later
- Windows Defender Antivirus feature enabled and updated with the latest platform update

After installation, feature updates and bug fixes will be delivered through KB5005292 (EDR sensor update) and KB405263 (antimalware platform update).

## Windows 10 and later, Windows Server 2019 and later

Like any recent Windows version, prerequisites will be met if you are running a currently supported Windows version that has received regular updates. For some newer capabilities that were backported, you may encounter specifically required updates.



The following updates are required for security settings management without enrollment:

- KB5007744 for Windows Server 2019 and later
- KB5006738 for Windows 10 Enterprise 2019/LTSC and later

## macOS

There are no specific prerequisites for macOS, but it is highly recommended to keep **System Integrity Protection (SIP)** enabled.

System requirements follow those of the macOS version that is installed.

## Linux

Aside from distribution-specific requirements for kernel versions (specifically), the following are required:

- Core requirements:
  - systemd system manager
  - **fanotify** kernel option must be enabled
  - Audit framework (**auditd**) must be enabled
- For Red Hat Enterprise 6.7-6.10 and CentOS 6.7-6.10:
  - SystemV or Upstart system manager

System requirements are recommendations that should consider the current utilization of the system and its workloads:

- **Disk space:** 1 GB minimum
- **Cores:** 2 minimum, 4 preferred
- **Memory:** 1 GB minimum, 4 GB preferred

Now that you understand what's supported by your clients, let's move on to portal configuration. Several settings depend on client capabilities.

# Configuration options for the portal

The M365D settings node houses configuration options for endpoints, the portal experience itself through **security.microsoft.com**, as well as any integrations.

Within the M365D portal, there are settings nodes for each integrated product and the overall portal. In this section, you will find explanations for all the settings under the **Endpoints** node, as well as **Device discovery**. The following screenshot shows the different top-level settings nodes you might see in an integrated XDR environment:

## Settings








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

Figure 6.1 – Breakdown of settings categories

## General options

This is the first section heading you'll encounter; it covers advanced feature configuration first, and then the basics such as licenses, email notification setup, and automated remediation.

## Advanced features

In this section, you are provided with various toggles that affect either your portal experience or what happens on onboarded endpoints. Not all settings are related to integration with other products.

## **Automated Investigation**

This will enable the capability at the tenant level; then, you can decide per device group what you want the level of automation to be. This is great to help build confidence in the capability, but you may also consider excluding certain mission-critical devices from this feature. In general, you should strive to have this at least on all user endpoints as it can help greatly reduce the number of incidents you need to respond to.

## **Live response**

Like automated investigation, this turns the ability on for the tenant. The next step is to determine which capabilities are available per role. This feature is very powerful and therefore requires some consideration when delegating this to specific roles in your organization.

## **Live response for Servers**

This follows the same global enablement as the previous setting but is specific to servers. This feature is useful if you want to prevent this level of control on servers as there may be security considerations where having this level of remote control on a server would be undesirable.

## **Live response unsigned script execution**

This requires some consideration and is desirable to have enabled. Though enforcing signed scripts can produce additional overhead for your SOC/IR team, it does reduce the potential for untrustworthy or malicious scripts from running. You may want to consider some governance and even signing your own scripts with a CA that is specifically trusted by your organization, as good practice.

## **Restrict correlation to within scoped device groups**

This setting is primarily used to prevent cross-scope incidents that would potentially create an issue with the separation of duties or even compliance – for example, in a complex organization with multiple SOCs operating in the same MDE tenant. Since attackers do not respect these organizational boundaries, you may wish to carefully consider your operational model – if there's no way to otherwise accommodate regulatory compliance constraints.

## Enable EDR in block mode

This capability is intended for when you are running a third-party anti-malware solution. It will not perform any blocks that Defender Antivirus would not perform if it were the active antimalware solution.

### *COLD SNACK*

*There's typically a lot of confusion around this setting and hesitation to enable it. Please refer to **Chapter 2**, Exploring Next-Generation Protection, for a full explanation of **passive** mode and EDR in **block** mode. The best lens to apply here is that EDR in **block** mode would not do anything Defender Antivirus wouldn't do; in fact, what happens here is that EDR, after noticing potentially malicious activity, asks the Defender Antivirus engine to scan a file and perform its default remediation action.*

## Automatically resolve alerts

This setting is particularly useful when used in tandem with the Intune integration. Why? Because active alerts raise the risk level of a device. This risk level is sent to Intune, where it is used in compliance policies to mark the device as noncompliant. In turn, you can take device compliance status as input for **Azure Active Directory (Azure AD)** conditional access policies. It's also a great way to reduce the volume of alerts or incidents you need to deal with.

### *COLD SNACK*

*As the preceding explanation around the Intune integration requires multiple moving parts, let's simplify this into a scenario: a device with active alerts can no longer access certain corporate resources because there is an active alert on the device. Automated investigation cleans up the threat and closes the alert(s). Now, the device is allowed to access the resources again.*

## **Allow or block file**

This setting controls whether you can block a file across the entire organization using Defender Antivirus. It's a simple but very effective response capability. If you don't use Defender Antivirus as your primary antimalware, you may wish to turn this off to avoid confusion (the button will not work) and find an alternative way to block the file.

## **Custom network indicators**

This is another setting that depends on Defender Antivirus – and the network protection feature. Like **Allow or block file**, if you don't use Defender Antivirus as your primary antimalware solution, you should probably turn this off to avoid confusion. However, this is a very useful capability to have as it does not depend on any network infrastructure; you can block connections on any onboarded device in any location.

## **Tamper protection**

This toggle will allow you to send a dynamic signature to all onboarded devices in your organization. It will ensure that Defender Antivirus goes into a mode that disallows changes to certain critical capabilities such as real-time protection, cloud protection, and so on. It's a strong tool that makes it much harder for attackers to bypass prevention capabilities, but it can also get in the way of troubleshooting (which is where troubleshooting mode can come in). This toggle is not the only way to apply or remove **tamper protection (TP)**. See [\*Chapter 2, Exploring Next-Generation Protection\*](#), for more information about TP.

## **Show user details**

This setting, which adds details to user entities, is mostly a compliance-related one. There may be requirements in some organizations revolving around privacy – equally so for when you have outsourced your SOC.

### Skype for business integration

The setting is inclusive of Teams and allows you to easily connect to users via a chat or call by adding a button to the user page. This is particularly useful if you need to ask a user about some questionable behavior or when you have, for example, isolated their machine.

### Microsoft Defender for Identity integration

This setting has been around for quite a while and is a great example of the **extended detection and response (XDR)** concept in Microsoft 365 Defender. Being able to correlate, create alerts and incidents, and pivot without abandoning context is incredibly valuable when investigating lateral movement and the scope of a compromise.

### COLD SNACK

**Microsoft Defender for Identity (MDI)** used to be called *Azure Advanced Threat Protection*. At the time, it had very little to do with Azure apart from running on it as a cloud service; it was always a solution that provides various on-premises Active Directory detection and response capabilities.

### Office 365 Threat Intelligence connection

Like the Microsoft Defender for Identity integration, this setting revolves around being able to pivot into a deeper integration of what's happening on a given user's email and collaboration workloads through **Microsoft Defender for Office (MDO)**. It also allows you to exchange signals and automated investigation triggers across products. This is another showcase of the road to XDR that MDE started many years ago!

### Microsoft Defender for Cloud Apps

To use any **cloud access security broker (CASB)** to detect shadow IT, analyze usage patterns, and spot anomalies, you need one critical thing: data. This integration sends web browsing activity from MDE to **Microsoft Defender for Cloud Apps (MDCA)**. This allows you to, without having to send any additional data from, for example, your proxies, perform shadow IT discovery, put activity in the context of incidents, and generally tell the story of how a compromise led to data exfiltration.

In addition, this integration allows you to block unsanctioned cloud applications in MDCA, which creates custom URL block indicators in MDE, effectively blocking that cloud app on all endpoints.

Lastly, MDCA also monitors user activity as it integrates, in turn, with Azure Active Directory and Office 365. This unlocks several other capabilities, involving detecting data exfiltration, identity activity, and more.

### **Web content filtering**

This is a global switch. Since it depends on Defender Antivirus and network protection, it's optional. It enables you to send policies that govern access to specific categories of websites.

### **Download quarantined files**

Unless you have compliance/privacy concerns, this is a super useful capability to ensure that whatever Defender Antivirus puts into quarantine, you can download and analyze it somewhere else. Be careful with this one as you are dealing with what is very likely malware.

### **Share endpoint alerts with Microsoft Compliance Center**

This is a great example of how to reuse what you are already gathering on an endpoint. Being able to share signals from the security suite to Microsoft's compliance suite means you don't need to deploy additional agents, infrastructure, or impact endpoints in any other way to provide a whole slew of additional security services. Though outside the scope of

this book, compliance goes hand in hand with security in most organizations.

## Authenticated telemetry

This is an anti-spoofing measure intended to address CVE-2022-23278 and related concerns. It may have some impact on outdated machines.

## Microsoft Intune connection

This toggle will enable integration with Intune, providing the following benefits and additional options:

- Device risk can be sent from MDE to Intune, based on the risk calculated by MDE. This can then be used to determine device compliance, which can then feed into conditional access policies.
- This connection can also be used for app protection policies. This means that, on mobile devices, you can determine what the risk level should be at or under to comply with the policy that is specific to an app, as opposed to the device; this does not require the device to be enrolled into Intune management.
- Through the same **Mobile Threat Defense (MTD)** connection, it's possible to gain insights into unmanaged applications running on mobile devices.

## Device discovery

This is the main enablement switch that will trigger all capable devices to start scanning the network(s) they are connected to, detecting and assessing devices that are not onboarded to MDE.

Note that there is a section where you can manage device discovery. To do so, go to **Microsoft 365 Defender | Settings | Device discovery**.

## Preview features



This descriptive setting will help you light up the settings for preview feature enablement. These preview features are as follows:

- Off by default
- Supported by Microsoft customer support
- Intended for evaluation so that you can decide to roll them out

## Endpoint attack notifications

This option turns on these very useful notifications. It is highly recommended. For more information about this integration and Microsoft Defender Experts, please refer to [\*\*\*Chapter 4\*\*, Understanding Endpoint Detection and Response\*](#).

## Licenses

This provides a license count that comes from the Microsoft 365 admin center. Note that this only pertains to **user** licenses (licenses covering user devices); servers are typically licensed using either the *true-up* system (you provide a count to Microsoft as to how many you want to add to your agreement) or pay as you go through **Microsoft Defender for Cloud (MDC)**. When it comes to licensing, always consult with your provider to determine what model applies to your organization.

## Email notifications

Here, you can create email notifications for alerts or vulnerabilities. This is best used selectively; use cases can be for VIP machines or other high-value assets that you wish to draw more attention to. Some organizations monitor a Teams channel or shared mailbox around this, as an extra tier for their SOC.

### *COLD SNACK*

*Note that both alerting and email are not fully real-time notifications – meaning both firing an alert and an email of this alert arriving come with*

*some delay. As such, you should consider that this may not be the best process to base your incident response on, but if you don't have a SIEM and continuous monitoring, this may be a good alternative.*

## Auto remediation

If you have globally enabled automated investigation in **Advanced Features**, this is where you can go to determine what automation level to apply to each device group when there is a triggering alert. Note that you can only configure automation levels for existing device groups; you can also configure these levels in the **Device Groups** section itself.

The available levels are as follows:

- **No automated response:** Do nothing
- **Semi - require approval for all folders:** Will not remediate anything until you approve it
- **Semi - require approval for non-temp folders:** Everything that's not a temporary folder will require you to approve the remediation; everything else is fine
- **Semi - require approval for core folders:** Core here means system folders
- **Full - remediate threats automatically:** The recommended setting

*COLD SNACK*

**Auto remediation** *respects allow and block indicators.*

## Permissions

Though we worked through permissions in ***Chapter 5, Planning and Preparing for Deployment***, we wanted to reiterate the basic understanding here as we step through the options available in the portal.

There are two possible permissions models for MDE: basic permissions and **role-based access control (RBAC)**:

- Basic permissions adopt full access (Global/Security Administrator) or read-only (Security Readers) roles from **Azure AD** that you have associated with your tenant (the global admin involved in initial tenant creation)
- With the RBAC model, the Global and Security Administrator roles in Azure AD retain full access by default (don't get locked out!), but after switching to this model, you will need to specifically assign permissions to Azure AD groups – create roles

If you are adopting/have adopted the Microsoft 365 Defender permissions model, roles should be defined at a higher level to allow you to reuse these roles for all the services available. Once you do, you can no longer modify the permissions for these roles inside the individual products! An import function allows you to transition more easily if you have already set up custom roles in MDE or MDO. We've provided an example of an RBAC approach in ***Chapter 5**, Planning and Preparing for Deployment*.

### *COLD SNACK*

*Setting up the right role-based access model requires thoughtful consideration and can dictate how you operate your SOC. The sooner you define the right framework, the more likely you are to avoid having to rework things to fit the model.*

## **Roles**

This is where you can define roles and permissions and assign Azure AD security groups. In the basic model, you will only have full access and read-only options. Once you adopt the RBAC model, you need to explicitly assign a role to an Azure AD group.

## **Device groups**

This is where you go to define your device groups, a logical grouping used to scope the following:

- Alert suppression
- Automated investigation remediation levels
- User groups from Azure AD
- Indicators
- Web content filtering

Remember that, when you create a group, you can also define the desired automation level. Groups are populated by defining conditions such as device names, domain, OS, and tags. The latter, tags, will allow for a more fine-grained approach toward grouping if needed. Tags can be configured through the registry (Windows), configuration (Linux, macOS), the portal, or an API.

### *COLD SNACK*

*MDE coverage extends to devices that are not registered in any directory, workgroup, or other central store. As such, though MDE integrates with Azure AD to be able to provide authenticated access to the portal and operations, as well as to provide deep integration and experiences across other security solutions, there is no requirement for devices to be in any specific domain or directory.*

## APIs

This section of the portal configuration pages is specific to API integrations, including those with a **Security Information and Event Management (SIEM)** system.

## Security Information and Event Management

In 2022, Microsoft started replacing the existing **SIEM** API connector with a new one – a **REST API** leveraging **OAuth 2.0** that provides an interface to retrieve incidents and alerts. This interface provides access to

Microsoft 365 Defender incidents and MDE alerts, and the **Microsoft 365 Streaming API** provides event data streaming.

As such, the information in the SIEM section is relevant primarily to organizations that have already enabled a connection to their SIEM using the previous APIs.

## Rules

The **Rules** section contains items that were created as part of your security operations, including incident response and importing **Indicators of Compromise (IOCs)**. For more information about how and when to create these, please refer to *[Chapter 8, Establishing Security Operations](#)*.

## Alert suppression

In this section, you will be able to review and edit the alert suppression rules you have created.

## Indicators

Here, you can review, edit, and create custom indicators and response actions for four entity types:

- **File by hash:** SHA256/SHA1/MD5 are valid inputs.

This requires Defender Antivirus as the primary antimalware with cloud-delivered protection and the **Allow or block file** global setting to be enabled in **Advanced Features**.

- **File by signer (certificate):** Valid inputs are **.CER** and **.PEM** files.

Same requirements as **File by hash**. You need to add the specific signing certificate to match.

- **IP addresses:** Only single IP addresses are valid inputs.

This also requires the network protection feature and the **Custom network indicators** global setting to be enabled in advanced features.

- **URLs/domains:** You can add domain names (for example, **.com**) and specific URLs (for example, for the domain/page).

Same requirements as IP address indicators.

### *COLD SNACK*

*Here, the **EnableFileHashComputation** setting for Defender Antivirus comes into play! Most of the time, hash calculation will happen on the fly by either EDR or Antivirus in one of the many flows (locally by MDE, in the cloud); however, for files that have never been observed, you may notice that indicator matching does not occur immediately as the hash has not been calculated. **EnableFileHashComputation** instructs Defender Antivirus to generate hashes for **all** files it scans, not just new arrivals from the internet – which means there is a performance penalty to pay. You will want to tread lightly for machines that encounter many new files and slower disks.*

For every indicator, you can determine what the desired response action will be:

- **Allow:** Let the file run
- **Audit:** Generate an alert if there is a match based on the events coming from the machine
- **Block execution:** Disallows the execution of a file
- **Block and remediate:** Defender Antivirus will perform the remediation
- **Warn:** Sends a warning to the user that they can override

The following things are good to know:

- If a file is already excluded in Defender Antivirus, indicators to block the file will not work.
- Not all response capabilities are available for each indicator type.

- Warn indicators require a user interface. As such, on server operating systems or those where there is no user interface, this type may be unsuitable.
- Indicators can also be created from an investigation context or through a CSV file import.
- Note that it can take anywhere between 30 minutes to 3 hours for a custom indicator to activate or deactivate.
- You need Edge to be able to block HTTPS URLs.

## Process Memory Indicators

During an active automated investigation, when you navigate to the **Evidence** section, you have the option to add a process, by hash, that was a part of the memory content analysis to the allow or block list. It will show up on this page, where you can remove it if desired.

## Web content filtering

This is where you create policies for web content filtering by selecting categories and assigning the policies to device groups. For more information about web content filtering, see [\*\*\*Chapter 2\*\*, Exploring Next-Generation Protection\*](#).

## Automation uploads

In this section, you can configure what **Automated Investigation and Response (AIR)** can upload.

## File content analysis

This setting allows you to turn off file content analysis and restrict which file types you agree to automatically submit for analysis when an automated investigation runs. Just like the Defender Antivirus automatic sample submission setting (for more information, see [\*\*\*Chapter 2\*\*, Exploring Next-Generation Protection\*](#)), this can help with regulatory compliance/privacy concerns.

## Memory Content Analysis

Similar to file uploads, there's potential for usernames and other identifiers to be collected and sent. From a security perspective, you should enable this capability as it provides significant value. As always, you will need to investigate how this complies with the regulations your organization is subject to. Microsoft provides documentation and contractual guarantees regarding compliance boundaries.

## Automation folder exclusions

These exclusions will only apply to automated investigations – while Defender Antivirus exclusions also apply to automated investigations, this does not work the other way around.

## Configuration management

In this section, you can select options for the security configuration management feature.

## Enforcement scope

This option allows you to scope, in various ways, the dynamics around configuration management. This is mainly to ensure that various configuration management tools can coexist and provide an opportunity to gradually enroll devices into MDE management.

The global switch will enable this capability in your environment; you will need to hit the corresponding toggle in Intune to complete the connection.

The settings available here will allow you to differentiate between client and server devices – in case you want this separation from a delegation perspective or simply if you want to narrow the scope for testing or gradual rollout purposes. Another tool to achieve this is the *pilot mode* toggle,



which will ensure that only devices with the **MDE-Management** tag will automatically enroll.

## Device management

On these pages, you will find all the installation and onboarding/offboarding packages/scripts required for different deployment tools.

### Onboarding

This section contains various onboarding packages/scripts/installers. Note that some deployment tools, such as MDC and **Microsoft Endpoint Configuration Manager (MECM)**, already have access to onboarding information and/or installation packages, depending on which version you are using.

### Offboarding

To remove a device from being monitored and/or managed by MDE, you will need to apply an offboarding script/package. These expire after 30 days – you do not want these to end up in the wrong hands. You can either use an offboarding script or, in the case of MECM, the **.offboarding** file.

## Network assessments

This section is no longer in use. Instead, a new page was introduced in Microsoft 365 Defender (on the **Microsoft 365 Defender | Settings | Device discovery** page) inclusive of the integration of Defender for IoT (technology from the CyberX acquisition in 2020), as shown in *Figure 6.2*. This allows you to combine sensors to perform device discovery; on-boarded endpoints perform continuous discovery, authenticated scans from dedicated machines provide additional context and inventory of network devices, and the Defender for IoT network sensor provides visi-

bility on devices in network segments it was deployed in. This integration also allows you to share detections:

Settings > Device discovery

## Device discovery

Discovery setup

Exclusions

Monitored networks

Data sources

Enterprise IoT

Authenticated scans

**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. [Learn more about it](#)

☐

Basic

Discover and identify unmanaged devices by passively listening to network events captured by onboarded devices.

☒

Standard discovery (recommended)

Enrich device information and discover even more devices by using smart, active device probing.

☒

Enable Log4j2 detection (CVE-2021-44228)

Detect devices with applications using the vulnerable Log4j2 library through unauthenticated probing. This option will also enable discovery using Server 2019+ onboarded devices. [Learn more about it](#)

**Select which devices to use for Standard discovery**

☒

All devices (recommended)

Enable Standard discovery for supported devices that have been onboarded.

☐

Select tags

Enable Standard discovery on device or device groups based on selected tags.

[Edit selected tags](#)

Save

Figure 6.2 – Device discovery settings

## Discovery setup

[https://learning.oreilly.com/library/view/microsoft-defender-for/9781804615461/B18990\\_06.xhtml](https://learning.oreilly.com/library/view/microsoft-defender-for/9781804615461/B18990_06.xhtml)

34/50

Here, you can choose between basic and standard discovery. Basic discovery discovers devices passively by monitoring network requests.

Standard discovery executes a series of PowerShell scripts to perform active scanning of network devices. In specific cases, it attempts to discover attempted exploits for known vulnerabilities on the network. You may trigger some other security tools inside your network as a result, so make sure everyone is familiar with this dynamic!

You can scope discovery to specific devices by using tagging.

## **Assessment jobs**

Here, you can download scanner software and set up scanning jobs for use with the device inventory in vulnerability management. You can set up scanners that use Active Directory for authentication to (unmanaged) Windows machines, or SNMP for (unmanaged) network devices, and define which networks you would like to scan.

## **Exclusions**

Fairly self-explanatory, this will allow you to exclude some devices from being discovered – of course, this is something to be used wisely and requires some consideration of where devices are located. In a heavily distributed network environment or with roaming devices, where IP address space is not controlled, you will only have basic discovery for the IP addresses or ranges you specify.

## **Monitored networks**

Pattern recognition is used here to determine corporate networks. This section will allow for some fine-tuning to reduce noise – if you have many mobile workers that connect to home networks with their devices, those networks are likely to be filtered out intentionally unless you add them for monitoring.

## **Data sources**

This provides toggles for integration – if you have security solutions that are performing discovery inside networks where there may be no MDE onboarded devices, this will help extend discovery there and retrieve signals at the same time.

## Enterprise IoT

This page shows the optional integration with Microsoft Defender for IoT as an additional sensor for device discovery and threat detection.

Through this integration, you can populate the **IoT devices** tab in **Device inventory** and receive alerts, recommendations, and vulnerabilities.

## Authenticated scans

This option will allow you to provide credentials and settings for authenticated scans that are related to assessment jobs.

Once you've set up the portal so that you can leverage the capabilities on your endpoint, it's time to select a deployment tool and method.

# Selecting your deployment methodology

MDE itself does not deploy agents; that said, agents are only required for operating systems that do not have the components already built in.

Ensuring you can deploy the latest versions and are ready to apply regular updates is key; however, as prerequisites typically involve having up-to-date operating systems to begin with, you may need to take a step back and consider the best strategy for maintaining a strong security posture.

***Chapter 7***, *Managing and Maintaining the Security Posture*, goes into more detail on this critical part of strong security practices.

## Onboarding packages and installers

The **Onboarding** section in the MDE portal, accessible through <https://security.microsoft.com>, provides downloads for various onboarding packages and installers. You will want to download the relevant ones for your target operating systems and deployment tools.

## Windows

For Windows operating systems, the following options are available:

- A local onboarding script for testing purposes or manual onboarding. Note that this script requires user interaction; as such, it is not suitable for any type of automation.
- A script for use with **Group Policy**. Typically, you would set up a group policy with this script as a one-time scheduled task. This script can also be used for automated installation through any deployment tool that does not provide a native MDE onboarding capability.
- An onboarding script for use with non-persistent VDI devices. This script applies an additional configuration to the Windows device to allow you to avoid duplicate machine objects of the same name from being created in the portal. Aside from this aspect, it can be used in the same way as the group policy script.
- A **.onboarding** file containing onboarding information for use with Microsoft **Configuration Manager (ConfigMgr)**. In ConfigMgr, you would import this file into a Defender ATP policy.
- The installation package for Windows Server 2012 R2 and 2016. This package is in the standard Windows installer (**.msi**) format. Note that there is a script available on GitHub to help with automating installation and upgrades from the previous MMA-based solution.
- Workspace information for use with MMA for Windows 7, 8.1, and 2008 R2. You should use this information when setting up MMA or with a Windows Defender ATP policy inside ConfigMgr.

## *COLD SNACK*

*For virtual desktop deployments where devices can be created and destroyed in rapid succession (ephemeral or non-persistent), the recommendation is to leverage the relevant script to avoid duplication of objects. It's equally as important to onboard the machines early in the boot/startup process to make sure there is enough time to onboard before the first user session lands on the machine!*

## Linux

For Linux, you can find the following packages in the portal:

- A Python onboarding script for manual or scripted deployment. This can be used with a variety of tools and can be used with automation as it requires no user interaction.
- An archive containing a **.json** file with onboarding information for use with Puppet, Chef, and Ansible.
- For Linux, at the time of writing, the installer package is obtained through Microsoft's repositories at <https://packages.microsoft.com>. You can use your distribution's native package manager (such as yum or apt) to automatically pull the package or install it manually.

## macOS

These are the options offered in the portal for macOS:

- A Python onboarding script for manual or scripted deployment. This can be used with a variety of tools and can be used with automation as it requires no user interaction.
- A ZIP file containing onboarding files for use with Intune or JAMF.
- An installation package (**wdav.pkg**) that can either be deployed manually or through a **mobile device management (MDM)** solution.

## Mobile operating systems

Both Android and iOS packages are available from the respective platform's app stores.

## Group policy

Group policy, while not necessarily a deployment tool, can be leveraged in various ways to execute scripts and installers. As such, it does provide an opportunity for environments where there are no deployment tools available to get started with MDE on Windows.

Group policy can be used to apply onboarding scripts to machines that have shipped with MDE components; it can also be used to deploy the installation package for the modern, unified solution for Windows Server 2012 R2 and 2016.

## Intune

Intune is Microsoft's holistic device management suite of products and includes MDM capabilities through two primary products. Intune is cloud-based and Microsoft Configuration Manager (ConfigMgr) is a classic infrastructure-based solution.

## Mobile device management

Windows 10 and later, as well as macOS and mobile devices running Android and iOS, can be managed through an MDM solution. Intune is Microsoft's mobile device management solution which can, for our purposes:

- Onboard Windows 10 and 11 by applying the onboarding configuration to the built-in components
- Deploy the Defender app to macOS, Android, and iOS
- Deploy onboarding profiles and the required configuration for the Defender application to install and run

At the time of writing, Microsoft does not provide deployment or management capabilities for Linux-based operating systems.

## Microsoft Configuration Manager

ConfigMgr is a comprehensive endpoint management suite. Though Intune and ConfigMgr both allow you to configure client devices and deliver software to them, ConfigMgr also allows you to configure and deliver software to servers, deploy operating systems, and more granularly control how security updates are delivered.

ConfigMgr has built-in support for MDE deployment, onboarding, and configuration of MDE on Windows devices. For operating systems with the MDE components built in, simply download the **.onboarding** package from the MDE portal, then create a **Defender ATP Policy** to perform the onboarding.

Once deployed, you can look at the success of that deployment from the **Monitoring** section of the ConfigMgr console, as shown in *Figure 6.3*:

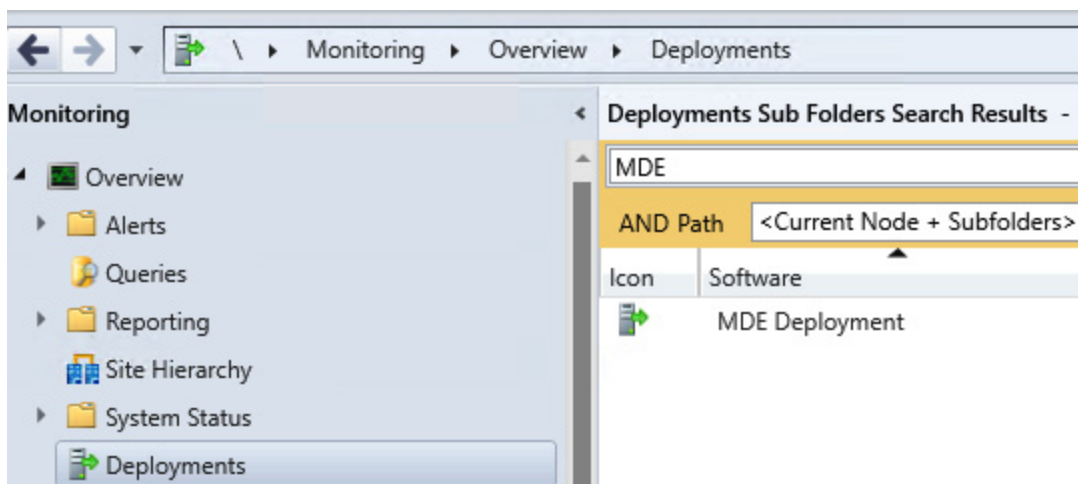


Figure 6.3 – The Monitoring section in the SCCM console

Starting with ConfigMgr Current Branch version 2207, support was added for deploying the modern, unified solution for Windows Server 2012 R2 and 2016. This requires selecting the **MDE client (recommend)** option in the client settings for **Endpoint Protection**, as shown in *Figure 6.4*:



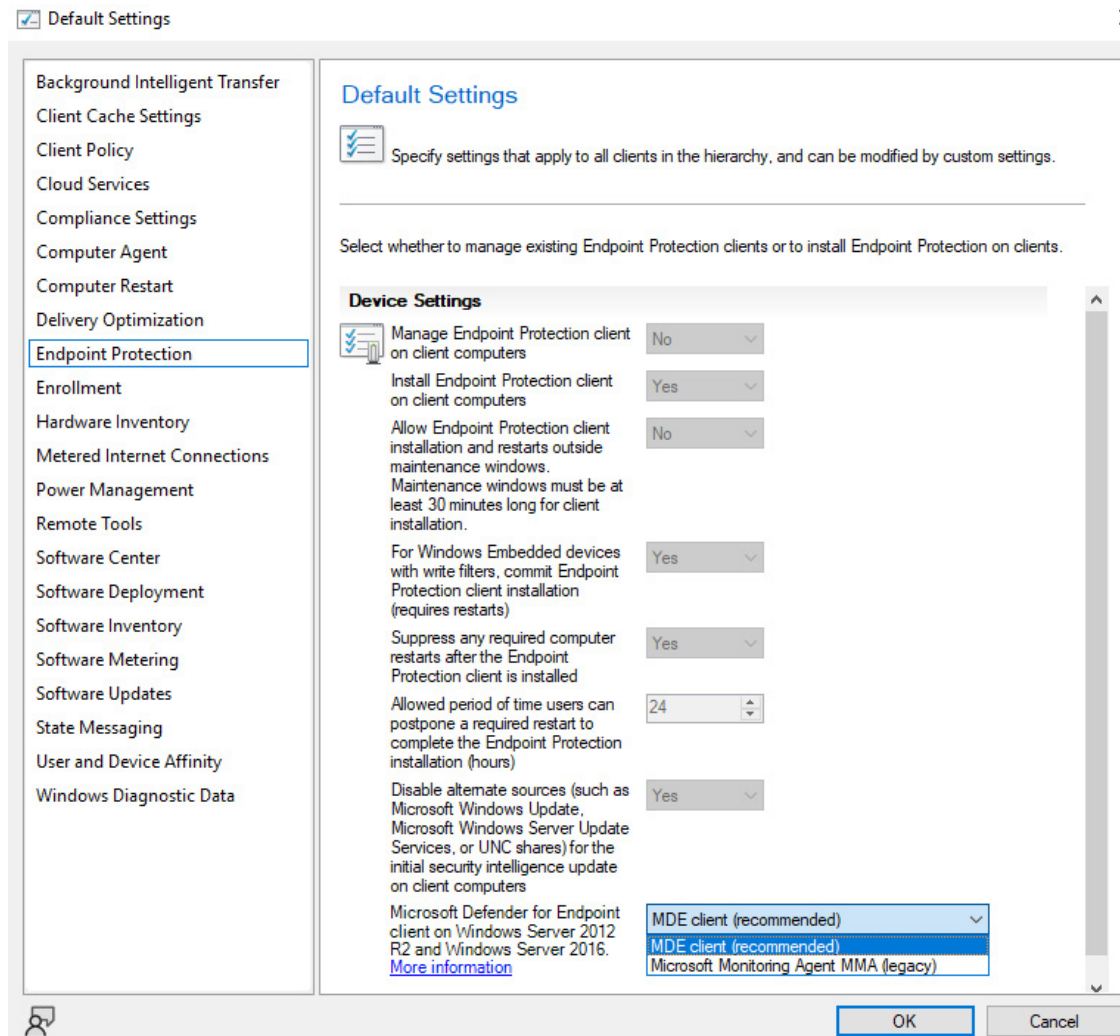


Figure 6.4 – Enabling a unified solution in SCCM

You can create a separate **Client settings** package and roll this out in a more granular fashion, or simply change the **Default Client Settings** option.

If you are running an older version of ConfigMgr, to deploy the package, you must create an application. By leveraging core ConfigMgr functionality, you can orchestrate installation and onboarding steps. The installer helper script (**install.ps1**), published on GitHub, can assist in this task. See <https://github.com/microsoft/mdefordownlevelserver> for more details.

## Microsoft Defender for Cloud

**Microsoft Defender for Cloud (MDC)** covers, among other cloud-enabled workloads such as databases, containers, cloud storage, and more, virtual server operating systems as well – you can consider it a **Cloud Native Application Protection Platform (CNAPP)**. It offers plans that contain the full MDE feature set, to extend security coverage and to offer additional capabilities for these cloud-enabled workloads. Consequently, you can use MDC to deploy and onboard MDE agents at a large scale.

## Automatic provisioning with Microsoft Defender for Servers

If you have onboarded your servers to MDC and enabled the integration with MDE, the **MDE.Windows** or **MDE.Linux** extensions will be automatically pushed. These extensions will then orchestrate the installation of MDE agents and perform onboarding. This means you do not need to download onboarding packages or installers.

For machines that are not running in an Azure subscription, it's required to install **Azure Arc** to bring them into the scope of MDC. Note that this agent comes with its own system and connectivity requirements and requires you to have an Azure subscription available.

## Azure Arc and Azure Policy's built-in initiative definitions

As an alternative to automatically provisioning the **MDE.Windows** or **MDE.Linux** extensions through MDC, it's possible to use Azure Policy's built-in initiative definitions to perform the same thing: either through the Azure VM extensions or Azure Arc (for servers not running on Azure), the **MDE.Linux** or **MDE.Windows** extensions will orchestrate installation and onboarding.

One benefit of this method, aside from automated deployment, is that it is possible to target these initiatives more granularly, such as on an Azure management group, resource group, or individual resource level.

## Other deployment methods

Aside from being able to deploy through a variety of Microsoft tools, in most cases, the installation packages and/or scripts can be used with any script-based tool – often referred to as infrastructure automation tools.

For the most popular ones – Chef, Puppet, and Ansible – Microsoft has documented how to deploy MDE to Linux machines by providing samples or *recipes*.

The unified installer package, which was published in 2022 for Windows Server 2012 R2 and 2016, also comes with a companion script that is hosted on GitHub

(<https://github.com/microsoft/mdefordownlevelserver>). This script is intended to assist with migrating from the old solution as well as handling common prerequisites and orchestrating the onboarding steps. As such, it can be used in a variety of situations, including with infrastructure automation tools or any other tool that provides a script-based deployment method – including group policy, and ConfigMgr.

After choosing a deployment tool or method, you will want to choose how to configure devices. This can be the same tool, of course, but you may have other scenarios to cover. Read on to find out what the considerations are for the various configuration options for MDE.

## Configuration management considerations

Though we handled configuration management selection in detail in [\*Chapter 5, Planning and Preparing for Deployment\*](#), we'll go ahead and discuss some of the finer points here to add additional context for consideration, especially if you're thinking about adding a net new configuration management approach.

At a high level, each possible configuration tool consists of three elements that will allow you to create a policy object, send it to the device, and apply it, at which point Defender picks it up:

- A template in an admin interface
- A management channel (service and client combination)
- A client-side interface/API

The following diagram shows a typical flow that illustrates how configuration is performed:

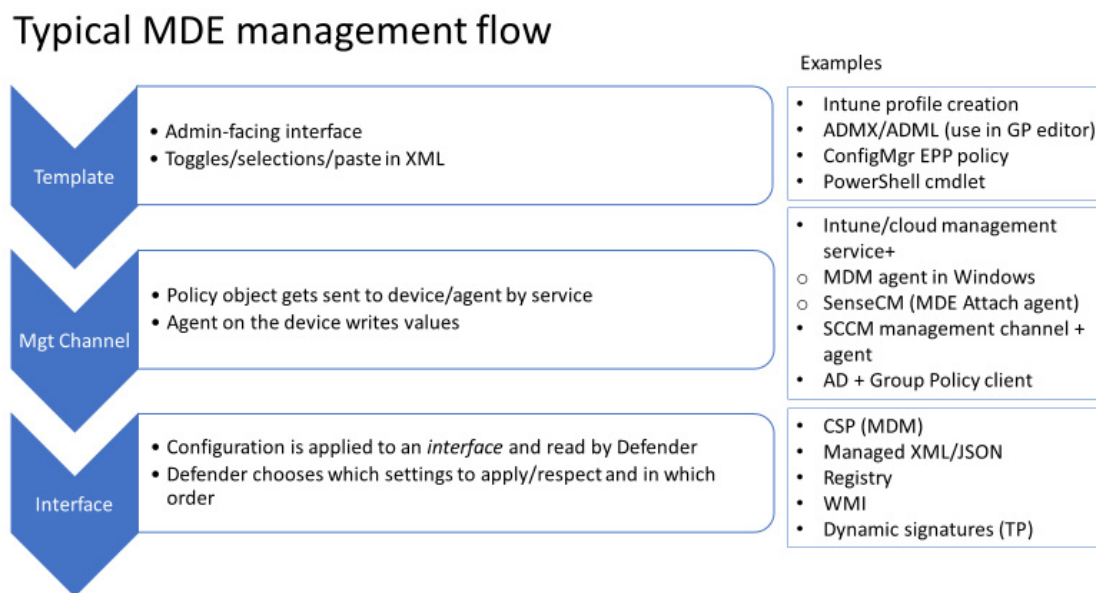


Figure 6.5 – Typical MDE management flow

While the best configuration management experience for MDE is arguably provided through the Intune **Unified Endpoint Management (UEM)** suite and the **Endpoint Security** node, you may have already invested in a configuration management platform and may find it convenient that configuration for MDE can be performed through it. In other cases, you may be used to a clearer separation between systems management teams and security management teams and are looking for a dedicated configuration experience only for MDE.

## Shell options

On Windows operating systems, PowerShell can be used to perform configuration. The most important thing to know is that all configurations applied via PowerShell are considered preferences and, as such, can be overruled by any other channel.

This is the reason configuration via PowerShell uses the **Set-MpPreference** cmdlet, which is available on all Windows operating systems from 2012 R2 (running the unified solution) onwards.

On macOS and Linux, the command-line configuration is very similar and uses **mdatp config** as the equivalent command. In the same fashion as on Windows, a managed configuration coming in would take preference over any local configuration you perform – especially if tamper protection comes into play.

Some key considerations are as follows:

- Intended for local configuration primarily (could use a form of desired state configuration such as Azure Guest Configuration with the PowerShell extension)
- Used for quickly configuring *preferences* only; a managed configuration will win
- A great way to test a setting or feature
- Easy to script a configuration or even perform actions, such as scans

The **Get-MPPreference** and **Get-MpComputerStatus** cmdlets are also incredibly useful to get the current status and configuration. For a full overview of PowerShell cmdlets, configuration items, and details about which setting does what, please look at [\*Chapter 10, Reference Guide, Tips, and Tricks\*](#).

## Group policy

Since Defender Antivirus has been a part of Windows 10 and Server 2016 and above, and many organizations have standardized the use of Active

Directory, all Defender configurations can be performed through group policies. With the modern, unified solution for Windows Server 2012 R2, the same group policy templates can also be used there. For Windows 7 SP1 and Windows Server 2008 R2, there are templates available for SCEP as well.

Some key considerations are as follows:

- This is Windows only (there are some alternative options but none of those are formally supported by Microsoft and/or MDE)
- Use the latest available group policy templates
- Requires domain-joined machines
- Many other Windows settings are available for configuration
- No clear separation of only Defender settings, so delegation in your organization may be tricky

### *COLD SNACK*

*If you are using group policy in a domain setting, typically, you would set up a central store. This will allow you to centrally configure settings in policies – from experience, many organizations do not regularly update the policy definitions (ADMX and ADML) in the central store.*

*For a modern, unified solution, you need to make sure to use the latest definitions as they contain settings that can apply all the way down to Windows Server 2012 R2. Missing a setting? Update policy definitions! They get released twice a year.*

## **Mobile Device Management (Intune)**

Let's talk about MDM. Nowadays, client operating systems (macOS and Windows 10 and later) can be managed as if they were mobile devices. The main benefits include the following:

- You can use the same tool for all client devices

- It is often cloud-based, so fits well in a modern workspace strategy where devices are not necessarily contained inside your corporate network
- In the Microsoft ecosystem, it plays very well with advanced cloud access controls in Azure AD while facilitating a **zero-trust** approach

The downside of MDM is that it is geared toward mobile devices – servers typically do not fall into this category and neither do full or virtual desktops. Regarding the latter, note that all scenarios require some tweaking to account for VDI specifics.

## Microsoft Endpoint Configuration Manager

**SMS (Systems Management Server**, not Slow-Moving Software), **Systems Center Configuration Manager (SCCM)**, MECM, and now ConfigMgr – this product has been around for many years and has probably been renamed more than Defender (but who's counting?).

Other books have been written about this family of products, and deep product understanding isn't the goal here. For educational purposes, let's zoom in only on components relevant to MDE.

As a first-party product, endpoint protection in ConfigMgr has been around as a management role, a security agent, and a separate license bundle since Forefront Endpoint Protection (2007) was introduced and later absorbed into and renamed System Center Endpoint Protection (2012). While many have their quarrels with client health, maintaining client health, or what have you, it remains one of the most robust pieces of software on the planet.

In the latest, supported version of ConfigMgr (Configuration Manager Current Branch, or CB), there is still a reference to **Endpoint Protection**. This is kind of a hybrid approach:



- The **Endpoint Protection** role provides management on top of SCEP or Defender, depending on the OS.
- Make note of the supported OS versions and the right version of ConfigMgr (CB) to manage either SCEP (2012 and above at the time of writing) or Defender (2016 and above).
- From MECM 2111 with the hotfix rollup, you can configure the unified agent.
- MECM 2207 and later also offer automated deployment of the MSI package for the unified agent.
- Tenant attach is a reference to cloud-attaching your ConfigMgr environment to Intune. For a unified MDE configuration management experience, this may be your best bet if you are already invested in on-premises ConfigMgr infrastructure.
- Co-management is another option, essentially allowing you to specify which capabilities/workloads you wish to move from ConfigMgr to Intune – with both agents active on the client system.

The process to start using Endpoint Protection to manage MDE is fairly streamlined but it's good to understand the following:

- Endpoint protection policies are generic in nature and new templates typically arrive later than group policy template updates. That said, the user interface may be considered by some to be friendlier than, for example, group policy.
- Endpoint protection policies apply to Defender protection features, not EDR (related). For EDR onboarding, you must create a **Microsoft Defender ATP** policy.
- For the unified agent, you need to select the new **MDE client** to ensure you are using the modern solution as opposed to the MMA-based one.
- ConfigMgr is holistic, meaning it is intended for all aspects of systems management. This means the functional scope is much larger than simply MDE management.

## Security management for Microsoft Defender for Endpoint



In 2022, the Defender team released a new management channel within the Intune portal called **Security management for Microsoft Defender for Endpoint**. This channel is no longer required to bring the entire system into management (meaning enrolling the device into Intune or ConfigMgr is not required for MDE configuration). Note that this also means that you can only manage MDE configuration, and nothing else, which is an important distinction as your configuration management needs may extend beyond this scope; critical areas such as patch management, user experience settings, and software deployment still require more tooling.

The experience for configuration is offered entirely through the **Endpoint Security** blade of the Intune portal at <https://endpoint.microsoft.com> and provides templates for various parts of the MDE configuration; the difference mainly consists of the channel the policy targets. This means the overall experience is the same as if you were to configure Endpoint security policies for Intune (MDM) managed devices.

The following are its benefits and constraints:

- Provides a targeted, unified experience within the **Endpoint Security** section. This can also help with tasks that have been previously delegated to the team responsible for endpoint security, which you may have traditionally separated since you might have had a separate portal for it with a third-party solution.
- Does not require enrollment into full device management. This further supports some BYOD scenarios and expands the scope of control to previously unmanaged (or otherwise managed) devices.
- Does not provide any other management capabilities you may need, such as OS patching, software deployment, and so on.
- Like Intune, it depends on Azure Active Directory for targeting purposes. This may present a tricky dynamic if you are in a multi-org situation.

This section covered the available options for configuring the various components of MDE; most of them can get the job done but you need to consider which tool is the fittest for your purpose within your organization's dynamic.

## Summary

If you only use detection and response capabilities in MDE, you likely would not be configuring a lot of settings on your endpoints. Typically, you may have sufficient controls available in the MDE portal and use a management solution from your current antimalware vendor.

If you are using the full MDE stack, which is highly recommended, in this chapter, you will have learned that Microsoft has ensured you can use whatever existing deployment and configuration tools that may already be available in your environment. For operating systems where the MDE components are built in, such as modern Windows, you may only need to perform onboarding; this works out well. Minimal effort is needed. For other operating systems, or if you need to perform advanced configuration, you will want to select a tool that is more geared toward systems management, such as Intune or Configuration Manager. However, the endpoint security-tailored experience is also available for a more focused experience.

Now that you have configured your portal and have the information needed to select a tool for deployment and configuration, you will want to start deploying to production. The guidance provided in [\*Chapter 7, Managing and Maintaining the Security Posture\*](#), will help you successfully operationalize MDE.