Microsoft Defender for Endpoint

Master Class

Trainer DI Thomas Schleich

November 2024

1

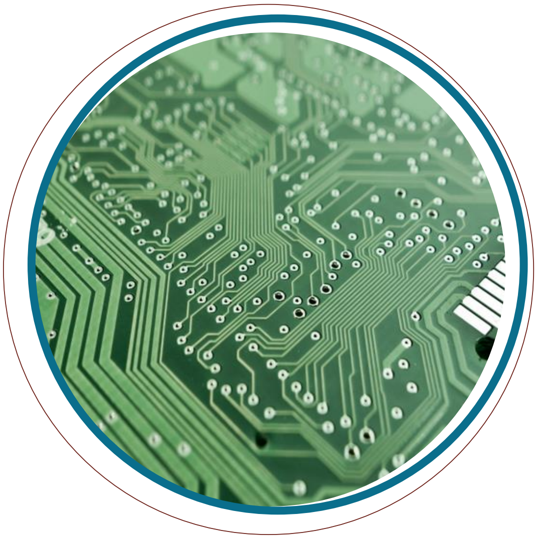
Module 2

Device Onboarding

2

Module 2 Contents:

- **Windows 10/11**
  - Local Script
  - Intune
  - GPO
- **Azure VM**
- **On-prem Server**
- **Device discovery**
- **Non-Windows devices**
- **Offboarding**



Onboarding

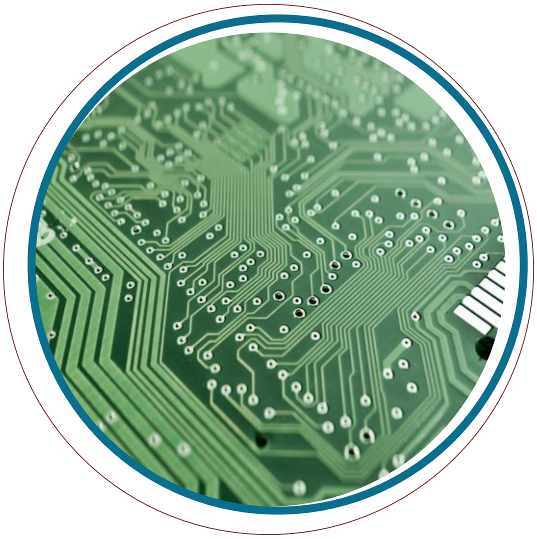
Requirements

Source: https://learn.microsoft.com/en-us/defender-endpoint/configure-environment

Onboarding

Requirements

- OS Versions
  - sometimes necessary updates
- Network connectivity
  - Documentation
  - Streamlined (consolidated URLs)
  - Spreadsheet(s)

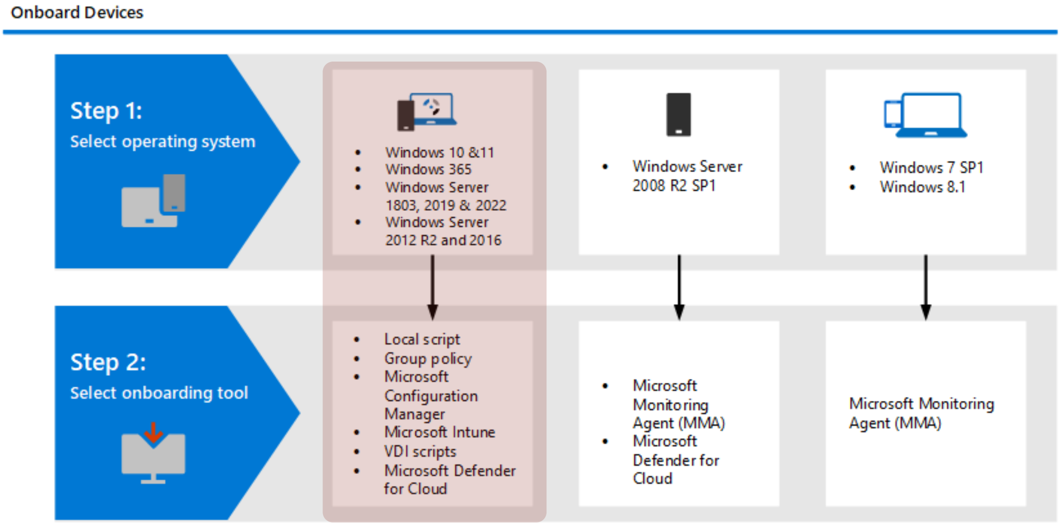


Onboarding

Windows

Source: https://learn.microsoft.com/en-us/defender-endpoint/onboard-windows-client

Onboarding Windows Systems



Onboard Devices

Step 1: Select operating system

- Windows 10 &11
- Windows 365
- Windows Server 1803, 2019 & 2022
- Windows Server 2012 R2 and 2016

- Windows Server 2008 R2 SP1

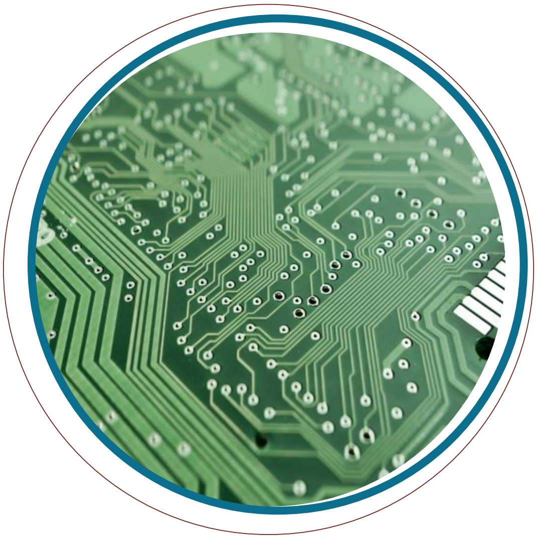
- Windows 7 SP1
- Windows 8.1

Step 2: Select onboarding tool

- Local script
- Group policy
- Microsoft Configuration Manager
- Microsoft Intune
- VDI scripts
- Microsoft Defender for Cloud

- Microsoft Monitoring Agent (MMA)
- Microsoft Defender for Cloud

Microsoft Monitoring Agent (MMA)



Onboarding

Windows 10/11

Source: https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-reduction

Local Script

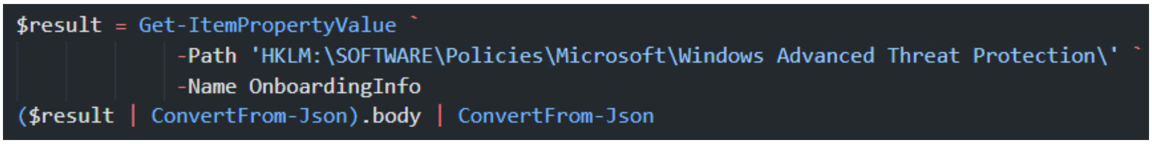
Procedure:

1. Settings | Endpoints | Device Management/Onboarding
2. Select OS: 'Windows 10 or 11'
3. Connectivity type: Streamlined
4. Deployment method: Local Script
5. Click 'Download onboarding script'
6. Copy the script to the new client and extract it there
7. Start the script as administrator and follow the instructions

Local Script

What the script is doing

- Check if elevated
- Adds some registry values
  - WMI permissions for Security Center
  - Onboarding Info



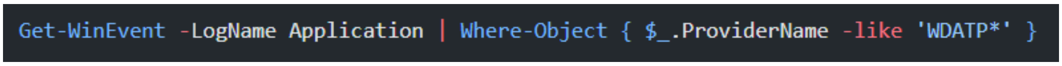
```
$result = Get-ItemPropertyValue `
            -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection\' `
            -Name OnboardingInfo
($result | ConvertFrom-Json).body | ConvertFrom-Json
```

  - orgID could be found in XDR Settings

Local Script

What the script is doing - continued

- ELAM driver installation
- Starting service SENSE
- Creating Event in Application Log
  - Source/ProviderName: WDATPOnboarding
  - EventID: 20



```
Get-WinEvent -LogName Application | Where-Object { $_.ProviderName -like 'WDATP*' }
```

- Reload engine

Group Policy objects

- suitable for ADDS Members

- Higher level steps
- Download Onboarding package for Group policies
  - script is step-by-step local onboarding script
  - just no confirmation and output
- Extract script to an accessible file share
- Create a GPO and create a scheduled task via preferences
- Action of this task downloads the scipt and executes it

Refer to this step-by-step guide

Microsoft Intune

- suitable for already in Intune enrolled devices

High level steps

- Establish a service-to-service connection
  - between Intune and MDE
- Create a policy for onboarding
  - Device configuration policy or
  - EDR policy

Source: https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-onboarding#troubleshoot-onboarding-when-deploying-with-a-script
https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-onboarding#view-agent-onboarding-errors-in-the-device-event-log

Troubleshooting

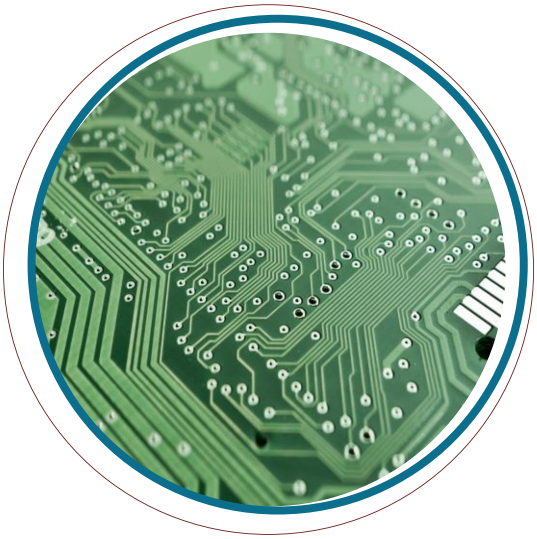
Windows

Problems executing script

- Event Viewer - Application Log
  - Source **WDATPOnboarding**

Problems performing onboarding process

- Event Viewer - Applications and Services Logs > Microsoft > Windows > SENSE
  - Filter for Warning, Error and Critical



Onboarding

Azure VM

Azure VM

- Virtual Machines running in Azure
- Microsoft Defender for Cloud (MDC)
  - allows you to configure MDE protection
  - includes licenses

Microsoft Defender for Cloud - 2 main parts

Cloud Security Posture Management

- Secure Score
- Recommendations
- Regulatory Compliance

Microsoft Defender for Cloud
Unify your DevOps Security Management
Strengthen and manage your cloud security posture
Protect your cloud workloads
aws

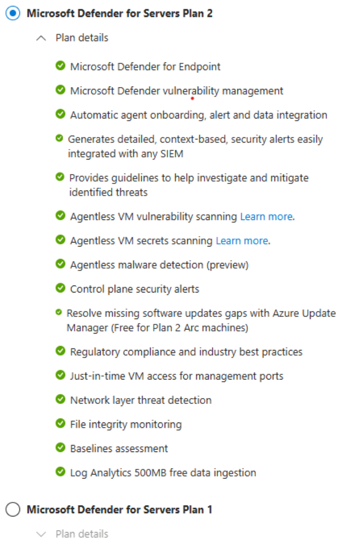
Cloud Workload Protection Platform

Defender for

- Servers
- App Services
- Databases
- Storage
- Containers
- Key Vault
- Resource Manager
- APIs

Source: Support for the Defender for Servers plan in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

Microsoft Defender for Servers



● Microsoft Defender for Servers Plan 2

Plan details

- ✓ Microsoft Defender for Endpoint
- ✓ Microsoft Defender vulnerability management
- ✓ Automatic agent onboarding, alert and data integration
- ✓ Generates detailed, context-based, security alerts easily integrated with any SIEM
- ✓ Provides guidelines to help investigate and mitigate identified threats
- ✓ Agentless VM vulnerability scanning Learn more.
- ✓ Agentless VM secrets scanning Learn more.
- ✓ Agentless malware detection (preview)
- ✓ Control plane security alerts
- ✓ Resolve missing software updates gaps with Azure Update Manager (Free for Plan 2 Arc machines)
- ✓ Regulatory compliance and industry best practices
- ✓ Just-in-time VM access for management ports
- ✓ Network layer threat detection
- ✓ File integrity monitoring
- ✓ Baselines assessment
- ✓ Log Analytics 500MB free data ingestion

○ Microsoft Defender for Servers Plan 1

Plan details

Features

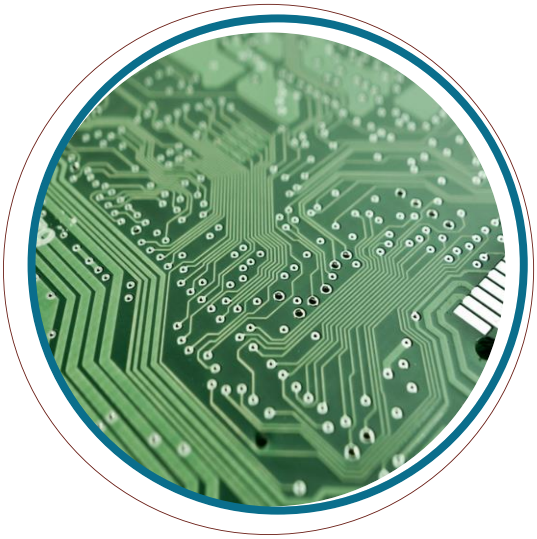
- **MDE in both plans available**
- OS Support
  - Windows Server 2022, 2019, 2016, 2012 R2, 2008 R2 SP1, Windows 10/11 Enterprise multi-session (formerly Enterprise for Virtual Desktops)
  - Not available on: Azure VMs running Windows 10 or Windows 11
- *For Azure VM with Windows 11/10 use already explained onboarding methods*

Source: https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-agents#defender-for-endpoint-extensions
https://learn.microsoft.com/en-us/defender-endpoint/minimum-requirements
https://learn.microsoft.com/en-us/defender-endpoint/configure-server-endpoints#windows-server-2016-and-windows-server-2012-r2

Microsoft Defender for Servers

MDE protection

- Azure VMs are automatically onboarded to MDE
  - Extension MDE.Windows or MDE.Linux is installed
  - Connection to *.endpoint.security.microsoft.com* is mandatory
- All requirements of a Windows Server to be onboarded to MDE must be fulfilled.
- MDE must be activated already



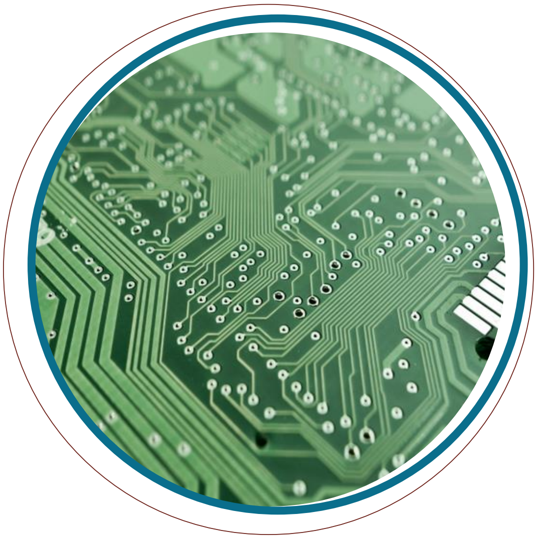
Onboarding

On-premises Servers or VMs

Other Servers

- Server could be hosted
  - on-premises physical
  - on-premises virtual
  - in 3rd party clouds

- Onboard directly (if OS is supported)
- Use Azure Arc
  - install the connected machine agent (CMA) on that servers
  - automatically protected by Defender for Cloud (Servers)
  - therefor automatically onboarded to MDE



Onboarding

Device discovery

Source: https://learn.microsoft.com/en-us/defender-endpoint/device-discovery

Device discovery

- '… *helps you find unmanaged devices connected to your corporate network without the need for extra appliances or cumbersome process changes.*'
- onboarded devices are used for discovery
- Could be found:
  - Endpoints (workstations, server and mobile devices)
  - Network devices (routers, switches)
  - IoT (printers, cameras, …)

Source: https://learn.microsoft.com/en-us/defender-endpoint/device-discovery

Device discovery

Discovery methods

- Basic
  - SenseNDR.exe
  - passive; network traffic seen by onboarded device is investigated
  - no network traffic initiated
- Standard
  - actively find devices
  - common discovery protocols using multicast queries are used
  - minimal and negligible activity generated

Source: https://learn.microsoft.com/en-us/defender-endpoint/device-discovery
https://learn.microsoft.com/en-us/defender-endpoint/network-devices

Device discovery

Discovered devices onboarding states

- Onboarded
- Can be onboarded
- Unsupported
- Insufficient info

- Check device inventory (Assets | Devices/Computers & Mobile)

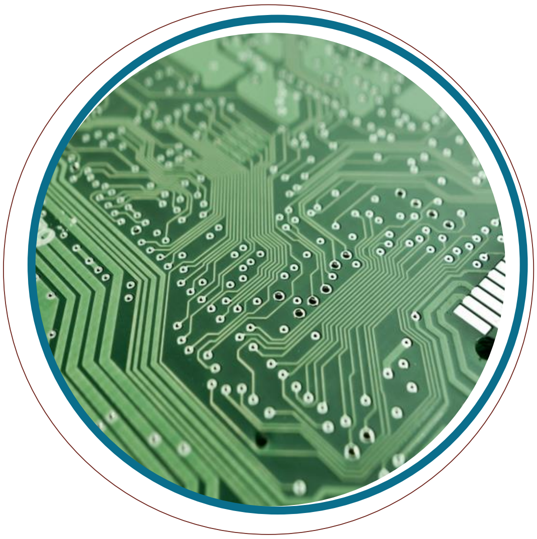
Network devices

- Download and configure scanner
- Check device inventory (Assets | Devices/Network devices)

Device discovery

Configuration

- Settings | Endpoints | Adv Features | Device discovery (on default)
- Settings | Device discovery
- Discovery setup
  - Select mode (Basic/Standard)
  - Select already onboarded devices which should discover
- Exclusions
  - Provide IP addresses and/or ranges of devices to exclude
- Monitored Network
  - Corporate networks vs. non-corporate networks
  - each found network could be excluded / included



Onboarding

Linux

Source: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint-linux

Onboarding Linux endpoints

System requirements - refer to source

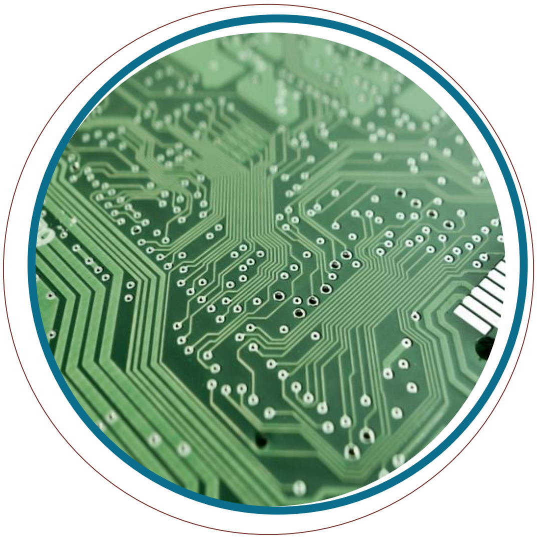
- Disk space > 2GB
- Cores: 2 (4 preferred)
- Memory: 1GB (4GB preferred)
- supported distribution
- supported filesystem
- auditd must be enabled
- executable permission for wdavdaemon
- package dependencies

Source: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint-linux
https://learn.microsoft.com/en-us/defender-endpoint/linux-install-manually

Onboarding Linux endpoints

Onboarding - refer to source

- manually
- Using (all documented by Microsoft)
  - Puppet
  - Ansible
  - Chef
  - Saltstack



Onboarding

MacOS

Source: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint-mac
https://learn.microsoft.com/en-us/defender-endpoint/mac-install-manually

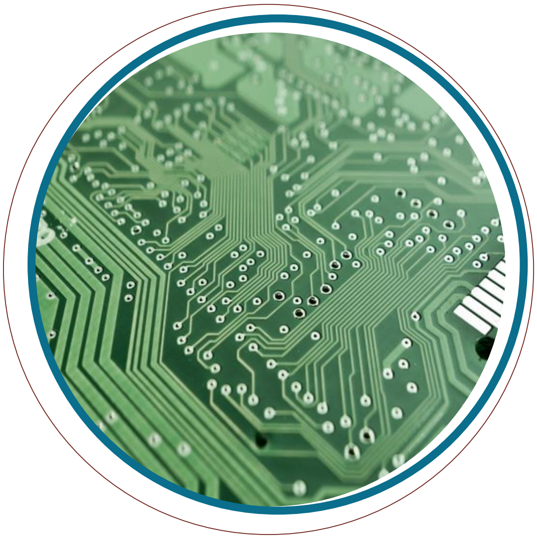
Onboarding macOS endpoints

System requirements - refer to source

- Disk space > 1GB
- supported OS: v12 and later
- Beta versions are not supported (!)

Onboarding

- manually
- Intune
- Non-Microsoft
  - JAMF
  - 3rd party MDM



Onboarding

iOS/iPadOS

Source: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint-mac
https://learn.microsoft.com/en-us/defender-endpoint/mac-install-manually

Onboarding

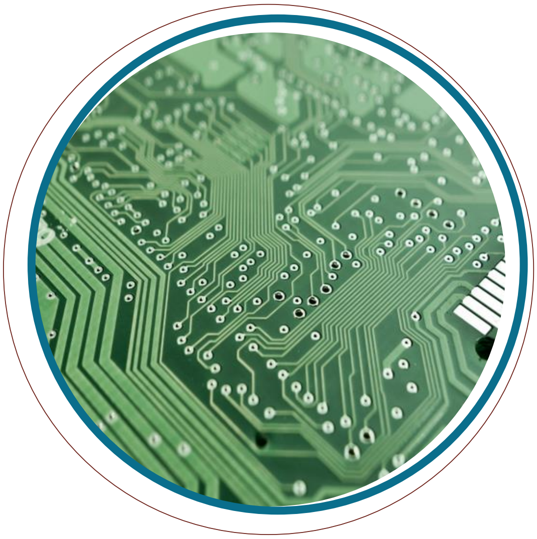
iOS/iPadOS

best with Intune enrolled devices

- Deploy Microsoft Defender App from Apple Store
  - via Intune policy

with non-enrolled devices

- Install Microsoft Authenticator and sign in to your account
- Install Microsoft Defender App and sign in with same account
- only Web protection available - later more …



Onboarding

Android

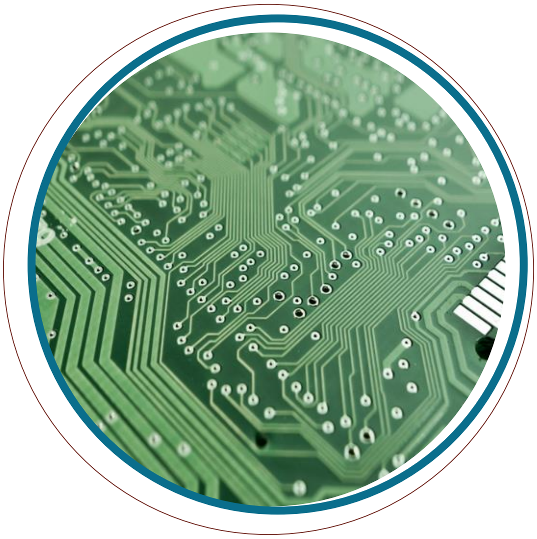
Source: https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint-mac
https://learn.microsoft.com/en-us/defender-endpoint/mac-install-manually

Onboarding

Android

- best with Intune enrolled devices
- non-enrolled devices supported now

- Install Company Portal app for Google Play



Offboarding

Offboarding

Windows

- Download script/package
  - local script; GPO; Intune; Config Manager
- valid for 7 days

- Deployment guide could be found in documentation where onboarding is explained

Source: https://learn.microsoft.com/en-us/defender-endpoint/overview-attack-surface-reduction

Offboarding Script

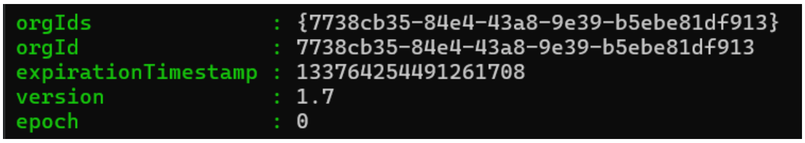
Procedure:

1. Settings | Endpoints | Device Management/Onboarding
2. Select OS: 'Windows 10 or 11'
3. Deployment method: Local Script
4. Click 'Download package'
5. Copy the script to the new client and extract it there
6. Start the script as administrator and follow the instructions

Offboarding Script

What the script is doing

- Check if elevated
- Querying Org Id from registry
  - check if Org Id is correct
- current Onboarding Info in registry deleted
- New value is added: 696C1FA1-4030-4FA4-8713-FAF9B2EA7C0A
  - Content similar to this:



```
orgIds              : {7738cb35-84e4-43a8-9e39-b5ebe81df913}
orgId               : 7738cb35-84e4-43a8-9e39-b5ebe81df913
expirationTimestamp : 133764254491261708
version             : 1.7
epoch               : 0
```

- 'Windows Defender Advanced Threat Protection Service' stopped

End of Module 2