# Windows 11 Security

HOW TO SETUP A SECURE WINDOWS 11 ENDPOINT

Security for all

# Powerful security, from chip to cloud

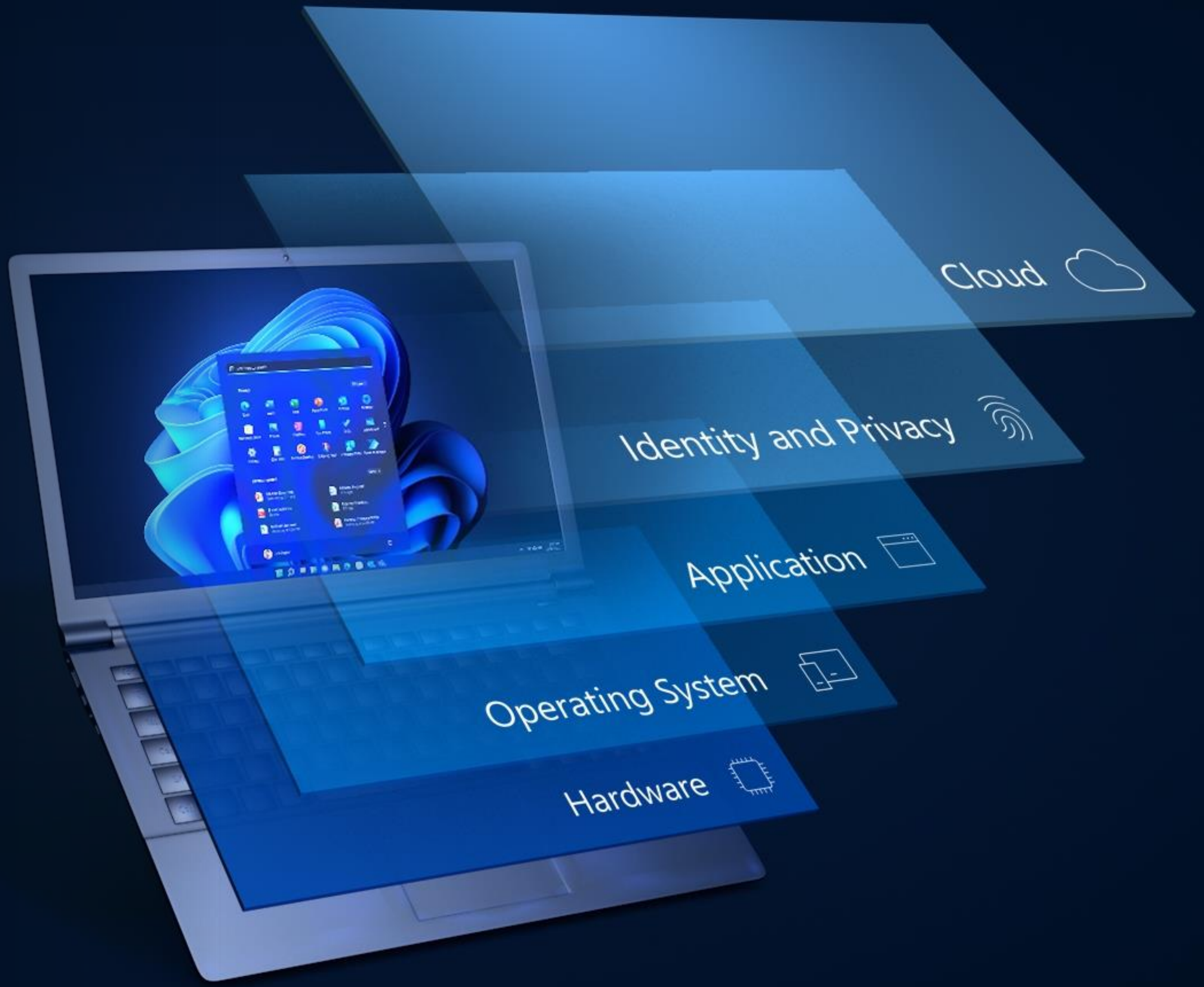
Our customers need modern security solutions that deliver end-to-end protection anywhere. Windows 11 is built with Zero Trust principles for the new era of hybrid work.

# Security by default

## Windows 11 delivers powerful protection from chip to cloud

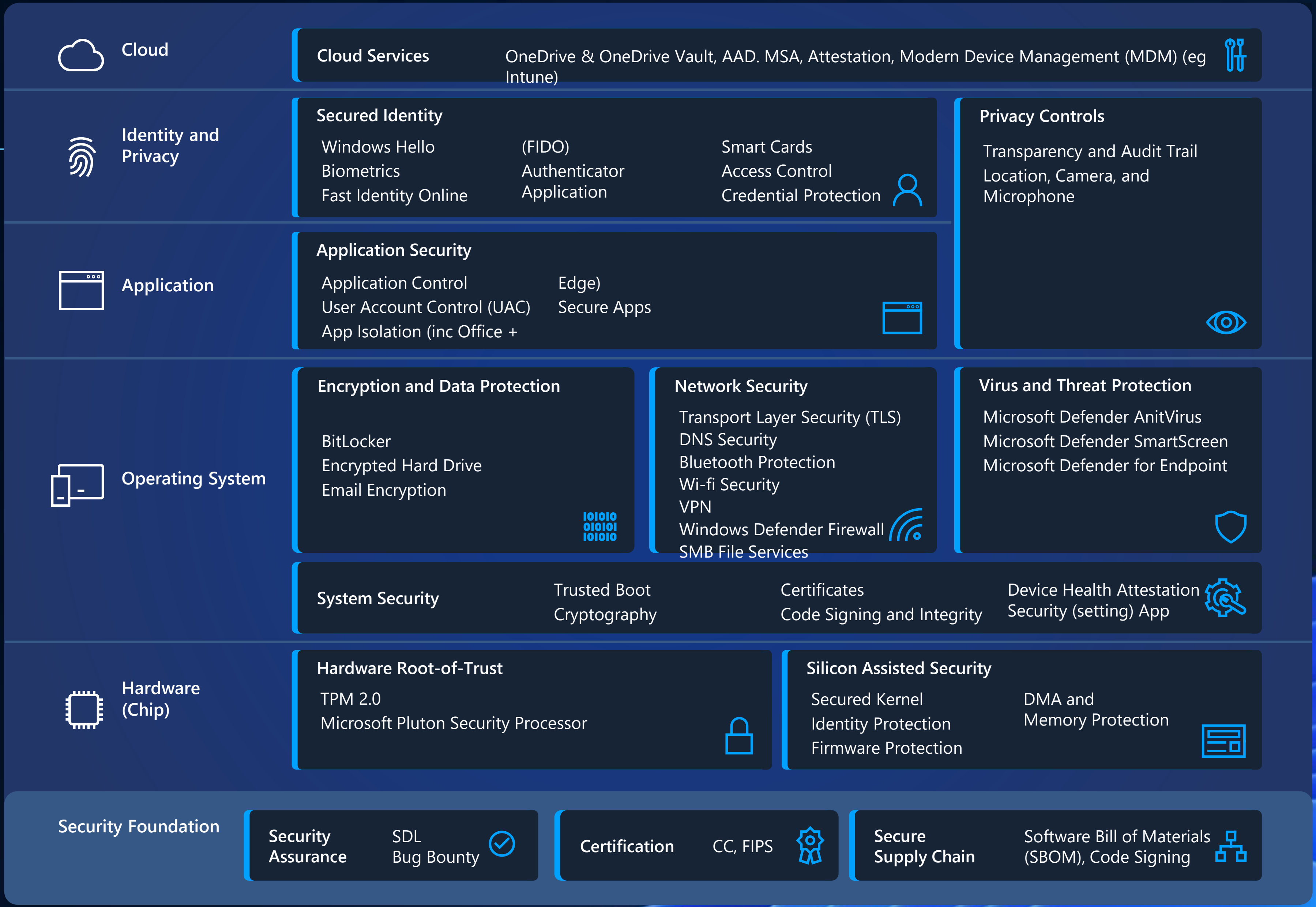
In Windows 11, hardware and software security work together to help keep users, data, and devices protected.

- Protects against threats by separating hardware from software with **hardware root-of-trust**, for powerful security from the start
- **Protect the OS against unauthorized access** to critical data
- Delivers **robust application security** and prevents access to unverified code
- **Protects user identities** with passwordless security
- **Extends security to the cloud** to help protect devices, data, apps, and identities from anywhere



# Security Overview

In Windows 11, hardware and software work together for protection from the CPU all the way to the cloud.



## Cloud

**Cloud Services**
OneDrive & OneDrive Vault, AAD. MSA, Attestation, Modern Device Management (MDM) (eg Intune)

## Identity and Privacy

**Secured Identity**
Windows Hello
Biometrics
Fast Identity Online
(FIDO)
Authenticator
Application
Smart Cards
Access Control
Credential Protection

**Privacy Controls**
Transparency and Audit Trail
Location, Camera, and Microphone

## Application

**Application Security**
Application Control
User Account Control (UAC)
App Isolation (inc Office +
Edge)
Secure Apps

## Operating System

**Encryption and Data Protection**
BitLocker
Encrypted Hard Drive
Email Encryption

**Network Security**
Transport Layer Security (TLS)
DNS Security
Bluetooth Protection
Wi-fi Security
VPN
Windows Defender Firewall
SMB File Services

**Virus and Threat Protection**
Microsoft Defender AnitVirus
Microsoft Defender SmartScreen
Microsoft Defender for Endpoint

**System Security**
Trusted Boot
Cryptography
Certificates
Code Signing and Integrity
Device Health Attestation
Security (setting) App

## Hardware (Chip)

**Hardware Root-of-Trust**
TPM 2.0
Microsoft Pluton Security Processor

**Silicon Assisted Security**
Secured Kernel
Identity Protection
Firmware Protection
DMA and Memory Protection

## Security Foundation

**Security Assurance**
SDL
Bug Bounty

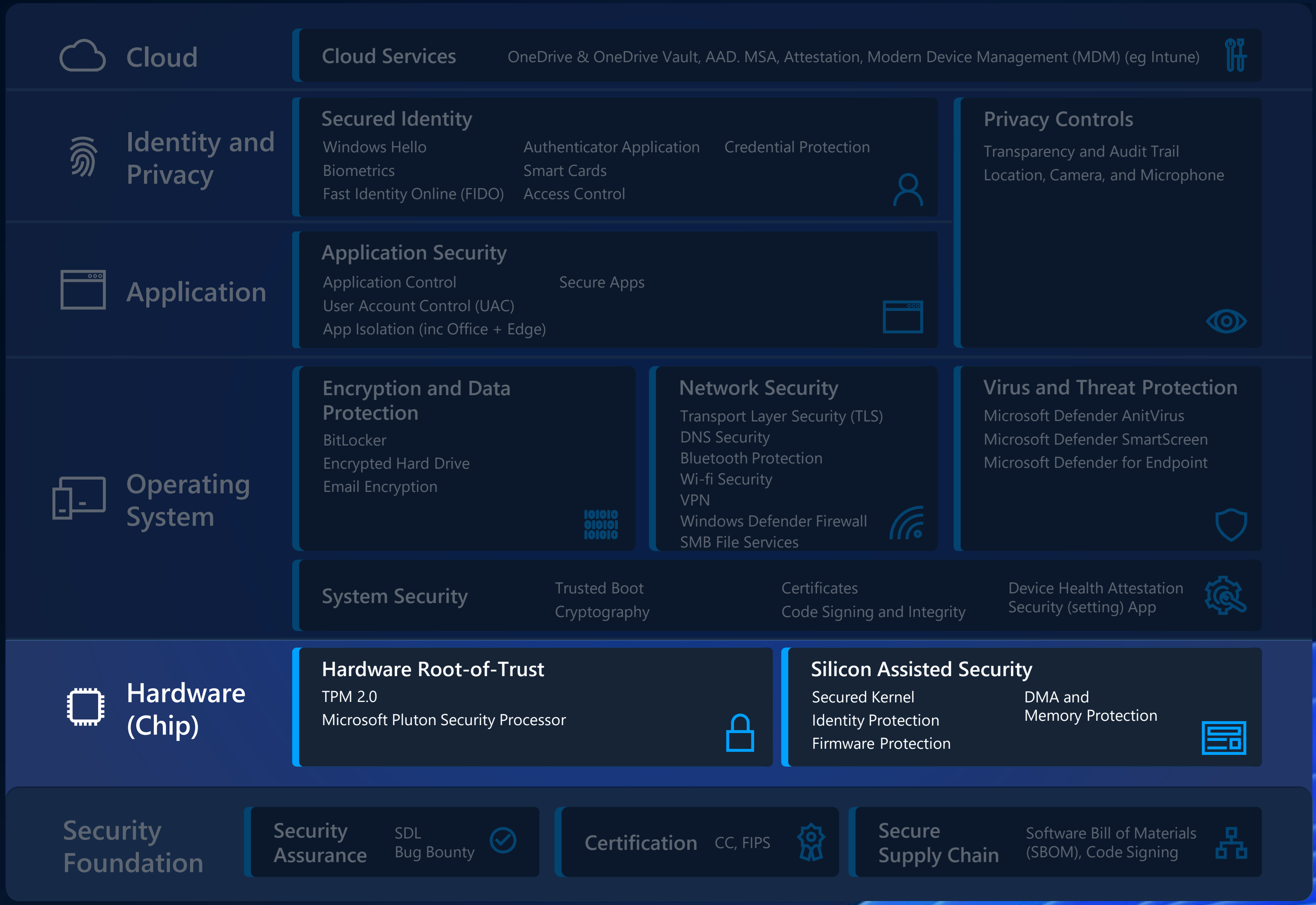
**Certification**
CC, FIPS

**Secure Supply Chain**
Software Bill of Materials (SBOM), Code Signing

# Hardware Overview

Through a powerful combination of hardware root-of-trust and silicon-assisted security, Windows 11 delivers built-in hardware protection out-of-the box.

- **Protects and maintains system integrity** as the firmware loads.
- **Strengthens security** for features like Windows Hello and BitLocker with TPM 2.0.
- **Protects code integrity and critical information** with virtualization-based security (VBS).



Cloud

Cloud Services — OneDrive & OneDrive Vault, AAD. MSA, Attestation, Modern Device Management (MDM) (eg Intune)

Identity and Privacy

Secured Identity
Windows Hello
Biometrics
Fast Identity Online (FIDO)
Authenticator Application
Smart Cards
Access Control
Credential Protection

Privacy Controls
Transparency and Audit Trail
Location, Camera, and Microphone

Application

Application Security
Application Control
User Account Control (UAC)
App Isolation (inc Office + Edge)
Secure Apps

Operating System

Encryption and Data Protection
BitLocker
Encrypted Hard Drive
Email Encryption

Network Security
Transport Layer Security (TLS)
DNS Security
Bluetooth Protection
Wi-fi Security
VPN
Windows Defender Firewall
SMB File Services

Virus and Threat Protection
Microsoft Defender AnitVirus
Microsoft Defender SmartScreen
Microsoft Defender for Endpoint

System Security
Trusted Boot
Cryptography
Certificates
Code Signing and Integrity
Device Health Attestation
Security (setting) App

Hardware (Chip)

Hardware Root-of-Trust
TPM 2.0
Microsoft Pluton Security Processor

Silicon Assisted Security
Secured Kernel
Identity Protection
Firmware Protection
DMA and Memory Protection

Security Foundation

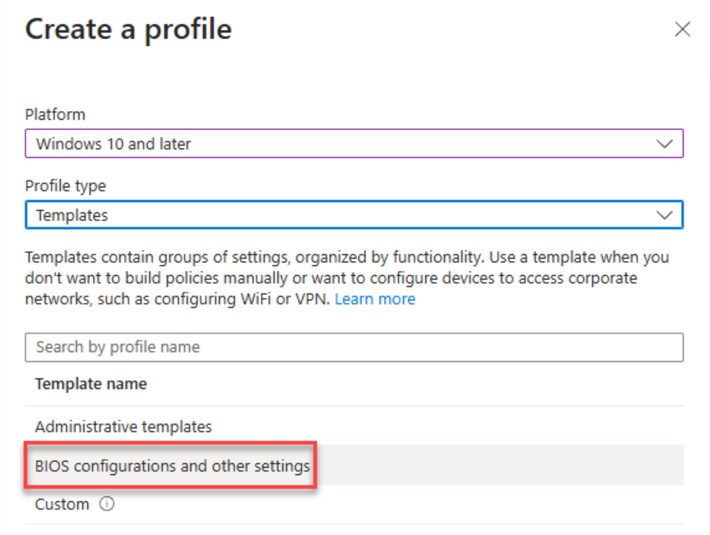
Security Assurance — SDL, Bug Bounty

Certification — CC, FIPS

Secure Supply Chain — Software Bill of Materials (SBOM), Code Signing

# BIOS Configuration using Intune

- Currently for Dell only
- Process:
  - Create UEFI (BIOS) Config File using OEM tooling
  - Install OEM Win32 App on devices using Intune
  - Create UEFI (BIOS) Configuration policy in Intune
  - Assign policy to devices
- BIOS Passwords
  - Should be blank initially
  - Are set by Intune as configured in the policy
  - Passwords are stored in Intune (and accessible via Graph)



Create a profile

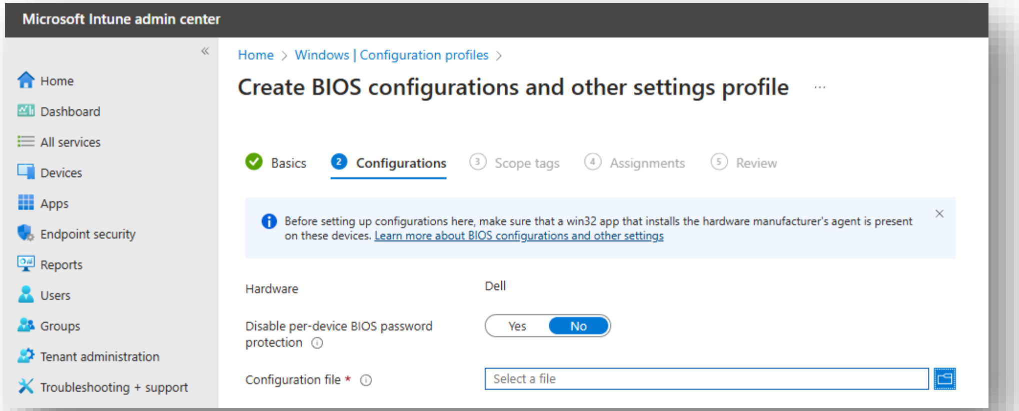
Platform: Windows 10 and later

Profile type: Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

Search by profile name

| Template name |
|---|
| Administrative templates |
| BIOS configurations and other settings |
| Custom ⓘ |



Home > Windows | Configuration profiles >

Create BIOS configurations and other settings profile

Before setting up configurations here, make sure that a win32 app that installs the hardware manufacturer's agent is present on these devices. Learn more about BIOS configurations and other settings

Hardware: Dell

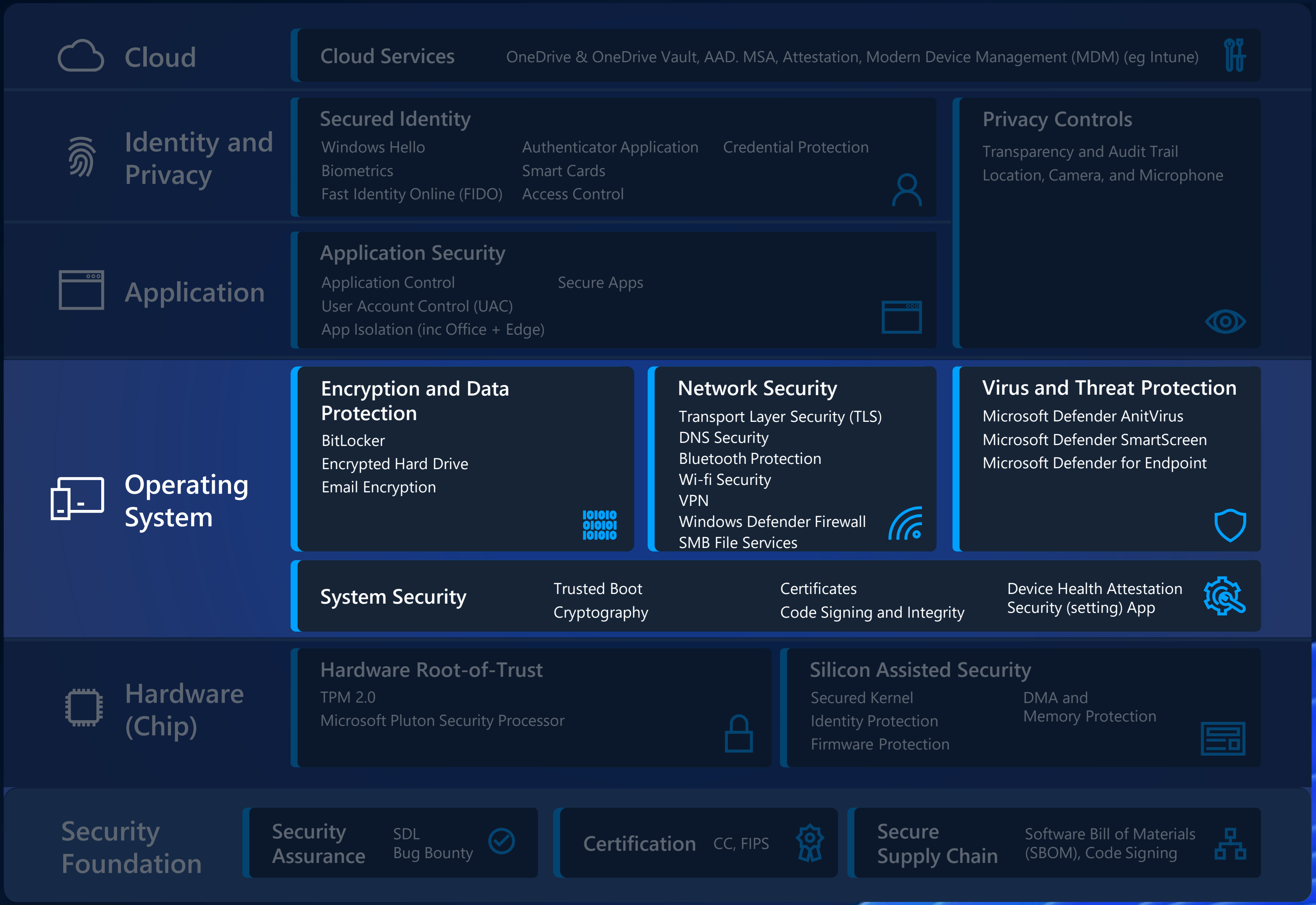
Disable per-device BIOS password protection ⓘ: Yes [✓ No]

Configuration file * ⓘ: Select a file

# Operating System Overview

In Windows 11, hardware and software work together to protect the operating system.

- **Reduces risk of lost or stolen data** with advanced encryption in BitLocker[1] and Windows Information Protection[2]
- **Strengthens network security** with multiple layers of protection.
- **Delivers intelligent protection** against viruses and other threats.
- **Powerful system security** safeguards credentials, code integrity, and network access.



Cloud

Cloud Services
OneDrive & OneDrive Vault, AAD. MSA, Attestation, Modern Device Management (MDM) (eg Intune)

Identity and Privacy

Secured Identity
Windows Hello
Biometrics
Fast Identity Online (FIDO)
Authenticator Application
Smart Cards
Access Control
Credential Protection

Privacy Controls
Transparency and Audit Trail
Location, Camera, and Microphone

Application

Application Security
Application Control
User Account Control (UAC)
App Isolation (inc Office + Edge)
Secure Apps

Operating System

Encryption and Data Protection
BitLocker
Encrypted Hard Drive
Email Encryption

Network Security
Transport Layer Security (TLS)
DNS Security
Bluetooth Protection
Wi-fi Security
VPN
Windows Defender Firewall
SMB File Services

Virus and Threat Protection
Microsoft Defender AnitVirus
Microsoft Defender SmartScreen
Microsoft Defender for Endpoint

System Security
Trusted Boot
Cryptography
Certificates
Code Signing and Integrity
Device Health Attestation
Security (setting) App

Hardware (Chip)

Hardware Root-of-Trust
TPM 2.0
Microsoft Pluton Security Processor

Silicon Assisted Security
Secured Kernel
Identity Protection
Firmware Protection
DMA and Memory Protection

Security Foundation

Security Assurance
SDL
Bug Bounty

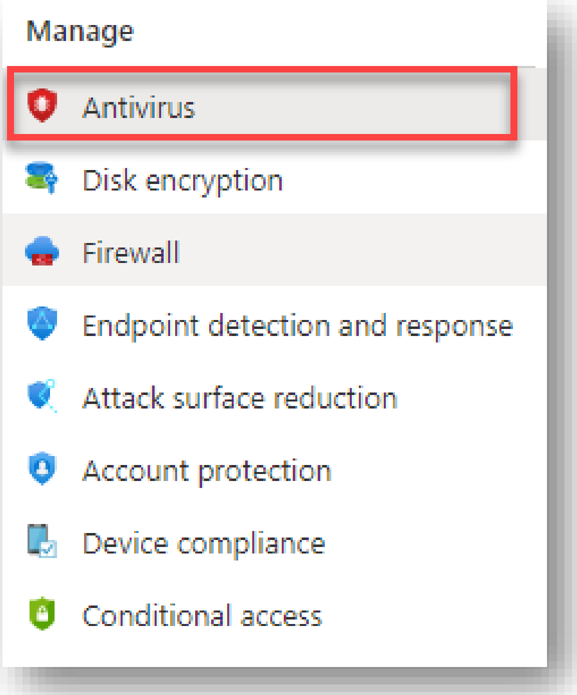
Certification
CC, FIPS

Secure Supply Chain
Software Bill of Materials (SBOM), Code Signing

[1] Requires TPM 2.0
[2] Windows Information Protection requires either Mobile Device Management or System Center Configuration Manager to manage settings. These products are sold separately. Active Directory makes management easier but is not required.

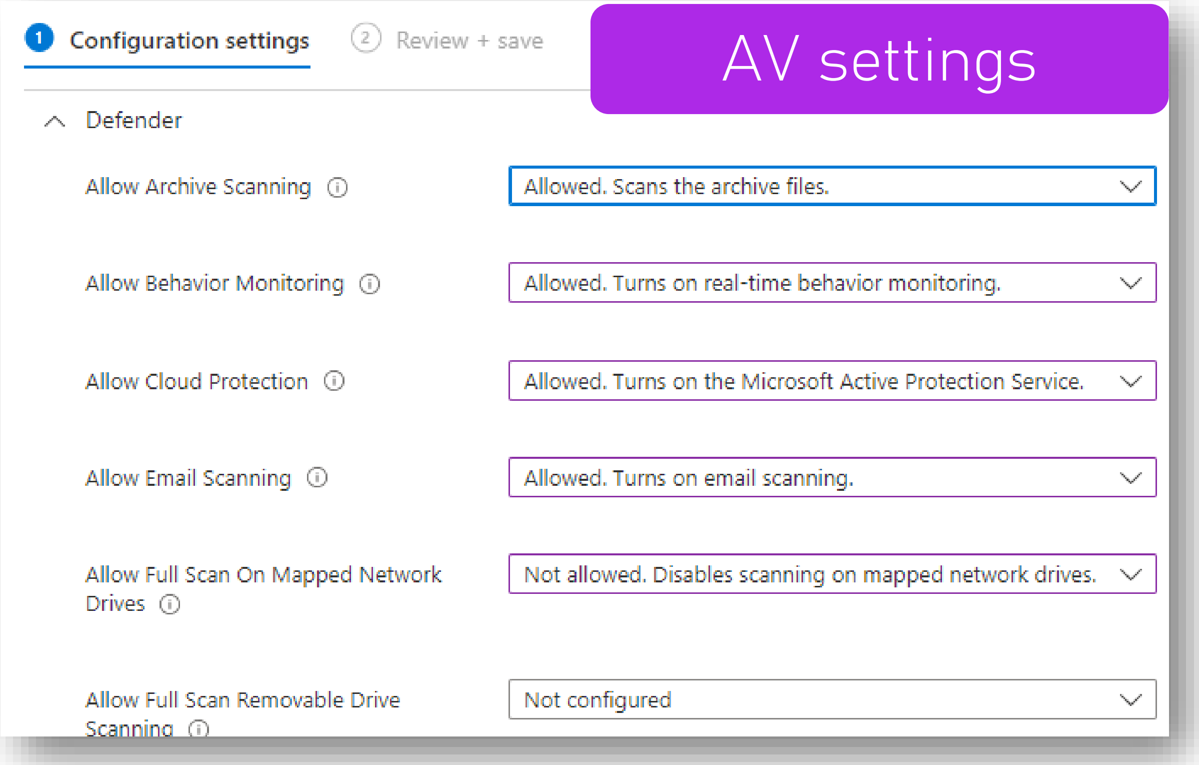
# Antivirus Profile

- Configures Defender Update Controls
- Configures Defender AV Exclusions
- Configure Defender AV
- Configures the Windows Security Exp



Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access



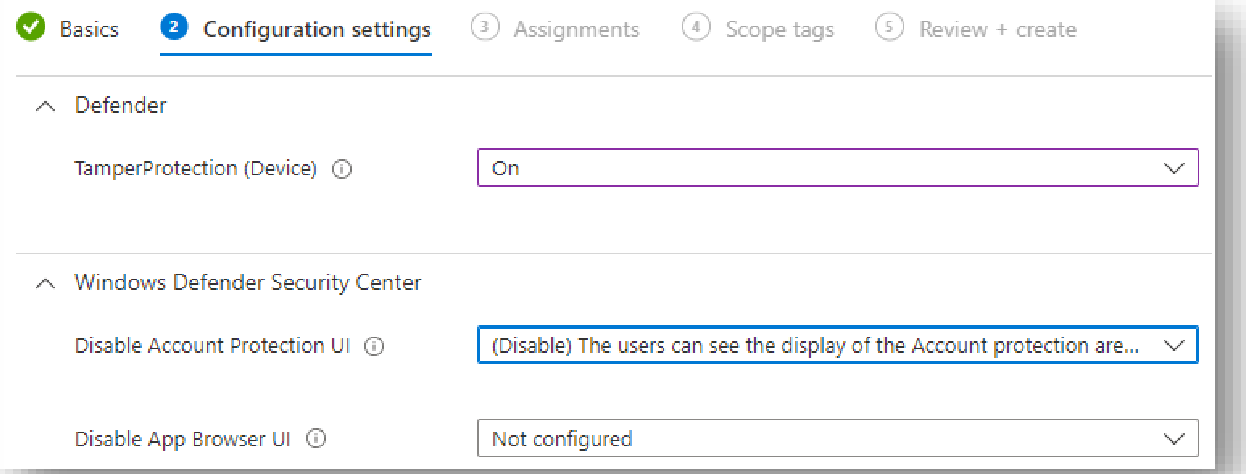
AV settings

1 Configuration settings · 2 Review + save

Defender

| Setting | Value |
|---|---|
| Allow Archive Scanning ⓘ | Allowed. Scans the archive files. |
| Allow Behavior Monitoring ⓘ | Allowed. Turns on real-time behavior monitoring. |
| Allow Cloud Protection ⓘ | Allowed. Turns on the Microsoft Active Protection Service. |
| Allow Email Scanning ⓘ | Allowed. Turns on email scanning. |
| Allow Full Scan On Mapped Network Drives ⓘ | Not allowed. Disables scanning on mapped network drives. |
| Allow Full Scan Removable Drive Scanning ⓘ | Not configured |

Security app settings



✓ Basics · 2 Configuration settings · 3 Assignments · 4 Scope tags · 5 Review + create

Defender

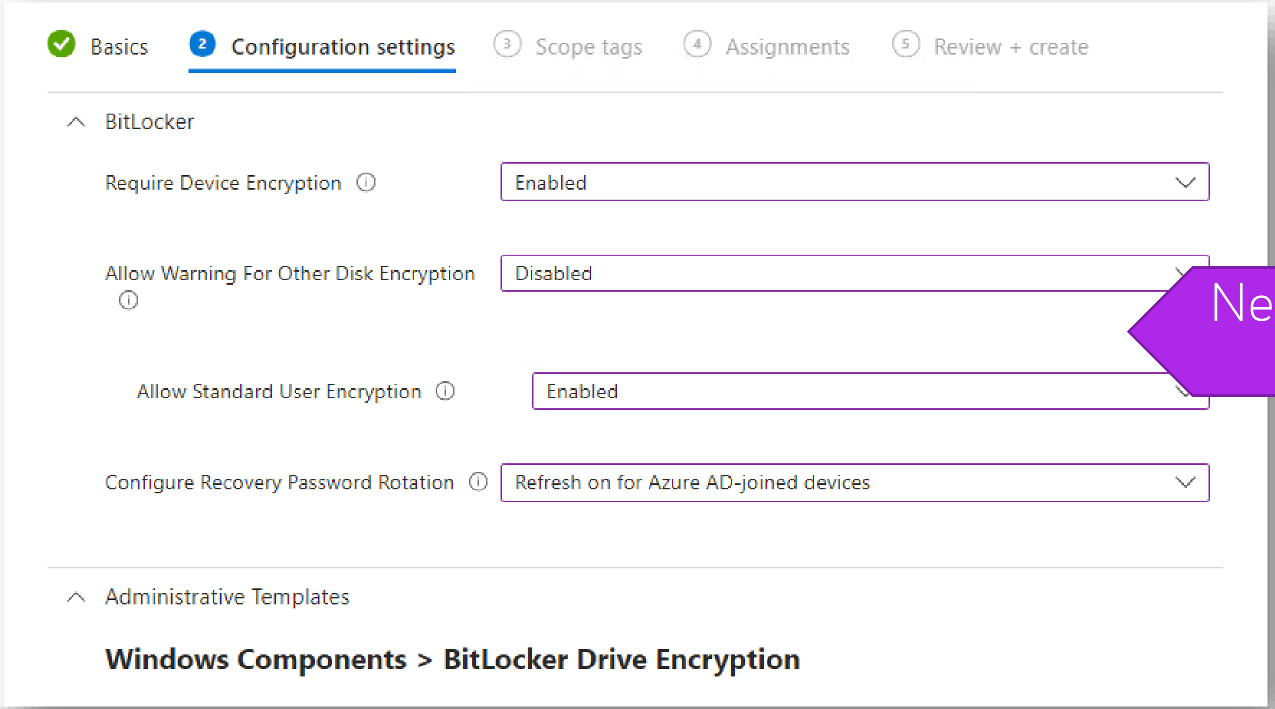
| Setting | Value |
|---|---|
| TamperProtection (Device) ⓘ | On |

Windows Defender Security Center

| Setting | Value |
|---|---|
| Disable Account Protection UI ⓘ | (Disable) The users can see the display of the Account protection are... |
| Disable App Browser UI ⓘ | Not configured |

# Disk Encryption Profile

- Silently enable BitLocker for Entra ID Joined Devices



BitLocker

Require Device Encryption ⓘ: Enabled

Allow Warning For Other Disk Encryption ⓘ: Disabled

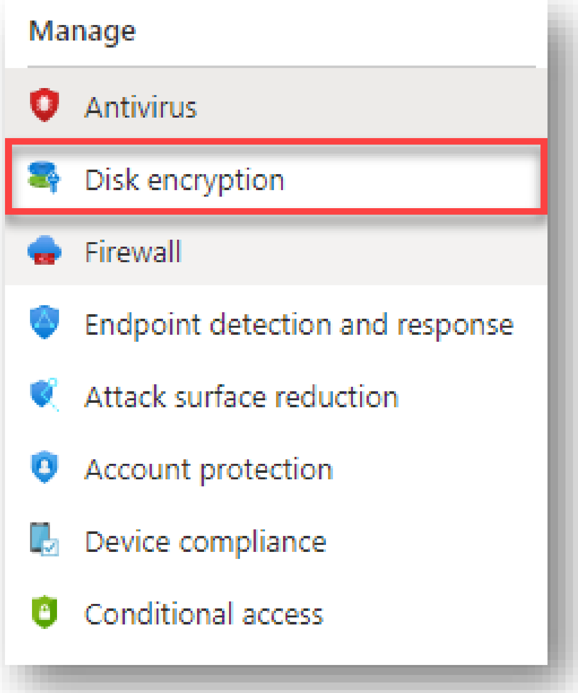
Allow Standard User Encryption ⓘ: Enabled

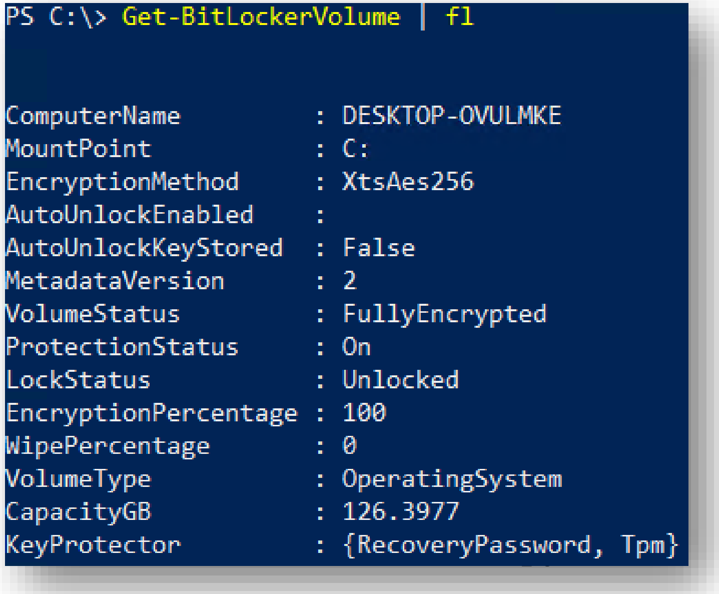
Configure Recovery Password Rotation ⓘ: Refresh on for Azure AD-joined devices

Administrative Templates

**Windows Components > BitLocker Drive Encryption**

Needed for silent encryption



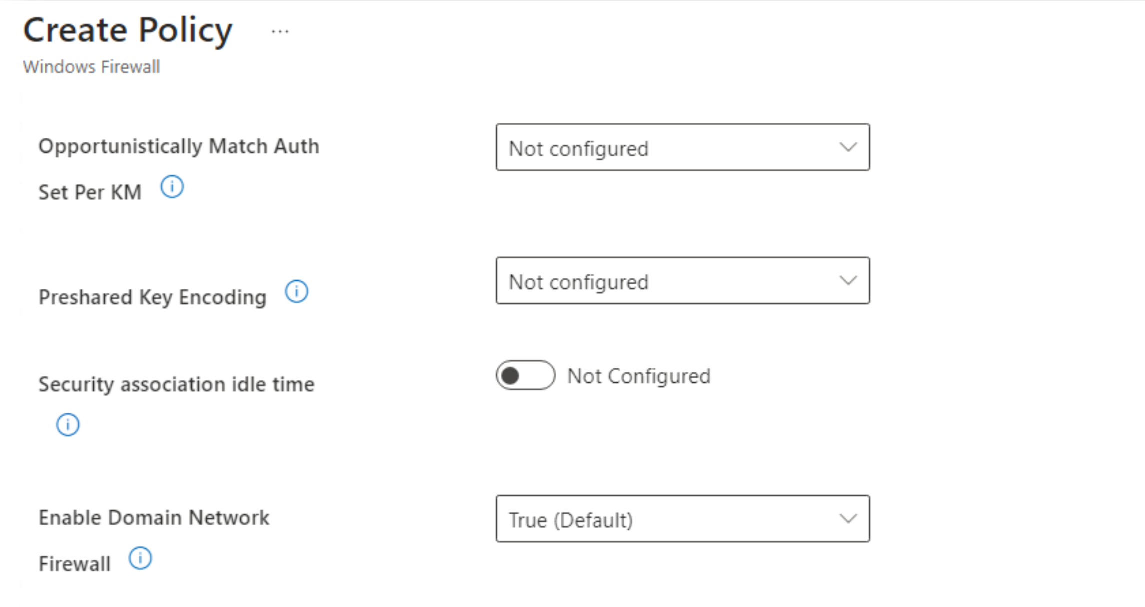


```
PS C:\> Get-BitLockerVolume | fl


ComputerName         : DESKTOP-OVULMKE
MountPoint           : C:
EncryptionMethod     : XtsAes256
AutoUnlockEnabled    :
AutoUnlockKeyStored  : False
MetadataVersion      : 2
VolumeStatus         : FullyEncrypted
ProtectionStatus     : On
LockStatus           : Unlocked
EncryptionPercentage : 100
WipePercentage       : 0
VolumeType           : OperatingSystem
CapacityGB           : 126.3977
KeyProtector         : {RecoveryPassword, Tpm}
```

# Windows Firewall Profile

- Windows Firewall has 3 different profile types (Firewall, Firewall Rules and Hyper-V Firewall Rules)

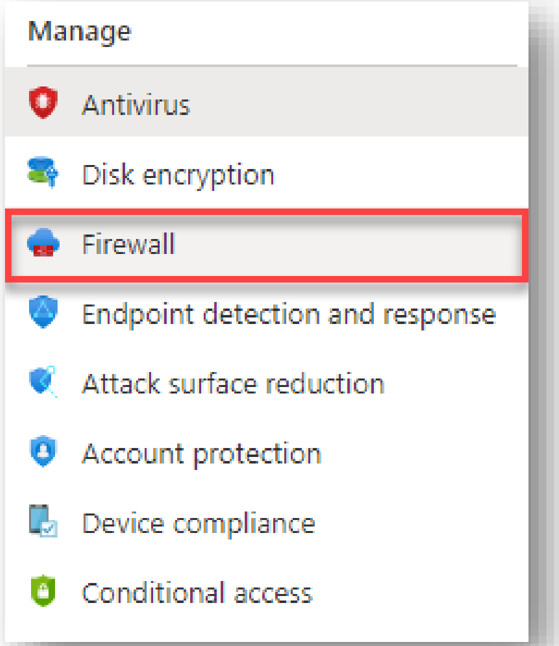


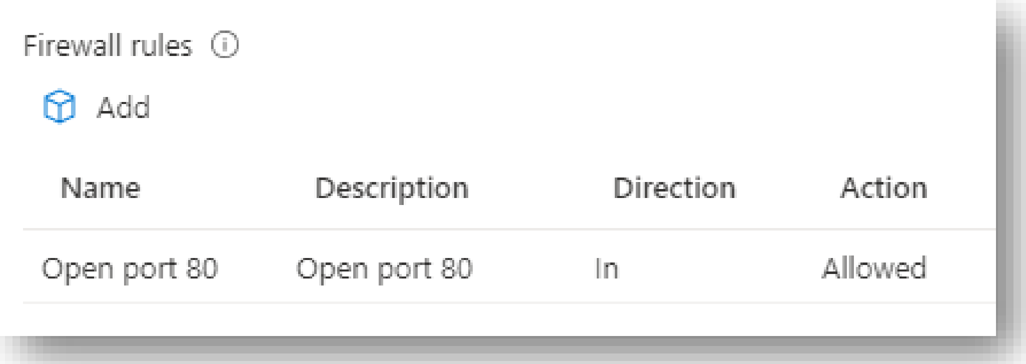
**Create Policy** ···

Windows Firewall

| | |
|---|---|
| Opportunistically Match Auth Set Per KM ⓘ | Not configured |
| Preshared Key Encoding ⓘ | Not configured |
| Security association idle time ⓘ | ○ Not Configured |
| Enable Domain Network Firewall ⓘ | True (Default) |

General settings
(conflicts not sent to device)





Firewall rules ⓘ

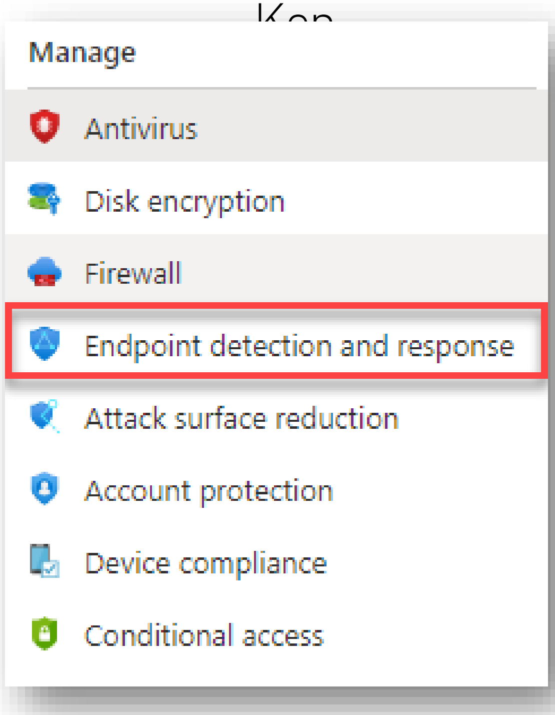
Add

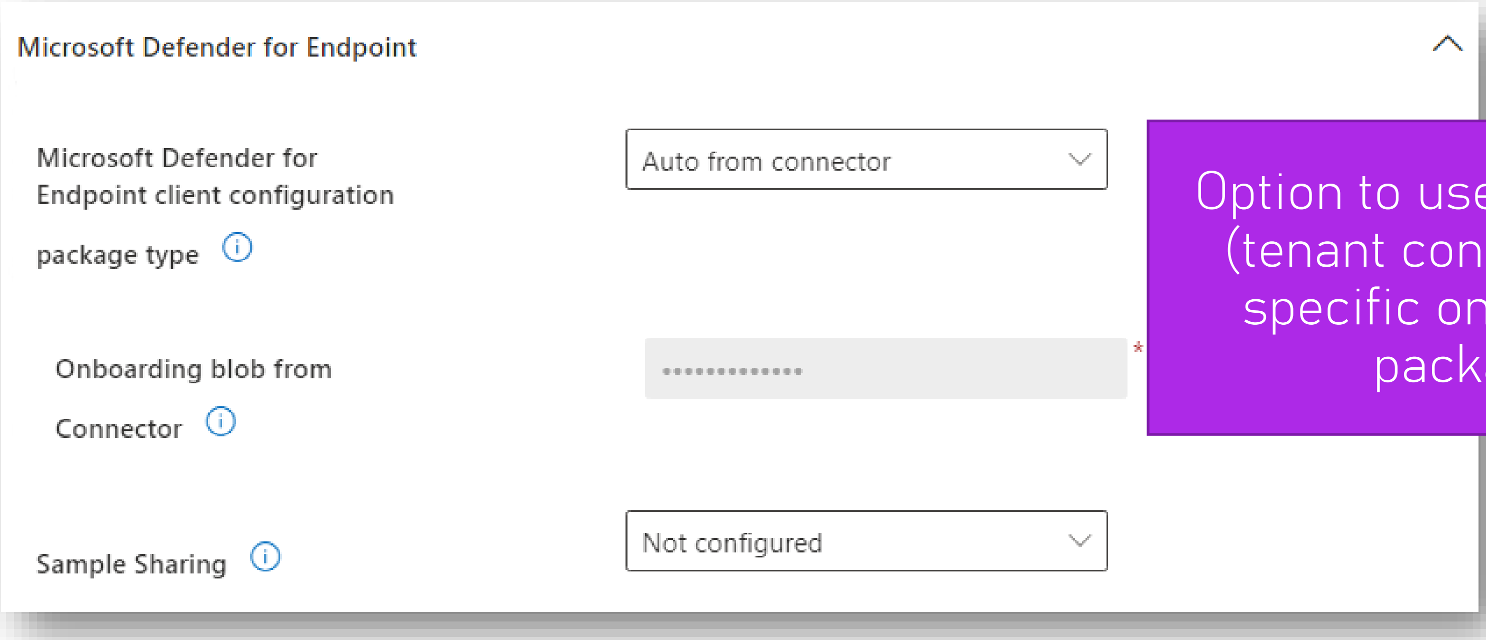
| Name | Description | Direction | Action |
|---|---|---|---|
| Open port 80 | Open port 80 | In | Allowed |

Rule settings (settings merged)

# Defender for Endpoint

- Detection and Response



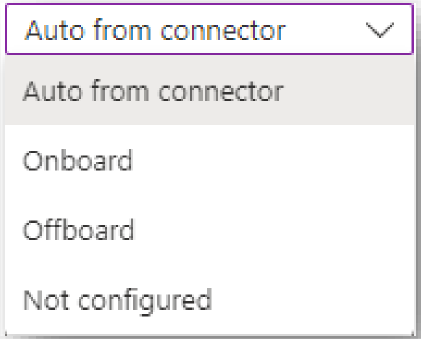

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint client configuration package type: Auto from connector

Onboarding blob from Connector: ••••••••••••• *

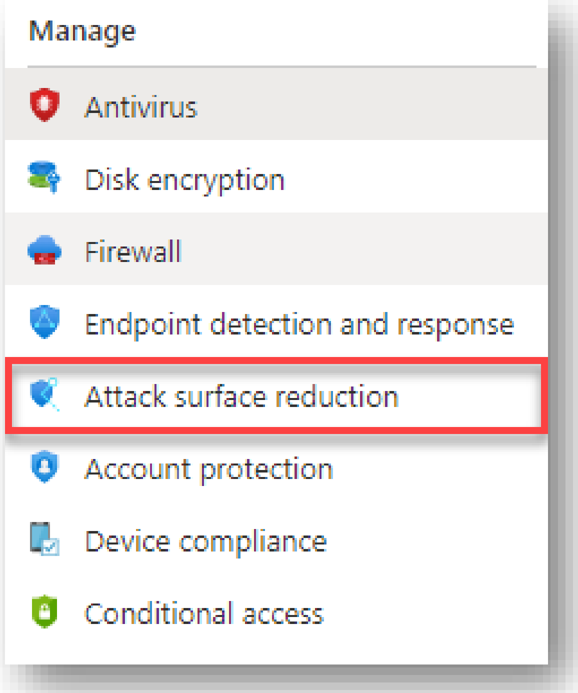
Sample Sharing: Not configured

Option to use automatic (tenant connector) or specific onboarding package



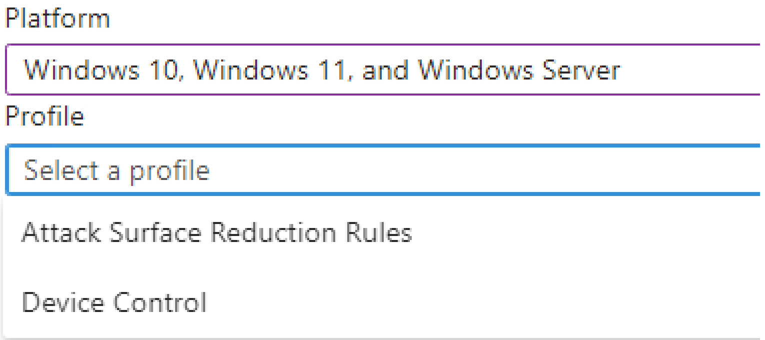
# Attack Surface Reduction

- Device control (Secures removable media access, USB)
- Attack surface reduction rules (Behaviour monitoring)
- App and browser isolation (Run app/browser in isolated VM)
- Exploit protection (Applies process mitigations)
- Web protection (Blocks access to malicious sites)
- Application control (Restrict applications)



Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access



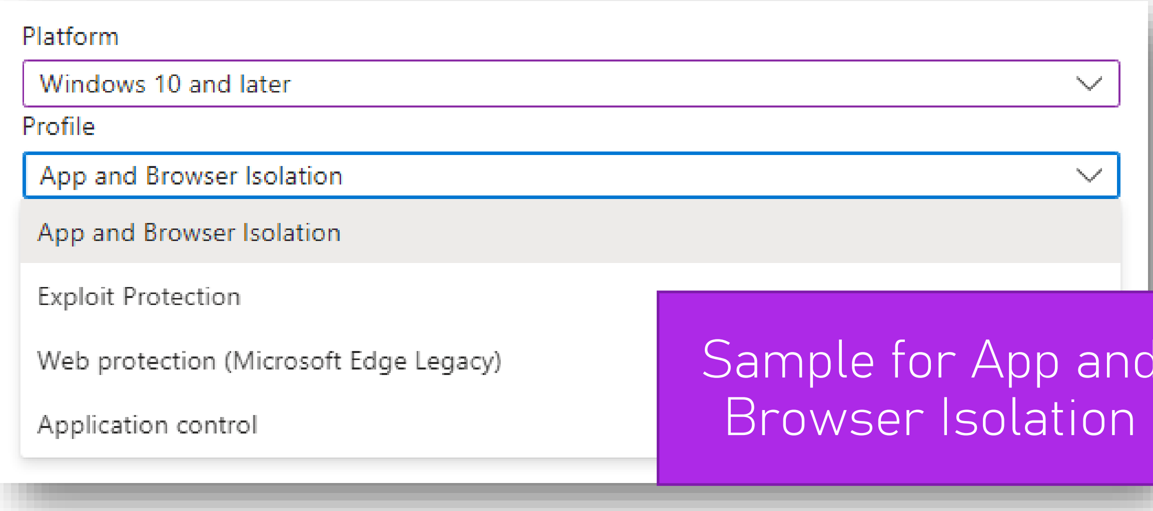
Platform

Windows 10, Windows 11, and Windows Server

Profile

Select a profile

- Attack Surface Reduction Rules
- Device Control



Platform

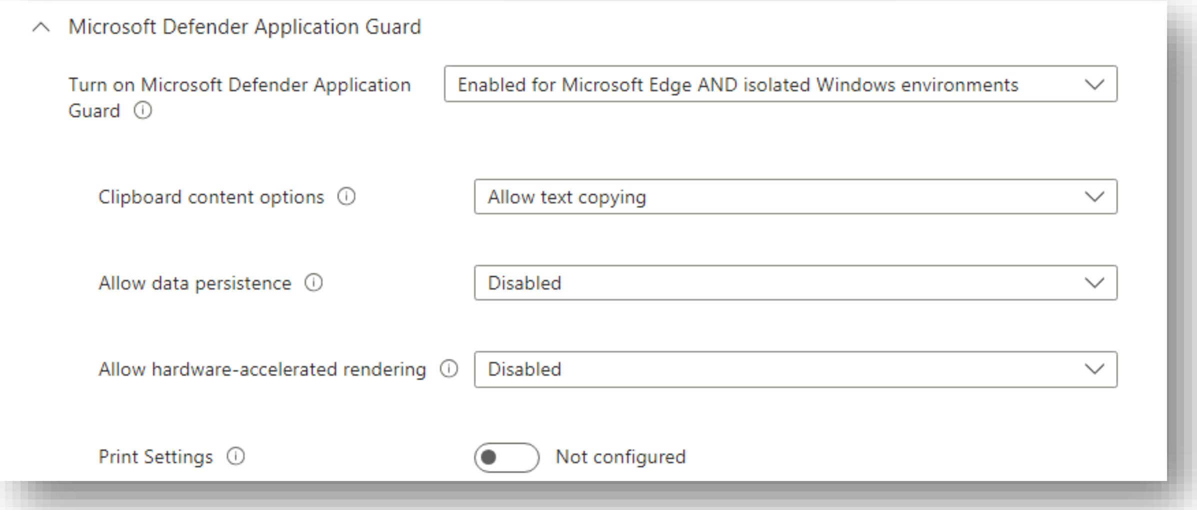
Windows 10 and later

Profile

App and Browser Isolation

- App and Browser Isolation
- Exploit Protection
- Web protection (Microsoft Edge Legacy)
- Application control

Sample for App and Browser Isolation



Microsoft Defender Application Guard

Turn on Microsoft Defender Application Guard ⓘ: Enabled for Microsoft Edge AND isolated Windows environments

Clipboard content options ⓘ: Allow text copying

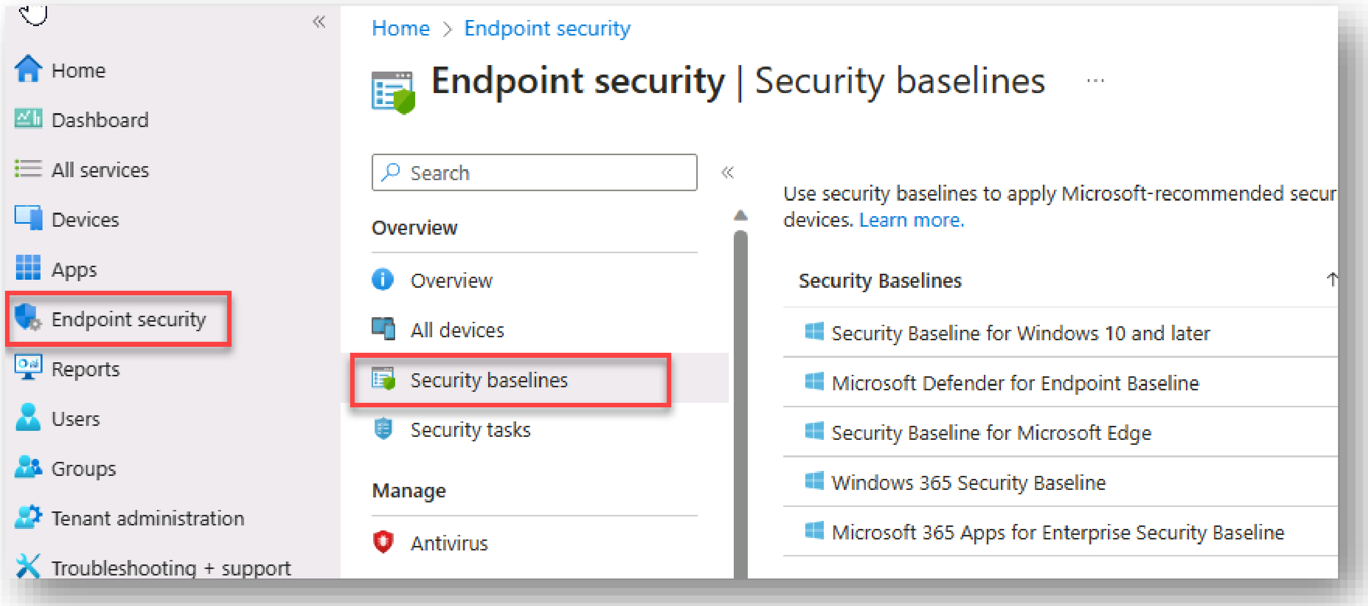
Allow data persistence ⓘ: Disabled

Allow hardware-accelerated rendering ⓘ: Disabled

Print Settings ⓘ: Not configured

# Security Baselines

- Security Baselines to help securing and protecting users and devices
- Automatically creates settings recommended by the security teams
  - Enables Bitlocker
  - Creates password settings
  - Disables basic authentication
  - .....



Use security baselines to apply Microsoft-recommended secur devices. Learn more.

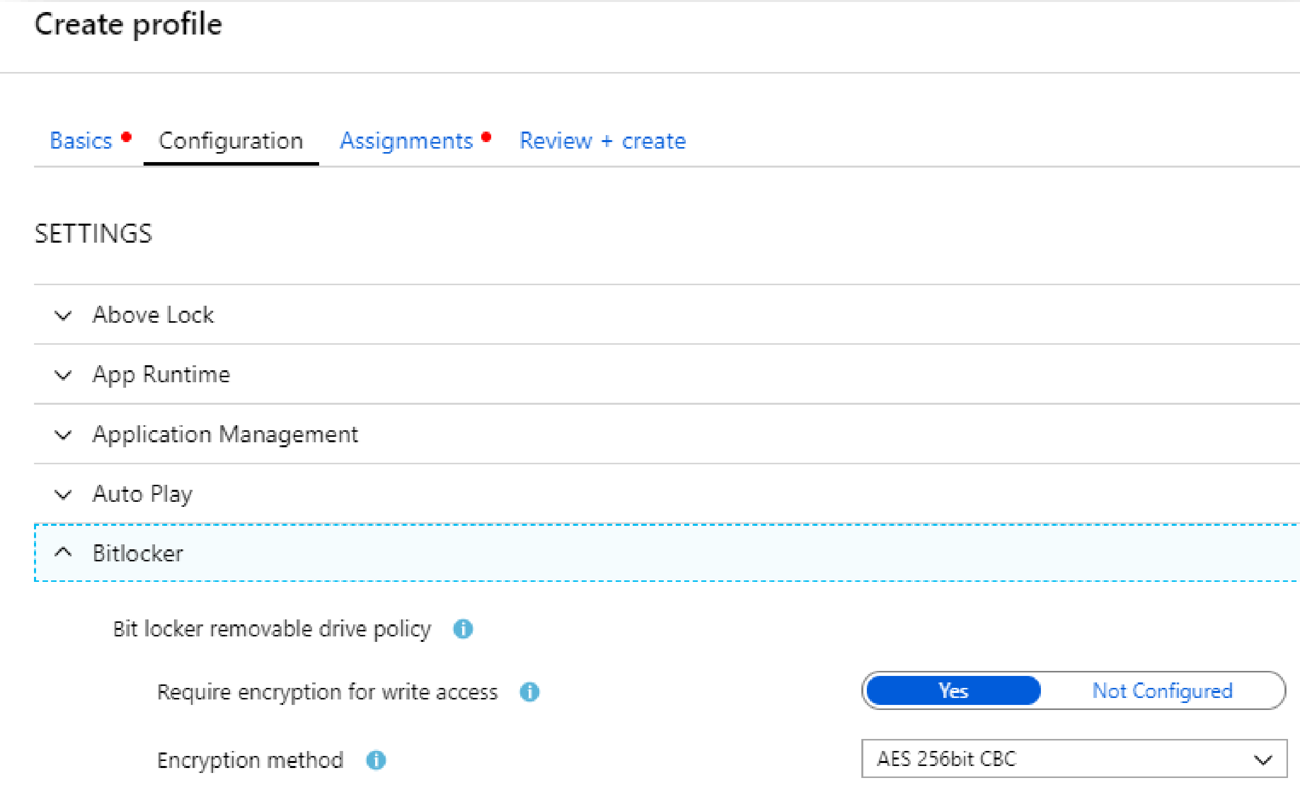
Security Baselines

- Security Baseline for Windows 10 and later
- Microsoft Defender for Endpoint Baseline
- Security Baseline for Microsoft Edge
- Windows 365 Security Baseline
- Microsoft 365 Apps for Enterprise Security Baseline

Analyze and test the settings before production!

# Configuring via Intune

- A Security Baseline creates a standard configuration profile
- Assignment and monitoring works as usual



Create profile

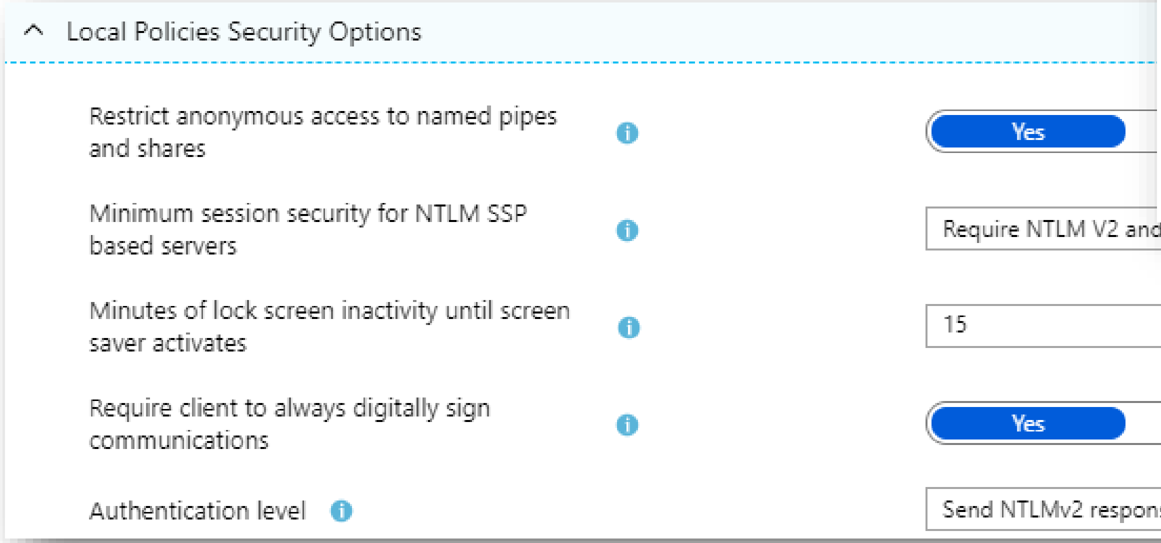
Basics • | Configuration | Assignments • | Review + create

SETTINGS

- Above Lock
- App Runtime
- Application Management
- Auto Play
- Bitlocker

Bit locker removable drive policy

| | |
|---|---|
| Require encryption for write access | Yes / Not Configured |
| Encryption method | AES 256bit CBC |



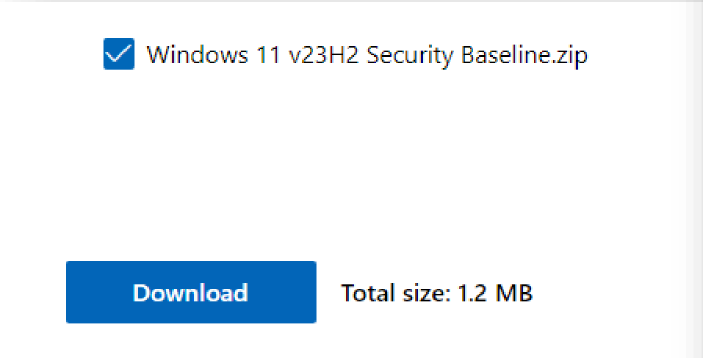
Local Policies Security Options

| | |
|---|---|
| Restrict anonymous access to named pipes and shares | Yes |
| Minimum session security for NTLM SSP based servers | Require NTLM V2 and 128 bit encryption |
| Minutes of lock screen inactivity until screen saver activates | 15 |
| Require client to always digitally sign communications | Yes / Not Configured |
| Authentication level | Send NTLMv2 response only. Refuse LM... |

samples

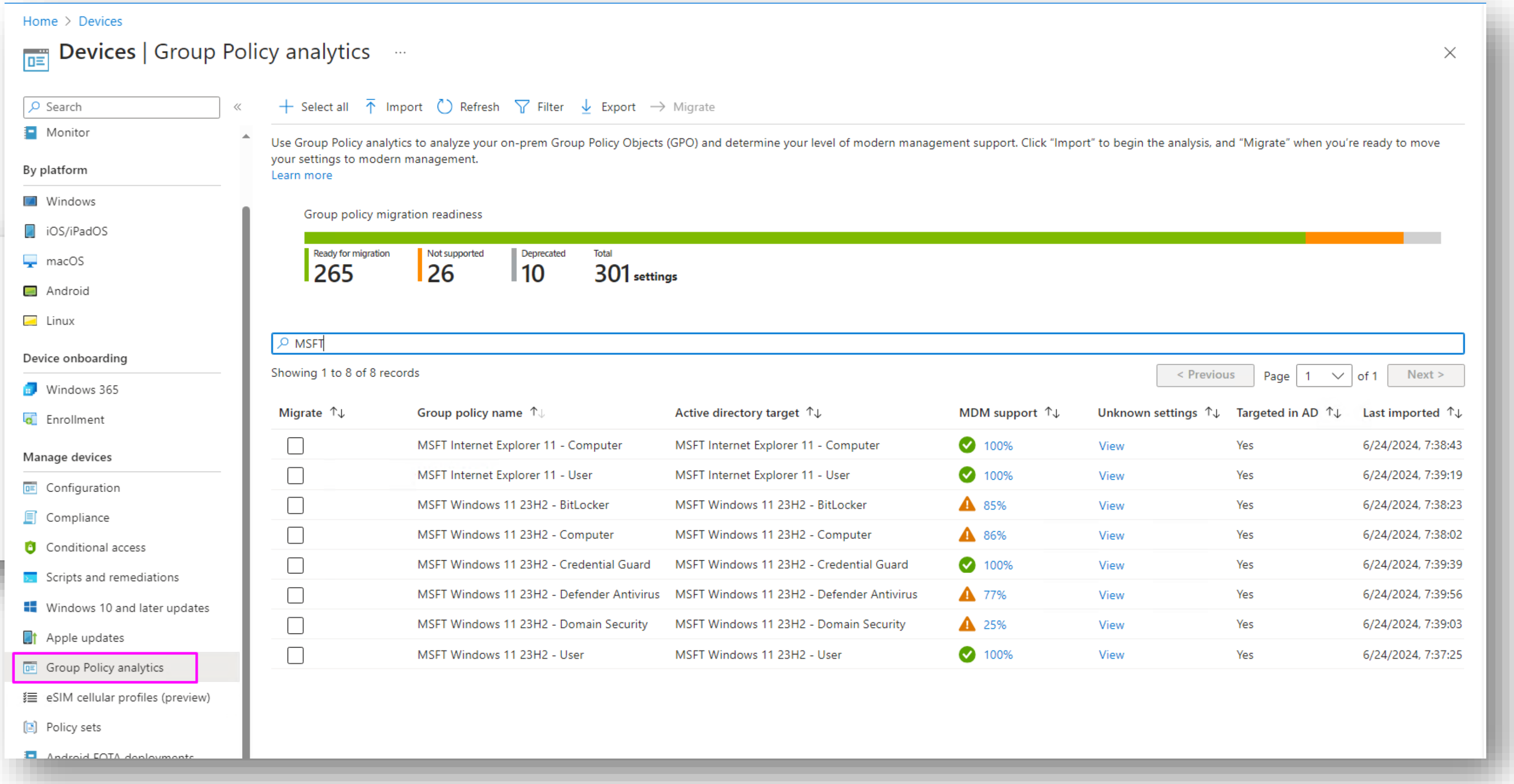
# Security Baselines – What with new versions of Windows?

- Download the latest version [Microsoft Security Compliance Toolkit 1.0]



☑ Windows 11 v23H2 Security Baseline.zip

Total size: 1.2 MB



Use Group Policy analytics to analyze your on-prem Group Policy Objects (GPO) and determine your level of modern management support. Click "Import" to begin the analysis, and "Migrate" when you're ready to move your settings to modern management.
Learn more

Group policy migration readiness

| Ready for migration | Not supported | Deprecated | Total |
|---|---|---|---|
| 265 | 26 | 10 | 301 settings |

MSFT

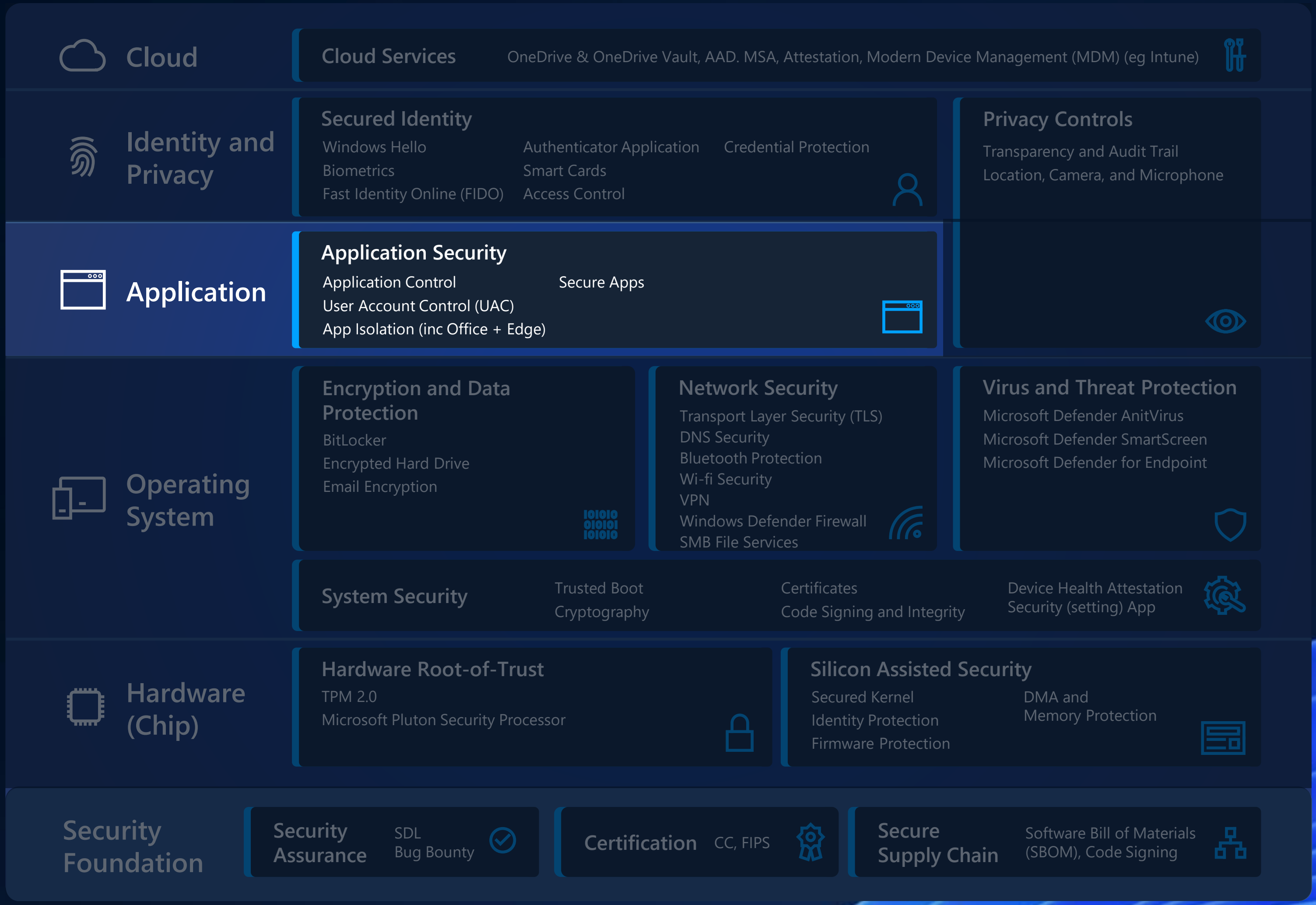
Showing 1 to 8 of 8 records

| Migrate | Group policy name | Active directory target | MDM support | Unknown settings | Targeted in AD | Last imported |
|---|---|---|---|---|---|---|
| □ | MSFT Internet Explorer 11 - Computer | MSFT Internet Explorer 11 - Computer | ✓ 100% | View | Yes | 6/24/2024, 7:38:43 |
| □ | MSFT Internet Explorer 11 - User | MSFT Internet Explorer 11 - User | ✓ 100% | View | Yes | 6/24/2024, 7:39:19 |
| □ | MSFT Windows 11 23H2 - BitLocker | MSFT Windows 11 23H2 - BitLocker | ⚠ 85% | View | Yes | 6/24/2024, 7:38:23 |
| □ | MSFT Windows 11 23H2 - Computer | MSFT Windows 11 23H2 - Computer | ⚠ 86% | View | Yes | 6/24/2024, 7:38:02 |
| □ | MSFT Windows 11 23H2 - Credential Guard | MSFT Windows 11 23H2 - Credential Guard | ✓ 100% | View | Yes | 6/24/2024, 7:39:39 |
| □ | MSFT Windows 11 23H2 - Defender Antivirus | MSFT Windows 11 23H2 - Defender Antivirus | ⚠ 77% | View | Yes | 6/24/2024, 7:39:56 |
| □ | MSFT Windows 11 23H2 - Domain Security | MSFT Windows 11 23H2 - Domain Security | ⚠ 25% | View | Yes | 6/24/2024, 7:39:03 |
| □ | MSFT Windows 11 23H2 - User | MSFT Windows 11 23H2 - User | ✓ 100% | View | Yes | 6/24/2024, 7:37:25 |

# Application Overview

To help keep users secure and productive, Windows 11 protects critical data and code integrity with  multiple layers of application security.

- **Helps IT pros enforce what apps and drivers run on Windows devices** with Windows Application Control.
- **Runs websites and Office files safely in virtual containers** with Microsoft Defender Application Guard.[1]
- **Helps prevent malware from gaining admin rights** and making changes to the PC.
- **Protects filesystem and registry** by running Universal Windows Platform Apps in virtual containers.
- **Enables developers to build in security** from the ground up.



Cloud

Cloud Services — OneDrive & OneDrive Vault, AAD. MSA, Attestation, Modern Device Management (MDM) (eg Intune)

Identity and Privacy

Secured Identity — Windows Hello, Biometrics, Fast Identity Online (FIDO), Authenticator Application, Smart Cards, Access Control, Credential Protection

Privacy Controls — Transparency and Audit Trail, Location, Camera, and Microphone

Application

Application Security — Application Control, User Account Control (UAC), App Isolation (inc Office + Edge), Secure Apps

Operating System

Encryption and Data Protection — BitLocker, Encrypted Hard Drive, Email Encryption

Network Security — Transport Layer Security (TLS), DNS Security, Bluetooth Protection, Wi-fi Security, VPN, Windows Defender Firewall, SMB File Services

Virus and Threat Protection — Microsoft Defender AnitVirus, Microsoft Defender SmartScreen, Microsoft Defender for Endpoint

System Security — Trusted Boot, Cryptography, Certificates, Code Signing and Integrity, Device Health Attestation, Security (setting) App

Hardware (Chip)

Hardware Root-of-Trust — TPM 2.0, Microsoft Pluton Security Processor

Silicon Assisted Security — Secured Kernel, Identity Protection, Firmware Protection, DMA and Memory Protection

Security Foundation

Security Assurance — SDL, Bug Bounty

Certification — CC, FIPS

Secure Supply Chain — Software Bill of Materials (SBOM), Code Signing

[1] OEMs provide the hardware necessary to enable Application Guard

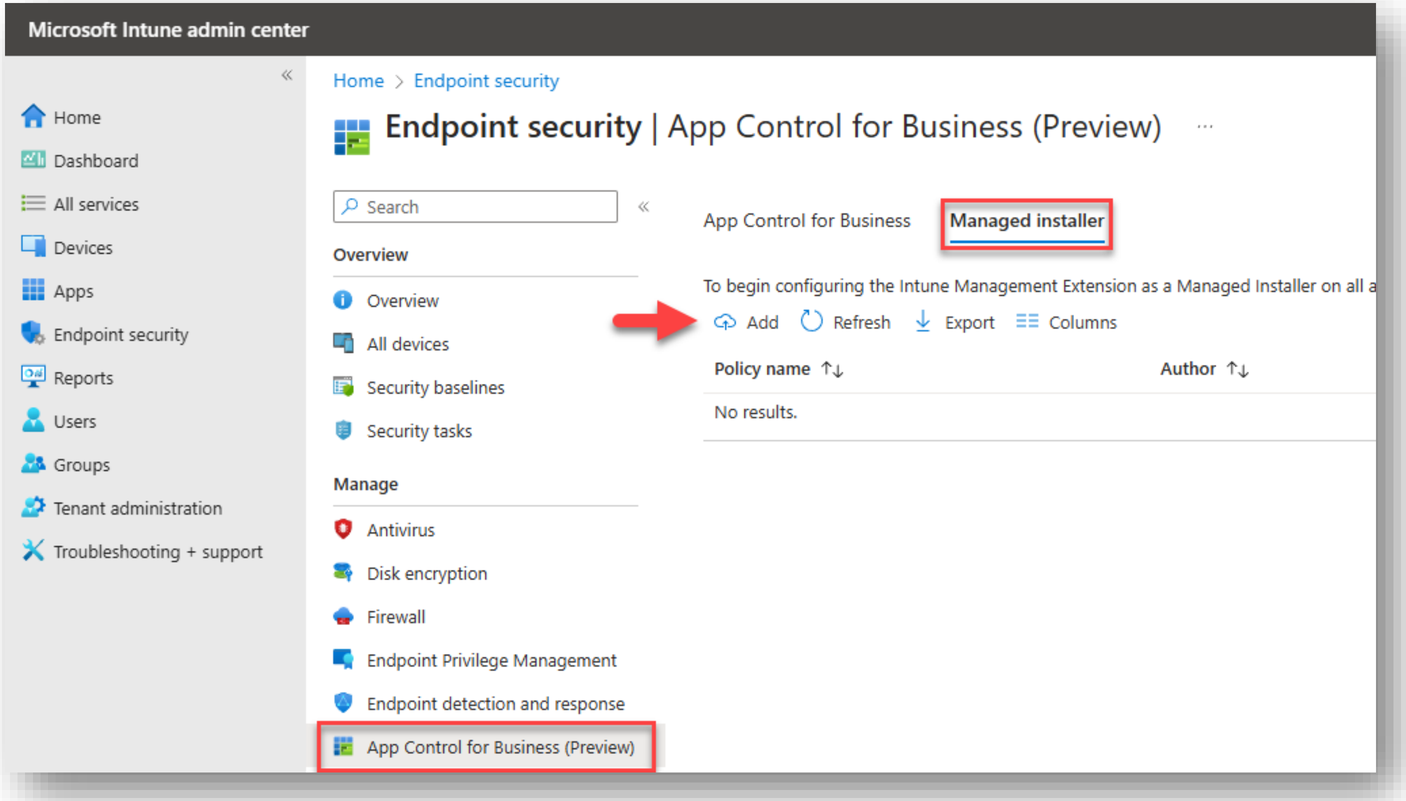
# Application Control for Business

- Prevents undesired apps from running on your managed Windows devices
- Intune Managed (preview)
  - App Control for Business policies
  - Managed Installer policies

# Managed Installer Policy

- Enabling Intune as a managed installer
  - All apps deployed to Windows devices through Intune are marked with the managed installer tag
- Tenant-wide Configuration // automatically applied to all managed Windows devices
- Tags are used with WDAC policies to determine which apps can run
- Important :
  - Tagging is not retroactive – previously deployed apps are not tagged!
  - Turning off the policy does not remove tags set previously
- Removing IME as managed installer requires clean-up script (CatCleanIMEOnly.ps1)

# Managed Installer Policy – Configuration



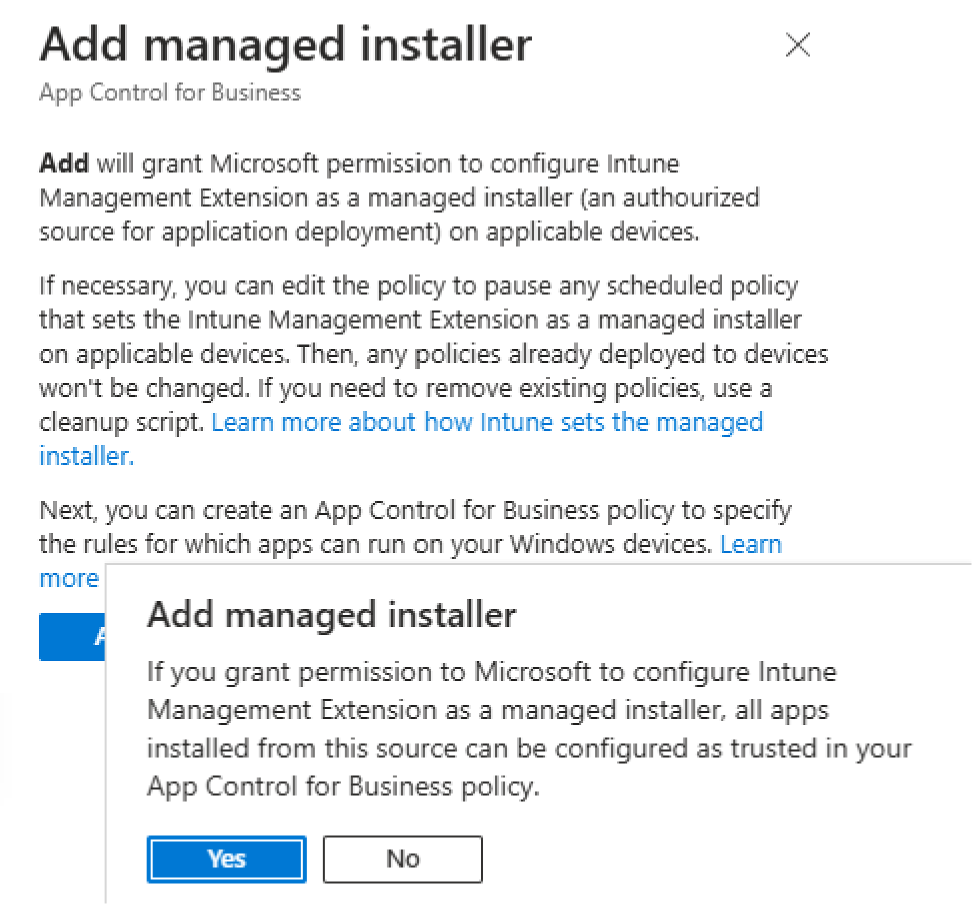
Microsoft Intune admin center

Home > Endpoint security

## Endpoint security | App Control for Business (Preview)

To begin configuring the Intune Management Extension as a Managed Installer on all a

| Policy name ↑↓ | Author ↑↓ |
|---|---|
| No results. | |



## Add managed installer

App Control for Business

**Add** will grant Microsoft permission to configure Intune Management Extension as a managed installer (an authourized source for application deployment) on applicable devices.

If necessary, you can edit the policy to pause any scheduled policy that sets the Intune Management Extension as a managed installer on applicable devices. Then, any policies already deployed to devices won't be changed. If you need to remove existing policies, use a cleanup script. Learn more about how Intune sets the managed installer.

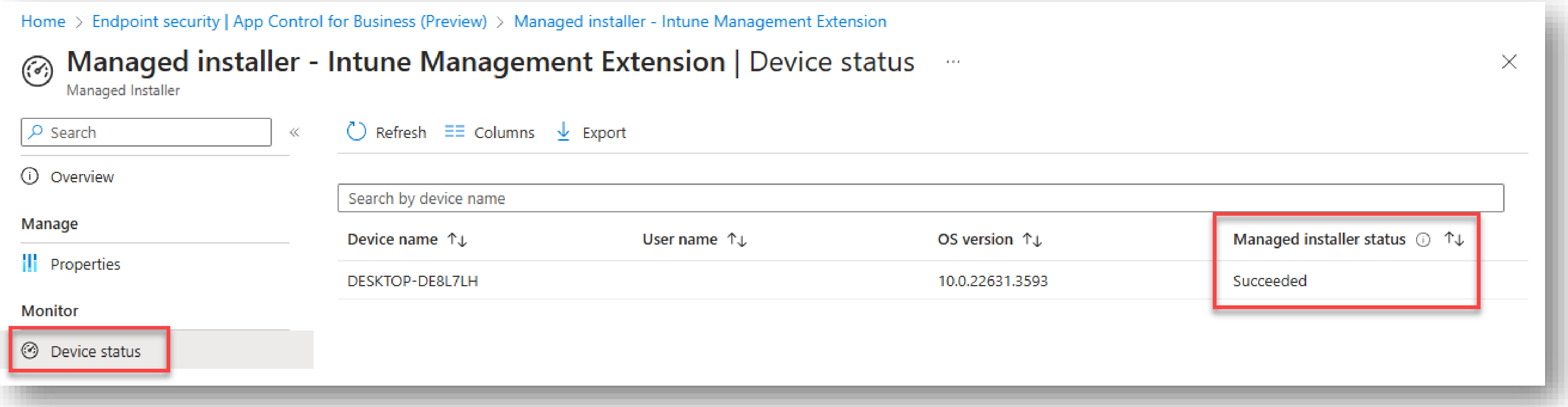
Next, you can create an App Control for Business policy to specify the rules for which apps can run on your Windows devices. Learn more

### Add managed installer

If you grant permission to Microsoft to configure Intune Management Extension as a managed installer, all apps installed from this source can be configured as trusted in your App Control for Business policy.

# Managed Installer Policy – Validation

- Via Device Status pane



Home > Endpoint security | App Control for Business (Preview) > Managed installer - Intune Management Extension

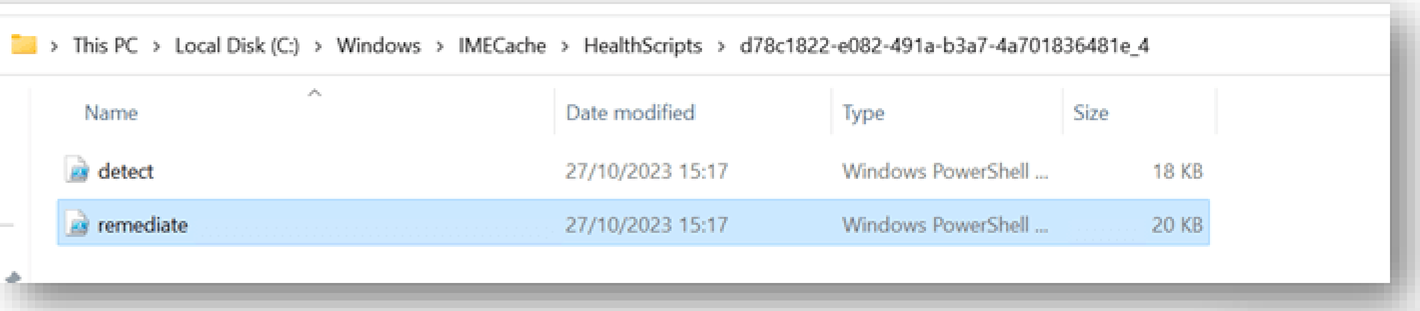
**Managed installer - Intune Management Extension** | Device status

Managed Installer

| Device name | User name | OS version | Managed installer status |
|---|---|---|---|
| DESKTOP-DE8L7LH | | 10.0.22631.3593 | Succeeded |

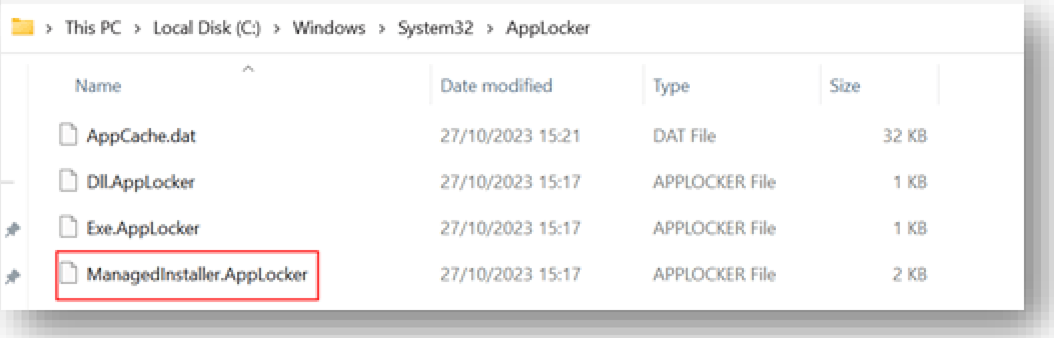
# Managed Installer Policy – Validation

- On the device



› This PC › Local Disk (C:) › Windows › IMECache › HealthScripts › d78c1822-e082-491a-b3a7-4a701836481e_4

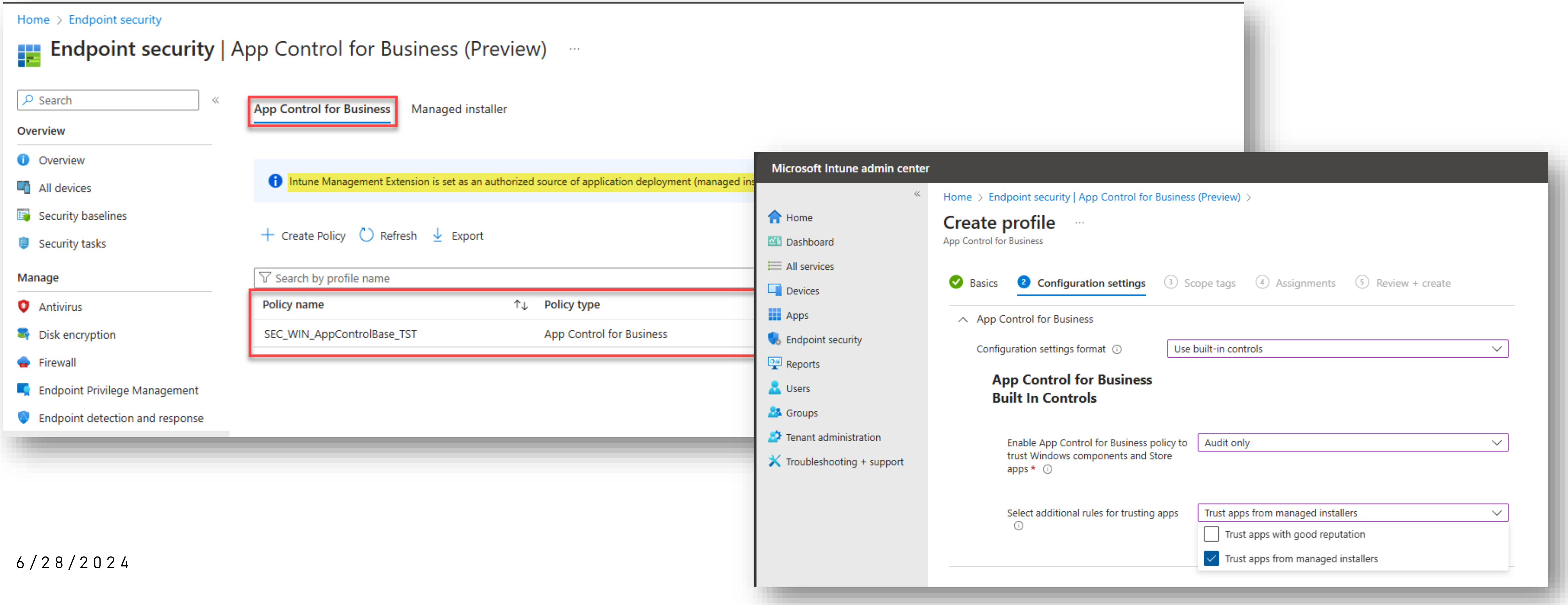
| Name | Date modified | Type | Size |
|---|---|---|---|
| detect | 27/10/2023 15:17 | Windows PowerShell ... | 18 KB |
| remediate | 27/10/2023 15:17 | Windows PowerShell ... | 20 KB |



› This PC › Local Disk (C:) › Windows › System32 › AppLocker

| Name | Date modified | Type | Size |
|---|---|---|---|
| AppCache.dat | 27/10/2023 15:21 | DAT File | 32 KB |
| Dll.AppLocker | 27/10/2023 15:17 | APPLOCKER File | 1 KB |
| Exe.AppLocker | 27/10/2023 15:17 | APPLOCKER File | 1 KB |
| ManagedInstaller.AppLocker | 27/10/2023 15:17 | APPLOCKER File | 2 KB |

# App Control for Business Policy – Configuration (1)



Endpoint security | App Control for Business (Preview)

Intune Management Extension is set as an authorized source of application deployment (managed ins

| Policy name | Policy type |
|---|---|
| SEC_WIN_AppControlBase_TST | App Control for Business |

Create profile

App Control for Business

App Control for Business

Configuration settings format: Use built-in controls

App Control for Business Built In Controls

Enable App Control for Business policy to trust Windows components and Store apps *: Audit only

Select additional rules for trusting apps: Trust apps from managed installers

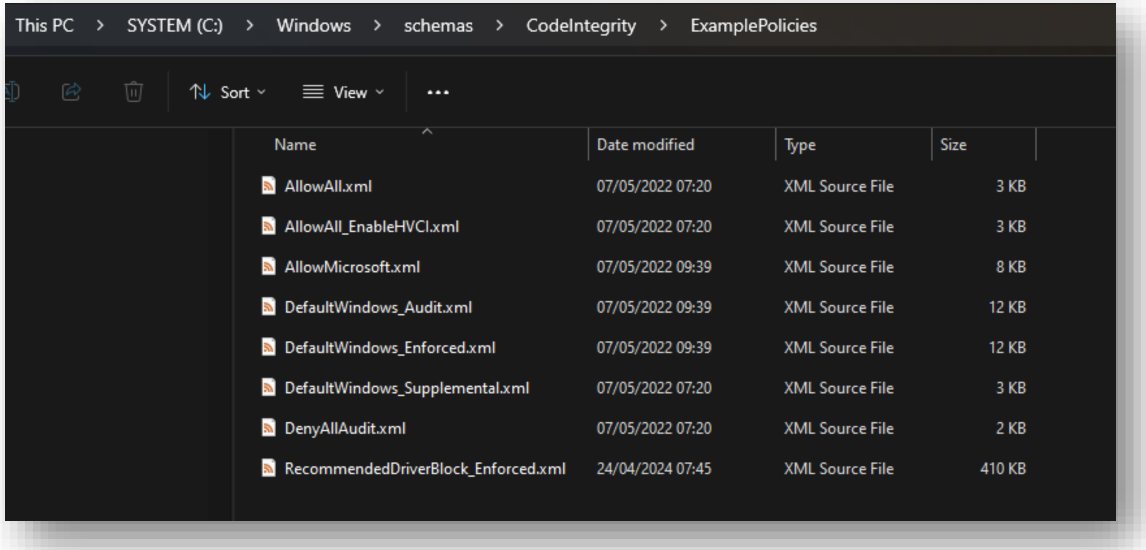
☐ Trust apps with good reputation

☑ Trust apps from managed installers

# App Control for Business Policy – Configuration (2)

- WDAC Policy Wizard
  [Microsoft WDAC Wizard (webapp-wdac-wizard.azurewebsites.net)](https://webapp-wdac-wizard.azurewebsites.net)

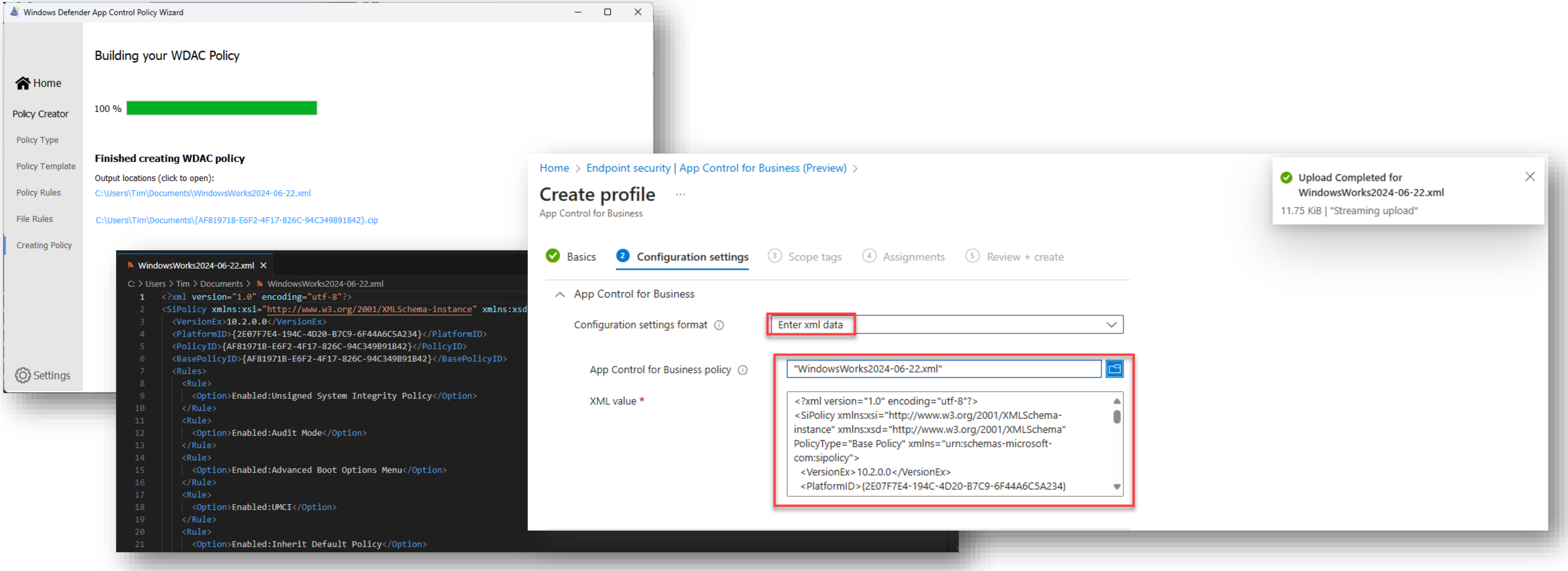
- Sample policies (on every Windows 11 device)



This PC > SYSTEM (C:) > Windows > schemas > CodeIntegrity > ExamplePolicies

| Name | Date modified | Type | Size |
|---|---|---|---|
| AllowAll.xml | 07/05/2022 07:20 | XML Source File | 3 KB |
| AllowAll_EnableHVCI.xml | 07/05/2022 07:20 | XML Source File | 3 KB |
| AllowMicrosoft.xml | 07/05/2022 09:39 | XML Source File | 8 KB |
| DefaultWindows_Audit.xml | 07/05/2022 09:39 | XML Source File | 12 KB |
| DefaultWindows_Enforced.xml | 07/05/2022 09:39 | XML Source File | 12 KB |
| DefaultWindows_Supplemental.xml | 07/05/2022 07:20 | XML Source File | 3 KB |
| DenyAllAudit.xml | 07/05/2022 07:20 | XML Source File | 2 KB |
| RecommendedDriverBlock_Enforced.xml | 24/04/2024 07:45 | XML Source File | 410 KB |

# App Control for Business Policy – Configuration (3)



Windows Defender App Control Policy Wizard

Building your WDAC Policy

100 %

**Finished creating WDAC policy**

Output locations (click to open):

C:\Users\Tim\Documents\WindowsWorks2024-06-22.xml

C:\Users\Tim\Documents\{AF81971B-E6F2-4F17-826C-94C349B91B42}.cip

WindowsWorks2024-06-22.xml

C: > Users > Tim > Documents > WindowsWorks2024-06-22.xml

```xml
<?xml version="1.0" encoding="utf-8"?>
<SiPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd
  <VersionEx>10.2.0.0</VersionEx>
  <PlatformID>{2E07F7E4-194C-4D20-B7C9-6F44A6C5A234}</PlatformID>
  <PolicyID>{AF81971B-E6F2-4F17-826C-94C349B91B42}</PolicyID>
  <BasePolicyID>{AF81971B-E6F2-4F17-826C-94C349B91B42}</BasePolicyID>
  <Rules>
    <Rule>
      <Option>Enabled:Unsigned System Integrity Policy</Option>
    </Rule>
    <Rule>
      <Option>Enabled:Audit Mode</Option>
    </Rule>
    <Rule>
      <Option>Enabled:Advanced Boot Options Menu</Option>
    </Rule>
    <Rule>
      <Option>Enabled:UMCI</Option>
    </Rule>
    <Rule>
      <Option>Enabled:Inherit Default Policy</Option>
```

Home > Endpoint security | App Control for Business (Preview) >

Create profile ...

App Control for Business

Upload Completed for WindowsWorks2024-06-22.xml

11.75 KiB | "Streaming upload"

App Control for Business

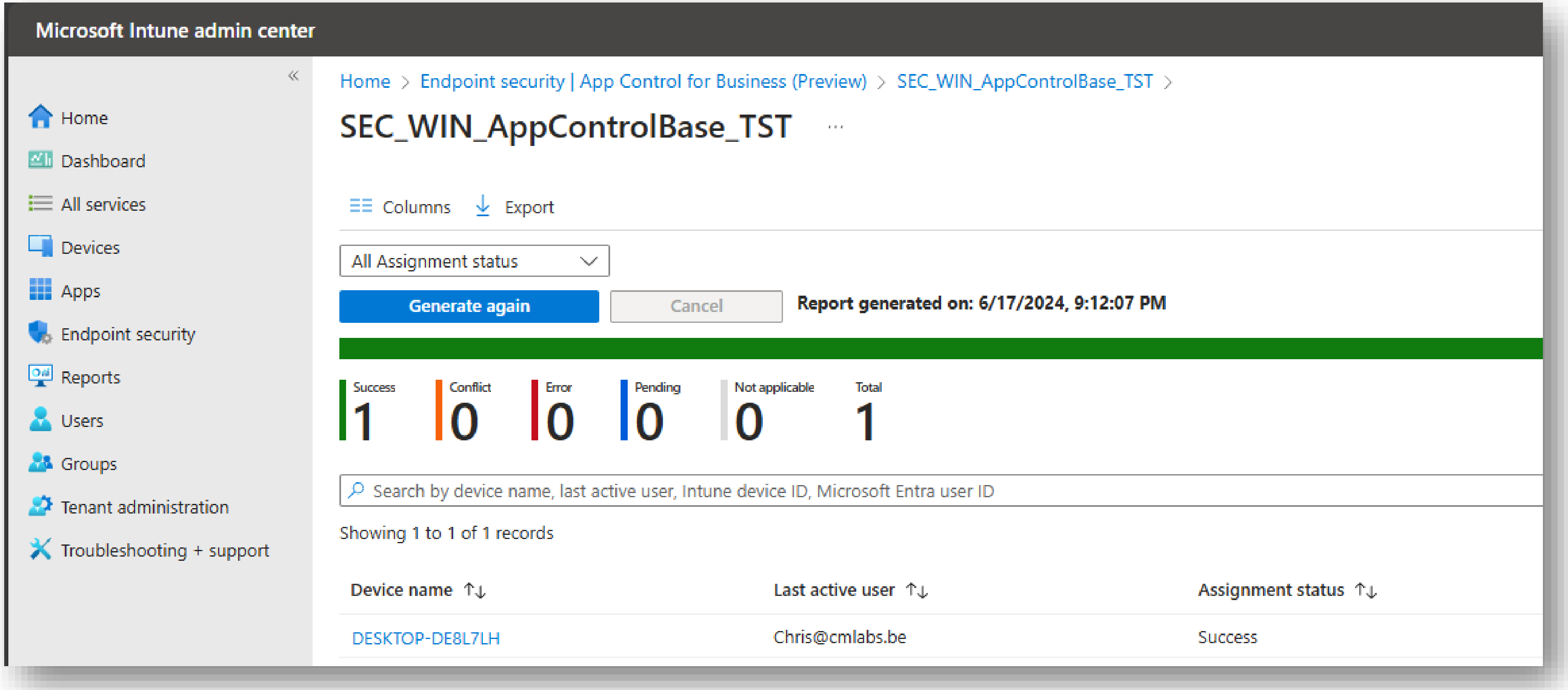
Configuration settings format: Enter xml data

App Control for Business policy: "WindowsWorks2024-06-22.xml"

XML value *

```xml
<?xml version="1.0" encoding="utf-8"?>
<SiPolicy xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
PolicyType="Base Policy" xmlns="urn:schemas-microsoft-
com:sipolicy">
  <VersionEx>10.2.0.0</VersionEx>
  <PlatformID>{2E07F7E4-194C-4D20-B7C9-6F44A6C5A234}
```

# App Control for Business Policy – Validating



Home > Endpoint security | App Control for Business (Preview) > SEC_WIN_AppControlBase_TST >

SEC_WIN_AppControlBase_TST ...

All Assignment status

**Report generated on: 6/17/2024, 9:12:07 PM**

| Success | Conflict | Error | Pending | Not applicable | Total |
|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 1 |

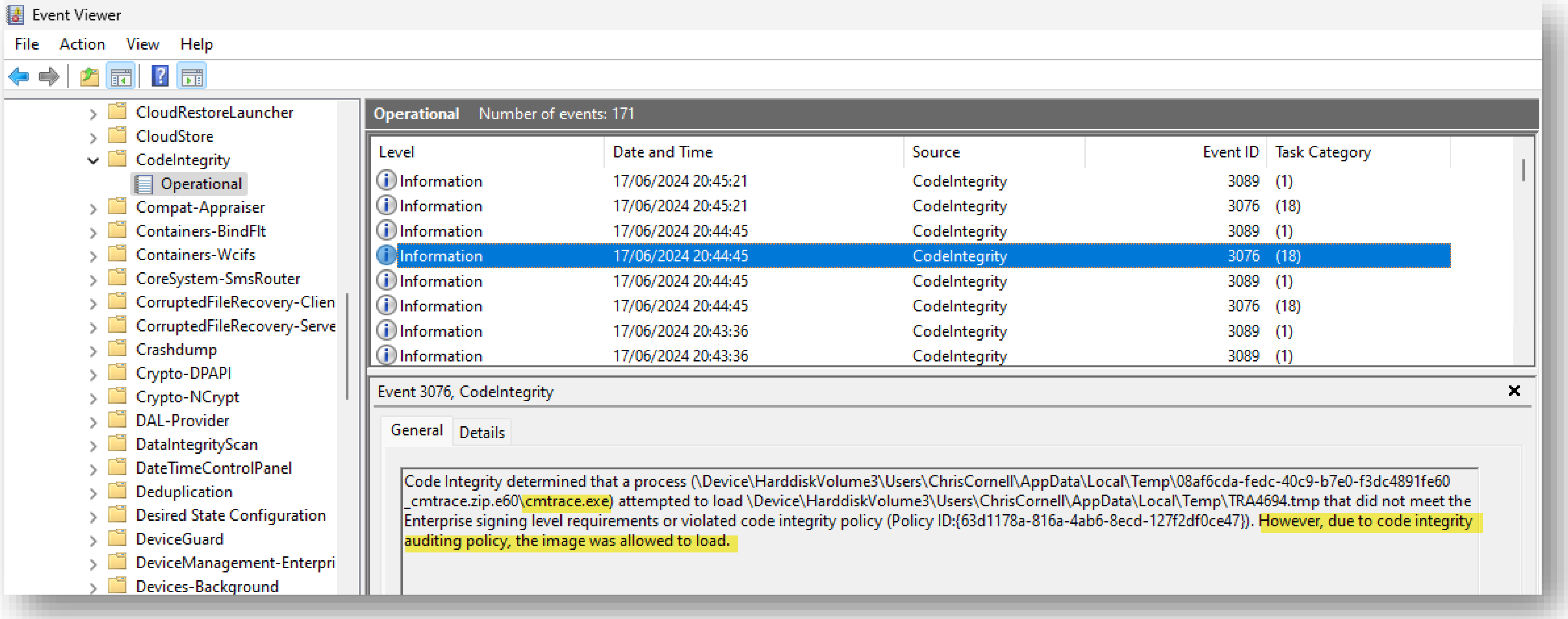
Search by device name, last active user, Intune device ID, Microsoft Entra user ID

Showing 1 to 1 of 1 records

| Device name ↑↓ | Last active user ↑↓ | Assignment status ↑↓ |
|---|---|---|
| DESKTOP-DE8L7LH | Chris@cmlabs.be | Success |

# App Control for Business Policy – Validating

- Application and Services Logs > Microsoft > Windows > CodeIntegrity > Operational



| Level | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Information | 17/06/2024 20:45:21 | CodeIntegrity | 3089 | (1) |
| Information | 17/06/2024 20:45:21 | CodeIntegrity | 3076 | (18) |
| Information | 17/06/2024 20:44:45 | CodeIntegrity | 3089 | (1) |
| Information | 17/06/2024 20:44:45 | CodeIntegrity | 3076 | (18) |
| Information | 17/06/2024 20:44:45 | CodeIntegrity | 3089 | (1) |
| Information | 17/06/2024 20:44:45 | CodeIntegrity | 3076 | (18) |
| Information | 17/06/2024 20:43:36 | CodeIntegrity | 3089 | (1) |
| Information | 17/06/2024 20:43:36 | CodeIntegrity | 3089 | (1) |

Event 3076, CodeIntegrity

Code Integrity determined that a process (\Device\HarddiskVolume3\Users\ChrisCornell\AppData\Local\Temp\08af6cda-fedc-40c9-b7e0-f3dc4891fe60_cmtrace.zip.e60\cmtrace.exe) attempted to load \Device\HarddiskVolume3\Users\ChrisCornell\AppData\Local\Temp\TRA4694.tmp that did not meet the Enterprise signing level requirements or violated code integrity policy (Policy ID:{63d1178a-816a-4ab6-8ecd-127f2df0ce47}). However, due to code integrity auditing policy, the image was allowed to load.

# App Control for Business Policy

- Deleting Policy results in removal from the Windows Endpoint
  - But stay in effect until next reboot!

# Old school applocker?

- XML import in Intune for quick migration

# Reuse Applocker Policies (1)

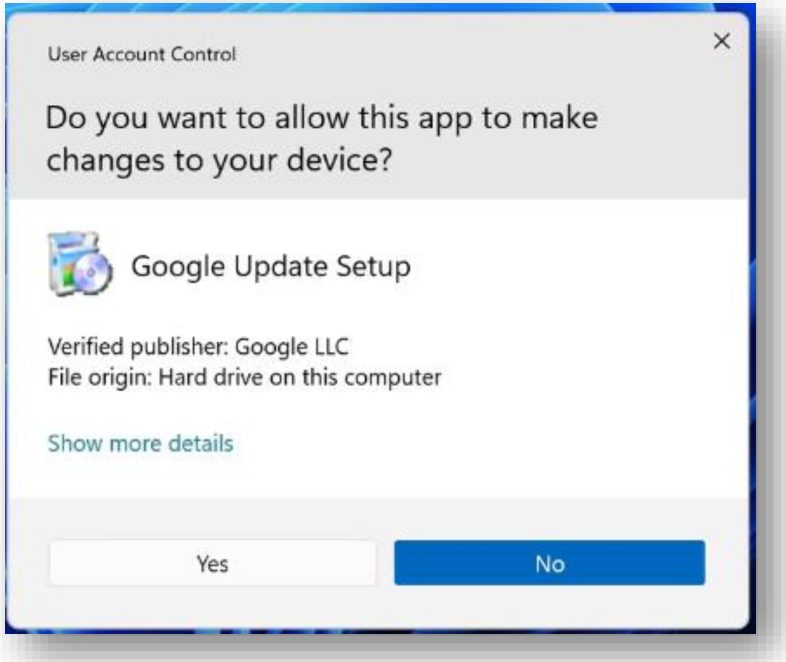
- XML import in Intune for quick migration
  - Using secpol.msc export Application Control Policies in XML Format
  - Create new Device Configuration Profile in Intune (Custom)
  - Add OMA-URI setting – example for EXE files:
    - Name: Applocker Demo
    - Description: Executables Rule
    - OMA-URI: ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/apps/EXE/Policy
    - Data type: String
    - Value: Copy and Paste XML file content from <RuleCollection Type> to </RuleConnection>

# Reuse Applocker Policies (2)

- Also works for other file types
  - MSI: ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/apps/MSI/Policy
  - Script: ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/apps/Script/Policy
  - Appx: ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/apps/StoreApps/Policy
  - DLL: ./Vendor/MSFT/AppLocker/ApplicationLaunchRestrictions/apps/DLL/Policy

# User Account Control (UAC)

- Designed to protect the operating system from unauthorized changes
- Notifies user when change requires admin permissions
- Enabled by default // Manageable through policy



User Account Control

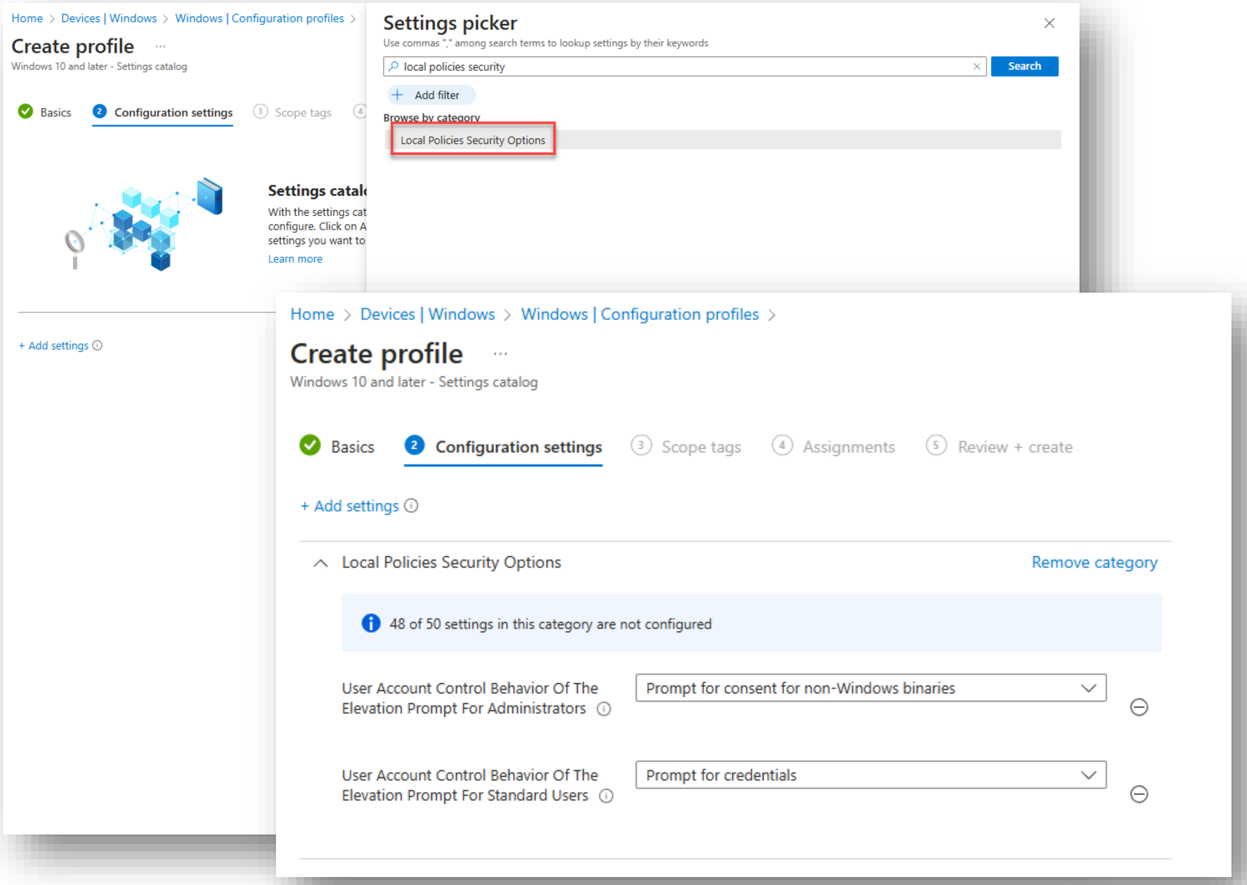
Do you want to allow this app to make changes to your device?

Google Update Setup

Verified publisher: Google LLC
File origin: Hard drive on this computer

# UAC Policy – Configuration

- Using Intune Settings Catalog



With the settings cat
configure. Click on A
settings you want to

Use commas "," among search terms to lookup settings by their keywords

local policies security

48 of 50 settings in this category are not configured

User Account Control Behavior Of The Elevation Prompt For Administrators: Prompt for consent for non-Windows binaries

User Account Control Behavior Of The Elevation Prompt For Standard Users: Prompt for credentials

# Demo - Apps

User

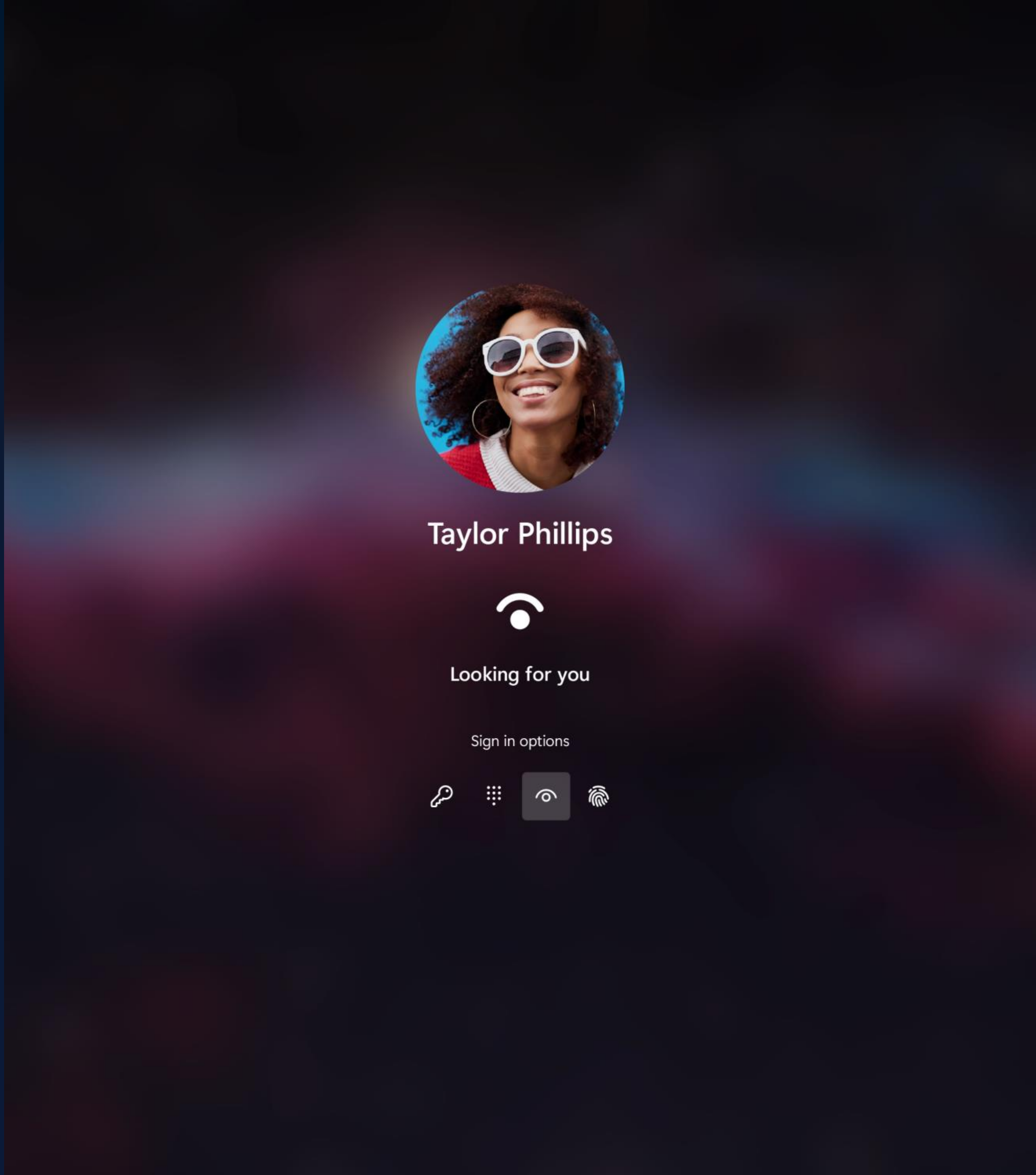
# Identity and access security: Windows Hello for Business

## User friendly and privacy protecting

- Sign on simply and securely with passwordless authentication.
- **Biometrics** or a **PIN**
- Biometrics **never leave the device**
- Now supports **multiple camera** with enablement of the external camera when docking.
- Secure camera and fingerprint implementations using enhanced sign-in security
- **SSO** with Windows apps
- **Private key is never shared**

## Enterprise-grade

- Strong **multi-factor** authentication
- **Asymmetric key pair** auth model
- Can be deployed in **cloud**, **hybrid** or **on-premises** environments.
- **Key-** or **certificate-based** options
- For hybrid deployments the PKI requirements, and the need to sync keys from AAD to AD were removed.



User

Identity and Privacy

# Identity and access security: Passwordless authentication

### Overview

- Standards-based multi-factor authentication
- Supports TOTP, Push Approvals, Biometrics + Number Match

### Windows

Passwordless authentication

- Device registration in OOBE
- Windows Hello provisioning

### Mobile

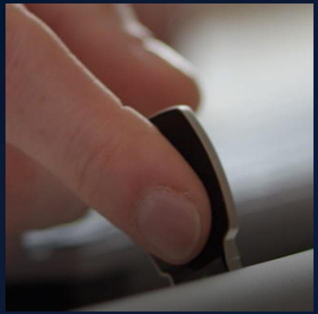
- SSO to native mobile apps

## Identity and access security: Passwordless with FIDO2 security keys

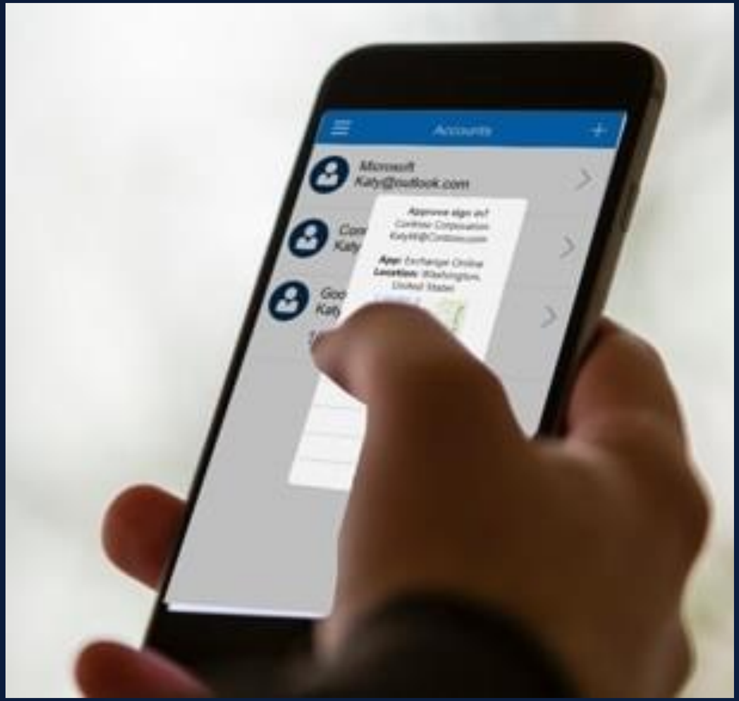
Protect your organization against the most damaging remote credential stealing and phishing attacks

USB/NFC Key

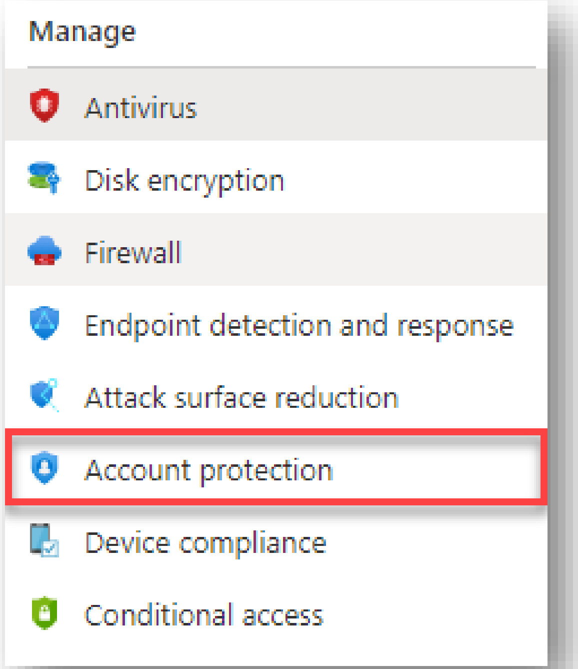
NFC & BLE



USB Biometric Key

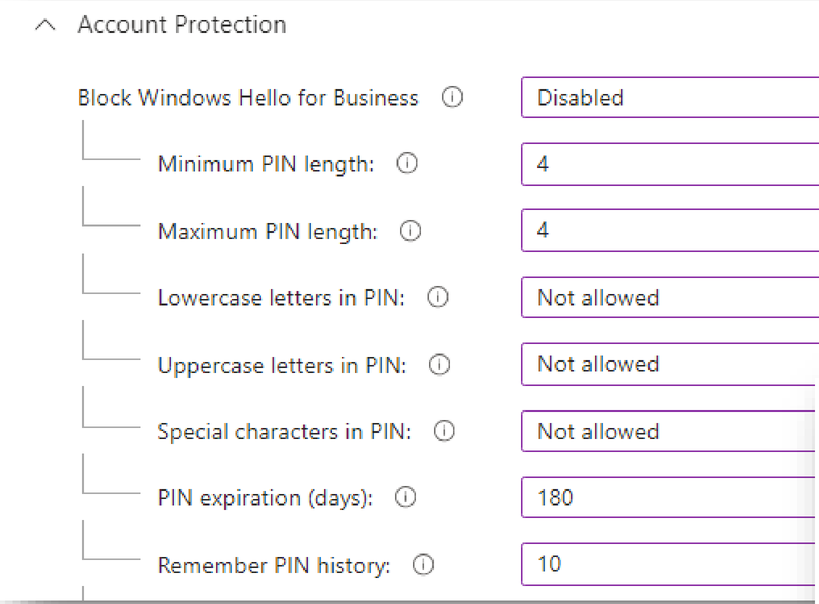


# Windows Hello for Business Profile



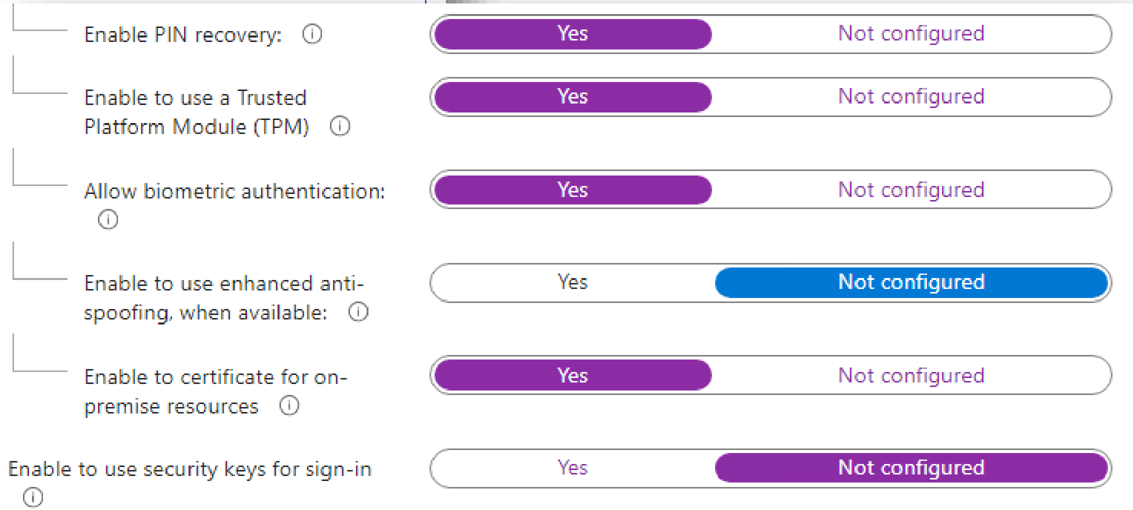
Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access



Account Protection

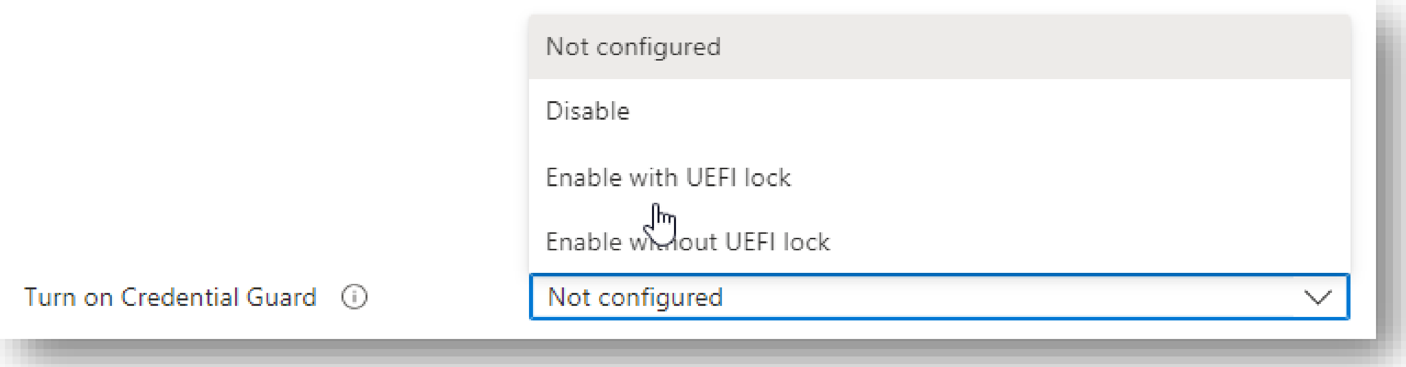
| | |
|---|---|
| Block Windows Hello for Business | Disabled |
| Minimum PIN length: | 4 |
| Maximum PIN length: | 4 |
| Lowercase letters in PIN: | Not allowed |
| Uppercase letters in PIN: | Not allowed |
| Special characters in PIN: | Not allowed |
| PIN expiration (days): | 180 |
| Remember PIN history: | 10 |



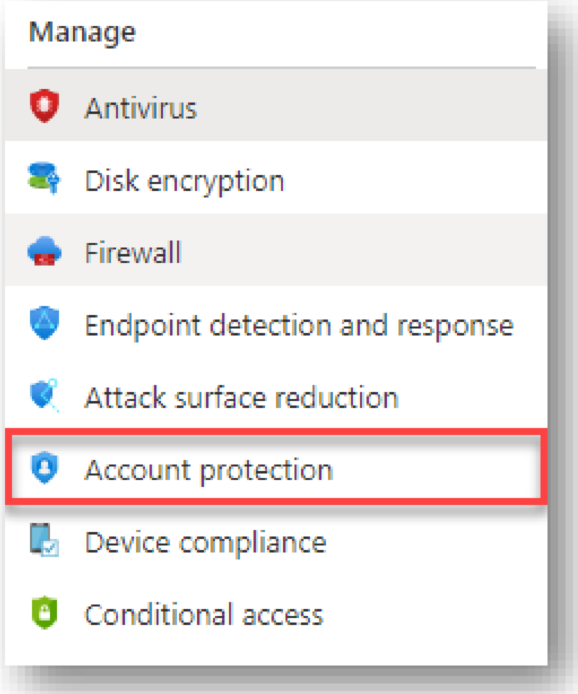
| | |
|---|---|
| Enable PIN recovery: | [✓ Yes] Not configured |
| Enable to use a Trusted Platform Module (TPM) | [✓ Yes] Not configured |
| Allow biometric authentication: | [✓ Yes] Not configured |
| Enable to use enhanced anti-spoofing, when available: | Yes [✓ Not configured] |
| Enable to certificate for on-premise resources | [✓ Yes] Not configured |
| Enable to use security keys for sign-in | Yes [✓ Not configured] |

# Credential Guard Profile

- Enabled by default on Win11 22H2 and later
- Enable or disable via Intune
- With or without UEFI Lock
- Relies on VBS (virtualization-based security)



Turn on Credential Guard ⓘ Not configured



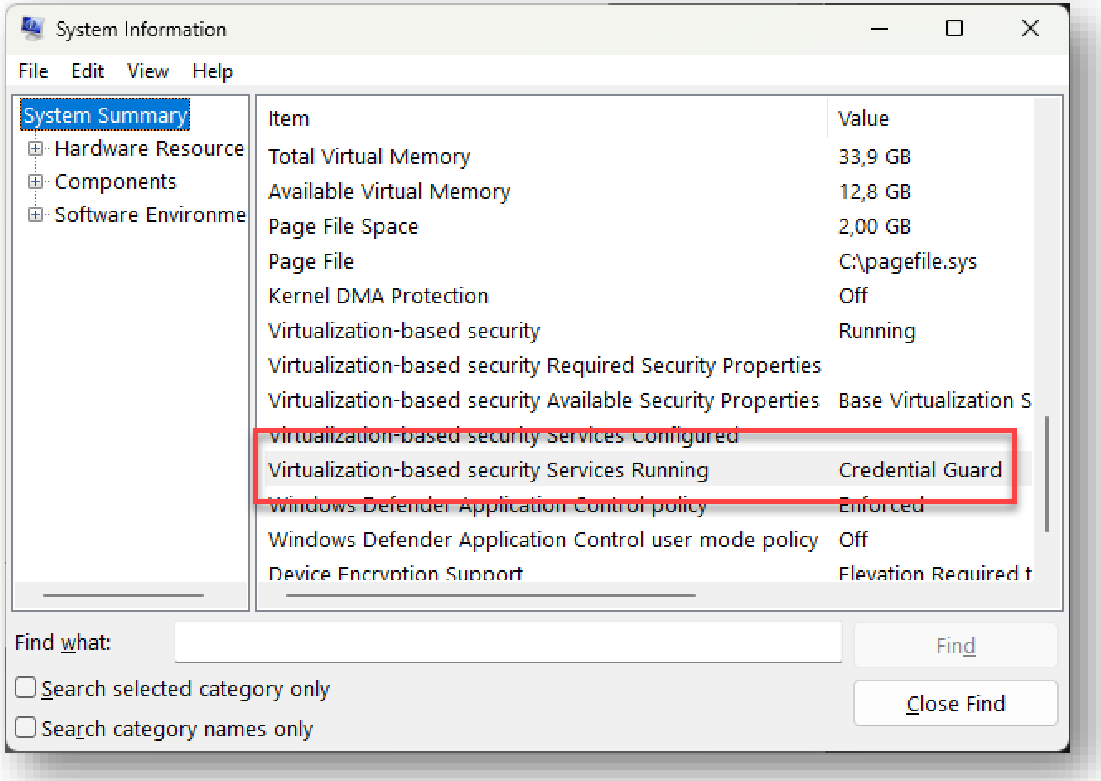
# Credential and Device Guard Readiness Tool

https://www.microsoft.com/en-us/download/details.aspx?id=53337

1. Check if the device can run Device Guard or Credential Guard
2. Check if the device is compatible with the Hardware Lab Kit tests that are ran by partners
3. Enable and disable Device Guard or Credential Guard
4. Check the status of Device Guard or Credential Guard on the device
5. Integrate with System Center Configuration Manager or any other deployment mechanism to configure registry settings that reflect the device capabilities
6. Use an embedded ConfigCI policy in audit mode that can be used by default to enable Device Guard when a custom policy is not provided

# Credential Guard – Verify configuration (1)

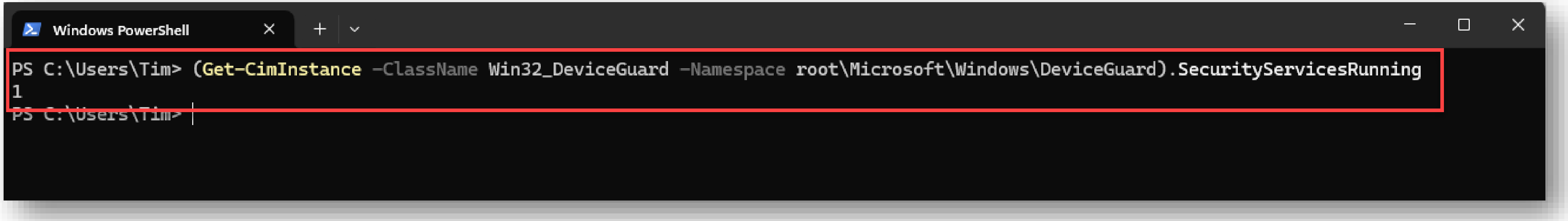
- Via MSInfo32



| Item | Value |
|---|---|
| Total Virtual Memory | 33,9 GB |
| Available Virtual Memory | 12,8 GB |
| Page File Space | 2,00 GB |
| Page File | C:\pagefile.sys |
| Kernel DMA Protection | Off |
| Virtualization-based security | Running |
| Virtualization-based security Required Security Properties | |
| Virtualization-based security Available Security Properties | Base Virtualization S |
| Virtualization-based security Services Configured | |
| Virtualization-based security Services Running | Credential Guard |
| Windows Defender Application Control policy | Enforced |
| Windows Defender Application Control user mode policy | Off |
| Device Encryption Support | Elevation Required t |

# Credential Guard – Validate configuration (2)

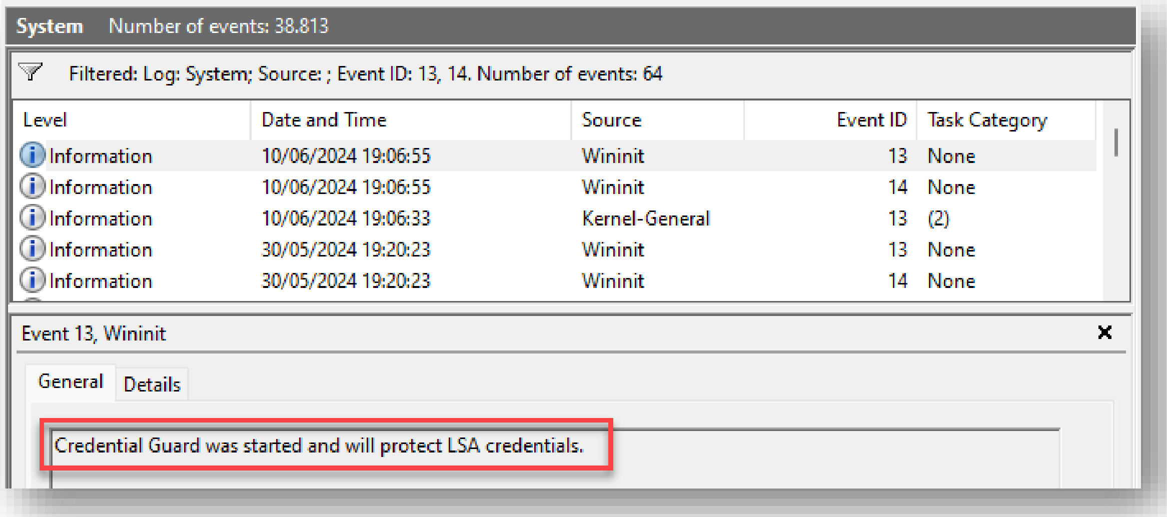
- Via Powershell
  - (Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning
  - Output
    - 0: Credential Guard is disabled (not running)
    - 1: Credential Guard is enabled (running)



```
PS C:\Users\Tim> (Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning
1
PS C:\Users\Tim>
```

# Credential Guard – Validate configuration (3)

- Via EventVwr
  - System Log
  - Look for Event IDs 13 – 14 – 15 – 16 and 17



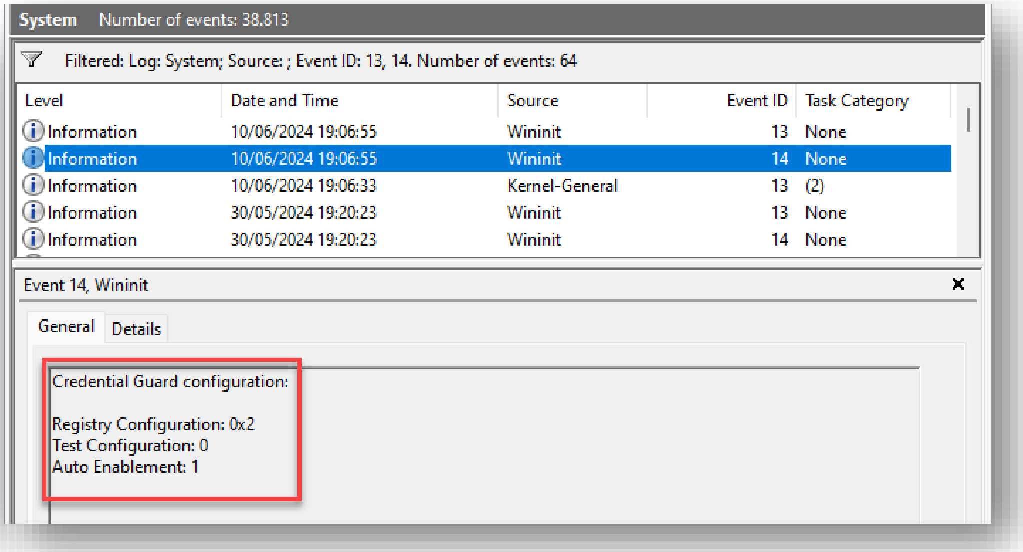
**System** Number of events: 38.813

Filtered: Log: System; Source: ; Event ID: 13, 14. Number of events: 64

| Level | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Information | 10/06/2024 19:06:55 | Wininit | 13 | None |
| Information | 10/06/2024 19:06:55 | Wininit | 14 | None |
| Information | 10/06/2024 19:06:33 | Kernel-General | 13 | (2) |
| Information | 30/05/2024 19:20:23 | Wininit | 13 | None |
| Information | 30/05/2024 19:20:23 | Wininit | 14 | None |

Event 13, Wininit

Credential Guard was started and will protect LSA credentials.



**System** Number of events: 38.813

Filtered: Log: System; Source: ; Event ID: 13, 14. Number of events: 64

| Level | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Information | 10/06/2024 19:06:55 | Wininit | 13 | None |
| Information | 10/06/2024 19:06:55 | Wininit | 14 | None |
| Information | 10/06/2024 19:06:33 | Kernel-General | 13 | (2) |
| Information | 30/05/2024 19:20:23 | Wininit | 13 | None |
| Information | 30/05/2024 19:20:23 | Wininit | 14 | None |

Event 14, Wininit

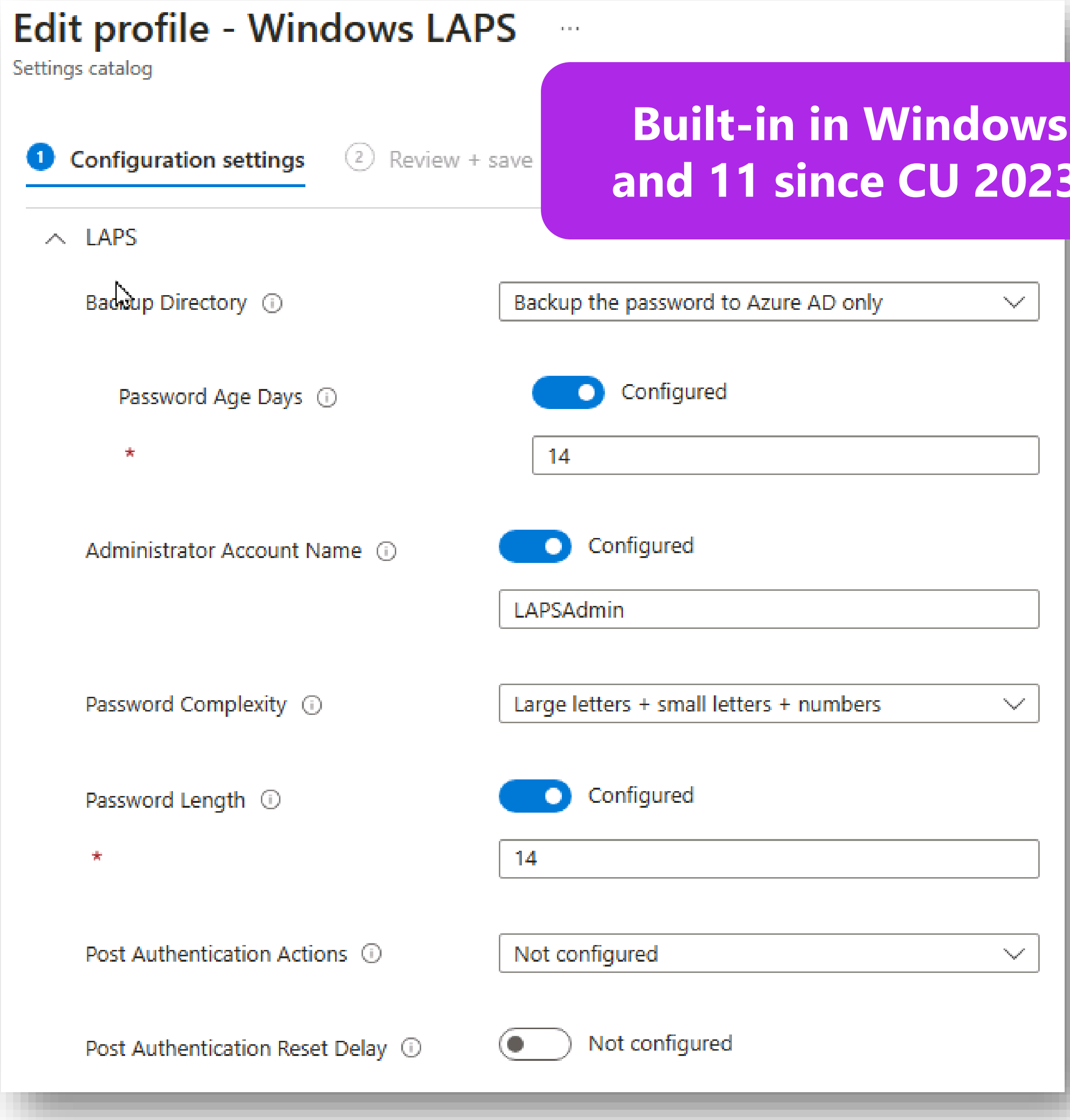
Credential Guard configuration:

Registry Configuration: 0x2
Test Configuration: 0
Auto Enablement: 1

# Configuring via Intune

### Windows LAPS

- Protection against pass-the-hash and lateral-traversal attacks
- Improved security for remote help desk scenarios
- Ability to sign in to and recover devices that are otherwise inaccessible
- Fine-grained security model
- Support for the Azure role-based access control model for securing passwords that are stored in Azure Active Directory



Edit profile - Windows LAPS

Settings catalog

LAPS

Backup Directory: Backup the password to Azure AD only

Password Age Days: Configured

* 14

Administrator Account Name: Configured

LAPSAdmin

Password Complexity: Large letters + small letters + numbers

Password Length: Configured

* 14

Post Authentication Actions: Not configured

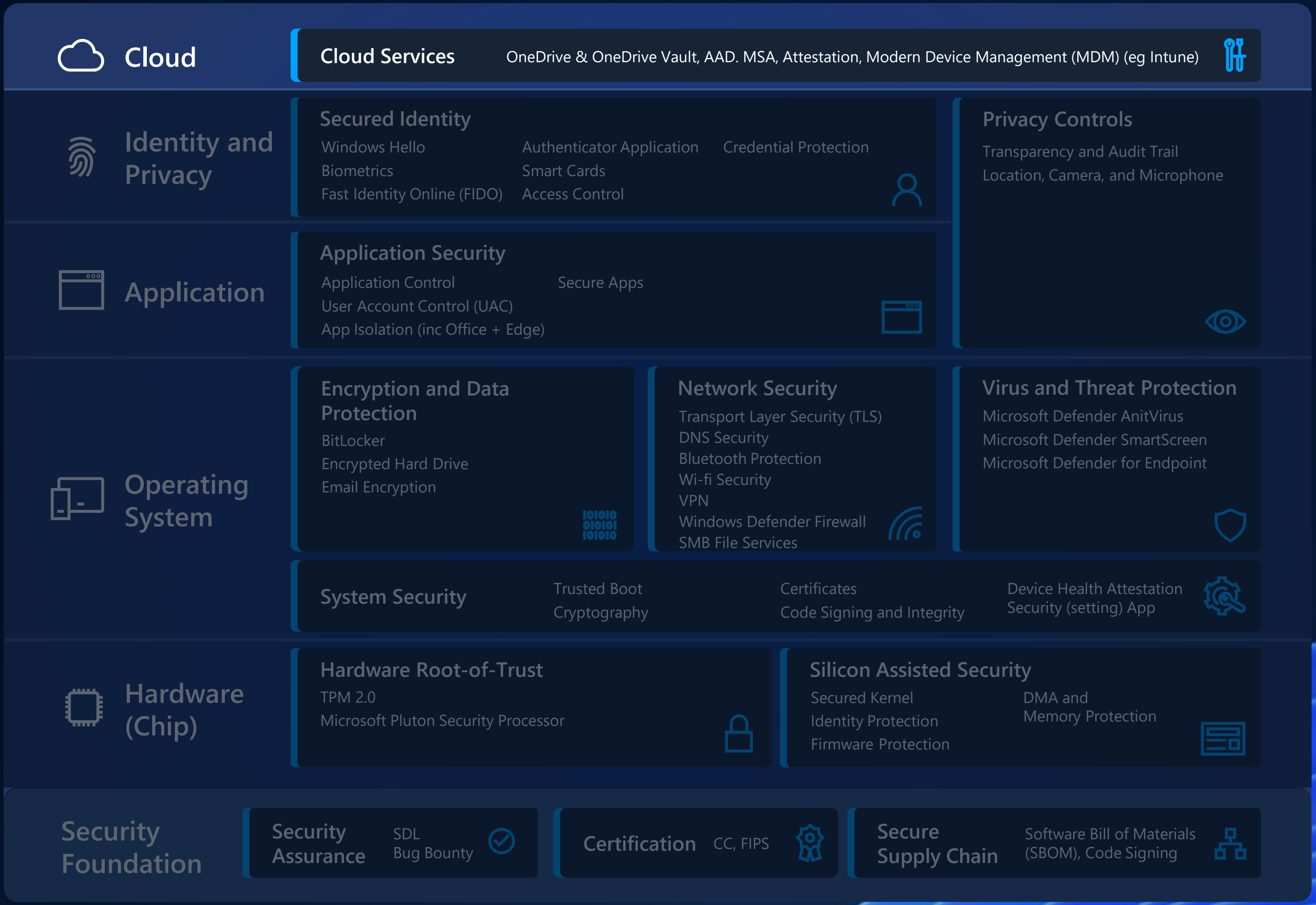
Post Authentication Reset Delay: Not configured

**Built-in in Windows 10 and 11 since CU 2023-04**

# Cloud Overview

Windows 11 works with Microsoft cloud services to help organizations strengthen their multi-cloud security infrastructure, protect hybrid cloud workloads, and safeguard sensitive information while controlling access and mitigating threats. You can:

- **Store and protect your files in the cloud** with Microsoft OneDrive including OneDrive.[1]
- **Provide secure access, identity management, and single sign-on** to apps and services from anywhere.[2]
- **Enforce security compliance and conditional access** with Microsoft Intune.[1,2]
- **Ensure the health and safety of devices** connecting to networks with Microsoft Azure Attestation.



Cloud

Cloud Services — OneDrive & OneDrive Vault, AAD. MSA, Attestation, Modern Device Management (MDM) (eg Intune)

Identity and Privacy

Secured Identity — Windows Hello, Biometrics, Fast Identity Online (FIDO), Authenticator Application, Smart Cards, Access Control, Credential Protection

Privacy Controls — Transparency and Audit Trail, Location, Camera, and Microphone

Application

Application Security — Application Control, User Account Control (UAC), App Isolation (inc Office + Edge), Secure Apps

Operating System

Encryption and Data Protection — BitLocker, Encrypted Hard Drive, Email Encryption

Network Security — Transport Layer Security (TLS), DNS Security, Bluetooth Protection, Wi-fi Security, VPN, Windows Defender Firewall, SMB File Services

Virus and Threat Protection — Microsoft Defender AnitVirus, Microsoft Defender SmartScreen, Microsoft Defender for Endpoint

System Security — Trusted Boot, Cryptography, Certificates, Code Signing and Integrity, Device Health Attestation, Security (setting) App

Hardware (Chip)

Hardware Root-of-Trust — TPM 2.0, Microsoft Pluton Security Processor

Silicon Assisted Security — Secured Kernel, Identity Protection, Firmware Protection, DMA and Memory Protection

Security Foundation

Security Assurance — SDL, Bug Bounty

Certification — CC, FIPS

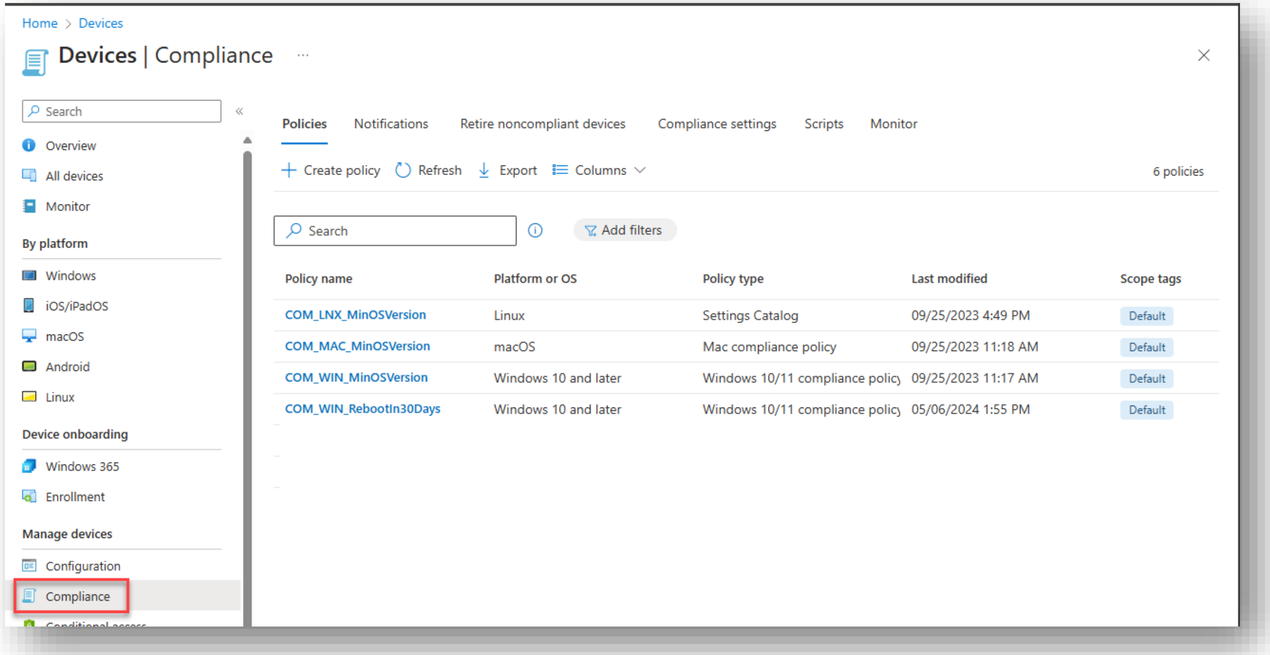
Secure Supply Chain — Software Bill of Materials (SBOM), Code Signing

[1] Sold separately

[2] Requires Azure Active Directory; sold separately

# Compliance Policies in Intune

- Rules and conditions used to evaluate device configuration
- Helps securing organizational data from devices not meeting requirements
- Integration with Conditional Access – only allow compliant devices to access data



| Policy name | Platform or OS | Policy type | Last modified | Scope tags |
|---|---|---|---|---|
| COM_LNX_MinOSVersion | Linux | Settings Catalog | 09/25/2023 4:49 PM | Default |
| COM_MAC_MinOSVersion | macOS | Mac compliance policy | 09/25/2023 11:18 AM | Default |
| COM_WIN_MinOSVersion | Windows 10 and later | Windows 10/11 compliance policy | 09/25/2023 11:17 AM | Default |
| COM_WIN_RebootIn30Days | Windows 10 and later | Windows 10/11 compliance policy | 05/06/2024 1:55 PM | Default |

# Compliance policy settings – Configuration

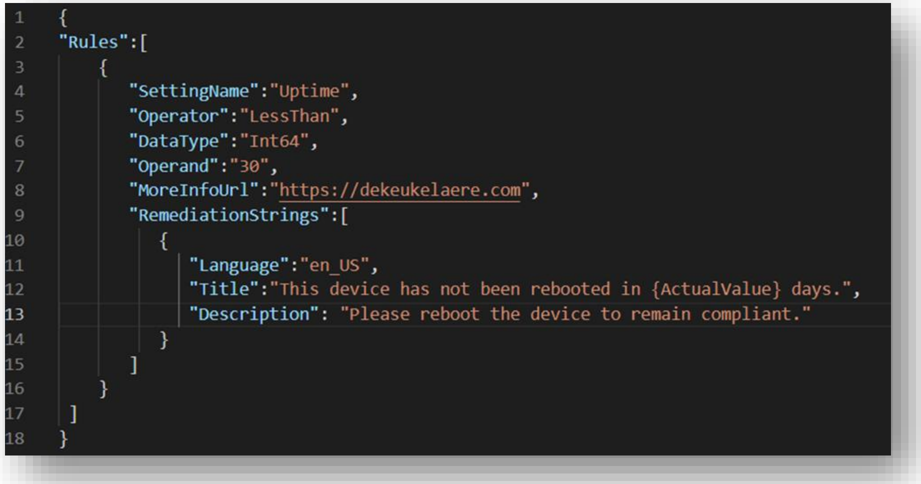
- Tenant-Wide Settings
- Mark devices with no Compliance Policy
  - Compliant (default)
  - Not Compliant
- Compliance Status validity period
  - Period in which device must report compliance
  - Default is 30 days // can be set from 1 – 120 days
  - If not reported in time, device is marked non-compliant

# Device Compliance Policies – Configuration

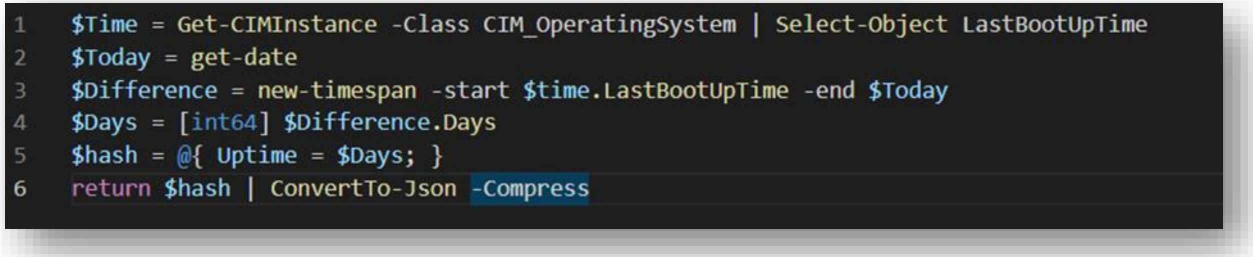
- Built-in rules and settings for compliance
  - Minimum OS Version
  - Jail-broken and rooted devices
  - Threat Level (when integrating w threat mgmt. tools)
- Define actions for non compliance
  - Mark device as non-compliant (default)
  - Notify user via email
  - Remote Lock
  - Mark for retirement

# Device Compliance Policies – Configuration

- Custom Compliance
  - Windows and Linux only
- Built on 2 components
  - JSON file --- Defines what to check
  - Powershell Script --- Performs the check
- Marks device as (non-) compliant based on outcome

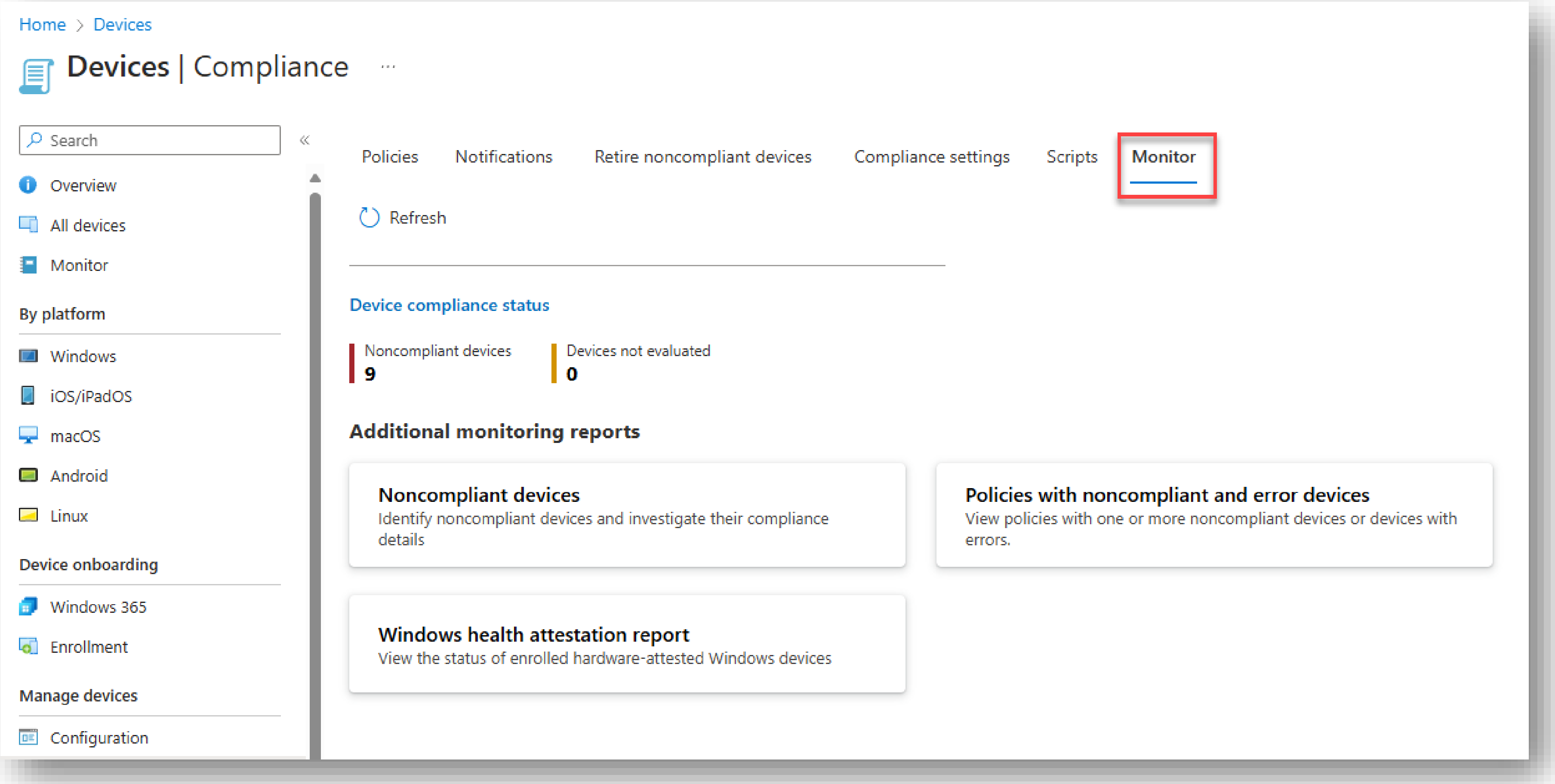


```json
{
"Rules":[
    {
       "SettingName":"Uptime",
       "Operator":"LessThan",
       "DataType":"Int64",
       "Operand":"30",
       "MoreInfoUrl":"https://dekeukelaere.com",
       "RemediationStrings":[
          {
             "Language":"en_US",
             "Title":"This device has not been rebooted in {ActualValue} days.",
             "Description": "Please reboot the device to remain compliant."
          }
       ]
    }
 ]
}
```



```powershell
$Time = Get-CIMInstance -Class CIM_OperatingSystem | Select-Object LastBootUpTime
$Today = get-date
$Difference = new-timespan -start $time.LastBootUpTime -end $Today
$Days = [int64] $Difference.Days
$hash = @{ Uptime = $Days; }
return $hash | ConvertTo-Json -Compress
```

# Compliance policy settings – Validating



Device compliance status

Noncompliant devices
9

Devices not evaluated
0

Additional monitoring reports

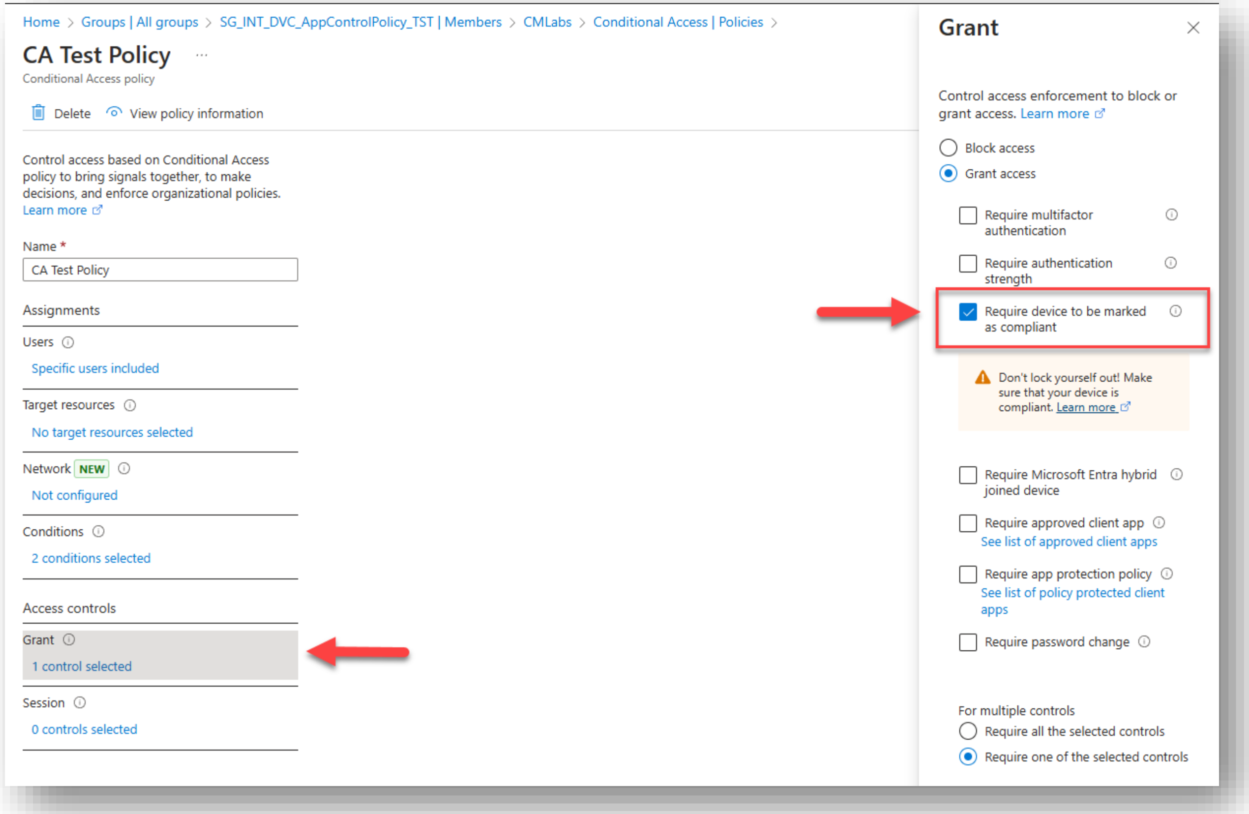
**Noncompliant devices**
Identify noncompliant devices and investigate their compliance details

**Policies with noncompliant and error devices**
View policies with one or more noncompliant devices or devices with errors.

**Windows health attestation report**
View the status of enrolled hardware-attested Windows devices

# Conditional Access and Compliance

- Compliance information is sent to Microsoft Entra ID where Conditional Access decides to grant or block access to resources.



Home > Groups | All groups > SG_INT_DVC_AppControlPolicy_TST | Members > CMLabs > Conditional Access | Policies >

CA Test Policy ...

Conditional Access policy

Delete   View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

CA Test Policy

Assignments

Users

Specific users included

Target resources

No target resources selected

Network NEW

Not configured

Conditions

2 conditions selected

Access controls

Grant

1 control selected

Session

0 controls selected

Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

□ Require multifactor authentication

□ Require authentication strength

☑ Require device to be marked as compliant

Don't lock yourself out! Make sure that your device is compliant. Learn more

□ Require Microsoft Entra hybrid joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy
See list of policy protected client apps

□ Require password change

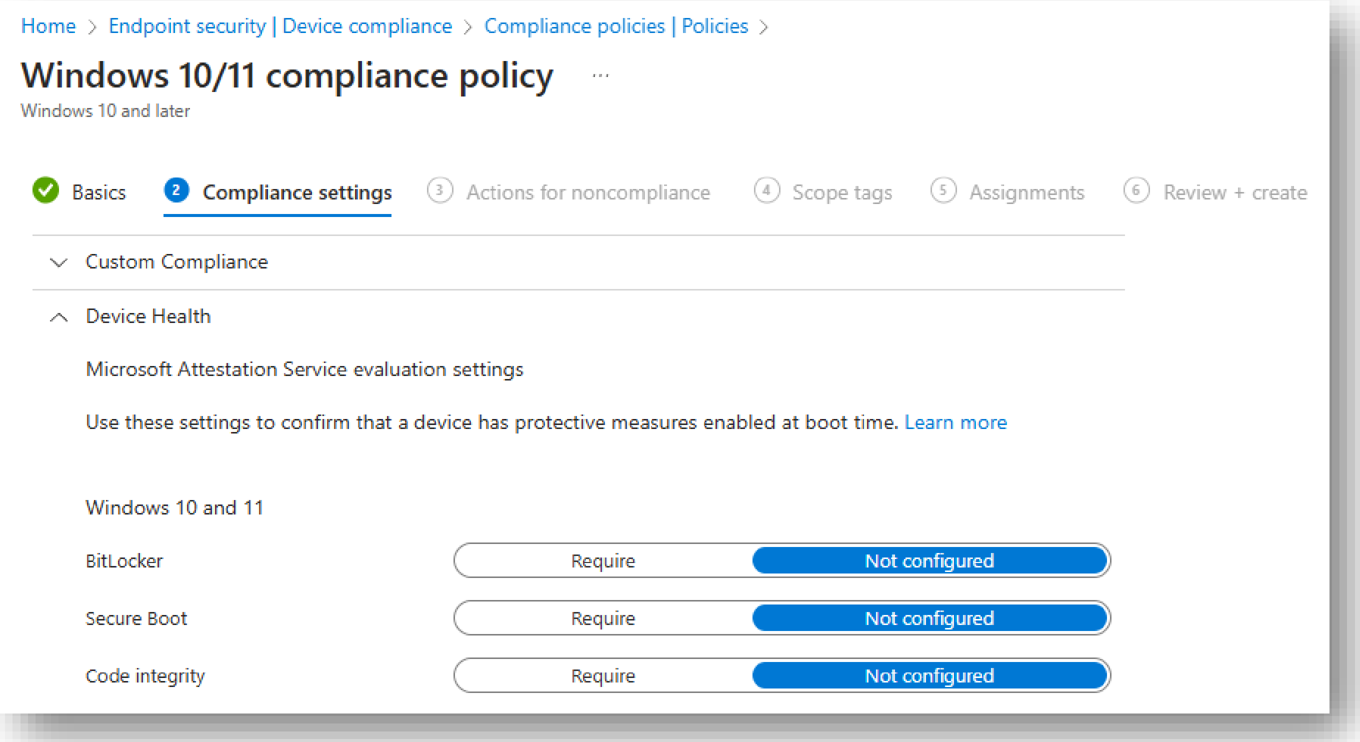
For multiple controls

○ Require all the selected controls

● Require one of the selected controls

# Credential Guard - Validate configuration (4)

- Intune Compliance



Home > Endpoint security | Device compliance > Compliance policies | Policies >

Windows 10/11 compliance policy ...

Windows 10 and later

✓ Basics · 2 Compliance settings · 3 Actions for noncompliance · 4 Scope tags · 5 Assignments · 6 Review + create

Custom Compliance

Device Health

Microsoft Attestation Service evaluation settings

Use these settings to confirm that a device has protective measures enabled at boot time. Learn more

Windows 10 and 11

| | | |
|---|---|---|
| BitLocker | Require | Not configured |
| Secure Boot | Require | Not configured |
| Code integrity | Require | Not configured |

# Demo - Cloud