

# Microsoft Endpoint Manager

## Compliance Policy

- 1 Overview of Compliance Rules in SCCM
- 2 Switch Compliance Policy from SCCM to Intune
- 3 How to Configure Compliance Policies with Intune
- 4 How to Configure Conditional Access with Intune
- 4 Microsoft 365 Compliance Manager - Templates

# Overview of Compliance Rules in SCCM

---

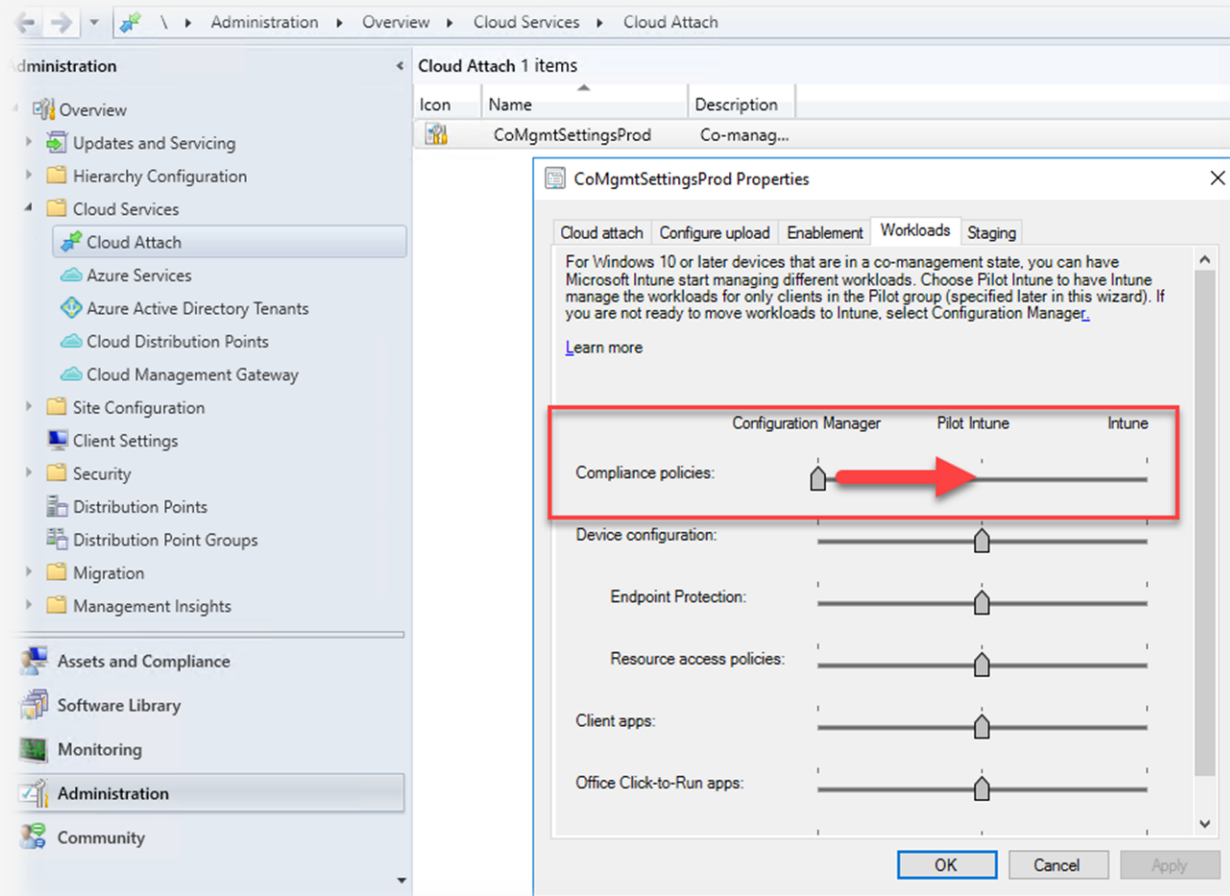


- Monitor, report and remediate device configurations
- Use group policy to enforce device security and SCCM compliance policy can be used to check if the device is compliant or non-compliant and remediate if needed
- You can still use SCCM Compliance items with Intune



# Switch Compliance policy to Intune

- Switch Compliance policy workload from SCCM to Intune



# Compliance Policies with Intune

---

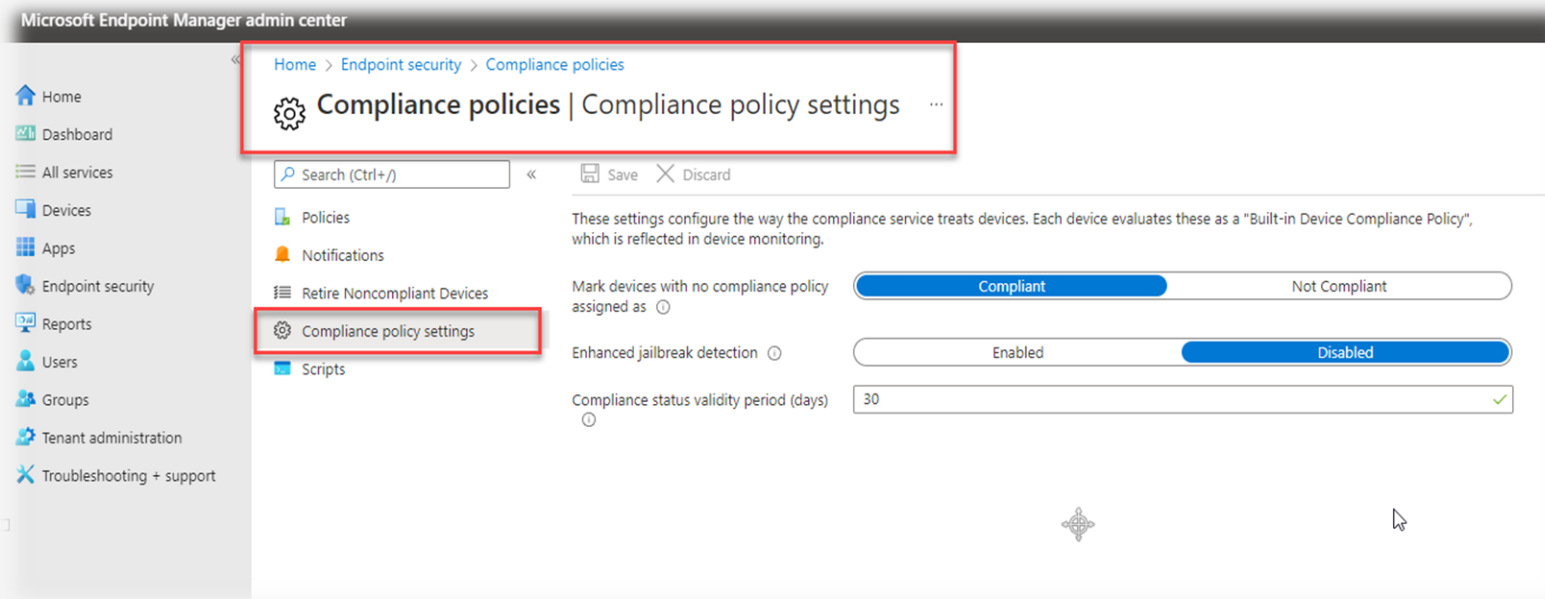


- Intune can help organizations to protect their data from their user devices by using the Intune Compliance Policy to meet the compliance security compliance.
- Compliance policies in Intune:
  - Configure compliance policy rules and settings that organization user's devices must meet to be compliant.
  - These rules are actions which will check user's devices against compliance rules that being set by their organizations and mark them as compliant or non-compliant.
  - Can be combined with Conditional Access, which can then block users and devices that don't meet the rules.



## There are two parts to compliance policies in Intune:

- **Compliance policy settings** – Tenant-wide settings that are like a built-in compliance policy that every device receives. Compliance policy settings set a baseline for how compliance policy works in your Intune environment, including whether devices that haven't received any device compliance policies are compliant or noncompliant.



Microsoft Endpoint Manager admin center

Home > Endpoint security > Compliance policies

Compliance policies | Compliance policy settings

Search (Ctrl+/) Save Discard

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as  Compliant  Not Compliant

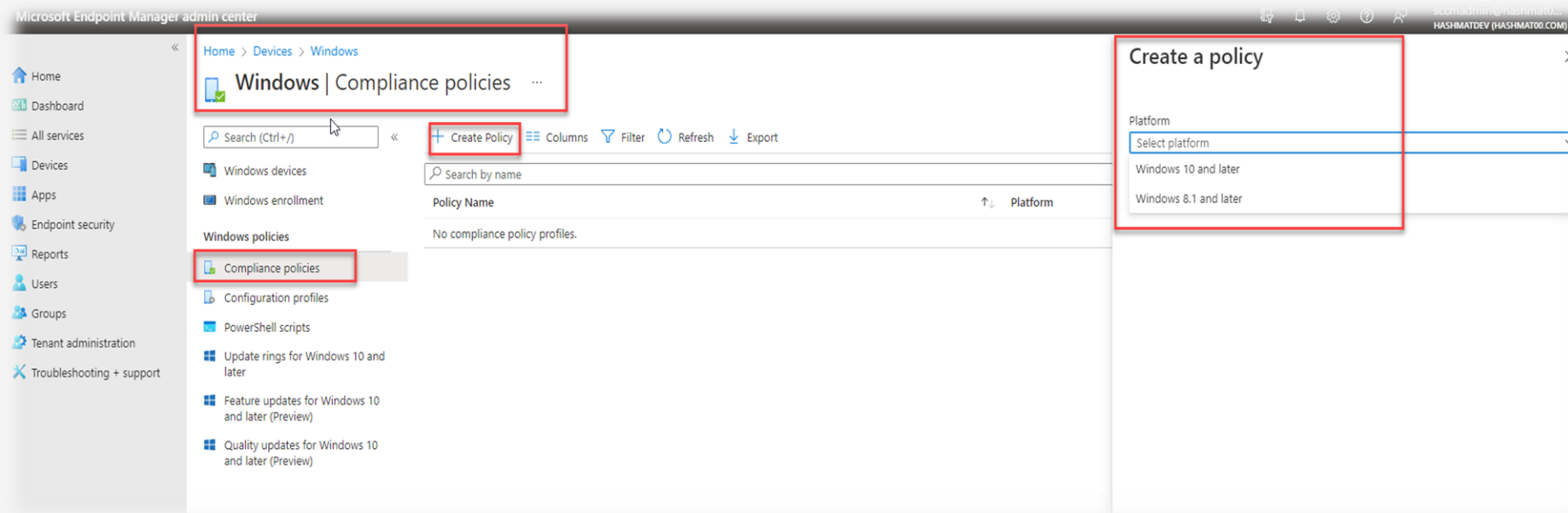
Enhanced jailbreak detection  Enabled  Disabled

Compliance status validity period (days) 30 ✓

The screenshot shows the Microsoft Endpoint Manager admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Compliance policies | Compliance policy settings'. It includes a search bar, 'Save' and 'Discard' buttons, and a description: 'These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.' There are three settings: 'Mark devices with no compliance policy assigned as' with a radio button selected for 'Compliant'; 'Enhanced jailbreak detection' with a radio button selected for 'Disabled'; and 'Compliance status validity period (days)' with a text input field containing '30' and a green checkmark icon.

# There are two parts to compliance policies in Intune:

- **Device compliance policy** – Platform-specific rules you configure and deploy to groups of users or devices. These rules define requirements for devices, like minimum operating systems or the use of disk encryption. Devices must meet these rules to be considered compliant.



The screenshot displays the Microsoft Endpoint Manager admin center interface. The breadcrumb navigation path is 'Home > Devices > Windows', with 'Windows' highlighted. The main content area shows 'Windows | Compliance policies' with a '+ Create Policy' button. A 'Create a policy' dialog box is open, showing a 'Platform' dropdown menu with options: 'Select platform', 'Windows 10 and later', and 'Windows 8.1 and later'. The 'Create Policy' button and the 'Compliance policies' link in the left sidebar are also highlighted with red boxes.

# Conditional Access with Intune

---



- When you use Conditional Access, you can configure your Conditional Access policies to use the results of your device compliance policies to determine which devices can access your organizational resources. This access control is in addition to and separate from the actions for noncompliance that you include in your device compliance policies.
- When a device enrolls in Intune it registers in Azure AD. The compliance status for devices is reported to Azure AD. If your Conditional Access policies have Access controls set to Require device to be marked as compliant, Conditional access uses that compliance status to determine whether to grant or block access to email and other organization resources.
- If you'll use device compliance status with Conditional Access policies, review how your tenant has configured Mark devices with no compliance policy assigned as, which you manage under Compliance policy settings.





# Microsoft 365 Compliance Manager

---



- Microsoft Compliance Manager is a feature in the Microsoft 365 compliance center that helps you manage your organization's compliance requirements with greater ease and convenience.
- Microsoft Compliance Manager provides a comprehensive set of templates for creating assessments. These templates can help your organization comply with national, regional, and industry-specific requirements governing the collection and use of data.
- Templates are added to Compliance Manager as new laws and regulations are enacted. Compliance Manager also updates its templates when the underlying laws or regulations change
- <https://compliance.microsoft.com/compliancemanager>



# Microsoft 365 Compliance Manager



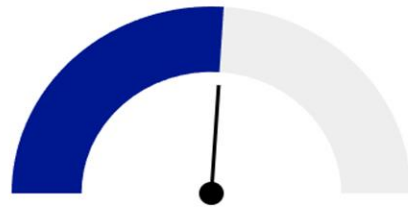
compliance.microsoft.com/compliancemanager/viewid=overview

Microsoft 365 compliance

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Trials
- Solutions
  - Catalog
  - Audit
  - Content search
  - Communication compliance
  - Data loss prevention
  - eDiscovery
  - Information governance
  - Information protection
  - Information Barriers
  - Insider risk management
  - Records management

## Overall compliance score

Your compliance score: **52%**



12210/23448 points achieved

Your points achieved **259** / 11497

Microsoft managed points achieved **11951** / 11951

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

[Learn how your Compliance score is calculated](#)

## Compliance score breakdown

### Protect information

**4%**

54/1350 points achieved

## Key improvement actions

Not completed **844** | Completed **9** | Out of scope **0**

Improvement action	Impact	Test status	Group	Action type
Enable self-service password reset	+27 points	Failed high risk	Default Group	Technical
Conceal information with lock screen	+27 points	None	Default Group	Technical
Use boundary protection devices for unclas...	+27 points	None	Default Group	Technical
Wide just-in-time notification or system ...	+27 points	None	Default Group	Technical
Block email application from creating child ...	+27 points	None	Default Group	Technical
Block outdated ActiveX controls	+27 points	None	Default Group	Technical
Disable 'Domain member: Disable machine...	+27 points	None	Default Group	Technical
Enable 'Consistent MIME Handling'	+27 points	None	Default Group	Technical
Enable cloud-delivered protection	+27 points	None	Default Group	Technical

[View all improvement actions](#)

## Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remaining actions
Audit	0/61 points	7
Azure	0/112 points	6
Azure Active Direct...	178/1024 points	46
Communication co...	0/37 points	5
Compliance Manager	27/3561 points	442
Data classification	0/57 points	3
Data loss prevention	0/216 points	8
Defender for Cloud ...	0/194 points	16
eDiscovery	0/27 points	1

[View all solutions](#)

### Govern information

**0%**

0/326 points achieved

### Control access

**14%**

178/1268 points achieved

### Manage devices

**0%**

0/1505 points achieved



- **Use compliance policies to set rules for devices you manage with Intune**
  - <https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>
- **Device Compliance settings for Windows 10/11 in Intune**
  - <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows>
- **Microsoft 365 Compliance Manager**
  - <https://compliance.microsoft.com/compliancemanager>