

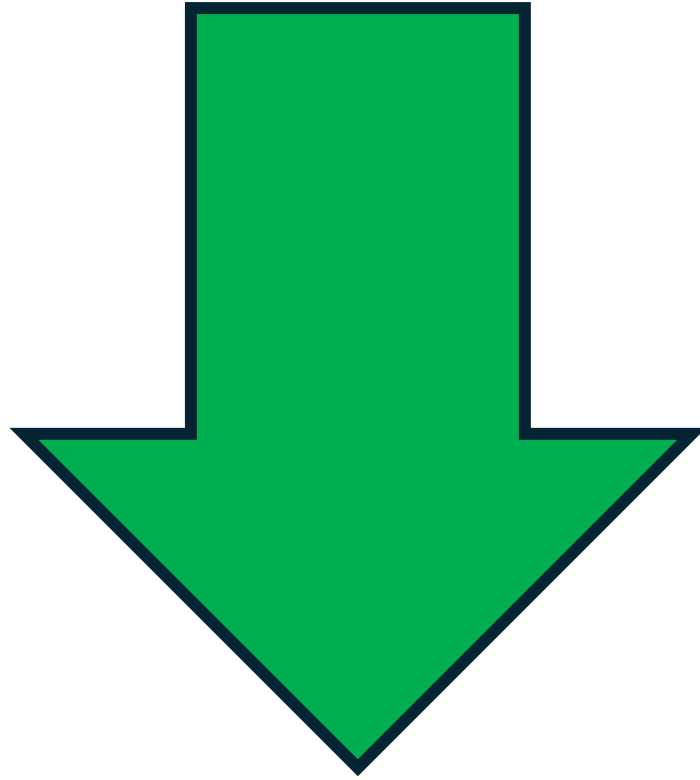
The Essential 8 in a Microsoft 365 world

July 2024

@directorcia

<http://about.me/ciaops>

Good security



Reduces Risk

Good security

Is boring



Boring is

Repetitive

Consistent

Simple

Dependable

A hand in a light-colored suit sleeve points to a specific location on a dense, multi-colored transit map. The map features a complex network of lines in blue, orange, red, green, and purple, representing different transit routes. The background is slightly blurred, focusing attention on the hand and the map.

What is a Framework?

A set of guidelines, tools, and best practices that are designed to structure and support the development of a specific project or system.

It provides a standardized approach to address common issues and tasks, ensuring consistency, efficiency, and quality.

You will be measured
against the security
framework you choose

- Customers
- Boards
- Insurance companies
- Competitors



Essential Eight

“Foundational cyber security measures that make it much harder for adversaries to compromise systems”

The mitigation strategies that constitute the Essential Eight are:

1. Patch applications
2. Patch operating systems
3. Multi-factor authentication
4. Restrict administrative privileges
5. Application control
6. Restrict Microsoft Office macros
7. User application hardening
8. Regular backups

Essential Eight Maturity Levels:

Based on mitigating increasing levels of tradecraft (i.e. tools, tactics, techniques and procedures) and targeting

Level 1 - malicious actors who are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, a system.

Level 2 - malicious actors operating with a modest step-up in capability from the previous maturity level.

Level 3 - malicious actors who are more adaptive and much less reliant on public tools and techniques.

Some limitations of the Essential Eight are:

1. Designed for Windows devices only
2. Doesn't address mobiles
3. Not designed for Cloud
4. Not aimed at SMB
5. Not a standard, it's a framework
6. Point in time activity
7. Doesn't address emerging technologies like AI

Services you'll need for Microsoft Cloud with Essential 8

1. Entra ID
2. Intune
3. Defender for Endpoint
4. Sentinel
5. Purview

The minimum starting point will therefore typically be:

Microsoft 365 Business Premium

Because of:

- Conditional Access
- Defender for Business
- Intune
- Litigation Hold
- And More

Handy Links

<https://learn.microsoft.com/en-us/compliance/essential-eight/e8-overview>

<https://m365maps.com/files/Essential-8.htm>

Patch Applications

More help can be found at: <https://aka.ms/winget-command-help>

```
C:\Users\RobertDCrane>winget list
```

Name	Id	Version	Source
Git	Git.Git	2.45.2	winget
Microsoft 365 Apps for enterprise - en-us	Microsoft.Office	16.0.17726.20160	winget
Microsoft OneDrive	Microsoft.OneDrive	24.126.0623.0001	winget
Microsoft Monitoring Agent	ARP\Machine\X64\{2821726D-A54C-47AF-97C7-346...	10.20.18067.0	
Microsoft Teams Meeting Add-in for Microsoft...	ARP\Machine\X64\{A7AB73A3-CB10-4AA5-9D38-6AE...	1.24.14501	
Microsoft Update Health Tools	ARP\Machine\X64\{C6FD611E-7EFE-488C-A0E0-974...	5.72.0.0	
Brave	Brave.Brave	126.1.67.134	winget
KeePass Password Safe 2.57	DominikReichl.KeePass	2.57	winget
Microsoft Edge	Microsoft.Edge	126.0.2592.102	winget
Microsoft Edge Update	ARP\Machine\X86\Microsoft Edge Update	1.3.193.5	
Microsoft Edge WebView2 Runtime	Microsoft.EdgeWebView2Runtime	126.0.2592.113	winget
Microsoft Windows Desktop Runtime - 6.0.32 (...)	Microsoft.DotNet.DesktopRuntime.6	6.0.32	winget
Camtasia 2023	ARP\Machine\X86\{362f501d-a96a-4784-9a1b-c39...	23.1.0.46311	
Global Secure Access Client	ARP\Machine\X86\{42a8494d-1231-430f-9e5e-c72...	1.7.669	
PowerShell	Microsoft.PowerShell	7.4.3.0	winget
PowerShell 7.4.2.0-x64	Microsoft.PowerShell	7.4.2.0	winget
Microsoft Visual C++ 2015-2022 Redistributab...	Microsoft.VCRedist.2015+.x64	14.40.33810.0	winget
Microsoft Windows Desktop Runtime - 8.0.7 (x...	Microsoft.DotNet.DesktopRuntime.8	8.0.7	winget
Microsoft Intune Management Extension	ARP\Machine\X86\{D2B35FA1-3BD5-4A16-A2A3-705...	1.80.132.0	
GoToMeeting 10.20.0.19992	GoTo.GoToMeeting	10.20.0.19992	winget
Open Live Writer	OpenLiveWriter.OpenLiveWriter	0.6.2	winget
Microsoft Visual Studio Code (User)	Microsoft.VisualStudioCode	1.91.1	winget
Microsoft Clipchamp	MSIX\Clipchamp.Clipchamp_3.1.10920.0_neutral...	3.1.10920.0	

Patch Applications

Home > Apps | All apps >

Add App

Windows catalog app (Win32)

1 App information

2 Program

3 Requirements

4 D

Microsoft does not assert compliance or authorizations for apps distributed through the Windows catalog app that apps meet their requirements.

Select app *

Search the Enterprise App Catalog

Previous

Next

Search the Enterprise App catalog

Select app

Configuration

Search

App name	Publisher
3CXPhone for Windows	3CX
3DF Zephyr Free	3Dflow srl
4K Video Downloader	OpenMedia
7-Zip	Igor Pavlov
8x8 Work	8x8 Inc.
Able2Extract Professional	Investintech.com Inc.
ActiveState Software Komodo Edit	ActiveState Software Inc.
Adobe AIR	HARMAN International

Next

Patch Operating Systems

Overview Alerts Timeline Security recommendations Software inventory Discovered vulnerabilities Missing KBs

 Customize columns   Export 30 items per page 

Bulletin	OS version	Products	CVEs addressed	KB ↓
June 2020 Security Updates	1809	windows_10 , internet_explorer	90	4561608
May 2020 Security Updates	1809	windows_10 , internet_explorer	83	4551853
April 2020 Security Updates	1809	windows_10 , internet_explorer	67	4549949
March 2020 Security Updates	1809	internet_explorer , windows_10	79	4538461
January 2020 Security Updates	1809	internet_explorer	1	4534273
February 2020 Security Updates	1809	windows_10 , internet_explorer	78	4532691
December 2019 Security Updates	1809	internet_explorer	1	4530715
November 2019 Security Updates	1809	internet_explorer	2	4523205
October 2019 Security Updates	1809	internet_explorer	7	4519338
September 2019 Security Updates	1809	internet_explorer	4	4512578
August 2019 Security Updates	1809	internet_explorer	3	4511553
July 2019 Security Updates	1809	internet_explorer	6	4507469

Patch Operating Systems

Create Update ring for Windows 10 and later

Windows 10 and later

1 Basics 2 Update ring settings 3 Assignments 4 Review + create

Update settings

Microsoft product updates *

Allow Block

Windows drivers *

Allow Block

Quality update deferral period (days) *

0

Feature update deferral period (days) *

0

Upgrade Windows 10 devices to Latest Windows 11 release

Yes No

Set feature update uninstall period (2 - 60 days) *

10

Enable pre-release builds *

Enable Not Configured

Select pre-release channel

Windows Insider - Release Preview

User experience settings

Automatic update behavior

Auto install at maintenance time

Active hours start *

8 AM

Active hours end *

5 PM

Option to pause Windows updates

Enable Disable

Option to check for Windows updates

Enable Disable

Change notification update level

Use the default Windows Update notifications

Use deadline settings

Allow Not configured

Deadline for feature updates

Number of days, 0 to 30

Deadline for quality updates

Number of days, 0 to 30

Grace period

Number of days, 0 to 7

Auto reboot before deadline

Yes No

Patch Operating Systems

[Home](#) > [Devices | Apple updates](#) >

Create profile

...

iOS/iPadOS

✓ Basics

2 Update policy settings

3 Assignments

4 Review + create

Create a profile to force assigned devices to automatically install the latest iOS/iPadOS updates. These settings determine how and when software updates deploy. This profile doesn't prevent users from updating the OS manually, which can be prevented for up to 90 days with a device configuration restriction policy. Updates will only apply to supervised devices.

[Learn More](#)

Select version to install ⓘ

Latest update


Update policy schedule settings:

By default, when an update policy is assigned to a device, Intune deploys the latest updates at device check-in. You can instead create a weekly schedule with customized start and end times. If you choose to update outside of the scheduled time, Intune won't deploy updates until the scheduled time ends.

Schedule type ⓘ

Update at next check-in

Multi Factor Authentication


**Authentication methods | Policies** ...


ciaopslabs - Microsoft Entra ID Security


⌵ ⏪


[+ Add external method \(Preview\)](#) [🔄 Refresh](#) | [🗨️ Got feedback?](#)


✓ Manage

 **Policies**

 Password protection

 Registration campaign

 Authentication strengths

 Settings

> Monitoring

Use this policy to configure the authentication methods your users may register and use. If a user is in scope for a method, 1 methods aren't supported for some scenarios). [Learn more](#)

Manage migration

On September 30th, 2025, the legacy multifactor authentication and self-service password authentication methods here in the authentication methods policy. Use this control to migrate to a unified policy. [Learn more](#)

[Manage migration](#)

Method	Target	Enabled
▼ Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS		No
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Third-party software OATH tokens		No
Voice call		No
Email OTP		Yes
Certificate-based authentication		No

Multi Factor Authentication


Are you trying to sign in?

CIAOPS
admin@ciaops365.com

Enter the number shown to sign in.

App
OfficeHome

Location
NSW, Australia



Apple Maps Legal

No, it's not me

Yes

☐ Persistent browser session ⓘ

A secure sign-in session requires all long-lived tokens (the Microsoft Entra session cookie and refresh token) to be bound to the device using software key binding or hardware security module binding where available.

[Learn more](#)

☐ Require token protection for sign-in sessions (Preview) ⓘ

☐ Use Global Secure Access security profile ⓘ

Restrict Administrative Privileges

Create a profile

Platform

Windows 10 and later

Profile

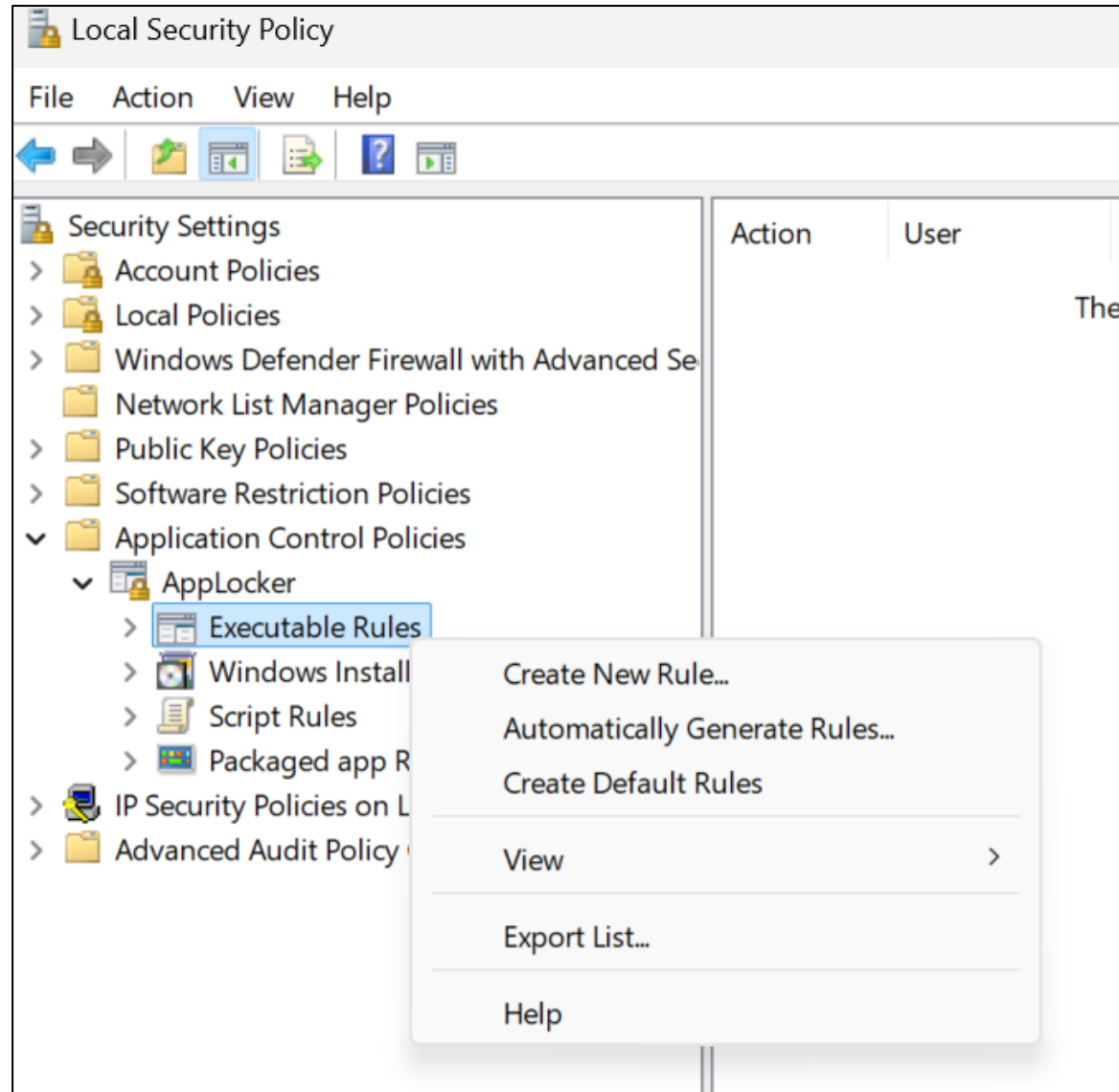
Select a profile

Account Protection

Local admin password solution (Windows LAPS)

Local user group membership

Application Control



Application Control

[Home](#) > [Endpoint security | App Control for Business \(Preview\)](#) >

Create profile ...

App Control for Business

✓ Basics


2 Configuration settings

③ Scope tags

④ Assignments


⑤ Review + create

^ 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  * ⓘ

Enforce

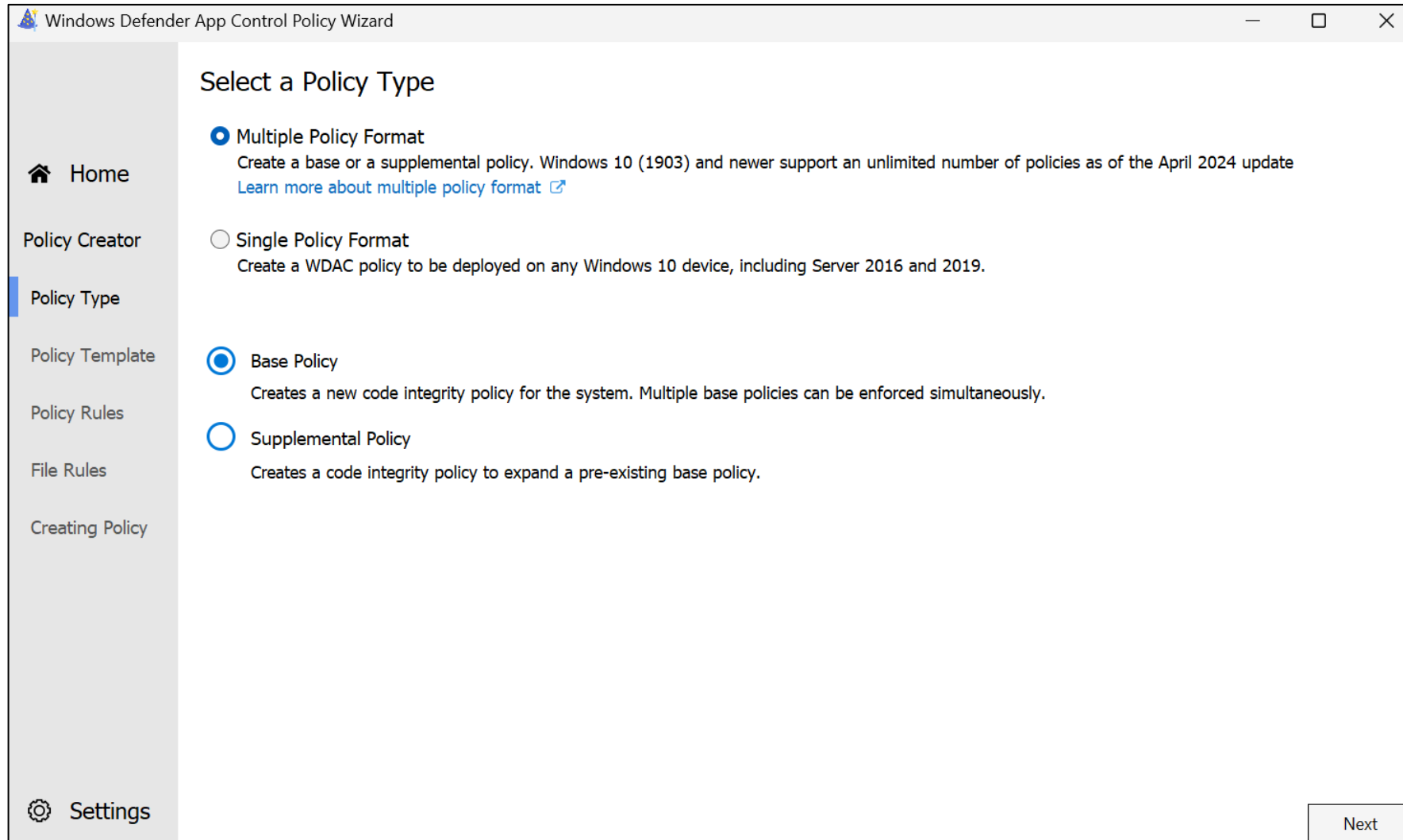
Select additional rules for trusting apps  ⓘ

0 selected

☐ Trust apps with good reputation

☐ Trust apps from managed installers


Application Control



The screenshot shows the 'Windows Defender App Control Policy Wizard' window. The title bar includes the Windows logo, the text 'Windows Defender App Control Policy Wizard', and standard window controls (minimize, maximize, close). The left sidebar contains a vertical list of navigation items: 'Home' (with a house icon), 'Policy Creator', 'Policy Type' (highlighted with a blue bar), 'Policy Template', 'Policy Rules', 'File Rules', 'Creating Policy', and 'Settings' (with a gear icon). The main content area is titled 'Select a Policy Type' and contains four radio button options. The first option, 'Multiple Policy Format', is selected and includes a description and a link. The second option, 'Single Policy Format', is unselected. The third option, 'Base Policy', is selected. The fourth option, 'Supplemental Policy', is unselected. A 'Next' button is located in the bottom right corner of the window.

Windows Defender App Control Policy Wizard

Select a Policy Type

- ☒ Multiple Policy Format
Create a base or a supplemental policy. Windows 10 (1903) and newer support an unlimited number of policies as of the April 2024 update
[Learn more about multiple policy format](#) 
- ☐ Single Policy Format
Create a WDAC policy to be deployed on any Windows 10 device, including Server 2016 and 2019.
- ☒ Base Policy
Creates a new code integrity policy for the system. Multiple base policies can be enforced simultaneously.
- ☐ Supplemental Policy
Creates a code integrity policy to expand a pre-existing base policy.

Home

Policy Creator

Policy Type

Policy Template

Policy Rules

File Rules

Creating Policy

Settings

Next

Application Control

[Home](#) > [Endpoint security | App Control for Business \(Preview\)](#) >

Create profile ...

App Control for Business

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

^ App Control for Business

Configuration settings format  

Enter xml data



App Control for Business policy  

"wdac-p1.xml"




XML value *

```
<?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> 10.3.0.0</VersionEx>
  <PlatformID> {2E07F7E4-194C-4D20-B7C9-6F44A6C5A234}
```



Restrict Office Macro Settings

[Home](#) > [Devices | Configuration](#) >





ACSC Office Hardening Guidelines



Device configuration profile

 Summarize with Copilot  Delete



Word Options > Security > Trust Center

Block macros from running in Office files from the Internet (User)  



Enabled

Disable Trust Bar Notification for unsigned application add-ins and block them (User) (Deprecated)  

Enabled

Require that application add-ins are signed by Trusted Publisher (User)  

Enabled

Turn off trusted documents (User)  

Enabled

Attack Surface Reduction (ASR) Rules



Minimize the attack surface

Attack surface reduction (ASR) rules help to control entry points to your Windows devices using cloud intelligence, such as behavior of Office macros.

Productivity apps rules

- Block Office apps from creating executable content
- Block Office apps from creating child processes
- Block Office apps from injecting code into other processes
- Block Win32 API calls from Office macros
- Block Adobe Reader from creating child processes

Email rule

- Block executable content from email client and webmail
- Block only Office communication applications from creating child processes

Script rules

- Block obfuscated JS/VBS/PS/macro code
- Block JS/VBS from launching downloaded executable content

Polymorphic threats


- Block executable files from running unless they meet a prevalence (1000 machines), age (24hrs), or trusted list criteria
- Block untrusted and unsigned processes that run from USB
- Use advanced protection against ransomware

Lateral movement & credential theft

- Block process creations originating from PSEXEC and WMI commands
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)
- Block persistence through WMI event subscription



User Application Hardening

[Home](#) > [Devices | Configuration](#) >





ACSC Windows Hardening Guidelines

Device configuration profile

 Summarize with Copilot  Delete

Windows Components > Windows Remote Shell



Allow Remote Shell Access

Disabled



Windows Components > Windows Remote Management (WinRM) > WinRM Service

Allow Basic authentication



Disabled

Allow unencrypted traffic

Disabled

Disallow WinRM from storing RunAs credentials

Enabled

Regular Backups

- Difficult to provide prescriptive guidance as the implementation varies considerably based on each organization's unique needs.
- Way you go about that with Microsoft 365 will naturally be different to how you may currently protect your on-premises file shares.
- Organizations should focus on configuring the built-in retention settings to ensure data is protected within the service as necessary to meet business requirements.
- Retention policies and labels provide a means to control how data is retained in Microsoft 365.
- Rather than backing up client devices to preserve setting and applications, modern management approaches ensure client devices are easily replaced with minimal impact to users.
- Microsoft 365 retention ensures data stored within the services is captured and retained in a highly resilient environment.

Backups

OneDrive

Search

Restore your OneDrive

If something went wrong, you can restore your OneDrive to a previous time. Select a date preset or use the slider to find a date with unusual activity in the chart. Then select the changes that you want to undo.

Select a date

Custom date and time

All changes after 6/13/2022, 10:27:43 AM will be rolled back

RestoreCancel

Move the slider to quickly scroll the list to a day.

Days ago

Select a change in the list below to highlight it and all the changes before it. Then select the Restore button to undo all the highlighted changes.

8 days ago - 6/13/2022 (39)

<input checked="" type="checkbox"/>		Updated by [redacted]	10:28:09 AM		[redacted]
<input checked="" type="checkbox"/>		Added by [redacted]	10:28:08 AM		[redacted]
<input checked="" type="checkbox"/>		Renamed by [redacted]	10:27:48 AM		[redacted]
<input checked="" type="checkbox"/>		Updated by [redacted]	10:27:43 AM		[redacted]
<input checked="" type="checkbox"/>		Added by [redacted]	10:27:43 AM		[redacted]
<input checked="" type="checkbox"/>		Updated by [redacted]	6:20:19 AM		[redacted]

ODFB Retention

2. Enter the number of days you want to retain OneDrive files in the **Days to retain files in OneDrive after a user account is marked for deletion** box.

The setting takes effect for the next user that is deleted as well as any users that are in the process of being deleted. The count begins as soon as the user account was deleted in the Microsoft 365 admin center, even though the deletion process takes time. The minimum value is 30 days and the maximum value is 3650 days (ten years).

Logging

```
C:\Windows\System32>auditpol /get /category:*
System audit policy
Category/Subcategory                Setting
System
  Security System Extension          Success and Failure
  System Integrity                   No Auditing
  IPsec Driver                       No Auditing
  Other System Events                 Success and Failure
  Security State Change               No Auditing
Logon/Logoff
  Logon                              Success and Failure
  Logoff                             No Auditing
  Account Lockout                     Success and Failure
  IPsec Main Mode                     No Auditing
  IPsec Quick Mode                    No Auditing
  IPsec Extended Mode                 No Auditing
  Special Logon                       No Auditing
  Other Logon/Logoff Events            No Auditing
  Network Policy Server                No Auditing
  User / Device Claims                 No Auditing
  Group Membership                     No Auditing
Object Access
  File System                         Success and Failure
  Registry                           No Auditing
  Kernel Object                       No Auditing
  SAM                                 No Auditing
  Certification Services               No Auditing
```

Centralized Logging

[Home](#) > [Microsoft Sentinel | Workbooks](#) >

Archiving, Basic Logs, and Retention - ciaopsau

ciaopsau

Edit Open Help Auto refresh: Off

Data Archive Basic Logs Search and Restore **Cost Estimation**

Data is based on the Last 30 days

The below table shows current Workspace Retention and Data Archive Cost Estimates.

These are only estimates and do not reflect current billed costs. You can use these for planning before enabling Data Archive

Update the **Total Retention in Days** for estimate on Data Archiving. The TotalRetention column reflects the current settings.

Total Retention in Days

Estimated Data Retention Costs - Planning for Data Archiving

Search

Integrated with Conditional Access

Grant [X]

☒ Grant access

- ☐ Require multifactor authentication ⓘ
- ☐ Require authentication strength ⓘ
- ☐ Require device to be marked as compliant ⓘ
- ☐ 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 ⓘ

Select

Where to start?

- Perform a risk assessment
- Secure score
- Hardware inventory
- Software inventory
- Enable all auditing
- Implement Sentinel
- Conditional access
- Intune Baselines
- Attack Surface Reduction

The Essential 8 is not your only framework option

- Secure Cloud (AU)
- CIS SCUBA (US)
- NIST (US)

- M365 is more integrated with US frameworks, especially CIS

Resources



<https://bit.ly/ciaopse8>

CIAOPS Resources



- Blog – <http://blog.ciaops.com>
- Free Office 365, Azure video tutorials – <http://www.youtube.com/directorciaops>
- Free documents, presentations, eBooks – <http://slideshare.net/directorcia>
- Office 365, Azure, Cloud podcast – <http://ciaops.podbean.com>
- Office 365, Azure online training courses – <http://www.ciaopsacademy.com>
- Office 365 and Azure community – <http://www.ciaopspatron.com>
- CIAOPS Github – <https://github.com/directorcia>
- CIAOPS Best Practices Github – <https://github.com/directorcia/bp>

[Twitter/X](#)
[@directorcia](#)

[Facebook](#)
<https://www.facebook.com/ciaops>

[Email](#)
director@ciaops.com

[Teams](#)
[director@ciaops.com](https://teams.microsoft.com/join/director@ciaops.com)