

#CIAOPS

Don't overlook these things  
when configuring Microsoft 365

October 2024

@directorcia

<http://about.me/ciaops>

Code

Primary SMTP address = director@ciaopslabs.com.au

Created = 27/05/2021 5:22:31 PM

Audit enabled = True

Audit log limit (days) = 180

Retain Deleted items for (days) = 14

Litigation hold = False

Archive status = None

Max send size = 35 MB (36,700,160 bytes)

Max receive size = 36 MB (37,748,736 bytes)

POP3 enabled = True

IMAP enabled = False

Mailbox = Super User [ superuser@ciaopslabs.onmicrosoft.com ]

Primary SMTP address = superuser@ciaopslabs.onmicrosoft.com

Created = 22/05/2021 12:05:54 PM

Audit enabled = True

Audit log limit (days) = 180

Retain Deleted items for (days) = 14

Litigation hold = False

Archive status = None

Max send size = 35 MB (36,700,160 bytes)

Max receive size = 36 MB (37,748,736 bytes)

POP3 enabled = True

IMAP enabled = True

No CSV created

Finish checking mailboxes

Script completed

```
Get-Mailbox -ResultSize unlimited -Filter "RecipientTypeDetails -eq 'UserMailbox'" `
| Set-Mailbox -RetainDeletedItemsFor 30
```

| + New flow                  | Import | Search |  |                    |                    |           |
|-----------------------------|--------|--------|--|--------------------|--------------------|-----------|
| (2100) Articles             |        |        |  |                    | Activity suspended | Scheduled |
| NASA Image                  |        |        |  | 1 yr ago           |                    | Scheduled |
| Outbound Spam BP - 10am     |        |        |  | 1 yr ago           |                    | Instant   |
| Joke of the day - Immediate |        |        |  | 1 yr ago           |                    | Instant   |
| New Patron added            |        |        |  | 1 yr ago           |                    | Automated |
| Teams contributions         |        |        |  | 2 yr ago           |                    | Instant   |
| Device Capture              |        |        |  | 2 yr ago           |                    | Instant   |
| Device Offboard             |        |        |  | 2 yr ago           |                    | Instant   |
| Dilbert - 10am              |        |        |  | Activity suspended |                    | Scheduled |
| Vulnerabilities             |        |        |  | 2 yr ago           |                    | Instant   |
| Secure Score                |        |        |  | 2 yr ago           |                    | Instant   |

- Home
- Create
- Learn
- Apps

- Tables
- Flows
- Solutions
- More

- Power Platform

Let's build an app. What should it do?

Collect RSVPs

Track sales leads

List inventory

Manage inspections

Use everyday words to describe what your app should collect, track, list, or manage ...

This feature uses generative AI. [See terms](#)

Other ways to create an app

Start with data

Create new tables, select existing tables, or connect to external data sources.

Start with a page design

Select from a list of different designs and layouts to get your app going.

Start with an app template

Select from a list of fully-functional business app templates. Use as-is or customize to suit your needs.

Your apps











|                                 | Name                   |  | Modified    | Owner        | Type         |
|---------------------------------|------------------------|--|-------------|--------------|--------------|
|                                 | Power Pages Management |  | 1 year ago  | SYSTEM       | Model-driven |
|                                 | Azure Registrations    |  | 2 years ago | Robert Crane | Canvas       |
|                                 | Event Signup           |  | 3 years ago | Robert Crane | Canvas       |
|                                 | Standard               |  | 3 years ago | Robert Crane | Canvas       |
|                                 | Solution Health Hub    |  | 4 years ago | SYSTEM       | Model-driven |
| <a href="#">See more apps</a> → |                        |  |             |              |              |

Self Service

## Self-service trials and purchases

View and manage which products users can try or buy on their own. Self-service gives users the flexibility to try or buy the products they need to be more productive, and helps admins understand and manage demand.

[Learn more about self-service purchases](#)

| Product ↑  | Self-service settings                  |
|--|--|
|  Dynamics 365 Marketing                                 | <input type="radio"/> Do not allow     |
|  Dynamics 365 Marketing Additional Application          | <input type="radio"/> Do not allow     |
|  Dynamics 365 Marketing Additional Non-Prod Application | <input type="radio"/> Do not allow     |
|  Dynamics 365 Marketing Attach                          | <input type="radio"/> Do not allow     |
|  Microsoft 365 Copilot                                  | <input checked="" type="radio"/> Allow |
|  Microsoft 365 F3                                     | <input type="radio"/> Do not allow     |
|  Microsoft ClipChamp                                  | <input type="radio"/> Do not allow     |
|  Microsoft Purview Discovery                          | <input type="radio"/> Do not allow     |
|  Power Apps per user                                  | <input type="radio"/> Do not allow     |
|  Power Automate per user plan                         | <input type="radio"/> Do not allow     |
|  Power Automate Per User with Attended RPA Plan       | <input type="radio"/> Do not allow     |



# Logs

## Mailbox actions logged by mailbox audit logging

When you enable mailbox audit logging for a mailbox, access to the mailbox and certain administrator and delegate actions are logged by default. To log actions taken by the mailbox owner, you must specify which owner actions should be audited.

| Action             | Description   | Admin            | Delegate         | Owner            |
|--------------------|---|------------------|------------------|------------------|
| Copy               | An item is copied to another folder.  | Yes              | No               | No               |
| Create             | An item is created in the Calendar, Contacts, Notes, or Tasks folder in the mailbox; for example, a new meeting request is created. Note that message or folder creation isn't audited. | Yes <sup>1</sup> | Yes <sup>1</sup> | Yes              |
| FolderBind         | A mailbox folder is accessed.   | Yes <sup>1</sup> | Yes <sup>2</sup> | No               |
| HardDelete         | An item is deleted permanently from the Recoverable Items folder.   | Yes <sup>1</sup> | Yes <sup>1</sup> | Yes              |
| MailboxLogin       | The user signed in to their mailbox.  | No               | No               | Yes <sup>3</sup> |
| MessageBind        | An item is accessed in the reading pane or opened.  | Yes              | No               | No               |
| Move               | An item is moved to another folder.   | Yes <sup>1</sup> | Yes              | Yes              |
| MoveToDeletedItems | An item is moved to the Deleted Items folder.   | Yes <sup>1</sup> | Yes              | Yes              |
| SendAs             | A message is sent using Send As permissions.  | Yes <sup>1</sup> | Yes <sup>1</sup> | No               |
| SendOnBehalf       | A message is sent using Send on Behalf permissions.   | Yes <sup>1</sup> | Yes              | No               |
| SoftDelete         | An item is deleted from the Deleted Items folder.   | Yes <sup>1</sup> | Yes <sup>1</sup> | Yes              |
| Update             | An item's properties are updated.   | Yes <sup>1</sup> | Yes <sup>1</sup> | Yes              |

Home > ciaopslabs

➡️

ciaopslabs

Sign-ins

📌 ...

Azure Active Directory

- «
- 📄 Download ▾

⚙️ Export Data Settings

✖️ Troubleshoot

🔄 Refresh

|

☰ Columns

|

🗨️ Got feedback?
- 📘 Overview

🚧 Preview features

✖️ Diagnose and solve problems
- Manage

👤 Users

👥 Groups

🏢 External Identities

👤 Roles and administrators

🏢 Administrative units

🏢 Enterprise applications

📄 Devices

🏢 App registrations

📘 Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 24 hours**

Show dates as : **Local**

+🔍 Add filters

**User sign-ins (interactive)**

User sign-ins (non-interactive)

Service principal sign-ins

Managed identity sign-ins

| Date                 | ↕ | Request ID            | ↕ | User                 | ↕ | Application            | ↕ | Status      | IP address    | ↕ | Location              |
|----------------------|---|-----------------------|---|----------------------|---|------------------------|---|-------------|---------------|---|-----------------------|
| 8/2/2021, 1:42:19 PM |   | 89d68567-99e9-4fb...  |   | 09dabc45-a14b-47a... |   | Azure Portal           |   | Interrupted | 203.129.21.57 |   |                       |
| 8/2/2021, 1:39:58 PM |   | 37a89011-e1c3-477...  |   | Robert Crane         |   | Microsoft App Acces... |   | Success     | 203.129.21.57 |   | Coogee, New South     |
| 8/2/2021, 1:39:50 PM |   | ca294ba3-5859-49d...  |   | Robert Crane         |   | My Profile             |   | Success     | 203.129.21.57 |   | Morwell, Victoria, Al |
| 8/2/2021, 1:39:39 PM |   | a231f36d-f776-4c7e... |   | Robert Crane         |   | Azure Portal           |   | Success     | 203.129.21.57 |   | Morwell, Victoria, Al |
| 8/2/2021, 1:39:37 PM |   | bfc6db96-ab38-47bf... |   | Robert Crane         |   | Azure Portal           |   | Interrupted | 203.129.21.57 |   | Coogee, New South     |

◀

▶

How long does Azure AD store the data?

Activity reports

| Report             | Azure AD Free | Azure AD Premium P1 | Azure AD Premium P2 |
|--------------------|---------------|---------------------|---------------------|
| Audit logs         | 7 days        | 30 days             | 30 days             |
| Sign-ins           | 7 days        | 30 days             | 30 days             |
| Azure AD MFA usage | 30 days       | 30 days             | 30 days             |

Security signals

| Report         | Microsoft Entra ID Free | Microsoft Entra ID P1 | Microsoft Entra ID P2 |
|----------------|-------------------------|-----------------------|-----------------------|
| Risky users    | No limit                | No limit              | No limit              |
| Risky sign-ins | 7 days                  | 30 days               | 90 days               |



# Users | User settings ...

CIAOPS



Refresh



Got feedback?



All users



Audit logs



Sign-in logs



Diagnose and solve problems



Deleted users



Password reset



User settings

## Default user role permissions

[Learn more](#)

Users can register applications ☐ No

Restrict non-admin users from creating tenants ☒ Yes

Users can create security groups ☐ No

-



# Authentication methods | Password protection

Contoso - Microsoft Entra ID Security

Search << Save Discard | Got feedback?

## Manage

Policies

Password protection

Registration campaign

Authentication strengths

Settings

## Monitoring

Activity

User registration details

Registration and reset events

Bulk operation results

### Custom smart logout

Lockout threshold ⓘ

10



Lockout duration in seconds ⓘ

60



### Custom banned passwords

Enforce custom list ⓘ

Yes

No

Custom banned password list ⓘ

contoso  
fabrikam  
tailwind  
michigan  
wolverine  
harbaugh  
howard

### Password protection for Windows Server Active Directory

Enable password protection on Windows  
Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit



[Home](#) > [Security | Authentication methods](#) > [Authentication methods | Policies](#) >

## Passkey (FIDO2) settings ...

Passkeys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. [Learn more](#).  
Passkeys are not usable in the Self-Service Password Reset flow.

Enable and Target Configure

### GENERAL

Allow self-service set up

Yes

No

Enforce attestation

Yes

No

### KEY RESTRICTION POLICY

Enforce key restrictions

Yes

No

Restrict specific keys

Allow

Block



Microsoft Authenticator (Preview) ⓘ

# Alerts



# Protection Alerts

Home > Alert policies

## Alert policies

Use alert policies to track user and admin activities, malware threats, or data loss incidents in your organization. After choosing the activity you want to be alerted on, refine the policy by adding conditions, deciding when to trigger the alert, and who should receive notifications. [Learn more about alert policies](#)

Looking for activity alert policies that are not showing up here? Manage them in [Activity alerts](#)

+ New alert policy

Search

Filter

| <input type="checkbox"/> | Name ^                                    | Severit... | Type   | Category ...   | Date modified    | Status                              |
|--------------------------|---|------------|--------|----------------|------------------|-------------------------------------|
| <input type="checkbox"/> | A potentially malicious URL click was ... | High       | System | Threat mana... | -                | ...                                 |
| <input type="checkbox"/> | Added exempt user agent                   | Medium     | Custom | Others         | 8/12/18 10:59 am | <input checked="" type="checkbox"/> |



Detected malware in files



High

Custom

Threat mana...

8/12/18 10:59 am



Suspicious email sending patterns de...



Medium

System

Threat mana...

-

|                          |   |                |        |                 |                  |                                     |
|--------------------------|---|----------------|--------|-----------------|------------------|-------------------------------------|
| <input type="checkbox"/> | Creation of forwarding/redirect rule    | Low            | System | Threat mana...  | -                | ...                                 |
| <input type="checkbox"/> | Detected malware in files               | High           | Custom | Threat mana...  | 8/12/18 10:59 am | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> | DLP policy match                        | Medium         | Custom | Information ... | 8/12/18 10:59 am | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> | eDiscovery search started or exported   | Medium         | System | Threat mana...  | -                | ...                                 |
| <input type="checkbox"/> | Elevation of Exchange admin privilege   | Low            | System | Permissions     | -                | ...                                 |
| <input type="checkbox"/> | Email messages containing malware ...   | Information... | System | Threat mana...  | -                | ...                                 |
| <input type="checkbox"/> | Email messages containing phish UR...   | Information... | System | Threat mana...  | -                | ...                                 |
| <input type="checkbox"/> | Email reported by user as malware or... | Information... | System | Threat mana...  | -                | ...                                 |
| <input type="checkbox"/> | Email sending limit exceeded            | Medium         | System | Threat mana...  | -                | ...                                 |

# Activity Alerts

[Home](#) > [Manage alerts](#)

## Activity alerts

! We are working on a better experience for you to manage and view security and compliance alerts. Go to [Alert policies](#)

[+ New alert policy](#)

| Name                          | Recipients          | Status | Date modified       |
|-------------------------------|---------------------|--------|---------------------|
| Role Alert                    | admin@ciaops365.com | On     | 2018-07-03 13:01:37 |
| Administrator Password change | director@ciaops.com | On     | 2017-10-03 18:17:45 |
| Company Information Alert     | admin@ciaops365.com | On     | 2018-07-03 13:01:37 |
| File and Page Alert           | admin@ciaops365.com | On     | 2018-07-03 13:01:29 |
| Site Alert                    | admin@ciaops365.com | On     | 2018-07-03 13:01:32 |
| Domain Alert                  | admin@ciaops365.com | On     | 2018-07-03 13:01:38 |
| Sharing Alert                 | admin@ciaops365.com | On     | 2018-07-03 13:01:30 |
| Access Alert                  | admin@ciaops365.com | On     | 2018-07-03 13:01:32 |
| OneDrive sharing              | admin@ciaops365.com | On     | 2017-05-07 10:51:06 |
| Anonymous Links Alert         | admin@ciaops365.com | On     | 2018-07-03 13:01:30 |
| Office Alert                  | admin@ciaops365.com | On     | 2018-07-03 13:01:33 |
| Password Alert                | admin@ciaops365.com | On     | 2018-07-03 13:01:36 |
| Mailbox Alert                 | admin@ciaops365.com | On     | 2018-07-03 13:01:34 |

<https://security.microsoft.com/managealerts>

Exchange

# Configuration analyzer

The Configuration analyzer can help identify issues in your current configuration and help improve your policies for better security. Want to automatically stay updated with recommendation configuration? Switch on [presets](#). [Learn more](#).

**Standard recommendations**   Strict recommendations   Configuration drift analysis and history

Anti-spam  
**4**

Anti-phishing  
**12**

DKIM  
**1**

Outlook  
**1**

Apply recommendation   View policy   Export   Refresh

1 of 18 selected   Search   Filter

| <input type="checkbox"/> Recommendations               | Policy                      | Policy group/setting name               | Policy type   | Current configuration     | Last modified        | Status      |
|--|-----------------------------|---|---------------|---------------------------|----------------------|-------------|
| <input checked="" type="checkbox"/> Quarantine message | Default                     | High confidence spam detection action   | Anti-spam     | Move to Junk Email folder | Sep 23, 2024 4:18 PM | Not started |
| <input type="checkbox"/> Quarantine message            | Default                     | Phishing email detection action         | Anti-spam     | Move to Junk Email folder | Sep 23, 2024 4:18 PM | Not started |
| <input type="checkbox"/> Change 7 to 6                 | Default                     | Bulk email threshold                    | Anti-spam     | 7                         | Sep 23, 2024 4:18 PM | Not started |
| <input type="checkbox"/> Change 15 to 30               | Default                     | Quarantine retention period             | Anti-spam     | 15                        | Sep 23, 2024 4:18 PM | Not started |
| <input type="checkbox"/> Change false to true          | Office365 AntiPhish Default | Add users to protect                    | Anti-phishing | false                     | Sep 23, 2024 4:18 PM | Not started |
| <input type="checkbox"/> Change false to true          | Office365 AntiPhish Default | Automatically include the domains I own | Anti-phishing | false                     | Sep 23, 2024 4:18 PM | Not started |
| <input type="checkbox"/> Change false to true          | Office365 AntiPhish Default | Include custom domains                  | Anti-phishing | false                     | Sep 23, 2024 4:18 PM | Not started |

# Office ATP Recommended Configuration Analyzer Report

Version 1.0

This report details any tenant configuration changes recommended within your tenant.

Recommendations

7

OK

21

## Summary

### Areas

[Content Filter Policies](#)

1 0

[DKIM](#)

1 1

[Transport Rules](#)

0 1

[Zero Hour Autopurge](#)

0 1

[Tenant Settings](#)

0 1

[Malware Filter Policy](#)

0 2

[Advanced Threat Protection Policies](#)

1 1

## Content Filter Policies

### Bulk Complaint Level



Bulk Complaint Level threshold is set to 6 or lower

OK

The differentiation between bulk and spam can sometimes be subjective. The bulk complaint level is based on the number of complaints from the sender. Decreasing the threshold can decrease the amount of perceived spam received.

Effected objects

**Content Filter Policy**

**Bulk Complaint Level Threshold**

Default

6

OK

[Bulk Complaint Level values](#)

### Mark Bulk as Spam



Bulk is marked as spam

OK

The differentiation between bulk and spam can sometimes be subjective. The bulk complaint level is based on the number of complaints from the sender. Marking bulk as spam can decrease the amount of perceived spam received.

Effected objects

# Clients

```
C:\Windows\System32>auditpol /get /category:*
```

```
System audit policy
```

```
Category/Subcategory
```

```
Setting
```

```
System
```

```
Security System Extension
```

```
Success and Failure
```

```
System Integrity
```

```
Success and Failure
```

```
IPsec Driver
```

```
No Auditing
```

```
Other System Events
```

```
Success and Failure
```

```
Security State Change
```

```
Success
```

```
Logon/Logoff
```

```
Logon
```

```
Success and Failure
```

```
Logoff
```

```
Success
```

```
Account Lockout
```

```
Success and Failure
```

```
IPsec Main Mode
```

```
No Auditing
```

```
IPsec Quick Mode
```

```
No Auditing
```

```
IPsec Extended Mode
```

```
No Auditing
```

```
Special Logon
```

```
Success
```

```
Other Logon/Logoff Events
```

```
No Auditing
```

```
Network Policy Server
```

```
Success and Failure
```

```
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
```

```
Application Generated
```

```
No Auditing
```

```
Handle Manipulation
```

```
No Auditing
```

```
File Share
```

```
No Auditing
```

```
Filtering Platform Packet Drop
```

```
No Auditing
```

```
Filtering Platform Connection
```

```
No Auditing
```

```
Other Object Access Events
```

```
Success and Failure
```

## Attack Surface Reduction Rules

16 of 16 ASR rules found active

Block executable content from email client and webmail = Enabled

Block all Office applications from creating child processes = Enabled

Block Office applications from creating executable content = Enabled

Block Office applications from injecting code into other processes = Enabled

Block JavaScript or VBScript from launching downloaded executable content = Enabled

Block execution of potentially obfuscated scripts = Enabled

Block Win32 API calls from Office macros = Enabled

Block executable files from running unless they meet a prevalence, age, or trusted list criterion = Enabled

Use advanced protection against ransomware = Enabled

Block credential stealing from the Windows local security authority subsystem (lsass.exe) = Enabled

Block process creations originating from PSExec and WMI commands = Enabled

Block untrusted and unsigned processes that run from USB = Enabled

Block Office communication application from creating child processes = Enabled

Block Adobe Reader from creating child processes = Enabled

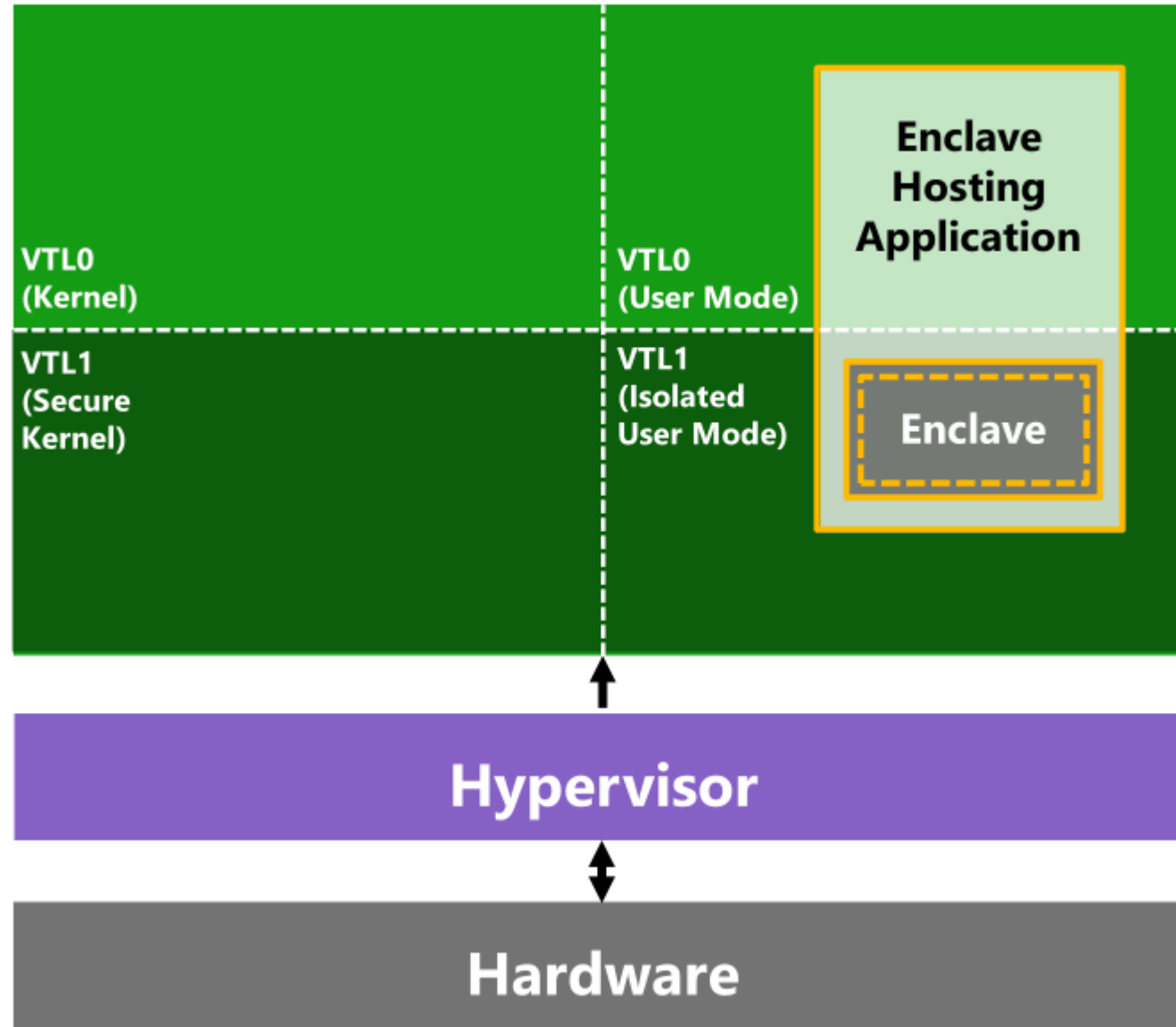
Block persistence through WMI event subscription = Enabled

Block abuse of exploited vulnerable signed drivers = Enabled

Script completed



# OS (Host or Guest)



Virtualisation-based security

Virtualisation-based security required security properties

Virtualisation-based security available security properties

Virtualisation-based security services configured

Virtualisation-based security services running

Running

Base Virtualisation Support, Secure Boot, DMA Protection

Base Virtualisation Support, Secure Boot, DMA Protection, UEFI Code Readonly, SMM Security Mitigations 1.0, Mode Based Execution Control

Credential Guard, Hypervisor enforced Code Integrity, Secure Launch

Credential Guard, Hypervisor enforced Code Integrity



New tab

Ctrl+T



New window

Ctrl+N



New InPrivate window

Ctrl+Shift+N



New Application Guard window

Ctrl+Shift+Q

# Exposure Insights

Collapse Navigation

# Initiatives

Key initiatives

External Attack Surface Protection

No data available

Ransomware Protection

No data available

Endpoint Security

No data available

Business Email Compromise - Financial fraud

47%

No change (last 14 days)

Domain initiatives

Threat initiatives

11 items

Search

Filter

Suggest new initiative

| 14 day change trend | Initiative name   | Current score | Workloads  | 14 day change drift | Last updated           |
|---------------------|---|---------------|--|---------------------|------------------------|
| <div></div>         | <div><div>Business Email Compromise - Financial fraud</div><div>Business email compromise (BEC) financial fraud is a social engineering attack that aims to steal money or sensitive information. The attacker tricks the target into believing they are interacting with a trusted entity to conduct either personal or professional business. After deceiving the target, the attacker persuades them to share valuable information or process a payment.</div></div>   | 47%           | Defender for Office, Defender for Identity, Microsoft Entra ID | No change           | Oct 6, 2024 5:58:03 pm |
| <div></div>         | <div><div>CIS M365 Foundations Benchmark</div><div>The CIS Microsoft 365 Foundations Benchmark (v3.0.0) is a set of security assessments developed by the Center for Internet Security (CIS). It provides prescriptive guidance for establishing a secure baseline configuration for Microsoft 365. The benchmark includes configuration baselines and best practices for securely configuring a system. The benchmark is internationally recognized as a security standard for defending IT systems and data against cyber attacks. This initiative contains a subset of security...</div></div> | 49%           | -  | -5%                 | Oct 7, 2024 4:03:51 pm |

Secure  
Score

# Microsoft Secure Score

There are new permissions options available for Secure Score. You can now configure users' Secure Score data visibility based on data source. [Learn more about this change.](#)

Overview Recommended actions History Metrics & trends

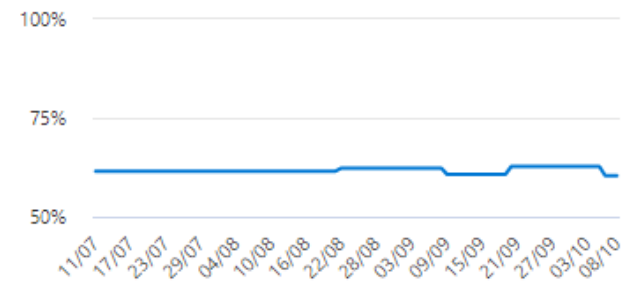
Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Your secure score Include

Secure Score: 60.4%

230.73/382 points achieved

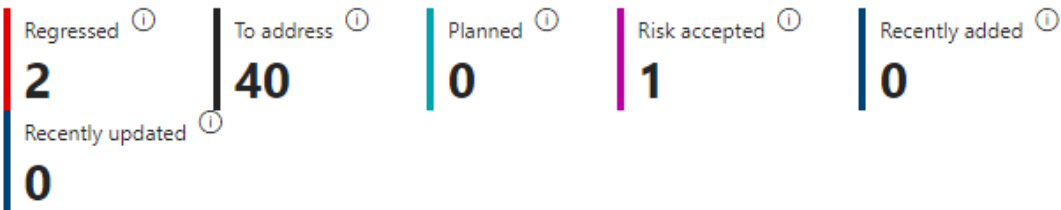


Breakdown points by: Category

Identity 12.67%

Data 88.89%

Actions to review



Top recommended actions

| Recommended action  | Score impact | Status        | Category |
|---|--------------|---------------|----------|
| Ensure multifactor authentication is enabled for all users        | +2.36%       | Risk accepted | Identity |
| Enable impersonated domain protection                             | +2.09%       | To address    | Apps     |
| Enable Conditional Access policies to block legacy authentica...  | +2.09%       | To address    | Identity |
| Ensure the 'Password expiration policy' is set to 'Set passwor... | +2.09%       | To address    | Identity |

Azure

# All services

- All
- Favorites
- Recents
- Recommended for you
- Categories
- AI + machine learning
- Analytics
- Compute
- Containers
- Databases
- DevOps
- General
- Hybrid + multicloud
- Identity
- Integration
- Internet of Things
- Management and governance
- Migration
- Mixed reality
- Monitor
- Networking
- Security
- Storage
- Web & Mobile

Filter services

Service providers : All

Release Status : All



Microsoft  
Entra ID



Virtual  
machines



Resource  
groups



App Services



Storage  
accounts



SQL  
databases



Cost  
Management



Virtual  
networks

## AI + machine learning (22)



Azure AI Studio



Azure AI services



Anomaly detectors



Content moderators



Face APIs



Metrics advisors



Speech services



Azure Synapse Analytics



Azure Machine Learning



Azure AI services multi-service account



Bot Services



Custom vision



Immersive readers



Azure OpenAI



Translators



AI Search



Azure AI Video Indexer



Computer vision



Document intelligences



Language



Personalizers



Intelligent Recommendations Accounts

## Analytics (22)



Analysis Services



Data Lake Analytics



HDInsight clusters



Microsoft Graph Data Connect PREVIEW



Data Shares



Apache Airflow™ on Astro - An Azure Native ISV ... PARTNER



Data Lake Storage Gen1



Azure HDInsight on AKS clusters (preview) PREVIEW



Azure Data Explorer Clusters



Power BI Embedded



Data factories



Azure Databricks



Informatica Intelligent Data Management Cloud ... PARTNER



Data Share Invitations



Apache Kafka® & Apache Flink® on Confluent ... PARTNER



Sentinel

Search

Refresh Guides & Feedback

- News & guides
- Search
- Threat management
  - Incidents
  - Workbooks
  - Hunting
  - Notebooks
  - Entity behavior
  - Threat intelligence
  - MITRE ATT&CK (Preview)
  - SOC optimization
- Content management
  - Content hub
  - Repositories (Preview)
  - Community
- Configuration
  - Workspace manager (Preview)
  - Data connectors**
  - Analytics
  - Summary rules (Preview)
  - Watchlist
  - Automation
  - Settings

22 Connectors 16 Connected

More content at Content hub

Search by name or provider

Providers : Microsoft Data Types : All Status : Connected (16)

|  |   |     |
|--|---|-----|
|  | Microsoft Defender for Office 365 (Preview)<br>Microsoft                | ... |
|  | Microsoft Defender Threat Intelligence (Preview)<br>Microsoft           | ... |
|  | Microsoft Defender XDR<br>Microsoft                                     | ... |
|  | Microsoft Entra ID<br>Microsoft   | ... |
|  | Microsoft Entra ID Protection<br>Microsoft                              | ... |
|  | Microsoft Purview Information Protection (Preview)<br>Microsoft         | ... |
|  | Security Events via Legacy Agent<br>Microsoft                           | ... |
|  | Tenant-based Microsoft Defender for Cloud (Preview)<br>Microsoft        | ... |
|  | Threat Intelligence Platforms - BEING DEPRECATED (Preview)<br>Microsoft | ... |
|  | Windows DNS via Legacy Agent (Preview)<br>Microsoft                     | ... |

Microsoft Entra ID

Connected Status

Microsoft Provider

3 Days Ago  
Last Log Received

Related content

0 Workbooks

2 Queries

103 Analytics rules templates

Data received

Go to log analytics

1/8

SigninLogs

160

MicrosoftGraph...

68K

Data types


- SigninLogs 05/10/2024, 5:12:50 am
- AuditLogs 05/10/2024, 1:59:44 am
- AADNonInteractiveUserSignInLogs 05/10/2024, 5:21:54 am

Open connector page

Defender  
EASM

Assets


08/10/2024, 2:05:24 pm AEDT



Domains

6


Last 30 days: 0



Hosts

19


Last 30 days: ▲ 1



Pages

38


Last 30 days: ▲ 3



SSL certificates

33


Last 30 days: ▲ 6



ASNs

0


Last 30 days: 0



IP blocks

0


Last 30 days: 0



IP addresses

0

Last 30 days: 0




Contacts

1

Last 30 days: 0

Attack surface insights

07/10/2024, 2:51:35 pm AEDT



0

High priority observations

Found from 0 of 149 insights

Top observations

CVE-2019-11073 Paessler PRTG Network Monitor Unauthenticated Remot... 0


CVE-2024-23917 - TeamCity Critical Auth Bypass 0

Entrolink PPX-AnyLink Remote Code Execution 0

CVE-2022-22972 - VMware vRealize Automation Authentication Bypass V... 0

CVE-2023-45849 - Perforce Helix Core Unauthenticated Remote Code Exe... 0

All 149 insights



0

Medium priority observations

Found from 0 of 185 insights

Top observations

[Potential] CVE-2023-41998 - Arcserve UDP Multiple Vulnerabilities 0


[Potential] Directorist WordPress Plugin CSRF 0

[Potential] US-CERT Issues Alert On Critical Vulnerabilities Exploited By Ru... 0

[Potential] CVE-2020-7067 PHP Out-of-Bounds Read Flaw 0

Approved Insecure Login Forms 0

All 185 insights



11

Low priority observations

Found from 3 of 21 insights

Top observations

Expired SSL Certificates 8

Deprecated Tech - JQuery 2

Self Signed Certificates 1

Deprecated Tech - PHP 0

Deprecated Tech - Nginx 0

All 21 insights

# Security Copilot



## Vulnerability impact assessment

Summarize Write me an executive summary report for the vulnerability, threat actor insights, and recommendations for someone who is less technical. in a short narrative. Indicate if this vulnerability is a remote code execution and if it impacts devices on the Internet. Finally, include a bullet point list of impacted technology for easy reference.

✓ 3 steps completed 55 seconds

> ✓ Chose Microsoft Defender Threat Intelligence 42 seconds

> ✓ Looked up threat intelligence information 5 seconds

> ✓ Prepared your response 7 seconds

Apr 1, 9:39 AM | 1 minute

Based on the available data, it appears that there is no specific threat intelligence information related to the vulnerability, threat actor insights, recommendations, remote code execution, or impacts on devices on the Internet. This could be due to a variety of reasons, such as the information not being available in the current threat intelligence sources, or the search terms not matching any known threat analytics.

However, it's important to note that the absence of information does not necessarily mean that there is no threat. It's always recommended to keep systems and software up-to-date, use strong, unique passwords, and follow best security practices to minimize the risk of exploitation.

Unfortunately, without specific threat intelligence data, it's not possible to provide a bullet point list of impacted technology at this time.

😊 How's this response?



## How Copilot can help

Copilot can make mistakes, so remember to verify the results.



### Explore device

Get answers about this device's properties and the policies and apps assigned to it.



### Compare to another device

Select another device and understand the differences in hardware and device configurations



### Analyze error code

See an error code that you don't understand? Get answers and learn how you can remediate.

**BEC financial fraud attack was launched from a compromised account (attack disruption)**

[Copilot](#) [Manage incident](#) [Activity log](#) [...](#)

High Active AlpineSkiHouse - AlpineSkiHouse BIC Fraud Credential Theft Defender Experts Attack Disruption BIC Email Threats Alerts

<sup>1</sup> Important! A potentially compromised account was disabled automatically by attack detection in Microsoft 365 Defender. For more details, select the Assets + Users tab or go to the [action center](#).

[Attack story](#) [Alerts \(20\)](#) [Assets \(4\)](#) [Investigations \(2\)](#) [Evidence and Response \(25\)](#) [Recommended actions \(21\)](#) [Summary](#) [Similar incidents \(0\)](#)

The screenshot displays the Microsoft Defender Security Center interface. On the left, a list of alerts is shown, including 'Activity from a Tor IP address', 'Suspicious inbox manipulation rule', and 'A potentially malicious URL click was detected'. The main area features an 'Incident graph' with a central node representing a user account, connected to nodes for '2 Cloud Applications', '3 IPs', and 'Update'. The right sidebar provides 'Incident details' for a specific incident, including 'Assigned to', 'Classification', 'First activity', 'Last activity', and 'Impacted assets'. A 'Copilot' panel on the far right offers an 'Incident summary' and a list of related threats.



# Syntax

# Syntex

Explore, set up, and manage the Syntex services that enhance content processes in Microsoft 365.

[Learn more about Syntex](#)



## Manage pay-as-you-go billing

An Azure subscription is linked to Microsoft Syntex.

### Syntex services for

Documents & images

Videos

Storage

Apps

## Document & image services

| Service ↑  | Description   |
|--|---|
| Autofill columns                                 | Let users add prompts to columns to extract or generate information from file contents.                                     |
| Content assembly                                 | Let users create modern templates with data sources and generate repetitive structured documents.                           |
| Document translation                             | Let users create translated copies of documents.  |
| eSignature <small>SUPPORTED REGIONS ONLY</small> | Let users set up PDFs for internal and external stakeholders to sign.   |
| Image tagging                                    | Let users categorize and label images with descriptive keywords.  |
| Optical character recognition                    | Let users use enhanced search that can recognize text in images.  |
| Prebuilt document processing                     | Let users configure pretrained models to extract info from common documents like contracts, invoices, and receipts.         |
| Structured and freeform document processin...    | Let users train custom models to extract info from structured documents like forms and freeform documents like letters a... |
| Taxonomy tagging                                 | Let users automate file tagging using your organization's terms.  |
| Unstructured document processing                 | Let users train custom models to classify and extract info from the widest range of file types.                             |

AI



Chat



Teams



Calendar



Calls



OneDrive



Planner



Viva Insights



Viva Conne...



Viva Learning



Viva Engage



Microsoft C...



Meet



Copilot

▼ Pinned



Robert Crane (You)

▼ Recent

I have a customer who have a SharePoint library where all permissions on the root level and most things inherited Typically all staff will get access to everything but they have one contractor they'd only like to allow access to certain reports/files they're working on. It would mean we'd have to break inheritance throughout the document library, while we'd still maintain the existing permissions I am not a fan of the idea of breaking inheritance on all these random folders within the library.

It sounds like you're dealing with a common challenge in SharePoint permissions management. Breaking inheritance can indeed be cumbersome and lead to potential issues down the line. Here are a few alternative approaches you might consider:

1. **Create a Separate Library or Folder:** Instead of breaking inheritance on multiple folders, you could create a separate document library or a specific folder within the existing library for the contractor. This way, you can set unique permissions on this new library or folder without affecting the rest of the structure.
2. **Use SharePoint Groups:** Create a SharePoint group specifically for the contractor and assign permissions to this group. You can then add the contractor to this group and grant access only to the necessary files or folders.
3. **Share Individual Files:** If the number of files the contractor needs access to is relatively small, you could share individual files directly with the contractor. This approach avoids breaking inheritance and keeps the overall permissions structure intact.
4. **Metadata-Based Security:** If your SharePoint environment supports it, you could use metadata to control access. By tagging documents with specific metadata, you can create views or filters that only show documents the contractor is allowed to see.
5. **Azure AD B2B:** If the contractor is external to your organization, consider using Azure AD B2B (Business to Business) to manage their access. This allows you to invite external users and manage their permissions more effectively.

Would any of these solutions work for your scenario? If you need more details on any of these approaches, feel free to ask!



Edit in Pages



Copy

● 1 of 30 responses

AI-generated content may be incorrect





Robert Crane 13:10

Patron Copilot Please explain the benefits of using the tenant release preference in Microsoft 365 to gain access to the latest releases of all the services



Patron Copilot AI generated 13:10

Using the tenant release preference in Microsoft 365 offers several benefits, especially for small businesses looking to stay ahead with the latest features and improvements. Here are some key advantages:

#### 1. Early Access to New Features

- **Innovation:** Gain early access to the latest features and updates, allowing your business to leverage new tools and functionalities before they are generally available.
- **Competitive Edge:** Stay ahead of competitors by utilizing the most recent advancements in Microsoft 365 services.

#### 2. Improved Productivity

- **Enhanced Tools:** Benefit from the latest productivity tools and enhancements, which can streamline workflows and improve overall efficiency.
- **User Experience:** Provide your team with the most up-to-date user experiences, which can lead to higher satisfaction and better adoption rates.

#### 3. Better Planning and Preparation

- **Testing and Feedback:** Test new features in your environment and provide feedback to Microsoft, helping to shape the final release.
- **Training:** Prepare your team for upcoming changes by offering training and resources ahead of the general release.

#### 4. Security and Compliance

- **Latest Security Features:** Access the newest security features and updates, ensuring your business is protected against the latest threats.
- **Compliance:** Stay compliant with the latest

Forms



## Café Drink Orders

Please select a drink to order

\* Required

1. Your name \*

2. Email \*

3. Mobile

4. Drink

☐ Caffe Latte

Power  
Automate





When a new response is submitted



Apply to each



Get response details



Compose



Create item



Get items



Select



## Copilot



### Automate

Be more efficient than ever with AI assistance. Simply tell Copilot what you want to do and it will help you get started.

1 of 3

Next

Welcome back! If you want me to change your flow, just say what you want. For example:

- Add an action that sends an email
- Explain what an action does
- Add a condition

Check the flow's actions to see if any parameters need to be set. Don't forget to save when you're done!

AI-generated content may be incorrect



Connected to **Microsoft Forms**

Connected to **SharePoint**

Connected to **Mail**

Ask a question or describe how you want to change this flow

0/2000



Make sure AI-generated content is accurate and appropriate before using.

Free  
Support



## Summary

- Are you using all the free included capabilities?
- Are you using the low cost addons available from Microsoft?
- Are you using code to achieve scale and save time?
- Are overlooking the integration between services?
- Are you utilising all the support available?

<https://bit.ly/cia-m365overlooked>

