

Complete Security with Microsoft Defender

Version 24.12

Ahmed Abdelwahed

ahmed@abdelwahed.me

www.abdelwahed.me

[LinkedIn](#)

Microsoft Defender for Office 365

Microsoft Defender for Office 365 is a comprehensive security solution designed to protect organizations using Microsoft 365 from various cyber threats such as phishing, malware, ransomware, and business email compromise (BEC). Here's an in-depth look at its features, functionalities, and capabilities:

Key Features

1. Email Protection

- **Anti-phishing:** Identifies and blocks sophisticated phishing attacks using machine learning and impersonation detection.
- **Anti-spam:** Prevents spam and bulk emails with advanced filtering techniques.
- **Malware Detection:** Scans emails and attachments for known and unknown malware using AI and heuristic-based analysis.

2. Threat Investigation and Response

- **Threat Explorer and Real-Time Detections:** Provides administrators with tools to investigate and respond to threats.
- **Automated Investigation and Response (AIR):** Automates threat response by identifying, investigating, and mitigating risks without manual intervention.
- **Attack Simulation Training:** Allows organizations to simulate phishing attacks and train employees on recognizing threats.

3. Advanced Threat Protection

- **Safe Attachments:** Scans email attachments in a secure sandbox before delivering them to recipients.
- **Safe Links:** Protects users by scanning URLs in emails and documents to identify malicious links.
- **Zero-Hour Auto Purge (ZAP):** Removes phishing and spam emails post-delivery if later identified as harmful.

4. Collaboration Security

- **Microsoft Teams Protection:** Safeguards Teams chats and shared content from malicious files and phishing attempts.
- **SharePoint and OneDrive Protection:** Detects and blocks malicious files in cloud storage and collaboration platforms.

5. Reporting and Analytics

- **Advanced Reporting:** Provides detailed insights into detected threats, attack trends, and user vulnerabilities.
- **Compliance Reports:** Helps organizations meet regulatory requirements by providing exportable threat intelligence reports.
- **Security Score Integration:** Improves security posture with actionable recommendations in Microsoft Secure Score.

Deployment and Integration

Microsoft Defender for Office 365 integrates seamlessly with the broader Microsoft 365 ecosystem, including Azure AD, Microsoft Endpoint Manager, and other security solutions like Microsoft Defender for Identity and Cloud App Security.

Plans and Licensing:

- **Plan 1:** Basic protection for email and collaboration tools.
- **Plan 2:** Includes Plan 1 features plus advanced threat hunting, investigation, and response capabilities.

Use Cases

1. Phishing Attack Prevention:

- Protect users from spear-phishing attempts targeting executive employees.
- Block fake login pages using Safe Links.

2. Incident Response:

- Automate incident response to minimize the time between detection and mitigation.
- Use Threat Explorer to identify impacted mailboxes and isolate malicious content.

3. Data Loss Prevention (DLP):

- Integrate with Microsoft Purview DLP to prevent sensitive information from being shared via email.

4. User Education:

- Conduct regular phishing simulations and track employee progress in recognizing phishing emails.

Steps for Implementation

1. Enable Policies:

- Configure anti-phishing, anti-spam, and anti-malware policies in the Microsoft 365 Defender portal.

2. Set Up Safe Attachments and Safe Links:

- Define policies to scan attachments and links in real-time.

3. Monitor and Respond:

- Regularly use Threat Explorer to monitor potential threats.
- Configure Automated Investigation and Response (AIR) to handle low-priority incidents.

4. Educate Users:

- Implement Attack Simulation Training to educate users on recognizing threats.

Benefits

- Comprehensive protection across email and collaboration tools.
- Reduced administrative overhead with automated threat response.
- Enhanced security awareness among users through training simulations.
- Detailed insights into organizational threat landscapes.

Using Defender for Office 365

Microsoft 365 Defender portal

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

Preset Security Policies

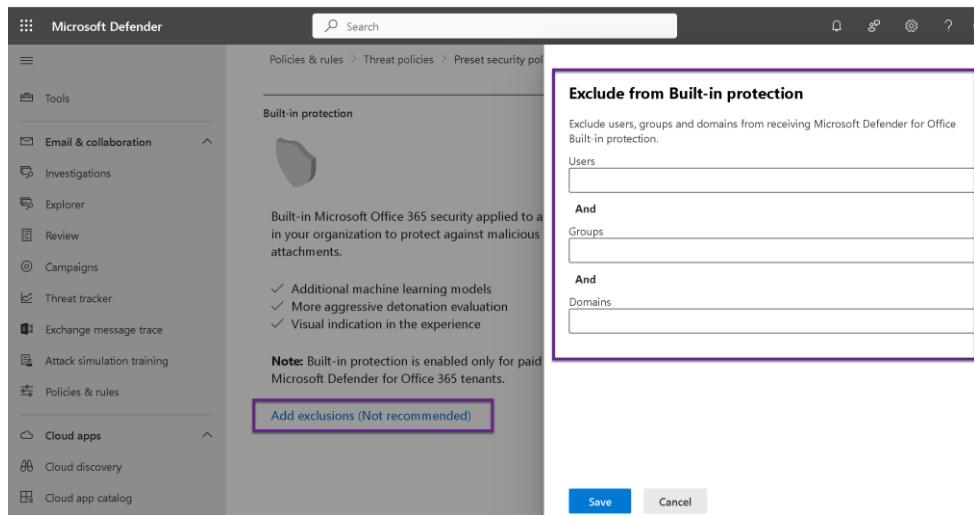
Preset Security Policies are pre-defined configurations in Microsoft Defender for Office 365 designed to enforce security controls for:

Feature	Standard Protection	Strict Protection
Anti-Spam	Balanced approach to spam filtering.	Aggressive spam and bulk email blocking.
Anti-Phishing	Protects against impersonation attacks.	Enhanced anti-impersonation and spoofing.
Safe Links	Scans URLs in emails and Office documents.	Enforces stricter scanning and monitoring.
Safe Attachments	Scans and quarantines suspicious files.	Uses advanced heuristics for attachments.

These policies help reduce administrative overhead and ensure your organization aligns with Microsoft's recommended security settings.

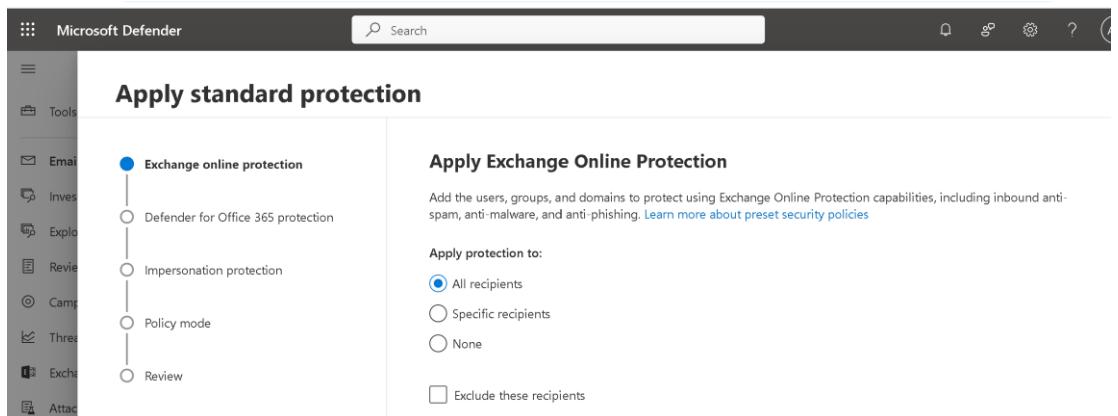
The image shows two screenshots of the Microsoft Defender portal. The top screenshot displays the 'Threat policies' page under 'Policies & rules > Threat policies'. It features a sidebar with 'Email & collaboration' and 'Policies & rules' selected. The main area shows 'Templated policies' with 'Preset Security Policies' highlighted, and a list of 'Policies' including Anti-phishing, Anti-spam, Anti-malware, Safe Attachments, and Safe Links. The bottom screenshot shows the 'Preset security policies' page under 'Policies & rules > Threat policies > Preset security policies'. It compares 'Built-in protection' (disabled for free tenants), 'Standard protection' (selected), and 'Strict protection'. Each profile is described with its features and a 'Manage protection settings' button.

Complete Security with Microsoft Defender



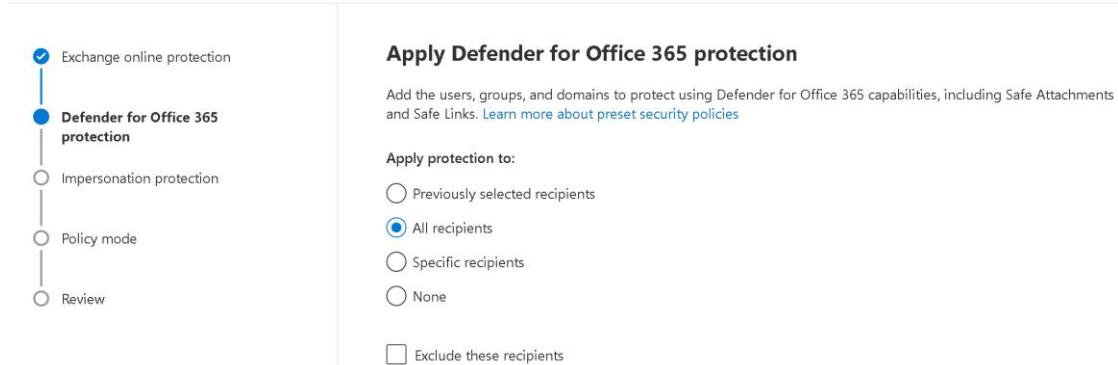
The screenshot shows the Microsoft Defender interface with the 'Policies & rules' and 'Threat policies' navigation paths. The main content area is titled 'Built-in protection' and describes the built-in Microsoft Office 365 security applied to the organization. It lists three features: Additional machine learning models, More aggressive detonation evaluation, and Visual indication in the experience. A note states that built-in protection is enabled only for paid Microsoft Defender for Office 365 tenants. A purple box highlights the 'Add exclusions (Not recommended)' button. To the right, a modal dialog box titled 'Exclude from Built-in protection' is open, with fields for 'Users', 'And', 'Groups', 'And', and 'Domains', each with a text input field. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Setting up the Preset Security Policies



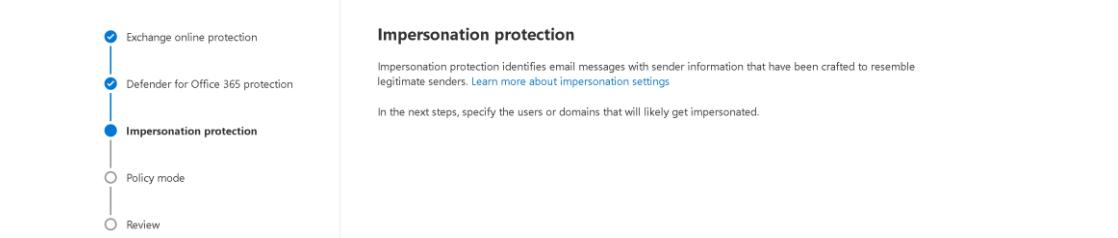
The screenshot shows the Microsoft Defender interface with the 'Policies & rules' and 'Threat policies' navigation paths. The main content area is titled 'Apply standard protection' and shows a tree view of protection types: Exchange online protection (selected), Defender for Office 365 protection, Impersonation protection, Policy mode, and Review. To the right, a section titled 'Apply Exchange Online Protection' provides instructions to add users, groups, and domains for inbound anti-spam, anti-malware, and anti-phishing protection. It includes radio buttons for 'All recipients', 'Specific recipients', and 'None', and a checkbox for 'Exclude these recipients'.

Apply standard protection



The screenshot shows the Microsoft Defender interface with the 'Policies & rules' and 'Threat policies' navigation paths. The main content area is titled 'Apply standard protection' and shows a tree view of protection types: Exchange online protection (selected), Defender for Office 365 protection (selected), Impersonation protection, Policy mode, and Review. To the right, a section titled 'Apply Defender for Office 365 protection' provides instructions to add users, groups, and domains for Safe Attachments and Safe Links protection. It includes radio buttons for 'Previously selected recipients', 'All recipients', 'Specific recipients', and 'None', and a checkbox for 'Exclude these recipients'.

Apply standard protection



The screenshot shows the Microsoft Defender interface with the 'Policies & rules' and 'Threat policies' navigation paths. The main content area is titled 'Apply standard protection' and shows a tree view of protection types: Exchange online protection (selected), Defender for Office 365 protection (selected), Impersonation protection (selected), Policy mode, and Review. To the right, a section titled 'Impersonation protection' provides instructions to identify email messages with sender information that resemble legitimate senders. It includes a note: 'In the next steps, specify the users or domains that will likely get impersonated.'

Apply standard protection

- Exchange online protection
- Defender for Office 365 protection
- Impersonation protection**
- Protected custom users (0/350)
 - Protected custom domains (0/50)
 - Trusted senders (0) and domains (0)
- Policy mode
- Review

Add email addresses to flag when impersonated by attackers

Add internal or external addresses of people who might be impersonated by attackers, such as top-level executives, board members, and other people in key roles. Messages detected with impersonated senders will be quarantined. [Learn more about impersonation settings](#)

Add a name Add a valid email Add

0 items Search

Display name Sender email address

No data available

Apply standard protection

- Exchange online protection
- Defender for Office 365 protection
- Impersonation protection**
- Protected custom users (0/350)
- Protected custom domains (0/50)**
- Trusted senders (0) and domains (0)
- Policy mode
- Review

Add domains to flag when impersonated by attackers

These domains could be yours or domains that belong to your key suppliers and partners. Messages detected with impersonated sender domains will be quarantined. [Learn more about impersonation settings](#)

Add domains Add

Name Remove

Apply standard protection

- Exchange online protection
- Defender for Office 365 protection
- Impersonation protection**
- Protected custom users (0/350)
- Protected custom domains (0/50)
- Trusted senders (0) and domains (0)**
- Policy mode
- Review

Add trusted email addresses and domains to not flag as impersonation

Email messages from these senders will not be flagged as impersonation.

Add domains Add

Name Type Remove

Apply standard protection

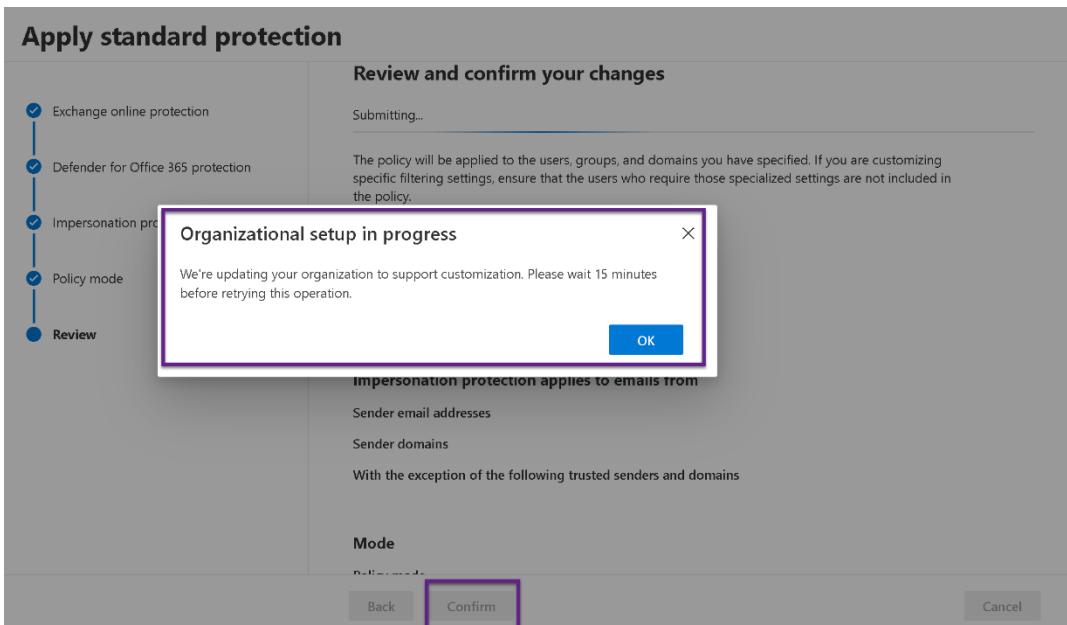
- Exchange online protection
- Defender for Office 365 protection
- Impersonation protection
- Policy mode**
- Review

Policy mode

Select if you want this policy turned on or off after completing this wizard.

- Turn on the policy when finished
 Leave it turned off

Complete Security with Microsoft Defender

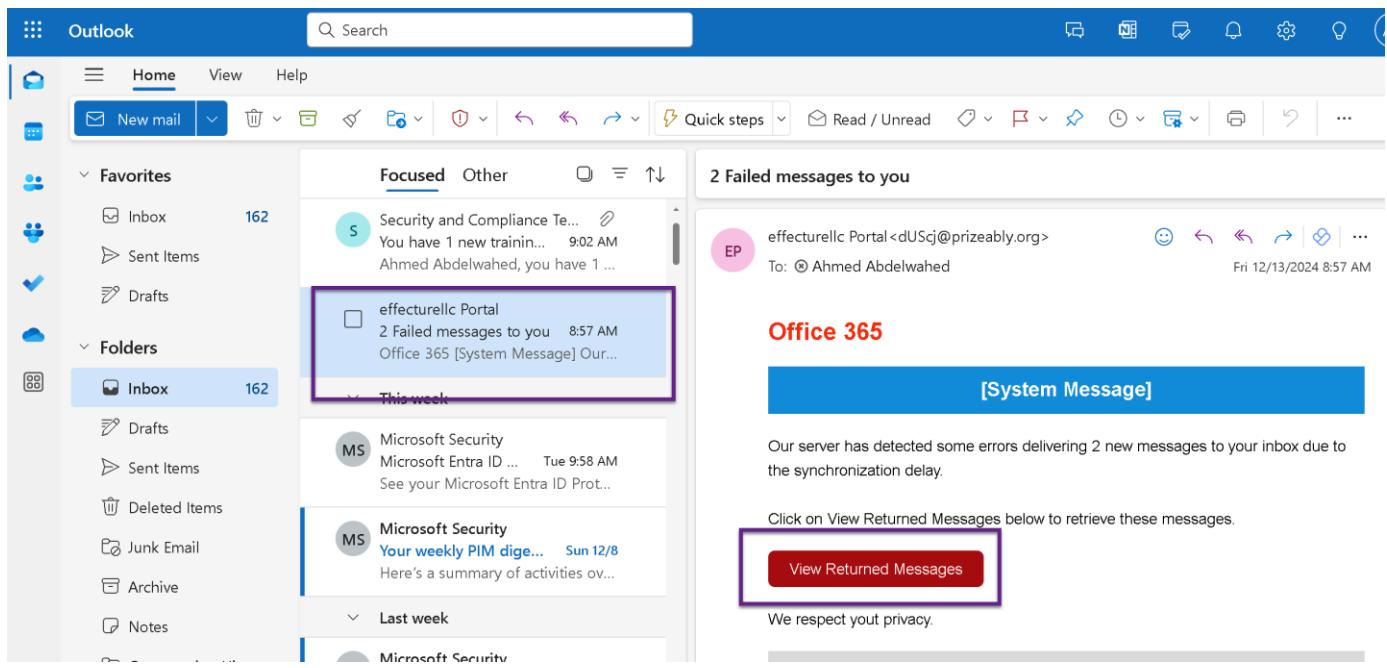


Simulate attack

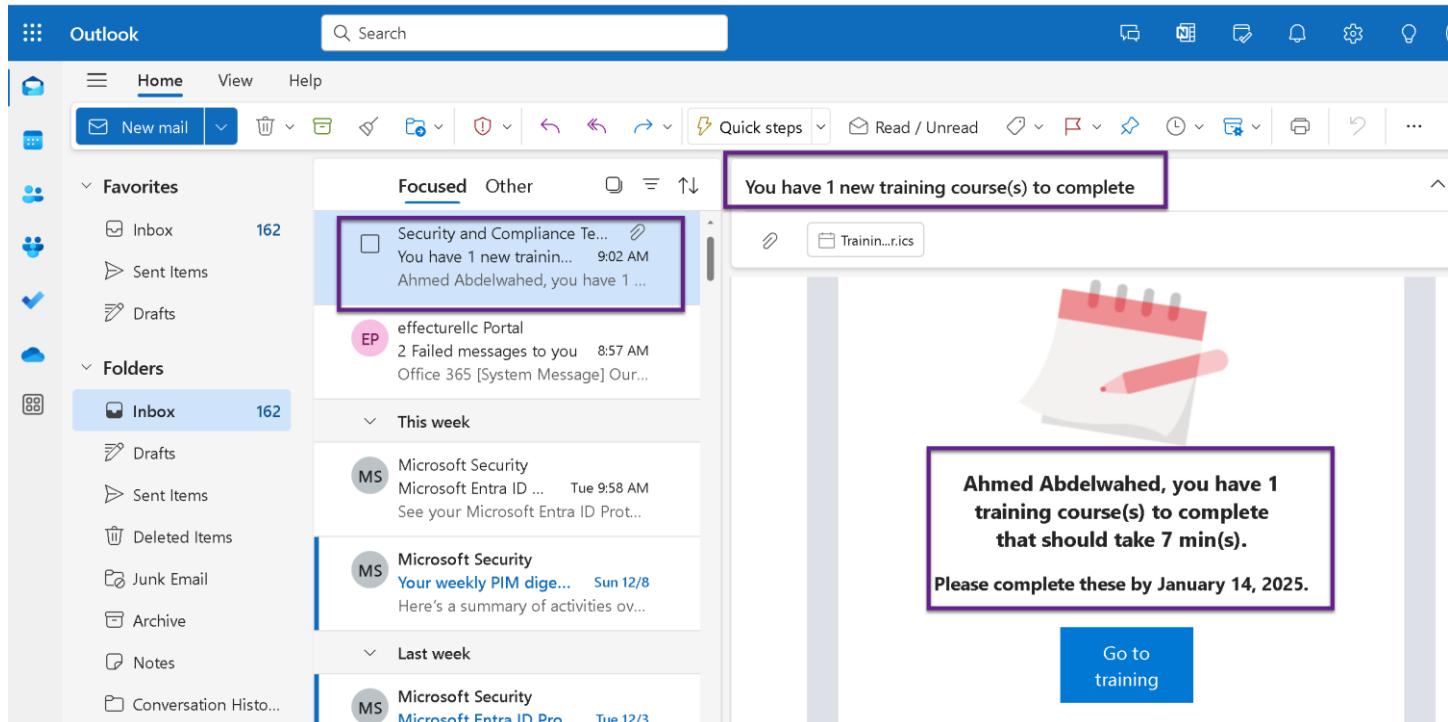
The screenshot shows the Microsoft Defender interface with the 'Attack simulation training' section highlighted in the sidebar. The main area displays 'Top actions to help you get started' with 'Create a simulation' and 'Explore Payload library' sections. On the right, a 'Launch an instant simulation' panel shows a simulation preview for 'Office 365' with a 'System Message' and a 'View Returned Messages' button. The 'Simulation Name' is listed as 'Baseline Credential Harvest' with a 'Launch Simulation' button highlighted with a purple box. A 'Create your own simulation' button is also visible.

Complete Security with Microsoft Defender

Users will receive the following message as simulation



Once the user interact with the email, will receive another email



Complete Security with Microsoft Defender

You can see the result

The image displays three screenshots of the Microsoft Defender interface, highlighting the 'Attack simulation training', 'User Coverage', and 'Email Explorer' sections.

Attack simulation training (Top Screenshot):

- Left sidebar:** Shows navigation items including 'Attack simulation training' (highlighted with a purple box).
- Header:** 'Microsoft Defender' with a search bar and global settings.
- Content:** 'Attack simulation training' report with the following data:
 - Simulation coverage:** 95% users have not experienced the simulation. (Highlight: 'View simulation coverage rep...')
 - Training completion:** 0% users have completed training. (Highlight: 'View training completion report')
 - Repeat offenders:** 0 user(s) are repeat offender. (Highlight: 'View repeat offender report')

User Coverage (Middle Screenshot):

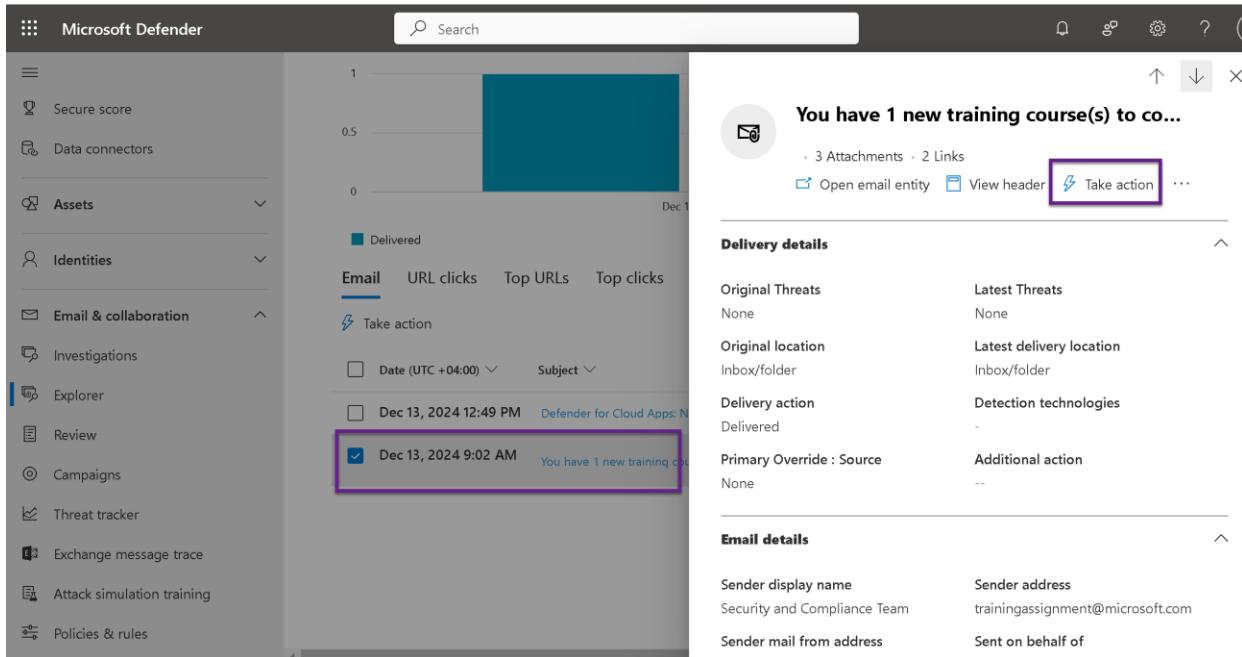
- Left sidebar:** Shows navigation items including 'User Coverage' (highlighted with a purple box).
- Header:** 'Attack simulation training > Attack simulation report' with a search bar and global settings.
- Content:** 'User Coverage' report showing:
 - Simulated users: 1 (highlighted with a purple box)
 - Non-simulated users: 18 (highlighted with a purple box)With buttons for 'Export' and 'Refresh'.

Email Explorer (Bottom Screenshot):

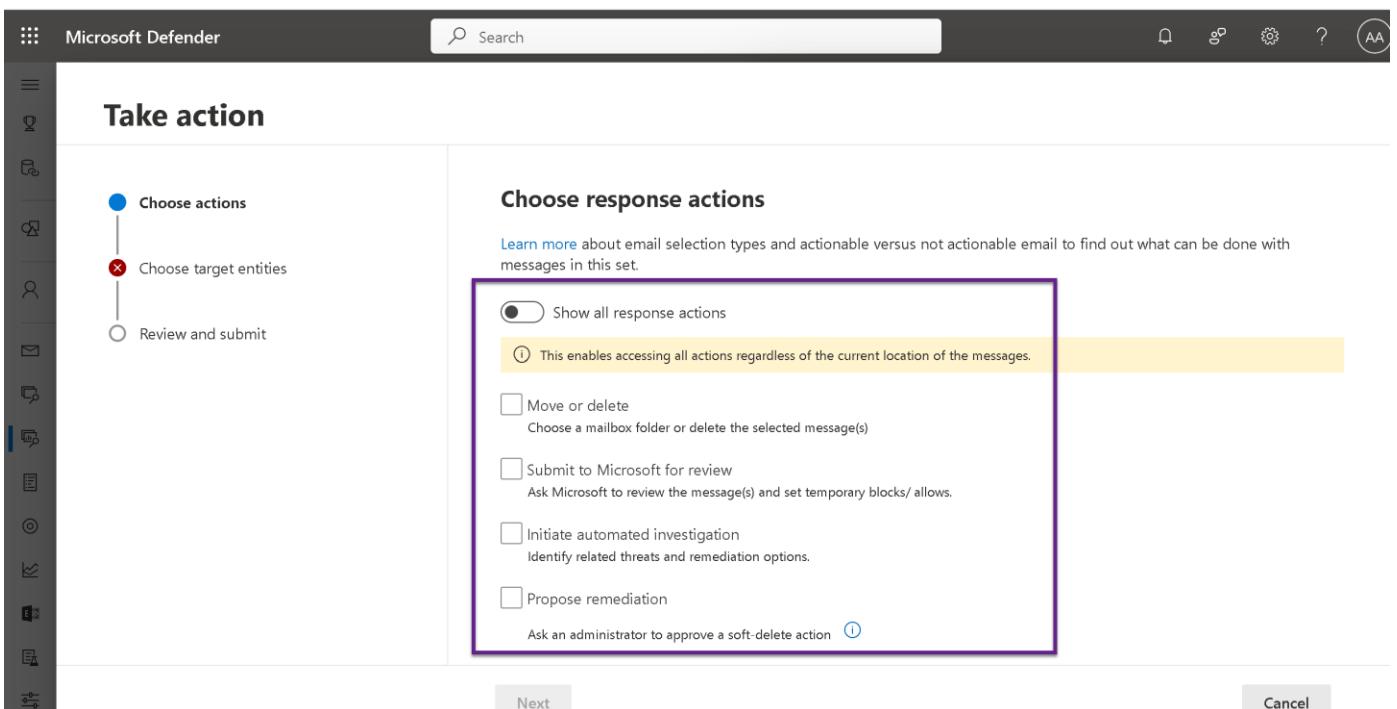
- Left sidebar:** Shows navigation items including 'Email & collaboration' and 'Email Explorer' (highlighted with a purple box).
- Header:** 'Microsoft Defender' with a search bar and global settings.
- Content:** 'All email' report with a histogram chart showing data for 'Delivered' emails. The chart shows a single bar at 1.0 for the date 'Dec 13, 2024 9:00 AM'. With buttons for 'Export chart data' and 'Customize columns'.
- Below chart:** Filter and search bar for 'Email' (highlighted with a purple box), 'URL clicks', 'Top URLs', 'Top clicks', 'Top targeted users', 'Email origin', and 'Campaign'.
- Bottom:** Action buttons for 'Take action', 'Export', and 'Customize columns'.

Complete Security with Microsoft Defender

- **Take Action:** Provides remediation steps for handling the alert, such as:
 - Quarantine or delete the email.
 - Report the email as phishing or spam.
 - Investigate related threats across the environment.



The screenshot shows the Microsoft Defender interface. On the left, a sidebar lists various security categories: Secure score, Data connectors, Assets, Identities, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, and Policies & rules. The main pane displays a chart with a teal bar representing 'Delivered' messages. Below the chart, a list of items includes 'Dec 13, 2024 12:49 PM' and 'Defender for Cloud Apps: N...'. A specific item, 'Dec 13, 2024 9:02 AM' with the subject 'You have 1 new training course...', is highlighted with a purple box. To the right of this item is a summary box with the heading 'You have 1 new training course(s) to co...'. It contains a 'Take action' button, which is also highlighted with a purple box. Below this summary are sections for 'Delivery details' and 'Email details', each with several data points.



The screenshot shows the 'Take action' wizard. On the left, a sidebar lists three steps: 'Choose actions' (highlighted with a blue circle), 'Choose target entities' (highlighted with a red cross), and 'Review and submit'. The main pane is titled 'Choose response actions'. It includes a note: 'Learn more about email selection types and actionable versus not actionable email to find out what can be done with messages in this set.' Below this is a toggle switch labeled 'Show all response actions'. A callout box with a purple border highlights the note: 'This enables accessing all actions regardless of the current location of the messages.' A list of actions follows, each with a checkbox:

- Move or delete: Choose a mailbox folder or delete the selected message(s).
- Submit to Microsoft for review: Ask Microsoft to review the message(s) and set temporary blocks/allows.
- Initiate automated investigation: Identify related threats and remediation options.
- Propose remediation: Ask an administrator to approve a soft-delete action. (with a blue info icon)

At the bottom of the pane are 'Next' and 'Cancel' buttons.

Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security) is a **Cloud Access Security Broker (CASB)** solution that provides visibility, control, and protection for data and applications in the cloud. It integrates seamlessly with other Microsoft security tools to deliver comprehensive cloud security for applications like Microsoft 365, Google Workspace, AWS, and more.

Key Features of Microsoft Defender for Cloud Apps

1. Discovery and Visibility

- **Cloud Discovery:**
 - Identifies shadow IT by analyzing traffic logs to detect unsanctioned cloud applications used within the organization.
 - Provides insights into application usage, risk levels, and compliance.
- **App Catalog:**
 - Evaluates over 31,000 cloud apps against 80+ risk factors, such as compliance, data handling, and security.

2. Threat Protection

- **Behavioral Analytics:**
 - Detects anomalies and suspicious activities using machine learning.
 - Identifies unusual logins, excessive downloads, or access from unknown locations.
- **Threat Intelligence:**
 - Correlates threat signals with Microsoft Defender products (e.g., Defender for Endpoint, Defender for Identity).

3. Data Protection

- **Access Controls:**
 - Enforce session controls to prevent unauthorized data sharing or downloads.
 - Provide real-time monitoring and restriction of activities within applications.
- **Data Loss Prevention (DLP):**
 - Protect sensitive data by applying DLP policies across cloud environments.
 - Detects and prevents data sharing that violates organizational policies.

4. Compliance and Governance

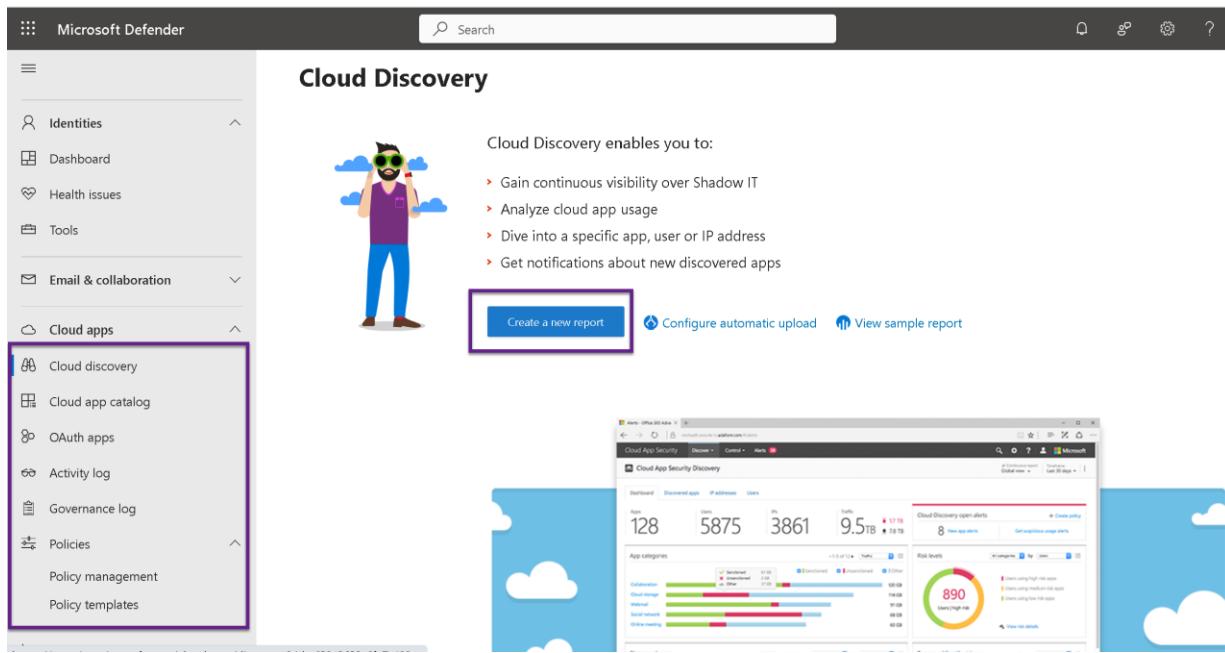
- **Compliance Reporting:**
 - Monitors applications for compliance with regulatory standards such as GDPR, ISO 27001, and HIPAA.
- **Sanctioned and Unsanctioned Apps:**
 - Mark apps as sanctioned or unsanctioned based on organizational risk tolerance.
 - Block or restrict access to unsanctioned apps.

5. Integration with Other Microsoft Tools

- Works with:
 - **Microsoft Defender for Endpoint:** Correlates device activity with cloud app usage.
 - **Microsoft Defender for Identity:** Detects compromised identities accessing cloud applications.
 - **Microsoft Sentinel:** Provides advanced SIEM integration for threat hunting.

Complete Security with Microsoft Defender

To get data here you have to build a report and import the app logs



Create new Cloud Discovery snapshot report

[Guide](#)

OVERVIEW ————— REPORT DETAILS ————— UPLOAD TRAFFIC LOGS ————— FINISH



Create new snapshot report

Snapshot reports provide ad-hoc visibility into a set of traffic logs you manually upload from your firewalls and proxies.

[How to create snapshot report?](#)

Create new Cloud Discovery snapshot report

[Guide](#)

OVERVIEW ————— REPORT DETAILS ————— UPLOAD TRAFFIC LOGS ————— FINISH

Report Name *

SonicWall Firewall Report

Description

(empty)

Source *

SonicWALL

ⓘ This data source contains partial information

Some data attributes are missing from the standard log format of this data source. [Explore alternatives](#)

[View details](#)

ⓘ Verify your log format

Make sure your log files are in the expected format for your data source, otherwise they cannot be processed. To add a custom format, reconfigure your data source settings to match your format.

[View log format](#)

Complete Security with Microsoft Defender



Upload traffic logs *

 [Browse...](#)

Files with activities up to 90 days old and up to 1 GB in size per log file

Create new Cloud Discovery snapshot report

[Guide](#)

Your Cloud Discovery snapshot report is being generated

You can track its status in [Snapshot reports](#)

What happens next?

Upload → Parse → Data analysis → Generated report

⌚ Analysis can takes up to 24 hours

Microsoft Defender

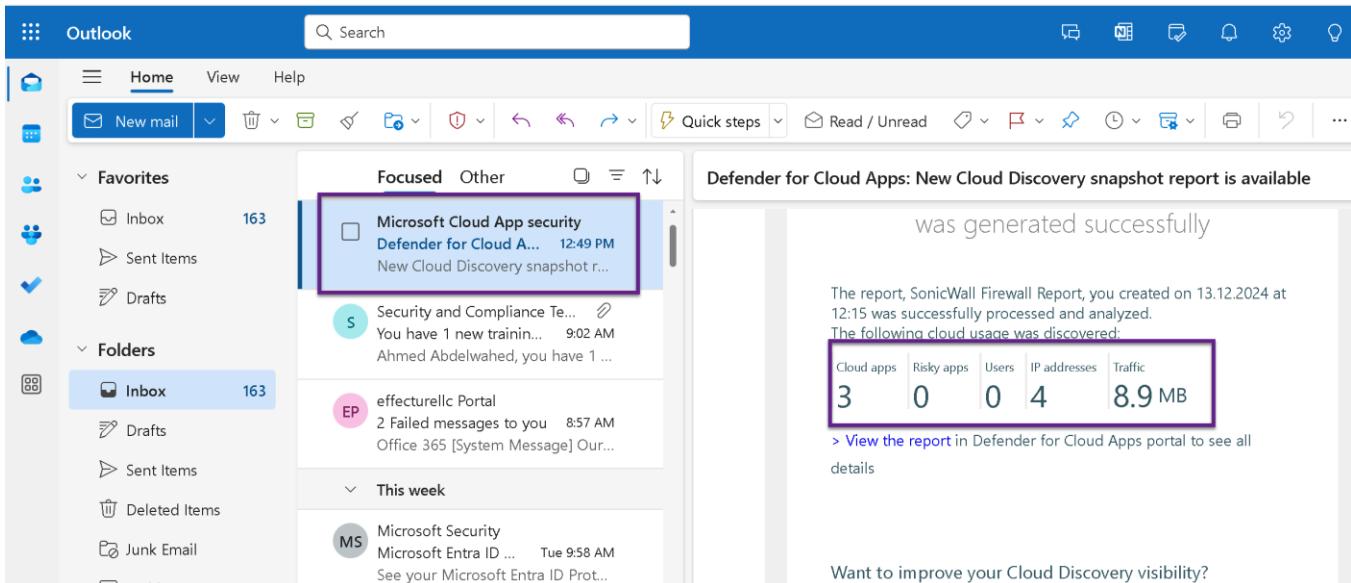
Settings > Cloud apps

Cloud Discovery

Snapshot reports

Name	Date	Last Log	Advertiser	Status
SonicWall Firewall	Sonic...	1	Dec 13...	aabdel... Processing

Complete Security with Microsoft Defender



Policy Templates in Microsoft Defender for Cloud Apps provide pre-configured policies that organizations can use to quickly detect and mitigate common security risks in their cloud environments. These templates are based on Microsoft's best practices and threat intelligence.

This screenshot shows the 'Policy templates' page in Microsoft Defender for Cloud Apps. The left sidebar includes sections for Attack simulation training, Policies & rules, Cloud apps (selected), Cloud discovery, Cloud app catalog, OAuth apps, Activity log, Governance log, Policies (selected), Policy management, and Policy templates (selected). The main content area displays a table of policy templates, with the first five rows highlighted in a blue box. The columns are: Template, Severity (High), Linked policies (0), and Published (Jan 21, 2024 5:27 PM). Each row also has a '+' icon to the right.

Template	Severity	Linked policies	Published
Logon from a risky IP address	High	0	Jan 21, 2024 5:27 PM
Administrative activity from a non-corporate IP address	High	0	Jan 21, 2024 5:27 PM
Potential ransomware activity	High	0	Jan 21, 2024 5:27 PM
Block upload of potential malware (based on Microsoft 1	High	0	Jan 21, 2024 5:27 PM
Block download of potential malware (based on Microso	High	0	Jan 21, 2024 5:27 PM

Complete Security with Microsoft Defender

The **Policy Management** section in **Microsoft Defender for Cloud Apps** allows administrators to create, manage, and customize security policies to monitor and enforce actions across cloud applications. These policies enable granular control over activity, access, and data handling in your cloud environment.

Types of Policies in Microsoft Defender for Cloud Apps

The screenshot highlights the ability to create various types of policies, including:

1. Activity Policy

- Monitors specific user or system activities in connected cloud apps.
- Example Use Case: Detects excessive downloads or file deletions by a single user, signaling possible insider threats.

2. File Policy

- Applies to files stored or shared in cloud apps to enforce compliance and security.
- Example Use Case: Detects files containing sensitive data (e.g., PII or credit card numbers) being shared externally.

3. App Discovery Policy

- Helps identify and control the usage of unsanctioned or risky cloud applications.
- Example Use Case: Flags high-risk applications used by employees that are not approved by IT (shadow IT).

4. Access Policy

- Regulates how users access cloud apps based on conditions like IP address, device, or location.
- Example Use Case: Restricts access to corporate apps from non-corporate IP addresses or untrusted devices.

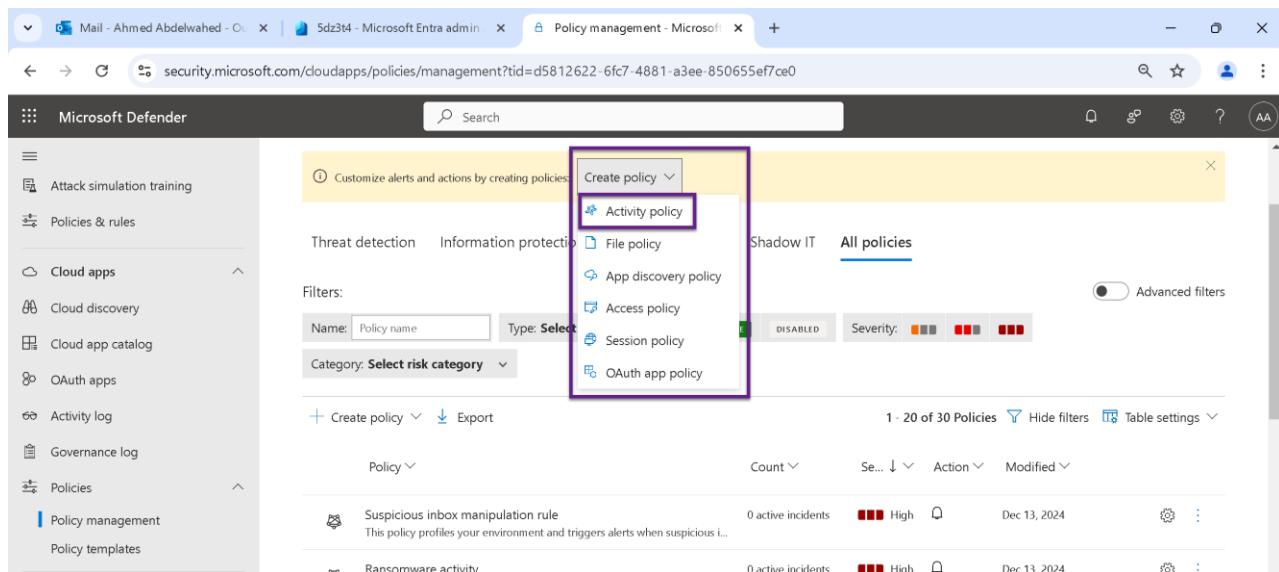
5. Session Policy

- Provides real-time session control over user activities within cloud applications.
- Example Use Case: Blocks downloads of sensitive files to unmanaged devices during a session.

6. OAuth App Policy

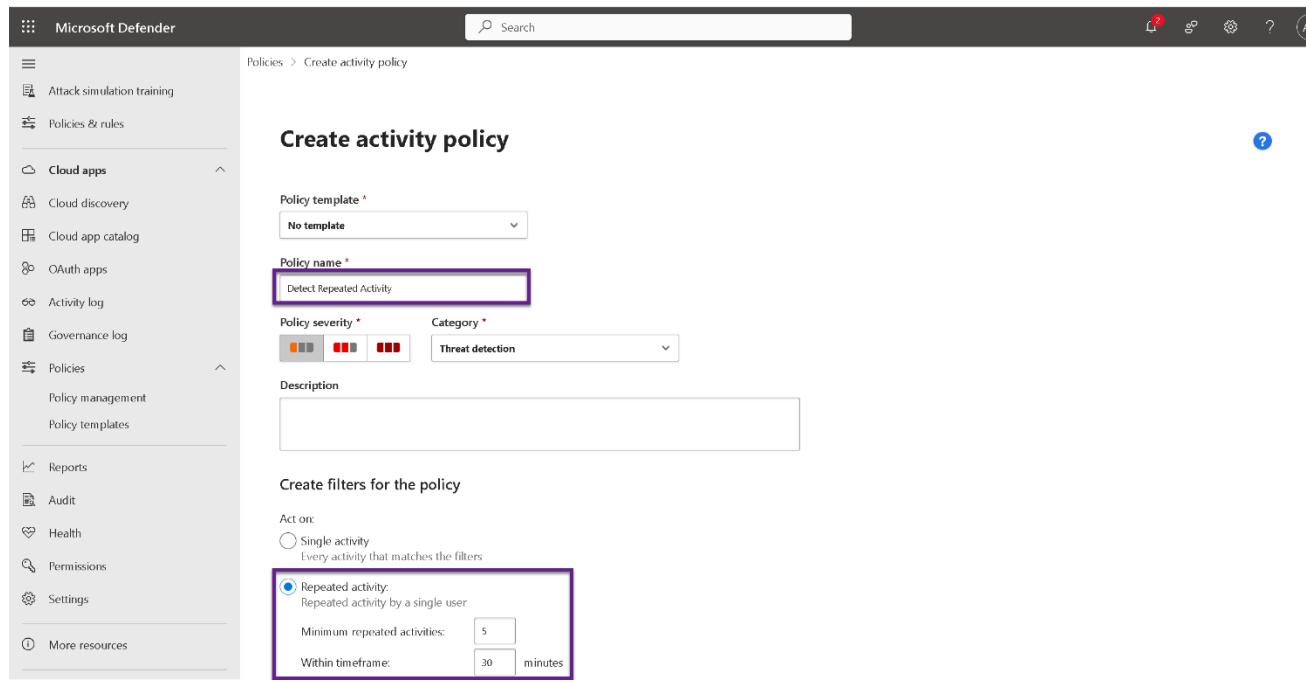
- Monitors and controls third-party OAuth app connections to cloud environments.
- Example Use Case: Detects and blocks malicious or unauthorized OAuth applications attempting to access corporate data.

Create activity policy to Detect Repeated Activity (Download & Delete)



The screenshot shows the Microsoft Defender Policy management interface. The left sidebar navigation includes 'Attack simulation training', 'Policies & rules', 'Cloud apps', 'Cloud discovery', 'Cloud app catalog', 'OAuth apps', 'Activity log', 'Governance log', 'Policies', 'Policy management' (which is selected and highlighted in blue), and 'Policy templates'. The main content area has a header 'Customize alerts and actions by creating policies' with a 'Create policy' button. A dropdown menu is open, showing 'Activity policy' (which is highlighted with a purple box), 'File policy', 'App discovery policy', 'Access policy', 'Session policy', and 'OAuth app policy'. Below this, there are filters for 'Name' (Policy name), 'Type' (Select), 'Category' (Select risk category), and a severity slider. The table below shows 1-20 of 30 Policies, with columns for Policy name, Count, Action, and Modified. Two policies are listed: 'Suspicious inbox manipulation rule' (0 active incidents, High severity, modified Dec 13, 2024) and 'Ransomware activity' (0 active incidents, High severity, modified Dec 13, 2024). The 'All policies' tab is selected in the top right.

Complete Security with Microsoft Defender



Create activity policy

Policy template *
No template

Policy name *
Detect Repeated Activity

Policy severity * **Category ***
Medium Threat detection

Description

Create filters for the policy

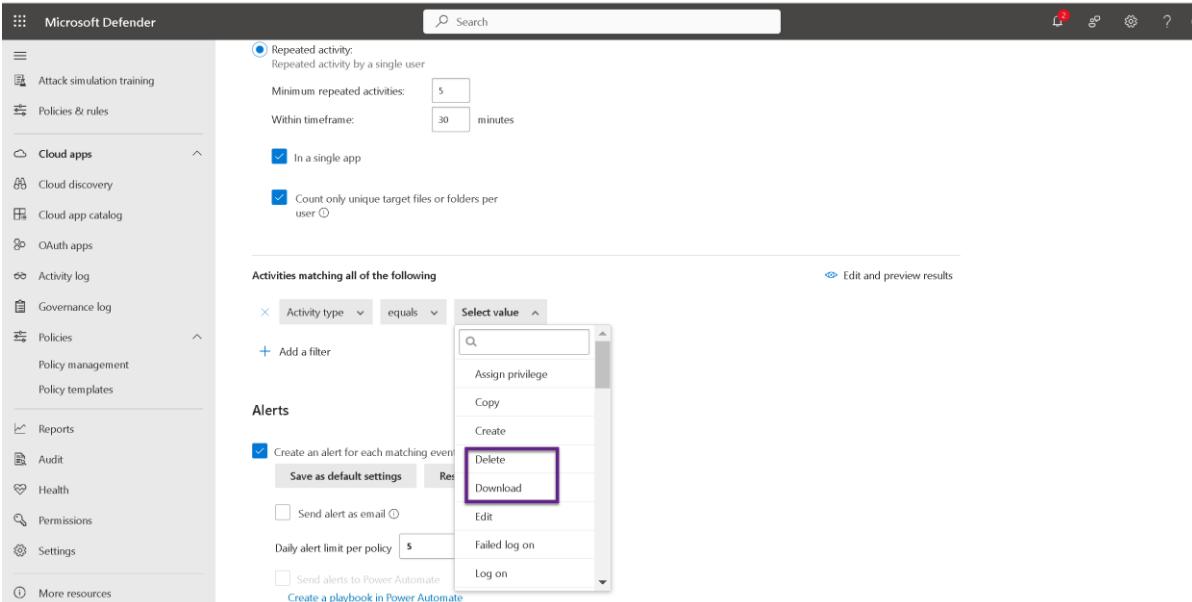
Act on:

Single activity Every activity that matches the filters

Repeated activity: Repeated activity by a single user

Minimum repeated activities: 5

Within timeframe: 30 minutes



Repeated activity:
Repeated activity by a single user

Minimum repeated activities: 5

Within timeframe: 30 minutes

In a single app

Count only unique target files or folders per user

Activities matching all of the following

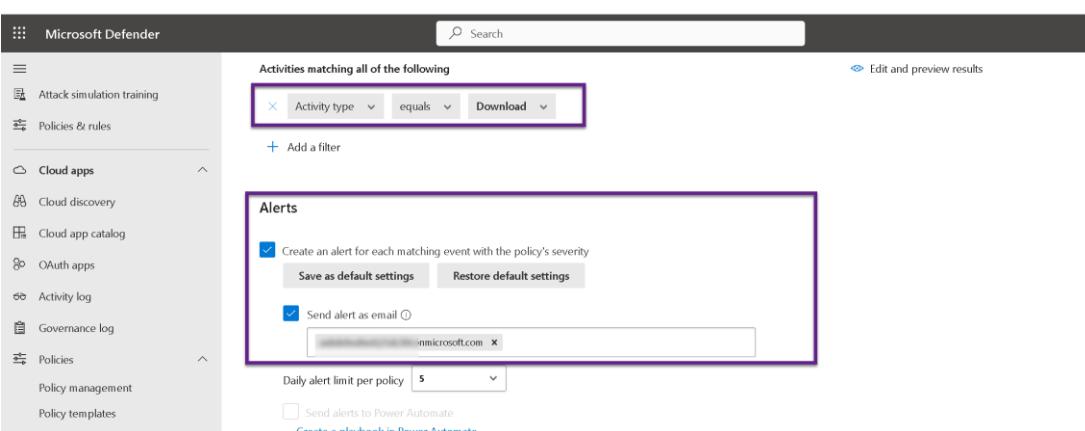
Alerts

Create an alert for each matching event

Select value

- Assign privilege
- Copy
- Create
- Delete
- Download
- Edit
- Failed log on
- Log on

[Edit and preview results](#)



Activities matching all of the following

Alerts

Create an alert for each matching event with the policy's severity

Save as default settings **Restore default settings**

Send alert as email

microsoft.com

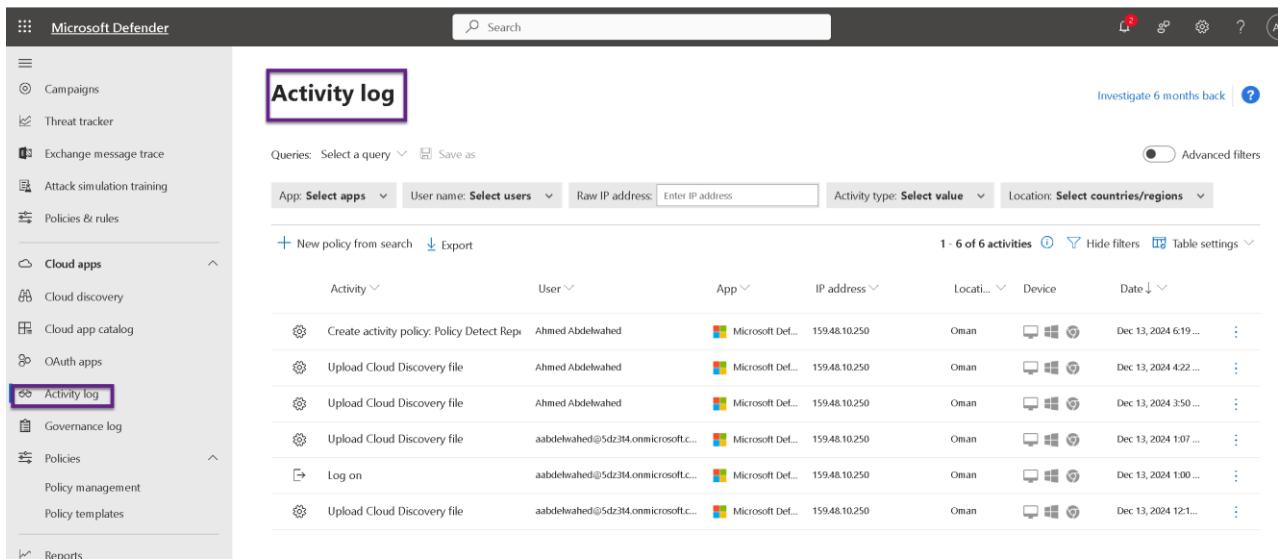
Daily alert limit per policy: 5

Send alerts to Power Automate

[Create a playbook in Power Automate](#)

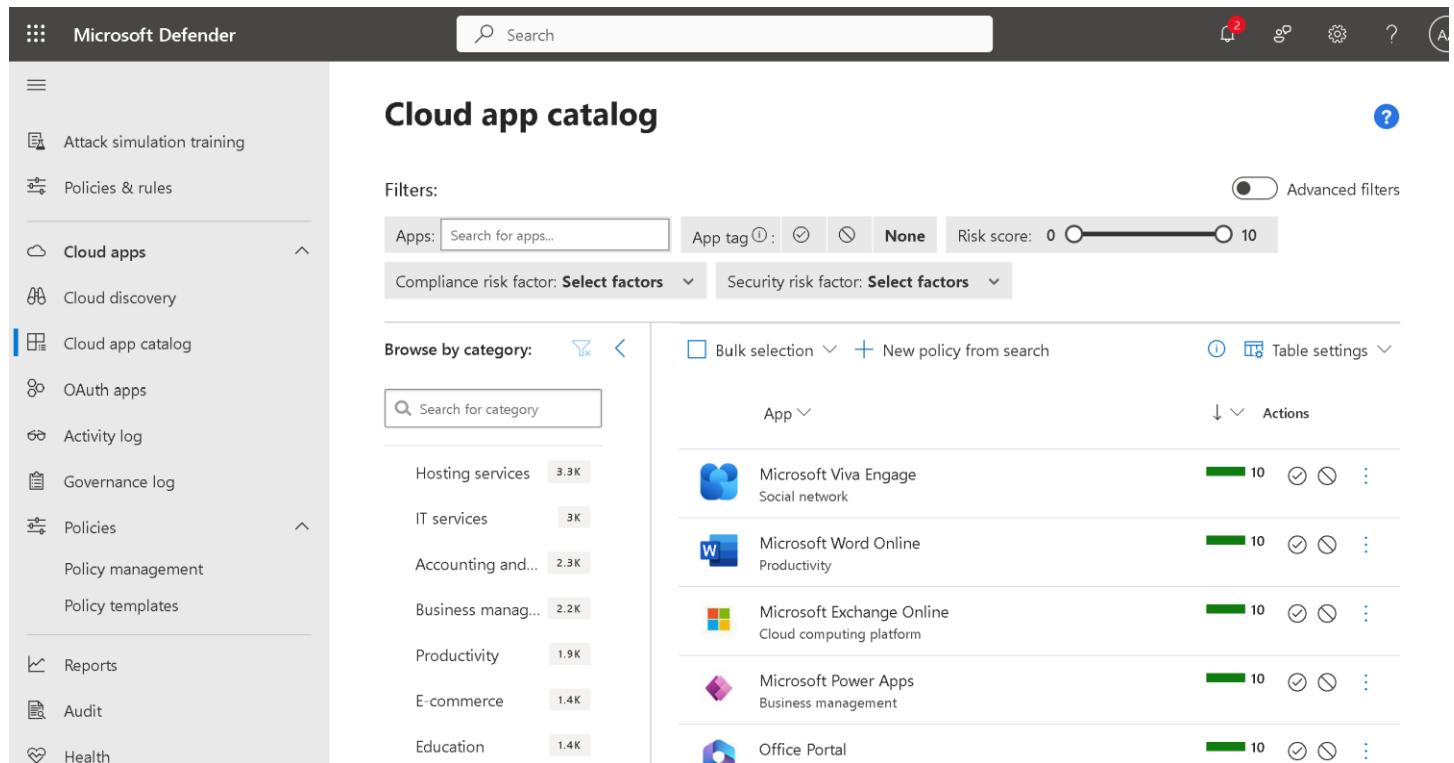
Complete Security with Microsoft Defender

Activity log



The screenshot shows the Microsoft Defender interface with the 'Activity log' section highlighted. The left sidebar includes options like 'Campaigns', 'Threat tracker', 'Exchange message trace', 'Attack simulation training', 'Policies & rules', 'Cloud apps', 'Cloud discovery', 'Cloud app catalog', 'OAuth apps', 'Activity log' (which is selected and highlighted with a purple box), 'Governance log', 'Policies', 'Policy management', 'Policy templates', and 'Reports'. The main area is titled 'Activity log' and shows a table of 6 activities. The columns include 'Activity', 'User', 'App', 'IP address', 'Location', 'Device', and 'Date'. The activities listed are: 'Create activity policy: Policy Detect Rep...', 'Upload Cloud Discovery file', 'Upload Cloud Discovery file', 'Upload Cloud Discovery file', 'Log on', and 'Upload Cloud Discovery file'. All activities are from 'Ahmed Abdelwahed' and occurred on '159.48.10.250' in 'Oman' on 'Dec 13, 2024' at various times.

Cloud App Catalog



The screenshot shows the Microsoft Defender interface with the 'Cloud app catalog' section highlighted. The left sidebar includes options like 'Attack simulation training', 'Policies & rules', 'Cloud apps' (which is selected and highlighted with a blue box), 'Cloud discovery', 'Cloud app catalog' (which is selected and highlighted with a blue box), 'OAuth apps', 'Activity log', 'Governance log', 'Policies', 'Policy management', 'Policy templates', 'Reports', 'Audit', and 'Health'. The main area is titled 'Cloud app catalog' and shows a table of cloud applications. The columns include 'App', 'Actions', and a 'Risk score' slider. The applications listed are: 'Microsoft Viva Engage' (Social network), 'Microsoft Word Online' (Productivity), 'Microsoft Exchange Online' (Cloud computing platform), 'Microsoft Power Apps' (Business management), and 'Office Portal'. Each application has a green risk score bar at 10, and checkboxes for 'Bulk selection' and 'New policy from search'.

Microsoft Defender for Endpoint

Microsoft Intune admin center

5dz3t4

Welcome to the fresh look for Intune

Explore the updated homepage. Inside is still the familiar unified management solution for all your endpoints.

Give us your feedback

Status

Metric	Value
Devices not in compliance	0
Configuration policies with error or conflict	0
Client app install failure	0
Connector errors	0
Service health	Healthy
Account status	Active

The **Endpoint Security | Security Baselines** section in **Microsoft Intune** provides pre-configured security settings recommended by Microsoft for different scenarios. These baselines help organizations quickly apply consistent and secure configurations to their enrolled devices without needing to manually configure every policy.

Microsoft Intune admin center

Home > Endpoint security

Endpoint security | Security baselines

Search

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint Privilege Management
- Endpoint detection and response
- App Control for Business (Preview)
- Attack surface reduction

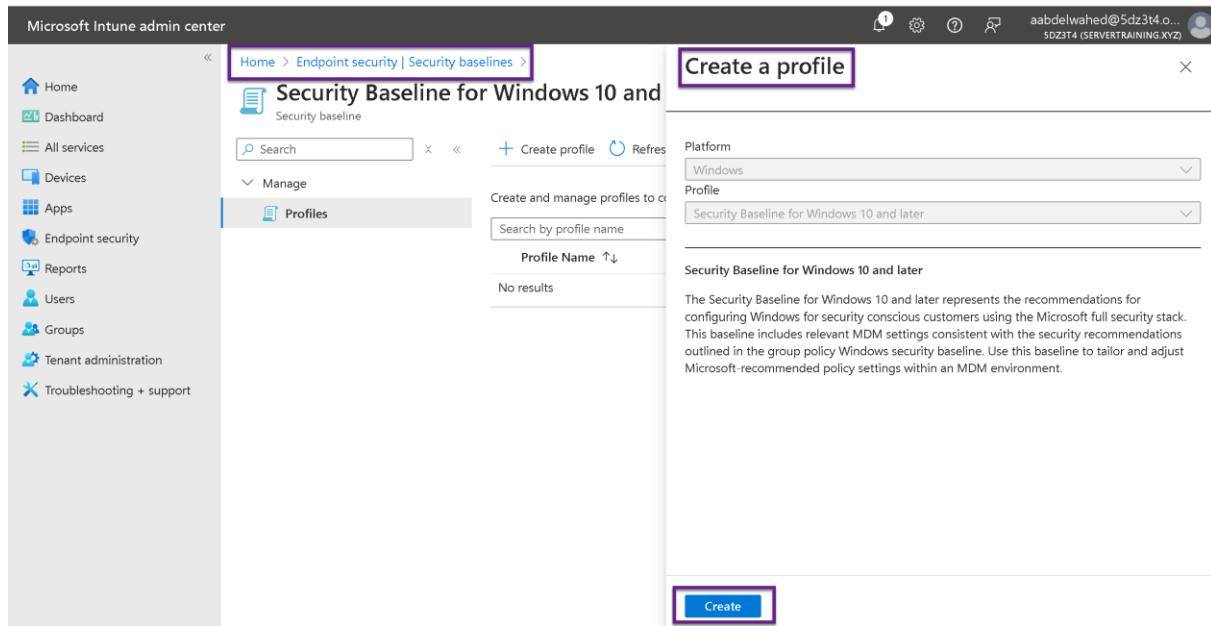
Use security baselines to apply Microsoft-recommended security configuration settings to your enrolled devices. [Learn more.](#)

Baseline	Version
Security Baseline for Windows 10 and later	Version 23H2
Microsoft Defender for Endpoint Security Baseline	Version 24H1
Security Baseline for Microsoft Edge	Version 117
Windows 365 Security Baseline	Version 24H1
Advanced Security Baseline for HoloLens 2	Version 1
Standard Security Baseline for HoloLens 2	Version 1
Microsoft 365 Apps for Enterprise Security Baseline	Version 2306

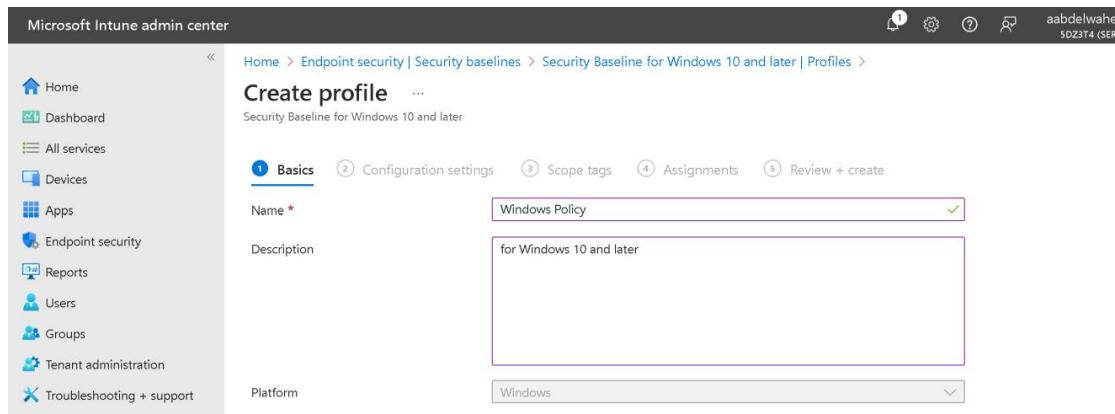
Complete Security with Microsoft Defender

Create Security Baselines for windows 10 and later

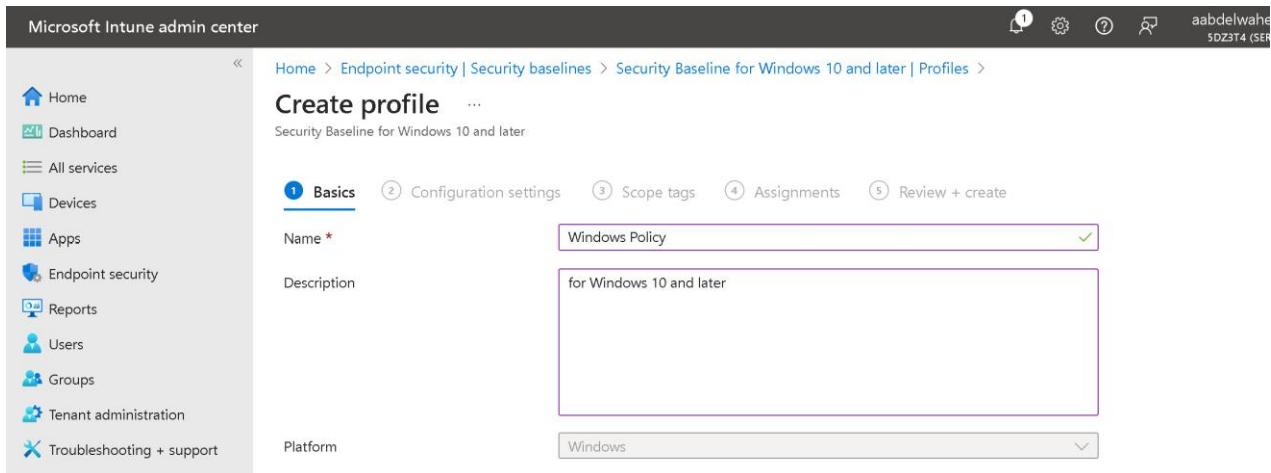
To configure and apply preset settings to Windows 10 and later devices using the Security Baseline for Windows 10 and later, follow these steps in the Microsoft Intune Admin Center:



The screenshot shows the Microsoft Intune Admin Center interface. The left sidebar includes Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main navigation bar shows 'Home > Endpoint security | Security baselines > Security Baseline for Windows 10 and later'. The 'Profiles' tab is selected. A purple box highlights the 'Create profile' button. The right panel displays the 'Create a profile' form for the 'Security Baseline for Windows 10 and later'. It includes fields for Platform (Windows), Profile (Security Baseline for Windows 10 and later), and a detailed description of the baseline. A large purple box highlights the 'Create' button at the bottom.



The screenshot shows the 'Create profile' page for the 'Security Baseline for Windows 10 and later'. The left sidebar and main navigation bar are identical to the previous screenshot. The right panel shows the 'Create profile' form with the 'Basics' tab selected. The 'Name' field is set to 'Windows Policy' and the 'Description' field contains 'for Windows 10 and later'. The 'Platform' dropdown is set to 'Windows'. A purple box highlights the 'Create' button at the bottom.



The screenshot shows the 'Create profile' page for the 'Security Baseline for Windows 10 and later'. The left sidebar and main navigation bar are identical to the previous screenshots. The right panel shows the 'Create profile' form with the 'Basics' tab selected. The 'Name' field is set to 'Windows Policy' and the 'Description' field contains 'for Windows 10 and later'. The 'Platform' dropdown is set to 'Windows'. A purple box highlights the 'Create' button at the bottom.

Complete Security with Microsoft Defender

Microsoft Intune admin center

Home > Endpoint security | Security baselines > Security Baseline for Windows 10 and later | Profiles > Create profile

Defender

Device Guard

Device Lock

Dma Guard

Experience

Firewall

The Firewall configuration service provider configures the Windows Defender Firewall global settings, as well as the desired set of custom rules to be enforced on the device. Using the Firewall CSP the IT admin can now manage non-domain devices, and reduce the risk of network security threats across all systems connecting to the corporate network.

Enable Domain Network Firewall: True

Enable Log Dropped Packets: Enable Logging Of Dropped Packets

Default Outbound Action: Allow

Previous Next

Microsoft Intune admin center

Home > Endpoint security | Security baselines > Security Baseline for Windows 10 and later | Profiles > Create profile

Scope tags

Default

+ Select scope tags

Microsoft Intune admin center

Home > Endpoint security | Security baselines > Security Baseline for Windows 10 and later | Profiles > Create profile

Assignments

Included groups

+ Add groups + Add all users + Add all devices

All devices

Group Members: None

Filter: None

Edit filter

Excluded groups

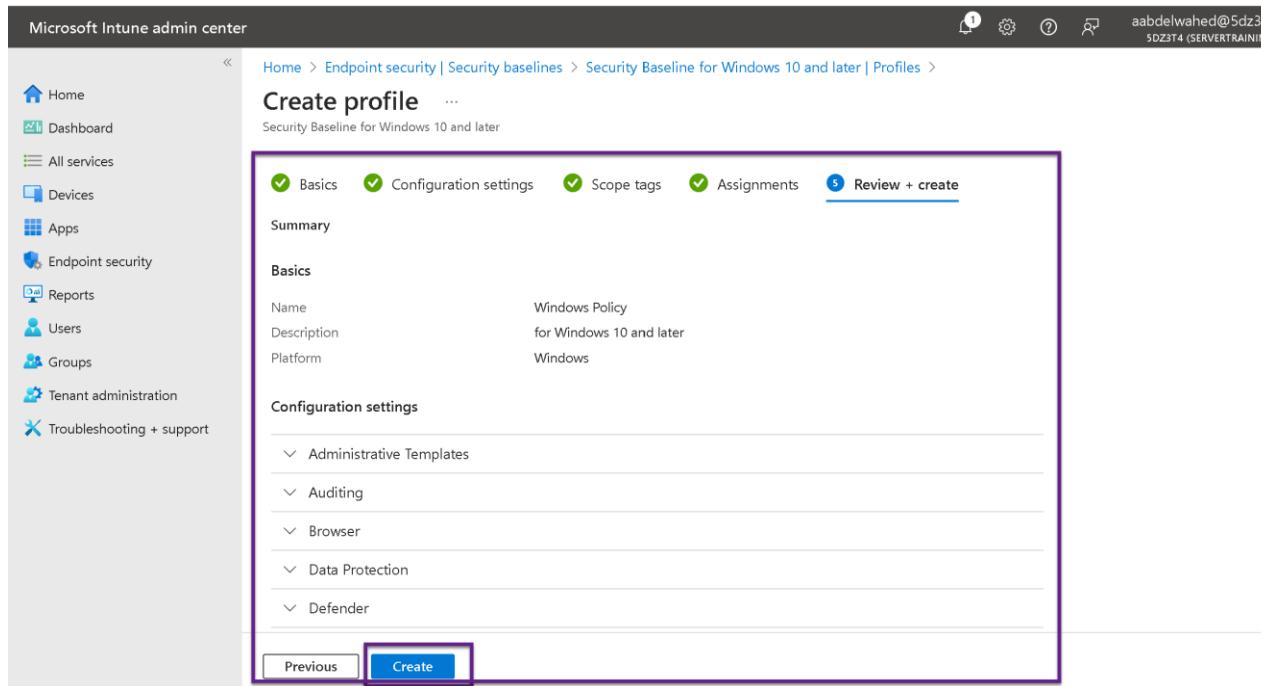
When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more about excluding groups.](#)

+ Add groups

Groups: No groups selected

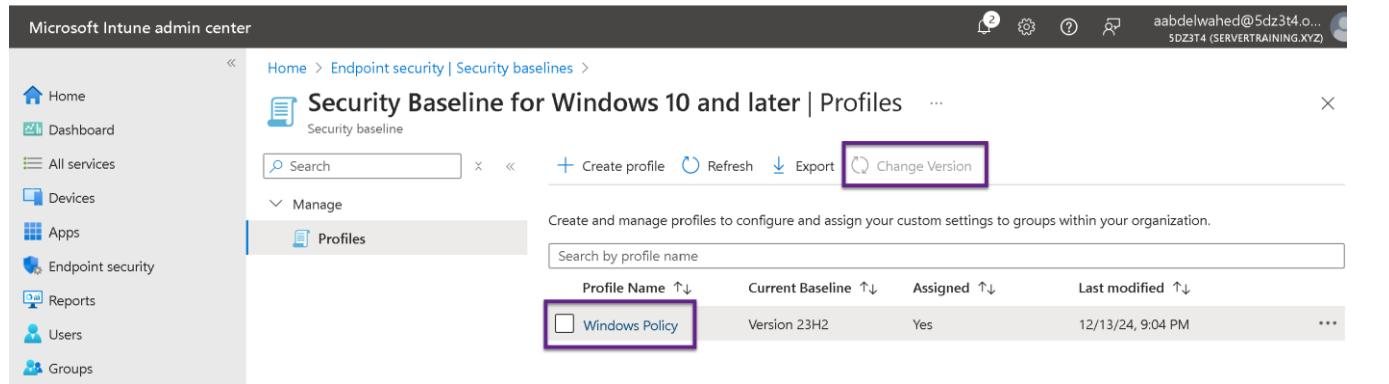
Group Members: Remove

Complete Security with Microsoft Defender



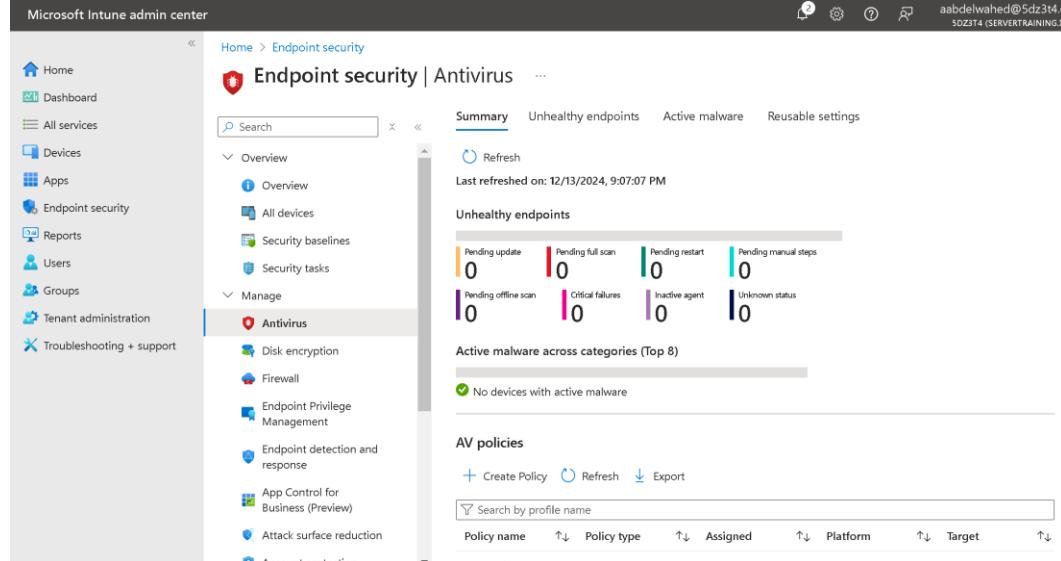
The screenshot shows the 'Create profile' page in the Microsoft Intune admin center. The page is titled 'Create profile' and is part of the 'Security Baseline for Windows 10 and later' section. It has tabs for 'Basics', 'Configuration settings', 'Scope tags', and 'Assignments', with 'Review + create' selected. The 'Basics' section shows a 'Name' of 'Windows Policy', a 'Description' of 'for Windows 10 and later', and a 'Platform' of 'Windows'. The 'Configuration settings' section lists categories like 'Administrative Templates', 'Auditing', 'Browser', 'Data Protection', and 'Defender'. At the bottom are 'Previous' and 'Create' buttons, with 'Create' highlighted.

Any Microsoft coming updates, you can update your policy from the below option



The screenshot shows the 'Security Baseline for Windows 10 and later | Profiles' page in the Microsoft Intune admin center. It displays a list of profiles, with 'Windows Policy' selected. The table includes columns for 'Profile Name' (Windows Policy), 'Current Baseline' (Version 23H2), 'Assigned' (Yes), and 'Last modified' (12/13/24, 9:04 PM). A 'Change Version' button is highlighted with a purple box.

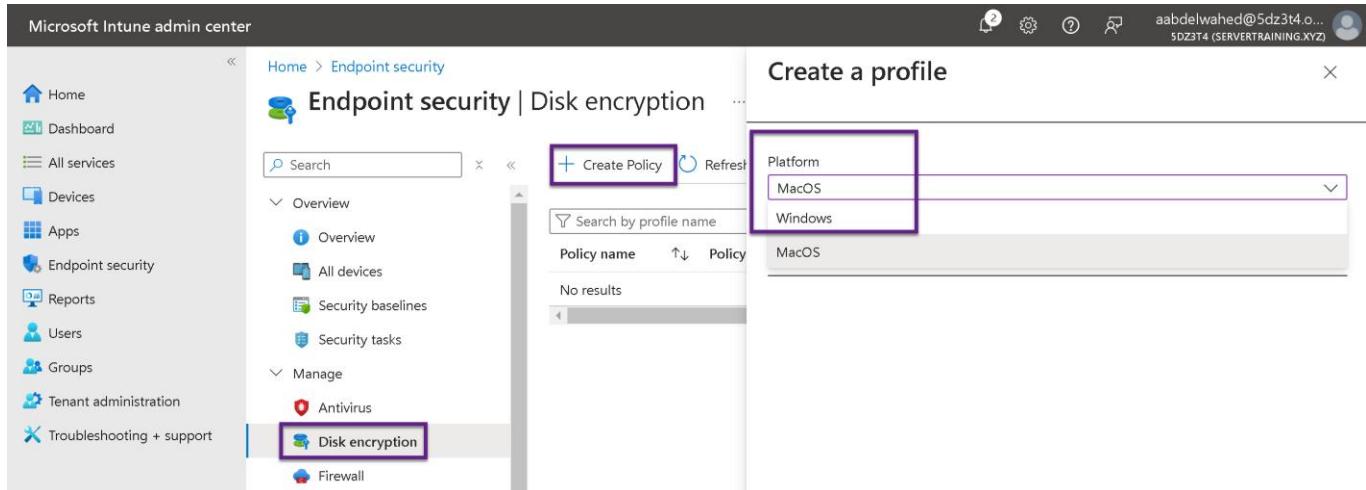
Managing Antivirus



The screenshot shows the 'Endpoint security | Antivirus' page in the Microsoft Intune admin center. It includes sections for 'Overview' (with links to 'Overview', 'All devices', 'Security baselines', 'Security tasks', 'Disk encryption', 'Firewall', 'Endpoint Privilege Management', 'Endpoint detection and response', 'App Control for Business (Preview)', 'Attack surface reduction', and 'Account protection'), 'Unhealthy endpoints' (with metrics for Pending update, Pending full scan, Pending restart, Pending offline scan, Critical failures, Inactive agent, and Unknown status), 'Active malware across categories (Top 8)' (with a note that 'No devices with active malware'), and 'AV policies' (with 'Create Policy', 'Refresh', and 'Export' buttons).

Complete Security with Microsoft Defender

Disk Encryption



Microsoft Intune admin center

Home > Endpoint security

Endpoint security | Disk encryption

Search + Create Policy Refresh

Overview + Overview All devices Security baselines Security tasks

Manage + Antivirus Disk encryption Firewall

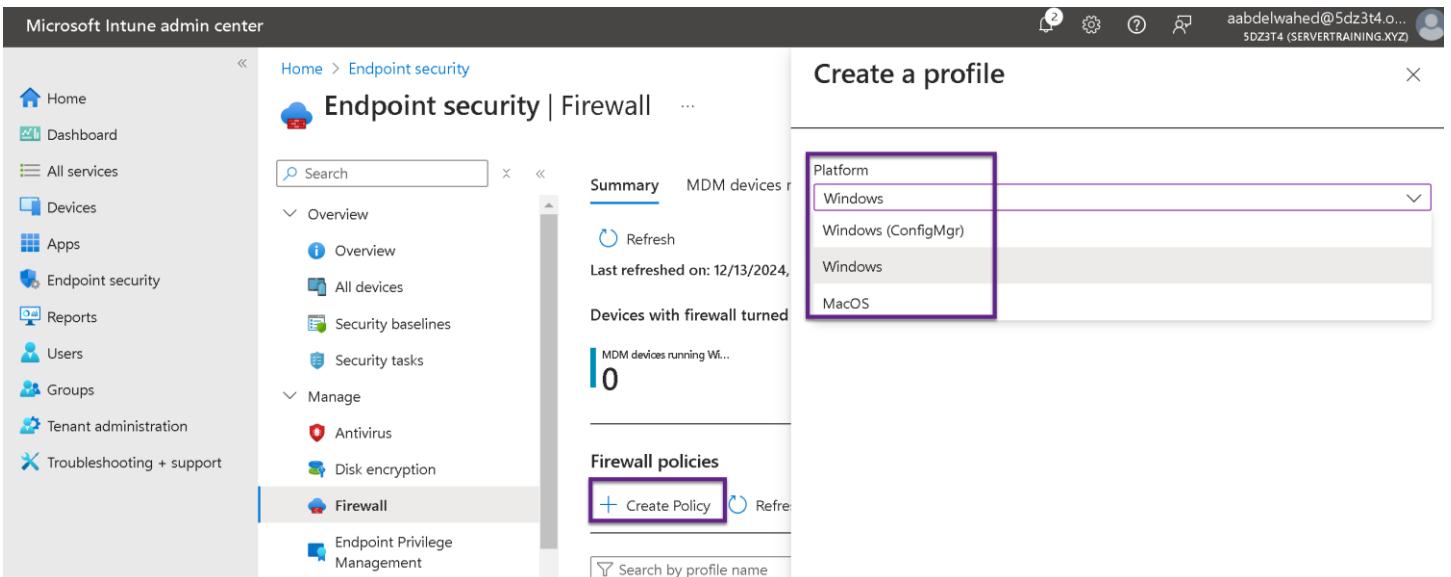
Create a profile

Platform + MacOS Windows

Policy name ↑ ↓ Policy

No results

Managing and Monitoring Firewall



Microsoft Intune admin center

Home > Endpoint security

Endpoint security | Firewall

Search + Create Policy Refresh

Overview + Overview All devices Security baselines Security tasks

Manage + Antivirus Disk encryption Firewall Endpoint Privilege Management

Create a profile

Platform + Windows Windows (ConfigMgr) Windows MacOS

MDM devices running Wi...

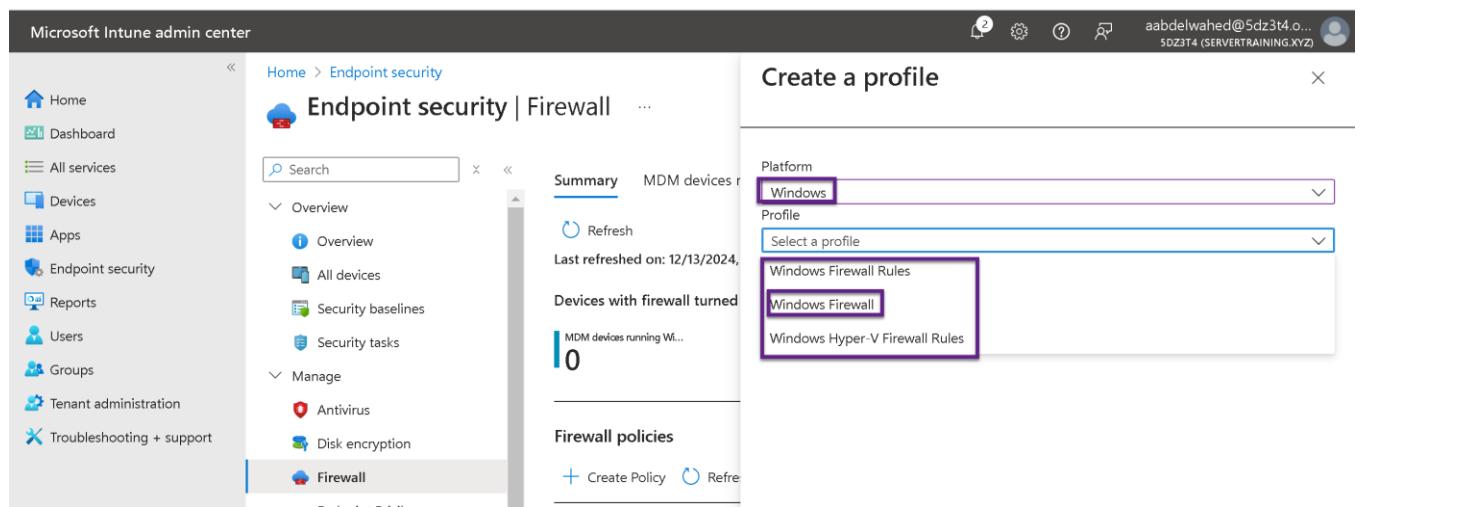
Last refreshed on: 12/13/2024

Devices with firewall turned 0

MDM devices running Wi...

Firewall policies + Create Policy Refresh

Search by profile name



Microsoft Intune admin center

Home > Endpoint security

Endpoint security | Firewall

Search + Create Policy Refresh

Overview + Overview All devices Security baselines Security tasks

Manage + Antivirus Disk encryption Firewall

Create a profile

Platform + Windows

Profile + Select a profile

Windows Firewall Rules + Windows Firewall Windows Hyper-V Firewall Rules

MDM devices running Wi...

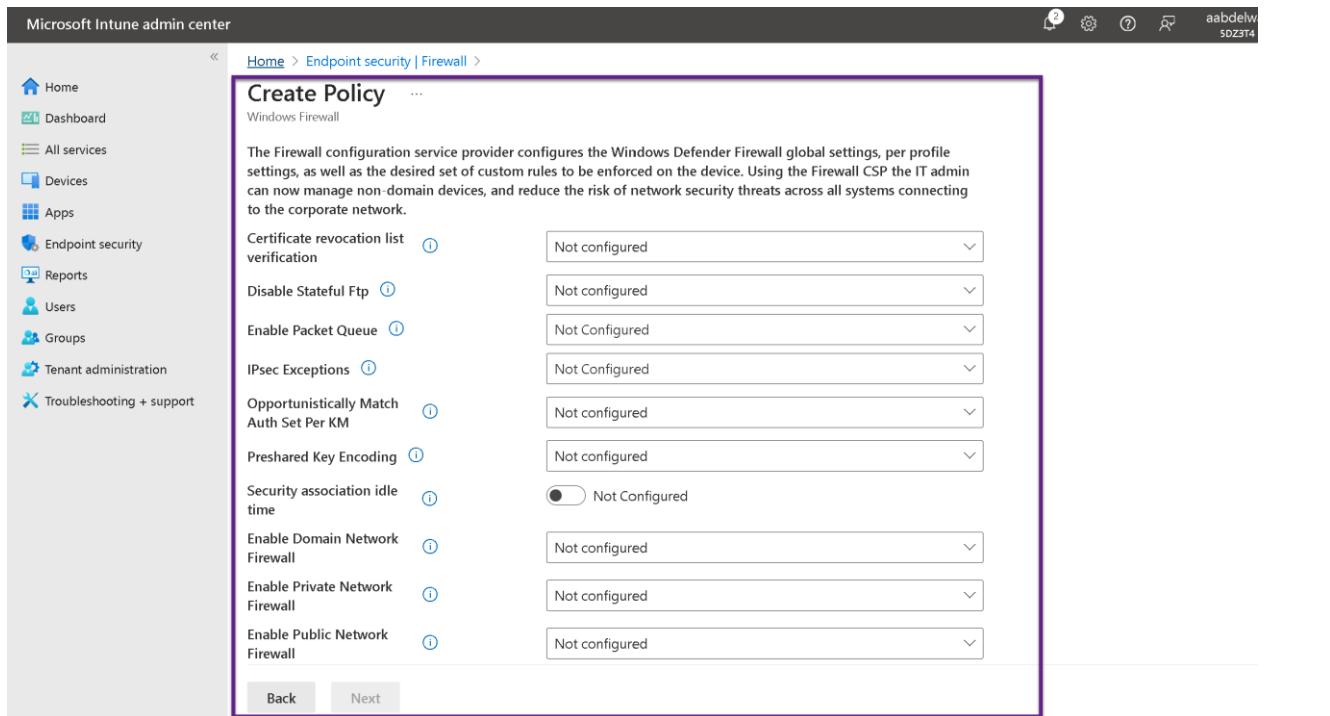
Last refreshed on: 12/13/2024

Devices with firewall turned 0

MDM devices running Wi...

Firewall policies + Create Policy Refresh

Complete Security with Microsoft Defender



The Firewall configuration service provider configures the Windows Defender Firewall global settings, per profile settings, as well as the desired set of custom rules to be enforced on the device. Using the Firewall CSP the IT admin can now manage non domain devices, and reduce the risk of network security threats across all systems connecting to the corporate network.

Create Policy

Certificate revocation list verification: Not configured

Disable Stateful Ftp: Not configured

Enable Packet Queue: Not Configured

IPsec Exceptions: Not Configured

Opportunistically Match Auth Set Per KM: Not configured

Presharded Key Encoding: Not configured

Security association idle time: Not Configured

Enable Domain Network Firewall: Not configured

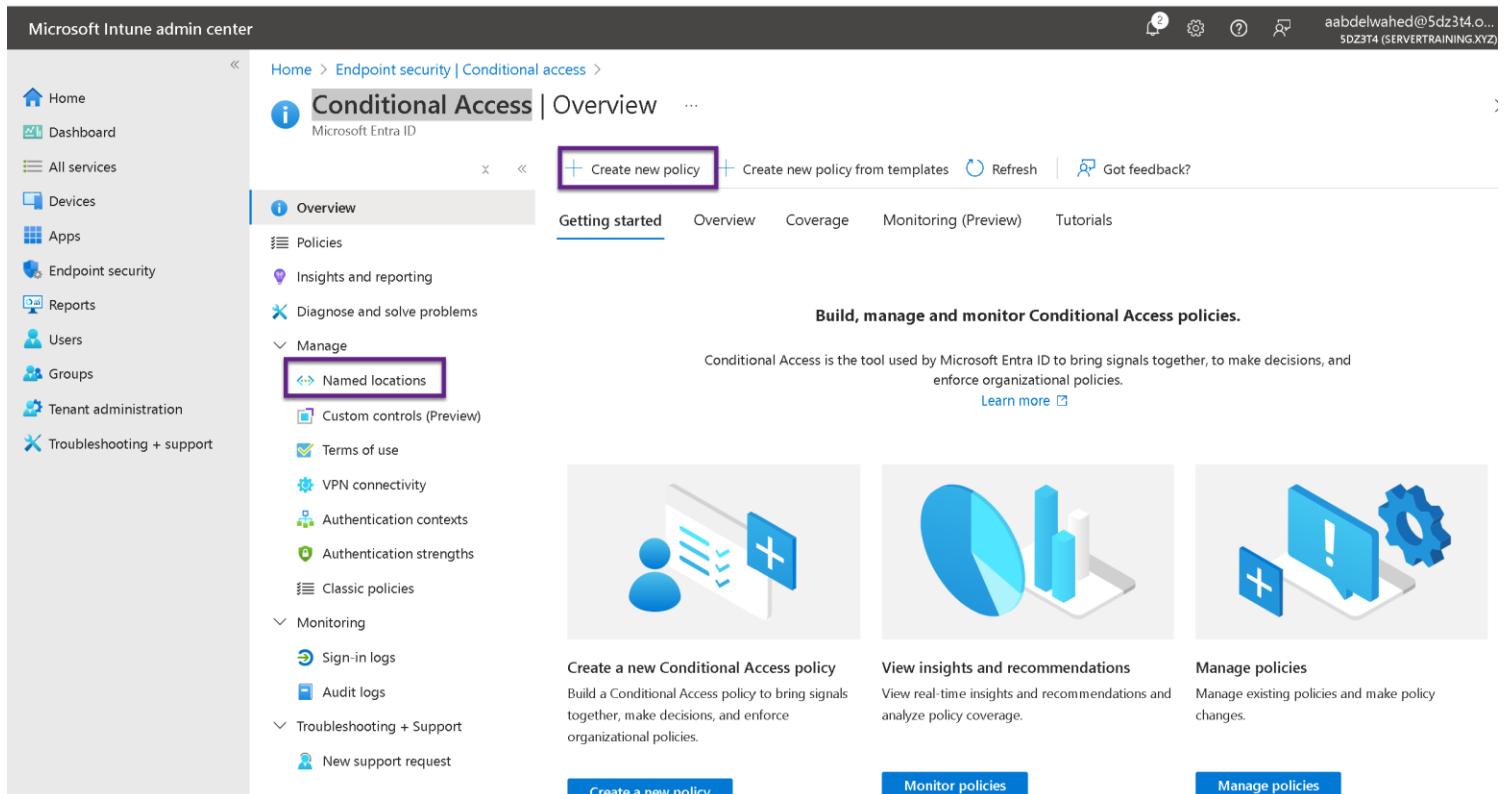
Enable Private Network Firewall: Not configured

Enable Public Network Firewall: Not configured

Back **Next**

Conditional Access

The **Conditional Access** feature in the **Microsoft Intune Admin Center**, allows you to enforce organizational policies by requiring specific conditions to be met before granting or denying access to resources. For example, restrict access based on location.



Conditional Access | Overview

Create new policy **Create new policy from templates** **Refresh** **Got feedback?**

Overview **Getting started** **Overview** **Coverage** **Monitoring (Preview)** **Tutorials**

Named locations

Custom controls (Preview) **Terms of use** **VPN connectivity** **Authentication contexts** **Authentication strengths**

Classic policies

Sign-in logs **Audit logs**

Troubleshooting + Support

New support request

Build, manage and monitor Conditional Access policies.

Conditional Access is the tool used by Microsoft Entra ID to bring signals together, to make decisions, and enforce organizational policies.

Create a new Conditional Access policy

Build a Conditional Access policy to bring signals together, make decisions, and enforce organizational policies.

Create a new policy

View insights and recommendations

View real-time insights and recommendations and analyze policy coverage.

Monitor policies

Manage policies

Microsoft Defender for Identity

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection or Azure ATP) is a cloud-based security solution designed to help protect your on-premises Active Directory (AD) environment and identify potential threats, compromised identities, and malicious insider actions.

Key Features of Microsoft Defender for Identity

1. Monitor Active Directory Activities

- Tracks and analyzes authentication traffic in your on-premises AD environment.
- Detects unusual user behavior, suspicious access attempts, and potential identity breaches.

2. Threat Detection

- Uses built-in machine learning and behavioral analytics to identify threats such as:
 - Pass-the-Ticket attacks.
 - Pass-the-Hash attacks.
 - Reconnaissance activities (e.g., LDAP enumeration).
 - Brute force and unusual sign-in patterns.

3. Entity Tagging

- **Sensitive Accounts:** Tag privileged or high-risk accounts (e.g., domain admins) to monitor closely.
- **Honeypot Accounts:** Deploy decoy accounts to detect attackers.

4. Integration with Defender Suite

- Integrates seamlessly with Microsoft Defender for Endpoint and other Microsoft Defender products to provide unified incident response capabilities.

5. Alerting and Reporting

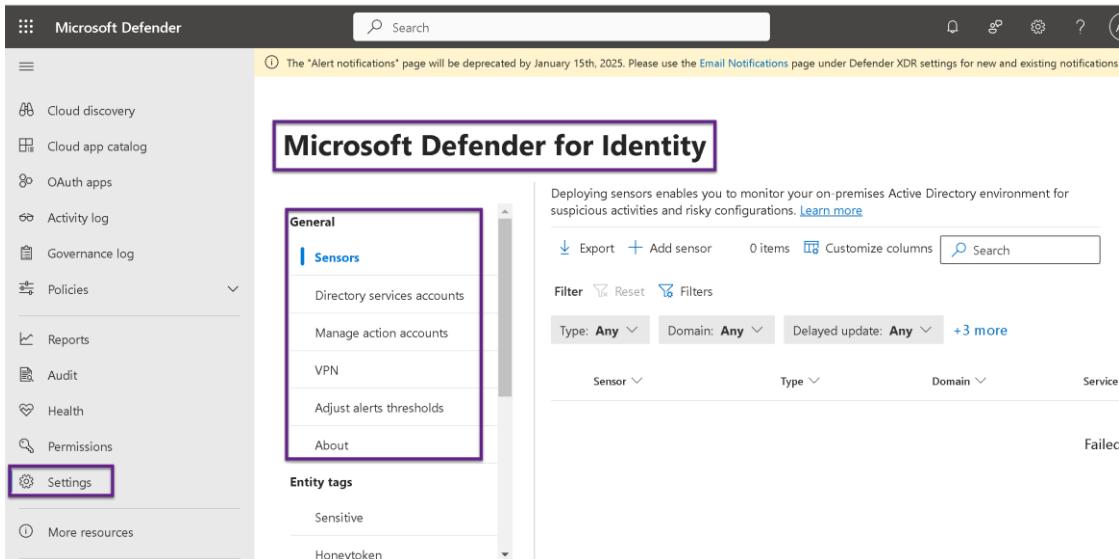
- Generates real-time alerts for detected threats or suspicious activities.
- Provides detailed forensic reports for security investigations.

6. VPN Integration

- Monitors and correlates VPN sign-in data to detect suspicious remote access patterns.

7. Risk Assessment

- Assesses risky configurations in your AD environment and provides actionable recommendations to improve security.



The screenshot shows the Microsoft Defender for Identity interface. The left sidebar includes options like Cloud discovery, Cloud app catalog, OAuth apps, Activity log, Governance log, Policies, Reports, Audit, Health, Permissions, and Settings (which is highlighted with a purple box). The main content area is titled 'Microsoft Defender for Identity' and contains a 'General' section with 'Sensors' as the active tab. Other options in this section include Directory services accounts, Manage action accounts, VPN, Adjust alerts thresholds, and About. Below this is an 'Entity tags' section with 'Sensitive' and 'Honeytoken' listed. The right side of the interface shows a table with columns for Sensor, Type, Domain, and Service, with one row showing 'Failed' under the Service column. At the top of the main content area, there is a message about alert notifications being deprecated and a link to the Email Notifications page. There are also buttons for Export, Add sensor, and Search.

Complete Security with Microsoft Defender

The **Action Center** in **Microsoft Defender** provides a centralized location for security teams to manage and respond to alerts and incidents across various Defender products, such as Defender for Endpoint, Defender for Identity, Defender for Office 365, and Defender for Cloud Apps. It is designed to streamline workflows, prioritize actions, and ensure effective incident resolution.

Key Features of the Action Center

1. Centralized Incident Management

- Consolidates alerts and incidents from different Defender solutions into a single dashboard.
- Provides a unified view to track and resolve security issues efficiently.

2. Automated Investigation and Remediation (AIR)

- Investigates alerts automatically using AI and machine learning.
- Suggests or takes automated actions like isolating devices, terminating processes, or blocking malicious URLs.

3. Manual Action Approval

- Displays recommended actions that require manual approval.
- Example: Approving the removal of a suspicious file or applying a configuration change.

4. Prioritized Alerts

- Categorizes alerts by severity (e.g., High, Medium, Low) to help focus on critical issues first.
- Groups related alerts into incidents for better context and prioritization.

5. Incident Timeline and Context

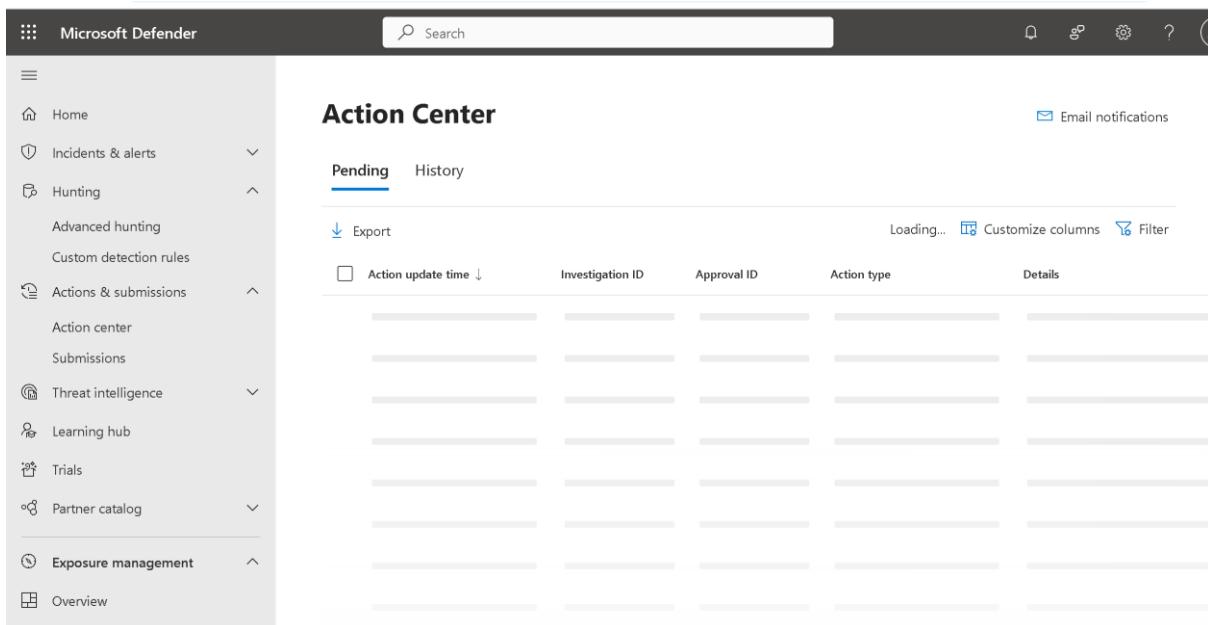
- Provides a detailed timeline of events leading to the alert.
- Displays affected users, devices, files, and applications to aid investigation.

6. Integration Across Defender Products

- Works seamlessly with Defender for Endpoint, Defender for Identity, Defender for Cloud Apps, and Defender for Office 365.
- Correlates alerts from different sources for comprehensive incident handling.

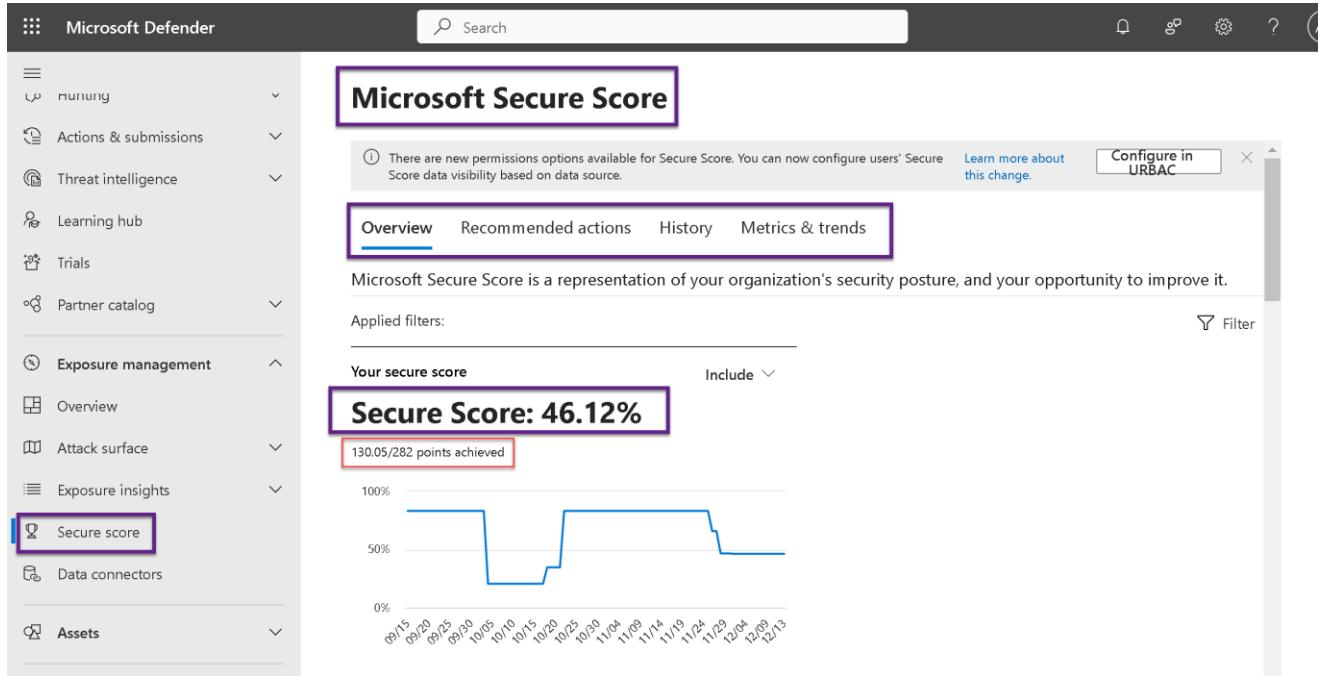
7. Audit and Reporting

- Tracks all actions taken (automated or manual) for compliance and reporting purposes.
- Provides insights into resolution times and trends.



Complete Security with Microsoft Defender

Microsoft Secure Score is a measurement of an organization's security posture in Microsoft 365, Azure, and other integrated environments. It provides actionable recommendations to improve the overall security of your organization.



The screenshot shows the Microsoft Defender interface with the 'Secure score' option highlighted in the left sidebar. The main dashboard is titled 'Microsoft Secure Score' and displays the following information:

- Secure Score: 46.12%** (highlighted with a red box)
130.05/282 points achieved
- A line chart showing the Secure Score trend over time, starting at 100% on 09/15 and fluctuating between 50% and 100% through December.
- Applied filters:** A 'Filter' button is available.
- Overview** (highlighted with a blue box) is the active tab, followed by Recommended actions, History, and Metrics & trends.
- A notification bar at the top right indicates new permissions options for Secure Score, with a 'Learn more about this change' link and a 'Configure in URBAC' button.
- The left sidebar includes sections for Running, Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, Attack surface, Exposure insights, Assets, and Secure score (highlighted with a purple box).

Microsoft Entra ID Protection

Microsoft Entra ID Protection is a cloud-based security solution within **Microsoft Entra**. It helps organizations identify, detect, and mitigate identity-related risks by leveraging AI and machine learning to protect users and workloads.

Key Features of Microsoft Entra ID Protection

1. Risk-Based Identity Protection

- Detects risky behaviors and compromised credentials by analyzing authentication events and user activities.
- Uses **real-time risk signals** to classify risk into:
 - **User Risk**: Indicates the likelihood that a user's identity is compromised.
 - **Sign-In Risk**: Highlights suspicious or unusual sign-in attempts.
 - **Workload Identity Risk**: Monitors service accounts and workload identities.

2. Risk Detection

- Provides alerts on risks such as:
 - **Impossible Travel**: User logs in from geographically distant locations within a short time.
 - **Sign-ins from Anonymous IPs**: Logins originating from TOR or VPNs.
 - **Leaked Credentials**: Detects credentials exposed in public data breaches.
 - **Malware-Linked IPs**: Identifies logins from IPs associated with malicious activity.

3. Risk Remediation Policies

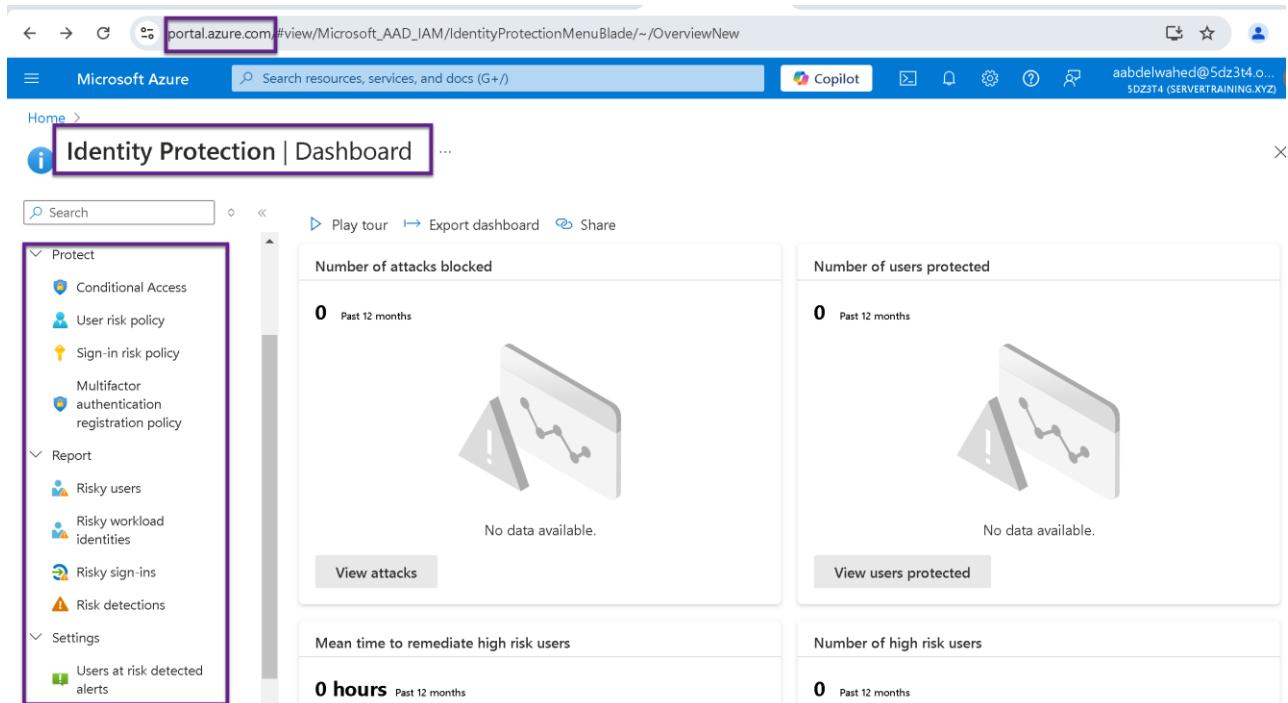
- Enables automatic responses to detected risks using **User Risk Policies** and **Sign-In Risk Policies**:
 - Force **password reset** for compromised accounts.
 - Require **multi-factor authentication (MFA)** for high-risk sign-ins.
 - Block access based on certain conditions.

4. Detailed Reporting Tracks:

- **Risky Users**: Lists all users flagged for risky behavior.
- **Risky Sign-Ins**: Shows all sign-ins categorized as high or medium risk.
- **Risky Workload Identities**: Highlights potential risks for service accounts and apps.

5. Integration with Conditional Access

- Works seamlessly with **Conditional Access Policies** to enforce stricter controls for risky users or sign-ins.



Identity Protection | Dashboard

Number of attacks blocked: 0 Past 12 months

Number of users protected: 0 Past 12 months

Mean time to remediate high risk users: 0 hours Past 12 months

Number of high risk users: 0 Past 12 months

Number of users at risk detected alerts: 0 Past 12 months

The **Advanced Hunting** feature in **Microsoft Defender** is a powerful query-based threat hunting tool that allows security analysts to proactively search for security threats, anomalies, and malicious behaviors across an organization's environment. It enables deep investigation using data collected by Microsoft Defender services.

Key Features of Advanced Hunting

1. Query-Based Threat Hunting

- Uses **KQL (Kusto Query Language)** to craft and execute custom queries.
- Searches data sources such as device events, network traffic, identity activities, and cloud activity logs.

2. Built-In Schema

- Provides predefined tables and fields (e.g., DeviceEvents, IdentityInfo, EmailEvents) for easy access to data.
- Example: The query in the screenshot uses the IdentityInfo schema to summarize account activities over the last 14 days.

3. Custom Detection Rules

- Queries can be converted into **custom detection rules** to automate threat detection.
- Example: Set alerts if specific suspicious activities are identified.

4. Integration Across Defender Products

- Correlates signals from **Defender for Endpoint**, **Defender for Identity**, **Defender for Cloud**, and **Defender for Office 365** for a comprehensive view.

5. Visualization and Insights

- Allows exporting query results and visualizing them for deeper analysis.
- Supports creating dashboards in tools like Microsoft Sentinel or Power BI.

6. Collaboration and Sharing

- Share queries across teams or save them for future investigations.
- Use **query templates** provided by Microsoft for common hunting scenarios.

Use Case Scenarios

1. Detect Anomalous Logins

```
IdentityInfo | where Timestamp > ago(7d) | where AccountObjectId != "expected_admin_account_id" | summarize count() by AccountDisplayName, IPAddress | order by count_ desc
```

- Purpose: Identify suspicious login patterns, such as logins from unexpected IPs or accounts.

2. Investigate Malware Activity

```
DeviceFileEvents | where FileName endswith ".exe" and FileSize > 5000000 | summarize count() by FileName, DeviceName
```

- Purpose: Detect large executable files being dropped or executed.

3. Monitor Identity Threats

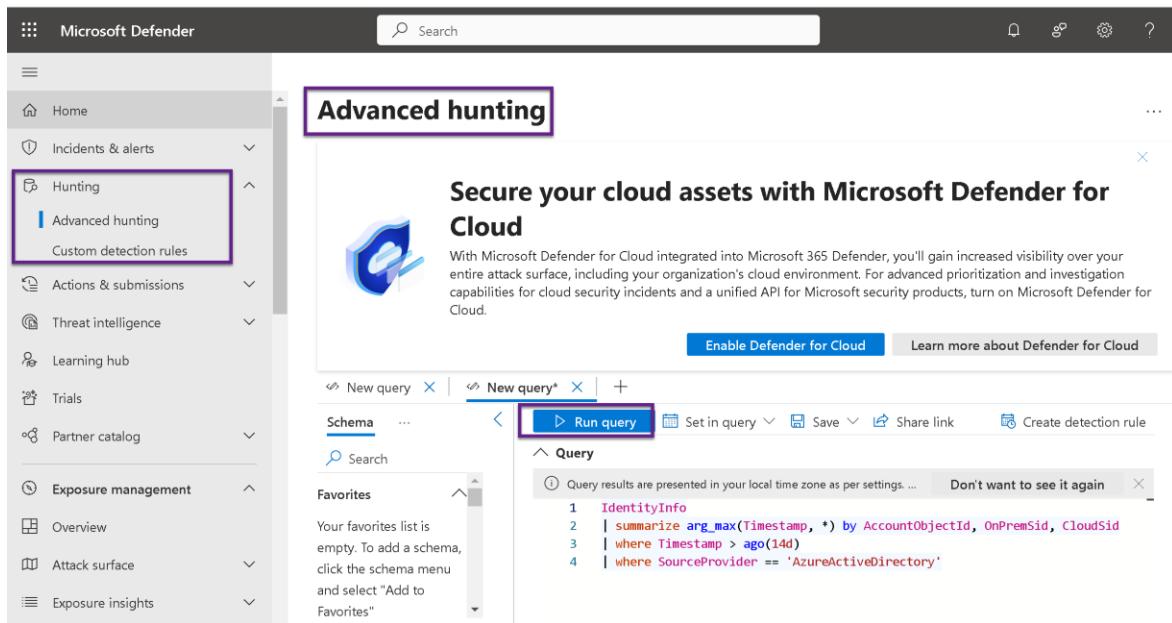
```
IdentityInfo | where Timestamp > ago(14d) | where SourceProvider == 'AzureActiveDirectory' | summarize arg_max(Timestamp, *) by AccountObjectId, OnPremSid, CloudSid
```

- Purpose: Monitor identity activities from Azure AD for potential threats.

4. Identifying attachments with specific patterns in their names

```
EmailAttachmentInfo | where FileName contains "data"
```

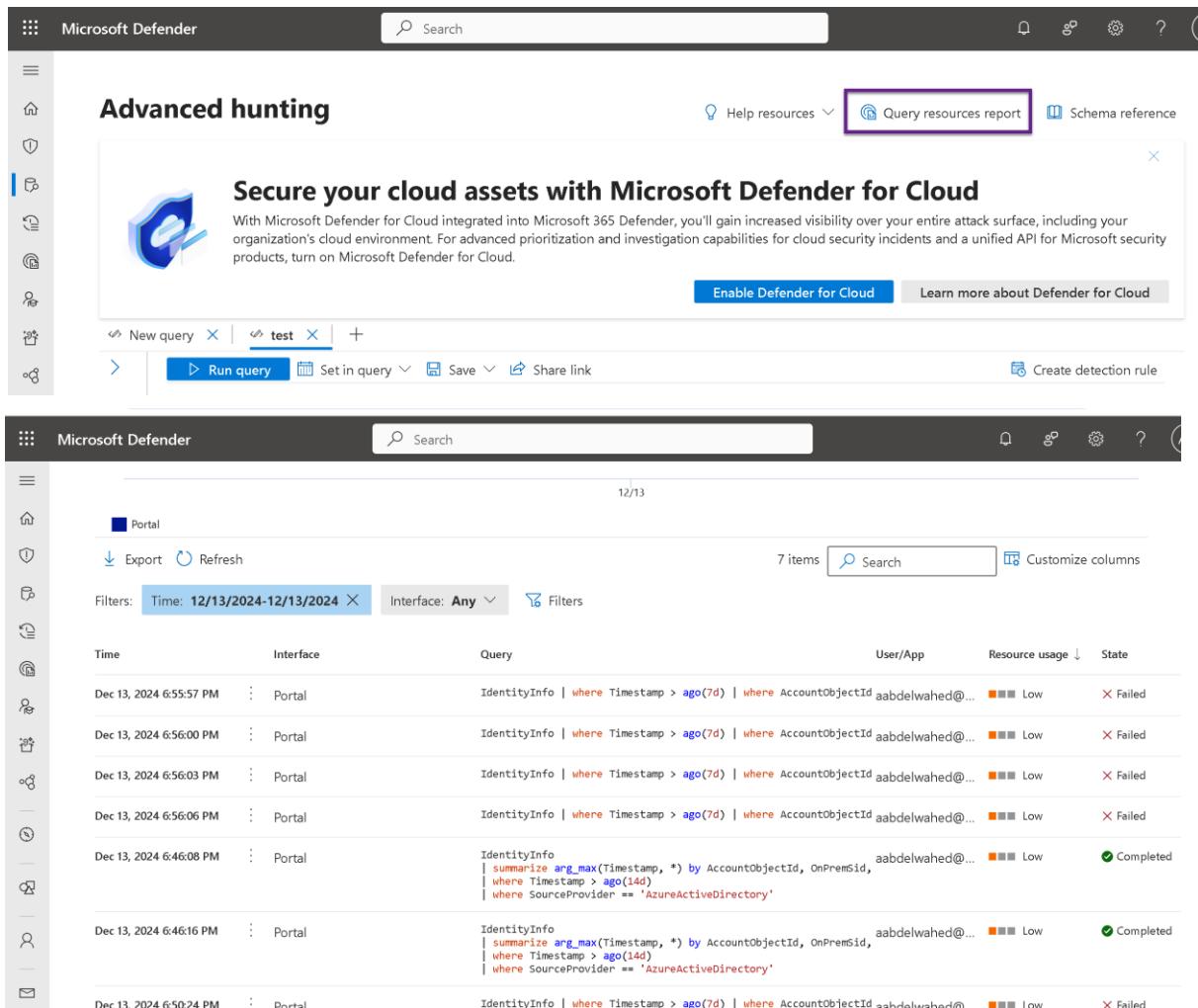
Complete Security with Microsoft Defender



The screenshot shows the Microsoft Defender interface with the 'Advanced hunting' section selected in the sidebar. The main area displays a 'Secure your cloud assets with Microsoft Defender for Cloud' card. Below it is a query editor with a 'Run query' button highlighted. The query itself is:

```
1 IdentityInfo
2 | summarize arg_max(Timestamp, *) by AccountObjectId, OnPremSid, CloudSid
3 | where Timestamp > ago(14d)
4 | where SourceProvider == 'AzureActiveDirectory'
```

To see the result



The screenshot shows the Microsoft Defender interface with the 'Advanced hunting' section selected. The main area displays a 'Secure your cloud assets with Microsoft Defender for Cloud' card. Below it is a query editor with a 'Run query' button highlighted. The results of the query are displayed in a table:

Time	Interface	Query	User/App	Resource usage	State
Dec 13, 2024 6:55:57 PM	Portal	IdentityInfo where Timestamp > ago(7d) where AccountObjectId aabdelwahed@...	aabdelwahed@...	Low	Failed
Dec 13, 2024 6:56:00 PM	Portal	IdentityInfo where Timestamp > ago(7d) where AccountObjectId aabdelwahed@...	aabdelwahed@...	Low	Failed
Dec 13, 2024 6:56:03 PM	Portal	IdentityInfo where Timestamp > ago(7d) where AccountObjectId aabdelwahed@...	aabdelwahed@...	Low	Failed
Dec 13, 2024 6:56:06 PM	Portal	IdentityInfo where Timestamp > ago(7d) where AccountObjectId aabdelwahed@...	aabdelwahed@...	Low	Failed
Dec 13, 2024 6:46:08 PM	Portal	IdentityInfo summarize arg_max(Timestamp, *) by AccountObjectId, OnPremSid, aabdelwahed@..., where Timestamp > ago(14d) where SourceProvider == 'AzureActiveDirectory'	aabdelwahed@...	Low	Completed
Dec 13, 2024 6:46:16 PM	Portal	IdentityInfo summarize arg_max(Timestamp, *) by AccountObjectId, OnPremSid, aabdelwahed@..., where Timestamp > ago(14d) where SourceProvider == 'AzureActiveDirectory'	aabdelwahed@...	Low	Completed
Dec 13, 2024 6:50:24 PM	Portal	IdentityInfo where Timestamp > ago(7d) where AccountObjectId aabdelwahed@...	aabdelwahed@...	Low	Failed

Microsoft Defender for Cloud

Microsoft Defender for Cloud is a comprehensive security management and threat protection service offered by Microsoft Azure. It provides tools to strengthen the security posture of cloud workloads, protect hybrid environments, and detect and respond to threats in real-time.

Key Features of Microsoft Defender for Cloud

1. Cloud Security Posture Management (CSPM)

- **Secure Score:**
 - Evaluates your cloud environment's security posture and provides a score based on applied security controls.
 - Offers actionable recommendations to improve security.
- **Compliance Assessments:**
 - Continuously assesses your environment against industry-standard regulatory frameworks like ISO 27001, PCI DSS, and NIST.
- **Asset Visibility:**
 - Provides an inventory of resources across Azure, AWS, and Google Cloud with their security states.

2. Cloud Workload Protection Platform (CWPP)

- Protects workloads running across Azure, AWS, Google Cloud, and on-premises:
 - **Virtual Machines (VMs):**
 - Monitors OS configurations, vulnerabilities, and unauthorized access.
 - **Containers:**
 - Scans container images for vulnerabilities and ensures secure configurations.
 - **Databases:**
 - Monitors Azure SQL, Cosmos DB, and other databases for security misconfigurations.
 - **Storage:**
 - Detects malware and suspicious access patterns in storage accounts.

3. Threat Protection

- **Real-Time Threat Detection:**
 - Identifies malicious activities such as brute force attacks, SQL injection attempts, and suspicious file uploads.
- **Alerts and Recommendations:**
 - Provides actionable insights and step-by-step remediation guidance for detected threats.
- **Advanced Threat Detection:**
 - Leverages AI, machine learning, and threat intelligence to detect unknown threats.

4. Hybrid and Multicloud Security

- Supports **Azure Arc** to extend security features to on-premises and non-Azure environments (e.g., AWS, GCP).
- Offers unified security management for resources across hybrid environments.

5. Integration with Security Tools

- Integrates with **Microsoft Sentinel** for advanced security orchestration, automation, and threat hunting.
- Works seamlessly with other Microsoft Defender services (e.g., Defender for Endpoint, Defender for Identity).

Complete Security with Microsoft Defender

Core Components

1. Secure Score

- Provides a quantitative measure of your environment's security posture.
- Recommends improvements like enabling firewalls, applying encryption, or updating VMs.

2. Regulatory Compliance

- Maps resources to compliance controls.
- Flags compliance gaps and suggests remediation actions.

3. Advanced Threat Protection

- Offers protection for:
 - App Services:** Protects Azure App Service applications.
 - Key Vaults:** Monitors access to sensitive secrets.
 - AKS (Azure Kubernetes Services):** Ensures secure configurations and detects vulnerabilities in Kubernetes clusters.

4. Workflow Automation

- Automates responses to threats using Logic Apps (e.g., isolate VMs, send alerts to teams, or open tickets in ServiceNow).

Use Cases

1. Strengthening Cloud Security Posture

- Continuously monitor cloud resources for vulnerabilities, misconfigurations, and policy violations.
- Example: Identify VMs with outdated OS versions and apply security patches.

2. Threat Detection and Response

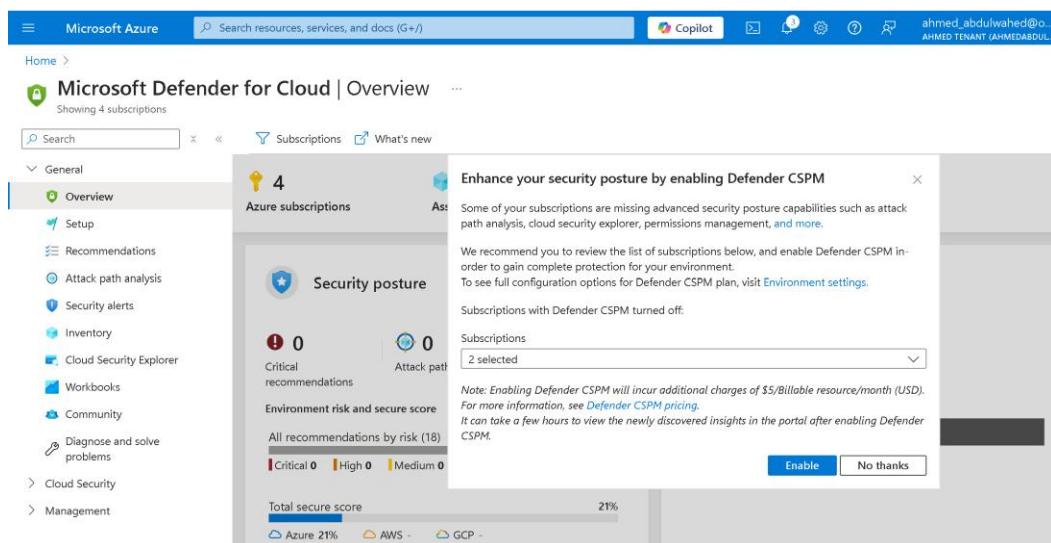
- Detects brute force attacks, unusual data exfiltration, and ransomware activity.
- Example: Monitor Azure SQL for suspicious query patterns.

3. Compliance Management

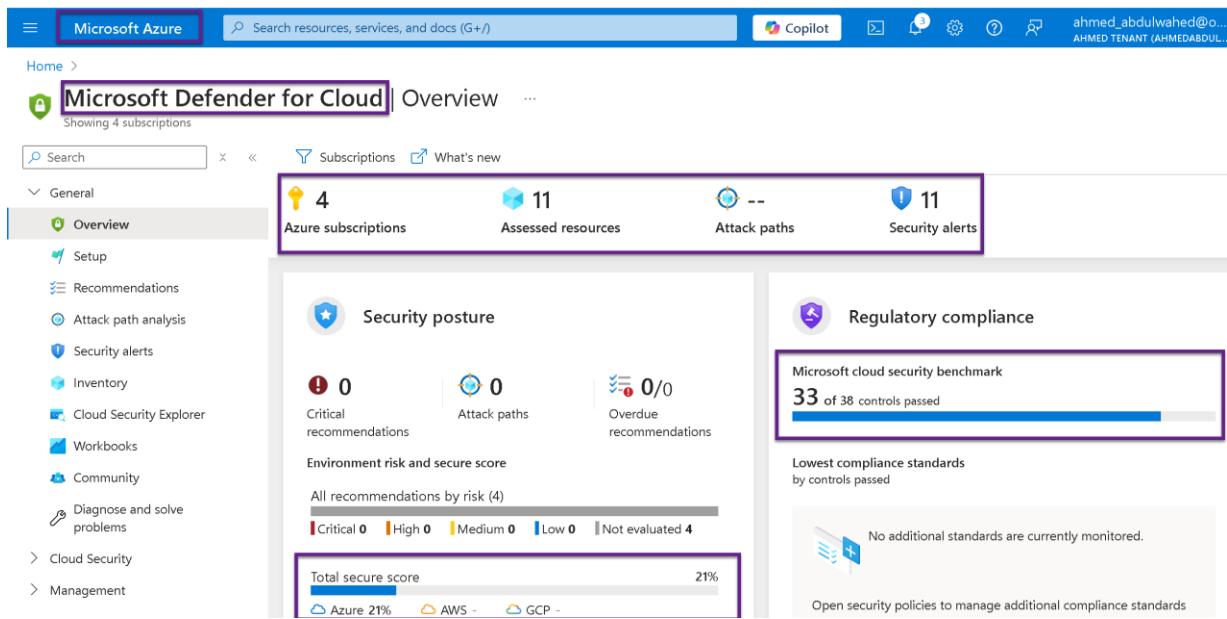
- Ensure your cloud environment adheres to compliance standards like HIPAA or GDPR.
- Example: Map compliance controls to Azure policies for automatic enforcement.

4. Hybrid Security

- Extend security monitoring to on-premises workloads and non-Azure clouds.
- Example: Use Azure Arc to protect AWS EC2 instances with Microsoft Defender.

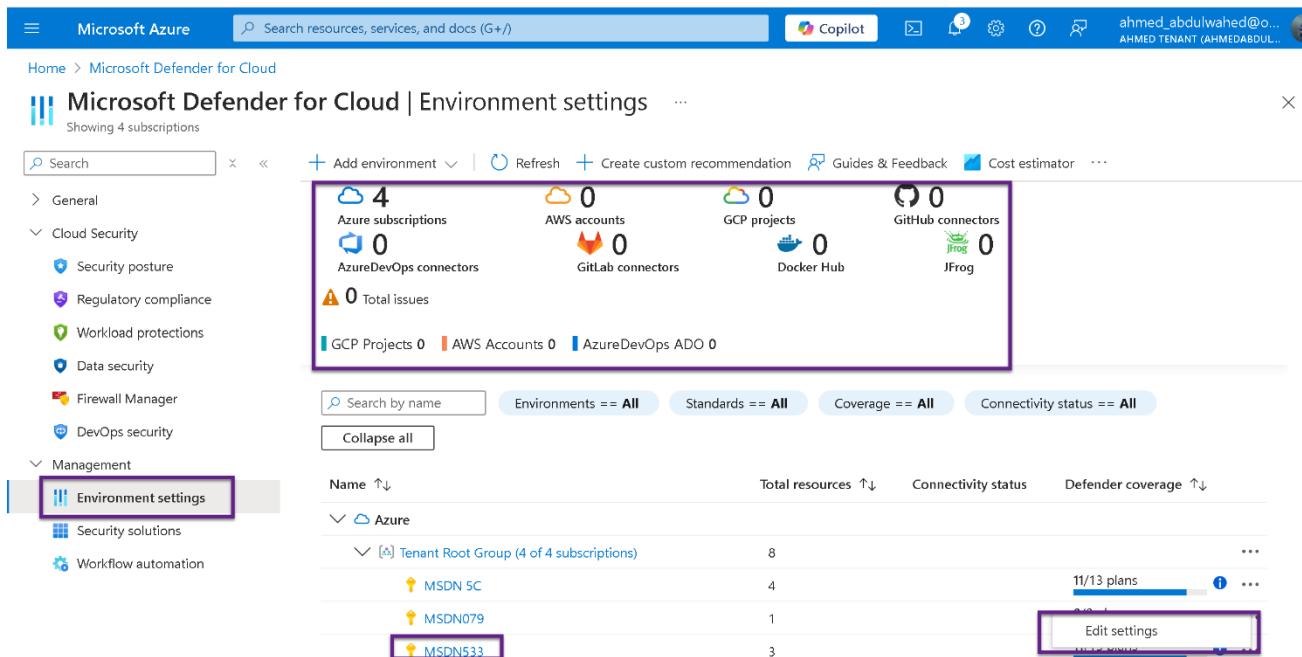


Complete Security with Microsoft Defender



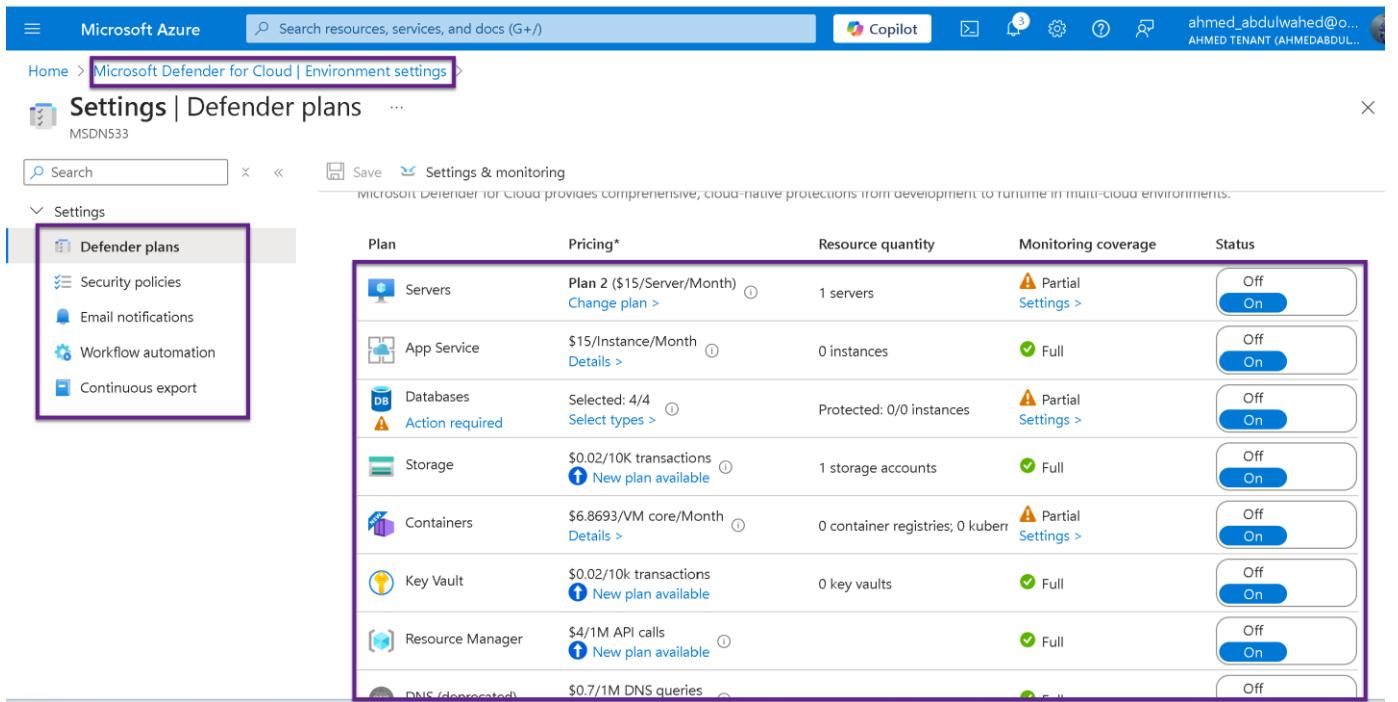
The screenshot shows the Microsoft Defender for Cloud Overview page. At the top, there are four key metrics: 4 Azure subscriptions, 11 Assessed resources, 11 Attack paths, and 11 Security alerts. Below these, the 'Security posture' section displays 0 Critical recommendations, 0 Attack paths, and 0/0 Overdue recommendations. It also shows the 'Environment risk and secure score' with a total score of 21% (Azure 21%, AWS 0%, GCP 0%). The 'Regulatory compliance' section shows a Microsoft cloud security benchmark with 33 of 38 controls passed. The page also includes sections for Cloud Security and Management.

The **Environment Settings** page in **Microsoft Defender for Cloud** is where you configure and manage the security settings and integrations for your cloud environments, including Azure, AWS, Google Cloud (GCP), and other resources. This section provides a comprehensive overview of your environment's security posture, resource coverage, and connected third-party integrations.



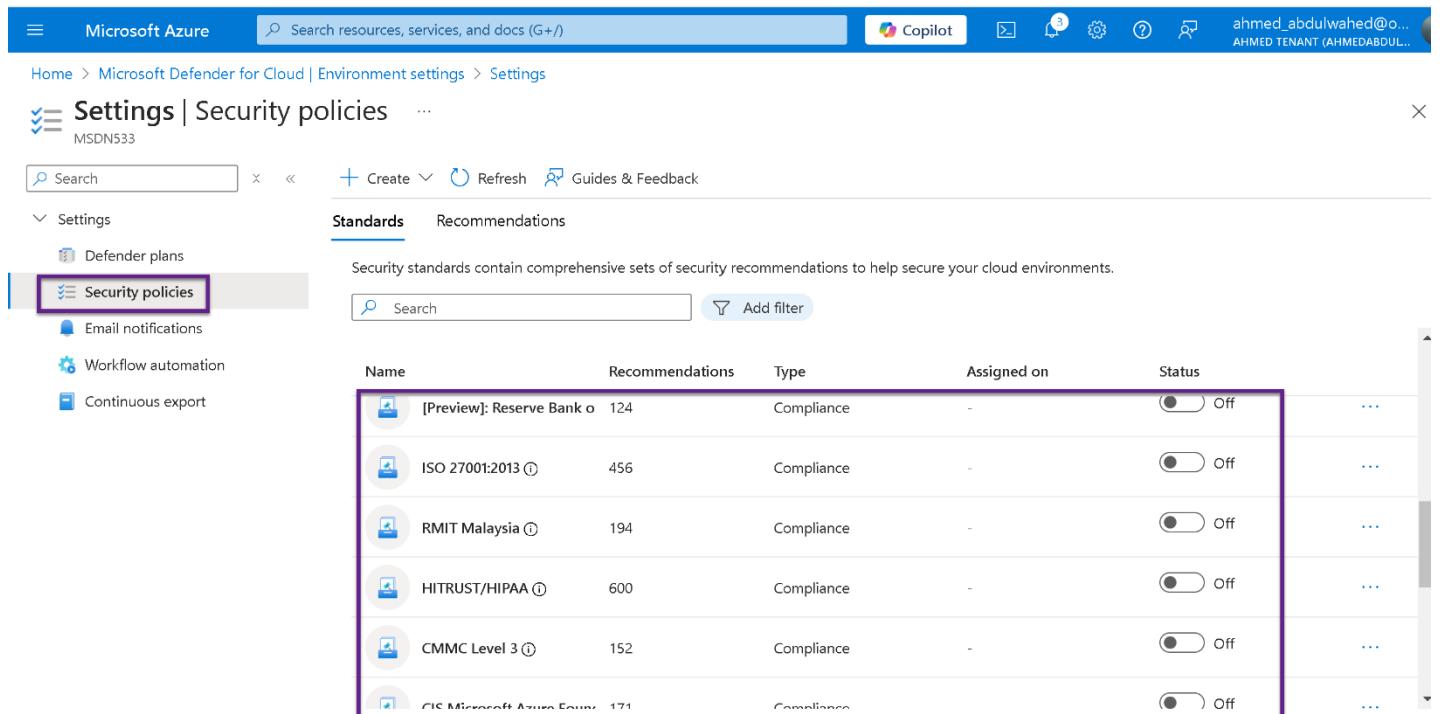
The screenshot shows the Microsoft Defender for Cloud Environment settings page. The left sidebar includes sections for General, Cloud Security (Security posture, Regulatory compliance, Workload protections, Data security, Firewall Manager, DevOps security), Management (Environment settings, Security solutions, Workflow automation), and a 'Showing 4 subscriptions' section. The main area displays connectivity status for various services: 4 Azure subscriptions, 0 AWS accounts, 0 GCP projects, 0 GitHub connectors, 0 AzureDevOps connectors, 0 GitLab connectors, 0 Docker Hub, and 0 JFrog. It also shows 0 Total issues. Below this, there are filters for 'Search by name', 'Environments == All', 'Standards == All', 'Coverage == All', and 'Connectivity status == All'. The 'Collapse all' button is also present. The 'Environment settings' section is highlighted with a purple box. The 'Edit settings' button for the 'MSDN533' resource is also highlighted with a purple box.

Complete Security with Microsoft Defender



The screenshot shows the Microsoft Azure Defender plans settings page. The left sidebar is titled 'Settings' and has a sub-section 'Defender plans' highlighted with a purple box. The main table lists various resource types with their monitoring coverage and status (Off or On). The table columns are: Plan, Pricing*, Resource quantity, Monitoring coverage, and Status.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 (\$15/Server/Month) Change plan >	1 servers	⚠ Partial Settings >	Off On
App Service	\$15/Instance/Month Details >	0 instances	✓ Full	Off On
Databases	Selected: 4/4 Select types >	Protected: 0/0 instances	⚠ Partial Settings >	Off On
Storage	\$0.02/10K transactions New plan available	1 storage accounts	✓ Full	Off On
Containers	\$6.8693/VM core/Month Details >	0 container registries; 0 kuber	⚠ Partial Settings >	Off On
Key Vault	\$0.02/10k transactions New plan available	0 key vaults	✓ Full	Off On
Resource Manager	\$4/1M API calls New plan available		✓ Full	Off On
DNS (deprecated)	\$0.7/1M DNS queries		✓ Full	Off



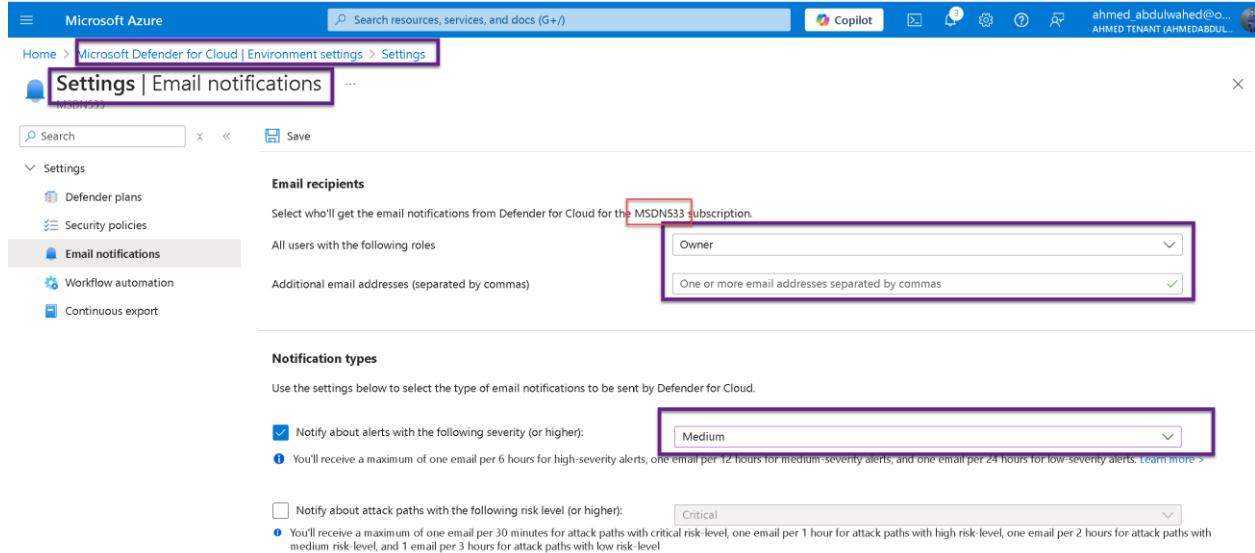
The screenshot shows the Microsoft Azure Security policies settings page. The left sidebar is titled 'Settings' and has a sub-section 'Security policies' highlighted with a purple box. The main table lists various security standards with their assigned status (Off). The table columns are: Name, Recommendations, Type, Assigned on, and Status.

Name	Recommendations	Type	Assigned on	Status
[Preview]: Reserve Bank	124	Compliance	-	Off
ISO 27001:2013	456	Compliance	-	Off
RMIT Malaysia	194	Compliance	-	Off
HITRUST/HIPAA	600	Compliance	-	Off
CMMC Level 3	152	Compliance	-	Off
CIS Microsoft Azure Edition	171	Compliance	-	Off

Complete Security with Microsoft Defender

Email notifications

- By default, email notifications are sent only for **high-severity alerts**.
- To include **medium-severity alerts**, you need to modify the notification settings and select **Medium** as the minimum severity level.



Microsoft Azure

Search resources, services, and docs (G+/-)

Copilot

ahmed_abdulwahed@o... AHMED TENANT (AHMEDABDUL)

Home > Microsoft Defender for Cloud | Environment settings > Settings

Settings | Email notifications

Search Save

Settings

Defender plans

Security policies

Email notifications

Workflow automation

Continuous export

Email recipients

Select who'll get the email notifications from Defender for Cloud for the **MSDN533** subscription.

All users with the following roles

Owner

One or more email addresses separated by commas

Notification types

Use the settings below to select the type of email notifications to be sent by Defender for Cloud.

Notify about alerts with the following severity (or higher):

Medium

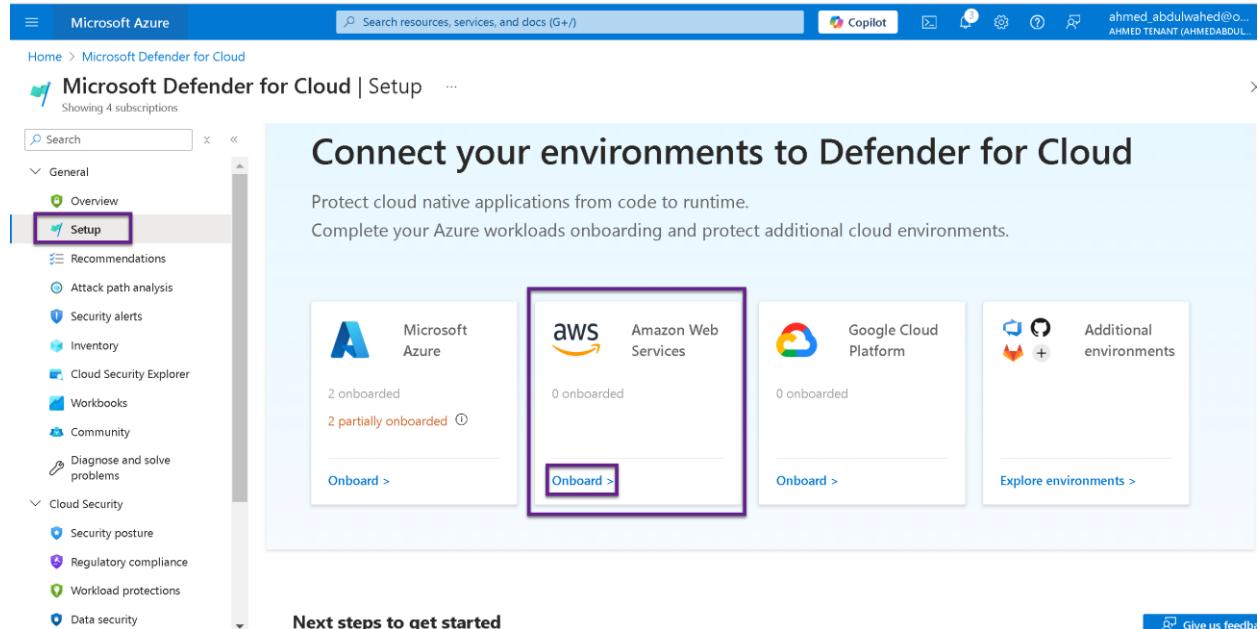
You'll receive a maximum of one email per 6 hours for high-severity alerts, one email per 12 hours for medium-severity alerts, and one email per 24 hours for low-severity alerts. [Learn more >](#)

Notify about attack paths with the following risk level (or higher):

Critical

You'll receive a maximum of one email per 30 minutes for attack paths with critical risk-level, one email per 1 hour for attack paths with high risk level, one email per 2 hours for attack paths with medium risk level, and 1 email per 3 hours for attack paths with low risk level. [Learn more >](#)

Microsoft Defender for AWS



Microsoft Azure

Search resources, services, and docs (G+/-)

Copilot

ahmed_abdulwahed@o... AHMED TENANT (AHMEDABDUL)

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Setup

Showing 4 subscriptions

Search

General

Overview

Setup

Recommendations

Attack path analysis

Security alerts

Inventory

Cloud Security Explorer

Workbooks

Community

Diagnose and solve problems

Cloud Security

Security posture

Regulatory compliance

Workload protections

Data security

Connect your environments to Defender for Cloud

Protect cloud native applications from code to runtime.

Complete your Azure workloads onboarding and protect additional cloud environments.

Microsoft Azure

2 onboarded

2 partially onboarded

Onboard >

aws

Amazon Web Services

0 onboarded

Onboard >

Google Cloud Platform

0 onboarded

Onboard >

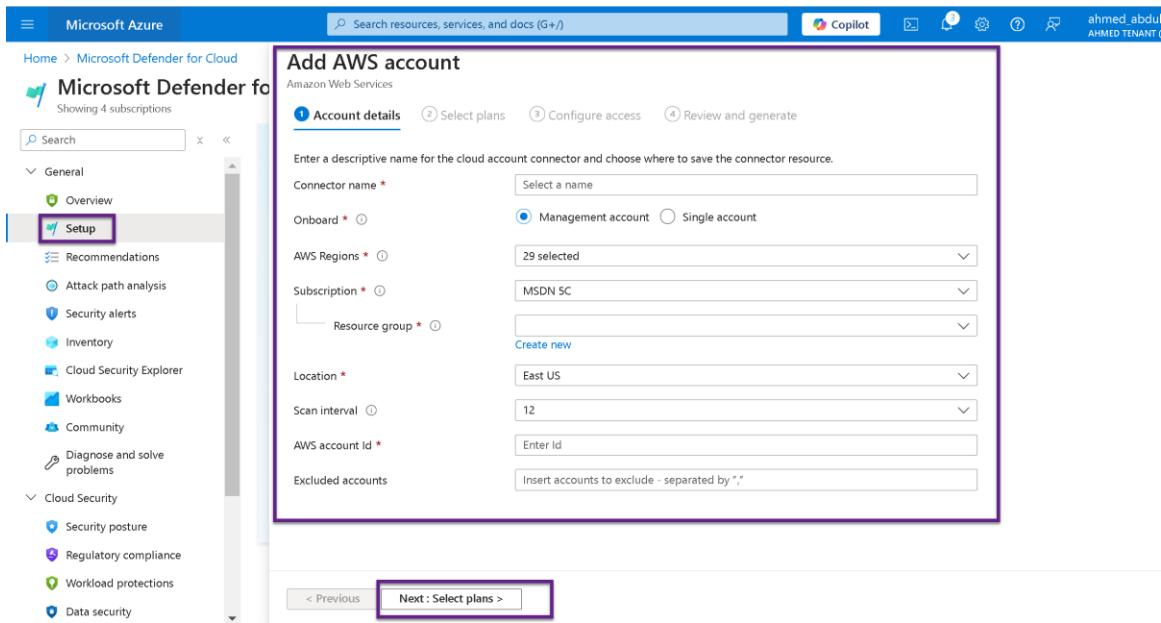
Additional environments

Explore environments >

Next steps to get started

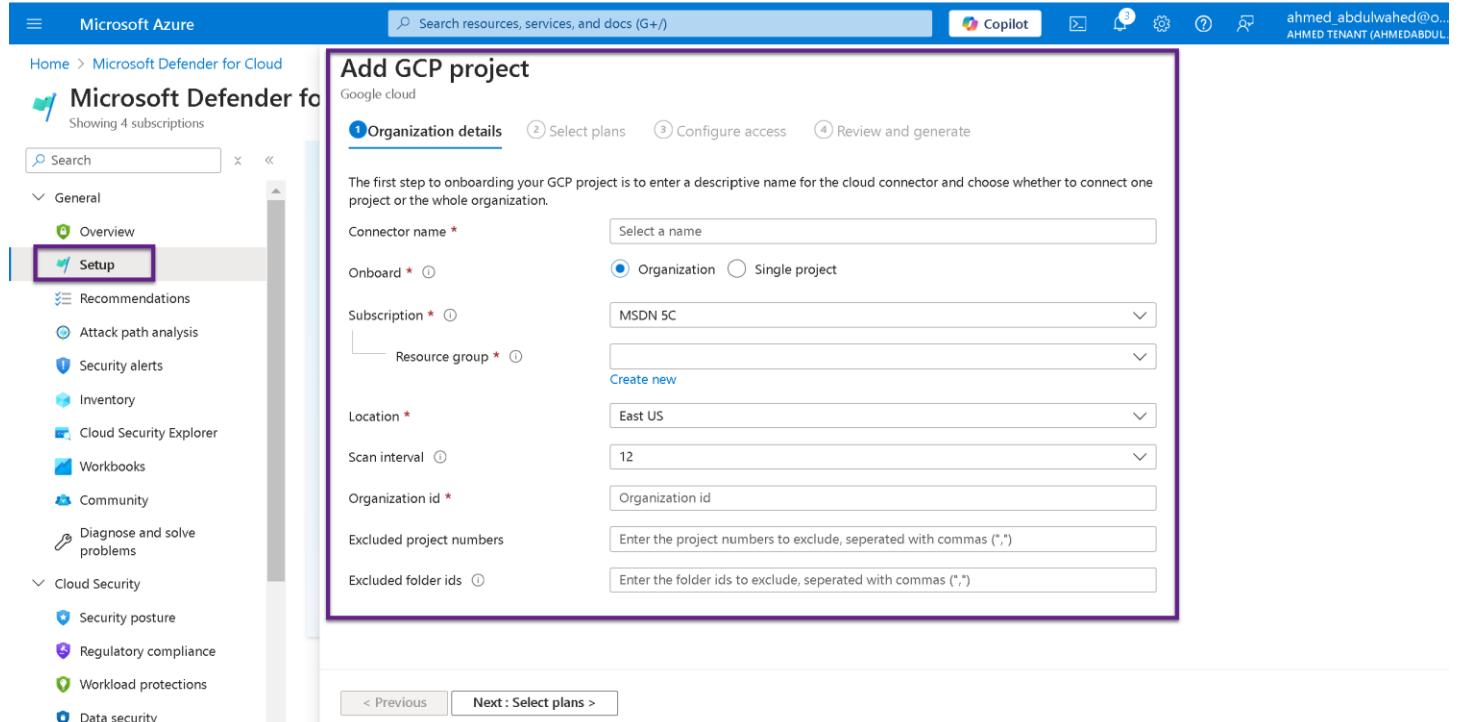
Give us feedback

Complete Security with Microsoft Defender



The screenshot shows the Microsoft Azure Microsoft Defender for Cloud interface. The left sidebar is titled 'Microsoft Defender for Cloud' and shows 'Showing 4 subscriptions'. The 'Setup' section is highlighted with a purple box. The main content area is titled 'Add AWS account' and is part of a four-step wizard: 1. Account details, 2. Select plans, 3. Configure access, 4. Review and generate. The 'Account details' step is active, showing fields for 'Connector name' (with a placeholder 'Select a name'), 'Onboard' (with 'Management account' selected), 'AWS Regions' (set to '29 selected'), 'Subscription' (set to 'MSDN 5C'), 'Resource group' (with a placeholder 'Create new'), 'Location' (set to 'East US'), 'Scan interval' (set to '12'), 'AWS account Id' (with a placeholder 'Enter Id'), and 'Excluded accounts' (with a placeholder 'Insert accounts to exclude - separated by ","'). At the bottom are 'Previous' and 'Next : Select plans >' buttons.

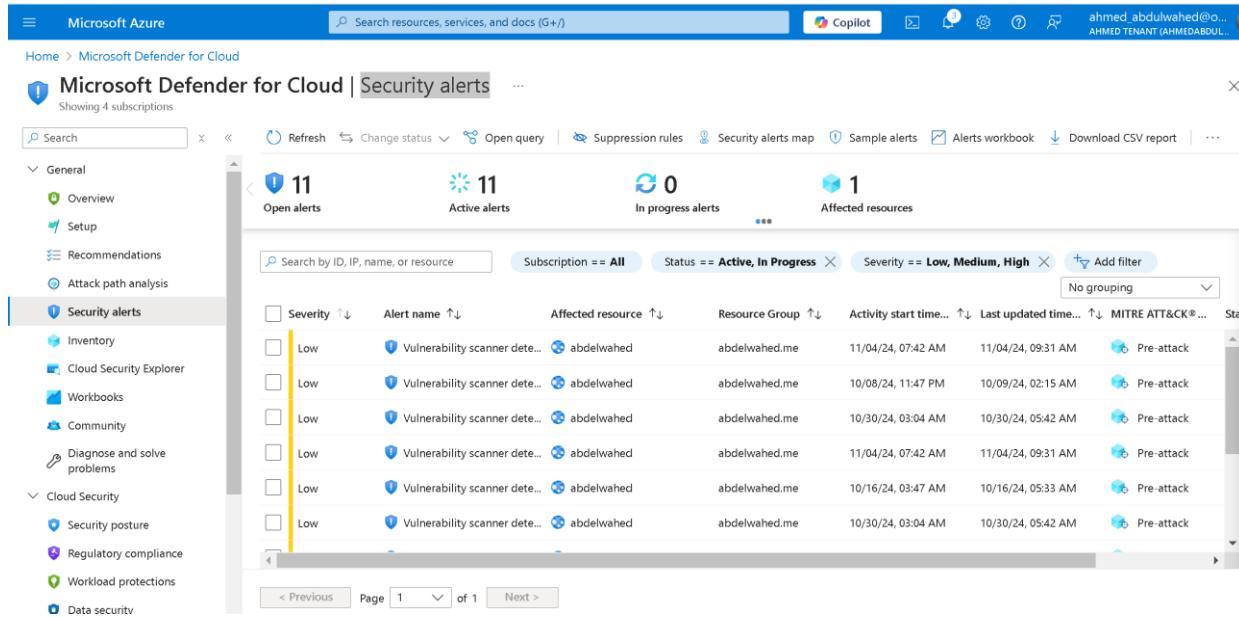
Microsoft Defender for GCP



The screenshot shows the Microsoft Azure Microsoft Defender for Cloud interface. The left sidebar is titled 'Microsoft Defender for Cloud' and shows 'Showing 4 subscriptions'. The 'Setup' section is highlighted with a purple box. The main content area is titled 'Add GCP project' and is part of a four-step wizard: 1. Organization details, 2. Select plans, 3. Configure access, 4. Review and generate. The 'Organization details' step is active, showing fields for 'Connector name' (with a placeholder 'Select a name'), 'Onboard' (with 'Organization' selected), 'Subscription' (set to 'MSDN 5C'), 'Resource group' (with a placeholder 'Create new'), 'Location' (set to 'East US'), 'Scan interval' (set to '12'), 'Organization id' (with a placeholder 'Organization id'), 'Excluded project numbers' (with a placeholder 'Enter the project numbers to exclude, separated with commas (",")'), and 'Excluded folder ids' (with a placeholder 'Enter the folder ids to exclude, separated with commas (",")'). At the bottom are 'Previous' and 'Next : Select plans >' buttons.

Complete Security with Microsoft Defender

Security alerts



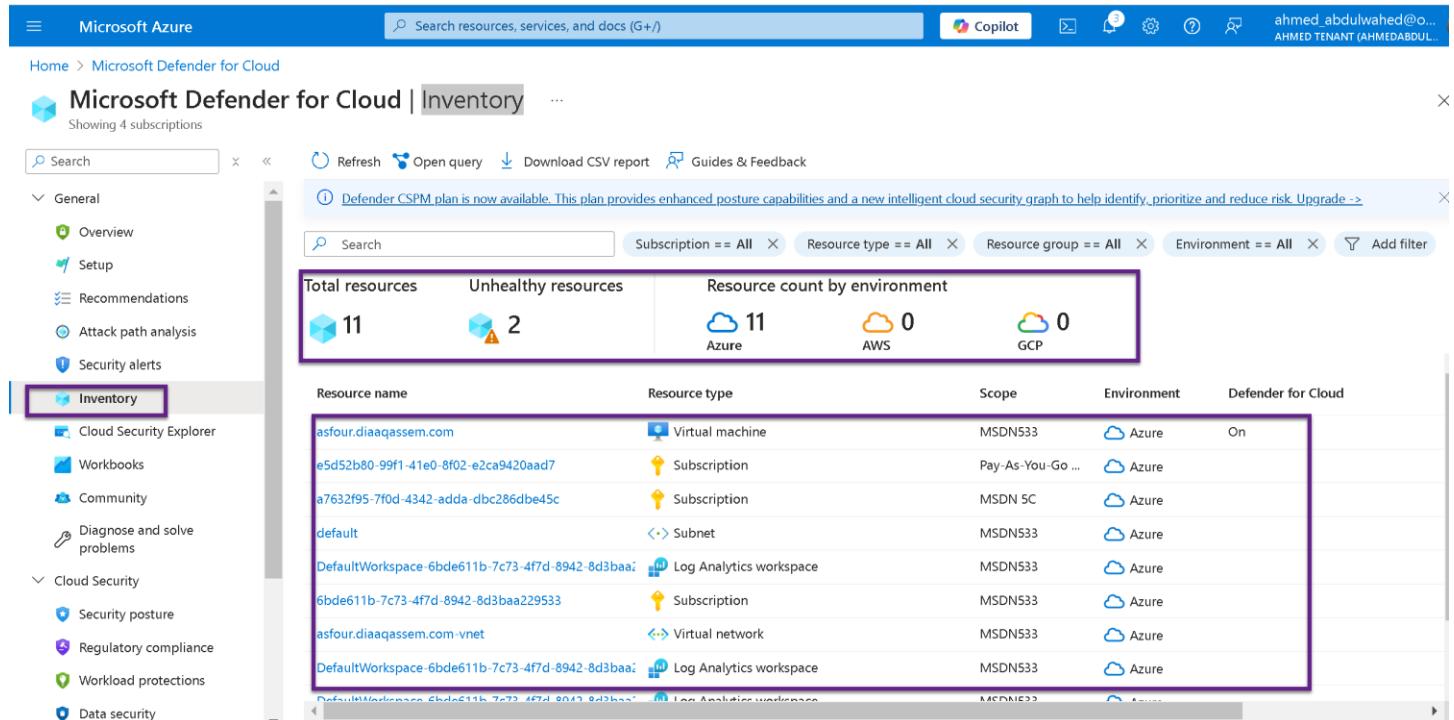
Microsoft Defender for Cloud | Security alerts

Showing 4 subscriptions

11 Open alerts | 11 Active alerts | 0 In progress alerts | 1 Affected resources

Severity	Alert name	Affected resource	Resource Group	Activity start time...	Last updated time...	MITRE ATT&CK®...
Low	Vulnerability scanner det...	abdelwahed	abdelwahed.me	11/04/24, 07:42 AM	11/04/24, 09:31 AM	Pre-attack
Low	Vulnerability scanner det...	abdelwahed	abdelwahed.me	10/08/24, 11:47 PM	10/09/24, 02:15 AM	Pre-attack
Low	Vulnerability scanner det...	abdelwahed	abdelwahed.me	10/30/24, 03:04 AM	10/30/24, 05:42 AM	Pre-attack
Low	Vulnerability scanner det...	abdelwahed	abdelwahed.me	11/04/24, 07:42 AM	11/04/24, 09:31 AM	Pre-attack
Low	Vulnerability scanner det...	abdelwahed	abdelwahed.me	10/16/24, 03:47 AM	10/16/24, 05:33 AM	Pre-attack
Low	Vulnerability scanner det...	abdelwahed	abdelwahed.me	10/30/24, 03:04 AM	10/30/24, 05:42 AM	Pre-attack

Inventory



Microsoft Defender for Cloud | Inventory

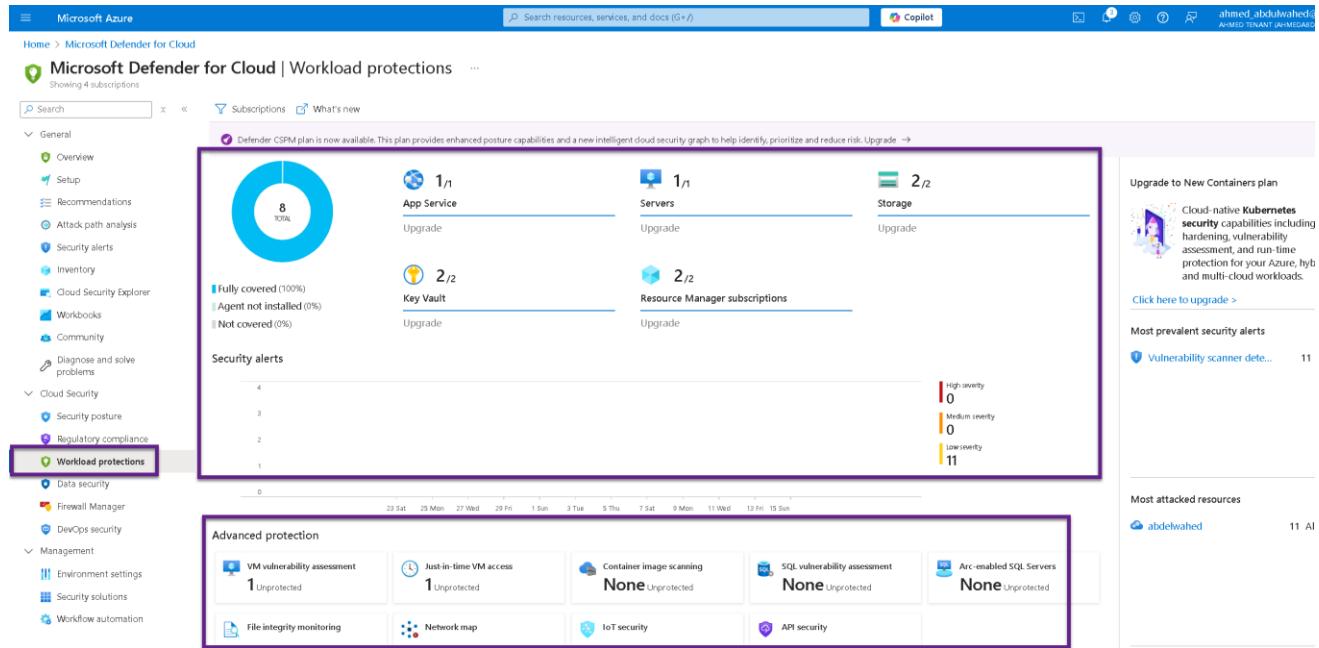
Showing 4 subscriptions

11 Total resources | 2 Unhealthy resources | Resource count by environment

Resource name	Resource type	Scope	Environment	Defender for Cloud
asfour.diaqassem.com	Virtual machine	MSDN533	Azure	On
e5d52b80-99f1-41e0-8f02-e2ca9420ad7	Subscription	Pay-As-You-Go ...	Azure	
a7632f95-7f0d-4342-adda-dbc286dbe45c	Subscription	MSDN 5C	Azure	
default	Subnet	MSDN533	Azure	
DefaultWorkspace-6bde611b-7c73-4f7d-8942-8d3baa...	Log Analytics workspace	MSDN533	Azure	
6bde611b-7c73-4f7d-8942-8d3baa229533	Subscription	MSDN533	Azure	
asfour.diaqassem.com-vnet	Virtual network	MSDN533	Azure	
DefaultWorkspace-6bde611b-7c73-4f7d-8942-8d3baa...	Log Analytics workspace	MSDN533	Azure	

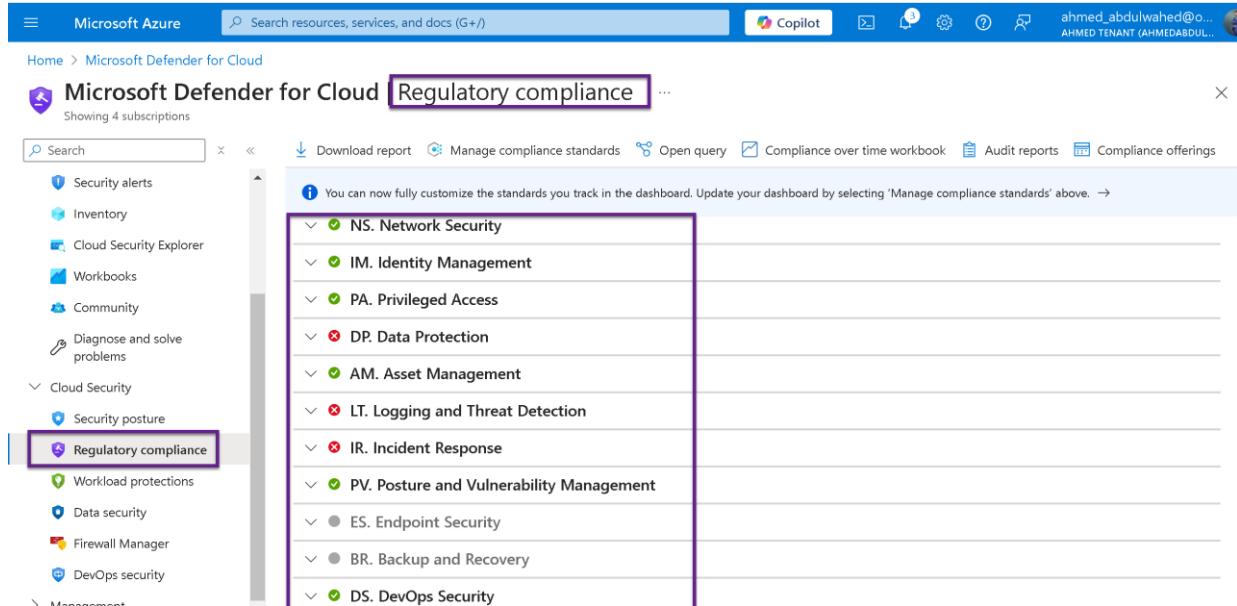
Complete Security with Microsoft Defender

Workload Protections in **Microsoft Defender for Cloud** focus on securing various workloads running in your hybrid and multi-cloud environments. These protections are designed to monitor, detect, and respond to threats targeting virtual machines, containers, databases, application services, and more.



The screenshot shows the Microsoft Defender for Cloud Workload protections dashboard. It features a summary section with a donut chart showing 8 total resources, categorized as Fully covered (100%), Agent not installed (0%), and Not covered (0%). Below this are sections for App Service, Servers, and Storage, each with a count of 1/n and a 'Upgrade' button. The 'Security alerts' section shows 4 alerts with 11 Low severity. The 'Advanced protection' section includes VM vulnerability assessment (1 Unprotected), Just-in-time VM access (1 Unprotected), Container image scanning (None Unprotected), SQL vulnerability assessment (None Unprotected), and Arc-enabled SQL Servers (None Unprotected). A sidebar on the left lists various security categories, with 'Workload protections' highlighted. A sidebar on the right provides information about upgrading to a new containers plan and lists the most prevalent security alerts.

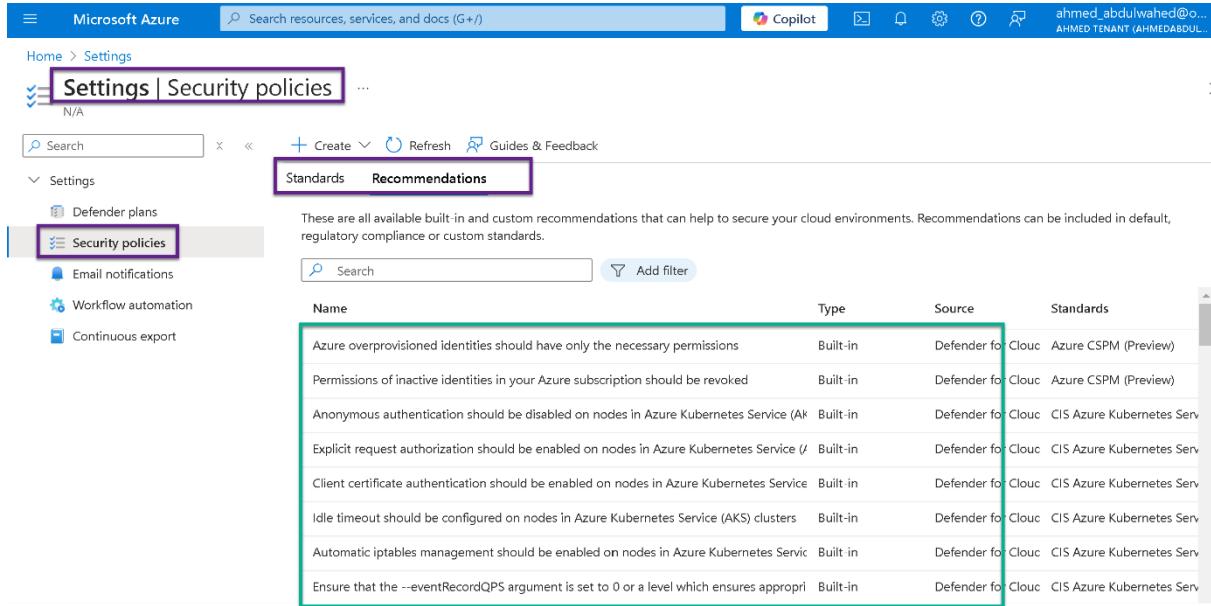
Regulatory Compliance is a feature that helps organizations continuously monitor and ensure that their cloud environments align with industry-standard regulatory requirements, such as ISO 27001, PCI DSS, or custom internal standards. It provides tools for tracking compliance, assessing resource configurations, and implementing remediation steps



The screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard. It lists various compliance standards: NS. Network Security, IM. Identity Management, PA. Privileged Access, DP. Data Protection, AM. Asset Management, LT. Logging and Threat Detection, IR. Incident Response, PV. Posture and Vulnerability Management, ES. Endpoint Security, BR. Backup and Recovery, and DS. DevOps Security. Most standards are marked as 'Green' (checked), except for DP. Data Protection and LT. Logging and Threat Detection which are 'Red' (unchecked). A sidebar on the left lists various security categories, with 'Regulatory compliance' highlighted.

Complete Security with Microsoft Defender

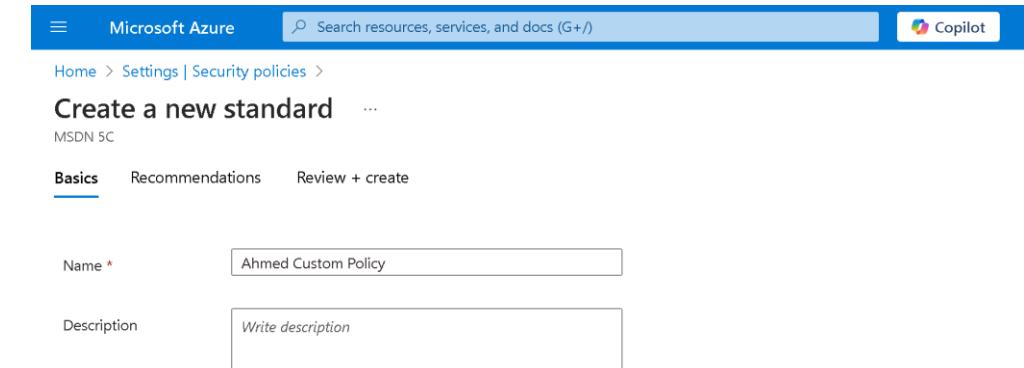
The **Security Policies** section in **Microsoft Defender for Cloud** under **Settings** allows you to define and enforce security configurations across your cloud resources. It provides centralized management for Azure Policy assignments that align with your organization's security and compliance requirements.



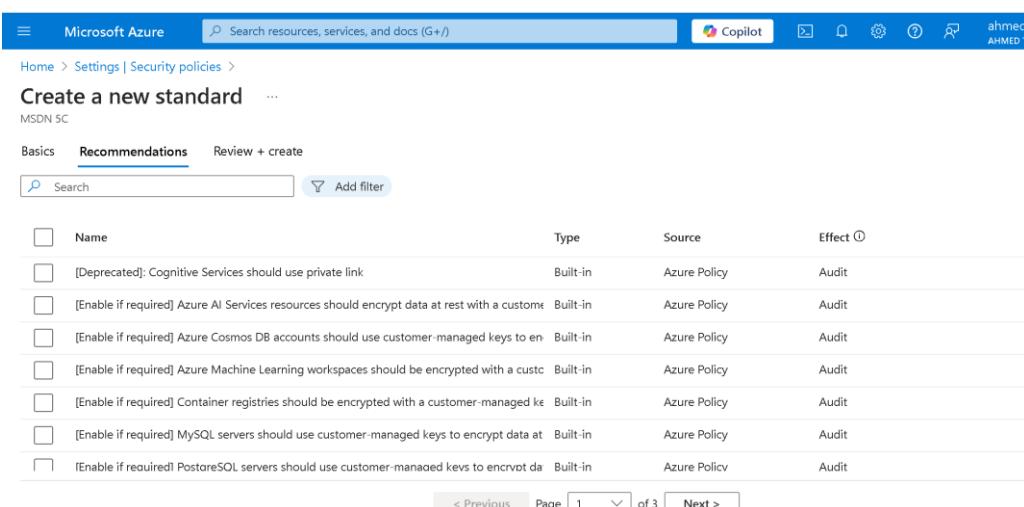
The screenshot shows the Microsoft Azure Settings | Security policies page. The 'Recommendations' tab is selected. A table lists various security recommendations, each with a checkbox, name, type, source, and standards. The recommendations are as follows:

Name	Type	Source	Standards
Azure overprovisioned identities should have only the necessary permissions	Built-in	Defender for Cloud	Azure CSPM (Preview)
Permissions of inactive identities in your Azure subscription should be revoked	Built-in	Defender for Cloud	Azure CSPM (Preview)
Anonymous authentication should be disabled on nodes in Azure Kubernetes Service (AKS)	Built-in	Defender for Cloud	CIS Azure Kubernetes Service
Explicit request authorization should be enabled on nodes in Azure Kubernetes Service (AKS)	Built-in	Defender for Cloud	CIS Azure Kubernetes Service
Client certificate authentication should be enabled on nodes in Azure Kubernetes Service (AKS)	Built-in	Defender for Cloud	CIS Azure Kubernetes Service
Idle timeout should be configured on nodes in Azure Kubernetes Service (AKS) clusters	Built-in	Defender for Cloud	CIS Azure Kubernetes Service
Automatic iptables management should be enabled on nodes in Azure Kubernetes Service (AKS)	Built-in	Defender for Cloud	CIS Azure Kubernetes Service
Ensure that the --eventRecordQPS argument is set to 0 or a level which ensures appropriate performance	Built-in	Defender for Cloud	CIS Azure Kubernetes Service

using create option, you can create your own



The screenshot shows the Microsoft Azure Create a new standard page under the 'Basics' tab. The 'Name' field is set to 'Ahmed Custom Policy'. The 'Description' field is empty. The page also shows the 'Recommendations' and 'Review + create' tabs.



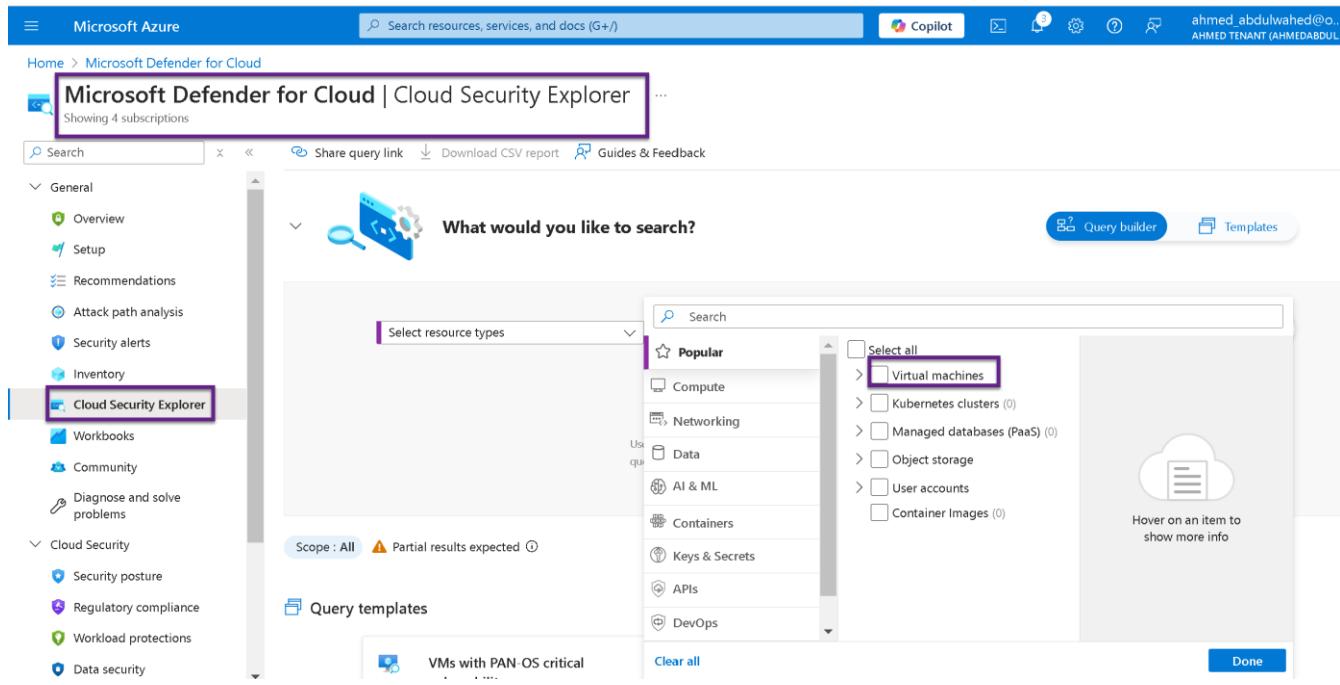
The screenshot shows the Microsoft Azure Create a new standard page under the 'Recommendations' tab. The table lists various recommendations with checkboxes, names, types, sources, and effects. The recommendations are as follows:

Name	Type	Source	Effect
[Deprecated]: Cognitive Services should use private link	Built-in	Azure Policy	Audit
[Enable if required] Azure AI Services resources should encrypt data at rest with a customer-managed key	Built-in	Azure Policy	Audit
[Enable if required] Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest	Built-in	Azure Policy	Audit
[Enable if required] Azure Machine Learning workspaces should be encrypted with a customer-managed key	Built-in	Azure Policy	Audit
[Enable if required] Container registries should be encrypted with a customer-managed key	Built-in	Azure Policy	Audit
[Enable if required] MySQL servers should use customer-managed keys to encrypt data at rest	Built-in	Azure Policy	Audit
[Enable if required] PostgreSQL servers should use customer-managed keys to encrypt data at rest	Built-in	Azure Policy	Audit

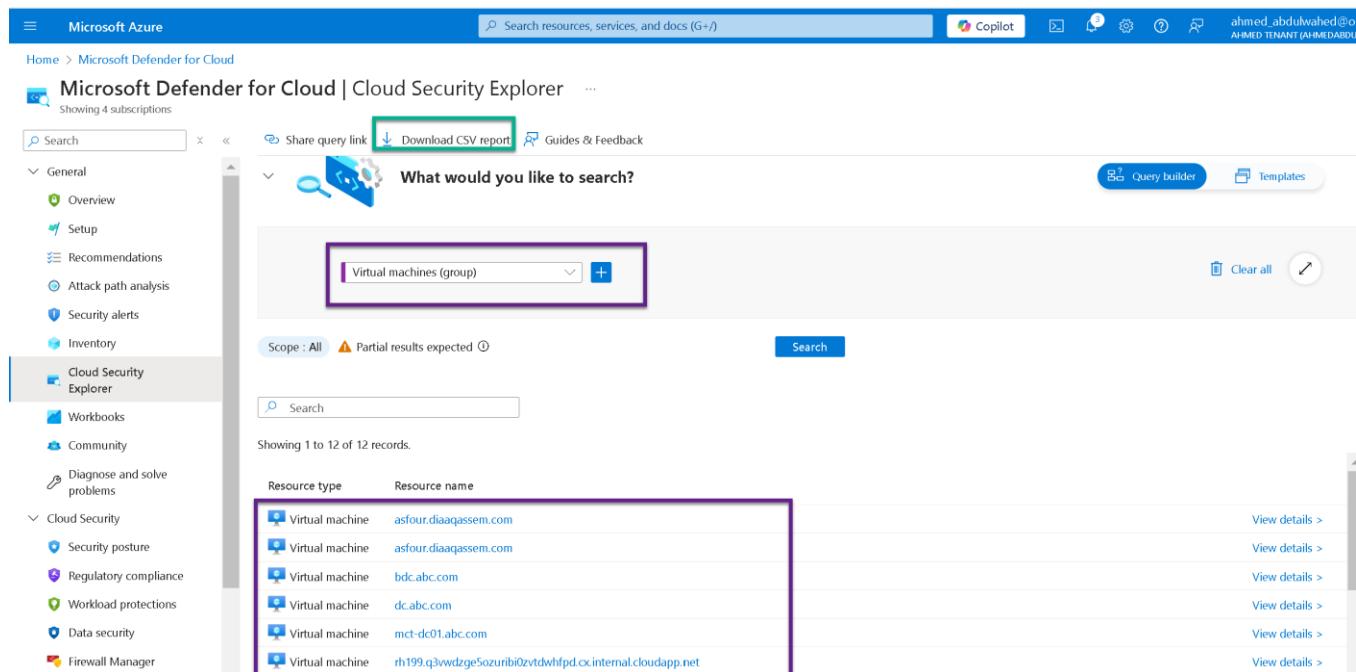
Complete Security with Microsoft Defender

Microsoft Defender for Cloud | Cloud Security Explorer (Reporting)

Cloud Security Explorer is a feature within **Microsoft Defender for Cloud** that provides **query-based exploration** of your cloud resources and their security context. It empowers administrators and security analysts to proactively discover, filter, and analyze resources, configurations, and potential vulnerabilities across multi-cloud environments.



The screenshot shows the Microsoft Defender for Cloud Cloud Security Explorer interface. The left sidebar is collapsed, and the main area is titled "Microsoft Defender for Cloud | Cloud Security Explorer". A search bar at the top right contains the placeholder "Search resources, services, and docs (G+)". Below the search bar are buttons for "Share query link", "Download CSV report", and "Guides & Feedback". The main content area is titled "What would you like to search?" and features a "Select resource types" dropdown. A "Popular" section lists several resource types with checkboxes: Compute, Networking, Data, AI & ML, Containers, Keys & Secrets, APIs, and DevOps. A tooltip "Hover on an item to show more info" points to the Compute checkbox. A "Query templates" section shows a template for "VMs with PAN-OS critical". At the bottom right is a "Done" button.



The screenshot shows the Microsoft Defender for Cloud Cloud Security Explorer search results for "Virtual machines (group)". The search bar at the top right is highlighted. The main content area shows a list of 12 virtual machines. The table has columns for "Resource type" and "Resource name". The "Resource type" column shows icons for Virtual machine. The "Resource name" column lists the names of the virtual machines. The first five entries are: asfour.diaaqassem.com, asfour.diaaqassem.com, bdc.abc.com, dc.abc.com, and mct-dc01.abc.com. The last entry is partially visible as rh199.q3wdzge5ozunbi0zvtdwhfpd.cx.internal.cloudapp.net. To the right of each resource name is a "View details >" link.

Resource type	Resource name	Action
Virtual machine	asfour.diaaqassem.com	View details >
Virtual machine	asfour.diaaqassem.com	View details >
Virtual machine	bdc.abc.com	View details >
Virtual machine	dc.abc.com	View details >
Virtual machine	mct-dc01.abc.com	View details >
Virtual machine	rh199.q3wdzge5ozunbi0zvtdwhfpd.cx.internal.cloudapp.net	View details >