Complete Security with Microsoft Defender

Version 24.12

Ahmed Abdelwahed
ahmed@abdelwahed.me
www.abdelwahed.me
LinkedIn
GitHub

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

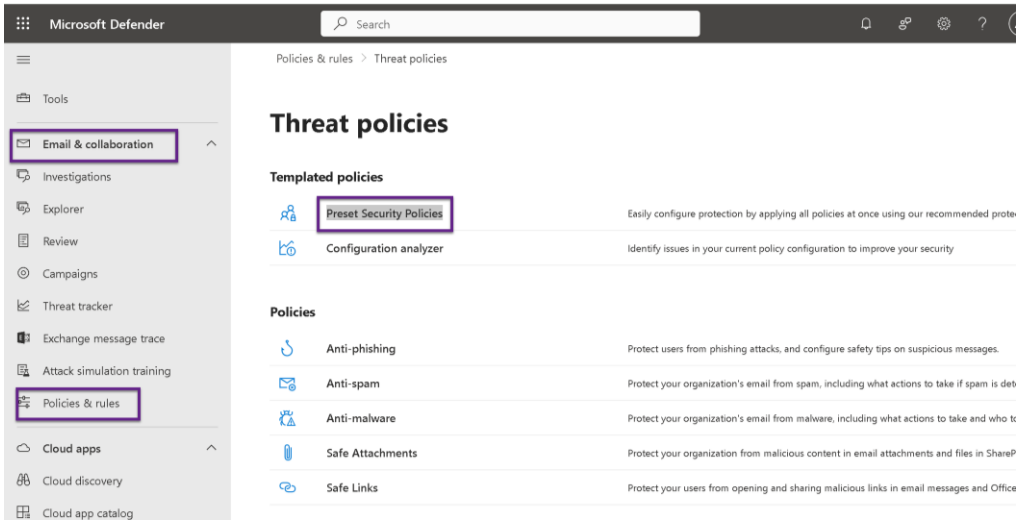
https://security.microsoft.com/

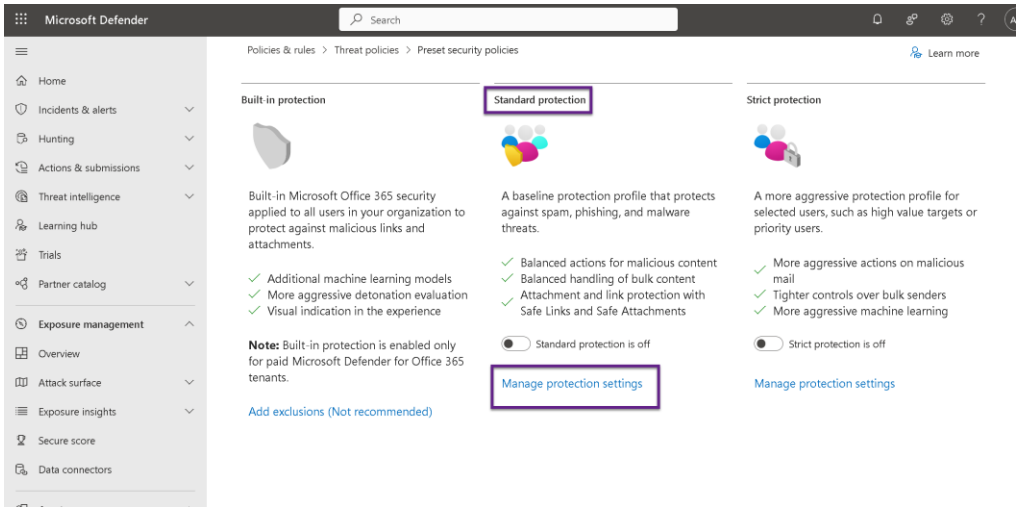
Preset Security Policies

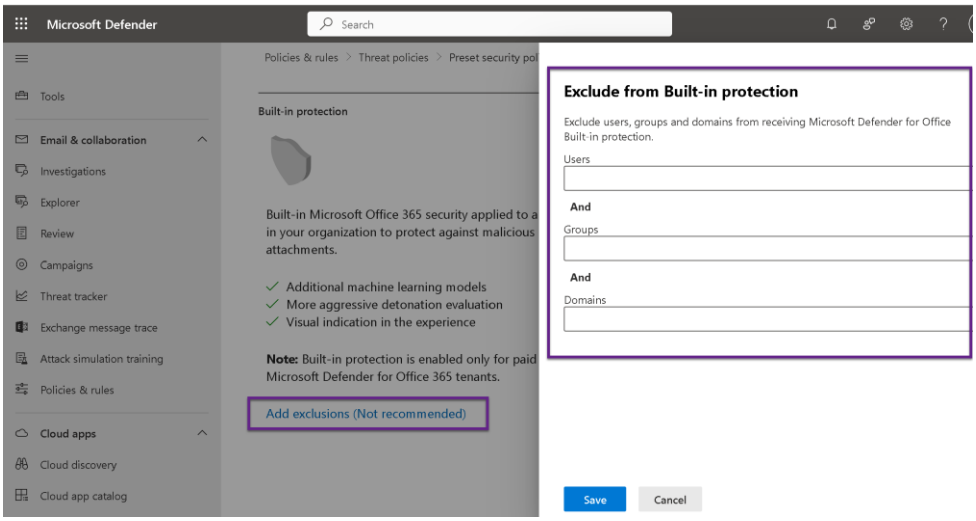
Preset Security Policies are pre-defined configurations in Microsoft Defender for Office 365 designed to enforce security controls for:

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.

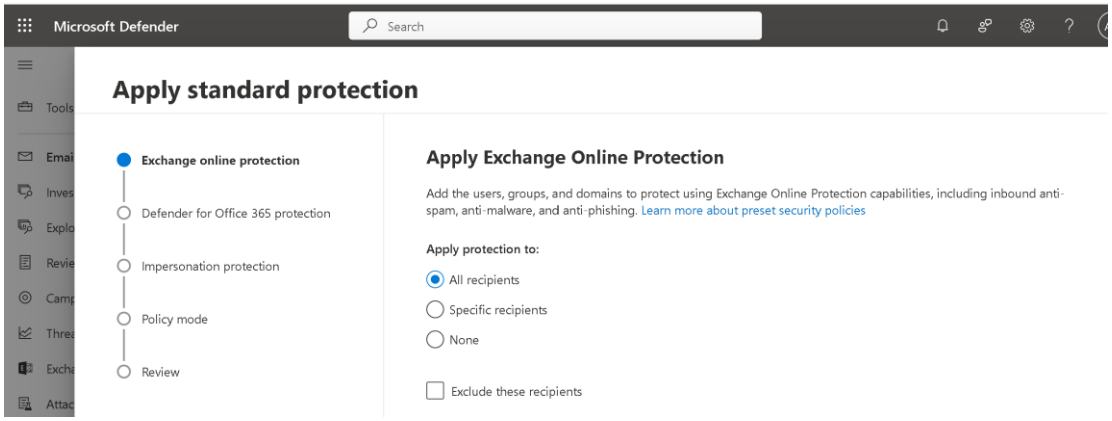
These policies help reduce administrative overhead and ensure your organization aligns with Microsoft's recommended security settings.

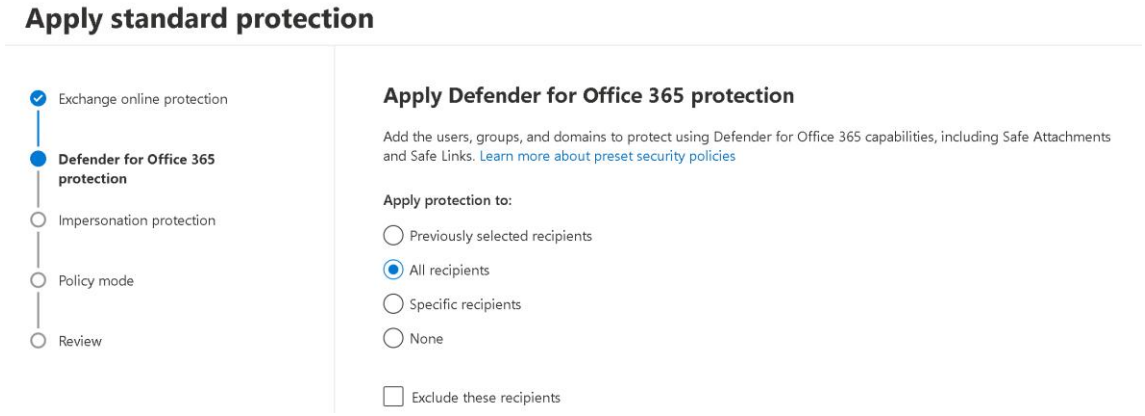


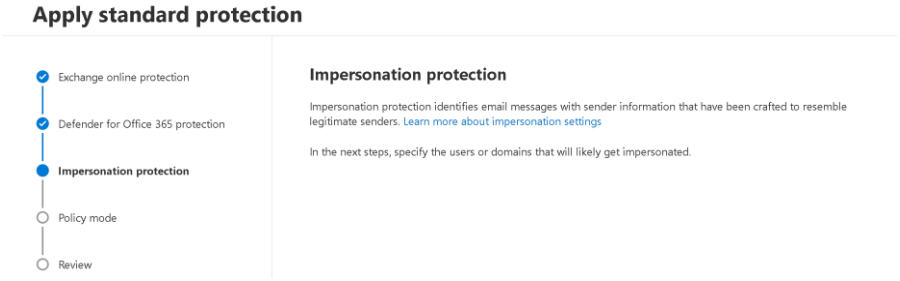


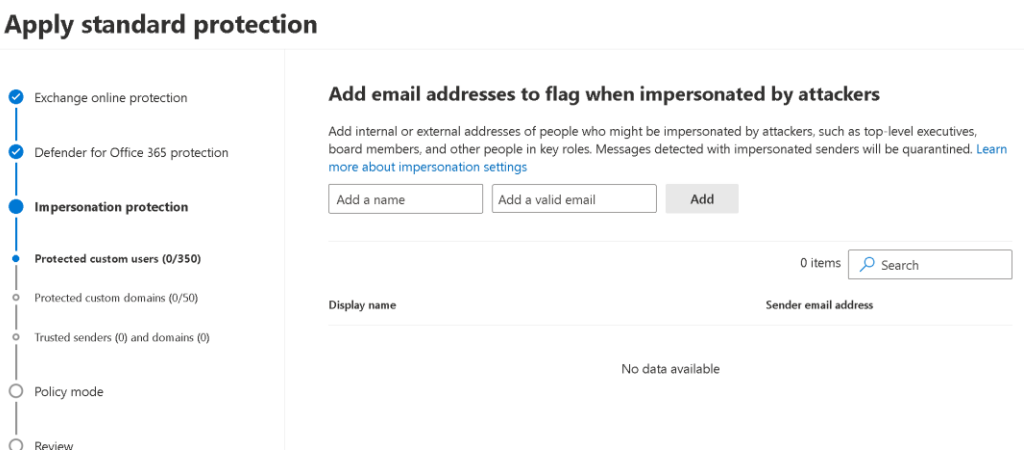


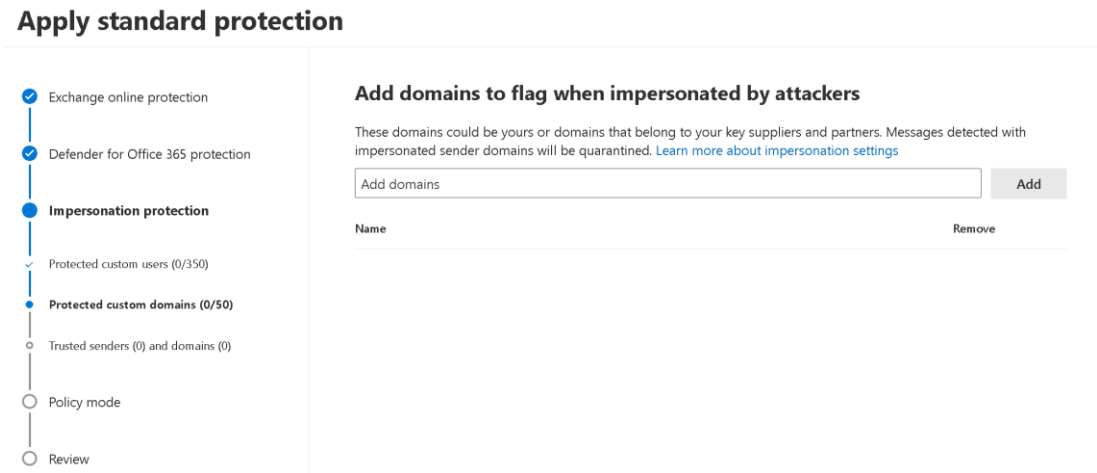
Setting up the Preset Security Policies

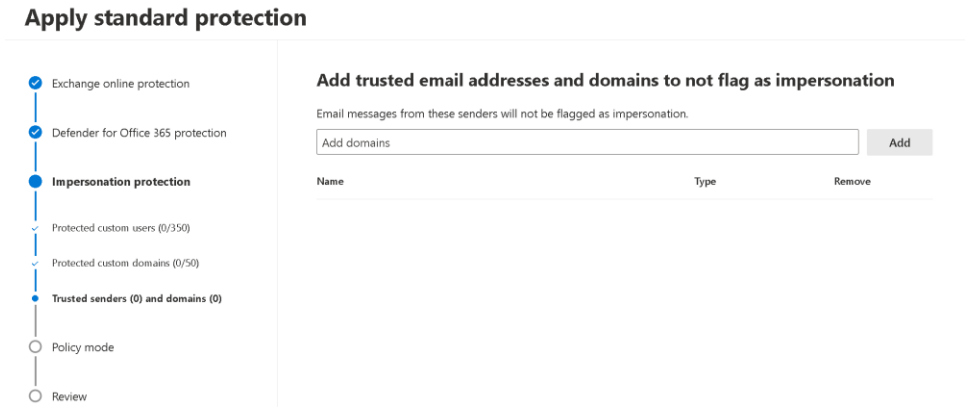


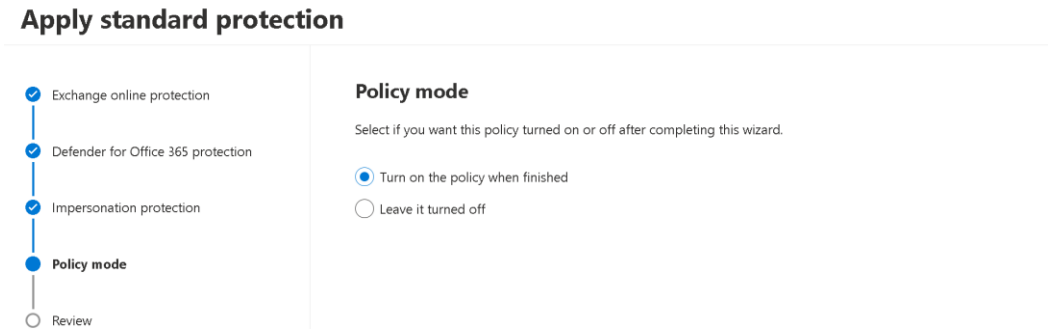


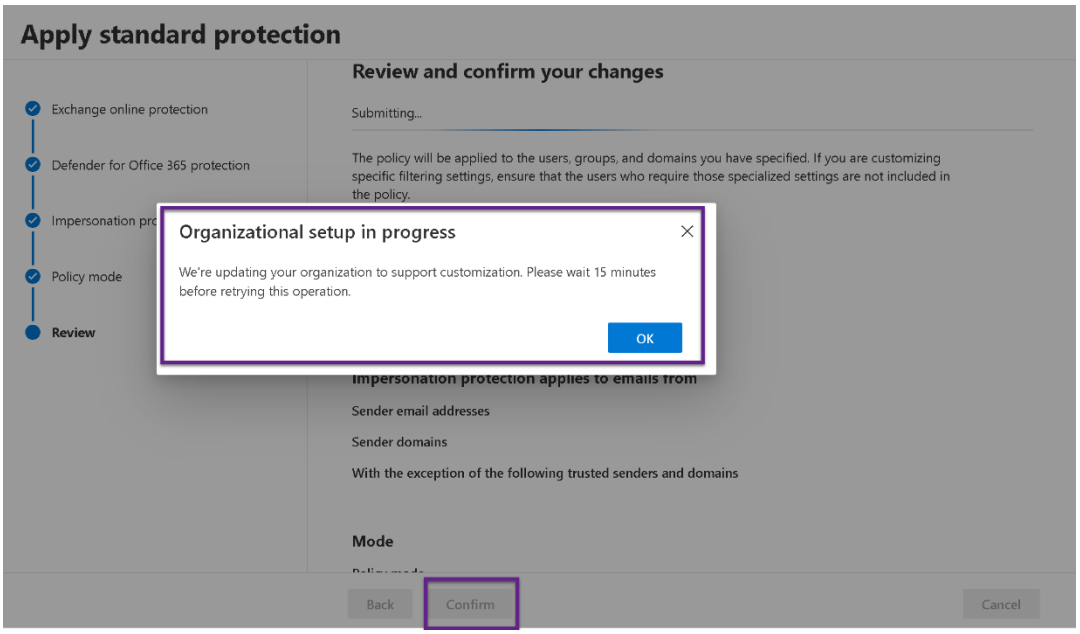



Apply standard protection
Exchange online protection
Defender for Office 365 protection
Impersonation protection
Protected custom users (0/350)
Protected custom domains (0/50)
Trusted senders (0) and domains (0)
Policy mode
Review
Add email addresses to flag when impersonated by attackers
Add internal 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

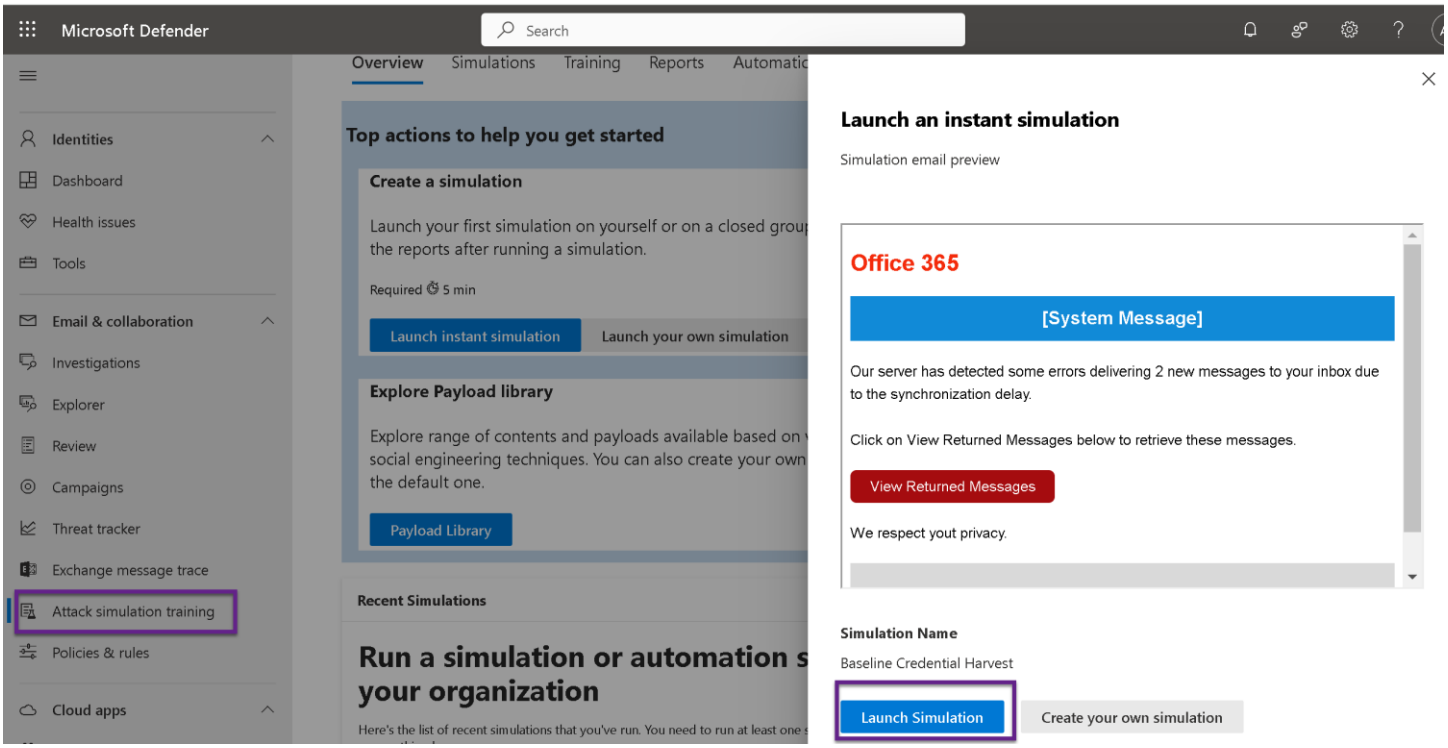

Apply standard protection
Exchange online protection
Defender for Office 365 protection
Impersonation protection
Protected custom users (0/350)
Protected custom domains (0/50)
Trusted senders (0) and domains (0)
Policy mode
Review
Add domains to flag when impersonated by attackers
These domains could 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

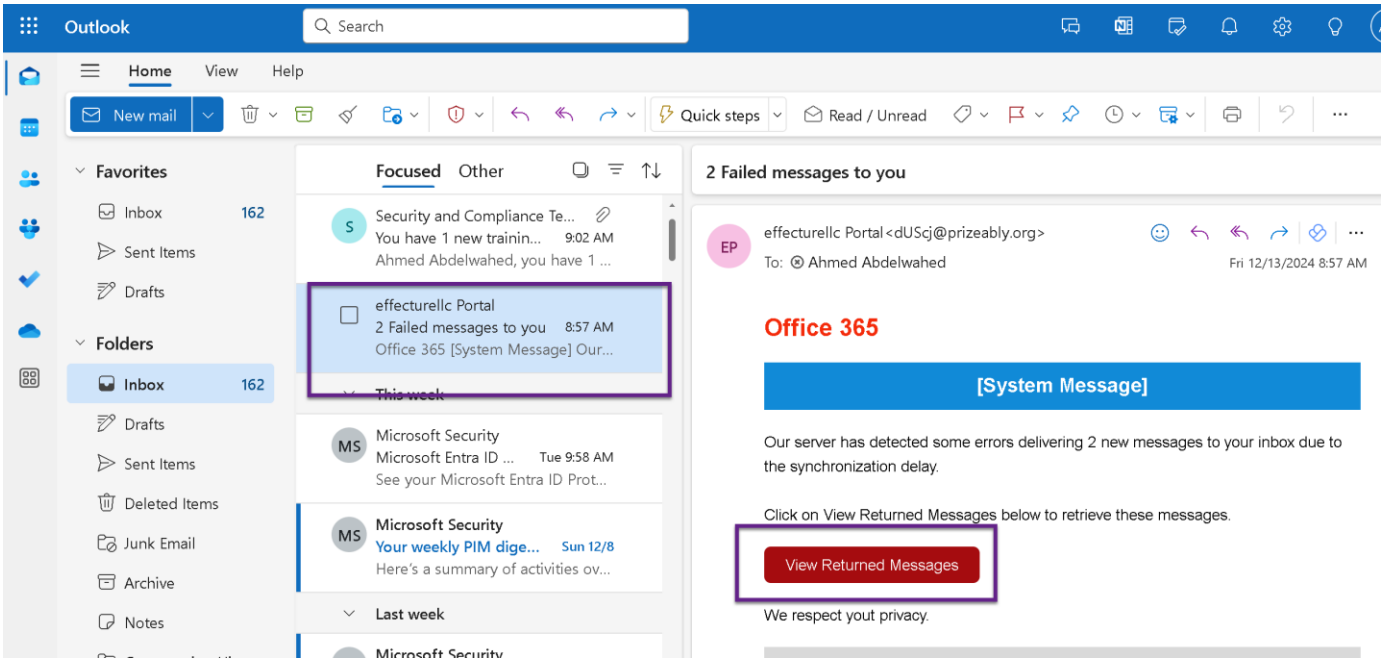

Apply standard protection
Exchange online protection
Defender for Office 365 protection
Impersonation protection
Policy mode
Review
Policy mode
Select if you want this policy turned on or off after completing this wizard.
Turn on the policy when finished
Leave it turned off



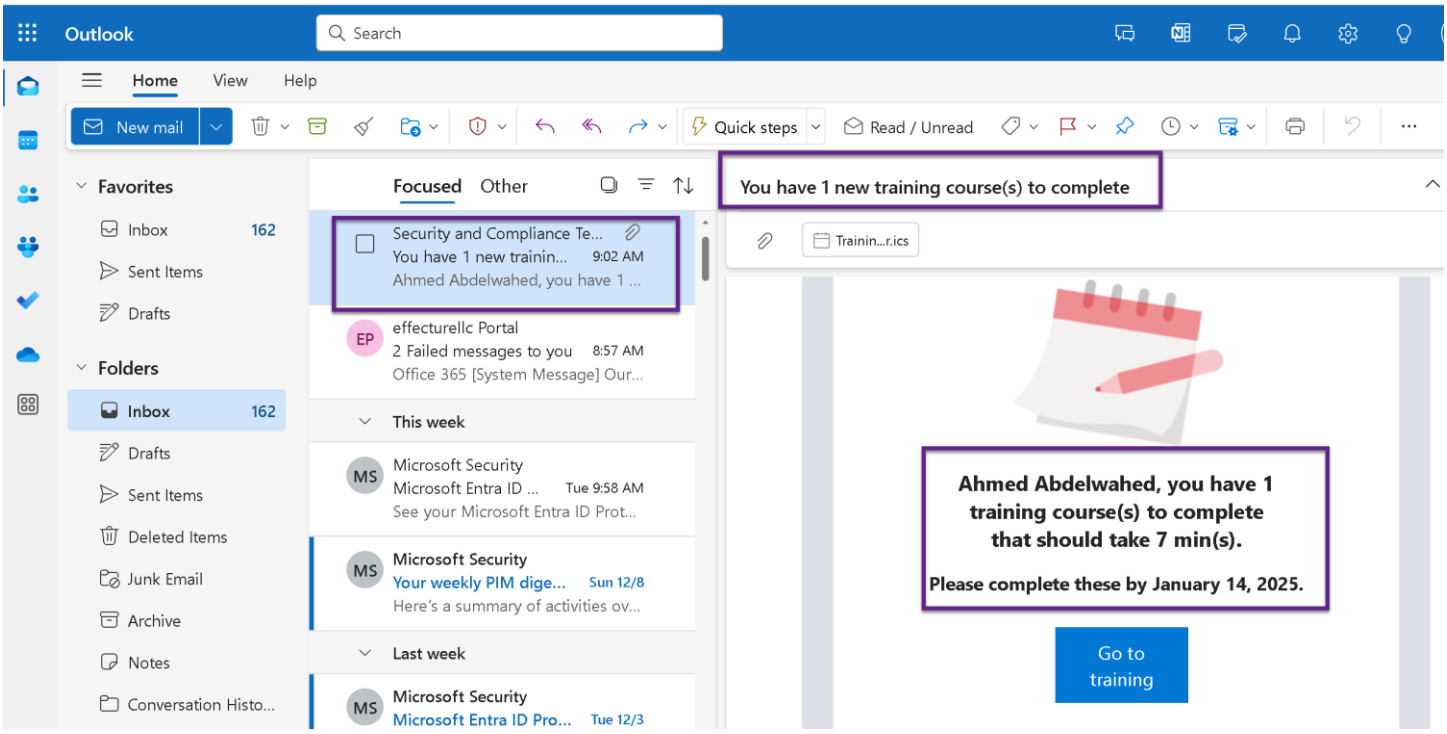
Simulate attack



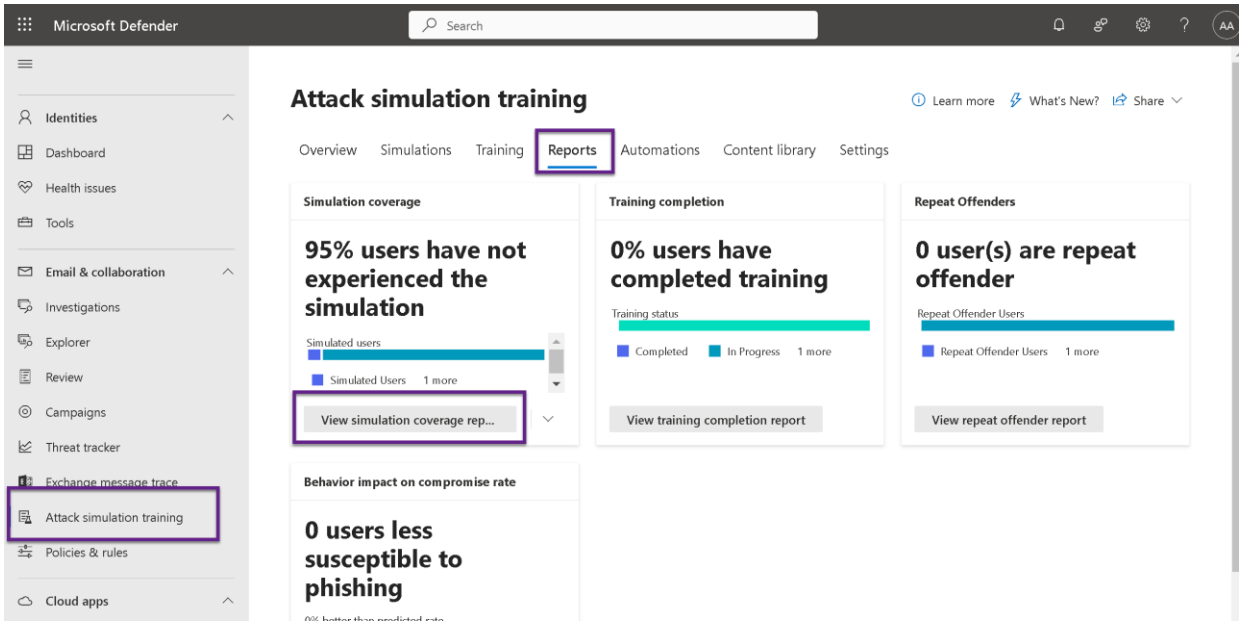
Users will receive the following message as simulation

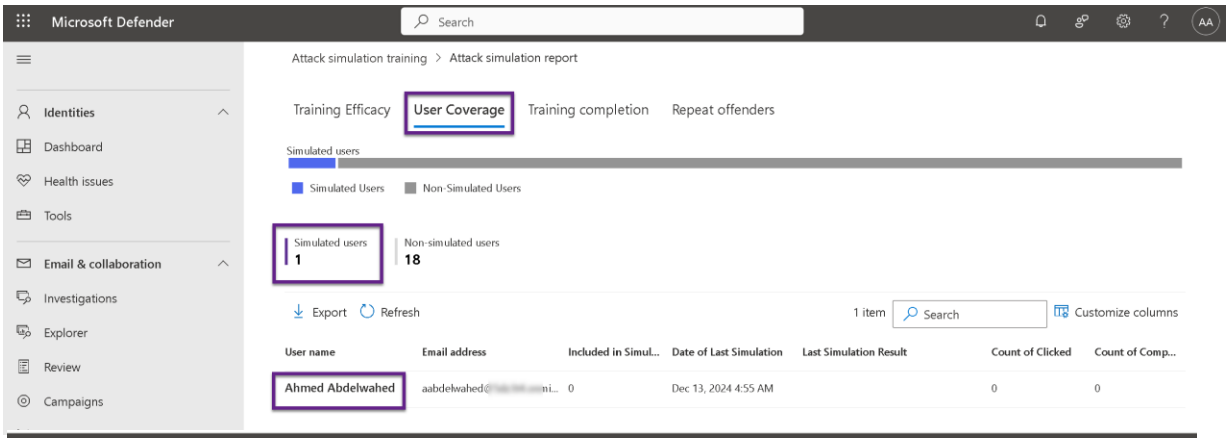


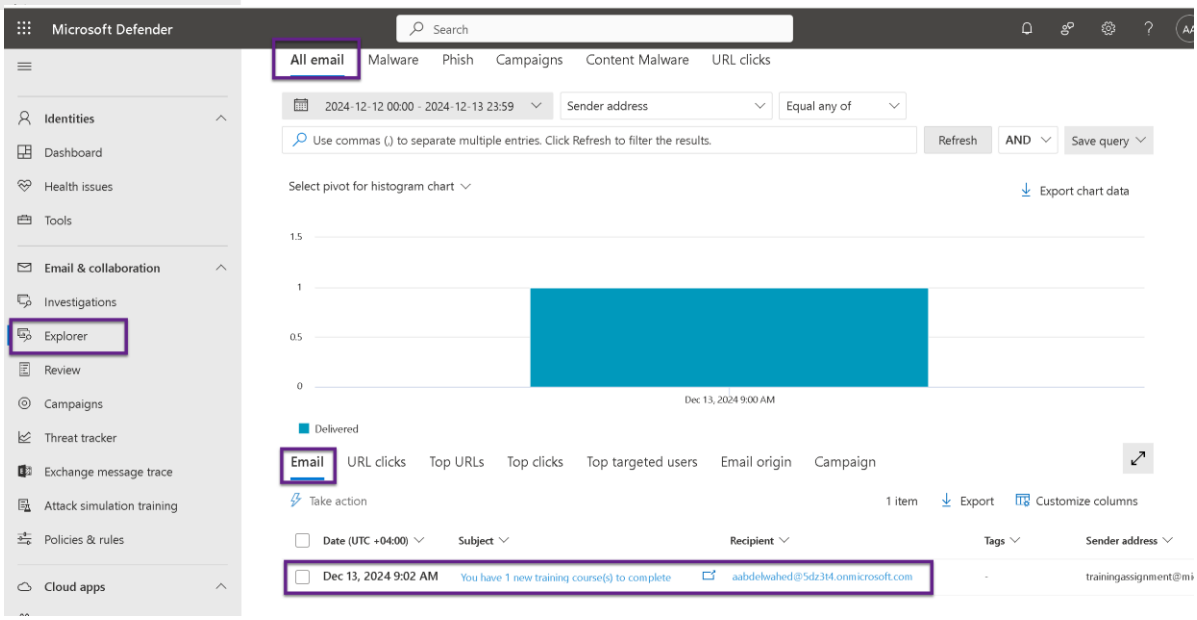
Once the user interact with the email, will receive another email



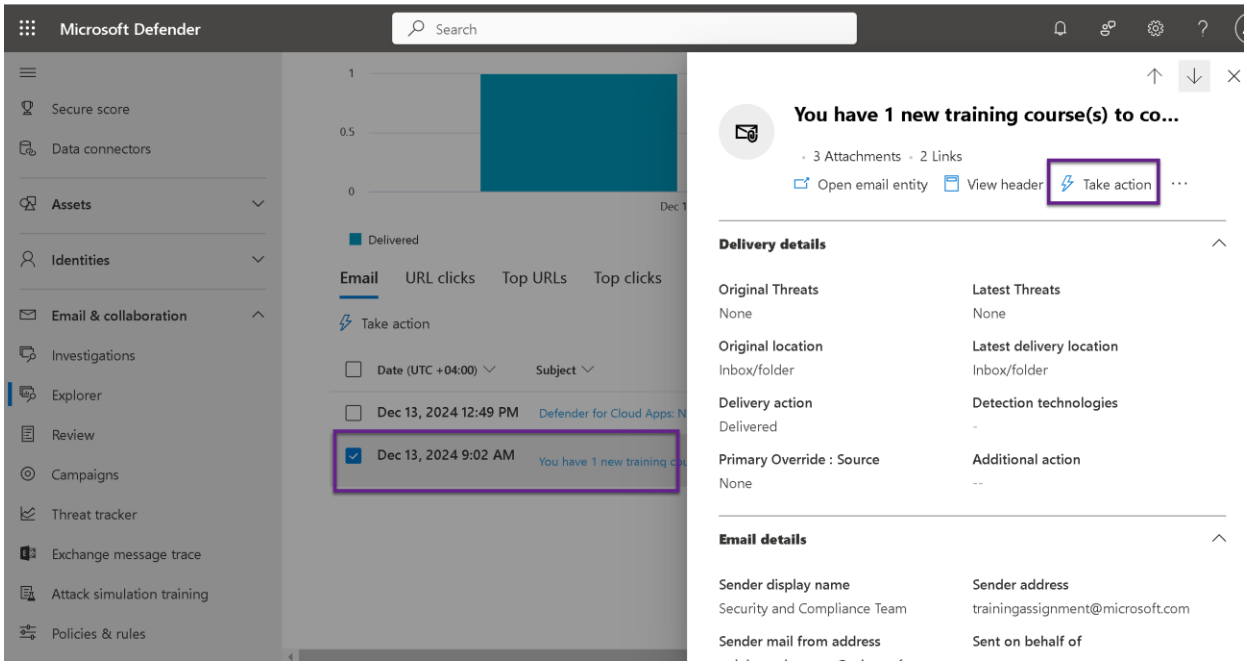
You can see the result

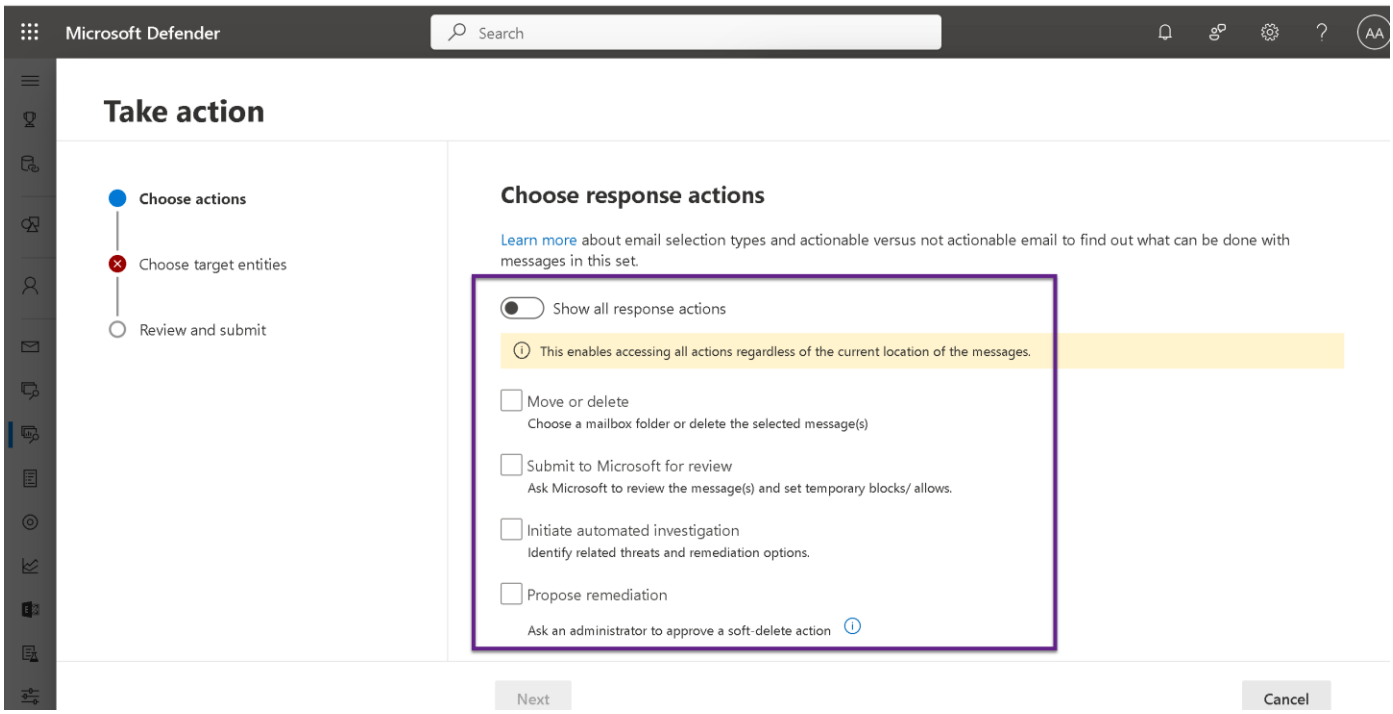






- **Take Action**: Provides remediation steps for handling the alert, such as:
    - Quarantine or delete the email.
    - Report the email as phishing or spam.
    - Investigate related threats across the environment.





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.

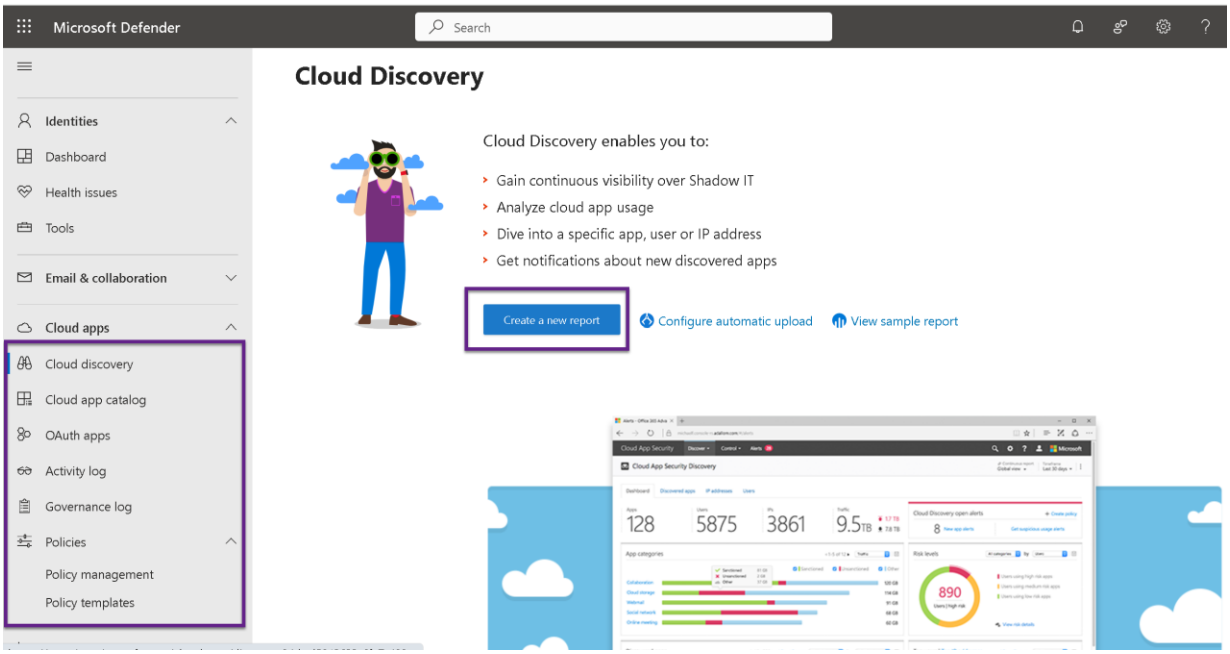
4. Compliance and Governance

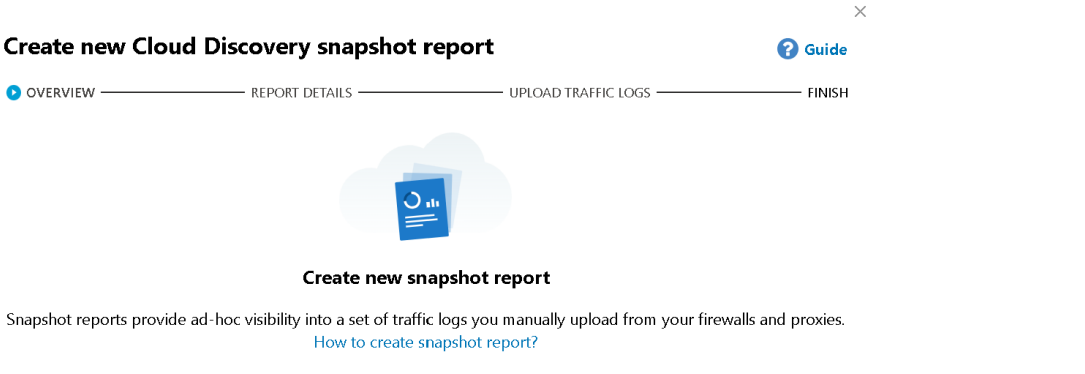
- **Compliance Reporting**:
  - Monitors applications for compliance with regulatory standards such as GDPR, ISO 27001, and HIPAA.
- **Sanctioned and Unsanctioned Apps**:
  - Mark apps as sanctioned or unsanctioned based on organizational risk tolerance.
  - Block or restrict access to unsanctioned apps.

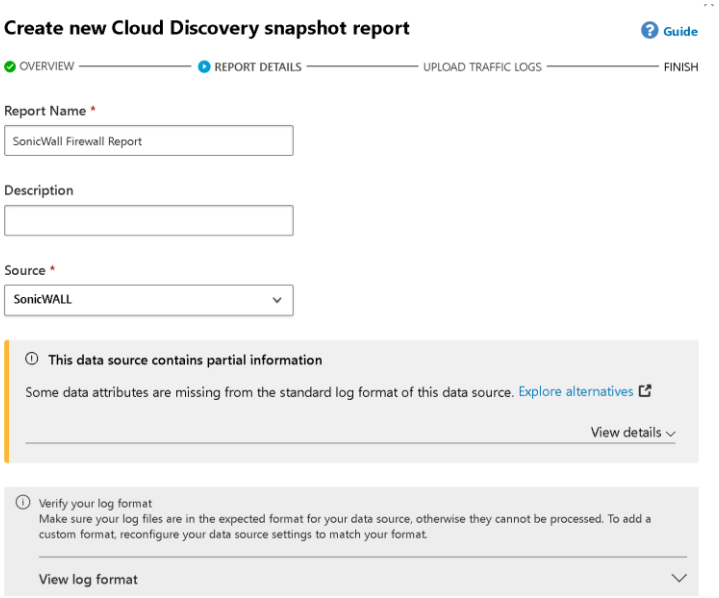
5. Integration with Other Microsoft Tools

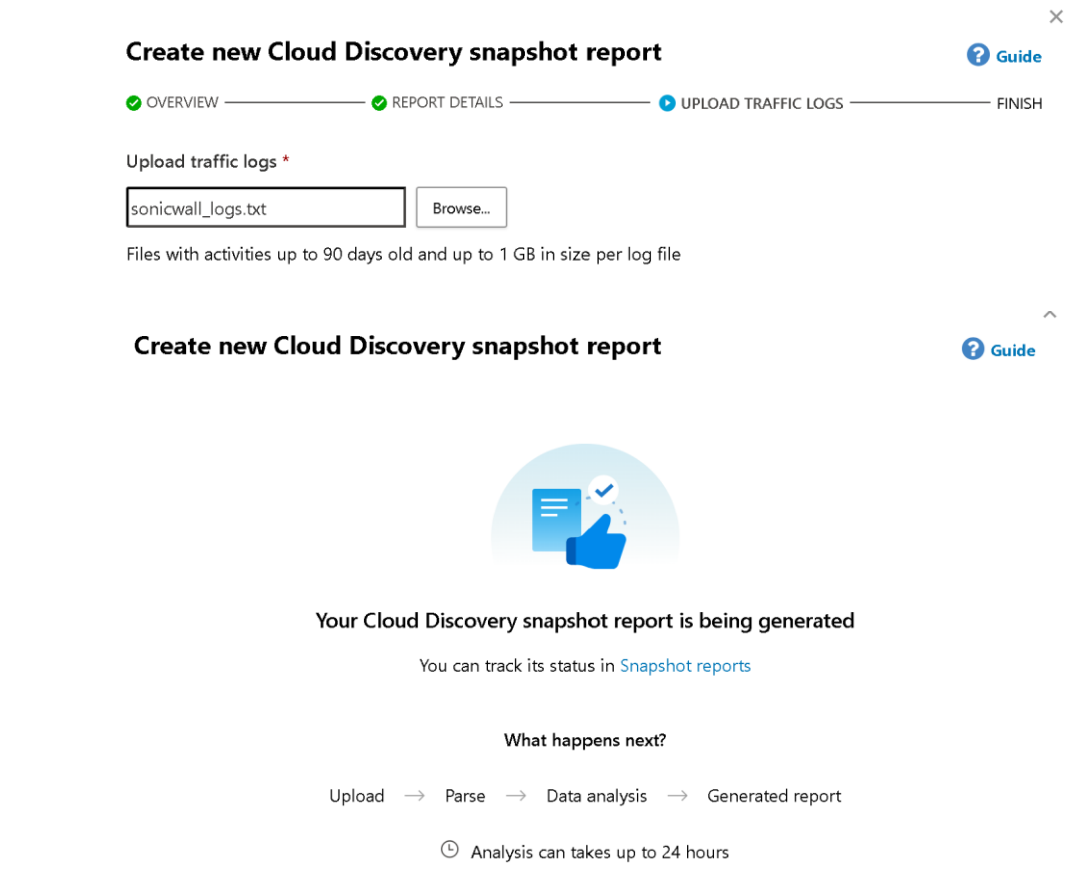
- Works with:
  - **Microsoft Defender for Endpoint**: Correlates device activity with cloud app usage.
  - **Microsoft Defender for Identity**: Detects compromised identities accessing cloud applications.
  - **Microsoft Sentinel**: Provides advanced SIEM integration for threat hunting.

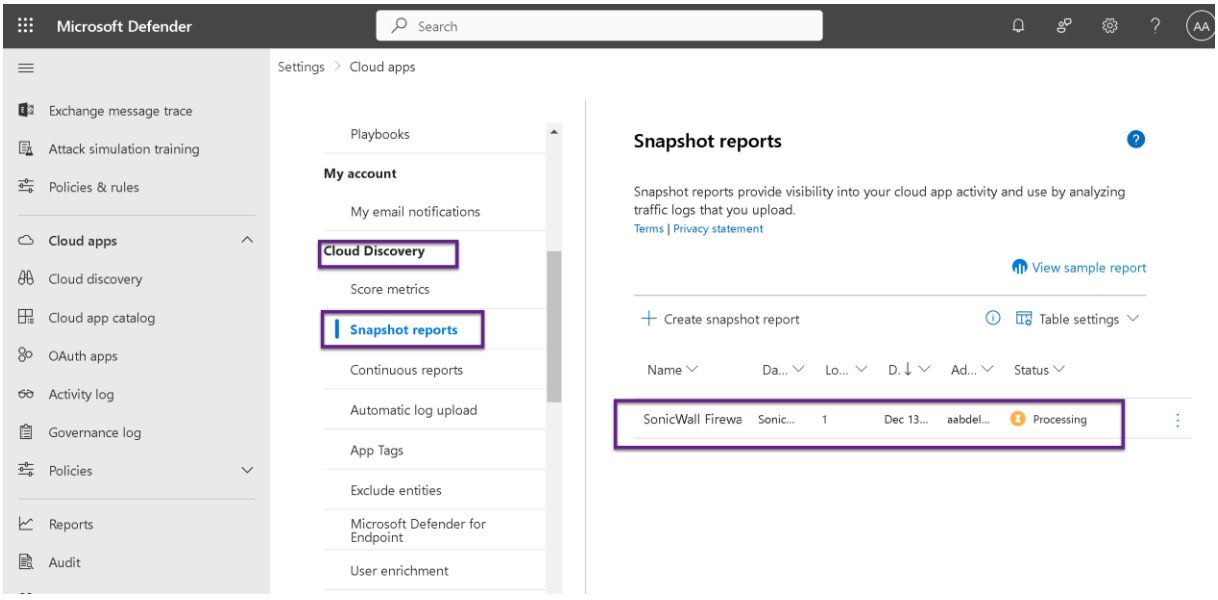
To get data here you have to build a report and import the app logs

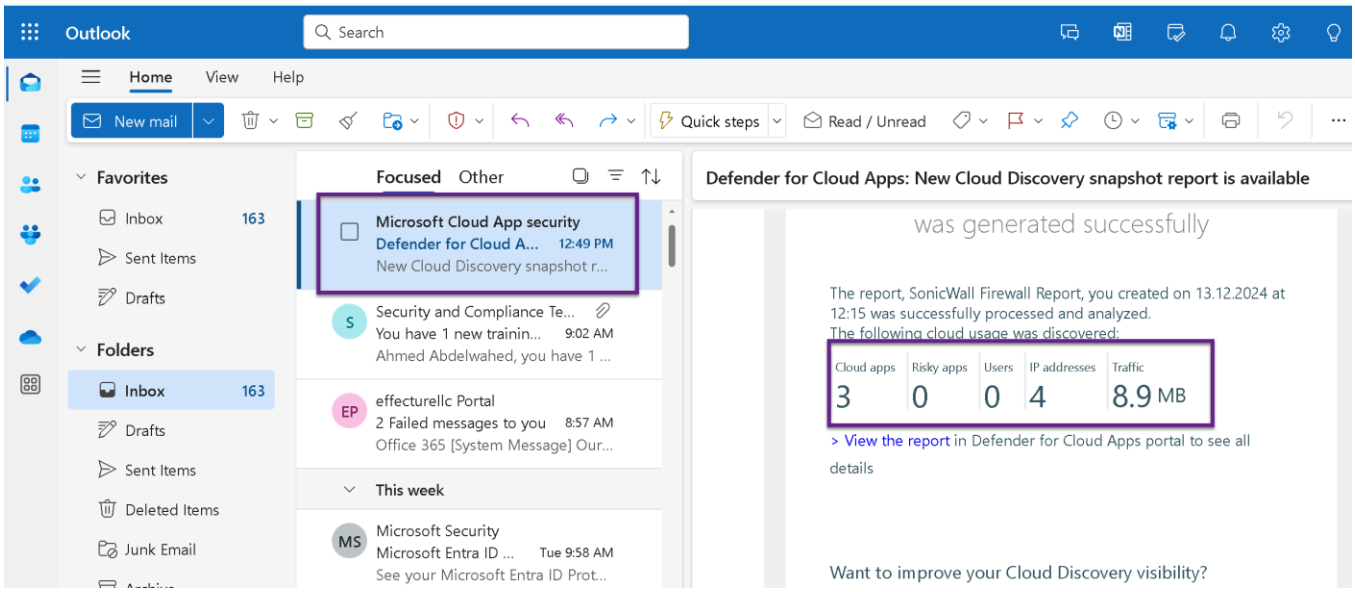




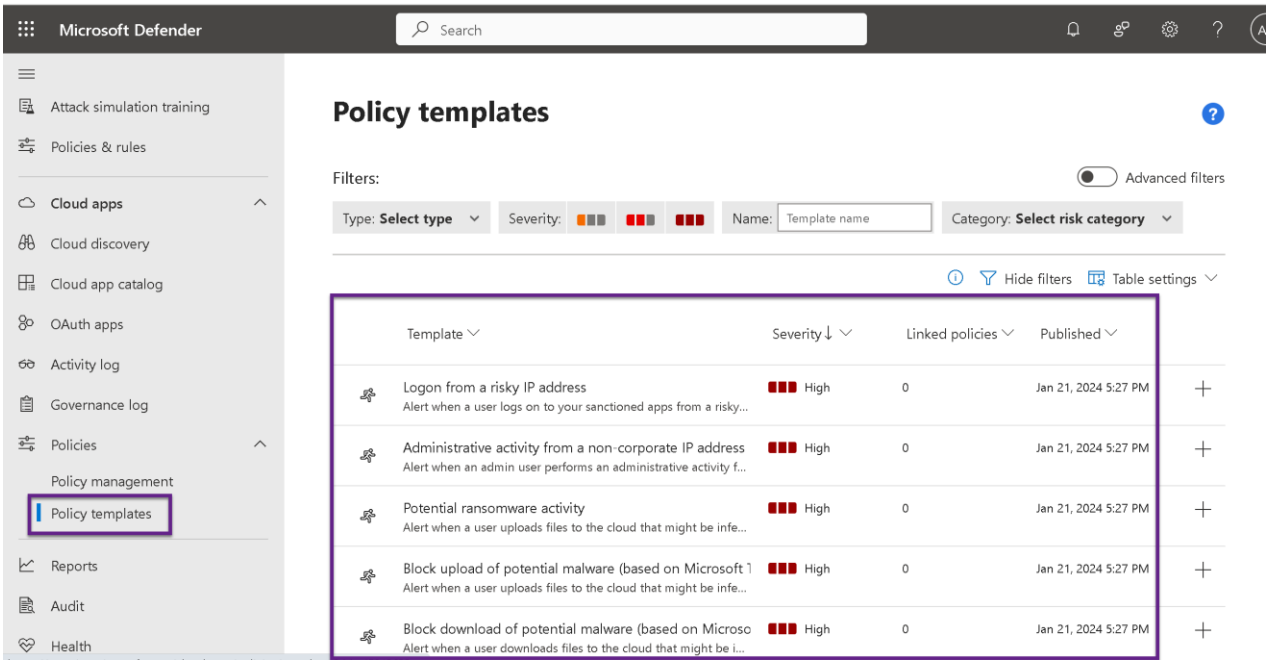



Create new Cloud Discovery snapshot report
Guide
OVERVIEW
REPORT DETAILS
UPLOAD TRAFFIC LOGS
FINISH
Upload traffic logs *
sonicwall_logs.txt
Browse...
Files with activities up to 90 days old and up to 1 GB in size per log file
Create new Cloud Discovery snapshot report
Guide
Your Cloud Discovery snapshot 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
Search
Settings > Cloud apps
Exchange message trace
Attack simulation training
Policies & rules
Cloud apps
Cloud discovery
Cloud app catalog
OAuth apps
Activity log
Governance log
Policies
Reports
Audit
Playbooks
My account
My email notifications
Cloud Discovery
Score metrics
Snapshot reports
Continuous reports
Automatic log upload
App Tags
Exclude entities
Microsoft Defender for Endpoint
User enrichment
Snapshot reports
Snapshot reports provide visibility into your cloud app activity and use by analyzing traffic logs that you upload.
Terms | Privacy statement
View sample report
Create snapshot report
Table settings
Name
Da...
Lo...
D.
Ad...
Status
SonicWall Firewa
Sonic...
1
Dec 13...
aabdel...
Processing



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.



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.

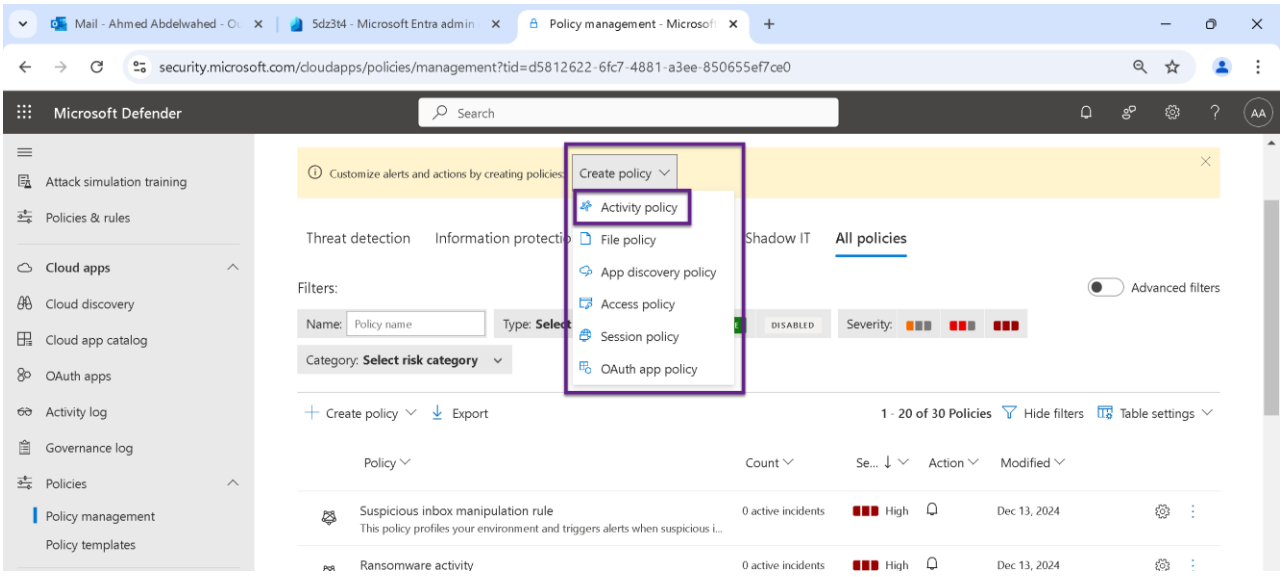
5. Session Policy

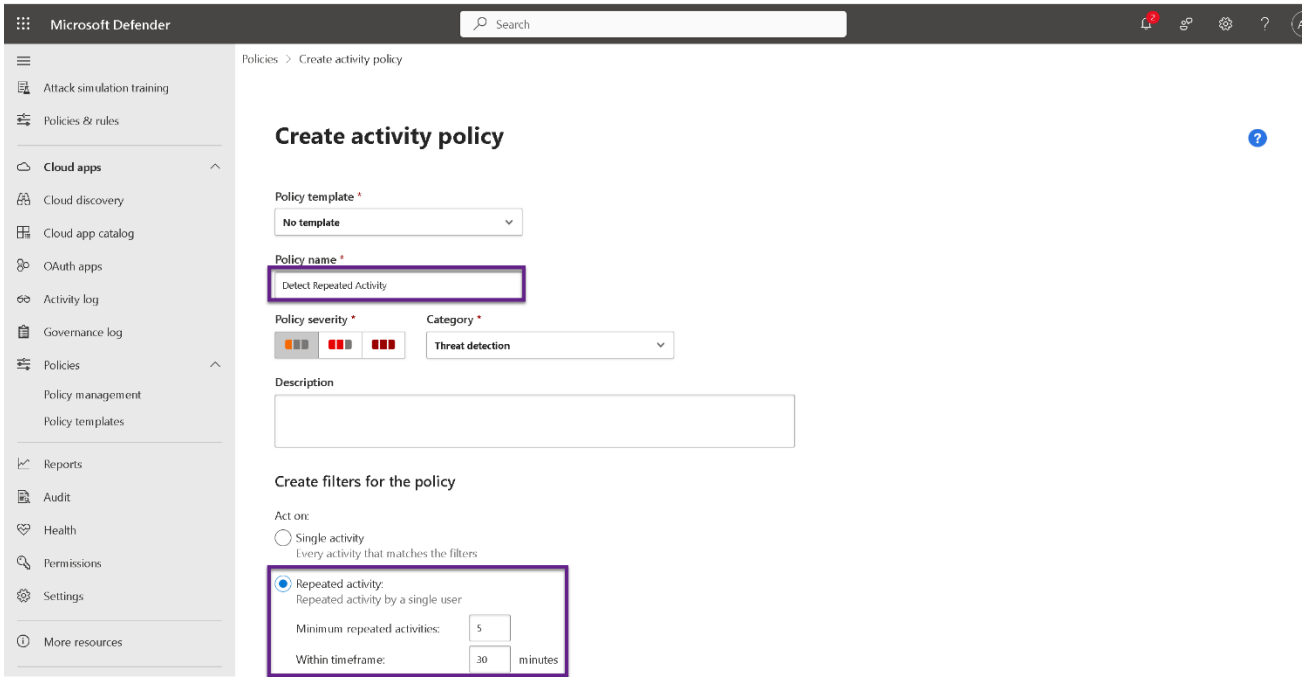
- Provides real-time session control over user activities within cloud applications.
- Example Use Case: Blocks downloads of sensitive files to unmanaged devices during a session.

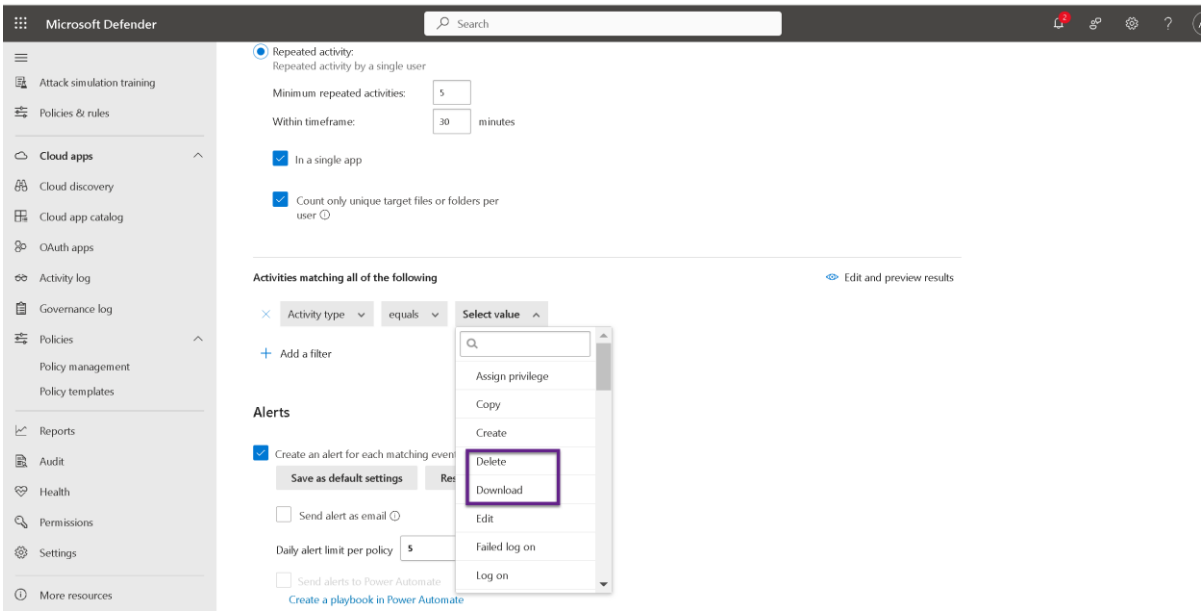
6. OAuth App Policy

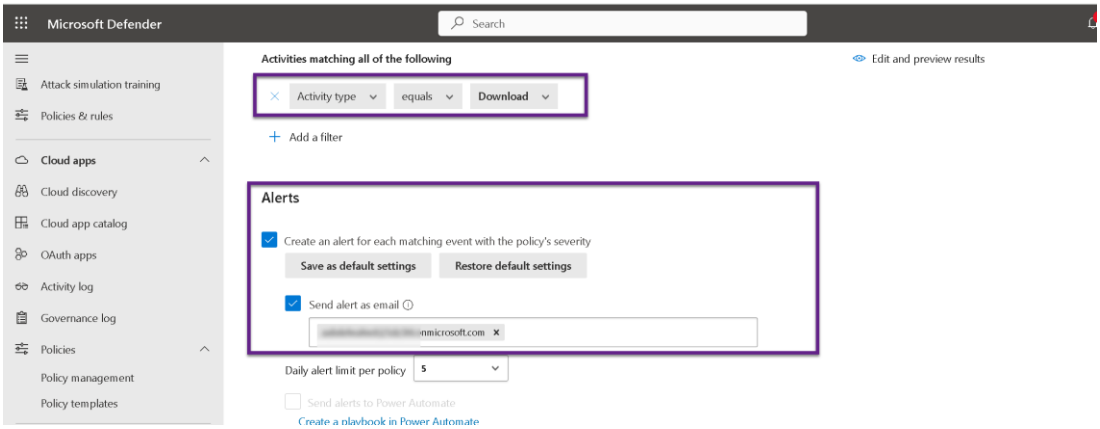
- Monitors and controls third-party OAuth app connections to cloud environments.
- Example Use Case: Detects and blocks malicious or unauthorized OAuth applications attempting to access corporate data.

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

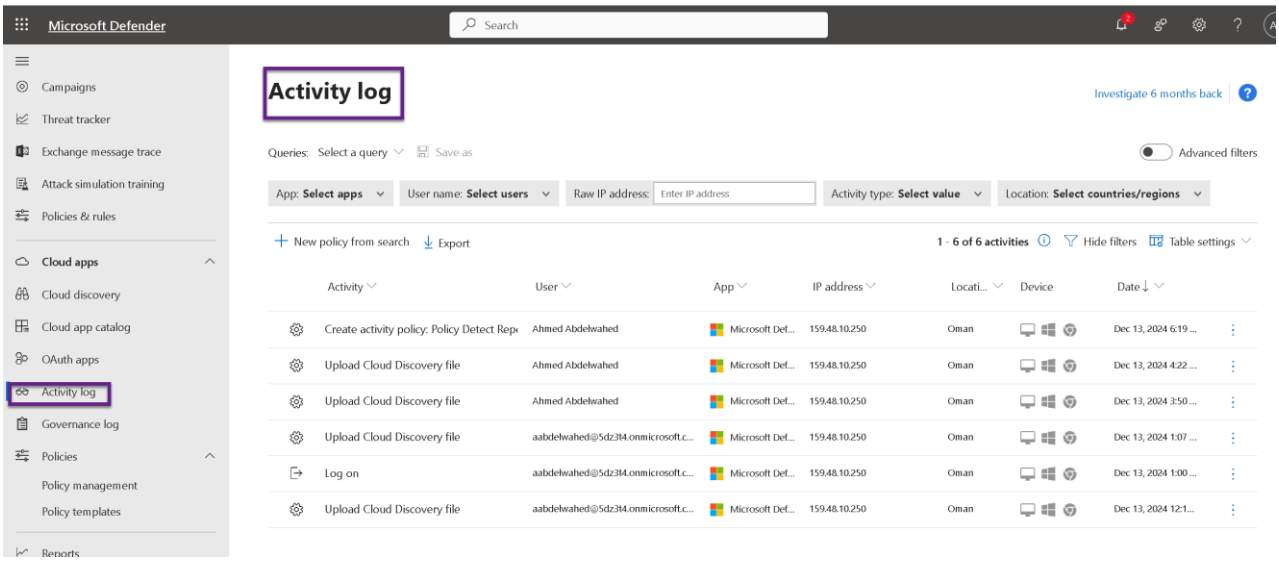



Microsoft Defender
Search
Policies > Create activity policy
Attack simulation training
Policies & rules
Cloud apps
Cloud discovery
Cloud app catalog
OAuth apps
Activity log
Governance log
Policies
Policy management
Policy templates
Reports
Audit
Health
Permissions
Settings
More resources
Create activity policy
Policy template *
No template
Policy name *
Detect Repeated Activity
Policy severity *
Category *
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

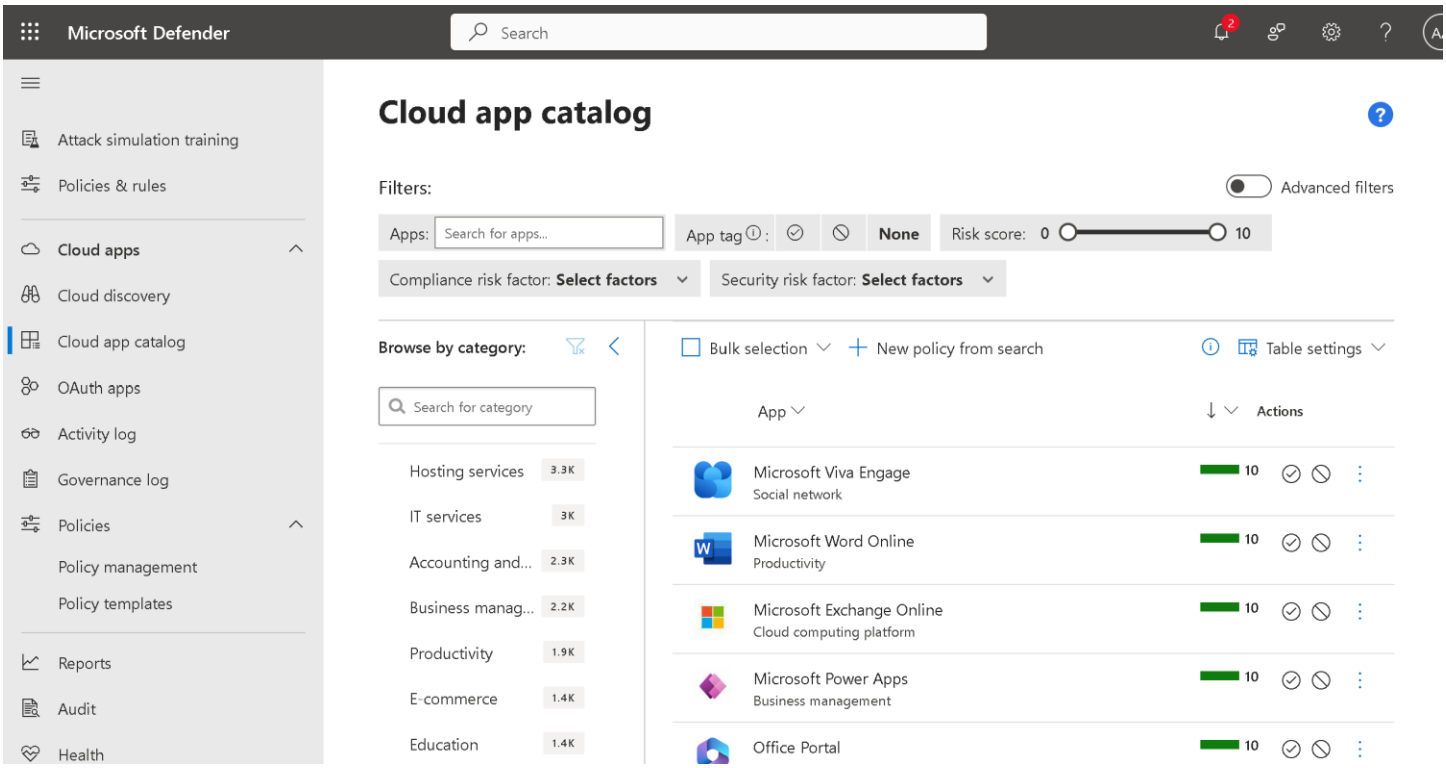

Microsoft Defender
Search
Repeated activity:
Repeated activity by a single user
Minimum repeated activities: 5
Within timeframe: 30 minutes
In a single app
Count only unique target files or folders per user
Activities matching all of the following
Edit and preview results
Activity type
equals
Select value
Add a filter
Assign privilege
Copy
Create
Delete
Download
Edit
Failed log on
Log on
Alerts
Create an alert for each matching event
Save as default settings
Send alert as email
Daily alert limit per policy 5
Send alerts to Power Automate
Create a playbook in Power Automate


Microsoft Defender
Search
Activities matching all of the following
Edit and preview results
Activity type
equals
Download
Add a filter
Alerts
Create an alert for each matching event with the policy's severity
Save as default settings
Restore default settings
Send alert as email
Daily alert limit per policy 5
Send alerts to Power Automate
Create a playbook in Power Automate

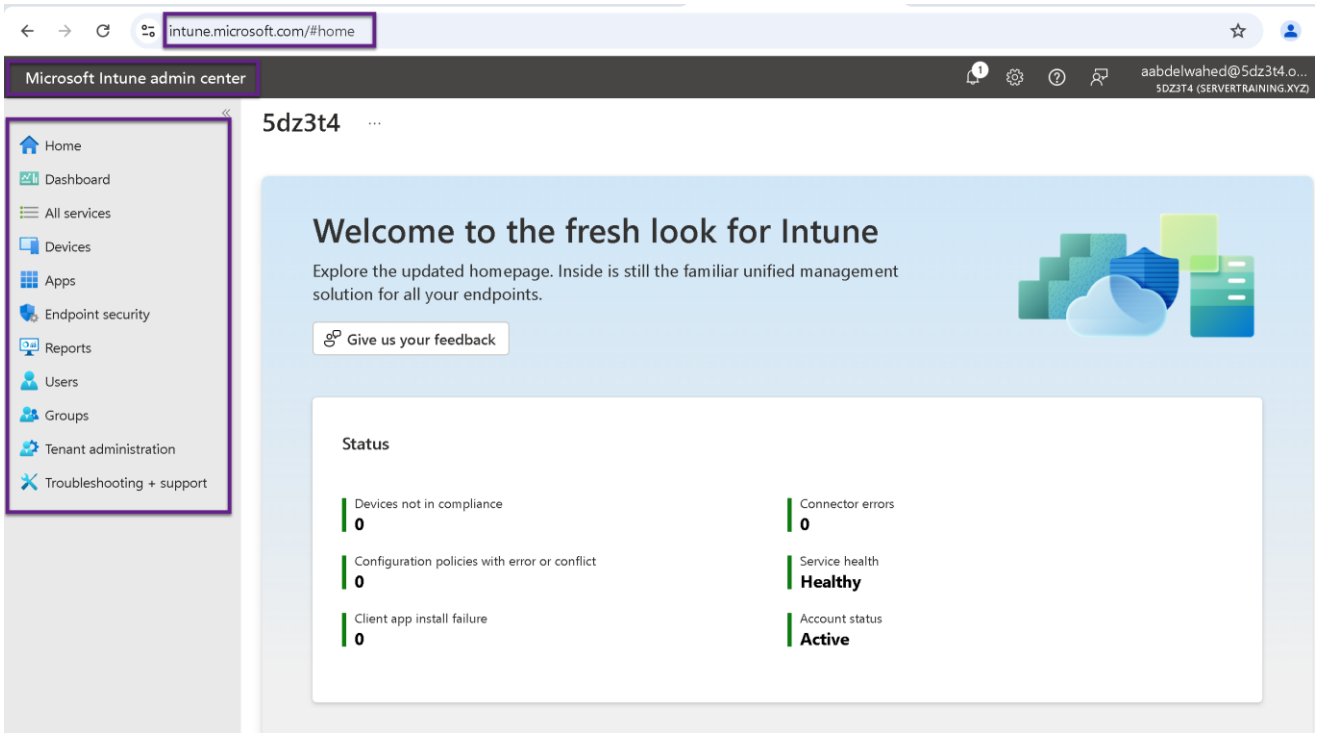
Activity log



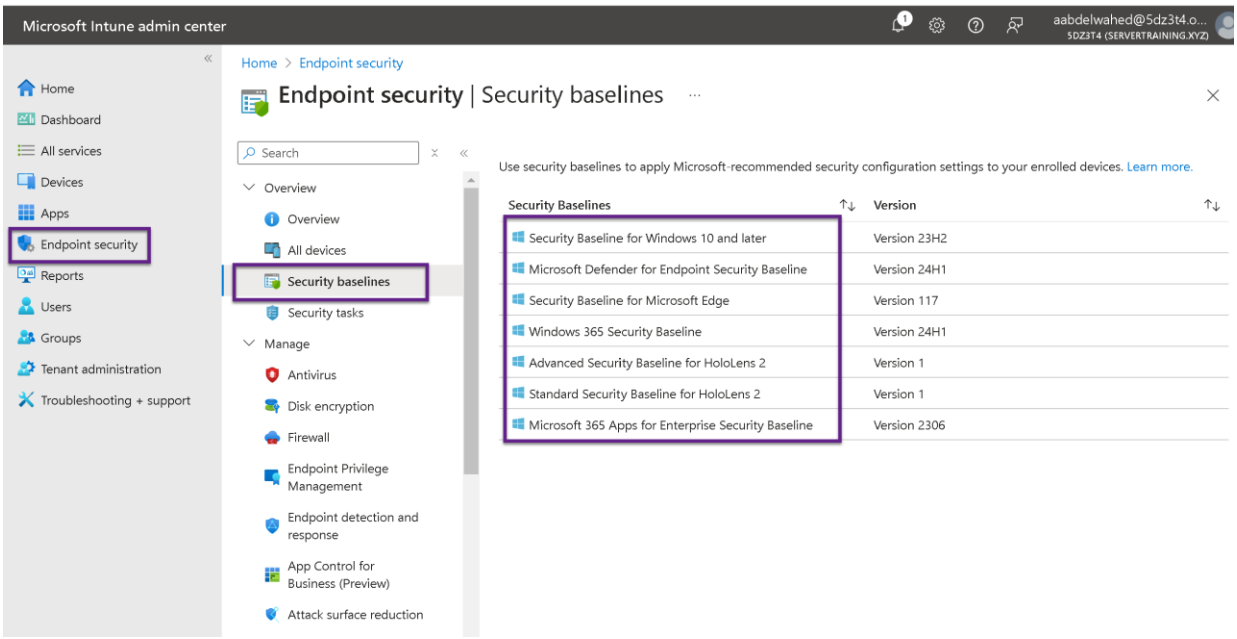
Cloud App Catalog



Microsoft Defender for Endpoint

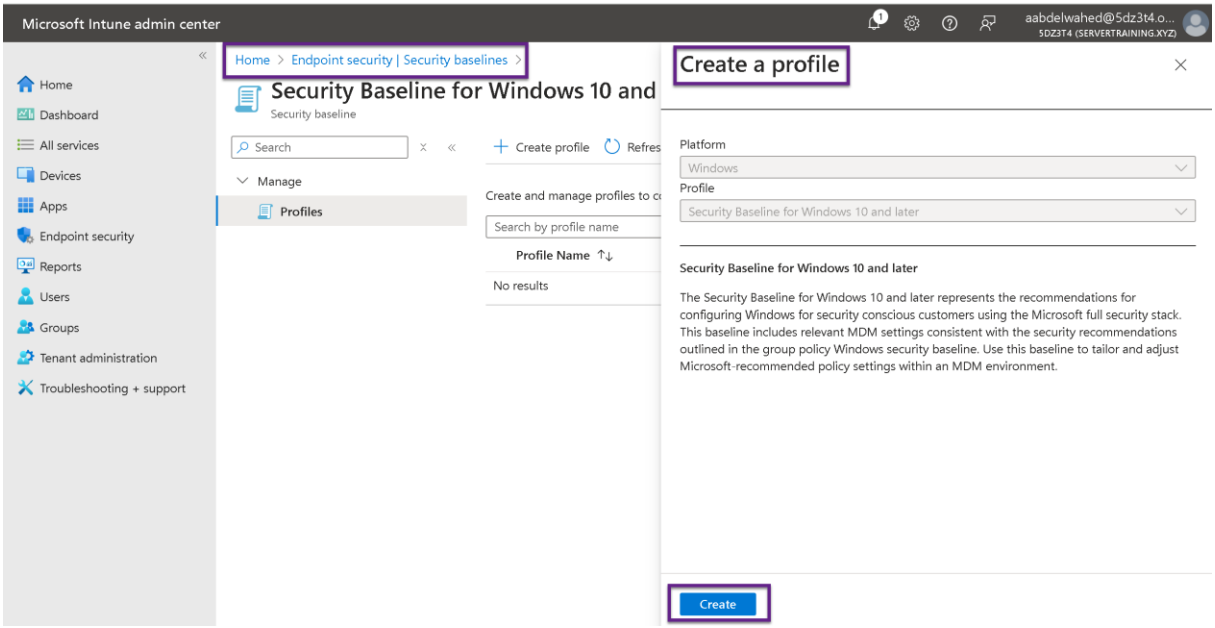


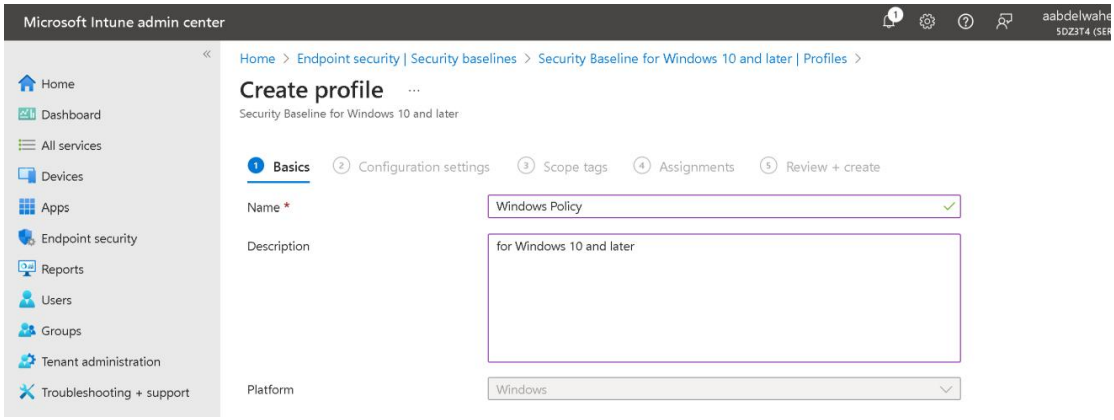
The **Endpoint Security | Security Baselines** section in **Microsoft Intune** provides pre-configured security settings recommended by Microsoft for different scenarios. These baselines help organizations quickly apply consistent and secure configurations to their enrolled devices without needing to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

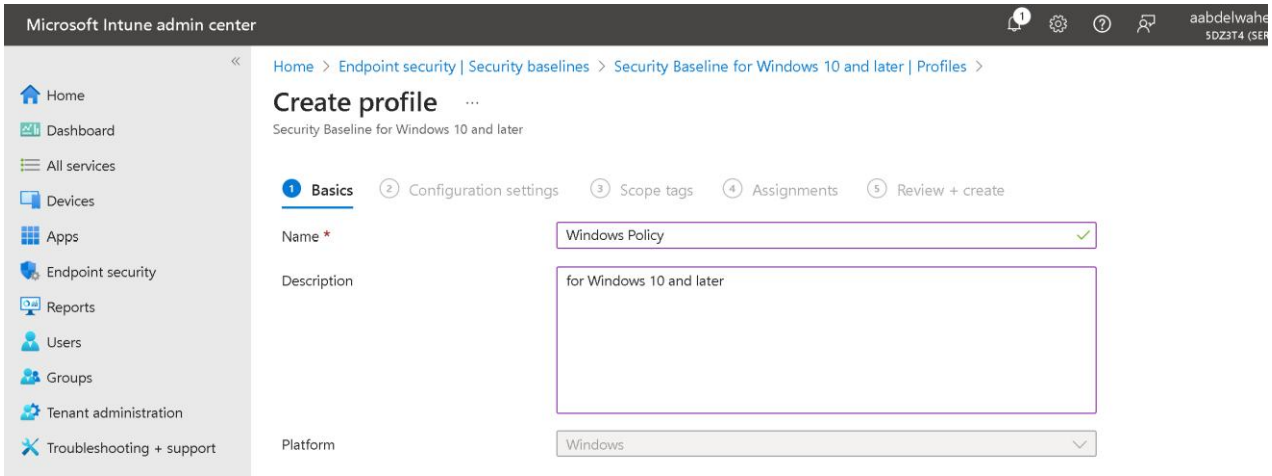


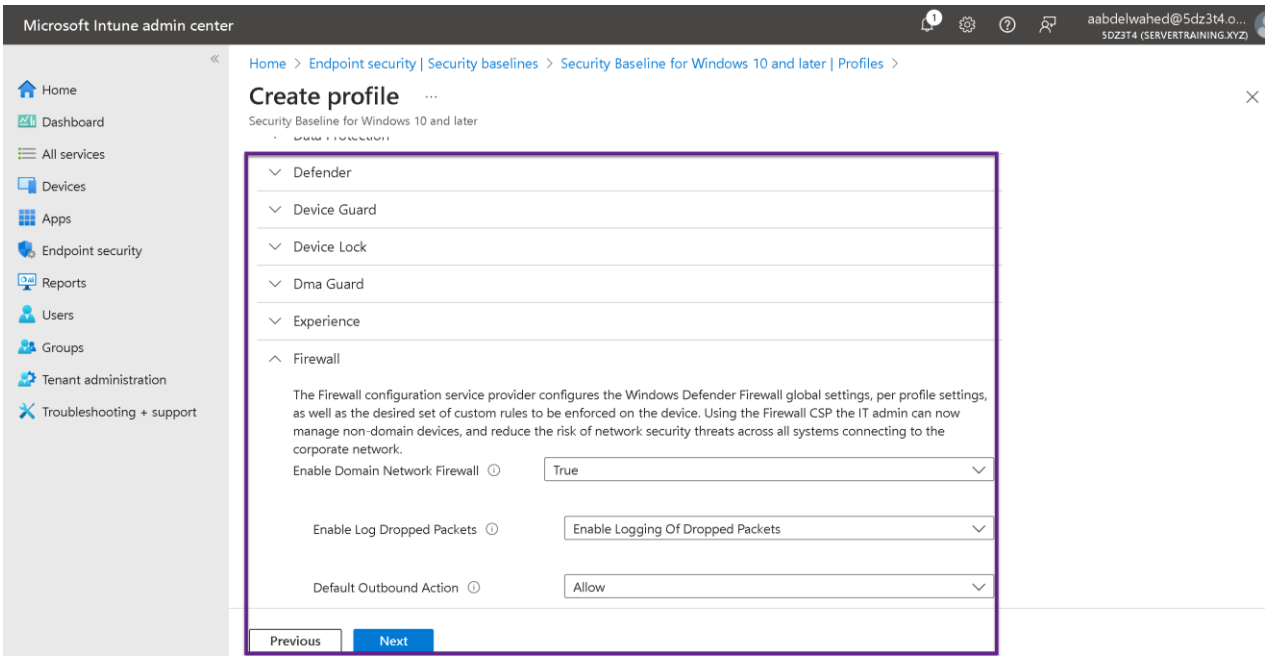
Create Security Baselines for windows 10 and later

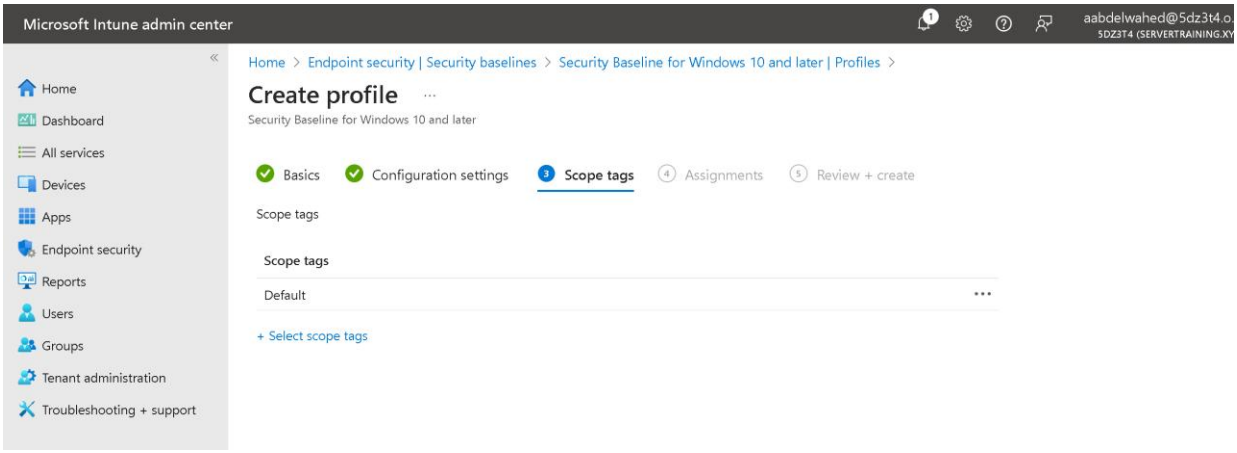
To configure and apply preset settings to Windows 10 and later devices using the Security Baseline for Windows 10 and later, follow these steps in the Microsoft Intune Admin Center:

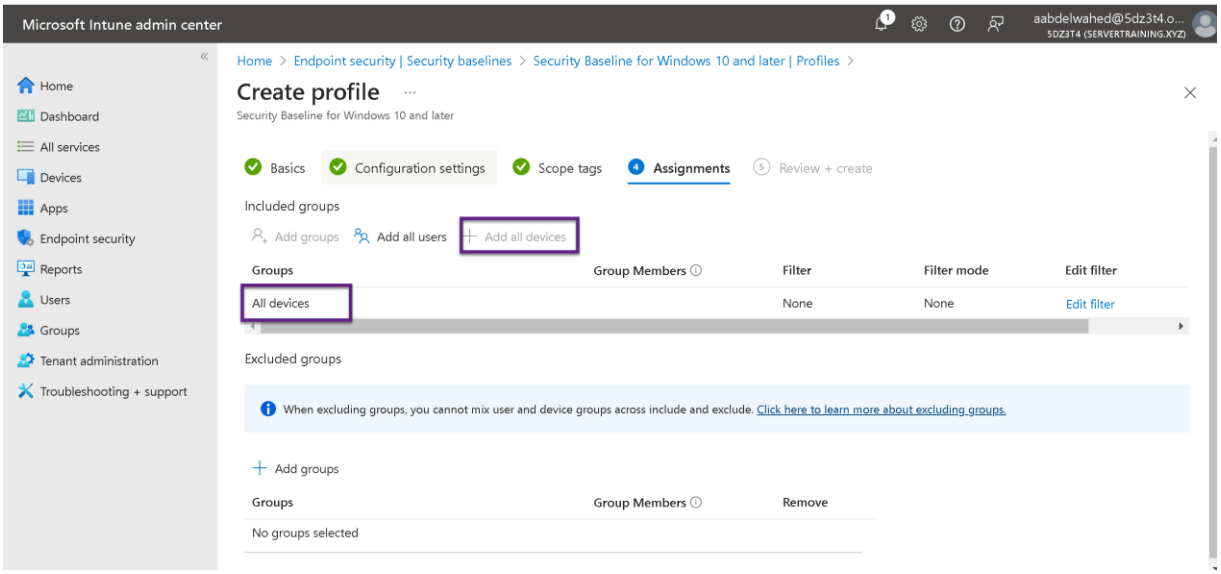


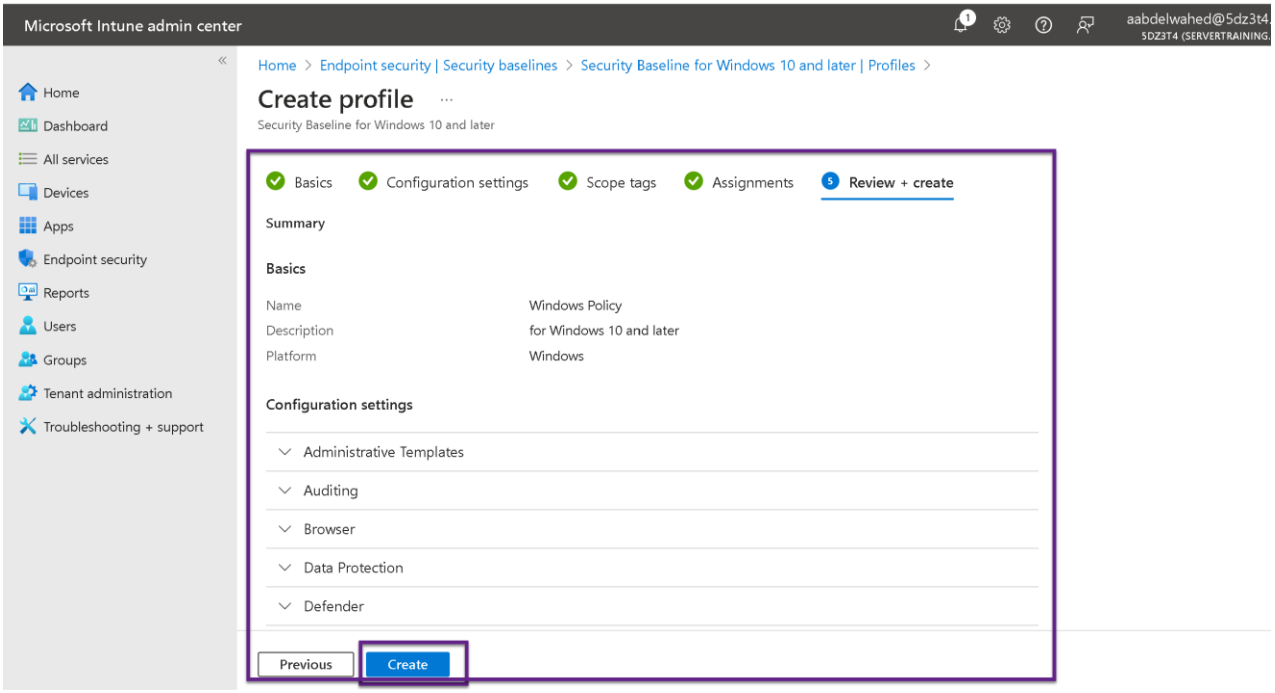




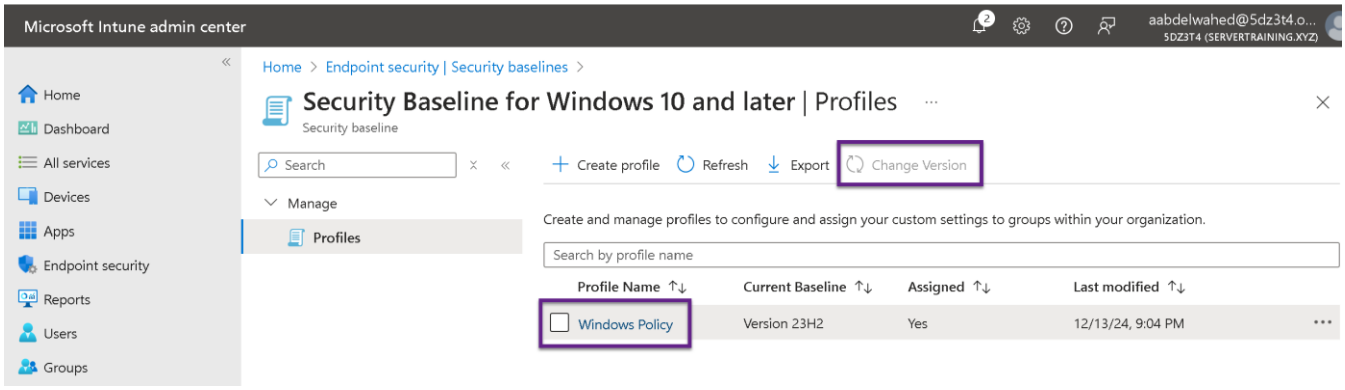

Microsoft Intune admin center
aabdelwahed@5dz3t4.o...
5DZ3T4 (SERVERTRAINING.XYZ)
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Security baselines > Security Baseline for Windows 10 and later | Profiles >
Create profile
Security Baseline for Windows 10 and later
Defender
Device Guard
Device Lock
Dma Guard
Experience
Firewall
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.
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
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Security baselines > Security Baseline for Windows 10 and later | Profiles >
Create profile
Security Baseline for Windows 10 and later
Basics
Configuration settings
Scope tags
Assignments
Review + create
Scope tags
Scope tags
Default
+ Select scope tags

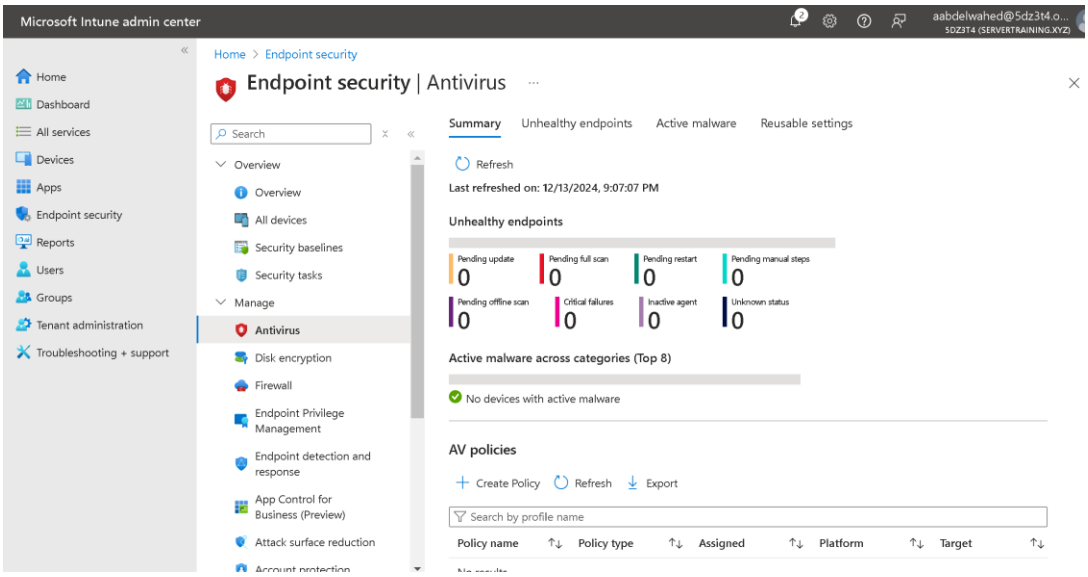

Microsoft Intune admin center
aabdelwahed@5dz3t4.o...
5DZ3T4 (SERVERTRAINING.XYZ)
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Security baselines > Security Baseline for Windows 10 and later | Profiles >
Create profile
Security Baseline for Windows 10 and later
Basics
Configuration settings
Scope tags
Assignments
Review + create
Included groups
Add groups
Add all users
Add all devices
Groups
Group Members
Filter
Filter mode
Edit filter
All devices
None
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
Group Members
Remove
No groups selected



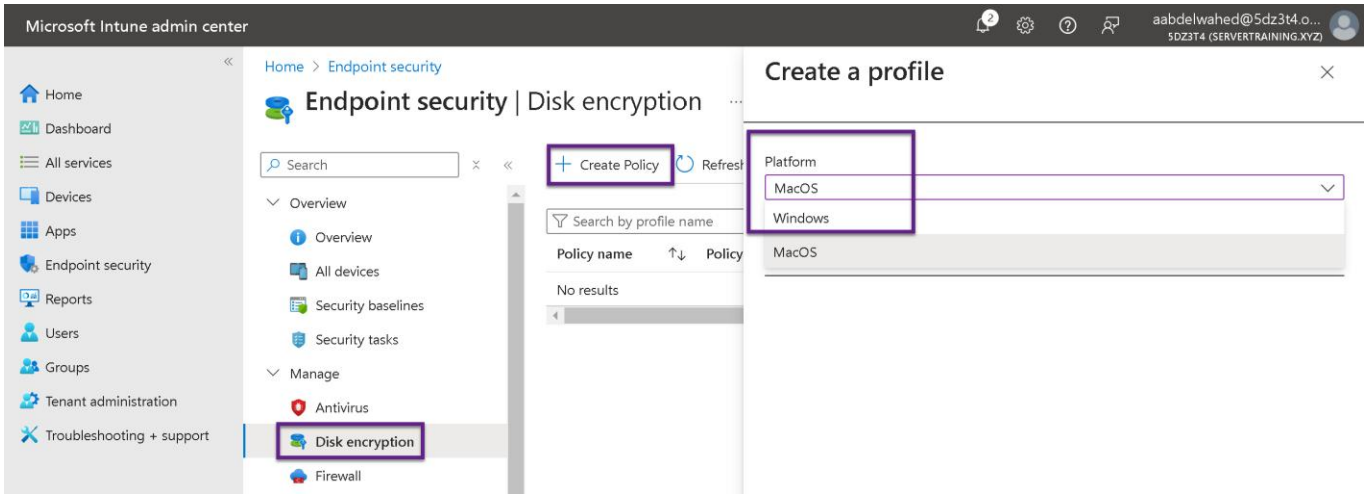
Any Microsoft coming updates, you can update your policy from the below option



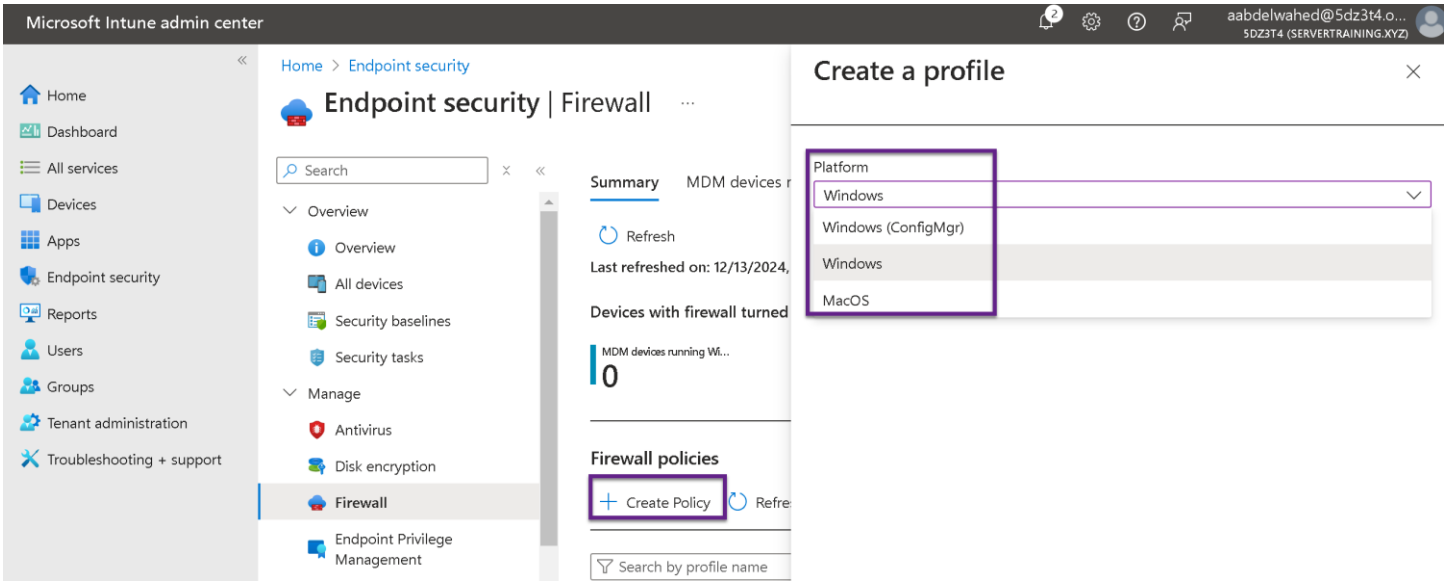
Managing Antivirus

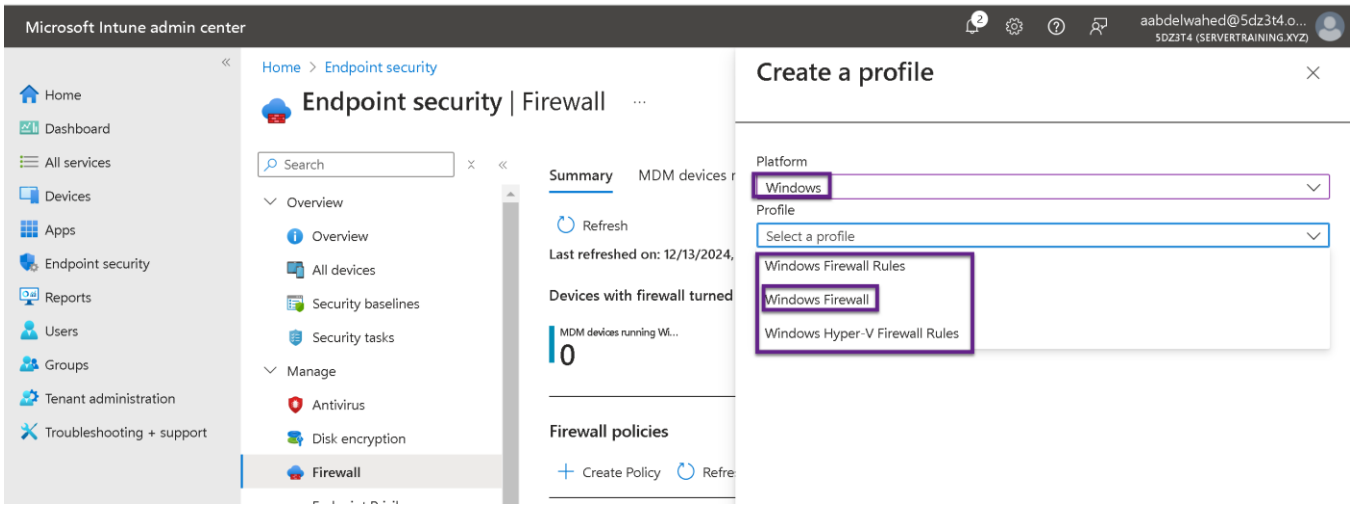


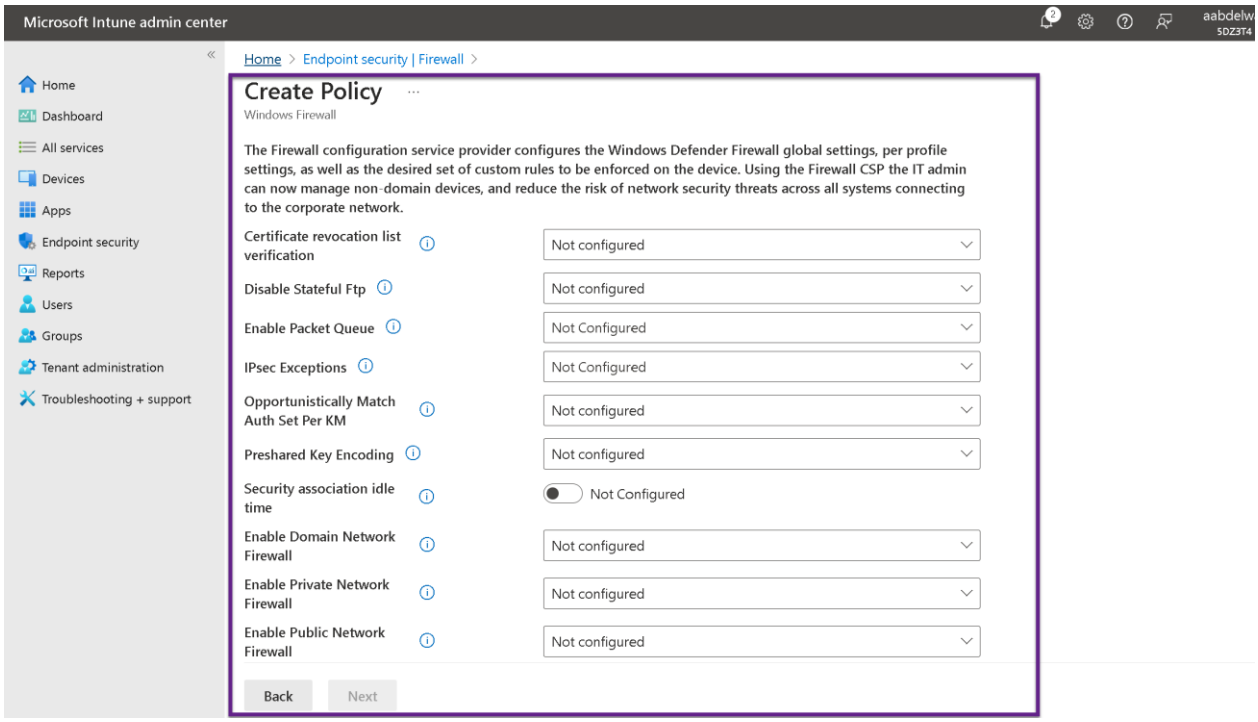
Disk Encryption



Managing and Monitoring Firewall

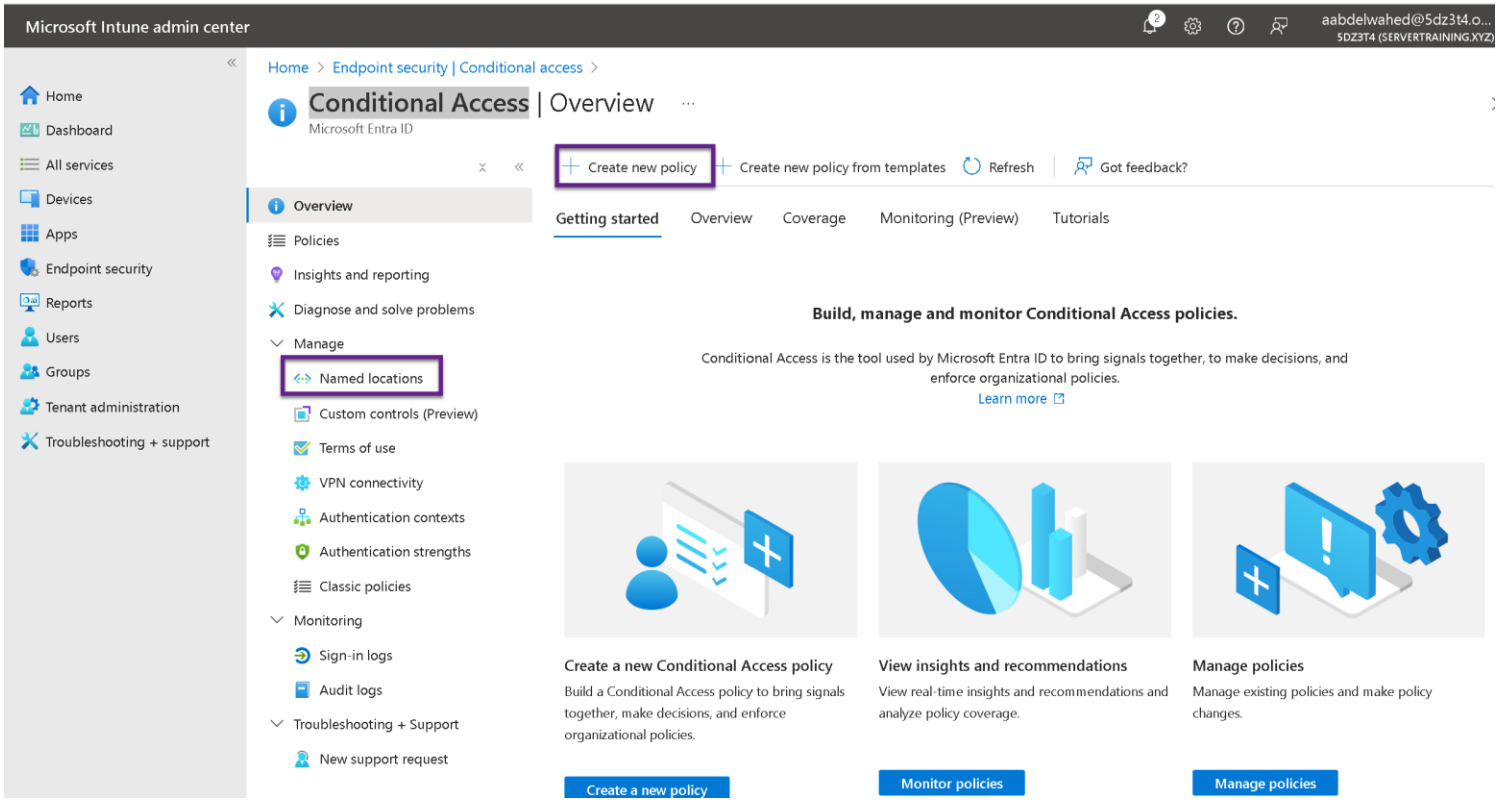






Conditional Access

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.



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

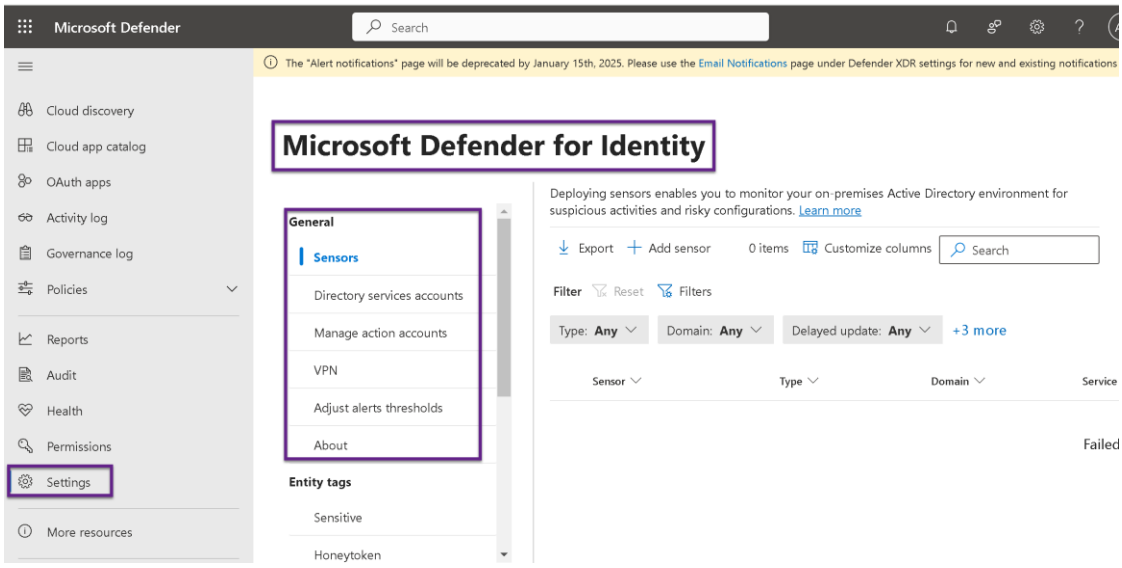
- Generates real-time alerts for detected threats or suspicious activities.
- Provides detailed forensic reports for security investigations.

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 **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

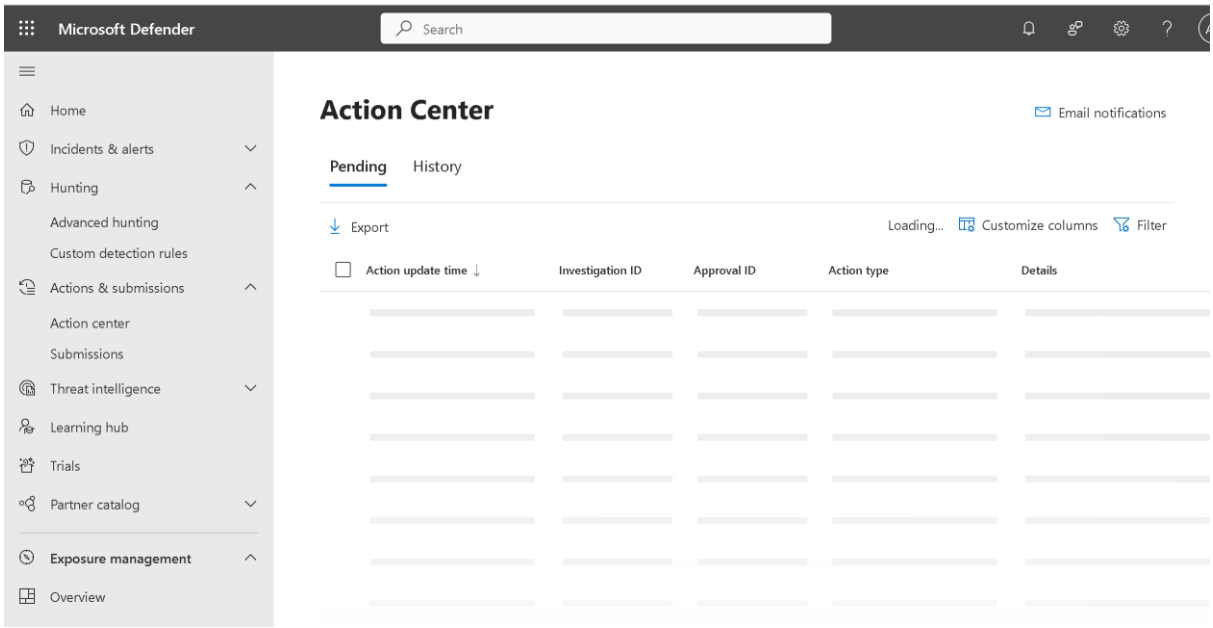
- Provides a detailed timeline of events leading to the alert.
- Displays affected users, devices, files, and applications to aid investigation.

6. Integration Across Defender Products

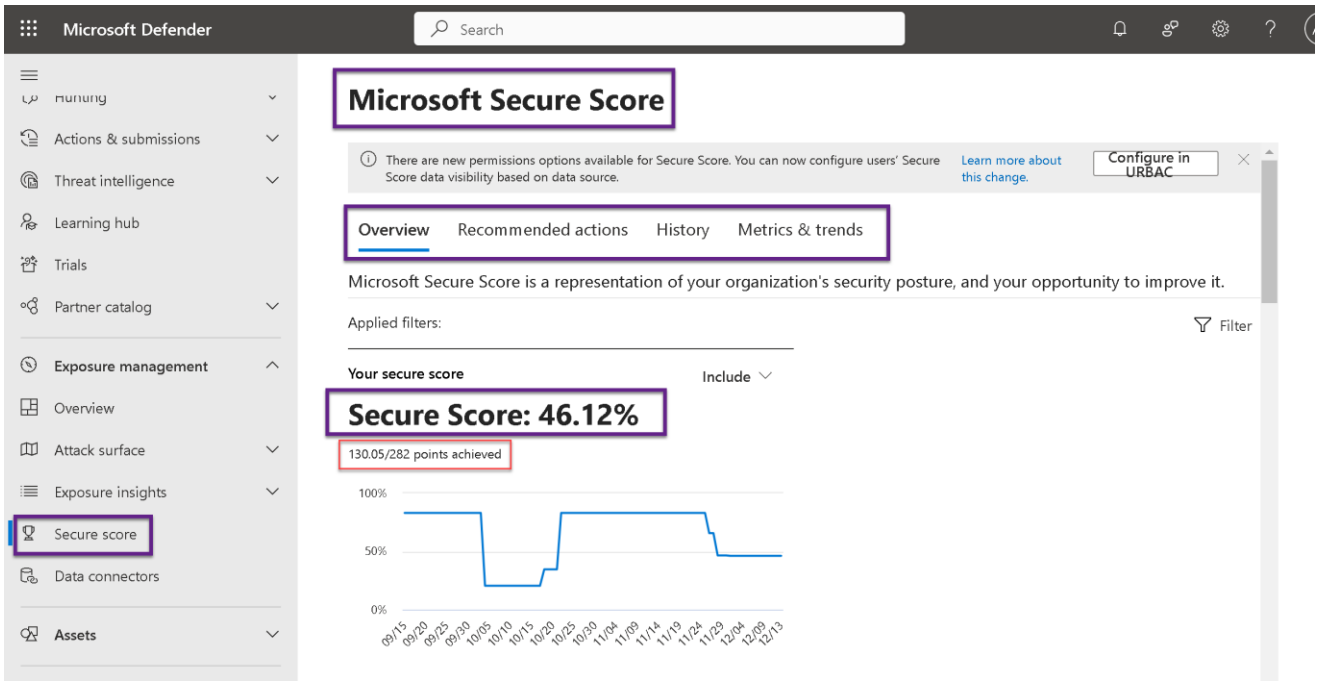
- Works seamlessly with Defender for Endpoint, Defender for Identity, Defender for Cloud Apps, and Defender for Office 365.
- Correlates alerts from different sources for comprehensive incident handling.

7. Audit and Reporting

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



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.



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

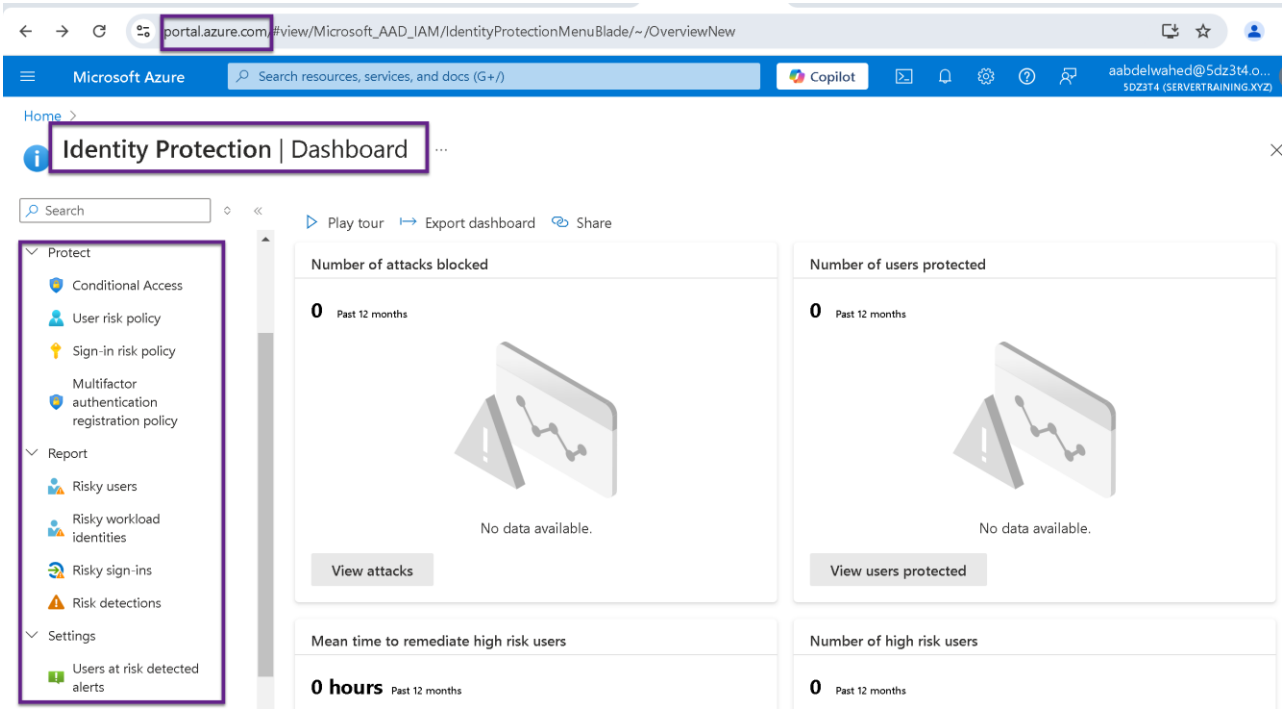
- Enables automatic responses to detected risks using **User Risk Policies** and **Sign-In Risk Policies**:
  - Force **password reset** for compromised accounts.
  - Require **multi-factor authentication (MFA)** for high-risk sign-ins.
  - Block access based on certain conditions.

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.



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.

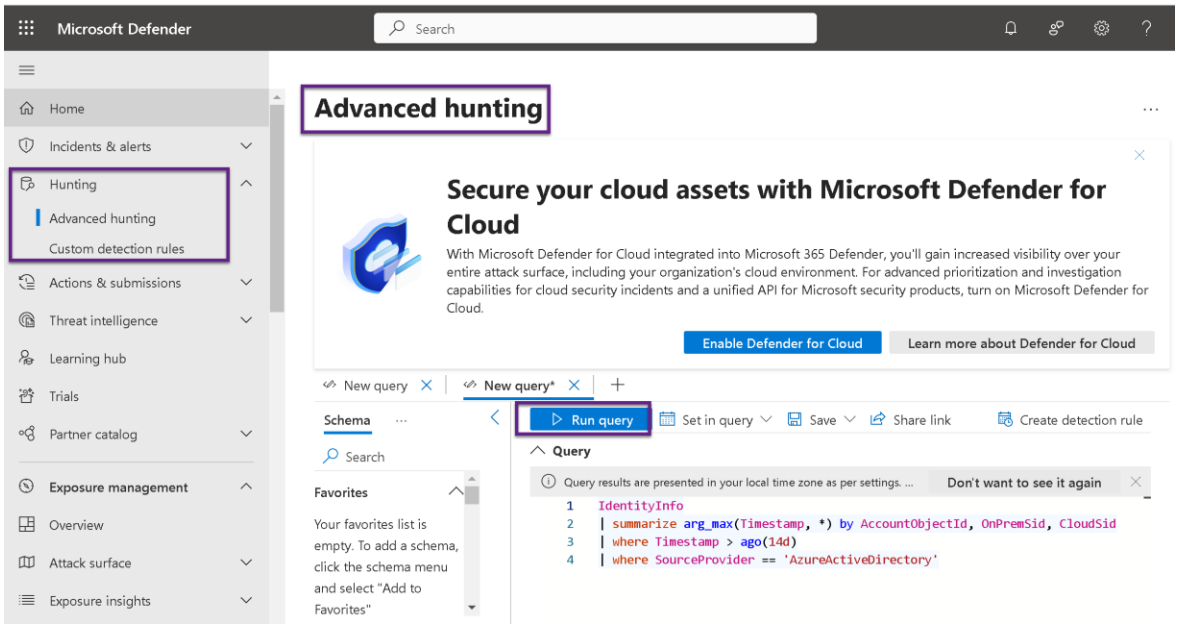
3. Monitor Identity Threats

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

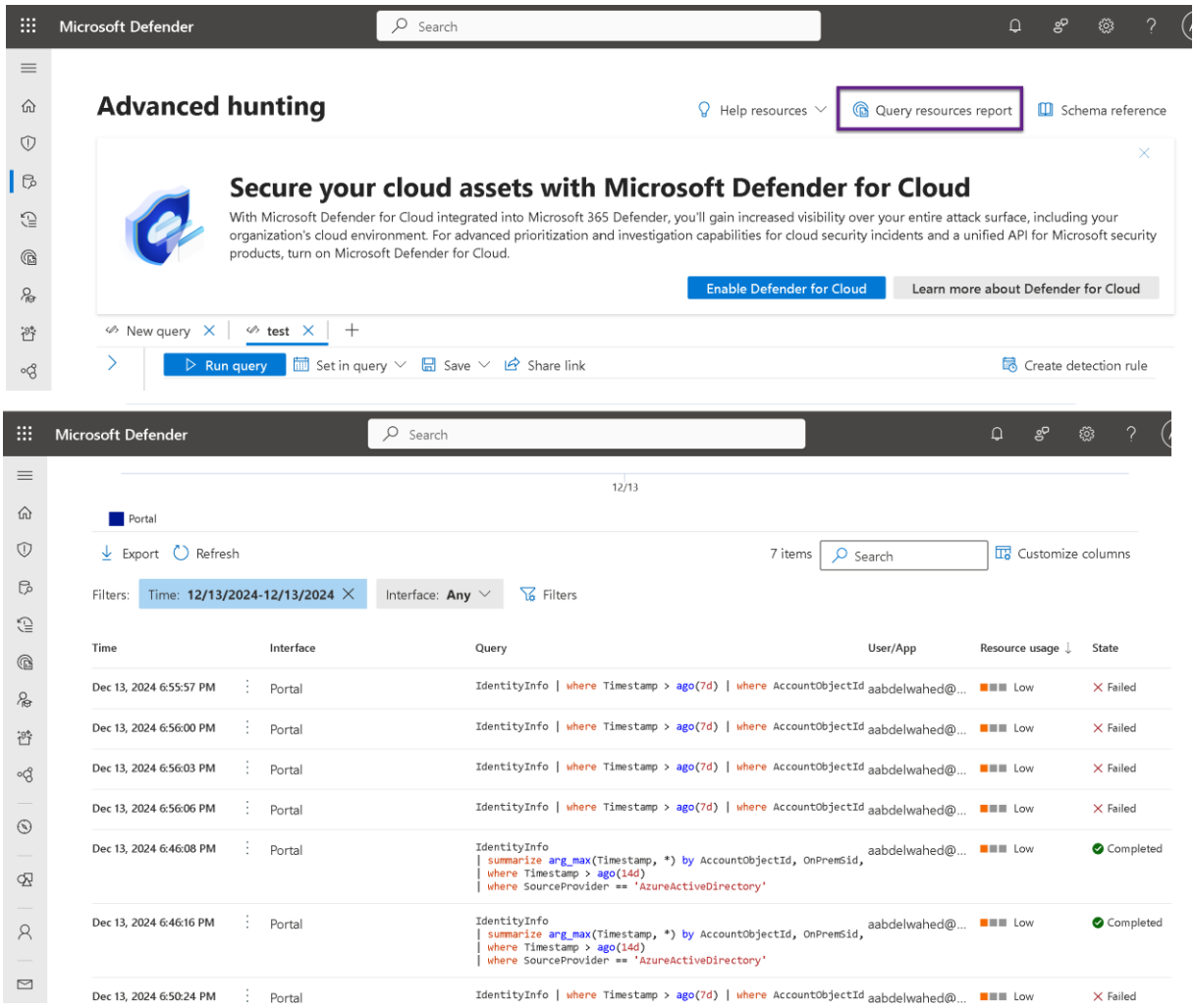
- Purpose: Monitor identity activities from Azure AD for potential threats.

4. Identifying attachments with specific patterns in their names

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



To see the result



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).

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

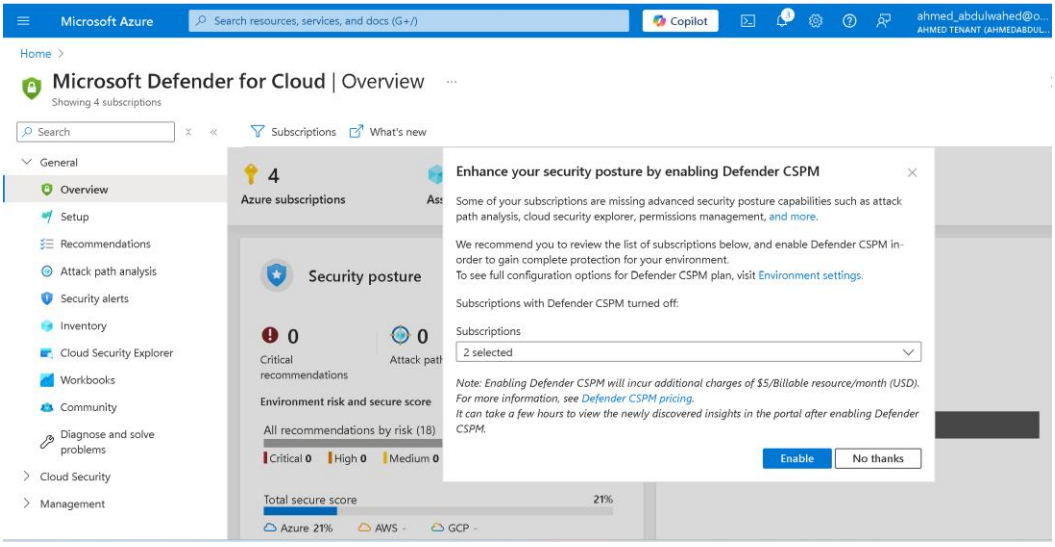
- Detects brute force attacks, unusual data exfiltration, and ransomware activity.
- Example: Monitor Azure SQL for suspicious query patterns.

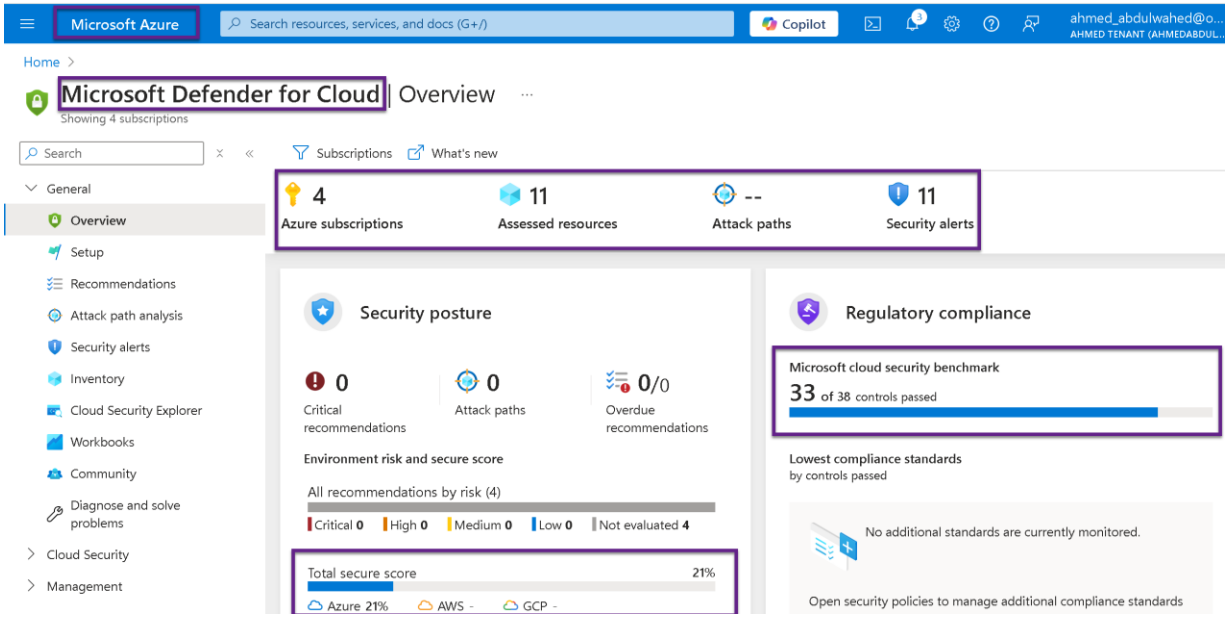
3. Compliance Management

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

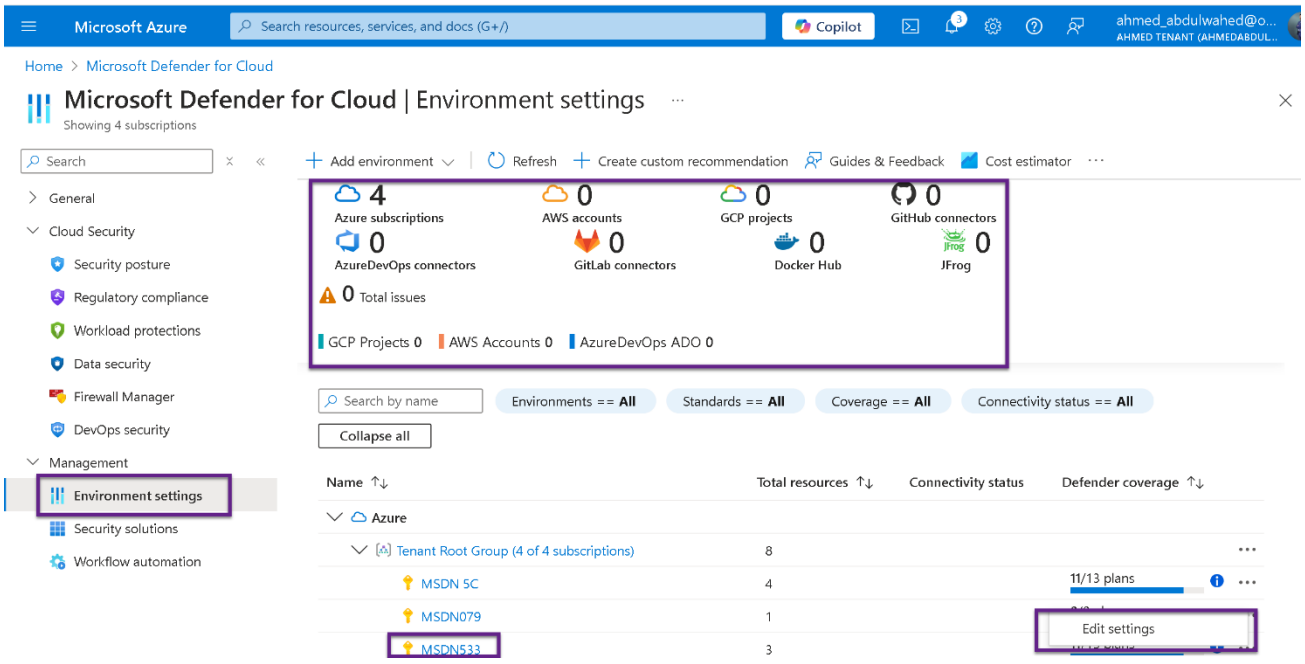
4. Hybrid Security

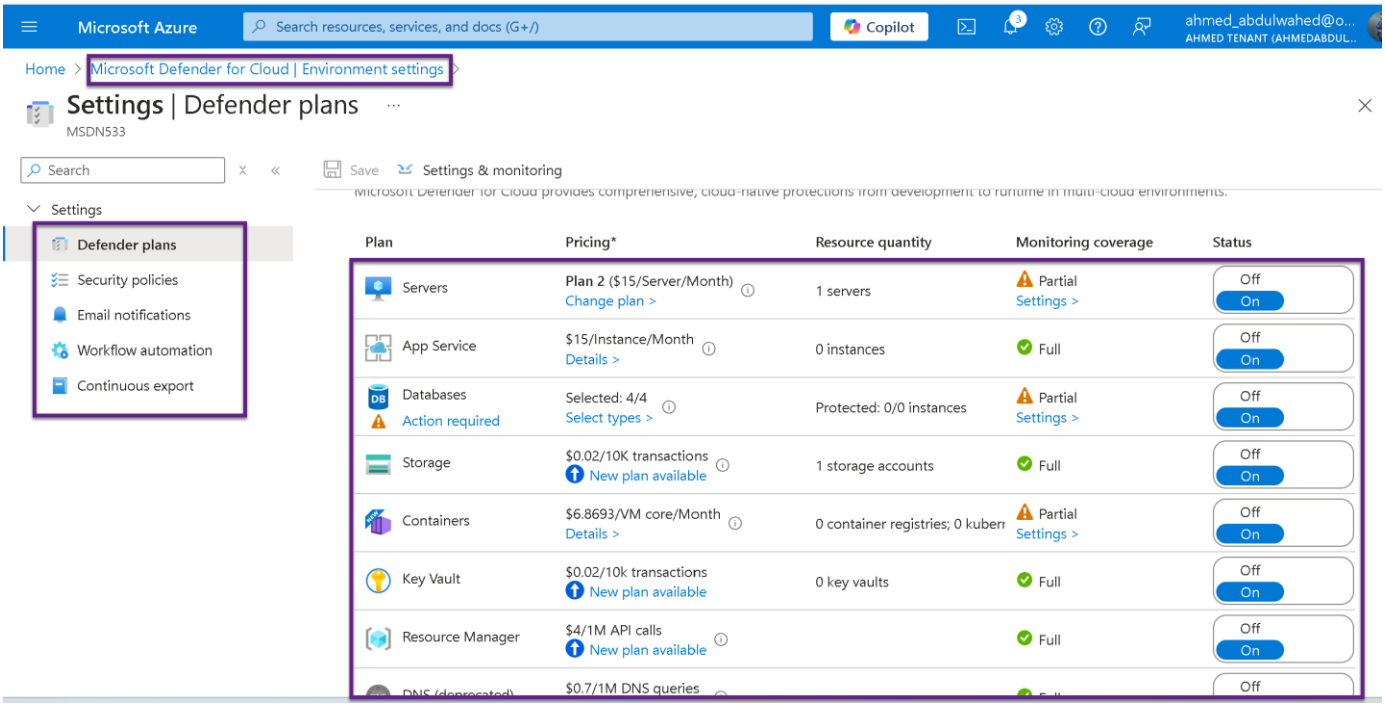
- Extend security monitoring to on-premises workloads and non-Azure clouds.
- Example: Use Azure Arc to protect AWS EC2 instances with Microsoft Defender.

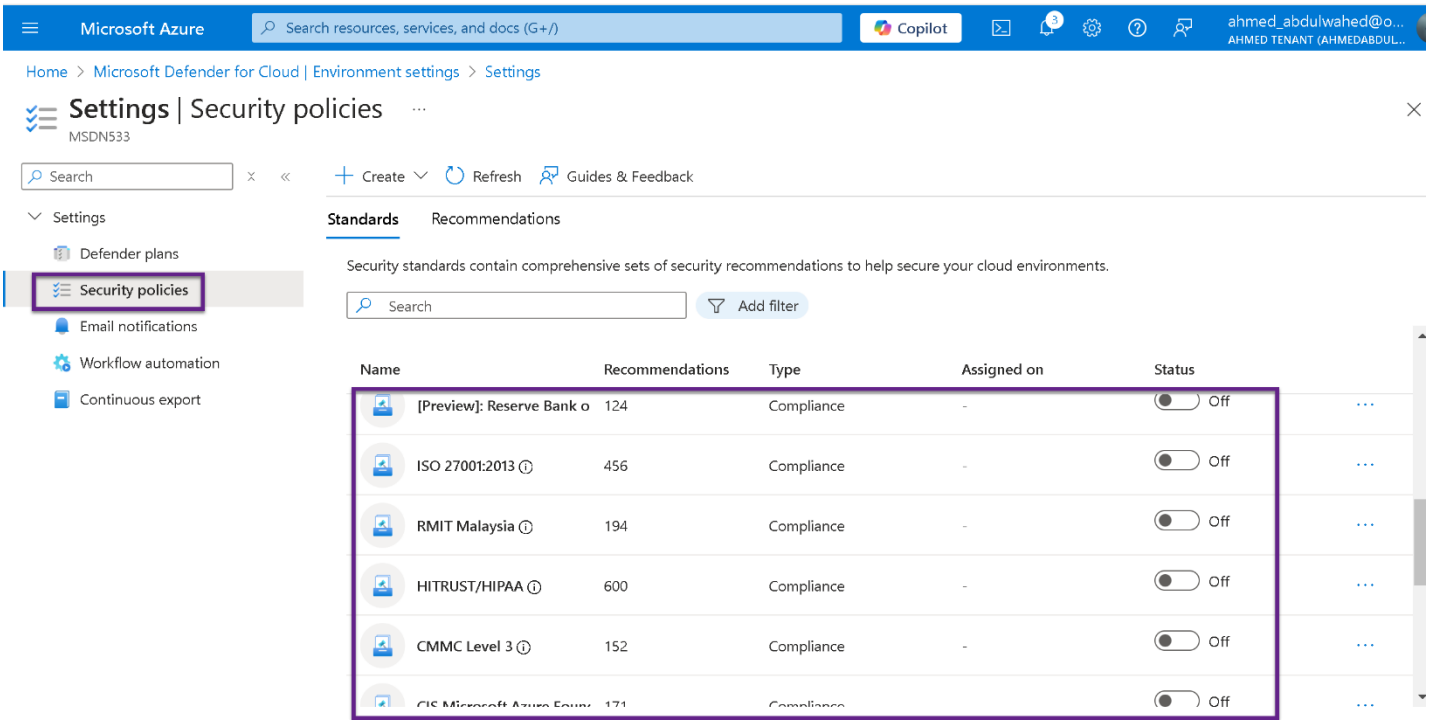




The **Environment Settings** page in **Microsoft Defender for Cloud** is where you configure and manage the security settings and integrations for your cloud environments, including Azure, AWS, Google Cloud (GCP), and other resources. This section provides a comprehensive overview of your environment's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

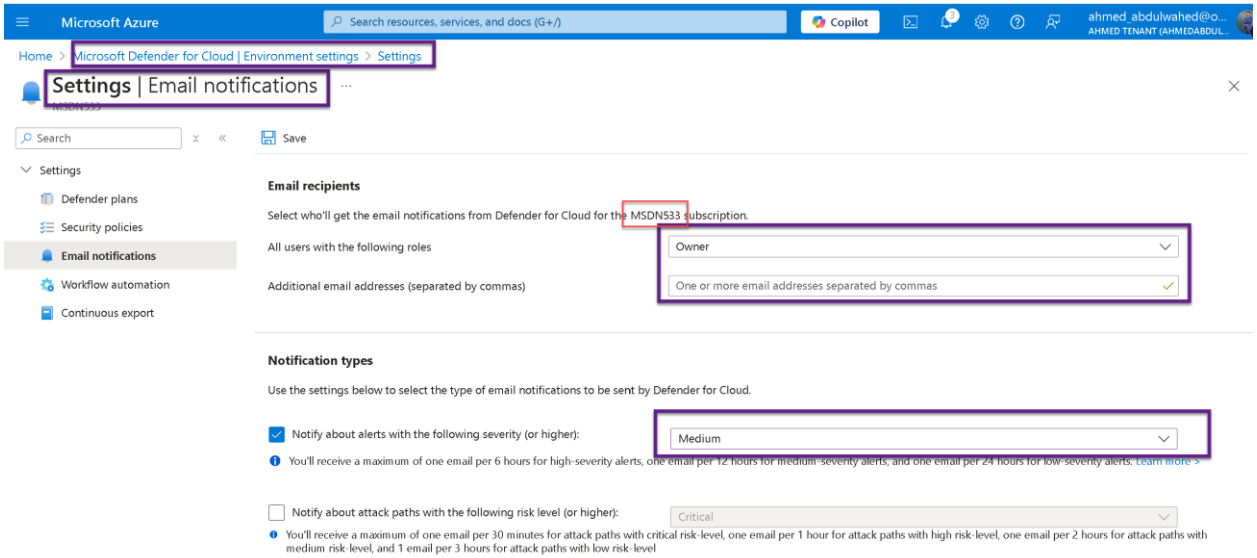



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ahmed_abdulwahed@o...
AHMED TENANT (AHMEDABDUL...
Home > Microsoft Defender for Cloud | Environment settings
Settings | Defender plans
MSDN533
Search
Save
Settings & monitoring
Settings
Defender plans
Security policies
Email notifications
Workflow automation
Continuous export
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
Databases
Action required
Selected: 4/4
Select types >
Protected: 0/0 instances
Partial
Settings >
Storage
$0.02/10K transactions
New plan available
1 storage accounts
Full
Containers
$6.8693/VM core/Month
Details >
0 container registries; 0 kuberr
Partial
Settings >
Key Vault
$0.02/10k transactions
New plan available
0 key vaults
Full
Resource Manager
$4/1M API calls
New plan available
Full
$0.7/1M DNS queries
Off

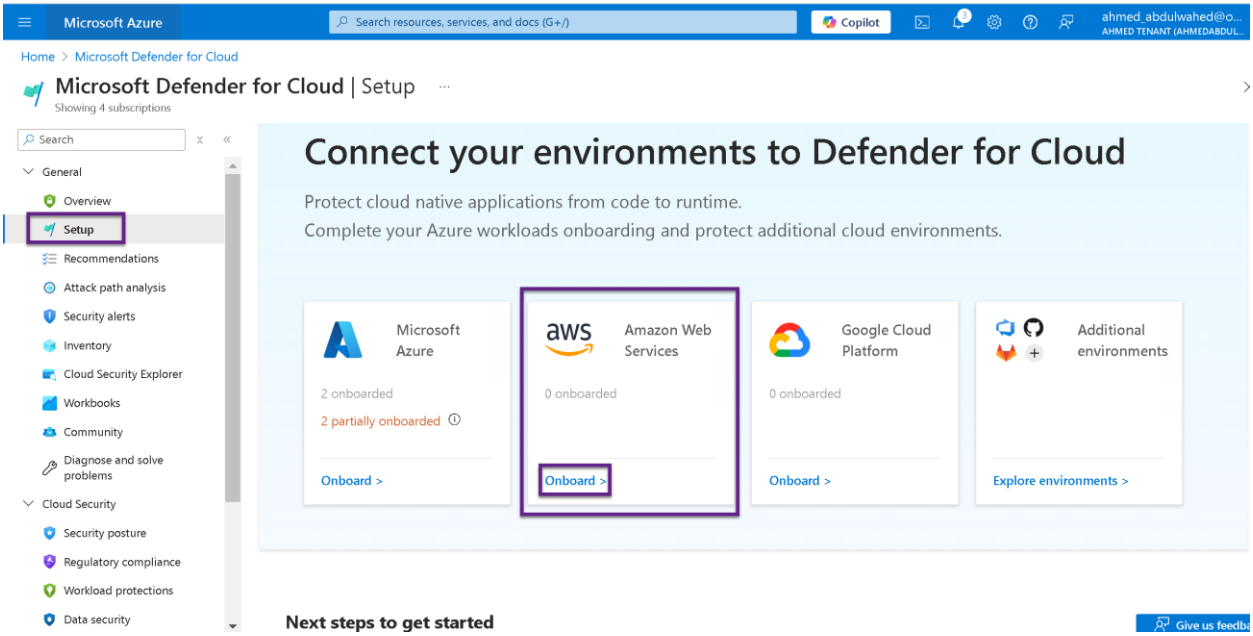

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ahmed_abdulwahed@o...
AHMED TENANT (AHMEDABDUL...
Home > Microsoft Defender for Cloud | Environment settings > Settings
Settings | Security policies
MSDN533
Search
Create
Refresh
Guides & Feedback
Settings
Defender plans
Security policies
Email notifications
Workflow automation
Continuous export
Standards
Recommendations
Security standards contain comprehensive sets of security recommendations to help secure your cloud environments.
Search
Add filter
Name
Recommendations
Type
Assigned on
Status
[Preview]: Reserve Bank o
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
Off

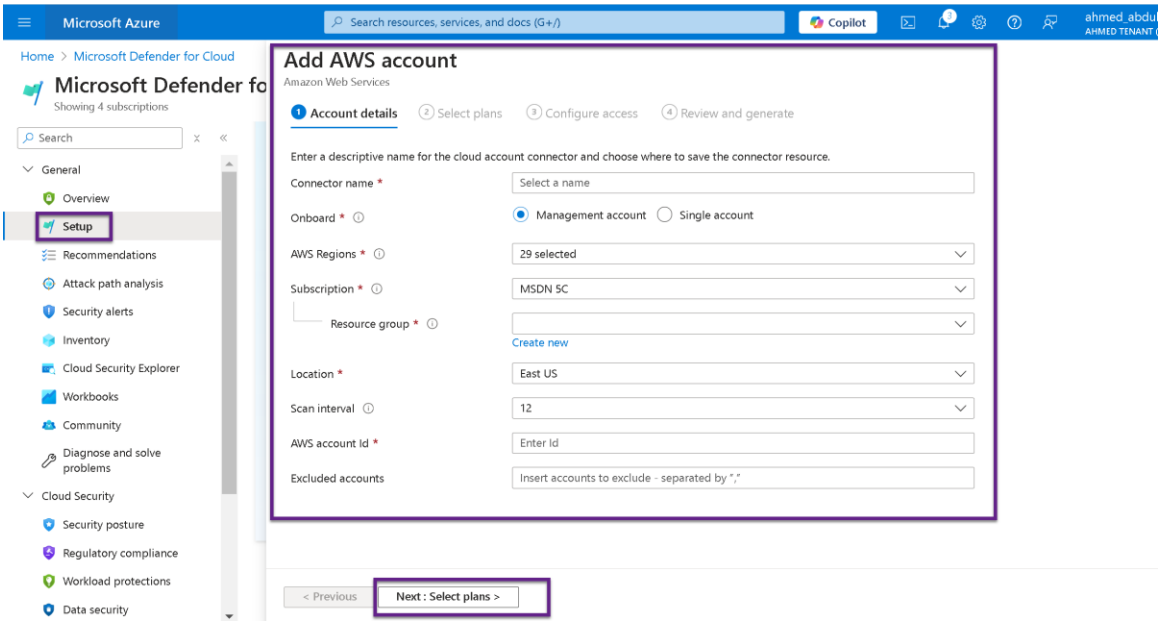
Email notifications

- 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.

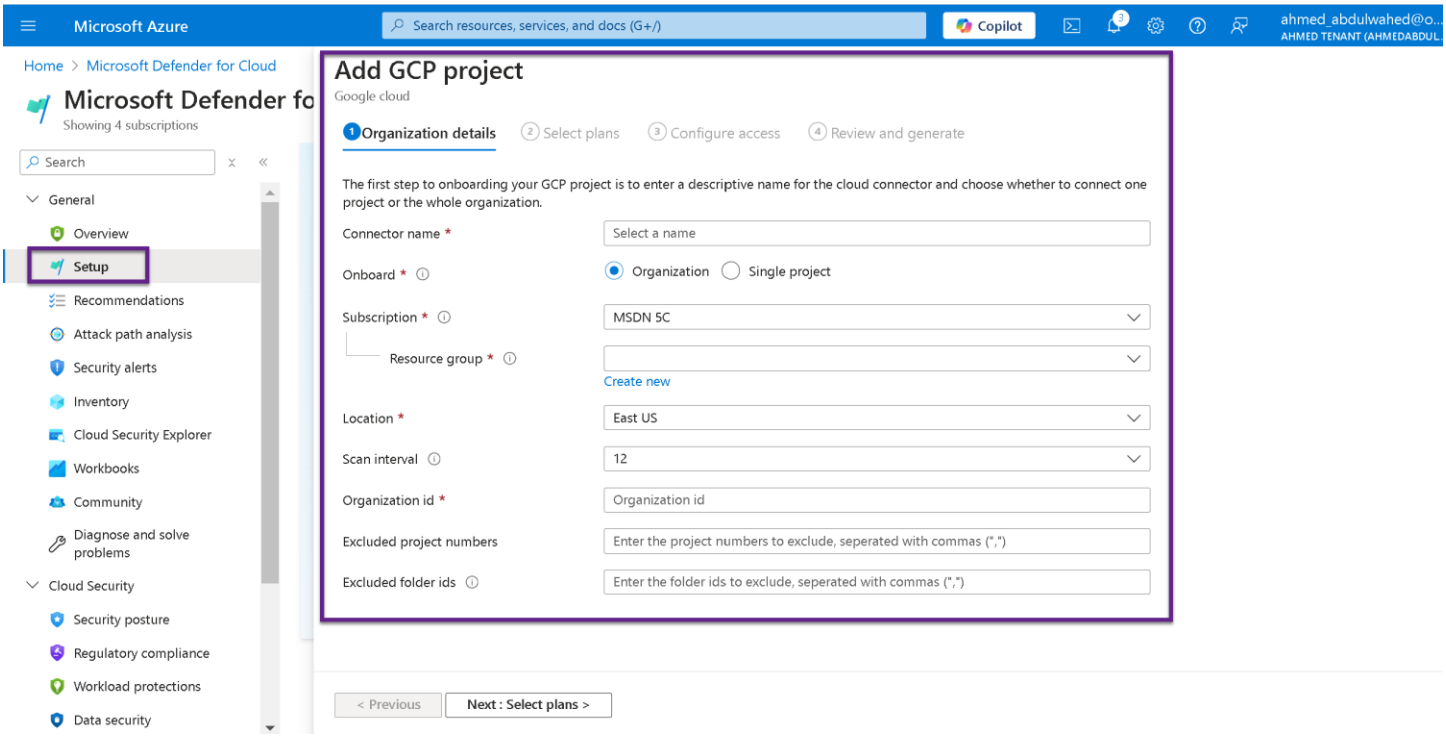


Microsoft Defender for AWS

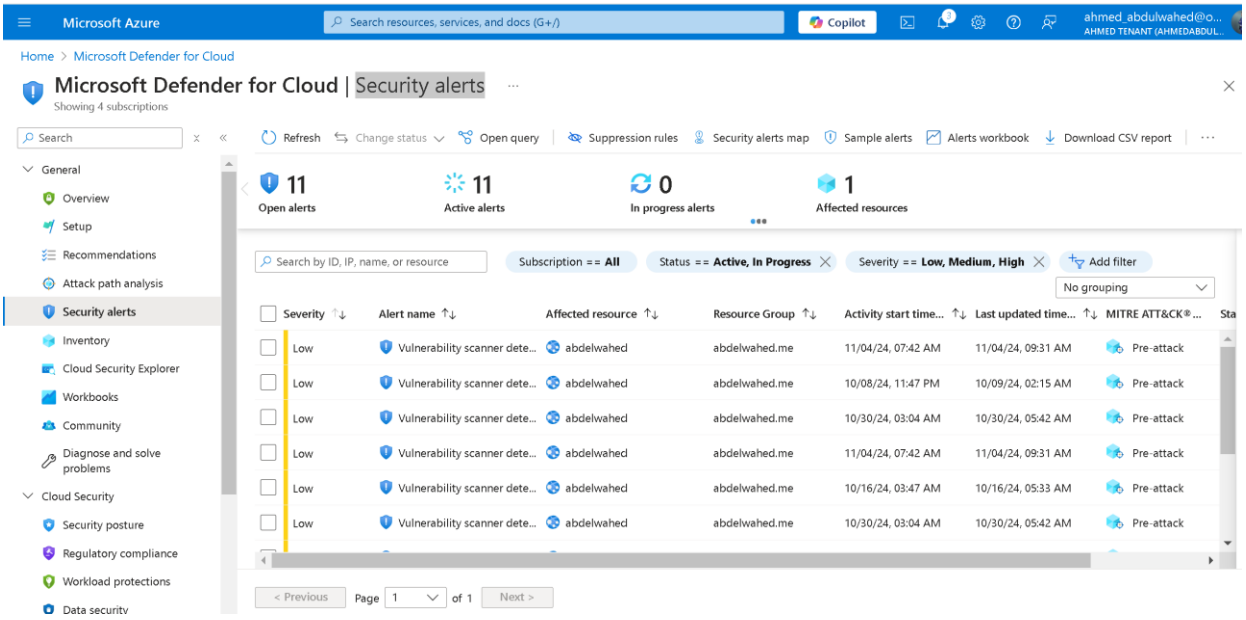




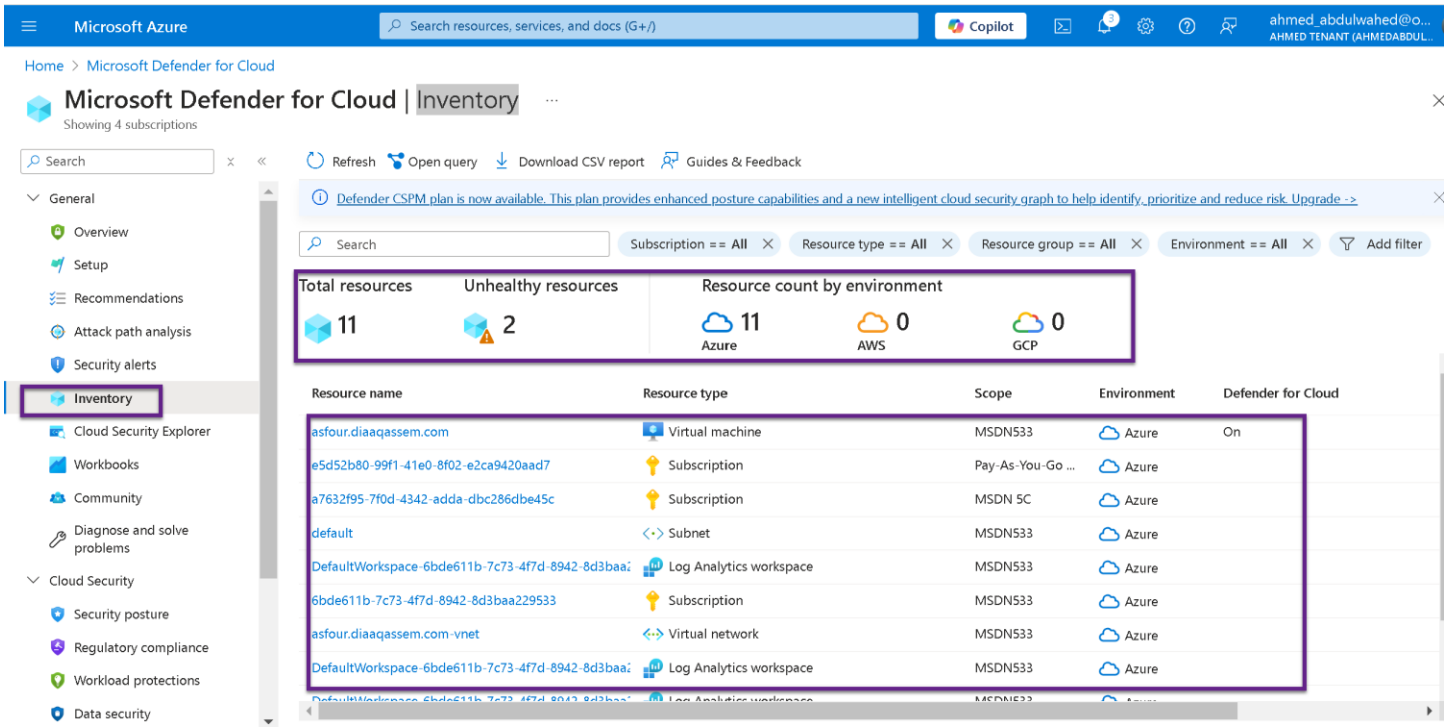
Microsoft Defender for GCP



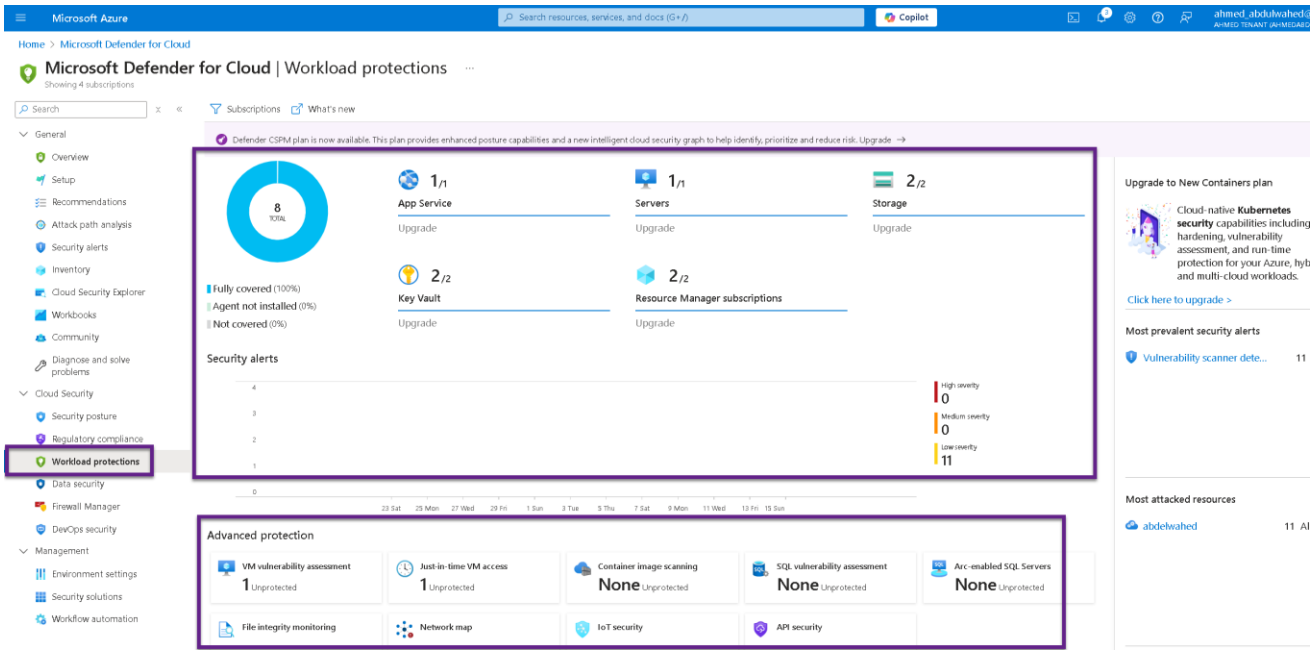
Security alerts



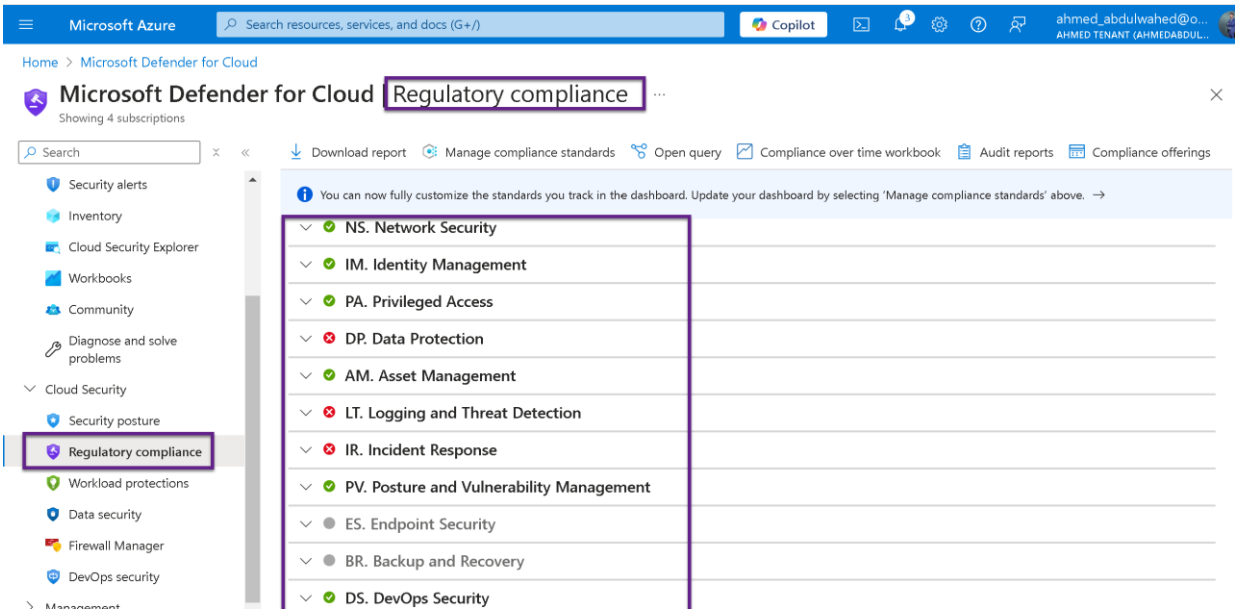
Inventory



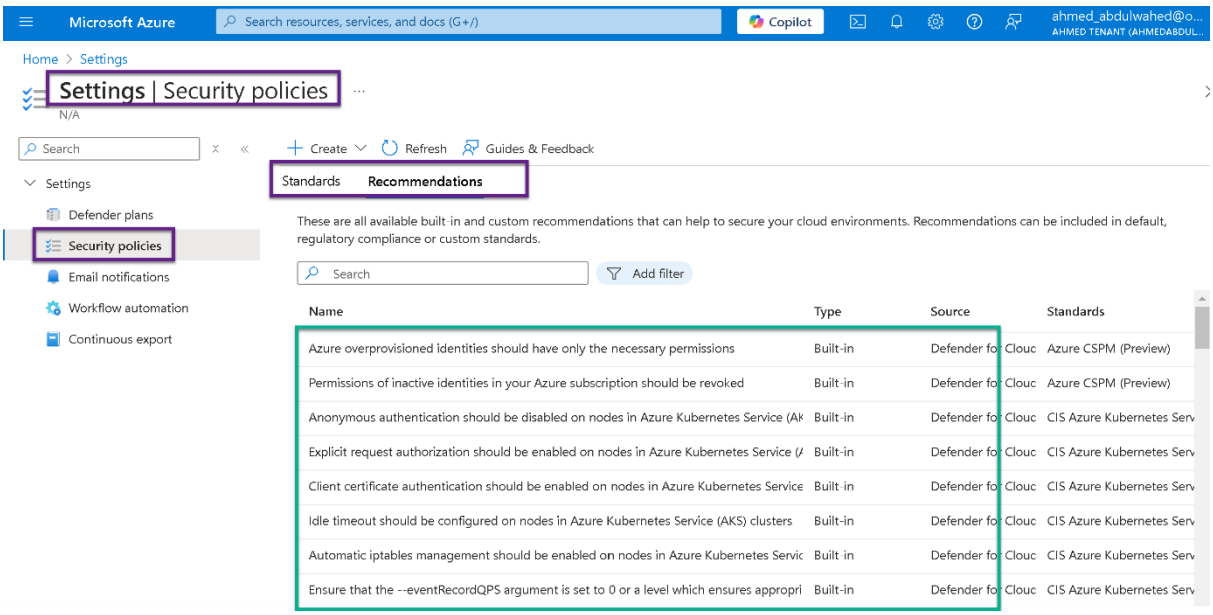
Workload Protections in **Microsoft Defender for Cloud** focus on securing various workloads running in your hybrid and multi-cloud environments. These protections are designed to monitor, detect, and respond to threats targeting virtual machines, containers, databases, application services, and more.



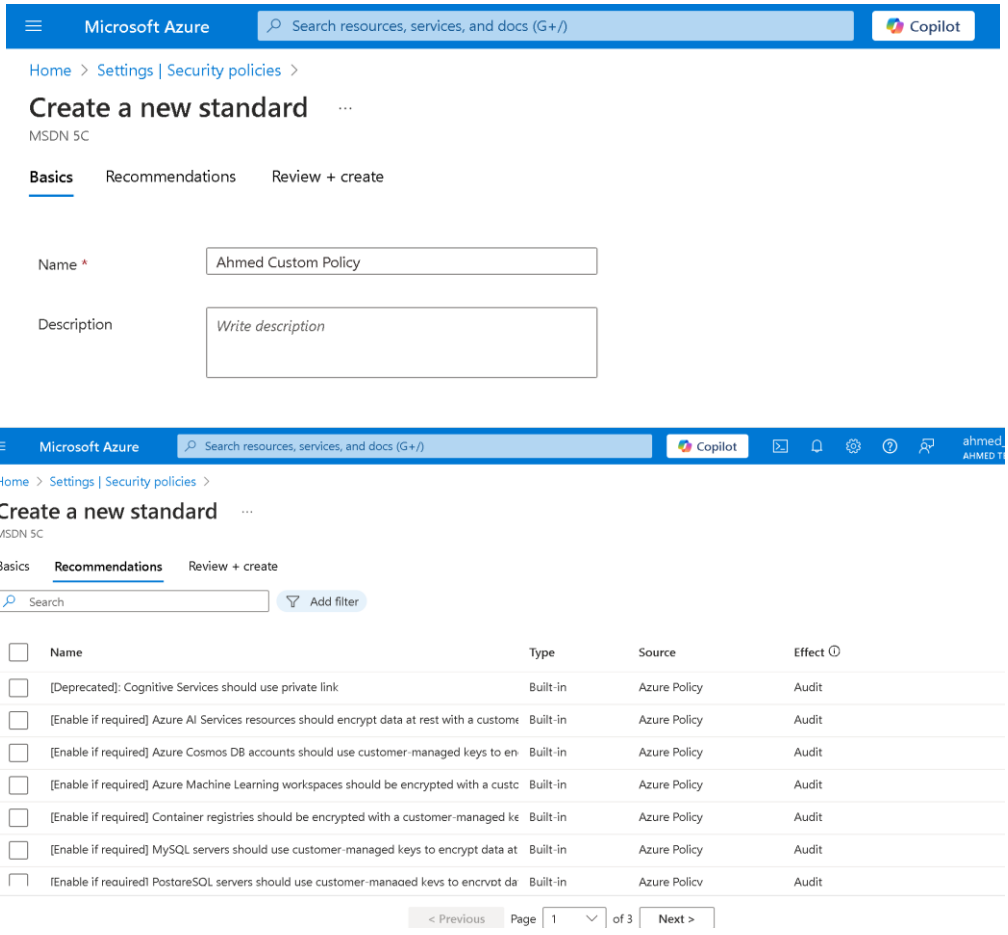
Regulatory Compliance is a feature that helps organizations continuously monitor and ensure that their cloud environments align with industry-standard regulatory requirements, such as ISO 27001, PCI DSS, or custom internal standards. It provides tools for tracking compliance, assessing resource configurations,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



The **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.



using create option, you can create your own



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.