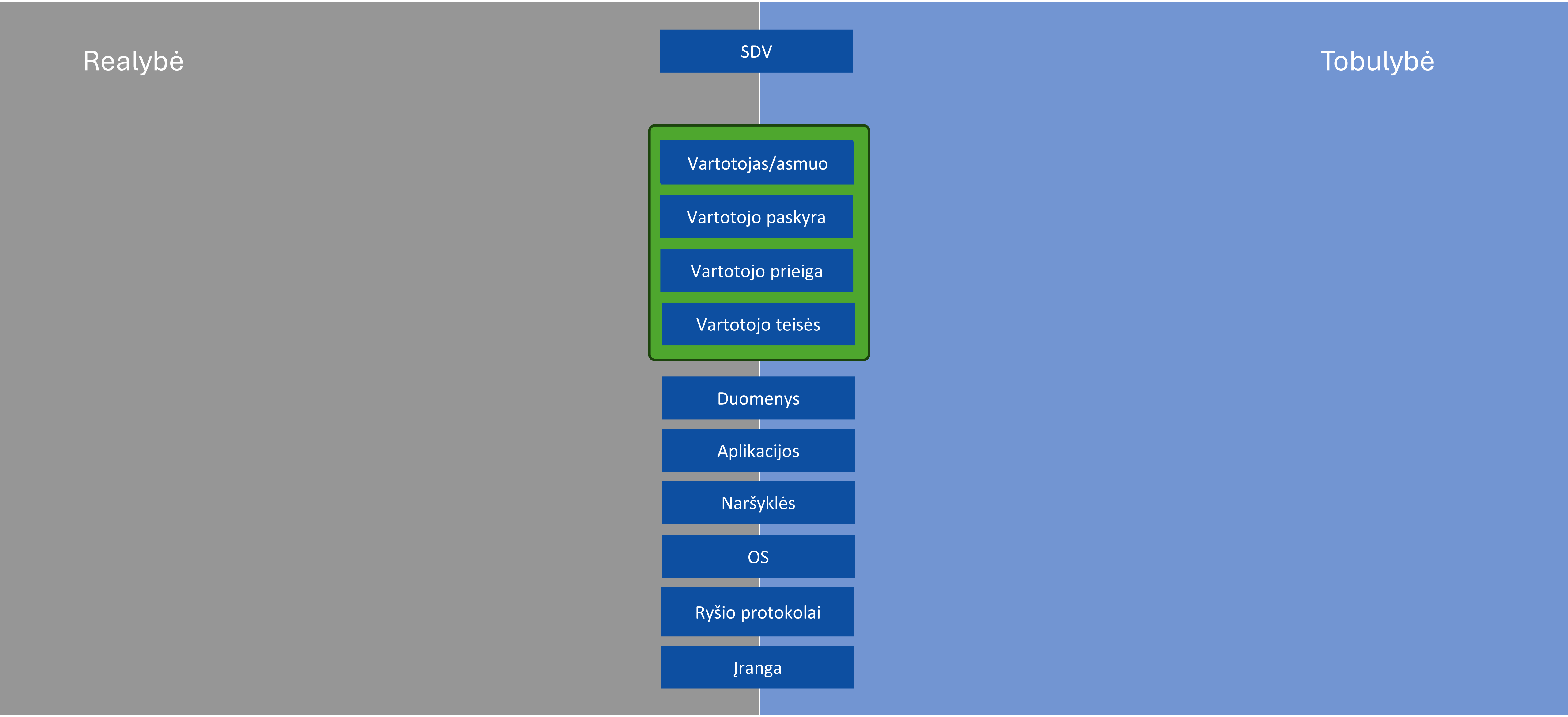
# Darbo vietų saugumas tarp tobulybės ir realybės

Rimas Kareiva

Skaitmeninių darbo vietų kompetencijų centras

Grupės vadovas

# Kur esame?



Realybė

Tobulybė

SDV

Vartotojas/asmuo

Vartotojo paskyra

Vartotojo prieiga

Vartotojo teisės

Duomenys

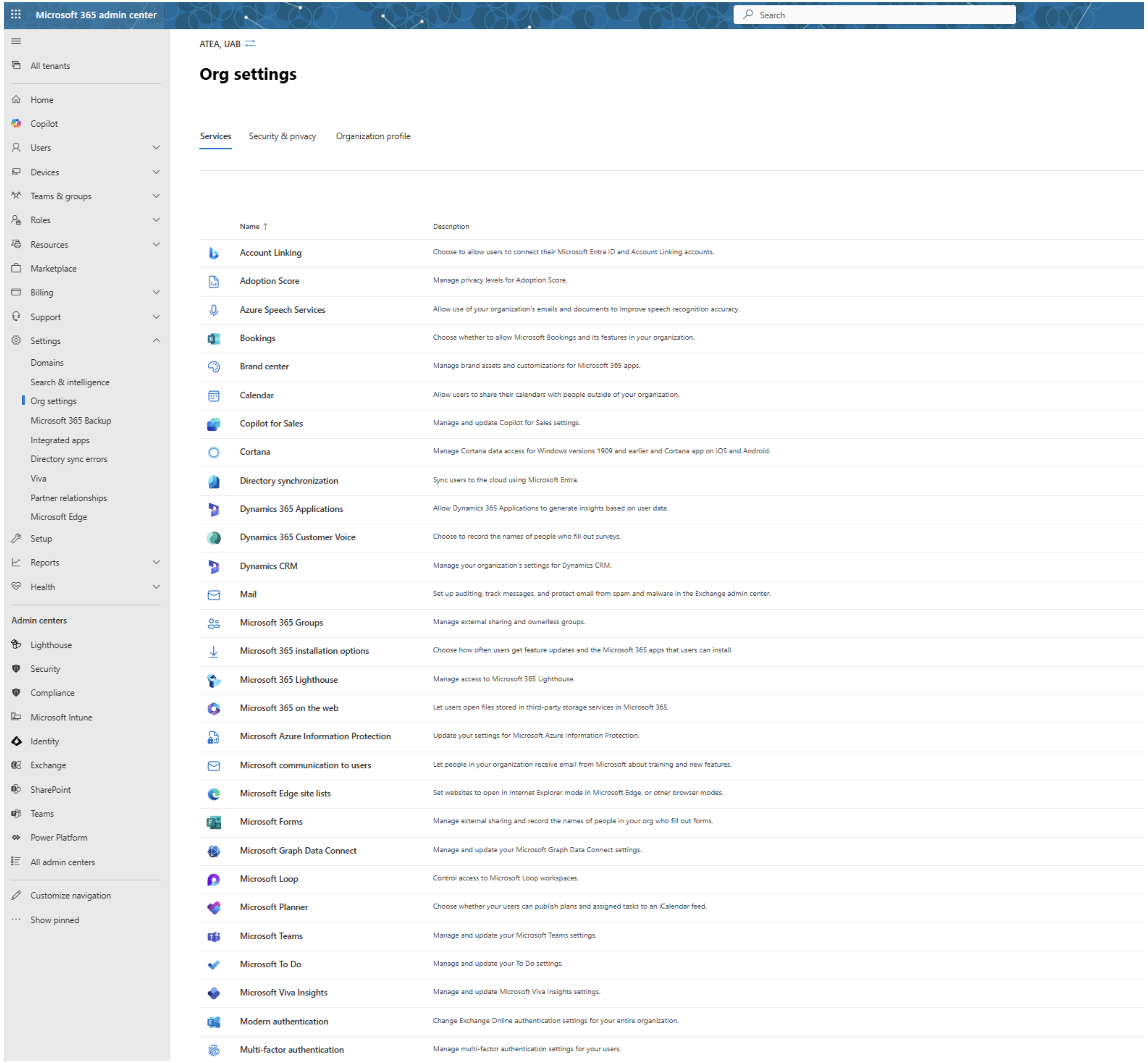
Aplikacijos

Naršyklės

OS

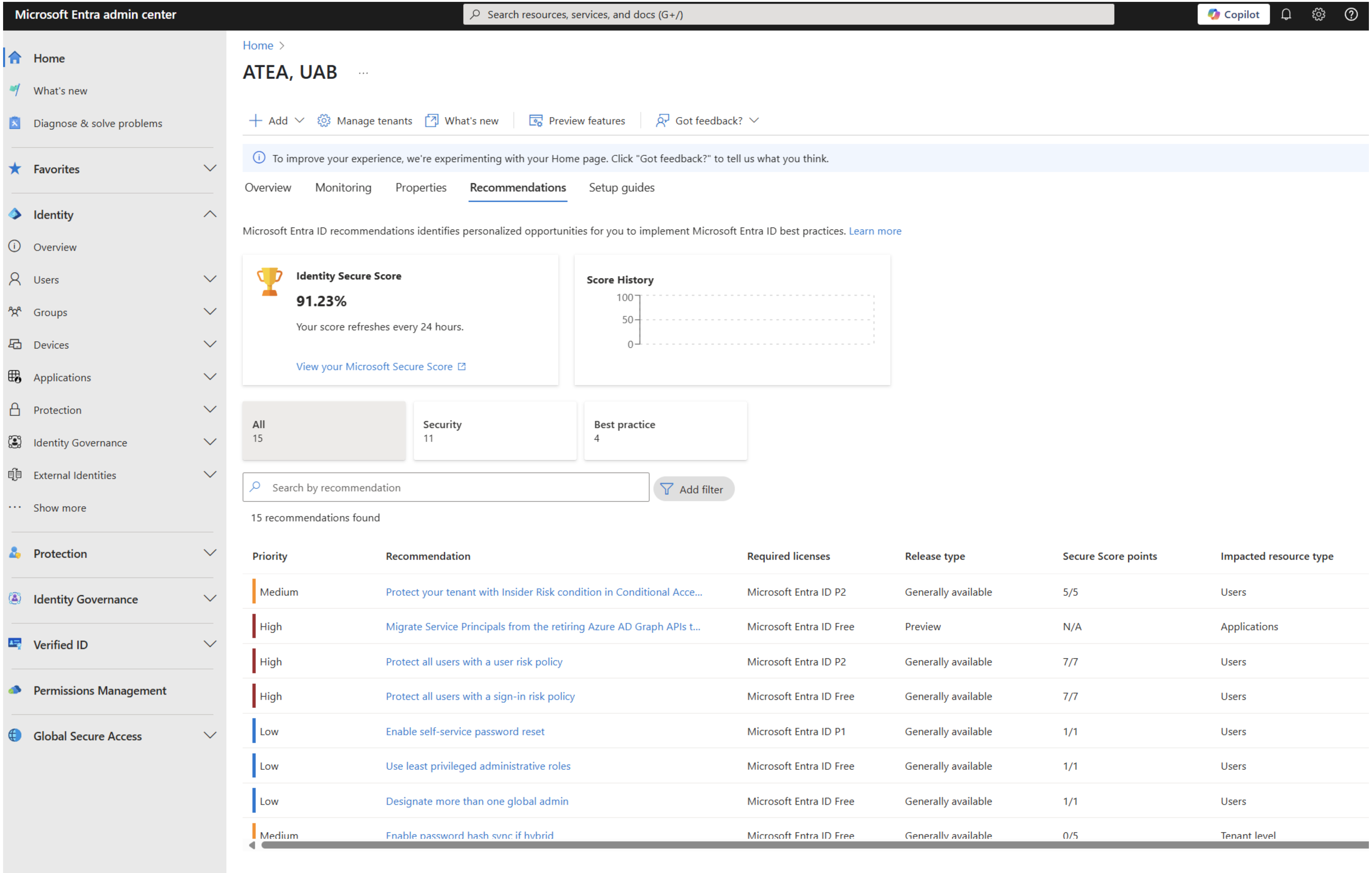
Ryšio protokolai

Įranga



# Org settings

| Name ↑ | Description |
|---|---|
| Account Linking | Choose to allow users to connect their Microsoft Entra ID and Account Linking accounts. |
| Adoption Score | Manage privacy levels for Adoption Score. |
| Azure Speech Services | Allow use of your organization's emails and documents to improve speech recognition accuracy. |
| Bookings | Choose whether to allow Microsoft Bookings and its features in your organization. |
| Brand center | Manage brand assets and customizations for Microsoft 365 apps. |
| Calendar | Allow users to share their calendars with people outside of your organization. |
| Copilot for Sales | Manage and update Copilot for Sales settings. |
| Cortana | Manage Cortana data access for Windows versions 1909 and earlier and Cortana app on iOS and Android. |
| Directory synchronization | Sync users to the cloud using Microsoft Entra. |
| Dynamics 365 Applications | Allow Dynamics 365 Applications to generate insights based on user data. |
| Dynamics 365 Customer Voice | Choose to record the names of people who fill out surveys. |
| Dynamics CRM | Manage your organization's settings for Dynamics CRM. |
| Mail | Set up auditing, track messages, and protect email from spam and malware in the Exchange admin center. |
| Microsoft 365 Groups | Manage external sharing and ownerless groups. |
| Microsoft 365 installation options | Choose how often users get feature updates and the Microsoft 365 apps that users can install. |
| Microsoft 365 Lighthouse | Manage access to Microsoft 365 Lighthouse. |
| Microsoft 365 on the web | Let users open files stored in third-party storage services in Microsoft 365. |
| Microsoft Azure Information Protection | Update your settings for Microsoft Azure Information Protection. |
| Microsoft communication to users | Let people in your organization receive email from Microsoft about training and new features. |
| Microsoft Edge site lists | Set websites to open in Internet Explorer mode in Microsoft Edge, or other browser modes. |
| Microsoft Forms | Manage external sharing and record the names of people in your org who fill out forms. |
| Microsoft Graph Data Connect | Manage and update your Microsoft Graph Data Connect settings. |
| Microsoft Loop | Control access to Microsoft Loop workspaces. |
| Microsoft Planner | Choose whether your users can publish plans and assigned tasks to an iCalendar feed. |
| Microsoft Teams | Manage and update your Microsoft Teams settings. |
| Microsoft To Do | Manage and update your To Do settings. |
| Microsoft Viva Insights | Manage and update Microsoft Viva Insights settings. |
| Modern authentication | Change Exchange Online authentication settings for your entire organization. |
| Multi-factor authentication | Manage multi-factor authentication settings for your users. |



ATEA, UAB ...

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Microsoft Entra ID recommendations identifies personalized opportunities for you to implement Microsoft Entra ID best practices. Learn more

**Identity Secure Score**

**91.23%**

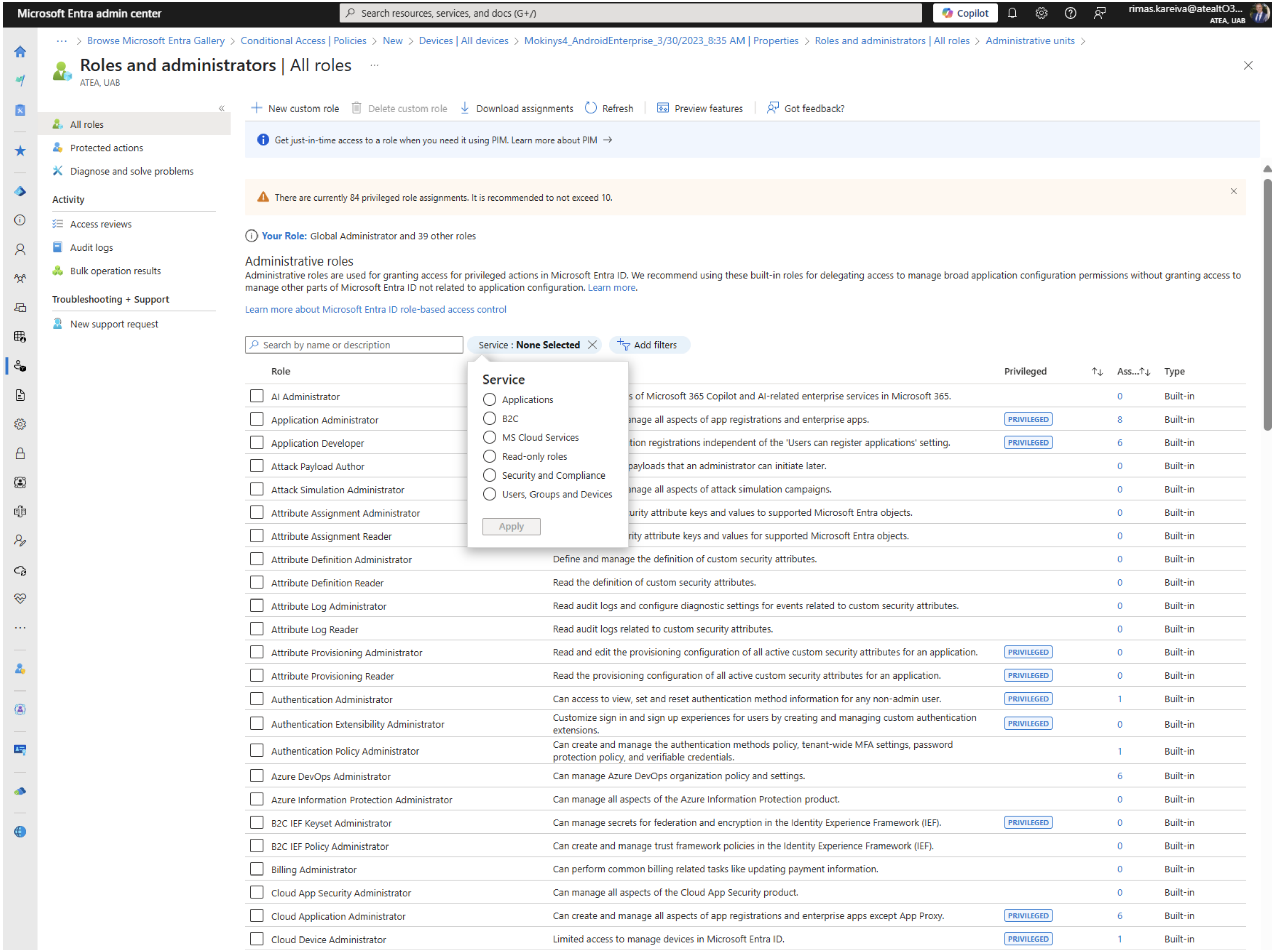
Your score refreshes every 24 hours.

View your Microsoft Secure Score

| All | Security | Best practice |
|---|---|---|
| 15 | 11 | 4 |

15 recommendations found

| Priority | Recommendation | Required licenses | Release type | Secure Score points | Impacted resource type |
|---|---|---|---|---|---|
| Medium | Protect your tenant with Insider Risk condition in Conditional Acce... | Microsoft Entra ID P2 | Generally available | 5/5 | Users |
| High | Migrate Service Principals from the retiring Azure AD Graph APIs t... | Microsoft Entra ID Free | Preview | N/A | Applications |
| High | Protect all users with a user risk policy | Microsoft Entra ID P2 | Generally available | 7/7 | Users |
| High | Protect all users with a sign-in risk policy | Microsoft Entra ID Free | Generally available | 7/7 | Users |
| Low | Enable self-service password reset | Microsoft Entra ID P1 | Generally available | 1/1 | Users |
| Low | Use least privileged administrative roles | Microsoft Entra ID Free | Generally available | 1/1 | Users |
| Low | Designate more than one global admin | Microsoft Entra ID Free | Generally available | 1/1 | Users |
| Medium | Enable password hash sync if hybrid | Microsoft Entra ID Free | Generally available | 0/5 | Tenant level |



Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
rimas.kareiva@atealtO3...
ATEA, UAB
... > Browse Microsoft Entra Gallery > Conditional Access | Policies > New > Devices | All devices > Mokinys4_AndroidEnterprise_3/30/2023_8:35 AM | Properties > Roles and administrators | All roles > Administrative units >

# Roles and administrators | All roles

ATEA, UAB

All roles
Protected actions
Diagnose and solve problems
Activity
Access reviews
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
+ New custom role
Delete custom role
Download assignments
Refresh
Preview features
Got feedback?

Get just-in-time access to a role when you need it using PIM. Learn more about PIM →

There are currently 84 privileged role assignments. It is recommended to not exceed 10.

**Your Role:** Global Administrator and 39 other roles

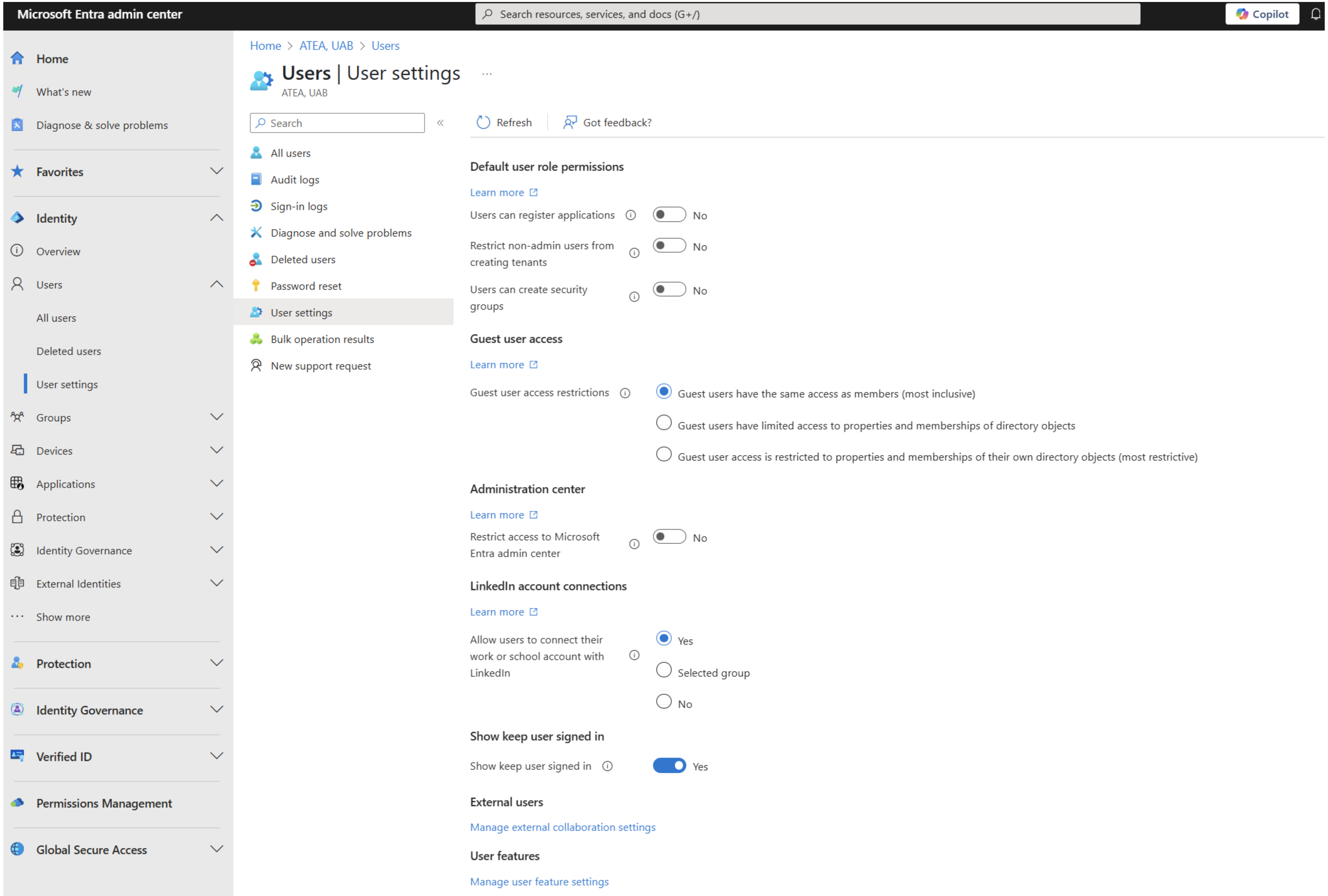
## Administrative roles

Administrative roles are used for granting access for privileged actions in Microsoft Entra ID. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Microsoft Entra ID not related to application configuration. Learn more.

Learn more about Microsoft Entra ID role-based access control

Service
○ Applications
○ B2C
○ MS Cloud Services
○ Read-only roles
○ Security and Compliance
○ Users, Groups and Devices
Apply

| | Role | | Privileged | Ass... | Type |
|---|---|---|---|---|---|
| □ | AI Administrator | s of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365. | | 0 | Built-in |
| □ | Application Administrator | anage all aspects of app registrations and enterprise apps. | PRIVILEGED | 8 | Built-in |
| □ | Application Developer | tion registrations independent of the 'Users can register applications' setting. | PRIVILEGED | 6 | Built-in |
| □ | Attack Payload Author | payloads that an administrator can initiate later. | | 0 | Built-in |
| □ | Attack Simulation Administrator | anage all aspects of attack simulation campaigns. | | 0 | Built-in |
| □ | Attribute Assignment Administrator | urity attribute keys and values to supported Microsoft Entra objects. | | 0 | Built-in |
| □ | Attribute Assignment Reader | rity attribute keys and values for supported Microsoft Entra objects. | | 0 | Built-in |
| □ | Attribute Definition Administrator | Define and manage the definition of custom security attributes. | | 0 | Built-in |
| □ | Attribute Definition Reader | Read the definition of custom security attributes. | | 0 | Built-in |
| □ | Attribute Log Administrator | Read audit logs and configure diagnostic settings for events related to custom security attributes. | | 0 | Built-in |
| □ | Attribute Log Reader | Read audit logs related to custom security attributes. | | 0 | Built-in |
| □ | Attribute Provisioning Administrator | Read and edit the provisioning configuration of all active custom security attributes for an application. | PRIVILEGED | 0 | Built-in |
| □ | Attribute Provisioning Reader | Read the provisioning configuration of all active custom security attributes for an application. | PRIVILEGED | 0 | Built-in |
| □ | Authentication Administrator | Can access to view, set and reset authentication method information for any non-admin user. | PRIVILEGED | 1 | Built-in |
| □ | Authentication Extensibility Administrator | Customize sign in and sign up experiences for users by creating and managing custom authentication extensions. | PRIVILEGED | 0 | Built-in |
| □ | Authentication Policy Administrator | Can create and manage the authentication methods policy, tenant-wide MFA settings, password protection policy, and verifiable credentials. | | 1 | Built-in |
| □ | Azure DevOps Administrator | Can manage Azure DevOps organization policy and settings. | | 6 | Built-in |
| □ | Azure Information Protection Administrator | Can manage all aspects of the Azure Information Protection product. | | 0 | Built-in |
| □ | B2C IEF Keyset Administrator | Can manage secrets for federation and encryption in the Identity Experience Framework (IEF). | PRIVILEGED | 0 | Built-in |
| □ | B2C IEF Policy Administrator | Can create and manage trust framework policies in the Identity Experience Framework (IEF). | | 0 | Built-in |
| □ | Billing Administrator | Can perform common billing related tasks like updating payment information. | | 0 | Built-in |
| □ | Cloud App Security Administrator | Can manage all aspects of the Cloud App Security product. | | 0 | Built-in |
| □ | Cloud Application Administrator | Can create and manage all aspects of app registrations and enterprise apps except App Proxy. | PRIVILEGED | 6 | Built-in |
| □ | Cloud Device Administrator | Limited access to manage devices in Microsoft Entra ID. | PRIVILEGED | 1 | Built-in |



# Users | User settings

ATEA, UAB

## Default user role permissions

Learn more

Users can register applications: No

Restrict non-admin users from creating tenants: No

Users can create security groups: No

## Guest user access

Learn more

Guest user access restrictions

- ● Guest users have the same access as members (most inclusive)
- ○ Guest users have limited access to properties and memberships of directory objects
- ○ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

## Administration center

Learn more

Restrict access to Microsoft Entra admin center: No

## LinkedIn account connections

Learn more

Allow users to connect their work or school account with LinkedIn

- ● Yes
- ○ Selected group
- ○ No

## Show keep user signed in

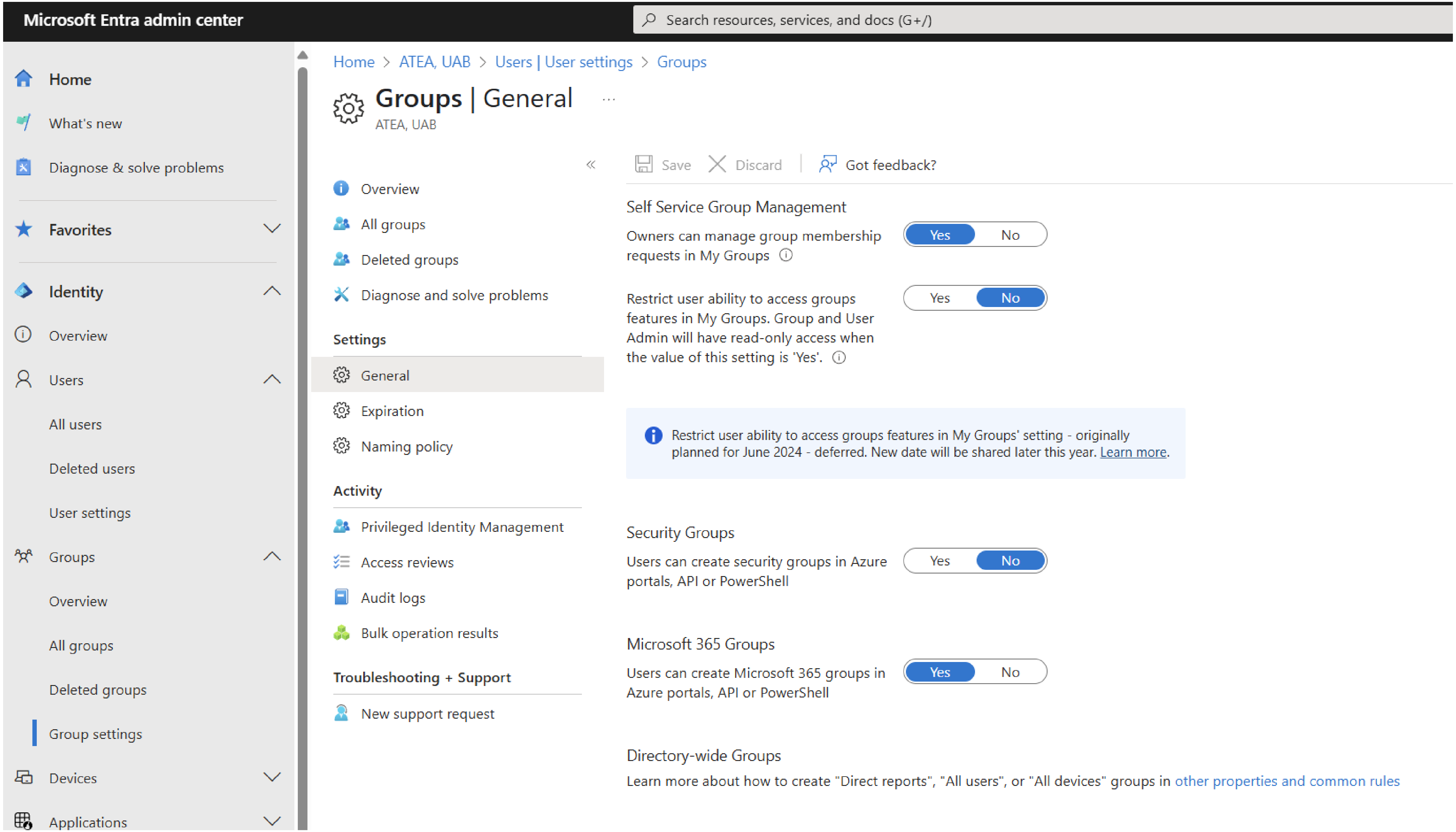
Show keep user signed in: Yes

## External users

Manage external collaboration settings

## User features

Manage user feature settings



# Groups | General

ATEA, UAB

## Self Service Group Management

Owners can manage group membership requests in My Groups [✓ Yes] No

Restrict user ability to access groups features in My Groups. Group and User Admin will have read-only access when the value of this setting is 'Yes'. Yes [✓ No]

Restrict user ability to access groups features in My Groups' setting - originally planned for June 2024 - deferred. New date will be shared later this year. Learn more.

## Security Groups

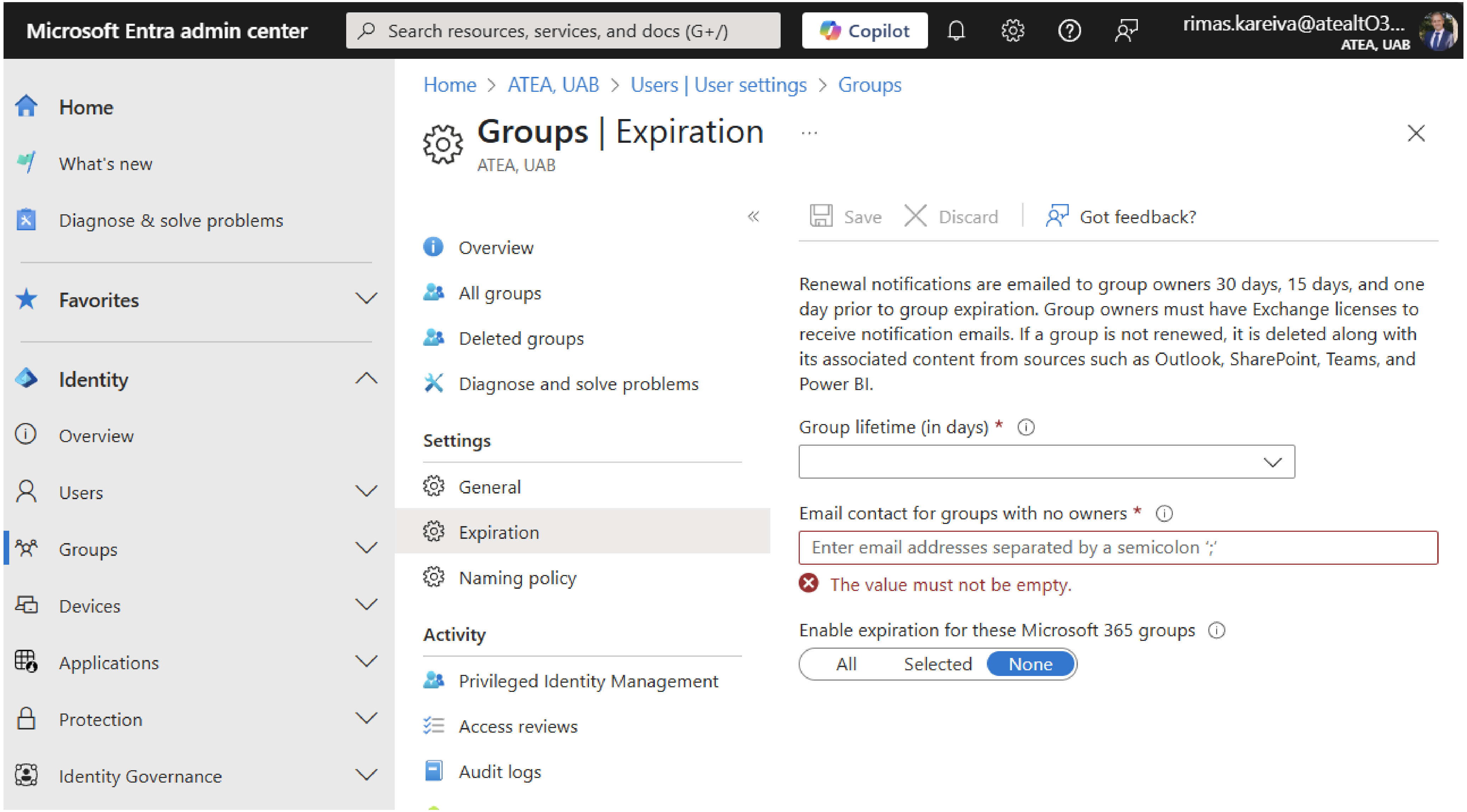
Users can create security groups in Azure portals, API or PowerShell Yes [✓ No]

## Microsoft 365 Groups

Users can create Microsoft 365 groups in Azure portals, API or PowerShell [✓ Yes] No

## Directory-wide Groups

Learn more about how to create "Direct reports", "All users", or "All devices" groups in other properties and common rules



Groups | Expiration

ATEA, UAB

Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Teams, and Power BI.

Group lifetime (in days) *

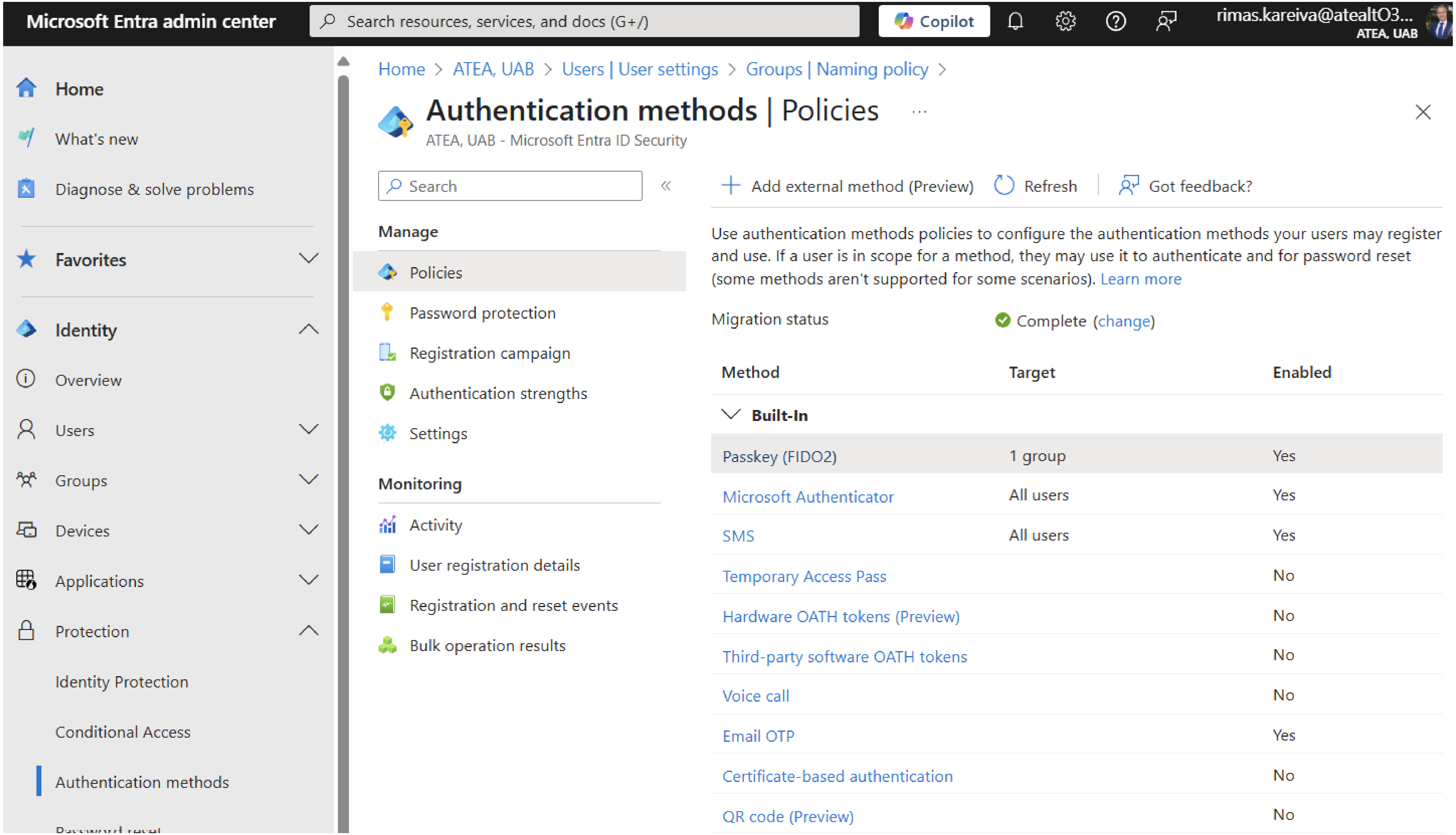
Email contact for groups with no owners *

Enter email addresses separated by a semicolon ';'

The value must not be empty.

Enable expiration for these Microsoft 365 groups

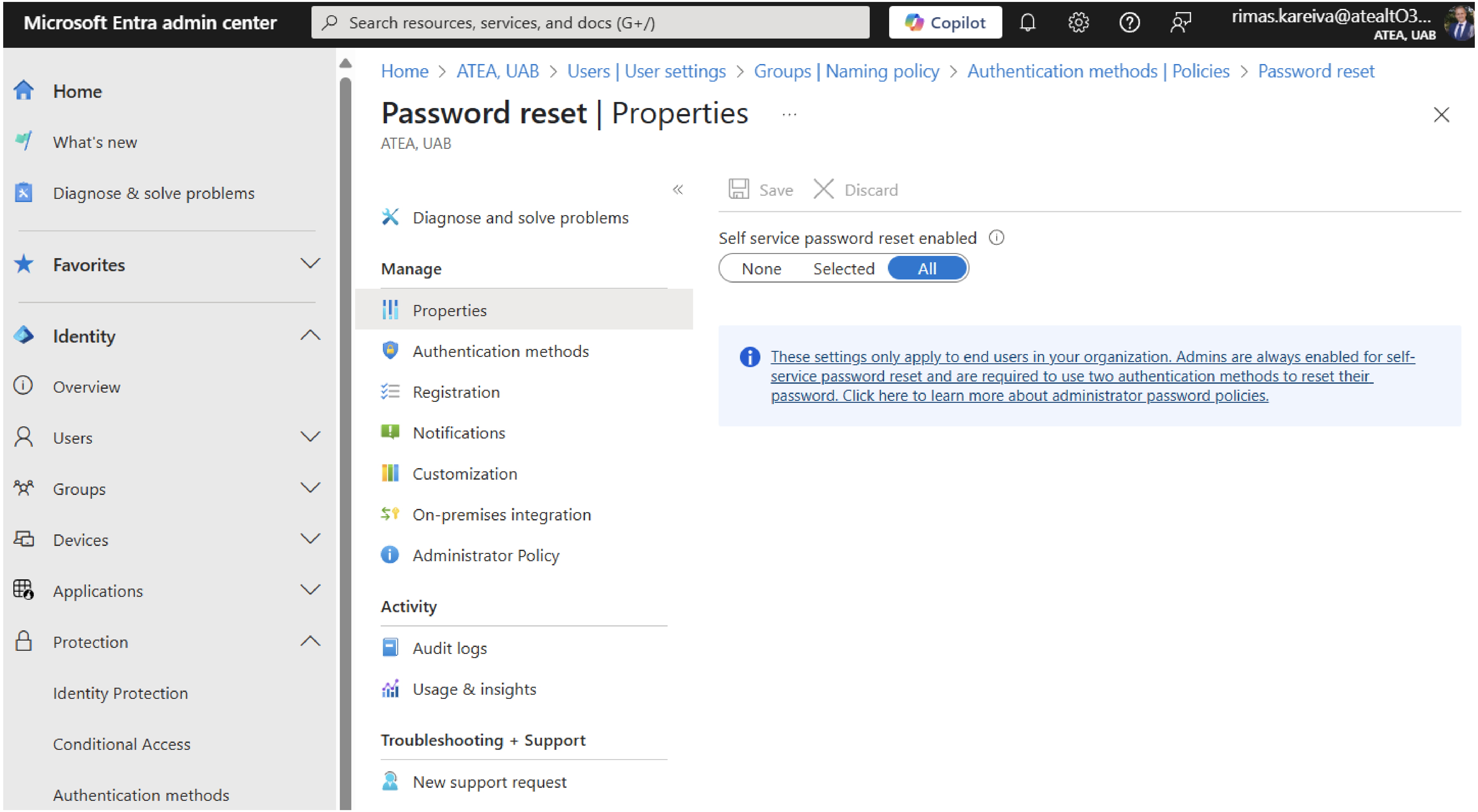
All Selected [✓ None]


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
rimas.kareiva@atealt03...
ATEA, UAB
Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Home > ATEA, UAB > Users | User settings > Groups | Naming policy >
Authentication methods | Policies
ATEA, UAB - Microsoft Entra ID Security
Search
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results
Add external method (Preview)
Refresh
Got feedback?

Use authentication methods policies to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). Learn more

Migration status ✓ Complete (change)

| Method | Target | Enabled |
|---|---|---|
| **Built-In** | | |
| Passkey (FIDO2) | 1 group | Yes |
| Microsoft Authenticator | All users | Yes |
| SMS | All users | Yes |
| Temporary Access Pass | | No |
| Hardware OATH tokens (Preview) | | No |
| Third-party software OATH tokens | | No |
| Voice call | | No |
| Email OTP | | Yes |
| Certificate-based authentication | | No |
| QR code (Preview) | | No |

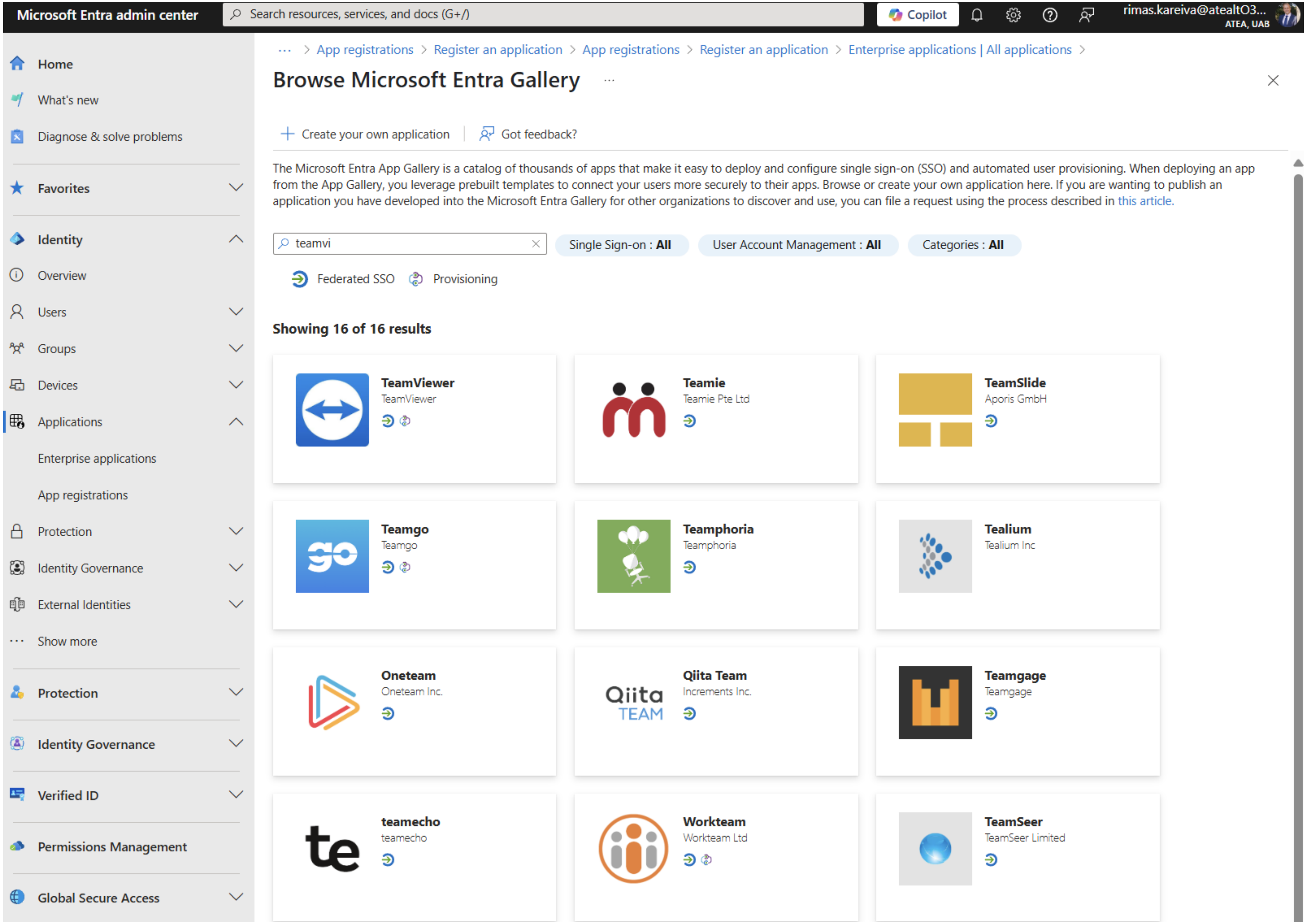


Password reset | Properties

ATEA, UAB

Self service password reset enabled: None Selected [✓ All]

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.



Microsoft Entra admin center

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

Copilot

rimas.kareiva@atealtO3...
ATEA, UAB

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
  - Overview
  - Users
  - Groups
  - Devices
  - Applications
    - Enterprise applications
    - App registrations
  - Protection
  - Identity Governance
  - External Identities
  - Show more
- Protection
- Identity Governance
- Verified ID
- Permissions Management
- Global Secure Access

... > App registrations > Register an application > App registrations > Register an application > Enterprise applications | All applications >

# Browse Microsoft Entra Gallery

+ Create your own application | Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in this article.

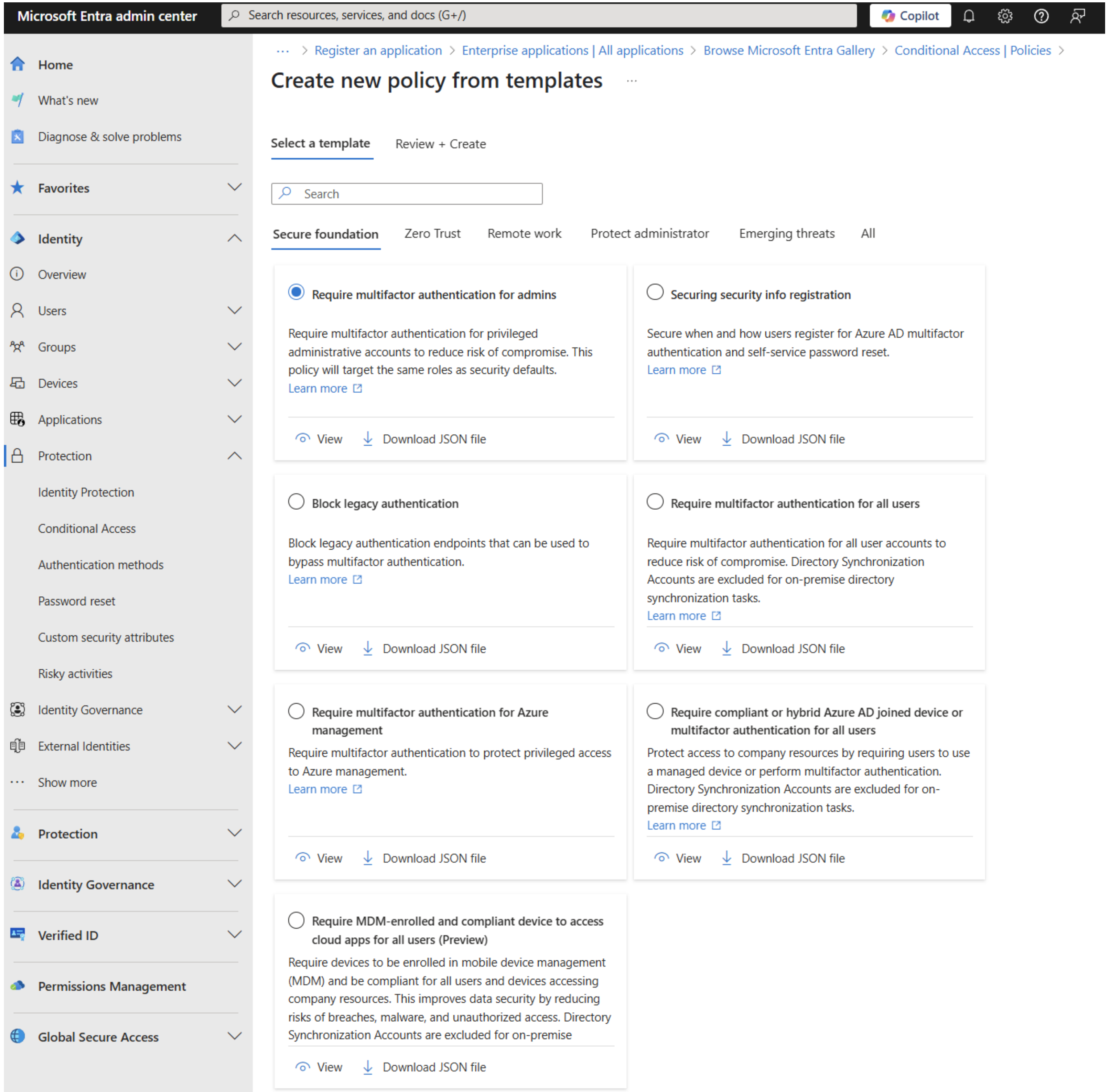
teamvi

Single Sign-on : **All** | User Account Management : **All** | Categories : **All**

Federated SSO | Provisioning

**Showing 16 of 16 results**

| | | |
|---|---|---|
| **TeamViewer**<br>TeamViewer | **Teamie**<br>Teamie Pte Ltd | **TeamSlide**<br>Aporis GmbH |
| **Teamgo**<br>Teamgo | **Teamphoria**<br>Teamphoria | **Tealium**<br>Tealium Inc |
| **Oneteam**<br>Oneteam Inc. | **Qiita Team**<br>Increments Inc. | **Teamgage**<br>Teamgage |
| **teamecho**<br>teamecho | **Workteam**<br>Workteam Ltd | **TeamSeer**<br>TeamSeer Limited |



Microsoft Entra admin center

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

Copilot

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Custom security attributes

Risky activities

Identity Governance

External Identities

Show more

Protection

Identity Governance

Verified ID

Permissions Management

Global Secure Access

… > Register an application > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Conditional Access | Policies >

Create new policy from templates …

Select a template    Review + Create

Search

Secure foundation    Zero Trust    Remote work    Protect administrator    Emerging threats    All

● **Require multifactor authentication for admins**

Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults.
Learn more

View    Download JSON file

○ **Securing security info registration**

Secure when and how users register for Azure AD multifactor authentication and self-service password reset.
Learn more

View    Download JSON file

○ **Block legacy authentication**

Block legacy authentication endpoints that can be used to bypass multifactor authentication.
Learn more

View    Download JSON file

○ **Require multifactor authentication for all users**

Require multifactor authentication for all user accounts to reduce risk of compromise. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks.
Learn more

View    Download JSON file

○ **Require multifactor authentication for Azure management**

Require multifactor authentication to protect privileged access to Azure management.
Learn more

View    Download JSON file

○ **Require compliant or hybrid Azure AD joined device or multifactor authentication for all users**

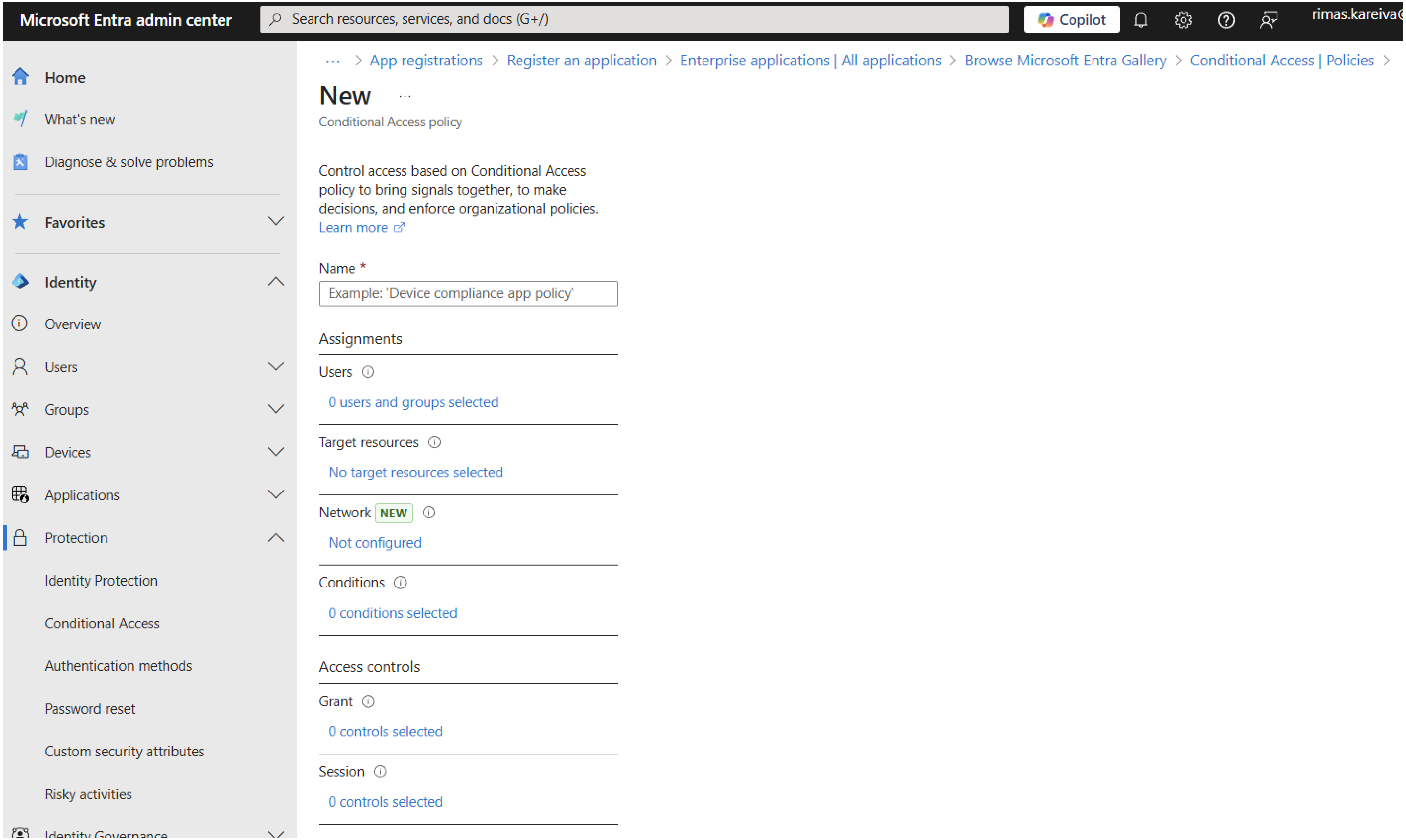
Protect access to company resources by requiring users to use a managed device or perform multifactor authentication. Directory Synchronization Accounts are excluded for on-premise directory synchronization tasks.
Learn more

View    Download JSON file

○ **Require MDM-enrolled and compliant device to access cloud apps for all users (Preview)**

Require devices to be enrolled in mobile device management (MDM) and be compliant for all users and devices accessing company resources. This improves data security by reducing risks of breaches, malware, and unauthorized access. Directory Synchronization Accounts are excluded for on-premise

View    Download JSON file


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
rimas.kareiva
Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Identity Governance
… > App registrations > Register an application > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Conditional Access | Policies >

New …

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users ⓘ

0 users and groups selected

Target resources ⓘ

No target resources selected

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

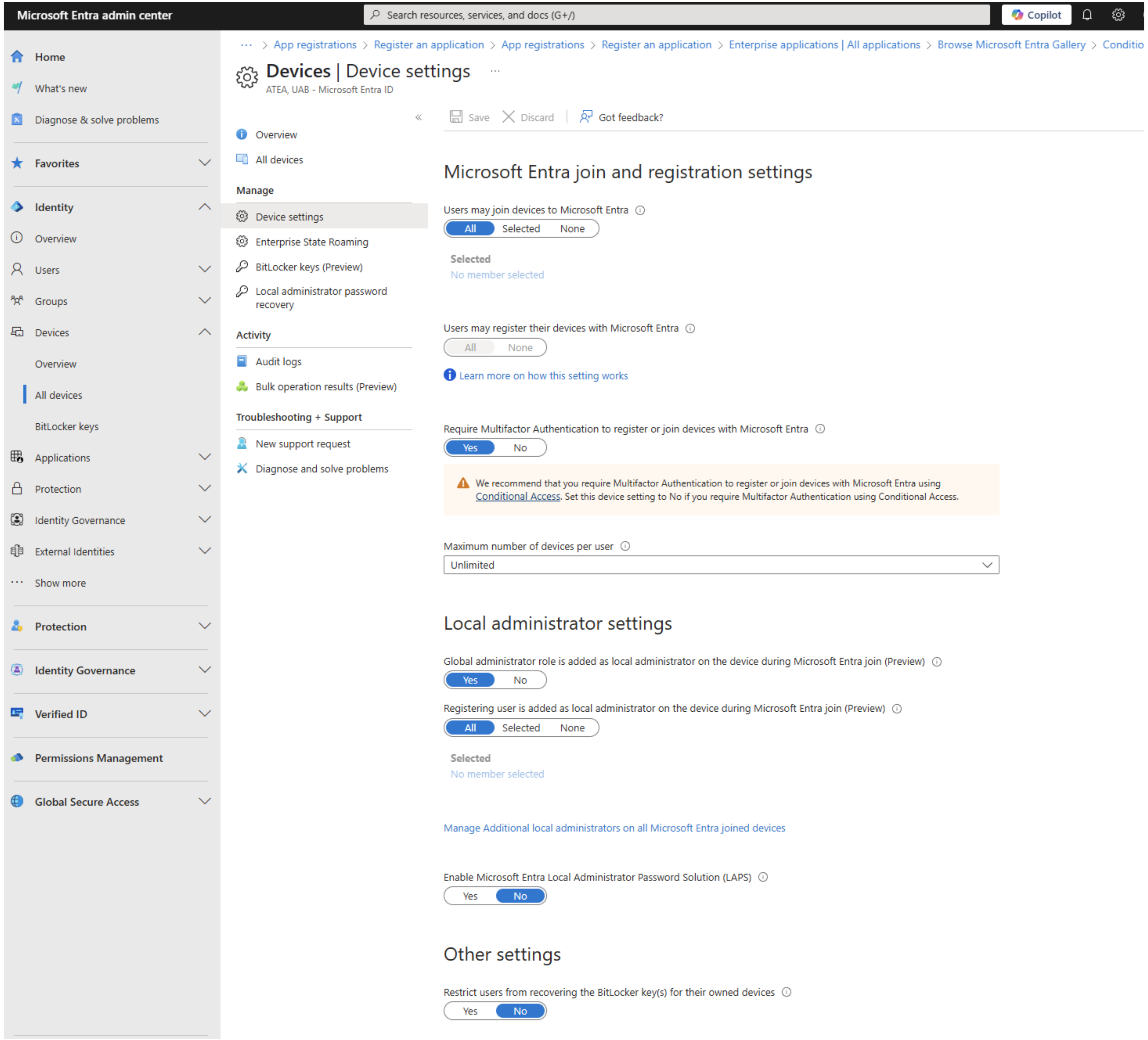
Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected



Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Overview
All devices
BitLocker keys
Applications
Protection
Identity Governance
External Identities
Show more
Protection
Identity Governance
Verified ID
Permissions Management
Global Secure Access
... > App registrations > Register an application > App registrations > Register an application > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Conditio
Overview
All devices
Manage
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Local administrator password recovery
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Diagnose and solve problems
Save
Discard
Got feedback?

# Devices | Device settings

ATEA, UAB - Microsoft Entra ID

## Microsoft Entra join and registration settings

Users may join devices to Microsoft Entra

[✓ All] Selected None

Selected

No member selected

Users may register their devices with Microsoft Entra

[✓ All] None

Learn more on how this setting works

Require Multifactor Authentication to register or join devices with Microsoft Entra

[✓ Yes] No

We recommend that you require Multifactor Authentication to register or join devices with Microsoft Entra using Conditional Access. Set this device setting to No if you require Multifactor Authentication using Conditional Access.

Maximum number of devices per user

Unlimited

## Local administrator settings

Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)

[✓ Yes] No

Registering user is added as local administrator on the device during Microsoft Entra join (Preview)

[✓ All] Selected None

Selected

No member selected

Manage Additional local administrators on all Microsoft Entra joined devices

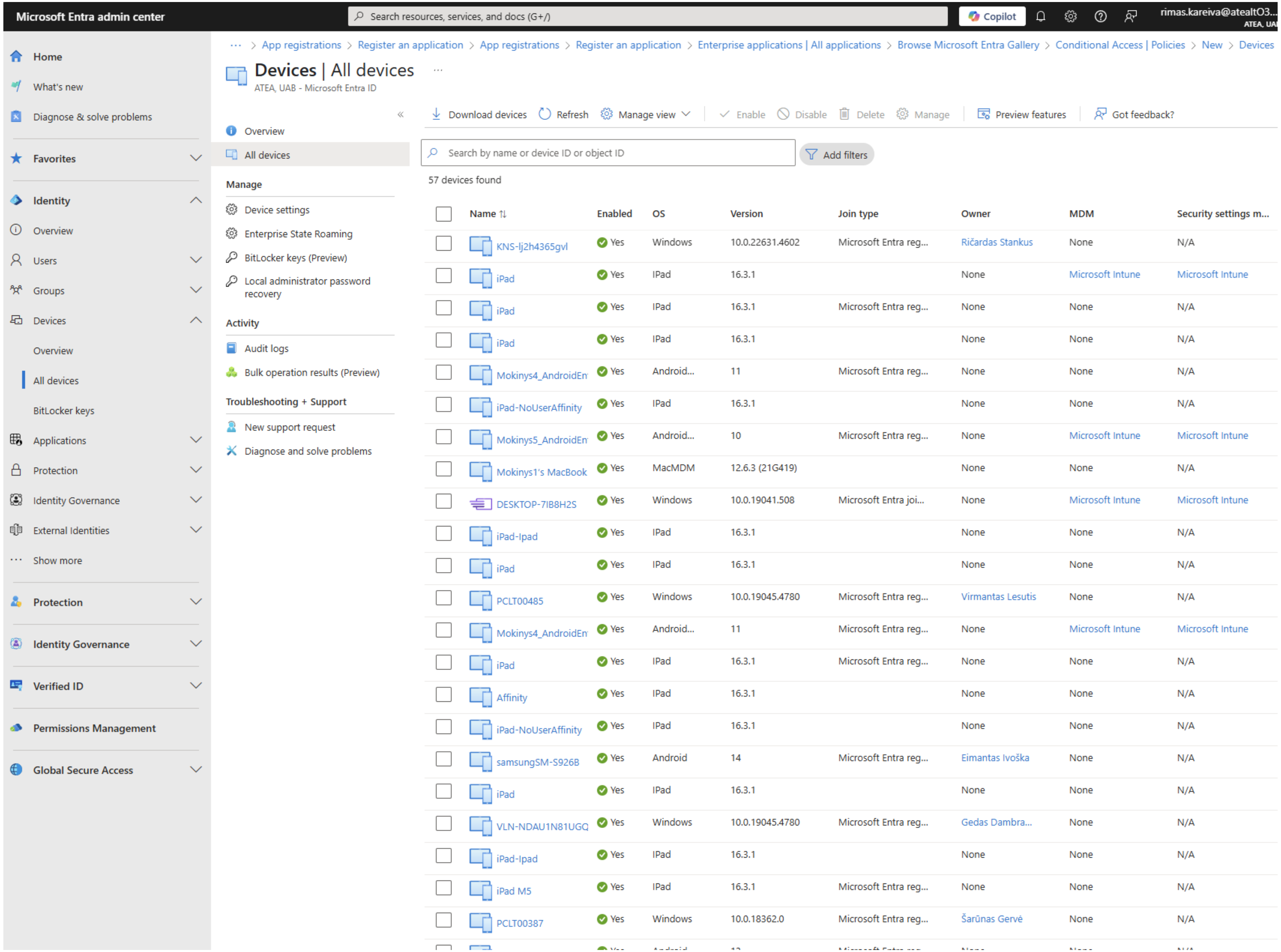
Enable Microsoft Entra Local Administrator Password Solution (LAPS)

Yes [✓ No]

## Other settings

Restrict users from recovering the BitLocker key(s) for their owned devices

Yes [✓ No]

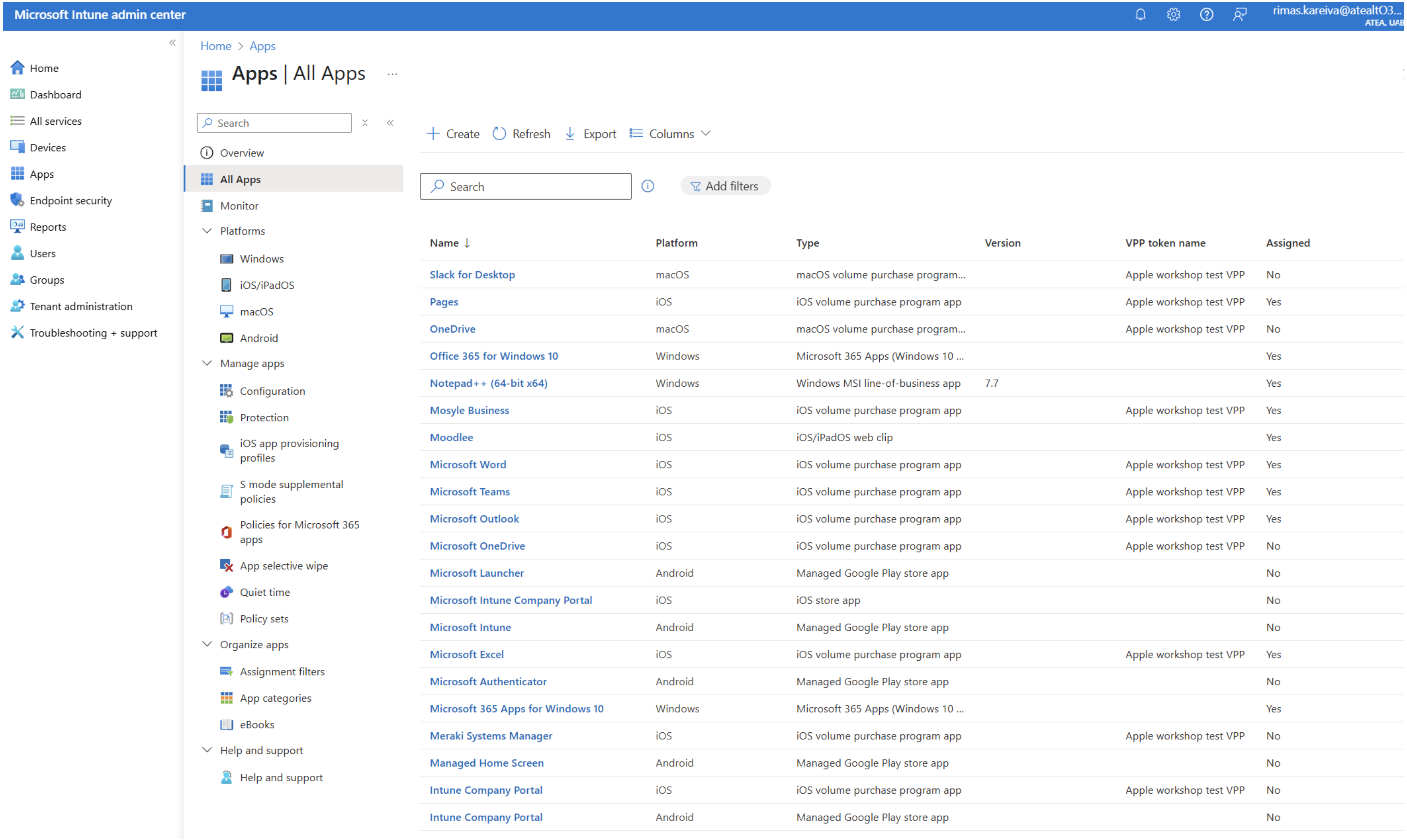

Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
rimas.kareiva@atealtO3...
ATEA, UAI
Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Overview
All devices
BitLocker keys
Applications
Protection
Identity Governance
External Identities
Show more
Protection
Identity Governance
Verified ID
Permissions Management
Global Secure Access
... > App registrations > Register an application > App registrations > Register an application > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Conditional Access | Policies > New > Devices
Overview
All devices
Manage
Device settings
Enterprise State Roaming
BitLocker keys (Preview)
Local administrator password recovery
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Diagnose and solve problems
Download devices
Refresh
Manage view
Enable
Disable
Delete
Manage
Preview features
Got feedback?
Search by name or device ID or object ID
Add filters

Devices | All devices

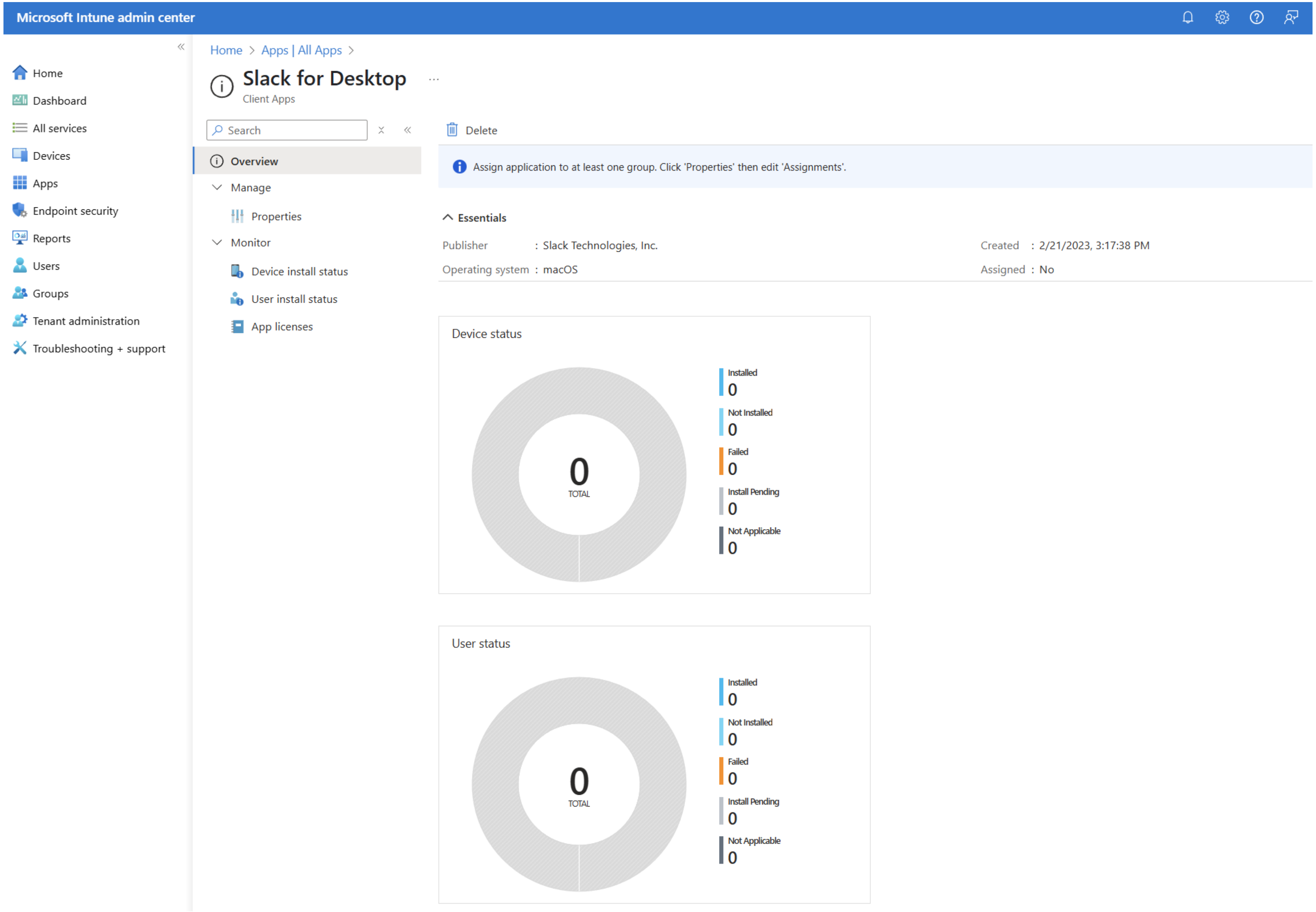
ATEA, UAB - Microsoft Entra ID

57 devices found

| □ | Name ⇅ | Enabled | OS | Version | Join type | Owner | MDM | Security settings m... |
|---|---|---|---|---|---|---|---|---|
| □ | KNS-lj2h4365gvl | ✓ Yes | Windows | 10.0.22631.4602 | Microsoft Entra reg... | Ričardas Stankus | None | N/A |
| □ | iPad | ✓ Yes | IPad | 16.3.1 | | None | Microsoft Intune | Microsoft Intune |
| □ | iPad | ✓ Yes | IPad | 16.3.1 | Microsoft Entra reg... | None | None | N/A |
| □ | iPad | ✓ Yes | IPad | 16.3.1 | | None | None | N/A |
| □ | Mokinys4_AndroidEn | ✓ Yes | Android... | 11 | Microsoft Entra reg... | None | None | N/A |
| □ | iPad-NoUserAffinity | ✓ Yes | IPad | 16.3.1 | | None | None | N/A |
| □ | Mokinys5_AndroidEn | ✓ Yes | Android... | 10 | Microsoft Entra reg... | None | Microsoft Intune | Microsoft Intune |
| □ | Mokinys1's MacBook | ✓ Yes | MacMDM | 12.6.3 (21G419) | | None | None | N/A |
| □ | DESKTOP-7IB8H2S | ✓ Yes | Windows | 10.0.19041.508 | Microsoft Entra joi... | None | Microsoft Intune | Microsoft Intune |
| □ | iPad-Ipad | ✓ Yes | IPad | 16.3.1 | | None | None | N/A |
| □ | iPad | ✓ Yes | IPad | 16.3.1 | | None | None | N/A |
| □ | PCLT00485 | ✓ Yes | Windows | 10.0.19045.4780 | Microsoft Entra reg... | Virmantas Lesutis | None | N/A |
| □ | Mokinys4_AndroidEn | ✓ Yes | Android... | 11 | Microsoft Entra reg... | None | Microsoft Intune | Microsoft Intune |
| □ | iPad | ✓ Yes | IPad | 16.3.1 | Microsoft Entra reg... | None | None | N/A |
| □ | Affinity | ✓ Yes | IPad | 16.3.1 | | None | None | N/A |
| □ | iPad-NoUserAffinity | ✓ Yes | IPad | 16.3.1 | | None | None | N/A |
| □ | samsungSM-S926B | ✓ Yes | Android | 14 | Microsoft Entra reg... | Eimantas Ivoška | None | N/A |
| □ | iPad | ✓ Yes | IPad | 16.3.1 | | None | None | N/A |
| □ | VLN-NDAU1N81UGQ | ✓ Yes | Windows | 10.0.19045.4780 | Microsoft Entra reg... | Gedas Dambra... | None | N/A |
| □ | iPad-Ipad | ✓ Yes | IPad | 16.3.1 | | None | None | N/A |
| □ | iPad M5 | ✓ Yes | IPad | 16.3.1 | Microsoft Entra reg... | None | None | N/A |
| □ | PCLT00387 | ✓ Yes | Windows | 10.0.18362.0 | Microsoft Entra reg... | Šarūnas Gervė | None | N/A |



| Name ↓ | Platform | Type | Version | VPP token name | Assigned |
|---|---|---|---|---|---|
| Slack for Desktop | macOS | macOS volume purchase program... | | Apple workshop test VPP | No |
| Pages | iOS | iOS volume purchase program app | | Apple workshop test VPP | Yes |
| OneDrive | macOS | macOS volume purchase program... | | Apple workshop test VPP | No |
| Office 365 for Windows 10 | Windows | Microsoft 365 Apps (Windows 10 ... | | | Yes |
| Notepad++ (64-bit x64) | Windows | Windows MSI line-of-business app | 7.7 | | Yes |
| Mosyle Business | iOS | iOS volume purchase program app | | Apple workshop test VPP | Yes |
| Moodlee | iOS | iOS/iPadOS web clip | | | Yes |
| Microsoft Word | iOS | iOS volume purchase program app | | Apple workshop test VPP | Yes |
| Microsoft Teams | iOS | iOS volume purchase program app | | Apple workshop test VPP | Yes |
| Microsoft Outlook | iOS | iOS volume purchase program app | | Apple workshop test VPP | Yes |
| Microsoft OneDrive | iOS | iOS volume purchase program app | | Apple workshop test VPP | No |
| Microsoft Launcher | Android | Managed Google Play store app | | | No |
| Microsoft Intune Company Portal | iOS | iOS store app | | | No |
| Microsoft Intune | Android | Managed Google Play store app | | | No |
| Microsoft Excel | iOS | iOS volume purchase program app | | Apple workshop test VPP | Yes |
| Microsoft Authenticator | Android | Managed Google Play store app | | | No |
| Microsoft 365 Apps for Windows 10 | Windows | Microsoft 365 Apps (Windows 10 ... | | | Yes |
| Meraki Systems Manager | iOS | iOS volume purchase program app | | Apple workshop test VPP | No |
| Managed Home Screen | Android | Managed Google Play store app | | | No |
| Intune Company Portal | iOS | iOS volume purchase program app | | Apple workshop test VPP | No |
| Intune Company Portal | Android | Managed Google Play store app | | | No |



Slack for Desktop

Client Apps

Assign application to at least one group. Click 'Properties' then edit 'Assignments'.

Essentials

Publisher : Slack Technologies, Inc.

Operating system : macOS

Created : 2/21/2023, 3:17:38 PM

Assigned : No

Device status

0 TOTAL

Installed 0

Not Installed 0

Failed 0

Install Pending 0

Not Applicable 0

User status

0 TOTAL

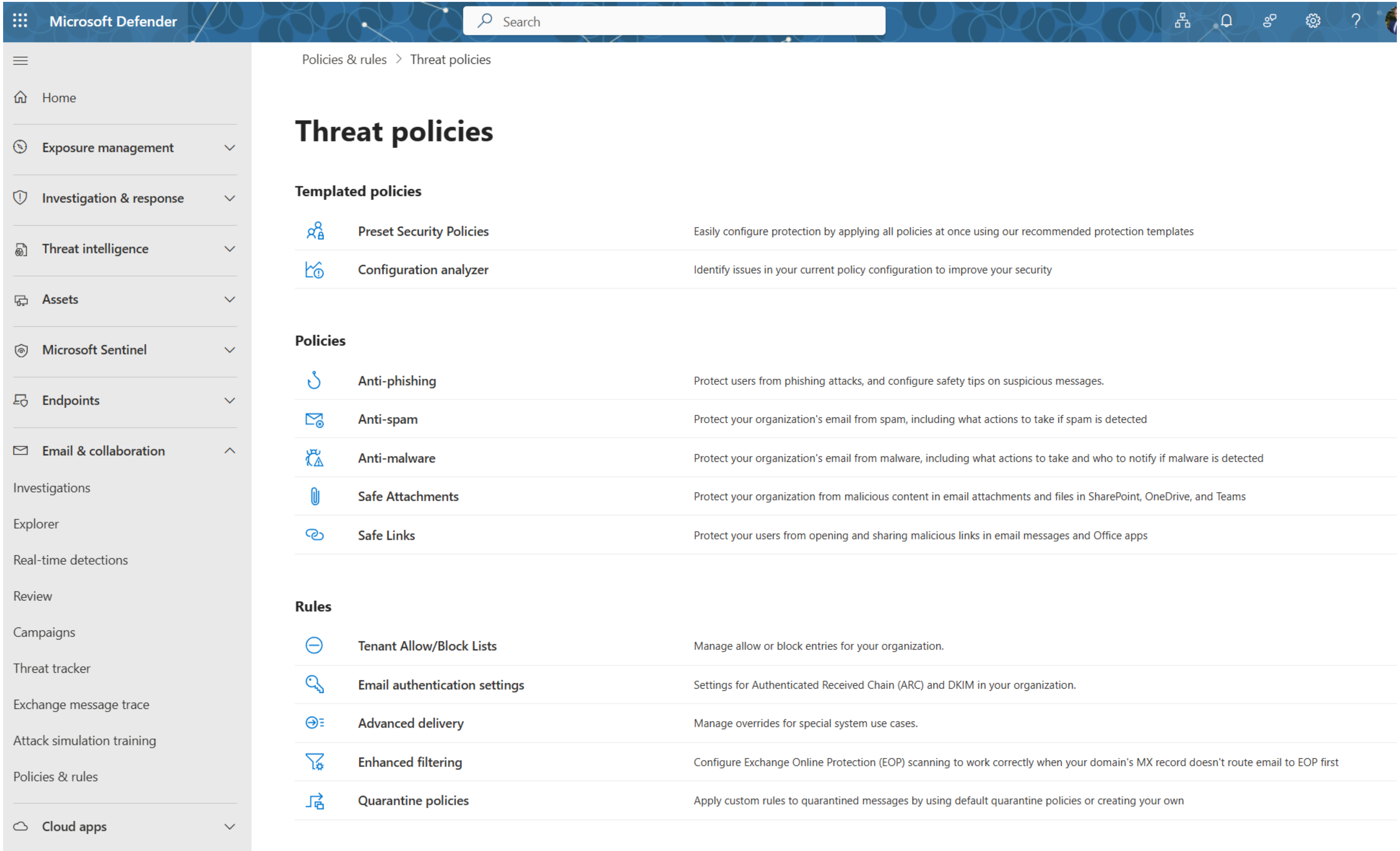
Installed 0

Not Installed 0

Failed 0

Install Pending 0

Not Applicable 0



Policies & rules > Threat policies

# Threat policies

## Templated policies

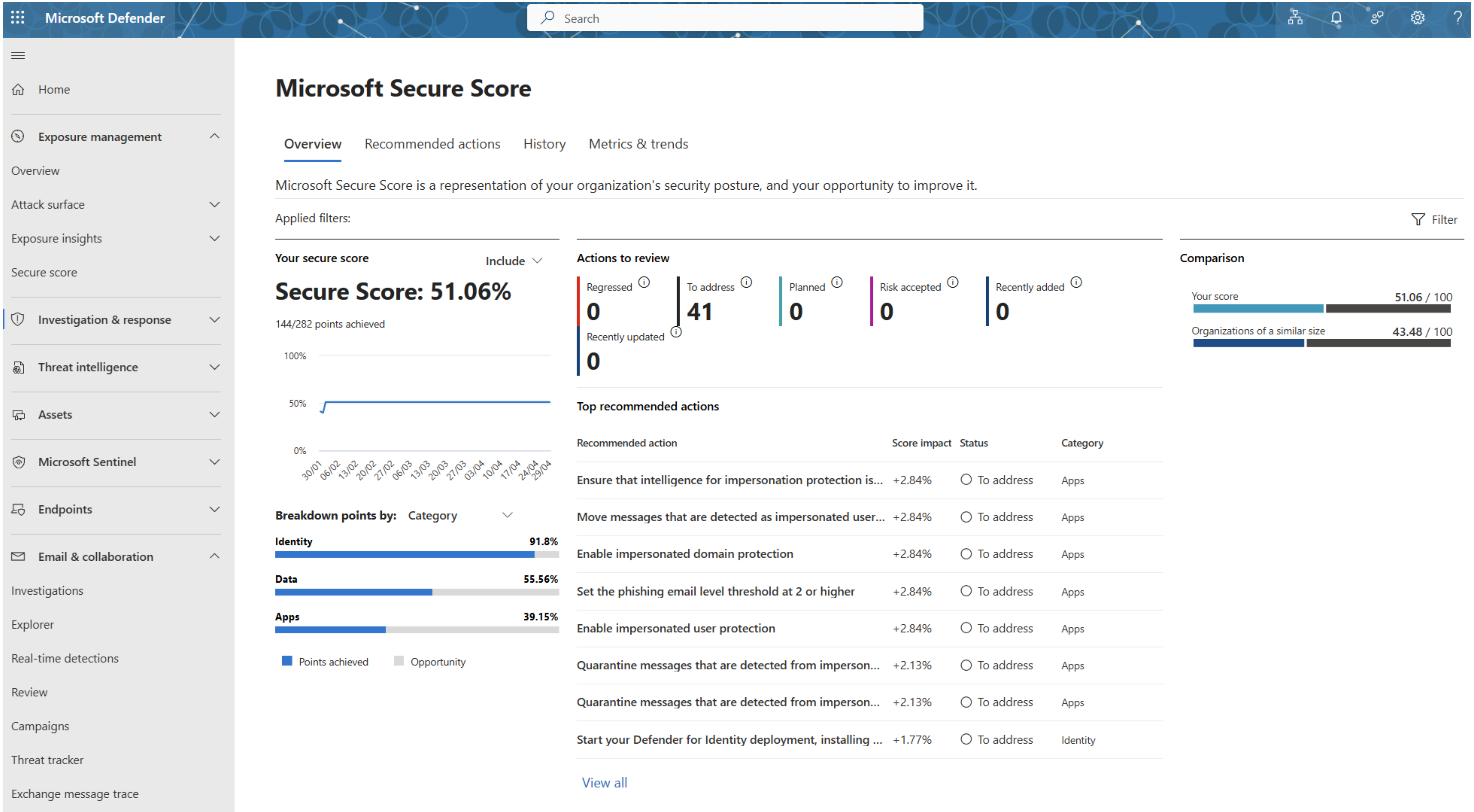
| | |
|---|---|
| Preset Security Policies | Easily configure protection by applying all policies at once using our recommended protection templates |
| Configuration analyzer | Identify issues in your current policy configuration to improve your security |

## Policies

| | |
|---|---|
| Anti-phishing | Protect users from phishing attacks, and configure safety tips on suspicious messages. |
| Anti-spam | Protect your organization's email from spam, including what actions to take if spam is detected |
| Anti-malware | Protect your organization's email from malware, including what actions to take and who to notify if malware is detected |
| Safe Attachments | Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams |
| Safe Links | Protect your users from opening and sharing malicious links in email messages and Office apps |

## Rules

| | |
|---|---|
| Tenant Allow/Block Lists | Manage allow or block entries for your organization. |
| Email authentication settings | Settings for Authenticated Received Chain (ARC) and DKIM in your organization. |
| Advanced delivery | Manage overrides for special system use cases. |
| Enhanced filtering | Configure Exchange Online Protection (EOP) scanning to work correctly when your domain's MX record doesn't route email to EOP first |
| Quarantine policies | Apply custom rules to quarantined messages by using default quarantine policies or creating your own |



# Microsoft Secure Score

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

Applied filters:

**Your secure score**

**Secure Score: 51.06%**

144/282 points achieved

**Breakdown points by:** Category

| | |
|---|---|
| **Identity** | **91.8%** |
| **Data** | **55.56%** |
| **Apps** | **39.15%** |

🟦 Points achieved ⬜ Opportunity

**Actions to review**

| Regressed | To address | Planned | Risk accepted | Recently added |
|---|---|---|---|---|
| 0 | 41 | 0 | 0 | 0 |

Recently updated
0

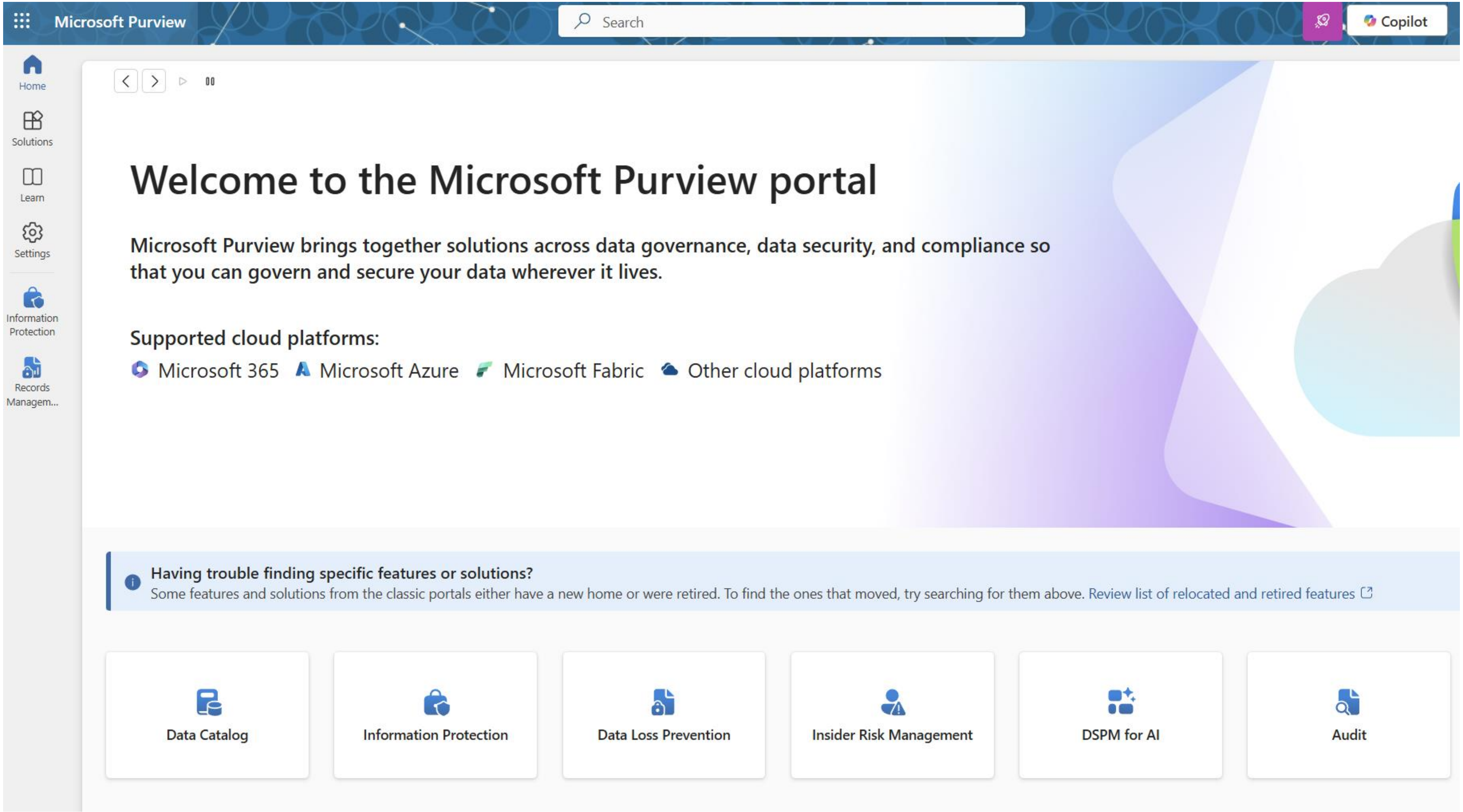
**Comparison**

| | |
|---|---|
| Your score | 51.06 / 100 |
| Organizations of a similar size | 43.48 / 100 |

**Top recommended actions**

| Recommended action | Score impact | Status | Category |
|---|---|---|---|
| Ensure that intelligence for impersonation protection is... | +2.84% | ○ To address | Apps |
| Move messages that are detected as impersonated user... | +2.84% | ○ To address | Apps |
| Enable impersonated domain protection | +2.84% | ○ To address | Apps |
| Set the phishing email level threshold at 2 or higher | +2.84% | ○ To address | Apps |
| Enable impersonated user protection | +2.84% | ○ To address | Apps |
| Quarantine messages that are detected from imperson... | +2.13% | ○ To address | Apps |
| Quarantine messages that are detected from imperson... | +2.13% | ○ To address | Apps |
| Start your Defender for Identity deployment, installing ... | +1.77% | ○ To address | Identity |

View all



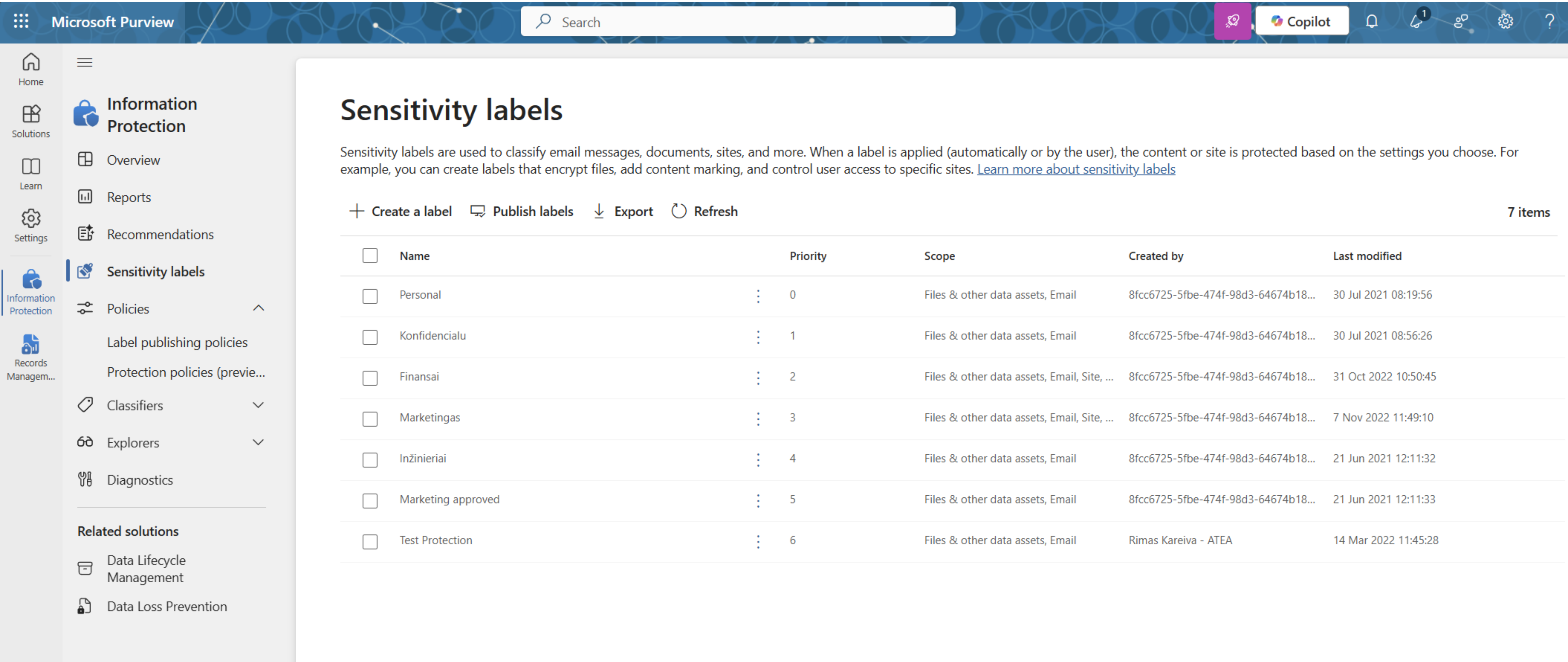
# Welcome to the Microsoft Purview portal

Microsoft Purview brings together solutions across data governance, data security, and compliance so that you can govern and secure your data wherever it lives.

Supported cloud platforms:

Microsoft 365 Microsoft Azure Microsoft Fabric Other cloud platforms

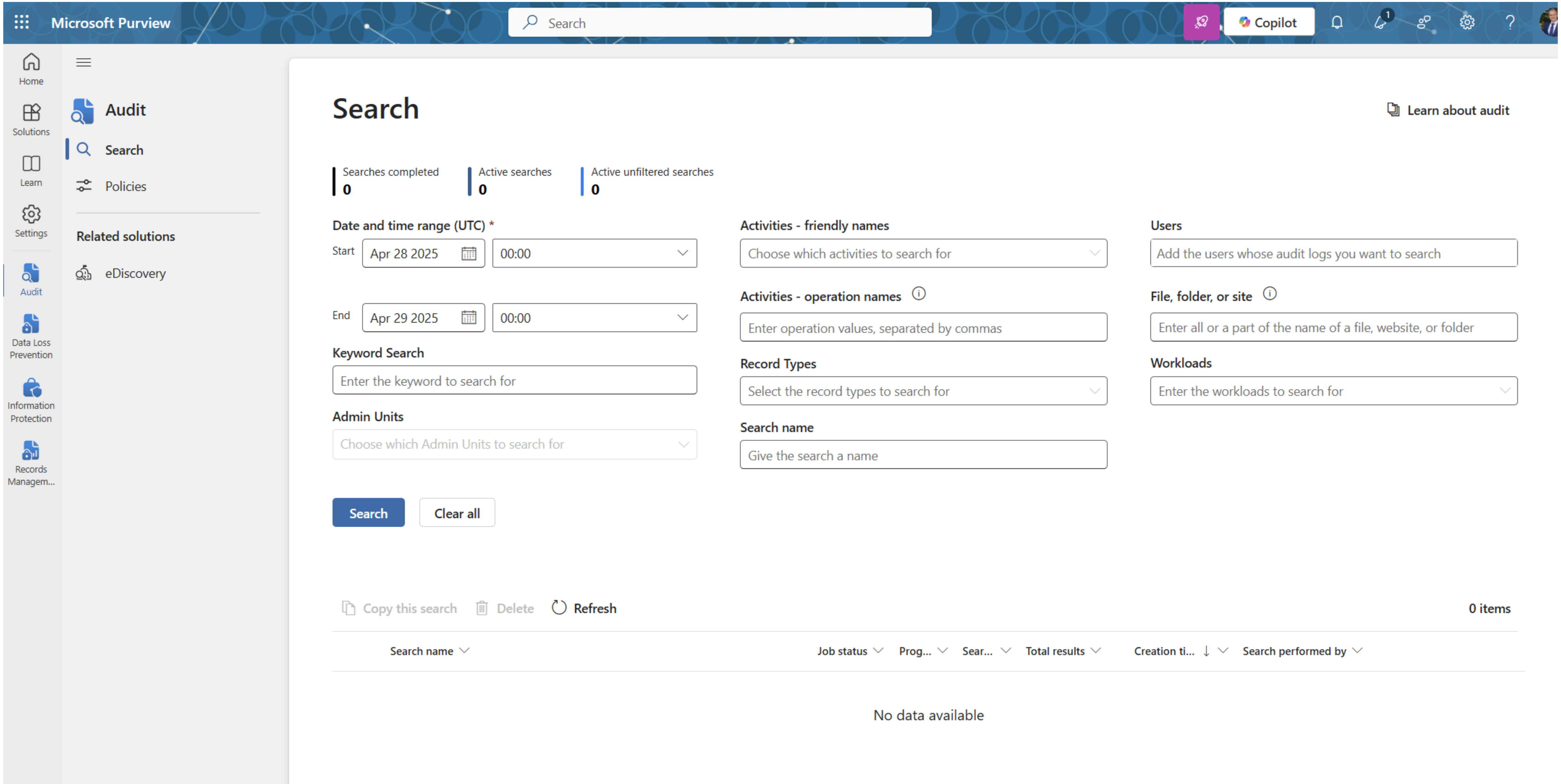
**Having trouble finding specific features or solutions?**
Some features and solutions from the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. Review list of relocated and retired features



# Sensitivity labels

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

| □ | Name | Priority | Scope | Created by | Last modified |
|---|---|---|---|---|---|
| □ | Personal | 0 | Files & other data assets, Email | 8fcc6725-5fbe-474f-98d3-64674b18... | 30 Jul 2021 08:19:56 |
| □ | Konfidencialu | 1 | Files & other data assets, Email | 8fcc6725-5fbe-474f-98d3-64674b18... | 30 Jul 2021 08:56:26 |
| □ | Finansai | 2 | Files & other data assets, Email, Site, ... | 8fcc6725-5fbe-474f-98d3-64674b18... | 31 Oct 2022 10:50:45 |
| □ | Marketingas | 3 | Files & other data assets, Email, Site, ... | 8fcc6725-5fbe-474f-98d3-64674b18... | 7 Nov 2022 11:49:10 |
| □ | Inžinieriai | 4 | Files & other data assets, Email | 8fcc6725-5fbe-474f-98d3-64674b18... | 21 Jun 2021 12:11:32 |
| □ | Marketing approved | 5 | Files & other data assets, Email | 8fcc6725-5fbe-474f-98d3-64674b18... | 21 Jun 2021 12:11:33 |
| □ | Test Protection | 6 | Files & other data assets, Email | Rimas Kareiva - ATEA | 14 Mar 2022 11:45:28 |



# Search

Searches completed 0

Active searches 0

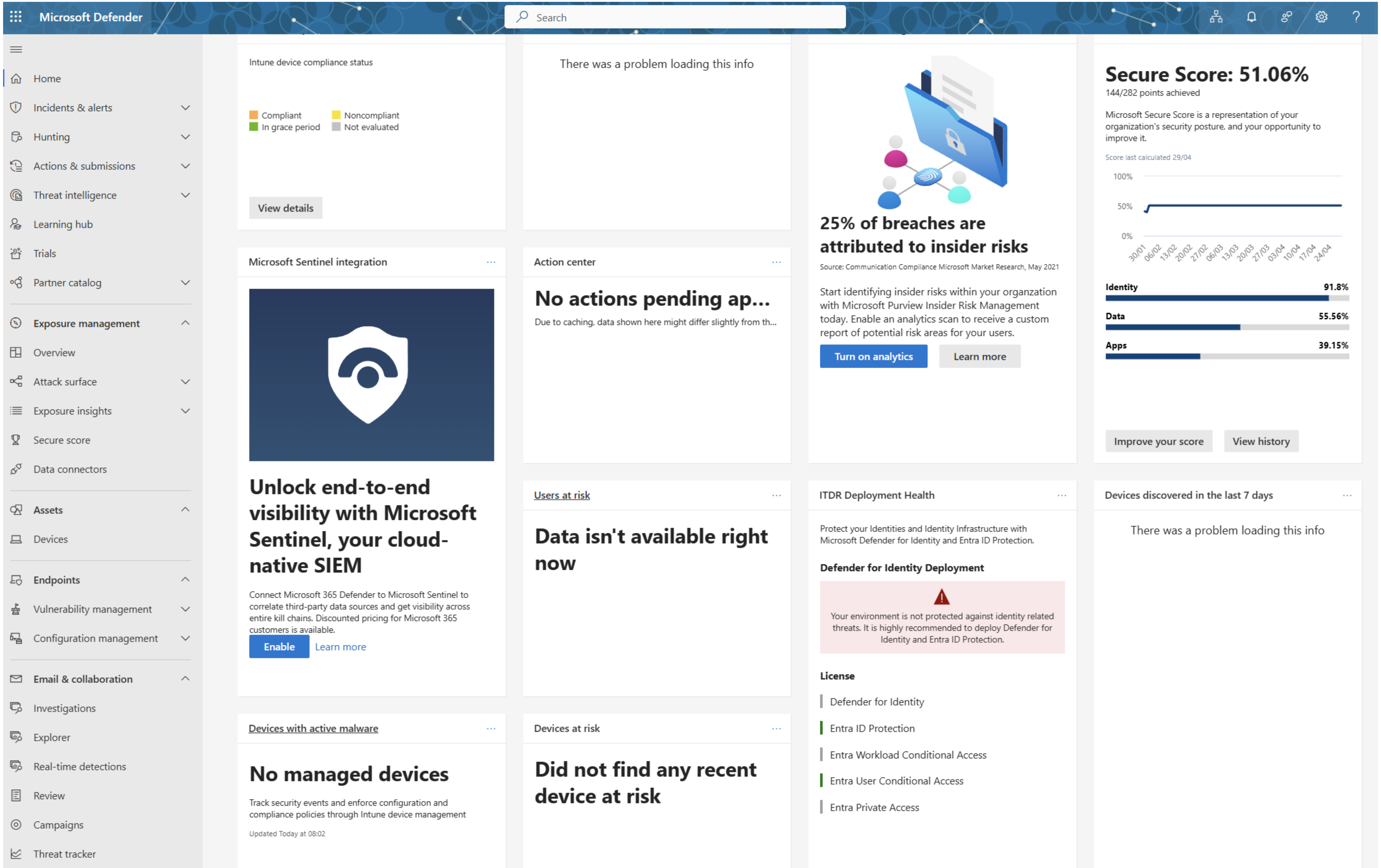
Active unfiltered searches 0

| | |
|---|---|
| Date and time range (UTC) * | |
| Start | Apr 28 2025 · 00:00 |
| End | Apr 29 2025 · 00:00 |
| Keyword Search | Enter the keyword to search for |
| Admin Units | Choose which Admin Units to search for |
| Activities - friendly names | Choose which activities to search for |
| Activities - operation names | Enter operation values, separated by commas |
| Record Types | Select the record types to search for |
| Search name | Give the search a name |
| Users | Add the users whose audit logs you want to search |
| File, folder, or site | Enter all or a part of the name of a file, website, or folder |
| Workloads | Enter the workloads to search for |

0 items

| Search name | Job status | Prog... | Sear... | Total results | Creation ti... ↓ | Search performed by |
|---|---|---|---|---|---|---|

No data available



Intune device compliance status

🟧 Compliant
🟨 Noncompliant
🟩 In grace period
⬜ Not evaluated

There was a problem loading this info

25% of breaches are attributed to insider risks

Source: Communication Compliance Microsoft Market Research, May 2021

Start identifying insider risks within your organzation with Microsoft Purview Insider Risk Management today. Enable an analytics scan to receive a custom report of potential risk areas for your users.

Secure Score: 51.06%

144/282 points achieved

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

Score last calculated 29/04

| | |
|---|---|
| Identity | 91.8% |
| Data | 55.56% |
| Apps | 39.15% |

Microsoft Sentinel integration

Unlock end-to-end visibility with Microsoft Sentinel, your cloud-native SIEM

Connect Microsoft 365 Defender to Microsoft Sentinel to correlate third-party data sources and get visibility across entire kill chains. Discounted pricing for Microsoft 365 customers is available.

Action center

No actions pending ap...

Due to caching, data shown here might differ slightly from th...

Users at risk

Data isn't available right now

ITDR Deployment Health

Protect your Identities and Identity Infrastructure with Microsoft Defender for Identity and Entra ID Protection.

Defender for Identity Deployment

Your environment is not protected against identity related threats. It is highly recommended to deploy Defender for Identity and Entra ID Protection.

License

- Defender for Identity
- Entra ID Protection
- Entra Workload Conditional Access
- Entra User Conditional Access
- Entra Private Access

Devices discovered in the last 7 days

There was a problem loading this info

Devices with active malware

No managed devices

Track security events and enforce configuration and compliance policies through Intune device management

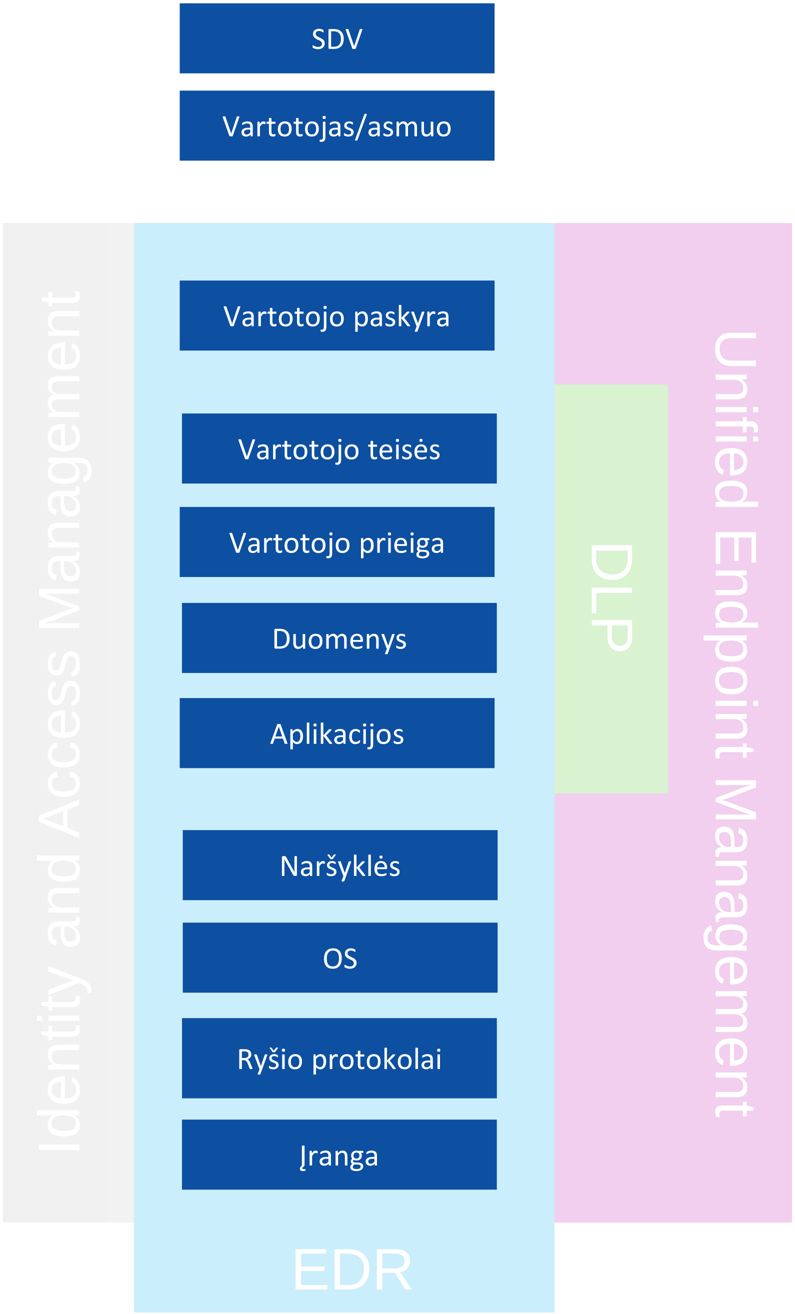
Updated Today at 08:02

Devices at risk

Did not find any recent device at risk

# Kaip stiprinti saugumą?

- Pasitikrinti/pakoreguoti visas bendrines tenant’o konfigūracijas
- Pasitikrinti/pakoreguoti atskirų aplikacijų saugumo nuostatas
- Peržiūrėti bendrines vartotojų, jų grupių nuostatas ir politikas
- Įvertinti galimybes naudojamas aplikacijas registruoti su Entra ID
- Įjungti MFA visoms prieigoms per Entra ID
- Pradėti taikyti *Conditional Access* politikas atskiroms aplikacijoms
- Įrenginius registruoti su ar įtraukti į Entra ID
- Pradėti naudoti MDM įrankius
  - Saugumo politikų taikymas, kontrolė ir atnaujinimas
  - Aplikacijų ir jų atnaujinimų diegimas (EDR, VPN, … )
- Įsivesti reagavimo į kibernetinius incidentus taisykles



SDV

Vartotojas/asmuo

Identity and Access Management

Vartotojo paskyra

Vartotojo teisės

Vartotojo prieiga

Duomenys

Aplikacijos

Naršyklės

OS

Ryšio protokolai

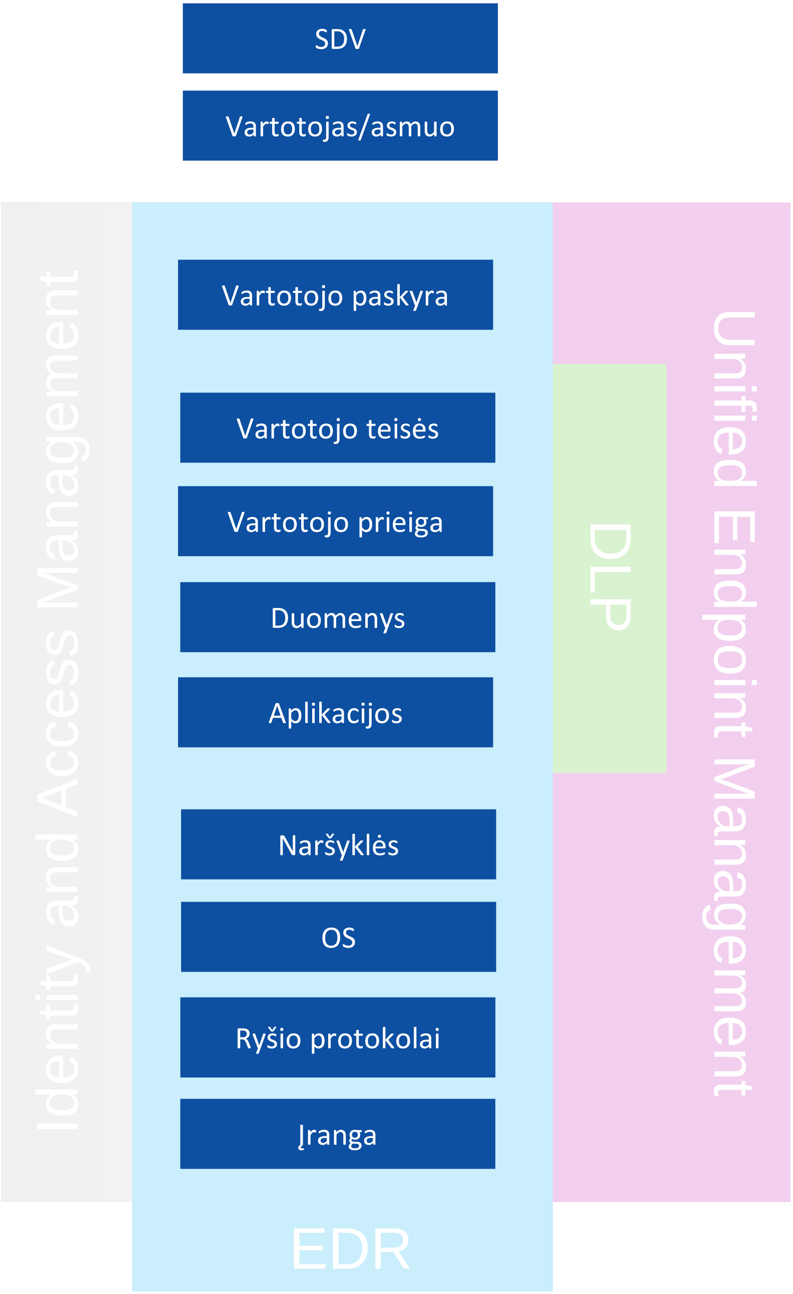
Įranga

EDR

DLP

Unified Endpoint Management

- Tvarka
- Įrankiai
- Instrukcijos
- Kontrolė



SDV

Vartotojas/asmuo

Identity and Access Management

Vartotojo paskyra

Vartotojo teisės

Vartotojo prieiga

Duomenys

Aplikacijos

Naršyklės

OS

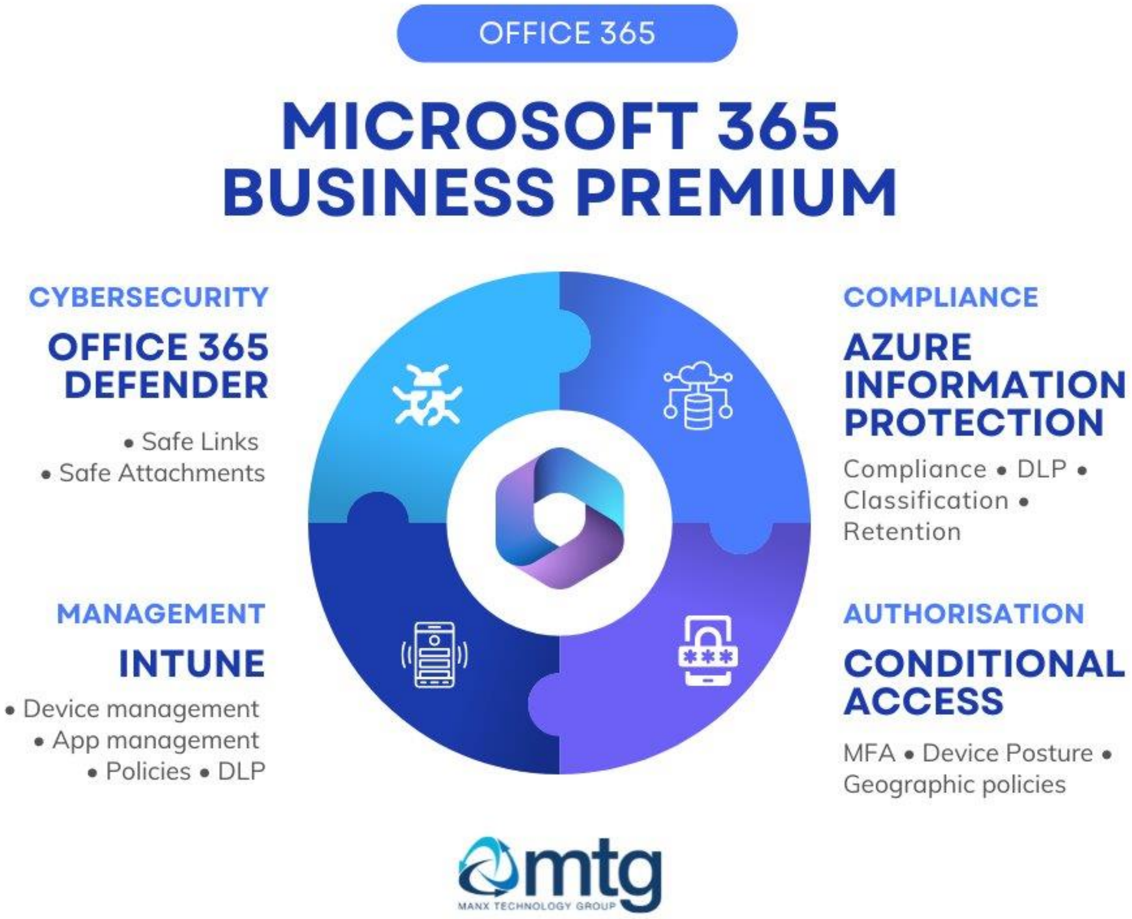
Ryšio protokolai

Įranga

EDR

DLP

Unified Endpoint Management



OFFICE 365

MICROSOFT 365 BUSINESS PREMIUM

CYBERSECURITY

OFFICE 365 DEFENDER

- Safe Links
- Safe Attachments

COMPLIANCE

AZURE INFORMATION PROTECTION

Compliance • DLP • Classification • Retention

MANAGEMENT

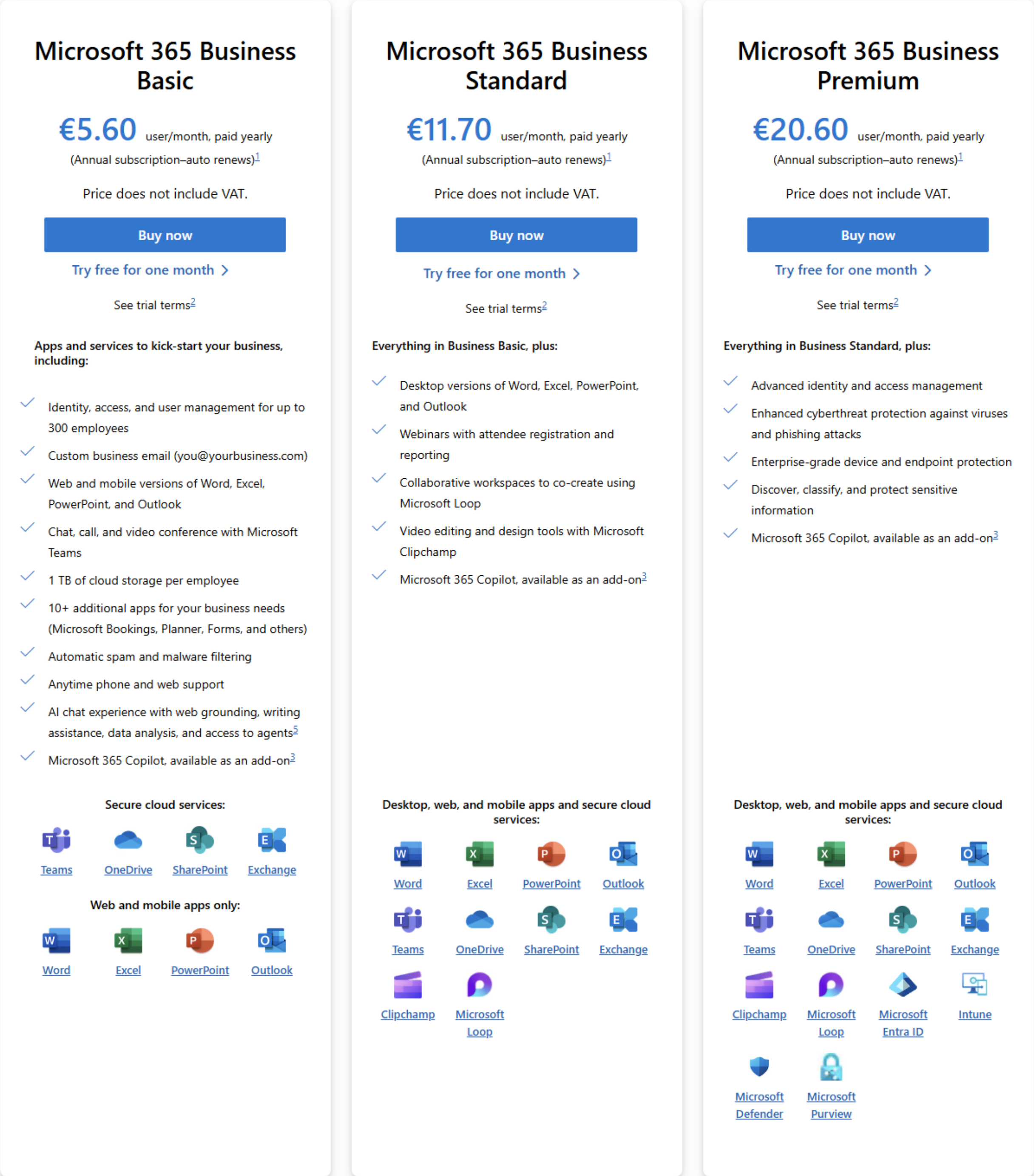
INTUNE

- Device management
- App management
- Policies • DLP

AUTHORISATION

CONDITIONAL ACCESS

MFA • Device Posture • Geographic policies



## Microsoft 365 Business Basic

€5.60 user/month, paid yearly

(Annual subscription–auto renews)[1]

Price does not include VAT.

Buy now

Try free for one month >

See trial terms[2]

**Apps and services to kick-start your business, including:**

- ✓ Identity, access, and user management for up to 300 employees
- ✓ Custom business email (you@yourbusiness.com)
- ✓ Web and mobile versions of Word, Excel, PowerPoint, and Outlook
- ✓ Chat, call, and video conference with Microsoft Teams
- ✓ 1 TB of cloud storage per employee
- ✓ 10+ additional apps for your business needs (Microsoft Bookings, Planner, Forms, and others)
- ✓ Automatic spam and malware filtering
- ✓ Anytime phone and web support
- ✓ AI chat experience with web grounding, writing assistance, data analysis, and access to agents[5]
- ✓ Microsoft 365 Copilot, available as an add-on[3]

**Secure cloud services:**

Teams OneDrive SharePoint Exchange

**Web and mobile apps only:**

Word Excel PowerPoint Outlook

## Microsoft 365 Business Standard

€11.70 user/month, paid yearly

(Annual subscription–auto renews)[1]

Price does not include VAT.

Buy now

Try free for one month >

See trial terms[2]

**Everything in Business Basic, plus:**

- ✓ Desktop versions of Word, Excel, PowerPoint, and Outlook
- ✓ Webinars with attendee registration and reporting
- ✓ Collaborative workspaces to co-create using Microsoft Loop
- ✓ Video editing and design tools with Microsoft Clipchamp
- ✓ Microsoft 365 Copilot, available as an add-on[3]

**Desktop, web, and mobile apps and secure cloud services:**

Word Excel PowerPoint Outlook

Teams OneDrive SharePoint Exchange

Clipchamp Microsoft Loop

## Microsoft 365 Business Premium

€20.60 user/month, paid yearly

(Annual subscription–auto renews)[1]

Price does not include VAT.

Buy now

Try free for one month >

See trial terms[2]

**Everything in Business Standard, plus:**

- ✓ Advanced identity and access management
- ✓ Enhanced cyberthreat protection against viruses and phishing attacks
- ✓ Enterprise-grade device and endpoint protection
- ✓ Discover, classify, and protect sensitive information
- ✓ Microsoft 365 Copilot, available as an add-on[3]

**Desktop, web, and mobile apps and secure cloud services:**

Word Excel PowerPoint Outlook

Teams OneDrive SharePoint Exchange

Clipchamp Microsoft Loop Microsoft Entra ID Intune

Microsoft Defender Microsoft Purview