

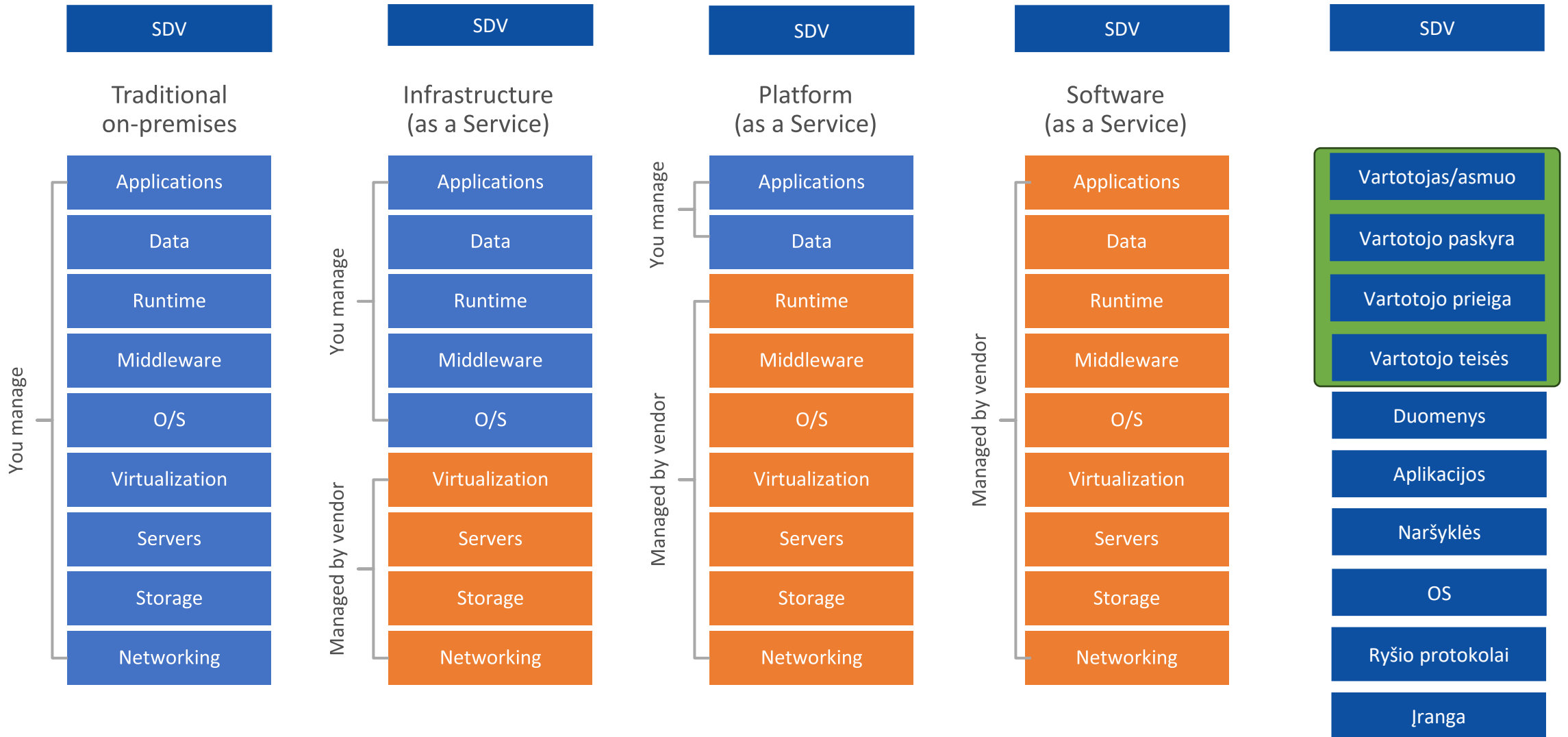
*Greitos ir maksimaliai efektyvios priemonės
skaitmeninei tapatybei apsaugoti*

Rimas Kareiva
Skaitmeninių darbo vietų kompetencijų centras
Grupės vadovas

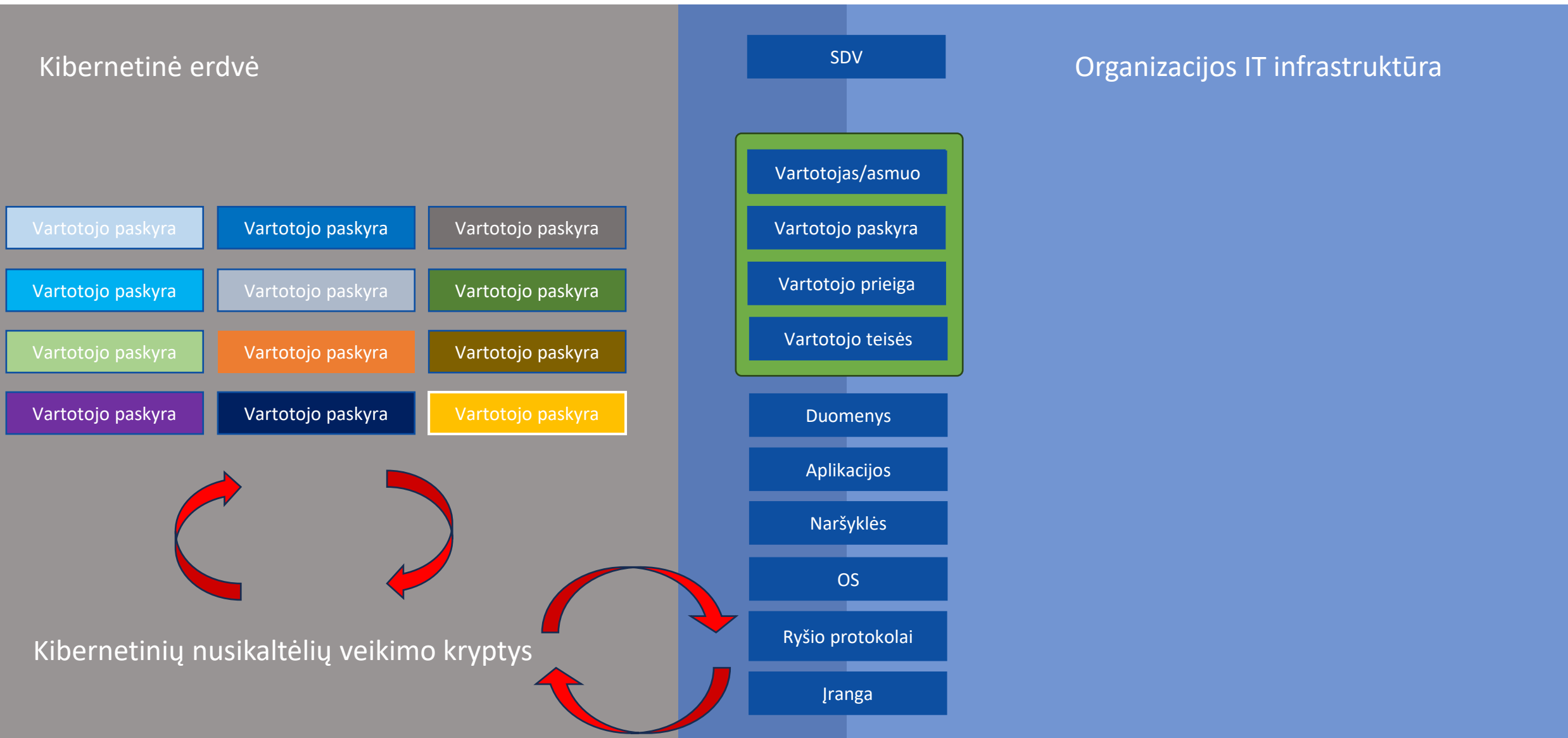
rimas.kareiva@atea.lt

ATEA

Skaitmeninė tapatybė – kas tai?



Skaitmeninė tapatybė – problematika



In Azure Active Directory we observe 50 million password attacks daily, yet only 20% of users and 30% of global admins are using strong authentications such as MFA.

Microsoft Digital Defense Report | October 2021

*Hackers don't break in,
they log in.*

Microsoft Entra data shows that of more than 600 million identity attacks per day, more than 99% are password-based. Advances such as default security configurations and Conditional Access policies have helped more organizations embrace multifactor authentication (MFA), increasing adoption to 41% among Microsoft enterprise customers.

Microsoft Digital Defense Report | October 2024

Entra ID MFA

Username
someone@example.com
Password



- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
- Overview
- Users
- Groups
- Devices
- Applications
- Protection
- Identity Governance
- External Identities
- Show more
- Protection

Home > ATEA, UAB >

ATEA, UAB

[+](#) Add [Manage tenants](#) [What's new](#) |
 [Preview features](#) |
 [Got feedback?](#)

[Overview](#) |
 [Monitoring](#) |
 [Properties](#) |
 [Recommendations](#) |
 [Setup guides](#)

Search your tenant

Basic information

Name	ATEA, UAB	Users	204
Tenant ID	474253dd-9e4a-4eec-898d-d64d21c73ba4 📄	Groups	144
Primary domain	atealt0365.onmicrosoft.com	Applications	35
License	Microsoft Entra ID Free	Devices	59

Alerts



Migrate to the converged Authentication methods policy

Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact

[Learn more](#) [🔗](#)

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
 - Overview
 - Users
 - Groups
 - Devices
 - Applications
 - Protection
 - Identity Governance
 - External Identities
 - Show more
- Protection
- Identity Governance
- Verified ID
- Permissions Management
- Learn & support

Home > ATEA, UAB >

ATEA, UAB

+ Add Manage tenants What's new Preview features Got feedback?

Overview Monitoring **Properties** Recommendations Setup guides

Country or region	Lithuania
Data location	EU Model Clause compliant datacenters
Notification language	English
Tenant ID	474253dd-9e4a-4eec-898d-d64d21c73ba4
Technical contact	pagalba@atealto365.onmicrosoft.com
Global privacy contact	
Privacy statement URL	https://www.atea.lt/apie-atea/asmens-duomenu-saugumas/

Access management for Azure resources

Rimas Kareiva (rimas.kareiva@atealt0365.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this tenant. [Learn more](#)

Yes

Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will... [Learn more](#)

Your organization is protected by security defaults. [Manage security defaults](#)

Save Discard

Security defaults

Security defaults
Enabled (recommended)

Your organization is currently using security defaults.

99.9% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.

Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.

Save Cancel

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 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 here.

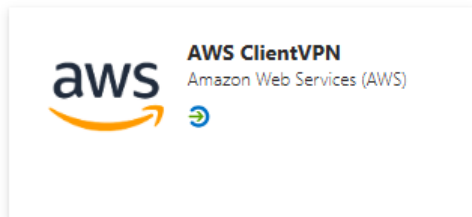
Single Sign-on : All

User Account Management : All

Categories : All

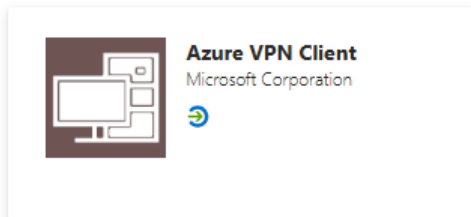
[🔄 Federated SSO](#) | [🔄 Provisioning](#)

Showing 4 of 4 results



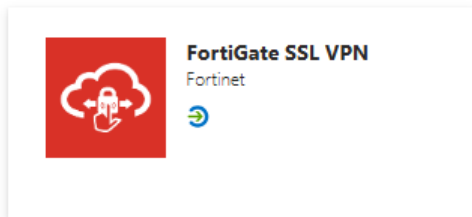
AWS ClientVPN
Amazon Web Services (AWS)

🔄



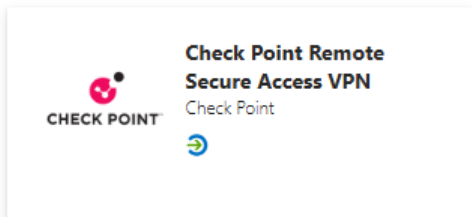
Azure VPN Client
Microsoft Corporation

🔄



FortiGate SSL VPN
Fortinet

🔄



Check Point Remote Secure Access VPN
Check Point

🔄

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
- Overview
- Users
- Groups
- Devices
- Applications
 - Enterprise applications
 - App registrations
- Protection
- Identity Governance
- External Identities

Microsoft Entra admin center

🏠 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

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 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 organiz

🔍 Search application


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

Cloud platforms


Amazon Web Services (AWS)



Google Cloud Platform



Oracle



On-premises applications

Add an on-premises application

Configure Microsoft Entra application proxy to enable secure remote access.

Learn about Application Proxy

Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

On-premises app

Automate creating, up premises or in a virtual

🔄 Federated SSO 🔄 Provisioning

Create your own application

🗨️ Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Input name

- What are you looking to do with your application?
- Configure Application Proxy for secure remote access to an on-premises application
 - Register an application to integrate with Microsoft Entra ID (App you're developing)
 - Integrate any other application you don't find in the gallery (Non-gallery)

App registrations

+ New registration | Endpoints | Troubleshoot | Refresh | Download | Preview features | Got feedback?

i Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. You may need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications | Owned applications | Deleted applications

vpn Add filters

2 applications found

Display name	Application (client) ID	Created on
fs FortiGate SSL VPN	afe69e7b-a8e6-4cd3-ba5d-928bcc41e3bc	9/8/2023
vs VPN Server	b21da5b8-ee70-4892-9d1c-b7e1a5ff94f9	3/21/2023

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
 - Overview
 - Users
 - Groups
 - Devices
 - Applications
 - Enterprise applications
 - App registrations**
 - Protection

- Home
- Diagnose & solve problems
- Favorites
- Identity
- Protection
 - Security Center
 - Identity Secure Score
 - Multifactor authentication
 - Authentication methods
 - Password reset
 - Custom security attributes
 - Show less
- Identity Governance
- Verified ID
- Permissions Management
- Global Secure Access

Home >

Per-user multifactor authentication

Bulk update | Got feedback?

Do not allow users to create app passwords to sign in to non-browser apps

Trusted IPs [Learn more](#)

Skip multifactor authentication for requests from federated users on my intranet

Skip multifactor authentication for requests from following range of IP address subnets:

Verification options [Learn more](#)

i Authentication methods for MFA and SSPR can now be managed in one converged policy. [Learn more](#)

Methods available to users:


- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

Remember multifactor authentication on trusted device [Learn more](#)


Allow users to remember multifactor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for

For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. [Learn more about reauthentication prompts](#)




For your desktop or laptop




YubiKey 5C Nano FIPS

Two Factor Authentication USB Security Key, Fits USB-A Ports - Protect Your Online Accounts with More Than a Password, FIDO Certified USB Password Key, Extra Compact Size

- 1 + [Add](#) [Learn More](#)



For your mobile device



YubiKey 5C NFC FIPS

Two Factor Authentication USB and NFC Security Key, Fits USB-C Ports and Works with Supported NFC Mobile Devices - Protect Your Online Accounts with More Than a Password

- 1 + [Add](#) [Learn More](#)

- 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

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

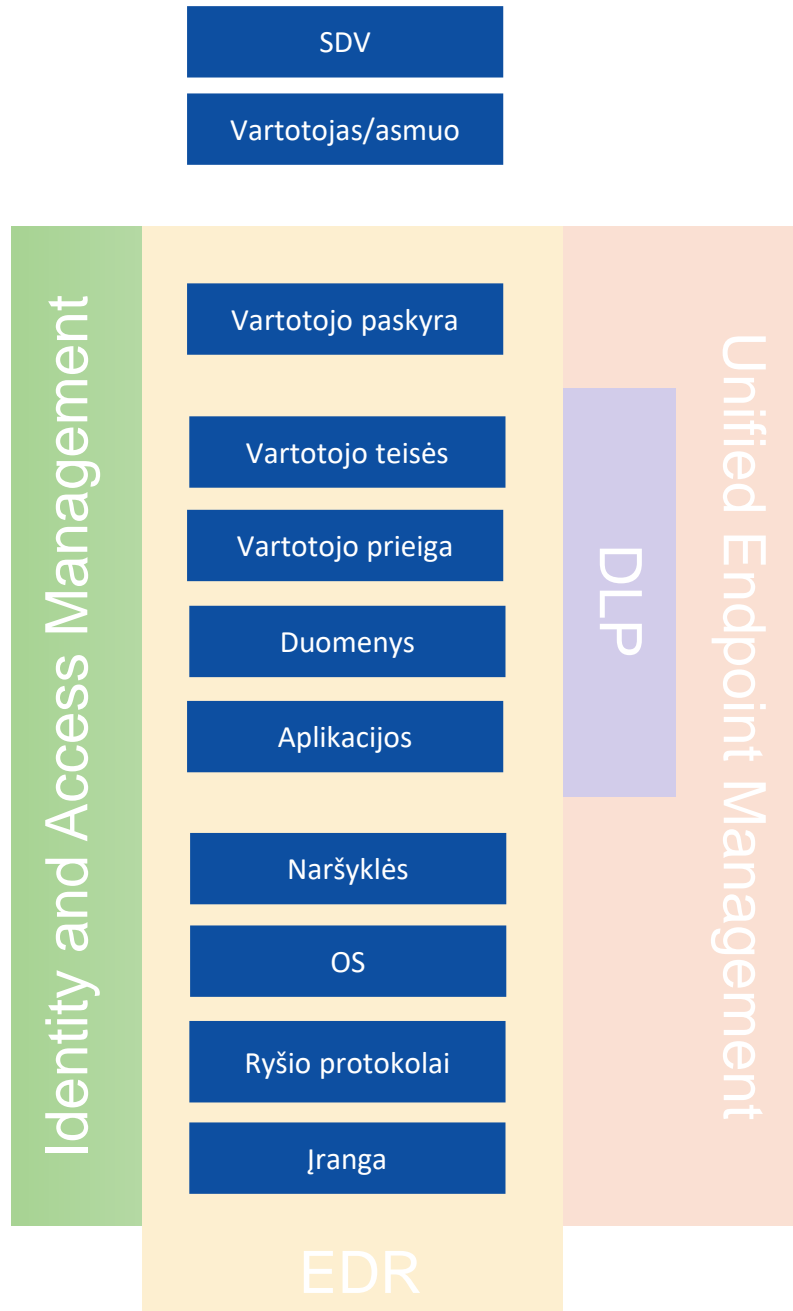
Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected



- Tvarka
- Įrankiai
- Instrukcijos
- Kontrolė

Ačiū už kantrybę ir dėmesį!!!

Klausimai?

Rimas Kareiva

Skaitmeninių darbo vietų kompetencijų centro vadovas

rimas.kareiva@atea.lt

ATEA