

Išmanus darbo vietų įrangos valdymas

Rimas Kareiva
Skaitmeninių darbo vietų kompetencijų centro vadovas

rimas.kareiva@atea.lt

ATEA

Pagrindinė žinutė

Unifikuotas SDV valdymas (angl. UEM)

Integruoti platforminiai sprendimai

Pilno SDV gyvavimo ciklo supratimas





Active Directory

GPO

MAM

OS image deployment

Security management

RMM

MDM

WSUS

Application deployment

Patching

<<

Home >

Devices | Overview

Search

Refresh

View tour

Overview

All devices

Monitor

By platform

Windows

iOS/iPadOS

macOS

Android

Linux

Device onboarding

Windows 365

Enrollment

Manage devices

Configuration

Compliance

Conditional access

Scripts and remediations

Windows 10 and later updates

Apple updates

Group Policy analytics

eSIM cellular profiles (preview)

Policy sets

Android FOTA deployments

Device clean-up rules

Device categories

Filters

Partner portals

Manage devices by platform

Windows
0 devices

iOS/iPadOS
0 devices

macOS
0 devices

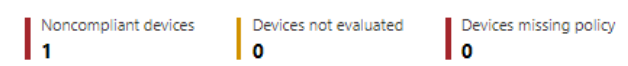
Android
1 device

Linux
0 devices

Configuration policy assignment failures

✔ No profiles with errors or conflicts

Noncompliant devices



Deployment status per Windows update ring

✔ No devices with error or conflict

Additional monitoring reports

Device actions
View a list of requested device actions and their statuses

Other devices


ChromeOS
Set up the enterprise connector and view ChromeOS devices

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support


Home > Devices

Devices | Partner portals ...

- All devices
- Monitor
- By platform
- Windows
- iOS/iPadOS
- macOS
- Android
- Linux
- Device onboarding
- Windows 365
- Enrollment
- Manage devices
- Configuration
- Compliance
- Conditional access
- Scripts and remediations
- Windows 10 and later updates
- Apple updates
- Group Policy analytics
- eSIM cellular profiles (preview)
- Policy sets
- Android FOTA deployments
- Device clean-up rules
- Device categories
- Filters
- Partner portals



HP Connect
Update, configure, and secure the BIOS on your HP devices



Surface Management Portal
Manage your Surface devices and warranties

Create New Policy

- 1 Policy Information
- 2 Policy Settings

Policy Settings

Enter the information below to create a new policy

Should this policy manage BIOS settings globally or only a specific HP Platform?

Select Global Policy to have these BIOS settings take effect on all HP Platforms inside a group. Some unique platform-specific settings may not be available.

Select Platform Policy to assign BIOS settings to a specific HP Platform.

- Global Policy
- Platform Policy

HP ProBook 450 G6 Notebook PC - 8538, R71

Search BIOS Settings

You have no settings selected Show Selected Only

- Allow OPAL Hard Drive SID Authentication
Default Value: Disable
- Asset Tracking Number
Default Value: Not Configured
- Audio Alerts During Boot
Default Value: Enable
- Audio Device
Default Value: Enable
- Automatic BIOS Update Setting
Default Value: Disable
- Automatically Check for Updates
Default Value: Monthly
- Backlit keyboard timeout
Default Value: 15 secs.
- Battery Health Manager
Default Value: Let HP manage my battery charging
- BIOS Administrator visible at Power-on Authentication
Default Value: Enable
- BIOS Power-On Hour
Default Value: 0
- BIOS Power-On Minute
Default Value: 0

Cancel

Previous

Save

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

- Home >
- ## Apps | Overview
- Search
- Overview
 - All apps
 - Monitor
- By platform
- Windows
 - iOS/iPadOS
 - macOS
 - Android
- Policy
- App protection policies
 - App configuration policies
 - iOS app provisioning profiles
 - S mode supplemental policies
 - Policies for Office apps
 - Policy sets
 - Quiet time
- Other
- App selective wipe
 - App categories
 - E-books
 - Filters
- Help and support
- Help and support

Microsoft Intune recommends managing Microsoft 365 Apps with Current Channel. [Learn more](#)

Essentials

Tenant name : atealtO365.onmicrosoft.com
 Tenant location : Europe 0201

MDM authority : Microsoft Intune
 Account status : [Active](#)

Installation status App protection policy status

Top installation failures by devices

Microsoft Intune	Android	0
FileZilla FTP Client v3.31....	Windows	0
Circle K	iOS	0

Apps with installation failures

0

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home >

Endpoint security | Overview

Search

- Overview

- All devices
 - Security baselines
 - Security tasks
- Manage**
- Antivirus
 - Disk encryption
 - Firewall
 - Endpoint Privilege Management
 - Endpoint detection and response
 - App Control for Business (Preview)
 - Attack surface reduction
 - Account protection
 - Device compliance
 - Conditional access
- Monitor**
- Assignment failures
- Setup**
- Microsoft Defender for Endpoint
- Help and support**
- Help and support

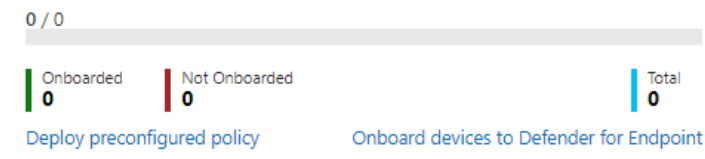
Summary

Refresh Report generated 05/28/2024, 05:43 AM

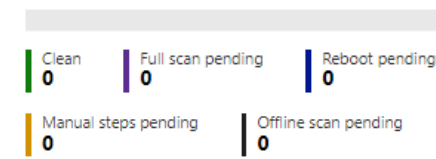
Defender for Endpoint Connector Status

Defender for Endpoint connector unavailable

Windows devices onboarded to Defender for Endpoint



Antivirus agent status



Other monitoring reports

- Detected Malware**
 See the malware state of your devices.
- Firewall Status**
 View if Defender Firewall is enabled on devices.
- Link to Defender portal for more**
 View sensor and AV health data.

Tenant admin | Intune add-ons

All add-ons Your add-ons Capabilities

Refresh

The Intune add-ons below are available for trial or purchase. If your organization has more than one billing account, you'll only see subscription status for the account you've selected. [Learn more about Intune add-ons](#)

- Tenant status
- Remote Help
- Microsoft Tunnel Gateway
- Cloud PKI
- Connectors and tokens
- Filters
- Roles
- Microsoft Entra Privileged Identity Management
- Diagnostics settings
- Audit logs
- Device diagnostics
- Multi Admin Approval
- Intune add-ons**
- Copilot (preview)
- End user experiences
 - Customization
 - Organizational messages
 - Custom notifications
 - Terms and conditions
- Windows Autopatch
 - Tenant enrollment
- Microsoft Managed Desktop
 - Tenant enrollment
- Help and support
 - Help and support

Intune add-on name	Subscription status	Description	Try o
Microsoft Intune Suite	Available for trial or purchase	A suite of advanced endpoint and security management solutions unified in Microsoft Intune that includes these standalone add-ons: Learn more about Microsoft Intune Suite	View
Remote Help		Remote Help allows secure, helpdesk-to-endpoint connections with role-based remote access permissions. Additionally, ServiceNow incidents are visible in Troubleshooting. Learn more about Remote Help	
Intune Plan 2		Intune Plan 2 is an add-on bundle to the Microsoft Intune service that offers a collection of advanced endpoint management capabilities. Learn more about Intune Plan 2	
Endpoint Privilege Management		Microsoft Intune Endpoint Privilege Management allows standard users to perform elevations approved by their organization. Learn more about Endpoint Privilege Management	
Enterprise App Management		Microsoft Intune Enterprise App Management enables IT admins to easily discover prepackaged apps, deploy them, and keep them updated using a securely hosted enterprise catalog. Learn more about Enterprise App Management	
Advanced Analytics		With fuller visibility into the state of your environment and actionable insights, Microsoft Intune Advanced Analytics enables simple, secure endpoint management and helps you proactively Learn more about Advanced Analytics	



Home > Tenant admin

Tenant admin | Copilot (preview) ...

- Tenant status
- Remote Help
- Microsoft Tunnel Gateway
- Cloud PKI
- Connectors and tokens
- Filters
- Roles
- Microsoft Entra Privileged Identity Management
- Diagnostics settings
- Audit logs
- Device diagnostics
- Multi Admin Approval
- Intune add-ons
- Copilot (preview)

End user experiences

- Customization
- Organizational messages
- Custom notifications
- Terms and conditions

Windows Autopatch

- Tenant enrollment

Microsoft Managed Desktop

- Tenant enrollment

Help and support

- Help and support

Copilot hasn't been set up yet. To use Copilot, your Global or Billing Administrator will have to add capacity. Then have your Security Administrator set it up. [Learn more about setting up Copilot for Security](#)

Refresh

Copilot in Intune

Not set up

What can you do with Microsoft Copilot in Intune?

Copilot can help you with regular management tasks like policy management and troubleshooting devices. Look for Copilot throughout Intune to help you understand and manage your devices more efficiently and effectively.

[Learn more about Copilot in Intune](#)

How Copilot works

How Copilot in Intune gets answers

When you ask Copilot a question in Intune, it gets sent to Copilot for Security, which processes the input and generates a response. Copilot for Security uses data from your tenant and authoritative Microsoft documentation sources to generate its response.

The response comes back from Copilot for Security and is displayed in Intune. You can see all of your interactions in Copilot for Security by looking at your sessions in [Copilot for Security](#)

[Privacy and data security in Microsoft Copilot for Security](#)

Interpreting Copilot's results

Monitoring usage

Let us know how Copilot is doing

Copilot can make mistakes so remember to verify the results. To help improve the experience, share your feedback with us as you use Copilot.

Pagrindinė žinutė

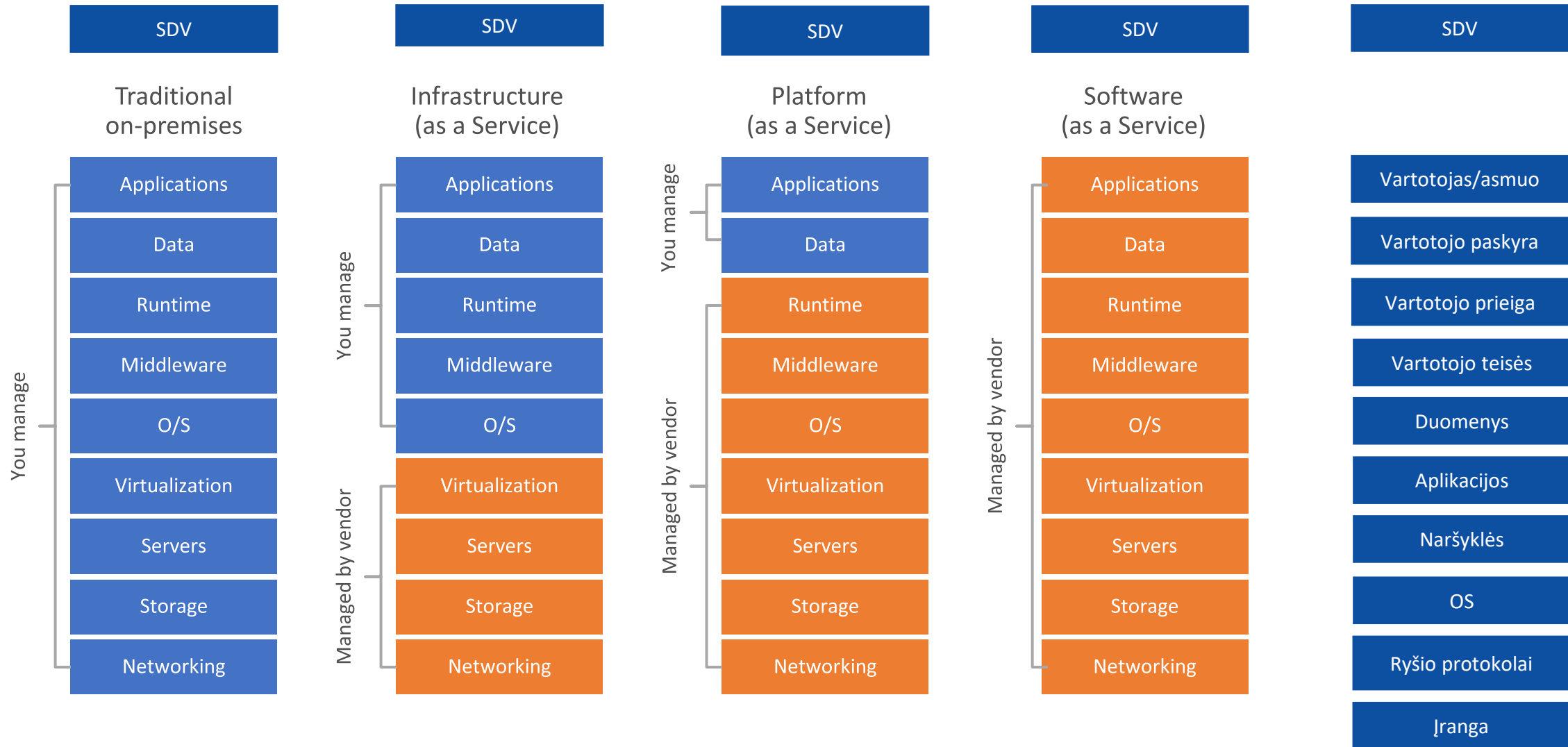
Unifikuotas SDV valdymas (angl. UEM)

Integruoti platforminiai sprendimai

Pilno SDV gyvavimo ciklo supratimas



DIGITAL WORKPLACE – Skaitmeninė darbo vieta



Office 365

Activity Reports	Adoption Score	Alert Policies	Audio Conferencing (free add-on)	Audit (standard)	Basic Mobility & Security
Bookings	Briefing Email	Compliance Manager	Content Search	Data Loss Prevention	Defender for Office 365 Plan 1
eDiscovery (standard)	Exchange Online Archiving	Exchange Online Plan 1	Information Protection for M365	Message Encryption (basic)	Microsoft 365 Apps for Business (with SCA)
Microsoft 365 Mobile App	Microsoft Dataverse for Teams	Microsoft Forms	Microsoft Lists	Microsoft Search	Microsoft Teams
Microsoft To Do	Microsoft Whiteboard	Office for the Web (incl Visio)	OneDrive for Business Plan 1	Planner	Power Apps for Office 365
Power Automate for Office 365	Power Virtual Agents for Teams	Project & Roadmap View Access	Secure Score	SharePoint Online Plan 1	Stream for Office 365
Sway	Viva Connections	Viva Engage	Viva Insights - Personal (basic)	Viva Learning (basic)	Webinars

Office 365

Enterprise Mobility + Security

Application Management			Device Management		Endpoint Analytics		Information Protection	
Intune Plan 1 for Business								
Administrative Units	Advanced Security Reports & Alerts	App Proxy, including PingAccess	Cloud App Discovery	Conditional Access	Custom Security Attributes			
Customized Sign-In Page	Dynamic Groups	Enterprise State Roaming	Entra ID Connect Health	External ID	Microsoft Identity Manager			
Multi-Factor Auth (MFA)	Password Protection	Passwordless Authentication	Self-Service Group Management	Self-Service Password Reset in AD	Self-Service Activity Reports			
Service Level Agreement	Shared Account Password Roll-Over	Single-Sign-On to other SaaS	SMS Sign-In	Temporary Access Pass	Terms of Use			
Verified ID	Windows Autopilot	3rd Party MFA Integration						
Entra ID Plan 1								

Enterprise Mobility + Security

Windows Pro

Application Control	Application Guard	AppLocker	Assigned Access
BitLocker	BitLocker to Go	Cortana	Defender Antivirus
Domain Join	Edge for Business	Entra ID Join	LAPS
Manage by MDM	Power Automate Attended Desktop Flows	Unbranded Boot	Universal Print
Windows Conditional Access	Windows Firewall	Windows Hello for Business	Windows Information Protection (retiring)
Windows Update for Business	24 months support for Windows 11		

Microsoft 365 Business Premium includes Windows Pro upgrade from earlier Pro versions + Universal Print

Windows Pro

Automated Investigations	Block at First Sight
Cross-Platform Support	Endpoint Detection & Response
Enhanced ASR	Mobile Threat Defence
Next Gen Protection	Tamper Protection
Threat Analytics	Vulnerability Management (core)
Web Content Filtering	
Defender for Business	

Office 365 F3

Activity Reports	Adoption Score	Alert Policies	Audio Conferencing (free add-on)	Audit (standard)
Basic Mobility & Security	Bookings	Compliance Manager	Content Search	Entra ID for Office 365
Exchange Online Kiosk (2 GB)	Exchange Online Protection	Information Protection for M365 (from EMS E3)	Kaizala Pro (retiring)	Message Encryption (basic) (from EMS E3)
Microsoft 365 Mobile App	Microsoft Dataverse for Teams	Microsoft Forms	Microsoft Lists	Microsoft Search
Microsoft Teams	Microsoft To Do	Microsoft Whiteboard	Office for the Web (incl Visio)	OneDrive for Business (2 GB)
Planner	Power Apps for Office 365	Power Automate for Office 365 (2,000 st/day)	Power Virtual Agents for Teams	Project & Roadmap View Access
Retention Labels	Secure Score	SharePoint Online Kiosk	Stream (consume)	Sway
Viva Connections	Viva Engage	Viva Learning (basic)		

Limitations:

No productivity server access, No desktop Outlook access, No voicemail

Office 365 F3

Enterprise Mobility + Security E3 (EMS E3)

Administrative Units	Advanced Security Reports & Alerts	App Proxy, including PingAccess	Cloud App Discovery	Conditional Access
Custom Security Attributes	Customized Sign-In Page	Dynamic Groups	Enterprise State Roaming	Entra ID Connect Health
External ID	Microsoft Identity Manager	Multi-Factor Auth (MFA)	Password Protection	Passwordless Authentication
Self-Service Group Management	Self-Service Password Reset in AD	Self-Service Activity Reports	Service Level Agreement	Shared Account Password Roll-Over
Single-Sign-On to other SaaS	SMS Sign-In	Temporary Access Pass	Terms of Use	Verified ID
Windows Autopilot	3rd Party MFA Integration			

Entra ID Plan 1

Application Management	Config Manager	Active Directory RMS	Advanced Threat Analytics (retiring)	Azure RMS
Device Management	Endpoint Analytics	Config Manager Endpoint Protection	Information Protection	Windows Server CAL Rights

Intune Plan 1

Enterprise Mobility + Security E3 (EMS E3)

Windows Enterprise for Microsoft 365 F3

Always On VPN	Application Control	Application Guard	AppLocker	App Assure	Assigned Access
Attack Surface Reduction	BitLocker	BitLocker to Go	BranchCache	Cortana	Credential Guard
Custom Logon	Custom Shell	Defender Antivirus	DirectAccess	Domain Join	Edge for Business
Entra ID Join	Keyboard Filter	LAPS	Manage by MDM	Persistent Memory	Power Automate Attended Desktop Flows
Resilient File System (ReFS)	SMB Direct	Unbranded Boot	Unified Write Filter	Universal Print	Windows Conditional Access
Windows Firewall	Windows Hello for Business	Windows Information Protection (retiring)	Windows Update for Business	Windows Virtualization Rights	36 months support for Windows 11

Microsoft 365 F3 includes Windows Enterprise except for Autopatch, Long Term Servicing Channel (LTSC), and Microsoft Desktop Optimization Pack (MDOP) features

Windows Enterprise for Microsoft 365 F3

Microsoft 365 F3

Microsoft 365 F3

Office 365 for Microsoft 365 F1

Activity Reports	Adoption Score	Alert Policies	Audio Conferencing (free add-on)	Audit (standard)
Basic Mobility & Security	Bookings	Compliance Manager	Content Search	Entra ID for Office 365
Exchange Online Kiosk (calendar)	Information Protection for M365 (from EMS E3)	Message Encryption (basic) (from EMS E3)	Microsoft 365 Mobile App (read-only)	Microsoft Forms (consume)
Microsoft Lists	Microsoft Search	Microsoft Teams	Office for the Web (read-only)	OneDrive for Business (2 GB)
Planner	Secure Score	SharePoint Online Kiosk	Stream (consume)	Sway
Viva Connections	Viva Engage	Viva Learning (basic)		

Limitations:

No productivity server access, No desktop Outlook access

Office 365 for Microsoft 365 F1

Microsoft 365 F1

Microsoft 365 F1

Enterprise Mobility + Security E3 (EMS E3)

Administrative Units	Advanced Security Reports & Alerts	App Proxy, including PingAccess	Cloud App Discovery	Conditional Access	Application Management	Config Manager
Custom Security Attributes	Customized Sign-In Page	Dynamic Groups	Enterprise State Roaming	Entra ID Connect Health	Device Management	Endpoint Analytics
External ID	Microsoft Identity Manager	Multi-Factor Auth (MFA)	Password Protection	Passwordless Authentication	Intune Plan 1	
Self-Service Group Management	Self-Service Password Reset in AD	Self-Service Activity Reports	Service Level Agreement	Shared Account Password Roll-Over	Active Directory RMS	Advanced Threat Analytics (retiring)
Single-Sign-On to other SaaS	SMS Sign-In	Temporary Access Pass	Terms of Use	Verified ID	Azure RMS	Config Manager Endpoint Protection
Windows Autopilot	3rd Party MFA Integration				Information Protection	Windows Server CAL Rights

Entra ID Plan 1

Enterprise Mobility + Security E3 (EMS E3)

Groups | All groups

ATEA, UAB

- All groups
- Deleted groups
- Diagnose and solve problems
- Settings
 - General
 - Expiration
 - Naming policy
- Activity
- Troubleshooting + Support

New group
 Download groups
 Refresh
 Manage view
 Delete
 Got feedback?

Info Azure Active Directory is now Microsoft Entra ID. [Learn more](#)

Search mode Contains

139 groups found

<input type="checkbox"/>	Name ↑	Object Id	Group type	Membership type
<input type="checkbox"/>	Intune - Android - Security Level 1	74d24572-0660-49c7-928c-3a70e2a5cd6b	Security	Assigned
<input checked="" type="checkbox"/>	Intune - Windows - Autopilot Devices	ea29ca60-dea3-479f-a889-f96725209703	Security	Dynamic
<input type="checkbox"/>	Intune - Windows - Autopilot Devices Baseline	9167a57a-35f3-4393-8802-b4c94eb12f71	Security	Assigned
<input type="checkbox"/>	Intune - Windows - Bitlocker Policy	01badef9-2d26-4c63-aac9-c4cad6572ed6	Security	Assigned
<input type="checkbox"/>	Intune - Windows - Block Legacy	cffa21b-7ed8-4eb3-b15a-2c540a72abd1	Security	Assigned
<input type="checkbox"/>	Intune - Windows - Deployment profile	aa47d2d3-71f5-40ba-ba36-f96d6cee1a13	Security	Assigned
<input type="checkbox"/>	Intune - Windows - MAM User Scope	3a6aa946-5ef6-4383-ba05-bf0d918d9fd6	Security	Assigned
<input type="checkbox"/>	Intune - Windows - MDM User Scope	986ab5d6-363e-44b7-8257-deb9ceb08cba	Security	Assigned

Home > Devices

Devices | Configuration

🔍 Search

- Overview
- All devices
- Monitor

By platform

- Windows
- iOS/iPadOS
- macOS
- Android
- Linux

Device onboarding

- Windows 365
- Enrollment

Manage devices

- Configuration**
- Compliance
- Conditional access
- Scripts and remediations
- Windows 10 and later updates
- Apple updates
- Group Policy analytics
- eSIM cellular profiles (preview)
- Policy sets
- Android FOTA deployments
- Device clean-up rules
- Device categories
- Filters

Policies Import ADMX Monitor

+ Create Refresh Export Columns

🔍 Search ⓘ

🔗 Add filters

Policy name	Platform	Policy type
Baseline	Windows 10 and later	Settings catalog
Fully managed basic security configuration (Level 1) v1.2	Android Enterprise	Device restrictions
Fully managed enhanced security configuration (Level 2) v1.2	Android Enterprise	Device restrictions
Fully managed high security configuration (Level 3) v1.2	Android Enterprise	Device restrictions
Intune Demo - Bitlocker policy	Windows 10 and later	Endpoint protection
Intune Demo - OneDrive FKM	Windows 10 and later	Administrative templates
Intune Demo - Wallpaper policy	Windows 10 and later	Device restrictions
Restrictions	iOS/iPadOS	Settings catalog
Restrictions V2	iOS/iPadOS	Device restrictions
SDL	iOS/iPadOS	Wi-Fi
Tracking	iOS/iPadOS	Settings catalog
Wallpaper	iOS/iPadOS	Device features
Work profile enhanced security configuration (Level 2) v1.3	Android Enterprise	Device restrictions
Work profile high security configuration (Level 3) v1.2	Android Enterprise	Device restrictions

Create a profile

Platform
Windows 10 and later

Profile type
Templates

Templates contain groups of settings, organized by function. If you don't want to build policies manually or want to configure settings for networks, such as configuring WiFi or VPN. [Learn more](#)

🔍 Search by profile name

- Template name**
- Administrative templates
- BIOS configurations and other settings
- Custom ⓘ
- Delivery optimization ⓘ
- Device firmware configuration interface ⓘ
- Device restrictions ⓘ
- Device restrictions (Windows 10 Team) ⓘ
- Domain join ⓘ
- Edition upgrade and mode switch ⓘ
- Email ⓘ
- Endpoint protection ⓘ
- Identity protection ⓘ
- Imported Administrative templates (Preview)
- Kiosk ⓘ
- Microsoft Defender for Endpoint (Desktop devices rule)
- Network boundary ⓘ
- PKCS certificate ⓘ
- PKCS imported certificate ⓘ
- SCEP certificate ⓘ

Create

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support



Home > Devices | Configuration >

Domain Join

Windows 10 and later

- Basics
- 2 Configuration settings**
- 3 Scope tags
- 4 Assignments
- 5 Applicability Rules
- 6 Review + create

Computer name prefix * ⓘ

Not configured

Domain name * ⓘ

Not configured

Organizational unit ⓘ

Not configured

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Home > Endpoint security | Conditional access > Conditional Access | Overview >

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

Enable policy

Report-only On Off

⚠ It looks like you're about to manage your organization's security configurations. That's great! You must first [disable security defaults](#) before enabling a Conditional Access p

Create

Grant

Control access enforcement to block or grant access. [Learn more](#)

- Block access
- Grant access

Require multifactor authentication

Require authentication strength

Require device to be marked as compliant

⚠ Don't lock yourself out! Make sure that your device is compliant. [Learn more](#)

Require Microsoft Entra hybrid joined device

Require approved client app
[See list of approved client apps](#)

Require app protection policy
[See list of policy protected client apps](#)

iOS Terms of Use Demo

For multiple controls

- Require all the selected controls
- Require one of the selected controls

Select

Pagrindinė žinutė

Unifikuotas SDV valdymas (angl. UEM)

Integruoti platforminiai sprendimai

Pilno SDV gyvavimo ciklo supratimas



Skaitmeninė darbo vieta

Įrangos parinkimas



Ką pirkti?

Kibernetinis saugumas, tvarumas, ilgaamžiškumas, darbo įrankiai, mokymai ...

Kiek pirkti?

1:1, 1:keli įrenginiai, keli:1 įrenginys ...

Kam pirkti?

Darbo funkcija, darbo aplinka, ...



Kaip pirkti?

Pirkimas, nuoma, lizingas

Iš ko pirkti?

Ad hoc, patikimi tiekėjai

Kokiu būdu pirkti?

E-Shop, Free Choice, konkursas, užklausa

Per kiek laiko nupirkti?

X dienų, iš rezervo ASAP

Pirkimo proceso optimizavimas



Ar ruošia?

Ne, tik įtraukia į AD, ruošia

Kaip ruošia?

GPO, iš „image‘ų“, UEM, MDM tiesioginis kontaktas

Kas ruošia?

IT komanda, aptarnaujanti įmonė, pats darbuotojas, gamintojas

Konfigūravimas ir parengimas



Kaip prižiūri?

Įrankis, apimtis, periodiškumas

Kas prižiūri?

Nuosava IT komanda, samdomas tiekėjas

Kaip vertina paslaugas?

Nevertina, KPI, periodiniai vertinimai

Priežiūra

Remontas



Kokie garantiniai reikalavimai?

On-site, laikmenų palikimas klientui

Kur taiso negarantinius įrenginius?

Patys, sertifikuotas serviso centras, kita serviso įmonė

Koks gyvavimo ciklas?

Nėra, kol veikia garantija, 5 metai

Kas vykdo sunaikinimą?

Patys, samdomas tiekėjas

Ar vykdomas laikmenų ištrynimasis?

Taip, ne.



Utilizavimas

Prekės konfigurācija, nustatymai



x1  Apple iPhone 14 - midnight - 5G smartphone - 128 GB - GSM

Apple iPhone 14 - midnight - 5G smartphone - 128 GB - GSM

Įtraukti į Apple Business Manager *

Organisation ID *

Taip

65757791

Pažymėjus šį laukelį perkami Apple įrenginiai bus automatiškai įtraukti į Jūsų įmonės Apple Business Manager sistemą.

Baigti

Pagrindinė žinutė

Unifikuotas SDV valdymas (angl. UEM)

Integruoti platforminiai sprendimai

Pilno SDV gyvavimo ciklo supratimas





Lenovo



DELL



SAMSUNG



A nighttime aerial view of Vilnius, Lithuania, showing the Neris river winding through the city. The skyline is dominated by modern skyscrapers with illuminated windows, contrasting with older, traditional buildings. A bridge with a distinctive arch design spans the river in the foreground. The overall atmosphere is vibrant and modern.

Kuriame *saugią* Lietuvą su IT

ATEA