Martin Haller

⟨ Microsoft Entra ID Defense ⟩

PATRON ⟨IT⟩ OCHRANA A SPRÁVA SÍTÍ

Entra ID: Defense

How we got here?

- Goals of attack (monetization)
- Entra ID: Attack surface
- Entra ID: Lateral movement & persistence

Where to start?

- Actual and future threats
- Research of others
  - https://www.cisa.gov/
  - https://www.purple-knight.com/security-indicators/
  - https://www.pingcastle.com/
  - https://cyberdom.blog/2022/11/09/cloud-misconfiguration-risks-azure/

Main ingredietns

- Hardening (attack surface reduction)
- Monitoring
- Backup
- KISS (Keep It Simple, Stupid)
- Step by step

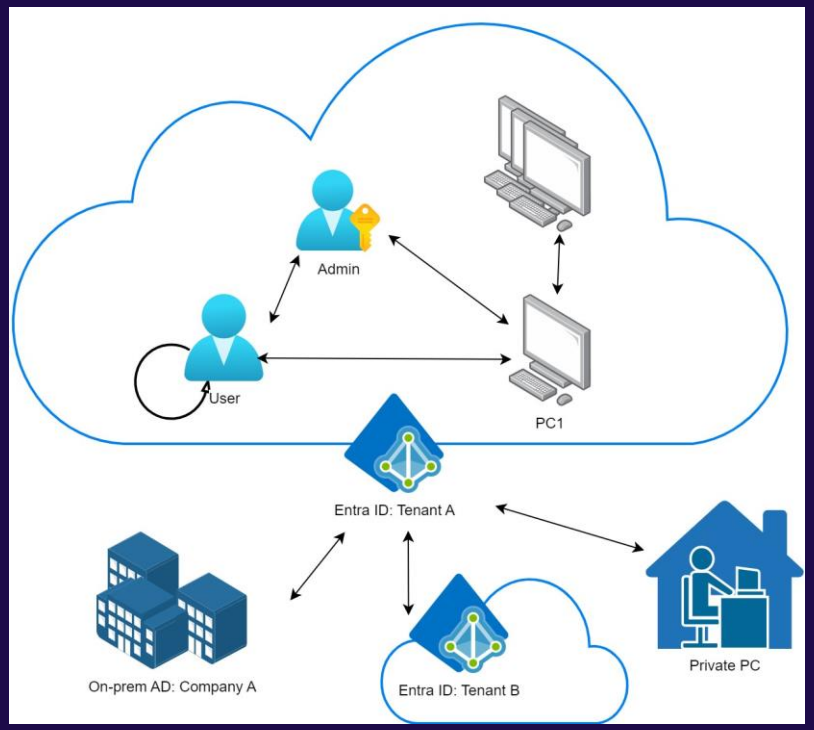
Context

Company with up to 1.000 seats and small internal IT department.

Entra ID: Hardening

Privileged accounts

- Never use hybrid accounts (synchronized between Entra ID and AD)
- Separated regular and privileged accounts
- Protect Azure AD Connect server (?Entra ID Connect?)



Display name ↑	User principal name ⇅	User type	On-premises sy...
__VMware_Conv_SA__	__VMware_Conv_SA__@...	Member	Yes

Native apps

- Microsoft Authenticator (Passwordless, Push, higher security)
- Microsoft Outlook (Purview, MAM, easier support, more functionality)
- Microsoft 365 Mobile App

Easy configuration

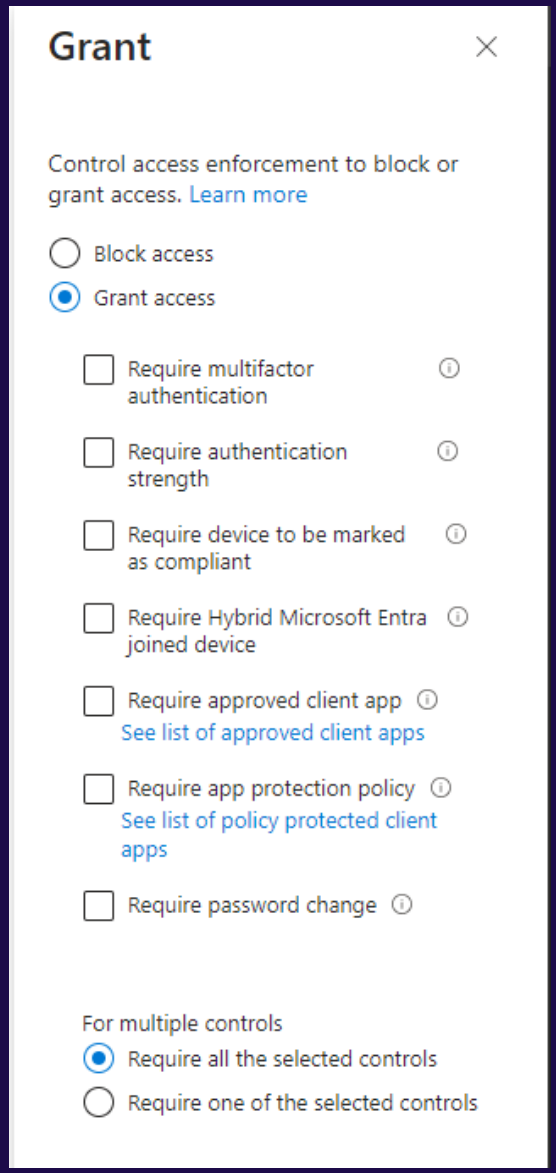
- Limit Entra ID Join
- Limit App Registration
- Limit App Consent
- Limit Group Creation
- Limit Entra ID portal for users
- Limit Guests Invitations
- Limit Guests Visibility

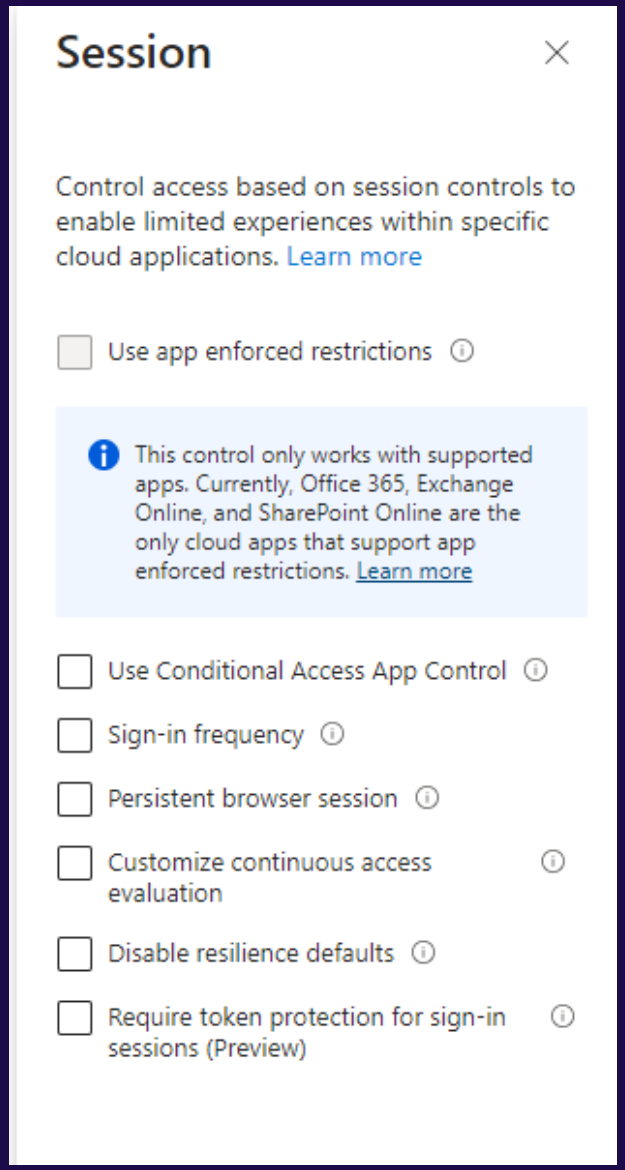
Other configuration

- Exchange External Tag
- Self-serve password reset portal (disable for admins)
- Authentication methods
- Unified audit logging

DEMO: Hardening

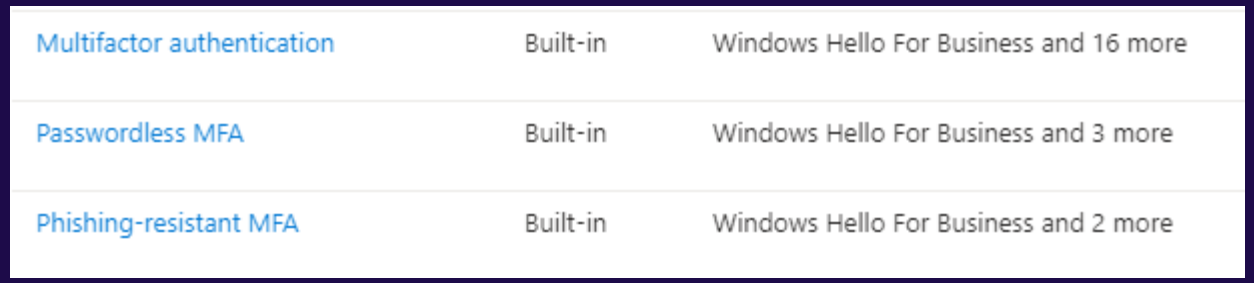
Entra ID: Conditional Access


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
Require Hybrid Microsoft Entra joined device
Require approved client app
See list of approved client apps
Require app protection policy
See list of policy protected client apps
Require password change
For multiple controls
Require all the selected controls
Require one of the selected controls


Session
Control access based on session controls to enable limited experiences within specific cloud applications. Learn more
Use app enforced restrictions
This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Learn more
Use Conditional Access App Control
Sign-in frequency
Persistent browser session
Customize continuous access evaluation
Disable resilience defaults
Require token protection for sign-in sessions (Preview)

Conditional Access (CA)

- Under which conditions you can access apps
- Security defaults vs. CA
- Default allow
- Not everything can be set as requirement
- All policies are being evaluated
- Azure App Web Proxy
- Guest access and MFA
- How many CA policies is limit?
- Authentication strength



Multifactor authentication	Built-in	Windows Hello For Business and 16 more
Passwordless MFA	Built-in	Windows Hello For Business and 3 more
Phishing-resistant MFA	Built-in	Windows Hello For Business and 2 more

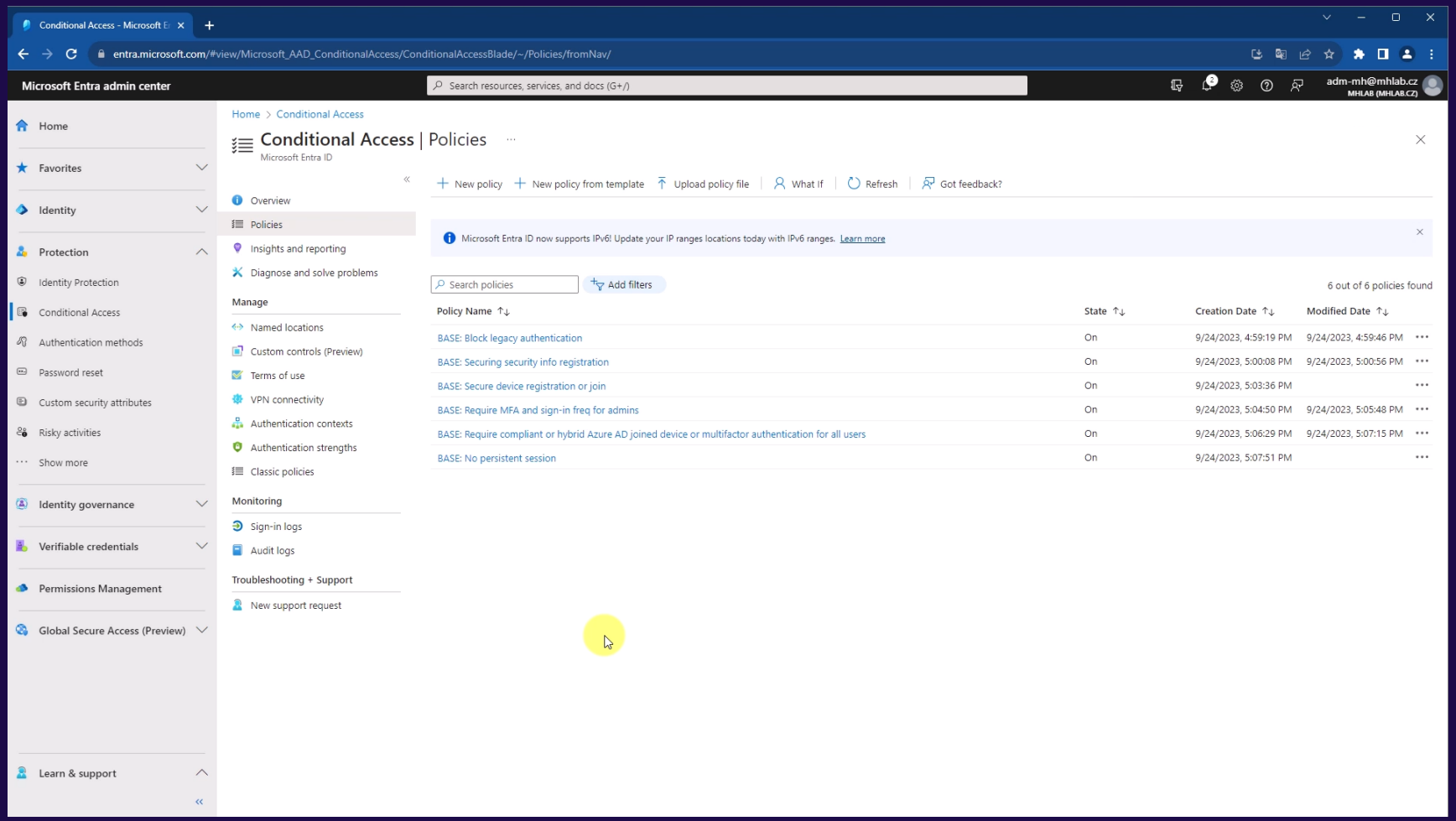
Conditional Access - essentials

- Global rules:
  - Block legacy authentication
  - **Recommended**:
    - Register Security information: MFA or trusted network
    - Register or join devices: MFA
- Privileged users
  - No persistent session, signing frequency
  - **Recommended**: FIDO2, trusted network
- Users
  - Start: MFA, Hybrid Joined Device or Compliant device
  - **Recommended**: MFA (on company devices WHfB)
  - No persistent session

Conditional Access – tiering?

- **Public**: BYOD (MAM)
- **Restricted**: Enterprise devices (Intune/GPO, EDR)
- **Confidential**: Subset of Enterprise devices (stricter configuration)
- **Special**:
  - **VPN**: sign-in frequency
  - **RDP**

DEMO: Conditional Access



Entra ID: Monitoring

Monitoring - essentials

» Risky users

User risk detections

Risk detection	Detection type	Type
Possible attempt to access Primary Refresh Token (PRT)	Offline	Premium
Anomalous user activity	Offline	Premium
User reported suspicious activity	Offline	Premium
Additional risk detected	Real-time or Offline	Nonpremium
Leaked credentials	Offline	Nonpremium
Microsoft Entra threat intelligence	Offline	Nonpremium

Zdroj: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#additional-risk-detected-sign-in

Monitoring

- Risky users
- Risky sign-ins

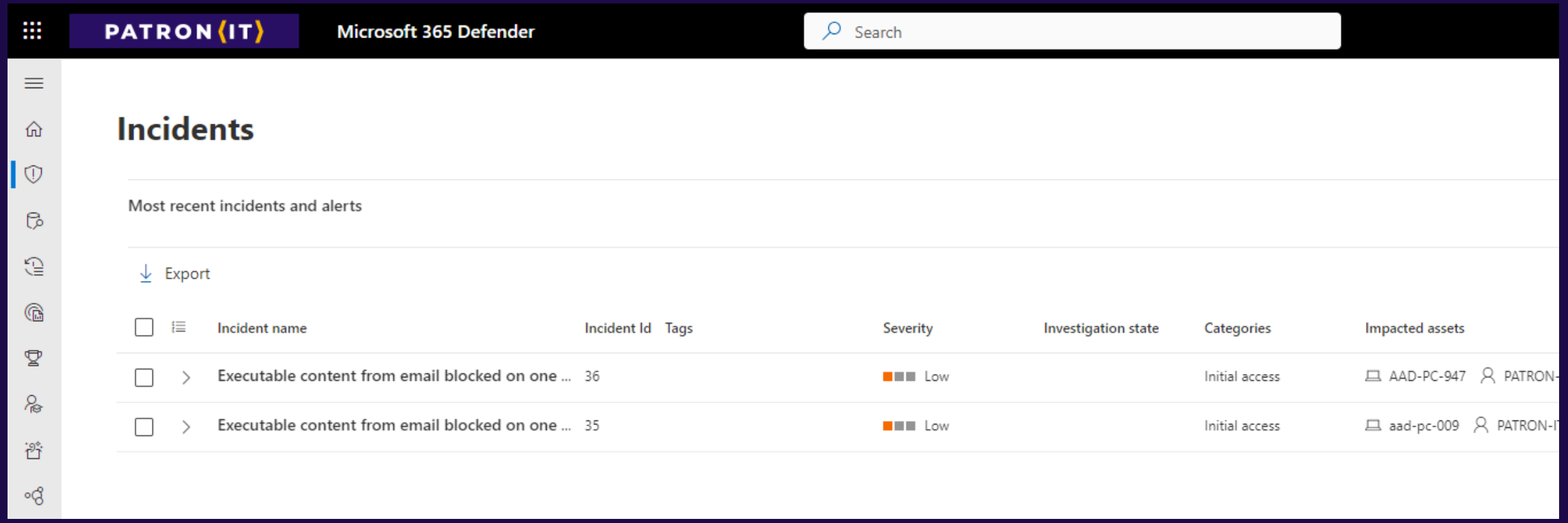
Zdroj: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#additional-risk-detected-sign-in

Sign-in risk detections

Risk detection	Detection type	Type
Atypical travel	Offline	Premium
Anomalous Token	Offline	Premium
Token Issuer Anomaly	Offline	Premium
Malware linked IP address	Offline	Premium **This detection has been deprecated.**
Suspicious browser	Offline	Premium
Unfamiliar sign-in properties	Real-time	Premium
Malicious IP address	Offline	Premium
Suspicious inbox manipulation rules	Offline	Premium
Password spray	Offline	Premium
Impossible travel	Offline	Premium
New country	Offline	Premium
Activity from anonymous IP address	Offline	Premium
Suspicious inbox forwarding	Offline	Premium
Mass Access to Sensitive Files	Offline	Premium
Verified threat actor IP	Real-time	Premium
Additional risk detected	Real-time or Offline	Nonpremium
Anonymous IP address	Real-time	Nonpremium
Admin confirmed user compromised	Offline	Nonpremium
Microsoft Entra threat intelligence	Real-time or Offline	Nonpremium

Monitoring - essentials

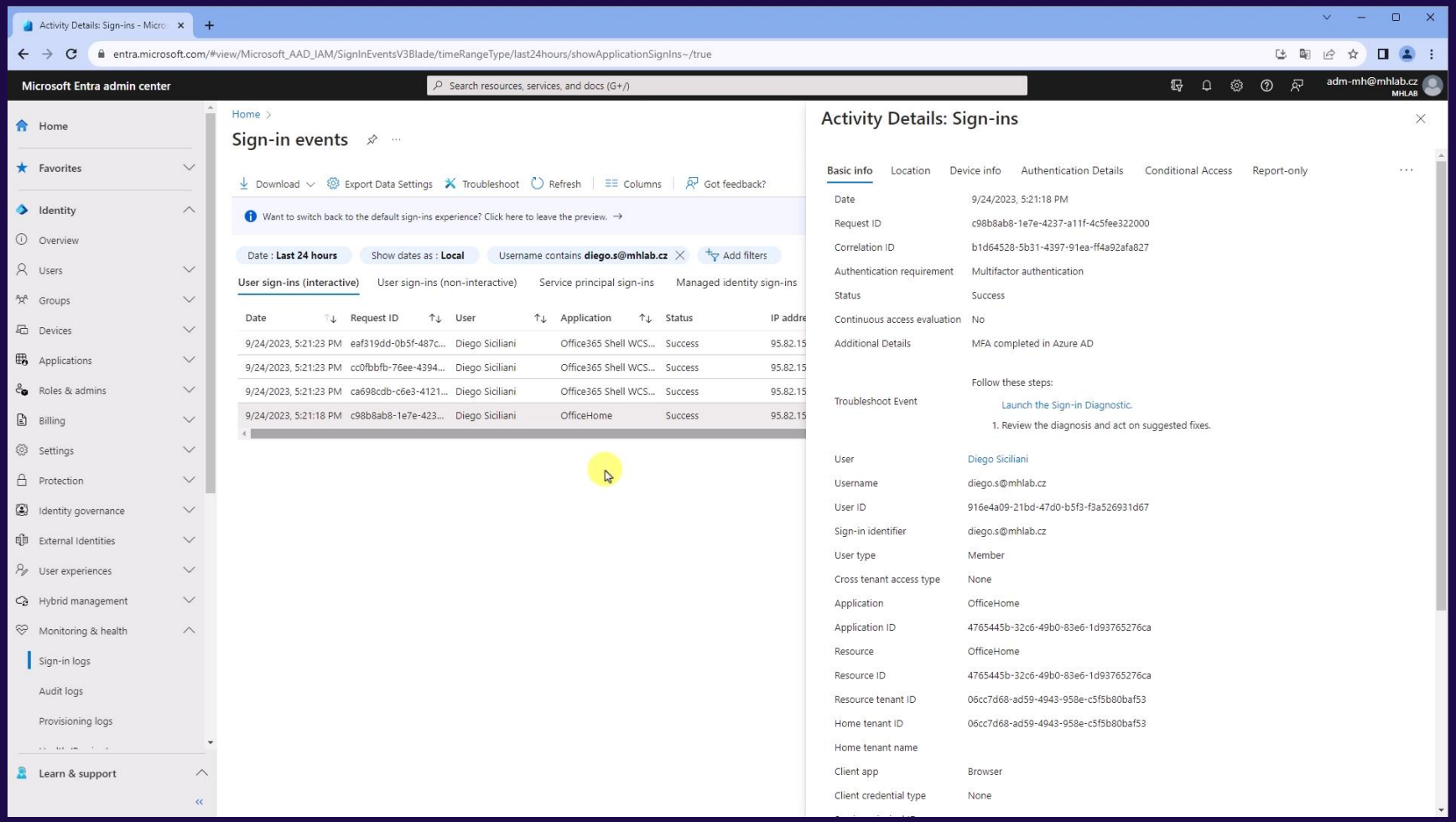
- Risky users
- Risky sign-ins
- Defender alerts



Monitoring - logs

- Azure AD Audit Log
  - Contains: changes done in Entra ID
  - Retention: Free = 7 days, P1 = 30 days
  - https://entra.microsoft.com/#view/Microsoft_AAD_IAM/AuditEventsV2PillsBlade
- Azure AD Sign-in Log
  - Contains: sign-ins to M365
  - Retention: Free = 7 days, P1 = 30 days
  - https://entra.microsoft.com/#view/Microsoft_AAD_IAM/SignInEventsV3Blade
- Office 365 Unified Access Log (Microsoft Purview Audit)
  - Not enabled by default.
  - Retention: Free = 90 days (180 days), E5 = 1 year
  - https://compliance.microsoft.com/auditlogsearch
- Log Analytics / Sentinel
- Everything you wanted to know about Security and Audit Logging in Office 365

DEMO: Sign-in logs



Další čtení: https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Protection
Identity governance
External Identities
User experiences
Hybrid management
Monitoring & health
Sign-in logs
Audit logs
Provisioning logs
Health (Preview)
Log Analytics
Diagnostic settings
Workbooks
Usage & insights
Learn & support

Audit Logs

Download | Export Data Settings | Refresh | Columns | Got feedback?

Date : **Last 24 hours** | Show dates as : **Local** | Service : **All** | Category : **All** | Activity : **All** | Add filters

Date	Service	Category	Activity	Status	Status reason	Target(s)	Initiated
9/4/2023, 3:55:57 PM	Core Directory	DirectoryManagement	Set Company Inform...	Success		MHLab	adm-lh@
9/4/2023, 3:55:33 PM	Authentication Meth...	ApplicationManage...	Authentication Meth...	Success	NoContent	Authentication Meth...	Lidia Holl
9/4/2023, 3:55:33 PM	Core Directory	Policy	Update policy	Success		Default User Credent...	Azure Cre
9/4/2023, 3:52:08 PM	Core Directory	DirectoryManagement	Set Company Inform...	Success		MHLab	adm-lh@
9/4/2023, 3:52:03 PM	Authentication Meth...	ApplicationManage...	Authentication Meth...	Success	NoContent	Authentication Meth...	Lidia Holl
9/4/2023, 3:52:03 PM	Core Directory	Policy	Update policy	Success		Default User Credent...	Azure Cre
9/4/2023, 3:43:19 PM	Authentication Meth...	ApplicationManage...	Authentication Meth...	Success	NoContent	Authentication Meth...	Lidia Holl
9/4/2023, 3:43:19 PM	Core Directory	Policy	Update policy	Success		Default User Credent...	Azure Cre
9/4/2023, 2:36:35 PM	Core Directory	DirectoryManagement	Set Company Inform...	Success		MHLab	adm-lh@
9/4/2023, 2:36:09 PM	Authentication Meth...	ApplicationManage...	Authentication Meth...	Success	NoContent	Authentication Meth...	Lidia Holl
9/4/2023, 2:36:09 PM	Core Directory	Policy	Update policy	Success		Default User Credent...	Azure Cre
9/4/2023, 2:08:19 PM	Self-service Passwor...	UserManagement	Change password (s...	Success	None	Lidia Holloway (ADM)	adm-lh@
9/4/2023, 2:08:19 PM	Core Directory	UserManagement	Update StsRefreshTo...	Success		adm-lh@mhlab.cz	adm-lh@

Monitoring – what to search for in logs

- Privileged groups/roles
- Break glass admin use
- GDAP / DAP
- Consent to apps
- Application permissions changes
- Application secrets modification
- Changes in authentication methods
- Use of TAP (temporary access password)
- Changes in trusted CA
- Changes in PTA (AAD Connect)
- Cross tenant sync
- Changes in mail flow
- Mass changes/deletions
- Hunting (apps, user agent, not passing MFA, used countries)

Auditování

- Configuration revision
- Not used accounts (guests)
- Tools:
  - https://github.com/cisagov/ScubaGear
  - https://www.pingcastle.com/
  - https://www.purple-knight.com/

IT - Ing. Martin Haller | Authentication methods

+ Add authentication method | Reset password | Require re-register multifactor authentication | Revoke multifactor authentication sessions | View authentication methods policy | Got feedback?

Want to switch back to the old user authentication methods experience? Click here to go back. →

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. Learn more

Default sign-in method (Preview) Microsoft Authenticator notification

Usable authentication methods

Authentication method	Detail
FIDO2 security key	MH - Kensington C
FIDO2 security key	MH - YubiKey BIO C
Windows Hello for Business	
Windows Hello for Business	NB-MH2
Microsoft Authenticator	iPhone
Microsoft Authenticator	iPhone 12 Pro

Non-usable authentication methods

Authentication method	Detail
No non-usable methods.	

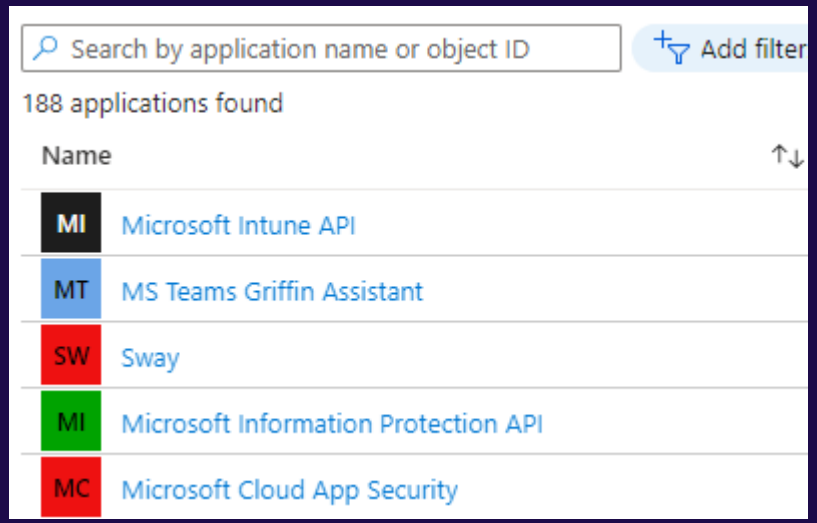
System preferred multifactor authentication method

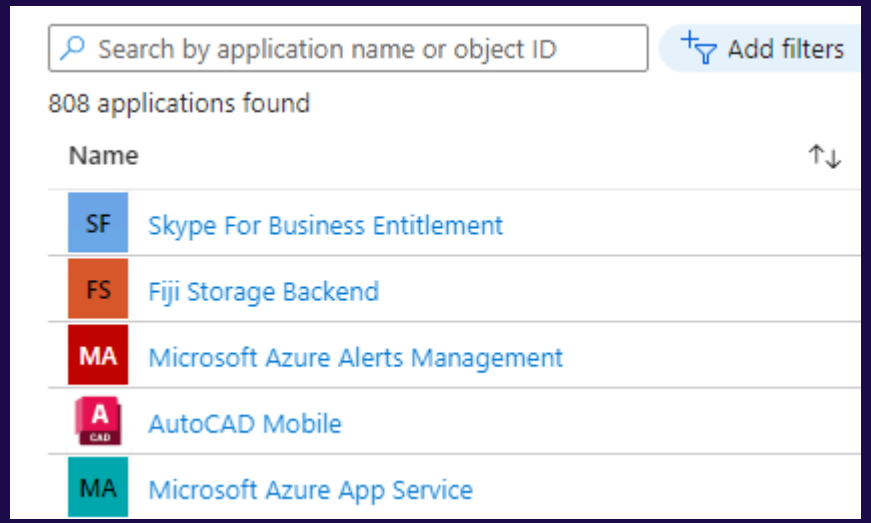
Feature status	System preferred MFA method
Disabled	N/A

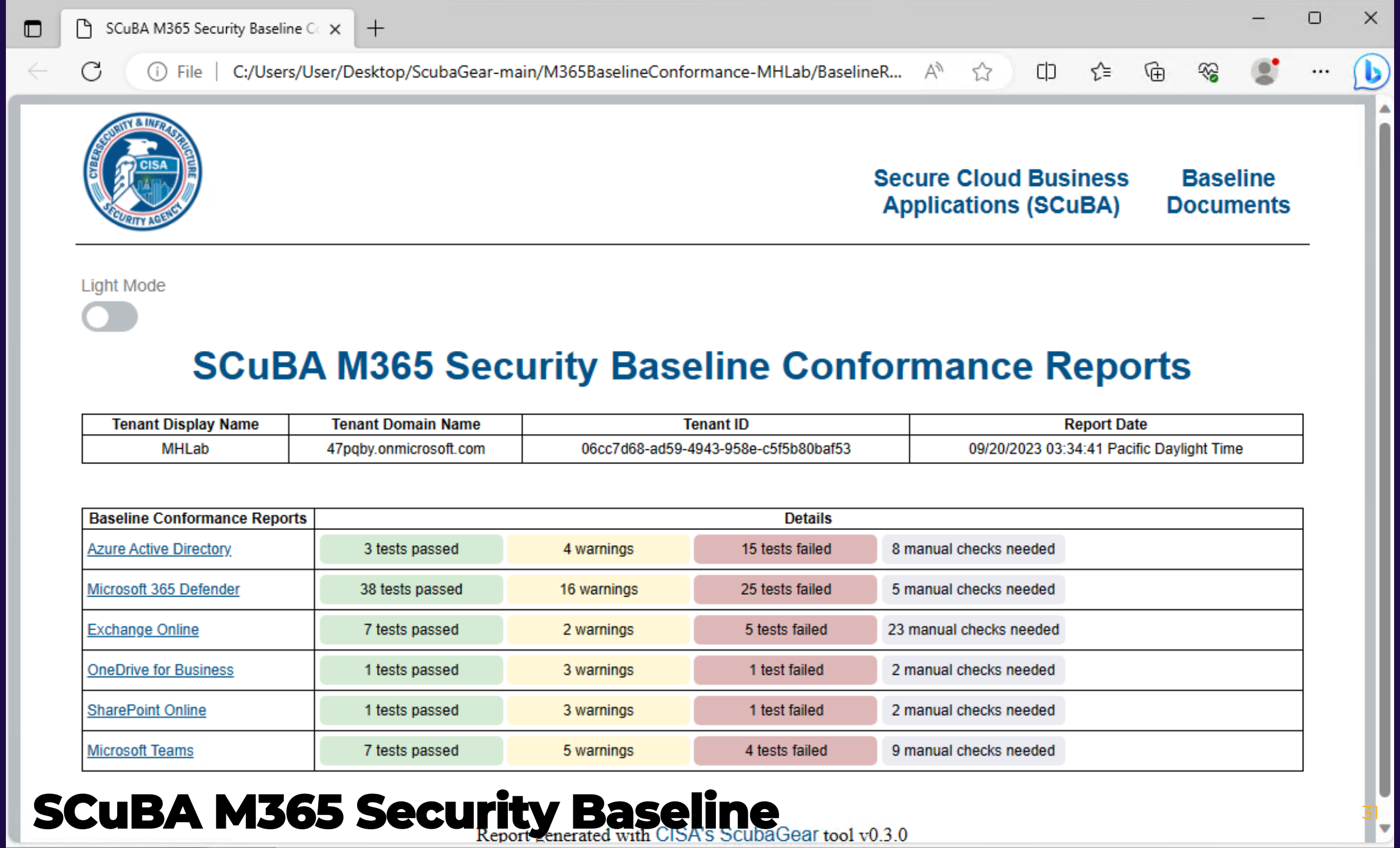
73 devices found

Name	Enabled	OS	Version	Join type	Owner	MDM	Compliant	Registered	Activity
BLACK	No	Windows	10.0.18363.0	Azure AD registered		None	N/A	8/6/2020, 1:41 PM	4/10/2022, 1:
DESKTOP-G5MP43G	Yes	Windows	10.0.19044.1706	Azure AD registered		None	N/A	5/28/2022, 8:54 AM	5/28/2022, 8:
NUC-2	Yes	Windows	10.0.18363.0	Azure AD registered		None	N/A	5/2/2019, 1:09 PM	7/18/2022, 8:
PC-01	Yes	Windows	10.0.19042.1826	Azure AD registered		None	N/A	9/1/2022, 9:34 AM	9/15/2022, 4:
NUC-7	Yes	Windows	10.0.16299.0	Azure AD registered		None	N/A	9/24/2018, 8:28 AM	10/18/2022,
DESKTOP-H8MNQ6E	Yes	Windows	10.0.17134.0	Azure AD registered		None	N/A	11/11/2018, 10:14 AM	11/7/2022, 8:
DESKTOP-I8T5KIL	Yes	Windows	10.0.19044.1586	Azure AD registered		None	N/A	3/15/2022, 2:59 PM	11/30/2022,
LAPTOP-GEEJOBIS	Yes	Windows	10.0.18362.0	Azure AD registered		None	N/A	12/26/2019, 10:07 AM	12/7/2022, 5:
AAD-WIN11-B	Yes	Windows	10.0.22621.963	Azure AD joined		None	No	2/15/2023, 3:40 PM	2/15/2023, 3:
NUC-3	Yes	Windows	10.0.16299.0	Azure AD registered		None	N/A	3/27/2018, 1:48 PM	3/20/2023, 1
PC-WIN11-B2	Yes	Windows	10.0.22621.963	Azure AD joined		Microsoft Intune	No	2/15/2023, 4:28 PM	3/28/2023, 3:
iPhone 11	Yes	iOS	16.4.1	Azure AD registered		None	N/A	12/16/2019, 9:30 AM	3/31/2023, 8:
NUC-1	Yes	Windows	10.0.19044.1889	Azure AD registered		None	No	9/13/2022, 10:30 AM	4/1/2023, 4:5
PC-06	No	Windows	10.0.19042.867	Azure AD registered		None	N/A	4/1/2021, 8:46 AM	4/4/2023, 8:2
PC-WIN-11	Yes	Windows	10.0.22000.1696	Azure AD joined		Microsoft Intune	N/A	4/4/2023, 10:51 AM	4/4/2023, 10:

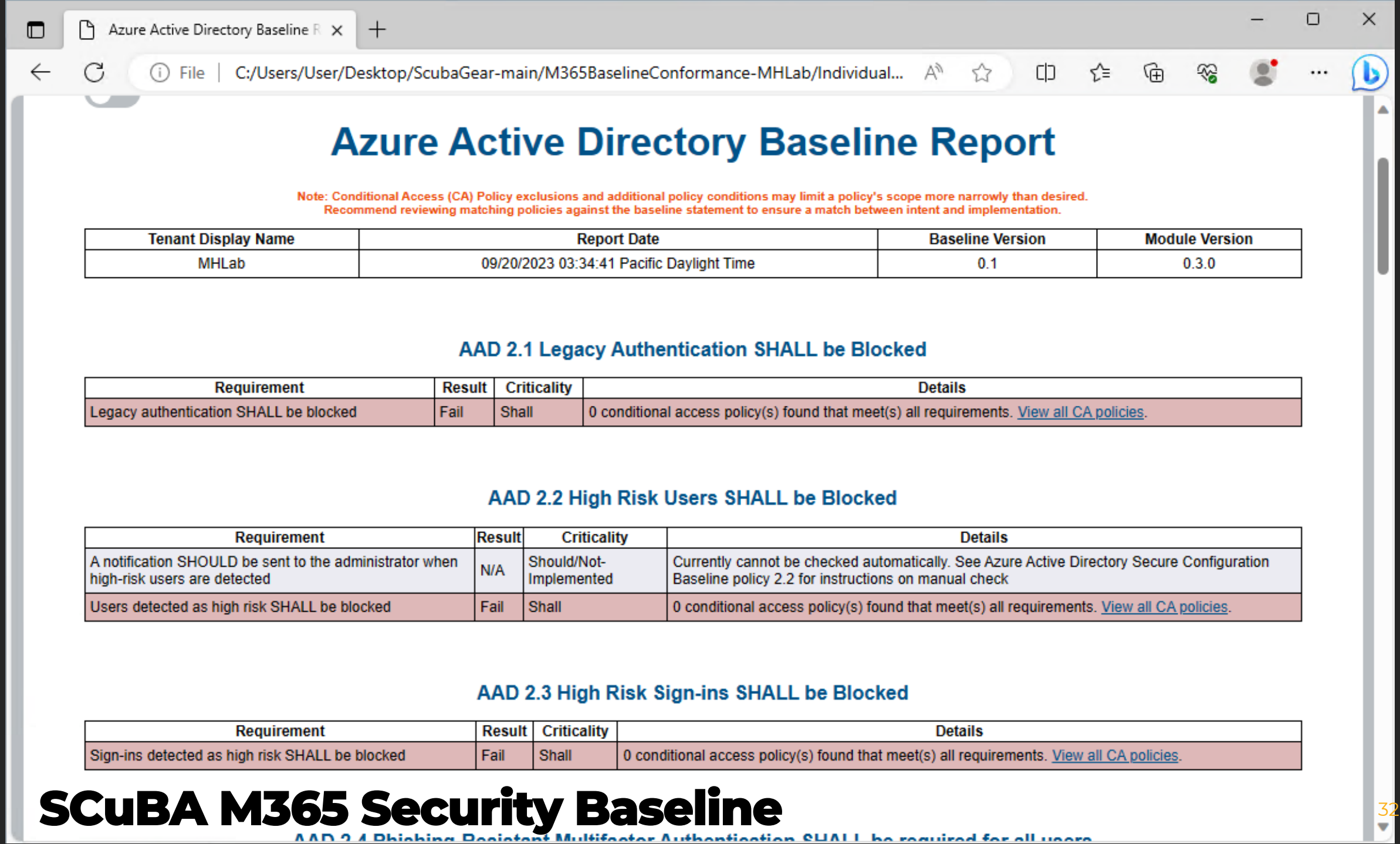
Number of applications in tenant?







SCuBA M365 Security Baseline



Azure Active Directory Baseline Report

Note: Conditional Access (CA) Policy exclusions and additional policy conditions may limit a policy's scope more narrowly than desired.
Recommend reviewing matching policies against the baseline statement to ensure a match between intent and implementation.

Tenant Display Name	Report Date	Baseline Version	Module Version
MHLab	09/20/2023 03:34:41 Pacific Daylight Time	0.1	0.3.0

AAD 2.1 Legacy Authentication SHALL be Blocked

Requirement	Result	Criticality	Details
Legacy authentication SHALL be blocked	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. View all CA policies.

AAD 2.2 High Risk Users SHALL be Blocked

Requirement	Result	Criticality	Details
A notification SHOULD be sent to the administrator when high-risk users are detected	N/A	Should/Not-Implemented	Currently cannot be checked automatically. See Azure Active Directory Secure Configuration Baseline policy 2.2 for instructions on manual check
Users detected as high risk SHALL be blocked	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. View all CA policies.

AAD 2.3 High Risk Sign-ins SHALL be Blocked

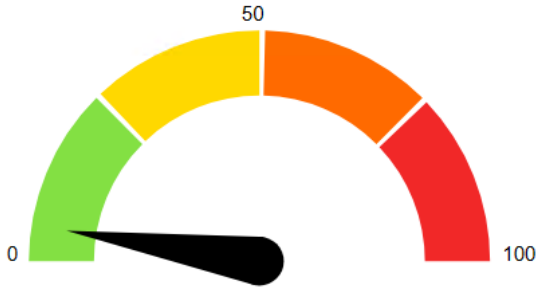
Requirement	Result	Criticality	Details
Sign-ins detected as high risk SHALL be blocked	Fail	Shall	0 conditional access policy(s) found that meet(s) all requirements. View all CA policies.

AAD 2.4 Phishing-Resistant Multifactor Authentication SHALL be required for all users

SCuBA M365 Security Baseline

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Domain Risk Level: 5 / 100

It is the score computed based on the rules that matched during the analysis

Maturity Level

This section represents the maturity score (inspired from ANSSI).

This feature is reserved for customers who have purchased a license

MITRE ATT&CK®

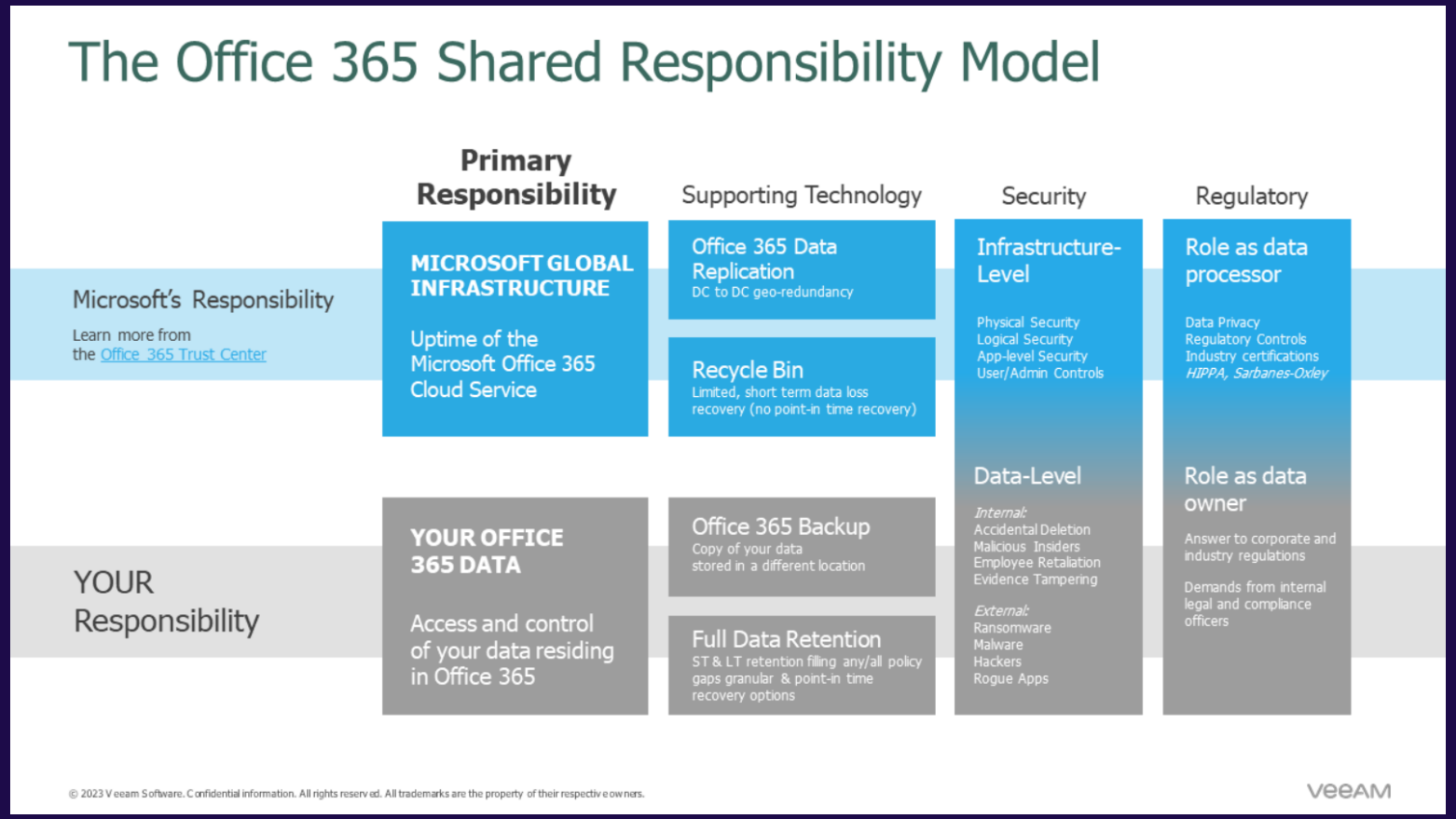
This section represents an evaluation of the techniques available in the MITRE ATT&CK®

This feature is reserved for customers who have purchased a license

Rules

Entra ID: Backup

» Veeam Backup for Microsoft 365



Zdroj: https://www.veeam.com/backup-microsoft-office-365.html

Entra ID: Implementation

How to do it?

- Multitenancy is the challenge?
- Custom scripts
- 3rd party tools (MS Lighthouse, N-able, AdminDroid)
- Auditing tools (PingCastle, Purple Knight, Bloodhound, SCuBA)
- Licences: Microsoft 365 Business Premium (20,6 EUR/month)
  - Office Apps,
  - Exchange, Sharepoint, OneDrive, ?Teams,
  - Entra ID P1,
  - Intune,
  - Defender Business,
  - Azure Information Protection

In case of account compromise

- Disable sign-in
- Revoke sessions
- Check authentication methods for the user
- Reset password
- Inspect audit logs
- Enable sign-in

Keep on working

- Extending hardening and monitoring
- Observation of trends in attacks
- Defender for *
- Intune (LAPS, Baselines, Applocker, WHfB)
- Azure resources

Summary

Summary

- Audit
- Hardening
- Monitoring
- Backup
- KISS!! Small steps!
- Keep learning

Other resources

Other resources

» https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

» https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model

» https://aadinternals.com/aadkillchain/

» https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

» https://www.huntress.com/blog/legitimate-apps-as-traitorware-for-persistent-microsoft-365-compromise

» https://github.com/WillOram/AzureAD-incident-response/blob/main/README-OFFENSIVETECHNIQUES.md

» https://github.com/hevnsnt/Awesome_Incident_Response

» https://learn.microsoft.com/en-us/security/operations/token-theft-playbook

» https://call4cloud.nl/2021/08/the-battle-between-aadj-and-aadr/

Thank ⟨YOU⟩