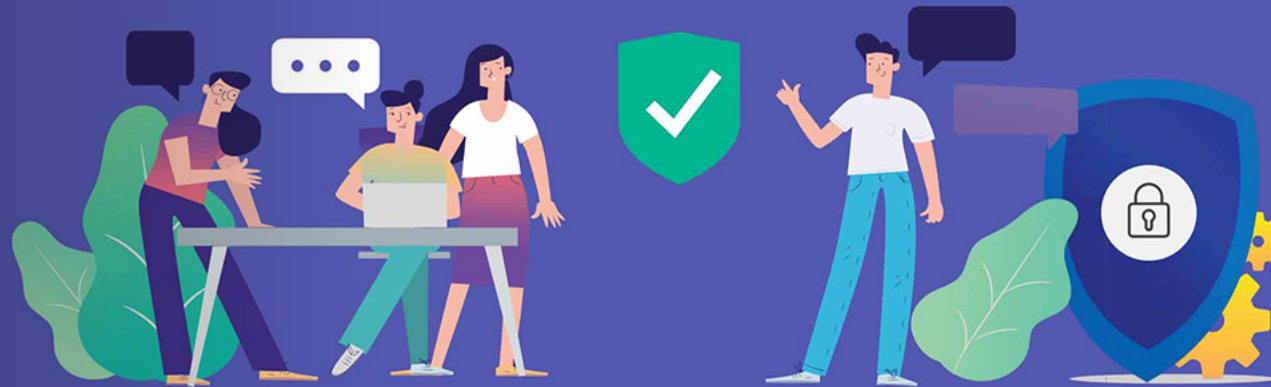


Microsoft 365 Tenant-Security

Verstehen. Anwenden. Absichern.



Über Marco

- Marco Schmittnägel
- SharePoint seit 2008
- Microsoft Cloud seit 2012
- Architektur, Beratung, Umsetzung
- Schwerpunkte aktuell
 - Tenant Architekturen
 - Teams, SharePoint, OneDrive
 - Machine Learning / AI



Über Bernd

- Bernd Jahn
- Seit 2018 in der IT
- Seit 2020 im Cloud-Umfeld
- Information Security Officer
- M365 Security Expert
- AvePoint Certified Specialist



Das (medienwirksame) Thema mit der Sicherheit

Resentful employee deletes 1,200 Microsoft Office 365 accounts, gets prison

<https://www.bleepingcomputer.com/news/security/resentful-employee-deletes-1-200-microsoft-office-365-accounts-gets-prison/>

AI Attacks Surge as Microsoft Process 100 Trillion Signals Daily

<https://www.infosecurity-magazine.com/news/microsoft-process-100-trillion/>

Deutschland mit am meisten von Cyberangriffen betroffen

Deutschland lag zuletzt laut einem Microsoft-Bericht weltweit an vierter Stelle der von Cyberangriffen betroffenen Staaten. Länder wie Russland weiteten diese aus.

<https://www.zeit.de/digital/internet/2025-10/microsoft-bericht-cyber-sicherheit>

Microsoft Patches Critical Entra ID Flaw Enabling Global Admin Impersonation Across Tenants

<https://thehackernews.com/2025/09/microsoft-patches-critical-entra-id.html>

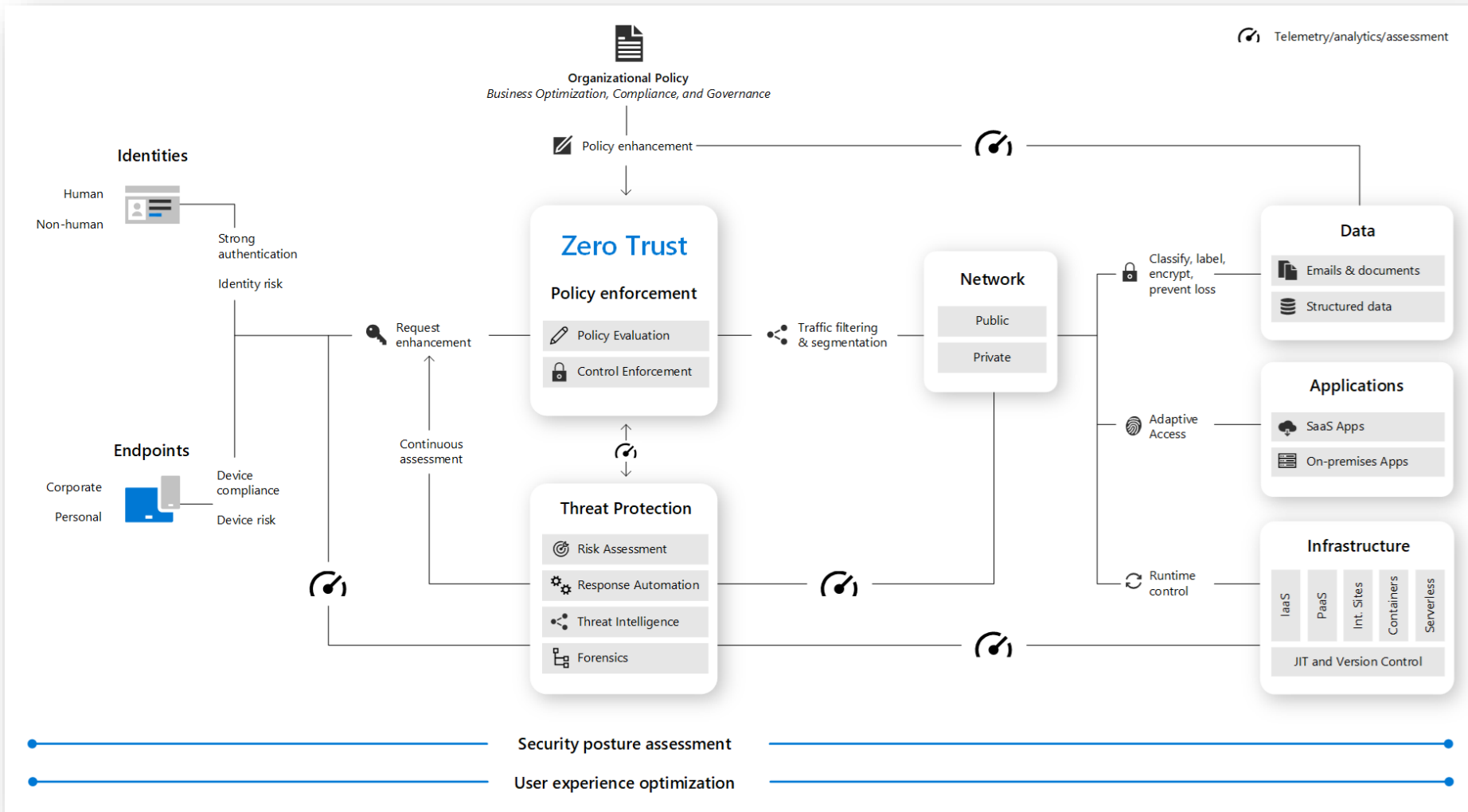
Was ist anders als früher?

Angriffe können durch Automatisierung und neuerdings durch KI nahezu grenzenlos skaliert werden.

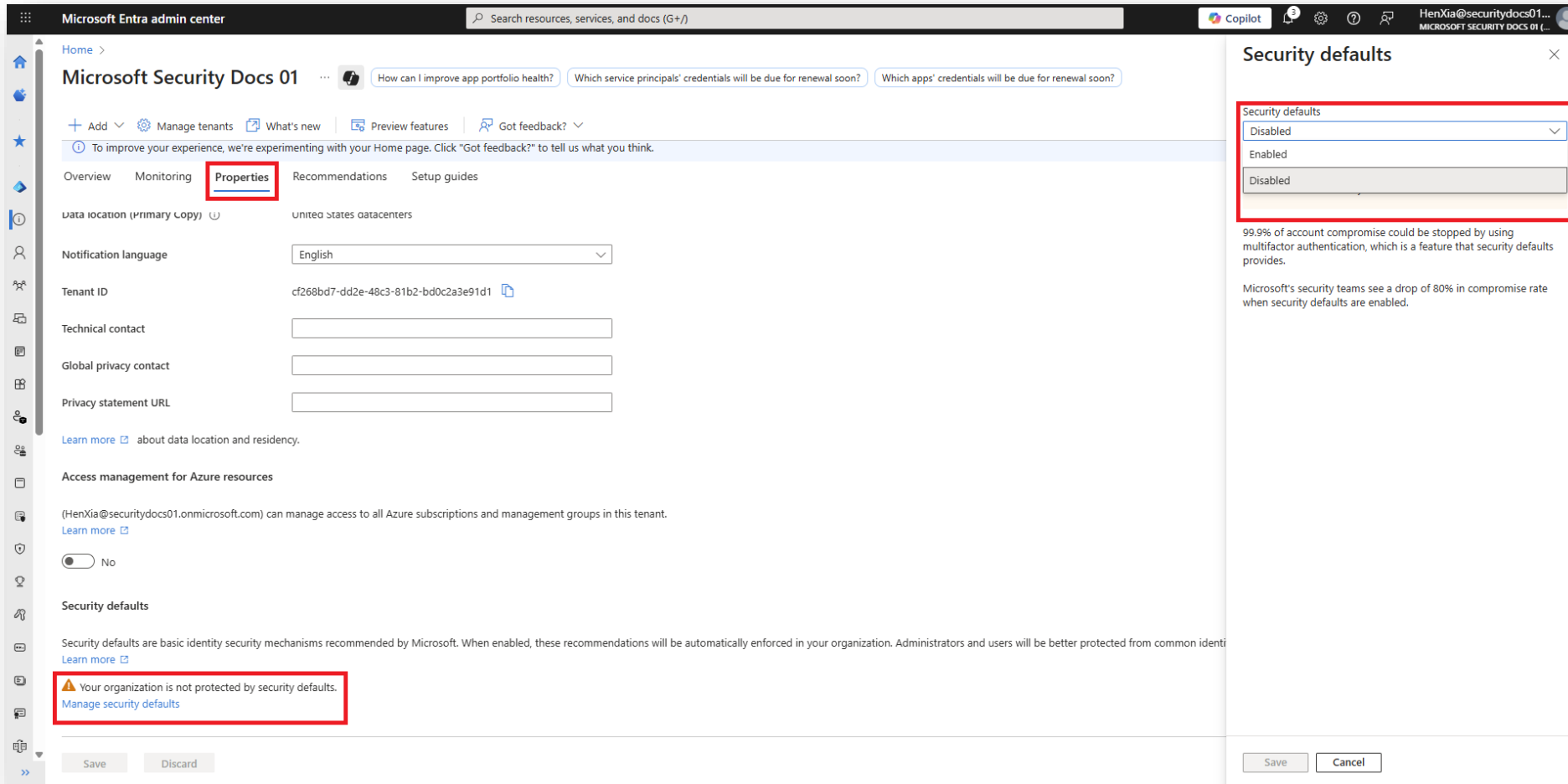
Gleichzeitig steigt deren Komplexität so weit, dass sie oft nur noch durch hochspezialisierte Experten oder Systeme erkannt und abgewehrt werden können.



Sicherheitsarchitektur zu Zeiten von Cloud und KI



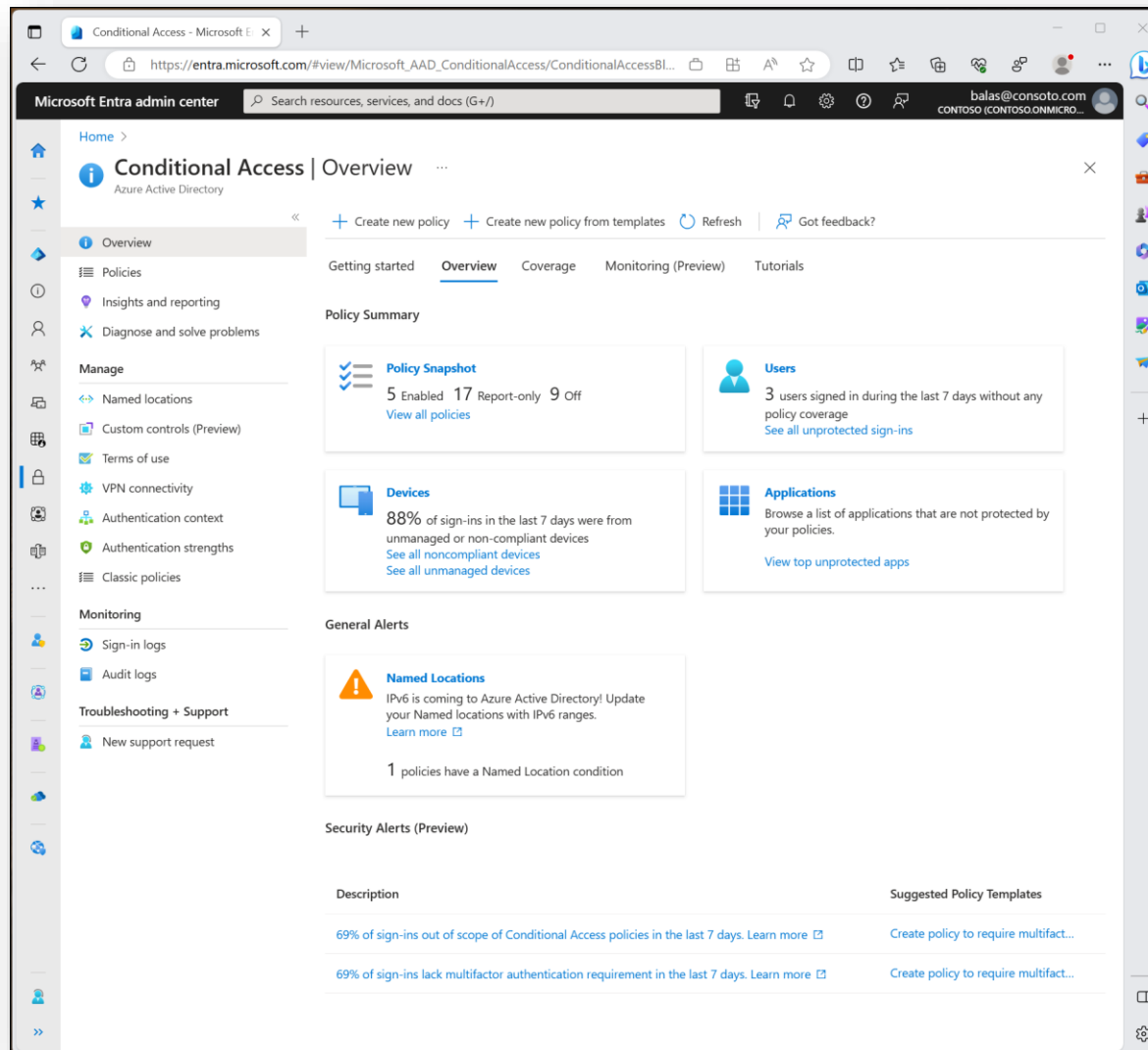
Security Defaults als Ausgangspunkt



The screenshot shows the Microsoft Entra admin center interface. The 'Properties' tab is selected, and the 'Security defaults' section is visible. A warning message states: "Your organization is not protected by security defaults." The 'Security defaults' dropdown menu is open, showing 'Disabled' as the selected option. The 'Save' and 'Cancel' buttons are visible at the bottom of the panel.

➔ Multifaktor-Authentifizierung + Alte Protokolle ausschalten + Admin-Funktionen zusätzlich absichern

Conditional Access als die Grundlage, es richtig zu machen



Enthalten in:

- Entra ID P1
- Microsoft 365 Business Premium
- Microsoft 365 F1 / F3
- Microsoft 365 E3 / E5
- Microsoft 365 A3 / A5

(NICHT enthalten in Office 365-Plänen)

Unterschiedliche Authentifizierungsstärken anwenden

Home > Conditional Access

Conditional Access | Authentication strengths

Microsoft Entra ID

Overview Policies Deleted Policies (Preview) Insights and reporting Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication contexts
- Authentication strengths**
- Classic policies

Monitoring

- Sign-in logs
- Audit logs

Troubleshooting + Support

- New support request

« + New authentication strength Refresh

Authentication strengths determine the combination of authentication methods that can be used. [Learn more](#)

Type: All Authentication methods: All Reset filters

Authentication strength	Type	Authentication methods
Multifactor authentication	Built-in	Windows Hello For Business / Platform Credential and 16 more
Passwordless MFA	Built-in	Windows Hello For Business / Platform Credential and 3 more
Phishing-resistant MFA	Built-in	Windows Hello For Business / Platform Credential and 2 more

New authentication strength

Custom

Configure Review

Name *

Description

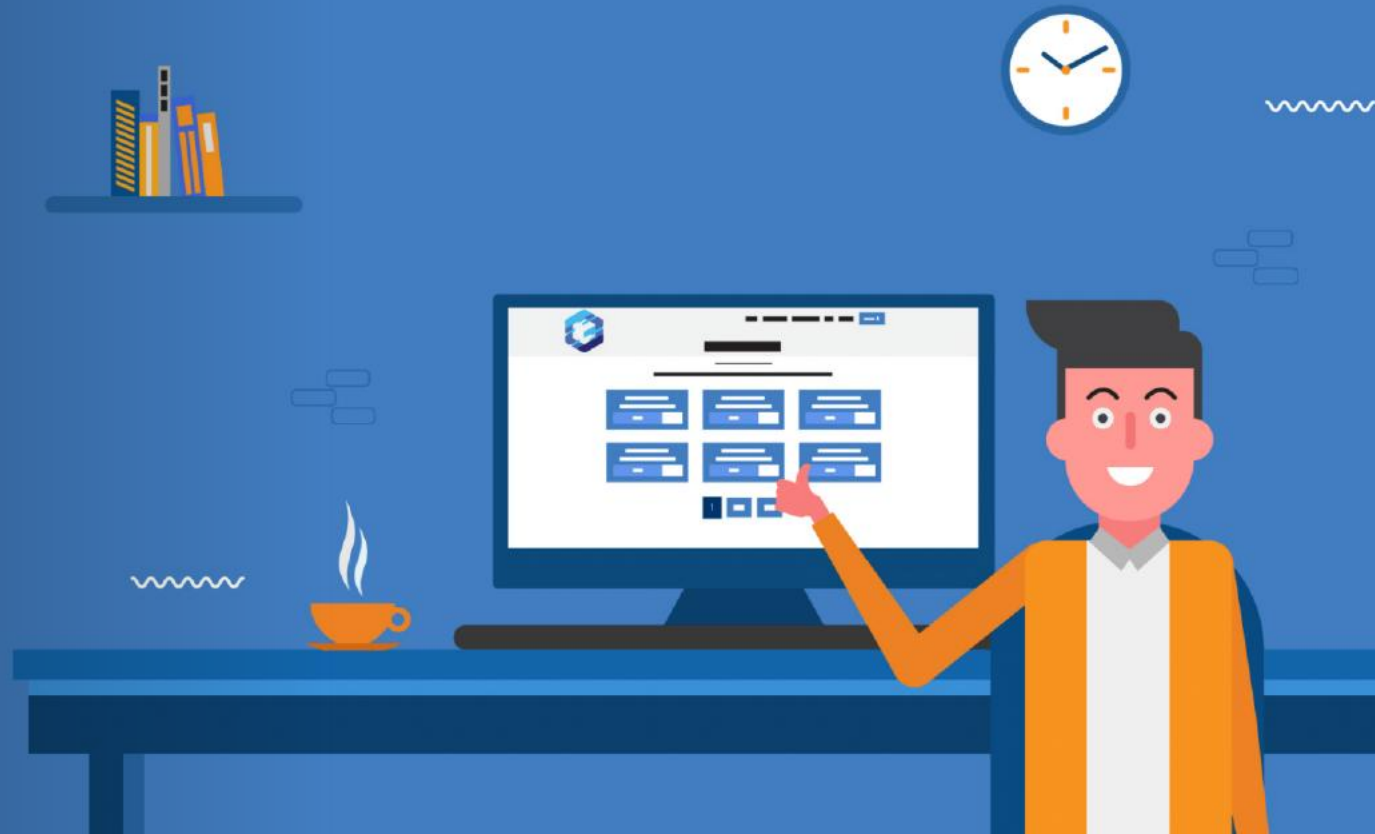
Search authentication combinations

- Phishing-resistant MFA (3)**
 - Windows Hello For Business / Platform Credential
 - Passkeys (FIDO2) [Advanced options](#)
 - Certificate-based Authentication (Multifactor) [Advanced options](#)
- Passwordless MFA (1)**
 - Microsoft Authenticator (Phone Sign-in)
- Multifactor authentication (13)**
 - Temporary Access Pass (One-time use)
 - Temporary Access Pass (Multi-use)
 - Password + Microsoft Authenticator (Push Notification)
 - Password + Software OATH token
 - Password + Hardware OATH token
 - Password + SMS
 - Password + Voice
 - Federated Multifactor
 - Federated Single factor + Microsoft Authenticator (Push Notification)
 - Federated Single factor + Software OATH token
 - Federated Single factor + Hardware OATH token
 - Federated Single factor + SMS
 - Federated Single factor + Voice
- Single factor authentication (5)**

Previous **Next**

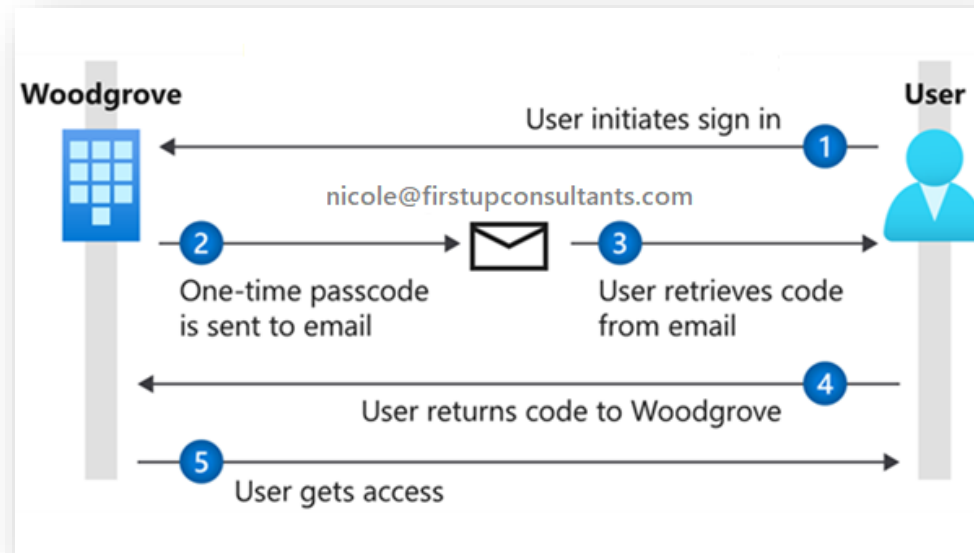
Gäste & Conditional Access

Demo



Hinweis zu der Teilen-Funktion & Gästen

Früher wurde die Absicherung beim Teilen von Dateien und Ordnern über SharePoint geregelt.



Empfehlung:

Aktivierung der auf Entra B2B Integration, wobei dadurch einmalig alle alten Links kaputt gehen.

Benutzertypen gezielt sichern

Wie viel Sicherheit darfs denn sein?



Umgang mit unterschiedlichen Benutzertypen

Endbenutzer

- Größter Schulungsbedarf
- Größte Angriffsfläche
- MFA verpflichtend
- Ziel: Passwordless

Externe Benutzer

- Zugriff begrenzt
- Regelmäßig aufräumen
- MFA verpflichtend

Servicebenutzer

- Stattdessen Workload Identities nutzbar?
- MFA und Nutzung begrenzen

Privilegierte Benutzer

- PIM nutzen
- Maximal starke Authentifizierung
- Nutzung begrenzen

Sonstige

- z.B. Shared Mailboxes
- Individuell entscheiden
- Nach Möglichkeit deaktivieren

Die Gefahr durch privilegierte Benutzer

Home > Groups | Overview > App registrations >

Roles and administrators | All roles

Wolke7

+ 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 →

Search by name or description | Privileged: Yes | Add filters

Role	Description	Privileged	Ass...↑↓	Type
<input type="checkbox"/> Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Attribute Provisioning Administrator	Read and edit the provisioning configuration of all active custom security attributes for an application.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Attribute Provisioning Reader	Read the provisioning configuration of all active custom security attributes for an application.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.	PRIVILEGED	0	Built-in
<input type="checkbox"/> B2C IEF Keyset Administrator	Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).	PRIVILEGED	0	Built-in
<input type="checkbox"/> Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	PRIVILEGED	1	Built-in
<input type="checkbox"/> Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Conditional Access Administrator	Can manage Conditional Access capabilities.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Domain Name Administrator	Can manage domain names in cloud and on-premises.	PRIVILEGED	0	Built-in
<input type="checkbox"/> External Identity Provider Administrator	Can configure identity providers for use in direct federation.	PRIVILEGED	0	Built-in
<input checked="" type="checkbox"/> Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	PRIVILEGED	5	Built-in
<input type="checkbox"/> Global Reader	Can read everything that a Global Administrator can, but not update anything.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Hybrid Identity Administrator	Can manage AD to Microsoft Entra cloud provisioning, Microsoft Entra Connect, and federation settings.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Intune Administrator	Can manage all aspects of the Intune product.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Lifecycle Workflows Administrator	Create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Microsoft Entra ID.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Password Administrator	Can reset passwords for non-administrators and Password Administrators.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Privileged Authentication Administrator	Can access to view, set and reset authentication method information for any user (admin or non-admin).	PRIVILEGED	2	Built-in
<input type="checkbox"/> Privileged Role Administrator	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Security Administrator	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.	PRIVILEGED	2	Built-in
<input type="checkbox"/> Security Operator	Creates and manages security events.	PRIVILEGED	0	Built-in
<input type="checkbox"/> Security Reader	Can read security information and reports in Microsoft Entra ID and Microsoft 365.	PRIVILEGED	0	Built-in
<input type="checkbox"/> User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	PRIVILEGED	1	Built-in

Getrennte Benutzerkonten für Administratoren

Administratoren leben in zwei Welten:

- Normale Tätigkeiten als Endbenutzer (z.B. Mails)
- Administrative Tätigkeiten

→ Gleicher Benutzer = Größere Angriffsfläche



Getrennte Benutzerkonten für Administratoren

Endbenutzer-Konto:

- Standard-Lizenzierung
- MFA (idealerweise Passwordless)
- Endbenutzer-Berechtigungen auf Inhalte und Funktionen

Administrator-Konto:

- Idealerweise Entra ID P2 oder E5
- Phishing-resistent MFA
- Keine dauerhaften Berechtigungen auf Inhalte
- Ausschließlich für administrative Tätigkeiten – aktiviert durch PIM



PIMst du schon?

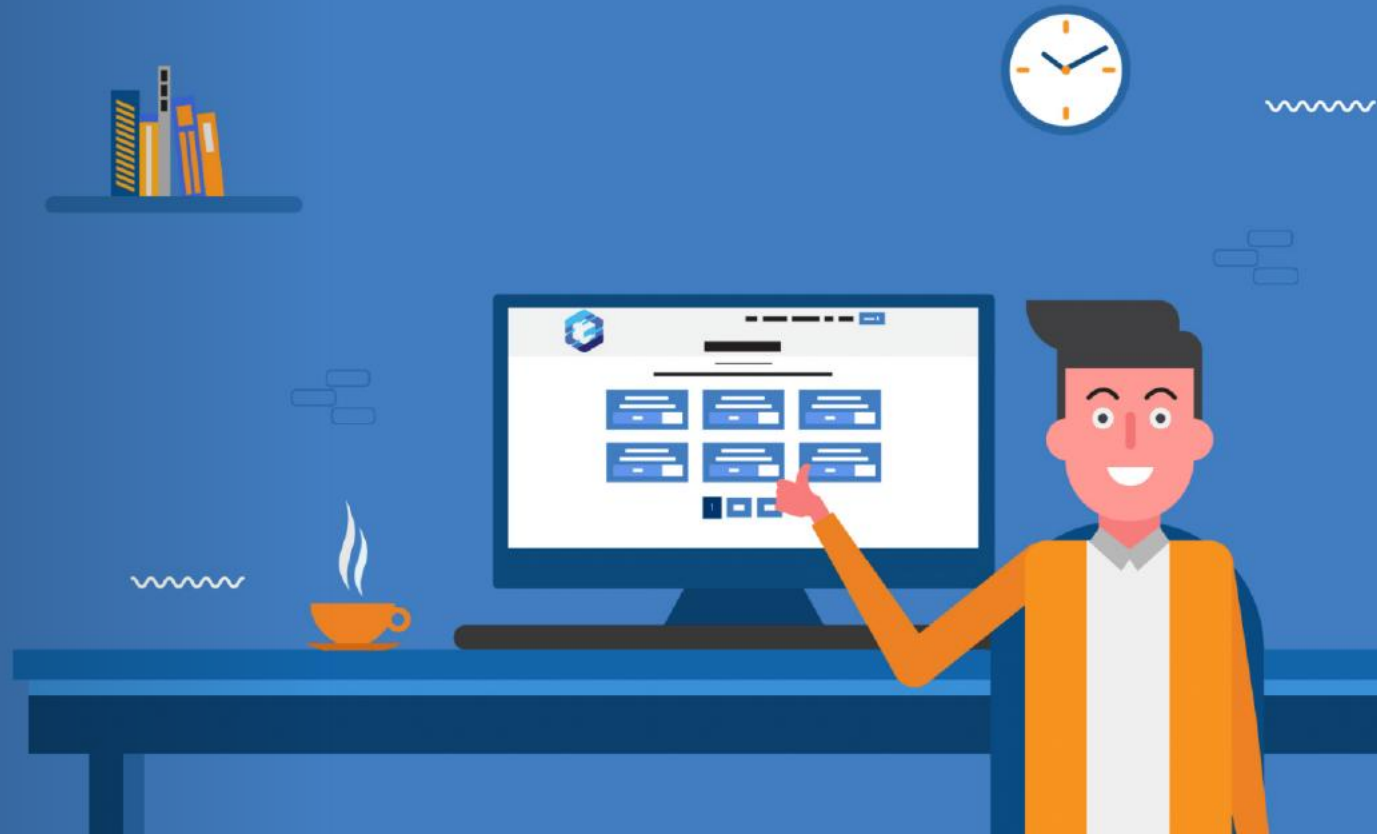
Privileged Identity Management ermöglicht es, dass administrative Berechtigungen nur bei Bedarf aktiviert und ggf. genehmigt werden müssen.

→ Selbst wenn das Admin-Konto kompromittiert wird, darf es zunächst nichts



Privileged Identity Management

Demo



Break Glass Accounts für den Notfallzugriff

Gesonderte Benutzerkonten mit Global Admin Rolle, die nur im Notfall verwendet werden und deren Authentifizierungsinformationen nur wenigen vertrauenswürdigen Personen zugänglich sind (z.B. Safe oder Bankschließfach)

Gute Anleitung von Microsoft dazu:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access>



Workload Identities

Zugriffe durch Dienste und Anwendungen



Workload Identity = Zugriff durch eine Anwendung auf unseren Tenant



karl.klammer@wolkesieben.onmicrosoft.com

Angeforderte Berechtigungen

Für Ihre Organisation überprüfen



Diese Anwendung wird nicht von Microsoft veröffentlicht.

Diese App benötigt folgende Berechtigungen:

- ✓ Alle Gruppen lesen und schreiben
- ✓ Vollständige Profile aller Benutzer lesen
- ✓ Anmelden und Benutzerprofil lesen
- ✓ Lesezugriff auf Benutzerprofile
- ✓ Lese- und Schreibzugriff auf verwaltete Metadaten
- ✓ Verfügt über Vollzugriff auf alle Sitesammlungen.

Wenn Sie zustimmen, erhält diese App Zugriff auf die angegebenen Ressourcen für alle Benutzer in Ihrer Organisation. Niemand sonst wird zur Überprüfung dieser Berechtigungen aufgefordert.

Durch das Akzeptieren dieser Berechtigungen gestatten Sie dieser App, Ihre Daten gemäß den Vertragsbedingungen und den Datenschutzbestimmungen zu verwenden. Unter <https://myapps.microsoft.com> können Sie diese Berechtigungen ändern. [Details anzeigen](#)

Wirkt diese App verdächtig? [Hier melden](#)

Abbrechen
Akzeptieren

Home > Wolke7 > Enterprise applications | All applications > Lansco easyGroups

Lansco easyGroups | Permissions

Enterprise Application

Review permissions Refresh Got feedback?

Overview
Deployment Plan
Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

Security

- Conditional Access
- Permissions**
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews

Troubleshooting + Support

- New support request

Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). [Learn more](#)

You can review, revoke, and restore permissions. [Learn more](#)

To configure requested permissions for apps you own, use the app registration. [Application registration](#)

Grant admin consent for Wolke7

Admin consent User consent

API name	Claim value	Permission	Type	Granted throu...	Granted by
Microsoft Graph (2)					
Microsoft Graph	Group.ReadWrite.All	Read and write all groups	Application	Admin consent	An administrat... ⋮
Microsoft Graph	User.Read.All	Read all users' full profiles	Application	Admin consent	An administrat... ⋮
Office 365 SharePoint Online (3)					
Office 365 SharePoint Online	TermStore.ReadWrite.All	Read and write managed metadata	Application	Admin consent	An administrat... ⋮
Office 365 SharePoint Online	User.Read.All	Read user profiles	Application	Admin consent	An administrat... ⋮
Office 365 SharePoint Online	Sites.FullControl.All	Have full control of all site collections	Application	Admin consent	An administrat... ⋮

Workload Identities gezielt steuern und überwachen

The screenshot displays the Microsoft Entra admin center interface for managing Enterprise applications. The left sidebar contains navigation options such as Home, Agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, Authentication methods, Password reset, Custom security attributes, Certificate authorities, External Identities, Cross-tenant synchronization, and Entra Connect.

The main content area shows the 'Enterprise applications | All applications' view. It includes a search bar, filters for 'Application type == Enterprise Applications' and 'Application ID starts with', and a table listing 53 applications found. The table columns are Name, Object ID, Application ID, Homepage URL, Created on, Certificate Expiration, and Active C.

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expir...	Active C
AvePoint Insights for Microsoft365	00d61a95-90dc-4b9...	ed6f3a56-29b3-4033...	https://www.avepoin...	19.9.2024	-	-
PM PnP Management Shell	090d64ec-aaab-4fc6...	31359c7f-bd7e-475c...	https://aka.ms/m365...	7.3.2022	-	-
AvePoint Cloud Governance for Power Platfo...	09e3e2b8-1616-43ff...	db5de099-d0ed-416...	https://www.avepoin...	19.9.2024	-	-
MG Microsoft Graph Command Line Tools	10ec52dc-c873-43c6...	14d82eec-204b-4c2f...	https://docs.microso...	29.4.2025	-	-
F FlowRPCustomConnector	146ce045-7525-469...	ccc737ba-4bcc-4a71...	https://us.flow.micro...	27.8.2018	-	-
AvePoint tyGraph for SharePoint	1627c112-0d36-4fb6...	8229eae2-480b-4e7...		16.1.2025	-	-
Lansco easyGroups	287304e9-6b57-492...	8efa7ae2-3a38-4680...		3.8.2020	-	-
AvePoint Cloud Backup for Microsoft365 (All...	296b4418-17c2-4daf...	c21d796d-56a5-430...	https://identity.avep...	24.3.2025	-	-
Confluence Cloud	2ba65c8d-85d1-4a0...	4aa38041-66a2-41a...		9.5.2022	-	-
AvePoint Online Services	335d427f-2b2a-488...	ae16e128-c76e-4a38...	https://identity.avep...	17.9.2024	-	-
AvePoint Cloud Backup for Azure	35f2f488-16df-4512-...	6adeb4df-f01f-43e2-...	https://identity.avep...	19.9.2024	-	-
AvePoint Fly for Entra ID Source and Destina...	3a527e4e-1ca5-46df...	1da3c5b1-ad1e-417...	https://www.avepoin...	9.7.2025	-	-
MC MSC Chat Copilot Backend	3f2233b3-e02d-41c0...	2c8131de-cddd-44d...		3.9.2023	-	-
AVA	3fcf2af6-222d-4829-...	6f30434d-3cfa-4cf8-...	https://login.microso...	4.11.2024	-	-
AvePoint Fly	431d1600-09e0-4d0...	34be87c0-bd08-47a...	https://identity.avep...	9.7.2025	-	-
Sync to ASW Dev Tenant	44d16985-e0f1-4344...	978ff7fc-da1f-43cc-8...	https://account.activ...	16.6.2025	-	-
PnP PowerShell	4731f6e9-9d12-49f5...	bb0c5778-9d5c-41e...		15.6.2018	-	-
RD Rencore Deploy SPFx package	4d1d902f-1566-428...	be278e09-27a8-47a...		19.3.2019	-	-
APElements Security and Analysis	59521907-d8f6-4f49...	97c60a23-521e-407...		16.1.2025	-	-
AvePoint Cloud Governance for Microsoft365	63610cfa-79ee-4bb8...	1a7f2da3-4c8d-4896...	https://www.avepoin...	19.9.2024	-	-
PnP PowerShell	64bcfa27-5887-46cc...	b8f82186-3b88-4d4...		12.9.2024	-	-


Consent für Workload Identities klar regeln

Home > Wolke7 > Enterprise applications | All applications > Lansco easyGroups | Permissions > Enterprise applications | User settings >


Consent and permissions | User consent settings ...


«  Save  Discard |  Got feedback?

Manage

 User consent settings

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

 Admin consent settings

 Permission classifications

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

- Do not allow user consent
An administrator will be required for all apps.
- Allow user consent for apps from verified publishers, for selected permissions
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.
- Let Microsoft manage your consent settings (Recommended)
Automatically update your organization to Microsoft's current user consent guidelines. [Learn more](#)

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings

Was ist mit Device Management?

Device Management ist wie Identity & Access Management ein zentraler Bestandteil des Zero Trust-Modells.

Intune bietet eine sehr gute Integration in die restlichen Security-Funktionen der Microsoft Cloud.

Um nicht den Rahmen zu sprengen:
Bei Interesse gerne melden 😊



Evergreen Security



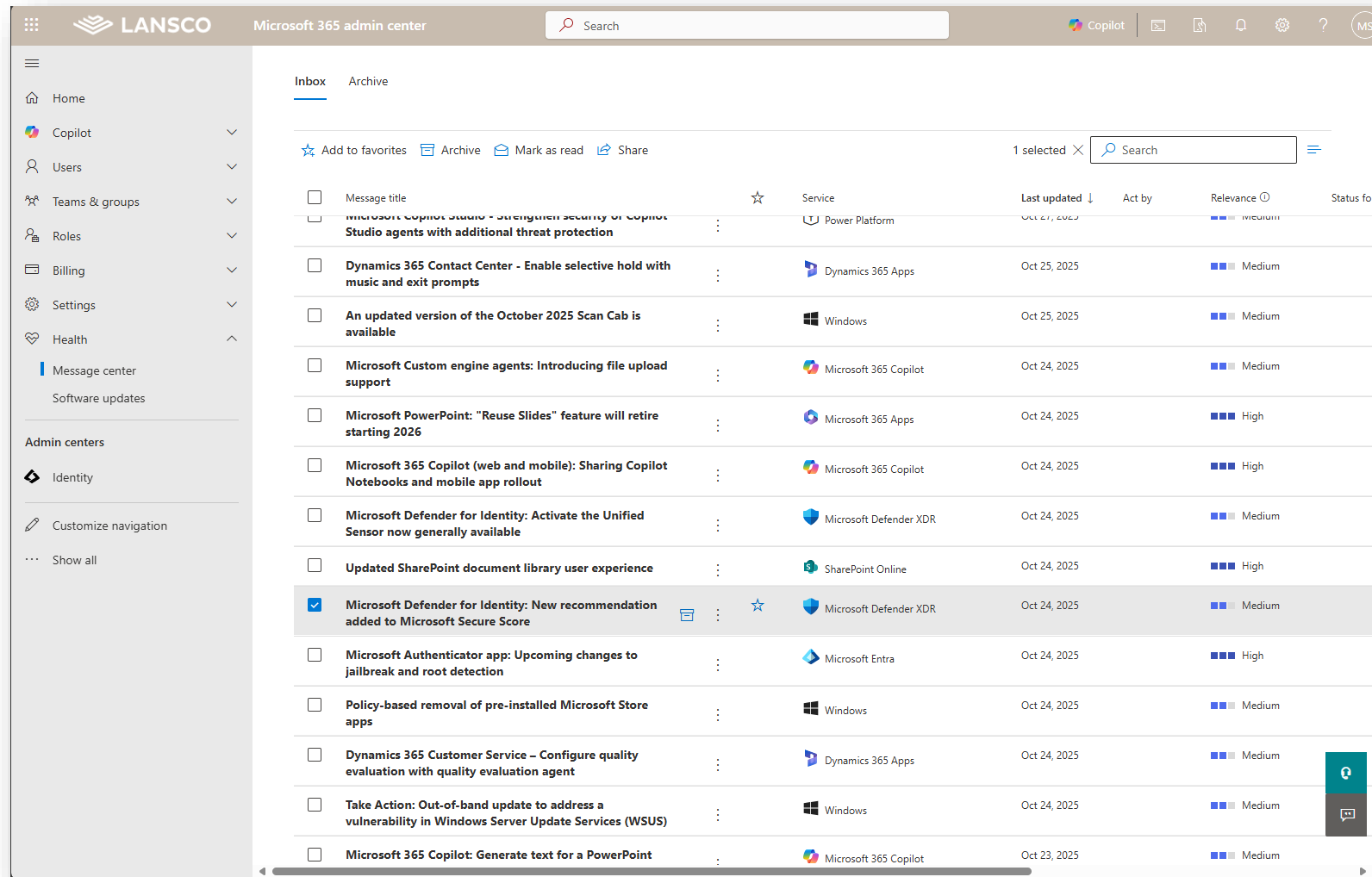
Prozesse für den laufenden Betrieb

Welche Prozesse sollten mindestens etabliert sein?

1. Lebenszyklus für Benutzerkonten
2. Lebenszyklus für Workload Identities
3. Verarbeitung des Message Centers
4. Überwachung des Secure Scores
5. Reaktion auf Security Alerts
6. Vorgehen für Forensik und Logsichtungung
7. Vorgehen für Notfallzugriff



Message Center als Quelle für (sicherheitsrelevante) Neuerungen

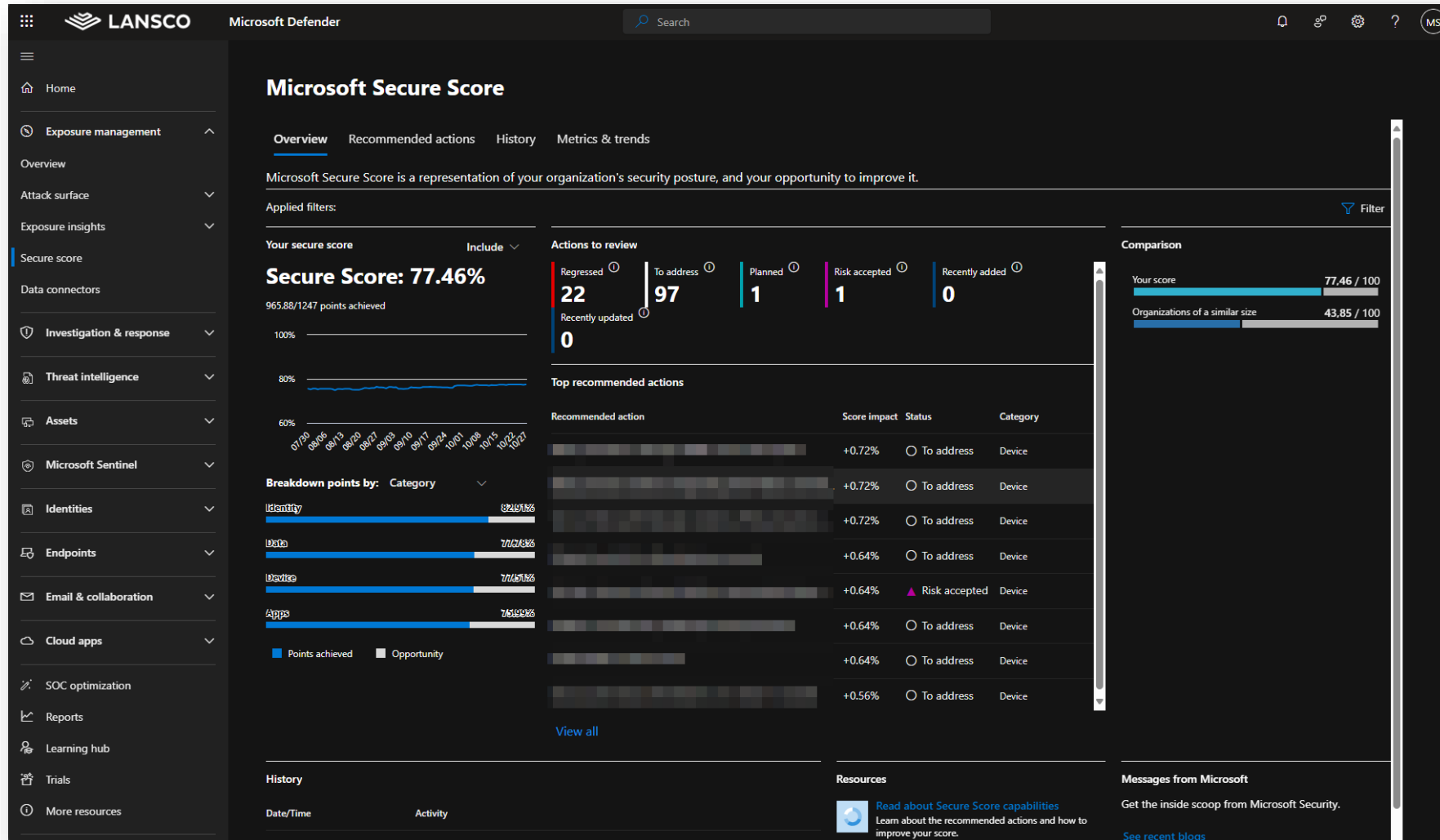


The screenshot displays the Microsoft 365 admin center interface, specifically the Message Center. The left sidebar shows navigation options like Home, Copilot, Users, Teams & groups, Roles, Billing, Settings, Health, Message center, and Software updates. The main content area shows a list of messages with the following columns: Message title, Service, Last updated, Act by, Relevance, and Status. One message is selected, indicated by a checkmark in the left margin.

Message title	Service	Last updated	Act by	Relevance	Status
Microsoft Copilot Studio - Strengthen security of Copilot Studio agents with additional threat protection	Power Platform	Oct 21, 2025		Medium	
Dynamics 365 Contact Center - Enable selective hold with music and exit prompts	Dynamics 365 Apps	Oct 25, 2025		Medium	
An updated version of the October 2025 Scan Cab is available	Windows	Oct 25, 2025		Medium	
Microsoft Custom engine agents: Introducing file upload support	Microsoft 365 Copilot	Oct 24, 2025		Medium	
Microsoft PowerPoint: "Reuse Slides" feature will retire starting 2026	Microsoft 365 Apps	Oct 24, 2025		High	
Microsoft 365 Copilot (web and mobile): Sharing Copilot Notebooks and mobile app rollout	Microsoft 365 Copilot	Oct 24, 2025		High	
Microsoft Defender for Identity: Activate the Unified Sensor now generally available	Microsoft Defender XDR	Oct 24, 2025		Medium	
Updated SharePoint document library user experience	SharePoint Online	Oct 24, 2025		High	
Microsoft Defender for Identity: New recommendation added to Microsoft Secure Score	Microsoft Defender XDR	Oct 24, 2025		Medium	
Microsoft Authenticator app: Upcoming changes to jailbreak and root detection	Microsoft Entra	Oct 24, 2025		High	
Policy-based removal of pre-installed Microsoft Store apps	Windows	Oct 24, 2025		Medium	
Dynamics 365 Customer Service - Configure quality evaluation with quality evaluation agent	Dynamics 365 Apps	Oct 24, 2025		Medium	
Take Action: Out-of-band update to address a vulnerability in Windows Server Update Services (WSUS)	Windows	Oct 24, 2025		Medium	
Microsoft 365 Copilot: Generate text for a PowerPoint	Microsoft 365 Copilot	Oct 23, 2025		Medium	

<https://admin.cloud.microsoft/?#/MessageCenter>

Secure Score als Metrik und Leitfaden für einen sicheren Tenant



<https://security.microsoft.com/exposure-secure-score>

Alerts Policies nutzen

Alert policy

Mail flow alerts have moved to the new Exchange admin center. Starting Oct 2021, customers will only be able to create/view/edit mail flow alerts in the new Exchange admin center. [Try it now](#)

+ New Alert Policy Refresh 48 items Search Filter

Name	Severity	Type	Category	Date modified(UTC)	Tags	Status
[Redacted]	Medium	Custom	Information governance	Oct 1, 2025 12:33 PM	-	On
[Redacted]	High	Custom	Permissions	Nov 21, 2024 8:38 PM	-	On
<input type="checkbox"/> MIP AutoLabel simulation completed	Low	System	Threat management	Mar 9, 2021 8:31 PM	-	On
<input type="checkbox"/> Suspicious email sending patterns detected	Medium	System	Threat management	Feb 11, 2020 6:29 PM	-	On
<input type="checkbox"/> Email messages removed after delivery	Informational	System	Threat management	Apr 8, 2022 3:12 PM	-	On
<input type="checkbox"/> Email messages from a campaign removed after delivery	Informational	System	Threat management	Apr 8, 2022 3:12 PM	-	On
<input type="checkbox"/> Admin triggered user compromise investigation	Medium	System	Threat management	Aug 3, 2021 10:42 AM	-	On
<input type="checkbox"/> A user clicked through to a potentially malicious URL	High	System	Threat management	May 31, 2022 10:34 AM	-	On
<input type="checkbox"/> Suspicious connector activity	High	System	Threat management	May 10, 2022 3:31 PM	-	On
<input type="checkbox"/> Successful exact data match upload	Low	System	Threat management	Feb 16, 2021 5:11 PM	-	On
<input type="checkbox"/> Administrative action submitted by an Administrator	Informational	System	Threat management	Apr 3, 2025 5:34 PM	-	On
<input type="checkbox"/> Elevation of Exchange admin privilege	Low	System	Permissions	Nov 29, 2018 6:02 AM	-	On
<input type="checkbox"/> Reply-all storm detected	High	System	Mail flow	Feb 28, 2025 9:34 PM	-	On
<input type="checkbox"/> Email messages containing malware removed after deli...	Informational	System	Threat management	May 4, 2021 5:24 PM	-	On
<input type="checkbox"/> Email messages containing malicious URL removed afte...	Informational	System	Threat management	Apr 8, 2022 3:12 PM	-	On

<https://security.microsoft.com/alertpoliciesv2>

<https://learn.microsoft.com/en-us/defender-xdr/alert-policies>

Audit- und Signin-Logs um Ereignisse nachzuvollziehen

The image shows two overlapping screenshots from Microsoft's cloud management tools. The background screenshot is the Microsoft Purview Audit search results page, displaying a table of 132 items. The foreground screenshot is the Microsoft Entra admin center, showing a detailed view of sign-in events for a user named 'karl.klamme'.

Microsoft Purview Audit Search Results (Sample Data):

Date (UTC)	IP Address	User	Record Type	Activity	Item
Oct 15, 2025 5:50 ...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	Inhaltssammlung...
Oct 15, 2025 5:44...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	Inhaltssammlung...
Oct 15, 2025 5:44...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	fa2fa1d2-2589-46...
Oct 15, 2025 5:44...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	IKP Inhaltssamml...
Oct 15, 2025 5:26...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	__sitelcon_.jpg
Oct 15, 2025 5:26...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	AllItems.aspx
Oct 15, 2025 5:23 ...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	AllItems.aspx
Oct 15, 2025 5:23 ...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	AllItems.aspx
Oct 15, 2025 5:23 ...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	AllItems.aspx
Oct 15, 2025 5:23 ...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	AllItems.aspx
Oct 15, 2025 5:23 ...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	AllItems.aspx
Oct 15, 2025 5:23 ...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	AllItems.aspx
Oct 15, 2025 5:23 ...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	AllItems.aspx
Oct 15, 2025 5:23 ...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	AllItems.aspx
Oct 15, 2025 5:23 ...	[Redacted]	marco.schmittnae...	SharePointFileOp...	Accessed file	AllItems.aspx

Microsoft Entra admin center Sign-in events (Sample Data):

Date	Request ID	User principal name	Application	Status	IP address	Resc
2025-10-27T14:32:06Z	099e63d3-51e7-44ab-a8a2-5445...	karl.klamme	Lansco easyGroups	Interrupted	[Redacted]	Win
2025-10-27T14:31:29Z	099e63d3-51e7-44ab-a8a2-5445...	karl.klamme	Azure Portal	Success	[Redacted]	Azu
2025-10-27T14:31:22Z	d4e32826-64e5-4f90-894a-8a6a...	karl.klamme	Azure Portal	Success	[Redacted]	Azu
2025-10-27T14:24:00Z	788d1d52-5e2d-4947-979d-06b...	karl.klamme	Azure Portal	Success	[Redacted]	Azu
2025-10-27T14:12:20Z	7a9d3064-f639-4826-807d-9271...	karl.klamme	Office 365 SharePoint O...	Failure	[Redacted]	Offi
2025-10-27T13:44:30Z	322e6108-64d4-4672-96b2-237a...	karl.klamme	Office365 Shell WCSS-CL...	Success	[Redacted]	Offi
2025-10-27T13:44:25Z	68683fcb-5e3b-4f72-973f-40b49...	karl.klamme	SharePoint Online Web ...	Success	[Redacted]	Micr
2025-10-27T13:44:23Z	ccc3e44f-42b6-4a21-8a1a-a400d...	karl.klamme	Office 365 SharePoint O...	Success	[Redacted]	Offi
2025-10-27T13:29:10Z	56d85c8f-ffc5-4ccf-adc2-7497d9...	karl.klamme	Azure Portal	Success	[Redacted]	Azu
2025-10-27T13:14:14Z	ae96deb-a814-449a-8205-c2d0...	karl.klamme	Office365 Shell WCSS-CL...	Success	[Redacted]	Offi
2025-10-27T13:14:11Z	6bc0f883-ec9e-4785-ade6-55f70...	karl.klamme	Power Virtual Agents	Success	[Redacted]	Pow
2025-10-27T13:05:39Z	dca3c829-1b35-4fc2-865a-583f9...	karl.klamme	Azure Portal	Success	[Redacted]	Azu
2025-10-27T12:30:28Z	905dc008-48a7-43b7-b776-ee54...	karl.klamme	Office365 Shell WCSS-CL...	Success	[Redacted]	Offi
2025-10-27T12:30:18Z	653d7c6a-4850-491f-afb2-19ed9...	karl.klamme	Office365 Shell WCSS-CL...	Success	[Redacted]	Offi
2025-10-27T12:30:11Z	de7aca02-7f4f-413e-88f5-7bdc1...	karl.klamme	SharePoint Online Web ...	Success	[Redacted]	Micr
2025-10-27T12:30:08Z	1b840a3b-190f-4900-8d09-8003...	karl.klamme	Office 365 SharePoint O...	Success	[Redacted]	Offi
2025-10-27T12:27:04Z	6f44da75-24f7-41d4-a9e7-2ada3...	karl.klamme	One Outlook Web	Success	[Redacted]	Offi
2025-10-27T12:26:47Z	868c8c90-75b9-4ef5-9157-5e16...	karl.klamme	Azure Portal	Success	[Redacted]	Azu
2025-10-27T12:26:25Z	b5842f7e-cdbb-43a3-8506-dea9...	karl.klamme	Azure Portal	Success	[Redacted]	Azu
2025-10-27T12:26:22Z	0cb7768a-5b05-45c7-8ce0-90e7...	karl.klamme	Azure Portal	Interrupted	[Redacted]	Azu

<https://purview.microsoft.com/audit/auditsearch>

https://entra.microsoft.com/#view/Microsoft_AAD_IAM/SignInLogsList.ReactView

Wie könnt ihr konkret als nächstes tun?

1. Lizenzierung klären: Conditional Access für Endbenutzer & PIM für Admins
(siehe <https://m365maps.com/matrix.htm>)
2. Getrennte Konten & PIM für Admins einführen
3. Break Glass Accounts einrichten
4. MFA über Conditional Access gezielt erzwingen
5. Secure Score und dessen Empfehlungen sichten



Fragen & Diskussion

