

Compliance mit IT

Identity Governance & Administration (IGA) im Kontext Compliance

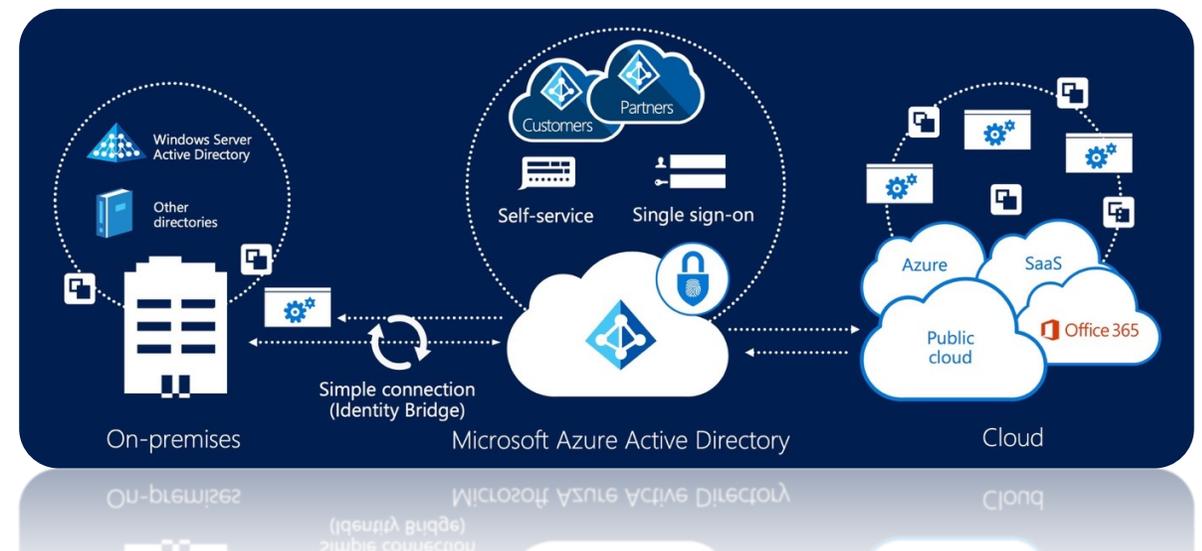


Jens Lorenz
Strategic Consultant, CISSP, CCSP, CIPT
Swiss IT Security Deutschland GmbH

Azure AD - Identity as a Service

Zentraler Cloud-basierter Identitäts-Provider

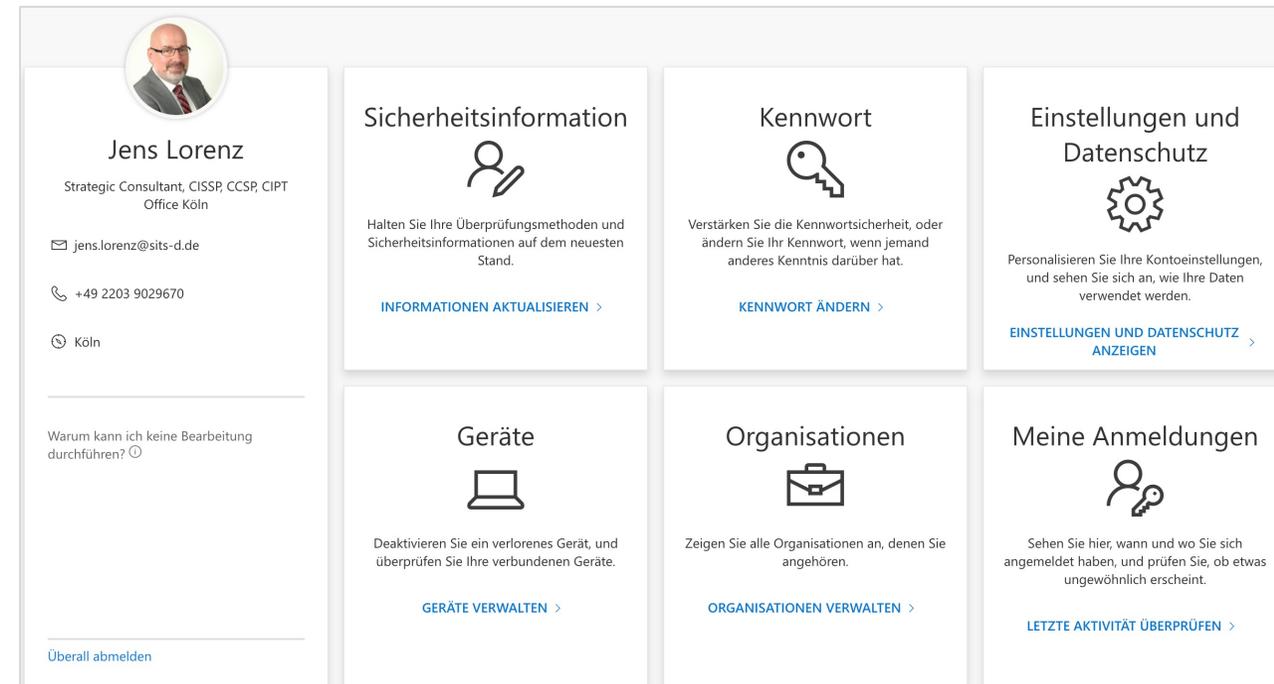
- Bereitstellen von hybriden Identitäten
 - Integration von dezentralen Identitätsquellen
- Zentrale Authentifizierung und Autorisierung
 - Single Sign-On für angebundene Applikationen



Azure AD - Identity as a Service

Zentraler Cloud-basierter Identitäts-Provider

- Self-Service Funktionalitäten
 - Kennwort ändern / zurücksetzen
 - Delegation von Gruppenverwaltung
 - Geräte und Anmeldungen
 - Sicherheitsinformationen
 - Datenschutzinformationen und Einstellungen



The screenshot displays the user interface for a self-service portal. At the top left, there is a profile card for Jens Lorenz, a Strategic Consultant, with contact information for email, phone, and location. Below this is a help link. The main area consists of eight tiles, each representing a different self-service function: 'Sicherheitsinformation' (Security Information), 'Kennwort' (Password), 'Einstellungen und Datenschutz' (Settings and Privacy), 'Geräte' (Devices), 'Organisationen' (Organizations), and 'Meine Anmeldungen' (My Sign-ins). Each tile includes an icon, a brief description of the function, and a link to access the service. At the bottom left, there is a link to 'Überall abmelden' (Sign out everywhere).

Jens Lorenz
Strategic Consultant, CISSP, CCSP, CIPT
Office Köln

✉ jens.lorenz@sits-d.de
☎ +49 2203 9029670
📍 Köln

Warum kann ich keine Bearbeitung durchführen? ⓘ

[Überall abmelden](#)

Sicherheitsinformation
Halten Sie Ihre Überprüfungsmethoden und Sicherheitsinformationen auf dem neuesten Stand.
[INFORMATIONEN AKTUALISIEREN >](#)

Kennwort
Verstärken Sie die Kennwortsicherheit, oder ändern Sie Ihr Kennwort, wenn jemand anderes Kenntnis darüber hat.
[KENNWORT ÄNDERN >](#)

Einstellungen und Datenschutz
Personalisieren Sie Ihre Kontoeinstellungen, und sehen Sie sich an, wie Ihre Daten verwendet werden.
[EINSTELLUNGEN UND DATENSCHUTZ ANZEIGEN >](#)

Geräte
Deaktivieren Sie ein verlorenes Gerät, und überprüfen Sie Ihre verbundenen Geräte.
[GERÄTE VERWALTEN >](#)

Organisationen
Zeigen Sie alle Organisationen an, denen Sie angehören.
[ORGANISATIONEN VERWALTEN >](#)

Meine Anmeldungen
Sehen Sie hier, wann und wo Sie sich angemeldet haben, und prüfen Sie, ob etwas ungewöhnlich erscheint.
[LETZTE AKTIVITÄT ÜBERPRÜFEN >](#)

Bring Your Own Identity

Azure AD Externe Identitäten

- Authentifizierung von externen Konten in der eigenen Organisation, Autorisierung der Zugriffe in der Ziel-Organisation
 - Azure Active Directory
 - Microsoft Konto
 - Einmalpasscode (OTP)
 - SAML/WS-Fed IdP
 - Social Identities
 - Google (gmail)
 - Facebook

User type	Source
Guest	Microsoft Account
Guest	External Azure Active Directory
Guest	External Azure Active Directory
Guest	OTP
Guest	OTP

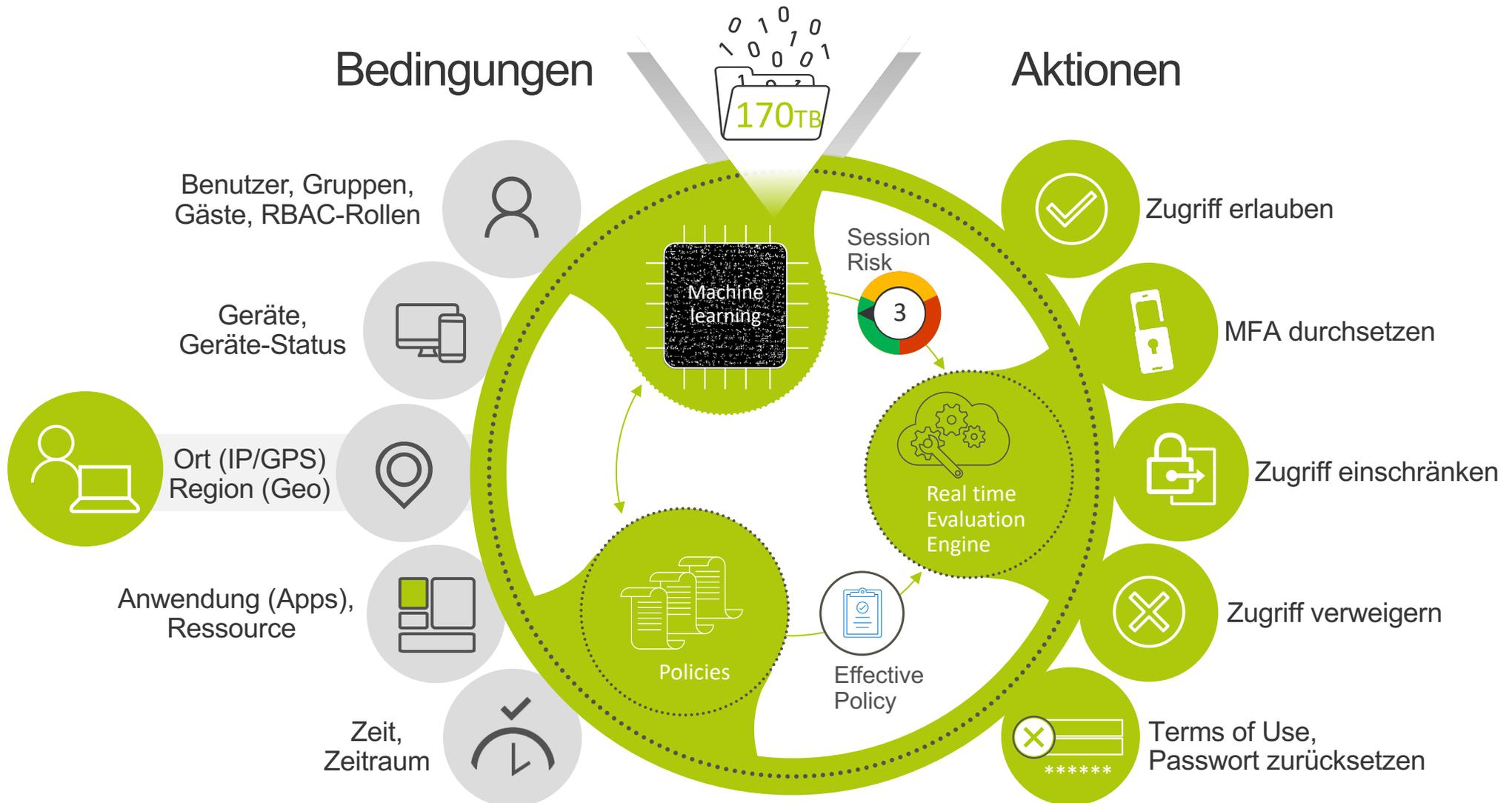
Das „Zero-Trust“ Modell



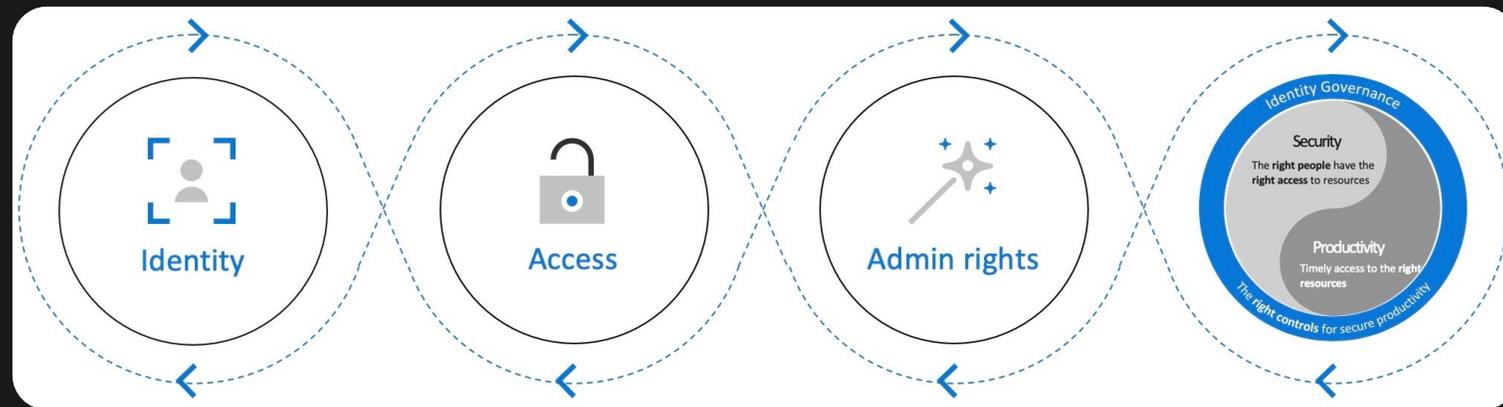
Zero-Trust Prinzipien



Azure AD Bedingter Zugriff



Azure AD Identity Governance



Azure AD Identity Governance

Rollen- und Rechtemanagement, Delegation, Prüfung und Re-Zertifizierung

- Lebenszyklus einer Identität
- Zugriffslebenszyklus
- Privilegierter Zugriffslebenszyklus

Für Interne und externe Identitäten



Entitlement management



Access reviews

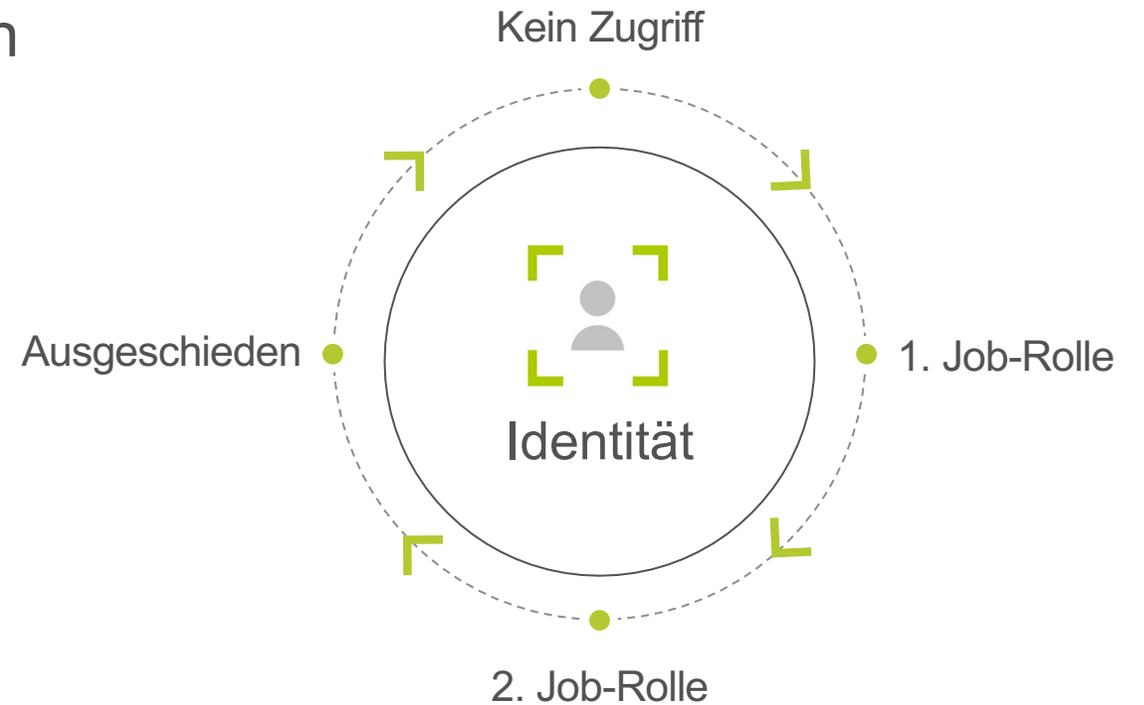


Privileged Identity Management

Azure AD Identity Governance

Lebenszyklus einer Identität

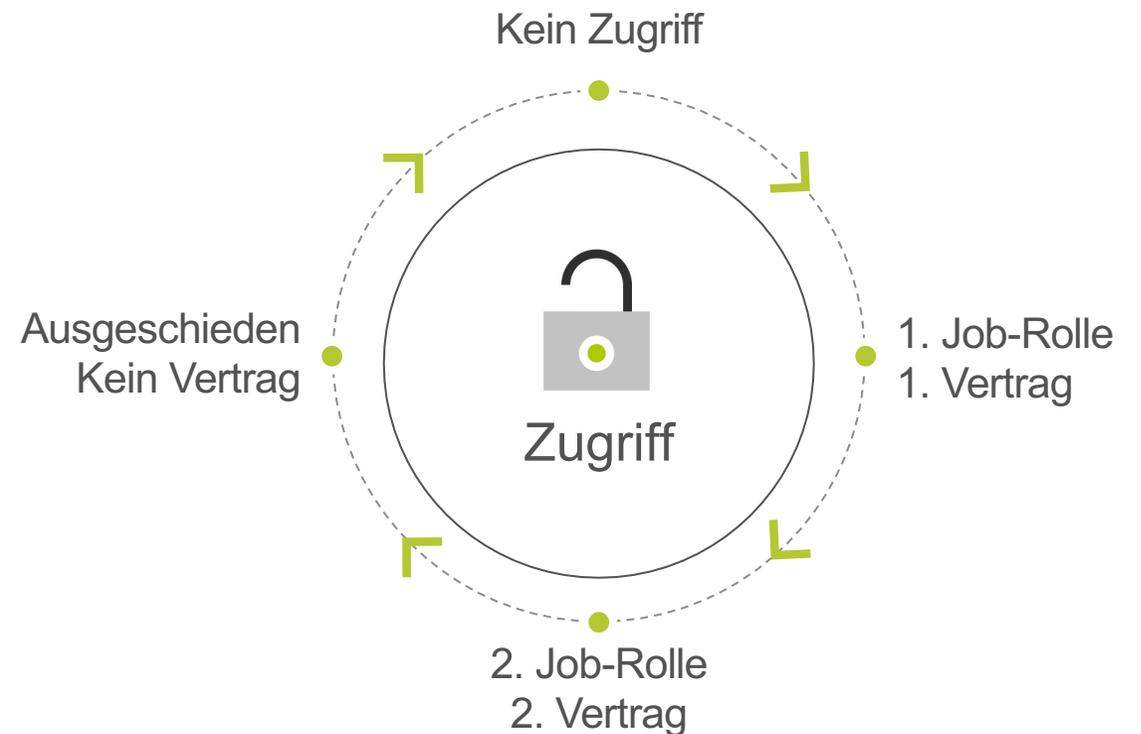
- Benutzer-Provisionierung/Deprovisionierung
- Zeitgerechte Zugriffe auf Ressourcen
- Zugriffsänderungen über die Zeit



Azure AD Identity Governance

Zugriffslebenszyklus

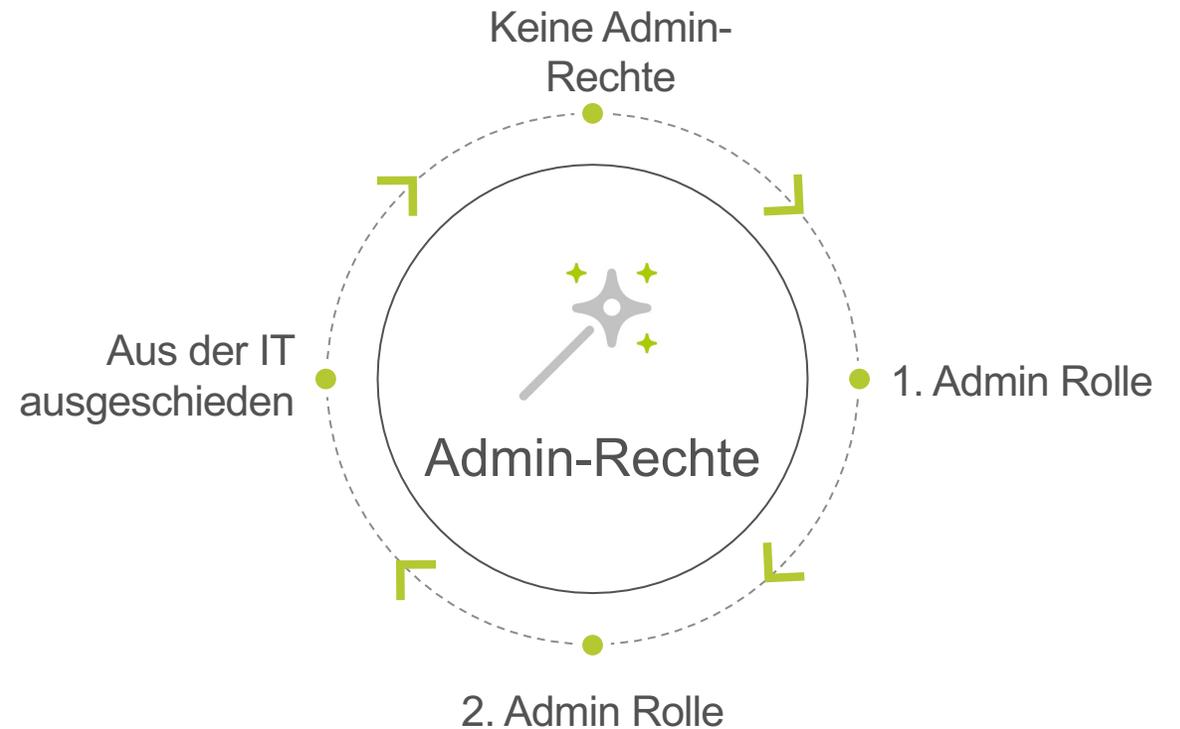
- Verwalten von Zugriffsänderungen über die Zeit
- Delegation von Genehmigungs-Workflows für Zugriffe
- Re-Zertifizierungen
- Prozess-Automatisierung



Azure AD Identity Governance

Priviligiierter Zugriffslebenszyklus

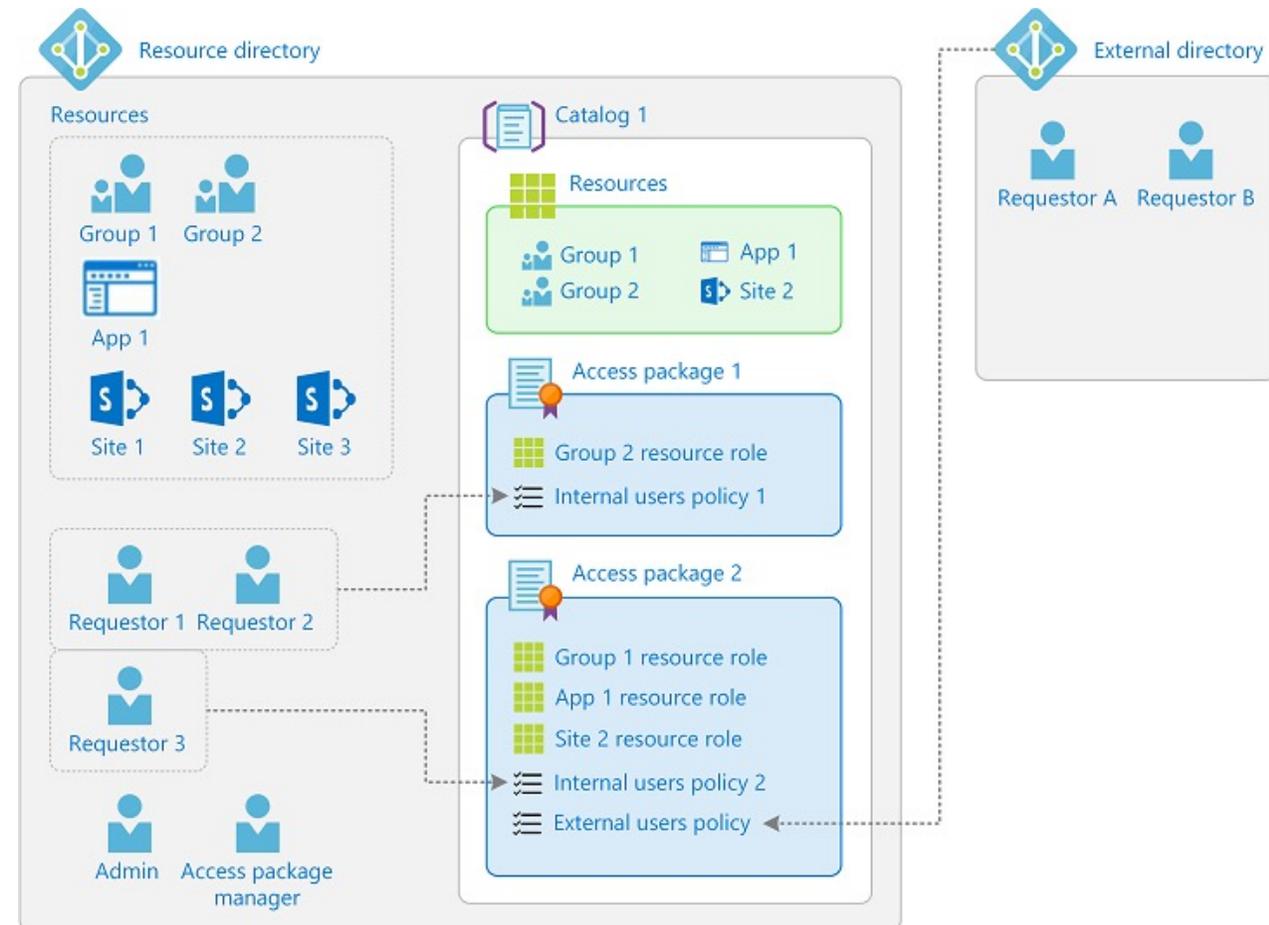
- „Just-in-Time“-Zugriff
- Zeitgebundener Zugriff
- Genehmigungsprozesse
- Re-Zertifizierungen
- Mehrstufige Authentifizierung
- Überwachung und Alarmierung
- Bedingter Zugriff



Azure AD Identity Governance

Entitlement Management

- Ressourcen
- Kataloge
- Zugriffspakete
- Ressourcen Rollen
- Benutzer-Richtlinien
- Anforderer (Intern/Extern)
- Genehmigungsprozesse (Einfach oder Mehrstufig)
- Genehmigende Person/en



Azure AD Identity Governance

Entitlement Management

- Richtlinien für Zugriffspakete
 - Zuweisungen
 - Genehmigungsprozess

* Basics * **Requests** Requestor information (Preview) * Lifecycle Rules (Preview)

Users who can request access

For users in your directory
Allow users and groups in your directory to request this access package

For users not in your directory
Allow users in connected organizations (other directories and domains) to request this access package

None (administrator assignments only)
Allow administrators to directly assign specific users to this access package; other users cannot request this access package

Specific users and groups
 All members (excluding guests)
 All users (including guests)

Select users and groups 0 selected
[* + Add users and groups](#)

Approval

Require approval * Yes No

Enable

Enable new requests and assignments * Yes No

Approval

Require approval * Yes No

Require requestor justification Yes No

How many stages 1 2 3 (Preview)

First Approver

Manager as approver

Manager as approver

Choose specific approvers [* + Add fallback](#)

Decision must be made in how many days? Maximum 14

Require approver justification Yes No

[Hide advanced request settings](#)

If no action taken, forward to alternate approvers? Yes No

Alternate Approver

Second level manager as alternate approver (Preview)

Fallback 0 selected
[* + Add fallback](#)

Forward to alternate approver(s) after how many days? (Allowed number of days is 8 - 13)

Second Approver

Choose specific approvers

Select approvers 0 selected
[* + Add approvers](#)

Decision must be made in how many days? Maximum 14

Require approver justification Yes No

[Hide advanced request settings](#)

If no action taken, forward to alternate approvers? Yes No

Alternate Approver

Choose specific alternate approvers

Select alternate approvers 0 selected
[* + Add alternate approvers](#)

Forward to alternate approver(s) after how many days? (Allowed number of days is 8 - 13)

Azure AD Identity Governance

Entitlement Management

- Informationen zum Antragsteller
 - Fragen, z.B. zur Unterstützung des Genehmigers
 - Attribute – Verzeichnis-Schema oder Schema-Erweiterung

* Basics * Requests **Requestor information** * Lifecycle

Collect information and attributes from requestor. Go to Catalogs to add attributes for this access package's catalog resources. [Learn more](#)

Questions Attributes (Preview)

Question	Answer format	Multiple choice options	Required
This access needs validation. Please enter your first name and last name as stated on an identification you will need to produce during the validation process. By submitting this request, you agree that	Multiple choice	Edit and localize	<input checked="" type="checkbox"/>
First name (as stated in your passport or similar form of identity - middle names are not required) *	Short text		<input checked="" type="checkbox"/>

Attribute type	Attribute	Default display string	Answer format	Multiple choice options	Attribute value is editable	Keep value when assignment is removed
Built-in	Choose attribute	Enter string	Answer format			No
Choose		Enter string	Answer format			No

- User.city
- User.companyName
- User.country
- User.department
- User.displayName

Azure AD Identity Governance

Entitlement Management

- Zugriffslebenszyklus
 - Ablauf von Zuweisungen
 - Re-Zertifizierung
 - Automatisierung

If reviewers don't respond ⓘ

Show reviewer decision helpers ⓘ

Require reviewer justification ⓘ

Take recommend... ^

No change

Remove access

Take recommendation

* Basics Resource roles * Requests Requestor information (Preview) * Lifecycle Rules (Preview)

Expiration

Access package assignments expire ⓘ On date **Number of days** Never

Assignments expire after 365

[Hide advanced expiration settings](#)

Allow users to extend access * ⓘ **Yes** No

Require approval to grant extension * ⓘ **Yes** No

Access Reviews

Require access reviews * **Yes** No

Starting on ⓘ 23/02/2021

Review frequency ⓘ Annually Bi-annually **Quarterly** Monthly Weekly (preview)

Duration (in days) ⓘ 25
Maximum 80

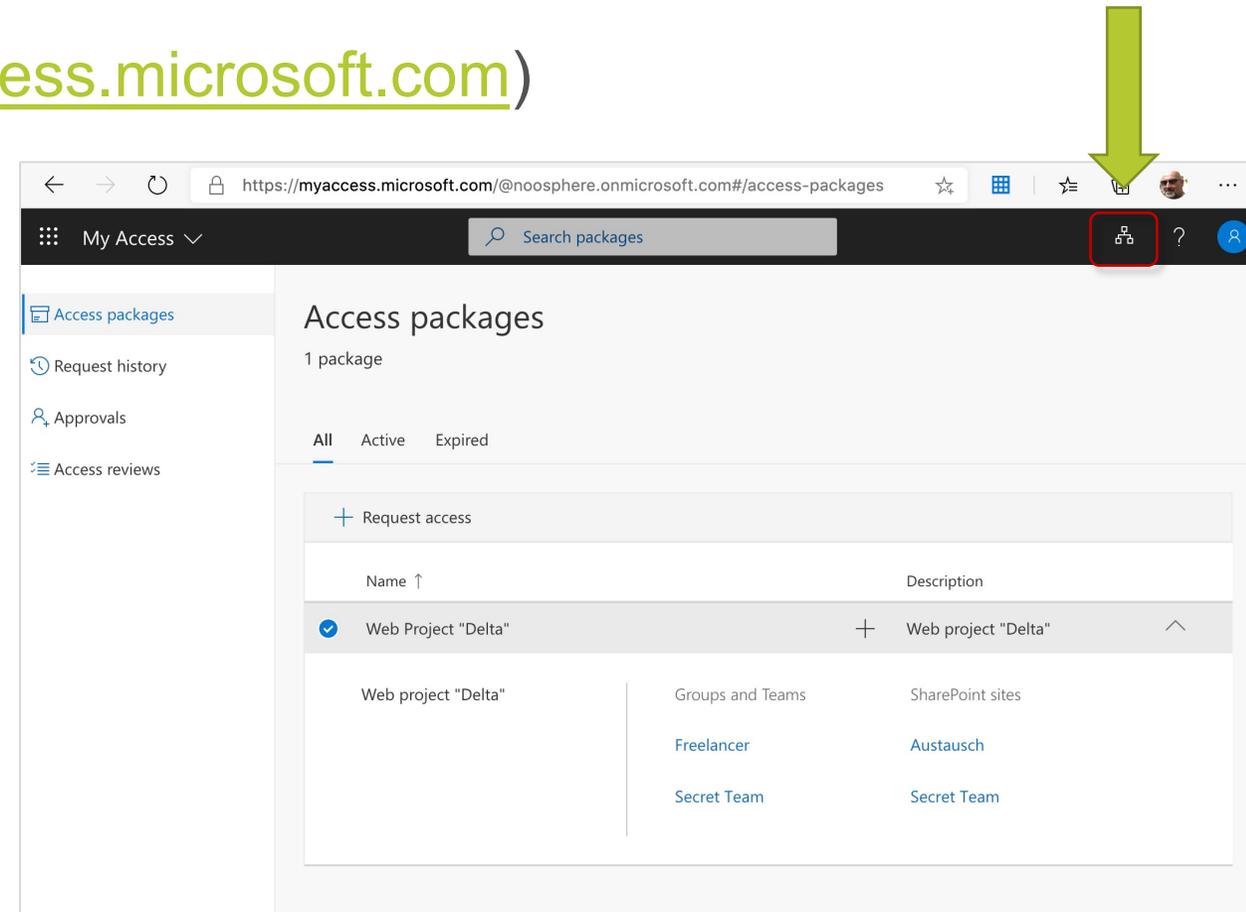
Reviewers ⓘ Self-review Specific reviewer(s) Manager (Preview)

Select fallback reviewers ⓘ 0 selected
[+ Add fallback reviewers](#)

Azure AD Identity Governance

Entitlement Management

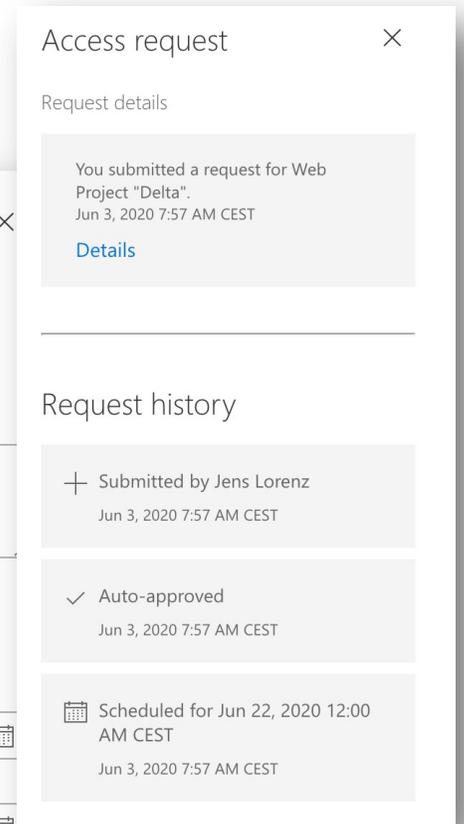
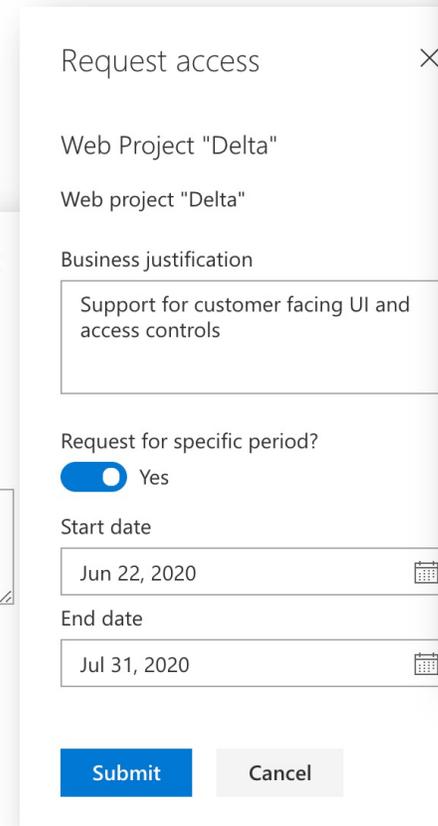
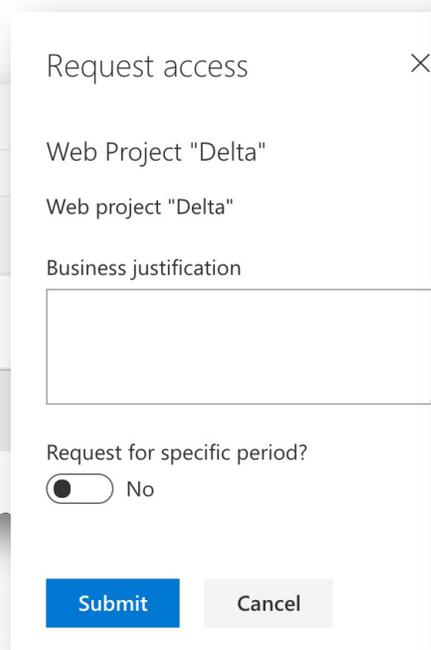
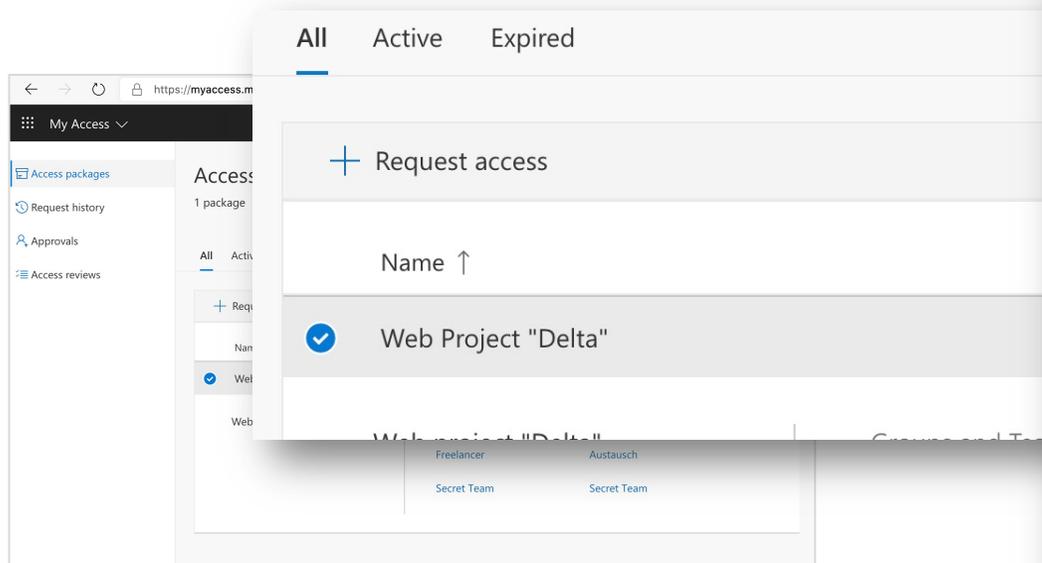
- Sicht des Anfordernden
 - My Access Portal (<https://myaccess.microsoft.com>)
 - Zugriffspakete
 - Historie
 - Genehmigungen
 - Re-Zertifizierungen
 - Organisations-übergreifend
 - Multi-Lingual



Azure AD Identity Governance

Entitlement Management

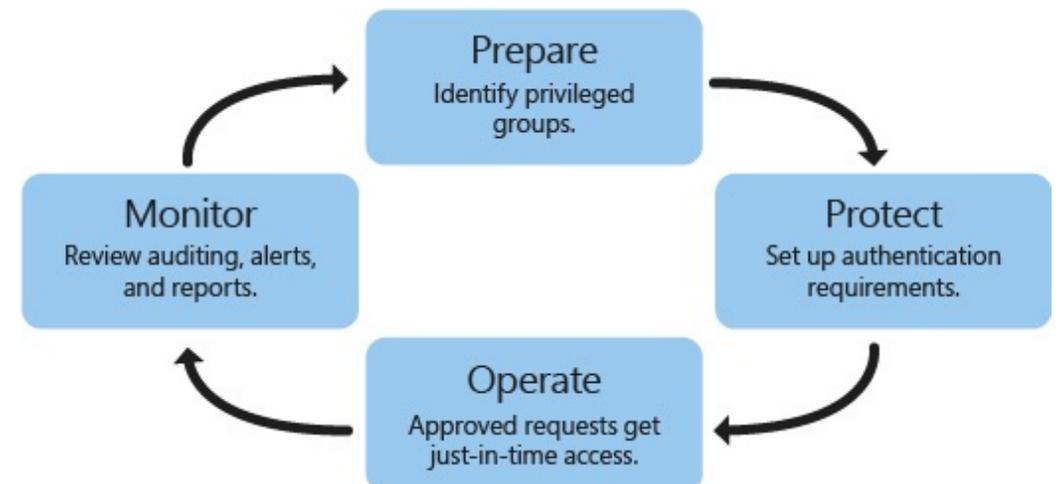
- Sicht des Anfordernden
 - Beispiel: Web Projekt „Delta“



Azure AD Identity Governance

Privileged Identity Management

- „Just-enough-Administration“ (Least Privilege)
 - Dedizierte RBAC Rollen mit definierten Privilegien
- „Just-in-time-Administration“ (Need to Know)
 - Zeitbasierte Zuweisung von privilegierten Rollen
- Genehmigungsprozesse
 - Z.B. „Peer-Review“
- Nachverfolgbarkeit
- Re-Zertifizierung von privilegierten Rollenzuweisungen



Azure AD Identity Governance

Privileged Identity Management

- Privileged Access Groups
 - Definition von privilegierten operativen Rollen in der Organisation
 - Zuweisung von Rollen und Rechten über PAG
 - „Just-in-Time“- und zeitgebundene Zuweisungen
 - Integration in Entitlement Management

The screenshot shows the Azure AD management console for 'noosphere - Azure Active Directory'. The main heading is 'Groups | Privileged access groups (Preview)'. The left sidebar contains navigation options: 'All groups', 'Deleted groups', 'Diagnose and solve problems', 'Settings' (with sub-items: General, Expiration, Naming policy), 'Activity' (with sub-items: Privileged access groups (Preview), Access reviews), and 'Refresh' and 'Activate role' buttons. The main content area displays a list of groups with a search bar and a 'Group type: All' filter. The list includes:

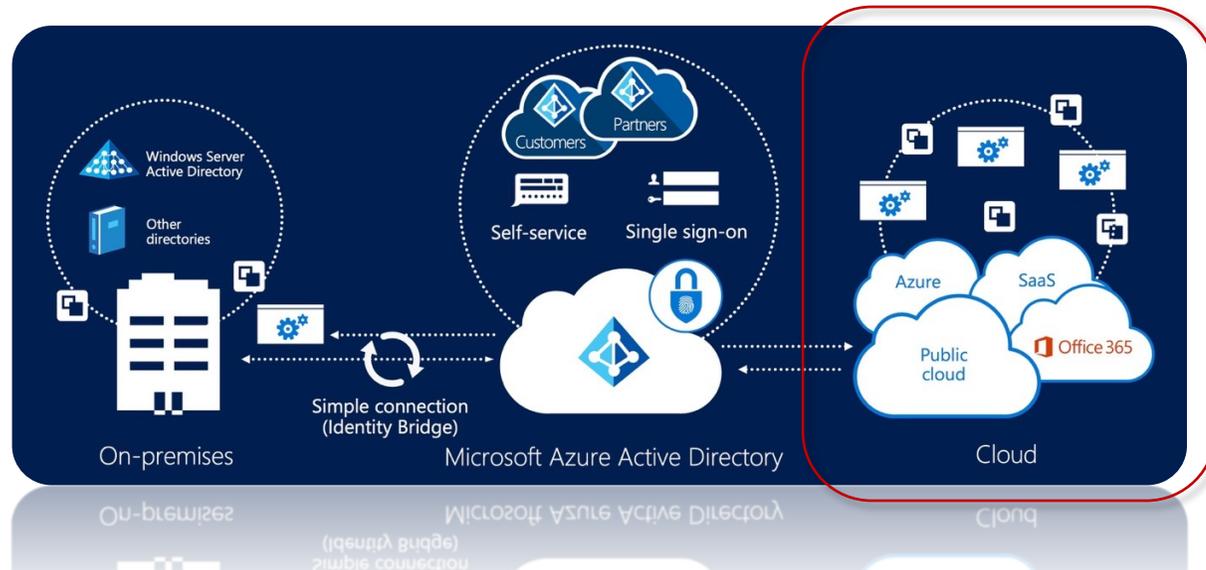
Group
PI PIM-Testgroup
SO Security Operations
MA MDATP Admins
TM Threat Management Operations
MS MGMT-SOC Security Analyst

Azure AD Cloud App Discovery mit Microsoft Cloud App Security

Azure AD Cloud App Discovery

Azure AD als zentraler Identity Provider

- Integration von Cloud Apps
 - Microsoft und Drittanbieter
 - Zentrale Authentifizierung und Autorisierung
 - Integration in Azure AD Conditional Access (Zero-Trust)



Azure / Active Directory / Anwendungsverwaltung / Tutorials für SaaS-Anwendungen

Nach Titel filtern

Tutorials für SaaS-Anwendungen

- > 0-9
- > Ein
- > B
- > C
- > D-E
- > F-G
- > H-I
- > J-K
- > L-M
- > N-O
- > P
- > Q-R
- > E
- > T-V
- > W-Z

Tutorials für die Benutzerbereitstellung

- > 0-9
- > A-F
- > G-M
- > N-S
- > T-Z

Tutorials zur Integration von SaaS-Anwendungen in Azure Active Directory

23.06.2021 • 2 Minuten Lesedauer • 📄 📌

Um Sie bei der Integration Ihrer cloudfähigen SaaS[®]-Anwendungen (Software-as-a-Service) in Azure Active Directory zu unterstützen, haben wir eine Sammlung von Tutorials entwickelt, in denen die Konfiguration erläutert wird.

Eine Liste mit allen in Azure AD integrierten SaaS-Apps finden Sie im [Active Directory-Marketplace](#).

Verwenden Sie das [Anwendungsnetzwerkportal](#), um das Hinzufügen einer SCIM-fähigen Anwendung zum Katalog für die automatische Bereitstellung oder das Hinzufügen einer SAML/OIDC-fähigen Anwendung zum Katalog für einmaliges Anmelden (SSO) anzufordern.

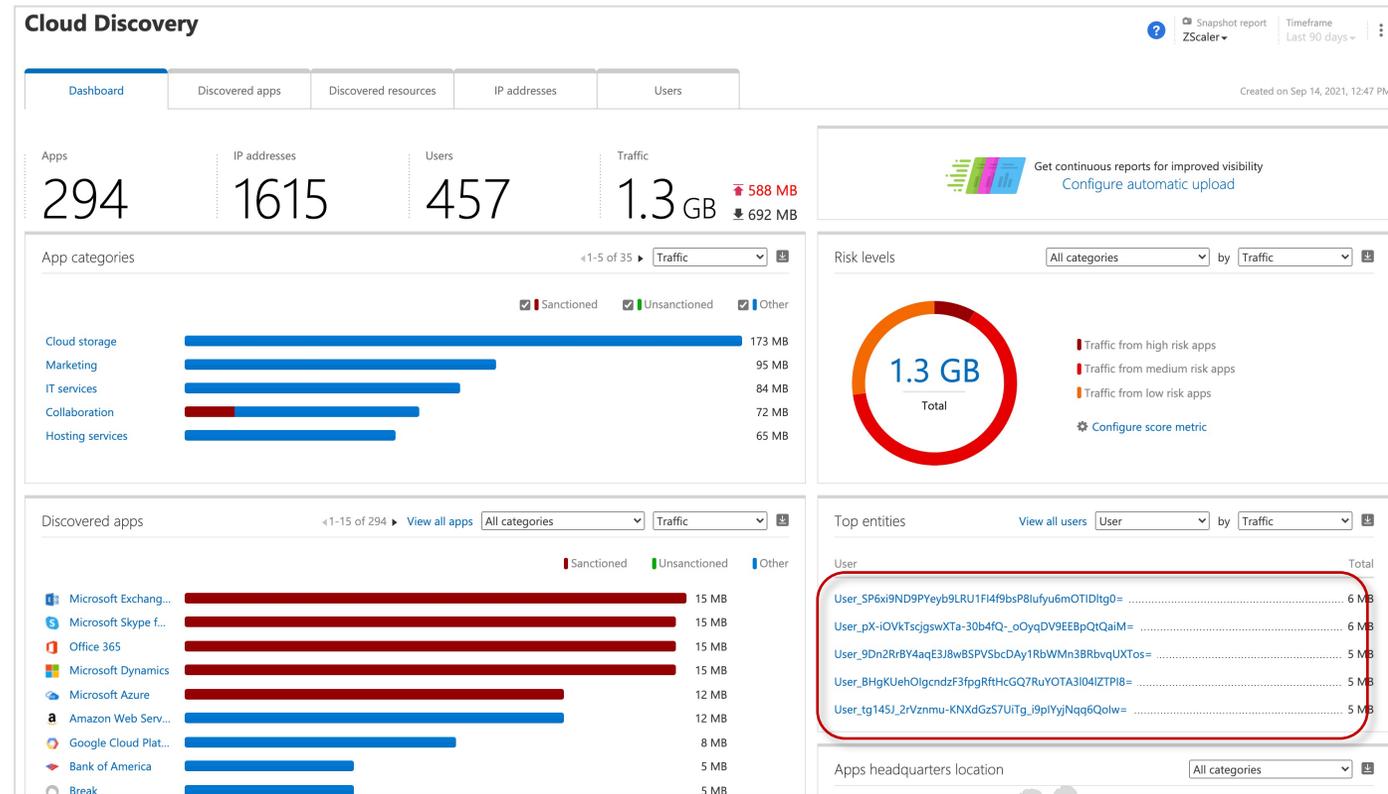
Quicklinks

Logo	Anwendungstutorial für einmaliges Anmelden	Anwendungstutorial für die Benutzerbereitstellung
	Atlassian Cloud	Atlassian Cloud – Benutzerbereitstellung
	ServiceNow	ServiceNow – Benutzerbereitstellung
	Slack	Slack – Benutzerbereitstellung
	SuccessFactors	SuccessFactors – Benutzerbereitstellung
	Workday	Workday – Benutzerbereitstellung

Azure AD Cloud App Discovery

Erfassen und Bewerten von Cloud Apps

- Integration mit Proxy Anbietern
- Integration mit Microsoft Defender for Endpoint
 - Kategorisierung
 - Risikobewertung
- Pseudonomisierung von Benutzerinformationen



Azure AD Cloud App Discovery

Bewertung nach Compliance und Security

- Filtern nach Risiko-Bewertung, Compliance oder Security Faktoren
- Sanktionieren von Apps
 - Verwenden für Data Loss Prevention Funktionen (Microsoft 365 DLP)

The screenshot displays the Azure AD Cloud App Discovery interface. At the top, there are navigation tabs: Dashboard, Discovered apps (selected), Discovered resources, IP addresses, and Users. Below the tabs, there are filters for App tag (Sanctioned, Unsanctioned, None), Risk score (0 to 6), Compliance risk factor (selected), and Security risk factor. A search bar is visible above the app list. The app list includes columns for App, Score, Compliance risk factor, Security risk factor, Users, IP addresses, and Last seen. A dropdown menu is open for the Compliance risk factor, showing a search bar and a list of factors: COBIT, COPPA, FERPA, FFIEC, FINRA, FISMA, GAAP, GAPP, and GDPR. The table shows the following data:

App	Score	Compliance risk factor	Security risk factor	Users	IP addresses	Last seen
Drupal Content management	6					
join.me Online meetings	6					
NetworkSolutions Hosting services	6					
Hootsuite Marketing	6					
Pandora Radio	6	4 MB	2 MB	12	12	9

Azure AD Cloud App Discovery

Bewertung nach Compliance und Security

- Filtern nach spezifischen Risiken (z.B. Datenpannen)
 - Automatische Alarmierungen

T-Mobile
Communications

5 4 MB 2 MB 12 12

T-Mobile is redefining the way consumers and businesses buy wireless services.

8 GENERAL

Category: Communications Headquarters: Germany Data center: United Kingdom
Founded: 1995 Holding: Public Domain: [*t-mobile.com](https://t-mobile.com)
Domain registration: Jan 13, 2000 Consumer popularity: 10 Privacy policy: t-mobile.com/privacy-cen...
Vendor: Deutsche Telekom Data types: 3 Documents, Media files, ... Disaster Recovery Plan

6 SECURITY

Latest breach: Aug 18, 2021 Data-at-rest encryption method: Not sup... Multi-factor authentication

✓ User audit trail ✗ Admin audit trail ✗ Data audit trail

Save as

Security risk factor Latest breach after (date/time) 01/01/2021

+ Add a filter

Browse by category:

Search for category...

Communications 1
Hosting services 1

Bulk selection Hide category panel + New policy from search Export

1 - 2 of 2 discovered

App	Score	Traffic	Upload	Transactio...	Users	IP
DigitalOcean Hosting services	7	3 MB	2 MB	10	10	8
T-Mobile Communications	5	4 MB	2 MB	12	12	7

Azure AD Cloud App Discovery

Anpassung an die Anforderungen der Organisation

- Gewichtung in den Bewertungen
- Relevanz von Compliance Anforderungen

Score metrics

Configure your own preferences and priorities for each app property to customize the calculation of discovered app scores.

General

Field	Importance
Founded The year in which the provider was founded.	Medium (x2)
Holding Displays whether the provider is a publicly or privately held company.	Medium (x2)
Domain registration The date on which the domain was registered.	Medium (x2)
Consumer popularity Popularity of this app among SaaS users world-wide. A high score indicates a popular app with high-use rates.	Medium (x2)
Disaster Recovery Plan Does the app support Disaster Recovery Plan, which includes a backup and restore strategy?	Medium (x2)

Security

Field	Importance
Data-at-rest encryption method The type of encryption of data-at-rest performed on the app.	Medium (x2)

Compliance Category importance: Medium (x2)

Field	Importance	N/A values <input type="checkbox"/>
FINRA Does this app comply with FINRA, a standard set by a non-profit organization authorized by the US Congress to regulate and enforce the protection of investors and safeguard market integrity?	Ignored (x0)	<input checked="" type="checkbox"/> Exclude N/As
FISMA Does this app comply with FISMA, the US legislation that defines a comprehensive framework to protect government information, operations and assets within federal agencies, against threats?	Ignored (x0)	<input checked="" type="checkbox"/> Exclude N/As
GAAP Does this app comply with GAAP, a collection of commonly-followed accounting rules and standards for financial reporting?	Low (x1)	<input checked="" type="checkbox"/> Exclude N/As
HIPAA Does this app comply with HIPAA, the US legislation that sets standards for protecting the confidentiality and security of individually identifiable health information?	Ignored (x0)	<input checked="" type="checkbox"/> Exclude N/As
ISAE 3402 Does this app comply with ISAE 3402, the global standard providing assurance that a service organization has appropriate controls in place?	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As
ISO 27001 Is this app ISO 27001 certified, a certificate given to companies upholding internationally recognized guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization?	High (x4)	<input checked="" type="checkbox"/> Exclude N/As
ITAR Does this app comply with ITAR, regulations controlling the export and import of defense-related articles and services found on the US Munitions List?	Low (x1)	<input checked="" type="checkbox"/> Exclude N/As
SOC 1 Does this app comply with SOC 1, reporting on controls at a service organization which are relevant to user entities' internal control over financial reporting?	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As

Webinar-Reihe „Compliance mit IT“

Nachfolgende Webinare:

- Mittwoch, 27.10.2021: *Datenmanagement im Kontext Compliance* ([Anmelden](#))
- Mittwoch, 24.11.2021: *Adressieren von Insider-Risiken* ([Anmelden](#))

Vielen Dank!

Jens Lorenz

Strategic Consultant, CISSP, CSSP, CIPT

mail: jens.lorenz@sits-d.de

fon: +49-170-4516565

LinkedIn: <https://de.linkedin.com/in/jenslorenz>

