Priviledged Identity Management in der Praxis

Christian Decker

Wer bin ich?

- Seit über 30 Jahren in der IT-Branche
- Seit 2017 bei ACP als Cloud Architekt
- Immer mit dem Mehrwert von IT-Lösungen für Menschen beschäftigt
- Autor von https://derdecker.at
- Moderator der LinkedIn Gruppe Microsoft Conditional Access
- Seit März 23 erster Security MVP in Österreich

Wovon lebe ich?

- Begleitung von Unternehmen zu M365 in folgenden Bereichen:
  - Governance
  - Security
  - Datenschutz
  - User Adoption
- Entwicklung von Standards für M365 innerhalb der ACP-Gruppe

Und sonst?

CEO (Chief Entertainment Officer) des VIP-Zeltes beim Red Bull Erzberg-Rodeo seit über 10 Jahren

DISCLAIMER

- Das Admin-Konzept folgt nicht den Prinzipien des least privileged Access, sondern einem praxistauglichen, täglich anwendbaren Rollenkonzeptes in M365

- Die hier vorgeschlagenen Rollenkonzepte beziehen sich auf normale Admin Tätigkeiten in Microsoft 365 – Azure wird hier nicht mit berücksichtigt (kann aber natürlich in das Konzept eingegliedert werden)

Grundsätzliches zu Admin-Accounts

- Der normale Benutzeraccount sollte IMMER getrennt sein von einem Account mit erhöhten Berechtigungen
- Ein OnPrem Account mit erhöhten Berechtigungen sollte in der Cloud keine erhöhten Berechtigungen haben
- Option 1:
  zusätzlichen Account OnPrem anlegen, zu M365 synchronisieren und dort mit Berechtigungen versehen
- Option 2:
  Cloud Only Accounts mit erhöhten Berechtigungen anlegen
- Empfehlung: Option 2
  (Voraussetzung: der Life-Cycle für diese Accounts ist gewährleistet!)

Authentifizierung von Admins

- Zweiter Faktor steht außer Diskussion
- Neuerliche Anmeldung zumindest alle 10 Stunden
- Keine persistent Sessions im Browser

- Folgende Vorgehensweisen sind empfohlen
  - alle Adminrollen nur mit FIDO-Key erlauben
  - Adminzugriffe nur von einem domain joined Windows PC
  - Adminzugriffe nur aus Österreich/Deutschland

Glass Break Admin

- Es sollte zumindest einen Glass Break Admin geben
- Cloud Only Account mit der Rolle „Globaler Administrator“
  - Kein PW-Ablauf, kein zweiter Faktor
  - Wird in jeder Conditional Access Policy ausgenommen
- Komplexes, zufälliges Passwort
  - Ausschließlich AUSGEDRUCKT in einem versiegelten Kuvert
  - Achten auf „lesbare“ Zeichen (dh kein kleines l oder großes I, kein 0 oder O, …)
- JEDE Aktion mit diesem User muss einen Alert auslösen!
  - Erfolgreiche, aber auch nicht erfolgreiche Anmeldungen
  - Passwort-Wechsel
- Regelmässig (4 x Jahr) Anmelden, danach PW wechseln und Alerts testen
- NIEMALS nutzen (außer im Notfall, wenn nichts anderes mehr geht)

Rollen in Microsoft 365

https://docs.microsoft.com/en-US/microsoft-365/admin/add-users/about-admin-roles?WT.mc_id=365AdminCSH_inproduct

- Rollenverwaltung im M365 Admin Portal Role assignments - Microsoft 365 admin center
- Umfangreiche Rollen in M365 vorhanden
- Vergleich von Rollen leicht möglich
- ein Benutzer sollte keine Rolle haben, die in einer anderen Rolle integriert ist

3 besonders heikle Rollen

- **Globaler Administrator**
- Hat (nahezu) alle Berechtigungen im Tenant

- **Privileged Role Admininstrator**
- Managed alle Funktionen in Privileged Identity Management

- **eDiscovery Manager bzw eDiscovery Admin**
- Hat im Zuge von eDiscovery die Möglichkeit, auf ALLE Daten im Tenant zuzugreifen
- Kann nicht über PIM verwaltet werden

- **Empfehlung**:
- Keine permanente aktive Zuweisung dieser Rollen
- 4 Augen Prinzip bei der Aktivierung dieser Rollen

Wichtige Rollen

Applikations- und Sicherheitsrollen

Exchange Admin

- Users with this role have global permissions within Microsoft Exchange Online, when the service is present.

SharePoint Admin

- Users with this role have global permissions within Microsoft SharePoint Online, when the service is present, as well as the ability to manage support tickets and monitor service health.

Teams Admin

- Users in this role can manage all aspects of the Microsoft Teams workload via the Microsoft Teams & Skype for Business admin center and the respective PowerShell modules. This includes, among other areas, all management tools related to telephony, messaging, meetings, and the teams themselves. This role also grants the ability to manage O365 groups.

Yammer Admin

- Users with this role have global permissions within Yammer, when the service is present, as well as the ability to create and manage all Microsoft 365 groups, manage support tickets, and monitor service health.

Intune Admin

- Users with this role have global permissions within Microsoft Intune Online, when the service is present. Additionally, this role contains the ability to manage users and devices in order to associate policy, as well as create and manage groups

Office Apps Administrator

- Users in this role can manage Office 365 apps cloud settings. This includes managing cloud policies, self-service download management and the ability to view Office apps related report. This role additionally grants the ability to manage support tickets, and monitor service health within the main admin center. Users assigned to this role can also manage

Wichtige Rollen

Applikations- und Sicherheitsrollen

Globale Reader

- Users with this role can read everything that a Global Administrator can, but not update anything.

User Admin

- Users with this role can create and manage all aspects of users and groups. Additionally, this role includes the ability to manage support tickets and monitors service health. Some restrictions apply. For example, this role does not allow deleting a global administrator. User Account administrators can change passwords for users, Helpdesk administrators, and other User Account administrators only

(Cloud) Device Admin

- Users in this role can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device

Billing Admin

- Makes purchases, manages subscriptions, manages support tickets, and monitors service health.

Security Admin

- Users with this role have all of the read-only permissions of the Security reader role, plus the ability to manage configuration for security-related services: Azure Active Directory Identity Protection, Azure Information Protection, Privileged Identity Management, and Office 365 Security & Compliance Center.

Hybrid Identity Admin

- Users in this role can create, manage, and deploy provisioning configuration setup from AD to Azure AD using Cloud Provisioning as well as manage federation settings. Users can also troubleshoot and monitor logs using this role.

Wichtige Rollen

Applikations- und Sicherheitsrollen

External Identity Provider Admin

- This administrator manages federation between Azure Active Directory tenants and external identity providers. With this role, users can add new identity providers and configure all available settings (e.g. authentication path, service id, assigned key containers). This user can enable the tenant to trust authentications from external identity providers.

Authentication Policy Admin

- Users in this role can create, deploy, and maintain password protection policies and configure authentication methods in a tenant. An Authentication policy administrator can perform the following tasks - manage authentication method settings; configure smart lockout settings; manage a custom banned password list. Users in this role cannot set, change, or reset any individual users' registered authentication methods. This role is intended for managing policy rather than managing users. For example, an Authentication policy administrator will be able to configure that passwords are required to be registered, and the lockout policy for those passwords, but will not be able to reset a user's password.

Privileged Authentication Admin

- Users with this role can view the current authentication method information and set or reset non-password credentials for all users, including global administrators. Privileged Authentication Administrators can force users to re-register against existing non-password credential (e.g. MFA, FIDO) and revoke 'remember MFA on the device', prompting for MFA on the next login of all users.

Application Admin

- Users in this role can add, manage, and configure enterprise applications, app registrations and manage on-premises like app proxy.

Compliance Admin

- Users with this role have management permissions within in the Office 365 Security & Compliance Center and Exchange Admin Center.

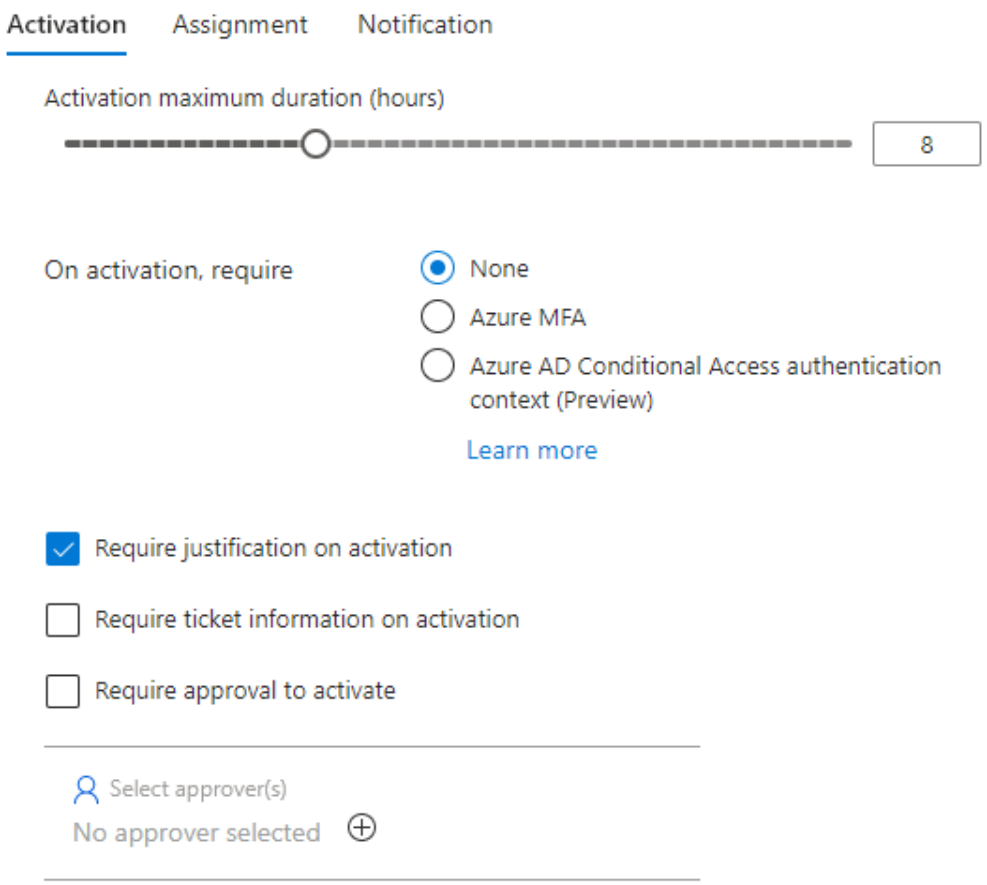
Wichtige Rollen

Applikations- und Sicherheitsrollen

Exchange Admin	Admin für Office Apps	Billing Admin	Privileged Authentication Admin
SharePoint Admin	Globale Reader	Security Admin	Application Admin
Teams Admin	User Admin	Hybrid Identity Admin	Compliance Admin
Viva Engage Admin	Microsoft Entra Joined	External Identity Provider Admin	Device Local Admin
Intune Admin			

Konfiguration von Rollen

Für jede Rolle können folgende Optionen definiert werden



Wie lange kann die Rolle aktiviert werden

Was benötigt der Benutzer bei Aktivierung

Wird eine Begründung für die Aktivierung verlangt (Textfeld)

Wird ein Ticket für die Aktivierung verlangt

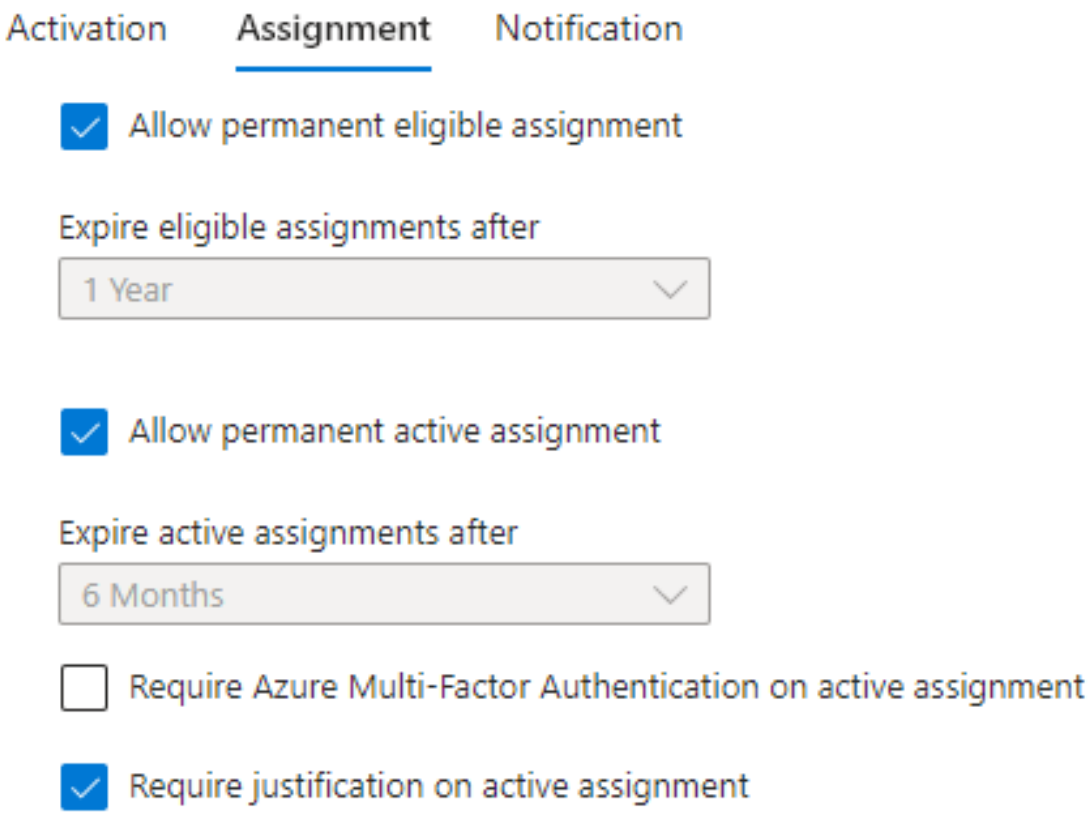
- 2 Textfelder:
  - Ticketsystem
  - Ticketnummer
- Achtung: keine Verifizierung!

Wird ein Approval benötigt ?

- Approver benötigt keine Admin-Rollen

Konfiguration von Rollen

Für jede Rolle können folgende Optionen definiert werden



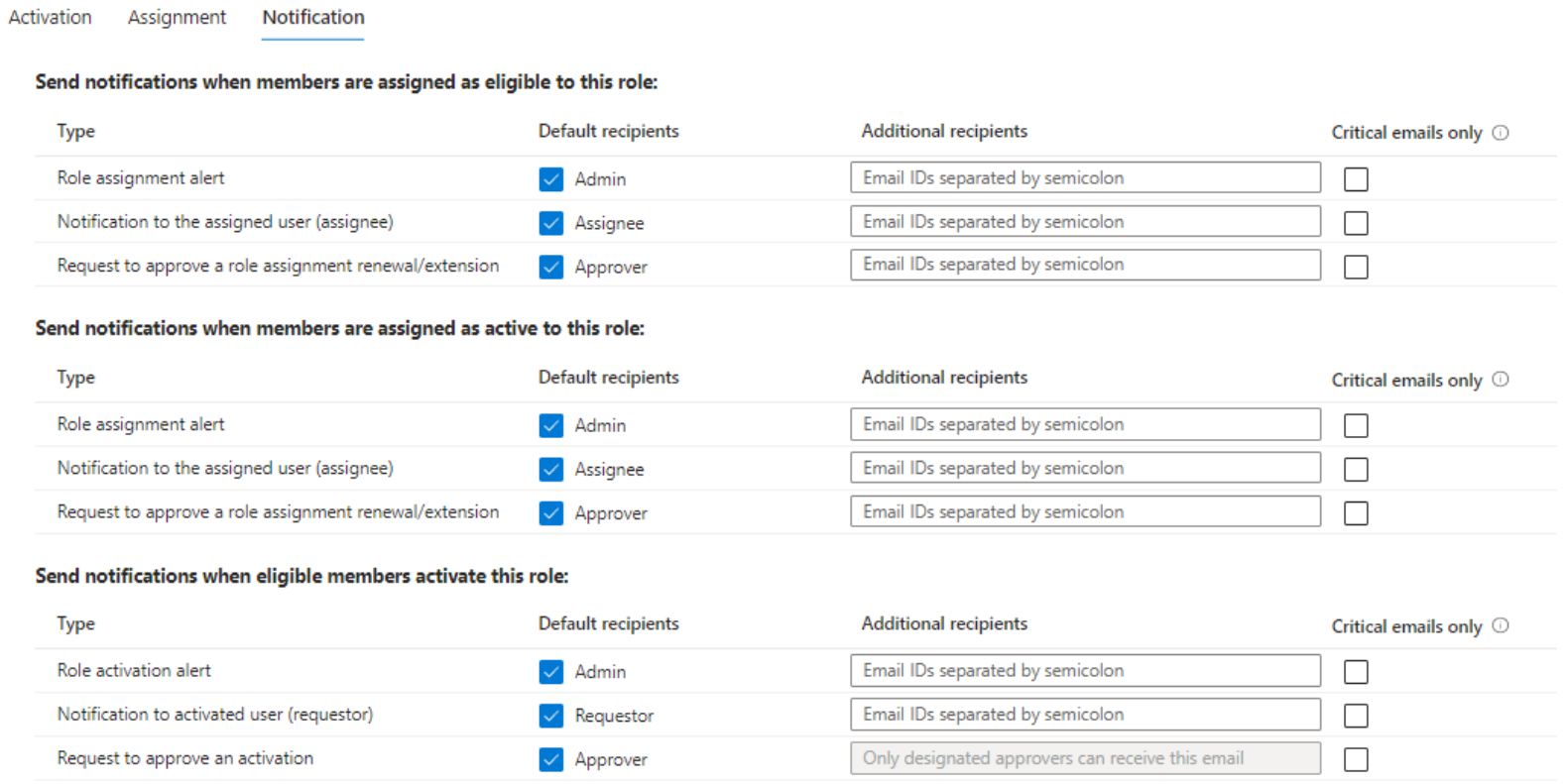
ELIGIBLE
User kann die Rolle aktivieren

ACTIVE
User besitzt die Rolle

EXPIRE
Nach diesem Zeitraum muss die Zuweisung zur Rolle neu aktiviert werden

Konfiguration von Rollen

Für jede Rolle können folgende Optionen definiert werden



Notifizierung

- Assign Members as eligible
- Assign members as active
- Member activate Role

Empfänger (default)

- Admin
- Assigner
- Approver

Konfiguration von Gruppen

- Rollen können einer (neu erstellten) Gruppe zugewiesen werden (Eligible und Active)
- Gruppen können Besitzer und/oder Mitglieder haben
- Besitzer können Mitglieder der Rolle zuweisen
- Zuweisung kann Eligible oder Active sein
- Zuweisung kann ablaufen

Konfiguration von Gruppen

Anlage der Gruppe

- Gruppe muss im AzureAD neu erstellt werden
  - Muss Security Gruppe sein
  - „Azure AD roles can be assigned to the group“ muss aktiviert sein
  - Membership type muss „Assigned“ sein

- Diese Gruppe kann nur von einem globalen Administrator administriert werden

- Owner und Member sollten über PIM verwaltet werden!
- Wenn Gruppe mehrere Rollen zugeordnet werden sollen, können die hier zugewiesen werden

Konfiguration von Gruppen

Demo

Adele – steigt auf https://aka.ms/myroles ein

Verwalten, Gruppen, PIM_Helpdesk

Verwalten Rollen, Zuweisung hinzufügen

Rolle: Member, Mitglied(er) auswählen (Alex Wilber)

Zuweisungstyp: Berechtigt

Adele hat als Owner KEINE besonderen Adminrollen!
(Könnte sich aber als Member hinzufügen!)

Alex – steigt auf https://aka.ms/myroles ein

Meine Rollen, Gruppen, berechtigte Zuweisungen

- Aktivieren

Alex hat dann alle zugewiesnene Rollen

Global Admin und Privilege Admin Role

- Berechtige Accounts werden über PIM zugeordnet
- Aktivierung dieser Rolle erfordert Approval
  - Achtung: Approval darf nur nach Nachfrage der Aktivierung erfolgen!
- Aktivierung für 1 Stunde
- Aktivierung benötigt MFA

- Nutzung nur, wenn wirklich notwendig!

Gruppe „Global-Work-Admin“

Für die Admins, die die M365 Admintätigkeiten durchführen im Tenant,
Gibt es Service-spezifische Rollen, kann auf dieser Basis eine Service-Gruppe definiert werden

- Erstellen einer Gruppe im EntraID „Global-Work-Admin“
- Zuweisung dieser Rollen zu dieser Gruppe:
  Exchange Admin, SharePoint Admin, Teams Admin, Yammer Admin, Intune Admin, Admin für Office Apps, Globale Reader, User Admin, Device Admin, Billing Admin, Security Admin, Hybrid Identity Admin, External Identity Provider Admin, Authentication Policy Admin, Privileged Authentication Admin, Application Admin, Compliance Admin
- Zuweisung des eligible OWNERS über PIM (IT-Leiter)
- Zuweisung der eligible Member über PIM durch OWNER

- Zuweisung der Member endet nach 6 Monaten

- Aktivierung für 2 Stunden (Diskussionsbasis – max. 10 Stunden!)
- Begründung notwendig
- MFA immer notwendig

Gruppe „Read Only Admin“

Für alle Admin-Rollen. Oft reicht der Read-Only Zugang um Dinge kontrollieren zu können oder Fehler suchen zu können

- Erstellen einer Gruppe im EntraID „ReadOnly Admin“
- Zuweisung folgender Rollen zu dieser Gruppe: Global Reader, Security Reader

- Zuweisung des eligible OWNERS über PIM (IT-Leiter)
- Zuweisung der eligible Member über PIM durch OWNER

- Zuweisung der Member endet nach 6 Monaten

- Aktivierung für 10 Stunden
- MFA notwendig

Gruppe „Helpdesk“

Für MitarbeiterInnen im First Level Helpdesk

- Erstellen einer Gruppe im EntraID „Helpdesk“
- Zuweisung dieser Rollen zu dieser Gruppe: Authentication Administrator, Global Reader, User Admin, Help Desk

- Zuweisung des eligible OWNERS über PIM (Helpdesk Leitung)
- Zuweisung der eligible Member über PIM durch OWNER

- Zuweisung der Member endet nach 6 Monaten

- Aktivierung für 10 Stunden
- MFA notwendig

Absichern von PIM

- Jede Aktivierung soll verpflichtend MFA erfordern
  - Geht nicht out of the box, wenn User schon gültigen MFA Token hat
- Entra ID > Security > Conditional Access > Authentication Context > New
- RequireReAuth – Publish to Apps
- Neue CondAcc Regel:
- All Users, Target resource: Authentication context „requireReAuth“, Session: Sign-In Frequency Every Time
- In PIM bei Edit Role/Group Setting:
- On activation, require „Microsoft Entra Conditional Access authentication context – RequireReAuth“

[A new, must-have Conditional Access policy – 365 by Thijs]

Anmerkungen

- Ein Gruppenbesitzer ist kein Gruppenmitglied.
  ABER: Ein Gruppenbesitzer kann sich selber zum Gruppenmitglied machen