

SECURITY & COMPLIANCE

Erweiterte Security-Administrator-Rolle in Entra für schnellere Incident-Response

Executive Summary

Microsoft baut die eingebaute Rolle Security Administrator in Microsoft Entra ID um vier Aktionen aus, die bisher der Identitätsverwaltung vorbehalten waren: Benutzer deaktivieren, Benutzer wieder aktivieren, alle Refresh-Token widerrufen und Kennwörter zurücksetzen. Aus 82 Directory-Actions werden 86. Der Rollout läuft seit August 2026 und ist bis Ende September 2026 in allen Tenants abgeschlossen. Du musst dafür nichts tun – und genau das ist der Punkt, an dem es interessant wird.

Klingt nach einer Fußnote in den Release Notes. Ist es nicht. Die Änderung verschiebt die Grenze zwischen „wir wissen, dass das Konto kompromittiert ist“ und „wir haben etwas dagegen getan“. In genau dieser Lücke passieren die teuren Dinge: die Weiterleitungsregel im Postfach, der Rundbrief an die Kreditorenbuchhaltung, der OneDrive-Export um 03:47 Uhr. Wer die Lücke von zwei Stunden auf zwei Minuten drückt, hat mehr für die Sicherheit getan als mit dem nächsten Awareness-Video.

Der Haken: Security Administrator war schon vorher keine Kuschelrolle, und jetzt hat sie zusätzlich einen Knopf, der Konten stilllegt. Wer die Rolle bisher großzügig als „Lesezugriff fürs Security-Reporting“ verteilt hat, verteilt ab sofort etwas anderes. Die Hausaufgabe für die nächsten Wochen heißt deshalb nicht „neue Rechte aktivieren“, sondern „alte Zuweisungen aufräumen“.

FAKTEN: Was sich technisch ändert

Der Rolle Security Administrator (Template-ID 194ae4cb-b126-40b2-bd5b-6091b380977d) werden die Actions `microsoft.directory/users/disable`, `users/enable`, `users/invalidateAllRefreshTokens` und `users/password/update` hinzugefügt. Alle vier sind in Entra als privileged gekennzeichnet. Sie wirken ausschließlich auf nicht administrative Benutzerkonten.

Worum geht es im Detail?

Bis heute ist die Arbeitsteilung in den meisten Tenants absurd: Das SOC sieht in Entra ID Protection, in Defender XDR und in Sentinel haargenau, was passiert. Es sieht den Sign-in aus Lagos, den Token-Replay, die frisch registrierte MFA-Methode. Und dann darf es ... ein Ticket schreiben. Denn die Aktionen, die den Angreifer tatsächlich stoppen, hängen an ganz anderen Rollen: User Administrator, Helpdesk Administrator, Authentication Administrator oder Privileged Authentication Administrator. Das Ergebnis ist eine Organisation, die den Brand in Echtzeit sieht und den Feuerlöscher per Laufzettel anfordert.

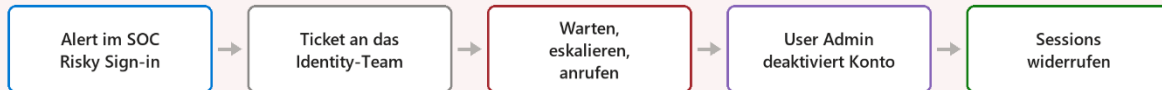
Genau diese Trennung räumt Microsoft jetzt ab. Die vier neuen Actions decken die drei Handgriffe ab, mit denen jedes Identitäts-Playbook der Welt beginnt. Erstens: das Konto deaktivieren, damit kein neuer Token mehr ausgestellt wird. Zweitens: alle Refresh-Token invalidieren, damit die bereits laufenden Sitzungen nicht einfach weiterlaufen. Drittens: das Kennwort zurücksetzen, damit der Angreifer mit den gestohlenen Zugangsdaten nichts mehr anfangen kann. Die vierte Action ist das Gegenstück zur ersten – Benutzer wieder aktivieren –, und sie ist wichtiger, als sie

aussieht. Ohne sie kann das SOC nur kaputtmachen, nicht reparieren, und jeder Fehlalarm würde erneut ein Ticket auslösen.

Die Containment-Kette: wer drückt eigentlich den Knopf?

Bis zum Rollout: Ticket-Ping-Pong

Der Analyst sieht alles, darf aber nichts. Also wandert der Vorfall durch die Organisation.



Zeit bis Containment: 30 Minuten bis mehrere Stunden – nachts gern auch bis zum Frühstück

Ab Ende September 2026: der Analyst handelt selbst

Vier neue Actions in der Rolle Security Administrator – der Umweg entfällt.



Zeit bis Containment: Minuten – CAE meldet das kritische Ereignis nahezu in Echtzeit, bis zu 15 Min. Laufzeit

Skizze: boddenberg.de – Consulting Briefing

Skizze 1: Der Weg vom Alarm zur Eindämmung – vorher und nachher.

Der zweite Punkt – das Widerrufen der Sitzungen – ist der, den Praktiker am häufigsten unterschätzen. Ein Kennwortwechsel allein räumt bestehende Browser-Sitzungen nicht zuverlässig ab; der Angreifer sitzt weiter im Postfach, während der Benutzer schon brav sein neues Kennwort tippt. Erst das Invalidieren der Refresh-Token schiebt den Riegel vor. Seit Februar 2026 hat Microsoft dafür auch im Entra Admin Center aufgeräumt: Aus den beiden verwirrend nebeneinander stehenden Schaltflächen – die eine wirkte nur auf die veraltete Per-User-MFA – ist eine einzige Schaltfläche „Revoke sessions“ geworden, die dasselbe tut wie das Cmdlet `Revoke-MgUserSignInSession`.

Wie schnell das wirkt, entscheidet nicht Entra allein, sondern Continuous Access Evaluation. CAE abonniert kritische Ereignisse – Konto deaktiviert oder gelöscht, Kennwort geändert oder zurückgesetzt, MFA aktiviert, Administrator widerruft alle Refresh-Token, hohes Benutzerrisiko erkannt – und schiebt sie an Exchange Online, SharePoint Online und Teams. Die Dienste werfen den Zugriff dann nahezu in Echtzeit weg, dokumentiert sind bis zu 15 Minuten Laufzeit. Ohne CAE hängst du am regulären Ablauf des Access Token, und der ist in CAE-fähigen Sitzungen inzwischen bis zu 28 Stunden lang. Das ist kein Detail, das ist der Unterschied zwischen Eindämmung und Zuschauen.

WARNUNG: Gastkonten sind nicht dabei

CAE unterstützt keine Gastbenutzer. Widerrufereignisse und IP-basierte Richtlinien greifen dort nicht sofort. Bei einem kompromittierten Gastkonto aus der Lieferkette hilft dir der schöne neue Knopf also deutlich langsamer als beim eigenen Personal – und Lieferkette ist erfahrungsgemäß genau der Weg, den der Angreifer nimmt.

Die Rolle Security Administrator steht dabei nicht allein. Microsoft hat im Sommer 2026 zwei weitere Bausteine geliefert, und wer Least Privilege ernst meint, sollte den Unterschied kennen. Der Entra SOC Identity Responder ist die chirurgische Variante: eine schmale Rolle, die genau diese Eindämmungsaktionen kann und sonst nichts – dafür aber auf administrative Einheiten einschränkbar ist. Der Security Operator hat die Aktionen ebenfalls bekommen und bringt zusätzlich die Risiko-Workflows aus ID Protection mit. Und der Security Administrator ist der breite Alleskönner, der jetzt eben auch eindämmen darf.

Rolle	Kann eindämmen	Was sonst noch drin ist	Auf AU einschränkbar	Typischer Einsatz
Security Administrator	Ja, ab Ende Sept. 2026	Breite Security-Konfiguration: Richtlinien, DLP, Threat Intelligence, Federation, Password-Hash-Sync	Nein	Security-Leitung, wenige Köpfe
Entra SOC Identity Responder	Ja, seit Sommer 2026	Nichts. Genau drei bis vier Actions.	Ja	SOC-Analysten im Schichtbetrieb
Security Operator	Ja	Risky Users bestätigen und verwerfen, Sign-in- und Audit-Logs, Security & Compliance Center	Nein	Level-2-Analyse mit Risikofreigabe
User Administrator	Ja, klassisch	Vollständige Benutzerverwaltung inklusive Anlegen und Löschen	Ja	IT-Betrieb, nicht das SOC

WICHTIG: „Ohne privilegierte Rollen“ stimmt so nicht ganz

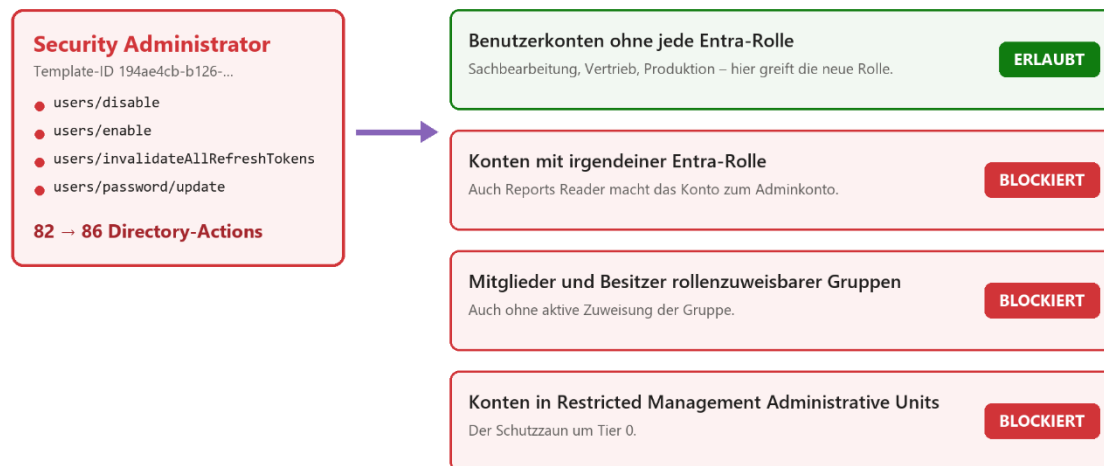
In der Ankündigung liest es sich, als käme das SOC nun ohne privilegierte Rollen aus. Tatsächlich trägt Security Administrator in Entra selbst das Kennzeichen PRIVILEGED, und die vier neuen Actions sind ebenfalls als privilegiert markiert. Richtig ist: Du brauchst keine zusätzliche Rolle mehr. Du brauchst aber weiterhin PIM, Access Reviews und ein wachsames Auge auf die Zuweisungsliste.

Was sind Chancen? Was sind Risiken?

Die größte Chance ist banal und wird trotzdem regelmäßig übersehen: Du sparst eine Organisationsgrenze. Jede Übergabe zwischen zwei Teams kostet in der Praxis nicht Minuten, sondern Viertelstunden – Ticket schreiben, Priorität verhandeln, Rückfrage beantworten, Rufbereitschaft wecken. Ein Kunde aus der Fertigung hat mir seine Zahlen gezeigt: Erkennung im Schnitt nach vier Minuten, Eindämmung nach 152 Minuten. Dazwischen lag ausschließlich Verwaltung. Die Erkennung war nie das Problem.

Die zweite Chance ist die Automatisierung. Wenn die Rolle, unter der deine Playbooks laufen, die Eindämmungsaktionen selbst besitzt, brauchst du kein Dienstkonto mehr, das mit User Administrator ausgestattet in einer Automatisierung schlummert und dort seit drei Jahren niemandem auffällt. Solche Konten sind das Lieblingsziel jedes Angreifers, der es über den ersten Sprung hinaus geschafft hat. Weniger stehende Berechtigung ist immer ein Gewinn, auch wenn sie an einer anderen Stelle wieder auftaucht.

Wie weit reicht der neue Knopf? Die Grenzen der Rolle



Merksatz für das Runbook

Der Angreifer, der dir wirklich weh tut, sitzt am Ende auf einem Adminkonto – und genau da hört die neue Rolle auf. Für Tier-0-Containment brauchst du weiterhin Privileged Authentication Administrator oder Global Administrator, sauber über PIM als Just-in-Time-Aktivierung mit Genehmigung und Begründung.

Skizze: boddenberg.de – Consulting Briefing

Skizze 2: Auf welche Konten die neuen Aktionen wirken – und auf welche nicht.

Damit sind wir beim ersten Risiko, und es ist ein hartes. Die neuen Aktionen wirken ausschließlich auf nicht administrative Konten. Das steht so in der Dokumentation, und es gilt für Security Administrator, Security Operator und Entra SOC Identity Responder gleichermaßen. Konten mit irgendeiner Entra-Rolle sind tabu. Mitglieder und Besitzer rollenzuweisbarer Gruppen sind tabu. Konten in einer Restricted Management Administrative Unit sind tabu. Der Angreifer, der dir wirklich schadet, hat sich aber genau dorthin hochgearbeitet. Wenn dein Runbook nicht sauber unterscheidet, steht der Analyst um vier Uhr morgens vor einer ausgegrauten Schaltfläche und fängt an zu improvisieren. Improvisation um vier Uhr morgens ist die teuerste Betriebsart, die es gibt.

Das zweite Risiko heißt Rollenhygiene. Security Administrator ist historisch gewachsen und ziemlich fett: Die Rolle darf die Federation-Eigenschaft von Domains ändern, sie darf die Password-Hash-Synchronisierung in Entra Connect verwalten, sie liest BitLocker-Wiederherstellungsschlüssel und LAPS-Kennwörter. Wer diese Rolle hat, ist bereits nahe am Kontrollpunkt der Identität. Jetzt kommt die Fähigkeit dazu, beliebige Nicht-Adminkonten stillzulegen. In vielen Tenants sitzen auf dieser Rolle zwölf bis zwanzig Personen, weil sie irgendwann als „Darf ins Security-Portal schauen“ verteilt wurde. Das war schon vorher falsch. Ab Ende September ist es auch operativ gefährlich.

WARNUNG: Denial of Service durch Fehlbedienung

Ein Analyst mit dieser Rolle kann in wenigen Minuten die halbe Buchhaltung aussperren – versehentlich, übermüdet oder weil ein Skript eine Liste falsch herum sortiert hat. Und das Zurückdrehen dauert länger als das Sperren: Nach dem Wiederaktivieren braucht SharePoint Online und Teams typischerweise rund 15 Minuten, Exchange Online 35 bis 40 Minuten, bis das Konto in den nachgelagerten Diensten wieder als aktiv gilt. Plane diese Asymmetrie in dein Runbook ein, bevor du sie im Ernstfall lernst.

Chance	Wofür sie zählt	Risiko auf der Gegenseite
Mean Time to Contain sinkt deutlich	Weniger Datenabfluss, weniger Folgeschaden, bessere Position gegenüber Aufsicht und Versicherung	Falsch-positive Sperrungen treffen produktive Abläufe sofort
Weniger stehende privilegierte Zuweisungen	Least-Privilege-Design wird endlich abbildbar statt nur behauptet	Die Berechtigung wandert nur in eine andere, ebenfalls privilegierte Rolle
Playbooks in Sentinel und Defender werden einfacher	Keine Sonderdienstkonten mit User Administrator mehr nötig	Automatisierte Massenaktion ohne Vier-Augen-Prinzip
Klare Zuständigkeit im Schichtbetrieb	Der Analyst, der den Alarm sieht, drückt den Knopf	Ohne Runbook wird improvisiert, ohne Protokollierung nicht nachvollziehbar

Was müssen wir jetzt schon vorbereiten?

Der Rollout kommt ohne Schalter und ohne Terminabsprache. Bis Ende September 2026 hat deine Rolle die neuen Rechte, ob du vorbereitet bist oder nicht. Es gibt also genau zwei Zustände: Du hast bis dahin aufgeräumt, oder du hast eine unbemerkt gewachsene Berechtigung im Tenant. Die folgende Reihenfolge hat sich bewährt.

Fang mit dem Inventar an. Zieh dir die aktuellen Zuweisungen und schau sie dir namentlich an – nicht als Zahl in einem Dashboard, sondern als Liste mit Menschen darauf. Jede Zeile, bei der du überlegen musst, warum die Person dort steht, ist eine Zeile zu viel.

Connect-MgGraph -Scopes "RoleManagement.Read.Directory"

Get-MgBetaRoleManagementDirectoryRoleAssignment -ExpandProperty roleDefinition `
 -Filter "roleDefinition/isPrivileged eq true" | Format-List

Maßnahme	Warum sie jetzt dran ist	Wer	Bis wann
Zuweisungen für Security Administrator inventarisieren und kürzen	Die Rolle bekommt neue Macht, ohne dass jemand zustimmt	Identity-Betrieb	sofort
Rolle in PIM überführen, Aktivierung mit MFA, Begründung und Zeitlimit	Stehende privilegierte Rechte sind der eigentliche Angriffspfad	Identity-Betrieb	September 2026
Entra SOC Identity Responder für die Schicht prüfen	Schmalere Rolle, auf administrative Einheiten einschränkbar	SOC-Leitung	September 2026
Tier-o-Konten in eine Restricted Management Administrative Unit legen	Schützt Adminkonten vor allem, was unterhalb von Privileged Auth Admin liegt	Identity-Architektur	Q4 2026
Runbook „Konto kompromittiert“ neu schreiben	Der Ablauf ändert sich, die Eskalation für Adminkonten bleibt	SOC-Leitung	Oktober 2026
Alarmierung auf die vier neuen Actions im Audit-Log	Wer sperrt, muss selbst überwacht sein	SOC Engineering	Oktober 2026
Kennwortrückschreibung für synchronisierte Konten prüfen	Ohne Writeback läuft das Zurücksetzen bei Hybridkonten ins Leere	Identity-Betrieb	September 2026
CAE-Abdeckung und Clientstand prüfen	Ohne CAE-fähige Clients wirkt der Widerruf erst nach Tokenablauf	Client Management	Q4 2026

TIPP: Die Hybrid-Falle steht schon bereit

Bei aus dem lokalen Active Directory synchronisierten Konten nützt dir das Deaktivieren in Entra nur

die halbe Miete: Der nächste Synchronisierungslauf kann den Zustand aus dem AD zurückschreiben. Sperre deshalb parallel im AD und setz das Kennwort dort zweimal hintereinander – das ist kein Aberglaube, sondern die dokumentierte Maßnahme gegen Pass-the-Hash bei verzögerter Replikation. Schreib genau das in dein Runbook, mit Cmdlet und Beispiel, nicht als Prosa.

Und dann der Teil, den fast alle auslassen: Übt es. Ein Runbook, das noch nie unter Zeitdruck gelaufen ist, ist eine Meinung, kein Prozess. Setz eine Stunde an, nimm ein Testkonto, lass einen Analysten aus der zweiten Reihe den Ablauf durchgehen und stopp die Zeit. Du wirst drei Dinge lernen: dass niemand weiß, wo das Konto in der Restricted Management AU liegt, dass die Freigabe für Adminkonten nirgends hinterlegt ist, und dass die Wiederaktivierung länger dauert, als alle geglaubt haben. Genau dafür macht man Übungen.

TIPP: Zwei Sätze für die Geschäftsführung

Wenn du das Thema nach oben tragen musst, brauchst du keine Rollentabelle. Es reicht: „Wir können ein übernommenes Konto künftig in Minuten statt in Stunden stilllegen, ohne dafür zusätzliche Adminrechte zu verteilen. Damit das trägt, räumen wir vorher auf, wer diese Rolle überhaupt hat.“ Das versteht jeder Vorstand, und es ist nicht einmal vereinfacht.

Häufig gestellte Fragen

Muss ich die Rolle neu zuweisen, damit die zusätzlichen Rechte wirken?

Nein. Microsoft erweitert die Definition der eingebauten Rolle serverseitig, bestehende Zuweisungen erben die neuen Aktionen automatisch. Genau deshalb solltest du vor Abschluss des Rollouts Ende September 2026 prüfen, wer die Rolle heute besitzt.

Kann ein Security Administrator damit auch ein Administratorkonto sperren?

Nein. Die Aktionen wirken ausschließlich auf nicht administrative Konten; Konten mit einer Entra-Rolle, Mitglieder rollenzuweisbarer Gruppen und Konten in einer Restricted Management Administrative Unit sind ausgenommen. Für diese Fälle brauchst du weiterhin Privileged Authentication Administrator oder Global Administrator.

Wie schnell ist ein Benutzer nach dem Widerruf der Sitzungen tatsächlich draußen?

Bei Diensten mit Continuous Access Evaluation – Exchange Online, SharePoint Online und Teams – greift der Rauswurf nahezu in Echtzeit, dokumentiert sind bis zu 15 Minuten Laufzeit für die Ereignisverteilung. Ohne CAE-fähige Clients oder Dienste bleibt das alte Access Token bis zu seinem Ablauf gültig, in CAE-Sitzungen sogar bis zu 28 Stunden.

Funktioniert das Zurücksetzen des Kennworts auch bei synchronisierten Konten?

Nur dann, wenn die Kennwortrückschreibung aus Entra ins lokale Active Directory eingerichtet ist. Ohne Writeback läuft der Versuch ins Leere, und du musst zusätzlich im lokalen Verzeichnis sperren und das Kennwort dort zurücksetzen.

Brauche ich dann überhaupt noch die Rolle Entra SOC Identity Responder?

In den meisten Fällen ja, denn sie ist die deutlich schmalere Wahl: Sie kann genau die Eindämmungsaktionen und sonst nichts, und sie lässt sich auf administrative Einheiten einschränken. Für Analysten im Schichtbetrieb ist sie die bessere Rolle, während Security Administrator wegen der breiten Konfigurationsrechte wenigen Köpfen vorbehalten bleiben sollte.