

Entra im Oktober: Continuous Access Evaluation in GSA reagiert jetzt auf Gerätesignale

Stell dir vor, die Personalabteilung sperrt um 16:02 Uhr das Konto eines frisch gekündigten Vertrieblers. Um 16:03 Uhr kopiert genau dieser Vertriebler gemütlich die Kundendatenbank vom Fileserver – über einen Tunnel, den du ihm selbst gebaut hast. Das ist kein Horrorfilm, das war bisher schlicht OAuth. Mit dem Oktober-Update von Microsoft Entra schließt sich diese Lücke ein weiteres Stück: Universal CAE in Global Secure Access hört jetzt nicht nur auf Kontoänderungen, sondern auch auf Gerätesignale.

Executive Summary

Global Secure Access (GSA), Microsofts Security Service Edge aus Internet Access und Private Access, authentifiziert seine Tunnel mit ganz normalen Entra-ID-Access-Tokens. Die leben 60 bis 90 Minuten – und zwar unabhängig davon, ob der Benutzer inzwischen gefeuert, gehackt oder sein Laptop im Baggersee versenkt wurde. **Universal Continuous Access Evaluation** sorgt dafür, dass GSA bei kritischen Ereignissen nicht bis zum Tokenablauf wartet, sondern den Benutzer sofort zur Neuansmeldung zwingt.

Neu im Oktober (als Public Preview): Neben den bekannten Benutzersignalen wie gesperrtem Konto oder hohem Nutzerrisiko wertet Universal CAE jetzt auch aus, ob das zugreifende **Gerät gelöscht, deaktiviert oder nicht mehr compliant** ist. Der Benutzer bekommt einen Toast im GSA-Client und hat zwei Minuten Zeit, sich erfolgreich neu anzumelden. Schafft er das nicht, werden alle GSA-Tunnel getrennt.

Klingt nach Zero Trust zum Einschalten. Ist es auch – mit einem Haken, der größer ist als er aussieht: Das Signal ist nur so gut wie deine Compliance-Policies. Wenn Intune deine Geräte heute schon grundlos rot färbt, kappt dir Universal CAE morgen grundlos die Verbindung. Und wenn du keine passende Conditional-Access-Policy hast, passiert schlicht gar nichts.

Fakten: Das Wichtigste in drei Zeilen

Was: Universal CAE in GSA reagiert auf Geräteereignisse (gelöscht, deaktiviert, non-compliant) und Nutzerrisiko.

Status: Gerätesignale in Public Preview; Benutzersignale wie Kontosperrung, Passwortreset und Token-Widerruf bereits etabliert.

Wirkung: Toast im GSA-Client, zwei Minuten Frist, danach sind Microsoft-, Internet- und Private-Access-Tunnel getrennt.

Worum geht es im Detail?

Fangen wir beim Grundproblem an, denn das erklärt, warum es dieses Feature überhaupt braucht. Nach OAuth-2-Spezifikation ist ein Access Token gültig, bis es abläuft. Punkt. Sperrst du ein Konto, invalidiert Entra ID zwar sofort den Refresh Token – der Benutzer bekommt also kein neues Access Token mehr. Das alte Token aber läuft munter weiter, bei GSA bis zu 90 Minuten. In dieser

Zeit ist der Tunnel offen, und hinter dem Tunnel liegen Fileserver, RDP-Hosts, das ERP im Rechenzentrum und jede SaaS-Anwendung im Internet.

Das klassische CAE von Entra ID hat dieses Problem schon vor Jahren angegangen – allerdings nur für Anwendungen, die CAE selbst verstehen. Das sind im Wesentlichen Microsofts eigene Dienste wie Exchange Online, SharePoint Online, Teams und Microsoft Graph. Jede Anwendung muss dafür spezielle Bibliotheken einbauen. Dein zwanzig Jahre altes Warenwirtschaftssystem wird das in diesem Leben nicht mehr tun, und dein Fileserver auch nicht.

Universal CAE dreht den Spieß um: Nicht die Anwendung prüft, sondern die **GSA-Edge**. Bei jeder neuen Verbindung zu einer Anwendungsressource wird der Zugriff validiert. Meldet Entra ID ein kritisches Ereignis, schickt GSA dem Client eine Claims Challenge – obwohl das Token formal noch gültig ist. Damit profitiert jede Anwendung, die über GSA erreicht wird, ohne dass sie von CAE je gehört haben muss. Das ist der eigentliche Clou.

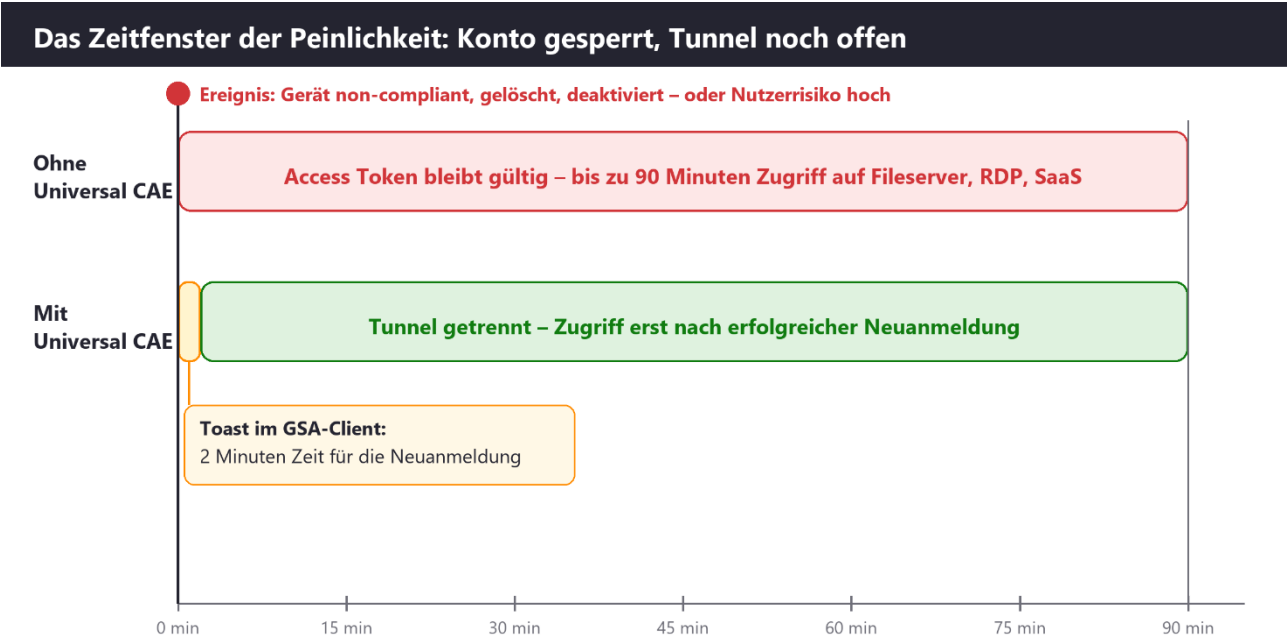


Abbildung 1: Ohne Universal CAE bleibt der Tunnel bis zum Tokenablauf offen, mit Universal CAE nach spätestens zwei Minuten zu.

Welche Signale lösen die Neuanmeldung aus? Hier ist die Übersicht, inklusive der Neuzugänge aus dem Oktober:

Signal	Quelle	Typ	Status
Konto gelöscht oder deaktiviert	Entra ID	Benutzer	verfügbar
Passwort geändert oder zurückgesetzt	Entra ID	Benutzer	verfügbar
MFA für den Benutzer aktiviert	Entra ID	Benutzer	verfügbar
Admin widerruft alle Refresh Tokens	Entra ID	Benutzer	verfügbar
Hohes Nutzerrisiko erkannt	Entra ID Protection	Benutzer	neu im Fokus
Gerät gelöscht oder deaktiviert	Entra ID Geräteobjekt	Gerät	Preview
Gerät nicht mehr compliant	Intune bzw. Compliance-Partner	Gerät	Preview

Der Ablauf ist angenehm brutal: GSA empfängt das Ereignis, der GSA-Client zeigt einen Toast, der Benutzer muss sich neu anmelden. Kommt die erfolgreiche Anmeldung nicht innerhalb von **zwei Minuten**, trennt der Client alle Tunnel – Microsoft-Traffic, Internet Access und Private Access.

Schafft der Benutzer die Anmeldung später doch noch, kommt auch die Verbindung zurück. Für den gekündigten Vertriebler heißt das: Er darf sich noch zwei Minuten lang überlegen, wie er seinem Anwalt das erklärt.

Wichtig: Ohne Conditional Access ist das Signal ein Rauchmelder ohne Batterie

Gerätecompliance und Nutzerrisiko sind ausdrücklich dafür gedacht, mit einer passenden Conditional-Access-Policy zusammenzuarbeiten. Fehlt die Policy, läuft die Neuansmeldung still im Hintergrund durch – und niemand reagiert auf das Ereignis.

Typische Paare: **Alle Benutzer → alle Internetressourcen über GSA → konformes Gerät erforderlich** sowie **Alle Benutzer → alle Ressourcen → Nutzerrisiko hoch → Risikobehhebung erforderlich**.

Wie ein Gerätesignal deinen Tunnel kappt

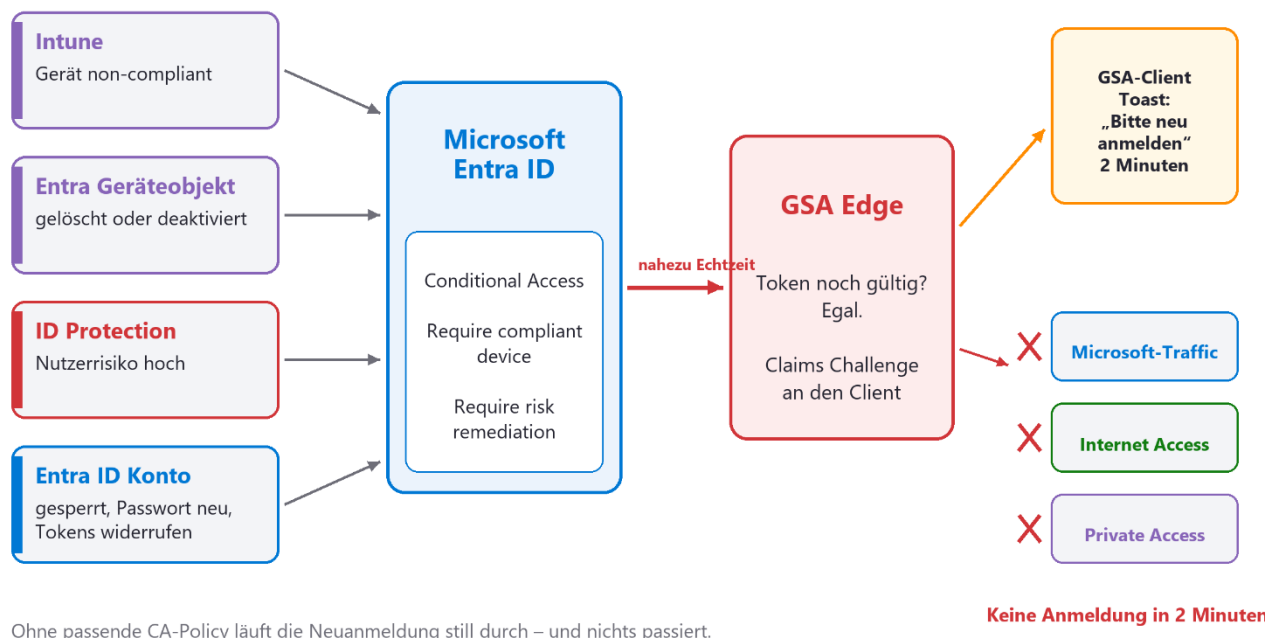


Abbildung 2: Vom Intune-Statuswechsel bis zum getrennten Tunnel – Conditional Access ist das Bindeglied, ohne das nichts passiert.

Zwei weitere Bausteine gehören ins Bild. Erstens die **Netzwerkbindung**: Wenn du per Conditional Access verlangst, dass Benutzer aus bestimmten Netzen kommen, erzwingt ein Netzwerkwechsel eine Neuauthentifizierung samt Neubewertung der standortbasierten Policies. Zweitens der **Strict Enforcement Mode**: Er blockiert Zugriffe sofort, wenn das Token von einer anderen IP-Adresse wiederverwendet wird als bei der Anmeldung. Das ist der Schutz gegen Token-Diebstahl und Replay – und gleichzeitig die zuverlässigste Methode, dich bei unsauberem Routing selbst auszusperren.

Und noch ein Detail, das Nerven spart: Universal CAE ist standardmäßig **opportunistisch**. Unterstützte GSA-Clients versuchen, ein CAE-fähiges Token zu bekommen. Klappt das nicht, etwa wegen einer alten Clientversion, gibt es ein normales Token. Du musst das Feature also nicht

abschalten, nur weil noch ein paar Gurken-Clients im Feld stehen – die bekommen dann eben auch keinen Schutz.

Was sind Chancen? Was sind Risiken?

Die Chancen liegen auf der Hand, und sie sind größer als „ein Häkchen mehr im Zero-Trust-Bingo“. Zum ersten Mal bekommst du eine nahezu sofortige Reaktion auf Geräteereignisse **für alle Anwendungen hinter GSA** – auch für die, die du nie modernisieren wirst. Der RDP-Zugriff auf den Buchhaltungsserver, das SMB-Share mit den Konstruktionsdaten, der Upload zu irgendeinem Filehoster: alles hängt jetzt am selben Not-Aus.

Ein Praxisfall aus einem Kundenprojekt im Maschinenbau: Ein Außendienstler meldet morgens seinen Laptop als gestohlen. Der Helpdesk deaktiviert das Gerät in Entra ID, klopft sich auf die Schulter und geht Kaffee holen. Bisher hätte der Dieb – sofern er das Gerät entsperrt bekam – noch bis zu anderthalb Stunden Zugriff auf Private-Access-Ressourcen gehabt. Mit Universal CAE ist nach zwei Minuten Schluss. Der Kaffee schmeckt gleich besser.

Chancen	Risiken
Not-Aus für Legacy-Apps, Fileserver und RDP ohne eine Zeile Code in der Anwendung	Unzuverlässige Compliance-Policies kappen produktive Benutzer – im Zweifel alle gleichzeitig
Kündigung, Diebstahl, kompromittiertes Gerät: Reaktion in Minuten statt nach Tokenablauf	Gerätesignale sind Preview: Verhalten und Latenzen können sich noch ändern
Nutzerrisiko aus ID Protection wirkt endlich auch auf Netzwerkebene	Ohne passende CA-Policy gibt es keine Wirkung, aber trügerische Sicherheit
Strict Enforcement schützt GSA-Tokens vor Diebstahl und Replay	Strict Enforcement bei unklarem Routing sperrt legitime Benutzer aus
Ein Signal, eine Logik für Microsoft-, Internet- und Private-Traffic	Helpdesk-Welle, wenn Benutzer den Toast nicht verstehen oder ignorieren

Und jetzt der schwarze Teil. Universal CAE ist ein Verstärker. Es verstärkt gute Compliance – und es verstärkt kaputte Compliance. Aus einem anderen Projekt: Montagmorgen, 7:45 Uhr. Eine Compliance-Policy verlangt eine Mindestversion von Windows, das Patch-Ring-Rollout hängt seit Freitag, und der Grace-Period-Zeitraum ist zufällig genau übers Wochenende abgelaufen. Ergebnis: 340 Notebooks auf einen Schlag non-compliant. Früher hätte das „nur“ den Zugriff auf Exchange blockiert. Mit Universal CAE und Require-Compliant-Device für GSA ist auch das Internet weg, der Fileserver weg und die Remote-Session zur Produktion weg. Der Helpdesk erreicht übrigens niemand, denn das Telefonsystem ist natürlich eine SaaS-Anwendung hinter Internet Access.

Warnung: Compliance-Flattern ist jetzt ein Produktionsrisiko

Geräte, die zwischen compliant und non-compliant hin- und herspringen, waren bisher ein Schönheitsfehler im Intune-Bericht. Ab jetzt sind sie ein Verfügbarkeitsproblem. Wer seine Compliance-Policies seit 2021 nicht angefasst hat, sollte das tun, bevor er Gerätesignale scharf schaltet – und nicht danach, mit dem Vorstand am Telefon.

Weitere Stolperfallen: Die Einstellung, wie Geräte **ohne zugewiesene Compliance-Policy** bewertet werden, entscheidet über Wohl und Wehe ganzer Gerätegruppen. Die Gültigkeitsdauer des Compliance-Status sorgt dafür, dass Geräte, die sich länger nicht gemeldet haben, irgendwann still auf non-compliant kippen – typischerweise das Notebook aus der Elternzeit. Und Compliance-Signale aus Partnerlösungen wie Defender for Endpoint oder Mobile-Threat-Defense-Produkten hängen an Konnektoren, deren Ausfall plötzlich direkt im Netzwerkzugang spürbar ist.

Was müssen wir jetzt schon vorbereiten?

Die gute Nachricht: Du musst nichts überstürzen, denn die Gerätesignale sind Preview und wirken nur mit passender CA-Policy. Die schlechte: Die Vorarbeit liegt komplett auf deiner Seite, und sie dauert länger als das Einschalten. So gehst du vor:

1. **Compliance-Inventur:** Exportiere den Compliance-Status aller Geräte der letzten 30 Tage. Wie viele Geräte wechseln mehr als einmal pro Woche den Status? Das ist deine Flutter-Quote, und die muss gegen null gehen.
2. **Policies entrümpeln:** Prüfe Mindest-OS-Versionen, Grace Periods, die Gültigkeitsdauer des Compliance-Status und die Bewertung von Geräten ohne Policy. Jede Regel muss sich mit einem echten Risiko begründen lassen, nicht mit „hatten wir schon immer“.
3. **Geräte-Lifecycle klären:** Wer löscht oder deaktiviert Geräteobjekte, und wann? Ein Aufräumskript, das „alte“ Geräte deaktiviert, kann sonst auch aktive Notebooks erwischen.
4. **CA-Policies im Report-only-Modus testen:** Require Compliant Device für GSA-Internetressourcen und Risk Remediation für hohes Nutzerrisiko erst beobachten, dann scharf schalten.
5. **Pilotgruppe definieren:** IT plus ein mutiger Fachbereich. Nicht die Geschäftsführung, nicht die Produktion.
6. **GSA-Clients aktualisieren:** Alte Clientversionen bekommen nur normale Tokens und damit keinen Schutz.
7. **Helpdesk briefen:** Der Toast muss bekannt sein. Ein Satz im Intranet erspart dir hundert Tickets mit dem Betreff „Internet kaputt“.
8. **Strict Enforcement erst nach Routing-Analyse:** Erst wenn klar ist, über welche IP-Adressen Authentifizierung und Datenverkehr laufen.

Aufgabe	Verantwortlich	Aufwand	Priorität
Compliance-Flutter-Quote ermitteln	Endpoint-Team	1–2 Tage	hoch
Compliance-Policies bereinigen	Endpoint-Team + Security	1–3 Wochen	hoch
Geräte-Lifecycle-Prozess dokumentieren	IT-Betrieb	3–5 Tage	mittel
CA-Policies in Report-only	Identity-Team	1 Tag + 2 Wochen Beobachtung	hoch
Pilot mit Gerätesignalen	Identity + Endpoint	2–4 Wochen	mittel
Helpdesk-Schulung und Kommunikation	Service Desk	2 Tage	mittel

Tipp: Die Report-only-Wahrheit

Schalte die Policy „konformes Gerät für GSA“ zwei Wochen lang im Report-only-Modus und werte die Anmeldeprotokolle aus. Jeder Eintrag, der dort als Blockade aufgetaucht wäre, ist ein Benutzer, der dich später angerufen hätte. Diese Liste ist dein Arbeitsvorrat – und das beste Argument gegenüber dem Management, warum du nicht einfach „mal eben“ einschaltest.

Zum Schluss ein Gedanke für die Strategie: Mit Universal CAE wird Gerätecompliance von einer Statistik zu einem Schalter, der Menschen den Arbeitsplatz abdreht. Das ist genau das, was Zero Trust verspricht. Es ist aber auch der Moment, in dem das Endpoint-Team und das Identity-Team endlich miteinander reden müssen – falls sie das bisher erfolgreich vermieden haben.

Häufig gestellte Fragen

Was ist der Unterschied zwischen klassischem CAE und Universal CAE in Global Secure Access?

Klassisches CAE funktioniert nur bei Anwendungen, die CAE selbst unterstützen, im Wesentlichen Microsoft-Dienste wie Exchange Online, SharePoint Online und Teams. Universal CAE setzt an der Global-Secure-Access-Edge an und wirkt damit auf jede Anwendung, die über GSA erreicht wird, auch auf Fileserver, RDP und SaaS-Dienste anderer Hersteller.

Wie schnell wird der Zugriff gesperrt, wenn ein Gerät nicht mehr compliant ist?

Nach dem Ereignis erhält der Benutzer nahezu in Echtzeit eine Aufforderung zur Neuansmeldung im GSA-Client. Gelingt die Anmeldung nicht innerhalb von zwei Minuten, werden alle GSA-Tunnel getrennt, bis eine erfolgreiche Anmeldung erfolgt.

Brauche ich für Universal CAE mit Gerätesignalen eine eigene Conditional-Access-Policy?

Ja, Gerätecompliance und Nutzerrisiko entfalten ihre Wirkung nur zusammen mit einer passenden Conditional-Access-Policy, etwa „konformes Gerät erforderlich“ für Internetressourcen über GSA. Ohne diese Policy läuft die Neuansmeldung still durch und der Zugriff bleibt bestehen.

Muss ich Universal CAE abschalten, wenn noch alte GSA-Clients im Einsatz sind?

Nein, Universal CAE arbeitet standardmäßig opportunistisch: Kann ein Client kein CAE-fähiges Token beziehen, erhält er ein normales Access Token. Diese Clients sind dann allerdings auch nicht durch CAE geschützt, deshalb lohnt sich ein zügiges Update.

Was passiert, wenn meine Intune-Compliance-Policies fehlerhaft Geräte als nicht konform markieren?

Dann trennt Universal CAE bei aktiver Conditional-Access-Policy auch die GSA-Verbindungen dieser Geräte, also Internetzugang, Private Access und Microsoft-Traffic. Bereinige deshalb vor der Aktivierung deine Compliance-Policies und teste die Conditional-Access-Regeln zunächst im Report-only-Modus.