Bedingter Zugriff, MFA und SSO auf dem Terminalserver



WISSEN

Alles zu CosyTrack.Drive: SharePoint, Teams und OneDrive als Laufwerksbuchstaben, am Arbeitsplatz und auf dem Terminalserver.

› CosyTrack.Drive

BERATUNG

Richtlinien, Sitzungshosts und Laufwerke sollen zusammenpassen? Wir gehen deine Umgebung mit dir im Pilot durch.

› Beratung zu CosyTrack.Drive

SCHULUNG

Onboarding für Admins: Laufwerksquellen, Richtlinien, Admin-Kit und Fehlersuche auf dem Sitzungshost.

› Schulung und Onboarding für CosyTrack.Drive

Montag, 8:12 Uhr. Die Buchhaltung meldet sich am Terminalserver an, Outlook will ein Kennwort, Teams will eine Bestätigung in der Authenticator-App, OneDrive hätte gern beides, und irgendwo im Hintergrund wartet ein Browserfenster auf einen Klick. Um 8:15 Uhr ruft die erste Kollegin an und fragt, ob ihr Konto gehackt wurde. Um 8:16 Uhr fragst du dich, ob du Schafzüchter hättest werden sollen.

Bedingter Zugriff auf dem Terminalserver ist kein exotisches Thema, sondern der Normalfall in jeder Umgebung, die Microsoft 365 aus RDS-Sitzungen nutzt. Die Richtlinien in Microsoft Entra ID wurden aber meist für Notebooks gebaut: ein Gerät, ein Benutzer, ein Intune-Konformitätsstatus. Ein Sitzungshost ist das Gegenteil davon. Viele Benutzer teilen sich ein Gerät, alle kommen mit derselben IP-Adresse ins Internet, und Intune kennt den Server womöglich gar nicht.

Dieser Beitrag nimmt die Admin- und Security-Perspektive ein. Du erfährst, welche Bedingungen und Gewährungssteuerelemente auf einem Sitzungshost tragen, wie Anmeldehäufigkeit und Primary Refresh Token zusammenspielen und warum ausgerechnet die gut gemeinte Einstellung „MFA speichern“ für mehr Abfragen sorgen kann. Alle Grenzwerte und Verhaltensweisen stammen aus Microsoft Learn. Die Grundlagen zum Terminalserver selbst setzen wir voraus; dafür gibt es SharePoint als Laufwerk auf dem Terminalserver und OneDrive auf dem Terminalserver.

FAKTEN · Bedingter Zugriff in drei Sätzen

Bedingter Zugriff ist eine Funktion von Microsoft Entra ID P1 oder P2. Eine Richtlinie kombiniert Zuweisungen (Benutzer, Zielressourcen, Bedingungen wie Standort, Geräteplattform oder Filter für Geräte) mit Zugriffssteuerungen (blockieren oder zulassen unter Auflagen wie MFA) und Sitzungssteuerungen (etwa Anmeldehäufigkeit oder beständige Browsersitzung).

Ausgewertet wird bei der Tokenanfrage für eine Ressource, nicht bei der Windows-Anmeldung. Laut Microsoft Learn werden Richtlinien weder bei der Ausgabe noch bei der Erneuerung eines Primary Refresh Token ausgewertet.

Mehrere Richtlinien gelten gleichzeitig. Gewährt wird nur, wenn alle zutreffenden Richtlinien erfüllt sind.

Was auf dem Sitzungshost anders ist

Am Arbeitsplatz ist das Modell übersichtlich: Ein Windows-11-Gerät ist in Microsoft Entra ID eingebunden, Intune meldet den Konformitätsstatus, und der Benutzer meldet sich an seinem eigenen Gerät an. Auf dem Terminalserver verschieben sich gleich drei Annahmen.

Ein Gerät, viele Benutzer

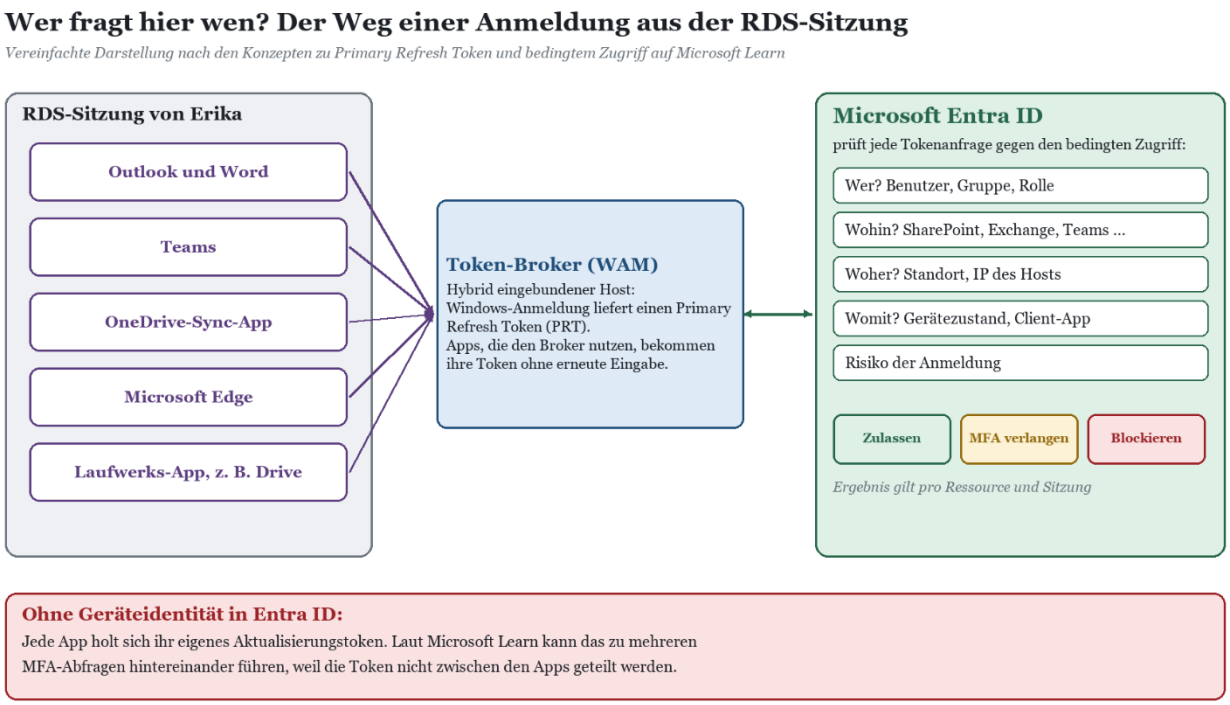
Der Sitzungshost ist für Entra ID ein einziges Gerät. Jede Benutzersitzung auf diesem Host bringt dieselbe Geräteidentität mit, sofern der Host eine hat. Für den bedingten Zugriff ist das gut und schlecht zugleich: Eine Richtlinie, die einen hybrid eingebundenen Host verlangt, ist für alle Sitzungen auf einmal erfüllt. Eine Richtlinie, die auf ein persönliches, konformes Gerät zielt, läuft dagegen ins Leere.

Eine IP-Adresse für alle

Alle Sitzungen eines Hosts gehen mit derselben ausgehenden Adresse ins Internet, meist der Adresse deines Rechenzentrums oder deiner Firewall. Benannte Standorte im bedingten Zugriff sehen deshalb immer „Firmennetz“, egal ob die Kollegin im Büro sitzt oder per RD-Gateway vom Küchentisch aus arbeitet. Wer den Standort als Ersatz für MFA benutzt, verschenkt auf dem Terminalserver genau den Schutz, den er eigentlich wollte. Wie Benutzer von unterwegs an ihre Laufwerke kommen, ohne dass das Firmennetz die halbe Sicherheitsarbeit übernimmt, beschreibt Netzlaufwerk ohne VPN: S: im Homeoffice und unterwegs.

Wer hier wen fragt: PRT, Broker und App-Token

Damit Single Sign-on funktioniert, braucht Windows einen Primary Refresh Token, kurz PRT. Microsoft Learn beschreibt ihn als das zentrale Artefakt für SSO auf Windows: Auf einem in Entra ID eingebundenen oder hybrid eingebundenen Gerät wird er bei der Windows-Anmeldung ausgestellt. Der Token-Broker (Web Account Manager, WAM) nutzt ihn, um Apps wie Office, Teams und Edge ohne erneute Eingabe mit Token zu versorgen. Ein PRT ist 90 Tage gültig und wird laufend erneuert, solange der Benutzer das Gerät aktiv nutzt; das CloudAP-Plug-in aktualisiert ihn bei der Windows-Anmeldung alle vier Stunden.



Der entscheidende Satz für Terminalserver steht etwas versteckt in der Dokumentation zu MFA-Abfragen: Auf einem Gerät ohne Identität in Entra ID kann ein Benutzer mehrere MFA-Abfragen sehen, weil jede Anwendung ihr eigenes Aktualisierungstoken hat, das sie nicht mit anderen Apps teilt. Übersetzt: Ein Sitzungshost, der nur in der lokalen Domäne steht, aber nicht hybrid eingebunden ist, produziert Anmeldeabfragen am Fließband. Outlook fragt, Teams fragt, OneDrive fragt, und jede weitere App, die auf Microsoft 365 zugreift, fragt auch.

WICHTIG · Hybrid Join ist auf dem Terminalserver keine Kür

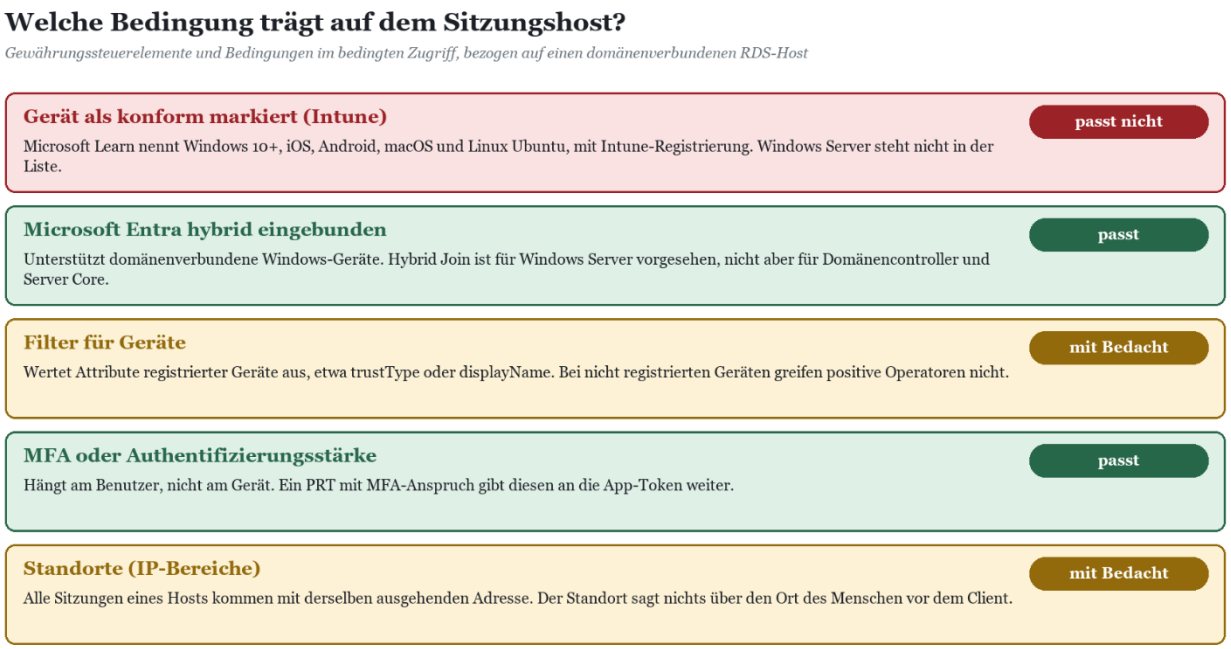
Microsoft empfiehlt für SSO über Anwendungen hinweg verwaltete Geräte, also Entra-Join oder Hybrid Join, oder nahtloses SSO. Für domänenverbundene Sitzungshosts ist Hybrid Join der realistische Weg. Die Planungsseite auf Microsoft Learn nennt Windows Server 2016, 2019 und 2022 ausdrücklich; die Seite zu Geräteidentität und Desktopvirtualisierung zählt „Windows Server 2019 oder höher“ zu den aktuellen Windows-Geräten. Nicht unterstützt sind Domänencontroller und Server Core.

Richtlinien für bedingten Zugriff mit Bordmitteln planen

Mit den Bordmitteln von Microsoft lässt sich ein Sitzungshost sauber in den bedingten Zugriff einbinden. Die Kunst besteht darin, die Bedingungen zu wählen, die auf einem gemeinsam genutzten Server tatsächlich ein Signal liefern, statt Richtlinien vom Notebook eins zu eins zu übernehmen.

Gerätezustand: konform oder hybrid eingebunden?

Die beliebteste Gewährung am Arbeitsplatz ist „Gerät muss als konform markiert sein“. Laut Microsoft Learn unterstützt dieses Steuerelement nur Windows 10 und neuer, iOS, Android, macOS und Linux Ubuntu, und zwar Geräte, die in Entra ID registriert und bei Intune angemeldet sind. Windows Server taucht in dieser Liste nicht auf. Für Sitzungshosts ist deshalb „Microsoft Entra hybrid eingebundenes Gerät verlangen“ das passende Gegenstück: Es unterstützt domänenverbundene Windows-Geräte.



Steuerelement oder Bedingung	Am Arbeitsplatz	Auf dem Sitzungshost	Worauf du achtest
Gerät als konform markiert	Standard für verwaltete Clients	Kein Signal, Windows Server nicht unterstützt	Richtlinie so formulieren, dass Hosts über ein anderes Steuerelement durchkommen
Hybrid eingebundenes Gerät	Für domänenverbundene Clients	Passendes Gerätesignal	Hybrid Join vor dem Rollout prüfen, Images sauber vorbereiten
MFA verlangen	Unabhängig vom Gerät	Unabhängig vom Gerät	Mit PRT und Broker bleibt es bei einer Abfrage statt vieler
Authentifizierungsstärke	Etwa phishingresistente Methoden	Methode muss in der RDS-Sitzung nutzbar sein	Im Pilot mit echten Benutzern testen
App-Schutzrichtlinie	iOS, Android; für Edge unter Windows in der Vorschau	Kein Ersatz für Gerätesignale	Nicht als Hauptbaustein für RDS planen

Eine typische Konstruktion: Eine Richtlinie verlangt für Office 365 „konformes Gerät ODER hybrid eingebundenes Gerät“, eine zweite verlangt für alle Benutzer MFA. Das Notebook erfüllt die erste Bedingung über Intune, der Sitzungshost über Hybrid Join, und MFA gilt überall. Standardmäßig verlangt bedingter Zugriff alle ausgewählten Steuerelemente; die Oder-Verknüpfung musst du bewusst auswählen.

Filter für Geräte: Sitzungshosts gezielt ansprechen

Willst du für die Sitzungshosts eigene Regeln, etwa eine kürzere Anmeldehäufigkeit, hilft die Bedingung „Filter für Geräte“. Sie kennt unter anderem die Attribute displayName, operatingSystem, trustType (ServerAD steht für hybrid eingebundene Geräte) und die Erweiterungsattribute 1 bis 15. Ein Namenspräfix für deine Hosts ist damit plötzlich mehr als Ordnungsliebe.

```
device.displayName -startsWith "RDS-" -and device.trustType -eq "ServerAD"
```

WARNUNG · Positive Operatoren und nicht registrierte Geräte

Microsoft Learn weist ausdrücklich darauf hin: Für ein Gerät, das nicht in Entra ID registriert ist, gelten alle Geräteeigenschaften als leer. Ein Filter mit positiven Operatoren wie Equals oder StartsWith greift dann schlicht nicht. Ist dein Host also nicht sauber hybrid eingebunden, fällt er unbemerkt aus der Richtlinie heraus. Für Erweiterungsattribute gilt zusätzlich: Ihre Werte stehen nur zur Verfügung, wenn das Gerät von Intune verwaltet, konform oder hybrid eingebunden ist.

Keine Arbeitskonten auf dem Host registrieren lassen

Viele Office-Apps bieten nach der Anmeldung an, das Konto „überall auf diesem Gerät“ zu verwenden und die Organisation das Gerät verwalten zu lassen. Klickt ein Benutzer auf einem Sitzungshost auf Ja, wird der Host für diesen Benutzer zusätzlich als Entra-registriertes Gerät geführt. Microsoft beschreibt diesen Doppelzustand aus hybrid eingebunden und registriert in der Planung zu Hybrid Join und nennt den Riegel dagegen: einen Registrierungswert unter den Richtlinien.

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin
BlockAADWorkplaceJoin = dword:00000001
```

Für nicht persistente Umgebungen empfiehlt Microsoft Learn denselben Wert ausdrücklich. Auf einem Terminalserver, auf dem sich viele Benutzer dasselbe Gerät teilen, ist er schlicht Hygiene. Verteilen lässt er sich wie jede andere Computerrichtlinie per GPO.

Testen, bevor es knallt: Nur-Bericht-Modus und What If

Microsoft rät, Richtlinien mit Blockierung vor dem Scharfschalten im Nur-Bericht-Modus laufen zu lassen und mit dem What-If-Werkzeug durchzuspielen. Für Terminalserver lohnt sich ein eigener Prüfschritt: Spiele die Anmeldung eines Pilotbenutzers vom Sitzungshost aus durch, nicht vom Admin-Notebook. Sonst testest du die Richtlinie für das falsche Gerät und wunderst dich am Montag.

TIPP · Notfallkonten nicht vergessen

Schließe deine Notfallkonten aus jeder Richtlinie mit Blockierung aus, wie es Microsoft in den Beispielrichtlinien vorsieht. Ein Terminalserver, auf dem sich niemand mehr anmelden kann, ist sehr sicher. Aber eben auch sehr nutzlos.

Anmeldehäufigkeit, Sitzungsdauer und MFA-Abfragen

Die zweite große Baustelle ist die Frage, wie oft Benutzer überhaupt gefragt werden. Hier lohnt ein Blick auf die Standardwerte, bevor du an Schrauben drehst.

Der Standard: 90 Tage rollierend

Die Standardkonfiguration von Microsoft Entra ID für die Anmeldehäufigkeit ist ein rollierendes Fenster von 90 Tagen. Das klingt für Security-Leute zunächst nach Leichtsinn. Microsoft begründet es so: Wer ständig nach Anmeldedaten gefragt wird, gibt sie irgendwann reflexhaft ein, auch in eine gefälschte Abfrage. Und jede Verletzung einer Richtlinie, etwa eine Kennwortänderung, ein deaktiviertes Konto oder ein nicht konformes Gerät, widerruft die Sitzung ohnehin. Die Grundregel lautet: Frage nicht erneut, wenn sich am Sicherheitszustand der Sitzung nichts geändert hat.

Anmeldehäufigkeit per Richtlinie

Mit der Sitzungssteuerung „Anmeldehäufigkeit“ legst du fest, nach welcher Zeit ein Benutzer sich erneut anmelden muss. Sie gilt inzwischen nicht nur für den ersten Faktor, sondern auch für MFA. Auf eingebundenen und hybrid eingebundenen Geräten zählt dabei der Zeitpunkt der letzten PRT-Aktualisierung, und die erfolgt beim Entsperren oder bei einer interaktiven Anmeldung höchstens alle vier Stunden. Deshalb kommt die Abfrage manchmal später, als du nach der eingestellten Dauer erwarten würdest.



Die Einstellung „Jedes Mal“ verlangt eine vollständige erneute Authentifizierung, sobald die Sitzung ausgewertet wird. Microsoft rechnet dabei fünf Minuten Uhrabweichung ein und rät, „Jedes Mal“ nur für wenige, besonders sensible Anwendungen einzusetzen. Für Apps aus dem Microsoft-365-Stapel empfiehlt Microsoft eine zeitbasierte Anmeldehäufigkeit. Die Warnung dazu ist deutlich: „Jedes Mal“ ohne MFA kann zu Anmeldeschleifen führen. Auf einem Terminalserver mit Office, Teams und Laufwerken, die alle auf SharePoint zugreifen, ist das der kürzeste Weg zu einer Belegschaft, die deinen Namen kennt.

Details und Beispiele findest du in der Dokumentation zu den Richtlinien für die adaptive Sitzungsdauer im bedingten Zugriff auf Microsoft Learn.

Die Einstellungen, die sich gegenseitig beißen

In vielen Mandanten liegen alte und neue Mechanismen übereinander. Microsoft ist dazu eindeutig: Die restriktivste Einstellung bestimmt, wann sich ein Benutzer erneut anmelden muss.

Einstellung	Was sie tut	Wechselwirkung laut Microsoft Learn
Angemeldet bleiben? (KMSI)	Beständiges Browser-Cookie nach Zustimmung des Benutzers	Gilt nur für den Browser; wird von der Richtlinie „Beständige Browsersitzung“ überschrieben
MFA speichern	Cookie für 1 bis 365 Tage nach „Nicht erneut fragen“	Verringert Abfragen im Web, erhöht sie bei Office-Clients, wenn der Wert unter 90 Tagen liegt; vor dem Einsatz der Anmeldehäufigkeit abschalten
Anmeldehäufigkeit (bedingter Zugriff)	Dauer bis zur erneuten Anmeldung, für Client und Browser	Empfohlener Weg mit Entra ID P1 oder P2

Beständige Browsersitzung (bedingter Zugriff)	Admin legt fest, ob der Browser angemeldet bleibt	Für nicht verwaltete oder gemeinsam genutzte Geräte nicht unbedingt wünschenswert
Konfigurierbare Tokenlebensdauer	Altes Verfahren für Sitzungs- und Aktualisierungstoken	Durch die Sitzungsverwaltung im bedingten Zugriff ersetzt; nicht parallel betreiben

FAKTEN · Das 14-Tage-Beispiel von Microsoft

Ist „Angemeldet bleiben“ aktiv und gleichzeitig „MFA speichern“ auf 14 Tage gesetzt, muss sich der Benutzer alle 14 Tage erneut anmelden, obwohl das beständige Cookie allein keine erneute Anmeldung im Browser verlangen würde. Die strengste Einstellung gewinnt.

Beständige Browsersitzung auf dem gemeinsam genutzten Server

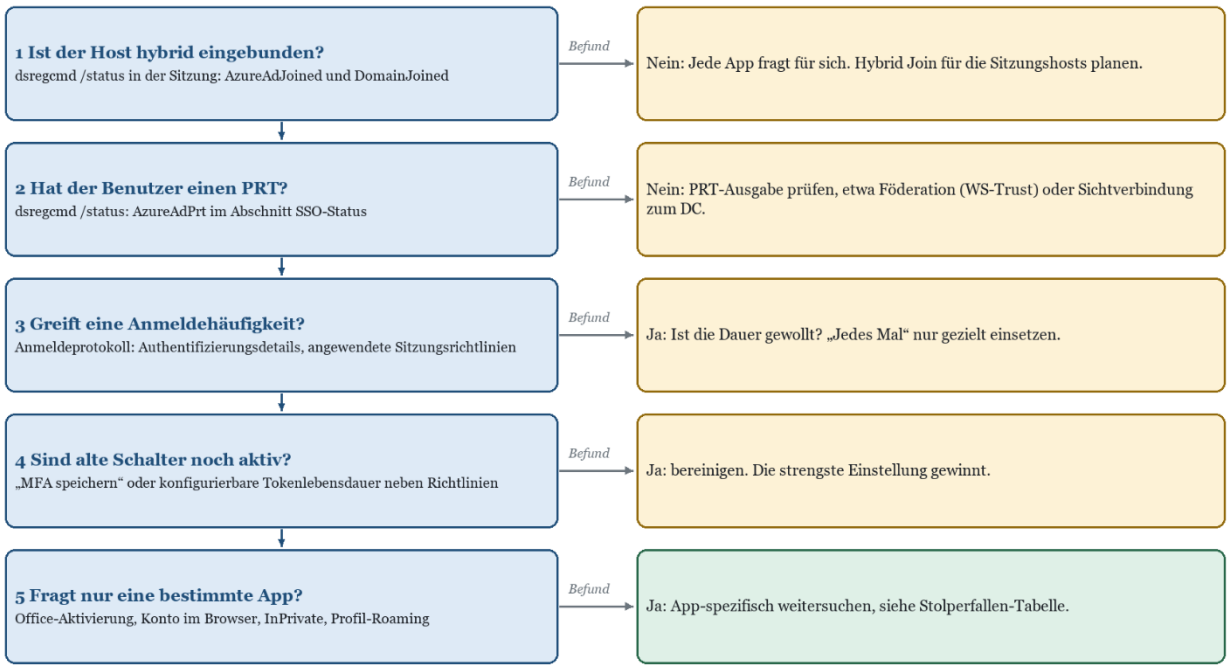
Für den Browser auf dem Sitzungshost gilt eine Besonderheit: Er ist gleichzeitig ein gemeinsam genutztes Gerät und ein sehr persönlicher Arbeitsplatz, denn das Browserprofil liegt im Benutzerprofil. Microsoft nennt den Zugriff von gemeinsam genutzten Geräten ausdrücklich als Szenario für eingeschränkte Sitzungsdauer. Ob du die beständige Browsersitzung auf den Hosts erlaubst, hängt also an deinem Profilkonzept. Auf einem hybrid eingebundenen Host holt sich Edge das SSO ohnehin über den PRT, sodass das Cookie weniger wichtig ist als auf einem nicht verwalteten Gerät. Im InPrivate-Modus funktioniert dieses Browser-SSO allerdings nicht.

Stolperfallen: „Warum fragt das Ding schon wieder?“

Die meisten Anmeldeschleifen auf Terminalservern haben eine von einer Handvoll Ursachen. Prüfe sie in einer festen Reihenfolge, von der Geräteidentität zur einzelnen App. Das spart dir Stunden in den Anmeldeprotokollen.

„Warum fragt das Ding schon wieder?“ Ein Prüfpfad in fünf Fragen

Von der Geräteidentität bis zur App: erst die billigen Fragen, dann die teuren



Skizze: Reihenfolge der Prüfung, kein Ersatz für die Anmeldeprotokolle

Prüfschritte mit Bordmitteln

1. **Sitzungshost prüfen:** Öffne in einer Benutzersitzung eine Eingabeaufforderung und führe dsregcmd /status aus. Im Gerätestatus sollten AzureAdJoined und DomainJoined auf YES stehen, im SSO-Status AzureAdPrt ebenfalls.
2. **Anmeldeprotokoll lesen:** Öffne im Microsoft Entra Admin Center das Anmeldeprotokoll des betroffenen Benutzers. Auf der Registerkarte mit den Authentifizierungsdetails siehst du, welche Sitzungsrichtlinien angewendet wurden, und in den Details zum bedingten Zugriff, welche Richtlinie die Abfrage ausgelöst hat.
3. **Alte Schalter suchen:** Prüfe, ob „MFA speichern“ oder konfigurierbare Tokenlebensdauern neben der Anmeldehäufigkeit aktiv sind, und bereinige sie.
4. **Richtlinie simulieren:** Spiele die Anmeldung mit dem What-If-Werkzeug für genau diesen Benutzer, diese App und diesen Host durch.
5. **App eingrenzen:** Fragt nur eine einzelne Anwendung, geh in die Stolperfallen-Tabelle.

Die üblichen Verdächtigen

Symptom	Häufige Ursache	Abhilfe mit Bordmitteln
Jede App fragt einzeln nach MFA	Host ohne Entra-Geräteidentität, kein PRT	Hybrid Join für die Sitzungshosts einrichten und prüfen
Abfragen trotz Hybrid Join	PRT wird nicht ausgestellt, etwa wegen Föderation ohne WS-Trust oder fehlender Sichtverbindung zum Domänencontroller	dsregcmd /status, Föderationsendpunkte und Netzweg prüfen
Abfrage alle paar Tage, obwohl keine Anmeldehäufigkeit gesetzt ist	„MFA speichern“ mit kurzem Wert	Einstellung abschalten, Anmeldehäufigkeit per Richtlinie nutzen
Endlose Anmeldeschleife	Anmeldehäufigkeit „Jedes Mal“ ohne MFA	Zeitbasierte Anmeldehäufigkeit für Microsoft-365-Apps verwenden
Office zeigt „Office aktivieren“	Aktivierung für gemeinsam genutzte Computer ohne SSO, Lizenztoken abgelaufen	SSO einrichten; Lizenztoken ist 30 Tage gültig und wird bei Nutzung erneuert
Abfragen nach Profilwechsel oder auf jedem Host neu	Broker- und Token-Ordner werden unpassend mitgenommen oder fehlen	Liste der nicht zu roamenden Ordner auf Microsoft Learn gegen dein Profilkonzept prüfen
Host taucht doppelt im Verzeichnis auf	Benutzer haben ihr Arbeitskonto auf dem Host registriert	BlockAADWorkplaceJoin per Richtlinie setzen

Profile und Token: was nie den Host verlassen darf

Für nicht persistente Desktops listet Microsoft Learn Ordner und Registrierungsschlüssel auf, die ein Profilwerkzeug niemals vom Gerät mitnehmen darf, darunter die Ordner TokenBroker, IdentityCache, OneAuth und das Paket Microsoft.AAD.BrokerPlugin unter %localappdata%. Auch das Gerätezertifikat des Arbeitskontos darf nicht roamen. Wer mit eigenen Roaming-Lösungen oder Profilmigrationswerkzeugen arbeitet, sollte diese Liste neben sein Profilkonzept legen. Die vollständige Aufstellung steht in Geräteidentität und Desktopvirtualisierung auf Microsoft Learn. Wie FSLogix und Benutzerprofil-Datenträger mit SharePoint-Dateien zusammenpassen, beschreiben Benutzerprofil-Datenträger oder FSLogix: was passt zu SharePoint-Dateien? und FSLogix und OneDrive: wenn die Profilcontainer explodieren.

Office und OneDrive als Sonderfälle

Microsoft 365 Apps holen sich auf dem Terminalserver über die Aktivierung für gemeinsam genutzte Computer ein Lizenztoken pro Benutzer und Host. Dieses Token ist 30 Tage gültig und wird automatisch erneuert, solange der Benutzer Office nutzt. Microsoft empfiehlt ausdrücklich SSO, damit Benutzer bei der Aktivierung seltener gefragt werden. Ohne SSO rät Microsoft, den Lizenzordner im Benutzerprofil mitwandern zu lassen. Welche Versionen von Microsoft 365 Apps auf welchem Server noch unterstützt sind, steht in Microsoft 365 Apps auf Windows Server 2022: was nach Oktober 2026 gilt und Windows Server 2025 als Terminalserver mit SharePoint-Dateien.

OneDrive verdient ein eigenes Kapitel, und das hat es auch: Warum die Sync-App auf dem Terminalserver gern nach der Anmeldung fragt und wie du das mit Bordmitteln abstellst, erklärt OneDrive fragt auf dem Terminalserver ständig nach der Anmeldung. Wer zusätzlich die Ordnersicherung nutzt, findet die Details in OneDrive-Ordnersicherung (Known Folder Move) auf dem Terminalserver.

CosyTrack.Drive unter denselben Richtlinien

Jetzt die Frage, die in jedem Projekt kommt: Was passiert mit den Laufwerken, wenn wir den bedingten Zugriff verschärfen? Die ehrliche Antwort ist unspektakulär. CosyTrack.Drive bindet SharePoint- und Teams-Bibliotheken sowie OneDrive als Windows-Laufwerksbuchstaben ein und greift dafür auf dieselben Microsoft-365-Ressourcen zu wie Office, Teams und die OneDrive-Sync-App. Für Entra ID ist Drive damit eine von mehreren Anwendungen in der Sitzung, auf die deine Richtlinien wirken. Es gibt keinen Sonderweg an deinen Richtlinien vorbei, und das ist aus Security-Sicht genau richtig.

Drive läuft auf Arbeitsplätzen und auf Terminalservern mit Remote Desktop Services gleichermaßen; auf dem Sitzungshost bekommt jeder Benutzer seine eigenen Laufwerke. Für deine Richtlinienplanung heißt das: Die Laufwerke auf dem Notebook unterliegen denselben Regeln wie Office auf dem Notebook, die Laufwerke auf dem Host denselben Regeln wie Office auf dem Host. Ein Konzept, zwei Einsatzorte.

Was du im Pilot prüfst

Wie sich Drive im Zusammenspiel mit deinen konkreten Richtlinien verhält, prüfst du am besten so, wie du jede andere App prüfst: im Pilot mit deiner eigenen Umgebung, mit echten Benutzerkonten, vom Sitzungshost aus. Nimm Drive in den Nur-Bericht-Lauf neuer Richtlinien auf und schau ins Anmeldeprotokoll, welche Richtlinien für die Zugriffe gegriffen haben.

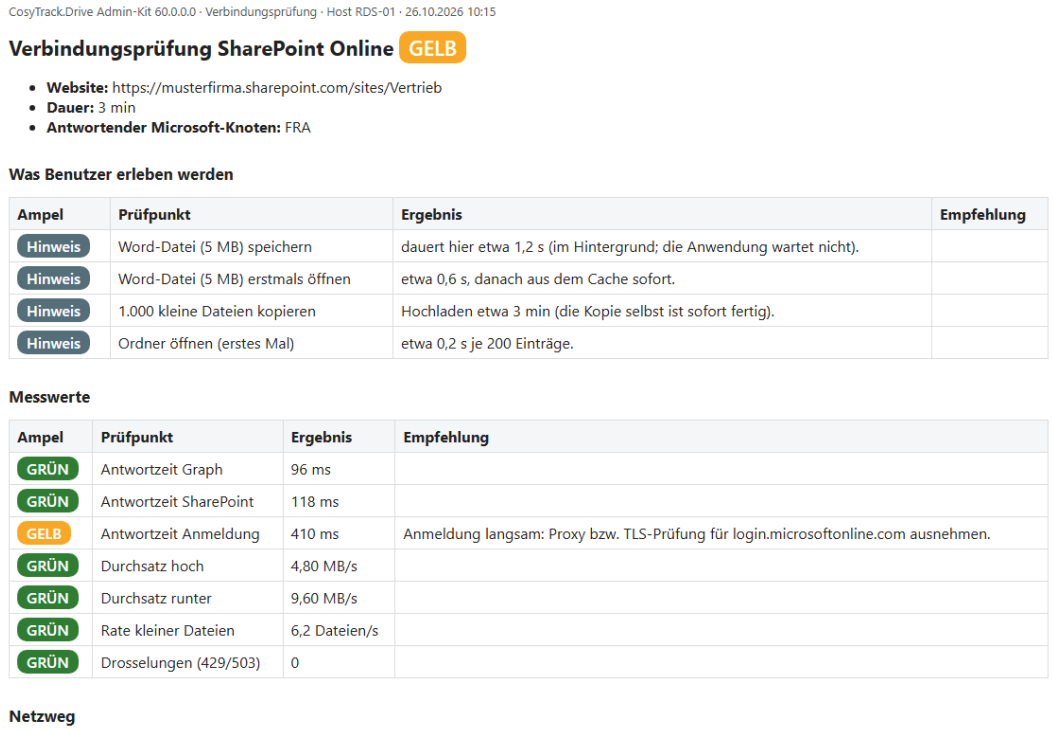
- **Gleiche Zielressourcen:** Richtlinien, die SharePoint Online und OneDrive betreffen, wirken auf alle Apps, die darauf zugreifen. Plane keine Ausnahme nur für eine Laufwerks-App.
- **Rechte zusätzlich begrenzen:** Pro Laufwerk legst du fest, ob es nur lesend oder lesend und schreibend eingebunden wird. Schreiben umfasst Speichern, Umbenennen, Löschen und Ordner anlegen. Das ersetzt keine Berechtigungen in SharePoint, verkleinert aber die Angriffsfläche auf gemeinsam genutzten Hosts. Mehr dazu in Nur lesen oder schreiben – Rechte pro Laufwerk.
- **Zentral steuern:** Konfiguriert wird Drive per GPO oder Intune, also über dieselben Wege, über die du auch BlockAADWorkplaceJoin und die Office-Aktivierung verteilst. Für Tests gibt es zusätzlich eine Konfigurations-App.

Wie die Richtlinien für Drive im Einzelnen aussehen, steht in CosyTrack.Drive per GPO und Intune steuern.

Netzweg und Anmeldung messbar machen

Zur aktuellen Generation 60 von Drive, die komplett neu gebaut wurde, gehört ein Admin-Kit. Für die Security-Perspektive ist vor allem die Verbindungsprüfung interessant: Sie misst den Weg vom

Host zu SharePoint und Microsoft Graph und weist Antwortzeiten einzeln aus, auch für den Anmeldeschritt. Liegt ein Proxy mit TLS-Prüfung zwischen Host und Microsoft 365, siehst du das hier, bevor es als „Drive ist langsam“ oder „die Anmeldung hängt“ im Ticketsystem landet. Den Bericht kannst du als Beleg für die Freigaben an der Firewall verwenden.



CosyTrack.Drive Admin-Kit 60.0.0.0 · Verbindungsprüfung · Host RDS-01 · 26.10.2026 10:15

Verbindungsprüfung SharePoint Online GELB

- **Website:** https://musterfirma.sharepoint.com/sites/Vertrieb
- **Dauer:** 3 min
- **Antwortender Microsoft-Knoten:** FRA

Was Benutzer erleben werden

Ampel	Prüfpunkt	Ergebnis	Empfehlung
Hinweis	Word-Datei (5 MB) speichern	dauert hier etwa 1,2 s (im Hintergrund; die Anwendung wartet nicht).	
Hinweis	Word-Datei (5 MB) erstmals öffnen	etwa 0,6 s, danach aus dem Cache sofort.	
Hinweis	1.000 kleine Dateien kopieren	Hochladen etwa 3 min (die Kopie selbst ist sofort fertig).	
Hinweis	Ordner öffnen (erstes Mal)	etwa 0,2 s je 200 Einträge.	

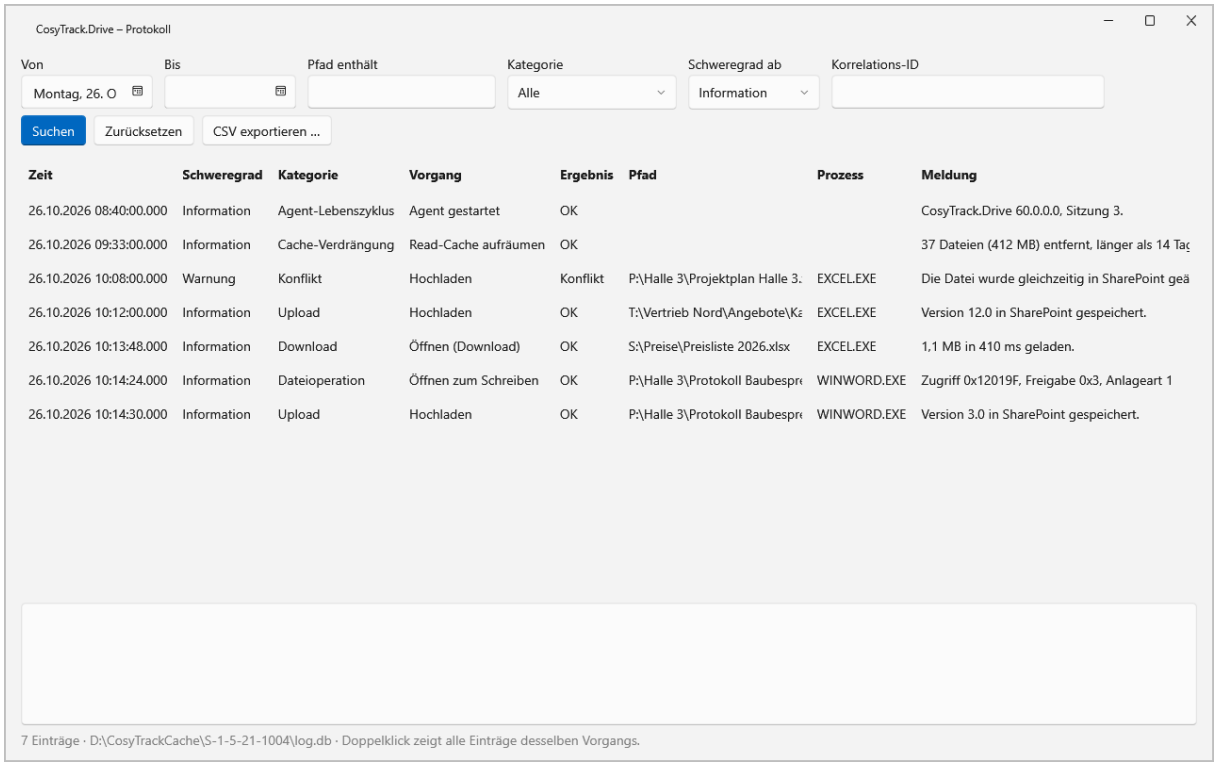
Messwerte

Ampel	Prüfpunkt	Ergebnis	Empfehlung
GRÜN	Antwortzeit Graph	96 ms	
GRÜN	Antwortzeit SharePoint	118 ms	
GELB	Antwortzeit Anmeldung	410 ms	Anmeldung langsam: Proxy bzw. TLS-Prüfung für login.microsoftonline.com ausnehmen.
GRÜN	Durchsatz hoch	4,80 MB/s	
GRÜN	Durchsatz runter	9,60 MB/s	
GRÜN	Rate kleiner Dateien	6,2 Dateien/s	
GRÜN	Drosselungen (429/503)	0	

Netzweg

Hier liest du im Bericht der Verbindungsprüfung, dass die Anmeldung gelb steht und Proxy oder TLS-Prüfung für den Anmeldedienst ausgenommen werden sollten.

Im Betrieb protokolliert Drive nachvollziehbar, was passiert. Im Protokoll filterst du nach Zeitraum, Pfad, Kategorie und Schweregrad. Das ist praktisch, wenn du eine Meldung aus dem Anmeldeprotokoll von Entra ID mit den Dateivorgängen in der Sitzung abgleichen willst.

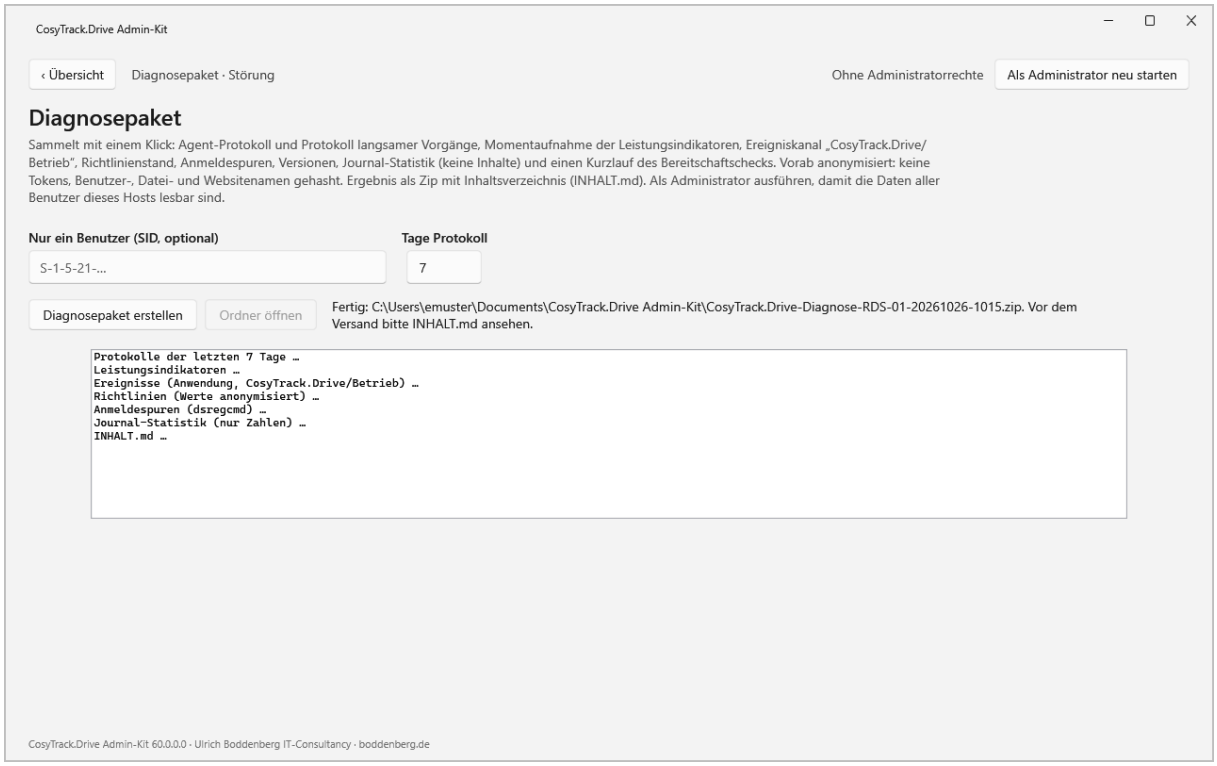


So grenzt du im Protokoll von CosyTrack.Drive Uploads, Downloads und Konflikte nach Zeitraum und Schweregrad ein.

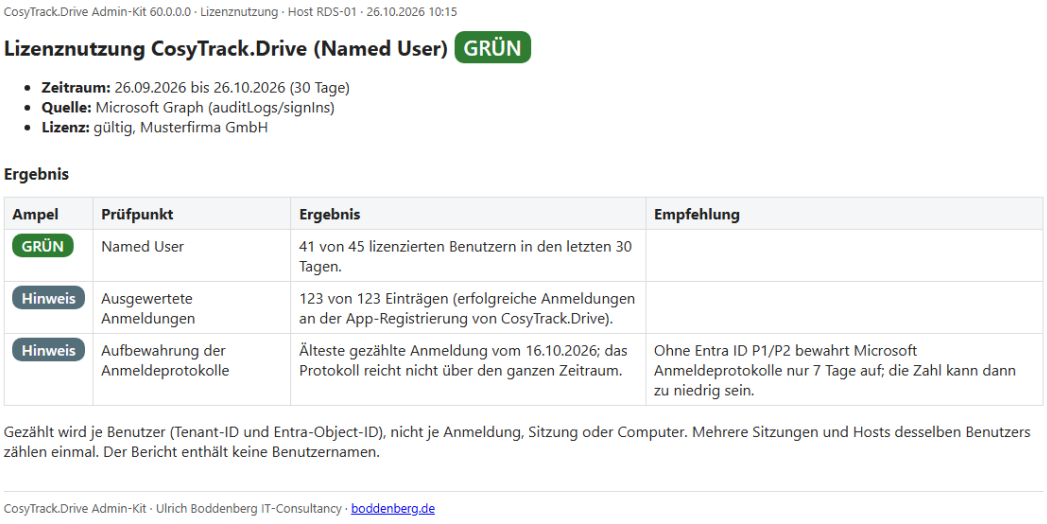
Für Leistungsfragen gibt es Leistungszähler, von übertragenen Dateien bis zur Übertragungsgeschwindigkeit, als Windows-Leistungsindikatoren und im Statusfenster. Wie du sie auswertest, steht in Microsoft-365-Anbindung messen mit Leistungszählern.

Diagnose und Lizenznutzung für den Audit

Wenn doch etwas klemmt, erstellt das Admin-Kit ein Diagnosepaket mit Protokollen, Leistungsindikatoren, Ereignissen und Richtlinien, das du an den Support weitergeben kannst. Die Seite „Lizenz und Lizenznutzung“ wertet die Anmeldeprotokolle über Microsoft Graph aus und zeigt, wie viele Benutzer im gewählten Zeitraum aktiv waren. Drive wird pro Named User lizenziert; der Bericht hilft dir, die Lizenzzahl gegen die tatsächliche Nutzung zu halten, und ist nebenbei ein schöner Anlass, die Aufbewahrungsdauer deiner Anmeldeprotokolle zu prüfen.



So erstellst du im Admin-Kit ein Diagnosepaket mit Protokollen, Ereignissen und Richtlinien für den Support.



So liest du den Lizenznutzungsbericht: Die Ampel zeigt die Gesamtlage, die Hinweise zeigen, wie vollständig die Anmeldeprotokolle sind.

AUS DER PRAXIS · Filialisierter Lebensmittelbetrieb

Ein filialisierter Lebensmittelbetrieb betreibt die Verwaltung auf einer kleinen RDS-Farm, die Marktleitungen arbeiten an Notebooks. Nach der Einführung einer MFA-Richtlinie für alle Benutzer

häufen sich auf den Sitzungshosts die Abfragen: Outlook, Teams und die Laufwerke fragen jeweils einzeln. dsregcmd /status zeigt das Problem in Sekunden: Die Hosts stehen in der Domäne, sind aber nicht hybrid eingebunden. Nach Hybrid Join, BlockAADWorkplaceJoin per GPO und dem Abschalten von „MFA speichern“ zugunsten einer zeitbasierten Anmeldehäufigkeit bleibt eine Abfrage pro Anmeldung übrig. Die Laufwerke auf Hosts und Notebooks laufen unter denselben Richtlinien wie Office, ohne Ausnahme.

Wenn du Richtlinien, Sitzungshosts und Laufwerkskonzept in einem Zug sauber aufstellen willst, ist die Beratung zu CosyTrack.Drive der richtige Ansprechpartner; dort gibt es auch Test und Angebot. Den Weg vom Pilot bis zum Rollout beschreibt Einführungsfahrplan für CosyTrack.Drive.

FAQ: Bedingter Zugriff auf dem Terminalserver

Kann ich für Terminalserver „Gerät muss als konform markiert sein“ verlangen?

Nicht sinnvoll. Laut Microsoft Learn unterstützt dieses Steuerelement Windows 10 und neuer, iOS, Android, macOS und Linux Ubuntu mit Intune-Registrierung. Für domänenverbundene Sitzungshosts ist „Microsoft Entra hybrid eingebundenes Gerät verlangen“ das passende Gerätesignal, gern als Oder-Verknüpfung mit der Konformität für Clients.

Warum fragt jede App auf dem Terminalserver einzeln nach MFA?

Meist fehlt dem Host eine Geräteidentität in Entra ID. Ohne sie gibt es keinen PRT, und jede App holt sich ihr eigenes Aktualisierungstoken. Microsoft Learn beschreibt genau dieses Verhalten. Abhilfe schafft Hybrid Join für die Sitzungshosts.

Wie lange gilt eine Anmeldung standardmäßig?

Die Standardkonfiguration von Microsoft Entra ID ist ein rollierendes Fenster von 90 Tagen. Ein PRT ist 90 Tage gültig und wird bei aktiver Nutzung laufend erneuert. Kürzere Zeiträume setzt du mit der Anmeldehäufigkeit im bedingten Zugriff.

Sollte ich auf Terminalservern „Jedes Mal“ als Anmeldehäufigkeit setzen?

Für Microsoft-365-Apps nicht. Microsoft empfiehlt dafür eine zeitbasierte Anmeldehäufigkeit und warnt, dass „Jedes Mal“ ohne MFA zu Anmeldeschleifen führen kann. „Jedes Mal“ eignet sich für wenige, besonders sensible Anwendungen.

Hilft ein vertrauenswürdiger Standort für das Firmennetz?

Auf dem Terminalserver nur bedingt. Alle Sitzungen eines Hosts kommen mit derselben ausgehenden Adresse, unabhängig davon, wo der Benutzer tatsächlich sitzt. Der Standort ersetzt deshalb weder MFA noch ein Gerätesignal.

Was bewirkt BlockAADWorkplaceJoin?

Der Registrierungswert verhindert, dass Benutzer ihr Arbeitskonto auf einem domänenverbundenen Gerät zusätzlich als Entra-registriertes Gerät hinzufügen. Microsoft Learn nennt ihn in der Planung zu Hybrid Join und empfiehlt ihn für nicht persistente Desktops.

Gelten meine Richtlinien auch für CosyTrack.Drive?

Ja. Drive greift auf SharePoint, Teams-Bibliotheken und OneDrive zu, und Richtlinien für diese Ressourcen wirken auf jede App, die darauf zugreift. Wie sich Drive mit deinen konkreten Richtlinien verhält, prüfst du im Pilot mit deiner eigenen Umgebung.

Läuft CosyTrack.Drive nur auf Terminalservern?

Nein. Drive läuft auf Arbeitsplätzen und auf Terminalservern gleichermaßen, gesteuert per GPO oder Intune. Auf dem Sitzungshost hat jeder Benutzer seine eigenen Laufwerke.

Fazit: Erst die Geräteidentität, dann die Richtlinie

Bedingter Zugriff auf dem Terminalserver scheitert selten an zu wenig Sicherheit, sondern an Richtlinien, die für ein anderes Gerät geschrieben wurden. Wer den Sitzungshost als das behandelt, was er ist, nämlich ein gemeinsam genutztes, domänenverbundenes Gerät mit einer einzigen IP-Adresse, kommt mit wenigen Bausteinen aus: Hybrid Join statt Konformität, MFA am Benutzer statt Vertrauen in den Standort, eine zeitbasierte Anmeldehäufigkeit statt historisch gewachsener Schalter und BlockAADWorkplaceJoin als Hygienemaßnahme.

Alles, was in der Sitzung auf Microsoft 365 zugreift, läuft dann unter denselben Regeln: Office, Teams, OneDrive und die Laufwerke von CosyTrack.Drive, am Arbeitsplatz wie auf dem Terminalserver. Grundlagen zu Websites und Bibliotheken findest du im Kompetenzbereich SharePoint, für Berechtigungen und Informationsarchitektur hilft die SharePoint-Beratung, und damit dein Team Laufwerke und Admin-Kit im Betrieb sicher beherrscht, gibt es Schulung und Onboarding für CosyTrack.Drive. Dann fragt das Ding am Montag genau einmal. Und das ist die Art von Langeweile, für die man Security-Leute bezahlt.

WEITERLESEN · Weiter im Thema

› OneDrive fragt auf dem Terminalserver ständig nach der Anmeldung
› SharePoint als Laufwerk auf dem Terminalserver
› OneDrive auf dem Terminalserver
› Windows Server 2025 als Terminalserver mit SharePoint-Dateien
› SharePoint-Laufwerke auf Azure Virtual Desktop und Windows 365
› SharePoint als Laufwerk unter Citrix Virtual Apps
› Benutzerprofil-Datenträger oder FSLogix: was passt zu SharePoint-Dateien?
› FSLogix und OneDrive: wenn die Profilcontainer explodieren
› CosyTrack.Drive per GPO und Intune steuern
› Microsoft-365-Anbindung messen mit Leistungszählern