

Microsoft 365 von Federated auf Managed umstellen – mit Staged Rollout

ADFS · Microsoft 365 · Staged Rollout

Von Federated auf Managed – ohne dass am Montag das Telefon brennt

Password Hash Sync vorbereiten, Pilotgruppen umleiten, Domäne umstellen und den Rückweg so planen, dass du ihn nie brauchst.



boddenberg.de

WISSEN

Grundlagen, Architektur und alle Praxisbeiträge rund um ADFS an einem Ort.

› [Active Directory Federation Services](#)

BERATUNG

Du willst Microsoft 365 von der Farm lösen, aber nicht am Montagmorgen 4.000 Tickets erklären? Wir planen die Wellen mit.

› [Consulting zu ADFS](#)

SCHULUNG

Staged Rollout, Domänenumstellung und Rückfall einmal im Labor durchspielen – mit Absicht kaputt machen inklusive.

› [ADFS-Schulungen](#)

Es gibt diesen einen Moment im Leben einer ADFS-Farm, in dem jemand im Lenkungsreis fragt: „Brauchen wir das eigentlich noch für Microsoft 365?“ Meist kommt die Frage drei Tage nach einem abgelaufenen Token-Signing-Zertifikat, und meist stellt sie jemand, der in jener Nacht nicht wach war. Die ehrliche Antwort lautet: Für die Anmeldung an Microsoft 365 brauchst du die Farm in den allermeisten Fällen nicht mehr. Die ebenso ehrliche Zusatzantwort: Wer die Domäne an einem Freitagnachmittag einfach umschaltet, lernt am Montag sehr viele Menschen aus der Buchhaltung persönlich kennen.

In diesem Beitrag geht es um genau einen Handgriff, und zwar so, wie Admins ihn suchen: Microsoft 365 von ADFS auf Managed umstellen. Du bereitest Password Hash Sync oder Pass-Through Authentication samt Seamless SSO vor, schickst Pilotgruppen per Staged Rollout an der Farm vorbei, stellst danach die Domäne mit Microsoft Graph PowerShell oder Entra Connect um und hältst die ganze Zeit einen Rückweg offen. Dazu kommt ein Kapitel über die Geräte, denn Hybrid Join ist der Teil, über den in den meisten Anleitungen ein höfliches Schweigen liegt. Was ADFS grundsätzlich ist und warum es in vielen Unternehmen seit über zehn Jahren zuverlässig läuft, steht auf der Übersichtsseite [Active Directory Federation Services](#). Hier setzen wir voraus, dass deine Farm läuft und Entra Connect bereits synchronisiert.

FAKTEN – Federated auf Managed in Kürze

Staged Rollout schickt einzelne, synchronisierte Benutzer per Sicherheitsgruppe an ADFS vorbei zur Cloud-Authentifizierung, während die Domäne föderiert bleibt. Es ist laut Microsoft ausdrücklich als temporäres Testwerkzeug gedacht, nicht als Dauerzustand.

Pro Funktion – Password Hash Sync, Pass-Through Authentication, Seamless SSO – sind höchstens zehn Gruppen möglich. Verschachtelte und dynamische Gruppen werden nicht unterstützt, Kontakte in der Gruppe blockieren das Hinzufügen. Beim ersten Hinzufügen einer Gruppe sollten es höchstens 200 Mitglieder sein.

Für Staged Rollout brauchst du mindestens die Rolle Hybrid Identity Administrator, für Seamless SSO zusätzlich Domänenadministrator-Rechte im jeweiligen AD-Forest.

Die eigentliche Domänenenumstellung erledigt Staged Rollout nicht. Die machst du mit Update-MgDomain oder über Entra Connect („Benutzeranmeldung ändern“). Microsoft plant dafür bis zu 60 Minuten ein.

Microsoft empfiehlt Password Hash Sync als Cloud-Authentifizierung – auch dann, wenn du am Ende Pass-Through Authentication wählst, ist der Hash-Sync als Reserve sinnvoll.

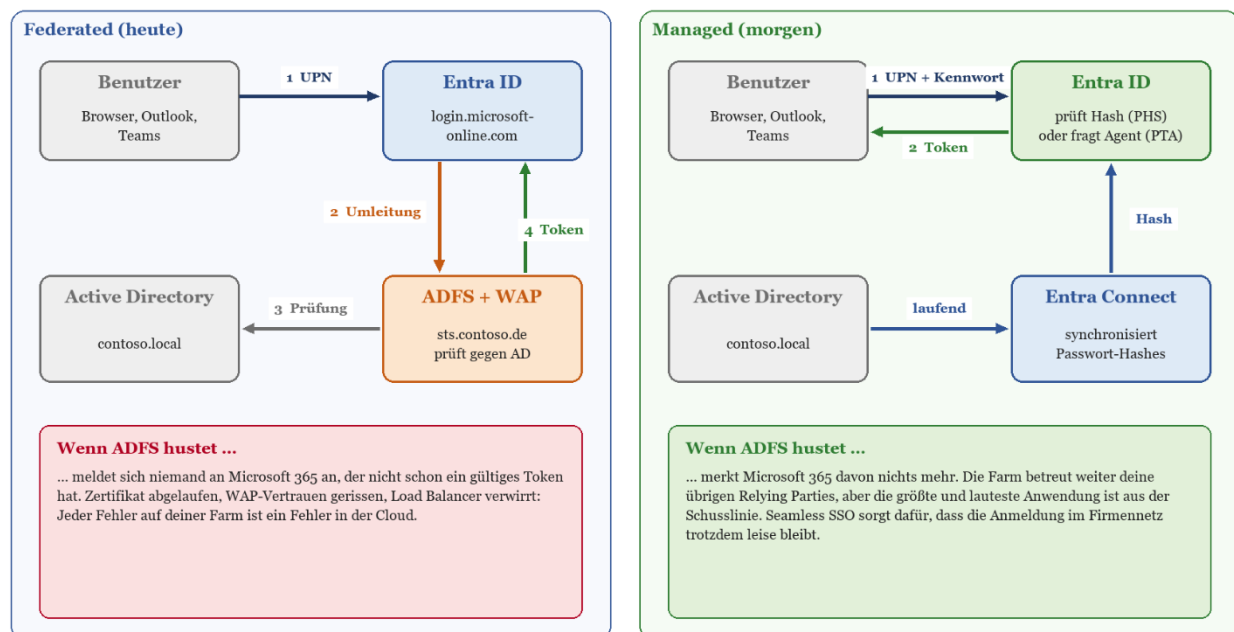
Warum umstellen – und warum nicht in einem Rutsch

Microsoft 365 ist in fast jeder ADFS-Farm die Relying Party mit den meisten Anmeldungen, den lautesten Benutzern und dem kürzesten Geduldsfaden. Solange die Domäne föderiert ist, hängt jede neue Anmeldung an Exchange Online, Teams oder SharePoint Online an deiner Farm, deinem Web Application Proxy, deinem Load Balancer und deinen Zertifikaten. Das funktioniert – oft seit Jahren, oft hervorragend. Aber jeder dieser Bausteine ist ein Grund, warum ein ruhiger Dienstagabend zu einer Telefonkonferenz werden kann.

Dazu kommt die Sicherheitsseite. Eine föderierte Domäne vertraut jedem Token, das mit dem Token-Signing-Zertifikat deiner Farm signiert ist. Wer dieses Zertifikat stiehlt, stellt sich seine Token selbst aus – das Stichwort heißt Golden SAML und ist im Beitrag [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#) ausführlich beschrieben. Nach der Umstellung prüft Entra ID selbst, kann Smart Lockout, Erkennung kompromittierter Anmeldedaten und Conditional Access ohne Umweg anwenden, und die Farm ist für Microsoft 365 schlicht nicht mehr zuständig.

Skizze 1: Wohin der Browser abbiegt – vorher und nachher

Federated: Entra ID schickt zu ADFS. Managed: Entra ID prüft selbst, ADFS bekommt Microsoft 365 nicht mehr zu sehen.



Skizze 1: Der Anmeldefluss vor und nach der Umstellung

Was sich ändert und was nicht

Wichtig für die Erwartungshaltung im Projekt: Du schaltest nicht ADFS ab. Du nimmst der Farm nur eine Aufgabe weg. Alle anderen Relying Parties – das SAML-Reisekostenportal, die SharePoint-Server-Farm, die Partneranbindung – laufen unverändert weiter. Wer ADFS danach

ganz loswerden will, braucht ein eigenes Projekt, beginnend mit [Relying Parties inventarisieren – die Bestandsaufnahme vor der Entra-Migration](#). Die Domänenenumstellung ist Schritt eins, nicht der letzte.

Thema	Federated (heute)	Managed (nach der Umstellung)
Wer prüft das Kennwort?	ADFS gegen Active Directory	Entra ID per Hash (PHS) oder über Agenten gegen AD (PTA)
Anmeldeseite extern	ADFS-Seite unter sts.contoso.de, ggf. mit onload.js angepasst	Entra-Anmeldeseite mit Unternehmensbranding; onload.js-Tricks entfallen
SSO im Firmennetz	Windows-integrierte Authentifizierung an der Farm	Primary Refresh Token auf Windows 10/11, Seamless SSO für Browser und ältere Szenarien
MFA	ADFS-Adapter oder Entra-MFA mit federatedIdpMfaBehavior	Entra-MFA über Conditional Access
Zugriffsregeln	Claim Rules, Access Control Policies auf der M365-RP	Conditional Access, Authentifizierungsstärken
Ausfallrisiko	Farm, WAP, Load Balancer, Zertifikate	Entra Connect (PHS) bzw. PTA-Agenten
Kennwortänderung	sofort wirksam, Prüfung gegen AD	bei PHS bis etwa zwei Minuten Verzögerung, bei PTA sofort

Tabelle 1: Was sich durch die Umstellung ändert

WICHTIG — Erst die Regeln, dann der Schalter

Hängen an der Microsoft-365-Relying-Party eigene Autorisierungsregeln – etwa „nur aus dem Firmennetz“ oder „nur Gruppe X darf Exchange Online“ –, verschwinden diese mit der Umstellung kommentarlos. Übersetze sie vorher in Conditional Access. Wie das sauber geht, steht in [Claim Rules nach Conditional Access übersetzen](#).

Vorbereitung: PHS oder PTA, Seamless SSO und eine ehrliche Bestandsaufnahme

Die Vorbereitung ist der Teil, der am wenigsten spektakulär aussieht und am meisten entscheidet. Alles, was du hier tust, hat keinen Einfluss auf die laufende Anmeldung: Solange die Domäne föderiert ist und niemand in einer Staged-Rollout-Gruppe steckt, schickt Entra ID weiterhin alle Benutzer zur Farm. Du kannst also in Ruhe arbeiten. Das ist ungewohnt und sollte genossen werden.

Bestandsaufnahme und Sicherung

Bevor du irgendetwas umstellst, dokumentierst du, wie es heute ist. Das ist nicht Bürokratie, sondern die Grundlage für den Rückweg. Auf der Entra-Seite interessieren dich alle Domänen und ihre Föderationseinstellungen, insbesondere PreferredAuthenticationProtocol, federatedIdpMfaBehavior und PromptLoginBehavior. Auf der ADFS-Seite sicherst du die Microsoft-365-Relying-Party samt Claim Rules und, wenn noch nicht geschehen, die ganze Farm.

```
# Entra-Seite: Domänen und Föderationseinstellungen dokumentieren
Connect-MgGraph -Scopes "Domain.Read.All","Directory.Read.All"
Get-MgDomain | Select-Object Id, AuthenticationType, IsVerified

$fed = Get-MgDomainFederationConfiguration -DomainId "contoso.de"
$fed | Format-List DisplayName, IssuerUri, PassiveSignInUri, ActiveSignInUri, `
    MetadataExchangeUri, SignOutUri, PreferredAuthenticationProtocol, `
    FederatedIdpMfaBehavior, PromptLoginBehavior
$fed | Export-Clixml "C:\Migration\contoso.de-federation.xml"
```

```
# ADFS-Seite (auf einem Farmknoten): Microsoft-365-Relying-Party sichern
$rp = Get-AdfsRelyingPartyTrust -Identifizier "urn:federation:MicrosoftOnline"
$rp | Export-Clixml "C:\Migration\M365-RelyingPartyTrust.xml"
$rp.IssuanceTransformRules | Out-File "C:\Migration\M365-Transform.txt" -Encoding utf8
$rp.IssuanceAuthorizationRules | Out-File "C:\Migration\M365-Authorization.txt" -Encoding utf8
```

Listing 1: Ist-Zustand sichern – die Grundlage für jeden Rückfall

TIPP – Den Namen der Relying Party nicht raten

Je nachdem, wann und womit die Föderation eingerichtet wurde, heißt die Microsoft-365-Relying-Party „Microsoft Office 365 Identity Platform“, „... Worldwide“ oder irgendwann von jemandem umbenannt. Der Bezeichner urn:federation:MicrosoftOnline ist dagegen verlässlich. Deshalb fragt Listing 1 per -Identifizier und nicht per -Name ab.

Wer die Farm noch nie vollständig gesichert hat, holt das jetzt nach: [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#).

Password Hash Sync oder Pass-Through Authentication?

Die Gretchenfrage jedes Projekts. Die kurze Version: Microsoft empfiehlt Password Hash Sync, und in der Praxis spricht selten etwas Belastbares dagegen. Synchronisiert wird nicht das Kennwort und auch nicht der Hash aus dem AD, sondern ein daraus abgeleiteter, mehrfach gehashter Wert. Die Anmeldung funktioniert auch dann, wenn dein Rechenzentrum gerade unter Wasser steht. Pass-Through Authentication prüft dagegen jedes Kennwort live über Agenten gegen deine Domänencontroller – sinnvoll, wenn eine Richtlinie verbietet, dass irgendetwas Hash-Ähnliches das Haus verlässt, oder wenn AD-Kontosperren und Anmeldezeiten sofort greifen müssen.

Kriterium	Password Hash Sync	Pass-Through Authentication
Abhängigkeit vom eigenen RZ	keine für die Anmeldung, nur für die Synchronisation	hoch: ohne erreichbare Agenten und DCs keine Anmeldung
Infrastruktur	läuft auf dem Entra-Connect-Server mit	mindestens zwei, besser drei Agenten auf eigenen Servern
Gesperrte oder abgelaufene AD-Konten	wirken mit Synchronisationsverzögerung	wirken sofort, weil der DC live gefragt wird
Erkennung kompromittierter Anmeldedaten	ja, Abgleich mit bekannten Leaks möglich	nur, wenn PHS zusätzlich aktiv ist
Ablaufende Kennwörter	ohne zusätzliche Einstellung kein Kennwortablauf in der Cloud	AD-Richtlinie greift direkt
Typischer Einwand	„Hashes in die Cloud? Nie!“ – meist ohne Kenntnis des Verfahrens	„Wir wollen alles im Haus“ – bis der Agent-Server patcht

Tabelle 2: PHS und PTA im Vergleich – und warum PHS fast immer mitläuft

WICHTIG – PHS auch dann einschalten, wenn du PTA wählst

Selbst wenn die Anmeldung künftig über Pass-Through Authentication läuft, lohnt sich Password Hash Sync als Reserve: Fallen alle PTA-Agenten aus, kannst du auf PHS umschalten, statt auf die Wiederbelebung der Agenten zu warten. Und Leaked-Credential-Erkennung bekommst du ohnehin nur mit synchronisierten Hashes.

Password Hash Sync aktivierst du im Entra-Connect-Assistenten unter „Optionale Features“. Das ändert an der Anmeldung nichts, solange die Domäne föderiert ist – die Hashes liegen dann einfach bereit. Entscheidend ist, dass mindestens ein vollständiger Synchronisationszyklus gelaufen ist, bevor der erste Pilotnutzer umgeleitet wird. Sonst testet dein Pilot ein Kennwort, das Entra ID noch gar nicht kennt, und du testest die Frustrationstoleranz der IT-Leitung.

```
# Auf dem Entra-Connect-Server: Zustand der Kennwort-Hash-Synchronisation prüfen
Import-Module ADSyncDiagnostics
Invoke-ADSyncDiagnostics -PasswordSync

# Synchronisationsplan und letzter Lauf
Get-ADSyncScheduler
```

Listing 2: Ist die Hash-Synchronisation durchgelaufen?

WARNUNG — Kennwortablauf und UPN-Änderungen nicht vergessen

Benutzer, die per Password Hash Sync in der Cloud authentifizieren, bekommen standardmäßig keinen Kennwortablauf aus der Cloud. Wer das will, schaltet CloudPasswordPolicyForPasswordSyncedUsersEnabled ein – dann gelten fest 90 Tage ab dem Setzen des Kennworts im AD, ohne Anpassungsmöglichkeit.

Außerdem muss die Synchronisationsfunktion synchronizeUpnForManagedUsersEnabled aktiv sein, sonst übernimmt Entra ID UPN-Änderungen lizenzierter Benutzer in verwalteten Domänen nicht. Prüfen kannst du das mit Get-MgDirectoryOnPremiseSynchronization.

Seamless SSO: leise Anmeldung im Firmennetz

Ohne ADFS fehlt im Firmennetz zunächst die Windows-integrierte Anmeldung, die deine Benutzer seit Jahren für selbstverständlich halten. Auf Windows 10 und 11 übernimmt das der Primary Refresh Token, sofern die Geräte hybrid oder in Entra ID eingebunden sind. Für Browser-Szenarien und alles, was nicht über den PRT läuft, gibt es Seamless SSO: Entra Connect legt im AD ein Computerkonto namens AZUREADSSOACC an, dessen Kerberos-Schlüssel mit Entra ID geteilt wird. Der Browser holt sich ein Kerberos-Ticket für eine Microsoft-URL, und Entra ID meldet den Benutzer still an. Wer verstehen will, warum das manchmal doch nach dem Kennwort fragt, ist bei [Microsoft Kerberos](#) richtig.

```
# Auf dem Entra-Connect-Server, PowerShell als Administrator
cd "$env:ProgramFiles\Microsoft Azure Active Directory Connect"
Import-Module .\AzureADSSO.psd1
New-AzureADSSOAuthenticationContext          # Anmeldung als Hybrid Identity Administrator
Get-AzureADSSOStatus | ConvertFrom-Json      # zeigt, für welche Forests SSO aktiv ist

$creds = Get-Credential                     # Domänenadministrator des Ziel-Forests
Enable-AzureADSSOForest -OnPremCredentials $creds
```

Listing 3: Seamless SSO pro Forest einschalten – wirkt nur für Pilotnutzer, solange die Domäne föderiert ist

FAKTEN — Der Name täuscht

Das Modul AzureADSSO.psd1 liegt im Programmverzeichnis von Entra Connect und hat mit dem ausgemusterten AzureAD-PowerShell-Modul nichts zu tun – es heißt nur noch so. Es ist der von Microsoft dokumentierte Weg, Seamless SSO zu verwalten.

Seamless SSO verlangt, dass die Anmelde-URL von Entra ID im Browser der Zone „Lokales Intranet“ zugeordnet ist. Das verteilst du per Gruppenrichtlinie, bevor die erste Pilotgruppe startet.

Den Kerberos-Schlüssel des Kontos AZUREADSSOACC solltest du laut Microsoft mindestens alle 30 Tage erneuern. Das passiert nicht automatisch – also in den Betriebskalender damit.

Conditional Access, MFA und Branding vorziehen

Der Pilotnutzer landet nach der Umleitung auf der Entra-Anmeldeseite. Dort sollte er sein Firmenlogo sehen und nicht das Microsoft-Standardbild, sonst hältst du deinen eigenen Pilotversuch für Phishing – zu Recht. Hinterlege also vorher das Unternehmensbranding. Wichtiger noch: Wenn die MFA heute auf ADFS stattfindet, muss sie für Pilotnutzer vorher in Entra ID greifen. Conditional-Access-Richtlinien für MFA, die Blockade von Legacy-

Authentifizierung und die kombinierte Registrierung der Authentifizierungsmethoden gehören vor Welle 1, nicht danach. Wie die beiden MFA-Welten in der Übergangszeit zusammenspielen, beschreibt [ADFS mit Entra-MFA koppeln – Adapter, Zertifikat und Fallstricke](#).

Staged Rollout mit Pilotgruppen

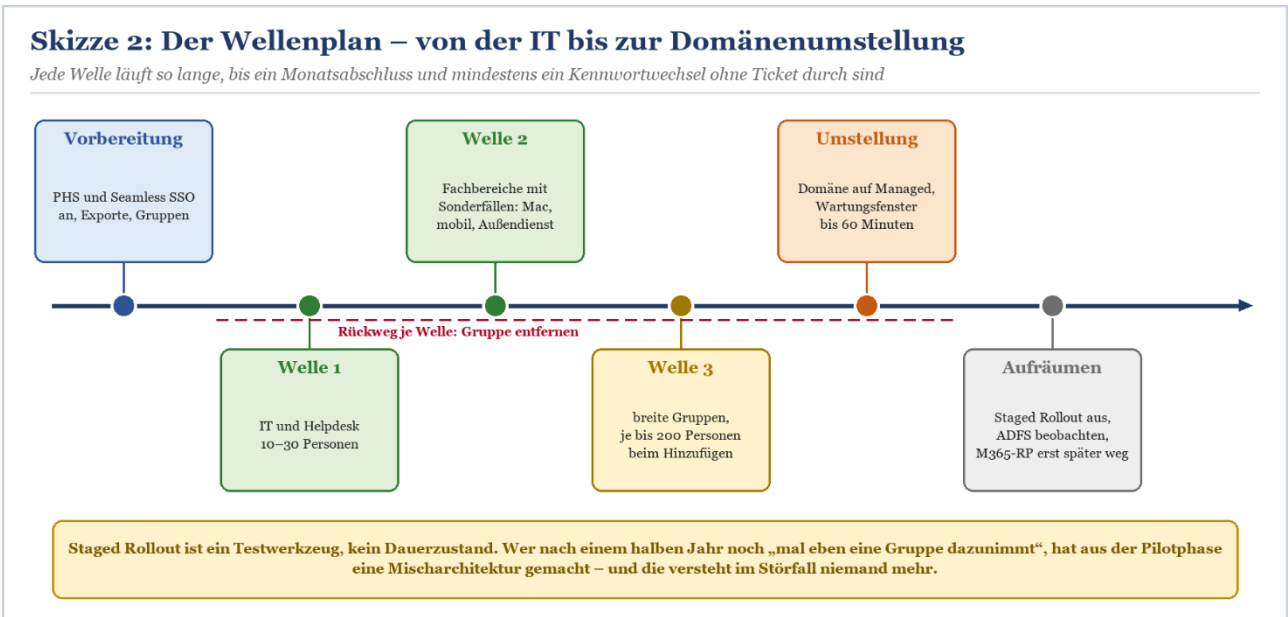
Staged Rollout ist der Grund, warum diese Umstellung heute kein Hochseilakt mehr ist. Statt die ganze Domäne umzuschalten, legst du Sicherheitsgruppen fest, deren Mitglieder Entra ID künftig selbst authentifiziert – alle anderen landen weiter auf der Farm. Du testest also mit echten Menschen, echten Geräten und echten Anwendungen, aber mit einem Notausgang, der nur einen Mausklick entfernt ist.

Die Gruppen richtig schneiden

Nimm Cloud-Gruppen, keine aus dem AD synchronisierten Gruppen. Das empfiehlt Microsoft selbst, weil du sonst bei jeder Änderung auf den nächsten Sync-Zyklus wartest. Halte die Gruppen flach – verschachtelte und dynamische Gruppen funktionieren nicht – und bleib beim ersten Hinzufügen unter 200 Mitgliedern. Danach kannst du weitere Benutzer direkt in die Gruppe aufnehmen. Wichtig fürs Timing: Wird eine neue Gruppe hinzugefügt, gelten deren Mitglieder sofort als Pilotnutzer. Änderst du die Mitgliedschaft einer bereits eingetragenen Gruppe, kann es bis zu 24 Stunden dauern.

Welle	Wer	Warum diese Leute	Dauer (Richtwert)
1	IT-Betrieb, Helpdesk, Projektteam	verzeihen Fehler, melden sie präzise und wissen, was ein Sign-in-Log ist	zwei Wochen
2	Fachbereiche mit Sonderfällen	Mac-Nutzer, Außendienst mit Mobilgeräten, Assistenzen mit Postfach-Delegationen, Kolleginnen und Kollegen mit Scan-to-Mail-Geräten	zwei bis vier Wochen
3	Breite Gruppen in Blöcken	Standortweise oder abteilungsweise, damit der Helpdesk nicht alles auf einmal abbekommt	je Block eine Woche
–	Geschäftsführung	kommt in Welle 3, nicht in Welle 1. Du willst Erfolgsmeldungen nach oben, keine Fehlerberichte	–

Tabelle 3: Ein bewährter Zuschnitt der Pilotwellen



Skizze 2: Wellenplan vom ersten Piloten bis zum Aufräumen

Staged Rollout einschalten

Im Entra Admin Center findest du die Funktion unter Entra ID > Entra Connect > Connect Sync, Abschnitt „Staged rollout of cloud authentication“, Link „Enable staged rollout for managed user sign-in“. Dort schaltest du die gewünschten Funktionen ein und ordnest Gruppen zu. Erlaubt sind die Kombinationen Password Hash Sync mit Seamless SSO oder Pass-Through Authentication mit Seamless SSO – nicht aber PHS, PTA und Seamless SSO gleichzeitig. Seamless SSO greift nur für Benutzer, die zusätzlich in einer PHS- oder PTA-Gruppe stecken.

Wer lieber skriptet oder die Konfiguration dokumentieren will, nutzt die Feature-Rollout-Richtlinien in Microsoft Graph. So stand es früher in jeder Anleitung mit Cmdlets aus dem AzureAD-Preview-Modul – das ist ausgemustert, der heutige Weg führt über Microsoft Graph PowerShell:

```
Connect-MgGraph -Scopes "Policy.ReadWrite.HybridAuthentication","Directory.ReadWrite.All"

# Welche Staged-Rollout-Richtlinien gibt es, welche sind aktiv?
Get-MgPolicyFeatureRolloutPolicy | Select-Object Id, DisplayName, Feature, IsEnabled

# Pilotgruppe der PHS-Richtlinie zuordnen
$gruppe = Get-MgGroup -Filter "displayName eq 'SR-Welle1-IT'"
$policy = Get-MgPolicyFeatureRolloutPolicy | Where-Object Feature -eq "passwordHashSync"
New-MgPolicyFeatureRolloutPolicyApplyToByRef -FeatureRolloutPolicyId $policy.Id `
    -OdataId "https://graph.microsoft.com/v1.0/directoryObjects/$($gruppe.Id)"

# Kontrolle: welche Gruppen hängen an der Richtlinie?
Get-MgPolicyFeatureRolloutPolicy -FeatureRolloutPolicyId $policy.Id -ExpandProperty appliesTo |
    Select-Object -ExpandProperty AppliesTo
```

Listing 4: Staged Rollout mit Microsoft Graph PowerShell prüfen und Gruppen zuordnen

WARNUNG — Die eine Anmeldung zu viel

Kommt ein Benutzer neu in eine Staged-Rollout-Gruppe, schaltet Entra ID ihn nicht sofort um. Er muss sich noch einmal interaktiv über ADFS anmelden, erst danach gilt für ihn die Cloud-Authentifizierung. Umgekehrt genauso: Wer aus der Gruppe fliegt, braucht eine weitere Anmeldung über Entra ID, bevor er wieder zur Farm geschickt wird.

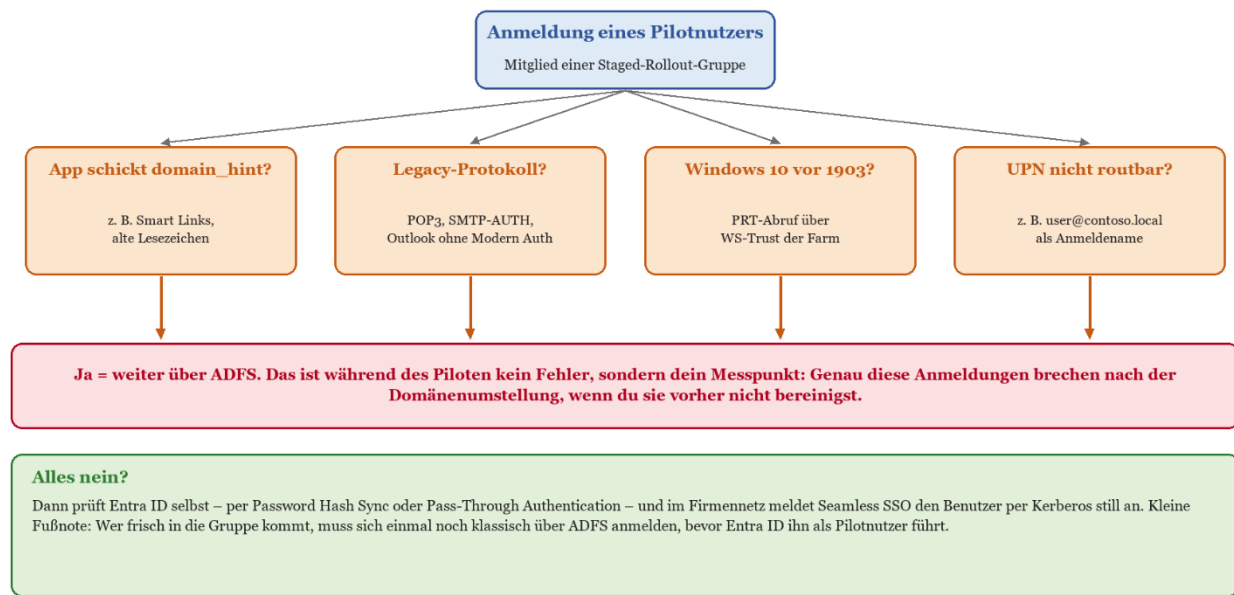
Auch Self-Service-Kennwörterücksetzung und das Bereinigen von Risiken in ID Protection können den Status zurücksetzen. Microsoft beschreibt als Abhilfe einen befristeten Zugriffspass (Temporary Access Pass) direkt nach dem Hinzufügen – Entra ID wertet ihn vor der Weiterleitung zur Farm aus.

Was trotz Staged Rollout bei ADFS landet

Und jetzt der Teil, der in Pilotphasen für Verwirrung sorgt: Manche Anmeldungen von Pilotnutzern laufen weiterhin über die Farm. Das ist kein Fehler, sondern Design – und es ist dein wichtigster Messpunkt. Denn genau diese Anmeldungen brechen nach der Domänenenumstellung, wenn du sie nicht vorher bereinigst.

Skizze 3: Pilotnutzer – und trotzdem bei ADFS gelandet?

Diese Abzweigungen ignorieren den Staged Rollout und laufen weiter über die Farm



Skizze 3: Vier Abzweigungen, die den Staged Rollout ignorieren

Fall	Was passiert im Pilot	Was passiert nach der Umstellung	Was du tust
Anwendung schickt domain_hint	Benutzer wird trotz Pilot zur Farm geschickt	Entra ID authentifiziert selbst, alles gut	Smart Links und Lesezeichen mit domain_hint identifizieren, Pilot dort nicht als gescheitert werten
Legacy-Authentifizierung (POP3, SMTP AUTH, uralte Clients)	läuft weiter föderiert	Basic Auth ist in Exchange Online ohnehin weitgehend abgeschaltet – Reste fallen auf	Legacy-Auth per Conditional Access blockieren und Reste vorher finden
Windows 10 älter als 1903	PRT-Abruf über den WS-Trust-Endpunkt der Farm	kein PRT mehr, SSO bricht	Clients aktualisieren – das solltest du ohnehin längst haben
Nicht routbarer UPN (z. B. @contoso.local)	PRT über WS-Trust der Farm	funktioniert nicht mehr	UPN-Suffix auf eine verifizierte Domäne umstellen
Nicht-persistente VDI	–	laut Microsoft nicht unterstützt	VDI-Domäne föderiert lassen oder VDI-Konzept ändern

Tabelle 4: Fälle, die im Pilot unauffällig sind und nach der Umstellung auffallen

Wie misst du das? Auf der Farm zeigt dir das Audit, welche Benutzer noch Token für die Relying Party urn:federation:MicrosoftOnline erhalten. Taucht ein Pilotnutzer dort regelmäßig auf, schau dir an, von welchem Gerät und welcher Anwendung die Anfrage kommt. Wie du die Audit-Ereignisse einschaltest und auswertest, steht in [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#); einen bequemen Überblick über Anmeldungen pro Relying Party liefert Entra Connect Health, beschrieben in [ADFS überwachen – Health Checks, Diagnose-Toolbox und Entra Connect Health](#). Auf der Entra-Seite helfen die Anmeldeprotokolle und die Hybrid-Auth-Arbeitsmappen, die Microsoft für Staged Rollout bereitstellt.

TIPP – Der Pilot ist erst fertig, wenn der Kalender durch ist

Ein Pilot über zwei ruhige Wochen beweist wenig. Lass mindestens einen Monatsabschluss, einen Kennwortwechsel und einen Urlaub mit Hotel-WLAN durchlaufen. Die interessantesten Fehler

kommen nicht am ersten Tag, sondern am Tag, an dem jemand sein Kennwort ändert und gleichzeitig am Smartphone, im Outlook und auf dem Leih-Notebook angemeldet ist. Bei PHS braucht das neue Kennwort bis zu zwei Minuten, bis es in der Cloud gilt – sag das deinen Pilotnutzern, bevor sie es selbst herausfinden.

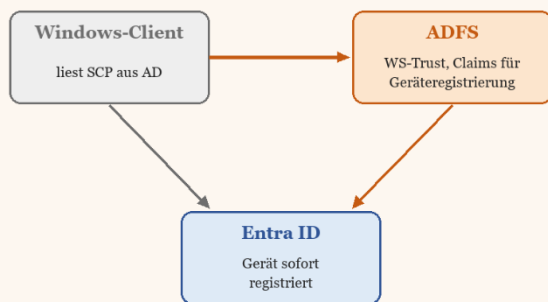
Geräte und Hybrid Join: der unterschätzte Teil

Bei vielen Umgebungen, die Hybrid Join vor Jahren mit Entra Connect eingerichtet haben, hilft die Farm beim Registrieren der Windows-Geräte mit: Entra Connect hat dafür eigene Claim Rules in die Microsoft-365-Relying-Party geschrieben, und der Client holt sich über den WS-Trust-Endpunkt der Farm ein Token, mit dem er sich sofort in Entra ID registriert. Nach der Umstellung gibt es diesen Weg nicht mehr. Dann registriert sich das Gerät über die Synchronisation: Der Client schreibt ein Zertifikat an sein Computerobjekt im AD, Entra Connect synchronisiert das Objekt, und erst danach ist das Gerät in Entra ID vollständig registriert. Bis dahin steht es dort als „Ausstehend“.

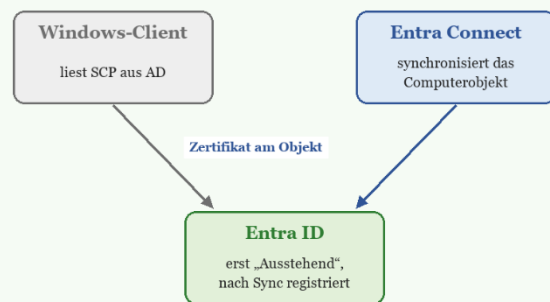
Skizze 4: Hybrid Join – wer registriert die Geräte nach der Umstellung?

Föderiert kann die Farm beim Join mithelfen. Managed übernimmt Entra Connect über die Synchronisation der Computerobjekte.

Federated: Join mit Hilfe der Farm



Managed: Join über Sync



Prüfen, bevor du umstellst

Liegen alle Computer-OUs im Sync-Bereich von Entra Connect? Zeigt der SCP auf den richtigen Tenant? Sind keine Windows-10-Clients älter als 1903 mehr im Bestand? Stammen Windows-Hello-Zertifikate nicht aus der Farm als Registrierungsstelle? Läuft keine nicht-persistente VDI? Fünfmal Ja – dann los.

Skizze 4: Geräteregistrierung mit und ohne Farm

Für bestehende, bereits registrierte Geräte ändert sich dadurch nichts – sie bleiben hybrid eingebunden. Kritisch sind drei Gruppen: neue Geräte, deren Computerobjekte nicht im Synchronisationsbereich liegen, alte Windows-10-Versionen vor 1903 und Szenarien, in denen die Farm eine Zusatzrolle spielt, etwa als Registrierungsstelle für Windows Hello for Business mit Zertifikatsvertrauen. Letzteres unterstützt Staged Rollout ausdrücklich nicht – hier lohnt der Wechsel auf Cloud Kerberos Trust vor der Umstellung.

```

# Hybrid eingebundene Geräte nach Betriebssystemversion zählen
Connect-MgGraph -Scopes "Device.Read.All"
Get-MgDevice -All -Filter "trustType eq 'ServerAd'" `
  -Property DisplayName, OperatingSystem, OperatingSystemVersion,
  ApproximateLastSignInDateTime |
  Group-Object OperatingSystemVersion | Sort-Object Name |
  Select-Object Count, Name

# SCP prüfen: auf welchen Tenant zeigen die Domänencomputer?
  
```

```
$conf = (Get-ADRootDSE).configurationNamingContext
Get-ADObject -Identity "CN=62a0ff2e-97b9-4513-943f-0d221bd30080,CN=Device Registration
Configuration,CN=Services,$conf" `
-Properties keywords | Select-Object -ExpandProperty keywords
```

Listing 5: Geräte-Bestandsaufnahme vor der Umstellung

Prüfpunkt	Wie prüfen	Gut, wenn ...
Computer-OU's im Sync-Bereich	Entra-Connect-Assistent, Domänen- und OU-Filterung	alle OU's mit Windows-Clients ausgewählt sind
SCP vorhanden und korrekt	Listing 5, Attribut keywords	Tenant-Name und Tenant-ID deines Tenants enthalten sind
Windows-Versionen	Listing 5, Gruppierung nach Version	keine Builds unter 10.0.18362 (Version 1903) mehr auftauchen
Ausstehende Geräte	Entra Admin Center, Geräteliste, Status „Ausstehend“	die Liste klein ist und neue Geräte nach dem nächsten Sync verschwinden
Windows Hello for Business	Bereitstellungsmodell in der GPO bzw. im Intune-Profil	Cloud Kerberos Trust oder Key Trust, keine Zertifikate von der Farm
VDI	Inventar der Terminalserver- und VDI-Pools	keine nicht-persistenten Windows-10/11-Pools an der umzustellenden Domäne

Tabelle 5: Geräte-Checkliste vor der Domänenumstellung

WARNUNG — Die Farm verschwindet nicht aus dem Gedächtnis der Clients

Hast du Hybrid Join früher clientseitig per Registrierungsschlüssel gezielt gesteuert oder den SCP bewusst nicht im AD hinterlegt, sondern per GPO verteilt, prüfe diese Einstellungen jetzt. Sie verweisen nicht auf die Farm, aber sie sind genau die Art Altlast, die nach der Umstellung niemand mehr auf dem Schirm hat.

Die Domäne umstellen – mit Graph PowerShell oder Entra Connect

Wenn die letzte Welle ruhig läuft, die Geräte geprüft sind und das Audit auf der Farm nur noch die erwarteten Ausnahmen zeigt, kommt der eigentliche Schalter. Plane ein Wartungsfenster außerhalb der Geschäftszeiten: Microsoft nennt bis zu 60 Minuten für die Umstellung, in denen neue Anmeldungen an browserbasierten Anwendungen hängen können. Moderne Clients mit gültigem Refresh Token arbeiten in der Zwischenzeit weiter und bemerken die Umstellung in der Regel gar nicht.

Variante A: Entra Connect

Hat Entra Connect die Föderation damals selbst eingerichtet – das siehst du im Assistenten unter „Zusätzliche Aufgaben“ > „Verbund verwalten“ > „Verbundkonfiguration anzeigen“ –, ist der Assistent der bequemste Weg. Unter „Benutzeranmeldung ändern“ wählst du Password Hash Sync oder Pass-Through Authentication und optional „Einmaliges Anmelden aktivieren“. Bei PHS setzt du den Haken „Benutzerkonten nicht konvertieren“. Achtung: Mit dem Klick auf „Konfigurieren“ werden alle föderierten Domänen des Tenants umgestellt, nicht nur eine.

Variante B: Microsoft Graph PowerShell, Domäne für Domäne

Hast du mehrere Domänen oder wurde die Föderation von Hand eingerichtet, stellst du jede Domäne einzeln um. Das ist auch die kontrolliertere Variante, wenn du mit einer kleinen Domäne beginnen willst. Früher stand an dieser Stelle in jeder Anleitung Set-MSolDomainAuthentication aus dem MSOnline-Modul – das ist Geschichte. Heute sieht es so aus:

```
Connect-MgGraph -Scopes "Domain.ReadWrite.All", "Directory.AccessAsUser.All"
```

```
# Vorher: Stand festhalten
Get-MgDomain -DomainId "contoso.de" | Select-Object Id, AuthenticationType

# Umstellen
Update-MgDomain -DomainId "contoso.de" -AuthenticationType "Managed"

# Nachher: muss "Managed" zeigen
Get-MgDomain -DomainId "contoso.de" | Select-Object Id, AuthenticationType
```

Listing 6: Eine Domäne von Federated auf Managed umstellen

Wählst du Pass-Through Authentication und stellst per PowerShell um, ziehst du die Anmeldemethode im Entra-Connect-Assistenten anschließend nach, damit Entra Connect PTA als aktiv erkennt. Vor der Umstellung müssen die PTA-Agenten im Entra Admin Center als „Aktiv“ erscheinen – sonst schaltest du die Anmeldung auf einen Dienst um, der gerade niemanden prüfen kann.

Der Ablaufplan mit Erfolgskriterium und Rollback

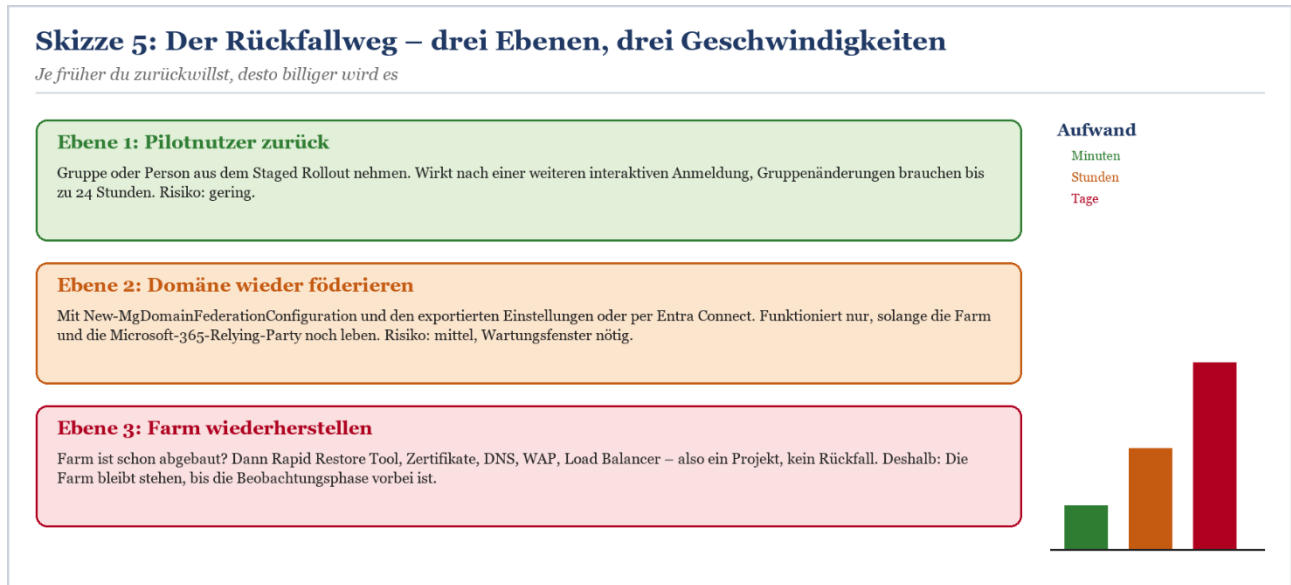
Die folgende Tabelle ist das Herzstück jedes Change-Antrags für diese Umstellung. Jeder Schritt hat ein messbares Erfolgskriterium und einen definierten Rückweg. Fehlt eins von beiden, ist der Schritt nicht fertig geplant.

Nr.	Schritt	Erfolgskriterium	Rollback
0	Ist-Zustand sichern (Listing 1), Farm-Backup	Exporte liegen vor und sind lesbar; Domänenliste dokumentiert	nicht nötig – es wurde nichts geändert
1	Password Hash Sync aktivieren (bzw. PTA-Agenten installieren)	Invoke-ADSyncDiagnostics meldet erfolgreiche Synchronisation; PTA-Agenten „Aktiv“	Funktion wieder abschalten – Anmeldung ist unberührt
2	Seamless SSO aktivieren, Intranetzone per GPO	AZUREADSSOACC vorhanden, Status in Entra aktiv	GPO zurücknehmen, Seamless SSO deaktivieren
3	Branding, Conditional Access, MFA-Registrierung	Pilotnutzer haben Methoden registriert; CA im Bericht ohne Überraschungen	Richtlinien auf „Nur Bericht“ setzen
4	Staged Rollout Welle 1 (IT, Cloud-Gruppe ≤ 200)	Anmeldungen der Gruppe im Entra-Log ohne Umweg über die Farm; keine offenen Tickets	Gruppe aus dem Staged Rollout entfernen
5	Welle 2 (Sonderfälle)	Mac, mobil, Außendienst, Delegationen funktionieren; Ausnahmen aus Tabelle 4 erklärt	Gruppe entfernen; Sonderfall analysieren
6	Welle 3 (breite Blöcke)	Helpdesk-Aufkommen im Normalbereich; Monatsabschluss überstanden	betroffenen Block entfernen
7	Geräte-Check (Tabelle 5)	alle Prüfpunkte grün	Umstellung verschieben, nicht Geräte opfern
8	Domänenumstellung im Wartungsfenster (Listing 6 oder Entra Connect)	AuthenticationType = Managed; Testanmeldungen intern und extern erfolgreich	Domäne wieder föderieren (Listing 7)
9	Staged Rollout abschalten, Beobachtungsphase	keine Token mehr für urn:federation:MicrosoftOnline außer erklärten Altlasten	solange Farm und RP leben: erneut föderieren
10	Microsoft-365-Relying-Party entfernen	Wochen ohne Anmeldungen an der RP; alle Benutzer melden sich über Entra ID an	RP aus dem Export wiederherstellen

Tabelle 6: Ablaufplan mit Erfolgskriterium und Rollback je Schritt

Der Rückfallweg: zurück auf Federated

Kein Change-Board der Welt sollte eine Domänenumstellung ohne Rückweg genehmigen. Die gute Nachricht: Solange die Farm läuft und die Microsoft-365-Relying-Party existiert, ist der Rückweg eine Sache von Minuten plus Wartezeit. Die schlechte: Wer die Farm am Tag nach der Umstellung voller Tatendrang abbaut, hat keinen Rückweg, sondern ein Wiederaufbauprojekt.



Skizze 5: Drei Rückfallebenen – je früher, desto billiger

Während des Piloten

Hier ist der Rückweg trivial: Entferne die Gruppe aus dem Staged Rollout oder einzelne Personen aus der Gruppe. Denk an die zusätzliche Anmeldung, die nötig ist, bis Entra ID den Benutzer wieder zur Farm schickt, und an die bis zu 24 Stunden bei Mitgliedschaftsänderungen. Willst du den Staged Rollout ganz beenden, schiebst du den Schalter der jeweiligen Funktion zurück auf „Aus“.

Nach der Domänenumstellung

Microsoft beschreibt den Rückweg über New-MgDomainFederationConfiguration: Du legst die Föderationskonfiguration mit den Werten neu an, die du in Listing 1 exportiert hast, und die Domäne ist wieder föderiert. Alternativ richtet Entra Connect die Föderation mit ADFS erneut ein, wenn sie ursprünglich darüber konfiguriert war.

```
Connect-MgGraph -Scopes "Domain.ReadWrite.All","Directory.AccessAsUser.All"
$alt = Import-Clixml "C:\Migration\contoso.de-federation.xml"

New-MgDomainFederationConfiguration -DomainId "contoso.de" `
  -DisplayName $alt.DisplayName `
  -IssuerUri $alt.IssuerUri `
  -PassiveSignInUri $alt.PassiveSignInUri `
  -ActiveSignInUri $alt.ActiveSignInUri `
  -MetadataExchangeUri $alt.MetadataExchangeUri `
  -SignOutUri $alt.SignOutUri `
  -SigningCertificate $alt.SigningCertificate `
  -PreferredAuthenticationProtocol $alt.PreferredAuthenticationProtocol `
  -FederatedIdpMfaBehavior $alt.FederatedIdpMfaBehavior

Get-MgDomain -DomainId "contoso.de" | Select-Object Id, AuthenticationType # erwartet: Federated
```

Listing 7: Rückfall – Domäne mit den gesicherten Einstellungen wieder föderieren

WARNUNG — Das Zertifikat von gestern ist nicht immer das Zertifikat von heute

Listing 7 setzt das Token-Signing-Zertifikat aus dem Export. Hat die Farm seit dem Export per AutoCertificateRollover ein neues Zertifikat aktiviert, förderst du mit einem veralteten Schlüssel, und jede Anmeldung scheitert mit einem Signaturfehler. Vergleiche vorher das aktuelle primäre Zertifikat mit Get-AdfsCertificate -CertificateType Token-Signing. Hintergründe stehen in [ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover](#) und [Microsoft-365-Federation-Trust nach Zertifikatswechsel aktualisieren](#).

Wann du die Microsoft-365-Relying-Party wirklich löschst

Microsoft rät, die Relying Party erst zu entfernen, wenn die Nutzungsdaten keine neuen Anmeldungen mehr zeigen und alle Benutzer und Clients erfolgreich über Entra ID authentifizieren. Wir würden ergänzen: und wenn ein Monatsabschluss und ein Quartalsende ohne Rückfallwunsch vergangen sind. Bis dahin bleibt sie, wo sie ist, und kostet dich nichts außer einem Eintrag in der Verwaltungskonsole. Danach entfernst du sie mit Remove-AdfsRelyingPartyTrust – den Export aus Listing 1 hast du ja.

Läuft auf der Farm danach nichts mehr, steht der nächste Schritt an: [ADFS abschalten – die Farm sauber außer Betrieb nehmen](#). Hängen noch SAML-Anwendungen daran, geht es mit [SAML-Anwendungen von ADFS nach Entra ID migrieren](#) weiter. Und wenn du die Planung lieber mit jemandem durchgehst, der diese Umstellung schon in einigen Umgebungen begleitet hat, findest du Unterstützung im [Consulting zu ADFS \(Active Directory Federation Services\)](#).

WEITER — Passende Beiträge für die nächsten Schritte

- › [Relying Parties inventarisieren – die Bestandsaufnahme vor der Entra-Migration](#)
- › [Claim Rules nach Conditional Access übersetzen](#)
- › [ADFS mit Entra-MFA koppeln – Adapter, Zertifikat und Fallstricke](#)
- › [SAML-Anwendungen von ADFS nach Entra ID migrieren](#)
- › [ADFS abschalten – die Farm sauber außer Betrieb nehmen](#)
- › [Microsoft Entra ID](#)

Fazit: Schalter umlegen ist leicht, Wellen planen ist die Arbeit

Die Domäne von Federated auf Managed umzustellen, ist technisch ein einziger Befehl. Das Projekt drumherum ist der Grund, warum es am Montag ruhig bleibt: Password Hash Sync rechtzeitig einschalten, Seamless SSO und Conditional Access vorziehen, Pilotgruppen in sinnvollen Wellen durch den Staged Rollout schicken, die Ausnahmen ernst nehmen, die Geräte prüfen und den Rückweg so vorbereiten, dass er in Minuten funktioniert. ADFS wird dadurch nicht schlechter oder überflüssig – die Farm verliert nur ihre anstrengendste Aufgabe und kann sich in Ruhe um die Relying Parties kümmern, die sie noch hat.

Wer die Umstellung so angeht, erlebt eine merkwürdig undramatische Wartungsnacht. Das ist das schönste Kompliment, das man einem Identitätsprojekt machen kann. Die Hintergründe zu Föderation, Vertrauensstellungen und Migrationspfaden vertieft [ADFS in der Praxis – das Buch im Detail](#), und wer Staged Rollout, Umstellung und Rückfall einmal ohne Produktionsdruck üben will, findet das passende Format in den [ADFS-Schulungen](#).

FAQ: Microsoft 365 von ADFS auf Managed umstellen

Wie stelle ich Microsoft 365 von ADFS auf Managed um?

Password Hash Sync oder Pass-Through Authentication vorbereiten, Seamless SSO aktivieren, mit Staged Rollout Pilotgruppen testen und anschließend jede Domäne mit Update-MgDomain - AuthenticationType Managed oder über Entra Connect („Benutzeranmeldung ändern“) umstellen.

Wie lange dauert die Umstellung einer Domäne?

Microsoft nennt bis zu 60 Minuten. In dieser Zeit können neue Browser-Anmeldungen hängen; Clients mit gültigem Refresh Token arbeiten weiter. Plane ein Wartungsfenster außerhalb der Geschäftszeiten.

Kann ich Staged Rollout dauerhaft nutzen?

Nein. Microsoft beschreibt Staged Rollout ausdrücklich als temporäres Testwerkzeug und rät von einem dauerhaften Mischbetrieb ab. Nach erfolgreichem Test stellst du die Domäne um und schaltest Staged Rollout ab.

Wie viele Gruppen und Benutzer unterstützt Staged Rollout?

Bis zu zehn Gruppen je Funktion. Die Benutzerzahl ist nicht begrenzt, beim ersten Hinzufügen einer Gruppe sollten es aber höchstens 200 Mitglieder sein. Verschachtelte und dynamische Gruppen werden nicht unterstützt.

Warum landet ein Pilotnutzer trotzdem auf der ADFS-Anmeldeseite?

Häufige Gründe sind Anwendungen mit domain_hint, Legacy-Authentifizierung, Windows 10 vor Version 1903, ein nicht routbarer UPN oder ein frisch hinzugefügter Benutzer, der sich noch einmal über ADFS anmelden muss.

Brauche ich Seamless SSO, wenn alle Clients Windows 11 sind?

Auf hybrid oder in Entra ID eingebundenen Windows-10/11-Geräten liefert der Primary Refresh Token das SSO. Seamless SSO ist trotzdem sinnvoll für Browser-Szenarien und Geräte ohne PRT und wird von Microsoft für den Staged Rollout empfohlen.

Was passiert mit hybrid eingebundenen Geräten?

Bereits registrierte Geräte bleiben registriert. Neue Geräte registrieren sich nach der Umstellung über die Synchronisation der Computerobjekte durch Entra Connect und erscheinen bis dahin als „Ausstehend“. Prüfe Sync-Bereich, SCP und Windows-Versionen vorher.

Wie komme ich nach der Umstellung zurück auf Federated?

Mit New-MgDomainFederationConfiguration und den vorher gesicherten Föderationseinstellungen oder über Entra Connect. Voraussetzung ist, dass Farm und Microsoft-365-Relying-Party noch existieren und das Token-Signing-Zertifikat aktuell ist.

Kann ich Set-MsolDomainAuthentication noch verwenden?

Nein, das MSOnline-Modul ist ausgemustert. Der aktuelle Weg ist Update-MgDomain aus Microsoft Graph PowerShell oder der Entra-Connect-Assistent.

Wann kann ich die Microsoft-365-Relying-Party in ADFS löschen?

Wenn die Nutzungsdaten über einen längeren Zeitraum keine Anmeldungen mehr zeigen und alle Benutzer und Clients sauber über Entra ID authentifizieren. Exportiere sie vorher.

Muss ich ADFS nach der Umstellung abschalten?

Nein. Die Farm betreut weiterhin alle anderen Relying Parties. Ob und wann du sie außer Betrieb nimmst, entscheidet die Bestandsaufnahme der übrigen Anwendungen.