

MFA für SharePoint Server on-premises: drei Wege, die funktionieren — und einer, der nur so aussieht

Es gibt diesen Moment in jedem Sicherheitsaudit, in dem jemand fragt: „Und der SharePoint? Da ist doch auch MFA drauf, oder?“ Dann wird es im Raum sehr still, jemand schaut auf den Boden, und schließlich sagt der Kollege aus dem Betrieb den Satz, den du schon geahnt hast: „Da meldet man sich einfach mit dem Windows-Konto an. Das geht ganz automatisch.“ Genau. Das ist das Problem.

SharePoint Server on-premises ist in vielen Häusern die letzte große Anwendung, die noch munter mit integrierter Windows-Anmeldung läuft. In der Cloud hast du längst Conditional Access, Gerätekonformität und Passkeys ausgerollt. Auf der Farm im Keller hängt weiterhin ein Portal, das jeden hereinlässt, der ein gültiges Kennwort kennt — und jeden, der es sich besorgt hat. Das ist keine Nachlässigkeit, das ist Architektur: NTLM und Kerberos wurden nicht dafür gebaut, einen zweiten Faktor abzufragen.

Die gute Nachricht: Es gibt Wege, und sie sind alle dokumentiert und erprobt. Die schlechte: Welcher Weg dir offensteht, entscheidet nicht dein Sicherheitskonzept, sondern die Versionsnummer deiner Farm. Und die ist, wenn wir ehrlich sind, bei vielen genau der Grund, warum das Thema seit Jahren vor sich hin schwelt.

Dieser Beitrag sortiert die Optionen: AD FS mit MFA-Adapter, Entra ID als Identitätsanbieter für die Subscription Edition, Reverse-Proxy- und Application-Proxy-Varianten — und die Frage, was Kerberos in dieser Geschichte eigentlich noch beiträgt. Mit Anmeldeflüssen, Voraussetzungen, den üblichen Stolpersteinen und einer ehrlichen Einschätzung, wo der Aufwand steht.

Warum deine Farm bis heute ohne zweiten Faktor läuft

SharePoint Server kennt seit jeher drei Arten, Menschen hereinzulassen: Windows-Authentifizierung, formularbasierte Anmeldung und tokenbasierte Anmeldung über SAML 1.1 zusammen mit dem WS-Federation Passive Requestor Profile. Erst die Subscription Edition kam mit einem vierten Verfahren dazu: OpenID Connect 1.0. Diese Liste ist wichtig, weil sie den gesamten Handlungsspielraum beschreibt. Was nicht drinsteht, geht auch nicht — jedenfalls nicht in der Farm selbst.

Der Klassiker in Bestandsumgebungen ist die Windows-Authentifizierung in der Standardzone. Sie ist bequem: keine Anmeldemaske, kein Zertifikatszirkus, der Browser reicht das Ticket durch, und alles funktioniert. Sie ist auch der Grund, warum ein einziges abgephishtes Kennwort in vielen Häusern immer noch für den vollen Lesezugriff auf sämtliche Projektablagen reicht.

Was ein Kerberos-Ticket beweist — und was nicht

Kerberos ist ein hervorragendes Protokoll. Es ist schnell, es entlastet die Domänencontroller, es unterstützt AES und gegenseitige Authentifizierung, und es kann Anmeldeinformationen delegieren. Wenn du wissen willst, wie die Ticketmechanik im Detail funktioniert und welche

Dienstprinzipalnamen du für eine SharePoint-Farm brauchst, findest du das an anderer Stelle ausführlich beschrieben.

Für unsere Frage zählt allerdings nur eine Eigenschaft: Ein Dienstticket sagt SharePoint, dass der Schlüsselverteilungsdienst diesem Konto ein Ticket ausgestellt hat. Es sagt nicht, wie sich das Konto beim Domänencontroller ausgewiesen hat, und es sagt schon gar nicht, ob dabei ein zweiter Faktor im Spiel war. SharePoint kann diese Information also gar nicht auswerten, weil sie im Ticket in verwertbarer Form nicht vorkommt. Mehr zur Mechanik dahinter im [Kompetenzbereich Kerberos](#).

Der Kerberos-Fallback und seine Grenzen

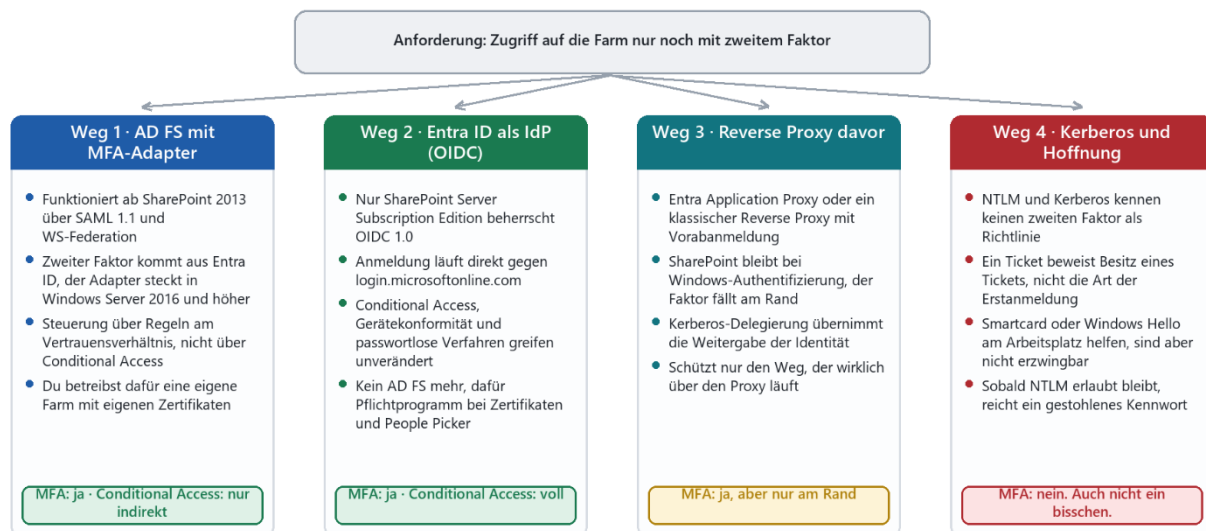
Trotzdem hält sich hartnäckig das Argument, Kerberos sei doch eigentlich schon fast MFA. Die Begründung geht so: Wer sich am Arbeitsplatz mit Windows Hello for Business oder einer Smartcard anmeldet, hat Besitz und Wissen beziehungsweise Biometrie kombiniert. Das Ticket, das daraus entsteht, sei damit implizit mehrfaktoriell abgesichert.

Am Ausgangspunkt stimmt das sogar. Nur trägt die Argumentation nicht weit genug, und zwar aus vier Gründen. Erstens kannst du diese Eigenschaft in SharePoint nicht erzwingen: Es gibt keine Einstellung „Windows-Zone nur für Sitzungen mit starker Erstanmeldung“. Zweitens gilt sie nur für verwaltete Arbeitsplätze — das Notebook im Homeoffice, der private Rechner in der VPN-Sitzung und der Browser auf dem Terminalserver eines Dienstleisters sind damit nicht abgedeckt. Drittens fällt das ganze Konstrukt in sich zusammen, sobald NTLM als Rückfallebene erlaubt bleibt: Dann reicht wieder ein Kennwort. Und viertens bekommst du keine Richtlinie, kein Protokoll und keine Sitzungssteuerung dazu.

Das heißt nicht, dass du Kerberos abschaffen sollst. Im Gegenteil: Du brauchst weiterhin eine Zone mit Windows-Authentifizierung, weil der Suchcrawl darauf angewiesen ist und weil eine ganze Reihe von Diensten und Anwendungen sonst stillsteht. Kerberos ist die Rückfallebene für Maschinen und für das interne Netz. Es ist nur eben keine Antwort auf die Frage nach dem zweiten Faktor.

Vier Wege zur MFA vor SharePoint Server

Drei davon führen zu einem zweiten Faktor. Einer führt nur zu einem guten Gefühl.



Die Wege schließen sich nicht aus: In der Praxis kombinierst du eine föderierte Zone für Menschen mit einer Windows-Zone für Suchcrawl und Dienste.

Skizze 1: Die vier Optionen im Überblick. Weg 4 ist der Zustand, in dem sich die meisten Farmen heute befinden.

Version	Windows	Formulare	SAML 1.1 / WS-Fed	OIDC 1.0	Support
SharePoint 2013	ja	ja	ja	nein	seit April 2023 beendet
SharePoint 2016	ja	ja	ja	nein	seit 14. Juli 2026 beendet
SharePoint 2019	ja	ja	ja	nein	seit 14. Juli 2026 beendet
Subscription Edition	ja	ja	ja	ja	Modern Lifecycle, laufend

Tabelle 1: Was welche Version tatsächlich kann. Die Spalte ganz rechts erklärt, warum die Diskussion in vielen Häusern gerade dringend geworden ist.

WICHTIG · Die Uhr ist bereits abgelaufen

SharePoint Server 2016 und 2019 haben am 14. Juli 2026 das Ende des erweiterten Supports erreicht. Seitdem gibt es keine Sicherheitsupdates mehr — auch nicht für Lücken, die aktiv ausgenutzt werden. Wenn deine Farm auf einer dieser Versionen läuft, ist MFA das zweitwichtigste Thema auf deiner Liste. Das wichtigste ist der Umstieg auf die Subscription Edition oder nach Microsoft 365. Beides zusammen ist übrigens kein Zufall: Die Subscription Edition ist gleichzeitig die einzige Version, die OpenID Connect beherrscht.

- › Klassische Windows-Anmeldung ohne Ansprüche gibt es seit 2016 ohnehin nicht mehr — alle Zonen arbeiten anspruchsbasiert.
- › SAML 1.1 über AD FS funktioniert auch auf den alten Versionen, verlängert deren Lebensdauer aber kein Stück.

Zum Vergleich: In SharePoint Online ist dieselbe Anforderung eine Frage von zwei Richtlinien und einem Nachmittag. Wie das dort aussieht, steht in [MFA für SharePoint Online erzwingen](#). Der Unterschied im Aufwand zwischen beiden Beiträgen ist ungefähr das ehrlichste Argument für eine Migration, das ich kenne.

Weg 1: AD FS mit MFA-Adapter

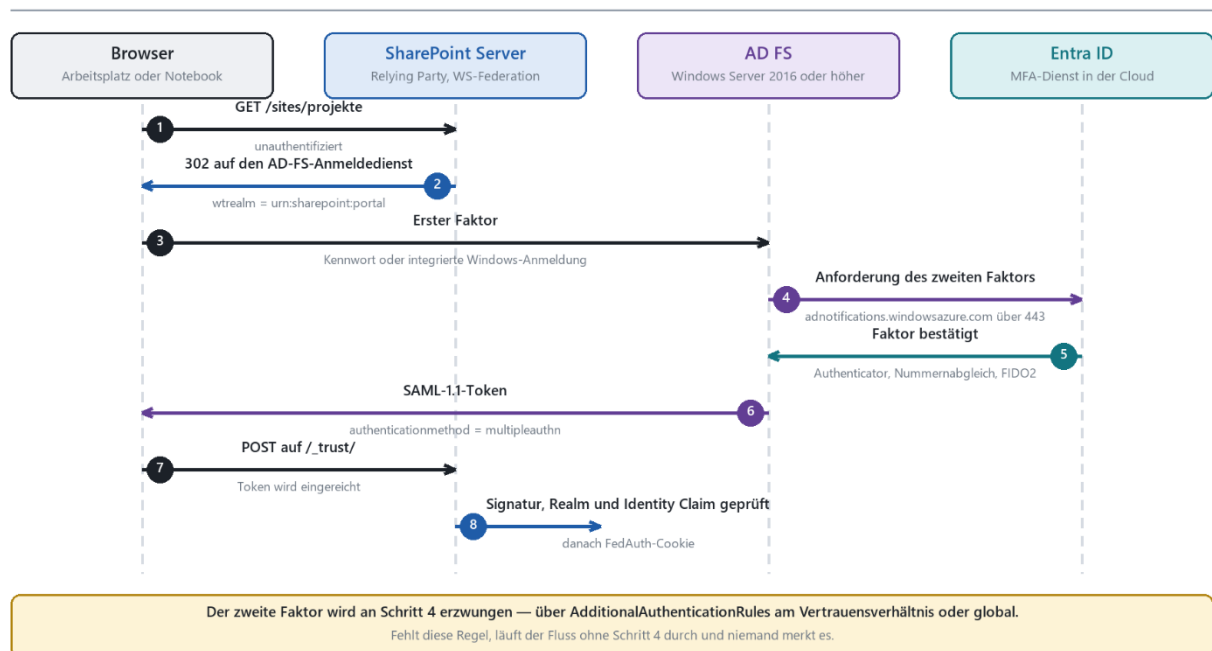
Der klassische Weg, und für alle Versionen vor der Subscription Edition der einzige, der innerhalb der Farm funktioniert: Du stellst SharePoint auf tokenbasierte Anmeldung um und setzt AD FS als Identitätsanbieter davor. AD FS führt die Anmeldung durch, fordert den zweiten Faktor an und stellt am Ende ein SAML-Token aus, das SharePoint akzeptiert.

Der zweite Faktor kommt dabei aus Entra ID. Der dafür nötige Adapter ist in Windows Server 2016 und höher bereits enthalten, du musst nichts installieren. Den früher üblichen Azure MFA Server im eigenen Rechenzentrum brauchst du nicht mehr — und darfst ihn auch nicht mehr einsetzen: Seit dem 30. September 2024 beantwortet er keine Anfragen mehr. Wer ihn noch betreibt, hat kein MFA-Problem, sondern ein Anmeldeproblem.

So läuft die Anmeldung

Anmeldefluss: AD FS mit Entra-MFA-Adapter

SharePoint sieht am Ende nur ein Token. Ob darin ein zweiter Faktor steckt, entscheidet AD FS.



Skizze 2: Anmeldefluss mit AD FS und dem Entra-MFA-Adapter. SharePoint prüft am Ende nur, ob das Token gültig ist.

Der interessante Teil steckt in Schritt 4. AD FS fragt den zweiten Faktor nicht automatisch ab, sondern nur, wenn eine Regel es verlangt. Diese Regel liegt entweder global oder — deutlich besser — am Vertrauensverhältnis zu genau dieser SharePoint-Webanwendung. So kannst du den zweiten Faktor für den Zugriff aus dem Extranet verlangen und ihn im internen Netz weglassen, oder ihn nur für bestimmte Gruppen erzwingen.

Wenn der Faktor erfolgreich war, schreibt AD FS einen Anspruch mit der verwendeten Authentifizierungsmethode in das Token. SharePoint wertet diesen Anspruch nicht aus — das ist wichtig zu verstehen. Die Farm vertraut dem Aussteller vollständig. Alles, was an Sicherheitsanforderungen durchgesetzt wird, wird bei AD FS durchgesetzt, und nur dort.

Was du auf den AD-FS-Servern einrichtest

Die Einrichtung des Adapters ist überschaubar, hat aber eine Falle: Du musst sie auf jedem AD-FS-Server der Farm durchführen. Zuerst erzeugst du auf jedem Server ein Zertifikat, dann hinterlegst du es als Anmeldeinformation am Dienstprinzipal des MFA-Clients in deinem Mandanten, und zuletzt registrierst du den Mandanten einmal für die gesamte Farm.

```
# je AD-FS-Server:
$certbase64 = New-AdfsAzureMfaTenantCertificate -TenantID <mandanten-id>

# Zertifikat am Dienstprinzipal des MFA-Clients hinterlegen
Connect-MgGraph -Scopes 'Application.ReadWrite.All'
# AppId des Azure-MFA-Clients: 981f26a1-7f43-403b-a875-f8b09b8cd720

# einmal je AD-FS-Farm:
Set-AdfsAzureMfaTenant -TenantId <mandanten-id> `
  -ClientId 981f26a1-7f43-403b-a875-f8b09b8cd720

# danach: AD-FS-Dienst je Server neu starten, Server einzeln aus der
# Lastverteilung nehmen und Verbindungen auslaufen lassen
```

FAKTEN · Voraussetzungen für den MFA-Adapter an AD FS

Bevor du anfängst, prüfe diese Punkte — sie erklären die meisten gescheiterten Versuche:

- › AD FS auf Windows Server 2016 oder höher; die lokale Verzeichnismgebung ist mit Entra ID föderiert.
- › Entra ID P1 oder P2 beziehungsweise eine Enterprise Mobility Suite; MFA ist keine kostenlose Beigabe.
- › Ausgehend Port 443 von jedem AD-FS-Server zu den Microsoft-Endpunkten für Benachrichtigungen und Anmeldung; ein Proxy dazwischen muss das durchlassen.
- › Die erzeugten Zertifikate sind zwei Jahre gültig. Trage dir die Erneuerung ein, sonst steht die Anmeldung an einem Dienstagmorgen.
- › Bei AD FS 2019 als primäre Methode muss der Ankeranspruch der Active-Directory-Anspruchsanbieter-Vertrauensstellung auf den Benutzerprinzipalnamen umgestellt werden.

Wo es in der Praxis klemmt

Der erste Stolperstein hat nichts mit Technik zu tun, sondern mit Menschen: AD FS kann die Registrierung von Authentifizierungsmethoden nicht selbst durchführen. Wer noch keine Methode hinterlegt hat, bekommt an der Anmeldemaske eine wenig hilfreiche Fehlermeldung und ruft an. Du kannst die Anmeldeseite anpassen und die Betroffenen auf die Registrierungsseite umleiten, aber das ist Handarbeit, die du vorher einplanen musst.

Der zweite: AD FS ist kein Conditional Access. Du kannst mit Anspruchsregeln erstaunlich viel abbilden — Netzbereich, Gruppenmitgliedschaft, Anwendung — aber du bekommst keine Gerätekonformität, keine Risikobewertung und keine Berichte im vertrauten Format. Wer beides sauber nebeneinanderlegen will, findet die Gegenseite in [Conditional Access: Baselines, die nicht nerven](#) beschrieben.

Der dritte ist organisatorisch: Du betreibst damit dauerhaft eine weitere Serverrolle mit eigenem Zertifikatsmanagement, eigener Hochverfügbarkeit und eigenem Aktualisierungszyklus. Wenn AD

FS bei dir ohnehin steht, weil andere Anwendungen daran hängen, ist das ein vertretbarer Preis. Wenn du AD FS nur für SharePoint aufbauen würdest, solltest du dir Weg 2 sehr genau ansehen.

TIPP · AD FS kann auch OIDC

Falls du bereits auf der Subscription Edition bist, aber AD FS aus anderen Gründen behalten willst: SharePoint SE kann AD FS auch als OpenID-Connect-Anbieter einbinden statt über SAML 1.1. Der Anmeldefluss entspricht dann Skizze 3, nur mit deinem eigenen Anbieter statt Entra ID in der Mitte. Das ist der saubere Zwischenschritt, wenn die Anmeldung aus regulatorischen Gründen im eigenen Rechenzentrum stattfinden muss.

Weg 2: Entra ID als Identitätsanbieter für SharePoint SE

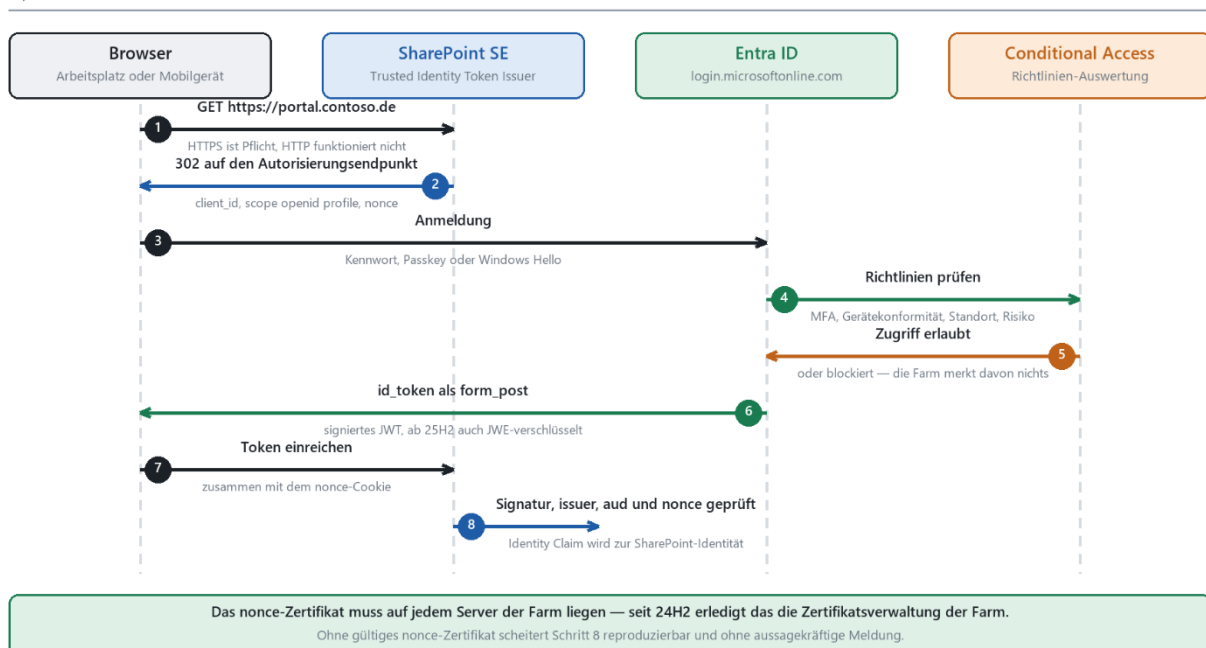
Das ist der Weg, auf den Microsoft die Produktentwicklung ausgerichtet hat, und es ist der einzige, bei dem du den vollen Werkzeugkasten aus der Cloud auf eine lokale Farm anwenden kannst: Conditional Access mit Gerätekonformität, Standort und Risikobewertung, passwortlose Verfahren, zentrale Anmeldeprotokolle. Der Preis: Er setzt die Subscription Edition voraus, ohne Ausnahme und ohne Umweg.

OpenID Connect statt SAML: was sich ändert

Technisch verschiebt sich einiges. Statt eines SAML-Tokens, das per Formular an den Vertrauensendpunkt der Farm geschickt wird, bekommst du ein signiertes JSON Web Token. SharePoint prüft dessen Signatur gegen die veröffentlichten Schlüssel des Anbieters, vergleicht Aussteller und Zielgruppe und gleicht einen zufälligen Wert gegen ein eigenes Cookie ab. Genau dieses nonce-Cookie ist der Grund, warum du ein zusätzliches Zertifikat brauchst — und warum die Einrichtung auf mehreren Servern früher so unangenehm war.

Anmeldefluss: Entra ID als IdP für SharePoint SE

OpenID Connect 1.0 — kein AD FS mehr in der Mitte, dafür Conditional Access in voller Breite.



Skizze 3: Anmeldefluss mit Entra ID als Identitätsanbieter. Schritt 4 und 5 laufen vollständig außerhalb der Farm.

Der entscheidende Unterschied zu Weg 1 steckt in den Schritten 4 und 5. Die Richtlinienauswertung findet in Entra ID statt, mit demselben Regelwerk, das du für Exchange Online, Teams und alles andere schon gebaut hast. Deine lokale Farm erscheint dort als ganz normale Anwendung. Du kannst also verlangen: nur von konformen Geräten, nur aus zugelassenen Ländern, immer mit phishingresistentem Faktor. Die Farm bekommt davon nichts mit — sie sieht am Ende entweder ein gültiges Token oder gar keines.

FAKTEN · Was in SharePoint SE dafür nötig ist

Die Liste ist kurz, aber jeder Punkt darauf ist eine harte Voraussetzung. Fehlt einer, scheitert die Anmeldung — meist ohne brauchbare Fehlermeldung:

- › SharePoint Server Subscription Edition. OIDC 1.0 gibt es in keiner älteren Version, auch nicht per Nachrüstung.
- › HTTPS auf der föderierten Zone. Ein Zertifikat gehört an die Webanwendung, per Set-SPWebApplication oder gleich bei der Erweiterung der Zone.
- › Ein nonce-Cookie-Zertifikat mit privatem Schlüssel auf jedem Server der Farm. Ab Version 24H2 übernimmt das die Zertifikatsverwaltung der Farm über `$farm.UpdateNonceCertificate()`; davor musstest du es je Server importieren und dem Anwendungspoolkonto Leserechte auf den privaten Schlüssel geben.
- › Eine Anwendungsregistrierung in Entra ID mit der Farm-URL als Umleitungsziel, aktivierten ID-Token, den delegierten Berechtigungen email und profile sowie den optionalen Ansprüchen email und upn. Im Manifest wird das Umleitungsziel auf die Form mit abschließendem Platzhalter erweitert.
- › Ein SPTrustedIdentityTokenIssuer mit Identity Claim, DefaultClientIdentifier und Scope. Für den Metadatenendpunkt unterstützt SharePoint bislang nur die Variante 1.0 der Ermittlungsadresse.
- › Eine Zone mit Windows-Authentifizierung, die bleibt — der Suchcrawl braucht sie.

Die Einrichtung in Kurzform

Die Reihenfolge ist nicht beliebig: Ohne nonce-Zertifikat kannst du den Tokenaussteller zwar anlegen, die Anmeldung scheitert aber später an einer Stelle, an der niemand sucht. Arbeite dich von unten nach oben durch.

Schritt	Wo	Was passiert
1 · Anwendung registrieren	Entra ID	Umleitungsziel setzen, ID-Token aktivieren, optionale Ansprüche und Gruppenanspruch ergänzen, Mandanten- und Anwendungs-ID notieren
2 · nonce-Zertifikat	SharePoint-Farm	Zertifikat erzeugen, in die Zertifikatsverwaltung importieren, farmweit als nonce-Zertifikat setzen
3 · Tokenaussteller	SharePoint-Farm	New-SPTrustedIdentityTokenIssuer mit Anspruchszuordnung, Metadatenendpunkt und DefaultClientIdentifier
4 · Zone anlegen	SharePoint-Farm	Neue Webanwendung oder Erweiterung einer bestehenden auf eine eigene Zone mit HTTPS und dem neuen Anbieter
5 · Zertifikat binden	SharePoint-Farm	Serverzertifikat der Zone zuweisen, alternative Zugriffszuordnungen prüfen

6 • Administratoren setzen	Websitesammlung	Je ein Windows-Konto und ein föderiertes Konto als Administrator eintragen — als Rückfallebene unbezahlbar
7 • People Picker	Benutzerprofildienst	Profilabgleich aus dem Mitgliederspeicher des Anbieters einrichten, damit die Personenauswahl wieder prüft statt rät

Tabelle 2: Die Einrichtungsschritte in der Reihenfolge, in der sie gemacht werden wollen.

```
# 1) Anspruch festlegen, der zur SharePoint-Identität wird
#   $upnClaimType enthält den Anspruchstyp für den
#   Benutzerprinzipalnamen
$claim = New-SPClaimTypeMapping `
    -IncomingClaimType $upnClaimType `
    -IncomingClaimTypeDisplayName 'UPN' -SameAsIncoming

# 2) Tokenaussteller anlegen; $metadata verweist auf die
#   Ermittlungsadresse des Mandanten in der Variante 1.0,
#   $clientId auf die Anwendungs-ID der Registrierung
New-SPTrustedIdentityTokenIssuer -Name 'Entra ID' -Description 'Entra ID' `
    -ClaimsMappings $claim -IdentifierClaim $claim.InputClaimType `
    -DefaultClientIdentifier $clientId `
    -MetadataEndPoint $metadata -Scope 'openid profile'

# 3) Anbieter an eine Zone binden
$ap = New-SPAuthenticationProvider -TrustedIdentityTokenIssuer `
    (Get-SPTrustedIdentityTokenIssuer 'Entra ID')
```

Die Wahl des Identity Claim ist die Entscheidung, die dich am längsten begleitet. Sie bestimmt, wie Benutzer in Berechtigungen gespeichert werden, und sie lässt sich später nur mit erheblichem Aufwand ändern. Nimm einen Wert, der wirklich eindeutig und stabil ist. E-Mail-Adressen sind bequem und ändern sich bei Heirat, Umbenennung oder Fusion. Der Benutzerprinzipalname ist üblicherweise die bessere Wahl.

People Picker, Suchcrawl und andere Nebenwirkungen

Die föderierte Anmeldung hat eine unangenehme Eigenschaft, die dich am ersten Tag im Betrieb trifft: Die Personenauswahl prüft nichts mehr. Sie zeigt jede Eingabe an, als wäre sie ein gültiger Anspruch — auch Tippfehler, auch erfundene Adressen. Wer sich vertippt, vergibt eine Berechtigung an ein Konto, das es nicht gibt, und wundert sich drei Wochen später. In der Subscription Edition löst du das über die Personenauswahl, die den Benutzerprofildienst als Datenquelle nutzt. Dafür muss der Profilabgleich aus dem Mitgliederspeicher des Anbieters laufen, und das ist ein eigenes kleines Projekt.

Der Suchcrawl ist der zweite Punkt. Er benötigt eine Zone mit Windows-Authentifizierung. In der Praxis heißt das: Die Standardzone bleibt bei Windows, die föderierte Anmeldung läuft auf einer zweiten Zone mit eigener URL. Das ist auch aus anderen Gründen die bessere Bauform, hat aber eine Konsequenz, die du unbedingt einplanen musst — dazu gleich der Warnkasten.

Drittens die Anwendungen auf dem Arbeitsplatz. Office-Programme, eingebundene Netzlaufwerke, ältere Erweiterungen und alles, was SharePoint-Adressen aus E-Mails heraus öffnet, reagiert auf föderierte Anmeldung empfindlicher als ein Browser. Plane einen echten Pilotbetrieb mit den Abteilungen ein, die täglich Dokumente aus SharePoint heraus bearbeiten. Nicht mit drei Leuten aus der IT, die den Sonderfall schon kennen.

WARNUNG • Die Windows-Zone ist die offene Hintertür

Sobald du eine zweite Zone für die föderierte Anmeldung baust, existiert dieselbe Websitesammlung

unter zwei Adressen: einmal mit MFA, einmal ohne. Wer die alte URL kennt — und das sind alle, die sie seit Jahren im Lesezeichen haben — meldet sich weiterhin ohne zweiten Faktor an. Dein schöner neuer Anmeldefluss ist dann ein Angebot, kein Zwang.

- › Die Windows-Zone gehört auf das interne Netz begrenzt, per Firewall und per Bindung an interne Adressen.
- › Aus dem Internet erreichbar ist ausschließlich die föderierte Zone beziehungsweise der Proxy davor.
- › Dienstkonten für Crawl, Sicherung und Schnittstellen bekommen die Windows-Zone. Menschen nicht.
- › Prüfe die alternativen Zugriffszuordnungen: Was dort steht, landet in Benachrichtigungen und generierten Links.

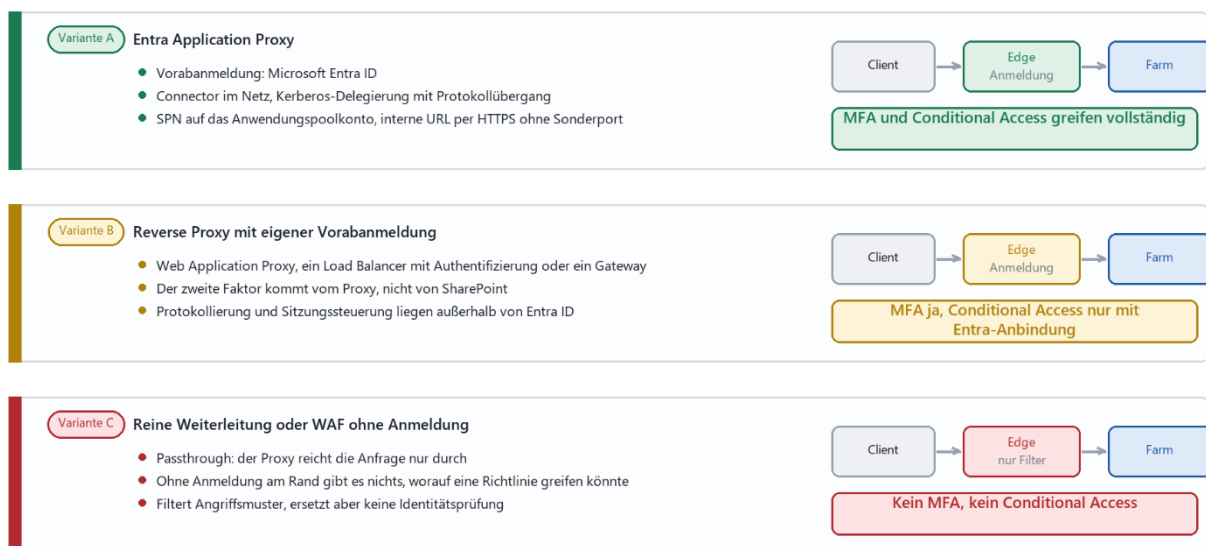
Wenn du an dieser Stelle ohnehin am Anmeldeverhalten schraubst, lohnt sich der Blick auf die phishingresistenten Verfahren: Ein föderierter SharePoint profitiert unmittelbar davon, weil der Faktor in Entra ID fällt. Wie das in der Praxis aussieht, steht in [Passwordless: FIDO2 und Passkeys in der Praxis](#). Und wenn im selben Zug alte Anmeldeverfahren verschwinden sollen, hilft [Legacy Authentication endgültig abschalten](#).

Weg 3: Reverse Proxy und Entra Application Proxy

Die dritte Familie von Lösungen lässt SharePoint so, wie es ist, und setzt die Anmeldung davor. Das klingt nach Notlösung, ist aber in zwei Fällen genau richtig: wenn deine Farm noch nicht auf der Subscription Edition läuft und du sie nicht anfassen willst, und wenn es dir konkret um den Zugriff von außen geht — was in der Praxis der Fall ist, der die Auditoren umtreibt.

Drei Reverse-Proxy-Varianten und ihr Sicherheitsgewinn

Entscheidend ist nicht das Blech davor, sondern wer die Anmeldung tatsächlich durchführt.



In allen drei Varianten bleibt die interne Windows-Zone erreichbar. Wer sie nicht absichert, hat den Proxy nur dekorativ aufgestellt.

Skizze 4: Drei Bauformen, drei sehr unterschiedliche Ergebnisse. Der Unterschied liegt allein in der Voranmeldung.

Entra Application Proxy mit Kerberos-Delegierung

Die interessanteste Variante: Du veröffentlichst die Farm als Anwendung in Entra ID. Ein Connector im eigenen Netz baut eine ausgehende Verbindung auf, es muss also kein Port von außen geöffnet werden. Die Vorabanmeldung übernimmt Entra ID, samt Conditional Access und MFA. Anschließend besorgt der Connector im Namen des angemeldeten Benutzers ein Kerberos-Ticket und reicht die Anfrage an die Farm weiter — die dabei glaubt, es handle sich um eine ganz normale interne Windows-Anmeldung.

Der Mechanismus dahinter ist eingeschränkte Delegierung mit Protokollübergang. Du registrierst einen Dienstprinzipalnamen auf das Anwendungspoolkonto der Webanwendung und erlaubst dem Connector-Computer, für genau diesen Dienst zu delegieren — mit der Einstellung, jedes Authentifizierungsprotokoll zuzulassen. Das ist genau die Konstruktion, die in [Kompetenzbereich Kerberos](#) im Detail beschrieben ist, und sie ist der Grund, warum Kerberos in dieser Geschichte doch noch eine Hauptrolle bekommt: nicht als Sicherheitsmerkmal, sondern als Übersetzungsschicht.

Es gibt dabei eine Reihe von Einzelheiten, an denen Projekte regelmäßig hängenbleiben. Die interne Adresse muss über HTTPS laufen, ohne Sonderport, und im DNS ein echter Hosteintrag sein — kein Alias. Die Übersetzung von Adressen in Kopfzeilen und im Antworttext bleibt ausgeschaltet, dafür müssen die alternativen Zugriffszuordnungen in SharePoint die interne und die externe Adresse korrekt abbilden. Das Anwendungspoolkonto muss ein Domänenkonto sein, sonst funktioniert Kerberos nicht. Und für die delegierte Anmeldeidentität wählst du je nach Gesamtstruktur den lokalen Kontonamen oder den Benutzerprinzipalnamen.

Klassischer Reverse Proxy und WAF

Alles, was eine eigene Vorabanmeldung mitbringt — ein Anwendungsgateway, ein Load Balancer mit Authentifizierungsmodul, ein Fernzugriffsportal — kann ebenfalls einen zweiten Faktor erzwingen. Das ist legitim, und in Umgebungen mit einer etablierten Zugangsplattform oft der Weg des geringsten Widerstands. Du bezahlst allerdings damit, dass Anmeldeprotokolle, Sitzungssteuerung und Richtlinien an einer zweiten Stelle gepflegt werden. Wer Auswertungen zentral fahren will, hat damit eine zusätzliche Datenquelle statt einer weniger.

WARNUNG · Passthrough ist kein Schutz

Wenn du eine Anwendung im Application Proxy mit Vorabanmeldung „Passthrough“ veröffentlichst, findet in Entra ID keine Authentifizierung statt. Damit greifen auch keine Conditional-Access-Richtlinien — sie werden ausschließlich für erfolgreich in Entra ID angemeldete Konten ausgewertet. Dasselbe gilt für eine Web Application Firewall, die nur Angriffsmuster filtert: Sie ist eine sinnvolle zusätzliche Schicht, aber sie ersetzt keine Identitätsprüfung. Wer Passthrough konfiguriert und im Sicherheitskonzept „MFA über Entra ID“ einträgt, dokumentiert eine Maßnahme, die es nicht gibt.

Entscheiden, planen, umschalten

Vier Wege, drei brauchbare Ergebnisse. Welcher es wird, hängt an wenigen Fragen: Auf welcher Version läuft die Farm? Steht AD FS ohnehin schon? Geht es um den Zugriff von außen oder um alle Zugriffe? Und wie viel Betriebsaufwand willst du dauerhaft tragen?

Weg	Voraussetzung	MFA	Conditional Access	Aufwand	Grenzen
AD FS mit MFA-Adapter	SharePoint 2013+, AD FS 2016+, Entra ID P1	ja	nein, nur Anspruchsregeln	hoch im Betrieb	eigene Serverrolle, keine Gerätekonformität, keine Selbstregistrierung
Entra ID als IdP (OIDC)	nur Subscription Edition	ja	vollständig	mittel bei der Einführung	Personenauswahl, Office-Anwendungen, Zonenschnitt
Entra Application Proxy	SharePoint 2016+, Connector, Kerberos-Delegierung	ja	vollständig	mittel	schützt nur den Weg über den Proxy
Reverse Proxy mit eigener Anmeldung	beliebige Version	ja	nur mit Entra-Anbindung	abhängig von der Plattform	zweite Stelle für Richtlinien und Protokolle
Windows-Authentifizierung	vorhanden	nein	nein	keiner	kein zweiter Faktor, NTLM als Rückfallebene

Tabelle 3: Die Wege im direkten Vergleich. Die Spalte „Grenzen“ ist die, über die im Projekt gestritten wird.

Zonen sauber schneiden

Ganz gleich, welchen Weg du nimmst: Der Zonenschnitt entscheidet, ob die Maßnahme wirkt oder nur existiert. Eine Webanwendung kann bis zu fünf Zonen haben, jede mit eigener Adresse und eigener Authentifizierung. Die Standardzone sollte die sicherste Konfiguration tragen, weil sie greift, wenn eine Anfrage keiner Zone zugeordnet werden kann — und weil generierte Links auf sie zeigen. Gleichzeitig braucht der Crawl irgendwo Windows. Diese beiden Anforderungen musst du bewusst gegeneinander abwägen, statt sie dem Zufall zu überlassen.

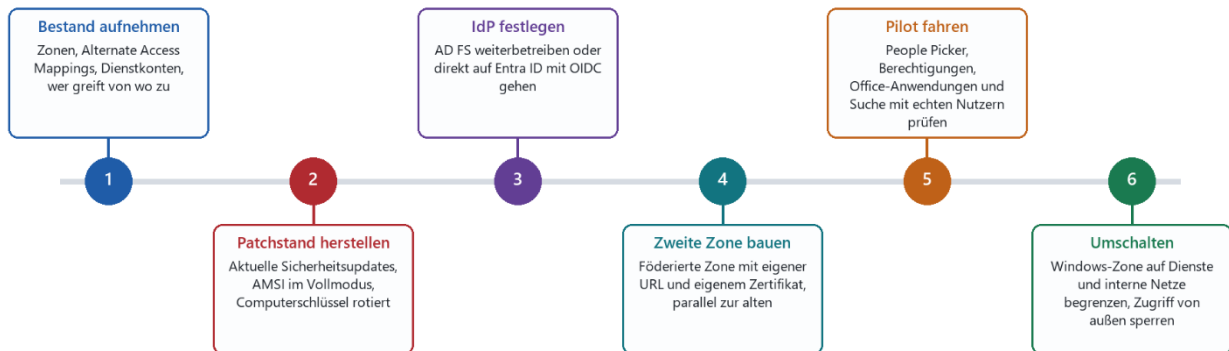
Zone	Adressmuster	Anmeldung	Wer	Erreichbar von
Standard	portal — öffentlich bekannter Name	föderiert (OIDC oder SAML)	alle Personen	intern und, sofern gewünscht, extern
Intranet	sp-intern — nur im internen Namensraum	Windows (Kerberos)	Suchcrawl, Dienstkonten, Schnittstellen	ausschließlich intern, per Firewall begrenzt
Extranet	extern — eigener Name für Partner	föderiert mit strengerer Richtlinie	externe Beteiligte	extern über Proxy, nur zugewiesene Konten

Tabelle 4: Ein bewährter Zonenplan für eine föderierte Farm.

Der Fahrplan

Fahrplan: von der Windows-Farm zur MFA-pflichtigen Anmeldung

Sechs Schritte, von denen nur zwei technisch sind. Der Rest ist Bestandsaufnahme und Disziplin.



Schritt 2 zuerst: Eine Farm mit offenen Lücken wird durch MFA nicht sicher, sondern nur schwerer zu bedienen.

Skizze 5: Sechs Schritte. Zwei davon sind technisch, vier sind Bestandsaufnahme, Test und Disziplin.

Schritt 1 wird regelmäßig übersprungen und ist regelmäßig der Grund, warum Schritt 6 scheitert. Bevor du irgendetwas umstellst, brauchst du eine belastbare Liste: welche Webanwendungen, welche Zonen, welche alternativen Zugriffszuordnungen, welche Dienstkonten, welche Schnittstellen, welche Skripte greifen von wo zu. In fast jeder gewachsenen Farm findet sich dabei mindestens eine Integration, an die sich niemand mehr erinnert und die genau am Umstellttag auffällt. Wie du das mit dem übrigen MFA-Rollout verzahnst, steht in [MFA in Microsoft 365 richtig einführen](#); den Gesamtüberblick über die Bausteine findest du im Kompetenzbereich [Microsoft 365 Security](#).

Erst patchen, dann föderieren

Es gibt einen Grund, warum Schritt 2 vor allem anderen steht. Im Juli 2025 wurde eine Angriffskette gegen lokale SharePoint-Server aktiv ausgenutzt, die unter dem Namen ToolShell bekannt geworden ist. Über eine Deserialisierungslücke ließ sich die Authentifizierung umgehen, kryptografisches Schlüsselmaterial auslesen und beliebiger Code auf dem Server ausführen. Microsoft hat dabei zwei staatlich zugeordnete Gruppen sowie einen weiteren Akteur benannt, der über denselben Weg Ransomware ausgerollt hat.

Der unangenehme Teil daran: Wenn Angreifer die Computerschlüssel einer Farm besitzen, können sie sich gültige Anmeldeinformationen selbst ausstellen. Kein Anmeldefluss der Welt hilft dagegen — auch keiner mit zweitem Faktor. Die Empfehlung lautete deshalb: Sicherheitsupdates einspielen, die AMSI-Integration zusammen mit Defender aktivieren und danach die ASP.NET-Computerschlüssel rotieren. In der Subscription Edition ist die automatische Rotation der Computerschlüssel inzwischen ein reguläres Produktmerkmal, und die AMSI-Prüfung des Anfragetexts läuft standardmäßig im Vollmodus.

WICHTIG · MFA ist die zweite Maßnahme, nicht die erste

Eine ungepatchte, aus dem Internet erreichbare SharePoint-Farm wird durch eine schöne Anmeldeseite nicht sicherer. Sie wird nur umständlicher zu bedienen — für die eigene Belegschaft, nicht für Angreifer. Die Reihenfolge lautet: Aktualisieren, härten, Schlüsselmaterial erneuern, prüfen,

ob bereits jemand da war. Erst danach wird der Anmeldefluss umgebaut.

- › Prüfe, ob die Farm überhaupt aus dem Internet erreichbar sein muss. Sehr oft lautet die ehrliche Antwort: nein, nur für fünf Personen — und dafür gibt es einen Proxy.
- › Aktiviere die AMSI-Integration und stelle sicher, dass ein Virenschutz auf allen Servern der Farm aktiv ist.
- › Rotiere die Computerschlüssel nach jedem Verdachtsfall, nicht erst nach dem Nachweis.

Wie eine solche Kompromittierung im Ernstfall abläuft und was in den ersten Stunden zählt, ist im Dossier [TerminalFix und der Berlin-Hack](#) nachgezeichnet. Für die Vorbereitung auf den Fall, dass es doch passiert, sind [Ransomware-Vorsorge in Microsoft 365](#) und [Incident-Response-Plan für Microsoft 365](#) die passenden Anlaufstellen.

Typische Fehlerbilder

Symptom	Wahrscheinliche Ursache	Prüfen
Anmeldung endet in einer Schleife	nonce-Zertifikat fehlt auf einem Server oder das Anwendungspoolkonto hat keine Leserechte auf den privaten Schlüssel	Zertifikat auf jedem Server, Berechtigung auf den privaten Schlüssel, Farmeigenschaft
„Keine gültige starke Authentifizierungsmethode gefunden“	Die zusätzliche Methode ist an AD FS nicht aktiviert oder der Betroffene hat keine Methode registriert	Authentifizierungsmethoden in AD FS, Registrierungsstand des Kontos
Berechtigung vergeben, Zugriff verweigert	Identity Claim passt nicht zum eingetragenen Wert, oder die Personenauswahl hat einen Tippfehler durchgewinkt	Anspruchszuordnung, Wert im Token, Profilabgleich
Suche findet nichts mehr	Der Crawl hat keine Zone mit Windows-Authentifizierung mehr	Zonen der Webanwendung, Inhaltsquelle, Crawlkonto
Anmeldung ohne zweiten Faktor möglich	Die alte Windows-Zone ist weiterhin erreichbar	Alternative Zugriffszuordnungen, Firewallregeln, IIS-Bindungen
Zugriff bricht nach zwei Jahren ab	Das MFA-Zertifikat an AD FS ist abgelaufen	Gültigkeit des Zertifikats je AD-FS-Server, Erneuerungsvorgang

Tabelle 5: Was im Betrieb schiefgeht — und wo du zuerst nachsiehst.

Damit du solche Zustände nicht erst durch Anrufe erfährst, gehört eine Überwachung dazu: Anmeldeprotokolle in Entra ID, Warnungen auf auffällige Muster und, wo vorhanden, die Auswertung im SIEM. Die Grundlagen dafür stehen in [Alert Policies und Benachrichtigungen richtig aufsetzen](#) und [Microsoft Sentinel anbinden: wann es sich lohnt](#). Für die lokale Verzeichnisumgebung, an der die Farm hängt, ist [Defender for Identity: das Active Directory im Blick](#) der passende Baustein.

Häufige Fragen

Kann ich MFA für SharePoint Server 2019 erzwingen?

Ja, aber nicht mit Entra ID als direktem Identitätsanbieter. Für 2019 bleiben dir SAML 1.1 über AD FS mit MFA-Adapter oder ein vorgeschalteter Proxy mit Vorabanmeldung. Beides funktioniert. Wichtiger ist allerdings: SharePoint Server 2019 hat am 14. Juli 2026 das Supportende erreicht und bekommt keine Sicherheitsupdates mehr. Investiere den Aufwand lieber in den Umstieg auf die Subscription Edition — dort bekommst du MFA praktisch als Beifang.

Brauche ich für Entra ID als Identitätsanbieter zwingend die Subscription Edition?

Ja. OpenID Connect 1.0 ist ausschließlich in der Subscription Edition implementiert. Es gibt kein Nachrüstpaket und keinen unterstützten Umweg für 2016 oder 2019. Wer Entra ID als Anmeldestelle vor einer älteren Farm haben will, kommt nur über den Application Proxy dorthin — dann meldet sich der Benutzer in Entra ID an, und die Farm sieht davon nichts.

Reicht Conditional Access, wenn ich den Entra Application Proxy nutze?

Nur wenn die Vorabanmeldung auf Microsoft Entra ID steht. Bei Passthrough findet keine Anmeldung in Entra ID statt, und ohne Anmeldung greift auch keine Richtlinie. Das ist der häufigste Konfigurationsfehler in dieser Variante, weil Passthrough beim Testen so schön reibungslos funktioniert.

Was passiert mit dem Suchcrawl, wenn ich auf föderierte Anmeldung umstelle?

Der Crawl braucht eine Zone mit Windows-Authentifizierung. Wenn du sie ihm nicht gibst, indexiert er nichts mehr, und die Suche liefert leere Ergebnisse — was üblicherweise erst drei Tage später jemandem auffällt. Behalte also eine interne Zone mit Windows bei und beschränke sie strikt auf das interne Netz und auf Dienstkonten.

Funktionieren die Office-Programme mit föderierter Anmeldung?

Grundsätzlich ja, aber sie sind empfindlicher als der Browser. Direkt geöffnete Dokumente, eingebundene Netzlaufwerke und ältere Erweiterungen sind die Stellen, an denen es hakt. Das ist kein Grund, es zu lassen — es ist ein Grund, einen echten Pilotbetrieb mit den Abteilungen zu fahren, die den ganzen Tag Dokumente aus SharePoint heraus bearbeiten, statt mit drei wohlwollenden Testpersonen aus der IT.

Welche Lizenz brauche ich für MFA an AD FS?

Der MFA-Adapter greift auf den Entra-MFA-Dienst zu, und der ist in Entra ID P1 beziehungsweise P2 enthalten, ebenso in der Enterprise Mobility Suite. Der Adapter selbst kostet nichts und ist in Windows Server 2016 und höher bereits enthalten. Was du zusätzlich brauchst, ist eine bestehende Föderation deiner Verzeichnismgebung mit Entra ID.

Kann ich AD FS und Entra ID parallel betreiben?

Ja, und in Übergangsphasen ist das oft der pragmatische Weg. Eine Webanwendung kann mehrere Anbieter auf derselben Zone haben, und du kannst mehrere Tokenaussteller in der Farm konfigurieren. Der Nutzer bekommt dann eine Auswahlseite, was erklärungsbedürftig ist. Eleganter: verschiedene Zonen mit verschiedenen Anbietern und einer klaren Kommunikation, welche Adresse für wen gilt. Beachte dabei, dass ein Signaturzertifikat nur einmal pro Farm für einen Tokenaussteller verwendet werden kann.

Wie verhindere ich, dass jemand die alte URL benutzt und MFA umgeht?

Netzwerkseitig. Die Windows-Zone bekommt eine interne Adresse, eine IIS-Bindung auf interne Schnittstellen und eine Firewallregel, die den Zugriff auf Dienstknoten und definierte Netze beschränkt. Rein organisatorisch — „bitte benutzt ab jetzt die neue Adresse“ — funktioniert es nicht. Das ist keine Vermutung, das ist Erfahrungswert.

Was mache ich mit Notfallkonten?

Genau das, was du im Mandanten auch machst: ein bis zwei Notfallkonten mit langen, an getrennter Stelle hinterlegten Anmeldeinformationen, ausgenommen von den Richtlinien, überwacht bei jeder Verwendung. In der Farm kommt dazu, dass jede Websitesammlung mindestens einen Administrator über die Windows-Zone haben sollte — wenn die Föderation ausfällt, ist das dein Weg zurück ins System.

Ist AD FS damit ein Auslaufmodell?

Für neue Vorhaben würde ich es nicht mehr aufbauen, wenn Entra ID als Anbieter infrage kommt. Wo AD FS steht und trägt, gibt es allerdings keinen Grund zur Hektik — und für Szenarien, in denen die Anmeldung aus regulatorischen Gründen im eigenen Rechenzentrum stattfinden muss, ist es weiterhin die naheliegende Antwort. Die Subscription Edition kann AD FS wahlweise über SAML 1.1 oder über OpenID Connect einbinden.

Fazit

MFA für SharePoint Server on-premises ist kein Häkchen, sondern ein Umbau des Anmeldeflusses. Wie groß dieser Umbau ausfällt, hat deine Farm längst entschieden: Auf der Subscription Edition führst du Entra ID als Identitätsanbieter ein, bekommst Conditional Access, Gerätekonformität und passwortlose Verfahren gleich mit und beschäftigst dich anschließend hauptsächlich mit Zertifikaten, Personenauswahl und Zonenschnitt. Auf allen älteren Versionen bleiben AD FS mit MFA-Adapter oder ein Proxy mit Vorabanmeldung — beides funktioniert, beides ist mehr Betrieb.

Was in keinem Fall funktioniert, ist die Hoffnung, Kerberos werde das schon irgendwie richten. Ein Ticket beweist, dass ein Ticket ausgestellt wurde. Mehr nicht. Die eigentliche Arbeit steckt ohnehin nicht in den Cmdlets, sondern in der Bestandsaufnahme: welche Zonen es gibt, wer über welche Adresse kommt, welche Schnittstelle seit 2017 mit einem Dienstkonto arbeitet, das

niemand mehr kennt. Wer diese Liste hat, schaltet an einem Wochenende um. Wer sie nicht hat, schaltet an drei Wochenenden wieder zurück.

Und wenn die Anmeldung steht, lohnt der Blick auf das, was in den Bibliotheken tatsächlich liegt: Klassifizierung und Schutz von Inhalten reichen mit dem passenden Werkzeug bis in lokale Ablagen hinein — der Einstieg dazu steht im [Kompetenzbereich Microsoft Purview](#). Wenn du den Umbau nicht allein stemmen willst, ist die [Microsoft-365-Security-Beratung](#) der Weg, auf dem wir das gemeinsam sortieren — von der Bestandsaufnahme bis zum Umschalttag.

Weiter im Thema

- › [MFA für SharePoint Online erzwingen](#) — dieselbe Anforderung, ein Bruchteil des Aufwands
- › [MFA in Microsoft 365 richtig einführen](#) — der Rahmen, in den dieser Umbau gehört
- › [Conditional Access: Baselines, die nicht nerven](#) — die Richtlinien, die hinter Weg 2 stehen
- › [Kompetenzbereich Kerberos](#) — Tickets, Dienstprinzipalnamen und Delegierung im Detail
- › [Passwordless: FIDO2 und Passkeys in der Praxis](#) — der phishingresistente Faktor für die föderierte Zone
- › [Break-Glass-Konten anlegen und überwachen](#) — der Weg zurück, wenn die Föderation ausfällt
- › [Tenant-Härtung: die 20 wichtigsten Schrauben](#) — was rund um die Anmeldung sonst noch fest sein sollte
- › [Zero Trust im Mittelstand: pragmatisch statt dogmatisch](#) — warum der Zonenschnitt mehr ist als ein Detail
- › [Schulung Microsoft 365 Security](#) — wenn das Team den Umbau selbst tragen soll