

SPN, DNS und Kerberos für ADFS – warum die interne Anmeldung auf Formular zurückfällt

WISSEN

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

› [Active Directory Federation Services](#)

BERATUNG

SPN-Wildwuchs, DNS-Altlasten und Browser-Richtlinien gemeinsam durchleuchten – mit Befund statt Bauchgefühl.

› [Consulting zu ADFS](#)

SCHULUNG

Kerberos, SPNs und WIA-Diagnose im Workshop an einer echten Farm kaputtmachen und reparieren.

› [ADFS-Schulungen](#)

Es ist Montagmorgen, der Kaffee ist noch zu heiß, und im Ticketsystem steht der Klassiker: „Seit dem Wochenende muss ich mich im Büro bei Microsoft 365 wieder mit Benutzername und Kennwort anmelden. Das war doch früher automatisch?“ War es. Irgendwer hat am Freitag „nur schnell“ einen DNS-Eintrag aufgeräumt, ein altes Dienstkonto reaktiviert oder den Browser-Rollout auf Chrome umgestellt. ADFS läuft weiter, die Anmeldung funktioniert auch – nur eben nicht mehr unsichtbar. Aus Single Sign-on ist Single Sign-Ärger geworden.

Genau dieses Symptom nimmt sich dieser Beitrag vor: Du sitzt im internen Netz, an einem domänenverbundenen Rechner, mit einem Domänenkonto angemeldet – und ADFS zeigt dir trotzdem die Anmeldemaske. Die Grundlagen zu Farm, Proxy und Claims setzen wir voraus, die findest du auf der Pillar-Seite [Active Directory Federation Services](#). Und weil ein guter Teil der Ursachen in Kerberos steckt, lohnt sich für das Fundament ein Abstecher in unseren Leitfaden [Microsoft Kerberos](#) – dort steht, was ein Ticket Granting Ticket ist, warum Uhrzeiten wichtig sind und wie der KDC Dienste findet. Hier geht es um die Anwendung auf ADFS: SPN, DNS, Browserzone, User-Agents und die Frage, wer eigentlich entscheidet, ob du ein Formular siehst.

Vorweg ein Befund, der dir viel Zeit spart: Das ADFS-Formular und das graue Windows-Popup sind zwei völlig verschiedene Symptome. Das Formular ist fast immer eine bewusste Entscheidung von ADFS, bevor Kerberos überhaupt ins Spiel kommt. Das Popup ist fast immer ein Kerberos- oder NTLM-Problem. Wer beides in einen Topf wirft, dreht drei Tage an SPNs, während in Wahrheit der Browser gar nicht auf der Gästeliste steht.

FAKTEN – Die Kurzfassung für Eilige

ADFS bietet die integrierte Windows-Authentifizierung (WIA) nur an, wenn die Anfrage aus dem Intranet kommt, also nicht über den Web Application Proxy, und der User-Agent des Browsers zu einem Eintrag in WIASupportedUserAgents passt. Sonst gibt es das Formular.

Seit ADFS 2016 enthält die Standardliste das Muster `=~Windows\s*NT.*Edg.*` für Microsoft Edge. Chrome und Firefox musst du selbst ergänzen.

Das ADFS-Dienstkonto braucht den SPN `HOST/sts.contoso.de` – genau einmal im Forest. Der Browser fragt zwar nach `HTTP/sts.contoso.de`, der KDC bildet HTTP standardmäßig auf HOST ab.

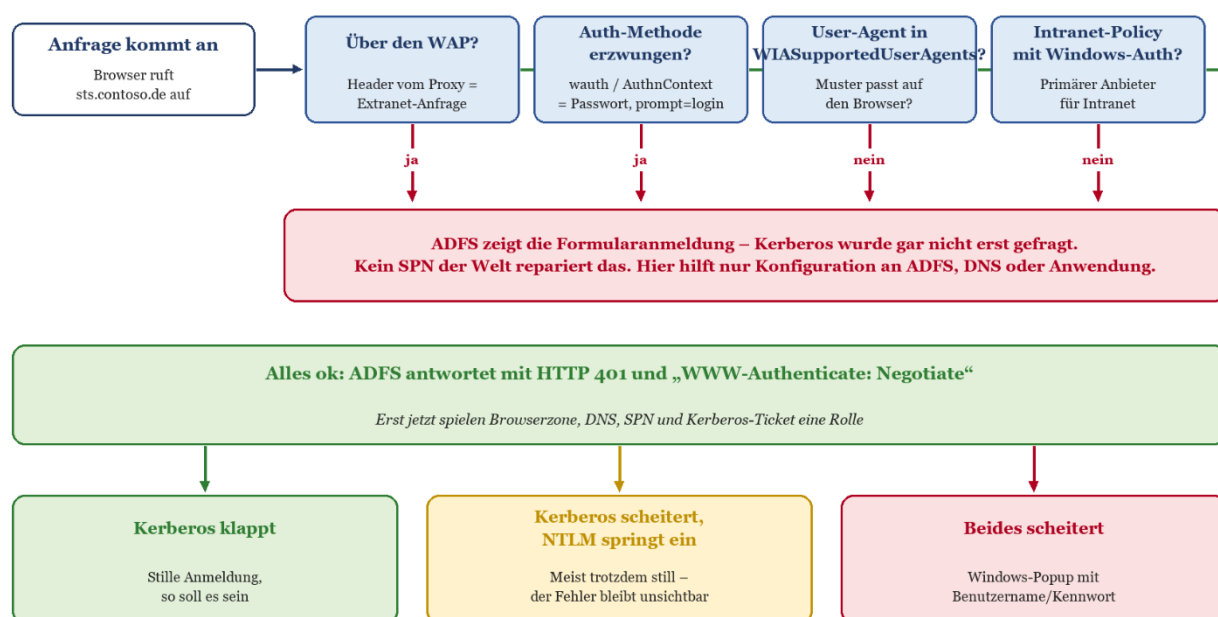
Der Farmname muss laut Microsoft ein A-Record sein, kein CNAME. Browser unter Windows bilden den SPN sonst aus dem Zielnamen des CNAME.

Der Browser schickt ein Kerberos-Ticket nur ohne Nachfrage, wenn `sts.contoso.de` in der Zone „Lokales Intranet“ liegt (oder in der AuthServerAllowlist von Edge und Chrome steht).

Scheitert Kerberos, springt meist NTLM leise ein. Der Fehler bleibt unsichtbar, bis jemand NTLM einschränkt.

Skizze 1: Wie ADFS entscheidet – Windows-Anmeldung oder Formular

Bevor Kerberos überhaupt eine Chance bekommt, hat ADFS schon viermal abbiegen können



Merksatz: Das ADFS-Formular ist fast nie ein Kerberos-Problem, sondern eine Entscheidung von ADFS. Das graue Windows-Popup dagegen ist fast immer eines. Wer beides verwechselt, sucht drei Tage am falschen Ende.

Skizze 1: ADFS prüft vier Dinge, bevor es überhaupt „Negotiate“ anbietet. Scheitert eine dieser Prüfungen, kommt das Formular – und kein SPN der Welt hilft.

Formular oder Popup: Wer da eigentlich entscheidet

Der häufigste Denkfehler bei diesem Problem lautet: „Anmeldemaske heißt Kerberos kaputt.“ Das stimmt nur für das Popup. Das Formular mit deinem Firmenlogo stammt von ADFS selbst. ADFS entscheidet sich dafür, wenn es die Windows-Anmeldung für unpassend hält. Und das passiert an mehreren Stellen, lange bevor ein Ticket überhaupt angefordert wird.

Die vier Weichen vor dem ersten Ticket

Kommt eine Anfrage an, prüft ADFS zuerst, ob sie über den Web Application Proxy kam. Der Proxy kennzeichnet weitergeleitete Anfragen, ADFS behandelt sie dann als Extranet-Anfragen und wendet die Extranet-Authentifizierung an. Standard dort: Formular. Liegt dein internes DNS also falsch und zeigt sts.contoso.de auf den WAP statt auf die interne VIP, bekommt jeder im Büro das Formular – reproduzierbar, flächendeckend und völlig unabhängig vom SPN.

Die zweite Weiche ist die Anwendung. Fordert die Relying Party ausdrücklich eine Kennworteingabe an, gehorcht ADFS. Bei WS-Federation erkennst du das am Parameter wauth mit dem Wert urn:oasis:names:tc:SAML:1.0:am:password, bei SAML an einem AuthnContextClassRef mit urn:oasis:names:tc:SAML:2.0:ac:classes:Password. Bei Microsoft 365 kommt eine Spezialität dazu: Fordert Entra ID mit prompt=login eine frische Anmeldung an, übersetzt die Federation-Einstellung PromptLoginBehavior das je nach Wert in eine Kennwortabfrage. Dazu gleich mehr.

Die dritte Weiche ist der User-Agent. ADFS vergleicht die Browserkennung mit der Liste WIASupportedUserAgents. Passt nichts, schaltet ADFS auf Formular um – sofern WindowsIntegratedFallbackEnabled in der globalen Authentifizierungsrichtlinie auf True steht. Die vierte Weiche ist die Richtlinie selbst: Ist für das Intranet keine Windows-Authentifizierung als primärer Anbieter aktiv, gibt es auch intern nur das Formular.

```
# Auf einem ADFS-Knoten, PowerShell als Administrator
# Weiche 3: Welche Browser dürfen WIA?
Get-AdfsProperties | Select-Object -ExpandProperty WIASupportedUserAgents

# Weiche 3 und 4: Fallback und primäre Anbieter
Get-AdfsGlobalAuthenticationPolicy |
    Format-List PrimaryIntranetAuthenticationProvider,
                PrimaryExtranetAuthenticationProvider,
                WindowsIntegratedFallbackEnabled

# Nebenbei: Wie streng ist die Kanalbindung eingestellt?
Get-AdfsProperties | Format-List ExtendedProtectionTokenCheck
```

Die ADFS-Seite der Diagnose. Alle drei Cmdlets stammen aus dem ADFS-Modul und ändern nichts – du kannst sie gefahrlos im Betrieb ausführen.

Das Symptom richtig lesen

Bevor du irgendetwas änderst, schau dir also genau an, was die Leute sehen. Ein Screenshot aus dem Helpdesk ist hier mehr wert als drei Absätze Problembeschreibung. Die folgende Tabelle ordnet die Erscheinungsbilder ihren wahrscheinlichsten Ursachen zu.

Was du siehst	Wer hat entschieden	Wahrscheinliche Ursache	Erster Blick
ADFS-Formular mit Firmenlogo, bei allen internen Nutzern	ADFS	Intern löst sts.contoso.de auf den WAP auf, oder Intranet-Policy ohne Windows-Auth	nslookup, Get-AdfsGlobalAuthenticationPolicy
ADFS-Formular nur in Chrome oder Firefox, Edge klappt	ADFS	User-Agent fehlt in WIASupportedUserAgents	Get-AdfsProperties
ADFS-Formular nur bei einer bestimmten Anwendung	Anwendung	wauth, AuthnContext oder prompt=login erzwingen Kennwort	Anfrage im Browser-Entwicklertool ansehen
Graues Windows-Popup „Anmelden bei sts.contoso.de“	Browser	Kerberos und NTLM scheitern: Zone, SPN, CNAME oder Kanalbindung	klist, setspn, Zonen-Zuordnung
Keine Maske, aber auffällig langsame Anmeldung	niemand	Kerberos scheitert, NTLM rettet leise	klist: fehlt das Ticket für HTTP/sts...?
Nur einzelne Nutzer oder Standorte betroffen	wechselnd	Doppelter SPN, abweichende GPO, falscher DNS-Server am Standort	setspn -X, gpresult, nslookup je Standort

Tabelle 1: Symptom zuerst, Werkzeug danach. Die Spalte „Wer hat entschieden“ sagt dir, an welcher Stelle du überhaupt suchen musst.

WICHTIG — NTLM ist der Schweigsame im Raum

Scheitert Kerberos, verhandelt Negotiate meist stillschweigend NTLM. Die Anmeldung klappt dann weiterhin ohne Maske, und niemand merkt, dass Kerberos seit Jahren kaputt ist. Microsoft hat NTLM als veraltet eingestuft, viele Häuser schränken es per Richtlinie ein. Genau dann kommt der alte SPN-Fehler ans Licht – als Popup-Welle am Tag nach dem Härtings-Change.

Wenn du also NTLM einschränken willst: Prüfe vorher mit klist auf ein paar Clients, ob für HTTP/sts.contoso.de wirklich ein Kerberos-Ticket entsteht.

Wenn die Anwendung das Formular bestellt

Bei Microsoft 365 lohnt ein Blick auf die Federation-Einstellung PromptLoginBehavior. Diese Einstellung steuert, was Entra ID an ADFS schickt, wenn eine Anwendung mit prompt=login eine erneute Anmeldung verlangt. Mit translateToFreshPasswordAuthentication sendet Entra ID wauth

und wfresh, ADFS zeigt daraufhin das Formular. Mit nativeSupport geht prompt=login unverändert an ADFS, mit disabled wird gar nichts mitgeschickt. Früher stand in jeder Anleitung ein Befehl aus dem MSONline-Modul, heute ist Microsoft Graph PowerShell der Weg:

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

$fed = Get-MgDomainFederationConfiguration -DomainId contoso.de
$fed | Format-List DisplayName, PromptLoginBehavior

# Nur ändern, wenn du weißt, was die Anwendungen erwarten:
Update-MgDomainFederationConfiguration -DomainId contoso.de `
    -InternalDomainFederationId $fed.Id -PromptLoginBehavior nativeSupport

Disconnect-MgGraph
```

PromptLoginBehavior mit Microsoft Graph PowerShell prüfen. Der Schreibbefehl ist optional und betrifft nur Anfragen mit prompt=login – nicht die normale Anmeldung.

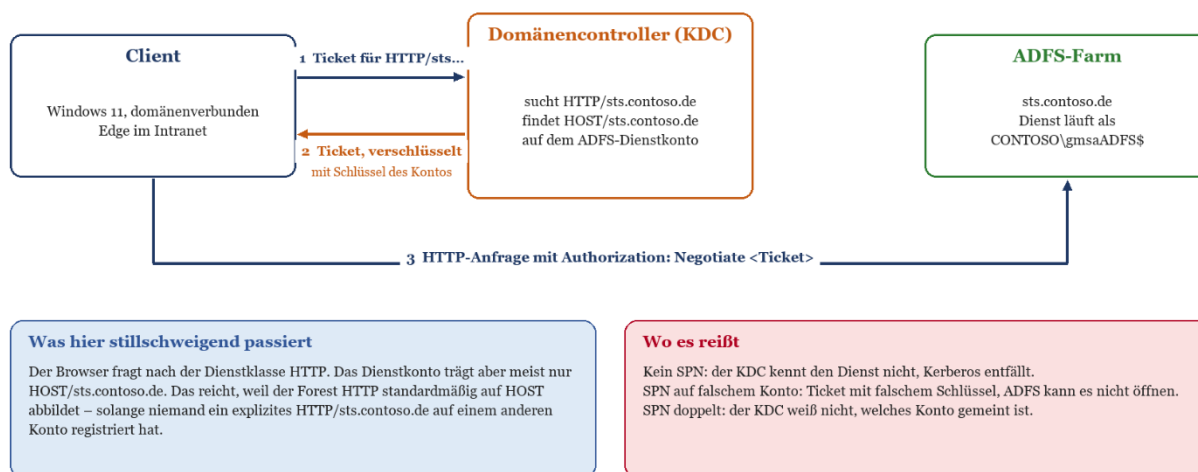
Ändere diese Einstellung nicht aus einer Laune heraus. Manche Anwendungen verlangen bewusst eine frische Kennworteingabe, etwa vor besonders heiklen Aktionen. Welche Regeln du auf ADFS-Seite zusätzlich setzen kannst, ohne Claim Rules zu jonglieren, zeigt der Beitrag [Access Control Policies in ADFS – Zugriffsregeln ohne Claim-Rule-Akrobatik](#).

SPN HOST/sts: Der Name, unter dem Kerberos ADFS findet

Bietet ADFS Negotiate an und der Browser spielt mit, braucht der Client ein Kerberos-Ticket für den Dienst. Er fragt beim KDC nach HTTP/sts.contoso.de. Der KDC sucht im Forest nach einem Konto mit passendem Service Principal Name und verschlüsselt das Ticket mit dessen Schlüssel. ADFS läuft als genau dieses Konto und kann das Ticket öffnen. So weit die Theorie – und so weit der Grund, warum der SPN auf genau dem Konto hängen muss, unter dem der ADFS-Dienst läuft.

Skizze 2: Woher der Browser sein Kerberos-Ticket bekommt

Der SPN ist die Adresse, unter der der KDC das richtige Konto für sts.contoso.de findet



In allen drei Fällen fällt Negotiate leise auf NTLM zurück, sofern NTLM erlaubt ist. Die Anmeldung funktioniert dann scheinbar – bis jemand NTLM einschränkt und das halbe Haus plötzlich Popups sieht.

Skizze 2: Der Browser fragt nach HTTP/sts.contoso.de, der KDC findet HOST/sts.contoso.de auf dem ADFS-Dienstkonto. Hängt der SPN woanders oder doppelt, reißt die Kette.

Warum HOST und nicht HTTP

In fast jeder ADFS-Farm steht auf dem Dienstkonto nur HOST/sts.contoso.de. Das irritiert, weil der Browser doch HTTP anfragt. Der Grund: Active Directory kennt eine Abbildungsliste, über die HOST stellvertretend für eine ganze Reihe von Dienstklassen steht, darunter HTTP. Findet der KDC kein explizites HTTP/sts.contoso.de, nimmt er HOST/sts.contoso.de. Das ist bequem – und gefährlich, sobald irgendwo ein explizites HTTP/sts.contoso.de auf einem anderen Konto herumliegt. Dazu gleich mehr.

Der ADFS-Konfigurationsassistent versucht bei der Farmeinrichtung, den SPN selbst zu setzen. Das gelingt, wenn das Konto, mit dem du die Farm einrichtest, dafür die Rechte im AD hat. Fehlen sie, bleibt die Farm ohne SPN – sie funktioniert dann trotzdem, nur eben mit NTLM oder Formular. Wie die Einrichtung sauber abläuft, steht in [ADFS-Farm installieren – Schritt für Schritt auf Windows Server 2022](#).

```
REM Welcher Dienst läuft unter welchem Konto?
sc.exe qc adfssrv

REM Wem gehört der SPN? (muss genau ein Treffer sein)
setspn -Q HOST/sts.contoso.de
setspn -Q HTTP/sts.contoso.de

REM Welche SPNs trägt das Dienstkonto? (gMSA mit $ am Ende)
setspn -L CONTOSO\gmsaADFS$

REM Fehlenden SPN setzen - -S prüft vorher auf Duplikate
setspn -S HOST/sts.contoso.de CONTOSO\gmsaADFS$
```

SPN-Grundcheck in der Eingabeaufforderung. setspn -S statt des alten -A: Der Schalter verweigert das Anlegen, wenn der SPN schon woanders existiert.

TIPP — Kurzname nur, wenn du ihn wirklich benutzt

Einen SPN für den Kurznamen HOST/sts brauchst du nur, wenn Clients ADFS tatsächlich über den Kurznamen aufrufen. Bei ADFS ist das praktisch nie der Fall – Anwendungen, Metadaten und Zertifikat sprechen den vollqualifizierten Namen. Weniger SPNs heißt weniger Gelegenheiten für Duplikate.

Ein SPN pro Farm, nicht pro Knoten: Alle ADFS-Server laufen unter demselben Dienstkonto, der SPN hängt am Konto, nicht an den Computerkonten der Knoten.

Doppelte SPNs finden mit setspn -X

Ein SPN darf im gesamten Forest nur einmal vorkommen. Kommt er doppelt vor, weiß der KDC nicht, welches Konto gemeint ist, und Kerberos für diesen Dienst ist kaputt. Der klassische Weg dorthin: Die Farm lief jahrelang unter einem normalen Benutzerkonto, dann wurde sie auf ein gMSA umgestellt, der SPN wurde auf dem neuen Konto gesetzt – und auf dem alten nie entfernt. Wie die Umstellung ohne solche Hinterlassenschaften gelingt, zeigt [gMSA als ADFS-Dienstkonto einrichten und umstellen](#).

```
REM Duplikate in der Domäne suchen
setspn -X

REM Duplikate im ganzen Forest suchen (dauert in großen Umgebungen)
setspn -X -F

REM Altlast vom falschen Konto entfernen
setspn -D HOST/sts.contoso.de CONTOSO\svc-adfs

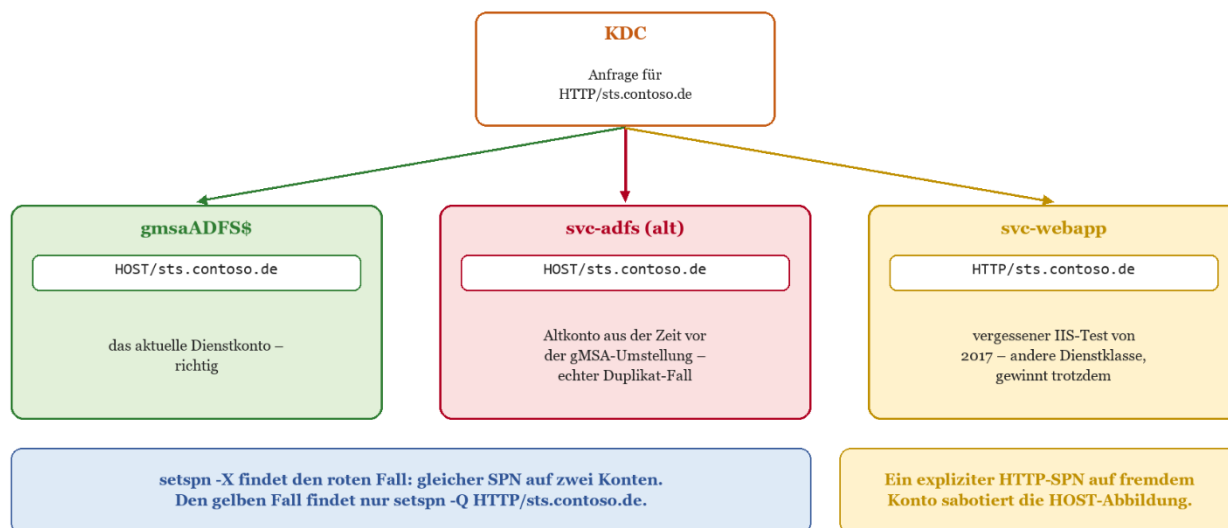
REM Auf dem Client: alte Tickets wegwerfen und neu anfordern
klist purge
```

```
klist get HTTP/sts.contoso.de
```

Duplikate finden und bereinigen. `setspn -X` listet alle doppelten SPNs, auch solche, die mit ADFS nichts zu tun haben – filtere die Ausgabe nach „sts“.

Skizze 4: Doppelte SPNs – und der Doppelgänger, den `setspn -X` nicht findet

Zwei Konten, ein Name: Der KDC kann nur einem davon das Ticket zuordnen



Spannend daran: Der Fehler taucht oft erst auf, wenn ein Client das „falsche“ Ticket bekommt. Manche Nutzer sind betroffen, andere nicht – die Sorte Fehler, die Admins graue Haare und Tickets den Status „nicht reproduzierbar“ beschert.

Skizze 4: Der rote Fall ist ein echtes Duplikat, das `setspn -X` findet. Der gelbe Fall ist ein expliziter HTTP-SPN auf einem fremden Konto – kein Duplikat im Sinne von `setspn`, aber genauso tödlich.

Den gelben Fall aus der Skizze übersehen selbst erfahrene Admins. `setspn -X` sucht nach exakt gleichen SPNs. `HOST/sts.contoso.de` und `HTTP/sts.contoso.de` sind für das Werkzeug zwei verschiedene Einträge. Für den KDC ist ein explizites `HTTP/sts.contoso.de` aber der bessere Treffer als die `HOST`-Abbildung. Das Ticket wird mit dem Schlüssel des falschen Kontos verschlüsselt, ADFS kann es nicht öffnen. Deshalb gehört `setspn -Q HTTP/sts.contoso.de` fest in deine Prüfliste.

Befehl	Was er tut	Wann du ihn brauchst
setspn -Q HOST/sts.contoso.de	Sucht den SPN forestweit und zeigt das besitzende Konto	Immer zuerst – ein Treffer, richtiges Konto?
setspn -Q HTTP/sts.contoso.de	Sucht den expliziten HTTP-SPN	Erwartet: kein Treffer
setspn -L <Konto>	Listet alle SPNs eines Kontos	Prüfen, was am Dienstkonto hängt
setspn -X (-F)	Findet doppelte SPNs in Domäne oder Forest	Nach Kontowechsel, Migration, Aufräumaktionen
setspn -S <SPN> <Konto>	Legt SPN an, prüft vorher auf Duplikate	Fehlenden SPN setzen
setspn -D <SPN> <Konto>	Entfernt SPN von einem Konto	Altlasten beseitigen
klist purge / klist get	Leert den Ticket-Cache, fordert gezielt ein Ticket an	Nach jeder Änderung auf dem Testclient

Tabelle 2: Die SPN-Werkzeugkiste. `setspn` und `klist` sind Bordmittel von Windows, du brauchst kein zusätzliches Modul.

WARNUNG — Nicht im Blindflug löschen

Bevor du einen SPN mit `setspn -D` entfernst, prüfe, ob das Konto noch lebt und wofür. Ein „altes“ Dienstkonto betreibt manchmal noch einen Testknoten oder eine vergessene Anwendung. Dokumentiere Konto, SPN und Uhrzeit – wer um 16:55 Uhr am Freitag SPNs löscht, sollte zumindest wissen, welche.

Änderungen an SPNs replizieren wie jede andere AD-Änderung. Teste nicht sofort gegen einen DC am anderen Ende der Welt und wundere dich dann.

DNS: A-Record statt CNAME – und das richtige Ziel

DNS ist der zweite große Verdächtige. Microsoft schreibt es in der Troubleshooting-Dokumentation ohne Umschweife: Der Farmname soll ein A-Record sein, kein CNAME. Der Grund ist ein Verhalten der Browser unter Windows, das viele nicht kennen.

Warum der CNAME den SPN verbiegt

Edge und Chrome unter Windows bilden den SPN für Kerberos standardmäßig nicht aus dem Namen, den du in die Adresszeile tippst, sondern aus dem kanonischen Namen, den DNS zurückliefert. Zeigt sts.contoso.de per CNAME auf lb-vip01.contoso.local, fragt der Browser ein Ticket für HTTP/lb-vip01.contoso.local an. Diesen SPN hat dein ADFS-Dienstkonto nicht. Im besten Fall gibt es ihn gar nicht, im schlechtesten hängt er am Computerkonto irgendeines Servers, und der KDC stellt munter ein Ticket aus, das ADFS nicht öffnen kann.

Skizze 3: CNAME oder A-Record – ein DNS-Eintrag, zwei Welten

Browser unter Windows bilden den SPN aus dem kanonischen Namen, nicht aus der eingetippten Adresse

Falsch: CNAME

sts.contoso.de CNAME lb-vip01.contoso.local

Browser fragt Ticket an für
HTTP/lb-vip01.contoso.local

Diesen SPN hat das ADFS-Dienstkonto nicht. Entweder gibt es ihn gar nicht, oder er hängt am Computerkonto irgendeiner Maschine. Ergebnis: kein Kerberos, NTLM-Fallback oder Popup.

Richtig: A-Record

sts.contoso.de A 10.10.20.50

Browser fragt Ticket an für
HTTP/sts.contoso.de

Der KDC findet HOST/sts.contoso.de auf dem ADFS-Dienstkonto, stellt das Ticket aus, ADFS entschlüsselt es. Stille Anmeldung, zufriedene Belegschaft, ruhiger Helpdesk.

Die IP-Adresse gehört der internen VIP deines Load Balancers, nicht einem einzelnen ADFS-Knoten. Und intern darf sts.contoso.de niemals auf den Web Application Proxy zeigen – sonst landet jede Anfrage als Extranet-Anfrage bei ADFS und bekommt das Formular, egal wie schön dein SPN ist.

Skizze 3: Mit CNAME fragt der Browser nach dem SPN des Zielnamens, mit A-Record nach dem Farmnamen. Nur der zweite passt zum ADFS-Dienstkonto.

Edge und Chrome kennen dafür die Richtlinie `DisableAuthNegotiateCnameLookup`. Damit kannst du das Auflösen des CNAME abschalten. Das ist aber ein Pflaster, kein Heilmittel: Die Richtlinie wirkt nur auf verwalteten Browsern, und der nächste Client mit eigenem Kopf – ein Office-Anmeldedialog, eine Fachanwendung mit eingebettetem Browser – hat davon nie gehört. Der saubere Weg ist ein A-Record.

REM Zeigt, ob ein CNAME im Spiel ist und wohin der Name wirklich zeigt
`nslookup sts.contoso.de`

REM Ausführlicher, mit Typ-Angabe
`nslookup -type=CNAME sts.contoso.de`

```
nslookup -type=A sts.contoso.de
```

DNS-Check auf einem internen Client. Taucht „Aliases:“ in der Ausgabe auf, ist ein CNAME im Spiel.

Split-DNS: intern nie auf den Proxy

Die zweite DNS-Falle ist nicht der Typ des Eintrags, sondern sein Ziel. Intern muss sts.contoso.de auf die interne VIP des Load Balancers vor den ADFS-Knoten zeigen, extern auf den Web Application Proxy. Fehlt die interne Zone oder hat jemand sie „vereinfacht“, gehen interne Clients über den WAP. ADFS sieht dann eine Proxy-Anfrage, behandelt sie als Extranet – und liefert das Formular. Das ist Weiche Nummer eins aus Skizze 1, und sie ist gnadenlos: Kein SPN, keine Zone, kein User-Agent ändert daran etwas. Die Rolle des Proxys in der Gesamtarchitektur beschreibt [Web Application Proxy: Architektur und Ablöse](#).

DNS-Situation intern	Ergebnis beim Nutzer	Richtig so?
sts.contoso.de A auf interne VIP vor den ADFS-Knoten	WIA möglich, stille Anmeldung	Ja
sts.contoso.de CNAME auf lb-vip01.contoso.local	Kerberos mit falschem SPN, NTLM-Fallback oder Popup	Nein
sts.contoso.de A auf externe Adresse des WAP	Extranet-Behandlung, Formular für alle	Nein
sts.contoso.de A auf einzelner ADFS-Knoten	Funktioniert, bis der Knoten gewartet wird	Nur im Labor
Kein interner Eintrag, Auflösung über öffentliches DNS	Wie „externe Adresse des WAP“	Nein

Tabelle 3: Interne DNS-Varianten und ihre Folgen. Nur die erste Zeile ist produktionsstauglich.

WICHTIG — Load Balancer und Kanalbindung

Terminiert der interne Load Balancer TLS und baut danach eine neue TLS-Verbindung zu ADFS auf (SSL-Bridging), passt die Kanalbindung nicht mehr. ADFS erkennt, dass etwas zwischen Browser und Dienst sitzt, und lehnt die Windows-Anmeldung ab. Ergebnis laut Microsoft: Popup statt SSO. Dasselbe passiert mit Fiddler oder einem TLS-inspizierenden Proxy.

Der Standardwert von ExtendedProtectionTokenCheck ist Allow. Ihn auf None zu setzen, ist ein Sicherheitsabbau, keine Lösung. Besser: den Load Balancer für ADFS auf TLS-Durchleitung (Layer 4) umstellen. Wie das sauber geht, steht in [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#) und auf unserer Seite zum [Kemp LoadMaster](#).

Browser: Intranetzone und WIA-unterstützte User-Agents

Selbst wenn ADFS Negotiate anbietet und SPN wie DNS stimmen, entscheidet am Ende der Browser, ob er ungefragt ein Ticket schickt. Und er schickt es nur an Adressen, denen er vertraut. Unter Windows heißt das: die Zone „Lokales Intranet“.

Warum sts.contoso.de nicht automatisch im Intranet liegt

Windows ordnet Namen mit Punkten – also jeden vollqualifizierten Namen – standardmäßig der Internetzone zu. Dass sts.contoso.de intern auflöst, interessiert die Zonenlogik nicht. In der Internetzone meldet sich der Browser nicht automatisch an. Die Lösung ist eine Gruppenrichtlinie: Unter „Liste der Site-zu-Zonenzuweisungen“ trägst du den Farmnamen sts.contoso.de samt HTTPS-Schema mit dem Wert 1 für die Intranetzone ein. Dazu gehört die Einstellung „Automatische Anmeldung nur in der Intranetzone“, die in dieser Zone Standard ist.

Edge und Chrome übernehmen die Zonenzuordnung von Windows. Alternativ – oder zusätzlich – kennen beide die Richtlinie AuthServerAllowlist, in der du erlaubte Server für integrierte

Anmeldung hinterlegt. Firefox macht sein eigenes Ding: Dort gehört der Name in network.negotiate-auth.trusted-uris, am besten zentral über die Firefox-Richtlinien verteilt.

Browser	Wo die Freigabe herkommt	Steht in WIASupportedUserAgents?
Microsoft Edge	Zone „Lokales Intranet“ oder Richtlinie AuthServerAllowlist	Ja, ab ADFS 2016 per Muster =~Windows\s*NT.*Edg.*
Google Chrome	Zone „Lokales Intranet“ oder Richtlinie AuthServerAllowlist	Nein, musst du ergänzen
Mozilla Firefox	network.negotiate-auth.trusted-uris, per Richtlinie verteilt	Nein, musst du ergänzen
Internet Explorer	Zone „Lokales Intranet“	Ja – aber du willst ihn nicht mehr benutzen
Office-Apps, eingebettete Anmeldedialoge	Folgen meist der Windows-Zonenlogik	Je nach User-Agent – im Debug-Log prüfen

Tabelle 4: Zwei Freigaben müssen stimmen – die im Browser und die in ADFS. Fehlt eine, gibt es Popup oder Formular.

WIASupportedUserAgents erweitern

Die Liste WIASupportedUserAgents ist ein Relikt aus einer Zeit, in der „Browser“ und „Internet Explorer“ Synonyme waren. Die Liste enthält Zeichenfolgen für IE-Versionen, die niemand mehr einsetzt, und seit ADFS 2016 ein reguläres Ausdrucksmuster für Edge. Einträge mit dem Präfix =~wertet ADFS als regulären Ausdruck aus, alle anderen als Teilzeichenfolge. Chrome fehlt in der Standardliste. Wer den Browser-Rollout umstellt, ohne diese Liste anzufassen, erzeugt genau das Ticket vom Montagmorgen.

```
# Aktuelle Liste sichern, bevor du sie anfasst
Get-AdfsProperties | Select-Object -ExpandProperty WIASupportedUserAgents |
    Out-File C:\Temp\wia-useragents-vorher.txt -Encoding utf8

# Chrome unter Windows ergänzen (Muster aus der Microsoft-Dokumentation)
$wia = Get-AdfsProperties | Select-Object -ExpandProperty WIASupportedUserAgents
if ($wia -notcontains '=~Windows\s*NT.*Chrome') {
    $wia = $wia + '=~Windows\s*NT.*Chrome'
}
Set-AdfsProperties -WIASupportedUserAgents $wia

# Kontrolle
Get-AdfsProperties | Select-Object -ExpandProperty WIASupportedUserAgents
```

Ergänzen statt Überschreiben. Set-AdfsProperties ersetzt die komplette Liste – wer nur den neuen Eintrag übergibt, hat danach genau einen unterstützten Browser.

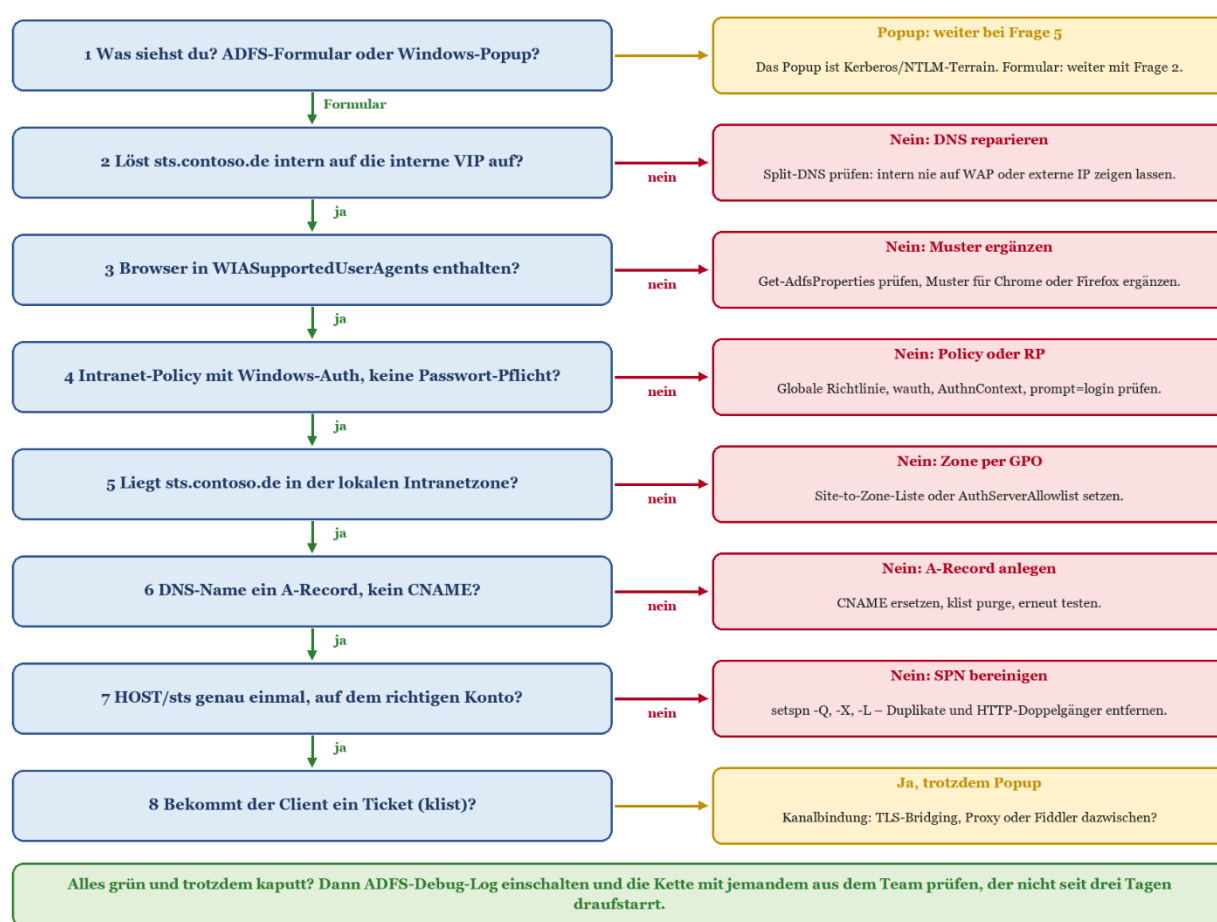
Die Einstellung gilt farmweit, ein Neustart des Dienstes ist nach unserer Erfahrung nicht nötig, schadet aber auch nicht, wenn du sie im Wartungsfenster setzt. Die komplette, von Microsoft empfohlene Liste für ADFS ab Windows Server 2016 findest du in der Dokumentation [Microsoft Learn: Browser für die integrierte Windows-Authentifizierung mit AD FS konfigurieren](#).

WARNUNG — Muster nicht zu großzügig wählen

Ein Eintrag wie „Mozilla/5.0“ passt auf praktisch jeden Browser der Welt, auch auf Smartphones und Mac-Rechner ohne Domänenkonto. ADFS bietet diesen Geräten dann WIA an, die können nichts damit anfangen, und das Ergebnis ist ein Popup statt eines Formulars. Deshalb stehen in den Mustern „Windows NT“ und der Browsername – so trifft es nur Windows-Desktops. Für Geräte, die intern WIA nicht können, ist das Formular die richtige Antwort. Das ist kein Fehler, das ist Absicht.

Skizze 5: Diagnose-Entscheidungsbaum „intern kommt die Anmeldemaske“

Von oben nach unten abarbeiten – jede Frage in unter fünf Minuten beantwortet



Skizze 5: Der Diagnose-Entscheidungsbaum. Arbeite ihn von oben nach unten ab – die ersten vier Fragen betreffen ADFS und DNS, erst danach geht es an Zone, SPN und Ticket.

Der Diagnoseablauf in der Praxis

Mit dem Entscheidungsbaum aus Skizze 5 kommst du in den meisten Fällen in unter einer Stunde zur Ursache. Nimm dir dafür einen Testclient, auf dem das Problem auftritt, und ein Konto mit Leserechten im AD. Die ADFS-Cmdlets laufen auf einem Farmknoten. Wenn alles grün ist und es trotzdem hakt, schalte das Debug-Tracing ein und schau dir an, welche Authentifizierungsmethode ADFS gewählt hat. Wie das geht und welche Einträge relevant sind, beschreibt [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#).

Schritt	Prüfung	Werkzeug	Soll-Ergebnis
1	Formular oder Popup?	Screenshot vom Nutzer	Legt fest, ob du bei ADFS oder bei Kerberos suchst
2	Interne Namensauflösung	nslookup sts.contoso.de	Interne VIP, kein Alias
3	User-Agent freigeschaltet	Get-AdfsProperties	Muster passt auf den Browser
4	Intranet-Policy	Get-AdfsGlobalAuthenticationPolicy	Windows-Authentifizierung im Intranet aktiv
5	Intranetzone	Internetoptionen, gpresult /r	sts.contoso.de in „Lokales Intranet“
6	A-Record	nslookup -type=CNAME	Kein CNAME
7	SPN eindeutig	setspn -Q, setspn -X	HOST/sts genau einmal, auf dem

			Dienstkonto; kein HTTP/sts
8	Ticket vorhanden	klist purge, klist get HTTP/sts.contoso.de	Ticket wird ausgestellt

Tabelle 5: Die Prüfschritte aus dem Entscheidungsbaum mit Werkzeug und Soll-Ergebnis – zum Ausdrucken neben die Tastatur.

TIPP — Ein Praxisfall zum Mitschmunzeln

In einer mittelgroßen Verwaltung meldeten plötzlich nur die Kolleginnen und Kollegen eines Außenstandorts das Formular. Zentrale: alles gut. Nach zwei Tagen SPN-Archäologie fiel auf, dass der Standort einen eigenen DNS-Server mit Weiterleitung ins Internet hatte – ohne interne Zone für contoso.de. sts.contoso.de löste dort auf den WAP auf. Die Reparatur dauerte fünf Minuten, die Suche zwei Tage. Frage 2 im Entscheidungsbaum steht nicht zufällig so weit oben.

Wenn du solche Diagnosen nicht nur nachlesen, sondern selbst üben willst: In unseren [ADFS-Schulungen](#) bauen wir genau diese Fehler absichtlich in eine Laborfarm ein. Und wer die Zusammenhänge von Kerberos, Claims und Proxy lieber in Ruhe nachschlagen möchte, findet sie ausführlich im Buch [ADFS in der Praxis – das Buch im Detail](#).

Fazit: Erst lesen, wer entschieden hat – dann reparieren

„Intern kommt trotzdem die Anmeldemaske“ ist kein Rätsel, sondern eine Kette von Prüfungen, die du der Reihe nach abarbeitest. Das ADFS-Formular ist eine Entscheidung von ADFS: falsches DNS-Ziel, fehlender User-Agent, strenge Richtlinie oder eine Anwendung, die ausdrücklich ein Kennwort verlangt. Das Windows-Popup ist der Browser, der mit Kerberos und NTLM nicht weiterkommt: Zone, CNAME, doppelter oder falscher SPN, gebrochene Kanalbindung.

Die Grundausrüstung ist überschaubar: ein A-Record, der intern auf die VIP zeigt; ein einziger SPN HOST/sts.contoso.de auf dem Dienstkonto; kein HTTP-Doppelgänger; sts.contoso.de in der Intranetzone; die eingesetzten Browser in WIASupportedUserAgents. Wer das einmal sauber dokumentiert und nach jedem Kontowechsel oder Browser-Rollout kurz prüft, hat Ruhe. ADFS ist an dieser Stelle nicht zickig, es ist nur ehrlich: Es zeigt dir, dass irgendwo im Unterbau etwas nicht stimmt.

Und mit Blick nach vorn: Die meisten Unternehmen werden ADFS irgendwann ablösen. Bis dahin lohnt es sich, die Farm sauber zu betreiben – auch weil eine Kerberos-Umgebung ohne SPN-Leichen dir später bei der Umstellung auf Microsoft Entra ID hilft. Wie der Weg für Microsoft 365 aussieht, beschreibt [Microsoft 365 von Federated auf Managed umstellen – mit Staged Rollout](#). Wenn du bei SPN-Wildwuchs, DNS-Altlasten oder dem Ausstiegsplan eine zweite Meinung brauchst, sprich uns über [Consulting zu ADFS \(Active Directory Federation Services\)](#) an.

WEITER — Passend zum Thema

- › [Microsoft Kerberos](#) – das Kerberos-Fundament: Tickets, SPNs, Delegierung
- › [ADFS-Anmeldung schlägt fehl – die häufigsten Ursachen und ihre Lösung](#) – wenn die Anmeldung nicht nur lästig ist, sondern scheitert
- › [gMSA als ADFS-Dienstkonto einrichten und umstellen](#) – Dienstkontowechsel ohne verwaiste SPNs
- › [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#) – TLS-Durchleitung statt Bridging
- › [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#) – warum du ExtendedProtectionTokenCheck nicht einfach abschaltest

FAQ: SPN, DNS und Kerberos für ADFS

Welchen SPN braucht ADFS für die integrierte Windows-Authentifizierung?

HOST/sts.contoso.de – also HOST plus den vollqualifizierten Farmnamen – auf dem Konto, unter dem der ADFS-Dienst läuft. Ein expliziter HTTP-SPN ist nicht nötig, weil der KDC HTTP standardmäßig auf HOST abbildet. Der SPN hängt am Dienstkonto, nicht an den Computerkonten der einzelnen Knoten.

Wie finde ich doppelte SPNs?

Mit setspn -X für die Domäne oder setspn -X -F für den ganzen Forest. Prüfe zusätzlich mit setspn -Q HTTP/sts.contoso.de, ob irgendwo ein expliziter HTTP-SPN für den Farmnamen existiert. Den erkennt setspn -X nicht als Duplikat, er stört Kerberos aber genauso.

Warum darf der ADFS-Name kein CNAME sein?

Weil Browser unter Windows den Kerberos-SPN aus dem kanonischen Namen bilden, auf den der CNAME zeigt. Der Browser fragt dann ein Ticket für den Zielnamen an, und der passt nicht zum ADFS-Dienstkonto. Microsoft empfiehlt deshalb ausdrücklich einen A-Record für den Farmnamen.

Warum bekomme ich in Chrome das Formular, in Edge aber nicht?

Weil ADFS ab Windows Server 2016 in der Standardliste WIASupportedUserAgents ein Muster für Edge enthält, aber keines für Chrome. Ergänze ein passendes Muster wie =~Windows\s*NT.*Chrome mit Set-AdfsProperties und prüfe, dass sts.contoso.de in der Intranetzone liegt.

Was ist der Unterschied zwischen ADFS-Formular und Windows-Popup?

Das Formular zeigt ADFS, wenn es sich gegen die Windows-Anmeldung entscheidet – etwa wegen des User-Agents, einer Proxy-Anfrage oder einer Anforderung der Anwendung. Das Popup zeigt der Browser, wenn ADFS Negotiate angeboten hat, Kerberos und NTLM aber scheitern. Das eine suchst du in ADFS und DNS, das andere bei Zone, SPN und Kanalbindung.

Muss ich ExtendedProtectionTokenCheck auf None setzen?

In aller Regel nicht. Der Standardwert Allow schützt vor Man-in-the-Middle-Szenarien. Wenn ein Load Balancer mit SSL-Bridging oder ein TLS-inspizierender Proxy die Kanalbindung bricht, stell lieber die Infrastruktur um – zum Beispiel auf TLS-Durchleitung – statt den Schutz abzuschalten.

Warum funktioniert es intern, obwohl der SPN fehlt?

Weil Negotiate bei fehlendem oder falschem SPN meist auf NTLM zurückfällt. Die Anmeldung bleibt dann still, nur eben ohne Kerberos. Das fällt erst auf, wenn NTLM eingeschränkt wird. Mit klist get HTTP/sts.contoso.de auf einem Client siehst du sofort, ob ein Kerberos-Ticket entsteht.

Muss ich den SPN nach der Umstellung auf ein gMSA neu setzen?

Ja, der SPN muss auf das neue Dienstkonto, und vom alten Konto musst du ihn entfernen. Sonst hast du genau das Duplikat, das Kerberos lahmlegt. Prüfe nach der Umstellung mit `setspn -Q HOST/sts.contoso.de`, dass nur noch das gMSA als Besitzer auftaucht.

Kann ich Kerberos auch über den Web Application Proxy nutzen?

Nicht für die Anmeldung an ADFS selbst. Anfragen über den WAP behandelt ADFS als Extranet-Anfragen, dort greift die Extranet-Authentifizierung, standardmäßig das Formular. Interne Clients sollen deshalb per Split-DNS direkt auf die interne VIP der ADFS-Farm gehen.