

ADFS-Anmeldung schlägt fehl – die häufigsten Ursachen und ihre Lösung

ADFS · Troubleshooting

Anmeldung fehlgeschlagen? Erst sortieren, dann reparieren

Zeit, Zertifikate, Identifizier, Konten, SPN, WAP-Trust, Proxy und Cookies – die acht üblichen Verdächtigen.

boddenberg.de



WISSEN

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

› [Active Directory Federation Services](#)

BERATUNG

Die Anmeldung hakt, und die Zeit drängt? Wir suchen mit dir – und räumen die Ursache dauerhaft ab.

› [Consulting zu ADFS](#)

SCHULUNG

Im Labor kaputt machen, was in der Produktion nie kaputtgehen soll: Fehlerbilder gezielt erzeugen und lösen.

› [ADFS-Schulungen](#)

Es ist Montag, 7:58 Uhr. Das Telefon klingelt, bevor der Kaffee durchgelaufen ist. Am anderen Ende: die Buchhaltung, der Vertrieb und – Klassiker – die Geschäftsführung, die aus dem Hotel in Mailand nicht in Outlook kommt. Auf dem Bildschirm steht eine ADFS-Fehlerseite mit einer Aktivitäts-ID, die niemand abgeschrieben hat, oder eine Anwendung, die freundlich mitteilt, das Token sei ungültig. Wenn du jetzt „adfs anmeldung fehlgeschlagen“ in die Suchmaschine tippst, bist du in bester Gesellschaft. Und du bist hier richtig.

Die gute Nachricht vorweg: ADFS ist kein launisches Wesen. Eine Farm, die zehn Jahre stabil gelaufen ist, hört nicht einfach auf zu funktionieren, weil Montag ist. Wenn die Anmeldung scheitert, steckt fast immer eine von acht Ursachen dahinter, die sich mit erstaunlicher Treue wiederholen: eine Uhr, die falsch geht, ein Zertifikat, das abgelaufen ist, ein Identifizier, der nicht passt, ein gesperrtes Konto, ein fehlender oder doppelter SPN, ein abgelaufener WAP-Trust, ein Proxy, der sich in die Verbindung drängelt, und Browser-Cookies, die mehr wissen wollen als gut ist. Dieser Leitfaden geht vom Symptom aus, nicht von der Theorie. Die Grundlagen zu Farm, Relying Parties und Web Application Proxy findest du auf der Übersichtsseite [Active Directory Federation Services](#).

FAKTEN – ADFS-Anmeldung fehlgeschlagen – das Wichtigste auf einen Blick

Fehler, die ADFS selbst erkennt, landen im Ereignisprotokoll „AD FS/Admin“ auf dem Server, der die Anfrage bearbeitet hat – meist als Ereignis 364 mit der Aktivitäts-ID von der Fehlerseite.

Kerberos toleriert standardmäßig fünf Minuten Zeitabweichung. Viele Anwendungen tolerieren beim SAML-Token deutlich weniger.

Drei Zertifikatsarten sind kritisch: SSL (Service-Communications), Token-Signing und das Proxy-Trust-Zertifikat des WAP.

MSIS7007 heißt: ADFS kennt den angefragten Relying Party Trust nicht. Fast immer ist der Identifizier falsch geschrieben.

MSIS7042 ist die Schleifenerkennung: Laut Microsoft greift sie, wenn dieselbe Browsersitzung

innerhalb von 20 Sekunden fünfmal ein Token anfordert.

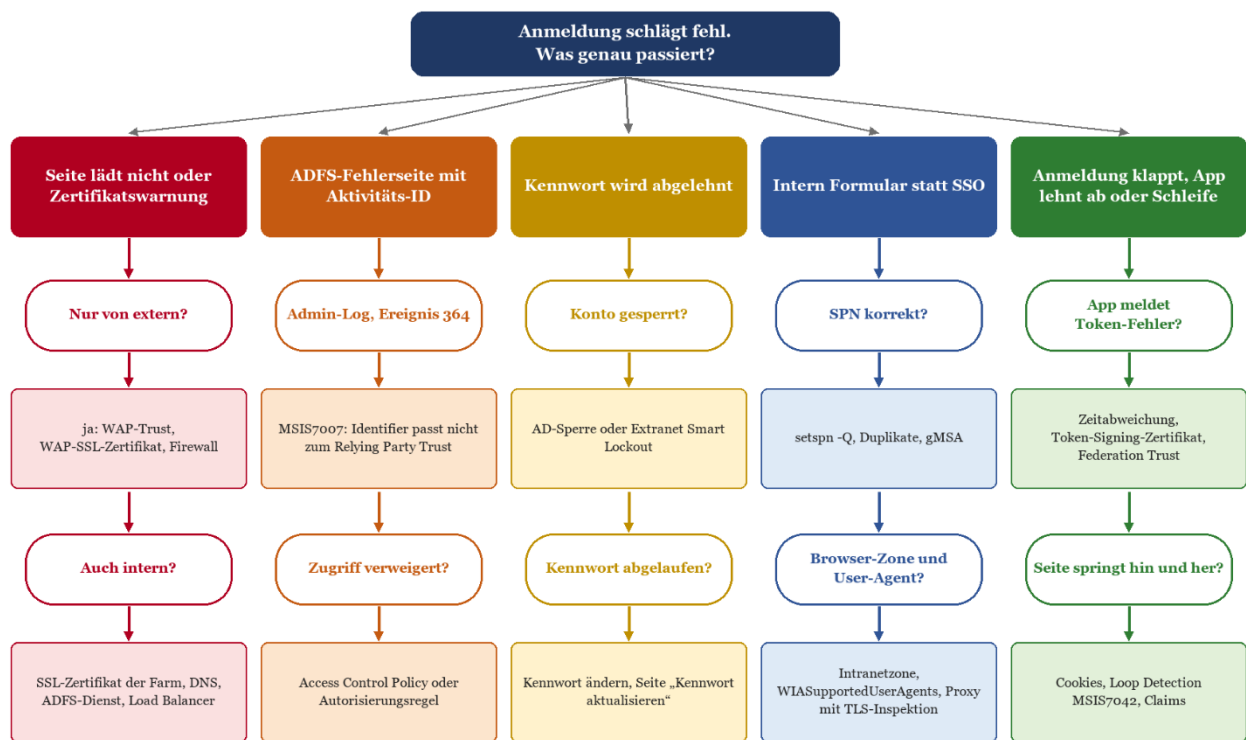
Bricht nur die Anmeldung von extern, liegt die Ursache meist am Web Application Proxy. Bricht nur die interne Anmeldung, sind SPN, DNS und Browser verdächtig.

Erst sortieren, dann reparieren: der Entscheidungsbaum

Der größte Fehler bei der Fehlersuche ist nicht die falsche Lösung, sondern die richtige Lösung für das falsche Problem. Wer bei einer Zertifikatswarnung die Claim Rules umschreibt oder bei einer Kontosperrung das SSL-Zertifikat tauscht, beschäftigt sich und das Change-Board, aber nicht die Ursache. Deshalb steht am Anfang eine einfache Frage: Was genau sieht die Anwenderin oder der Anwender? Eine leere Seite? Eine ADFS-Fehlerseite? Eine Fehlermeldung der Anwendung? Oder eine Seite, die im Sekundentakt neu lädt, als hätte sie Schluckauf?

Skizze 1: Entscheidungsbaum – was siehst du, wenn die Anmeldung scheitert?

Vom Symptom zur wahrscheinlichsten Ursache in drei Ebenen



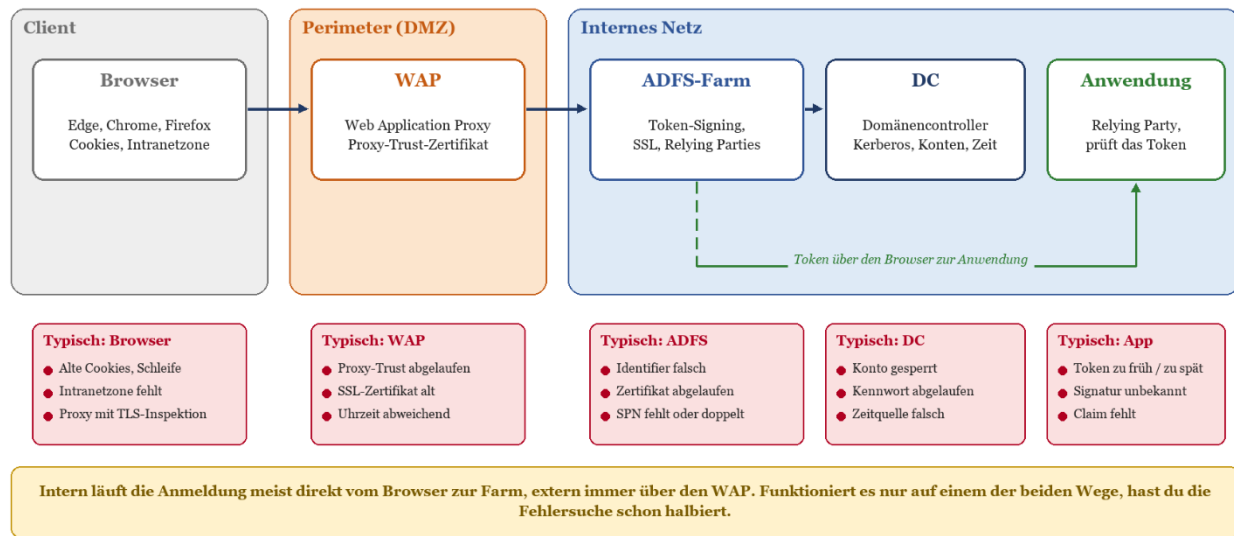
Faustregel: Kommt die Fehlerseite von ADFS, steht die Ursache fast immer im ADFS-Admin-Log. Kommt sie von der Anwendung, hat ADFS seinen Job erledigt – und das Problem liegt bei Zeit, Zertifikat oder Claims.

Skizze 1: Entscheidungsbaum vom Symptom zur wahrscheinlichsten Ursache

Die fünf Äste des Baums decken erfahrungsgemäß den allergrößten Teil der Störungen ab. Der Trick besteht darin, dass jede Station auf dem Weg einer Anmeldung ihre eigenen Fehlerbilder hat. Der Browser scheitert anders als der Web Application Proxy, der WAP anders als die Farm, die Farm anders als der Domänencontroller und der Domänencontroller anders als die Anwendung, die am Ende das Token prüft.

Skizze 2: Der Weg einer Anmeldung – und wo er reißt

Jede Station hat ihre typischen Bruchstellen – und jede scheitert auf ihre eigene Art



Skizze 2: Die Stationen einer Anmeldung und ihre typischen Bruchstellen

Die Aktivitäts-ID ist dein bester Freund

Zeigt ADFS eine eigene Fehlerseite, steht dort eine Aktivitäts-ID, meist dazu der Zeitpunkt und der Name der Relying Party. Diese ID ist Gold wert. Bitte deine Kolleginnen und Kollegen, einen Screenshot zu schicken statt „geht nicht“ ins Ticket zu schreiben. Mit der ID suchst du im Ereignisprotokoll „AD FS/Admin“ den passenden Eintrag – in einer Farm allerdings auf dem Server, der die Anfrage tatsächlich bearbeitet hat. Hinter einem Load Balancer heißt das: auf allen Knoten suchen. Wie du Admin-Log, Debug-Tracing und Sicherheitsauditing gezielt einsetzt, steht im Beitrag [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#).

```
# Aktivitäts-ID von der Fehlerseite auf allen Farmknoten suchen
$id = "00000000-0000-0000-a1b2-0080000000c3"
$nodes = "adfs01.contoso.local", "adfs02.contoso.local"
foreach ($n in $nodes) {
    Get-WinEvent -ComputerName $n -LogName "AD FS/Admin" -MaxEvents 2000 |
        Where-Object { $_.Message -like "*$id*" } |
        Select-Object @{n="Server";e={$n}}, TimeCreated, Id, Message
}
```

Listing 1: Ereignisse zur Aktivitäts-ID auf allen Knoten der Farm finden

TIPP – Fehlerseite gesprächiger machen

Auf der Fehlerseite kannst du mit `Set-AdfsGlobalWebContent -ErrorPageSupportEmail` eine Support-Adresse hinterlegen und mit `-ErrorPageDescriptionText` erklären, dass die Aktivitäts-ID bitte mitgeschickt werden soll. Wie das sauber aussieht, zeigt der Beitrag [ADFS-Anmeldeseite anpassen – Logo, Texte, Hilfelinks](#).

Intern, extern oder beides?

Die zweite Frage halbiert die Fehlersuche: Scheitert die Anmeldung nur von außen, nur im Firmennetz oder überall? Von außen läuft jede Anmeldung über den Web Application Proxy, im internen Netz löst der DNS-Name `sts.contoso.de` in aller Regel direkt auf die Farm oder deren Load Balancer auf. Klappt es intern und extern nicht, liegt die Ursache in der Farm, im Active Directory oder bei der Anwendung. Klappt es nur extern nicht, schau zuerst auf den WAP. Klappt es nur

intern nicht – oder fällt intern die Anmeldung auf das Formular zurück –, sind SPN, DNS und Browser-Einstellungen die üblichen Verdächtigen.

Die Testseite als neutraler Schiedsrichter

Um ADFS unabhängig von einer Anwendung zu testen, eignet sich die IdP-initiierte Anmeldeseite unter <https://sts.contoso.de/adfs/ls/idpinitiatedsignon.aspx>. Seit ADFS unter Windows Server 2016 ist sie standardmäßig abgeschaltet. Funktioniert die Anmeldung dort, ist ADFS grundsätzlich gesund, und der Fehler liegt bei der Relying Party oder ihrer Konfiguration. Funktioniert sie dort nicht, brauchst du dich mit der Anwendung gar nicht erst zu beschäftigen.

```
# Testseite für die Dauer der Fehlersuche einschalten ...
Set-AdfsProperties -EnableIdpInitiatedSignonPage $true

# ... und danach wieder ausschalten
Set-AdfsProperties -EnableIdpInitiatedSignonPage $false
```

Listing 2: IdP-initiierte Anmeldeseite vorübergehend aktivieren

WARNUNG – Nicht dauerhaft offen lassen

Die Testseite verrät jedem, der sie aufruft, die Namen deiner Relying Parties. Für Angreifer ist das eine nette Speisekarte. Einschalten, testen, ausschalten – und den Schritt ins Change-Protokoll schreiben, damit nicht in zwei Jahren jemand rätselt, warum sie offen ist. Mehr zur Härtung im Beitrag [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#).

Die große Diagnose-Tabelle: Symptom, Ursache, Prüfung, Lösung

Bevor wir in die einzelnen Ursachen eintauchen, hier die Tabelle zum Ausdrucken und an die Monitorkante Kleben. Sie ist nach Symptom sortiert, nicht nach Technik – denn das Symptom ist das, was du um 7:58 Uhr kennst. Die Prüfbefehle stammen aus dem ADFS-Modul, dem Modul des Web Application Proxy, den Bordmitteln von Windows und Microsoft Graph PowerShell.

Symptom	Wahrscheinliche Ursache	Prüfung	Lösung
Browser zeigt Zertifikatswarnung für sts.contoso.de	SSL-Zertifikat abgelaufen oder Zwischenzertifikat fehlt	netsh http show sslcert, Get-AdfsSslCertificate	Zertifikat tauschen, siehe SSL-Zertifikat auf ADFS und Web Application Proxy tauschen
Extern Fehlerseite des WAP, intern alles gut	Proxy-Trust zwischen WAP und Farm abgelaufen	Ereignisse im Protokoll des WAP, Uhrzeit, Erreichbarkeit der Farm	Install-WebApplicationProxy erneut ausführen, siehe WAP-Proxy-Vertrauen erneuern – wenn der Web Application Proxy plötzlich nicht mehr will
Anwendung meldet „Token noch nicht gültig“ oder „abgelaufen“	Zeitabweichung zwischen ADFS und Anwendung	w32tm /query /status auf beiden Seiten	Zeitquelle korrigieren, notfalls NotBeforeSkew am Trust
ADFS meldet Erfolg, Anwendung lehnt	Token-Signing-Zertifikat gewechselt, Anwendung kennt es nicht	Get-AdfsCertificate -CertificateType Token-Signing	Neues Zertifikat bei der Anwendung hinterlegen, siehe

Signatur ab			ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover
Microsoft 365: Föderationsfehler nach Zertifikatswechsel	Signaturzertifikat in Entra ID veraltet	Get-MgDomainFederationConfiguration	Federation Trust aktualisieren, siehe Microsoft-365-Federation-Trust nach Zertifikatswechsel aktualisieren
Microsoft 365: AADSTS50107, Realm-Objekt existiert nicht	Issuer-URI im Token passt nicht zur Domänenkonfiguration	Get-MgDomainFederationConfiguration, Claim-Regel für den Issuer	Issuer-URI angleichen, Claim-Regel prüfen
ADFS-Fehlerseite, im Admin-Log MSIS7007	Identifizier der Anfrage passt zu keinem Relying Party Trust	Get-AdfsRelyingPartyTrust - Identifizier ...	Identifizier exakt angleichen, siehe Relying Party Trust anlegen – per Metadaten und von Hand
ADFS-Fehlerseite „Zugriff verweigert“	Access Control Policy oder Autorisierungsregel greift	Get-AdfsRelyingPartyTrust Select AccessControlPolicyName	Richtlinie anpassen, siehe Access Control Policies in ADFS – Zugriffsregeln ohne Claim-Rule-Akrobatik
Kennwort richtig, Anmeldung trotzdem abgelehnt	Konto im AD gesperrt oder Extranet Smart Lockout aktiv	Get-ADUser -Properties LockedOut, Get-AdfsAccountActivity	Unlock-ADAccount bzw. Reset-AdfsAccountLockout, siehe Extranet Smart Lockout – ADFS gegen Passwort-Spray schützen
Meldung „Kennwort abgelaufen“	Kennwort im AD abgelaufen, keine Änderungsseite aktiv	Get-ADUser -Properties PasswordExpired	Kennwort ändern lassen, Endpunkt zum Aktualisieren prüfen
Intern Formular statt Single Sign-on	SPN fehlt, ist doppelt oder steht am falschen Konto	setspn -Q HTTP/sts.contoso.de, setspn -X	SPN aufs Dienstkonto setzen, siehe SPN, DNS und Kerberos für ADFS – warum die interne Anmeldung auf Formular zurückfällt
Intern Formular nur mit bestimmtem Browser	Intranetzone fehlt oder User-Agent nicht in WIASupportedUserAgents	Get-AdfsProperties Select -Expand WIASupportedUserAgents	Zone per Gruppenrichtlinie, User-Agent ergänzen
Interne Anmeldung scheitert hinter Proxy mit TLS-Inspektion	Proxy bricht TLS auf, Extended Protection schlägt an	Proxy-Ausnahmen, ExtendedProtectionTokenCheck	sts.contoso.de von der Inspektion ausnehmen
Seite lädt endlos neu, im Log MSIS7042	Schleife: Anwendung nimmt das Token nicht an	Admin-Log, Fiddler- oder Browser-Mitschnitt	Ursache bei der Anwendung beheben, Cookies löschen
Nur ein Nutzer betroffen, im	Alte oder kaputte ADFS-Cookies im Browser	Test im InPrivate-Fenster	Cookies für sts.contoso.de löschen

privaten Fenster geht es

Tabelle 1: Die große Diagnose-Tabelle für fehlgeschlagene ADFS-Anmeldungen

WICHTIG – Eine Änderung nach der anderen

Die Versuchung ist groß, bei Druck aus der Chefetage drei Dinge gleichzeitig zu ändern. Lass es. Wenn es danach geht, weißt du nicht warum – und wenn es nicht geht, weißt du nicht, was du kaputtgemacht hast. Ändern, testen, notieren, nächster Schritt. Und vor größeren Eingriffen ein aktuelles Backup der Konfiguration, wie im Beitrag [ADFS sichern und wiederherstellen – Rapid Restore Tool in der Praxis](#) beschrieben.

Zeit und Zertifikate: die Klassiker mit Ansage

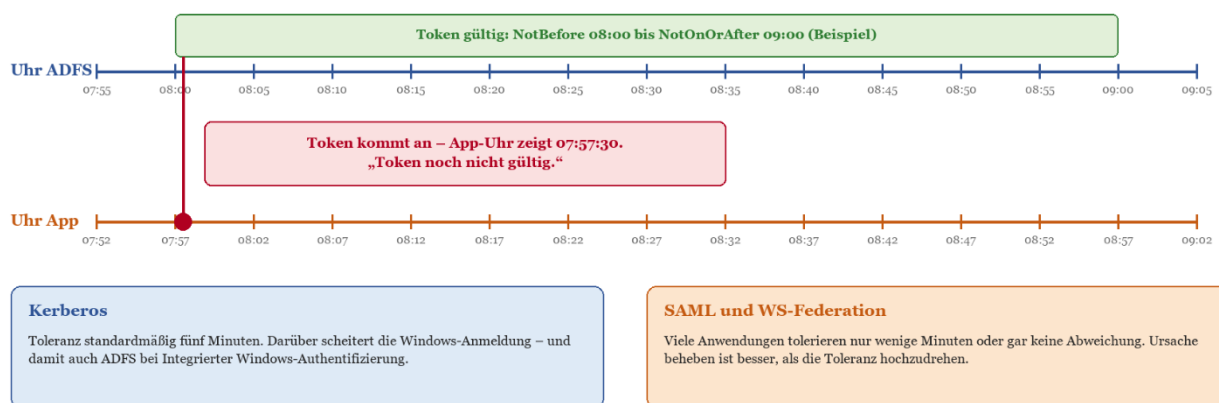
Zeit und Zertifikate haben eines gemeinsam: Sie gehen nicht plötzlich kaputt, sie laufen ab oder laufen weg. Beides kündigt sich an, wenn man hinschaut. Leider schaut selten jemand hin, weil die Farm ja seit Jahren läuft. Das ist der Teil der ADFS-Störungen, bei dem schwarzer Humor besonders gut hilft – denn im Nachhinein stand das Ablaufdatum immer irgendwo.

Zeitabweichung: drei Minuten, die alles kaputtmachen

Jedes Token, das ADFS ausstellt, trägt einen Gültigkeitszeitraum: nicht vor, nicht nach. Die Anwendung prüft diesen Zeitraum mit ihrer eigenen Uhr. Geht die Uhr der Anwendung drei Minuten nach, kommt ein frisch ausgestelltes Token für sie aus der Zukunft – und wird abgelehnt. Geht sie vor, ist das Token unter Umständen schon abgelaufen, bevor es geprüft wird. Bei der Integrierten Windows-Authentifizierung kommt Kerberos dazu: Weichen die Uhren von Client, ADFS-Server und Domänencontroller mehr als die standardmäßig erlaubten fünf Minuten ab, scheitert schon das Kerberos-Ticket. Und Microsoft nennt die Zeitabweichung ausdrücklich auch als Ursache für einen kaputten Proxy-Trust zwischen WAP und Farm.

Skizze 3: Drei Minuten zu früh – wie eine Zeitabweichung ein gültiges Token kilt

ADFS stempelt das Token mit seiner Uhr, die Anwendung prüft mit ihrer eigenen



Skizze 3: Ein gültiges Token, zwei Uhren, eine Ablehnung

```
# Zeitquelle und Abweichung auf ADFS-Server, WAP und Anwendungsserver prüfen
w32tm /query /status
w32tm /query /source
w32tm /stripchart /computer:dc01.contoso.local /samples:5 /dataonly

# Domänenmitglieder synchronisieren über die Domänenhierarchie
w32tm /config /syncfromflags:domhier /update
```

w32tm /resync

Listing 3: Zeit prüfen und neu synchronisieren

Der WAP steht in vielen Umgebungen nicht in der Domäne. Er bekommt seine Zeit dann nicht automatisch vom Domänencontroller, sondern von einer Quelle, die irgendjemand vor Jahren eingetragen hat – oder von gar keiner. Prüfe gezielt, woher der WAP seine Zeit bezieht, und gib ihm eine zuverlässige Quelle, die auch die Farm nutzt. Bei virtuellen Maschinen kommt die Zeitsynchronisierung über den Hypervisor dazu, die sich gern mit der Domänenhierarchie streitet.

WARNUNG – NotBeforeSkew ist ein Pflaster, keine Therapie

Mit Set-AdfsRelyingPartyTrust -TargetName "Contoso Portal" -NotBeforeSkew 2 setzt ADFS den Beginn der Gültigkeit um zwei Minuten zurück. Das hilft gegen eine Anwendung, deren Uhr leicht nachgeht und die du nicht selbst betreibst. Es ändert aber nichts daran, dass irgendwo eine Uhr falsch geht. Erst die Zeitquelle reparieren, dann über Toleranzen nachdenken.

Abgelaufene Zertifikate: welches denn?

„Das Zertifikat ist abgelaufen“ ist ein Satz, der in ADFS-Umgebungen drei völlig verschiedene Dinge bedeuten kann. Das SSL-Zertifikat schützt die HTTPS-Verbindung. Das Token-Signing-Zertifikat signiert die Tokens. Und das Proxy-Trust-Zertifikat weist den WAP gegenüber der Farm aus. Jedes hat sein eigenes Ausfallbild, und wer die Bilder kennt, erkennt am Symptom, welches Zertifikat er suchen muss.

Skizze 4: Drei Zertifikate, drei Ausfallbilder

Wer wissen will, warum die Anmeldung scheitert, muss wissen, welches Zertifikat gerade fehlt

SSL / Service-Communications	Token-Signing	Proxy-Trust (WAP)
Aufgabe Schützt die HTTPS-Verbindung zu sts.contoso.de auf ADFS und WAP.	Aufgabe Signiert jedes ausgestellte Token. Die Anwendung kennt den öffentlichen Schlüssel.	Aufgabe Client-Zertifikat, mit dem sich der WAP gegenüber der Farm ausweist. Erneuert sich selbst.
Wenn es fehlt oder abläuft Browser zeigt Zertifikatswarnung, Clients brechen ab, WAP verliert den Kontakt.	Wenn es fehlt oder abläuft ADFS meldet Erfolg, die Anwendung lehnt das Token ab – oder Microsoft 365 meldet Föderationsfehler.	Wenn es fehlt oder abläuft Extern geht nichts mehr, intern alles. Der WAP kann seine Konfiguration nicht laden.
Prüfen <pre>netsh http show sslcert Get-AdfsSslCertificate</pre>	Prüfen <pre>Get-AdfsCertificate -CertificateType Token-Signing</pre>	Prüfen <pre>Install-WebApplicationProxy (Trust neu aufbauen)</pre>

Skizze 4: Die drei kritischen Zertifikate und ihre Ausfallbilder

```
# Alle ADFS-Zertifikate mit Ablaufdatum
Get-AdfsCertificate |
    Select-Object CertificateType, IsPrimary,
        @{n="Ablauf";e={$_.Certificate.NotAfter}},
        @{n="Betreff";e={$_.Certificate.Subject}}

# Automatischer Rollover aktiv?
Get-AdfsProperties | Select-Object AutoCertificateRollover,
    CertificateGenerationThreshold, CertificatePromotionThreshold

# SSL-Bindung auf ADFS-Server und WAP
Get-AdfsSslCertificate
netsh http show sslcert
```

Listing 4: Zertifikate der Farm auf einen Blick

Beim SSL-Zertifikat ist der Fall meist eindeutig: Der Browser schimpft, und spätestens beim Blick auf das Ablaufdatum ist die Sache klar. Tückischer sind zwei Varianten. Erstens: Das Zertifikat wurde auf der Farm getauscht, aber nicht auf dem WAP – dann scheitert nur der externe Zugriff. Zweitens: Das neue Zertifikat ist gültig, aber die Zwischenzertifizierungsstelle fehlt auf dem Server, sodass Clients die Kette nicht aufbauen können. Auf ADFS tauschst du das Zertifikat mit Set-AdfsSslCertificate -Thumbprint, auf dem WAP mit Set-WebApplicationProxySslCertificate -Thumbprint. Die Details samt Stolperfallen beim Tausch stehen im Beitrag [SSL-Zertifikat auf ADFS und Web Application Proxy tauschen](#).

Beim Token-Signing-Zertifikat ist das Bild subtiler. ADFS stellt fröhlich Tokens aus, die Anmeldeseite funktioniert, nur die Anwendung lehnt ab, weil sie das neue Zertifikat nicht kennt. Mit AutoCertificateRollover erzeugt ADFS ein neues Zertifikat rechtzeitig vor Ablauf und macht es nach einer Übergangszeit zum primären. Anwendungen, die die Föderationsmetadaten regelmäßig abrufen, bekommen das mit. Anwendungen, bei denen jemand das Zertifikat vor drei Jahren von Hand hochgeladen hat, bekommen es nicht mit – und fallen am Tag des Wechsels um. Wie du den Wechsel planst und ankündigst, beschreibt der Beitrag [ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover](#).

Microsoft 365 ist ein Sonderfall, der eine eigene Erwähnung verdient. Entra ID kennt das Signaturzertifikat deiner Farm aus der Föderationskonfiguration der Domäne. Ist sie nach einem Wechsel nicht aktualisiert, scheitern die Anmeldungen der föderierten Domäne. Prüfen und aktualisieren kannst du das heute mit Microsoft Graph PowerShell. Früher stand in jeder Anleitung Update-MsolFederatedDomain aus dem MSOnline-Modul – das Modul ist ausgemustert, der aktuelle Weg führt über Graph oder Entra Connect.

```
Connect-MgGraph -Scopes "Domain.Read.All"

# Welches Signaturzertifikat kennt Entra ID für die Domäne?
Get-MgDomainFederationConfiguration -DomainId "contoso.de" |
    Select-Object IssuerUri, PassiveSignInUri, SigningCertificate, NextSigningCertificate

# Zum Vergleich: das primäre Token-Signing-Zertifikat der Farm
$cert = (Get-AdfsCertificate -CertificateType Token-Signing |
    Where-Object IsPrimary).Certificate
[Convert]::ToBase64String($cert.RawData)
```

Listing 5: Signaturzertifikat in Entra ID und in der Farm vergleichen

Unterscheiden sich die beiden Werte, ist der Fall klar. Wie du die Konfiguration mit Update-MgDomainFederationConfiguration oder über Entra Connect aktualisierst, beschreibt Schritt für Schritt der Beitrag [Microsoft-365-Federation-Trust nach Zertifikatswechsel aktualisieren](#). Ein zweiter Klassiker in diesem Umfeld ist der Fehler AADSTS50107: Entra ID findet zum Issuer im Token kein passendes Föderationsobjekt. Dann passt die Issuer-URI, die ADFS ausstellt, nicht zu der, die in der Domänenkonfiguration steht – typischerweise bei mehreren föderierten Domänen, wenn die Claim-Regel für den Issuer fehlt oder verändert wurde. Hintergründe dazu liefert der [ADFS Claim Rules – der Leitfaden](#).

Zertifikat	Wer prüft es?	Typisches Symptom bei Ablauf	Erneuerung
SSL (Service-Communications)	Browser, Clients, WAP	Zertifikatswarnung, Verbindungsabbruch	Von Hand auf allen ADFS-Servern und WAPs
Token-Signing	Jede Relying Party, Entra ID	Anwendung lehnt Token ab	Automatisch mit AutoCertificateRollover oder von Hand
Token-Decrypting	ADFS selbst bei verschlüsselten Tokens von Claims Providern	Anmeldung über Partner-IdP scheitert	Wie Token-Signing

Proxy-Trust	ADFS-Farm	Extern keine Anmeldung, WAP lädt keine Konfiguration	Automatisch, solange der WAP Kontakt hat; sonst Install-WebApplicationProxy
Zertifikat des MFA-Adapters	Entra ID	MFA-Schritt scheitert nach erfolgreichem Kennwort	Siehe ADFS mit Entra-MFA koppeln – Adapter, Zertifikat und Fallstricke

Tabelle 2: Zertifikate rund um ADFS und ihr Ausfallbild

TIPP – Ablaufdaten gehören ins Monitoring, nicht in den Kalender von Kollege Meier

Ein kleines Skript, das täglich Get-AdfsCertificate und die SSL-Bindungen auf Farm und WAP ausliest und 60 Tage vor Ablauf alarmiert, erspart dir die Montagmorgen-Feuerwehr. Wie du Überwachung und Health Checks aufsetzt, steht im Beitrag [ADFS überwachen – Health Checks, Diagnose-Toolbox und Entra Connect Health](#).

Identifizier, Konten und Kerberos: wenn ADFS genau weiß, was es nicht will

In diesem Kapitel geht es um Fehler, die ADFS sehr präzise erkennt – und trotzdem nur unhöflich knapp meldet. Die Anwenderin sieht „Ein Fehler ist aufgetreten“, du siehst im Admin-Log eine Exception mit MSIS-Code. Der Code ist die halbe Diagnose.

Falscher Identifizier: MSIS7007 und seine Verwandten

Jede Anfrage an ADFS nennt die Relying Party, für die ein Token gewünscht wird – bei SAML im Issuer der Anfrage, bei WS-Federation im Parameter wtrealm. ADFS sucht nach einem Relying Party Trust mit genau diesem Identifizier. Genau heißt genau: Groß- und Kleinschreibung in Pfaden, ein abschließender Schrägstrich, http statt https oder ein Port, der in der Anwendung steht, aber nicht im Trust. Findet ADFS nichts, landet im Admin-Log der Fehler MSIS7007: Der angeforderte Relying Party Trust ist nicht angegeben oder wird nicht unterstützt.

```
# Welche Identifizier kennt die Farm?
Get-AdfsRelyingPartyTrust | Select-Object Name, Enabled, Identifizier

# Gezielt nach dem Identifizier aus der Fehlermeldung suchen
Get-AdfsRelyingPartyTrust -Identifizier "https://portal.contoso.de/saml"

# Identifizier ergänzen, ohne den bestehenden zu verlieren
$rp = Get-AdfsRelyingPartyTrust -Name "Contoso Portal"
Set-AdfsRelyingPartyTrust -TargetName "Contoso Portal" `
    -Identifizier ($rp.Identifizier + "https://portal.contoso.de/saml/")
```

Listing 6: Identifizier prüfen und ergänzen

Zwei weitere Fehlerbilder sehen ähnlich aus, haben aber andere Ursachen. Ist der Trust vorhanden, aber deaktiviert, zeigt Get-AdfsRelyingPartyTrust das in der Eigenschaft Enabled. Und erwartet die Anwendung eine Signatur mit SHA-256, während der Trust noch auf SHA-1 steht – oder umgekehrt –, stellt ADFS das Token zwar aus, die Anwendung verwirft es aber. Die Eigenschaft SignatureAlgorithm am Trust verrät, was eingestellt ist. Fehlende oder falsch formatierte Claims, vor allem eine NameID im falschen Format, gehören ebenfalls in diese Kategorie. Wie du einen Trust sauber anlegst, steht im Beitrag [Relying Party Trust anlegen – per Metadaten und von Hand](#), ein durchgespieltes SaaS-Beispiel im Beitrag [SAML-Anwendung an ADFS anbinden – Praxisbeispiel SaaS](#).

FAKTEN – Fehlercodes, die du kennen solltest

MSIS7007 – der angefragte Relying Party Trust ist unbekannt. Identifizier prüfen.

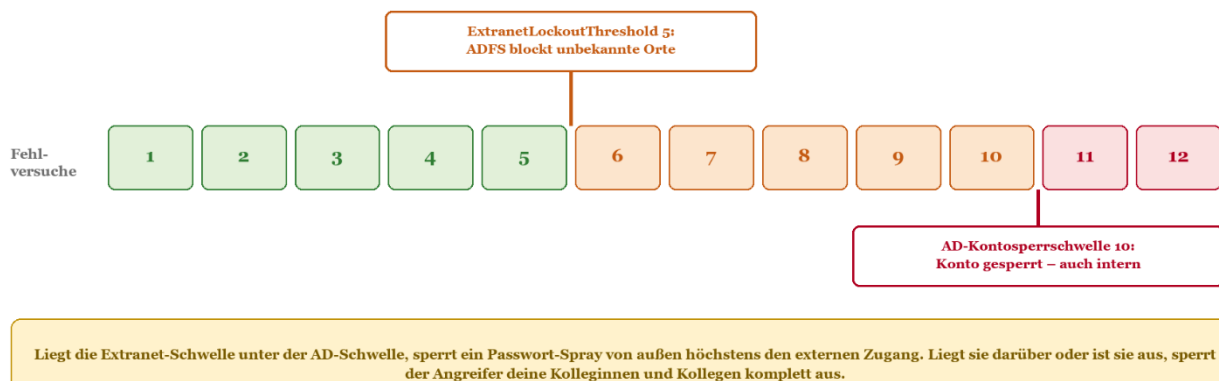
MSIS7042 – Schleifenerkennung: zu viele Token-Anfragen derselben Browsersitzung in kurzer Zeit.
AADSTS50107 – Entra ID findet zum Issuer im Token kein Föderationsobjekt. Issuer-URI prüfen.
Ereignis 364 im Admin-Log – der Sammelbehälter für Fehler bei passiven Anfragen. Die eigentliche Ursache steht in der Exception im Ereignistext.

Gesperrte Konten: AD-Sperre und Extranet Smart Lockout

„Mein Kennwort ist richtig, ich hab’s dreimal geprüft!“ – oft stimmt das sogar. Das Konto ist trotzdem gesperrt, weil das alte Kennwort noch im Smartphone, im Mailprogramm zu Hause oder auf dem Tablet der Tochter steckt und dort im Minutentakt gegen ADFS anrennt. Oder weil ein Passwort-Spray von außen läuft und genau dieses Konto erwisch hat. ADFS kennt zwei Sperren, die du auseinanderhalten musst: die Kontosperre im Active Directory, die überall gilt, und die Extranet-Sperre von ADFS, die nur Anmeldungen über den WAP betrifft.

Skizze 5: Zwei Sperren, eine Reihenfolge

Extranet Smart Lockout muss vor der AD-Kontosperre greifen – Beispielwerte, nicht Standardwerte



Skizze 5: Die Extranet-Sperre muss vor der AD-Kontosperre greifen

```
# Sperre im Active Directory
Get-ADUser anna.beispiel -Properties LockedOut, BadLogonCount, LastBadPasswordAttempt, PasswordExpired |
    Select-Object Name, LockedOut, BadLogonCount, LastBadPasswordAttempt, PasswordExpired
Unlock-ADAccount -Identity anna.beispiel

# Extranet Smart Lockout: Zustand des Kontos aus Sicht von ADFS
Get-AdfsAccountActivity -Identity "anna.beispiel@contoso.de"

# Sperre für unbekannte Orte zurücksetzen
Reset-AdfsAccountLockout -UserPrincipalName "anna.beispiel@contoso.de" -Location Unknown
```

Listing 7: AD-Sperre und Extranet-Sperre prüfen und zurücksetzen

Get-AdfsAccountActivity zeigt dir, ob ADFS das Konto für bekannte oder unbekannte Orte blockt und von welchen IP-Adressen die Fehlversuche kommen. Steht dort eine Liste fremder Adressen, hast du keinen Supportfall, sondern einen Sicherheitsvorfall. Wie du Passwort-Spray und Brute Force erkennst, zeigt der Beitrag [Passwort-Spray und Brute Force auf ADFS erkennen](#). Entscheidend ist die Reihenfolge der Schwellen: Microsoft empfiehlt, die Extranet-Schwelle unter die Kontosperrschwelle des AD zu legen, damit ein Angriff von außen höchstens den externen Zugang blockiert. Einrichtung und Betriebsmodi von Smart Lockout erklärt der Beitrag [Extranet Smart Lockout – ADFS gegen Passwort-Spray schützen](#).

WARNUNG – Entsperren ohne Ursache ist Beschäftigungstherapie

Wenn ein Konto zehn Minuten nach dem Entsperren wieder gesperrt ist, hilft kein elftes Entsperren. Finde das Gerät mit dem alten Kennwort. Die Domänencontroller protokollieren die Sperre mit dem Namen des aufrufenden Systems – steht dort ein ADFS-Server, kommen die Fehlversuche über ADFS, und Get-AdfsAccountActivity verrät dir die IP-Adressen.

SPN-Probleme: wenn intern plötzlich das Formular erscheint

Im Firmennetz soll die Anmeldung per Integrierter Windows-Authentifizierung still durchlaufen. Erscheint stattdessen das Anmeldeformular oder ein Kennwortdialog des Browsers, ist Kerberos fast immer der Grund. Der Browser fragt ein Ticket für HTTP/sts.contoso.de an. Dazu muss genau dieser Service Principal Name an genau einem Konto hängen – dem ADFS-Dienstkonto, heute idealerweise einem gMSA. Fehlt der SPN, fällt der Browser auf NTLM oder das Formular zurück. Ist er doppelt vorhanden, etwa weil jemand ihn zusätzlich an ein Computerkonto oder ein altes Dienstkonto gehängt hat, scheitert Kerberos ganz.

```
# Wer besitzt den SPN?
setspn -Q HTTP/sts.contoso.de

# Doppelte SPNs im Forest finden
setspn -X -F

# SPN am gMSA setzen (-S prüft vorher auf Duplikate)
setspn -S HTTP/sts.contoso.de CONTOSO\gmsa-adfs$
```

Listing 8: SPN prüfen und korrekt setzen

Ist der SPN in Ordnung, liegt es meist am Browser. Der Name sts.contoso.de muss in der Zone „Lokales Intranet“ stehen, sonst bietet der Browser kein Kerberos an. Edge und Chrome übernehmen diese Zone aus den Windows-Einstellungen, Firefox hat eigene Richtlinien. Und ADFS bietet Integrierte Windows-Authentifizierung nur Browsern an, deren User-Agent in WIASupportedUserAgents steht. Fehlt der Eintrag für einen neuen Browser, bekommt er das Formular – zuverlässig und ohne Fehlermeldung. Die ganze Kette aus SPN, DNS, Zone und User-Agent erklärt der Beitrag [SPN, DNS und Kerberos für ADFS – warum die interne Anmeldung auf Formular zurückfällt](#), die Kerberos-Grundlagen dahinter die Seite [Microsoft Kerberos](#). Läuft der Dienst unter einem gMSA oder soll er dorthin umziehen, hilft der Beitrag [gMSA als ADFS-Dienstkonto einrichten und umstellen](#).

```
# Welche Browser bekommen Windows-Authentifizierung angeboten?
Get-AdfsProperties | Select-Object -ExpandProperty WIASupportedUserAgents

# Eintrag ergänzen, ohne die bestehende Liste zu überschreiben
$ua = (Get-AdfsProperties).WIASupportedUserAgents
Set-AdfsProperties -WIASupportedUserAgents ($ua + "Edg/")
```

Listing 9: User-Agents für Windows-Authentifizierung prüfen und ergänzen

TIPP — Ein DNS-Eintrag als CNAME kann Kerberos verwirren

Löst sts.contoso.de per CNAME auf einen anderen Namen auf, fragen manche Clients das Ticket für den Zielnamen an statt für den Dienstenamen. Ein A-Eintrag für den Federation Service Namen auf die virtuelle IP des Load Balancers erspart dir diese Sorte Rätsel.

WAP, Proxy und Browser: die Strecke vor dem Server

Ein guter Teil der Störungen entsteht gar nicht in der Farm, sondern auf dem Weg dorthin. Der Web Application Proxy, Proxys und Inspektionssysteme im Netz, Load Balancer und schließlich der Browser selbst haben alle ihre eigene Meinung dazu, was eine gültige Verbindung ist.

WAP-Trust abgelaufen: extern geht nichts, intern alles

Der Web Application Proxy weist sich gegenüber der Farm mit einem Proxy-Trust-Zertifikat aus, das in seinem Zertifikatsspeicher als „ADFS ProxyTrust“ mit dem Namen des WAP erscheint. Das Zertifikat erneuert sich automatisch, solange der WAP regelmäßig mit der Farm spricht. Microsoft nennt als typische Ursachen für einen kaputten Trust: Der WAP war zu lange ausgeschaltet, die Verbindung zur Farm war unterbrochen, die Zertifikatsinfrastruktur hat ein Problem, oder die Uhren von WAP und Farm laufen auseinander. Der Klassiker in der Praxis ist der Reserve-WAP, der monatelang ausgeschaltet im Hypervisor lag und nach dem Einschalten seelenruhig Verbindungen annimmt, die er nicht bedienen kann.

```
# Auf dem WAP: Konfiguration und veröffentlichte Anwendungen
Get-WebApplicationProxyConfiguration
Get-WebApplicationProxyApplication | Select-Object Name, ExternalUrl, BackendServerUrl

# Proxy-Trust-Zertifikat im Computerspeicher
Get-ChildItem Cert:\LocalMachine\My |
    Where-Object Subject -like "*ADFS ProxyTrust*" |
    Select-Object Subject, NotBefore, NotAfter

# Trust neu aufbauen (Anmeldedaten eines lokalen Administrators der ADFS-Server)
$cred = Get-Credential
Install-WebApplicationProxy -FederationServiceName "sts.contoso.de" `
    -CertificateThumbprint "<Fingerabdruck des SSL-Zertifikats>" `
    -FederationServiceTrustCredential $cred
```

Listing 10: WAP-Trust prüfen und neu aufbauen

Bevor du den Trust neu aufbaust, prüfe die Punkte, die Microsoft für diesen Fall auflistet: Zeitabweichung, SSL-Bindung auf Farm und WAP mit netsh http show sslcert – der Fingerabdruck muss zum Zertifikat passen, und als Speicher für die Zertifikatsvertrauensliste muss AdfsTrustedDevices eingetragen sein –, sowie nicht selbstsignierte Zertifikate im Speicher der vertrauenswürdigen Stammzertifizierungsstellen. Letztere gehören in den Speicher der Zwischenzertifizierungsstellen. Dazu kommen die SPNs: host/ muss auf das ADFS-Dienstkonto auflösen. Alle Details zum Erneuern des Vertrauens beschreibt der Beitrag [WAP-Proxy-Vertrauen erneuern – wenn der Web Application Proxy plötzlich nicht mehr will](#), Architektur und Ablöseoptionen des WAP die Seite [Web Application Proxy: Architektur und Ablöse](#).

WICHTIG – Reserve-WAPs regelmäßig einschalten – oder aus dem Pool nehmen

Ein WAP, der im Load-Balancer-Pool steht, aber keinen gültigen Trust mehr hat, beantwortet jede x-te externe Anmeldung mit einem Fehler. Das ergibt das schönste aller Fehlerbilder: „Manchmal geht’s.“ Nimm Knoten, die du nicht betreibst, aus dem Pool, und lass die Health Probe des Load Balancers nicht nur Port 443, sondern den Probe-Endpunkt prüfen.

Proxy-Vertrauen im Netz: TLS-Inspektion, Load Balancer und SNI

Zwischen Browser und Farm stehen in vielen Netzen weitere Geräte, die TLS aufbrechen: Webproxys mit TLS-Inspektion, Next-Generation-Firewalls oder Load Balancer, die TLS terminieren und neu aufbauen. Für den normalen Webverkehr ist das gewollt, für ADFS ist es Gift. Bei der Integrierten Windows-Authentifizierung bindet ADFS die Anmeldung über Extended Protection an den TLS-Kanal. Bricht ein Gerät dazwischen TLS auf, passt die Bindung nicht mehr, und die Anmeldung scheitert. Die Eigenschaft ExtendedProtectionTokenCheck in Get-AdfsProperties zeigt, wie streng ADFS hier prüft. Abschalten ist die falsche Antwort. Richtig ist, sts.contoso.de von der Inspektion auszunehmen und den Load Balancer im Durchreich-Modus zu betreiben.

Ein zweiter Proxy-Effekt betrifft die Zertifikatsauswahl. ADFS und WAP binden ihre Zertifikate per SNI an den Hostnamen. Clients oder Health Probes, die keinen Hostnamen mitschicken, bekommen dann kein oder das falsche Zertifikat und brechen ab. Wie du Health Probe, SNI und Persistenz am Load Balancer richtig einstellst, steht im Beitrag [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#). Wer mit dem Kemp LoadMaster arbeitet, findet Hintergründe auf der Seite [Kemp LoadMaster](#).

Gerät im Pfad	Was es mit ADFS anstellt	Folge	Abhilfe
Webproxy mit TLS-Inspektion	Bricht TLS auf, präsentiert eigenes Zertifikat	Windows-Authentifizierung scheitert, Formular erscheint	sts.contoso.de von Inspektion ausnehmen
Load Balancer mit TLS-Terminierung	Baut neue TLS-Verbindung zur Farm auf	Extended Protection und Zertifikatsauthentifizierung brechen	TLS durchreichen (Layer 4)
Health Probe ohne SNI	Fragt ohne Hostnamen an	Knoten wird fälschlich als tot markiert	Probe-Endpunkt per HTTP prüfen
Firewall mit kurzem Leerlauf-Timeout	Trennt lange Verbindungen	Sporadische Abbrüche, WAP verliert Kontakt	Timeout erhöhen, Verbindung zur Farm freigeben

Tabelle 3: Geräte im Pfad und ihre Wirkung auf ADFS

Browser-Cookies und Schleifen: wenn die Seite Schluckauf hat

ADFS merkt sich die Anmeldung einer Browsersitzung in Cookies, deren Namen mit MSIS beginnen, etwa MSISAuth und MSISAuthenticated. Dazu kommt ein Cookie für die Schleifenerkennung. Meistens arbeiten diese Cookies unauffällig. Auffällig werden sie, wenn sie aus einer alten Sitzung stammen, wenn eine Anwendung ihre eigenen Cookies nicht setzen kann oder wenn eine Browser-Richtlinie Cookies für sts.contoso.de blockiert. Dann schickt die Anwendung den Browser zu ADFS, ADFS stellt brav ein Token aus, die Anwendung nimmt es nicht an und schickt den Browser zurück. Nach einigen Runden zieht ADFS die Notbremse und meldet MSIS7042.

Laut Microsoft liegt die Ursache einer solchen Schleife fast immer bei der Anwendung, die das Token nicht verarbeitet – nicht bei ADFS. Die Schleifenerkennung lässt sich zwar mit LoopDetectionMaximumTokensIssuedInInterval und LoopDetectionTimeIntervalInSeconds in Set-AdfsProperties anpassen, dauerhaft abschalten solltest du sie aber nicht: Sie schützt die Farm vor Clients, die sie in Endlosschleifen mit Anfragen bombardieren. Schau stattdessen, was die Anwendung mit dem Token macht: falsche Antwort-URL, fehlender Claim, Zeitabweichung oder ein Cookie, das an den SameSite-Regeln moderner Browser scheitert, weil die Anwendung es ohne die nötigen Attribute setzt.

TIPP – Der Zehn-Sekunden-Test

Bevor du ein Ticket eskalierst: privates Browserfenster öffnen, anmelden. Geht es dort, liegt das Problem im Cookie-Speicher des Browsers oder in einer Erweiterung. Cookies für sts.contoso.de und die Anwendung löschen, fertig. Geht es auch dort nicht, ist es kein Browserproblem – und du hast eine Ursache mit einem einzigen Klick ausgeschlossen.

WEITER – Wenn die Anmeldung erst beim zweiten Faktor scheitert

- › [ADFS mit Entra-MFA koppeln – Adapter, Zertifikat und Fallstricke](#) – Adapter, Zertifikat und die typischen Stolperfallen der MFA-Kopplung
- › [Access Control Policies in ADFS – Zugriffsregeln ohne Claim-Rule-Akrobatik](#) – warum eine Richtlinie Zugriff verweigert, obwohl das Kennwort stimmt

Fazit: Die meisten Ausfälle haben ein Ablaufdatum

Wenn eine ADFS-Anmeldung fehlschlägt, ist das selten ein Rätsel und fast nie ein Fall für Panik. Zeit, Zertifikate, Identifier, Konten, SPN, WAP-Trust, Proxys und Cookies – diese acht Kandidaten erklären die allermeisten Störungen. Wer vom Symptom ausgeht, die Aktivitäts-ID ernst nimmt und zuerst klärt, ob intern, extern oder beides betroffen ist, hat die Ursache meist in einer Viertelstunde eingekreist. Der Rest ist Handwerk: eine Änderung nach der anderen, testen, notieren.

Noch besser ist natürlich die Störung, die gar nicht erst kommt. Fast alle Fehlerbilder in diesem Beitrag kündigen sich an: Zertifikate haben ein Ablaufdatum, Uhren driften messbar, Reserve-WAPs liegen sichtbar im Hypervisor. Ein Monitoring, das diese Dinge im Blick behält, macht aus dem Montagmorgen wieder einen normalen Tag. Und das gilt unabhängig davon, ob du die Farm noch zehn Jahre betreibst oder die Umstellung nach Entra ID schon plant – bis zum letzten Tag soll sie sauber laufen. Den Weg dorthin beschreiben die Seite [Microsoft Entra ID](#) und der Beitrag [Microsoft 365 von Federated auf Managed umstellen – mit Staged Rollout](#).

Wenn du bei einer hartnäckigen Störung eine zweite Meinung brauchst oder die Farm gleich systematisch durchleuchten lassen willst, unterstützen wir dich im [Consulting zu ADFS \(Active Directory Federation Services\)](#). Wer die Fehlerbilder lieber im Labor selbst erzeugt und löst, bevor sie in der Produktion auftauchen, ist in den [ADFS-Schulungen](#) richtig. Fehlersuche, Protokolle und Betrieb der Farm vertieft außerdem das Buch – mehr dazu unter [ADFS in der Praxis – das Buch im Detail](#).

WEITER — Die Einzelthemen im Detail

- › [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#) – die Aktivitäts-ID richtig verfolgen
- › [SSL-Zertifikat auf ADFS und Web Application Proxy tauschen](#) – wenn der Browser schimpft
- › [ADFS Token-Signing-Zertifikat erneuern – mit und ohne AutoCertificateRollover](#) – wenn die Anwendung schimpft
- › [Microsoft-365-Federation-Trust nach Zertifikatswechsel aktualisieren](#) – wenn Microsoft 365 schimpft
- › [Relying Party Trust anlegen – per Metadaten und von Hand](#) – Identifier, Signatur und Claims sauber setzen
- › [Extranet Smart Lockout – ADFS gegen Passwort-Spray schützen](#) – Sperren, die schützen statt aussperren
- › [SPN, DNS und Kerberos für ADFS – warum die interne Anmeldung auf Formular zurückfällt](#) – wenn intern das Formular erscheint
- › [WAP-Proxy-Vertrauen erneuern – wenn der Web Application Proxy plötzlich nicht mehr will](#) – wenn extern nichts mehr geht
- › [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#) – Health Probe, SNI und Persistenz
- › [ADFS überwachen – Health Checks, Diagnose-Toolbox und Entra Connect Health](#) – damit der nächste Montag ruhig bleibt

FAQ: ADFS-Anmeldung fehlgeschlagen

Wo finde ich die Ursache, wenn die ADFS-Anmeldung fehlschlägt?

Im Ereignisprotokoll „AD FS/Admin“ des ADFS-Servers, der die Anfrage bearbeitet hat. Suche nach der Aktivitäts-ID von der Fehlerseite. Ereignis 364 ist der übliche Eintrag, die eigentliche Ursache steht in der Exception im Ereignistext. In einer Farm musst du gegebenenfalls alle Knoten durchsuchen.

Was bedeutet MSIS7007?

ADFS kennt den angefragten Relying Party Trust nicht. Der Identifier in der Anfrage passt nicht zu einem Trust in der Farm – oft wegen eines abschließenden Schrägstrichs, http statt https oder eines Tippfehlers. Prüfe mit Get-AdfsRelyingPartyTrust -Identifier und gleiche den Identifier exakt an.

Warum geht die Anmeldung intern, aber nicht von extern?

Weil der externe Weg über den Web Application Proxy führt. Häufigste Ursachen sind ein abgelaufener Proxy-Trust, ein veraltetes SSL-Zertifikat auf dem WAP, eine abweichende Uhrzeit des WAP oder eine Firewall, die die Verbindung zur Farm blockiert. Den Trust baust du mit Install-WebApplicationProxy neu auf.

Warum erscheint im Firmennetz das Anmeldeformular statt Single Sign-on?

Meist fehlt der SPN HTTP/sts.contoso.de am ADFS-Dienstkonto oder er ist doppelt vergeben. Weitere Ursachen: Der Name steht nicht in der Intranetzzone des Browsers, der User-Agent fehlt in WIASupportedUserAgents, oder ein Proxy mit TLS-Inspektion steht im Weg.

Wie viel Zeitabweichung verträgt ADFS?

Kerberos toleriert standardmäßig fünf Minuten. Bei SAML- und WS-Federation-Tokens entscheidet die Anwendung, viele erlauben nur sehr wenig Abweichung. Sorge dafür, dass ADFS, WAP und Anwendungen dieselbe zuverlässige Zeitquelle nutzen. NotBeforeSkew am Relying Party Trust ist nur eine Notlösung.

Was passiert, wenn das Token-Signing-Zertifikat abläuft?

ADFS kann keine gültigen Tokens mehr signieren, und Anwendungen lehnen die Anmeldung ab. Mit AutoCertificateRollover erneuert ADFS das Zertifikat selbst – Anwendungen, die das Zertifikat von Hand hinterlegt haben, und Microsoft 365 müssen das neue Zertifikat aber kennen. Prüfe das rechtzeitig vor dem Wechsel.

Wie entsperre ich ein Konto, das ADFS per Extranet Smart Lockout blockiert?

Mit Get-AdfsAccountActivity siehst du den Zustand, mit Reset-AdfsAccountLockout -UserPrincipalName und -Location Unknown oder Familiar setzt du die Sperre zurück. Eine Sperre im Active Directory hebst du unabhängig davon mit Unlock-ADAccount auf. Finde vorher die Quelle der Fehlversuche.

Was tun bei der Fehlermeldung MSIS7042?

Das ist die Schleifenerkennung von ADFS. Die Anwendung nimmt das Token nicht an und schickt den Browser immer wieder zurück. Prüfe Antwort-URL, Claims, Zeit und Cookies der Anwendung. Die Schleifenerkennung dauerhaft abzuschalten ist keine Lösung.

Hilft es, Browser-Cookies zu löschen?

Wenn nur einzelne Personen betroffen sind und die Anmeldung im privaten Fenster funktioniert, ja. Lösche die Cookies für den Federation Service und die Anwendung. Sind viele betroffen, liegt die Ursache woanders.

Wie teste ich ADFS unabhängig von der Anwendung?

Schalte mit Set-AdfsProperties -EnableIdpInitiatedSignonPage \$true die IdP-initiierte Anmeldeseite ein und melde dich dort an. Klappt das, ist ADFS grundsätzlich gesund. Schalte die Seite nach dem Test wieder ab.