

Extranet Smart Lockout – ADFS gegen Passwort-Spray schützen

ADFS · Schutz vor Passwort-Spray

Sperr den Angreifer aus – nicht deine eigenen Leute

Extranet Lockout, Smart Lockout, vertraute Standorte und die Frage, welche IP-Adresse ADFS eigentlich sieht.

boddenberg.de

sts.contoso.de

Vertrauter Standort

Kennwort richtig > willkommen

Zähler: 2 von 10

Tür bleibt offen

Unbekannter Standort

Kennwort-Spray aus aller Welt

Zähler: 10 von 10

Tür zu – nur für diese Seite

WISSEN Grundlagen, Architektur und alle Praxisbeiträge rund um ADFS an einem Ort. > Active Directory Federation Services	BERATUNG Montags gesperrte Vorstände, nachts Spray aus aller Welt? Wir stellen Smart Lockout mit dir sauber ein – inklusive Load Balancer. > Consulting zu ADFS	SCHULUNG Im Labor spraysen, sperren, entsperren: Smart Lockout einmal gefahrlos von beiden Seiten erleben. > ADFS-Schulungen
---	--	---

Montag, 7:40 Uhr. Das Telefon der Hotline klingelt im Minutentakt, und alle sagen dasselbe: „Ich komme nicht mehr in Outlook, und mein Kennwort stimmt ganz sicher.“ Es stimmt tatsächlich. Das Problem ist nur, dass irgendwer am Wochenende aus ein paar hundert Adressen weltweit ausprobiert hat, ob „Sommer2026!“ bei euch funktioniert – für jedes Konto, dessen Namen er kannte. Die AD-Kontosperre hat brav gezählt und brav gesperrt. Der Angreifer ist nicht hereingekommen. Deine Kolleginnen und Kollegen aber auch nicht. Man könnte sagen, die Sicherheitsmaßnahme hat perfekt funktioniert, nur leider für die falsche Mannschaft.

Genau dagegen hat Microsoft in ADFS zwei Funktionen eingebaut, die gern verwechselt werden: das klassische Extranet Lockout aus Windows Server 2012 R2 und das Extranet Smart Lockout (ESL), das mit Windows Server 2016 nachgerüstet wurde und ab Windows Server 2019 fest dabei ist. Wer „adfs extranet smart lockout“ sucht, will meist wissen, wie das eine vom anderen abweicht, welche Schwellwerte sinnvoll sind und wie man ESL einführt, ohne am ersten Tag die halbe Belegschaft auszusperrern. Darum geht es hier – plus um das Detail, an dem in der Praxis die meisten Einführungen scheitern: die Client-IP-Adresse am Load Balancer. Die Grundlagen zu Farm, Proxy und Relying Parties findest du auf der Übersichtsseite [Active Directory Federation Services](#).

FAKTEN – Extranet Smart Lockout auf einen Blick

ESL gibt es für ADFS auf Windows Server 2016 (mit den Updates ab Juni 2018 und Farmverhalten 2016) und ist ab Windows Server 2019 eingebaut.

ESL greift nur bei Anmeldungen mit Benutzername und Kennwort, die über den Web Application Proxy oder einen Drittanbieter-Proxy mit MS-ADFSPIP-Unterstützung hereinkommen.

Für jeden Benutzer führt ADFS zwei Zähler: einen für vertraute und einen für unbekannte Standorte. Bis zu 20 vertraute IP-Adressen merkt sich ADFS pro Benutzer.

Der Standardmodus heißt ADPasswordCounter – das ist das klassische Extranet Lockout. Smart

Lockout kennt die Modi `ADFSSmartLockoutLogOnly` und `ADFSSmartLockoutEnforce`.
 Microsoft empfiehlt ein Beobachtungsfenster von 30 Minuten und eine ADFS-Schwelle von etwa der Hälfte der AD-Kontosperrschwelle.

Extranet Lockout und Smart Lockout: ein Name, zwei Philosophien

Beide Funktionen hängen an derselben ADFS-Eigenschaft, `EnableExtranetLockout`, und beide werden über `Set-AdfsProperties` gesteuert. Das ist ungefähr so hilfreich, als würde man Feuerlöscher und Rauchmelder unter derselben Artikelnummer verkaufen. Der Unterschied liegt in der Frage, wessen Fehlversuche gezählt werden – und wen die Sperre am Ende trifft.

Das klassische Extranet Lockout: der Türsteher mit einer Strichliste

Das Extranet Lockout aus Windows Server 2012 R2 – in der Dokumentation auch Extranet Soft Lockout genannt, im Parameter `ExtranetLockoutMode` als `ADPasswordCounter` geführt – schaut vor jeder Kennwortprüfung auf den Zähler `badPwdCount` des Benutzers im Active Directory. Ist der Zähler auf oder über `ExtranetLockoutThreshold`, weist ADFS die Anfrage aus dem Extranet ab, ohne das Kennwort überhaupt noch an einen Domänencontroller zu schicken. Erst wenn seit dem letzten Fehlversuch ein Beobachtungsfenster (`ExtranetObservationWindow`) verstrichen ist, darf wieder ein Versuch durch. Damit das zuverlässig funktioniert, fragt ADFS den PDC-Emulator, denn nur dort sind die Fehlversuche domänenweit aktuell.

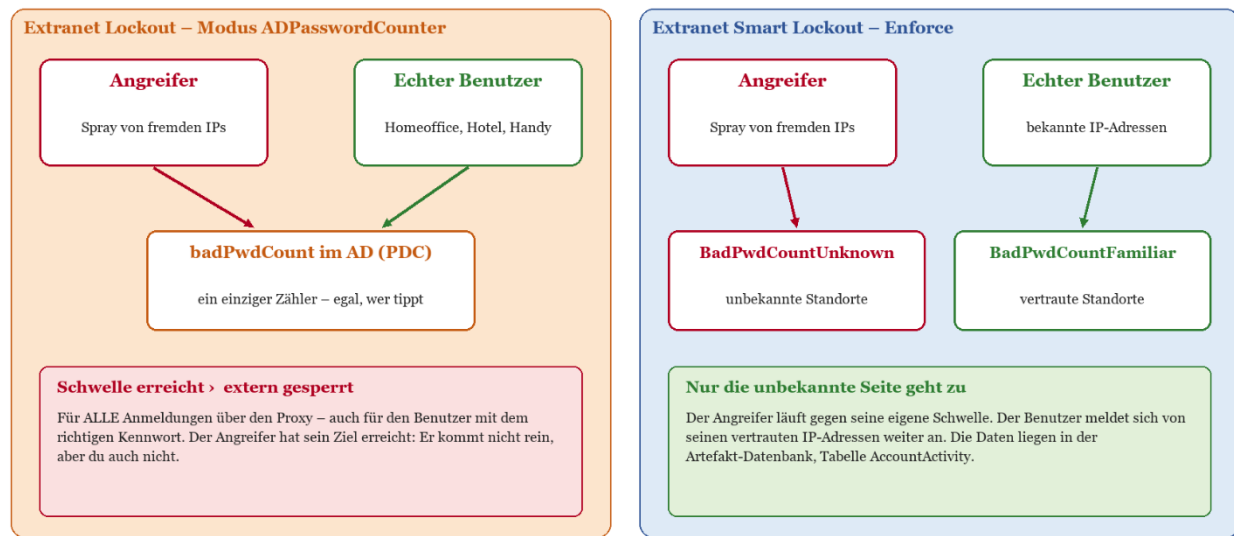
Der Nutzen ist real: Solange die ADFS-Schwelle unter der AD-Schwelle liegt, kann ein Angreifer aus dem Internet das AD-Konto nicht mehr sperren. Intern kann der Benutzer weiterarbeiten. Der Haken ist genauso real: Der Zähler unterscheidet nicht zwischen Angreifer und Benutzer. Ist die Schwelle erreicht, ist das Konto für alle externen Anmeldungen zu – auch für den Vertriebsmitarbeiter im Hotel, der sein Kennwort ganz richtig eintippt. Das Homeoffice, die Outlook-App auf dem Smartphone, der Laptop im Zug: alles draußen.

Extranet Smart Lockout: der Türsteher, der Gesichter kennt

Smart Lockout führt die Zählerei selbst – nicht mehr im AD, sondern in der Artefakt-Datenbank der Farm, in einer eigenen Tabelle `AccountActivity`. Und es führt pro Benutzer zwei Zähler: `BadPwdCountFamiliar` für Fehlversuche von vertrauten Standorten und `BadPwdCountUnknown` für alles andere. Erreicht der Angreifer die Schwelle auf der unbekannten Seite, wird nur diese Seite geschlossen. Der echte Benutzer meldet sich von seinen bekannten Adressen aus weiter an und merkt im Idealfall gar nichts.

Skizze 1: Ein Zähler für alle oder zwei Zähler pro Benutzer

Extranet Lockout (seit 2012 R2) gegen Extranet Smart Lockout (2016 mit Update, ab 2019 eingebaut)



Gilt nur für Benutzername und Kennwort über WAP oder einen MS-ADFSPIF-fähigen Proxy. Interne Anmeldungen direkt an der Farm prüft ESL nicht.

Skizze 1: Klassisches Extranet Lockout mit einem Zähler im AD gegen Smart Lockout mit zwei Zählern pro Benutzer

Merkmal	Extranet Lockout (ADPasswordCounter)	Extranet Smart Lockout
Verfügbar seit	Windows Server 2012 R2	Windows Server 2016 mit Updates ab Juni 2018, eingebaut ab 2019
Wo wird gezählt?	badPwdCount im AD, abgefragt am PDC	Tabelle AccountActivity in der Artefakt-Datenbank
Zähler pro Benutzer	einer	zwei: vertraute und unbekannte Standorte
Wen trifft die Sperre?	alle externen Anmeldungen des Kontos	nur Anmeldungen von unbekannten Standorten (solange der Angreifer keine vertraute IP nutzt)
Zurücksetzen	über das AD bzw. Ablauf des Fensters	Reset-AdfsAccountLockout, nach Standort getrennt
Lernphase	keine	Log-Only-Modus, empfohlen 3 bis 7 Tage
Schutz vor Konto-Sperrung durch Angreifer	ja, für das AD-Konto intern	ja, intern und extern für vertraute Standorte
Schutz, wenn das Kennwort erraten wurde	nein	nein – dafür braucht es MFA

Tabelle 1: Extranet Lockout und Smart Lockout im direkten Vergleich

WICHTIG – Smart Lockout verhindert Sperren, keine Einbrüche

Errät der Angreifer das Kennwort, ist die Anmeldung aus ESL-Sicht ein Erfolg: richtiges Kennwort, neue IP-Adresse. Die Adresse des Angreifers wandert anschließend sogar in die Liste der vertrauten Standorte. ESL schützt deine Leute vor der Aussperrung und bremst Passwort-Spray aus – den erfolgreichen Treffer verhindert es nicht. Dafür gibt es MFA und vernünftige Kennwortregeln.

Vertraute und unbekannte Standorte – was ADFS darunter versteht

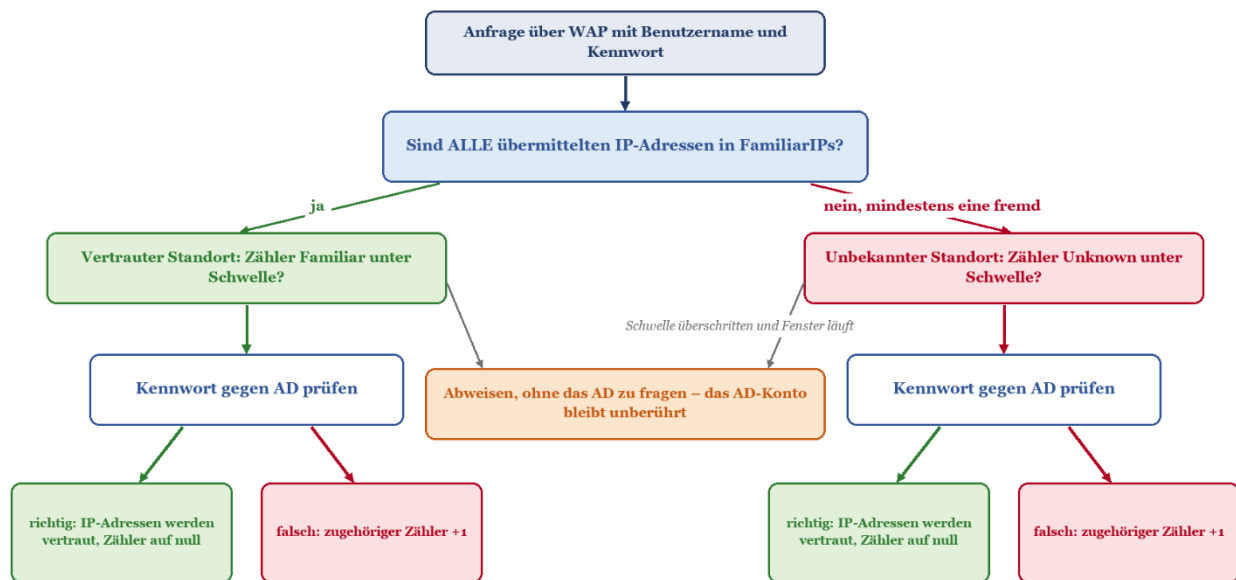
„Standort“ klingt nach Geografie, ist aber schlichter: Gemeint sind IP-Adressen. Bei jeder Anfrage sammelt ESL alle Adressen ein, die es zu sehen bekommt – die Netzwerkadresse, die vom Proxy weitergereichte Client-Adresse und, falls vorhanden, den Inhalt von X-Forwarded-For. Im

Sicherheitsprotokoll stehen diese Adressen im Feld IpAddress in der Reihenfolge x-ms-forwarded-client-ip, x-forwarded-for, x-ms-proxy-client-ip. Nur wenn ALLE Adressen der Anfrage schon in der Liste FamiliarIPs des Benutzers stehen, gilt der Versuch als vertraut. Eine einzige fremde Adresse genügt, und die Anfrage läuft über den Zähler für unbekannte Standorte.

Wie kommt eine Adresse auf die Liste? Durch eine erfolgreiche Anmeldung. Dann übernimmt ADFS alle Adressen dieser Anfrage. Die Liste fasst höchstens 20 Einträge; kommt ein einundzwanzigster dazu, fliegt der älteste raus. Ein Benutzer, der sich bisher nie von einer Adresse aus angemeldet hat, ist dort also zunächst ein Fremder – auch wenn er im Firmenwagen vor dem eigenen Rechenzentrum sitzt. Gibt er sein Kennwort ein paarmal falsch und dann richtig ein, ist das kein Problem: Die erfolgreiche Anmeldung setzt den Zähler zurück und macht die Adresse vertraut. Kritisch wird es erst, wenn er die Schwelle für unbekannte Standorte vorher überschreitet.

Skizze 2: Was ESL bei jeder externen Anmeldung prüft

Vor der Kennwortprüfung, nach der Kennwortprüfung – und wo der Zähler hochgeht



Nach Ablauf des Beobachtungsfensters ist genau ein neuer Versuch gegen das AD erlaubt. Ist der wieder falsch, beginnt das Fenster von vorn.

Skizze 2: Prüfungen von Smart Lockout vor und nach der Kennwortprüfung

Eine Eigenheit des Sperrzustands solltest du kennen, weil sie Helpdesk-Gespräche verkürzt: Ist ein Zähler über der Schwelle, lässt ADFS nach Ablauf des Beobachtungsfensters genau einen Versuch gegen das AD durch. Ist der falsch, beginnt das Fenster von vorn. Von selbst auf null fällt der Zähler nur nach einer erfolgreichen Anmeldung – oder wenn du ihn zurücksetzt. Mehr dazu im Abschnitt über den Reset.

FAKTEN – Wo ESL nicht hinschaut

Anmeldungen, die direkt an der Farm im internen Netz ankommen, laufen an ESL vorbei. Für sie gilt nur die AD-Kontosperre.

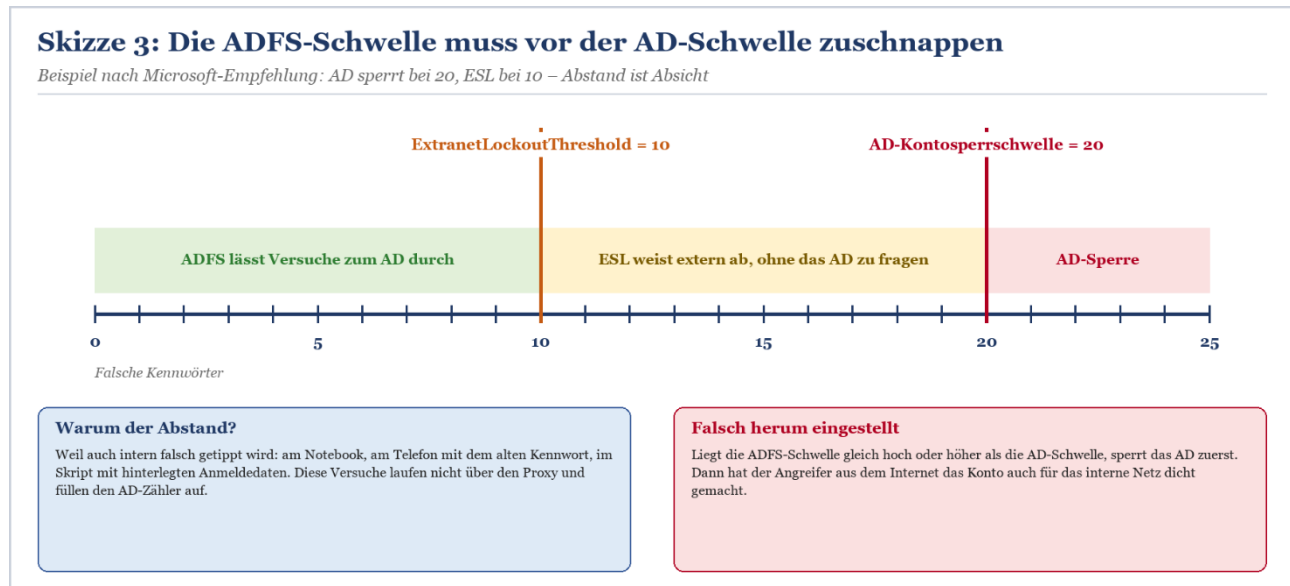
ESL betrifft ausschließlich Benutzername und Kennwort. Zertifikatsanmeldung oder Windows-integrierte Anmeldung fallen nicht darunter.

In einer Farm mit WID hält immer der primäre Knoten die Rolle „User Activity“. In einer SQL-Farm wählt ADFS einen Knoten aus. Welcher es ist, zeigt (Get-AdfsFarmInformation).FarmRoles.

Die sekundären Knoten fragen den Rolleninhaber bei jeder neuen Anmeldung über Port 80 nach dem aktuellen Stand und melden das Ergebnis zurück.

Schwellwerte: das Zusammenspiel mit der AD-Kontosperre

Die AD-Kontosperre und Smart Lockout arbeiten unabhängig voneinander. Das AD weiß nicht, dass ADFS mitzählt, und ADFS stellt keine AD-Richtlinie um. Damit der Schutz aufgeht, muss ADFS deshalb früher zuschnappen als das AD. Microsoft formuliert das als Faustregel: ExtranetLockoutThreshold etwa halb so hoch wie die AD-Schwelle. Bei einer AD-Kontosperre nach 20 Fehlversuchen landest du also bei 10.



Skizze 3: Die ADFS-Schwelle liegt bewusst deutlich unter der AD-Kontosperrschwelle

Warum nicht einfach 19? Weil das AD auch Fehlversuche zählt, die nie über den Proxy laufen: der Kollege, der am Notebook dreimal das alte Kennwort tippt, das Smartphone mit dem hinterlegten Kennwort von letzter Woche, der geplante Task mit Anmeldedaten, die beim letzten Kennwortwechsel niemand angepasst hat. Diese Versuche landen im AD-Zähler. Liegt die ADFS-Schwelle zu knapp darunter, reichen ein paar interne Tippfehler plus ein paar externe Spray-Runden, und das AD sperrt doch. Der Abstand ist der Puffer für das echte Leben.

AD-Kontosperrschwelle	ExtranetLockoutThreshold	ExtranetObservationWindow	Einschätzung
20	10	30 Minuten	Microsoft-Empfehlung, guter Ausgangspunkt
10	5	30 Minuten	streng, funktioniert mit ESL deutlich besser als mit dem klassischen Lockout
keine AD-Sperre	10	30 Minuten	ESL schützt trotzdem; prüfe, ob das der Sicherheitsrichtlinie genügt
5	5	beliebig	falsch: AD sperrt gleichzeitig oder

			zuerst, ESL bringt kaum etwas
20	25	beliebig	falsch herum: der Angreifer sperrt das AD-Konto, bevor ADFS reagiert

Tabelle 2: Beispielwerte für Schwellen und Beobachtungsfenster

TIPP — Erst die AD-Richtlinie lesen, dann ADFS einstellen

Schau nach, welche Kontosperrrichtlinie tatsächlich gilt – in der Default Domain Policy und in eventuellen Fine-Grained Password Policies für besondere Gruppen. Ein ESL-Wert, der zur Standardrichtlinie passt, kann für die Administratorengruppe mit strengerer PSO zu hoch sein. Der niedrigste AD-Wert, der für extern genutzte Konten gilt, bestimmt deine ADFS-Schwelle.

Beobachtungsfenster und PDC-Abhängigkeit

Das Beobachtungsfenster bestimmt, wie lange Anmeldungen von unbekannten Standorten nach Erreichen der Schwelle abgewiesen werden. 30 Minuten sind ein vernünftiger Kompromiss: lang genug, um ein Spray-Werkzeug ins Leere laufen zu lassen, kurz genug, dass ein ausgesperrter Benutzer nicht den ganzen Vormittag verliert. Wer längere Fenster wählt, sollte einen schnellen Reset-Prozess für die Hotline haben – sonst wird aus Sicherheit ein Produktivitätsproblem mit Ticketnummer.

Der Parameter ExtranetLockoutRequirePDC regelt, ob ADFS für das Lockout zwingend den PDC-Emulator erreichen muss. Microsoft empfiehlt \$false: Ist der PDC nicht erreichbar, weicht ADFS auf einen anderen Domänencontroller aus, statt Anmeldungen zu verweigern. Gerade in Umgebungen mit mehreren Standorten, in denen der PDC gern mal hinter einer wackeligen WAN-Strecke steht, erspart dir das unschöne Nebenwirkungen.

```
# Aktuelle Einstellungen ansehen
Get-AdfsProperties | Select-Object EnableExtranetLockout, ExtranetLockoutThreshold,
    ExtranetObservationWindow, ExtranetLockoutRequirePDC, ExtranetLockoutMode

# Schwellen setzen (Beispiel: AD sperrt bei 20 Fehlversuchen)
Set-AdfsProperties -EnableExtranetLockout $true `
    -ExtranetLockoutThreshold 10 `
    -ExtranetObservationWindow (New-TimeSpan -Minutes 30) `
    -ExtranetLockoutRequirePDC $false
```

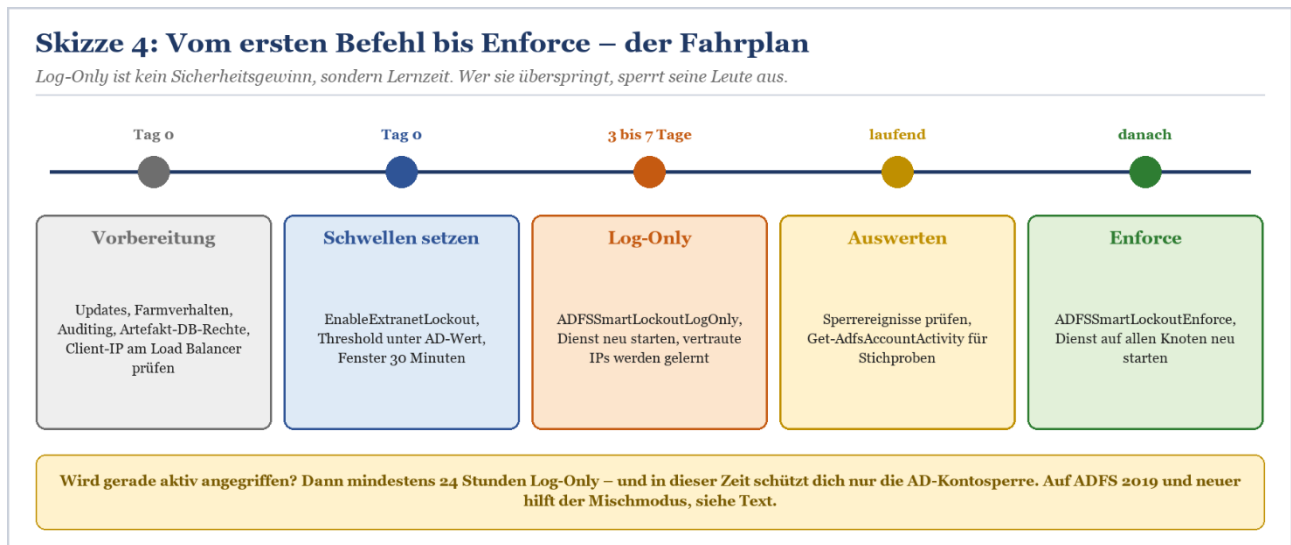
Listing 1: Schwellenwerte prüfen und setzen – auf einem beliebigen Farmknoten mit administrativen Rechten

Einführung mit Log-Only-Modus: erst lernen, dann sperren

Der häufigste Fehler bei Smart Lockout ist Ungeduld. Wer ESL direkt in den Modus Enforce schaltet, hat eine leere Tabelle AccountActivity – ADFS kennt für niemanden einen vertrauten Standort. Damit verhält sich ESL zunächst wie der alte Einheitszähler: Läuft gerade ein Angriff auf ein Konto, landen Angreifer und Benutzer auf derselben, unbekannten Seite, und der Benutzer kommt auch mit dem richtigen Kennwort nicht herein. Glückwunsch, du hast eine neue Funktion eingeführt, die exakt das alte Problem reproduziert.

Deshalb gibt es den Modus ADFS SmartLockoutLogOnly. Darin führt ADFS die Zähler, lernt die vertrauten Adressen und schreibt Überwachungsereignisse, weist aber niemanden ab. Microsoft empfiehlt drei bis sieben Tage Lernzeit. Steht die Farm gerade unter aktivem Beschuss, sind mindestens 24 Stunden Pflicht, bevor du auf Enforce gehst. Eine normale Arbeitswoche mit

Homeoffice-Tagen, Dienstreisen und Smartphones ist ein gutes Maß, weil dann die typischen Adressen der meisten Benutzer einmal vorbeigekommen sind.



Skizze 4: Fahrplan von der Vorbereitung bis zum Modus Enforce

Voraussetzungen, bevor du den ersten Schalter umlegst

Voraussetzung	Warum	Wie du es prüfst
Updates und Farmverhalten	Auf Windows Server 2016 braucht ESL die Updates ab Juni 2018 und das Farmverhalten 2016	Get-AdfsFarmInformation zeigt das aktuelle Farmverhalten; Details im Beitrag ADFS-Farm upgraden – Farm Behavior Level anheben ohne Ausfall
Sicherheitsüberwachung aktiv	ESL-Ereignisse landen im Sicherheitsprotokoll – ohne Auditing siehst du im Log-Only-Modus nichts	Einrichtung beschrieben in ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing
Windows-Remoteverwaltung	Microsoft nennt WinRM auf jedem ADFS-Server als Voraussetzung	Dienst WinRM läuft auf allen Knoten
Rechte auf der Artefakt-Datenbank	Das Dienstkonto muss die Tabelle AccountActivity anlegen dürfen	Update-AdfsArtifactDatabasePermission; bei SQL ggf. Rechte durch die DBA
Platz und Arbeitsspeicher	Die Artefakt-Datenbank wächst um bis zu 1 GB je 100.000 Benutzer	bei WID mindestens 5 GB frei unter C:\Windows\WID\Data; mehr zur Datenbank in WID oder SQL Server als ADFS-Konfigurationsdatenbank
Echte Client-IP-Adressen	Ohne sie gibt es keine sinnvollen vertrauten Standorte	siehe nächstes Kapitel – vor dem Log-Only-Modus klären

Tabelle 3: Checkliste vor der Einführung von Smart Lockout

```
# Einmalig: dem ADFS-Dienstkonto das Anlegen der Tabelle AccountActivity erlauben
$cred = Get-Credential # Konto mit ADFS-Adminrechten (bei SQL: mit Rechten auf dem SQL Server)
Update-AdfsArtifactDatabasePermission -Credential $cred

# Wer hält die Rolle "User Activity"?
(Get-AdfsFarmInformation).FarmRoles
```

Listing 2: Datenbankrechte vorbereiten und Rolleninhaber ermitteln

Log-Only einschalten, auswerten, Enforce aktivieren

Der Moduswechsel wirkt erst nach einem Neustart des ADFS-Dienstes, und zwar auf allen Knoten der Farm. Plane das als kleines Wartungsfenster und starte die Knoten nacheinander neu, damit der Load Balancer jeweils auf die verbleibenden ausweichen kann. Die Reihenfolge laut Microsoft: Modus setzen, Dienst neu starten, Lockout aktivieren.

```
# 1. Log-Only: lernen, protokollieren, nicht sperren
Set-AdfsProperties -ExtranetLockoutMode ADFSsmartLockoutLogOnly
Restart-Service adfssrv # auf JEDEM Farmknoten
Set-AdfsProperties -EnableExtranetLockout $true

# 2. Nach 3 bis 7 Tagen: Stichproben prüfen
Get-AdfsAccountActivity -UserPrincipalName max.muster@contoso.de

# 3. Scharf schalten
Set-AdfsProperties -ExtranetLockoutMode ADFSsmartLockoutEnforce
Restart-Service adfssrv # wieder auf JEDEM Farmknoten
```

Listing 3: Von Log-Only zu Enforce

Modus (ExtranetLockoutMode)	Was passiert	Wann sinnvoll
ADPasswordCounter	klassisches Extranet Lockout mit dem AD-Zähler; Standardwert	Ausgangszustand, Altfarmen ohne ESL
ADFSsmartLockoutLogOnly	ESL zählt und lernt vertraute Standorte, sperrt aber nicht	Lernphase vor Enforce
ADFSsmartLockoutEnforce	ESL sperrt unbekannte Standorte bei Erreichen der Schwelle	Dauerbetrieb
3 (nur ADFS 2019 und neuer)	ESL lernt im Log-Only-Modus, das klassische Extranet Lockout bleibt dabei aktiv	Lernphase ohne Schutzlücke

Tabelle 4: Die Modi von Extranet Lockout und Smart Lockout

WARNUNG — Auf Windows Server 2016 ist Log-Only eine Schutzlücke

Auf ADFS 2016 schaltet der Log-Only-Modus das klassische Extranet Lockout ab, falls es vorher aktiv war. Während der Lernphase schützt dich gegen Sperren von außen also nur noch die AD-Kontosperre – also genau das, was du eigentlich loswerden wolltest. Ab ADFS 2019 gibt es dafür den Mischmodus mit Set-AdfsProperties -ExtranetLockoutMode 3: Smart Lockout lernt, das alte Lockout bleibt aktiv. Auf 2016 plane die Lernphase in eine ruhige Woche und beobachte die Sperren im AD besonders aufmerksam.

Was wertest du in der Lernphase aus? Im Sicherheitsprotokoll schreibt ADFS für jeden falschen Kennwortversuch das Ereignis 1203 und für jede Sperre das Ereignis 1210 – auch im Log-Only-Modus, wo die Sperre nur protokolliert wird. Für jede gemeldete Sperre schaust du mit Get-AdfsAccountActivity nach: Kam sie von vertrauten oder unbekannten Adressen? Stehen in FamiliarIPs plausible Adressen – Firmen-NAT, Mobilfunk, Heimanschlüsse – oder verdächtig oft dieselbe interne Adresse? Letzteres ist der Moment, in dem du das nächste Kapitel liest, bevor du Enforce einschaltest.

Ereignis	Protokoll	Bedeutung
1203	Sicherheit (AD FS Auditing)	falsches Kennwort; erreicht der Zähler die Schwelle, sperrt ADFS für das Beobachtungsfenster
1210	Sicherheit (AD FS Auditing)	ein Benutzer wurde gesperrt
516	AD FS/Admin	Konto wegen zu vieler falscher Kennwörter gesperrt, mit Client-IP und Zählerstand
515	AD FS/Admin	Konto war gesperrt, aber das richtige Kennwort wurde eingegeben – möglicherweise kompromittiert
512	AD FS/Admin	Konto gesperrt, Anmeldeversuch wird aufgrund der Konfiguration trotzdem zugelassen
557, 562, 563	AD FS/Admin (ADFS 2019)	Kommunikationsprobleme mit dem Knoten, der die Kontoaktivität hält

Tabelle 5: Ereignisse rund um Smart Lockout laut Microsoft-Dokumentation

TIPP — Ereignis 515 verdient einen Alarm

Wenn ein gesperrtes Konto plötzlich mit dem richtigen Kennwort auftaucht, ist das entweder ein Benutzer, der nach fünf Tippfehlern doch noch draufgekommen ist – oder ein Angreifer, der getroffen hat. Diese Unterscheidung willst du nicht erst am nächsten Morgen treffen. Wie du aus solchen Ereignissen ein Frühwarnsystem baust, zeigt [Passwort-Spray und Brute Force auf ADFS erkennen](#).

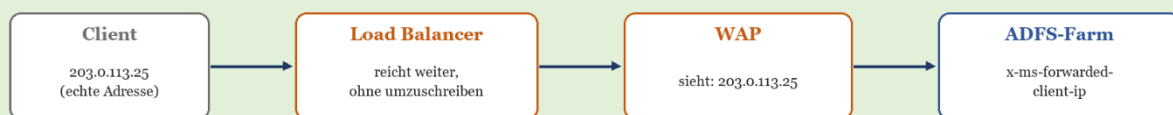
Client-IP-Weitergabe am Load Balancer: ohne echte Adressen kein Smart Lockout

Jetzt kommt der Teil, der in keiner Kurzanleitung steht und an dem trotzdem die meisten ESL-Einführungen scheitern. Smart Lockout steht und fällt mit der Frage, welche IP-Adresse ADFS für eine Anfrage sieht. Der Web Application Proxy reicht der Farm die Quelladresse weiter, die er selbst auf der TCP-Verbindung sieht – im Header x-ms-forwarded-client-ip. Steht vor den WAP-Servern ein Load Balancer, der die Quelladresse per Source-NAT durch seine eigene ersetzt, sieht der WAP für jede Anfrage dieselbe Adresse. Und reicht genau die brav an ADFS weiter.

Skizze 5: Welche IP-Adresse kommt bei ADFS an?

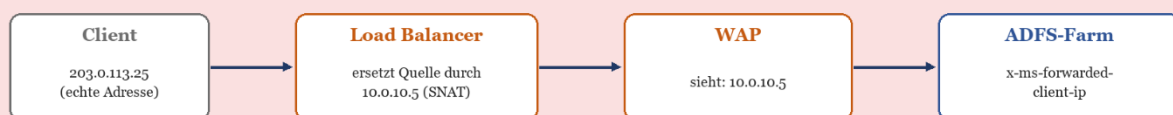
Der WAP meldet der Farm die Quelladresse, die er sieht. Ein Load Balancer mit Source-NAT schreibt sie um.

Richtig: Quelladresse bleibt erhalten (transparent oder Layer 4 ohne SNAT)



ESL sieht jeden Client einzeln. Vertraute und unbekannte Standorte funktionieren wie gedacht.

Falsch: Source-NAT ohne Weitergabe der echten Adresse



Alle Anfragen kommen scheinbar von 10.0.10.5. Nach der ersten erfolgreichen Anmeldung ist das für jeden Benutzer ein vertrauter Standort – auch wenn der Angreifer anklopft. Beide landen auf demselben Zähler.

Skizze 5: Mit und ohne erhaltene Client-IP-Adresse vor dem Web Application Proxy

Was dann passiert, ist schwarzer Humor in Reinform: Nach der ersten erfolgreichen Anmeldung steht die Adresse des Load Balancers in der FamiliarIPs-Liste des Benutzers. Ab da gilt jede Anfrage für dieses Konto als vertraut – auch die des Angreifers, der ja über denselben Load Balancer hereinkommt. Angreifer und Benutzer landen wieder auf demselben Zähler, diesmal auf dem vertrauten. Du hast Smart Lockout eingeführt, die Lernphase sauber durchgezogen, und am Ende sperrt der Angreifer deine Leute trotzdem aus. Nur mit mehr Aufwand.

Wie du die Client-IP sauber durchreichst

Variante am Load Balancer	Was beim WAP ankommt	Eignung für Smart Lockout
---------------------------	----------------------	---------------------------

Layer 4 ohne Source-NAT (transparent, Rückweg über den Load Balancer als Gateway)	echte Client-Adresse	gut – die sauberste Lösung
Layer 7 mit TLS-Terminierung und Neuverschlüsselung, Header X-Forwarded-For eingefügt	Adresse des Load Balancers plus X-Forwarded-For	brauchbar, weil ESL X-Forwarded-For mit auswertet; Header nur vom eigenen Load Balancer zulassen
Source-NAT ohne Weitergabe der Client-Adresse	Adresse des Load Balancers	ungeeignet – ESL wird wirkungslos
Kein Load Balancer, DNS-Round-Robin oder NAT der Firewall mit erhaltener Quelle	echte Client-Adresse	gut, sofern die Firewall die Quelle nicht umschreibt

Tabelle 6: Load-Balancer-Varianten vor dem Web Application Proxy und ihre Wirkung auf ESL

Welche Variante bei dir greift, findest du am schnellsten im Sicherheitsprotokoll eines ADFS-Knotens heraus: Öffne ein beliebiges Ereignis 1203 oder 1200 einer externen Anmeldung und schau ins Feld IpAddress. Stehen dort öffentliche Adressen, die zu deinen Benutzern passen, ist alles gut. Steht dort immer wieder dieselbe Adresse aus deiner DMZ, hat der Load Balancer zugeschlagen. Diese Prüfung gehört vor den Log-Only-Modus, nicht danach – sonst lernt ADFS eine Woche lang die falschen Adressen.

WARNUNG – X-Forwarded-For ist kein Ausweis

Den Header X-Forwarded-For kann jeder Client selbst mitschicken. Wenn dein Load Balancer einen vom Client mitgebrachten Header ungeprüft durchreicht, kann ein Angreifer sich theoretisch eine Adresse dazudichten. Da ESL eine Anfrage nur dann als vertraut wertet, wenn ALLE Adressen bekannt sind, verschafft ihm das allein keinen Vorteil – trotzdem gehört es zur Hygiene, eingehende X-Forwarded-For-Header zu verwerfen und nur den selbst erzeugten weiterzureichen.

Wie Persistenz, Health Probes und SNI für ADFS und WAP grundsätzlich eingerichtet werden, steht im Beitrag [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#). Wer einen Kemp LoadMaster einsetzt, findet die passenden Einstellungen für transparente virtuelle Services und das Einfügen von Headern auf der Seite [Kemp LoadMaster](#). Die Architektur des Proxys selbst – und was nach dem WAP kommt – beschreibt [Web Application Proxy: Architektur und Ablöse](#).

FAKTEN – Exchange Online und die Microsoft-Adressen im Protokoll

Laufen bei dir noch Legacy-Anmeldungen über Exchange Online gegen ADFS, siehst du im Protokoll Microsoft-Adressen statt der Client-Adresse. Laut Microsoft steht die Adresse des eigentlichen Absenders dann in x-ms-forwarded-client-ip, die Adresse des Exchange-Servers in x-ms-client-ip. ESL wertet beide aus – deshalb lässt sich auch ein über Exchange Online geführtes Spray auf die unbekannte Seite sperren. Solche Anfragen erkennst du an der Activity ID 00000000-0000-0000-0000-000000000000.

Gespernte Konten zurücksetzen und den Betrieb regeln

Irgendwann ruft jemand an, der wirklich gesperrt ist. Mit Smart Lockout ist das seltener, aber nicht unmöglich: der neue Mitarbeiter, der sich noch nie extern angemeldet hat und sein Kennwort im Hotel zehnmals falsch tippt; die Kollegin, deren Kennwort tatsächlich gestohlen wurde; der Benutzer, der in der Lernphase nicht da war. Für diese Fälle bringt das ADFS-Modul drei Cmdlets mit, die sich automatisch mit dem Knoten verbinden, der die Rolle „User Activity“ hält. Mit -Server lässt sich ein anderer Knoten angeben.

Cmdlet	Zweck	Typischer Einsatz
Get-AdfsAccountActivity	zeigt Zähler, letzte Fehlversuche, Sperrstatus und vertraute IP-Adressen	erste Diagnose am Telefon

Reset-AdfsAccountLockout	setzt den Zähler für vertraute (-Location Familiar) oder unbekannte (-Location Unknown) Standorte zurück	Benutzer ist nachweislich der Richtige
Set-AdfsAccountActivity	fügt mit -AdditionalFamiliarIps zusätzliche vertraute Adressen hinzu	neuer Standort, neue Außenstelle

Tabelle 7: Die drei Cmdlets für die Kontoaktivität

```
# Zustand ansehen
Get-AdfsAccountActivity -UserPrincipalName max.muster@contoso.de |
    Select-Object BadPwdCountFamiliar, BadPwdCountUnknown,
        LastFailedAuthFamiliar, LastFailedAuthUnknown,
        FamiliarLockout, UnknownLockout, FamiliarIps

# Sperre für unbekannte Standorte aufheben
Reset-AdfsAccountLockout -UserPrincipalName max.muster@contoso.de -Location Unknown

# Sperre für vertraute Standorte aufheben (Verdacht: Angreifer nutzt bekannte Adresse)
Reset-AdfsAccountLockout -UserPrincipalName max.muster@contoso.de -Location Familiar

# Neue Außenstelle als vertrauten Standort hinterlegen (Dokumentationsadresse als Beispiel)
Set-AdfsAccountActivity -UserPrincipalName max.muster@contoso.de -AdditionalFamiliarIps
"198.51.100.17"
```

Listing 4: Diagnose und Reset eines gesperrten Kontos

Zwei Sperren, zwei Schlüssel

Ein Reset in ADFS hebt nur die ADFS-Sperre auf. War das Konto zusätzlich im AD gesperrt – etwa weil die Schwellen falsch herum standen oder weil intern falsch getippt wurde –, musst du es dort wie gewohnt entsperren, über „Active Directory-Benutzer und -Computer“ oder das Werkzeug, das deine Hotline ohnehin nutzt. Umgekehrt gilt dasselbe: Wer nur im AD entsperrt, wundert sich, dass der Benutzer von außen weiterhin abgewiesen wird. Halte im Hotline-Leitfaden fest, dass beide Stellen geprüft werden.

Symptom	Wahrscheinliche Ursache	Was du tust
Nur extern gesperrt, intern geht alles	ESL-Sperre, meist UnknownLockout	Get-AdfsAccountActivity, dann Reset-AdfsAccountLockout -Location Unknown
Auch von bekannten Adressen gesperrt	FamiliarLockout – jemand tippt von einer vertrauten Adresse falsch	Kennwort zurücksetzen lassen, Gerät mit altem Kennwort suchen, dann Reset Familiar
Intern und extern gesperrt	AD-Kontosperre	im AD entsperren, Schwellenverhältnis prüfen
Alle Benutzer haben dieselbe vertraute IP	Source-NAT am Load Balancer	Client-IP-Weitergabe korrigieren, dann Lernphase wiederholen
Benutzer kommt trotz Sperre mit richtigem Kennwort durch	Ereignis 515: möglicher Treffer	Konto prüfen, Kennwort ändern, MFA erzwingen – siehe ADFS mit Entra-MFA koppeln – Adapter, Zertifikat und Fallstricke

Tabelle 8: Typische Sperrbilder und was dahintersteckt

TIPP – Den Reset an die Hotline delegieren – aber eng

Microsoft beschreibt, wie sich die ESL-Cmdlets per Just Enough Administration (JEA) an die Hotline delegieren lassen, ohne dass dort jemand ADFS-Adminrechte bekommt. Gib der Hotline Get-AdfsAccountActivity und Reset-AdfsAccountLockout, aber nicht Set-AdfsAccountActivity: Wer vertraute Adressen hinzufügen darf, kann im Zweifel einem Angreifer die Tür aufhalten.

Wenn das Kennwort schon weg ist

Steht fest, dass ein Angreifer das Kennwort kennt, reicht ein Zähler-Reset nicht. Seine Adresse steht nach der erfolgreichen Anmeldung in den vertrauten Standorten des Kontos. Microsoft empfiehlt in diesem Fall, die Kontoaktivität in ADFS zu bereinigen und mehrstufige Authentifizierung zu verlangen; dazu kommt natürlich der Kennwortwechsel. Für die Kennwortqualität insgesamt nennt Microsoft Entra Password Protection, das erratbare Kennwörter wie „Sommer2026!“ gar nicht erst zulässt. Die größere Einordnung – Angriffswege, Härtung der Farm, Golden SAML und MFA – findest du im Beitrag [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#); das wiederholen wir hier bewusst nicht.

Betrieb auf Dauer

- Rolleninhaber im Blick behalten: Fällt in einer WID-Farm der primäre Knoten aus, schreiben die sekundären Knoten Fehler ins Admin-Log, verarbeiten Anmeldungen aber weiter und speichern den Stand nur lokal. Alle zehn Minuten versuchen sie es erneut.
- Speicher planen: Microsoft rechnet mit bis zu 1 GB Datenbankwachstum je 100.000 Benutzer und bis zu 1 GB zusätzlichem Arbeitsspeicher bei bis zu 500.000 Benutzern.
- Überwachung einrichten: Microsoft nennt Entra Connect Health als bevorzugten Weg, Risky IPs und Fehlversuche auszuwerten. Was das Werkzeug kann und wie du es mit eigenen Prüfungen ergänzt, steht in [ADFS überwachen – Health Checks, Diagnose-Toolbox und Entra Connect Health](#).
- Nach jeder Änderung am Load Balancer oder an der Firewall vor den WAP-Servern: Feld IpAddress in einem aktuellen Ereignis prüfen.
- Wenn eine Anmeldung trotz allem rätselhaft scheitert: [ADFS-Anmeldung schlägt fehl – die häufigsten Ursachen und ihre Lösung](#) hilft beim Eingrenzen.

FAKTEN – Und wenn du ohnehin Richtung Entra ID gehst?

Solange eine Domäne in Microsoft 365 föderiert ist, prüft ADFS das Kennwort – und damit auch Smart Lockout. Stellst du auf verwaltete Authentifizierung um, übernimmt Entra ID mit seiner eigenen Smart-Lockout-Logik. Bis dahin lohnt sich ESL trotzdem, denn so eine Umstellung dauert erfahrungsgemäß länger als die nächste Spray-Welle. Wie der Wechsel gelingt, beschreibt [Microsoft 365 von Federated auf Managed umstellen – mit Staged Rollout](#).

Fazit: Den Angreifer aussperren, nicht die eigene Mannschaft

Das klassische Extranet Lockout war ein Fortschritt, aber ein grobschlächtiger: ein Zähler für alle, und wenn er voll ist, bleibt draußen, wer draußen ist. Smart Lockout macht daraus zwei Zähler und eine Liste vertrauter Adressen – und damit das, was man eigentlich von Anfang an wollte: Der Angreifer läuft gegen eine geschlossene Tür, deine Leute gehen durch die offene. Damit das klappt, braucht es vier Dinge. Eine ADFS-Schwelle deutlich unter der AD-Schwelle, die Microsoft-Empfehlung mit der Hälfte ist ein guter Start. Eine Lernphase im Log-Only-Modus, drei bis sieben Tage, auf Windows Server 2019 und neuer im Mischmodus ohne Schutzlücke. Echte Client-Adressen am Web Application Proxy, also kein Source-NAT am Load Balancer ohne Weitergabe. Und einen eingeübten Reset-Prozess, der ADFS und AD gleichermaßen im Blick hat.

Das ist kein Hexenwerk, aber auch nichts, was man nebenbei zwischen zwei Tickets einschaltet. Eine Farm, die seit Jahren zuverlässig läuft, verdient diese Sorgfalt – ob sie noch lange bleibt oder der Umstieg auf Entra ID schon geplant ist. Wenn du Smart Lockout mit Unterstützung einführen

oder deinen Load Balancer prüfen lassen willst, findest du uns im [Consulting zu ADFS \(Active Directory Federation Services\)](#). Wer Spray-Angriffe und Sperren lieber im Labor durchspielt als am Montagmorgen in der Produktion, ist in den [ADFS-Schulungen](#) richtig. Schutzmechanismen und Betrieb der Farm vertieft außerdem das Buch – mehr dazu unter [ADFS in der Praxis – das Buch im Detail](#).

WEITER — Passende Beiträge zum Schutz der Farm

- › [Passwort-Spray und Brute Force auf ADFS erkennen](#) – Angriffe in den Protokollen erkennen, bevor die Hotline klingelt
- › [ADFS-Sicherheit: Angriffe, Härtung, Golden SAML und MFA](#) – das große Bild: Angriffe, Härtung, Golden SAML und MFA
- › [ADFS hinter dem Load Balancer – Health Probe, SNI und Persistenz](#) – damit die Client-IP am WAP ankommt
- › [ADFS-Ereignisprotokolle lesen – Admin-Log, Debug-Tracing und Auditing](#) – Auditing einschalten, damit ESL überhaupt etwas protokolliert

FAQ: ADFS Extranet Smart Lockout

Was ist der Unterschied zwischen Extranet Lockout und Extranet Smart Lockout?

Das klassische Extranet Lockout nutzt den Fehlversuchszähler im AD und sperrt bei Erreichen der Schwelle alle externen Anmeldungen des Kontos. Smart Lockout führt in der Artefakt-Datenbank je Benutzer zwei Zähler, für vertraute und unbekannte Standorte, und sperrt nur die Seite, auf der die Fehlversuche passieren.

Ab welcher ADFS-Version gibt es Smart Lockout?

Für ADFS auf Windows Server 2016 mit den Updates ab Juni 2018 und Farmverhalten 2016. Ab Windows Server 2019 ist Smart Lockout eingebaut und um getrennte Schwellen für vertraute und unbekannte Standorte sowie den Mischmodus erweitert.

Welchen Wert sollte ExtranetLockoutThreshold haben?

Deutlich weniger als die AD-Kontosperrschwelle. Microsoft empfiehlt etwa die Hälfte, also 10 bei einer AD-Schwelle von 20, und ein Beobachtungsfenster von 30 Minuten.

Wie lange sollte der Log-Only-Modus laufen?

Laut Microsoft drei bis sieben Tage. Wird die Farm gerade aktiv angegriffen, mindestens 24 Stunden, damit ADFS die vertrauten Standorte der Benutzer gelernt hat, bevor du auf Enforce schaltest.

Muss ich den ADFS-Dienst nach dem Moduswechsel neu starten?

Ja. Der neue Wert von ExtranetLockoutMode wirkt erst nach Restart-Service adfssrv, und zwar auf allen Knoten der Farm.

Wie entsperre ich einen Benutzer in ADFS?

Mit `Reset-AdfsAccountLockout` und dem Parameter `-Location Unknown` oder `-Location Familiar`. Den aktuellen Zustand zeigt vorher `Get-AdfsAccountActivity`. Eine zusätzliche Sperre im AD musst du dort separat aufheben.

Wie viele vertraute IP-Adressen merkt sich ADFS pro Benutzer?

Höchstens 20. Kommt eine weitere hinzu, entfernt ADFS die älteste aus der Liste.

Warum haben alle Benutzer dieselbe vertraute IP-Adresse?

Weil ein Load Balancer vor dem Web Application Proxy die Quelladresse per Source-NAT ersetzt. Dann sieht ADFS für jede Anfrage dieselbe Adresse, und Smart Lockout kann Angreifer und Benutzer nicht mehr unterscheiden. Abhilfe schafft ein transparenter Betrieb oder das Einfügen von X-Forwarded-For.

Schützt Smart Lockout auch Anmeldungen im internen Netz?

Nein. ESL wirkt nur auf Anmeldungen mit Benutzername und Kennwort, die über den Web Application Proxy oder einen MS-ADFSPiP-fähigen Proxy kommen. Intern gilt nur die AD-Kontosperre.

Verhindert Smart Lockout, dass ein Angreifer ein Kennwort errät?

Nein. Es bremst Passwort-Spray aus und verhindert, dass Angreifer deine Benutzer aussperren. Ein richtig erratenes Kennwort ist für ESL eine erfolgreiche Anmeldung. Dagegen helfen MFA und Regeln gegen schwache Kennwörter.