

MFA vor OWA, ECP und Co.: Zwei-Faktor am LoadMaster

Der Türsteher will jetzt zwei Ausweise sehen

Kennwort allein reicht nicht mehr. Die Frage ist nur, wer den zweiten Faktor prüft und wer an der Tür vorbeischiebt.



MFA für Browser ist einfach. MFA für alles andere ist Architektur.

Skizze: Ausgangslage, Beispieldomäne contoso.de

WISSEN

Alles zum Kemp LoadMaster mit Microsoft-Brille: Exchange, SharePoint, ADFS, RDS und Kerberos an einem Ort.

› [Kemp LoadMaster](#)

BERATUNG

MFA vor Exchange und Co., ohne dass am Montag alle Smartphones offline sind? Wir planen die Aufteilung der Pfade mit dir.

› [Beratung zum Kemp LoadMaster](#)

SCHULUNG

RADIUS, NPS-Erweiterung und SAML im Labor durchspielen, inklusive Timeout-Drama und Challenge-Formular.

› [Kemp-LoadMaster-Schulung](#)

Irgendwann kommt die Mail. Mal von der Versicherung, mal vom Datenschutz, mal vom neuen Sicherheitsbeauftragten, der frisch von einer Konferenz zurück ist: „Wir brauchen MFA für alles, was von außen erreichbar ist. Bis Quartalsende.“ Und dann schaust du auf dein OWA, das seit Jahren mit Benutzername und Kennwort im Internet steht, auf das ECP, das da eigentlich gar nicht stehen sollte, und auf die Handvoll ActiveSync-Geräte, von denen niemand so genau weiß, wem sie gehören. Zwischen all dem und dem Internet steht ein LoadMaster. Naheliegende Idee: Der soll das jetzt regeln.

Die gute Nachricht: Er kann. Das Edge Security Pack bringt Vorauthentifizierung mit, und die lässt sich mit einem zweiten Faktor kombinieren, per RADIUS, per RSA SecurID oder per Umleitung zu Entra ID über SAML oder OIDC. Die schlechte Nachricht: MFA am LoadMaster funktioniert nur dort, wo ein Mensch vor einem Browser sitzt, der ein Formular anzeigen kann. Outlook, ActiveSync und Autodiscover gehören nicht dazu. Wer das ignoriert, baut sich eine sehr sichere Tür, durch die niemand mehr kommt, oder eine sehr sichere Haustür neben einem offenen Kellerfenster.

Dieser Beitrag sortiert die drei Wege, zeigt, wo jeder von ihnen in der Praxis knallt, und erklärt, was du mit den Protokollen machst, die keine Formularanmeldung können. Er gehört zur Serie rund um den [Kemp LoadMaster](#) und setzt voraus, dass du weißt, was ein Virtual Service, ein SubVS und eine SSO-Domäne ist. Falls nicht: Die Grundlagen der Vorauthentifizierung stehen im Beitrag [Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz](#).

FAKTEN • Das Wichtigste in fünf Sätzen

MFA am LoadMaster ist eine Funktion des Edge Security Packs und hängt an der Client-

Authentifizierung des Virtual Service beziehungsweise SubVS.

Für Formularanmeldung mit zweitem Faktor stehen RADIUS (etwa gegen NPS mit der Entra-MFA-Erweiterung) und RSA SecurID zur Verfügung, jeweils optional kombiniert mit LDAP für Gruppenprüfungen.

SAML oder OIDC gegen Entra ID verlagert Anmeldung und MFA zu Microsoft und bringt Bedingten Zugriff, Gerätestatus und Anmeldeprotokolle mit.

ActiveSync, MAPI über HTTP, Outlook Anywhere, EWS, Autodiscover und OAB können kein Formular. Sie brauchen eigene SubVS ohne ESP-Formular oder Hybrid Modern Authentication.

Der eigentliche Aufwand liegt nicht im Häkchen, sondern in der Aufteilung der Pfade und in den Timeouts.

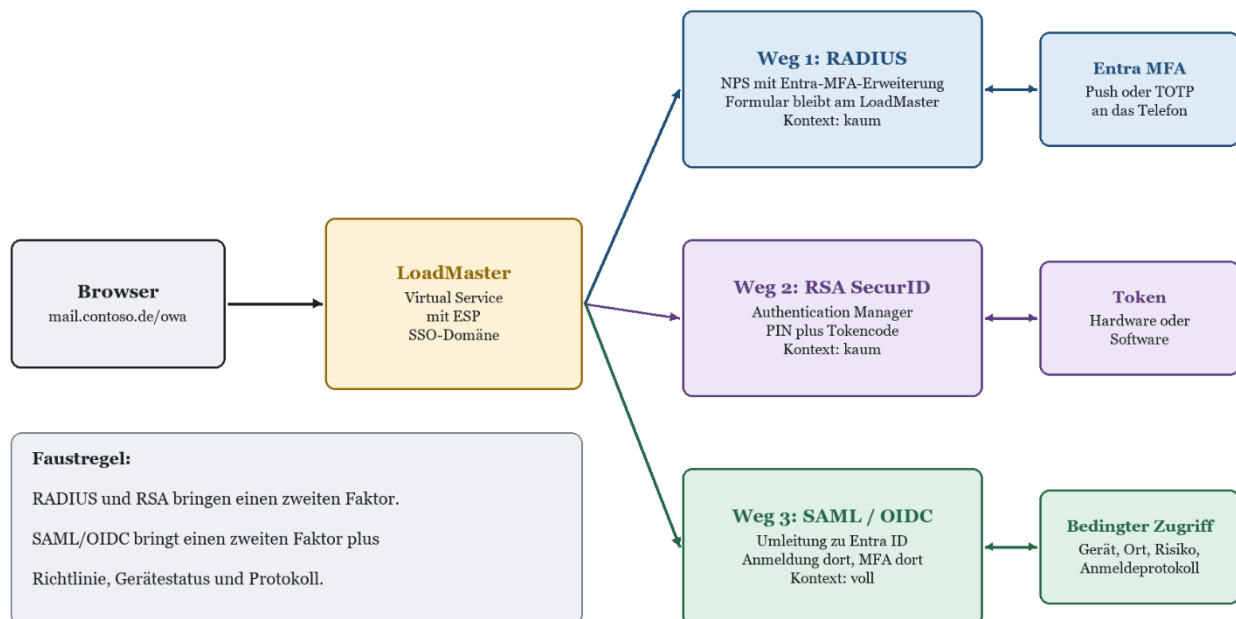
Was „MFA am LoadMaster“ eigentlich bedeutet

Bevor du irgendetwas konfigurierst, lohnt ein Blick auf die Arbeitsteilung. Ohne ESP reicht der LoadMaster die Anfrage einfach an Exchange durch, und Exchange entscheidet, wer hereinkommt. Mit ESP schiebt sich der LoadMaster davor: Er fängt unangemeldete Anfragen ab, zeigt ein eigenes Anmeldeformular oder leitet zu einem Identitätsanbieter um, prüft die Anmeldung gegen eine SSO-Domäne und reicht erst dann die Anfrage weiter, entweder mit den Anmeldedaten im Gepäck oder mit einem Kerberos-Ticket, das er sich per KCD stellvertretend besorgt hat.

Der zweite Faktor hängt an genau dieser Vorab-Prüfung. Der LoadMaster selbst erzeugt keine Einmalcodes und verschickt keine Push-Nachrichten. Er fragt jemanden, der das kann: einen RADIUS-Server, einen RSA Authentication Manager oder einen Identitätsanbieter wie Entra ID. Das ist kein Mangel, sondern Absicht. Ein Load Balancer soll Verkehr verteilen und Türen bewachen, nicht nebenbei ein Identitätssystem betreiben.

Drei Wege zum zweiten Faktor

Wer prüft die Identität, und wer kennt den Kontext der Anmeldung?



Skizze: vereinfachte Übersicht, Optionsnamen sinngemäß

Formular gegen Umleitung: der eigentliche Unterschied

RADIUS und RSA SecurID arbeiten mit dem Anmeldeformular des LoadMasters. Der Benutzer tippt Benutzername und Kennwort, gegebenenfalls einen Tokencode, und der LoadMaster reicht das an das Backend weiter. Für den Benutzer sieht das aus wie früher am TMG oder UAG, nur mit einem zusätzlichen Feld oder einer Push-Nachricht.

SAML und OIDC arbeiten anders: Der LoadMaster zeigt gar kein Formular, sondern schickt den Browser zu Entra ID. Dort passiert die Anmeldung, dort greift MFA, dort wertet der Bedingte Zugriff Gerät, Standort und Risiko aus, und dort landet der Eintrag im Anmeldeprotokoll. Zurück kommt eine signierte Assertion oder ein Token, das der LoadMaster prüft. Wie das im Detail funktioniert, steht im Beitrag [SAML, OIDC und Entra ID: der LoadMaster als moderner Identitätsvermittler](#).

Merkmal	RADIUS / NPS-Erweiterung	RSA SecurID	SAML / OIDC gegen Entra ID
Wo wird angemeldet?	Formular am LoadMaster	Formular am LoadMaster	Anmeldeseite von Entra ID
Zweiter Faktor	Entra MFA (Push, Anruf, TOTP)	RSA-Token (PIN plus Code)	alle Entra-Methoden inklusive FIDO2 und Passkeys
Bedingter Zugriff	kaum, Entra sieht die NPS-Adresse	nein	voll, inklusive Gerätestatus
Phishing-Resistenz	gering	gering bis mittel	hoch mit FIDO2 oder Passkeys
Anmeldeprotokoll	NPS-Log plus Entra-Protokoll	RSA-Protokoll	Entra-Anmeldeprotokoll
Voraussetzung	Benutzer synchronisiert, Entra ID P1	RSA Authentication Manager	Benutzer synchronisiert, Entra ID P1 für Bedingten Zugriff
Server-Seite	Basic-Weitergabe oder KCD	KCD (Kennwort fehlt meist)	KCD

WICHTIG · Der Server darf nicht selbst noch einmal fragen

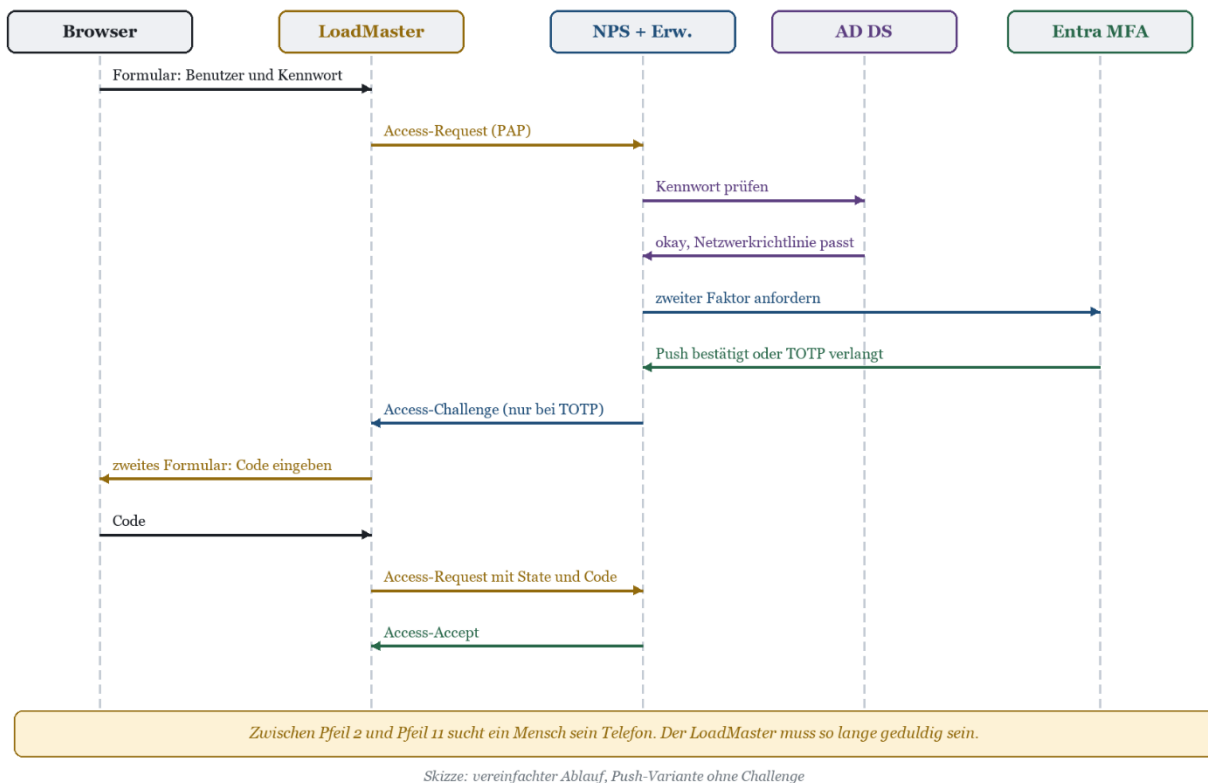
Wenn der LoadMaster per ESP vorauthentifiziert, muss das virtuelle Verzeichnis dahinter zur Server-Seite passen. Für OWA und ECP heißt das in der Regel: keine formularbasierte Authentifizierung auf Exchange, sondern Basic oder integrierte Windows-Authentifizierung, je nachdem, ob der LoadMaster Anmeldedaten weiterreicht oder per KCD ein Ticket holt. Sonst meldet sich der Benutzer zweimal an und hält das Ganze für ein besonders gründliches Sicherheitskonzept.

Weg 1: RADIUS gegen NPS mit der Entra-MFA-Erweiterung

Das ist der Weg, den die meisten Microsoft-Umgebungen zuerst ausprobieren, weil alle Bausteine schon im Haus sind. Der Netzwerkrichtlinienserver (NPS) ist eine Windows-Server-Rolle, die NPS-Erweiterung für Microsoft Entra MFA ist ein kostenloser Download von Microsoft, und die Benutzer haben die Authenticator-App ohnehin schon für Microsoft 365 auf dem Telefon. Der LoadMaster wird im NPS als RADIUS-Client eingetragen, im LoadMaster legst du eine SSO-Domäne mit RADIUS als Authentifizierungsprotokoll an, fertig. Theoretisch.

RADIUS mit NPS-Erweiterung: wer wartet auf wen?

Jede Pfeilspitze ist ein Timeout, das du kennen solltest



So läuft eine Anmeldung ab

Der LoadMaster schickt Benutzername und Kennwort als Access-Request an den NPS. Der NPS prüft das Kennwort gegen das Active Directory und gibt die Anfrage danach an die Erweiterung weiter. Die fordert bei Entra ID den zweiten Faktor an, identifiziert den Benutzer dabei standardmäßig über den lokalen UPN und wartet. Bestätigt der Benutzer die Push-Nachricht, antwortet der NPS mit Access-Accept, und der LoadMaster lässt die Anfrage durch.

Interessant wird es bei Einmalcodes. Microsoft beschreibt, dass NPS keine Nummernabgleich-Anzeige beherrscht. Seit der Erweiterungsversion 1.2.2216.1 werden Benutzer, die eine TOTP-Methode registriert haben, deshalb nach einem Code gefragt, statt nur „Genehmigen“ oder „Ablehnen“ zu tippen. Technisch ist das ein Access-Challenge: Der NPS antwortet nicht mit Ja oder Nein, sondern mit „gib mir noch etwas“. Der LoadMaster beherrscht RADIUS Challenge/Response, zeigt dann ein zweites Formular für den Code und schickt ihn zusammen mit dem State-Attribut in einem zweiten Access-Request hinterher. Wer keine TOTP-Methode registriert hat, bekommt weiterhin die schlichte Push-Abfrage, ohne Nummer und damit anfällig für MFA-Müdigkeit: Wer nachts um drei zum zwölften Mal auf „Genehmigen“ tippt, damit das Telefon endlich Ruhe gibt, hat den Angreifer gerade eigenhändig hereingelassen.

PAP ist hier kein Relikt, sondern Pflicht

Welche MFA-Methoden funktionieren, hängt am Kennwortverfahren zwischen RADIUS-Client und NPS. Laut Microsoft unterstützt nur PAP alle Methoden, also Anruf, SMS, Push-Benachrichtigung, OATH-Hardwaretoken und Code aus der App. CHAPv2 und EAP können nur Anruf und Push. Wenn deine Benutzer Codes eintippen sollen, muss die Netzwerkrichtlinie im NPS für den LoadMaster also PAP erlauben. Das fühlt sich für jeden, der RADIUS aus der WLAN-Ecke kennt, falsch an, ist hier aber richtig.

WARNUNG · PAP heißt: Die Strecke muss vertrauenswürdig sein

Bei PAP schützt nur das Shared Secret das Kennwort auf dem Weg zum NPS, und RADIUS über UDP ist kryptografisch keine Glanzleistung. Seit der als Blast-RADIUS bekannt gewordenen Schwachstelle von 2024 gilt erst recht: Die Strecke zwischen LoadMaster und NPS gehört in ein internes, gefiltertes Netz, das Shared Secret ist lang und zufällig, und du prüfst, ob beide Seiten das Message-Authenticator-Attribut verwenden. RADIUS quer durch ein Netz zu schicken, in dem auch Gäste sitzen, ist keine Zwei-Faktor-Architektur, sondern eine Einladung.

Timeouts: das eigentliche Minenfeld

RADIUS läuft über UDP, und UDP kennt keine Geduld. Schickt der NPS nicht schnell genug eine Antwort, wiederholt der Client die Anfrage. Der NPS erkennt die Wiederholung und verwirft sie, solange die Erweiterung noch auf den Benutzer wartet. Das ist gewollt, damit niemand fünf Push-Nachrichten für eine Anmeldung bekommt, füllt aber das Ereignisprotokoll mit verworfenen Anfragen. Microsoft empfiehlt für RADIUS-Clients vor der NPS-Erweiterung einen Timeout von mindestens 60 Sekunden, bei Bedarf 90 oder 120 Sekunden.

Am LoadMaster gibt es zusätzlich den L7 Client Token Timeout. Er legt fest, wie lange der LoadMaster während einer laufenden Anmeldung auf den Token des Clients wartet, und gilt für RSA SecurID und RADIUS. Der Wert liegt zwischen 60 und 300 Sekunden, Standard sind 120 Sekunden. Diese Wartezeit muss zur Realität passen: Ein Mensch, der sein Telefon erst in der Jackentasche im Nebenraum suchen muss, braucht mehr als 30 Sekunden. Ein Angreifer, der auf einen versehentlichen Klick hofft, freut sich über jede Sekunde mehr. Irgendwo dazwischen liegt dein Wert.

Stellschraube	Wo	Empfehlung	Was passiert, wenn falsch
RADIUS-Timeout	RADIUS-Client-Seite (LoadMaster)	mindestens 60 s	Wiederholungen, doppelte Prompts, Abbruch vor der Bestätigung
L7 Client Token Timeout	LoadMaster, L7-Konfiguration	Standard 120 s, Bereich 60 bis 300 s	Codeformular läuft ab, während der Benutzer tippt
Netzwerkrichtlinie	NPS	PAP für den LoadMaster-Client erlauben	nur Push und Anruf möglich, Codes scheitern
REQUIRE_USER_MATCH	NPS, Registrierung	in Produktion nicht auf FALSE	Benutzer ohne MFA-Registrierung kommen ohne zweiten Faktor durch
Zertifikat der Erweiterung	NPS, Computerzertifikatspeicher	Ablauf überwachen (zwei Jahre)	alle Anmeldungen scheitern mit Token-Fehlern

Was du über die Erweiterung wissen musst

- **Alles oder nichts pro NPS:** Ist die Erweiterung installiert, verlangt dieser NPS für jeden RADIUS-Client MFA. Wenn derselbe NPS auch WLAN oder Switches authentifiziert, brauchst du einen eigenen NPS für den LoadMaster.
- **Kein Proxy:** Der NPS mit Erweiterung muss die Anfrage selbst bearbeiten, er kann sie nicht an einen anderen RADIUS-Server weiterreichen.
- **Lizenz:** Die Erweiterung setzt Lizenzen für Entra MFA voraus, typischerweise über Entra ID P1 oder P2. Verbrauchsbasierte Modelle passen laut Microsoft nicht.

- **Identität:** Der Benutzer muss lokal und in Entra ID existieren und für MFA registriert sein. Cloud-only-Konten und Gäste fallen hier heraus.
- **Kein Kennwortwechsel:** Abgelaufene Kennwörter lassen sich auf diesem Weg nicht ändern, und auch die Kennwortänderung im ESP funktioniert mit RADIUS laut Kemp nicht.
- **Gruppen:** Zugelassene Gruppen prüft der LoadMaster nur über LDAP. Wer das braucht, kombiniert RADIUS mit LDAP in der SSO-Domäne.

FAKTEN · MFA Server ist Geschichte

Der alte lokale Azure MFA Server, der in vielen Umgebungen als RADIUS-Ziel für Load Balancer diente, bearbeitet seit dem 30. September 2024 keine MFA-Anfragen mehr. Wer noch eine RADIUS-Konfiguration auf ihn zeigen hat, hat entweder schon gemerkt, dass nichts mehr geht, oder eine sehr ungewöhnliche Ausnahmeregel. Beides lohnt einen Blick. Der Nachfolger für RADIUS ist die NPS-Erweiterung, eine Migration von Benutzereinstellungen gibt es nicht: Die Benutzer registrieren sich in Entra ID neu.

AUS DER PRAXIS · Die Push-Nachricht, die nie ankam

Ein typischer Fall: Ein mittelständisches Unternehmen stellt OWA auf RADIUS gegen NPS mit Erweiterung um. Im Test klappt alles, in Produktion beschwerten sich am ersten Morgen Dutzende Benutzer über doppelte Push-Nachrichten und abgebrochene Anmeldungen. Ursache: Der RADIUS-Timeout auf der Client-Seite stand noch auf wenigen Sekunden, ein Überbleibsel aus der Zeit, als RADIUS nur Kennwörter prüfte. Nach der Anhebung auf 60 Sekunden war Ruhe. Die verworfenen Anfragen im NPS-Protokoll waren übrigens kein Fehler, sondern das Symptom.

Weg 2: RSA SecurID am LoadMaster

RSA SecurID ist der Klassiker aus der Zeit, als Zwei-Faktor noch ein Schlüsselanhänger mit sechs Ziffern war. In Verwaltungen und regulierten Branchen lebt er bis heute, oft weil der Authentication Manager ohnehin für VPN und Administratorzugänge betrieben wird. Der LoadMaster unterstützt RSA SecurID im ESP nativ: Er wird im Authentication Manager als Authentication Agent registriert, du erzeugst dort die Agent-Konfiguration und eine Node-Secret-Datei und lädst sie auf den LoadMaster. Der Benutzer gibt im Formular dann seine PIN und den aktuellen Tokencode als ein zusammengesetztes Kennwort ein.

Next Token, New PIN und andere Überraschungen

RSA kennt zwei Challenge-Response-Fälle, die der LoadMaster abbildet: Next Token, wenn der Authentication Manager einen zweiten Code sehen will, etwa nach mehreren Fehlversuchen, und New PIN, wenn der Benutzer eine neue PIN festlegen muss. Beides läuft über ein Folgeformular und damit wieder über den L7 Client Token Timeout. Standardmäßig hat der Benutzer drei Versuche, der Wert ist einstellbar.

Und das Kennwort für den Server?

Hier liegt der Haken, den viele erst beim Testen bemerken. Wer nur PIN und Tokencode eingibt, hat dem LoadMaster kein Windows-Kennwort verraten. Basic-Weitergabe an Exchange scheidet damit aus. Entweder du kombinierst RSA SecurID mit LDAP, damit der Benutzer zusätzlich sein AD-Kennwort eingibt, oder du setzt auf der Server-Seite auf Kerberos Constrained Delegation. Letzteres ist sauberer, aber eine eigene Baustelle mit SPNs, Delegationskonto und Verschlüsselungstypen. Wie das geht, beschreibt der Beitrag [Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten](#).

TIPP · RSA geht auch über RADIUS

Der RSA Authentication Manager kann auch als RADIUS-Server auftreten. Dann konfigurierst du am LoadMaster RADIUS statt RSA SecurID. Das ist praktisch, wenn mehrere Systeme dieselbe RADIUS-Schnittstelle nutzen sollen. Welche Variante du nimmst, ist weniger eine technische als eine Betriebsfrage: Wer pflegt den Agent-Eintrag, wer das Shared Secret, und wer ist am Wochenende erreichbar, wenn beides bricht?

Weg 3: SAML oder OIDC gegen Entra ID mit Bedingtem Zugriff

Aus Microsoft-Sicht ist das der Weg, den du eigentlich willst. Der LoadMaster leitet unangemeldete Browser zu Entra ID um, die Anmeldung findet dort statt, und damit gilt alles, was du in Entra ID ohnehin pflegst: dieselbe MFA-Registrierung wie für Microsoft 365, Richtlinien für Bedingten Zugriff, Anmelderrisiko, Gerätekonformität, Standortregeln und ein Anmeldeprotokoll, das dein SOC schon kennt. Phishing-resistente Methoden wie FIDO2-Schlüssel oder Passkeys funktionieren hier ebenfalls, was bei RADIUS und RSA grundsätzlich nicht geht.

Was der Bedingte Zugriff hier wirklich bringt

Der Unterschied zu RADIUS ist nicht der zweite Faktor, sondern der Kontext. Bei der NPS-Erweiterung sieht Entra ID nur, dass der NPS-Server im Rechenzentrum einen zweiten Faktor anfordert. Wo der Benutzer sitzt, mit welchem Gerät und mit welchem Browser, bleibt unsichtbar. Bei SAML oder OIDC spricht der Browser des Benutzers direkt mit Entra ID. Damit kannst du festlegen, dass OWA nur von konformen oder hybrid eingebundenen Geräten erreichbar ist, dass von außerhalb der EU blockiert wird oder dass bei erhöhtem Anmelderrisiko eine stärkere Methode nötig ist. Für das ECP ist das Gold wert: Administrative Oberflächen gehören hinter die strengste Richtlinie, die du hast.

Hinten bleibt es Kerberos

Entra ID liefert dem LoadMaster eine Identität, aber kein Windows-Kennwort. Für die Server-Seite brauchst du deshalb KCD: Der LoadMaster besorgt sich per S4U2Self und S4U2Proxy ein Kerberos-Ticket für den Benutzer und reicht es an Exchange, SharePoint oder die Eigenentwicklung weiter. Damit das klappt, muss der Wert aus der Assertion, meist der UPN, im lokalen AD genau einen Benutzer treffen. Abweichende UPN-Suffixe, Alternate Login IDs und Cloud-only-Konten sind die üblichen Verdächtigen, wenn Entra ID „ja“ sagt und der Benutzer trotzdem eine Fehlerseite sieht.

WARNUNG · Exchange, Extended Protection und der LoadMaster

Seit Microsoft Extended Protection für Exchange Server zum Standard gemacht hat, ist TLS-Offloading vor Exchange nicht mehr unterstützt, SSL Bridging dagegen schon. Plane die Re-Encryption also von Anfang an ein. Und teste jede Kombination aus ESP, KCD und Extended Protection mit deiner konkreten Firmware und deinem Exchange-Build, bevor du sie in Produktion nimmst. Kanalbindung und stellvertretende Anmeldung sind keine Freunde, die sich auf Anhieb verstehen.

Die Alternative ohne ESP: Hybrid Modern Authentication für OWA und ECP

Mit Microsoft-Brille gehört noch eine Option auf den Tisch, die den LoadMaster aus der Authentifizierung ganz heraushält. Seit dem Hotfix-Update vom April 2024 für Exchange Server 2019 CU14 unterstützt Exchange Hybrid Modern Authentication auch für OWA und ECP, und Exchange Server SE hat das übernommen. Exchange leitet dann selbst zu Entra ID um, MFA und Bedingter Zugriff greifen dort, und der LoadMaster verteilt nur noch Last. Die Voraussetzungen

sind allerdings nicht ohne: alle Benutzer nach Entra ID synchronisiert, eine klassische Hybridkonfiguration mit funktionierendem OAuth zwischen lokalem Exchange und Exchange Online, und kein TLS-Offloading, sondern höchstens SSL Bridging. Administratorkonten, die nicht synchronisiert sind, kommen dann übrigens nicht mehr ins ECP. Das merkt man gern genau dann, wenn man es dringend braucht.

Welche Variante für deine Umgebung trägt, hängt vor allem daran, ob du ohnehin hybrid unterwegs bist. Wie du Exchange am LoadMaster grundsätzlich aufbaust, also Namespaces, SubVS und Health Checks, steht im Beitrag [Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks](#).

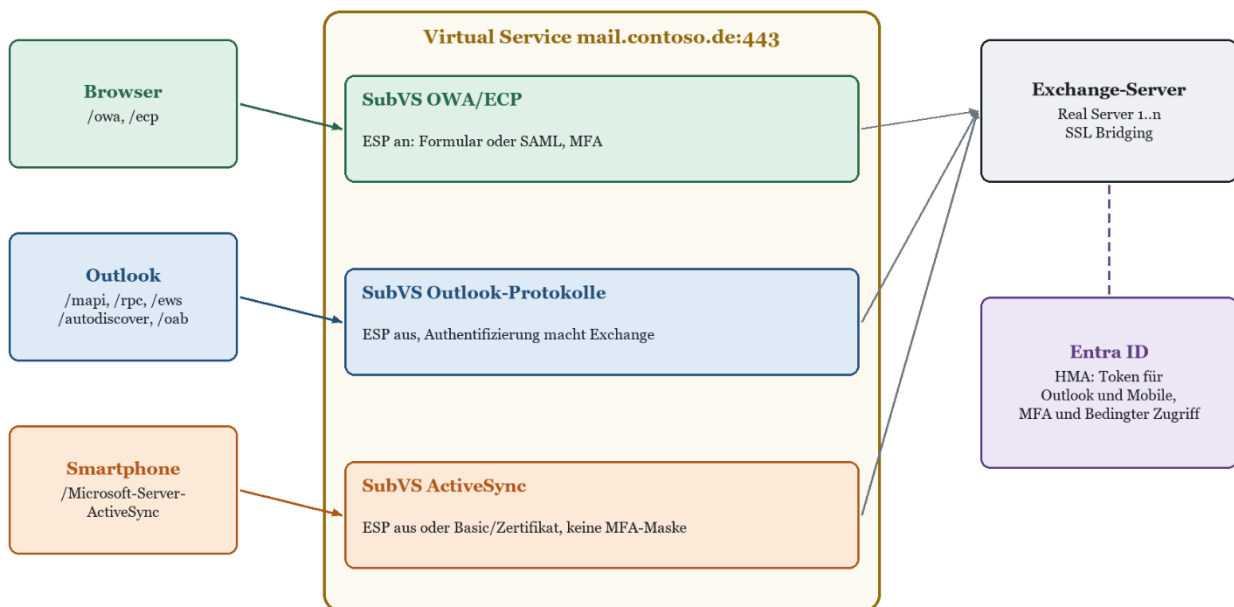
ActiveSync, Outlook und Autodiscover: die Protokolle ohne Formular

Jetzt der Teil, an dem die meisten MFA-Projekte vor Exchange ins Stolpern geraten. OWA und ECP sind Webseiten. Alles andere, was Exchange nach außen anbietet, sind Protokolle für Programme: Outlook spricht MAPI über HTTP oder, in älteren Umgebungen, Outlook Anywhere. Es holt sich seine Konfiguration per Autodiscover, lädt das Offline-Adressbuch über OAB und nutzt EWS für Frei/Gebucht-Informationen und Abwesenheitsnotizen. Smartphones mit nativer Mail-App sprechen ActiveSync. Keiner dieser Clients kann ein HTML-Formular anzeigen, ein Häkchen setzen oder einen Tokencode in ein Feld tippen, das er nicht erwartet. Er schickt Anmeldedaten im HTTP-Header und erwartet eine Antwort, kein Formular.

Legst du ESP mit Formularanmeldung über den gesamten Exchange-Namespace, passiert Folgendes: Outlook bekommt statt einer Autodiscover-Antwort ein HTML-Formular, versteht es nicht und fragt den Benutzer endlos nach dem Kennwort. ActiveSync-Geräte synchronisieren einfach nicht mehr. Und der Helpdesk lernt deinen Namen auswendig.

Ein Exchange, zwei Welten am LoadMaster

Browserpfade bekommen ESP und MFA, Protokollpfade bekommen Lastverteilung und Ruhe



Wer ESP mit Formular über alle Pfade legt, hat am Montag ein Postfach voller Tickets und kein einziges Smartphone mehr online.

Skizze: Aufteilung per SubVS nach Pfad, Namen fiktiv

Getrennte Virtual Services oder SubVS nach Pfad

Die Lösung am LoadMaster ist eine saubere Aufteilung. Entweder bekommt jeder Dienst einen eigenen Namespace und damit einen eigenen Virtual Service, oder du trennst innerhalb eines

Virtual Service per Content Rule nach Pfad und leitet auf SubVS mit unterschiedlicher Client-Authentifizierung. Die Exchange-Vorlagen von Kemp bringen genau diese SubVS-Struktur schon mit. Das SubVS für /owa und /ecp bekommt ESP mit MFA. Die SubVS für /mapi, /rpc, /ews, /autodiscover, /oab und /Microsoft-Server-ActiveSync bekommen entweder gar kein ESP oder einen Modus ohne Formular, bei dem der Client weiterhin per Header authentifiziert.

WARNUNG · Eine Ausnahme ist eine offene Tür

Jedes SubVS ohne MFA ist ein Weg, auf dem ein gestohlenes Kennwort weiterhin funktioniert. Wer OWA mit MFA absichert, ActiveSync und EWS aber mit Basic Authentication offen lässt, hat das Problem verschoben, nicht gelöst. Angreifer probieren Kennwörter bevorzugt genau dort aus, wo kein zweiter Faktor wartet. Jede Ausnahme braucht deshalb eine eigene Antwort: Hybrid Modern Authentication, Zertifikate, Geräteverwaltung oder schlicht Abschalten.

Die Protokolle im Überblick

Protokoll / Pfad	MFA am LoadMaster möglich?	Alternative
OWA (/owa)	ja, Formular mit RADIUS oder RSA, oder SAML/OIDC	HMA für OWA direkt in Exchange
ECP (/ecp)	ja, wie OWA	von außen gar nicht veröffentlichen, nur intern oder über strengste Richtlinie
ActiveSync	nein, kein Formular	Outlook Mobile mit HMA, Zertifikatsanmeldung, Geräteverwaltung oder abschalten
MAPI über HTTP (/mapi)	nein	HMA: Outlook holt sich ein Entra-Token, MFA und Bedingter Zugriff greifen dort
Outlook Anywhere (/rpc)	nein	auf MAPI über HTTP umstellen, dann HMA; extern möglichst nicht mehr anbieten
EWS (/ews)	nein	HMA; Zugriff für Apps per Exchange-Richtlinie einschränken
Autodiscover	nein, muss ohne Formular erreichbar sein	eigenes SubVS ohne ESP; Authentifizierung macht Exchange
OAB (/oab)	nein	eigenes SubVS ohne ESP, HMA für Outlook
RD Gateway	nein, RDP über HTTPS kennt kein Formular	NPS-Erweiterung direkt am RD Gateway; RD Web dagegen per ESP
SharePoint mit Office-Clients	nur für den Browser sinnvoll	Office-Clients brauchen eine Lösung ohne LoadMaster-Formular, sonst endlose Anmeldeschleifen

Hybrid Modern Authentication: MFA dort, wo Outlook sie versteht

Für Outlook und Outlook Mobile ist HMA die eigentliche Antwort. Der Client erkennt, dass Exchange OAuth anbietet, holt sich bei Entra ID ein Token, und die Anmeldung inklusive MFA und Bedingtem Zugriff passiert in einem Fenster von Microsoft, das Outlook selbst anzeigt. Exchange prüft danach nur noch das Token. Für den LoadMaster bedeutet das: Er muss sich aus der Authentifizierung dieser Pfade heraushalten, Header wie Authorization unverändert durchlassen und die Verbindung per SSL Bridging zum Server weiterreichen. Das ist weniger spannend als ESP, aber genau richtig.

Sobald HMA läuft, lohnt sich der nächste Schritt: Basic Authentication auf den externen Pfaden abschalten, entweder auf Exchange über Authentifizierungsrichtlinien oder zusätzlich am

LoadMaster, indem du Anfragen mit Basic-Header auf diesen Pfaden per Content Rule abweist. Erst dann ist das Kellerfenster wirklich zu.

TIPP · Autodiscover nicht vergessen

Autodiscover ist der Dienst, über den Outlook überhaupt erst erfährt, wohin es soll. Steht er hinter einem ESP-Formular, scheitert die Profilerstellung, bevor HMA überhaupt eine Chance hat. Prüfe nach jeder Änderung mit einem frischen Outlook-Profil und einem Testgerät außerhalb des Firmennetzes, nicht mit dem Administrator-PC, der per Kerberos intern alles darf.

WICHTIG · Pfadprüfung ist Groß- und Kleinschreibungssache

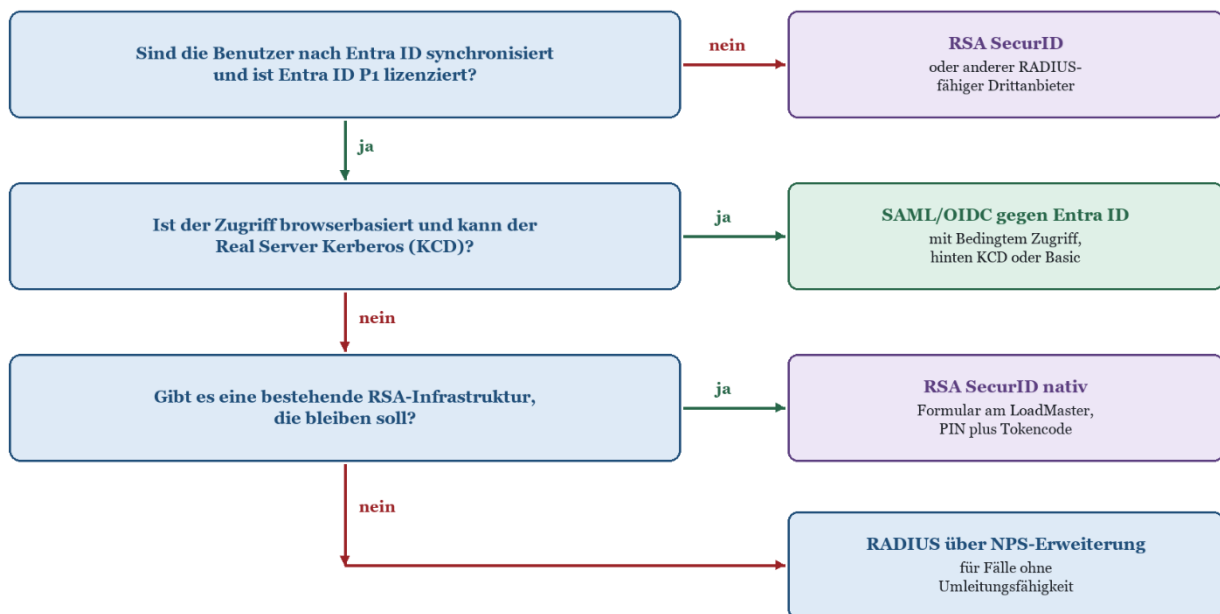
Content Rules, die nach Pfad trennen, müssen die Schreibweisen abdecken, die Clients tatsächlich schicken, etwa /Microsoft-Server-ActiveSync, /autodiscover und /Autodiscover. Setze die Regeln so, dass sie Groß- und Kleinschreibung ignorieren, und lege ein Standard-SubVS fest, das unbekannte Pfade abweist statt sie durchzuwinken. Sonst findet irgendwann ein Scanner den Pfad, an den du nicht gedacht hast.

Welcher Weg für welchen Laden?

Zum Schluss eine grobe Entscheidungshilfe. Sie ersetzt keine Anforderungsaufnahme, aber sie verhindert, dass du drei Wochen in RADIUS-Timeouts investierst, obwohl SAML die bessere Antwort gewesen wäre.

Welcher Weg für welchen Laden?

Drei Fragen, und meistens ist die Antwort schon klar



Skizze: grobe Entscheidungshilfe, ersetzt keine Anforderungsaufnahme

Ausgangslage	Empfehlung	Begründung
Hybrid mit Entra ID P1, Exchange 2019 CU14 oder SE	HMA für Outlook und OWA, LoadMaster ohne ESP auf Exchange	MFA und Bedingter Zugriff einheitlich in Entra ID, LoadMaster verteilt nur Last
Hybrid, aber Alt-Anwendungen mit	SAML/OIDC am LoadMaster plus KCD	moderne Anmeldung vorne, nichts umbauen hinten

Windows-Authentifizierung		
Synchronisiert, aber keine Umleitungsfähigkeit gewünscht	RADIUS gegen NPS mit Erweiterung	vertrautes Formular, Entra MFA, aber wenig Kontext
Bestehende RSA-Infrastruktur, eher reine On-Premises-Welt	RSA SecurID nativ oder per RADIUS	kein Cloud-Zwang, dafür eigener Betrieb des Authentication Manager
Rein lokal ohne Entra ID, aber mit ADFS	SAML gegen ADFS mit MFA-Adapter	Bedingter Zugriff nur in ADFS-Logik, Weg langfristig auslaufend

FAQ: Häufige Fragen zu Kemp MFA

Kann der LoadMaster selbst Einmalcodes erzeugen oder prüfen?

Nein. Der LoadMaster fragt einen RADIUS-Server, einen RSA Authentication Manager oder einen Identitätsanbieter. Den zweiten Faktor selbst verwaltet er nicht, und das ist auch gut so.

Warum bekommen meine Benutzer bei RADIUS keine Nummer zum Abgleich angezeigt?

Weil NPS den Nummernabgleich nicht unterstützt. Aktuelle Versionen der NPS-Erweiterung fragen Benutzer mit registrierter TOTP-Methode stattdessen nach einem Code. Ohne TOTP-Registrierung bleibt es bei Genehmigen oder Ablehnen.

Funktioniert ActiveSync mit MFA am LoadMaster?

Nicht mit Formularanmeldung. ActiveSync-Clients schicken Anmeldedaten im Header und können kein Formular anzeigen. Der Weg zu MFA führt über Outlook Mobile mit Hybrid Modern Authentication, über Zertifikate oder über Geräteverwaltung.

Muss ich für MFA ein eigenes NPS aufsetzen?

In den meisten Fällen ja. Die Erweiterung verlangt MFA für alle RADIUS-Clients eines NPS. Wenn derselbe Server auch WLAN oder Netzwerkgeräte bedient, trennst du das besser auf zwei Server.

Brauche ich für SAML oder OIDC am LoadMaster zwingend KCD?

Wenn der Real Server Windows-Authentifizierung erwartet, praktisch ja, denn Entra ID liefert kein Kennwort, das der LoadMaster weiterreichen könnte. Anwendungen, die selbst keine Authentifizierung verlangen oder Header auswerten, kommen auch ohne aus.

Sollte das ECP überhaupt von außen erreichbar sein?

Im Idealfall nicht. Wenn es sein muss, dann nur mit der strengsten MFA-Richtlinie, die du hast, und am besten zusätzlich auf bekannte Quelladressen beschränkt. Eine Content Rule, die /ecp von außen schlicht abweist, ist die günstigste Sicherheitsmaßnahme dieses ganzen Artikels.

Was passiert bei einem Failover im HA-Paar mit laufenden MFA-Sitzungen?

Die Konfiguration inklusive SSO-Domänen wird synchronisiert. Laufende ESP-Sitzungen können verloren gehen. Bei SAML merkt der Benutzer dank bestehender Entra-Sitzung meist nur eine kurze Umleitung, bei RADIUS und RSA muss er sich erneut anmelden, inklusive zweitem Faktor.

Fazit: Die Haustür ist schnell gesichert, die Kellerfenster nicht

MFA vor OWA und ECP ist am LoadMaster in einem Nachmittag eingerichtet, egal ob per RADIUS gegen NPS mit Entra-Erweiterung, per RSA SecurID oder per SAML und OIDC gegen Entra ID. Wer die Wahl hat, nimmt SAML oder OIDC: Dort bekommst du nicht nur einen zweiten Faktor, sondern auch Bedingten Zugriff, Gerätestatus, phishing-resistente Methoden und ein Protokoll,

mit dem dein SOC etwas anfangen kann. RADIUS ist der pragmatische Weg, wenn Umleitungen keine Option sind, verlangt aber PAP, eine geschützte Strecke und Timeouts, die zu Menschen mit Telefonen in der Jackentasche passen.

Die eigentliche Arbeit steckt woanders: in der Trennung zwischen Browserpfaden und Protokollpfaden. ActiveSync, MAPI, Outlook Anywhere, EWS, Autodiscover und OAB können kein Formular, und jede Ausnahme, die du für sie anlegst, ist eine Tür ohne zweiten Faktor. Erst Hybrid Modern Authentication und das Abschalten von Basic Authentication auf diesen Pfaden machen aus „MFA für OWA“ ein „MFA für Exchange“. Alles andere ist ein sehr gutes Schloss an einer Tür, neben der die Wand fehlt.

TIPP · Unterstützung bei Planung und Umsetzung

Wenn du MFA vor Exchange, SharePoint oder RDS sauber aufteilen und dabei LoadMaster, NPS-Erweiterung und Hybrid Modern Authentication gegeneinander abwägen willst, hilft dir die [Beratung zum Kemp LoadMaster](#). Wer RADIUS-Challenge, SAML und KCD mit dem eigenen Team im Labor aufbauen und gezielt kaputtmachen will, findet das in der [Kemp-LoadMaster-Schulung](#).

WEITERLESEN · Weiter im Thema

- › [Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz](#)
- › [SAML, OIDC und Entra ID: der LoadMaster als moderner Identitätsvermittler](#)
- › [Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks](#)
- › [Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten](#)