Office 365 beveiligen met Okta

okta

Inhoudsopgave

Achtergrond

Okta is een toonaangevende, onafhankelijke identity provider voor enterprises en integreert naadloos met meer dan 5500 applicaties. Het merendeel van deze applicaties is via het internet toegankelijk en is regelmatig het doelwit van kwaadwillenden. Okta's beveiligingsteam ziet ontelbare inbreukpogingen bij klanten, waaronder phishing-, wachtwoord-spraying-, KnockKnock- en beveiligingsaanvallen. Zij houden deze aanvallen continu in de gaten en ondernemen snel actie om de klanttenants en de Okta-service te beschermen. De meeste van deze aanvallen zijn gericht tegen Office 365, een zakelijke productiviteitsservice in de cloud die door Microsoft is ontwikkeld.

Okta's klanten maken veelal gebruik van een combinatie van single sign-on (SSO), geautomatiseerde provisioning en multi-factor authenticatie (MFA) om hun Office 365-tenants tegen deze aanvallen te beschermen. Office 365 gebruikt echter verschillende authenticatiemethoden en toegangsprotocollen, waaronder opties die geen MFA tijdens het authenticatieproces ondersteunen. Het komt steeds vaker voor dat aanvallers via deze opties inbreuk maken op zakelijke e-mailaccounts.

In dit document wordt ingegaan op de bovengenoemde beveiligingsproblemen en wordt aangegeven hoe u Office 365 met Okta configureert om de kloof te overbruggen die door het gebrek aan MFA voor Office 365 ontstaat. Deze informatie is gebaseerd op intern onderzoek dat door het Okta-beveiligingsteam is uitgevoerd en geldt niet als vervanging voor Okta-documentatie waarin de configuratie van Office 365 voor Okta wordt besproken.

Begrippen

Authenticatiemethoden

A. **Basisauthenticatie**
Basisauthenticatie in de Office 365-suite is een legacy authenticatiemechanisme waarbij alleen een gebruikersnaam en wachtwoord nodig zijn. Dit mechanisme is ondoeltreffend gebleken en wordt niet aangeraden voor de moderne IT-omgeving, met name wanneer authenticatiestromen via het internet lopen, zoals bij Office 365 het geval is.

B. **Moderne authenticatie**
Om de veelvoorkomende beveiligingsproblemen bij Office 365-implementaties aan te pakken en tegelijkertijd tegemoet te komen aan de wensen van de eindgebruiker, heeft Microsoft de Active Directory Authentication Library (ADAL) voor Office 365-clientapplicaties geïntroduceerd. Dit wordt "moderne authenticatie" genoemd. Moderne authenticatie helpt Office 365-resources te beschermen met behulp van meervoudige authenticatie (Multi-Factor Authentication), authenticatie op basis van certificaten en op SAML gebaseerde logins (zoals federatie met Okta), om een écht single sign-on mogelijk te maken.

Toegangsprotocollen

Office 365 ondersteunt verschillende protocollen die door clients worden gebruikt om toegang tot Office 365 te krijgen. In dit document worden met "toegangsprotocollen" protocollen bedoeld zoals POP, IMAP, Exchange ActiveSync, Exchange-webservices (EWS), MAPI en PowerShell. In het kader van authenticatie vallen deze protocollen in twee categorieën:

A. **Legacy authenticatieprotocollen**
Protocollen zoals POP en IMAP, die geen moderne authenticatiemethoden ondersteunen, worden "legacy authenticatieprotocollen" genoemd.

B. **Protocollen die moderne authenticatie ondersteunen**
Protocollen zoals Exchange ActiveSync, EWS, MAPI en PowerShell, die zowel basis- als moderne authenticatiemethoden ondersteunen, worden in dit document als moderne authenticatieprotocollen aangemerkt.

E-mailbericht bij toegang vanaf nieuw device

Okta ondersteunt een beveiligingsvoorziening waarbij een gebruiker via e-mail bericht krijgt als iemand zich vanaf een nieuw device of via een browser bij zijn/haar Okta-gebruikersaccount aanmeldt. In de e-mail staan onder andere het tijdstempel, de locatie en de device-informatie, zoals IP-adres en gebruikersagent (versie besturingssysteem/browser).

Office 365-beleid voor clienttoegang

Okta biedt een benadering voor een applicatiegebonden aanmeldbeleid om toegangsbeslissingen te nemen op basis van factoren zoals groepslidmaatschap, netwerklocaties, platform (desktop of mobiel) en multi-factor authenticatie, om er maar een paar te noemen. Bij het Office 365-beleid voor clienttoegang kan de toegangsbeslissing ook worden genomen op basis van clienttype, zoals webbrowser en clients die met moderne of legacy authenticatie werken. Zie Aan de slag met het Office 365-beleid voor clienttoegang voor meer informatie.

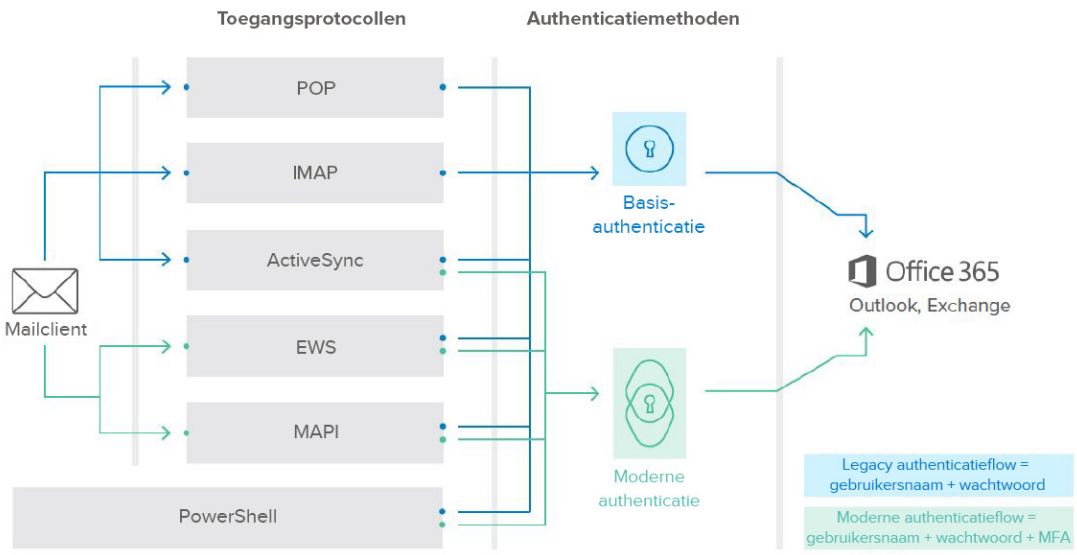
Inleiding

De toegang tot de e-mail van Office 365 wordt bepaald door twee attributen: een authenticatie-methode en een toegangsprotocol. E-mailclients maken gebruik van een combinatie van elk van de twee attributen om toegang te krijgen tot de e-mail van Office 365. Het is belangrijk dat organisaties zich bewust zijn van alle toegangsprotocollen waarmee gebruikers toegang tot de e-mail van Office 365 kunnen krijgen, omdat sommige legacy authenticatieprotocollen geen ondersteuning voor bijvoorbeeld multi-factor authenticatie bieden. In tabel 1 staan de Office 365-toegangsprotocollen en de authenticatiemethoden die ze ondersteunen.

Toegangsprotocollen	Basisauthenticatie	Moderne authenticatie
POP	✓	✗
IMAP	✓	✗
Active Sync	✓	✓
EWS	✓	✓
MAPI	✓	✓
PowerShell	✓	✓

Tabel 1: Protocol en ondersteunde authenticatiemethoden

"PowerShell" is geen echt protocol dat door e-mailclients wordt gebruikt, maar is nodig voor de interactie met Exchange. In afbeelding 1 hieronder staat de toegangsmatrix van Office 365 op basis van de toegangsprotocollen en authenticatiemethoden die in tabel 1 zijn genoemd:



Probleemstelling

In de meeste zakelijke omgevingen is het tegenwoordig een must om multi-factor authenticatie te gebruiken om de e-mailtoegang te beveiligen. In verband met de volgende beperkingen is het niet altijd mogelijk om dit voor elke Office 365-aanmelding te doen:

A. Niet alle toegangsprotocollen die door Office 365-e-mailclients worden gebruikt, ondersteunen moderne authenticatie. Protocollen zoals POP en IMAP ondersteunen alleen basisauthenticatie en kunnen daarom geen MFA in hun authenticatieprocedure afdwingen.

B. Los van het gebruikte toegangsprotocol, hebben e-mailclients die basisauthenticatie ondersteunen, alleen maar een gebruikersnaam en wachtwoord nodig om zich aan te melden bij en toegang te krijgen tot Office 365, ondanks het feit dat federatie MFA afdwingt.

C. Moderne authenticatieprotocollen, zoals Exchange ActiveSync, EWS en MAPI, kunnen ook met basisauthenticatie worden gebruikt. Zo kunnen Outlook-clients standaard op basisauthenticatie worden ingesteld door het register op Windows-computers te wijzigen.

D. Bij Office 365 is het op dit moment niet mogelijk om basisauthenticatie uit te schakelen. Dit houdt in dat zelfs als moderne authenticatie op een Office 365-tenant is ingeschakeld, e-mailclients daar nog steeds met basisauthenticatie toegang toe hebben.

E. In een omgeving waarin Okta voor federatie wordt gebruikt, wordt bij het gebruik van legacy authenticatieprotocollen (POP en IMAP), die met basisauthenticatie werken, geen e-mailbericht verstuurd als er toegang vanaf een nieuw device wordt gedetecteerd.

Deze complexiteit levert een lastige evenwichtsoefening op tussen enerzijds het ondersteunen van de favoriete e-mailapplicaties van eindgebruikers en anderzijds het afdwingen van MFA in de hele Office 365-omgeving. In het gedeelte "Verwachte gedragingen/wijzigingen" hierna wordt ingegaan op de compromissen die moeten worden gemaakt om MFA voor Office 365 af te dwingen.

Authenticatiemethoden voor Office 365

Achter de schermen maakt de Office 365-suite gebruik van Azure AD om de authenticatie af te handelen; er wordt dus standaard een Azure AD-instantie bij de Office 365-licentie geleverd. Azure AD ondersteunt twee van de belangrijkste methoden voor het configureren van gebruikersauthenticatie:

A. **Cloudauthenticatie** met:

   a. wachtwoord-hashsynchronisatie of
   b. Pass Through-authenticatie

B. **Federatie**

   Later in dit document wordt ingegaan op de wijzigingen die nodig zijn om MFA voor Office 365 af te dwingen met federatieve authenticatie met Okta als IDP. Er moeten echter een paar kanttekeningen worden gemaakt bij de eerdergenoemde cloudauthenticatiemethoden.

Wachtwoord-hashsynchronisatie Bij wachtwoord-hashsynchronisatie moet de wachtwoord-hash van een on-prem Active Directory (AD) worden gesynchroniseerd met een cloudinstantie van Azure AD. Zo kunnen gebruikers zich met hetzelfde wachtwoord als voor de lokale AD authenticeren bij cloudservices als Office 365. In dit scenario **kan MFA alleen worden afgedwongen via Azure MFA**; MFA-oplossingen van andere aanbieders worden niet ondersteund.

Bij **Pass Through-authenticatie** kunnen gebruikers met een wachtwoord toegang krijgen tot cloudservices zoals Office 365, zoals met het wachtwoord dat in on-prem AD is opgeslagen. In het geval van Pass Through-authenticatie hoeft de wachtwoord-hash niet met een cloud-Azure AD te worden gesynchroniseerd via tussenliggende systemen, zogeheten "agents voor Pass Through-authenticatie", die als koppelstuk tussen on-premises AD en Azure AD fungeren. Een belangrijke opmerking hierbij is dat MFA alleen via Azure-MFA kan worden afgedwongen als Pass Through-authenticatie wordt gebruikt; MFA van andere aanbieders en methoden voor on-prem MFA worden niet ondersteund.

Nu we de MFA-vereisten voor de cloudauthenticatiemethode hebben besproken, kunnen we ons gaan richten op de beveiliging van federatieve authenticatie bij Office 365 met Okta als ID-provider.

Federatieve Office 365 beveiligen met Okta

Om MFA af te dwingen in Office 365 dat met Okta is gefedereerd, moet een aantal stappen worden uitgevoerd. Met het afdwingen van MFA wordt in dit verband bedoeld dat alle achterdeurtjes worden gedicht die zouden kunnen worden benut om de MFA-controlemechanismen te omzeilen. Het is heel belangrijk dat de stappen voor deze configuratiewijzigingen worden uitgevoerd en dat ze in de aangegeven volgorde worden uitgevoerd:

A. **Office 365-authenticatie federeren met Okta**
B. **Moderne authenticatie inschakelen voor Office 365**
C. **Legacy authenticatieprotocollen uitschakelen voor Office 365 (OPTIONEEL)**
D. **Basisauthenticatie uitschakelen voor Office 365**
E. **Het Office 365-beleid voor clienttoegang configureren in Okta**
F. **Vernieuwingstokens intrekken in Exchange**

De volgorde van de stappen is belangrijk, omdat bij de laatste stap de huidige Office 365-tokens die aan gebruikers zijn afgegeven, ongeldig worden gemaakt, wat pas moet worden gedaan nadat het Office 365-beleid voor clienttoegang in Okta is ingesteld. Dit zorgt ervoor dat bestaande gebruikerssessies (met zowel niet-moderne als moderne authenticatie) worden beëindigd en dat er voor de nieuwe sessies moderne authenticatie wordt gebruikt.

De minimale bevoegdheden die voor Office 365 en het Okta-platform nodig zijn om deze wijzigingen door te voeren, staan in tabel 2:

Platform	Bevoegdheid
Office 365	Organisatiebeheer
Okta	Outlook 2016

Tabel 2: Benodigde platformbevoegdheid

Verwachte gedragingen/wijzigingen

Voordat we verdergaan, moeten we opmerken dat de configuratiewijzigingen die in dit document worden genoemd, de volgende gedragingen tot gevolg hebben:

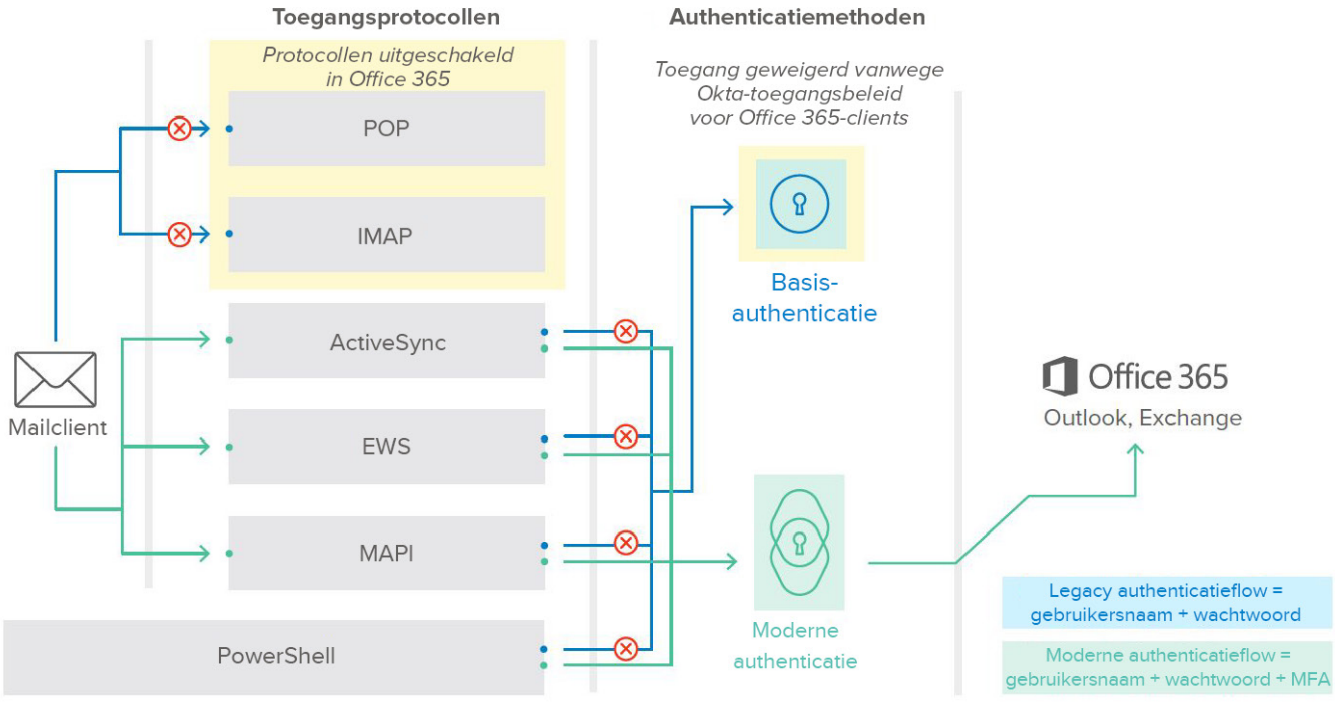
A. Alle toegang tot Office 365 vindt plaats via moderne authenticatie.

B. Clients die gebruikmaken van legacy authenticatieprotocollen (waaronder legacy Outlook- en Skype-clients en een paar native clients), wordt de toegang tot Office 365 ontzegd. Meer informatie over ondersteunde clients volgt.

C. Clients die moderne authenticatieprotocollen ondersteunen, kunnen via basisauthenticatie geen toegang tot Office 365 krijgen.

D. Beheerders van Office 365 hebben de PowerShell-module met ondersteuning voor moderne authenticatie nodig om verbinding te maken met online Exchange.

In afbeelding 2 staat de toegangsmatrix voor Office 365 nadat de configuraties zijn geïmplementeerd:



Afbeelding 2: Toegangsmatrix Office 365 na beveiligingsconfiguratie

Als er een legitieme zakelijke reden is om verkeer te laten lopen via legacy authenticatieprotocollen waarvoor basisauthenticatie wordt gebruikt, biedt het Office 365-beleid voor clienttoegang de mogelijkheid om een uitzondering op gebruikers-/groepsniveau toe te voegen. De uitzonderingen kunnen worden gekoppeld aan netwerkzones in Okta om de kwetsbaarheid voor aanvallen te verminderen. Een voorbeeld van een legitieme zakelijke reden zou een SaaS-integratie zijn waarvoor POP3 of IMAP wordt gebruikt, zoals Jira. Organisaties zouden het Office 365-beleid voor clienttoegang ook aan device trust kunnen koppelen in geval van beheerde iOS-devices om toegang tot Office 365 toe te staan.

A. Office 365-authenticatie federereren met Okta

Federatieve authenticatie is een methode waarbij de authenticatie wordt gedelegeerd aan de ID-provider (IDP), in dit geval Okta. Om de authenticatie voor Office 365 te regelen met beleidsregels die in Okta zijn gedefinieerd, moet federatie voor Office 365 worden ingeschakeld. Informatie over hoe u federatie voor Office 365 met Okta configureert, is te vinden in de implementatiegids voor Office 365.

B. Moderne authenticatie inschakelen

Bij gebruik van moderne authenticatie voor Office 365 zijn aanmeldingsvoorzieningen mogelijk zoals multi-factor authenticatie en op SAML gebaseerde aanmelding met ID-providers (zoals Okta). Als in Office 365 "Moderne authenticatie" is ingeschakeld, gebruiken clients die moderne authenticatie ondersteunen deze methode in plaats van basisauthenticatie.

Moderne authenticatie kan voor een Office 365-tenant worden ingeschakeld door in PowerShell de volgende opdrachten uit te voeren:

1. Om verbinding te maken met Office 365 Exchange, opent u de module Exchange Online PowerShell en voert u de volgende opdracht in (vervang 'adminuser@domain' door de beheerdersreferenties in Exchange):

   ```
   Connect-EXOPSSession -UserPrincipalName @domain>
   ```

2. Voer de volgende opdracht in om de huidige configuratie te zien:

   ```
   Get-OrganizationConfig | Format-Table -Auto Name,OAuth*
   ```

3. Als de waarde van OAuth2ClientProfileEnabled Waar is, is moderne authenticatie voor het domein ingeschakeld. Zo niet, dan gebruikt u de volgende opdracht om het in te schakelen:

   ```
   Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
   ```

Omdat Office 365 geen mogelijkheid biedt om basisauthenticatie uit te schakelen, is het inschakelen van moderne authenticatie op zichzelf niet voldoende om MFA voor Office 365 af te dwingen. Terwijl nieuwere e-mailclients standaard moderne authenticatie gebruiken, kan die standaardinstelling aan de clientkant door eindgebruikers worden overschreven. Daarom moeten we ook het Office 365-beleid voor clienttoegang in Okta afdwingen. Raadpleeg het gedeelte "Het Office 365-beleid voor clienttoegang configureren in Okta" voor meer informatie.

C. Legacy authenticatieprotocollen uitschakelen

Dit is een optionele stap om ervoor te zorgen dat legacy authenticatieprotocollen zoals POP en IMAP, die alleen basisauthenticatie ondersteunen, in Exchange worden uitgeschakeld.

De console van Office 365 Exchange Online biedt geen mogelijkheid om de legacy authenticatie-protocollen voor alle gebruikers tegelijk uit te schakelen. Dit kan wel via de module Exchange Online PowerShell.

Met de volgende opdrachten controleert u op gebruikers waarvoor legacy authenticatieprotocollen zijn ingeschakeld en schakelt u de legacy protocollen voor die gebruikers uit. In de opdrachten hieronder wordt het POP-protocol als voorbeeld gebruikt. U moet 'Pop' in die opdrachten vervangen door 'Imap' en 'ActiveSync' om ook die protocollen uit te schakelen.

1. Vraag een lijst op met alle gebruikers waarvoor POP, IMAP en ActiveSync is ingeschakeld.

```
Get-CASMailbox -ResultSize Unlimited -Filter
{(RecipientTypeDetails -eq 'UserMailbox')} | where
{$_.PopEnabled -eq $true} | FL name
```

2. Schakel legacy authenticatieprotocollen uit.

```
Get-CASMailbox -ResultSize Unlimited -Filter
{(RecipientTypeDetails -eq 'UserMailbox')} | where
{$_.PopEnabled
-eq $true} | Set-CASMailbox -PopEnabled $false
```

Om ervoor te zorgen dat deze legacy authenticatieprotocollen worden uitgeschakeld voor nieuwe gebruikers die aan Exchange worden toegevoegd, kunnen Administrators de commandlet SET-CSAMailboxPlan in PowerShell uitvoeren. Met deze methode wordt overigens alleen de configuratie ingesteld voor nieuwe postbussen en niet voor bestaande postbussen.

1. Geef alle postvakplannen weer

```
Get-CASMailboxPlan | Select Name,IsDefault
```

2. Schakel POP en IMAP uit

```
Set-CASMailboxPlan -ImapEnabled:$false -PopEnabled:$false
```

D. Basisauthenticatie uitschakelen voor Office 365

In deze stap configureert u een authenticatiebeleid in Office 365 om basisauthenticatie te blokkeren. Met dit beleid blokkeert u de toegang tot legacy protocollen op pre-authenticatieniveau, wat inhoudt dat logins die via legacy eindpunten binnenkomen, helemaal niet worden geëvalueerd. De console van Office 365 Exchange Online biedt geen mogelijkheid om basisauthenticatie voor alle gebruikers tegelijk uit te schakelen. Dit kan wel via de module Exchange Online PowerShell. De volgende opdrachten geven aan hoe u een beleid maakt waarmee basisauthenticatie wordt geweigerd en hoe u gebruikers aan het beleid toewijst.

1. Om Exchange PowerShell-opdrachten op uw Windows-computer (of server) uit te voeren, installeert u Windows Management Framework 5.1.

```
Connect-EXOPSSession -UserPrincipalName @domain>
```

2. Open PowerShell als Administrator en maak verbinding met Exchange:

```
Set-ExecutionPolicy RemoteSigned
$UserCredential - Get-Credential
```

> **Opmerking:** Als voor uw Administrator-account MFA is ingeschakeld, volgt u de aanwijzingen in de documentatie van Microsoft.

3. Meld u aan bij uw Office 365 Exchange-tenant:

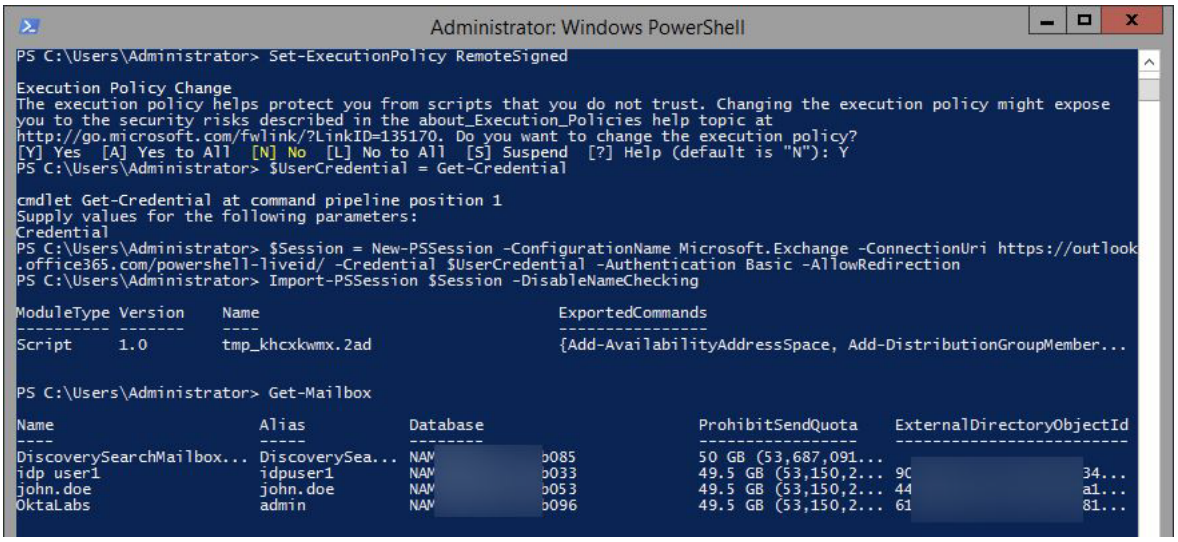
```
$Session = New-PSSession -ConfigurationName
Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential
$UserCredential -Authentication Basic -AllowRedirection


Import-PSSession $Session -DisableNameChecking
```

4. Om te bevestigen dat de verbinding tot stand is gebracht, voert u de volgende opdracht in:

```
Get-Mailbox
```

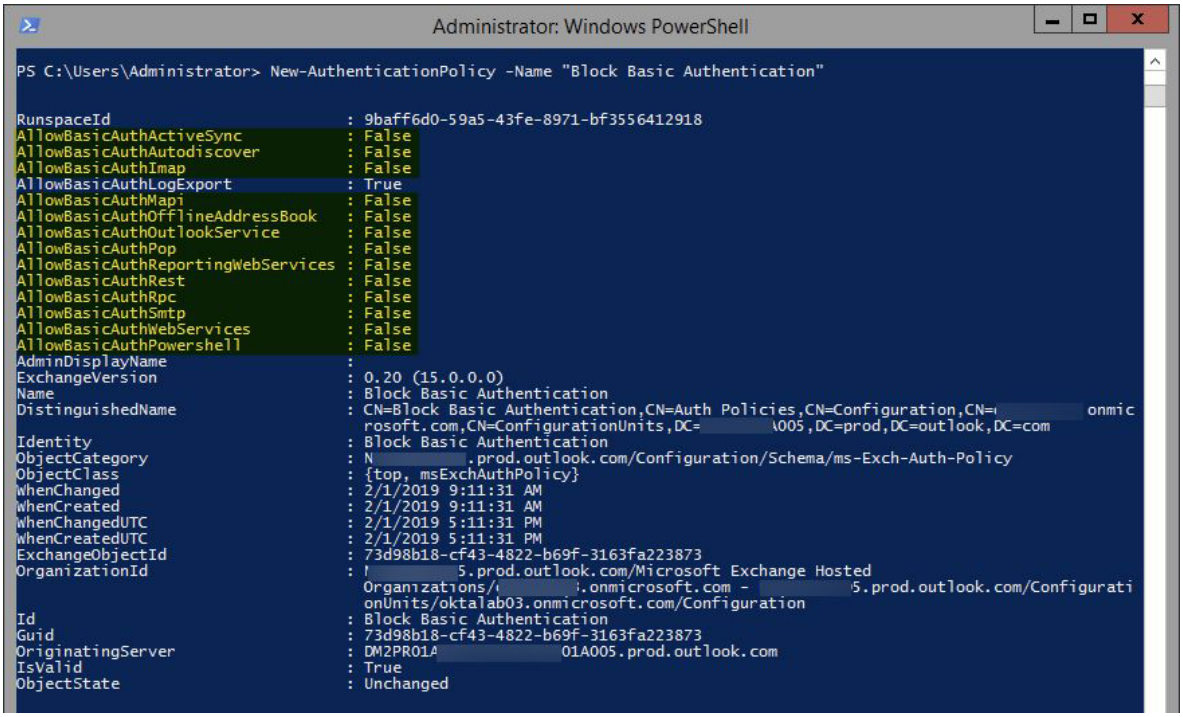
U ziet nu een lijst met gebruikers van uw Office 365-tenant:



5. Om een authenticatiebeleid te maken waarmee basisauthenticatie wordt geweigerd, voert u de volgende opdracht in (hiermee worden alle legacy protocollen geblokkeerd, zoals in de Microsoft-documentatie wordt vermeld):

```
New-AuthenticationPolicy -Name "Block Basic Authentication"
```

De beleidseigenschappen worden in de terminal weergegeven. U ziet dat basisauthenticatie is uitgeschakeld:



6. Om te bevestigen dat het beleid bestaat, of om het beleid te bekijken, voert u de volgende opdracht in:

```
Get-AuthenticationPolicy -Identity "Block Basic Authentication"
```

7. Om een gebruiker toe te voegen aan het beleid, gebruikt u de volgende opdracht:

```
Set-User -Identity <UserId> -AuthenticationPolicy "Block Basic
Authentication"
```

8. Laat eventueel het beleid over 30 minuten ingaan (in plaats van 24 uur) door de gebruikerstokens in te trekken:

```
Set-User -Identity <UserId> -STSRefreshTokensValidFrom
$([System.DateTime]::UtcNow)
```

9. Gebruik eventueel de volgende PowerShell-fragmenten om het authenticatiebeleid toe te wijzen of om tokens voor meerdere gebruikers te wissen (raadpleeg de Microsoft-documentatie voor meer voorbeelden):

Voorbeeld 1: Gebruikers blokkeren van wie de titel het woord "Engineering" bevat

```
$Engineers = Get-User -ResultSize unlimited -Filter
{(RecipientType -eq 'UserMailbox') -and (Title -like
'*Engineering*')}
$EngId = $Engineers.MicrosoftOnlineServicesID
$EngId | foreach {Set-User -Identity $_ -AuthenticationPolicy
"Block Basic Authentication"}
$EngId | foreach {Set-User -Identity $_
-STSRefreshTokensValidFrom $([System.DateTime]::UtcNow)}
```

Voorbeeld 2: Gebruikers in een lijst blokkeren: list.txt contents:

list.txt contents:

```
jan.janssen@mijndomein.nl
joke.janssen@mijndomein.nl
```

PowerShell:

```
$List = Get-Content "C:\temp\list.txt"
$List | foreach {Set-User -Identity $_ -AuthenticationPolicy
"Block Basic Authentication"}
$List | foreach {Set-User -Identity $_
-STSRefreshTokensValidFrom $([System.DateTime]::UtcNow)}
```

Voorbeeld 3: Het nieuwe authenticatiebeleid als standaard voor alle gebruikers instellen:

```
Set-OrganizationConfig -DefaultAuthenticationPolicy "Block Basic
Authentication"
```

E. Het Office 365-beleid voor clienttoegang configureren in Okta

Om moderne authenticatie voor Office 365-authenticatie af te dwingen, moet het beleid worden geconfigureerd in het aanmeldingsgedeelte voor de Office 365-applicatie in de Okta Admin Console (Okta-beheerconsole). Meer specifiek moeten we twee beleidsregels voor clienttoegang voor Office 365 in Okta toevoegen.

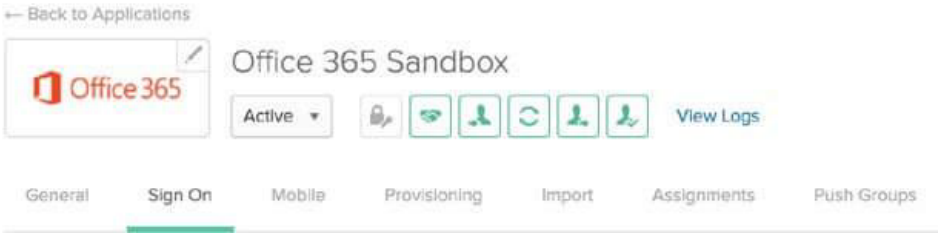
A. Weiger toegang wanneer clients basisauthenticatie gebruiken, en

B. Dwing MFA af voor nieuwe aanmeldingen/sessies voor clients die moderne authenticatie gebruiken.

Deze beleidsregels zijn nodig voor het geval gebruikers niet door het authenticatiebeleid van Office 365 worden beschermd.

U configureert het beleid als volgt:

1. **Kies in de Okta Admin Console de opties Applications > Office 365 > Sign-on > Sign-on policy**



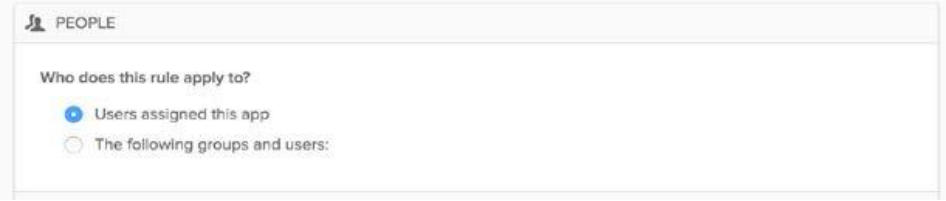
Afbeelding 3: Configuratie van Office 365-applicatie in Okta

2. **Maak een beleid om legacy authenticatieprotocollen te weigeren**

   Het doel van een "blokkeerbeleid" is om, ongeacht locatie en deviceplatform, de toegang te weigeren aan clients die gebruikmaken van legacy authenticatieprotocollen die alleen basisauthenticatie ondersteunen.

   De beleidsconfiguratie bestaat uit het volgende:

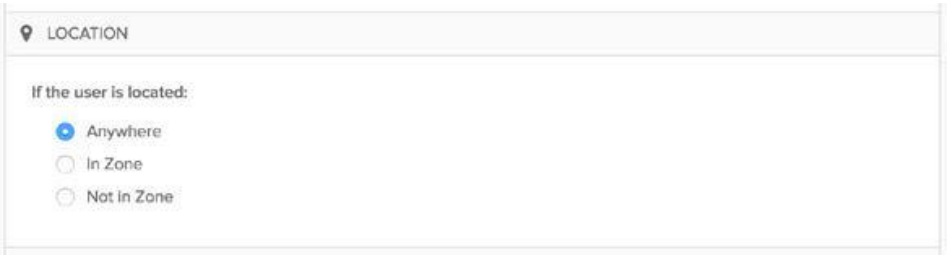
   People: Selecteer alle gebruikers/groepen die toegang tot deze applicatie hebben.



Afbeelding 4: Office 365-beleid voor clienttoegang (Weigeren) – deel 1

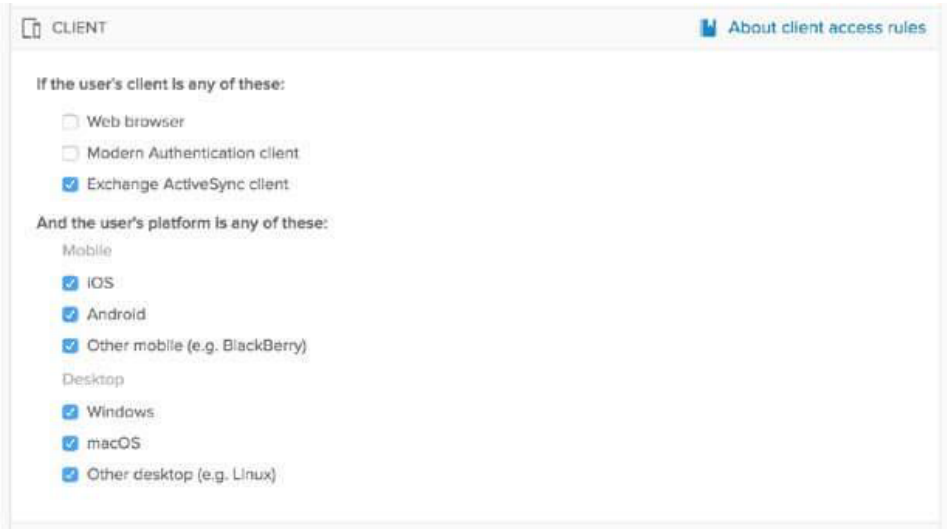
Opmerking: Als er een zakelijke noodzaak is om toegang te verlenen aan legacy authenticatieprotocollen, maakt u een groep van die gebruikers-/serviceaccounts en sluit u die groep vervolgens van deze regel uit door de optie "Exclude the following users and groups from this rule" in te schakelen. Voor de uitgesloten groep kunt u overwegen om een afzonderlijk aanmeldbeleid te maken en om via netwerkzones beperkte toegang te verlenen.

Location: Selecteer **Anywhere:**



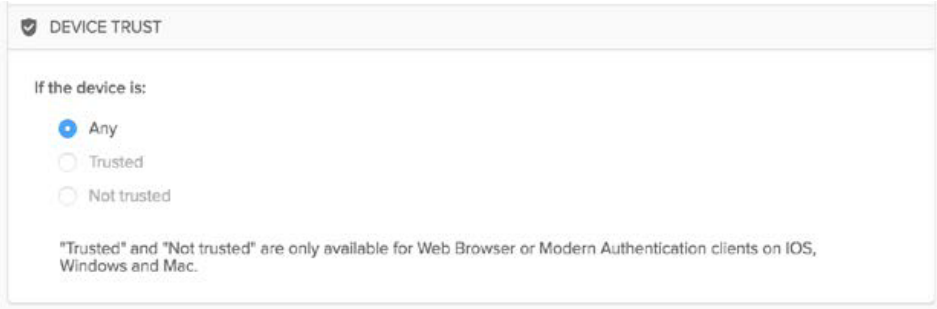
Afbeelding 5: Office 365-beleid voor clienttoegang (Weigeren) – deel 2

Client: Kies "Exchange ActiveSync client" en alle gebruikersplatforms. **Hiermee wordt in feite de toegang beperkt op basis van basisauthenticatie via alle toegangsprotocollen (MAPI, EWS, ActiveSync, POP en IMAP)**.



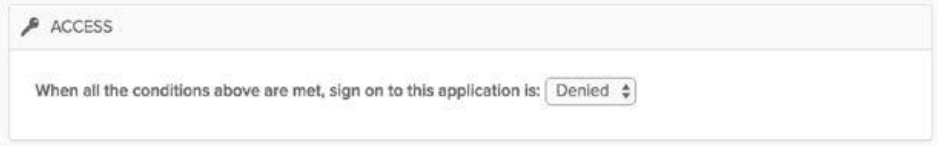
Afbeelding 6: Office 365-beleid voor clienttoegang (Weigeren) – deel 3

Device Trust: Kies "Any", dat wil zeggen, zowel vertrouwde als niet-vertrouwde devices.



Afbeelding 7: Office 365-beleid voor clienttoegang (Weigeren) – deel 4

Actions: Kies "Denied".

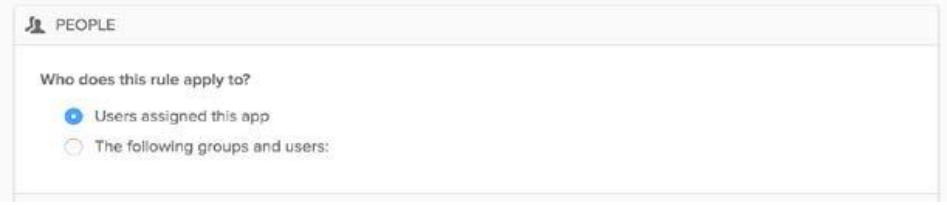


Afbeelding 8: Office 365-beleid voor clienttoegang (Weigeren) – deel 5

3. **Maak een beleid voor MFA bij moderne authenticatie**

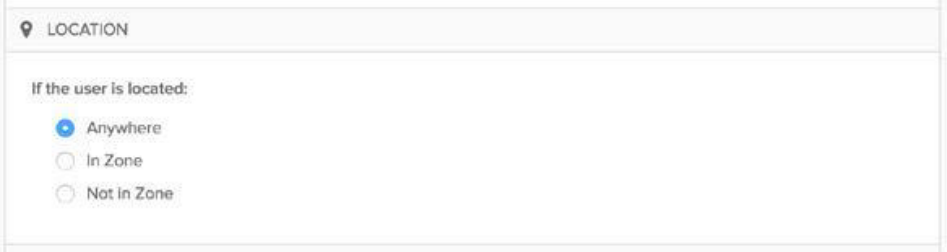
Het doel van dit beleid is om voor elke aanmelding bij de Office 365-applicatie MFA af te dwingen, ongeacht de locatie en het deviceplatform. De beleidsconfiguratie bestaat uit het volgende:

People: Selecteer alle gebruikers/groepen die toegang tot deze applicatie hebben.



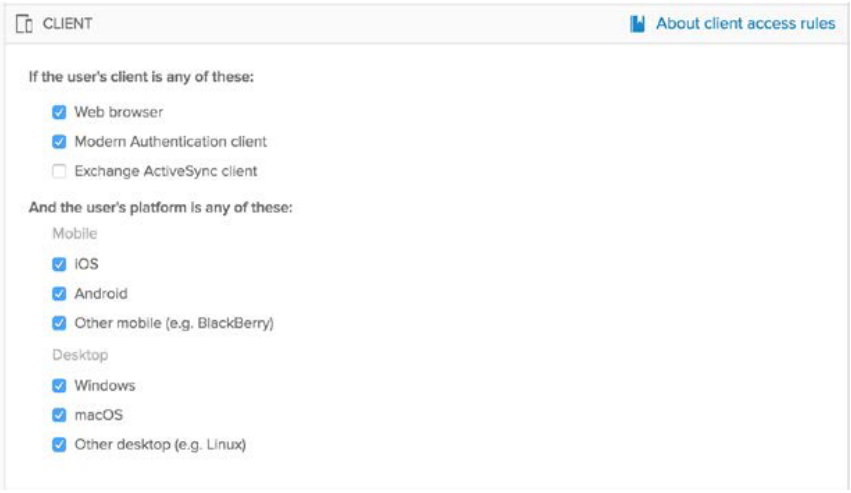
Afbeelding 9: Office 365-beleid voor clienttoegang (Toestaan) – deel 1

Location: Selecteer **Anywhere:**



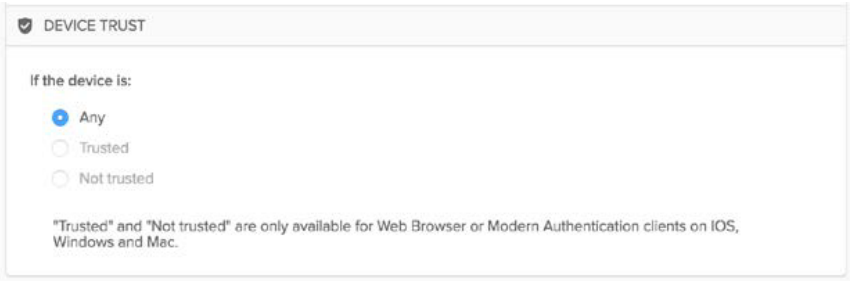
Afbeelding 10: Office 365-beleid voor clienttoegang (Toestaan) – deel 2

Client: Selecteer "Web browser" en "Modern Authentication client" en alle platforms:



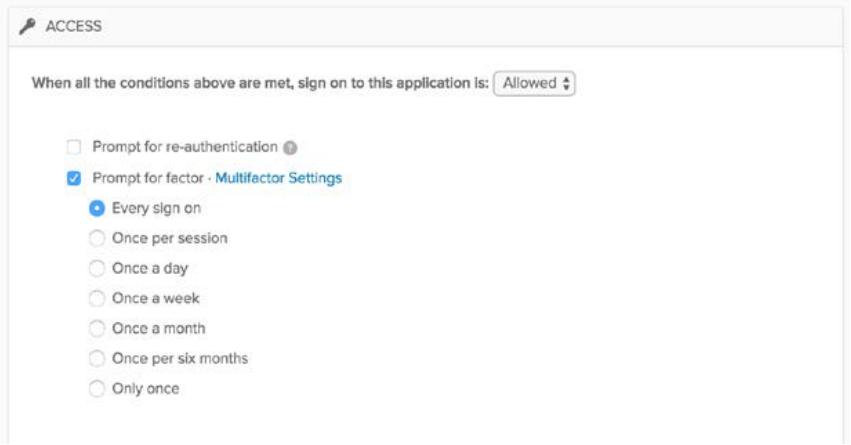
Afbeelding 11: Office 365-beleid voor clienttoegang (Toestaan) – deel 3

Device Trust: Kies "Any", dat wil zeggen, zowel vertrouwde als niet-vertrouwde devices.



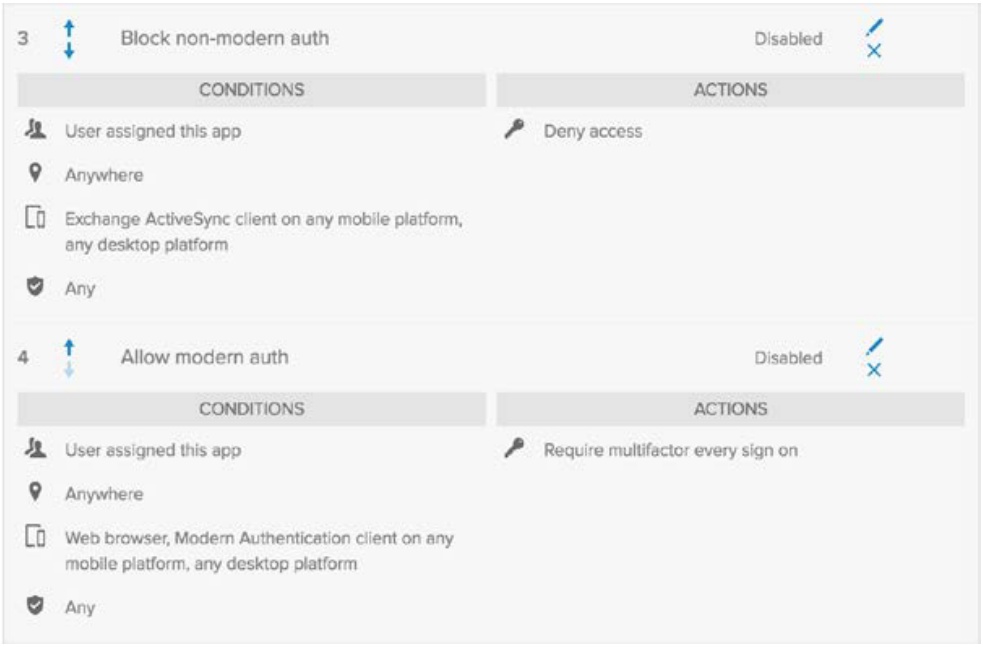
Afbeelding 12: Office 365-beleid voor clienttoegang (Toestaan) – deel 4

Actions: Selecteer "Allowed" en schakel "Prompt for factor" in. De frequentie van de factorvraag kan worden ingesteld op basis van het vertrouwelijkheidsniveau van gebruikers/groepen. Als dit beleid bijvoorbeeld wordt toegepast op belangrijke gebruikers of leidinggevenden, kan worden ingesteld dat er bij elke aanmelding of elke sessie om de factor wordt gevraagd.



Afbeelding 13: Office 365-beleid voor clienttoegang (Toestaan) – deel 5

Nadat de bovenstaande beleidsregels zijn toegepast, zou de uiteindelijke configuratie er ongeveer als in afbeelding 14 moeten uitzien:



Afbeelding 14: Samenvatting van Office 365-beleid voor clienttoegang

F. Vernieuwingstokens intrekken

Om het aantal gebruikersaanmeldingen bij de Office 365-applicatie te beperken, geeft Azure AD twee soorten tokens uit: het toegangstoken en het vernieuwingstoken. Beide tokens worden uitgegeven wanneer een gebruiker zich voor de eerste keer aanmeldt. Een toegangstoken wordt verleend voor de combinatie van gebruiker, client en resource die wordt gebruikt wanneer de gebruiker zich voor het eerst aanmeldt. Standaard is het toegangstoken één uur geldig (aan te passen tot minimaal 10 minuten). Vernieuwingstokens zijn geldig voor een periode van 90 dagen en worden gebruikt om nieuwe sets toegangs-/vernieuwingstokens te verkrijgen.

Wanneer de gebruiker een geldig vernieuwingstoken heeft, wordt hij niet meer gevraagd om zich aan te melden en houdt hij toegang totdat het vernieuwingstoken verloopt. Om ervoor te zorgen dat alle configuraties die eerder in dit document zijn vermeld, onmiddellijk van kracht worden**, moeten de vernieuwingstokens worden ingetrokken.

** **Ook nadat een "vernieuwingstoken" is ingetrokken, kan de gebruiker nog steeds toegang hebben tot Office 365 zolang zijn toegangstoken geldig is.** Het verkorten van de levensduur van een toegangstoken vergt een afweging tussen de prestaties en de tijd dat clients op basis van de huidige configuratie toegang houden.

Om de levensduur van een toegangstoken te wijzigen of een vernieuwingstoken in te trekken, volgt u de hier genoemde stappen in PowerShell.

1. Open een nieuw PowerShell-venster als administrator en installeer de module Azure AD PowerShell:

```
Install-Module -Name AzureAD
```

2. Om het vernieuwingstoken voor één gebruiker in te trekken, meldt u zich via de module Exchange Online PowerShell aan bij Exchange:

```
Connect-AzureAD
Revoke-AzureADUserAllRefreshToken -ObjectId
```

3. Als u de vernieuwingstokens voor alle gebruikers wilt intrekken, gaat u als volgt te werk:

```
(Get-AzureADUser).ObjectId | Revoke-AzureADUserAllRefreshToken
```

Bekende e-mailclients die moderne authenticatie ondersteunen

De officiële lijst met Outlook-clients die ten tijde van deze publicatie moderne authenticatie ondersteunen, is opgenomen in tabel 3 en is ook beschikbaar op de Microsoft-website. Deze clients werken zoals verwacht nadat de in dit document genoemde wijzigingen zijn doorgevoerd. De **Outlook Web App** (OWA) werkt voor alle browsers en besturingssystemen, aangezien de app via de browser werkt en niet van legacy authenticatieprotocollen afhankelijk is.

Besturingssysteem	Eigen e-mailclient
Windows	Outlook 2013 & Outlook 2016
Mac OS	Outlook 2016
Android	Outlook-app
iOS	Outlook-app
*nix	N.v.t. (*nix-platform ondersteunt Outlook-client officieel niet)

Tabel 3: Outlook-clients die moderne authenticatie ondersteunen

Raadpleeg de hier genoemde Microsoft-documentatie voor een volledige lijst met applicaties (afgezien van Outlook-clients) die moderne authenticatie ondersteunen. Om met PowerShell toegang te krijgen tot Exchange Online via moderne authenticatie, installeert u de module Exchange Online Remote PowerShell Module.

Microsoft Outlook-clients die geen ondersteuning bieden voor moderne authenticatie worden hieronder genoemd.

Besturingssysteem	Niet-ondersteunde Outlook-client
Windows	Outlook 2010 & lager
Mac OS	Outlook 2011 & lager

Tabel 4: Outlook-clients die geen ondersteuning bieden voor moderne authenticatie

Lijst met e-mailclients die door Okta zijn getest

In tabel 5 staan de versies van Microsoft Outlook en de eigen e-mailclients van besturingssystemen die door het informatiebeveiligingsteam van Okta zijn getest op ondersteuning van moderne authenticatie.

Platform	Eigen e-mailclient	Outlook-client
Windows 10	MailVersion: 17.9126.21785.0	Outlook 2016 Versie: 16.0 en hoger
OSX 10.13.4	Native e-mailclient biedt geen ondersteuning voor moderne authenticatie	Outlook 2016 Versie: 16.12 en hoger
iOS 10.3.3	Native e-mailclient biedt geen ondersteuning voor moderne authenticatie	Outlook Versie: 2.75.0 en hoger
iOS 11.3.1	Native e-mailclient (Exchange Discover)	Outlook Versie: 2.75.0 en hoger
Android 8.1.0	Native e-mailclient biedt geen ondersteuning voor moderne authenticatie	Outlook Versie: 2.2143 en hoger
*nix	Native e-mailclient biedt geen ondersteuning voor moderne authenticatie	Niet beschikbaar

Tabel 5: Outlook en native clients die door Okta zijn getest

Conclusie

Door de richtlijnen in dit document te volgen, kunnen Okta-klanten MFA afdwingen op alle e-mailclients die moderne authenticatie ondersteunen en zo hun Office 365-applicatie beschermen tegen phishing-, wachtwoord-spraying-, KnockKnock- en beveiligingsaanvallen. Andere e-mailclients en platforms die niet in het kader van dit onderzoek zijn getest, moeten mogelijk nader worden geëvalueerd.

Referenties

Okta Adaptive MFA

Office 365-beleid voor clienttoegang in Okta

Aanmeldbeleid voor apps in Okta

Netwerkzones in Okta

Disclaimer

De inhoud van dit document dat Okta aan haar klanten ter beschikking stelt, geldt als aanbeveling. Dit document doet geen afbreuk aan de garanties die Okta aan haar klanten geeft met betrekking tot de beveiligingspraktijken die Okta hanteert om haar Okta-producten te beveiligen, zoals wordt beschreven in Okta's beveiligings- & privacydocumentatie (te vinden op https://www.okta.com/trustandcompliance/.