Salesforce Beheerdersbeveiliging

Installatiegids phishing-resistente MFA

Ingangsdatum: Productie-omgevingen vanaf 1 juli 2026 | Sandboxen vanaf 22 juni 2026. Lees ook **Voorbereiding phishing-resistente MFA (beheerders):** help.salesforce.com/s/articleView?id=005321563.

1. Wat is vereist?

Vanaf 1 juli 2026 moeten alle bevoorrechte Salesforce-gebruikers inloggen met een phishing-resistente MFA-methode. Bevoorrechte gebruikers zijn gebruikers met:

- het profiel Systeembeheerder of Systeembeheerder Mysolution
- Systeempermissie Modify All Data, View All Data, Customize Application of Author Apex

Standaard authenticator-apps (zoals Google Authenticator, Microsoft Authenticator of Authy) die 6-cijferige TOTP-codes genereren, voldoen niet aan de nieuwe eis. Gebruikers die geen geschikte methode hebben geregistreerd, worden geblokkeerd bij het inlogscherm.

Gekwalificeerde methoden zijn:

- Ingebouwde authenticators: Touch ID, Face ID (Mac/iPhone), Windows Hello (Windows 10/11)
- Fysieke beveiligingssleutels: YubiKey, Google Titan Key, of een andere WebAuthn/FIDO2/U2F-sleutel
- Gesynchroniseerde passkeys opgeslagen in een wachtwoordmanager (Apple iCloud Keychain, 1Password, Bitwarden, etc.)

> ℹ Salesforce raadt aan om minimaal twee gekwalificeerde methoden per beheerder te registreren als back-up, voor het geval een apparaat kwijtraakt of niet beschikbaar is.

2. Overzicht scenario's

De onderstaande tabel geeft een overzicht van de meest voorkomende configuraties en de bijbehorende inlogervaring na de instelling.

Platform	Methode	Inlogervaring na instelling	Gekwalificeerd?
Windows	Fysieke beveiligingssleutel (YubiKey etc.)	Sleutel insteken/tikken + knop aanraken	☑ Gekwalificeerd
Windows	Windows Hello (pincode / gezicht / vingerafdruk)	Windows Hello-venster – vrijwel naadloos	☑ Gekwalificeerd
Windows	Externe passkey (1Password, Bitwarden)	Pop-up van extensie, bevestigen in app	☑ Gekwalificeerd
Mac	Apple Passkey (iCloud Keychain)	Naadloos – Touch ID of Mac-loginvenster	☑ Gekwalificeerd
Mac	Externe passkey (1Password, Bitwarden)	Pop-up van extensie, bevestigen in app	☑ Gekwalificeerd
Mac	Fysieke beveiligingssleutel (YubiKey etc.)	Sleutel insteken/tikken + knop aanraken	☑ Gekwalificeerd
Alle	TOTP-app (Google/Microsoft Authenticator)	Geblokkeerd – voldoet NIET aan de eis	✗ Niet gekwalificeerd

3. Activatie Beveiligingssleutel

Zoals aangegeven zal deze methode vanaf 1 juli 2026 vanuit Salesforce verplicht worden. Voor deze datum kun je dit voor gebruikers met een systeembeheerders profiel activeren. Ga daarvoor naar Setup, Identiteitsverificatie en activeer de bijbehorende opties, conform het beleid van je organisatie:

Registreer je wachtwoordsleutel voor je account in de productieomgeving en herhaal deze stappen voor je eventuele Sandbox gebruikersaccounts. Kies uit een van de installatie methoden in Windows of Mac.

> ⚠ Registreer altijd een reservesleutel als back-up. Als je de enige sleutel verliest, word je geblokkeerd en moet je contact opnemen met Salesforce Support om de toegang te herstellen.

4. Installatie-instructies

Scenario A: Windows Hello (Windows)

Aanbevolen voor: Gebruikers van Windows 10/11 met een apparaat dat pincode, gezichtsherkenning of vingerafdrukontgrendeling ondersteunt.

1. Zorg dat Windows Hello is geconfigureerd op je apparaat (Instellingen, Accounts, Aanmeldingsopties).
2. Log in bij Salesforce en klik op je avatar rechtsboven. Kies Instellingen, Geavanceerde gebruikersgegevens.
3. Klik in het gedeelte App-registratie: Beveiligingssleutels en ingebouwde authenticators op Registreren.
4. De browser toont een Windows-beveiligingsvenster. Verifieer met je Windows Hello-methode (pincode, gezicht of vingerafdruk).
5. De registratie is voltooid. De sleutel wordt opgeslagen in de TPM (Trusted Platform Module) van het apparaat.

> ℹ Windows Hello-sleutels zijn apparaat gebonden — ze worden niet gesynchroniseerd naar andere apparaten. Registreer Windows Hello afzonderlijk op elk Windows-apparaat waarmee je Salesforce gebruikt.

Scenario B: Wachtwoordsleutel op iPhone, iPad of Android telefoon (Windows)

Aanbevolen voor: Gebruikers van Windows 10/11 in combinatie met een telefoon die biometrische inlogmethode ondersteund.

1. Log in bij Salesforce en klik op je avatar rechtsboven. Kies Instellingen, Geavanceerde gebruikersgegevens.
2. Klik in het gedeelte App-registratie: Beveiligingssleutels en ingebouwde authenticators op Registreren.
3. Er volgt een account-verificatie via e-mail. Geef de verificatiecode op die je via e-mail ontvangt.

4. Kies in het volgende scherm voor het registreren van de Beveiligingssleutel.
5. De browser toont een Windows-beveiligingsvenster om de wachtwoordsleutel op te slaan. Kies in het scherm voor de optie ‘Wijziging’ om de sleutel op te slaan op een ander apparaat dan een USB-sleutel/Security key.
6. Kies in het volgende scherm voor de optie iPhone, iPad of Android apparaat.
7. Scan de QR-code en voltooi de registratie van de wachtwoordsleutel in de wachtwoord manager van je telefoon.
8. Geef de Wachtwoordsleutel een naam om deze te herkennen voor jouw omgeving.

Scenario C: Apple Passkey (iCloud Keychain op Mac)

Aanbevolen voor: Mac-gebruikers die vertrouwd zijn met iCloud en de meest naadloze ervaring willen.

1. Log in bij Salesforce en klik op je avatar rechtsboven. Kies Instellingen, Geavanceerde gebruikersgegevens.
2. Klik in het gedeelte App-registratie: Beveiligingssleutels en ingebouwde authenticators op Registreren.
3. Scan de QR-code met je iPhone en bevestig het aanmaken op je telefoon.
4. De passkey wordt opgeslagen in iCloud Keychain en gesynchroniseerd naar andere Apple-apparaten die zijn aangemeld bij hetzelfde Apple-ID.

Scenario D: Fysieke beveiligingssleutel als YubiKey of Google Titan (Windows en Mac)

Aanbevolen voor: Organisaties met strikt beveiligingsbeleid, gedeelde werkstations, of gebruikers die de voorkeur geven aan een puur hardware-matige aanpak.

Dezelfde procedure als Scenario A. De stappen zijn identiek — sleutel insteken, browserprompt volgen. Je slaat nu de wachtwoordsleutel op in een speciale USB-sleutel van bijvoorbeeld YubiKey.

Scenario E: Externe wachtwoordmanager op (Windows en Mac)

Aanbevolen voor: Gebruikers die een platform-onafhankelijke oplossing willen of al gebruik maken van 1Password, Bitwarden, etc.

1. Zorg dat de browser extensie van je wachtwoordmanager is geïnstalleerd en actief is in Chrome of Edge.
2. Log in bij Salesforce en klik op je avatar rechtsboven. Kies Instellingen, Geavanceerde gebruikersgegevens.
3. Klik in het gedeelte App-registratie: Beveiligingssleutels en ingebouwde authenticators op Registreren.
4. Wanneer het passkey-dialoogvenster verschijnt, selecteer je de wachtwoordmanager uit de opties.
5. Bevestig in de extensie van de wachtwoordmanager met je hoofdwachtwoord of biometrie.
6. De passkey wordt opgeslagen in je kluis en is beschikbaar op elk apparaat waarop de wachtwoordmanager is geïnstalleerd.

5. SSO-gebruikers

Als jouw organisatie gebruik maakt van Single Sign-On (bijv. Azure AD, Okta, Ping), moet aan de phishing-resistente MFA-vereiste worden voldaan op het niveau van de identiteitsprovider (IdP), niet rechtstreeks in Salesforce.

- Je IdP moet ACR/AMR-signalen (RFC 8176) doorgeven die bevestigen dat een phishing-resistente methode is gebruikt.
- Als die signalen ontbreken, vraagt Salesforce de gebruiker om een gekwalificeerde methode rechtstreeks te registreren.