Azure MFA als authenticatiemiddel

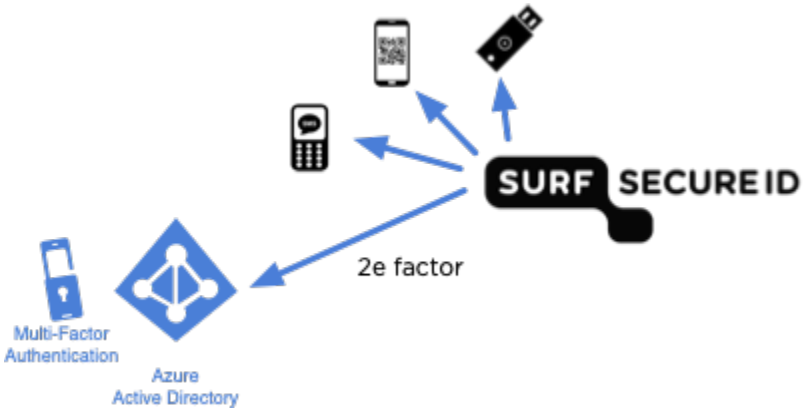
Achtergrond

Azure MFA en SURFsecureID ondersteunen elk verschillende typen 2FA-middelen. Voor gebruikers is het onhandig en verwarrend als zij verschillende 2FA-middelen naast elkaar moeten gebruiken. Bijvoorbeeld voor de ene applicatie de Microsoft Authenticator app en voor een andere applicatie de tiqr mobiele app.

We willen het mogelijk maken dat een instelling zowel Azure MFA als SURFsecureID kan gebruiken, terwijl de gebruiker maar één 2FA-middel hoeft te gebruiken. Als een gebruiker één van de Azure MFA middelen gebruikt (bijvoorbeeld de MS Authenticator app), kan hij dit middel ook in SURFsecureID registreren. Zo heeft de gebruiker maar één 2FA-middel en kan hij dit gebruiken voor diensten die Azure MFA of SURFsecureID gebruiken. En de diensten die via SURFsecureID zijn gekoppeld kunnen blijven vertrouwen op het hoog betrouwbaarheidsniveau van de gebruikersidentiteiten.

Koppeling met Azure AD

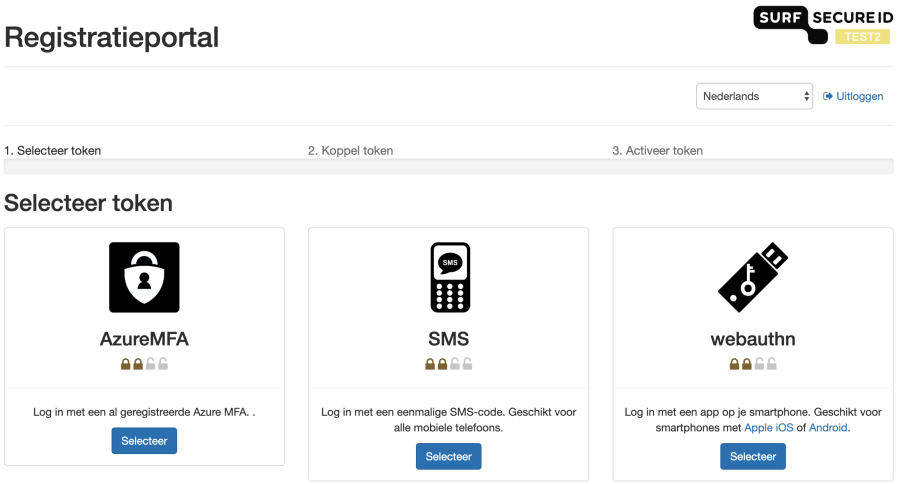
Volg de stappen op deze pagina om deze integratie te configureren in Azure AD.



Registratie Azure MFA middel door een gebruiker

Het uitgangspunt is dat een gebruiker al een Azure MFA middel heeft voordat hij dit bij SURFsecureID registreert. Hoewel de meesten de Microsoft Authenticator zullen gebruiken, maakt het in principe niet uit welk Azure MFA middel een gebruiker heeft.

Een eindgebruiker gaat naar het registratie portaal (test registratie portaal, afhankelijk van de SURFsecureID omgeving waarop je bent aangesloten) en kan daar nu Azure MFA als middel selecteren.



Voor de aanroep van Azure MFA gebruikt SURFsecureID het email adres van de gebruiker welke via de SURFconext login op het registratie portaal is verkregen. Het is dus belangrijk dat dit email adres hetzelfde is als waarmee een gebruiker door Azure AD wordt geïdentificeerd wordt.

RA activeert Azure MFA middel

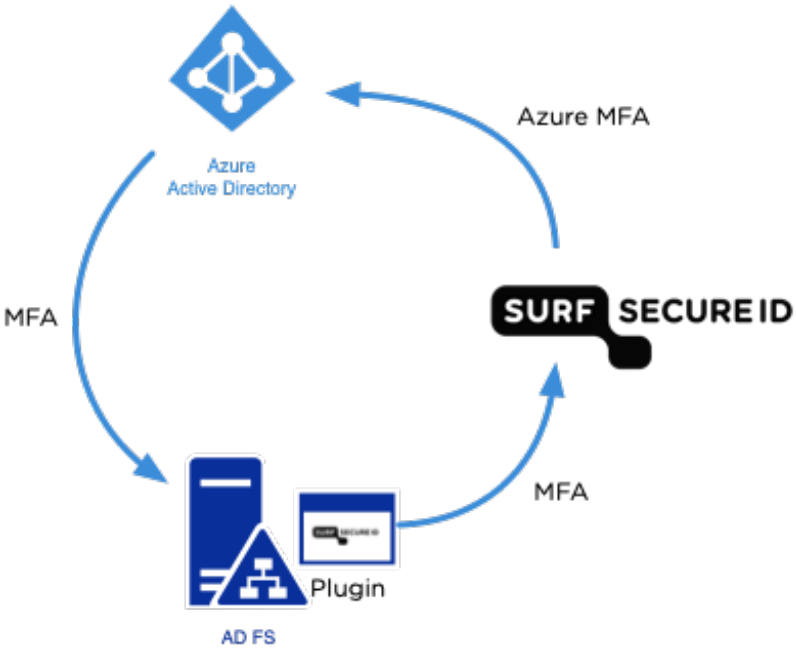
Het Azure MFA middel moet voor SURFsecureID geactiveerd worden door een RA(A). Hiertoe moet hetzelfde proces doorlopen worden als voor de andere tokens. Het enige verschil is dat de eindgebruiker tijdens dit proces niet het bezit van het Azure MFA token hoeft aan te tonen. De reden hiervoor is namelijk dat als deze stap nog wel uitgevoerd moest worden, de eindgebruiker zou moeten inloggen met zijn credentials op de computer van de RA(A). Vanuit security oogpunt is dit zeer ongewenst.

Let op voor authenticatie "loop"

Met het gebruik van deze feature bestaat er in een specifiek geval het risico dat er een authenticatie "loop" ontstaat. Dit kan optreden als je Azure MFA als SURFsecureID middel combineert met het uitbesteden van de MFA authenticatie in Azure AD aan SURFsecureID.

Dat zit zo:

1. Azure AD is geconfigureerd om de MFA uit te besteden aan ADFS. Je Azure AD domein is dan gefedereerd met je ADFS, én gebruikt de "supportsMFA=true" parameter.
2. Je ADFS gebruikt de SURFsecureID ADFS plugin om MFA verzoeken door SURFsecureID af te laten handelen.
3. De gebruiker heeft in SURFsecureID het Azure MFA middel gekozen en geregistreerd. Hierdoor wordt de 2e factor voor deze gebruiker uitbesteed aan Azure AD.
4. goto (1)



Om deze authenticatie "loop" te voorkomen zul je:

- bij gebruik van Azure MFA als SURFsecureID middel, niet SURFsecureID gebruiken om de MFA voor diensten achter Azure AD af te handelen.
- òf als je SURFsecureID gebruikt voor de MFA van diensten achter Azure AD, niet Azure MFA als middel toestaan.

Ondersteuning

Voor technische hulp en vragen kun je contact opnemen met support@surfconext.nl. Noem duidelijk in het onderwerp en de email zelf dat het gaat om testen met de Azure MFA integratie met SURFsecureID.