Handleiding inloggen op de RA omgeving (macOS)

Remote Access Microdata

Voorwoord

Welkom bij dit document dat is ontworpen om u te begeleiden bij het opzetten van een verbinding naar de Remote Access omgeving op een macOS-systeem. Deze specifieke omgeving maakt gebruik van een VPN in combinatie met RSA tokens voor sterke authenticatie, wat een veilige toegang tot de Remote Access omgeving waarborgt.

In de volgende secties worden de stappen gedetailleerd beschreven die moeten worden uitgevoerd om met succes een verbinding tot stand te brengen met de Remote Access omgeving.

Inhoudsopgave

Installatievoorbereiding en systeemeisen

Voordat u begint met het opzetten van de Remote Access Microdata-sessie, is het essentieel ervoor te zorgen dat uw werkplek aan bepaalde voorwaarden voldoet. Hieronder volgen de installatievoorbereidingen en systeemeisen:

1. **VPN Client:**
   - Zorg ervoor dat de door het CBS verstrekte VPN-client op uw werkplek is geïnstalleerd.

2. **VMware Horizon Client:**
   - Installeer de VMware-client op uw systeem. U kunt de meest recente versie verkrijgen vanaf de officiële VMware-website via de volgende link voor Mac: klik hier
   - Selecteer bij "Select Version" de laatste beschikbare versie en volg de instructies om de client te downloaden en te installeren.

3. **Systeemeisen voor Remote Access Microdata-sessie:**
   - Het systeem dat wordt gebruikt om de Remote Access Microdata sessie mee op te zetten moet voldoen aan de volgende eisen.
   - We hanteren bij het CBS een T-1 beleid, wat inhoud dat de Horizon Client en het OS moet voldoen aan specifieke eisten. Op de RA informatiepagina is verdere informatie hierover te vinden.

Benodigde Internet Connectiviteit
Onderstaand verkeer naar de VPN gateway (87.213.43.223) IPSEC and IKE (UDP on port 500) FW1_scv_keep_alive (UDP port 18233) HTTPS (TCP 443)

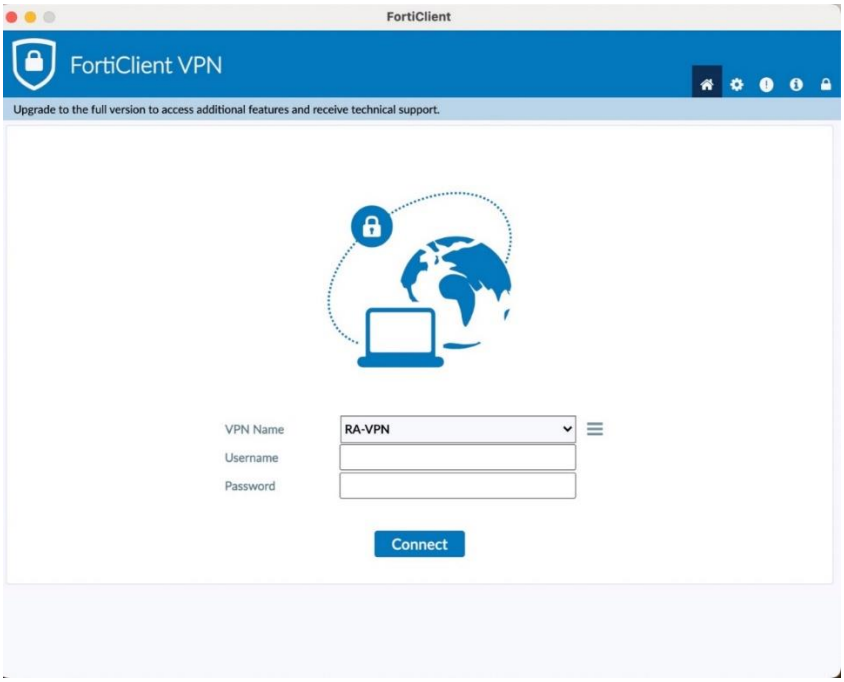
Opzetten VPN verbinding in FortiVPN client

Voordat u toegang kunt krijgen tot de Remote Access-omgeving, is het noodzakelijk om een VPN-verbinding met het CBS op te zetten.

Dit gaat als volgt:

1. Open de **FortiVPN client** op uw laptop of desktop

Onderstaande scherm verschijnt.



Bent u in het bezit van een (fysieke) RSA hardware token, vul dan het volgende in:

- bij Username: uw 4 letterige gebruikersnaam (zonder @remoteaccess.cbs.nl)
- bij Password: de PIN code + RSA tokencode van de hardware token (zonder de '+' teken).

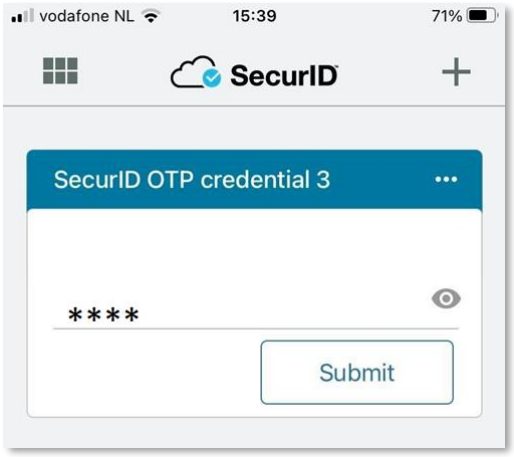
Bent u in het bezit van een RSA software token, volg dan de stappen hieronder:

Kanttekening: De RSA applicatie op uw telefoon laat altijd een 8 cijferige tokencode zien. Ook wanneer u het veld leeg laat OF een incorrecte PIN ingeeft. Dit vanwege beveiligingsredenen.

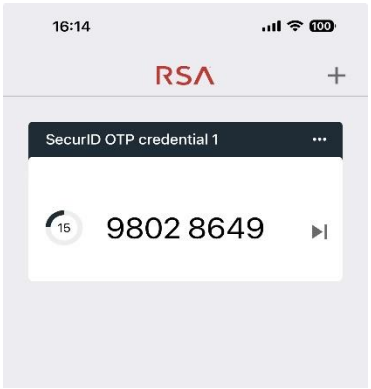
Tip: wanneer u twijfelt of u wel uw correcte persoonlijke PIN hebt ingegeven, sluit de RSA applicatie dan af en begin opnieuw.

Om in te loggen met het RSA software token in de FortiVPN client, ga als volgt te werk:

1. Start de **RSA applicatie** op het mobiele apparaat en open de **FortiVPN client** op uw laptop of desktop.
2. In **FortiVPN client**, bij **Username**, vul uw **4 letterige gebruikersnaam** in.
3. Vul uw **persoonlijke PIN** in de **RSA applicatie** en druk op **Submit**

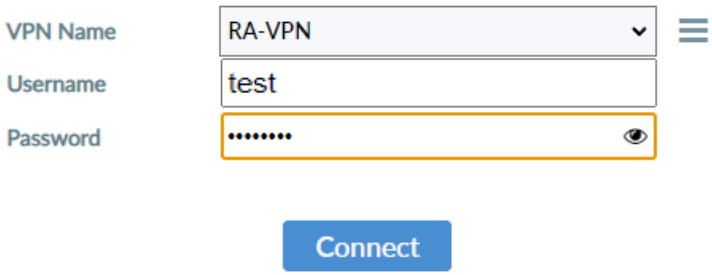


4. Vervolgens wordt de 8 cijferige tokencode gegenereerd.



Opmerking: Een tokencode kan niet meerdere malen gebruikt worden. Heeft u bijvoorbeeld een foutieve PIN code gebruikt en wilt u opnieuw inloggen, dan dient u te wachten totdat er een nieuwe tokencode verschijnt op het token

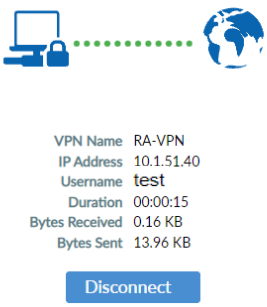
5. Vul deze 8 cijfers in FortiVPN client bij **Password** en druk op **Connect**



OPMERKING Wanneer FortiVPN client vraagt om een **'SMS'** en/of **'Answer'** na het invoeren van een correcte tokencode, wacht dan tot de 8 cijferige tokencode in de RSA applicatie verspringt naar een nieuwe tokencode en voer vervolgens de nieuwe tokencode in.

Na 5x foutief inloggen is uw token vergrendeld en dient u contact op te nemen met Microdata Services.

6. Het volgende scherm verschijnt als er succesvol een VPN-verbinding is opgezet met het CBS.



Door deze verbinding worden alle internet en netwerkverbindingen geblokkeerd en kan er alleen verbinding worden gemaakt met de Remote Access-omgeving van het CBS.

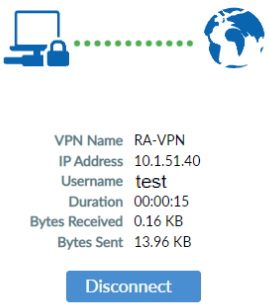
Als er succesvol een VPN is opgezet is het enkel mogelijk om naar de CBS Remote Access omgevingen te connecteren. Andere internet en netwerk adressen zijn niet benaderbaar.

Tip: Om de VPN verbinding af te breken, klik op het FortiVPN client icoon boven in het MacOS scherm en kies voor **Disconnect RA-VPN**. Hierna zijn alle internet en netwerk adressen weer benaderbaar.

Configuratie van de VMware Horizon Client en verbinding met de RA-omgeving

De initiële configuratie van de VMware-client is een essentiële stap bij het voor de eerste keer gebruiken ervan. Volg onderstaande stappen om dit te voltooien:

1. Zet een **VPN verbinding** op in de **FortiVPN client**

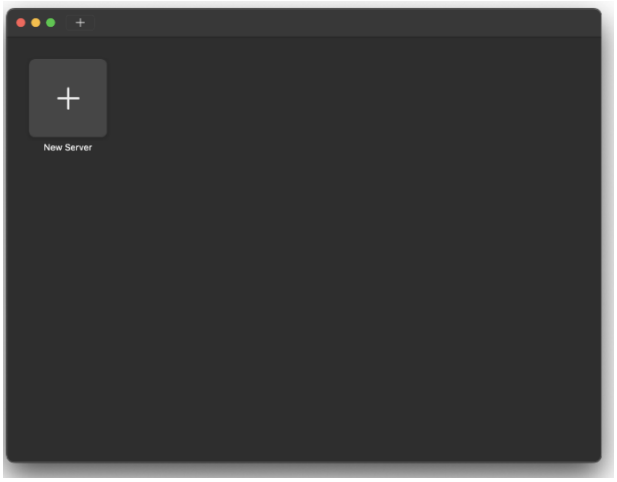


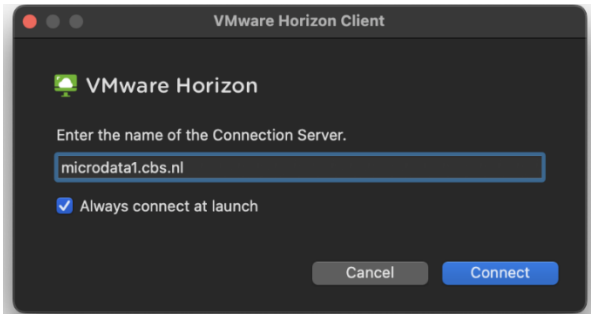
2. Open **VMware Horizon Client**

Als u de VMware-client nog niet heeft geïnstalleerd, volg dan de installatie-instructies zoals eerder vermeld.

*De download link is hierboven te vinden bij **Installatievoorbereiding en systeemeisen***

3. Klik op **Add Server**, vul vervolgens **"microdata1.cbs.nl"** in als het adres van de server.

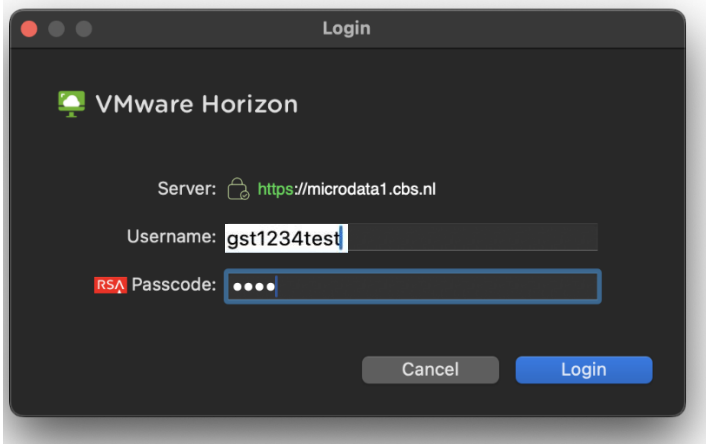




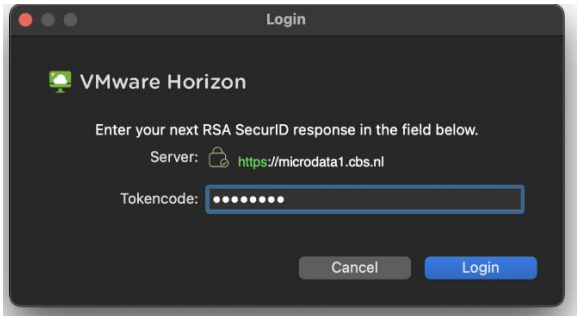
4. Klik op **Accept**

5. Vul bij **Username** uw **Microdata accountnaam** in **(gst-projectnr-gebruikersnaam)**
6. Vul bij **RSA Passcode** het **projectnummer** in

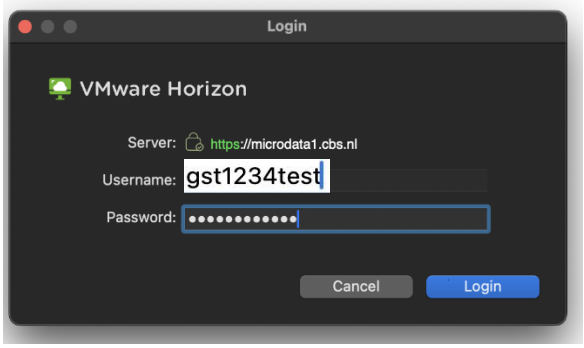
   bijvoorbeeld als uw Microdata accountnaam: gst1234test is, dan is de RSA Passcode: 1234.
7. Klik vervolgens op **Login**



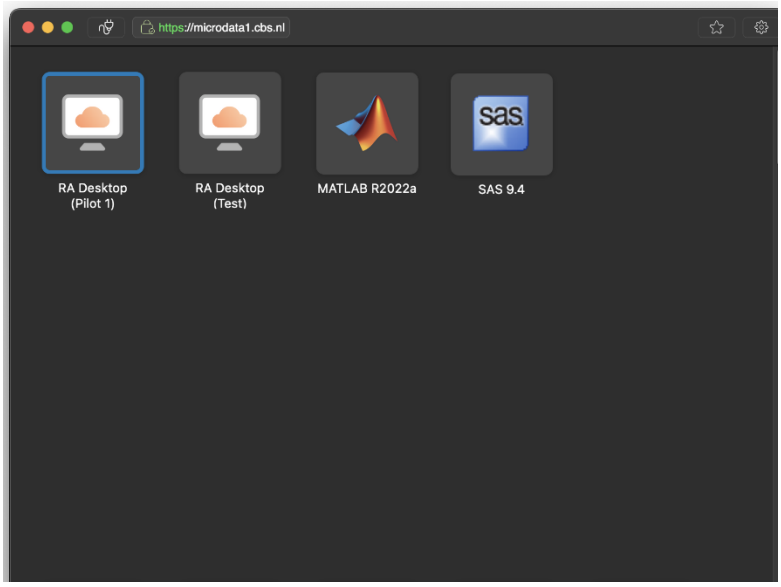
8. Een **8-cijferige toegangscode** is naar uw **mobiele telefoon** verzonden voor verificatie. Voer de ontvangen code in het volgende scherm in om in te loggen.
9. Klik op **Login**



10. Vul in het volgende scherm het wachtwoord van het Microdata account in.
11. Klik op **Login**



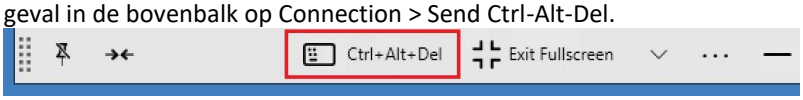
U bent nu ingelogd in de VMware Microdata omgeving en er kan nu een applicatiesessie worden gestart.



Om een applicatie te starten, dubbelklik op het pictogram van de applicatie

Nuttige informatie

CTRL + ALT + DEL
Als de sessie is vergrendeld, staat er op het scherm dat CTRL + ALT + DEL ingedrukt moet worden. Druk hierbij als je op een Windows computer werkt niet de toetsen op het toetsenbord in, maar gebruik de CTRL + ALT + DEL knop in de grijze bovenbalk om de sessie te ontgrendelen(zie hieronder). Werk je op MacOS? Klik in dat geval in de bovenbalk op Connection > Send Ctrl-Alt-Del.



Snelkoppelingen aanmaken
Je kunt snelkoppelingen aanmaken op het bureaublad als alternatief voor de favorietenlijst in de tegel interface. Om een snelkoppeling te plaatsen, kan je eerst het start menu openen via de Start knop links onder in beeld. Klik vervolgens op “Alle apps”. Nu verschijnt er een lijst met alle applicaties waar jij toegang tot hebt. Sleep jouw favoriete applicaties vanuit deze lijst naar het bureaublad om daar een snelkoppeling van te maken.

Verbinding verbreken, vergrendelen of afmelden

- Vergrendelen van het scherm: Als je wegloopt van jouw werkplek kan je het beste kiezen voor het vergrendelen van het scherm. Deze optie vindt je in het Start menu. Open het Start menu, klik op het grijze rondje met het poppetje erin en kies voor “Vergrendelen”:

- Verbinding verbreken: Heb je nog scripts of verwerkingen lopen die door moeten gaan? Verbreek dan de verbinding via de balk bovenaan het scherm. Klik in de bovenbalk op het kruisje om de verbinding te verbreken:

- Afmelden: Ben je klaar met jouw werk en is alles opgeslagen en afgesloten? Meld dan de sessie af. Het is aan te raden om deze optie zo veel mogelijk te gebruiken. Daarmee blijft de omgeving het meest stabiel werken. Je vindt deze optie ook in het Start menu. Open het Start menu, klik op het grijze rondje met het poppetje erin en kies voor “Afmelden”: