Citrix Secure Access voor Android

Contents

Citrix Secure Access voor Android-apparaten **2**

Citrix Secure Access gebruiken vanaf uw Android-apparaat **2**

Verbinding maken met uw bedrijfsnetwerk via Citrix SSO Secure Access, geconfigureerd in een Intune-omgeving **11**

Citrix Secure Access voor Android-apparaten

March 15, 2024

De Citrix Secure Access-client voor Android (voorheen bekend als de Citrix SSO-app voor Android) is de beste oplossing op de markt voor toegang tot toepassingen en gegevensbescherming via NetScaler Gateway. U kunt nu altijd en overal veilig toegang krijgen tot bedrijfskritieke toepassingen, virtuele bureaubladen en bedrijfsgegevens.

> **Opmerkingen:**
>
> - Vanaf versie 23.12.1 wordt Citrix SSO voor Android gewijzigd naar Citrix Secure Access. We werken onze documentatie en de schermafbeeldingen van de gebruikersinterface bij om deze naamswijziging weer te geven.
> - Voor beheerdersspecifieke instructies over Citrix Secure Access voor Android, zie Citrix Secure Access voor Android-apparaten.

Citrix Secure Access gebruiken vanaf uw Android-apparaat

March 15, 2024

> **Opmerkingen:**
>
> - Vanaf versie 23.12.1 wordt Citrix SSO voor Android gewijzigd naar Citrix Secure Access. We werken onze documentatie en de schermafbeeldingen van de gebruikersinterface bij om deze naamswijziging weer te geven.
> - Voor beheerdersspecifieke instructies over het gebruik van Citrix Secure Access voor Android, zie Citrix Secure Access voor Android-apparaten..

Installeer Citrix Secure Access vanuit de Play Store. Gebruikers die voor het eerst verbinding maken, moeten een verbinding met NetScaler Gateway maken door de server in een niet-MDM-implementatie toe te voegen. Hierna kunt u verbinding maken met een bestaande verbinding of een verbinding toevoegen. U kunt ook bestaande verbindingen bewerken, indien uw beheerder dit toestaat in een MDM-implementatie. U kunt ook de logboeken bekijken en daarna toepasselijke acties ondernemen.

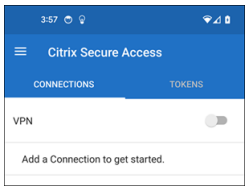
> **Opmerkingen:**
>
> - Via MDM geïmplementeerde verbindingen kunnen niet worden bewerkt.

> - Vanaf Citrix SSO voor Android 23.8.1 wordt u mogelijk gevraagd om toestemming voor Query all packages te geven aan de Citrix SSO-app. Zodra de toestemming is verleend, zal de Citrix SSO-app:
>
>   – Receives the package install notification from the operating system.
>   – Restarts the Always On VPN.
>
> Wanneer u voor de eerste keer verbinding maakt met uw VPN-profiel, wordt u gevraagd om toestemming te geven (vereist volgens het beleid van Google) dat informatie over het geïnstalleerde pakket wordt verzameld. Als u toestemming geeft, wordt de VPN-verbinding tot stand gebracht. Als u de toestemming weigert, wordt de VPN-verbinding verbroken. Het toestemmingsscherm verschijnt niet opnieuw nadat de toestemming is verleend.

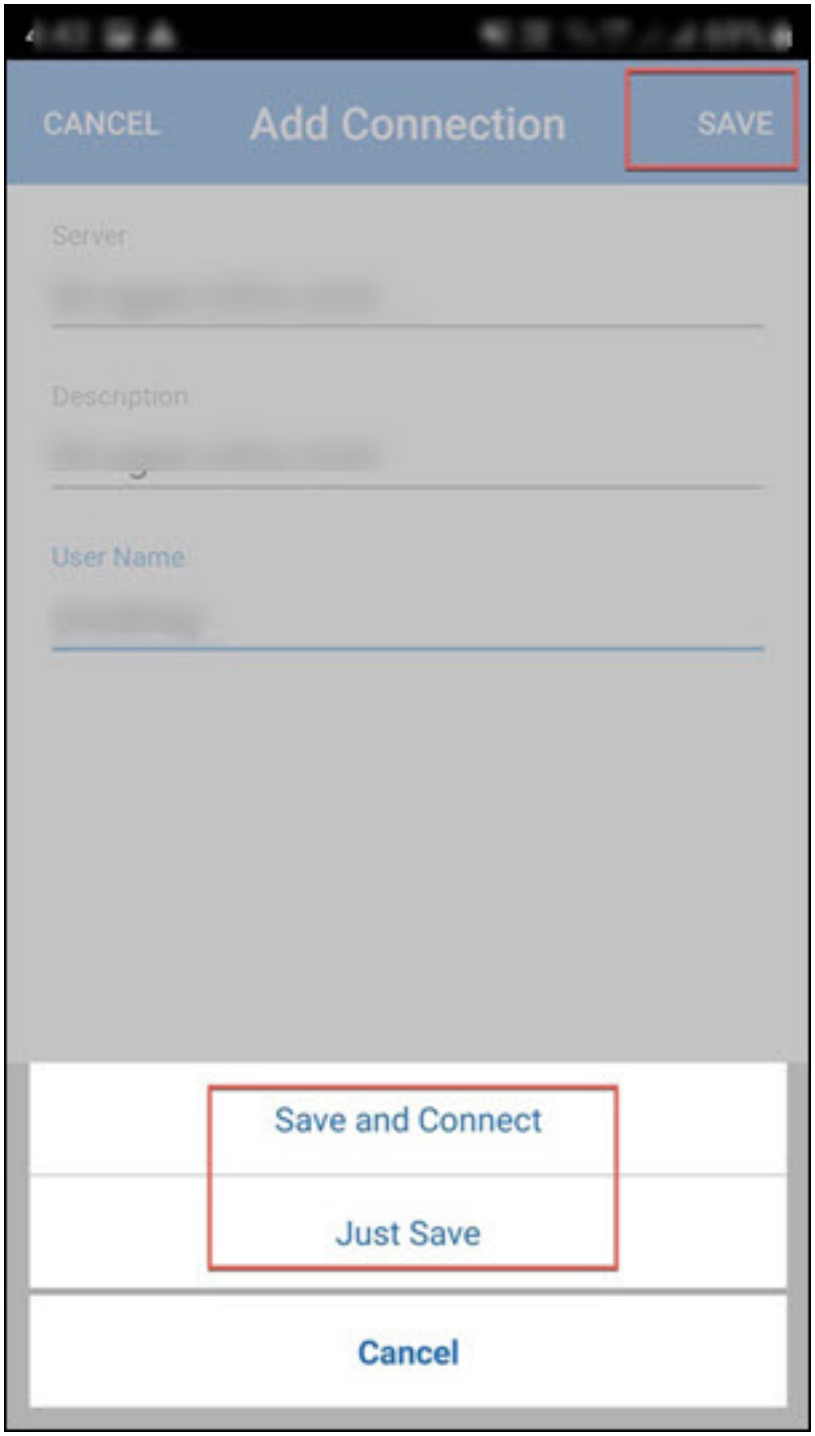
Een verbinding toevoegen

Opmerking: Deze stap is alleen vereist in een niet-MDM-implementatie.

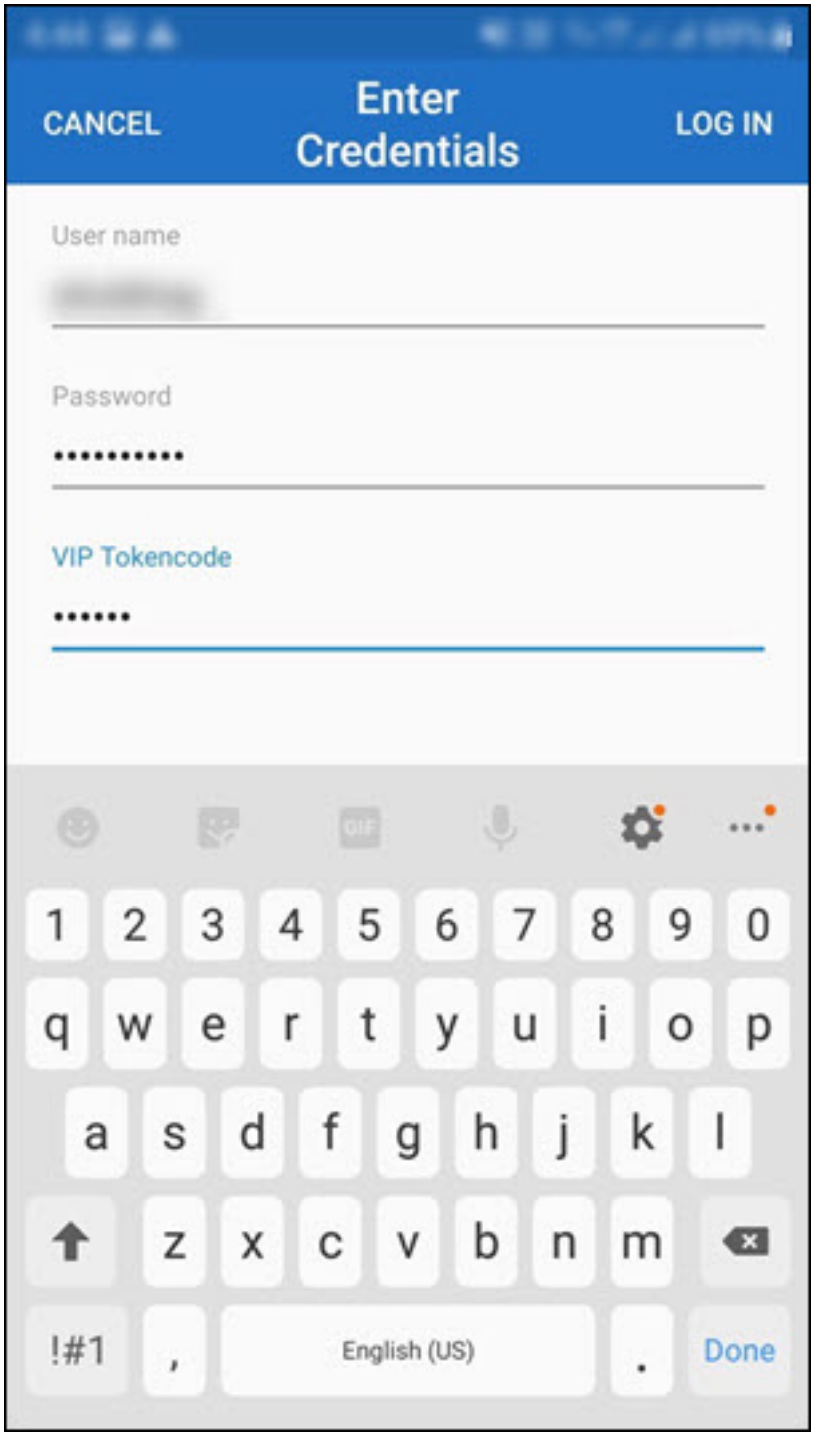
Nadat u Citrix Secure Access hebt geïnstalleerd en de app hebt geopend op uw Android-apparaat, verschijnt het volgende scherm.



1. Klik op **+** om een verbinding toe te voegen.
2. Voer de basis-URL (bijvoorbeeld https://gateway.mycompany.com) en de naam voor de VPN-verbinding in. U kunt optioneel de gebruikersnaam invoeren.
3. Klik op **Opslaan** en klik daarna op de optie **Opslaan en verbinden** of **Gewoon opslaan**.

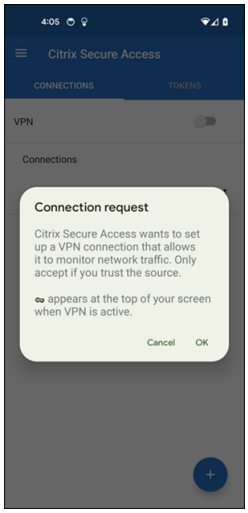


4. Geef referenties voor verificatie van de server op en tik op **AANMELDEN** of **Voltooid** op het toetsenblok.

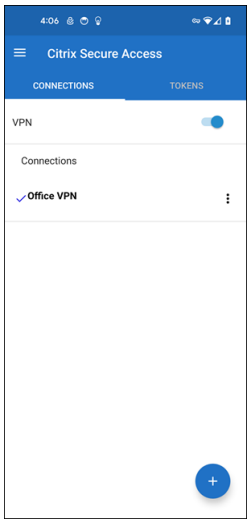


Het aanvraagbericht voor de verbinding verschijnt. Klik op **OK**.

Opmerking: Dit bericht verschijnt alleen de eerste keer dat een VPN-verbinding tot stand wordt gebracht door Citrix Secure Access. Als de gebruiker de eerste keer de verbinding toestaat, wordt dit bericht niet opnieuw weergegeven totdat de gebruiker de app verwijdert en opnieuw installeert.



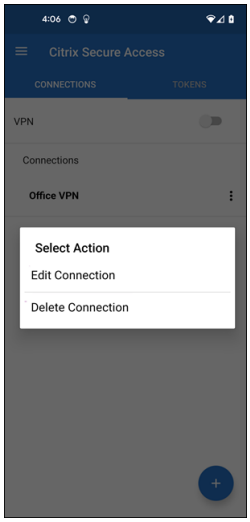
Opmerking: Als u zich wilt afmelden bij Citrix Secure Access, zet u de **VPN-schakelaar** UIT.



Een bestaande verbinding wijzigen of verwijderen

U kunt een verbinding bewerken of verwijderen nadat u zich bij Citrix Secure Access hebt afgemeld.

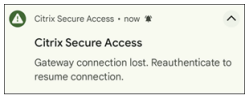
Tik op de servernaam en houd deze vast en selecteer **Verbinding bewerken** of **Verbinding verwijderen**.



Maak opnieuw verbinding met NetScaler Gateway na een mislukte VPN-verbinding - Preview

Vanaf versie 23.10.1 vraagt Citrix SSO voor Android u om u opnieuw te verifiëren bij NetScaler Gateway wanneer een VPN-verbinding wordt verbroken. In de gebruikersinterface en in het meldingenpaneel van uw Android-apparaat wordt aangegeven dat de verbinding met de NetScaler Gateway is verbroken en dat u zich opnieuw moet verifiëren om de verbinding te hervatten.

> **Opmerking:**
>
> Deze functie is in preview.

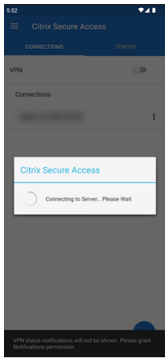


Meldingen ontvangen of blokkeren op Android 13+ apparaten

Vanaf Citrix Secure Access voor Android versie 23.12.1 wordt u bij de installatie of herinstallatie van de Citrix Secure Access-client op Android 13+ apparaten gevraagd toestemming te geven voor het ontvangen van meldingen van de Citrix Secure Access-client. Als u de toestemming weigert, ontvangt u geen VPN-status of pushmeldingen van de Citrix Secure Access-client op uw Android-apparaat.

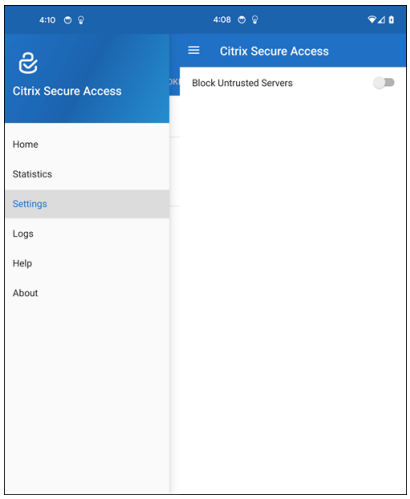
U kunt op uw Android-apparaat naar **Instellingen > Meldingen** gaan om de meldingsmachtigingen te wijzigen.

In het volgende voorbeeld zijn de VPN-statusmeldingen uitgeschakeld.



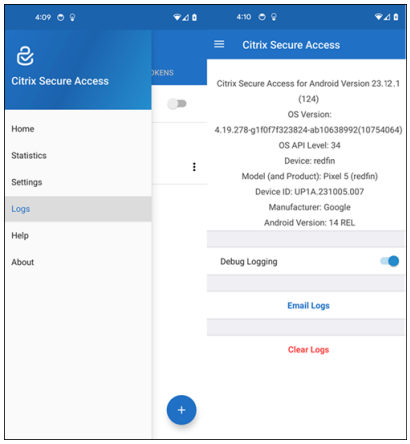
Niet-vertrouwde servers blokkeren

Citrix Secure Access maakt standaard geen verbinding met niet-vertrouwde servers. Niet-vertrouwde servers zijn servers die zelfondertekende certificaten gebruiken of die geen vertrouwd basiscertificaat hebben voor de gateway. Als u dergelijke verbindingen wilt toestaan, dan zet u de **Niet-vertrouwde servers blokkeren** schakelaar **UIT**.



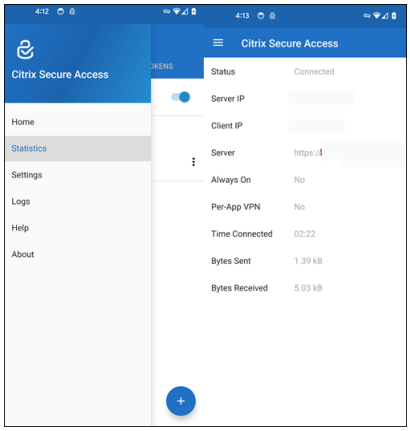
Foutopsporingslogboeken inschakelen

Het vastleggen van foutopsporingslogboeken is een cruciaal onderdeel van het oplossen van problemen of het melden van problemen aan Citrix Support.
Tik op de knop **Logboekregistratie foutopsporing** om foutopsporing voor Citrix Secure Access **AAN** te zetten. U kunt de logboeken e-mailen bij het oplossen van verbindingsproblemen via de koppeling **Logboeken e-mailen**.



Statistieken weergeven

U kunt de verbindingsstatistieken weergeven wanneer VPN is verbonden.



Wachtwoordtokens

U kunt een 6-cijferig wachtwoordtoken toevoegen als een tweede verificatiefactor. Deze code gebruikt het op tijd gebaseerde eenmalige wachtwoordprotocol om de OTP-code te genereren.

U kunt handmatig een wachtwoordtoken toevoegen of een wachtwoordtoken registreren met behulp van de QR-code scanmethode. Verificatie in twee stappen met behulp van pushmeldingen is niet ingeschakeld als u kiest om het token handmatig in te voeren.

Een wachtwoordtoken registreren

1. Meld u aan bij de pagina voor het beheren van eenmalige PIN's van uw organisatie in de webbrowser van een desktop of laptop.

2. Klik op **Apparaat toevoegen**.
3. Voer een naam in voor uw apparaat en klik op **Ga**.

   Er wordt een QR-code gegenereerd.

Voeg een wachtwoordtoken toe door de QR-code in de browser te scannen

1. Navigeer naar het tabblad **Tokens** in het **beginscherm**.
2. Tik op **+** en tik op **QR-code scannen**.
3. Stel de camera scherp op de QR-code in uw browser.

Citrix Secure Access vult automatisch de apparaatnaam en de geheime sleutel in.

U kunt de geheime sleutel die boven de QR-code verschijnt ook handmatig invoeren.

Citrix Secure Access valideert de QR-code en registreert vervolgens bij de gateway voor push-meldingen. Als er geen fouten zijn in het registratieproces, wordt het token aan het tabblad Tokens toegevoegd.

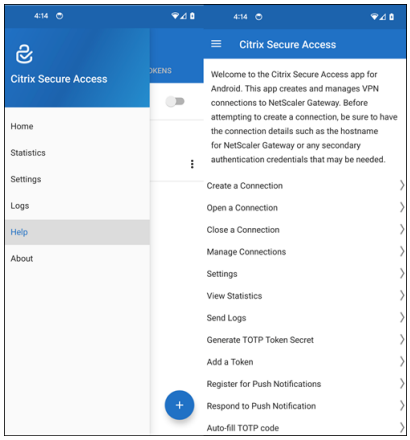
> **Opmerking:**
>
> - U moet de camera voor Citrix Secure Access machtigen om de QR-code vast te leggen.
> - U moet de PIN/het wachtwoord van het apparaat inschakelen op uw apparaat.

Een wachtwoordtoken handmatig toevoegen

1. Navigeer naar het tabblad **Tokens** in het **beginscherm**.
2. Tik op + en tik op **Handmatig invoeren**.
3. Voer de apparaatnaam en de geheime sleutel in zoals deze worden weergegeven op het in de browser gegenereerde wachtwoordtoken.

Help-onderwerpen

Zie **Help** voor meer informatie over het gebruik van Citrix Secure Access.



Verbinding maken met uw bedrijfsnetwerk via Citrix SSO Secure Access, geconfigureerd in een Intune-omgeving

March 15, 2024

> **Opmerking:**
>
> Voor beheerdersspecifieke instructies over Citrix Secure Access voor Android, zie Citrix Secure Access voor Android-apparaten.

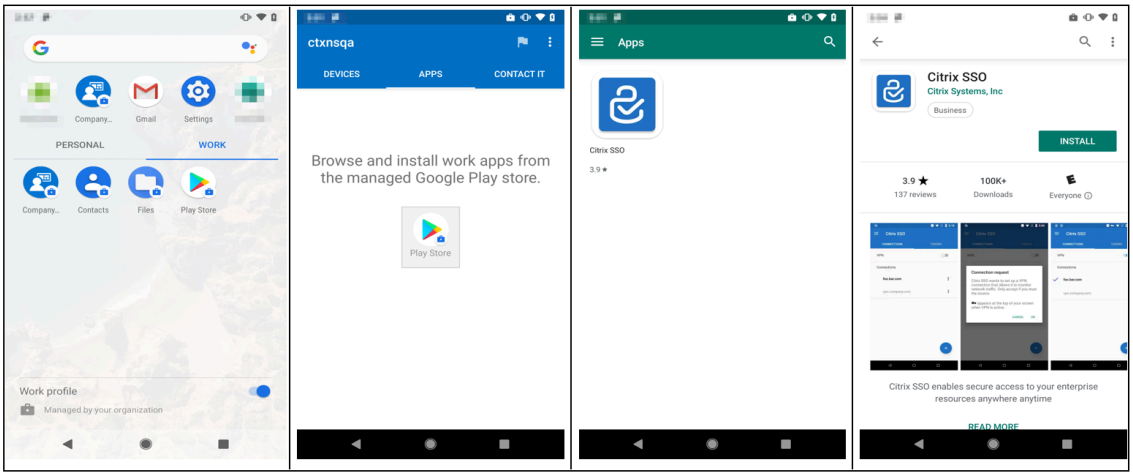
In dit onderwerp worden de stappen beschreven om verbinding te maken met uw bedrijfsnetwerk met behulp van de Citrix Secure Access-client die in een Microsoft Intune Android Enterprise-omgeving is geconfigureerd.

Aannames:

- U hebt het apparaat geregistreerd in Intune met behulp van de Intune-bedrijfsportal-app.
- Het werkprofiel voor de gebruiker is ingesteld op het apparaat.

1. Open de **Intune-bedrijfsportal-app** op het apparaat vanuit het werkprofiel.
2. Klik op het menu met de drie puntjes om instellingen voor de app te openen en schuif naar de onderkant van het scherm. Tik op **SYNC** om te synchroniseren met de Intune-server en navigeer vervolgens naar het hoofdscherm van de app.
3. Tik op het tabblad **APPS** en tik op de koppeling **Beheerde Google Play Store**.

   De lijst met goedgekeurde apps voor de gebruiker wordt weergegeven.



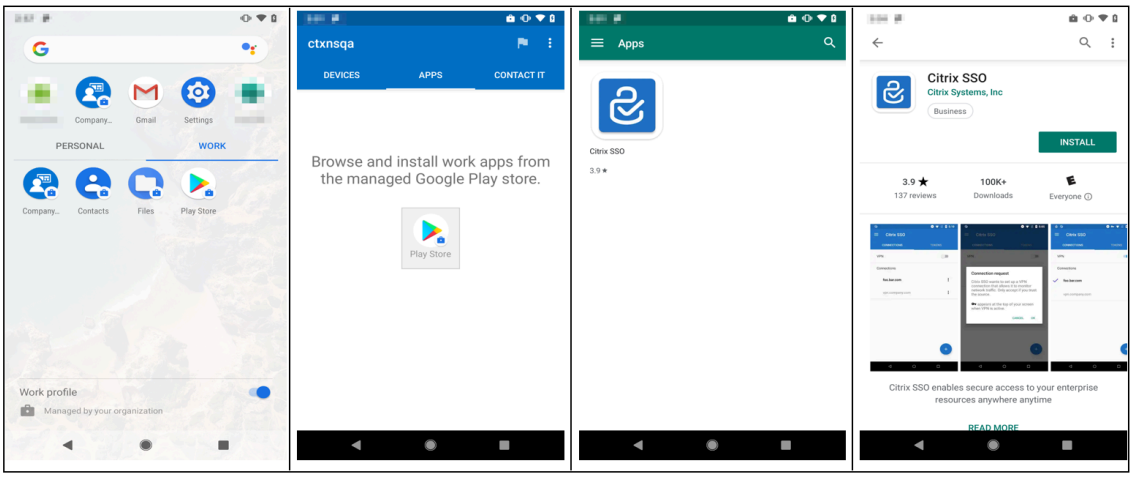
4. Tik op **Citrix Secure Access**.

   De Citrix Secure Access-client verschijnt in de beheerde Google Play Store.

5. Tik op **INSTALLEREN**.

6. Ga terug naar de lijst met apps voor uw werkprofiel. De Citrix Secure Access wordt toegevoegd aan de lijst met geïnstalleerde apps.

7. Tik op het Citrix Secure Access-pictogram in de lijst met apps bij het **WERK**profiel om de app te openen.



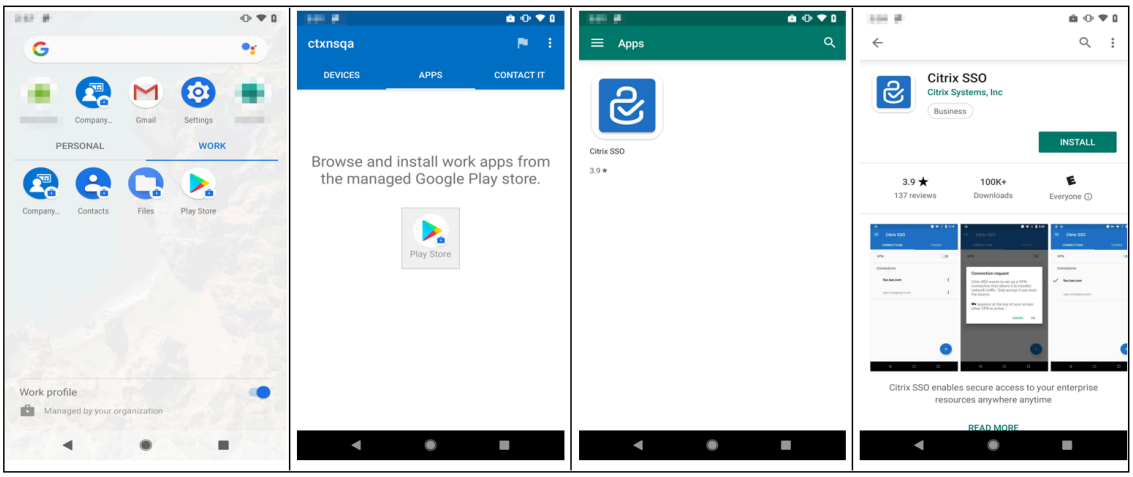
   Citrix Secure Access wordt geopend. U wordt gevraagd om machtiging te verlenen of te weigeren om veilig met het interne netwerk van uw bedrijf te communiceren.

8. Tik op **TOESTAAN** om de machtiging te verlenen. Citrix Secure Access wordt gesloten als u **NIET TOESTAAN** kiest en u kunt de Citrix Secure Access-client niet gebruiken.

   > **Opmerking:**
   >
   > U wordt mogelijk gevraagd om **machtiging te verlenen of te weigeren om telefoonge-**

> **sprekken te beheren en te voeren** (indien dit nog niet via Intune is verleend). Tik op **Toestaan** om machtiging te verlenen. U kunt deze machtiging weigeren, maar als Intune NAC-controle vereist is voor apparaatverificatie op NetScaler Gateway, kunt u geen verbinding maken met uw interne bedrijfsnetwerk totdat u deze machtiging hebt verleend.

9. De **My Corporate VPN** (of de naam die u hebt gekozen in de Citrix Secure Access-configuratie in Intune) wordt weergegeven in de sectie Beheerde verbindingen van het tabblad **VERBINDINGEN**. Tik op deze verbinding. U wordt gevraagd om de referenties te verifiëren bij NetScaler Gateway.
10. Voer de referenties in voor verificatie bij NetScaler Gateway en tik op **AANMELDEN**.



Mogelijk wordt u gevraagd om een certificaat te selecteren als clientcertificaatverificatie in NetScaler Gateway is geconfigureerd. U kunt toegang geven tot het certificaat.

11. U wordt door het Android-systeem gevraagd om **Verbindingsaanvraag** voor VPN-tunnelconfiguratie toe te staan. Tik op **OK** om Citrix Secure Access te machtigen om een veilige verbinding tot stand te brengen met uw interne bedrijfsnetwerk.

    Opmerking: deze prompt wordt alleen weergegeven wanneer u voor het eerst een beveiligde verbinding met NetScaler Gateway tot stand brengt. Bij latere verbindingspogingen wordt de prompt niet weergegeven totdat Citrix Secure Access is verwijderd en daarna opnieuw op het apparaat is geïnstalleerd.

U bent verbonden met uw interne bedrijfsnetwerk. Er verschijnt een sleutelpictogram in de statusbalk van het apparaat ten teken dat de VPN-verbinding actief is. Het VPN-servicemeldingspictogram van de Citrix Secure Access-client verschijnt ook op de statusbalk. De status van de verbindingsschakelaar verandert in verbonden en er verschijnt een vinkje naast de naam van het VPN-profiel.