Citrix Secure Access für Android

Contents

Citrix Secure Access für Android-Geräte

March 15, 2024

Der Citrix Secure Access Client für Android (früher bekannt als Citrix SSO-App für Android) bietet eine erstklassige Lösung für Anwendungszugriff und Datensicherung über NetScaler Gateway. Sie können nun überall und jederzeit sicher auf wichtige Anwendungen, virtuelle Desktops und Unternehmensdaten zugreifen.

> **Hinweise:**
>
> - Ab Version 23.12.1 wird Citrix SSO für Android in Citrix Secure Access umbenannt. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.
> - Administratorspezifische Anweisungen zu Citrix Secure Access für Android finden Sie unter Citrix Secure Access für Android-Geräte.

Citrix Secure Access auf dem Android-Gerät verwenden

March 15, 2024

> **Hinweise:**
>
> - Ab Version 23.12.1 wird Citrix SSO für Android in Citrix Secure Access umbenannt. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.
> - Administratorspezifische Anweisungen zur Verwendung von Citrix Secure Access für Android finden Sie unter Citrix Secure Access für Android-Geräte.

Installieren Sie Citrix Secure Access über den Play Store. Erstbenutzer müssen eine Verbindung mit NetScaler Gateway herstellen, indem sie den Server im Nicht-MDM-Modus hinzufügen. Bei nachfolgender Verwendung können Sie eine Verbindung zu einer vorhandenen Verbindung herstellen oder eine Verbindung hinzufügen und vorhandene Verbindungen bearbeiten, sofern Ihr Administrator dies in einer MDM-Bereitstellung zulässt. Sie können die Protokolle anzeigen und entsprechende Aktionen durchführen.

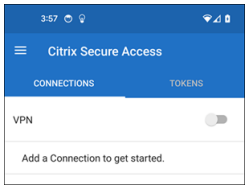
> **Hinweise:**
>
> - Verbindungen, die über MDM bereitgestellt werden, können nicht bearbeitet werden.

> - Ab Citrix SSO für Android 23.8.1 werden Sie möglicherweise aufgefordert, der Citrix SSO-App die Zustimmung Query all packages zu erteilen. Sobald die Zustimmung erteilt wurde, gilt für die Citrix SSO-App:
>
>   - Receives the package install notification from the operating system.
>   - Restarts the Always On VPN.
>
>   Wenn Sie sich zum ersten Mal mit Ihrem VPN-Profil verbinden, werden Sie aufgefordert, Ihre Zustimmung (gemäß den Google-Richtlinien erforderlich) zur Erfassung von Informationen über das installierte Paket zu erteilen. Wenn Sie die Zustimmung erteilen, wird die VPN-Verbindung initiiert. Wenn Sie die Zustimmung verweigern, wird die VPN-Verbindung abgebrochen. Die Seite zur Zustimmung wird nicht wieder angezeigt, wenn die Zustimmung erteilt wurde.

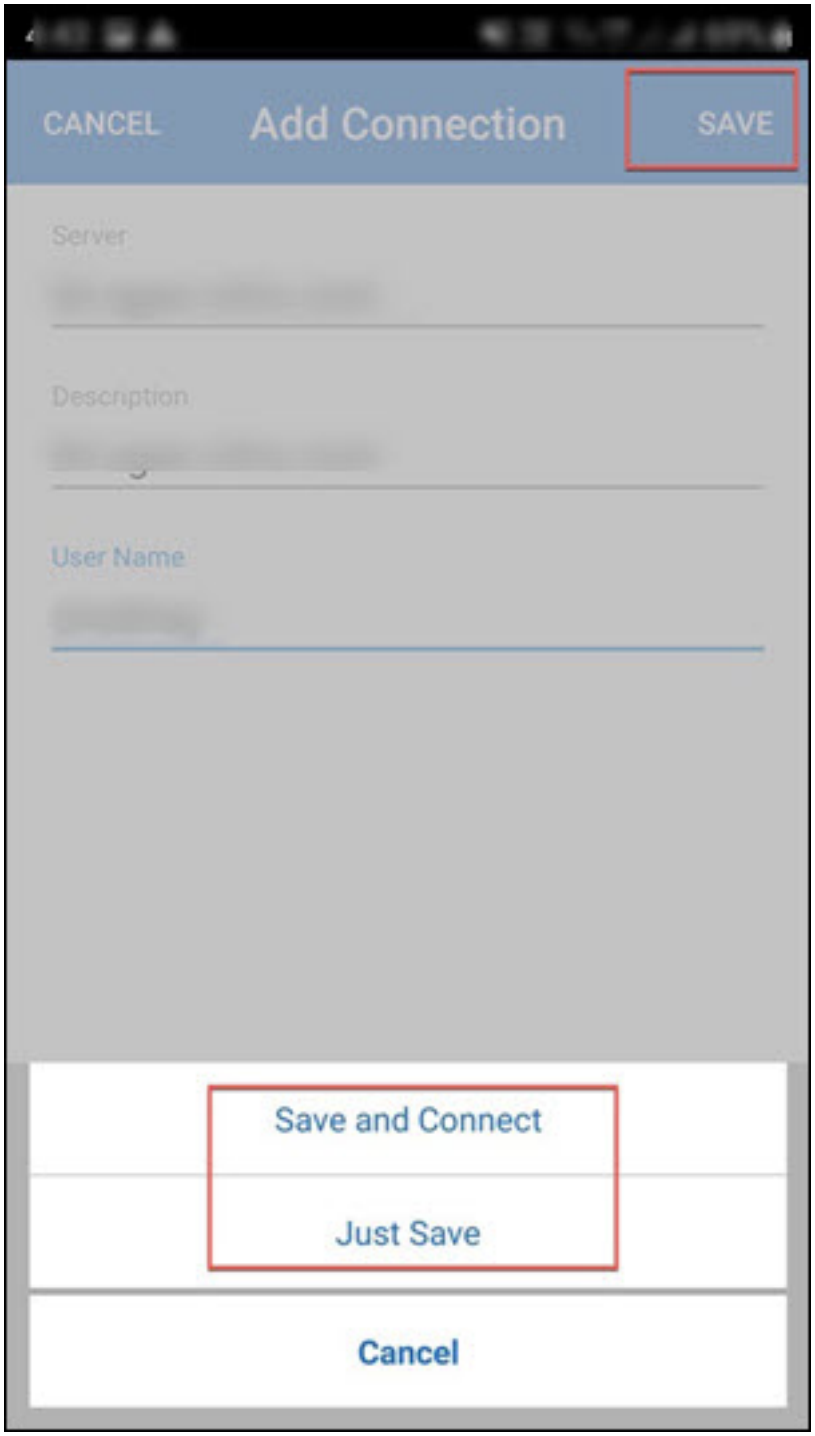
Hinzufügen einer Verbindung

Hinweis: Dieser Schritt ist nur im Nicht-MDM-Modus erforderlich.

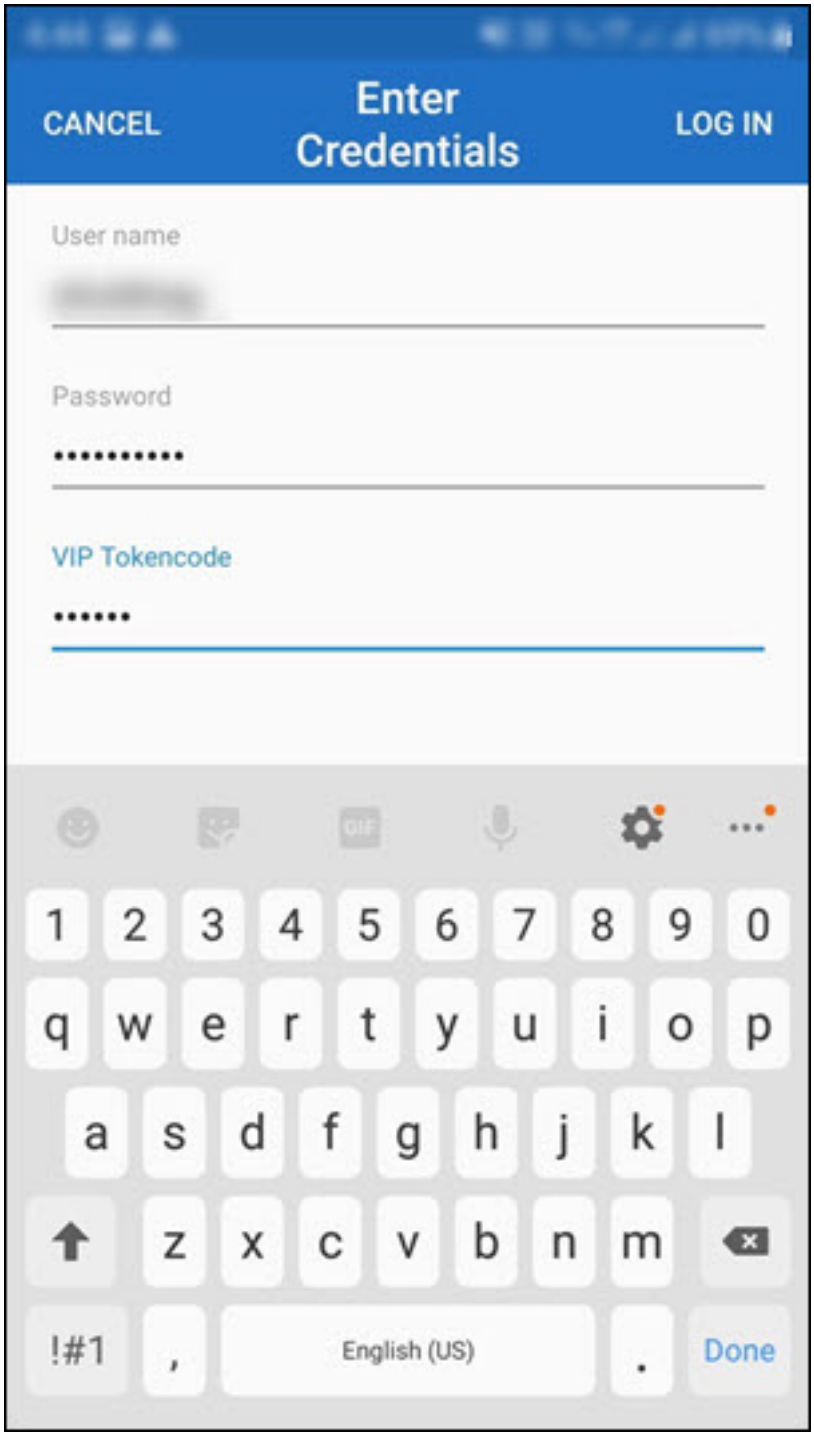
Nachdem Sie Citrix Secure Access installiert und die App auf dem Android-Gerät geöffnet haben, wird der folgende Bildschirm angezeigt.



1. Klicken Sie auf das **+**, um eine Verbindung hinzuzufügen.
2. Geben Sie die Basis-URL (z. B. https://gateway.mycompany.com) und den Namen für die VPN-Verbindung ein. Optional können Sie den Benutzernamen eingeben.
3. Klicken Sie auf **Speichern** und dann nach Bedarf auf **Speichern und Verbinden** oder **Nur speichern**.

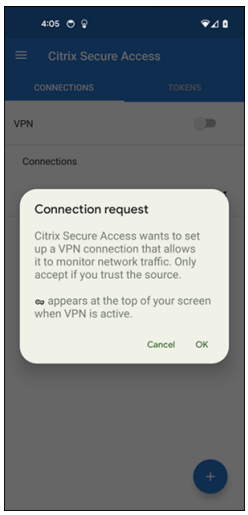


4. Geben Sie Anmeldeinformationen zur Authentifizierung für Ihren Server ein und tippen Sie auf **Anmelden** oder auf der Tastatur auf **Fertig**.

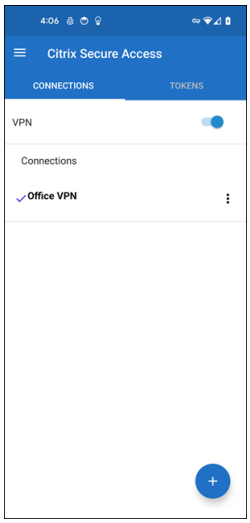


Die Verbindungsanforderungsmeldung wird angezeigt. Klicken Sie auf **OK**.

Hinweis: Diese Meldung wird nur angezeigt, wenn zum ersten Mal eine VPN-Verbindung von Citrix Secure Access hergestellt wird. Wenn der Benutzer die Verbindung zum ersten Mal zulässt, wird diese Meldung erst wieder angezeigt, wenn der Benutzer die App deinstalliert und erneut installiert.



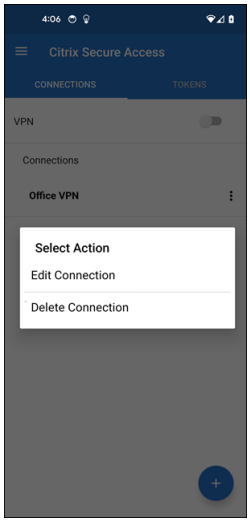
Hinweis: Um sich von Citrix Secure Access abzumelden, stellen Sie den **VPN-Schalter** auf AUS.



Eine vorhandene Verbindung ändern oder löschen

Sie können eine Verbindung bearbeiten oder löschen, nachdem Sie sich von Citrix Secure Access abgemeldet haben.

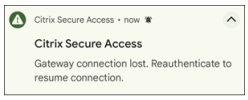
Tippen Sie auf den Servernamen und halten Sie ihn gedrückt. Wählen Sie dann **Verbindung bearbeiten** oder **Verbindung löschen** aus.



Verbindung zu NetScaler Gateway nach VPN-Verbindungsfehler wiederherstellen – Preview

Ab Version 23.10.1 fordert Sie Citrix SSO für Android auf, sich erneut bei NetScaler Gateway zu authentifizieren, wenn eine VPN-Verbindung unterbrochen wird. Sie werden auf der Benutzeroberfläche und im Benachrichtigungsbereich Ihres Android-Geräts darüber informiert, dass die Verbindung zu NetScaler Gateway unterbrochen wurde und Sie sich erneut authentifizieren müssen, um die Verbindung wieder herzustellen.

> **Hinweis:**
>
> Dieses Feature ist als Preview verfügbar.

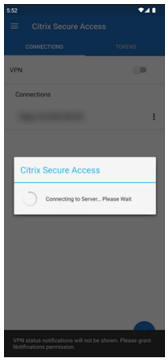


Benachrichtigungen auf Geräten mit Android 13+ empfangen oder blockieren

Ab Citrix Secure Access für Android Version 23.12.1 werden Sie bei der Installation oder Neuinstallation des Citrix Secure Access Client auf Geräten mit Android 13+ aufgefordert, Berechtigungen für den Empfang von Benachrichtigungen vom Citrix Secure Access Client bereitzustellen. Wenn Sie die Berechtigung verweigern, erhalten Sie keine VPN-Status- oder Push-Benachrichtigungen vom Citrix Secure Access Client auf Ihrem Android-Gerät.

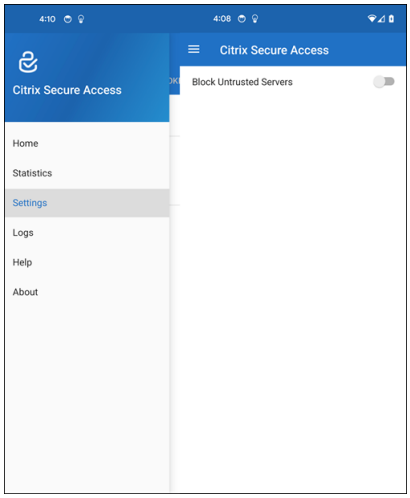
Sie können auf Ihrem Android-Gerät zu **Einstellungen > Benachrichtigungen** navigieren, um die Benachrichtigungsberechtigungen zu ändern.

Im folgenden Beispiel wurden die VPN-Statusbenachrichtigungen deaktiviert.



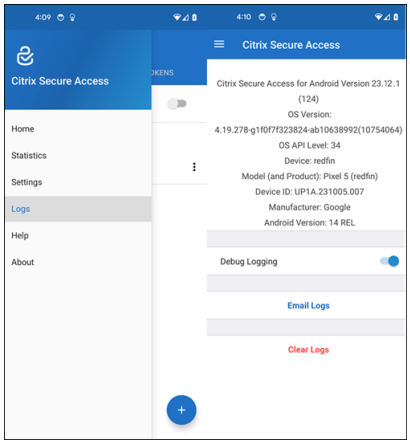
Nicht vertrauenswürdige Server blockieren

Citrix Secure Access stellt standardmäßig keine Verbindung zu nicht vertrauenswürdigen Servern her. Nicht vertrauenswürdige Server sind Server, die selbstsignierte Zertifikate verwenden oder kein vertrauenswürdiges Stammzertifikat für das Gateway haben. Um diese Verbindungsarten zuzulassen, legen Sie **Nicht vertrauenswürdige Server blockieren** auf **AUS** fest.



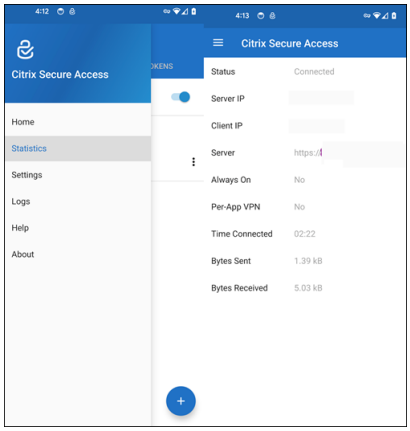
Debugprotokolle aktivieren

Das Erfassen von Debugprotokollen ist wichtig für die Fehlerbehebung und das Melden von Problemen an den Citrix Support.
Stellen Sie den Schalter **Debugprotokollierung** auf **EIN**, um die Debugprotokollierung für Citrix Secure Access zu aktivieren. Mit dem Link **Protokolle per E-Mail senden** können Sie die Protokolle per E-Mail senden, wenn Sie Verbindungsprobleme beheben.



Statistiken anzeigen

Sie können die Verbindungsstatistiken anzeigen, wenn eine Verbindung über VPN besteht.



Kennworttoken

Sie können einen 6-stelligen Kennworttoken für die zweistufige Authentifizierung hinzufügen. Dieser Code verwendet das zeitbasierte Einmalkennwortprotokoll, um den OTP-Code zu generieren.

Sie können einen Kennworttoken manuell hinzufügen oder mit der QR-Code-Scanmethode registrieren. Die zweistufige Authentifizierung per Pushbenachrichtigungen ist nicht aktiviert, wenn Sie den Token manuell eingeben.

Kennworttoken registrieren

1. Melden Sie sich auf einem Desktop oder Laptop in Ihrem Webbrowser an der Seite zum Verwalten der Einmal-PIN Ihrer Organisation an.

2. Klicken Sie auf **Gerät hinzufügen**.
3. Geben Sie einen Namen für Ihr Gerät ein und klicken Sie auf **Start**.

   Ein QR-Code wird generiert.

Kennworttoken durch Scannen des QR-Codes im Browser hinzufügen

1. Navigieren Sie auf der **Home**-Seite zur Registerkarte **Token**.
2. Tippen Sie auf das **+** und tippen Sie auf **QR-Code scannen**.
3. Fokussieren Sie die Kamera auf den QR-Code im Browser.

Citrix Secure Access füllt automatisch den Gerätenamen und den geheimen Schlüssel aus.

Alternativ können Sie den geheimen Schlüssel, der über dem QR-Code angezeigt wird, manuell eingeben.

Citrix Secure Access validiert den QR-Code und registriert sich dann beim Gateway für Pushbenachrichtigungen. Wenn beim Registrierungsvorgang keine Fehler auftreten, wird der Token auf der Registerkarte “Token”hinzugefügt.

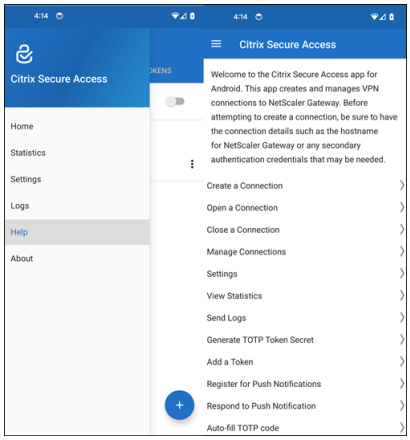
> **Hinweis:**
>
> - Sie müssen Citrix Secure Access Zugriff auf Ihre Kamera gewähren, um den QR-Code zu erfassen.
> - Sie müssen eine PIN bzw. ein Kennwort auf Ihrem Gerät aktivieren.

Kennworttoken manuell hinzufügen

1. Navigieren Sie auf der **Home**-Seite zur Registerkarte **Token**.
2. Tippen Sie auf das + und dann auf **Manuell eingeben**.
3. Geben Sie den Gerätenamen und den geheimen Schlüssel ein, wie er auf dem im Browser generierten Kennworttoken angezeigt wird.

Hilfethemen

Weitere Informationen zur Verwendung von Citrix Secure Access finden Sie in der **Hilfe**.



Mit Ihrem Unternehmensnetzwerk über Citrix Secure Access in einer Intune-Umgebung verbinden

March 15, 2024

> **Hinweis:**
>
> Administratorspezifische Anweisungen zu Citrix Secure Access für Android finden Sie unter Citrix Secure Access für Android-Geräte.

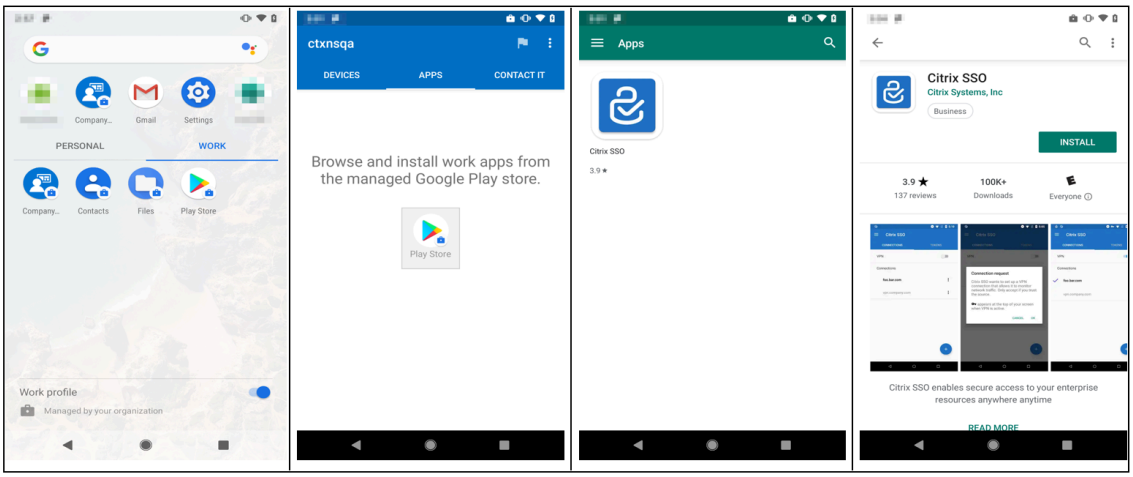
In diesem Thema finden Sie Details, wie Sie sich mit Ihrem Unternehmensnetzwerk über den Citrix Secure Access Client verbinden, der in der Microsoft Intune Android Enterprise-Umgebung konfiguriert ist.

Annahmen:

- Sie haben das Gerät mit der Intune-Unternehmensportalapp in Intune registriert.
- Das Arbeitsprofil für den Benutzer ist auf dem Gerät eingerichtet.

1. Öffnen Sie die **Intune-Unternehmensportal**-App auf dem Gerät über das Arbeitsprofil.
2. Klicken Sie auf das Menü mit den drei Punkten, um die Einstellungen für die App zu öffnen, und scrollen Sie zum unteren Bildschirmrand. Tippen Sie auf **Synchronisieren**, um mit dem Intune-Server zu synchronisieren, und navigieren Sie dann zum Hauptbildschirm der App.
3. Tippen Sie auf die **Apps**-Registerkarte und tippen Sie auf den Link **Managed Google Play Store**.

   Die Liste der genehmigten Apps für den Benutzer wird angezeigt.



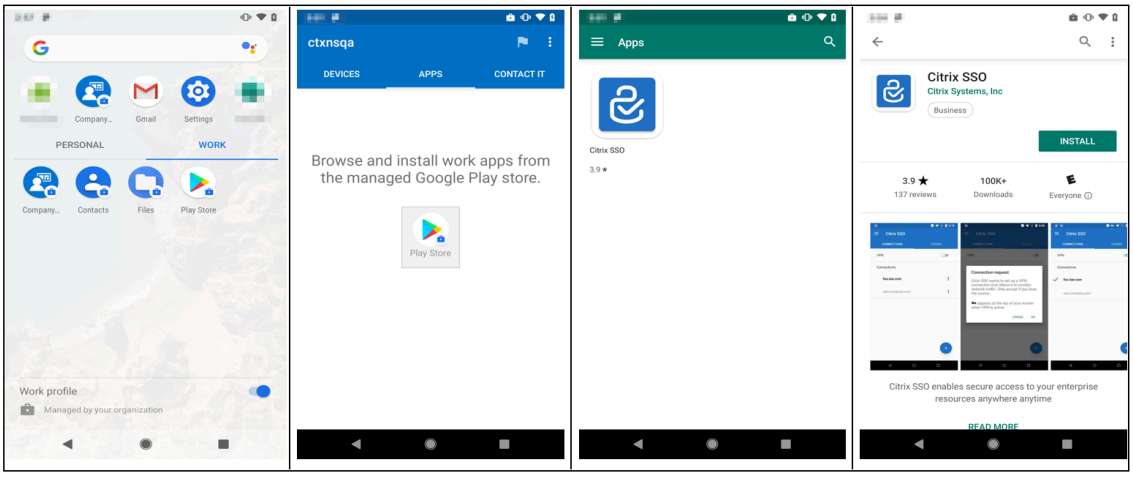
4. Tippen Sie auf **Citrix Secure Access**.

   Der Citrix Secure Access Client wird im Managed Google Play Store angezeigt.

5. Tippen Sie auf **Installieren**.

6. Navigieren Sie zurück zur Liste der Arbeitsprofil-Apps. Citrix Secure Access wurde zur Liste der installierten Apps hinzugefügt.

7. Tippen Sie in der App-Liste des Profils **Firma** auf das Citrix Secure Access-Symbol, um es zu öffnen.

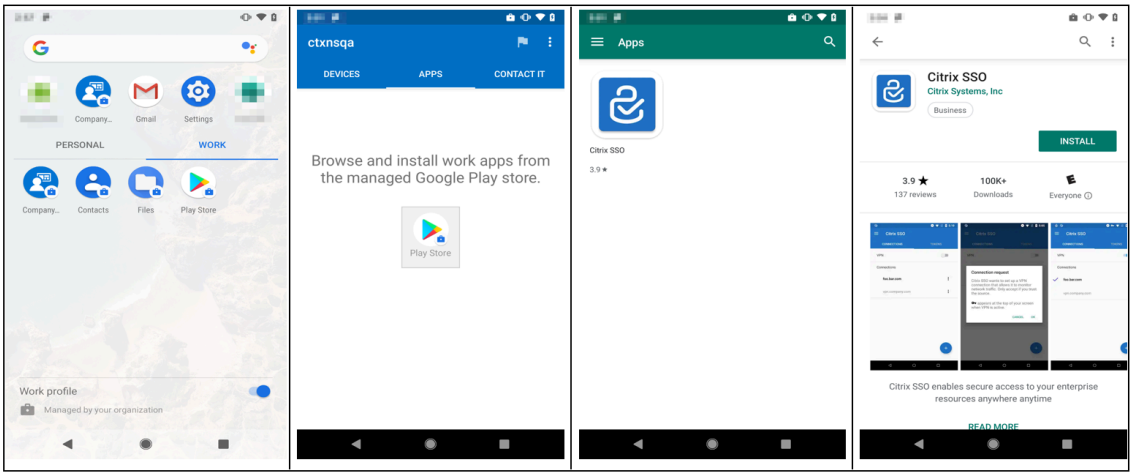


   Citrix Secure Access wird geöffnet. Sie werden aufgefordert, die Berechtigung zur sicheren Kommunikation mit dem internen Netzwerk Ihres Unternehmens zuzulassen oder nicht zuzulassen.

8. Tippen Sie auf **Zulassen**, um die Berechtigung zu erteilen. Citrix Secure Access wird geschlossen, wenn Sie **Nicht zulassen** wählen, und Sie können den Citrix Secure Access Client nicht verwenden.

> **Hinweis:**
>
> Möglicherweise werden Sie aufgefordert, **Telefonanrufe** zu erlauben oder zu verweigern (falls nicht bereits über Intune erteilt). Tippen Sie auf **Zulassen**, um die Berechtigung zu erteilen. Sie können diese Berechtigung verweigern, aber wenn die Intune-NAC-Prüfung für die Geräteauthentifizierung bei NetScaler Gateway erforderlich ist, können Sie erst dann eine Verbindung mit dem internen Netzwerk Ihres Unternehmens herstellen, wenn Sie diese Berechtigung erteilen.

9. **Mein Firmen-VPN** (oder der Name, den Sie in der Citrix Secure Assess-Konfiguration in Intune gewählt haben) wird im Abschnitt “Verwaltete Verbindungen”auf der Registerkarte **Verbindungen** aufgeführt. Tippen Sie auf diese Verbindung. Sie werden aufgefordert, die Anmeldeinformationen für die Authentifizierung bei NetScaler Gateway einzugeben.
10. Geben Sie Anmeldeinformationen für die Authentifizierung bei NetScaler Gateway an, und tippen Sie auf **LOG IN**.



Sie werden möglicherweise aufgefordert, ein Zertifikat auszuwählen, wenn die Clientzertifikatauthentifizierung in NetScaler Gateway konfiguriert ist. Sie können den Zugriff auf das Zertifikat gewähren.

11. Sie werden vom Android-System aufgefordert, die **Verbindungsanforderung** für das Einrichten des VPN-Tunnels zuzulassen. Tippen Sie auf **OK**, um Citrix Secure Access die Berechtigung zu erteilen, eine sichere Verbindung mit Ihrem internen Unternehmensnetzwerk herzustellen.

    Hinweis: Diese Aufforderung wird nur angezeigt, wenn Sie zum ersten Mal eine sichere Verbindung mit NetScaler Gateway herstellen. Für nachfolgende Verbindungsversuche wird sie nur angezeigt, wenn Citrix Secure Access deinstalliert und dann neu auf dem Gerät installiert wurde.

Sie sind mit Ihrem internen Unternehmensnetzwerk verbunden. In der Gerätestatusleiste wird ein Schlüsselsymbol angezeigt, das Sie darüber informiert, dass die VPN-Verbindung aktiv ist.

Das VPN-Dienst-Benachrichtigungssymbol des Citrix Secure Access Clients wird ebenfalls in der Statusleiste angezeigt. Der Verbindungsschalter ändert den Status in “Verbunden”und neben dem VPN-Profilnamen wird ein Häkchen angezeigt.