# Citrix Secure Access para Android

# Contents



# Citrix Secure Access para dispositivos Android

March 16, 2024

El cliente Citrix Secure Access para Android (antes conocido como aplicación Citrix SSO para Android) ofrece la mejor solución de protección de datos y acceso a las aplicaciones con NetScaler Gateway. Ahora puede acceder de forma segura a las aplicaciones críticas para el negocio, los escritorios virtuales y los datos corporativos en cualquier momento y desde cualquier lugar.

> **Notas:**
>
> - A partir de la versión 23.12.1, Citrix SSO para Android pasa a llamarse Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.
> - Para obtener instrucciones específicas para administradores sobre Citrix Secure Access para Android, consulte Citrix Secure Access para dispositivos Android.

# Cómo usar Citrix Secure Access desde el dispositivo Android

March 16, 2024

> **Notas:**
>
> - A partir de la versión 23.12.1, Citrix SSO para Android pasa a llamarse Citrix Secure Access. Estamos actualizando nuestra documentación y las capturas de pantalla de la interfaz de usuario para reflejar este cambio de nombre.
> - Para obtener instrucciones específicas para administradores sobre cómo usar Citrix Secure Access para Android, consulte Citrix Secure Access para dispositivos Android.

Instale Citrix Secure Access desde Play Store. Los nuevos usuarios deben agregar el servidor en implementaciones que no sean MDM para crear una conexión con NetScaler Gateway. Para usos posteriores, es posible conectarse a una conexión existente o agregar una conexión, así como modificar las conexiones existentes, si el administrador lo permite en una implementación MDM. También pueden consultarse los registros y actuar en consecuencia.

> **Notas:**
>
> - Las conexiones implementadas a través de MDM no se pueden modificar.
> - A partir de Citrix SSO para Android 23.8.1, es posible que se le pida que conceda a la apli-

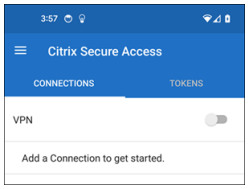
 

> cación Citrix SSO permiso para consultar todos los paquetes. Una vez concedido el consentimiento, la aplicación Citrix SSO hará lo siguiente:
>
> - Receives the package install notification from the operating system.
> - Restarts the Always On VPN.
>
> Cuando se conecte a su perfil de VPN por primera vez, se le pedirá que dé su consentimiento (exigido por las directivas de Google) para recopilar información del paquete instalado. Si usted otorga el consentimiento, se inicia la conexión VPN. Si deniega el consentimiento, se interrumpe la conexión VPN. La pantalla de consentimiento no vuelve a aparecer una vez que se ha otorgado el consentimiento.

## Agregar una conexión

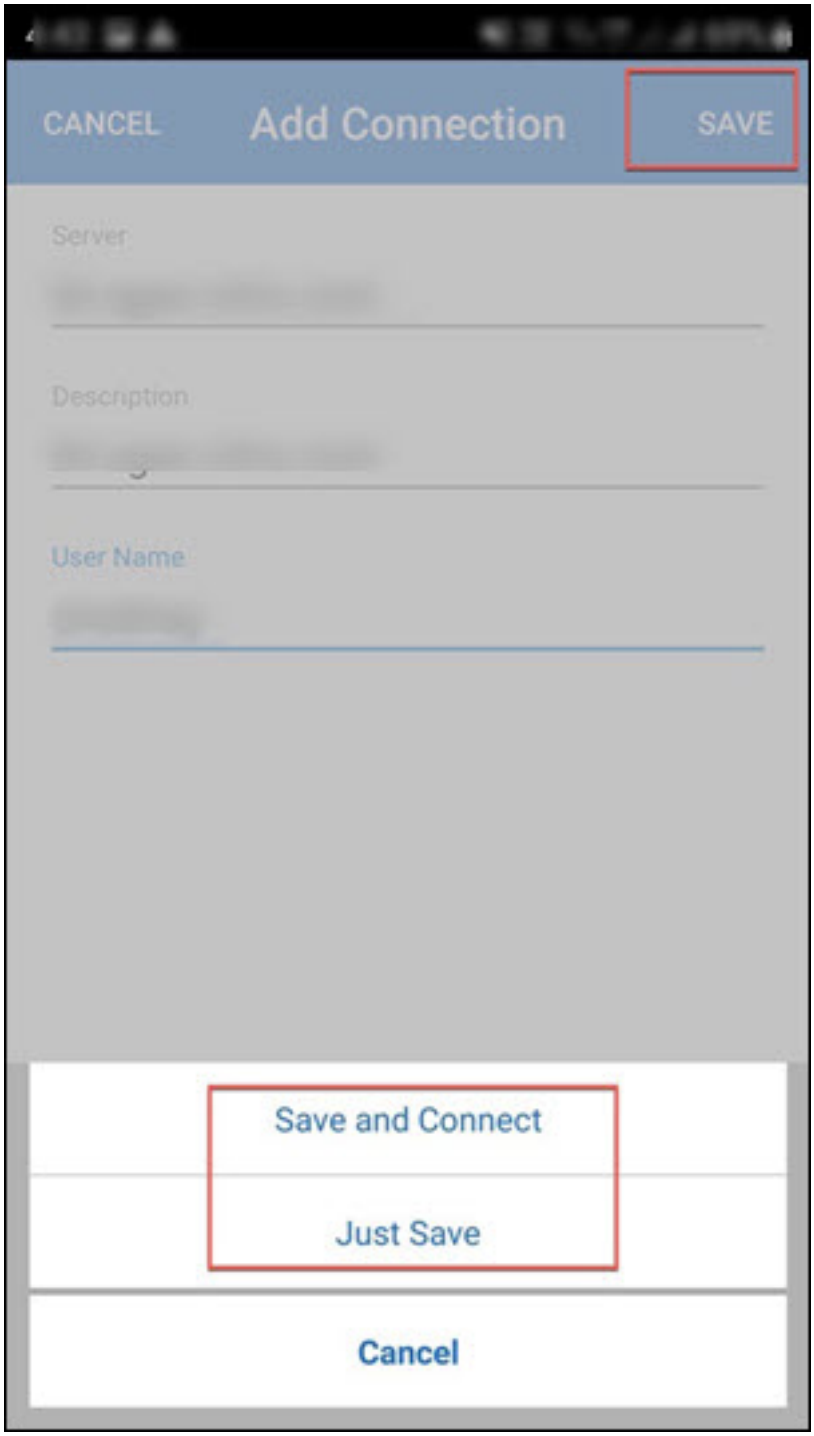
**Nota**: Este paso solo es necesario en implementaciones que no sean MDM.

Tras instalar Citrix Secure Access y abrir la aplicación en el dispositivo Android, se muestra la siguiente pantalla.



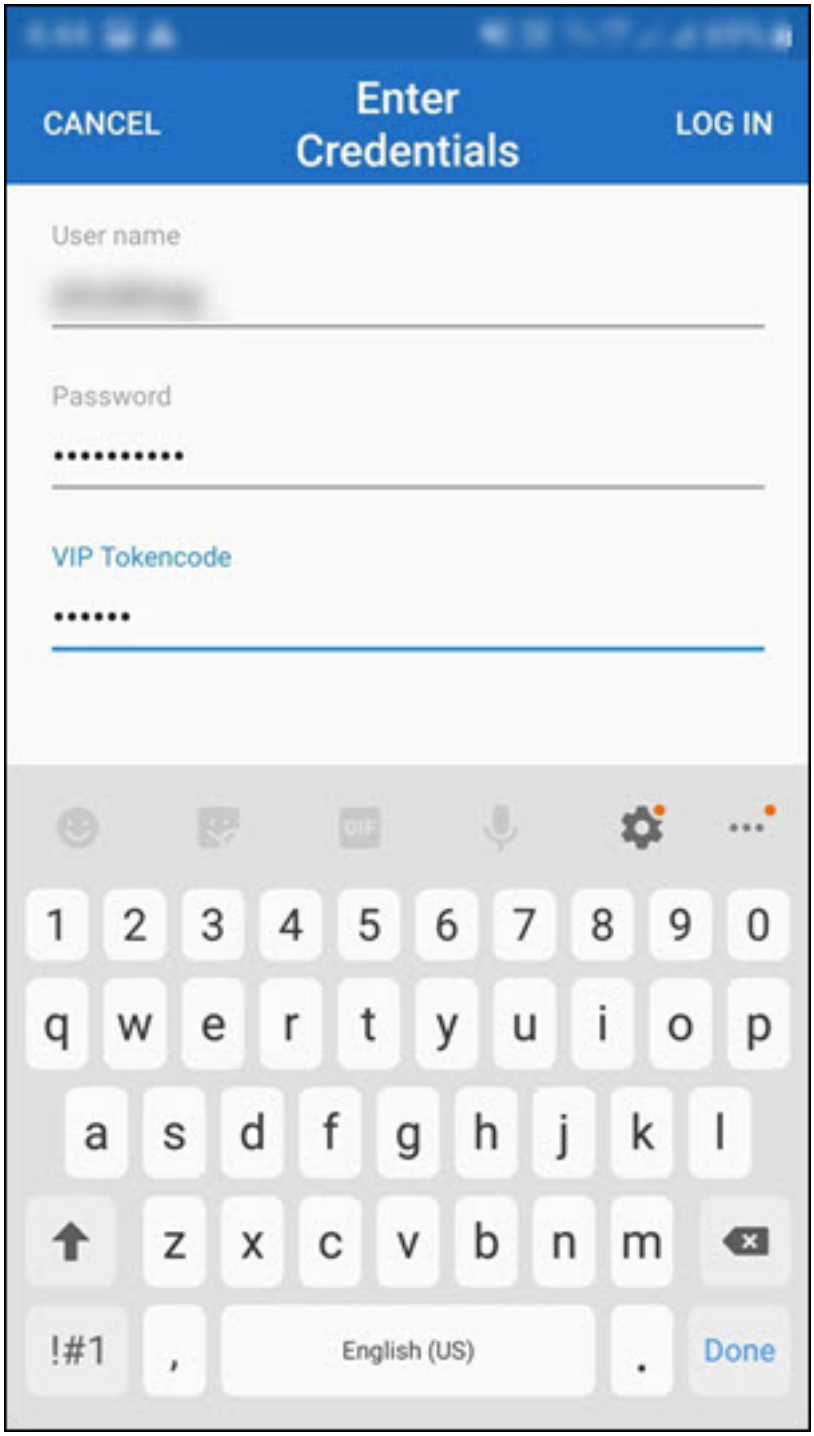

1. Haga clic en **+** para agregar una conexión.
2. Introduzca la URL base (por ejemplo, https://gateway.mycompany.com) y el nombre de la conexión VPN. Opcionalmente, puede introducir el nombre de usuario.
3. Haga clic en **Guardar** y, a continuación, en **Guardar y conectar** o en **Solo guardar**, según corresponda.




4. Proporcione las credenciales de autenticación de su servidor y toque **Iniciar sesión** o **Listo** en el teclado.

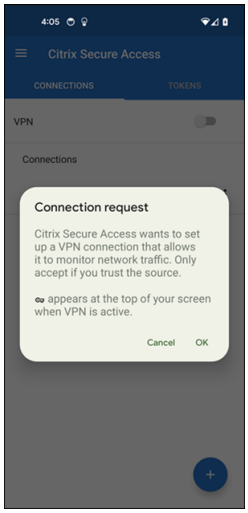
 



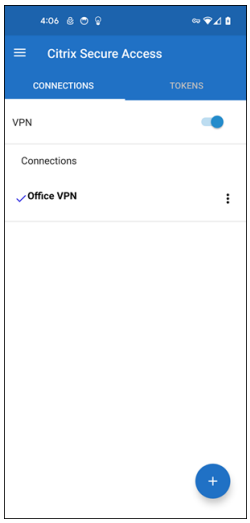

Aparecerá el mensaje de solicitud de conexión. Haga clic en **Aceptar**.

**Nota**: Este mensaje solo se muestra la primera vez que Citrix Secure Access establece una conexión VPN. Si el usuario permite la conexión por primera vez, este mensaje no se muestra de nuevo hasta que el usuario desinstale e instale de nuevo la aplicación.




**Nota**: Para cerrar sesión en Citrix Secure Access, **desactive la VPN**.

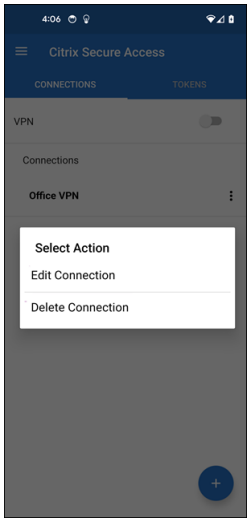



## Modificar o eliminar una conexión existente

Puede modificar o eliminar una conexión después de cerrar sesión en Citrix Secure Access.

Toque y mantenga pulsado en el nombre del servidor y seleccione **Modificar conexión** o **Eliminar conexión**.

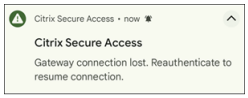
 




### Reconectarse a NetScaler Gateway tras un error en la conexión VPN - Technical Preview

A partir de la versión 23.10.1, la aplicación Citrix SSO para Android le pide que vuelva a autenticarse en NetScaler Gateway cuando se interrumpe una conexión VPN. En la interfaz de usuario y en el panel de notificaciones de su dispositivo Android se le notificará que se ha perdido la conexión con NetScaler Gateway y que debe volver a autenticarse para reanudar la conexión.

> **Nota:**
>
> Esta función se encuentra en Tech Preview.



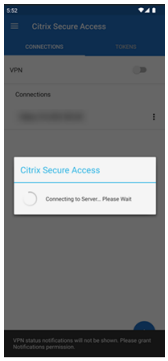

### Reciba o bloquee notificaciones en dispositivos con Android versión 13 o posterior

A partir de la versión 23.12.1 de Citrix Secure Access para Android, al instalar o instalar de nuevo el cliente Citrix Secure Access en dispositivos Android 13 o posterior, se le solicitará que conceda permisos para recibir notificaciones del cliente Citrix Secure Access. Si deniega el permiso, no recibirá ninguna notificación push o de estado de la VPN del cliente Citrix Secure Access en su dispositivo Android.

Puede ir a **Ajustes > Notificaciones** en su dispositivo Android para cambiar los permisos de notificaciones.

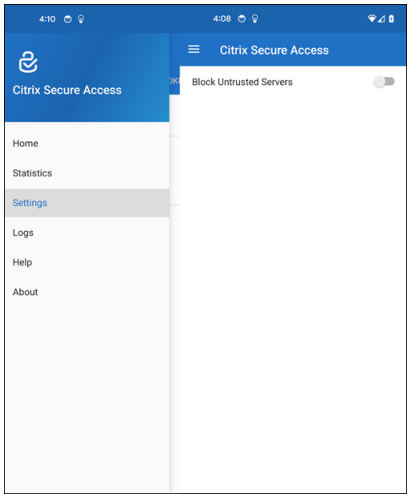
En el siguiente ejemplo, se han inhabilitado las notificaciones de estado de la VPN.




## Bloquear servidores que no son de confianza

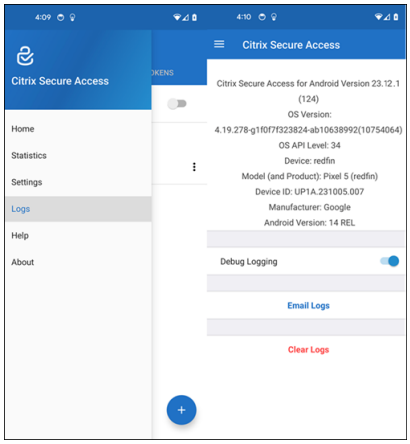
De manera predeterminada, Citrix Secure Access no se conecta a servidores que no son de confianza. Por servidores que no son de confianza se entiende aquellos servidores que utilizan certificados autofirmados o que no tienen un certificado raíz de confianza para la puerta de enlace. Para autorizar este tipo de conexiones, puede **desactivar** el conmutador **Bloquear servidores que no son de confianza**.




## Habilitar registros de depuración

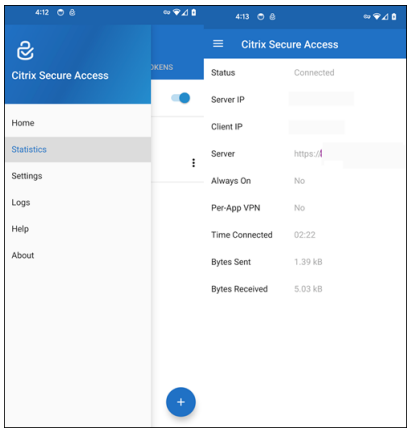
La captura de registros de depuración es parte esencial de la solución de problemas o de su notificación a Citrix Support.
Toque el conmutador **activado** de **Registros de depuración** para activar la función de depuración para Citrix Secure Access. Puede utilizar el enlace **Enviar registros por correo electrónico** para enviar dichos registros cuando solucione problemas de conexión.




## Ver estadísticas

Puede ver las estadísticas de conexión cuando la VPN está conectada.




## Tokens de contraseña

Puede agregar un token de contraseña de 6 dígitos como segundo factor de autenticación. Este código utiliza el protocolo de contraseña temporal de un solo uso para generar el código OTP.

Puede agregar un token de contraseña manualmente o registrar un token de contraseña con el método de escaneo de códigos QR. La autenticación de segundo factor mediante notificaciones push no estará habilitada si decide introducir el token manualmente.

### Registrar un token de contraseña

1. Inicie sesión en la página de administración de PIN de un solo uso de su organización desde un explorador web con un equipo de escritorio o portátil.
2. Haga clic en **Agregar dispositivo**.

3. Introduzca un nombre para el dispositivo y, a continuación, haga clic en **Ir**.

   Se generará un código QR.

#### Agregar un token de contraseña escaneando el código QR en el explorador

1. Acceda a la ficha **Tokens** desde la vista **Inicio**.
2. Toque **+** y, a continuación, **Escanear código QR**.
3. Enfoque la cámara hacia el código QR de su explorador.

Citrix Secure Access rellena automáticamente el nombre del dispositivo y la clave secreta.

Alternativamente, puede introducir manualmente la clave secreta que aparece encima del código QR.

Citrix Secure Access valida el código QR y después se registra en la puerta de enlace para notificaciones push. Si no hay errores en el proceso de registro, el token se agrega a la ficha de tokens.

> **Nota:**
>
> - Debe autorizar permisos de cámara para que Citrix Secure Access capture el código QR.
> - Debe habilitar el PIN o la contraseña del dispositivo en su dispositivo.

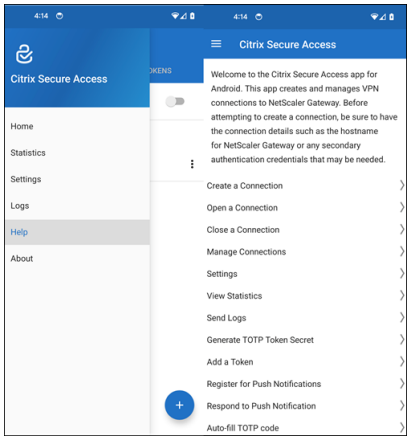
#### Agregar un token de contraseña manualmente

1. Acceda a la ficha **Tokens** desde la vista **Inicio**.
2. Toque + y, a continuación, **Introducir manualmente**.
3. Introduzca el nombre del dispositivo y la clave secreta, tal como aparecen en el token de contraseña generado en el explorador.

## Temas de Ayuda

Para obtener más información sobre cómo usar Citrix Secure Access, consulte **Ayuda**.




# Conectarse a su red corporativa mediante Citrix Secure Access configurado en un entorno Intune

March 16, 2024

> **Nota:**
>
> Para obtener instrucciones específicas para administradores sobre Citrix Secure Access para Android, consulte Citrix Secure Access para dispositivos Android.

En este tema, se recogen detalles acerca de la conexión a la red corporativa mediante Citrix Secure Access configurada en el entorno de Android Enterprise y Microsoft Intune.

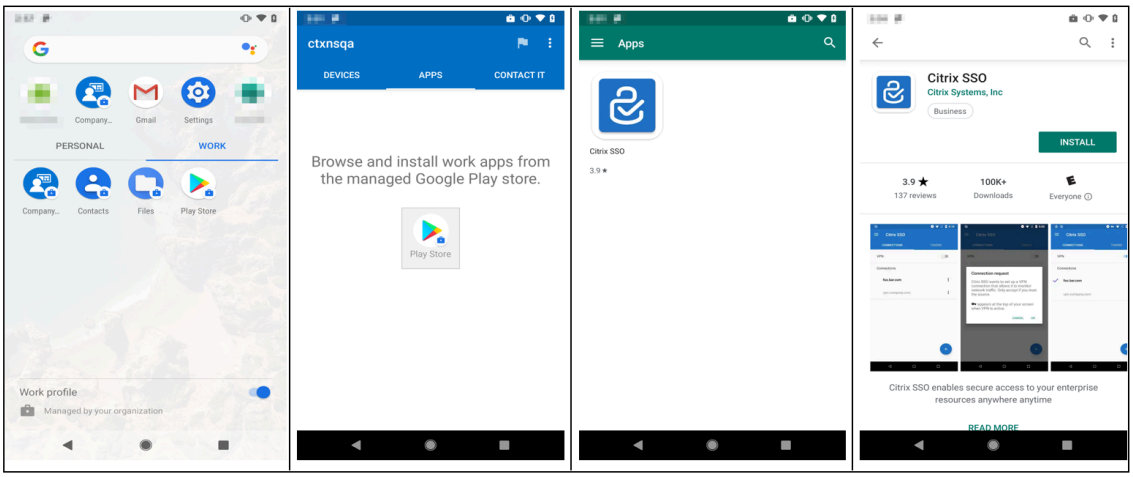
**Supuestos:**

- Ha inscrito el dispositivo en Intune mediante la aplicación Portal de empresa de Intune.
- Se ha configurado un perfil de trabajo para el usuario en el dispositivo.

1. Desde el perfil de trabajo, abra la aplicación **Portal de empresa de Intune** en el dispositivo.
2. Haga clic en el menú de tres puntos para abrir los parámetros de la aplicación y desplácese a la sección inferior de la pantalla. Toque **SINCRONIZAR** para sincronizar con el servidor Intune y después vaya a la pantalla principal de la aplicación.
3. Toque la ficha **APLICACIONES** y, a continuación, en el enlace **Google Play Store administrado**.

   Aparecerá la lista de aplicaciones aprobadas para el usuario.



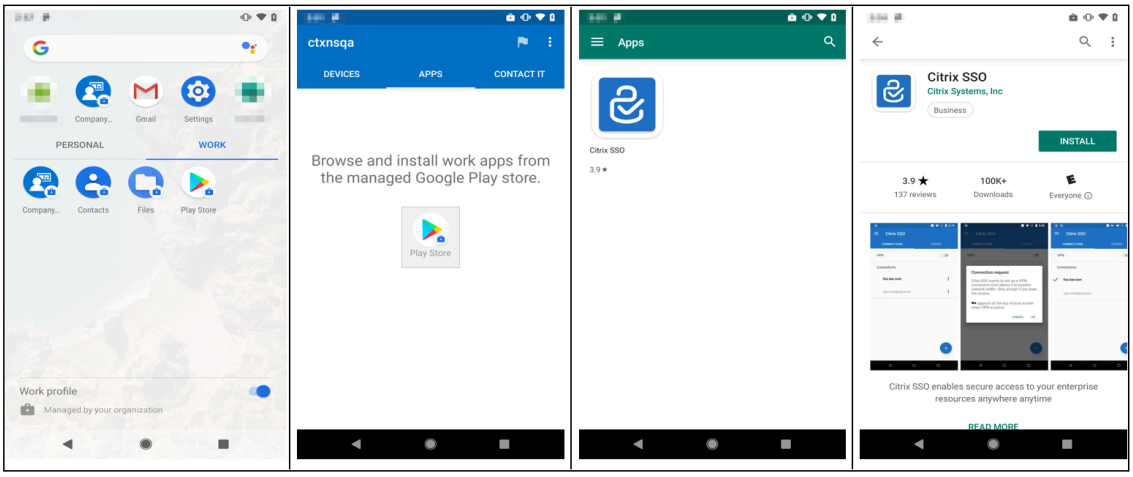

4. Toque **Citrix Secure Access**.

   El cliente Citrix Secure Access se muestra en la Google Play Store administrada.

5. Toque **INSTALAR**.

6. Vuelva a la lista de aplicaciones del perfil de trabajo. Citrix Secure Access se agrega a la lista de aplicaciones instaladas.

7. Toque el icono de Citrix Secure Access en la lista de aplicaciones del perfil de **TRABAJO** para abrirlo.




   Se abre Citrix Secure Access. Se le pedirá que conceda o deniegue permiso para comunicarse de forma segura con la red interna de su empresa.

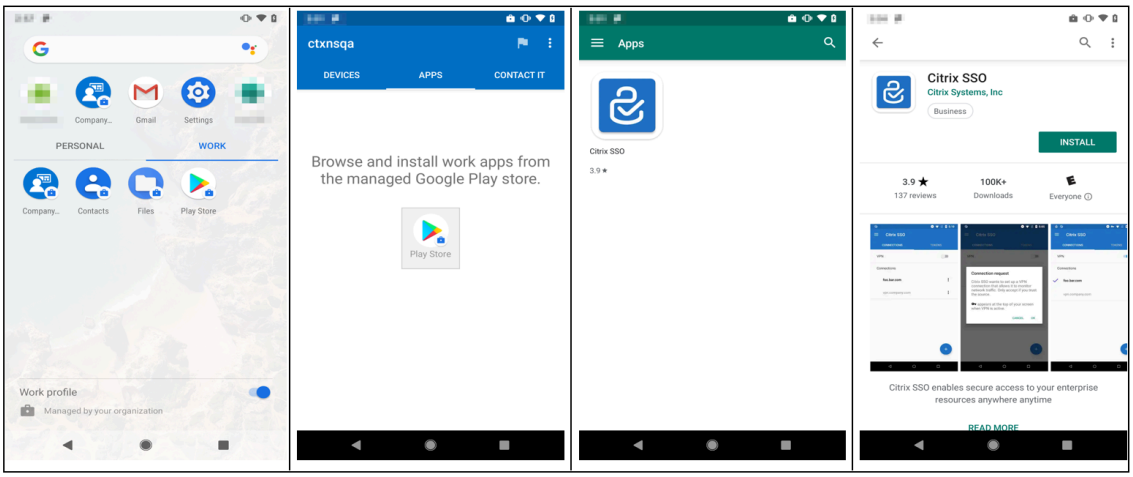
8. Toque **PERMITIR** para conceder el permiso. Citrix Secure Access se cierra si elige **NO PERMITIR** y no puede usar el cliente Citrix Secure Access.

   > **Nota:**
   >
   > Es posible que se le pida que conceda o deniegue **permiso para administrar y hacer lla-**

> **madas telefónicas** (si no se ha concedido ya a través de Intune). Toque **Permitir** para conceder permiso. Puede denegar este permiso, pero, si se requiere comprobación de control de acceso a la red (NAC) de Intune para la autenticación de dispositivos en NetScaler Gateway, no podrá conectarse a la red interna de su empresa hasta que conceda este permiso.

9. **Mi VPN corporativa** (o el nombre elegido en la configuración de Citrix Secure Access en Intune) se muestra en la sección Conexiones administradas de la ficha **CONEXIONES**. Toque en esta conexión. Se le pedirán las credenciales de autenticación con NetScaler Gateway.
10. Proporcione las credenciales para la autenticación con NetScaler Gateway y toque **INICIAR SESIÓN**.




Es posible que se le pida que seleccione un certificado si la autenticación de certificados de cliente está configurada en NetScaler Gateway. Puede proporcionar acceso al certificado.

11. El sistema Android le pedirá que autorice la **solicitud de conexión** para la configuración del túnel VPN. Toque **Aceptar** para permitir que Citrix Secure Access establezca una conexión segura con la red interna de su empresa.

    **Nota:** Este mensaje solo se muestra cuando se establece una conexión segura con NetScaler Gateway por primera vez. No se muestra en los intentos de conexión posteriores hasta que Citrix Secure Access se desinstala y se instala de nuevo en el dispositivo.

Ahora estará conectado a la red interna de su empresa. Un icono de llave en la barra de estado del dispositivo indica que la conexión VPN está activa. El icono de notificación del servicio VPN del cliente Citrix Secure Access también se muestra en la barra de estado. El estado del conmutador de conexión cambia a conectado y aparece un icono de marca de verificación junto al nombre del perfil VPN.