Quick Start de RSA SecurID® Software Token 2.0.4 for Android™

Introducción

Bienvenido a RSA SecurID Software Token 2.0.4 for Android, un software de autenticación que transforma su teléfono inteligente o tableta Android en un dispositivo de autenticación de RSA SecurID.

Para usar la aplicación, debe importar un token de software. La aplicación genera un nuevo tokencode cada 60 o 30 segundos. El tokencode se utiliza para acceder a los recursos protegidos por SecurID (por ejemplo, la VPN corporativa). Si el token de software requiere un PIN de SecurID, utilice un PIN combinado con tokencode, que es un passcode. El tokencode o passcode es una contraseña de un solo uso (OTP).

En este documento, se describe cómo instalar la aplicación RSA SecurID y cómo importar y utilizar un token de software. Puede importar un máximo de 10 tokens de software en el dispositivo. Debe importar cada token por separado.

Instalación de la aplicación RSA SecurID

Instale la aplicación gratuita desde Google Play (Play Store).

Para instalar la aplicación:

1. Asegúrese de que el dispositivo cuente con conexión a Internet.
2. En la lista de aplicaciones, puntee el icono **Google Play** o **Play Store**.
3. Puntee la opción **Buscar** y escriba las palabras clave **RSA SecurID**.
4. Seleccione **RSA SecurID Software Token**.
5. Puntee la opción **Instalar**.

   El dispositivo muestra una lista de funciones para las cuales la aplicación requerirá acceso.
6. Para iniciar la descarga, puntee **Aceptar**.

   El icono de estado muestra el progreso de la descarga. Cuando finalice la descarga, aparece un icono de notificación en la barra de estado. La aplicación también se muestra la ventana Notificaciones.

Inicio de la aplicación RSA SecurID

Para iniciar la aplicación:

1. En la lista de aplicaciones, puntee el icono RSA SecurID.
2. Lea el contrato de licencia y seleccione **He leído y acepto los términos del acuerdo**. Puntee la opción **Continuar**.

Paso siguiente

Después de aceptar el acuerdo de licencia, podrá importar un token de software.

- Si el administrador le solicitó el ID del dispositivo, vaya a la sección siguiente, "Envío del ID del dispositivo por correo electrónico".
- Si el administrador le envió un token de software sin solicitarle el ID del dispositivo, vaya a la sección siguiente, "Importación de un token del software".

Envío del ID del dispositivo por correo electrónico

Es posible que el administrador le solicite el ID del dispositivo antes de enviarle un token. El ID de dispositivo se usará para vincular el token de software con su dispositivo y garantizar que el token de software no pueda ser utilizado en otro dispositivo. Asegúrese de que la cuenta de correo electrónico esté configurada en el dispositivo. Asegúrese de tener la dirección de correo electrónico del administrador.

Para enviar el ID del dispositivo por correo electrónico:

1. En la pantalla de bienvenida, puntee **ID del dispositivo**.
2. Realice una de las siguientes acciones:
   - Puntee la opción **Enviar el ID del dispositivo por correo electrónico** para abrir un mensaje de correo electrónico que contenga el ID del dispositivo.
   - Puntee la opción **Copiar el ID del dispositivo** para copiar el ID del dispositivo.
3. Si selecciona la opción de correo electrónico, escriba la dirección de correo electrónico del administrador en el campo **Destinatario:** y envíe el correo electrónico.
4. Vaya a "Importación de un token del software".

Enviar su ID de dispositivo por correo electrónico para tokens adicionales

Si necesita tokens de software adicionales y su administrador quiere vincularlos, debe proporcionarle el ID del dispositivo con cada solicitud. Su ID de dispositivo aparecerá en la pantalla Información.

Para enviar el ID del dispositivo por correo electrónico para tokens adicionales:

1. Puntee **Información**.
2. Realice una de las siguientes acciones:
   - Puntee **ID del dispositivo** > **Enviar el ID del dispositivo por correo electrónico** para abrir un mensaje de correo electrónico que contenga el ID del dispositivo.
   - Puntee **ID del dispositivo** > **Copiar el ID del dispositivo** para copiar el ID del dispositivo.
3. Si selecciona la opción de correo electrónico, escriba la dirección de correo electrónico del administrador en el campo **Destinatario:** y envíe el correo electrónico.
4. Vaya a "Importación de un token del software".

Importación de un token del software

Recibirá un token del software en un mensaje de correo electrónico como archivo adjunto mediante un enlace a una URL, o quizás su administrador le pida que escanee un QR Code®. Es posible que también deba proporcionar una de las siguientes opciones cuando se le solicite:

- Una contraseña
- Un código de activación de un solo uso

Quick Start de RSA SecurID® Software Token 2.0.4 for Android™

Asegúrese de tener la contraseña o el código de activación disponibles antes de comenzar la importación del token.

Utilice uno de los siguientes procedimientos de importación, según las instrucciones por correo electrónico que haya recibido.

Archivos adjuntos de correo electrónico

Para importar un token desde un archivo adjunto de correo electrónico:

1. Abra el correo electrónico en su dispositivo y busque el mensaje con el archivo adjunto (extensión de archivo .sdtid).
2. Toque el archivo adjunto.
3. Si se le solicita, introduzca la contraseña. Puntee **Aceptar**.
4. Por motivos de seguridad, elimine el correo electrónico.

Enlace a URL

Para importar un token desde un enlace a una URL recibido en un correo electrónico:

1. Abra el correo electrónico del dispositivo y busque el mensaje con el enlace a la URL.
2. Toque el enlace a la URL.
3. Cuando se le solicite "Complete action using", puntee **RSA SecurID**.
4. Si se le solicita, introduzca el código de activación o la contraseña. Puntee **Aceptar**.
5. Si se le solicita aceptar un certificado de servidor, puntee **Aceptar**.
6. Por motivos de seguridad, elimine el correo electrónico.

Opción de importación de URL

Utilice el siguiente procedimiento manual si no puede importar token punteando un enlace a una URL.

Para importar un token de software mediante la opción Importar URL:

1. Abra el correo electrónico del dispositivo y busque el mensaje con el enlace a la URL.
2. El enlace a la URL texto comienza con **http://127.0.0.1/securid**. Puntee y sostenga el enlace y seleccione la opción Copiar.
3. Desplácese a la aplicación RSA SecurID. En la pantalla de bienvenida, puntee **Importar token > Importar URL**.
4. En el campo de texto, puntee y sostenga, y luego puntee **Pegar**.
5. Si se le solicita, introduzca el código de activación o la contraseña, y puntee el botón Introducir.
6. Si se le solicita aceptar un certificado de servidor, puntee **Aceptar**.
7. Por motivos de seguridad, elimine el correo electrónico.

Nota: Para importar tokens adicionales manualmente, puntee **Lista de tokens** y, a continuación, **Importar URL**.

Examen de QR Code

Siga las instrucciones del administrador para acceder al QR Code que contiene los datos de su token. A continuación, siga las instrucciones del administrador para capturar el QR Code.

Para importar un token de software mediante el escaneo de un QR Code:

1. Desplácese a la aplicación RSA SecurID. En la pantalla de bienvenida, puntee **Importar token > Examen de QR Code**.
2. Asegúrese de que el QR Code esté claramente visible en su totalidad. Apunte la cámara hacia el QR Code para capturarlo.
3. Si se le solicita, introduzca el código de activación o la contraseña, y puntee **Aceptar**.

Nota: Para importar tokens adicionales mediante el escaneo de un QR Code, puntee **Lista de tokens** y, a continuación, **Examen de QR Code**.

Configuración de un PIN

Nota: Si el token no requiere un PIN, vaya a "Autenticación en un recurso protegido".

Antes de empezar

Según el token importado, al iniciar la aplicación RSA SecurID, verá la pantalla Introducir PIN en la pantalla Tokencode.

Realice una de las siguientes acciones:

- Si ve la pantalla Introducir PIN, vaya a la sección siguiente, "Establecer un PIN (Pantalla Introducir PIN)".
- Si ve la pantalla Tokencode, vaya a "Establecer un PIN (pantalla Tokencode)".

Establecer un PIN (Pantalla Introducir PIN)

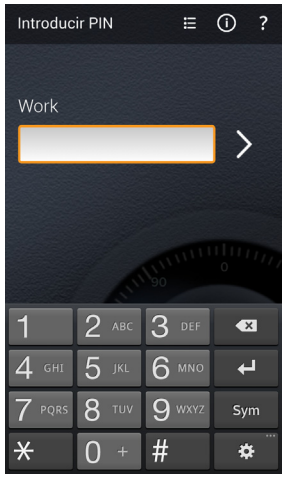
Para establecer un PIN mediante la pantalla Introducir PIN (ejemplo de VPN):

1. Desde su equipo (o su dispositivo, según corresponda), conéctese a la VPN corporativa.
2. Introduzca el nombre de usuario y deje abierta la pantalla de inicio de sesión.

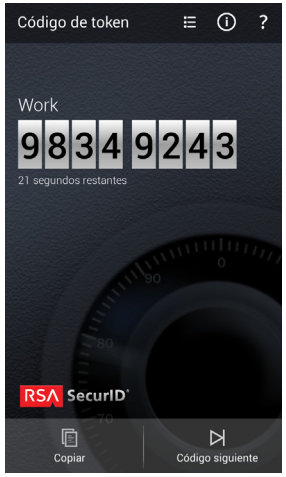
3. En el dispositivo, inicie la aplicación SecurID.

Quick Start de
RSA SecurID® Software Token 2.0.4 for Android™

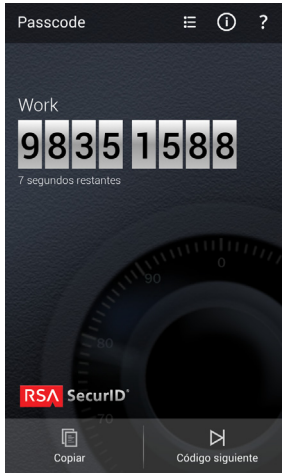
4. En la pantalla Introducir PIN, puntee la tecla **Introducir** o deslice el dedo hacia la izquierda.



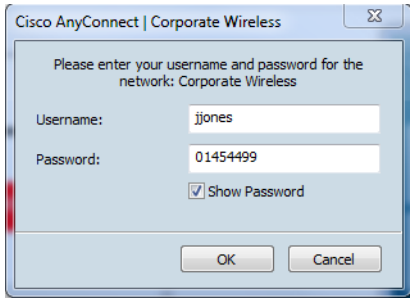
El dispositivo mostrará un tokencode.



5. Desde la pantalla de inicio de sesión de VPN, introduzca el tokencode en el campo **Passcode o contraseña**. Se le solicitará que cree un PIN. El PIN debe contener entre 4 y 8 dígitos y no puede comenzar con un cero.
6. Introduzca y confirme el nuevo PIN. La VPN le solicitará que introduzca un passcode.
7. En el dispositivo, puntee el botón **Volver** o deslice el dedo hacia la derecha para volver a la pantalla Introducir PIN.
8. Introduzca el PIN y puntee la tecla **Introducir** o deslice el dedo hacia la izquierda para mostrar un passcode.



9. Desde la pantalla de inicio de sesión de VPN, introduzca el passcode y haga clic en **Aceptar**.



Nota: Si accede al cliente de VPN desde su dispositivo, puede puntear la opción **Copiar** desde el menú de la aplicación para copiar el passcode y luego pegar el passcode en la pantalla de inicio de sesión de VPN.

Establecer un PIN (pantalla Tokencode)

Para establecer un PIN mediante la pantalla Tokencode (ejemplo de VPN):

1. Desde su equipo (o su dispositivo, según corresponda), conéctese a la VPN corporativa.
2. Introduzca el nombre de usuario y deje abierta la pantalla de inicio de sesión.

3. En el dispositivo, inicie la aplicación SecurID y vea el tokencode.

4. Desde la pantalla de inicio de sesión de VPN, introduzca el tokencode en el campo **Passcode o contraseña**. Se le solicitará que cree un PIN. El PIN debe contener entre 4 y 8 caracteres y no puede comenzar con un cero.

5. Introduzca y confirme el nuevo PIN. La VPN le solicitará que introduzca un passcode.
6. En el dispositivo, puntee **Código siguiente**.
7. Vuelva a la pantalla de inicio de sesión de VPN. En el campo **Passcode o contraseña**, introduzca el PIN. (Aquí, el PIN es 18395862). Introduzca el código de token a la derecha del PIN. Haga clic en **Aceptar**.

Autenticación en un recurso protegido

Siga estas instrucciones para autenticarse en un recurso protegido del equipo o del dispositivo. En el siguiente ejemplo, el recurso reside en un equipo.

Selección de un token (si es necesaria)

Si tiene varios tokens de software y necesita utilizar un token que no es el token activo, seleccione el token antes de iniciar el proceso de autenticación.

Para seleccionar otro token:

1. En el dispositivo, inicie la aplicación RSA SecurID.
2. Seleccione **Lista de tokens**.
3. Puntee el nombre del token que necesita. Con esto, se activa el token.

Autenticación

Para autenticarse (ejemplo de VPN):

1. Conéctese a la VPN corporativa.
2. Introduzca el nombre de usuario y deje abierta la pantalla de inicio de sesión.
3. En el dispositivo, inicie la aplicación RSA SecurID.
4. Realice una de las siguientes acciones:
   - Si ve la pantalla Introducir PIN, introduzca el PIN y puntee **Introducir**. El dispositivo mostrará un passcode. Introdúzcalo en el campo **Passcode** (o **Contraseña**) de la VPN.
   - Si el token requiere un PIN y la aplicación RSA SecurID muestra la pantalla Tokencode, escriba su PIN en el campo **Passcode** (o **Contraseña**) de la VPN e introduzca el tokencode que se muestra a la derecha de su PIN.
   - Si el token no requiere un PIN, escriba el tokencode en el campo **Passcode** (o **Contraseña**) de la VPN.

Autenticación con código siguiente

A veces, después de introducir una contraseña de un solo uso, es posible que se le solicite introducir el código siguiente (tokencode o passcode) para completar el proceso de autenticación. Esto puede deberse a diferentes motivos, por ejemplo, si se introducen demasiadas contraseñas de un solo uso incorrectas consecutivamente. Solicitar el código siguiente ayuda a garantizar que el código es generado por un token que está en poder de un propietario autorizado.

Para autenticarse con el código siguiente:

1. Cuando se le solicite el código siguiente, vuelva a la aplicación RSA SecurID en el dispositivo.
2. Puntee la opción **Código siguiente**.
3. En el recurso protegido, introduzca el código.