Guide

End User Journey Guide

Configuring Device Trust with JumpCloud Protect App™ and JumpCloud Go™

Configuring Mobile Device Trust

JumpCloud Mobile Device Trust brings JumpCloud Go™ to mobile devices and enables seamless, secure access to JumpCloud-protected resources on the go. Using the JumpCloud Protect mobile app, you can register your device with JumpCloud Go, and enable biometric, passwordless verification when accessing protected resources.

The creation of Conditional Access Policies in combination with JumpCloud Go for Mobile, enforces Device Trust. This protects your company's resources by ensuring you can access them only on trusted devices. Using a combination of JumpCloud Device Management, JumpCloud Go, JumpCloud Protect, and Conditional Access Policies (CAPs), IT Admins can safeguard access to both the JumpCloud User Portal and individual apps (native and SSO).

Prerequisites:

1. Your device is enrolled in JumpCloud Device Management:
   - **For a company-owned device, you'll need to work with your admin to enroll it.**
     - For Apple devices, see **Add Company-Owned iOS Devices to MDM.**
     - For Android devices, see **Enrolling Company-Owned Android Devices**.
   - For a personal or BYOD device, you can enroll it yourself. See **Enrolling a Personal Device in Device Management** to learn more.
2. Your admin deploys the JumpCloud Protect app to your device. If you don't see it on your device, contact your admin.
3. Your device meets certain security and compliance requirements. For example, your device must be running a supported OS:
   - **Apple:**
     - iOS 14+
     - iPadOS 14+
   - **Android:**
     - Android 5.0+
     - Google Play Services must be enabled on your device.
4. Biometrics are configured on your device.

Note: Mobile devices can be trusted when they are enrolled in JumpCloud Device Management, have the JumpCloud Protect app deployed using Software Management, and are registered with JumpCloud Go.

Note: You can only access resources that are assigned by your admin. Once registered, if you don't see a particular SSO app available in the User Portal, contact your admin.

Configuring the JumpCloud Protect App

JumpCloud Protect is a mobile app for iOS and Android that can be used for Multi-Factor Authentication (MFA) or 2-step verification. Once the app is downloaded, and the device is enrolled, the app can be used for push notifications, as an authenticator (TOTP) or for passwordless (JumpCloud Go).

After enrolling your device in Device Management, your admin needs to deploy the JumpCloud Protect app to your device. If you don't see the app on your device home screen or app library, contact your admin.

Configuring the JumpCloud Protect app varies depending your device and enrollment type:

For Android devices:

- When your device is enrolled in Android EMM, your admin will either install the JumpCloud Protect app onto your device or Work Profile, or it will be available in the Managed Google Play Store for you to install at your leisure.

For Apple devices:

- **Automated Device Enrollment** (Company-owned): JumpCloud MDM can silently push a managed instance of JumpCloud Protect or silently take over a personally installed version of JumpCloud Protect.
- **Profile-driven Device Enrollment** (Company-owned): JumpCloud MDM can push a managed instance of JumpCloud Protect or take over a personally installed version of JumpCloud Protect, but will prompt you to approve.
- **User Enrollment** (BYOD): JumpCloud MDM can push a managed instance of JumpCloud Protect and prompt you to approve. However, if you already have a personally installed version of JumpCloud Protect, you will need to decide whether to remove it and have the admin push it or you can use the existing JumpCloud Protect app.

Warning: Deleting the JumpCloud Protect app will remove and invalidate your Mobile Push, TOTP tokens, and JumpCloud Go token.

Registering Your Device with JumpCloud Go

Use the managed JumpCloud Protect app to register your device with JumpCloud Go and create a secure token on your device for accessing protected company resources.

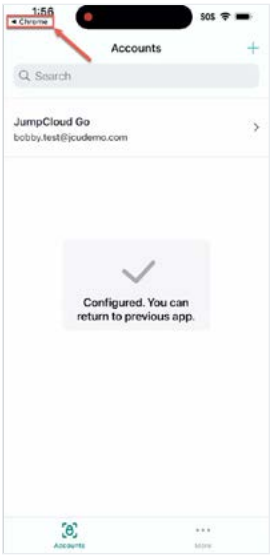
Note: You can't register your device directly from the JumpCloud Protect app; you must register your **device from the JumpCloud User Portal in the browser.**

1. In your device browser, go to the JumpCloud User Portal.
2. In the **Email** field, enter your company email address and tap **Continue**.
3. The **JumpCloud Passwordless Login** automatically appears.
   - (On Apple devices) At the popup for **"JumpCloud Protect"** wants to use **"jumpcloud.com" to Sign In**, select **Continue**.

Important: For Android devices with a Work Profile, you must configure biometrics and a PIN specifically for the Work Profile to proceed.

4. The **User Login** page appears. In the **Email** field, enter your company email address and select **Continue**.
5. In the **Password** field, enter your password and select **Log in**.
   - If your organization requires multi-factor authentication (MFA), approve the authentication request with your configured authentication method. See MFA for Users to learn more.

6. The **Passwordless Login** screen appears and redirects you to JumpCloud Protect to complete the registration process.
   - (On Apple devices) When complete, the JumpCloud Protect app displays this message: **Configured. You can return to the previous app**.
   - (On Apple devices) Tap the top left of the screen to return to the browser and the User Portal.



Apple Tutorial: Review the tutorial, **Using JumpCloud Go on iOS and iPadOS** for a guided walkthrough of the registration process on Apple iOS and iPadOS devices.

Android Tutorial: Review the tutorial, **Using JumpCloud Go on Android** for a guided walkthrough of the registration process on Android devices.

7. Your device is registered with JumpCloud Go. When you return to the User Portal, use JumpCloud Go to verify your identity with biometrics.

Verifying Your Identity with JumpCloud Go

Registering your mobile device with JumpCloud Go enables seamless access to any of your protected resources. When you access the User Portal or a protected resource, JumpCloud Protect is automatically called and uses JumpCloud Go to verify your identity with device biometrics (fingerprint or FaceID for example). You don't need to enter any additional credentials.

Checking JumpCloud Go in the Protect App

You can check your JumpCloud Go registration status, or disable it as an authentication method within the JumpCloud Protect app:

1. On your mobile device, open the JumpCloud Protect app and select the **Accounts** tab.
2. Locate the **JumpCloud Go** entry in the list and tap to select it.
3. (Optional) You can view more details on the token, or delete it if you need.
4. (Optional) In the bottom right of the Protect app, go to the **More** tab and select Settings. Under **JumpCloud Go**, you can toggle JumpCloud Go to disable it.

Tip: Disabling JumpCloud Go in the JumpCloud Protect application lets you sign in without passwordless functionality. This can be helpful if you are testing with other credentials or you run into issues with the JumpCloud Go authentication.