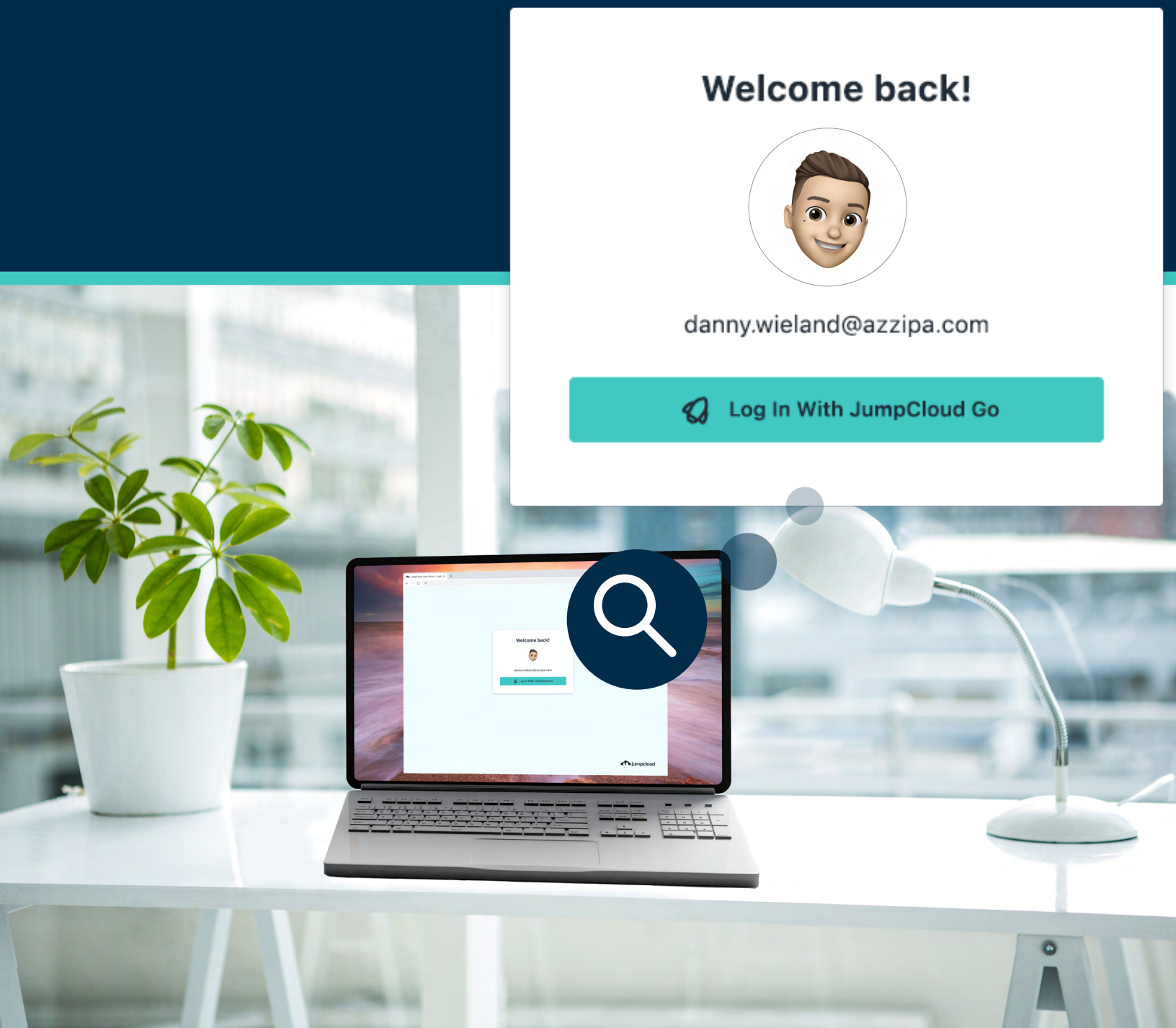
jumpcloud™

Whitepaper

JumpCloud Go™

Offer users a faster, safer, more seamless login experience with phishing-resistant passwordless multi-factor authentication



Contents

What is JumpCloud Go™?

JumpCloud Go is a hardware-protected and phishing-resistant multi factor login method that allows organizations to limit their attack surface and protect employees working online from JumpCloud managed work devices.

Enabling strong multi-factor authentication is the single most important thing organizations can do to stay safe online, however as with any technology, the security provided by a solution depends on the underlying capabilities. JumpCloud Go is more than just a MFA solution, it is a modern multifactor device authenticator that uses a combination of up to three factors (what you know, what you are, and what you have) to validate a user's identity. This greatly reduces the risk of phishing attacks, session theft, and drastically limits an organization's risk exposure to MFA bypass attacks.

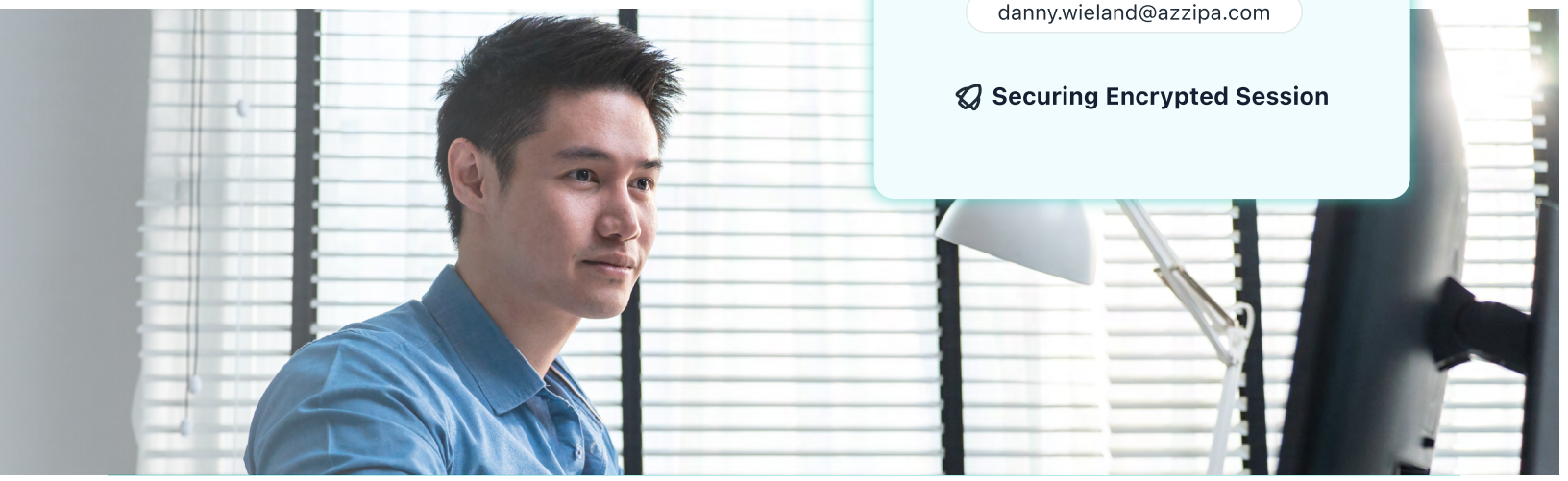
JumpCloud Go is supported on macOS and Windows and integrates with device biometric authenticators (Apple Touch ID or Windows Hello) to satisfy traditional password sign-in prompts, allowing for a passwordless user login experience. JumpCloud Go is also supported on Linux and integrates with local device password authentication prompts. Users experience minimal interruptions with JumpCloud Go, and are prompted for input only when required. This simpler and more secure login experience drastically reduces exposure to cyber attacks, improving both security and productivity.

To use JumpCloud Go, users must be working from JumpCloud Agent-managed devices that have a JumpCloud Go browser extension installed. The JumpCloud Agent can be used alongside any device management tool and is not dependent on organizations utilizing JumpCloud for full device management.

Organizations can deploy the required browser extension effortlessly using JumpCloud policies or leverage JumpCloud's deep integration with Chrome Browser Cloud Management to facilitate and enforce extension installation in Chrome via the Google Admin console.

Passwordless login is facilitated by integrations with device biometric authenticators, such as Apple's Touch ID or Windows Hello, which combine with JumpCloud Go to allow users to satisfy traditional password sign-in or MFA challenges without inputting a username or password.

By integrating with device authenticators on trusted and managed devices, JumpCloud Go authentication always represents two authentication factors representing both "Proof of Possession" and "User Verification / Inherence" factors. When a request is made for a JumpCloud-protected SSO resource using JumpCloud Go, the session is issued only after requests are cryptographically verified by a hardware protected key and the JumpCloud login service. JumpCloud Go is phishing-resistant by default and sessions are only issued to JumpCloud Agent managed user accounts on trusted devices.



Benefits of JumpCloud Go

Mitigate Risk Of Session Hijacking

Session hijacking – sometimes called cookie hijacking or cookie side-jacking – occurs when an attacker gains unauthorized access to a user's accounts via an attack that compromises their web session.

As one of the commonly leveraged attack methodologies used by adversaries to target users (according to **MITRE ATT&CK**), JumpCloud Go mitigates this risk by limiting their ability to replay sessions. If a bad actor manages to gain access to a user's JumpCloud session by capturing their cookie, the attacker is powerless to leverage this session to gain access to managed resources outside of the physical device. User sessions are issued only after requests are cryptographically verified by a hardware protected key and the JumpCloud login service. Nonces are used extensively to prevent any reply attacks during the JumpCloud Go authentication flows in addition to a modified PKCE (Proof Key for Client Exchange) to ensure that state is maintained between JumpCloud and the device.

Phishing-Resistant Authentication

Everytime an authentication flow sends a one-time password or a push notification, it exposes users to a potential phishing attack. JumpCloud Go uses hardware protected cryptographic security tied to physical devices to reduce an organization's exposure to potential phishing attacks. After users register their devices for JumpCloud Go, all subsequent logins are phishing-resistant. This drastically reduces the risk of a user's device being compromised by a 2FA bypass attack.

Zero Trust Foundation

Zero trust emphasizes that only trusted devices access resources. JumpCloud Go anchors trust to both the device and the device identity within Apple's Secure Enclave or the Trusted Platform Module (TPM). Using device-specific cryptographic methods instead of passwords boosts security and forms the basis for Zero Trust.

3rd Party MDM & EMM Compatible

JumpCloud Go is deployed using the JumpCloud Agent which can be used with any device management tool. Pair it with JumpCloud MDM or integrate it with any enterprise mobility management (EMM) or mobile device management (MDM) solution.

Passwordless Login

Users on macOS and Windows can enjoy a passwordless and secure multifactored login experience to all of their JumpCloud web based resources using JumpCloud Go. Access is secured by continuous authentication and authorization to resources using hardware-based cryptographic functions. Users gain significant time back when they are not constantly required to authenticate using a password and higher friction MFA factors to access organizational resources.

Minimize Potential Impact of Compromise

JumpCloud Go enables organizations to configure an adaptive security posture where the risk level of each application can be used to determine the session duration. Organizations can default to the shortest supported durations service providers support with negligible impact on the user experience. Application sessions are secured continuously and transparently, without needing any user interaction. If an attacker gains access to an active session their time to perform malicious activities is limited to the remaining duration of the session.

Authenticator Assurance Level 3

Authenticator Assurance Level 3 (AAL3) ensures the highest level of confidence in verifying that a user has access to specific authenticators enrolled to their account during authentication. This level verifies access using cryptographic methods that prove the user has a specific key on a specific device. For AAL3 authentication, a secure physical device is required. JumpCloud Go represents control of two separate authentication methods, using recognized cryptographic methods.

Simpler and Safer Employee Experience

The JumpCloud Go user login experience is simpler and safer for users than traditional methods. It transparently creates safer login habits while reducing authentication fatigue. JumpCloud Go significantly reduces the amount of login prompts users face daily and saves organizations valuable time without requiring the storage of the user's password in a password management system. IT organizations benefit from less end user support requests related to assisting users with lockout, password, or account recovery issues.

Key Concepts

The following key concepts power JumpCloud Go.

JumpCloud Agent

Installing the JumpCloud Agent on a device registers it within the JumpCloud Directory Platform and unlocks device identity management capabilities. Via the JumpCloud Agent, cloud accounts can be provisioned to or joined with existing local accounts.The agent facilitates integration with JumpCloud's open directory, granting command and control over local device account management, authentication (AuthN), and authorization (AuthZ).

JumpCloud Managed Local Device Account

Administrators have the ability to manage the lifecycle and state of the local accounts on devices using the JumpCloud Agent. The JumpCloud Directory Platform allows administrators to create or migrate local device accounts to JumpCloud management. This is done by associating a JumpCloud user account with a managed device or via user led self-service on device sign ins.

The username attribute, or the Local User Account attribute if populated, of the associated JumpCloud user account is used to determine if a net new account will be created on the device or if an existing account will be migrated. JumpCloud managed accounts have their password synced with the associated JumpCloud user account, can be required to sign in with configured JumpCloud MFA factors, and have local device account permissions (AuthZ) controlled via JumpCloud.

JumpCloud Fully Managed Workstation

MacOS and Windows Desktop devices are considered "fully JumpCloud managed" when the JumpCloud Agent is installed and they are enrolled in JumpCloud Mobile Device Management (MDM). Linux devices are considered fully managed when the JumpCloud Agent is installed. When configuring and deploying workstations for end users, administrators have multiple ways to enroll devices into JumpCloud that result in full management. JumpCloud Go does not require full management as the JumpCloud Go components and authentication framework are delivered via the JumpCloud Agent only.

When a device is enrolled into JumpCloud, an object with a unique identifier in the JumpCloud directory is generated and decorated with additional context about the device such as the device's hostname, OS version, model, management status and more.

A JumpCloud org administrator can search for a JumpCloud fully managed device in the admin UI and take actions on the device related to device identity, device configuration, and management. By associating JumpCloud user accounts with fully managed devices, org admins can control the JumpCloud managed user accounts on the device that are capable of using JumpCloud Go.

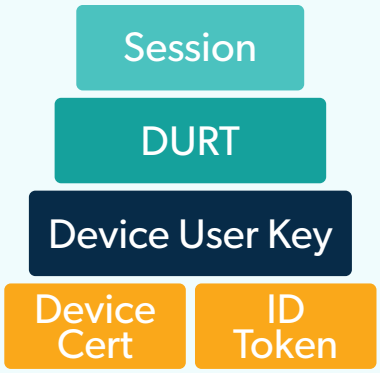
JumpCloud Jointly Managed Workstation

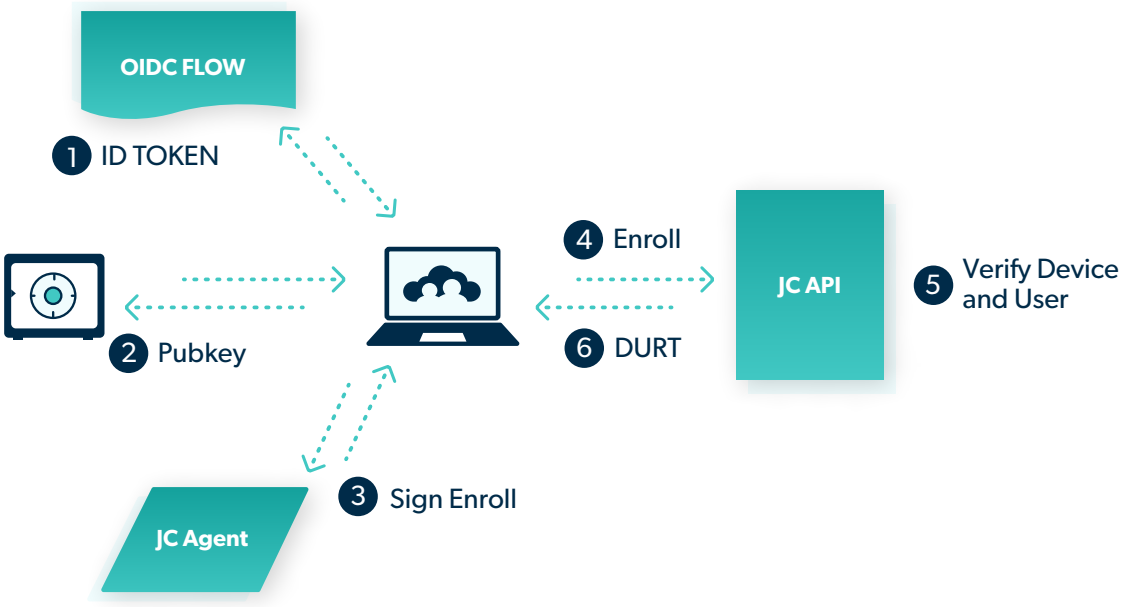
MacOS and Windows devices can be jointly managed with the JumpCloud Agent and an external 3rd Party MDM or EMM. Devices that are under joint management can leverage JumpCloud Go authentication capabilities.

JumpCloud Go in Depth

Enrollment

Installing the JumpCloud Agent on a device registers it within the JumpCloud Directory Platform and unlocks device identity management capabilities. Via the JumpCloud Agent, cloud accounts can be provisioned to or joined with existing local accounts.The agent facilitates integration with JumpCloud's open directory, granting command and control over local device account management, authentication (AuthN), and authorization (AuthZ).





JumpCloud Go anchors its trust to both the device and the user. During the enrollment process the user authenticates to JumpCloud's OpenID Connect service and is issued an ID Token for the JumpCloud Go application. A new DUK (Device User Key) is created from the Secure Enclave (on Apple devices) or the Trusted Platform Module (TPM) (on Windows systems). This is added to a JWT (JSON Web Token) that is then signed by the JumpCloud Agent certificate unique to the device and used by the JumpCloud Agent to authenticate all traffic back to JumpCloud.

The JumpCloud Go enrollment request is validated by JumpCloud's DURT (Device User Refresh Token) API through the following process:

1. The JWT's signature is validated by first ensuring the certificate in the x5c claim in the JWT header is a valid JumpCloud Agent certificate in good standing.
2. The JWT signature is checked to ensure it was signed by the private key of the same agent certificate.
3. The JWT is inspected to ensure it hasn't expired and is otherwise valid.
4. The embedded ID Token is validated back to the JumpCloud OpenID Connect service via its embedded signature using the OIDC JWKS.

After registration is complete, a new DURT (Device User Refresh Token) is generated by the DURT API and registered to the unique user-device combination. The DURT is sent back down to the client where it is treated in a similar fashion to an OAuth Access token. The DURT is kept in the local user's keychain along with a reference to the DUK stored in the hardware-backed encryption service on the device.

The registration process is kicked off when a user navigates to a JumpCloud-protected SSO resource in Chrome. The user will be redirected to JumpCloud's User Portal and prompted to authenticate. This also happens if the user navigates directly to the portal.

When the portal loads it will look for the JumpCloud Go Chrome extension. If the extension is installed and the device is not currently registered with JumpCloud Go, the user will be offered a JumpCloud Go button to sign in, or they can provide an email address to sign in without JumpCloud Go.

Selecting a JumpCloud Go login will take the user through a normal sign in process, complete with MFA, if that's required. This process will generate an OIDC ID Token and start the registration process.

Enrollment

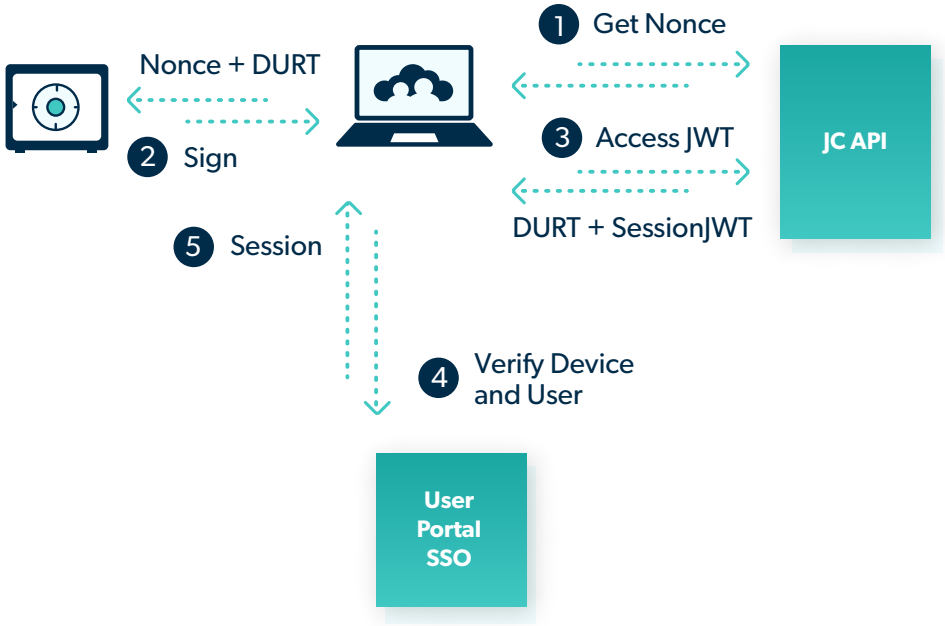
Once registered, when a user navigates to any SSO resource in Chrome, they will be directed to JumpCloud's User Portal to sign in. This will trigger a similar process to the registration flow; however, in this case a Device User Refresh Token is already available on the system.

JumpCloud's User Portal will generate a PKCE challenge and a request to be used with the DURT to grant access to the resource. The Chrome extension will forward this request to a Native Messaging Host that will in turn connect to a local service (on macOS) or the JumpCloud Agent (on Windows and Linux).

The request will be combined with the current DURT and a nonce issued by the DURT API into a JWT and then signed by the Device User Key (DUK) on the device and sent to the DURT API. The API will validate the signature with the DUK by looking at the current registration for that device and user, ensure the nonce has not been used before, and then ensure the DURT has not been used.

If everything passes, the DURT API will create a DUST (Device User Session Token) signed by the DURT API, and create a new DURT and send both back to the device. The new DURT will replace the previous DURT in the local user's keychain. The DUST will then be sent to JumpCloud's User Portal which will accept the DUST for user authentication and then go through its normal conditional access process to determine if that user has access to this resource.

If the user passes those checks, JumpCloud will issue a SAML assertion or an Open ID Connect token set, depending on the type of SSO connection that was requested, back to the SSO resource which will then sign the user in and take whatever next steps are appropriate.



User Flows

Scenario 1: A user's first time logging in with JumpCloud Go

1. User is working within a web browser running the JumpCloud Go extension from a JumpCloud Agent managed local device account.
2. User initiates authentication to a JumpCloud protected resource by clicking the Log in with JumpCloud Go button.
3. Users are prompted to enter their user email address, password, and challenged with any MFA requirements to access their resource.
4. Users authenticate successfully using their work email address that is associated with and uniquely joined to the active session of the managed local device account.
5. A DURT is issued to the local device accounts hardware protected module (Secure Enclave/TPM).
6. Users are authenticated to resources via JumpCloud Go and granted access to the JumpCloud-protected resource using device-specific cryptographic methods instead of their password.

Scenario 2:

A user accesses a JumpCloud-protected web resource on a device with a valid and unlocked DURT

1. User navigates to a JumpCloud-protected resource and requests access.
2. A DURT is unlocked and valid.
3. JumpCloud Go passwordless login silently authenticates the user to the resource using device-specific cryptographic methods instead of a password
4. User is granted passwordless secure access to the JumpCloud-protected resource.

Scenario 3:

A user accesses a JumpCloud-protected web resource on a device with a valid and locked DURT

1. User navigates to a JumpCloud-protected resource and requests access.
2. A DURT is locked and valid.
3. Users are prompted to unlock the DURT using local device authenticators.
4. User successfully authenticates locally on device and unlocks DURT.
5. JumpCloud Go passwordless login silently authenticates the user to the resource using device-specific cryptographic methods instead of a password.
6. User is granted passwordless secure access to the JumpCloud-protected resource.

FAQ

Is JumpCloud Go enabled by default?

Yes. JumpCloud Go is the system-preferred most secure authentication method.

Can I use JumpCloud Go without using JumpCloud MDM?

Yes.

Can end users use JumpCloud Go from personal, unmanaged devices?

No.

Is JumpCloud Go supported on Linux Desktops?

Yes. JumpCloud is supported on Linux devices that have a TPM chip and are running a Linux distribution that supports the GNOME graphical user interface.

If JumpCloud Go is disabled, what happens when I enable it?

Enabling the JumpCloud Go feature has no direct end user facing impact. The presence of the JumpCloud Go browser extension on a managed device once the feature is enabled is the event that allows users to authenticate using JumpCloud Go.

Can I use Device Trust and JumpCloud Go?

Yes. JumpCloud Go supports and respects all conditional access policies.

Can biometric authenticators be used with JumpCloud Go?

Yes. With JumpCloud Go, users can use device biometric authenticators (Apple Touch ID or Windows Hello) to satisfy authentication challenges.

Are end users forced to use biometrics with JumpCloud Go?

No. Device biometric authenticators (Apple Touch ID or Windows Hello) are purposely built to complement local account passwords, not replace them. Users can opt to authenticate locally with a knowledge factor in place of a device biometric.

If users do not authenticate with biometrics do they realize the security benefits of JumpCloud Go?

Yes. The security benefits of JumpCloud Go are realized by all users. All JumpCloud Go user sessions are issued only after requests are cryptographically verified by a hardware protected key and the JumpCloud login service. The addition of a biometric gives you an additional optional factor that further mitigates security risks and speeds up authentication.

FAQ cont.

How can I install the JumpCloud Go browser extension on managed devices?

On fully managed devices organizations can use device policies to automate the deployment of the JumpCloud Go browser extension. Google Workspace customers can use Chrome Browser Cloud Management to deploy the extension to users. Users can also install the extension directly from extension web stores.

Does JumpCloud Go capture or store device login pictures?

No. During user verification the device login picture is displayed to the user on their local device. The device login picture is not captured or stored by JumpCloud. The device login picture is used to indicate to users that their local device account is secured by JumpCloud Go.

What happens if I disable JumpCloud Go?

Users working from managed devices will not be able to enroll via the Log in with JumpCloud Go flow. Users will be able to authenticate using a valid set of JumpCloud credentials. Existing JumpCloud Go issued sessions will be ignored.

Does JumpCloud hash local computer passwords during passwordless logins?

No. JumpCloud Go does not store or hash the local password during passwordless logins or during platform reauthentication.

What is the lifetime of a Device User Refresh Token (DURT)?

Once issued, a DURT is valid for 14 days and is continuously renewed as long as the user is actively using the DURT for passwordless authentication.

How long does a Device User Refresh Token (DURT) provide passwordless authentication?

Once issued, a DURT stays active for 12 hours. Users are prompted to authenticate using local device authenticators to re authenticate an inactive DURT when authenticating to JumpCloud protected resources.

How can I control who can authenticate with JumpCloud Go?

JumpCloud Go requires the JumpCloud Go browser extension. Having organizational management and control over users' browser setup can enable organizations to have complete control over which users have the ability to use JumpCloud Go.

Deploying JumpCloud Go to Your Workforce

JumpCloud Go authentication is enabled for new organizations by default.

Find the latest information surrounding the ways to deploy and enforce JumpCloud Go authentication for your users below.

Get Started: JumpCloud Go™

jumpcloud™

JumpCloud® helps IT teams **Make Work Happen**® by centralizing management of user identities and devices, enabling small and medium-sized enterprises to adopt Zero Trust security models. JumpCloud has been used by more than 200,000 organizations, including GoFundMe, Grab, ClassPass, Beyond Finance, and Foursquare. JumpCloud has raised over $400M from world-class investors including Sapphire Ventures, General Atlantic, Sands Capital, Atlassian, and CrowdStrike.

Get Started →

Blog

Daily insights on directory services, IAM, LDAP, identity security, SSO, system management, and the cloud.

Learn More →

Resources

JumpCloud's hub for videos, documentation, case studies, partner enablement tools, and more.

Learn More →

In the Press

Read what people are saying about JumpCloud.

Learn More →