Chrome Enterprise
Recommended

jumpcloud™

Integrate JumpCloud and Google Chrome Enterprise to Elevate Modern Device Trust

Secure applications on managed or unmanaged devices by enforcing Conditional Access Policies through Managed Chrome browser or Profiles.

Traditional perimeter based security controls are no longer sufficient in today's world of remote work and increased BYOD adoption. Granting access solely based on user credentials might lead to unsecured browser sessions, increasing security blind spots. Organizations need a zero-trust model that not only focus on identifying the user but also evaluates the device and browser posture at the access point.

JumpCloud's partnership with Chrome Enterprise revolutionizes how organizations trust devices. By enforcing security policies directly within the Chrome browser, regardless of the device being used, this integration offers a new level of control. It combines JumpCloud's Conditional Access Policies with Chrome's managed browser features, giving businesses a robust, adaptable, and scalable solution for secure access.

Discover the benefits

Gain a powerful, flexible and scalable way to secure access

- Enforce browser & user-based access rules; restrict non-Chrome access to critical apps.
- Protect sensitive data via Chrome DLP, even on personal devices.
- Secure at the browser level, reducing risk from unmanaged devices.
- Boost security with JumpCloud MFA if device trust is low.

Managed Device

User

Access

SSO Apps   User Portal

Managed Browser & Managed Work Profile
(based on allowed Organisation enrolment domains)

→ [Sign Up for a Free JumpCloud Trial](#)