

Google Chrome auf Apple Hardware

Das definitive Handbuch für die
Bereitstellung und Konfiguration
von Chrome auf Mac, iPad und
iPhone.



Chrome ist der von Google entwickelte Browser für Desktop- und Mobilgeräte mit über 2 Milliarden Benutzern. Da immer mehr Arbeitnehmer und Studierende für Arbeit und Ausbildung auf Geräte angewiesen sind, wird Chrome für die Produktivität der Benutzer immer wichtiger. Chrome wird von Unternehmen und Bildungseinrichtungen verwendet, um Benutzer auf sichere Art und Weise mit Online-Ressourcen zu verbinden.

Chrome ist mehr als nur ein Browser

Dank Erweiterungen, Richtlinienverwaltung und einer Vielzahl von unterstützten Plattformen ist Chrome mehr als nur ein Standardbrowser. Die Flexibilität und Erweiterbarkeit, die Chrome bietet, sorgt für eine verbesserte Zusammenarbeit und Anpassung, die es den Endbenutzern ermöglicht, das Internet nach ihren Wünschen zu gestalten, ohne die Sicherheit zu beeinträchtigen.

Chrome unterstützt Apple im Unternehmen

Der Typ des Installationspakets, die Verteilung, die Aktualisierungsmethoden und die Verwaltung der Einstellungen sowie die Kontrolle der Benutzerdaten sind Überlegungen, die Entwickler und Mac Administratoren bei der Erstellung und Bereitstellung von Unternehmenssoftware berücksichtigen müssen. Das Google Chrome Team hat eine Vielzahl der Best Practices übernommen.

Installationsprogramme

Unternehmen wollen schnellen Zugriff auf Mac freundliche Installer. Kein Administrator möchte seine Zeit mit dem Neupacken von DMGs verbringen. Das Chrome Team hat der Einfachheit Vorrang eingeräumt und bietet nun PKGs zur einfachen Verteilung an.

Chrome bietet die folgenden Installationsprogramme für Unternehmen an:

- Universal PKG Installer (x86 und ARM) für den Stable- und den Beta-Kanal (empfohlene Verteilungsmethode)
- Universal DMG Installer (x86 und ARM) für den Stable- und den Beta-Kanal

[Besuchen Sie die Seite für Unternehmensinstallationsprogramme von Google Chrome, um loszulegen.](#)

Konfigurieren von Chrome auf dem Mac – Chrome Browser Cloud Management

Bedeutung eines verwalteten Browsers

Als Hauptinstrument für den Zugriff auf Online-Ressourcen sollten Administratoren die Optimierung des Browser-Erlebnisses für Benutzer innerhalb ihrer Organisation in Betracht ziehen sowie verschiedene Richtlinien zur Informationssicherheit durchsetzen. Chrome verfügt über Hunderte von Richtlinien und Erweiterungs-Workflows, um sicherzustellen, dass Administratoren ihre Daten sicher und ihre Benutzer produktiv halten.

Was versteht man unter Chrome Browser Cloud Management?

- Chrome Browser Cloud Management ist der Ansatz von Google für ein modernes Browser-Management. Er ermöglicht Administratoren die zentrale Verwaltung des Browser-Einsatzes auf allen Plattformen im Unternehmen. Chrome Browser Cloud Management unterstützt derzeit macOS, Windows, verschiedene Linux-Distributionen, Chrome OS und iOS. Die Unterstützung von Android ist für 2021 geplant.

Mit Chrome Browser Cloud Management können Administratoren von einer benutzerfreundlichen Oberfläche aus verschiedene Richtlinien durchsetzen, Lesezeichen verwalten und auf Erweiterungssteuerungen zugreifen. Darüber hinaus können Administratoren dank der integrierten Berichtsfunktion Einblicke in die Browser-Situation erhalten.

Erfahren Sie mehr oder melden Sie sich für das [Chrome Browser Cloud Management](#) an



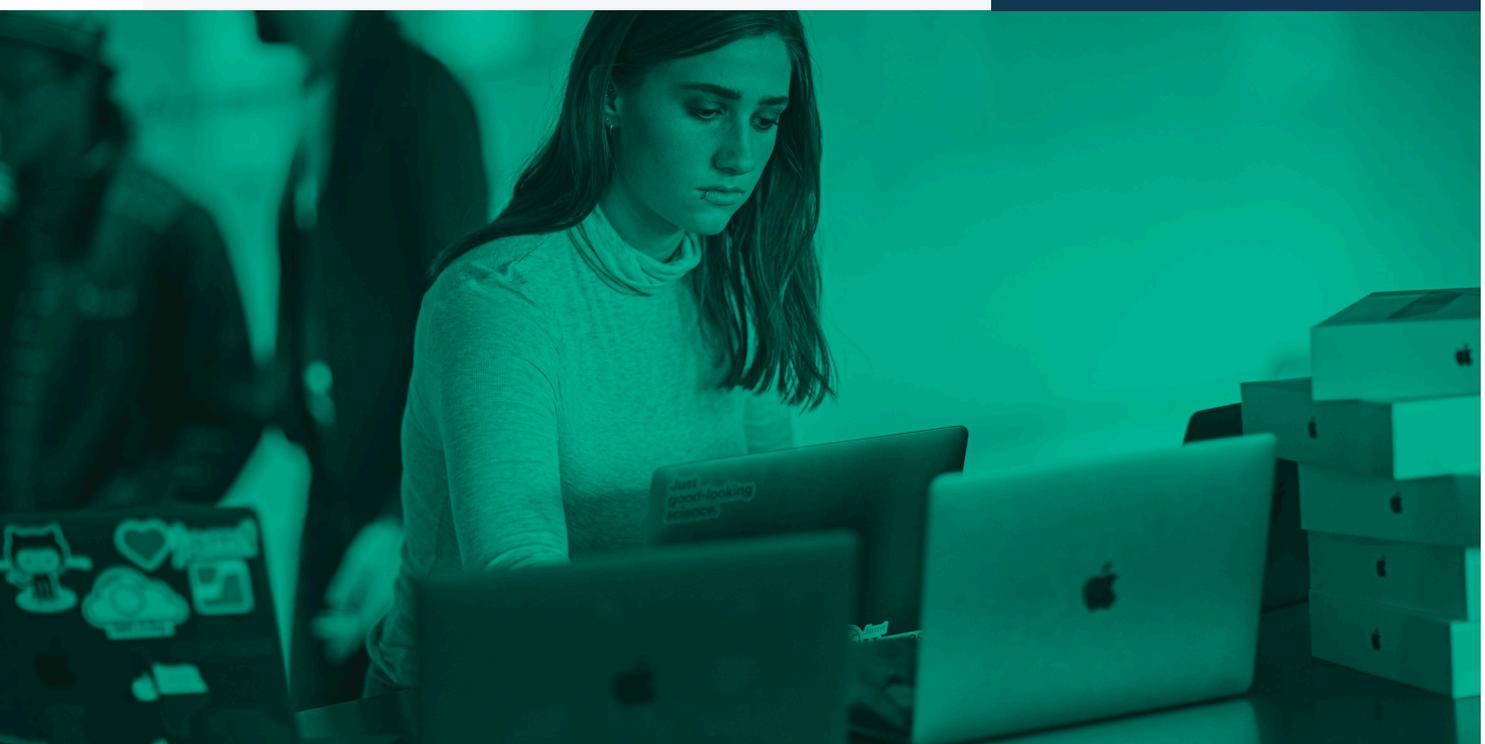
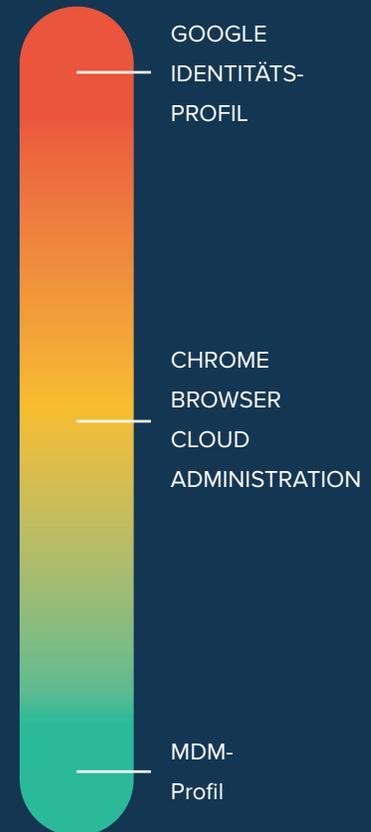
Was sind Anmeldetoken und Organisationseinheiten?

- Ein Anmeldetoken wird verwendet, um die Browser in der Cloud-Management-Lösung anzumelden. Diese Token können in Jamf Pro eingebracht werden, um die Anmeldung von Chrome auf einem Mac oder Smartphone zu vereinfachen. Der Token ermöglicht es Administratoren, Geräte basierend auf einer Organisationseinheit zu segmentieren, die geografisch oder auf einen Anwendungsfall ausgerichtet sein kann. Mithilfe der Organisationseinheit können Administratoren verschiedene Berichte filtern, die in der Verwaltungskonsole verfügbar sind. Der Token ist für alle Rechner, die sich bei einer bestimmten Organisationseinheit anmelden, gleich.

Managementebenen

- Bezüglich der Art und Weise, wie der Browser verwaltet werden kann, ist Chrome extrem flexibel. Standardmäßig hat das Vor-Ort-Management Vorrang vor dem Cloud-Management, und der Administrator hat die Möglichkeit, die Vorzugsreihenfolge umzukehren.
- Maschinenrichtlinien haben immer Vorrang vor Benutzerrichtlinien und werden auf der Grundlage der Google Identität angewendet, die der Benutzer im Browserprofil anmeldet. Dies ermöglicht Administratoren, eine gemeinsame Richtlinienenerfahrung auf allen Chrome Instanzen durchzusetzen. Unabhängig davon, wer im Chrome Profil angemeldet ist, erweitert Chrome das Erlebnis mit verschiedenen Richtlinien, die auf Benutzerebene festgelegt werden.

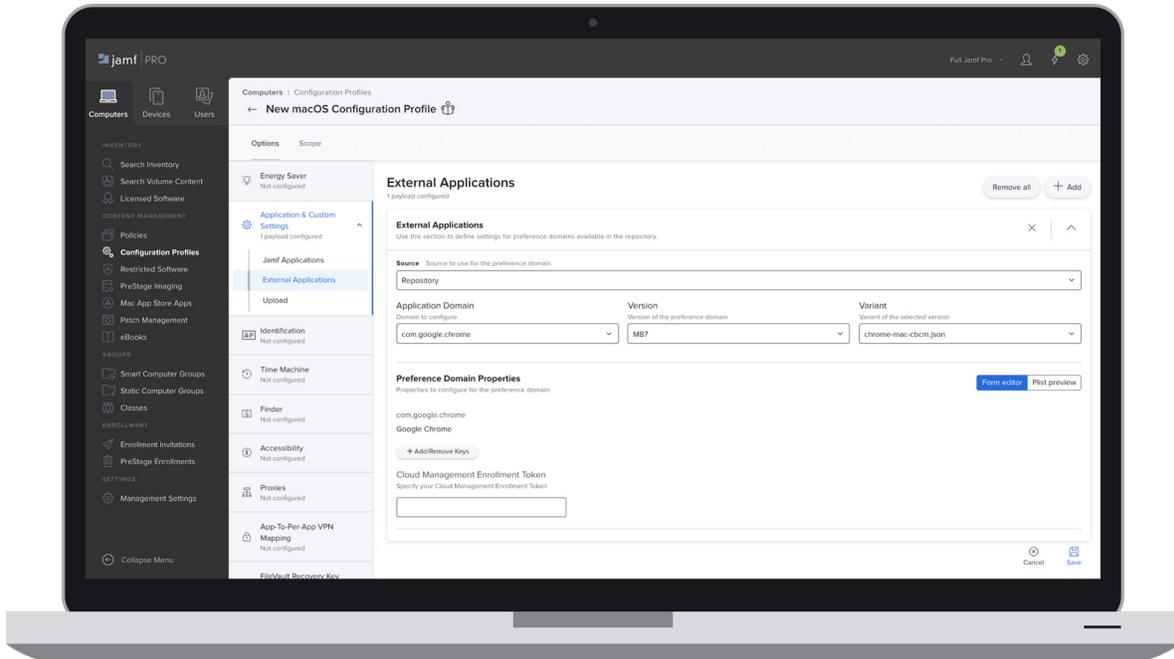
PRIORITÄT DES MANAGEMENTS



So melden Sie Chrome im Chrome Browser Cloud Management mit Jamf Pro an

Auch hier macht es Jamf den Administratoren extrem einfach, den Anmeldetoken zu konfigurieren.

Dazu wählt der Administrator [Chrome aus dem benutzerdefinierten Anwendungs-Repository](#) in einem Jamf Konfigurationsprofil aus, fügt den entsprechenden Anmeldetoken ein und weist ihn verschiedenen Geräten oder Gruppen zu.



Richtlinien

[Mit Chrome Richtlinien](#) können Administratoren verschiedene Funktionen und das Verhalten des Browsers konfigurieren. Ihre Funktionalität reicht von der Einstellung von Präferenzen bis hin zur Durchsetzung von Sicherheitsverfahren. Einige der am häufigsten eingesetzten Richtlinien sind:

- Homepage
- RelaunchNotification
- Google Sync Verhalten
- Speicherung von Cookies und Verläufen
- Unternehmensweit verwaltete Lesezeichen
- Deaktivieren des Inkognito-Modus
- Proxy-Konfiguration
- Erzwingung von Popup-Sperren

Erweiterungen

[Erweiterungen](#) ermöglichen es Administratoren oder Benutzern, die Funktionalität des Browsers zu erweitern. Die Funktion „Chrome Browser Cloud Management“ bietet Administratoren eine Vielzahl von Steuerungsmöglichkeiten für Erweiterungen.

Erweiterungsmanagement für den Bildungsbereich:

- Für einen Anwendungsfall im Bildungsbereich bietet Chrome Browser Cloud Management Administratoren die Möglichkeit, die Installation von Erweiterungen basierend auf den vom Browser angeforderten Berechtigungen zu beschränken. Administratoren können auch Erweiterungen blockieren, die aus anderen Quellen als dem Chrome Web Store installiert wurden. Zum Beispiel können Administratoren die Installation/Ausführung von Erweiterungen unterbinden, wenn diese versuchen, VPN- oder Proxy-Funktionen bereitzustellen.

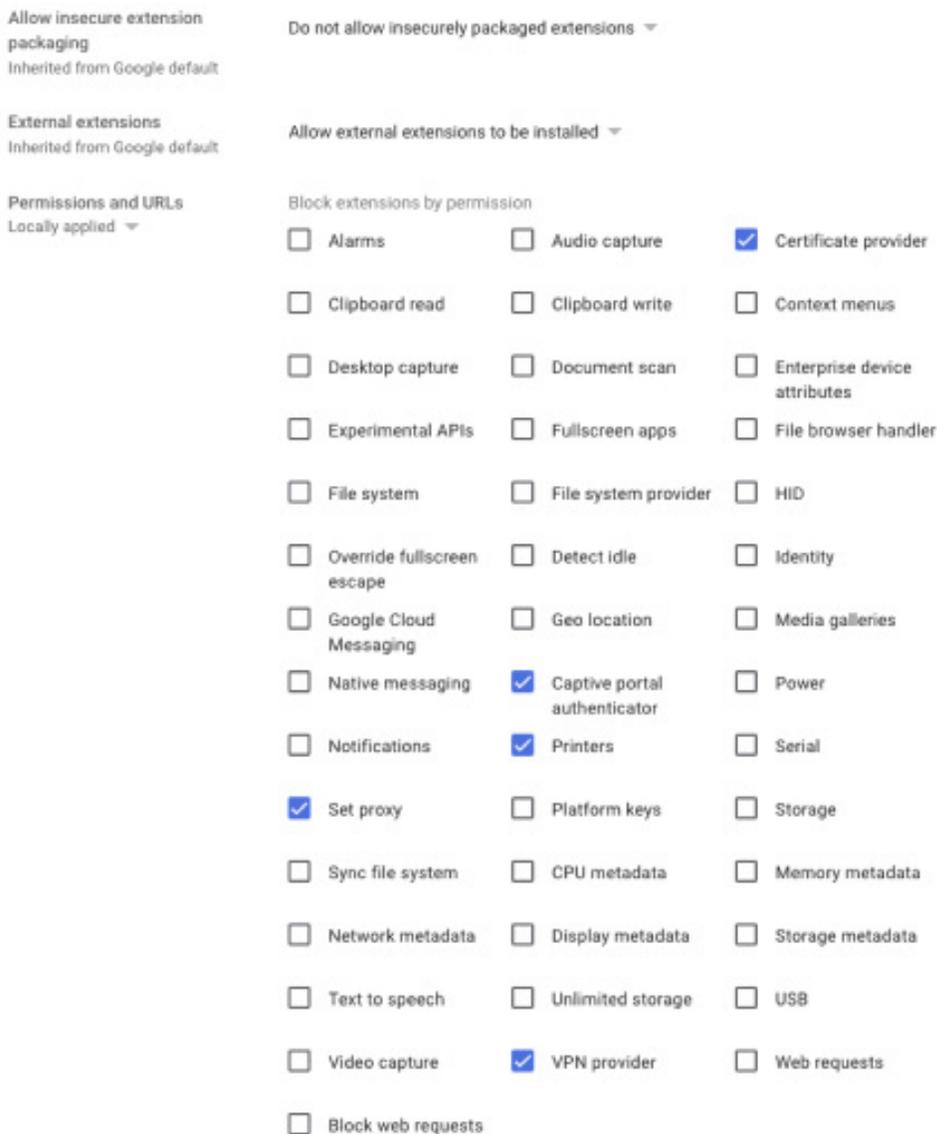
Conditional Access, gestützt durch BeyondCorp Enterprise, Jamf Pro und Chrome

Allgemeine Verfügbarkeit mit Jamf in Kürze.

BeyondCorp Enterprise, das Zero-Trust-Angebot von Google Cloud, ermöglicht Administratoren den Aufbau eines Compliance- und Sicherheits-Frameworks, das kontextbezogene Attribute wie Identitäts- und Geräteinformationen anstelle eines Netzwerkperimeters verwendet. Indem der Managementstatus von Jamf Pro in die Zugriffsrichtlinien übernommen wird, bestimmt BeyondCorp Enterprise, ob die Benutzer berechtigt sind, auf Unternehmensressourcen und SaaS-Anwendungen zuzugreifen. Diese Integration wird zum Teil von Chrome Erweiterungen unterstützt, und es wird empfohlen, dass Administratoren, die dieses Zero-Trust-Framework implementieren, die Erweiterungsverwaltung für die Durchsetzung von Richtlinien verwenden.

Erfahren Sie mehr über BeyondCorp Enterprise [Conditional Access auf dem Jamf Marketplace](#).

Erweiterungsmanagement mit Berechtigungen



The image shows a screenshot of the Chrome extension permissions settings page. The page is divided into three main sections: 'Allow insecure extension packaging', 'External extensions', and 'Permissions and URLs'. The 'Permissions and URLs' section is expanded, showing a list of permissions with checkboxes. The 'Do not allow insecurely packaged extensions' dropdown is set to 'Do not allow insecurely packaged extensions'. The 'Allow external extensions to be installed' dropdown is set to 'Allow external extensions to be installed'. The 'Block extensions by permission' section is expanded, showing a list of permissions with checkboxes. The 'Set proxy' checkbox is checked. The 'Certificate provider' checkbox is checked. The 'VPN provider' checkbox is checked. The 'Block web requests' checkbox is unchecked.

| | |
|--|--|
| Allow insecure extension packaging Inherited from Google default | Do not allow insecurely packaged extensions ▾ |
| External extensions Inherited from Google default | Allow external extensions to be installed ▾ |
| Permissions and URLs Locally applied ▾ | Block extensions by permission |
| | <input type="checkbox"/> Alarms |
| | <input type="checkbox"/> Audio capture |
| | <input checked="" type="checkbox"/> Certificate provider |
| | <input type="checkbox"/> Clipboard read |
| | <input type="checkbox"/> Clipboard write |
| | <input type="checkbox"/> Context menus |
| | <input type="checkbox"/> Desktop capture |
| | <input type="checkbox"/> Document scan |
| | <input type="checkbox"/> Enterprise device attributes |
| | <input type="checkbox"/> Experimental APIs |
| | <input type="checkbox"/> Fullscreen apps |
| | <input type="checkbox"/> File browser handler |
| | <input type="checkbox"/> File system |
| | <input type="checkbox"/> File system provider |
| | <input type="checkbox"/> HID |
| | <input type="checkbox"/> Override fullscreen escape |
| | <input type="checkbox"/> Detect idle |
| | <input type="checkbox"/> Identity |
| | <input type="checkbox"/> Google Cloud Messaging |
| | <input type="checkbox"/> Geo location |
| | <input type="checkbox"/> Media galleries |
| | <input type="checkbox"/> Native messaging |
| | <input checked="" type="checkbox"/> Captive portal authenticator |
| | <input type="checkbox"/> Power |
| | <input type="checkbox"/> Notifications |
| | <input checked="" type="checkbox"/> Printers |
| | <input type="checkbox"/> Serial |
| | <input checked="" type="checkbox"/> Set proxy |
| | <input type="checkbox"/> Platform keys |
| | <input type="checkbox"/> Storage |
| | <input type="checkbox"/> Sync file system |
| | <input type="checkbox"/> CPU metadata |
| | <input type="checkbox"/> Memory metadata |
| | <input type="checkbox"/> Network metadata |
| | <input type="checkbox"/> Display metadata |
| | <input type="checkbox"/> Storage metadata |
| | <input type="checkbox"/> Text to speech |
| | <input type="checkbox"/> Unlimited storage |
| | <input type="checkbox"/> USB |
| | <input type="checkbox"/> Video capture |
| | <input checked="" type="checkbox"/> VPN provider |
| | <input type="checkbox"/> Web requests |
| | <input type="checkbox"/> Block web requests |

Erweiterung über Chrome Browser Cloud Management Beta

Dank Chrome Browser Cloud Management haben Administratoren die Möglichkeit, einen Workflow für Erweiterungsanfragen zu konfigurieren. Beim Durchsuchen des Chrome Web Stores wird dem Benutzer statt der Möglichkeit, die Erweiterung zu installieren, eine Schaltfläche „Anfordern“ angezeigt. Der Administrator wird über die Anforderung benachrichtigt und kann dann Maßnahmen ergreifen, um die Installation der Erweiterung zuzulassen oder abzulehnen. Wenn eine Erweiterungsanforderung zum ersten Mal genehmigt wird, erhalten alle Benutzer in derselben Organisationseinheit die Berechtigung, die angegebene Erweiterung zu installieren.

Bitte wenden Sie sich an Google, um beim Testen dieser Funktion dabei zu sein.

Remote-Befehle Beta

Chrome Browser Cloud Management bietet Administratoren die Möglichkeit, verschiedene Remote-Befehle für einen verwalteten Browser auszuführen. Derzeit können Administratoren den Cache und/oder die Cookies für ein bestimmtes Browser-Profil aus der Ferne löschen. Dies ermöglicht eine optimierte Benutzerunterstützung am ersten Problemlösungspunkt. Zusätzliche Remote-Befehle werden weiterhin ausgegeben und an Administratoren verteilt, darunter erzwungene Browser-Neustarts.

The screenshot displays the 'USERS & BROWSERS' section of the Chrome Browser Cloud Management console. It shows a table of extension requests with columns for 'App', 'Request count', and 'The latest request time'. A details panel for the 'Dark Mode YT' extension is open on the right, showing its ID, a link to view it in the Chrome Web Store, and sections for 'Permissions', 'Devices', 'Users', and 'Risk Score'.

| App | Request count | The latest request time |
|---|---------------|-------------------------|
| mekedaspoiaomickpephkoicnimegci mekedaapoaomickpephkoicnimegci | 1 | Jun 16, 2020, 12:48 PM |
| Dark Mode YT ppdkhgjfdhkhkhhfcgjd | 1 | Jun 16, 2020, 12:52 PM |
| Material Incognito Dark Theme ahfonsrpgbsdjtshgpfkmlapfoel | 1 | Jun 16, 2020, 12:52 PM |
| gelbmiohojhapemcjilbjpndeicfob gelbmiohojhapemcjilbjpndeicfob | 1 | Jun 16, 2020, 12:48 PM |
| Custom Cursor for Chrome™ ogdpmhglpejioimcodrpprfgcpmgale | 1 | Aug 19, 2020, 1:27 PM |
| macOS Mojave Dark Mode emoadcoophlühfgtjadllggrrnemdigh | 1 | Jun 16, 2020, 12:52 PM |

Dark Mode YT

ID: ppdkgjfdhkhkhhfcgjd
[View in Chrome Web Store](#)

Permissions
This extension does not request any permissions.

Devices
BLACKRANK

Users
None

Risk Score
TBD

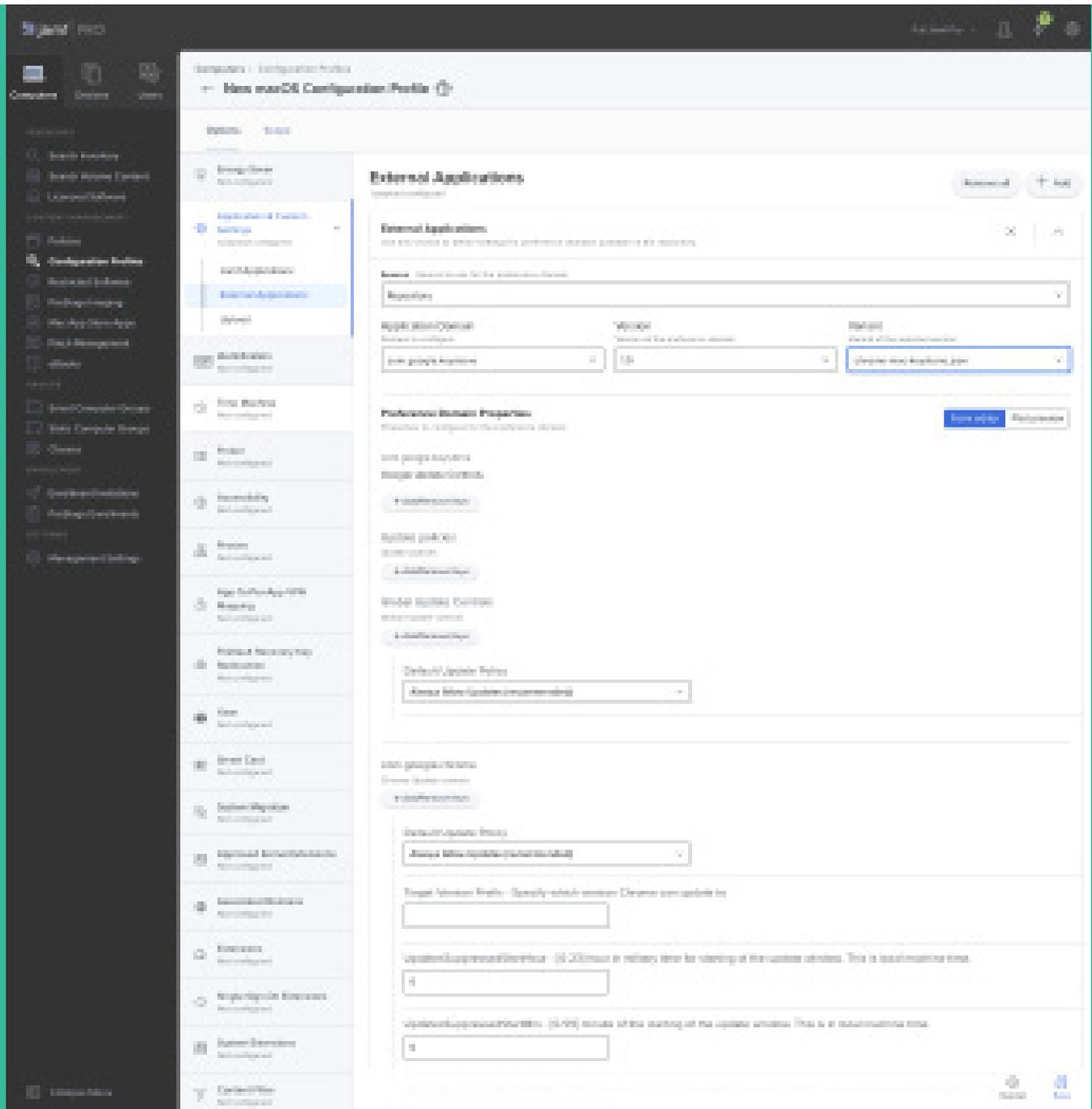
Approve
Deny

Konfiguration von Updates

Das Management von Update-Richtlinien für Benutzer ist der beste Weg, um sicherzustellen, dass auf den Geräten die neuesten Versionen von Chrome ausgeführt werden. Es gibt mehrere Möglichkeiten, die Versionskontrolle für Ihre Benutzer zu handhaben, und viele haben festgestellt, dass Keystone ein zuverlässiges Tool ist, das gut für Google Produkte geeignet ist.

Konfiguration von Keystone

Was ist Keystone? Keystone ist die mit Google Chrome gebündelte Hilfsanwendung, die Google Produkte auf dem neuesten Stand hält. Wie können Sie mit Keystone arbeiten? Sie können [das flexible und leistungsfähige Repository für benutzerdefinierte Einstellungen von Jamf](#) verwenden, um problemlos Keystone Richtlinien in Bezug auf Update-Kontrollen für Google Chrome zu konfigurieren. Das Jamf Team hat die Bereitstellung dieser Richtlinien für einen Administrator mit nur wenigen Klicks benutzerfreundlich gestaltet, indem es alle verfügbaren Steuerelemente in einer einfachen Oberfläche anbietet.



Konfiguration von Chrome auf iPads und iPhones

Chrome ist überall verfügbar, wo gesurft wird, auch auf mobilen Apple Geräten. Dies bietet ein beständiges und einheitliches Browsing-Erlebnis über macOS und iOS/iPadOS Geräte hinweg.

Ein aktuelles Update von Chrome für Mobilgeräte beinhaltet die Anmeldung für das Google Browser Cloud Management über AppConfig. Die gemanagte Erfahrung, die Benutzer auf dem Mac bereits haben, ist nun auch auf dem Mobiltelefon zu finden.

Chrome Browser Cloud Management per AppConfig

- Administratoren können Einstellungen und Konfigurationen zusammen mit Apps über AppConfig bereitstellen. Chrome nutzt diese Funktion, um den Browser im Chrome Browser Cloud Management auf iOS und iPadOS anzumelden.
- Zukünftige Erweiterungen werden es ermöglichen, dass mehr Richtlinien von AppConfig definiert werden können.

Benutzergesteuerte Verwaltung von Voreinstellungen

- Mit iOS 14 wurde die Möglichkeit eingeführt, Standardanwendungen für Browser und E-Mail festzulegen. Mit dieser benutzergesteuerten Einstellung kann eine Organisation den Chrome Browser auf das Gerät pushen und dem Benutzer die Möglichkeit geben, sich für eine neue Voreinstellung zu entscheiden. Diese Option finden Sie unter *Einstellungen* → *Chrome* → *Standard-Browser-App*.

Bitte [wenden Sie sich an Google](#), um beim Testen dieser Funktion dabei zu sein.

Chrome auf Apple, ermöglicht durch Jamf

Chrome und die zusätzlichen Anpassungen, durch die es sich hervorragend für Unternehmen eignet, sind mit Jamf einfach zu implementieren. Chrome als Plattform ist der Ausgangspunkt für Erweiterungen und Web-Apps, die Produktivität und Personalisierung in das Web-Erlebnis bringen.

Implementieren, registrieren und verwalten Sie Google Chrome mit Jamf Pro zur Unterstützung Ihrer Apple Enterprise Geräte.

Starten Sie noch heute Ihre kostenlose Testversion von Jamf Pro oder erfahren Sie mehr über [Google Integrationen mit Jamf](#).

[Test starten](#)

Oder wenden Sie sich an Ihren bevorzugten Apple Hardware-Händler, um loszulegen.

