chrome enterprise

Google Chrome für Unternehmen – Leitfaden für den Datenschutz: Datenschutzmodi

Einführung

Der Browser bietet Zugriff auf wichtige Anwendungen und Daten – jederzeit und von überall aus. Tatsächlich verbringen die meisten geschäftlichen Nutzer heute mehr als die Hälfte ihres Arbeitstages im Browser. Gleichzeitig sehen Organisationen sich mit immer mehr Anforderungen in Bezug auf Sicherheit, Datenschutz und Compliance konfrontiert, während sie ihren Nutzern auch weiterhin rund um die Uhr schnellen, zuverlässigen und sicheren Zugriff auf ihre Webanwendungen ermöglichen möchten.

Sie erwarten einen vertrauenswürdigen und sicheren Browser, der über Möglichkeiten verfügt, die Daten der Organisation und der Nutzer gleichermaßen effizient zu schützen. Mit den zahlreichen Richtlinien von Google Chrome können Sie die individuellen Anforderungen Ihres Unternehmens in Bezug auf Datenschutz und Compliance erfüllen. Im Folgenden gehen wir näher darauf ein, wie Ihre Administratoren den Mitarbeitern Datenschutzmodi und Richtlinien bereitstellen können, mit denen sich Arbeits- und Nutzerprofile voneinander trennen lassen. Außerdem stellen wir Tools vor, mit denen Sie Ihren Mitarbeitern vermitteln können, wie genau die Browser verwaltet werden.

chrome enterprise

Datenschutzmodi und -richtlinien in Chrome

Als IT-Administrator können Sie Richtlinien auf den von Ihnen verwalteten Browsern anwenden. Chrome sucht regelmäßig nach Updates für Richtlinien in Ihrer Arbeitsumgebung. Um das private Surfen in Ihrem Unternehmen zu ermöglichen, können Sie die folgenden Datenschutzmodi von Chrome in Betracht ziehen. Sie werden für gemeinsam genutzte oder öffentliche Terminals empfohlen, die von mehreren Mitarbeitern verwendet werden.

Gastmodus: Im Gastmodus können Sie Informationen in anderen Chrome-Profilen weder einsehen noch bearbeiten. Wenn Sie die Sitzung beenden, werden Ihre Browseraktivitäten von dem Computer gelöscht. Der Gastmodus eignet sich optimal, wenn Geräte untereinander verliehen werden oder für die Öffentlichkeit zugänglich sind.

Wenn die Richtlinie BrowserGuestModeEnabled auf „true“ gesetzt oder nicht konfiguriert ist, sind in Chrome Gastsitzungen aktiviert. Gastsitzungen sind sitzungsspezifisch. Sie starten mit einer leeren Benutzeroberfläche und hinterlassen keinerlei Informationen. Wenn diese Richtlinie auf „false“ gesetzt ist, können in Chrome keine Gastprofile aufgerufen werden.

Außerdem steht Ihnen die Richtlinie BrowserGuestModeEnforced zur Verfügung, die den Gastmodus bei jedem Start des Chrome-Browsers erzwingt. Ist diese Richtlinie aktiviert, lässt sich der Browser mit bestehenden Profilen nicht öffnen. Gastsitzungen sind Google Chrome-Profile, bei denen sich alle Fenster im Inkognitomodus befinden. Wenn diese Richtlinie deaktiviert oder nicht festgelegt wurde oder der Gastmodus mit der Richtlinie „BrowserGuestModeEnabled“ nicht aktiv ist, ist in Chrome die Nutzung neuer und bestehender Profile zugelassen.

Flüchtiger Modus: Um Ihren MItarbeitern zu ermöglichen, mit ihrem persönlichen Laptop oder einem gemeinsam genutzten, als vertrauenswürdig eingestuften Gerät zu arbeiten, können Sie Chrome-Profile mit einer Richtlinie dazu zwingen, im flüchtigen Modus zu starten. Dies senkt die Wahrscheinlichkeit, dass Informationen zum Browserverlauf auf dem entsprechenden Gerät verbleiben. Während dieser Sitzung hat der Nutzer vollen Zugriff auf den Browser und kann sich anmelden, um Funktionen zu nutzen, die normalerweise im Nutzerprofil verfügbar sind, darunter Chrome-Synchronisierung, Cloud-Drucker, Cloud-Richtlinien, Passwortspeicher, Lesezeichen sowie Autofill- und andere Daten. Außerdem lassen sich alle zum Unternehmen gehörenden Inhalte aufrufen, die im flüchtigen Modus aktiviert wurden – z. B. Webmail, Dokumente und Intranetseiten. Wenn Sie den flüchtigen Modus verwenden, empfehlen wir Ihnen dringend, auch die Chrome-Synchronisierung zu nutzen. Bei aktivierter Chrome-Synchronisierung werden alle Änderungen, die der Nutzer an den Browsereinstellungen oder den eigenen Chrome-Daten (Lesezeichen, Verlauf, Apps usw.) vornimmt, für zukünftige Sitzungen gespeichert. Die Einstellungen werden im Google-Konto des Nutzers in der Cloud gespeichert. Wenn die Google Chrome-Synchronisierung nicht aktiviert ist, gehen beim Verlassen des Browsers alle Änderungen des Nutzers verloren.

Wenn die Richtlinie ForceEphemeralProfiles aktiviert ist, zwingt sie Profile in den flüchtigen Modus. Ist die Richtlinie als Betriebssystemrichtlinie definiert (z. B. als Gruppenrichtlinienobjekt auf Windows), wirkt sie sich auf jedes Profil im System aus. Ist sie hingegen als Cloud-Richtlinie definiert, wird sie nur auf das Profil angewendet, das mit einem verwalteten Konto angemeldet ist.

chrome enterprise

Inkognitomodus: Wenn Sie nicht möchten, dass Google Chrome die Aktivitäten der Nutzer speichert, können Sie den Inkognitomodus aktivieren, um das private Surfen auf ihren eigenen Geräten zu ermöglichen. Die Nutzer können ihre Informationen und Einstellungen sehen, ohne dass der Browserverlauf gespeichert wird. Der Inkognitomodus stellt eine Surfmöglichkeit für Nutzer, dar, während der flüchtige Modus eine Richtlinie ist, die vom Administrator der Organisation erzwungen werden kann. Mithilfe dieser Richtlinie können Administratoren festlegen, ob sie den Inkognitomodus für ihre Nutzer aktivieren möchten oder nicht. Nutzer im Inkognitomodus können sich nicht anmelden und profitieren daher auch nicht von den Vorteilen der Chrome-Synchronisierung (z. B. geschäftlichen Lesezeichen).

Anwendungen und Erweiterungen sind im Inkognitomodus nicht standardmäßig aktiv, können jedoch durch den Nutzer aktiviert werden. Im flüchtigen Modus sind Anwendungen und Erweiterungen standardmäßig aktiviert. Im flüchtigen Modus profitieren die Mitarbeiter von Produktivitätsvorteilen, während gleichzeitig das Risiko, Daten zu hinterlassen, reduziert wird. Wenn dieser Modus über die Admin-Konsole auf Nutzerebene festgelegt wurde, funktionieren Richtlinien und Synchronisierung nur dann, wenn die Nutzer sich anmelden. Die Richtlinien sollten nur auf Geräten verwendet werden, denen die Nutzer vertrauen und die den Anforderungen anderer Unternehmensrichtlinien entsprechen. Das Profil wird erst zum Löschen vorgemerkt, wenn der Nutzer sich abmeldet oder alle Browserfenster, die mit dem Profil verknüpft sind, manuell schließt. Beim nächsten Start von Chrome wird das Profil gelöscht. Nutzen Sie den flüchtigen Modus nicht, wenn Sie unter Windows den Chrome-Browser mit Roaming-Nutzerprofilen verwenden. Es gibt auch noch detailliertere Richtlinien, mit denen festgelegt werden kann, ob und wie bestimmte Datentypen unter Chrome aufbewahrt werden.

Über die Richtlinie IncognitoModeAvailability legen Sie fest, ob Nutzer Seiten im Inkognitomodus öffnen können. Ist diese Richtlinie aktiviert oder nicht konfiguriert, können Seiten im Inkognitomodus geöffnet werden. Ist sie deaktiviert, können Seiten nicht im Inkognitomodus geöffnet werden. Ist sie erzwungen, können Seiten ausschließlich im Inkognitomodus geöffnet werden.

Sie können alle Modi in jedem verwalteten Browser mithilfe einer Richtlinie aktivieren – abhängig von Ihrem jeweiligen Betriebssystem entweder über die Admin-Konsole, die Gruppenrichtlinien, den JSON-Dateieditor oder in Ihrem Chrome-Konfigurationsprofil. Wenn Sie Chrome-Richtlinien anwenden, müssen Nutzer Chrome neu starten, damit die Einstellungen wirksam werden. Sie können die Nutzergeräte prüfen, um festzustellen, ob die Richtlinie wie vorgesehen angewendet wird.

Im Inkognito- oder Gastmodus lassen sich die Informationen beschränken, die Chrome auf Ihrem System speichert. Bestimmte Informationen werden von Chrome nicht gespeichert. Darunter:

- Grundlegende Informationen zum Browserverlauf wie URLs, im Cache gespeicherter Seitentext oder IP-Adressen von Seiten, die auf den von Ihnen besuchten Websites verlinkt sind
- Snapshots der von Ihnen besuchten Seiten
- Listen Ihrer Downloads, auch wenn die von Ihnen heruntergeladenen Dateien an anderer Stelle auf Ihrem Computer oder Gerät gespeichert bleiben

chrome enterprise

Umgang mit Ihren Informationen durch Chrome im Inkognito- oder Gastmodus

Chrome teilt keine vorhandenen Cookies mit Websites, die Sie im Inkognito- oder Gastmodus besuchen. Im Inkognito- oder Gastmodus sind keine bestehenden Cookies vorhanden. Für die Dauer der Sitzung können Websites Cookies lesen und schreiben. Die Sitzung ist beendet, sobald der letzte Tab oder das Browserfenster geschlossen werden. Daraufhin werden alle Cookies dauerhaft gelöscht. Wenn Sie Änderungen in Ihrer Browserkonfiguration vornehmen, während Sie sich im Inkognitomodus befinden (z. B. Lesezeichen setzen oder Bedienungshilfen einstellen), werden diese Informationen gespeichert. Dies trifft nur auf den Inkognitomodus zu – nicht auf den Gastmodus. Berechtigungen, die Sie im Inkognitomodus gewähren, werden nicht in Ihrem bestehenden Profil gespeichert. Im Inkognitomodus haben Sie weiterhin Zugriff auf Informationen aus Ihrem bestehenden Profil, z. B. auf Vorschläge basierend auf Ihrem Browserverlauf und auf gespeicherte Passwörter. Im Gastmodus können Sie surfen, ohne Informationen aus bestehenden Profilen zu sehen. Der Gastmodus öffnet jedes Mal eine völlig neue Sitzung ohne bestehende Nutzerdaten.

Profile, um zwischen geschäftlichen und privaten Daten zu unterscheiden

Anhand von Richtlinien lässt sich festlegen, dass Nutzer sich auf Windows-, Mac- oder Linux-Computern im Unternehmen zuerst mit ihren verwalteten Konten anmelden müssen, um Chrome zu nutzen. Bei Konflikten zwischen einer Nutzerrichtlinie, die in der Admin-Konsole festgelegt ist, und einer Geräterichtlinie, die z. B. mit der Chrome-Verwaltung über die Cloud oder einer Windows-Gruppenrichtlinie konfiguriert wurde, hat die Geräterichtlinie Vorrang.

BrowserSignin

Gibt an, ob Nutzer sich im Chrome-Browser anmelden und Browserinformationen mit ihrem Google-Konto synchronisieren können. Wählen Sie eine dieser Optionen aus:

0 – Anmeldung im Browser deaktivieren: Nutzer können sich nicht im Chrome-Browser anmelden oder Browserinformationen mit ihrem Google-Konto synchronisieren.

1 – Anmeldung im Browser aktivieren: Nutzer können sich im Chrome-Browser anmelden und Browserinformationen mit ihrem Google-Konto synchronisieren. Wenn sie sich in einem Google-Dienst wie Gmail anmelden, erfolgt die Anmeldung im Chrome-Browser automatisch.

2 – Anmeldung im Browser erzwingen: Nutzer müssen sich im Chrome-Browser anmelden, bevor sie ihn verwenden können. Sekundäre Nutzer können sich nicht im Chrome-Browser anmelden. Die Synchronisierung ist standardmäßig aktiviert und Nutzer können das nicht ändern. Administratoren können diese Einstellung aber mithilfe der Richtlinie SyncDisabled deaktivieren.

Nicht festgelegt: Nutzer können sich im Chrome-Browser anmelden. Wenn sie sich in einem Google-Dienst wie Gmail anmelden, erfolgt die Anmeldung im Chrome-Browser automatisch. Nutzer können die Einstellung ändern.

RestrictSigninToPattern

Damit wird eingeschränkt, welche Google-Konten im Chrome-Browser als primäre Nutzer angemeldet sein können.

In Verbindung mit der Richtlinie „BrowserSignin“ können Sie Nutzer mit mehreren Chrome-Profilen dazu zwingen, sich in einem bestimmten Profil anzumelden, um Chrome zu verwenden. Nutzer können sich nur mit solchen Profilen anmelden, die den von Ihnen angegebenen Mustern entsprechen.

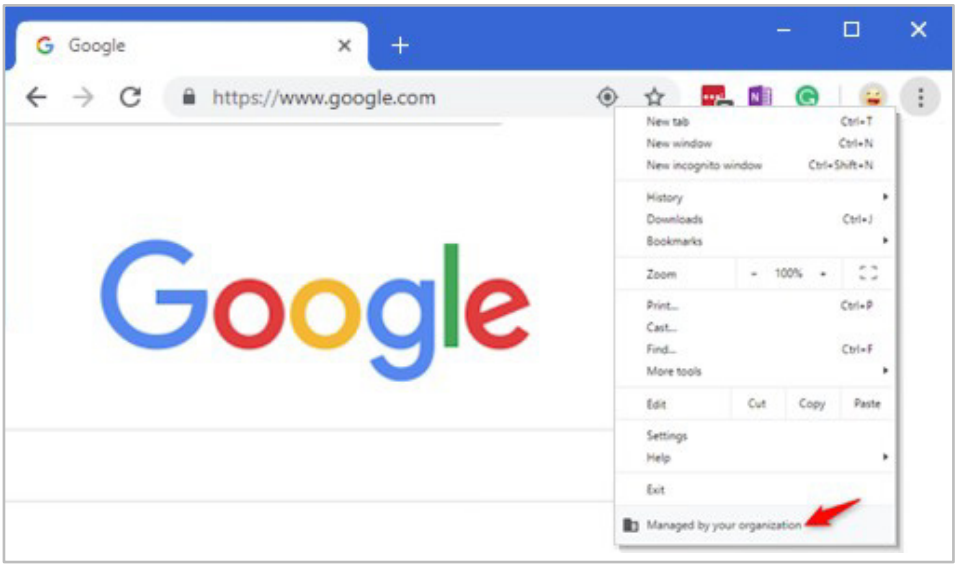
Nicht festgelegt: Nutzer können sich mit einem beliebigen Google-Konto als primäre Nutzer im Chrome-Browser anmelden.

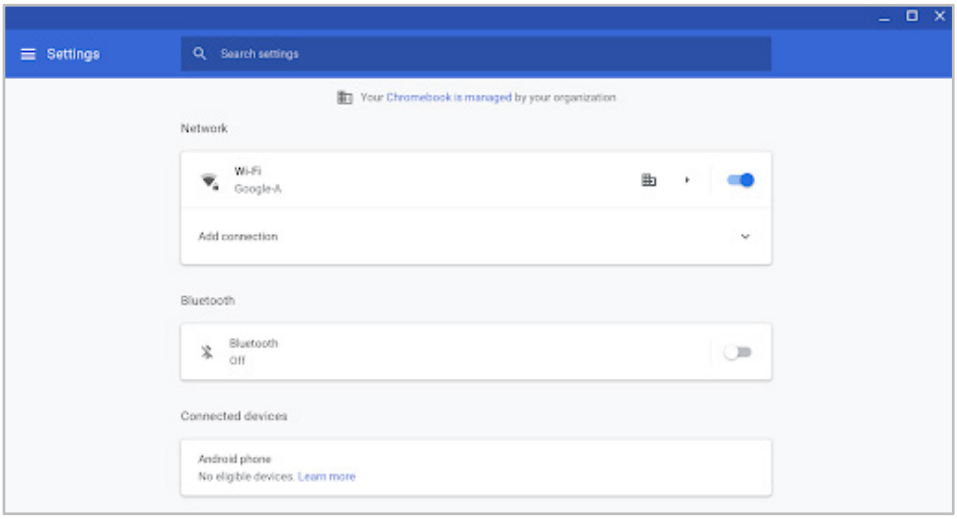
chrome enterprise

Nutzern vermitteln, wie ihre Browser verwaltet werden

Datenschutz und Transparenz gehen Hand in Hand. Chrome möchte seinen Nutzern auch auf Unternehmensebene Einblicke in Einstellungen und Konfigurationen ermöglichen. Google stellt dabei vier Methoden zur Verfügung, mit denen Nutzer Informationen darüber erhalten können, welche Funktionen in ihren Browsern verwaltet werden.

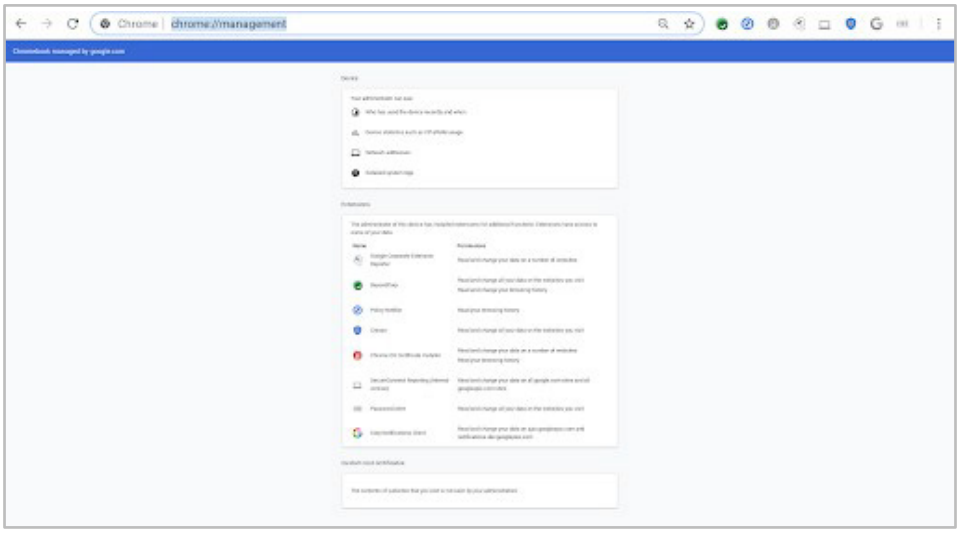
1. Verwaltet von: Ihre Nutzer sehen, dass ihr Gerät von der IT ihrer Organisation verwaltet wird. Sie können sich bei Fragen an ihren Administrator wenden. Der Hinweis „Von Ihrer Organisation verwaltet“ steht im Menü beim letzten Punkt „Beenden“. Nutzer sehen ihn aber auch in den Einstellungen.





chrome enterprise

2. Unter chrome://management können Nutzer die Erweiterungen sehen, die Sie als Administrator implementiert haben. Außerdem ist aufgelistet, welche Informationen aus der Perspektive des Administrators sichtbar sind. Mit Eingabe von chrome://policy lässt sich auch aufrufen, welche Richtlinien Sie als Administrator auf ihren Geräten aktiviert haben.



chrome enterprise

Fazit

Alle diese Verwaltungsoptionen bieten Ihnen die Möglichkeit, die Datenschutz- und Compliancestandards Ihrer Organisation umzusetzen. Außerdem können Sie Ihren Nutzern vermitteln, wie der Browser verwaltet wird. Dieser Leitfaden richtet sich an Administratoren, die den Chrome-Browser mit benutzerdefinierten Richtlinien für Unternehmen oder Schulen konfigurieren möchten, um die Anforderungen ihrer Organisation in Bezug auf Privatsphäre, Datenschutz und Compliance zu erfüllen. Da dieser Leitfaden jedoch nicht als Rechtsberatung zu verstehen ist, empfehlen wir Ihnen, zusätzlich einen Rechtsexperten hinzuzuziehen, um sich zu den besonderen Anforderungen Ihrer Organisation beraten zu lassen.

Um Ihr Wissen über die Modi für privates Surfen im Chrome-Browser zu vertiefen, **empfehlen wir Ihnen außerdem das folgende Infomaterial**:

Weitere Informationen zum flüchtigen Modus

Weitere Informationen zum privaten Surfen

Weitere Informationen zum Gastmodus in Chrome

Weitere Informationen dazu, wie das private Surfen aktiviert wird

Weitere Möglichkeiten mit der Chrome-Verwaltung über die Cloud

Chrome-Browser für Ihr Unternehmen herunterladen

Weitere Informationen zum Support für Google Chrome für Unternehmen

Liste der Richtlinien für Google-Chrome

Versionshinweise für Chrome Enterprise und Education

Dank Chrome Releases-Blog immer über die neuesten Aktualisierungen auf dem Laufenden bleiben

Offizieller Google-Blog zu Sicherheit und Schutz

Die Chrome Enterprise und Education-Hilfe und das Google Chrome-Hilfeforum

Öffentlicher Tracker für Programmfehler in Google Chrome