Erweiterungen im Unternehmen verwalten

Chrome-Erweiterung skalierbar und sicher verwalten

Inhalt

Ziel dieses Leitfadens

Einführung

Überlegungen zur Verwaltung von Chrome-Erweiterungen
- Was sind Erweiterungsberechtigungen?
- Wie werden Erweiterungen aktualisiert?

Erweiterungen verwalten

Überblick über die verschiedenen Richtlinien zur Erweiterungsverwaltung

Erweiterungen nach ihren Berechtigungen blockieren
- Erweiterungen in der Chrome-Verwaltung über die Cloud über ihre Berechtigungen verwalten
- Erweiterungen in Gruppenrichtlinien nach ihren Berechtigungen verwalten
- Ausnahmen für Erweiterungen mit riskanten Berechtigungen erstellen

Erweiterungen mit der Richtlinie „ExtensionSettings“ verwalten
- Richtlinie in der Windows-Registrierung konfigurieren
- Richtlinie über einen JSON-String im Windows-Editor für Gruppenrichtlinien konfigurieren
- Verhindern, dass Webseiten durch Erweiterungen geändert werden

Erweiterungen in der Admin-Konsole zulassen oder blockieren
- Alle Erweiterungen bis auf bestimmte Ausnahmen zulassen
- Alle Erweiterungen bis auf bestimmte Ausnahmen blockieren
- Eine einzelne Erweiterung blockieren oder zulassen
- Installation von Erweiterungen erzwingen

Nutzern ermöglichen, Erweiterungen anzufordern: Workflows

Erweiterungen über die Gruppenrichtlinie zulassen oder blockieren
- Alle Erweiterungen bis auf bestimmte Ausnahmen zulassen
- Eine einzelne Erweiterung blockieren oder zulassen
- Installation von Erweiterungen erzwingen

Richtlinien validieren

Eigene Erweiterungen selbst hosten
- Alternativen zum Hosting auf dem eigenen Server
  - Möglichkeiten, Erweiterungen zu veröffentlichen
- Erweiterungen in der Admin-Konsole auf eine bestimmte Version festlegen
- Erweiterungen selbst hosten – Anforderungen
- Erweiterung packen
- Erweiterung hosten
- Updates für die Erweiterung veröffentlichen
- Selbst gehostete Erweiterungen verteilen

Erweiterungen in der Chrome-Verwaltung über die Cloud verwalten

Weitere Ressourcen

Ziel dieses Leitfadens

Es gibt viele nützliche Erweiterungen für den Chrome-Browser. Und möglicherweise werden auch viele davon auf den Computern Ihrer Nutzer ausgeführt. Da ist es für IT-Administratoren manchmal nicht leicht, die Kontrolle zu behalten.

Dieser Leitfaden richtet sich an Administratoren, die Erweiterungen möglichst effizient verwalten möchten. Sie finden hier Anleitungen dafür, wie Sie Erweiterungen sowohl in der Chrome-Verwaltung über die Cloud als auch mithilfe von Windows-Gruppenrichtlinien verwalten.

Dieser Leitfaden ist nach den unterschiedlichen Möglichkeiten zur Verwaltung von Erweiterungen gegliedert. Sie können:

1. Erweiterungen nach ihren Berechtigungen blockieren
2. Festlegen, auf welche Websites Erweiterungen Zugriff haben
3. Erweiterungen in der Chrome-Verwaltung über die Cloud oder mithilfe von Windows-Gruppenrichtlinien zulassen oder blockieren
4. Ihre eigenen Erweiterungen lokal hosten

Themen	Anleitungen und Empfehlungen zur Verwaltung von Chrome-Erweiterungen im Unternehmen
Hauptzielgruppe	Administratoren, die mit Microsoft® Windows® und der Chrome-Verwaltung über die Cloud arbeiten (unter Windows, Mac oder Linux)
Kernpunkte	Best Practices für die Verwaltung von Erweiterungen im Chrome-Browser

Zuletzt aktualisiert: *29. Oktober 2021*

Veröffentlicht unter: *https://support.google.com/chrome/a/answer/9296680*

Einführung

Unternehmen möchten die Daten ihrer Nutzer schützen. Deshalb ist es wichtig für sie, dass sie ohne großen Aufwand testen können, ob Erweiterungen sicher und für die Nutzer relevant sind. Zu den Aufgaben von IT-Administratoren zählt daher Folgendes:

1. Verhindern, dass schädliche Erweiterungen installiert werden
2. Dafür sorgen, dass benötigte Erweiterungen verfügbar sind
3. Den Zugriff von Erweiterungen auf Nutzer- und Unternehmensdaten einschränken

In diesem Leitfaden erfahren Sie, wie Sie Erweiterungen effizient verwalten können. Dafür gibt es mehrere Methoden. Hier werden die verschiedenen Möglichkeiten beschrieben und Sie erhalten Informationen dazu, wie Sie die richtige Methode für Ihr Unternehmen auswählen.

Überlegungen zur Verwaltung von Chrome-Erweiterungen

Ihre Nutzer müssen in ihrem Arbeitsalltag auf bestimmte Apps, Websites und Erweiterungen zugreifen. Als IT-Administrator ist es Ihre Aufgabe, die Nutzer- und Unternehmensdaten zu schützen. Sie benötigen deshalb eine Strategie zur effizienten Verwaltung von Erweiterungen.

Stellen Sie sich dabei die folgenden Fragen:

- Welche Vorschriften und Compliance-Auflagen müssen erfüllt werden?
- Welcher Geräte- oder Websitezugriff könnte gegen die Sicherheitsrichtlinien des Unternehmens verstoßen?
- In welchem Umfang sind Nutzer- oder Unternehmensdaten auf den Geräten der Nutzer gespeichert?

Mit Richtlinien von Google haben Sie nun folgende Möglichkeiten:

- Erweiterungen basierend auf Ihren Datenschutzrichtlinien blockieren oder zulassen
- Die Installation benötigter Erweiterungen auf den Geräten Ihrer Nutzer erzwingen
- Erweiterungen verwalten und auf die funktionsrelevanten Berechtigungen einschränken

Eine herkömmliche Verwaltungsmethode ist, bestimmte Erweiterungen zuzulassen oder zu blockieren. Es gibt darüber hinaus aber eine einfachere Methode. Sie können Erweiterungen über die dafür benötigten Berechtigungen verwalten. Entscheiden Sie, welche Berechtigungen Sie zulassen möchten. Dann können Sie Richtlinien erzwingen, über die Erweiterungen zugelassen oder blockiert werden, je nachdem ob sie die Anforderungen erfüllen.

Was sind Erweiterungsberechtigungen?

Manche Erweiterungen müssen Änderungen auf einem Gerät oder einer Webseite vornehmen, damit sie einwandfrei funktionieren. Sie benötigen also die entsprechenden Berechtigungen. Entwickler müssen angeben, welche Zugriffs- und anderen Berechtigungen für ihre Erweiterungen erforderlich sind. Es gibt zwei Hauptkategorien, die bei vielen Erweiterungen beide relevant sind:

- Websiteberechtigungen für den Zugriff auf die von Ihren Nutzern aufgerufenen Websites. Beispiele: Eine Webseite ändern, auf Cookies zugreifen, Tabs ändern
- Geräteberechtigungen für den Zugriff auf das Gerät, auf dem der Browser ausgeführt wird. Beispiele: Zugriff auf USB-Anschluss/Speicher/Bildschirm

Wie werden Erweiterungen aktualisiert?

Erweiterungen werden nur aktualisiert, wenn Chrome ausgeführt wird. Die Updates erfolgen in den ersten Minuten nach dem Start von Chrome und dann alle fünf Stunden.

- Der Updateprozess funktioniert bei Erweiterungen so:
    a. Chrome sendet eine Anfrage mit einer Liste von installierten Erweiterungen und Versionen an einen Google-Server.
    b. Unsere Server antworten mit Anweisungen dazu, welche Erweiterungen aktualisiert werden müssen.
    c. Chrome fordert dann für jede betroffene Erweiterung die CRX-Datei an und führt das Update lokal aus.
- Wenn eine Erweiterung nicht auf dem neuesten Stand ist, kann das folgende Gründe haben:
    a. Wenn das Update sehr groß ist oder ein Nutzer sehr viele Erweiterungen hat, bleibt während einer kurzen Nutzersitzung unter Umständen nicht genug Zeit für das Update.
    b. Chrome wurde nicht gestartet.
    c. Die Entwickler einer Erweiterung installieren das Update nur auf einer beschränkten Anzahl von Clients.
    d. Wenn ein Unternehmen Erweiterungen selbst hostet, kann ein Zugriffsproblem oder ein Konfigurationsfehler der Grund sein.
    e. Aufgrund von Fehlern im Code einer Erweiterung können Probleme auftreten.

Wenn Sie veraltete Erweiterungen auf den neuesten Stand bringen möchten, können Sie sie deinstallieren und dann wieder installieren. Eine andere Möglichkeit ist, ein Update manuell zu erzwingen. Gehen Sie dafür so vor: Rufen Sie chrome://extensions auf > aktivieren Sie den Entwicklermodus > klicken Sie auf die Schaltfläche „Aktualisieren“.

Erweiterungen verwalten

Bei den meisten Organisationen ist am sinnvollsten, Erweiterungen in Hinsicht auf die erforderlichen Berechtigungen und die Websites, auf die sie Zugriff haben, zu verwalten. Diese Methode ist sicherer und einfacher. Außerdem ist sie skalierbar.

Sie sparen damit Zeit, da Sie die Richtlinien nur einmal konfigurieren müssen. Sie müssen also keine endlos langen Zulassungs- und Sperrlisten mehr verwalten. Bei Bedarf können Sie trotzdem eine kurze Sperrliste mit Erweiterungen hinzufügen, die nicht installiert werden dürfen. Und mit der Richtlinie „Hosts mit Laufzeitsperrung“ sind Ihre wichtigsten Websites geschützt. So verwalten Sie die Erweiterungen in Ihrem Unternehmen mit dieser Methode:

1. Bringen Sie in Erfahrung, welche Erweiterungen auf den Computern Ihrer Nutzer installiert sind.
    - **Methode 1 (empfohlen):** Nutzen Sie die Chrome-Verwaltung über die Cloud. Diese Funktion steht Ihren Nutzern ohne zusätzliche Kosten zur Verfügung. Sie sehen die folgenden Informationen zu den Erweiterungen:

        - Installierte Version, Anzahl der installierten Instanzen und ob die Installation vom Nutzer oder vom Administrator durchgeführt wurde
        - Erforderliche Berechtigungen
        - Status (aktiv oder deaktiviert)
    - Eine Anleitung zur Einrichtung der Chrome-Verwaltung über die Cloud finden Sie hier.
    - Nachdem Sie die Konsole eingerichtet, die Geräte registriert und die Cloud-Berichterstellung aktiviert haben, sehen Sie alle installierten Erweiterungen unter **Geräte > Chrome > Nutzungsbericht zu Apps und Erweiterungen**.
        - Wenn Sie auf eine Erweiterung klicken, werden Ihnen nähere Informationen dazu angezeigt, welche Berechtigungen dafür erforderlich sind, sowie Beispiele dazu, wo sie installiert wird.
            - Demnächst (ab Ende 2021 oder Anfang 2022) wird eine neue Detailseite (siehe unten) aufgerufen, wenn Sie auf eine Erweiterung klicken.
            - Sie enthält verschiedene Informationen zu der Erweiterung, darunter die erforderlichen Berechtigungen, sowie Informationen direkt aus dem Eintrag im Chrome Web Store.
            - Weitere Informationen zur Verwaltung von Erweiterungen mit der Chrome-Verwaltung über die Cloud finden Sie in diesem YouTube-Video.
        - Außerdem können Sie mit der Takeout API der Chrome-Verwaltung über die Cloud alle Informationen zu den Erweiterungen der registrierten Browser in eine CSV-Datei exportieren.
            - Weitere Informationen Detaillierte Anleitung | Blogartikel | Demo-Video
    - **Methode 2:** Umfrage Fragen Sie Ihre Arbeitskollegen und Manager, welche Erweiterungen sie regelmäßig verwenden. Erstellen Sie eine Liste der Erweiterungen, die die Nutzer benötigen.

2. Legen Sie fest, welche Websites geschützt werden müssen:
    - Finden Sie heraus, bei welchen Websites oder Domains mit vertraulichen Inhalten Sie Erweiterungen daran hindern müssen, Daten zu lesen oder zu ändern.
        - Sie verhindern den Zugriff auf diese Websites, indem Sie die API-Aufrufe blockieren, wenn die Erweiterung ausgeführt wird. Blockiert werden Webanfragen, das Lesen von Cookies, das Einschleusen von JavaScript-Code, XHR usw.

3. Ermitteln Sie, welche Berechtigungen für die Nutzer mit Risiken verbunden sind:
    - Gehen Sie die Liste der Erweiterungen durch, die Sie in Schritt 1 erstellt haben. Welche Erweiterungen sind installiert und welche Berechtigungen sind dafür erforderlich?
        - **Wichtiger Tipp:** Es ist nicht immer eindeutig, welche Berechtigungen eine Erweiterung benötigt. Weitere Informationen hierzu erhalten Sie von den Anbietern

der jeweiligen Erweiterung. Entwickler müssen angeben, welche Änderungen ihre Erweiterung auf Geräten und Websites vornehmen kann.

- Sehen Sie sich diese Liste an. Hier sind alle Berechtigungen aufgeführt, die eine Erweiterung verwenden kann. Entscheiden Sie dann, welche Berechtigungen Sie in Ihrem Unternehmen zulassen möchten.

    - Weitere Informationen zu den Risiken bestimmter Erweiterungsberechtigungen finden Sie in diesem Hilfeartikel.

4. Erstellen Sie jeweils eine Liste mit den Informationen, die Sie gesammelt haben, darunter:
    - **Erforderliche Erweiterungen:** Sie können die Liste weiter nach Abteilung, Standort des Büros oder anderen relevanten Informationen unterteilen.
    - **Zulassungsliste:** Hier stehen erforderliche Erweiterungen mit Berechtigungen, die eigentlich blockiert werden würden, die aber zugelassen werden müssen. Beispiele:
        - Erweiterungen, die Nutzer für ihre Arbeit benötigen
        - Erweiterungen, die laut Auskunft ihrer Anbieter kein Risiko darstellen
    - **Sperrliste:**

        - Auf dieser Liste sammeln Sie alle Erweiterungen, deren Installation blockiert werden soll.

            - Dazu zählen auch die Berechtigungen, die nicht ausgeführt werden dürfen.

        - Hier geben Sie die Websites und Domains an, die geschützt werden müssen, indem der Zugriff von Erweiterungen unterbunden wird.

            - Vergleichen Sie diese Sperrliste mit anderen, die Sie verwenden. Unter Umständen können Sie die aktuellen Sperrlisten-Einstellungen sogar etwas lockern.

5. Lassen Sie die Liste von den relevanten Stakeholdern und vom IT-Team genehmigen.
6. Testen Sie die neuen Richtlinien in Ihrem Unternehmen zuerst in einer dafür ausgelegten Umgebung oder in einem kleinen Pilotprojekt.
7. Führen Sie die neuen Richtlinien dann nach und nach für die Mitarbeiter ein.
8. Berücksichtigen Sie das Feedback der Nutzer.
9. Wiederholen und optimieren Sie den Prozess monatlich, vierteljährlich oder einmal pro Jahr.

Mithilfe der oben beschriebenen Schritte schaffen Sie eine Ausgangsbasis für die Berechtigungen, die Sie zulassen und die Sie blockieren. Websites mit vertraulichen Inhalten sind geschützt. Die Arbeit im Browser ist sicherer und nutzerfreundlicher. Unter Umständen können Mitarbeiter sogar Erweiterungen installieren, die sie vorher nicht verwenden durften. Sie lassen sich lediglich auf Ihren Websites mit vertraulichen Inhalten nicht ausführen, es sei denn, Sie erlauben das explizit. Die Anleitungen zur Einrichtung dieser Methode finden Sie in diesen Abschnitten des Leitfadens:

- Erweiterungen in der Chrome-Verwaltung über die Cloud nach ihren Berechtigungen verwalten
- Verhindern, dass Webseiten durch Erweiterungen geändert werden
- Installation von Erweiterungen erzwingen
- Erweiterungen zulassen oder blockieren

Weitere Informationen dazu, wie Sie Erweiterungen mit der Chrome-Verwaltung über die Cloud verwalten, finden Sie in diesem Video.

Überblick über die verschiedenen Richtlinien zur Erweiterungsverwaltung

Viele dieser Richtlinien werden zwar in anderen Teilen dieses Dokuments genauer erläutert. Hier haben wir allerdings schon einmal einige der aktuellen Optionen zur Verwaltung von Erweiterungen mit Gruppenrichtlinien (Windows) oder Plists (Mac) zusammengefasst. Einige gelten auch für Apps.

- ExtensionInstallAllowlist: Über diese Richtlinie legen Sie die Erweiterungen fest, die in Ihrer Umgebung installiert werden dürfen.
- ExtensionInstallBlocklist: Wenn diese Richtlinie konfiguriert ist, blockieren Sie die Erweiterungen, die nicht installiert werden dürfen. Sollte eine dieser Erweiterungen bereits installiert sein, wird sie deaktiviert. Installationsversuche werden blockiert. Es gibt auch eine entsprechende neue Funktion im Chrome Web Store. Die Schaltfläche „Zu Chrome hinzufügen“ ist rot und der Nutzer wird darauf hingewiesen, dass die Erweiterung nicht installiert werden darf.
- ExtensionInstallForcelist: Hiermit wird die Erweiterung auf den Geräten der Nutzer im Hintergrund installiert. Die Nutzer können die Erweiterung weder deaktivieren noch deinstallieren. Diese Einstellung hat Vorrang vor der Richtlinie zur Anwendung der Sperrliste für Erweiterungen.
- BlockExternalExtensions: Mit dieser Einstellung können Sie die Installation von Erweiterungen aus externen Quellen blockieren. Beispiel: Wenn eine installierte Anwendung über die Registrierung eine Erweiterung in Chrome hinzufügt, wird mit dieser Einstellung verhindert, dass die Erweiterung lädt.
- ExtensionAllowedTypes: Hiermit können Sie eine Liste der Erweiterungs- und Anwendungstypen erstellen, die installiert werden dürfen. Mögliche Werte sind Erweiterungen, Designs, Nutzerskripte, gehostete Anwendungen, gepackte Legacy-Anwendungen und Plattformanwendungen.
    - Alle Typen, die Sie erlauben möchten, müssen in der Liste enthalten sein. Was nicht auf der Liste steht, wird auch nicht installiert.
    - Weitere Informationen zu den unterschiedlichen Typen finden Sie hier.
- ExtensionInstallSources: In den Vorgängerversionen konnten Nutzer auf den Link zu einer CRX-Datei klicken und die Datei nach einigen Warnhinweisen in Chrome installieren. Diese Funktion war bis Chrome 21 verfügbar und wurde dann aus Sicherheitsgründen entfernt.
    - Mit dieser Richtlinie können Sie diese Funktion auf bestimmte URLs anwenden. Hier finden Sie die URL-Muster, die Sie in dieser Richtlinie verwenden können.

- ExtensionsSettings: Diese Richtlinie beinhaltet mehrere Funktionen. Sie müssen dafür ein JSON-Skript in Form eines einzeiligen Strings erstellen.
    - Diese Einstellung kann sehr komplex sein. Sie wird an verschiedenen Stellen dieses Dokuments genauer erläutert.
        - Wir empfehlen, die Chrome-Verwaltung über die Cloud zu verwenden. Sie bietet fast alle Funktionen ohne das Schreiben von JSON-Code. Außerdem können Sie damit installierte Erweiterungen prüfen.

Ein Hinweis zu unserer Selbstverpflichtung, die Namensgebung inklusiver zu machen. Die folgenden Richtlinien wurden eingestellt und sind in Chrome 97 nicht mehr enthalten. Bis dahin müssen Sie also auf die neuen Richtlinien umstellen.

- ExtensionInstallWhitelist wurde ersetzt durch ExtensionInstallAllowlist.
- ExtensionInstallBlacklist wurde ersetzt durch ExtensionInstallBlocklist.

Erweiterungen nach ihren Berechtigungen blockieren

Sie können über die Berechtigungen steuern, welche Erweiterungen Nutzer installieren dürfen. Bereits installierte Erweiterungen werden deaktiviert, wenn Sie von ihnen benötigte Erweiterungen blockieren. Die anderen Erweiterungen mit blockierten Berechtigungen lassen sich vom Nutzer nicht installieren.

Erweiterungen in der Chrome-Verwaltung über die Cloud über ihre Berechtigungen verwalten

(Windows, Mac und Linux)

Sie haben die Möglichkeit, Erweiterungen zu blockieren, die nicht zulässige Berechtigungen benötigen. Beispiel: Sie können Erweiterungen blockieren, die auf USB-Geräte oder auf Cookies zugreifen.

1. Gehen Sie in der Admin-Konsole zu **Geräte > Chrome > Apps und Erweiterungen > Nutzer und Browser**.
2. Wählen Sie die Organisationseinheit aus, für deren Nutzer Sie Erweiterungen zulassen möchten.
3. Klicken Sie auf „Zusätzliche Einstellungen“ . 

4. Setzen Sie im Bereich **Berechtigungen und URLs** bei jeder Berechtigung, die Sie blockieren möchten, ein Häkchen. Anderenfalls wird sie zugelassen.

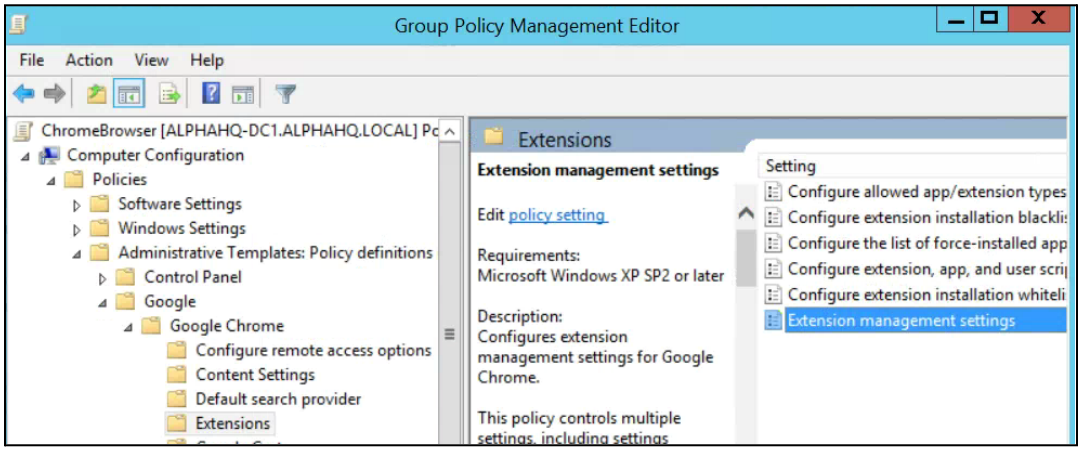
   a. Sie können auch auf dem Tab „Nutzer und Browser“ auf eine Erweiterung klicken, um sie unter „Berechtigungen und URL-Zugriff“ > „Berechtigungen für diese App/Erweiterungen anpassen“ nach Berechtigungen zu verwalten.
      i. Hinweis: Die hier ausgewählten Einstellungen haben Vorrang vor globalen Richtlinien, die für die Erweiterung gelten.
      ii. Details zu den einzelnen Berechtigungen finden Sie im Hilfeartikel Berechtigungen für Chrome-Apps und -Erweiterungen.
5. Klicken Sie auf **Speichern**.

Erweiterungen in Gruppenrichtlinien nach ihren Berechtigungen verwalten

(nur Windows)

1. Gehen Sie in der Microsoft Management Console (MMC) zum Gruppenrichtlinienobjekt.
2. Klicken Sie mit der rechten Maustaste und klicken Sie dann auf **Bearbeiten**.

3. Gehen Sie im Gruppenrichtlinien-Editor zu **Richtlinien > Administrative Vorlagen > Google Chrome > Erweiterungen > Einstellungen für die Erweiterungsverwaltung**.



Pfad zu den Einstellungen für die Erweiterungsverwaltung

4. Aktivieren Sie die Richtlinie und geben Sie dann die Berechtigungen ein, die zugelassen oder blockiert werden sollen. Komprimieren Sie die Daten in einen JSON-String.

Formatieren Sie die JSON-Daten nach diesem Beispiel. (Hiermit werden alle Erweiterungen blockiert, die auf USB zugreifen.)

```
{
	"*": {
		"blocked_permissions": ["usb"]
	}
}
```

Komprimierte JSON-Daten:

```
{"*":{"blocked_permissions":["usb"]}}
```

Wichtiger Tipp:

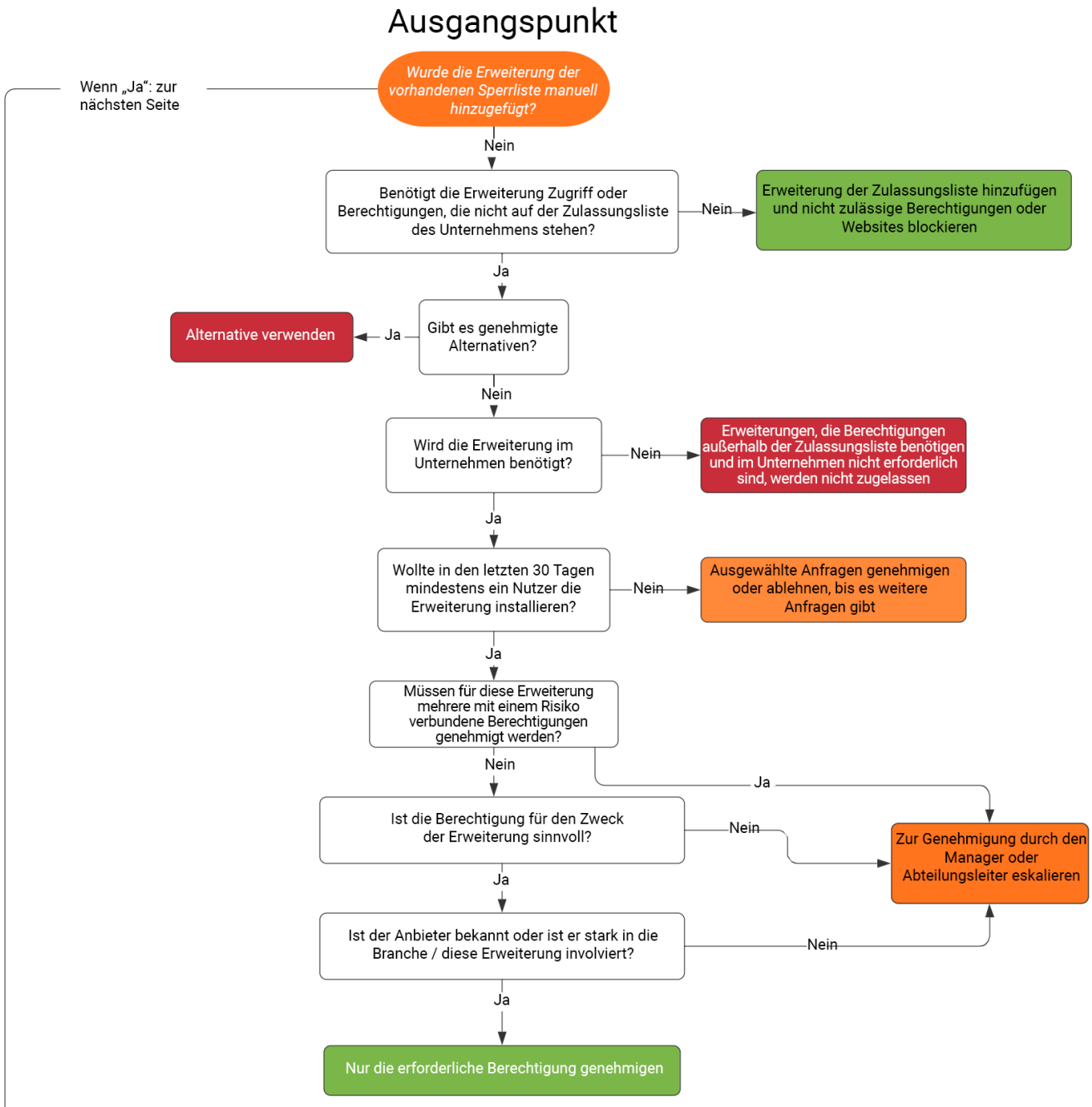
- Wenn Sie alle Erweiterungen mit dieser Berechtigung blockieren möchten, verwenden Sie ein Sternchen (wie oben) als Erweiterungs-ID.
- Sie können auch mehrere Berechtigungen über JSON blockieren. In diesem Beispiel wird der Zugriff auf die Stromversorgung, Drucker, serielle Ports und USB für alle Erweiterungen blockiert.
    - {"*":{"blocked_permissions":["power","printerProvider","serial","usb"]}}
- Wenn Sie eine bestimmte Erweiterungs-ID angeben, wird die Richtlinie nur auf diese Erweiterung angewendet. Ersetzen Sie einfach das Sternchen * im Beispiel oben durch die Erweiterungs-ID. Sie

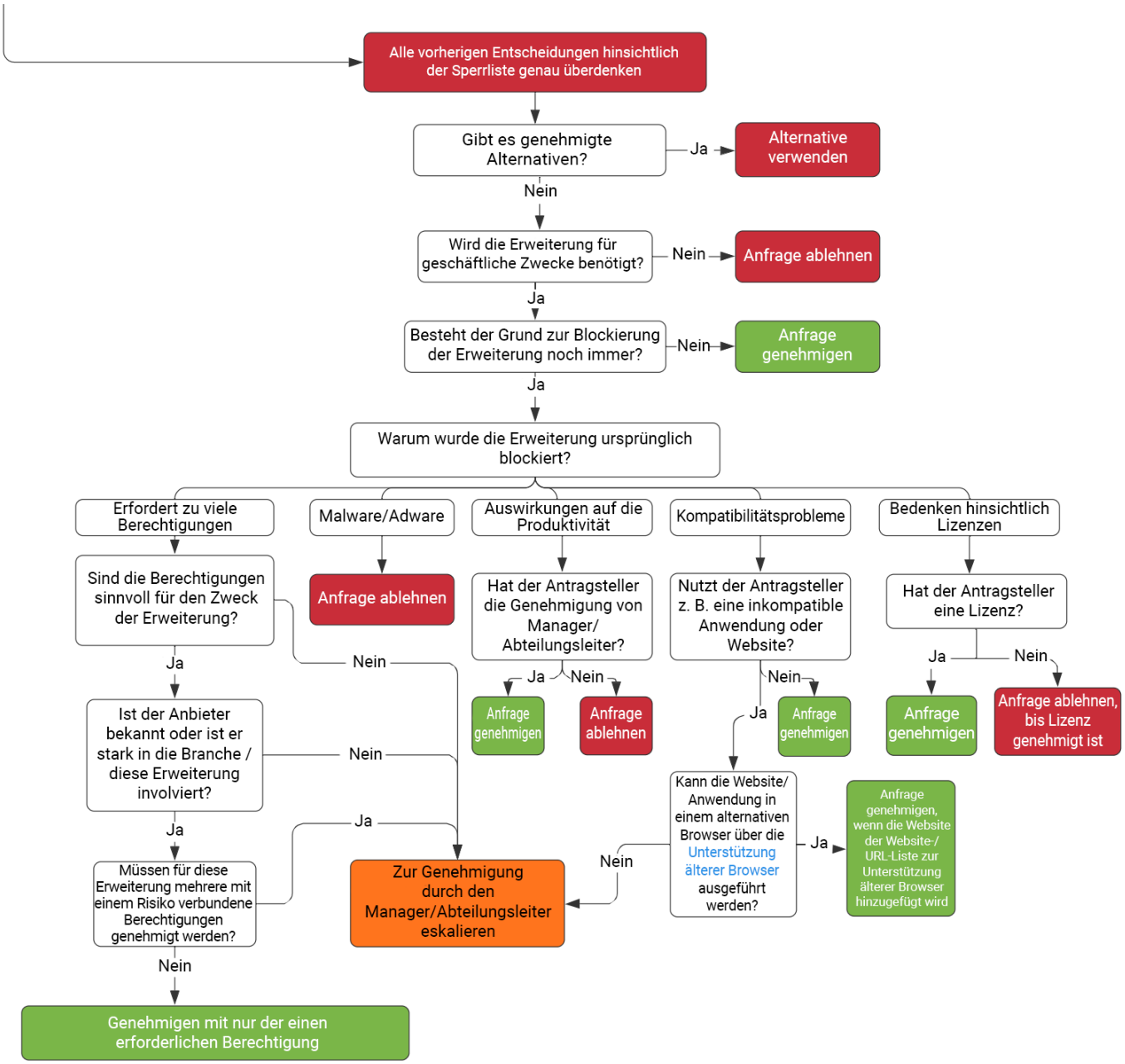
können auch mehrere Erweiterungen blockieren. Diese müssen im JSON-String jeweils eigene Einträge haben.

- Informationen dazu, wie Sie die Erweiterungs-ID ermitteln, finden Sie in diesem Hilfeartikel unter Schritt 3.

Ausnahmen für Erweiterungen mit riskanten Berechtigungen erstellen

Es kann vorkommen, dass im Unternehmen Erweiterungen benötigt werden, deren erforderliche Berechtigungen Sie eigentlich als zu riskant für Ihre Umgebung eingestuft haben. Hier ein Beispiel für einen Erweiterungs-Workflow für eine angeforderte Erweiterung, die eine blockierte Berechtigung erfordert.





- Hinweis: Dieser Workflow dient lediglich als Beispiel. Jedes Unternehmen hat seine eigenen Workflows und Änderungsmanagement-Prozesse.

Erweiterungen mit der Richtlinie „ExtensionSettings“ verwalten

In Windows haben Sie mehrere Möglichkeiten zum Verwalten von Einstellungen. Eine gängige Methode besteht darin, in einem JSON-String oder in der Windows-Registrierung mit der Richtlinie ExtensionSettings mehrere Richtlinien festzulegen.
Wichtiger Tipp: Diese Richtlinie ist kompatibel mit Mac, Chrome OS und Linux. Auf dieser Seite finden Sie Beispielwerte für die anderen Plattformen.

Mit dieser Richtlinie können Sie verschiedene Einstellungen steuern, darunter die Update-URL, die Download-URL für die Erstinstallation sowie blockierte Berechtigungen. Weitere Informationen erhalten Sie hier sowie in den folgenden Hilfeartikeln: Richtlinie „ExtensionSettings“ konfigurieren und Richtlinien für Apps und Erweiterungen

Sie haben die Wahl: Sie können alle Einstellungen für Erweiterungen über diese Richtlinie festlegen oder für jede Einstellung eine eigene Richtlinie verwenden.

- Die Einstellung für Hosts mit Laufzeitberechtigung/-sperrung, mit der Sie die festgelegten Erweiterungen auf den genannten Websites blockieren, lässt sich bei der Richtlinie „ExtensionSettings“ nurüber ein Gruppenrichtlinienobjekt festlegen.
    - Sie können die Einstellung aber auch über die Chrome-Verwaltung über die Cloud konfigurieren.
- Hinweis: Mit der Richtlinie „ExtensionSettings“ können Sie andere Richtlinien in den Gruppenrichtlinien überschreiben, darunter:
    - ExtensionAllowedTypes
    - ExtensionInstallAllowlist
    - ExtensionInstallForcelist
    - ExtensionInstallSources
    - ExtensionInstallBlocklist

Sie haben zwei Möglichkeiten, die Richtlinie „ExtensionSettings“ zu konfigurieren:

- Windows-Registrierung
- JSON-String im Windows-Editor für Gruppenrichtlinien

Wichtige Tipps:

- Es ist keine leichte Aufgabe, einen JSON-String korrekt zu formatieren. Verwenden Sie daher ein JSON-Prüftool, bevor Sie die Richtlinie implementieren.
- Wenn bei der Formatierung Probleme auftreten, können Sie einen Registrierungsschlüssel verwenden. Chrome führt dann die Konvertierung in JSON im Browser auf dem Zielgerät unter chrome://policy durch.
    - Kopieren Sie dafür einfach den JSON-Code und wenden Sie ihn über ein Gruppenrichtlinienobjekt bei der Richtlinie „ExtensionSettings“ an.
    - Sie können die Erweiterungseinstellungen auch in der Chrome-Verwaltung über die Cloud festlegen und die JSON-Ausgabe kopieren.

Richtlinie in der Windows-Registrierung konfigurieren

Die Richtlinie „ExtensionSettings“ muss unter dem folgenden Pfad in die Registrierung geschrieben werden:
`HKLM\Software\Policies\Google\Chrome\ExtensionSettings\`

- Sie haben die Möglichkeit, HKCU statt HKLM zu verwenden. Den entsprechenden Pfad können Sie über ein Gruppenrichtlinienobjekt angeben.
- Die Schlüssel lassen sich mit der von Ihnen bevorzugten Methode auf den Nutzergeräten erstellen.

Bei Chrome beginnen alle Einstellungen mit diesem Schlüssel:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\`

Der nächste Schlüssel ist für den Umfang der Richtlinie. Verwenden Sie die Erweiterungs-ID als Schlüsselnamen, wenn Sie die Richtlinie auf eine bestimmte Erweiterung anwenden möchten. Wenn sie für alle Erweiterungen gelten soll, verwenden Sie als Namen ein Sternchen. Hier ein Beispiel für Einstellungen, die nur für die Google Hangouts-Erweiterung gelten sollen:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\nckgahadagoaajjgafhacjanaoiihapd`

Bei Einstellungen, die für alle Erweiterungen gelten sollen, verwenden Sie:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\*`

Das Format variiert je nach Einstellung. Es kommt darauf an, ob es sich um einen String oder ein String-Array handelt. Bei Array-Werten müssen Sie **[" value "]** angeben. Bei String-Werten benötigen Sie [“ ”] nicht. Hier sehen Sie, bei welcher Einstellung es sich um ein Array und bei welcher um einen String handelt:

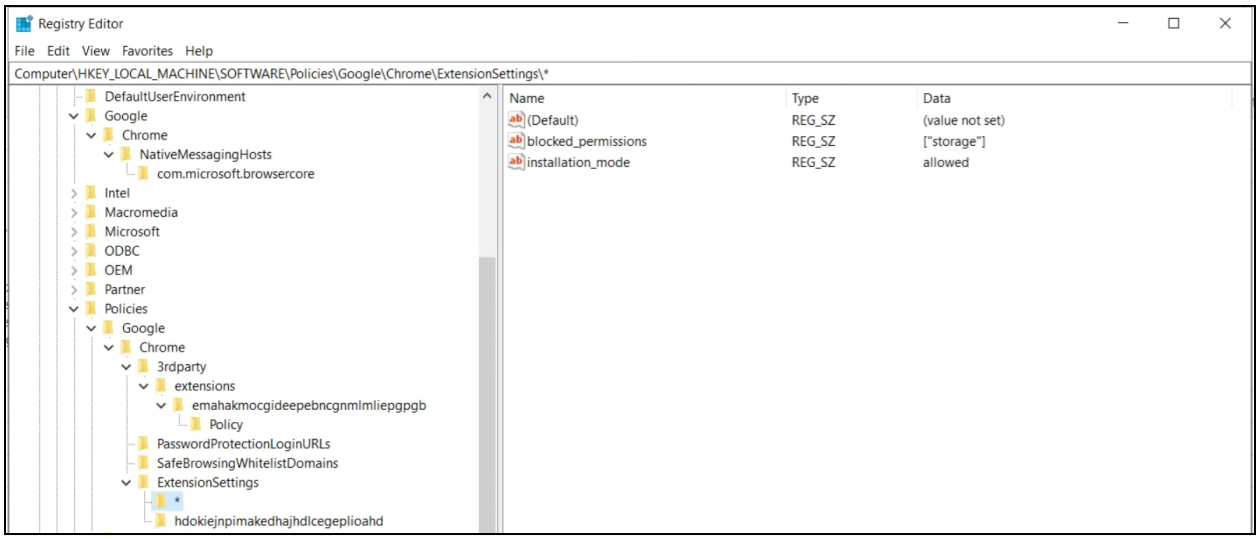
- Installation_mode = String
- update_url = String
- blocked_permissions = String-Array
- allowed_permissions = String-Array
- minimum_version_required = String
- runtime_blocked_hosts = String-Array
- runtime_allowed_hosts = String-Array
- blocked_install_message = String

Hier ein Beispiel für eine Syntax mit mehreren Werten in einem String (z. B. blockierte Berechtigungen):

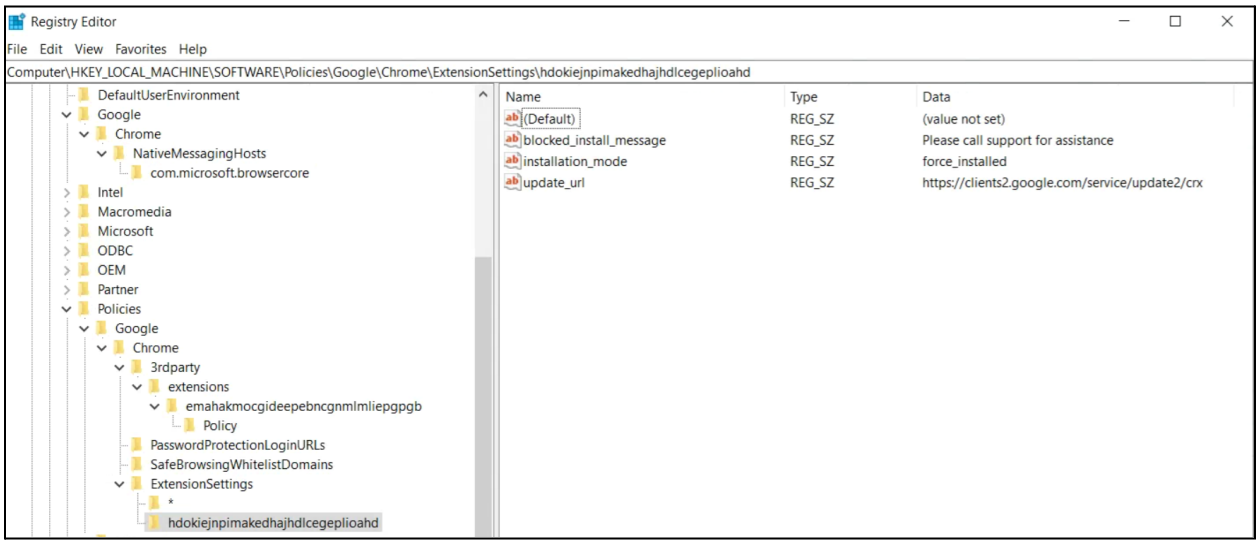
- [“power”,”printerProvider”,”serial”,”usb”]

Name	Type	Data
(Default)	REG_SZ	(value not set)
blocked_permissions	REG_SZ	["power", "printerProvider", "serial", "usb"]

Beispiele für Schlüssel innerhalb der Registrierung:



Schlüssel und Werte für Standardumfang (*)



Schlüssel und Werte für individuellen Umfang

Hier werden die Schlüssel in der Registrierung mit der Richtlinie im Browser unter chrome://policy in JSON konvertiert:

Chrome policies

Gilt für	Stufe	Quelle	Richtlinienname
Computer	Verbindlich	Plattform	DefaultBrowserSetting Enabled
Computer	Verbindlich	Plattform	ExtensionSettings


```
{
  "*": {
  "blocked-permissions": [ "storage" ],
  "installationjnode": "allowed"
  },
  "hdokiejnpimakedhajhdlcegeplioahd": {
  "blocked_install_message": "Please call support for assistance",
   "installation_mode": "force_installed",
  "update_url": "https://clients2.google.com/service/update2/crx"
   }
}
```


Richtlinie über einen JSON-String im Windows-Editor für Gruppenrichtlinien konfigurieren

Hierfür wird vorausgesetzt, dass Sie die ADM-/ADMX-Vorlagen für Chrome-Richtlinien importiert haben.

Anleitungen für andere Plattformen: Mac | Linux | Chrome OS

1. Gehen Sie im Editor zur Verwaltung von Gruppenrichtlinienobjekten zu **Google Chrome > Erweiterungen > Einstellungen für die Erweiterungsverwaltung**.
2. Aktivieren Sie die Richtlinie und geben Sie ihre komprimierten JSON-Daten (JavaScript Object Notation) als eine Zeile ohne Zeilenumbrüche in das Textfeld ein.
   Mit diesem Komprimierungstool eines Drittanbieters für JSON können Sie Richtlinien prüfen und auf eine Zeile komprimieren (Beispiel für JSON-Daten siehe unten).

So formatieren Sie den JSON-String für die Richtlinie „ExtensionSettings“:
Bei dieser Methode ist es wichtig, zwischen dem **Standardumfang** und dem **individuellen Umfang** zu unterscheiden. Der Standardumfang gilt für alle Erweiterungen. Der individuelle Umfang gilt nur für die angegebene Erweiterung.

Der Standardumfang wird mit einem Sternchen (*) angegeben. In diesem Beispiel werden ein Standardumfang und ein individueller Umfang für eine einzelne Erweiterung definiert:

```
{
   "*": {},
   "nckgahadagoaajjgafhacjanaoiihapd": {}
}
```

Für eine Erweiterung gilt jeweils nur ein Umfang. Wenn es einen individuellen Umfang gibt, werden die darin konfigurierten Einstellungen angewendet. Gibt es keinen individuellen Umfang, wird der Standardumfang verwendet.

Mit diesem JSON-Beispiel wird die Ausführung aller Erweiterungen auf .beispiel.de blockiert sowie alle Erweiterungen, die USB-Zugriff erfordern:

```
{
  "*": {
    "runtime_blocked_hosts": ["*://*.beispiel.de"],
    "blocked_permissions": ["usb"]
  }
}
```

Komprimierte JSON-Daten:

```
{"*":{"runtime_blocked_hosts":["*://*.beispiel.de"],"blocked_permissions":
["usb"]}}
```

Beispiele mit Beispielwerten für die Verwaltung der Erweiterungsinstallation:

- "allowed" (default)
  Nutzer dürfen die Erweiterung selbst über den Chrome Web Store installieren.
  JSON-Beispiel:
  `{ "*": {"installation_mode": "allowed" }}`

- "blocked"
  Nutzer dürfen die Erweiterung nicht selbst über den Chrome Web Store installieren.
  JSON-Beispiel:
  `{ "*": {"installation_mode": "blocked" }}`

- "blocked_install_message"
  Sie können eine benutzerdefinierte Nachricht angeben, die angezeigt wird, wenn die Installation blockiert ist.
  JSON-Beispiel: blocked_install_message:
  `{"*": {"blocked_install_message": ["Call IT(408 - 555 - 1234) for an exception"]}}`

- "force_installed"
  - Die Erweiterung wird automatisch ohne Eingreifen des Nutzers installiert.
  - Der Nutzer kann die Erweiterung nicht deaktivieren oder entfernen.

  `{ "*": {"installation_mode": "force_installed" }}`

- "normal_installed"
  Die Erweiterung wird automatisch installiert, aber der Nutzer kann sie deaktivieren.
  `{ "*": {"installation_mode": "normal_installed" }}`

- “removed”
  (Chrome-Version 75 oder höher): Nutzer können die Erweiterung nicht installieren. Wenn Nutzer die Erweiterung bereits installiert haben, wird sie vom Chrome-Browser entfernt.
  `{ "*": {"installation_mode": "removed" }}`

- `"toolbar_pin"`

  Damit wird gesteuert, ob das Erweiterungssymbol an die Symbolleiste angepinnt wird. Sie haben folgende Möglichkeiten:
  force_pinned: Das Erweiterungssymbol wird an der Symbolleiste angepinnt und ist immer sichtbar. Der Nutzer kann es im Erweiterungsmenü nicht ausblenden.
  default_unpinned: Die Erweiterung ist im Erweiterungsmenü zuerst ausgeblendet und der Nutzer kann sie an die Symbolleiste anpinnen.
  Wenn Sie nichts festlegen, wird das Feld auf das Standardverhalten „default_unpinned“ gesetzt.
  `{ "*": {"toolbar_pin": "forced_pinned" }}`

Wenn Sie für eine Erweiterung die Funktion „installation_mode“ verwenden, muss das Feld „update_url“ einen Wert enthalten (die Download-URL).

- Wenn die Erweiterung im Chrome Web Store gehostet wird, verwenden Sie „`https://clients2.google.com/service/update2/crx`“.

- Wenn Sie die Erweiterung auf Ihrem eigenen Server hosten, geben Sie die URL ein, von der Chrome die gepackte Erweiterung (CRX-Datei) herunterladen kann.
  JSON-Beispiel: Erweiterung mit „force_installed“ und „update_url“:
  `{"nckgahadagoaajjgafhacjanaoiihapd": {"installation_mode": "force_installed","update_url": "https://clients2.google.com/service/update2/crx"}}`
- Ab Chrome 89 können Sie auch mit der Einstellung „override_update_url“ angeben, dass Chrome für zukünftige Updates der Erweiterung die URL im Feld „update_url“ oder die in der Richtlinie „ExtensionInstallForcelist“ angegebene Update-URL verwenden soll.
  - Wenn die Richtlinie nicht konfiguriert oder auf „false“ gesetzt ist, wird für Updates stattdessen die URL verwendet, die im Manifest der Erweiterung angegeben ist.

Verhindern, dass Webseiten durch Erweiterungen geändert werden

Mit dieser Einstellung können Sie verhindern, dass Erweiterungen auf Websites mit vertraulichen Inhalten Daten lesen oder ändern.
Folgende Aktionen von Erweiterungen werden unterbunden:

- Skripte einschleusen
- Cookies lesen
- Webanfragen ändern

Diese Einstellung verhindert jedoch nicht, dass Nutzer Erweiterungen installieren oder entfernen. Sie verhindert lediglich, dass Erweiterungen die von Ihnen angegebenen Websites ändern.

Hierfür gibt es zwei Einstellungen:

- **runtime_blocked_hosts**: Die Interaktion der Erweiterungen mit den angegebenen Hosts wird blockiert.
- **runtime_allowed_hosts**: Die Interaktion der Erweiterungen mit den Hosts in dieser Liste wird explizit erlaubt. Das gilt auch dann, wenn ein Host ebenfalls in „runtime_blocked_hosts“ angegeben ist.

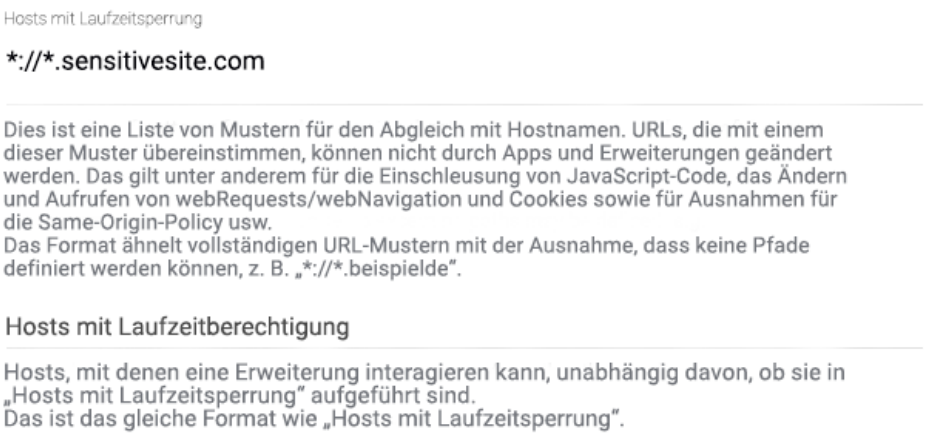
Wichtiger Tipp: Jede Instanz von „runtime_blocked_hosts“ und „runtime_allowed_hosts“ kann maximal 100 Hostmuster enthalten. Wenn Sie mehr definieren, ist die Richtlinie ungültig.

Chrome-Verwaltung über die Cloud

Hosts mit Laufzeitsperrung lassen sich in der Chrome-Verwaltung über die Cloud einfacher definieren als in Gruppenrichtlinienobjekten. Sie müssen keinen JSON-Code schreiben, sondern lediglich in den Erweiterungseinstellungen die URL eingeben, die blockiert werden soll. Dafür müssen Ihre Chrome-Geräte in der Chrome-Verwaltung über die Cloud registriert sein. Diese Funktion steht Ihnen ohne zusätzliche Kosten zur Verfügung. Hier finden Sie eine Anleitung zur Registrierung.

1. Gehen Sie in der Admin-Konsole zu **Geräte > Chrome > Apps und Erweiterungen > Nutzer und Browser**.
2. Wählen Sie die Organisationseinheit aus, für deren Nutzer Sie Erweiterungen zulassen möchten.
3. Klicken Sie auf „Zusätzliche Einstellungen“  .
4. Geben Sie im Bereich „Hosts mit Laufzeitsperrung“ die URLs der Websites mit vertraulichen Inhalten ein, die Sie für Erweiterungen blockieren möchten. Syntaxbeispiele finden Sie in diesem Hilfeartikel.
    a. Sie können mehrere URLs eingeben. Drücken Sie für jeden weiteren Eintrag einfach die Eingabetaste.
    b. Sie können auch auf eine Erweiterung klicken und dann im Bereich „Berechtigungen und URL-Zugriff“ die Hosts angeben, die zugelassen und die blockiert werden sollen.
        i. Hinweis: Die hier ausgewählten Einstellungen haben Vorrang vor globalen Richtlinien, die für die Erweiterung gelten.
        ii. Für URLs in der Liste „Hosts mit Laufzeitsperrung“ gibt es auch die Liste „Zulässige Hosts“ für Ausnahmen.

5. Klicken Sie auf **Speichern**.



Bereich „Hosts mit Laufzeitsperrung" unter „Geräte" > „Chrome" > „Apps und Erweiterungen" > „Nutzer und Browser" > „Zusätzliche Einstellungen"

Gruppenrichtlinienobjekt
Die folgende Anleitung bezieht sich auf die Verwaltung des Gruppenrichtlinienobjekts auf Windows-Computern. Anleitungen für andere Plattformen: Mac | Linux

In der Richtlinie „ExtensionSettings“ können Sie die folgenden Einstellungen festlegen, um zu verhindern oder zuzulassen, dass Erweiterungen Websites oder Domains ändern:

- Runtime_blocked_hosts
  Wenn Sie diese Einstellung aktivieren, können Erweiterungen die Daten auf den ausgewählten Websites weder lesen noch ändern.

- Runtime_allowed_hosts
  Mit dieser Einstellung erlauben Sie, dass Erweiterungen die Daten auf den ausgewählten Websites lesen und ändern.

Bei beiden Richtlinien müssen Sie die Websites im JSON-String in folgendem Format angeben:

```
[http|https|ftp|*]://[subdomain|*].[hostname|*].[eTLD|*] [http|https|ftp|*],
```

Hinweis: Die Abschnitte [hostname|*] und [eTLD|*] sind obligatorisch, der Abschnitt [subdomain|*] dagegen optional.

Beispiele für gültige Hostmuster und übereinstimmende Muster:

Gültige Hostmuster	Stimmt überein mit	Stimmt nicht überein mit
://.beispiel.*	http://beispiel.de https://test.beispiel.de	https://beispiel.google.com http://beispiel.google.de
http://beispiel.*	http://beispiel.de http://beispiel.ly	https://beispiel.de http://test.beispiel.de
http://beispiel.de	http://beispiel.de	https://beispiel.de http://test.beispiel.de
://	allen URLs	

Hier ein Beispiel für einen JSON-String, mit dem eine bestimmte Erweiterung blockiert wird. Mit diesem String wird verhindert, dass eine Erweiterung eine bestimmte Website ändert:

```
{
      "aapbdbdomjkkjkaonfhkkikfgjllcleb": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      }
}
```

Komprimierte JSON-Daten:

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb":
{"runtime_blocked_hosts":["*://*.importantwebsite"]}}
```

Hier ein Beispiel für einen String, mit dem mehrere Websites für alle Erweiterungen blockiert werden:

```
{
   "*": {"runtime_blocked_hosts": [ "*://*.importantwebsite.com",
"*://*.importantwebsite2.com" ]
   }
```

Komprimierte JSON-Daten:

```
{"*":{"runtime_blocked_hosts":["*://*.importantwebsite.com","*://*.importantweb
site2.com"]}}
```

Verwenden Sie bei mehreren Erweiterungen getrennte Einträge für jede App-ID, die Sie blockieren möchten. Hier ein Beispiel dafür, wie Sie die Ausführung von zwei Erweiterungen in derselben Domain blockieren:

```
{
      "aapbdbdomjkkjkaonfhkkikfgjllcleb": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      },
      "bfbmjmiodbnnpllbbbfblcplfjjepjdn": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      }
}
```

Komprimierte JSON-Daten:

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb": {"runtime_blocked_hosts":
["*://,*.importantwebsite"]},"bfbmjmiodbnnpllbbbfblcplfjjepjdn":
{"runtime_blocked_hosts": ["*://*.importantwebsite"]}}
```

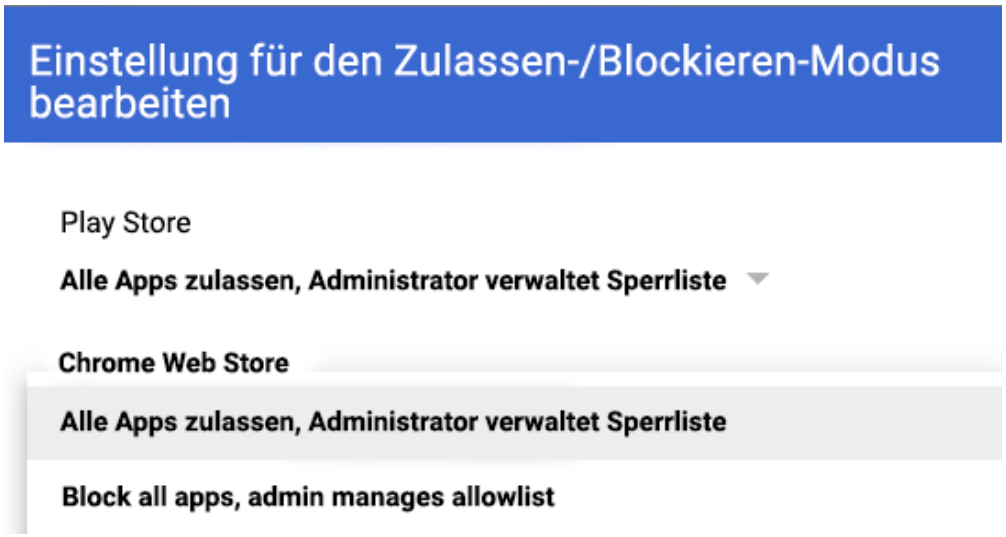
Erweiterungen in der Admin-Konsole zulassen oder blockieren

Als Administrator können Sie steuern, welche Erweiterungen Ihre Nutzer installieren dürfen, indem Sie Zulassungs- und Sperrlisten erstellen. Sie haben die Möglichkeit, Nutzern zu erlauben, jede Anwendung oder Erweiterung zu installieren. Und Sie können Richtlinien festlegen, um Anwendungen für alle Nutzer oder für bestimmte Mitarbeiter zu blockieren oder zuzulassen.

Hinweis: Bei der folgenden Anleitung wird davon ausgegangen, dass Sie sich mit dem Ändern von Einstellungen in der Admin-Konsole auskennen.

Alle Erweiterungen bis auf bestimmte Ausnahmen zulassen

1. Gehen Sie in der Admin-Konsole zu **Geräte > Chrome > Apps und Erweiterungen > Nutzer und Browser > Zusätzliche Einstellungen**.
2. Wählen Sie links die Organisationseinheit aus, für die Sie Erweiterungen zulassen möchten.
3. Scrollen Sie nach unten zum Bereich „Zulassen-/Blockieren-Modus“ unter „Chrome Web Store“, klicken Sie auf „Bearbeiten“ und aktivieren Sie die Option **Alle Apps zulassen, Administrator verwaltet Sperrliste**.

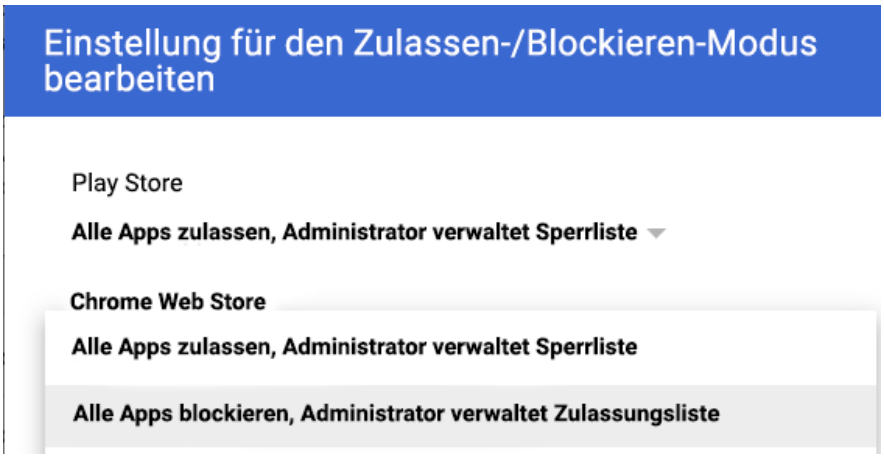


Einstellung „Zulassen-/Blockieren-Modus“

4. Klicken Sie auf **Speichern**.
5. Klicken Sie auf den Tab „Nutzer und Browser“, um zur vorherigen Seite zurückzukehren.
6. Fügen Sie die Erweiterungen, die Sie blockieren möchten, einzeln hinzu, indem Sie rechts unten auf das gelbe Pluszeichen klicken.
7. Wählen Sie die Methode zum Hinzufügen zur Konsole aus (aus dem Chrome Web Store, über die Erweiterungs-ID oder über die URL).
8. Wählen Sie im Drop-down-Menü neben der Erweiterung die Option **Blockieren** aus.
9. Klicken Sie auf **Speichern**.

Alle Erweiterungen bis auf bestimmte Ausnahmen blockieren

1. Gehen Sie in der Admin-Konsole zu **Geräte > Chrome > Apps und Erweiterungen > Nutzer und Browser > Zusätzliche Einstellungen**.
2. Wählen Sie links die Organisationseinheit aus, für die Sie Erweiterungen blockieren möchten.
3. Scrollen Sie nach unten zum Bereich „Zulassen-/Blockieren-Modus“ unter „Chrome Web Store“, klicken Sie auf „Bearbeiten“ und aktivieren Sie die Option **Alle Apps blockieren, Administrator verwaltet Zulassungsliste**.

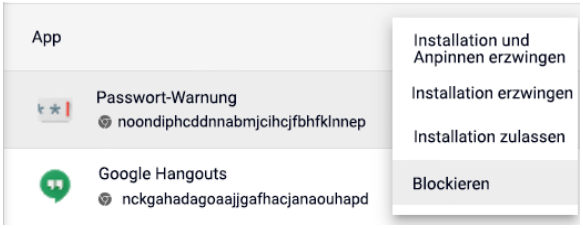


4. Klicken Sie auf **Speichern**.
5. Klicken Sie auf den Tab „Nutzer und Browser“, um zur vorherigen Seite zurückzukehren.
6. Fügen Sie die Erweiterungen, die Sie zulassen möchten, einzeln hinzu, indem Sie rechts unten auf das gelbe Pluszeichen klicken.
7. Wählen Sie die Methode zum Hinzufügen zur Konsole aus (aus dem Chrome Web Store, über die Erweiterungs-ID oder über die URL).
8. Wählen Sie im Drop-down-Menü neben der Erweiterung die Option **Installation zulassen** aus.
   a. Mit der Option „Installation erzwingen“ können Sie die Installation von Erweiterungen auch erzwingen.
9. Klicken Sie auf **Speichern**.

Eine einzelne Erweiterung blockieren oder zulassen

1. Gehen Sie in der Admin-Konsole zu **Geräte > Chrome > Apps und Erweiterungen > Nutzer und Browser**.
2. Wählen Sie die Organisationseinheit aus, für die Sie die Erweiterung zulassen oder blockieren möchten.
   - Hinweis: Für eine Organisationseinheit werden die Einstellungen der übergeordneten Organisationseinheit übernommen. Diese können Sie überschreiben, indem Sie einen Wert für die jeweilige untergeordnete Organisationseinheit festlegen.
3. Wählen Sie die gewünschte Erweiterung aus oder fügen Sie sie unter (siehe Schritte 6 und 7 des vorherigen Abschnitts) hinzu.

4. Wählen Sie in der Spalte „Installationsrichtlinien“ die Option „Blockieren“, „Installation erzwingen“ oder „Installation zulassen“ aus.

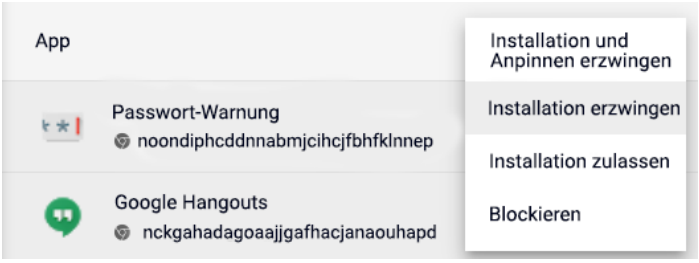


5. Klicken Sie auf **Speichern**.

Installation von Erweiterungen erzwingen

Wenn Sie wissen, dass Nutzer eine bestimmte Erweiterung benötigen, können Sie die Installation erzwingen. Es werden dann alle Berechtigungen gewährt, die erforderlich sind, um die Erweiterung auszuführen. Sie wird im Hintergrund installiert und kann vom Nutzer nicht entfernt werden. Wenn Sie eine Erweiterung aus der Liste „Installation erzwingen“ entfernen, wird sie automatisch von den entsprechenden Nutzergeräten entfernt.

1. Gehen Sie in der Admin-Konsole zu **Geräte > Chrome > Apps und Erweiterungen > Nutzer und Browser**.
2. Wählen Sie die Organisationseinheit aus, für die Sie die Installation von Erweiterungen erzwingen möchten.
3. Wählen Sie die gewünschten Erweiterungen aus oder fügen Sie sie hinzu.
   a. Klicken Sie rechts unten auf das gelbe Pluszeichen neben einer Erweiterung, um sie hinzuzufügen.
   b. Wählen Sie die Methode zum Hinzufügen zur Konsole aus (aus dem Chrome Web Store, über die Erweiterungs-ID oder über die URL).
4. Wählen Sie die gewünschten Erweiterungen aus und klicken Sie dann im Drop-down-Menü der Spalte „Installationsrichtlinien“ auf die Option **Installation erzwingen**.



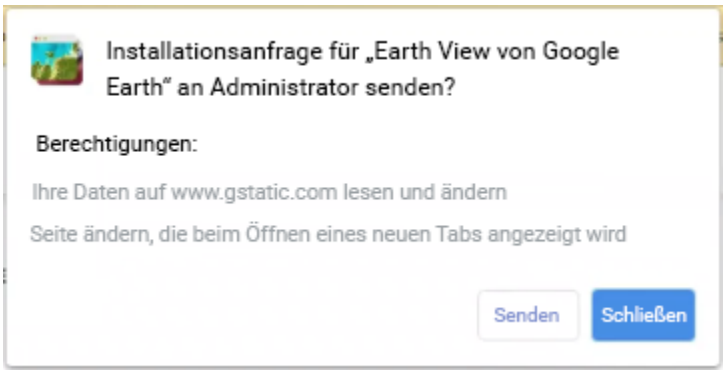
5. Klicken Sie auf **Speichern**.

Hinweis: Sie können im Chrome Web Store eine benutzerdefinierte Liste der vom Administrator ausgewählten Erweiterungen anlegen, die den Nutzern angezeigt wird. Hierfür müssen die Nutzer mit ihren geschäftlichen Anmeldedaten in der Google-Identität Ihres Unternehmens angemeldet sein.

- Sie finden diese Einstellung in der Admin-Konsole unter „Geräte“ > „Chrome“ > „Apps und Erweiterungen“ > „Nutzer und Browser“ > „Zusätzliche Einstellungen“ > „Chrome Web Store-Startseite“ > „Chrome Web Store-Sammlung verwenden“.
    - Dann können Sie entweder alle Erweiterungen auf dieser Seite anzeigen lassen oder im Bereich „Nutzer und Browser“ für einzelne Erweiterungen die Option „In Chrome Web Store-Sammlung aufnehmen“ über die Ein-/Aus-Schaltfläche aktivieren.

Nutzern ermöglichen, Erweiterungen anzufordern: Workflows

Als Administrator können Sie Nutzern über die Admin-Konsole erlauben, die erforderlichen Erweiterungen im Chrome Web Store anzufordern. Anschließend können Sie die gewünschten Erweiterungen zulassen, blockieren oder automatisch installieren.

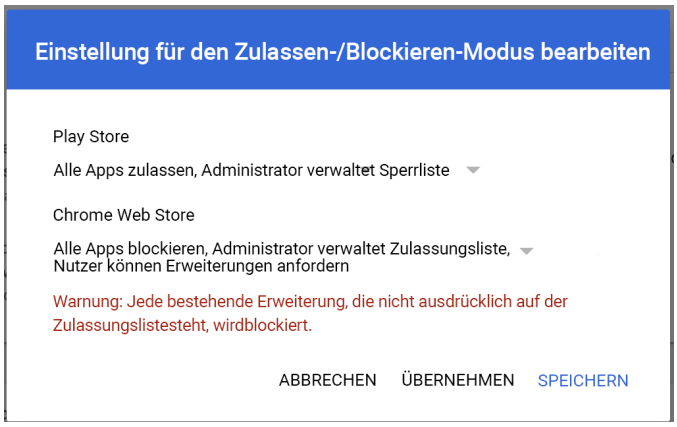


Beispiel für ein Dialogfeld zum Anfordern einer Erweiterung aus dem Chrome Web Store

Hinweis: Diese Funktion entspricht einer Zulassungs-/Sperrliste. Wenn sie aktiviert ist, werden standardmäßig **alle** Erweiterungen blockiert. Wir empfehlen, so vorzugehen, um Probleme zu vermeiden:

1. Finden Sie über die Takeout API der Chrome-Verwaltung über die Cloud heraus, welche Erweiterungen Ihre Nutzer aktuell verwenden.
    - Weitere Informationen dazu, wie Sie die Takeout API einrichten, finden Sie in diesem YouTube-Video.
2. Erstellen Sie basierend auf den in Schritt 1 gewonnenen Informationen eine Liste mit wichtigen Erweiterungen (per Gruppenrichtlinienobjekt oder in der Admin-Konsole).
3. Gehen Sie zu **Geräte > Chrome > Apps und Erweiterungen > Nutzer und Browser > Zusätzliche Einstellungen > Zulassen-/Blockieren-Modus** und klicken Sie auf „Bearbeiten“, um den Erweiterungs-Workflow zu aktivieren.

4. Wählen Sie unter „Chrome Web Store“ im Drop-down-Menü die folgende Option aus: **Alle Apps blockieren, Administrator verwaltet Zulassungsliste, Nutzer können Erweiterungen anfordern**



Workflows für Erweiterungen in der Admin-Konsole aktivieren

   - Wir empfehlen, die Einstellungen zuerst auf eine geringe Anzahl von Nutzern und Geräten in einer Testorganisationseinheit anzuwenden, um Probleme für die Endnutzer zu vermeiden und Feedback einzuholen. Wenn Sie mit den Ergebnissen der Testphase zufrieden sind, können Sie die Einstellungen dann für die gesamte Organisation übernehmen.
5. Angeforderte Erweiterungen können Sie unter **Geräte > Chrome > Apps und Erweiterungen > Anfragen** genehmigen oder ablehnen.
6. Klicken Sie auf die Zeile mit der Erweiterungsanfrage, die Sie ansehen möchten.
7. Hier finden Sie Details zu der Erweiterung und können die Installationsrichtlinie aus dem Drop-down-Menü auswählen:
   - Installation erzwingen: Die Erweiterung wird im Hintergrund installiert und kann vom Nutzer nicht entfernt werden.
   - Installation zulassen: Nutzer dürfen die Erweiterung installieren.
   - Blockieren: Nutzer dürfen die Erweiterung nicht installieren. Bei Nutzern, die die Erweiterung bereits installiert haben, wird sie entfernt.

Weitere Informationen zu dieser Funktion finden Sie im Hilfeartikel Workflows für Erweiterungen oder in diesem YouTube-Video.

Erweiterungen über die Gruppenrichtlinie zulassen oder blockieren

Hinweise: Bei den folgenden Schritten wird davon ausgegangen, dass Sie verwaltete Chrome-Geräte für Ihre Nutzer verwenden. Weitere Informationen dazu, wie Sie Chrome unter Windows bereitstellen, finden Sie im Bereitstellungshandbuch für Chrome (Windows). Informationen zur Bereitstellung und Richtlinienverwaltung auf dem Mac® finden Sie im Hilfeartikel Chrome-Browser auf einem Mac einrichten.

Für Windows sind zwei Typen von Richtlinienvorlagen verfügbar: eine ADM- und eine ADMX-Vorlage. Überprüfen Sie, welchen Vorlagentyp Sie in Ihrem Netzwerk einsetzen können. In den Vorlagen sehen Sie, welche Registrierungsschlüssel für die Konfiguration von Chrome festgelegt werden können und welche Werte möglich sind. Chrome sucht nach den in diesen Registrierungsschlüsseln festgelegten Werten und verhält sich dementsprechend.

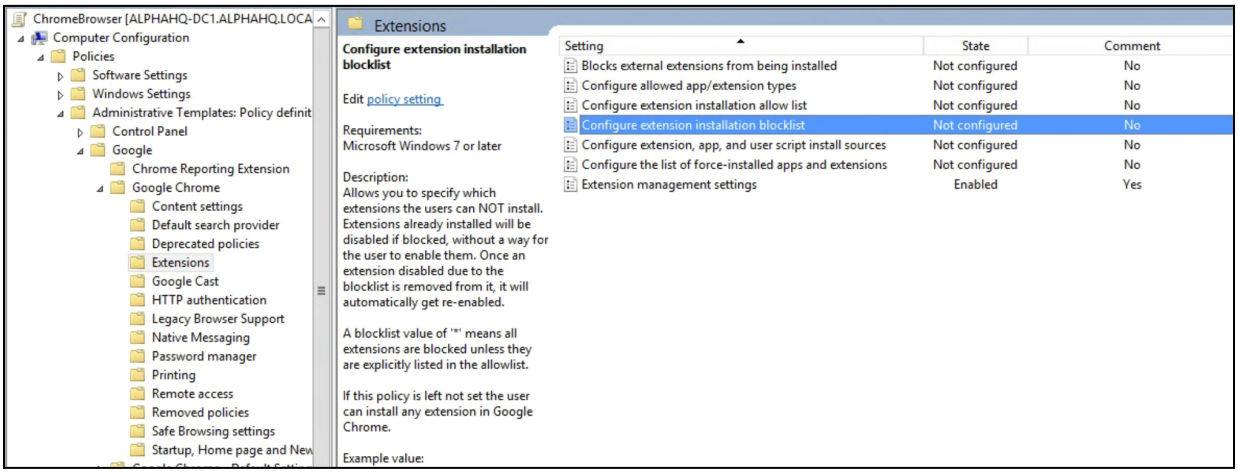
1. Laden Sie Chrome-Richtlinienvorlagen herunter.
   Die Windows-Vorlagen sowie die allgemeinen Richtlinien für alle Betriebssysteme finden Sie hier.
2. So öffnen Sie die heruntergeladene ADM- oder ADMX-Vorlage:
   a. Gehen Sie zu **Start > Ausführen: gpedit.msc**.
   b. Gehen Sie zu **Richtlinie für „Lokaler Computer“ > Computerkonfiguration > Administrative Vorlagen**.
   c. Klicken Sie mit der rechten Maustaste auf **Administrative Vorlagen** und wählen Sie **Vorlagen hinzufügen/entfernen** aus.
   d. Fügen Sie über das Dialogfeld die Vorlage „chrome.adm“ hinzu.

Anschließend wird unter „Administrative Vorlagen“ ein Ordner mit dem Namen „Google“ oder „Google Chrome“ angelegt, falls dieser nicht bereits vorhanden ist.

- Wenn Sie die ADM-Vorlage unter Windows 7 oder 10 hinzufügen, wird sie unter „Klassische administrative Vorlagen“ / „Google“ / „Google Chrome“ angezeigt.

Alle Erweiterungen bis auf bestimmte Ausnahmen zulassen

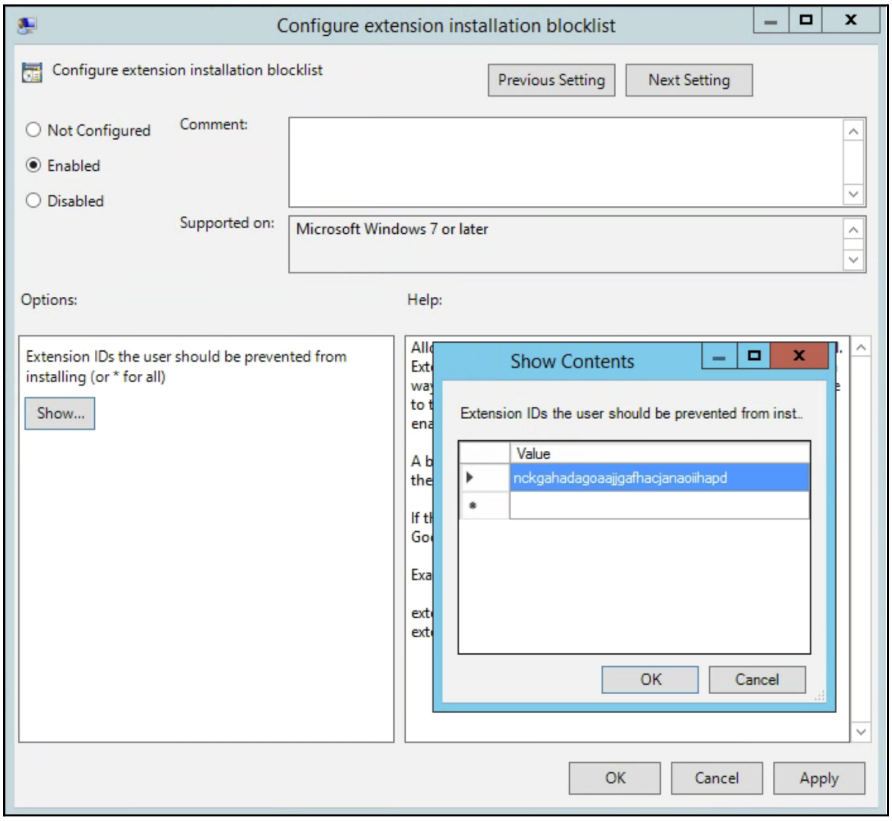
1. Öffnen Sie die soeben hinzugefügte Vorlage im Gruppenrichtlinien-Editor.
2. Gehen Sie zu **Google > Google Chrome > Erweiterungen > Sperrliste für Installation von**



Erweiterungen konfigurieren.

Pfad zu den Richtlinien zur Erweiterungsverwaltung

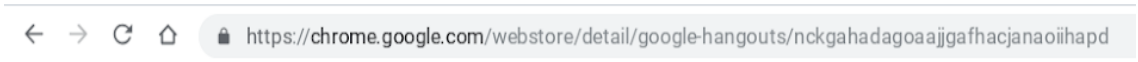
2. Wählen Sie für die Einstellung **Aktiviert** aus.
3. Klicken Sie auf **Anzeigen**.
4. Geben Sie die App-ID der Erweiterungen ein, die Sie blockieren möchten.



Sperrliste für Installation von Erweiterungen konfigurieren

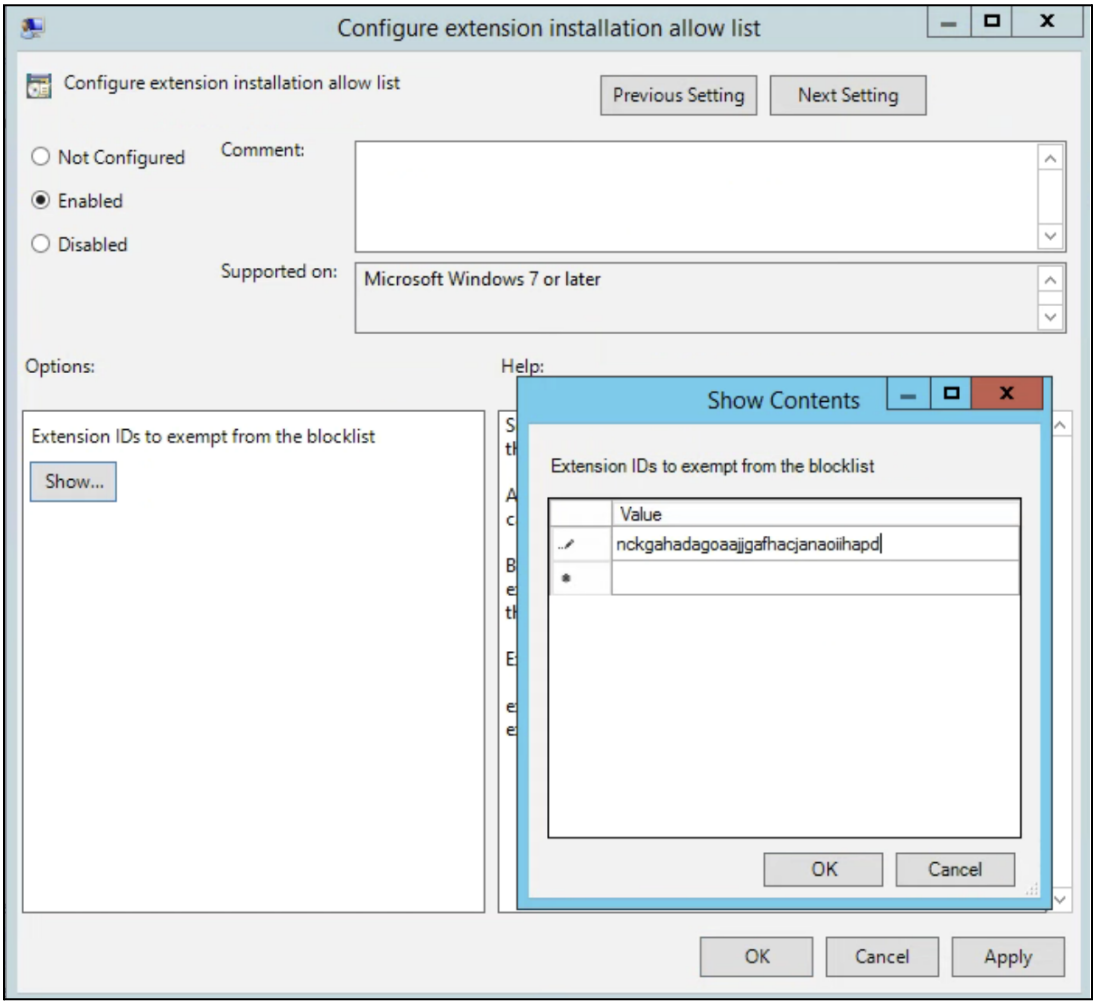
Hinweise:

- Wenn Sie die App-ID einer Erweiterung nicht finden können, sehen Sie im Chrome Web Store nach. Suchen Sie die Erweiterung. Die App-ID befindet sich am Ende der URL in der Chrome-Omnibox:



Beispiel für die App-ID nach google-hangouts/

- Geben Sie ein Sternchen ***** ein, um festzulegen, dass keine Erweiterung installiert werden darf. Sie können diese Einstellung zusammen mit der Richtlinie „Zulassungsliste für die Installation von Erweiterungen konfigurieren“ verwenden. So haben Sie die Möglichkeit, Ihren Nutzern die Installation bestimmter Erweiterungen zu erlauben und den Rest zu blockieren.
- Sie können auch Erweiterungen, die bereits auf Nutzergeräten installiert sind, der Sperrliste hinzufügen. Dadurch werden sie deaktiviert und die Nutzer können sie nicht wieder aktivieren. Hinweis: Die Erweiterung wird nicht deinstalliert, sondern lediglich deaktiviert.



Zulassungsliste für die Installation von Erweiterungen konfigurieren

Eine einzelne Erweiterung blockieren oder zulassen

Wenn Sie eine einzelne Erweiterung blockieren möchten, fügen Sie in der Einstellung „Sperrliste für Installation von Erweiterungen konfigurieren“ die entsprechende App-ID hinzu. Die Installation aller anderen Erweiterungen wird zugelassen.

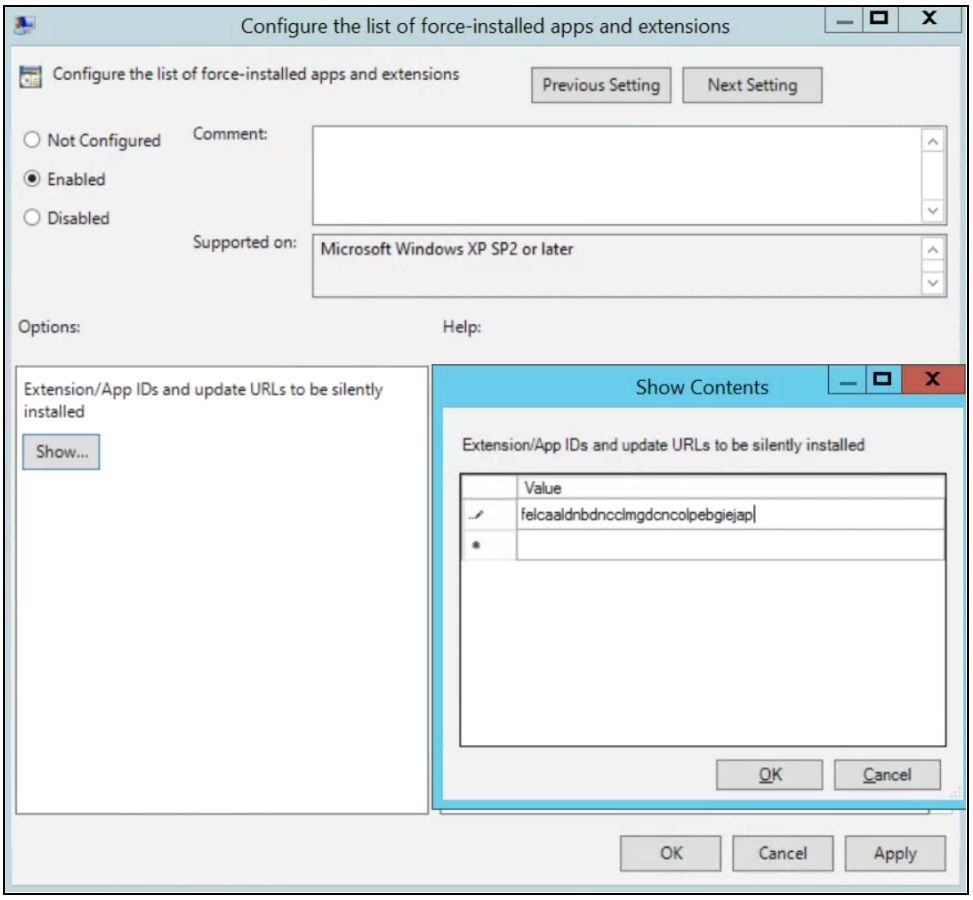
So lassen Sie eine einzelne Erweiterung zu:

1. Geben Sie im Bereich „Inhalt“ der Einstellung „Sperrliste für Installation von Erweiterungen konfigurieren“ ein Sternchen ***** ein.
   So wird die Installation aller Erweiterungen auf der Liste blockiert.
2. Fügen Sie in der Einstellung „Zulassungsliste für Installation von Erweiterungen konfigurieren“ die App-ID der Erweiterung hinzu, die Sie zulassen möchten.

Installation von Erweiterungen erzwingen

1. Gehen Sie im Gruppenrichtlinien-Editor zu **Google > Google Chrome > Erweiterungen > Liste der Apps und Erweiterungen konfigurieren, deren Installation erzwungen wurde**.
2. Wählen Sie **Aktiviert** aus.
3. Klicken Sie auf **Anzeigen**.
4. Geben Sie die App-IDs der Erweiterungen ein, deren Installation erzwungen werden soll.

Die Erweiterungen werden im Hintergrund installiert. Die Nutzer können sie nicht deinstallieren oder deaktivieren. Diese Einstellung hat Vorrang vor allen aktivierten Sperrlisten-Richtlinien.



Liste der Apps und Erweiterungen konfigurieren, deren Installation erzwungen wurde

Richtlinien validieren

Sie können prüfen, ob Richtlinien gültig sind und wie erwartet funktionieren, indem Sie sie auf ein Testgerät anwenden. Führen Sie auf dem Testgerät die folgenden Schritte aus.

1. Gehen Sie zu chrome://policy.
2. Klicken Sie auf die Schaltfläche „Richtlinien neu laden“.
3. Geben Sie oben rechts im Feld zum Filtern von Richtlinien „ExtensionSettings“ ein.
4. Setzen Sie ein Häkchen in das Kästchen neben „Richtlinien ohne Wert zeigen“.
5. Der „Status“ Ihrer Richtlinie muss „Ok“ lauten.
6. Klicken Sie auf „Wert anzeigen“ und vergewissern Sie sich, dass das Feld nicht leer ist.
7. Glückwunsch! Die Richtlinie ist gültig.

Eigene Erweiterungen selbst hosten

Wenn Sie Erweiterungen im Chrome Web Store hosten, profitieren Sie von vielen Sicherheitsfunktionen.

- Dazu gehören automatische und manuelle Codescans.
    - Damit lässt sich verhindern, dass auf den Geräten Ihrer Nutzer schädlicher Code installiert wird.

Sie haben aber auch die Möglichkeit, Ihre Erweiterungen auf einem eigenen Server zu hosten. Hier haben wir einige Vor- und Nachteile dieser Möglichkeit für Sie aufgelistet:

Vorteile:

- Wenn Sie Ihre Erweiterungen auf einem eigenen Server hosten, gelten die Regeln und Anforderungen des Chrome Web Store nicht für Sie.
    - Die Erweiterungen werden nicht so genau geprüft und das Risiko, dass sie aufgrund von Verstößen gegen die Nutzungsbedingungen entfernt werden, wird minimiert.

Nachteile:

- Der Einrichtungsaufwand ist höher und Sie benötigen einen eigenen Dateiserver für die Erweiterungsdateien.
- Es ist keine einfache Aufgabe, die Sicherheit der Erweiterungen zu prüfen und sie auf dem neuesten Stand zu halten. Im Chrome Web Store erfolgt das automatisch.

In diesem Abschnitt wird beschrieben, wie Sie Ihre Erweiterungen selbst hosten können. Sie erfahren, wie Sie eine Erweiterung packen und ohne den Chrome Web Store hosten. Außerdem finden Sie hier eine Anleitung dazu, wie Sie diese Erweiterungen auf den Geräten Ihrer Nutzer bereitstellen.

Alternativen zum Hosting auf dem eigenen Server

Möglichkeiten, Erweiterungen zu veröffentlichen

Alternativ können Sie interne Erweiterungen im Chrome Web Store als privat kennzeichnen. Es gibt drei Optionen zur Veröffentlichung von Erweiterungen: „Öffentlich“, „Privat“ und „Nicht gelistet“. Hier sehen Sie auf einen Blick, was jede Option bietet:

	Auffindbar mit der Chrome Web Store-Suche	Anmeldung erforderlich	Kompatibel mit der Chrome-Verwaltung über die Cloud
Öffentlich	Ja	Nein	Ja
Privat	Nein	Ja	Ja
Nicht gelistet	Nein	Nein – Nutzer benötigen einen Link für die Installation	Ja

Weitere Informationen finden Sie in diesem Blog, in dem es darum geht, wie sich Erweiterungen auf Ihre Domain beschränkt veröffentlichen lassen, ohne sie auf einem eigenen Server zu hosten.

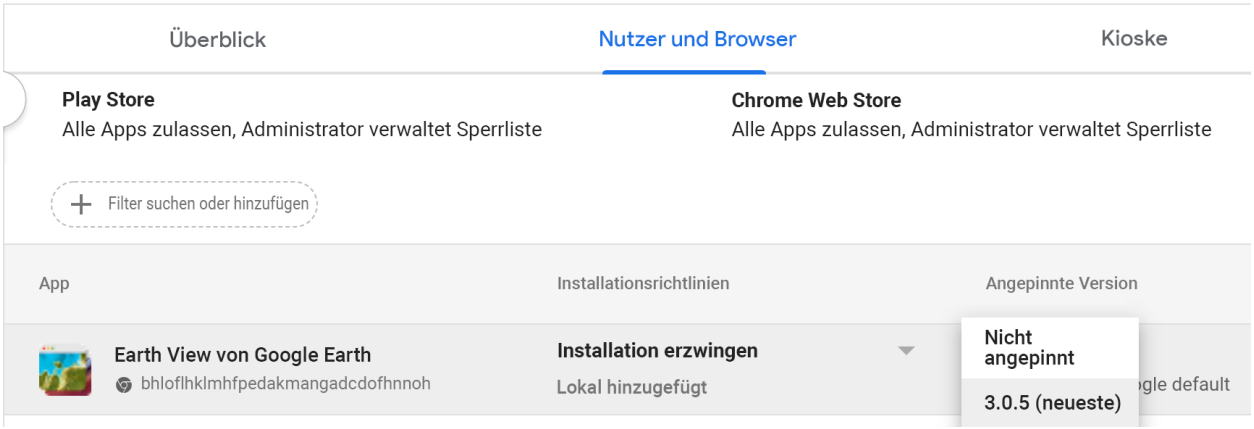
- Hinweis: Wenn Sie Ihre Erweiterungen über die Admin-Konsole verwalten, müssen Sie die Einstellung „Chrome Web Store-Berechtigungen“ konfigurieren, damit private Erweiterungen für Ihre Nutzer sichtbar sind.
    - Gehen Sie zu „Geräte“ > „Chrome“ > „Apps und Erweiterungen“ > „Zusätzliche Einstellungen“ > „Chrome Web Store-Berechtigungen“ und aktivieren Sie die Option „Nutzern erlauben, auf Ihre Domain beschränkte Apps im Chrome Web Store zu veröffentlichen“.

Erweiterungen in der Admin-Konsole auf eine bestimmte Version festlegen

In der Admin-Konsole gibt es zur Verwaltung von Erweiterungen jetzt einige neue Optionen. Sie haben beispielsweise die Möglichkeit, Erweiterungen auf eine bestimmte Version festzulegen. In einigen Unternehmen kann es aus Stabilitätsgründen erforderlich sein, eine bestimmte Version einer Erweiterung zu verwenden. Es ist jedoch nicht empfehlenswert, über einen längeren Zeitraum die veraltete Version einer Erweiterung zu verwenden. Greifen Sie höchstens für einen kurzen Zeitraum zu dieser Maßnahme, sodass Sie nicht zu lange ohne Funktions- und Sicherheitsupdates auskommen müssen. Diese Funktion ist nur für Erweiterungen mit erzwungener Installation verfügbar. Weitere Informationen finden Sie in diesem Hilfeartikel.

1. Gehen Sie in der Admin-Konsole zu **Geräte > Chrome > Apps und Erweiterungen > Nutzer und Browser**.

2. Wählen Sie die Organisationseinheit mit der gewünschten Erweiterung aus.
3. Wählen Sie eine Erweiterung aus oder fügen Sie eine neue hinzu, wählen Sie im Drop-down-Menü der Spalte „Angepinnte Version“ die Version aus, auf die Sie die Erweiterung festlegen möchten, und klicken Sie auf „Speichern“.
    a. Hinweis: Apps und Erweiterungen mit angepinnter Version werden nicht aktualisiert, auch nicht mit Sicherheits- und Kompatibilitätsupdates.
    b. Sie können nur die aktuelle Version der Erweiterung anpinnen, die bei der Einrichtung im Chrome Web Store verfügbar ist.
    c. Sie können auch die Versionen selbst gehosteter Apps und Erweiterungen anpinnen und die URL in der Admin-Konsole aktualisieren. Weitere Informationen finden Sie in diesem Hilfeartikel unter „Selbst gehostete Apps anpinnen“.



Versionen in der Admin-Konsole anpinnen

Erweiterungen selbst hosten – Anforderungen

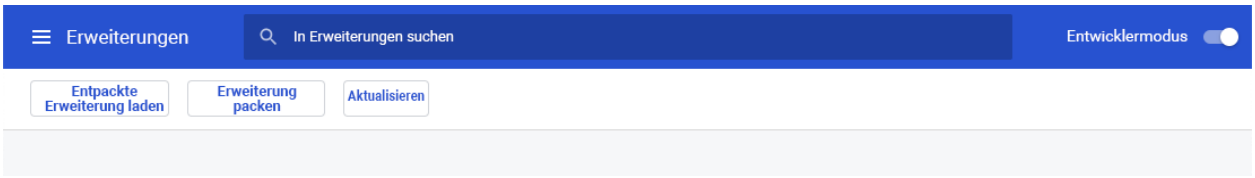
Wenn Sie Erweiterungen selbst hosten möchten, benötigen Sie eigene Webhosting-Dienste und die Manifest-Datei der Erweiterung. Der Hosting-Ort sollte keine Authentifizierung erfordern. Geräte müssen von überall aus darauf zugreifen können. Berücksichtigen Sie dies, wenn Sie die Datei in Ihrem internen Repository hosten möchten.

Für diese Schritte wird davon ausgegangen, dass Sie bereits eine Erweiterung erstellt haben und sich mit XML-Dateien auskennen. Außerdem wird vorausgesetzt, dass Sie wissen, wie Sie Gruppenrichtlinien und die Windows-Registrierung verwenden. Diese Anleitung eignet sich nicht für Erweiterungen von Drittanbietern, die Sie nicht entwickelt haben. Wenn Sie die Erweiterung eines Drittanbieters selbst hosten möchten, wenden Sie sich am besten direkt an den Anbieter.

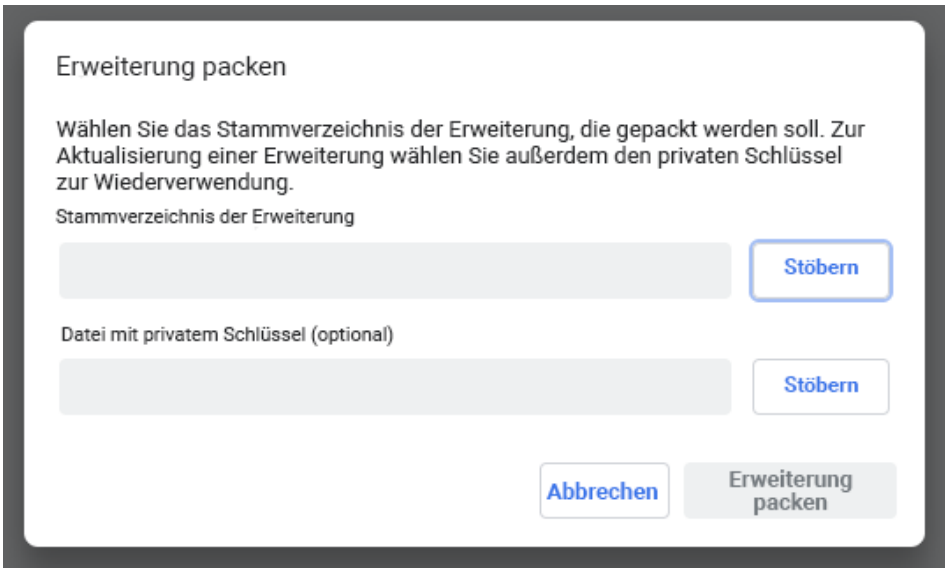
Erweiterung packen

Die Erweiterung muss zuerst als CRX-Datei gepackt werden. Das geht so:

1. Geben Sie in der Chrome-Adressleiste **chrome://extensions** ein und klicken Sie die Option **Entwicklermodus** an.



2. Erstellen Sie im Entwicklermodus die CRX-Datei, indem Sie auf **Erweiterung packen** klicken.

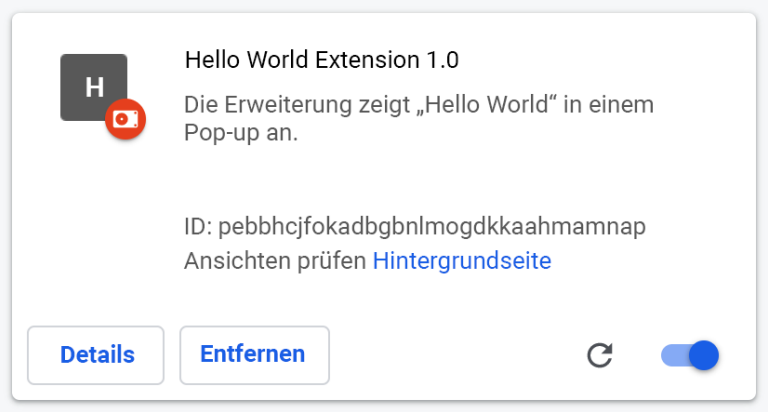


3. Wählen Sie das Stammverzeichnis aus. Die CRX-Datei und eine PEM-Datei werden erstellt.

Wichtiger Tipp: Speichern Sie die PEM-Datei an einem sicheren Ort. Sie ist der Schlüssel zu Ihrer Erweiterung. Sie benötigen sie für zukünftige Updates.

4. Ziehen Sie die CRX-Datei in das Erweiterungsfenster und prüfen sie, ob sie geladen wird.
    a. Hinweis: Unter Windows und Mac ist die Erweiterung standardmäßig deaktiviert, bei Linux jedoch nicht.

5. Testen Sie die Erweiterung und notieren Sie sich die ID und die Versionsnummer. Sie benötigen diese später.



6. Legen Sie die CRX-Datei auf dem Host an dem Ort ab, von dem die Nutzer oder Geräte sie herunterladen werden.
    - Notieren Sie die URL des Uploadpfads.
    - Sie brauchen sie später für die Manifest-XML-Datei.
7. Zum Erstellen der Manifest-XML-Datei mit der App-/Erweiterungs-ID, der Download-URL und der Version definieren Sie diese drei Felder:
    - **appid** (die Erweiterungs-ID aus Schritt 5)
    - **codebase** (die Download-URL der CRX-Datei aus Schritt 3)
    - **version** (die Version der App/Erweiterung aus Schritt 5)

    Beispiel einer Manifest-XML-Datei:

```
<?xml version='1.0' encoding='UTF-8'?>
<gupdate xmlns='http://www.google.com/update2/response' protocol='2.0'>
  <app appid='abcdefghijklmnopqrstuvwxyz123456
'>
    <updatecheck codebase='https://example.com/chrome/helloworld.crx'
version='1.0' />
  </app>
</gupdate>
```

8. Laden Sie die fertige XML-Datei an einen Ort hoch, an dem Nutzer oder Geräte sie herunterladen können, und notieren Sie sich die URL.

Erweiterung hosten

Der Server, auf dem Sie die CRX-Dateien der Erweiterung hosten, muss die entsprechenden HTTP-Header haben, damit Nutzer die Erweiterung durch Klicken auf einen Link installieren können.
Für Google Chrome ist eine Datei installierbar, wenn einer der folgenden Punkte zutrifft:

- Die Datei hat den Inhaltstyp „application/x-chrome-extension“.
- Das Suffix der Datei ist „.crx“ und die folgenden Punkte treffen beide zu:
    - Die Datei weist nicht den folgenden HTTP-Header auf: X-Content-Type-Options: nosniff
    - Die Datei hat einen der folgenden Inhaltstypen:
        - Leerer String
        - "text/plain"
        - "application/octet-stream"
        - "unknown/unknown"
        - "application/unknown"
        - "*/*"

Das Senden des Headers „X-Content-Type-Options: nosniff“ durch den Server ist der häufigste Grund dafür, dass eine Installationsdatei nicht erkannt wird. Der zweithäufigste Grund ist das Senden eines unbekannten Inhaltstyps, der sich nicht in der oben stehenden Liste befindet. Das Problem mit dem HTTP-Header lässt sich beheben, indem Sie die Konfiguration des Servers ändern oder die CRX-Datei auf einem anderen Server hosten.

Updates für die Erweiterung veröffentlichen

Stellen Sie sicher, dass Sie die erforderlichen Änderungen vorgenommen haben, und testen Sie die Erweiterung. So veröffentlichen Sie Updates:

1. Erhöhen Sie die Versionsnummer in der Manifest-JSON-Datei der Erweiterung.
   Beispiel:
   `"version": "versionString"`
   Bei `"version":"1.0"` können Sie die Versionsangabe auf `"version":"1.1"` oder eine beliebige andere höhere Nummer als `"1.0"` erhöhen.

2. Passen Sie in der XML-Datei die Angabe `"version"` unter `<updatecheck>` an die im letzten Schritt in der Manifestdatei angegebene Nummer an.
   Ein weiteres Beispiel:
   `<updatecheck codebase='https://app.somecompany.com/chrome/helloworld.crx' version='1.1' />`

3. Erstellen Sie eine neue CRX-Datei mit den letzten Änderungen:
    a. Geben Sie in der Chrome-Adressleiste **chrome://extensions** ein.
    b. Klicken Sie die Option **Entwicklermodus** an.

4. Erstellen Sie die CRX-Datei. Klicken Sie dazu auf **Erweiterung packen** und wählen Sie das Stammverzeichnis aus.

Hinweis: Verwenden Sie als PEM-Datei die Datei, die beim ersten Erstellen der CRX-Datei generiert wurde und die Sie gespeichert haben.

5. Ziehen Sie die CRX-Datei in das Erweiterungsfenster und prüfen sie, ob sie geladen wird.
6. Testen Sie die Erweiterung.
7. Ersetzen Sie die alte CRX-Datei und XML-Datei durch die neue Datei.
    a. Diese muss sich auf dem Host an demselben Ort befinden, von dem Nutzer oder Geräte die Dateien zuvor bereits heruntergeladen haben.

Die Änderungen werden bei der nächsten Richtliniensynchronisierung übernommen.

Referenz-URLs:

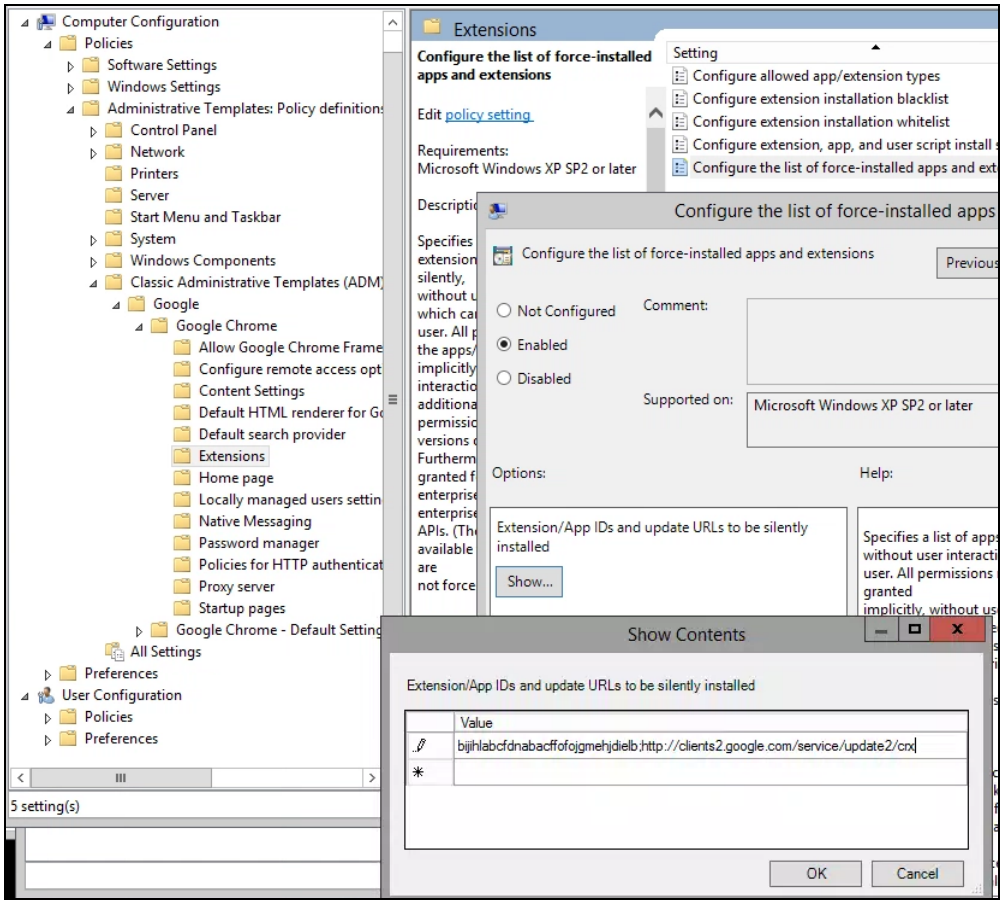
- Autoupdating (automatische Aktualisierung)
- Update URL (Update-URL)
- Update manifest (Update-Manifest)

Selbst gehostete Erweiterungen verteilen

Über die Gruppenrichtlinien: Momentan lassen sich selbst gehostete Erweiterungen nur über Gruppenrichtlinien verteilen. Mit der Richtlinie „Liste der Apps und Erweiterungen konfigurieren, deren Installation erzwungen wurde“ können Sie die Installation von Erweiterungen auf Nutzergeräten erzwingen.

Für selbst gehostete Apps (nicht im Chrome Web Store) verwenden Sie einen String nach folgendem Muster:
`pckdojakecnhhplcgfflhndiffaohfah;https://sites.google.com/site/pushcrx/privatewebstore/extension_info.xml`

Die URL wird eher mit **update.xml** der internen App statt über die öffentliche URL `clients2.google.com` angegeben.



Gruppenrichtlinienobjekt „Liste der Apps und Erweiterungen konfigurieren, deren Installation erzwungen wurde“ (Inhalt anzeigen)

Dann können Sie die Richtlinien auf die ausgewählten Nutzer und/oder Geräte anwenden. Es kann etwas dauern, bis die Richtlinien wirksam werden. Sie können den Prozess beschleunigen, indem Sie auf den Nutzergeräten „gpupdate“ ausführen.

Erweiterungen in der Chrome-Verwaltung über die Cloud verwalten

Sie können die Chrome-Browser auf Ihren Windows-, Mac- und Linux-Geräten an einem Ort verwalten und erhalten einen genauen Einblick in den Chrome-Status in Ihrer Umgebung. Die Einstellungen für den Chrome-Browser lassen sich mit der Chrome-Verwaltung über die Cloud sehr gut verwalten. Die Konsole ist ohne zusätzliche Kosten verfügbar. Alle Bereiche in diesem Dokument, die auf die Admin-Konsole verweisen, können Sie mit dieser Chrome-Funktion aufrufen. In der Konsole können Sie im Handumdrehen folgende Informationen aufrufen:

- Die auf Ihren Geräten momentan installierten Chrome-Versionen
- Die in den einzelnen Browsern installierten Erweiterungen
- Die auf die einzelnen Browser angewendeten Richtlinien
- Weitere Informationen dazu, wie Sie Erweiterungen mit der Chrome-Verwaltung über die Cloud verwalten, finden Sie in diesem Video.

Weitere Ressourcen

Hier einige weitere Ressourcen mit nützlichen Informationen zur Chrome-Verwaltung in Ihrem Unternehmen:

- Startseite der Chrome-Verwaltung über die Cloud
- Chrome Enterprise-Bundle
- Liste der Chrome Enterprise-Richtlinien
- Chrome Enterprise-Versionshinweise
- Strategien für die Updateverwaltung in Chrome
- Google Chrome Enterprise-Hilfe
- Chrome als Standardbrowser festlegen (Windows 10)
- Chrome Insider-Blogreihe
- Blogartikel zur Umstellung von Chrome-Erweiterungen auf Manifest V3