

Technischer Leitfaden zu Updates



Inhalt

Einführung

- Was ist Google Update?
- Was ist das Framework für Chrome-Varianten?
- Tests mit Release-Versionen für Chrome optimieren

Strategien für die Updateverwaltung

- Strategie 1: Automatische Updates (verfügbare Updates werden automatisch installiert)
 - Chrome so konfigurieren, dass Updates installiert werden, sobald sie verfügbar sind
 - Zusätzliche Steuerelemente
- Strategie 2: Versionsfixierung (Sie legen fest, wann Updates installiert werden)
 - Chrome so konfigurieren, dass Updates installiert werden, wenn die Voraussetzungen stimmen
 - Zusätzliche Steuerelemente
- Strategie 3: Ausschließlich manuelle Updates (Sie installieren Updates manuell per Push)

Weitere Überlegungen

- Mit begrenzter Bandbreite arbeiten
 - Wartungsfenster einrichten
 - Updates verteilen
 - Updates im Cache speichern
- Umgang mit Programmfehlern und Kompatibilitätsproblemen
 - Neustart-Benachrichtigungen
 - Rollback
 - Varianten deaktivieren
 - Updates für Komponenten deaktivieren

Fehlerbehebung

- Protokolldaten erfassen
- URL-Zulassungsliste
- Wird Chrome auch aktualisiert, wenn der Browser nicht ausgeführt wird?
- Werden alle Browser auf einmal aktualisiert?

Fazit

- Weitere Informationen

Einführung

Durch die automatischen Updates von Chrome erhalten Ihre Nutzer direkt die neuesten Funktionen und Sicherheitsupdates. So können sie in einer geschützten Umgebung produktiv arbeiten. Chrome bietet verschiedene Steuerelemente für Updates, die Sie so auswählen können, dass Sie den Sicherheits- und Kontrollanforderungen Ihrer Organisation gerecht werden.

In diesem technischen Leitfaden werden die Updatemechanismen für Chrome und die dafür verfügbaren Steuerelemente der drei Hauptstrategien für die Updateverwaltung erläutert. Außerdem finden Sie hier weitere Informationen zur Updateverwaltung in Ihrer Umgebung, darunter Tipps zum Umgang mit Fehlern und Inkompatibilitäten sowie zur Problembeseitigung.

Hinweis: Erweiterungen werden in einem separaten Prozess aktualisiert, der im [technischen Leitfaden zur Verwaltung von Erweiterungen](#) beschrieben wird.

Was ist Google Update?

Google Update ist unsere Technologie für automatische Updates in Chrome. Google Update unterstützt Software-Patching für Chrome (und andere Google-Produkte) auf Windows-Geräten. Das Pendant für den Mac ist Google Software Update.

Wenn Sie Google Update verwenden, müssen Sie neue Chrome-Versionen nicht manuell verwalten und selbst im Push-Verfahren auf Ihren Geräten bereitstellen. Das umfasst auch Sicherheitspatches.

Außerdem haben Sie die Möglichkeit, Google Update mithilfe von Richtlinien so zu konfigurieren, dass für einige Nutzer eine bestimmte Chrome-Version festgelegt wird oder dass ein Rollback auf eine frühere Version ausgeführt wird – ohne manuelle Schritte und ohne neue MSI-Datei. Es ist in den Chrome-Installationsprogrammen integriert, muss also nicht separat installiert werden. Richtlinien für Google Update lassen sich über die [Admin-Konsole](#) (nur stabile Release-Version) oder über Gruppenrichtlinienobjekte (alle Release-Versionen) festlegen. Hinweis: Über Gruppenrichtlinienobjekte konfigurierte Richtlinien haben Vorrang, es sei denn, **CloudPolicyOverridesPlatformPolicy** ist für Google Update festgelegt (nicht zu verwechseln mit der Chrome-Richtlinie mit demselben Namen). [Hier können Sie die neueste administrative Vorlage von Google Update herunterladen](#).

Die Hauptinstallation für den Chrome-Browser erfordert einen Speicherplatz von etwa 56 MB.

- Nachfolgende Updates von einer Version auf die nächste sind jeweils ca. 10 bis 15 MB.
- Patch-Updates typischerweise 3 bis 5 MB groß.

Bei Updates von einer Version auf eine höhere, nicht unmittelbar nachfolgende Version ist in der Regel eine komplette Neuinstallation erforderlich.

Was ist das Framework für Chrome-Varianten?

Mit dem Framework für Chrome-Varianten lassen sich Funktionen und Korrekturen nach und nach aktivieren und erforderlichenfalls auch schnell wieder deaktivieren. Das sind die Vorteile dieses Ansatzes:

- Sie können kleine Nutzergruppen neue Funktionen testen lassen und Feedback einholen.
- Änderungen lassen sich für einen vorher festgelegten Prozentanteil der Nutzer kontrolliert einführen, um das Risiko von Kompatibilitätsproblemen zu minimieren.
- Sie erhalten sicherheitsrelevante und andere wichtige Updates schneller.
- Bei Bedarf können Sie ein Rollback ausführen, ohne auf eine neue Version von Chrome warten zu müssen. Die Nutzer müssen lediglich ihre Computer neu starten, um die neue Konfiguration zu aktivieren.

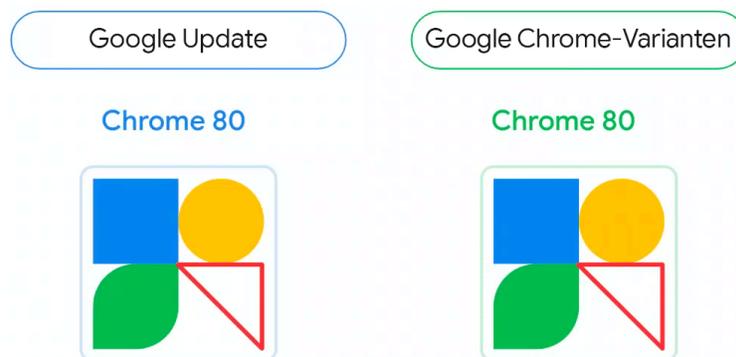


Abb. 1: Visueller Vergleich von Google Update und dem Framework für Chrome-Varianten. Das Dreieck steht für eine Funktion, die über Chrome-Varianten aktiviert und deaktiviert wird.

Tests mit Release-Versionen für Chrome optimieren

Wir veröffentlichen etwa alle vier Wochen eine neue Hauptversion von Chrome. Jede Release-Version von Chrome repräsentiert eine andere Phase des Release-Zyklus. So können Sie sich besser auf neue Versionen vorbereiten.

- Für die **meisten Nutzer** empfehlen wir die **stabile Version**. Sie ist vollständig getestet und wird von Google unterstützt.

- Organisationen, bei denen es erforderlich ist, dass einige Nutzer dieselbe Chrome-Version länger als vier Wochen verwenden, können die **erweiterte stabile Version** verwenden. Bei dieser Version wird jeweils eine Hauptversion übersprungen, sodass die Hauptversion alle acht Wochen aktualisiert wird. Sie enthält aber auch wichtige sicherheitsrelevante Korrekturen. Damit haben Administratoren einen doppelt so langen Zyklus zur Verwaltung von Updates. Hinweis: Bei der erweiterten stabilen Version werden zwar etwa alle zwei Wochen Sicherheitsupdates veröffentlicht, um wichtige Fehler zu korrigieren. Einige Sicherheitsverbesserungen und neue Funktionen sind in der stabilen Version jedoch eher verfügbar – dies ist also die sicherere Option. Da hier aber jede zweite Hauptversion der stabilen Version angewendet wird, sind die ersten vier Wochen des Zyklus identisch mit der stabilen Version. In den folgenden Abschnitten zu [Chrome-Varianten](#) und [Updates für Komponenten](#) wird erläutert, wie Sie diese Richtlinien bei Konfigurationen mit der erweiterten stabilen oder der stabilen Version effektiv anwenden.
- **5 % der Nutzer** sollten die **Beta-Version** verwenden. Die Betaversion ist unser Release-Kandidat. Hiermit bleiben Sie über neue Funktionen auf dem Laufenden – bei minimalem Risiko. Sie wird von Google vollständig unterstützt. Betanutzer sollten eine breite Palette von Funktionen testen, sodass möglichst viele Fehler und Kompatibilitätsprobleme entdeckt werden, bevor die Version als stabil veröffentlicht wird. Windows- und Mac-Nutzer [können die Beta- und die stabile Version parallel ausführen](#), sodass sie einfach zur stabilen Version wechseln können, falls sie einmal aufgrund eines schwerwiegenden Problems in der Betaversion nicht weiterarbeiten können. Das kommt jedoch nur selten vor. Wir empfehlen auch, [MetricsReportingEnabled](#) zu aktivieren, um die Nutzungsstatistiken zu erfassen. So kann Google Abstürze in der Betaversion einfacher erkennen und die Fehler korrigieren. Sie können diese Richtlinie als „Empfohlen“ festlegen, sodass sie sich bei Bedarf von den Nutzern deaktivieren lässt.
- **IT-Mitarbeiter und Entwickler** können mit der **Entwicklerversion** neue Funktionen noch früher testen. Es ist nicht garantiert, dass diese Funktionen in die Beta- oder die stabile Version übernommen werden, aber es ist eine gute Möglichkeit, neue Entwicklungen zu testen. Da die Entwicklerversion instabil sein kann, empfehlen wir, sie parallel zur stabilen Version auszuführen, statt sie über die TargetChannel-Einstellung als einzige verfügbare Chrome-Instanz für die Nutzer festzulegen.

Tipp: Informieren Sie Ihre Betanutzer darüber, wie Sie das IT-Team kontaktieren können, wenn sie Fehler entdecken.

Admin-Konsole:
Seite mit Nutzer- und Browsereinstellungen >
Weitere Einstellungen >
Berichterstellung für Messwerte

GPO: Google >
Google Chrome >
Enable reporting of usage and crash-related data
(Berichte mit Nutzungs- und Absturzdaten erstellen)

Mac:
MetricsReportingEnabled

chrome enterprise

- Für **Entwickler**, die daran interessiert sind, brandneue Chrome-Funktionen zu testen, gibt es die **Canary-Version**. Hinweis: Die Canary-Version wird nicht von Google getestet und kann instabil oder sogar nicht ausführbar sein. Sie eignet sich ausschließlich zu Testzwecken.

Version	Release-Häufigkeit	Unterstützt	Tests durch Google	Empfohlen für
 Stabil	Etwa alle 2 Wochen (Nebenversionen) Alle 4 Wochen (Hauptversionen)	Ja	Vollständig getestet	Die meisten Nutzer
 Stabil (erweitert)	Etwa alle 2 Wochen (Nebenversionen) Alle 8 Wochen (Hauptversionen)	Ja	Vollständig getestet	Nutzer, für die zusätzliche Stabilität erforderlich ist
 Beta	In der Regel wöchentlich (Nebenversionen) Alle 4 Wochen (Hauptversionen)	Ja	Release-Kandidat	5 % der Nutzer
 Entwickler	Ein- oder zweimal wöchentlich		Minimal getestet	IT-Mitarbeiter (ausschließlich)
 Canary	Täglich, direkt nach Fertigstellung des Builds		Nicht getestet	Entwickler, nur zu Testzwecken

Wenn Sie Chrome mit dem Binärprogramm der stabilen Version installiert haben, können Sie die Release-Version unter [Windows](#) und [Mac](#) angeben, indem Sie **TargetChannel** auf **stable**, **extended beta** oder **dev** einstellen. Die Binärprogramme der Beta-, Entwickler- und Canary-Version sind auf die jeweiligen Versionen beschränkt.

Strategien für die Updateverwaltung

Am sichersten ist es, automatische Updates zu aktivieren. Damit wird Chrome über Google Update aktualisiert, sobald eine neue Version verfügbar ist. In einigen Fällen müssen Sie jedoch genauer kontrollieren, welche Chrome-Version die Nutzer in einer bestimmten Organisationseinheit verwenden. Mit Chrome können Sie das richtige Maß an Kontrolle und Transparenz für Ihre Umgebung konfigurieren. Sie haben dafür verschiedene Möglichkeiten, die sich in drei Strategien für die Updateverwaltung zusammenfassen lassen:

1. [Automatische Updates: Updates werden automatisch installiert, wenn sie verfügbar sind.](#)
2. [Versionsfixierung: Sie kontrollieren, wann Updates installiert werden.](#)
3. [Ausschließlich manuelle Updates: Sie installieren Updates manuell per Push.](#)

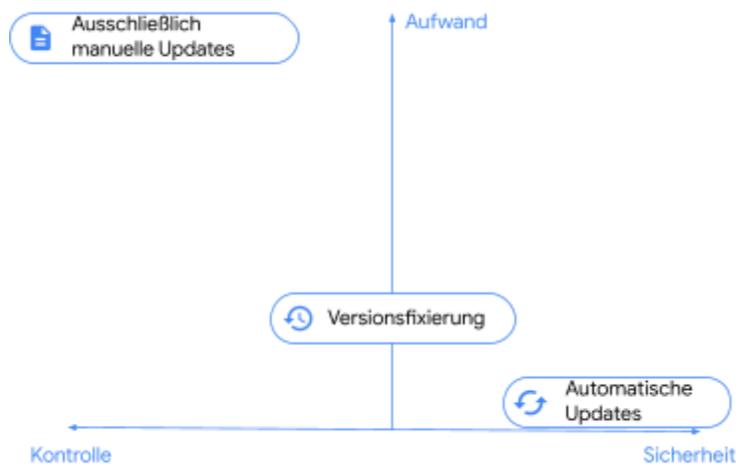


Abb. 2: Vergleich der Strategien für die Updateverwaltung

Die meisten Unternehmen kombinieren mehrere Strategien, wobei für den Großteil der Nutzer automatische Updates und für kleine Nutzergruppen je nach Bedarf eine andere Strategie verwendet wird. Welche Strategie Sie für eine bestimmte Nutzergruppe wählen, hängt davon ab, welches Maß an Kontrolle Sie für deren Browser benötigen und welche Kompromisse Sie bei der Sicherheit ihrer Umgebungen eingehen können.

Strategie 1: Automatische Updates (verfügbare Updates werden automatisch installiert)

Am sichersten ist es, automatische Updates für den Großteil der Browser zu aktivieren. Bei dieser Einstellung wird Chrome über Google Update aktualisiert, sobald eine neue Version verfügbar ist. So können Sie sicher sein, dass alle Nutzer wichtige Sicherheitsupdates und neue Funktionen ohne Verzögerung erhalten.

Vorteile	Nachteile
<ul style="list-style-type: none">• Dies ist die empfohlene Best Practice, die auch von Google intern verwendet wird.• Die Nutzer erhalten wichtige Sicherheitsupdates und neue Funktionen, sobald sie verfügbar sind.• Die Versionen und Sicherheitspatches müssen nicht manuell bereitgestellt oder zentral verwaltet werden. Der Browser wird automatisch aktualisiert.• Das Risiko von Abstürzen und Sicherheitslücken wird minimiert.• Die Nutzer verwenden immer eine unterstützte Version von Chrome.• Mit der Betaversion können Sie neue Funktionen bis zu vier Wochen vor der Veröffentlichung in der stabilen Version testen.• Mit der erweiterten stabilen Version haben Sie noch mehr Zeit für Ihre Tests.	<ul style="list-style-type: none">• Änderungsmanagement: Testzyklen, die länger als acht Wochen sind, werden nicht unterstützt.• Erfordert eine enge Zusammenarbeit zwischen IT-Mitarbeitern und App-Inhabern, um die fortlaufende Kompatibilität sicherzustellen.

Chrome so konfigurieren, dass Updates installiert werden, sobald sie verfügbar sind

Damit Updates für die Nutzer installiert werden, sobald sie verfügbar sind, müssen Sie **Update policy override** (Updaterrichtlinie außer Kraft setzen) auf **Always allow updates** (Updates immer zulassen) festlegen. Dann werden Updates automatisch installiert, wenn sie bei der regelmäßigen Suche nach Updates oder bei der manuellen Suche auf `chrome://settings/help` gefunden werden.

Weitere Optionen sind **Automatic silent updates only** (Nur automatische Updates im Hintergrund), mit der *nur* Updates installiert werden, die bei der regelmäßigen Suche gefunden werden, und **Manual updates only** (Nur manuelle Updates), mit der *nur* Updates installiert werden, die bei der manuellen Suche auf `chrome://settings/help` gefunden werden. Manuelle Updates können nur auf Testgeräten verwendet werden, die erst aktualisiert werden sollen, wenn der Nutzer prüft, ob Updates verfügbar sind. Hinweis: In jedem Fall besteht das Risiko, dass verfügbare Updates nicht zeitnah installiert werden, insbesondere, wenn die Nutzer dafür aktiv werden müssen.

Admin-Konsole
(nur Windows):
Seite mit Nutzer- und
Browsereinstellungen >
Chrome-Updates >
Chrome-Updates

GPO: Google >
Google Update >
Applications
(Anwendungen) >
Google Chrome >
Update policy override
(Updaterrichtlinie außer
Kraft setzen)

Mac: UpdateDefault

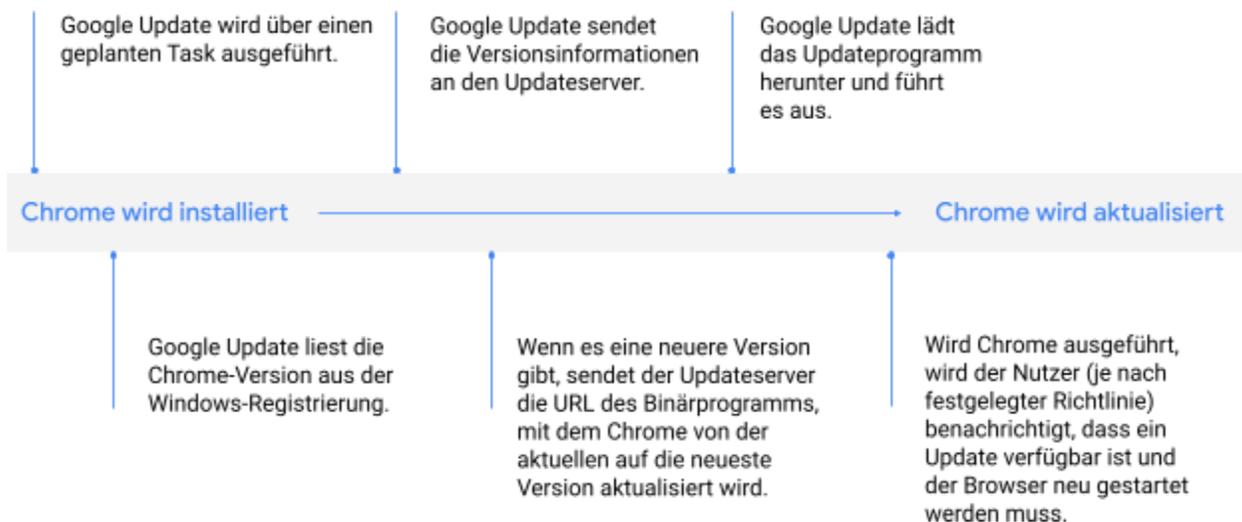


Abb. 3: So wird Chrome über Google Update automatisch aktualisiert

Zusätzliche Steuerelemente

Damit Ihre Nutzer optimal von allen Updates profitieren, sobald sie verfügbar sind, muss das Framework für Chrome-Varianten aktiviert sein. So ermöglichen Sie Updates über Varianten zwischen den Versionen. Hierfür muss [ChromeVariations](#) auf **Chrome-Varianten aktivieren** gesetzt sein. Mit den Richtlinien für Neustart-Benachrichtigungen können Sie außerdem die Versionsakzeptanz beschleunigen.

Strategie 2: Versionsfixierung (Sie legen fest, wann Updates installiert werden)

Einige Unternehmen sind an strenger kontrollierte Prozesse gebunden, etwa aufgrund von geschäftlichen Vorgaben oder Anforderungen älterer Systeme. Diese Prozesse dauern unter Umständen länger als acht Wochen. Es kann auch sein, dass bestimmte Nutzergruppen eine Umgebung benötigen, bei sich an den verwendeten Funktionen über einen festen Zeitraum hinweg nichts ändert. Für diese Nutzer können Sie eine bestimmte Chrome-Version festlegen, bis die Voraussetzungen zur Installation einer neuen Version gegeben sind.

Sie können Google Update über eine Richtlinie so konfigurieren, dass die Nutzer in einer Organisationseinheit an eine bestimmte Chrome-Version gebunden werden, bis sie für ein Update bereit sind. Dabei müssen Sie Chrome nicht manuell bereitstellen.

Admin-Konsole
(nur Windows):
Seite mit Nutzer- und
Browsereinstellungen >
Chrome-Varianten >
Varianten

GPO: Google >
Google Chrome >
Determine the availability of
variations (Die Verfügbarkeit
von Varianten bestimmen)

Mac: ChromeVariations

Vorteile	Nachteile
<ul style="list-style-type: none">• Änderungsmanagement: Diese Strategie ermöglicht Testzyklen, die länger als acht Wochen sind.• Der manuelle Aufwand ist minimal.• Dies ist eine gute Möglichkeit, wenn in Ihrem Unternehmen eine kleine Gruppe von Nutzern eine bestimmte Chrome-Version benötigt.	<ul style="list-style-type: none">• Ältere Versionen haben möglicherweise wichtige Fehlerkorrekturen nicht und werden nicht unterstützt.

Chrome so konfigurieren, dass Updates installiert werden, wenn die Voraussetzungen stimmen

Wenn Sie Nutzer in einer Organisationseinheit auf eine bestimmte Chrome-Version festlegen möchten, setzen Sie das **Präfix der Zielversion** auf die von Ihnen geprüfte und getestete Hauptversion. Bei Chrome 80 wäre das beispielsweise **80**. (einschließlich des Dezimalpunkts). Wenn Sie diese Möglichkeit nutzen, [abonnieren](#) Sie auch die [Chrome Enterprise-Versionshinweise](#).

Hinweis: Bei der Versionsfixierung auf eine Hauptversion erhalten die Nutzer weiterhin kleinere Updates, einschließlich Sicherheitspatches. Sie können Nutzer auch auf eine spezifische Version (z. B. **80.0.3987.158**) festlegen. Das wird jedoch nicht empfohlen, da die Nutzer dann *keine* Updates oder Sicherheitspatches mehr erhalten.

Die Versionsfixierung – auch auf Hauptversionen – über einen längeren Zeitraum ist nicht empfehlenswert, da wichtige Sicherheitsupdates dann möglicherweise nicht installiert werden und die Chrome-Version vom [Support für Google Chrome für Unternehmen](#) nicht mehr unterstützt wird.

Wenn eine neue Version verfügbar ist, entscheiden Sie anhand der Versionshinweise, welche Tests erforderlich sind, und beginnen Sie mit der Prüfung. Wie bereits erwähnt, können Sie die nächste Hauptversion in der Betaversion bis zu vier Wochen lang testen, bevor sie in der stabilen Version veröffentlicht wird. Ändern Sie das Präfix für die Zielversion anschließend auf die aktuelle geprüfte Version oder entfernen Sie es, sodass die Nutzer ihre Browser auf die neueste Chrome-Version aktualisieren können.

Falls Sie sich für die Fixierung auf eine neue Version entscheiden, beachten Sie bitte diesen Hinweis: Neue Versionen werden über einen bestimmten Zeitraum nach und nach veröffentlicht, sodass die Nutzer die neue Version möglicherweise erst erhalten, wenn sie vollständig eingeführt wurde. Siehe auch [Werden alle Browser auf einmal aktualisiert?](#) weiter unten.

Admin-Konsole
(nur Windows):
Seite mit Nutzer- und
Browsereinstellungen >
Chrome-Updates >
Präfix der Zielversion

GPO: Google >
Google Update >
Applications
(Anwendungen) >
Google Chrome >
Target version prefix
override (Präfix der
Zielversion überschreiben)

Mac: TargetVersionPrefix

Zusätzliche Steuerelemente

Wenn Sie noch mehr Kontrolle darüber benötigen, welche Chrome-Version eine bestimmte Nutzergruppe in Ihrem Unternehmen verwendet, können Sie [ChromeVariations](#) auf **Nur Variationen für wichtige Fehlerbehebungen aktivieren** einstellen. So erhalten diese Nutzer wichtige Fehlerkorrekturen, die über das Framework für Chrome-Varianten eingeführt wurden. Nicht essenzielle neue Funktionen erhalten die Nutzer aber erst, wenn Sie die Fixierung aufheben oder eine neuere Version auswählen.

Sie können Chrome-Varianten auch komplett deaktivieren, indem Sie für [ChromeVariations](#) die Option **Varianten deaktivieren** auswählen. Dies wird jedoch **nicht empfohlen** und sollte nur vorübergehend in Umgebungen verwendet werden, in denen die Stabilität Vorrang vor der Sicherheit hat. Mit den Richtlinien für Neustart-Benachrichtigungen können Sie außerdem die Versionsakzeptanz beschleunigen.

Admin-Konsole
(nur Windows):
Seite mit Nutzer- und
Browsereinstellungen >
Chrome-Varianten >
Varianten

GPO: Google >
Google Chrome >
Determine the availability of
variations (Die Verfügbarkeit
von Varianten bestimmen)

Mac: ChromeVariations

Strategie 3: Ausschließlich manuelle Updates (Sie installieren Updates manuell per Push)

Einige Unternehmen verwenden Chrome in extrem eingeschränkten Umgebungen, die keine Internetverbindung haben und in denen der Browser nur für interne Web-Apps verwendet wird. In solchen Szenarien können Sie Google Update nicht verwenden, um Chrome zu aktualisieren, sondern müssen jedes Mal per Push eine neue MSI-Datei bereitstellen.

Ausschließlich manuelle Updates sind zwar manchmal aus Compliancegründen notwendig, sollten aufgrund der damit verbundenen Risiken aber möglichst auf ein Minimum an Nutzern beschränkt werden. Ohne automatische Updates besteht das Risiko, dass wichtige Fehlerkorrekturen nicht angewendet werden. So kann es in Ihrer Umgebung zu Sicherheitslücken kommen. Alle Updates zeitnah manuell auszuführen ist extrem aufwendig. Dasselbe gilt für erforderliche Rollbacks. Hinzu kommt auch hier, dass ältere Chrome-Versionen vom Support für Google Chrome für Unternehmen möglicherweise nicht abgedeckt werden, falls Probleme auftreten.

Hinweis: Selbst bei diesem Ansatz müssen Sie Chrome nicht deinstallieren, bevor Sie eine neue Version installieren. Verteilen Sie die neue MSI-Datei einfach per Push auf alle Geräte, die Sie aktualisieren möchten.

Vorteile	Nachteile
<ul style="list-style-type: none">• Änderungsmanagement: Diese Strategie ermöglicht Testzyklen, die länger als acht Wochen sind.• Es ist keine Internetverbindung erforderlich.	<ul style="list-style-type: none">• Der manuelle Aufwand ist sehr hoch.• Sicherheitsupdates und Fehlerkorrekturen werden nicht automatisch installiert.• Ältere Versionen werden vom Support unter Umständen nicht mehr abgedeckt.• Rollbacks sind nur möglich, wenn die entsprechenden MSI-Dateien noch verfügbar sind.

Weitere Überlegungen

Mit begrenzter Bandbreite arbeiten

Wenn in Umgebungen mit begrenzter Bandbreite alle Browser gleichzeitig aktualisiert werden, kann es zu einer Netzwerküberlastung kommen, sodass es nicht mehr möglich ist, produktiv zu arbeiten. Solche Szenarien können Sie vermeiden, indem Sie in Google Update für Chrome (und andere darüber verwaltete Software) Wartungszeitfenster planen. Sie haben auch die Möglichkeit, Updates über einen Zeitraum zu verteilen oder im Cache zu speichern.

Wartungszeitfenster einrichten

Mithilfe von Wartungszeitfenstern sorgen Sie dafür, dass Chrome außerhalb der Geschäftszeiten aktualisiert wird, um Unterbrechungen für die Nutzer zu vermeiden. Sie können Zeiten angeben, in denen Chrome *nicht* automatisch aktualisiert werden soll. Dazu geben Sie an, **zu welchen Tageszeiten die Suche nach automatischen Updates unterbunden werden soll**, die Zeit (in **Stunden** und **Minuten**), zu der Updates unterdrückt und **wie lange** (in Minuten) sie zurückgehalten werden sollen. Hinweis: Die Einträge basieren auf der lokalen Uhrzeit des Computers und müssen im 24-Stunden-Format angegeben werden.

Updates verteilen

Sie können die Updates in Umgebungen mit begrenzter Bandbreite auch verteilt installieren, sodass nicht alle Browser auf einmal aktualisiert werden. Hierzu legen Sie einen benutzerdefinierten Zeitraum zwischen Updateüberprüfungen fest, sodass die Updates mit einer entsprechenden Verzögerung installiert werden. Hinweis: Durch diese Vorgehensweise wird zwar die Spitzenauslastung reduziert, die Bandbreitennutzung insgesamt kann sich aber trotzdem erhöhen.

Für verteilte Updates aktivieren Sie **Auto-update check period override** (Intervall der automatischen Updateüberprüfungen außer Kraft setzen) und geben Sie im Feld **Minutes between update checks** (Minuten zwischen Updateüberprüfungen) eine Zahl zwischen 1 und 43.200 ein.

Admin-Konsole (nur Windows):

- Seite mit Nutzer- und Browsereinstellungen > Chrome-Updates > Suche nach automatischen Updates unterdrücken

GPO:

- Google > Google Update > Preferences (Einstellungen) > Time period in each day to suppress auto-update check (Täglicher Zeitraum, an dem die Suche nach automatischen Updates unterdrückt werden soll)

Mac:

- UpdatesSuppressedStartHour
- UpdatesSuppressedStartMin
- UpdatesSuppressedDurationMin

Admin-Konsole (nur Windows):

- Seite mit Nutzer- und Browsereinstellungen > Chrome-Updates > Häufigkeit, mit der nach automatischen Updates gesucht wird

GPO:

- Google > Google Update > Preferences (Einstellungen) > Auto-update check period override (Intervall der automatischen Updateüberprüfungen außer Kraft setzen)

Mac: noch nicht verfügbar

Updates im Cache speichern

Chrome-Updates lassen sich auch im Cache der meisten Proxyserver mit webbasiertem Caching speichern. Wenn Sie den Google Update-Server anweisen möchten, Chrome-Updates über eine URL zu senden, die sich einfacher im Cache eines Proxyservers speichern lässt, setzen Sie **Download URL class override** (Download-URL-Klasse außer Kraft setzen) auf **Cacheable download URLs** (Im Cache speicherbare Download-URLs).

Wenn beim Speichern von Chrome-Updates im Cache des Proxyservers weiterhin Probleme auftreten, versuchen Sie es mit den folgenden Einstellungen:

- **Maximum file object size** (Maximale Größe für Dateiobjekte): Geben Sie hier mindestens 1 GB an.
- **Cache directory size** (Verzeichnisgröße des Cache): Es muss ausreichend Speicherplatz vorhanden sein, entweder im Arbeitsspeicher (schneller) oder auf der Festplatte.
- **URL settings** (URL-Einstellungen): Konfigurieren Sie eine höhere Priorität für **dl.google.com/*** und **www.google.com/dl/***.
- **Maximum object size in memory** (Maximale Objektgröße im Arbeitsspeicher): beispielsweise 2.000 KB.
- **Cache space on disk** (Speicherplatz im Festplatten-Cache): Bei einer großen Festplatte (mehr als 30 GB) können Sie einen höheren Wert angeben, um mehr Objekte zu speichern.

Mit einem Cache lassen sich in Umgebungen mit begrenzter Bandbreite oder langsamer Verbindungsgeschwindigkeit bessere Reaktionszeiten erzielen. Außerdem sparen Sie Bandbreite für wichtigere Aufgaben.

Admin-Konsole (nur Windows):

- Seite mit Nutzer- und Browsereinstellungen > Chrome-Updates > Im Cache speicherbare URLs

GPO:

- Google > Google Update > Preferences (Einstellungen) > Download URL class override (Download-URL-Klasse außer Kraft setzen)

Mac:

- DownloadPreference

Umgang mit Programmfehlern und Kompatibilitätsproblemen

Wenn Sie in einer bestimmten Chrome-Version ein Problem entdecken, stellen Sie eine Supportanfrage oder [melden Sie einen Fehler](#). Anschließend müssen Sie logischerweise alle Browser aktualisieren, damit alle Nutzer von der Fehlerkorrektur profitieren.

In der Admin-Konsole können Sie auf der Seite [Versionsverlauf](#) sehen, ob alle Nutzer das Update erhalten haben. Hier sehen Sie alle Chrome-Browser und alle Chrome OS-Versionen, die auf den Geräten in Ihrem Pool verwendet werden, zusammengefasst in einer Übersicht. Außerdem haben Sie die Möglichkeit, nach der letzten Aktivität zu filtern.

Neustart-Benachrichtigungen

Wenn ein Browser, auf dem das Update installiert werden sollte, noch eine ältere Version aufweist, muss er vielleicht neu gestartet werden. Sie können Ihre Nutzer daran erinnern, Chrome neu zu starten, indem Sie [RelaunchNotification](#) auf **Recommended** (Empfohlen) setzen und mit [RelaunchNotificationPeriod](#) ein Zeitintervall für die Benachrichtigungen angeben. Die Standardeinstellung ist eine Woche, der Mindestwert eine Stunde.

Sie können einen Neustart aber auch erzwingen. Dazu setzen Sie [RelaunchNotification](#) auf **Required** (Erforderlich) und geben mit [RelaunchNotificationPeriod](#) die Zeit bis zum Neustart ein. Der Mindestwert ist eine Stunde (3.600.000 Millisekunden) und die Standardeinstellung eine Woche (168 Stunden oder 604.800.000 Millisekunden). Hinweis: In der Admin-Konsole wird das Zeitintervall bis zum Neustart in Stunden statt Millisekunden angegeben.

Rollback

In seltenen Fällen ist ein Rollback auf eine frühere Chrome-Version durchzuführen, während Sie auf eine Fehlerkorrektur warten. Dazu setzen Sie das **Präfix der Zielversion** auf die Version, zu der Sie zurückkehren möchten. Das sollte auf jeden Fall die neueste Version sein, die in Ihrer Umgebung wie erwartet funktioniert. Damit der Rollback ausgeführt wird, müssen Sie außerdem **Rollback auf die Zielversion** aktivieren.

Admin-Konsole (nur Windows):

- Seite mit Nutzer- und Browsereinstellungen > Chrome-Updates > Benachrichtigungen bei Neustart
- Seite mit Nutzer- und Browsereinstellungen > Chrome-Updates > Zeitraum

GPO:

- Google > Google Chrome > Notify a user that a browser relaunch or device restart is recommended or required (Nutzer benachrichtigen, dass ein Neustart des Browsers empfohlen wird oder erforderlich ist)
- Google > Google Chrome > Set the time period for update notifications (Zeitraum für Updatebenachrichtigungen festlegen)

Mac:

- RelaunchNotification
- RelaunchNotificationPeriod

Admin-Konsole (nur Windows):

- Seite mit Nutzer- und Browsereinstellungen > Chrome-Updates > Präfix der Zielversion
- Seite mit Nutzer- und Browsereinstellungen > Chrome-Updates > Zielversion wiederherstellen

GPO:

- Google > Google Update > Applications (Anwendungen) > Google Chrome > Target version prefix override (Präfix der Zielversion überschreiben)
- Google > Google Update > Applications (Anwendungen) > Google Chrome > Rollback to Target version (Rollback auf die Zielversion)

Mac:

- TargetVersionPrefix
- RollbackToTargetVersion

[In diesem Hilfeartikel](#) finden Sie Informationen darüber, wie Nutzer ihre Browserinformationen behalten. Bei älteren Chrome-Versionen (vor 84) benötigen die Nutzer dafür die **Chrome-Synchronisierung**.

Für ein automatisches Rollback müssen automatische Updates über Google Update aktiviert sein. Außerdem muss das Gerät einer Domain angehören und/oder der Browser muss in der Chrome-Verwaltung über die Cloud registriert sein. Ein Rollback ist nur auf eine der letzten drei Chrome-Versionen möglich. Für Browser, die manuell aktualisiert werden oder auf eine ältere Version zurückgesetzt werden müssen, ist ein [manuelles Downgrade](#) erforderlich.

Varianten deaktivieren

Wenn es aufgrund einer über das Framework für Chrome-Varianten aktivierten Funktion zu einer Inkompatibilität kommt, können Sie als Notfallmaßnahme [ChromeVariations](#) auf **Nur Variationen für wichtige Fehlerbehebungen aktivieren** oder auf **Varianten deaktivieren** setzen. Letzteres wird jedoch nicht empfohlen. Funktionen, die über das Framework für Varianten aktiviert wurden, werden dann nach einem Neustart von Chrome deaktiviert.

Updates für Komponenten deaktivieren

Chrome hat Komponenten, bei denen es sich um wichtige Code-Elemente handelt, die möglicherweise dynamisch aktualisiert werden müssen. Normalerweise werden Komponenten nur bei einem schwerwiegenden Problem außerhalb des regulären Release-Zyklus aktualisiert. Als Notfallmaßnahme können Sie [ComponentUpdatesEnabled](#) deaktivieren, dies wird jedoch nicht empfohlen.

Admin-Konsole

(nur Windows):
Seite mit Nutzer- und
Browsereinstellungen >
Chrome-Varianten >
Varianten

GPO: Google >
Google Chrome > Determine
the availability of variations
(Die Verfügbarkeit von
Varianten bestimmen)

Mac: ChromeVariations

Fehlerbehebung

Protokolldaten erfassen

Wenn bei Google Update unerwartete Probleme auftreten, sind Protokolldaten hilfreich bei der Fehlerbehebung. Außerdem sind sie nützlich, wenn Sie eine Supportanfrage stellen. Eine Anleitung dazu, wie Sie Protokolldaten erfassen, finden Sie [in der Hilfe](#).

URL-Zulassungsliste

Google Update muss Zugriff auf die URLs zur Aktualisierung von Chrome haben. Dazu fügen Sie Ihrer Zulassungsliste die entsprechenden URLs hinzu. [Eine Liste finden Sie in der Hilfe](#).

Wird Chrome auch aktualisiert, wenn der Browser nicht ausgeführt wird?

Solange das Gerät eingeschaltet ist und über eine Netzwerkverbindung verfügt sowie Google Update nicht über eine Richtlinie deaktiviert wurde, wird Chrome im Hintergrund aktualisiert, wenn ein neues Update verfügbar ist. Beim nächsten Start von Chrome wird dann die neue Version geladen. Hinweis: Bis zum Start von Chrome enthält der Versionsbericht in der Admin-Konsole möglicherweise noch die alte Version. In dem Fall können Sie nach der letzten Aktivität filtern. Dadurch werden Browser herausgefiltert, die schon längere Zeit inaktiv sind. In Tools von Drittanbietern wird die Chrome-Version nicht immer richtig angezeigt. Am besten verwenden Sie daher den Versionsbericht in der Admin-Konsole oder `chrome://version` auf dem Zielgerät.

Wenn Chrome auf Geräteebene statt auf Nutzerebene installiert wird, funktioniert das auch, wenn kein Nutzer auf dem Gerät angemeldet ist. Im Betriebssystem angemeldete Nutzer benötigen *in keinem Fall* Administratorberechtigungen für die automatische Aktualisierung von Chrome.

Werden alle Browser auf einmal aktualisiert?

Neue Chrome-Versionen werden zuerst auf einem kleinen Prozentanteil zufällig ausgewählter Browser eingeführt und dann nach und nach auf allen Browsern installiert. Es kann eine Woche oder länger dauern, bis alle Geräte in einem Pool aktualisiert wurden. Das hängt davon ab, wie schnell wir auf 100 % kommen und ob die Einführung pausiert werden muss. Hinweis: Wenn Sie eine Versionsfixierung auf die neueste Hauptversion eingerichtet haben, erhalten Ihre Nutzer die neue Version möglicherweise erst, wenn sie vollständig eingeführt wurde. Sie können das jedoch umgehen, indem Sie Chrome auf eine vollständig angegebene Nebenversion festlegen. Bei der Fixierung auf eine Nebenversion müssen Sie das Präfix für die Zielversion entfernen oder aktualisieren, damit Updates installiert werden können. [Weitere Informationen finden Sie hier](#). Sie können den Versionsverlauf von Chrome auch über die [Version History API](#).

Fazit

Dies sind einige der vielen Möglichkeiten von Chrome, mit denen Sie für Ihre Umgebung das richtige Maß an Kontrolle und Transparenz konfigurieren können. Mit den hier beschriebenen Steuerelementen lassen sich Sicherheit und Stabilität entsprechend den Anforderungen der Nutzer einstellen. Für die meisten Szenarien empfehlen wir Folgendes:

- Aktivieren Sie automatische Updates über Google Update.
- Lassen Sie Chrome-Varianten aktiviert.
- Testen Sie anstehende Releases in der Betaversion.
- Abonnieren Sie die Chrome Enterprise-Versionshinweise.

Weitere Informationen

- [Technischer Leitfaden zur Chrome-Verwaltung über die Cloud](#): Einstieg in die Chrome-Verwaltung über die Admin-Konsole
- [Technischer Leitfaden zur Verwaltung von Erweiterungen](#): Details zur Verwaltung von Erweiterungen, darunter auch Updates
- [Chrome Enterprise-Versionshinweise](#)
- [Chrome Enterprise-Downloads](#): Installationsprogramme und Richtlinienvorlagen für Chrome (einschließlich Betaversion) und Google Update
- [Monitorlose Chrome-Version](#) zum automatisierten Testen für Entwickler