Microsoft Intune (MDM) auf Android-Tablets

Sicheres DNS in Google Chrome erzwingen & andere Browser unterbinden (6/26)

Kurzfazit

Thema	Ergebnis
a) Secure DNS	Setzen: ja, per App-Konfigurationsrichtlinie für Chrome (Policies DnsOverHttpsMode + DnsOverHttpsTemplates). Überwachen: nur eingeschränkt – Intune zeigt den Bereitstellungsstatus, der effektiv wirksame Wert ist nur am Gerät via chrome://policy bzw. über separates Chrome-Reporting prüfbar.
b) Browser sperren	Zuverlässig nur bei vollständig verwalteten / dedizierten Geräten (Allowlist-Prinzip). Bei Corporate-Owned Work Profile nur app-für-app im Arbeitsprofil. Bei BYOD / persönlichem Work Profile NICHT für das persönliche Profil.

Hinweis: Bei Android hängt fast alles vom Enrollment-Typ ab (BYOD Work Profile, vollständig verwaltet „fully managed“, dediziert, oder Corporate-Owned Work Profile). Dies entscheidet besonders bei Punkt b) über den möglichen Umfang.

a) „Sicheres DNS“ (eigener Anbieter) in Chrome setzen und überwachen

Setzen – ja, das ist möglich

Google Chrome wird als Managed-Google-Play-App ausgerollt und lässt sich über eine App-Konfigurationsrichtlinie konfigurieren (Apps → App-Konfigurationsrichtlinien → Verwaltete Geräte, Configuration Designer oder JSON). Voraussetzung ist ein in Intune registriertes Android-Enterprise-Gerät.

Relevante Chrome-Richtlinien für Secure DNS (DNS-over-HTTPS):

- **DnsOverHttpsMode** – Modus des DoH-Resolvers. „secure“ sendet ausschließlich DoH-Anfragen und schlägt bei Fehlern fehl (keine Auflösung). „automatic“ versucht zuerst DoH und weicht im Fehlerfall ggf. auf unsichere Anfragen aus. Für „eigenen Anbieter erzwingen“ i. d. R. secure.
- **DnsOverHttpsTemplates** – die DoH-URL / Resolver-Vorlage deines Anbieters („Anderer Anbieter“).

Beide Richtlinien werden auf Android seit Chrome 85 unterstützt. Werden sie per Richtlinie gesetzt, können Nutzer die Secure-DNS-Einstellung im Chrome-Menü i. d. R. nicht mehr ändern (ausgegraut) – meist gewünscht.

Beispiel-Konfiguration (Configuration Designer):

Konfigurationsschlüssel	Beispielwert
`DnsOverHttpsMode`	`secure`
`DnsOverHttpsTemplates`	`https://dein-anbieter.example/dns-query`

Konkrete URL durch die DoH-Vorlage des gewählten Anbieters ersetzen.

Überwachen – nur eingeschränkt

- **Bereitstellungsstatus:** Intune zeigt den Status der App-Konfigurationsrichtlinie (zugewiesen, ausstehend, Fehler).

- **Effektiver Wert:** Intune liest den tatsächlich in Chrome wirksamen Wert NICHT zurück. Verifikation erfolgt am Gerät über chrome://policy.
- **Echtes Auditing:** Für zentrales Reporting des wirksamen Werts ist ein zusätzliches Chrome-Enterprise-/Cloud-Reporting (Chrome Browser Cloud Management) nötig.

Einschränkung: DoH in Chrome verschlüsselt nur die DNS-Anfragen von Chrome selbst – andere Apps nutzen weiter das System-DNS. Für systemweite Erzwingung ist die Android-Funktion „Privates DNS“ (auf Geräteebene via Intune) eine Alternative bzw. Ergänzung.

b) Andere Browser verhindern (Installation / Nutzung)

Der mögliche Umfang hängt entscheidend vom Enrollment-Typ ab:

Enrollment-Typ	Möglichkeit, andere Browser zu unterbinden
Vollständig verwaltet / dediziert (Corporate-Owned)	Volle Kontrolle (Allowlist-Prinzip). Standardmäßig nur vom Admin freigegebene Managed-Google-Play-Apps installierbar. „Zugriff auf alle Apps im Google Play Store zulassen“ auf Blockieren/Nicht konfiguriert lassen → nur z. B. Chrome erlaubt. Zusätzlich Sideloading aus unbekannten Quellen blockieren.
Corporate-Owned Work Profile (COPE)	Im Arbeitsprofil steuerbar; im persönlichen Profil können Nutzer grundsätzlich Browser frei installieren. Gezieltes Sperren benannter Apps per Blockliste (Deinstallationsabsicht) möglich – aber kein vollständiger Riegel.
BYOD / persönliches Work Profile	Nicht vollständig möglich. Intune verwaltet nur das Arbeitsprofil; außerhalb installierte Apps sind prinzipbedingt nicht steuerbar. Über Compliance + Conditional Access lässt sich höchstens der Zugriff auf Unternehmensressourcen sperren – keine echte Installationssperre.

Zur Formulierung „Nutzung verhindern“

Das reine Sperren des Startens einer beliebigen App bietet Android-MDM nicht generisch. Der saubere Weg ist die Installationssperre (vollständig verwaltet mit Allowlist) bzw. der Kiosk-/Dedicated-Modus, in dem das Gerät auf bestimmte freigegebene Apps beschränkt ist.

Empfehlung

- Wenn beide Ziele (DNS erzwingen UND andere Browser ausschließen) zuverlässig erreicht werden sollen: vollständig verwaltete bzw. dedizierte Geräte verwenden.
- Secure DNS über DnsOverHttpsMode = secure und DnsOverHttpsTemplates = <DoH-URL> in der Chrome-App-Konfiguration setzen.
- Nur Chrome als Managed-Google-Play-App freigeben, Play-Store-Vollzugriff und unbekannte Quellen blockieren.
- Wirksamkeit per chrome://policy auf einem Testgerät verifizieren; für fortlaufendes Auditing ggf. Chrome Browser Cloud Management ergänzen.

Stand: Juni 2026. Funktionsumfänge von Intune, Android Enterprise und Chrome können sich ändern; vor Rollout in der jeweils aktuellen Microsoft-Learn- und Chrome-Enterprise-Dokumentation prüfen.

***KI-Transparenz**: Dieser Leitfaden wurde mit Claude KI (Opus 4.8) erstellt. Bitte sichern/speichern Sie alle Einstellungen, bevor Sie Änderungen vornehmen, damit ein Rollback möglich ist.*