Private DNS (DNS-over-TLS) auf Android-Tablets

Fernkonfiguration und Überwachung mit Microsoft Intune und Samsung Knox Service Plugin

Technische Dokumentation und Rollout-Leitfaden für das IT-Team (Stand: 6/26)

Inhalt

1. Überblick und Zielsetzung

Ziel ist es, auf verwalteten Android-Tablets den Private-DNS-Eintrag (DNS-over-TLS, kurz DoT) per Fernkonfiguration zentral zu setzen, gegen Änderungen durch Endnutzer zu sperren und den Status zu überwachen. DoT verschlüsselt DNS-Anfragen über TLS auf Port 853 und verhindert damit das Mitlesen oder Manipulieren von Namensauflösungen im Netzwerkpfad.

Microsoft Intune bietet hierfür keine native Einstellung. Der unterstützte Weg auf Samsung-Geräten führt über das Knox Service Plugin (KSP), Samsungs OEMConfig-App, die als App-Konfigurationsrichtlinie in Intune ausgerollt wird. Innerhalb von KSP steuert die Funktion Deep Settings Customization den Private-DNS-Eintrag.

Wichtigster Vorbehalt: Intune kann den auf dem Gerät tatsächlich gesetzten Private-DNS-Hostnamen nicht als natives Compliance-Signal zurücklesen. Echte Wirksamkeit wird am verlässlichsten serverseitig am DoT-Resolver nachgewiesen (siehe Abschnitt 6).

2. Technische Grundlagen

2.1 Private DNS als geräteweite Einstellung

Der Private-DNS-Eintrag ist unter Android eine globale Geräteeinstellung. Sie lässt sich technisch nur über die DevicePolicyManager-Methode setGlobalPrivateDnsModeSpecifiedHost setzen, die seit API-Level 29 (Android 10) existiert. Daraus folgt eine harte Voraussetzung an die Verwaltungsform.

2.2 Voraussetzung: Device Owner

Die Tablets müssen als Device Owner registriert sein, das heißt als Fully Managed (COBO) oder Dedicated/Kiosk (COSU). Im persönlichen Arbeitsprofil (BYOD) kann der Work-Profile-DPC diese geräteweite Einstellung nicht setzen. Bei reinem Arbeitsprofil funktioniert keiner der hier beschriebenen Wege.

2.3 Betriebsmodi des Private-DNS-Eintrags

Wert	Bedeutung
`off`	Verwendet die Standard-DNS-Server des Netzwerks (keine erzwungene Verschlüsselung).
`opportunistic`	Automatik-Modus: nutzt sichere DNS-Server, sofern verfügbar, mit Fallback auf unverschlüsseltes DNS. Robuster, aber nicht erzwungen.
DoT-Hostname, z. B. `dns.google`	Strict-Modus: erzwingt verschlüsseltes DNS gegenüber dem angegebenen Resolver. Kein Fallback – ist der Resolver über Port 853 nicht erreichbar, schlägt die Namensauflösung komplett fehl.

3. Voraussetzungen im Detail

- Tablets sind als Fully Managed (COBO) oder Dedicated (COSU) registriert (Device Owner).
- Gerätemodelle erreichen **Knox 3.11 oder höher** (Voraussetzung für die Private-DNS-Steuerung über Deep Settings Customization).
- Knox Platform for Enterprise **Premium-Lizenz** vorhanden (kostenlos; nötig für Deep Settings Customization, die generell ab Knox 3.4 verfügbar ist).
- Managed Google Play ist in Intune angebunden.
- DoT-Resolver festgelegt und Hostname bekannt (z. B. dns.google, 1dot1dot1dot1.cloudflare-dns.com oder eigener Endpoint).
- DoT-Resolver über Port 853 aus allen relevanten Netzen erreichbar (Firewall, Captive-Portal-Situationen geprüft).
- Entscheidung getroffen: fester Hostname (Strict-Modus) vs. opportunistic (Automatik mit Fallback).

4. Konfiguration Schritt für Schritt

4.1 KSP-App in Intune bereitstellen

1. Intune Admin Center öffnen: Apps → Alle Apps → Hinzufügen → Verwaltete Google Play-App.
2. Knox Service Plugin suchen, genehmigen und synchronisieren.
3. KSP-App den Ziel-Tablet-Gruppen als Erforderlich (Required) zuweisen.
4. Auto-Update für die App aktivieren, um Probleme bei KSP-Schema-Updates zu vermeiden.

4.2 App-Konfigurationsrichtlinie anlegen

5. Apps → App-Konfigurationsrichtlinien → Hinzufügen → Verwaltete Geräte.
6. Plattform: Android Enterprise. Zugeordnete App: Knox Service Plugin.
7. Konfigurationsformat: Konfigurations-Designer (rendert das KSP-Schema als Formular).

4.3 Die konkreten KSP-Felder (Deep Settings Customization)

Nach Samsungs offiziellem Ablauf werden folgende Felder gesetzt:

8. Device-wide policies → **Device customization controls (Premium)** = **True**.
9. Device and Settings customization profile → **Configure values in settings menu** → neuen Eintrag hinzufügen.
10. **Name of the Setting item** = **Connections > More connection settings > Private DNS**.
11. **Set value for the setting** = **Use specified value**.
12. **Specify value** = einer der folgenden Werte (für dieses Projekt im Regelfall der DoT-Hostname):

- `off` – Standard-DNS des Netzwerks
- `opportunistic` – Automatik mit Fallback
- DoT-Hostname (z. B. `dns.google`, `1dot1dot1dot1.cloudflare-dns.com`) – fester privater Resolver (Strict-Modus)

13. **Allow end-user modification of this setting** = **False** → der Eintrag ist auf dem Gerät ausgegraut und nicht änderbar (empfohlen für eine durchgesetzte Konfiguration).
14. (Optional) **Configure to hide settings** = **True** → blendet den Menüpunkt ganz aus.

4.4 Zuweisen

- Die App-Konfigurationsrichtlinie denselben Gruppen zuweisen wie die KSP-App.
- Zuweisungslogik prüfen: Ohne installierte KSP-App greift die Konfiguration nicht.

5. Wichtige Betriebshinweise

- Strict-Modus (fester Hostname) bedeutet keinen Fallback. Ist der Resolver über Port 853 nicht erreichbar (z. B. hinter Captive Portal oder bei gesperrtem Port), schlägt die Namensauflösung komplett fehl. Wer Robustheit über Zwang stellt, wählt opportunistic.
- KSP wendet Konfigurationen teils verzögert an. Gelegentlich ist auf dem Gerät Apply Latest Configuration nötig. Beim Pilot einplanen.
- Die Knox-Version hängt an Modell und Firmware; vor Rollout je Modell verifizieren, dass Knox 3.11+ erreicht wird.
- Das KSP-Schema wird laufend erweitert. Exakte Feldbeschriftungen vor Produktivstart gegen das aktuelle Schema im Intune-Konfigurations-Designer und gegen die Samsung-Doku abgleichen.

6. Überwachung

Echtes Monitoring des gesetzten Eintrags ist nur eingeschränkt möglich. Folgende Ebenen stehen zur Verfügung:

- **Zustellstatus in Intune:** Anwendungsstatus der App-Konfiguration je Gerät (Erfolg/Fehler).
- **KSP-Feedback-Kanal:** KSP meldet einen Anwendungsstatus an die UEM zurück.
- **Knox Asset Intelligence:** sofern vorhanden, zur weitergehenden Nachverfolgung der KSP-Konfigurationen.
- **Serverseitige Verifikation (verlässlichster Wirknachweis):** am DoT-Resolver prüfen, welche Geräte/IP-Bereiche tatsächlich verschlüsselt anfragen.

Hinweis: Intune liest den real gesetzten Private-DNS-Hostnamen nicht als natives Compliance-Signal zurück. Es gibt für Android keine benutzerdefinierten Compliance-Skripte wie unter Windows.

7. Troubleshooting

Symptom	Prüfen / Maßnahme
Konfiguration greift nicht oder verzögert	KSP installiert? Auto-Update aktiv? Ggf. Apply Latest Configuration auf dem Gerät. Konflikte unter neuen Android-Versionen prüfen.
Couldn't connect / DNS schlägt fehl	Hostname korrekt? Port 853 erreichbar? Im Strict-Modus gibt es keinen Fallback – ggf. auf opportunistic wechseln.

Symptom	Prüfen / Maßnahme
Setting nicht steuerbar	Knox-Version unter 3.11? Premium-Lizenz aktiv? Enrollment wirklich Device Owner (COBO/COSU)?
Feldname weicht ab	KSP-Schema im Intune-Designer wurde aktualisiert – Pfad/Bezeichnung gegen aktuelle Samsung-Doku abgleichen.

8. Rollout-Checkliste

Phase 0 – Voraussetzungen

- ☐ Tablets als Fully Managed (COBO) oder Dedicated (COSU) registriert (Device Owner).
- ☐ Gerätemodelle erreichen Knox 3.11 oder höher.
- ☐ Knox Platform for Enterprise Premium-Lizenz vorhanden.
- ☐ Managed Google Play in Intune angebunden.
- ☐ DoT-Resolver festgelegt und Hostname bekannt.
- ☐ DoT-Resolver über Port 853 aus relevanten Netzen erreichbar.
- ☐ Entscheidung Strict-Modus vs. opportunistic getroffen.

Phase 1 – KSP-App bereitstellen

- ☐ Apps → Alle Apps → Hinzufügen → Verwaltete Google Play-App.
- ☐ Knox Service Plugin suchen, genehmigen, synchronisieren.
- ☐ KSP-App den Zielgruppen als Erforderlich zuweisen.
- ☐ Auto-Update der App aktivieren.

Phase 2 – App-Konfigurationsrichtlinie anlegen

- ☐ Apps → App-Konfigurationsrichtlinien → Hinzufügen → Verwaltete Geräte.
- ☐ Plattform Android Enterprise; zugeordnete App Knox Service Plugin.
- ☐ Konfigurationsformat: Konfigurations-Designer.
- ☐ Device customization controls (Premium) = True.
- ☐ Configure values in settings menu → Eintrag hinzufügen.
- ☐ Name of the Setting item = Connections > More connection settings > Private DNS.
- ☐ Set value = Use specified value; Specify value = DoT-Hostname (bzw. off / opportunistic).
- ☐ Allow end-user modification of this setting = False (sperren).
- ☐ Optional: Configure to hide settings = True.

Phase 3 – Zuweisung

- ☐ App-Konfigurationsrichtlinie denselben Gruppen zuweisen wie die KSP-App.
- ☐ Zuweisungslogik prüfen (ohne KSP-App keine Wirkung).

Phase 4 – Pilot

- ☐ 2–3 repräsentative Geräte-/Firmware-Stände in Pilotgruppe aufnehmen.
- ☐ Auf dem Gerät prüfen: Einstellungen → Verbindungen → Weitere Verbindungseinstellungen → Privates DNS zeigt den Hostnamen.
- ☐ Bei Sperrung: Eintrag ausgegraut / ausgeblendet.
- ☐ Wirknachweis am DoT-Resolver: Pilotgerät fragt verschlüsselt an.
- ☐ Verzögerungsverhalten von KSP testen.
- ☐ Strict-Modus gegen reale Netze testen (WLAN, Mobilfunk, Gäste-/Captive-Netze).

Phase 5 – Breiter Rollout

- ☐ Pilot-Erkenntnisse eingearbeitet.
- ☐ Stufenweise (ringbasiert) auf weitere Gruppen ausweiten.
- ☐ Statusüberwachung je Ring vor der nächsten Stufe.

Phase 6 – Überwachung

- ☐ Anwendungsstatus der App-Konfiguration je Gerät prüfen.
- ☐ KSP-Feedback-Kanal auswerten.
- ☐ Ggf. Knox-Asset-Intelligence-Integration nutzen.
- ☐ Serverseitige Verifikation am DoT-Resolver als Wirknachweis.
- ☐ Dokumentieren: Intune liest den Hostnamen nicht als Compliance-Signal zurück.

9. Wichtige Quellen

Samsung Knox – zentraler Konfigurationspunkt

- Deep Settings Customization (Private-DNS-Eintrag, Werte off / opportunistic / Hostname)
- Knox Service Plugin – Überblick (Admin)
- KSP – Mindestvoraussetzungen
- KSP – Einrichtung mit einer UEM (z. B. Intune)
- KSP – Schema-Struktur (Referenz)
- KSP – Policy-Beschreibungen (Referenz)
- KSP – Release Notes (Schema-Änderungen verfolgen)
- KSP – Entwicklerdoku zu Managed Configurations / OEMConfig

Microsoft Intune / Microsoft Learn

- Android-Einstellungsliste im Settings Catalog
- Geräteeinschränkungen für Android Enterprise (Referenz)
- Geräteeinschränkungen konfigurieren (Anleitung)

Android-Plattform-Grundlage (zugrunde liegende API)

- DevicePolicyManager.setGlobalPrivateDnsModeSpecifiedHost

DoT-Hintergrund / Resolver-Referenz

- Cloudflare – DNS over TLS (Hostnamen / Port 853)
- Cloudflare-Blog – Private DNS unter Android einrichten und verifizieren

Zur Vollständigkeit: Eine offizielle Microsoft-Learn-Seite mit einer nativen Private-DNS-Einstellung gibt es nicht – Intune bietet diese Einstellung nicht nativ an, daher der KSP-Weg. Den genauen Feldnamen bitte weiterhin gegen die erste Samsung-Quelle abgleichen, da sich das Schema ändern kann.

KI Transparenz: Dieser Leitfaden wurde mit Unterstützung durch Claude KI (Opus 4.8) erstellt. Bitte sichern/speichern Sie alle Einstellungen, bevor Sie Änderungen vornehmen, so dass Sie wieder zurückrollen können, wenn notwendig.
Stand: 04.06.2026