IT Operations & Enterprise Governance

IT Installation & Deployment Playbook

Sovereign Runtime Deployment für Microsoft Edge & Google Chrome. Stand Oktober 2026.

Extension-ID
bdhbnbpkkcageebgfabcecolflgembfe

Version
v2.6.8 (Enterprise Managed)

Bereitstellung
Silent Force-Install (Intune / GPO / Registry)

Architektur
100% lokaler RAM · Zero-Retention

1. Core Deployment Metadata

Parameter	Wert
Extension ID	`bdhbnbpkkcageebgfabcecolflgembfe`
Update URL	`https://deskgate.app/ext/updates.xml`
CRX Package	`https://deskgate.app/ext/deskgate-operator-2.6.8.crx`
Outbound Rule	HTTPS nur zu `https://deskgate.app` Port 443
Browser	Microsoft Edge, Google Chrome (Windows & macOS)

Signaturschlüssel & ID-Stabilität: Alle Releases und Updates verwenden denselben kryptografischen Signaturschlüssel. Die Extension-ID bleibt release-übergreifend stabil. Enterprise Force-Install-Policies müssen somit nur einmalig im Tenant hinterlegt werden.

2. Force-Install Konfiguration

Deployment-String für die Unternehmensrichtlinie beider Browser (Extension-ID + Update-URL):

```
bdhbnbpkkcageebgfabcecolflgembfe;https://deskgate.app/ext/updates.xml
```

Microsoft Edge (Chromium)

- **Microsoft Intune:** Settings Catalog → Microsoft Edge → Extensions → ExtensionInstallForcelist
- **Group Policy (GPO):** Computer Configuration → Administrative Templates → Microsoft Edge → Extensions → Control which extensions are installed silently
- **Windows Registry:** siehe `Edge-ForceInstall.reg`

Google Chrome

- **Google Admin Console:** Devices → Chrome → Apps & Extensions → Add by ID → From a custom URL
- **Group Policy (GPO):** Computer Configuration → Administrative Templates → Google Chrome → Extensions → Configure the list of force-installed apps and extensions
- **Windows Registry:** siehe `Chrome-ForceInstall.reg`

3. Operational Onboarding (erste 20 Minuten)

1. **Policy prüfen:** In der Browser-Adresszeile `edge://policy` oder `chrome://policy` aufrufen und auf Policies neu laden klicken. Die Richtlinie `ExtensionInstallForcelist` muss aktiv und fehlerfrei angezeigt werden.

2. **Extension bestätigen:** Die DeskGate Operator Extension (v2.6.8) erscheint als enterprise-managed und kann von Endbenutzer:innen weder deaktiviert noch deinstalliert werden.
3. **CONFIG hinterlegen:** Seitenpanel öffnen, auf **CONFIG** klicken. Endpoint `https://deskgate.app`, Desk-Code und Desk-Key eintragen. Der Schweiz-Modus ist standardmässig aktiviert.
4. **Hard-Refresh:** Alle geöffneten KIS- und Portal-Tabs mit Ctrl+F5 (bzw. Cmd+Shift+R) neu laden.
5. **Testlabor durchspielen:** Den synthetischen Testfall (Lukas Brunner / AlpaCare) durchführen.

---

4. IT-Security & Datenschutz-Einwände

Einwand / Anforderung	Architektur & Technische Antwort
Patientendaten dürfen nicht an externe KI-Modelle gesendet werden.	**100 % lokale Ausführung im flüchtigen Browser-RAM.** Im Schweiz-Modus findet keine Übermittlung medizinischer Freitexte statt. Keine Speicherung in `localStorage`, Cookies oder externen Datenbanken.
Netzwerk blockiert externe Verbindungen und WebSockets.	**Isoliertes Frontend-Tool.** Kein `eval()`, keine persistenten WebSockets. Outbound-Traffic beschränkt sich auf statuslose HTTPS-Check-ins (Port 443) zur Lizenzvalidierung.
Wie werden Nutzungsmetriken erfasst ohne Payer-IDs oder Akten preiszugeben?	**Kryptografischer SHA-256-Hash.** Die Eingangsnummer wird bereits im Browser gehasht. Der Server erhält nur Zählzeilen und Hashes. Gehostet bei der Flow Swiss AG in Baar ZG.

Datenschutz-Garantie (Art. 9 DSG): Für Schweizer Einrichtungen liegt der vollständige Auftragsbearbeitungsvertrag (Schedule CH · AVV) vor. Zur Einsicht: Schedule CH online lesen oder als PDF herunterladen.