

Field Enrollment unter G/On 5

Nutzen und Vorteile beim Einsatz des Zusatzmoduls

Vorteile für den Administrator

- **Maximale Zeitersparnis beim Rollout von Token**
Erzeugt der Administrator den Token selbst vor Ort, so reduziert sich der Aufwand um bis zu 15%, weil das Ausrollen sowie das Anlegen der Policies pro Token entfällt. Das Deployment läuft als Hintergrundprozess. Verlagert der Administrator die Tätigkeit per Field Enrollment direkt auf den einzelnen User, dann sind nur noch Autorisierung und Freischaltung notwendig, alle anderen Schritte entfallen (für den Administrator bis zu 90% Zeitersparnis).
- **Kein "Einsammeln" von Geräten**
Token und Notebooks müssen nicht mehr zentral eingesammelt / angeliefert oder vor Ort durch den Administrator ausgerollt werden. Dies reduziert Zeit, Kosten, CO₂- und Umweltbelastung durch Vermeidung unnötiger Wege. Dies ist speziell beim Einsatz von Computer User Token ein grosser Vorteil.
- **Höchste Flexibilität bei der Token-Erstellung**
Durch Field Enrollment kann das Ausrollen und Erstellen von Token immer und überall stattfinden. Das Installationspaket wird zum Beispiel einfach auf einem USB-Gerät, einem Netzwerkshare oder einem Webserver abgelegt und kann von jedem User zur Generierung seines eigenen Tokens von dort bezogen werden.
- **Reduzierung der Systemlast bei der Token-Erstellung**
Der Installationsprozess läuft automatisiert im Hintergrund am Client-PC. Die Installation erfolgt offline und ohne Kommunikation zum G/On Server, daher mit geringster Last für den Server und die Datenverbindung.
- **Vereinfachte Fehlerbehebung und automatisches Update**
Jedes Tokengerät lässt sich via Field Enrollment in einem Prozess zurücksetzen, löschen und neu verteilen. Dies ist ideal, wenn Aktualisierungen (z. B. neue G/On Releases bzw. zusätzliche Applikationsclients) verteilt werden müssen oder ein Token wieder in den Originalzustand gebracht werden soll. Dies ersetzt auch die Fehlersuche im Problemfall: Es muss keine Prüfung auf defekte Pakete, gelöschte oder beschädigte Dateien vorgenommen werden, weil das Field-Enrollment sämtliche notwendigen Pakete überinstalliert.
- **Ausfallzeiten spürbar reduzieren**
Ist ein Firmennotebook physisch defekt, kann mittels Field-Enrollment in kürzester Zeit ein Ersatzgerät für G/On ausgerollt werden. Der Anwender muss nicht auf den Zugriff verzichten, sondern kann sofort weiterarbeiten, ohne das defekte Gerät zuerst auszutauschen.
- **Eingrenzung der installierbaren Token-Typen**
Über Definitionsdateien ist vordefinierbar, welche Token-Typen installiert werden dürfen. Dies verhindert wirksam den Rollout auf unerwünschten Geräten und schützt vor Bedienungsfehlern durch den Anwender.
- **Paketprüfungen während des Rollouts**
Jedes Paket wird vor der Installation überprüft. Hierdurch ist die Datenkonsistenz sichergestellt und es werden Fehler, die beim Download entstehen können, vermieden.

Keine Kenntnis der User-Credentials notwendig

Für das Field Enrollment muss grundsätzlich weder der Benutzer angemeldet sein, noch irgend jemand Kenntnis über dessen Passworte erlangen. Führt der Administrator den Rollout komplett für den Anwender durch, kann er dies mit seinem Benutzernamen tun und anschliessend den Namen des Users aus dem Directory-Service in die entsprechende Policy ziehen.

Vorteile für den G/On-Anwender

- **Token kann selbstständig ausgerollt werden**
Ein Token für den G/On-Zugriff lässt sich jederzeit erzeugen, ohne dass sich der Anwender in das Unternehmen begeben muss. Im Fehlerfall kann der Nutzer auch unterwegs neue Software oder einen neuen Token ausrollen und direkt weiterarbeiten.
- **Höchstmögliche Geschwindigkeit bei der Token-Erstellung**
Das Field Deployment richtet den Token in einem Prozess vollständig mit allen Paketen ein. Besonders bei Tokengeräten mit CD-Partition ist dies ein grosser Performance-Vorteil.

Vorteile auf der Serverseite

- **Offline-Deployment**
Das Token-Deployment und -Enrollment findet offline (ohne Serververbindung) statt, daher reduzieren keine Downloads oder Datenübertragungen die Bandbreite während der Token-Erstellung und der Server bietet volle Performance für die G/On-Verbindungen.
- **Beliebige Anzahl gleichzeitiger Installationen**
Es gibt keine Einschränkung hinsichtlich der parallelen Enrollments. Dies ist besonders wichtig, wenn viele Anwender zeitgleich ihre Token aktualisieren bzw. ausrollen möchten.

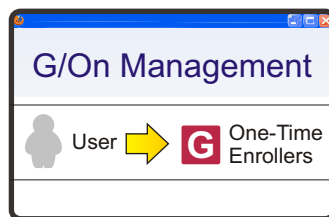
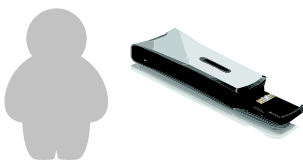
G/On 5 Field Enrollment Gegenüberstellung Vergleich mit der Token-Verteilung unter G/On 3.6

In G/On 3.6 war der Zugriff auf den G/On-Server sowie die Softwareverteilung durch Kopieren der sogenannten Identity-Datei möglich. Sie enthielt den Private Key des von G/On 3.6 verwendeten Schlüssel-paars aus Private- und Public-Signing-Key. Dieses Verfahren zur Token-Verteilung war ausschliesslich mit den Hagiwara-Token sowie dem G/On Desktop Client möglich.

G/On 5.4.x hingegen arbeitet einem RSA-2048 Private- und Public-Key pro Tokengerät und nicht pro Server. Je nach Tokengerät kommen ausserdem weitere Methoden zum Einsatz: Beispielsweise erzeugt ein Smartcard-Controller auf dem Token den Private-Key mit dem eigenen Prozessor und legt ihn im Zertifikatspeicher der Smartcard ab. Dieser Private-Key kann nie ausgelesen oder von der Smartcard ermittelt werden. Das dazugehörige Challenge-Response-Verfahren wird direkt vom G/On-Server initiiert. Ein einfacher Verbindungsaufbau vom Client mittels eines kopierten Schlüssels ist technisch und unter Sicherheitsaspekten bei G/On 5 nicht mehr möglich. Das Ausrollen der Tokengeräte erfolgt deshalb entweder durch den Administrator einzeln, manuell oder über das optionale "Field Enrollment" voll automatisch bei maximaler Zeitersparnis.

G/On 5 Field Enrollment Schema

1. Autorisierung des User für das Field Enrollment

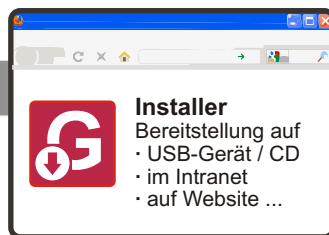


Der Anwender erhält sein Tokengerät LEER ausgehändigt oder zugesandt.

Der Administrator legt im Management eine Berechtigung an, die dem Anwender das Field-Enrollment ermöglicht.

Der Administrator kann dieses Management im Netzwerk oder über eine G/On-Verbindung durchführen.

2. Ausführen des Enrollments im Feld



Der Administrator stellt dem Nutzer das Installationspaket bereit (lokal auf Datenträgern, im Intranet, im Web).

Der Anwender startet den Installer. Der Token wird offline mit dem G/On-Client und allen im Paket enthaltenen Anwendungen vorbereitet.

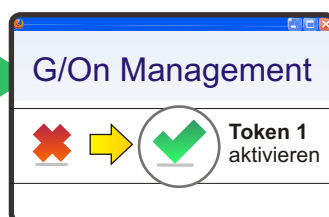
Anschließend startet das Field-Enrollment.

3. Token wird ausgerollt und am G/On-Server bekannt gemacht



Beim Enrollment teilt der Token dem G/On-Server seine Token-Information mit und speichert sie in der G/On-Datenbank. Dann wird der Private und Public Key (RSA 2048) auf der Smartcard erzeugt und der Public Key zum G/On-Server übertragen. Bei Tokengeräten ohne eigenen Prozessor werden diese Keys über den Systemprozessor berechnet. Gleichzeitig entfernt G/On den Anwender aus der Liste der "One-Time-Enrollers". Nun wird das Personal Token Assignment durchgeführt. In einer Policy erfolgt die Zuweisung des neu angelegte Token zum authentifizierten User. Der ausgerollte Token wird normalerweise nicht automatisch aktiviert, sondern wartet auf eine Prüfung und Freigabe durch den Administrator.

4. Aktivierung des ausgerollten Tokens durch den Administrator



Der Administrator kontrolliert im zentralen G/On Management, ob der Anwender seinen Token entsprechend der Policy ausgerollt hat.

Abhängig von der Voreinstellung des G/On-Servers ist der Token dann entweder sofort verwendbar oder wird vom Administrator aktiviert.