Best Practices - WatchGuard AuthPoint - Active Directory / LDAP Integration

Thomas Fleischmann

Senior Sales Engineer, Central Europe
Thomas.Fleischmann@watchguard.com

Agenda

- Kurz – Was ist WatchGuard AuthPoint?

- Beschreibung des Konzept
  - Synchronisation mit LDAP / AD
  - AuthPoint Gateway
  - External Identities

- Live Demo

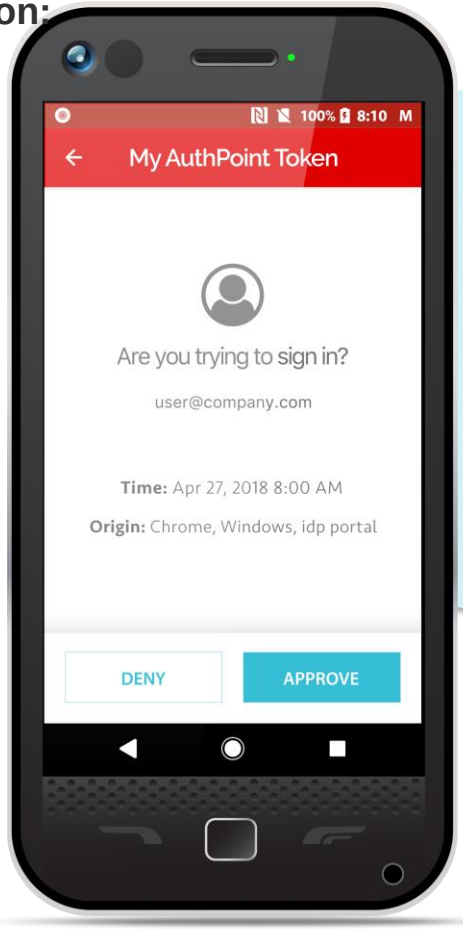
Was ist WatchGuard AuthPoint?

Was ist Multi-Faktor-Authentifizierung?

Verwendung von 2 oder mehr Authentifizierungsfaktoren von:

- **Etwas, das du kennst** (Passwort, PIN)
- **Etwas, das du hast** (Token, Handy)
- **Etwas, was du bist** (Fingerabdruck, Gesicht)

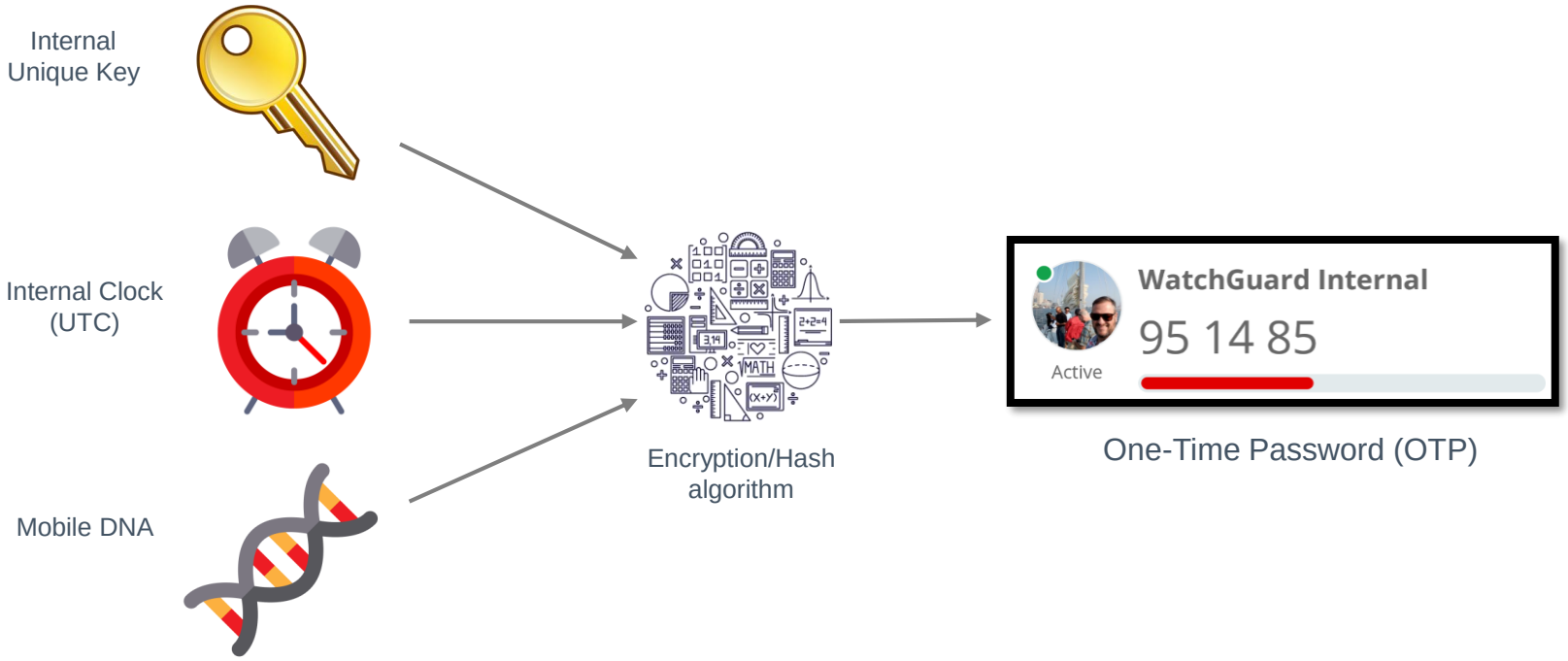
Password



AuthPoint-Faktoren:

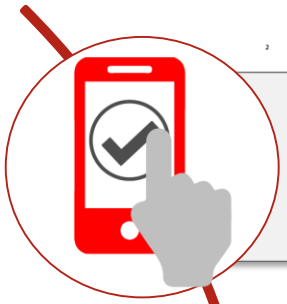
1. **Ihr Passwort**
2. **Genehmigung für Ihren mobilen Authentifikator**
3. **Korrekte Handy-DNA**
4. **Ein Fingerabdruck für den Zugriff (**mit bestimmten Telefonmodellen**)**

Erweiterte Sicherheit mit Handy-DNA



Macht den Authentifikator noch einzigartiger!

WatchGuard AuthPoint - MFA Das ist **wirklich** einfach



Multi-Factor Authentication

Password | Push Message | Phone Biometrics | Mobile Phone DNA

AuthPoint Mobile App

iOS & Android | 11 Sprachen | OTP | QR Code | Multiple Authenticators

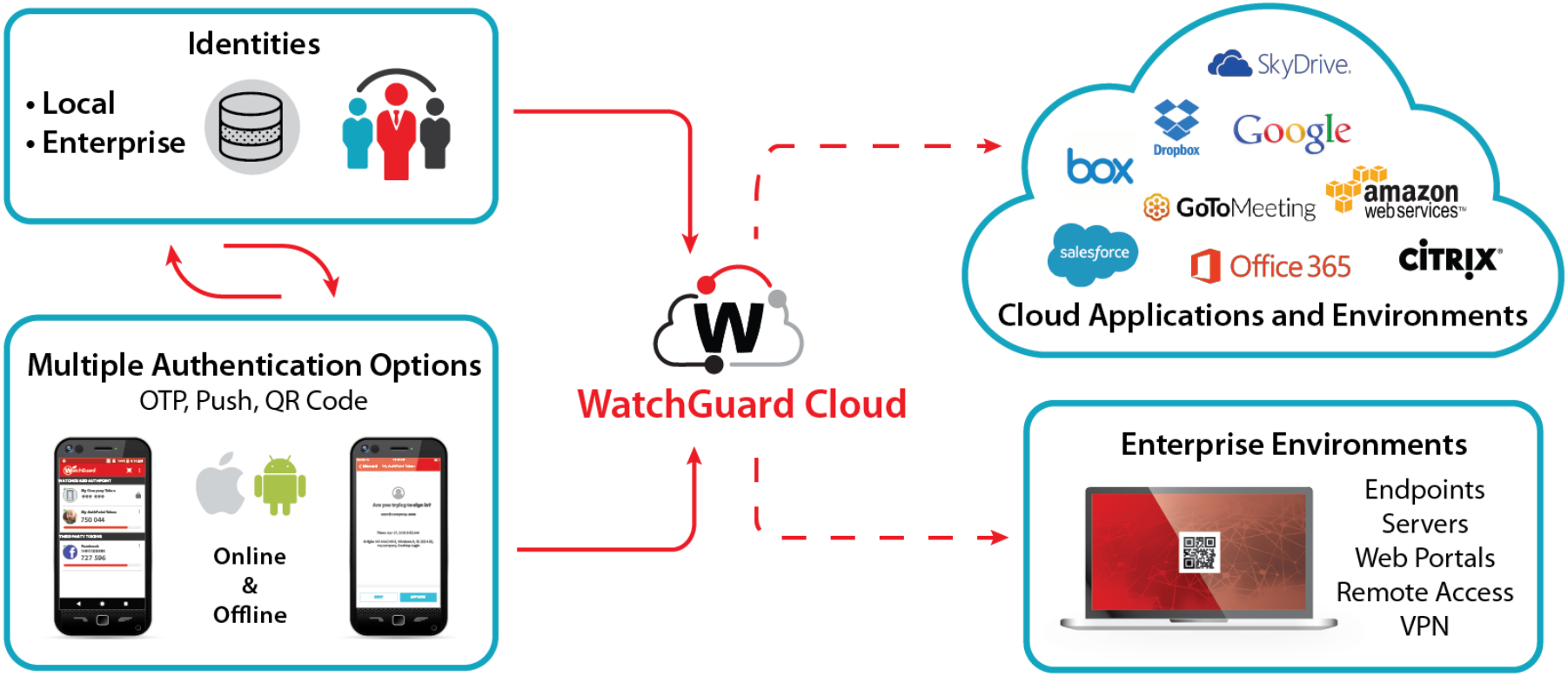
WatchGuard Cloud

Visibility | Configuration | Management | Token-Zuweisung in Sekunden

Umfangreiche MFA-Abdeckung

Dutzende von 3rd Party Integrationen | Web SSO | Windows/Mac Computer Logon

Schützt VPNs, Web Apps, PC-Anmeldung und mehr!



Beschreibung des Konzept

Synchronisation mit LDAP / AD

- WatchGuard AuthPoint bietet den Administrator die Möglichkeit, seine interne Benutzerdatenbank zu verwenden.
  - Unterstützt werden LDAP- und AD Benutzerdatenbanken.

Synchronisation mit LDAP / AD

- Dazu verwendet WatchGuard AuthPoint ein Softwarepaket, welches auf einen DC- oder Member-Server der Domäne installiert werden muss.

- Voraussetzung im Bereich Software und Betriebssystem sind aktuell:
  - Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016
  - Java (Version JRE 8u162 oder neuer)

Synchronisation mit LDAP / AD

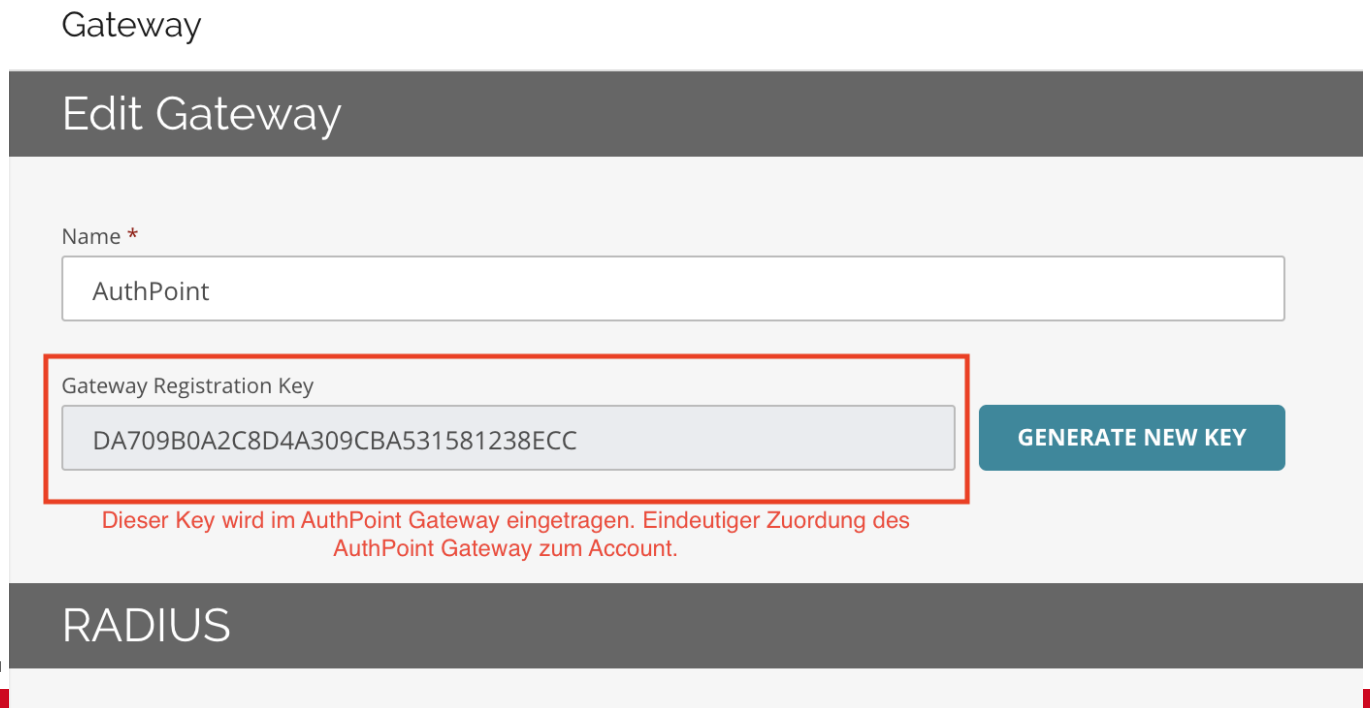
- Das WatchGuard AuthPoint Gateway installiert und konfiguriert zurzeit 4 Dienste:
  - WatchGuard AuthPoint Gateway
  - WatchGuard AuthPoint LDAP
  - WatchGuard AuthPoint RADIUS
  - WatchGuard AuthPoint ADFS (zurzeit Beta)

- Es existiert keine grafische Oberfläche für die Dienste.

AuthPointADFS	5640	WatchGuard AuthPoint ADFS	Wird ausgeführt
AuthPointGateway	5672	WatchGuard AuthPoint Gateway	Wird ausgeführt
AuthpointLDAP	5988	WatchGuard AuthPoint LDAP	Wird ausgeführt
AuthPointRadius	3304	WatchGuard AuthPoint RADIUS	Wird ausgeführt

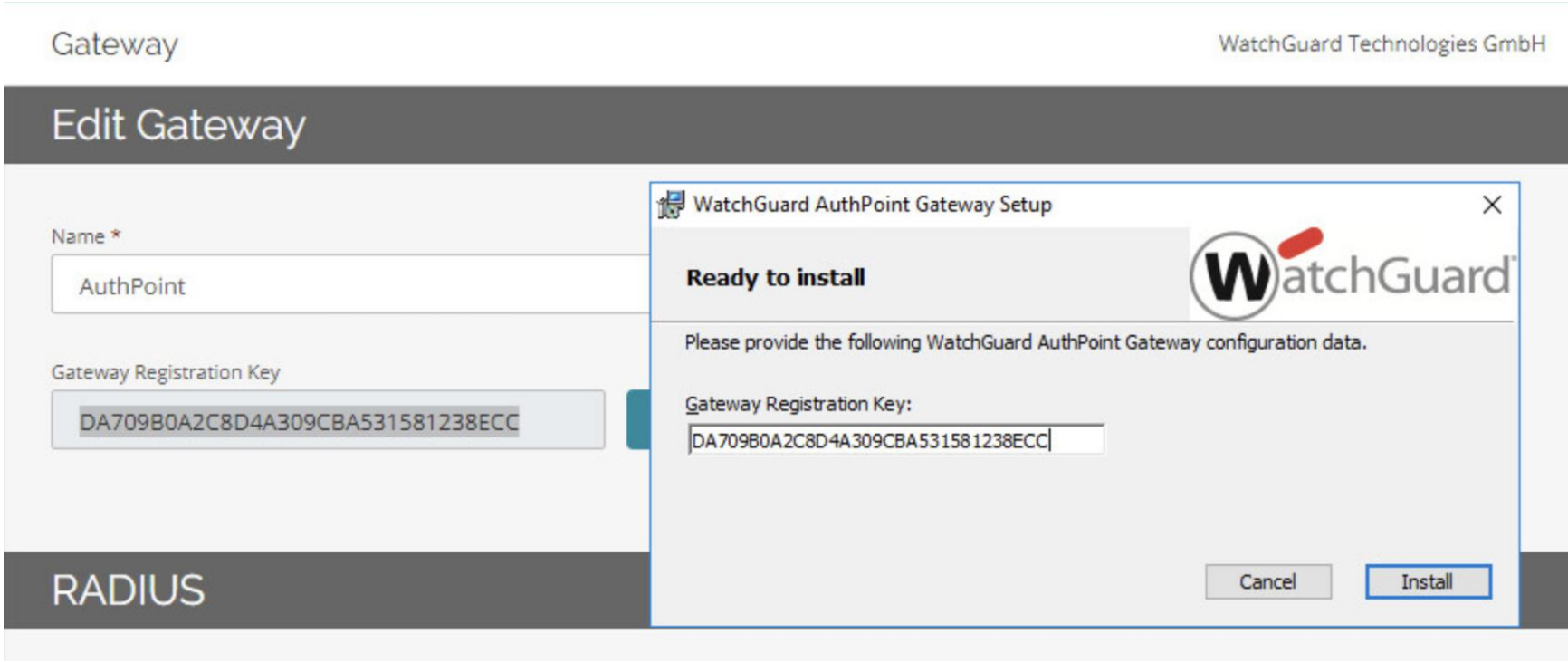
Synchronisation mit LDAP / AD

- Bei der Konfiguration des Gateways in der WatchGuard Cloud wir beim Anlegen des selbigen ein *Gateway Registration Key* erzeugt.
- Dieser kann nur einmal verwendet werden !



Synchronisation mit LDAP / AD

- Bei der Installation des Gateways auf einen Rechner wird der *Gateway Registration Key* als einzige Information eingetragen.



Synchronisation mit LDAP / AD

- Um eine Synchronisation mit den LDAP / AD herzustellen, muss in der WatchGuard Cloud im Bereich *External Identities* die Verbindung mit der Domäne eingerichtet werden.

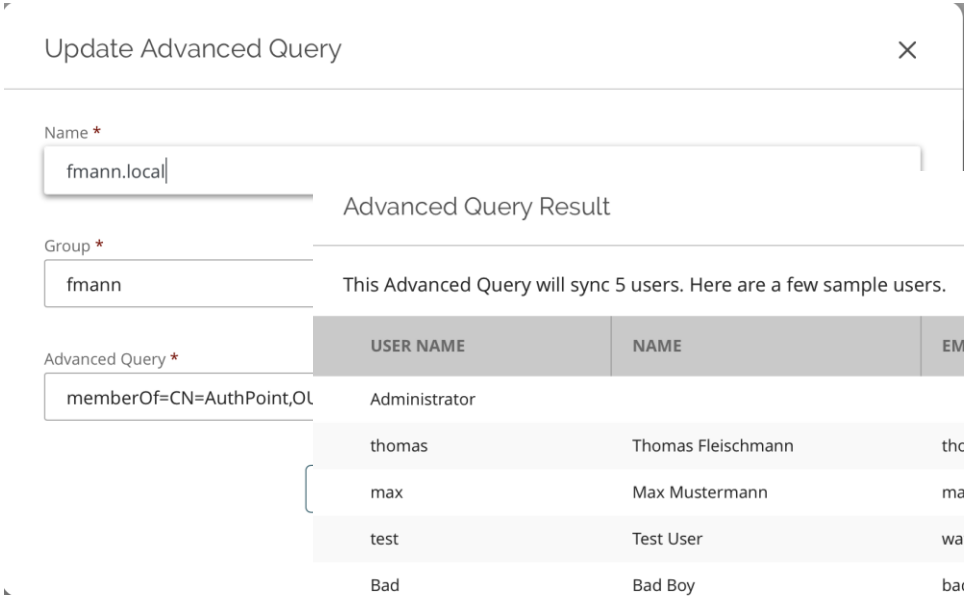
- Der *System User* muss lesende Zugriff auf das LDAP / AD haben. Es muss nicht ein Administrator sein!

- Die Verbindung kann auch per LDAPS erfolgen.

- Die Verbindung kann durch *Check Connection* überprüft werden.

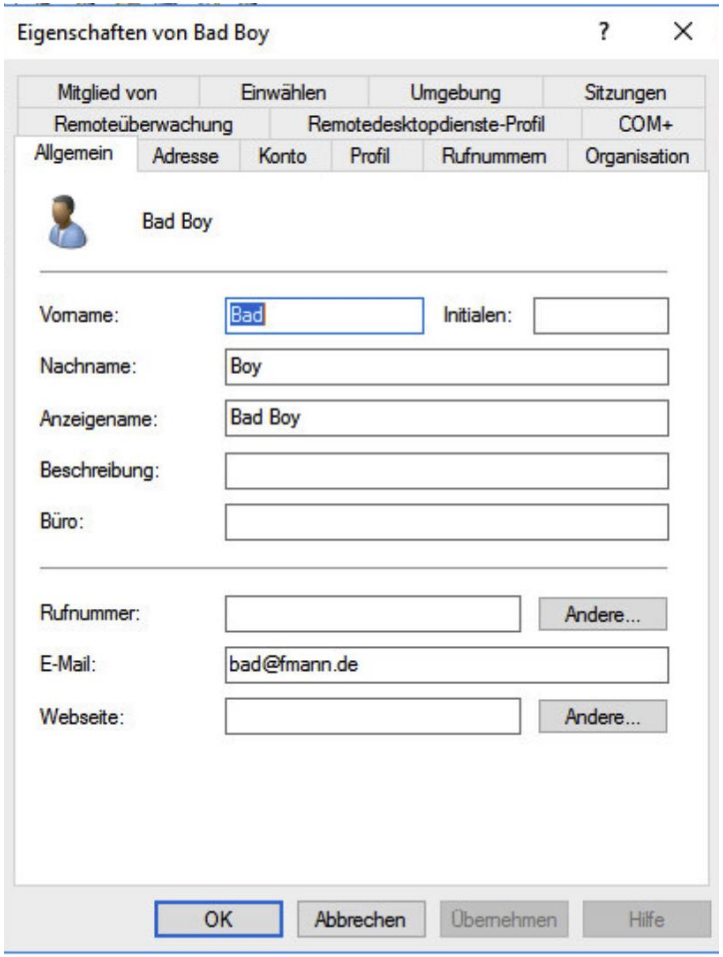
Synchronisation mit LDAP / AD

- Nach erfolgreichen Check der Verbindung, kann man nun über zwei unterschiedliche Verfahren User mit WatchGuard AuthPoint synchronisieren:
  - Group Sync – Auswahl von Gruppen direkt aus dem LDAP / AD.
  - Advanced Query – Abfrage einer Gruppenzugehörigkeit mit Hilfe des „distinguished name“.



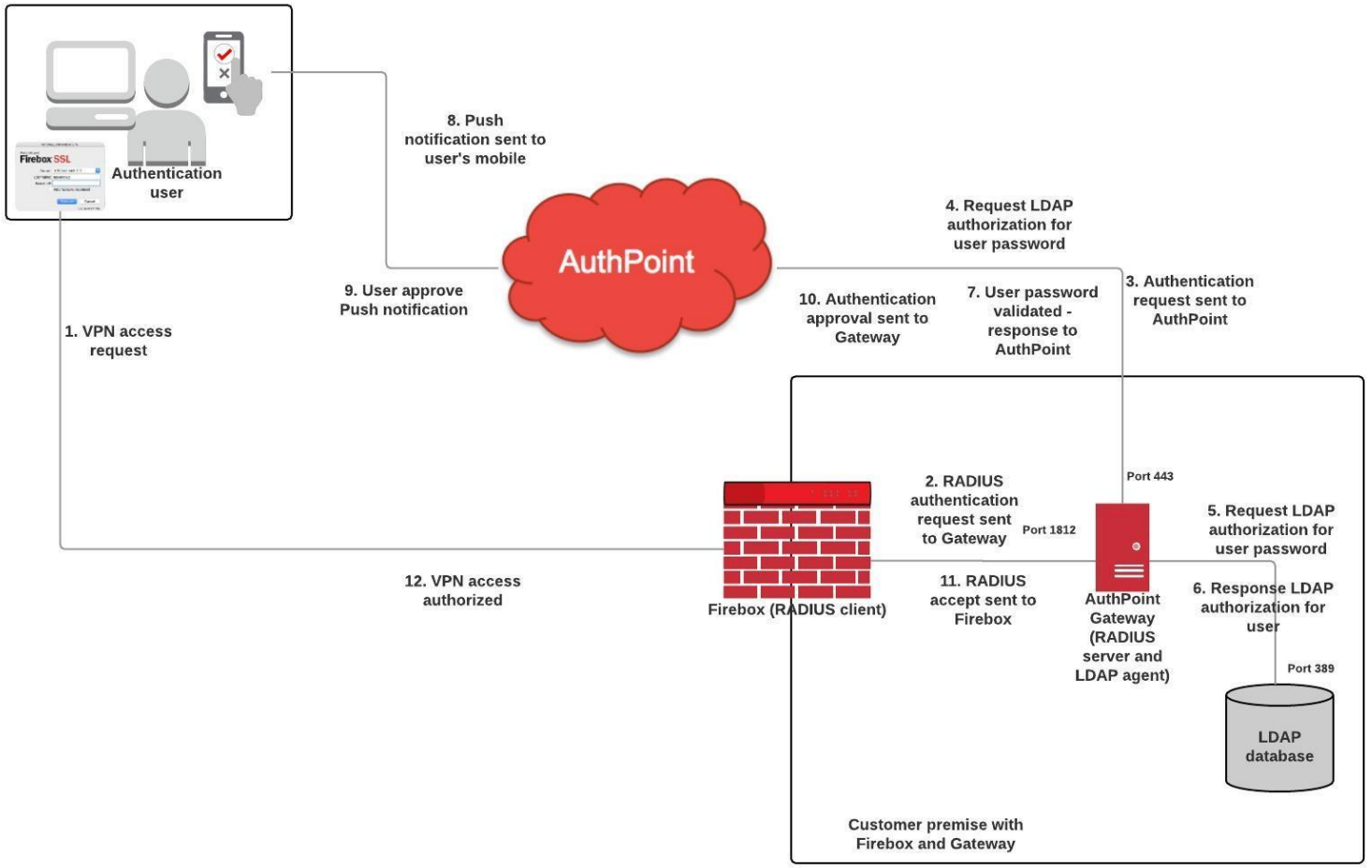
Synchronisation mit LDAP / AD

- Hinweis:
  - Es werden nur Benutzer in WatchGuard AuthPoint angelegt, wenn diesen eine E-Mail Adresse im LDAP / AD hinterlegt haben.
  - Das Passwort des User wird NICHT synchronisiert. Eine Abfrage des Passwort Hash erfolgt immer direkt gegen das LDAP / AD.
  - Der Benutzer kann nur einer AuthPoint Gruppe zugeordnet sein.

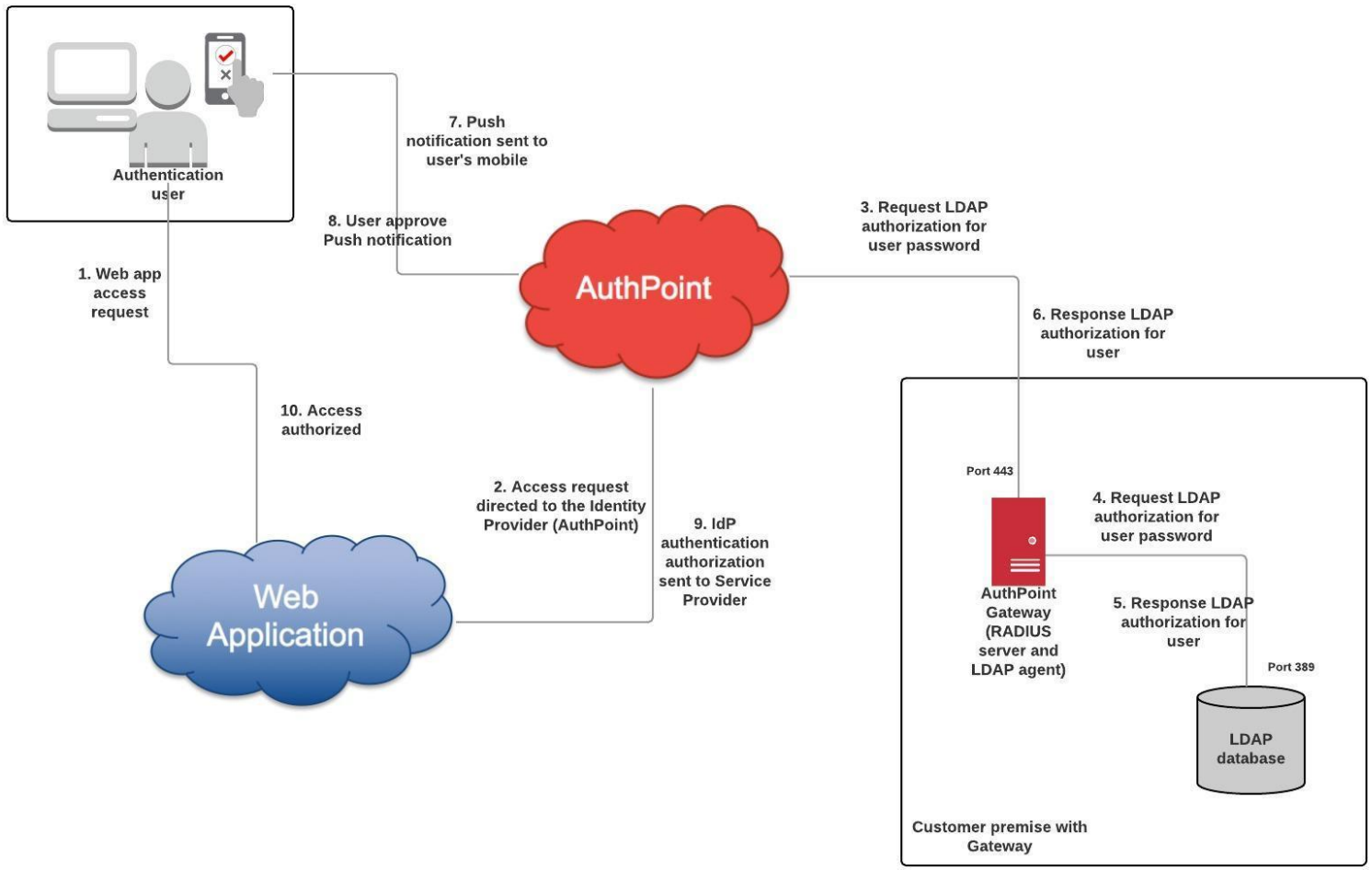


Schaubild

AUTHPOINT - RADIUS AUTHENTICATION FOR LDAP USER



Schaubild



Zukunft von WatchGuard AuthPoint

- Im Bereich Authentifizierung gegen LDAP / AD werden weitere Funktionen in diesen Jahr umgesetzt.
  - ADFS Support
    - **Diese Funktion ist gerade in der Beta Phase.**
    - Mit dem AuthPoint ADFS-Agenten können Sie ADFS zur zusätzlichen Sicherheit die Multi-Faktor-Authentifizierung (MFA) hinzufügen. Der ADFS-Agent enthält folgende Funktionen:
      - MFA mit Push, QR-Code oder OTP
      - Offline-Authentifizierung mittels QR-Code oder OTP
      - Forgot Token ermöglicht Benutzern die Authentifizierung ohne ihren Token
      - Möglichkeit, sich nur mit Ihrem Passwort anzumelden
      - Um MFA mit ADFS verwenden zu können, muss das AuthPoint Gateway installiert sein.

Zukunft von WatchGuard AuthPoint

- Im Bereich Authentifizierung gegen LDAP / AD werden weitere Funktionen in diesen Jahr umgesetzt.
  - Neue LogonApp für Windows
    - Diese wird dann einen Agenten für RDP Services beinhalten.
  - Azure AD Agent
    - Direkte Integration in die AD von Azure.
  - Anbindung von Cloud basierten LDAP / AD Services
  - …


Live Demo