



Wir nutzen die AWS Cloud

DARUM NUTZEN UNTERNEHMEN FOXPASS + SSO

Warum Unternehmen Foxpass zusätzlich
zu ihrem SSO/SAML-Anbieter nutzen:



Authentifizierung
in WLAN-Netzwerken



VPN



LDAP-Clients



Authentifizierung
auf Geräten

Automatisieren Sie die Bereitstellung durch automatische Synchronisierung zwischen Foxpass und Ihrem Hauptverzeichnis

Foxpass verwaltet über 100.000 Mitarbeitende

hackerone



greenlots
A Member of the Shell Group



lyft

imgur

Rollbar



Segment

Zugriffskontrolle für **WLAN- & LAN-Netzwerke**

Was wir bieten:

Wir bieten wahlweise

- Cloud-gehostetes RADIUS auf Basis von Benutzername/Kennwort
- Zertifikatsbasiertes, Cloud-gehostetes RADIUS
- PKI (SCEP): Macht Kennwörter überflüssig, da nur Geräte mit installierten Zertifikaten ins Netzwerk gelangen.

Was ist RADIUS?

Während beim WLAN-Zugang zu Hause oder im Café alle das gemeinsame Kennwort kennen müssen, sollte in einem Unternehmen jeder Benutzer eigene Anmeldedaten haben. RADIUS ist das Protokoll, mit dem der Access Point einen Benutzer gegenüber einer Quelle für Anmeldedaten authentifiziert.

Zweck des Netzwerkschutzes:

- Netzwerkgeräte vor Angriffen schützen (Computer, angeschlossene Speicher, Drucker usw.)
- Schutz vor Man-in-the-Middle-Angriffen
- Bandbreitendiebe stoppen
- Nutzung der Firmen-IP-Adresse durch Nicht-Mitarbeitende verhindern
- Compliance-Anforderungen nach PCI, SOX, SOC2 und HIPAA

OKTA-Integration:

- Endbenutzer können ihr bestehendes Okta-Kennwort für die WLAN-Anmeldung verwenden (bei der Methode mit Benutzername und Kennwort)
- Benutzer und Gruppen werden automatisch aus Okta synchronisiert

Was noch?

- Volle Unterstützung für RADIUS-Attribute
- RADIUS-Protokolle – sogar mit der Möglichkeit, die Protokolle über AWS Kinesis zu streamen, damit sie in einem SIEM wie SPLUNK oder SumoLogic verfügbar sind
- RadSec-Unterstützung

Was kostet das?

Siehe <https://foxpass.com/pricing/>

(Rabatte bei jährlicher Zahlung,
für gemeinnützige
Organisationen, MSPs und
Großkunden)

