Best Practices WatchGuard AuthPoint - Integration in die WatchGuard Firebox

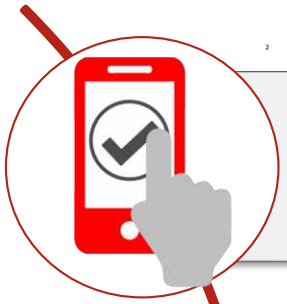
Thomas Fleischmann
Senior Sales Engineer CE
Thomas.Fleischmann@watchguard.com

Agenda

- Konzept von AuthPoint
- Schnittstellen in der Firebox zu AuthPoint
  - VPN mit RADIUS
  - Access Portal mit SAML / RADIUS
  - User Login Firebox mit RADIUS
- *Live Demo*

Konzept von AuthPoint

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

Vorausetzungen

- Benutzer sind im AD und bei WachtGuard AuthPoint angelegt.
- Benutzer können ihren Token verwenden.
- WatchGuard AuthPoint Gateway ist installiert.
- RADIUS funktioniert mit der Firebox für VPN oder andere Funktionen.

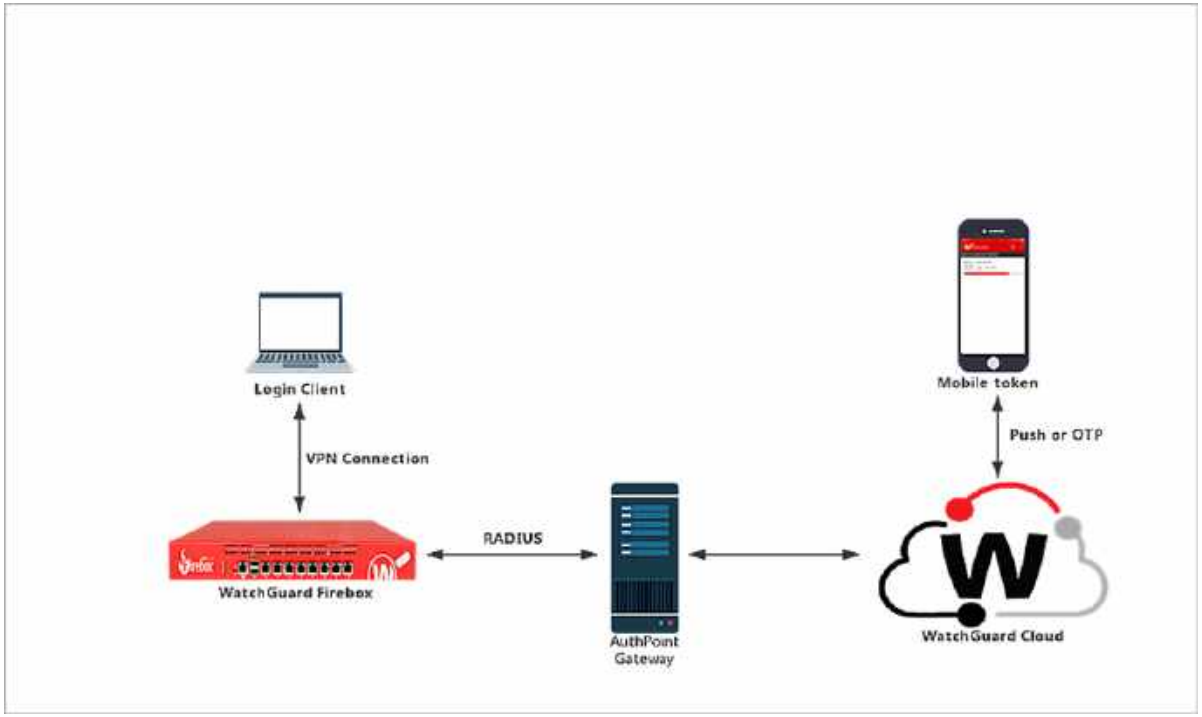
VPN mit RADIUS

- Integration Guides zu den einzelnen VPN Arten mit AuthPoint können unter folgende Links gefunden werden:

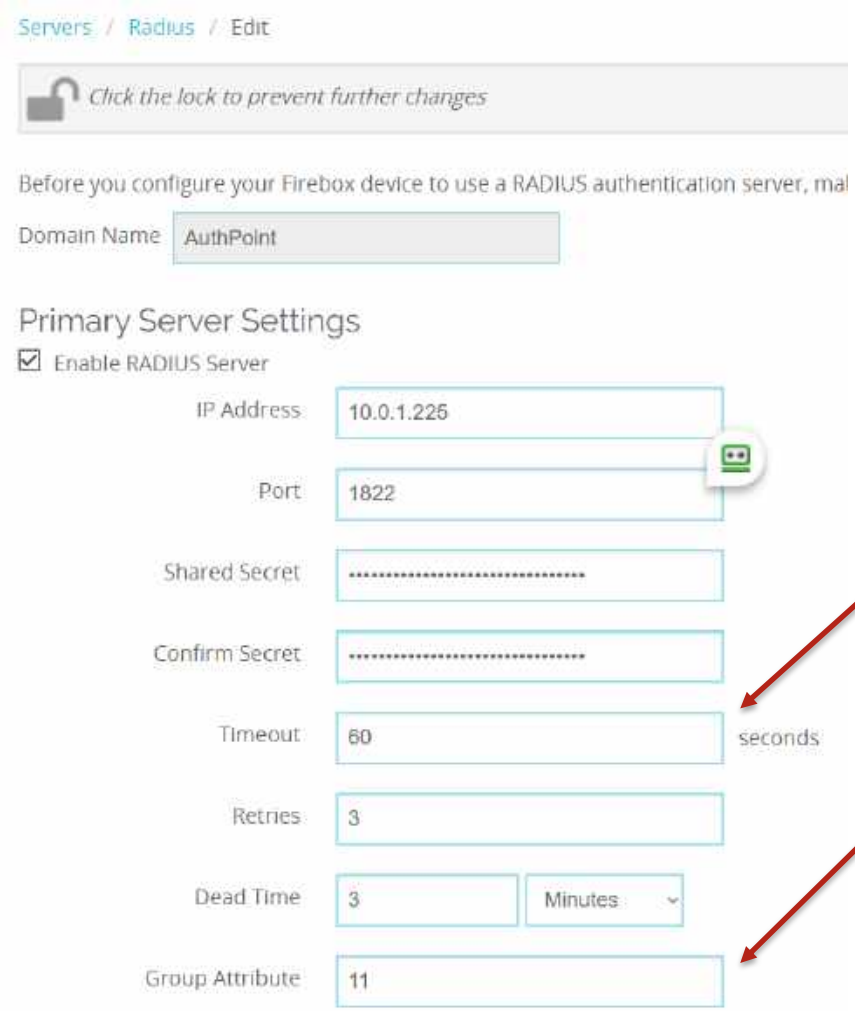
  - IPSec: https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/firebox-ipsec-vpn-radius_authpoint.html?tocpath=Self-Help%20Tools%7CIntegration%20Guides%7CAuthPoint%7C_____4
  - SSL VPN: https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/firebox-ssl-vpn-radius_authpoint.html?tocpath=Self-Help%20Tools%7CIntegration%20Guides%7CAuthPoint%7C_____2
  - L2TP: https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/firebox-l2tp-vpn-radius_authpoint.html?tocpath=Self-Help%20Tools%7CIntegration%20Guides%7CAuthPoint%7C_____3
  - IKEv2: https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/firebox-ikev2-vpn-radius_authpoint.html?tocpath=Self-Help%20Tools%7CIntegration%20Guides%7CAuthPoint%7C_____1

VPN mit RADIUS

- Als Beispiel wird hier kurz die folgende Integration dargestellt
  - „Firebox Mobile VPN with SSL Integration with AuthPoint”

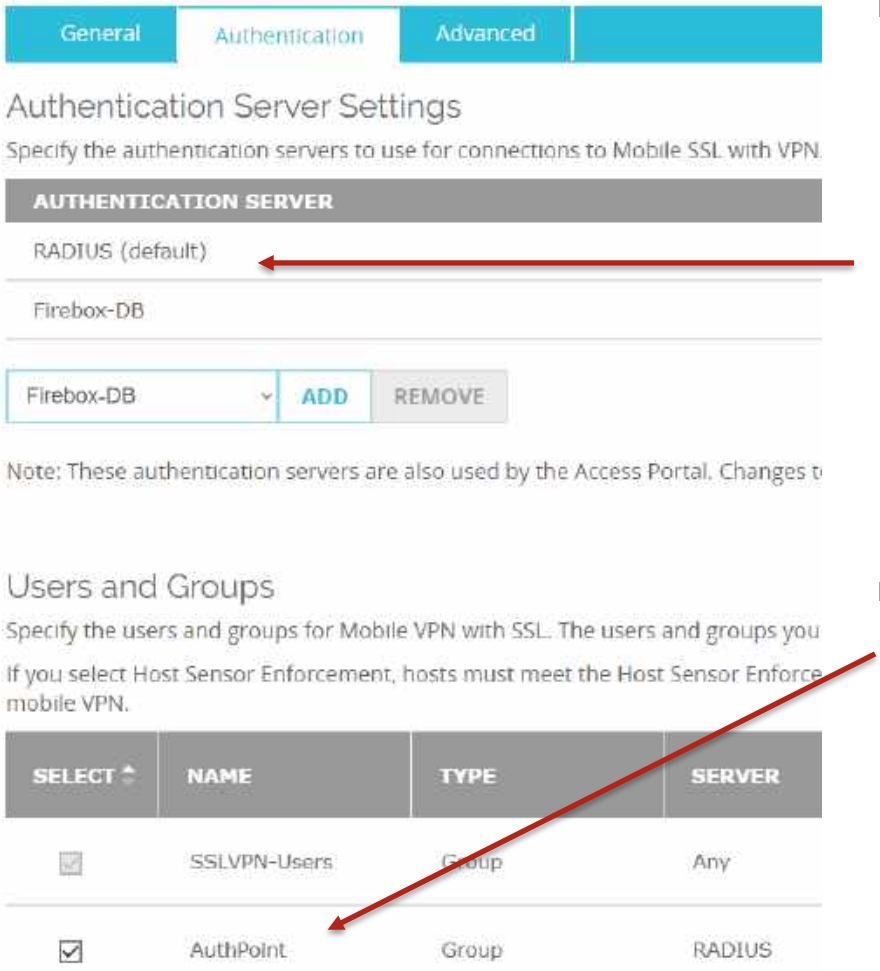


VPN mit RADIUS



- Zu einem überprüft man die Einstellung des RADIUS Server auf der Firebox.
  - Timeout sollte man auf 60 Sekunden ändern.
  - Group Attribute muß den Wert 11 enthalten. Dieser Wert ist auch als Filter-Id bekannt.

VPN mit RADIUS

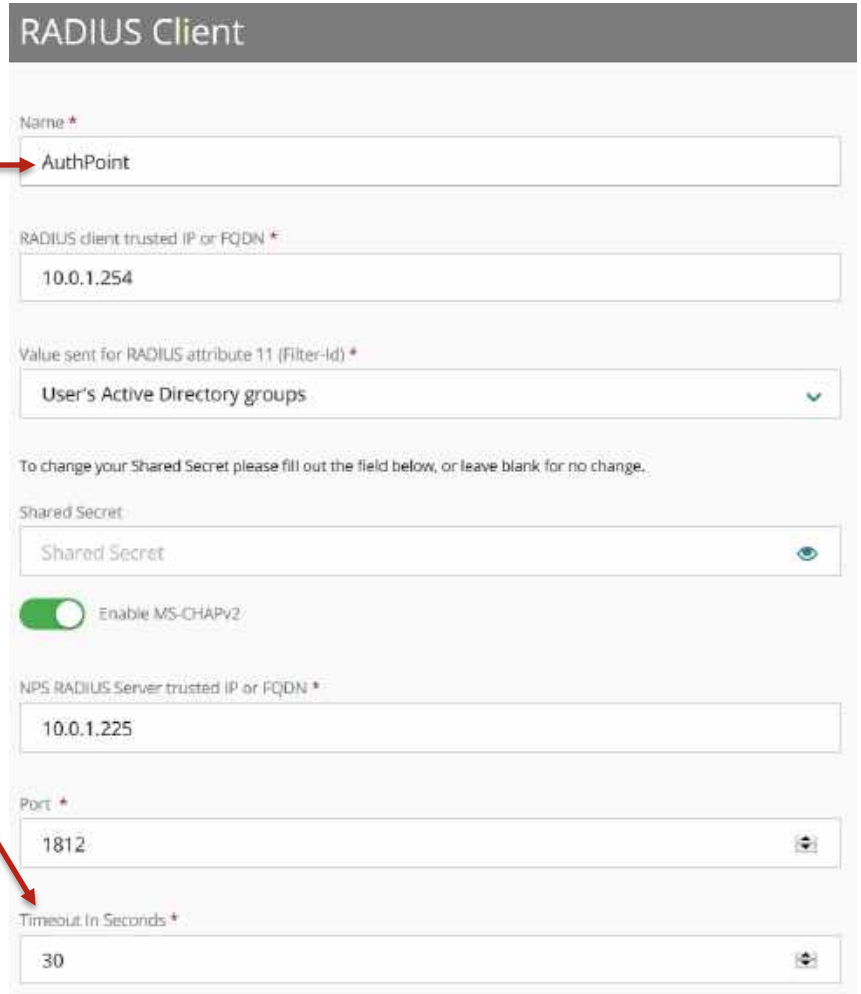


- Im der Mobile User VPN Einstellung für SSL muß der RADIUS Server als Authentifizierung Server aktiviert werden.
- Des Weiteren muß eine Gruppe mit den Gruppennamen des RADIUS Server dort hinterlegt sein.

VPN mit RADIUS

- Unter den Einstellungen in WatchGuard AuthPoint ist es wichtig, dass der RADIUS Name mit den Einstellungen auf dem RADIUS Client in der Firebox übereinstimmt.

- Die Timeout Einstellungen sollten entsprechend angepasst werden.



VPN mit RADIUS

- Im AuthPoint Gateway Einstellungen muß die Radius Ressource hinzugefügt werden.
- Wichtig ist hierbei, dass man den RADIUS Port auf den notwendigen Wert einstellt.

VPN mit RADIUS

- Zum Schluss sollte man überprüfen, ob der Benutzer auch die Ressource über seine Gruppe erhält !
- Hier ist es wichtig bei den VPN Ressourcen zu definieren, ob der User sich per Push oder Eingabe des OTP am System authentifiziert.

Resources	Resource Type	Password	OTP	Push	QR Code
Access Portal	SAML	✓	✓	✓	✓
AuthPoint	RADIUS Client	✓		✓	
WGDCE	IDP Portal	✓	✓	✓	✓
LogonApp	Logon App	✓	✓	✓	✓
Salesforce	SAML	✓	✓	✓	✓
Dimension	RADIUS Client	✓		✓	
Home AP	SAML	✓	✓	✓	✓

Access Portal mit SAML / RADIUS

Anleitung

- Die Anleitung finden sie unter

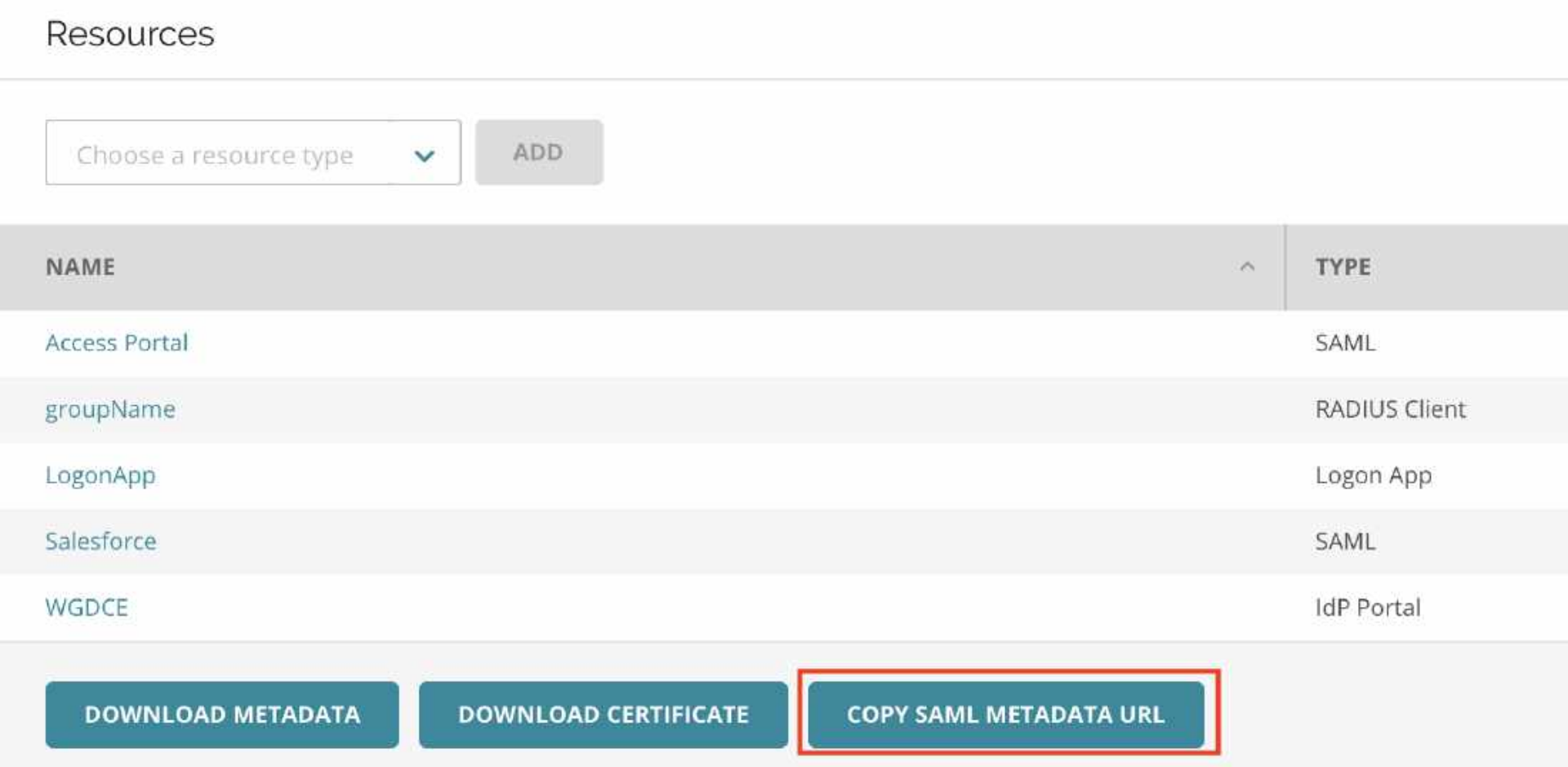
https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/access-portal-saml_authpoint.html?tocpath=Integration-Guides%7CAuthPoint%7CAmazon%20Web%20Services%20Integration%20with%20AuthPoint%7C_____18

- Weitere Anleitungen unter

https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/_intro/authpoint-integrations.html

Konfiguration des WatchGuard Access Portals

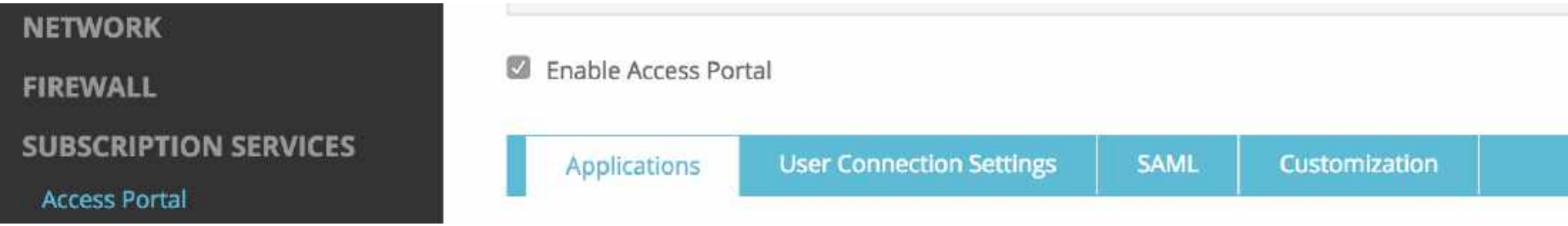
- Unter https://cloud.watchguard.com – einloggen.
- Im AuthPoint Bereich unter „Resources“ den Link „Copy SAML Metadata URL“ kopieren.



Konfiguration des WatchGuard Access Portals

- In der Konfiguration der WatchGuard Firewall im Bereich „Subscription Services“ den Menü-Punkt “Access Portal“ auswählen.

- Den Punkt „Enable Access Portal“ anklicken und speichern.



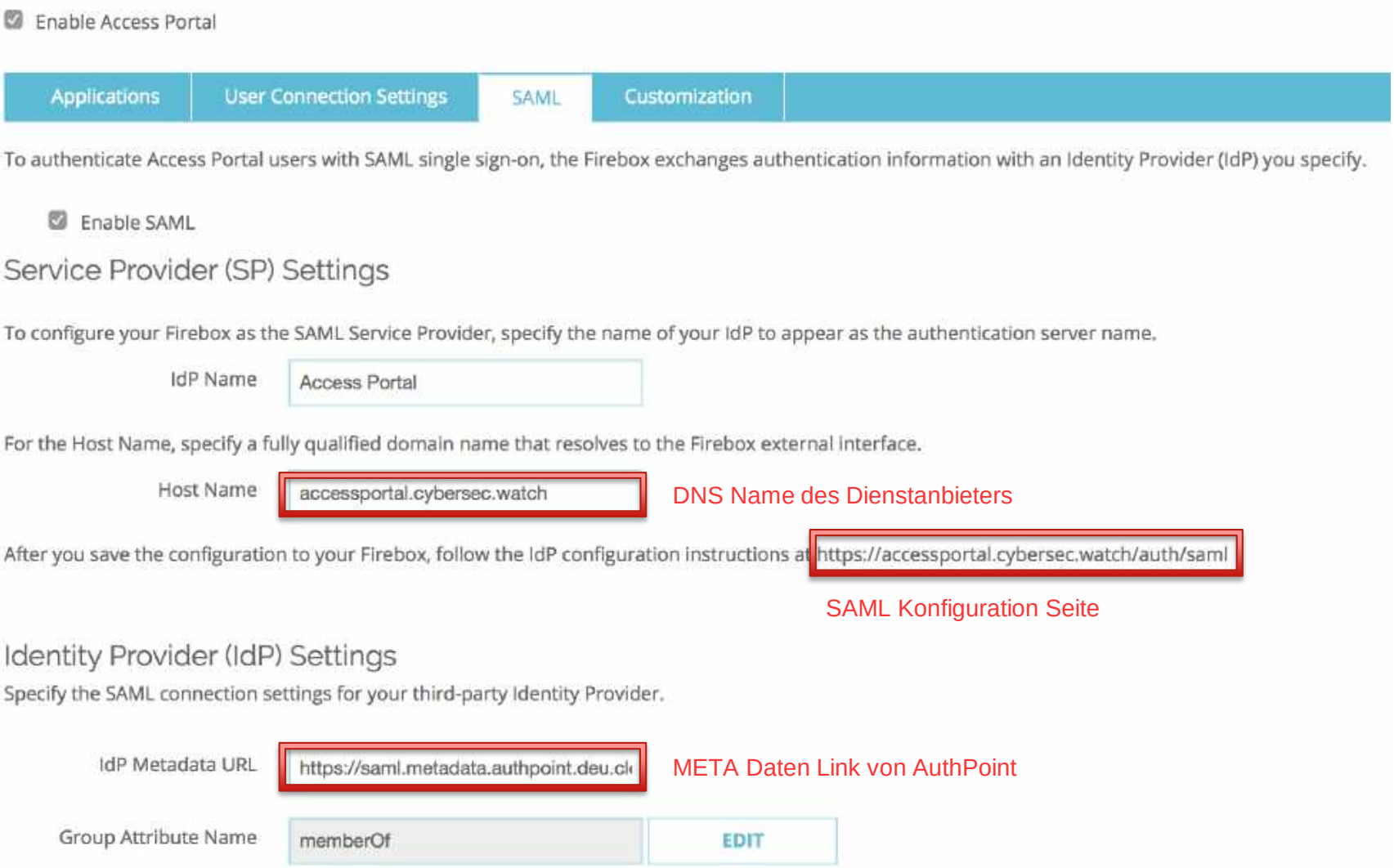
Konfiguration des WatchGuard Access Portals

- Version 12.1.x:
  - Öffnen des Bereichs „User Connection Settings“ und dort den Button „Configure“ anklicken.
  - Den Karteireiter „SAML“ auswählen.

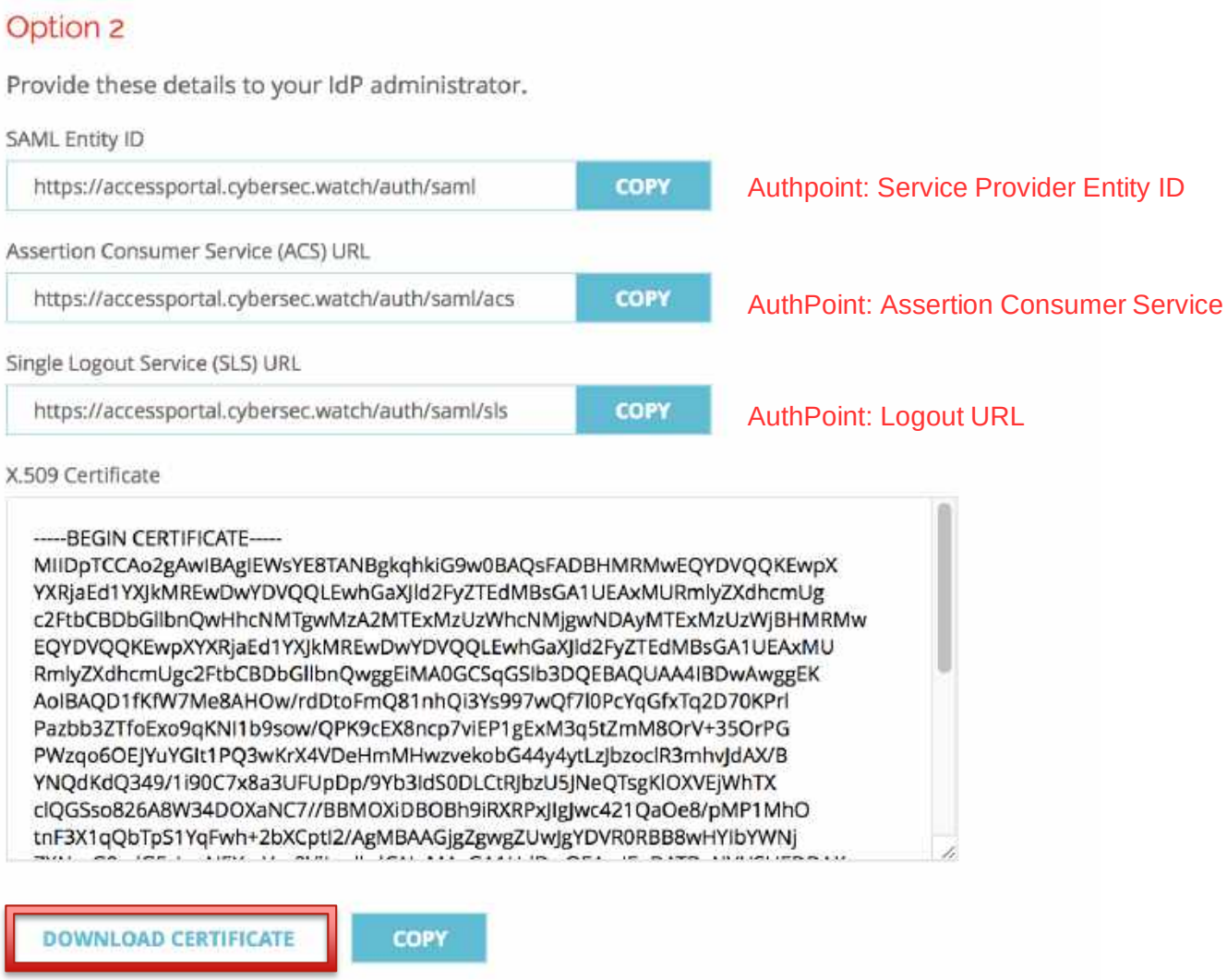
- Version 12.2:
  - Direkte Wahl des Karteireiters „SAML“.

- Auswahl „Enable SAML“, um ein SAML basierte MFA zu konfigurieren.

Konfiguration des WatchGuard Access Portals



Konfiguration des WatchGuard Access Portals



Authpoint: Service Provider Entity ID

AuthPoint: Assertion Consumer Service

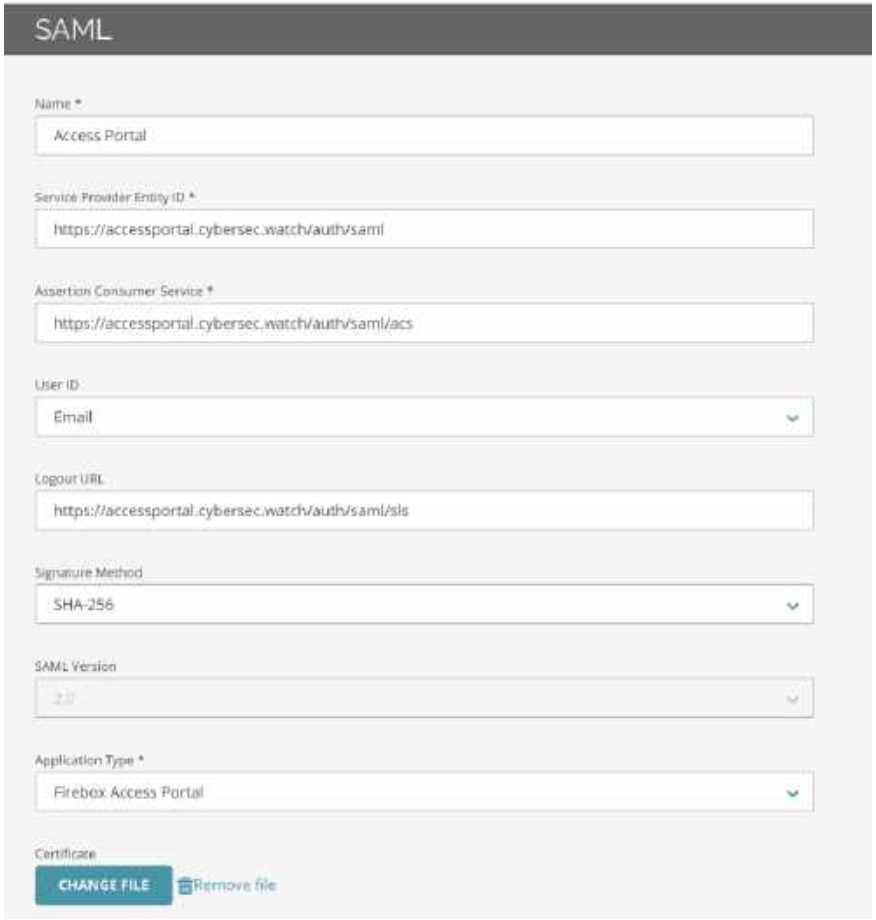
AuthPoint: Logout URL

DOWNLOAD CERTIFICATE COPY

Zertifikat, was in AuthPoint mit der Ressource gespeichert werden muss.

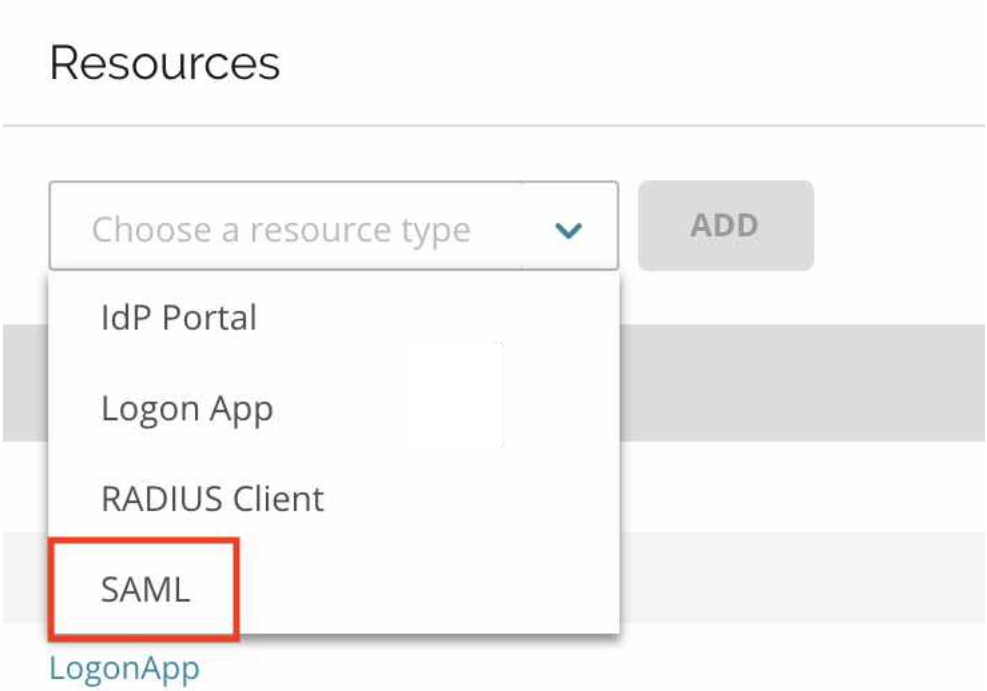
Konfiguration von WatchGuard AuthPoint

- Die Daten aus dem Access Portal übernehmen (Copy & Paste).



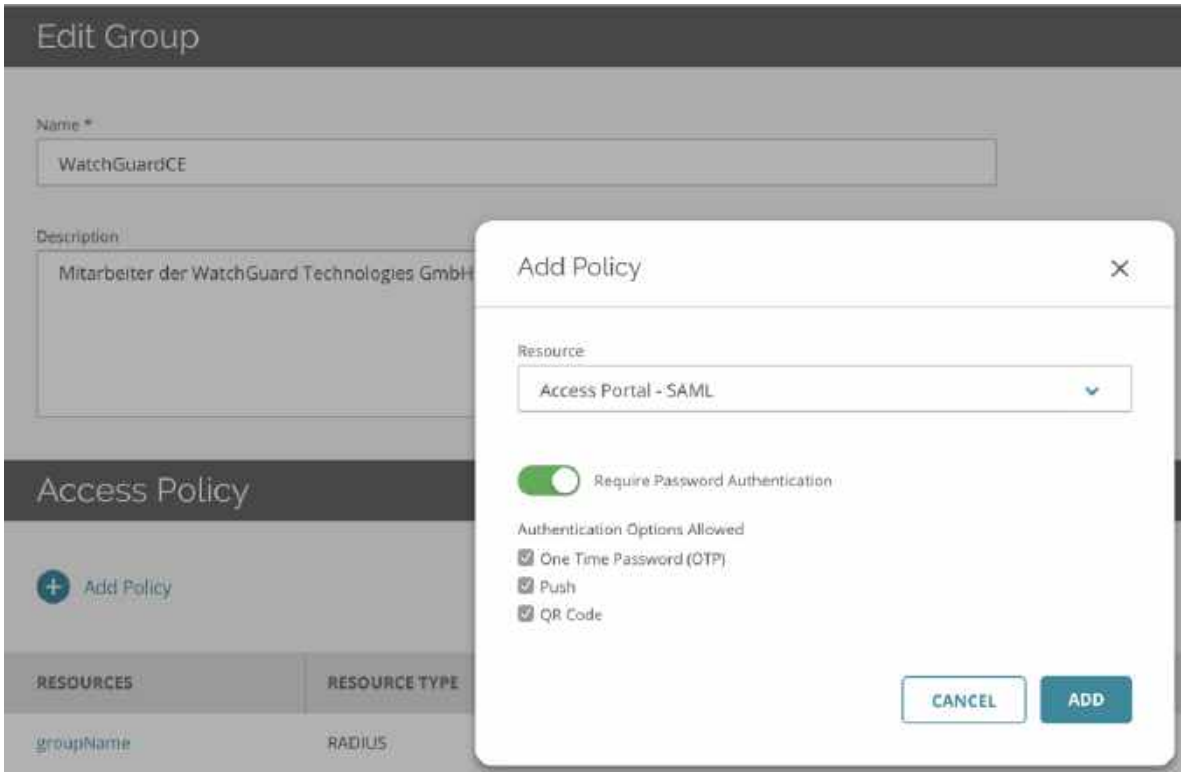
Konfiguration von WatchGuard AuthPoint

- Unter der Konfiguration von WatchGuard AuthPoint eine neue Ressource des Typ „SAML“ erstellen.



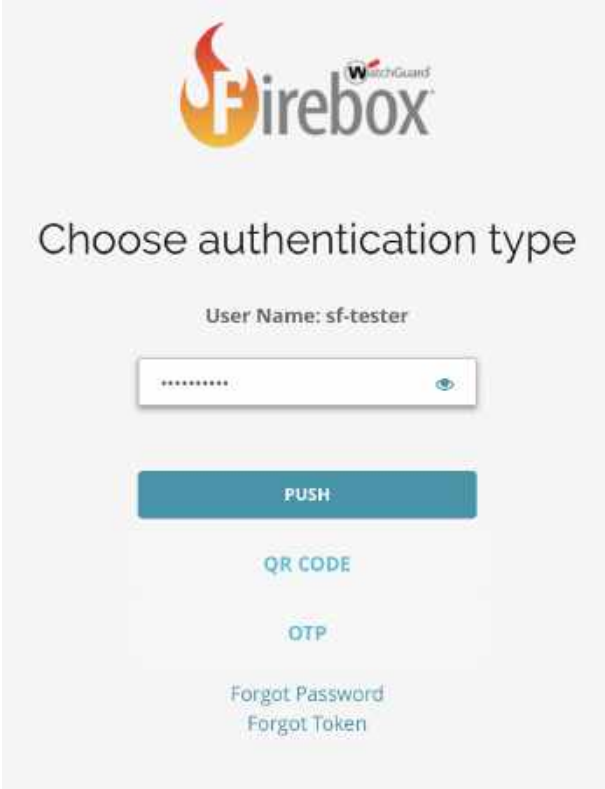
Konfiguration von WatchGuard AuthPoint

- Die gespeicherte Ressource für das Access Portal einer Gruppe in AuthPoint hinzufügen.
- Festlegen, welche Access Policy die Gruppe hat.



Test

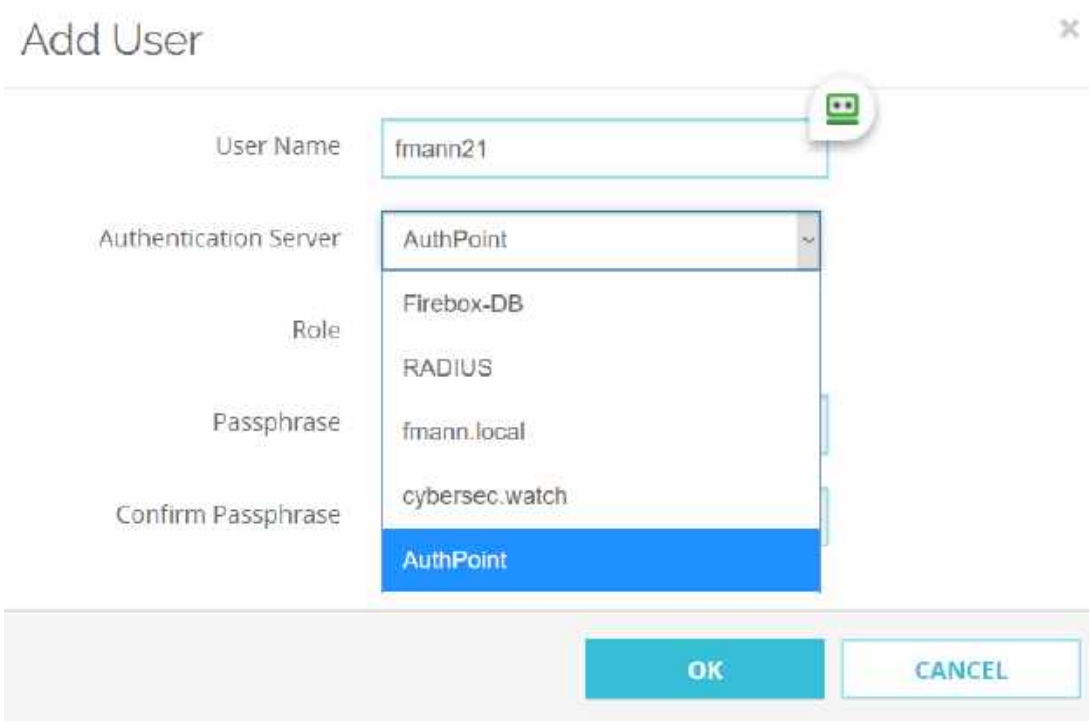
- Anmelden an dem Access Portal der Firewall
  - https://<FQDN der Firebox>
- Auswahl der MFA Authentifizierung
  - Gewählter IdP Name im Portal
- Auf dem IdP-Portal anmelden
  - Je nach zugelassener Methode



User Login Firebox mit RADIUS

User Login Firebox mit RADIUS

- Im Bereich User and Roles kann man weitere Systeme Benutzer anlegen.
- In der Konfiguration des Benutzer wird dann die Art der Authentifizierung festgelegt.

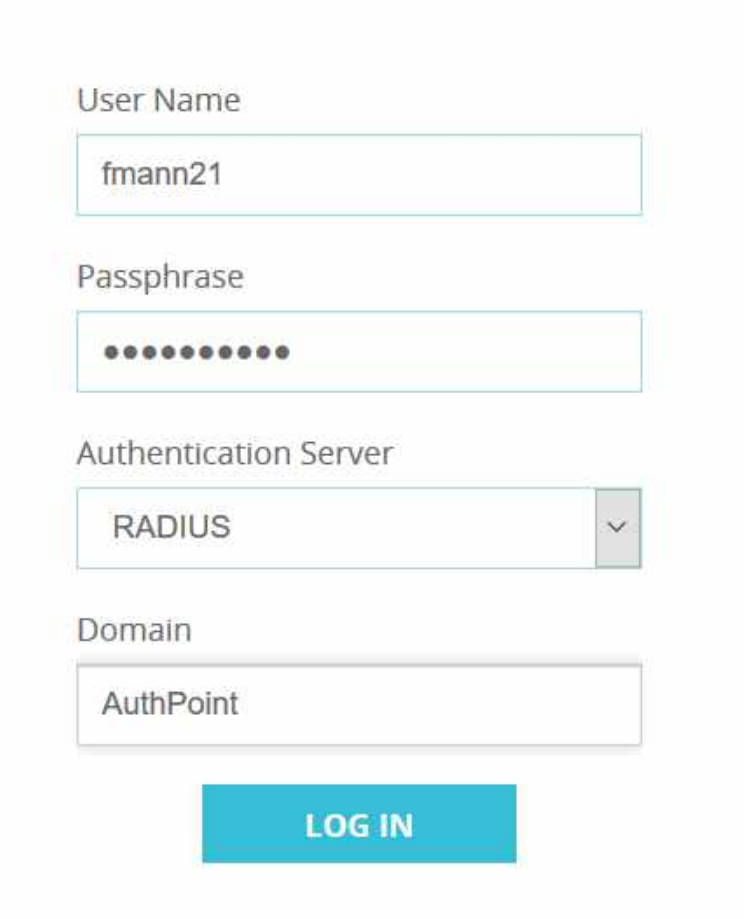


User Login Firebox mit RADIUS

- Beim Login an der Firebox muß man nun folgende Informationen angeben.
  - Username
  - Passwort
  - RADIUS

  (Authentifizierungsmethode)
  - RADIUS Gruppe

  (Hier als Wert DOMAIN abgefragt)



Troubleshooting

Troubleshooting

- Es existiert mehrere Informationen zu Anmeldungen im System.

- In der WatchGuard Cloud werden im Bereich Monitor Anmeldungen und Fehlschläge der selbigen als Report generiert.
- Im Bereich Administration -> Audit Log werden auch alle Anmeldungen (Erfolgreich und Fehlgeschlagene) erfasst und mit Informationen dargestellt.

Troubleshooting

Fehlerbehebung bei RADIUS-Authentifizierung

- Sehen Sie sich diese Logmeldungen und Fehlermeldungen an:
  - Audit-Protokolle in der WatchGuard-Cloud
  - RADIUS-Protokolle auf dem AuthPoint Gateway
  - RADIUS-Client-Fehlermeldungen
  - Firebox-Protokollmeldungen - Wenn die Firebox als RADIUS-Client konfiguriert ist, durchsuchen Sie die Firebox-Protokollmeldungen nach Benutzerauthentifizierungsereignissen und Verbindungsfehlern zwischen der Firebox und dem AuthPoint Gateway.

Troubleshooting

Fehlerbehebung bei der LDAP-Authentifizierung

- Sehen Sie sich diese Logmeldungen an:
  - Suchen Sie in den LDAP-Protokollen auf dem Gateway:
    - Ergebnisse der Konnektivitätstests
    - Synchronisierungsereignisse
    - Anfragen zur Benutzerauthentifizierung
    - Fehler bei Verbindungen mit dem Domänencontroller
  - Suchen Sie in den Audit-Protokollen der WatchGuard-Cloud nach:
    - LDAP-Änderungen der external identity
    - LDAP-Benutzer-Synchronisationsfehler

- In diesem Verzeichnis finden Sie die Gateway-Protokolldateien: *C:\ProgramData\WatchGuard\AuthPoint\Protokolle*


Live Demo


Danke