Best-Practices – WatchGuard Access Portal mit MFA Integration

Thomas Fleischmann

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

Agenda

- Voraussetzung
- Schnittstellen zu Multifaktor Authentifizierungen
- WatchGuard Access Portal - Integration WatchGuard AuthPoint
- Live Demo

Voraussetzung

Voraussetzung

- Das Access Portal ist seit der Version 12.1 in der WatchGuard FireOS enthalten.

- Das Access Portal ist auf folgenden Modellen unterstützt:

- Firebox T40 und T80
- Firebox M Series außer M200 und M300
- FireboxV und Firebox Cloud

Voraussetzung

- Die Lizenz für das Access Portal ist Bestandteil der Total Security Suite (TSS) von WatchGuard.

- Seit Juni 2020 ist das Access Portal für folgende Firebox Modelle Bestandteil in einfachen Support Vertrag:
  - Firebox T40 / T80
  - Firebox M4800 / M5800

Schnittstellen zu Multifaktor Authentifizierungen

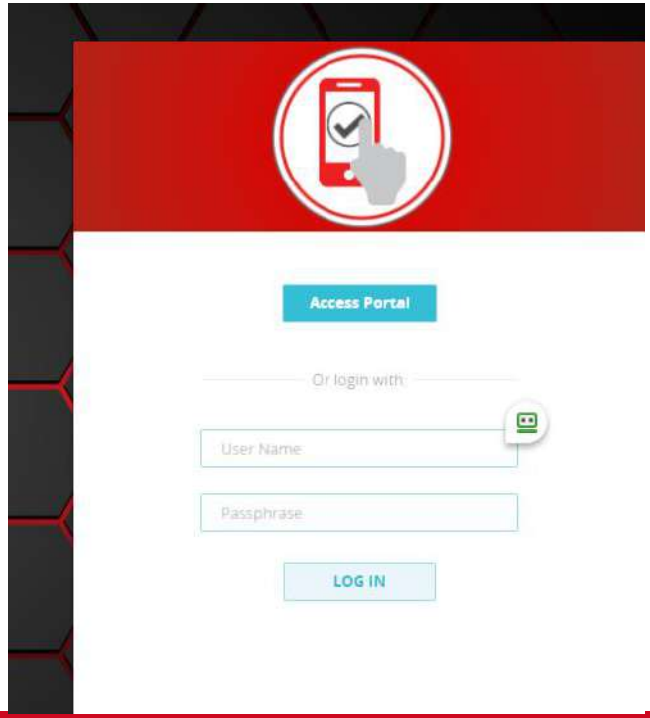
Schnittstellen

- Um mit Anbietern von MFA Applikationen sich zu verbinden, hat man zwei Standards in der WatchGuard Firebox zur Verfügung

  – RADIUS

  oder

  – SAML 2.0



RADIUS

- Remote Authentication Dial-In User Service (RADIUS, deutsch Authentifizierungsdienst für sich einwählende Benutzer) ist ein Client-Server-Protokoll, das zur Authentifizierung, Autorisierung und zum Accounting (Triple-A-System) von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient.

- Folgende RFC sind aktuell gelistet
  - RFC 2865 Remote Authentication Dial In User Service (RADIUS)
  - RFC 2866 RADIUS Accounting
  - RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support
  - RFC 2868 RADIUS Attributes for Tunnel Protocol Support
  - RFC 2869 RADIUS Extensions

SAML 2.0

- Die Security Assertion Markup Language (SAML) ist ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen. Sie stellt Funktionen bereit, um sicherheitsbezogene Informationen zu beschreiben und zu übertragen.

- Anwendungsfälle sind:
  - Single Sign-on
    - ein Benutzer ist nach der Anmeldung an einer Webanwendung automatisch auch zur Benutzung weiterer Anwendungen authentisiert.
  - Autorisierungsdienste
    - die Kommunikation mit einem Dienst läuft über eine Zwischenstation, die die Berechtigung überprüft.

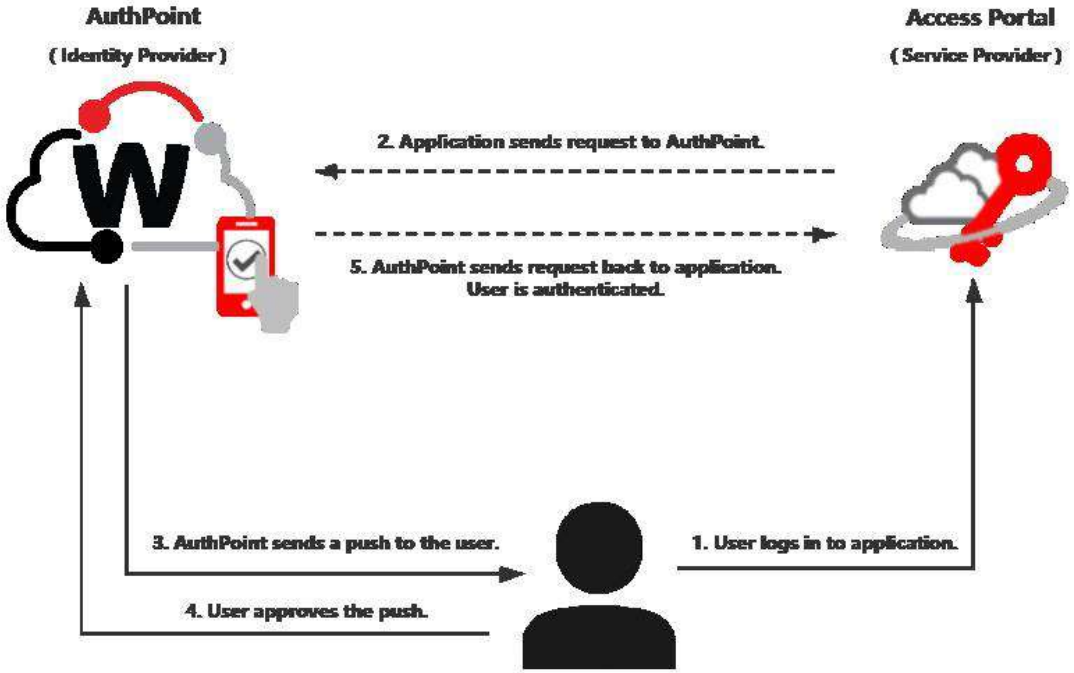
Schnittstelle

- Für Web-basierte Authentifizierung ist der Standard SAML in der Version 2.0 heute bei vielen Applikationen gesetzt.

- Dienstanbieter wie Microsoft (Office 365), Dropbox, Box, Google Apps, usw. nutzen diesen Standard für ihre Dienste.

- Das Access Portal unterstützt SAML 2.0 in zwei Arten
  - Für die Autorisierung des User an der Firebox
  - Als Portal für die Einwahl per Web SSO für die freigegebenen Ressourcen

Schematische Darstellung



Anleitung

- Die Anleitung finden sie unter

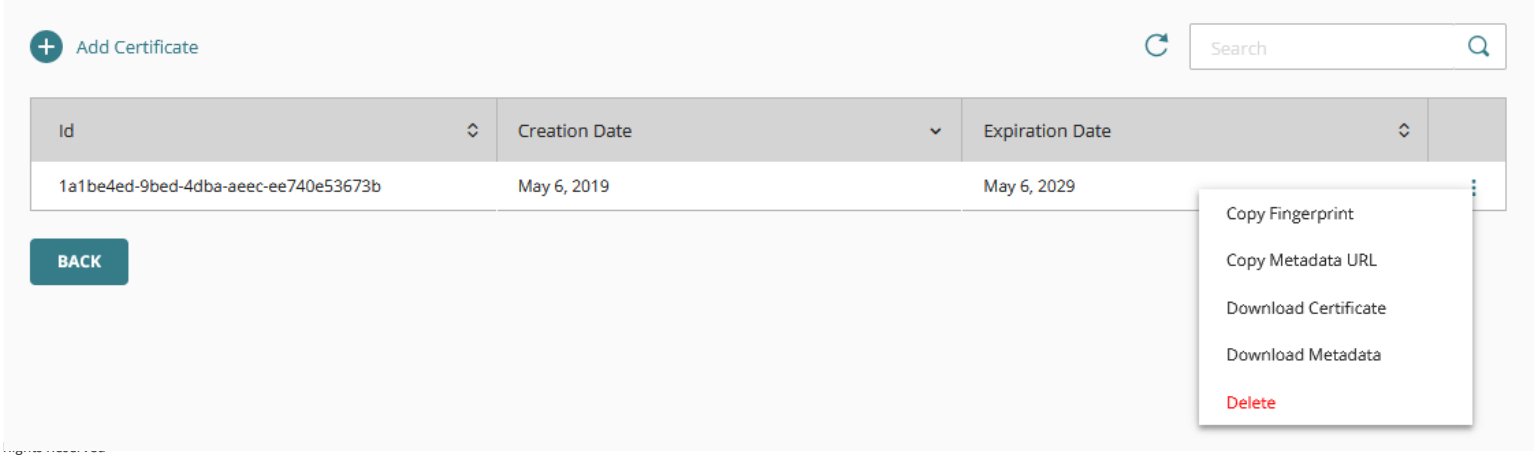
https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/access-portal-saml_authpoint.html?tocpath=Integration-Guides%7CAuthPoint%7CAmazon%20Web%20Services%20Integration%20with%20AuthPoint%7C_____18

- 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

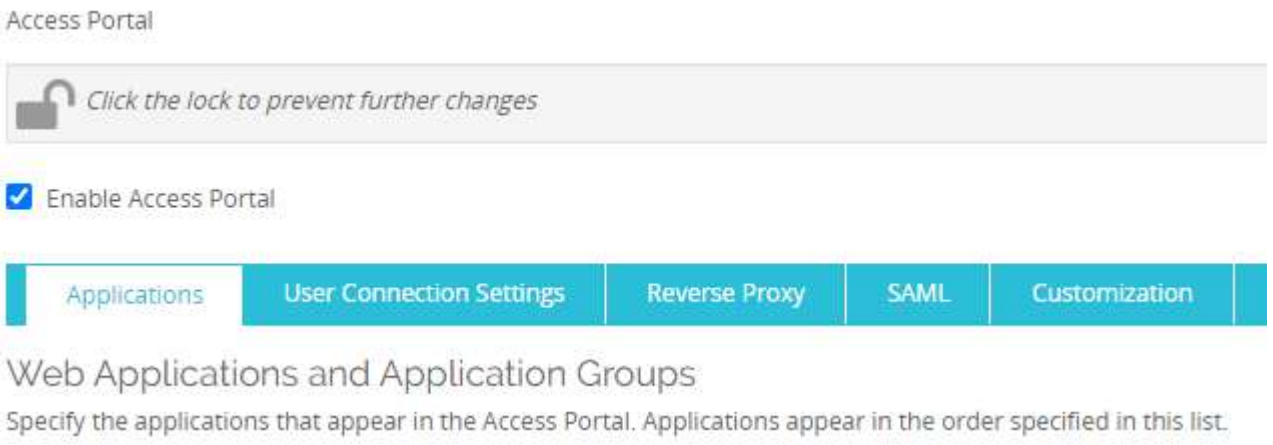
- Unter https://cloud.watchguard.com – einloggen.
- Im AuthPoint Bereich unter „Resources“ den Button „Certificates“ klicken.
- Das zu verwendende Zertifikat wählen.
- „Copy Metadata URL“ ausführen.



Konfiguration des WatchGuard Access Portals

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

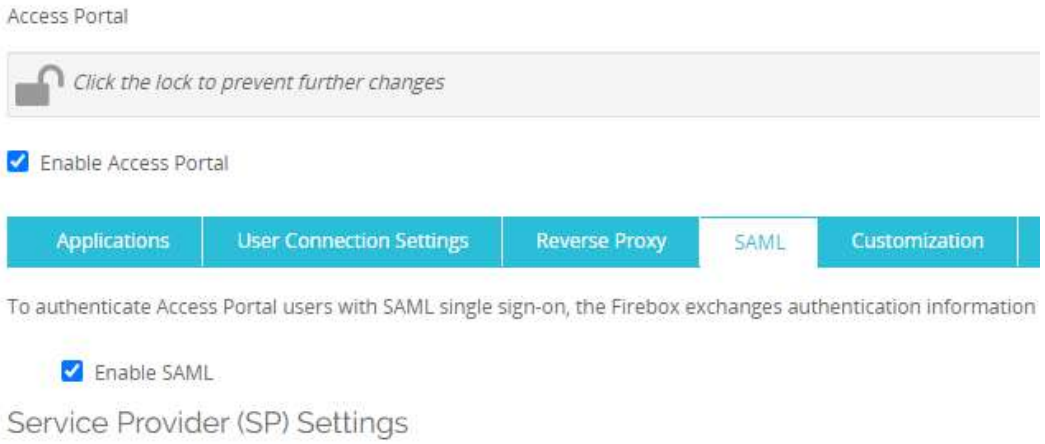
- Den Punkt „Enable Access Portal“ anklicken und speichern.



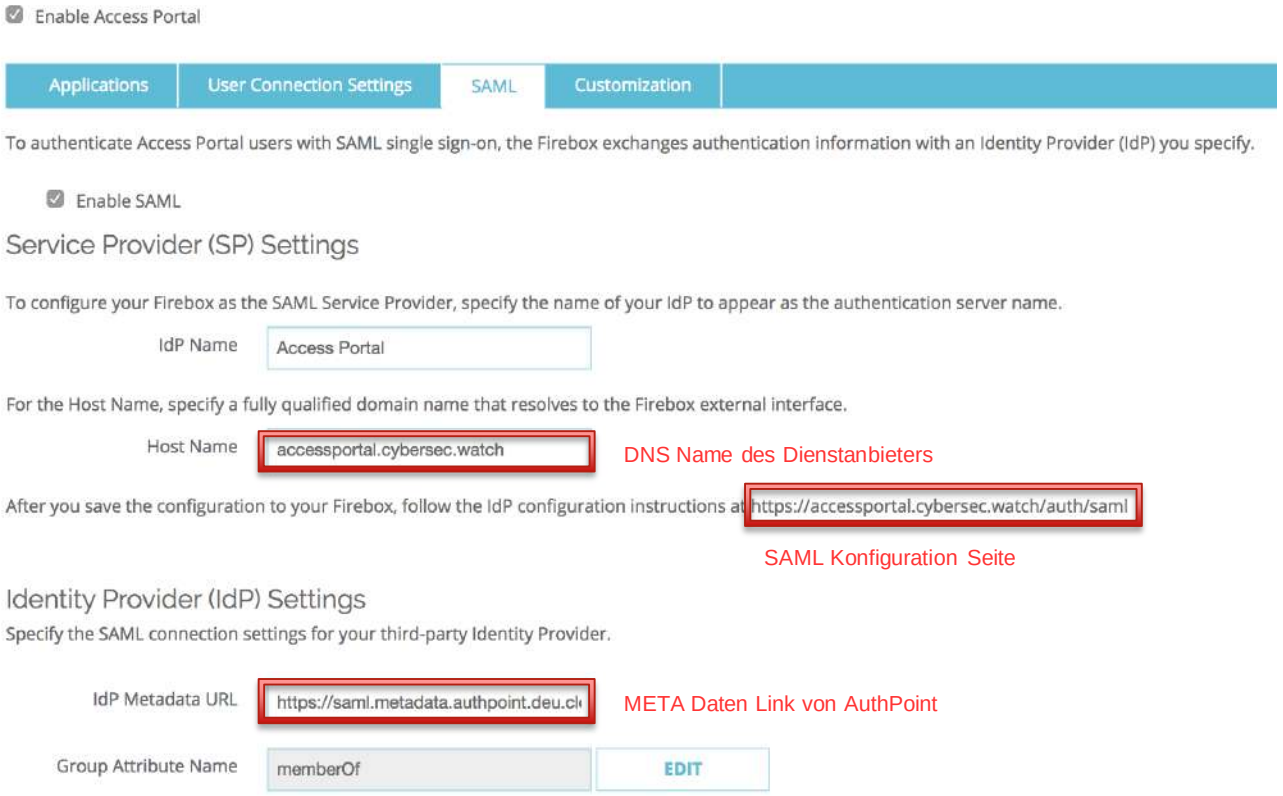
Konfiguration des WatchGuard Access Portals

- Seit der Version 12.2 und höher ist der Bereich „SAML“ direkt als einzelner Karteireiter im den Konfigurationseinstellungen der Firebox zu finden

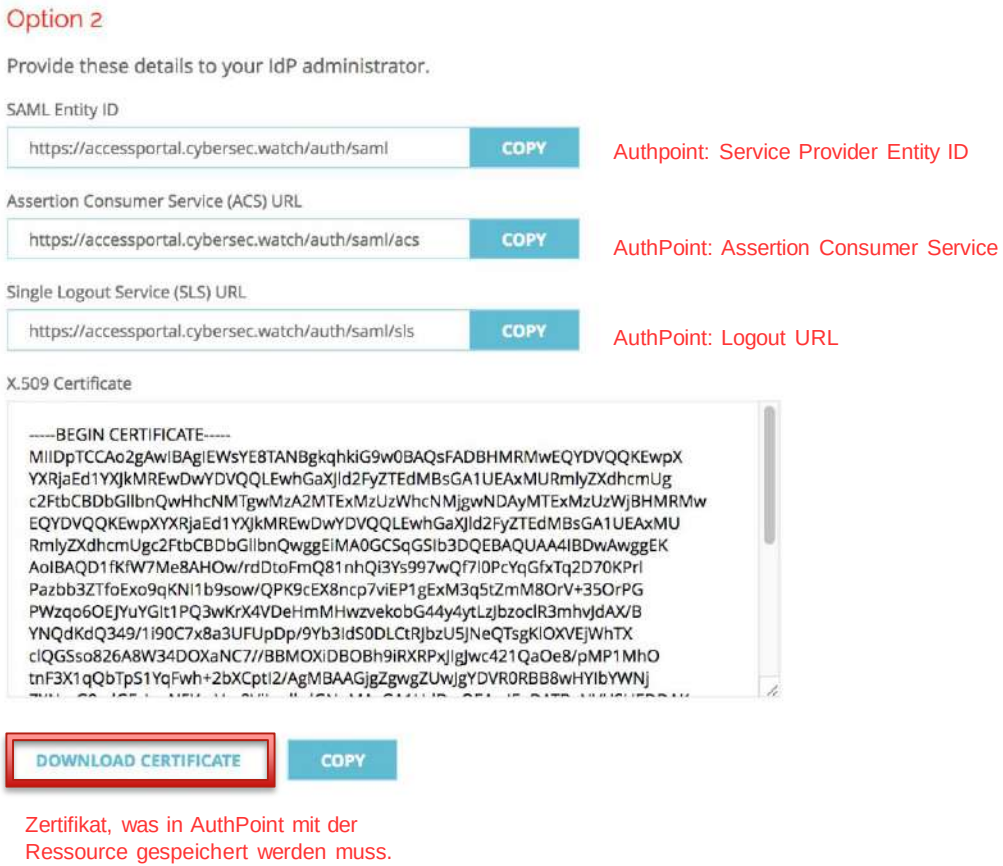
- Auswahl „Enable SAML“, um ein SAML basierte MFA zu konfigurieren.



Konfiguration des WatchGuard Access Portals

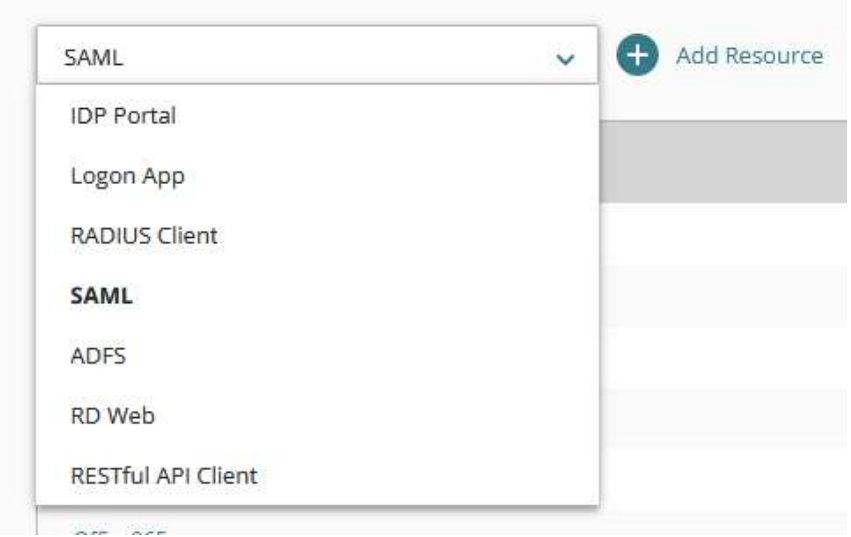


Konfiguration des WatchGuard Access Portals



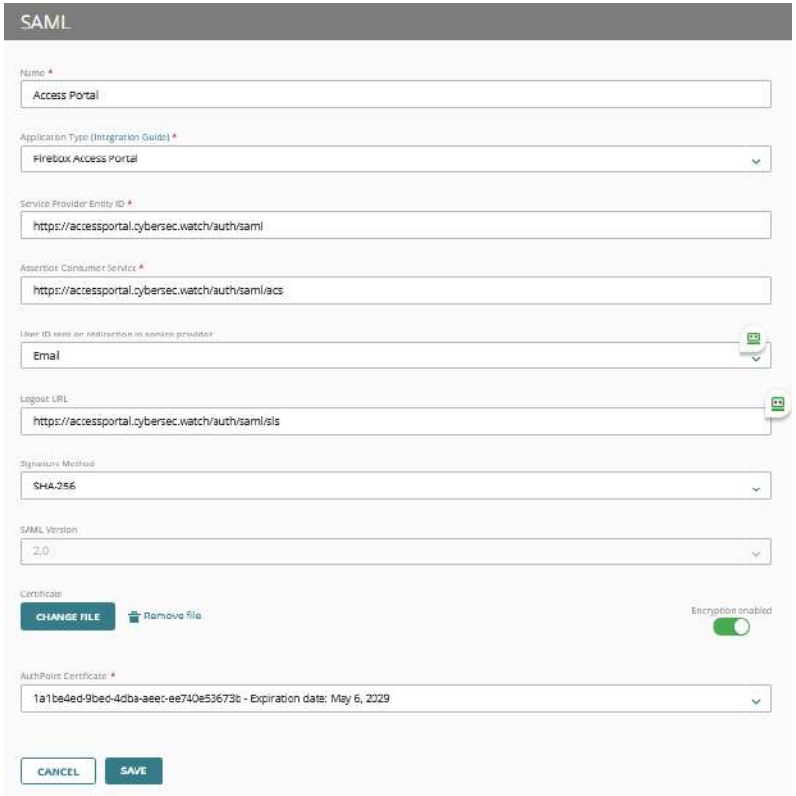
Zertifikat, was in AuthPoint mit der Ressource gespeichert werden muss.

Konfiguration von WatchGuard AuthPoint



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

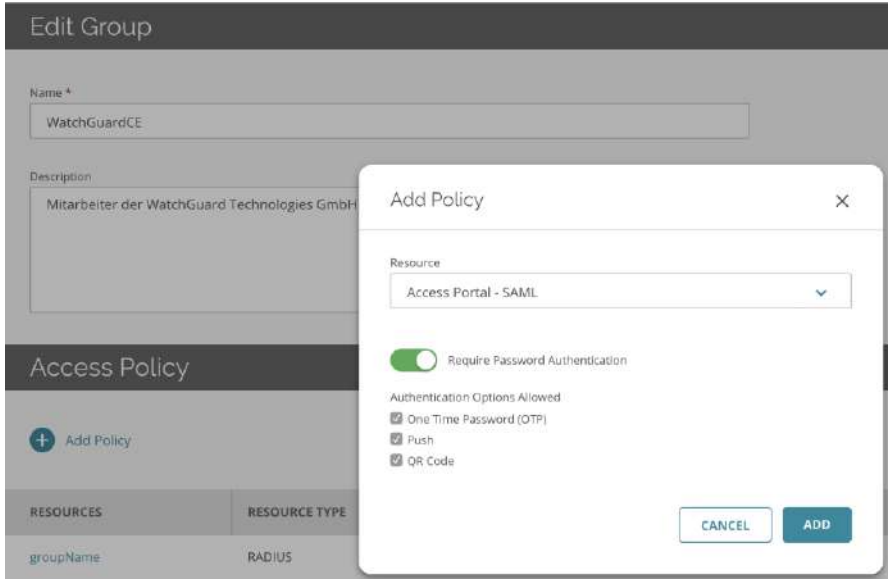
Konfiguration von WatchGuard AuthPoint



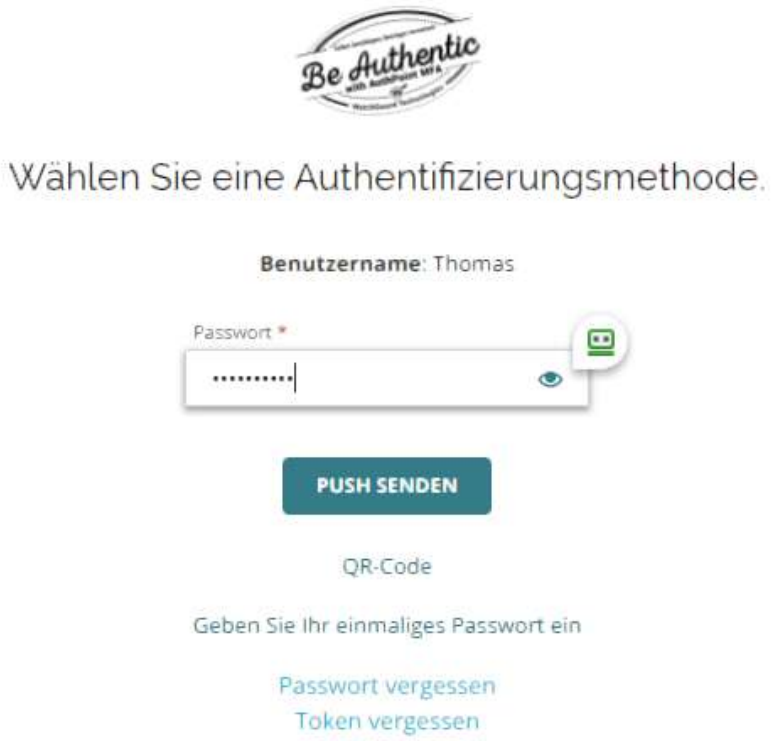
- Die Daten aus dem Access Portal übernehmen (Copy & Paste).
- Überprüfen, ob das richtige AuthPoint Zertifikat ausgewählt wurde.

Konfiguration von WatchGuard AuthPoint

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



Test

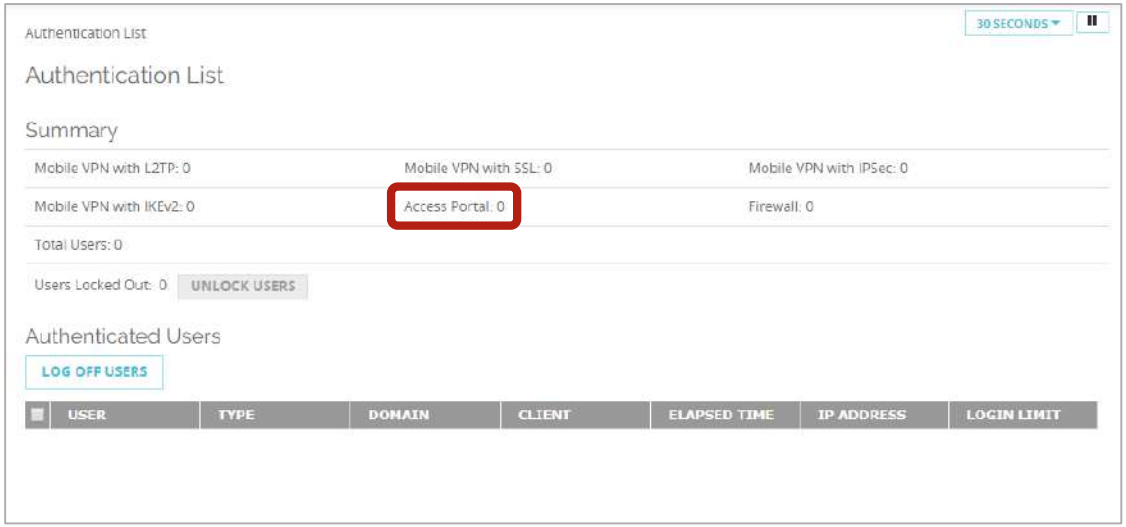


- Anmelden an dem Access Portal der Firewall
  - https://<FQDN der Firebox>
- Auswahl der MFA Authentifizierung
  - Gewählter IdP Name im Portal
- Auf dem IdP-Portal anmelden
  - Je nach zugelassener Methode

Weitere Informationen

Access Portal — Authenticated Users

- Sie können die Benutzer sehen, die mit dem Access Portal verbunden sind:
  - Auf der Fireware-Webbenutzeroberfläche auf der Seite Systemstatus > Authentifizierungsliste



Access Portal — Diagnostic Log Level

- Sie können auch die Diagnoseprotokollierungsstufe für Access Portal-Verbindungen festlegen
  - Gehen sie unter System > Diagnostic Log
  - Legen Sie im Abschnitt **Security Subscriptions** die Protokollstufe für die Option Zugriffsportal fest


Live Demo