



# Best-Practices – WatchGuard Access Portal mit MFA Integration

Thomas Fleischmann

Senior Sales Engineer, Central Europe  
[Thomas.Fleischmann@watchguard.com](mailto: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

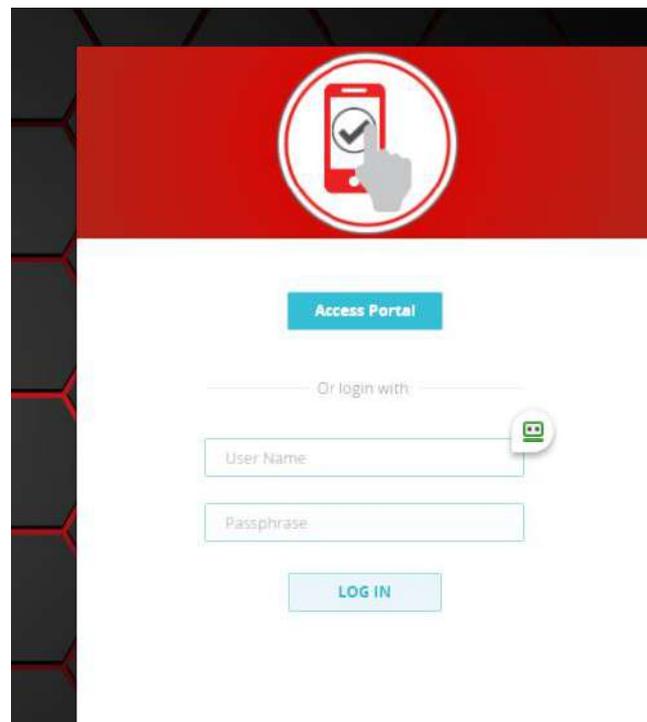
# Schnittstellen

- 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.

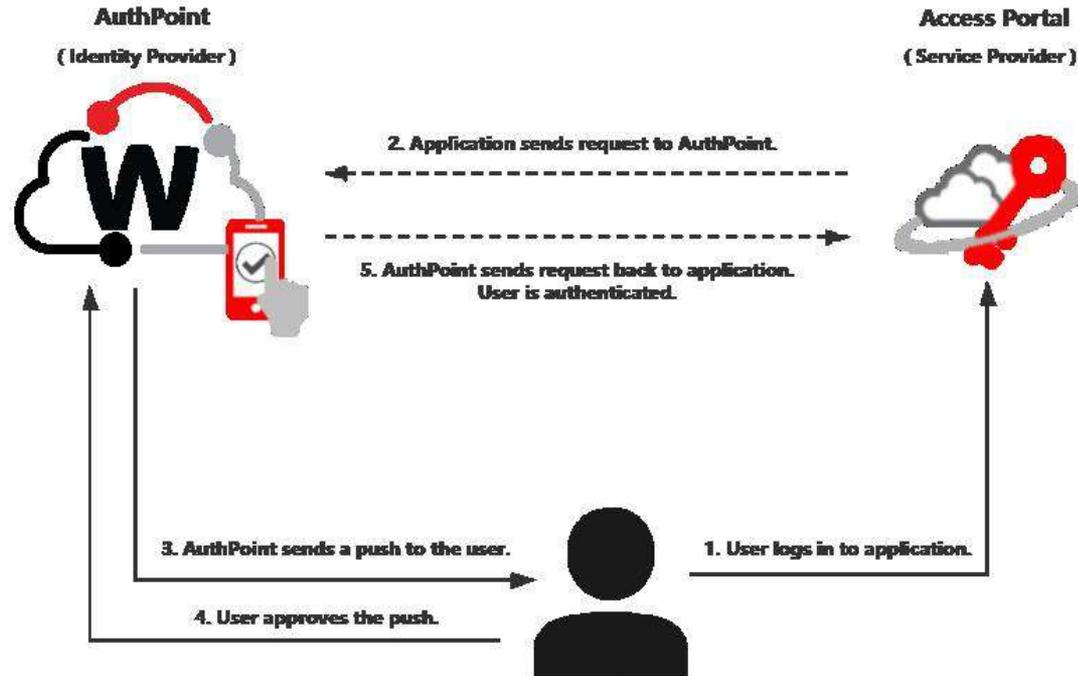
# Schnittstelle

- 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

The background of the slide is a vibrant red color. It features a stylized world map in a darker shade of red, overlaid with a network of white and light red lines that represent global connectivity. The lines form a grid and various circular paths, suggesting a digital or network environment. The overall aesthetic is modern and technological.

# WatchGuard Access Portal - Integration WatchGuard AuthPoint

# 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](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.

The screenshot shows the WatchGuard Cloud interface for managing certificates. At the top left, there is a '+ Add Certificate' button. To the right is a search bar with a magnifying glass icon. Below this is a table with the following columns: Id, Creation Date, and Expiration Date. The table contains one row with the following data:

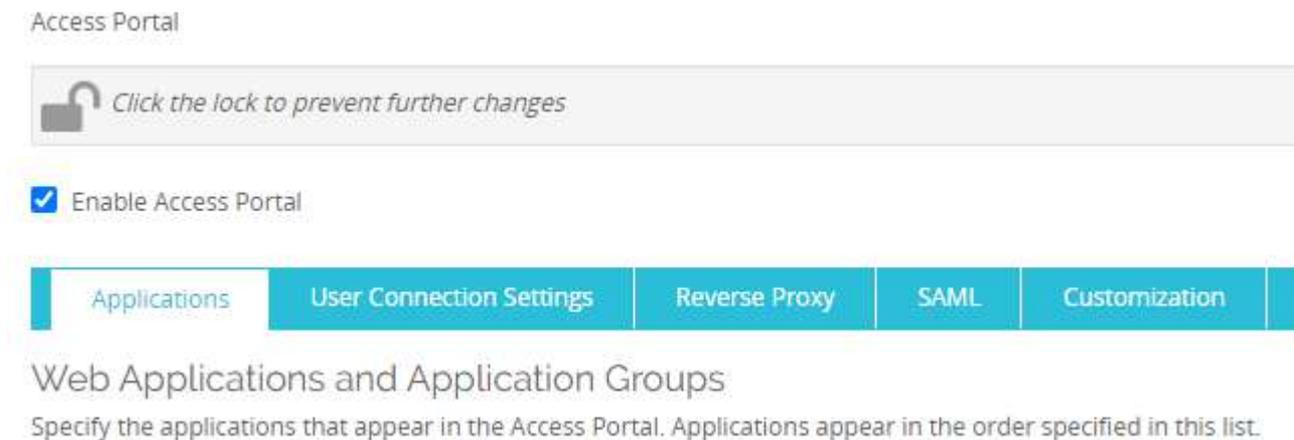
| Id                                   | Creation Date | Expiration Date |
|--------------------------------------|---------------|-----------------|
| 1a1be4ed-9bed-4dba-aeec-ee740e53673b | May 6, 2019   | May 6, 2029     |

Below the table is a 'BACK' button. A context menu is open over the first certificate, showing the following options:

- Copy Fingerprint
- Copy Metadata URL
- Download Certificate
- Download Metadata
- Delete

# 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.

## Access Portal



Click the lock to prevent further changes

Enable Access Portal

Applications

User Connection Settings

Reverse Proxy

SAML

Customization

To authenticate Access Portal users with SAML single sign-on, the Firebox exchanges authentication information



Enable SAML

Service Provider (SP) Settings

# Konfiguration des WatchGuard Access Portals

Enable Access Portal



To authenticate Access Portal users with SAML single sign-on, the Firebox exchanges authentication information with an Identity Provider (IdP) you specify.

Enable SAML

## Service Provider (SP) Settings

To configure your Firebox as the SAML Service Provider, specify the name of your IdP to appear as the authentication server name.

IdP Name

For the Host Name, specify a fully qualified domain name that resolves to the Firebox external interface.

Host Name  DNS Name des Dienstanbieters

After you save the configuration to your Firebox, follow the IdP configuration instructions at <https://accessportal.cybersec.watch/auth/saml>

SAML Konfiguration Seite

## Identity Provider (IdP) Settings

Specify the SAML connection settings for your third-party Identity Provider.

IdP Metadata URL  META Daten Link von AuthPoint

Group Attribute Name

# Konfiguration des WatchGuard Access Portals

## Option 2

Provide these details to your IdP administrator.

SAML Entity ID

COPY

Authpoint: Service Provider Entity ID

Assertion Consumer Service (ACS) URL

COPY

AuthPoint: Assertion Consumer Service

Single Logout Service (SLS) URL

COPY

AuthPoint: Logout URL

X.509 Certificate

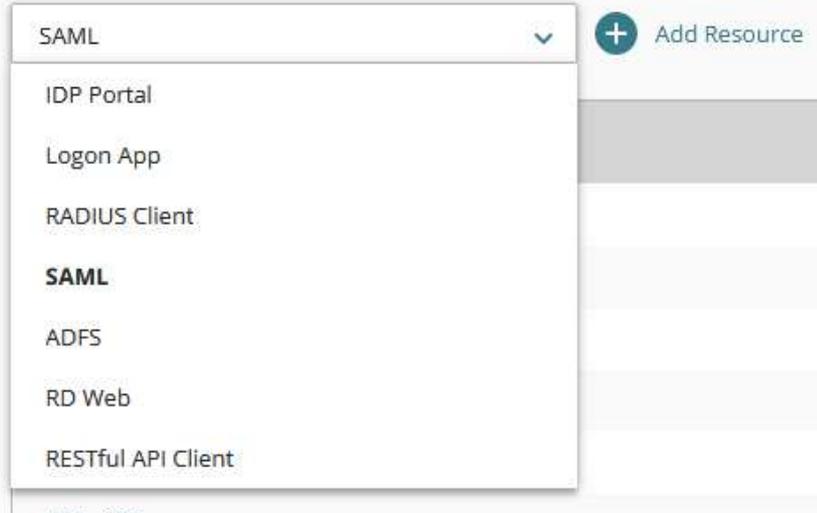
```
-----BEGIN CERTIFICATE-----
MIIDpTCCAo2GAWiBAGlEWSyE8TANBgkqhkiG9w0BAQsFADBHMRRmEQYDVQKKEwpX
YXRjaEd1YXJkMREwDwYDVQLLEwhGaxJld2FyZTEdMBSGA1UEAxMURmlyZXdhcmUg
c2FtbCBDbGllbnQwHhcNMjgwMzA2MTEwMzUzWhcNMjgwMzA2MTEwMzUzWjBHMRRm
EQYDVQKKEwpYXRjaEd1YXJkMREwDwYDVQLLEwhGaxJld2FyZTEdMBSGA1UEAxMUR
mlyZXdhcmUgc2FtbCBDbGllbnQwggEIMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQD1fkiW7Me8AHOw/rdDtoFmQ81nhQi3Ys997wQf7i0PcYqGfxTq2D70KPrI
Pazbb3ZTfoExo9qKN11b9sow/QPK9cEX8ncp7viEP1gExM3q5tZmM8OrV+35OrPG
PWzq6OEJYUgIt1PQ3wKrX4VDeHmMHwzvekobG44y4ytLzJbzoclR3mhvJdAX/B
YNQdKdQ349/1i90C7x8a3UFUpDp/9Yb3id50DLCTrJbzU5jNeQTSgKiOXVEjWhTX
clQGSso826A8W34DOXaNC7//BBMOXiDBOBh9iRXRPxjlgjwc421QaOe8/pMP1MhO
tnF3X1qQbTpS1YqFwh+2bXCptl2/AgMBAAGjgZGwgZUwJgYDVR0RB8wHYIBYWNj
-----END CERTIFICATE-----
```

DOWNLOAD CERTIFICATE

COPY

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

**SAML**

Name \*  
Access Portal

Application Type (Integration Guide) \*  
Firebox Access Portal

Service Provider Entity ID \*  
http://accessportal.cybersec.watch/auth/saml

Assertion Consumer Service \*  
http://accessportal.cybersec.watch/auth/saml/acs

User ID email or redirection to service provider \*  
Email

Logout URL  
http://accessportal.cybersec.watch/auth/saml/sls

Signature Method  
SHA-256

SAML Version  
2.0

Certificate  
CHANGE FILE Remove file  
Encryption enabled

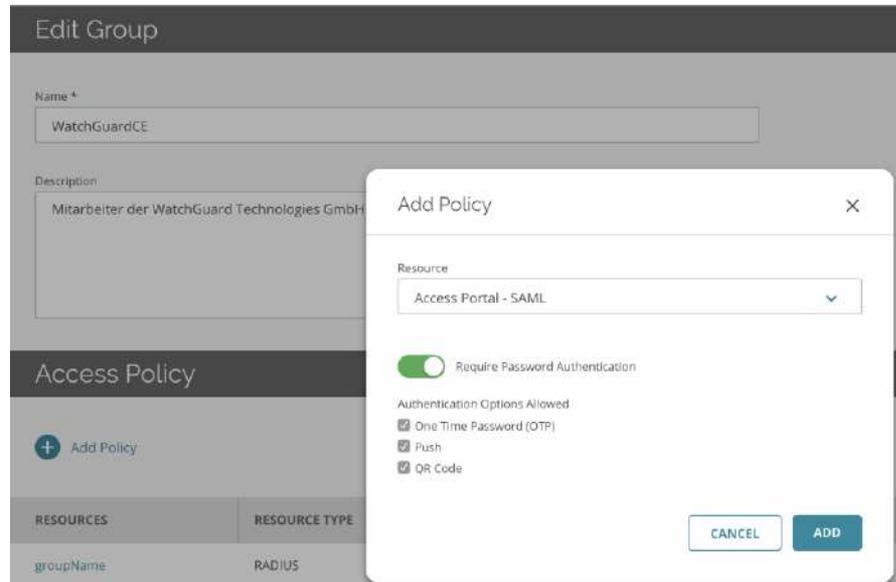
AuthPoint Certificate \*  
1a1be4ed-9bec-4dba-aeec-ee740e53673c - Expiration date: May 6, 2029

CANCEL SAVE

- 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



Wählen Sie eine Authentifizierungsmethode.

**Benutzername:** Thomas

Passwort \*

.....

**PUSH SENDEN**

QR-Code

Geben Sie Ihr einmaliges Passwort ein

[Passwort vergessen](#)

[Token vergessen](#)

- 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 Firewall-Webbenutzeroberfläche auf der Seite Systemstatus > Authentifizierungsliste

Authentication List 30 SECONDS ⏸

### Authentication List

#### Summary

|                          |                         |                          |
|--------------------------|-------------------------|--------------------------|
| Mobile VPN with L2TP: 0  | Mobile VPN with SSL: 0  | Mobile VPN with IPsec: 0 |
| Mobile VPN with IKEv2: 0 | <b>Access Portal: 0</b> | Firewall: 0              |

Total Users: 0

Users Locked Out: 0 UNLOCK USERS

#### Authenticated Users

LOG OFF USERS

| USER | TYPE | DOMAIN | CLIENT | ELAPSED TIME | IP ADDRESS | LOGIN LIMIT |
|------|------|--------|--------|--------------|------------|-------------|
|------|------|--------|--------|--------------|------------|-------------|

# 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



The image features a central globe rendered in a dark red color, showing the continents of North and South America. The globe is surrounded by a complex network of white, glowing orbital lines that intersect at several points, each marked with a small white dot. A prominent horizontal red band with a slight gradient passes through the center of the globe, serving as a background for the text. The overall aesthetic is futuristic and technological, with a monochromatic red color scheme.

**Live Demo**



**Danke !**