



# Best Practices – Firebox Access Portal – Integration mit Multi Faktor Authentifizierung

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.
- Die Lizenz für das Access Portal ist Bestandteil der Total Security Suite (TSS) von WatchGuard.
- Das Access Portal funktioniert **nicht** auf folgende Produkten: XTM, XTMv, T Series, M200 oder M300.
- Das Access Portal unterstützt FireboxV, FireboxCloud, und alle anderen Firebox Modelle (M370 oder höher).

The background of the slide is a vibrant red. 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. Several glowing white nodes are scattered across the map, and there are subtle light effects and lens flares, giving it a high-tech, digital feel.

# Schnittstellen zu Multifaktor Authentifizierungen

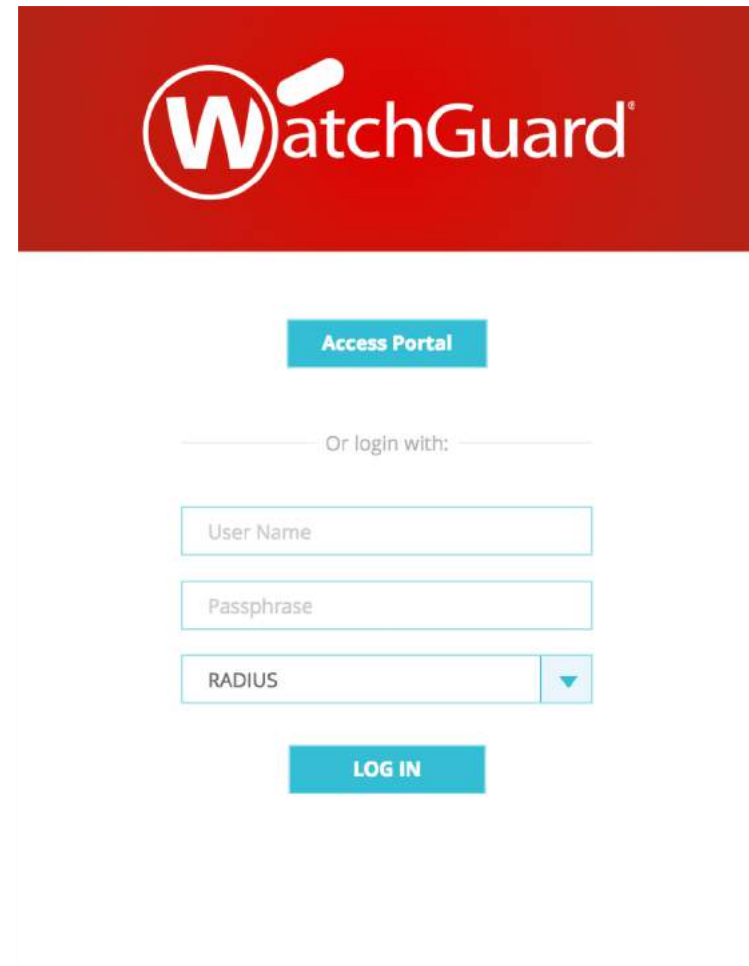
# Schnittstellen

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

- RADIUS

oder

- SAML 2.0



The screenshot shows the WatchGuard Access Portal login page. At the top, there is a red header with the WatchGuard logo. Below the header, there is a blue button labeled "Access Portal". Underneath, there is a section for "Or login with:" followed by three input fields: "User Name", "Passphrase", and a dropdown menu currently set to "RADIUS". At the bottom of the form, there is a blue button labeled "LOG IN".

# 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

A red-themed background featuring a stylized world map with white grid lines and glowing red lines representing a network or data flow. The text is centered in white.

# WatchGuard Access Portal - Integration WatchGuard AuthPoint

# 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](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](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.

## Resources

Choose a resource type 

ADD

NAME	TYPE
Access Portal	SAML
groupName	RADIUS Client
LogonApp	Logon App
Salesforce	SAML
WGDCE	IdP Portal

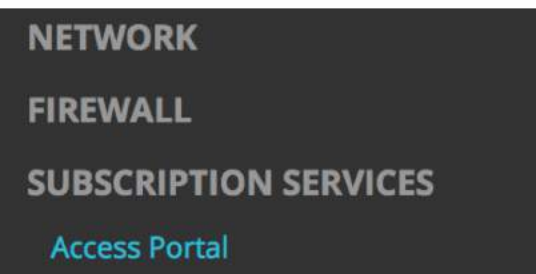
DOWNLOAD METADATA

DOWNLOAD CERTIFICATE

COPY SAML METADATA URL

# 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.



Enable Access Portal

Applications

User Connection Settings

SAML

Customization

# 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.

Enable Access Portal

Applications

User Connection Settings

SAML

Customization

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

# 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 Dienstansbieters

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-----
MIIDpTCCAo2gAwIBAgI EWsYE8TANBgkqhkiG9w0BAQsFADBHMRMwEQYDVQQKEwpX
YXRjaEd1YXJkMREwDwYDVQQLEWhGaXJld2FyZTEdMBsGA1UEAxMURmlyZXdhcmUg
c2FtbCBDDbGllbnQwHhcNMTEwMzA2MTEwMzUzWWhcNMjgwNDYyMTEwMzUzWjBHMRMw
EQYDVQQKEwpYXRjaEd1YXJkMREwDwYDVQQLEWhGaXJld2FyZTEdMBsGA1UEAxMU
RmlyZXdhcmUgc2FtbCBDDbGllbnQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQD1fKfW7Me8AHOw/rDToFmQ81nhQi3Ys997wQf7I0PcYqGfxTq2D70KPrI
Pazbb3ZTfoExo9qKNI1b9sow/QPK9cEX8ncp7viEP1gExM3q5tZmM8OrV+35OrPG
PWzqo6OEJYuYGI1PQ3wKrX4VDeHmMHwzvekobG44y4ytLzJbzoclR3mhvJdAX/B
YNQdKdQ349/1i90C7x8a3UFUpDp/9Yb3ldS0DLctRjzbzU5JNeQTsgKIOXVejWhTX
clQG5so826A8W34DOXAnc7//BBMOXiDBOBh9iRXRPxJlgjwc421QaOe8/pMP1MhO
tnF3X1qQbTpS1YqFwh+2bXCptl2/AgMBAAGjgZGwgZUwJgYDVR0RB8wHYIbYWNj
-----END CERTIFICATE-----
```

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).

## SAML

Name \*

Service Provider Entity ID \*

Assertion Consumer Service \*

User ID

Logout URL

Signature Method

SAML Version

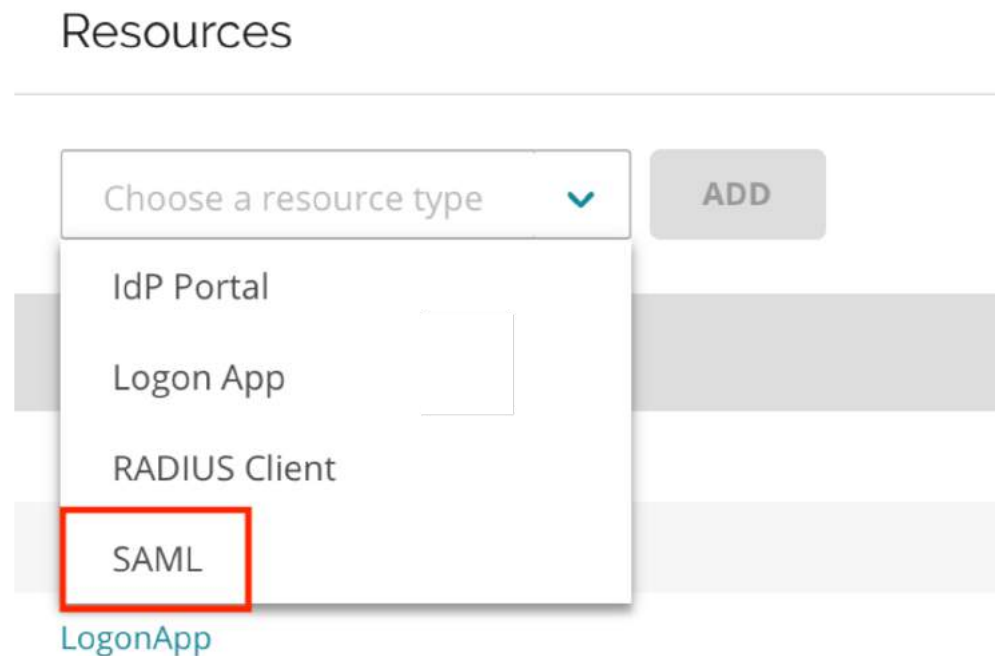
Application Type \*

Certificate

[CHANGE FILE](#) [Remove file](#)

# 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.

**Edit Group**

Name \*  
WatchGuardCE

Description  
Mitarbeiter der WatchGuard Technologies GmbH

**Access Policy**

+ Add Policy

RESOURCES	RESOURCE TYPE
groupName	RADIUS

**Add Policy**

Resource  
Access Portal - SAML

Require Password Authentication

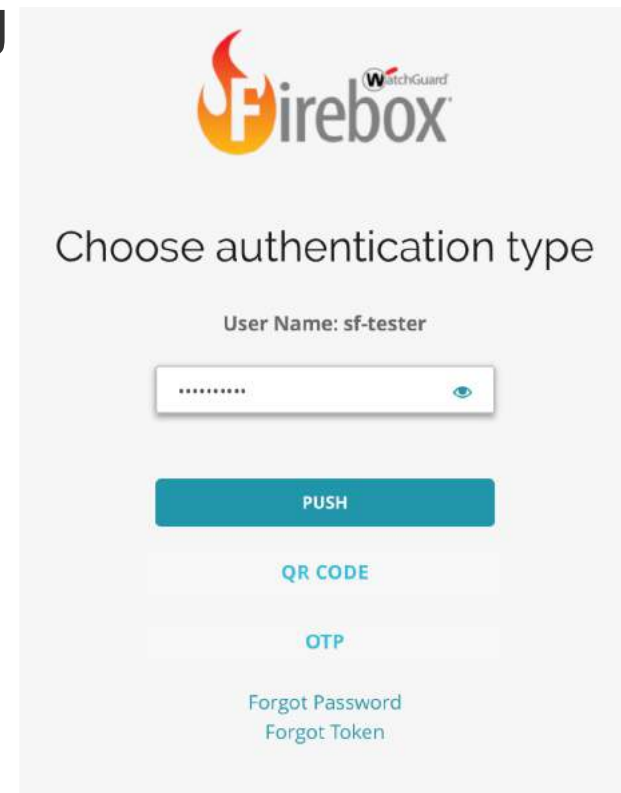
Authentication Options Allowed

- One Time Password (OTP)
- Push
- QR Code

CANCEL ADD

# 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

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

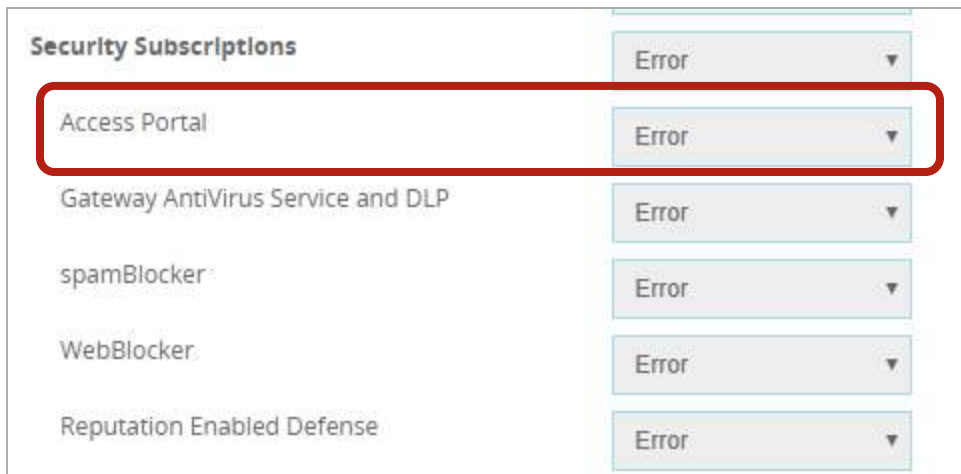
Authenticated Users

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





**Live Demo**





**Danke !**