Rohde & Schwarz Cybersecurity

WEB ACCESS MANAGER

Simplify access and increase application security of R&S®Web Application Firewall

The proliferation of applications and their corresponding passwords poses a challenge for the IT departments in companies. It has become difficult for them to protect company data and attend to tickets for password resets. There is a strong need to identify users but it is inconvenient for users to remember too many passwords. Users spend too much time logging into individual applications. Moreover, security breaches mostly originate from vulnerabilities caused by poor password practices. When it comes to cloud services, it is also important to know who has access to which applications and how they are using them. Single sign-on (SSO) portals without multi-factor authentication (MFA) can lead to decreased security. Businesses need the capability to enforce the same level of security for all their applications.

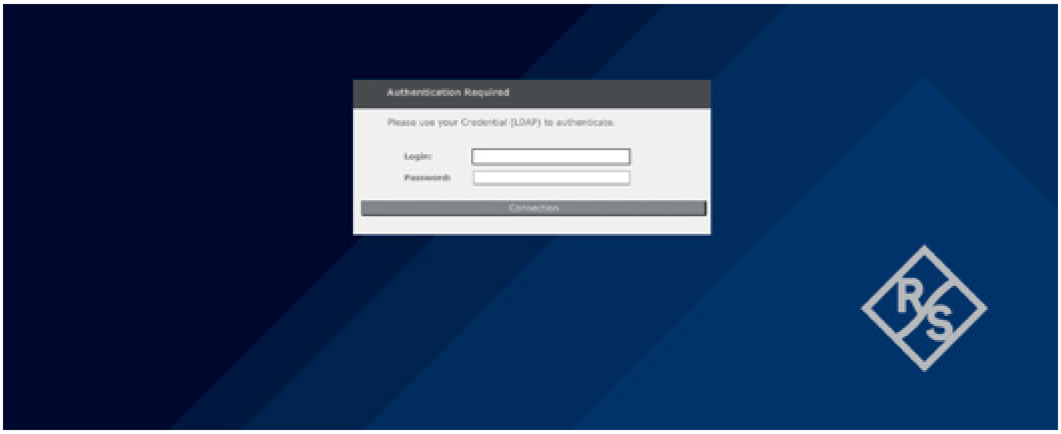
Solution overview

The Web Access Manager (WAM) is a part of Identity and Access Management (IAM) that controls access to web applications by providing various services including web single sign-on (WebSSO). WebSSO is a functionality allowing access to multiples applications based on one single user authentication while maintaining access control and authorization rules during the user's session. For authentication, the world of WebSSO is divided into two types of entities:

- Identity providers:
  a component that certifies the identity of an individual based on authentication factors and propagates that identity using cryptographic tokens (SAML Assertion, JSON Web Token, encrypted cookies, etc.)
- Service providers:
  a component that provides the application and it is the identity consumer (cryptographic token)

The Web Access Manager can handle the previous case using an Active Directory, a SQL database, or a radius server for multi-factor authentication (MFA).

Therefore, the web single sign-on integrated in the R&S®Web Application Firewall enables it to have better policies and plays a key role in optimizing security for both modern and legacy applications.

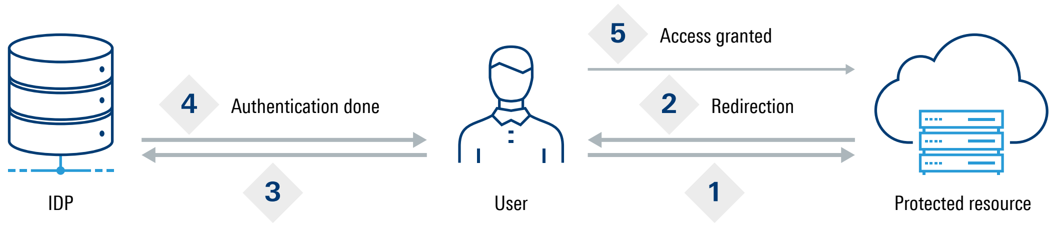


Please use your Credential (LDAP) to authenticate.

Web single sign-on portal

ROHDE & SCHWARZ

Make ideas real



SAML authentication

Benefits

- **Simplification & centralization of user access to all web applications**
  Password fatigue presents a major challenge. Thanks to WebSSO, only one credential is to be remembered for different applications and it does not have to be reentered until the end of the day. This ability to increase end user productivity and convenience is one of its greatest benefits.

- **Agentless approach, very transparent for applications**
  Being the single point of control for authentication and authorization, WebSSO increases rationalization and promotes easy management. It allows complete traceability of who has access to what via a central audit.

- **Adaptive & secure authentication based on the context (Risk-Based Authentication)**
  It enables monitoring of user behavior, geolocation, device details to add an extra layer of security. Overall, WebSSO integrated into R&S®Web Application Firewall makes it relevant for all the different security scenarios, which in turn is one of the key reasons why customers prefer to buy R&S®Web Application Firewall.

- **Combination of different authentication factors (multi-factor authentication) from different directories (B2E, B2B, B2C)**
  WebSSO combined with MFA improves security by providing the authentication for all the protected applications. It checks if the user is active, or if the password has expired in which case user is redirected to a change password screen. It creates an encrypted session throughout so that the user can be securely authenticated.

How it works

Authorization is done using LDAP group (RBAC or Role Based Access Control), but it can also be defined based on attribute (ABAC or Attribute Based Access Control). The authentication sequence is very simple (here an example of SAML):

1. User connects to the protected resource.
2. If it is not authenticated, it is redirected to the Identity Provider (IDP) for authentication.
3. It authenticates on the IDP.
4. Once authenticated and authorized, it is redirected to the protected resource.
5. The proof of authentication is validated and the user can access the protected resource.

SAML is mostly used for enterprise SSOs. Like SAML, OAuth is another protocol for providing delegated authorization of resources. The OAuth process is similar to the SAML process detailed here.

After perimeter authentication of the user on WebSSO, its authentication is propagated on the application by different credentials propagation protocols like credentials replay, HTTP header etc.

Rohde & Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

Rohde & Schwarz GmbH & Co. KG
www.rohde-schwarz.com

PD 3607.6867.32 | Version 01.00 | October 2020 (sch)
Web Access Manager
Data without tolerance limits is not binding | Subject to change

3607686732