WatchGuard Access Portal

Extending WatchGuard protection to business-critical assets in the cloud

What is the Access Portal?

Access Portal, part of WatchGuard's Total Security Suite (TSS), is a service that allows you to quickly and easily deploy centralized access for your cloud-hosted application services. Designed with organizations in mind that rely on cloud resources, the Access Portal allows small and midsize businesses to avoid expensive authentication deployments. Access Portal includes an HTML5 application portal, SSO support for RDP/SSH intranet services, and SAML 2.0-enablement for reduced administrative burden. Adoption of cloud platforms and related services are set to grow at a 22% CAGR between 2015 and 2020 to $236B, controlling access to sensitive assets in the cloud is essential.

What is SAML 2.0?

Security Assertion Markup Language (SAML) is a standard for logging users into applications based on their sessions in another context. This single sign-on (SSO) login standard has significant advantages over logging in using a username/password:

- No need to type in credentials
- No need to remember and renew passwords
- No weak passwords

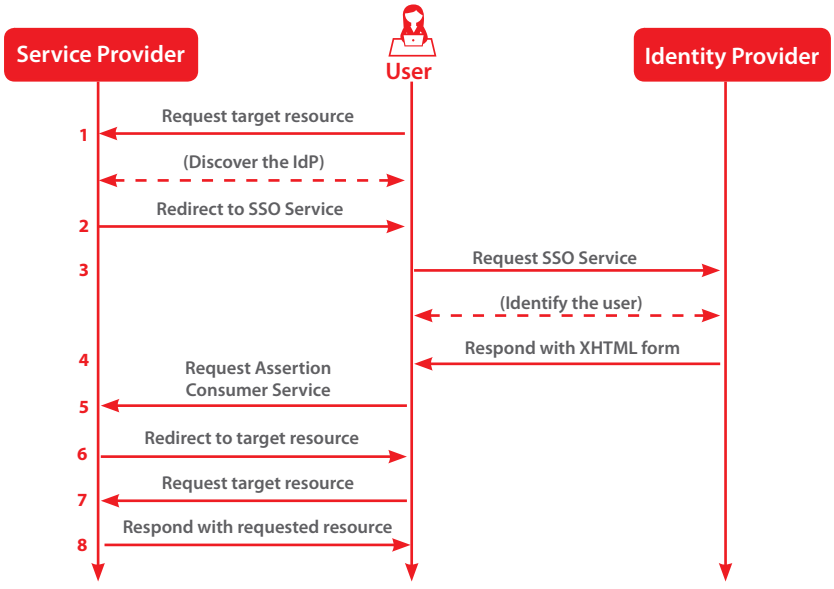
Most organizations already know the identity of users because they are logged in to their Active Directory domain or intranet. It makes sense to use this information to log users in to other applications, such as web-based applications, and one of the more elegant ways of doing this is by using SAML.

How does SSO work with SAML 2.0?

SAML SSO works by transferring the user's identity from one place (the identity provider) to another (the service provider). This is done through an exchange of digitally signed XML documents.

Consider the following scenario: a user is logged into a system that acts as an identity provider (IdP). The user wants to log in to a remote application, such as for office productivity software (the service provider or SP). The following happens:

1. The user accesses the remote application using a link on an intranet, a bookmark, or something similar and the application loads.
2. The application identifies the user's origin (by application subdomain, user IP address, or similar) and redirects the user back to the IdP asking for authentication. This is the authentication request.
3. The user either has an existing active browser session with the IdP or establishes one by logging into the IdP.
4. The IdP builds the authentication response through an XML form containing the user's username or email address, signs it using an X.509 certificate, and posts this information to the SP.
5. The SP, which already knows the IdP and has a certificate fingerprint, retrieves the authentication response and validates it using the certificate fingerprint.
6. The identity of the user is established and the user is provided with entry into the Access Portal application store.



How does the Access Portal change Authentication?

The Access Portal can be enabled as a service provider – and through the digital signing of certificates with your selected identity provider – can be another point of access for the user to initiate logins for IT admins desiring centralized access to RDP and SSH resources residing on the company intranet.

For the privileged user, the Access Portal can be shifted and expanded into a central service for logging into web applications hosted externally to the company intranet. WatchGuard's Access Portal service fully supports popular IdPs for organizations desiring MFA solutions. Compatibility with the following identity providers is available:

- Shibboleth
- OneLogin
- Okta
- ADFS (Active Directory Federation Services)

Popular software tokens that can be used in conjunction with the Access Portal include:

- RSA SecureID
- Duo Mobile
- OneLogin Protect
- Google Authenticator
- Okta Mobile

Top Firebox® Use Cases

WSSO to Privileged Intranet

To provide protection to secure shell or remote desktop servers, the WatchGuard Access Portal can be configured for strong authentication to enable multi-factor authentication and SSO workflows for convenient and secure access to intranet resources via RDP/SSH.

Clientless Access for Remote Network Administrators

The privileged network administrator needs a central point of reference to access cloud-hosted office productivity software such as O365, One-Drive, Box, etc. The WatchGuard Access Portal offers privileged account access as well as IdP-initiated SSO for such office productivity products in one centralized location. With SAML 2.0, the Access Portal can be configured through the IdP provider for centralized remote access.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, and network intelligence products and services to more than 80,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com