

Cloud Single Sign-On (SSO)

Simplify and Unify SSO for On-Premise, B2B and Cloud with Axway API Gateway



Serving as a unified federation gateway, Axway API Gateway enables single sign-on to any combination of cloud-based services, traditional B2B services and on-premise applications.

Without proper planning, cloud-based services can easily become technology silos, particularly in the area of security. To avoid creating yet another IT island, it is best to enable single sign-on (SSO) using a federation standard instead of manually creating separate user accounts or provisioning user identities into each service. Fortunately, in the last five years, Security Assertion Mark-up Language (SAML) has become widely adopted by all major cloud service providers.

Axway API Gateway can be deployed as a unified federation gateway enabling SAML-based SSO access to any combination of cloud-based services, traditional B2B services and on-premise applications.

Mediate identities and security tokens

Despite best efforts to reduce the number of access control systems and identity repositories, few organizations have only one. In addition to SAML, a typical large organization has to deal with the proprietary token from its enterprise identity and access management (IAM) platform, the Kerberos ticket from its Microsoft technology stack, tokens from legacy systems, tokens from bespoke B2B integrations, and more than a few forms of certificates.

Axway API Gateway has a built-in Security Token Service (STS) that can exchange any standard-based or proprietary token, allowing any enterprise application — new or legacy, Microsoft or Java — to SSO to cloud-based services. The STS also manages trust relationships using standards such as WS-Trust and WS-Federation.

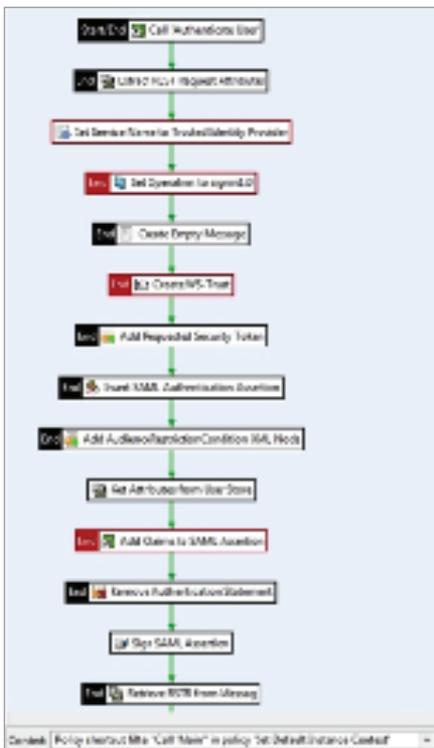
Axway API Gateway is a next-generation technology that enables enterprises to standardize the API development and delivery capabilities required to provide business services via cloud, mobile and partner channels. Encapsulating application gateway, cloud service broker and identity middleware functionality in a unified platform, it provides an agile API environment that leverages existing back-end applications, services and data to help speed time-to-market for new business services.

Axway API Management Solution Pack is a dedicated API management solution that works with Axway API Gateway to simplify all aspects of publishing, promoting and managing APIs in a secure, scalable environment.



Other Axway API Gateway Solutions include:

- API and SOA Security
- API Identity and Access Federation
- Application Services Governance
- Bring Your Own Device (BYOD)
- Cloud API and Service Brokering
- Cloud Data Security
- Cloud Identity Service
- Fine-Grained Authorization
- Mobile API
- SharePoint Gateway



Example of a token mediation policy

Integrate with IAM platforms

Most medium and large organizations have at least one enterprise-wide IAM platform from a leading vendor such as CA, IBM, Oracle or RSA. To avoid creating additional identity and policy silos, SSO to cloud-based services should be integrated with the IAM platform. Unfortunately, this is not a trivial task because IAM products use proprietary tokens, their SAML support is poor, and their OAuth support is even worse. In addition, because existing IAM platforms are highly user- and browser-centric, SSO to cloud-based APIs often require heavy customization.

Axway API Gateway provides out-of-the-box integrations to all leading IAM platforms and extends them with seamless SAML/OAuth support and API access control, including SSO to cloud-based APIs and client- and application-based authentication.

In addition, Axway API Management Solution Pack enables secure administration and storage of all forms of API and SOA security artifacts such as tokens, keys and certificates.

Integrate with IAM-as-a-Service (IAMaaS) offerings

Since the leading IAM platforms have poor cloud SSO support, many organizations have adopted IAM-as-a-service (IAMaaS) offerings such as Okta, Symplified, and VMware Horizon Application Manager, which are essentially cloud-based SAML Security Token Services.

For organizations using IAMaaS to supplement an on-premise IAM platform, Axway API Gateway helps to integrate the two. For organizations using only IAMaaS, Axway API Gateway provides a policy enforcement point (PEP) that enables users who have signed in at the IAMaaS to SSO to any on-premise application.

For More Information, visit www.axway.com

Copyright © Axway 2013. All rights reserved.

