



## Security matters.

Protect your investments and bring your IT infrastructure to a secure next level

### OpenAM

OpenAM technology underpins many of the globe's largest corporate and government agency security infrastructures. Here is why and how you can leverage the power and security of OpenAM in your organization.

When companies extend their business, connecting to external partners or offering companies' services externally, the complexity of securing the resources becomes a real challenge. The need to keep the business risk at a minimum while still providing a scalable and secure infrastructure to meet the requirements from partners and service providers becomes essential to enable an organization to compete successfully in the network economy. Traditionally this challenge has been approached using multiple solutions addressing each of the constituent requirements to fulfill access management: authentication, authorization, federation, secure web services, and fine grained entitlements. However, as the network environment continues to grow larger and more complex, this approach is becoming increasingly difficult, costly and, ultimately, unsustainable.

Rather than trying to meet these requirements using multiple solutions, a single integrated approach is recommended as best practice. With a single solution for managing authentication, authorization, and personalization for Web, federated, and Web services environments, companies can secure the access to core business assets with OpenAM.

OpenAM provides a comprehensive solution for **centralized authentication** and **authorization** services, **single sign-on (SSO)** between multiple network applications, and **federation** with other organizations.

Users benefit from an OpenAM deployment by having to log in only once, rather than for every application they require, and by not having to remember multiple passwords. Administrators benefit from the **centralization of user accounts** and **access policies** which reduces the amount of time taken to set up and manage user access. For stronger security, integration with **token cards** and **digital certificates** is seamless. User authentication and application access are audited.

**Federation** provides the opportunity to leverage services from other organizations, such as customers, partners, suppliers or cloud service providers such as **Google**, **Salesforce.com** and many others. It has also been used successfully to allow **rapid integration** in company mergers and acquisitions.

Integration with applications is achieved in the following ways:

- ✓ **Policy Agents**, for web and application servers
- ✓ Open Identity Gateway, OpenIG, for integration with legacy applications without even touching the target application
- ✓ Federation, based on standards i.e. **SAML 2.0**
- ✓ **"Fedlets"**, light-weight federation support for .NET services and Java
- ✓ **OAuth** for Web 2.0 applications
- ✓ Custom integration using **AMSDK**

**OpenAM** is a fully **Open Source** project originally branded as OpenSSO by Sun Microsystems, and now overseen, developed and supported by ForgeRock. ForgeRock's goal is to deliver the most free and comprehensive **next-generation** access management product to enterprise customers across the globe.

# Functionality

## Access Management

OpenAM manages authorized access to network services and resources. By implementing authentication and authorization, OpenAM (along with an installed policy agent) ensures that access to protected resources is restricted to authorized users.

It supports 18 out of the box authentication methods and the possibility to extend by developing Custom Authentication Modules (Plugins), based on JAAS. A Risk Based Authentication module can assess the conditions to determine if more credentials or a different challenge is needed to identify the user.

## Entitlements

OpenAM provides both a coarse-grained policy engine and a fine-grained entitlements service based on XACML (eXtensible Access Control Markup Language).

## Federation

With the introduction of federation protocols into the process of access management, identity information and entitlements can be communicated across security domains, spanning multiple trusted partners.

OpenAM supports several open federation technologies including the Security Assertion Markup Language (SAML) versions 1 and 2, WS-Federation, and the Liberty Alliance Identity Federation Framework (Liberty ID-FF), therefore encouraging an interoperable infrastructure among providers.

OpenAM can also be configured as a SAML 2.0 SP, IdP and IdP Proxy.

It supports federation standards like: SAML1.x, SAML2 (SP, IdP, ECP and IdP Proxy), WS-Federation (Asserting and relying party), Liberty ID-FF 1.x.

## Securing Web Services

OpenAM ensures the integrity, confidentiality and security of web services through the application of a comprehensive security model is critical for both enterprises and consumers. A successful security model

associates identity data with the web services and creates secure service-to-service interactions. The security model adopted by OpenAM identifies the user and preserves that identity through multiple interactions, maintains privacy and data integrity, uses existing technologies, and logs the interactions.

Supported Web Services Security standards are Liberty ID-WSF 1.x, WS-I Basic Security Profile, WS-Trust (STS) and WS-Policy.

## Identity Web Services

OpenAM exposes functions as simple identity web services allowing developers to easily invoke them when developing their applications. Identity Web Services are available using:

- ✓ SOAP and Web Services Description Language (WSDL)
- ✓ Representational State Transfer (REST)

## Policy Agents

OpenAM provides a number of policy agents that are available for a variety of web servers and J2EE application servers. Policy Agents protect the content on the web server or the application server. Before a user can access their requested content, they first must be authenticated to and authorized. OpenAM policy agents are extremely flexible and can be made to work in complex environments. A full list of Policy Agents is available on the ForgeRock website.

## Identity Gateway

For the integration of legacy applications to the SSO ecosystem, the Open Identity Gateway (OpenIG) addresses this problem and solves it without ever modifying or touching the target application. This greatly reduces the integration time.

OpenIG is a high-performance identity reverse-proxy with specialized session management and credential replay functionality.

## Core features

FEATURES	DESCRIPTION
Ease of Deployment	OpenAM is delivered as a Web application ARchive (WAR) that can be easily deployed as a Java EE application in different web containers. Most configuration files and required libraries are inside the WAR to avoid the manipulation of the classpath in the web container's configuration file. The OpenAM WAR is supported on several application servers.
Portability	OpenAM is supported on several operating systems
Open Standards	OpenAM is built using open standards and specifications as much as possible. For example, features designed for federation management and web services security are based on the Security Assertion Markup Language (SAML), the Liberty Alliance Project specifications, and the WS-Security standards.
Ease of Administration	OpenAM contains a web-based, graphical administration console as well as command line interfaces for configuration tasks and administrative operations. Additionally, an embedded, centralized data store allows for one place to store server and agent configuration data.
Security	<ul style="list-style-type: none"><li>✓ OpenAM services can be accessed by authorized entities only.</li><li>✓ Administration security ensures only authorized updates are made to the OpenAM configuration data.</li><li>✓ Deployment security implements best practices for installing OpenAM on different operating systems, web containers, and so forth.</li><li>✓ All security actions are logged.</li></ul>
Configuration Data Store	OpenAM writes the server configuration data to a centralized configuration data store.
User Data Store Independence	OpenAM allows you to view and retrieve user information without making changes to an existing user data. Supported directory servers include Directory Server 5.1, 5.2 & 6.2, IBM Tivoli Directory 6.1, Microsoft Active Directory 2003 and 2008, OpenDS 2.0 and 2.2, and OpenDJ 2.4 among others.
Performance, Scalability and Availability	OpenAM can be scaled horizontally and vertically to handle increased workloads and changing security needs over time. It is deployable in configurations that prevent single point of failure.
Distributed Architecture	Server and client components can be deployed across the enterprise or across domain boundaries as all application programming interfaces (API) provide remote access to OpenAM based on an identity-services architecture.
Flexibility and Extensibility	Many OpenAM services expose a service provider interface (SPI) allowing expansion of the framework to provide for specific deployment needs.
Internationalization	OpenAM contains a framework for multiple language support. Customer facing messages, API, CLI, and user interfaces are localized in the supported languages.
Authentication	OpenAM supports multiple authentication methods out-of-the-box, custom modules can be written using the extensibility features of the authentication framework.
Risk Based Authentication	The authentication framework can make a risk assessment to determine if additional challenges are needed to complete the process successfully.

## Authentication modules

AUTHENTICATION MODULE	DESCRIPTION
Active Directory	Authenticate your users stored in Active Directory
Anonymous	Ideal when you need to give customers guest access to public websites
Certificate	Provides strong authentication using X509 certificates
Data Store	Uses the user data store to perform authentication
Federation	Authenticate using a federation protocol such as SAML2
HTTP Basic	Browser based authentication
JDBC	Authenticate using user credentials stored in a database
LDAP	Valid your users using any LDAPv3 directory server
Membership	Allows users to self register, ideal for portals
MSISDN	Authenticates using their mobile number (via a WAP gateway)
OTP	Generates a One Time Password sent to the user via email or SMS
RADIUS	Authenticate a user using RADIUS
SAE	Used to authenticate during SAML2 Security Attribute Exchange
Windows Desktop SSO	Instant Single Sign On for Windows Desktop users
Windows NT	Authenticate users against a Windows NT domain
WSSAuth	Authenticate Web Service clients using Web Services Security
RSA SecurId	Authenticate against an RSA ACE server
SafeWord	Authenticate against a SafeWord server
Risk Based Authentication	Adaptive authentication for risk assessment

## History of OpenAM

OpenAM is the continuation of the open source project OpenSSO from Sun Microsystems. ForgeRock made the first release of OpenAM in February 2010 which was based on Build 9 of OpenSSO.

OpenSSO had its origins in the Sun Microsystems Sun Access Manager 7.1, "Sun Access Manager SAMLv2 Plugin" and "Sun Federation Manager 7.0". The 3 products from Sun were combined to create the open source project OpenSSO.

Since the initial release of OpenAM, more than 800 bugs, some of them severe, as well as security issues and improvements have been resolved. The OpenAM community has never been stronger, or more active. Release 10.0 of OpenAM (Q2 2012) is a major upgrade and sets the agenda for the next steps of a more modern architecture and many new important features.

## About ForgeRock

A global company with bases in the UK, USA, France and Norway, ForgeRock is committed to continuity of innovation and service for the existing and new open source interaction, identity, and integration software found within the I<sup>3</sup> platform. ForgeRock provides customers with enterprise-class subscriptions for the platform as well as training and access to an extensive partner community.

For more information, visit <http://www.forgerock.com>.

## Contact

- ✓ [info@forgerock.com](mailto:info@forgerock.com)
- ✓ phone: +47 21520108
- ✓ <http://www.forgerock.com>

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is provided "as-is" and not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. ForgeRock, OpenAM, OpenDJ and OpenIDM are trademarks of ForgeRock AS. All other product or service names are trademarks of their respective companies.

