

## Why Upgrade to OpenAM?

### Introduction

ForgeRock recommends customers running a version of the old Sun Identity Server or Access Manager product; review this document before deciding on the best path to upgrading their existing environment.

### Product Philosophy

ForgeRock believes in Open Source. The company is founded on these values and these values have been re-enforced through many years of the pain of working with closed proprietary software.

ForgeRock believes that a secure integrated Access Management solution using closed software can be expensive and full of unknowns thanks to the lack of code. Access Management project often require integration into customer environment and existing systems and must meet customers requirements.

ForgeRock experience is that an open source product coupled with excellent commercial support will provide the customer with best environment for a successful project.

### Installation

OpenAM can be up and running in minutes and has no external dependencies on your IT infrastructure other than a J2EE web container in which to run.

OpenAM is a single product that tightly integrates all of the required Authentication, Authorization, Entitlement and Federation functionality together into a single unit.

### Configuration

The product provides a web based administration interface that is simple to use and allows for quick configuration.

OpenAM provides configuration inheritance for both clusters of OpenAM servers and Policy Agents. Configuration inheritance means that an administrator only need change a configuration item in a single location and have the change take effect on all associated servers.

The majority of configuration underpinning OpenAM and Policy Agent 3.0 is now dynamic removing the requirement to restart.

### Production Deployment

OpenAM is now distributed a single industry standard J2EE war file, this encapsulation means the footprint of OpenAM on a production system is minimised.

OpenAM single war file deployment mode allows customisations to be fully integrated with the product allowing deployment to continue without impacting support staff.

OpenAM can be easily integrated into an automatic

install procedure such as Chef using the new deploy tools.

### Authentication

OpenAM features many different authentication mechanisms out of the box.

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

Most customers will find an authentication module that meets their needs out of the box. Some customers might require a simple customisation to one of the existing modules. OpenAM authentication modules are open source allowing customers immediate access to make their minor customisations. Customers will find complex requirements will find creating their own custom authentication modules is straightforward. OpenAM seamlessly integrates custom authentication modules into the product.

### Authorization and Entitlements

OpenAM has a tried and tested authorization mechanism used by the policy agents to protect access to web site and J2EE application resources. The latest release of OpenAM introduces a brand new entitlements mechanism accessed using the industry standard XACML language. The new entitlements framework is designed to support fine-grained

authorization requirements. OpenAM has kept the evaluation APIs backwardly compatible whilst providing new interfaces, such as RESTful, to speed integration.

## Integration

Customers often need to be integrate OpenAM into their existing environment and many customers can accomplish said integration by means of simple configuration. Customers with more complex and/or non-standard environments will require customisations in order to complete the integration. OpenAM has been designed around the plug-in plan. The plug-in plan is simple; customise a small component whilst leveraging the rest of the standard product. Since OpenAM is open-source, developers have access to all of the source code ensuring the task of implementing their customisation is a painless as possible. OpenAM has the following plug-in points:

- Authentication Modules: Implement your own authentication module and use it alongside the built-in modules in the usual way.
- Post Authentication Plug-in: Prepare your user for their OpenAM session.
- Policy plug-ins to implement custom policy: Custom the policy and entitlement frameworks to meet your fine grain authorisation requirements.
- Federation account and attribute mappers: Map your user accounts and user data into formats agree with your federation partners.
- Custom Data Stores: Integrate OpenAM with user data stores outside of the normal LDAP or relational database repositories.

OpenAM provides a full set of Java/C SDK and SOAP/RESTful web services to facilitate application integration.

## Federation

Federation is OpenAM's trump card and can be configured in minutes. OpenAM provides support for the following federation protocols:

- SAML2.0
- WS-Federation
- ID-FF
- Liberty ID-WSF 1.0 and 1.1

Federation allows for simple SSO and SLO between you and your partners different Access Management systems and OpenAM allows for this integration to happen quickly and easily.

At the heart of the OpenAM federation engine is the multi-protocol hub. The hub allows clients speaking different protocols to communicate transparently as OpenAM sits at the centre and translates. OpenAM comes complete with Federation validator to ensure everything is configured correctly.

## 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 application server. Before a user can access their requested content, they must first be authenticated to and authorized by OpenAM. OpenAM policy agents are extremely flexible and can be made to work in complex environments:

- Behind load balancers
- In clusters with shared central configuration
- Built-in POST data preservation caching.

A full list of available Policy Agents is available on the ForgeRock website.

## About ForgeRock

ForgeRock, founded in 2010, is a software company (ISV), whose core mission is to deliver an open source enterprise-class application platform to solve real customers needs. Our employees have solid experience with projects from customers all over the world.

Our people are our greatest asset and they are here to support you. It is our aim to provide customer care that is superior and second to none.

The company is Norwegian but the strategy is international with employees based in Benelux, UK, Spain, Germany, Hungary and the USA - in addition to the Nordic countries.

Please visit our website at <http://www.forgerock.com/> for more information or send us an email to [info@forgerock.com](mailto:info@forgerock.com)

**ForgeRock AS**  
Josefines gate 25  
0351 Oslo  
Norway

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.