

Glossary

- [Administration Console](#)
- [Discovery service](#)
- [DMZ](#)
- [Entity](#)
- [Federation](#)
- [Identity Provider \(IdP\)](#)
- [Metadata](#)
- [NTP](#)
- [OpenAthens MD](#)
- [RPM](#)
- [Runtime](#)
- [SAML](#)
- [Scope](#)
- [Service Provider](#)
- [sudo](#)
- [WAYF](#)
- [WAYF-less URL](#)
- [yum](#)

Administration Console

The OpenAthens LA administration console is a self-contained web-server and web-application that enables OpenAthens LA to be configured via a web browser.

Discovery service

A page or lookup that allows a user to tell a service provider where they are from so that the service provider can refer them to the correct IdP for authentication. Sometimes referred to by the Shibboleth term WAYF.

DMZ

A DMZ (demilitarised) zone is a physical or logical subnetwork that contains and exposes an organisation's external services to the Internet. The purpose of a DMZ is to add an additional layer of security to an organisation's local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network. The OpenAthens runtime might sit here.

Entity

A generic descriptor given to both Identity Providers and Service Providers. Each is identified by an Entity ID.

Federation

A federation is a group of organisations that use and operate a common set standards and protocols to achieve Single Sign-On between services. A federation exists to provide registration and governance to its members. It will usually require members to abide by a set of terms, conditions and best-practice guidelines. A federation is split into Identity Providers and Service Providers.

Identity Provider (IdP)

An Identity Provider is a software application that provides users with a means to authenticate to services (Service Providers, SPs) in a federation. An Identity Provider will typically be run by an organisation (e.g. University or company) to provide Single Sign-On for its members or employees. The term *Identity Provider* will often be used to refer to this organisation itself rather than simply the software it runs. This is often shortened to IdP.

Metadata

SAML metadata describes one or more *entities* in a machine readable XML format. It is used by Service Providers and Identity Providers to identify and interact with each other and contains information about where the entities reside and their security credentials. While individual entities may publish their own metadata, federations will often compile a single file containing the metadata of all their members.

NTP

The Network Time Protocol (NTP) is used to keep the clock of a system synchronised against one or more known servers. This is used to prevent clocks from drifting over time so that they always keep an accurate time. This is particularly important for OpenAthens LA because the protocols it uses depend on time-stamped messages to ensure that they are secure.

OpenAthens MD

OpenAthens MD is a complete hosted service for the creation and management of user identities and entitlements for single sign-on access to resources. The main difference between OpenAthens MD and OpenAthens LA is that OpenAthens MD is hosted by us whereas you host OpenAthens LA yourself, locally.

RPM

The RPM Package Manager is a package management system used by many Linux distributions. OpenAthens provides pre-built RPM packages of the OpenAthens LA Runtime and Administration Console which can be installed using the yum package manager.

Runtime

The OpenAthens LA runtime is a web-server that provides a Single Sign-On service to online services. It provides the sign-on page for end-users to login to applications, and supports multiple federated identity and authentication standards and protocols (e.g. SAML, LDAP etc). It is provided as a self-contained Virtual Machine Image, though also can be installed on physical hardware.

It is a high-availability and high-performance system, based on Linux and the Apache web-server.

SAML

SAML is an acronym for Security Assertion Markup Language and is the XML format used by SAML entities to communicate.

Scope

The scope is a globally unique identifier for your organisation. A commonly followed convention is to use your Internet Domain name (e.g. domain.com). If you have more than one domain name, you would usually use the most commonly used one, or the one that best represents the organisation or business unit running OpenAthens LA. Different organisational units within your organisation might have different scopes - e.g. london.domain.com and newyork.domain.com.

Service Provider

In Federated Identity terms a Service Provider is a software application that restricts access to online-content in a Federation. A Service Provider may be run by any organisation or individual wishing to share or publish content that may be consumed by users belonging to Identity Providers in a Federation. The term *Service Provider* will often be used to refer to this organisation itself rather than simply the software it runs.

This has the advantage that users of an Identity Provider will gain Single Sign-On to multiple Service Providers without having to login again, and avoids the need for a Service Provider to maintain a large database of user accounts. The term Service Provider is often shortened to the initials, SP.

sudo

sudo allows a permitted user to execute a command as the superuser (or another user) on linux systems.

WAYF

WAYF is an acronym for Where Are You From which is a Shibboleth term for a discovery service that has entered common usage. An interface that allows users to search for or pick their home organisation from a list. Some service providers have their own implementation, others use a central service provided by a federation.

WAYF-less URL

A WAYF-less URL is used to allow links to be provided to end-users to Service Providers or resources that, by including information about the Identity Provider in the URL, allow the user to by-pass the WAYF on the Service Provider's site.

yum

yum is a package manager used by Red Hat and CentOS that manages the installation, update and removal of RPM packages.