

AUTHORIZE

Smart organisations now realise that system access must be brought under control in a centralised manner

Benefits

- Centralised control and configuration
- Consolidated view of access across many systems
- Policy based
- Application independent constraints such as time and user location are supported
- Multi level caching for fast response times
- Faster system development
- Improved system security
- Technology independent
- Flexible PCIM based rules engine
- Highly scalable
- Reliable
- Robust

Authorize Enterprise Service

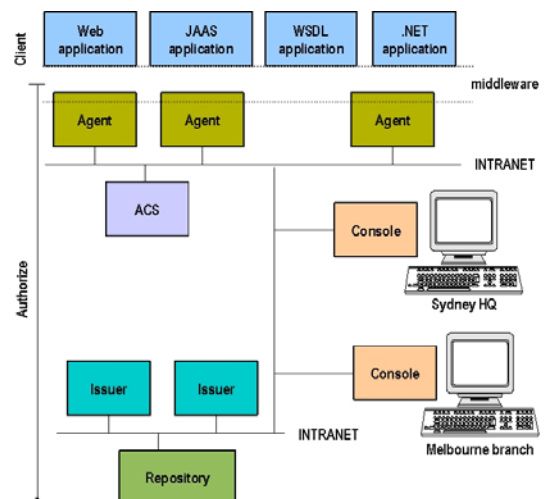
It's a jungle out there!

The modern enterprise landscape has become a sea of isolated and semi integrated enterprise systems. Neat architectural diagrams may show system deployment, function and data flow but they hide a jungle of access control policies hidden in individual applications, outdated documents and administrators' heads. Do you know what systems your users actually have access to? Does anybody? Do you have confidence that when people change roles or leave your organisation, that their access rights are updated accordingly? Can you comply with your privacy obligations regarding access to your clients' personal data?

These are just some of the questions that **Authorize** can help you answer. **Authorize** is a technology independent authorisation service that allows you to model your real world authorisation needs and enforce them as enterprise wide policies that control access to all participating systems. **Authorize** supports the full range of entities needed to do real world modelling. Policies are created from Users, Roles, Groups, Commands, Targets, Permissions and Time and are enforced using an ultra flexible and easy to use rules engine. Access can be controlled down to very specific system functions, the data values entered or the parameters used in commands.

If users change job, then simply remove them from their old roles and add them to their new ones. Their access across all participating systems will be modified accordingly.

Technology independence means that the same server can concurrently control access to web services, internal applications and configuration of equipment from door locks to telephone exchanges.



The distributed architecture enables you to start with a single server and then to grow to as many federated servers as needed. The flexibility provided by the policies and the rules engine means that complex rules can be applied independently of the application seeking authorisation.

FORGE

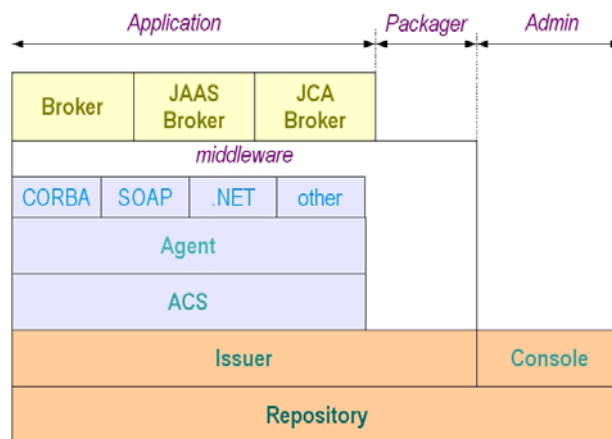
A Generic Solution to a Pervasive Problem

Aspect Oriented

Authorize is an aspect oriented service, which means that it provides a mechanism for separating authorisation functions away from individual applications and allows them to be controlled in a uniform manner across the enterprise. This provides real advantage from a number of perspectives. Application developers simply need to use a server plug-in or a drop-in class to which they direct all authorisation requests. All policy generation, distribution, decision and enforcement are handled transparently by the authorisation service. Authorisation administrators map the corporate authorisation policies onto any number of participating systems through one or more consoles connected to a central repository providing a single view of access across many systems. This centralised control ensures that new users are given all of the necessary access rights required in one easy operation. Similarly access by any user, group of users or to any system or group of systems can be suspended, cancelled or otherwise modified with a single action.

Architecture

Authorize is built upon a proven architecture that can scale from complete deployment on a single server to multi tier deployment with different components deployed on many federated servers. It contains the following components, which can be deployed in a configuration to suit your needs.



Broker

The Policy Enforcement Point (or PEP). This is a client convenience component that submits Authorisation Requests specific to the client's application. If **Authorize** is being integrated directly with an application, then this component written in the language of choice is used to interact with **Authorize**. **Authorize** comes with some pre-built brokers. In the case where **Authorize** is being plugged into an application server for example as a JAAS plug in, then the broker is not required. In this case **Authorize** can provide a superset of JAAS functionality without any source code changes.

Agent

The Policy Decision Point (or PDP). This is mainly a rules-based engine that processes each Authorisation Request against the Actor's Authorisation Attribute Certificate (AAC). That certificate is either included in the Authorisation Request (PUSH model) or issued by the Issuer subsequent to a request submitted by the Agent. Certificates are cached on the agent to enable very fast response times.

Attribute Certificate Server (ACS)

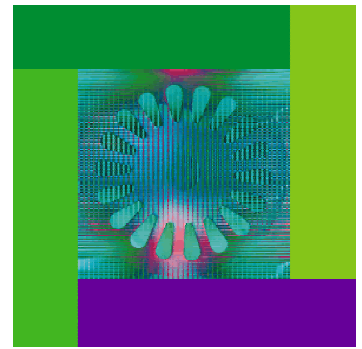
This is an AAC cache. It is optional, and if present, is aimed at reducing the workload on the Repository (and its Issuers). Even though each Agent has its own cache, this component ensures multiple Agent requests for the same certificate are honoured quickly.

Repository (and its Issuer(s))

This is where the authorisation-related information is stored. Requests to issue AACs are received by the Issuer(s), while data manipulation of the authorisation-related information is done through Console(s).

Administration Console

One or many Consoles are used to create and manage authorisation policies. In addition to the Console, existing policy information such as that stored in a JAAS policy file can be imported resulting in automatic creation of users, roles, permissions etc.



Access Mechanisms

- CORBA
- XML-RPC
- RMI
- WSDL / SOAP (Web services)
- JAAS Plug-In
- EJB and J2EE

Policies can be constructed from any combination of

- Users
- Roles
- Systems
- Targets
- Permissions
- Labels (e.g. Top Secret)
- Regulations
- Rules
- Conditions (including time)

Forge Research

Suite 116, Bay 9
Locomotive Workshop
Australian Technology Park
Cornwallis Street, Eveleigh
NSW 1430 Australia

Phone: +61 2 9209 4152
Fax: +61 2 9209 4172
Email: info@forge.com.au
Web: www.forge.com.au

FORGE