IDENTITY PROVIDER

DATA SHEET

API MANAGEMENT
Single sign-on and delegated access control.
Single Sign-on

OpenID Connect Provider

Identity Provider includes enterprise-class implementation of identity layer on top of OAuth 2.0 authorization framework, fully compliant with OpenID Connect 1.0 specification. API consumers can utilize web console or REST interface to manage their end-user accounts and client applications, and benefit from using the following authentication services:

- **Single Sign-on** — federated authentication across systems.
- **Identity Bridging** — delegated authentication to social platforms.
- **Identity Federation** — directory-based account synchronization.
- **Two-factor Authentication** — one-time password enforcement.
- **Account Management** — user profile/credentials management.
- **Client Registration** — dynamic client application enrollment.

Identity Management

User profiles and credentials are stored in the Identity Provider database or in a federated LDAP directory. Trust can be established with social identity providers, to access third-party cloud services. Enhanced security includes password policies and mobile two-factor authentication.

### Authentication Element | Target Object / System
--- | ---
Identity Token | Realm, User, Session
Client Application | Realm
Password Policy | Realm
Login Session | User, Client
User Group | Realm, Group, Directory
User | Realm, Group, Directory

**KEY BENEFITS**

- Decoupled from API resources.
- Uses industry standards to manage end-user and system identities.
- Allows synchronizing user accounts with existing directory services.
- Provides seamless authentication to popular social identity providers.
- Can be used in web application and API resource access scenarios.

Identity Services
OAuth Provider

Identity Provider includes enterprise-class implementation of Authorization and Resource Servers compliant with OAuth 2.0 and UMA 2.0 standards. Client applications can use OAuth interface to gain access to API resources, and benefit from utilizing the following authorization services:

- **Access Control** — delegated, token-based API authorization.
- **Security Realms** — multi-tenant access control administration.
- **Policy Management** — access condition definition/enforcement.
- **Security Role Mapping** — category-based resource access control.
- **Permission Management** — fine-grained resource/policy mapping.
- **Security Event Auditing** — centralized event logging and alerting.

API Management Security

API Management platforms can rely on Identity Provider to control access to application services, and relieve API developers from implementing the intricacies of API resource security. Meanwhile, API consumers can register their client applications with Identity Provider, and focus on the integration and data processing aspects of the API access.

<table>
<thead>
<tr>
<th>Authorization Element</th>
<th>Target Object / System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Token</td>
<td>Realm, Client, Session</td>
</tr>
<tr>
<td>Security Realm</td>
<td>Identity Provider</td>
</tr>
<tr>
<td>Client Scope</td>
<td>Client, Resource, Token</td>
</tr>
<tr>
<td>Access Policy</td>
<td>Client, Policy, Role, Group, User</td>
</tr>
<tr>
<td>Security Role</td>
<td>Client, Scope, Role, Group, User</td>
</tr>
<tr>
<td>Permission</td>
<td>Resource, Scope</td>
</tr>
</tbody>
</table>

Identity Provider enables third-party applications with OAuth 2.0 based authorization. Ideal for API Management platforms exposing secure application services.

The complexity of low-level API resource access control is hidden behind the implementation. Modern enterprise and mobile applications can take advantage of convenient OAuth2 interface to obtain access tokens and quickly integrate cloud services into their solutions.