Identity Platform Guide

/ ForgeRock Identity Platform 6.5

Latest update: 6.5.2

ForgeRock AS.
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Abstract

Guide to ForgeRock Identity Platform™ modules.

Table of Contents

About the ForgeRock Identity Platform

The ForgeRock Identity Platform is the only offering for access management, identity management, user-managed access, directory services, and an identity gateway, designed and built as a single, unified platform.

This guide describes in general terms the ForgeRock modules that compose the ForgeRock Identity Platform, and indicates where to find the documentation corresponding to each module:

ForgeRock® Access Management (AM)

	Intelligent Authentication	Authorization	Federation	User-Managed Access	

ForgeRock® Identity Management (IDM)

Identity Synchronization	Self-Service	Workflow	Social Identity	Identity Lifecycle and Relationship	Access Request	Access Review

ForgeRock® Directory Services (DS)

	Directory Server	Directory Proxy Server	

ForgeRock® Edge Security

	Identity Gateway	Microservices	

In addition to the modules listed in this guide, you can use the following ForgeRock software to enhance platform deployments:

ForgeRock DevOps Examples

DevOps Examples demonstrate installation, configuration, and deployment of ForgeRock Identity Platform components using DevOps techniques.

See the ForgeRock DevOps documentation.

ForgeRock Authenticator Application

This app allows end users to perform multi-factor authentication and transactional authorization from a registered Android or iOS device. It is designed for use in both multi-factor and passwordless authentication scenarios. It is associated with a Push Authentication Simple Notification Service module that depends on the module described in "Intelligent Authentication Module".

See *About Push Authentication* and *Introducing Transactional Authorization*.

For further details and help gaining access to additional software, contact ForgeRock at info@forgerock.com. If your project or deployment requires source code access, also contact ForgeRock.

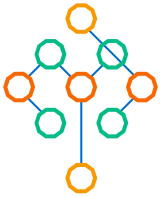
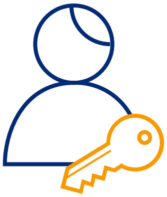
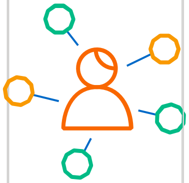
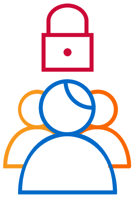
This guide includes general statements of functionality for the following software:

- ForgeRock Access Management 6.5, with Web Agent 5 and Java Agent 5
- ForgeRock Identity Management 6.5
- ForgeRock Directory Services 6.5
- ForgeRock Edge Security Modules

This document is not meant to serve as a statement of functional specifications. Software functionality may evolve in incompatible ways in major and minor releases, and occasionally in maintenance (patch) releases. Release notes cover many incompatible changes. If you see an incompatible change for a stable interface that is not mentioned in the release notes, please report an issue with the product documentation for that release.

Chapter 1
Access Management

Access Management modules:

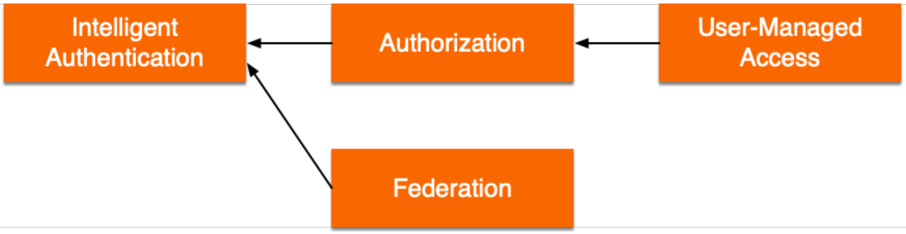
	 Intelligent Authentication	 Authorization	 Federation	 User-Managed Access	

1.1. Overview of Capabilities

- Intelligent authentication
- Mobile authentication
- Push authentication
- Adaptive risk authentication
- Authorization policies and enforcement
- Federation
- Single sign-on (SSO)
- User self-services and social sign-on
- High-availability and scalability
- Adaptable monitoring and auditing services
- Developer-friendly, rich standards support

1.2. Dependencies

Several Access Management modules require other modules. For example, the Federation module requires the Intelligent Authentication module. The following diagram summarizes Access Management module dependencies:



1.3. Intelligent Authentication Module

This module will help you build secure, robust, centrally managed single sign-on services. The user, application, or device signs on once and then is granted appropriate access everywhere. Authentication management integrates delegated authentication chains with many authentication methods supported by default. Authentication trees store authentication sessions in the client as a cookie, or in the CTS store. If the AM server goes down or the user is redirected to another AM while authenticating, the new AM server can grab the authentication session and continue the flow. All authentication-related events are logged for auditing and reporting purposes.

Required modules: none.

Feature	Description	Documentation
Authentication Trees and Nodes	Authentication trees provide fine-grained authentication, social authentication, and multi-factor authentication. Trees are made up of authentication nodes. Authentication nodes allow multiple paths and decision points throughout the authentication flow, enabling AM to handle different modes of authenticating users.	*About Authentication Trees*
Authentication Modules	AM provides more than 25 authentication modules, including multi-factor and strong authentication, to handle different modes of authenticating users or entities. The modules can be chained together so that a user's or entity's credentials	*Authentication Module Properties*

Feature	Description	Documentation
	must be evaluated by one module before control passes to another module.	
Adaptive Risk Module	Risk assessment based on predetermined characteristics to determine whether to complete further authentication steps in a chain.	*Adaptive Risk Authentication Module*
Session High Availability	Persistent access management sessions, authenticating the user until the session expires.	Session high availability is enabled by default with no setup required.
Multi-Factor and Strong Authentication	Capability to challenge for additional credentials when authentication takes place under centrally-defined risky or suspicious conditions.	*About Multi-Factor Authentication*
External Configuration Store	Configuration storage in ForgeRock Directory Services for high-availability.	*Preparing an External Configuration Data Store*
REST and SOAP STS	Secure Token Service (STS) for bridging identities across web and enterprise identity access management (IAM) systems through a token transformation process, securely providing cross-system access to service resources by authenticated requesting applications.	*Introducing the Security Token Service*
Web and Java Agents for SSO	Intercept requests to access protected resources and redirect for appropriate authentication.	*Web Agents User Guide* and *Java Agents User Guide*
Mobile Authenticator	Sample iOS and Android applications for strong multi-factor authentication with one-time passwords, secure QR code provisioning, and recovery codes for lost or stolen devices.	*Sample Mobile Authentication Applications*
User Login Analytics	Measure authentication flows using counters and start/stop timers to monitor performance.	*Timer Node Start*, *Timer Node Stop*, *Meter Node*, and *Monitoring Metric Types*

1.4. Authorization Module

This module will help you create powerful, context-based policies with a GUI-based policy editor and with REST APIs to control access to online resources. Resources can be URLs, external services, or devices and things. Authorization management lets you manage policies centrally and enforce them locally through installable agents, or through REST, C, and Java applications. Authorization management is extensible, making it possible to define external subjects, complex conditions, and custom access decisions.

Required module: Intelligent Authentication.

Feature	Description	Documentation
Entitlement Policies	Modern web-based policy editor for building policies, making it possible to add and update policies as needed without touching the underlying applications.	*Introducing Authorization*
Web and Java Agents for Enforcement	Access enforcement for online resources with the capability to require higher levels of authentication and session upgrade when accessing sensitive resources.	*Web Agents User Guide* and *Java Agents User Guide*
Transactional Authorization	Requires a user to perform additional actions such as reauthenticating to a module or node, or responding to a push notification, to gain access to a protected resource.	*Implementing Transactional Authorization*
OAuth 2.0 Dynamic Scopes	A single OAuth 2.0 client configured for a comprehensive list of scopes can serve different scope subsets to resource owners based on policy conditions.	*Policy Decisions* and *Authorization Examples*

1.5. Federation Module

This module will help you extend SSO capabilities across organization boundaries based on standards-based interoperability.

Required module: Intelligent Authentication.

Feature	Description	Documentation
SAML 2.0 IDP and SP	Identity federation with SaaS applications, such as Salesforce.com, Google Apps, WebEx, and many more.	*Configuring IdPs, SPs, and COTs*
SAML 2.0 SSO and SLO	Web Single Sign-On and Single Logout profile support.	*Implementing SAML v2.0 SSO and SLO*
ADFS	Federation with Active Directory Federation Services.	*Introducing SAML v2.0 Support*
SAML 2.0 Attribute and Advanced Profiles	Support for transmitting only attributes used by targeted applications.	*SAML v2.0 Deployment Overview*
OpenID Connect	OpenID Connect 1.0 compliance for running an OpenID Provider, including advanced profiles, such as Mobile Connect.	*Introducing OpenID Connect 1.0*

Feature	Description	Documentation
OAuth 2.0	OAuth 2.0 compliance for running an authorization server.	*Introducing OAuth 2.0*
Social Login	For acting as an OAuth 2.0 client of social identity providers, such as Facebook, Google, and Microsoft.	*Implementing Social Authentication*
OAuth 2.0 Dynamic Scopes	A single OAuth 2.0 client configured for a comprehensive list of scopes can serve different scope subsets to resource owners based on policy conditions.	*Policy Decisions* and *Authorization Examples*

1.6. User-Managed Access Module

This module consists of a consumer-facing implementation of the User-Managed Access (UMA) 2.0 standard. The standard defines an OAuth 2.0-based protocol designed to give individuals a unified control point for authorizing who and what can access their digital data, content, and services. For example, you can use this module to build a solution where end users can delegate access through a share button, and then monitor and change sharing preferences through a central dashboard.

Required modules: Authorization, Intelligent Authentication.

Feature	Description	Documentation
UMA Standard Conformance	Conformance to the UMA 2.0 standard for interoperability with organizational and partner systems, including federated authorization and customer-centric use cases.	*Introducing UMA 2.0*
UMA Authorization Server	Authorization server with dynamic resource set registration, end user control of resource sharing, responses to access requests, and full audit history.	*Introducing UMA 2.0*
UMA Protector	ForgeRock Identity Gateway protection for resources and services with the UMA 2.0 standard.	*Supporting UMA Resource Servers*

Chapter 2
Identity Management

ForgeRock Identity Management 6.5 brings together multiple sources of identity for policy and workflow-based management that puts you in control of the data. Build a solution to consume, transform, and feed data to external sources to help you maintain control over identities of users, devices, and things. Identity governance features in ForgeRock Identity Management let you gain visibility into employee provisioning, and help you proactively take action in managing employee access to external systems.

Identity Management modules:

Identity Synchronization	Self-Service	Workflow	Social Identity	Identity Lifecycle and Relationship	Access Request	Access Review

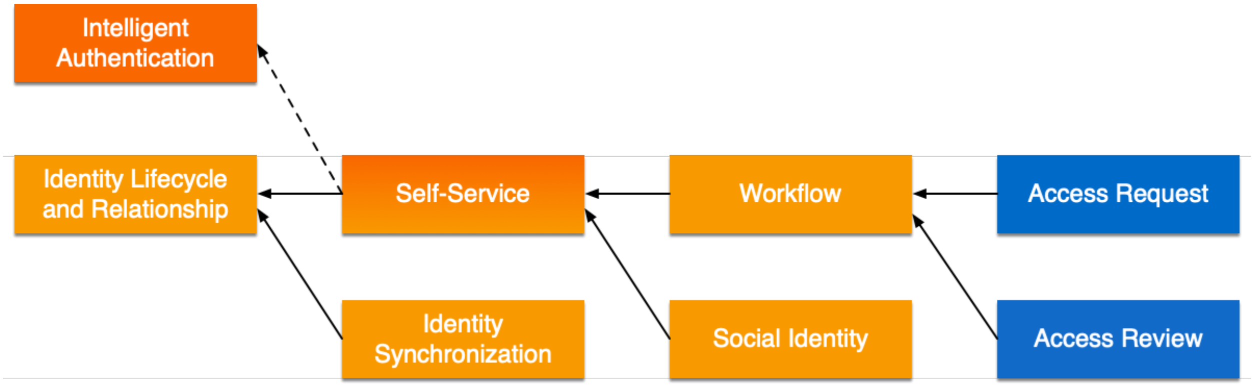
2.1. Overview of Capabilities

- Provisioning
- Synchronization and reconciliation
- Adaptable monitoring and auditing services
- Connections to cloud services with simple social registration
- Flexible developer access
- Password synchronization
- Identity data visualization
- Delegated administration
- User self-service

- Privacy and consent
- Progressive profile completion
- Workflow engine
- OpenICF connector framework to external systems
- Access request (Identity Governance)
- Access review and reporting (Identity Governance)

2.2. Dependencies

Several Identity Management modules require other modules. For example, the Synchronization module requires the Identity Lifecycle and Relationship module. The following diagram summarizes Identity Management module dependencies:



2.3. Identity Synchronization Module

This module can serve as the foundation for provisioning and identity data reconciliation. Synchronization capabilities are available as a service and through REST APIs to be used directly by external applications. Activities occurring in the system can be configured to log and audit events for reporting purposes.

Required module: Identity Lifecycle and Relationship.

Feature	Description	Documentation
Discovery and Synchronization	Synchronization of identity data across managed data stores.	*Synchronizing Data Between Resources*

Feature	Description	Documentation
Reconciliation	Alignment between accounts across managed data stores.	*Managing Reconciliation*
Password Synchronization	Near real-time password synchronization across managed data stores.	*Password Synchronization Plugin Guide*
Directory Services and Active Directory Plugins	Native password synchronization plugins for ForgeRock Directory Services and Microsoft Active Directory.	*Synchronizing Passwords With ForgeRock Directory Services (DS)*, and *Synchronizing Passwords With Active Directory*
Delegated Administration	Grant role-based, limited access to perform fine-grained administrative tasks on managed objects.	*Privileges and Delegation*
All Connectors	Extensible interoperability for identity, compliance, and risk management across a variety of specific applications and services.	*Connecting to External Resources*

2.4. Self-Service Module

This module can be used to allow end users to manage their own passwords and profiles securely according to predefined policies.

Required modules:

- Full capabilities: Identity Lifecycle and Relationship.
- Basic capabilities: Intelligent Authentication. See *Introducing User Self-Service* for information about self-service capabilities in AM.

Feature	Description	Documentation
User Self-Registration	End-user self-service UI that lets users create their own accounts with customizable criteria.	*User Self-Registration*
Password Management	End-user self-service UI for changing and resetting passwords based on predefined policies and security questions.	*Resetting User Passwords*
Password Reset	Mechanisms to allow users to reset their own passwords with predefined policies.	*Configuring User Self-Service*
Knowledge-Based Authentication	Verification for user identities based on predefined and end user-created security questions.	*Configuring Self-Service Questions (KBA)*

Feature	Description	Documentation
Forgotten Username	Mechanisms to allow users to recover their usernames with predefined policies.	*Forgotten Username*
Progressive Profile Completion	Short forms used to simplify registration and incrementally collect profile data over time.	*Progressive Profile Completion*
Profile and Privacy Management Dashboard	Dashboard for managing personal user information.	*Privacy: My Account Information in the Self-Service UI*
Consent and Preference Management	Configurable user preferences.	*Configuring Synchronization Filters With User Preferences*
Terms and Conditions (or Terms of Service) Versioning	Manage multiple terms and conditions.	*Adding Terms and Conditions*

2.5. Workflow Module

This module can be used to visually organize identity synchronization, reconciliation, and provisioning into repeatable processes with logging and auditing for reporting purposes.

Required modules: Self-Service, Identity Lifecycle and Relationship.

Feature	Description	Documentation
Activiti Workflow Engine	Lightweight workflow and business process management platform.	*Setting Up Activiti Integration*
BPMN 2.0 Support	Standards-based Business Process Model and Notation 2.0 support.	*BPMN 2.0 and the Activiti Tools*
Workflow-Driven Provisioning	Define provisioning workflows for self-service, sunrise and sunset processes, approvals, escalations, and maintenance.	*Integrating Business Processes and Workflows*

2.6. Social Identity Module

With this module, you can allow users to register and authenticate with specified standards-compliant social identity providers. These users can also link multiple social identity providers to the same account, thus establishing a single consumer identity.

With the attributes collected from each user profile, you can configure the module to authorize access to applications and resources, including lead generation tools.

Required modules: Self-Service, Identity Lifecycle and Relationship.

Feature	Description	Documentation
Registration	User registration with social identity accounts.	*Configuring Social Identity Providers*
Authentication	Social login for identity management.	*OpenID Connect Authorization Code Flow*
Account Linking	Users can select specific social identity providers for logins.	*Managing Links Between End User Accounts and Social ID Providers*
Attribute Scope Management	Administrators can include any or all scopes available, by social identity provider.	*Configuring Social Identity Providers*

2.7. Identity Lifecycle and Relationship Module

This module can help you to provision user identities into IDM, and includes the capability to manage roles, relationships between identities, and entitlements.

Required modules: none.

Feature	Description	Documentation
Inbound Provisioning Engine	Provisioning engine to import data from an external resource into IDM.	*Synchronizing Data Between Resources*
Data Modeling	Ability to map IDM objects to tables in a JDBC database or to organizational units in a DS repository.	*Using Generic and Explicit Object Mappings*
Identity Lifecycle Management	An extensible object model that enables you to manage the complete lifecycle of identity objects.	*Working With Managed Objects*
Identity Relationship Lifecycle Management	Ability to create and track relationship references between objects.	*Managing Relationships Between Objects*
Role Lifecycle Management	Provisioning roles to control how objects are exported to external systems and authorization roles to control authorization within IDM.	*Working With Managed Roles*
Entitlement Lifecycle Management	Entitlements to provision attributes or sets of attributes, based on role membership.	*Working With Role Assignments*

2.8. Access Request Module

This module helps users search for and request entitlements for themselves, as well as on behalf of other members of the organization. Users can also view the status of existing requests, and take action on pending work items. Requests can be automatically approved or can require one or more approvals.

Required modules: Workflow, Self-Service, Identity Lifecycle and Relationship.

Feature	Description	Documentation
Entitlement Bundles	Administrators can create and manage entitlement bundles. Bundles are groups of entitlements to which users can request access.	*Access Request Documentation*
User Notifications	Access Request can send customizable user notifications for specific events that occur within the request process.	*Access Request Documentation*
Identity Glossary	The glossary provides consolidated management of entitlement metadata, bulk export and import, and extended relationship mapping.	*Access Request Documentation*

2.9. Access Review Module

This module provides user certification, role management, policy enforcement, and reporting.

Required modules: Workflow, Self-Service, Identity Lifecycle and Relationship.

Feature	Description	Documentation
User Certification	Multi-stage certifications let any number of certifiers participate in access decision processes, and provide an escalation process to ensure timely responses.	*Access Review Documentation*
Role Management	An extensible glossary allows for consolidated management of role and entitlement metadata, bulk export and import, and extended relationship mapping.	*Access Review Documentation*
Policy Enforcement	Supports proper segregation of duties.	*Access Review Documentation*
Reporting	Helps you meet compliance regulations and enables you to obtain a comprehensive understanding of your identity governance system. The reporting module includes a variety of reporting options such as systems access, certification, policy violations, and so on.	*Identity Reporting Documentation*

Chapter 3

Directory Services

ForgeRock Directory Services 6.5 serves as a foundation for LDAPv3 and RESTful directories.

Directory Services modules:

	Directory Server	Directory Proxy Server	

3.1. Overview of Capabilities

- Large-scale, distributed read and write performance
- Flexible key-value data model for storing users, devices, and things
- Data storage with confidentiality, integrity, and security
- High-availability through data replication and proxy services
- Single logical entry point for use in protecting LDAPv3 directory services
- Load balancing and failover for LDAPv3 directory services
- Maximum interoperability and pass-through delegated authentication
- Adaptable monitoring and auditing services
- Easy installation, configuration, and management
- Developer-friendly, rich standards support

3.2. Dependencies

Neither of the Directory Services modules are dependent upon other modules.

3.3. Directory Server Module

The ForgeRock Directory Server module helps you store store identities for users, devices, and things in a highly available and secure way. This module provides data replication to help you build highly available directory services. It also offers fine-grained access control, password digests, encryption schemes, and customizable password policies to allow you to build very secure directory services. Data may be accessed using LDAP or REST with the same level of security constraints and access control.

Required modules: none.

Feature	Description	Documentation
LDAPv3	Compliance with the latest LDAP protocol standards.	*Understanding Directory Services*
REST APIs and REST to LDAP Gateway	HTTP-based RESTful access to user data and server configuration.	*RESTful Client Access Over HTTP*
DSMLv2 Gateway	HTTP-based SOAP access to LDAP operations for web services.	*DSML Client Access*
High-Availability Multi-Master Replication	Data replication for always-on services, enabling failover and disaster recovery.	*Managing Data Replication*
User/Object Store	Flexible key-value data model for storing users, devices, and things.	*Managing Directory Data*
Passwords and Data Security	Password digests, encryption schemes, and customizable rules for password policy compliance to help protect data on disk and shared infrastructure.	*Encrypting Directory Data*, *Configuring Password Policy*

3.4. Directory Proxy Server Module

The ForgeRock Directory Proxy Server module helps you increase the availability of a Directory Service deployment, providing a single point of access to a large-scale distributed data store. The module offers a choice of strategies for request load balancing and failover. Data may be accessed using LDAP or REST with the same level of security constraints and access control.

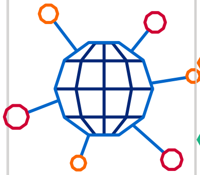
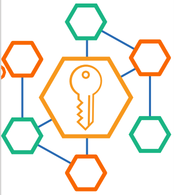
Required modules: none.

Feature	**Description**	**Documentation**
Single Point of Access	Uniform view of underlying LDAPv3 directory services for client applications.	*Deploying a Single Point of Directory Access*
High Service Availability	LDAP services with reliable crossover and DN-based routing.	*Deploying Proxy Services for High Availability*
Load Balancing and Failover	Configurable load balancing across directory servers with redundancy, and capabilities to handle referrals, connection failures, and network partitions.	*Choosing a Load Balancing Algorithm*
Protection For Directory Services	Secure incoming and outgoing connections, and provide coarse-grained access control.	*Securing Network Connections*, *About Global Access Control Policies*
Scaling Out Using Data Distribution	Distribute data across multiple shards.	*Scaling Out Using Data Distribution*
LDAPv3	Compliance with the latest LDAP protocol standards.	*Understanding Directory Services*
REST APIs	HTTP-based RESTful access to user data and server configuration.	*RESTful Client Access Over HTTP*

Chapter 4
Edge Security

Use ForgeRock Edge Security software to integrate web applications, APIs, microservices, Internet of Things devices, and cloud-based services with the ForgeRock Identity Platform.

Edge Security modules:

	 Identity Gateway	 Microservices	

4.1. Dependencies

Neither of the Edge Security modules are dependent upon other modules.

4.2. Identity Gateway Module

ForgeRock Identity Gateway helps you integrate web applications, APIs, and microservices with the ForgeRock Identity Platform, without modifying the application or the container where it runs. Based on reverse proxy architecture, it enforces security and access control in conjunction with the Access Management modules.

ForgeRock Identity Gateway software provides the following capabilities:

- Protection for IoT services, microservices, and APIs
- Policy enforcement
- Adaptable throttling, monitoring, and auditing
- Secure token transformation

- Support for identity standards such as OAuth 2.0, OpenID Connect, SAML 2.0, and UMA 2.0
- Password capture and replay
- Rapid prototyping

Required modules: none.

Feature	Description	Documentation
Studio	User interface for rapid development and prototyping.	*Configuring Routes With Studio* and *Technology Preview of Freeform Studio*
Single Sign-On	Single sign-on in a single domain and across domains.	*Single Sign-On and Cross-Domain Single Sign-On*
Password Replay	Secure replay of credentials to legacy applications or APIs.	*Getting Login Credentials From Data Sources* and *Getting Login Credentials From AM*
Policy Enforcement	Enforcement of centralized authorization policies for applications requiring Access Management.	*Enforcing Policy Decisions From AM* and *Hardening Authorization With Advice From AM*
Federation	OpenID Connect 1.0.	*Acting As an OpenID Connect Relying Party*
	OAuth 2.0.	*Acting As an OAuth 2.0 Resource Server*
	SAML 2.0.	*Acting As a SAML 2.0 Service Provider*
	SAML resources for mobile applications.	*Transforming OpenID Connect ID Tokens Into SAML Assertions*
Finance APIs	Support for OAuth 2.0 Mutual TLS and Financial-Grade APIs.	*Validating OAuth 2.0 Access Tokens Obtained Through mTLS* and *FapiInteractionIdFilter*
WebSocket Protocol	Detection of requests to upgrade from HTTPS to the WebSocket protocol, and creation of a secure, dedicated tunnel to send and receive WebSocket traffic.	*Proxying WebSocket Traffic*
Throttling	Throttling to limit access to protected applications.	*Throttling the Rate of Requests to Protected Applications*
UMA Resource Server	Protection for resources and services according to the UMA 2.0 standard.	*Supporting UMA Resource Servers*
DevOps Tooling	Deployment of basic and customized configurations through Docker.	*Deployment Guide*

4.3. Microservices Security Module

Required modules: none.

Microservice	Description	Documentation
Microgateway	Sidecar-type, container-optimized gateway for securing microservices.	*Microgateway Release Notes*
Token Validation Microservice	Platform satellite for introspection of stateful and stateless OAuth 2.0 access tokens.	*About the Token Validation Microservice*