Identity Platform Guide

ForgeRock Identity Platform 5

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

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. Table 1, "ForgeRock Identity Platform Modules" summarizes the modules available.

Table 1. ForgeRock Identity Platform Modules

Core Solution	Module	Find Details In
ForgeRock Access Management (AM)	Authentication	Section 1.1, "Authentication Module"
	Authorization	Section 1.2, "Authorization Module"
	Federation	Section 1.3, "Federation Module"
	Adaptive Risk	Section 1.4, "Adaptive Risk Module"
	User-Managed Access	Section 1.5, "User-Managed Access Module"
ForgeRock Identity Management (IDM)	Identity Synchronization	Section 2.1, "Identity Synchronization Module"
	Self-Service	Section 2.2, "Self-Service Module"
	Workflow	Section 2.3, "Workflow Module"
	Social Identity	Section 2.4, "Social Identity Module"
ForgeRock Directory Services (DS)	Directory Services	Section 3.1, "Directory Services Module"
	Directory Proxy Services	Section 3.2, "Directory Proxy Services Module"
ForgeRock Identity Gateway (IG)	Identity Gateway	Section 4.1, "Identity Gateway Module"

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

- ForgeRock Access Management 14.0.0, with web policy agents 4.0, and Java EE policy agents 3.5
- ForgeRock Identity Management 5.0.0

- ForgeRock Directory Services 4.0.0
- ForgeRock Identity Gateway 5.0.0

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

ForgeRock Access Management 14.0.0 software has been used to provide the following capabilities:

- Advanced authentication
- Mobile authentication
- Push authentication
- Adaptive risk authentication
- Centralized and distributed authorization
- 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

1.1. Authentication Module

This module will help you build secure, robust, centrally managed single sign-on services, where 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. All authentication-related events are logged for auditing and reporting purposes.

Authentication module features are described in Table 1.1, "Module Features".

Table 1.1. Module Features

Feature	Description	Documentation
Authentication Modules	More than twenty modules provided, including multi-factor and strong authentication	*Authentication Module Properties*

Feature	Description	Documentation
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	*About the STS*
Policy Agents for SSO	Intercept requests to access protected resources and redirect for appropriate authentication	*Java EE and Web Policy Agents Documentation*
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*

1.2. 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.

Authorization module features are described in Table 1.2, "Module Features".

Table 1.2. Module Features

Feature	Description	Documentation
Entitlement Policies	Modern web-based policy editor for building policies, making it possible to add and update policies as needed	*Introducing Authorization*

Feature	Description	Documentation
	without touching the underlying applications	
Policy Agents for Enforcement	Access enforcement for online resources with the capability to require higher levels of authentication and session upgrade when accessing sensitive resources	*Java EE and Web Policy Agents Documentation*
XACML Export	Support for eXtensible Access Control Markup Language (XACML) with export in XACML format for backup, transfer between servers, and storage in version control systems	*Importing and Exporting Policies*

1.3. Federation Module

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

Federation module features are described in Table 1.3, "Module Features".

Table 1.3. Module Features

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*
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*

1.4. Adaptive Risk Module

This module introduces risk assessment to the authentication and authorization processes. It can be customized to provide risk scoring, flexible conditions, and contextual determination of risk to bar invalid entrants in real time.

Adaptive Risk module features are described in Table 1.4, "Module Features".

Table 1.4. Module Features

Feature	Description	Documentation
Device Fingerprinting	Authentication decisions based on collection and comparison of remote user device characteristics in a unique device profile	*Device ID (Match) Authentication Module Properties*, *Device ID (Save) Authentication Module Properties*
Scripted AuthN and AuthZ Conditions	Authentication and authorization decisions incorporating custom, scripted logic	*About Scripting*
Adaptive Authentication	Risk assessment based on predetermined characteristics to determine whether to complete further authentication steps	*Adaptive Risk Authentication Module Properties*

1.5. User-Managed Access Module

This module consists of a consumer-facing implementation of the User-Managed Access (UMA) 1.0 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 though a share button, and then monitor and change sharing preferences through a central dashboard.

User-Managed Access module features are described in Table 1.5, "Module Features".

Table 1.5. Module Features

Feature	Description	Documentation
UMA Standard Conformance	Conformance to the UMA 1.0 standard for interoperability with organizational and partner systems, including federated authorization and customer-centric use cases	*Introducing UMA 1.0*
UMA Authorization Server	Authorization server with dynamic resource set registration, end user control of resource sharing, responses	*Implementing UMA 1.0*

Feature	Description	Documentation
	to access requests, and full audit history	
UMA Protector	ForgeRock Identity Gateway protection for resources and services with the UMA 1.0 standard	*Supporting UMA Resource Servers*

Chapter 2

Identity Management

ForgeRock Identity Management 5.0.0 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.

ForgeRock Identity Management 5.0.0 software has been used to provide the following 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
- User self-services
- Workflow engine
- OpenICF connector framework to external systems

2.1. 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.

Identity Synchronization module features are described in Table 2.1, "Module Features".

Table 2.1. Module Features

Feature	Description	Documentation
Provisioning Engine	Centralized registration and provisioning for users, devices, and things	*Synchronizing Data Between Resources*
Discovery Engine	Live discovery and synchronization for account changes	*Types of Synchronization*
Synchronization	Synchronization of identity data across managed data stores	*Configuring Synchronization Between Two Resources*
Reconciliation	Alignment between accounts across managed data stores	*Managing Reconciliation*
Password Synchronization	Near real-time password synchronization across managed data stores	*Managing Passwords*
Directory Services and Active Directory Plugins	Native password synchronization plugins for ForgeRock Directory Services and Microsoft Active Directory	*Synchronizing Passwords With an LDAP Server*
Connector Servers for Java and .NET Connectors	Remote operation for provisioning across all managed data stores	*Connecting to External Resources*
All Connectors	Extensible interoperability for identity, compliance, and risk management across a variety of specific applications and services	*Connectors Guide*

2.2. Self-Service Module

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

The capabilities in this module are shared with ForgeRock Access Management as described in *Introducing User Self-Service*.

Self-Service module features are described in Table 2.2, "Module Features".

Table 2.2. Module Features

Feature	Description	Documentation
Password Management	End user dashboard to change and reset passwords based on predefined policies and security questions	*Working With the Self-Service UI*

Feature	Description	Documentation
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*
Profile Management	End user dashboard to manage user profile information	*The Self-Service UI Profile*
Forgotten Username	Mechanisms to allow users to recover their usernames with predefined policies	*Working With the Self-Service UI*

2.3. 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.

Workflow module features are described in Table 2.3, "Module Features".

Table 2.3. Module Features

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*

2.4. 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.

Social identity module features are described in Table 2.4, "Module Features".

Table 2.4. Module Features

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*
Consent and Preference Management	Configurable user preferences	*Configuring Synchronization Filters With User Preferences*
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 ID Providers*

Chapter 3
Directory Services

ForgeRock Directory Services 4.0.0 serves as a foundation for LDAPv3 and RESTful directories.

ForgeRock Directory Services software has been used to provide the following 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

3.1. Directory Services Module

ForgeRock Directory Services module features are described in Table 3.1, "Module Features".

Table 3.1. Module Features

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*

Feature	Description	Documentation
High-Availability Multi-Master Replication	Data replication for always-on services, enabling failover and disaster recovery	*Managing Data Replication*
Embedded Databases	Choice of Oracle Berkeley DB or ForgeRock DB	*Creating a New Database Backend*
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*

3.2. Directory Proxy Services Module

ForgeRock Directory Proxy Services module features are described in Table 3.2, "Module Features".

Table 3.2. Module Features

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*
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

Identity Gateway

ForgeRock Identity Gateway 5.0.0 can help 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 has been used to provide 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
- Password capture and replay
- Rapid prototyping

4.1. Identity Gateway Module

The ForgeRock Identity Gateway module features are described in Table 4.1, "Module Features".

Table 4.1. Module Features

Feature	Description	Documentation
OpenID Connect Authentication	Federation according to OpenID Connect 1.0 standards	*Identity Gateway As an OAuth 2.0 Client or OpenID Connect Relying Party*
OAuth 2.0 Authorization	Federation according to OAuth 2.0 standards	*Acting As an OAuth 2.0 Resource Server*, *Acting As an OAuth 2.0 Client or OpenID Connect Relying Party*
Access Policy Enforcement	Enforcement of centralized authorization policies for applications requiring Access Management	*Enforcing Policy Decisions and Supporting Session Upgrade*

Feature	Description	Documentation
OpenAM STS Token Translator	Access to SAML resources for mobile applications (requires Access Management)	*Transforming OpenID Connect ID Tokens Into SAML Assertions*
Throttling	Throttling to limit access to protected applications	*Throttling the Rate of Requests to Protected Applications*
Password Replay	Secure replay of credentials to legacy applications or APIs	*Getting Login Credentials From Data Sources*
Studio	User interface for rapid development and prototyping	*Creating Routes Through IG Studio*
DevOps Tooling	Deploying Basic and Customized Configurations Through Docker	*Deployment Guide*
UMA Resource Server	Protection for resources and services according to the UMA 1.0 standard	*Supporting UMA Resource Servers*