About the 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.

About this documentation

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

- ForgeRock Access Management 7.5, with Web Agent 2024.3 and Java Agent 2024.3
- ForgeRock Identity Management 7.5
- ForgeRock Directory Services 7.5
- ForgeRock Edge Security module

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

ForgeRock® Access Management (AM) modules

Intelligent Access

Authorization

Federation

User-Managed Access

ForgeRock® Identity Management (IDM) modules

Identity Synchronization

Self-Service

Workflow

Social Identity

Identity Lifecycle and Relationship

ForgeRock® Directory Services (DS) modules

Directory Server

Directory Proxy Server

ForgeRock® Edge Security module

Edge Security Identity Gateway

Deployment enhancements

In addition to the modules listed in the preceding section, you can use the following ForgeRock software to enhance platform deployments.

Run the platform in containers on Kubernetes

The ForgeRock Identity Platform (AM, IDM, DS, IG, and the platform UI) is supported when running in containers on Kubernetes platforms, including Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (Amazon EKS), Microsoft Azure Kubernetes Service (AKS), and IBM RedHat OpenShift. It is recommended that you have a support contract in place with your Kubernetes platform vendor or partner to resolve any infrastructure or Kubernetes platform-related issues, as ForgeRock supports the identity platform while the Kubernetes vendor or partner provides support for their platform.

Customers are responsible for building images and running containers of the ForgeRock software components using a supported operating system and all required software dependencies.

Kubernetes deployment tools from ForgeRock

ForgeRock provides a reference toolset in the forgeops and forgeops-extras Git repositories for automating the deployment of the ForgeRock Identity Platform in Kubernetes. These reference tools are provided for use with Google Kubernetes Engine, Amazon Elastic Kubernetes Service, and Microsoft Azure Kubernetes Service. (ForgeRock supports running the identity platform on IBM RedHat OpenShift but does not provide the reference tools for IBM RedHat OpenShift.)

ForgeRock also publishes reference Docker images for testing and development, but these images should *not* be used in production. For production deployments, it is recommended that customers build and run containers using a supported operating system and all required software dependencies. Additionally, to help ensure interoperability across container images and the ForgeOps tools, Docker images must be built using the Dockerfile templates as described in the ForgeOps documentation.

Partner offerings

ForgeRock's partner, Midships Limited, offers a Kubernetes deployment accelerator (supported by Midships) for Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (Amazon EKS), Microsoft Azure Kubernetes Service (AKS), and IBM RedHat OpenShift.

ForgeRock IoT

Things are physical objects that can connect with each other, and with other systems through the Internet, without human intervention. Examples include smart home devices, such as window sensors and door locks, smart TVs, health and fitness monitors, vehicles, and manufacturing equipment.

To participate in a connected system, a Thing needs an identity that it uses to authenticate, authorize, create relationships, and more. ForgeRock IoT enables dynamic registration, authentication, and authorization of Things with identities, without the need for human intervention.

As soon as Things connect to a network, they become a security concern. You need to be able to trust and monitor the Things that are connected to your network, and accessing your services or APIs. The ForgeRock Identity Platform, including ForgeRock IoT, provides standards-based authorization using the OAuth 2.0 authorization framework. It gives you a single view of all the identities in your system—customers, employees, Things, and the relationships between them. ForgeRock IoT also lets you manage offline and constrained devices, and delivers identities to Things at the edge of your network, where the data is being generated.

See the ForgeRock IoT 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 Access modules.

See MFA: push authentication and Transactional authorization.

Access Management

Access Management modules:

Intelligent Access

Authorization

Federation

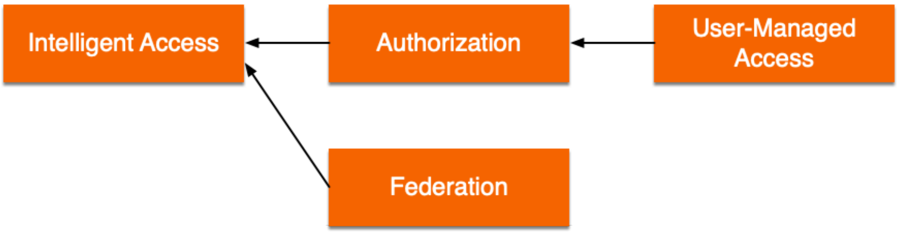
User-Managed Access

Overview of capabilities

- Intelligent access
- 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

Dependencies

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



Intelligent Access modules

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.	Authentication nodes and trees
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.	Multi-factor authentication

Feature	Description	Documentation
External configuration store	Configuration storage in ForgeRock Directory Services for high-availability.	Prepare configuration stores
Security token service	Bridges 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.	STS overview
Web and Java agents for SSO	Intercept requests to access protected resources and redirect for appropriate authentication.	Web policy agents and Java policy agents
User login analytics	Measure authentication flows using counters and start/stop timers to monitor performance.	Timer Start node, Timer Stop node, Meter node, and Monitoring metric types

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 Access.

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.	Authorization and policy decisions
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 policy agents and Java policy agents
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.	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.	Dynamic OAuth 2.0 authorization

Federation module

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

Required module: Intelligent Access.

Feature	Description	Documentation
SAML 2.0 IDP and SP	Identity federation with SaaS applications, such as Salesforce.com, Google Apps, WebEx, and many more.	Configure IdPs, SPs, and COTs
SAML 2.0 SSO and SLO	Web Single Sign-On and Single Logout profile support.	Implement SSO and SLO
ADFS	Federation with Active Directory Federation Services.	Introduction to SAML v2.0
SAML 2.0 Attribute and Advanced Profiles	Support for transmitting only attributes used by targeted applications.	SAML v2.0
OpenID Connect	OpenID Connect 1.0 compliance for running an OpenID Provider, including advanced profiles, such as Mobile Connect.	OpenID Connect 1.0
OAuth 2.0	OAuth 2.0 compliance for running an authorization server.	OAuth 2.0
Social login	For acting as an OAuth 2.0 client of social identity providers, such as Facebook, Google, and Microsoft.	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.	Dynamic OAuth 2.0 authorization

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 Access.

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.	User-Managed Access (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.	AM as UMA authorization server
UMA protector	ForgeRock Identity Gateway protection for resources and services with the UMA 2.0 standard.	UMA support

Identity Management

ForgeRock Identity Management 7.5 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

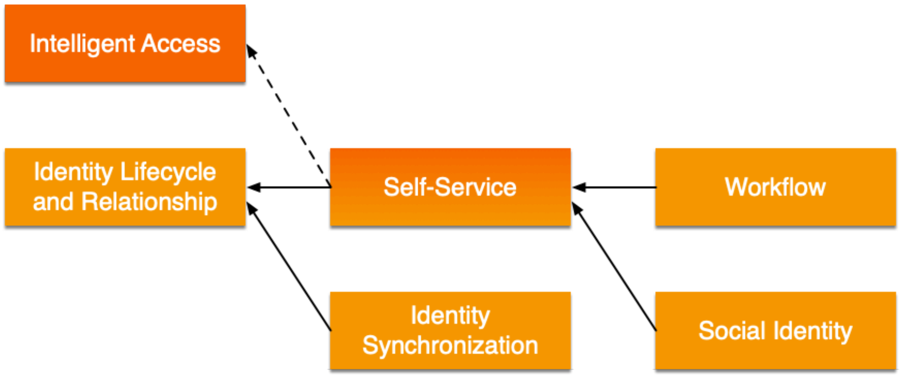
Identity Lifecycle and Relationship

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

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:



Identity Synchronization module

This module can serve as the foundation for provisioning and identity data reconciliation. Synchronization capabilities are available as a service and hrough 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.	Synchronization types
Reconciliation	Alignment between accounts across managed data stores.	Synchronization types
Password synchronization	Near real-time password synchronization across managed data stores.	Password synchronization plugins
Directory Services and Active Directory plugins	Native password synchronization plugins for ForgeRock Directory Services and Microsoft Active Directory.	Synchronize passwords with DS, Synchronize passwords with Active Directory

Feature	Description	Documentation
Delegated administration	Grant role-based, limited access to perform fine-grained administrative tasks on managed objects.	Delegated administration
All connectors	Extensible interoperability for identity, compliance, and risk management across a variety of specific applications and services.	Connector reference

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 Access. See 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.	Self-registration
Password reset	End-user self-service UI for changing and resetting passwords based on predefined policies and security questions.	Password reset
Knowledge-based authentication	Verification for user identities based on predefined and end user-created security questions.	Security questions

Feature	Description	Documentation
Forgotten username	Mechanisms to allow users to recover their usernames with predefined policies.	Username retrieval
Progressive profile completion	Short forms used to simplify registration and incrementally collect profile data over time.	Progressive profile
Profile and privacy management dashboard	Dashboard for managing personal user information.	Privacy: my account information in the End User UI
Consent and preference management	Configurable user preferences.	Privacy and consent
Terms and conditions (or terms of service) versioning	Manage multiple terms and conditions.	Terms & Conditions

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
BPMN 2.0 support	Standards-based Business Process Model and Notation 2.0 support.	BPMN 2.0 and workflow tools
Flowable process engine	Lightweight workflow and business process management platform.	Enable workflows
Workflow-driven provisioning	Define provisioning workflows for self-service, sunrise and sunset processes, approvals, escalations, and maintenance.	Create workflows, Invoke workflows

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.	Social registration
Authentication	Social login for identity management.	OpenID Connect authorization code flow
Account linking	Users can select specific social identity providers for logins.	Account claiming: links between accounts and social identity providers
Attribute scope management	Administrators can include any or all scopes available, by social identity provider.	Social registration

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.	Synchronization
Data modeling	Ability to map IDM objects to tables in a JDBC database or to organizational units in a DS repository.	Object mappings

Feature	Description	Documentation
Identity lifecycle management	An extensible object model that enables you to manage the complete lifecycle of identity objects.	Managed objects
Identity relationship lifecycle management	Ability to create and track relationship references between objects.	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.	Roles
Entitlement lifecycle management	Entitlements to provision attributes or sets of attributes, based on role membership.	Use assignments to provision users

Directory Services

ForgeRock Directory Services 7.5 serves as a foundation for LDAPv3 and RESTful directories.

Directory Services modules:

Directory Server

Directory Proxy Server

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
- REST API to access LDAP native capabilities over HTTP

Dependencies

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

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.	About directories
HDAP	Access LDAP data over HTTP using Directory Access Protocol (HDAP) APIs that transform HTTP operations into LDAP operations.	Learn HDAP
High-availability multi-master replication	Data replication for always-on services, enabling failover and disaster recovery.	Replication

Feature	Description	Documentation
User/object store	Flexible key-value data model for storing users, devices, and things.	Use LDAP
Passwords and data security	Password digests, encryption schemes, and customizable rules for password policy compliance to help protect data on disk and shared infrastructure.	Data encryption, Passwords
REST APIs and REST to LDAP gateway (deprecated)	HTTP-based RESTful access to user data.	Use REST/HTTP
DSMLv2 gateway (deprecated)	HTTP-based SOAP access to LDAP operations for web services.	Install a DSML gateway

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.	Single point of access
High service availability	LDAP services with reliable crossover and DN-based routing.	High availability

Feature	Description	Documentation
Load balancing and failover	Configurable load balancing across directory servers with redundancy, and capabilities to handle referrals, connection failures, and network partitions.	Load balancing
Protection for Directory Services	Secure incoming and outgoing connections, and provide coarse-grained access control.	Secure connections and Proxy global policies
Scaling out using data distribution	Distribute data across multiple shards.	Data distribution
LDAPv3	Compliance with the latest LDAP protocol standards.	Supported standards
REST APIs	HTTP-based RESTful access to user data.	Use HDAP

Edge Security

Use the 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 module:

Edge Security Identity Gateway

Dependencies

The Edge Security Identity Gateway module is not dependent upon any other modules.

Edge Security 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.	Studio guide
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.	Password replay from AM, Password replay from a database, and Password replay from a file
Policy enforcement	Enforcement of centralized authorization policies for applications requiring Access Management.	Enforce policy decisions from AM and Harden authorization with advice from AM

Feature	Description	Documentation
Federation	OpenID Connect 1.0.	OpenID Connect
	OAuth 2.0.	IG as an OAuth 2.0 client and IG as an OAuth 2.0 resource server
	SAML 2.0.	SAML
	SAML resources for mobile applications.	Transform OpenID Connect ID tokens into SAML assertions
Finance APIs	Support for OAuth 2.0 Mutual TLS and Financial-Grade APIs.	Validate certificate-bound access tokens 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.	WebSocket traffic
Throttling	Throttling to limit access to protected applications.	Throttling
UMA resource server	Protection for resources and services according to the UMA 2.0 standard.	UMA support
DevOps tooling	Deployment of basic and customized configurations through Docker.	Deployment guide
Integration with ForgeRock Identity Cloud	Protection and integration of APIs and applications with ForgeRock Identity Cloud for authentication and authorization.	Identity Cloud guide

Feature	Description	Documentation
Microgateway	Identity Gateway standalone deployed as a microgateway, securing microservices with OAuth 2.0.	IG as a microgateway
Token Validation Microservice	Platform satellite for introspection of stateful and stateless OAuth 2.0 access tokens.	Token Validation Microservice User Guide

Was this helpful? 👍 👎