



Identity Platform Guide

/ ForgeRock Identity Platform 7.1

Latest update: 7.1.0

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

Copyright © 2016-2019 ForgeRock AS.

Abstract

Guide to ForgeRock Identity Platform™ modules.



This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

© Copyright 2010-2020 ForgeRock, Inc. All rights reserved. ForgeRock is a registered trademark of ForgeRock, Inc. Other marks appearing herein may be trademarks of their respective owners.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, and distribution. No part of this product or document may be reproduced in any form by any means without prior written authorization of ForgeRock and its licensors, if any.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESSED OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

DejaVu Fonts

Bitstream Vera Fonts Copyright

Copyright (c) 2003 by Bitstream, Inc. All Rights Reserved. Bitstream Vera is a trademark of Bitstream, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Bitstream" or the word "Vera".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Bitstream Vera" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL BITSTREAM OR THE GNOME FOUNDATION BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the names of Gnome, the Gnome Foundation, and Bitstream Inc., shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from the Gnome Foundation or Bitstream Inc., respectively. For further information, contact: fonts@gnome.org.

Arev Fonts Copyright

Copyright (c) 2006 by Tavmjong Bah. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the modifications to the Bitstream Vera Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Tavmjong Bah" or the word "Arev".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Tavmjong Bah Arev" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL TAVMJONG BAH BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the name of Tavmjong Bah shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from Tavmjong Bah. For further information, contact: tavmjong@free.fr.

FontAwesome Copyright

Copyright (c) 2017 by Dave Gandy, <https://fontawesome.com/>.

This Font Software is licensed under the SIL Open Font License, Version 1.1. See <https://opensource.org/licenses/OFL-1.1>.

Table of Contents

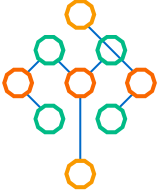
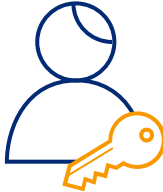

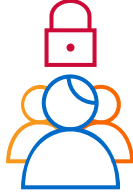
About the ForgeRock Identity Platform	iv
1. Access Management	1
Overview of Capabilities	1
Dependencies	2
Intelligent Access Module	2
Authorization Module	3
Federation Module	4
User-Managed Access Module	4
2. Identity Management	6
Overview of Capabilities	6
Dependencies	7
Identity Synchronization Module	7
Self-Service Module	8
Workflow Module	9
Social Identity Module	9
Identity Lifecycle and Relationship Module	10
Access Request Module	10
Access Review Module	11
3. Directory Services	12
Overview of Capabilities	12
Dependencies	13
Directory Server Module	13
Directory Proxy Server Module	13
4. Edge Security	15
Dependencies	15
Identity Gateway Module	15
Microservices Security Module	16

About the ForgeRock Identity Platform

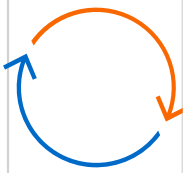
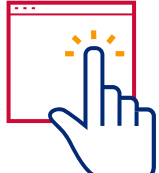
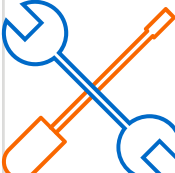



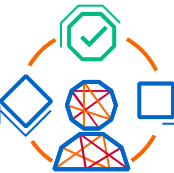
The ForgeRock Identity Platform is the only offering for access management, identity management, user-managed access, directory services, and an identity gateway, designed and built as a single, unified platform.

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:

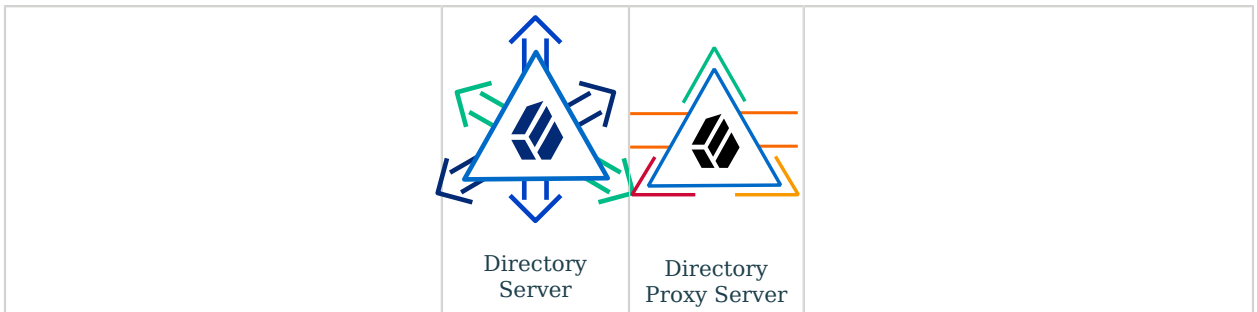
ForgeRock® Access Management (AM)

	 <p>Intelligent Access</p>	 <p>Authorization</p>	 <p>Federation</p>	 <p>User-Managed Access</p>	
--	---	--	---	---	--

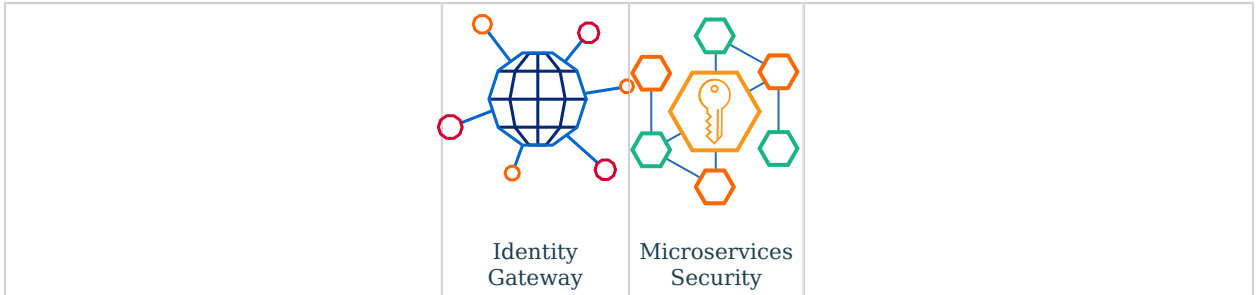
ForgeRock® Identity Management (IDM)

 <p>Identity Synchronization</p>	 <p>Self-Service</p>	 <p>Workflow</p>	 <p>Social Identity</p>	 <p>Identity Lifecycle and Relationship</p>	 <p>Access Request</p>	 <p>Access Review</p>
--	---	---	--	--	--	--

ForgeRock® Directory Services (DS)



ForgeRock® Edge Security



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

Cloud Developer's Kit (CDK) and Cloud Deployment Model (CDM)

The CDK and CDM demonstrates installation, configuration, and deployment of ForgeRock Identity Platform components using DevOps techniques.

See:

- [DevOps: Start Here](#)
- [Cloud Developer's Kit Documentation](#)
- [Cloud Deployment Model Documentation](#)
- [Deployment How-Tos](#)

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 Module".

See *MFA: Push Authentication and Transactional Authorization*.

For further details and help gaining access to additional software, contact ForgeRock at info@forgerock.com.

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

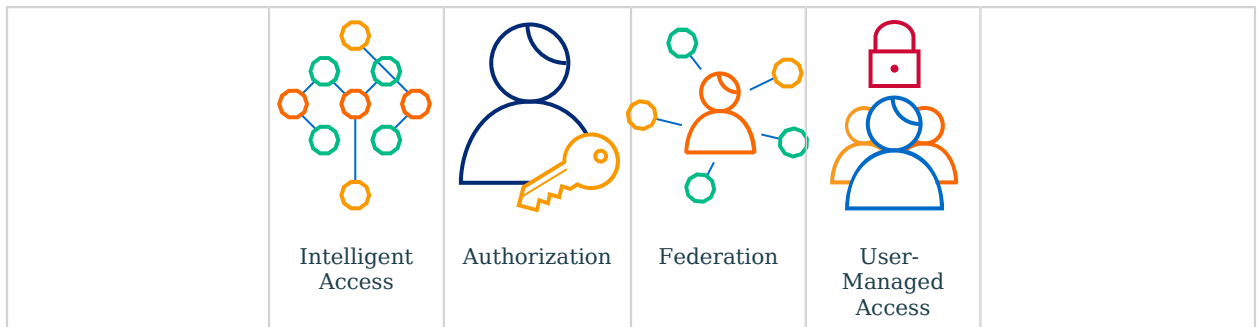
- ForgeRock Access Management 7.1, with Web Agent 5 and Java Agent 5
- ForgeRock Identity Management 7.1
- ForgeRock Directory Services 7.1
- ForgeRock Edge Security Modules

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:

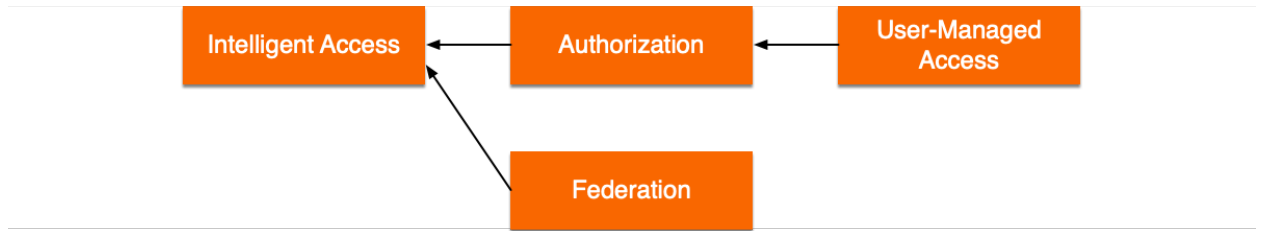


Overview of Capabilities

- 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 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.	<i>Authentication Nodes and Trees</i>
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.	<i>About Multi-Factor Authentication</i>

Feature	Description	Documentation
External Configuration Store	Configuration storage in ForgeRock Directory Services for high-availability.	<i>Preparing Configuration Stores</i>
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.	<i>Introducing the Security Token Service</i>
Web and Java Agents for SSO	Intercept requests to access protected resources and redirect for appropriate authentication.	<i>Web Agents User Guide</i> and <i>Java Agents User Guide</i>
User Login Analytics	Measure authentication flows using counters and start/stop timers to monitor performance.	<i>Timer Start Node, Timer Stop Node, Meter Node, and Monitoring Metric Types</i>

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.	<i>About Authorization and Policy Decisions</i>
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.	<i>Web Agents User Guide</i> and <i>Java Agents User Guide</i>
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.	<i>Transactional Authorization</i>

Feature	Description	Documentation
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.	<i>Dynamic OAuth 2.0 Authorization</i>

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.	<i>Configuring IdPs, SPs, and COTs</i>
SAML 2.0 SSO and SLO	Web Single Sign-On and Single Logout profile support.	<i>Implementing SSO and SLO</i>
ADFS	Federation with Active Directory Federation Services.	<i>Introducing SAML v2.0</i>
SAML 2.0 Attribute and Advanced Profiles	Support for transmitting only attributes used by targeted applications.	<i>SAML v2.0 Guide</i>
OpenID Connect	OpenID Connect 1.0 compliance for running an OpenID Provider, including advanced profiles, such as Mobile Connect.	<i>OpenID Connect 1.0 Guide</i>
OAuth 2.0	OAuth 2.0 compliance for running an authorization server.	<i>OAuth 2.0 Guide</i>
Social Login	For acting as an OAuth 2.0 client of social identity providers, such as Facebook, Google, and Microsoft.	<i>Social Authentication</i>
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.	<i>Dynamic OAuth 2.0 Authorization</i>

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.

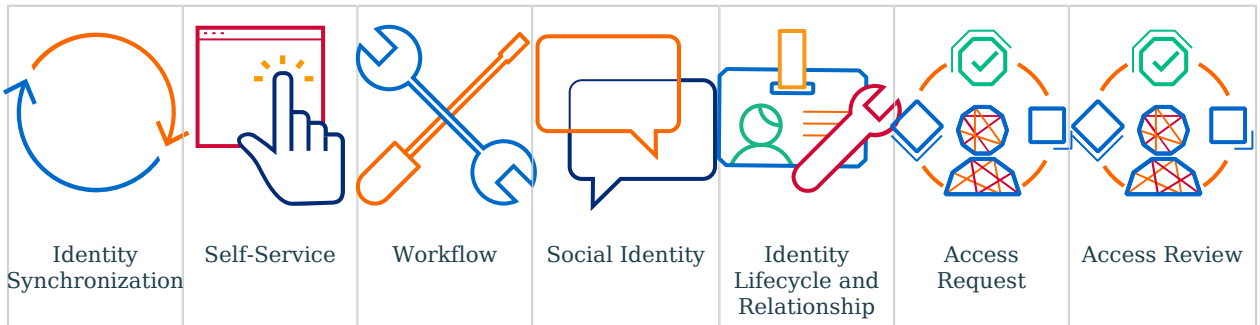
Required modules: Authorization, Intelligent Access.

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.	<i>UMA 2.0 Guide</i>
UMA Authorization Server	Authorization server with dynamic resource set registration, end user control of resource sharing, responses to access requests, and full audit history.	<i>AM as the UMA Authorization Server</i>
UMA Protector	ForgeRock Identity Gateway protection for resources and services with the UMA 2.0 standard.	<i>Supporting UMA Resource Servers</i>

Chapter 2 Identity Management

ForgeRock Identity Management 7.1 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:



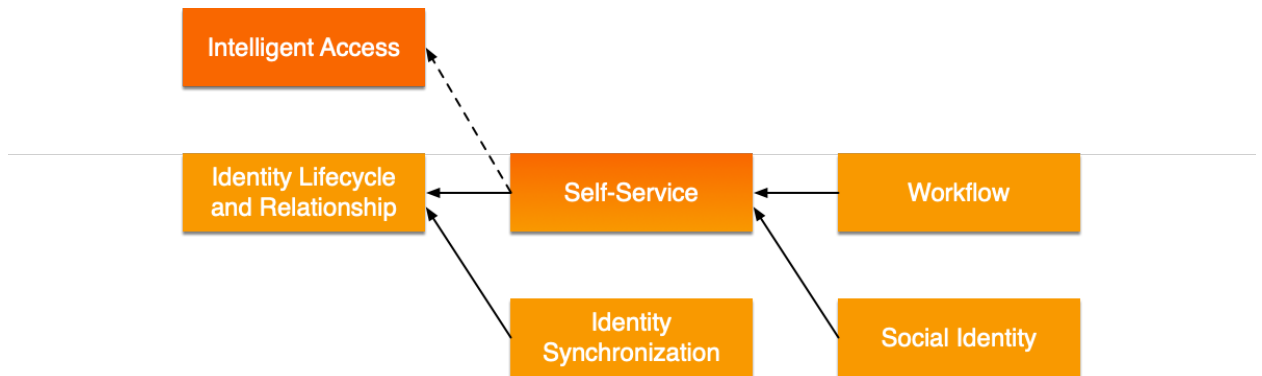
Overview of Capabilities

- 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)

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 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.	<i>LiveSync</i>

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

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 the *User Self-Service Guide* 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.	<i>Self Registration</i>
Password Reset	End-user self-service UI for changing and resetting passwords based on predefined policies and security questions.	<i>Password Reset</i>
Knowledge-Based Authentication	Verification for user identities based on predefined and end user-created security questions.	<i>Configure Security Questions</i>
Forgotten Username	Mechanisms to allow users to recover their usernames with predefined policies.	<i>Username Retrieval</i>

Feature	Description	Documentation
Progressive Profile Completion	Short forms used to simplify registration and incrementally collect profile data over time.	<i>Progressive Profile</i>
Profile and Privacy Management Dashboard	Dashboard for managing personal user information.	<i>Privacy: My Account Information in the End User UI</i>
Consent and Preference Management	Configurable user preferences.	<i>Configure Privacy and Consent</i>
Terms and Conditions (or Terms of Service) Versioning	Manage multiple terms and conditions.	<i>Terms & Conditions</i>

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.	<i>BPMN 2.0 and Workflow Tools</i>
Flowable Process Engine	Lightweight workflow and business process management platform.	<i>Enable Workflows</i>
Workflow-Driven Provisioning	Define provisioning workflows for self-service, sunrise and sunset processes, approvals, escalations, and maintenance.	<i>Create Workflows, Invoke Workflows</i>

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.	<i>Social Registration</i>

Feature	Description	Documentation
Authentication	Social login for identity management.	<i>OpenID Connect Authorization Code Flow</i>
Account Linking	Users can select specific social identity providers for logins.	<i>Account Claiming: Links Between Accounts and Social Identity Providers</i>
Attribute Scope Management	Administrators can include any or all scopes available, by social identity provider.	<i>Social Registration</i>

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.	<i>Synchronization Guide</i>
Data Modeling	Ability to map IDM objects to tables in a JDBC database or to organizational units in a DS repository.	<i>Generic and Explicit Object Mappings</i>
Identity Lifecycle Management	An extensible object model that enables you to manage the complete lifecycle of identity objects.	<i>Managed Objects</i>
Identity Relationship Lifecycle Management	Ability to create and track relationship references between objects.	<i>Relationships Between Objects</i>
Role Lifecycle Management	Provisioning roles to control how objects are exported to external systems and authorization roles to control authorization within IDM.	<i>Roles</i>
Entitlement Lifecycle Management	Entitlements to provision attributes or sets of attributes, based on role membership.	<i>Use Assignments to Provision Users</i>

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.	<i>Access Request Documentation</i>
User Notifications	Access Request can send customizable user notifications for specific events that occur within the request process.	<i>Access Request Documentation</i>
Identity Glossary	The glossary provides consolidated management of entitlement metadata, bulk export and import, and extended relationship mapping.	<i>Access Request Documentation</i>

Access Review Module

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

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

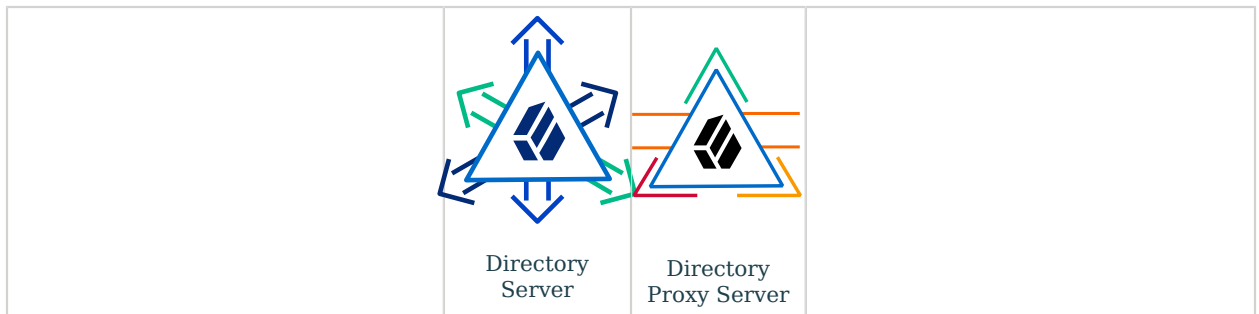
Feature	Description	Documentation
User Certification	Multi-stage certifications let any number of certifiers participate in access decision processes, and provide an escalation process to ensure timely responses.	<i>Access Review Documentation</i>
Role Management	An extensible glossary allows for consolidated management of role and entitlement metadata, bulk export and import, and extended relationship mapping.	<i>Access Review Documentation</i>
Policy Enforcement	Supports proper segregation of duties.	<i>Access Review Documentation</i>
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.	<i>Identity Reporting Documentation</i>

Chapter 3

Directory Services

ForgeRock Directory Services 7.1 serves as a foundation for LDAPv3 and RESTful directories.

Directory Services modules:



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

Dependencies

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

Directory Server Module

The ForgeRock Directory Server module helps you 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.	<i>About Directories</i>
REST APIs and REST to LDAP Gateway	HTTP-based RESTful access to user data and server configuration.	<i>Configure HTTP User APIs</i>
DSMLv2 Gateway	HTTP-based SOAP access to LDAP operations for web services.	<i>Install a DSML Gateway</i>
High-Availability Multi-Master Replication	Data replication for always-on services, enabling failover and disaster recovery.	<i>Replication</i>
User/Object Store	Flexible key-value data model for storing users, devices, and things.	<i>Use LDAP</i>
Passwords and Data Security	Password digests, encryption schemes, and customizable rules for password policy compliance to help protect data on disk and shared infrastructure.	<i>Data Encryption, Passwords</i>

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.

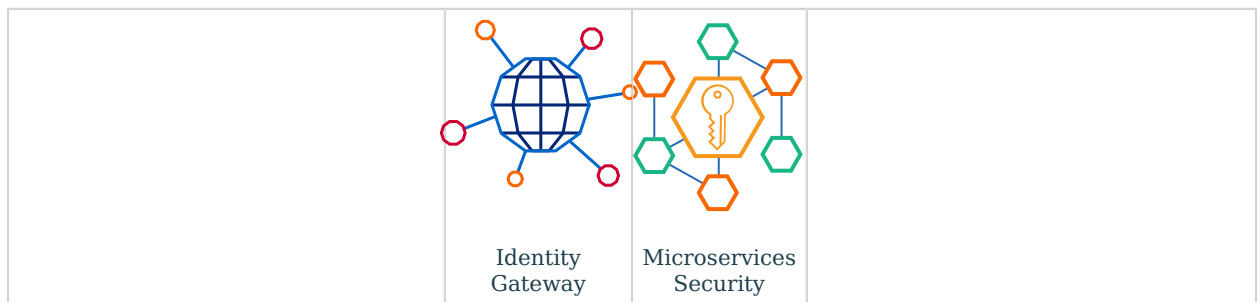
Feature	Description	Documentation
Single Point of Access	Uniform view of underlying LDAPv3 directory services for client applications.	<i>Single Point of Access</i>
High Service Availability	LDAP services with reliable crossover and DN-based routing.	<i>High Availability</i>
Load Balancing and Failover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

Chapter 4

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 modules:



Dependencies

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

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.	<i>Studio Guide</i>
Single Sign-On	Single sign-on in a single domain and across domains.	<i>Single Sign-On and Cross-Domain Single Sign-On</i>
Password Replay	Secure replay of credentials to legacy applications or APIs.	<i>Getting Login Credentials From Data Sources and Get Login Credentials From AM</i>
Policy Enforcement	Enforcement of centralized authorization policies for applications requiring Access Management.	<i>Enforce Policy Decisions From AM and Harden Authorization With Advice From AM</i>
Federation	OpenID Connect 1.0.	<i>Act As an OpenID Connect Relying Party</i>
	OAuth 2.0.	<i>Act As an OAuth 2.0 Resource Server</i>
	SAML 2.0.	<i>Act As a SAML 2.0 Service Provider</i>
	SAML resources for mobile applications.	<i>Transform OpenID Connect ID Tokens Into SAML Assertions</i>
Finance APIs	Support for OAuth 2.0 Mutual TLS and Financial-Grade APIs.	<i>Validate Certificate-Bound Access Tokens and FapiInteractionIdFilter</i>
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.	<i>Proxy WebSocket Traffic</i>
Throttling	Throttling to limit access to protected applications.	<i>Throttle the Rate of Requests to Protected Applications</i>
UMA Resource Server	Protection for resources and services according to the UMA 2.0 standard.	<i>Support UMA Resource Servers</i>
DevOps Tooling	Deployment of basic and customized configurations through Docker.	<i>Deployment Guide</i>
Integration with ForgeRock Identity Cloud	Protection and integration of APIs and applications with ForgeRock Identity Cloud for authentication and authorization.	<i>Identity Cloud Guide</i>

Microservices Security Module

Required modules: none.

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