



Identity Platform Guide

/ ForgeRock Identity Platform 6

Latest update: 6.0.0

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

Copyright © 2016-2022 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.

ForgeRock® and ForgeRock Identity Platform™ are trademarks of ForgeRock Inc. or its subsidiaries in the U.S. and in other countries. Trademarks are the property of their respective owners.

UNLESS OTHERWISE MUTUALLY AGREED BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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 NONINFRINGEMENT 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 at gnome dot 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 NONINFRINGEMENT 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, <http://fontawesome.io>.

This Font Software is licensed under the SIL Open Font License, Version 1.1. This license is available with a FAQ at: <http://scripts.sil.org/OFL>.

Table of Contents

About the ForgeRock Identity Platform	iv
1. Access Management	1
1.1. Intelligent Authentication Module	1
1.2. Authorization Module	3
1.3. Federation Module	4
1.4. User-Managed Access Module	4
2. Identity Management	6
2.1. Identity Synchronization Module	6
2.2. Self-Service Module	7
2.3. Workflow Module	8
2.4. Social Identity Module	8
3. Directory Services	10
3.1. Directory Server Module	10
3.2. Directory Proxy Server Module	11
4. Identity Gateway	12
4.1. Identity Gateway Module	12

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 Identity Platform Modules" summarizes the modules available.

ForgeRock Identity Platform Modules

Core Solution	Module	Find Details In
ForgeRock Access Management (AM)	Intelligent Authentication	"Intelligent Authentication Module"
	Authorization	"Authorization Module"
	Federation	"Federation Module"
	User-Managed Access	"User-Managed Access Module"
ForgeRock Identity Management (IDM)	Identity Synchronization	"Identity Synchronization Module"
	Self-Service	"Self-Service Module"
	Workflow	"Workflow Module"
	Social Identity	"Social Identity Module"
ForgeRock Directory Services (DS)	Directory Server	"Directory Server Module"
	Directory Proxy Server	"Directory Proxy Server Module"
ForgeRock Identity Gateway (IG)	Identity Gateway	"Identity Gateway Module"

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 DevOps Guide.

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 versions:

- ForgeRock Access Management 6, with Web Agent 5 and Java Agent 5
- ForgeRock Identity Management 6
- ForgeRock Directory Services 6
- ForgeRock Identity Gateway 6

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

The ForgeRock Access Management 6 software provides the following 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

1.1. 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.

Intelligent authentication module features are described in "Module Features".

Module Features

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>About Authentication Trees</i>
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 must be evaluated by one module before control passes to another module.	<i>Authentication Module Properties</i>
Adaptive Risk Module	Risk assessment based on predetermined characteristics to determine whether to complete further authentication steps in a chain.	<i>Adaptive Risk Authentication Module</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>
External Configuration Store	Configuration storage in ForgeRock Directory Services for high-availability.	<i>Preparing an External Configuration Data Store</i>
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.	<i>Introducing the Security Token Service</i>

Feature	Description	Documentation
Web and Java Agents for SSO	Intercept requests to access protected resources and redirect for appropriate authentication.	<i>Web Agents User Guide and Java Agents User Guide</i>
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.	<i>Sample Mobile Authentication Applications</i>
User Login Analytics	Measure authentication flows using counters and start/stop timers to monitor performance.	<i>Timer Node Start, Timer Node Stop, Meter Node, and Monitoring Metric Types</i>

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 "Module Features".

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 without touching the underlying applications	<i>Introducing Authorization</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 and 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>Implementing Transactional Authorization</i>
OAuth 2.0 Dynamic Scopes	A single OAuth 2.0 client configured for a comprehensive list of scopes can serve different scope subsets	<i>Policy Decisions and Authorization Examples</i>

Feature	Description	Documentation
	to resource owners based on policy conditions.	

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 "Module Features".

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

1.4. 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.

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

Module Features

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>Introducing UMA 2.0</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>Introducing UMA 2.0</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 6 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 6 software provides 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-service
- Privacy and consent
- Progressive profile completion
- 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 "Module Features".

Module Features

Feature	Description	Documentation
Discovery and Synchronization	Synchronization of identity data across managed data stores	<i>Synchronizing Data Between Resources</i>
Reconciliation	Alignment between accounts across managed data stores	<i>Managing 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>Synchronizing Passwords With ForgeRock Directory Services (DS), and Synchronizing Passwords With Active Directory</i>
Connector Servers for Java and .NET Connectors	Remote operation for provisioning across all managed data stores	<i>Overview of a Remote Connector Implementation</i>
All Connectors	Extensible interoperability for identity, compliance, and risk management across a variety of specific applications and services	<i>Connecting to External Resources</i>

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 "Module Features".

Module Features

Feature	Description	Documentation
Password Management	End-user self-service UI for changing and resetting passwords based on predefined policies and security questions	<i>Resetting User Passwords</i>
Password Reset	Mechanisms to allow users to reset their own passwords with predefined policies	<i>Configuring User Self-Service</i>

Feature	Description	Documentation
Knowledge-Based Authentication	Verification for user identities based on predefined and end user-created security questions	<i>Configuring Self-Service Questions (KBA)</i>
Forgotten Username	Mechanisms to allow users to recover their usernames with predefined policies	<i>Forgotten Username</i>
Progressive Profile Completion	Short forms used to simplify registration and incrementally collect profile data over time	<i>Progressive Profile Completion</i>
Profile and Privacy Management Dashboard	Dashboard for managing personal user information	<i>Privacy: My Account Information in the Self-Service UI</i>
Consent and Preference Management	Configurable user preferences	<i>Configuring Synchronization Filters With User Preferences</i>
Terms and Conditions (or Terms of Service) Versioning	Manage multiple terms and conditions	<i>Adding Terms and Conditions</i>

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 "Module Features".

Module Features

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

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 "Module Features".

Module Features

Feature	Description	Documentation
Registration	User registration with social identity accounts.	<i>Configuring Social Identity Providers</i>
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>Managing Links Between End User Accounts and Social ID Providers</i>
Attribute Scope Management	Administrators can include any or all scopes available, by social identity provider.	<i>Configuring Social Identity Providers</i>

Chapter 3

Directory Services

ForgeRock Directory Services 6 serves as a foundation for LDAPv3 and RESTful directories.

ForgeRock Directory Services software provides 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 Server Module

ForgeRock Directory Server module features are described in "Module Features".

Module Features

Feature	Description	Documentation
LDAPv3	Compliance with the latest LDAP protocol standards	<i>Understanding Directory Services</i>
REST APIs and REST to LDAP Gateway	HTTP-based RESTful access to user data and server configuration	<i>RESTful Client Access Over HTTP</i>
DSMLv2 Gateway	HTTP-based SOAP access to LDAP operations for web services	<i>DSML Client Access</i>

Feature	Description	Documentation
High-Availability Multi-Master Replication	Data replication for always-on services, enabling failover and disaster recovery	<i>Managing Data Replication</i>
Embedded Databases	Choice of Oracle Berkeley DB or ForgeRock DB	<i>Creating a New Database Backend</i>
User/Object Store	Flexible key-value data model for storing users, devices, and things	<i>Managing Directory Data</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>Encrypting Directory Data, Configuring Password Policy</i>

3.2. Directory Proxy Server Module

ForgeRock Directory Proxy Server module features are described in "Module Features".

Module Features

Feature	Description	Documentation
Single Point of Access	Uniform view of underlying LDAPv3 directory services for client applications	<i>Deploying a Single Point of Directory Access</i>
High Service Availability	LDAP services with reliable crossover and DN-based routing	<i>Deploying Proxy Services for 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>Choosing a Load Balancing Algorithm</i>
Protection For Directory Services	Secure incoming and outgoing connections, and provide coarse-grained access control	<i>Securing Network Connections, About Global Access Control Policies</i>
LDAPv3	Compliance with the latest LDAP protocol standards	<i>Understanding Directory Services</i>
REST APIs	HTTP-based RESTful access to user data and server configuration	<i>RESTful Client Access Over HTTP</i>

Chapter 4

Identity Gateway

ForgeRock Identity Gateway 6 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

4.1. Identity Gateway Module

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

Module Features

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

Feature	Description	Documentation
AM STS Token Translator	Access to SAML resources for mobile applications (requires Access Management)	<i>Transforming OpenID Connect ID Tokens Into SAML Assertions</i>
Throttling	Throttling to limit access to protected applications	<i>Throttling the Rate of Requests to Protected Applications</i>
Password Replay	Secure replay of credentials to legacy applications or APIs	<i>Getting Login Credentials From Data Sources</i>
Studio	User interface for rapid development and prototyping	<i>Creating Routes Through IG Studio</i>
DevOps Tooling	Deploying Basic and Customized Configurations Through Docker	<i>Deployment Guide</i>
UMA Resource Server	Protection for resources and services according to the UMA 2.0 standard	<i>Supporting UMA Resource Servers</i>