ForgeRock® Identity Gateway Core Concepts

Code:	IG-400
Length:	4 days
URL:	View Online

The ForgeRock® Identity Gateway Core Concepts course is for students who want to examine core concepts and implement key use cases and features of ForgeRock Identity Gateway (IG) to help extend access to and protect web applications, legacy applications, and application programming interfaces (APIs), within an access management solution. This course comprises a mix of instructor-led lessons and demonstrations with plenty of lab exercises to ensure an opportunity to fully understand each of the topics covered. It provides students with the necessary skills to plan, install, configure, and administer an IG deployment. The main goal of the course is to provide a thorough understanding of, and hands-on experience with IG, so students can control the most important functions of and manage a successful production deployment. Note that Revision B of this course is built on version 6.5 of ForgeRock Identity Gateway.

Skills Gained

Upon completion of this course, you should be able to:

- Describe the role and use cases where IG fits within a ForgeRock Identity Platform™ solution, the basic concepts of IG, and how to perform a basic installation and configuration of IG.
- Use IG to protect a legacy application.
- Configure agentless single sign-on with IG, where authentication can be delegated to AM, including cross-domain, to an OIDC provider, or to a SAML2 Identity provider.
- Extend IG to support the retrieval of user profile attributes.
- Use IG as a policy enforcement point to protect a given web application, where AM is the policy decision point, and configure authentication step-up and transactional authorization.
- Protect a REST API using OAuth2-based solutions.
- Extend the solution using scripting.
- Prepare for production of an IG project by addressing maintenance, tuning, security, and deployment questions.

Who Can Benefit

The following are the target audiences for this course:

- System Integrators
- System Consultants
- System Architects
- System Administrators
- Web Developers

Prerequisites

The following are the prerequisites to successfully completing this course:

- Basic knowledge and skills using the Linux operating system to complete labs
- Basic knowledge of HTTP and communications between clients and web applications is critical to understanding and working with IG
- Basic knowledge of JSON, JavaScript, REST, Java, Groovy, SQL, and XML helpful in understanding examples, especially Groovy for scripting within IG
- Attendance at AM400 ForgeRock Access Management Core Concepts course or equivalent knowledge

Course Details

Course Contents

Chapter 1: Integrating a web site and a legacy application with IG

Describe the role and use cases where IG fits within a ForgeRock Identity Platform solution, basic concepts of IG, and how to perform a basic installation and configuration of IG.

Lesson 1: Introducing ForgeRock Identity Gateway

- Provide an overview of IG
- Discuss IG use cases
- Present IG features

Lesson 2: Fronting a website with IG

- Show how IG acts as a reverse proxy
- Discuss proxying WebSocket traffic
- Describe installation requirements and install IG
- Use IG Studio to protect a website
- Examine IG configuration structure

Lesson 3: Routing and processing requests and responses

- Understand how IG routes requests depending on external conditions
- Describe how Handlers direct requests and responses within a route
- Explain how filters process requests and responses
- Implement password replay

Lesson 4: Understanding IG Object Model and Logging

- Understand the IG object model
- Examine request, response, context and session
- Use a CaptureDecorator to perform logging
- Configure the FileAttributesFilter

Chapter 2: Configuring Agentless Single Sign-On

Demonstrate how to integrate single sign-on in an IG solution by delegating authentication to either an AM solution, including cross-domain, an OIDC provider, or a SAML2 Identity provider.

Lesson 1: Implementing authentication with the SingleSignOnFilter

- Use Freeform technology preview to protect a website
- Configure an AM Service
- Describe the use of the SingleSignOnFilter
- Retrieve information from AM using the UserProfileFilter and SessionInfoFilter

Lesson 2: Configuring CDSSO for the legacy application

- Describe and implement a CrossDomainSingleSignOnFilter

Lesson 3: Performing SSO with IG as an OpenID Connect relying party

- Describe and implement an OAuth2ClientFilter

Lesson 4: Providing SSO with IG as a SAML2 Service Provider

- Describe and implement a SAML2FederationHandler
- Describe and implement a DispatchHandler

Chapter 3: Controlling access with IG as Policy Enforcement Point

Use IG as a policy enforcement point to protect a given web application, where AM is the policy decision point, using policies and policies with advice to provide authentication step-up and transactional authorization.

Lesson 1: Implementing authorization with a PolicyEnforcementFilter

- Describe and implement a PolicyEnforcementFilter

Lesson 2: Providing step-up authentication and transactional authorization

- Describe and implement step-up authentication
- Describe and implement transactional authorization

Chapter 4: Protecting a REST API

Use IG as an OAuth2 resource server to protect a REST API and demonstrate how the solution can be extended by using scripting.

Lesson 1: Configuring IG as an OAuth2 resource server

- Describe and implement an OAuth2ResourceServerFilter
- List access token resolvers
- Observe the flow with the TokenIntrospectionAccessTokenResolver

Lesson 2: Extending functionality with scripts

- Describe the scripting framework for extending IG functionality
- Examine and implement dynamic scopes solution

Chapter 5: Preparing for production with IG

Highlight various areas that must be taken into account when preparing to go to production with an IG solution, such as

maintenance, tuning, security, and deployment.

Lesson 1: Auditing, monitoring and tuning an IG solution

- Describe and implement auditing
- Discuss monitoring
- Examine tuning questions

Lesson 2: Developing awareness of security questions with IG

- Discuss IG best practices regarding security
- Examine and implement common secrets
- Describe and implement throttling

Lesson 3: Deploying IG

- Describe and implement property value substitution
- Set up multiple IG instances

Schedule (as of 3)

Date	Location	
Feb 18, 2020 – Feb 21, 2020	San Francisco	Enroll
Feb 18, 2020 – Feb 21, 2020	MVP San Jose	Enroll
Feb 18, 2020 – Feb 21, 2020	MVP Sacramento	Enroll
Feb 18, 2020 – Feb 21, 2020	iMVP	Enroll
Apr 6, 2020 – Apr 9, 2020	McLean	Enroll
Apr 6, 2020 – Apr 9, 2020	MVP Ottawa	Enroll
Apr 6, 2020 – Apr 9, 2020	MVP Toronto	Enroll
Apr 6, 2020 – Apr 9, 2020	MVP King of Prussia	Enroll
Apr 6, 2020 – Apr 9, 2020	MVP Edison	Enroll
Apr 6, 2020 – Apr 9, 2020	iMVP	Enroll
Jun 1, 2020 – Jun 4, 2020	McLean	Enroll
Jun 1, 2020 – Jun 4, 2020	MVP Ottawa	Enroll
Jun 1, 2020 – Jun 4, 2020	MVP Toronto	Enroll
Jun 1, 2020 – Jun 4, 2020	MVP King of Prussia	Enroll
Jun 1, 2020 – Jun 4, 2020	MVP Edison	Enroll
Jun 1, 2020 – Jun 4, 2020	iMVP	Enroll
Aug 4, 2020 – Aug 7, 2020	McLean	Enroll
Aug 4, 2020 – Aug 7, 2020	MVP Ottawa	Enroll
Aug 4, 2020 – Aug 7, 2020	MVP Toronto	Enroll
Aug 4, 2020 – Aug 7, 2020	MVP King of Prussia	Enroll

Aug 4, 2020 – Aug 7, 2020	MVP Edison	Enroll
Aug 4, 2020 – Aug 7, 2020	iMVP	Enroll
Oct 13, 2020 – Oct 16, 2020	San Francisco	Enroll
Oct 13, 2020 – Oct 16, 2020	MVP Sacramento	Enroll
Oct 13, 2020 – Oct 16, 2020	iMVP	Enroll
Dec 8, 2020 – Dec 11, 2020	McLean	Enroll
Dec 8, 2020 – Dec 11, 2020	MVP Ottawa	Enroll
Dec 8, 2020 – Dec 11, 2020	MVP Toronto	Enroll
Dec 8, 2020 – Dec 11, 2020	MVP King of Prussia	Enroll
Dec 8, 2020 – Dec 11, 2020	MVP Edison	Enroll
Dec 8, 2020 – Dec 11, 2020	iMVP	Enroll