ForgeRock Access Management Customization and APIs

Code: AM-421
Length: 5 days
URL: View Online

This course provides a hands-on technical introduction to ForgeRock® Access Management (AM) APIs and customization use cases. Students examine AM extension points and gain the skills required to extend and integrate an AM deployment in a real-world context. Additionally, students learn to implement various clients that communicate with AM. Development and testing best practices are demonstrated in a series of labs.

- This course uses version 7.3.0 of AM

Skills Gained

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

- List the extension points of AM
- List which customizable components are affected in common AM use cases
- Understand the basic concepts of scripting
- Use the administration interface to look up, edit, and configure scripts
- Describe how AM performs authentication
- Review authentication nodes and authentication trees
- Design and implement a custom authentication node
- Describe how scripted authentication works
- Explore how client-side scripts can be used with authentication nodes and trees
- Describe how server-side scripted authentication operates with authentication nodes and trees
- Use the administration interface to create and test authentication trees containing scripted nodes
- Discuss the policy concepts in AM
- Implement an EntitlementCondition or a scripted condition
- Describe the ForgeRock® Common REST API (Common REST)
- Enable Cross-Origin Resource Sharing (CORS) in AM
- Authenticate users through the REST API
- Manage identities and realms through the REST API
- Implement password reset by using the REST API
- Use the policy engine to protect non-URL-based resources
- Describe the policy management and evaluation REST APIs
- Describe OAuth 2.0 and OpenID Connect, including how to use their HTTP endpoints

- Demonstrate scope validation and customize the default behavior

Who Can Benefit

The following are the target audiences for this course:

- Application Developers, adapting client applications to use AM capabilities
- Software Developers, extending and integrating AM services for their organizations
- System Consultants
- System Architects

Prerequisites

The following are prerequisites to successfully completing this course:

- Completion of the AM-410 or IC-410 course or hands-on experience with AM
- Basic knowledge and skills using the Linux operating system to complete labs
- Knowledge of JSON, JavaScript, AngularJS, REST, Java, Groovy, and XML is important for mastering an understanding of material and examples
- Basic knowledge of LDAP may be helpful for understanding code and some examples

Course Details

Course Outline

Chapter 1: Introducing Customization in AM

- Lesson 1: Using Extension (Customization) Points

Chapter 2: Customizing Authentication

- Lesson 1: Introducing Authentication Trees and Nodes
- Lesson 2: Customizing with Authentication Trees and Nodes
- Lesson 3: Developing Scripts with Scripting APIs
- Lesson 4: Migrating Authentication Modules to Authentication Trees and Nodes

Chapter 3: Customizing Authorization

- Lesson 1: Customizing Authorization

Chapter 4: Customizing with REST Clients

- Lesson 1: Using the REST API
- Lesson 2: Authenticating with REST
- Lesson 3: Working with RESTful User Self-Service API
- Lesson 4: Authorizing with REST

Chapter 5: Federating with OAuth 2.0

- Lesson 1: Implementing OAuth Custom Scopes

Schedule (as of 3)

Date	Location	
Jun 10, 2024 – Jun 14, 2024	Live Virtual	**Enroll**