ForgeRock® Access Management and ForgeRock® Identity Management Combination Course

Code:	FR-641
Length:	5 days
URL:	View Online

This structured 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 a strong foundation for the design, installation, configuration, and administration of a ForgeRock® Access Management (AM) solution and how to implement ForgeRock® Identity Management (IDM) to manage the lifecycle and relationship of digital identities within the context of a Customer Identity and Access Management solution (CIAM), and the integration with the ForgeRock Identity Platform™.

- At this time this course is only available for private deliveries. Please contact us to learn more.

Who Can Benefit

The following are the target audiences for this course:

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

Prerequisites

The following are the prerequisites to successfully completing this course:

- Knowledge of Unix/Linux commands and text editing
- An appreciation of HTTP and web applications
- A basic appreciation of how directory servers function
- A basic understanding of REST
- A basic knowledge of Java based environments would be beneficial. Programming experience is not required.
- Basic knowledge and skills using the Linux operating system to complete labs
- Basic knowledge of JSON, JavaScript, REST and Java is helpful for understanding examples; however, programming experience is not required

Course Details

Chapter 1: Performing Basic Configuration

Lesson 1: Implementing Default Authentication

- Describe how to use AM to manage default authentication using cookies
- Implement default authentication with AM
- Understand the need for and the use of realms
- Implement separation of admins and users using realms
- Observe the function of cookies

Lesson 2: Protecting a Website

- List and describe AM authentication clients
- Describe web agent main functionality
- Implement policy enforcement using web agents
- Analyze the am-auth-jwt cookie

Lesson 3: Empowering Users Through Self-Service

- Describe the main capabilities of user self-service
- Configure user self-service self-registration basic flow

Chapter 2: Implementing Intelligent Authentication

Lesson 1: Extending Authentication Functionality

- Describe the authentication mechanisms of AM
- List the available nodes
- Compare tree and chain mechanisms
- Identify realm-level authentication settings
- Use the authentication tree designer and ForgeRock’s Marketplace
- Create and test an authentication tree containing an LDAP Decision node
- Use the recording tool for troubleshooting

Lesson 2: Retrieving User Information

- Understand the use of an identity store
- Explain the distinction between identity store and credentials store
- Implement user-specific features on the website
- Retrieve user profile information using REST

Lesson 3: Increasing Authentication Security

- Discuss the need to increase authentication security
- Implement account lockout
- Configure risk-based authentication

- Configure second-factor authentication
- Demonstrate push notification authentication

Chapter 3: Introducing IDM and Getting Started

Lesson 1: Introducing IDM and Exploring the FEC Solution

- Describe how IDM is used in the ForgeRock Identity Platform to deliver a CIAM solution
- Demonstrate each of the core concepts from an end user and administrator perspective

Lesson 2: Installing IDM

- Describe the basic IDM installation requirements for deploying IDM
- Install and start IDM for the first time and explore the default UIs
- Start IDM with the CSV sample configuration and run the sample
- Start IDM with the LDAP sample configuration and run the sample

Lesson 3: Deploying and Managing IDM as a Project

- Set up a new IDM project for development
- Configure IDM to run as a background process

Lesson 4: Performing Basic IDM Troubleshooting

- Examine the different log files in IDM
- Get additional help troubleshooting outside of IDM

Chapter 4: Enabling User Registration and Self-Service

Lesson 1: Configuring the Default User Registration Process

- Configure the outbound email service
- Enable email-based self-registration

Lesson 2: Configuring IDM User Self-Service

- Enable email-based password reset and username retrieval
- Expand the KBA options
- Add a custom field to the Self-Service UI registration page

Lesson 3: Delegating Administration Privileges

- Add a new internal role and set up privileges to delegate administration

Chapter 5: Managing Synchronization and Reconciliation

Lesson 1: Using the REST Interface to Access IDM

- Query and manipulate IDM objects using the API Explorer and cURL

Lesson 2: Connecting to External Resources Using OpenICF

- Describe how to connect to external resources using OpenICF
- Add a connector to an external LDAP resource

Lesson 3: Performing Basic Synchronization

- Describe how to create sync mappings to flow identity objects and properties between IDM and one or more external resources
- Add a sync mapping from the IDM repository to the LDAP server
- Add a sync mapping from the LDAP server to the IDM repository

Lesson 4: Running Selective Synchronization and LiveSync

- Run selective synchronization using filters
- Identify methods of determining change events with LiveSync
- Schedule LiveSync with the LDAP directory

Lesson 5: Configuring Role-Based Provisioning

- Provision attributes to one or more external resources based on static role assignments
- Provision attributes to one or more external resources based on dynamic role assignments
- Add temporal constraints to a role