ForgeRock Access Management Essentials (On Demand)

Code: AM-100-OD
URL: View Online

This course provides a high-level overview of ForgeRock® Access Management (AM) so you can get started with the fundamentals of AM.

Skills Gained

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

- Describe AM core concepts
- Explain how to protect an application with intelligent authentication
- Understand how to control access with AM authorization
- Understand the role of AM when using OAuth2-based protocols to protect REST APIs
- Understand the role of AM when using OAuth2-based protocols to integrate mobile applications
- Describe how AM implements a zero trust approach to security
- Describe the role of AM in a SAML2 context

Who Can Benefit

The following are the target audiences for this course:

- Evaluators
- System Integrators
- System Consultants
- System Architects
- System Administrators

Course Details

Module 1: Introducing AM Core Concepts

Explain AM's approach to access management solutions, and how AM provides users with a great experience during their authentication journey:

- Introduce access management
- Provide a great user experience
- Demonstrate SSO between FEC website and AM

Module 2: Protecting an Application with Intelligent Authentication

Introduce the concept of intelligent authentication, describe the mechanisms used by AM to implement intelligent authentication, and the available authentication methods:

- Introduce intelligent authentication
- Describe authentication mechanisms
- Describe available nodes
- Describe multi-factor authentication
- Demonstrate various authentication methods

Module 3: Controlling Access to an Application with AM Authorization

Introduce the concept of entitlement management, describe the authorization mechanisms that AM provides to control access, and demonstrate how AM uses policies to restrict access to resources for a specific group of users:

- Introduce authorization
- Describe authorization mechanisms
- Demonstrate how access can be restricted to a specific group of users

Module 4: Protecting REST APIs and Integrating Mobile Applications with OAuth2-Based Protocols

Introduce OAuth2 and OIDC concepts, describe how AM can be configured as an authorization server or an OIDC provider, and explain how AM can be part of a solution that protects REST APIs and integrates mobile applications:

- Introduce AM roles in the OAuth2 and OpenID Connect (OIDC) contexts
- Protect a REST API
- Integrate a mobile application
- Demonstrate how REST clients obtain and use access and ID tokens

Module 5: Improving Security with a Zero Trust Approach

Introduce the concept of zero trust, describe how AM can take into account the context, check the risk level of requests continuously in order to take access decisions, explain how WebAuthn improves the user experience without impacting security, and demonstrate device nodes and WebAuthn:

- Introduce zero trust approach to security
- Calculate risk with contextual adaptive intelligent authentication
- Demonstrate the use of device nodes
- Check risk level continuously
- Improve user experience without impacting security with WebAuthN
- Demonstrate usernameless authentication with WebAuthn

Module 6: Integrating with Third-Party SAML2 Entities

Introduce SAML2 standard core concepts, explain how AM can be configured as a SAML2 service provider or identity provider, and demonstrate SSO between federated SAML2 entities:

- Introduce SAML2 standard
- Use AM as a SAML2 entity
- Demonstrate SSO between federated SAML2 entities