

Course Description

AM-410 Revision B.1

ForgeRock University
training@forgerock.com



ForgeRock®

ForgeRock® Access Management: Deep Dive

Description

The aim of this course is to showcase the key features and capabilities of the versatile and powerful ForgeRock® Access Management (AM). It provides the student with the knowledge and confidence to manage their own environment. It is accepted that this course is not able to demonstrate all the features and capabilities of AM. Further information and guidance can be found in the documentation and knowledge base in the online repositories at: Backstage <https://backstage.forgerock.com>.

Note: This course revision is based on version 7 of AM.

Target Audiences

The target audiences for this course include:

- ForgeRock Access Management Administrators
- System Integrators
- System Consultants
- System Architects
- System Developers

Objectives

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

- Start with an unprotected website and end up with a fully functional access management solution where every user trying to access the website is redirected to AM for authentication

- Improve access management security in AM with multi-factor authentication (MFA), context-based risk analysis, and continuous risk checking
- Implement OAuth 2.0 (OAuth2) based protocols; namely, OAuth2 and OpenID Connect 1.0 (OIDC), to enable low-level devices and mobile applications to make requests that access resources belonging to a subscriber. AM can be configured to function as an OIDC client and delegate authentication to social media OIDC providers
- Demonstrate federation across entities using SAML v2.0 (SAML2) with AM
- Install a new AM instance configured with external directory server data stores as the foundation for an AM cluster

Prerequisites

The following are the prerequisites for successfully completing this course:

- Completion of the ForgeRock® Access Management Essentials course available at:
<https://www.forgerock.com/support/university/forgerock-university/forgerock-access-management-essentials>
- Knowledge of UNIX/Linux commands
- An understanding of HTTP and web applications
- A basic understanding of how directory servers function
- A basic understanding of REST
- A basic knowledge of Java based environments would be beneficial, but no programming experience is required

Duration

5 days

Course Contents

Chapter 1: Enhancing Intelligent Access

Start with an unprotected website and end up with a fully functional access management solution where every user trying to access the website is redirected to AM for authentication.

Lesson 1: Exploring Authentication Mechanisms

Explore the AM Admin UI, view the role of cookies used during and after authentication, and describe authentication trees and nodes:

- Introduce AM authentication
- Understand realms

- Describe authentication life cycle
- Explain sessions
- Examine session cookies
- Access the lab environment
- Examine an initial AM installation
- Configure a realm and examine AM default authentication
- Experiment with session cookies
- Describe the authentication mechanisms of AM
- Create and manage trees
- Explore tree nodes
- Create a login tree
- Test the login tree

Lesson 2: Protecting a Website With IG

Show how ForgeRock® Identity Gateway (IG), integrated with AM, can protect a website:

- Present AM edge clients
- Describe IG functionality as an edge client
- Review the FEC website protected by IG
- Integrate the FEC website with AM
- Observe the IG token cookie
- (Optional) Review IG configuration
- Authenticate identities with AM
- Create an authentication tree with an LDAP Decision node
- Integrate identities in AM with an identity store
- Integrate an identity store with AM

Lesson 3: Controlling Access

Create security policies to control which users can access specific areas of the website:

- Describe entitlements with AM authorization
- Define AM policy components
- Define policy environment conditions and response attributes
- Describe the process of policy evaluation
- Implement access control on a website

Chapter 2: Improving Access Management Security

Improve access management security in AM with MFA, context-based risk analysis, and continuous risk checking.

Lesson 1: Increasing Authentication Security

Increase authentication security using MFA:

- Describe MFA
- Register a device
- Include recovery codes
- Examine OATH authentication
- Implement TOTP authentication
- (Optional) Implement HOTP authentication
- Examine Push notification authentication
- (Optional) Implement Push notification authentication
- Implement passwordless WebAuthn
- (Optional) Implement passwordless WebAuthn
- Examine HOTP authentication using email or SMS
- (Optional) Implement HOTP authentication using email or SMS

Lesson 2: Modifying a User's Authentication Experience Based on Context

Describe how AM can take into account the context of an authentication request in order to make access decisions:

- Introduce context-based risk analysis
- Describe device profile nodes
- Determine the risk based on the context
- Implement a browser context change script
- Lock and unlock accounts
- Implement account lockout

Lesson 3: Checking Risk Continuously

Review the AM tools used to check the risk level of requests continuously:

- Introduce continuous contextual authorization
- Describe step-up authentication
- Implement step-up authentication flow
- Describe transactional authorization
- Implement transactional authorization
- Prevent users from bypassing the default tree

Chapter 3: Extending Services Using OAuth2-Based Protocols

Implement OAuth2 based protocols; namely, OAuth2 and OIDC, to enable low-level devices and mobile applications to make requests that access resources belonging to a subscriber. AM can be configured to function as an OIDC client and delegate authentication to social media OIDC providers.

Lesson 1: Integrating Applications With OAuth2

Integrate clients using OAuth2 by demonstrating the use of the OAuth2 Device Code grant type flow with AM configured as the OAuth2 authorization server (AS):

- Discuss OAuth2 concepts
- Describe OAuth2 tokens and codes
- Describe refresh tokens, macaroons, and token modification
- Request OAuth2 access tokens with OAuth2 grant types
- Explain OAuth2 scopes and consent
- Configure OAuth2 in AM
- Configure AM as an OAuth2 provider
- Configure AM with an OAuth2 client
- Test the OAuth2 Device Code grant type flow

Lesson 2: Integrating Applications With OIDC

Integrate an application using OIDC and the Authorization grant type flow with AM as an OIDC provider:

- Introduce OIDC
- Describe OIDC tokens
- Explain OIDC scopes and claims
- List OIDC grant types
- Create and use an OIDC script
- Create an OIDC claims script
- Register an OIDC client and configure the OAuth2 Provider settings
- Test the OIDC Authorization Code grant type flow

Lesson 3: Authenticating OAuth2 Clients and using mTLS in OAuth2 for PoP

Authenticate OAuth2 clients with AM using various approaches and obtain certificate-bound access tokens using mutual TLS (mTLS) to provide token proof-of-possession (PoP):

- Examine OAuth2 client authentication
- Examine OAuth2 client authentication using JWT profiles

- Examine OAuth2 client authentication using mTLS
- Authenticate an OAuth2 client using mTLS
- Examine certificate-bound PoP when mTLS is configured
- Obtain a certificate-bound access token

Lesson 4: Transforming OAuth2 Tokens

Request and obtain security tokens from an OAuth2 authorization server, including security tokens that employ impersonation and delegation semantics:

- Describe OAuth2 token exchange
- Explain token exchange types and purpose for exchange
- Describe token scopes and claims
- Implement a token exchange impersonation pattern
- Implement a token exchange delegation pattern
- Configure token exchange in AM
- Configure AM for token exchange
- Test token exchange flows

Lesson 5: (Optional) Implementing Social Authentication

Provide a way for users to register and authenticate to AM using a social account:

- Delegate registration and authentication to social media providers
- Implement social registration and authentication with Google

Chapter 4: Federating Across Entities Using SAML2

Demonstrate federation across entities using SAML2 with AM.

Lesson 1: Implementing SSO Using SAML2

Demonstrate single sign-on (SSO) functionality across organizational boundaries:

- Discuss SAML2 entities and profiles
- Explain the SAML2 flow from the IdP point of view
- Examine SSO across SPs
- Configure AM as an IdP and integrate with third-party SPs
- Examine SSO between an SP and IdP and across SPs

Lesson 2: Delegating Authentication Using SAML2

Delegate authentication to a third-party IdP using SAML2 and examine the metadata:

- Explain the SSO flow from the SP point of view
- Describe the metadata content and purpose

- Configure AM as a SAML2 SP and integrate with a third-party IdP

Chapter 5: Installing and Deploying AM

Install a new AM instance configured with external directory server data stores as the foundation for an AM cluster, modify the AM configuration to harden security, upgrade an AM instance to a new version, and deploy the ForgeRock® Identity Platform (Identity Platform) to the Google Cloud Platform (GCP).

Lesson 1: Installing and Upgrading AM

Install AM using interactive and command-line methods creating the foundations for a cluster topology, and upgrade an AM 7.0.1 instance to AM 7.3:

- Plan deployment configurations
- Prepare before installing AM
- Deploy AM
- Outline tasks and methods to install AM
- Install AM with the web wizard
- Install an AM instance with the web wizard
- Install AM and manage configuration with Amster
- Install Amster
- Describe the AM bootstrap process
- Upgrade an AM instance
- Upgrade AM with the web wizard
- (Optional) Upgrade AM with the configuration tool

Lesson 2: Hardening AM Security

Explore a few default configuration and security settings that need to be modified before migrating to a production-ready solution:

- Harden AM security
- Adjust default settings
- Harden AM security
- Describe secrets, certificates, and keys
- Describe keystores and secret stores
- Manage the AM keystore, aliases, and passwords
- Configure and manage secret stores
- Configure an HSM secret store to sign OIDC ID tokens
- Describe the monitoring tools
- Describe the audit logging
- Describe debug logging

- Capture troubleshooting information
- Capture troubleshooting information

Lesson 3: Clustering AM

Create an AM cluster with a second AM instance added to the first AM instance that has already been installed:

- Explore high availability solutions
- Scale AM deployments
- Describe AM cluster concepts
- Create an AM cluster
- Prepare the initial AM cluster
- Install another AM server in the cluster
- Test AM cluster failover scenarios
- (Optional) Modify the cluster to use client-side sessions

Lesson 4: Deploying the Identity Platform to the Cloud

Deploy the Identity Platform into a cluster in a Google Kubernetes Environment (GKE):

- Describe the Identity Platform
- Prepare your deployment environment
- Deploy and access the Identity Platform
- Access and authenticate your GCP account
- Prepare to deploy the Identity Platform
- Deploy the Identity Platform with the Cloud Development Kit (CDK)
- Remove the Identity Platform deployment