Course Description

AIC-410 Revision A

Ping Training

training@pingidentity.com

PingOne Advanced Identity Cloud Deep Dive: Access Management

Ping Identity is starting to rebrand all products and courses under the Ping Identity brand. The content will remain the same and our curriculum developers will continue to prioritize courses that need development.

Description

The aim of this course is to showcase the key features and capabilities of the versatile and powerful access management solution in a PingOne Advanced Identity Cloud (Advanced Identity Cloud) environment, formerly known as ForgeRock® Identity Cloud. 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 the access management component of Advanced Identity Cloud. Further information and guidance can be found in the documentation and knowledge base in the online repositories at: Backstage https://backstage.forgerock.com.

Target Audiences

The target audiences for this course include:

- Advanced Identity Cloud 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 Advanced Identity Cloud for authentication
- Improve access management security in Advanced Identity Cloud 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.
- Demonstrate federation across entities using SAML2 with Advanced Identity Cloud

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-essentialss

- Completion of the *Getting Started With PingOne Advanced Identity Cloud for Administrators* course available at:

  https://www.forgerock.com/support/university/forgerock-university/getting-started-forgerock-identity-cloud

Duration

3 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 Advanced Identity Cloud) for authentication.

Lesson 1: Exploring Authentication Mechanisms

Explore the Identity Cloud Admin UI and view the role of cookies used during and after authentication:

- Introduce Identity Cloud authentication

- Describe authentication life cycle
- Explain sessions
- Examine session cookies
- Prepare the lab environment
- Examine Identity Cloud default authentication
- Experiment with session cookies
- Describe the authentication mechanisms of Identity Cloud
- Create and manage journeys
- Explore journey nodes
- Create a login journey
- Test the login journey

Lesson 2: Protecting a Website With IG

Show how IG, integrated with Identity Cloud, can protect a website:

- Present Identity Cloud edge clients
- Describe IG functionality as an edge client
- Review the FEC website protected by IG
- Integrate the FEC website with Identity Cloud
- Observe the IG token cookie
- (Optional) Review IG configuration

Lesson 3: Controlling Access

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

- Describe entitlements with Identity Cloud authorization
- Define Identity Cloud policy components
- Define policy environment conditions and response attributes
- Process of Identity Cloud policy evaluation
- Implement access control on a website

Chapter 2: Improving Access Management Security

Improve access management security in ForgeRock® Identity Cloud (Identity Cloud) with multi-factor authentication (MFA), context-based risk analysis, and continuous risk checking.

Lesson 1: Increasing Authentication Security

Increase authentication security using MFA:

- Describe multi-factor authentication
- Register a device
- Include recovery codes

- Examine OATH authentication
- Implement TOTP authentication
- (Optional) Implement HOTP authentication
- Examine 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 Journey Based on Context

Describe how Identity Cloud can take into account the context of an authentication request in order to take 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 Identity Cloud 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 journey

Chapter 3: Extending Services Using OAuth2-Based Protocols

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. ForgeRock® Identity Cloud (Identity Cloud) is also 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 Identity Cloud configured as the OAuth2 authorization server:

- 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 Identity Cloud
- Configure Identity Cloud 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 Identity Cloud 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 OIDC Provider settings
- Test the OIDC Authorization Code grant type flow

Lesson 3: 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 Identity Cloud
- Configure Identity Cloud for token exchange
- Test token exchange flows

Chapter 4: Federating Across Entities Using SAML2

Demonstrate federation across entities using SAML2 with ForgeRock® Identity Cloud (Identity Cloud).

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 Identity Cloud as an IdP and integrate with third-party SPs
- Examine SSO between SP and IdP and across SPs

Lesson 2: Delegating Authentication Using SAML2

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

- Explain the SSO flow from the SP point of view
- Describe the metadata content and use
- Configure Identity Cloud as a SAML2 SP and integrate with a third-party IdP