

PingOne Advanced Identity Cloud Identity Governance

OEM: Ping Identity • Code: IGA-400-BVP Rev A.1

COURSE DESCRIPTION

This course provides a hands-on technical introduction to PingOne Advanced Identity Cloud Identity Governance (Identity Governance). Further information and guidance can be found in the documentation and knowledge base. Note: This course is based on PingOne Advanced Identity Cloud (Advanced Identity Cloud) with the Identity Governance functionality added.

AUDIENCE PROFILE

- This section doesn't contain any content.

PREREQUISITES

- The following are the prerequisites for successfully completing this course:
- Completion of the Getting Started With PingOne Advanced Identity Cloud for Administrators course.
- Recommended completion of the PingOne Advanced Identity Cloud Administration course.
- Knowledge of basic Windows/PowerShell commands
- An understanding of HTTP and web applications
- A basic understanding of how directory servers function
- A basic understanding of REST
- A familiarity with the Advanced Identity Cloud admin and end-user UIs

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- Discover how to access, manage, and work with Identity Governance capabilities
- Create target applications and configure their mapping with Advanced Identity Cloud, reconcile entitlements from the applications, and provision accounts to the applications
- Create and manage workflows, access requests for resources (entitlements, applications, roles), forms for access requests, and governance glossary items
- Create and start scheduled and event-based certification campaigns to verify user access, and manage compliance by implementing Segregation of Duties (SoD) policies and rules

Module 1: Chapter 1: Introducing Identity Governance

- Discover how to access, manage, and work Identity Governance capabilities.

Lesson 1: Introducing Identity Governance

- Describe Identity Governance and the related capabilities available in Advanced Identity Cloud:
- Describe the purpose of Identity Governance
- Access Advanced Identity Cloud
- Describe the course environment and architecture
- Access your CloudShare environment
- Access your Advanced Identity Cloud tenant
- Access and explore your PingOne tenant environment

Lesson 2: Onboarding Applications and Identities

- Create applications for onboarding users:
- Explain Identity Governance terminology
- Describe application types
- Register and manage applications
- Connect an application with an identity source
- Configure application provisioning
- Onboard and provision users, roles, and entitlements
- Create a connector server in Advanced Identity Cloud
- Connect the RCS with Advanced Identity Cloud
- Customize the Advanced Identity Cloud user schema
- Register an authoritative application and onboard identities

Module 2: Chapter 2: Managing Identity Lifecycle and Entitlements

- Create target applications and configure their mapping with Advanced Identity Cloud, reconcile entitlements from the applications, and provision accounts to the applications.

Lesson 1: Reconciling Entitlements

- Load and manage entitlements from target applications in Advanced Identity Cloud:
- Describe entitlements
- Manage entitlements
- Assign and revoke entitlements to/from users and roles
- Request access for an entitlement
- Reconcile entitlements from Active Directory (AD)
- Reconcile entitlements from PingOne

Lesson 2: Synchronizing Identity Data

- Describe synchronization as a foundation of identity lifecycle management in Identity Governance, and provision and manage application accounts:
- Describe the need for synchronization
- Explore synchronization in Identity Governance

- Describe how changes are managed during synchronization
- Provision and manage application accounts
- Provision an account to AD
- Provision an account and entitlement to PingOne

Module 3: Chapter 3: Creating and Managing Workflows and Access Requests

- Create and manage workflows, access requests for resources (entitlements, applications, roles), forms for access requests, and governance glossary items.

Lesson 1: Managing Access Requests for Resources

- Create, review, and manage access requests for resources, such as applications, entitlements, and roles:
- Explain access request concepts
- Request access to resources
- Review and handle access requests
- Request to provision an AD account with entitlements
- Request to provision PingOne accounts with entitlements
- Define a conditional provisioning role
- Define and request a provisioning role

Lesson 2: Managing Glossary Items and Scopes

- Create and manage governance glossary items and scopes to manage what can be requested:
- Describe the governance glossary
- Define and populate glossary attribute values
- Use glossary attribute values as filters
- Request access to entities for others
- Create scopes to control what can be requested
- Define glossary items for use in workflows and scopes
- Create access requests for others and add scopes

Lesson 3: Creating Workflows, Request Types, and Forms

- Manage workflows, request types, and forms for customizing access requests, and schedule a task scanner job:
- Create and manage workflows
- Build a workflow with nodes
- Create and manage request types
- Create and manage forms for customized user-interaction
- Designing forms in the form editor
- Create and manage a task scanner
- Create new workflows and update default workflows
- Create and manage forms to customize user interaction

Module 4: Chapter 4: Managing Certifications and Compliance

- Create and start scheduled and event-based certification campaigns to verify user access, and manage compliance by implementing SoD policies and rules.

Lesson 1: Configuring and Running Certifications

- Prepare and perform certification of access to applications:
- Certify access in Identity Governance
- Create certification templates
- Configure the certification templateManage certification templates
- Create certification campaigns
- Perform access reviews
- Certify access based on events
- Configure and initiate entitlement certifications
- Certify entitlements for the certification campaign
- Configure an event that triggers certification
- Configure an event that initiates a workflow
- Manage approvals for triggered events

Lesson 2: Managing Compliance With SoD

- Manage compliance and implement SoD policies:
- Describe SoDDefine policy rules
- Configure compliance policies
- Run compliance scans
- Manage violations and exceptions
- Create an SoD rule and policy
- Run a compliance scan
- Make a request that violates compliance