NetIQ Access Manager Foundations (3-7230)

ID 3-7230   **Price** on request   **Duration** 4 days

Who should attend

All members of the project teams, including security, architects, project managers, developers, administrators, and operations personnel.

Prerequisites

To be successful in this course, you should have the following prerequisites or knowledge:

- A basic understanding of the concept of Access Management.
- An understanding of NetIQ eDirectory, NetIQ Identity Manager, and Linux.
- A familiarity with basic web services, HTTP Requests and Responses, HTML tags, and server-side dynamic content (JSP, ASP, or similar), and having familiarity with PHP, JavaScript, ECMAscript, or RESTful scripting is required.

Course Objectives

On completion of this course, participants should be able to:

- Identify the Access Manager solution.
- Describe the difference between appliance and component installations.
- Build and configure a Reverse Proxy.
- Configure SSL for a self-signed environment.
- Identify Risk Management.
- Create and utilize Classes, Methods, and Contracts, and how to use them in Policy and Proxies.
- Create and utilize role-based decision making

Course Content

Chapter 1: Configuring the Administration Console

- Describing Access Manager concepts.
- Describing Access Manager deployment options.
- Configuring the Administration Console.
- Additional Adjustments.
- Troubleshooting installation issues.

Chapter 2: Configuring Access Gateway Service

- Connecting the IDP to the IDM Server.
- Describing the NetIQ Access Manager clusters.
- Explaining Access Gateway configuration.
- Adding an advanced File Configurator.
- Adding Additional Administrators.

Chapter 3: Rewriting Web Code

- Rewriting Web Content.
- Validating Web Content.
- Configuring the Pin List and other options.

Chapter 4: Configuring Reverse Proxies

- Configuring Network Settings to support multiple websites.
- Explaining Proxy configuration.
- Explaining Web Proxy logging.
- Describing Proxy logic.
- Creating additional power users.

Chapter 5: Enable and Protect NAM Websites

- Explaining the SSL.
- Describing the SSL mechanics.
- Enabling SSL inside Proxies.
- Enabling and protecting NAM websites with SSL Certs.

Chapter 6: Authentication

- Explaining the Authentication Framework.
- Authenticating to a Site.
- Describing Classes, Methods, and Contracts.

Chapter 7: Configuring Domain and Multi-Homing

- Preparing for Multi-Homing.
- Configuring Multi-Homing.
- Explaining web server acceleration.
- Identifying the types of Proxy options.
- Configuring the Proxy.

Chapter 8. Mitigating Risk

- Introducing the Policy.
- Creating and managing a Risk Policy.

opentext™

- Explaining how Risk works?
- Detailing the Integration.

Chapter 9: Modifying the Portal Interface

- Customizing the Identity Server pages.
- Customizing the Identity Server messages.
- Customizing the Access Gateway error messages.
- Customizing the Access Gateway logout requests.

Chapter 10: Using Appmarks and Enabling Mobile

- Explaining the Web Access portal
- Configuring Mobile Access.

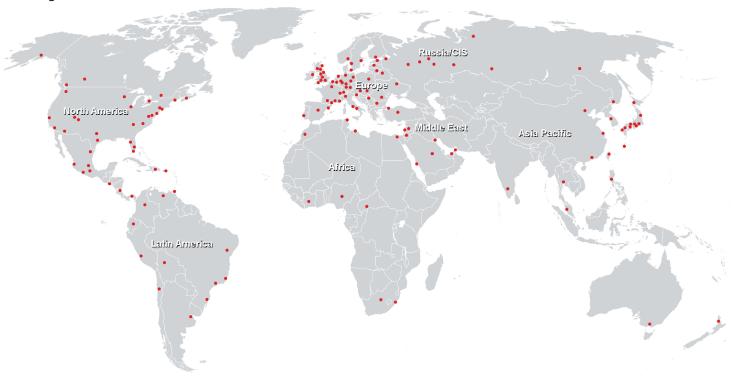**Chapter 11: Applications Configuration Using Roles**

- Reviewing Policy.
- Identifying the Access Manager roles.
- Explaining the Access Manager Authorization.
- Explaining how it works (Business Case).
- Using the Policy Troubleshooting tools.
- Troubleshooting steps.

Chapter 12: Advanced Applications Configuration

- Overview of Identity Injection.
- Explaining basic and custom Header Options.
- Using Form Fill Options.
- Using Form Fill Shared Secrets.

opentext™

Training Centres worldwide

Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch