Implement Adaptive Multi-Factor Authentication

okta Edu

Course overview

Strengthen authentication into your systems beyond passwords with Okta Adaptive Multi-Factor Authentication in Web Applications, Cloud Applications, and On-Premises Systems.

Learn how to integrate Okta MFA with AD FS, Cloud Applications such as Salesforce, RADIUS apps, and Windows RDP. You will also define MFA enrollment and enforcement in Okta using policies and rules, as well as control Adaptive MFA based on the user context and behaviors.

Using your own computer, you will access individual Okta tenants, virtual environments, and 3rd party applications to practice a full spectrum of setup and configuration tasks.

Who should attend

- System Administrators
- Security Administrators
- IT Architects

Prerequisites

- Familiarity with Authentication
- Familiarity with Active Directory
- Familiarity with Active Directory Federation Services (optional)
- Okta Basics (highly recommended)

Format

- Instructor-led with hands-on labs
- Duration: 1 day
- Delivered through public class schedule or as a private onsite event

Setup requirements

- Students use their own computers and mobile device (Android or iOS)
- Okta provides access to an Okta org, software credentials, and virtual machines to complete hands-on lab activity

Learn how to:

- Describe Okta Identity Cloud and the Okta Adaptive Multi-Factor Authentication Suite.
- Review basic administrative tasks, such as onboard users from AD, create admin accounts, manage users and grous, and monitor system logs.
- Identify Okta Adaptive MFA capabilities and integration scenarios.
- Decide what are the best factors and security policies for distinct business scenarios.
- Configure policies for MFA enrollment and MFA enforcement.
- Implement MFA for accessing cloud and on-premises Applications.
- Integrate Okta MFA with AD FS.
- Integrate Okta MFA with cloud applications such as Salesforce.
- Implement MFA on RADIUS and RDP connections.
- Implement adaptive MFA based on user context.
- Implement adaptive MFA based on the user behavior.

Implement Adaptive Multi-Factor Authentication

okta Edu

Course outline

1: Introduction

Describe Okta Identity Cloud
Describe Okta Adaptive Multi-Factor Authentication
Describe Okta Adaptive MFA capabilities and integration scenarios
Perform Basic Okta Administrative Tasks

2: Implement MFA in Web Applications

Describe MFA, factors, and policies
Compare and select MFA factors
Configure MFA Enrollment and Enforcement
Compare MFA using AD FS and using Okta native capabilities
Integrate Okta with AD FS
Integrate Okta with a Cloud App (Pinterest)
Configure MFA Enforcement when accessing Okta and Cloud Apps

Bonus: Introduction to Device Trust

Describe what's Device Trust
Describe Contextual MFA based on Device Trust

3: Implement MFA in On-Premise Apps

Describe how applications can consume Okta MFA
Compare the SSO, RADIUS, RDP, and Okta API integrations
Describe the SSO, RADIUS, RDP, and Okta API authentication flow and configuration milestones
Configure MFA Enforcement in RADIUS
Configure MFA Enforcement in RDP

4: Implement Adaptive MFA

Describe how Okta MFA implements contextual and behavioral filters
Compare filters
Describe what are Gateways and external IPs
Describe how the Geo Location is determined
Implement Contextual MFA based on IP Zones and Geo Location
Implement Behavioral MFA based on Geo Location and Device.