CA EDUCATION COURSE DESCRIPTION

# CA Advanced Authentication r8.1 Differences 200

## Course Overview

CA Advanced Authentication is a flexible and scalable solution that incorporates both risk-based authentication methods like device identification, geolocation and user activity, as well as a wide variety of multi-factor, strong authentication credentials. This solution can allow the organization to create the appropriate authentication process for each application or transaction.

This release includes a significant focus on implementing CA Advanced Authentication in mobile device applications including mobile Device DNA™, SDK, and an iOS sample application.

This course covers the new features available with release 8.1, including use case, feature description, and steps necessary to implement the new features.

Several of the new features (SDKs and APIs) aid application developers in incorporating CA Advanced Authentication into their mobile and desktop applications. For those features, an overview of the feature is included. This course does not provide developer level instruction.

### PRODUCT RELEASE

CA Advanced Authentication r8.1

### COURSE TYPE, LENGTH & CODE

- Web Based Training (WBT)
- 60 Minutes
- 04AAA20140

### PREREQUISITES

- General knowledge of Advanced Authentication functionality

### WHO SHOULD ATTEND

- CA Advanced Authentication Administrator
- IT Architect
- Partner (services delivery and presales)
- Technical support analyst
- Security specialists

## What You Will Learn

- Describe CA Advanced Authentication features for use in mobile devices
- Describe Risk & Strong Authentication enhancements
- Use administrative manageability improvements
- Upgrade from release 8.0
- Describe platform support and certification changes

## For Managers

CA Advanced Authentication is a key component in your security infrastructure. In order to maintain your security infrastructure at the highest levels, your security professionals must take advantage of the latest technologies available. Understanding and implement the latest features enables and protects your business while providing the greatest ROI and customer satisfaction.

**RECOMMENDED NEXT COURSES**

- N/A

# Course Agenda

| 1) Use Mobile Device Features | 2) Implement Risk Authentication New Features |
|---|---|
| ▪ Use mobile device DNA matching<br>▪ Use the mobile device DNA SDK and iOS sample application<br>▪ Use the mobile channel for risk evaluation | ▪ Configure risk advice thresholds<br>▪ Use risk REST APIs<br>▪ Use the Mobility Index model element<br>▪ Enable the Model Score (UBP)<br>▪ Create custom rule types |
| **3) Implement Strong Authentication New Features** | **4) Use Simplification and Manageability Enhancements** |
| ▪ Use client SDKs to extend CA Advanced Authentication<br>▪ Describe the CA AuthID Crypto SDK<br>▪ Describe the CA Mobile OTP Crypto SDK | ▪ Integrate CA AMDS with Adapter<br>▪ Manage database log data<br>▪ Describe sequence number improvements |
| **5) Upgrade from Release 8.0** | **6) Describe Platform Support and Certivication Changes** |
| ▪ Describe the upgrade process<br>▪ Use Python scripts to upgrade the database from release 8.0 | ▪ Changes to platforms supported<br>▪ Certification changes |

Visit **www.ca.com/education** to explore the many course offerings, training options, and education solutions available to meet your skill development needs, budget, and travel requirements.