CA EDUCATION COURSE DESCRIPTION

CA Advanced Authentication r8.0: Foundations 200

PRODUCT RELEASE

CA Advanced Authentication r8.0 and greater

COURSE TYPE, LENGTH & CODE

- Instructor Led Training (ILT) One (1) day
- Course Code: 04AAA20111

PREREQUISITES

- CA Advanced Authentication: basic understanding of the purpose and function of the product including the various authentication credentials and risk analysis Advanced Authentication provides.

  General: Windows server knowledge, basic user directory understanding (Active Directory preferred), application server (Apache Tomcat preferred) functionality, MS SQL Server

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.

In this course, you will be taught how to perform a typical complete installation, perform general administrative tasks like creating organizations and administrators, and use out-of-the-box authentication and risk configurations.

The dynamic lab environment enables hands-on practice using multiple credential types to create authentication configurations. You will create a Risk Authentication ruleset and apply it to an organization. You will test utilizing the included Adapter and SAML sample application, allowing you to experience the end-user authentication and enrollment process flows based on your configurations.

What You Will Learn

- Implement and administer the server components
- Configure authentication and risk assessment processes
- Use the SAML sample application and Adapter for testing
- Utilize reporting capabilities

For Managers

Organizations need to protect their users with a strong, cost-effective method of authentication and risk evaluation, especially when it involves confidential, proprietary, or regulated data. The user-convenient, easily insertable authentication of CA Advanced Authentication enables you to protect your customers, partners, and employees from identity theft and fraud.

Your team members will be taught the tasks necessary to install CA Advanced Authentication, customize credentials, create risk evaluation rulesets, and manage users and organizations.

WHO SHOULD ATTEND

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

RECOMMENDED NEXT COURSES

- Refer to learn.ca.com for additional courses in the CA Advanced Authentication learning path.

Course Agenda

Module 1: Implement CA Advanced Authentication

- Prepare the server for installation
- Install CA Advanced Authentication server components
- Run database scripts
- Prepare the application server and deploy java applications
- Verify the installation
- Create an organization
- Create an administrator
- Create an authentication flow with Adapter and test with SAML sample application

Module 2: Perform General Administration

- Use Advanced Authentication (administration console)
- Organize configurations
- Manage server instances
- Adjust server logging
- Locate reports

Module 3: Administer Strong Authentication

- Manage authentication methods
- Create issuance profiles
- Create authentication policies
- Assign credential defaults
- Use global defaults in the organization
- Manage user credentials
- Use authentication reports
- Locate and review log files

Module 4: Administer Risk Authentication

- Describe the Risk Authentication workflow
- Describe rule categories and rule sets
- Use OOTB rules
- Create custom rules
- Describe risk score and advice
- Use risk reports
- Locate and review log files

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.