Entrust Identity as a Service (IDaaS) In Depth

Course Description

ENTRUST

About this course

Identity as a Service in depth is a two-day, instructor-led, hands-on deeper look at Entrust Identity as a Service (IDaaS) our authentication management tool in the cloud.
The course begins where IDaaS Kickstart ended with a discussion of the security requirement of authentication, and you will now define how users authenticate with applications. Using an example organization, you will learn how to define a user base, using bulk load and import from other directory sources.
Next, you will define and assign authenticators for users. Finally, applications will be identified, and resource rules will be used to apply risk-based authentication.

Course Objectives

Upon completion of this course, participants will be able to:

- Demonstrate how to define and organize users in their IDaaS environment including via bulk load and import from external sources
- Demonstrate how to define authenticators, how they are assigned to users and how properties are defined.
- Demonstrate how to define resources and resource rules to manage user risk-based authentication

Prerequisites

IDaaS Kickstart is recommended. It is also recommended students sign up for the IDaaS trial.

Who should attend this course

This course is intended for technology professionals who would like to have a deeper look at the capabilities of IDaaS including:

- Administrators
- Customized administrative users
- Auditors
- Technical Support or Help Desk staff

This course is ideal for Administrators who will be responsible for managing the IDaaS service on behalf of their organization.

Course Lessons

The Identity as a Service in-depth course includes the following lessons.

LESSON 1

Identity Management with IDaaS

This lesson is a review of the concepts from the Kickstart course that are important for this session.

LESSON 2

Defining our User Population

This lesson demonstrates how to add users in bulk, how user grouping works and how to import users from external sources such as LDAP directory.

LESSON 3

Defining Authenticators

This lesson will walk through each authenticator and its policy considerations and configuration. We will learn how authenticators are assigned to users.

LESSON 4

In depth Management of IDaaS

The lesson takes much deeper look at the IDaaS Management interface from a super user administration perspective.

LESSON 5

Resources

This lesson will show how resources are set up with resource rules. How to set up risk based authentication and define risk factors.

LESSON 6

A deeper look at Smart Credentials

What is a Smart Credential, and why does it require a PKI. We will define a PKI in our IDaaS environment and show how we can issue SM to a phone app.

LESSON 7

Gateways

Why do we need a Gateway, and how is it installed on site.

LESSON 8

Putting it all together

In our labs we implement 3 use cases for access to applications for user populations using specific authenticators