Entrust Identity Enterprise Comprehensive

Course Description

ENTRUST

About this course

Entrust Identity Enterprise Comprehensive is a five-day, instructor-led, hands-on overview of Entrust Identity Enterprise.

You will plan, install, and configure Entrust Identity Enterprise and some of its optional components on Windows Server.

- The course begins with a discussion of the security requirement of authentication, and you will review different authentication methods that are available.
- Entrust Identity Enterprise is introduced as a solution for authenticating the identity of users.
- A review of the architecture and components of the Entrust Identity Enterprise environment will precede an installation of the server components.
- You will perform administrative operations using both Entrust Identity Enterprise Master User Shell and Entrust Identity Enterprise Administration Interface and set system configuration using Entrust Identity Enterprise Properties Editor.
- As part of the course, you will configure authentication using grids, hardware tokens, software tokens, machine information, one-time passwords, external information and smart credentials.
- You will also enable email delivery of authentication information, including one-time passwords, eGrid and QR codes using a classroom mail server. Participants will customize policies, groups, and roles to tailor the environment to an organization's security requirements.
- Participants will also learn how to personalize the authentication experience based on conditions such as the geographical location of the user login request through the concept of adaptive authentication.
- Additional repositories will be configured to allow users accounts to be distributed across multiple databases and LDP Directories.
- Entrust Identity Enterprise logs and reports will be examined to allow administrators to track operations within the system.
- Authenticating accounts using mobile devices will be examined, including configuring the mobile enrollment of digital IDs for smartphones and tablets. This section also describes how a managed Certification Authority, defined in Entrust Identity Enterprise, creates trusted digital IDs.
- The Entrust Identity Enterprise Radius Proxy is introduced as a mechanism to incorporate second-factor authentication challenges into a VPN login.
- The course closes with an examination of SSL security in Entrust Identity Enterprise and disaster recovery through backup and restore operations.
- In addition to exercises using Entrust Identity Enterprise server, course participants will also install and configure the Entrust Identity Enterprise Self-Service Module.
- Hands-on exercises at the end of each lesson provide participants with the opportunity to apply the knowledge gained through the lecture segment of the lesson.

Lab Exercises

Students will be provided with an AWS lab accessed via RDP for the training duration. Use of the lab will require access to an RDP application and the inclusion of a public IP address in our firewall. The instructor will work with all students to arrange for access to the labs on the first day of class.

Lab assignments are provided at the end of each day of lecture and are to be done prior to the next day's lecture.

Course Objectives

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

- Demonstrate the value of authentication, and describe the authentication methods enabled through Entrust Identity Enterprise
- Describe the basic architecture of an Entrust Identity Enterprise system, including the function of the various applications, interfaces and processes
- Install Entrust Identity Enterprise, Entrust Identity Enterprise Self-Service Module, Entrust and Entrust Identity Enterprise Enrollment Module v13 on Windows Server
- Perform typical administrative tasks using Entrust Identity Enterprise Master User Shell, Entrust Identity Enterprise Administration, and bulk operations
- Modify the system configuration using Entrust Identity Enterprise Properties Editor
- Create and manage Entrust Identity Enterprise accounts, including administrative and end user accounts
- Configure a variety of authentication methods as well as the policies controlling the behavior of these methods
- Customize groups and roles
- Configure the email delivery of authentication details including one-time passwords, QR codes and eGrid
- Define multiple repositories for storing account information
- Configure a managed Certification Authority to create digital IDs
- Access and interpret logging information
- Configure the self-service portal for account registration and self-administration
- Recover from disaster scenarios related to the loss of configuration data
- Configure and assign PIV credentials using Entrust PKI as the CA

Prerequisites

While prior knowledge of the concept’s surrounding authentication is helpful, participants do not require any previous experience with Entrust products.

Previous experience with the Windows operating system is required as the hands-on exercises are completed on computers running Windows Serve

Who should attend this course

This five-day hands-on course is intended for technology professionals who will be responsible for planning, implementing, configuring, managing, and supporting Entrust Identity Enterprise.

Course Lessons

The Identity Enterprise Comprehensive course includes the following lessons.

LESSON 1 Authentication

This lesson introduces the concept of authentication and explores some of the different methods for authenticating the participants in a transaction.

LESSON 2 *Entrust Identity Enterprise Components*

This lesson provides an overview of the Entrust Identity Enterprise components and interfaces.

LESSON 3 Installing Entrust Identity Enterprise

This lesson describes the planning and installation tasks that must be completed when implementing Entrust Identity Enterprise.

LESSON 4 Entrust Identity Enterprise Properties Editor

This lesson introduces the Entrust Identity Enterprise Properties Editor as the preferred method for making changes to the Entrust Identity Enterprise system settings.

LESSON 5 *Entrust Identity Enterprise Master User Shell*

This lesson introduces the Entrust Identity Enterprise Master User Shell and the responsibilities of Master Users.

LESSON 6 Managing accounts

This lesson examines some of the account management operations performed in Entrust Identity Enterprise Administration.

LESSON 7 Authenticating using passwords

This lesson introduces the use of passwords for account authentication in Entrust Identity Enterprise.

LESSON 8 Authenticating using grids

This lesson introduces the use of physical grid cards and egrids for account authentication in Entrust Identity Enterprise.

LESSON 9 Authenticating using tokens

This lesson introduces hardware and software tokens for account authentication in Entrust Identity Enterprise.

LESSON 10 Authenticating using machine information

This lesson introduces machine information for account authentication in Entrust Identity Enterprise.

LESSON 11 Authenticating using one-time passwords

This lesson introduces one-time passwords for account authentication in Entrust Identity Enterprise.

LESSON 12 Authenticating using other methods

This lesson introduces some of the other methods available for account authentication in Entrust Identity Enterprise.

LESSON 13 Authenticating using mobile devices

This lesson introduces some of the authentication methods enabled using mobile devices including smartphones or tablets.

LESSON 14 Policies, groups, and roles

This lesson describes the purpose and relationship between policies, groups, and roles.

LESSON 15 Adding additional repositories

This lesson describes how additional repositories can be added to Entrust Identity Enterprise, allowing accounts to be spread across multiple databases and Directories.

LESSON 16 Authenticating using external information

This lesson describes how information is stored in an LDAP Directory or Windows domain controller can be used for account authentication in Entrust Identity Enterprise.

LESSON 17 Adaptive authentication

This lesson describes how the adaptive authentication process be used to customize the user authentication experience based on specific conditions, such as user location.

LESSON 18 Entrust Identity Enterprise logging

This lesson introduces the logging functionality in Entrust Identity Enterprise.

LESSON 19 Entrust Identity Enterprise reports

This lesson describes how reports are generated from information gathered from Entrust Identity Enterprise.

LESSON 20 Entrust Identity Enterprise Self-Service Module

This lesson introduces the Entrust Identity Enterprise Self-Service Module as a mechanism for allowing users to self-register and self-administer their accounts.

LESSON 21 Mobile enrollment

This lesson introduces mobile device enrollment to deliver digital IDs to a smartphone, tablets and other mobile devices.

LESSON 22 Authenticating using smart credentials

This lesson introduces smart credentials for account authentication in Entrust Identity Enterprise.

LESSON 23 Entrust Identity Enterprise Radius Proxy

This lesson introduces the Entrust Identity Enterprise Radius Proxy to enable authentication for VPN

LESSON 24 SSL security in Entrust Identity Enterprise

This lesson will examine how Secure Socket Layer (SSL) security is used to secure communications between Entrust Identity Enterprise and connecting applications.

LESSON 25 Recovering from data loss

This lesson provides an overview of the configuration backup and restore mechanism in Entrust Identity Enterprise.