Entrust Datacard™

Entrust IdentityGuard Comprehensive

Course Description

Entrust IdentityGuard Comprehensive

Entrust IdentityGuard Comprehensive is a five-day, instructor-led, hands-on overview of Entrust IdentityGuard. Course participants will plan, install and configure Entrust IdentityGuard and some of its optional components on Windows Server 2012 R2.

The course begins with a discussion of the security requirement of authentication and participants will review different authentication methods that are available. Entrust IdentityGuard is introduced as a solution for authenticating the identity of users. A review of the architecture and components of the Entrust IdentityGuard environment will precede an installation of the server components. Course participants will perform administrative operations using both the Entrust IdentityGuard Master User Shell and Entrust IdentityGuard Administration, as well as system configuration operations using Entrust IdentityGuard Properties Editor.

As part of the course, participants will configure authentication using grids, hardware tokens, software tokens, machine information, one-time passwords, external information and smart credentials. Participants will also enable email delivery of authentication information, including one-time passwords, egrids 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 IdentityGuard 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 IdentityGuard, creates trusted digital IDs. The Entrust IdentityGuard 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 IdentityGuard and disaster recovery through backup and restore operations.

In addition to exercises using Entrust IdentityGuard server, course participants will also install and configure the Entrust IdentityGuard Self-Service Module, Federation Module and Enrollment Module.

Hands-on exercises at the end of each lesson provides participants with the opportunity to apply the knowledge gained through the lecture segment of the lesson.

Course Objectives

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

- Demonstrate the value of authentication, and describe the authentication methods enabled through Entrust IdentityGuard
- Describe the basic architecture of an Entrust IdentityGuard system, including the function of the various applications, interfaces and processes
- Install Entrust IdentityGuard v12, Entrust IdentityGuard Self-Service Module v12, Entrust IdentityGuard Federation Module v10.2 and Entrust IdentityGuard Enrollment Module v10.1 on Windows Server 2012 R2
- Perform typical administrative tasks using Entrust IdentityGuard Master User Shell, Entrust IdentityGuard Administration, and bulk operations
- Modify the system configuration using Entrust IdentityGuard Properties Editor
- Create and manage Entrust IdentityGuard 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 egrids
- Define multiple repositories for storing account information
- Configure a managed Certification Authority to create of digital IDs
- Access and interpret logging information
- Configure the self-service portal for account registration and self administration
- Establish a SAML federation using Entrust IdentityGuard as the Identity Provider
- Recover from disaster scenarios related to the loss of configuration data

Prerequisites

While prior knowledge of the concepts 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 Server 2012 R2.

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 IdentityGuard.

Course Topics

Entrust IdentityGuard Comprehensive 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 IdentityGuard Components

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

LESSON 3

Installing Entrust IdentityGuard

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

LESSON 4

Entrust IdentityGuard Properties Editor

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

LESSON 5

Entrust IdentityGuard Master User Shell

This lesson introduces the Entrust IdentityGuard 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 IdentityGuard Administration.

LESSON 7

Policies, groups and roles

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

LESSON 8

Authenticating using passwords

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

LESSON 9

Authenticating using grids

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

LESSON 10

Authenticating using tokens

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

LESSON 11

Authenticating using machine information

This lesson introduces machine information for account authentication in Entrust IdentityGuard.

LESSON 12

Authenticating using other methods

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

LESSON 13

Authenticating using one-time passwords

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

LESSON 14

Adding additional repositories

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

LESSON 15

Authenticating using external information

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

LESSON 16

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 17

Entrust IdentityGuard logging

This lesson introduces the logging functionality in Entrust IdentityGuard.

LESSON 18

Entrust IdentityGuard reports

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

LESSON 19

Entrust IdentityGuard Self-Service Module

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

LESSON 20

Mobile enrollment

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

LESSON 21

Authenticating using smart credentials

This lesson introduces smart credentials for account authentication in Entrust IdentityGuard.

LESSON 22

Entrust IdentityGuard Radius Proxy

This lesson introduces the Entrust IdentityGuard Radius Proxy to enable authentication for VPN connections.

LESSON 23

Entrust IdentityGuard Federation Module

This lesson introduces the Entrust IdentityGuard Federation Module for enabling single sign-on authentication for enterprise and cloud applications.

LESSON 24

SSL security in Entrust IdentityGuard

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

LESSON 25

Recovering from data loss

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