ProTech *"Charting the Course ...*

protechtraining.com

... to Your Success!"

Symantec Encryption Management Server 3.3 and Desktop 10.3: Install, Configure, and Deploy

Course Summary

Description

The Symantec Encryption Management Server 3.3 and Desktop 10.3 Install, Configure, and Deploy course is designed to provide you with the fundamental knowledge and hands-on lab experience to install and administer the Symantec Encryption Management Server 3.3 and desktop client product. The hands-on labs include exercises for installation and configuration of the Symantec Encryption Management Server and Symantec Encryption Desktop products, including policy-based messaging security, manual and directory-style user and group management, and Symantec Encryption Desktop policy and usage, including for the Symantec Encryption Whole Disk Encryption product.

Additionally, you are introduced to the following Symantec Encryption products: Key Management Services, Symantec Encryption Mobile, Symantec Encryption iOS Viewer and Endpoint Device Control.

Objectives

After taking this course, students will be able to:

- Describe the features, concepts, components, and terminology of both the Symantec Encryption Management Server 3.3 and Symantec Encryption Desktop 10.3 products.
- Install Symantec Encryption Management Server 3.3 and complete setup using the most commonly configured options.
- Install a managed and customized Symantec Encryption Desktop 10.3 client.
- Configure, complete administration tasks for, and use Symantec Encryption Whole Disk Encryption and other Symantec Encryption Desktop features.
- Configure policy-based messaging security for internal and external recipients.
- Create and modify users, user policies, and groups using either manual or directory integration methods.
- Combine two or more Symantec Encryption Management Server into a cluster.

Topics

- Cryptography Essentials
- Symantec Encryption Product Introduction
- Installing Symantec Encryption Management Server
- Consumers and Groups
- Administrative Keys
- Server Messaging
- Monitoring and Reporting
- Mail Policy
- Key Not Found
- Web Email Protection
- Preparing SEMS for Encryption Desktop Clients
- Keys
- Configuring Client Enrollment
- Installing Symantec Encryption Desktop
- Create General Policy Settings
- Symantec Encryption Desktop Messaging
- Configuring Symantec Encryption Whole Disk Encryption
- Symantec Encryption Whole Disk Encryption Management nand Recovery
- Configuring Symantec Encryption NetShare
- Other Symantec Encryption Desktop Features
- Clustering

Symantec Encryption Management Server 3.3 and Desktop 10.3: Install, Configure, and Deploy

Course Summary (cont'd)

Audience

This course is intended for those responsible for the installation, configuration and maintenance of Symantec Encryption Management Server or Symantec Encryption Desktop.

Prerequisites

An understanding of information security concepts and terminology helps you succeed in this course. Also, this course requires familiarity with networking and computing concepts. Symantec recommends that students taking this course have at least one year of information technology experience.

Duration

Three days

Symantec Encryption Management Server 3.3 and Desktop 10.3: Install, Configure, and Deploy

Course Outline

I. Cryptography Essentials
- A. Cryptography defined
- B. Caesar cipher
- C. Symmetric-Key cryptography
- D. Public-Key cryptography
- E. Symantec Public-Key cryptography
- F. Digital signatures
- G. Trust Models
- H. Keys and key signatures
- I. Passphrases
- J. Certificates

II. Symantec Encryption Product Introduction
- A. Symantec Encryption Security products
- B. Symantec Encryption Management Server
- C. Symantec Encryption Desktop
- D. Symantec Encryption Command Line
- E. Symantec Encryption Mobile
- F. Symantec Encryption iOS Viewer

III. Installing Symantec Encryption Management Server
- A. Symantec Encryption Management Server installation steps
- B. System requirements
- C. Installing Symantec Encryption Management Server
- D. Configuring the Symantec Encryption Management Server
- E. Installing updates and upgrading the Encryption Server

Lab: Post installation tasks

IV. Consumers and Groups
- A. Introducing consumers, users and devices
- B. Introducing groups and policy

Lab: Creating groups and users

V. Administrative Keys
- A. The Organization Key
- B. Additional Decryption Key (ADK)
- C. SSL/TLS and X.509 Certificates
- D. Ignition key

Lab: Manage administrative keys

VI. Server Messaging
- A. Learn mode
- B. Mail proxies
- C. Server placement
- D. Mail flow

VII. Monitoring and Reporting
- A. Server monitoring and logging
- B. Protecting your Symantec Encryption Management Server

Lab: Create a backup and review logs and daily status email

VIII. Mail Policy
- A. Definition of policy chains and rules
- B. Rule conditions, actions, and key searches
- C. Default policy chains
- D. Adding custom chains to mail flow
- E. Custom chains and rules

Lab: Manage mail flow and work with mail policies

IX. Key Not Found
- A. External users
- B. Key Not Found and direct actions

X. Web Email Protection
- A. Introducing Web Messenger
- B. Configuring Web Messenger
- C. PDF Email Protection
- D. Out of Mail Stream
- E. X.509 Delivery
- F. External delivery options

Lab: Configure and work with Web Email protection

XI. Preparing SEMS for Encryption Desktop Clients
- A. What is directory synchronization
- B. How to use directory synchronization

Symantec Encryption Management Server 3.3 and Desktop 10.3: Install, Configure, and Deploy

Course Outline (cont'd)

XII. Keys
- A. Managed key configuration
- B. Key usage and tokens

XIII. Configuring Client Enrollment
- A. Definition of enrollment
- B. Methods of client enrollment

Lab: Configuring client enrollment

XIV. Installing Symantec Encryption Desktop
- A. System requirements
- B. Symantec Encryption Desktop installer
- C. Licensing Symantec Encryption Desktop
- D. Modifying the Symantec Encryption Desktop

Lab: Download and install Symantec Encryption Desktop

XV. Create General Policy Settings
- A. General Symantec Encryption Desktop options in Consumer Policy
- B. Updating policy settings

XVI. Symantec Encryption Desktop Messaging
- A. How Symantec Encryption Desktop affects messaging infrastructure
- B. MAPI buttons

XVII. Configuring Symantec Encryption Whole Disk Encryption
- A. What is Whole Disk Encryption
- B. Configuring Whole Disk Encryption
- C. Symantec Encryption Whole Disk Encryption for Mac OS X
- D. Symantec Encryption Whole Disk Encryption for Linux

Lab: Configure Whole Disk Encryption

XVIII. Symantec Encryption Whole Disk Encryption Management and Recovery
- A. Logon failure and reporting
- B. The WDE-ADMIN group
- C. The pgpwde command-line tool
- D. Recovery options
- E. Remote Disable and Destroy
- F. Configuring Remote Disable and Destroy

Lab: Recover hard drive manually

XIX. Configuring Symantec Encryption NetShare
- A. Encrypted folder creation
- B. How to configure Symantec Encryption Netshare
- C. Symantec Encryption NetShare Group Key
- D. Active Directory Group integration
- E. Miscellaneous information about Symantec Encryption NetShare

Lab: Configure Symantec Encryption Netshare

XX. Other Symantec Encryption Desktop Features
- A. Symantec Encryption Zip file and folder protection
- B. Symantec Encryption Shredder
- C. Shred Free Space
- D. Symantec Encryption Virtual Disk
- E. Symantec Encryption Portable

Lab: Create and use a virtual disk. Use Symantec Encryption Zip and Symantec Encryption Shredder

XXI. Clustering
- A. How Symantec Encryption Management Server Clustering works
- B. Using the DMZ Clustering Zone
- C. Cluster failover
- D. Web Messenger inbox replication

Lab: Configure a cluster