

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

COURSE 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.

Delivery Method

Instructor-led

Duration

Three days

Course Objectives

This course provides instruction on Symantec Encryption Management Server 3.3 and Symantec Encryption Desktop 10.3. At the completion of the course, you 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.

Who Should Attend

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.

Hands-On

This course includes practical exercises that enable you to test your new skills and begin to transfer them into your working environment, as well as several review exercises to help you remember what you have learned.

INSTALL, CONFIGURE, AND DEPLOY COURSE OUTLINE

Cryptography Essentials

- Cryptography defined
- Caesar cipher
- Symmetric-Key cryptography
- Public-Key cryptography
- Symantec Public-Key cryptography
- Digital signatures
- Trust Models
- Keys and key signatures
- Passphrases
- Certificates

Symantec Encryption Product Introduction

- Symantec Encryption Security products
- Symantec Encryption Management Server
- Symantec Encryption Desktop
- Symantec Encryption Command Line
- Symantec Encryption Mobile
- Symantec Encryption iOS Viewer

Installing Symantec Encryption Management Server

- Symantec Encryption Management Server installation steps
- System requirements
- Installing Symantec Encryption Management Server
- Configuring the Symantec Encryption Management Server
- Installing updates and upgrading the Encryption Server

Lab: Post installation tasks

Consumers and Groups

- Introducing consumers, users and devices
- Introducing groups and policy



Lab: Creating groups and users

Administrative Keys

- The Organization Key
- Additional Decryption Key (ADK)
- SSL/TLS and X.509 Certificates
- Ignition key

Lab: Manage administrative keys

Server Messaging

- Learn mode
- Mail proxies
- Server placement
- Mail flow

Monitoring and Reporting

- Server monitoring and logging
- Protecting your Symantec Encryption Management Server

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

Mail Policy

- Definition of policy chains and rules
- Rule conditions, actions, and key searches
- Default policy chains
- Adding custom chains to mail flow
- Custom chains and rules

Lab: Manage mail flow and work with mail policies

Key Not Found

- External users
- Key Not Found and direct actions

Web Email Protection

- Introducing Web Messenger
 - Configuring Web Messenger
 - PDF Email Protection
 - Out of Mail Stream
 - X.509 Delivery
 - External delivery options
- Lab: Configure and work with Web Email protection

Preparing SEMS for Encryption Desktop Clients

- What is directory synchronization
- How to use directory synchronization

Keys

- Managed key configuration
- Key usage and tokens

Configuring Client Enrollment

- Definition of enrollment
 - Methods of client enrollment
- Lab: Configuring client enrollment

Installing Symantec Encryption Desktop

- System requirements

- Symantec Encryption Desktop installer
- Licensing Symantec Encryption Desktop
- Modifying the Symantec Encryption Desktop

Lab: Download and install Symantec Encryption Desktop

Create General Policy Settings

- General Symantec Encryption Desktop options in Consumer Policy
- Updating policy settings

Symantec Encryption Desktop Messaging

- How Symantec Encryption Desktop affects messaging infrastructure
- MAPI buttons

Configuring Symantec Encryption Whole Disk Encryption

- What is Whole Disk Encryption
- Configuring Whole Disk Encryption
- Symantec Encryption Whole Disk Encryption for Mac OS X
- Symantec Encryption Whole Disk Encryption for Linux

Lab: Configure Whole Disk Encryption

Symantec Encryption Whole Disk Encryption Management and Recovery

- Logon failure and reporting
- The WDE-ADMIN group
- The `pgpude` command-line tool
- Recovery options
- Remote Disable and Destroy
- Configuring Remote Disable and Destroy

Lab: Recover hard drive manually

Configuring Symantec Encryption NetShare

- Encrypted folder creation
- How to configure Symantec Encryption Netshare
- Symantec Encryption NetShare Group Key
- Active Directory Group integration
- Miscellaneous information about Symantec Encryption NetShare

Lab: Configure Symantec Encryption Netshare

Other Symantec Encryption Desktop Features

- Symantec Encryption Zip file and folder protection
- Symantec Encryption Shredder
- Shred Free Space
- Symantec Encryption Virtual Disk
- Symantec Encryption Portable

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

Clustering

- How Symantec Encryption Management Server Clustering works
 - Using the DMZ Clustering Zone
 - Cluster failover
 - Web Messenger inbox replication
- Lab: Configure a cluster