

Symantec Endpoint Protection 11.0 MR4: Administration

COURSE DESCRIPTION

The *Symantec Endpoint Protection 11.0 MR4: Administration* course is designed for the network, IT security, and systems administration professional tasked with architecting, implementing, and monitoring antivirus and antispyware, as well as client firewall solutions. This class covers how to design, deploy, install, configure, and monitor Symantec Endpoint Protection.

Students also learn how to create and implement client firewall, intrusion prevention, and behavioral protection policies that guard the enterprise from viruses, hackers, and spam. In addition, students learn how to troubleshoot Symantec Endpoint Protection managers and clients.

Delivery Method

Instructor-led

Duration

Five days

Course Objectives

By the completion of this course, you will be able to:

- Describe Symantec Endpoint Protection products, components, product dependencies, and the system hierarchy.
- Install and configure Symantec Endpoint Protection management and client components.
- Deploy Symantec Endpoint Protection clients.
- Manage the client UI.
- Manage antivirus and antispyware policies.
- Configure TruScan Proactive Threat Scans.
- Design a Symantec Endpoint Protection environment.
- Monitor and maintain the Symantec Endpoint Protection environment.
- Configure firewall and intrusion prevention policies.
- Customize network threat protection.

Who Should Attend

This course is for network managers, resellers, systems administrators, client security administrators, systems professionals, and consultants who are charged with the installation, configuration, and day-to-day management of Symantec Endpoint Protection in a variety of network environments, and who are responsible for troubleshooting and tuning the performance of this product in the enterprise environment.

Prerequisites

You must have working knowledge of advanced computer terminology, including TCP/IP networking terms and Internet terms, and an administrator-level knowledge of Microsoft Windows 2000/XP/2003 operating systems.

Hands-On

This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

COURSE OUTLINE

Introduction

- Course Overview
- The Classroom Lab Environment

Symantec Endpoint Protection Product Solution

- Why Use Symantec Endpoint Protection?
- Symantec Endpoint Protection Components
- Symantec Endpoint Protection Policies and Concepts
- Key Design Factors

Installing Symantec Endpoint Protection

- Identifying Hardware and Software Requirements
- Preparing Servers and Clients
- Installing the Symantec Endpoint Protection Manager

Managing Symantec Endpoint Protection

- Identifying Important SEPM Elements
- Starting and Navigating the Symantec Endpoint Protection Manager
- Describing Policy Types and Components
- Describing SEPM and Console Communications

Deploying Clients

- Preparing for Client Deployment
- Choosing the Client Installation Method
- Installing Managed Clients
- Making Unmanaged Clients Managed
- Configuring Unmanaged Detector
- Scanning Clients
- Managing the User Environment
- Managing Groups, Policies, and Locations

Configuring LiveUpdate Policies

- Configuring LiveUpdate
- Configuring LiveUpdate for Clients
- Manually Updating Virus Definitions

Configuring Antivirus and Antispyware Protection

- Introducing Antivirus and Antispyware Policies
- Configuring Auto-Protect Scans
- Configuring TruScan Proactive Threat Scans
- Configuring Administrator-defined Scans
- Quarantining Files
- Configuring Miscellaneous Settings

Active Directory Integration

- What Is Active Directory?
- How Is Active Directory Used?
- Working with Active Directory Integration
- Using Active Directory

Migrating to Symantec Endpoint Protection

- Migrating Legacy Symantec Antivirus Server and Client
- Migrating to Symantec Endpoint Protection 11.04
- Describing Other Deployment Methods

Designing a Symantec Endpoint Environment

- Architecture and Sizing Considerations
- Designing the Architecture
- Determining Client-to-SEPM Ratios
- Content Distribution Methods
- SEPM and Database Sizing
- Completing the Deployment

Introduction to Network Threat Protection and Application and Device Control

- Network Threat Protection Basics
- The Firewall
- Intrusion Prevention
- Application and Device Control

Configuring Firewall Policies

- Configuring Firewall Policy Elements
- Configuring Firewall Rules
- Configuring Smart Traffic Filtering
- Configuring Traffic and Stealth Settings

Managing Intrusion Prevention System (IPS) Policies

- Configuring IPS
- Managing Custom Signatures

Configuring Application and Device Control Policies

- Introducing Application and Device Control
- Creating Application and Device Control Policies
- Customizing Application and Device Control Policies

Customizing Network Threat Protection and Application and Device Control

- Managing Locations
- Managing Policy Components
- Configuring Application Learning
- Configuring System Lockdown

Configuring Additional Protection

- Configuring Tamper Protection
- Configuring Centralized Exceptions

Monitoring and Reporting

- Viewing Summary Data
- Viewing and Managing Logs
- Configuring and Viewing Notifications
- Creating and Viewing Reports

Performing Server and Database Management

- Managing Symantec Endpoint Protection Servers
- Managing Server Security
- Communicating with Other Servers
- Managing Administrators
- Managing the Database
- Disaster Recovery Techniques

Installing Additional Management Components

- Installing Additional LiveUpdate Servers
- Installing and Configuring the Central Quarantine
- Expanding the Management Environment