# Symantec Endpoint Protection 12.1: Administration

## COURSE DESCRIPTION

The *Symantec Endpoint Protection 12.1: Administration* course is designed for the network, IT security, and systems administration professional tasked with architecting, implementing, and monitoring virus and spyware protection, zero-day protection, and network threat protection solutions. This class covers how to design, deploy, install, configure, manage, and monitor Symantec Endpoint Protection 12.1 (SEP 12.1).

Students learn how to create and implement the client firewall, intrusion prevention, application and device control, and behavioral protection policies that guard the enterprise from viruses and hackers. In addition, students learn how to perform server and database management, expand the management environment, use virtualization features for virtual clients, and interface the Symantec Endpoint Protection Manager with Protection Center.

**Delivery Method**
Instructor-led training (ILT)

**Duration**
Five days

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

- Describe Symantec Endpoint Protection products, components, dependencies, and system hierarchy.
- Install and configure Symantec Endpoint Protection management and client components.
- Deploy Symantec Endpoint Protection clients.
- Manage the client user interface.
- Manage product content updates.
- Design a Symantec Endpoint Protection environment.
- Manage Virus and Spyware Protection policies.
- Manage SONAR scans.
- Manage Firewall and Intrusion Prevention policies.
- Manage Application and Device Control policies.
- Manage virtualized clients.
- Configure replication and load balancing.
- Monitor and maintain the Symantec Endpoint Protection environment.
- Interface the Symantec Endpoint Protection Manager with Protection Center.

**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 technologies
- Symantec Endpoint Protection services
- Symantec Endpoint Protection components
- Symantec Endpoint Protection policies and concepts
- Symantec Endpoint Protection product tiers

**Installing Symantec Endpoint Protection**

- Identifying system requirements
- Preparing servers for installation
- Installing and configuring the Symantec Endpoint Protection Manager
- Describing Symantec Endpoint Protection migration and version compatibility

**Configuring the Symantec Endpoint Protection Environment**

- Starting and navigating the SEPM
- Describing policy types and components
- Console authentication
- Licensing the SEP environment

**Deploying Clients**

- Client requirements and deployment methods
- Preparing for client deployment
- Client installation packages, settings, and features
- Installing managed clients

- Configuring an unmanaged detector
- Upgrading Symantec Endpoint Protection clients

**Client and Policy Management**
- Describing SEPM and client communications
- Administering clients
- Configuring groups
- Configuring locations
- Active Directory integration with SEP 12.1
- Client configuration modes
- Configuring domains
- General client settings and Tamper Protection

**Configuring Content Updates**
- Introducing LiveUpdate
- Configuring the SEPM for LiveUpdate
- Configuring the LiveUpdate Settings and Content policies
- Configuring multiple group update providers (GUPs)
- Manually updating virus definitions

**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

**Introducing Antivirus, Insight, and SONAR**
- Virus and spyware protection needs and solutions
- Reputation and Insight
- Administrator-defined scans
- Auto-Protect
- Download Insight
- SONAR
- Included Virus and Spyware Protection policies

**Managing Virus and Spyware Protection Policies**
- Configuring administrator-defined scans
- Configuring protection technology settings and scans
- Configuring e-mail scans
- Configuring advanced options
- Configuring Mac client detection
- Managing scanned clients
- Configuring Mac Virus and Spyware Protection policy settings

**Managing Exception Policies**
- Exceptions and exclusions
- Configuring the Exceptions policy

**Introducing Network Threat Protection and Application and Device Control**
- Network threat protection basics
- The firewall
- Intrusion prevention
- Application access protection

**Managing Firewall Policies**
- Firewall policy overview
- Defining rule components
- Modifying firewall rules
- Configuring built-in rules
- Configuring protection and stealth settings
- Configuring Windows integration settings

**Managing Intrusion Prevention Policies**
- Configuring intrusion prevention
- Managing custom signatures

**Managing Application and Device Control Policies**
- Creating application and device control policies
- Defining application control
- Modifying policy rules
- Defining device control

**Customizing Network Threat Protection and Application and Device Control**
- Tools for customizing network threat protection
- Managing policy components
- Configuring learned applications
- Configuring system lockdown

**Virtualization**
- Introducing virtualization features
- Virtual image exception
- Shared Insight Cache
- Virtual client tagging
- Offline image scanner

**Configuring Replication and Failover and Load Balancing**
- About sites and replication
- How replication works
- Symantec Endpoint Protection replication scenarios
- Configuring replication
- Failover and load balancing

**Performing Server and Database Management**
- Managing SEPM servers
- Maintaining server security
- Communicating with other servers
- Managing administrators
- Managing the database
- Disaster recovery techniques

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Specifications and product offerings are subject to change without notice.

**Advanced Monitoring and Reporting**

- Monitoring the Home and Monitors page
- Analyzing and managing logs
- Configuring and viewing notifications
- Creating and reviewing reports
- Introducing IT Analytics

**Interfacing the SEPM with Protection Center**

- Describing Protection Center
- Describing the Protection Center appliance
- Configuring Protection Center
- Using Protection Center

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Specifications and product offerings are subject to change without notice.