Administration of Symantec™ Endpoint Protection 12.1
Study Guide

The following tables list the Symantec SCS Certification exam objectives for the Administration of Symantec Endpoint Protection 12.1 exam and how these objectives align to the Symantec Endpoint Protection 12.1: Administration course.

The recommended course to prepare for this exam is:

- *Symantec Endpoint Protection 12.1: Administration (ILT/VA/WBT)*
- *Symantec Endpoint Protection Tech Center Modules*

The product documentation for this course includes the following:

- Symantec Endpoint Protection 12.1 from Symantec, version 12.1
- http://www.symantec.com/business/security_response/index.jsp
- http://edm.symantec.com/endpointsecurity/
- http://www.symantec.com/business/support/endpointsecurity/migrate/index.jsp
- http://www.symantec.com/business/services/support_services.jsp

Note: Product documentation can be obtained from ***https://sort.symantec.com/documents***

Examples of Hands-on Experience (Real World or Virtual):

- Explain how communication works between clients, manager, and the console, and configure clients to communicate properly.
- Integrate with Active Directory or LDAP.
- Manage the embedded or Microsoft SQL Symantec Endpoint Protection Manager database settings.
- Have a basic knowledge of Symantec Endpoint Protection replication, load balancing, and failover.
- Perform basic troubleshooting for Symantec Endpoint Protection.
- Aware of the Symantec Endpoint Protection support tools including Power Eraser.
- Activate the product with the appropriate license or serial number
- Create and Manage Administrator accounts in the Symantec Endpoint Protection Manager console
- Have a basic knowledge of Symantec Endpoint Protection domains.
- Design basic architectures.

- Distinguish between client-mode and user-mode.
- Design complex architectures, for example, large sites with low bandwidth and multiple data centers.
- Interpret the results of reports and determine the action to take to remediate the situation.
- Use unmanaged detector feature.
- Install and configure Macintosh and Linux clients.
- Configure Symantec Endpoint Protection replication, load balancing, and failover.
- Configure and implement Symantec Endpoint Protection domains.
- Perform basic disaster recovery planning and implementation.
- Enable debugging and gather logs for technical support use.
- Deploy software packages to new systems and update Symantec Endpoint Protection on existing clients.
- Verify Symantec Endpoint Protection clients are online and functional.
- Respond to Symantec Endpoint Protection client messages and apply a solution accordingly.
- Create Symantec Endpoint Protection policies based on a specified design.
- Describe the components that make up the Symantec Endpoint Protection 12.1 infrastructure.
- Prepare for, install, and configure the Symantec Endpoint Protection Manager and client software.
- Explain the process to upgrade a Symantec Endpoint Protection Manager and client.
- Possess in-depth knowledge of the Symantec Endpoint Protection Manager console and menus
- Manage clients through groups and locations.
- Manage and apply policies, such as Virus and Spyware Protection policies, Firewall policies, Intrusion Prevention policies, Application and Device Control policies, LiveUpdate policies, and Centralized Exception policies.
- Use reports and logs to identify security problems and monitor status and security events.
- Update products and content.
- Explain the options for updating clients.

For more information on the Symantec Certification Program, visit http://go.symantec.com/certification.

EXAM AREA 1

Products and Concepts

SCS Exam Objectives	Course Topics from *Symantec Endpoint Protection 12.1: Administration*
Explain common threats and security risks to the endpoint and the technologies that can protect against them, such as virus and spyware protection, Symantec Online Network for Advanced Response (SONAR), application and device control, the client firewall, intrusion prevention, and Symantec Insight.	**Lesson:** The Symantec Endpoint Product Solution **Topics:** Why use Symantec Endpoint Protection, Symantec Endpoint Protection technologies, Symantec Endpoint Protection services **Lesson:** Introducing Antivirus, Insight, and SONAR **Topics:** *All* **Lesson:** Introducing Network Threat Protection and Application and Device Control **Topics:** *All*
Describe the Symantec Endpoint Protection components, such as the Symantec Endpoint Protection Manager (SEPM), the Symantec Endpoint Protection client, Shared Insight Cache, and the SEPM database.	**Lesson:** The Symantec Endpoint Product Solution **Topic:** Symantec Endpoint Protection components **Lesson:** Installing Symantec Endpoint Protection **Topic:** Identifying installation requirements **Lesson:** Deploying Clients **Topic:** Client requirements and deployment methods **Lesson:** Virtualization **Topic:** Shared Insight Cache **Lesson:** Interfacing the SEPM with Protection Center **Topic:** Describing Protection Center
Explain how policies and concepts, such as groups, locations, sites, domains, and client modes relate to the Symantec Endpoint Protection architecture.	**Lesson:** The Symantec Endpoint Product Solution **Topic:** Symantec Endpoint Protection policies and concepts **Lesson:** Configuring the Symantec Endpoint Protection Environment **Topic:** Describing policy types and components **Lesson:** Client and Policy Management **Topics:** *All*
Given a scenario, determine proper placement for Group Update Provider (GUP), SEPM, and LiveUpdate Administrator (LUA) for communication and content deployment.	**Lesson:** Configuring Content Updates **Topics:** *All* **Lesson:** Designing a Symantec Endpoint Environment **Topics:** *All*

EXAM AREA 2

Installation and Configuration

SCS Exam Objectives	Course Topics from *Symantec Endpoint Protection 12.1: Administration*
Describe how to prepare, install, license and configure the Symantec Endpoint Protection management infrastructure.	**Lesson:** Installing Symantec Endpoint Protection **Topics:** *All* **Lesson:** Configuring the Symantec Endpoint Protection Environment **Topics:** *All*
Describe how to create and manage groups and locations to effectively configure and manage clients, and how to import users and groups from Active Directory or LDAP.	**Lesson:** Client and Policy Management **Topics:** *All*
Describe how to prepare and install the Symantec Endpoint Protection clients including creating client packages and choosing an appropriate deployment method.	**Lesson:** Deploying Clients **Topics:** *All* **Lesson:** Client and Policy Management **Topics:** *All*
Identify how to verify client connectivity and find clients in the console display.	**Lesson:** Client and Policy Management **Topics:** Describing SEPM and client Communications, Administering clients
Describe how to configure communication settings, general settings, and security settings.	**Lesson:** Client and Policy Management **Topic:** General client settings and Tamper Protection
Describe how to configure Symantec Endpoint Protection 12.1 for a virtual environment.	**Lesson:** Virtualization **Topics:** *All*
Describe how to configure LiveUpdate policies.	**Lesson:** Configuring Content Updates **Topics:** *All*
Describe when and how to configure exceptions.	**Lesson:** Managing Exception Policies **Topics:** *All*

EXAM AREA 3

Configuring Virus and Spyware Protection

SCS Exam Objectives	Course Topics from *Symantec Endpoint Protection 12.1: Administration*
Describe how protection technologies interact and their dependencies.	**Lesson: Introducing Antivirus, Insight, and SONAR** **Topic:** All **Lesson:** Managing Virus and Spyware Protection Policies **Topic:** Configuring administrator-defined scans
Describe how to configure scheduled and on-demand scans.	**Lesson:** Introducing Antivirus, Insight, and SONAR **Topic:** Administrator-defined scans **Lesson:** Managing Virus and Spyware Protection Policies **Topics:** Configuring administrator-defined scans, Configuring advanced options, Configuring Virus and Spyware policy settings for Mac clients
Describe how to configure Auto-Protect for the file system and email clients.	**Lesson:** Introducing Antivirus, Insight, and SONAR **Topic:** Auto-Protect scans **Lesson:** Managing Virus and Spyware Protection Policies **Topics:** Configuring Auto-Protect, Configuring Virus and Spyware policy settings for Mac clients
Describe how to configure Insight and Download Insight.	**Lesson**: Introducing Antivirus, Insight, and SONAR **Topics**: Reputation and Insight, Download Insight **Lesson**: Managing Virus and Spyware Protection Policies **Topics:** Configuring administrator-defined scans, Configuring Download Insight, Configuring SONAR
Describe how to configure SONAR.	**Lesson:** Introducing Antivirus, Insight, and SONAR **Topic:** SONAR **Lesson:** Managing Virus and Spyware Protection Policies **Topic:** Configuring SONAR

SCS Exam Objectives	Course Topics from *Symantec Endpoint Protection 12.1: Administration*
Explain the remediation actions for infected files.	**Lesson:** Introducing Antivirus, Insight, and SONAR **Topics:** *All* **Lesson:** Managing Virus and Spyware Protection Policies **Topics:** Configuring advanced options, Managing scanned clients

EXAM AREA 4

Define and Configure Firewall, Intrusion Prevention, and Application and Device Control

SCS Exam Objectives	Course Topics from *Symantec Endpoint Protection 12.1: Administration*
Describe how to configure the Firewall policy, including firewall rule processing order, built-in rules, protection and stealth settings, and Windows integration settings.	**Lesson:** Introducing Network Threat Protection and Application and Device Control **Topic:** The firewall **Lesson:** Managing Firewall Policies **Topics:** *All*
Describe how to configure intrusion prevention policies including settings and exceptions for network and browser intrusion prevention.	**Lesson:** Introducing Network Threat Protection and Application and Device Control **Topic:** Intrusion Prevention **Lesson:** Managing Intrusion Prevention Policies **Topics:** *All*
Describe how to configure application and device control policies including application rule sets and system lockdown.	**Lesson:** Introducing Network Threat Protection and Application and Device Control **Topic:** Application and Device Control **Lesson:** Managing Application and Device Control Policies **Topics:** *All* **Lesson**: Customizing Network Threat Protection and Application and Device Control **Topics:** Tools for customizing network threat protection

SCS Exam Objectives	Course Topics from *Symantec Endpoint Protection 12.1: Administration*
Describe how to customize firewall, intrusion prevention, and application and device control policies using file fingerprint liSCS, host groups, network services, network adapters, and hardware devices, and learned applications.	**Lesson:** Client and Policy Management **Topic:** Configuring locations **Lesson:** Customizing Network Threat Protection and Application and Device Control **Topics:** *All*

EXAM AREA 5

Additional Management and Monitoring Tasks

SCS Exam Objectives	Course Topics from *Symantec Endpoint Protection 12.1: Administration*
Explain when to install additional Symantec Endpoint Protection Managers and sites and how to configure them for replication, failover, and load-balancing.	**Lesson:** Designing a Symantec Endpoint Environment **Topics:** *All* **Lesson:** Configuring Replication and Failover and Load Balancing **Topics:** *All*
Describe how to edit server and site properties, for example, adding notification email servers, directory servers, proxy servers, and external logging.	**Lesson:** Configuring the Symantec Endpoint Protection Environment **Topic:** Console authentication **Lesson:** Performing Server and Database Management **Topics:** *All*
Explain the procedures for Symantec Endpoint Protection database management, backup, restore and Symantec Endpoint Protection disaster recovery.	**Lesson:** Performing Server and Database Management **Topics:** *All*
Describe how to create, view, and manage notifications including how to create and view logs, monitors, and reports and act on events with actionable reports.	**Lesson:** Configuring the Symantec Endpoint Protection Environment **Topic:** Starting and Navigating the SEPM **Lesson:** Advanced Monitoring and Reporting **Topics:** *All*
Describe how to manage administrator accounts and delegation of roles using the Symantec Endpoint Protection Management console.	**Lesson:** Configuring the Symantec Endpoint Protection Environment **Topic:** Console authentication

SCS Exam Objectives	Course Topics from *Symantec Endpoint Protection 12.1: Administration*
Describe how and when to use supplemental Symantec tools, such as Power Eraser, Sylinkdrop, SymHelp, and IT Analytics (Understand and Apply with some Analyze/Evaluate scenario items possible)	**Lesson**: Installing Symantec Endpoint Protection **Topic**: Identifying system requirements **Lesson**: Client and Policy Management **Topic**: Configuring domains **Lesson**: The Symantec Protection Product Solution **Topic**: Symantec Endpoint Protection components

If you have questions about the Symantec Certification Program, send an email to Global_Exams@symantec.com.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com