BROADCOM®
SOFTWARE

Exam 250-428: Symantec Endpoint Protection 14 Technical Specialist

Exam Study Guide v. 4.0

Exam Description

Candidates can validate technical knowledge and competency by becoming a Broadcom Technical Specialist (BTS) based on your specific area of Symantec technology expertise. To achieve this level of certification, candidates must pass this proctored BTS exam that is based on a combination of Symantec training material, commonly referenced product documentation, and real-world job scenarios.

This exam targets IT Professionals using the Symantec Endpoint Protection 14 (or later) product in a Security Operations role. This certification exam tests the candidate's knowledge on how to how to install, configure and administer Symantec Endpoint Protection.

For more information about Broadcom Software's certification program, see
https://www.broadcom.com/support/education/software/certification

Recommended Experience

It is recommended that the candidate has at least 3-6 months experience working with the Symantec Endpoint Protection 14 (or later) products in a production or lab environment.

Study References

Self-Paced https://login.broadcom.com/app/broadcomincexternal_cornerstoneexterna

Symantec Endpoint Protection 14.x Planning and Implementation

(4-Hour Self-Paced eLearning)

- Architecting and Sizing the SEP Implementation
- Installing the Symantec Endpoint Protection Manager
- Benefiting from a SEPM Disaster Recovery Plan
- Managing Replication and Failover
- Deploying Windows Clients
- Deploying Linux Clients
- Deploying Mac Clients
- Upgrading and Cloud Enrollment

Instructor-Led https://www.broadcom.com/support/education/software

Symantec Endpoint Protection 14.2 Manage and Administer

(2-Day Classroom/Virtual)

- Managing Console Access and Delegating Authority
- Managing Client-to-Server Communication
- Managing Client Architecture and Active Directory Integration
- Managing Clients and Responding to Threats

- Monitoring the Environment and Responding to Threats
- Creating Incident and Health Status Reports
- Introducing Content Updates Using LiveUpdate
- Analyzing the SEPM Content Delivery System
- Managing Group Update Providers
- Managing Certified and Rapid Release Definitions
- Configuring Location Aware Content Updates

Symantec Endpoint Protection 14.2 Configure and Protect

(3-Day Classroom/Virtual)

- Introducing Network Threats
- Protecting against Network Attacks and Enforcing Corporate Policies using the Firewall Policy
- Blocking Threats with Intrusion Prevention
- Introducing File-Based Threats
- Preventing Attacks with SEP Layered Security
- Securing Windows Clients
- Securing Linux Clients
- Securing Mac Clients
- Providing Granular Control with Host Integrity
- Controlling Application and File Access
- Restricting Device Access for Windows and Mac Clients
- Hardening Clients with System Lockdown
- Customizing Policies based on Location
- Managing Security Exceptions

Symantec Endpoint Protection 14.2 Maintain and Troubleshoot

(3-Day Classroom/Virtual)

- Troubleshooting Techniques and Tools
- Troubleshooting the Console
- Installation and Migration Issues
- Client Communication Issues
- Content Distribution Issues
- Extending the SEP infrastructure
- Responding to a Security Incident
- Performance Issues

Documentation

https://support.broadcom.com/security

- Symantec Endpoint Protection Installation and Administration Guide: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all.html
- Related Documents (Includes the following):
  - Symantec Endpoint Protection Client Guides
  - Release Notes
  - Sizing and Scalability Best Practices Whitepaper
  - Quick Start
  - REST API Reference Guide

  https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Related-Documents.html

Product Websites

- Symantec Endpoint Security
- https://support.broadcom.com/web/ecx/productdetails?productName=Endpoint%20Protection

Exam Objectives

The following tables list the Certification exam objectives for the exam and how these objectives align to the corresponding course topics and their associated lab exercises as well as the referenced product documentation.

Candidates are encouraged to complete applicable lab exercises as part of their preparation for the exam.

For more information on the Broadcom Certification Program, visit
https://www.broadcom.com/support/education/software/certification/all-exams

Exam Section 1: Products and Concepts

Exam Objectives	Applicable Course Content
Explain common threats and security risks to the endpoint	**Symantec Endpoint Protection 14.2: Configure and Protect** • **Module:** Introducing File-based Threats • **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ What is Symantec Endpoint Protection?
Describe the Symantec Endpoint Protection components	**Symantec Endpoint Protection 14.x: Planning and Implementation** • **Module:** Architecting and Sizing the SEP Implementation

	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ Getting Started

Explain how policies and concepts relate to the Symantec Endpoint Protection architecture	**Symantec Endpoint Protection 14.2: Manage and Administer**
	• **Module:** Managing Client Architecture and Active Directory Integration
	• **Documentation:** Managing Client Architecture and Active Directory Integration
	• **Labs:** Working with groups and locations
	  ○ Integrating with Active Directory
	  ○ Importing an AD group into the SEPM
	  ○ Creating groups and organizing clients o
	  ○ Managing group inheritance
	  ○ Working with location specific settings
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Managing Groups, Clients, Administrators, Passwords and Domains

Determine proper placement for GUP, SEPM, and LUA for communication and content deployment	**Symantec Endpoint Protection 14.s: Planning and Implementation** • **Module:** Architecting and Sizing the SEP Implementation • **Documentation:** Sizing and Scalability Best Practices for Symantec Endpoint Protection 14

Exam Section 2: Installation and Configuration

Exam Objectives	Applicable Course Content
Describe how to prepare, install, license, and configure the Endpoint Protection management infrastructure	**Symantec Endpoint Protection 14.x: Planning and Implementation &** **Symantec Endpoint Protection 14.2: Maintain and Troubleshoot** • **Module**: Installing the SEPM (Planning and Implementation), Installation and Migration Issues (Maintain and Troubleshoot) • **Documentation**: Symantec Endpoint Protection Installation and Administration Guide ○ Getting Started

Describe how to create groups and locations to effectively configure and manage clients	**Symantec Endpoint Protection 14.2: Manage and Administer**
	• **Module:** Managing Client Architecture and Active Directory Integration
	• **Labs:** Working with groups and locations
	  ○ Integrating with Active Directory
	  ○ Importing an AD group into the SEPM
	  ○ Creating group and organizing clients
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Managing Groups, Clients, Administrators, Passwords and Domains

Describe how to prepare and install the Symantec Endpoint Protection clients including creating client packages and choosing an appropriate deployment method	**Symantec Endpoint Protection 14.x: Planning and implementation &** **Symantec Endpoint Protection 14.2: Maintain and Troubleshoot** • **Module:** Implementing the Best Method to Deploy Windows Clients (Planning and implementation) and Installation and Migration Issues (Maintain and Troubleshoot) • **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ Getting Started

Identify how to verify client connectivity and find clients in the console	**Symantec Endpoint Protection 14.2: Manage and Administer &**
	Symantec Endpoint Protection 14.2: Maintain and Troubleshoot
	• **Module:** Managing Client-to-Server Communication and Client Communication Issues
	• **Labs:** Sylink and communication (Manage and Administer)
	  ○ Enrolling new endpoints
	  ○ Interpreting sylink.xml
	  ○ Moving clients to new SEPM Client communication issues (Maintain and Troubleshoot)
	  ○ Workstations do not show in console
	  ○ WCWS01 shows as self-managed
	  ○ Misconfigured Firewall rules
	  ○ Failover troubleshooting
	  ○ Linux not registering in the SEPM

	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ Managing the client-server connection

Describe how to configure communication, general, and security settings	**Symantec Endpoint Protection 14.2: Manage and Administer**
	• **Module:** Managing Client Architecture and Active Directory Integration
	• **Labs:** Working with groups and locations
	  ○ Creating groups and organizing clients
	  ○ Managing group inheritance
	  ○ Locking Tamper Protection
	  ○ Working with location specific settings
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Managing the client-server connection and How to update content and definitions on the client

Describe how to configure Symantec Endpoint Protection 14 for a virtual environment	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ Using Symantec Endpoint Protection in virtual infrastructures

Describe how to configure LiveUpdate policies	**Symantec Endpoint Protection 14.2: Manage and Administer**
	• **Module:** Introducing Content Updates and LiveUpdate
	• **Labs:** Managing Content Updates (Manage and Administer)
	  ○ Configuring Group Update Providers
	  ○ Configuring the Content Distribution Monitor Tool
	  ○ Configuring location aware content updates Content Update Issues (Maintain and Troubleshoot)
	  ○ LiveUpdate fails
	  ○ LiveUpdate configuration
	  ○ Content Delivery by Group Update Provider
	  ○ GUP Failover
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ How to Update content and definitions on the clients

Describe when and how to configure exceptions	**Symantec Endpoint Protection 14.2: Configure and Protect &**
	Symantec Endpoint Protection 14.2: Maintain and Troubleshoot
	• **Module:** Managing Security Exceptions (Configure and Protect) and Responding to a Security Incident (Maintain and Troubleshoot)
	• **Labs:** Enforcing adaptive security
	  ○ Configuring scan exceptions
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Using Policies to Manage Security

Exam Section 3: Configuring Virus and Spyware Protection

Exam Objectives	Applicable Course Content

Describe how protection technologies interact and their dependencies	**Symantec Endpoint Protection 14.2: Configure and Protect**
	• **Module:** Preventing Attacks with SEP Layered Security
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Managing protection with security policies
	  ○ Managing Virus and Spyware Protection
	  ○ Customizing Scans

Describe how to configure scheduled and on-demand scans	**Symantec Endpoint Protection 14.2: Configure and Protect &** **Symantec Endpoint Protection 14.2: Maintain and Troubleshoot** • **Module:** Securing Windows Clients (Configure and Protect) and Responding to a Security Incident (Maintain and Troubleshoot) • **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ Using Policies to Manage Security
Describe how to configure Auto-Protect for file systems/email clients	**Symantec Endpoint Protection 14.2: Configure and Protect &**

	Symantec Endpoint Protection 14.2: Maintain and Troubleshoot
	• **Module:** Securing Windows Clients (Configure and Protect) and Responding to a Security Incident (Maintain and Troubleshoot)
	• **Labs:** Responding to a Security Incident Maintain and Troubleshoot)
	  ○ Protect Solusell
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Using Policies to Manage Security

Describe how to configure Insight and Download Insight	**Symantec Endpoint Protection 14.2: Configure and Protect**
	• **Module:** Securing Windows Clients
	• **Lab:** Securing Windows Clients
	  ○ Detecting unknown threats with Insight
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Using Policies to Manage Security

Describe how to configure SONAR	**Symantec Endpoint Protection 14.2: Configure and Protect**
	• **Module:** Securing Windows Clients
	• **Labs:** Enforcing adaptive security
	  ○ Configuring real-time behavioral protection (SONAR)
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Using Policies to Manage Security

Explain the remediation actions for infected files	**Symantec Endpoint Protection 14.2: Configure and Protect &**
	Symantec Endpoint Protection 14.2: Maintain and Troubleshoot
	• **Module:** Managing Exceptions (Configure and Protect) and Responding to a Security Incident (Maintain and Troubleshoot)
	• **Labs:** Enforcing adaptive security
	  ○ Configuring scan exceptions
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Using Policies to Manage Security

Exam Section 4: Define and Configure Firewall, Intrusion Prevention, and Application and Device Control

Exam Objectives	Applicable Course Content

Describe how to configure the firewall policy	**Symantec Endpoint Protection 14.2: Configure and Protect**
	• **Module:** Protecting against Network Attacks and Enforcing Corporate Policies using the Firewall Policy
	• **Labs:** Protecting against network attacks
	  ○ Preventing access to non-business sites
	  ○ Blocking remote access when the screensaver runs
	  ○ Blocking learned applications
	  ○ Block OS fingerprint and port scans
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Using Policies to Manage Security

Describe how to configure intrusion prevention policies	**Symantec Endpoint Protection 14.2: Configure and Protect**
	• **Module:** Blocking Threats with Intrusion Prevention
	• **Labs:** Blocking threats with Intrusion Prevention
	  ○ Protecting against memory tampering attacks
	  ○ Using custom IPS signatures to block a malicious site
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Using Policies to Manage Security

Describe how to configure application and device control policies	**Symantec Endpoint Protection 14.2: Configure and Protect**
	• **Module**: Controlling Application and File Access and Restricting Device Access for Windows and Mac Clients
	• **Labs:** Controlling application and file access
	  ○ Blocking unwanted applications with Application Control
	  ○ Restricting device access for Windows and Mac clients
	  ○ Disabling optical drives with Device Control
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ▪ Using Policies to Manage Security

Describe how to customize firewall, intrusion prevention and application and device control policies	**Symantec Endpoint Protection 14.2: Configure and Protect** • **Module:** Preventing Attacks with Symantec Endpoint Protection Layered Security • **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ Using Policies to Manage Security

Exam Section 5: Responding to Threats

Exam Objectives	Applicable Course Content
Explain when to install additional Symantec Endpoint Protection Managers and sites	**Symantec Endpoint Protection 14.x: Planning and implementation** • **Module**: Installing the SEPM • **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ Installing and Uninstalling the Management Server and Clients
Describe how to edit server and site properties	• **Documentation:** For server and site properties, search each topic in the Symantec Endpoint Protection Installation and Administration Guide
Explain the procedures for Symantec Endpoint Protection database management, backup, restore and Symantec Endpoint Protection disaster recovery	**Symantec Endpoint Protection 14.x: Planning and implementation** • **Module**: Benefiting from a SEPM Disaster Recovery Plan • **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ Managing management servers, sites, and databases

Describe how to create, view and manage notifications	**Symantec Endpoint Protection 14.2: Manage and Administer**
	• **Module:** Monitoring the Environment and Responding to Threats
	• **Labs:** Managing a security incident from the Monitors and Reports page
	  ○ Setting up alerting
	  ○ Observing an attack in progress
	  ○ Analyzing an incident
	  ○ Cleaning up the infection

	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ Managing Groups, Clients, Administrators, Passwords, and Domains

Describe how to manage administrator accounts and delegation of roles	**Symantec Endpoint Protection 14.2: Manage and Administer**
	• **Module:** Managing Console Access and Delegating Authority
	• **Labs:** Administering console accounts
	  ○ Resetting a login
	  ○ Creating a Limited Administrator account
	• **Documentation:** Symantec Endpoint Protection Installation and Administration Guide
	  ○ Managing Groups, Clients, Administrators, Passwords, and Domains

Describe how and when to use supplemental Symantec tools	**Symantec Endpoint Protection 14.2: Maintain and Troubleshoot** • **Module:** Troubleshooting Techniques and Tools and Responding to a Security Incident • **Documentation:** Symantec Endpoint Protection Installation and Administration Guide ○ Troubleshooting Symantec Endpoint Protection and Appendices

Sample Exam Questions

Review the following sample questions prior to taking an exam to gain a better understanding of the types of questions asked.

1. **Which protocol does an unmanaged detector use to identify systems on the network?**
   A. ICMP
   B. TCP
   C. ARP
   D. UDP

2. **An administrator has successfully installed Symantec Endpoint Protection Manager. Which component is deployed to the server at this point in time?**
   A. AntiVirus/AntiSpyware Protection
   B. Shared Insight Cache
   C. Apache T omcat Server
   D. Central Quarantine Server
   E. Internet Information Services (IIS)

3. **What is the first step an administrator must complete in order to integrate Active Directory with Symantec Endpoint Protection 14?**
   A. Import a Security Group or a Distribution Group.
   B. Import an Organizational Unit (OU), User Object, or Computer Object.
   C. Add the Active Directory server to the Symantec Endpoint Protection Site.
   D. Add the Active Directory server to a Symantec Endpoint Protection Manager.

4. **Which two methods can be used to identify the target machines to which the Symantec Endpoint Protection client can be installed when using the Client Deployment Wizard? (Select two.)**
   A. Browse through Windows networking.
   B. Import a file containing IP addresses.
   C. Specify a UNC path.
   D. Import a file from the Unmanaged Detector.
   E. Enable the ARP Discovery feature.

5. **When Auto-Protect is enabled, protection is optional for which type of file access?**
   A. Access
   B. Modify
   C. Backup
   D. Restore

6. **What happens when you mark the "Enable NetBIOS Protection" checkbox?**
   A. Verifies remote computer identity using WINS server lookup
   B. Blocks NetBIOS requests on all NetBIOS ports
   C. Permits NetBIOS connections from local subnet only
   D. Dynamically adds an allow rule for NetBIOS

7. **What are two uses of Application Control? (Select two.)?**
   A. Prevents applications from accessing the registry
   B. Prevents applications from creating files
   C. Prevents applications from accessing ports
   D. Prevents applications from replicating
   E. Prevents applications from accessing the network

8. **Scheduled reports are delivered as which type?**
   A. HTML
   B. XML
   C. MHT
   D. HTM

9. **How does an administrator manage Client User Interface Control Settings?**
   A. By group
   B. By location
   C. By domain
   D. By user

10. **Which criteria is used to define a Tamper Protection exception?**
    A. File fingerprint
    B. File name
    C. MD5 hash
    D. Process owner

11. **What should an administrator configure to prevent clients from receiving Proactive Threat Scan updates?**
    A. Virus and Spyware Protection policy
    B. LiveUpdate policy
    C. Intrusion Prevention policy
    D. LiveUpdate Content policy

12. **A company recently installed a proxy server and configured firewall rules to allow only HTTP traffic through the perimeter firewall. Since the change, Symantec Endpoint Protection 14 is unable to receive updates. Which step must be taken on the Symantec Endpoint Protection Manager to receive updates?**
    A. Configure proxy settings within Internet Explorer under Internet Options.
    B. Configure proxy settings under Server Properties.
    C. Configure proxy settings within the External Communication Settings.
    D. Configure proxy settings in the LiveUpdate policy.

13. **An administrator plans to make a duplicate of an existing policy and modify it for use on a test client in the Symantec Endpoint Protection Manager (SEPM). What is the quickest and simplest way to duplicate the existing policy?**
    A. Copy and paste the policy's XML file on the SEPM and log back into the console.
    B. Copy and paste the policy's XML file on the SEPM and restart the SEPM services.
    C. In the SEPM console's Policy page, copy the policy, and then paste the policy.
    D. Add a new client with inheritance turned off, then modify the policy.

14. **Which utility should be protected to prevent unauthorized access to the Symantec Endpoint Protection Manager in a production environment?**
    A. resetpass.bat
    B. sylinkdrop.exe
    C. scm.bat
    D. httpd.exe

15. **According to Symantec recommendations, a Symantec Endpoint Protection Manager should have how many replication partners?**
    A. Upto4
    B. Upto5
    C. Upto15
    D. Upto11

16. **Which two are used to block files using Download Insight, in addition to a file's reputation, (Select two.)?**
    A. The age of the file
    B. The website the file was downloaded from
    C. The protocol the file was downloaded with
    D. The number of other Symantec users with the same file
    E. A list of Internet domains

17. **In which two sets of circumstances would it be beneficial to exclude a host within an IPS policy? (Select two.)?**
    A. A company needs to set up custom intrusion prevent signatures in the IPS policy.
    B. To allow a vulnerability scanner on the network to ensure compliance with service agreements.
    C. A company may have computers on an internal network that need to be set up for testing purposes.
    D. To log the activity of a particular machine for auditing.
    E. To create an exception that will exclude particular IPS signatures.

18. **A company requires that sales representatives' laptops be managed even when they are out of the office. Which set up will ensure the most continuous management?**
    A. Create a remote location using location awareness.
    B. Place the Symantec Endpoint Protection Manager in the DMZ.
    C. Install an internal LiveUpdate server in the DMZ.
    D. Install Symantec Protection Center in the DMZ.

19. **Which is the most appropriate performance use case for searching clients by virtual platform version in the Symantec Endpoint Protection Manager's client view?**
    A. Moving clients to a group where Shared Insight Cache is enabled.
    B. Moving clients to a location where SONAR features are disabled.
    C. Moving clients to a group with disabled scheduled scans.
    D. Moving clients to a location with Download Insight enabled.

20. **What has the greatest impact on the size of the Symantec Endpoint Protection Manager database?**
    A. Number of content revisions.
    B. Number of log entries.
    C. Number of users.
    D. Number of backups to keep.

Sample Exam Answers:

1. C
2. C
3. D
4. A&B
5. C
6. C
7. A&B
8. C
9. B
10. B
11. D
12. B
13. C
14. A
15. B
16. A&D
17. B&C
18. B
19. A
20. B