



## Administration of Symantec™ Endpoint Protection 11.0 MR4 for Windows Exam Objectives

### SECTION 1

#### The Symantec Endpoint Protection Products and Concepts

- Define common threats and security risks to the endpoint as well as the technical controls that can prevent them from spreading past the endpoint.
- Describe the components of Symantec Endpoint Protection.
- Describe policies and how policies, groups, subgroups, locations, location awareness and policy inheritance relate to the Symantec Endpoint Protection architecture.

### SECTION 2

#### Symantec Endpoint Protection Installation

- Describe how to prepare, install and configure the Symantec Endpoint Protection management infrastructure.
- Describe how to create initial group structure and import users and groups from Active Directory or LDAP.
- Describe how to create client packages and choose appropriate deployment methods.
- Describe how to verify client connectivity and find clients in the console display.
- Describe how to install additional Symantec Endpoint Protection Managers and configure them for replication, failover, and load-balancing.
- Describe the upgrade/migration process from SAV/Sygate.

### SECTION 3

#### Configuring Antivirus, Antispyware, and Proactive Threat Scanning

- Describe how to configure exceptions.
- Describe how to configure scheduled and on-demand scans.
- Describe how to configure Autoprotect for the file system and email clients.
- Define actions for infected files.
- Describe how to configure proactive threat protection scans.

### SECTION 4

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

- Describe the basic function of a desktop/client firewall.
- Describe the elements necessary to configure the firewall policy.
- Describe the firewall rule processing order.
- Describe traffic blocking and stealth settings.
- Describe Intrusion Prevention System (IPS) functionality and how to modify policies.
- Describe Application and Device Control functionality and how to modify policies.
- Describe how to search for client applications.

### SECTION 5

#### Performing Additional Management and Monitoring Tasks

- Outline how to manage locations.
- Describe how to view and manage log files.
- Describe how to view and manage notifications.
- Describe how to create and view reports and monitors.
- Describe how to manage the client user interface control settings.
- Describe how to configure the LiveUpdate policies.

**SECTION 5 – Continued**

- Describe how to configure tamper protection.
- Describe how to manage Symantec Endpoint Protection Manager servers and sites.
- Describe how to manage role-based administration.
- Describe the Symantec Endpoint Protection database backup and restore.

**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](http://www.symantec.com)