McAfee Endpoint Security 10.7 Administration

Course Content –

Module 01: Course Welcome

- Introduce the course and course agenda.
- Introduce the training organization.
- Show common resources.
- Describe the lab environment and how to use the Lab Guide.

Module 02: McAfee Endpoint Security—Solution

- Overview
- Describe the solution and its key features.
- Identify new features and enhancements for this release.
- Identify the components in a basic deployment architecture.
- Explain how the solution works.

Module 03: Planning the Endpoint Security

- Deployment
- Identify considerations for defining business
- requirements or objectives.
- Identify supported operating systems and platform hardware for endpoints.
  Identify the components included with McAfee Endpoint Security.
- Identify legacy McAfee solutions you can migrate to McAfee Endpoint Security.
- Describe the key parts of a deployment plan.

Module 04: McAfee ePolicy Orchestrator

- Overview
- Identify key differences between McAfee ePO OnPremises, McAfee® ePO™ Cloud, and McAfee® MVISION™ ePO™.
- Identify the purpose of the McAfee Agent.
- Identify and distinguish between the menu bar options.
- Identify and explain the purpose of commonly used pages, such as the System Tree, Permissions Sets, and Users pages.
- Navigate through the interface and access commonly used pages.

Module 05: Installing McAfee Endpoint Security

- Packages and Extensions
- Explain how to obtain the required software components.
- Identify the steps to install McAfee Endpoint Security for use in McAfee ePO and standalone or selfmanaged environments.
- Identify and distinguish between the required software components.
- Add the required extensions and packages software to the McAfee ePO server.
- Verify the extensions and packages were added successfully to the McAfee ePO server.

Module 06: Migrating Legacy Settings

- Explain the purpose of Migration Assistant.
- Identify situations where manual or automatic migration is useful.
- Identify the steps to complete a manual migration.
- Identify the steps to complete an automatic migration.
- Identify which policy settings migrate.

Module 07: McAfee Endpoint Upgrade Assistant

- Identify the key features of the Endpoint Upgrade Assistant (EUA).
- Describe the differences between using the automatic upgrades and manual upgrades.
- Identify the products that can be migrated with the EUA.
- Identify limitations of EUA.
- Describe the supported command-line options.
- Describe how EUA works.
- Define what happens during the upgrade.
- Identify how to use the Package Creator to customize
- the McAfee Endpoint Security installation package.

Module 08: Deploy the McAfee Endpoint

- Security Client to the Endpoints
- Identify the different ways to deploy the required software components to endpoint systems.
- Deploy the required software components to the client endpoints.
- Verify the success of the deployment.

Module 09: Using the McAfee Endpoint Security

- Client
- Identify two ways to manage McAfee Endpoint Security clients.

- Open the McAfee Endpoint Security client interface.
- Log in as an administrator.
- Navigate through the client interface.
- Identify the default settings.

Module 10: Endpoint Security Policy

- Management Overview
- Explain the purpose of policies.
- Identify the various actions performed from the Policy Catalog page.
- Explain how policy inheritance works, as well as how to break inheritance.
- Explain policy ownership, as well as how to give other users permissions to control selected policy types.

Module 11: Configuring Common Settings

- Configure common settings that apply to all McAfee Endpoint Security modules and features, such as:
  − Client interface
  − Language
  − Logging
  − Proxy server for McAfee® Global Threat Intelligence
  (GTI) reputation
  − Update configuration
- 5 McAfee Endpoint Security 10.7 Administration

Module 12: Threat Prevention—Configuring

- Access Protection
- Describe the purpose of Access Protection policies.
- Identify types of McAfee-defined rules.
- Describe situations where user-defined rules are useful.
- Describe similarities and differences between McAfeedefined and user-defined rules.
- Describe how to enable and disable rules.
- Identify supported wildcards and syntax for exclusions.
- Customize a McAfee-defined rule.
- Create a user-defined rule.

Module 13: Threat Prevention—Configuring

- Exploit Prevention
- Describe the key features of McAfee Endpoint Security Exploit Prevention.
- Configure Exploit Prevention policies to meet customer requirements.
- Describe what happens if a system has both the Host Intrusion Prevention System and McAfee Endpoint Security installed.
- Describe how to configure the Network Intrusion feature of McAfee Endpoint Security.
- List the severities of the Exploit signatures.
- Define the types of expert rules.
- Define the application protection rules and how they work.
- Define how to create an exception for the signatures.

Module 14: Threat Prevention—Configuring OnAccess Scan

- Identify the different types of scanners that McAfee Endpoint Security provides.
- Explain how the on-access scanner works.
- Configure on-access scan settings to meet customer requirements.

Module 15: Threat Prevention—Configuring OnDemand Scans

- Identify the different types of on-demand scans that McAfee Endpoint Security provides.
- Explain how the on-demand scanners work.
- Configure on-demand scanner settings to meet customer requirements.

Module 16: Threat Prevention—Configuring the Options Policy

- Identify the purpose of the Quarantine Manager, Exclusions by Detection Name, and Potentially Unwanted Program (PUP) Detection.
- Describe some ways to manage quarantined items.
- Configure Quarantine Manager, Exclusions by Detection Name, and PUP Detection settings as necessary to meet customer requirements.

Module 17: Configuring Adaptive Threat Protection

- Identify the purpose of the Adaptive Threat Protection module.
- Deploy Adaptive Threat Protection.
- Identify the different policies available for Adaptive Threat Protection, as well as their default settings.
- Configure Adaptive Threat Protection policies to meet customer requirements.
- Configure Adaptive Threat Protection Server Settings.

Module 18: Firewall Overview and Configuring Firewall Options

- Identify the purpose of the Firewall module.
- Distinguish between the two types of Firewall policies.
- Configure settings in the Firewall Options policy to meet customer requirements.

Module 19: Configuring Firewall Rules and Groups

- Identify the purpose of Firewall rule and groups.
- Distinguish between settings for Firewall rules and groups.
- Identify considerations for rule design.
- Identify the purpose of location awareness, connection isolation, and timed groups.
- Describe best practices for Firewall configuration and rule design.
- Configure Firewall rules and groups to meet customer requirements.

Module 20: Configuring Web Control

- Identify the purpose of the Web Control module.
- Identify key features that Web Control provides.
- Identify the different policies available for Web Control, as well as their default settings.
- Configure Web Control policies to meet customer requirements.

Module 21: Monitoring and Reporting

- Access, navigate, and interpret dashboards.
- Describe situations where customized dashboards are useful.
- Generate and interpret queries and reports.
- View threat event detail.

Module 22: Protection Workspace Overview

- List the elements of the Protection Workspace user interface.
- Use the Protection Workspace dashboard to monitor your environment.

Module 23: McAfee Endpoint Security for Servers

- Describe the Smart Scheduler of McAfee Endpoint Security for Servers.
- Describe how to create resource-intensive tasks and a time slot for smart scheduling in the UI of the Smart Scheduler Catalog and Smart Scheduler.
- Describe the components and benefits of McAfee Endpoint Security for Servers.
- Describe how the CPU load is calculated.
- Describe how Smart Scheduler decides the number of instances that can run the on-demand scan while maintaining the CPU Utilization value below the threshold value.

- List the benefits of McAfee Endpoint Security for Servers.

Module 24: Data Exchange Layer and McAfee

- Threat Intelligence Exchange Overview
- Describe the Data Exchange Layer Overview (DXL) solution and its key features.
- Describe the McAfee Threat Intelligence Exchange (TIE) solution and its key features.