

---

# Course Objectives

## Chapter 1: Endpoint Security Media Encryption Overview

- Apply Endpoint Security Media Encryption in a corporate environment where appropriate, based on Media Encryption's use and methodology.
- Given your corporate network's structure and security policies, select the Endpoint Security Media Encryption components best suited to address security requirements.
- Given corporate requirements, install and configure Media Encryption Server.

## Chapter 2: Deploying Media Encryption

- Determine the most appropriate settings necessary to apply corporate requirements using the Endpoint Security Media Encryption Management Console.
- Create and apply profile templates using Device Manager, Removable Media Manager, Encryption Policy Manager, and Program Security Guard.
- Create and apply users, computers, and user and computer groups for Media Encryption according to corporate Security Policy requirements.
- Install and deploy Media Encryption Client.

## Chapter 3: Endpoint Security Media Encryption Client

- Test the deployed profiles using pre-constructed security risks.

- 
- Execute actions to initiate alerts for PSG, RMM and EPM.
  - Add a new device using the Device Configuration Editor in the management console, and test the new device from the client.
  - Encrypt, decrypt and verify removable media using the Encryption Policy Manager.

## Chapter 4: Logging, Auditing and Reporting

- Use Endpoint Security Media Encryption's internal logging and auditing functions to track and monitor user actions.
- Configure and execute reports based on Media Encryption audit events using pre-configured reports.
- By filtering audit events, identify a new device to add into Device Manager using the Device Configuration Editor in the administration console.