Trellix

DATASHEET

Trellix Endpoint Security Administration

Education Services Instructor-led Training

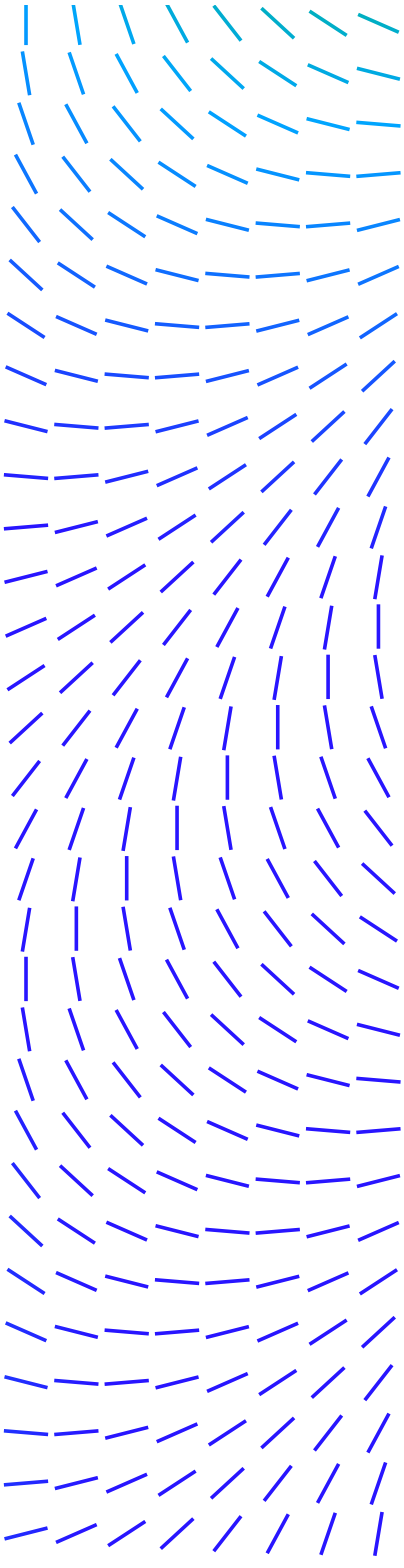
Introduction

Our Endpoint Security Administration course provides an in-depth introduction to the tasks crucial to set up and administer Endpoint Security. Endpoint Security combines Threat Prevention, Adaptive Threat Protection, Firewall, and Web Control to take immediate action against potentially dangerous applications, downloads, websites, and files. This course combines lectures and practical lab exercises, with significant time allocated for hands-on interaction with the Endpoint Security user interface and policies, as well as detailed instructions for the integration of this solution.

> This course provides in-depth introduction to the tasks crucial to set up and adminster Enpoint Security.

Audience

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with system endpoint security.



Agenda At A Glance

Day 1

- Module 01 - Welcome
- Module 02 - Solution Overview
- Module 03 - Planning the Deployment
- Module 04 - ePolicy Orchestrator Overview
- Module 05 - Installing Endpoint Security Software

Day 2

- Module 06 - Deploying the Endpoint Clients
- Module 07 - Using Endpoint Security Client
- Module 08 - Policy Management Overview
- Module 09 - Common Configuration Settings
- Module 10 - Threat Prevention: Configuring Access Protection

Day 3

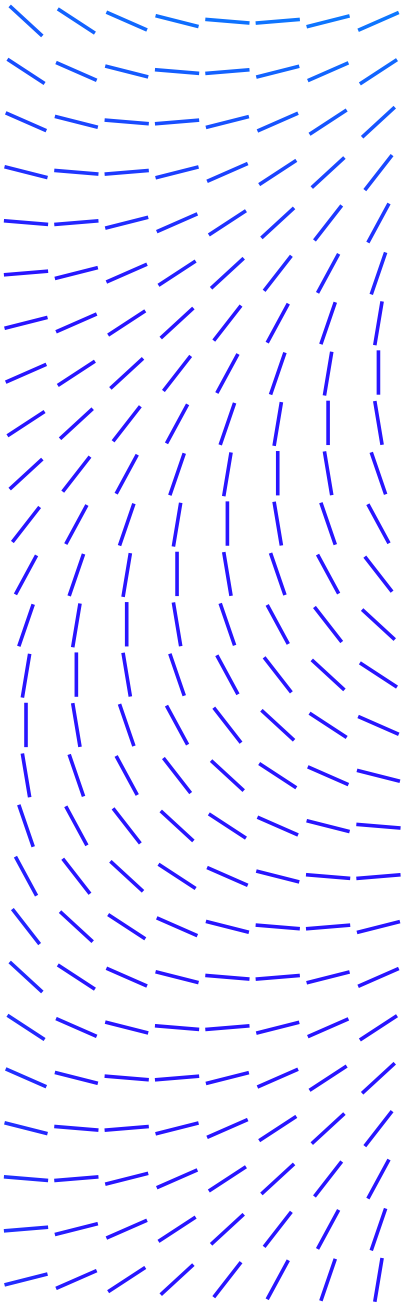
- Module 12 - Threat Prevention: Configuring On-Access Scanner
- Module 13 - Threat Prevention: Configuring On-Demand Scanners
- Module 14 - Configuring Threat Prevention Options
- Module 15 - Configuring Adaptive Threat Protection
- Module 16 - Firewall Overview and Configuring Firewall Options

Day 4

- Module 17 - Configuring Firewall Rules and Groups
- Module 18 - Configuring Web Control
- Module 19 - Monitoring and Reporting
- Module 20 - ENS for Servers
- Module 21 - Protection Workspace
- Module 22 - Data Exchange Layer and Threat Intelligence Exchange Overview

Recommended Pre-Work

- Solid knowledge of Windows and system administration and network technologies
- Basic understanding of computer security, command line syntax, malware/anti-malware, virus/ antivirus, and web technologies.
- Working knowledge of ePO software.



Course Learning Objectives

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: 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

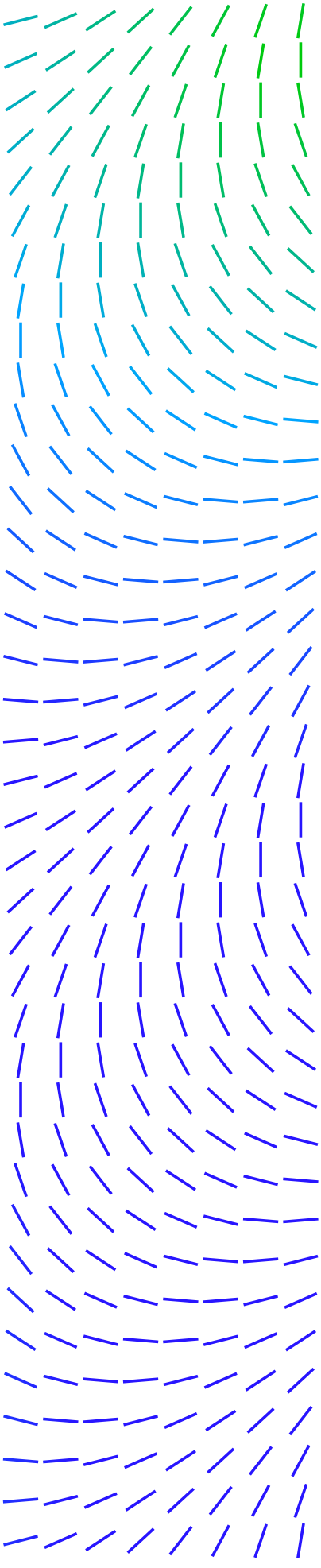
- Identify considerations for defining business requirements or objectives.
- Identify supported operating systems and platform hardware for endpoints.
- Identify the components included with ENS.
- Describe the key parts of a deployment plan.

Module 04: ePolicy Orchestrator Overview

- Identify key differences between ePolicy Orchestrator (ePO) On-Premises, ePolicy Orchestrator (ePO) Cloud, and 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 Endpoint Security Packages and Extensions

- Explain how to obtain the required software components.



- Identify the steps to install Endpoint Security for use in ePolicy Orchestrator and standalone or self-managed environments.
- Identify and distinguish between the required software components.
- Add the required extensions and packages software to the ePO server.
- Verify the extensions and packages were added successfully to the ePO server.

Module 06: Deploy the 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 07: Using the Endpoint Security Client

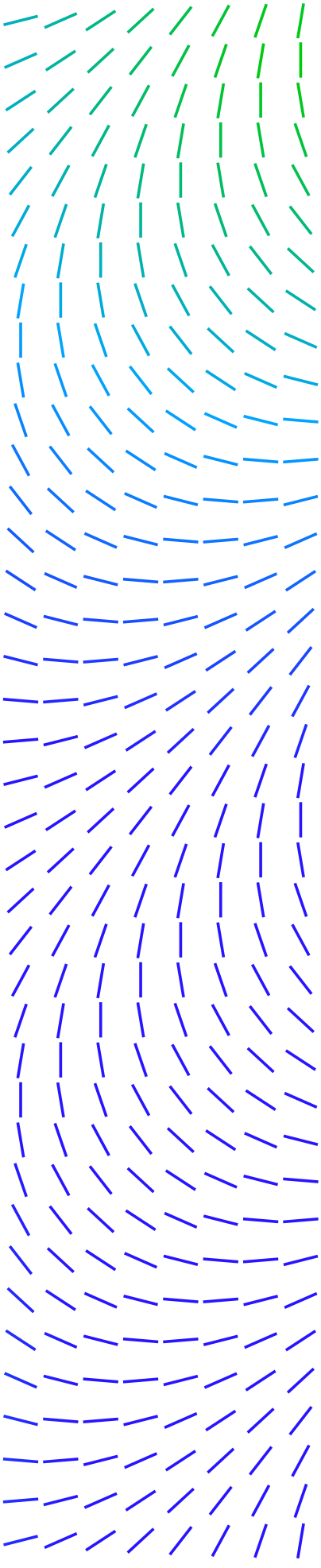
- Identify two ways to manage ENS clients.
- Open the ENS client interface.
- Log in as an administrator.
- Navigate through the client interface.
- Identify the default settings.

Module 08: 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 09: Configuring Common Settings

- Configure common settings that apply to all Endpoint Security modules and features, such as:
- Client interface
- Language



- Logging
- Proxy server for Global Threat Intelligence (GTI) reputation
- Update configuration

Module 10: Threat Prevention - Configuring Access Protection

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

Module 11: Threat Prevention - Configuring Exploit Prevention

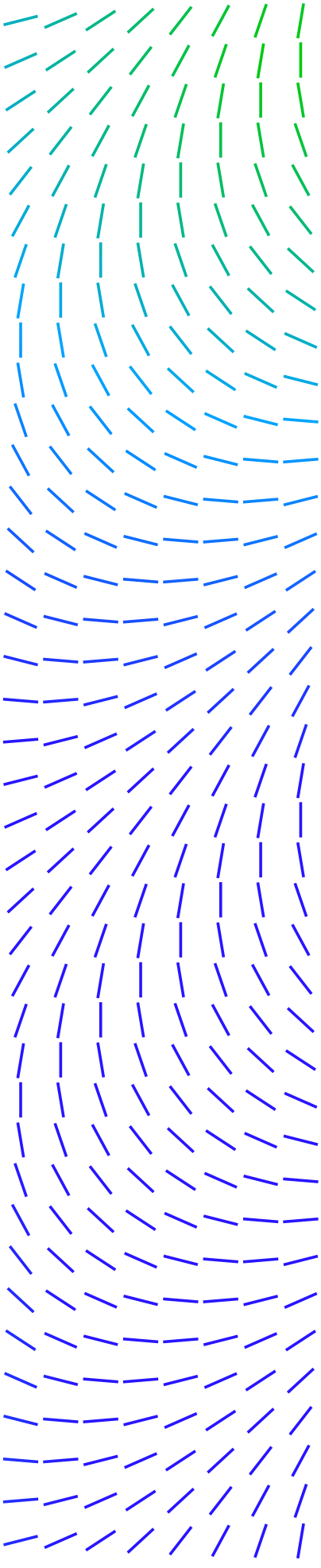
- Describe the key features of ENS Exploit Prevention.
- Configure Exploit Prevention policies to meet customer requirements.
- Describe how to configure the Network Intrusion feature of ENS.
- List the severities of the Exploit signatures.
- Define the types of expert rules.
- Define the application protection rules and how they work.
- Define how to create an exception for the signatures.

Module 12: Threat Prevention - Configuring On-Access Scan

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

Module 13: Threat Prevention - Configuring On-Demand Scans

- Identify the different types of on-demand scans that ENS provides.



- Explain how the on-demand scanners work.
- Configure on-demand scanner settings to meet c ustomer requirements.

Module 14: 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 15: 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 c ustomer requirements.
- Configure Adaptive Threat Protection Server Settings.

Module 16: 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 17: 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 18: 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 19: 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 20: Endpoint Security for Servers

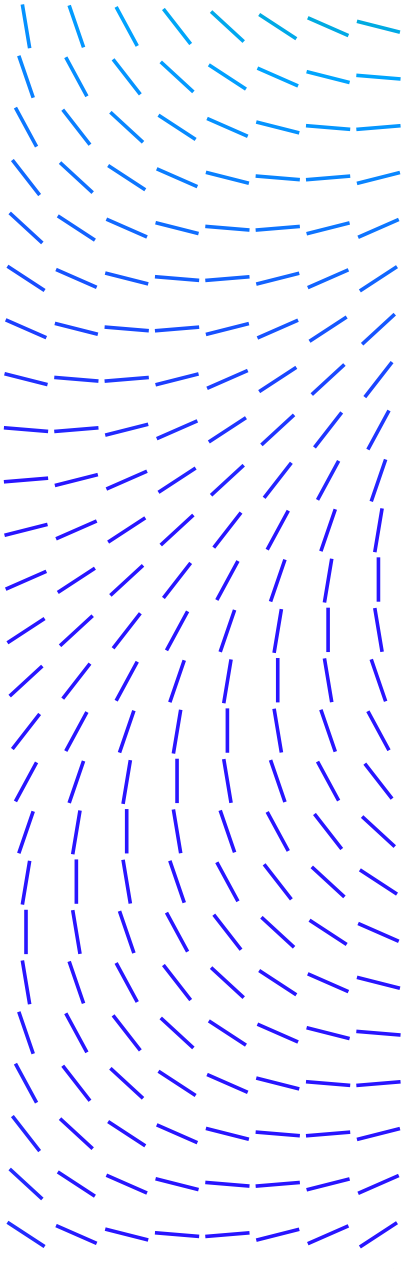
- Describe the Smart Scheduler of the ENS for Servers.
- Describe how to create resource-intensive tasks and a time slot for smart scheduling in the UI of the Smart Scheduler Catalog and Smart Scheduler.
- Describe the components and benefits of the ENS for Servers.
- Describe how the CPU load is calculated.
- 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 ENS for Servers.

Module 21: Protection Workspace Overview

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

Related Courses

- ePO Software Administration
- Advanced Threat Defense Administration
- Web Gateway Administration



Module 22: Data Exchange Layer and Threat Intelligence Exchange Overview

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

.