Trellix

DATASHEET

MVISION Endpoint with MVISION ePO Administration

Education Services Instructor-led Training

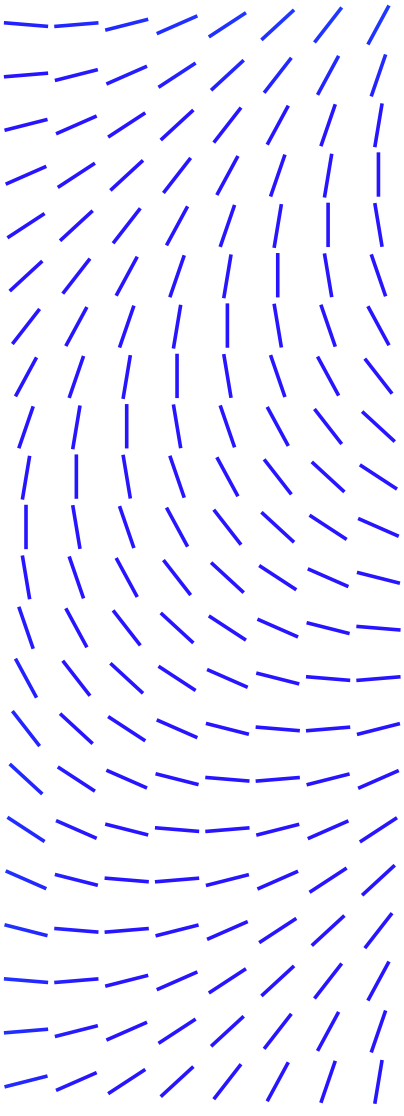
Introduction

Our MVISION Endpoint with MVISION ePolicy Orchestrator Administration course provides an in-depth introduction to the tasks crucial to set up and administer MVSION Endpoint in an MVISION ePO managed customer environment. MVISION Endpoint leverages and enhances built-in Windows 10 Windows Defender security with advanced protection for Windows 10 and Windows Server 2016 and newer systems. MVISION ePO is a SaaS-based centralized security management console that enables management of Microsoft Defender along with McAfee security products. This course combines lectures and practical lab exercises, with significant time allocated for hands-on interaction with the MVISION Endpoint policies in the MVISION ePO user interface, as well as detailed instructions for the integration of this solution.

> This course provides an in-depth introduction to the tasks crucial to set up and administer MVISION Endpoint in an MVISION ePO managed customer environment.

Audience

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with administering MVISION Endpoint on MVISION ePO. It is recommended that the students have a working knowledge of Microsoft Windows administration, Microsoft Windows Defender, system administration concepts, a basic understanding of computer security concepts, and a general understanding of viruses and anti-virus technologies.



Agenda At A Glance

Day 1

- Module 1: Welcome
- Module 2: MVISION ePO: Product Introduction
- Module 3: MVISION ePO: Features and Architecture
- Module 4: MVISION ePO: Role of an Administrator
- Module 5: MVISION ePO: Planning and Populating the System Tree

Day 2

- Module 6: MVISION ePO: Using the Tag Catalog
- Module 7: MVISION ePO: Client Tasks
- Module 8: MVISION ePO: Managing Policies
- Module 9: MVISION ePO: Automatic Responses and Notifications
- Module 10: MVISION Endpoint: Product Introduction
- Module 11: MVISION Endpoint: Product Deployment

Day 3

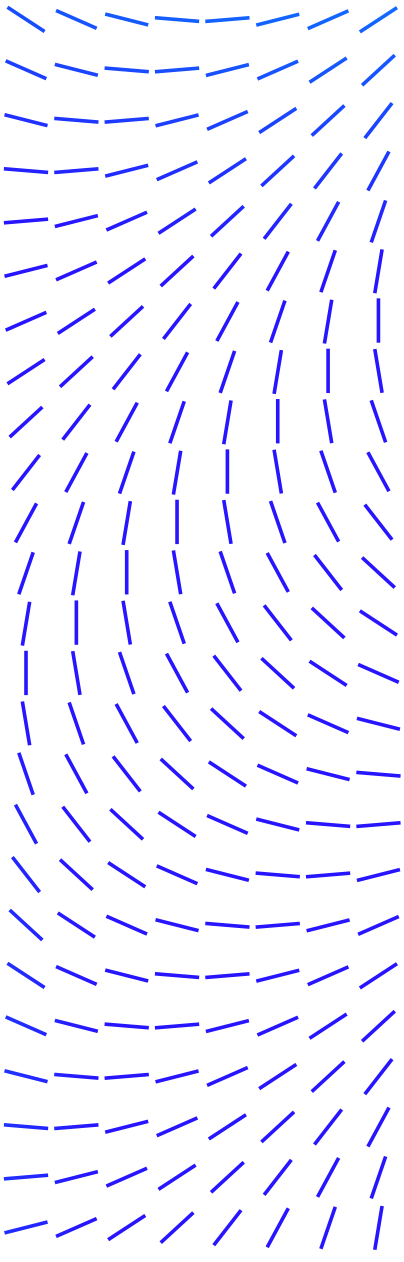
- Module 12: MVISION Endpoint: General Policy
- Module 13: MVISION Endpoint: Firewall Policy
- Module 14: MVISION Endpoint: Exclusions Policy, Evaluation Builds and Non-compliance Notifications
- Module 15: MVISION Endpoint: Exploit Guard and the MVISION Endpoint Exploit Protection Program Settings Policy
- Module 16: MVISION Endpoint: Protection Workspace Overview

Day 4

- Module 17: MVISION Endpoint: Quarantine Management
- Module 18: MVISION Endpoint: Log Files
- Module 19: MVISION ePO: Queries
- Module 20: MVISION ePO: Queries and Reports

Recommended Pre-Work

- Working knowledge of Microsoft Windows administration including Microsoft Windows Defender.
- Working knowledge of system administration concepts.
- Basic understanding of computer security concepts, and a general understanding of viruses and anti-virus technologies.



Course Learning Objectives

M01 - 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

M02 - MVISION ePO Product Introduction

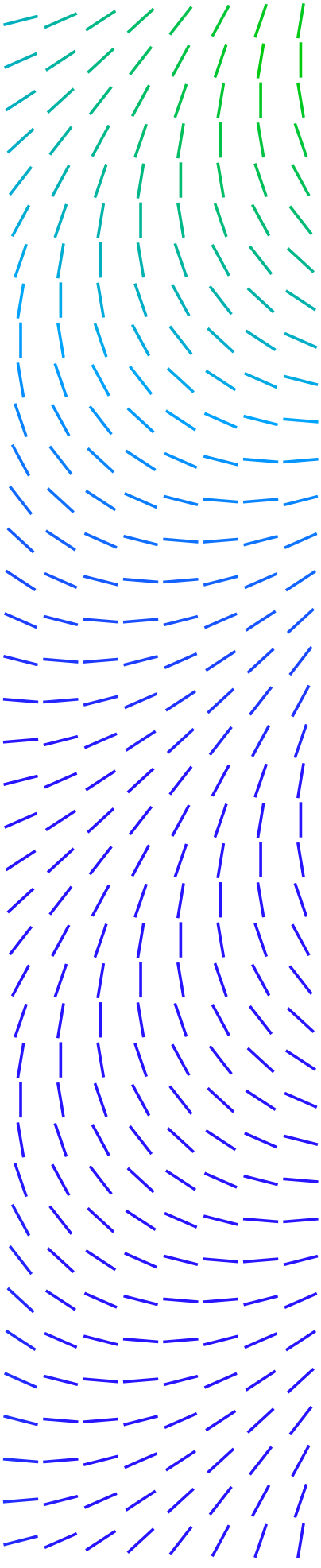
- Describe the MVISION ePolicy Orchestrator (MVISION ePO) offering.
- Explain the MVISION ePO deployment model.
- Describe the process for migrating from On-Prem ePO to MVISION ePO.
- Discuss integration with Endpoint Security (ENS) with Advanced Threat Protection (ATP).
- Discuss MVISION ePO integration with Security Information and Event Management (SIEM).
- Describe the support model for MVISION ePO.

M03 - MVISION ePO Features and Architecture

- Describe the basic features and functionalities for the MVISION ePO offering.
- Describe MVISION ePO architecture.

M04 - MVISION ePO Role of an Administrator

- Describe differences between Admin and user accounts in MVISION ePO.
- Describe how to configure and manage users accounts in MVISION ePO.
- Create a customized installation URL for system management in MVISON ePO.
- Create an agent installer package to distribute to systems for system management in MVISION ePO.
- Describe how to use custom queries and report in MVISION ePO.



- Describe how to configure server and client tasks in MVISION ePO.
- Describe how to remove product software using the existing product deployment task.

M05 – MVISION ePO Planning and Populating the System Tree

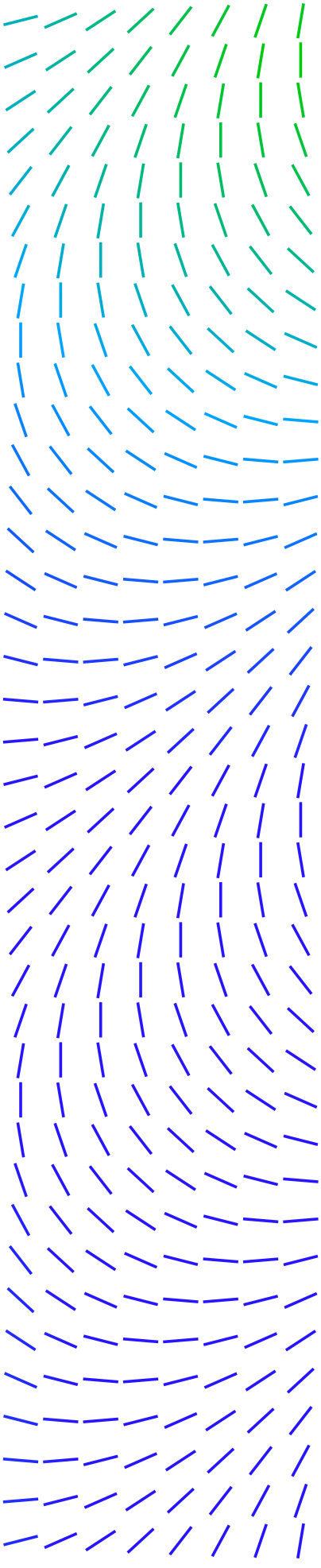
- Provide an overview of the ePolicy Orchestrator System Tree.
- Use different methods to create the System Tree.
- Describe the various methods of organizing the System Tree.

M06 - MVISION ePO Using the Tag Catalog

- Describe the purpose of tags and tag groups.
- List the types of tags that ePO supports.
- Access and navigate the Tag Catalog.
- Launch and navigate the New Tag Builder.
- Create and apply tags automatically, based on criteria and product properties.
- Create and apply tags manually.
- Restrict tag usage by permission set.
- Edit, move, and clear tags.
- Exclude systems from automatic tagging.

M07 - MVISION ePO Client Tasks

- Describe the purpose of client tasks.
- Communicate about client task concepts, such as inheritance.
- Access and navigate the Client Task Catalog.
- Identify client task types.
- Add, duplicate, edit, schedule, and delete a client task.
- Navigate and configure task using the Product Deployment Project.
- Navigate and configure task using the Deploy tab.



M08 - MVISION ePO Managing Policies

- Describe the purpose of policies.
- Create and edit policy objects.
- Manage policy configuration and assignment.
- See policy inheritance in action.
- Enforce policy changes on client machines (endpoints).

M09 - MVISION ePO Automatic Responses and Notifications

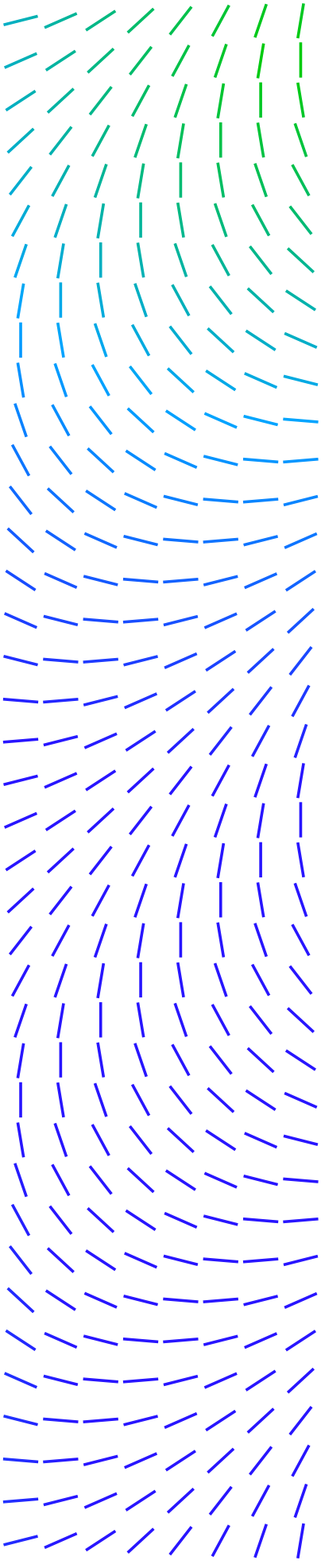
- Use Automatic Response rules to create alerts and perform pre-determined actions.
- Configure Automatic Responses.
- Describe permission set definitions for Automatic Responses.
- Describe how to configure contacts for notifications.

M10 - MVISION Endpoint Product Introduction

- Describe the MVISION Endpoint product components.
- Explain how MVISION Endpoint works with Microsoft Windows Defender®.
- List other McAfee products that work with MVISON Endpoint.

M11 - MVISION Endpoint Product Installation

- Determine the type of installation needed.
- Plan the installation.
- List the system requirements.
- Perform pre-installation tasks.
- Install MVISION Endpoint.
- Confirm the product installation.
- Upgrade to a new software version.
- Remove the MVISION Endpoint software.



M12 - MVISION Endpoint General Policy

- List the four default MVISION Endpoint policies available in ePO.
- Configure general policy security setting for managed systems on MVISION Endpoint.
- Use the MVISION Endpoint Updated extension to allow automatic updates on ePO and ePO on AWS managed installations.

M13 - MVISION Endpoint Firewall Policy

- Manage Windows Defender Firewall rules using the MVSION Endpoint Firewall policy.

M14 - MVISION Endpoint Exclusions Policy, Evaluation Builds and Non-compliance Notifications

- Configure and define exclusions for MVISION Endpoint and Windows Defender.
- Describe how to use MVISION Endpoint Evaluation builds for On-Premises ePO and ePO on AWS man-aged systems.
- Describe the Non-compliance notifications in MVISION Endpoint.

M15 - Exploit Guard and the MVISION Endpoint Exploit Protection Program Settings Policy

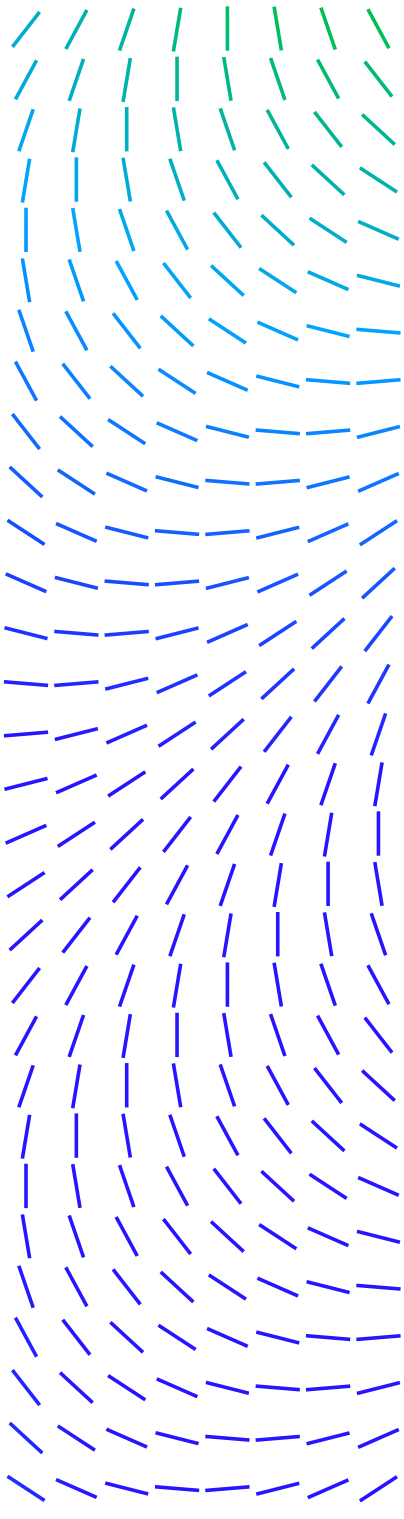
- List the four components of Windows Defender Exploit Guard and can be managed by MVISION End-point.
- Enable and configure Attack Surface Reduction rules in MVISION Endpoint.
- Enable and configure Network Protection in MVISION Endpoint.
- Enable and configure Controlled Folder Access in MVISION Endpoint.
- Enable and configure Exploit Protection in MVISION Endpoint.

M16 - Protection Workspace Overview

- List the elements of the Protection Workspace user interface.
- Use the Protection Workspace.

Related Courses

- MVISION ePO Essentials



M17 - MVISION Endpoint Quarantine Management

- Describe MVISION Endpoint Quarantine Management.
- List requirements for MVISION Endpoint Quarantine Management.
- Demonstrate the operation of MVISION Endpoint Quarantine Management.

M18 - MVISION Endpoint Log Files

- Use the MVISION Endpoint installation/uninstallation logs to troubleshoot software installation issues.
- Use the MVISION Endpoint product logs to troubleshoot s ystem issues.
- Set the logging level and log file size in the MVISION Endpoint General policy.
- Use the Story Graph feature to trace and troubleshoot MVISION Endpoint threat detections.

M19 - MVISION ePO Queries

- Using ePO query tools, create your own custom queries.
- Query the McAfee ePolicy Orchestrator database.
- Use the Query Builder to create your own queries.
- List the locations to find more details for your custom queries.

M20 - MVISION ePO Customizing Queries - Result Types and Charts

- Use the Query Builder to create your own queries.
- Define the different Chart types.
- Define the Common Labels that can be used in a query.
- Define the Common Values that can be used in a query.
- Describe the best settings to use when creating a query.