Trellix

DATASHEET

Drive Encryption

Education Services Instructor-led Training

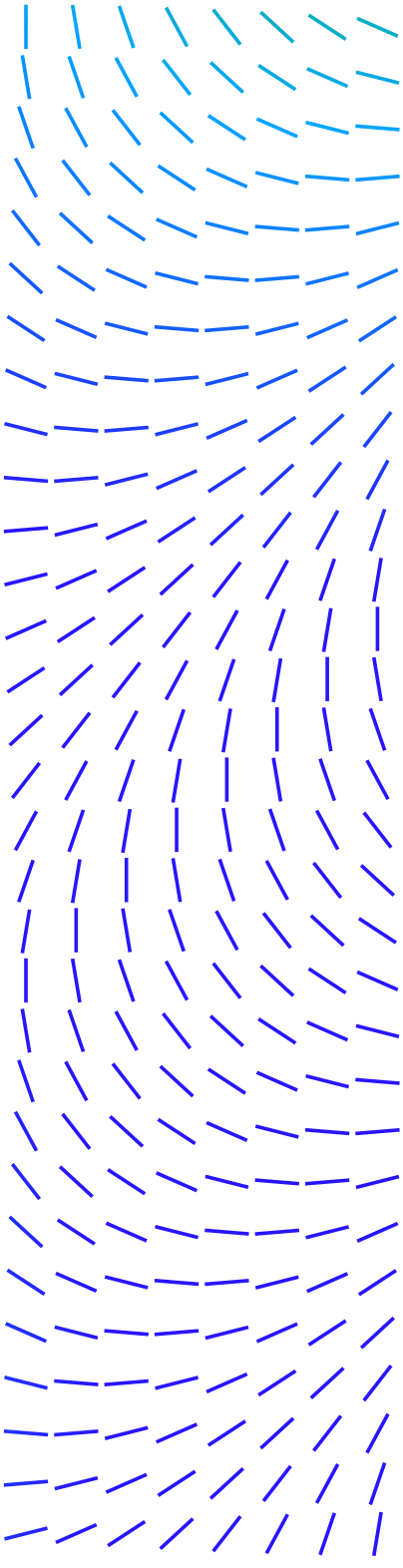
Introduction

Our Drive Encryption Administration course provides an in-depth introduction to the tasks crucial to set up and administer Drive Encryption. Drive Encryption is full disk encryption software that helps protect data on Microsoft Windows tablets, laptops, and desktop PCs to prevent the loss of sensitive data, especially from lost or stolen equipment. It is designed to make all data on a system drive unintelligible to unauthorized persons, which in turn helps meet compliance requirements. This course combines lectures and practical lab exercises, with significant time allocated for hands-on interaction with virtual lab systems, as well as detailed instructions for the integration of this solution.

> This course provides an in-depth introduction to the tasks cruicial to set up and administer Drive Encryption.

Audience

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



Agenda At A Glance

Day 1

- M01 Welcome
- M02 ePO Overview
- M03 The McAfee Agent
- M04 MDE Planning
- M05 Encryption Technologies
- M06 McAfee Drive Encryption (MDE) Overview
- M07 Extensions and Packages

Day 2

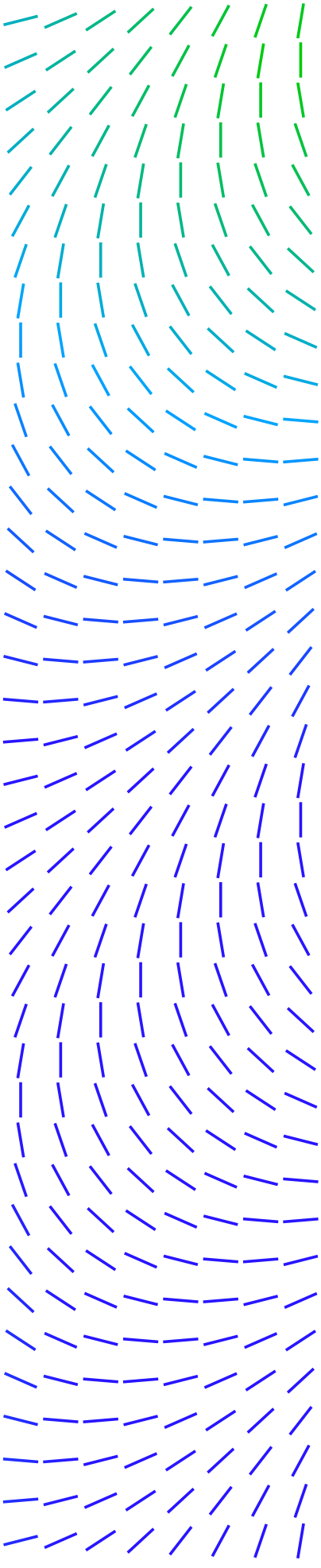
- M08 Active Directory Configuration
- M09 MDE Users
- M10 MDE Policies
- M11 Deployment Methods
- M12 Deploying MDE Software
- M13 MDE Permission Sets
- M14 Troubleshooting MDE

Day 3

- M15 Administrator Recovery
- M16 Drive Recovery
- M17 Scripting
- M18 Password Recovery Tools
- M19 MDE Dashboards and Queries
- M20 MDE Offline Activation

Day 4

- M21 Upgrading
- M22 Uninstall
- M23 File and Removable Media Protection (FRP)



Course Learning Objectives

M01 - 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 - ePO 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 the architecture and overview of ePO.

M03 - McAfee Agent

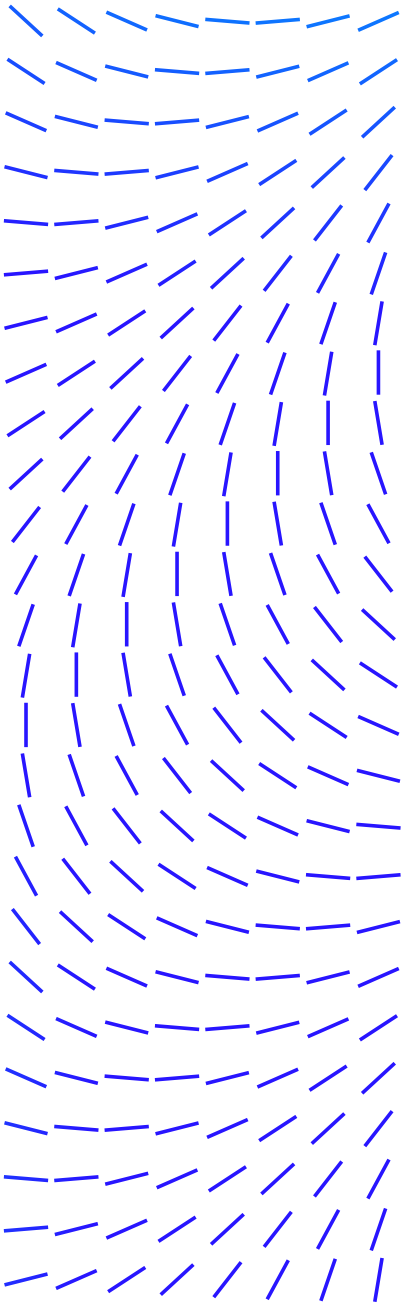
- Define the Agent and explain its purpose, key characteristics, and functions.
- Define and give examples of managed systems.
- Identify platform requirements including hardware, software, and extensions.
- Explain and give examples of Agent communications within the ePO environment.
- Identify ways to convert an Agent to a managed mode.
- Describe ways to remove an Agent.
- Explain ways to use the command line to customize an Agent installation or upgrade.
- Navigate the Agent interface.

M04 - Planning the MDE Deployment

- What is a planning overview?
- Requirements for ePO and the McAfee Agent
- Supported Microsoft Server OS for MDE
- Supported Microsoft Client OS for MDE
- Required ports

Recommended Pre-Work

- Solid knowledge of Windows and system administration, network technologies
- Solid knowledge of computer security, command line syntax, malware/anti-malware, virus/anti-virus, and web technologies
- Prior experience using ePolicy Orchestrator (ePO)



- The Tech Check
- Planning the pilot
- Change control

M05 - Encryption Technologies

- State why data at rest requires safeguarding.
- Explain the differences between disk and file encryption.
- Differentiate the features and benefits of various authentication/token options.
- Describe the computer boot process and give definitions for key computer terms used in the boot process.

M06 - MDE Overview

- Identify the key features of McAfee Drive Encryption.
- Draw a high-level MDE overview and describe the function of each component.
- Describe how key management is handled in MDE.
- Identify MDE documentation and online resources.

M07 - MDE Extensions and Packages

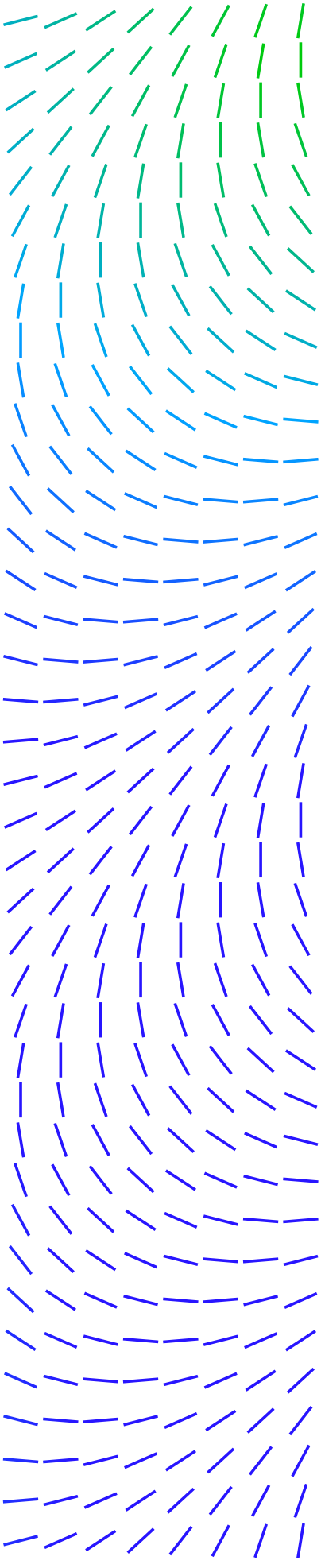
- Install extensions and check packages in EPO.
- Locate and navigate new menus used with DE.
- Install the help files and use them to locate information.
- Configure server settings.

M08 - Active Directory Configuration

- Register an LDAP server in ePO
- Configure ePO and MDE for LDAP synchronization
- Verify synchronization task

M09 - MDE Users

- Add a LDAP user in ePO and assign to a client system.
- Add LDAP group users in ePO and assign to a client system.
- Create a DE user group at the domain level for inheritance to child systems.



M10 - Drive Encryption Policies

- Differentiate between the purposes of the DE Product Setting Policy and User Based Policy
- Determine required DE user settings and configure the policy to match
- Differentiate between methods of policy assignment to a user, system, or system group and explain inher-itance
- Assign a policy to a user through a Policy Assignment Rule
- Assign a policy to a system through the System Tree
- Create an Add Local Domain User (ALDU) blacklist policy

M11 - Deployment Options

- Differentiate between the various DE deployment methods
- Perform Product deployment to client machines
- Create a client deployment task in ePO
- Perform a Wake up Agent Task

M12 - Deploying MDE to the Clients

- Deploy the DE client to Endpoint systems and verify installation and function
- Describe deployment best practice recommendations

M13 - MDE Permission Sets

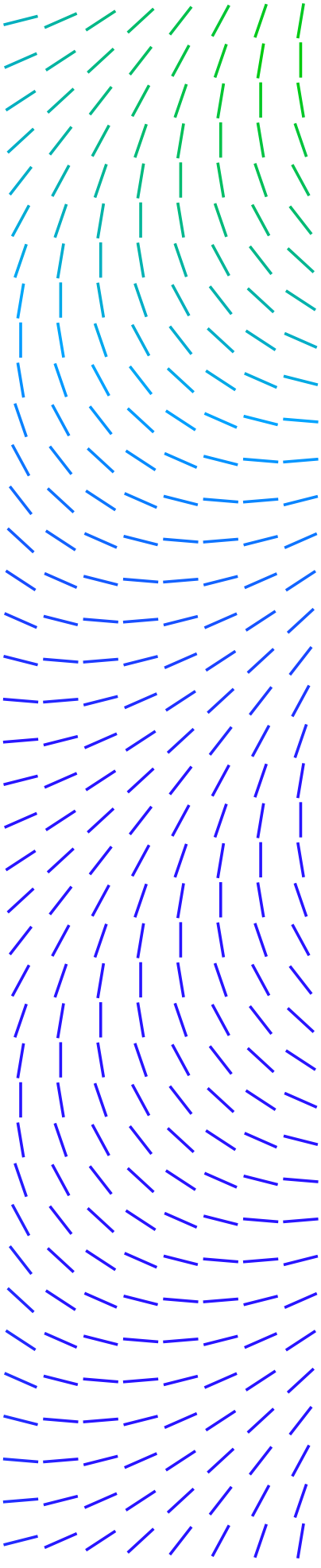
- Create and assign a DE permission set
- Create a DE Administrative User

M14 - MDE Troubleshooting Methods

- Effectively research DE issues
- Gather data for escalation
- Locate server and client logs useful to troubleshooting
- Match error codes to definitions

M15 - MDE Recovery Options

- Configure systems for self recovery
- Enable administrator recovery



M16 - Drive Recovery

- Build a DETech Recovery CD
- Build a DETech Standalone Recovery CD
- Export recovery information from ePO
- Use file or token authentication to remove encryption on a corrupt disk
- Restore a Master Boot Record.

M17 - MDE Scripting

- Install the Python Client
- Use DE Scripting to perform basic DE Administrative Tasks

M18 - Endpoint Assistant and DPSSP

- Understand Endpoint Assistant (EA)
- Use EA for DE recovery
- Understand McAfee Data Protection Self-Service Portal (DPSSP)
- Use DPSSP with DE

M19 - MDE Dashboards, Queries, and Reports

- Use the DE dashboard to view new client information
- Build new monitors for the dashboard
- Configure queries

M20 - MDE Offline Activation

- Learn the components needed for a manual install

M21 - Upgrading MDE

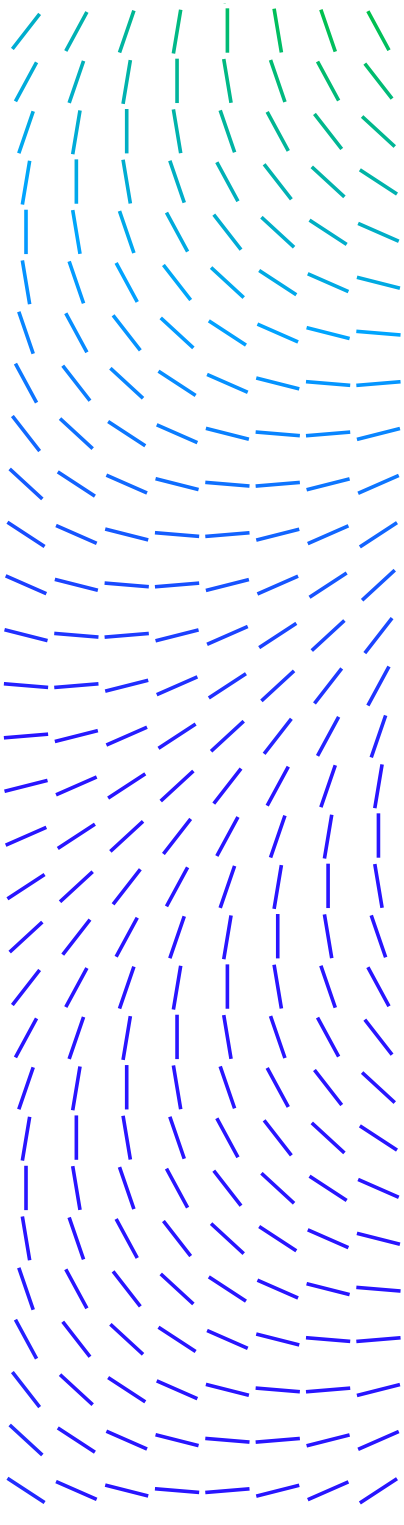
- Upgrade Drive Encryption to the current release

M22 - Deactivate and Uninstall MDE

- Deactivate and uninstall Drive Encryption from managed systems.

Related Courses

McAfee ePolicy Orchestrator Administration



DATASHEET

M23 - File and Removable Media Protection

- Describe the File and Removable Media Protection (FRP) solution
- Identify solution requirements
- Install FRP software
- Describe supported encryption key types
- Configure encryption key access
- Manage FRP keys
- Distinguish between FRP policies
- Define FRP permission sets and user controls
- View FRP dashboards and use FRP queries and reports
- Explain how Data Loss Prevention Endpoint (DLPe) uses encryption for an extra layer of control