

ManageEngine Endpoint Central MSP

Course Table of Contents

About the Course

This training equips users with the knowledge to work with Endpoint Central MSP, and covers the best practices that help you get started quickly.

Course Objectives

By the end of the course, participants will be able to:

- Automate patching for Microsoft and non-Microsoft applications
- Deploy software to users and computers
- Track hardware and software inventory and manage licenses
- Detect unauthorized software
- Remotely access and troubleshoot computers
- Restrict USB usage and apply power settings
- Configure Windows desktops and applications
- Manage mobile devices

Who Should Attend

IT managers, system administrators, and operators who have deployed Endpoint Central and want to use its systems management features to the fullest.

Course Agenda

Module 1: Introduction & Architecture

- 1.1 What is Endpoint Central MSP, and who it is for
- 1.2 MSP architecture: Server, Agents, Distribution Servers
- 1.3 Customer (client) management concept in MSP

Module 2: Installation & Server Setup

- 2.1 System requirements
- 2.2 Installing the server
- 2.3 Configuring the firewall
- 2.4 Enabling secure communication (HTTPS)
- 2.5 User and role-based access control
- 2.6 Mail server for email notifications
- 2.7 Changing server ports and communication mode

Module 3: Discovering & Onboarding Computers

- 3.1 Adding domains and workgroups
- 3.2 Adding computers to manage
- 3.3 Adding remote offices
- 3.4 Installing Distribution Servers
- 3.5 Defining IP scopes
- 3.6 Configuring agent settings

Module 4: Agent Installation

- 4.1 Installation methods: Console, Windows GPO, Script, Manual
- 4.2 Configuring the firewall on client computers (automatic and manual)
- 4.3 Ports to be opened
- 4.4 Verifying agent installation status

Module 5: Patch Management

- 5.1 Patch management workflow
- 5.2 Setting up: proxy and system health policy
- 5.3 Updating the patch database (manual, scheduled, periodic sync)
- 5.4 Identifying missing patches
- 5.5 Installing missing patches (one patch to all systems, all patches to one system)
- 5.6 Patch approval (test and approve)
- 5.7 Automatic patch deployment
- 5.8 Declining patches (exclude from missing reports)
- 5.9 Scheduling deployment and verifying status
- 5.10 Reports: Vulnerable Systems, Vulnerable Patches, Latest Patches
- 5.11 Alerts: notify when a task is complete

Module 6: Software Deployment

- 6.1 Setting up: network share
- 6.2 Adding packages: MSI, EXE, templates
- 6.3 Deploying software and scheduling
- 6.4 Pre- and post-installation tasks
- 6.5 Verifying deployment status
- 6.6 Self Service Portal

Module 7: Inventory & Asset Management

- 7.1 Scanning for assets (manual and scheduled)
- 7.2 Email alerts for scan events
- 7.3 Software metering
- 7.4 Software license management and compliance
- 7.5 Grouping similar software
- 7.6 Prohibited software
- 7.7 Reports: Software, Hardware, License Compliance, Custom

Module 8: Configurations

- 8.1 User vs. computer configurations
- 8.2 Configuration states
- 8.3 Templates and collections
- 8.4 Key configurations: security policies, custom scripts, file/folder operations, user and group management
- 8.5 Configuration status report

Module 9: Device Control & Power Management

- 9.1 Securing USB devices (enable/disable, user and computer level, device types such as Bluetooth, printer, CD-ROM, portable devices)
- 9.2 Power schemes (Green IT)
- 9.3 Shutdown, lock, standby, hibernate (manual, scheduled, group-based)
- 9.4 Wake-up of remote computers (manual, scheduled)
- 9.5 Power management report

Module 10: Remote Control & System Tools

- 10.1 Remote control settings: ports, user confirmation, connection reasons, communication mode
- 10.2 Remote session features: video recording, multi-monitor swap, blacken monitor, disable remote keyboard/mouse
- 10.3 Collaboration: chat, voice/video call, technician collaboration, shadow user
- 10.4 File transfer between computers
- 10.5 System tools: scheduling tasks, Check Disk, Clean Disk, Defragmentor, System Manager

Module 11: Mobile Device Management (MDM)

- 11.1 Setting up MDM: NAT, proxy, mail server, APNs certificate, authentication policy
- 11.2 Device enrollment: manual, bulk, Apple Configurator, Apple DEP, QR code, NFC, Windows ICD
- 11.3 Profile management: profiles, groups, association
- 11.4 App management: repository, distribution, blacklist/whitelist, silent install, AFW/VPP
- 11.5 Geo tracking, Lost Mode, location history
- 11.6 Kiosk mode (Single App Mode)
- 11.7 Remote troubleshooting
- 11.8 Security: remote wipe, corporate wipe, clear passcode, remote lock
- 11.9 MDM asset management and reports

Module 12: Reports

- 12.1 Active Directory reports
- 12.2 Scheduling and emailing reports
- 12.3 User logon reports
- 12.4 Custom reports and custom query reports

Module 13: Integrations & Help Desk

- 13.1 Integration with help desk applications (ticketing, alerts)
- 13.2 Integration with ServiceDesk Plus (workflow, asset data, software deployment, announcements and chat, full console integration)

Module 14: Audit & Administration

- [14.1](#) Auditing actions performed in Endpoint Central
- [14.2](#) Remote control audit and inventory alerts
- [14.3](#) Custom user/computer groups
- [14.4](#) Personalizing the web console
- [14.5](#) Scheduling database backup