+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 01/29/2026

Register

EPM Ivanti patching and compliance training

2 days (14 hours)

Overview

This Ivanti EPM training course teaches you how to industrialize patching and manage compliance on a Windows environment, with measurable results (risk reduction, visibility, audits). You will work on concrete use cases: patch deployment, exception management, and proof of compliance.

During this training, we cover the entire chain: inventory, vulnerability analysis, target group creation, planning, deployment, post-installation control, and remediation. The goal is to secure workstations and servers while limiting user impact (maintenance windows, reboots, rollbacks).

The approach is practical: guided workshops, administration demos, troubleshooting exercises, and dashboard building. You will leave with reusable deliverables: patching policy templates, compliance checklists, operating procedures, and sample audit reports.

Objectives

- Configure patch inventory and status collection in Ivanti EPM.
- Build patching campaigns (targeting, planning, reboots, maintenance).
- Automate remediation via tasks, scripts, and compliance rules.
- Analyze failures and troubleshoot deployments (agent, distribution, prerequisites).
- Produce compliance reports and actionable audit evidence.

Target audience

- System administrators / workstations
- Operations/support engineers N2-N3
- Security managers / GRC managers in charge of compliance
- ITSM/endpoint management tool project managers

Prerequisites

- Windows administration (services, registry, rights, logs)
- Basic network knowledge (DNS, ports, proxy, segmentation)
- Understanding of patching cycles and vulnerability risks
- Log reading and basic diagnostics

Technical prerequisites

- PC with 16 GB of RAM recommended (8 GB minimum) and 4-core CPU
- Windows 10/11 or Windows Server (local admin access)
- Access to an Ivanti EPM console (test environment) and an EPM admin account
- Tools: PowerShell, modern browser, network access to lab endpoints

EPM Ivanti patching and compliance training program

[Day 1 - Morning]

Ivanti EPM fundamentals and patch management preparation

- EPM architecture: Core Server, Agents, Console, roles, and network flows
- Hardware/software inventory: sources, frequency, data quality, and standardization
- Patching prerequisites: maintenance windows, reboots, dependencies, and business constraints
- Best practices for segmentation: groups, queries, pilot targets, and deployment rings
- Hands-on workshop: Building a segmentation (Pilot/Pre-production/Production) from the inventory.

[Day 1 - Afternoon]

Patching implementation: content, deployments, and execution control

- Patch content management: catalogs, synchronization, approval, and exclusions
- Creating patch tasks: targeting, scheduling, pre/post-actions, and restarting
- Deployment strategies: progressive, deadlines, maintenance windows, and bandwidth management
- Execution monitoring: statuses, agent logs, common errors, and remediation
- Hands-on workshop: Deploy a batch of patches to a pilot group and analyze execution feedback.

[Day 2 - Morning]

Compliance and reporting: indicators, dashboards, and audit evidence

- Defining compliance: patch levels, SLAs, exceptions, and scopes (servers/workstations)
- EPM reports: templates, filters, scheduling, and controlled distribution
- Operational KPIs: compliance rate, coverage, remediation time, and top vulnerabilities
- Traceability: history, proof of deployment, exception management, and supporting documentation
- Hands-on workshop: Produce a monthly compliance report with documented exceptions.

[Day 2 - Afternoon]

Process hardening: governance, automation, and patch incident management

- Patch governance: RACI, cycles (weekly/monthly), communication, and change validation
- Automation: rings, approval rules, recurring deployments, and prerequisite checks
- Failure management: diagnostics (agent, content, WUA, prerequisites), workarounds, and retries
- Continuous improvement: post-mortem, backlog reduction, network optimization, and standardization
- Hands-on workshop: Implementing a remediation runbook and patch automation routine.

Target companies

This training is intended for both individuals and companies, large or small, wishing to train their teams in advanced new IT technology or to acquire specific business knowledge or modern methods.

Positioning at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon final registration, the learner receives a self-assessment questionnaire that allows us to assess their estimated level of knowledge of different types of technologies, their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and discussion sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

of skills.

Certification

A certificate will be issued to each trainee who has completed the entire training course.