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

Updated on 02/09/2026

Register

# Omnissa Workspace ONE Training - Deploy and manage

ALL-IN-ONE: EXAM INCLUDED IN THE PRICE

5 days (35 hours)

## Overview

Omnissa Workspace ONE allows you to deploy, secure, and manage a fleet of devices (Windows, macOS, iOS, Android) from a unified console. The training focuses on real-world scenarios: user onboarding, compliance, application distribution, and reducing support tickets.

During this training, you will learn how to design an operational UEM strategy: enrollment, profiles, certificates, identity management, security policies, and automation of remediation actions. The focus is on production deployment: architecture choices, best practices, and user-side impact control.

The approach is practical, with guided workshops and demos: tenant creation, group configuration, app deployment, compliance rules, and reporting. You will leave with a deployment checklist, policy templates, and an operations runbook.

## Objectives

- Configure the Workspace ONE architecture and basic integrations.
- Set up enrollment and profiles by device type.
- Deploy and maintain applications, updates, and content.
- Apply compliance and security policies with remediation.
- Monitor via dashboards, reports, and operational alerts.

## Target audience

- System and workstation administrators

- Mobility/UEM engineers
- N2/N3 support teams
- Security/IAM managers (interface)

## Prerequisites

- Basic knowledge of Windows/macOS administration and networking concepts (DNS, proxy, certificates)
- Understanding of directories and authentication (AD/Azure AD, SSO)
- Basic knowledge of fleet management, application packaging, or scripts
- Security culture: encryption, compliance, hardening

## Technical prerequisites

- PC with 16 GB RAM recommended (8 GB minimum) and 4-core CPU
- OS: Windows 10/11 or recent macOS, up-to-date Chrome/Edge browser
- Access to a Workspace ONE environment (tenant/lab) and administrator rights
- Tools: PowerShell/Bash terminal, editor (VS Code), outgoing Internet access

## Omnissa Workspace ONE training program - Deploy and manage

### [Day 1 - Morning]

### Workspace ONE architecture and environment preparation

- Positioning components: Workspace ONE UEM, Access, Intelligence, and integrations
- Choose the deployment model: SaaS vs. On-Prem, network and DNS prerequisites
- Configuring admin access: roles, accounts, best practices for separating rights
- Set up the basics: Organization Group, Location Groups, global settings
- Hands-on workshop: Initialize a UEM tenant and structure the Organization Groups tree.

### [Day 1 - Afternoon]

### Onboarding devices and certificates

- Compare enrollment methods: DEP/ABM, Android Enterprise, Windows Autopilot, user enrollment
- Configure connectors: Directory Services, Email, Content Gateway as needed
- Set up a PKI: SCEP, certificates, certificate-based Wi-Fi/VPN profiles
- Validate user experience: portal, authentication, initial compliance
- Hands-on workshop: Enroll a device (iOS/Android/Windows) and deploy a Wi-Fi profile with certificate.

[Day 2 - Morning]

## Profiles, restrictions, and compliance

- Creating profiles: passcode, restrictions, VPN, email, certificates, specific payloads
- Structure targeting: Smart Groups, dynamic criteria, exclusions, and priorities
- Defining compliance rules: jailbreak/root, encryption, minimum OS, remediation deadline
- Implement actions: notification, quarantine, access withdrawal, selective deletion
- Hands-on workshop: Build a compliance policy and apply automatic remediation.

[Day 2 - Afternoon]

## Application and content management

- Publish applications: public, internal, VPP/Managed Play, MSI/Win32
- Manage the lifecycle: versions, progressive deployment, dependencies, uninstallation
- Configure managed apps: app configuration, permissions, per-app VPN
- Distributing content: Content Locker, repositories, access policies, and synchronization
- Hands-on workshop: Deploy a managed application with configuration and targeting by Smart Group.

[Day 3 - Morning]

## Security, conditional access, and device posture

- Implement conditional access: Microsoft Entra ID/O365 integration and posture rules
- Configuring security policies: encryption, firewalls, OS restrictions, data protection
- Managing identities and authentication: SSO, certificates, factors, policies by population
- Automating response: locking, wiping, certificate rotation, compliance-based actions
- Hands-on workshop: Enable a conditional access scenario based on UEM compliance.

[Day 3 - Afternoon]

## Monitoring, logs, and operational troubleshooting

- Reading key indicators: enrollments, compliance, service health, deployment errors
- Leveraging logs: UEM console, device events, diagnostics, and agent-side traces
- Resolving common incidents: profiles not applied, failed apps, expired certificates, APNs push
- Set up dashboards and exports for N1/N2 support

- Hands-on workshop: Diagnosing an application deployment failure and correcting the cause.

## [Day 4 - Morning]

### Windows management: profiles, patching, and scripts

- Configure Windows management: MDM, configuration profiles, policies, and baselines
- Deploy Windows applications: Win32, MSI, detection rules, and requirements
- Automating with scripts: PowerShell, execution, status feedback, logging
- Managing updates: policies, rings, restarts, and maintenance windows
- Hands-on workshop: Deploy a Win32 app with a post-install PowerShell script and detection rule.

## [Day 4 - Afternoon]

### Industrialization: templates, multi-environments, and governance

- Standardize: profile templates, nomenclature, tags, operating documentation
- Organizing multiple populations: groups, OGs, delegation, and separation of scopes
- Implementing a change process: validation, pilots, progressive deployment, rollback
- Securing administration: roles, auditing, best practices for least privilege
- Practical workshop: Build a pilot->production deployment plan with a rollback strategy.

## [Day 5 - Morning]

### Automation and API Workspace ONE UEM

- Understanding API uses: inventory, compliance, deployments, device operations
- Setting up authentication: API keys, service accounts, scopes, and security
- Performing common operations: device search, profile push, remote actions
- Industrialize: automation scripts, scheduling, error handling, and logs
- Hands-on workshop: Write a PowerShell script calling the UEM API to list non-compliant devices.

## [Day 5 - Afternoon]

### Closing: runbook, KPIs, and production launch

- Define a runbook: enrollment procedures, support, escalation, incident management
- Set up KPIs: enrollment rate, compliance, deployment success, MTTR

- Prepare for production: checklist, user communication, support training
- Plan for continuous improvement: monthly reviews, hardening, object cleanup
- Hands-on workshop: Produce an operations runbook and a go-live checklist.

## Companies involved

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

## Placement at the start of training

The placement test at the start of the training course complies with Qualiopi quality criteria. Once they have finalized their registration, learners receive a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training course, 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 reflection sessions, and group work.

## Validation

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

## Certification

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