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

Mis à jour le 09/02/2026

S'inscrire

Formation Omnissa Workspace ONE - Deploy and manage

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Omnissa Workspace ONE permet de déployer, sécuriser et administrer un parc de terminaux (Windows, macOS, iOS, Android) depuis une console unifiée. La formation cible des cas concrets : onboarding utilisateur, conformité, distribution d'applications et réduction des tickets support.

lors de cette formation, vous apprendrez à concevoir une stratégie UEM opérationnelle : enrôlement, profils, certificats, gestion des identités, politiques de sécurité et automatisation des actions de remédiation. L'accent est mis sur la mise en production : choix d'architecture, bonnes pratiques et contrôle des impacts côté utilisateur.

L'approche est pratique avec ateliers guidés et démos : création d'un tenant, configuration des groupes, déploiement d'apps, règles de conformité et reporting. En livrables, vous repartez avec une checklist de déploiement, des modèles de politiques et un runbook d'exploitation.

Objectifs

- Configurer l'architecture Workspace ONE et les intégrations de base.
- Mettre en place l'enrôlement et les profils par type de terminal.
- Déployer et maintenir applications, mises à jour et contenus.
- Appliquer des politiques de conformité et de sécurité avec remédiation.
- Superviser via tableaux de bord, rapports et alertes opérationnelles.

Public visé

- Administrateurs systèmes et postes de travail

- Ingénieurs mobilité / UEM
- Équipes support N2/N3
- Responsables sécurité / IAM (en interface)

Pré-requis

- Bases d’administration Windows/macOS et notions réseaux (DNS, proxy, certificats)
- Compréhension des annuaires et de l’authentification (AD/Azure AD, SSO)
- Notions de gestion de parc, packaging applicatif ou scripts
- Culture sécurité : chiffrement, conformité, durcissement

Pré-requis techniques

- PC avec 16 Go RAM recommandés (8 Go minimum) et CPU 4 cœurs
- OS : Windows 10/11 ou macOS récent, navigateur Chrome/Edge à jour
- Accès à un environnement Workspace ONE (tenant/lab) et droits administrateur
- Outils : terminal PowerShell/Bash, éditeur (VS Code), accès Internet sortant

Programme de formation Omnissa Workspace ONE - Deploy and manage

[Jour 1 - Matin]

Architecture Workspace ONE et préparation de l’environnement

- Positionner les composants : Workspace ONE UEM, Access, Intelligence et intégrations
- Choisir le modèle de déploiement : SaaS vs On-Prem, prérequis réseau et DNS
- Configurer les accès admin : rôles, comptes, bonnes pratiques de séparation des droits
- Mettre en place les bases : Organization Group, Location Groups, paramètres globaux
- Atelier pratique : Initialiser un tenant UEM et structurer l’arborescence Organization Groups.

[Jour 1 - Après-midi]

Onboarding des terminaux et certificats

- Comparer les méthodes d’enrôlement : DEP/ABM, Android Enterprise, Windows Autopilot, enrollment utilisateur
- Configurer les connecteurs : Directory Services, Email, Content Gateway selon le besoin
- Mettre en place une PKI : SCEP, certificats, profils Wi-Fi/VPN basés certificats
- Valider l’expérience utilisateur : portail, authentification, conformité initiale
- Atelier pratique : Enrôler un appareil (iOS/Android/Windows) et déployer un profil Wi-Fi avec certificat.

[Jour 2 - Matin]

Profils, restrictions et conformité

- Créer des profils : passcode, restrictions, VPN, email, certificats, payloads spécifiques
- Structurer le ciblage : Smart Groups, critères dynamiques, exclusions et priorités
- Définir des règles de conformité : jailbreak/root, chiffrement, OS minimum, délai de remédiation
- Mettre en œuvre des actions : notification, quarantaine, retrait d'accès, suppression sélective
- Atelier pratique : Construire une politique de conformité et appliquer une remédiation automatique.

[Jour 2 - Après-midi]

Gestion des applications et du contenu

- Publier des applications : public, internes, VPP/Managed Play, MSI/Win32
- Gérer le cycle de vie : versions, déploiement progressif, dépendances, désinstallation
- Configurer les apps managées : app configuration, permissions, per-app VPN
- Distribuer du contenu : Content Locker, dépôts, politiques d'accès et synchronisation
- Atelier pratique : Déployer une application managée avec configuration et ciblage par Smart Group.

[Jour 3 - Matin]

Sécurité, accès conditionnel et posture device

- Mettre en place l'accès conditionnel : intégration Microsoft Entra ID / O365 et règles de posture
- Configurer les politiques de sécurité : chiffrement, pare-feu, restrictions OS, protection des données
- Gérer les identités et l'authentification : SSO, certificats, facteurs, politiques par population
- Automatiser la réponse : verrouillage, effacement, rotation certificats, actions basées conformité
- Atelier pratique : Activer un scénario d'accès conditionnel basé sur la conformité UEM.

[Jour 3 - Après-midi]

Supervision, logs et dépannage opérationnel

- Lire les indicateurs clés : enrôlements, conformité, santé des services, erreurs de déploiement
- Exploiter les journaux : console UEM, événements device, diagnostics et traces côté agent
- Résoudre les incidents courants : profils non appliqués, apps en échec, certificats expirés, push APNs
- Mettre en place des tableaux de bord et exports pour le support N1/N2

- Atelier pratique : Diagnostiquer un échec de déploiement d’application et corriger la cause.

[Jour 4 - Matin]

Gestion Windows : profils, patching et scripts

- Configurer Windows management : MDM, profils de configuration, policies et baselines
- Déployer des applications Windows : Win32, MSI, règles de détection et exigences
- Automatiser avec scripts : PowerShell, exécution, retour de statut, journalisation
- Gérer mises à jour : stratégies, anneaux, redémarrages et fenêtres de maintenance
- Atelier pratique : Déployer une app Win32 avec script PowerShell de post-install et règle de détection.

[Jour 4 - Après-midi]

Industrialisation : templates, multi-environnements et gouvernance

- Standardiser : modèles de profils, nomenclature, tags, documentation d’exploitation
- Organiser multi-populations : groupes, OG, délégation et séparation des périmètres
- Mettre en place un processus de changement : validation, pilotes, déploiement progressif, rollback
- Sécuriser l’administration : rôles, audit, bonnes pratiques de moindre privilège
- Atelier pratique : Construire un plan de déploiement pilote->prod avec stratégie de rollback.

[Jour 5 - Matin]

Automatisation et API Workspace ONE UEM

- Comprendre les usages API : inventaire, conformité, déploiements, opérations device
- Mettre en place l’authentification : clés API, comptes de service, périmètres et sécurité
- Exécuter des opérations courantes : recherche device, push profile, remote actions
- Industrialiser : scripts d’automatisation, planification, gestion des erreurs et logs
- Atelier pratique : Écrire un script PowerShell appelant l’API UEM pour lister les devices non conformes.

[Jour 5 - Après-midi]

Clôture : runbook, KPI et mise en production

- Définir un runbook : procédures d’enrôlement, support, escalade, gestion incidents
- Mettre en place des KPI : taux d’enrôlement, conformité, succès de déploiement, MTTR

- Préparer la mise en production : check-list, communication utilisateurs, formation support
- Planifier l’amélioration continue : revues mensuelles, durcissement, nettoyage des objets
- Atelier pratique : Produire un runbook d’exploitation et une check-list de go-live.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2026. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg