MD-102

Microsoft 365 Endpoint Administrator

Durée : 5 jours, 35 heures | Niveau : intermédiaire

Référence	MD-102
Domaine	Microsoft 365 : gestion et sécurisation des terminaux avec Microsoft Intune
Certification	Prépare à l'examen MD-102 (Microsoft 365 Certified: Endpoint Administrator Associate), passage de l'examen en option

Présentation de la formation

Les appareils des collaborateurs, qu'il s'agisse de PC Windows, de Mac, de smartphones ou de tablettes, sont la première porte d'entrée vers les données de l'entreprise. L'administrateur de points de terminaison déploie, configure, sécurise, gère et supervise ces appareils et leurs applications, avec Microsoft Intune comme plateforme de gestion unifiée.

Cette formation de cinq jours apprend à planifier et à mettre en œuvre une stratégie complète de gestion des terminaux : jonction et inscription des appareils dans Microsoft Entra ID, enrôlement dans Intune, déploiement de Windows avec Windows Autopilot, profils de configuration, protection avec Microsoft Defender for Endpoint, gestion des mises à jour, déploiement et protection des applications, puis automatisation et supervision.

Le programme suit les domaines de compétences publiés par Microsoft pour l'examen MD-102 et prépare directement à cette certification.

Objectifs pédagogiques

À l'issue de la formation, les participants seront capables de :

- Joindre et inscrire des appareils dans Microsoft Entra ID, puis les enrôler dans Microsoft Intune (Windows, macOS, iOS, iPadOS et Android).
- Gérer l'identité et l'accès : rôles, administration déléguée, stratégies de conformité, accès conditionnel, Windows Hello Entreprise et Windows LAPS.
- Déployer et mettre à niveau Windows avec Windows Autopilot et Intune, et provisionner des Cloud PC Windows 365.
- Créer et cibler des profils de configuration pour toutes les plateformes prises en charge.
- Mettre en œuvre les fonctionnalités de la suite Intune : gestion des privilèges des points de terminaison, assistance à distance, Cloud PKI et Microsoft Tunnel.
- Protéger les terminaux : antivirus, chiffrement, pare-feu, réduction de la surface d'attaque, bases de référence de sécurité et Microsoft Defender for Endpoint.
- Gérer les mises à jour des appareils avec les anneaux de mise à jour, Windows Autopatch et Hotpatch.
- Déployer et protéger les applications : Win32, applications métier, Microsoft Store, Microsoft 365 Apps, protection et configuration des applications.
- Automatiser avec PowerShell et Microsoft Graph, et superviser la santé des terminaux avec les rapports et Endpoint Analytics.

Public concerné

Cette formation s'adresse notamment aux :

- Administrateurs de points de terminaison Microsoft 365 chargés du déploiement, de la configuration, de la sécurisation et de la supervision des appareils et des applications clientes.
- Administrateurs Microsoft 365 et administrateurs systèmes souhaitant maîtriser Intune.
- Techniciens et ingénieurs support évoluant vers la gestion moderne des postes de travail.

Prérequis

Pour suivre la formation dans de bonnes conditions, il est recommandé de disposer :

- D'une familiarité avec Microsoft Entra ID et les charges de travail Microsoft 365.
- D'une expérience solide du déploiement, de la configuration et de la maintenance d'appareils Windows 11 et non-Windows.

Programme détaillé

Le programme suit les cinq domaines de compétences de l'examen MD-102.

Jour 1 : Infrastructure des appareils, identité et conformité

Module 1 : Préparer l'infrastructure des appareils

- Choix du type de jonction (inscription ou jonction Microsoft Entra) et mise en œuvre.
- Groupes d'appareils dans Microsoft Entra ID, règles d'appartenance dynamique.
- Paramètres d'inscription Intune et inscription automatique de Windows.
- Inscription personnelle macOS, iOS et iPadOS.
- Profils d'inscription Android : entièrement géré, dédié, propriété de l'entreprise avec profil professionnel, restrictions et résolution des échecs d'inscription.
- Inscription d'entreprise via Apple Business Manager, Samsung Knox Mobile Enrollment et Google zero-touch.

Module 2 : Identité, accès et conformité

- Rôles intégrés et personnalisés pour Intune et Windows 365, étiquettes d'étendue et administration déléguée.
- Approbation multi-administrateurs.
- Stratégies de conformité pour toutes les plateformes et accès conditionnel exigeant un appareil conforme.
- Windows Hello Entreprise et Windows LAPS avec Intune et Microsoft Entra ID.
- Gestion de l'appartenance aux groupes locaux Windows avec Intune.

Jour 2 : Déploiement de Windows et profils de configuration

Module 3 : Déployer et mettre à niveau Windows avec les outils cloud

- Windows Autopilot : profils de déploiement ou stratégies de préparation d'appareil, modes pilotés par l'utilisateur, pré-approvisionnement et autodéploiement.
- Modèle de nom d'appareil et page d'état d'inscription (ESP).
- Planification et mise en œuvre des mises à niveau vers Windows 11 avec Intune.
- Provisionnement et configuration de Cloud PC Windows 365 : stratégies d'approvisionnement, connexions réseau et gestion des images.
- Sauvegarde Windows (Windows Backup) avec Intune.

Module 4 : Profils de configuration des appareils

- Profils pour Windows, avec import de fichiers ADMX et analyse des stratégies de groupe (Group Policy analytics).
- Profils pour Android, iOS, iPadOS et macOS.

- Profils pour appareils spécialisés : Microsoft Teams Rooms, HoloLens 2 et Zebra.
- Ciblage des profils avec des filtres d'affectation et le regroupement au moment de l'inscription.

Jour 3 : Suite Intune, actions à distance et sécurité des terminaux

Module 5 : Fonctionnalités de la suite Intune

- Gestion des privilèges des points de terminaison (EPM) : stratégies d'élévation et suivi des actions élevées.
- Enterprise App Catalog et assistance à distance (Remote Help).
- Microsoft Cloud PKI : mise en place, émission automatisée des certificats et suivi de leur état.
- Microsoft Tunnel pour la gestion des applications mobiles (MAM).
- Intune Advanced Analytics : détection d'anomalies, informations proactives et recommandations de stratégies basées sur le risque.

Module 6 : Actions à distance et diagnostic

- Synchronisation, redémarrage, mise hors service et effacement d'appareils, y compris en masse.
- Mise à jour des renseignements de sécurité de Microsoft Defender Antivirus.
- Rotation des clés de récupération BitLocker et des mots de passe d'administrateur local.
- Requêtes sur les appareils avec KQL.
- Collecte des diagnostics et des journaux, panneau de dépannage utilisateur.

Module 7 : Sécurité des terminaux

- Stratégies antivirus, de pare-feu et de chiffrement de disque (clés de récupération BitLocker, libre-service, conformité du chiffrement).
- Réduction de la surface d'attaque selon les principes Zero Trust.
- Bases de référence de sécurité avec Intune.
- Intégration d'Intune à Microsoft Defender for Endpoint : intégration des appareils, stratégies EDR, investigation des menaces et tri des incidents.
- Stratégies App Control for Business.

Jour 4 : Mises à jour et applications

Module 8 : Gestion des mises à jour des appareils

- Planification des mises à jour avec Intune.
- Anneaux de mise à jour, mises à jour de fonctionnalités et de qualité pour Windows.
- Windows Autopatch et stratégies Hotpatch.
- Mises à jour iOS, iPadOS et macOS avec le catalogue de paramètres, mises à jour Android par profils ou FOTA.
- Optimisation de la distribution (Delivery Optimization) et suivi des mises à jour.

Module 9 : Déployer et mettre à jour les applications

- Préparation et déploiement d'applications : Win32, applications métier et Microsoft Store.
- Stratégies de plages de silence (Quiet Time) pour les applications Android et iOS.
- Déploiement et gestion de Microsoft 365 Apps avec Intune, l'Office Deployment Tool et le centre d'administration Microsoft 365 Apps, y compris dans un déploiement Autopilot.
- Applications des magasins de plateformes : Apple Business Manager et Managed Google Play.
- Suivi des déploiements et résolution des échecs d'installation.

Module 10 : Protection et configuration des applications

- Stratégies de protection des applications pour les appareils gérés et non gérés (BYOD).
- Accès conditionnel pour la protection des applications.
- Stratégies de configuration des applications pour les applications et appareils gérés.

Jour 5 : Automatisation, supervision et préparation à l'examen

Module 11 : Automatiser les tâches de gestion

- Automatisation des tâches Intune avec PowerShell et Microsoft Graph.
- Extension de la conformité des appareils avec PowerShell.
- Agents Security Copilot dans Intune : investigation des menaces, analyse des performances des appareils et recommandations.

Module 12 : Superviser et optimiser la santé des terminaux

- Rapports et visibilité des données dans Intune : rapports personnalisés, classeurs, tableaux de bord et exports.
- Endpoint Analytics : scores de santé, performances de démarrage, fiabilité et expérience utilisateur.
- Scripts de correction (Remediations) : détection et résolution des problèmes courants, planification.
- Santé du tenant et communications du service Intune.
- Alertes et notifications : dérive de conformité, échecs d'inscription et conflits de configuration.

Révision et préparation à l'examen

- Synthèse des points clés des cinq domaines et conseils pour l'examen MD-102.

Méthodes pédagogiques

- Apports théoriques structurés alternant avec des mises en application immédiates.
- Démonstrations guidées dans Microsoft Intune, Microsoft Entra ID et Microsoft Defender.
- Mises en pratique sur des scénarios représentatifs d'un parc d'appareils en entreprise.
- Échanges avec le formateur autour des cas rencontrés en environnement de production.

Évaluation des acquis

Les acquis sont évalués tout au long de la session à travers des questions, des mises en pratique, des quiz et des mises en situation en lien avec les thèmes étudiés. Une évaluation de synthèse en fin de formation permet de vérifier la compréhension des notions essentielles et de repérer les points nécessitant un approfondissement.

Encadrement

La formation est animée par un formateur expert de la gestion des terminaux Microsoft, disposant d'une expérience opérationnelle sur Microsoft Intune, Microsoft Entra ID et la sécurité des postes de travail. L'accompagnement pédagogique s'appuie sur des démonstrations, des retours d'expérience et des mises en pratique adaptées aux objectifs de la session.

Certification et examen

La formation prépare à l'examen MD-102 : Endpoint Administrator, qui donne accès à la certification Microsoft 365 Certified: Endpoint Administrator Associate. Le passage de l'examen est optionnel et n'est pas inclus dans le tarif de la formation.