Smartfuture
Certifications | Training | Technology solutions

Formation & Certification • MD-102

# Administrateur de points de terminaison

La formation MD-102 forme les participants à gérer et sécuriser les terminaux avec Microsoft Endpoint Manager (Intune), en couvrant la gestion des identités, la conformité, le déploiement et la maintenance des appareils, la gestion des applications et la sécurité des points de terminaison.

Distributeur officiel Certiport

Cetre d'examen Certiport

Learn • Practice • Certify

**Durée**
5 jours
(35 heures)

**Examen**
MD-102

**Modalité**
Présentiel &
Distanciel à la
demande

**Niveau**
Administrateur
Intermédiaire

**INSCRIPTION / RÉSERVATION**

Je m'inscris maintenant

## OBJECTIFS PÉDAGOGIQUES

- Former les participants à gérer efficacement les dispositifs informatiques d'une organisation.
- Comprendre les bases des terminaux, leur cycle de vie et leurs enjeux de sécurité.
- Déployer, configurer, sécuriser et superviser les appareils avec Microsoft Intune.
- Ajouter références (notes, bibliographies, tables des matières).
- Diagnostiquer et résoudre les problèmes liés aux appareils, applications et conformité.

## PUBLIC CIBLE

- Administrateurs IT/Gestionnaires des systèmes d'information/Ingénieurs de sécurité.
- Toute personne responsable de la gestion et de la protection des dispositifs client dans un environnement Microsoft.

## PRÉREQUIS

- Connaissance de base des services Microsoft 365.
- Expérience dans la gestion des systèmes d'exploitation Windows.
- Familiarité avec les principes de sécurité des systèmes.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

**Préparer l'infrastructure pour des appareils**

- Ajouter des appareils à Microsoft Entra ID.
- Choisir un type de jonction d'appareil approprié.
- Joindre des appareils à Microsoft Entra ID.
- Inscrire des appareils à Microsoft Entra ID.
- Planifier et implémenter des groupes pour des appareils dans Microsoft Entra ID.
- Inscrire les appareils à Microsoft Intune.
- Configurer les paramètres d'inscription.
- Configurer l'inscription automatique pour Windows et l'inscription en bloc pour iOS et Android.
- Configurer des profils d'inscription pour des appareils Android, notamment des profils d'appareils complètement managés, dédiés, appartenant à l'entreprise et professionnels.

**Implémenter l'identité et la conformité**

- Gérer les rôles dans Intune.
- Implémenter des stratégies de conformité pour toutes les plateformes d'appareils prises en charge à l'aide d'Intune.
- Implémenter des stratégies d'accès conditionnel qui nécessitent un état de conformité.
- Configurer Windows Hello Entreprise.
- Implémenter et gérer la Solution de mot de passe d'administrateur local (LAPS) pour Microsoft Entra ID.
- Gérer l'appartenance de groupes locaux sur des appareils Windows en utilisant Intune.

**Effectuer la gestion et la maintenance d'appareils**

- Déployer et mettre à niveau des clients Windows à l'aide d'outils basés sur le cloud.
- Choisir entre Windows Autopilot et les packages d'approvisionnement.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Choisir un mode de déploiement Windows Autopilot.
- Appliquer un modèle de nom d'appareil.
- Implémenter un déploiement de clients Windows avec Windows Autopilot.
- Créer une page d'état de l'inscription (ESP, Enrollment Status Page).
- Planifier et implémenter des packages d'approvisionnement.
- Planifier et implémenter des mises à niveau d'appareils pour Windows 11.
- Implémenter un déploiement de Windows 365 PC Cloud.
- Planifier et implémenter des profils de configuration d'appareil.
- Créer des profils de configuration d'appareil pour des appareils Windows, notamment en important des fichiers ADMX.
- Créer des profils de configuration d'appareil pour des appareils Android.
- Créer des profils de configuration d'appareil pour des appareils iOS.
- Créer des profils de configuration d'appareil pour des appareils Mac OS.
- Créer des profils de configuration d'appareil pour des appareils multisessions d'entreprise.
- Cibler un profil à l'aide de filtres.
- Implémenter les fonctionnalités du module complémentaire Intune Suite.
- Configurer la Gestion des privilèges de points de terminaison.
- Gérer les applications à l'aide du Catalogue d'applications d'entreprise.
- Implémenter Analyses avancées Microsoft Intune.
- Configurer l'Assistance à distance Microsoft Intune.
- Identifier les cas d'usage de PKI cloud.
- Implémenter Microsoft Tunnel pour la gestion des applications mobiles.
- Effectuer des actions à distance sur des appareils.
- Synchroniser, redémarrer, mettre hors service ou effacer des appareils.
- Effectuer des actions distantes en bloc.
- Mettre à jour la veille de sécurité Windows Defender.
- Permuter des clés de récupération BitLocker.
- Exécuter une requête sur l'appareil à l'aide de KQL.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

## Gérer les applications

### Déployer et mettre à jour des applications

- Préparer des applications pour le déploiement à l'aide d'Intune.
- Déployer des applications en utilisant Intune.
- Déployer des applications Microsoft 365 en utilisant Intune.
- Configurer des stratégies pour les applications Office.
- Déployer Microsoft 365 Apps dans le cadre d'un déploiement Windows Autopilot à l'aide de l'outil Déploiement d'Office (ODT) ou de l'Outil de personnalisation Office (OPO).
- Gérer les applications Microsoft 365 en utilisant le Centre d'administration des applications Microsoft 365.
- Déployer des applications à partir de magasins d'applications propres à la plateforme à l'aide d'Intune.

### Planifier et implémenter des stratégies de protection et de configuration des applications

- Planifier et implémenter des stratégies de protection d'applications.
- Implémenter des stratégies d'accès conditionnel pour les stratégies de protection des applications.
- Planifier et implémenter des stratégies de configuration d'application pour les applications managées et les appareils managés.

## Protéger des appareils

### Configurer la sécurité des points de terminaison

- Créer des stratégies antivirus.
- Créer des stratégies de chiffrement de disque.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Créer des stratégies de pare-feu.
- Configurer des stratégies de réduction de la surface d'attaque.
- Planifier et implémenter des bases de référence de sécurité.
- Intégrer Intune à Microsoft Defender for Endpoint.
- Intégrer des appareils dans Microsoft Defender for Endpoint.

**Gérer les mises à jour d'appareils à l'aide d'Intune**

- Planifier les mises à jour des appareils.
- Créer et gérer des boucles de mise à jour en utilisant Intune.
- Créer et gérer des stratégies de mise à jour à l'aide d'Intune, y compris pour iOS et Mac OS.
- Gérer les mises à jour d'Android à l'aide de profils de configuration ou de déploiements FOTA (firmware-over-the-air).
- Configurer l'optimisation de la distribution de clients Windows en utilisant Intune.
- Superviser les mises à jour.