

# Microsoft Office 365 Administration

**Prix :** 2 995 €HT

**Durée :** 5 jours

**Code de Référence :** MS102

Catalogue Office 365

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour utiliser les éléments clés de l'administration de Microsoft 365 : Gestion des locataires Microsoft 365, Synchronisation des identités Microsoft 365 et Sécurité et conformité Microsoft 365. Les participants à cette formation apprendront à penser, mettre en œuvre et administrer Microsoft 365 pour répondre aux besoins de leur organisation. Cette formation MS102 remplace les cours MS100 et MS101 à compter du 1er juillet 2023.

**Elle permet de préparer la certification Microsoft MS-102 Microsoft 365 Certified Enterprise Administrator Expert.**

## Objectifs de la formation

A l'issue de cette formation Microsoft, vous serez capable de :

- Savoir configurer les locataires Microsoft 365, y compris le profil organisationnel, les options d'abonnement, les services de composants, les comptes d'utilisateurs et les licences, les groupes de sécurité et les rôles administratifs
- Pouvoir planifier et implémenter le déploiement de Microsoft 365 Apps for Enterprise
- Planifier et à mettre en œuvre chacune des options de synchronisation d'annuaire
- Gérer les identités synchronisées et mettre en œuvre la gestion des mots de passe dans Microsoft 365 à l'aide de l'authentification multifactorielle
- Garantir la sécurité de Microsoft 365 avec Exchange Online Protection, Safe Attachments et Safe Links
- Comprendre comment gérer la sécurité des clients (Microsoft 365 Defender, Microsoft Defender for Cloud Apps et Microsoft Defender for Endpoint)
- Comprendre la gestion de la conformité dans Microsoft 365 notamment autour de la gouvernance des données

## Public

Cette formation Microsoft 365 Administrator Essentials s'adresse aux Administrateurs Microsoft 365

## Prérequis

Les participants doivent commencer ce cours avec les compétences suivantes :

Avoir suivi une formation d'administrateur basé sur les rôles, tel que Messagerie, Travail d'équipe, Sécurité, Conformité ou Collaboration

Posséder une compréhension du DNS et une expérience pratique avec les services Microsoft 365

Posséder une compréhension approfondie des pratiques informatiques générales

Avoir une connaissance pratique de PowerShell

Compréhension de l'anglais et du vocabulaire anglais spécifique IT.

Vous souhaitez faire vérifier vos prérequis ? Contactez-nous pour l'organisation d'un entretien téléphonique avec un de nos consultants formateurs.

## Programme de la formation

### Configurer votre expérience Microsoft 365

- Introduction
- Configurer votre expérience Microsoft 365
- Gérer vos abonnements client dans Microsoft 365
- Intégrer Microsoft 365 aux applications d'engagement client
- Terminer la configuration de votre client dans Microsoft 365

### Gérer les utilisateurs, les licences et les contacts de messagerie dans Microsoft 365

- Introduction
- Déterminer le modèle d'identité utilisateur pour votre organisation
- Créer des comptes d'utilisateurs dans Microsoft 365
- Gérer les paramètres de compte d'utilisateur dans Microsoft 365
- Gérer les licences utilisateur dans Microsoft 365
- Récupérer des comptes d'utilisateurs supprimés dans Microsoft 365
- Effectuer une maintenance utilisateur en bloc dans Azure Active Directory
- Créer et gérer des utilisateurs invités
- Créer et gérer des contacts de messagerie

### Gérer des groupes dans Microsoft 365

- Introduction
- Examiner des groupes dans Microsoft 365
- Créer et gérer des groupes dans Microsoft 365
- Créer des groupes dynamiques à l'aide du Générateur de règles Azure
- Créer une stratégie d'appellation de groupe Microsoft 365
- Créer des groupes dans Exchange Online et SharePoint Online

### Ajouter un domaine personnalisé dans Microsoft 365

- Introduction
- Planifier un domaine personnalisé pour votre déploiement Microsoft 365
- Planifier les zones DNS pour un domaine personnalisé
- Planifier les exigences en matière d'enregistrement DNS pour un domaine personnalisé
- Créer un domaine personnalisé dans Microsoft 365

### Configurer la connectivité client à Microsoft 365

- Introduction
- Examiner le fonctionnement de la configuration automatique du client

- Explorer les enregistrements DNS requis pour la configuration du client
- Configurer les clients Outlook
- Résoudre les problèmes de connectivité client

## **Configurer des rôles administratifs dans Microsoft 365**

- Introduction
- Explorer le modèle d'autorisation Microsoft 365
- Explorer les rôles d'administrateur Microsoft 365
- Attribuer des rôles d'administrateur aux utilisateurs dans Microsoft 365
- Déléguer des rôles d'administrateur à des partenaires
- Gérer les autorisations à l'aide d'unités administratives dans Azure Active Directory
- Élever les privilèges à l'aide d'Azure AD Privileged Identity Management

## **Gérer l'intégrité et les services des locataires dans Microsoft 365**

- Introduction
- Surveiller l'intégrité des services Microsoft 365
- Surveiller l'intégrité des locataires à l'aide du score d'adoption Microsoft 365
- Surveiller l'intégrité des locataires à l'aide de l'analyse de l'utilisation de Microsoft 365
- Élaborer un plan d'intervention en cas d'incident
- Demander de l'aide à Microsoft

## **Déployer des applications Microsoft 365 pour les entreprises**

- Introduction
- Explorer les fonctionnalités des applications Microsoft 365 pour les entreprises
- Explorer la compatibilité de votre application à l'aide de Readiness Toolkit
- Effectuer une installation en libre-service de Microsoft 365 Apps for enterprise
- Déployer Microsoft 365 Apps for enterprise avec Microsoft Configuration Manager
- Déployer Microsoft 365 Apps for enterprise à partir du cloud
- Déployer Microsoft 365 Apps for enterprise à partir d'une source locale
- Gérer les mises à jour des applications Microsoft 365 pour les entreprises
- Explorer les canaux de mise à jour pour Microsoft 365 Apps for enterprise
- Gérer vos applications cloud à l'aide du Centre d'administration Applications Microsoft 365

## **Analyser les données d'espace de travail Microsoft 365 à l'aide de Microsoft Viva Insights**

- Introduction
- Examiner les fonctionnalités analytiques de Microsoft Viva Insights
- Créer une analyse personnalisée avec Microsoft Viva Insights
- Configurer Microsoft Viva Insights
- Examiner les sources de données Microsoft 365 utilisées dans Microsoft Viva Insights
- Préparer les données organisationnelles dans Microsoft Viva Insights

## **Explorer la synchronisation des identités**

- Introduction
- Examiner les modèles d'identité pour Microsoft
- Examiner les options d'authentification pour le modèle d'identité hybride
- Explorer la synchronisation d'annuaires

## **Préparer la synchronisation d'identité avec Microsoft 365**

- Introduction
- Planifier votre déploiement Azure Active Directory
- Préparer la synchronisation d'annuaires
- Choisir votre outil de synchronisation d'annuaires
- Planifier la synchronisation d'annuaires à l'aide d'Azure AD Connect
- Planifier la synchronisation d'annuaires à l'aide d'Azure AD Connect Cloud Sync

### **Mettre en œuvre des outils de synchronisation d'annuaires**

- Introduction
- Configurer les composants requis pour Azure AD Connect
- Configurer Azure AD Connect
- Surveiller les services de synchronisation à l'aide d'Azure AD Connect Health
- Configurer les conditions préalables pour Azure AD Connect Cloud Sync
- Configurer Azure AD Connect Cloud Sync

### **Gérer les identités synchronisées**

- Introduction
- Gérer les utilisateurs avec la synchronisation d'annuaires
- Gérer les groupes avec la synchronisation d'annuaires
- Utiliser les groupes de sécurité de synchronisation Azure AD Connect pour gérer la synchronisation d'annuaires
- Configurer des filtres d'objets pour la synchronisation d'annuaires
- Résoudre les problèmes de synchronisation d'annuaires

### **Gérer l'accès utilisateur sécurisé dans Microsoft 365**

- Introduction
- Gérer les mots de passe utilisateur
- Activer l'authentification directe
- Activer l'authentification multifacteur
- Activer la connexion sans mot de passe avec Microsoft Authenticator
- Explorer la gestion des mots de passe en libre-service
- Explorer Windows Hello Entreprise
- Implémenter Azure AD Smart Lockout
- Mettre en œuvre des stratégies d'accès conditionnel
- Explorer les valeurs de sécurité par défaut dans Azure AD
- Enquêter sur les problèmes d'authentification à l'aide des journaux de connexion

### **Examiner les vecteurs de menaces et les violations de données**

- Introduction
- Explorer le paysage actuel du travail et des menaces
- Examiner comment l'hameçonnage récupère des informations sensibles
- Examiner comment l'usurpation trompe les utilisateurs et compromet la sécurité des données
- Comparer le spam et les logiciels malveillants
- Examiner comment une violation de compte compromet un compte d'utilisateur
- Examiner les attaques d'élévation de privilèges
- Examiner comment l'exfiltration de données déplace les données hors de votre locataire
- Examiner comment les attaquants suppriment les données de votre locataire
- Examiner comment le déversement de données expose les données en dehors de votre locataire
- Examiner d'autres types d'attaques

## **Découvrez le modèle de sécurité Zero Trust**

- Introduction
- Examiner les principes et les composantes du modèle Zero Trust
- Planifier un modèle de sécurité Zero Trust dans votre organisation
- Examiner la stratégie de Microsoft pour le réseau Zero Trust
- Adopter une approche Zero Trust

## **Explorez les solutions de sécurité dans Microsoft 365 Defender**

- Introduction
- Améliorer la sécurité de votre messagerie à l'aide d'Exchange Online Protection et de Microsoft Defender pour Office 365
- Protéger les identités de votre organisation à l'aide de Microsoft Defender for Identity
- Protéger votre réseau d'entreprise contre les menaces avancées à l'aide de Microsoft Defender for Endpoint
- Protection contre les cyberattaques à l'aide de Microsoft 365 Threat Intelligence
- Fournir des informations sur les activités suspectes à l'aide de Microsoft Cloud App Security
- Examiner les rapports de sécurité dans Microsoft 365 Defender

## **Examinez Microsoft Secure Score**

- Introduction
- Explorer Microsoft Secure Score
- Evaluer votre posture de sécurité avec Microsoft Secure Score
- Améliorer votre score sécurisé
- Suivre votre historique Microsoft Secure Score et atteindre ses objectifs

## **Examinez la gestion des identités privilégiées**

- Introduction
- Explorer la gestion des identités privilégiées dans Azure AD
- Configurer la gestion des identités privilégiées
- Audit de la gestion des identités privilégiées
- Explorer Microsoft Identity Manager
- Contrôler les tâches d'administrateur privilégié à l'aide de la gestion des accès privilégiés

## **Examinez Azure Identity Protection**

- Introduction
- Explorer Azure Identity Protection
- Activer les stratégies de protection par défaut dans Azure Identity Protection
- Explorer les vulnérabilités et les événements de risque détectés par Azure Identity Protection
- Planifier votre enquête d'identité

## **Examinez Exchange Online Protection**

- Introduction
- Examiner le pipeline anti-programme malveillant
- Détecter les messages contenant du spam ou des logiciels malveillants à l'aide de la purge automatique Zero-hour
- Explorer la protection contre l'usurpation d'identité fournie par Exchange Online Protection
- Découvrir d'autres protections anti-usurpation d'identité
- Examiner le filtrage du courrier indésirable sortant

## **Examinez Microsoft Defender pour Office 365**

- Introduction
- Graver les échelons de la sécurité d'EOP à Microsoft Defender pour Office 365
- Étendre les protections EOP à l'aide de pièces jointes approuvées et de liens fiables
- Gérer les renseignements usurpés
- Configurer des stratégies de filtrage du courrier indésirable sortant
- Débloquer les utilisateurs de l'envoi d'e-mails

## **Gérez les pièces jointes fiables**

- Introduction
- Protéger les utilisateurs contre les pièces jointes malveillantes à l'aide de pièces jointes fiables
- Créer des stratégies de pièces jointes approuvées à l'aide de Microsoft Defender pour Office 365
- Créer des stratégies de pièces jointes fiables à l'aide de PowerShell
- Modifier une stratégie de pièces jointes fiables existante
- Créer une règle de transport pour contourner une politique de sécurité des pièces jointes
- Examiner l'expérience de l'utilisateur final avec les pièces jointes sécurisées

## **Gérer des liens fiables**

- Introduction
- Protéger les utilisateurs contre les URL malveillantes à l'aide de liens fiables
- Créer des stratégies de liens fiables à l'aide de Microsoft 365 Defender
- Créer des stratégies de liens fiables à l'aide de PowerShell
- Modifier une stratégie de sécurité existante
- Créer une règle de transport pour contourner une stratégie liens fiables
- Examiner l'expérience de l'utilisateur final avec les liens sécurisés (Safe Links)

## **Explorez les renseignements sur les menaces dans Microsoft 365 Defender**

- Introduction
- Découvrir Microsoft Intelligent Security Graph
- Explorer les stratégies d'alerte dans Microsoft 365
- Exécuter des enquêtes et des réponses automatisées
- Explorer la chasse aux menaces avec Microsoft Threat Protection
- Explorer la recherche avancée des menaces dans Microsoft 365 Defender
- Explorer l'analyse des menaces dans Microsoft 365
- Identifier les problèmes de menace à l'aide des rapports Microsoft Defender

## **Mettre en œuvre la protection des applications à l'aide de Microsoft Defender pour Cloud Apps**

- Introduction
- Découvrir les applications cloud Microsoft Defender
- Déployer Microsoft Defender pour Cloud Apps
- Configurer des stratégies de fichiers dans Microsoft Defender pour Cloud Apps
- Gérer les alertes et y répondre dans Microsoft Defender pour Cloud Apps
- Configurer Cloud Discovery dans Microsoft Defender pour Cloud Apps
- Résoudre les problèmes liés à la découverte de cloud dans Microsoft Defender pour applications cloud

## **Implémenter Endpoint Protection à l'aide de Microsoft Defender pour Endpoint**

- Introduction
- Explorer Microsoft Defender pour Endpoint

- Configurer Microsoft Defender pour Endpoint dans Microsoft Intune
- Intégrer des appareils à Microsoft Defender pour Endpoint
- Gérer les vulnérabilités Endpoint avec Microsoft Defender Vulnerability Management
- Gérer la détection d'appareils et l'évaluation des vulnérabilités
- Réduire votre exposition aux menaces et aux vulnérabilités

## **Mettre en œuvre une protection contre les menaces à l'aide de Microsoft Defender pour Office 365**

- Introduction
- Explorer la pile de protection Microsoft Defender pour Office 365
- Enquêter sur les attaques de sécurité à l'aide de l'Explorateur de menaces
- Identifier les problèmes de cybersécurité à l'aide de Threat Trackers
- Se préparer aux attaques grâce à la formation par simulation d'attaque

## **Méthodes pédagogiques**

Cette formation Microsoft Office 365 est rythmée par une alternance d'exposés et de travaux pratiques. Les exercices réalisés lors des travaux pratiques permettent la mise en œuvre des connaissances acquises.

## **Méthodes d'évaluation des acquis**

Afin d'évaluer l'acquisition de vos connaissances et compétences, il vous sera envoyé un formulaire d'auto-évaluation, qui sera à compléter en amont et à l'issue de la formation.

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.

## **Les plus de cette formation**

Nos consultants experts vous apportent leurs conseils et leurs retours d'expérience.

## **Certification**

Cette formation prépare la certification **Microsoft MS-102 Microsoft 365 Certified Enterprise Administrator Expert**.