

# Microsoft 365 – Les bases de l'administration

## INFORMATIONS GÉNÉRALES

**Type de formation :** Formation continue

**Éligible au CPF :** Non

**Domaine :** Systèmes et Réseaux

**Action collective :** Non

**Filière :** Systèmes et réseaux Microsoft

**Rubrique :** Office 365

**Code de formation :** MSMS102

## € Tarifs

**Prix public :** 3095 €

### Tarif & financement :

Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :

**Le plan de développement des compétences de votre entreprise :** rapprochez-vous de votre service RH.

**Le dispositif FNE-Formation.**

**L'OPCO** (opérateurs de compétences) de votre entreprise.

**France Travail:** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

**CPF -MonCompteFormation**

Contactez nous pour plus d'information : [contact@aston-institut.com](mailto:contact@aston-institut.com)

## PRÉSENTATION

### Objectifs & compétences

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 oeuvre chacune des options de synchronisation d'annuaire

Gérer les identités synchronisées et mettre en oeuvre 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

Moyens pédagogiques

### Public visé

Administrateurs Microsoft 365

### Pré-requis

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

## Lieux & Horaires

**Durée :** 35 heures

**Délai d'accès :** Jusqu'à 8 jours avant le début de la formation, sous condition d'un dossier d'inscription complet

## Prochaines sessions

Consultez-nous pour les prochaines sessions.

## PROGRAMME

### 1 - 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

### 2 - 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

### 3 - 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

**4 - 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

**5 - 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

**6 - 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

**7 - 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

**8 - Déployer des applications Microsoft 365**

**Introduction**  
Explorer les fonctionnalités des applications Microsoft 365 pour les organisations  
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 établissements  
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

**9 - 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

**10 - 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

**11 - 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

**12 - Mettre en oeuvre 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

### **13 - 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

### **14 - 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 oeuvre 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

### **15 - 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

### **16 - 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

### **17 - Explorer 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

### **18 - Examiner 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

### **19 - Examiner 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

**20 - Examiner 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

**21 - Examiner 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

**22 - Examiner Microsoft Defender pour Office 365**

Introduction

Gravir 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

**23 - Gérer 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

**24 - 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)

**25 - Explorer 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

**26 - Mettre en oeuvre 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

**27 - 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

### **28 - Mettre en oeuvre 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

## **MODALITÉS**

### **Modalités**

**Modalités :** en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.

**Pédagogie :** essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

**Ressources techniques et pédagogiques :** Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.

**Pendant la formation :** mises en situation, autodiagnostic, travail individuel ou en sous-groupe sur des cas réels.

### **Méthode**

**Fin de formation :** entretien individuel.

**Satisfaction des participants :** questionnaire de satisfaction réalisé en fin de formation.

**Assiduité :** certificat de réalisation.

**Validations des acquis :** grille d'évaluation des acquis établie par le formateur en fin de formation.

### **Les plus de la formation**

Cette formation couvre trois éléments centraux de l'administration d'entreprise Microsoft 365 : la gestion des locataires et des services Microsoft 365, la gestion Microsoft 365 et la gestion des identités Microsoft 365.

Cette formation remplace les cours MSMS100 "Microsoft 365 - Gestion des identités et des services" et MSMS101 "Microsoft 365 - Gestion de la sécurité et de la mobilité"

Une pédagogie basée sur l'alternance de phases théoriques, d'ateliers de mise en pratique, de retours d'expérience et d'échanges.

La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).