

IBM Certified Associate - MobileFirst Protect

RS2529 · RS · Publiée

L'essentiel

Code(s) NSF	326
Formacode(s)	31054
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	31/12/2021

Certificateur(s)

CIE IBM FRANCE · SIRET : 55211846503644

Résumé de la certification

OBJECTIFS ET CONTEXTE

Tout type d'entreprise ou association ayant plusieurs postes informatisés, et entreprises du secteur informatique à partir d'une personne.

La plate-forme IBM MobileFirst est une plate-forme d'applications mobiles modulaire qui aide les entreprises à intégrer et à gérer des applications mobiles en toute sécurité. Elle permet de créer, d'enrichir et de distribuer en continu des applications mobiles de manière efficace et rentable.

Le professionnel certifié IBM Certified Associate - MobileFirst Protect, en tant que responsable technique, est chargé de configurer et d'utiliser le portail IBM MobileFirst Protect pour y installer la solution IBM MobileFirst Protect, dans l'une de ses deux versions SaaS ou hébergée sur site.

Il travaille de façon autonome et sera en mesure d'effectuer ses tâches avec une assistance limitée de la part de ses pairs, de la documentation produit et des services de support technique.

Remarque : Cette certification est à rapprocher de la version SaaS intitulée IBM MobileFirst Protect (SaaS).

COMPÉTENCES ATTESTÉES

La certification IBM Certified Associate - MobileFirst Protect permettra au professionnel d'acquérir les compétences suivantes :

- Manipuler les fonctionnalités de MobileFirst Protect de gestion des dispositifs, des contenus sécurisés et des applications
- Intégrer MobileFirst Protect
- Réaliser un diagnostic des incidents techniques survenant sur MobileFirst Protect

Les compétences évaluées portent sur la capacité à :

Configurer le portail MobileFirst Protect (MaaS360) :

- Créer les portails requis pour une gestion correcte des dispositifs par le client
- Distinguer les comptes parent des comptes enfant et déceler la nécessité de créer une hiérarchie
- Configurer la sécurité des portails pour les administrateurs et définir leurs niveaux d'accès
- Créer et configurer un ensemble de règles en conformité avec la politique d'entreprise pour automatiser les contrôles de conformité, renforcer les règles et prendre les actions appropriées en cas de non conformité
- Créer des répertoires locaux d'utilisateurs et d'administrateurs
- Créer un catalogue d'applications en fonction des profils
- Vérifier le bon fonctionnement des filtres de confidentialité
- Prendre les mesures nécessaires pour faire appliquer les règles en fonction de la localisation des dispositifs
- Programmer des messages d'alerte à l'attention des administrateurs et/ou de l'utilisateur lorsque le seuil maximum de consommation des données est atteint
- Définir clairement les options de marquage au moyen d'icônes spécifiques personnalisés, au niveau des comptes enfant/parent

Utiliser le portail MobileFirst Protect (MaaS360) et Naviguer :

- Exposer les possibilités de navigation pour un administrateur d'appareils mobiles, depuis un appareil mobile, à travers les pages de gestion; expliquer comment il peut afficher des données, créer des rapports et changer l'état du dispositif géré.
- Utiliser la fonction 'recherche avancée' pour retrouver des mobiles
- Souscrire au programme d'alertes et de rapports
- Sélectionner les rapports qui peuvent être exportés dans le format approprié en fonction des besoins des clients
- Adapter un rapport existant pour en créer un nouveau conforme aux exigences
- Paramétrer la consultation, la sauvegarde et l'envoi des rapports par mail à l'administrateur ou l'utilisateur approprié
- Orienter l'utilisateur final mobile pour qu'il puisse naviguer sur les pages, consulter des données, changer des informations, localiser ou désactiver ses dispositifs mobiles

Intégrer MobileFirst Protect (MaaS360) :

- Définir les prérequis pour installer en parallèle MobileFirst Protect (MaaS360), Cloud Extender et Mobile Enterprise Gateway et offrir ainsi au client une infrastructure intégrée et sécurisée.
- Adapter les fonctionnalités de chaque module Cloud Extender et le service d'arrière-plan dans lequel il s'intègre, en fonction de l'environnement client
- Informer le client des prérequis nécessaires au Cloud Extender pour communiquer avec le portail MaaS360
- Cerner les ressources pour intégrer Mobile Enterprise Gateway afin de fournir aux dispositifs mobiles un accès au contenu situé derrière le pare-feu
- Renseigner sur l'intégration des services en ligne MobileFirst Protect extérieurs à la console MaaS360 et démontrer de la nécessité de les activer

Gérer les dispositifs mobiles dans MobileFirst Protect (MaaS360) :

- Vérifier les différents prérequis qui permettent l'enregistrement des dispositifs mobiles dans un contexte de systèmes d'exploitation multiples
- Exposer les différentes méthodes d'enregistrement des mobiles à gérer, par un administrateur
- Exécuter les étapes de création, configuration et publication de règles de gestion des appareils Android, iOS, Windows Phone et Mac OS X
- Vérifier les actions à disposition des administrateurs du portail pour la gestion des périphériques mobiles et faire en sorte que l'organisation dans son ensemble en comprenne les fonctionnalités
- Exposer les actions à prendre par rapport aux plateformes supportées par les ordinateurs sous Windows pour que des PC enregistrés puissent être gérés par MobileFirst Protect
- Déterminer ce qui peut être régi par la règle d'entreprise Workplace Persona Policy d'une part, et par la MDM Policy (Mobile Device Management) d'autre part
- Décrire les fonctionnalités du catalogue d'applications MaaS360 pour attribuer les applications appropriées sur les appareils mobiles

Sécuriser le Contenu :

- Expliquer comment doit être conçue l'architecture pour que les documents et les applications soient contrôlés afin de protéger les données, tout en procurant un maximum de flexibilité à la fois pour les utilisateurs et les administrateurs
- Trouver les méthodes permettant à la fois de sécuriser les informations contenues dans MobileFirst Protect (MaaS360) et les ressources de l'entreprise en dehors des applications MaaS360, par souci de garantir la sécurité des applications de l'entreprise et des applications publiques
- Mettre en place une bibliothèque MaaS360 pour répertorier des documents téléchargés, en vue de les distribuer aux groupes désignés, avec les propriétés sélectionnées

Diagnostiquer les incidents techniques :

- Repérer où sont générés les fichiers journaux et leur contenu, identifier les incidents, et/ou transférer ceux-ci au support technique pour une prise en charge et résoudre les problèmes liés au Cloud Extender

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Les candidats, quel que soit leur âge ou leur niveau scolaire, doivent posséder au préalable les connaissances ou l'expérience suivante :

- Connaissance pratique du portail IBM MobileFirst Protect et des capacités d'intégration d'IBM MobileFirst Protect
- Connaissance pratique de TCP/IP, de la topologie des réseaux et de la résolution des incidents techniques

- Connaissance pratique des systèmes d'exploitation supportés par les appareils mobiles, tels que IOS, Android and Windows Phone.
- Connaissance pratique des technologies de courrier électronique sur dispositifs mobiles
- Connaissance de base de LDAP et d'Active Directory

Base légale

Date d'échéance de l'enregistrement 31/12/2021

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

Lien de la certification :

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/2529/>