IBM MaaS360 Gateway Suite

Libérez le potentiel de vos systèmes et contenus d'entreprise

Principaux avantages

- Accès mobile protégé aux données d'entreprise sans utiliser de VPN
- Utilisation de SharePoint, du partage de fichiers Windows et de vos sites intranet
- Utilisation des tunnels VPN intégrés dans les applications pour accéder aux systèmes de votre entreprise
- Collaboration facile lors de vos déplacements
- Protection des données sensibles de l'entreprise grâce à des règles de sécurité robustes, notamment des contrôles DLP, du cryptage et des autorisations
- Possibilité d'accès sans devoir modifier votre réseau ou les paramètres de sécurité de votre pare-feu

Utilisez SharePoint, le partage de fichiers Windows et intranet

IBM® MaaS360® Gateway Suite offre un accès simple et sûr aux ressources de l'entreprise derrière le pare-feu, comme du contenu SharePoint ou Windows File Share, des sites intranet et des données d'applications, sans avoir besoin de modifier votre réseau, la configuration de sécurité du pare-feu ou le VPN de l'appareil.

Collaborez en toute convivialité lors de vos déplacements, tout en protégeant vos contenus, grâce à des règles permettant d'autoriser, de crypter et de « conteneuriser » les informations. La solution est simple à installer, à configurer et à maintenir. Elle ne nécessite ni matériel supplémentaire dans votre environnement informatique, ni connexions TCP/IP entrantes provenant d'appareils ou de services externes à votre réseau local.

Découvrez une manière fiable de collaborer professionnellement via mobile

Les utilisateurs peuvent accéder, afficher et partager des contenus professionnels à partir de SharePoint, du partage de fichiers Windows et d'autres solutions grâce à IBM® MaaS360® Content Suite ou IBM® MaaS360® Secure Mobile Browser sur leurs appareils mobiles. Qu'ils utilisent des appareils personnels ou professionnels, ils peuvent collaborer sur des documents pendant leurs déplacements.

Libérez en toute sécurité le potentiel des sites intranet et des applications internes telles que JIRA, des wikis internes, des bases de connaissances, des anciens systèmes ERP et plus encore en utilisant MaaS360 Secure Mobile.

Les données sont protégées dans un conteneur codé avec des contrôles contre la fuite d'informations (DLP). Si un employé quitte votre entreprise, vous pouvez choisir de supprimer uniquement les données et applications d'entreprise de l'appareil, ou encore de réinitialiser les réglages d'usine.

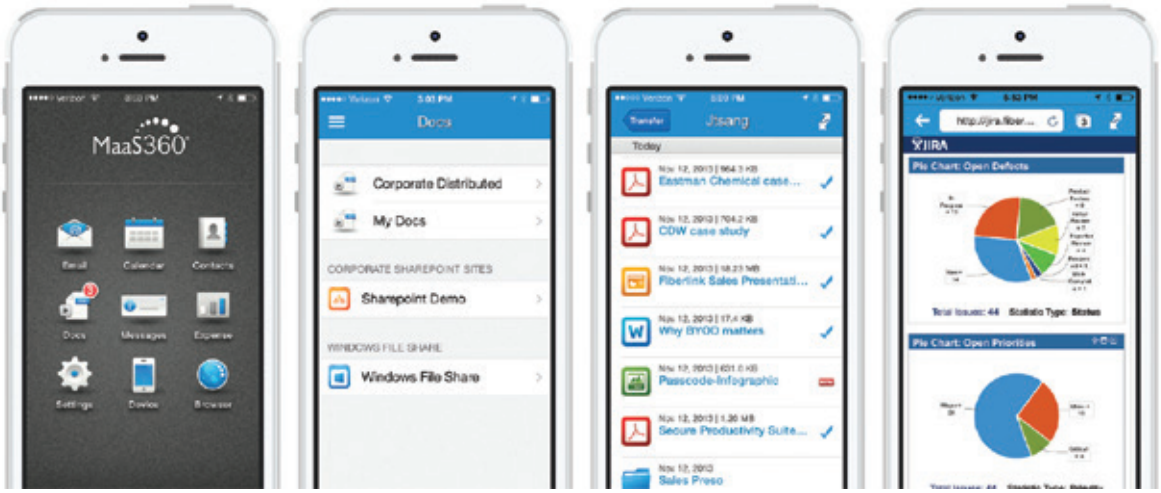

Figure 1 : Exemples du conteneur MaaS360, des référentiels de données, des documents et d'un site intranet sur les appareils mobiles

Accédez aux ressources de votre entreprise lors de vos déplacements

- Avec IBM MaaS360 Gateway for Documents, récupérez, affichez, modifiez et partagez du contenu d'entreprise à partir de SharePoint, de Windows File Share et d'autres solutions avec MaaS360 Content Suite sur les appareils mobiles
- Collaborez sur des documents lors de vos déplacements, par le biais d'appareils personnels ou professionnels
- Avec IBM MaaS360 Gateway for Browser, libérez en toute sécurité le potentiel des sites intranet et des applications internes telles que JIRA, des wikis internes, des bases de connaissances, des anciens systèmes ERP et bien plus encore en utilisant MaaS360 Secure Mobile Browser
- IBM MaaS360 Gateway for Apps permet des tunnels VPN dans les applications jusqu'aux systèmes de votre entreprise et aux bases de données des applications

Intégration facile à vos systèmes

- Aucun ajout de matériel à votre environnement informatique
- Aucun dispositif VPN (« VPN instantané » au niveau de l'application)
- Aucune modification sur votre réseau
- Aucune connexion TCP/IP entrante à partir d'appareils ou de services externes à votre réseau local
- Pas de reconfiguration de sécurité de votre pare-feu

Contrôlez les autorisations et les accès de manière détaillée

- Assurez-vous que les données de votre entreprise ne peuvent être visualisées que sur les appareils mobiles autorisés.
- La communication est intégralement codée entre la passerelle et les appareils.
- Activez ou bloquez les appareils individuels et les utilisateurs au sein de votre entreprise.
- Ne présentez que le contenu et les applications sélectionnés à vos partenaires, sous-traitants, consultants, etc.

Restreignez l'accès aux données sensibles de votre entreprise

- Protégez les données à l'aide d'un conteneur codé.
- Établissez et appliquez des règles détaillées pour bénéficier des contrôles DLP et d'une sécurité à toute épreuve sur les mobiles.
- Empêchez les personnes extérieures d'accéder à des données sensibles en imposant une authentification et en activant des autorisations.
  - Les données de l'entreprise ne sont pas stockées sur les appareils mobiles sous un format non encrypté.
  - Supprimez complètement les données d'un appareil, ainsi que les informations confidentielles en cas de perte ou de vol.
  - MaaS360 dirige le trafic entre la passerelle et les appareils sans lire les données cryptées
  - Aucune vulnérabilité n'est introduite dans le réseau vis-à-vis des vérifications et des attaques, contrairement à ce qui se produirait si un serveur d'application mobile était ouvert à l'Internet public.
  - Il n'est pas nécessaire d'utiliser un VPN, qui pourrait autoriser certaines applications indésirables à accéder à votre réseau local.

Accès intranet mobile

MaaS360 Gateway Suite libère le potentiel votre SharePoint, de Windows Files Share, les sites intranet et les bases de données des applications pour un accès transparent et protégé sur les appareils mobiles afin de permettre la collaboration de l'entreprise en déplacement.

Principales caractéristiques

- Accès sécurisé aux ressources de l'entreprise depuis un appareil mobile
- Affichage et partage des contenus à partir de SharePoint et du partage de fichiers Windows
- Navigation et récupération des informations à partir des sites intranet
- Activation de tunnels VPN intégrés dans les applications pour accéder aux bases de données internes
- Utilisation d'un conteneur avec chiffrement AES256, conforme à la norme FIPS 140-2
- Obligation d'authentification et d'autorisation
- Configuration des contrôles DLP, y compris restrictions du copier/coller, de l'ouverture de documents dans des applications personnelles, d'impression et de capture d'écran

Pour plus d'informations sur IBM MaaS360 et pour commencer un essai gratuit de 30 jours, visitez www.ibm.biz/EssayezMaaS360

Compagnie IBM France
17, avenue de l'Europe
92275 BOIS COLOMBES CEDEX

Produit aux États-Unis
Août 2016

Les données de performances et les exemples citant des clients ne sont présentés qu'à titre d'illustration. Les résultats de performances réels peuvent varier selon les configurations et les conditions de fonctionnement spécifiques. Il incombe à l'utilisateur d'évaluer et de vérifier le fonctionnement de tout autre produit ou programme avec les produits et programmes IBM.

LES INFORMATIONS CONTENUES DANS CE DOCUMENT SONT FOURNIES « EN L'ÉTAT », SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT SANS AUCUNE GARANTIE OU CONDITION DE QUALITÉ MARCHANDE OU D'APTITUDE A UN EMPLOI SPÉCIFIQUE ET SANS AUCUNE GARANTIE DE NON-CONTREFAÇON. Les produits IBM sont garantis conformément aux conditions de leur contrat de vente.

Le client est tenu de s'assurer du respect des lois et réglementations en vigueur. IBM ne fournit aucun conseil juridique et ne garantit pas que ses produits ou services assurent la conformité du client aux lois et réglementations en vigueur.

Toutes les déclarations relatives aux orientations futures d'IBM sont sujettes à modification ou retrait sans préavis. Elles n'expriment que les intentions et les objectifs d'IBM.

Déclaration de bonnes pratiques en matière de sécurité : La sécurité des systèmes informatiques implique la protection des systèmes et des informations en prévenant, détectant et réagissant aux accès non autorisés, qu'ils proviennent de l'entreprise ou de l'extérieur. Les accès non autorisés peuvent entraîner l'altération, la destruction ou l'utilisation inappropriée des informations, et ainsi causer des dommages ou une utilisation abusive de vos systèmes, par exemple pour attaquer des tiers. Aucun système ou produit informatiques ne doit être considéré comme entièrement sécurisé. Aucun produit ni aucune mesure de sécurité ne peut être totalement efficace contre les accès non autorisés. Les systèmes et produits IBM s'inscrivent dans une approche de sécurité complète qui implique des procédures opérationnelles supplémentaires et peuvent demander aux autres systèmes, produits ou services d'être plus efficaces. IBM ne garantit pas que ses systèmes et ses produits sont invulnérables face aux comportements malveillants ou illégaux provenant de tiers.

Recyclable

WGD03065-FRFR-02