

IBM MaaS360 (SaaS)

Ce Descriptif de Services détaille le Service Cloud qu'IBM fournit au Client. Le terme « Client » signifie la société et ses destinataires et utilisateurs autorisés du Service Cloud. Le Devis et l'Autorisation d'Utilisation sont fournis séparément sous la forme de Documents de Transaction.

1. Service Cloud

MaaS360 est une plateforme cloud facile à utiliser dotée de toutes les fonctionnalités essentielles permettant la gestion de bout en bout des appareils mobiles actuels utilisant les systèmes d'exploitation iOS, Android, Windows et Blackberry. Voici une brève description des Offres de Service Cloud :

1.1 IBM MaaS360 Mobile Device Management (SaaS) et IBM MaaS360 Mobile Device Management (SaaS) Step up for existing customers

Les fonctions de gestion d'appareil de mobilité principales (MDM) comprennent l'enregistrement et la configuration des appareils, la gestion de la stratégie de sécurité et les actions d'appareil, telles que l'envoi de message, la localisation, le verrouillage et l'effacement. Les fonctions MDM avancées comprennent les règles de conformité automatisées, les paramètres de confidentialité BYOD (bring your own device) et la génération de rapports et les tableaux de bord Mobility Intelligence.

1.2 IBM MaaS360 Mobile Application Management (SaaS) et IBM MaaS360 Mobile Application Management (SaaS) Step up for existing customers

MaaS360 Mobile Application Management permet d'ajouter des applications et de les distribuer aux appareils pris en charge gérés par MaaS360. Il s'agit notamment de MaaS360 App Catalog, une application permettant aux utilisateurs de consulter et d'installer des applications gérées et de recevoir des alertes relatives aux applications gérées mises à jour.

1.3 IBM MaaS360 Mobile Application Security (SaaS) et IBM MaaS360 Mobile Application Security (SaaS) Step up for existing customers

MaaS360 Mobile Application Security permet une protection de données supplémentaire pour les applications d'entreprise utilisant le SDK WorkPlace pendant le développement, ou permet aux applications iOS de télécharger facilement l'application (.ipa), de l'associer à un profil d'application des accès et d'intégrer automatiquement un certificat signataire. Mobile Application Security intègre l'application à Productivity Suite. Cela permet la connexion unique, l'accès Intranet via la passerelle d'entreprise mobile et l'application des paramètres de sécurité de données.

1.4 IBM MaaS360 Gateway for Apps (SaaS) et IBM MaaS360 Gateway for Apps (SaaS) Step up for existing customers

MaaS360 Gateway for Apps permet aux utilisateurs situés hors du réseau d'entreprise d'accéder directement aux ressources d'application internes sans qu'une connexion VPN de niveau appareil intégral nécessaire.

1.5 IBM MaaS360 Mobile Content Management (SaaS) et IBM MaaS360 Mobile Content Management (SaaS) Step up for existing customers

MaaS360 Mobile Content Management permet à l'administrateur d'ajouter et de distribuer des documents aux appareils pris en charge gérés par IBM MaaS360 Mobile Device Management. Il comprend notamment IBM MaaS360 Doc Catalogue, un conteneur d'appareil protégé par mot de passe qui fournit aux utilisateurs un moyen protégé et simple pour consulter et partager des documents et y accéder. Il inclut l'accès direct aux contenus et référentiels distribués tels que SharePoint, Box et Google Drive. L'accès aux partages de fichiers SharePoint et Windows privés est disponible à l'aide de MaaS360 Gateway for Documents. Les documents gérés par le biais de MaaS360 peuvent être soumis au contrôle des versions, audités et protégés via des options de règle de prévention de perte de données (DLP), notamment l'authentification obligatoire, la fonctionnalité de restriction des fonctions de Copier/Coller et l'interdiction d'ouverture ou de partage dans d'autres applications.

1.6 IBM MaaS360 Mobile Document Sync (SaaS) et IBM MaaS360 Mobile Document Sync (SaaS) Step up for existing customers

MaaS360 Mobile Document Sync permet aux utilisateurs de synchroniser le contenu d'utilisateur entre les appareils mobiles gérés. Les administrateurs peuvent garantir que les règles telles que la restriction des fonctions Couper/Copier/Coller et l'interdiction d'ouverture ou de partage de contenu dans d'autres applications sont en place pour le contenu utilisateur d'un appareil à l'autre. Le contenu est stocké de manière protégée, tant dans le Cloud que sur l'appareil, et n'est accessible que via MaaS360 Doc Catalogue.

1.7 IBM MaaS360 Mobile Document Editor (SaaS) et IBM MaaS360 Mobile Document Editor (SaaS) Step up for existing customers

MaaS360 Mobile Document Editor est une puissante suite bureautique qui permet aux utilisateurs de gérer des documents professionnels pendant qu'ils sont en déplacement. MaaS360 Mobile Document Editor permet les fonctions suivantes :

- Création et édition de fichiers .DOC, .PPT et .XLS
- Mode de présentation pour les diapositives
- Gestion simplifiée des pièces jointes d'e-mail et d'autres fichiers issus de MaaS360 pour iOS

1.8 IBM MaaS360 Gateway for Documents (SaaS) et IBM MaaS360 Gateway for Documents (SaaS) Step up for existing customers

MaaS360 Gateway for Documents permet aux entreprises d'utiliser MaaS360 Mobile Content Management pour fournir aux appareils situés hors du réseau d'entreprise un accès direct aux sites Connexions internes, aux sites SharePoint, à Windows File Shares et à d'autres magasins de fichiers sans qu'une connexion VPN de niveau appareil intégral soit nécessaire. MaaS360 Gateway for Documents requiert l'achat de MaaS360 Mobile Content Management. Il prend en charge iOS 5.0 et Android 4.0 ou version ultérieure.

1.9 IBM MaaS360 Email Management (SaaS) et IBM MaaS360 Email Management (SaaS) Step up for existing customers

MaaS360 Email Management comprend des fonctionnalités clés à l'appui de Microsoft Exchange ActiveSync et Lotus Traveler.

- Exchange ActiveSync : permet la prise en charge des appareils mobiles se connectant à Microsoft Exchange via le protocole ActiveSync. Il comprend des fonctionnalités telles que les fonctions principales de gestion d'appareil mobile, par exemple la configuration des appareils, la création, l'application des règles ActiveSync (code d'accès, blocage ou autorisation d'accès à la messagerie électronique), et l'exécution d'actions liées aux appareils, telles que le verrouillage et l'effacement, ainsi que la génération de rapport détaillé sur les attributs des appareils.
- Lotus Traveler : permet la prise en charge des appareils mobiles se connectant à IBM Lotus Notes® via le protocole Lotus Traveler. Il comprend des fonctionnalités telles que la configuration des appareils, le blocage ou l'autorisation d'appareils, l'application des règles de gestion de code d'accès, l'effacement des appareils et la génération de rapport détaillé sur les attributs des appareils.

1.10 IBM MaaS360 Secure Mobile Browser (SaaS) et IBM MaaS360 Secure Mobile Browser (SaaS) Step up for existing customers

MaaS360 Browser est un navigateur Web complet permettant l'accès aux sites intranet d'entreprise et mettant en application la conformité des règles de contenu en définissant des stratégies de sécurité et de filtrage de site Web pour garantir que les utilisateurs n'accèdent qu'à du contenu Web approuvé en fonction d'un certain nombre de catégories de contenu, telles que les réseaux sociaux, les sites explicites ou malveillants. Il comprend la fonction de désactivation des navigateurs Web natifs et tiers par le biais de la stratégie d'application ou du placement sur liste noire, lorsqu'il est associé à MobileFirst Protect Devices. Il permet de créer des listes blanches définissant des exceptions aux sites Web, de restreindre les cookies, de copier, de coller et d'imprimer les fonctionnalités et d'activer le mode Kiosk.

- 1.11 IBM MaaS360 Gateway for Browser (SaaS) et IBM MaaS360 Gateway for Browser (SaaS) Step up for existing customers**
- MaaS360 Gateway for Browser permet aux appareils pris en charge d'accéder aux sites Web internes approuvés sans qu'une connexion VPN de niveau appareil intégral soit nécessaire.
- 1.12 IBM MaaS360 for BlackBerry (SaaS) et IBM MaaS360 for BlackBerry (SaaS) Step up for existing customers**
- Permet la prise en charge des appareils mobiles connectés au BlackBerry Enterprise Server (BES) en utilisant des API BlackBerry. Les fonctionnalités incluses sont les actions distantes telles que l'envoi d'un message, la réinitialisation du code d'accès, l'affectation de règle BES et l'effacement, ainsi que la génération de rapport détaillé sur les attributs des appareils. L'installation de MaaS360 Cloud Extender est requise. Disponible uniquement pour les appareils consultés ou gérés avec MaaS360 via BES 5.0.
- 1.13 IBM MaaS360 Mobile Expense Management (SaaS) et IBM MaaS360 Mobile Expense Management (SaaS) Step up for existing customers**
- MaaS360 Mobile Expense Management permet à l'administrateur de créer des politiques d'utilisation de données et de les affecter aux appareils pris en charge gérés par MaaS360, et d'affecter ces politiques à un niveau d'appareil, de groupe ou global et de configurer des seuils d'alerte et la messagerie pour l'utilisation des données tant dans le réseau qu'en itinérance.
- 1.14 IBM MaaS360 Management Suite (SaaS) et IBM MaaS360 Management Suite (SaaS) Step up for existing IBM MaaS360 customers**
- Suite/groupe de produits comprenant MaaS360 Mobile Device Management, MaaS360 Mobile Application Management, MaaS360 Content Service et MaaS360 Mobile Expense Management.
- 1.15 IBM MaaS360 Productivity Suite (SaaS) et IBM MaaS360 Productivity Suite (SaaS) Step up for existing customers**
- Suite/groupe de produits comprenant MaaS360 Secure Mobile Mail, MaaS360 Mobile Application Management, MaaS360 Mobile Application Security, MaaS360 Content Service et MaaS360 Secure Mobile Browser.
- 1.16 IBM MaaS360 Secure Mobile Mail (SaaS) et IBM MaaS360 Secure Mobile Mail (SaaS) Step up for existing customers**
- MaaS360 Secure Mobile Mail fournit une application de productivité bureautique distincte permettant aux utilisateurs d'accéder et de gérer la messagerie, l'agenda et les contacts avec la possibilité de contrôler les e-mails et les pièces jointes pour empêcher la fuite de données en limitant le réacheminement ou le déplacement de contenu vers d'autres applications, d'appliquer l'authentification, de restreindre les fonctions Couper/Copier/Coller et de verrouiller les pièces jointes des e-mail à des fins de consultation uniquement.
- 1.17 IBM MaaS360 Gateway Suite (SaaS) et IBM MaaS360 Gateway Suite (SaaS) Step up for existing customers**
- MaaS360 Gateway Suite permet aux applications prises en charge sur iOS et Android de communiquer de manière transparente avec les ressources du réseau interne de l'entreprise.
- 1.18 IBM MaaS360 Content Suite (SaaS) et IBM MaaS360 Content Suite (SaaS) Step up for existing customers**
- Suite/groupe de produits comprenant MaaS360 Mobile Content Management, MaaS360 Mobile Document Editor et MaaS360 Mobile Document Sync.
- 1.19 IBM MaaS360 Mobile Threat Management (SaaS)**
- MaaS360 Mobile Threat Management permet la sécurité mobile améliorée, à l'aide de la détection de logiciel malveillant mobile et de la détection de jailbreak/root avancée. A l'aide de MaaS360 Mobile Threat Management, le Client pourra définir et gérer les règles de conformité relatives aux logiciels malveillants et autres vulnérabilités de sécurité détectés.

1.20 IBM MaaS360 Content Service (SaaS)

MaaS360 Content Service (SaaS) permet aux utilisateurs de télécharger des documents et des packages d'application vers le système de distribution de contenu de MaaS360.

IBM MaaS360 fournit à chaque Client 1 Go d'espace de stockage. IBM MaaS360 fournit également 6 Go de bande passante par unité et par an sous la forme d'un pool partagé de bande passante. La totalité du pool de bande passante est partagée au niveau de toutes les unités. Cette allocation de stockage et de bande passante de base n'augmente pas, quel que soit le nombre de groupes de produits ou de lignes article achetés. Les Clients sont tenus d'acheter du stockage et/ou de la bande passante additionnelle pour toute quantité utilisée ou requise au-delà de la quantité de base fournie.

1.21 IBM MaaS360 Content Service Storage (SaaS)

MaaS360 Content Service Storage (SaaS) permet aux utilisateurs d'acheter un espace de stockage de données total disponible pour MaaS360 Content Service (SaaS).

1.22 IBM MaaS360 Content Service Bandwidth (SaaS)

MaaS360 Content Service Bandwidth (SaaS) permet aux utilisateurs d'acheter la quantité totale de bande passante disponible pour MaaS360 Content Service (SaaS).

1.23 IBM MaaS360 Professional (SaaS)

Dédiée aux PME, cette offre permet de configurer à distance d'une manière rapide et simple des smartphones et des tablettes, de mettre en œuvre des règles de sécurité, de publier des applications et des documents et de protéger les données des appareils personnels et professionnels des employés. Le Client bénéficie de toutes les fonctions de gestion d'appareils mobiles dont son entreprise a besoin rapidement, facilement et à prix raisonnable.

1.24 IBM MaaS360 Laptop Management (SaaS)

Permet d'inscrire, de configurer, de gérer et de surveiller tous les appareils OS X et Windows du Client ainsi que ses smartphones et tablettes. Le Client peut gérer les profils et les règles de sécurité de manière cohérente entre les unités appartenant à l'entreprise et celles appartenant aux employés à l'aide de la même console de gestion MaaS360.

1.24.1 Windows

MaaS360 Laptop Management (SaaS) pour PC Windows fournit des informations sur les abonnements et les ressources gérées ainsi que sur le matériel, le système d'exploitation et les logiciels en cours d'utilisation. Le module de génération de rapports sur la sécurité des points d'extrémité fournit des analyses de données et des rapports interactifs sur les applications fournies par le Client, par exemple les solutions anti-virus, les solutions de restauration/reprise après incident, de chiffrement de données et de firewall personnel, ainsi que sur les correctifs de système d'exploitation manquants. Le module de protection des données fournit des analyses de données et des rapports interactifs pour les services de sécurité, notamment le chiffrement de données, la prévention des fuites de données, la restauration/reprise après incident et autres d'applications intégrées. Les systèmes d'exploitation pris en charge sont Windows XP SP3, Windows Vista, Windows 7, Windows 8+ et Windows 8+ Pro (versions 32 et 64 bits).

Les actions réalisables avec les unités sont les suivantes :

- Envoyer un message à l'unité
- Verrouiller l'unité
- Localiser l'unité (requiert MaaS360 Laptop Location)
- Arrêter, démarrer, redémarrer l'unité
- Eteindre et réamorcer l'unité
- Nettoyer le disque dur
- Configurer les paramètres des correctifs
- Distribuer des logiciels

1.24.2 Mac OS X

MaaS360 Laptop Management (SaaS) pour Mac OS X fournit des informations sur les abonnements et les ressources gérées ainsi que sur le matériel, le système d'exploitation et les logiciels en cours d'utilisation. Le module de génération de rapports sur la sécurité des points d'extrémité fournit des analyses de données et des rapports interactifs sur les applications fournies par le Client, par exemple les solutions anti-virus, les solutions de restauration/reprise après incident, de chiffrement de données et de firewall personnel, ainsi que sur les correctifs de système d'exploitation manquants. Le module de protection des données fournit des analyses de données et des rapports interactifs pour les services de sécurité, notamment le chiffrement de données. Le module de gestion des configurations permet de gérer à distance un certain nombre de paramètres d'utilisateur et d'unité, notamment pour les mots de passe, le courrier électronique, les réseaux privés virtuels et le Wi-Fi. Les systèmes d'exploitation pris en charge sont Mac OS X version 10.7.3 et les versions ultérieures.

Les actions réalisables avec les unités sont les suivantes :

- Verrouiller l'unité
- Nettoyer le disque dur
- Modifier les règles d'administration des unités

1.25 IBM MaaS360 Laptop Location (SaaS)

MaaS360 Laptop Location (SaaS) permet de localiser les tablettes et les ordinateurs portables pris en charge. MaaS360 communique les coordonnées de l'adresse IP ou du réseau Wi-Fi et convertit ces données en une adresse facile à identifier. L'emplacement actuel d'une unité peut être identifié dès lors que cette unité est connectée. MaaS360 consigne les emplacements successivement identifiés et peut fournir un historique de ces emplacements. Requiert MaaS360 Laptop Management (SaaS) for Windows. Les systèmes d'exploitation pris en charge sont Windows XP SP3, Windows Vista, Windows 7, Windows 8+ et Windows 8+ Pro (versions 32 et 64 bits).

1.26 IBM MaaS360 Laptop Lifecycle Management (SaaS)

Comprend les fonctions de l'offre MaaS360 Laptop Management (SaaS) et les fonctionnalités supplémentaires suivantes :

- Permet au Client de télécharger des modules vers la plateforme MaaS360 Content Service (SaaS) et de planifier la distribution des charges aux unités gérées par le service MaaS360 Laptop Management (SaaS) pour Microsoft Windows. Le Client contrôle tous les aspects de la distribution, dont les instructions d'installation, et le ciblage au niveau d'une unité, d'un groupe d'unités ou d'un ensemble. Il revient au Client de créer tous les fichiers d'installation et de conditionnement. IBM ne fournit pas d'assistance pour créer les modules d'installation.

1.27 IBM MaaS360 Laptop Security (SaaS)

Permet de gérer les profils et les règles de sécurité de manière cohérente entre les unités appartenant à l'entreprise et celles appartenant aux employés à l'aide de la console de gestion.

1.28 IBM MaaS360 Essentials Suite (SaaS)

Cette suite permet au Client de consulter et contrôler les appareils et applications mobiles entrant dans l'organisation du Client. Elle permet de gérer les dépenses, applications et appareils mobiles de l'entreprise à partir d'un écran unique.

1.29 IBM MaaS360 Deluxe Suite (SaaS)

Cette suite comprend, en plus de toutes les fonctionnalités de MaaS360 Essentials Suite, une application bureautique distincte et hautement sécurisée permettant aux utilisateurs d'accéder à et de gérer leur messagerie électronique, l'agenda et leurs contacts, et de discuter en ligne.

1.30 IBM MaaS360 Premier Suite (SaaS)

Cette suite comprend, en plus de toutes les fonctionnalités de MaaS360 Deluxe Suite, la sécurité d'application mobile, un navigateur et une passerelle mobiles sécurisés et la gestion de contenu mobile.

1.31 IBM MaaS360 Enterprise Suite (SaaS)

Cette suite comprend, en plus de toutes les fonctionnalités de MaaS360 Premier Suite, la gestion des menaces visant les appareils mobiles, un éditeur de document et la synchronisation des documents.

2. Description de la Sécurité

Ce Service Cloud se conforme aux principes de confidentialité et de sécurité de données d'IBM pour l'Offre IBM SaaS, qui sont disponibles à l'adresse <http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp>, ainsi qu'à toutes dispositions additionnelles stipulées dans la présente Clause. Les éventuelles modifications des règles de sécurité des données d'IBM ne dégraderont pas la sécurité du Service Cloud.

Ce Service Cloud est certifié US-EU Safe Harbor.

3. Accord Relatif aux Niveaux de Service

IBM fournit l'Accord Relatif aux Niveaux de Service (ci-après dénommé « Accord Relatif aux Niveaux de Service » ou « SLA ») de disponibilité ci-dessous pour le Service Cloud, comme indiqué dans une Autorisation d'Utilisation. Le SLA ne constitue pas une garantie et ne s'applique pas au Logiciel d'Activation. Il n'est disponible que pour le Client et ne peut être utilisé que dans les environnements de production.

3.1 Crédits de Disponibilité

Le Client doit consigner un ticket de support de Gravité 1 auprès du centre d'assistance technique IBM dans les 24 heures suivant la première fois où le Client a eu connaissance qu'un événement a eu une incidence sur la disponibilité du Service Cloud. Le Client doit raisonnablement aider IBM dans le cadre du diagnostic et de la résolution des problèmes.

Une demande de ticket de support pour non-respect d'un SLA doit être soumise dans les trois jours ouvrables suivant la fin du mois contractuel. Le dédommagement relatif à une réclamation de SLA valide sera un avoir sur une future facture du Service Cloud en fonction de la période de temps pendant laquelle le traitement du système de production pour le Service Cloud n'est pas disponible (« Durée d'Indisponibilité »). La Durée d'Indisponibilité est calculée depuis le moment où le Client signale l'événement jusqu'au moment où le Service Cloud est restauré ; elle ne comprend pas les périodes d'indisponibilité pour les raisons suivantes : indisponibilité de maintenance programmée ou annoncée, causes échappant au contrôle d'IBM, incidents liés au contenu, à la technologie, aux conceptions ou aux instructions du Client ou d'un tiers, plateformes et configurations de système non prises en charge ou autres erreurs du Client, incident de sécurité du fait du Client ou test de sécurité mené par le Client. IBM appliquera le dédommagement correspondant le plus élevé, en fonction de la disponibilité cumulée du Service Cloud pendant chaque mois contractuel, comme indiqué dans le tableau ci-dessous. Le dédommagement total relatif à tout mois contractuel ne pourra pas dépasser dix (10 %) d'un douzième (1/12ème) de la redevance annuelle du Service Cloud.

3.2 Niveaux de Service

Disponibilité du Service Cloud pendant un mois contractuel

Disponibilité pendant un Mois Contractuel	Crédit de Disponibilité (% de redevance d'abonnement mensuelle* pour le mois contractuel objet d'une réclamation)
Inférieure à 99,8 %	2 %
Inférieure à 98,8 %	5 %
Inférieure à 95,0 %	10 %

* Si le Service Cloud a été acquis auprès d'un Partenaire Commercial IBM, la redevance d'abonnement mensuelle sera calculée sur le prix en vigueur à ce moment-là pour le Service Cloud concerné pendant le mois contractuel qui fait l'objet d'une réclamation, avec une réduction de cinquante pour cent (50 %). IBM accordera une remise directement au Client.

La disponibilité, exprimée en pourcentage, est calculée comme suit : le nombre total de minutes d'un mois contractuel moins le nombre total de minutes de la Durée d'Indisponibilité au cours d'un mois contractuel, divisé par le nombre total de minutes d'un mois contractuel.

Exemple : 425 minutes de Durée d'Indisponibilité totale pendant un mois contractuel

Au total 43 200 minutes dans un Mois contractuel de 30 jours - 425 minutes de Durée d'Indisponibilité = 42 775 minutes <hr/> Au total 43 200 minutes	= 2 % de crédit de Disponibilité pour 99,0 % de disponibilité pendant le mois contractuel
---	---

4. Support Technique

Le support technique destiné au Service Cloud est fourni à l'aide de discussions en ligne, par téléphone et par e-mail.

IBM mettra à disposition le manuel IBM Software as a Service Support Handbook qui contient les coordonnées des personnes à contacter ainsi que des informations et processus relatifs au support technique.

Niveau de Gravité	Définition de la Gravité
1	Incidents ou problèmes liés au service qui interrompent ou empêchent toute la clientèle d'effectuer des opérations internes courantes. Incidents ou problèmes causés par le service qui ont un impact catastrophique sur les opérations internes courantes.
2	Incidents ou problèmes liés au service qui interrompent ou empêchent un pourcentage significatif de la clientèle d'effectuer des opérations internes courantes. Incidents ou problèmes causés par le service qui ont un impact majeur sur les opérations internes courantes.
3	Incidents ou problèmes liés au service qui interrompent ou empêchent un faible pourcentage de la clientèle d'effectuer des opérations internes courantes. Incidents ou problèmes causés par le service qui ont un impact significatif sur les opérations internes courantes.
4	Incidents ou problèmes liés au service qui interrompent ou empêchent un utilisateur individuel d'effectuer des opérations internes courantes. Incidents ou problèmes causés par le service qui ont un impact mineur sur les opérations internes courantes.

5. Droits d'Utilisation et Informations de Facturation

5.1 Unités de mesure des redevances

Le Service Cloud est disponible en fonction de l'unité de mesure de redevance indiquée dans le Document de Transaction :

- a. **Utilisateur Autorisé** : unité de mesure par laquelle le Service Cloud peut être acquis. Le Client doit se procurer des droits d'utilisation distincts et dédiés pour chaque Utilisateur Autorisé unique ayant reçu l'accès au Service Cloud directement ou indirectement (par exemple, via un logiciel de multiplexage, un périphérique ou un serveur d'applications), par quelque moyen que ce soit. Des Droits d'Utilisation suffisants doivent être obtenus pour couvrir le nombre d'Utilisateurs Autorisés ayant accès au Service Cloud pendant la période de mesure indiquée dans l'Autorisation d'Utilisation ou le Document de Transaction du Client.
- b. **Gigaoctet** : unité de mesure par laquelle le Service Cloud peut être acquis. Un Gigaoctet représente 2 puissance 30 d'octets de données (soit 1 073 741 824 octets). Des droits d'utilisation suffisants sont nécessaires pour couvrir le nombre total de Gigaoctets traités par le Service Cloud pendant la période de mesure indiquée dans l'Autorisation d'Utilisation ou le Document de Transaction du Client.

- c. **Unité Client Gérée** : unité de mesure par laquelle le Service Cloud peut être acquis. Une Unité Client est un système informatique utilisateur unique ou un capteur spécial ou une unité de télémétrie demandant l'exécution de, ou recevant à des fins d'exécution, un ensemble de commandes, de procédures ou d'applications à partir de ou fournissant des données à un autre système informatique qui est généralement désigné par serveur ou géré par le serveur. Plusieurs Unités Client peuvent partager l'accès à un serveur commun. Une Unité Client peut être dotée de certaines fonctionnalités de traitement ou peut être programmable afin de permettre à un utilisateur d'effectuer le travail. Le Client doit se procurer des droits d'utilisation pour chaque Unité Client gérée par le Service Cloud pendant la période de mesure indiquée dans l'Autorisation d'Utilisation ou le Document de Transaction du Client.
- d. **Unité Client** : unité de mesure par laquelle le Service Cloud peut être acquis. Une Unité Client est un système informatique utilisateur unique ou un capteur spécial ou une unité de télémétrie demandant l'exécution de, ou recevant à des fins d'exécution, un ensemble de commandes, de procédures ou d'applications à partir de ou fournissant des données à un autre système informatique qui est généralement désigné par serveur ou géré par le serveur. Plusieurs Unités Client peuvent partager l'accès à un serveur commun. Une Unité Client peut être dotée de certaines fonctionnalités de traitement ou peut être programmable afin de permettre à un utilisateur d'effectuer le travail. Le Client doit se procurer des Droits d'Utilisation pour chaque Unité Client qui exécute le Service Cloud, lui fournit des données, utilise des services fournis par le Service Cloud ou autrement accède au Service Cloud pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (ou « PoE ») ou le Document de Transaction du Client.

5.2 Redevances Mensuelles Partielles

Une Redevance Mensuelle Partielle, comme indiqué dans le Document de Transaction, peut être estimée au prorata.

5.3 Redevances de dépassement

Si l'utilisation réelle du Service Cloud pendant la période de mesure dépasse les droits indiqués dans l'Autorisation d'Utilisation, le Client sera facturé pour l'excédent, comme indiqué dans le Document de Transaction.

6. Durée et Options de Renouvellement

La durée du Service Cloud commence à la date à laquelle IBM notifie au Client que ce dernier a accès au Service Cloud, comme décrit dans l'Autorisation d'Utilisation. L'Autorisation d'Utilisation indiquera si le Service Cloud est renouvelé automatiquement, s'il se poursuit en continu ou s'il prend fin à l'issue de la durée.

6.1 Renouvellement automatique

Pour un renouvellement automatique, le Service Cloud est automatiquement renouvelé pour la durée indiquée dans l'Autorisation d'Utilisation, sauf si le Client notifie par écrit, avant la date d'expiration de la durée, son intention de ne pas renouveler.

LA QUANTITÉ D'AUTORISATIONS DE RENOUVELLEMENT SERA ÉGALE A LA VALEUR LA PLUS ÉLEVÉE ENTRE LA QUANTITÉ DE COMMANDES D'ORIGINE OU L'UTILISATION MENSUELLE SIGNALÉE POUR LE MOIS AVANT LA GÉNÉRATION DE LA FACTURE DE RENOUVELLEMENT, SAUF SI IBM REÇOIT UNE NOTIFICATION INDIQUANT UNE QUANTITÉ D'AUTORISATIONS DIFFÉRENTE.

LA QUANTITÉ D'AUTORISATIONS DE RENOUVELLEMENT POUR L'OFFRE STEP UP SERA ÉGALE A LA QUANTITÉ DE COMMANDES D'ORIGINE.

6.2 Facturation continue

Pour une utilisation en continu, le Service Cloud continuera d'être disponible mois par mois jusqu'à ce que le Client notifie la résiliation moyennant un préavis écrit de 90 jours. Le Service Cloud demeure disponible jusqu'à la fin du mois suivant ladite période de 90 jours.

7. Logiciel d'Activation

Ce Service Cloud comprend des logiciels d'activation, qui ne doivent être utilisés qu'en rapport avec l'utilisation du Service Cloud par le Client et uniquement pendant la durée du Service Cloud.

8. Informations Complémentaires

8.1 Limitation de l'Offre Step up

Pour les offres de Service Cloud désignées par « Step up for existing Customers » (« Step up SaaS »), le Client doit avoir acquis au préalable ou simultanément des autorisations de licence appropriées du logiciel IBM associé, comme identifié dans le nom de l'Offre Step up SaaS. Par exemple, le Client qui achète « IBM MobileFirst Protect – Devices (SaaS) Step up for existing customers » doit disposer d'autorisations de licence pour le logiciel IBM associé d'IBM MobileFirst. Les droits d'accès du Client à l'Offre Step up SaaS ne peuvent pas dépasser les droits d'accès du Client au logiciel IBM associé.

Lors de l'acquisition de l'Offre Step up SaaS, le Client n'est pas autorisé à utiliser les mêmes autorisations de licence du logiciel IBM associé dans son environnement installé sur site qu'avec les droits d'accès à l'Offre Step up SaaS. Par exemple, si le Client dispose de 250 droits d'utilisation d'Unité Client Gérée pour le logiciel IBM associé et qu'il choisit d'acquérir 100 droits d'utilisation d'Unité Client Gérée Step up SaaS, le Client peut gérer 100 Unités Client Gérées Step up SaaS à partir de l'environnement du Service Cloud et 150 Unités Client Gérées à partir du logiciel installé sur site.

Le Client déclare qu'il a acquis (1) les autorisations de licence applicables et (2) l'Abonnement et le Support du(es) Logiciel(s) IBM associé(s). Pendant la période d'abonnement à l'Offre Step up SaaS, le Client doit tenir à jour l'Abonnement et le Support pour les autorisations d'utilisation de logiciel IBM utilisées conjointement avec les autorisations d'utilisation de l'Offre Step up SaaS. En cas de résiliation de la licence d'utilisation du(es) logiciel(s) IBM associé(s) du Client ou de son Contrat d'Abonnement et de Support pour le(s) logiciel(s) IBM associé(s), son droit d'utilisation de l'Offre Step Up SaaS prend fin.

8.2 Cookies

Le Client accepte qu'IBM puisse utiliser des cookies et des technologies de suivi permettant de rassembler des informations identifiant une personne, dans le cadre de la collecte de statistiques et d'informations d'utilisation conçues pour aider à améliorer l'acquis utilisateur et/ou pour personnaliser les interactions avec les utilisateurs conformément au site <http://www-01.ibm.com/software/info/product-privacy/index.html>.

8.3 Informations personnelles sur la Santé Interdites

Le Service Cloud n'est pas conçu pour être conforme à la loi HIPAA et ne doit pas être utilisé pour la transmission et le stockage des informations personnelles sur la santé.

8.4 Données Normatives

Nonobstant toute disposition contraire, uniquement à des fins de recherche normative, d'analyse, de démonstration et de production de rapports, IBM est autorisée à conserver et utiliser au format anonyme et agrégé (de sorte que le Client ou les utilisateurs autorisés du Client ne puissent pas être identifiés comme source des données et que les informations personnelles permettant l'identification du Client ou des utilisateurs autorisés du Client soient supprimées) les données reflétant les expériences individuelles des utilisateurs autorisés du Client avec les Services Cloud.

8.5 Utilisation et Autorisation Légales

8.5.1 Autorisation de Collecte et de Traitement de Données

Le Service Cloud est conçu pour mettre à disposition, gérer, surveiller et contrôler des appareils mobiles. Il collectera des informations auprès des utilisateurs et des unités qui sont autorisés par le Client à interagir avec le Service Cloud auquel le Client a souscrit. Le Service Cloud collecte des informations qui, seules ou conjointement, peuvent être considérées comme Informations Personnelles dans certaines juridictions. Les données collectées peuvent inclure le nom, le numéro de téléphone, l'adresse e-mail enregistrée et l'emplacement de l'appareil de l'utilisateur autorisé, l'historique de la navigation et des ID utilisateur du navigateur MaaS360, des informations relatives au matériel, aux logiciels et aux paramètres de l'appareil de l'utilisateur final, ainsi que des informations générées par l'appareil. Le Client autorise IBM à collecter, traiter et utiliser ces informations conformément aux dispositions du présent Descriptif de Services.

8.5.2 Consentement en Connaissance de Cause des Personnes Concernées

L'utilisation du Service Cloud peut être soumise à diverses lois et réglementations. Le Service Cloud ne peut être utilisé qu'à des fins légales et de manière légale. Le Client s'engage à utiliser le Service Cloud conformément aux lois, règlements et réglementations applicables et assume toutes les responsabilités relatives au respect desdites lois, règlements et réglementations.

Le Client convient qu'il a obtenu ou qu'il obtiendra tous les consentements, autorisations ou licences en pleine connaissance de cause, nécessaires pour permettre l'utilisation légale des Services Cloud et pour permettre la collecte et le traitement des informations par IBM en tant que sous-traitant du traitement des données du Client par le biais du Service Cloud. Le Client autorise IBM par les présentes à obtenir des consentements en pleine connaissance de cause, nécessaires pour permettre l'utilisation légale du Service Cloud et pour collecter et traiter les informations décrites dans le contrat de licence d'utilisateur final disponible sur le site <http://www.ibm.com/software/sla/sladb.nsf/>.

8.6 Conservation des Données

IBM supprimera toute information collectée pouvant inclure des Informations Personnelles à l'expiration ou la résiliation du présent Descriptif de Services, à l'exception des informations devant être conservées pour les raisons citées plus haut ou conformément à une loi, règle ou réglementation applicable. Dans ce cas, IBM conservera les informations collectées pendant la durée requise par ladite cause, loi, règle ou réglementation applicable.

8.7 Confidentialité des Données

8.7.1 Transferts hors du Territoire

Si le Client communique des Informations Personnelles aux Services IBM Cloud dans les États Membres de l'Union Européenne, en Islande, au Liechtenstein, en Norvège, en Suisse ou en Turquie et tout autre pays européen disposant d'une législation protégeant la confidentialité des données, le Client accepte qu'IBM traite le Contenu, y compris toutes données personnelles, en vertu des lois et obligations applicables, hors du territoire à destination de sous-traitants ou sous-traitants ultérieurs du traitement des données dans les pays suivants hors de l'Espace Économique Européen et dans les pays considérés par la Commission Européenne comme ayant des niveaux de sécurité adéquats :

Nom du Sous-traitant/Sous-traitant ultérieur du traitement des données	Rôle (Sous-traitant/Sous-traitant ultérieur du traitement des données)	Etablissement
IBM Corporation	Sous-traitant ultérieur du traitement de données	1 New Orchard Rd. Armonk, NY 10504, USA I
IBM India Private Limited	Sous-traitant ultérieur du traitement de données	No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 Inde

Le Client accepte qu'IBM puisse, sur préavis, modifier cette liste de pays d'implantation lorsqu'elle juge cela raisonnablement nécessaire pour la fourniture des Services Cloud.

8.7.2 Confidentialité des Données dans l'Union Européenne

Si le Client communique des données personnelles aux Services IBM Cloud dans les États Membres de l'Union Européenne, en Islande, au Liechtenstein, en Norvège, en Suisse ou en Turquie et tout autre pays européen disposant d'une législation protégeant la confidentialité des données, ou si le Client dispose d'unités ou d'utilisateurs autorisés dans ces pays, le Client, en tant que seul responsable du traitement désigne IBM en tant que sous-traitant du traitement des données pour traiter (ces termes étant définis dans la Directive EU 95/46/EC) les Informations Personnelles. IBM ne traitera ces Informations Personnelles que dans les limites requises pour mettre à disposition l'offre de Services IBM Cloud conformément aux descriptions publiées d'IBM des Services IBM Cloud et le Client accepte que ledit traitement est conforme aux instructions du Client.

8.8 Données de Sécurité

Dans le cadre du Service Cloud, qui comprend des activités de production de rapport, IBM préparera et gèrera les informations anonymes et/ou cumulées extraites du Service Cloud (« Données de Sécurité »). Sauf disposition contraire stipulée dans le paragraphe (d) ci-dessous, les Données de Sécurité n'identifieront pas le Client ou un individu. En outre, le Client accepte par les présentes qu'IBM puisse utiliser et/ou copier les Données de Sécurité uniquement aux fins suivantes :

- publication et/ou distribution des Données de Sécurité (par exemple, dans les compilations et/ou analyses liées à la cybersécurité) ;
- développement ou amélioration des produits ou services ;
- réalisation d'étude en interne ou auprès de tiers ; et
- partage légal des informations confirmées relatives à un contrevenant tiers.