IBM Trusteer Pinpoint Verify

Ce Descriptif de Services détaille le Service Cloud. Les bons de commande applicables contiennent les prix et des détails supplémentaires concernant la commande du Client.

1. Service Cloud

IBM Trusteer Pinpoint Verify est doté de Step-Authenticate, une authentification renforcée qui peut être lancée sur certains cas à haut risque pour garantir que les interactions numériques sécurisées sont protégées par Pinpoint. Cela pallie le risque lorsque Trusteer prévoit un risque d'activité frauduleuse intentionnelle ou lorsque l'activité d'utilisateur nécessite un niveau d'assurance d'identité plus élevé.

1.1 Offres

1.1.1 IBM Trusteer Pinpoint Verify

Le Client doit tenir à jour son abonnement à IBM Trusteer Pinpoint Detect ou IBM Trusteer Pinpoint Assure avant de s'abonner à ce Service Cloud.

Ce Service Cloud offre des fonctionnalités demandant aux utilisateurs de s'authentifier pour un second facteur d'authentification afin de vérifier leur identité lorsqu'ils accèdent à un service numérique. Il est disponible pour Pinpoint Detect et Pinpoint Assure, afin de fournir une authentification à deux facteurs pour les applications protégées. La décision déterminant à quel moment demander aux utilisateurs une authentification à deux facteurs est générée par l'application protégée et peut être fondée sur les recommandations renvoyées par les plateformes Pinpoint Detect ou Pinpoint Assure ou toute autre politique définie par l'application protégée. Ce Service Cloud est géré par la technologie IBM Cloud Identity Verify.

2. Fiches Techniques sur le Traitement et la Protection des Données

L'Addendum d'IBM relatif au Traitement de Données à caractère personnel, disponible sur http://ibm.com/dpa (DPA) et la ou les Fiches Techniques (désignées par fiche(s) technique(s) ou Annexe(s) DPA) dans les liens ci-dessous contiennent des informations additionnelles sur la protection des données pour les Services Cloud et leurs options concernant les types de Contenus pouvant être traités, les activités de traitement impliquées, les dispositifs de protection des données et les détails de conservation et de retour de Contenu. Le DPA s'applique aux Données à caractère personnel du Contenu dans la mesure où i) Le Règlement Général sur la Protection des Données (UE/2016/679) (RGPD) ; ou ii) d'autres lois relatives à la protection des données identifiées sur http://ibm.com/dpa/dpl s'appliquent.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=D7AB2D30CB2C11E99CFB3A1B59E5A549

3. Niveaux de Service et Support Technique

3.1 Accord Relatif aux Niveaux de Service

IBM fournit au Client l'Accord relatif aux Niveaux de Service (« SLA ») de disponibilité ci-dessous. IBM appliquera le dédommagement correspondant le plus élevé, en fonction de la disponibilité cumulée du Service Cloud, comme indiqué dans le tableau ci-dessous. Le pourcentage de disponibilité est calculé comme suit : le nombre total de minutes d'un mois contractuel moins le nombre total de minutes d'indisponibilité du Service au cours du mois contractuel, divisé par le nombre total de minutes du mois contractuel. La définition de l'indisponibilité du Service, la procédure de réclamation et les moyens de contacter IBM concernant les problèmes de disponibilité de service figurent dans le guide de support de Services Cloud d'IBM à l'adresse https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilité	Avoir (% de redevance d'abonnement mensuelle*)
Inférieure à 99,9 %	2 %
Inférieure à 99,0 %	5 %
Inférieure à 95,0 %	10 %

* La redevance d'abonnement est le prix contractuel pour le mois objet de la réclamation.

3.2 Support Technique

Le support technique destiné au Service Cloud, y compris les coordonnées des personnes à contacter, les niveaux de gravité, les heures de disponibilité, les temps de réponse ainsi que d'autres informations et processus relatifs au support technique sont disponibles en sélectionnant le Service Cloud dans le guide de support IBM disponible à l'adresse https://www.ibm.com/support/home/pages/support-guide/.

4. Montant des Redevances

4.1 Unités de mesure des redevances

Les unités de mesure des redevances du Service Cloud sont indiquées dans le Document de Transaction.

Les unités de redevances suivantes s'appliquent à ce Service Cloud :

- Un Participant Admissible est un individu ou une entité habilitée à prendre part à un programme de prestation de service géré ou suivi par les Services Cloud.
- Une Connexion est une liaison ou une association d'une base de données, d'un serveur, d'une application ou de tout autre type de périphérique mis ou qui a été mis à disposition des Services Cloud.

5. Dispositions Additionnelles

Pour les Contrats de Services Cloud (ou des contrats Cloud de base équivalents) signés avant le 1er janvier 2019, les dispositions énoncées à l'adresse https://www.ibm.com/acs s'appliquent.

5.1 Solutions Intégrées

A des fins d'éclaircissement, les diverses offres sous la marque Trusteer peuvent constituer une solution intégrée. Par conséquent, si le Client résilie l'un des présents Services Cloud, IBM peut conserver les données du Client en vue de fournir au Client les Services Cloud restants ainsi que d'autres services Trusteer, conformément aux descriptions de service applicables à ces autres services Trusteer.

6. Dispositions dérogatoires

6.1 Utilisation de Données

La disposition suivante prévaut sur toute disposition contraire dans la clause « Contenu et protection des données » des conditions cadre de Service Cloud entre les parties : IBM n'utilisera ou ne communiquera pas les résultats découlant de l'utilisation du Service Cloud par le Client qui sont exclusivement liés au Contenu (Observations) du Client ou qui identifient le Client de quelque autre manière. IBM utilisera cependant le Contenu et d'autres informations issues du Contenu (à l'exception des analyses) dans le cadre du Service Cloud en vue d'améliorer le Service Cloud. IBM peut également partager des identificateurs de menaces et d'autres informations de sécurité intégrées au Contenu à des fins de détection des menaces et de protection.