Description de service pour
Services de communications unifiées en tant que service (UCaaS), par Cisco UCM dans le nuage
à l'intention des partenaires

Ce document (cette « **Description de service** ») décrit les fonctionnalités de service, les composants et les conditions des services gérés (« **Services** ») qui seront achetés par le partenaire auprès de Cisco pour un ou plusieurs clients finaux afin de prendre en charge Cisco Unified Communications Manager dans le nuage (« **UCM dans le nuage** »). La quantité et le type de Services spécifiques achetés par le partenaire seront précisés par écrit dans un document de commande convenu entre les parties. L'Annexe A à cette Description de service décrit les conditions applicables en matière de Services.

Cette Description de service, ainsi que le ou les documents de commande correspondants, est intégrée dans le contrat entre le partenaire et Cisco qui régit la prestation des services Cisco par le partenaire pour les clients finaux (le « **Contrat** »).

Résumé du service

- Cette description de service est destinée à être lue conjointement avec la description du service UCM dans le nuage de Cisco, qui décrit les conditions générales applicables à UCM dans le nuage et qui est disponible à l'adresse : https://www.Cisco.com/c/en/US/solutions/Collateral/collaboration/Unified-Communications-Manager-Cloud/salestool-C96-742547.html. Afin d'acheter les Services, le partenaire doit également acheter un abonnement à UCM dans le nuage et les services achetés par le partenaire pour un client final seront synchronisés avec la durée de l'abonnement à UCM dans le nuage du client final.
- Ces services se composent de la surveillance, de la gestion et du dépannage des applications UCM dans le nuage de base spécifiques à la configuration du client incluant les passerelles téléphoniques Cisco et, le cas échéant, certaines intégrations ou applications tierces utilisées dans le cadre d'UCM dans le nuage et identifiées dans le document de commande pour le client final concerné (dans le cadre de cette Description de service, les « **Composants gérés** »), ainsi que d'autres services en option pour soutenir l'utilisation d'UCM dans le nuage par le client final. Les services offerts sont fondés sur les pratiques recommandées de la bibliothèque d'infrastructures des technologies de l'information (Information Technology Infrastructure Library ou ITIL).
- Sauf s'il est expressément indiqué qu'ils sont fournis autrement, tous les Services seront fournis à distance par des centres d'exploitation de réseaux (Network Operations Centers ou NOC) mondiaux en utilisant le modèle de prestation continue et tous les Services seront fournis 24 heures sur 24, tous les jours de l'année, à moins d'indication contraire.
- Si elle est spécifiée dans le document de commande applicable, cette Description de service sera considérée comme incorporant, par référence, un ou plusieurs des suppléments suivants pour les Services gérés de Cisco : collaboration dans le centre de contact, collaboration vidéo ou collaboration vocale.

Tableau récapitulatif : Les tableaux suivants récapitulent les composants des Services et les Services facultatifs disponibles.

Composants des Services Sélect	Composants facultatifs du Services**
Transition du Service – Planification et prise en charge*	Responsable de la prestation des services orientés clients
Transition du service – Activation de Composant géré*	Exécution des demandes de services
Portail	Portail d'exécution des services
Gestion des stocks de ressources de services	Gestion des Composants gérés par des tiers
Services de sauvegarde et de restauration	Liaison intelligente pour CMS
Gestion d'événements	Plate-forme de services gérés de Cisco sur site pour un CPE
Gestion des incidents	
Gestion du changement	
Gestion des problèmes	
Responsable de la prestation des services	
Tableaux de bord et production de rapports à la demande	
Prise en charge du plan de numérotation	
Prise en charge de Cisco Emergency Responder	

* selon les besoins en fonction des composants de service ** frais supplémentaires applicables

Composants de services

Vous trouverez ci-dessous une description des services standards inclus dans le cadre des Services, dans la mesure applicable, en fonction des composants de service mentionnés dans le document de commande correspondant. Comme indiqué ci-dessous, certains composants de service peuvent ne pas être applicables à un client final donné.

Transition du service – planification et assistance (*applicable uniquement dans les limites convenues et décrites dans un document de commande*).	
Résumé : Le cas échéant, Cisco et le partenaire collaboreront pour fournir des informations sur l'étendue des services, notamment pour identifier les Composants gérés répertoriés dans le document de commande applicable et pour définir les exigences et planifier l'établissement de la connectivité entre Cisco et les Composants gérés. Pour plus d'informations, consultez la section 2.3 de l'Annexe A (*Conditions pour les services gérés*).	
Responsabilités de Cisco • Héberger et organiser une réunion de lancement par téléphone ou par conférence Web. • Définir le champ d'application global des travaux nécessaires pour convertir les composants applicables en Composants gérés, incluant l'évaluation des modifications à la plate-forme, au réseau et aux processus du client nécessaires pour activer les Composants gérés. • Définir les renseignements sur les stocks nécessaires et les exigences relatives à la topologie pour activer les Composants gérés. • Définir un interlocuteur unique (single point of contact ou SPOC) qui collaborera avec le client pendant la transition du Service. • Effectuer dans les temps définis dans le plan de transition les tâches identifiées comme étant une responsabilité de Cisco.	**Responsabilités du Partenaire** • À moins d'un avis contraire présent dans un accord écrit, fournir les informations relatives au stock et à la topologie faisant l'objet d'une demande raisonnable en respectant les dates fournies dans le plan de transition. • Passer en revue et approuver le plan de transition, notamment la ou les dates d'activation. • Désigner un interlocuteur unique qui collaborera avec Cisco pendant la transition du Service. • Effectuer les tâches identifiées comme étant une responsabilité du partenaire, et s'assurer que le client final a effectué les tâches identifiées comme étant une responsabilité du client final dans le plan de transition, à la date indiquée dans le plan de transition.
Livrable : Plan de transition	

Transition du Service – Activation d'un Composant géré (*applicable uniquement dans l'étendue convenue et décrite dans un document de commande*).	
Résumé : Le cas échéant, avec l'aide du partenaire, Cisco connectera les Composants gérés au centre d'exploitation des réseaux (NOC) de Cisco, effectuera des tests pour vérifier que les Composants gérés sont prêts pour la surveillance, la gestion et le dépannage à distance, et activera les Composants gérés sur la plate-forme des services gérés de Cisco (Cisco Managed Services Platform ou CMSP).	
Responsabilités de Cisco • Fournir au partenaire un point d'extrémité VPN (matériel ou logiciel) avec des instructions pour l'installation et la configuration du point d'extrémité. • Concevoir, mettre en œuvre et vérifier les fonctionnalités de gestion bidirectionnelles. • Fournir au partenaire des conseils généraux sur les activités de stabilisation requises pour permettre l'activation. • Intégrer ou retirer des Composants gérés, selon le ou les documents de commande applicables et les instructions du partenaire. • Mettre en œuvre la plate-forme des services gérés de Cisco (CMSP) et effectuer des tests pour vérifier que les Composants gérés sont activés et prêts à être gérés. • Signaler la réalisation de l'activation au partenaire. • Fournir au partenaire un brouillon de dossier d'exploitation.	**Responsabilités du Partenaire** • Installer et configurer un point d'extrémité VPN au niveau du ou des emplacements du client final conformément à sa documentation. • À moins que Cisco n'effectue des services d'installation, effectuer les installations matérielles ou logicielles requises, les modifications de configuration et d'autres activités de stabilisation nécessaires pour activer la connectivité et la communication entre les Composants gérés et CMSP. • Aider Cisco à établir et valider les fonctionnalités de gestion bidirectionnelle entre les Composants gérés et CMSP. • Au besoin, examiner et contrôler la préparation des tests et des résultats de Cisco. • Passer en revue et approuver les éléments spécifiques au client et au partenaire dans le dossier d'exploitation.
Livrables : Premier jet du dossier d'exploitation, inventaire initial des Composants gérés, demande de modification, au besoin.	

Portail
Résumé : Cisco fournira au partenaire un portail sécurisé pour lui permettre de consulter son tableau de bord, placer des demandes de rapports et des requêtes (p. ex., MACD). Pour des raisons de sécurité, le Portail est uniquement accessible par le tunnel VPN de Cisco et n'est pas accessible par l'Internet public. Cisco offrira au partenaire la possibilité de créer et d'administrer des comptes pour leurs utilisateurs autorisés. Les demandes envoyées par le partenaire sont considérées comme étant autorisées par le partenaire.

Gestion des stocks de ressources de services
Résumé : Cisco recueillera et tiendra à jour les renseignements sur les stocks des Composants gérés et de l'environnement connexe (excluant les actifs UCM dans le nuage de Cisco). Cisco rendra ces informations disponibles par l'entremise du portail ou suite à une demande écrite.
Livrable : Liste des Composants gérés et informations sur l'environnement.

Services de sauvegarde et de restauration	
Résumé : Si cette fonctionnalité est prise en charge par les Composants gérés, Cisco effectuera une sauvegarde des paramètres de configuration des Composants gérés (mais pas du contenu des Composants gérés) et restaurera ces données si nécessaire pour le maintien des Services ou en réponse à une demande de service.	
Responsabilités de Cisco • Fournir les exigences de stockage pour la sauvegarde. • Effectuer, vérifier et documenter dans CMSP que la sauvegarde est effectuée en fonction de la planification applicable. • Avertir le partenaire si la sauvegarde ne s'exécute pas comme prévu ou si Cisco remarque une erreur ou une défaillance de la sauvegarde. • Dans le cadre de la gestion d'incident ou du changement, restaurer le fichier de configuration et de paramètres des Composants gérés applicables en utilisant la dernière configuration correcte connue.	**Responsabilités du Partenaire** • Fournir de l'espace local pour les fichiers de sauvegarde. • S'assurer que les fichiers de sauvegarde répondent aux exigences de conservation. • S'assurer que Cisco dispose d'un accès 24 heures par jour et tous les jours de l'année aux fichiers de sauvegarde en cas de nécessité d'une restauration. • Effectuer la maintenance des fichiers de sauvegarde. • Fournir toutes les informations d'identification nécessaires (telles que définies dans le guide d'intégration) pour permettre à Cisco d'effectuer les sauvegardes. • Effectuer toutes les tâches spécifiées dans le processus du CAB (Change Advisory Board). • Fournir des moyens permettant à Cisco d'accéder aux applications et au matériel concernés et d'y apporter des modifications. • Faciliter la disposition post-activation des enregistrements de modification. • Déterminer toutes les dépendances pour les composants, les logiciels et les services non couverts. • Définir et garantir des fenêtres d'entretien avec le client final. • Effectuer toutes les tâches spécifiées dans le processus CAB (Change Advisory Board). • Faciliter la disposition post-activation des enregistrements de modification. • Déterminer toutes les dépendances pour les composants, les logiciels et les services non couverts. • Effectuer une sauvegarde des Composants gérés qui ne peuvent pas être sauvegardés par Cisco (p. ex., des Composants gérés par des tiers).
Livrable : Sauvegarde des paramètres des Composants gérés, qui seront stockés par le partenaire.	

Gestion d'événements
Résumé : Cisco surveillera les événements affectant les Composants gérés.
Responsabilités de Cisco • Créer et mettre en œuvre des règles de gestion des événements (p. ex., seuils de déclenchement). • Détecter si un événement s'est produit au niveau des Composants gérés en surveillant le syslog, les messages d'alerte SNMP, les indicateurs de performance clés (KPI) et les alertes de franchissement des seuils (AFS). • Aider au repérage des événements significatifs par la création de règles de filtrage et de corrélation. • Lorsqu'un événement se produit, mettre en œuvre la corrélation, le filtrage et la chronométrie des événements à l'aide des règles de gestion des événements.
Livrables : Réglages des règles de franchissement des seuils, règles de filtrage et de corrélation.

Gestion des incidents	
Résumé : Cisco participera à l'identification, au dépannage et à la remise en route des Composants gérés si un incident est détecté ou signalé par le partenaire.	
Responsabilités de Cisco • Créer des tickets pour les événements détectés ou signalés. • Gérer les incidents en classant, en hiérarchisant, en dépannant et en restaurant le fonctionnement des Composants gérés, ou en fournissant des recommandations pour la résolution de l'incident. • Attribuer et réévaluer les priorités des incidents conformément à la procédure définie dans l'Annexe A de la présente Description de service. • Avertir les parties concernées des incidents et les tenir informées jusqu'à ce que l'Incident soit résolu. • Fournir des rapports sur les incidents relatifs aux Composants gérés. • Formuler des recommandations pour résoudre un incident si la cause du problème ne relève pas de Cisco.	**Responsabilités du Partenaire** • Fournir les détails sur les contrats d'assistance et les autres documents ou autorisations requises pour simplifier la résolution de l'Incident. • Communiquer avec Cisco si le partenaire pense qu'un incident est en cours ou s'est produit, conformément au dossier d'exploitation. • Si les changements ne peuvent pas être effectués par Cisco ou s'ils ne relèvent pas de Cisco, mettre en œuvre les changements que Cisco ou une tierce partie a recommandés sur les Composants gérés ou sur le matériel, les logiciels ou les services tiers.
Livrables : Ticket d'incident, demande de modification pour résoudre l'incident, recommandation visant à résoudre l'incident**.**	

Gestion du changement	
Résumé : Cisco gérera le déploiement des changements techniques apportés aux Composants gérés (p. ex., les modifications de configuration) dans l'environnement du client final. Les types de changements pris en charge par la gestion du changement sont les changements d'urgence, les changements normaux, les changements spéciaux, les changements standards et les changements informationnels.	
Responsabilités de Cisco • Gérer le cycle de vie des demandes de gestion des modifications (par exemple, planification, test, réécriture, etc.) résultant d'un incident, d'un problème, d'une demande de service ou d'un accord écrit mutuel. • Coordonner et effectuer les changements aux Composants gérés en utilisant des efforts commerciaux raisonnables pour limiter les effets négatifs de ces changements sur l'environnement du client final. • Valider et hiérarchiser les demandes de modification en fonction de l'urgence, y compris les notifications de l'équipe de gestion des informations sur la sécurité des produits Cisco (Product Security Information Response Team ou PSIRT), le cas échéant. • Fournir du personnel qui participera à des réunions de CAB à raison d'un maximum de deux heures par semaine. • Identifier et recommander des modifications à apporter aux Composants gérés. • Avertir de la mise en œuvre et de la complétion des demandes de changement pour les changements affectant le client final. • Suivre la procédure de gestion du changement, comme il est décrit dans le Dossier d'exploitation. • Effectuer un contrôle de l'état de fonctionnement avant et après les changements.	**Responsabilités du Partenaire** • Signalez à Cisco les modifications apportées aux informations, ainsi que les mises à jour et les modifications prévues dans l'environnement du client final qui peuvent avoir un impact sur les Services. • Envoyer des demandes de modification (request for change ou RFC) en tant que demandes de service, modifications d'informations ou incidents à l'aide de la méthode approuvée. • Passer en revue, mettre en œuvre et exécuter les Demandes de changement initiées par Cisco, conformément à ses directives, comme décrit dans la Demande de changement. • Suivre la procédure de gestion du changement, comme il est décrit dans le Dossier d'exploitation. • Consulter Cisco au sujet des procédures de planification, de communication et de mise en œuvre des changements. • Inviter Cisco aux réunions de CAB et faciliter la communication entre Cisco et le CAB. • Identifier et limiter toutes les incidences sur les composants uniquement surveillés ou non couverts induites par un changement apporté aux Composants gérés. • Examiner et approuver rapidement les modifications en fonction de l'urgence de la demande. • Effectuer et aider Cisco dans l'exécution de toutes les tâches convenues par écrit via le processus de CAB.
Livrables : Recommandations relatives aux modifications, aux demandes de changement, à la planification des changements et à l'enregistrement des changements.	

Gestion des problèmes	
Résumé : Cisco analysera les incidents après la restauration pour identifier la cause première des incidents P1, ou des incidents récurrents similaires P2 (tels que définis dans l'Annexe B). Cisco effectuera de manière proactive des activités visant à identifier et à résoudre les problèmes avant que les incidents ne se produisent. Les activités proactives incluent notamment : l'analyse des tendances, les contrôles de fonctionnement et le réglage de la plate-forme.	
Responsabilités de Cisco • Créer un enregistrement du problème et analyser les événements (par exemple, les dépassements de seuils) et les incidents afin d'identifier les tendances ou les erreurs à partir des critères ci-dessus. • Effectuer des analyses prédictives afin de déterminer la source du problème. • Comparer aux enregistrements de problèmes les notifications élevées et critiques de l'équipe de gestion des informations sur la sécurité des produits Cisco (PSIRT), les vulnérabilités de sécurité de Cisco, les bases de données d'erreurs connues et les notifications sur le terrain. • Déterminer la correction pour les notifications de l'équipe de gestion des informations sur la sécurité des produits Cisco (PSIRT). • Fournir au partenaire des recommandations exploitables pour résoudre le problème et réduire ou éliminer les incidents résultant de ce problème. • Mettre en œuvre des modifications pour résoudre les problèmes selon la gestion des modifications. • Tenir à jour des enregistrements de problèmes afin de déterminer si la mesure prise a permis de résoudre le problème.	**Responsabilités du Partenaire** • Le cas échéant, collaborer avec des fournisseurs tiers pour résoudre les situations dans les cas où un Composant géré par un tiers ou un composant uniquement surveillé est la cause du problème. • Mettre en œuvre les changements recommandés par Cisco. • Approuver les recommandations de correction des notifications EIISP de Cisco. • Le cas échéant, collaborer avec des fournisseurs tiers pour résoudre les situations ou les cas d'incompatibilité dans lesquels un Composant géré par un tiers ou un périphérique tiers est à l'origine du problème. • Mettre en œuvre tous les changements recommandés par Cisco ou par une tierce partie, mais qui ne sont pas couverts par le Service ni contrôlés par Cisco. • Déterminer et limiter les impacts sur les périphériques uniquement surveillés ou non couverts à la suite des mises à niveau requises pour les nouvelles versions d'applications ou le noyau d'UCM dans le nuage ou d'autres modifications apportées aux Composants gérés.
Livrables : Demande de modification, enregistrement de changement, enregistrement de problème, recommandations pour résoudre un incident ou un problème.	

Responsable de la prestation des services	
Résumé : Dans le cadre des Services et pour garantir la qualité du service et confirmer que les processus de prestation du service sont en place, Cisco nommera un responsable de la prestation des services. Cet individu fournira une assistance directement au partenaire pour tous les clients finaux qui lui sont associés. Le responsable de la prestation des services n'interagira pas directement avec les clients finaux.	
Responsabilités de Cisco • Fournir un interlocuteur unique et un représentant de Cisco, afin d'aider les clients à atteindre leurs objectifs commerciaux. • Surveiller et gérer la prestation du service pour veiller au respect des	**Responsabilités du partenaire** • Désigner un interlocuteur de référence pour Cisco en lien avec les recours hiérarchiques, la résolution des problèmes commerciaux et les discussions portant sur les renouvellements des contrats.

obligations contractuelles. • Discuter de l'alignement des Services et des besoins de l'entreprise en constante évolution. • S'occuper des problèmes commerciaux, des renouvellements de contrats et des opportunités de croissance. • Mettre à jour le dossier d'exploitation pour s'assurer que les procédures opérationnelles sont documentées et actuelles.	• Désigner un représentant qui assistera à l'exécution des actions du partenaire en rapport avec les engagements de Cisco et qui sera chargé de les approuver. • Évaluer et approuver les mesures recommandées par Cisco, et effectuer les mises à jour relatives aux mesures antérieures.
Livrables : Recommandations, ordres du jour de réunion, préparation d'un premier jet des demandes de modification, rapports de performance.	

Tableaux de bord et production de rapports à la demande
Résumé : Cisco mettra à la disposition du partenaire la technologie et des tableaux de bord des entreprises et des rapports à la demande décrits dans le guide sur les rapports. Cisco mettra à disposition les rapports suivants, dont la liste peut être mise à jour occasionnellement : les rapports SLA et KPI, les rapports de disponibilité, les rapports sur l'adoption et l'utilisation, les rapports de gestion des incidents, les rapports de gestion des problèmes, les rapports de gestion des modifications et les rapports de gestion de la capacité.
Livrables : Tableaux de bord, rapports.

Prise en charge du plan de numérotation
Résumé : Cisco prendra en charge le plan de numérotation configuré dans le cadre de l'utilisation de UCM dans le nuage tel que décrit dans la description du service UCM dans le nuage de Cisco.

Prise en charge de Cisco Emergency Responder
Résumé : Cisco prendra en charge la fonctionnalité de répondeur d'urgence Cisco (Cisco Emergency Responder ou CER) configurée dans le cadre de l'UCM dans le nuage tel que décrit dans la Description de service de UCM dans le nuage de Cisco.

Composants facultatifs du Service

Un ou plusieurs des éléments suivants peuvent être achetés en tant qu'éléments de Service facultatifs, en plus de l'achat des Services :

Responsable des services orientés clients	
Résumé : Pour garantir la qualité du service et confirmer que les processus de prestation du service sont en place, Cisco nommera un responsable de la prestation des Services qui agira à titre d'interlocuteur unique pour le client final dans le cadre des Services.	
Responsabilités de Cisco	**Responsabilités du partenaire et du client final**
• Assigner un responsable des prestations (et une relève, le cas échéant) comme interlocuteur unique pour le fonctionnement quotidien des Services. • Fournir des ordres du jour et tenir des réunions mensuelles de gestion des opérations pour passer en revue et discuter des rapports, des performances de niveau de service, les données d'exploitation et de performance historiques et des tendances, et des risques opérationnels. • Fournir les ordres du jour et tenir des évaluations opérationnelles trimestrielles axées sur l'adoption des services, l'utilisation des fonctionnalités et les nouvelles fonctionnalités disponibles depuis la réunion précédente. • Effectuer toutes les tâches convenues par écrit suite à une réunion. • Mettre à jour le guide d'exploitation afin que les procédures opérationnelles soient documentées et alignées avec les pratiques existantes.	• Fournir un interlocuteur unique pour Cisco pour la réception et le fonctionnement quotidiens des Services. • Évaluer et approuver les mesures recommandées par Cisco, et effectuer les mises à jour relatives aux mesures antérieures. • Fournir un représentant pour participer et effectuer toutes les tâches convenues mutuellement par écrit suite à une réunion. • Évaluer, approuver les mesures recommandées et effectuer les mises à jour relatives aux mesures antérieures.
Livrables : Recommandations, ordres du jour de réunion, préparation d'un premier jet des demandes de modification, rapports de performance.	

Exécution des demandes de services	
Résumé : Cisco mettra en œuvre les demandes de service telles que décrites dans le catalogue des Services, ce qui consomme des unités de demande de service (Service Request Units ou SRU) du partenaire en fonction du coût des SRU tel qu'indiqué dans le catalogue de Services. Les types de demandes de service qui ne se trouvent pas dans le catalogue des Services seront évalués et feront l'objet d'un devis avant de continuer.	
Responsabilités de Cisco	**Responsabilités du partenaire**
• Mettre à disposition un portail sur lequel le partenaire peut soumettre des demandes de services et sur lequel Cisco peut classer, approuver, hiérarchiser et gérer les demandes de services. • Gérer les demandes de services durant les étapes de validation, d'exécution et de fermeture. • Traiter les demandes de services approuvées. • Traiter les Demandes de service urgentes en priorité pendant les heures de travail normales en fonction de la disponibilité et conformément au catalogue des Services.	• Créer des demandes de services. • Sur demande, confirmer que chaque demande de services a été satisfaite. • Fournir la liste des utilisateurs autorisés à soumettre des demandes de service. • Exécuter tous les changements physiques ou sur site à apporter aux Composants gérés faisant l'objet d'une demande raisonnable de Cisco afin de faciliter l'exécution des demandes de service. • Fournir des détails supplémentaires faisant l'objet d'une demande raisonnable concernant les demandes de service. • Hiérarchiser les demandes de service.

Livrables : Rapport de demande de service, catalogue de demandes de service.

Portail d'exécution des services	
Résumé : Cisco implantera une plate-forme Web de courtage de services infonuagiques. Le portail d'exécution des services propose trois fonctions au choix : un catalogue commercial, des flux de travail personnalisés et l'orchestration.	
Responsabilités de Cisco • Accorder au partenaire l'accès au portail d'exécution des services. • Configurer des flux de travail d'orchestration conformément aux listes convenues. • Configurer le catalogue d'entreprises du partenaire selon des listes convenues mutuellement. • Gérer les demandes de service conformément à des flux de travail jusqu'à l'exécution finale de telles demandes de service. • Communiquer des avis conformément au flux de travail d'orchestration applicable pour les demandes de service visées. • Autoriser la création de rapports pour le cycle d'exécution des Services du partenaire et pour l'inventaire des Services. • Fournir des rapports sur les demandes de service.	**Responsabilités du Partenaire** • Fournir une liste des utilisateurs autorisés à accéder au portail d'exécution des services avec leurs rôles respectifs. • Fournir des détails sur les Services pour les mentions dans la conception du Catalogue de services. • Fournir des détails pour personnaliser les flux de travail d'orchestration du Service. • Fournir la future feuille de route et aider à la mise en œuvre des changements apportés au catalogue commercial de portail d'exécution des Services. • Fournir un interlocuteur unique pour la gestion et la surveillance des responsabilités du client en rapport avec le portail d'exécution des Services. • Suivre le processus de gestion du changement pour les demandes de changement concernant le catalogue commercial de portail d'exécution des Services et le flux de travail d'orchestration des Services.
Livrables : Accès au portail d'exécution des services, rapport sur les demandes de service.	

Gestion des Composants gérés par des tiers	
Résumé : Cisco va gérer les Composants gérés par des tiers identifiés dans un document de commande, en vertu d'une lettre d'autorisation (LA) valide et comme décrit dans cette Description de service. Cisco supervisera les interactions et la gestion des fournisseurs tiers qui fournissent au client certains produits ou services tiers apparaissant dans le ou les documents de commande applicables à titre de Composants gérés par des tiers.	
Responsabilités de Cisco • Gérer les Composants gérés par des tiers mentionnés dans les documents de commande ou dans un accord écrit.	**Responsabilités du Partenaire** • Renseigner Cisco et le fournisseur tiers concerné à l'aide d'une lettre d'autorisation valide tel que décrit à l'Annexe A. • Mettre à jour le contrat d'assistance valide avec le fournisseur tiers concerné. • Déterminer les Composants gérés par des tiers et les fournisseurs tiers correspondants. • Gérer tous les incidents de sécurité, les notifications ou les alertes, et informer Cisco de tout incident de sécurité, de toute notification ou de toute alerte concernant les Composants gérés par des tiers. • Si la gestion des modifications ne fait pas partie de l'étendue des Services, gérer et effectuer les modifications apportées aux Composants gérés par des tiers.
Livrable : Communications avec les clients, en fonction des besoins.	

Liaison intelligente pour CMS	
Résumé : Cisco fournira des points d'intégration de la plate-forme CMSP (Cisco Managed Services Platform) pour permettre au système de gestion des TI (IT Service Management ou ITSM) du partenaire de communiquer avec la plate-forme CMSP et ainsi faciliter l'échange de dossiers, de mises à jour d'état, de processus de flux de travail et d'autres renseignements connexes. Sauf accord contraire par écrit, la liaison intelligente est limitée à une liaison unique entre la plate-forme CMSP de Cisco et le système ITSM du partenaire.	
Responsabilités de Cisco • Fournir une interface d'intégration ITSM entre la plate-forme CMSP et le système ITSM du partenaire afin de faciliter les échanges bidirectionnels pour la gestion des changements, la gestion des incidents, le flux de travail de gestion des demandes de services, la gestion des incidents et les mises à jour d'état et de tickets. • Fournir au partenaire la documentation et les spécifications d'une interface de programmation d'applications (API) pour permettre l'intégration de l'ITSM du partenaire avec le CMSP. • Informer le partenaire de tout changement d'ordre matériel concernant l'interface API de Cisco.	**Responsabilités du partenaire** • Personnaliser et configurer le système ITSM du partenaire pour qu'il interagisse avec l'interface API de la plate-forme CMSP. • Désigner un interlocuteur unique pour les opérations de liaison intelligente. • Respecter les exigences énoncées dans la documentation pour faciliter l'intégration. • Informer Cisco de tout changement matériel concernant les systèmes de gestion des tickets. • Communiquer avec Cisco si le partenaire croit que les données ou les renseignements sur la création de tickets de liaison intelligente sont inexacts.
Livrable : Spécification de l'API et de l'intégration.	

Plate-forme de services gérés de Cisco sur site pour un CPE

Résumé : Cisco fournira des outils de la plate-forme de services gérés Cisco (Cisco Managed Services Platform ou CMSP) détenus par Cisco ou sous licence pour une utilisation sur le site d'un client final (« **Outils CMSP** ») au lieu de CMSP hébergé dans le nuage ou en complément de CMSP hébergé dans le nuage.	
Responsabilités de Cisco • Fournir au partenaire un appareil autonome (matériel et logiciel), ainsi que les exigences et les instructions d'installation dans un centre de données d'un client final (par exemple, l'occupation de l'espace dans des bâtis, la consommation d'énergie, les connexions réseau, le plan d'adressage IP, etc.) pour le fonctionnement du Service. • Fournir des terminaux VPN dans les centres de données Cisco pour permettre la connectivité entre CMSP et les Outils CMSP sur site. • Fournir la conception de la connectivité réseau (par exemple, les ports, les protocoles, la bande passante, etc.) entre les Composants gérés et les Outils CMSP. • Fournir au partenaire les exigences techniques et environnementales (par exemple, l'alimentation, l'occupation de l'espace dans des bâtis, le processeur, le système d'exploitation, la ventilation, etc.) nécessaires à l'utilisation des Outils CMSP. • Aider le client à distance pour l'installation des Outils CMSP et pour apporter les modifications demandées par Cisco.	**Responsabilités du partenaire et du client final** • Configurer l'équipement fourni par le client final pour la connectivité VPN avec la tête de réseau de Cisco. • Fournir l'environnement qui répond aux spécifications (par exemple, l'espace dans le bâti, la consommation d'énergie, les connexions réseau, etc.), en fonction des besoins. • Avec un avis préalable raisonnable et des instructions de Cisco, installer et apporter les modifications nécessaires aux Outils CMSP (p. ex., mettre à jour les logiciels, remplacer et configurer l'appareil, modifier la configuration, etc.). • Fournir l'adressage IP et la connectivité réseau physique pour la plate-forme. • Fournir la connectivité nécessaire (ports et protocoles) sur tout le réseau du client final entre les Composants gérés et les outils CMSP.
Livrable : Outils CMSP et aide à distance pour l'installation.	

Annexe A : Conditions générales

1. Conditions reliées aux Services

1.1 **Portée des services supplémentaires.** À moins que les Services ne soient expressément mentionnés, tous les autres services Cisco sont exclus de cette Description de service. Par conséquent, en plus des demandes de service dans le catalogue des services, Cisco travaillera avec le partenaire pour prendre en compte les demandes de service personnalisées ou les services personnalisés (« **Services personnalisés** »). La portée et les frais associés aux Services personnalisés seront convenus par écrit entre Cisco et le client avant que Cisco n'entame la prestation des Services.

1.2 **Composants gérés**

(a) Dans le cadre de la transition du Service, Cisco identifiera les périphériques, le matériel ou les équipements du réseau d'un client final qui seront activés en tant que Composants gérés et identifiera toutes les limitations des Services en ce qui concerne les Composants gérés et/ou les composants uniquement surveillés, le cas échéant. Par exemple, certains Composants gérés par des tiers peuvent être uniquement surveillés en vue de leur disponibilité (parfois appelé « up/down ») avec des Services supplémentaires limités.

(b) Sauf indication expresse dans le ou les documents de commande applicables, Cisco ne fournira aucun Service pour les Composants gérés non autorisés (p. ex. marché gris) EoX (p. ex. en fin de vie, en fin de période d'assistance, etc.).

(c) S'ils ne sont pas documentés dans les documents de commande, la gestion des Composants gérés par des tiers ou de tout Composant géré de type EoX se limite à la gestion des événements, à la création et à la fermeture d'un ticket d'incident, ainsi qu'à la création de rapports standard basés sur les données disponibles.

(d) La gestion des appareils (c'est-à-dire les composants non gérés identifiés dans un document de commande) par Cisco se fera de manière raisonnable, sans aucune garantie d'aucune sorte.

(e) Le partenaire ou le client final concerné doit conserver un contrat de licence, d'assistance et de maintenance Cisco valide pour tous les Composants gérés. Cisco se réserve le droit de demander au partenaire des frais d'assistance et de maintenance équivalents pour les Composants gérés qui ne sont pas pris en charge ou de réduire les services (par exemple, les mises à jour, les demandes de remplacement d'équipement, etc.) pour les Composants gérés qui ne sont pas assortis d'un contrat de licence, d'assistance et de maintenance Cisco valide.

1.3 **Production de rapports.** Cisco fournira, ou mettra à disposition par l'entremise du portail, les rapports énumérés dans le guide des rapports fournis par Cisco. Cisco se réserve le droit d'ajouter, de modifier ou de supprimer des rapports à sa discrétion. Le partenaire devra passer en revue, analyser et (le cas échéant) discuter avec Cisco au sujet des renseignements contenus dans les rapports fournis. Le partenaire informera Cisco dans un délai raisonnable s'il pense qu'un rapport comporte une erreur.

1.4 **Plate-forme de services gérés Cisco (Cisco Managed Services Platform ou CMSP).** La plate-forme CMSP sera le système des registres pour les Services. À moins que le partenaire achète le service *Plate-forme de services gérés Cisco sur site pour le composant* CPE, la CMSP utilise des composants basés dans le nuage pour traiter les données des Composants gérés afin de fournir les Services. Ces composants sont hébergés dans un centre de données sécurisé avec au moins un système redondant. Cisco sera responsable de la maintenance de la plate-forme CMSP et des Outils CMSP avec un accès raisonnable et une assistance sur site fournie par le partenaire.

1.5 **Recommandations et modifications de Cisco.** Si le partenaire ne parvient pas à mettre en œuvre des recommandations ou des exigences Cisco faisant l'objet d'une demande raisonnable, ou ne peut pas permettre à Cisco d'apporter des modifications raisonnablement recommandées par rapport aux Composants gérés ou aux Services, Cisco ne sera pas responsable de tout délai, défaillance ou risque de sécurité accru en ce qui concerne la prestation des Services. En outre, si le partenaire ne parvient pas à mettre en œuvre des recommandations raisonnables de Cisco ou si son refus non raisonnable à Cisco d'apporter des modifications fait en sorte que Cisco doive engager des dépenses ou fournir des efforts supplémentaires pour fournir les Services, Cisco peut facturer des frais supplémentaires pour résoudre ce type de problème jusqu'à la mise en œuvre des recommandations.

1.6 **Formation et politiques.** Le personnel de Cisco requis pour accéder à un ou plusieurs sites du partenaire ou du client final, à des Composants gérés ou à tout autre système du partenaire ou du client final participera à distance à toute formation raisonnablement demandée par le partenaire (jusqu'à 6 heures maximum

par an) sans coût additionnel. De plus, Cisco se conformera de manière tangible à toutes les politiques de sécurité écrites raisonnables applicables aux Services, à condition que : (a) les politiques soient fournies par écrit à Cisco raisonnablement en avance de la date de conformité demandée; (b) Cisco dispose d'un contrôle suffisant pour mettre en œuvre les politiques; et (c) les politiques ne soient pas en conflit avec les politiques de Cisco, ne modifient pas ou n'entrent pas en conflit avec le Contrat ou cette Description de service, ne modifient pas l'attribution du risque ou de la responsabilité entre les parties, n'augmentent pas la portée des Services ou ne forcent pas Cisco à supporter des risques ou ces coûts accrus pour se conformer à ces politiques.

1.7 **Responsabilités générales du partenaire.** La fourniture des Services par Cisco dépend de la capacité du partenaire à assumer ses responsabilités, et de la capacité du partenaire à assurer que le client final peut faire de même, comme indiqué dans cette Description de service ou suite à une demande raisonnable de Cisco. Si le partenaire ou le client final ne parvient pas à assumer ses responsabilités ou si une exclusion (répertoriée dans la section 1.8 ci-dessous) s'applique, Cisco ne sera pas tenu de fournir les Services (y compris la réalisation des niveaux de service) dans la mesure et pour la période pendant laquelle le partenaire ou le client final ne peuvent assumer leurs responsabilités. De plus, Cisco se réserve le droit de facturer le partenaire pour les dépenses, les coûts ou des délais engagés, provoqués par l'incapacité du partenaire ou du client final d'assumer leurs responsabilités. En plus des responsabilités du partenaire et du client final énumérées ci-dessus, le partenaire sera également responsable et s'assurera que le client final sera responsable des éléments suivants :

(a) Fournir rapidement à Cisco les données techniques nécessaires et faisant l'objet d'une demande raisonnable (p. ex., les schémas de réseau, les adresses IP, les chaînes SNMP et les mots de passe), ainsi que d'autres renseignements semblables afin que Cisco puisse fournir les Services.
(b) Fournir une invite, une coopération et une assistance raisonnables à Cisco pour la fourniture des Services (p. ex., apporter des modifications à des Composants gérés ou à des Outils CMSP qui ne peuvent pas être effectués à distance, exécuter localement des tests ou des diagnostics sur des Composants gérés, mettre à jour des configurations ou des paramètres VPN, etc.).
(c) Mettre à disposition les sites et assurer leur entretien et la gestion des conditions environnementales, notamment l'alimentation, le système de chauffage, de ventilation et de climatisation (HVAC), la connectivité, l'espace (espace physique et espace de bâti), la sécurité, les planchers surélevés, le confinement des incendies, l'accès sécurisé hors bande et les autres conditions nécessaires au bon fonctionnement des Composants gérés, des Composants gérés par des tiers, des composants uniquement surveillés et des autres infrastructures et applications qui s'appliquent aux Services.
(d) Sauvegarder ses propres données et les protéger contre la perte, l'endommagement, le vol ou la destruction.
(e) Fournir un accès physique et distant (logique) à Cisco et au personnel de Cisco aux Composants gérés, à l'équipement Cisco, ainsi qu'à d'autres infrastructures du partenaire ou du client final, comme il sera raisonnablement nécessaire pour que Cisco puisse fournir les Services (par exemple, l'ouverture de ports, la modification des paramètres de pare-feu, la mise à disposition de fenêtres de changement, etc.). Cette responsabilité inclut la fourniture de toutes les autorisations ou licences internes ou tierces nécessaires.
(f) Gérer tous les produits ou services tiers qui ne sont pas inclus dans le cadre des Services, notamment l'application des contrats de niveau de service tiers et de tout autre contrat de niveau de service applicable.
(g) Avertir Cisco avant toute mise à jour ou tout changement planifié dans l'environnement du partenaire ou du client. L'omission d'informer Cisco de telles mises à jour ou de telles modifications pourrait faire en sorte que Cisco facture des unités de demandes de services supplémentaires.
(h) Déterminer toutes les dépendances pour les périphériques, les logiciels ou les services non couverts.
(i) Le cas échéant (p. ex., pour les licences détenues par le partenaire ou le client final pour des Composants gérés par des tiers ou d'autres logiciels, produits ou services de tiers), fournir une lettre d'agence liant tout fournisseur tiers et Cisco qui autorise Cisco et ses partenaires à agir en tant qu'agents du client final en ce qui concerne la gestion de tout Composant géré par des tiers ou de tout autre logiciel, produit ou service de tiers.
(j) Fournir et maintenir la connectivité (y compris les circuits locaux, les connexions croisées et les périphérique requis) avec le centre d'exploitation de réseaux (Network Operations Center ou NOC) de Cisco, notamment en prévoyant les autorisations raisonnablement requises. La vitesse de connexion Internet minimale pour le réseau VPN de Cisco est de 10 Mbit/s pour les téléchargements et les téléversements (circuit symétrique).

1.8 **Exclusions**

Les produits et services non décrits dans la présente Description de service sont exclus des Services, y compris, sans limitation, ceux cités en exemple ci-après :

- Toutes les connexions réseau, y compris, sans limitation, les circuits PSTN ou MPLS et les connexions croisées.
- Sauf indication contraire dans le ou les documents de commande applicables, les Services ou logiciels permettant de résoudre tout incident ou problème provoqué par un produit tiers ou résultant de causes échappant au contrôle de Cisco.
- Mises à niveau de logiciels ou de matériel, à moins qu'elles soient expressément mentionnées dans la présente description de service, dans les documents complétant la présente description de service ou dans les documents de commande pertinents.
- Gestion du changement ou mise en œuvre des changements relatifs aux équipements non gérés par Cisco.
- Sauf indication contraire dans un document de commande, fournir des Services sur site ou dans toute autre langue que l'anglais.
- Dépannage des incidents qui sont survenus avant l'activation du Service.

2 Modalités commerciales

2.1 **Sommaire des prix.** Les frais pour les Services (les « **Frais** ») seront décrits dans le document de commande applicable. Les Frais indiqués dans le document de commande correspondent à une charge par travailleur du savoir et par périphérique de zone commune (chacun, un « **Abonné** ») par mois. Pour éviter tout doute, toute augmentation du nombre de travailleurs du savoir ou de périphériques dans une zone commune sur l'UCM dans le nuage entraînera une augmentation des Frais pour les Services en fonction du nombre total de travailleurs du savoir et de périphériques dans une zone commune autorisés à accéder à l'UCM dans le nuage. Tous les Frais payés sont non remboursables.

2.2 **Facturation**

(a) Si le client a payé à l'avance pour les Services, Cisco facturera le partenaire à la date ou après la date d'entrée en vigueur décrite dans le document de commande correspondant (la « Date d'entrée en vigueur »).
(b) Si aucun terme de facturation n'est fourni dans les documents de commande, les Frais seront calculés au prorata pour le nombre d'années (ou toute partie de l'année) de la durée et payés annuellement à l'avance.

(c) Si les documents de commande prévoient la facturation lors de l'activation, Cisco commencera à facturer la Date d'activation estimée ou la Date d'activation initiale indiquée dans le plan de transition, selon la première éventualité. Cisco peut retarder la facturation au jour le jour si Cisco est la principale cause du retard de l'activation.

(d) Les droits de Cisco de percevoir les Frais reliés aux Services et l'obligation de paiement du partenaire ne seront pas touchés par (i) tout retard causé par le partenaire (ou toute personne agissant en son nom ou au nom du client), (ii) le manquement ou le retard du partenaire ou du client final dans l'exécution de ses obligations en vertu de la présente Description de service ou de la Description du service UCM dans le nuage ou (iii) le manquement du partenaire d'émettre un bon de commande.

2.3 **Activation.** La Date d'activation sera indiquée dans le plan de transition. Si aucune date n'est indiquée dans le plan de transition, les Composants gérés seront considérés comme activés à la Date d'activation réelle par Cisco ou quatre-vingt-dix (90) jours à compter de la Date d'entrée en vigueur du document de commande, selon la première éventualité.

2.4 **Périphériques supplémentaires ajoutés en tant que Composants gérés** Si le Client modifie le nombre de Composants gérés indiqué dans le document de commande applicable, les frais mensuels pour les Services seront ajustés en conséquence. Si le client souhaite ajouter de nouveaux appareils en tant que Composants gérés et qu'il n'y a pas mécanisme d'ajustement, d'audit, d'avis de tarification ou de provision similaire dans le document de commande, les parties suivront le processus standard de demande de modification de Cisco.

2.5 **Unités de demande de service (Service Request Units ou SRU) et Frais associés** Le ou les documents de commande applicables du partenaire indiqueront le nombre total de SRU achetés. Si le partenaire utilise tous ses SRU disponibles, le partenaire peut acheter des SRU supplémentaires. Les SRU ne sont pas remboursables et doivent être utilisés pendant le terme mentionné dans le document de commande correspondant sans quoi ils viennent à expiration. Cisco facturera au partenaire toute demande de services effectuée par Cisco au client au cours du mois de facturation applicable. Pour éviter tout doute, les Unités de demandes de services (SRU) ne peuvent pas servir à compenser les frais mensuels supplémentaires associés à l'augmentation du nombre total de Composants gérés.

2.6 **Durée minimale et Frais minimaux** Les Documents de commande indiqueront la durée minimale et les Frais minimaux associés aux Services.

2.7 **Durée, résiliation et renouvellement**

(a) **Durée.** La durée des Services sera indiquée dans les documents de commande. Sauf indication contraire dans les documents de commande, le calcul de la durée commence à la Date d'entrée en vigueur du document de commande et se termine en même temps que l'abonnement du client final au service UCM dans le nuage.

(b) **Résiliation.** Lorsqu'un document de commande précise un engagement ou une valeur de contrat minimal, si le client met fin aux Services pour des questions de commodité, Cisco facturera le reste de la valeur du contrat ou de l'engagement minimal dû en vertu du document de commande. Si le document de commande ne précise pas d'engagement minimal, le client ne peut pas mettre fin aux Services pour plus de commodité, même si le contrat l'autorise, sauf indication contraire dans le document de commande. Les droits de résiliation pour violation de matériel sont indiqués dans le Contrat.

(c) **Renouvellement.** Le Service se renouvellera automatiquement pour une période supplémentaire d'une année au même prix, dans la mesure où la commande du partenaire pour le service UCM dans le nuage est aussi renouvelée, sauf si Cisco informe le partenaire par écrit au moins quatre-vingt-dix (90) jours avant, ou si le partenaire avertit Cisco par écrit au moins quarante-cinq (45) jours avant l'expiration de la période en cours pour lui indiquer qu'il ne souhaite pas renouveler les services.

3 Conditions juridiques

3.1 **Définitions.** Les termes qui commencent par une lettre majuscule dans cette Description de service sont définis dans le glossaire de la Description de service pour les services gérés de Cisco (accessibles à l'adresse www.cisco.com/go/servicedescriptions) (« **Glossaire des termes** »). En cas de conflit entre les définitions apparaissant dans le corps de cette Description de service et une définition correspondante dans le Glossaire des termes, la définition apparaissant dans cette Description de service prévaut.

3.2 **Documents connexes.** Le présent document doit être consulté conjointement avec les documents suivants : (1) Glossaire des termes; (2) tout accord de niveau de service faisant état de la présente Description de service; (3) tout document supplémentaire; (4) la méthodologie et terminologie connexe utilisées pour décrire le niveau de priorité d'un incident qui est inclus dans l'Annexe B de la présente Description de service; et (5) le ou les documents de commande.

3.3 **Ordre de préférence.** En cas de conflit entre la présente Description de service, un document supplémentaire, un document de commande ou le Contrat applicable, l'ordre de priorité suivant s'appliquera (du plus haut au plus bas) : (a) tout document de commande, le cas échéant; (b) cette Description de service; (c) tout document complémentaire; et (d) le Contrat applicable.

3.4 **Respect des lois.** Cisco se conformera aux lois, aux règles et aux règlements en vigueur, notamment toute loi et toute réglementation en vigueur qui portent sur le contrôle des exportations. Le partenaire se conformera aux lois et le partenaire s'assurera que le client s'engagera à respecter toutes les lois, les règles et les réglementations en vigueur liées à la réception et à l'utilisation des Services et devra obtenir toutes les approbations et licences exigées par les tierces parties associées aux Composants gérés ainsi qu'aux sites, aux systèmes, aux logiciels et au réseau du partenaire ou du client final dont Cisco a besoin pour fournir les Services.

3.5 **Licence.** Cisco accorde au partenaire et au client final du partenaire une licence pour utilisation interne limitée, non transférable, non sous-licenciable, une licence pour utiliser la version exécutable du portail, tous les Outils CMSP et tout logiciel fourni par Cisco dans le cadre des Services (soit installé dans les locaux du partenaire ou du client final ou disponibles sous forme de logiciel en tant que service) uniquement dans la mesure et la durée raisonnablement nécessaires pour recevoir les Services. Il n'y a aucune garantie associée à ces éléments en dehors de leur utilisation dans le cadre des Services. Lors de l'expiration ou de la résiliation des Services, la licence du portail, des Outils CMSP et des logiciels est automatiquement interrompue. Le cas échéant, le partenaire renverra tous les composants matériels et logiciels appartenant à Cisco pour lesquels il avait obtenu une licence d'utilisation dans le cadre des Services (par exemple, les Outils de la plate-forme CMSP). Sauf dans les limites d'une responsabilité explicite de Cisco, le partenaire sera tenu responsable

de toute perte, tout vol ou tout endommagement aux outils de la plate-forme CMSP jusqu'à ce qu'ils soient retournés.

3.6 **Sécurité et programme de confidentialité des données.** Chaque partie veillera, et le partenaire veillera à ce que le client accepte de maintenir un programme raisonnable d'anonymat des données et de sécurité des renseignements grâce à des mesures techniques, administratives et physiques appropriées, dans le but : (i) d'empêcher tout accès non autorisé et toute utilisation, distribution ou suppression des données du partenaire ou du client final et (ii) de ne pas compromettre les Composants gérés. Vous trouverez de plus amples renseignements sur la politique de confidentialité et la sécurité de Cisco à l'adresse suivante : http://www.cisco.com/c/en/us/about/trust-transparency-center/data-protection.html. Si les parties ne disposent pas d'un accord de protection des données (ou de modalités équivalentes de confidentialité et de protection des données), le contrat mutuel de protection des données que voici est inclus dans la présente Description du service : https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf.

3.7 **Coopération.** Dans la mesure où une demande raisonnable est faite par l'autre partie et que cela est autorisé par la loi applicable, chaque partie fournira une aide raisonnable à l'autre partie, communiquera et coopérera avec elle, ainsi qu'avec tout sous-traitant ou prestataire qui fournit des services à une telle autre partie en rapport avec les Services. Chaque partie déploiera efforts commercialement raisonnables pour obtenir ce type de coopération auprès de ses propres sous-traitants et fournisseurs.

3.8 **Renseignements confidentiels.** Les informations sur le dossier d'exploitation, les Frais, le portail, les Outils CMSP et les performances des niveaux de service sont des informations confidentielles (telles que définies dans le Contrat). Ces renseignements ne peuvent être utilisés pour toute fin autre que dans le cadre de l'utilisation par le partenaire et le client final des Services concernés fournis par Cisco.

3.9 **Données télémétriques.** Cisco peut recueillir des données sur la manière dont le partenaire ou le client final recourt aux services en vue de maintenir, améliorer, commercialiser ou promouvoir les Services. De plus, Cisco peut utiliser des données anonymes et agrégées sur l'utilisation des Services par le partenaire ou le client final, les performances des Composants gérés (produits Cisco uniquement) et les performances du réseau (« **Données télémétriques** ») pour créer ou améliorer ses produits et services. Cisco se conformera en toutes circonstances à la Loi applicable liée à la collecte et à l'utilisation par Cisco des données décrites ci-haut et emploiera des moyens raisonnables physiques, techniques et procéduraux pour garantir la protection des données télémétriques qui renferment des données personnelles, conformément à la Politique de confidentialité en ligne de Cisco, qui est publiée à l'adresse URL https://www.cisco.com/c/fr_ca/about/legal/privacy-full.html ou sur tout autre site communiqué au public par Cisco de temps à autre.

3.10 **Sous-traitants.** Cisco peut faire appel à des sous-traitants pour fournir des Services au partenaire ou au client final en son nom dans le cadre de la fourniture des Services. Cisco demeure responsable de la conformité de ses sous-traitants aux obligations qui découlent de la présente Description de service et de ce Contrat comme si les prestations étaient effectuées par Cisco. Les références à Cisco dans cette Description de service comprennent ses sous-traitants, le cas échéant.

4. **Niveaux de service.** Le contrat de niveau de service pour les UCaaS de Cisco optimisé par UCM dans le nuage est intégré par référence à cette Description de service.

Annexe B : Niveaux de priorité

Cette annexe décrit la méthodologie utilisée pour définir le niveau de priorité d'un incident. Cisco classe les incidents en fonction de leur « Incidence » et de leur degré d'« Urgence », puis détermine la priorité de l'incident en se fondant sur les définitions des termes « Incidence » et « Urgence » indiquées dans le tableau ci-dessous.

Incidence Un Incident est classé en fonction de l'étendue de son incidence sur l'entreprise du client final (à savoir, l'ampleur, la portée et la complexité de l'Incident).	**Urgence** L'Urgence d'un Incident est classée en fonction de son incidence sur les Services ou la possibilité pour le client final de bénéficier des Services, et de l'incidence financière sur l'entreprise du client final.
Il existe quatre niveaux d'incidence : • Incidence généralisée : l'ensemble du Service est concerné (plus des trois quarts des personnes, des sites ou des Composants gérés). • Incidence de grande envergure : plusieurs sites sont concernés (entre la moitié et les trois quarts des personnes, des sites ou des Composants gérés). • Incidence localisée : un seul site ou plusieurs utilisateurs sont concernés (entre un quart et la moitié des personnes, des sites ou des Composants gérés). • Incidence individualisée : un seul utilisateur est concerné (moins d'un quart des personnes, des sites ou des Composants gérés).	Il existe quatre niveaux d'urgence • Niveau critique : les fonctions principales sont interrompues, sans redondance ni sauvegarde. Cette situation peut avoir une incidence financière immédiate et importante sur l'entreprise du client final. • Niveau majeur : les fonctions principales sont fortement dégradées et sont soutenues par une sauvegarde ou un système redondant. Il est probable que la situation ait une incidence financière importante sur l'entreprise du client final. • Niveau mineur : des fonctions non essentielles sont interrompues ou fortement dégradées. Il est possible que la situation ait une incidence financière sur l'entreprise du client final. • Faible / avertissement : des fonctions non essentielles sont dégradées. Il n'y a aucune incidence. Le partenaire ou le client final considère le problème comme faible.

Définition du terme « Priorité »
La Priorité définit le niveau d'effort qui sera fourni par Cisco et PAR le partenaire pour résoudre l'incident. Le niveau de Priorité est déterminé en se basant sur les définitions des termes « Incidence » et « Urgence » indiquées dans le tableau ci-dessous.

INCIDENCE					
URGENCE		Généralisée	De grande envergure	Localisée	Individualisée
	Critique	P1	P1	P2	P2
	Majeure	P1	P2	P2	P3
	Mineure	P2	P3	P3	P3
	Faible / avertissement	P4	P4	P4	P4

Remarques :

- Cisco ajustera le niveau de priorité des tickets en fonction de la mise à jour du niveau de Priorité de l'Incidence ou de la résolution de l'Incident.
- Les demandes du client pour transmettre les Incidents à une Priorité plus élevée que leur classement peuvent entraîner des frais supplémentaires.
- Le ticket peut rester ouvert pendant une période prescrite tout au long de l'évaluation de la stabilité opérationnelle.

Les priorités de Gestion des Incidents de Cisco sont définies comme suit :

- P1 : Cisco et le partenaire mobiliseront toutes les ressources nécessaires 24 h sur 24 et 7 j sur 7 afin de résoudre le problème.
- P2 : Cisco et le partenaire mobiliseront des ressources à temps plein pendant les heures de travail normales afin de résoudre le problème.
- P3 : Cisco et le partenaire envisagent de mobiliser des ressources pendant les heures de travail normales afin de restaurer le service à des niveaux satisfaisants.
- P4 : Cisco et le partenaire envisagent de mobiliser des ressources pendant les heures de travail normales afin de fournir des renseignements ou une assistance.