



CONDITIONS DE L'OFFRE POUR CISCO UMBRELLA DNS SECURITY (CENTRE SÉCURISÉ DE STOCKAGE DE LOGICIELS MALVEILLANTS [MSP])

L'utilisation par MSP de Cisco Umbrella DNS Security acheté selon les conditions d'utilisation des services infonuagiques de Cisco (Secure MSP Center) (« Conditions infonuagiques »), qui comprend l'utilisation de Umbrella DNS Security Essentials et/ou de Umbrella DNS Security Advantage (« Umbrella DNS Security » ou « Service en nuage »), comprend également les présentes conditions de l'offre. Les termes commençant par une majuscule utilisés, mais non définis dans les présentes conditions de l'offre, sont définis dans les Conditions infonuagiques.

Description du service en nuage

La solution Umbrella DNS Security est une plateforme infonuagique de sécurité de la couche DNS (système de noms de domaine) qui offre la première ligne de défense contre les menaces sur Internet en bloquant les demandes de destinations malveillantes (les domaines, les adresses IP, les URL) avant que la connexion soit établie. Elle fournit une protection contre les menaces sur tous les ports et pour tous les protocoles et peut protéger l'accès Internet pour tous les appareils sur votre réseau, pour tous les sites physiques ainsi que pour les utilisateurs en déplacement. Consultez la [documentation de Cisco Umbrella](#) pour obtenir de plus amples renseignements sur ses caractéristiques techniques, ses exigences en matière de configuration, ses fonctionnalités et autres caractéristiques.

Conditions supplémentaires

- 1. Limites de la portée et de l'utilisation.** Vous utiliserez le service en nuage en tant que service en nuage de marque Cisco (sous réserve du comarquage, comme cela est décrit ci-dessous) pour fournir des services logiciels aux utilisateurs finaux de MSP et ne modifierez pas le service en nuage, sauf à la demande de Cisco ou avec l'autorisation de cette dernière. Vous n'utiliserez pas un détenteur Cisco Umbrella (également appelé organisation Umbrella) unique pour plusieurs utilisateurs finaux de MSP.
- 2. Moyenne mensuelle de requêtes DNS.** La limitation d'utilisation suivante s'applique à votre utilisation d'Umbrella DNS Security. « Utilisateur final de MSP » vous inclut lorsque vous utilisez le Service en nuage à des fins internes, comme le permet la Section 1.2 des Conditions en nuage. « Utilisateurs autorisés » désigne les employés, les sous-traitants et les autres personnes dont les activités en ligne ou dans le nuage (p. ex., Internet, messagerie, utilisation d'applications en nuage) sont protégées de par l'utilisation de ce service en nuage.

La licence de Umbrella DNS Security est basée sur le nombre d'utilisateurs autorisés et sur un maximum de 5 000 requêtes DNS par Utilisateur autorisé par jour, calculé sur une moyenne mensuelle de requêtes DNS par Utilisateur final de MSP (comme elle est définie ci-dessous). Cisco effectuera un suivi en continu de votre utilisation de Umbrella DNS Security sur une base mensuelle pour déterminer votre moyenne mensuelle de requêtes DNS par Utilisateur final de MSP. Si, à tout moment, Cisco détermine que votre moyenne mensuelle de requêtes DNS pour un Utilisateur final de MSP a dépassé 5 000 requêtes DNS par Utilisateur autorisé par jour, Cisco se réserve le droit de vous demander d'acheter des licences supplémentaires.

Moyenne mensuelle de requêtes DNS = (nombre de requêtes DNS dans le mois en question pour un Utilisateur final de MSP/nombre de jours dans le mois en question)/nombre d'utilisateurs autorisés sous licence pour ce mois pour ces Utilisateurs finaux de MSP.

Par exemple, si un Utilisateur final de MSP a 1 000 utilisateurs autorisés sous licence par mois et qu'ils ont envoyé un total de 3 000 000 de requêtes DNS pendant ce mois, la moyenne mensuelle de requêtes DNS pour cet Utilisateur final de MSP est la suivante :

$$(3\,000\,000 / 30) / 1000 = 100$$

3. **Stockage S3 des journaux géré par Cisco.** Certaines offres groupées de Cisco Umbrella comprennent la possibilité de sélectionner le stockage S3 géré par Cisco ou le stockage géré par l'Entreprise (c.-à-d., votre propre stockage) pour le DNS, le mandataire et les journaux d'événements. Le stockage S3 des journaux géré par Cisco est offert avec des options de rétention de 7, 14 ou 30 jours. Si Vous avez besoin de plus de 30 jours de rétention, Vous devez sélectionner le stockage géré par l'Entreprise ou exporter les données du stockage géré par Cisco vers le stockage géré par Votre Entreprise avant l'expiration de la période de rétention. Si la journalisation vers un compartiment S3 géré par Cisco est activée, le téléchargement ou la synchronisation des fichiers de ce compartiment doivent être configurés de sorte que chaque fichier journal soit téléchargé une seule fois. Cisco se réserve le droit de suspendre le téléchargement des journaux à partir d'un compartiment S3 (par la rotation des clés ou d'autres méthodes) si les fichiers journaux sont téléchargés plusieurs fois au lieu d'une seule. Veuillez consulter la documentation relative au compartiment S3 géré par Cisco, disponible ici : <https://docs.umbrella.com/deployment-umbrella/docs/cisco-managed-s3-bucket>.
4. **Comarquage.** Tout co-marquage du service en nuage que vous effectuez est assujéti aux lignes directrices disponibles ici : <https://www.cisco.com/c/dam/en/us/products/collateral/security/umbrella/umbrella-sps-co-branding-guidelines.pdf>, ainsi qu'à toute ligne directrice sur les marques de commerce prévues dans les Conditions infonuagiques.
5. **Objectif de niveau de service.** Dans le cadre de cet objectif de niveau de service, le terme « Service » désigne un service DNS récursif de Cisco et ne comprend pas d'interfaces utilisateur Web, de systèmes de configuration ou d'autres méthodes d'accès ou de manipulation de données. Cisco déploiera des efforts commercialement raisonnables pour maintenir un taux de disponibilité de 99,999 % chaque mois civil pour le service. Le taux de disponibilité sera calculé en divisant le total des minutes de Temps de disponibilité durant le mois civil en question par le nombre total de minutes de ce même mois, moins les minutes d'Inaccessibilité où le Service Cisco Umbrella est indisponible en raison des périodes de maintenance planifiées et imputables aux Interventions d'un tiers (définies ci-dessous), le tout multiplié par 100. La formule du calcul est comme suit :

$$\text{Accessibilité} = (X \div Y) \times 100$$

X = total des minutes d'accessibilité au cours du mois de calendrier

Y = (total des minutes dans ce même mois de calendrier x) - (total des minutes d'inaccessibilité en raison des périodes de maintenance planifiées et des interventions de tiers)

Aux fins de ce calcul, i) « Inaccessibilité » signifie que le service est totalement inaccessible même si votre connexion Internet fonctionne correctement, ii) « Temps de disponibilité » désigne le nombre de minutes où le Service DNS de Cisco Umbrella était accessible, à l'exception des périodes d'Inaccessibilité en raison des opérations de maintenance planifiées et des Interventions d'un tiers, et iii) « Intervention d'un tiers » désigne toute intervention hors de la volonté de Cisco, y compris, sans s'y limiter, l'efficacité des réseaux Internet ou de carrefours d'échanges de données qui sont gérés par d'autres entreprises, les conflits de travail, les pénuries de main-d'œuvre, les émeutes, les insurrections, les incendies, les inondations, les perturbations météorologiques ou solaires, les explosions, les cas de force majeure, les conflits armés, les actes de terrorisme, les interventions gouvernementales, les conditions de travail, les séismes et les pénuries de matériel. En cas de différend, Cisco rendra sa décision sur l'Inaccessibilité en toute bonne foi sur la base de ses journaux du système, des rapports de surveillance et des registres de configuration et en ce qui concerne la présence des relevés ceux de Cisco prévalent sur ceux des clients. Cisco ne peut être tenue responsable d'aucune Inaccessibilité découlant des Interventions d'un tiers.

6. **Protection des données.** Pour en savoir plus sur les données personnelles traitées par Umbrella DNS Security, consultez les fiches techniques de confidentialité Umbrella dans le [Centre de sécurité et de confiance de Cisco](#).

- 7. Sécurité.** Lorsque vous fournirez des services logiciels aux utilisateurs finaux de MSP, vous devrez mettre en œuvre et maintenir les mesures techniques et organisationnelles standard appropriées du secteur pour protéger les données des Utilisateurs finaux de MSP contre une utilisation ou une destruction accidentelle ou illégale, une perte accidentelle, une altération et une divulgation non autorisées de ces dernières, ou l'accès à toutes données de l'Utilisateur final de MSP.