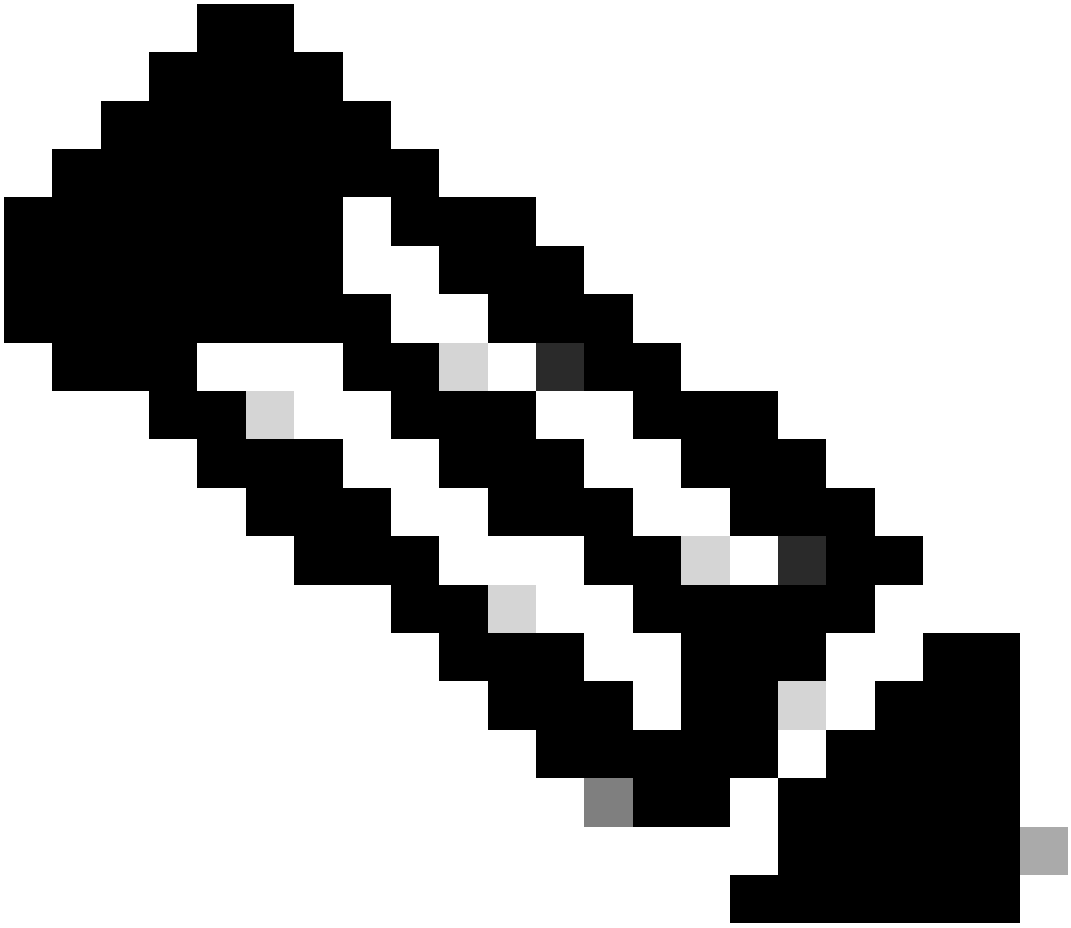
Dépannage de l'abonnement Umbrella ou expiration

Table des matières

Introduction

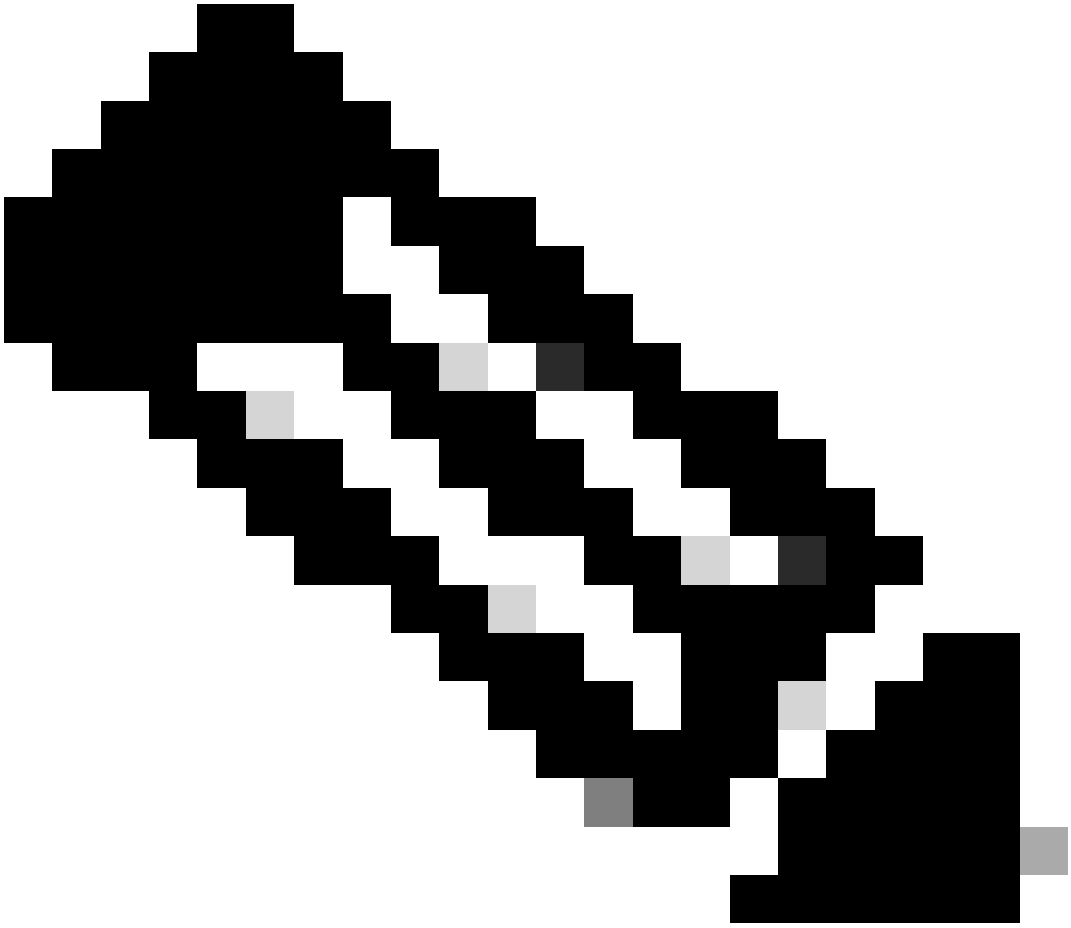
Ce document décrit ce qui se passe après l'expiration de votre abonnement Umbrella ou de votre version d'évaluation.



Remarque : Pour renouveler votre abonnement, acheter ou prolonger votre période d'essai, contactez votre gestionnaire de compte. Si vous ne connaissez pas leurs coordonnées, contactez le service commercial : https://umbrella.cisco.com/contact-us.

Explication

À la fin de l'abonnement ou de la période d'essai, si vous n'avez pas acheté le logiciel, votre organisation est automatiquement rétrogradée à un compte de surveillance DNS. La surveillance DNS est l'offre Cisco Umbrella la plus basique et offre beaucoup moins de fonctionnalités que notre offre Enterprise Umbrella.



Remarque : La résolution DNS continue de fonctionner même après l'expiration de l'abonnement ou de la version d'évaluation. La connectivité Internet n'est pas perdue et les sites Web ne cessent pas de se résoudre.

Modifications à l'expiration

- Vos statistiques dans les rapports continuent d'être enregistrées comme avant (y compris les catégorisations de sécurité), pour toutes les identités (par exemple, les réseaux, les clients itinérants, etc.) qui envoient toujours du trafic à Umbrella.
- L'accès aux rapports App Discovery et Destinations est supprimé.
- La mise en application de la stratégie est supprimée (inclut le client itinérant) :
  - Les paramètres de catégorie ne sont plus appliqués.
  - Les paramètres de sécurité ne sont plus appliqués. Tous les événements de sécurité sont autorisés.
  - Tous les paramètres de stratégie sont masqués et désactivés. Ils sont restaurés après l'abonnement à un forfait Umbrella.
- Seuls les réseaux et les périphériques réseau peuvent être gérés à partir du tableau de bord

; toutes les autres identités sont masquées.
- Aucune page de blocage n'est affichée : les comptes de surveillance DNS ne bloquent aucun trafic.

Client itinérant :

La résolution DNS et le cryptage DNS restent opérationnels (sans application de stratégie) après l'expiration d'un abonnement ou d'une version d'essai ; cependant, une liste de domaines internes à jour est nécessaire pour garantir que vos domaines locaux continuent à être résolus. Les clients d'itinérance Umbrella continuent de synchroniser la liste des domaines internes telle qu'elle est définie à l'expiration. Aucune modification de la liste des domaines internes ne peut être effectuée après l'expiration (si vous avez besoin d'une modification, et réabonnez-vous, écrivez-nous à umbrella-support@cisco.com. Vous ne prévoyez pas de vous réabonner ? Désinstaller le client itinérant). Il est important de noter que la résolution de domaine interne existante n'est pas affectée par l'expiration d'un abonnement ou d'un essai.

Nous ne pouvons pas prendre en charge le client d'itinérance sans abonnement actif.

Vous cherchez juste le cryptage DNS gratuit à Umbrella avec votre paquet de surveillance DNS ? Voir le projet DNScrypt.

Expiration de Secure Internet Gateway (SIG) Essentials

Si vous êtes un client potentiel, à l'expiration de votre abonnement ou de votre version d'évaluation SIG Essentials, vos paramètres de sécurité sont supprimés comme indiqué ci-dessus. Vous avez toujours accès à un tableau de bord de base qui vous permet d'afficher votre trafic DNS, mais les stratégies ne sont pas appliquées.

Si vous êtes un client de sécurité DNS Umbrella qui teste un package SIG, une fois la version d'évaluation terminée, vous revenez à vos paramètres d'évaluation précédents.

Les tunnels réseau IPsec et les règles de pare-feu sont conservés pendant sept jours. Au cours de cette période de sept jours, les tunnels réseau IPsec et les règles de pare-feu ne sont pas appliqués, mais les configurations sont automatiquement restaurées si l'abonnement est restauré (acheté ou essai prolongé). Au bout de ces sept jours, tous les tunnels réseau IPsec et toutes les règles de pare-feu sont automatiquement supprimés.

Étapes requises pour supprimer toutes les données d'Umbrella

Ces étapes sont nécessaires si vous souhaitez supprimer tout ou partie des données stockées par Umbrella.

Pour empêcher que les nouvelles données de requête DNS soient identifiées par Umbrella, vous devez arrêter d'envoyer des données DNS à Umbrella ou supprimer toutes les identités du tableau de bord qui existent encore :

1. Réseaux - Modifiez vos paramètres DNS pour ne plus transférer les requêtes vers Umbrella

et supprimez les adresses IP associées dans Déploiements > Identités principales > Réseaux.
2. Périphériques réseau - Suivez les instructions du fabricant pour supprimer l'intégration Umbrella sur votre périphérique. Supprimez le périphérique dans Déploiements > Identités principales > Périphériques réseau.
3. Ordinateurs itinérants : désinstallez le client Umbrella Roaming ou le module AnyConnect Umbrella Roaming Security de vos ordinateurs. Si vous avez été rétrogradé à la surveillance DNS, contactez le support pour que vos identités d'ordinateur itinérant soient supprimées. Notez que si les clients n'ont pas été désinstallés de votre machine, ils sont automatiquement réenregistrés dans le tableau de bord Umbrella si supprimés.
4. Appareils mobiles - Désinstallez l'application iOS ou Android de vos appareils. Si vous avez été rétrogradé à la surveillance DNS, contactez le support pour que vos identités d'appareil mobile soient supprimées. Notez que si les applications n'ont pas été désinstallées de votre ordinateur, elles sont automatiquement réenregistrées dans le tableau de bord Umbrella si elles sont supprimées.
5. Appareil virtuel - Supprimez de votre hyperviseur la machine virtuelle hébergeant l'appliance virtuelle. Si vous avez été rétrogradé à la surveillance DNS, contactez le support pour que vos identités d'appliance virtuelle soient supprimées.
6. Intégration Active Directory - Désinstallez les services du connecteur Umbrella AD de vos contrôleurs de domaine. Contactez le support technique pour supprimer vos identités Active Directory. Notez que si les connecteurs n'ont pas été désinstallés de votre ordinateur, ils renvoient automatiquement les identités AD au tableau de bord Umbrella si elles sont supprimées.
7. Réseaux internes - Supprimez les identités des réseaux internes dans Déploiements > Configuration > Réseaux internes.

Actuellement, les données de demande existantes ne peuvent pas être supprimées du tableau de bord Umbrella. Toutes les données expirent automatiquement 1 an après leur réception.

Pour supprimer des comptes utilisateur de votre organisation Umbrella, supprimez-les de Admin > Accounts. Notez que cela ne supprime que l'utilisateur de votre organisation, il ne les supprime pas d'Umbrella en général. Les utilisateurs qui souhaitent être complètement retirés d'Umbrella peuvent contacter l'assistance d'Umbrella ou privacy@cisco.com.

Si vous utilisez SAML pour l'authentification, désactivez SAML dans Admin > Authentication.

Pour mettre fin aux téléchargements d'Amazon S3, accédez à Admin > Log Management, puis cliquez sur « Stop Logging » dans la section Amazon S3.

Pour supprimer des clés API, accédez à Admin > API Keys, développez la clé API en question, puis cliquez sur « Delete ».

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.