Configuration de l'intégration Autotask et Umbrella

Table des matières

Introduction

Ce document décrit comment configurer l'intégration d'Autotask avec Umbrella.

Aperçu

L'intégration de Cisco Umbrella Autotask permet aux MSP d'être avertis des points d'extrémité potentiellement infectés nécessitant une attention en créant automatiquement des tickets dans Autotask. L'intégration pousse également les données d'état et de valeur de déploiement de service entre le tableau de bord Cisco Umbrella et un produit installé par Autotask Autotask (créé automatiquement) appelé « OpenDNS_Umbrella ».

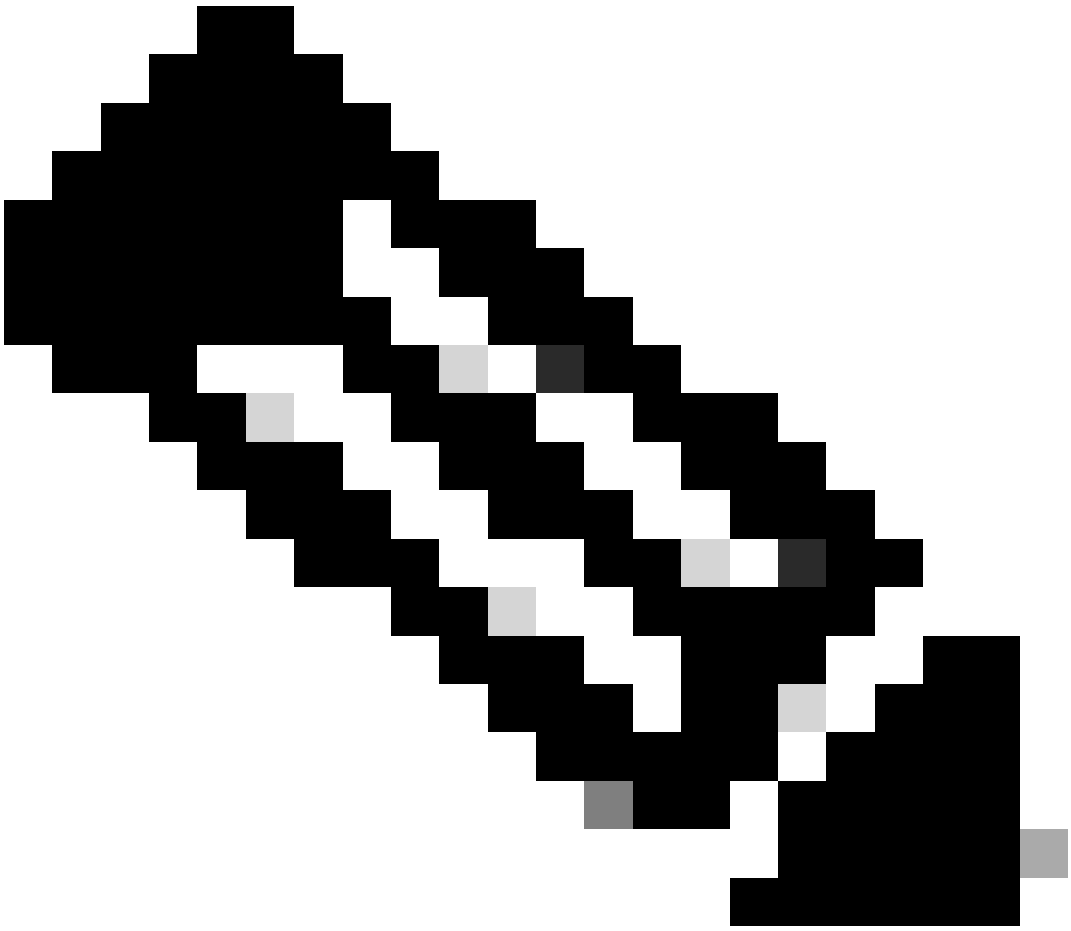
Étapes de l'intégration :

1. Conditions préalables
2. Authentification automatique initiale et configuration de Cisco Umbrella
3. Configurer la billetterie automatique
4. Mappage des entreprises dans Cisco Umbrella
5. Configuration de l'élément de configuration "OpenDNS_Umbrella"

Conditions préalables

Ce tableau présente la configuration logicielle de base requise pour l'installation :

le logiciel Cisco IOS	Version	Modèle hébergé
Cisco Umbrella	Sans objet	Hébergé
Masque Automatique	6.0 ou supérieur	Hébergé



Remarque : Vous ne pouvez ajouter qu'une (1) intégration PSA à la fois. Si vous avez déjà configuré une intégration Connectwise, vous devez la supprimer du tableau de bord avant de pouvoir poursuivre la configuration de la tâche automatique.

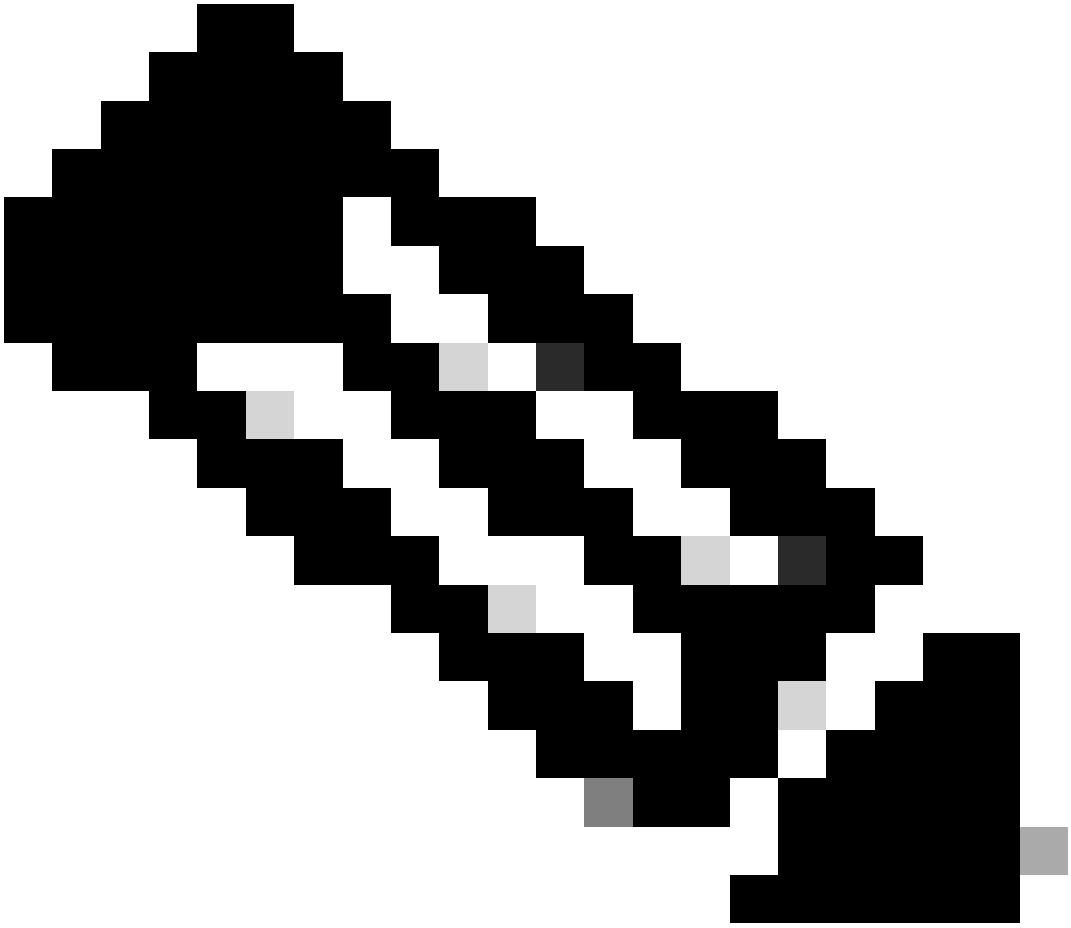
Authentification automatique initiale et configuration de Cisco

Umbrella

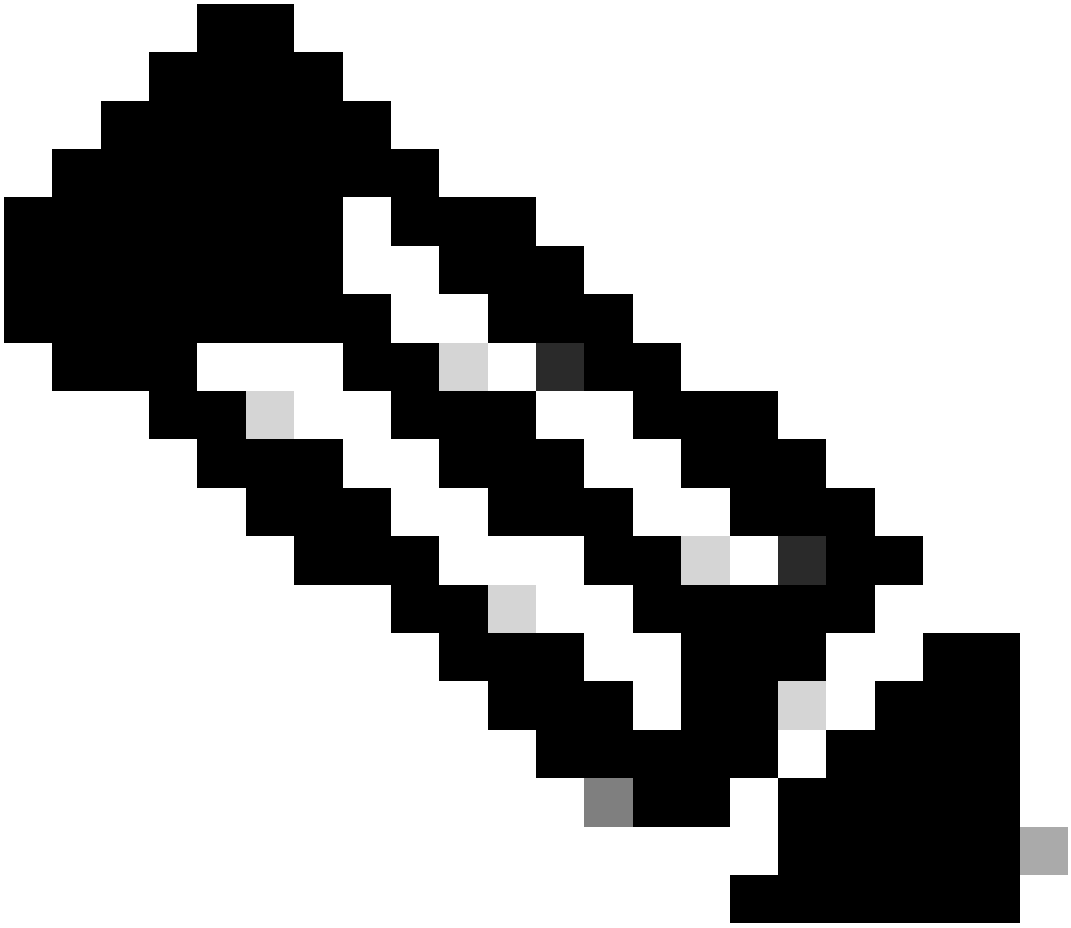
Établir un utilisateur pour l'authentification :

Pour se connecter à l'API AutoTask, Cisco Umbrella a besoin d'un identifiant de connexion pour Autotask. Il peut s'agir d'un nouveau compte de ressource utilisateur ou d'une connexion partagée existante.

- Utilisateur existant : Si vous disposez déjà d'une connexion Autotask que vous utilisez pour les intégrations, vérifiez que le compte est défini en tant qu'utilisateur API. Le compte ne doit pas utiliser l'authentification en deux étapes.
- Nouvel utilisateur : Pour créer une nouvelle ressource utilisateur :
    - Connectez-vous à votre tableau de bord AutoMasque.
    - Sélectionnez Admin > CiscoResources (Users) > New.
    - Renseignez les informations personnelles requises pour l'utilisateur sous les onglets RH.
    - Sous l'onglet Security, vérifiez que le niveau de sécurité pour cet utilisateur est défini sur "API User (system)".



Remarque : La case à cocher « Afficher les données non protégées » doit être activée pour l'utilisateur pour l'authentification dans Admin > Features & Settings > Resources/Users (HR) > Security > Protected Data Permission > [l'utilisateur pour l'authentification].

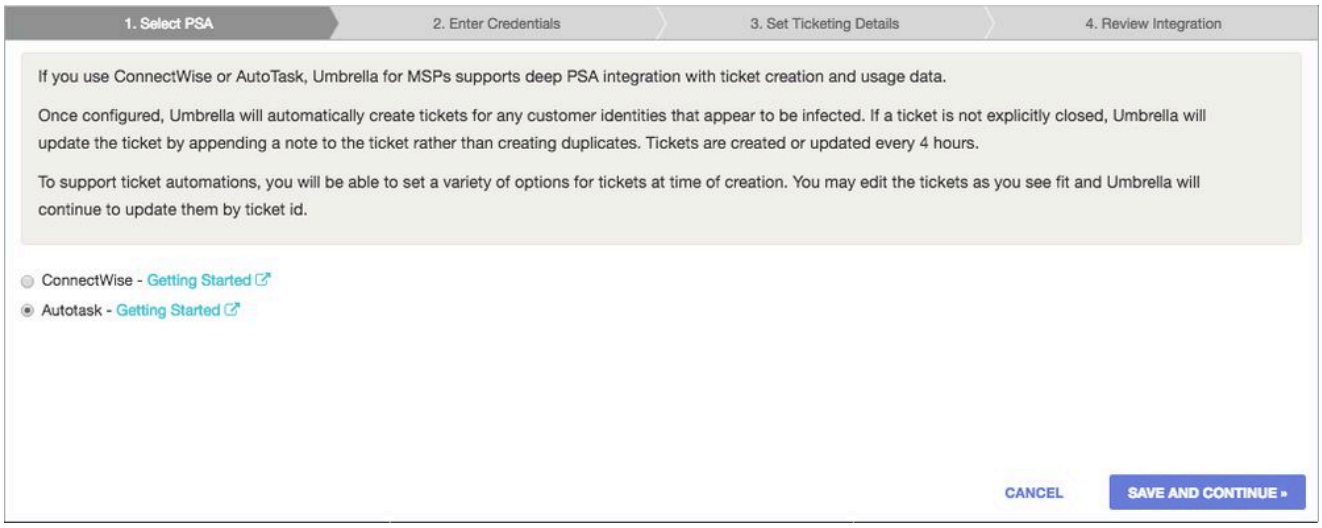


Remarque : À compter du 1er juin 2021, l'utilisateur pour l'authentification doit avoir un identificateur de suivi API défini. Pour plus d'informations, consultez l'article suivant de la base de connaissances Umbrella : Modifications apportées à l'intégration PSA Autotask avec Umbrella

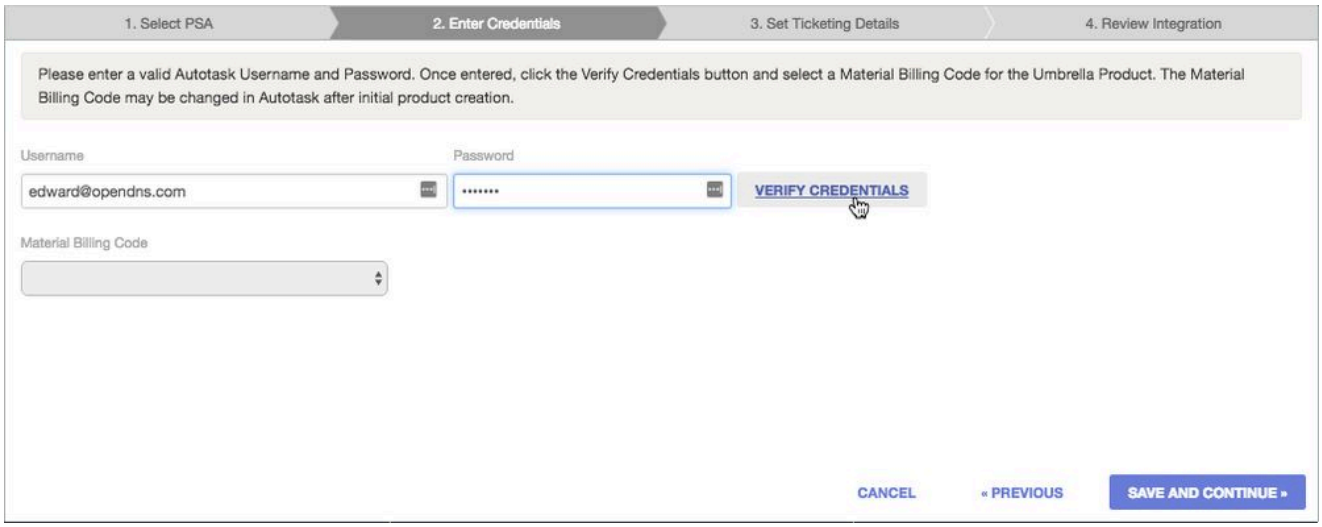
---

Une fois le compte créé ou sélectionné, accédez à Umbrella for MSPs.

1. Accédez à MSP Settings > PSA Integration Details.
2. Sélectionnez Set-Up Integration pour ouvrir l'assistant d'intégration.
3. Sous Select PSA, sélectionnez Autotask comme type d'intégration, puis sélectionnez Save and Continue.



4. Ensuite, vous êtes invité à saisir le compte sélectionné précédemment (adresse e-mail et mot de passe) et à vérifier vos informations d'identification pour sélectionner un code de facturation matériel :



Sélectionnez le code de facturation des matières approprié :

Une fois que vous vous êtes authentifié, le code de facturation du matériel affiche une sélection avec votre code de facturation du matériel AutoTask existant. Vous pouvez ultérieurement modifier le code de facturation du matériel pour le produit "OpenDNS_Umbrella" dans Autotask si vous le souhaitez.

Sélectionnez Enregistrer et continuer.

Configurer la billetterie automatique

Cisco Umbrella pour MSP vous avertit de manière proactive des hôtes infectés qui nécessitent une action en créant des tickets dans une file d'attente du centre de service Autotask. Lorsqu'il est correctement intégré, Cisco Umbrella vérifie automatiquement les hôtes infectés qu'il contient et crée des tickets pour vous.

Comment un ticket de file d'attente de service est généré par Cisco Umbrella :

Actuellement, ce critère doit être satisfait pour générer un ticket dans une file d'attente du centre de service Autotask :

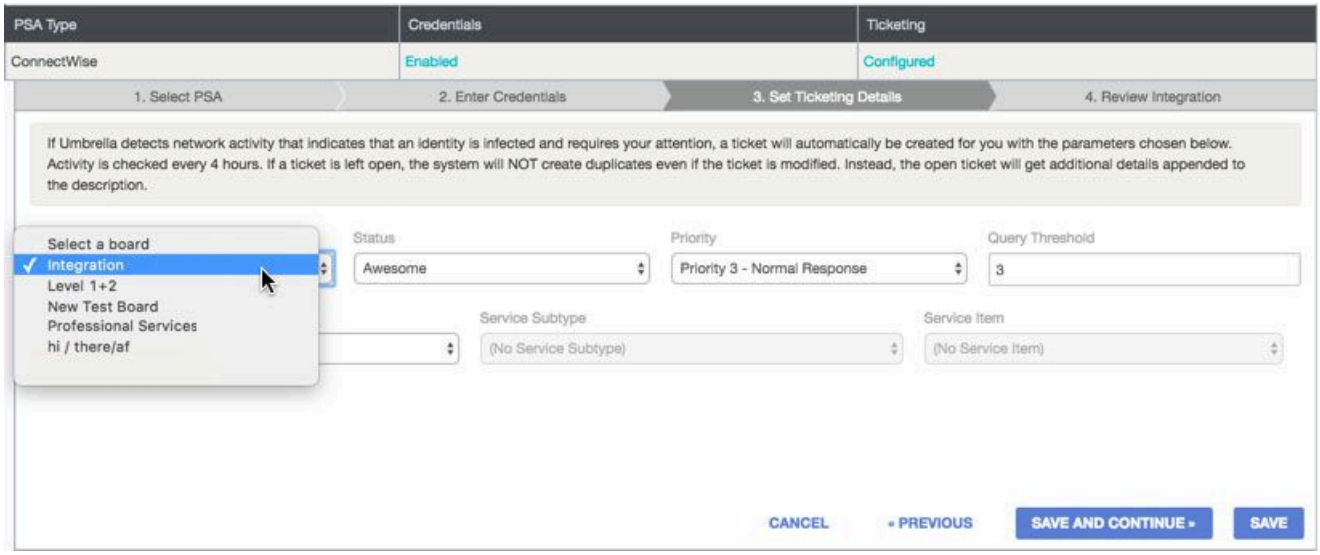
- Cisco Umbrella surveille vos identités pour détecter le blocage de l'« activité de botnet ». Cet exercice indique qu'un terminal est infecté et que Cisco Umbrella bloque activement les tentatives de « rappel à la maison » pour les mises à jour, pour le téléchargement de données volées ou pour faire partie d'un botnet. Si une identité de votre entreprise tente à plusieurs reprises d'atteindre un site classé comme « botnet ». Cela signifie que bien que Cisco Umbrella contienne les dommages, la machine est infectée par un programme malveillant et nécessite une action supplémentaire de votre part pour y remédier.
- Cisco Umbrella ne crée pas d'alertes lorsqu'il empêche les infections pour des catégories telles que les programmes malveillants ou les téléchargements en voiture, car ces événements empêchent l'utilisateur de visiter des sites malveillants. Aucune action supplémentaire n'est requise.
- Toutes les quatre heures, Cisco Umbrella vérifie toutes les organisations mappées aux organisations PSA dans votre console Cisco Umbrella pour MSP.
- Si une identité unique, par exemple un ordinateur sur lequel un agent est installé ou un réseau, comporte plus d'événements de botnet que le « seuil de requête » (trois par défaut) dans le bloc de quatre heures, Cisco Umbrella Integration ouvre automatiquement un ticket dans le Centre de service défini par l'intégration des détails de la billetterie dans l'Assistant d'intégration. Vous pouvez y modifier le seuil de la requête.
- Si la même identité continue de générer une activité de botnet supplémentaire dans la fenêtre de quatre heures suivante (ou une autre fenêtre temporelle après celle-ci) et que le ticket est toujours ouvert, des données supplémentaires sont ajoutées au ticket.
    - Cisco Umbrella référence le ticket par son numéro de ticket et ne crée pas de doublons inutiles même si un ticket est déplacé vers une autre file d'attente du centre de service ou si la copie est modifiée.
- Si le ticket a été marqué comme Fermé, un nouveau ticket est créé car il s'agit d'un nouvel événement de sécurité lié au botnet (tel qu'une réinfection) pour la même identité.

Définir les détails des tickets :

Si vous utilisez l'assistant d'intégration, vous êtes à l'étape 3 de l'assistant d'intégration. Si vous configurez la billetterie ultérieurement, sélectionnez PSA Integration > Integration Details.Vos informations d'identification s'affichent désormais comme activées, mais les tickets comme désactivés.

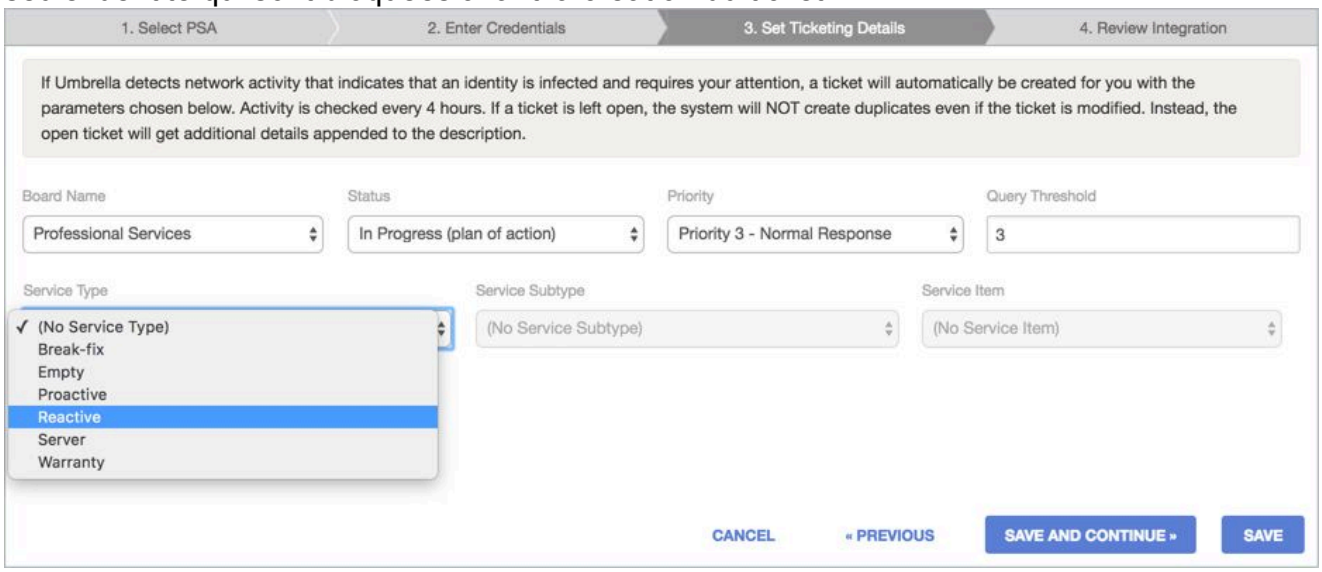
1. Sélectionnez Ticketing > Disabled pour définir les détails du ticket.

2. Sélectionnez d'abord une file d'attente. Cet exemple utilise la file d'attente de tri pour laisser des tickets dans. Vous devez d'abord sélectionner la file d'attente pour remplir les champs supplémentaires :



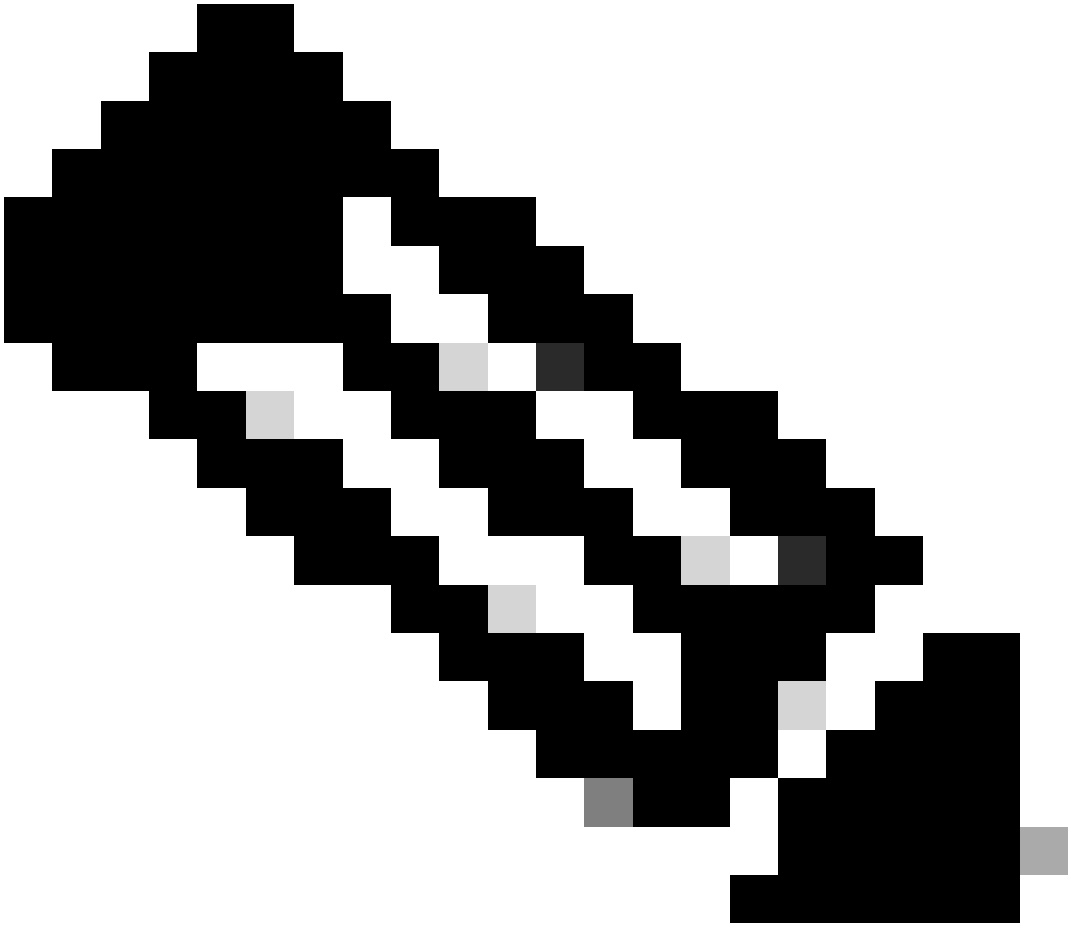
215690567

3. Après avoir sélectionné votre file d'attente, attendez quelques secondes que les détails soient renseignés pour les champs restants, puis sélectionnez le champ approprié. Chaque champ du tableau de bord Cisco Umbrella correspond au champ équivalent dans les tickets de la file d'attente du centre de service sélectionnée.
   Les paramètres exacts de chaque champ varient légèrement selon votre implémentation. Un champ à noter est le Seuil de requête, qui est le nombre d'activités de botnet à partir d'une seule identité qui sont bloquées avant la création du ticket.



4. Remplissez tous les champs, le cas échéant, puis sélectionnez Enregistrer et continuer.

La quatrième et dernière étape de l'intégration vous permet de vérifier tous vos paramètres pour vous assurer qu'ils correspondent à vos attentes.



Remarque : Si vous souhaitez générer un ticket de test, veuillez contacter l'assistance Cisco Umbrella et en faire la demande. Ce ticket est conforme à vos règles de billetterie AutoTask.

Mappage des entreprises dans Cisco Umbrella

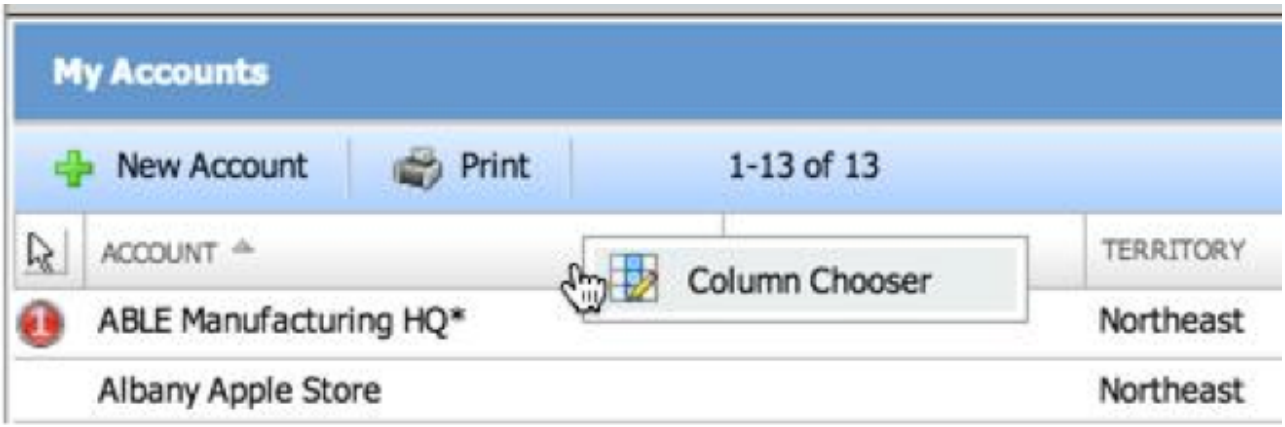
La mise en correspondance des entreprises clientes permet l'intégration et l'association des tickets et des produits installés au compte client. Le produit installé « OpenDNS_Umbrella » contient des statistiques précieuses sur l'utilisation et l'efficacité de Cisco Umbrella par les clients et est configuré à l'étape 5.

Pour synchroniser les clients entre Autotask et Cisco Umbrella, vous devez disposer de l'ID de compte de chaque client. Cette option n'est pas affichée par défaut dans le masque automatique.

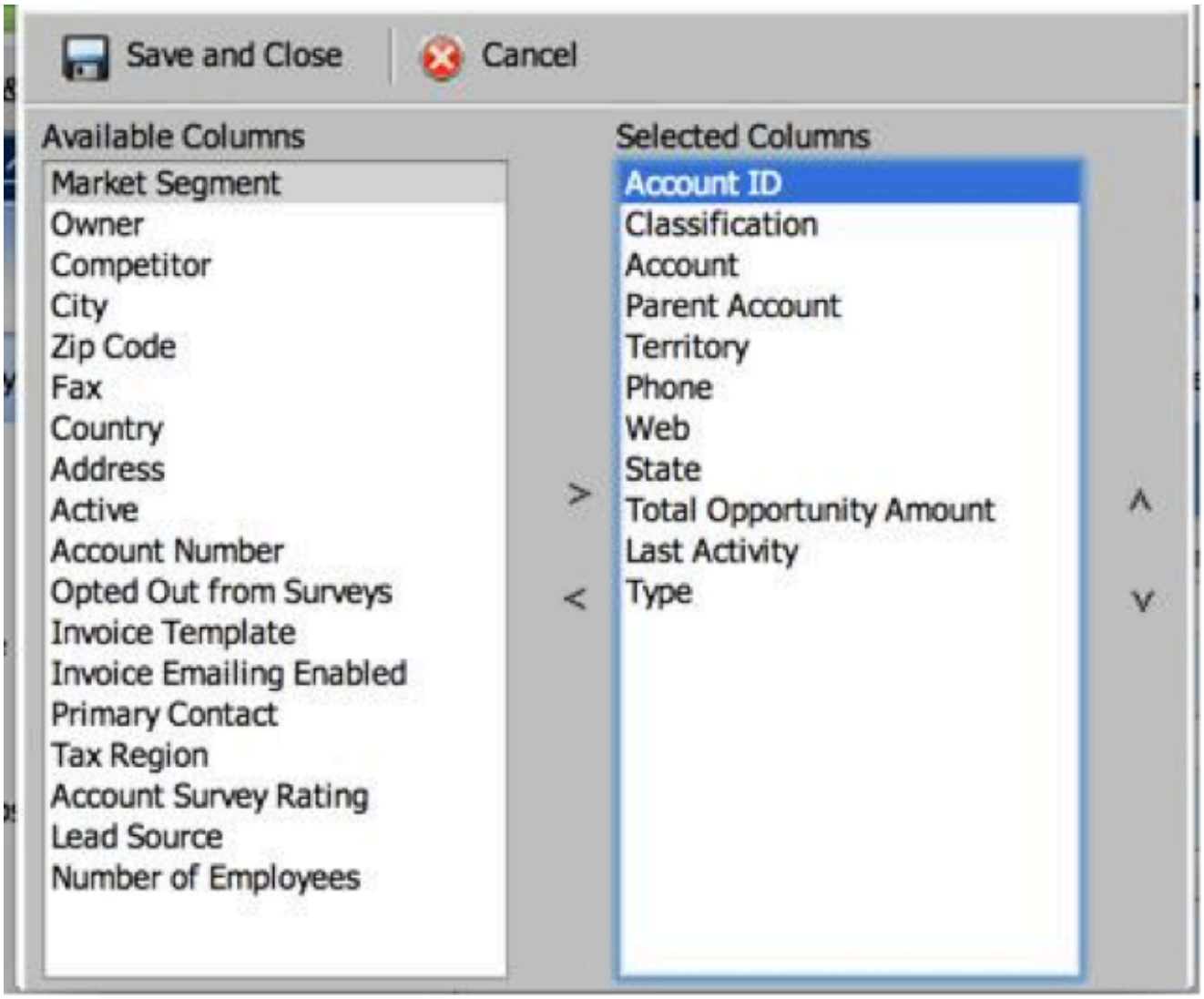
1. Pour afficher l'ID client dans le tableau de bord du masque automatique, sélectionnez CRM, puis choisissez Mes comptes dans la liste déroulante. Chaque compte a un ID de compte dans les propriétés de ce compte visibles en double-cliquant sur le nom du compte qui ouvre

une fenêtre contextuelle affichant l'ID de compte.

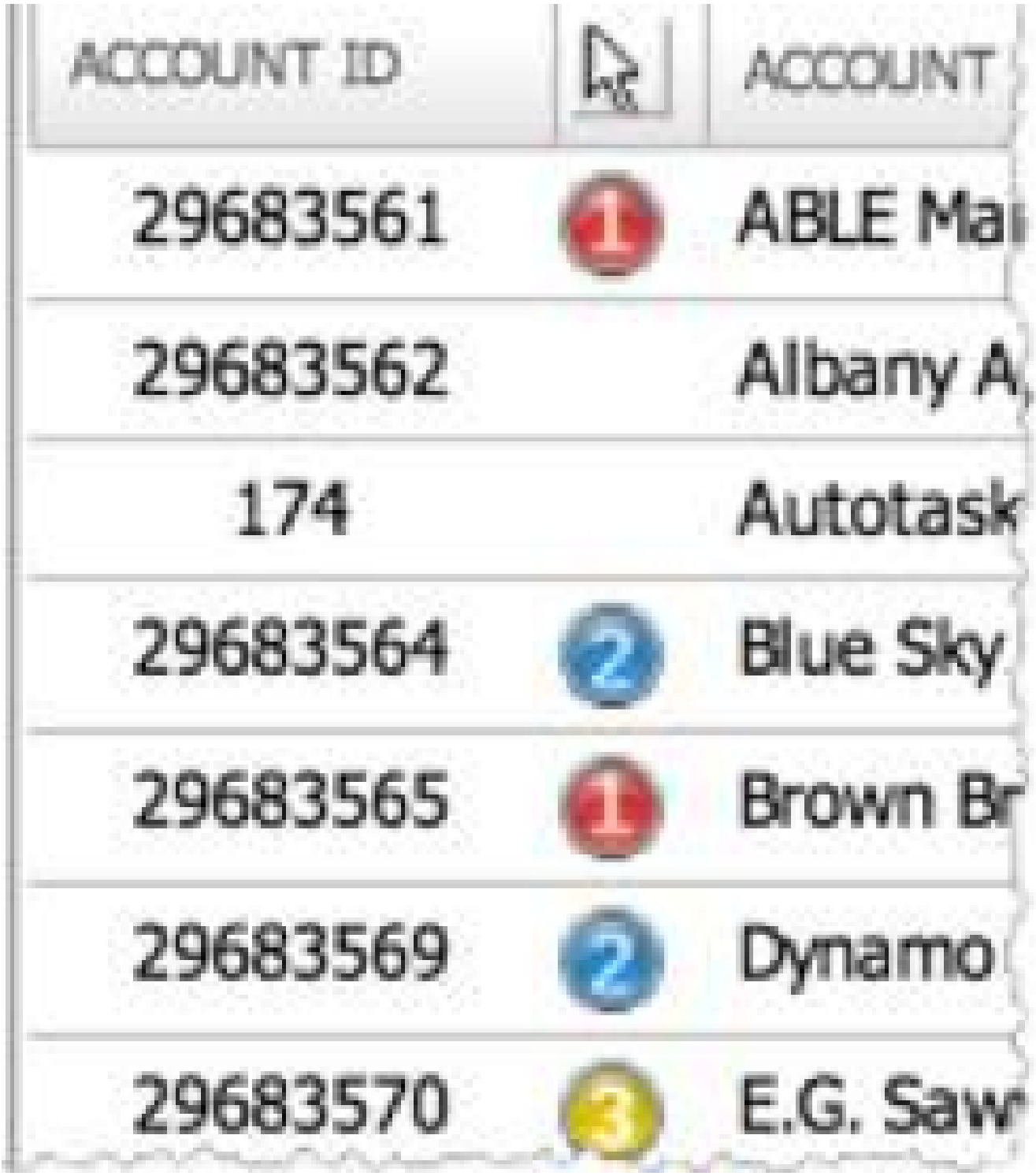
2. Pour afficher tous les ID de compte de vos clients dans la présentation, vous devez afficher une nouvelle colonne. Cliquez avec le bouton droit sur les colonnes pour afficher le sélecteur de colonnes.



3. Dans le sélecteur de colonnes, déplacez la colonne ID de compte vers Colonnes sélectionnées.



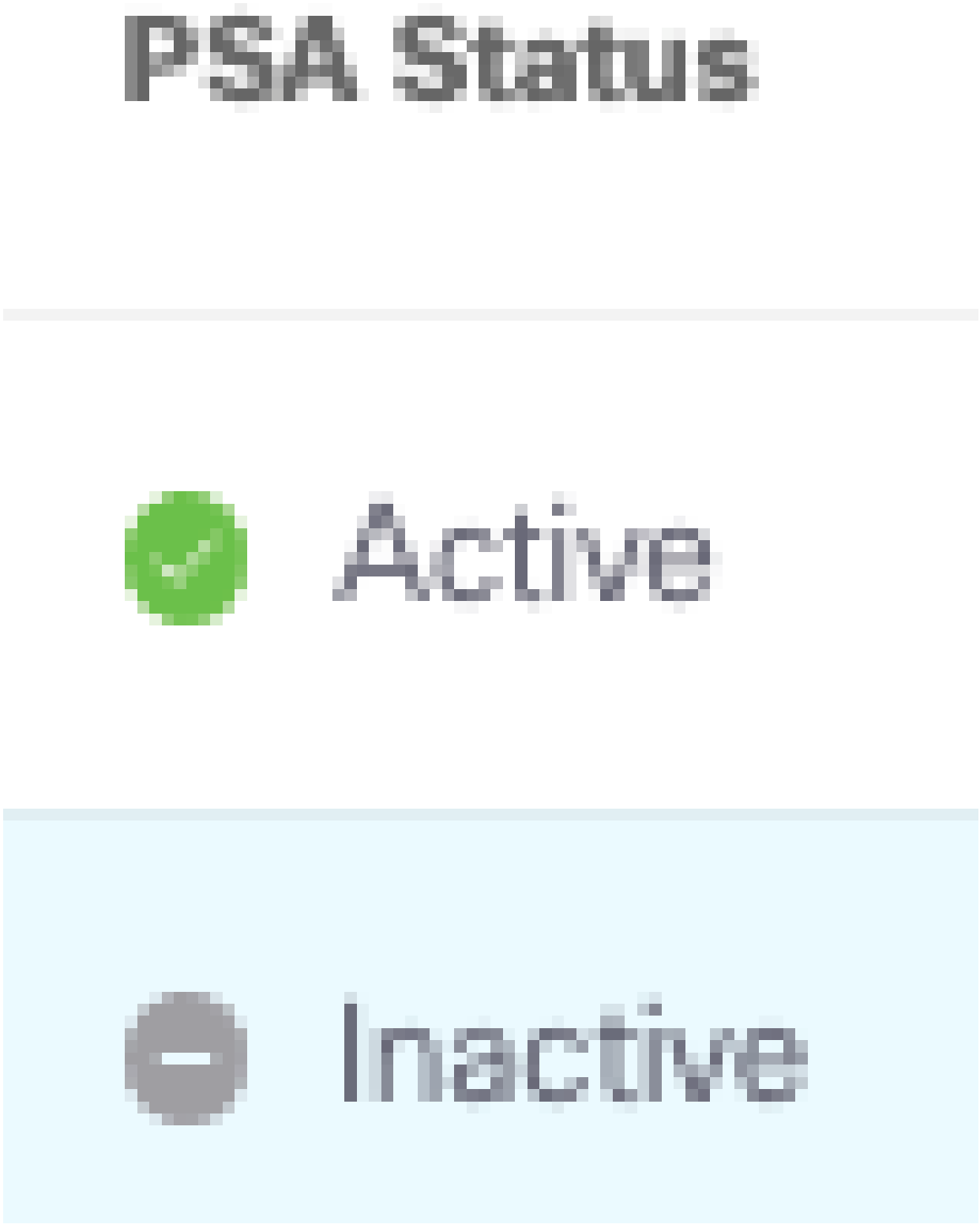
Vous voyez ainsi l'ID de compte du client :



4. Une fois que vous avez l'ID de compte de votre client, retournez à Cisco Umbrella pour les prestataires de services MSP.
5. Accédez à Gestion des clients pour afficher la liste des clients que vous avez configurés dans votre console
   Remarque : Si aucun client n'est répertorié ici, vous devez ajouter des clients à votre MSP Cisco Umbrella for MSPs. Veuillez lire le Guide de l'utilisateur de Cisco Umbrella for MSPs pour plus d'informations.
6. Sélectionnez ensuite le client à mapper sur le masque automatique. Cet exemple utilise « Able Manufacturing Co. »
7. Nous avons découvert précédemment qu'Able Manufacturing Co. avait un ID de compte de 29683561. Sélectionnez le nom du client, puis saisissez l'ID de compte de la société dans le

champ ID PSA.

8. Sélectionnez Save pour confirmer la modification. Vous recevez un message de confirmation concernant l'intégration en cours d'activation. À partir de ce moment, l'ID PSA s'affiche en regard du client pour lequel il est activé dans les détails du client.
9. Pour confirmer que votre intégration est activée, accédez à Rapports centralisés > État du déploiement. S'il est opérationnel, une colonne État PSA est remplie.
    - Les organisations avec des ID PSA valides s'affichent avec un état Actif vert.
    - Les organisations qui n'ont pas de valeur d'ID PSA affichent un état Inactif gris.



360053576152

Configuration de l'élément de configuration "OpenDNS_Umbrella" (facultatif)

Une fois l'ID de société PSA correctement intégré, un produit installé/élément de configuration nommé OpenDNS_Umbrella est automatiquement créé.

Vous pouvez afficher l'élément de configuration sous Répertoire > Comptes, puis sélectionner l'un des comptes que vous avez intégrés à l'étape 4. Dans ce compte, il y a maintenant un élément de configuration pour OpenDNS_Umbrella.

Notez que par défaut, l'élément de configuration inclut tous les champs possibles et les champs Cisco Umbrella que nous avons ajoutés dans l'intégration. Certains champs ne sont pas renseignés car ils ne s'appliquent pas à Cisco Umbrella, comme Marque ou Marque et modèle.

Pour modifier le produit afin qu'il n'inclue pas ces champs, configurez un type de configuration unique pour Cisco Umbrella.

Configuration du type de configuration

Les éléments de configuration créés dans Autotask via l'intégration Cisco Umbrella créent des champs définis par l'utilisateur (UDF) pour vos informations mises à jour automatiquement Cisco Umbrella. Par défaut, un nouveau produit affiche toutes les FDU et un type d'élément de configuration est recommandé. En raison des limitations de l'API Autotask actuelle, la création d'un type d'élément de configuration dans Autotask se limite à une intervention manuelle de votre part ou de votre administrateur Autotask. Ce tableau fournit la liste de tous les champs qui doivent être ajoutés à votre type d'élément de configuration.

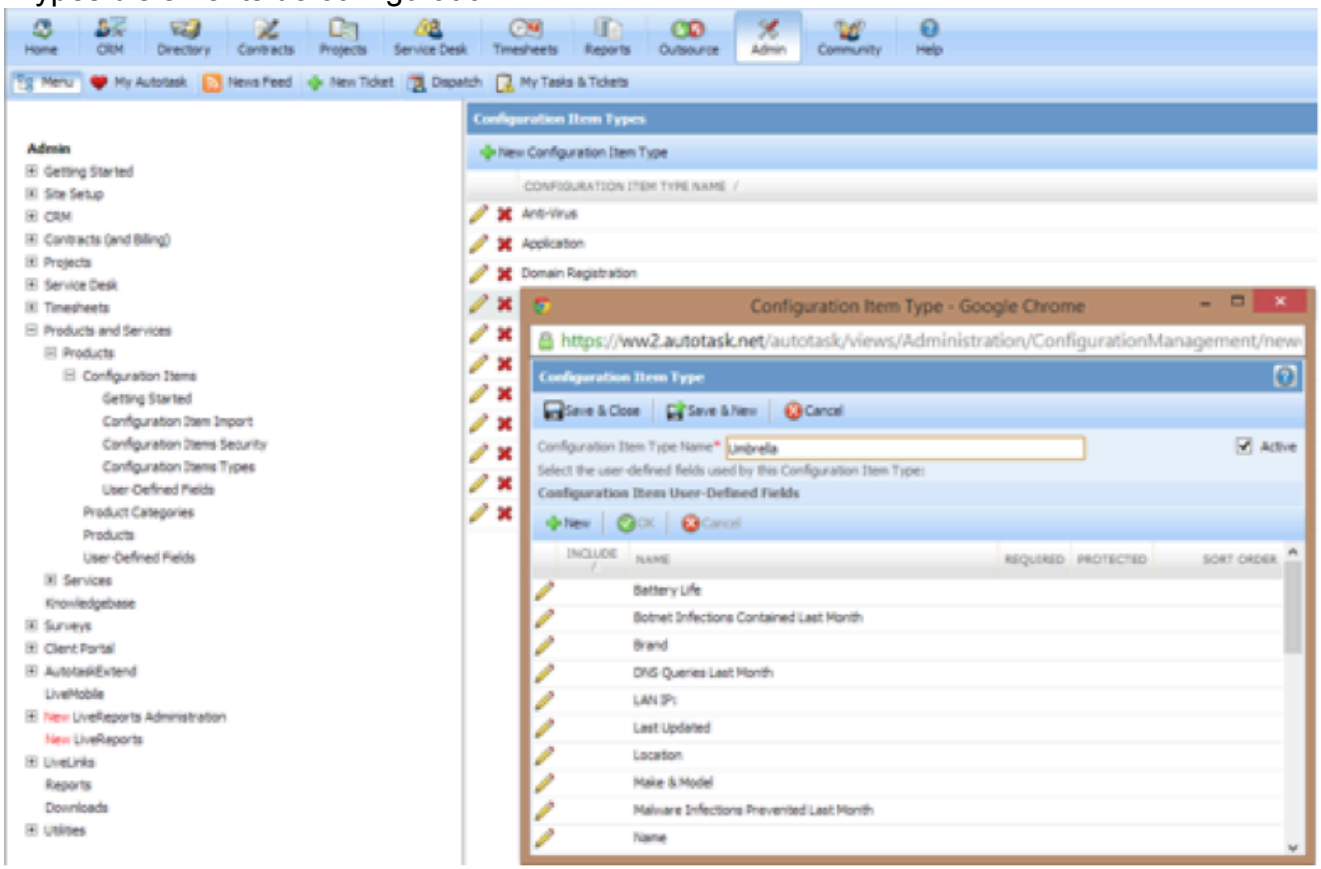
#	Nom du champ	Type
1	ID organisation	Texte (une ligne)
2	Dernière mise à jour	Texte (une ligne)
3	Emballage	Texte (une ligne)
4	Sièges	Texte (une ligne)

5	Total réseaux	Texte (une ligne)
6	Réseaux actifs au cours des 7 derniers jours	Texte (une ligne)
7	Réseaux inactifs au cours des 7 derniers jours	Texte (plusieurs lignes)
8	Agents parapluie déployés	Texte (une ligne)
9	Agents parapluie actifs au cours des 7 derniers jours	Texte (une ligne)
10	Agents parapluie inactifs au cours des 7 derniers jours	Texte (plusieurs lignes)
11	Requêtes DNS du mois dernier	Texte (une ligne)
12	Infections de programmes malveillants évitées le mois dernier	Texte (une ligne)
13	Infections de botnets contenues le mois dernier	Texte (une ligne)
14	Principaux domaines le mois dernier	Texte (plusieurs lignes)
15	Principaux domaines bloqués le mois dernier	Texte (plusieurs lignes)

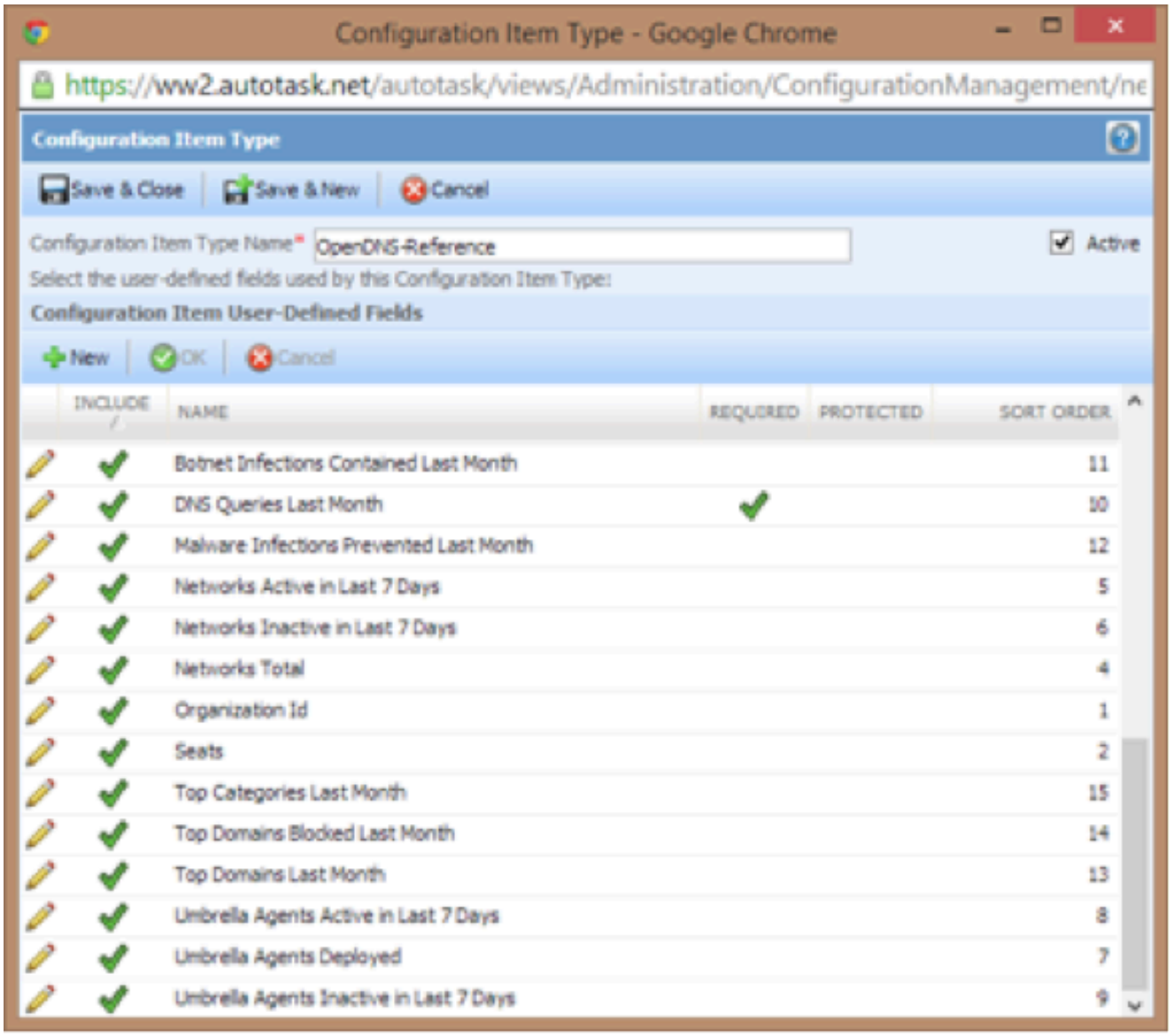
16	Premières catégories le mois dernier	Texte (plusieurs lignes)

Pour les utilisateurs qui ne sont pas familiers avec la configuration des nouveaux types d'éléments de configuration dans AutoTask, veuillez utiliser ces instructions pour créer le nouvel enregistrement dans le système :

1. Connectez-vous à Autotask en tant qu'administrateur.
2. Accédez à la section Admin à l'aide du menu supérieur.
3. Accédez à Produits et services > Produits > Éléments de configuration et sélectionnez "Types d'éléments de configuration".

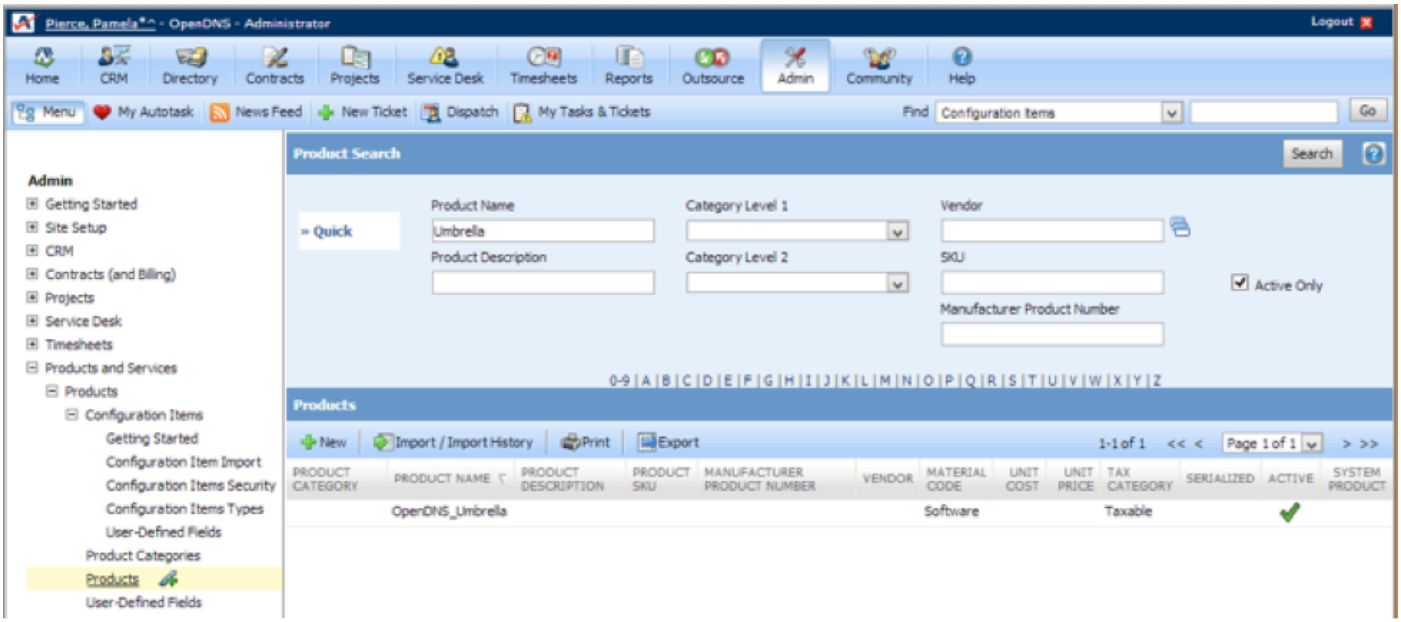


4. Sélectionnez l'option de menu Nouveau type d'élément de configuration.
5. Entrez un nom pour votre nouveau type d'élément de configuration.
6. Sélectionnez New et entrez les informations du premier champ en haut de la page.
7. Répétez l'étape 6 jusqu'à ce que vous ayez ajouté tous les champs du tableau au nouveau type d'élément.



8. Enregistrez et fermez votre nouveau type d'élément de configuration.

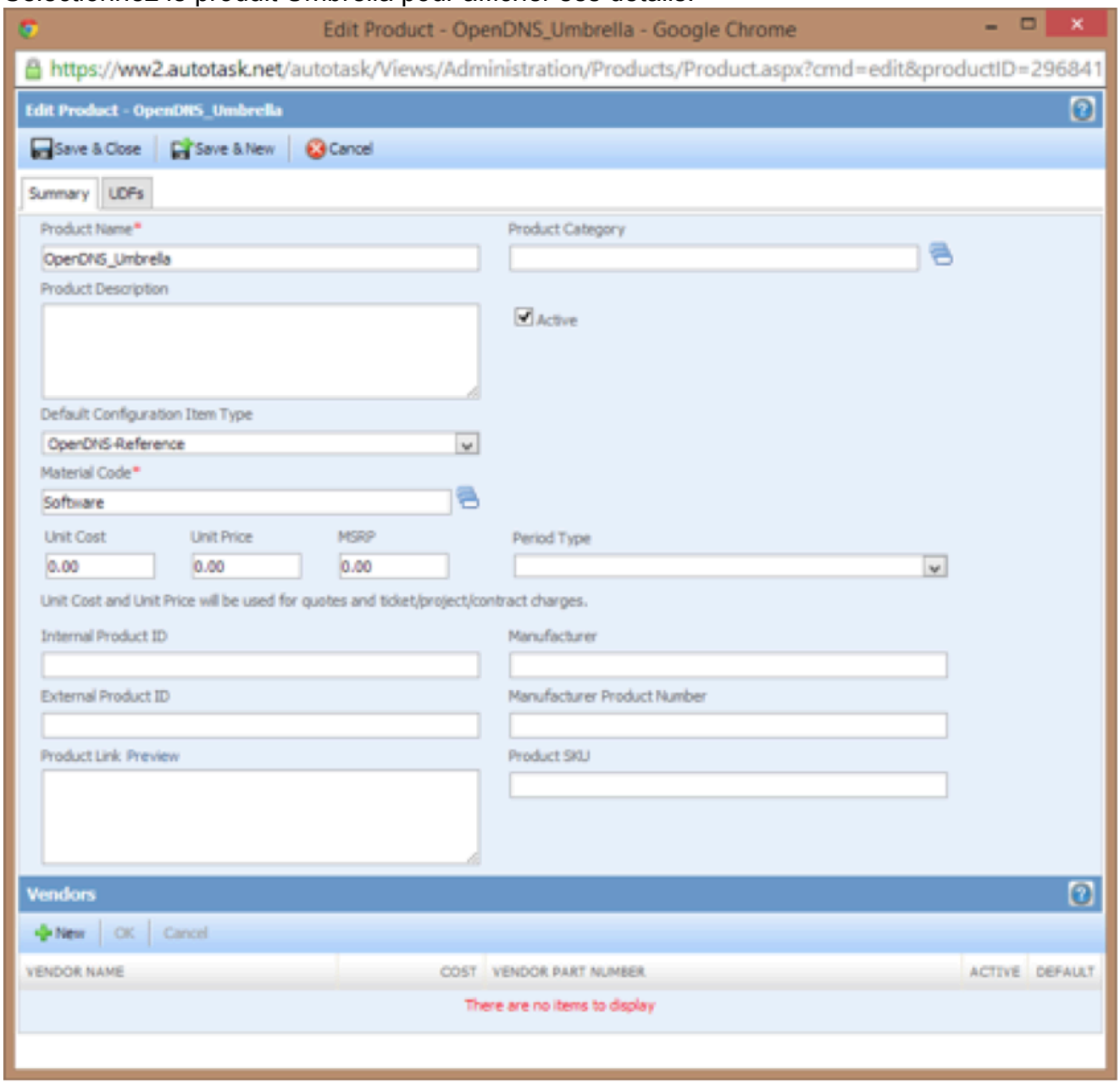
Configuration du produit



L'intégration Cisco Umbrella crée automatiquement un produit au sein de votre implémentation AutoTask pour lier les éléments de configuration au moment de leur création. Une fois le produit créé dans votre système, Cisco Umbrella vous recommande de mettre à jour la définition du produit avec des paramètres qui reflètent au mieux les normes et les besoins de votre entreprise.

Pour identifier la définition du produit et mettre à jour ses paramètres, procédez comme suit :

1. Connectez-vous à Autotask en tant qu'administrateur.
2. Accédez à la section Admin à l'aide du menu supérieur.
3. Accédez à Produits et services > Produits et sélectionnez Produits.
4. Saisissez « Umbrella » dans le champ de recherche Nom du produit et sélectionnez Rechercher.
5. Sélectionnez le produit Umbrella pour afficher ses détails.



6. Mettez à jour la définition du produit pour refléter les paramètres souhaités.
7. Sélectionnez Enregistrer et fermer.

Remarques :

- Ne modifiez pas la chaîne Nom du produit de "OpenDNS_Umbrella" en une autre chaîne. Cela interrompt l'intégration, mais si vous l'avez renommée, renommez-la de nouveau pour résoudre le problème.
- Assurez-vous que « Actif : est sélectionné comme vous le voyez dans la capture d'écran.

Les définitions de chacun des champs Tâche automatique Cisco Umbrella qui sont mis à jour et inclus dans l'élément de configuration sont répertoriées dans ce tableau :

Champ	Description
ID organisation	ID organisation interne parapluie
Dernière mise à jour	Date à laquelle la dernière synchronisation avec Umbrella a eu lieu
Sièges	Nombre total de postes appliqués à cette société.
Total réseaux	Nombre total de réseaux appliqués à cette société
Réseaux actifs (7 jours)	Nombre total de réseaux actifs au cours des sept derniers jours
Réseaux inactifs (7 jours)	Liste des noms de réseau inactifs au cours des sept derniers jours
Agents parapluie déployés	Nombre d'agents Umbrella Roaming déployés
Agents parapluie actifs 7 jours	Nombre d'agents Umbrella Roaming actifs au cours des sept derniers jours

Agents parapluie inactifs 7 jours	Noms des identités d'agent Umbrella Roaming inactives au cours des sept derniers jours
Requêtes DNS du mois dernier	Nombre total de demandes DNS pour cette société au cours du mois civil précédent
Infections de programmes malveillants évitées le mois dernier	Nombre de sites hébergeant des programmes malveillants dont l'accès a été interdit au cours du mois civil précédent
Infections de botnets contenues le mois dernier	Nombre de sites hébergeant la commande et le contrôle de botnet qui n'ont pas pu accéder au cours du mois civil précédent
Principaux domaines le mois dernier	Liste des noms des domaines les plus consultés au cours du mois civil précédent
Principaux domaines bloqués le mois dernier	Liste des noms des domaines les plus fréquemment bloqués au cours du mois civil précédent
Premières catégories le mois dernier	Liste des catégories de contenu les plus fréquemment demandées au cours du mois civil précédent, y compris le nombre de demandes par catégorie

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.