Configurazione dell'integrazione tra attività automatica e Umbrella

Sommario

Introduzione

Questo documento descrive come configurare l'integrazione di AutoTask con Umbrella.

Panoramica

L'integrazione Cisco Umbrella Autotask consente ai provider di servizi multimediali di essere informati sugli endpoint potenzialmente infetti che richiedono attenzione creando automaticamente ticket in Autotask. L'integrazione esegue inoltre il push dei dati relativi allo stato di distribuzione dei servizi e al valore tra Cisco Umbrella Dashboard e un prodotto installato con attività automatica (creato automaticamente) denominato "OpenDNS_Umbrella".

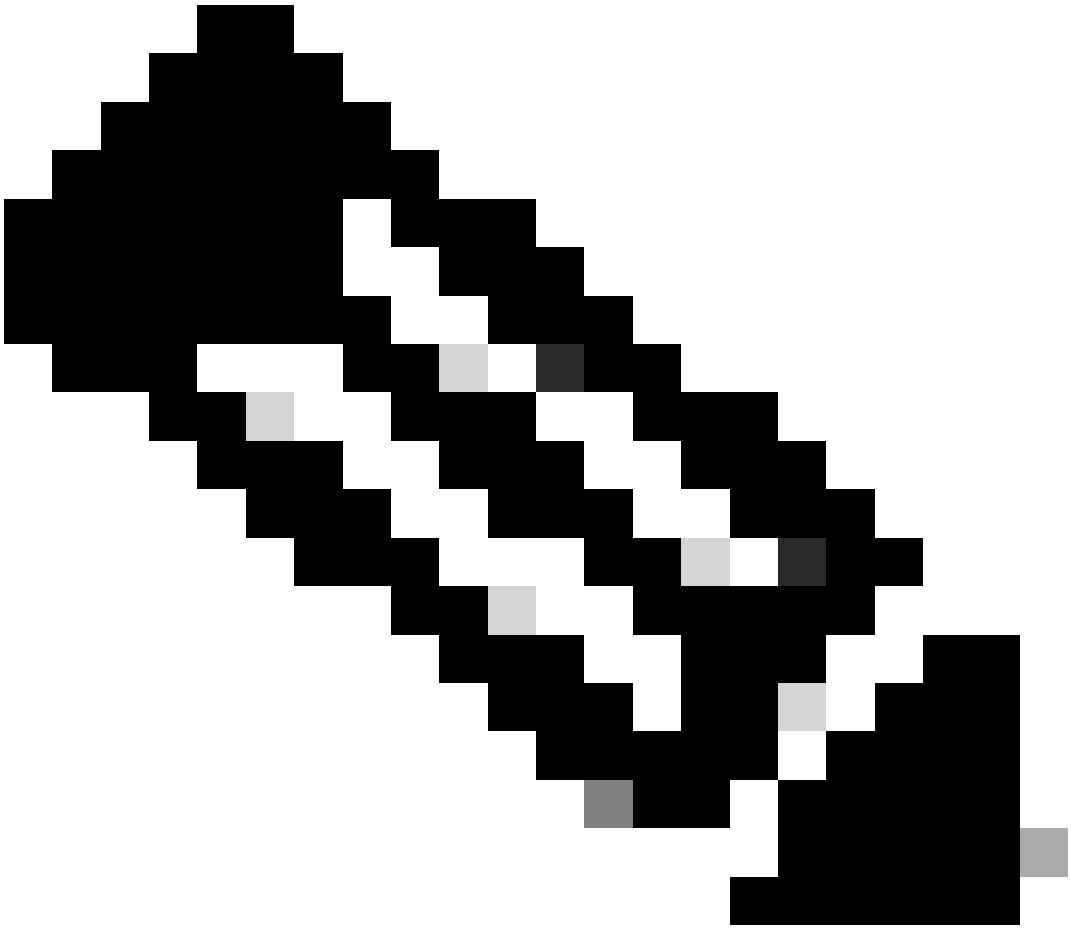
Passi per l'integrazione:

1. Prerequisiti
2. Autenticazione iniziale del task e configurazione di Cisco Umbrella
3. Configura ticket attività automatica
4. Mappatura delle aziende in Cisco Umbrella
5. Impostazione dell'elemento di configurazione "OpenDNS_Umbrella"

Prerequisiti

Questa tabella contiene i requisiti software di base per l'installazione:

Software	Version	Modello ospitato
Cisco Umbrella	Non applicabile	Ospitato
Task automatico	6.0 o superiore	Ospitato



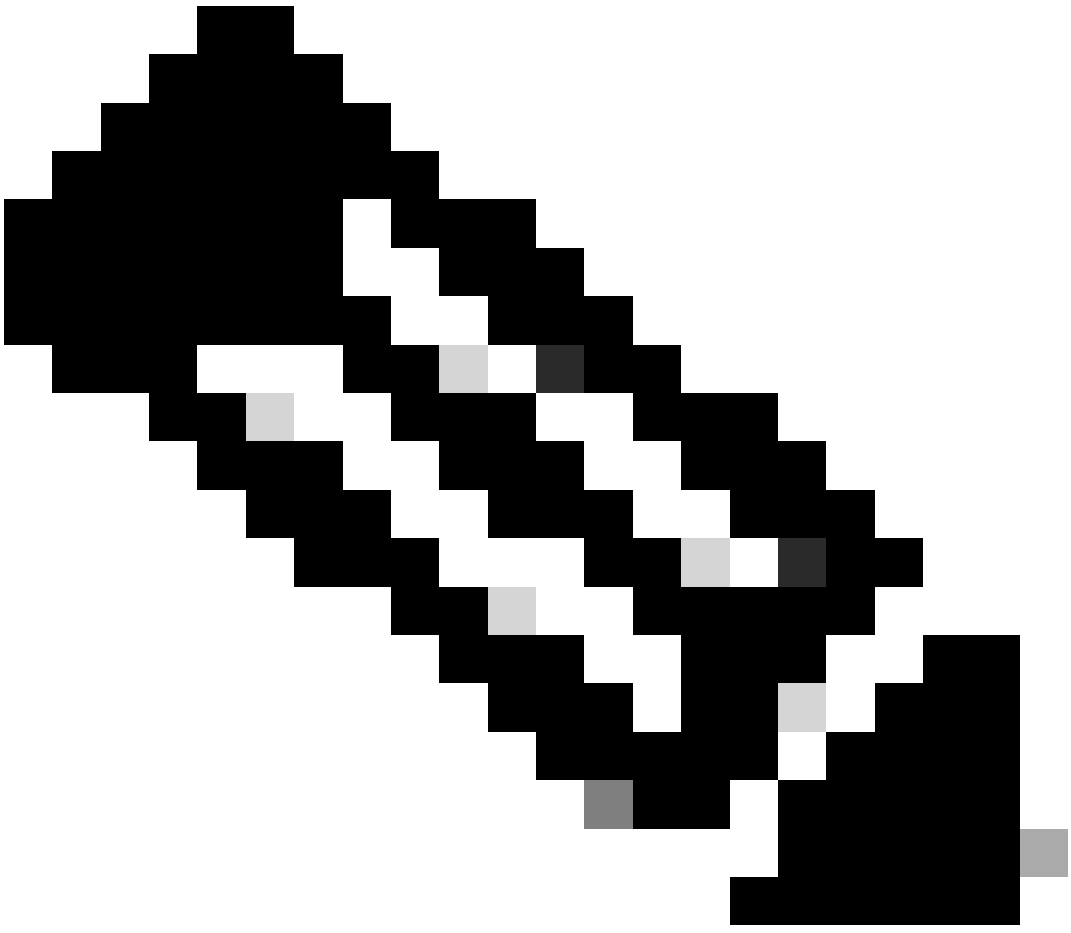
Nota: È possibile aggiungere una sola (1) integrazione PSA alla volta. Se è già stata configurata un'integrazione Connectwise, è necessario eliminarla dal dashboard prima di procedere con l'installazione dell'operazione automatica.

Autenticazione iniziale del task e configurazione di Cisco Umbrella

Stabilire un utente per l'autenticazione:

Per connettersi all'API AutoTask, Cisco Umbrella richiede un accesso per l'operazione automatica. Può trattarsi di un nuovo account della risorsa utente o di un account di accesso condiviso esistente.

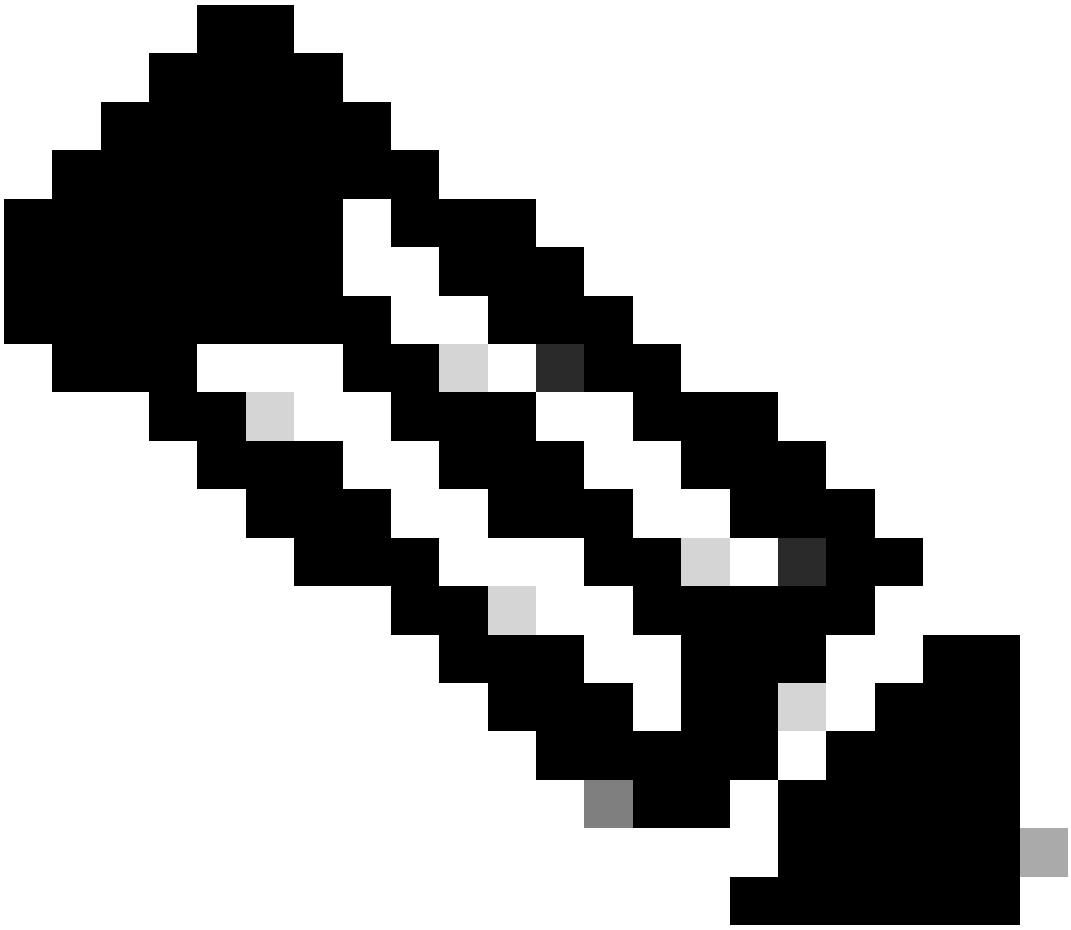
- Utente esistente: Se si dispone già di un accesso automatico da utilizzare per le integrazioni, verificare che l'account sia impostato come utente API. L'account non deve utilizzare l'autenticazione in due passaggi.
- Nuovo utente: Per creare una nuova risorsa utente:
  - Accedere al dashboard Attività automatica.
  - Selezionare Admin > Risorse Cisco (Utenti) > Nuovo.
  - Compilare i requisiti di informazioni personali per l'utente nelle schede HR.
  - Nella scheda Protezione, verificare che il livello di protezione per l'utente sia impostato su "Utente API (sistema)".



Nota: L'utente per l'autenticazione deve avere la casella di controllo "Visualizza dati non protetti" selezionata in Amministrazione > Funzionalità e impostazioni > Risorse/Utenti

---

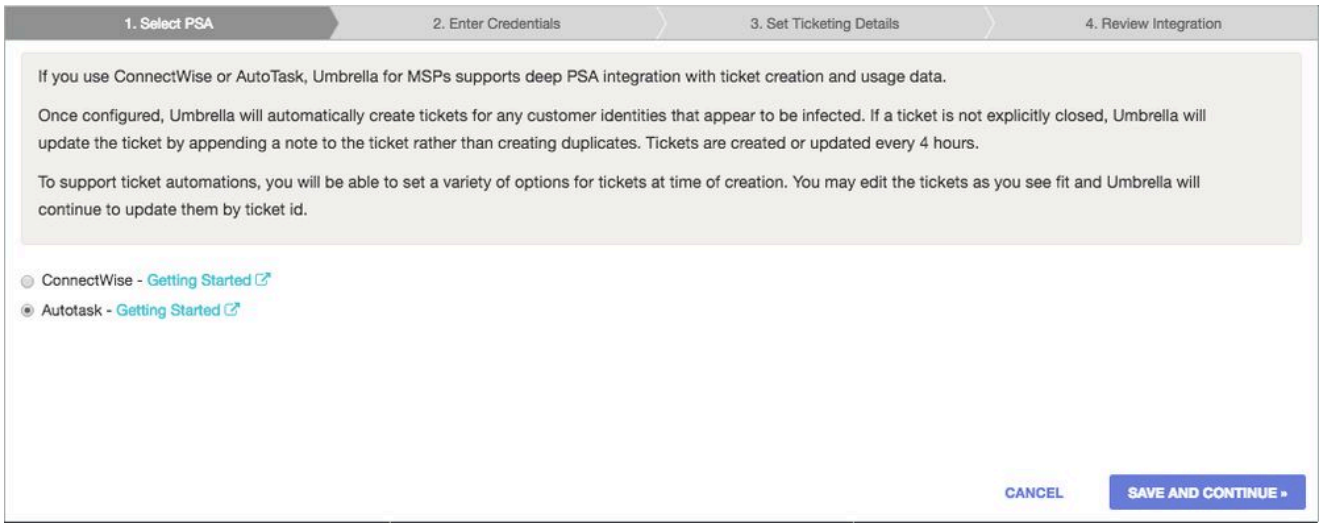
(HR) > Sicurezza > Autorizzazione dati protetti > [l'utente per l'autenticazione].



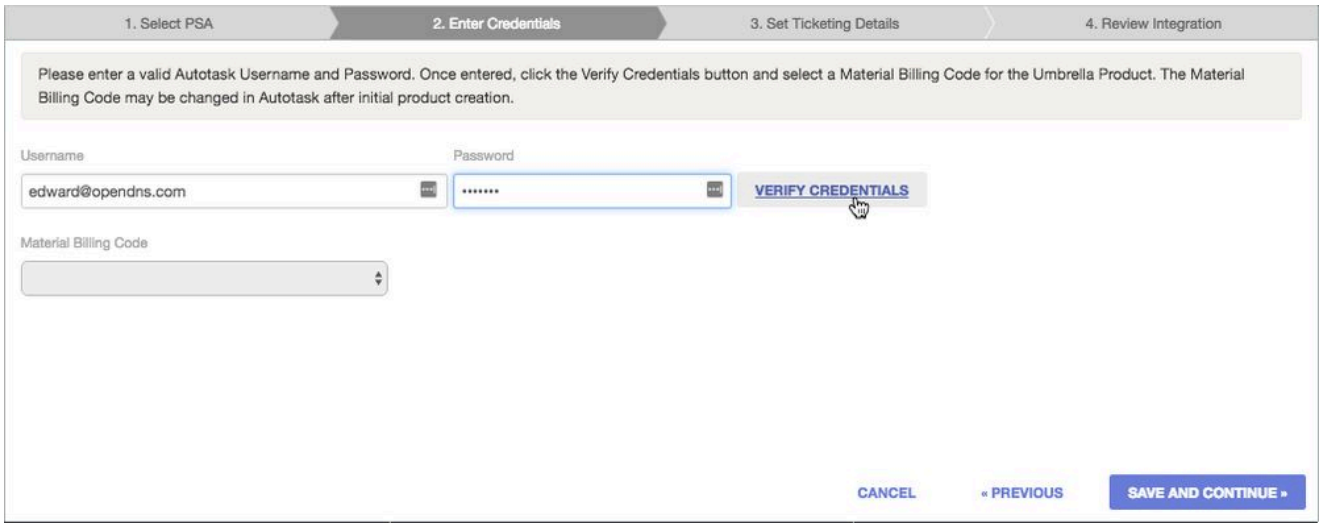
Nota: A partire dal 1° giugno 2021, l'utente per l'autenticazione deve avere un identificatore di rilevamento API impostato. Per ulteriori informazioni, consultare questo articolo della Umbrella Knowledge Base: Modifiche all'integrazione di PSA AutoTask con Umbrella

Dopo aver creato o selezionato un account, passare a Umbrella for MSPs.

1. Passare a Impostazioni MSP > Dettagli integrazione PSA.
2. Selezionare Configura integrazione per aprire la procedura guidata di integrazione.
3. In Seleziona PSA, selezionare Attività automatica come tipo di integrazione, quindi selezionare Salva e continua.



4. Successivamente, viene richiesto di immettere l'account selezionato in precedenza (indirizzo e-mail e password) e verificare le credenziali per selezionare un codice di fatturazione materiale:



Selezionare il codice di fatturazione del materiale appropriato:

Una volta autenticato, il codice di fatturazione del materiale mostra una selezione con il codice di fatturazione del materiale del task automatico esistente. In un secondo momento, è possibile modificare il codice di fatturazione del materiale per il prodotto "OpenDNS_Umbrella" all'interno di Autotask, se lo si desidera.

Selezionare Salva e continua.

Configura ticket attività automatica

Cisco Umbrella per MSP notifica in modo proattivo gli host infetti che richiedono un'azione creando ticket all'interno di una coda del servizio di assistenza per il task automatico. Quando è integrata correttamente, Cisco Umbrella controlla automaticamente se gli host infetti sono contenuti e crea i ticket per l'utente.

Come viene generato un ticket della coda di servizio da Cisco Umbrella:

Al momento, per generare un ticket all'interno di una coda del servizio di assistenza automatico è necessario che siano soddisfatti i seguenti criteri:

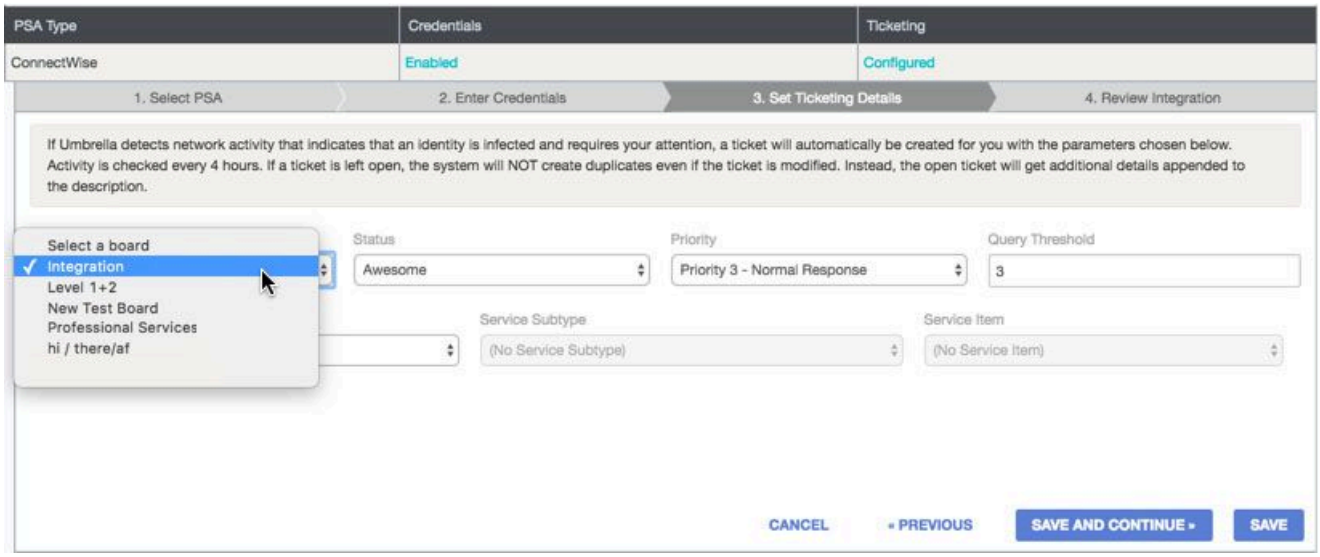
- Cisco Umbrella controlla le tue identità per controllare se le attività botnet sono bloccate. Questa attività indica un endpoint infetto e che Cisco Umbrella sta attivamente bloccando i tentativi di "call home" per gli aggiornamenti, per caricare dati rubati o per far parte di una botnet. Se un'identità dell'organizzazione tenta ripetutamente di raggiungere un sito classificato come "botnet". Ciò significa che mentre Cisco Umbrella contiene il danno, il computer è infettato da malware e richiede un'azione aggiuntiva da parte vostra per il rimedio.
- Cisco Umbrella non crea avvisi quando impedisce infezioni per categorie come malware o download di unità in quanto tali eventi impediscono preventivamente all'utente di visitare siti dannosi. Non sono necessarie ulteriori azioni.
- Ogni quattro ore, Cisco Umbrella controlla tutte le organizzazioni associate a organizzazioni PSA nella Cisco Umbrella per verificare la presenza di una console MSP.
- Se una singola identità, ad esempio un computer con un agente installato o una rete, ha più eventi botnet della "soglia query" (tre per impostazione predefinita) all'interno del blocco di quattro ore, Cisco Umbrella Integration apre automaticamente un ticket all'interno del Service Desk definito da Ticketing Details Integration nell'Integrazione guidata. È possibile modificare la soglia della query in questa posizione.
- Se la stessa identità continua a generare un'attività botnet aggiuntiva nella finestra successiva di quattro ore (o in un'altra finestra successiva) e il ticket è ancora aperto, al ticket vengono aggiunti dati aggiuntivi.
    - Cisco Umbrella fa riferimento al ticket tramite il relativo numero di ticket e non crea duplicati non necessari anche se un ticket viene spostato in un'altra coda del servizio assistenza o se la copia viene modificata.
- Se il ticket è stato contrassegnato come Chiuso, viene creato un nuovo ticket in quanto si presume che si tratti di un nuovo evento di sicurezza relativo alla botnet (ad esempio una nuova infezione) per la stessa identità.

Imposta dettagli ticket:

Se si utilizza l'Integrazione guidata, si sta eseguendo il passaggio 3 dell'Integrazione guidata. Se si sta configurando la creazione di biglietti in un secondo momento, selezionare Integrazione PSA > Dettagli integrazione.Le credenziali verranno visualizzate come abilitate ma l'impostazione del ticketing come disabilitata.

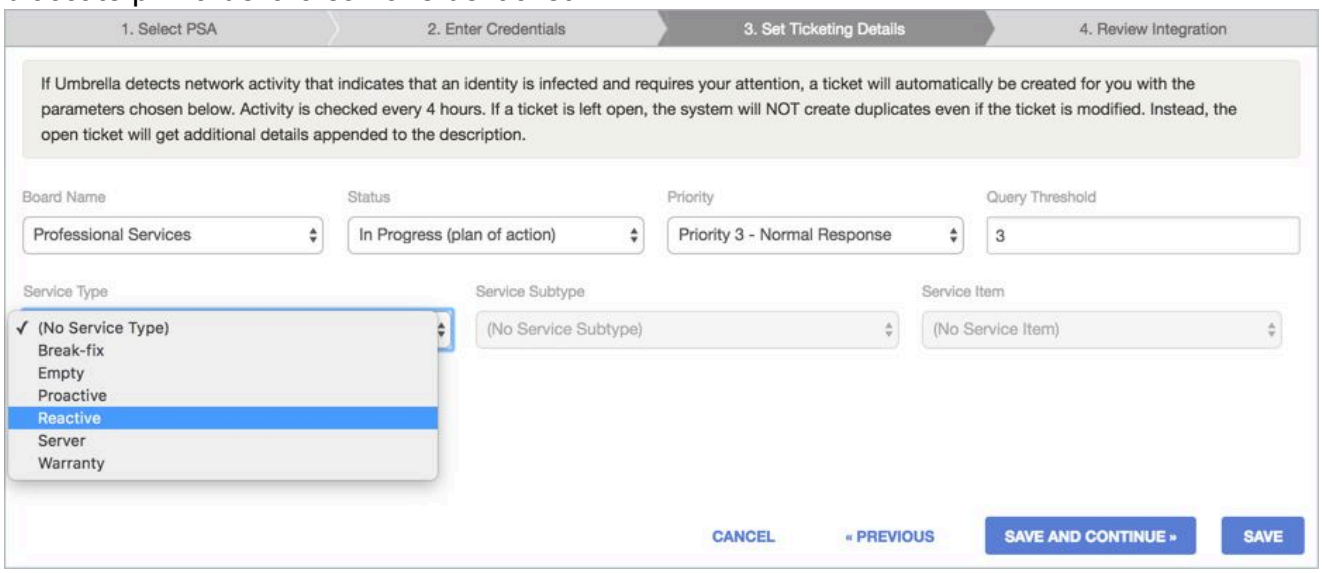
1. Se si seleziona Biglietto > Disabilitato, viene visualizzata la finestra Imposta dettagli ticket.

2. Selezionare innanzitutto una coda. In questo esempio viene utilizzata la coda Triage per lasciare i ticket in. È necessario selezionare prima la coda per popolare i campi aggiuntivi:



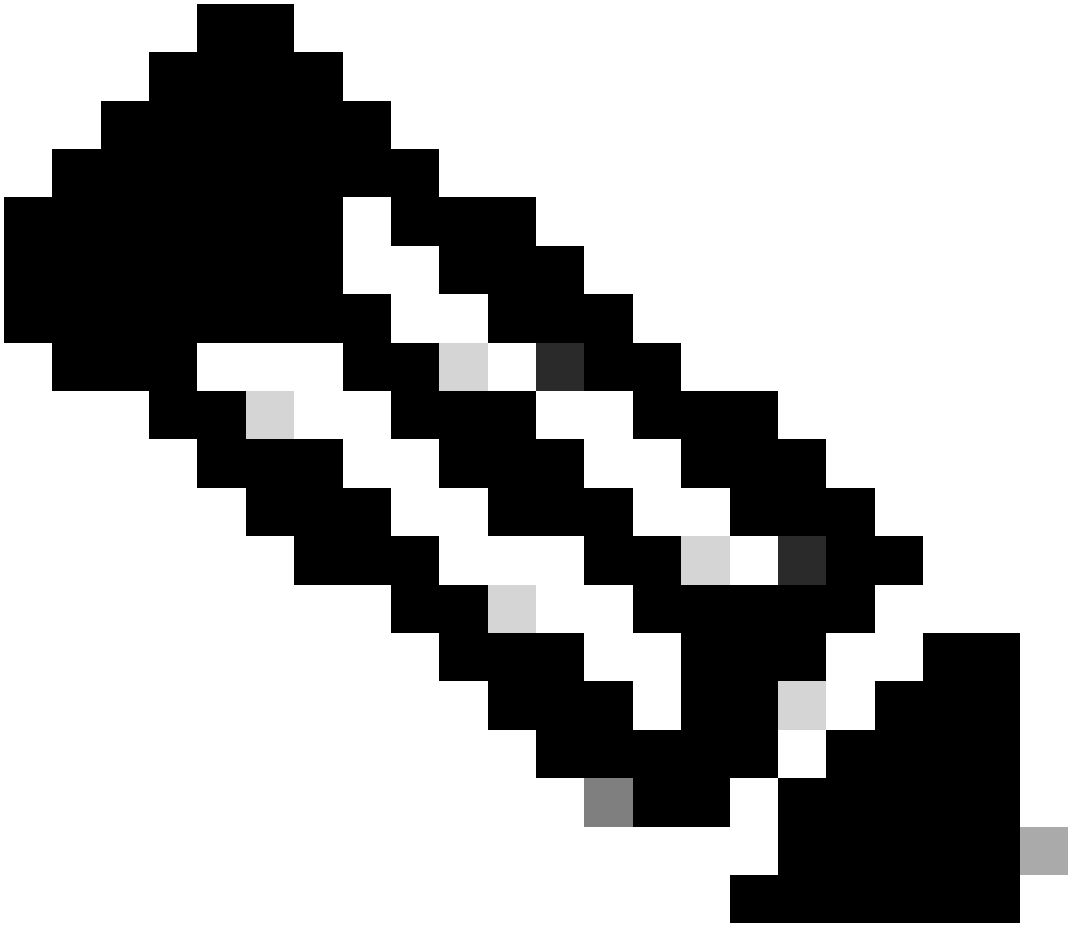
215690567

3. Dopo aver selezionato la coda, attendere alcuni secondi prima di popolare i dettagli dei campi rimanenti, quindi selezionare quello appropriato. Ogni campo di Cisco Umbrella Dashboard corrisponde al campo equivalente all'interno dei ticket per la coda del servizio assistenza selezionata.
   I parametri esatti per ogni campo variano leggermente in base all'implementazione. Un campo di nota è Soglia query, ovvero il numero di attività botnet da una singola identità bloccate prima della creazione del ticket.



4. Compilare tutti i campi, se applicabili, quindi selezionare Salva e continua.

Il quarto e ultimo passaggio dell'integrazione consente di rivedere tutte le impostazioni per verificare che siano quelle desiderate.



Nota: Se desideri generare un ticket di test, contatta il supporto Cisco Umbrella con una richiesta in tal senso. Questo biglietto rispetta le tue regole per la vendita automatica dei biglietti.

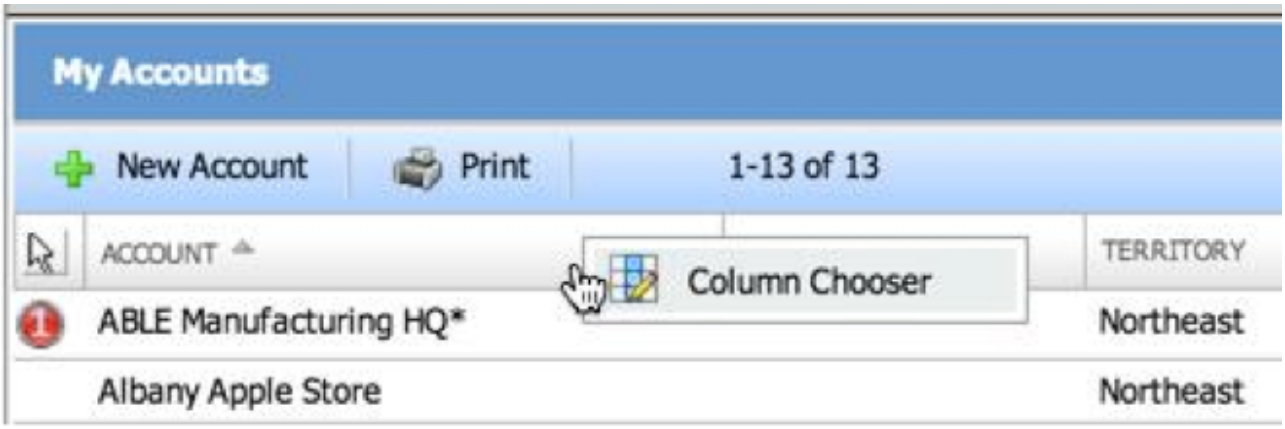
Mappatura delle aziende in Cisco Umbrella

La mappatura delle società del cliente consente l'integrazione e l'associazione dei biglietti e dei prodotti installati al conto del cliente. Il prodotto installato "OpenDNS_Umbrella" contiene statistiche preziose sull'uso e l'efficacia di Cisco Umbrella ed è configurato nel passo 5.

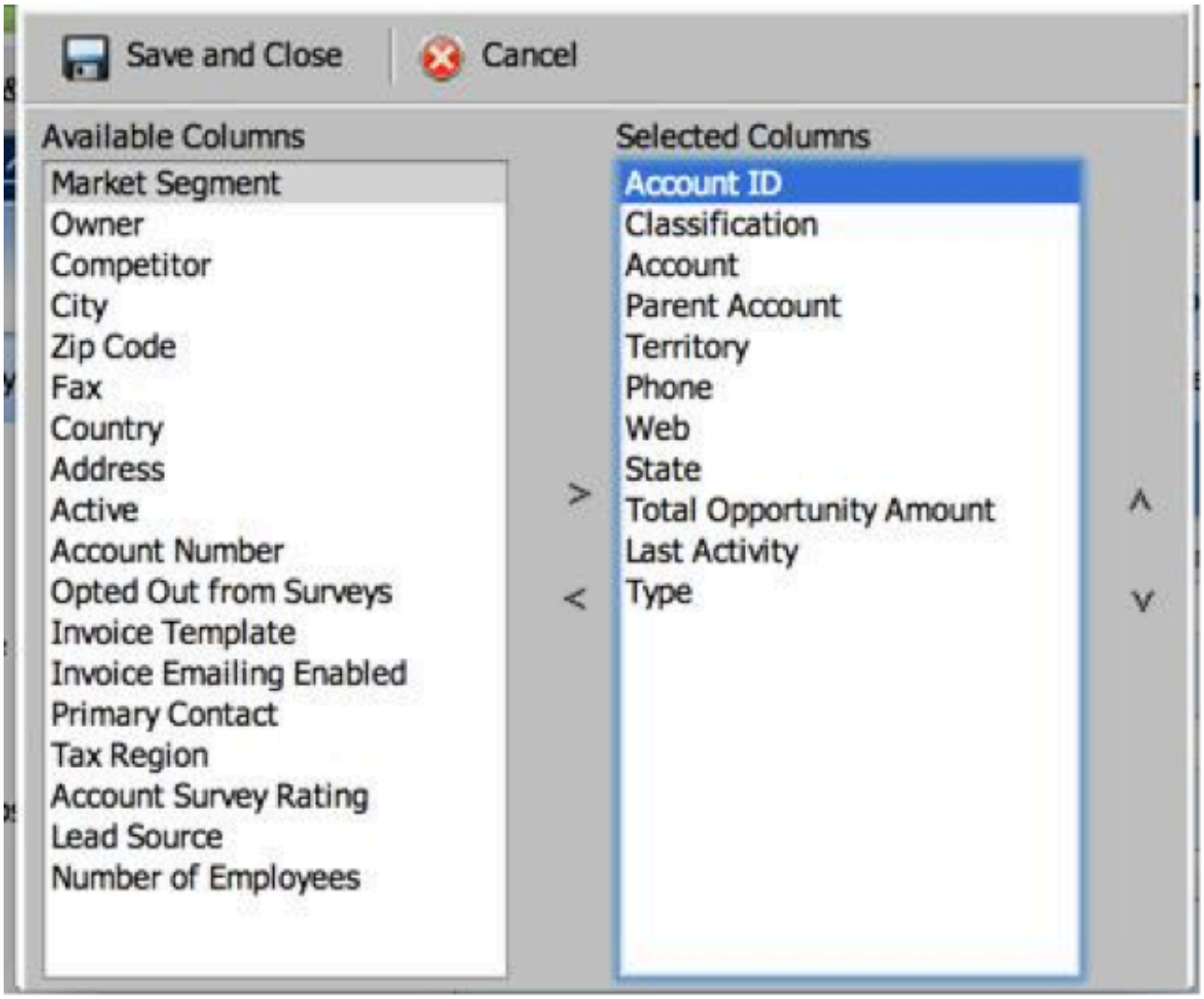
Per sincronizzare i clienti tra Autotask e Cisco Umbrella, è necessario disporre dell'ID account per ciascun cliente. Questa opzione non viene visualizzata in AutoTask per impostazione predefinita.

1. Per visualizzare l'ID cliente nel dashboard del task automatico, selezionare CRM, quindi scegliere Account personali dall'elenco a discesa. Ogni account dispone di un ID account nelle proprietà dell'account, visibile facendo doppio clic sul nome dell'account. Verrà visualizzata una finestra popup in cui è riportato l'ID account.

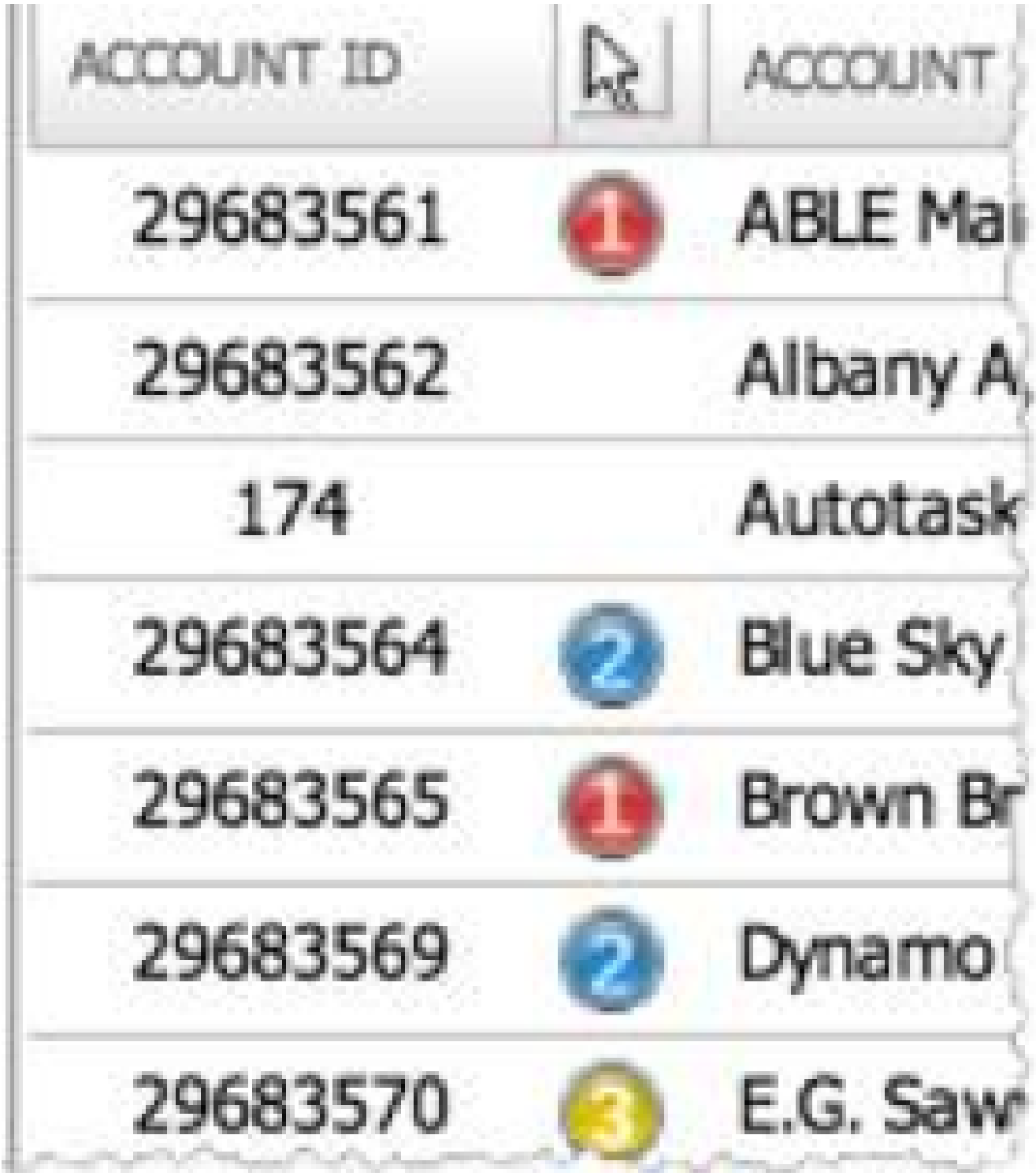
2. Per visualizzare tutti gli ID account dei clienti nella panoramica, è necessario esporre una nuova colonna. Fare clic con il pulsante destro del mouse sulle colonne per visualizzare Selezione colonne.



3. All'interno del selettore di colonna, spostare la colonna ID account in Colonne selezionate.

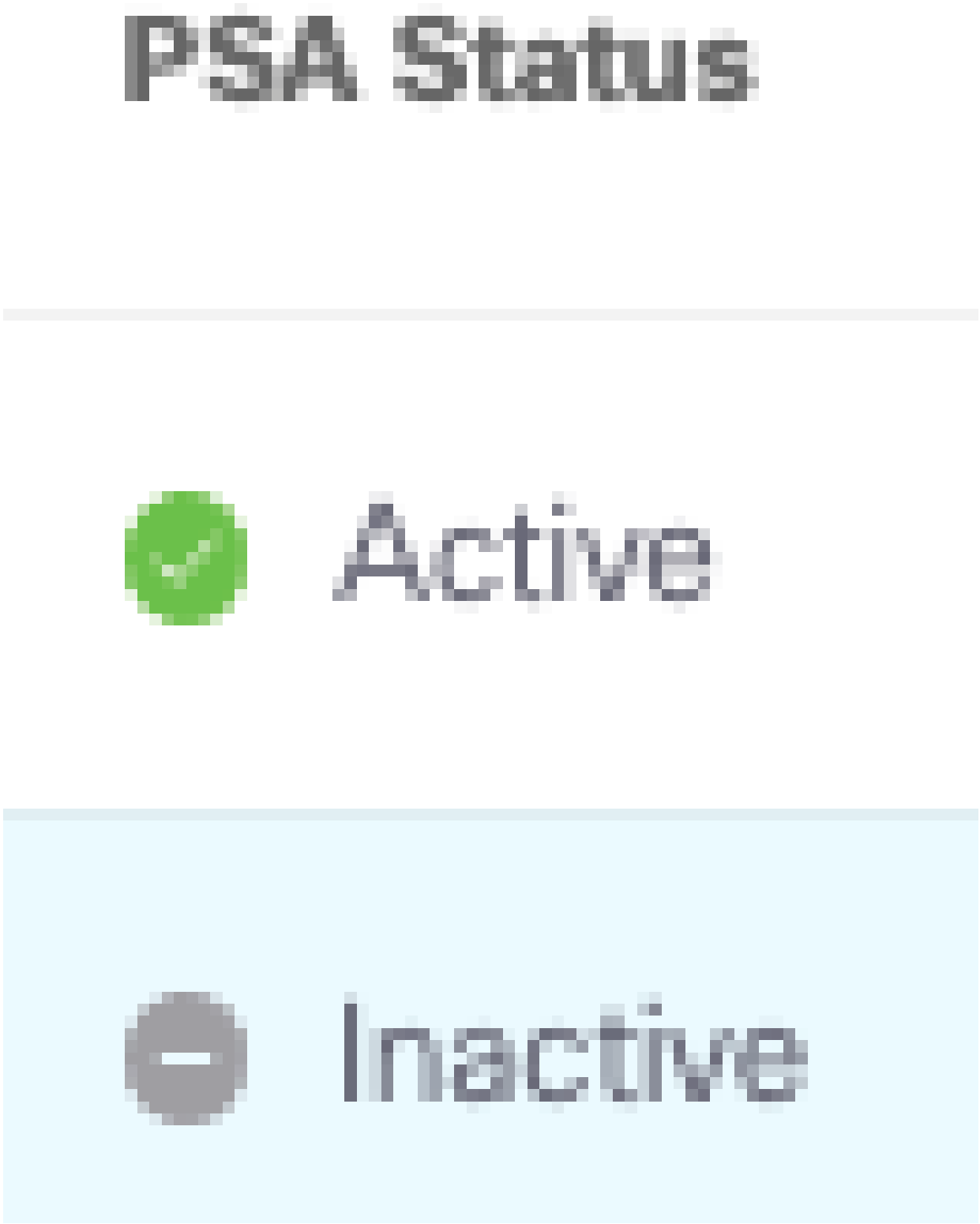


In questo modo viene visualizzato l'ID account del cliente:



4. Dopo aver ottenuto l'ID account per il cliente, tornare a Cisco Umbrella per MSP.
5. Passare a Gestione clienti per visualizzare un elenco dei clienti configurati nella console Nota: Se non sono elencati clienti, è necessario aggiungere clienti a Cisco Umbrella per MSP MSP. Per ulteriori informazioni, consultare la Guida per l'utente di Cisco Umbrella for MSP.
6. Quindi, selezionare il cliente da associare al task automatico. In questo esempio viene utilizzato "Enable Manufacturing Co."
7. In precedenza, è stato rilevato che Able Manufacturing Co. ha un ID account di 29683561. Selezionare il nome del cliente, quindi immettere l'ID account società nel campo relativo all'ID PSA.

8. Selezionare Salva per confermare la modifica. Viene visualizzato un messaggio di conferma dell'abilitazione dell'integrazione. Da quel momento in poi, l'ID PSA viene visualizzato accanto al cliente per il quale è abilitato in Dettagli cliente.
9. Per verificare che l'integrazione sia abilitata, passare a Report centralizzati > Stato distribuzione. Se è operativa, viene compilata una colonna Stato PSA.
    - Le organizzazioni con ID PSA validi vengono visualizzate con stato Attivo verde.
    - Le organizzazioni che non dispongono di un valore ID PSA vengono visualizzate con stato Inattivo grigio.



360053576152

Impostazione dell'elemento di configurazione "OpenDNS_Umbrella" (facoltativo)

Una volta che l'ID società PSA è stato integrato correttamente, viene creato automaticamente un elemento di configurazione/prodotto installato denominato OpenDNS_Umbrella.

È possibile visualizzare l'elemento di configurazione in Directory > Account, quindi selezionare uno degli account integrati nel passo 4. All'interno di questo account, è ora disponibile un elemento di configurazione per OpenDNS_Umbrella.

Per impostazione predefinita, l'elemento di configurazione include tutti i campi possibili e i campi Cisco Umbrella aggiunti nell'integrazione. Alcuni campi non sono compilati in quanto non applicabili a Cisco Umbrella, ad esempio Marca o Marca e modello.

Per modificare il prodotto in modo da non includere questi campi, impostare un tipo di configurazione univoco per Cisco Umbrella.

Installazione del tipo di configurazione

Gli elementi di configurazione creati in AutoTask tramite l'integrazione Cisco Umbrella creano campi definiti dall'utente (UDF, User-Defined Fields) per le informazioni aggiornate automaticamente di Cisco Umbrella. Per default, un nuovo prodotto visualizza tutte le FDU ed è consigliabile specificare un tipo di elemento di configurazione. A causa dei limiti dell'API di task automatico corrente, la creazione di un tipo di elemento di configurazione all'interno del task automatico è limitata all'intervento manuale dell'utente o dell'amministratore del task automatico. Questa tabella fornisce un elenco di tutti i campi che devono essere aggiunti al tipo di elemento di configurazione.

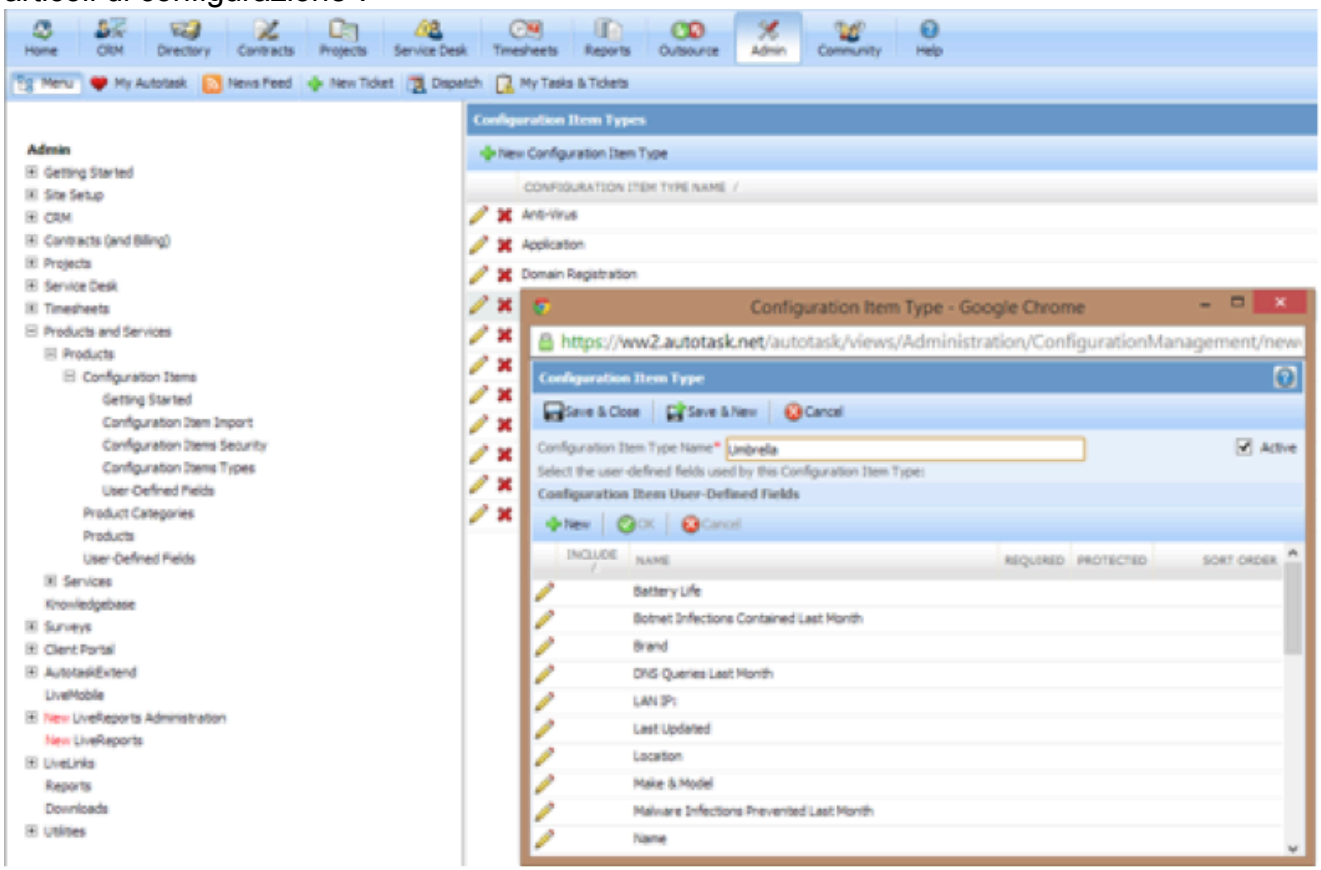
N.	Nome campo	Tipo
1	ID organizzazione	Testo (riga singola)
2	Ultimo aggiornamento	Testo (riga singola)
3	Pacchetto	Testo (riga singola)

4	Sedili	Testo (riga singola)
5	Totale reti	Testo (riga singola)
6	Reti attive negli ultimi 7 giorni	Testo (riga singola)
7	Reti inattive negli ultimi 7 giorni	Testo (multiriga)
8	Agenti Umbrella distribuiti	Testo (riga singola)
9	Agenti Umbrella attivi negli ultimi 7 giorni	Testo (riga singola)
10	Agenti Umbrella inattivi negli ultimi 7 giorni	Testo (multiriga)
11	Query DNS del mese scorso	Testo (riga singola)
12	Infezioni Malware Prevenute Il Mese Scorso	Testo (riga singola)
13	Infezioni Botnet Contenute Il Mese Scorso	Testo (riga singola)
14	Domini principali ultimo mese	Testo (multiriga)

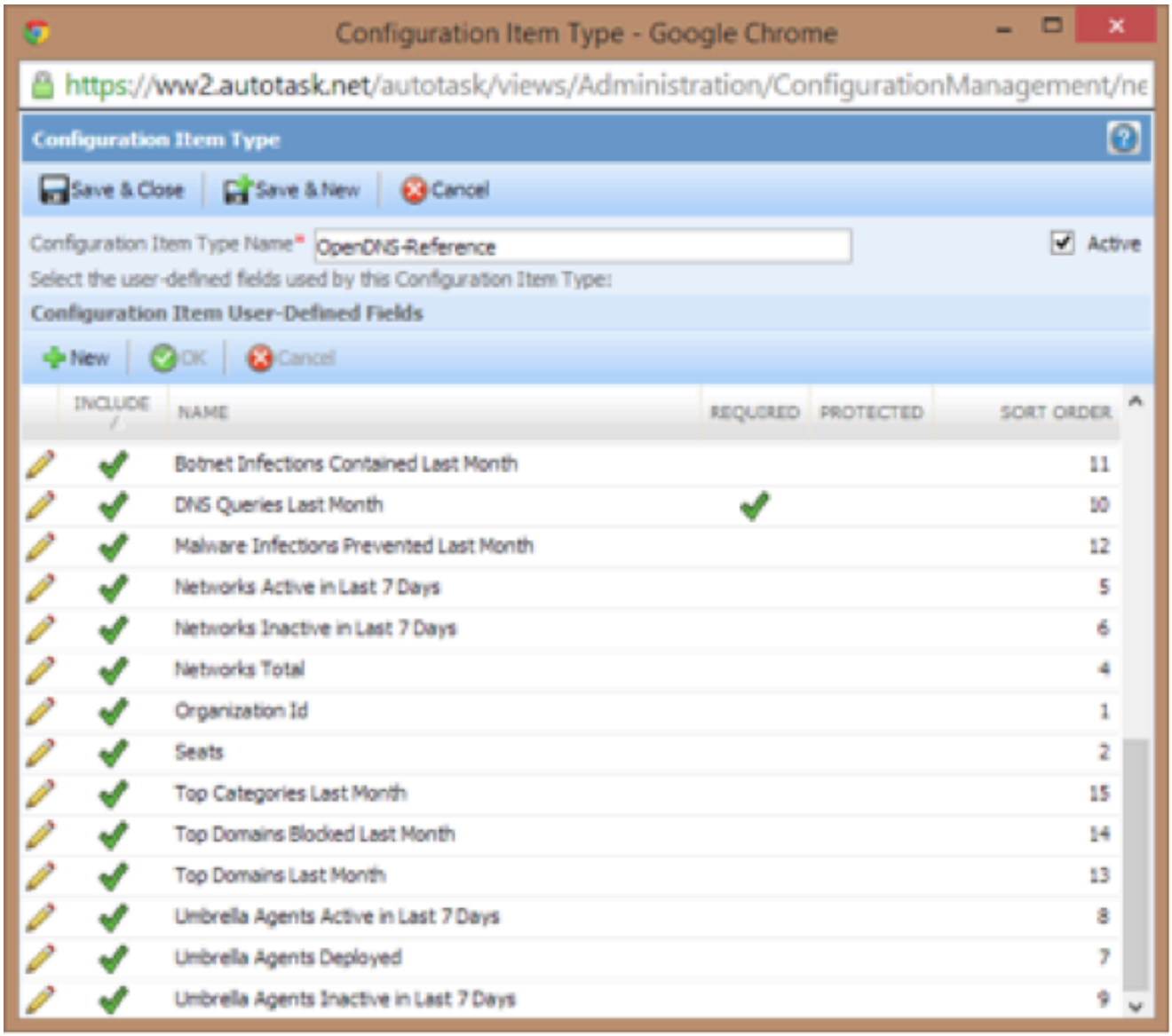
15	Primi domini bloccati il mese scorso	Testo (multiriga)
16	Categorie principali ultimo mese	Testo (multiriga)

Per gli utenti che non hanno familiarità con l'impostazione di nuovi tipi di elementi di configurazione in Task automatico, utilizzare queste istruzioni per creare il nuovo record nel sistema:

1. Accedere a Task automatico come amministratore.
2. Passare alla sezione Admin utilizzando il menu in alto.
3. Passare a Prodotti e servizi > Prodotti > Articoli di configurazione e selezionare "Tipi di articoli di configurazione".

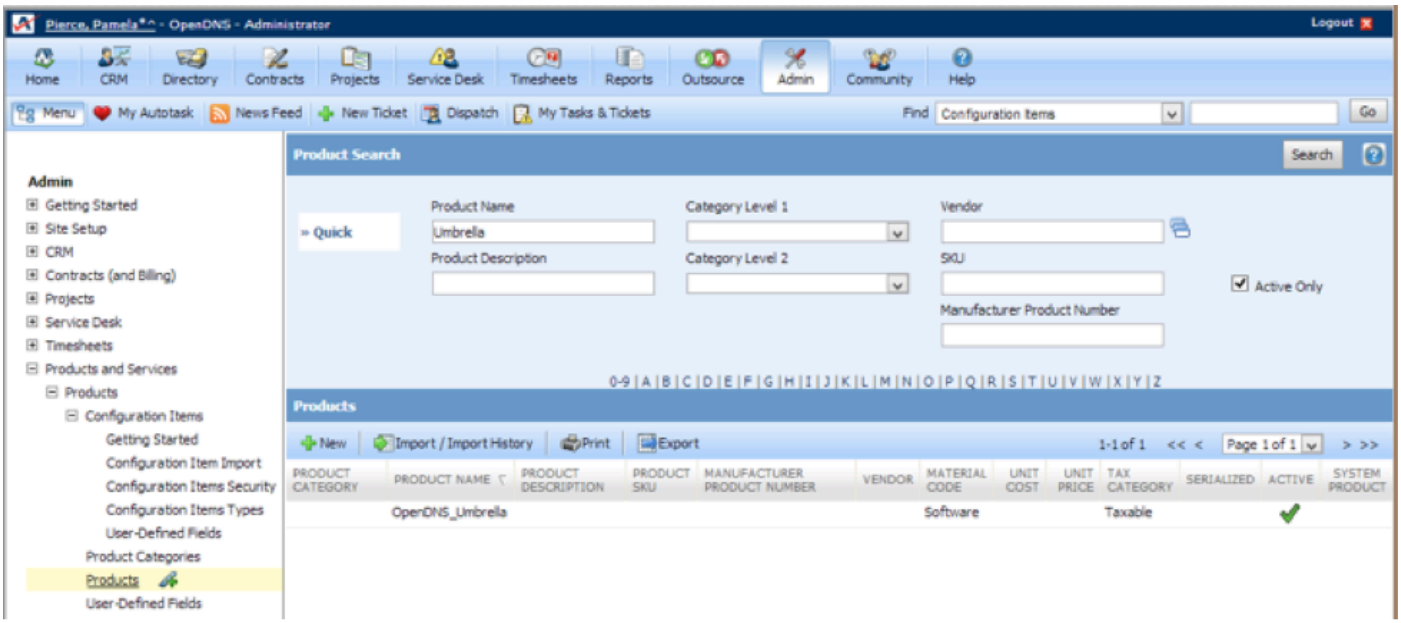


4. Selezionare l'opzione di menu Nuovo tipo di elemento di configurazione.
5. Immettere un nome per il nuovo tipo di elemento di configurazione.
6. Selezionare Nuovo e immettere le informazioni relative al primo campo nella parte superiore.
7. Ripetere il passaggio 6 fino ad aggiungere tutti i campi della tabella al nuovo tipo di elemento.



8. Salvare e chiudere il nuovo tipo di elemento di configurazione.

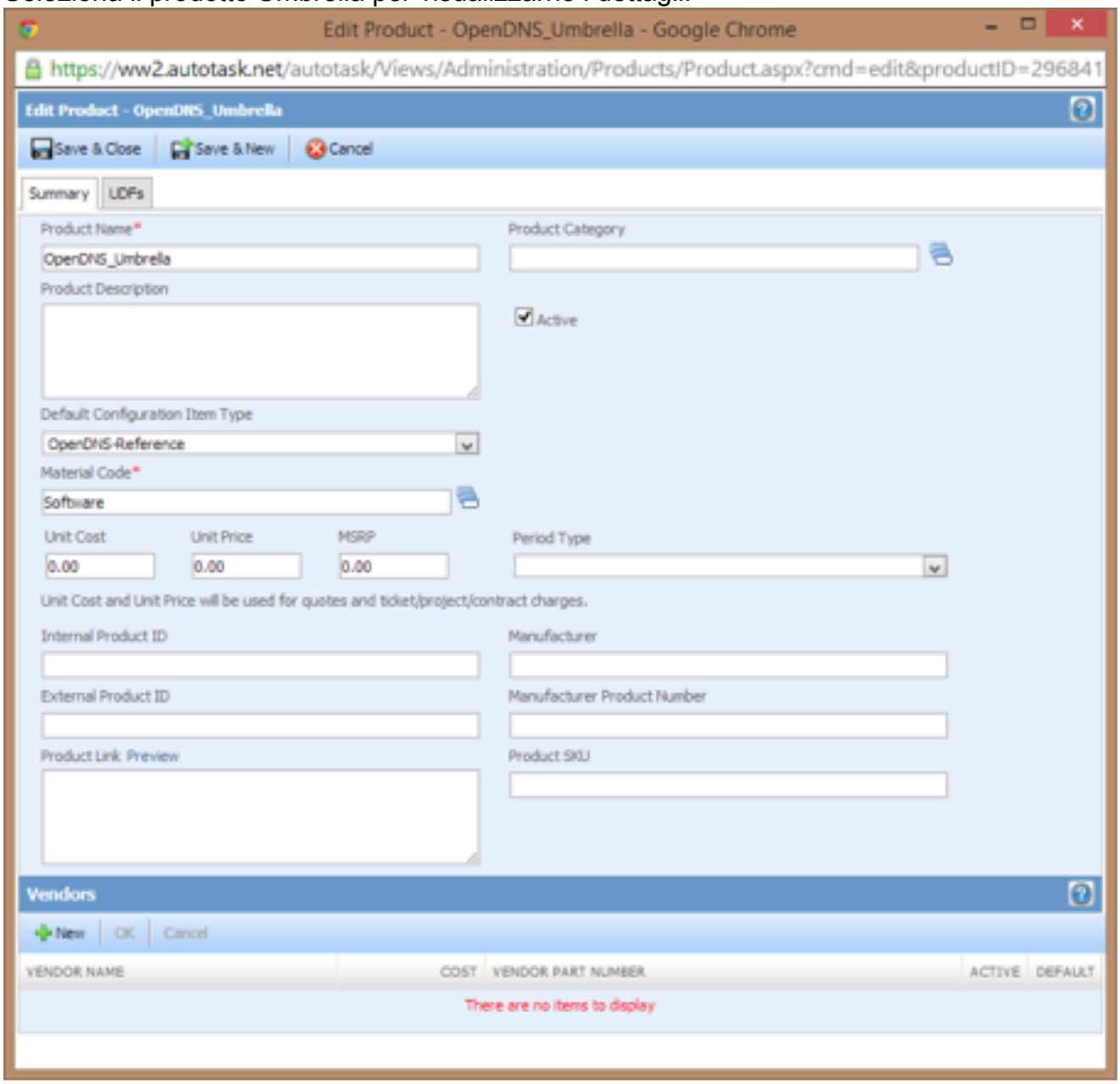
Impostazione prodotto



L'integrazione Cisco Umbrella crea automaticamente un prodotto all'interno dell'implementazione di attività automatica per collegare gli elementi di configurazione al momento della creazione. Dopo aver creato il prodotto nel sistema, Cisco Umbrella consiglia di aggiornare la definizione del prodotto con impostazioni che riflettano al meglio gli standard e le esigenze aziendali.

Per identificare la definizione del prodotto e aggiornarne le impostazioni, eseguire la procedura seguente:

1. Accedere a Task automatico come amministratore.
2. Passare alla sezione Admin utilizzando il menu in alto.
3. Passare a Prodotti e servizi > Prodotti e selezionare Prodotti.
4. Digitare "Umbrella" nel campo di ricerca Nome prodotto e selezionare Cerca.
5. Seleziona il prodotto Umbrella per visualizzarne i dettagli.



6. Aggiornare la definizione del prodotto in base alle impostazioni desiderate.
7. Selezionare Salva e chiudi.

Note:

- Non modificare la stringa Nome prodotto da "OpenDNS_Umbrella" ad altro. In questo modo si interrompe l'integrazione, ma se è stato rinominato, rinominarlo di nuovo per risolvere il problema.
- Assicurarsi che "Attivo: viene selezionato come mostrato nello screenshot.

Nella tabella seguente vengono elencate le definizioni di tutti i campi delle attività automatiche Cisco Umbrella aggiornati e inclusi nell'elemento di configurazione:

Campo	Descrizione
ID organizzazione	ID organizzazione interna ombrello
Ultimo aggiornamento	Data in cui è stata eseguita l'ultima sincronizzazione con Umbrella
Sedili	Numero totale di posti assegnati alla società.
Totale reti	Numero totale di reti applicate alla società
Reti attive (7 giorni)	Numero totale di reti attive negli ultimi sette giorni
Reti inattive (7 giorni)	Elenco di nomi di rete inattivi negli ultimi sette giorni
Agenti Umbrella distribuiti	Numero di agenti di roaming Umbrella distribuiti
Agenti Umbrella attivi 7 giorni	Numero di agenti di roaming Umbrella attivi negli ultimi sette giorni
Agenti Umbrella	Nomi delle identità degli agenti di roaming

inattivi per 7 giorni	Umbrella inattivi negli ultimi sette giorni
Query DNS del mese scorso	Numero totale di richieste DNS per la società nel mese di calendario precedente
Infezioni Malware Prevenute Il Mese Scorso	Numero di siti che ospitano malware a cui è stato impedito l'accesso nel mese di calendario precedente
Infezioni Botnet Contenute Il Mese Scorso	Numero di siti che ospitano il comando e il controllo botnet a cui è stato impedito l'accesso nel mese di calendario precedente
Domini principali ultimo mese	Elenco dei nomi dei domini con il maggior numero di accessi nel mese di calendario precedente
Primi domini bloccati il mese scorso	Elenco dei nomi dei domini bloccati più di frequente nel mese di calendario precedente
Categorie principali ultimo mese	Elenco delle categorie di contenuti più richieste nel mese di calendario precedente, incluso il numero di richieste per categoria

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).