# Configure Autotask and Umbrella Integration

## Contents

## Introduction

This document describes how to configure the integration of Autotask with Umbrella.

## Overview

The Cisco Umbrella Autotask integration allows MSPs to be notified of potentially infected end-points requiring attention by automatically creating tickets in Autotask. The integration also pushes service deployment status and value data between the Cisco Umbrella Dashboard and an Autotask Autotask-installed product (automatically created) called "OpenDNS_Umbrella."

Steps to Integration:

1. Prerequisites
2. Initial Autotask Authentication and Cisco Umbrella Setup
3. Configure Autotask Ticketing
4. Company Mapping in Cisco Umbrella
5. Setting up the "OpenDNS_Umbrella" Configuration Item

## Prerequisites

This table contains the base software requirements for installation:

| **Software** | **Version** | **Hosted Model** |
|---|---|---|
| **Cisco Umbrella** | Not applicable | Hosted |

| | | |
|---|---|---|
| **Autotask** | 6.0 or higher | Hosted |

**Note**: Only **one (1)** PSA integration can be added at a time. If you already have a Connectwise integration configured, you must delete it from the dashboard before the Autotask setup can proceed.

## Initial Autotask Authentication and Cisco Umbrella Setup

### Establish a user for authentication:

To connect to the AutoTask API, Cisco Umbrella needs a login for Autotask. This can be a new user resource account or an existing shared login.

- **Existing user:** If you already have an Autotask login that you use for integrations, please check that the account is set as an API User. The account must not be using two-step authentication.
- **New user:** To create a new user resource:
  - Log in to your Autotask dashboard.
  - Select **Admin > CiscoResources (Users) > New**.

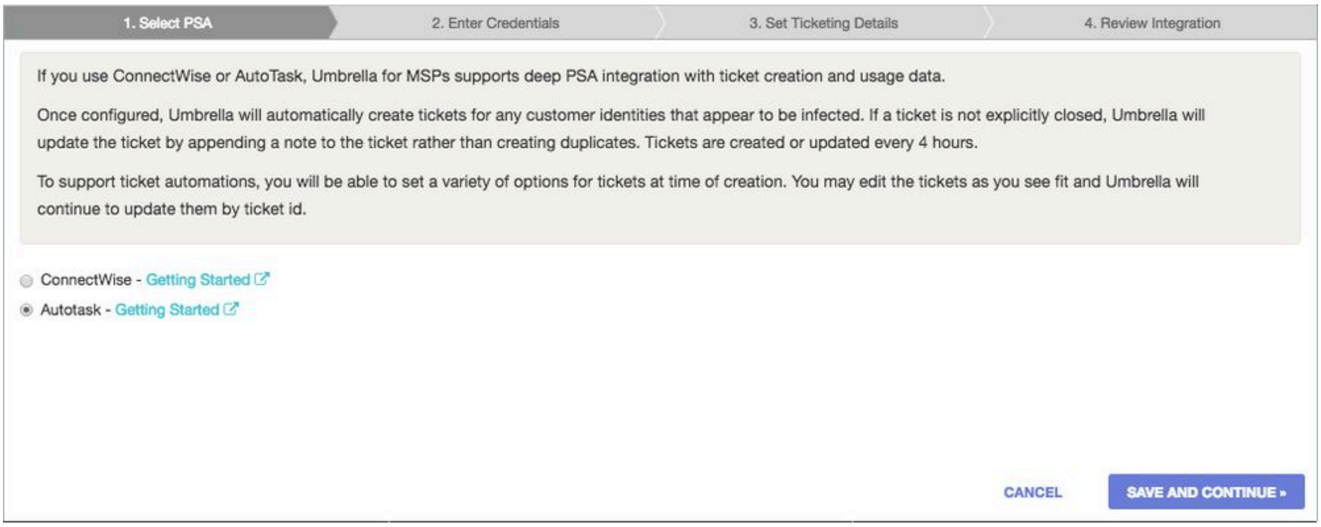
  - Fill in the personal information requirements for the user under the HR tabs.
  - Under the **Security** tab, ensure the Security Level for this user is set to "API User (system)".

**Note**: The user for authentication must have the “View Unprotected Data” checkbox selected in **Admin > Features & Settings > Resources/Users (HR) > Security > Protected Data Permission > [the user for authentication]**.

**Note**: Effective June 1, 2021, the user for authentication must have an API Tracking Identifier set. For more information, please see this Umbrella Knowledge Base article: Changes to Autotask PSA integration with Umbrella

Once an account has been created or selected, navigate to Umbrella for MSPs.

1. Navigate to **MSP Settings > PSA Integration Details**.
2. Select **Set-Up Integration** to open the Integration wizard.
3. Under **Select PSA,** select **Autotask** as the Integration type, then select **Save and Continue**.



If you use ConnectWise or AutoTask, Umbrella for MSPs supports deep PSA integration with ticket creation and usage data.

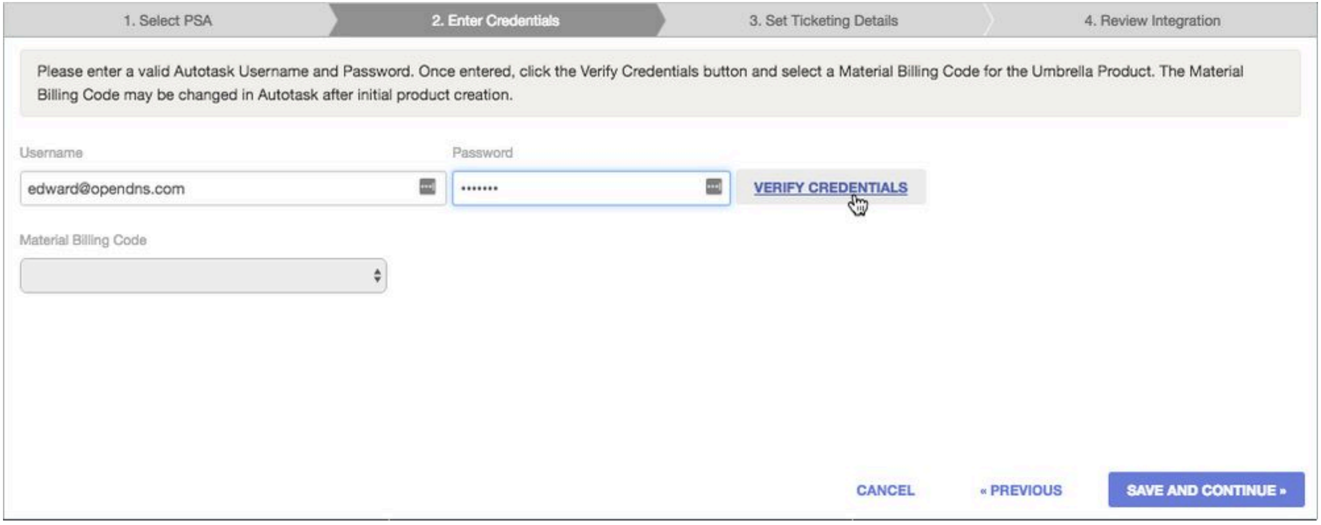
Once configured, Umbrella will automatically create tickets for any customer identities that appear to be infected. If a ticket is not explicitly closed, Umbrella will update the ticket by appending a note to the ticket rather than creating duplicates. Tickets are created or updated every 4 hours.

To support ticket automations, you will be able to set a variety of options for tickets at time of creation. You may edit the tickets as you see fit and Umbrella will continue to update them by ticket id.

○ ConnectWise - Getting Started

● Autotask - Getting Started

4. Next, you are asked to enter the account selected earlier (e-mail address and password) and verify your credentials to select a Material Billing Code:



Please enter a valid Autotask Username and Password. Once entered, click the Verify Credentials button and select a Material Billing Code for the Umbrella Product. The Material Billing Code may be changed in Autotask after initial product creation.

Username: edward@opendns.com

Password: •••••••

Material Billing Code:

### Select the appropriate Material Billing Code:

Once you have authenticated, the Material Billing Code shows a selection with your existing Autotask material billing code. At a later time, you can change the material billing code for the "OpenDNS_Umbrella" product within Autotask if you wish.

Select **Save & Continue**.

## Configure Autotask Ticketing

Cisco Umbrella for MSPs proactively notifies you of infected hosts that require action by creating tickets within an Autotask Service Desk queue. When correctly integrated, Cisco Umbrella automatically checks for infected hosts being contained and create tickets for you.

### How a Service Queue Ticket is generated by Cisco Umbrella:

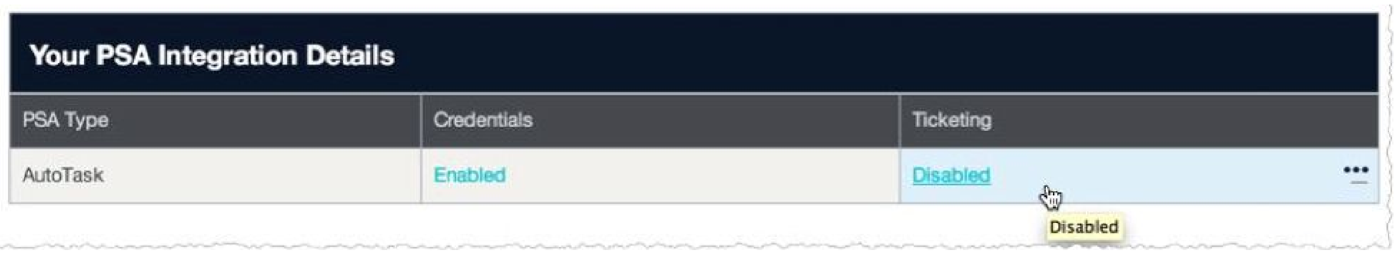
Currently, this criteria must be met to generate a ticket within an Autotask Service Desk queue:

- Cisco Umbrella monitors your identities for "botnet activity" being blocked. This activity indicates an endpoint that is infected and that Cisco Umbrella is actively blocking attempts to "call home" for updates, to upload stolen data, or to be a part of a botnet. If an identity in your organization is repeatedly trying to reach a site categorized as "botnet. This means that while Cisco Umbrella is containing the damage, the machine is infected with malware and needs additional action on your part for remediation.

- Cisco Umbrella does not create alerts when it prevents infections for categories such as malware or drive-by downloads since those events are preventively blocking the user from visiting malicious sites. No additional action is required.
- Every four hours, Cisco Umbrella checks all of the organizations that are mapped to PSA organizations in your Cisco Umbrella for MSP console.
- If a single identity, such as a computer with an agent installed or a network, has more botnet events than the "query threshold" (three by default) within the four-hour block, the Cisco Umbrella Integration automatically opens a ticket within the Service Desk defined by the Ticketing Details Integration in the Integration wizard. You can change the query threshold there.
- If the same identity continues to generate additional botnet activity in the next four-hour window (or another time window after that) and the ticket is still open, additional data is appended to the ticket.
    - Cisco Umbrella references the ticket by its ticket number and does not create unnecessary duplicates even if a ticket is moved to another service desk queue or the copy is changed.
- If the ticket has been marked Closed, then a new ticket is created as it is assumed that this is a new botnet-related security event (such as re-infection) for the same identity.

## Set Ticketing Details:

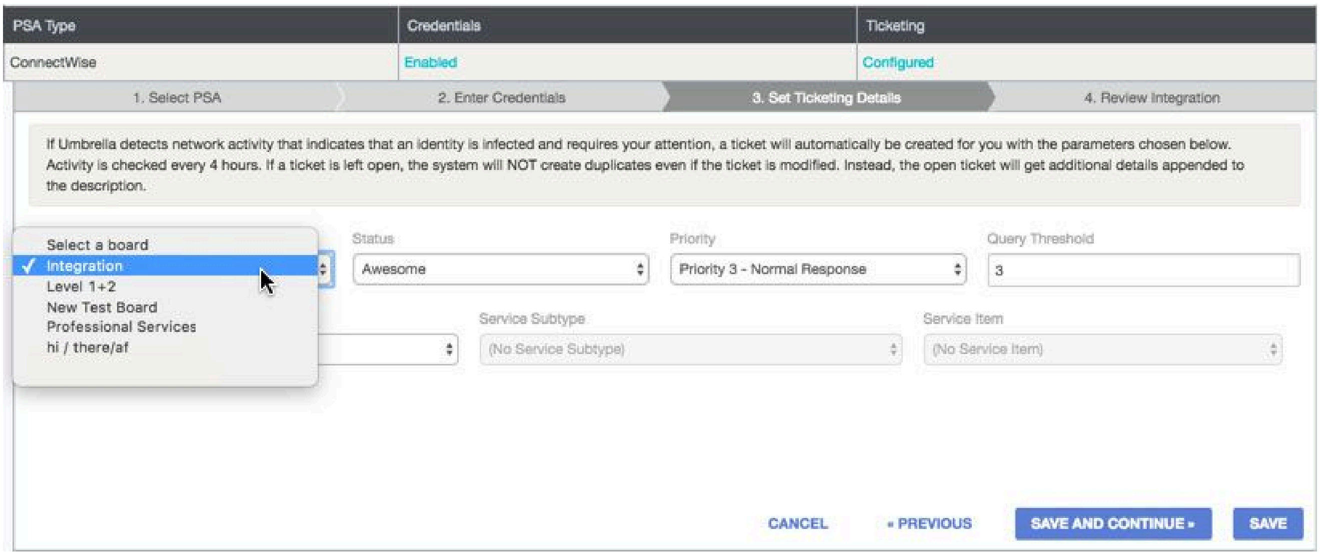
If you are using the Integration wizard, you are on step 3 of the Integration wizard. If you are configuring ticketing later, select **PSA Integration > Integration Details**.Your credentials now show as enabled but ticketing as disabled.



Your PSA Integration Details

| PSA Type | Credentials | Ticketing |
|---|---|---|
| AutoTask | Enabled | Disabled |

1. Selecting **Ticketing > Disabled** brings you to Set Ticketing Details.
2. First, select a queue. This example uses the Triage queue to leave tickets in. You must select the queue first to populate the additional fields:



| PSA Type | Credentials | Ticketing |
|---|---|---|
| ConnectWise | Enabled | Configured |

If Umbrella detects network activity that indicates that an identity is infected and requires your attention, a ticket will automatically be created for you with the parameters chosen below. Activity is checked every 4 hours. If a ticket is left open, the system will NOT create duplicates even if the ticket is modified. Instead, the open ticket will get additional details appended to the description.

Status: Awesome

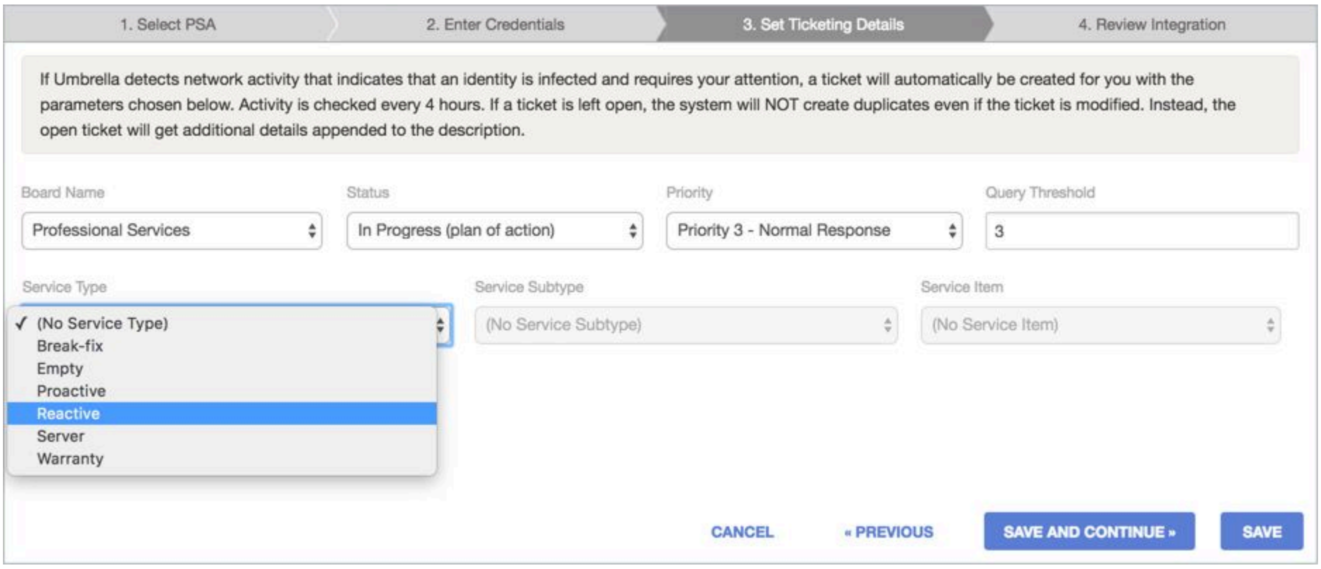
Priority: Priority 3 - Normal Response

Query Threshold: 3

Service Subtype: (No Service Subtype)

Service Item: (No Service Item)

3. After selecting your queue, wait a few seconds for the detail to be populated for the remaining fields, then select the appropriate one. Each field in the Cisco Umbrella Dashboard maps to the equivalent field within the tickets for the Service Desk queue selected.
   The exact parameters for each field varies slightly based on your implementation. One field of note is the Query Threshold, which is the number of botnet activities from a single identity that are blocked before the ticket is created.



If Umbrella detects network activity that indicates that an identity is infected and requires your attention, a ticket will automatically be created for you with the parameters chosen below. Activity is checked every 4 hours. If a ticket is left open, the system will NOT create duplicates even if the ticket is modified. Instead, the open ticket will get additional details appended to the description.

Board Name: Professional Services

Status: In Progress (plan of action)

Priority: Priority 3 - Normal Response

Query Threshold: 3

Service Type: (No Service Type)

Service Subtype: (No Service Subtype)

Service Item: (No Service Item)

4. Complete all fields as applicable, then select **Save and Continue**.

The fourth and final step of the integration allows you to review all of your settings to ensure they are what you expect.

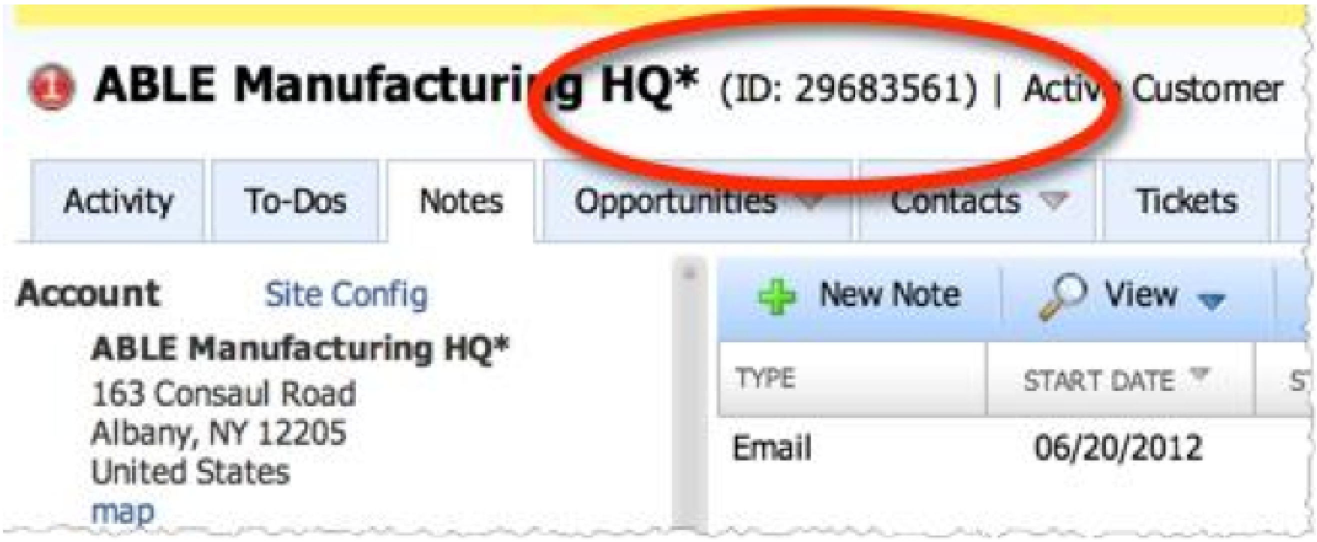
**Note**: If you would like to generate a test ticket, please contact Cisco Umbrella Support with a request to do so. This ticket obeys your Autotask ticketing rules.

## Company Mapping in Cisco Umbrella

Mapping customer companies enables the integration and allows tickets and installed products to be associated with the customer account. The Installed Product "OpenDNS_Umbrella" contains valuable statistics about the customer usage and efficacy of Cisco Umbrella and is configured in Step 5.

To synchronize customers between Autotask and Cisco Umbrella, you must have the Account ID for each customer. This is not shown in Autotask by default.

1. To see the customer ID in the Autotask dashboard, select **CRM**, then choose **My Accounts** from the drop-down list. Each account has an account ID in the properties for that account visible by double-clicking on the account name which opens a pop-up window showing the Account ID.

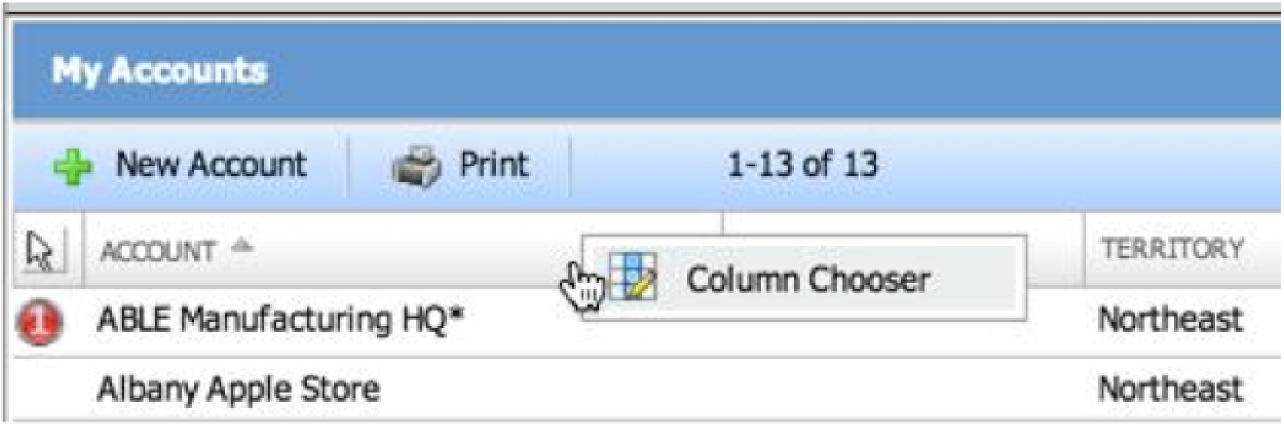


ABLE Manufacturing HQ* (ID: 29683561) | Active Customer

ABLE Manufacturing HQ*
163 Consaul Road
Albany, NY 12205
United States
map

| TYPE | START DATE |
|---|---|
| Email | 06/20/2012 |

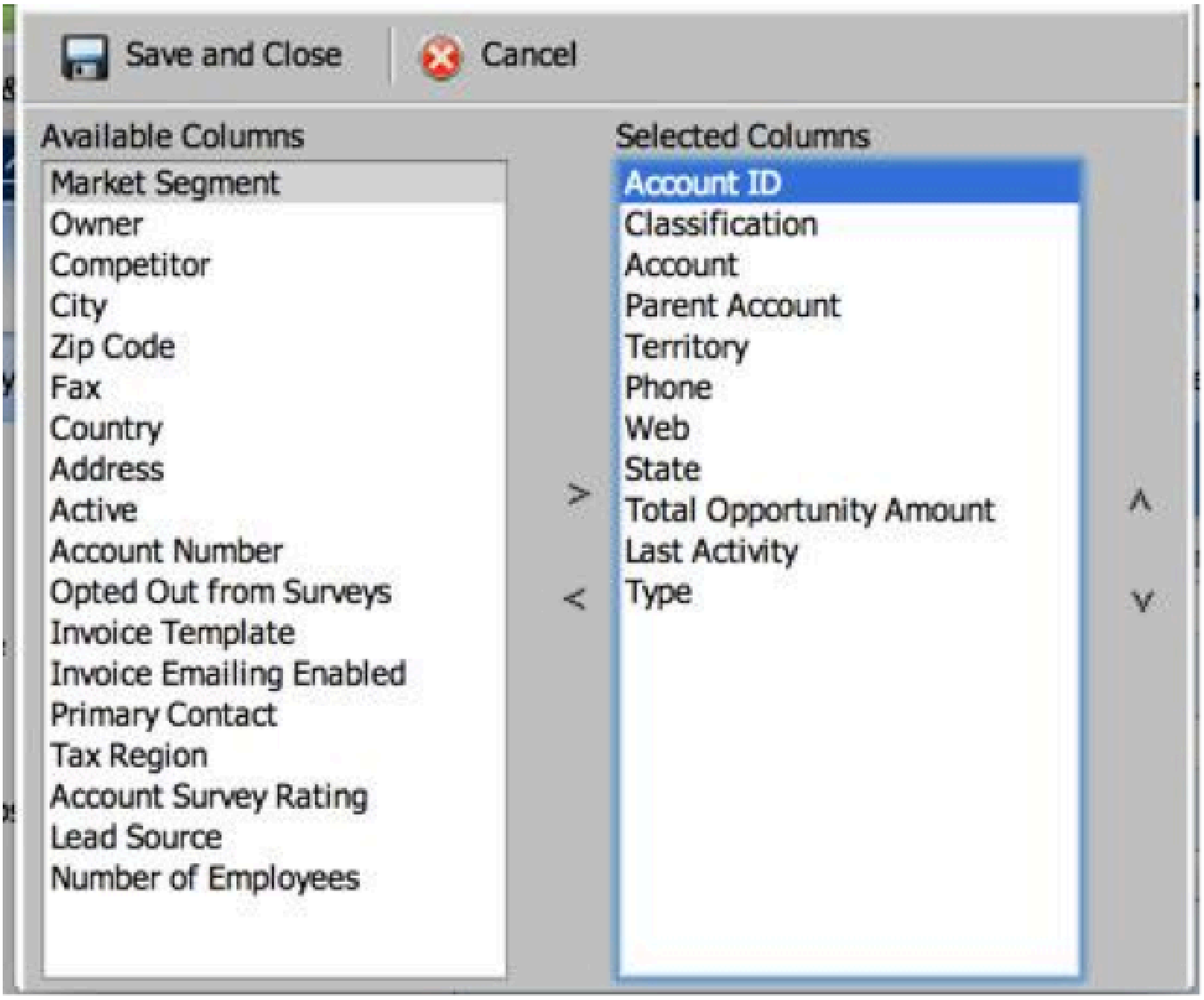
2. To see all of the Account IDs for your customers in the overview, you must expose a new column. Right-click the columns to show the **Column Chooser**.



My Accounts

| ACCOUNT | TERRITORY |
|---|---|
| ABLE Manufacturing HQ* | Northeast |
| Albany Apple Store | Northeast |

3. Within the column chooser, move the **Account ID** column to the **Selected Columns**.



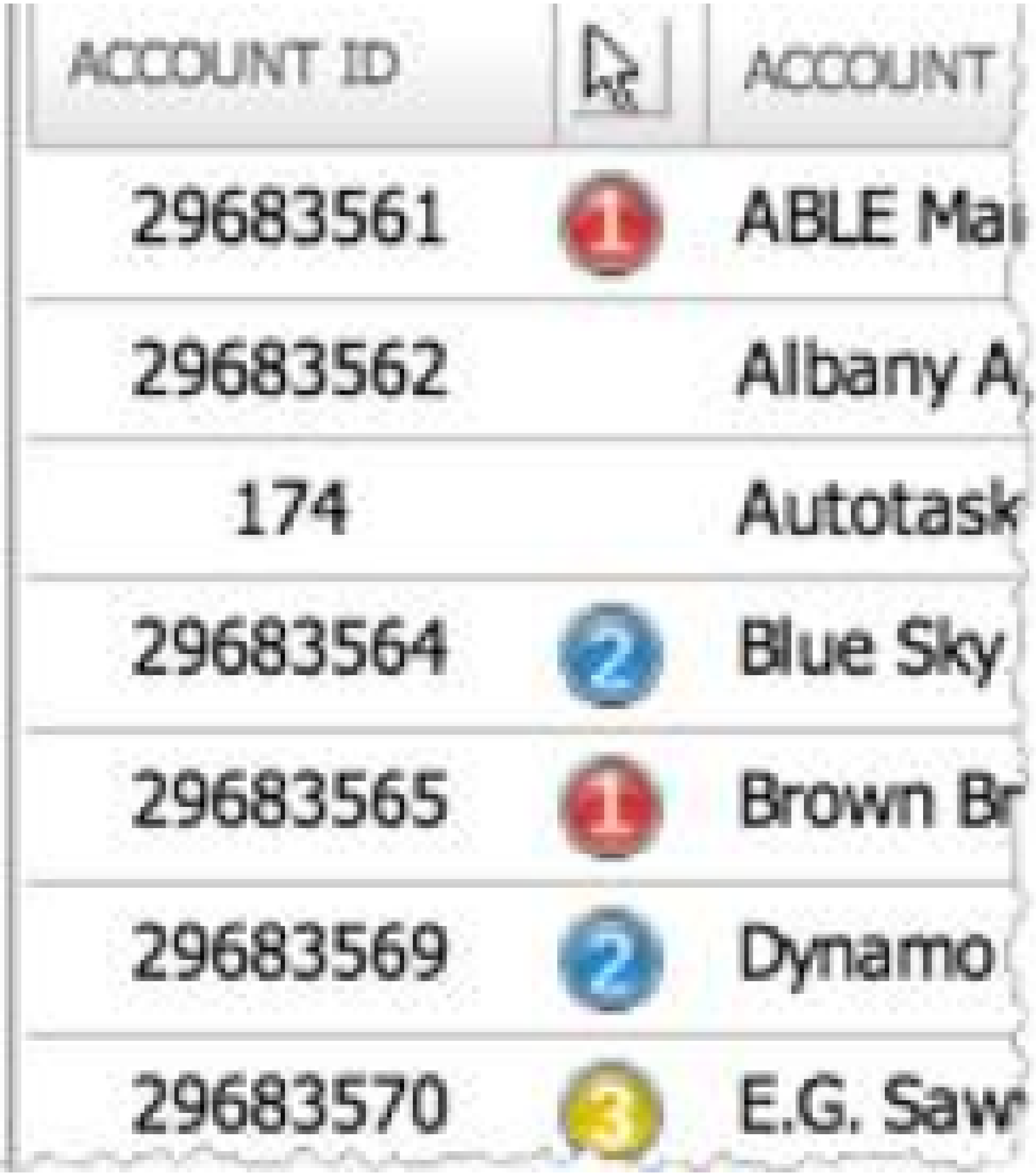
Available Columns

Market Segment
Owner
Competitor
City
Zip Code
Fax
Country
Address
Active
Account Number
Opted Out from Surveys
Invoice Template
Invoice Emailing Enabled
Primary Contact
Tax Region
Account Survey Rating
Lead Source
Number of Employees

Selected Columns

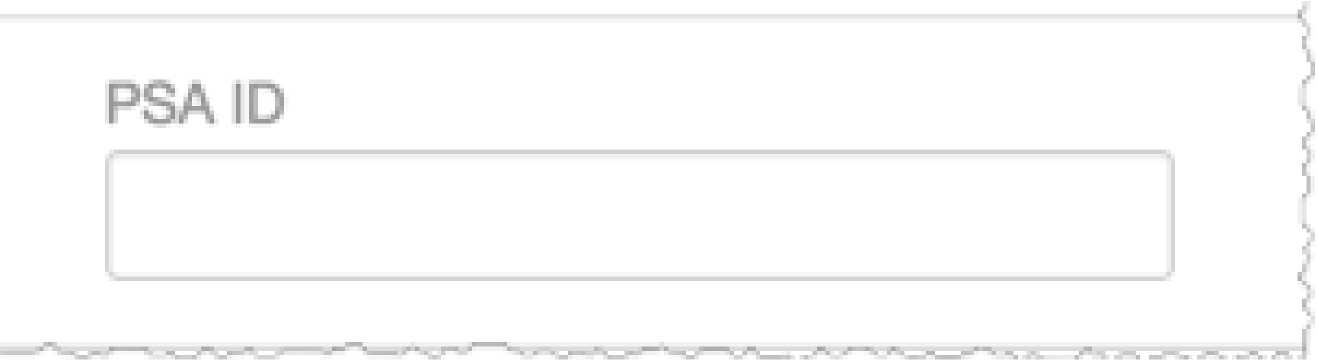
Account ID
Classification
Account
Parent Account
Territory
Phone
Web
State
Total Opportunity Amount
Last Activity
Type

This shows you the Account ID for the customer:



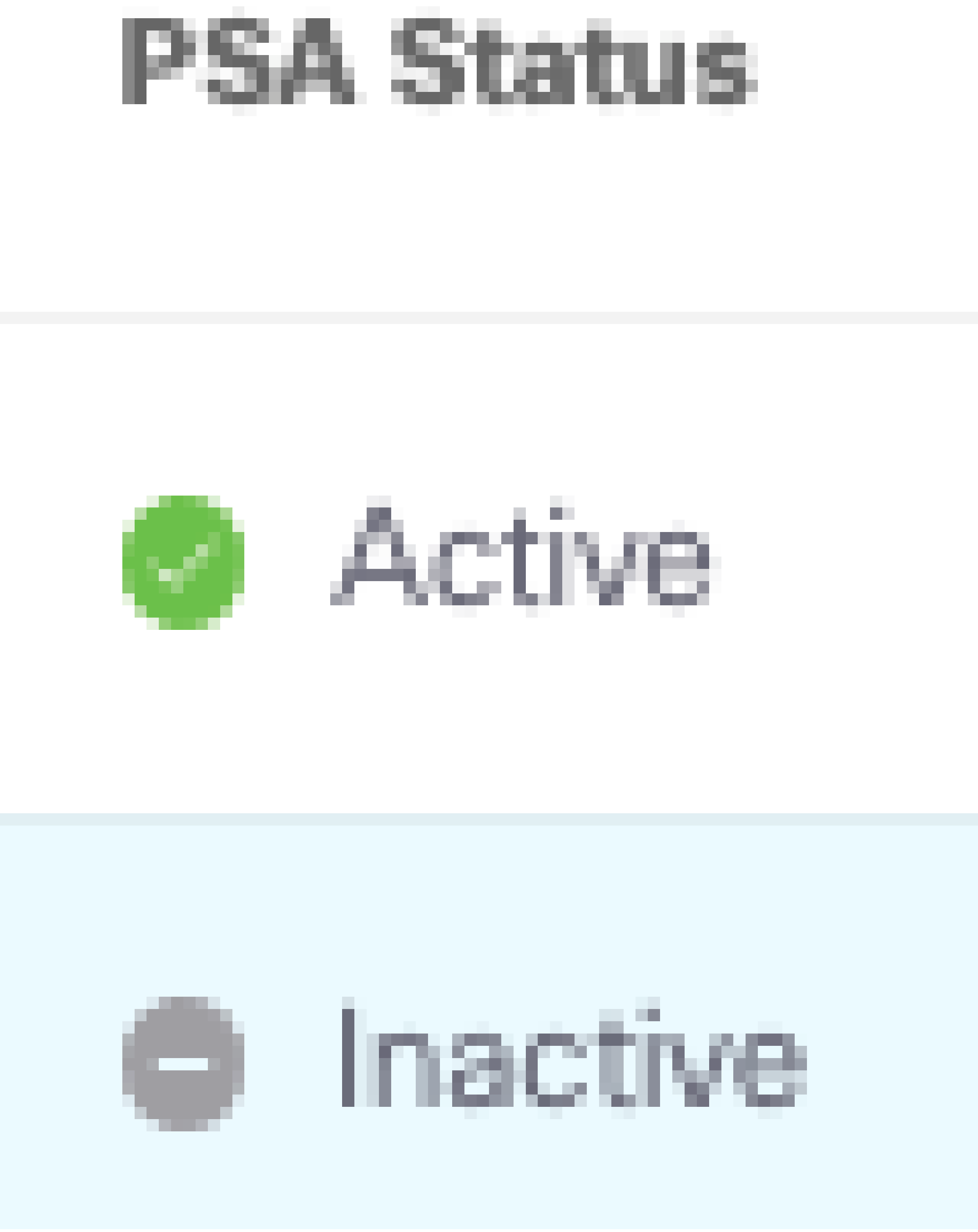
| ACCOUNT ID | | ACCOUNT |
|---|---|---|
| 29683561 | 1 | ABLE Ma |
| 29683562 | | Albany A |
| 174 | | Autotask |
| 29683564 | 2 | Blue Sky |
| 29683565 | 1 | Brown Br |
| 29683569 | 2 | Dynamo |
| 29683570 | 3 | E.G. Saw |

4. Once you have the account ID for your customer, return to Cisco Umbrella for MSPs.
5. Navigate to **Customer Management** to show a list of the customers you have configured in your console
   **Note:** If there are no customers listed here, you need to add customers to your Cisco Umbrella for MSPs MSP. Please read the Cisco Umbrella for MSPs User Guide for more information.
6. Next, select the customer to map to Autotask. This example uses "Able Manufacturing Co."
7. Earlier, we found that Able Manufacturing Co. has an Account ID of 29683561. Select the name of the customer and then enter the Company Account ID under the field for **PSA ID**.



PSA ID

8. Select **Save** to confirm the change. You receive a confirmation message about the integration being enabled. From that point forward, the PSA ID shows next to the customer it is enabled for in the Customer Details.
9. To confirm your integration is enabled, navigate to **Centralized Reports > Deployment Status**. If it is operational, a **PSA Status** column is populated.
   - Organizations with valid PSA IDs show up with a green **Active** status.
   - Organizations that do not have a PSA ID value show up with a gray **Inactive** status.



PSA Status

✓ Active

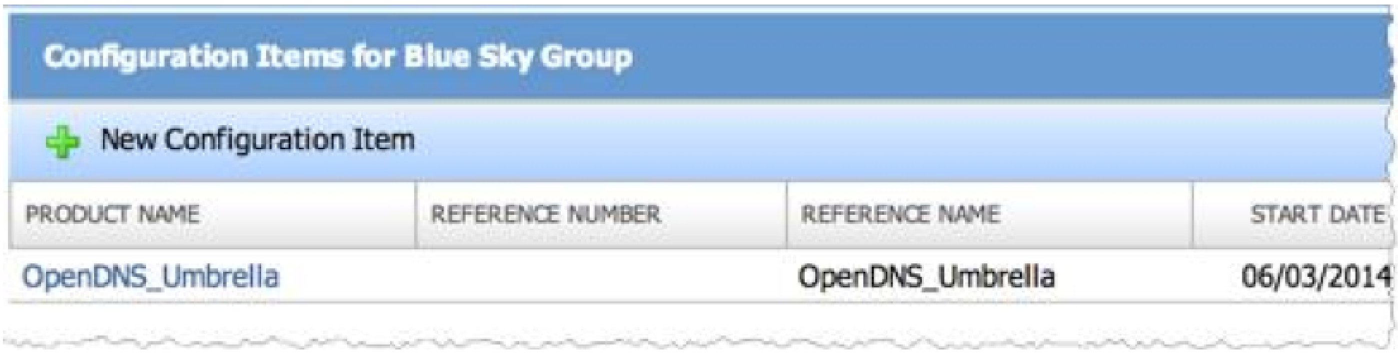
⊖ Inactive

*360053576152*

## Setting up the "OpenDNS_Umbrella" Configuration Item (Optional)

Once the PSA Company ID has been successfully integrated, an Installed Product/Configuration Item named OpenDNS_Umbrella are automatically created.

You can view the Configuration Item under **Directory** > **Accounts** and then select one of the accounts you integrated in Step 4. Within this account, there is now be a Configuration Item for OpenDNS_Umbrella.



Configuration Items for Blue Sky Group

New Configuration Item

| PRODUCT NAME | REFERENCE NUMBER | REFERENCE NAME | START DATE |
|---|---|---|---|
| OpenDNS_Umbrella | | OpenDNS_Umbrella | 06/03/2014 |

Note that by default, the Configuration Item includes all possible fields and the Cisco Umbrella fields we’ve added in the integration. Some fields are not filled as they are not applicable to Cisco Umbrella, such as Brand or Make & Model.

To change the product to not include these fields, set up a unique Configuration type for Cisco Umbrella.

## Configuration Type Setup

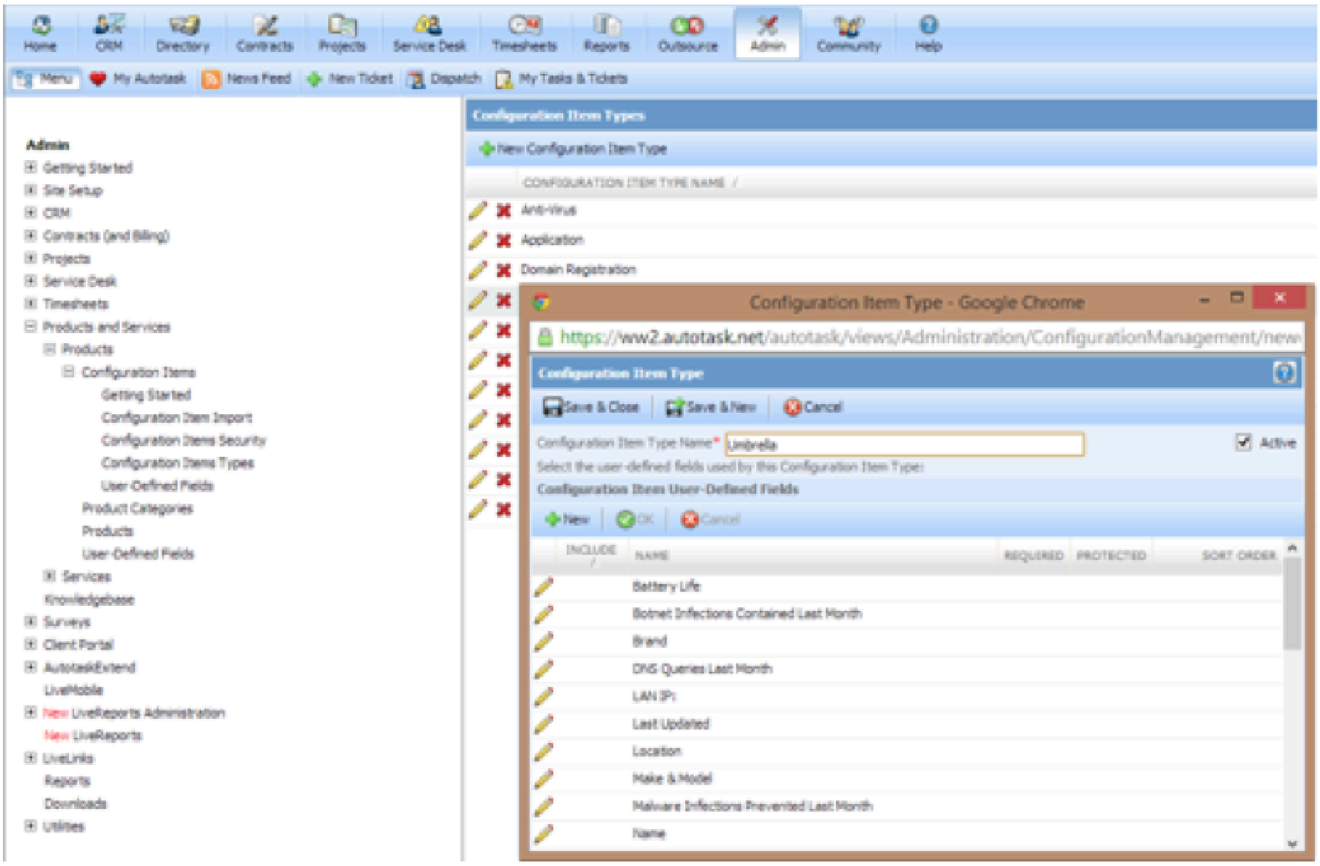
Configuration items created in Autotask through the Cisco Umbrella integration create user-defined fields (UDFs) for your Cisco Umbrella auto-updated information. By default, a new product shows all UDFs, and a configuration item type is recommended. Due to limitations with the current Autotask API, creating a Configuration Item Type within Autotask is limited to manual intervention by you or your Autotask administrator. This table provides a list of all fields which must be added to your Configuration Item Type.

| # | **Field Name** | **Type** |
|---|---|---|
| 1 | Organization Id | Text (Single Line) |
| 2 | Last Updated | Text (Single Line) |
| 3 | Package | Text (Single Line) |
| 4 | Seats | Text (Single Line) |
| 5 | Networks Total | Text (Single Line) |
| 6 | Networks Active in Last 7 Days | Text (Single Line) |

| | | |
|---|---|---|
| 7 | Networks Inactive in Last 7 Days | Text (Multi-Line) |
| 8 | Umbrella Agents Deployed | Text (Single Line) |
| 9 | Umbrella Agents Active in Last 7 Days | Text (Single Line) |
| 10 | Umbrella Agents Inactive in Last 7 Days | Text (Multi-Line) |
| 11 | DNS Queries Last Month | Text (Single Line) |
| 12 | Malware Infections Prevented Last Month | Text (Single Line) |
| 13 | Botnet Infections Contained Last Month | Text (Single Line) |
| 14 | Top Domains Last Month | Text (Multi-Line) |
| 15 | Top Domains Blocked Last Month | Text (Multi-Line) |
| 16 | Top Categories Last Month | Text (Multi-Line) |

For users who are unfamiliar with the setup of new Configuration Item Types in Autotask, please use these instructions to create the new record in the system:

1. Sign in to Autotask as an administrator.
2. Navigate to the **Admin** section using the top menu.
3. Navigate to **Products and Services > Products > Configuration Items** and select "Configuration Items Types."



Anti-Virus

Application

Domain Registration

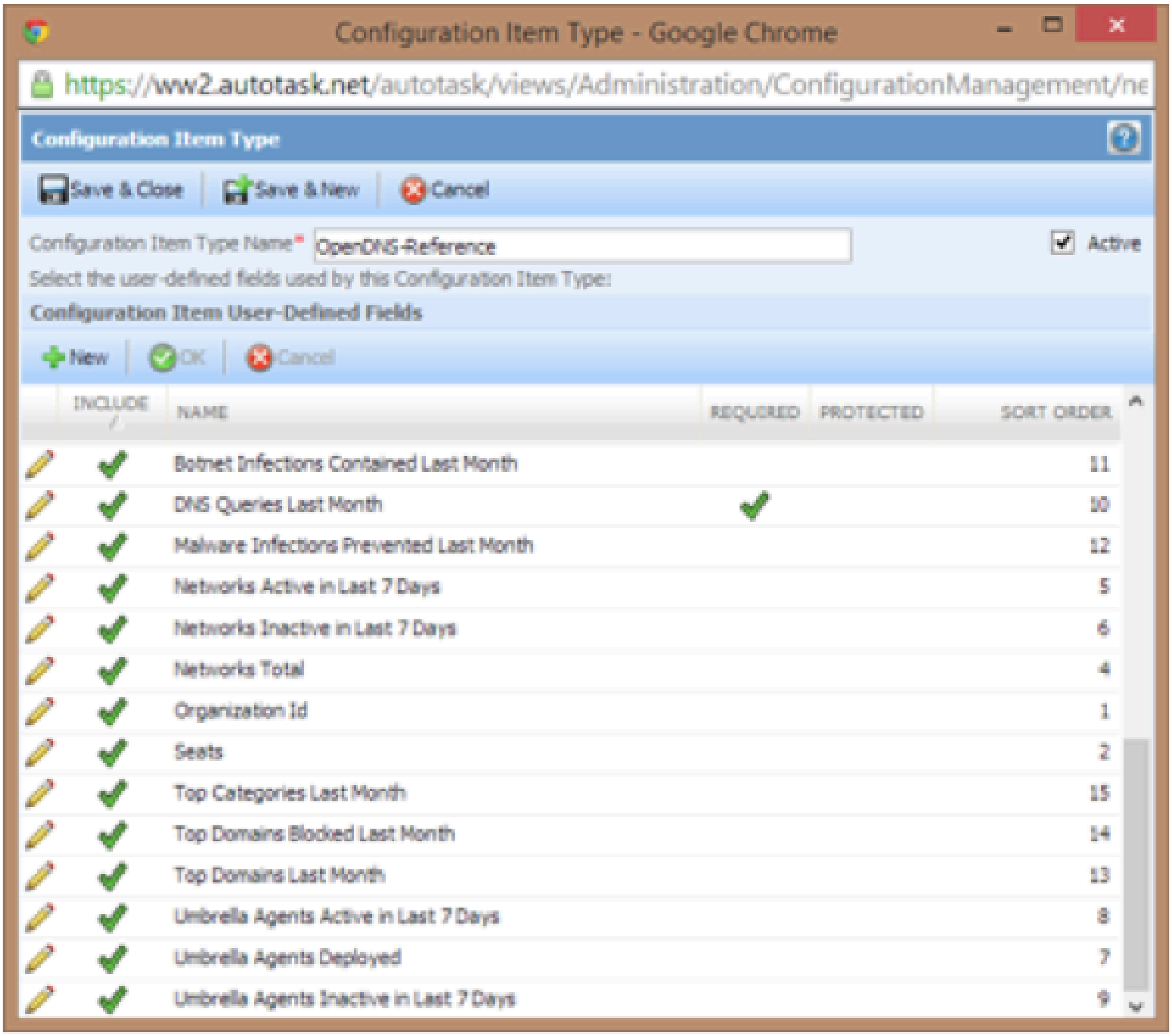
Configuration Item Type - Google Chrome
https://ww2.autotask.net/autotask/views/Administration/ConfigurationManagement/new
Configuration Item Type
Save & Close
Save & New
Cancel

Configuration Item Type Name* Umbrella ☑ Active

Select the user-defined fields used by this Configuration Item Type:

| INCLUDE | NAME | REQUIRED | PROTECTED | SORT ORDER |
|---|---|---|---|---|
| | Battery Life | | | |
| | Botnet Infections Contained Last Month | | | |
| | Brand | | | |
| | DNS Queries Last Month | | | |
| | LAN IP: | | | |
| | Last Updated | | | |
| | Location | | | |
| | Make & Model | | | |
| | Malware Infections Prevented Last Month | | | |
| | Name | | | |

4. Select the **New Configuration Item Type** menu option.
5. Enter a name for your new Configuration Item Type.
6. Select **New** and enter the field information for the first field at the top.
7. Repeat step 6 until you have added all the fields in the table to the new item type.


Configuration Item Type - Google Chrome
https://ww2.autotask.net/autotask/views/Administration/ConfigurationManagement/ne
Configuration Item Type
Save & Close
Save & New
Cancel
Configuration Item User-Defined Fields
New
OK
Cancel

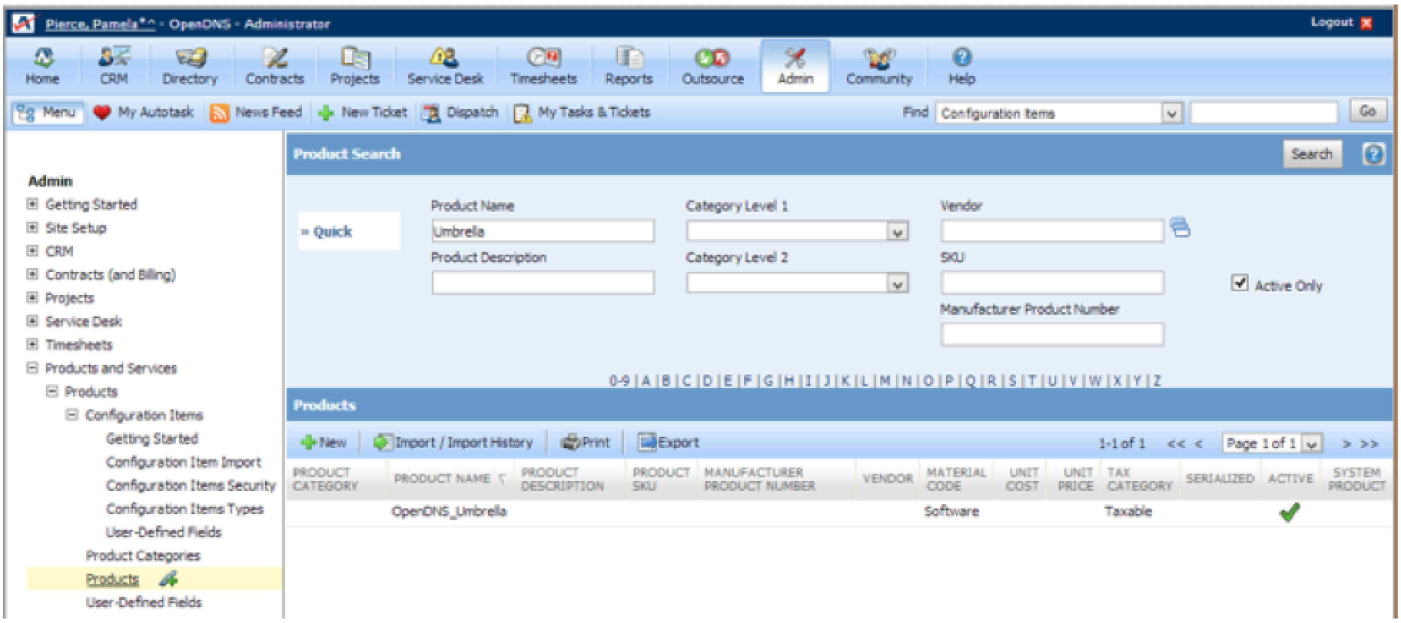
Configuration Item Type Name* OpenDNS-Reference ☑ Active

Select the user-defined fields used by this Configuration Item Type:

| | INCLUDE | NAME | REQUIRED | PROTECTED | SORT ORDER |
|---|---|---|---|---|---|
| ✎ | ✓ | Botnet Infections Contained Last Month | | | 11 |
| ✎ | ✓ | DNS Queries Last Month | ✓ | | 10 |
| ✎ | ✓ | Malware Infections Prevented Last Month | | | 12 |
| ✎ | ✓ | Networks Active in Last 7 Days | | | 5 |
| ✎ | ✓ | Networks Inactive in Last 7 Days | | | 6 |
| ✎ | ✓ | Networks Total | | | 4 |
| ✎ | ✓ | Organization Id | | | 1 |
| ✎ | ✓ | Seats | | | 2 |
| ✎ | ✓ | Top Categories Last Month | | | 15 |
| ✎ | ✓ | Top Domains Blocked Last Month | | | 14 |
| ✎ | ✓ | Top Domains Last Month | | | 13 |
| ✎ | ✓ | Umbrella Agents Active in Last 7 Days | | | 8 |
| ✎ | ✓ | Umbrella Agents Deployed | | | 7 |
| ✎ | ✓ | Umbrella Agents Inactive in Last 7 Days | | | 9 |

8. Save and close your new Configuration Item Type.

# Product Setup



Find: Configuration Items

Product Name: Umbrella

Product Description:

Category Level 1:

Category Level 2:

Vendor:

SKU:

Manufacturer Product Number:

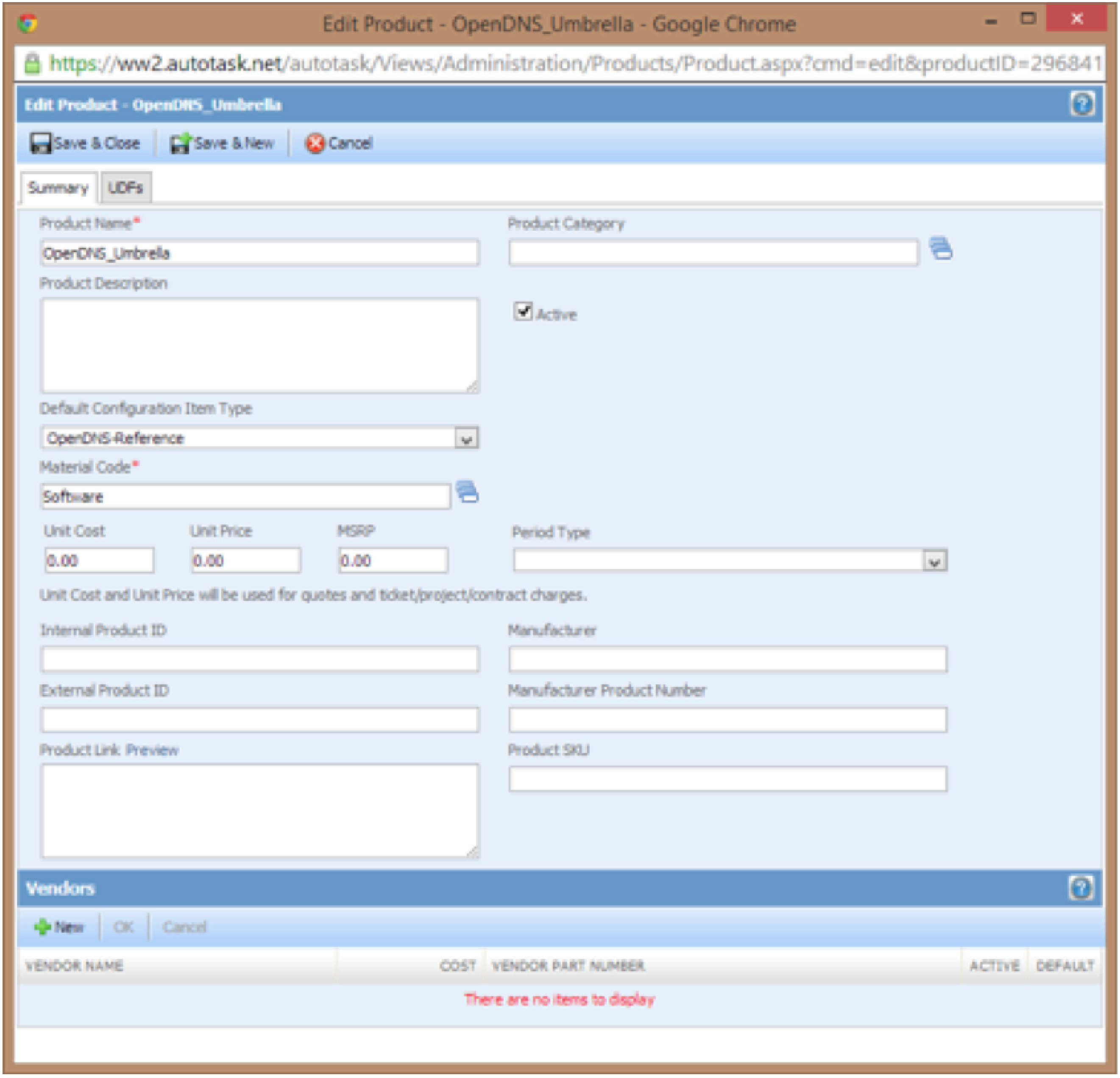
☑ Active Only

| PRODUCT CATEGORY | PRODUCT NAME | PRODUCT DESCRIPTION | PRODUCT SKU | MANUFACTURER PRODUCT NUMBER | VENDOR | MATERIAL CODE | UNIT COST | UNIT PRICE | TAX CATEGORY | SERIALIZED | ACTIVE | SYSTEM PRODUCT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | OpenDNS_Umbrella | | | | | Software | | | Taxable | | ✓ | |

The Cisco Umbrella integration automatically creates a Product within your Autotask implementation to tie configuration items to when being created. After the product has been created in your system, Cisco Umbrella recommends that you update the product definition with settings that best reflect your business standards and needs.

To identify the product definition and update its settings use these steps:

1. Sign in to Autotask as an administrator.
2. Navigate to the **Admin** section using the top menu.
3. Navigate to **Products and Services** > **Products** and select **Products**.
4. Type "Umbrella" into the Product Name search field and select **Search**.
5. Select the Umbrella product to view its details.



Edit Product - OpenDNS_Umbrella - Google Chrome

https://ww2.autotask.net/autotask/Views/Administration/Products/Product.aspx?cmd=edit&productID=296841

Edit Product - OpenDNS_Umbrella

Product Name*: OpenDNS_Umbrella

Product Category:

Product Description:

☑ Active

Default Configuration Item Type: OpenDNS-Reference

Material Code*: Software

Unit Cost: 0.00

Unit Price: 0.00

MSRP: 0.00

Period Type:

Unit Cost and Unit Price will be used for quotes and ticket/project/contract charges.

Internal Product ID:

Manufacturer:

External Product ID:

Manufacturer Product Number:

Product Link Preview:

Product SKU:

Vendors

| VENDOR NAME | COST | VENDOR PART NUMBER | ACTIVE | DEFAULT |
|---|---|---|---|---|

There are no items to display

6. Update the product definition to reflect your desired settings.
7. Select **Save & Close**.

**Notes:**

- Do not change the Product Name string from "OpenDNS_Umbrella" to something else. This breaks the integration, but if you did rename it,  rename it back to fix the issue.

- Make sure "Active: is selected as you see in the screenshot.

The definitions of each of the Cisco Umbrella AutoTask fields that are updated and included in the Configuration Item are listed in this table:

| Field | Description |
|---|---|
| Organization Id | Umbrella internal organization ID |
| Last Updated | Date at which the last sync with Umbrella took place |
| Seats | Total number of seats applied to this company. |
| Networks Total | Total number of networks applied to this company |
| Networks Active (7 Days) | Total number of active networks in the last seven days |
| Networks Inactive (7 Days) | List of network names inactive in the last seven days |
| Umbrella Agents Deployed | Number of Umbrella Roaming agents deployed |
| Umbrella Agents Active 7 Days | Number of Umbrella Roaming agents active in the last seven days |
| Umbrella Agents Inactive 7 Days | Names of Umbrella Roaming agent identities inactive in the last seven days |
| DNS Queries Last Month | Total number of DNS requests for this company in the previous calendar month |

| | |
|---|---|
| Malware Infections Prevented Last Month | Number of sites hosting malware prevented from access in the previous calendar month |
| Botnet Infections Contained Last Month | Number of sites hosting botnet command and control prevented from access in the previous calendar month |
| Top Domains Last Month | List of the names of the most heavily accessed domains in the previous calendar month |
| Top Domains Blocked Last Month | List of the names of the most frequently blocked domains in the previous calendar month |
| Top Categories Last Month | List of content categories most frequently requested in the previous calendar month, including number of requests per category |