# SecureX with Orbital Advanced Search Integration Guide

## Contents



## Introduction

This document describes the process required to integrate and verify Cisco SecureX with Cisco Orbital Advanced Search.

Contributed by Yeraldin Sanchez and Uriel Torres, Edited by Jorge Navarrete, Cisco TAC Engineers.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AMP for Endpoints Essentials with Orbital, Advantage or Premier License
- Cisco Orbital Advanced Search
- Basic Navigation in the SecureX Console
- Optional Virtualization of images

### Components Used

- AMP for Endpoints Console Version 5.4.20200804
- AMP for Endpoints Administrator Account
- Orbital Advanced Search Console Version 1.7
- SecureX Console Version 1.54
- SecureX Administrator Account
- Microsoft Edge Version 84.0.522.52

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Background Information

Orbital is an advanced capability in Cisco AMP for Endpoints designed to make security investigation and threat hunting simple. It provides an implementation of powerful Osquery technology on each of your AMP Endpoints. Orbital allows you to create custom queries to look across your network for information of interest, but also comes with over a hundred pre-canned queries, that allow you to quickly run complex queries on any or all endpoints.

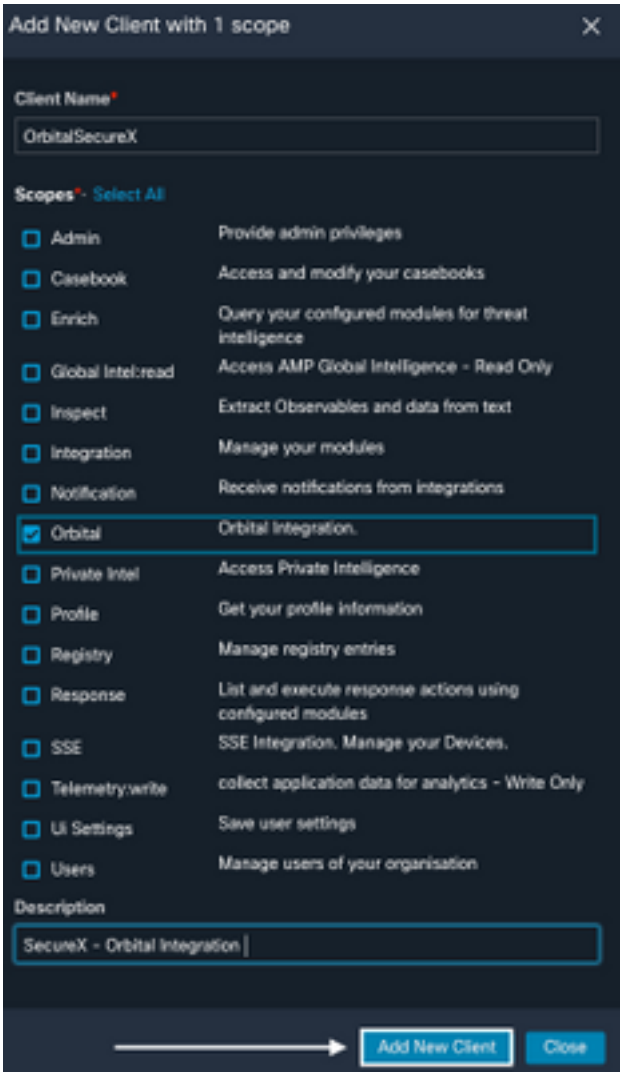
The Orbital module has 4 tiles that you can add to a SecureX dashboard.

- **Organization Query and Results Stats:**A set of metrics that describes organization queries and result
- **User Catalog Stats:** A set of metrics that describes the most highly used catalog queries for this user
- **Organization Catalog Stats:** A set of metrics that describes the most highly used catalog queries for this organization
- **User Query and Results Stats:** A set of metrics that describes user queries and results

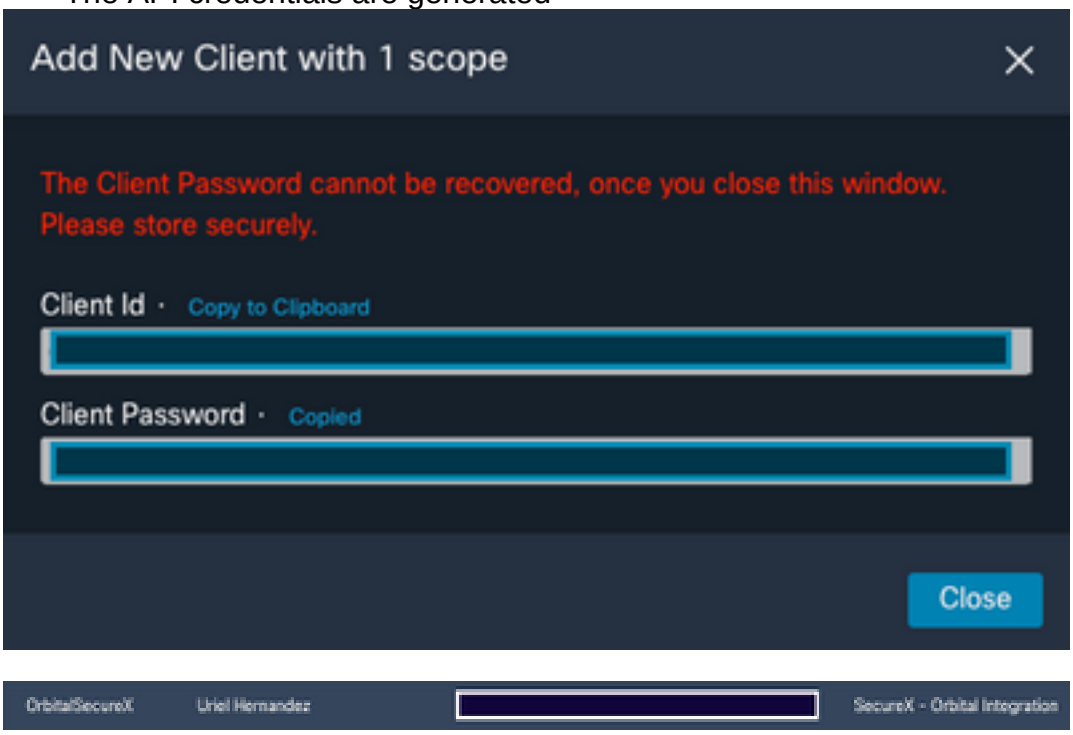
# Configure

## Generate the API Credentials in the SecureX Console

- Log in to SecureX
- Navigate to **Integrations** > **Settings** > **API Clients**
- Click on **Generate API Client**
- Name the Client, check **Orbital,** describe the API and click **Add New Client**




- The API credentials are generated



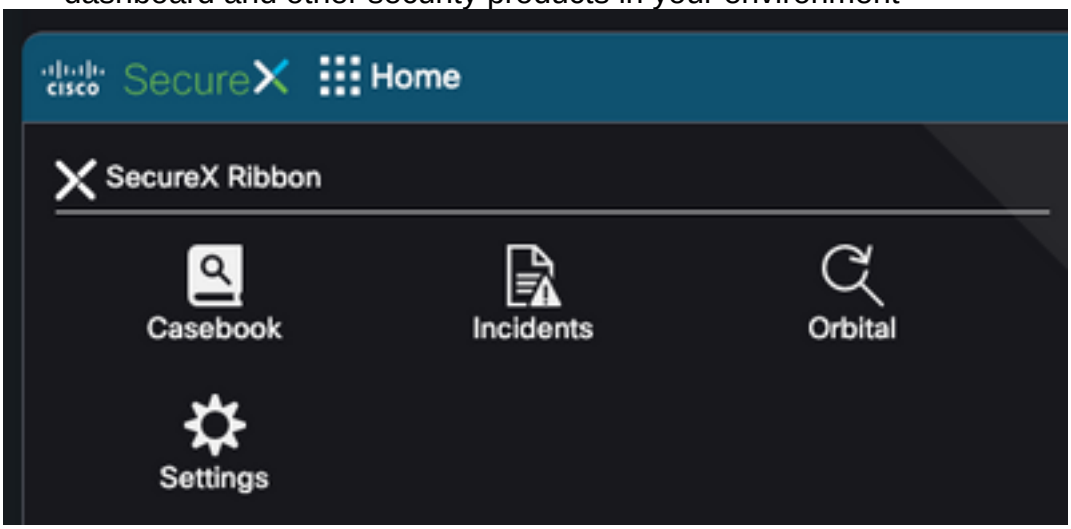

**Note**: This information is available only in this window, save your credentials in a backup file.

## Enable SecureX Ribbon in the AMP Console

SecureX is both a centralized console and a distributed set of capabilities that unify visibility, enable automation, accelerate incident response workflows, and improve threat hunting. These distributed capabilities are presented in the form of applications (apps) and tools in the SecureX Ribbon, the SecureX Ribbon can be enabled in the Orbital Console.

- Log in to Orbital Console
- On the Orbital Console
- Navigate to **<Yout User>** > **Settings**
- Enable the SecureX Ribbon

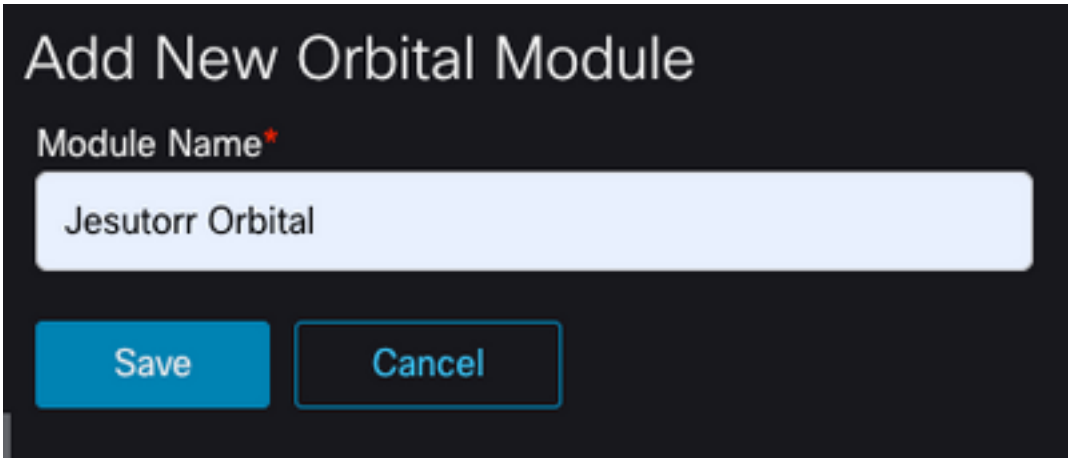

- The Ribbon is located in the lower portion of the page and persists as you move between the dashboard and other security products in your environment




## Integrate the Orbital Module in SecureX

Orbital can enrich information presented in the Threat Response relations graph by if you into Orbital to query and gather additional intelligence about your host, IP, IP4, IP6, MAC, and OS, etc. The Orbital app is available on the SecureX ribbon and allows you to run a live query. You can also view metrics and your recent queries in the right pane.

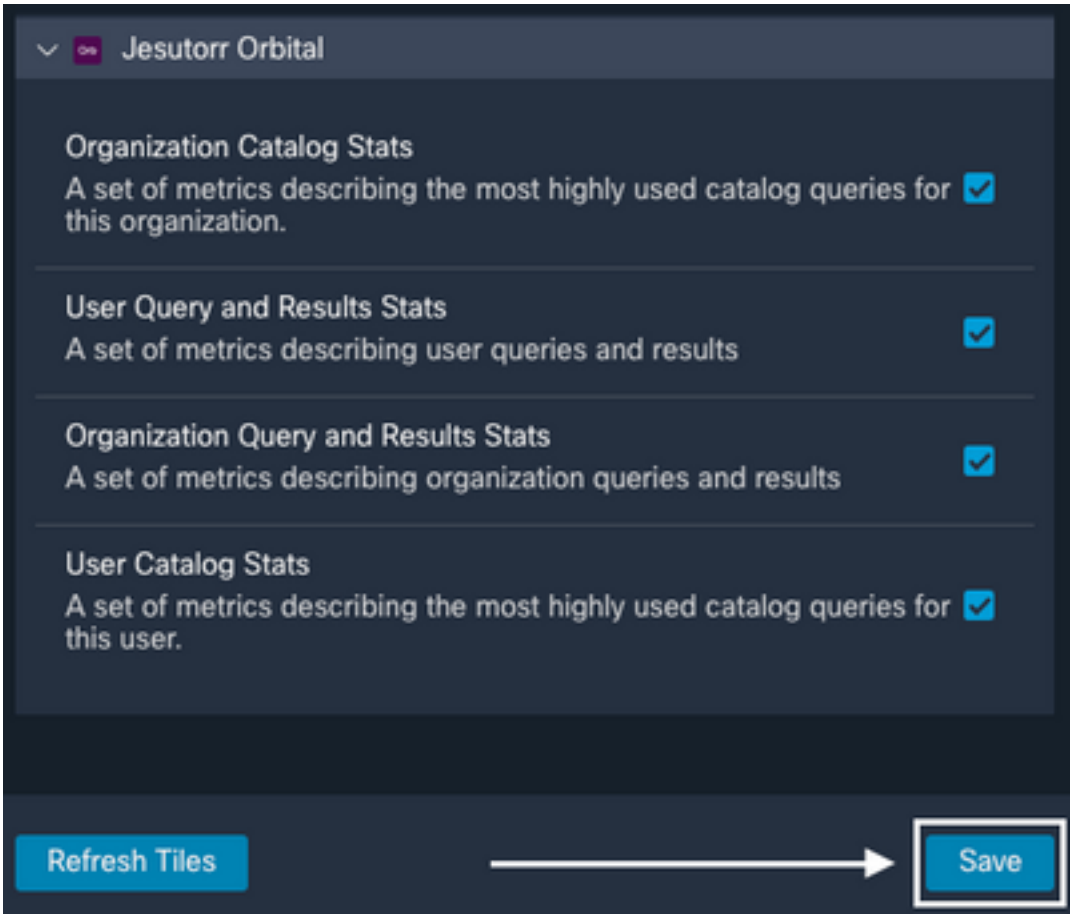
- On SecureX
- Navigate to **Integrations** > **Add New Module**
- Select Orbital and click on **Add New Module**
- Name the module and click on **Save**



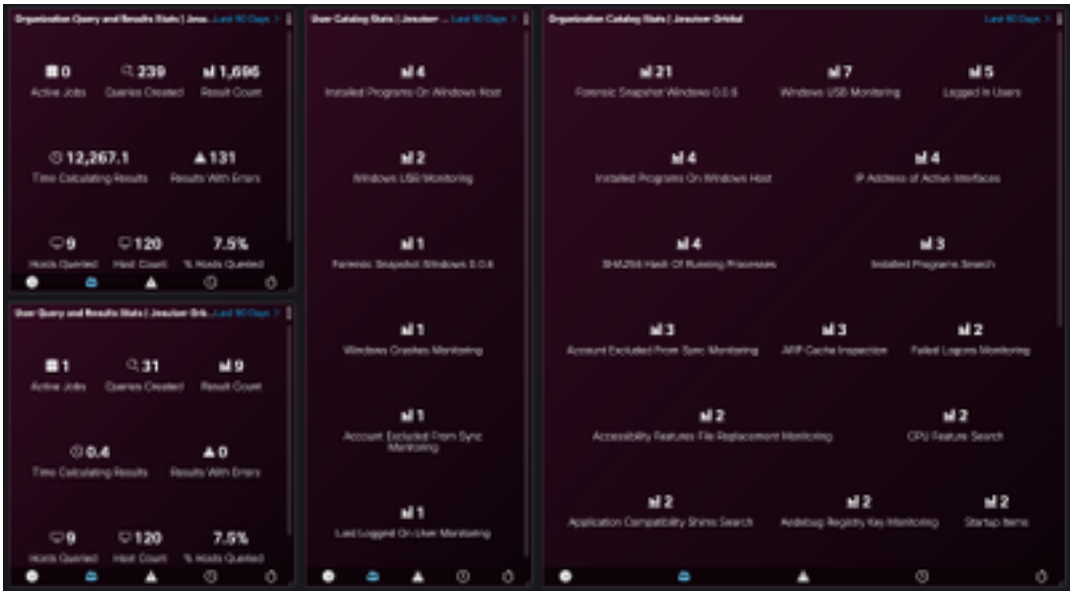

## Verify

Validate that the information from the Orbital Advanced Se Console is displayed in the SecureX Dashboard.

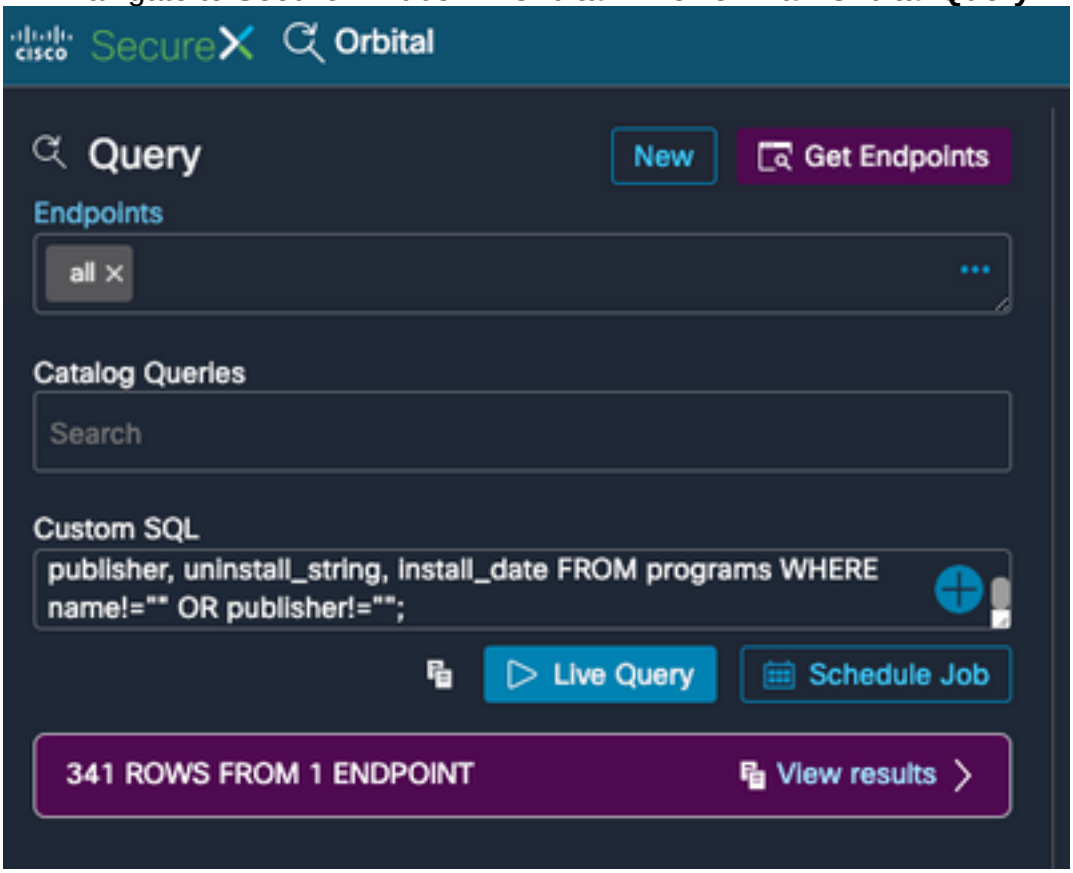
- On SecureX navigate to **Dashboard**
- Click on**New Dashboard** and name it
- Select the Orbital Module previously generated
- Select the tiles, for this guide all of them are added
- Click **Save**




- Select the **Timeframe** and verify if data from Orbital is displayed in SecureX



- An investigation can be launched from the SecureX Ribbon
- Navigate to **SecureXRibbon** > **Orbital** > **Perform an Orbital Query**




## Related Information

- **You can find videos about how to configure your product integrations here.**
- **Technical Support & Documentation - Cisco Systems**