Configure SecureX Integration with Tetration

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Generate the API credentials in Tetration Security Dashboard
Integrate the Tetration Module in SecureX
Verify
Video Guide

Introduction

This document describes the process required to integrate and verify Cisco SecureX with Cisco Tetration.

Contributed by Juan Castillero 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
- Tetration Security Dashboard
- Basic Navigation in the SecureX Console
- Optional Virtualization of images

Components Used

- TetrationvSecurity Dashboard
- Tetration Administrator account
- 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

The Cisco Tetration platform addresses workload and application security challenges that provides micro-segmentation and behavior-based anomaly detection capabilities across hybrid cloud infrastructure, the tetration module provides 3 tiles.

Tetration Vulnerable Workloads and Inventory: Metrics that describe workloads with known vulnerabilities and the total inventory count.

Tetration Policy Metrics: Metrics that describe configured segmentation policies.

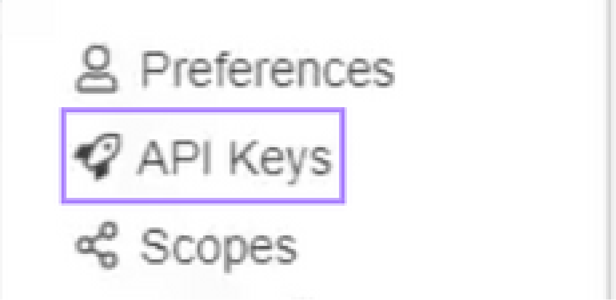
Tetration Software Agents Summary: Metrics that describe the connected software agents.

Configure

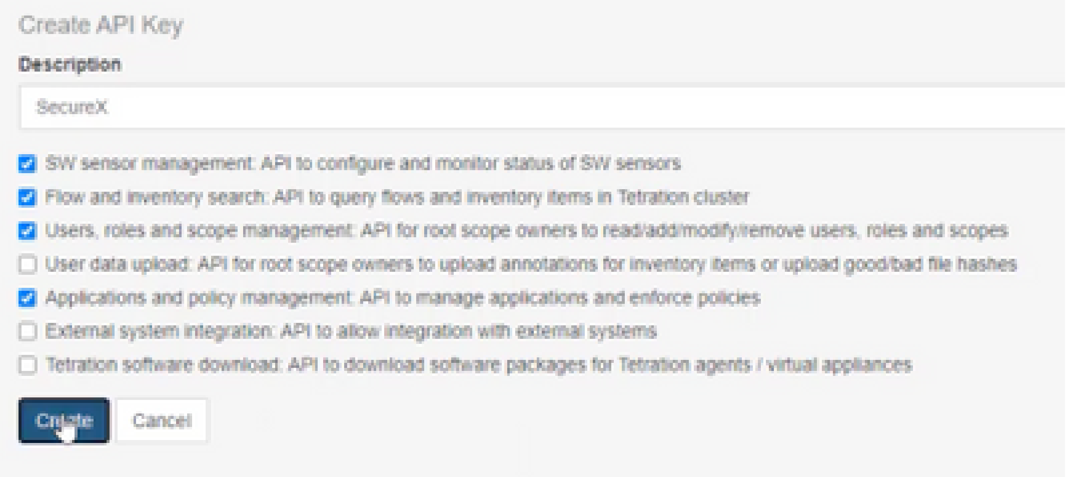
Generate the API credentials in Tetration Security Dashboard

In the Tetration Security Dashboard, new APIs are created

- Log in to the **Tetration Security Dashboard** with administration privileges.
- On the console navigate to **Your Account > API Keys**.



- Click on **Create API Key**
- Select these elements: SW sensor management: API to configure and monitor the status of SW sensors.Flow and inventory search: API to query flows and inventory items in the Tetration cluster.Users, roles, and scope management: API for root scope owners to read/add/modify/remove users, roles, and scopes.Applications and policy management: API to manage applications and enforce policies.



Create API Key

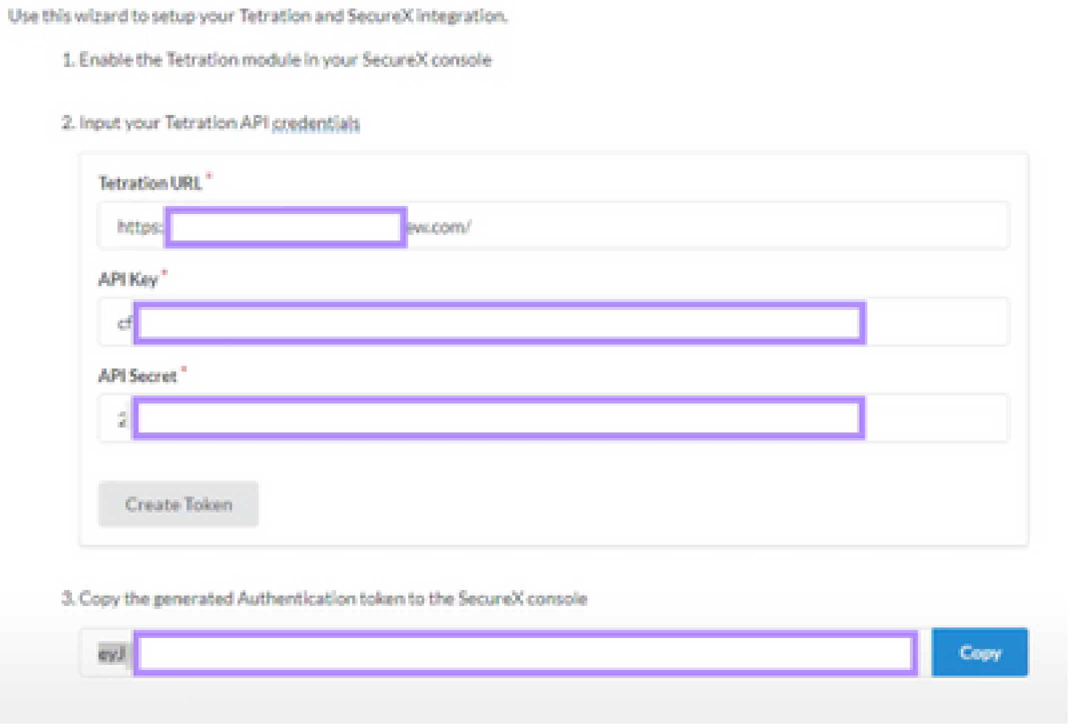
Description

SecureX

☑ SW sensor management: API to configure and monitor status of SW sensors
☑ Flow and inventory search: API to query flows and inventory items in Tetration cluster
☑ Users, roles and scope management: API for root scope owners to read/add/modify/remove users, roles and scopes
☐ User data upload: API for root scope owners to upload annotations for inventory items or upload good/bad file hashes
☑ Applications and policy management: API to manage applications and enforce policies
☐ External system integration: API to allow integration with external systems
☐ Tetration software download: API to download software packages for Tetration agents / virtual appliances

> **Important:** Retrieve these values before you close the dialog box; the generated API information cannot be retrieved once the tab is closed.

- Save the API credentials
- In order to create the integration token navigate to tetration-securex.link/setup
- Introduce your Tetration URL and the API Credentials
- Click **Create Token**
- Copy the integration token



Use this wizard to setup your Tetration and SecureX integration.

1. Enable the Tetration module in your SecureX console

2. Input your Tetration API credentials

Tetration URL *

https:[redacted]ew.com/

API Key *

cf[redacted]

API Secret *

2[redacted]

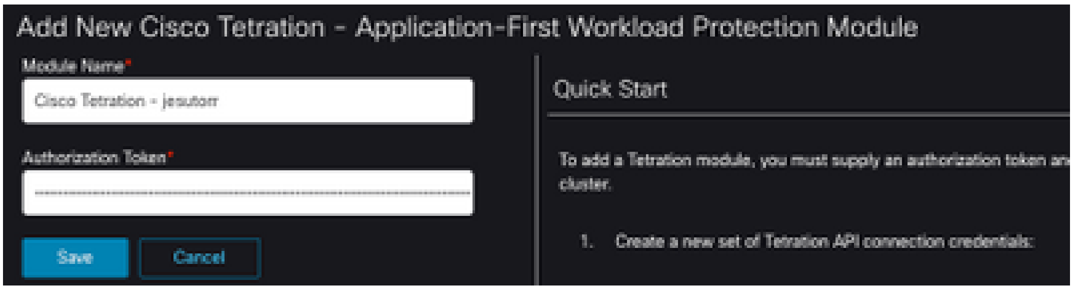
3. Copy the generated Authentication token to the SecureX console

eyJ[redacted]

Integrate the Tetration Module in SecureX

Integrate Tetration with SecureX to gain visibility into the health of your Tetration system, expose vulnerable workloads, track segmentation policy, and react to behavior deviations.

- On SecureX console navigate to **Integrations** > **Click Add New Module**
- Select the **Cisco Tetration** module and click **Add New Module**
- Name the module
- Paste the token and click on **Save**



Add New Cisco Tetration - Application-First Workload Protection Module

Module Name*

Cisco Tetration - jesutorr

Authorization Token*

••

Quick Start

To add a Tetration module, you must supply an authorization token an
cluster.

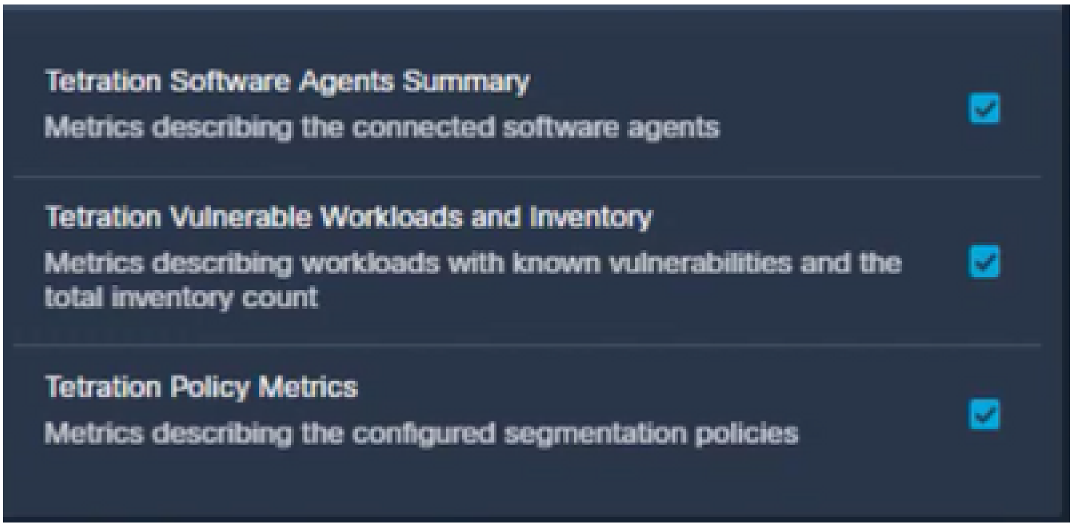
1. Create a new set of Tetration API connection credentials:

Verify

Validate that the information from the Tetration Security Dashboard is displayed in the SecureX Dashboard.

- On SecureX navigate to **Dashboard**

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

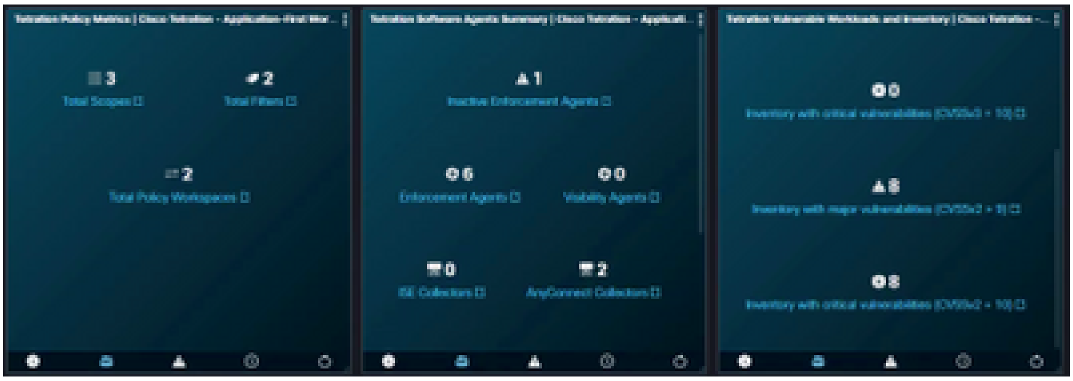


Tetration Software Agents Summary
Metrics describing the connected software agents ☑

Tetration Vulnerable Workloads and Inventory
Metrics describing workloads with known vulnerabilities and the total inventory count ☑

Tetration Policy Metrics
Metrics describing the configured segmentation policies ☑

- Select the **Timeframe** and verify if data from Tetration is Displayed in Secure


Tetration Policy Metrics | Cisco Tetration - Application-First Wor...
3
Total Scopes
2
Total Filters
2
Total Policy Workspaces
Tetration Software Agents Summary | Cisco Tetration - Applicati...
1
Inactive Enforcement Agents
6
Enforcement Agents
0
Visibility Agents
0
ISE Collectors
2
AnyConnect Collectors
Tetration Vulnerable Workloads and Inventory | Cisco Tetration -...
0
Inventory with critical vulnerabilities
8
Inventory with major vulnerabilities
8
Inventory with critical vulnerabilities

If issues arise and no data is displayed review the API keys are correctly applied. If the issue persists, contact the support team.

Video Guide