Troubleshoot Cisco XDR and Secure Malware Analytics Cloud Integration

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Troubleshoot
License
Module Tiles
Administrator role
Timeframe
Recreate Module

Introduction

This document describes how to troubleshoot Secure Malware Analytics Cloud module with Cisco XDR.

Contributed by Javi Martinez, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Malware Analytics Cloud
- Cisco XDR

Components Used

The information in this document is based on these software versions:

- Secure Malware Analytics Cloud console (User account with Administrator rights)
- Cisco XDR console (User account with Administrator rights)

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

Cisco Secure Malware Analytics Cloud is an advanced and automated malware analysis and malware threat intelligence platform in which suspicious files or web destinations can be detonated without impact the user environment.

In the integration with Cisco XDR, Secure Malware Analytics is a reference module and provides the ability to pivot into the Secure Malware Analytics Portal to gather additional intelligence about file hashes, IPs, domains, and URLs in the Secure Malware Analytics Cloud (SMA Cloud) knowledge store.

Please refer to the latest Secure Malware Analytics Cloud Integration Guide,

- NAM Cloud.
- EU Cloud.

Troubleshoot

License

- Verify you have a proper SMA license in order to get access to Secure Malware Analytics Cloud console

Module Tiles

- Verify you select the proper ***Tiles*** for Secure Malware Analytics Cloud Module
  Navigate to Cisco XDR portal > Dashboard > Customize button > Select the SMA Cloud module > Add the proper Tiles

Administrator role

- Verify you have a Secure Malware Analytics account with Administrator role in Secure Malware Analytics portal
  Navigate to Cisco XDR portal > Administration > Your account

- Verify you have a SecureX account with Administrator rights in SecureX portal
  Navigate to Malware Analytics portal > My Malware Analytics account

Note: If you don´t have Admin role in the Secure Malware Analytics console and Cisco XDR console, your Administrator is able to change the account role directly from the portal in question

Timeframe

- Verify the Timestamp is properly set on the Cisco XDR portal.
  Navigate to Cisco XDR portal > Dashboard > Timeframe option > Select the proper Timeframe in base on the SMA activity

Recreate Module

- Delete the old SMA module and create a new SMA module.
  Navigate to Secure Malware Analytics Cloud console > My Malware Analytics account > API Key > Copy the API key
  Navigate to Cisco XDR portal > Integration modules > Select the SMA Cloud module > Add the API key and URL (Select the SMA Cloud) > Create the Dashboard

Note: Only users with the Org Admin or Users role can obtain the API key that enables the Secure Malware Analytics integration module in Cisco XDR.