

SecureX with Advanced Malware Protection (AMP) for Endpoints Integration Guide

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Generate the API Credentials in the AMP console](#)

[Enable SecureX Ribbon in the AMP Console](#)

[Integrate the AMP for Endpoints Module in SecureX](#)

[Verify](#)

[Troubleshoot](#)

[API Client Does Not Have Write Access \[403\]](#)

[Error: Unknown API Key Or Client ID \[401\]](#)

[Video Guide](#)

Introduction

This document describes the process required to integrate and verify Cisco SecureX with Cisco Advanced Malware Protection (AMP) for Endpoints.

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
- 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
- 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

Cisco Advanced Malware Protection (AMP) for Endpoints is a core part of the endpoint security platform and is deployed as a preventative and investigative tool that supports detection and/or response functions for Windows, MacOS, Linux, Android, and iOS devices, the AMP for Endpoints module provides 5 tiles.

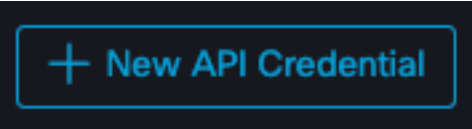
- **Compromises Detected by AMP:** A set of metrics that summarizes compromises detected by AMP
- **AMP Computers Summary:** A set of metrics that summarizes the state of AMP computers
- **AMP Summary:** A set of metrics that summarizes AMP detection and response
- **AMP Quarantines:** A set of metrics that summarizes AMP Quarantines by time
- **MITRE ATT&CK Tactics Detected by AMP:** A set of metrics that summarizes MITRE ATT&CK tactics detected by AMP

Configure

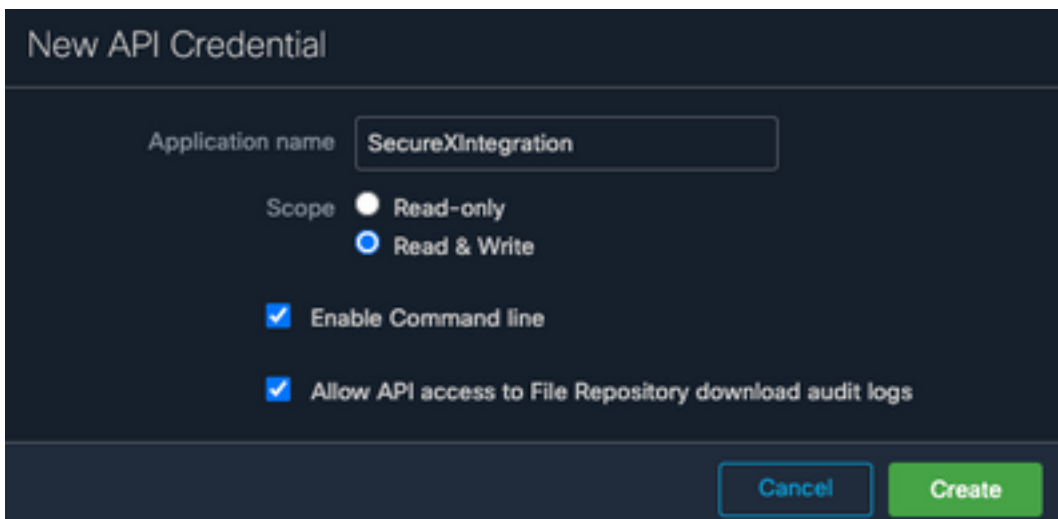
Generate the API Credentials in the AMP console

In the AMP console, new API credentials are created.

- Log in to the AMP Console with administrator privileges
- On the AMP Console navigate to **Accounts > API Credentials**
- Click on **New API Credential**



- Name the application
- Select **Read & Write**
- Check **Enable Command Line** and **Allow API access to File Repository download audit logs**
- Click on **Create**



New API Credential

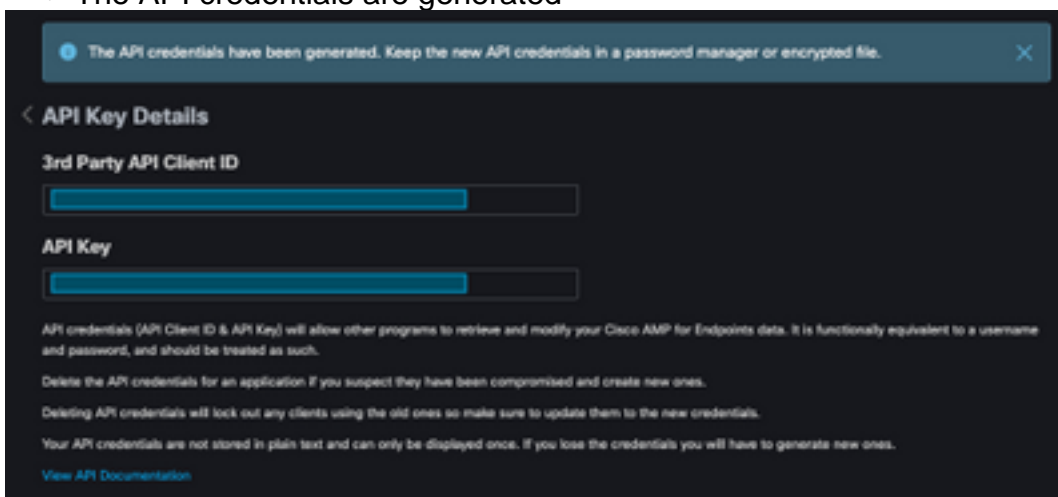
Application name

Scope Read-only Read & Write

Enable Command line

Allow API access to File Repository download audit logs

- The API credentials are generated



The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.

< API Key Details

3rd Party API Client ID

API Key

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a username and password, and should be treated as such.

Delete the API credentials for an application if you suspect they have been compromised and create new ones.

Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

Your API credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.

[View API Documentation](#)

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 AMP Console.

- Log in to SecureX
- On the AMP Console
- Navigate to **Accounts > Users > Click on your User**
- On **Settings** box click SecureX Ribbon **Authorize**

Settings

Two-Factor Authentication [Manage](#)

Remote File Fetch **Enabled**

Command Line **Enabled**

Endpoint Isolation **Enabled**

Time Zone **UTC**

Appearance **Auto** Light Dark

SecureX Ribbon [Authorize](#)

Google Analytics [Opt Out](#)

- You are redirected to the SecureX Threat Response
- Click **Authorize AMP for Endpoints**

Grant Application Access

The application **AMP for Endpoints** (console.amp.cisco.com) would like access to your Cisco Threat Response account.

Specifically, **AMP for Endpoints** is requesting the following:

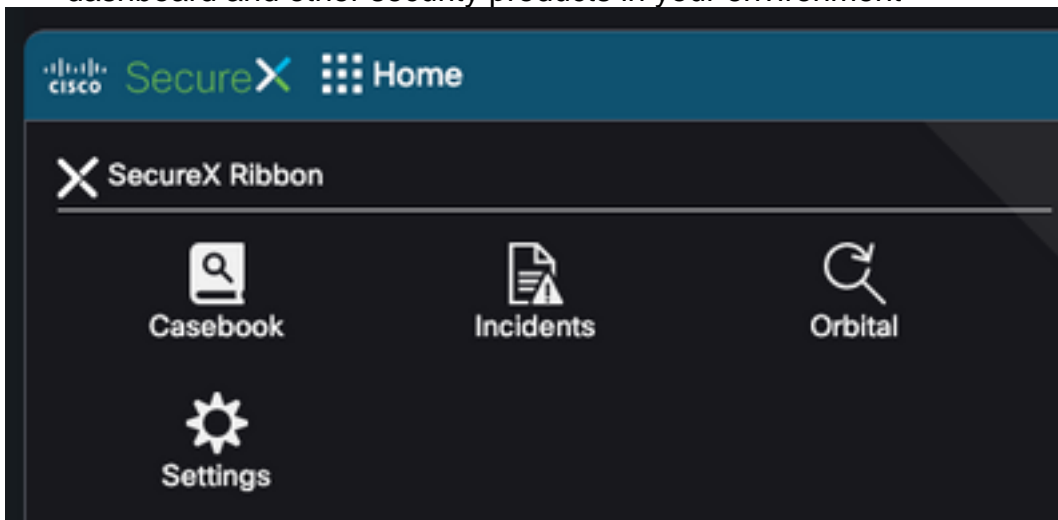
- **casebook**: access and modify your casebooks
- **enrich**: query your configured modules for threat intelligence (*enrich:read*)
- **global-intel**: query AMP Global Intelligence
- **inspect**: extract observables and data from text (*inspect:read*)
- **integration**: manage your integration modules configuration (*integration/module-instance:read, integration/module-type:read*)
- **orbital**
- **private-intel**: access Private Intelligence
- **profile**
- **registry** (*registry/user/ribbon*)
- **response**: list and execute response actions using configured modules
- **telemetry** (*telemetry:write*)
- **users**

[Authorize AMP for Endpoints](#)

[Deny](#)

- 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 AMP for Endpoints Module in SecureX

The AMP for Endpoints module allows you to investigate and identify multiple files with context from integrations across security products. It provides detailed information on affected endpoints and devices, including IP addresses, OS, and AMP GUID.

- On SecureX console navigate to **Integrations > Click Add New Module**
- Select the **AMP for Endpoints** module and click **Add New Module**
- Name the module
- Select the AMP Cloud
- The API Credentials gathered previously are entered under **3rd Party API Client ID** and **API Key**

Add New AMP for Endpoints Module

Module Name*

URL*

3rd Party API Client ID*

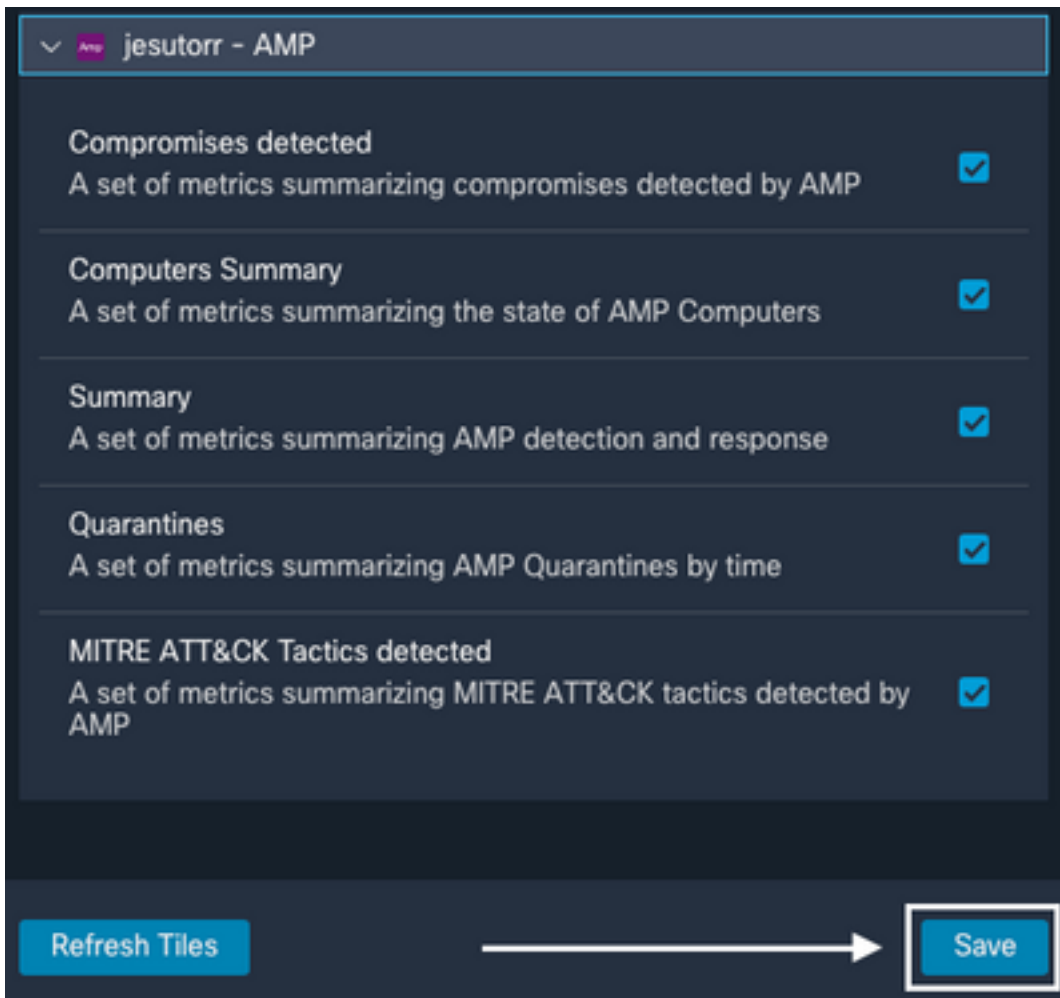
API Key*

Act in the name of Active User ?

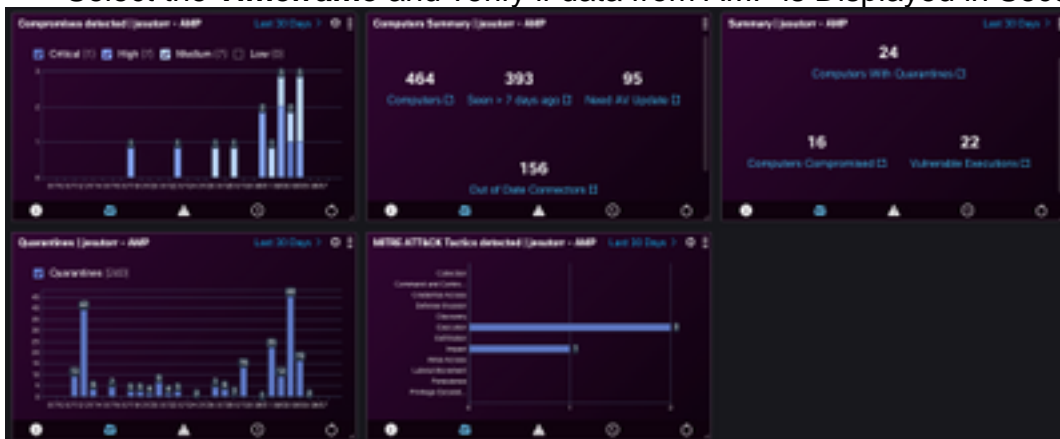
Verify

Validate that the information from the AMP Console is displayed in the SecureX Dashboard.

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



- Select the **Timeframe** and verify if data from AMP is Displayed in SecureX



Troubleshoot

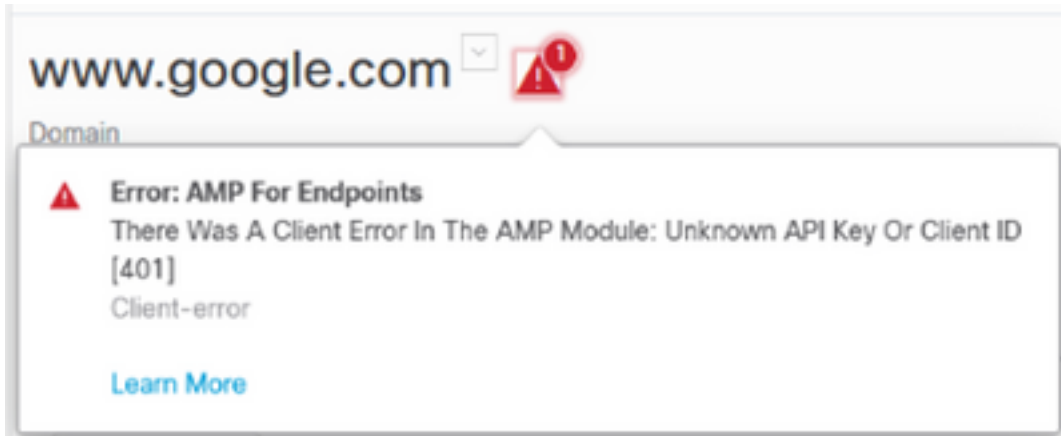
API Client Does Not Have Write Access [403]

The SecureX - AMP for Endpoints Integration requires **Read & Write** AMP for Endpoints APIs, if not, an error message is displayed as shown in the image.



Error: Unknown API Key Or Client ID [401]

If the APIs are not valid if an investigation is performed in SecureX Threat Response as shown in the image.



Verify the API credentials are valid or exist in the AMP Console, if not, try with new ones.

If after you review the information above you are still have issues, please contact Support.

Video Guide