Secure X with Stealthwatch Enterprise Integration Guide

Contents

Introduction

This document describes the steps to perform the Stealthwatch Enterprise integration with Secure X.

Contributed by Jesus Javier Martinez, Edited by Jorge Navarrete, Cisco TAC Engineers.

Prerequisites

Requirements

Stealthwatch Management Console (SMC) v7.2.1 or later.

Your Stealthwatch deployment generates security events and Alarms as expected.

Your SMC must be able to connect outbound to the Cisco clouds:

- North America clouds:
  api-sse.cisco.com, port 443
  visibility.amp.cisco.com, port 443
- EU clouds :
  api.eu.sse.itd.cisco.com, port 443
  visibility.eu.amp.cisco.com, port 443
- Asia (APJC) clouds:
  api.eu.sse.itd.cisco.com, port 443
  visibility.apjc.amp.cisco.com, port 443

You have an account to access SecureX. In order to use SecureX and associated tools, you must have an account on the regional cloud you use:

- Cisco Security Account
- AMP for Endpoints account
- Cisco Threat Grid account

Note: If you or your organization already has any of the above accounts on the regional cloud you use, use the existing account. Do not create a new account.

Components Used

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

- Cisco Security Services Exchange (SSE) console
- Stealthwatch Management Console (SMC)
- Secure X console

Note: The account in every console must have Administrator rights in order to perform the integration.

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 SecureX is the platform in the Cisco cloud that helps you detect, investigate, analyze, and respond to threats with data aggregated from multiple products and sources. This integration enables you to do this activities in Stealthwatch:

- Use Stealthwatch tiles on the SecureX dashboard to monitor key operational metrics.
- Utilize the SecureX context menu to pivot to your other Cisco Security and third-party integrations.
- Provide access to your SecureX security ribbon.
- Send Stealthwatch Alarms to SecureX.
- Allow SecureX to request Security Events from Stealthwatch to enrich the investigation context in Threat Response workflows.

Configure

Configure the SecureX Integration

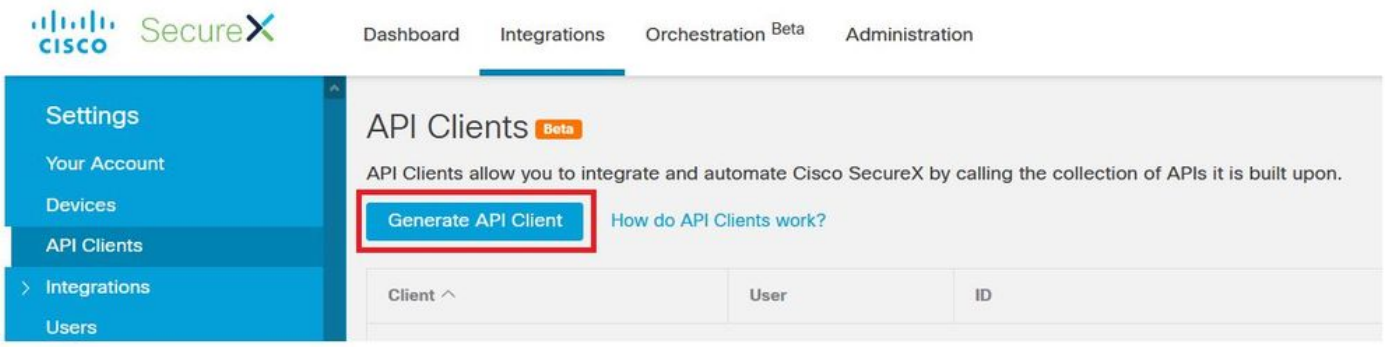
Step 1. Log into the SecureX portal. Navigate via a web browser to your regional SecureX cloud:

- North America cloud: securex.us.security.cisco.com
- Europe cloud: securex.eu.security.cisco.com
- Asia (APJC)cloud: securex.apjc.security.cisco.com

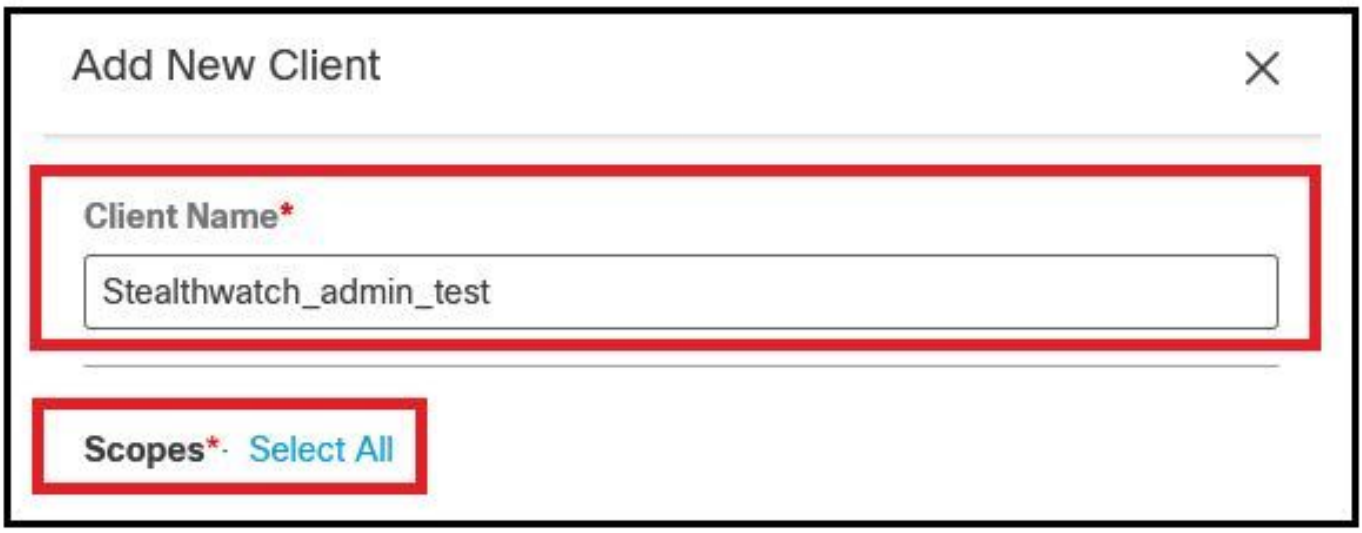
Step 2. Sign in with the credentials for your AMP for Endpoints, Cisco Threat Grid, or Cisco Security account.

Step 3. Navigate to the Integrations tab and then select API Clients under the Settings menu.

Step 4. Select Generate API Client, as shown in the image.



Step 5. Enter the name and description for the API Client and select **All** scopes, as shown in the image.
The scopes cannot be changed after the API Client has been generated.



Step 6. Select Add New Client, as shown in the image.