

Verify the Support Scope for SecureX

Contents

[Introduction](#)

[Background](#)

[Entitlement](#)

[SecureX Single Sign-On](#)

[Dashboard, Tiles, and Threat Response Investigation Issues](#)

[Cisco Security Products Integrations Issues](#)

[3rd-Party Integration Issues](#)

[APIs and Custom Scripts](#)

Introduction

This document describes the support scope from different Cisco Organizations for SecureX.

Background

The intention of the document is to provide clarification and clear expectations on the different types of services and support that Cisco has around SecureX.

Entitlement

Anyone with an active contract for any Cisco Security Product is entitled to open a case with TAC for SecureX support. In the you can find the information used by the Entitlement Team to validate and open cases with TAC, under the SecureX section you can find this message:

The customer is entitled if a contract covers any of the security solutions integrated into SecureX, like AMP for Endpoints, Cisco Umbrella, Email Security, Web Security, Stealthwatch, DUO, Tetration, Meraki, and ThreatGRID. For Umbrella, DUO, and Meraki that do not operate within CSOne, if the customer is not having any other integrated products with entitlement, choose "SecureX" as a bypass option.

SecureX Single Sign-On

Cisco TAC fully supports any issue related to SecureX Single Sign-On, login, or account management. For any request related to integrate a 3rd party IdP (Identity Provider), please use this guide:

[Cisco SecureX Sign-On Third-Party Identity Provider Integration Guide](#)

To create a METADATA file, use these instructions:

[How do we download the IDP.XML metadata file from a SAML Template App?](#)

Dashboard, Tiles, and Threat Response Investigation Issues

Cisco TAC fully supports any issues related to dashboard and tile creation, data population, and module integration on the SecureX Console. For Threat Response Investigations, Cisco TAC can help you to understand or clarify any query about the investigations performed with the Products Integrated, as well as to assist on any issue, error, or warning that can be part of the investigation.

Cisco Security Products Integrations Issues

Cisco TAC delivers full support on issues related to Cisco Security Products integrated into SecureX. This applies to both On-Prem Devices with indirect integration to SecureX (Security Services Exchange (SSE) and Cisco Security Services Proxy (CSSP) server) or any direct (Cloud-To-Cloud) integration for a Cisco Security Product.

3rd-Party Integration Issues

For 3rd-party integration issues, the support scope from Cisco TAC is to confirm that the APIs needed for the integration are properly configured with all the parameters and requirements specified in the [SecureX Integration Modules](#) documentation.

If after the API parameters and requirements are validated the issues persist, support from the 3rd-Party product needs to be engaged to work with TAC on the issue.

APIs and Custom Scripts

Cisco TAC supports that any documented API works appropriately; however, TAC does not support the custom usage that users apply to them, such as the use of API in a Python script.

For custom requests, please contact your Cisco Account Manager to get information on the subscription services available with the Cisco Professional Services Team (PS).

If you have any questions on the TAC Scope support for SecureX, please send an email to ats-cxtls@cisco.com.