

# 驗證SecureX的支援範圍

## 目錄

[簡介](#)

[背景](#)

[權利](#)

[SecureX單點登入](#)

[控制面板、磁貼和威脅響應調查問題](#)

[思科安全產品整合問題](#)

[第三方整合問題](#)

[API和自定義指令碼](#)

## 簡介

本文檔介紹不同思科組織的SecureX支援範圍。

## 背景

本文檔旨在對思科圍繞SecureX提供的不同型別的服務和支援提供說明和明確的期望。

## 權利

與任何思科安全產品具有有效合約的任何人都有權使用TAC就SecureX支援建立案例。在中，您可以找到權利團隊用於通過TAC驗證和提交案例的資訊，在SecureX部分下可以找到以下消息：

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單點登入

Cisco TAC完全支援任何與SecureX單點登入、登入或帳戶管理相關的問題。有關整合第三方IdP（身份提供程式）的任何請求，請使用以下指南：

[Cisco SecureX登入第三方身份提供商整合指南](#)

要建立後設資料檔案，請使用以下說明：

[如何從SAML模板應用下載IDP.XML後設資料檔案？](#)

## 控制面板、磁貼和威脅響應調查問題

Cisco TAC完全支援與SecureX控制檯上的控制面板和磁貼建立、資料填充和模組整合相關的任何

問題。對於Threat Response Investigations，Cisco TAC可以幫助您瞭解或澄清有關使用整合產品執行的調查的任何查詢，以及協助解決調查中可能涉及的任何問題、錯誤或警告。

## 思科安全產品整合問題

思科TAC針對整合到SecureX中的思科安全產品相關問題提供全面支援。這適用於間接整合到SecureX(安全服務交換(SSE)和思科安全服務代理(CSSP)伺服器)或任何直接(雲到雲)整合的內部裝置，適用於思科安全產品。

## 第三方整合問題

對於第三方整合問題，思科TAC的支援範圍是確認整合所需的API已正確配置並符合[SecureX整合模組文檔中指定的所有引數和要求](#)。

如果API引數和要求通過驗證後問題依然存在，則需要聯絡第三方產品的支援以與TAC解決此問題。

## API和自定義指令碼

Cisco TAC支援任何檔案化的API都能正確運作；但是，TAC不支援使用者對其應用的自定義用法，例如在Python指令碼中使用API。

對於自定義請求，請聯絡您的思科客戶經理，獲取有關思科專業服務團隊(PS)提供訂閱服務。

如果您對SecureX的TAC範圍支援有任何疑問，請傳送電子郵件至 [ats-cxtls@cisco.com](mailto:ats-cxtls@cisco.com)。