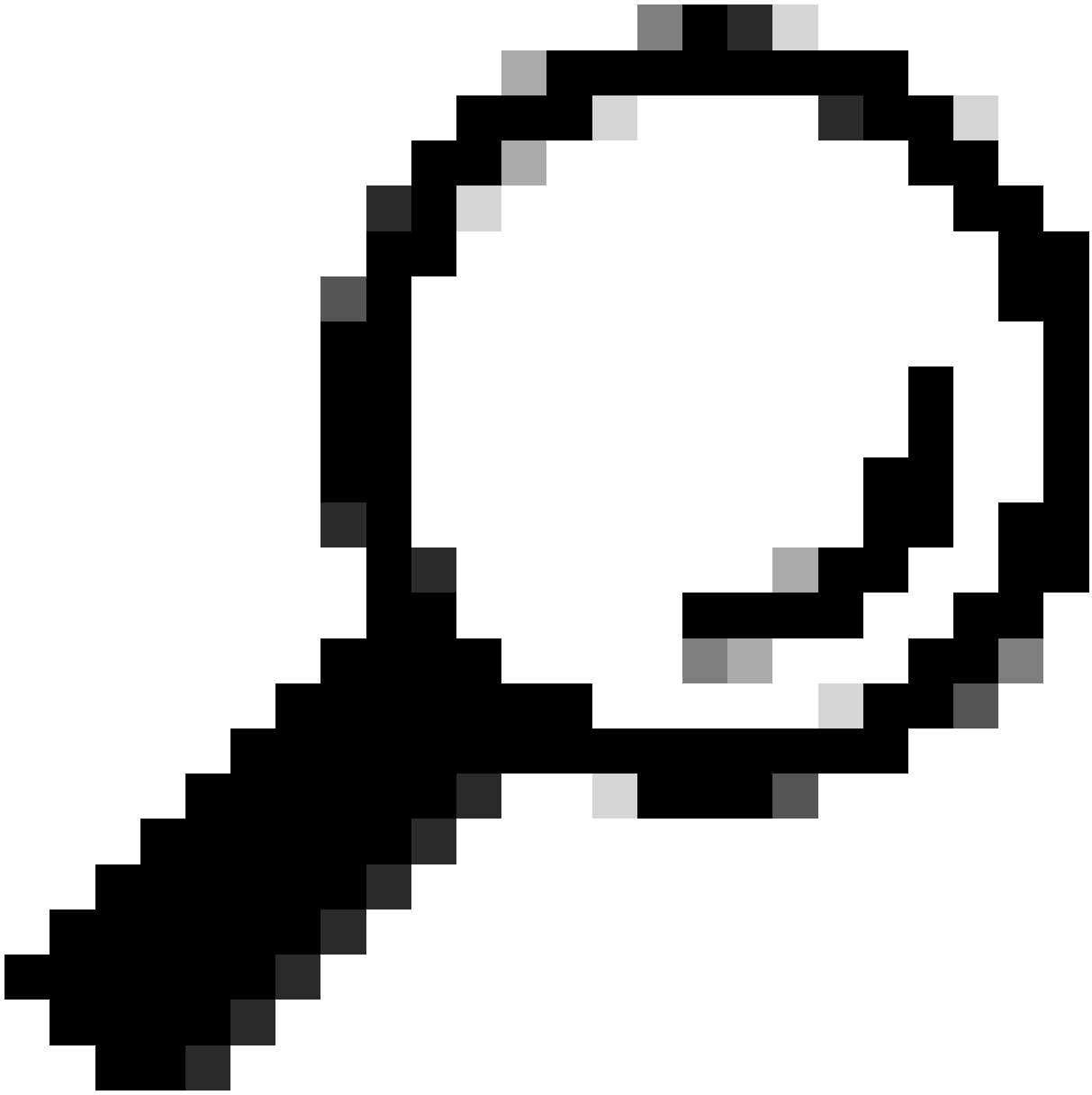
安全網路分析瞭解外部連線指南

目錄

簡介

使用此指南檢視某些安全網路分析功能快速運行所需的外部連線。 這些外部連線可以是域或端點。 域是用來標識網際網路上的資源的名稱，通常是網站或服務；和終端是指通過網路進行通訊的實際裝置或節點。由於本指南的重點是Web服務，因此這些服務將顯示為URL。 該表按字母順序列出外部連線URL。



提示：該表按字母順序列出外部連線URL。

外部連線

外部連線Url	目的
https://analytics.int.obsrvbl.com	由安全網路分析使用Secure Cloud Analytics服務進行遙測資料交換。
https://api.apj.sse.itd.cisco.com	在亞太地區、日本和中國地區

	(APJC)將資料傳輸到Amazon Web Services(AWS)時需要思科提供。在將警報轉發到Cisco XDR時使用，也用於客戶服務指標。
https://api.eu.sse.itd.cisco.com	歐洲(EU)區域的資料傳輸至Amazon Web Services(AWS)時需要思科提供的服務。在將警報轉發到Cisco XDR時使用，也用於客戶服務指標。
https://api-sse.cisco.com	美國(US)地區的資料傳輸至Amazon Web Services(AWS)時需要思科提供。在將警報轉發到Cisco XDR時使用，也用於客戶服務/成功指標。
https://apix.cisco.com	由Secure Network Analytics用於直接軟體下載功能。
https://dex.sse.itd.cisco.com	傳送和收集客戶成功指標時必需
https://est.sco.cisco.com	傳送和收集客戶成功指標時必需
https://eventing-ingest.sse.itd.cisco.com	傳送和收集客戶成功指標時必需
https://feodotracker.abuse.ch/downloads/ipblocklist.txt	Threat Feed（用於安全網路分析警報和觀察）需要（啟用Analytics時）。
https://id.cisco.com	由Secure Network

	Analytics用於直接軟體下載功能。
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz	Threat Feed（用於安全網路分析警報和觀察）需要（啟用Analytics時）。
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz	Threat Feed（用於安全網路分析警報和觀察）需要（啟用Analytics時）。
https://lancope.flexnetoperations.com/control/lncp/LancopeDownload	安全網路分析威脅情報源（用於安全網路分析警報和安全事件）所必需。這需要安全網路分析威脅情報源許可證。
https://mx*.sse.itd.cisco.com	傳送和收集客戶成功指標時必需
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json	允許在啟用分析時訪問警報的MITER資訊。
https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json	允許在啟用分析時訪問警報的MITER資訊。
https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	允許在啟用分析時訪問警報的MITER資訊。
https://s3.amazonaws.com/onconfig/global-blacklist	啟用「分析」後，用於安全網路分析警報和觀察的必需威脅源。
https://sensor.anz-prod.obsrvbl.com	在亞太地區、日本和中國地區(APJC)將資料傳輸到Amazon Web Services(AWS)時需要思科提供。在將警報轉發到Cisco XDR時使用，也用於客戶

	服務指標。
https://sensor.eu-prod.obsrvbl.com	歐洲(EU)區域的資料傳輸至Amazon Web Services(AWS)時需要思科提供的服務。在將警報轉發到Cisco XDR時使用，也用於客戶服務指標。
https://sensor.ext.obsrvbl.com	美國(US)地區的資料傳輸至Amazon Web Services(AWS)時需要思科提供。在將警報轉發到Cisco XDR時使用，也用於客戶服務指標。
smartreceiver.cisco.com	用於訪問思科智慧軟體許可。有關詳細資訊，請參閱《智慧許可指南》。如有需要，還可以使用其他離線許可。有關詳細資訊，請參閱發行說明。
https://software.cisco.com	由Secure Network Analytics用於直接軟體下載功能。
https://www.cisco.com	思科域必需，用於智慧許可、雲代理和防火牆連線測試。

其他資訊

要進一步評估如何使用特定域和終端連線及其原因，請參閱以下主題：

- 思科安全服務交換(SSE)
- 直接軟體下載(Beta)
- MITER ATT&CK®框架
- 威脅源

思科安全服務交換(SSE)

SSE終端用於資料傳輸至Amazon Web Services(AWS)，由思科用於客戶服務指標，還用於在將警報轉發至Cisco XDR時使用。這些視情況而定
基於區域和主機。使用SSE聯結器提供的服務發現機制動態發現這些端點。將檢測發佈到Cisco XDR時，Secure Network Analytics會嘗試發現名為「xdr-data-platform」的服務及其API終結點「Events」。

區域和主機

根據生產環境中的區域，主機如下所示。

美國：

- https://api-sse.cisco.com
- https://sensor.ext.obsrvbl.com

歐盟：

- https://api.eu.sse.itd.cisco.com
- https://sensor.eu-prod.obsrvbl.com

亞太地區、日本及中國：

- https://api.apj.sse.itd.cisco.com
- https://sensor.anz-prod.obsrvbl.com

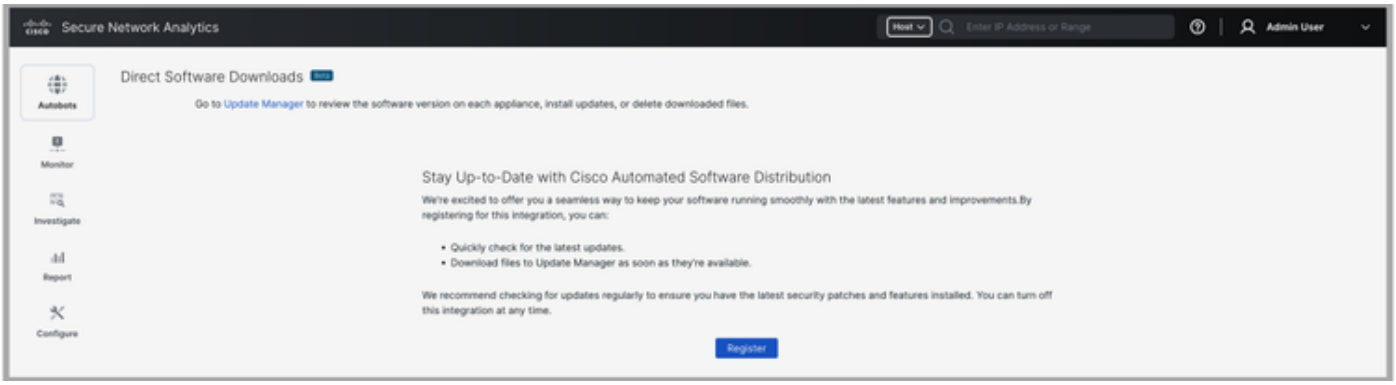
直接軟體下載(Beta)

直接軟體下載功能使用以下連線：

- https://apix.cisco.com
- https://software.cisco.com
- https://id.cisco.com

要使用此新功能將軟體和修補程式更新檔案直接下載到Update Manager，請確保已使用cisco.com使用者ID(CCOID)進行註冊。
1.登入到Manager。
2.從主選單中選擇「配置」>「全域性」>「集中管理」。
3.按一下Update Manager選項卡。
4.按一下Direct Software Downloads連結開啟註冊頁面。

5.按一下Register按鈕開始註冊過程。

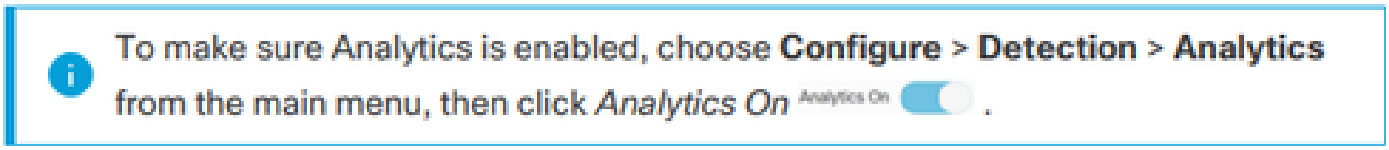


6.按一下提供的連結。
7.您將進入「啟用裝置」頁面。按一下下一步繼續。
8.使用您的cisco.com使用者ID(CCOID)登入。
9.啟用完成後，您將收到「裝置已啟用」消息。
10.返回Manager上的Direct Software Downloads頁面，然後按一下Continue。
11.按一下EULA和K9協定的連結閱讀並接受條款。接受條款後，按一下Continue。

如需直接軟體下載的詳細資訊，請聯絡思科支援人員

MITER ATT&CK®框架

MITER ATT&CK® Framework是一個基於真實世界觀測的公開的對手戰術和技術的知識庫。當您啟用了Secure Network Analytics中的Analytics後，MITER策略和技術可協助進行網路安全威脅情報、檢測和響應。



以下連線允許Secure Network Analytics訪問MITER資訊
對於警報：

- https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
- https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobileattack.json
- https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterpriseattack.json

威脅源

Cisco Secure Network Analytics Threat Feed（前身為Stealthwatch Threat Intelligence Feed）提供來自全球威脅源的有關網路威脅的資料。源經常更新，包括IP地址、埠號、協定、主機名以及已知用於惡意活動的URL。源中包含以下主機組：命令和控制伺服器、茂物和Tors。

要在集中管理中啟用威脅源，請按照幫助中的說明操作。

1.登入到您的主Manager。
2.選擇Configure > Global > Central Management。
3.按一下（「幫助」）圖示。選擇Help。
4.選擇Appliance Configuration > Threat Feed。

Please note that you will configure the DNS server and firewall as part of the instructions. Also, if you have a failover configuration, you need to enable Threat Feed on your primary Manager and secondary Manager.

有關威脅源的詳細資訊，請參閱系統配置指南。

聯絡支援人員

如果您需要技術支援，請執行以下操作之一：

- 聯絡您當地的思科合作夥伴
- 聯絡思科支援
- 要通過Web建立案例，請執行以下操作：http://www.cisco.com/c/en/us/support/index.html
- 如需電話支援：1-800-553-2447（美國）
- 對於全球支援號碼：https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。