配置安全惡意軟體分析（前身為Threat Grid）與Umbrella的整合

目錄

簡介

本文說明如何將Secure Malware Analytics（前身為Threat Grid）與Umbrella整合。

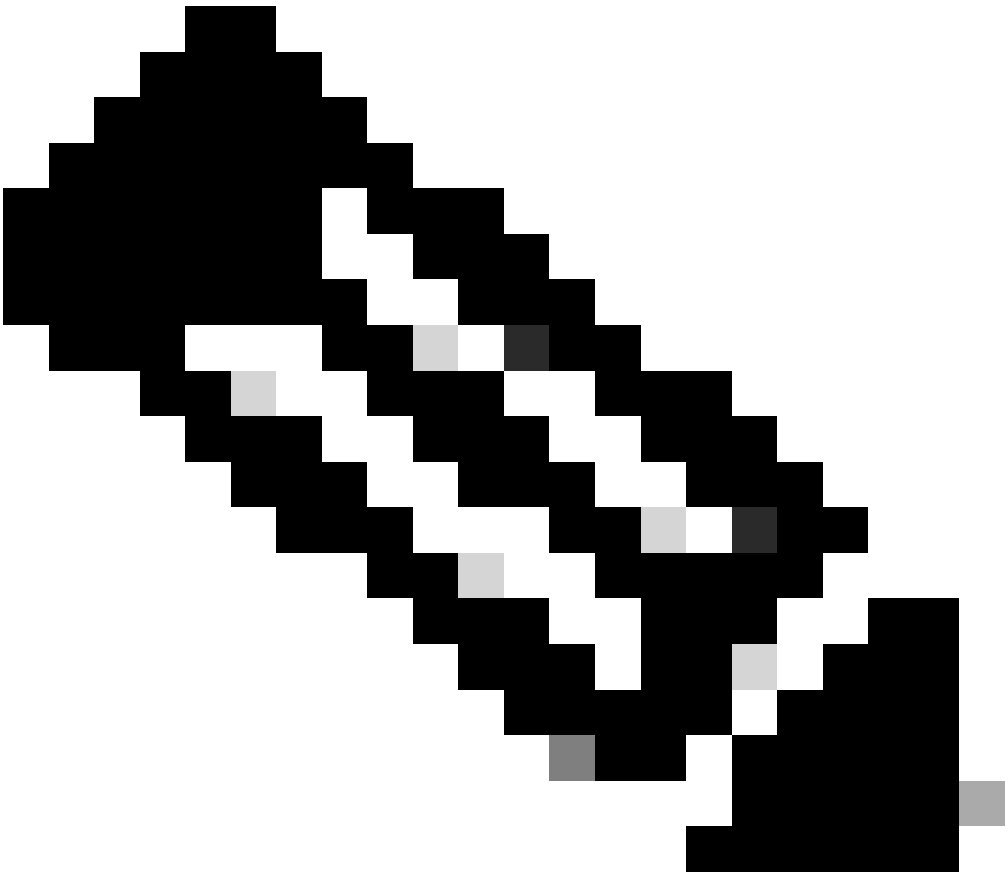
適用於Cisco Umbrella的Cisco Secure Malware Analytics(Threat Grid)整合概述

通過Cisco Secure Malware Analytics（前身為Threat Grid）與Cisco Umbrella之間的集成，安全團隊現在能夠擴展其可視性，針對漫遊筆記型電腦、平板電腦或電話的當今高級威脅實施保護，同時為分散式企業網路提供另一層實施層。

本指南概述如何配置思科安全惡意軟體分析(Threat Grid)以與Cisco Umbrella通訊，以便可以將思科安全惡意軟體分析(Threat Grid)生成的威脅情報自動整合到可以保護思科安全惡意軟體分析(Threat Grid)下的客戶端的策略中。

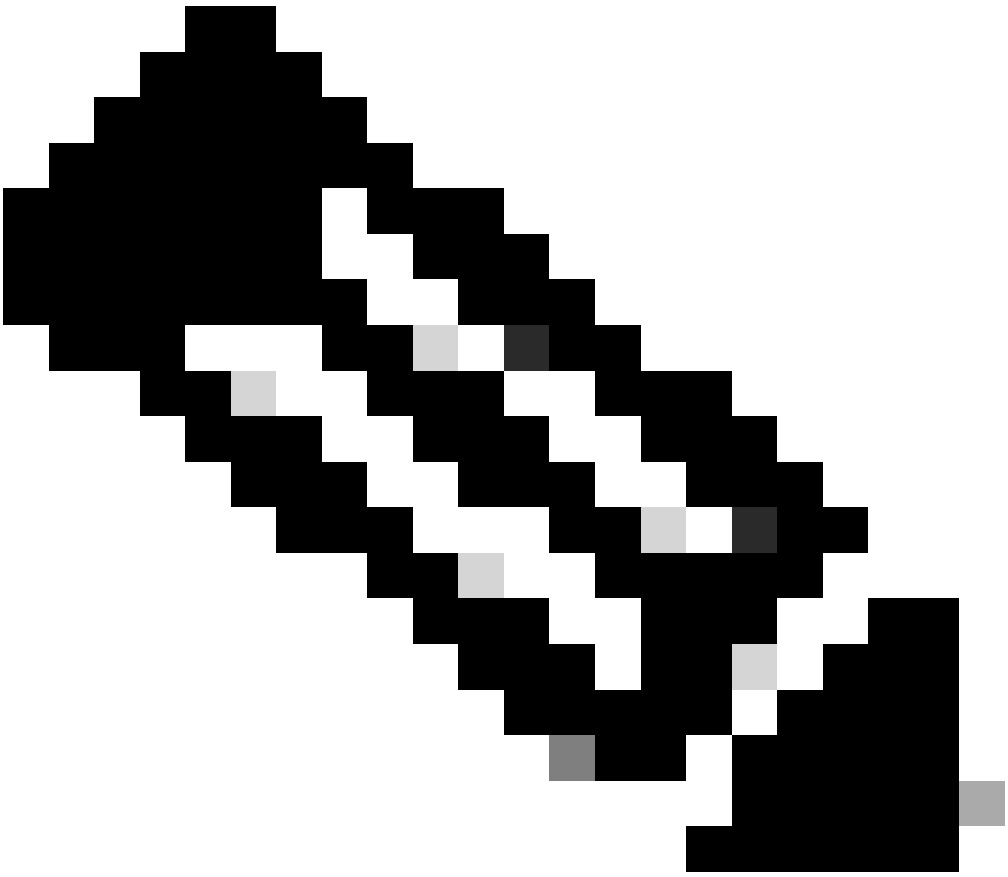
必要條件

- 功能強大的思科安全惡意軟體分析(Threat Grid)控制面板，可訪問您帳戶的API金鑰。



附註：目前不支援思科安全惡意軟體分析(Threat Grid)裝置和終端。

- Cisco Umbrella Dashboard管理許可權。
- Cisco Umbrella控制面板必須啟用Cisco Secure Malware Analytics(Threat Grid)整合。



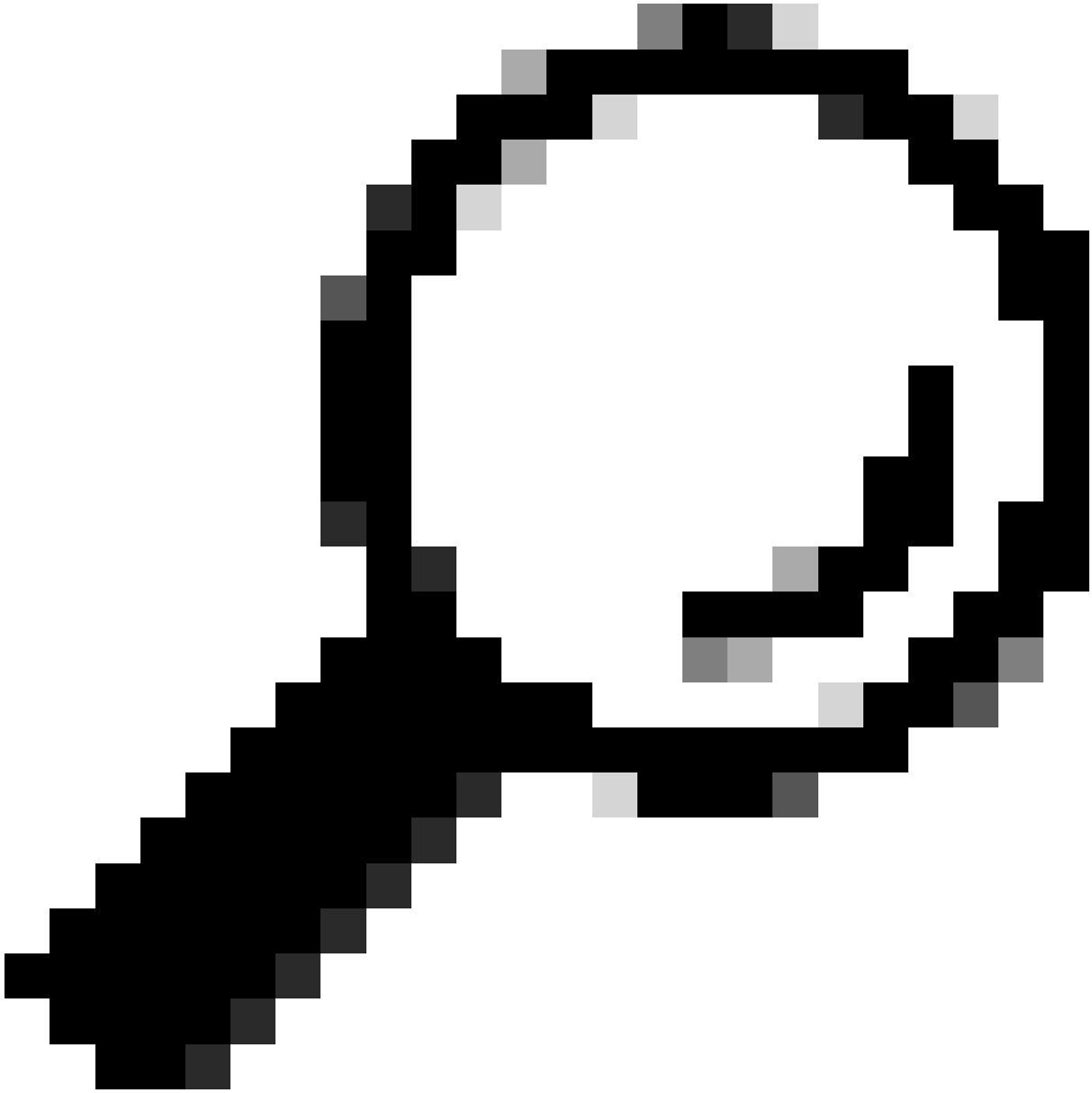
附註：Cisco Secure Malware Analytics(Threat Grid)整合僅包含在Cisco Umbrella軟體包中，如DNS Essentials、DNS Advantage、SIG Essentials或SIG Advantage。如果您沒有Cisco Umbrella軟體包並希望進行此整合，請聯絡您的Cisco Umbrella客戶經理。如果您有Cisco Umbrella包，但看不到思科安全惡意軟體分析(Threat Grid)作為控制面板整合，請與Cisco Umbrella支援聯絡。

此整合如何工作？

Cisco Umbrella會接觸思科安全惡意軟體分析(Threat Grid)API，並檢索通過分析惡意樣本生成的域清單。然後Cisco Umbrella通過Cisco Umbrella Enforcement API匯入此清單。此方法不同於其他整合在Cisco Umbrella中的運作方式，Cisco Umbrella通過向Cisco安全惡意軟體分析(Threat Grid)API進行API查詢，而不是接受來自將威脅情報推送到Cisco Umbrella服務的其他系統的事件，來引入威脅情報。

然後，Cisco Umbrella會驗證威脅，以確保將其新增到您的策略中。如果確認來自思科安全惡意軟體分析(Threat Grid)的資訊是威脅或不是已知正常域，則域地址會作為可應用於任何思科Umbrella策略的安全設定的一部分新增到思科安全惡意軟體分析(Threat Grid)目標清單。該策略會立即應用於使用思科安全惡意軟體分析(Threat Grid)整合策略從裝置發出的任何請求。

Cisco Umbrella從思科安全惡意軟體分析(Threat Grid)獲取兩個獨立的源：公共（全域性）源和僅客戶（專用，特定於單個客戶）源。



提示：雖然Cisco Umbrella會儘量驗證和允許已知安全域（例如Google和Salesforce），以避免任何不需要的中斷，我們建議您根據您的策略將您從未希望阻止的任何域新增到全域性允許清單或其他目標清單中。

示例包括：

- 您組織的首頁。
- 表示您提供的服務的域可能同時具有內部和外部記錄。例如，「mail.myservicedomain.com」和「portal.myotherservicedomain.com」。
- 您嚴重依賴於Cisco Umbrella可能不知道或在其自動域驗證中包含的知名度較低的雲應用。例如，「localcloudservice.com」。

這些域必須新增到Global Allow List中，該清單位於Cisco Umbrella中的Policies > Destination Lists下。

配置Cisco Umbrella Dashboard以從思科安全惡意軟體分析(Threat Grid)獲取資訊

第一步是在Cisco Secure Malware Analytics(Threat Grid)控制面板中查詢或生成API金鑰：

1. 登入您的Cisco Secure Malware Analytics(Threat Grid)控制面板並選擇您的帳戶詳細資訊。
2. 在Account Details下，如果您已經建立了API金鑰，則可能已經可見API金鑰。如果沒有，請選擇「生成新API金鑰」。

   然後，您的API金鑰在User Details > API Key下可見。

接下來，將API金鑰新增到Cisco Umbrella Dashboard中，使其從思科安全惡意軟體分析(Threat Grid)提取資料：

1. 以管理員身份登入您的Cisco Umbrella控制面板。
2. 導航到Policies > Policy Components > Integrations，然後在表格中選擇「Cisco AMP Threat Grid」(思科安全惡意軟體分析(Threat Grid))以展開該工具。
3. 選擇Enable，將API金鑰貼上到API金鑰框中，然後選擇Save。

此時，如果您收到錯誤，您的API金鑰或服務之間的通訊可能存在問題。請檢查您的API金鑰並重試，如果仍然失敗，請聯絡Cisco Umbrella支援。

如果您收到成功消息，則表明Cisco Umbrella服務能夠使用API金鑰建立與Cisco Secure Malware Analytics(Threat Grid)API的初始連線。Cisco Umbrella服務使用五分鐘的輪詢間隔從思科安全惡意軟體分析(Threat Grid)檢索資料。

即使在5分鐘間隔之後，如果Cisco Umbrella Dashboard沒有可用的有效資料或有效威脅事件，資訊也可能不會顯示。當首次啟用整合時，對於全域性訂閱源和僅組織訂閱源，它只需返回五分鐘即可；首次獲取資料的時間是在接下來的五分鐘間隔內，因此資料可能不會立即顯示。

如果思科安全惡意軟體分析(Threat Grid)端的API金鑰被停用或刪除，則整合將被禁用。要恢復整合，必須在Cisco Umbrella Dashboard中提供新的API金鑰。如果Cisco Umbrella和Cisco Secure Malware Analytics(Threat Grid)之間發生超時或內部服務錯誤，則會引發不同型別的異常，並且不會禁用整合，而是像正常情況下一樣，每五分鐘嘗試一次連線。

技術詳細資料

從思科安全惡意軟體分析(Threat Grid)獲取資訊所用的精確API查詢如下所示。請注意，僅收集嚴重性大於90、置信度大於90且型別為Domains的事件。此示例中的時間是一個五分鐘範圍，該範圍在下一個查詢中會遞增。Cisco Umbrella中提供的`api_key`用於代替`<key>`變量：

- 公共（全域性源）：

hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence

- 僅限客戶（專用饋送）：

hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence

或:

- 公共（全域性源）：

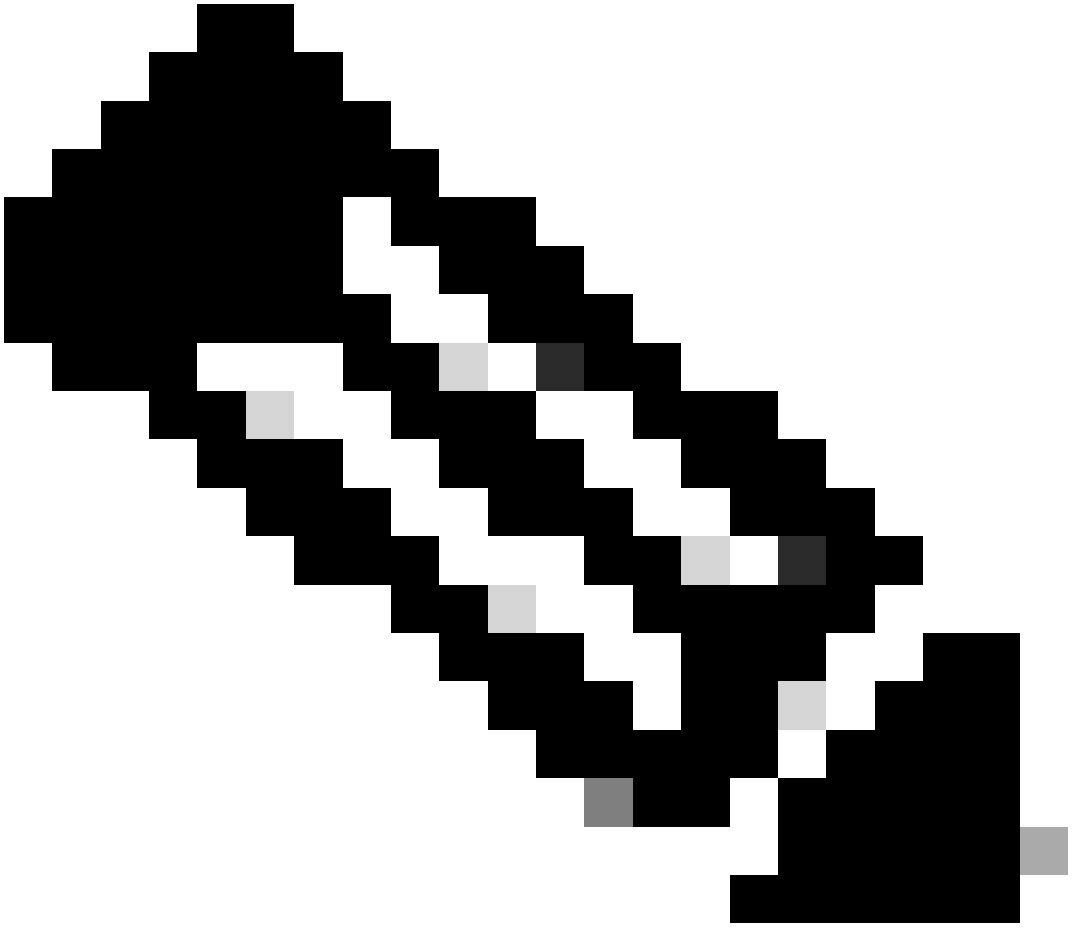
hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence

- 僅限客戶（專用饋送）：

hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence=

在「稽核模式」下觀察新增到思科安全惡意軟體分析(Threat Grid)的事件

隨著時間的推移，Cisco Secure Malware Analytics(Threat Grid)中的事件開始填充一個特定目標清單，該清單可以應用到Cisco Secure Malware Analytics(Threat Grid)類別策略中。預設情況下，目標清單和安全類別處於「稽核模式」，不會應用於任何策略，因此不會導致任何請求被阻止。但是，您可以看到哪些請求與Cisco AMP Threat Grid安全類別關聯（可能已被阻止）。



附註：根據您的部署配置檔案和網路配置，可以根據需要啟用「稽核模式」，甚至可以無限期啟用。

檢視目標清單

您可以隨時檢視思科安全惡意軟體分析(Threat Grid)目標清單。

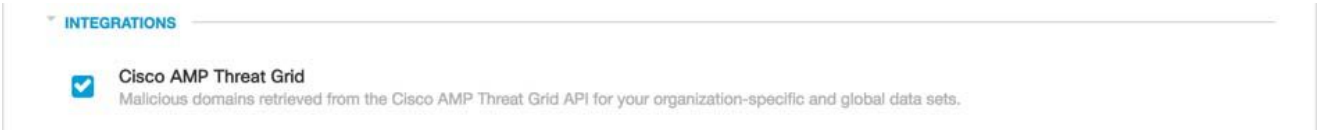
1. 導航到Policies > Policy Components > Integrations。
2. 展開表中的「思科AMP Threat Grid」(思科安全惡意軟體分析(Threat Grid))，然後選擇「檢視域」。

檢視策略的安全設定

您可以檢視可在Cisco Umbrella中隨時為策略啟用的安全設定：

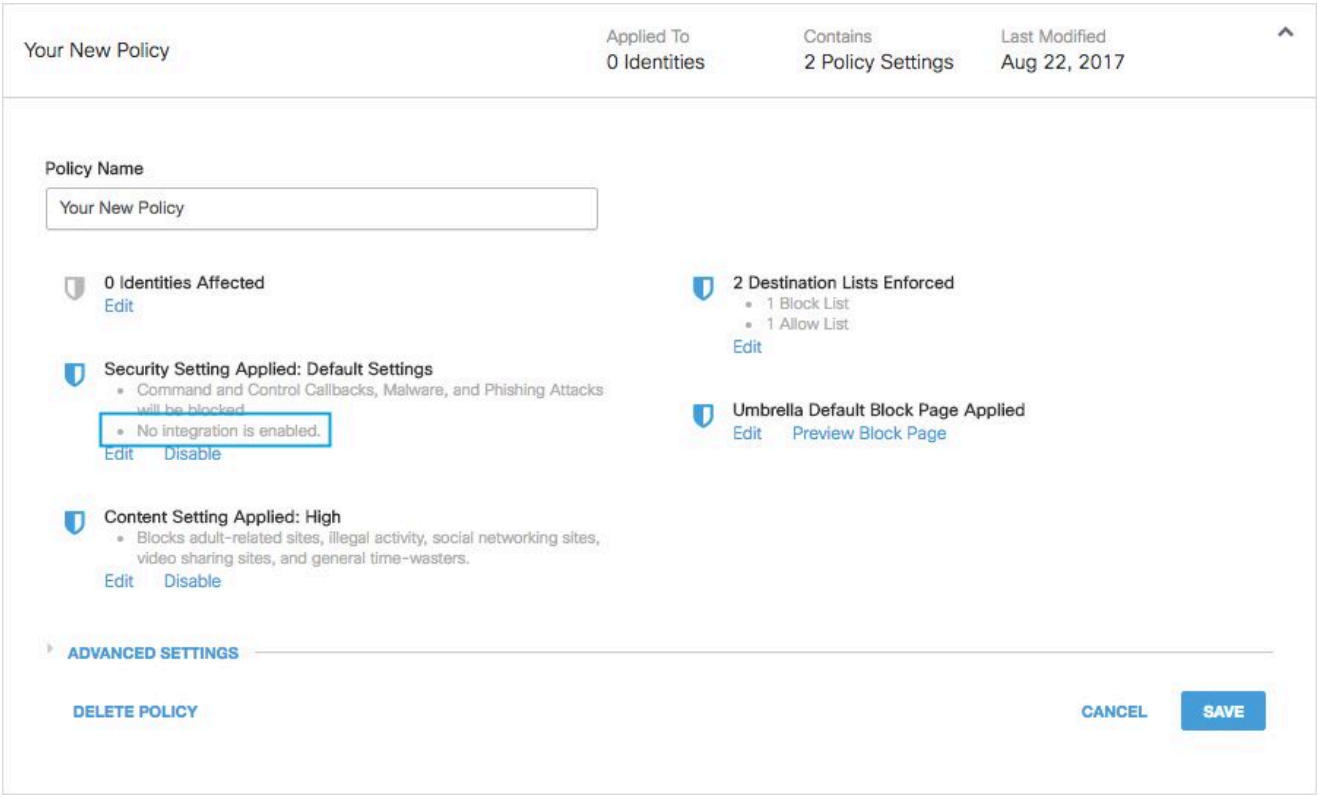
1. 導航到Policies > Policy Components > Security Settings。
2. 按一下表中的安全設定將其展開。

3. 滾動到Integrations部分，展開該部分以顯示思科AMP Threat Grid(思科安全惡意軟體分析(Threat Grid))整合。
4. 選中Cisco AMP Threat Grid整合(思科安全惡意軟體分析(Threat Grid))框，然後選擇Save。

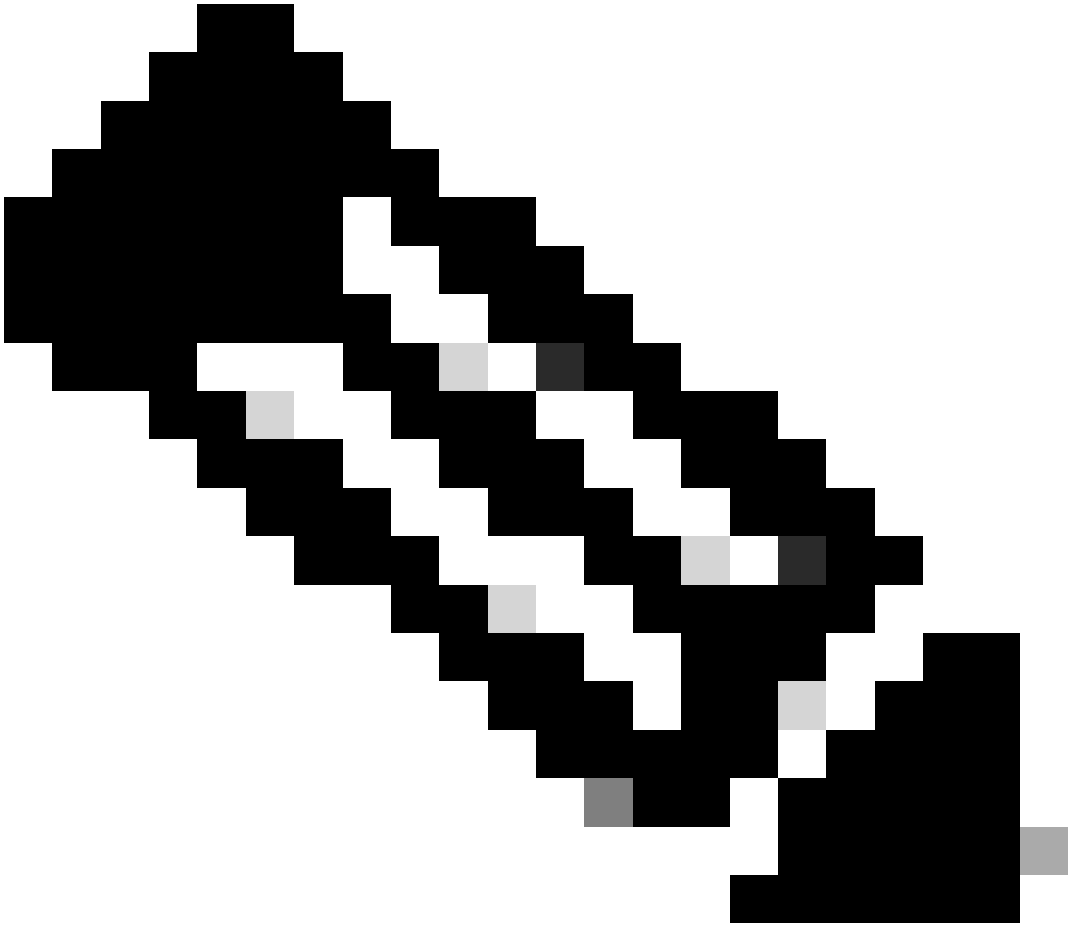


115014151543

您還可以通過「安全設定摘要」頁面檢視整合資訊。



20993269073556

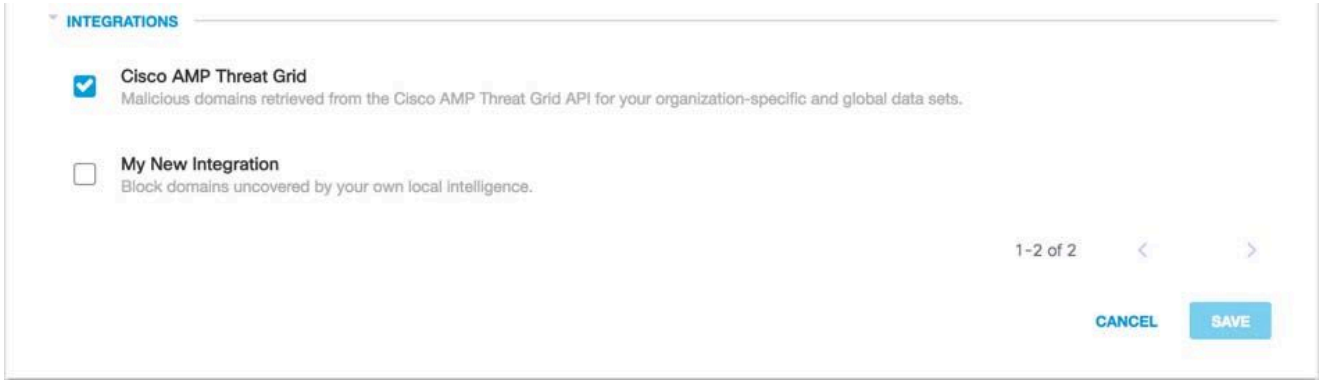


附註：應用設定可能需要最多五分鐘的時間，如果未將新事件注入到思科安全惡意軟體分析(Threat Grid)系統，則您可能看不到正在向整合中新增的新域。

在「阻止模式」下將思科安全惡意軟體分析(Threat Grid)安全設定應用於託管客戶端的策略

一旦準備好阻止這些域用於由Cisco Umbrella管理的客戶端，請更改現有策略的安全設定，或建立一個位於預設策略之上的新策略，以確保首先實施該策略。

1. 導航到Policies > Policy Components > Security Settings。
2. 在Integrations下，驗證「Cisco AMP Threat Grid」框是否已選中。否則，請選中該框並選擇儲存。



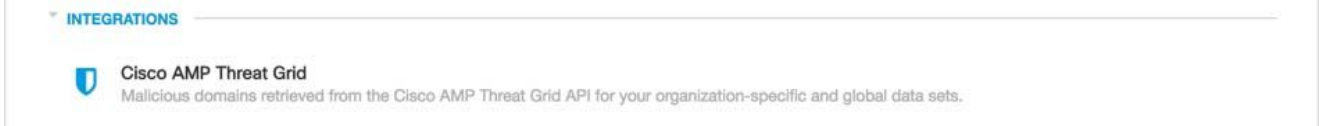
115013987086

接下來，在Cisco Umbrella Policy嚮導中，將安全設定新增到正在編輯的策略中：

1. 導航到Policies > Management > All Policies。
2. 展開策略並在Security Setting Applied下選擇Edit。
3. 在「Security Settings」下拉選單中，選擇包含「Cisco AMP Threat Grid」設定的安全設定。

20993282642708

「整合」(Integrations)下的遮蔽圖示將更新為藍色。



115013987446

4. 選擇Set & Return。

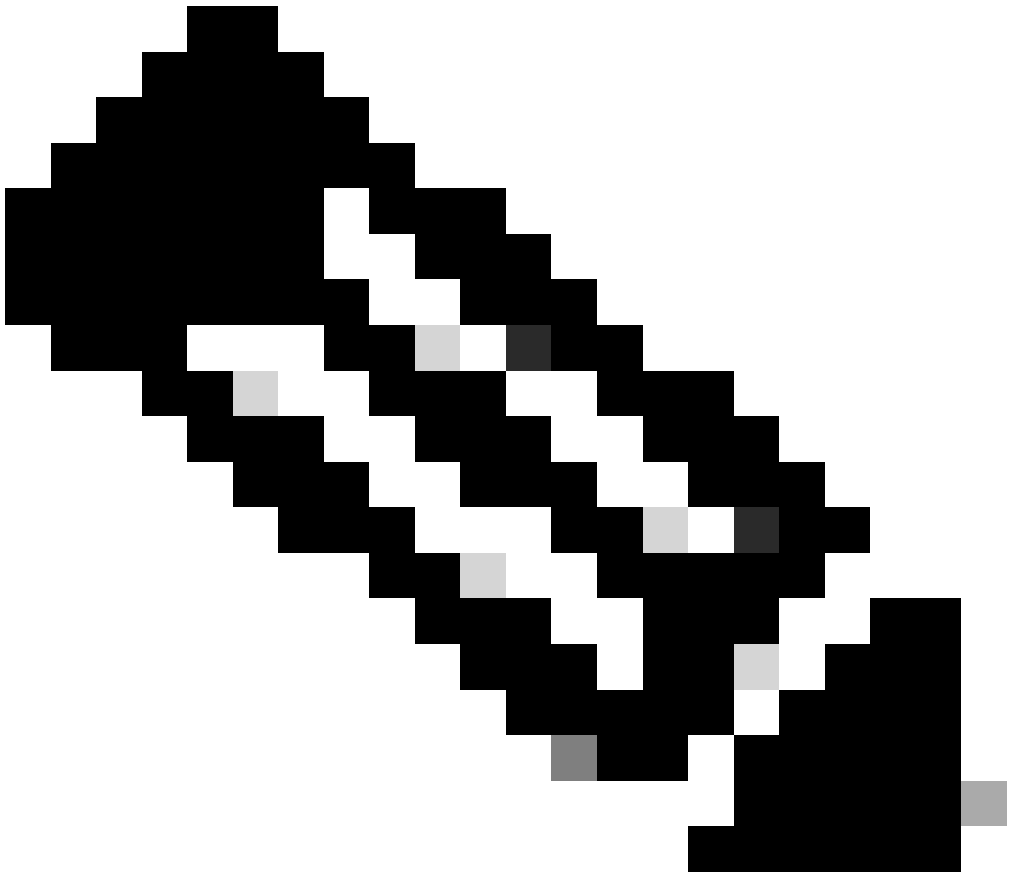
思科安全惡意軟體分析(Threat Grid)的安全設定中包含的思科安全惡意軟體分析(Threat Grid)域會使用策略對這些身份進行阻止。

思科安全惡意軟體分析事件的思科保護傘內報告

思科安全惡意軟體分析(Threat Grid)安全事件報告

Cisco Secure Malware Analytics(Threat Grid)Destination List是您可以報告的安全類別清單之一。大多數或全部報告使用安全類別作為過濾器。例如，您可以篩選安全類別，以便只顯示與思科安全惡意軟體分析(Threat Grid)相關的活動。

1. 導覽至Reporting > Core Reports > Activity Search，然後在Security Categories下選擇「Cisco AMP Threat Grid」(Cisco Secure Malware Analytics(Threat Grid))以篩選報告，使其僅顯示思科安全惡意軟體分析(Threat Grid)的安全類別。



附註：如果Cisco AMP Threat Grid整合被禁用，則不會顯示在「安全類別」篩選器中。

115014210123

2. 選擇Apply。

報告何時將域新增到思科安全惡意軟體分析(Threat Grid)目標清單

Cisco Umbrella Admin Audit日誌包括Cisco Secure Malware Analytics(Threat Grid)控制面板上的事件，因為它將域新增到目標清單。名為「Cisco AMP Threat Grid Domain List」（也標有Cisco徽標）的使用者生成事件。這些事件包括所新增的域以及新增該域的時間。

選擇Admin Audit Log（管理員稽核日誌）條目將展開該條目，顯示詳細資訊，包括新增的特定域。

通過為「Cisco AMP Threat Grid Domain List」使用者應用過濾器，您可以篩選僅包含思科安全惡意軟體分析(Threat Grid)更改。

處理不需要的檢測或誤報

兩種型別的思科安全惡意軟體分析(Threat Grid)檢測和兩種解決方案

目前，有兩種型別的思科安全惡意軟體分析(Threat Grid)塊：一個具有一種可能的解析度，而另一個具有一種當前的解析度，用於不需要的檢測。

1. Global Threat Grid條目（公共）：此時，允許該域的唯一方法是將其新增到您的允許清單中。
2. 僅客戶源（專用）：可以使用允許清單條目或從AMP Threat Grid整合清單中刪除進行定址。

允許清單

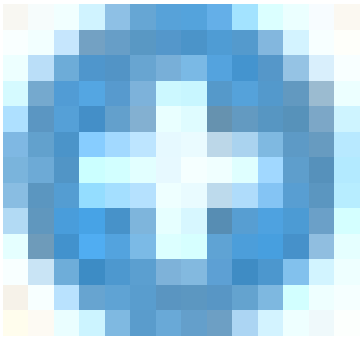
儘管可能性不大，但您的思科安全惡意軟體分析(Threat Grid)整合自動新增的域可能會觸發有害檢測，阻止您的使用者訪問特定網站。在這種情況下，我們建議將網域新增到允許清單(Policies > Destination Lists)中，此清單優先於所有其他型別的封鎖清單（包括安全設定）。

這一方法更受歡迎的原因有兩個。首先，如果Cisco Secure Malware Analytics(Threat Grid)控制面板在刪除域後再次重新新增域，則允許清單可防止出現進一步的問題。其次，允許清單顯示了問題域的歷史記錄，這些域可用於鑑證或審計報告。

預設情況下，全域性允許清單應用於所有策略。將域新增到全域性允許清單會導致在所有策略中允許該域。

如果阻止模式中的Cisco Secure Malware Analytics(Threat Grid)安全設定僅應用於受管Cisco Umbrella標識的子集（例如，它僅應用於漫遊電腦和流動裝置），則可以為這些標識或策略建立特定的允許清單。

要建立允許清單，請執行以下操作：



1. 導航到Policies > Policy Components > Destination Lists，然後選擇

   25463394696852

   （「新增」）。
2. 選擇Allow並將您的域新增到清單中。
3. 選擇Save。

儲存該清單後，可以將其新增到一個現有策略中，該策略將覆蓋那些受到該不需要的阻止影響的客戶端。

從思科安全惡意軟體分析(Threat Grid)目標清單中刪除域

思科安全惡意軟體分析(Threat Grid)清單中的每個域名旁邊都有一個（「刪除」）圖示。通過刪除域，可以在發生意外檢測時清除Cisco Secure Malware Analytics(Threat Grid)目標清單。

如果Cisco Secure Malware Analytics(Threat Grid)控制面板將域重新傳送到Cisco Umbrella，則刪除操作不是永久性的。

1. 導覽至Policies > Policy Components > Integrations，然後選擇「Cisco AMP Threat Grid」(思科安全惡意軟體分析(Threat Grid))以展開它。
2. 選擇See Domains。
3. 搜尋要刪除的域名。
4. 選擇（「刪除」）圖示。
5. 選擇Close。
6. 選擇Save。

如果出現不需要的檢測或誤報，我們建議立即在Cisco Umbrella中建立允許清單，然後在Cisco Secure Malware Analytics(Threat Grid)控制面板中修正誤報。稍後，您可以從Cisco Secure Malware Analytics(Threat Grid)目標清單中刪除該域。

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）。