

繞過安全Web裝置中的身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[免除身份驗證](#)

[在Cisco SWA中免除身份驗證的方法](#)

[繞過身份驗證的步驟](#)

[相關資訊](#)

簡介

本文檔介紹在安全Web裝置(SWA)中免除身份驗證的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- SWA管理。

思科建議您安裝以下工具：

- 物理或虛擬SWA
- 對SWA圖形使用者介面(GUI)的管理訪問

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

免除身份驗證

Cisco SWA中對特定使用者或系統免除身份驗證對於保持運營效率和滿足特定要求至關重要。首先，一些使用者或系統需要不間斷地訪問可能受到身份驗證過程阻礙的關鍵資源或服務。例如，執行定期更新或備份的自動化系統或服務帳戶需要無縫訪問，而不會出現身份驗證機制導致的延遲或潛在故障。

此外，在某些情況下，Web服務提供者建議不要使用Proxy來存取其服務。在這種情況下，免驗證可確保遵守提供商準則並保持服務可靠性。此外，為了有效地阻止某些使用者的流量，通常需要首先免除他們的身份驗證，然後應用適當的阻止策略。此方法允許對訪問許可權進行精確控制。

在某些情況下，所存取的Web服務是受信任且普遍可接受的，例如Microsoft更新。免除此類服務的身份驗證可簡化所有使用者的訪問。此外，在某些情況下，使用者作業系統或應用程式不支援SWA中配置的身份驗證機制，需要旁路以確保連線。

最後，具有固定IP地址的伺服器（沒有使用者登入且訪問受信任Internet有限）不需要身份驗證，因為它們的訪問模式是可預測和安全的。

透過對這些案例從戰略角度免除身份驗證，組織可以在安全需求和運營效率之間取得平衡。

在Cisco SWA中免除身份驗證的方法

SWA中的豁免驗證可透過各種方法實現，每種方法都針對特定的場景和要求量身定製。以下是配置身份驗證豁免的一些常用方法：

- IP地址或子網掩碼：最簡單的方法之一是免除對特定IP地址或整個子網的身份驗證。這對於具有固定IP地址或受信任網段的伺服器特別有用，因為它們需要不間斷地訪問網際網路或內部資源。透過在SWA配置中指定這些IP地址或子網掩碼，您可以確保這些系統繞過身份驗證過程。
- 代理埠：您可以將SWA配置為根據特定代理埠免除流量。當某些應用程式或服務使用指定埠進行通訊時，此功能非常有用。透過標識這些埠，您可以設定SWA以繞過對這些埠上的流量的身份驗證，從而確保相關應用或服務的無縫訪問。
- URL類別：另一種方法是根據URL類別免除身份驗證。這可以包括預定義的思科類別和根據貴公司的特定需求定義的自定義URL類別。例如，如果某些Web服務（例如Microsoft更新）被視為受信任且普遍可接受，您可以將SWA配置為繞過這些特定URL類別的身份驗證。這可確保所有使用者無需身份驗證即可訪問這些服務。
- 使用者代理：基於使用者代理的免除身份驗證在處理不支援已配置的身份驗證機制的特定應用程式或裝置時非常有用。透過辨識這些應用或裝置的使用者代理字串，您可以配置SWA以繞過來自這些應用或裝置的流量的身份驗證，從而確保無縫連線。

繞過身份驗證的步驟

以下是建立免於身份驗證的標識配置檔案的步驟：

步驟 1. 在GUI中，選擇網路安全管理器，然後按一下標識配置檔案。

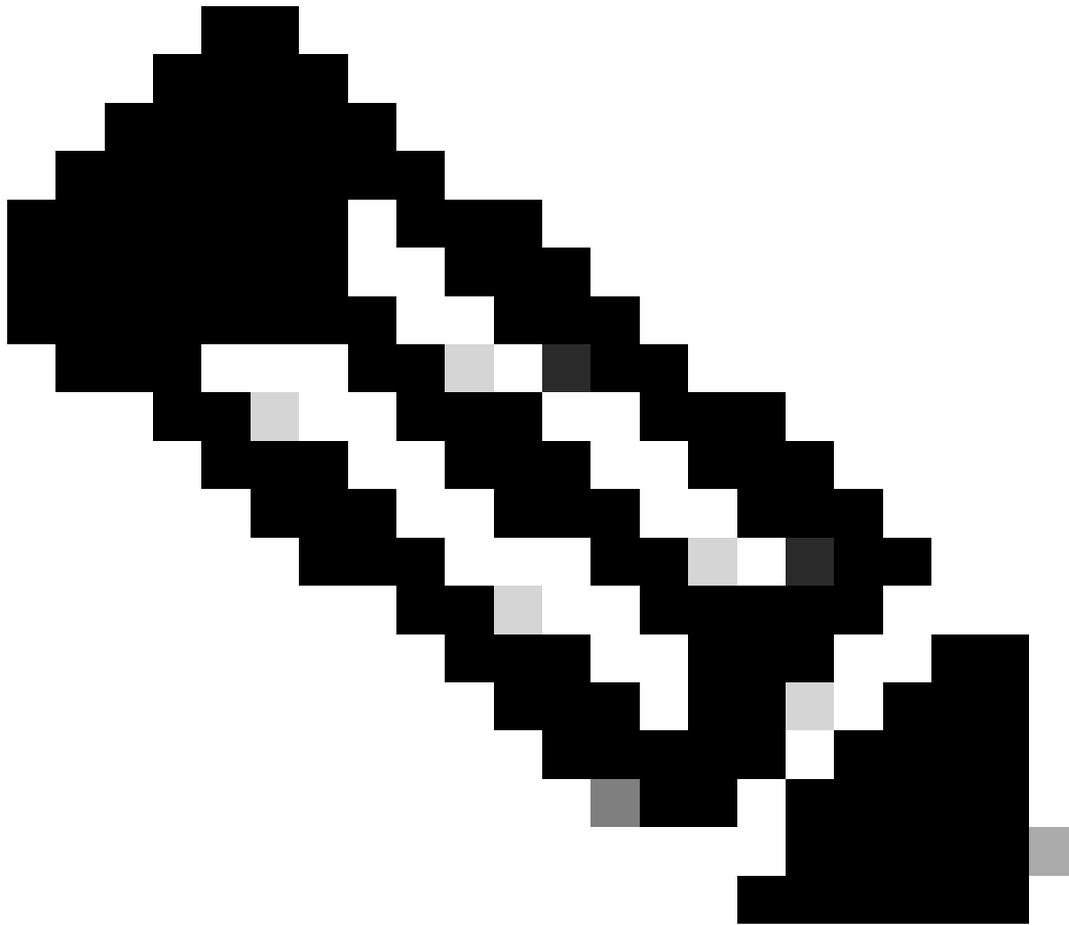
步驟 2. 按一下Add Profile以增加配置檔案。

步驟 3. 使用Enable Identification Profile覈取方塊可啟用此配置檔案，或者快速停用此配置檔案而不刪除它。

步驟 4. 指定唯一的設定檔名稱。

步驟 5. （可選）增加說明。

步驟 6.從「插入」下拉式清單中，選擇此設定檔在表格中的顯示位置。

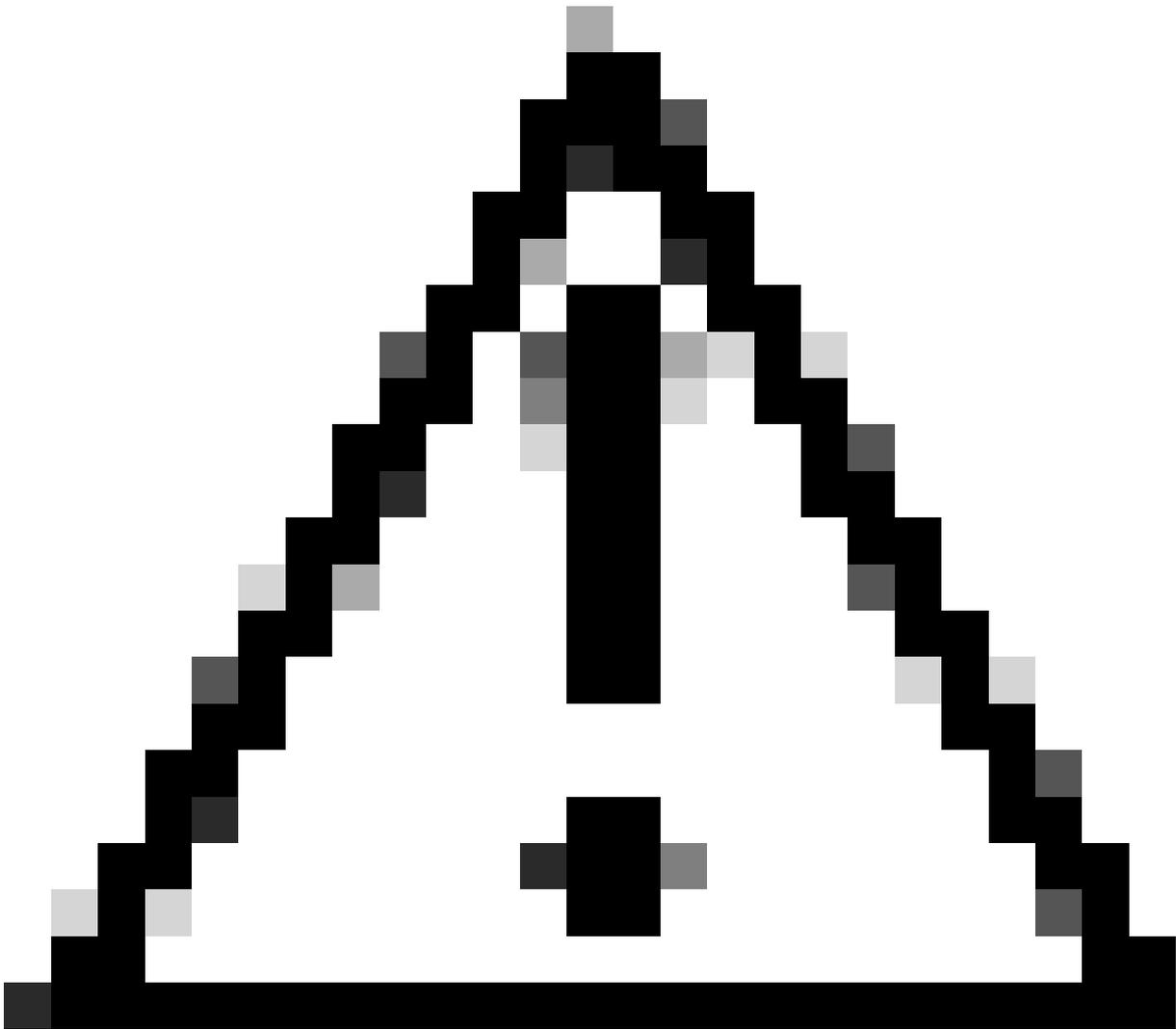


附註：將不需要驗證的辨識設定檔置於清單頂端。此方法可降低SWA的負載，將身份驗證隊列降至最低，並加快其他使用者的身份驗證速度。

步驟 7. 在User Identification Method部分中，選擇Exempt from authentication/identification。

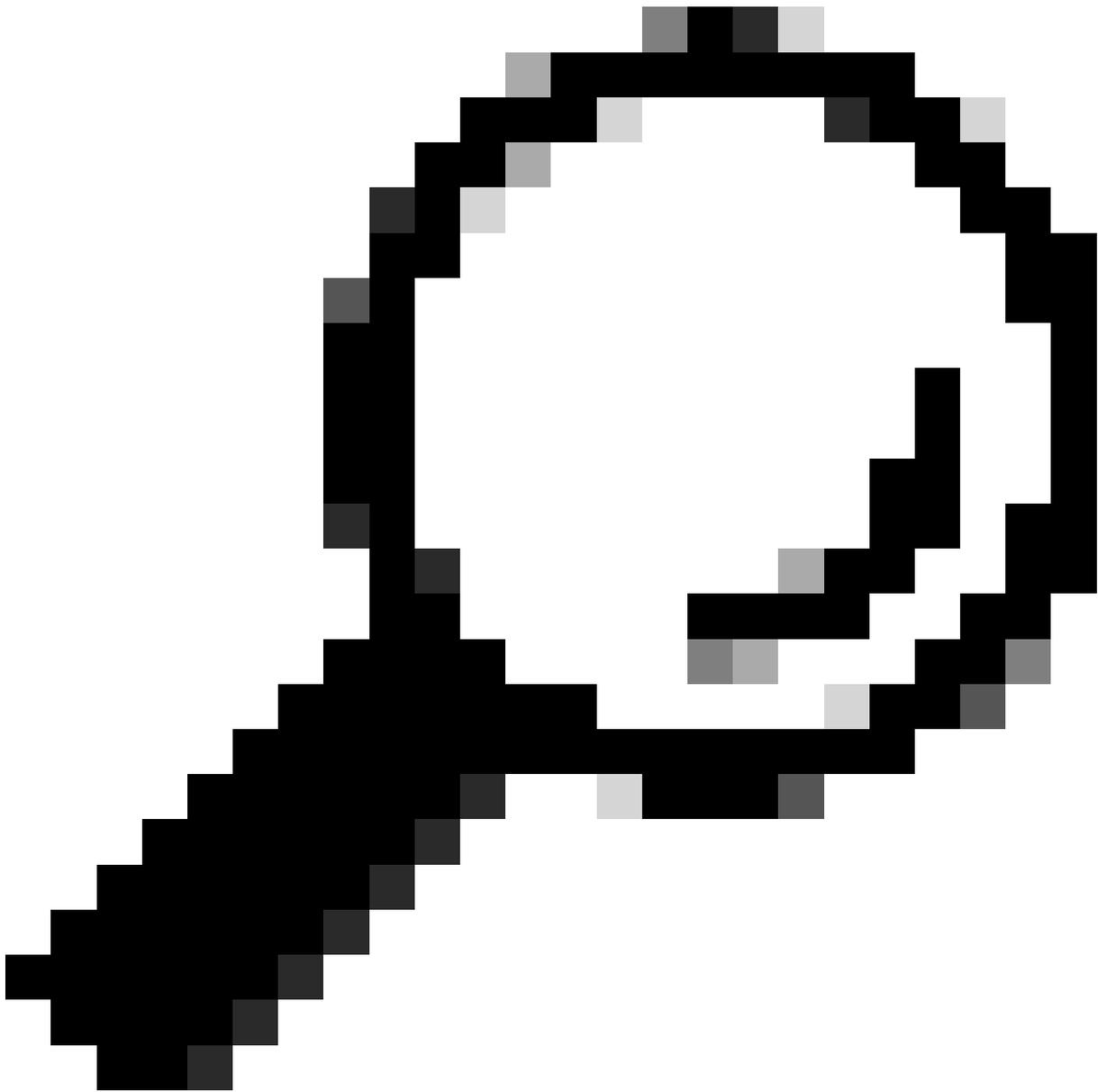
步驟 8.在Define Members by Subnet中，輸入此標識配置檔案必須應用的IP地址或子網。您可以使用IP地址、無類域間路由(CIDR)塊和子網。

第9步：(可選) 點選高級以定義其他成員資格條件，例如代理埠、URL類別或使用者代理。



注意：在透明代理部署中，SWA無法讀取HTTPS流量的使用者代理或完整URL，除非流量被解密。因此，如果使用使用者代理配置標識配置檔案，或使用正規表示式配置自定義URL類別，此流量將無法與標識配置檔案匹配。

有關如何配置自定義URL類別的詳細資訊，請訪問：[在安全Web裝置-思科中配置自定義URL類別](#)



提示：策略使用AND邏輯，這意味著必須滿足所有條件才能匹配ID配置檔案。設定 Advanced 選項後，必須滿足每個要求才能應用策略。

Identification Profiles: Add Profile

Client / User Identification Profile Settings

Enable Identification Profile

Name: ? Bypass Authentication
(e.g. my IT Profile)

Description: Subnets and IP Addresses that are Exempt from Authentication
(Maximum allowed characters 256)

Insert Above: 1 (auth)

User Identification Method

Identification and Authentication: ? Exempt from authentication / identification
This option may not be valid if any preceding Identification Profile requires authentication on all subnets.

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet: 10.1.0.0/16, 10.20.3.15
(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

Define Members by Protocol: HTTP/HTTPS

Advanced Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected
URL Categories: None Selected
User Agents: None Selected

The Advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories are not applicable for SOCKS transactions or transparent HTTPS (unless decrypted). When Advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.

Cancel Submit

圖-建立ID配置檔案以繞過身份驗證的步驟

步驟 10.提交和提交更改。

相關資訊

- [AsyncOS 15.0 for Cisco Secure Web Appliance使用手冊- GD \(常規部署\) -對終端使用者進行策略應用分類\[Cisco Secure Web Appliance\] -思科](#)
- [在安全Web裝置中配置自定義URL類別-思科](#)
- [如何在思科網路安全裝置\(WSA\)上免除Office 365流量身份驗證和解密-思科](#)

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）。