訪問安全Web裝置日誌

目錄

簡介

本文檔介紹檢視安全Web裝置(SWA)日誌的方法。

必要條件

需求

思科建議您瞭解以下主題：

- 已安裝物理或虛擬SWA。
- 許可證已啟用或已安裝。
- 安全殼層(SSH)使用者端。
- 安裝精靈已完成。

- 對SWA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。

SWA日誌型別

安全Web裝置透過將其寫入日誌檔案來記錄其自己的系統和流量管理活動。管理員可查閱這些日誌檔案來監控和排除裝置的故障。

此表格說明Secure Web Appliance記錄檔型別。

記錄檔型別	說明	是否支援Syslog推送？	預設情況下是否啟用？
訪問控制引擎日誌	記錄與Web代理ACL（訪問控制清單）評估引擎相關的消息。	否	否
安全EndpointEngine日誌	記錄有關檔案信譽掃描和檔案分析的資訊(安全終端。)	是	是
稽核記錄	記錄AAA（身份驗證、授權和記帳）事件。記錄與應用程式和命令列介面的所有使用者互動，並捕獲已提交的更改。 以下為部份稽核記錄詳細資訊： • 使用者-登入 • 使用者-登入失敗密碼不正確 • 使用者-登入失敗未知的使用者名稱 • 使用者-登入失敗的帳號已過期 • 使用者-註銷 • 使用者-鎖定 • 使用者-已啟動 • 使用者-密碼更改 • 使用者-密碼重置 • 使用者-安全設定/配置檔案更改 • 使用者-已建立 • 使用者-已刪除/已修改 • 群組/角色-刪除/修改 • 組/角色-許可權更改	是	是

記錄檔型別	說明	是否支援Syslog推送？	預設情況下是否啟用？
存取記錄	記錄Web Proxy使用者端歷史記錄。	是	是
ADC引擎架構日誌	記錄與Web代理和ADC引擎之間的通訊相關的消息。	否	否
ADC引擎日誌	記錄ADC引擎的調試消息。	是	是
身份驗證架構日誌	記錄身份驗證歷史記錄和消息。	否	是
AVC引擎架構日誌	記錄與Web代理和AVC引擎之間的通訊相關的消息。	否	否
AVC引擎日誌	記錄來自AVC引擎的調試消息。	是	是
CLI稽核日誌	記錄命令列介面活動的歷史審計。	是	是
配置日誌	記錄與Web代理組態管理系統相關的消息。	否	否
連線管理記錄	記錄與Web Proxy連線管理系統相關的訊息。	否	否
資料安全性記錄	記錄由思科資料安全過濾器評估的上傳請求的客戶端歷史記錄。	是	是
資料安全模組日誌	記錄與思科資料安全過濾器相關的消息。	否	否
DCA引擎架構日誌（動態內容分析）	記錄與Web代理和Cisco Web使用控制動態內容分析引擎之間的通訊相關的消息。	否	否
DCA引擎日誌（動態內容分析）	記錄與Cisco Web Usage Controls Dynamic Content Analysis Engine相關的消息。	是	是

記錄檔型別	說明	是否支援Syslog推送？	預設情況下是否啟用？
預設代理日誌	記錄與Web代理相關的錯誤。 這是所有Web Proxy相關記錄中最基本的記錄。若要疑難排解與Web代理相關的更多特定方面，請為適用的Web代理模組建立日誌訂閱。	是	是
磁碟管理員記錄	記錄與寫入磁碟上的快取相關的Web Proxy訊息。	否	否
外部身份驗證日誌	記錄與使用外部身份驗證功能相關的消息，例如與外部身份驗證伺服器通訊成功或失敗。 即使停用了外部身份驗證，此日誌也包含有關本地使用者成功登入或登入失敗的消息。	否	是
意見回饋記錄	記錄報告分類錯誤頁面的Web使用者。	是	是
FTP代理日誌	記錄與FTP代理相關的錯誤和警告消息。	否	否
FTP伺服器日誌	記錄所有使用FTP上傳到Secure Web裝置和從其下載的檔案。	是	是
GUI日誌 （圖形使用者介面）	在Web介面中記錄頁面重新整理的歷史記錄。GUI日誌還包含有關SMTP事務的資訊，例如有關從裝置傳送郵件的計畫報告的資訊。	是	是
Haystack日誌	Haystack日誌記錄Web事務跟蹤資料處理。	是	是
HTTPS日誌	記錄HTTPS代理特定的Web代理消息（啟用HTTPS代理時）。	否	否
ISE伺服器日誌	記錄ISE伺服器連線和操作資訊。	是	是
許可證模組日誌	記錄與Web代理的許可證和功能金鑰處理系統相關的消	否	否

記錄檔型別	說明	是否支援Syslog推送？	預設情況下是否啟用？
	息。		
記錄架構記錄	記錄與Web Proxy記錄系統相關的訊息。	否	否
記錄日誌	記錄與日誌管理相關的錯誤。	是	是
McAfee Integration Framework日誌	記錄與Web代理和McAfee掃描引擎之間的通訊相關的消息。	否	否
McAfee日誌	記錄來自McAfee掃描引擎的反惡意軟體掃描活動的狀態。	是	是
記憶體管理員記錄	記錄與管理所有記憶體（包括Web Proxy程式的記憶體內快取）相關的Web Proxy訊息。	否	否
其他Proxy模組記錄	記錄開發人員或客戶支援最常使用的Web Proxy訊息。	否	否
AnyConnect安全移動後台程式日誌	記錄Secure Web Appliance和AnyConnect客戶端之間的互動，包括狀態檢查。	是	是
NTP日誌 （網路時間協定）	記錄網路時間協定對系統時間所做的更改。	是	是
PAC檔案託管守護程式日誌	記錄使用者端的代理自動組態(PAC)檔案使用狀況。	是	是
代理旁路日誌	記錄繞過Web代理的事務。	否	是
報告日誌	記錄報告生成的歷史記錄。	是	是
報告查詢日誌	記錄與報告生成相關的錯誤。	是	是

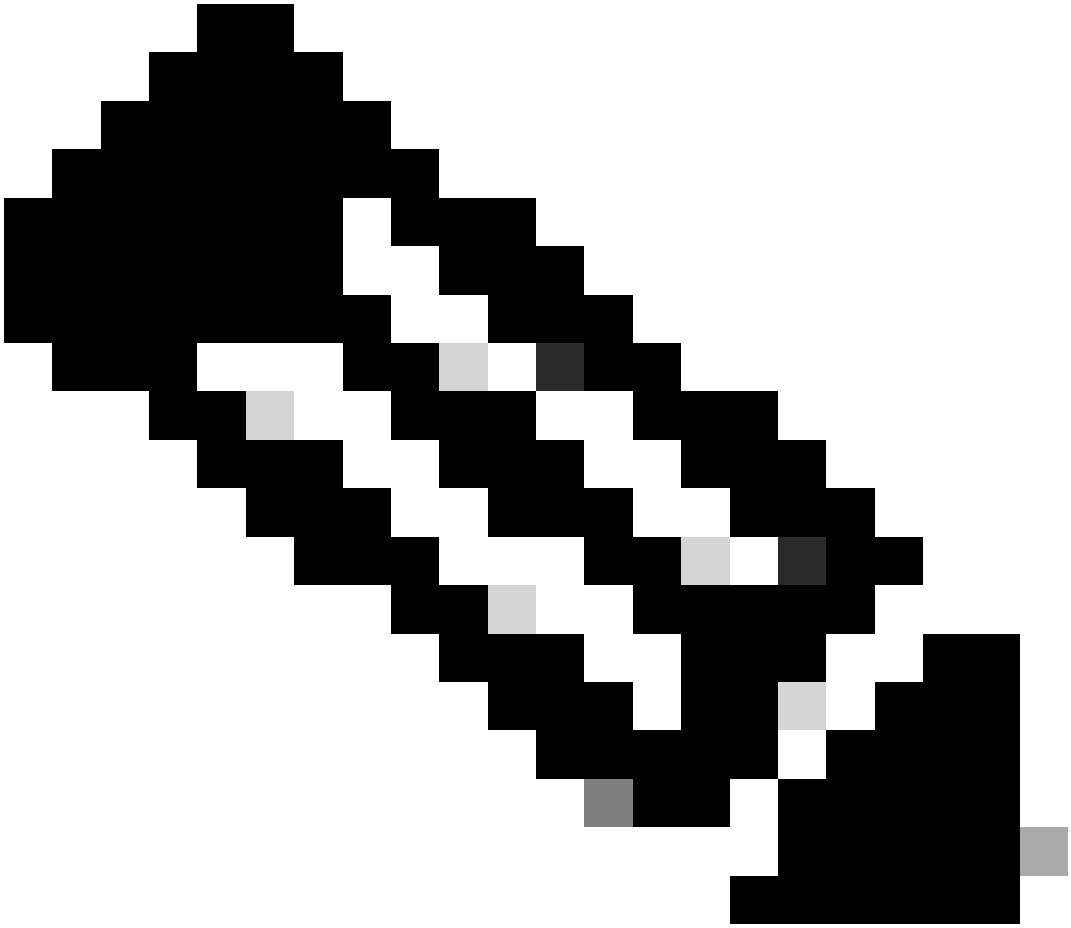
記錄檔型別	說明	是否支援Syslog推送？	預設情況下是否啟用？
請求調試日誌	從所有Web Proxy模組記錄型別中記錄特定HTTP交易的詳細偵錯資訊。建議建立此日誌訂閱，以便排除特定事務的Proxy問題，而無需建立所有其他的Proxy日誌訂閱。 注意：您只能在CLI中建立此日誌訂閱。	否	否
身份驗證日誌	記錄與存取控制功能相關的訊息。	是	是
SHD日誌 （系統健康狀態協助程式）	記錄系統服務的健全狀態歷史記錄，以及非預期的協助程式重新啟動歷史記錄。	是	是
SNMP日誌	記錄與SNMP網路管理引擎相關的調試消息。	是	是
SNMP模組日誌	記錄與SNMP監控系統互動相關的Web Proxy消息。	否	否
Sophos整合架構日誌	記錄與Web代理和Sophos掃描引擎之間的通訊相關的消息。	否	否
Sophos日誌	記錄來自Sophos掃描引擎的反惡意軟體掃描活動的狀態。	是	是
狀態日誌	記錄與系統相關的資訊，例如功能金鑰下載。	是	是
系統記錄	記錄DNS、錯誤和提交活動。	是	是
流量監控器錯誤日誌	記錄L4TM介面並捕獲錯誤。	是	是
流量監控器日誌	記錄增加到L4TM塊的站點並允許清單。	否	是
UDS日誌	記錄Web代理如何在不執行實際身份驗證的情況下發現	是	是

記錄檔型別	說明	是否支援Syslog推送？	預設情況下是否啟用？
（使用者發現服務）	使用者名稱的資料。它包括有關與安全移動的Cisco自適應安全裝置互動的資訊，以及與Novell eDirectory伺服器整合以實現透明使用者身份的資訊。		
更新程式日誌	記錄WBRS和其他更新的歷史記錄。	是	是
W3C日誌	以符合W3C的格式記錄Web代理客戶端歷史記錄。 更多資訊.	是	否
WBNP日誌 （SensorBase網路參與）	記錄Cisco SensorBase網路參與上傳到SensorBase網路的歷史記錄。	否	是
WBRS架構日誌 （Web信譽得分）	記錄與Web代理和Web信譽過濾器之間的通訊相關的消息。	否	否
WCCP模組日誌	記錄與實施WCCP相關的Web Proxy消息。	否	否
Webcat整合架構日誌	記錄與Web代理和與Cisco Web使用控制關聯的URL過濾引擎之間的通訊相關的消息。	否	否
Webroot整合架構日誌	記錄與Web代理和Webroot掃描引擎之間的通訊相關的消息。	否	否
Webroot日誌	記錄來自Webroot掃描引擎的反惡意軟體掃描活動的狀態。	是	是
歡迎頁面確認日誌	記錄點選終端使用者確認頁面上的「接受」按鈕的Web客戶端的歷史記錄。	是	是

檢視記錄

預設情況下，日誌儲存在SWA本地，您可以透過GUI下載本地儲存的日誌檔案，或者從CLI檢視日誌。

透過GUI下載日誌檔案



注意：必須在裝置上啟用FTP。要啟用FTP，請參閱本文中的「在安全Web裝置上啟用FTP」。

您可以從GUI下載記錄檔：

步驟 1.登入到GUI

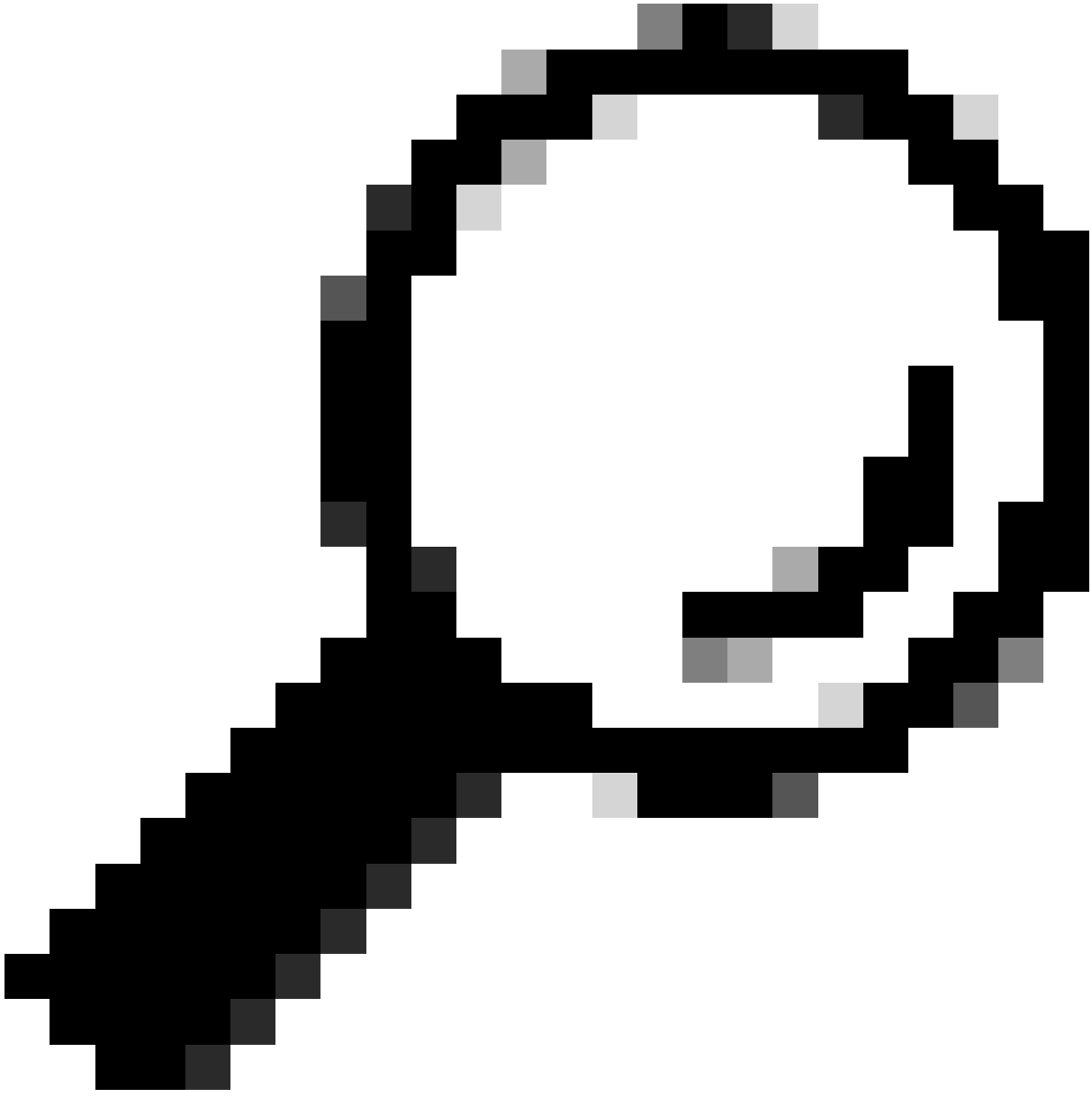
步驟 2.導航到「系統管理」

步驟 3.選擇記錄訂閱

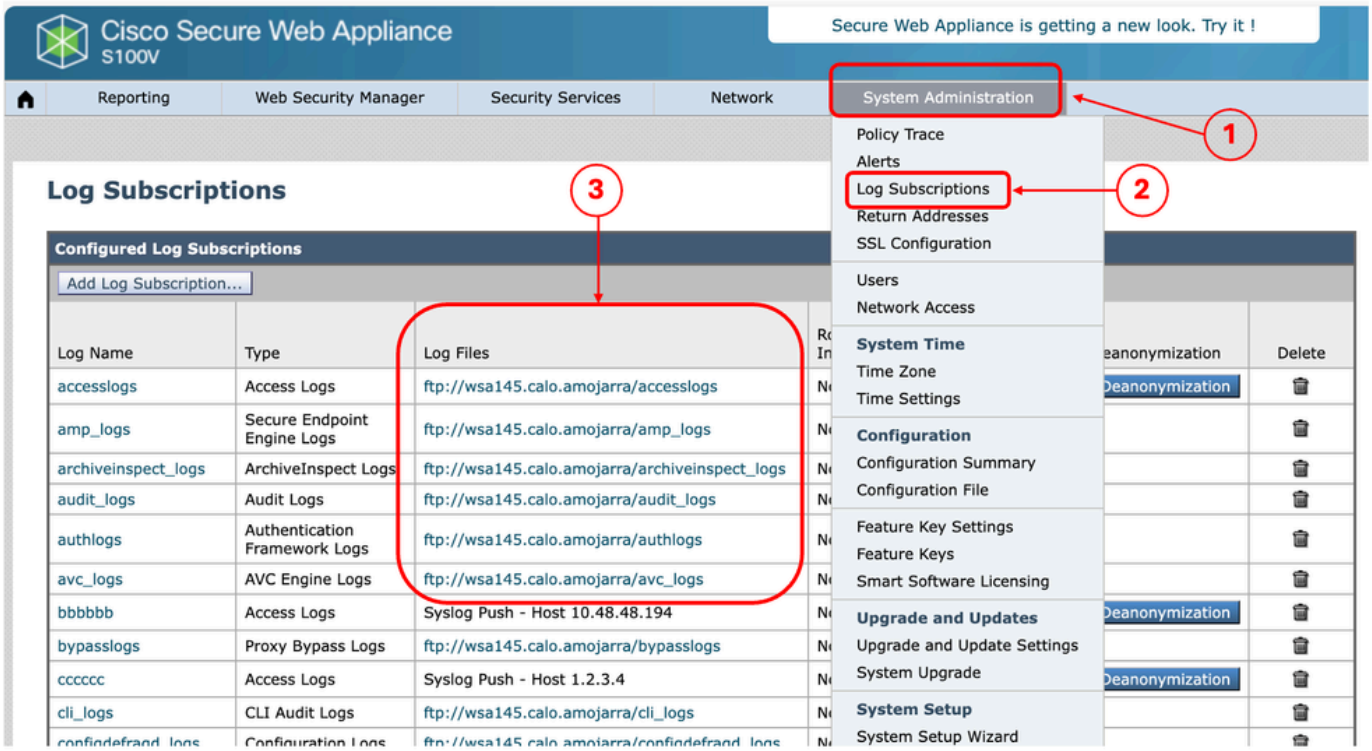
步驟4.在日誌訂閱清單的「日誌檔」欄中按一下日誌訂閱的名稱。

第5步：出現提示時，輸入用於訪問裝置的管理使用者名稱和密碼。

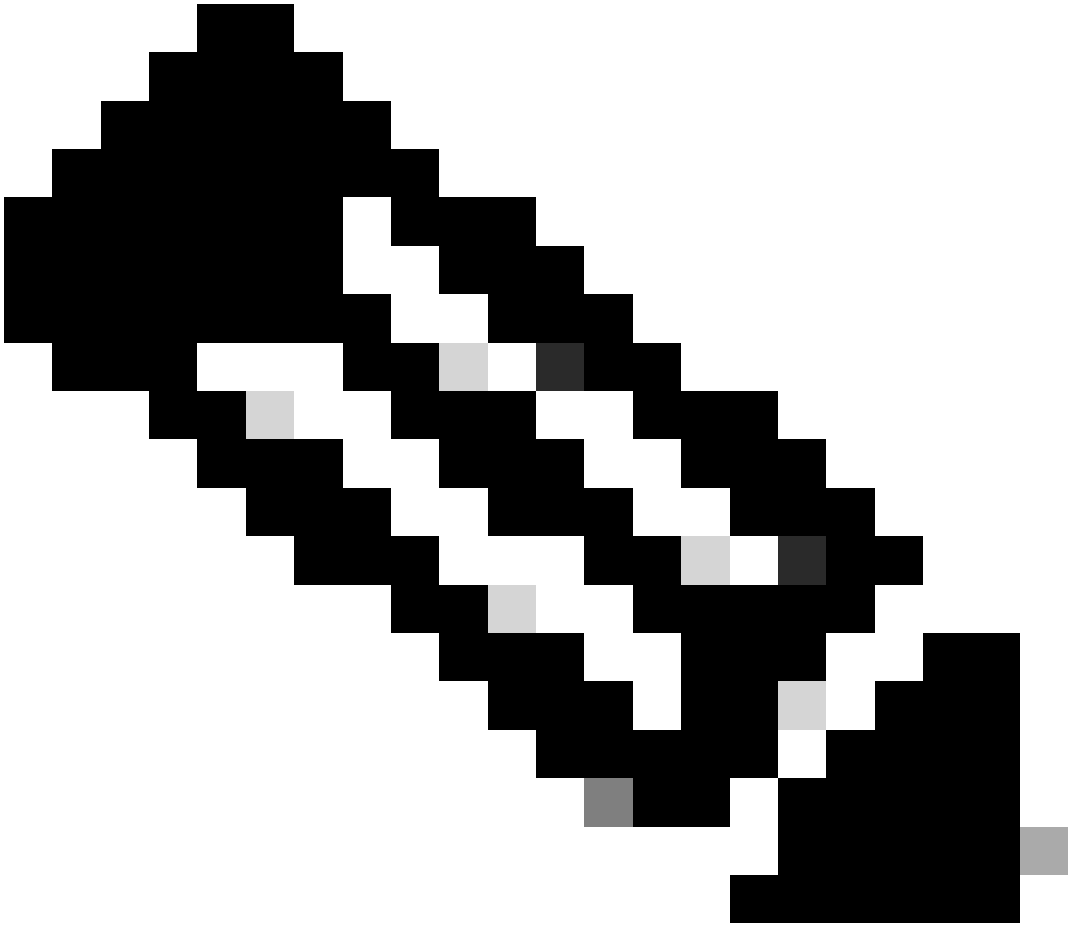
步驟6.登入後，按一下其中一個日誌檔案以在瀏覽器中檢視該檔案或將其儲存到磁碟。



提示：刷新瀏覽器以獲取更新的結果。


Cisco Secure Web Appliance
S100V
Secure Web Appliance is getting a new look. Try it !
Reporting
Web Security Manager
Security Services
Network
System Administration
Policy Trace
Alerts
Log Subscriptions
Return Addresses
SSL Configuration
Users
Network Access
System Time
Time Zone
Time Settings
Configuration
Configuration Summary
Configuration File
Feature Key Settings
Feature Keys
Smart Software Licensing
Upgrade and Updates
Upgrade and Update Settings
System Upgrade
System Setup
System Setup Wizard
1
2
3
Log Subscriptions
Configured Log Subscriptions
Add Log Subscription...
Log Name
Type
Log Files
Delete
accesslogs
Access Logs
ftp://wsa145.calo.amojarra/accesslogs
amp_logs
Secure Endpoint Engine Logs
ftp://wsa145.calo.amojarra/amp_logs
archiveinspect_logs
ArchiveInspect Logs
ftp://wsa145.calo.amojarra/archiveinspect_logs
audit_logs
Audit Logs
ftp://wsa145.calo.amojarra/audit_logs
authlogs
Authentication Framework Logs
ftp://wsa145.calo.amojarra/authlogs
avc_logs
AVC Engine Logs
ftp://wsa145.calo.amojarra/avc_logs
bbbbbb
Access Logs
Syslog Push - Host 10.48.48.194
bypasslogs
Proxy Bypass Logs
ftp://wsa145.calo.amojarra/bypasslogs
cccccc
Access Logs
Syslog Push - Host 1.2.3.4
cli_logs
CLI Audit Logs
ftp://wsa145.calo.amojarra/cli_logs

影像-下載記錄檔



注意：如果日誌訂閱已壓縮，請下載、解壓縮，然後打開它。

從CLI檢視記錄

您可以從CLI檢視記錄。在此情況下，您可以存取即時記錄或篩選記錄中的關鍵字。

步驟 1.連線到CLI

步驟 2. 鍵入grep，然後按Enter。

步驟 3.輸入要檢視的記錄編號

步驟4.（可選）可以透過定義正規表示式或詞來篩選輸出，否則請按Enter鍵

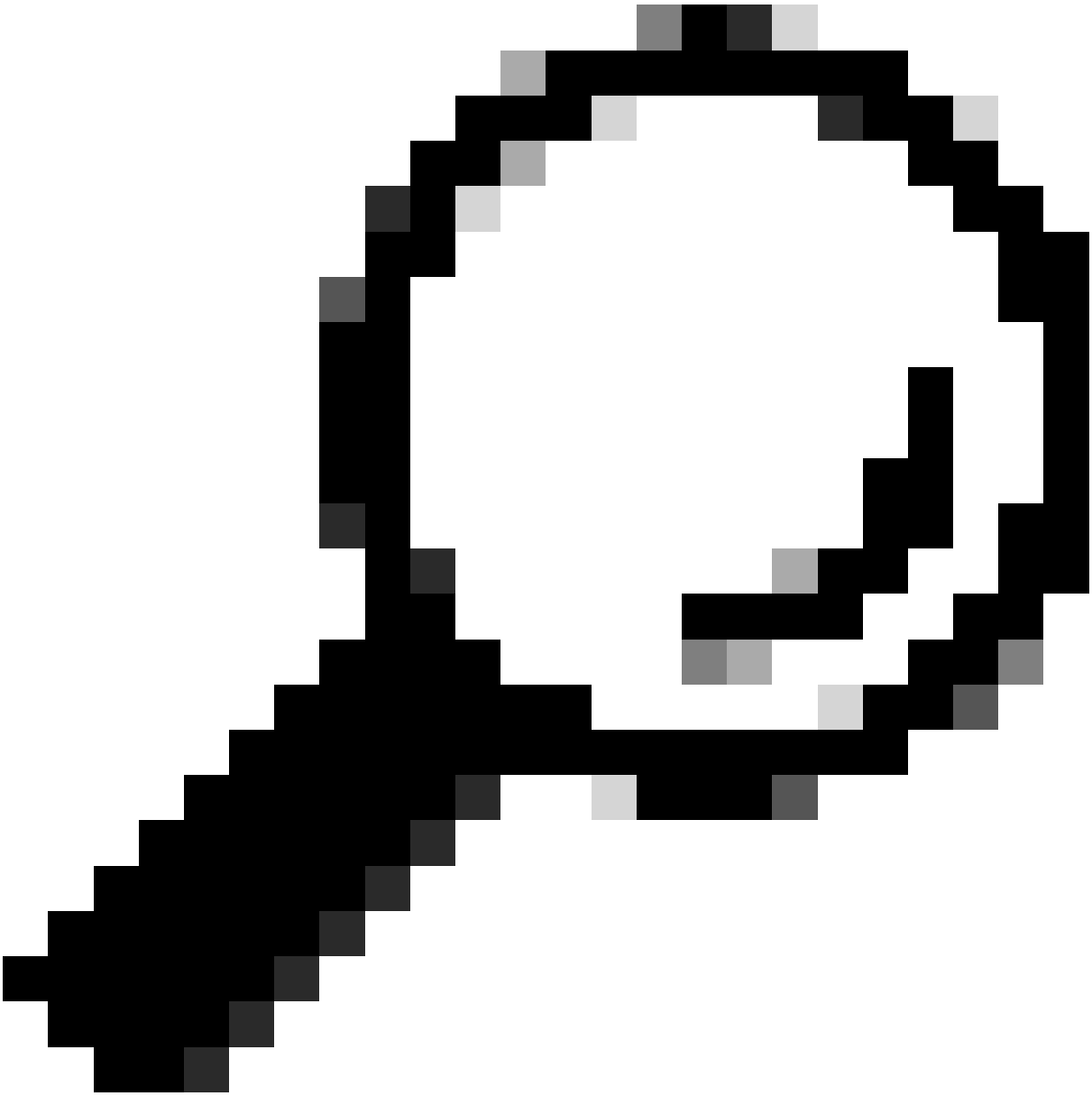
步驟5.如果您需要搜尋在步驟4中輸入的關鍵字，且關鍵字不區分大小寫，請在「您要此搜尋不區分大小寫嗎？」中按Enter鍵。[Y]>"，否則鍵入"N"並按Enter。

步驟 6.如果需要從搜尋中排除關鍵字，請在「是否要搜尋不匹配的行？」中鍵入「Y」。[N]>"，否

則請按Enter。

步驟 7. 如果需要檢視即時日誌，請在「是否要跟蹤日誌」中鍵入「Y」。[N]>"，否則請按Enter。

步驟 8.如果要對日誌進行分頁以逐頁檢視這些日誌，請在「是否要對輸出進行分頁？[N]>" ，否則請按Enter。



提示：如果選擇分頁，可以透過按「q」退出日誌

以下是輸出範例，顯示其中具有「警告」的所有行：

```
SWA_CLI> grep

Currently configured logs:
```

```
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "Secure Endpoint Engine Logs" Retrieval: FTP Poll
3. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
4. "audit_logs" Type: "Audit Logs" Retrieval: FTP Poll
5. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
6. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
7. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
8. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
...
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 40

Enter the regular expression to grep.
[]> Warning

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]>

Do you want to paginate the output? [N]>
```

在安全Web裝置上啟用FTP

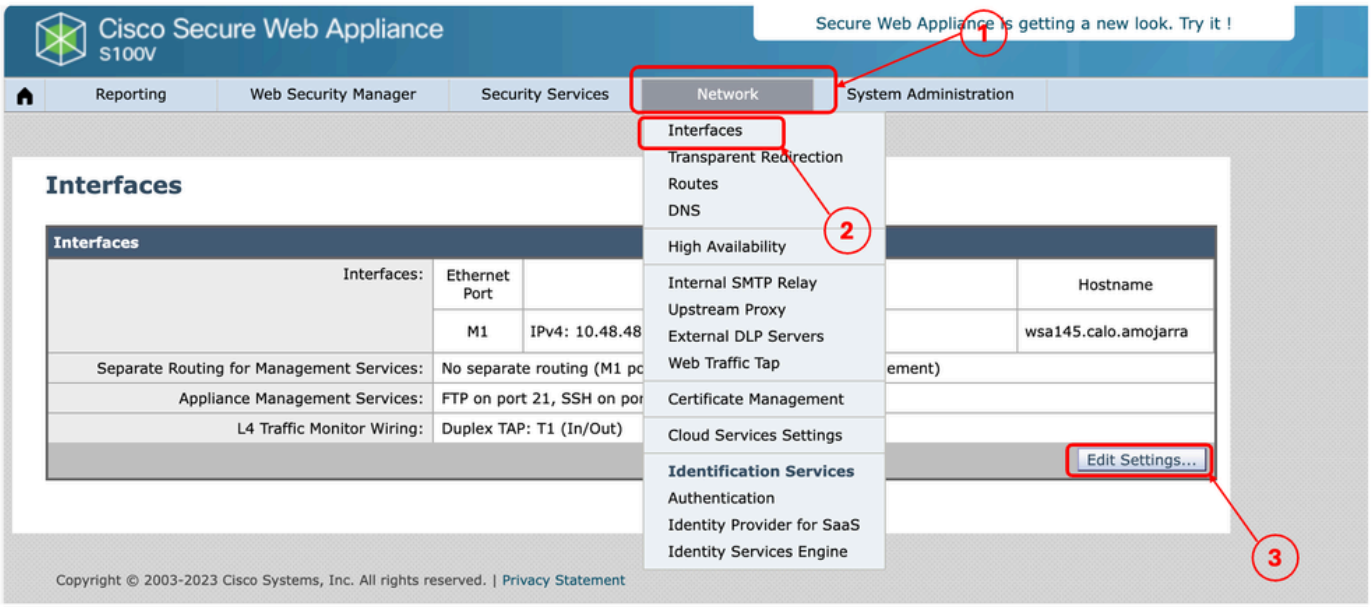
預設情況下，SWA上未啟用FTP。啟用FTP：

步驟 1.登入到GUI

步驟 2.導覽至Network

步驟 3.選擇Interfaces

步驟 4.按一下Edit Settings。

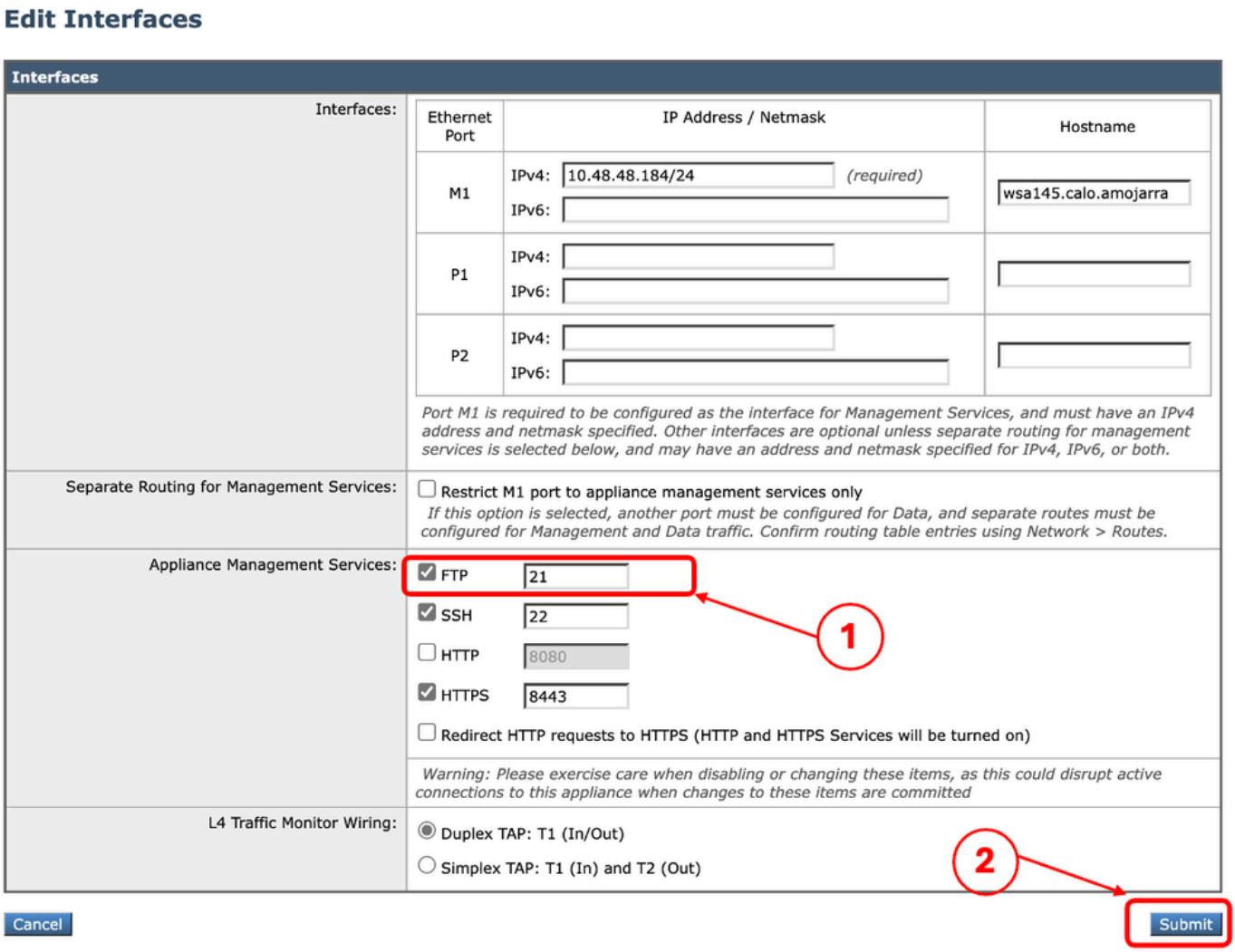


映像-在SWA上啟用FTP

步驟 5.選中FTP覈取方塊

步驟 6.為FTP提供TCP埠號（預設FTP埠為21）

步驟 7.提交和提交更改



映像-在SWA中配置FTP引數

相關資訊

- [Cisco Secure Web Appliance的AsyncOS 15.0使用手冊- LD（有限部署）-故障排除……]
- [使用Microsoft Server - Cisco在安全Web裝置中配置SCP推送日誌]

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）。