透過 FMC 設定 FTD 中的記錄

目錄

簡介

本文件說明透過 Firepower Management Center (FMC) 的 FirePOWER Threat Defense (FTD) 記錄設定。

必要條件

需求

思科建議您瞭解以下主題：

- FirePOWER 技術
- 調適型安全裝置(ASA)
- Syslog 通訊協定

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行軟體版本 6.0.1 及更高版本 ASA（5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X）的 ASA Firepower Threat Defense 影像

- 執行軟體版本 6.0.1 及更高版本 ASA（5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X）的 ASA Firepower Threat Defense 影像
- FMC 版本 6.0.1 及更高版本

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。

背景資訊

FTD 系統記錄檔提供您資訊以監控 FTD 設備並對其進行疑難排解。

這些記錄檔在日常疑難排解和處理事件時都十分實用。FTD 設備支援本機和外部記錄。

本機記錄可協助您解決即時問題。外部記錄是將 FTD 設備的記錄檔收集到外部 Syslog 伺服器的方法。

記錄到中央伺服器有助於彙總記錄檔和警示。外部記錄有助於為記錄檔建立關聯和處理事件。

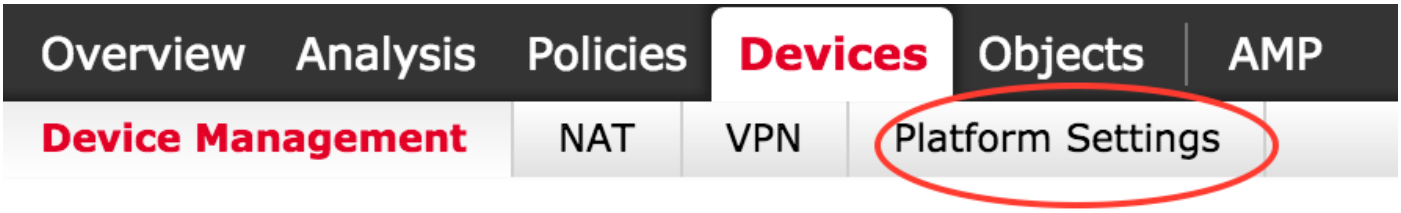
針對本機記錄，FTD 設備支援主控台、內部緩衝區選項和安全殼層 (SSH) 作業階段記錄。

針對外部記錄，FTD 設備支援外部 Syslog 伺服器和電子郵件中繼伺服器。

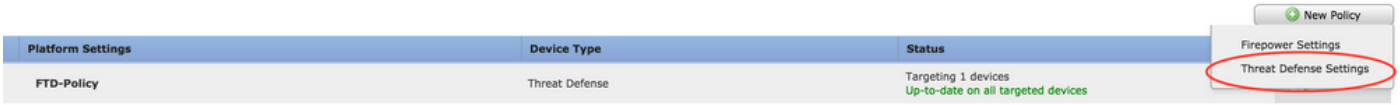
注意：如果大量流量通過裝置，請注意日誌記錄/嚴重性/速率限制的型別。這個作法是為了限制記錄檔的數量，進而避免影響到防火牆。

設定

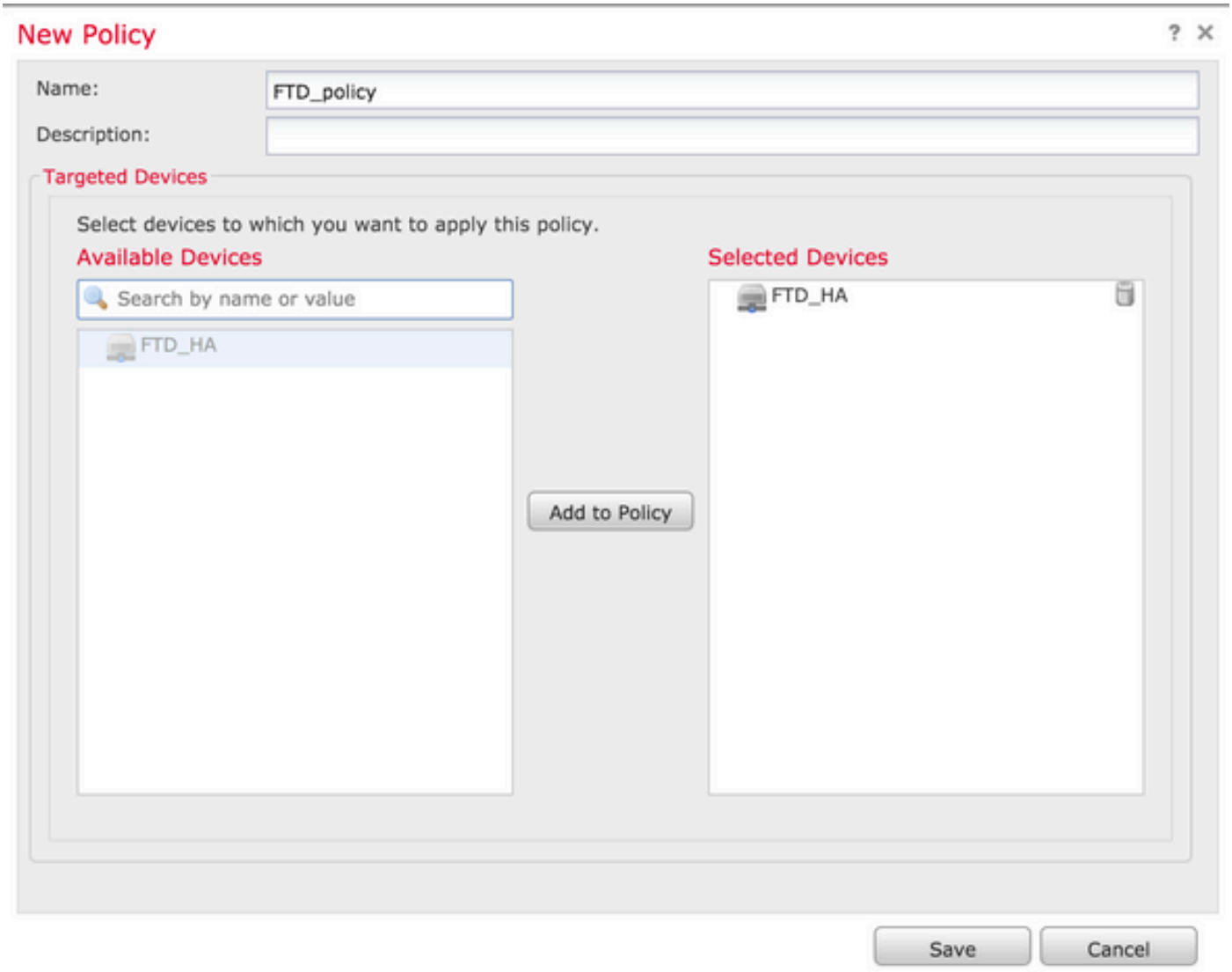
當您導航到 Platform Settings 頁籤的 Devices 頁籤。選擇 Devices > Platform Settings 如下圖所示。



按一下鉛筆圖示以編輯現有的策略，或者按一下 **New Policy**，然後選擇 **Threat Defense Settings**以便建立新的FTD原則，如下圖所示。



選擇要應用此策略的FTD裝置，然後按一下 **Save** 如下圖所示。



設定全域 Syslog 設定

特定設定同時適用於本機和外部記錄。本節介紹可以為 Syslog 設定的強制和選用參數。

記錄設定

記錄設定選項適用於本機和外部記錄。要配置日誌記錄設定，請選擇 **Devices > Platform Settings.**

選擇 **Syslog > Logging Setup.**

基本記錄設定

- Enable Logging：檢查 **Enable Logging** 覈取方塊，以便啟用日誌記錄。此為強制選項。
- Enable Logging on the failover standby unit：檢查 **Enable Logging on the failover standby unit** 覈取方塊，以便在作為FTD高可用性集群一部分的待命FTD上配置日誌記錄。
- Send syslogs in EMBLEM format：檢查 **Send syslogs in EMBLEM format** 覈取方塊，以便為每個目標啟用系統日誌格式為EMBLEM。EMBLEM 格式主要用於 CiscoWorks Resource Manager Essentials (RME) Syslog 分析器。此格式與路由器和交換器產生的 Cisco IOS 軟體 Syslog 格式相符，僅適用於 UDP Syslog 伺服器。
- Send debug messages as syslogs：檢查 **Send debug messages as syslogs** 覈取方塊以將調試日誌作為系統日誌消

息傳送到系統日誌伺服器。

- Memory size of the Internal Buffer:輸入 FTD 可以儲存記錄檔資料的內部記憶體緩衝大小。如果達到其緩衝限制，則會輪替記錄檔資料。

FTP 伺服器資訊（選填）

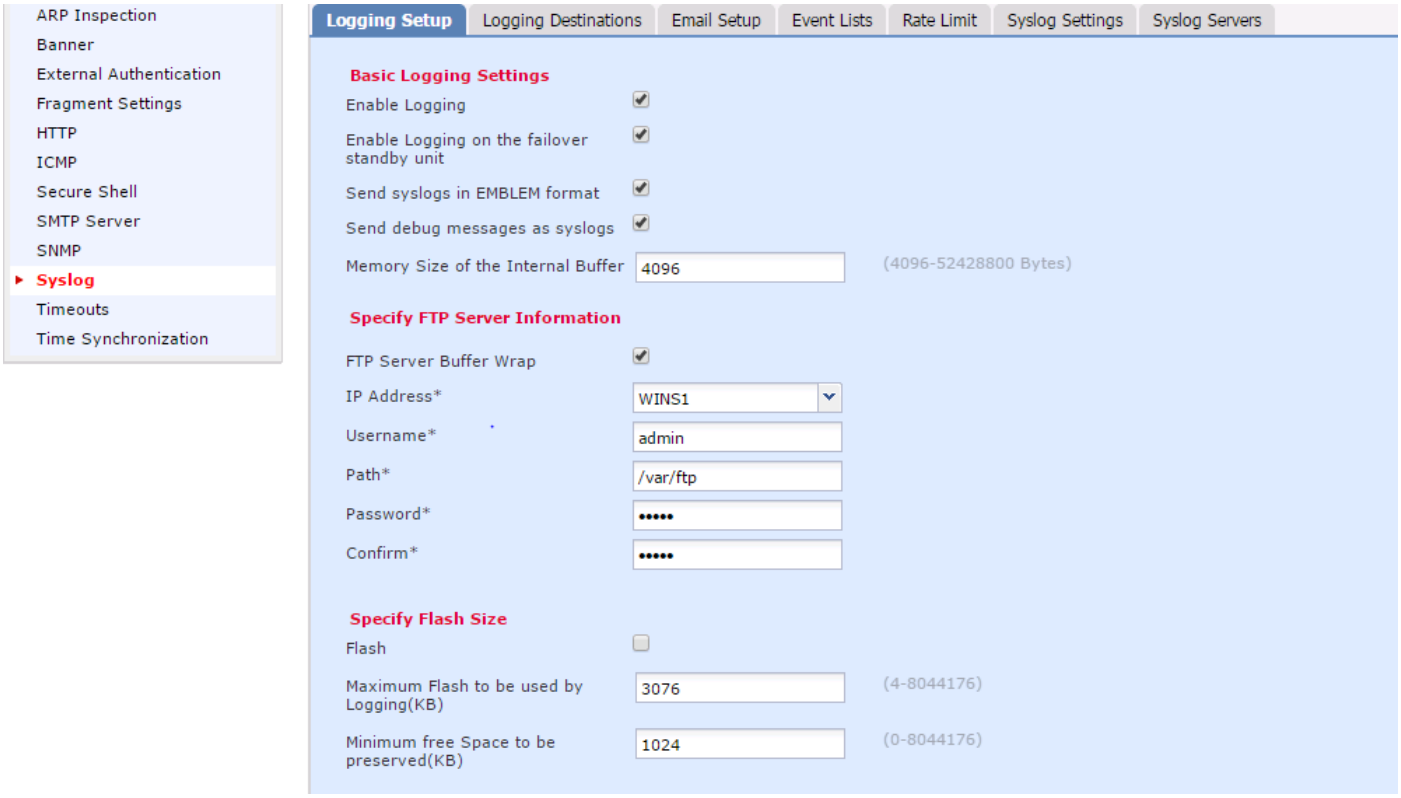
若要在 FTP 伺服器覆寫內部緩衝之前，將記錄檔資料傳送到 FTP 伺服器，請指定 FTP 伺服器詳細資訊。

- FTP Server Buffer Wrap：檢查 **FTP Server Buffer Wrap** 覈取方塊以將緩衝區日誌資料傳送到FTP伺服器。
- IP Address:輸入 FTP 伺服器的 IP 位址。
- Username:輸入 FTP 伺服器的使用者名稱。
- Path:輸入 FTP 伺服器的目錄路徑。
- Password:輸入 FTP 伺服器的密碼。
- Confirm:再次輸入相同的密碼。

快閃記憶體大小（選填）

若要在內部緩衝滿載時，將記錄檔資料儲存到快閃記憶體，請指定快閃記憶體大小。

- Flash：檢查 **Flash** 覈取方塊以將日誌資料傳送到內部快閃記憶體。
- Maximum Flash to be used by Logging(KB):輸入可用於記錄的快閃記憶體大小上限（以 KB 為單位）。
- Minimum free Space to be preserved(KB):輸入需要保留的快閃記憶體的大小下限（以 KB 為單位）。



按一下 **Save** 以儲存平台設定。選擇 **Deploy** 選項，選擇要應用更改的FTD裝置，然後按一下 **Deploy** 以便開始部署平台設定。

事件清單

「設定事件清單」選項可讓您建立/編輯事件清單，並指定要包含在事件清單篩選器中的記錄檔資料。在記錄目的地下設定記錄篩選器時，可以使用「事件清單」。

系統允許透過兩個選項來使用自訂事件清單的功能。

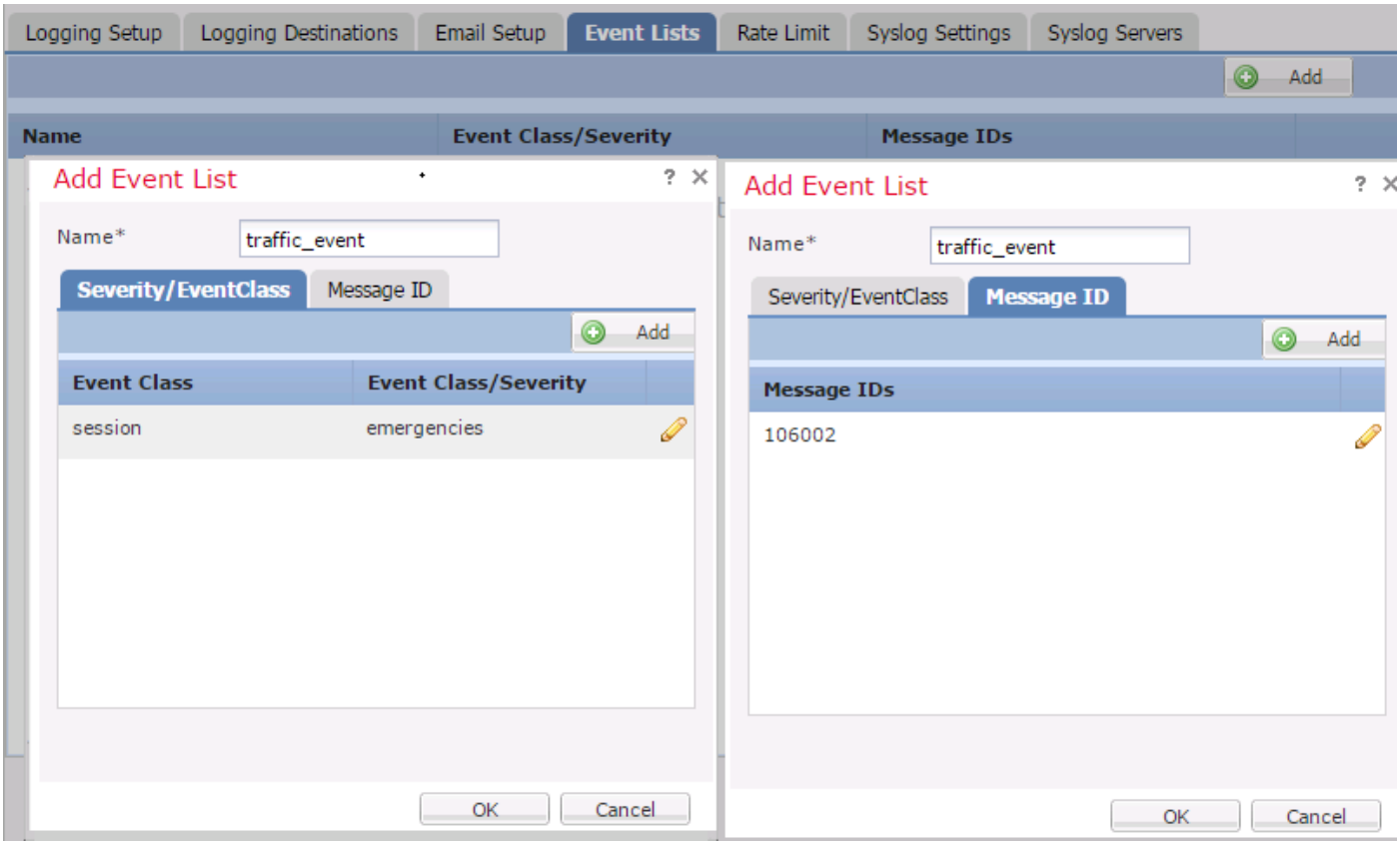
- 類別和嚴重性
- 消息ID

要配置自定義事件清單，請選擇 **Device > Platform Setting > Threat Defense Policy > Syslog > Event List** 然後按一下 **Add**.選項如下：

- Name:輸入事件清單的名稱。
- Severity/Event Class：在Severity/Event Class部分，按一下 **Add**.
- Event Class:從下拉清單，為所需的記錄檔資料類型選擇事件類別。「事件類別」定義一組表示相同功能的 Syslog 規則。

例如，作業階段的「事件類別」中包括與作業階段相關的所有 Syslog。

- Syslog Severity:從所選「事件類別」的下拉清單，選擇嚴重性。嚴重性的範圍可以從 0（緊急）到 7（偵錯）。
- Message ID：如果您對與消息ID相關的特定日誌資料感興趣，請按一下 **Add** 以便根據郵件ID設定過濾器。
- Message IDs:將訊息 ID 指定為個別/範圍格式。



按一下 **OK** 以儲存組態。

按一下 **Save** 以儲存平台設定。選擇以 **Deploy**中，選擇要應用更改的FTD裝置，然後按一下 **Deploy**以便

開始部署平台設定。

速率限制 Syslog

「速率限制」選項定義可以傳送到所有已設定目的地的訊息數量，並定義要指派速率限制的訊息嚴重性。

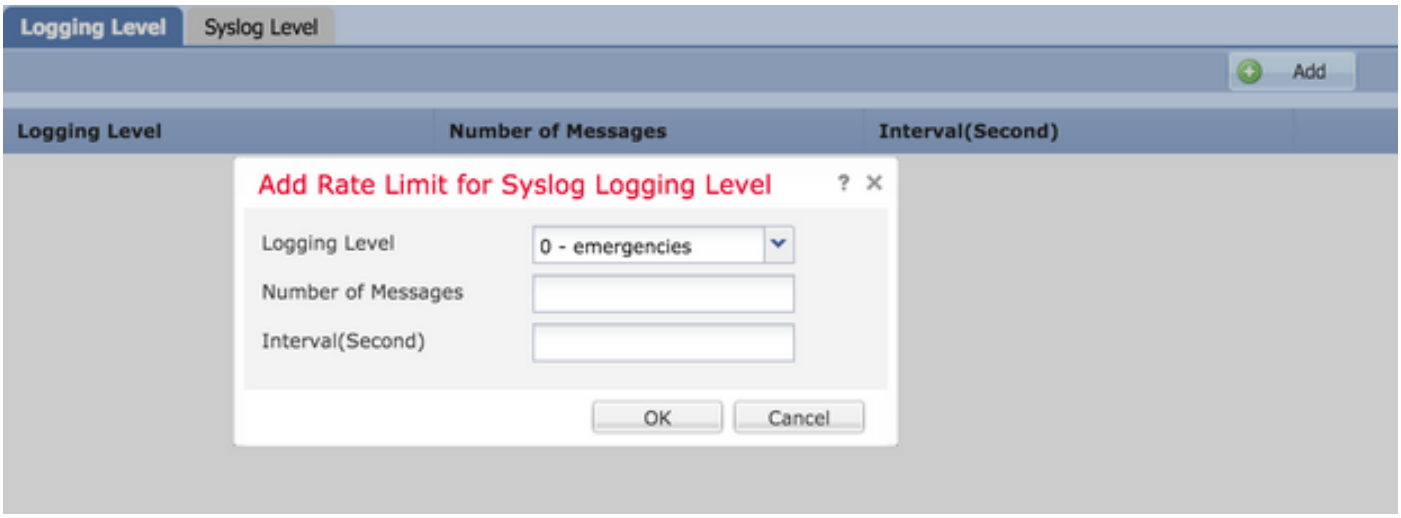
要配置自定義事件清單，請選擇 **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**.您有兩個選項，可以在此基礎上指定速率限制：

- 日誌記錄級別
- Syslog 層級

要啟用基於記錄級別的速率限制，請選擇 **Logging Level** 然後按一下 **Add**.

- Logging Level：來自 **Logging Level** 下拉選單中，選擇要對其執行速率限制的日誌記錄級別。
- Number of Messages:輸入在指定時間間隔內接收的 Syslog 訊息數量上限。
- Interval(Second):根據先前設定的參數「訊息數量」，輸入可以接收一組固定 Syslog 訊息的時間間隔。

Syslog 的速率是指訊息數/間隔數。

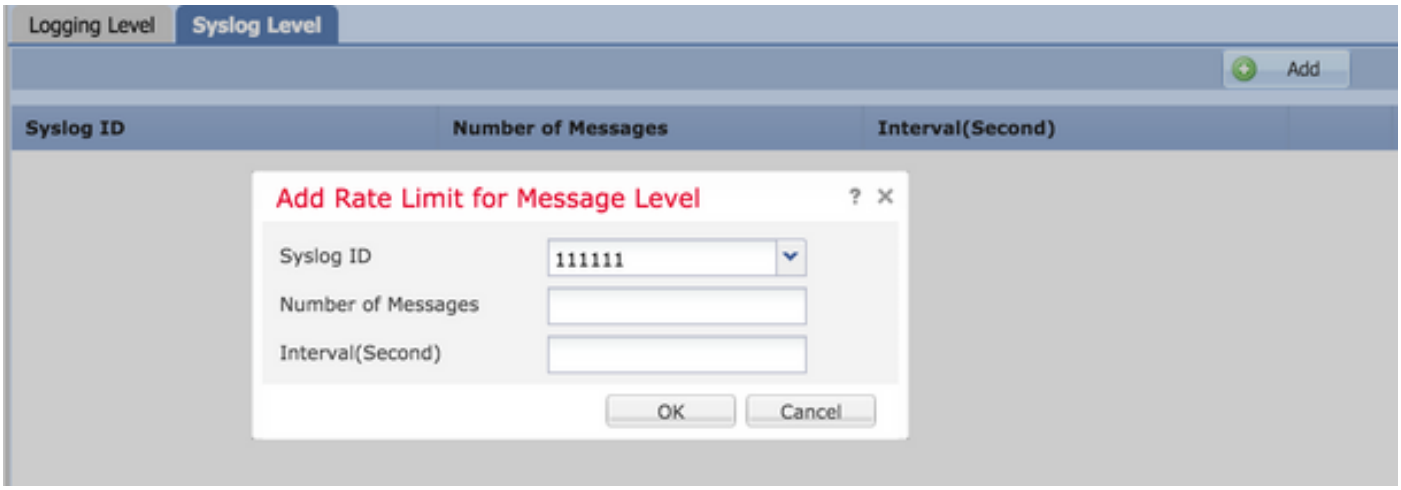


按一下 **OK** 以儲存日誌記錄級別配置。

要啟用基於記錄級別的速率限制，請選擇 **Logging Level** 然後按一下 **Add**.

- Syslog ID:Syslog ID 用於唯一識別 Syslog 訊息。從 **Syslog ID** 下拉選單中，選擇Syslog ID。
- Number of Messages:輸入在指定時間間隔內接收的 Syslog 訊息數量上限。
- Interval(Second):根據先前設定的參數「訊息數量」，輸入可以接收一組固定 Syslog 訊息的時間間隔。

Syslog 的速率是指訊息數/間隔數。



按一下 **OK** 以便儲存系統日誌級別配置。

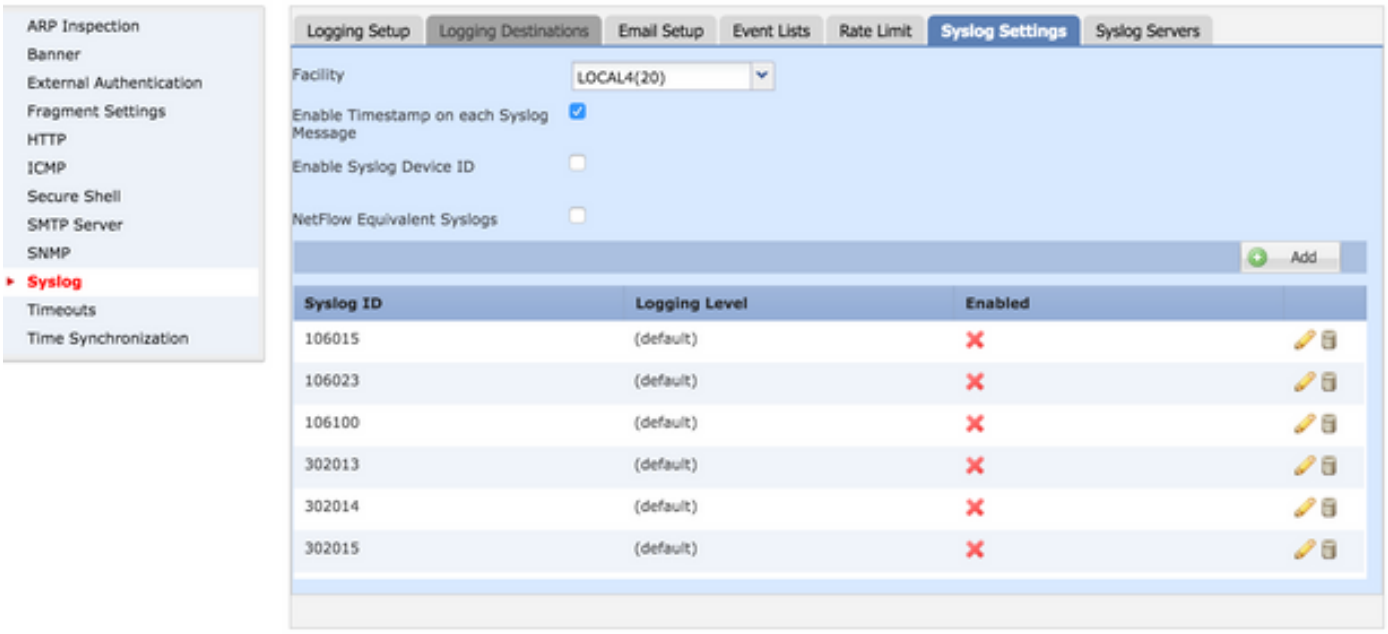
按一下 **Save** 以儲存平台設定。選擇以 **Deploy**中，選擇要應用更改的FTD裝置，然後按一下 **Deploy** 以便開始部署平台設定。

系統日誌設定

Syslog 設定允許將「設施」值設定為包含在 Syslog 訊息中。您也可以將時間戳記包含在記錄檔訊息和其他 Syslog 伺服器專屬參數中。

要配置自定義事件清單，請選擇 **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings.**

- Facility:設施代碼用於指定記錄訊息的程式類型。使用不同設施的訊息可透過不同方式處理。從 **Facility** 下拉選單，選擇設施值。
- Enable Timestamp on each Syslog Message：檢查 **Enable Timestamp on each Syslog Message** 覈取方塊以將時間戳包含在Syslog消息中。
- Enable Syslog Device ID：檢查 **Enable Syslog Device ID** 覈取方塊以將裝置ID包括在非EMBLEM格式的系統日誌消息中。
- Netflow Equivalent Syslogs：檢查 **Netflow Equivalent Syslogs** 覈取方塊，以便傳送NetFlow等效系統日誌。設備的效能可能會因此受到影響。
- 新增特定系統日誌ID：若要指定其他系統日誌ID，請按一下 **Add** 並指定 **Syslog ID/ Logging Level** 覈取方塊。



按一下 **Save** 以儲存平台設定。選擇以 **Deploy**中，選擇要應用更改的FTD裝置，然後按一下 **Deploy** 以便開始部署平台設定。

設定本機記錄

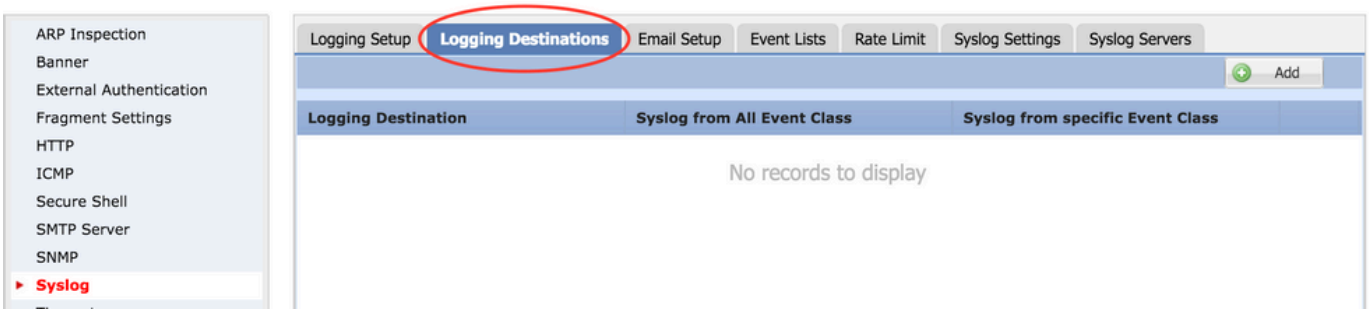
「記錄目的地」區段可用於將記錄設定到特定目的地。

可用的內部記錄目的地如下：

- 內部緩衝區：記錄到內部日誌緩衝區（日誌緩衝區）
- 控制檯：將日誌傳送到控制檯（日誌控制檯）
- SSH會話：將系統日誌記錄到SSH會話（終端監視器）

設定本機記錄有三個步驟。

步驟 1.選擇 **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations.**



步驟 2.按一下 **Add** 新增特定日誌記錄過濾器 **logging destination.**

日誌記錄目標：從 **Logging Destination** 下拉選單作為內部緩衝區、控制檯或SSH會話。

Event Class：來自 **Event Class** 下拉選單中，選擇Event類。如上所述，「事件類別」是指一組表示相同功能的 Syslog。您可以透過以下方式選擇事件類別：

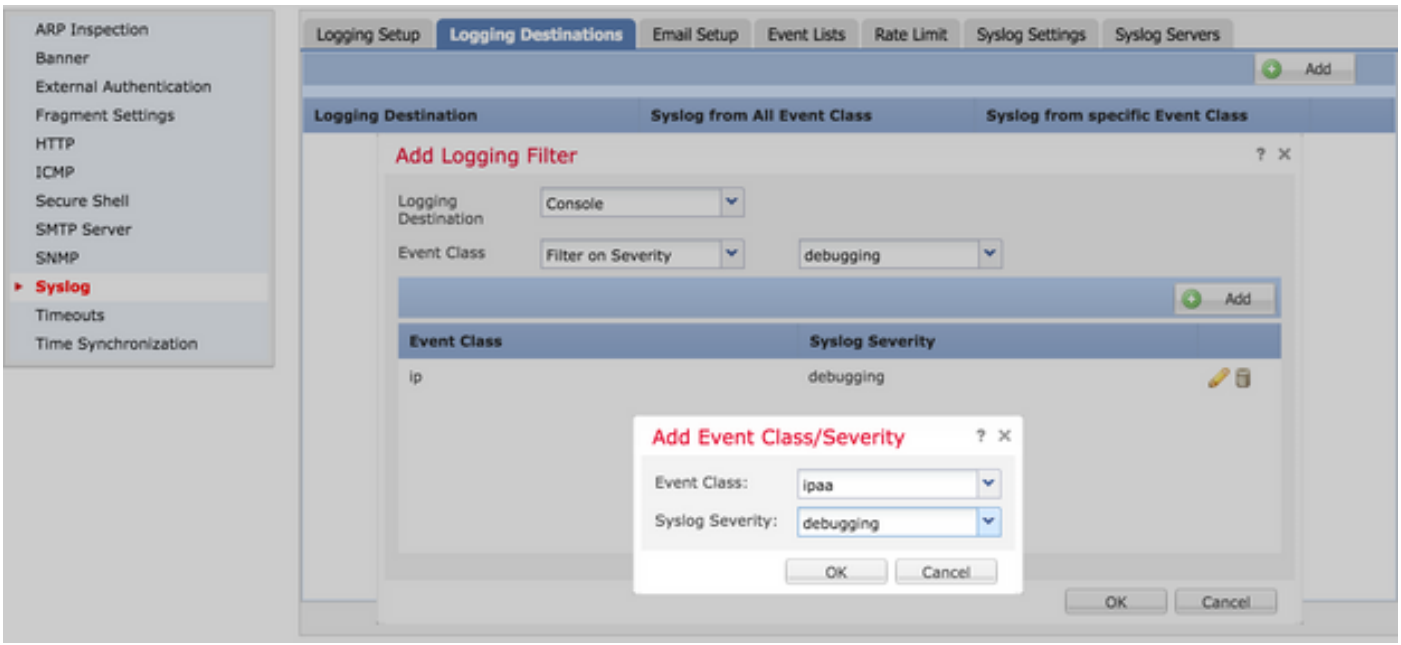
- Filter on Severity:事件類別根據 Syslog 的嚴重性進行篩選。
- User Event List:管理員可以使用自己的自訂事件類別，建立特定的事件清單（如前所述），並在本節中引用。
- Disable Logging:使用此選項可停用記錄所選記錄目的地和記錄層級。

日誌記錄級別：從下拉選單中選擇日誌記錄級別。記錄層級的範圍從 0（緊急）到 7（偵錯）。

步驟 3.若要向此日誌記錄過濾器新增單獨的Event類，請按一下 **Add**.

Event Class：從 **Event Class** 下拉選單。

Syslog Severity：從 **Syslog Severity** 下拉選單。



按一下 **OK** 將過濾器配置為新增特定日誌記錄目標的過濾器後。

按一下 **Save** 以儲存平台設定。選擇 **Deploy**中，選擇要應用更改的FTD裝置，然後按一下 **Deploy** 以便開始部署平台設定。

設定外部記錄

要配置外部日誌記錄，請選擇 **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations.**

FTD 支援這些類型的外部記錄。

- Syslog Server：將日誌傳送到遠端Syslog伺服器。
- SNMP陷阱：將註銷作為SNMP陷阱傳送。
- 電子郵件：使用預配置的郵件中繼伺服器通過電子郵件傳送日誌。

外部記錄和內部記錄的設定相同。選取記錄目的地會決定實作的記錄類型。您可以根據自訂事件清單將「事件類別」設定至遠端伺服器。

遠端 Syslog 伺服器

您可以設定 Syslog 伺服器，以從 FTD 遠端分析和儲存記錄檔。

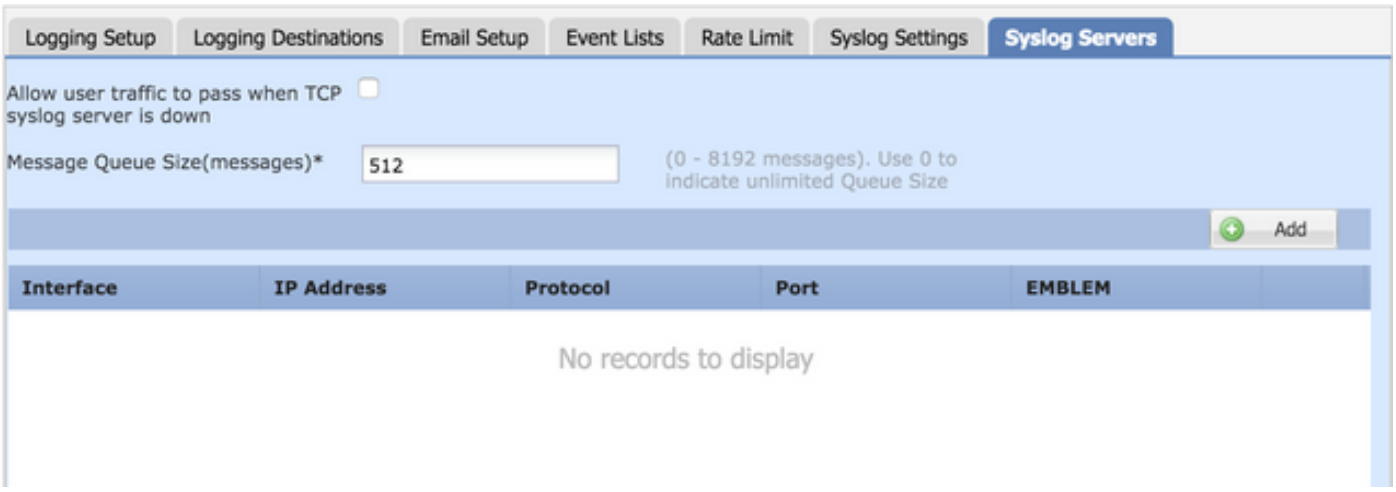
設定遠端 Syslog 伺服器有三個步驟。

步驟 1.選擇 **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers.**

步驟 2.配置與系統日誌伺服器相關的引數。

- 當TCP syslog伺服器關閉時，允許使用者流量通過：如果網路中部署了TCP Syslog伺服器且無法訪問，則通過ASA的網路流量將遭到拒絕。這僅適用於 ASA 和 Syslog 伺服器之間的傳輸通訊協定為 TCP 時。請檢視 **Allow user traffic to pass when TCP syslog server is down** 覈取方塊，以便在系統日誌伺服器關閉時允許流量通過介面。

- 消息隊列大小：消息隊列大小是當遠端系統日誌伺服器繁忙並且不接受任何日誌消息時，在FTD中排隊等候的消息數。預設值為512條消息，最小值為1條消息。如果此選項指定 0，則佇列大小視為無限。



步驟 3.要新增遠端Syslog伺服器，請按一下 **Add**.

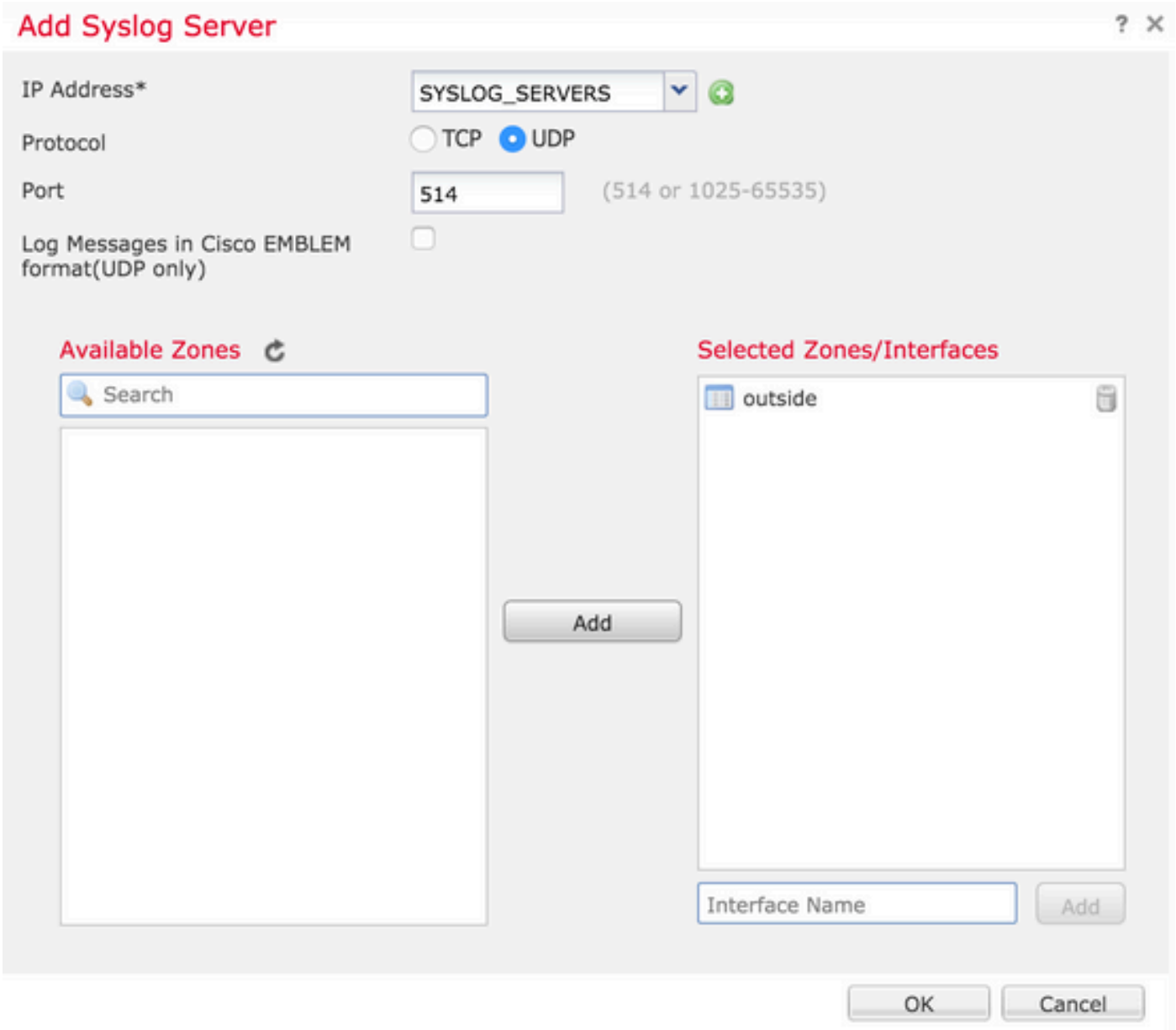
IP Address：來自 **IP Address** 下拉選單，選擇列出系統日誌伺服器的網路對象。若尚未建立網路物件，請按一下加號 (+) 圖示以建立新物件。

Protocol：按一下 **TCP** 或 **UDP** 用於系統日誌通訊的單選按鈕。

Port:輸入 Syslog 伺服器連接埠號碼。預設為 514。

Log Messages in Cisco EMBLEM format(UDP only)：按一下 **Log Messages in Cisco EMBLEM format (UDP only)** 覈取方塊，以便在需要以思科EMBLEM格式記錄消息時啟用此選項。這僅適用於 UDP 型 Syslog。

Available Zones:輸入 Syslog 伺服器可連線的安全區域，並將其移至「選取的區域/介面」欄位。



按一下 **OK** 和 **Save** 以儲存組態。

按一下 **Save** 以儲存平台設定。選擇 **Deploy**中，選擇要應用更改的FTD裝置，然後按一下 **Deploy** 以便開始部署平台設定。

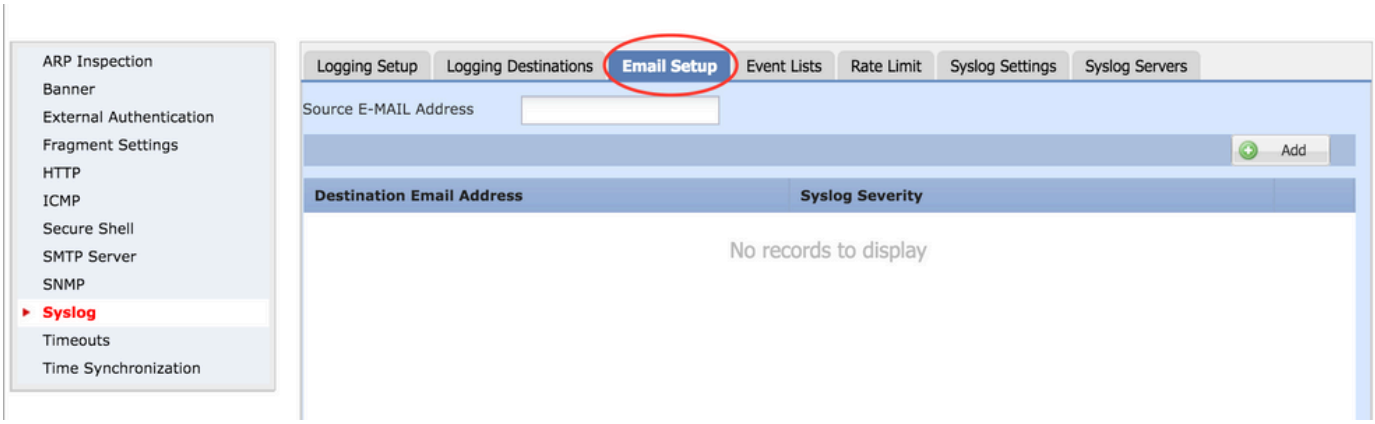
用於記錄的電子郵件設定

FTD 允許您將 Syslog 傳送至特定電子郵件地址。僅當已設定電子郵件中繼伺服器時，才能將電子郵件當作記錄目的地。

設定 Syslog 的電子郵件設定有兩個步驟。

步驟 1.選擇 **Device > Platform Setting > Threat Defense Policy > Syslog >Email Setup.**

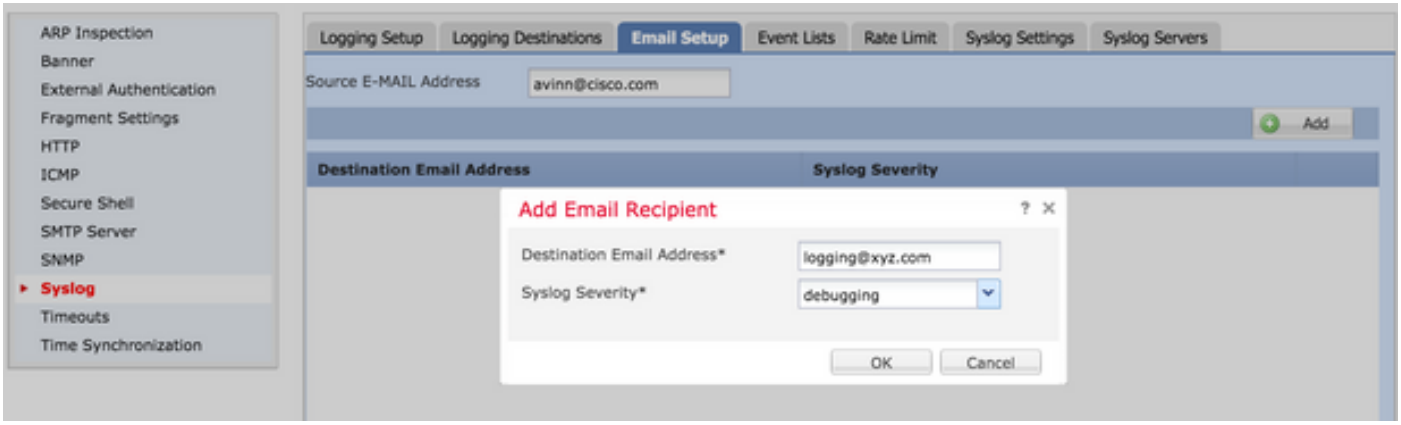
Source E-MAIL Address:輸入來源電子郵件地址，這會顯示於從 FTD 送出的所有包含 Syslog 的電子郵件上。



步驟 2.要配置目標電子郵件地址和系統日誌嚴重性，請按一下 **Add.**

Destination Email Address:輸入傳送 Syslog 訊息的目的地電子郵件地址。

Syslog Severity：從 **Syslog Severity** 下拉選單。



按一下 **OK** 以儲存組態。

按一下 **Save** 以儲存平台設定。選擇 **Deploy**中，選擇要應用更改的FTD裝置，然後按一下 **Deploy** 以便開始部署平台設定。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 在 FTD CLI 中驗證 FTD Syslog 設定。登入FTD的管理介面，並輸入 **system support diagnostic-cli** 命令，以便通過控制檯連線到診斷CLI。

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

><Press Enter>
firepower# sh run logging
logging enable
logging console emergencies
logging buffered debugging
logging host inside 192.168.0.192
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
logging permit-hostdown
```

- 確保可以從 FTD 連線 Syslog 伺服器。透過SSH登入FTD管理介面，並驗證與 **ping** 指令。

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)

> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# ping 192.168.0.192
```

- 您可以進行封包擷取，以驗證 FTD 和 Syslog 伺服器之間的連線。透過SSH登入FTD管理介面，並輸入命令 **system support diagnostic-cli**.如需封包擷取指令，請參閱使用 CLI 和 ASDM 進行 ASA 封包擷取的設定範例。
- 確保已順利套用原則部署。

相關資訊

- 適用於 ASA 的 Cisco Firepower Threat Defense 快速入門指南
- 技術支援與文件 - Cisco Systems

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）。