透過FDM設定和測試AMP檔案原則

目錄

簡介

本文檔介紹如何透過Firepower裝置管理器(FDM)配置和測試高級惡意軟體防護(AMP)檔案策略。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower裝置管理器(FDM)
- Firepower Threat Defense (FTD)

採用元件

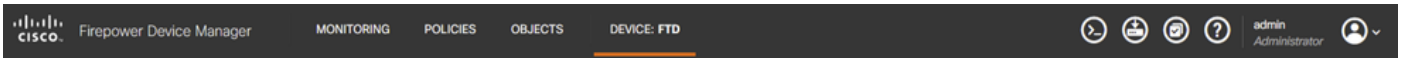
- 透過FDM管理的Cisco虛擬FTD 7.0版
- 評估許可證(評估許可證用於演示目的。思科建議獲取並使用有效的許可證)

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。

說明

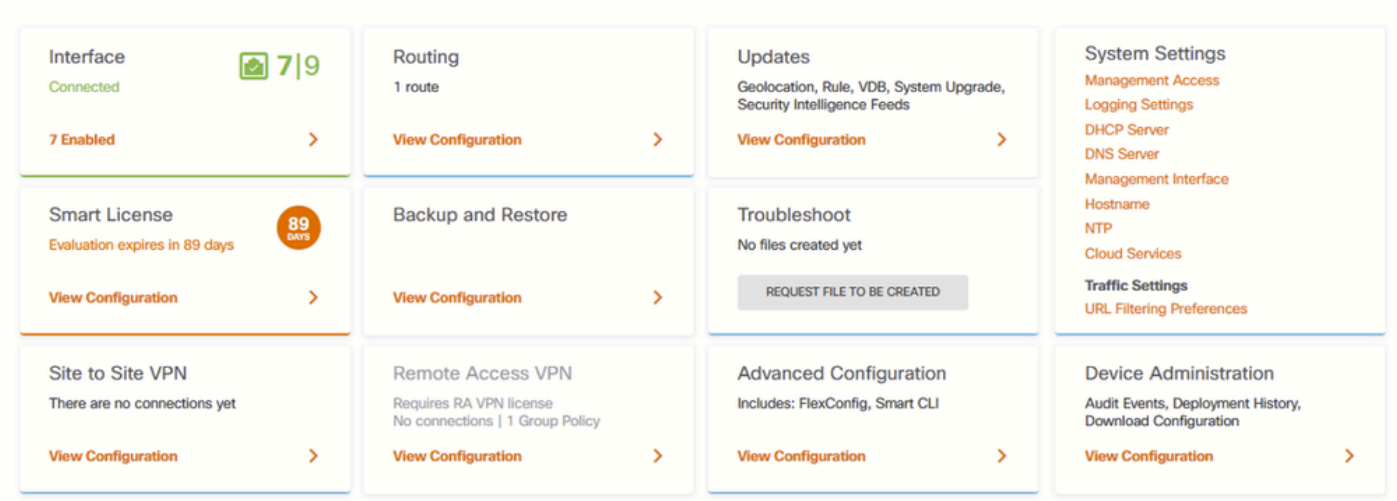
授權

1. 要啟用惡意軟體許可證，請導航到FDM GUI上的DEVICE頁。



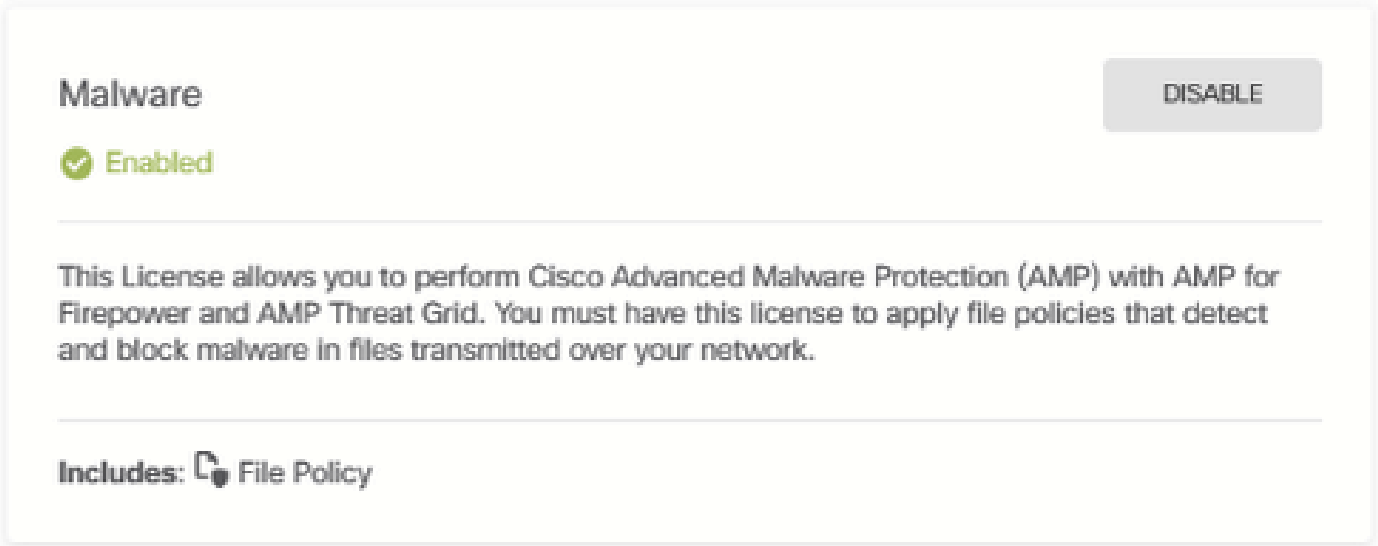
FDM裝置標籤

2. 找到標籤為Smart License的框，然後按一下View Configuration。



FDM裝置頁面

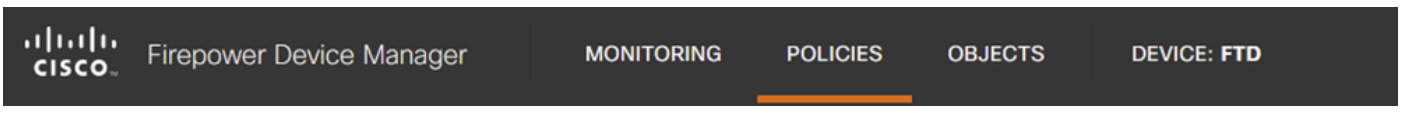
3. 啟用標籤為Malware的許可證。



惡意軟體許可證

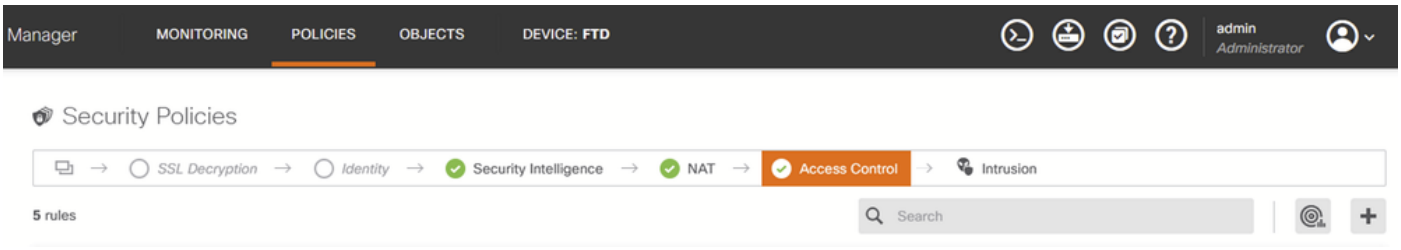
組態

1. 導覽至FDM上的POLICIES頁面。



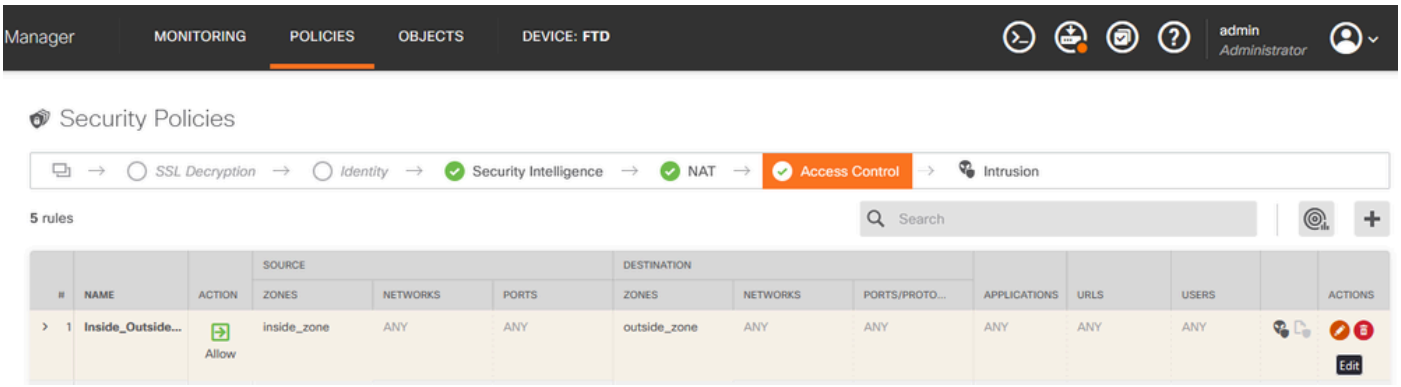
FDM原則標籤

2. 在安全策略下，導航到訪問控制部分。



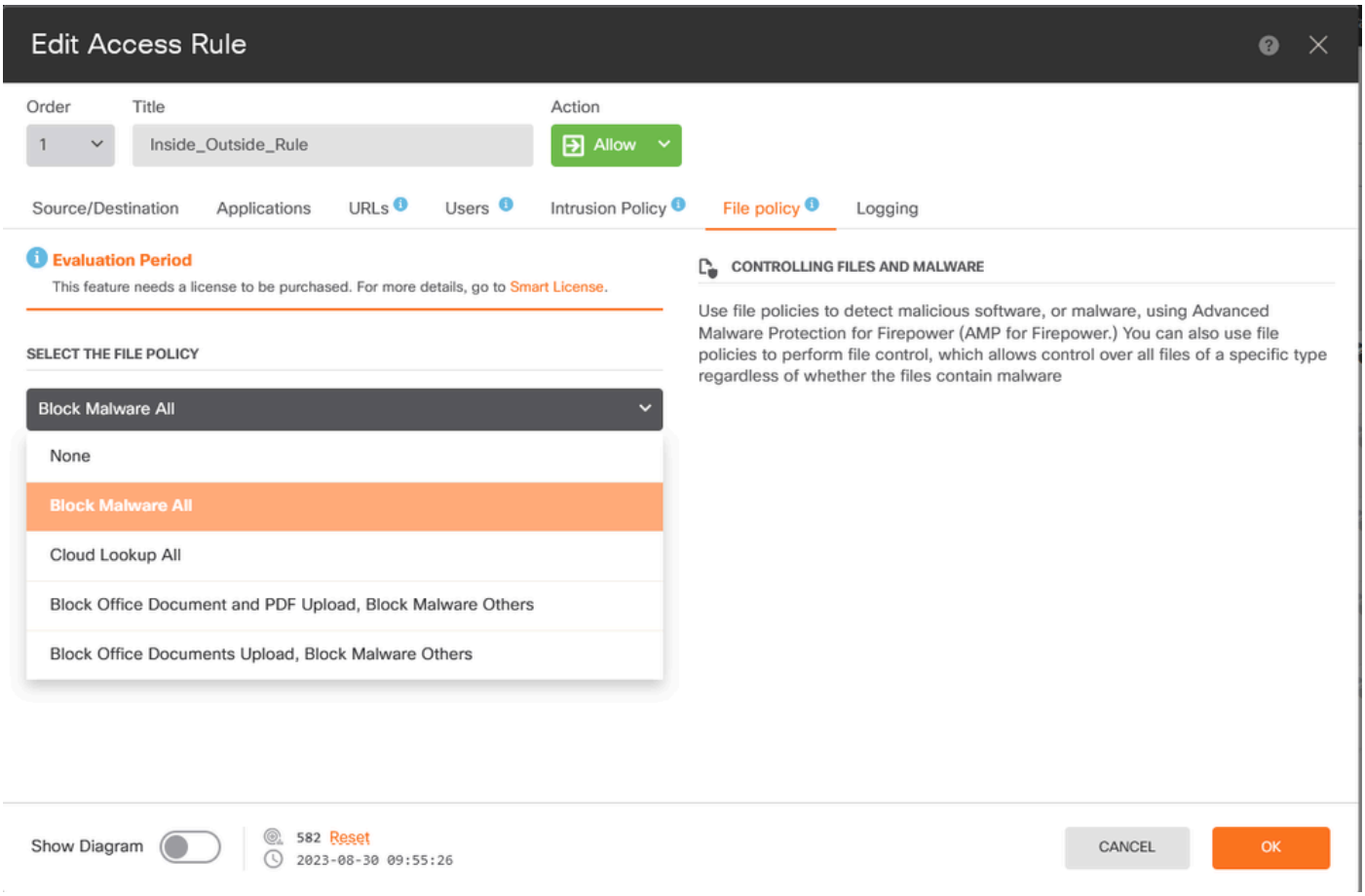
FDM存取控制標籤

3. 查詢或建立訪問規則以配置檔案策略。點選訪問規則編輯器。有關如何建立訪問規則的說明，請參閱此連結。



FDM存取控制規則

4. 按一下訪問規則上的檔案策略部分，然後從下拉選單中選擇首選的檔案策略選項。按一下OK以儲存對規則的更改。



FDM存取控制規則檔案原則標籤

5. 透過檢查檔案策略圖示是否已啟用，確認已將檔案策略應用於訪問規則。

檔案

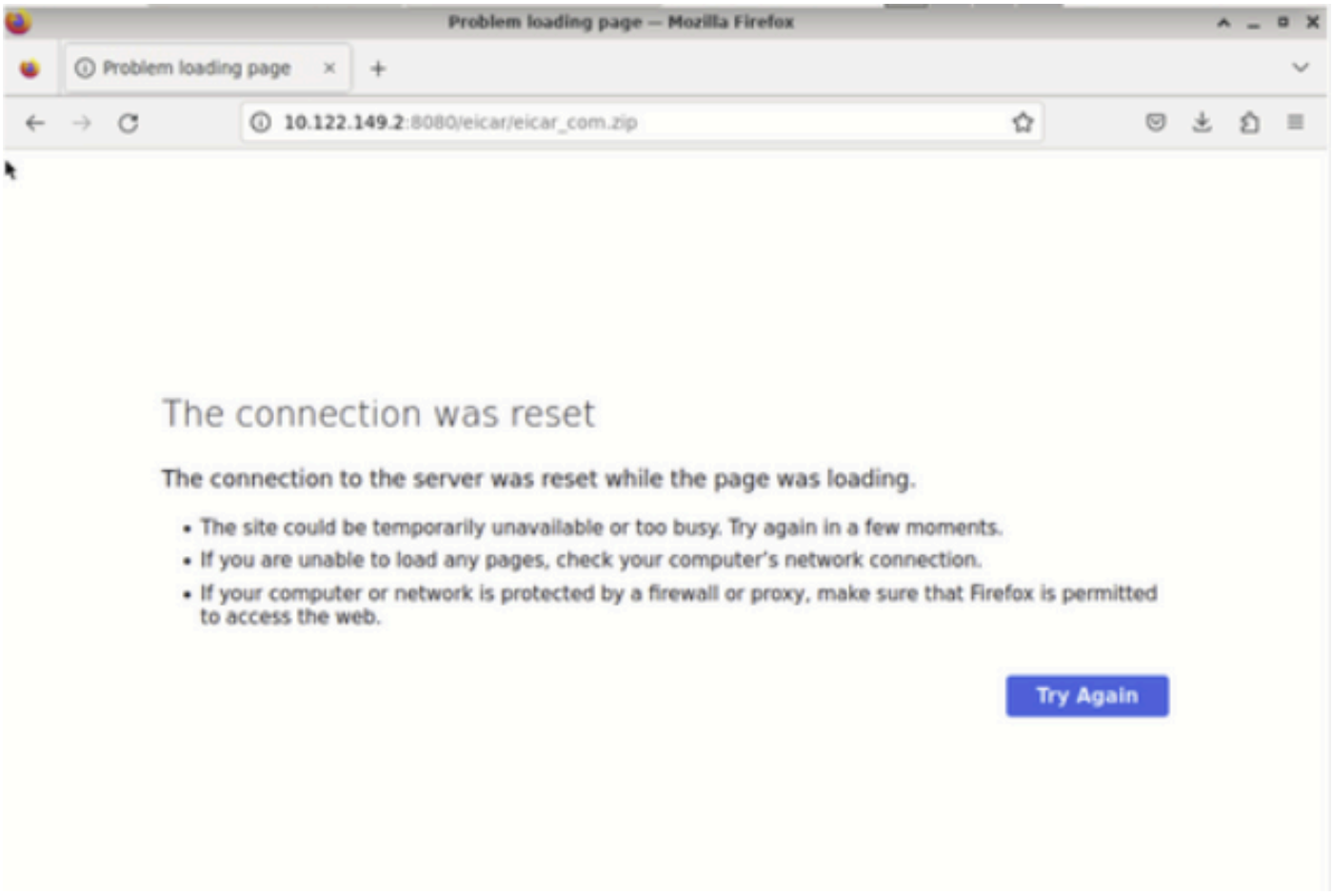
文件策略圖示已啟用

6.儲存並部署更改到受管裝置。

測試

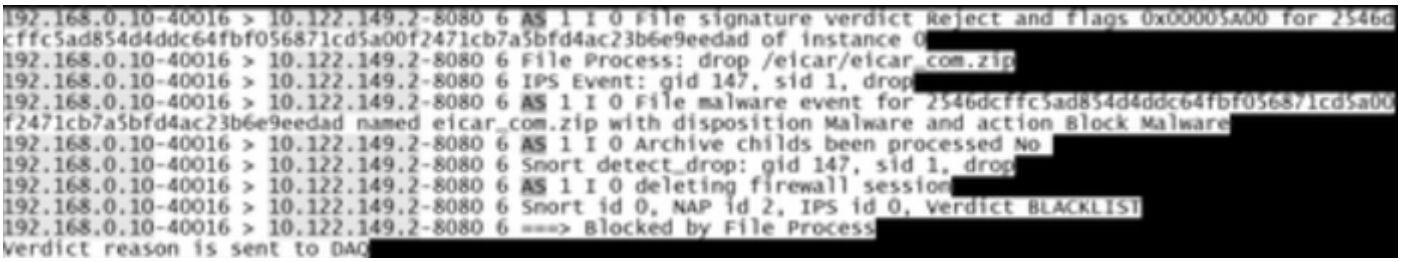
要驗證用於惡意軟體防護的配置檔案策略是否有效，請使用以下測試方案嘗試從終端主機的Web瀏覽器下載惡意軟體測試檔案。

如螢幕截圖所示，嘗試從Web瀏覽器下載惡意軟體測試檔案失敗。



瀏覽器下載測試

從FTD CLI中，系統支援追蹤顯示檔案下載被檔案程式封鎖。有關如何透過FTD CLI運行系統支援跟蹤的說明，請參閱此連結。



系統支援追蹤測試

這確認檔案策略配置成功阻止了惡意軟體。

疑難排解

如果在使用以前的配置時惡意軟體未被成功阻止，請參閱以下故障排除建議：

1. 驗證惡意軟體許可證未過期。

2. 確認訪問控制規則的目標流量是否正確。

3. 確認選定的檔案策略選項對於目標流量和所需惡意軟體防護是正確的。

如果問題仍無法解決，請與Cisco TAC聯絡以獲取其他支援。

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）。