# 刪除Windows上的FireAMP快取和歷史記錄檔案

## 目錄



## 簡介

本文提供一些需要在FireAMP for Endpoints中刪除資料庫檔案的方案，並描述了在必要時刪除這些檔案的正確過程。面向終端的FireAMP會保留其最近資料庫檔案中的檔案檢測和處置的記錄。在某些情況下，思科支援工程師可能會要求您移除某些資料庫檔案以排解問題。

> **警告**：只有在思科技術支援人員指示的情況下才能刪除資料庫檔案。

## 用於快取記憶體和歷史記錄的資料庫檔案

### 目的

快取記憶體資料庫檔案維護檔案的已知性質。歷史資料庫檔案跟蹤所有FireAMP檔案檢測，以及源檔名和SHA256值。

將阻止清單新增到策略並更新聯結器時，給定檔案的行為不會立即更改。這是因為快取已識別出該檔案不是惡意檔案。因此，阻止清單不會更改或覆蓋它。當快取在策略中每次過期且執行新查詢時，處置情況會更改 — 首先根據您的清單，然後根據雲執行。

### 刪除原因

如果從目錄中刪除歷史記錄資料庫和快取記憶體資料庫檔案，則在FireAMP服務重新啟動時重新建立它們。在某些情況下，可能需要從FireAMP目錄中刪除這些檔案。例如，如果要測試給定檔案的簡單自定義檢測或應用程式阻止清單。

資料庫可能會損壞，從而使您無法開啟或檢視資料庫中的檢測專案。或者，如果系統上的資料庫已

損壞，則可能導致FireAMP聯結器服務出錯，例如無法啟動聯結器或整體系統效能下降。在這些情況下，您可能希望從聯結器清除歷史記錄檔案，這樣可以避免效能相關問題被損壞，並能夠捕獲新日誌以供診斷。

## 標識資料庫檔案

在Microsoft Windows上，這些檔案通常位於C:\Program Files\Sourcefire\fireAMP或C:\Program Files\Cisco\AMP。

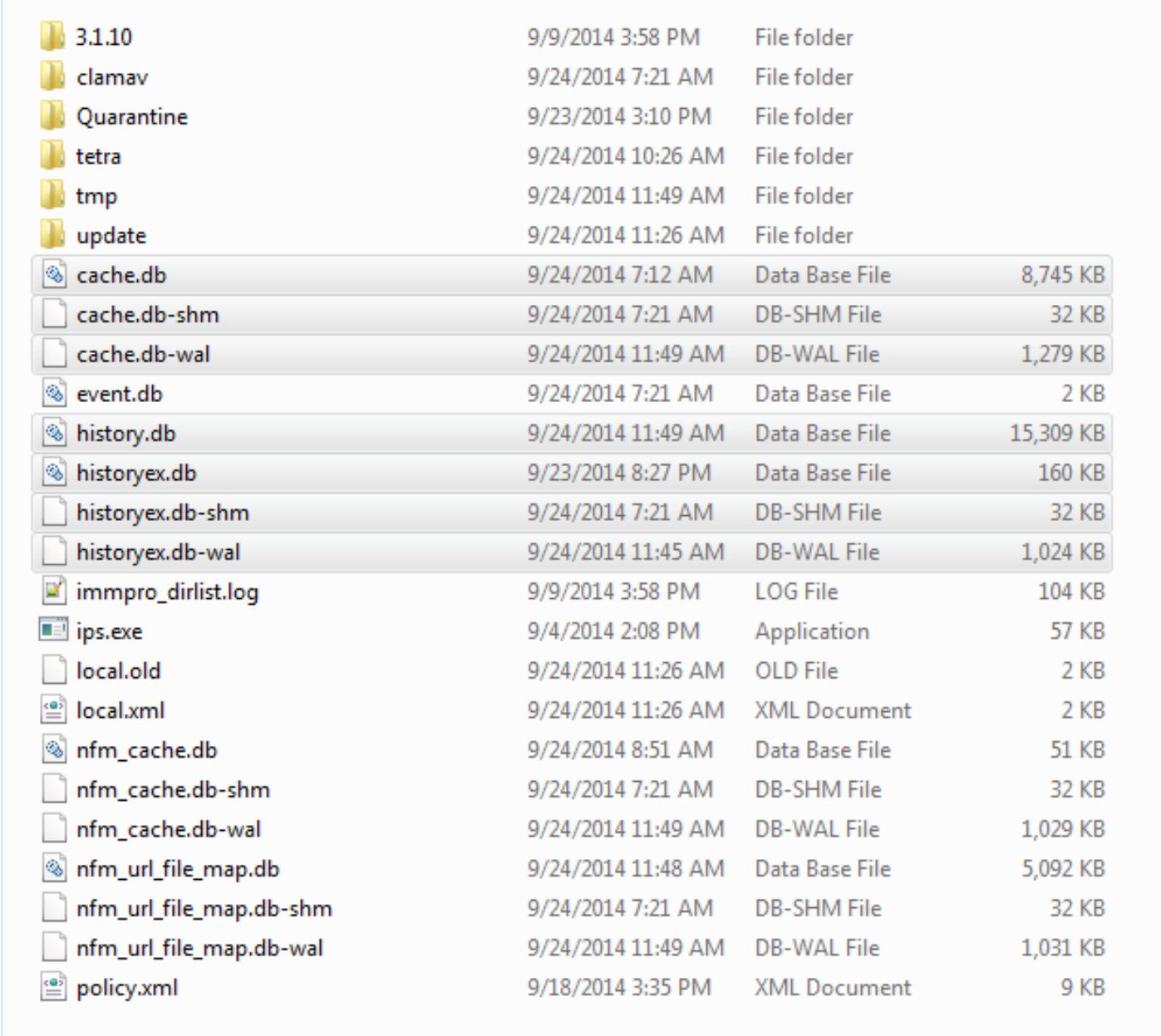
快取資料庫檔案的名稱為：

```
cache.db
cache.db-shm
cache.db-wal
```

歷史記錄資料庫檔案的名稱為：

```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

此螢幕截圖顯示Windows檔案資源管理器上的檔案：



| | | | |
|---|---|---|---|
| 3.1.10 | 9/9/2014 3:58 PM | File folder | |
| clamav | 9/24/2014 7:21 AM | File folder | |
| Quarantine | 9/23/2014 3:10 PM | File folder | |
| tetra | 9/24/2014 10:26 AM | File folder | |
| tmp | 9/24/2014 11:49 AM | File folder | |
| update | 9/24/2014 11:26 AM | File folder | |
| cache.db | 9/24/2014 7:12 AM | Data Base File | 8,745 KB |
| cache.db-shm | 9/24/2014 7:21 AM | DB-SHM File | 32 KB |
| cache.db-wal | 9/24/2014 11:49 AM | DB-WAL File | 1,279 KB |
| event.db | 9/24/2014 7:21 AM | Data Base File | 2 KB |
| history.db | 9/24/2014 11:49 AM | Data Base File | 15,309 KB |
| historyex.db | 9/23/2014 8:27 PM | Data Base File | 160 KB |
| historyex.db-shm | 9/24/2014 7:21 AM | DB-SHM File | 32 KB |
| historyex.db-wal | 9/24/2014 11:45 AM | DB-WAL File | 1,024 KB |
| immpro_dirlist.log | 9/9/2014 3:58 PM | LOG File | 104 KB |
| ips.exe | 9/4/2014 2:08 PM | Application | 57 KB |
| local.old | 9/24/2014 11:26 AM | OLD File | 2 KB |
| local.xml | 9/24/2014 11:26 AM | XML Document | 2 KB |
| nfm_cache.db | 9/24/2014 8:51 AM | Data Base File | 51 KB |
| nfm_cache.db-shm | 9/24/2014 7:21 AM | DB-SHM File | 32 KB |
| nfm_cache.db-wal | 9/24/2014 11:49 AM | DB-WAL File | 1,029 KB |
| nfm_url_file_map.db | 9/24/2014 11:48 AM | Data Base File | 5,092 KB |
| nfm_url_file_map.db-shm | 9/24/2014 7:21 AM | DB-SHM File | 32 KB |
| nfm_url_file_map.db-wal | 9/24/2014 11:49 AM | DB-WAL File | 1,031 KB |
| policy.xml | 9/18/2014 3:35 PM | XML Document | 9 KB |

# 刪除資料庫檔案的過程

## 第1步：停止FireAMP聯結器服務

您可以通過多種方式停止FireAMP聯結器服務：

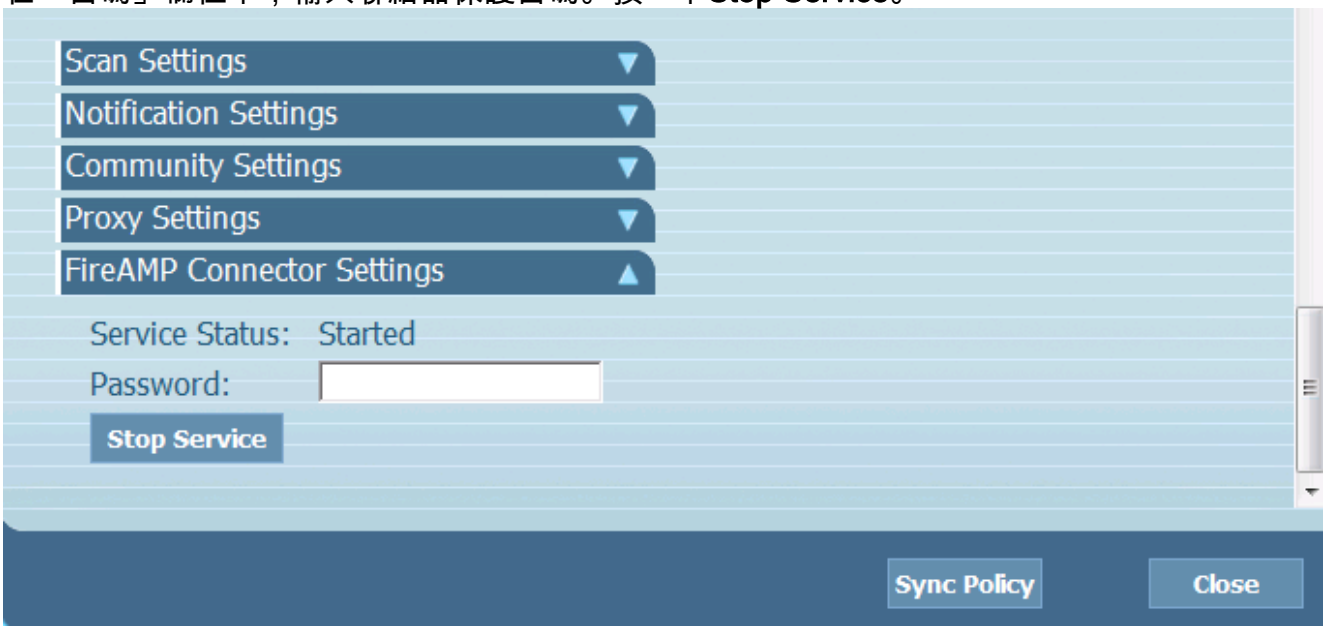
- FireAMP聯結器服務的使用者介面(UI)
- Windows服務控制檯
- 管理員的命令提示符

### 使用者介面

**附註**：如果啟用了聯結器保護，則必須使用UI以停止FireAMP聯結器服務。

1. 從托盤中開啟UI，然後按一下「**Settings**」。
2. 滾動到底部，展開「**FireAMP Connector Settings**」。

3. 在「密碼」欄位中，輸入聯結器保護密碼。按一下**Stop Service**。

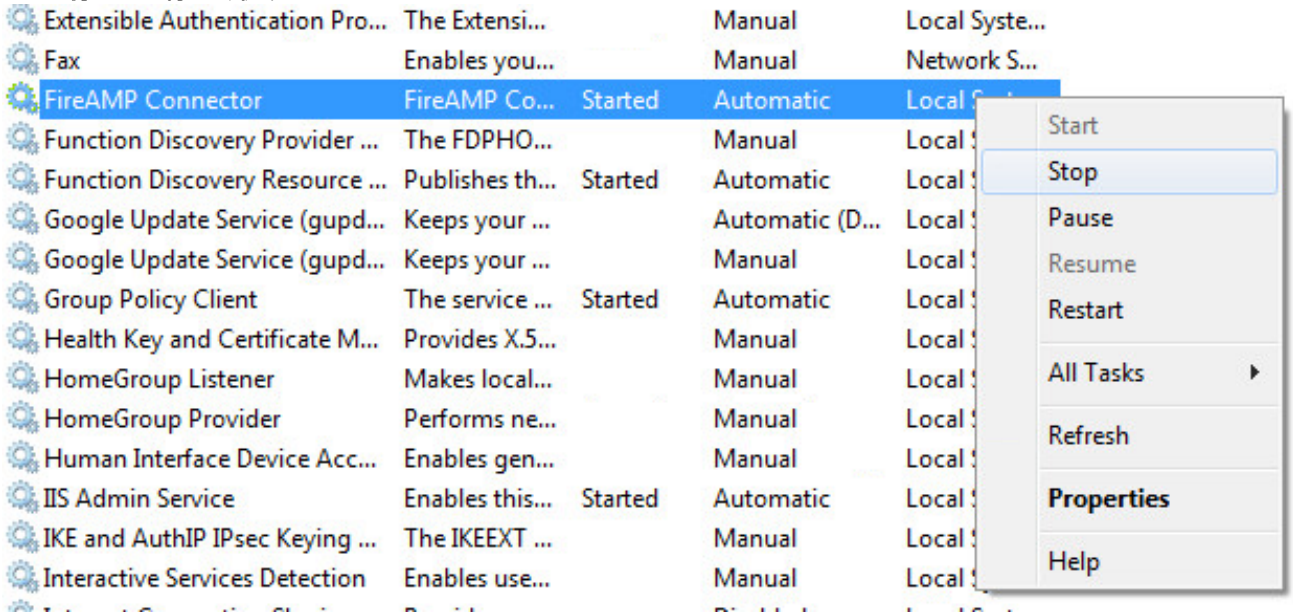



**服務主控台**

**附註**：要在「服務」控制檯中停止和啟動服務，您需要具有管理員許可權。

要從服務控制檯停止FireAMP聯結器服務，請完成以下步驟：

1. 導航到**開始選單**。
2. 輸入**services.msc**，然後按**Enter**。將開啟「服務」控制檯。
3. 選擇**FireAMP聯結器**服務，然後按一下右鍵服務名稱。
4. 選擇**停止**可停止服務。

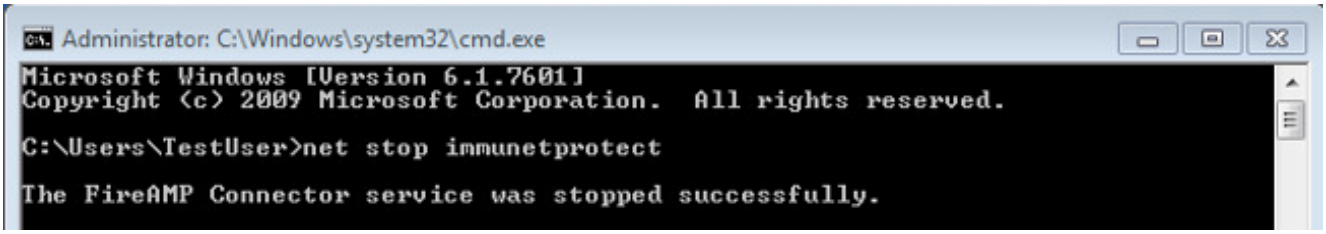



**命令提示符**

要從管理員的命令提示符停止FireAMP聯結器服務，請完成以下步驟：

1. 導航到**開始選單**。

2. 輸入**cmd.exe**，然後按**Enter**。將會開啟命令提示符視窗。
3. 輸入**net stop immunetprotect**命令。如果您使用的是5.0.1版或更高版本，請輸入**wmic service，其中「name like 'immunetprotect%'」呼叫startservice**命令。 此螢幕截圖顯示了成功停止的服務的示例
：




## 第2步：刪除所需的資料庫檔案

### 快取資料庫檔案

服務停止後，您可以刪除以下三個快取檔案：

> **警告：**如果沒有刪除所有相關的快取資料庫檔案，則可能會對重建的資料庫產生快取問題。因此，服務可能無法啟動或者您可能遇到服務效能下降的情況。

```
cache.db
cache.db-shm
cache.db-wal
```

### 歷史資料庫檔案

服務停止後，請刪除以下歷史記錄資料庫檔案：

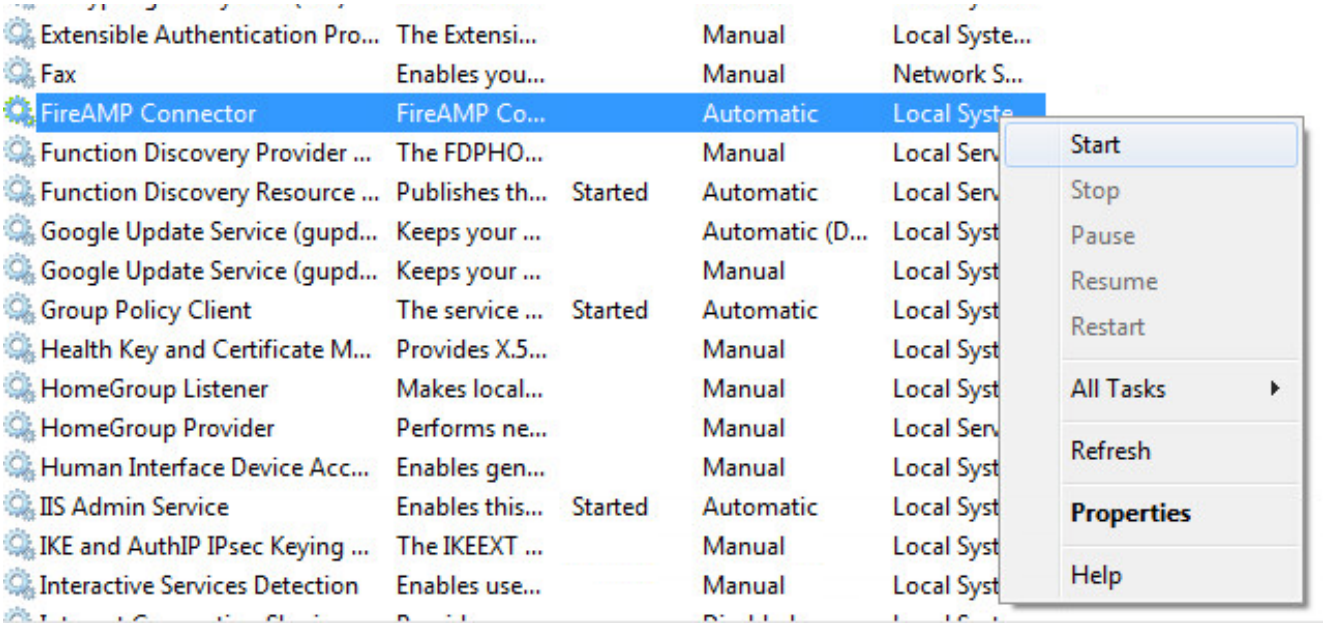
> **警告：**如果沒有刪除所有相關的歷史記錄資料庫檔案，則可能會對重新建立的資料庫產生快取問題。因此，服務可能無法啟動或者您可能遇到服務效能下降的情況。

```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

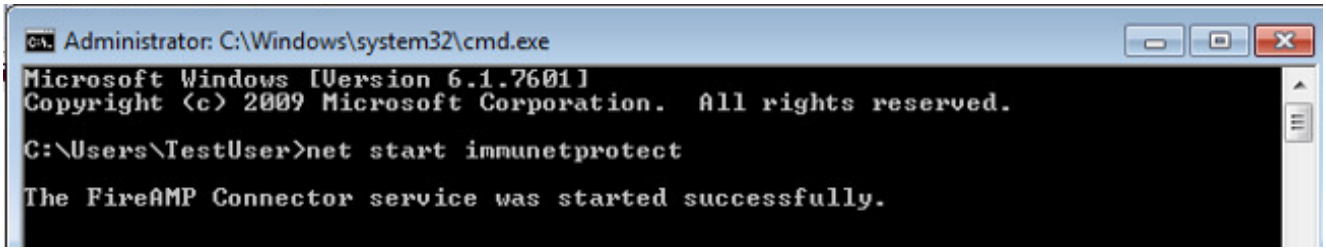
## 步驟3:啟動FireAMP聯結器服務

若要啟動FireAMP聯結器服務，請完成以下步驟：

1. 導航到**開始選單**。
2. 輸入**services.msc**，然後按**Enter**。將開啟「服務」控制檯。
3. 選擇**FireAMP Connector**服務並按一下右鍵該服務名稱。
4. 選擇**Start**以啟動服務。




或者，在管理員的命令提示符下，可以輸入**net start immunetprotect**命令。如果您使用的是5.0.1版或更高版本，請輸入**wmic service，其中「name like 'immunetprotect%'」呼叫startservice**命令。此螢幕截圖顯示了成功啟動的服務示例：




重新啟動服務後，將建立一組新的資料庫檔案。現在應為您提供一個包含當前白名單、阻止清單、排除項等的FireAMP聯結器的新例項。