

Entfernen des FireAMP-Cache und der Verlaufsdateien unter Windows

Inhalt

[Einführung](#)

[Datenbankdateien für Cache und Verlauf](#)

[Zweck](#)

[Gründe für das Entfernen](#)

[Identifizieren der Datenbankdateien](#)

[Verfahren zum Entfernen von Datenbankdateien](#)

[Schritt 1: Beenden Sie den FireAMP Connector-Dienst.](#)

[Benutzeroberfläche](#)

[Services-Konsole](#)

[Eingabeaufforderung](#)

[Schritt 2: Löschen der erforderlichen Datenbankdateien](#)

[Cache-Datenbankdateien](#)

[Verlaufsdatenbankdateien](#)

[Schritt 3: Starten Sie den FireAMP Connector-Dienst.](#)

Einführung

Dieses Dokument enthält einige Szenarien, die das Entfernen von Datenbankdateien in FireAMP für Endgeräte erfordern, und beschreibt ein geeignetes Verfahren, um diese bei Bedarf zu entfernen. FireAMP für Endgeräte speichert die neuesten Dateierkennungen und -status in Datenbankdateien. In bestimmten Fällen bittet Sie ein Cisco Support Engineer möglicherweise, einige Datenbankdateien zu entfernen, um ein Problem zu beheben.

Warnung: Sie können eine Datenbankdatei nur entfernen, wenn Sie vom technischen Support von Cisco dazu aufgefordert werden.

Datenbankdateien für Cache und Verlauf

Zweck

In den Cache-Datenbankdateien werden die bekannten Eigenschaften für Dateien beibehalten. Die Verlaufsdatenbankdateien verfolgen alle FireAMP-Dateierkennungen sowie die Namen der Quelldateien und die SHA256-Werte.

Wenn Sie einer Richtlinie eine Blockliste hinzufügen und den Connector aktualisieren, ändert sich das Verhalten für eine bestimmte Datei nicht sofort. Der Grund hierfür ist, dass der Cache bereits erkannt hat, dass die Datei nicht schädlich ist. Daher wird sie nicht von der Blockliste geändert oder überschrieben. Die Einstufung ändert sich, wenn der Cache bei jedem Ablaufen der Richtlinie abgelaufen ist und eine neue Suche durchgeführt wird - zuerst gegen Ihre Listen und

anschließend gegen die Cloud.

Gründe für das Entfernen

Wenn die Verlaufsdatenbank und die Cache-Datenbankdateien aus einem Verzeichnis entfernt werden, werden sie beim Neustart des FireAMP-Dienstes frisch neu erstellt. In bestimmten Fällen kann es erforderlich sein, diese Dateien aus dem FireAMP-Verzeichnis zu entfernen. Wenn Sie z. B. eine einfache benutzerdefinierte Erkennung oder eine Anwendungsblockliste für eine bestimmte Datei testen möchten.

Es ist möglich, dass eine Datenbank beschädigt wird, sodass Sie die Erkennungen in einer Datenbank nicht öffnen oder anzeigen können. Wenn die Datenbank in einem System beschädigt ist, kann sie auch Fehler im FireAMP Connector-Dienst verursachen, wie z. B. das Nichtstarten des Connectors oder die Beeinträchtigung der Gesamtsystemleistung. In diesen Fällen können Sie die Verlaufsdateien aus dem Connector löschen, um leistungsbezogene Probleme durch Korruption zu vermeiden und neue Protokolle zur Diagnose aufzeichnen zu können.

Identifizieren der Datenbankdateien

Unter Microsoft Windows finden Sie diese Dateien in der Regel unter C:\Program Files\Sourcefire\fireAMP or C:\Program Files\Cisco\AMP.

Der Name der Cache-Datenbankdateien lautet:

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

Der Name der Verlaufsdatenbankdateien lautet:

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

Dieser Screenshot zeigt die Dateien im Windows-Datei-Explorer:

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

Verfahren zum Entfernen von Datenbankdateien

Schritt 1: Beenden Sie den FireAMP Connector-Dienst.

Sie können den FireAMP Connector-Dienst auf verschiedene Weise beenden:

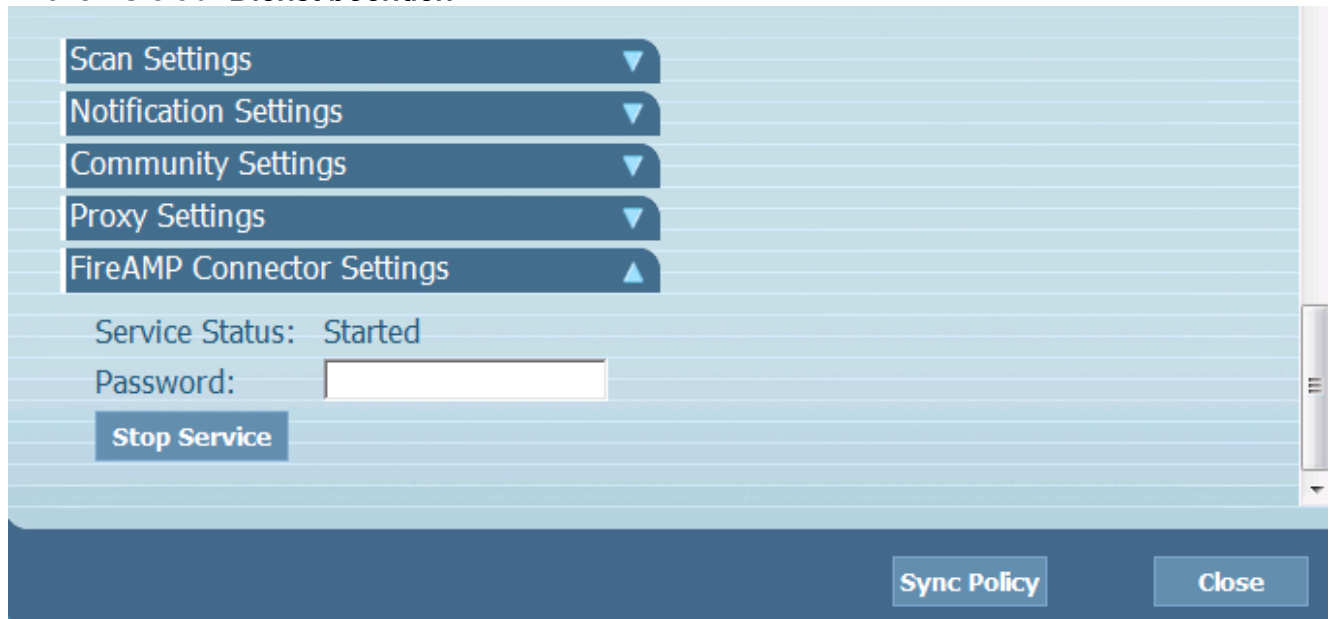
- Benutzeroberfläche (UI) des FireAMP Connector-Service
- Windows Services-Konsole
- Eingabeaufforderung des Administrators

Benutzeroberfläche

Hinweis: Wenn der Connector-Schutz aktiviert ist, müssen Sie die Benutzeroberfläche verwenden, um den FireAMP Connector-Dienst zu beenden.

1. Öffnen Sie die Benutzeroberfläche im Fach, und klicken Sie auf **Einstellungen**.

2. Blättern Sie nach unten, und erweitern Sie die **FireAMP Connector-Einstellungen**.
3. Geben Sie im Feld Password (Kennwort) das Kennwort für den Verbindungsschutz ein. Klicken Sie auf **Dienst beenden**.

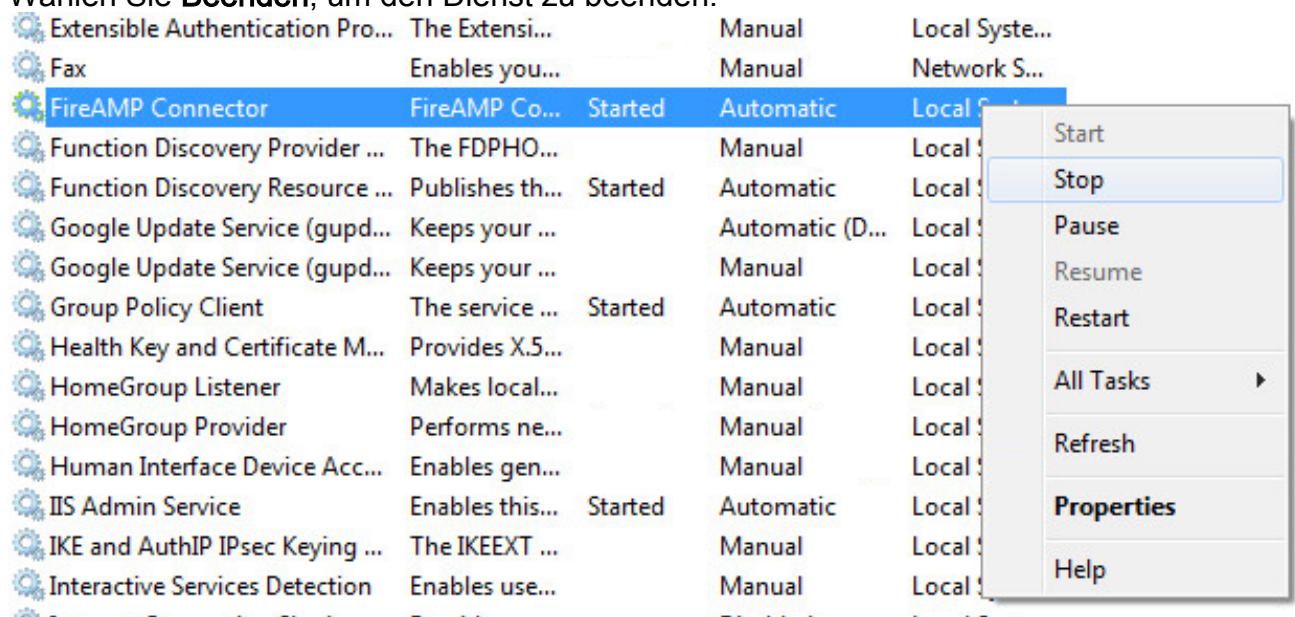


Services-Konsole

Hinweis: Um Dienste in der Konsole Dienste anzuhalten und zu starten, benötigen Sie Administratorrechte.

Gehen Sie wie folgt vor, um den FireAMP Connector-Dienst von der Konsole Dienste zu beenden:

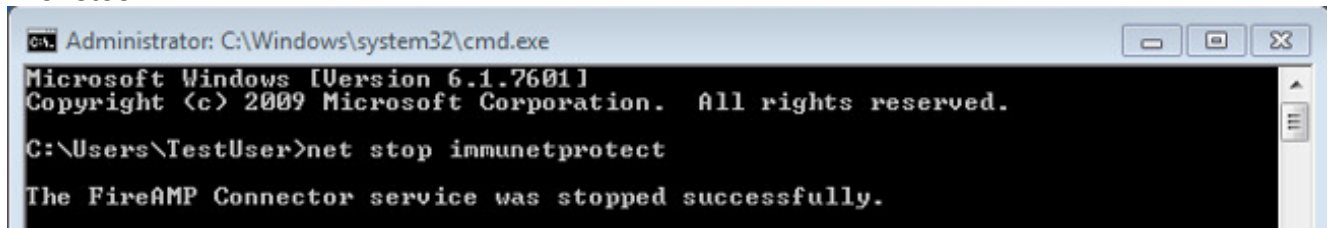
1. Navigieren Sie zum **Startmenü**.
2. Geben Sie **services.msc** ein, und drücken Sie die **Eingabetaste**. Die Konsole Dienste wird geöffnet.
3. Wählen Sie den **FireAMP Connector-Service** aus, und klicken Sie mit der rechten Maustaste auf den Dienstnamen.
4. Wählen Sie **Beenden**, um den Dienst zu beenden.



Eingabeaufforderung

Gehen Sie wie folgt vor, um den FireAMP Connector-Dienst über die Eingabeaufforderung eines Administrators zu beenden:

1. Navigieren Sie zum **Startmenü**.
2. Geben Sie **cmd.exe** ein, und drücken Sie die **Eingabetaste**. Ein Eingabeaufforderungs Fenster wird geöffnet.
3. Geben Sie den Befehl **net stop immunetprotect** ein. Wenn Sie Version 5.0.1 oder höher haben, geben Sie den **WiSM-Dienst ein, bei dem "name like 'immunetprotect%'"** den Befehl **startservice** stattdessen **aufruft**. Dieser Screenshot zeigt ein Beispiel für den erfolgreichen Stopp des Dienstes:



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\TestUser>net stop immunetprotect

The FireAMP Connector service was stopped successfully.
```

Schritt 2: Löschen der erforderlichen Datenbankdateien

Cache-Datenbankdateien

Wenn der Dienst beendet wurde, können Sie die folgenden drei Cache-Dateien löschen:

Warnung: Wenn Sie nicht alle zugehörigen Cache-Datenbankdateien löschen, können Zwischenspeicherungsprobleme mit der neu erstellten Datenbank erstellt werden. Daher kann es vorkommen, dass der Dienst nicht gestartet wird, oder dass die Leistung des Dienstes beeinträchtigt ist.

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

Verlaufsdatenbankdateien

Wenn der Dienst beendet ist, entfernen Sie die folgenden Datenbankdateien für die Versionsgeschichte:

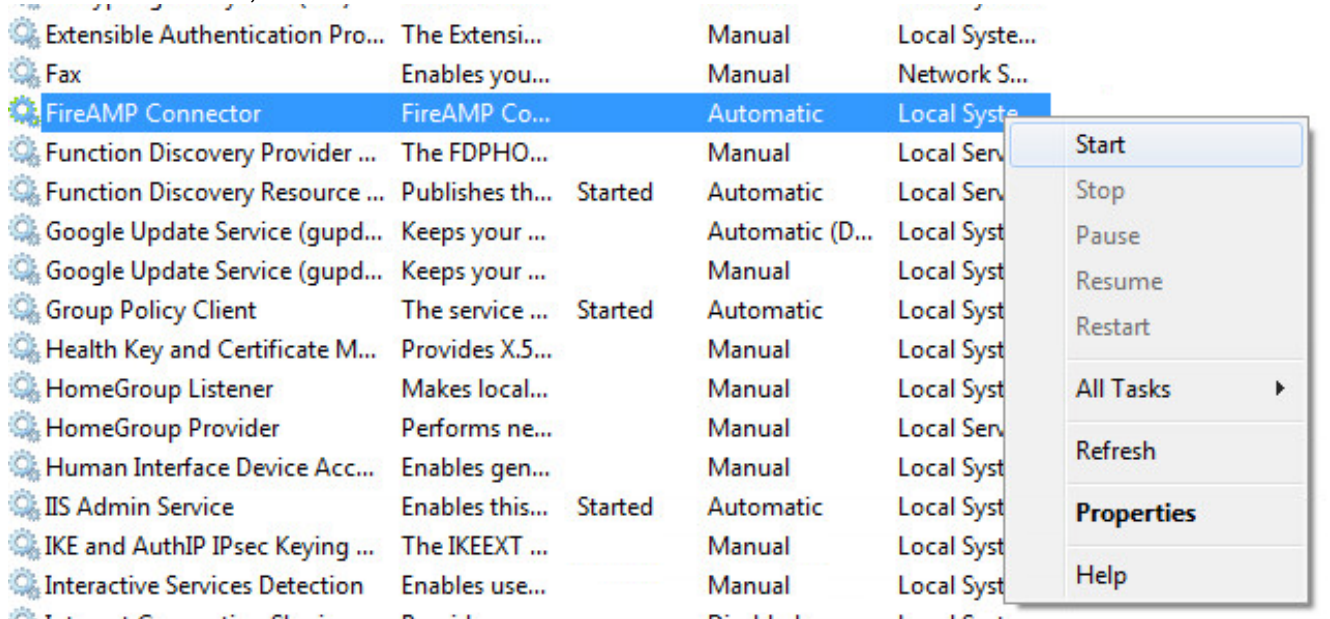
Warnung: Wenn Sie nicht alle verknüpften Verlaufsdatenbankdateien löschen, können Zwischenspeicherungsprobleme mit der neu erstellten Datenbank erstellt werden. Daher kann es vorkommen, dass der Dienst nicht gestartet wird, oder dass die Leistung des Dienstes beeinträchtigt ist.

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

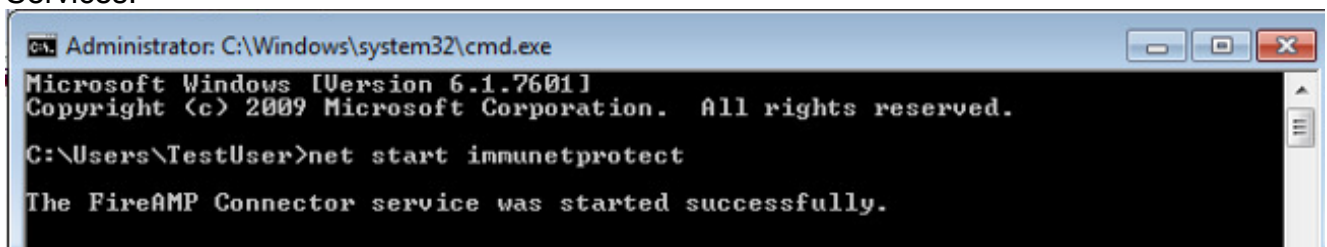
Schritt 3: Starten Sie den FireAMP Connector-Dienst.

Gehen Sie wie folgt vor, um den FireAMP Connector-Dienst zu starten:

1. Navigieren Sie zum **Startmenü**.
2. Geben Sie **services.msc** ein, und drücken Sie die **Eingabetaste**. Die Konsole Dienste wird geöffnet.
3. Wählen Sie den **FireAMP Connector**-Service aus, und klicken Sie mit der rechten Maustaste auf den Dienstenamen.
4. Wählen Sie **Start**, um den Dienst zu starten.



Alternativ können Sie an der Eingabeaufforderung des Administrators den Befehl **net start immunetprotect** eingeben. Wenn Sie Version 5.0.1 oder höher haben, geben Sie den **WISM-Dienst** ein, bei dem "name like 'immunetprotect%'" den Befehl **startservice** stattdessen aufruft. Dieser Screenshot zeigt ein Beispiel für den erfolgreichen Start des Services:



Nach dem Neustart der Dienste wird ein neuer Satz von Datenbankdateien erstellt. Damit erhalten Sie eine neue Instanz des FireAMP Connectors mit aktuellen Whitelists, Blocklisten, Ausschlüssen usw.