# Suppression du cache de FireAMP et des fichiers historiques sur Windows

## Contenu



## Introduction

Ce document fournit quelques scénarios qui exigent une suppression des fichiers de base de données dans FireAMP pour des points finaux et décrit une procédure appropriée pour les retirer si nécessaire. Le FireAMP pour des points finaux met à jour un enregistrement de ses détections et dispositions récentes de fichier dans des fichiers de base de données. Dans certains cas, un ingénieur d'assistance technique de Cisco pourrait te demander de retirer certains des fichiers de base de données afin de dépanner une question.

> **Avertissement :** Vous pouvez retirer un fichier de base de données seulement s'instruit par le support technique de Cisco.

## Fichiers de base de données pour le cache et l'historique

### But

Les fichiers de base de données de cache mettent à jour les dispositions connues pour des fichiers. Les fichiers de base de données dépistent toutes les détections de fichier de FireAMP, avec des noms de fichier source et des valeurs SHA256.

Quand vous ajoutez une liste de bloc à une stratégie et mettez à jour le connecteur, le comportement pour un fichier donné ne change pas immédiatement. C'est parce que le cache l'a déjà identifié que le fichier n'est pas malveillant. En soi, il ne sera pas changé ou sera ignoré par votre liste de bloc. La disposition change quand le cache est expiré par temps dans votre stratégie

et une nouvelle consultation est exécutée - d'abord contre vos listes et ultérieurement contre le nuage.

## Raisons pour la suppression

Si les fichiers de base de données de base de données et de cache d'historique sont retirés à partir d'un répertoire, ils sont frais recréé quand les reprises de service de FireAMP. Dans certain l'enferme pourrait être nécessaire pour retirer ces fichiers à partir du répertoire de FireAMP. Par exemple, si vous voulez tester une détection faite sur commande simple ou une liste de bloc d'application pour un fichier donné.

Il est possible qu'une base de données pourrait devenir corrompue, qui vous rend incapable d'ouvrir ou visualiser les détections dans une base de données. Alternativement, si la base de données est corrompue sur un système il peut entraîner des erreurs dans le service de connecteur de FireAMP tel que l'incapacité de commencer le connecteur ou la dégradation de la performance globale du système. Dans ces exemples vous pourriez vouloir effacer les fichiers historiques du connecteur de sorte que vous puissiez éviter des problèmes relatifs aux performances de la corruption et pouvoir capturer de nouveaux logs pour le diagnostic.

## Identifiez les fichiers de base de données

Sur Microsoft Windows, ces fichiers sont typiquement localisés chez C:\Program Files\Sourcefire\fireAMP ou C:\Program Files\Cisco\AMP.

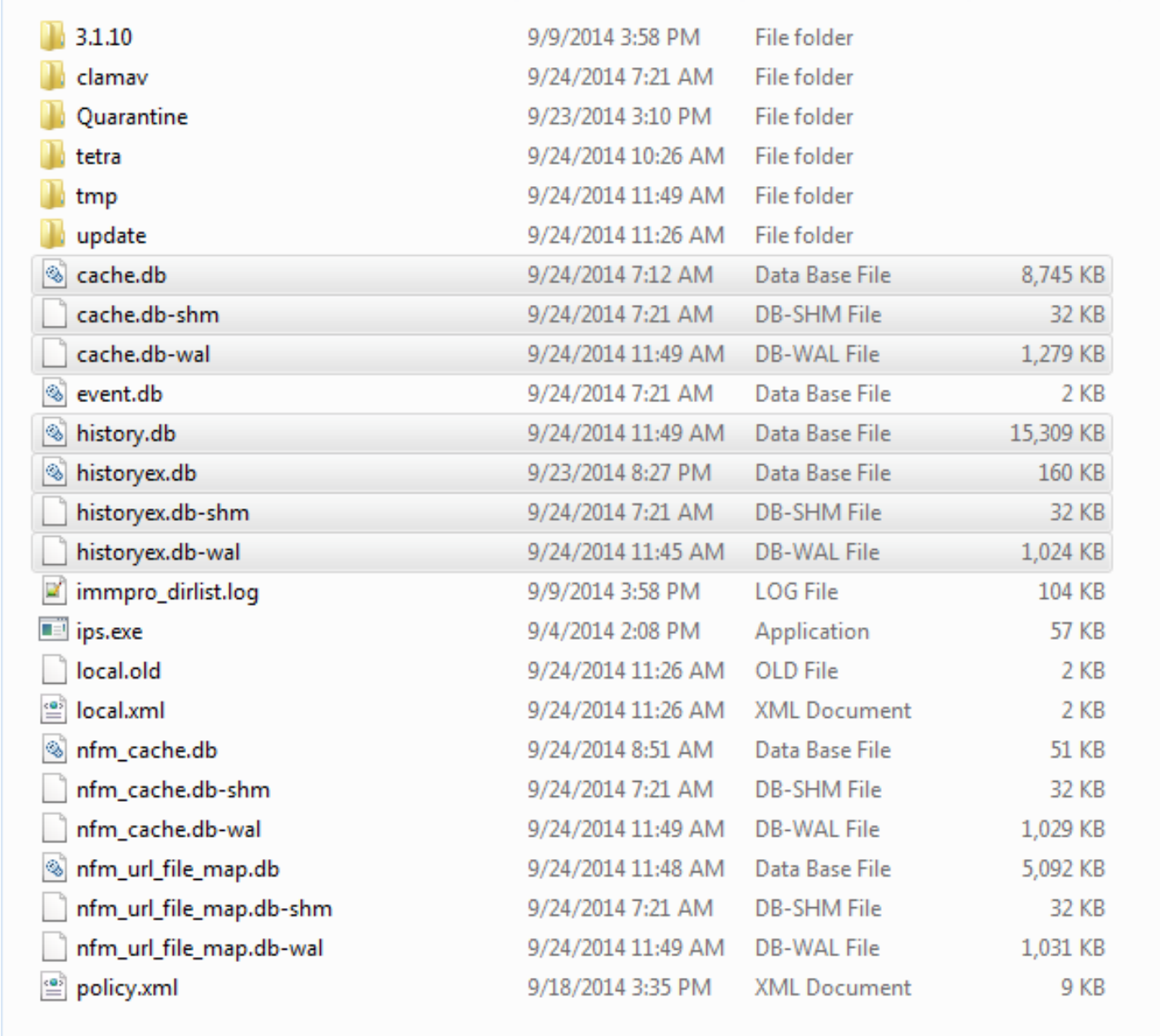
Le nom des fichiers de base de données de cache sont :

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

Le nom des fichiers de base de données d'historique sont :

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

Ce tir d'écran affiche les fichiers sur l'explorateur de fichier Windows :



| | | | |
|---|---|---|---|
| 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 |

# Procédure pour retirer des fichiers de base de données

## Étape 1 : Arrêtez le service de connecteur de FireAMP

Vous pouvez arrêter manières de service de connecteur de FireAMP les diverses :

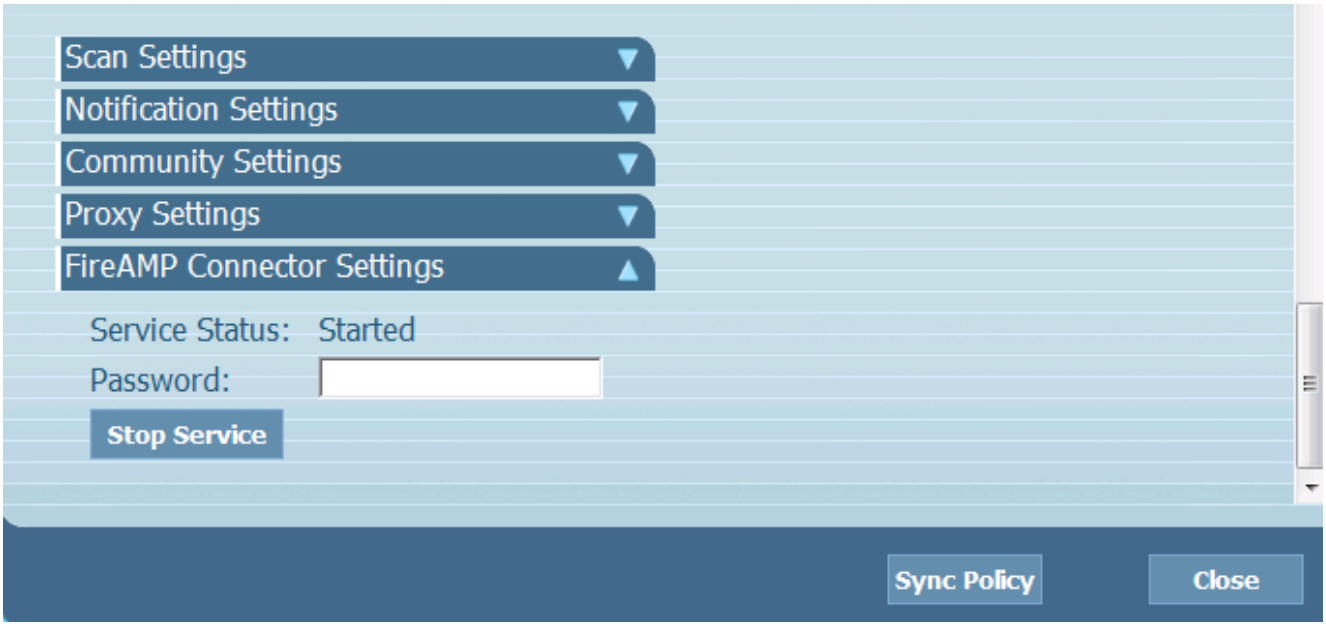
- Interface utilisateur (UI) du service de connecteur de FireAMP
- Console de services windows
- L'invite de commande de l'administrateur

### Interface utilisateur

> **Note**: Si vous avez la protection de connecteur vous a activé doit employer l'UI afin d'arrêter le service de connecteur de FireAMP.

1. Ouvrez l'UI de la barre d'état et cliquez sur les **configurations**.

2. Le défilement au bas et développent des **configurations de connecteur de FireAMP**.
3. Dans le domaine de mot de passe, entrez le mot de passe de protection de connecteur. **Service d'arrêt de** clic.

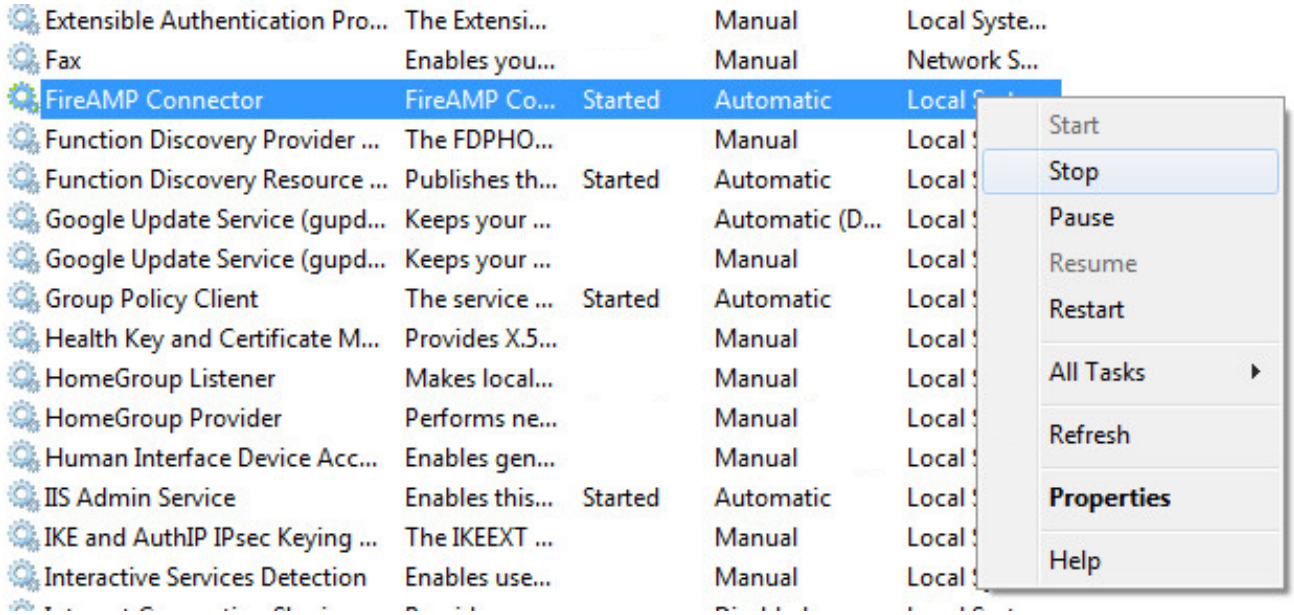



## Console de service

> **Note**: Afin d'arrêter et commencer des services dans la console de service vous avez besoin des privilèges d'administrateur.

Afin d'arrêter le connecteur de FireAMP entretenez à partir de la console de service, se terminent ces étapes :

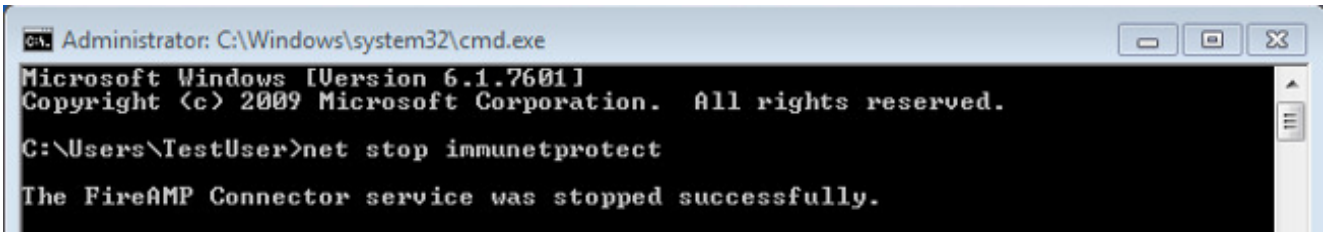
1. Naviguez vers le **menu de démarrage**.
2. Écrivez **services.msc et** l'appuyez sur entrent**.** La console de service s'ouvre.
3. Sélectionnez le service de **connecteur de FireAMP** et cliquez avec le bouton droit le nom de service.
4. Choisissez l'**arrêt** afin d'arrêter le service.



### Invite de commande

Afin d'arrêter le connecteur de FireAMP entretenez à partir de l'invite de commande d'un administrateur, se terminent ces étapes :

1. Naviguez vers le **menu de démarrage**.
2. Écrivez **cmd.exe et** l'appuyez sur entrent. Une fenêtre d'invite de commande s'ouvre.
3. Sélectionnez la commande **nette d'immunetprotect d'arrêt**. Si vous avez la version 5.0.1 ou ultérieures, entrez dans le **service wmic où le « nom comme « immunetprotect% » » startservice d'appel** commandent à la place. Ce tir d'écran affiche un exemple du service arrêté avec succès
   :




## Étape 2 : Supprimez les fichiers de base de données requis

### Fichiers de base de données de cache

Une fois que le service est arrêté vous pouvez supprimer ces fichiers de trois caches :

> **Avertissement :** Si vous ne supprimez pas tous les fichiers de base de données relatifs de cache il peut créer des questions de mise en cache avec la base de données recréée. En soi, le service pourrait pour commencer ou vous pourriez éprouver la représentation dégradée du service.

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

### Fichiers de base de données d'historique

Une fois que le service est arrêté, retirez ces fichiers de base de données d'historique :

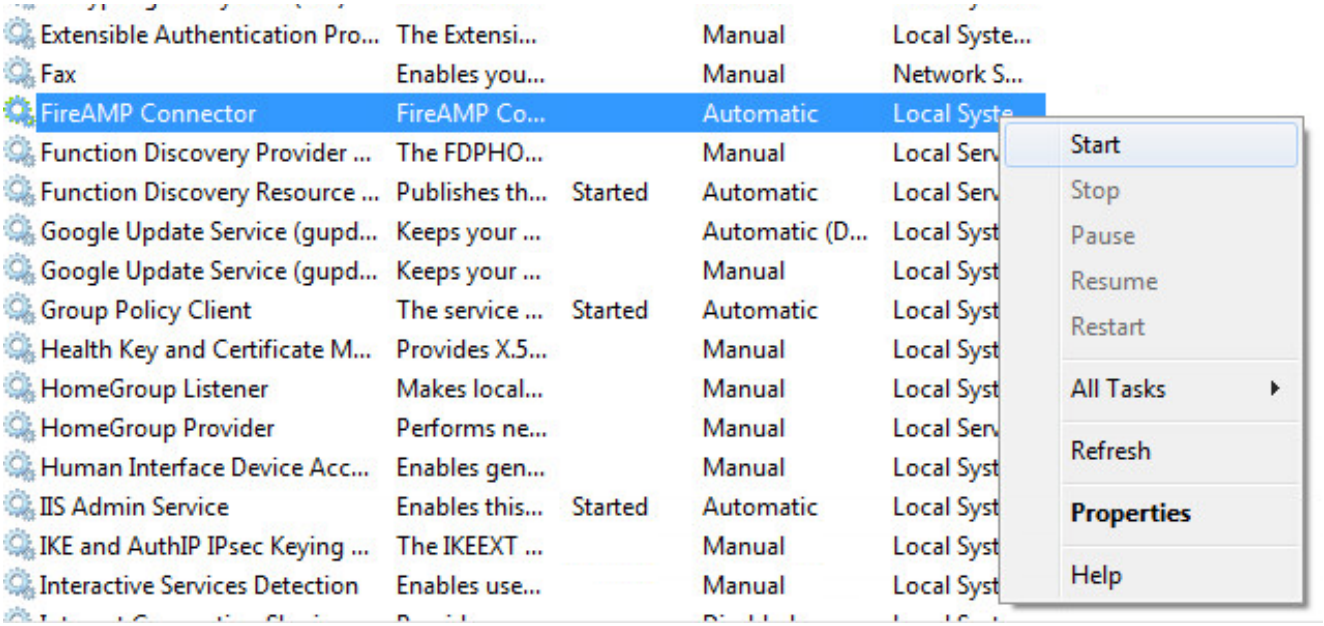
> **Avertissement :** Si vous ne supprimez pas tous les fichiers de base de données relatifs d'historique il peut créer des questions de mise en cache avec la base de données recréée. En soi, le service pourrait pour commencer ou vous pourriez éprouver la représentation dégradée du service.

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

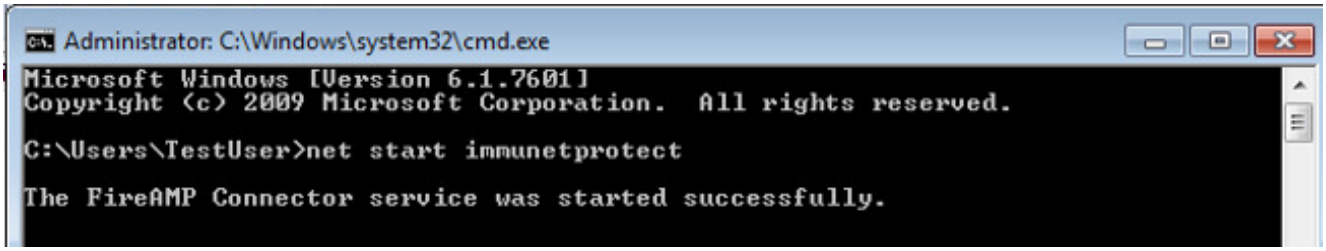
## Étape 3 : Commencez le service de connecteur de FireAMP

Afin de commencer le service de connecteur de FireAMP, terminez-vous ces étapes :

1. Naviguez vers le **menu de démarrage**.
2. Écrivez **services.msc et** l'appuyez sur entrent**.** La console de service s'ouvre.
3. Choisissez le service de **connecteur de FireAMP** et cliquez avec le bouton droit le nom de service.
4. Choisissez le **début** afin de commencer le service.




Alternativement, sur l'invite de commande de l'administrateur vous pouvez sélectionner la commande **nette d'immunetprotect de début**. Si vous avez la version 5.0.1 ou ultérieures, entrez dans le **service wmic où le « nom comme « immunetprotect% » » startservice d'appel** commandent à la place.Ce tir d'écran affiche un exemple du service commencé avec succès :




Après que vous redémarriez les services un nouvel ensemble de fichiers de base de données est créé. Ceci devrait maintenant te fournir un exemple frais du connecteur de FireAMP avec les listes blanches en cours, des listes de bloc, des exclusions, et ainsi de suite.