Windows에서 FireAMP 캐시 및 기록 파일 제거

목차

소개

이 문서에서는 FireAMP for Endpoints에서 데이터베이스 파일을 제거해야 하는 몇 가지 시나리오를 제공하며 필요한 경우 해당 파일을 제거하는 적절한 절차에 대해 설명합니다.FireAMP for Endpoints는 데이터베이스 파일의 최근 파일 탐지 및 성향 레코드를 유지 관리합니다.경우에 따라 Cisco 지원 엔지니어가 문제를 해결하기 위해 데이터베이스 파일 중 일부를 제거하도록 요청할 수 있습니다.

> **경고:**Cisco 기술 지원에서 지시한 경우에만 데이터베이스 파일을 제거할 수 있습니다.

캐시 및 기록용 데이터베이스 파일

목적

캐시 데이터베이스 파일은 파일의 알려진 속성을 유지합니다.기록 데이터베이스 파일은 소스 파일 이름 및 SHA256 값과 함께 모든 FireAMP 파일 탐지를 추적합니다.

정책에 차단 목록을 추가하고 커넥터를 업데이트할 때 지정된 파일의 동작은 즉시 변경되지 않습니다.파일이 악성이 아님을 캐시에서 이미 식별했기 때문입니다.따라서 차단 목록에 의해 변경되거나 재정의되지 않습니다.정책은 정책에 있는 시간 당 캐시가 만료되고 새 조회가 수행될 때 성향이 변경됩니다. 먼저 목록에 대해, 그리고 이후에 클라우드에 대해 수행됩니다.

제거 이유

기록 데이터베이스 및 캐시 데이터베이스 파일이 디렉토리에서 제거되면 FireAMP 서비스가 다시 시작될 때 새로 생성됩니다.FireAMP 디렉토리에서 이러한 파일을 제거해야 하는 경우도 있습니다

.예를 들어, 지정된 파일에 대해 간단한 맞춤형 탐지 또는 애플리케이션 차단 목록을 테스트하려는 경우

데이터베이스가 손상되어 데이터베이스에서 탐지를 열거나 볼 수 없습니다.또는 시스템에서 데이터베이스가 손상된 경우 커넥터를 시작할 수 없거나 전체 시스템 성능이 저하되는 등 FireAMP Connector 서비스 내에서 오류가 발생할 수 있습니다.이러한 경우 성능 관련 문제가 손상되는 것을 방지하고 진단을 위해 새 로그를 캡처할 수 있도록 커넥터에서 기록 파일을 지울 수 있습니다.

데이터베이스 파일 식별

Microsoft Windows에서 이러한 파일은 일반적으로 C:\Program Files\Sourcefire\fireAMP or C:\Program Files\Cisco\AMP에 있습니다.

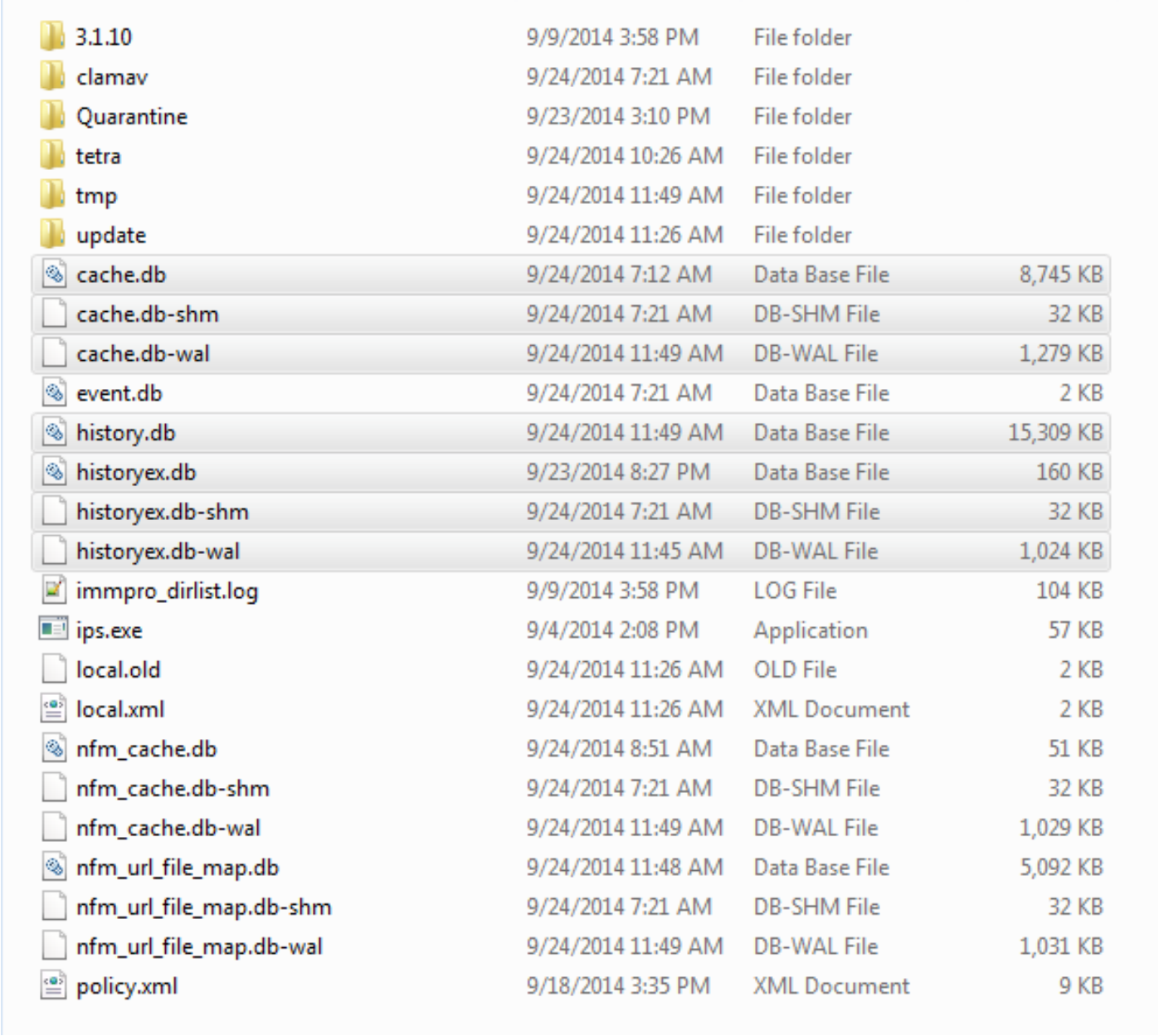
캐시 데이터베이스 파일의 이름은 다음과 같습니다.

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

기록 데이터베이스 파일의 이름은 다음과 같습니다.

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

이 스크린샷은 Windows 파일 탐색기의 파일을 보여줍니다.



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

데이터베이스 파일 제거 절차

1단계:FireAMP Connector 서비스 중지

다음과 같은 다양한 방법으로 FireAMP Connector 서비스를 중지할 수 있습니다.

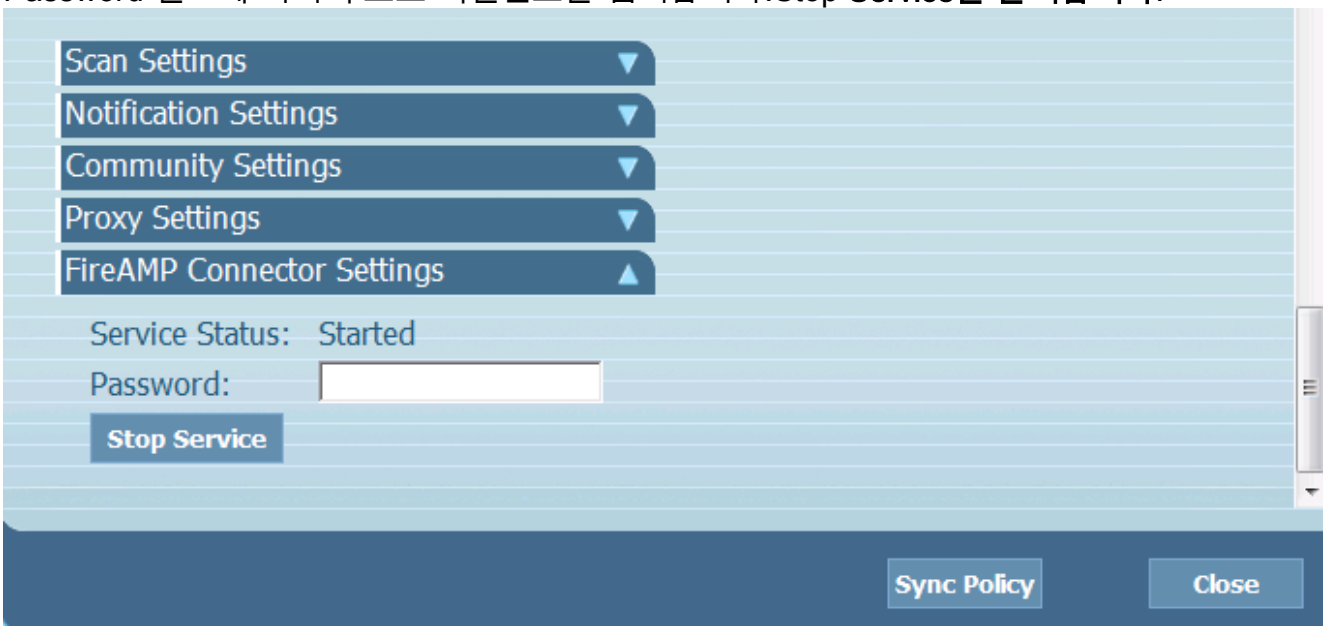
- FireAMP Connector 서비스의 UI(사용자 인터페이스)
- Windows 서비스 콘솔
- 관리자의 명령 프롬프트

사용자 인터페이스

> **참고:**커넥터 보호가 활성화된 경우 FireAMP Connector 서비스를 중지하려면 UI를 사용해야 합니다.

1. 트레이에서 UI를 열고 **설정**을 클릭합니다.

2. 아래로 스크롤하여 FireAMP Connector **Settings(FireAMP 커넥터 설정)를 확장합니다**.
3. Password 필드에 커넥터 보호 비밀번호를 입력합니다.Stop **Service를 클릭합니다**.

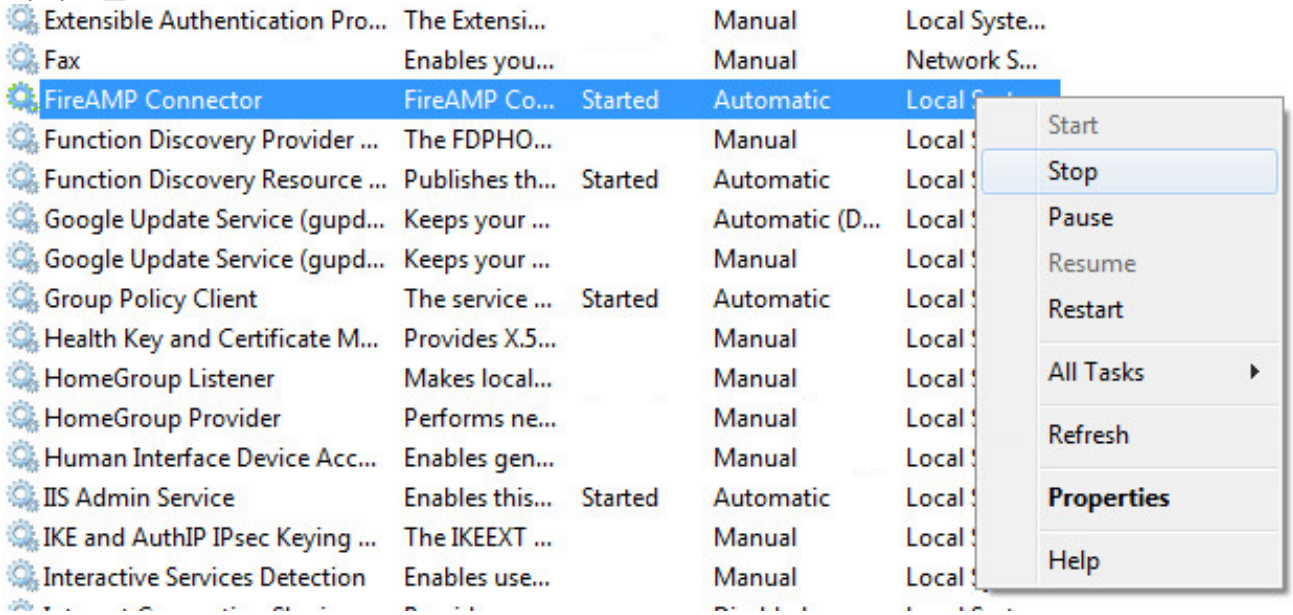


서비스 콘솔

참고:서비스 콘솔에서 서비스를 중지하고 시작하려면 관리자 권한이 필요합니다.

서비스 콘솔에서 FireAMP Connector 서비스를 중지하려면 다음 단계를 완료하십시오.

1. **시작 메뉴로 이동합니다**.
2. services.**msc를** 입력하고 Enter **키를 누릅니다**.서비스 콘솔이 열립니다.
3. FireAMP **Connector** 서비스를 선택하고 서비스 이름을 마우스 오른쪽 버튼으로 클릭합니다.
4. 서비스**를** 중지하려면 중지를 선택합니다.

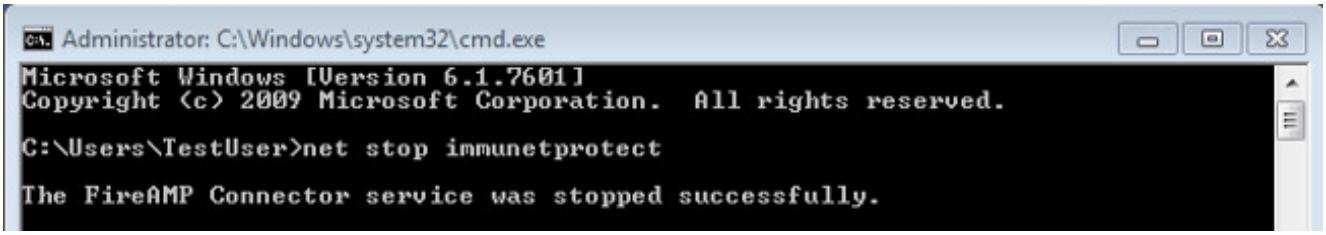


명령 프롬프트

관리자의 명령 프롬프트에서 FireAMP Connector 서비스를 중지하려면 다음 단계를 완료하십시오.

1. **시작 메뉴**로 **이동합니다**.
2. cmd**.exe를** 입력하고 **Enter**를 **누릅니다**.명령 프롬프트 창이 열립니다.
3. net stop immunetprotect 명령**을** 입력합니다.버전 5.0.1 이상이 있는 경우 **"name like 'immunetprotect%'" call startservice** 명령 대신 **wmic 서비스를** 입력합니다. 이 스크린샷은 성공적으로 중지된 서비스의 예를 보여줍니다

.



2단계:필요한 데이터베이스 파일 삭제

데이터베이스 파일 캐시

서비스가 중지되면 다음 세 개의 캐시 파일을 삭제할 수 있습니다.

> **경고:**모든 관련 캐시 데이터베이스 파일을 삭제하지 않으면 다시 만든 데이터베이스에 캐싱 문제를 만들 수 있습니다.따라서 서비스가 시작되지 않거나 서비스에서 성능이 저하될 수 있습니다.

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

기록 데이터베이스 파일

서비스가 중지되면 다음 기록 데이터베이스 파일을 제거합니다.

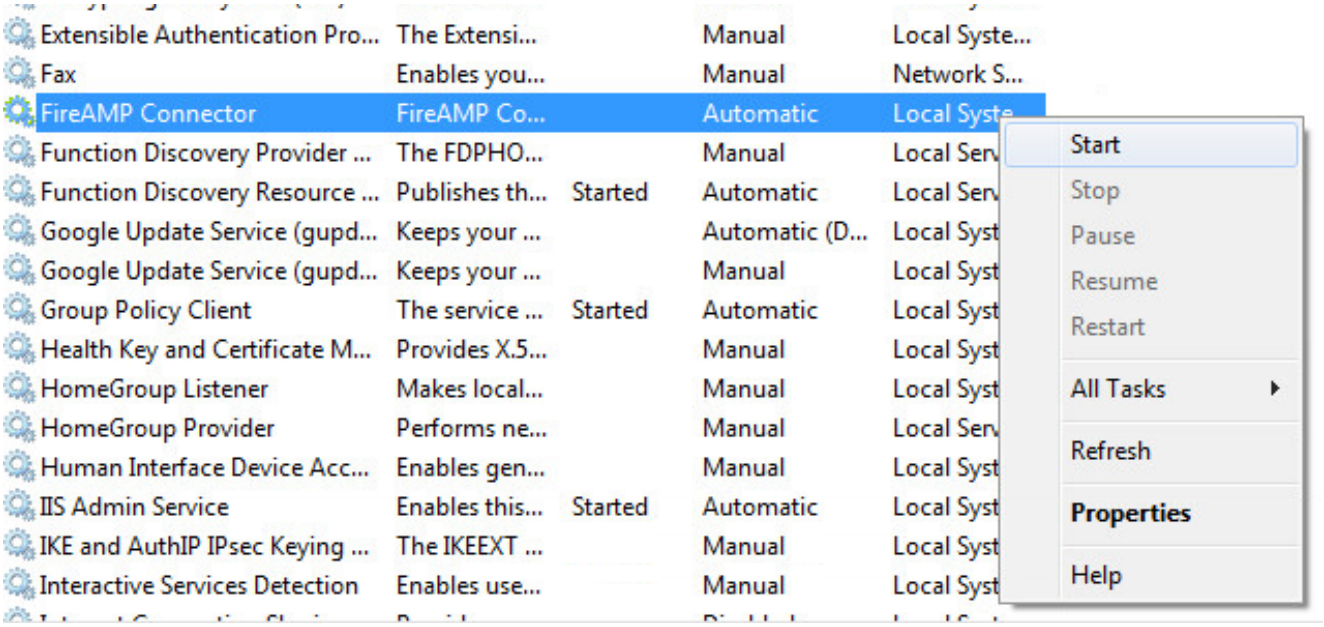
> **경고:**관련 기록 데이터베이스 파일을 모두 삭제하지 않으면 다시 만든 데이터베이스에 캐싱 문제를 만들 수 있습니다.따라서 서비스가 시작되지 않거나 서비스에서 성능이 저하될 수 있습니다.

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

3단계:FireAMP Connector 서비스 시작

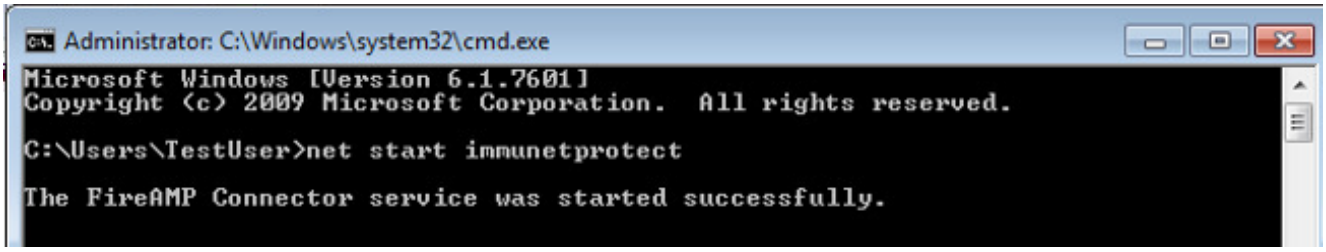
FireAMP Connector 서비스를 시작하려면 다음 단계를 완료하십시오.

1. **시작 메뉴**로 **이동합니다**.
2. services**.msc를** 입력하고 Enter **키를 누릅니다**.서비스 콘솔이 열립니다.
3. FireAMP **Connector** 서비스를 선택하고 서비스 이름을 마우스 오른쪽 버튼으로 클릭합니다.
4. 서비스를 시작하려면 시작을 선택합니다.



또는 관리자의 명령 프롬프트에서 **net start immunetprotect** 명령을 입력할 수 있습니다.버전 5.0.1 이상이 있는 경우 **"name like 'immunetprotect%'" call startservice** 명령 대신 **wmic 서비스를** 입력합니다.이 스크린샷은 성공적으로 시작된 서비스의 예를 보여줍니다

.



서비스를 다시 시작하면 새 데이터베이스 파일 집합이 만들어집니다.이제 FireAMP Connector의 새로운 인스턴스를 최신 화이트리스트, 차단 목록, 제외 등과 함께 제공합니다.