FMC에서 취약성 데이터베이스에 대한 자동 업데이트 구성

목차

소개

이 문서에서는 FMC에서 VDB(취약성 데이터베이스)에 대한 자동 업데이트를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD(Firepower Threat Defense)
- FMC(Firepower Management Center)
- VDB(취약성 데이터베이스)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FMC 7.0
- FTD 7.0

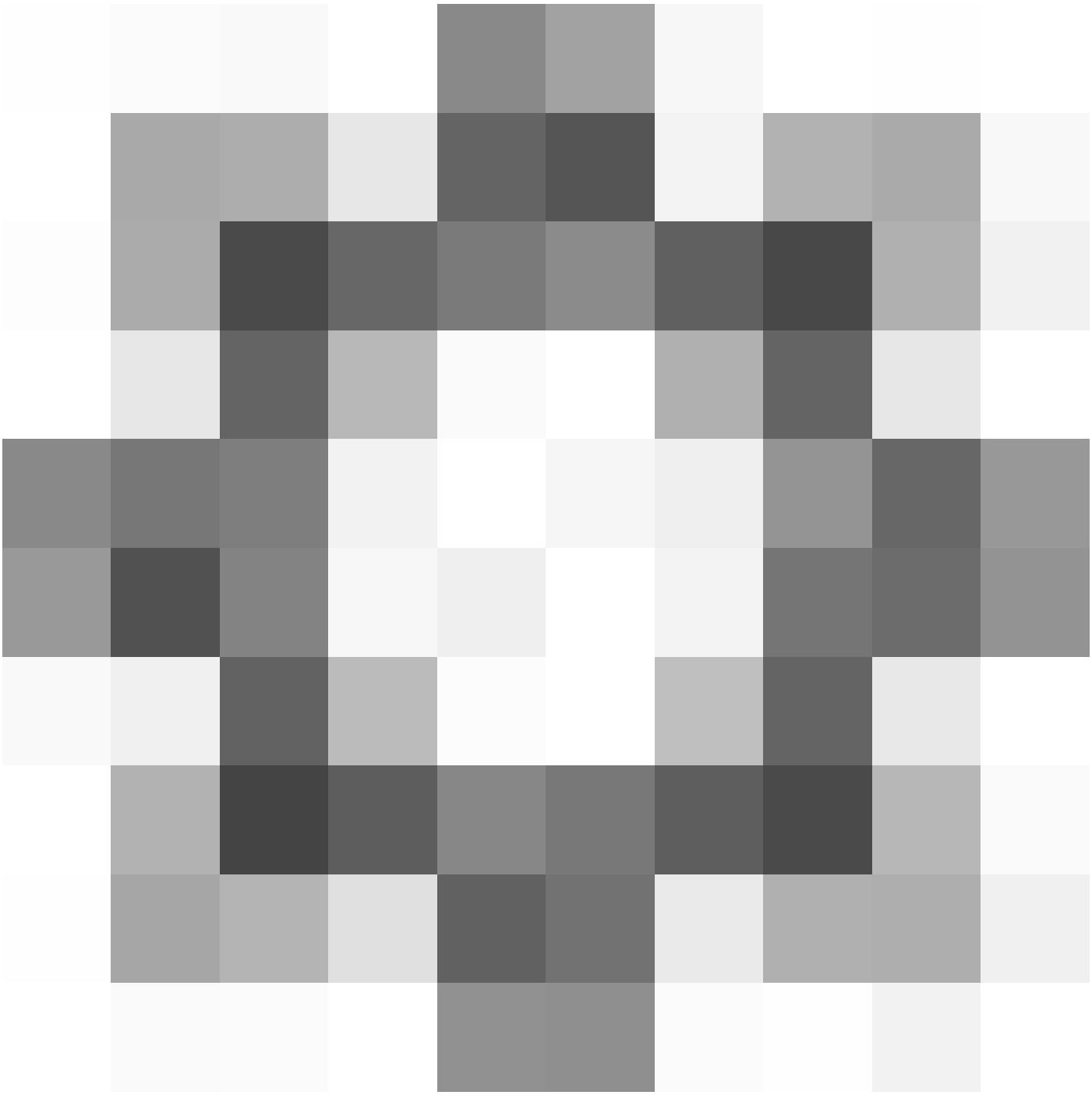
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

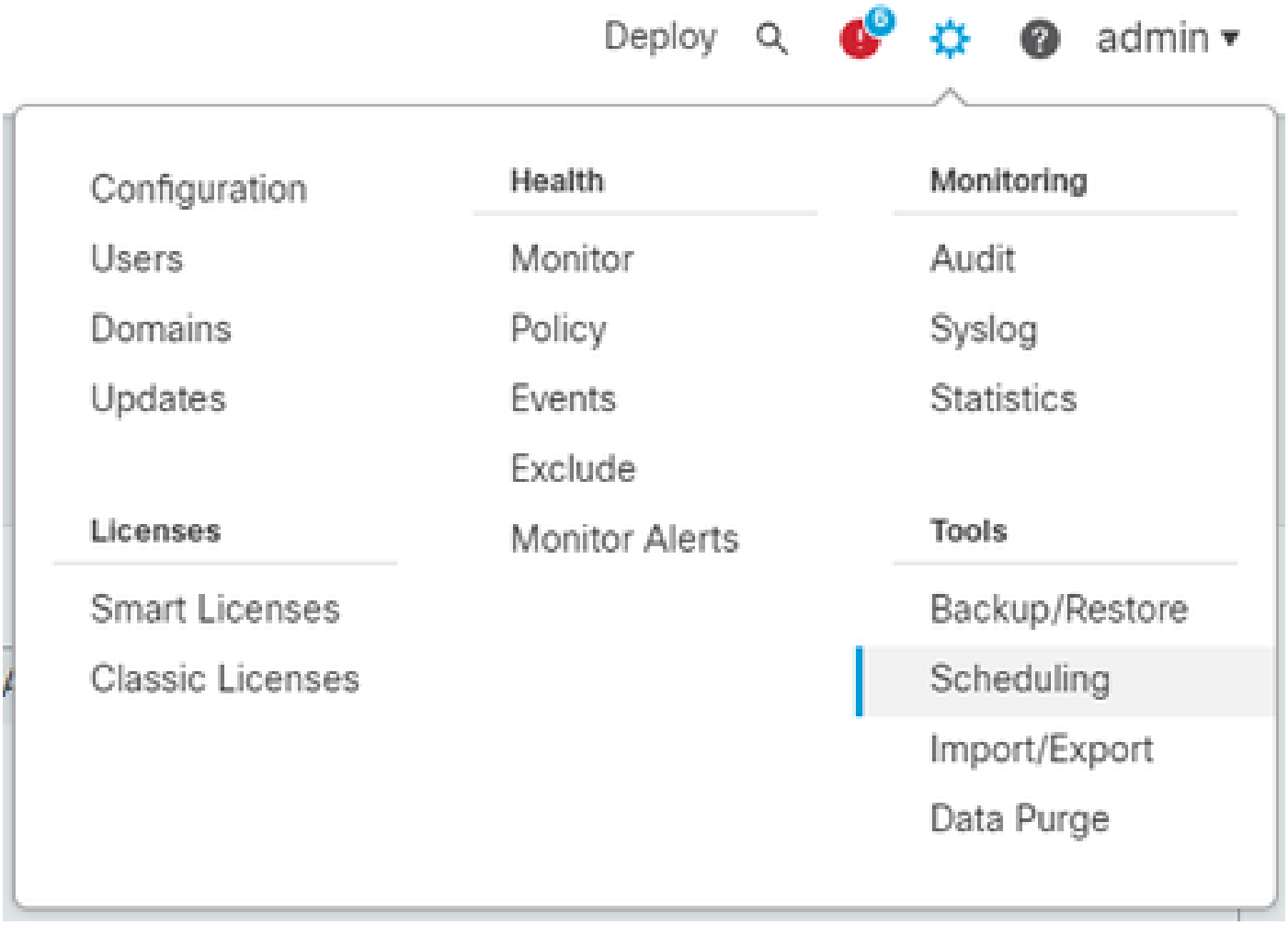
설정

1. firepower Management Center에 로그인합니다.

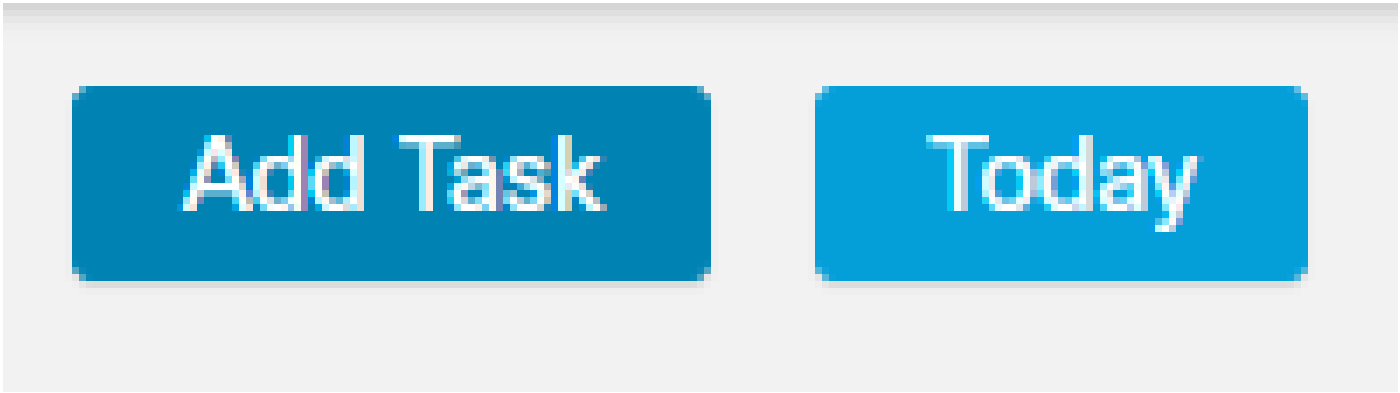
2. System(



)> Scheduling으로 이동합니다.



3. 스케줄링 화면의 오른쪽 상단에서 태스크 추가 버튼을 클릭합니다.

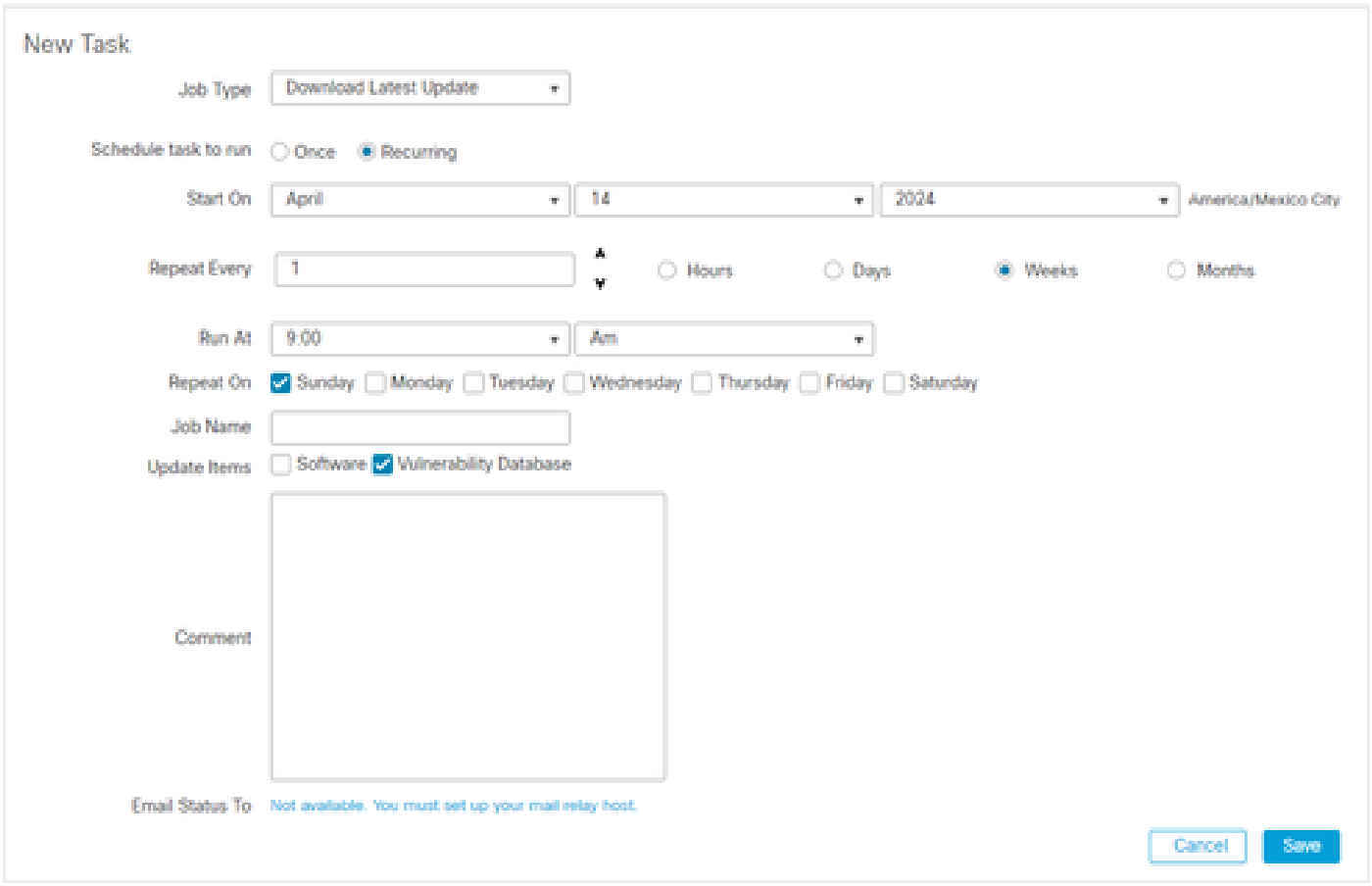


4. 신규 태스크 화면에서 작업 유형 드롭다운 메뉴에서 최신 갱신 다운로드를 선택하고 필요에 맞는 설정을 선택합니다.

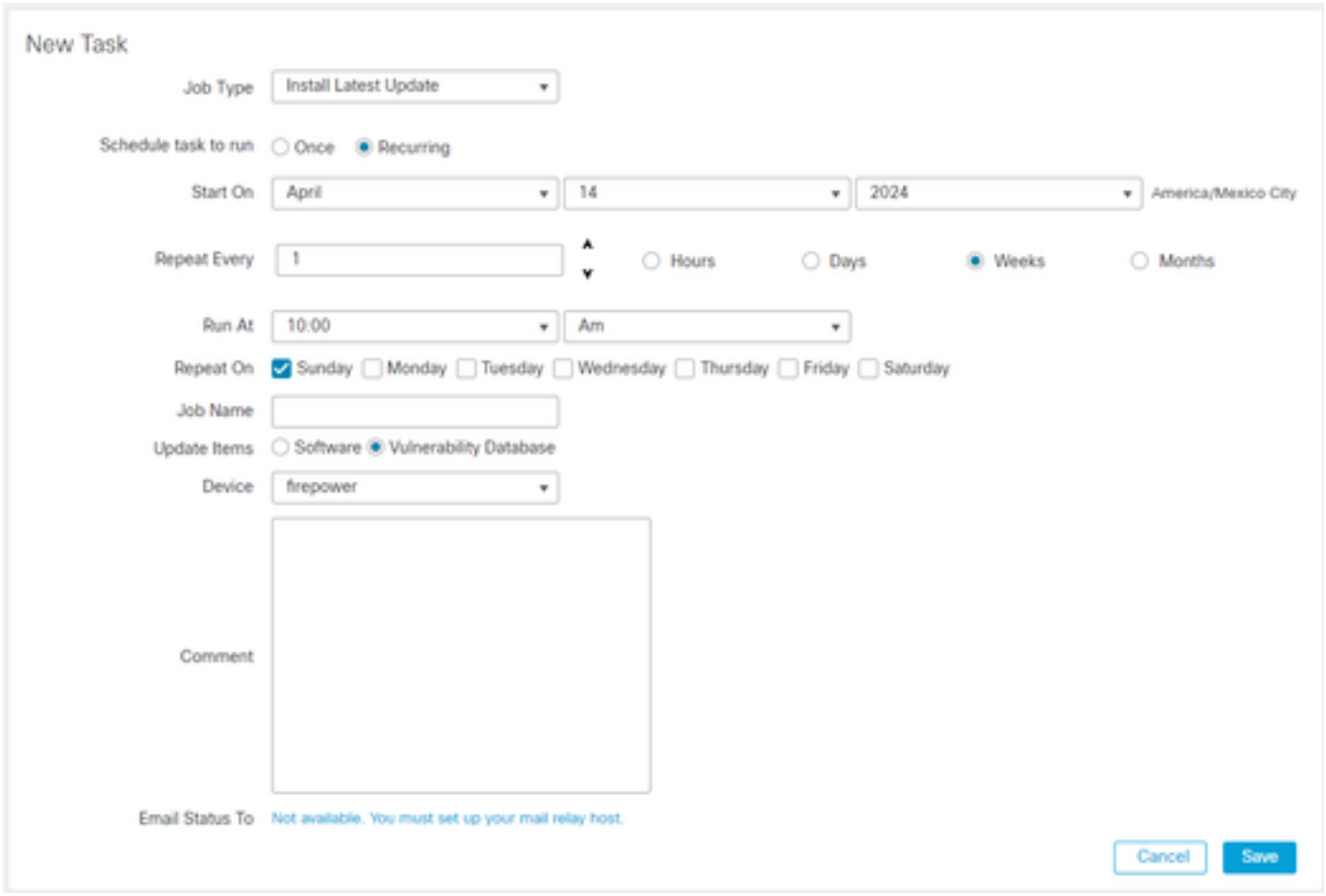
실행할 예약 작업에서 Recurring을 선택합니다.

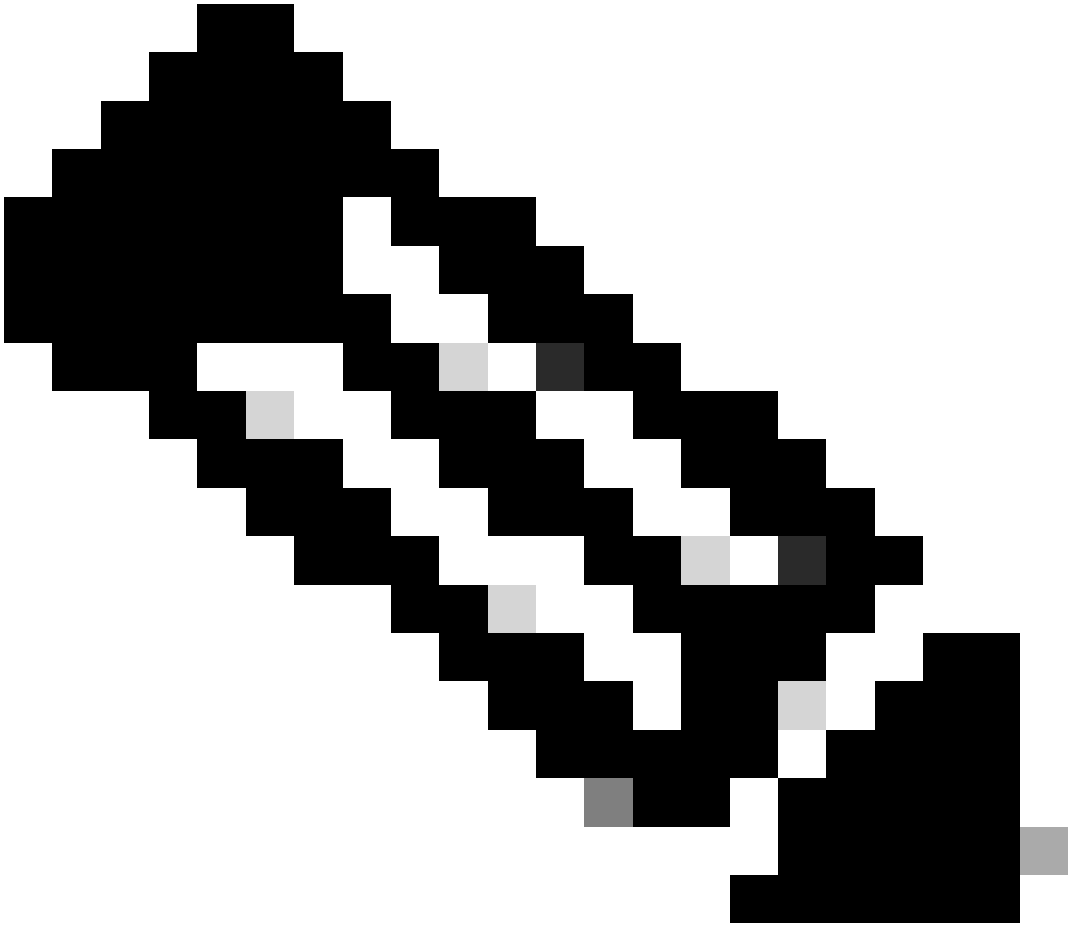
Update Items(항목 업데이트) 섹션에서 Vulnerability Database(취약성 데이터베이스)를 선택합니다.

그런 다음 Save(저장)를 클릭합니다.

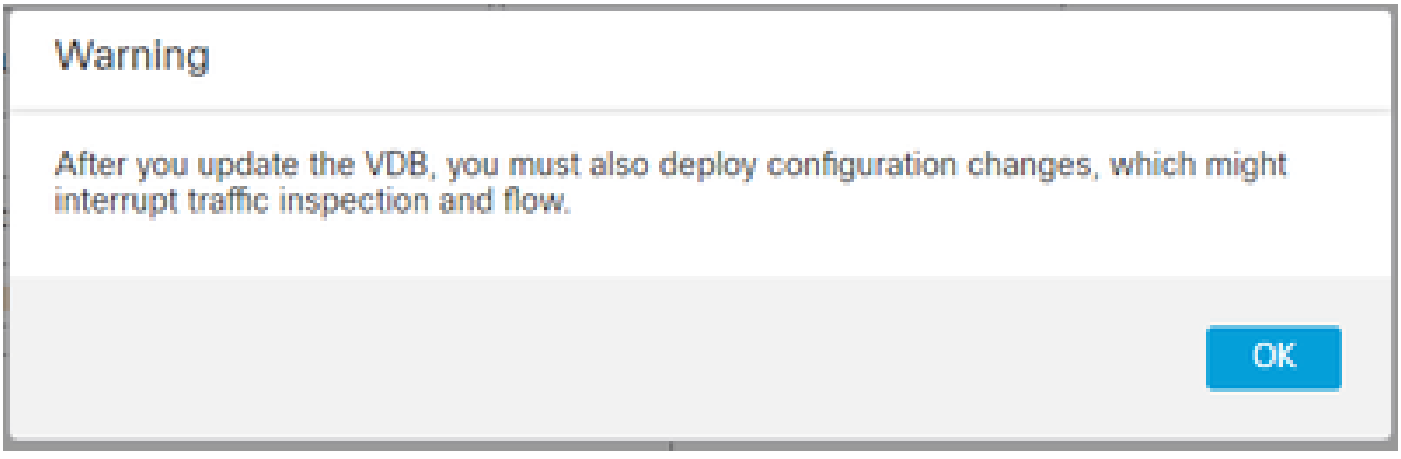


5. 3단계를 반복하여 새 작업 화면으로 돌아가 작업 유형 드롭다운 메뉴에서 최신 업데이트 설치를 선택하고 설정을 사용하여 요구 사항을 충족하고 저장을 클릭합니다.

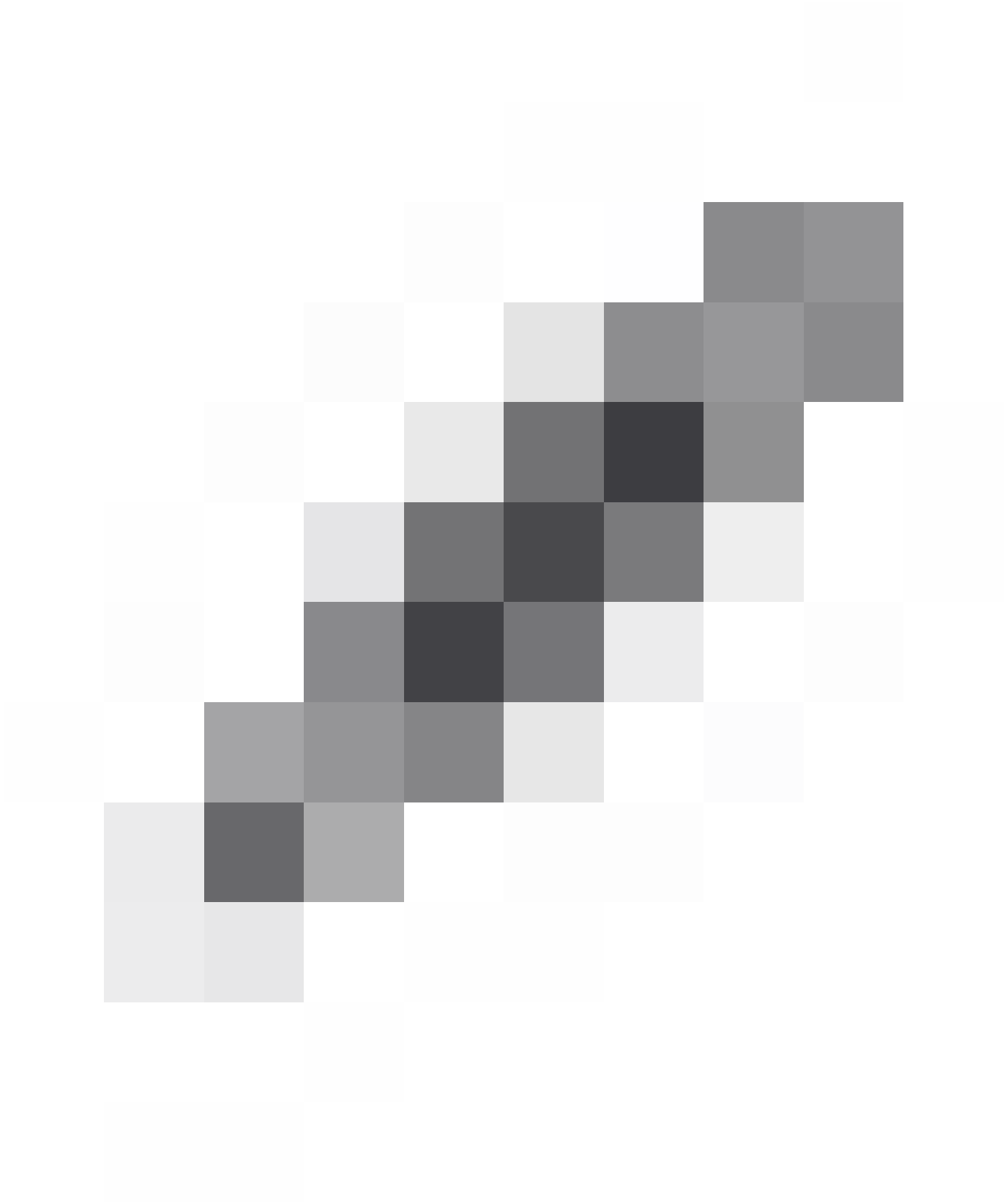

New Task
Job Type
Install Latest Update
Schedule task to run
Once
Recurring
Start On
April
14
2024
America/Mexico City
Repeat Every
1
Hours
Days
Weeks
Months
Run At
10:00
Am
Repeat On
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Job Name
Update Items
Software
Vulnerability Database
Device
firepower
Comment
Email Status To
Not available. You must set up your mail relay host.
Cancel
Save



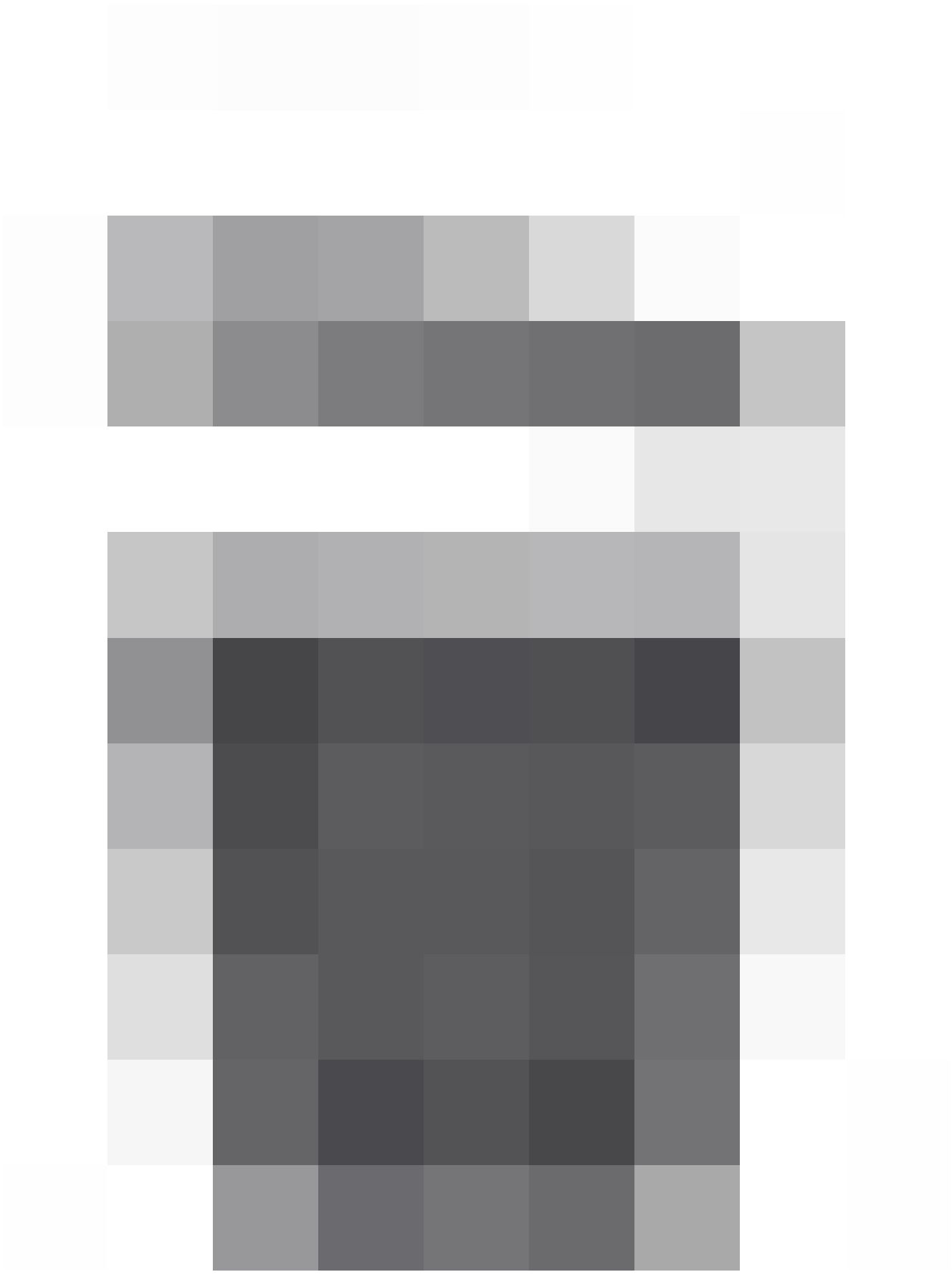
참고: VDB를 업데이트한 후에는 컨피그레이션 변경도 구축해야 하며, 이는 트래픽 검사 및 흐름을 방해할 수 있습니다.

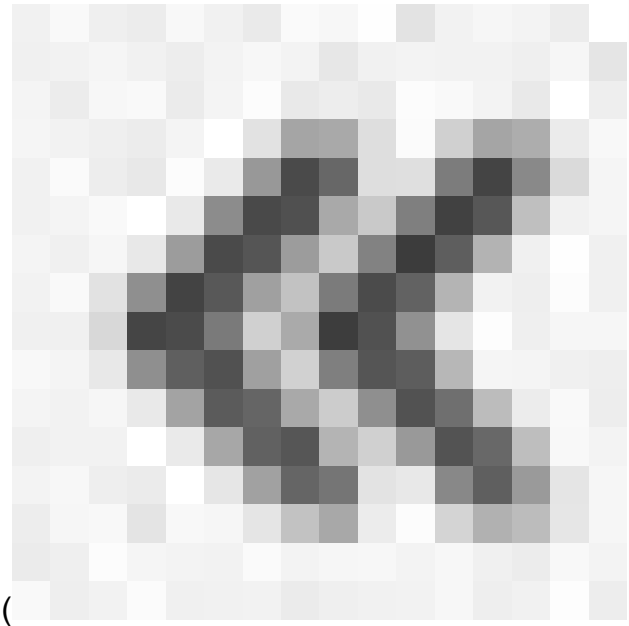
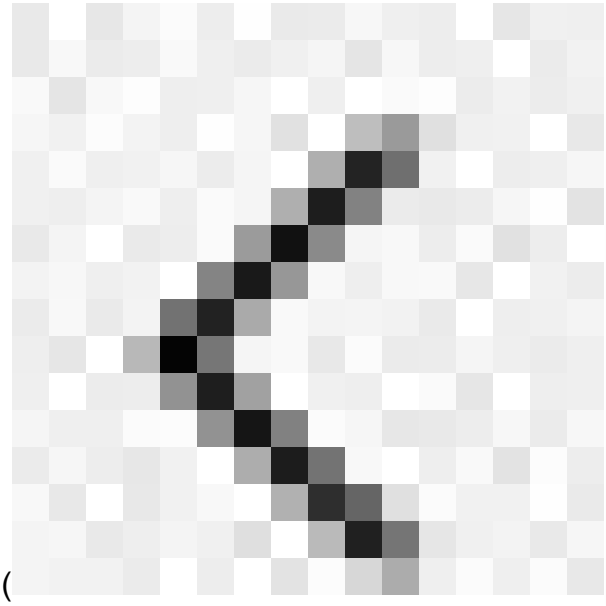
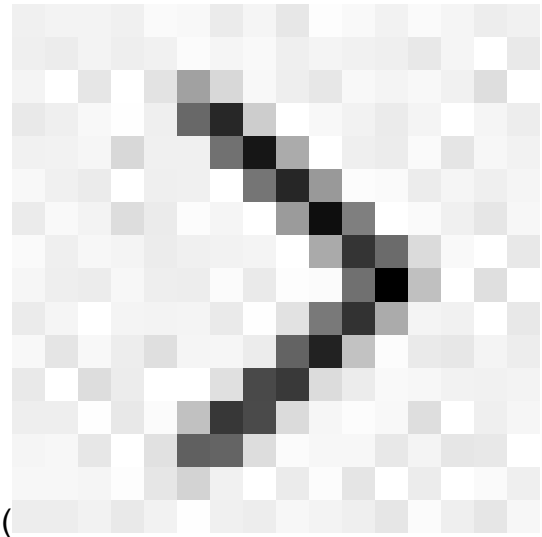


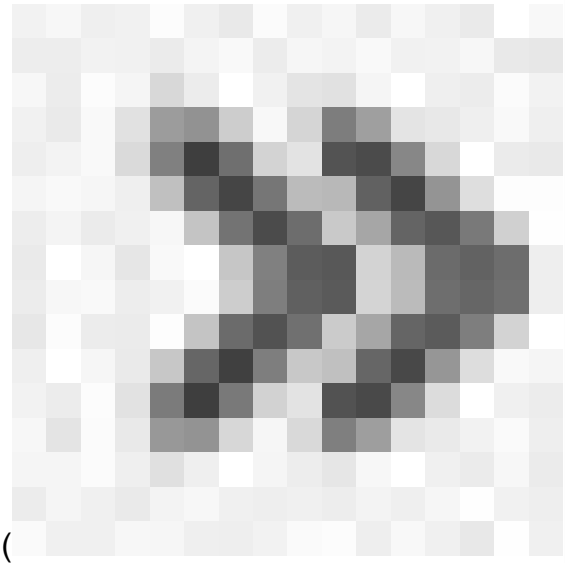
예약 화면의 작업 세부 정보 섹션에서 편집 펜(



)을 눌러 예약 작업을 세부 조정할 수 있으며 휴지통(



2단계	달력 보기를 사용하여 다음 작업을 수행할 수 있습니다. • 1년 뒤로 이동하려면 이중 왼쪽 화살표()를 클릭합니다. • 한 달 뒤로 이동하려면 단일 왼쪽 화살표()를 클릭합니다. • 한 달 앞으로 이동하려면 단일 오른쪽 화살표(

	)를 클릭합니다.  • 1년 앞으로 이동하려면 이중 오른쪽 화살표( )를 클릭합니다. • 현재 월 및 연도로 돌아가려면 현재를 클릭합니다. • 새 작업을 예약하려면 작업 추가를 누릅니다. • 작업 목록 테이블에서 특정 날짜에 대해 예약된 모든 작업을 보려면 날짜를 클릭합니다. • 특정 작업을 날짜에 클릭하여 작업 목록 테이블에 표시합니다.

문제 해결

VDB 자동 업그레이드가 예상대로 작동하지 않을 경우 VDB를 롤백할 수 있습니다.

단계:

관리 디바이스(FMC, FDM 또는 SFR 온박스) CLI에 대한 SSH

전문가 모드 및 루트로 전환하고 롤백 변수를 설정합니다.

<#root>

expert

sudo su
export ROLLBACK_VDB=1

다운그레이드하려는 VDB 패키지가 /var/sf/updates의 디바이스에 있는지 확인하고 설치합니다.

<#root>

```
install_update.pl --detach /var/sf/updates/<name of desired VDB Package file>
```

일반 vdb 설치 로그는 /var/log/sf/vdb-*의 해당 위치에 있습니다.

VDB 설치가 완료되면 디바이스에 정책을 구축합니다.

FMC에서 VDB의 설치 상태를 확인하려면 다음 디렉토리 내용을 검토할 수 있습니다.

root@firepower:/var/log/sf/vdb-4.5.0-338# ls -la
합계 40
drwxr-xr-x 5 루트 루트 4096 2023년 5월 15일
drwxr-xr-x 11 root root 4096 4월 23일 06:00 ..
-rw-r—r— 1 root 3308 5월 15 2023 flags.conf.complete
drwxr-xr-x 2 root 4096 5월 15일 2023 installer
drwxr-xr-x 2 root 4096 5월 15 2023 post
drwxr-xr-x 2 root 4096 2023년 5월 15일
-rw-r—r— 1 루트 루트 1603 2023년 5월 15일 status.log
-rw-r—r— 1 root root 5703 May 15 2023 vdb.log
-rw-r—r— 1 root root 5 May 15 2023 vdb.pid

FTD에서 VDB 설치 기록을 확인하려면 다음 디렉토리 내용을 확인합니다.

root@firepower:/ngfw/var/cisco/deploy/pkg/var/cisco/packages# ls -al
총 72912
drwxr-xr-x 5 root root 130 9월 1일 08:49 .
drwxr-xr-x 4 root root 34 8월 16일 14:40 ..
drwxr-xr-x 3 root root 18 8월 16일 14:40 exporter-7.2.4-169
-rw-r—r— 1 root root 2371661 7월 27일 15:34 exporter-7.2.4-169.tgz
drwxr-xr-x 3 root root 21 8월 16일 14:40 vdb-368
-rw-r—r— 1 root root 36374219 7월 27일 15:34 vdb-368.tgz
drwxr-xr-x 3 root root 21 Sep 1 08:49 vdb-369
-rw-r—r— 1 root root 35908455 9월 1일 08:48 vdb-369.tgz

관련 정보

VDB(취약성 데이터베이스) 업데이트

작업 예약

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.