

Automatische updates voor kwetsbaarheidsdatabase op FMC configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Configuraties](#)

[Verifiëren](#)

[Geplande taken op de agenda bekijken](#)

[Procedure](#)

[Probleemoplossing](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe de automatische updates voor de Vulnerability Database (VDB) op FMC moeten worden geconfigureerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Vulnerability Database (VDB)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VCC 7.0
- FTD 7.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

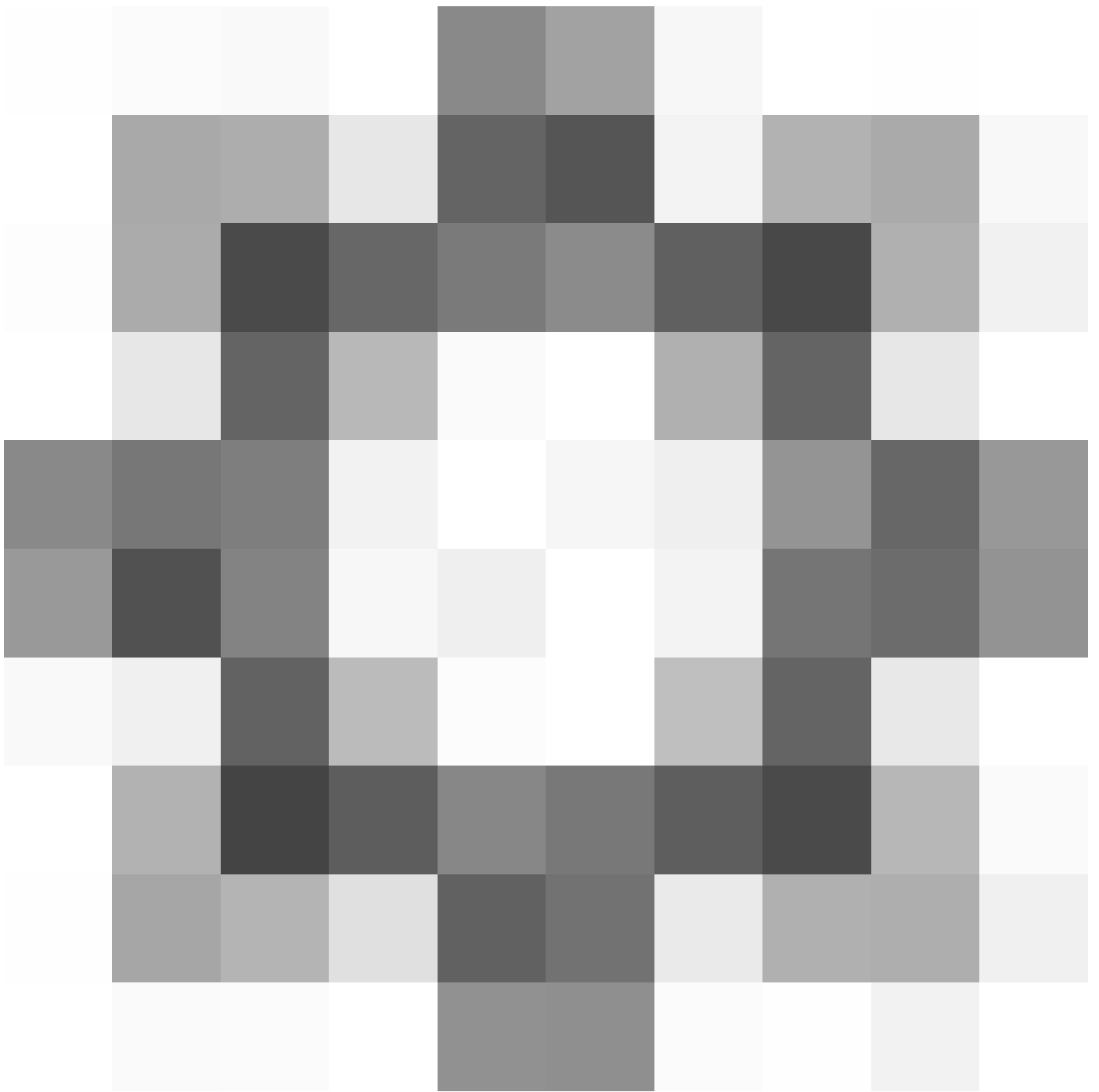
Configuraties

1. Meld u aan bij Firepower Management Center.

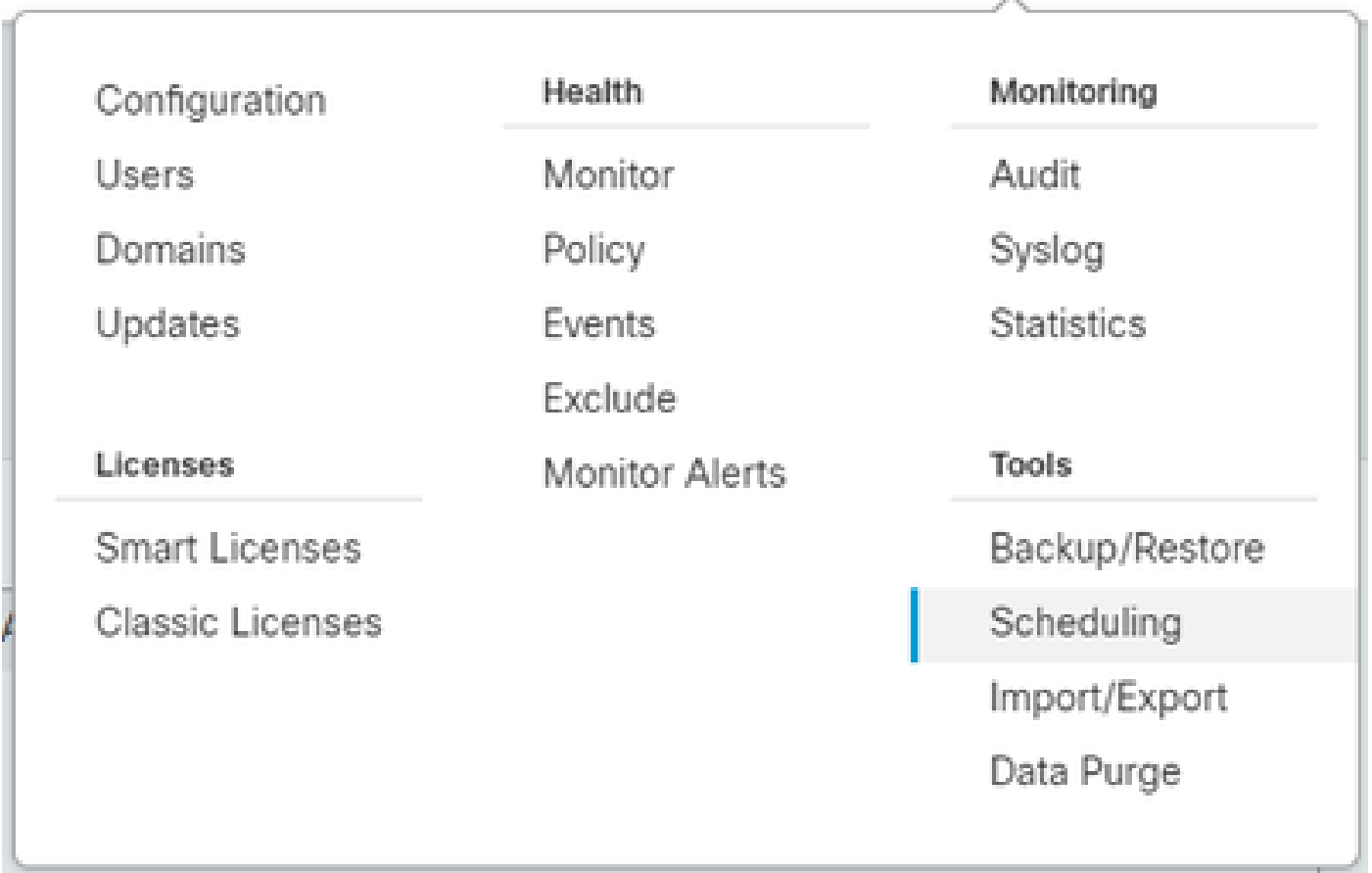


The screenshot shows the login interface for the Cisco Firepower Management Center. At the top center is the Cisco logo, consisting of a stylized bridge icon above the word "CISCO" in blue. Below the logo, the text "Firepower Management Center" is displayed in a large, grey, sans-serif font. Underneath the title, there are two input fields: the first is labeled "Username" and the second is labeled "Password". Both fields are empty and have a thin grey border. At the bottom center of the form is a blue button with the text "Log In" in white.

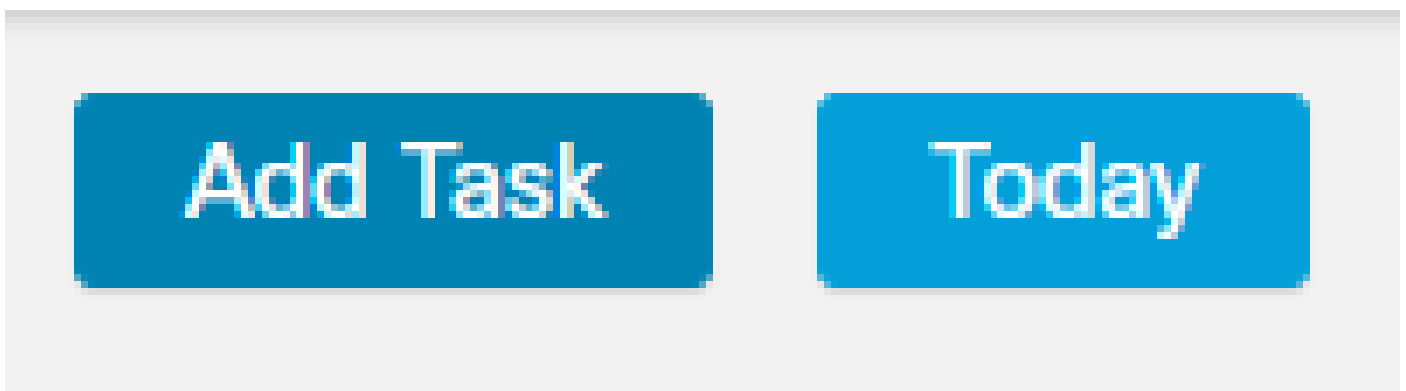
2. Navigeren naar systeem(



)> Scheduling.



3. Klik rechtsboven in het Schedulingscherm op de knop Taak toevoegen.



4. Selecteer in het scherm New Task de optie Download Latest Update vanuit het vervolgkeuzemenu Job Type en selecteer de instellingen die aan uw behoeften voldoen.

Selecteer de optie Terugkeren voor de uit te voeren taak.

Selecteer in het gedeelte Items bijwerken de optie Vulnerability Database.

Klik vervolgens op Opslaan.

New Task

Job Type

Schedule task to run Once Recurring

Start On

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Update Items Software Vulnerability Database

Comment

Email Status To Not available. You must set up your mail relay host.

5. Herhaal stap 3 om terug te gaan naar het scherm New Task en selecteer Install Latest Update in het vervolgkeuzemenu Taaktype en gebruik de instellingen om aan uw behoeften te voldoen en klik op Opslaan.

New Task

Job Type

Schedule task to run Once Recurring

Start On

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Update Items Software Vulnerability Database

Device

Comment

Email Status To Not available. You must set up your mail relay host.

Cancel

Save



Opmerking: let erop dat u na de VDB-update ook configuratiewijzigingen moet implementeren die de verkeersinspectie en doorstroming kunnen onderbreken.

Warning

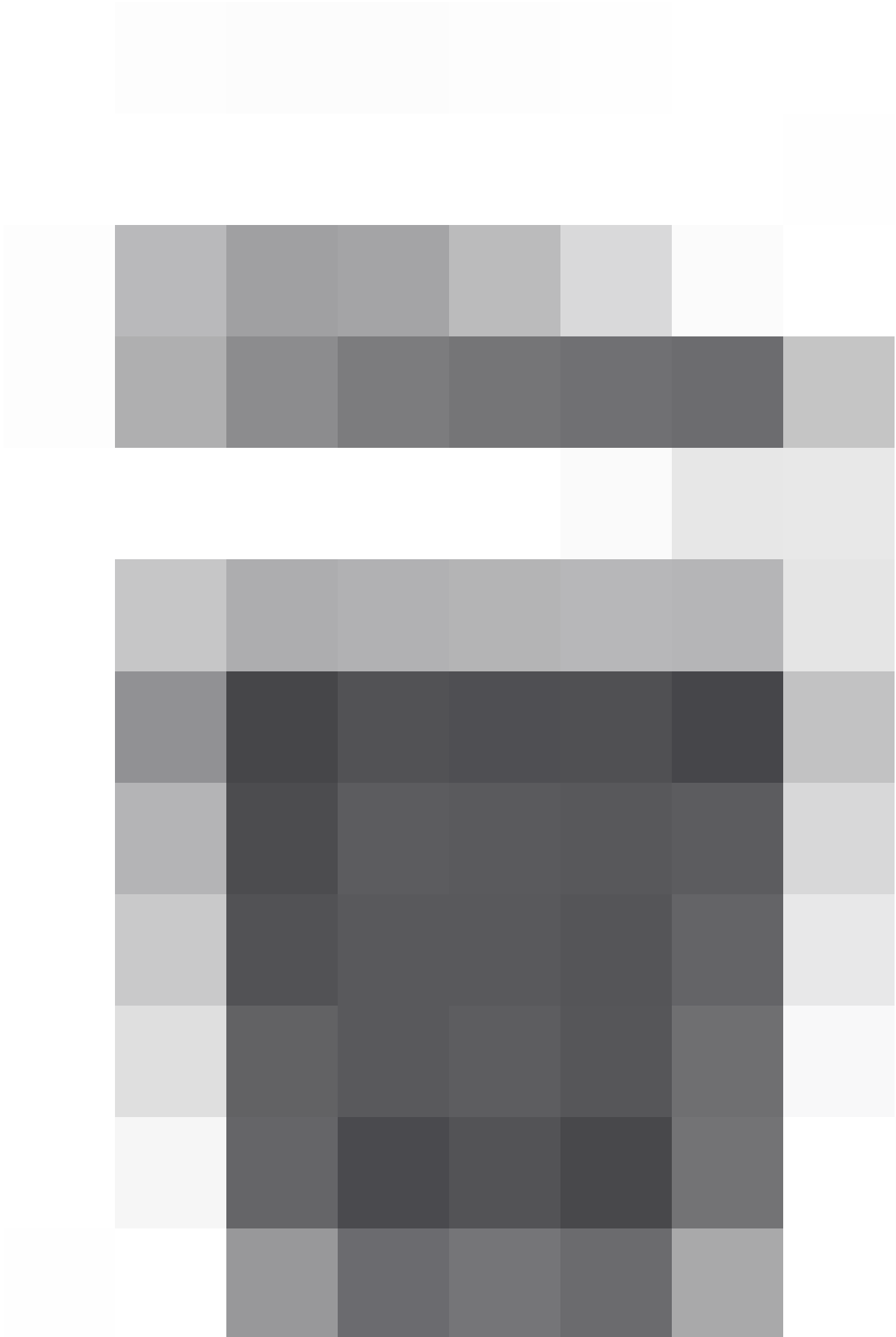
After you update the VDB, you must also deploy configuration changes, which might interrupt traffic inspection and flow.

OK

U kunt de geplande taken nauwkeurig afstemmen door op de bewerkingsspen (

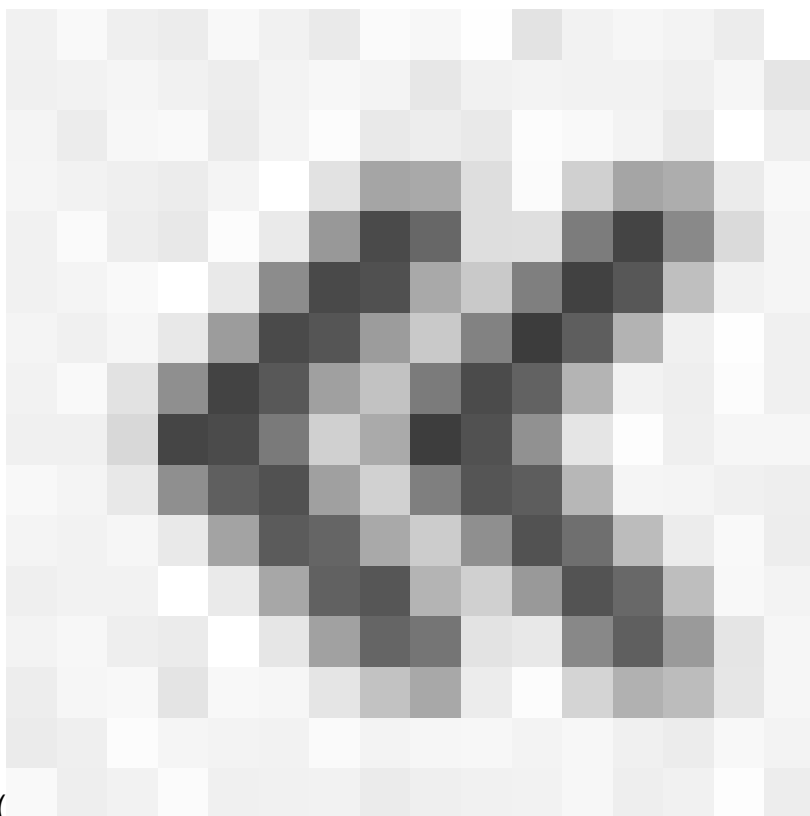


) te klikken of door op de vuilnisbak (

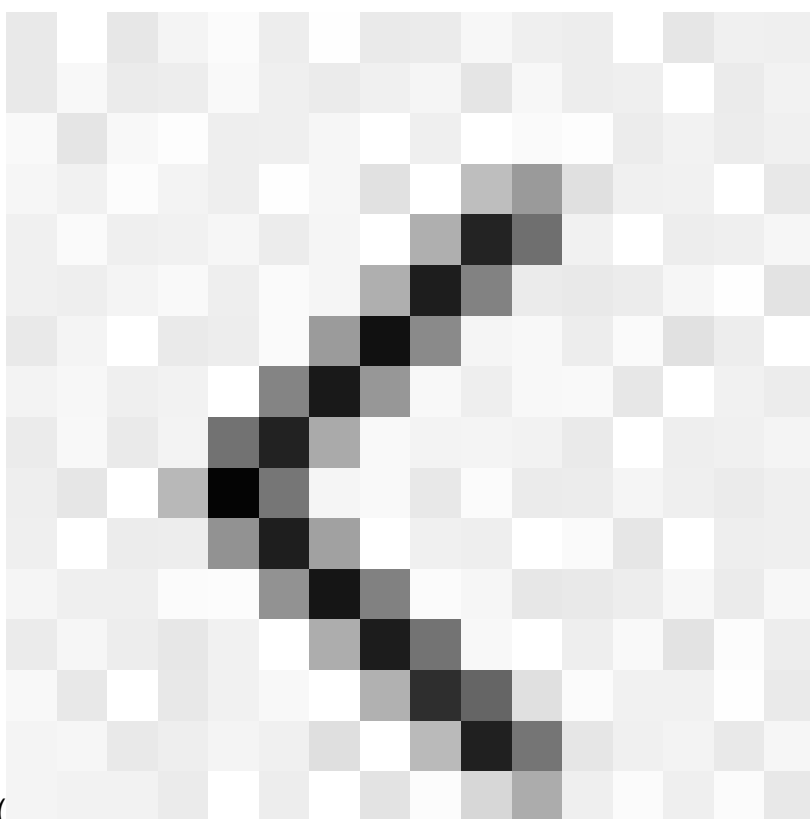


Stap 2

U kunt deze taken uitvoeren via de kalenderweergave:



- Klik op Dubbele linkerpijl() om een jaar terug te gaan.

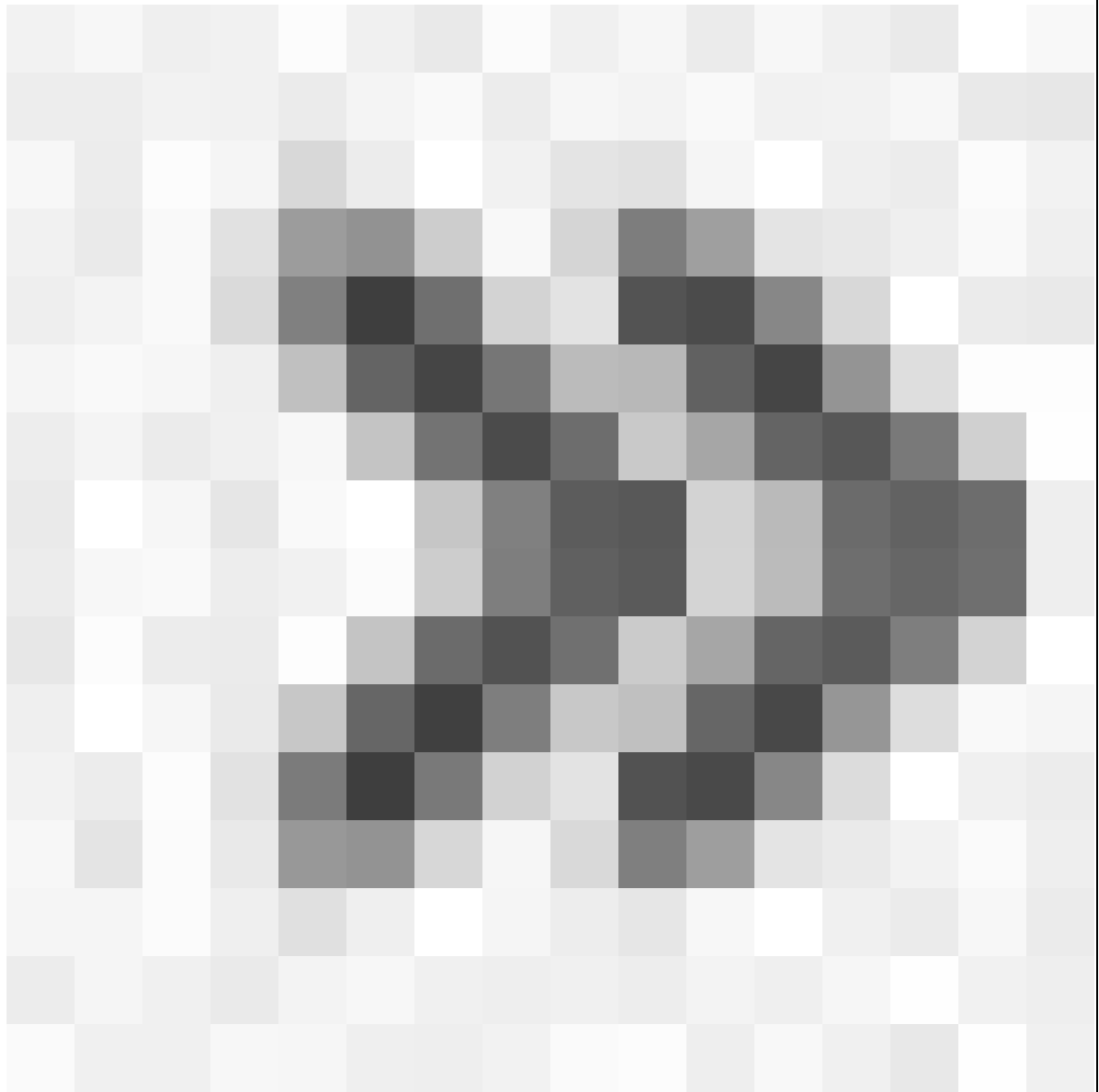


- Klik op Single Left Arrow() om een maand terug te gaan.
- Klik op de enkele pijl rechts(



) om een maand verder te gaan.

- Klik op Dubbele rechterpijl(



) om een jaar verder te gaan.

- Klik vandaag om terug te keren naar de huidige maand en jaar.
- Klik op Taken toevoegen om een nieuwe taak te plannen.
- Klik op een datum om alle geplande taken voor de specifieke datum in een tabel op de taaklijst weer te geven.
- Klik op een specifieke taak op een datum om deze in een tabel op de taaklijst te bekijken.

Probleemoplossing

Indien de automatische VDB-upgrade niet werkt zoals verwacht, kunt u de VDB terugdraaien.

Stappen:

SSH naar de CLI van het beheerapparaat (FMC, FDM of SFR onbox).

Switch naar expertmodus, en root en stel de terugdraaivariabele in:

```
<#root>
```

```
expert
```

```
sudo su  
export ROLLBACK_VDB=1
```

Bevestig dat het VDB-pakket dat u wilt downgraden naar zich op het apparaat bevindt in /var/sf/updates en installeer het:

```
<#root>
```

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

Normale vdb installatielogboeken zijn te vinden op de toepasselijke locatie op /var/log/sf/vdb-*

Nadat VDB is geïnstalleerd, implementeert u het beleid op apparaten.

Voor FMC, om de installatiestatus van VDB te controleren, kan deze directory inhoud worden herzien:

```
root@firepower:/var/log/sf/vdb-4.5.0-338# ls -la  
totaal 40  
drwxr-xr-x 5 wortelwortel 4096 mei 15 2023 .  
drwxr-xr-x 11 wortel 4096 apr 23 06:00 ..  
-rw-r--1 wortelwortel 3308 Mei 15 2023 flags.conf.complete  
drwxr-xr-x 2 wortelwortel 4096 May 15 2023 installateur  
drwxr-xr-x 2 root root 4096 May 15 2023 post  
drwxr-xr-x 2 wortelwortel 4096 Mei 15 2023 pre  
-rw-r--r-- 1 wortelwortel 1603 May 15 2023 status.log  
-rw-r--1 wortelwortel 5703 Mei 15 2023 vdb.log  
-rw-r--1 wortelwortel 5 mei 15 2023 vdb.pid
```

Voor FTD, om de geschiedenis van VDB installaties te controleren, controleer deze folder inhoud:

```
root@firepower:/ngfw/var/cisco/implementation/pkg/var/cisco/packers# ls -al  
totaal 72912  
drwxr-xr-x 5 wortelwortel 130 Sep 1 08:49 .  
drwxr-xr-x 4 wortelwortel 34 aug 16 14:40 ..  
drwxr-xr-x 3 wortelwortel 18 aug 16 14:40 exporteur-7.2.4-169  
-rw-r--r-- 1 wortelwortel 2371661 jul 27 15:34 exporteur-7.2.4-169.tgz  
drwxr-xr-x 3 wortelwortel 21 aug 16 14:40 vdb-368
```

```
-rw-r--r-- 1 wortelwortel 36374219 Jul 27 15:34 vdb-368.tgz  
drwxr-xr-x 3 wortelwortel 21 Sep 108:49 vdb-369  
-rw-r--r-- 1 wortelwortel 35908455 Sep 1 08:48 vdb-369.tgz
```

Gerelateerde informatie

[VDB \(Update Vulnerability Database\)](#)

[Taakplanning](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.