Configure Automatic Updates for Vulnerability Database on FMC

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Configurations

Verify

- Viewing Scheduled Tasks on the Calendar
  - Procedure

Troubleshooting

Related Information

Introduction

This document describes how to configure Automatic Updates for the Vulnerability Database (VDB) on FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software and hardware versions:

- FMC 7.0
- FTD 7.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

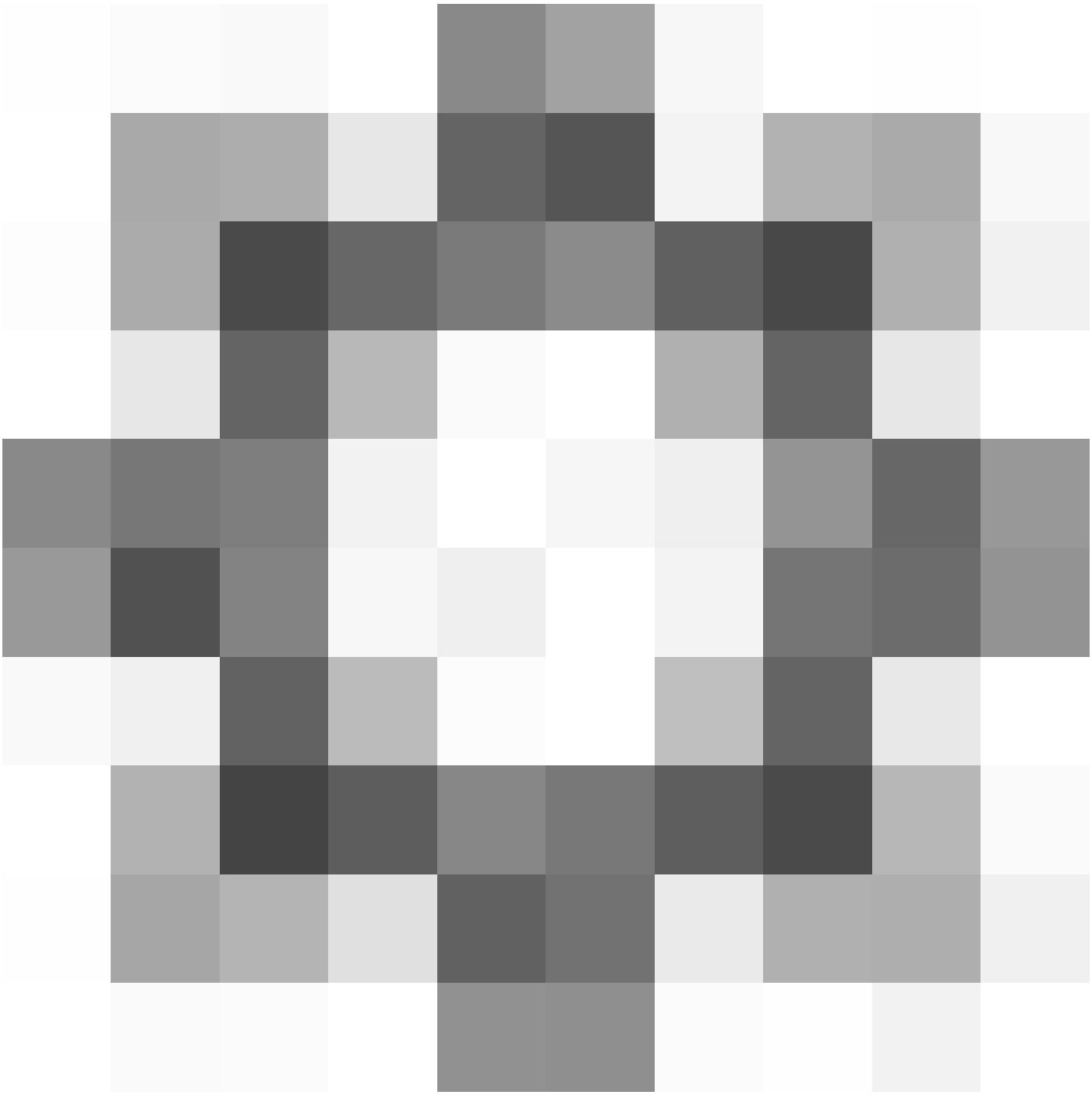
Configure

Configurations

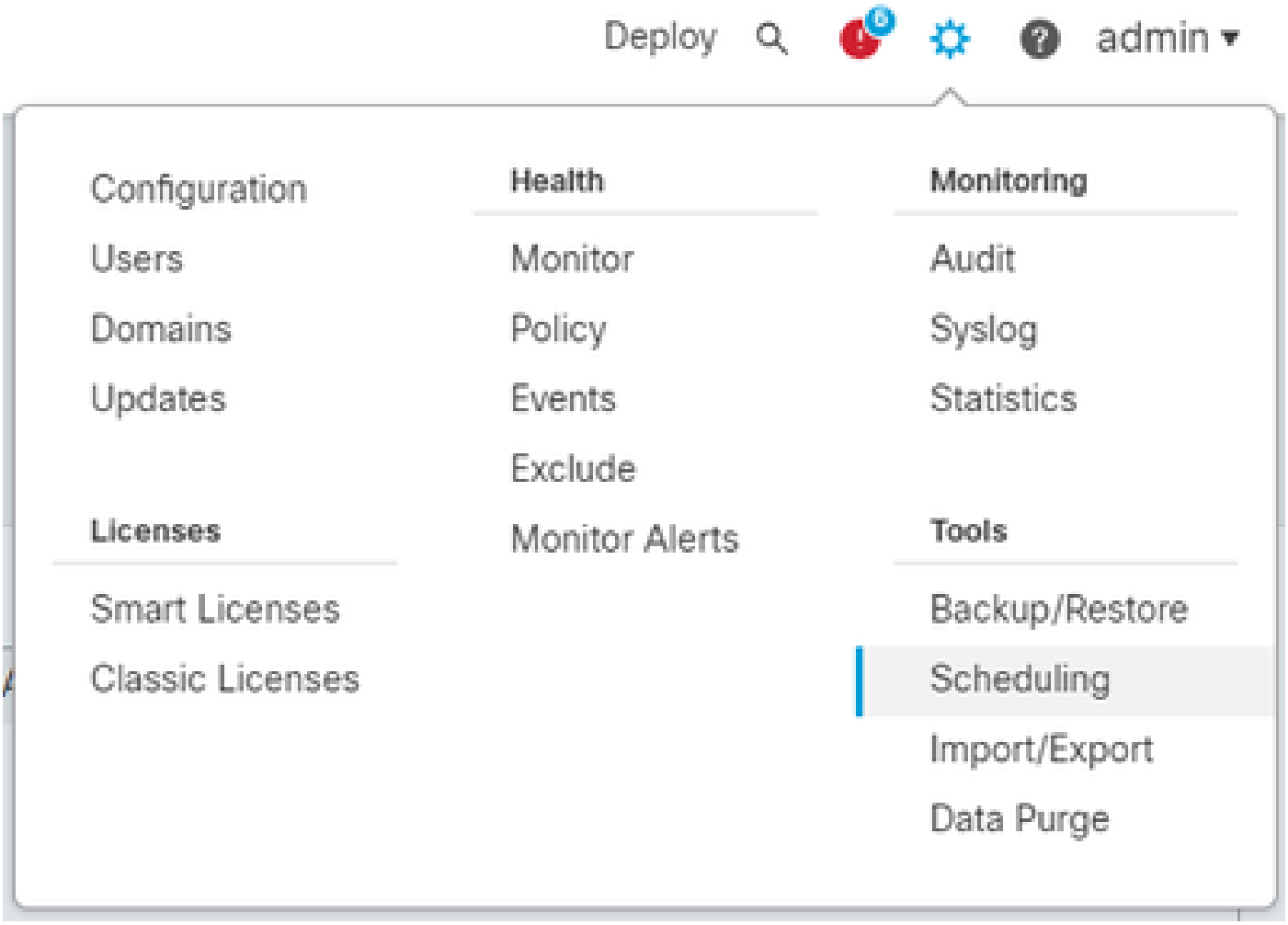
1. Log into Firepower Management Center.



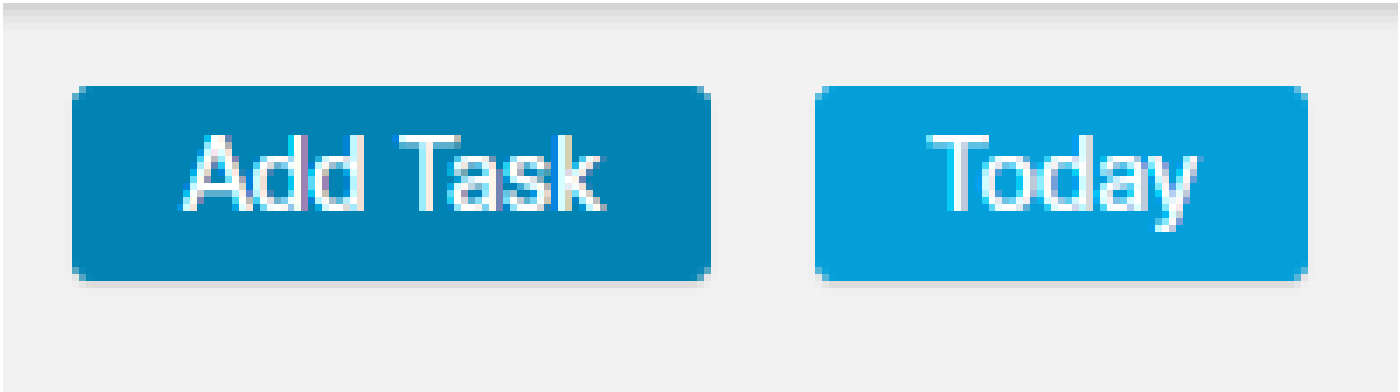
2. Navigate to **System(**



)> **Scheduling.**



3. On the top-right of the **Scheduling** screen, click the **Add Task** button.

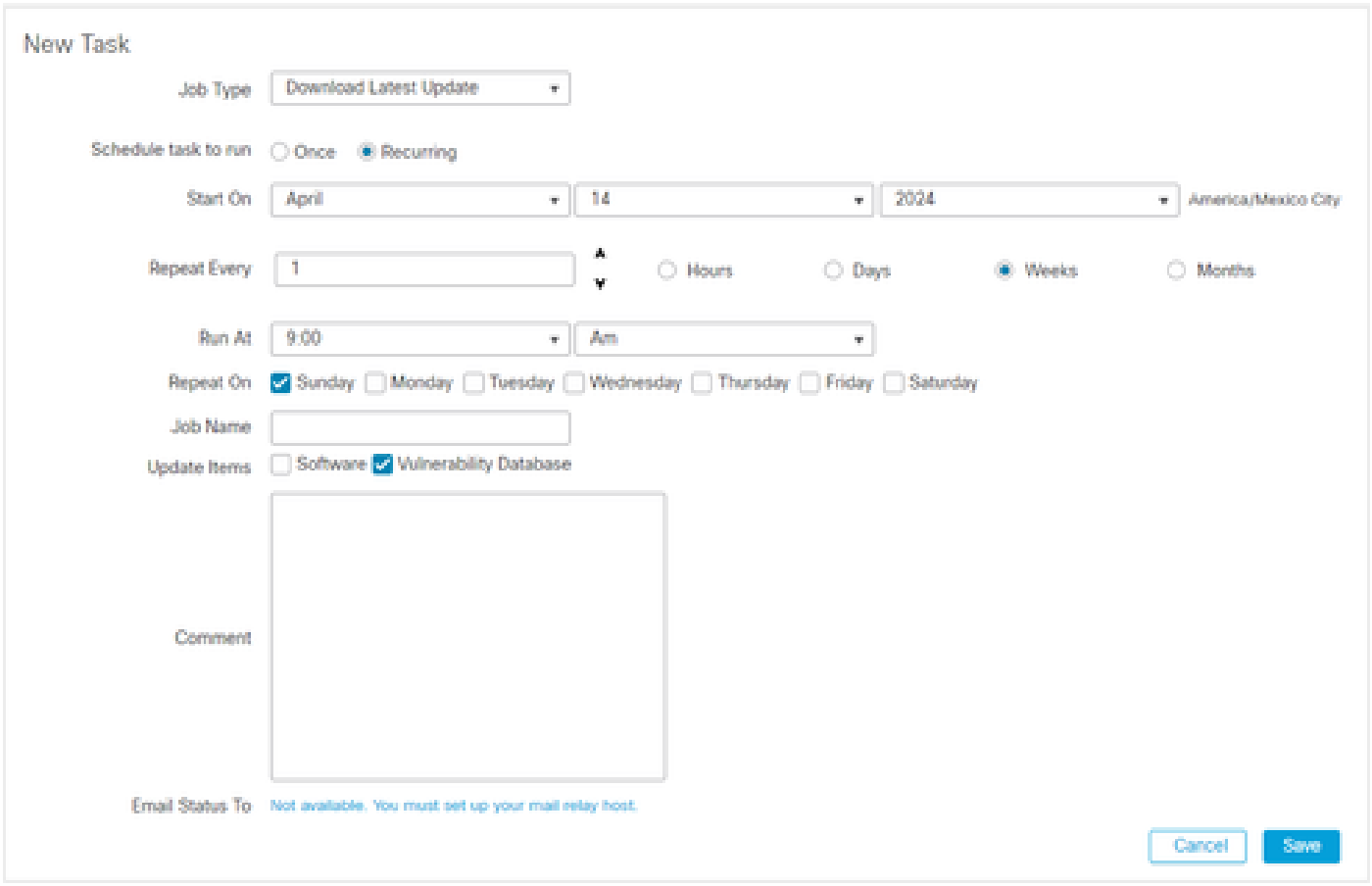


4. On the **New Task** screen, select **Download Latest Update** from **Job Type** drop-down menu and select the settings to fit your needs.

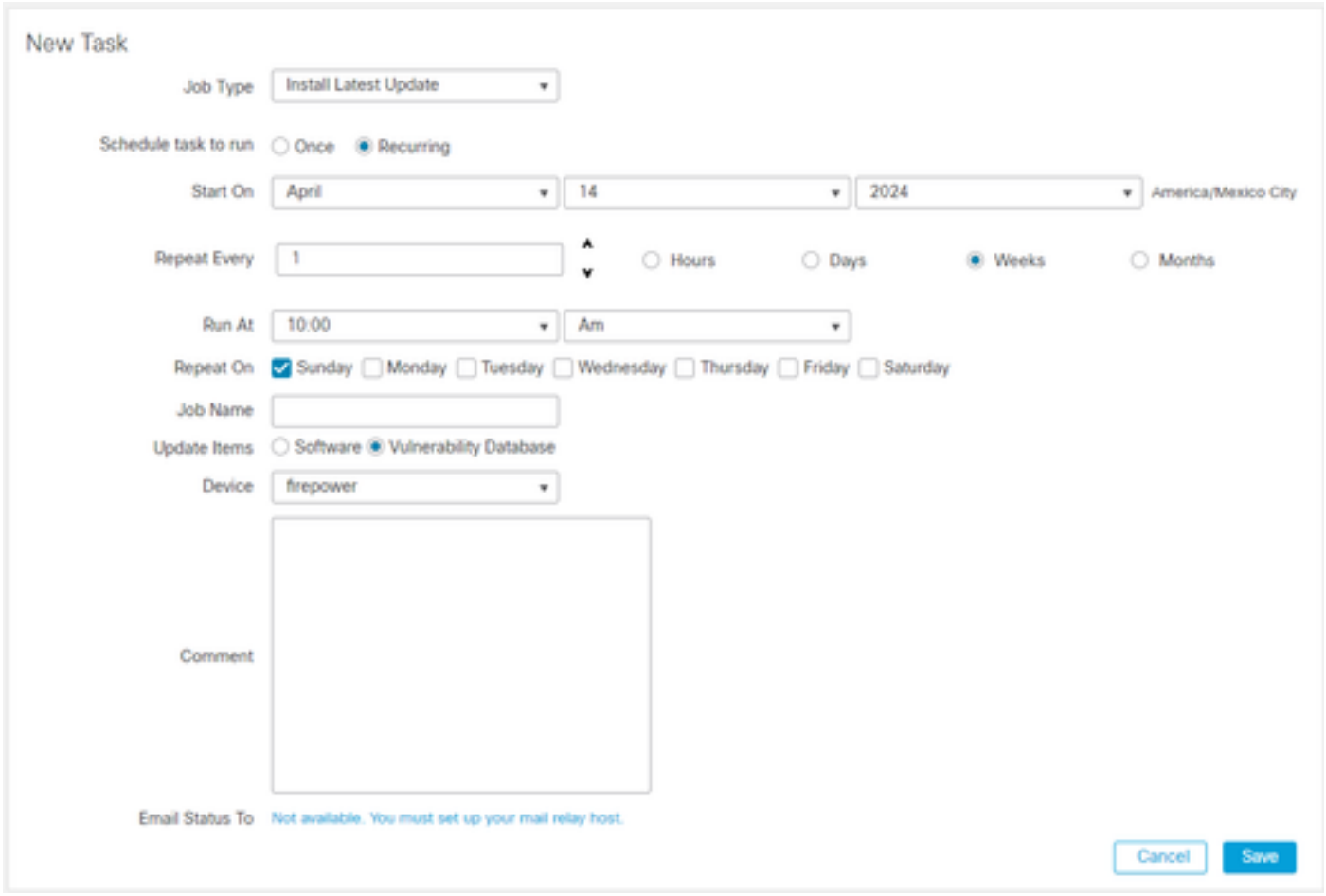
On the **Schedule task to run,** select **Recurring**.

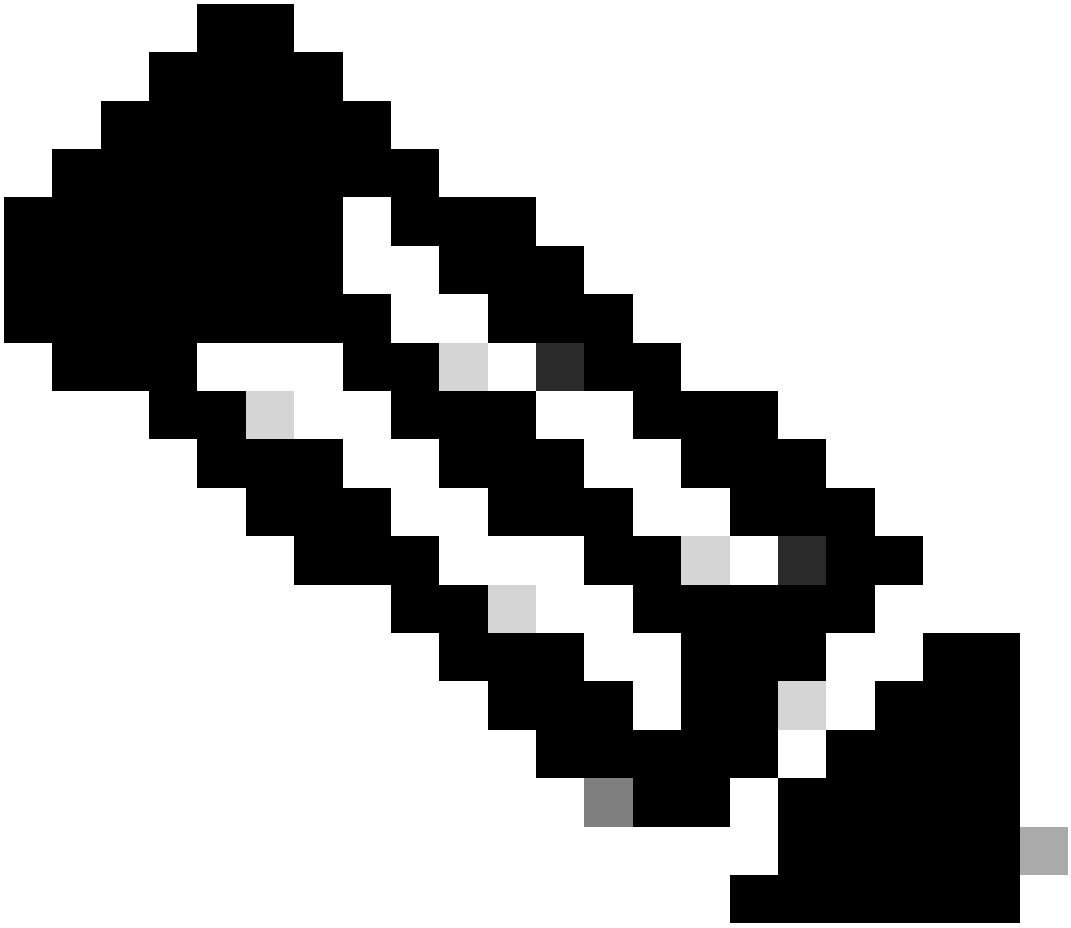
On the **Update Items** section, select **Vulnerability Database**.

Then, click **Save.**

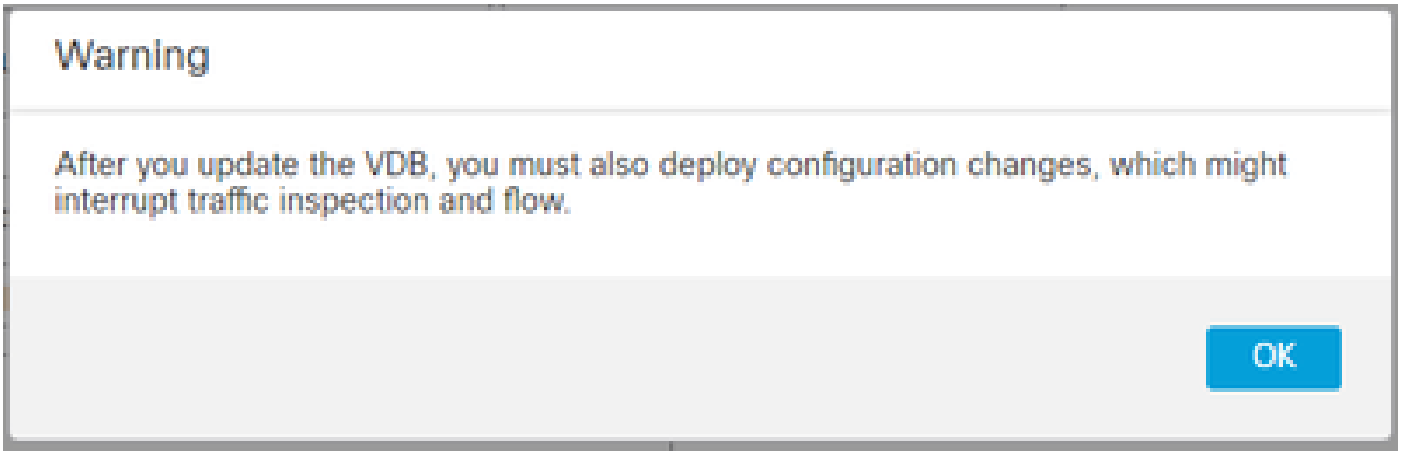


5. Repeat Step 3 to go back into the **New Task** screen and select **Install Latest Update** from the **Job Type** drop-down menu and use the settings to meet your needs and click **Save.**

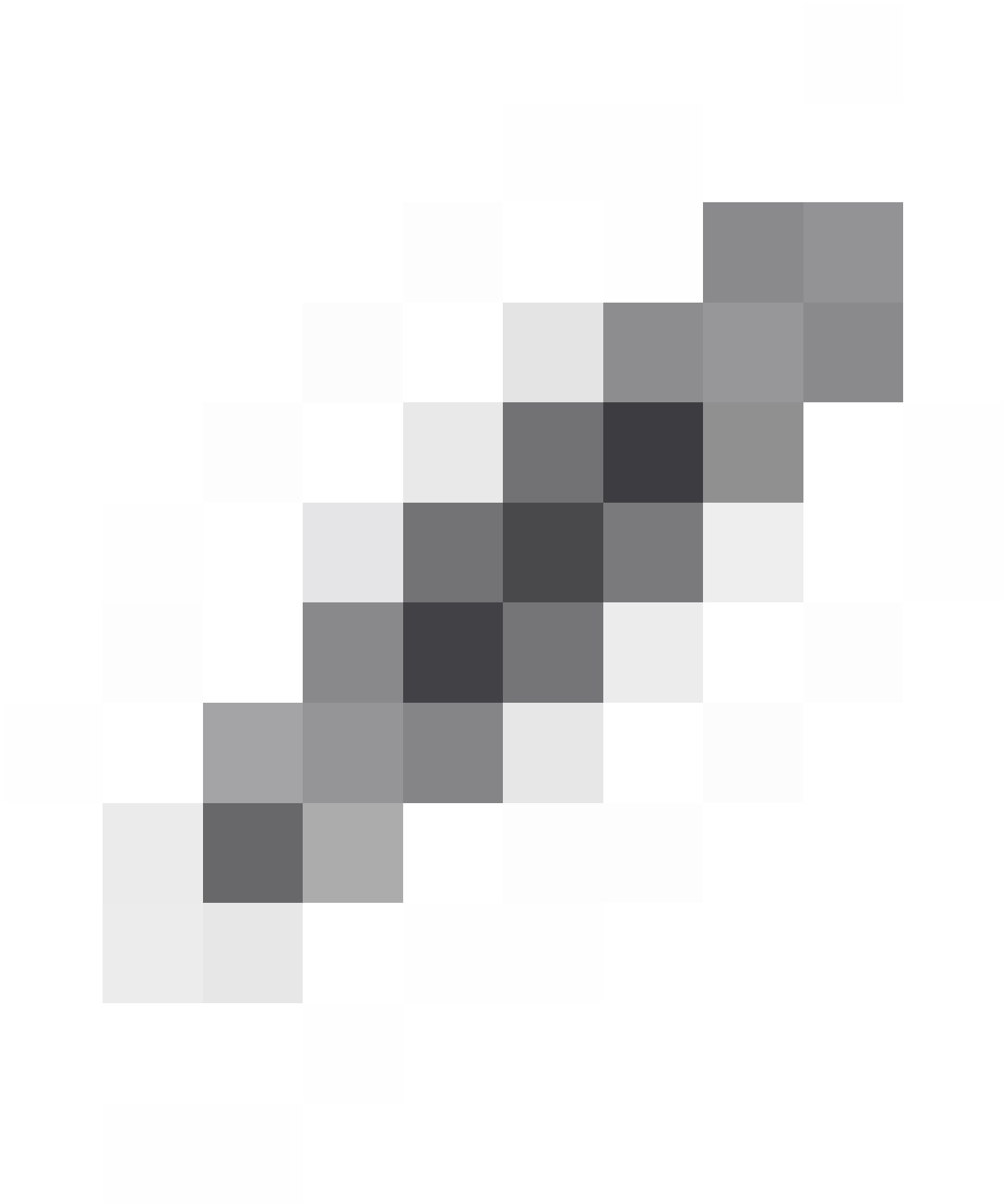




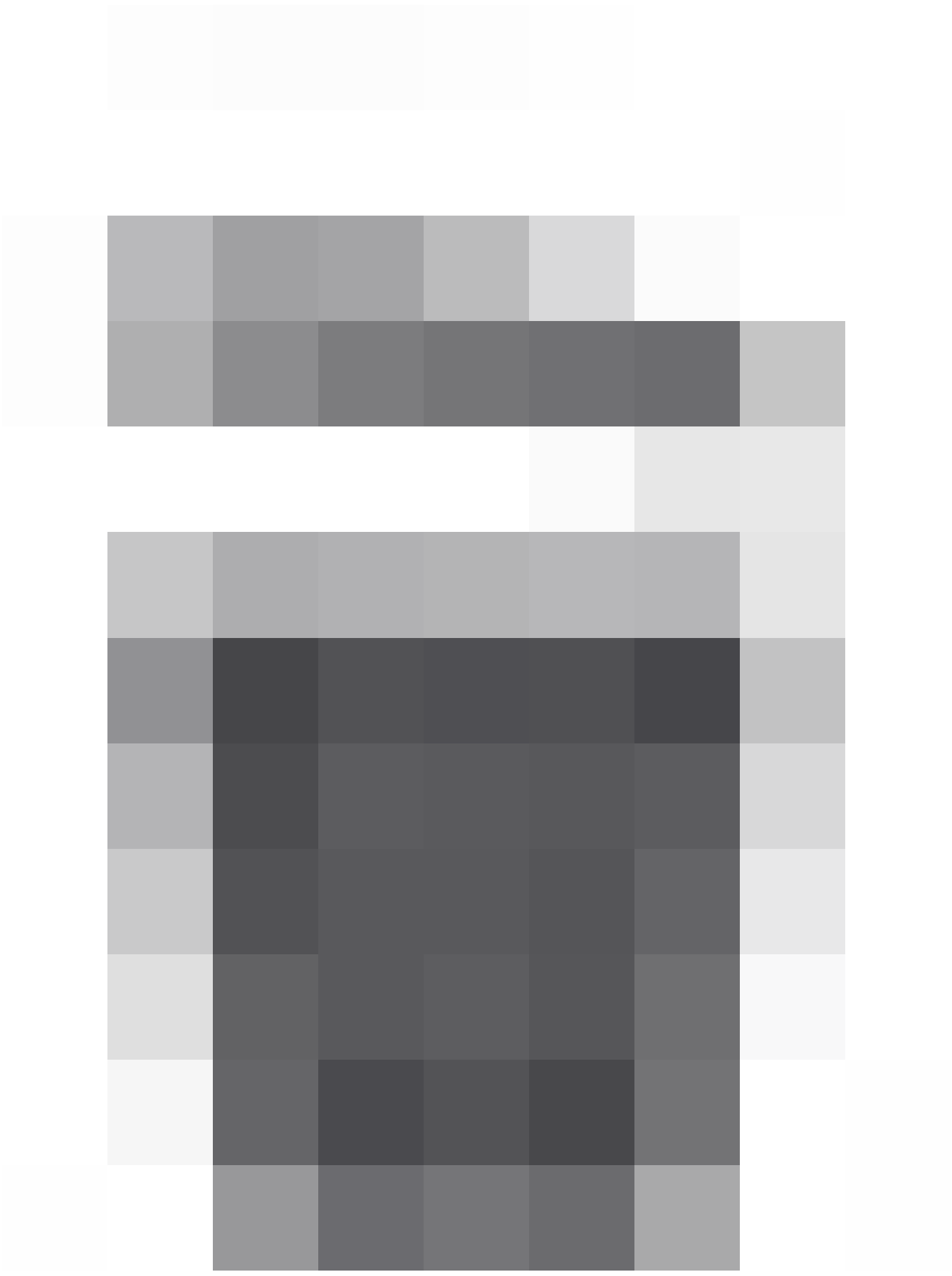
Note: be aware that after the VDB update, you must also deploy configuration changes which can interrupt traffic inspection and flow.

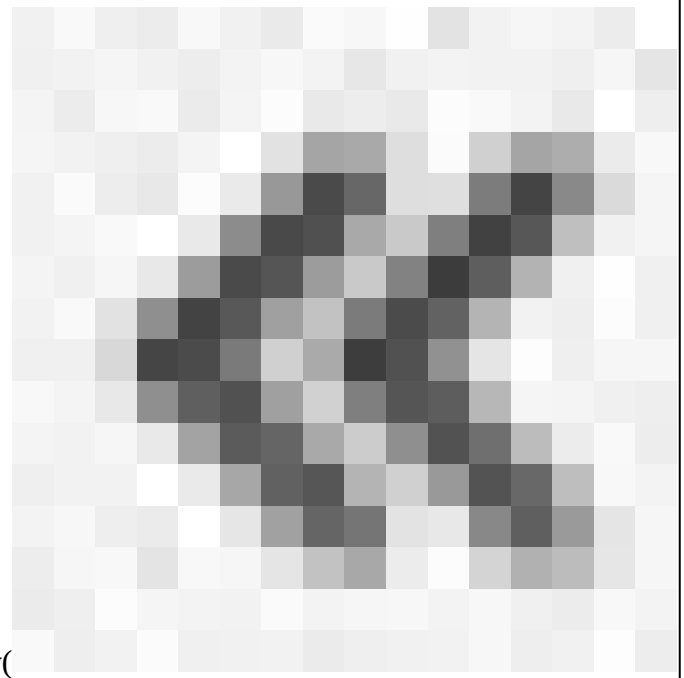
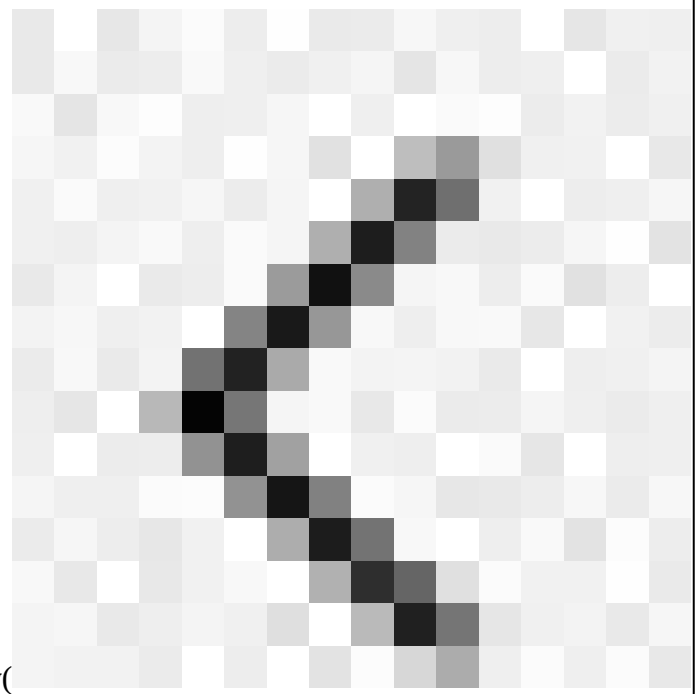


You can do fine tuning on the scheduled tasks by clicking the edit pen (



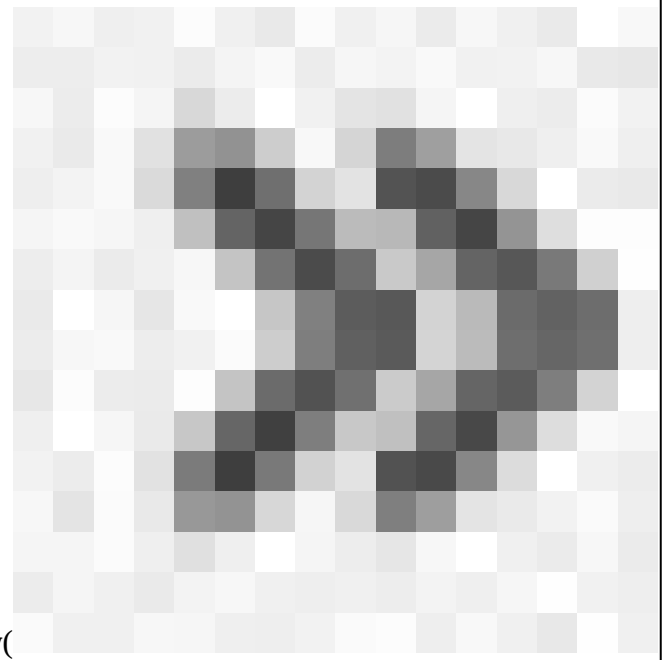
) or delete them by clicking the trash can (



Step 2	You can perform these tasks using the calendar view:  • Click**Double Left Arrow**( )to move back one year.  • Click**Single Left Arrow**( )to move back one month. • Click**Single Right Arrow**(



)to move forward one month.



- Click**Double Right Arrow**( )to move forward one year.
- Click**Today**to return to the current month and year.
- Click**Add Task**to schedule a new task.
- Click a date to view all scheduled tasks for the specific date in a task list table.

	• Click a specific task on a date to view it in a task list table.

Troubleshooting

In case the VDB automatic upgrade is not working as expected, you can rollback the VDB.

Steps:

SSH to the managing device (FMC, FDM, or SFR onbox) CLI.

Switch to expert mode, and root, and set the rollback variable:

<#root>

expert

sudo su
export ROLLBACK_VDB=1

Validate that the VDB package you intend to downgrade to is located on the device in /var/sf/updates and install it:

<#root>

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

Normal vdb install logs can be found at the applicable location at /var/log/sf/vdb-*

Once VDB install complete, deploy policy to devices.

On FMC, to check the installation status of VDB, these directory contents can be reviewed:

root@firepower:/var/log/sf/vdb-4.5.0-338# **ls -la**
total 40
drwxr-xr-x 5 root root 4096 May 15 2023 .
drwxr-xr-x 11 root root 4096 Apr 23 06:00 ..
-rw-r--r-- 1 root root 3308 May 15 2023 flags.conf.complete
drwxr-xr-x 2 root root 4096 May 15 2023 installer
drwxr-xr-x 2 root root 4096 May 15 2023 post
drwxr-xr-x 2 root root 4096 May 15 2023 pre
-rw-r--r-- 1 root root 1603 May 15 2023 **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

On FTD, to check the history of VDB installations, check these directory contents:

root@firepower:/ngfw/var/cisco/deploy/pkg/var/cisco/packages# **ls -al**
total 72912

drwxr-xr-x 5 root root 130 Sep 1 08:49 .
drwxr-xr-x 4 root root 34 Aug 16 14:40 ..
drwxr-xr-x 3 root root 18 Aug 16 14:40 exporter-7.2.4-169
-rw-r--r-- 1 root root 2371661 Jul 27 15:34 exporter-7.2.4-169.tgz
drwxr-xr-x 3 root root 21 Aug 16 14:40 **vdb-368**
-rw-r--r-- 1 root root 36374219 Jul 27 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 Sep 1 08:48 vdb-369.tgz

Related Information

Update Vulnerability Database (VDB)

Task Scheduling