

Configure a Regular Database Update Schedule for VDB on FDM

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Configurations](#)

[Verify](#)

[Troubleshooting](#)

[Related Information](#)

Introduction

This document describes how to configure a regular database update schedule for Rule or VDB on FDM.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Device Manager
- Vulnerability Database (VDB)

Components Used

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

- FDM 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.

Background Information

The Cisco Vulnerability Database (VDB) is a database of known vulnerabilities to susceptible hosts, as well as fingerprints for operating systems, clients, and applications.

The firewall system correlates the fingerprints with the vulnerabilities to help you determine whether a particular host increases your risk of network compromise. The Cisco Talos Intelligence Group

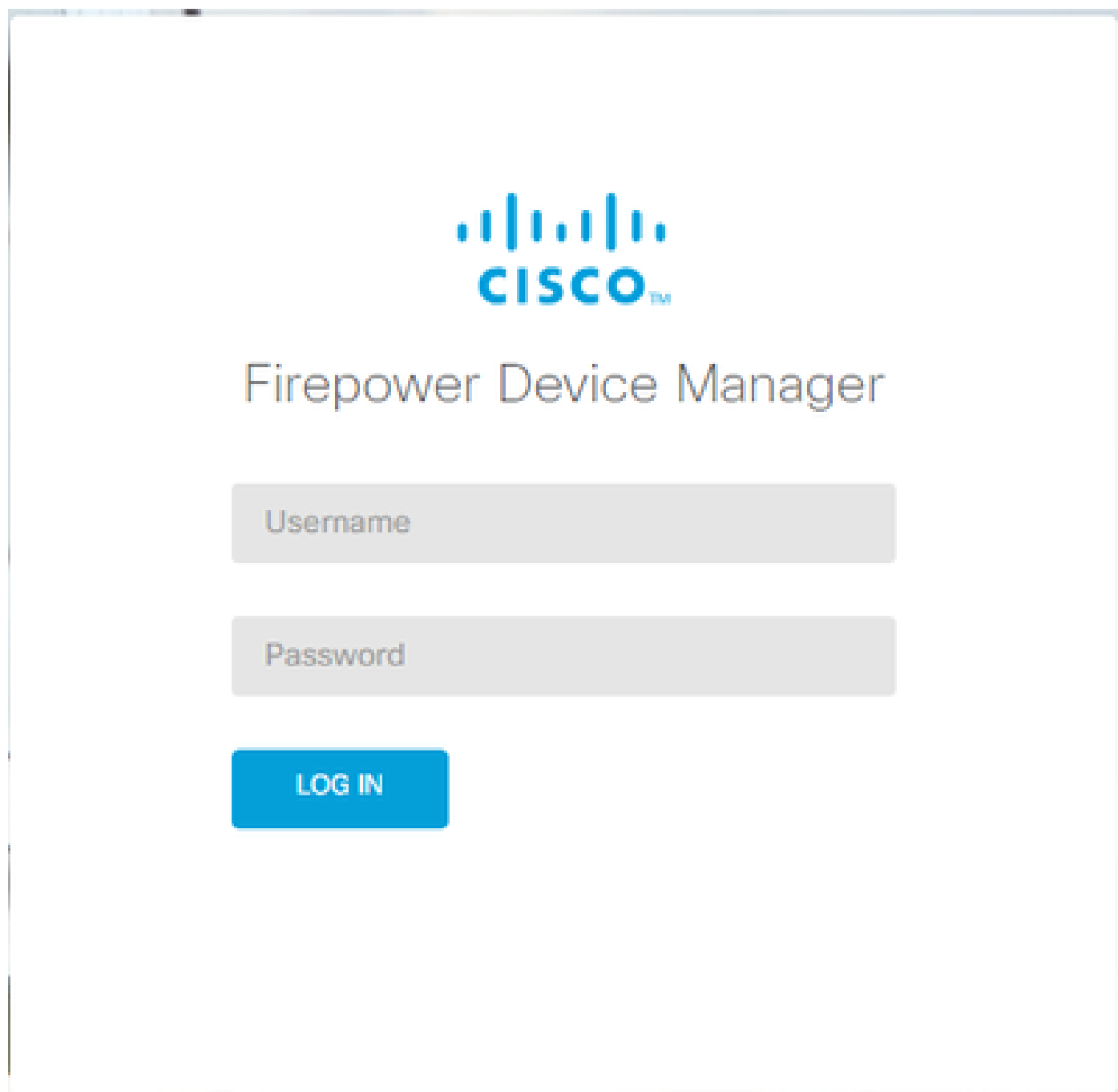
(Talos) issues periodic updates to the VDB.

It is recommended to enable the automatic scheduler during the onboarding process to regularly check for and apply security database updates. This ensures that the device stays up to date.

Configure

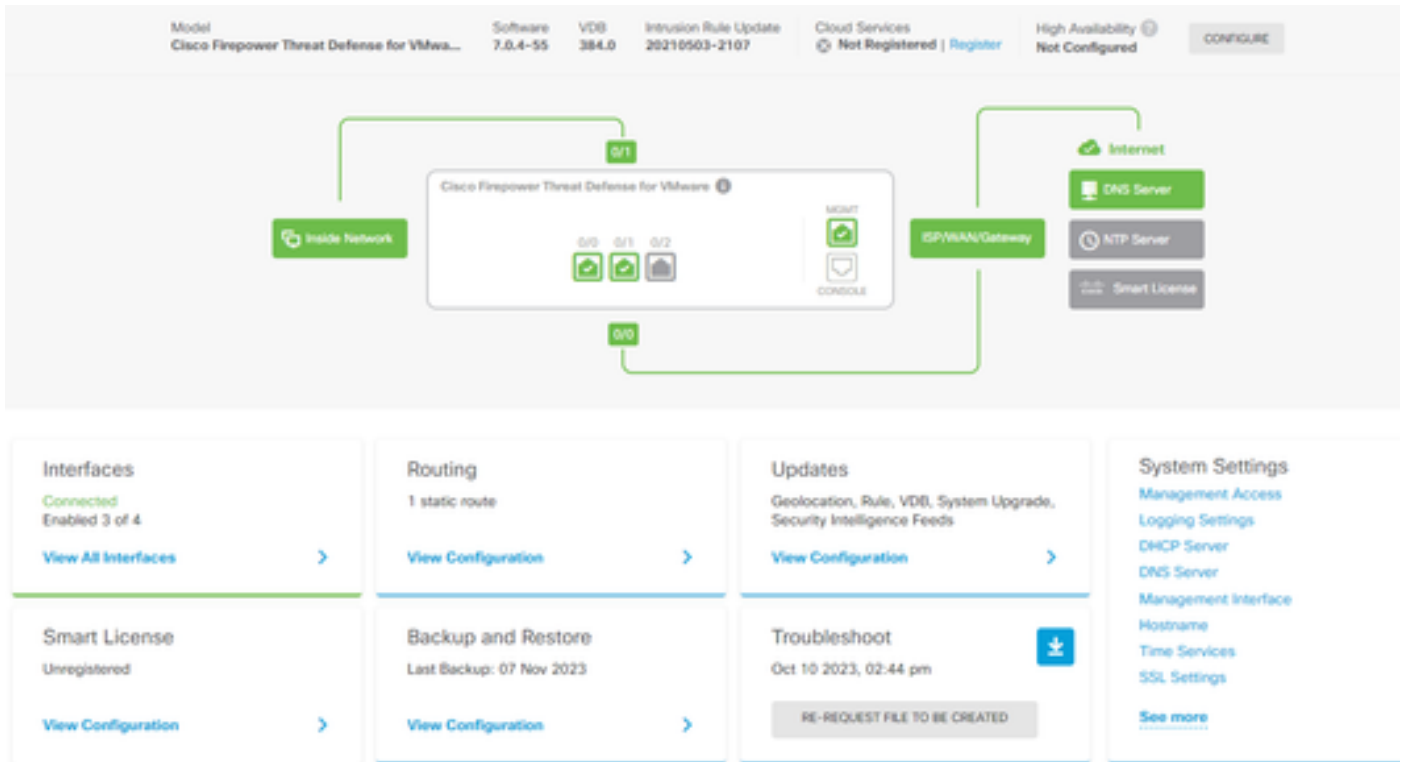
Configurations

1. Log into Firepower Device Manager

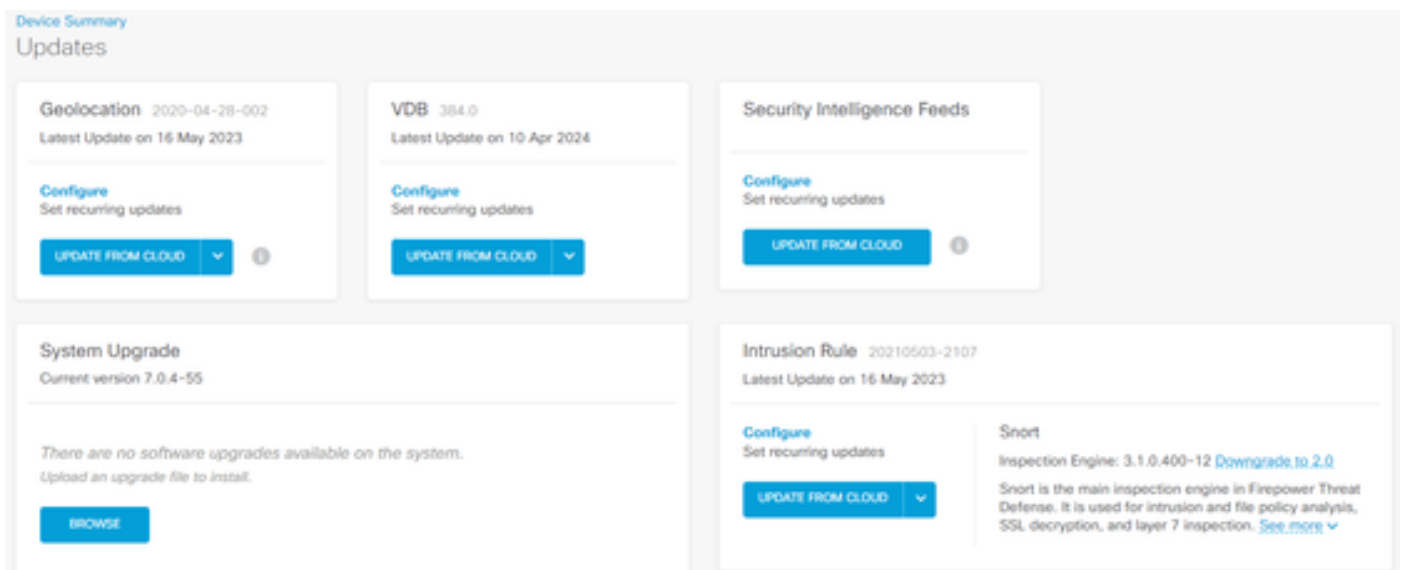


The screenshot shows the login interface for Cisco Firepower Device Manager. At the top center is the Cisco logo, consisting of a stylized signal icon above the word "CISCO" with a trademark symbol. Below the logo, the text "Firepower Device Manager" is displayed in a large, sans-serif font. Underneath, there are two input fields: the first is labeled "Username" and the second is labeled "Password". Both fields are currently empty. Below the password field is a blue rectangular button with the text "LOG IN" in white, uppercase letters.

2. On the **Devices** screen, navigate to **Updates > View Configuration**.



3. On the **Updates** screen, navigate to **VDB > Configure**.



4. On the **Set recurring updates** screen, change the default settings to your needs and click **Save**.

Set recurring updates ✕

Frequency

Weekly ▾

Days of Week

Sundays ✕ ▾ at 11 ▾ : 00 ▾

Time (UTC-05:00)
America/Mexico_City

Automatically deploy the update.
(Note: The deployment will also deploy all pending configuration changes.)

DELETE CANCEL SAVE

Verify

On the **Updates** screen, on the **VDB** section, the selected recurrent update option is reflected.

Device Summary

Updates

✔ **Schedule for VDB updates has been created**

Geolocation 2020-04-28-002

Latest Update on 16 May 2023

Configure

Set recurring updates

UPDATE FROM CLOUD



VDB 384.0

Latest Update on 10 Apr 2024



Weekly

on Sundays at 11:00 AM [Edit](#)

(UTC-05:00) America/Mexico_City

UPDATE FROM CLOUD



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>
```

Follow normal vdb install logs at the applicable location at **/var/log/sf/vdb-***

Once VDB install complete, deploy policy to devices.

On FTD CLI, to check the history of VDB installations, one way is to 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 14:40vdb-368
-rw-r--r-- 1 root root 36374219 Jul 27 15:34 vdb-368.tgz
drwxr-xr-x 3 root root 21 Sep 1 08:49vdb-369
-rw-r--r-- 1 root root 35908455 Sep 1 08:48 vdb-369.tgz
```

Related Information

[Updating System Databases](#)