Rollback VDB Version for Secure Firewall Management Center and Secure Firewall Device Manager

Contents

Introduction

This document describes the process to rollback the Vulnerability Database (VDB) for the Secure Firewall Management Center (FMC) and for the Secure Firewall Device Manager (FDM).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco Secure Firewall Management Center version 7.3 and VDB 361+
- Cisco Secure Firewall Management Center version 7.2.1 and VDB 343+
- Cisco Secure Firewall Device Manager version 7.0.6 and VDB 395+

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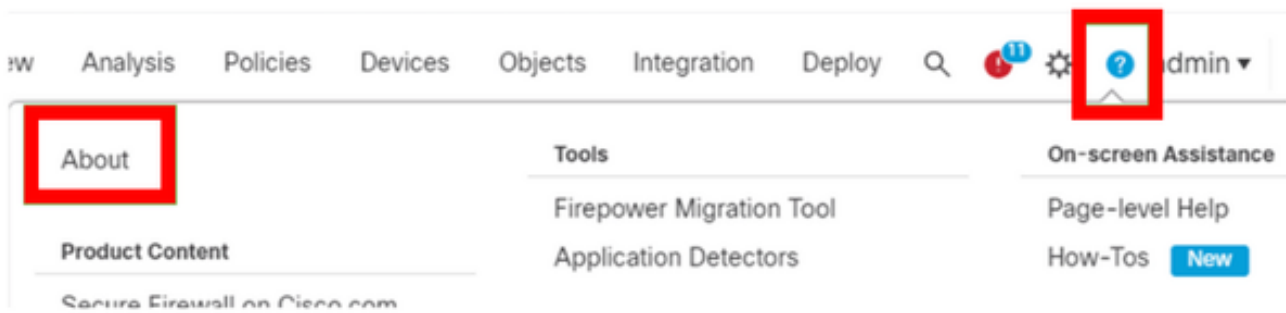
devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Initial Configurations

Initial configuration for FMC

From the FMC GUI, you can confirm the actual VDB version running by going to the **MainMenu >** **> About.**

From the FMC CLI, you can confirm the actual VDB version running with next command, **show version**:

<#root>

> show version

```
-------------------[ firepower ]--------------------
Model : Secure Firewall Management Center for VMware (66) Version 7.3.0 (Build 69)
UUID : e8f4b5de-4da1-11ed-b2ce-4637a3ef82f7
Rules update version : 2023-07-12-002-vrt
LSP version : lsp-rel-20230712-1621
```

VDB version : 361

```
----------------------------------------------------
```

Initial configuration for FDM

From the FDM GUI, you can confirm the actual VDB version running by going to the **Monitoring** dashboard, as follows:
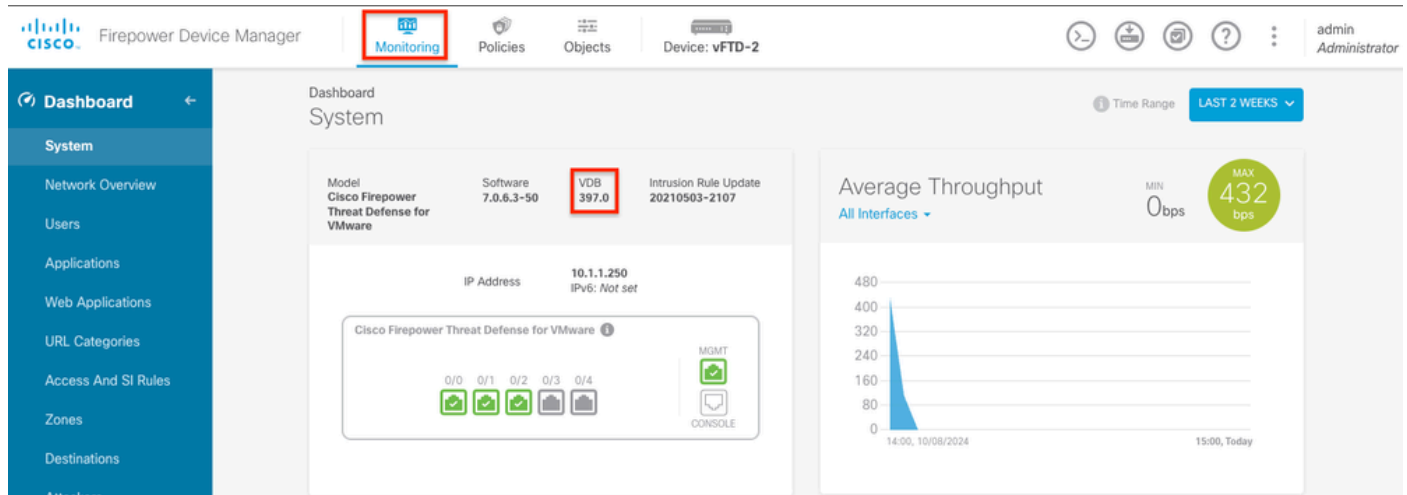
From the FDM CLI, you can confirm the actual VDB version running with next command '**cat /etc/sf/.versiondb/vdb.conf**':

```
root@vFTD-2:/ngfw/var/cisco/deploy/pkg/var/cisco/packages# cat /etc/sf/.versiondb/vdb.conf
CURRENT_VERSION=4.5.0
CURRENT_BUILD=397
CURRENT_APPID_VER=138
CURRENT_NAVL_VER=158
```

VDB Rollback Process for FMC v7.3+

These are the steps to follow to rollback the VDB version for an FMC v7.3+, in the next example we are rolling back from VDB 361 to VDB 359.
1. In case the VDB file to rollback to, is no longer stored on the FMC, then, you will need to upload it to the FMC, for this, navigate to **System (**
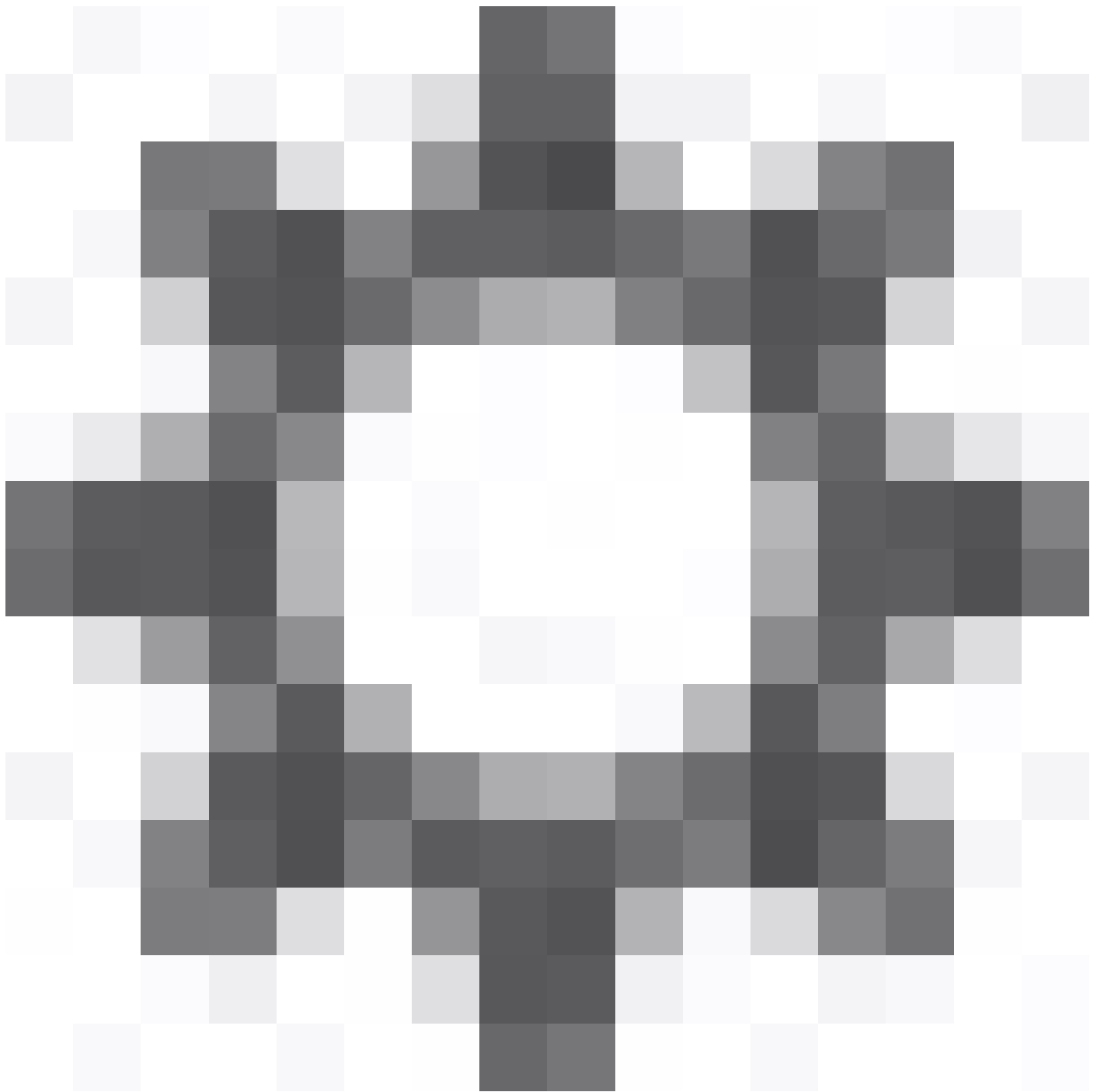
) > Updates > Product Updates > Available Updates> Upload Updates, select the VDB File from your local computer and click on **Upload**.

2. Once the VDB file is uploaded to the FMC, then, the older VDB version (version 359 in this example) will display the **Rollback** icon instead of the **Install** icon.

3. To proceed to rollback from VDB 361 to VDB 359, then, click on the rollback button.
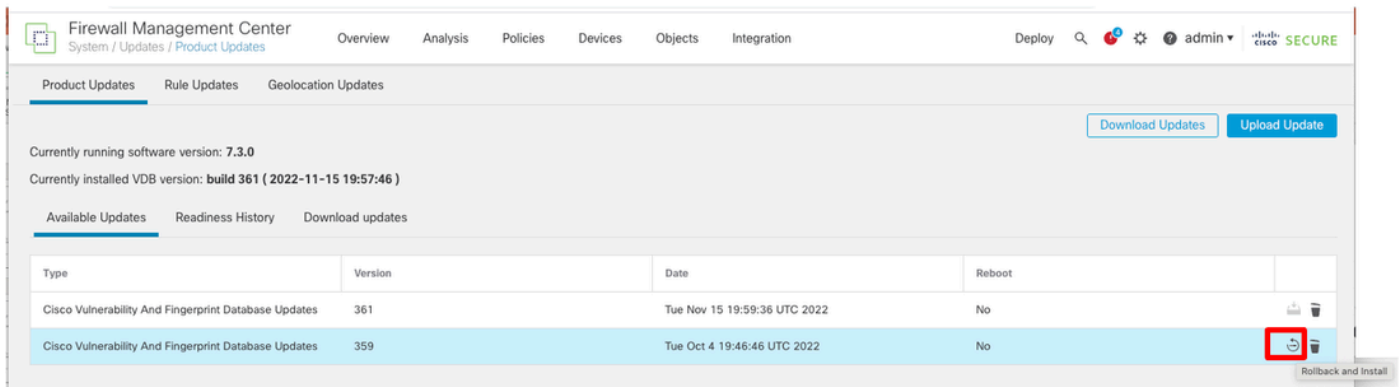
4. Then, check the FMC checkbox and click on **Install**.

5. A warning prompt is displayed to inform you about potential traffic disruption in case you deploy changes to the managed devices after the VDB rollback.
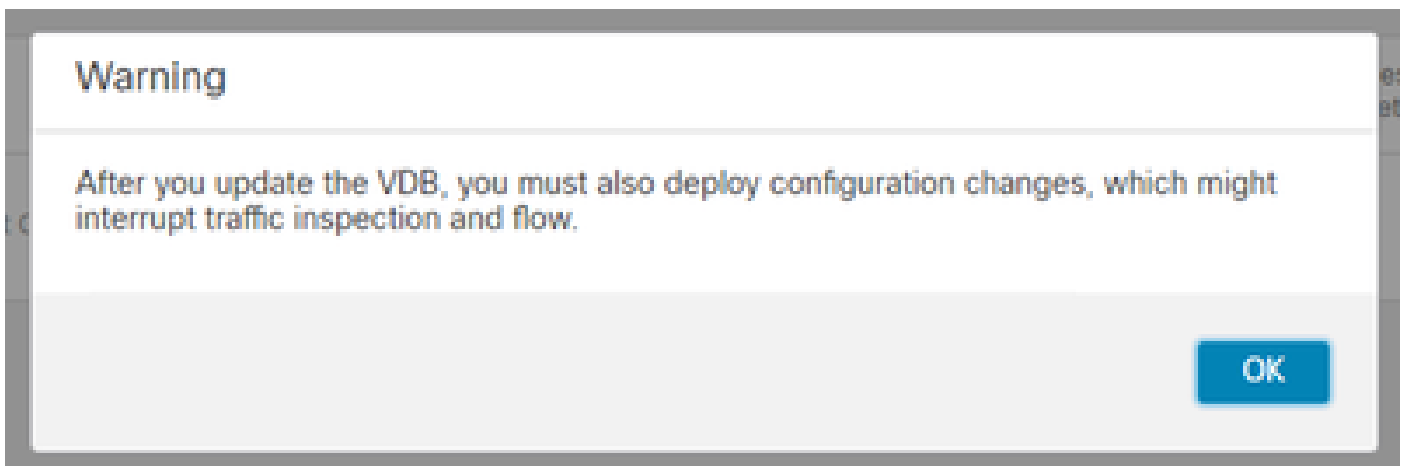
VDB Rollback Process for FMC v7.2.x and earlier

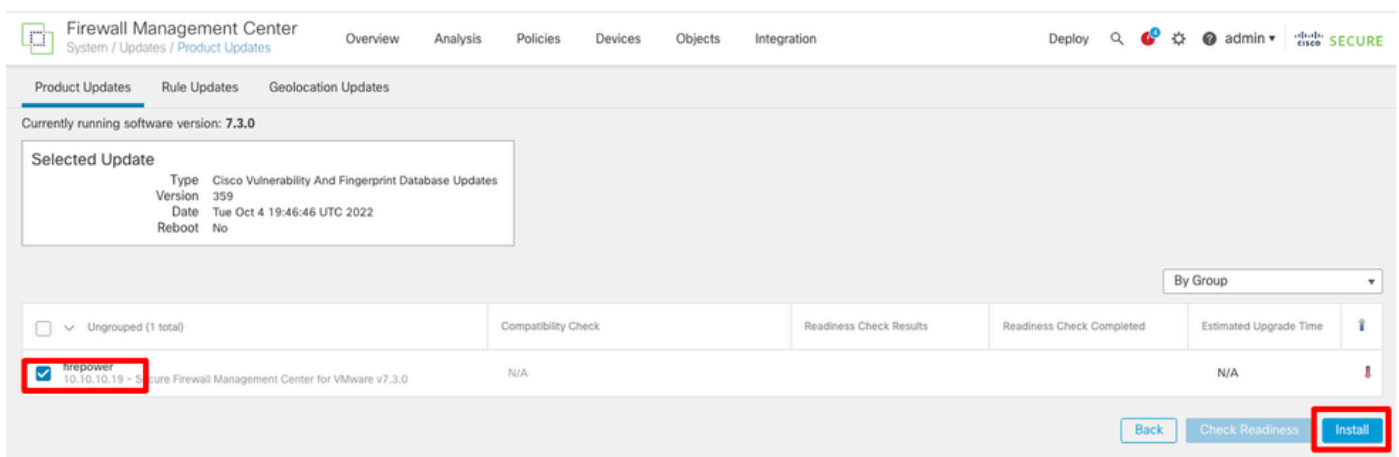These are the steps to follow to rollback the VDB version for an FMC v7.2.x and earlier.

1. SSH to the FMC CLI.

2. Switch to expert mode, and root, and set the rollback variable to '1', as follows:

<#root>

```
>expert
```

```
$sudo su
#export ROLLBACK_VDB=1
```

3. Validate that the VDB package you intend to rollback to, is located at the next FMC directory **/var/sf/updates**, in case the VDB file is not in this path, then upload the VDB file required to the FMC.

4. Then, proceed with the VDB rollback installation by entering next command:

<#root>

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

Example:

```
root@FMC:/var/sf/updates# install_update.pl --detach /var/sf/updates/Cisco_VDB_Fingerprint_Database-4.5
ARGV[0] = --detach
ARGV[1] = /var/sf/updates/Cisco_VDB_Fingerprint_Database-4.5.0-394.sh.REL.tar
bundle_filepath: /var/sf/updates/Cisco_VDB_Fingerprint_Database-4.5.0-394.sh.REL.tar
install_update.pl begins. bundle_filepath: /var/sf/updates/Cisco_VDB_Fingerprint_Database-4.5.0-394.sh.
Makeself GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_VDB_Fingerprint_Database-4.5.0-3
FILEPATH directory name /var/tmp/upgrade-patch at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm 1
Inside GetInfo FILEPATH :/var/tmp/upgrade-patch/Cisco_VDB_Fingerprint_Database-4.5.0-394.sh at /usr/loc
Use of uninitialized value in string ne at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm line 125
```

4. Monitor the vdb installation logs at the next directory location **/var/log/sf/<VDB Package file>** and check the VDB install progress from the **status.log** file.

```
root@FMC:/var/log/sf/vdb-4.5.0-394# tail -f status.log
state:running
ui:The install has begun.
ui:[ 0%] Running script pre/000_start.sh...
ui:[ 4%] Running script pre/001_check_required_upgrade.pl...
ui:[ 8%] Running script pre/005_check_low_end.pl...
ui:[12%] Running script pre/010_check_versions.sh...
ui:[15%] Running script pre/011_check_versions.pl...
ui:[19%] Running script pre/020_check_space.sh...
ui:[23%] Running script pre/500_stop_rna.pl...
ui:[27%] Running script pre/999_finish.sh...
ui:[31%] Running script installer/000_start.sh...
ui:[35%] Running script installer/100_install_files.pl...
ui:[38%] Running script installer/200_install_fingerprints.sh...
ui:[42%] Running script installer/300_install_vdb.sh...
ui:[46%] Running script installer/400_install_rdps.pl...
ui:[50%] Running script installer/420_delete_obsolete_ids.pl...
ui:[54%] Running script installer/430_change_dupe_custom_app_names.pl...
ui:[58%] Running script installer/450_resave_detectors.pl...
```

```
ui:[62%] Running script installer/480_update_dynamic_config_with_csds.pl...
ui:[65%] Running script installer/525_export_compliance_policies.pl...
ui:[69%] Running script installer/900_update_version.sh...
ui:[73%] Running script installer/901_update_db_version.pl...
ui:[77%] Running script installer/950_reapply_to_sensor.pl...
ui:[81%] Running script installer/975_export_data.pl...
ui:[85%] Running script installer/999_finish.sh...
ui:[88%] Running script post/000_start.sh...
ui:[92%] Running script post/500_start_rna.pl...
ui:[96%] Running script post/999_finish.sh...
ui:[100%] The install completed successfully.
ui:The install has completed.
state:finished
```

5. Once the VDB installation is completed, then, execute a policy deployment to the managed devices (In order to execute the policy deployment, a minimum change needs to be made in the configuration).

6. From the FMC CLI, run the **show version** command to confirm the actual VDB version running.

```
> show version
----------------[ FMC ]-----------------
Model                   : Secure Firewall Management Center for VMware (66) Version 7.2.1 (Build 40)
UUID                    : 597fda3e-386e-11ed-95e2-dbc141b3e897
Rules update version    : 2022-09-14-001-vrt
LSP version             : lsp-rel-20220511-1540
VDB version             : 394
----------------------------------------------------
```

VDB Rollback Process for FMC HA

1. Pause the FMC HA sync and then rollback the VDB on each FMC.

2. Once the VDB rollback process is done for each FMC, then resume the FMC HA.

- The HA page might still show "**vdb not in sync**" with the VDB version mismatch, this message can be ignored.

3. If after executing the rollback VDB process for the FMC, this does not work and the latest VDB update gets automatically re-installed, then locate the latest VDB files and delete them from below directories for both FMCs:

```
/var/sf/updates (.sh file)
/var/cisco/pacakges/ (.tgz file)
```

4. Then, repeat the steps 1 and 2 above to rollback the VDB for the FMC HA.

VDB Rollback Process for FDM

To rollback the VDB version for an FDM, proceed to open a Cisco TAC case and request for assistance by pointing the TAC engineer to this Cisco document.

Verify

From FTD CLI

On FTD, to check the history of VDB installations, one way is to check the following directory contents:

<#root>

```
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
```

From FMC GUI

Once the rollback task is completed, the VDB version can be confirmed under the main **Menu >**
> About.

Finally, after the VDB is rolled back, a policy deployment is required to push the new VDB configuration to the FMC managed Firewalls.

Limitations

- The VDB rollback button is not available for FMC versions prior to 7.3.

- You are not allowed to rollback the VDB to a version older than 357, if a VDB version older than 357 is uploaded to the FMC, then, the rollback button is grayed out.

| Cisco Vulnerability And Fingerprint Database Updates | 354 | | Wed Apr 27 19:42:09 UTC 2022 | No | ⊖ 🗑 |

VDB rollback is only supported starting with VDB version 357

- If the VDB version is lower than the base VDB version of the FMC, the successful rollback task that is completed is displayed, however, the VDB version displayed continue showing the same as prior the rollback attempt.

● Deployments   Upgrades   ● Health   ● Tasks   Show Notifications

| 20+ total | 0 waiting | 0 running | 0 retrying | 20+ success | 5 failures | 🔍 Filter |

✅ Local Install

Installing Cisco Vulnerability And Fingerprint Database Updates version: VDB-357   14s ✕
Successfully Installed

CISCO SECURE

Firewall Management Center

Version 7.3.0 (build 69)

Model	Secure Firewall Management Center for VMware
Serial Number	None
Snort Version	2.9.21 (Build 105)
Snort3 Version	3.1.36.1 (Build 101)
Rule Pack Version	2868
Module Pack Version	3244
LSP Version	lsp-rel-20230712-1621
VDB Version	build 361 (2022-11-15 19:57:46)
Rule Update Version	2023-07-12-002-vrt
Geolocation Update Version	Country Code: 2023-06-17-100, IP: 2023-06-17-100
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.13.0 (build 198)
Hostname	firepower

For technical/system questions, email tac@cisco.com phone: 1-800-553-2447 or 1-408-526-7209. Copyright 2004-2022, Cisco and/or its affiliates. All rights reserved.

Copy   Close

From the FMC CLI you can confirm that this happened because the rollback target version is lower than the base FMC version. This can be confirmed on the FMC CLI on the status.log file.

```
> expert
sudo su
cd /var/log/sf/vdb-4.5.0-<vdb number>/
cat status.log

root@firepower:/var/log/sf/vdb-4.5.0-357# cat status.log
state:running
ui:The install has begun.
ui:[ 0%] Running script pre/000_start.sh...
ui:[ 4%] Running script pre/010_check_versions.sh...
ui:[ 4%] Non-Fatal error: Non-Fatal error: Cannot rollback to version(357) lower than default VDB 358
ui:[ 4%] The install completed successfully.
ui:The install has completed.
state:finished


-----------------------------------------------------
```

Related Information

- **Cisco Technical Support & Downloads**