

Upgrade Procedure through FMC for Firepower Devices

Contents

- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Components Used](#)
- [Procedure](#)
- [Verify](#)
- [Firepower Management Center Upgrade](#)
- [Firepower Devices Upgrade](#)
- [Troubleshoot](#)

Introduction

This document describes the procedure to upgrade devices with Firepower Services, Adaptive Security Appliance (ASA), FTD and FMC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these products:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- FirePOWER (SFR) service module running on ASA

It is also required to download the software for firepower devices from:

<https://software.cisco.com/download/find/firepower>

Components Used

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

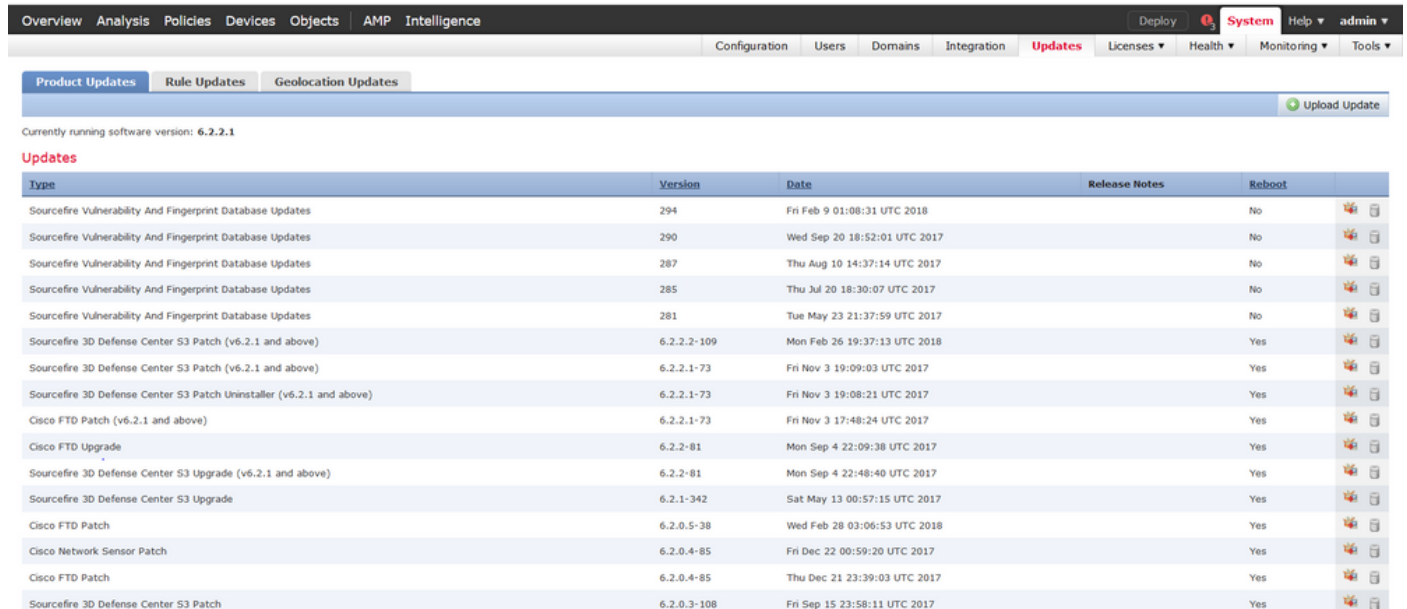
- Firepower Management Center
- FirePOWER service module running on ASA

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.

Procedure

Step 1. Navigate to **System > updates** and look for the version you want to upgrade to, as shown in the image.



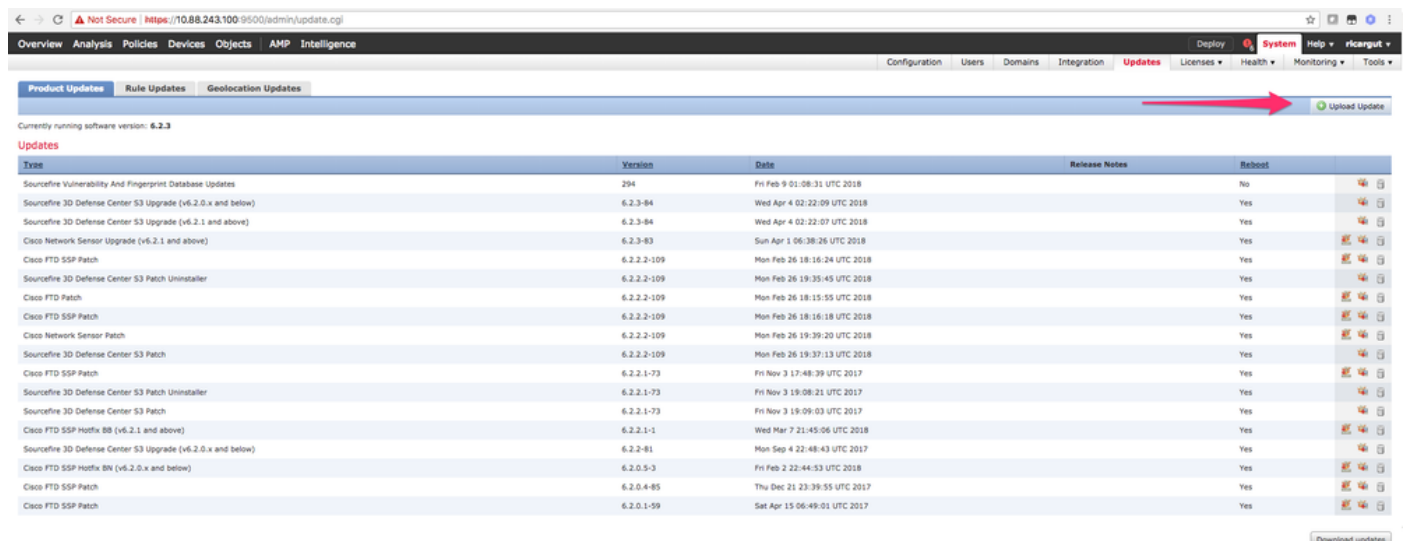
The screenshot shows the Cisco FMC interface with the 'System > updates' page. The 'Updates' tab is selected, and the 'Upload Update' button is visible. The table below lists various updates with their types, versions, dates, release notes, and reboot requirements.

| Type | Version | Date | Release Notes | Reboot | |
|--|-------------|------------------------------|---------------|--------|--|
| Sourcefire Vulnerability And Fingerprint Database Updates | 294 | Fri Feb 9 01:08:31 UTC 2018 | | No | |
| Sourcefire Vulnerability And Fingerprint Database Updates | 290 | Wed Sep 20 18:52:01 UTC 2017 | | No | |
| Sourcefire Vulnerability And Fingerprint Database Updates | 287 | Thu Aug 10 14:37:14 UTC 2017 | | No | |
| Sourcefire Vulnerability And Fingerprint Database Updates | 285 | Thu Jul 20 18:30:07 UTC 2017 | | No | |
| Sourcefire Vulnerability And Fingerprint Database Updates | 281 | Tue May 23 21:37:59 UTC 2017 | | No | |
| Sourcefire 3D Defense Center S3 Patch (v6.2.1 and above) | 6.2.2.2-109 | Mon Feb 26 19:37:13 UTC 2018 | | Yes | |
| Sourcefire 3D Defense Center S3 Patch (v6.2.1 and above) | 6.2.2.1-73 | Fri Nov 3 19:09:03 UTC 2017 | | Yes | |
| Sourcefire 3D Defense Center S3 Patch Uninstaller (v6.2.1 and above) | 6.2.2.1-73 | Fri Nov 3 19:08:21 UTC 2017 | | Yes | |
| Cisco FTD Patch (v6.2.1 and above) | 6.2.2.1-73 | Fri Nov 3 17:48:24 UTC 2017 | | Yes | |
| Cisco FTD Upgrade | 6.2.2-81 | Mon Sep 4 22:09:38 UTC 2017 | | Yes | |
| Sourcefire 3D Defense Center S3 Upgrade (v6.2.1 and above) | 6.2.2-81 | Mon Sep 4 22:48:40 UTC 2017 | | Yes | |
| Sourcefire 3D Defense Center S3 Upgrade | 6.2.1-342 | Sat May 13 00:57:15 UTC 2017 | | Yes | |
| Cisco FTD Patch | 6.2.0.5-38 | Wed Feb 28 03:06:53 UTC 2018 | | Yes | |
| Cisco Network Sensor Patch | 6.2.0.4-85 | Fri Dec 22 00:59:20 UTC 2017 | | Yes | |
| Cisco FTD Patch | 6.2.0.4-85 | Thu Dec 21 23:39:03 UTC 2017 | | Yes | |
| Sourcefire 3D Defense Center S3 Patch | 6.2.0.3-108 | Fri Sep 15 23:58:11 UTC 2017 | | Yes | |

If the version that you want to upgrade is not shown on the screen, continue with step 2.

If the version that you want to upgrade is shown on the screen, continue with step 4.

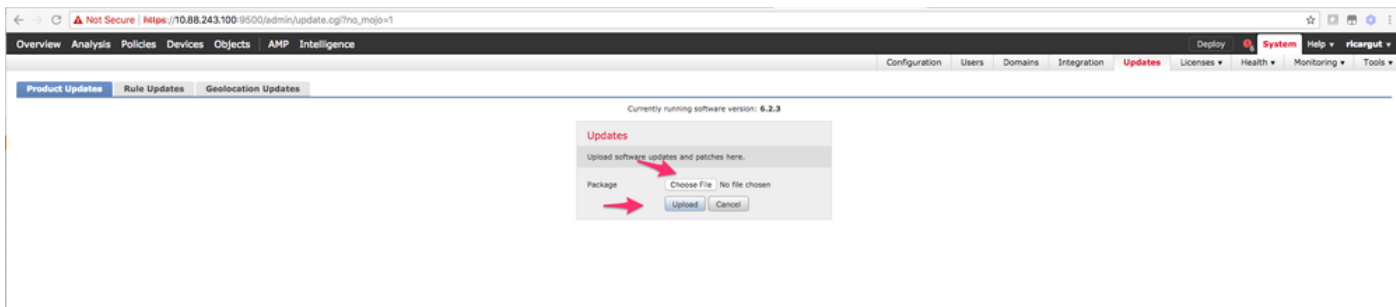
Step 2. Upload the upgrade files on the FMC. Navigate to **system>updates** and click **Upload Update**, as shown in the image.



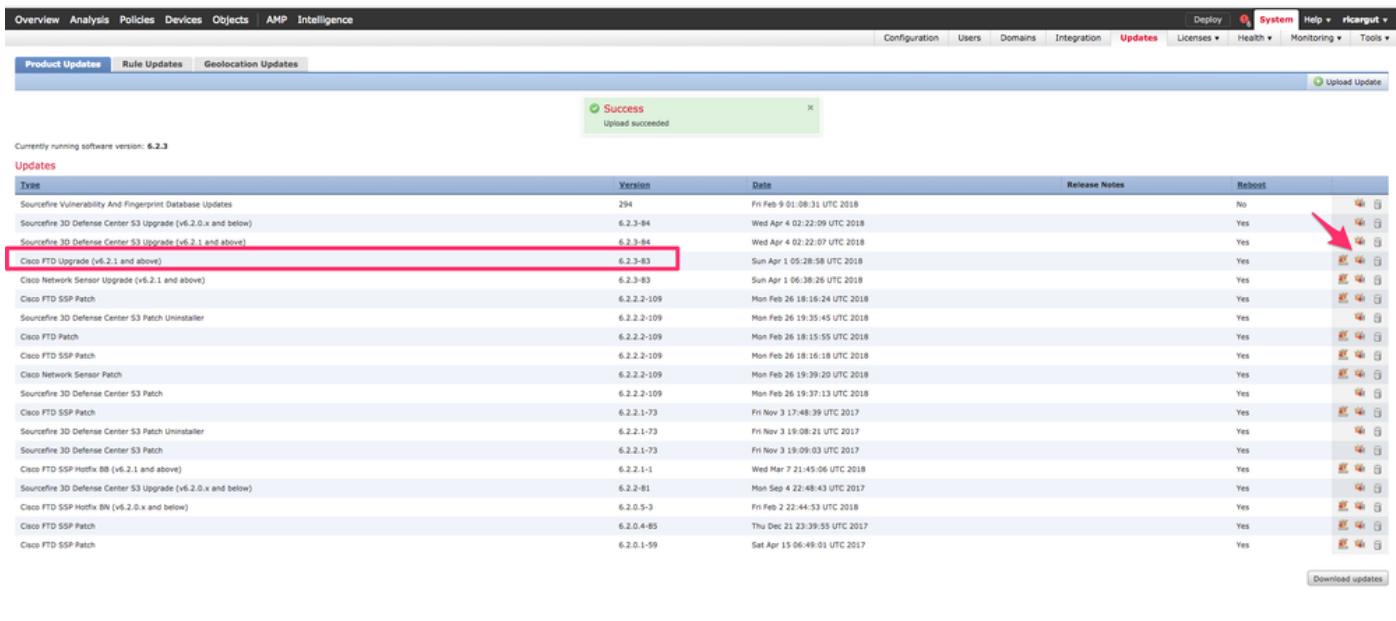
The screenshot shows the Cisco FMC interface with the 'System > updates' page. The 'Upload Update' button is highlighted with a red arrow. The table below lists various updates with their types, versions, dates, release notes, and reboot requirements.

| Type | Version | Date | Release Notes | Reboot | |
|--|-------------|------------------------------|---------------|--------|--|
| Sourcefire Vulnerability And Fingerprint Database Updates | 294 | Fri Feb 9 01:08:31 UTC 2018 | | No | |
| Sourcefire 3D Defense Center S3 Upgrade (v6.2.0.x and below) | 6.2.3-84 | Wed Apr 4 02:22:09 UTC 2018 | | Yes | |
| Sourcefire 3D Defense Center S3 Upgrade (v6.2.1 and above) | 6.2.3-84 | Wed Apr 4 02:22:07 UTC 2018 | | Yes | |
| Cisco Network Sensor Upgrade (v6.2.1 and above) | 6.2.3-83 | Sun Apr 1 06:38:26 UTC 2018 | | Yes | |
| Cisco FTD S5P Patch | 6.2.2-109 | Mon Feb 26 18:16:24 UTC 2018 | | Yes | |
| Sourcefire 3D Defense Center S3 Patch Uninstaller | 6.2.2.2-109 | Mon Feb 26 19:35:45 UTC 2018 | | Yes | |
| Cisco FTD Patch | 6.2.2.2-109 | Mon Feb 26 18:15:55 UTC 2018 | | Yes | |
| Cisco FTD S5P Patch | 6.2.2.2-109 | Mon Feb 26 18:16:18 UTC 2018 | | Yes | |
| Cisco Network Sensor Patch | 6.2.2.2-109 | Mon Feb 26 19:39:20 UTC 2018 | | Yes | |
| Sourcefire 3D Defense Center S3 Patch | 6.2.2.2-109 | Mon Feb 26 19:37:13 UTC 2018 | | Yes | |
| Cisco FTD S5P Patch | 6.2.2.1-73 | Fri Nov 3 17:48:39 UTC 2017 | | Yes | |
| Sourcefire 3D Defense Center S3 Patch Uninstaller | 6.2.2.1-73 | Fri Nov 3 19:08:21 UTC 2017 | | Yes | |
| Sourcefire 3D Defense Center S3 Patch | 6.2.2.1-73 | Fri Nov 3 19:09:03 UTC 2017 | | Yes | |
| Cisco FTD S5P Hostfix 88 (v6.2.1 and above) | 6.2.2.1-1 | Wed Mar 7 21:45:06 UTC 2018 | | Yes | |
| Sourcefire 3D Defense Center S3 Upgrade (v6.2.0.x and below) | 6.2.2-81 | Mon Sep 4 22:48:43 UTC 2017 | | Yes | |
| Cisco FTD S5P Hostfix 88 (v6.2.0.x and below) | 6.2.0.5-3 | Fri Feb 2 22:44:53 UTC 2018 | | Yes | |
| Cisco FTD S5P Patch | 6.2.0.4-85 | Thu Dec 21 23:39:55 UTC 2017 | | Yes | |
| Cisco FTD S5P Patch | 6.2.0.1-59 | Sat Apr 15 06:49:01 UTC 2017 | | Yes | |

Step 3. Choose the file that you want to upload, and then select **Upload**, as shown in the image.

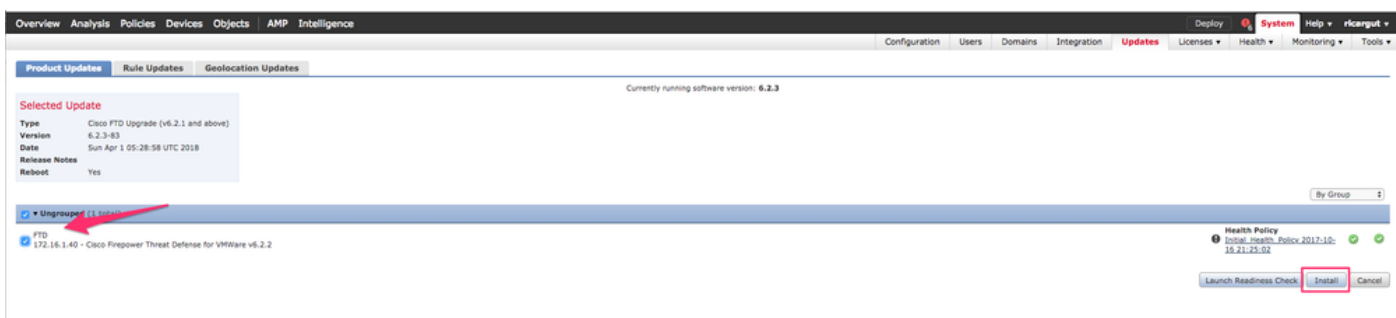


Step 4. Select the install icon, as shown in the image.

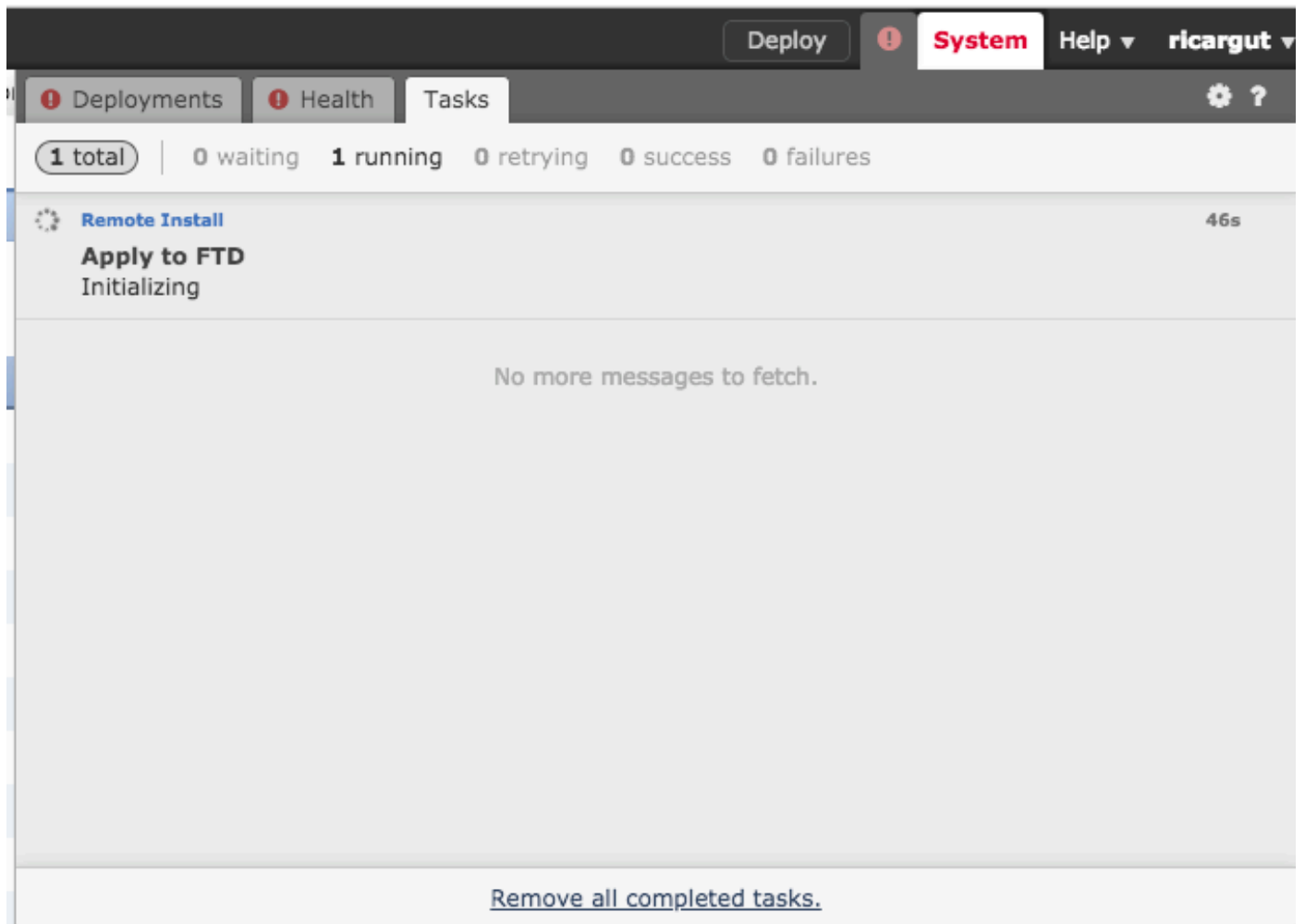


Caution: After the upgrade, the system performs a reboot.

Step 5. Choose the device and select the **Install** button to start the upgrade, as shown in the image.



Step 6. Verify the upgrade process on **Notification Icon > Tasks**, as shown in the image.



Verify

Firepower Management Center Upgrade

Navigate to **Help > About** to verify you have the desired version, as shown in the image.

| | |
|----------------------------|--|
| Model | Cisco Firepower Management Center for VMWare |
| Serial Number | None |
| Software Version | 6.2.3 (build 84) |
| OS | Cisco Fire Linux OS 6.2.3 (build13) |
| Snort Version | 2.9.12 GRE (Build 136) |
| Rule Update Version | 2017-10-26-001-vrt |
| Rulepack Version | 1981 |
| Module Pack Version | 2258 |
| Geolocation Update Version | None |
| VDB Version | build 294 (2018-02-09 01:06:55) |

Firepower Devices Upgrade

Navigate to **Devices > Device Management** and verify you have the desired version, as shown in the image.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Device Management

List of all the devices currently registered on the Firepower Management Center.

View By : All (3) | Error (1) | Warning (0) | Offline (0) | Normal (2) | Deployment Pending (0)

| Name | Model | Versi... | Licenses | Access Control Policy | Group |
|-----------------------------------|---|----------|--|-----------------------|-------|
| Ungrouped (3) | | | | | |
| FP7010 192.168.20.51 | Cisco FirePOWER 7010 | 6.2.2.2 | Protection, Control, Malware, URL Filtering, VPN | Blank | |
| FTDV623 192.168.20.17 - Routed | Cisco Firepower Threat Defense for VMWare | 6.2.3 | Base, Threat, Malware, URL Filtering | Blank | |
| NGIPS 192.168.20.18 | NGIPsv for VMware | 6.2.3 | Protection, Control, Malware, URL Filtering | Blank | |

Troubleshoot

If the upgrade procedure fails, generate the troubleshoot files and open a TAC case. Please refer

to this guide in order to generate the troubleshoot files.

[Cisco Firepower Troubleshoot File Generation Procedures](#)