

Upgrade-Verfahren durch FMC für FirePOWER-Geräte

Inhalt

–

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Vorgehensweise](#)

[Überprüfung](#)

[Upgrade von FirePOWER Management Center](#)

[Upgrade von FirePOWER-Geräten](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird das Verfahren zur Aktualisierung von Geräten mit Firepower Services, Adaptive Security Appliance (ASA), FTD und FMC beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit den folgenden Produkten vertraut sind:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- FirePOWER (SFR)-Servicemodul wird auf ASA ausgeführt

Sie müssen außerdem die Software für Firepower-Geräte von folgender Website herunterladen:

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

Verwendete Komponenten

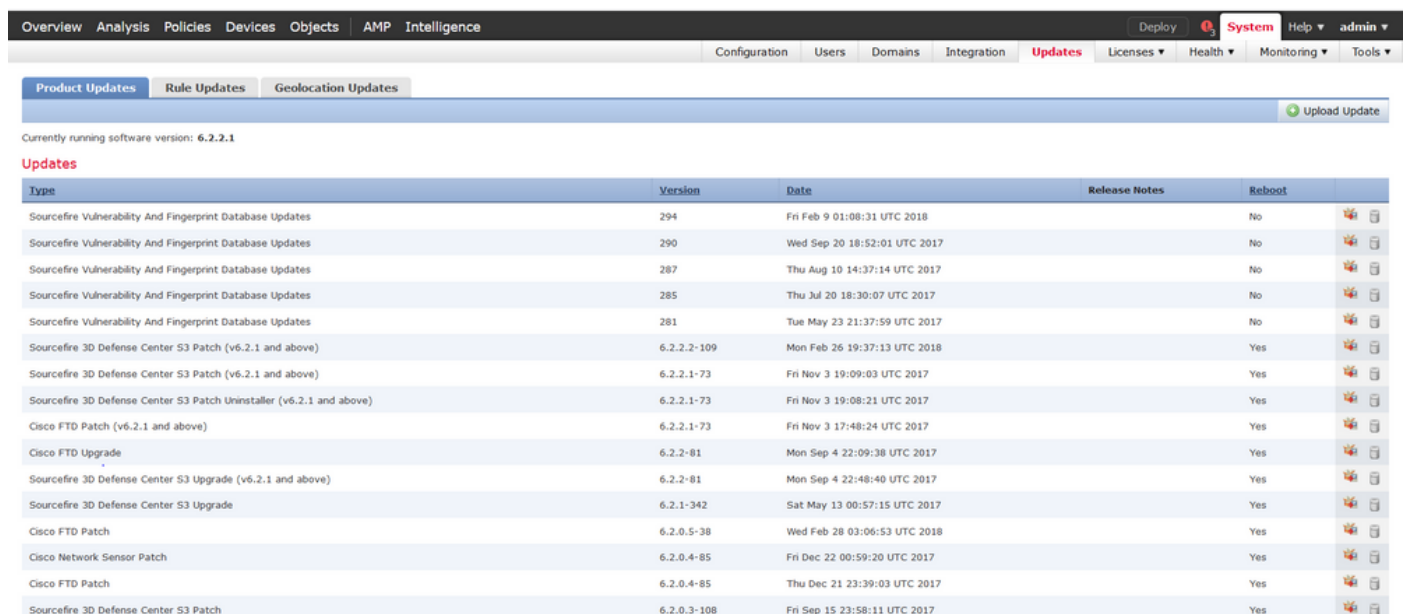
Die Informationen in diesem Dokument basieren auf den folgenden Produkten und Softwareversionen:

- FirePOWER Management Center
- FirePOWER-Servicemodul wird auf ASA ausgeführt

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Vorgehensweise

Schritt 1: Navigieren Sie zu **System > updates**, und suchen Sie nach der Version, auf die Sie aktualisieren möchten, wie im Abbild dargestellt.



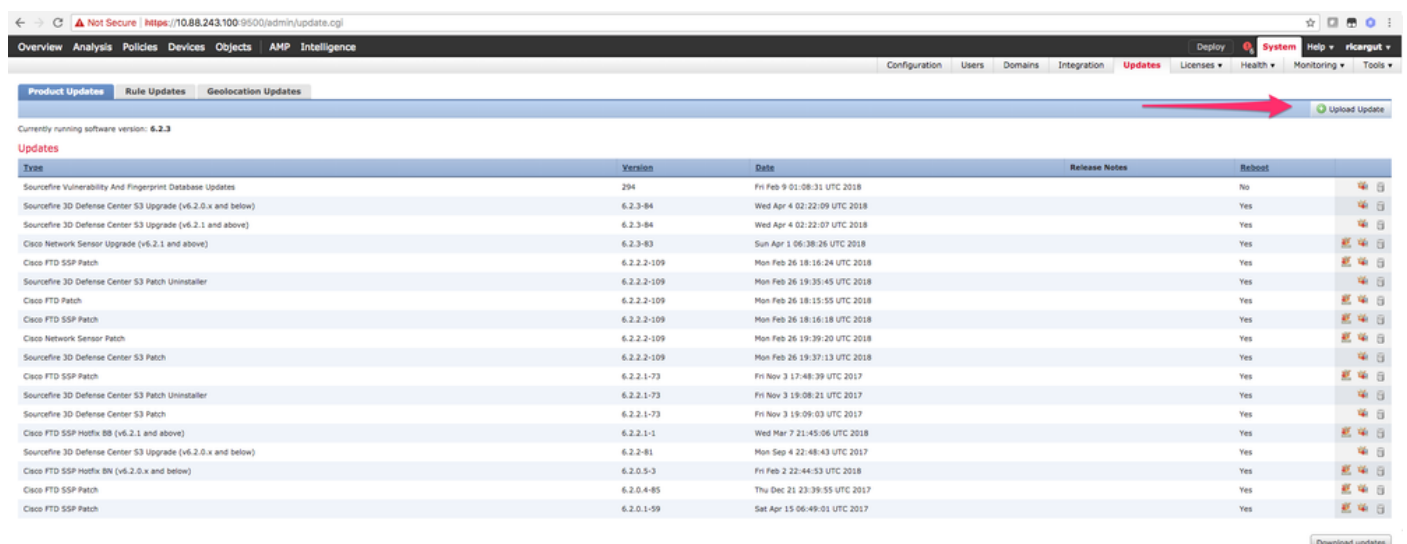
The screenshot shows the FMC interface with the 'System' menu open and 'updates' selected. The 'Product Updates' tab is active. The current software version is 6.2.2.1. A table of updates is displayed with columns for Type, Version, Date, Release Notes, and Reboot. The table lists various updates including Sourcefire Vulnerability And Fingerprint Database Updates, Sourcefire 3D Defense Center S3 Patch, and Cisco FTD Patch.

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

Wenn die Version, die Sie aktualisieren möchten, nicht auf dem Bildschirm angezeigt wird, fahren Sie mit Schritt 2 fort.

Wenn die Version, die Sie aktualisieren möchten, auf dem Bildschirm angezeigt wird, fahren Sie mit Schritt 4 fort.

Schritt 2: Hochladen der Upgrade-Dateien auf das FMC Navigieren Sie zu **system>updates**, und klicken Sie auf **Upload Update (Aktualisierung hochladen)**, wie im Bild dargestellt.

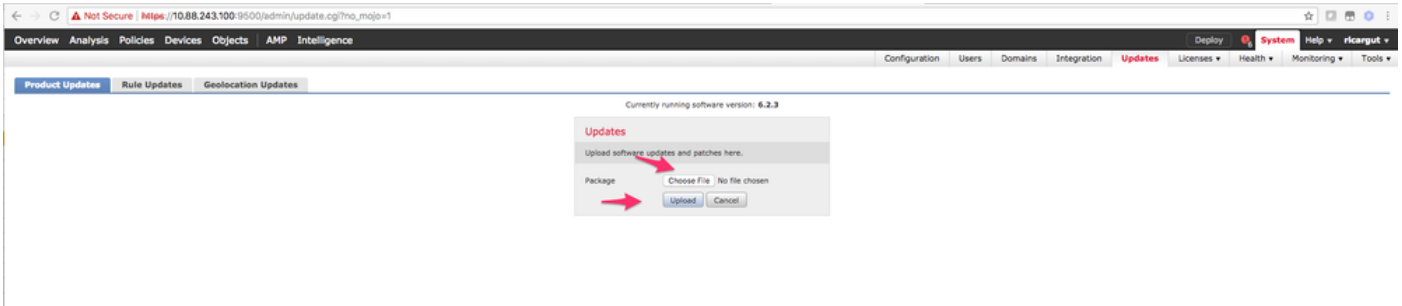


The screenshot shows the FMC interface with the 'System' menu open and 'updates' selected. The 'Product Updates' tab is active. The current software version is 6.2.3. A red arrow points to the 'Upload Update' button in the top right corner of the updates section.

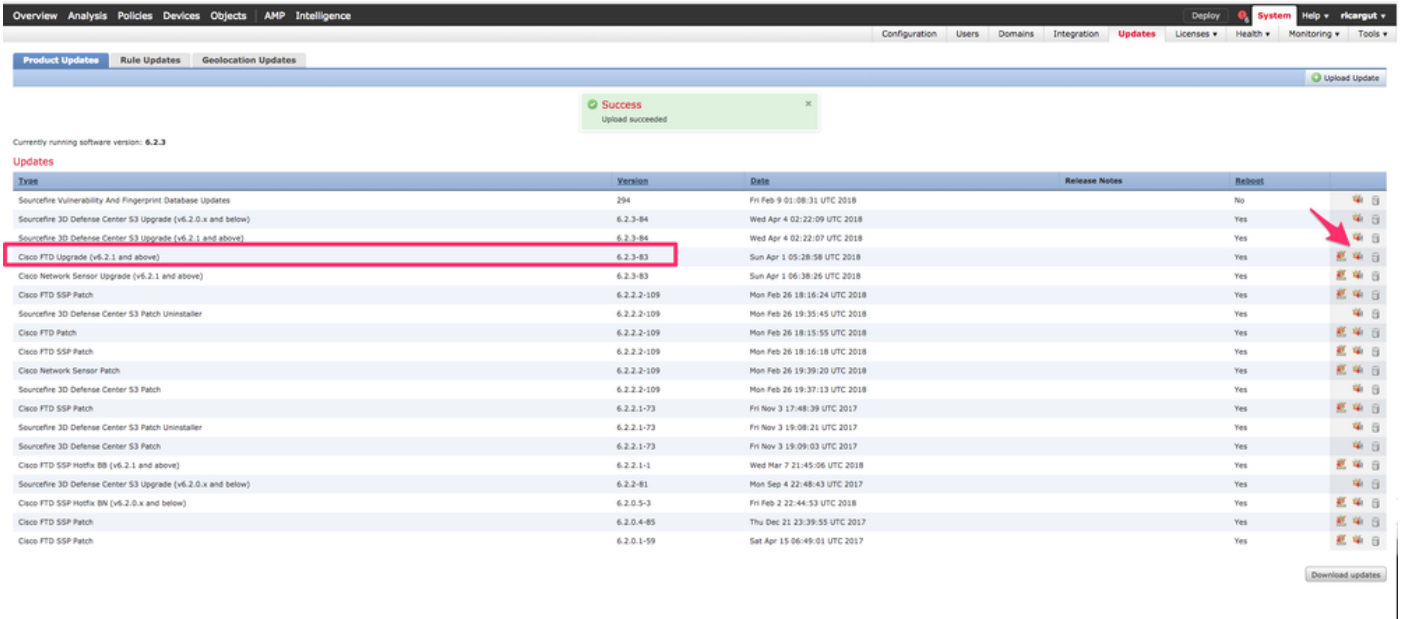
Type	Version	Date	Release Notes	Reboot
Sourcefire Vulnerability And Fingerprint Database Updates	294	Fri Feb 9 01:08:31 UTC 2018		No
Sourcefire 3D Defense Center S3 Upgrade (v6.2.0.x and below)	6.2.3-84	Wed Apr 4 02:22:09 UTC 2018		Yes
Sourcefire 3D Defense Center S3 Upgrade (v6.2.1 and above)	6.2.3-84	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 SSP Patch	6.2.2-109	Mon Feb 26 18:16:24 UTC 2018		Yes
Sourcefire 3D Defense Center S3 Patch Uninstaller	6.2.2-109	Mon Feb 26 19:35:45 UTC 2018		Yes
Cisco FTD Patch	6.2.2-109	Mon Feb 26 18:15:55 UTC 2018		Yes
Cisco FTD SSP Patch	6.2.2-109	Mon Feb 26 18:16:18 UTC 2018		Yes
Cisco Network Sensor Patch	6.2.2-109	Mon Feb 26 19:39:20 UTC 2018		Yes
Sourcefire 3D Defense Center S3 Patch	6.2.2-109	Mon Feb 26 19:37:13 UTC 2018		Yes
Cisco FTD SSP 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 SSP Hotfix B8 (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 SSP Hotfix B1 (v6.2.0.x and below)	6.2.0.5-3	Fri Feb 2 22:44:53 UTC 2018		Yes
Cisco FTD SSP Patch	6.2.0.4-85	Thu Dec 21 23:39:55 UTC 2017		Yes
Cisco FTD SSP Patch	6.2.0.1-59	Sat Apr 15 06:49:01 UTC 2017		Yes

Schritt 3: Wählen Sie die Datei aus, die Sie hochladen möchten, und wählen Sie dann **Hochladen**,

wie im Bild gezeigt.

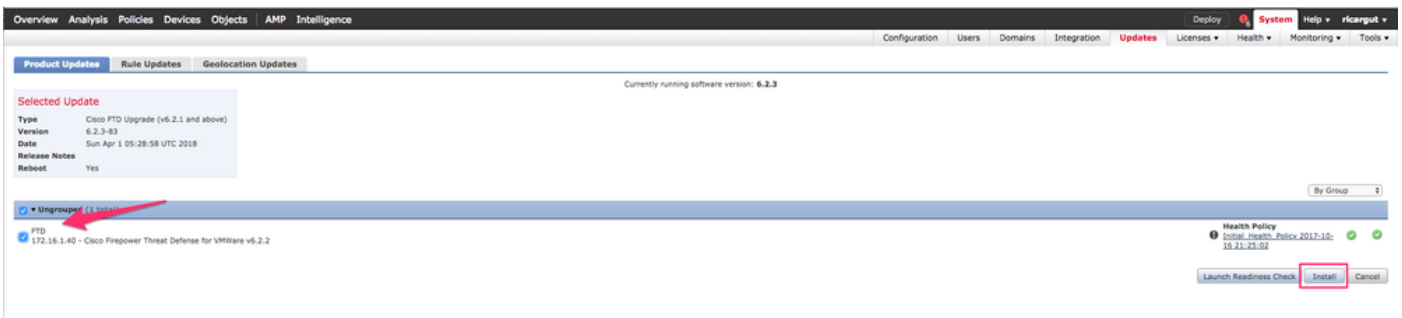


Schritt 4: Wählen Sie das Installationssymbol aus, wie im Bild gezeigt.

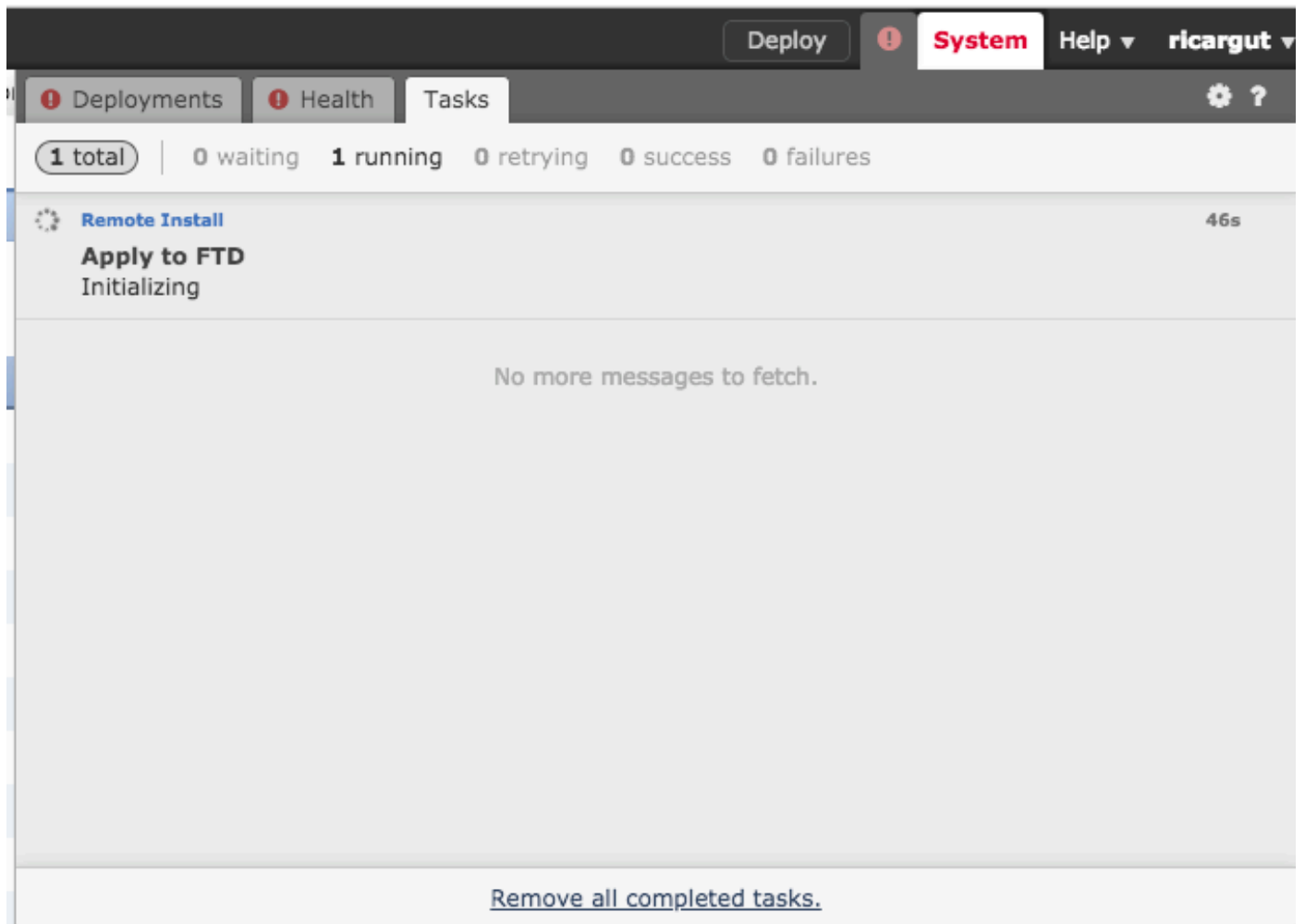


Vorsicht: Nach dem Upgrade führt das System einen Neustart durch.

Schritt 5: Wählen Sie das Gerät aus, und wählen Sie die Schaltfläche **Install** (Installieren) aus, um das Upgrade zu starten, wie im Image gezeigt.



Schritt 6: Überprüfen Sie den Aktualisierungsvorgang unter **Benachrichtigungssymbol > Aufgaben**, wie im Bild dargestellt.



Überprüfung

Upgrade von FirePOWER Management Center

Navigieren Sie zu **Hilfe > Info**, um zu überprüfen, ob Sie die gewünschte Version installiert haben, wie in der Abbildung dargestellt.

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)

Upgrade von FirePOWER-Geräten

Navigieren Sie zu **Devices > Device Management** (Geräte > Geräteverwaltung), und stellen Sie sicher, dass Sie die gewünschte Version installiert haben, wie im Bild gezeigt.










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	  

Fehlerbehebung

Wenn das Upgrade fehlschlägt, generieren Sie die Dateien zur Fehlerbehebung, und öffnen Sie

ein TAC-Ticket. Informationen zum Generieren der Fehlerbehebungsdateien finden Sie in diesem Handbuch.

[Cisco FirePOWER-Fehlerbehebung bei Dateigenerierungsverfahren](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.