

# Procedura di aggiornamento tramite FMC per dispositivi Firepower

## Sommario

–

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Procedura](#)

[Verifica](#)

[Aggiornamento di Firepower Management Center](#)

[Aggiornamento dispositivi Firepower](#)

[Risoluzione dei problemi](#)

## Introduzione

Questo documento descrive la procedura per aggiornare i dispositivi con Firepower Services, Adaptive Security Appliance (ASA), FTD e FMC.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti prodotti:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)
- Modulo di servizio FirePOWER (SFR) in esecuzione su ASA

È inoltre necessario scaricare il software per i dispositivi firepower da:

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

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e prodotti:

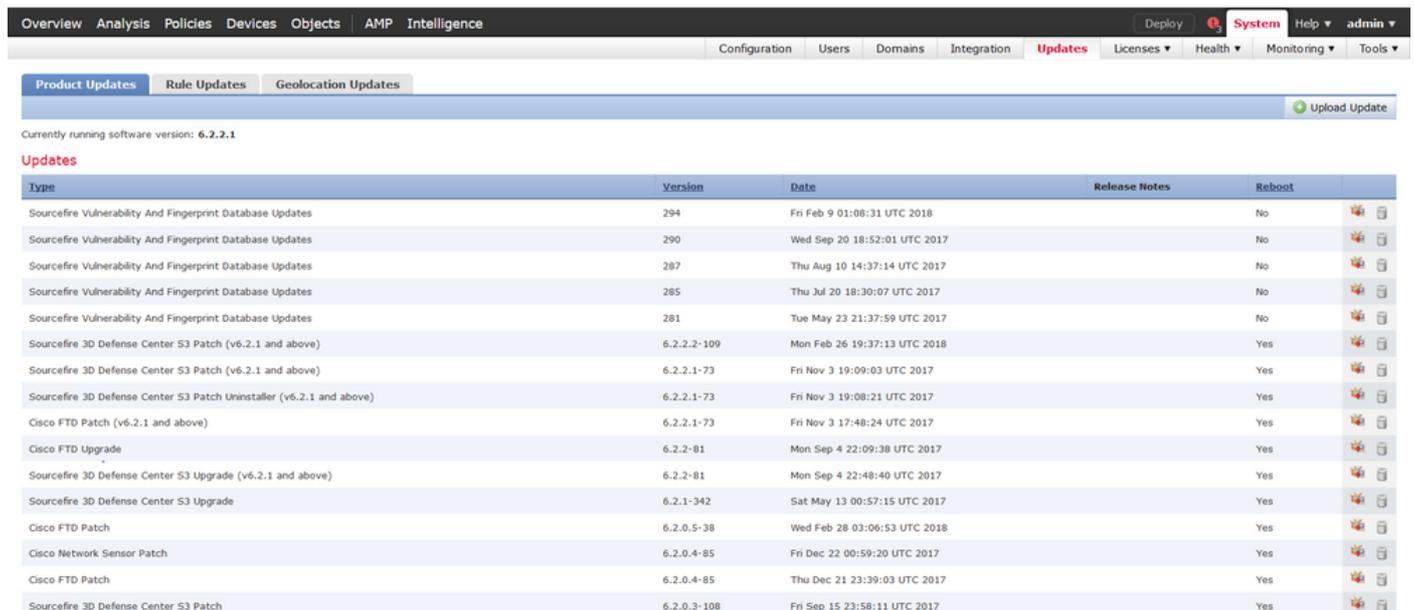
- Firepower Management Center
- Modulo di servizio FirePOWER in esecuzione su ASA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Procedura

Passaggio 1. Passare a **Sistema > Aggiornamenti** e cercare la versione a cui si desidera eseguire l'aggiornamento, come mostrato nell'immagine.



Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates

Currently running software version: 6.2.2.1

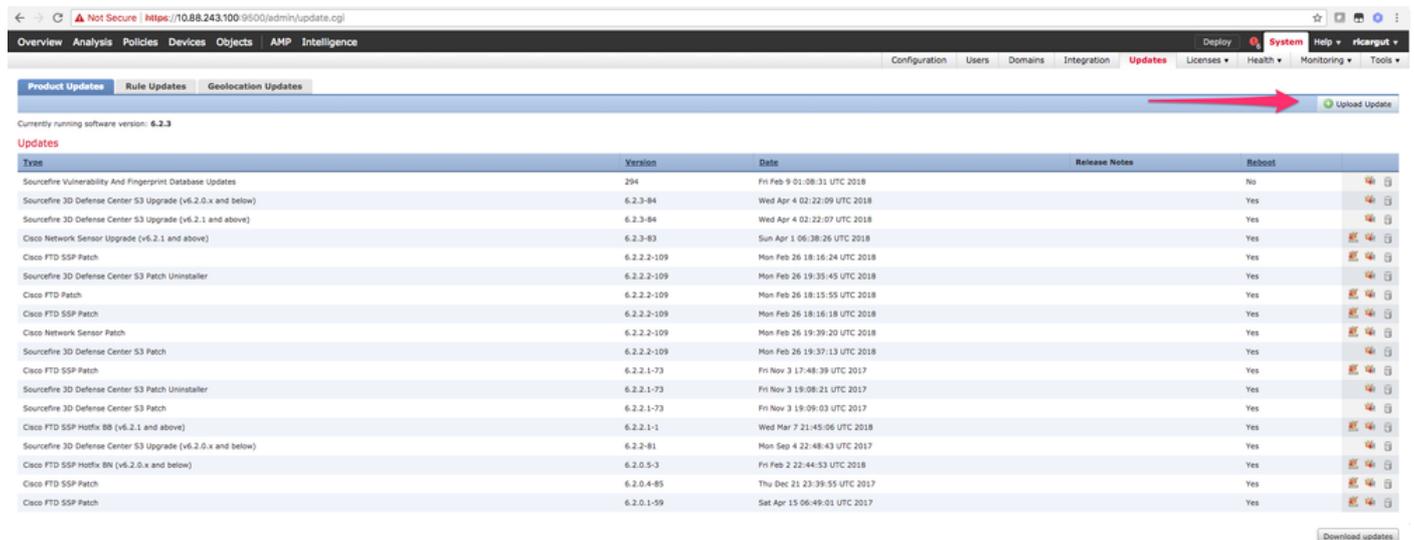
Updates

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	

Se la versione che si desidera aggiornare non è visualizzata, continuare con il passaggio 2.

Se sullo schermo viene visualizzata la versione che si desidera aggiornare, continuare con il passaggio 4.

Passaggio 2. Caricare i file di aggiornamento nel FMC. Passare a **system>updates** (sistema) e fare clic su **Upload Update** (Carica aggiornamento), come mostrato nell'immagine.



← Not Secure https://10.88.243.100:9500/admin/update.cgi

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help ricarguit

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates

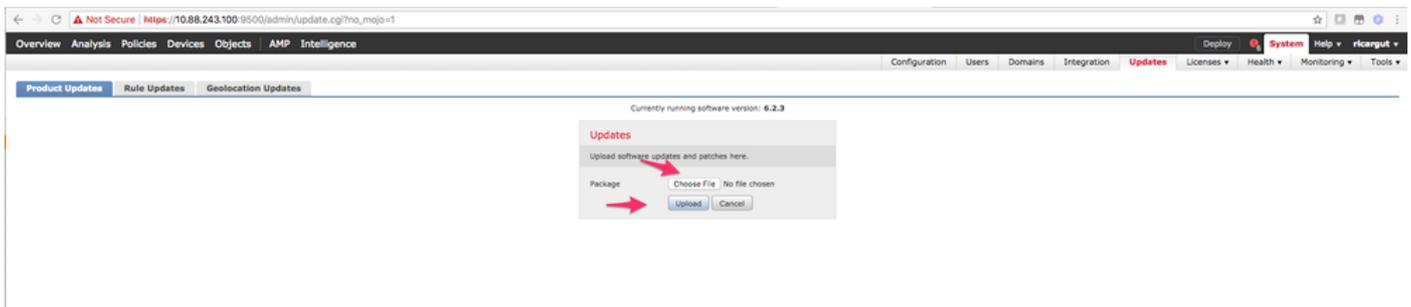
Currently running software version: 6.2.3

Updates

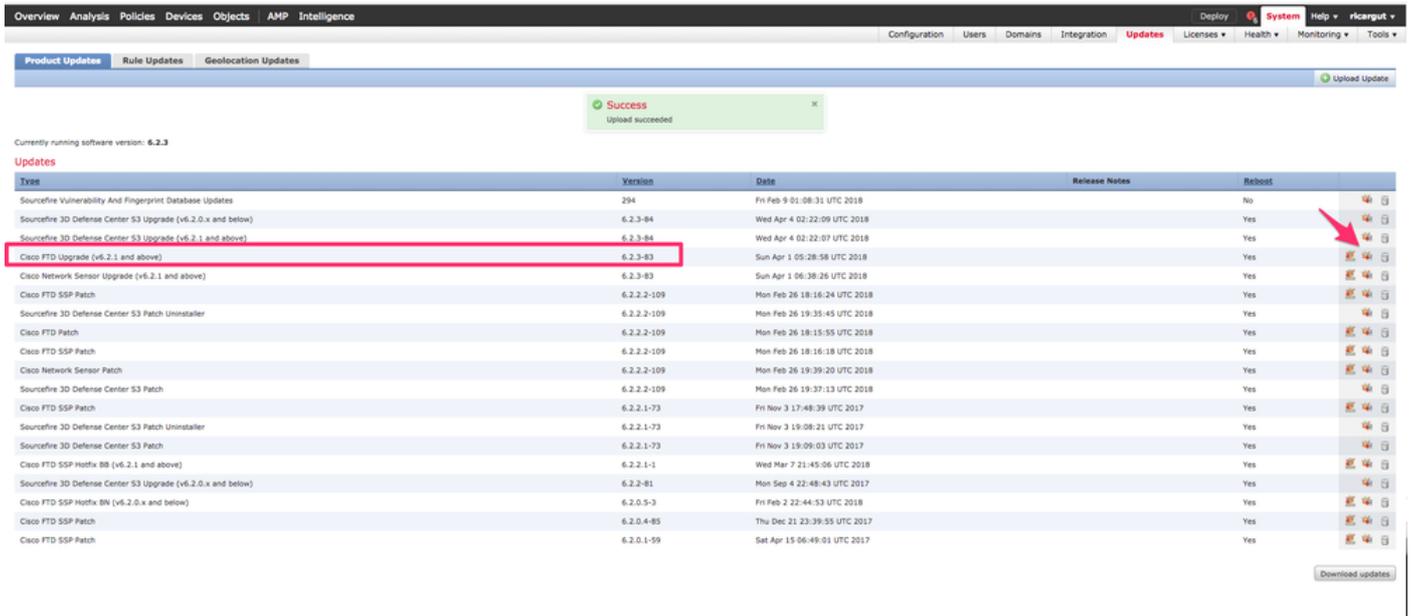
Type	Version	Date	Release Notes	Reboot	
Sourcefire Vulnerability And Fingerprint Database Updates	294	Fri Feb 9 01:08:31 UTC 2018		No	
Sourcefire 3D Defense Center S3 Upgrade (v6.2.0.x and below)	6.2.3-84	Wed Apr 4 02:22:09 UTC 2018		Yes	
Sourcefire 3D Defense Center S3 Upgrade (v6.2.1 and above)	6.2.3-84	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 B9 (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	

Download updates

Passaggio 3. Scegliere il file che si desidera caricare e quindi selezionare **Upload**, come mostrato nell'immagine.

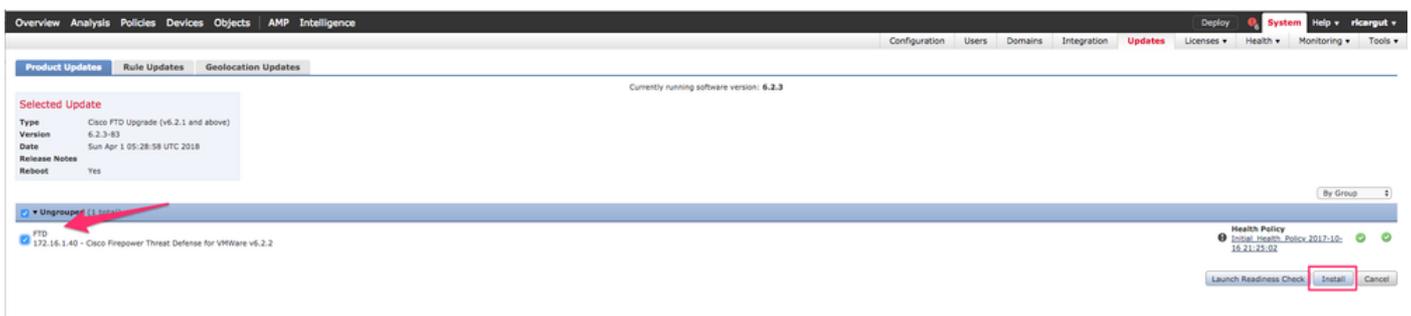


Passaggio 4. Selezionare l'icona di installazione, come illustrato nell'immagine.

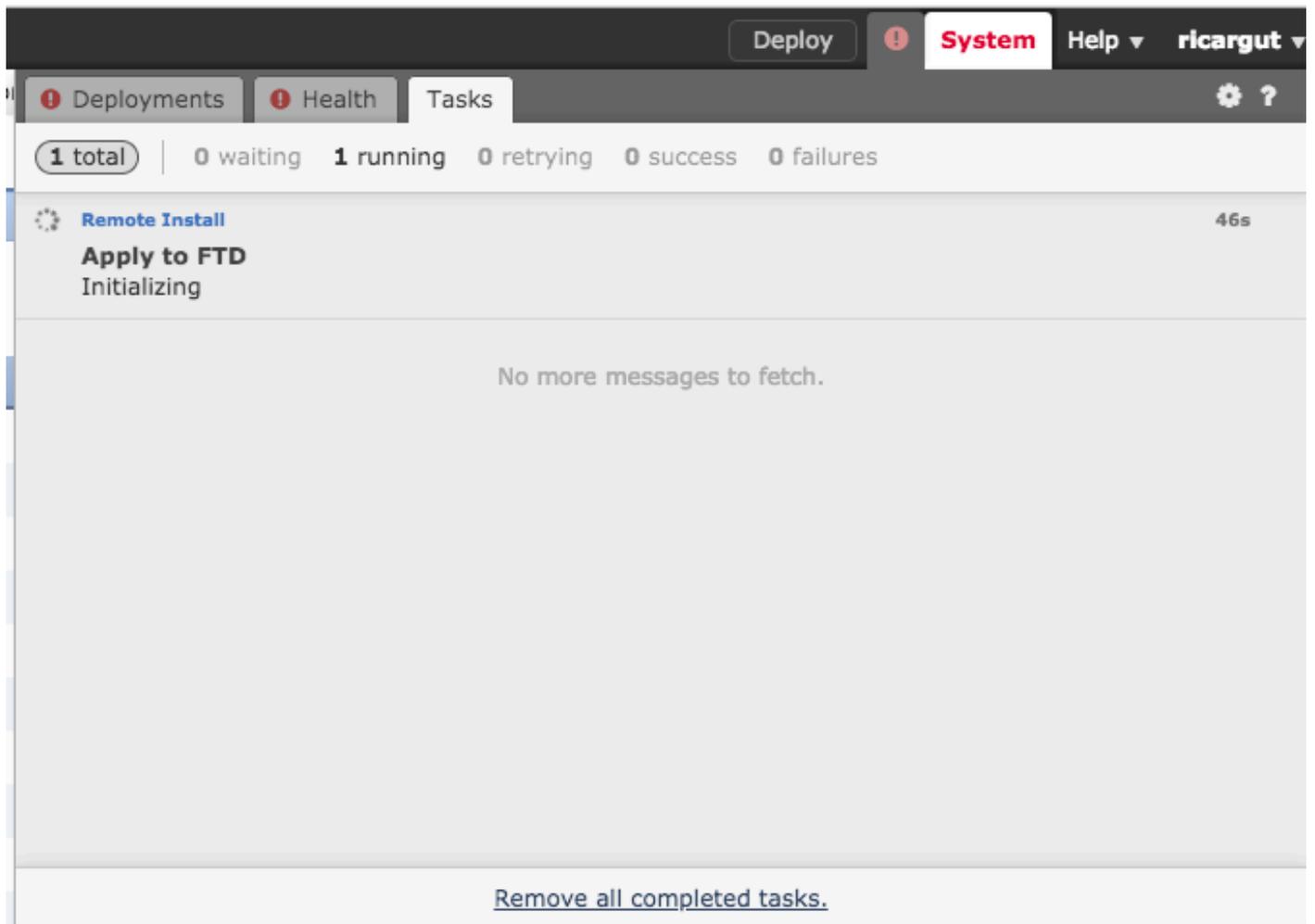


**Attenzione:** dopo l'aggiornamento, il sistema esegue un riavvio.

Passaggio 5. Scegliere il dispositivo e selezionare il pulsante **Installa** per avviare l'aggiornamento, come mostrato nell'immagine.



Passaggio 6. Verificare il processo di aggiornamento selezionando **Icona di notifica > Attività**, come mostrato nell'immagine.



## Verifica

### Aggiornamento di Firepower Management Center

Selezionare **Help > About** (Informazioni su) per verificare di disporre della versione desiderata, come mostrato nell'immagine.

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 )

## Aggiornamento dispositivi Firepower

Passare a **Dispositivi > Gestione dispositivi** e verificare di disporre della versione desiderata, come mostrato nell'immagine.

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)					
<b>FP7010</b> 192.168.20.51	Cisco FirePOWER 7010	6.2.2.2	Protection, Control, Malware, URL Filtering, VPN	Blank	
<b>FTDV623</b> 192.168.20.17 - Routed	Cisco Firepower Threat Defense for VMWare	6.2.3	Base, Threat, Malware, URL Filtering	Blank	
<b>NGIPS</b> 192.168.20.18	NGIPSV for VMWare	6.2.3	Protection, Control, Malware, URL Filtering	Blank	

## Risoluzione dei problemi

Se la procedura di aggiornamento non riesce, generare i file di risoluzione dei problemi e aprire

una richiesta TAC. Consultare questa guida per generare i file di risoluzione dei problemi.

[Cisco Firepower: risoluzione dei problemi relativi alle procedure di generazione dei file](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).