# Configurare l'aggiornamento automatico dei bundle CA per FMC e FDM

## Sommario



## Introduzione

Questo documento descrive l'utilizzo dell'aggiornamento automatico dei bundle Cisco CA per Secure Firewall Management Center e Secure Firewall Device Manager.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Cisco Secure Firewall Management Center (in precedenza Firepower Management Center) e Secure Firewall Device Manager (in precedenza Firepower Device Manager).
- conoscenza di Secure Firewall Appliance (in precedenza Firepower).

### Componenti usati

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

- Cisco Secure Firewall Management Center (FMC 1000, 1600, 2500, 2600, 4500, 4600 e virtuale) con software versione 7.0.5 e successive.
- Cisco Secure Firewall Management Center (FMC 1600, 2600, 4600 e versioni virtuali) con software versione 7.1.0-3 e successive.
- Cisco Secure Firewall Management Center (FMC 1600, 2600, 4600 e virtuale) con software versione 7.2.4 e successive.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 e virtuale) con software versione 7.0.5 e successive, gestito da Secure Firewall Device Manager.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 e virtuale) con software versione 7.1.0-3 e successive, gestito da Secure Firewall Device Manager.

- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000 e virtuale) con software versione 7.2.4 e successive, gestito da Secure Firewall Device Manager.

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.

# Premesse

## Utilizzi per bundle Cisco CA

I dispositivi Cisco Secure Firewall (in precedenza Firepower) utilizzano bundle CA locali contenenti certificati per accedere a diversi servizi Cisco (licenze Smart, software, VDB, SRU e aggiornamenti di geolocalizzazione). A questo punto, il sistema richiede automaticamente a Cisco nuovi certificati CA a un'ora definita dal sistema. In precedenza, era necessario aggiornare il software per aggiornare i certificati CA.

---

**Nota**: questa funzione non è supportata nelle versioni da 7.0.0 a 7.0.4, da 7.1.0 a 7.1.0-2 o da 7.2.0 a 7.2.3. Se si esegue l'aggiornamento da una versione supportata a una versione non supportata, la funzione viene temporaneamente disabilitata e il sistema non contatta più Cisco.

---

# Configurazione dell'aggiornamento automatico per i bundle CA in SFMC e SFDM

## Abilita aggiornamento automatico per bundle CA

Per abilitare l'aggiornamento automatico per i bundle CA in Centro gestione firewall protetto e Gestione dispositivi firewall protetto:

1. Accedere a SFMC o SFDM su CLI utilizzando SSH o Console.
2. Eseguire il comando configure cert-update auto-update enable sulla CLI:

<#root>

```
> configure cert-update auto-update enable

Autoupdate is enabled and set for every day at 18:06 UTC
```

3. Per verificare se l'aggiornamento del bundle CA è in grado di eseguire l'aggiornamento automatico, eseguire il comando configure cert-update test:

<#root>

```
> configure cert-update test

Test succeeded, certs can safely be updated or are already up to date.
```

### Esegui l'aggiornamento per i bundle CA manualmente

Per eseguire manualmente l'aggiornamento per i bundle CA in Centro gestione firewall protetto e Gestione dispositivi firewall protetto:

1. Accedere a SFMC o SFDM su CLI utilizzando SSH o Console.
2. Eseguire il comando configure cert-update run-now sulla CLI:

<#root>

```
> configure cert-update run-now

Certs have been replaced or was already up to date.
```

## Verifica

### Convalida aggiornamento automatico per bundle CA

Per convalidare la configurazione per l'aggiornamento automatico per i bundle CA in Centro gestione firewall protetto e Gestione dispositivi firewall protetto:

1. Accedere a SFMC o SFDM su CLI utilizzando SSH o Console.
2. Eseguire il comando show cert-update dalla CLI:

<#root>

```
> show cert-update

Autoupdate is enabled and set for every day at 18:06 UTC
CA bundle was last modified 'Wed Jul 19 03:11:31 2023'
```

# Risoluzione dei problemi

## Errore di aggiornamento

## Fasi consigliate:

1. Convalidare la configurazione DNS corrente.
2. Convalidare la configurazione di Internet e del proxy per l'interfaccia di gestione.
3. Confermare la presenza di connettività con tools.cisco.com utilizzando ICMP e curl con il comando in modalità Expert:
   ```
   sudo curl -vvk  https://tools.cisco.com
   ```

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).