FMC 6.6.1+ - Suggerimenti per prima e dopo un aggiornamento

Sommario

Introduzione

In questo documento vengono descritte le best practice di verifica e configurazione da completare

prima e dopo l'aggiornamento di Cisco Secure Firewall Management Center (FMC) alla versione 6.6.1+.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Hardware: Cisco FMC 1000
- Software: Release 7.0.0 (build 94)

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.

Operazioni principali prima dell'aggiornamento di FMC

Scegliere la versione del software di destinazione FMC

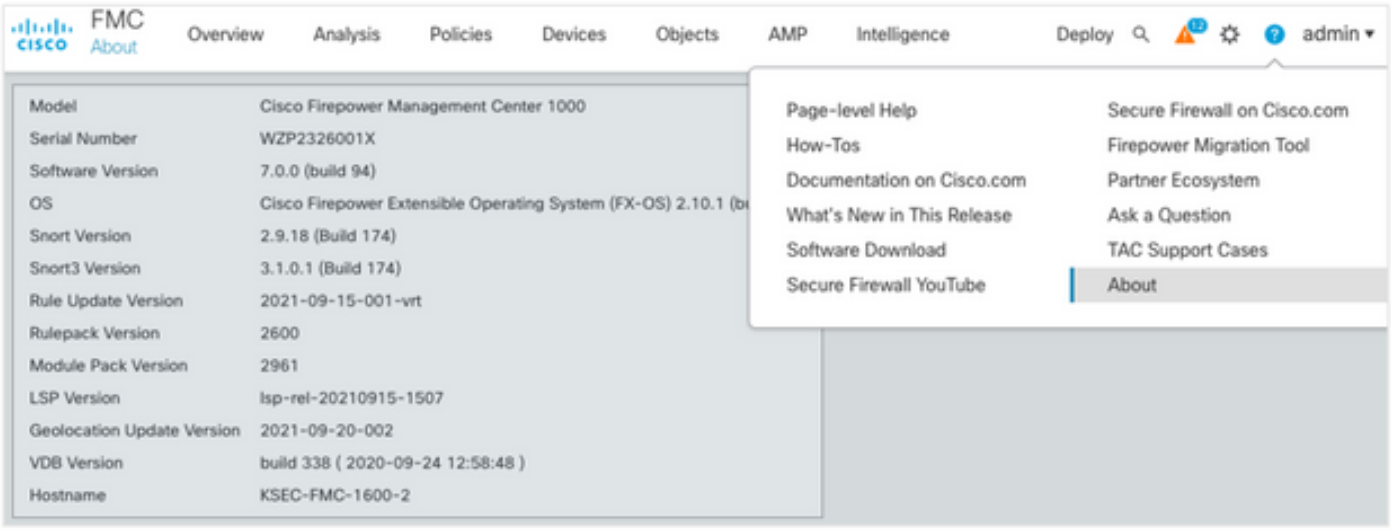
Consultare le note di rilascio di Firepower per la versione di destinazione e acquisire familiarità con:

- Compatibilità
- Caratteristiche e funzionalità
- Problemi risolti
- Problemi noti

Verifica del modello e della versione del software FMC correnti

Verificare il modello FMC e la versione software correnti:

1. Selezionare **? > Informazioni su**.
2. Verificare il **modello** e la **versione del software**.



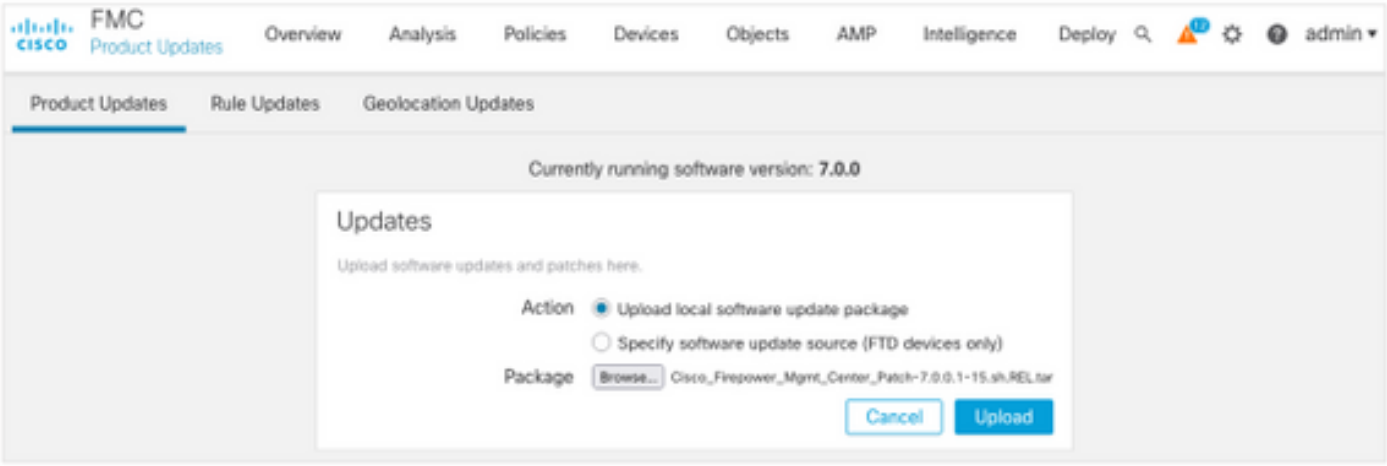
Pianificazione del percorso di aggiornamento

In base alla versione corrente e alla versione di destinazione del software FMC, potrebbe essere necessario un aggiornamento temporaneo. Nella Guida all'aggiornamento di Cisco Firepower Management Center, esaminare il **percorso di aggiornamento: Firepower Management Center** e pianificare il percorso di aggiornamento.

Carica pacchetti di aggiornamento

Per caricare il pacchetto di aggiornamento sul dispositivo, attenersi alla seguente procedura:

1. Scaricare il pacchetto di aggiornamento dalla pagina Download del software.
2. Nel FMC selezionare **Sistema > Aggiornamenti**.
3. Scegliere **Upload Update**.
4. Fare clic sul pulsante di opzione **Carica pacchetto di aggiornamento software locale**.
5. Fare clic su **Sfoglia** e scegliere il pacchetto.
6. Fare clic su **Upload**.



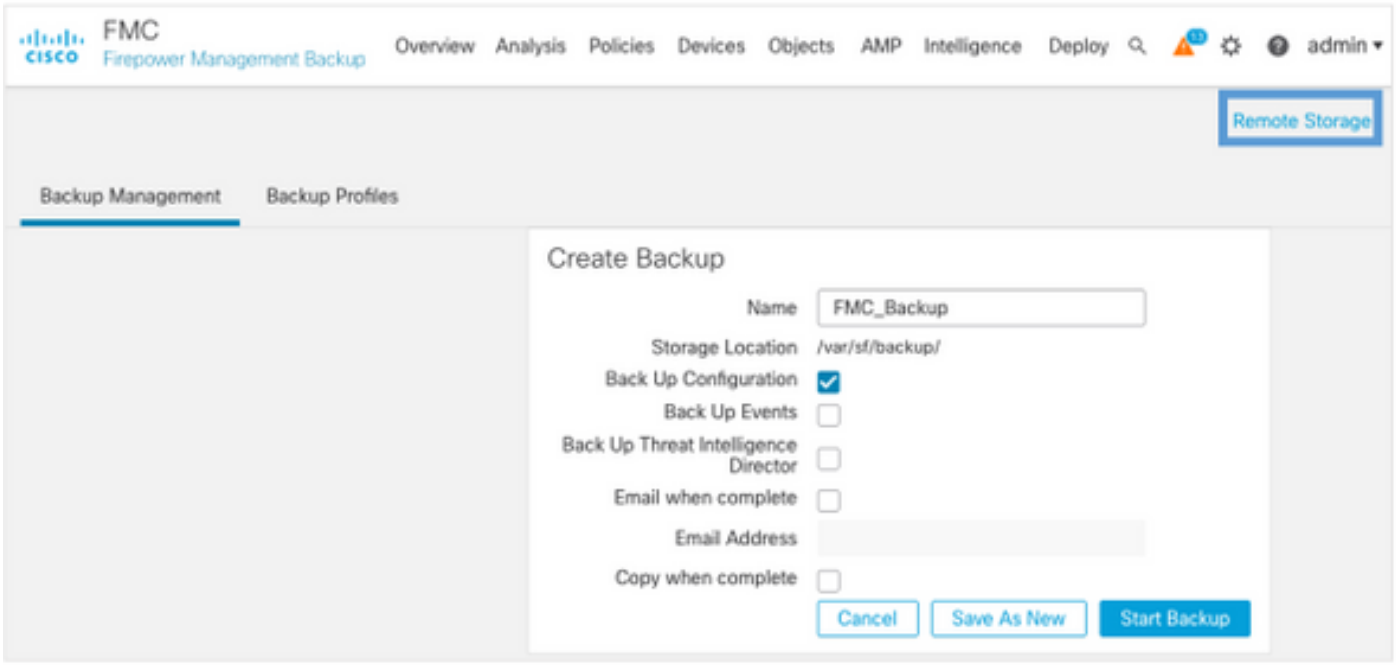
Crea backup FMC

Il backup è un'importante fase di disaster recovery, che consente di ripristinare la configurazione in caso di errore irreversibile di un aggiornamento.

1. Selezionare **Sistema > Strumenti > Backup/Ripristino**.

2. Scegliere il **backup di Firepower Management**.
3. Nel campo **Nome**, immettere il nome del backup.
4. Scegliere il percorso di archiviazione e le informazioni da includere nel backup.
5. Fare clic su **Avvia backup**.
6. Da **Notifica > Attività**, monitorare lo stato di creazione del backup.

Suggerimento: È consigliabile eseguire il backup in una posizione remota sicura e verificare che il trasferimento sia riuscito. È possibile configurare Archiviazione remota dalla pagina Gestione backup.



Per ulteriori informazioni, vedere:

- Guida alla configurazione di Firepower Management Center, versione 7.0 - Capitolo: Backup e ripristino
- Guida alla configurazione di Firepower Management Center, versione 7.0 - Gestione remota dello storage

Verifica sincronizzazione NTP

Per un aggiornamento corretto di FMC, è necessaria la sincronizzazione NTP. Per controllare la sincronizzazione NTP, attenersi alla seguente procedura:

1. Selezionare **Sistema > Configurazione > Tempo**.
2. Verificare lo **stato NTP**.

Nota: Stato: "In uso" indica che l'accessorio è sincronizzato con il server NTP.

Current Setting Via NTP (based on System Configuration Time Synchronization)
Current Time 2021-09-21 13:50

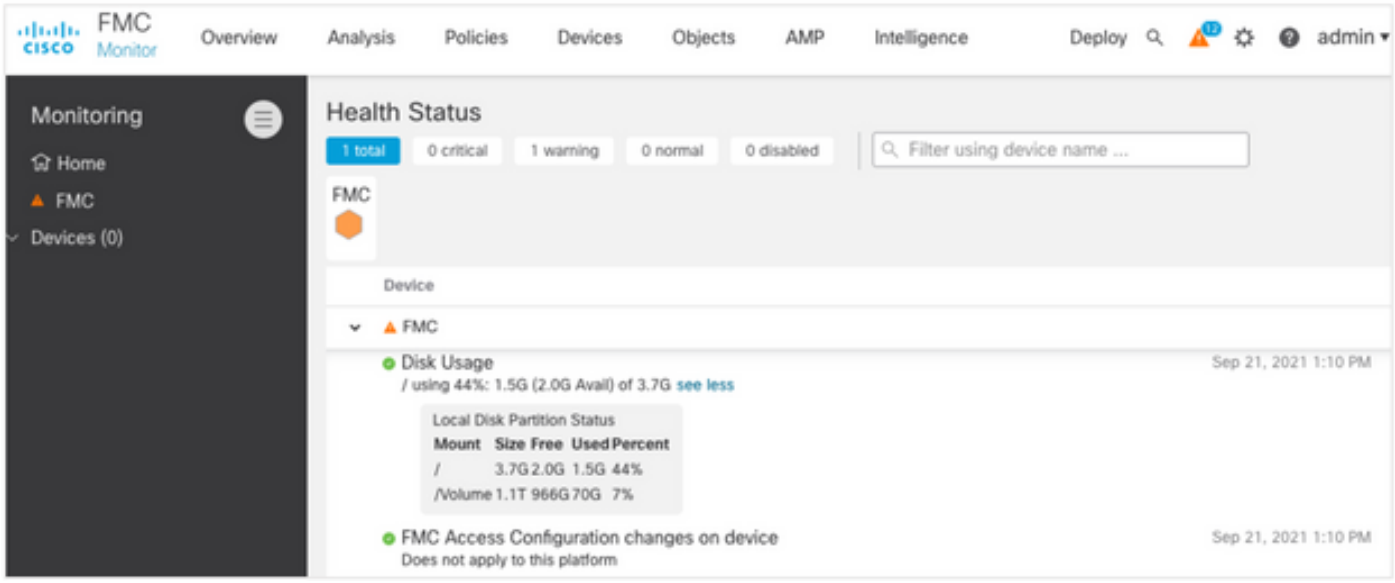
NTP Server	Status	Authentication	Offset	Last Update
173.38.201.115	Being Used	none	+0.011(milliseconds)	126(seconds)
173.38.201.67	Available	none	+0.042(milliseconds)	223(seconds)
127.127.1.1	Unknown	none	+0.000(milliseconds)	12d(seconds)

Per ulteriori informazioni, vedere Firepower Management Center Configuration Guide, Version 7.0 - Time and Time Synchronization.

Verifica dello spazio su disco

A seconda del modello e della versione di destinazione del CCP, assicurarsi che lo spazio disponibile su disco sia sufficiente, altrimenti l'aggiornamento non riesce. Per verificare lo spazio disponibile su disco del CCP, eseguire la procedura seguente:

1. Passare a **Sistema > Stato > Monitor**.
2. Scegliere il CCP.
3. Espandere il menu e cercare **Utilizzo disco**.
4. I requisiti di spazio su disco sono disponibili in Test di tempo e Requisiti di spazio su disco.

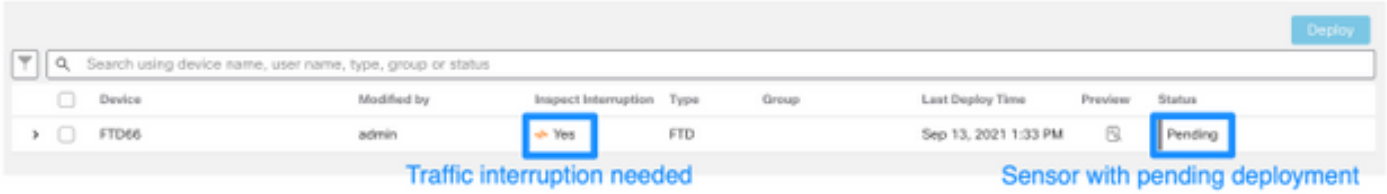


Distribuisci tutte le modifiche dei criteri in sospeso

Prima dell'installazione dell'aggiornamento o della patch, è necessario distribuire le modifiche nei sensori. Per garantire la distribuzione di tutte le modifiche in sospeso, eseguire la procedura seguente:

1. Passare a **Distribuisci > Distribuzione**.
2. Selezionare tutti i dispositivi nell'elenco e **Distribuisci**.

Attenzione: La colonna Ispect Interruption indica l'interruzione del traffico

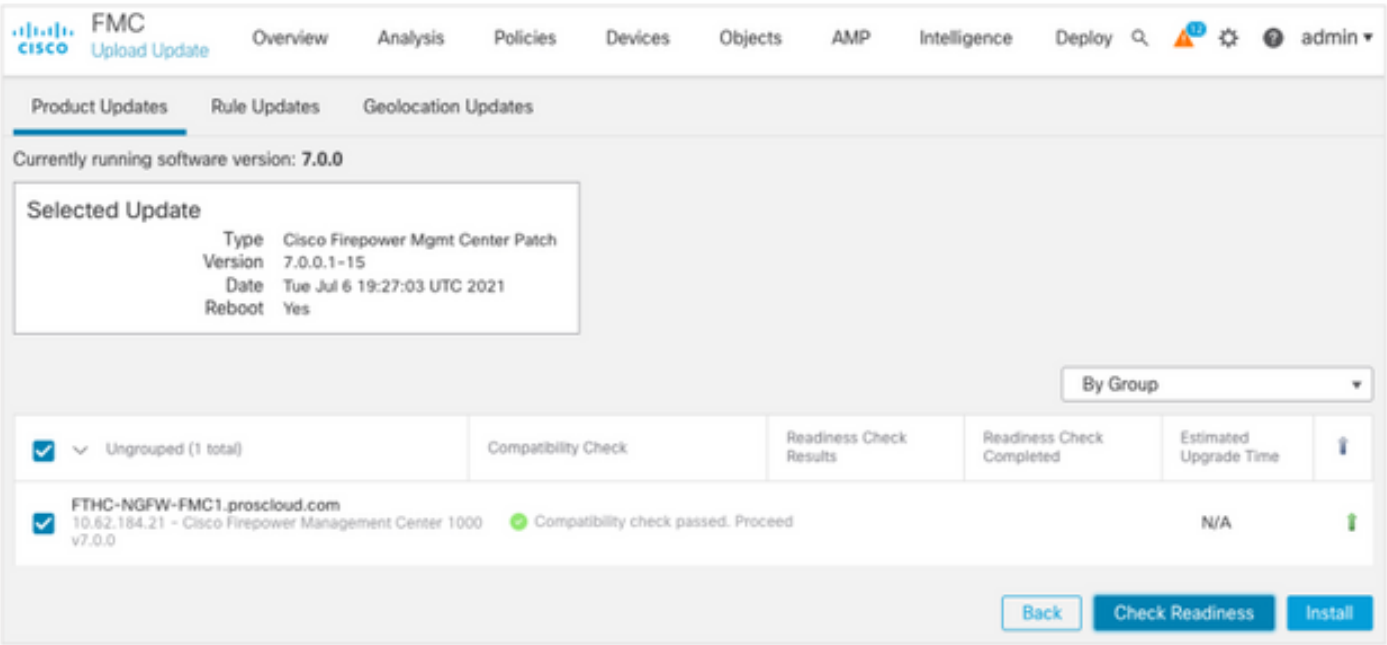


Esegui controlli di fattibilità del software Firepower

I controlli di fattibilità valutano il grado di preparazione di un'appliance Firepower all'aggiornamento del software.

Per eseguire i controlli di idoneità del software, attenersi alla seguente procedura:

1. Selezionare **Sistema > Aggiornamenti**.
2. Selezionare l'icona **Install** (Installa) accanto alla versione di destinazione.
3. Scegliere il CCP e fare clic su **Verifica preparazione**.
4. Nella finestra popup, fare clic su **OK**.
5. Controllare il processo di verifica della preparazione da **Notifiche > Task**.



Per ulteriori informazioni, vedere la [guida all'aggiornamento di Cisco Firepower Management Center - Firepower Software Readiness Checks] (informazioni in lingua inglese).

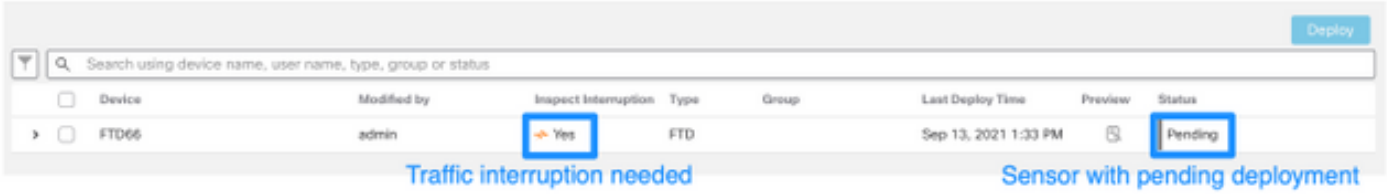
Operazioni principali dopo l'aggiornamento di FMC

Distribuisci tutte le modifiche dei criteri in sospeso

Subito dopo ogni aggiornamento o installazione di patch, è necessario implementare le modifiche nei sensori. Per garantire la distribuzione di tutte le modifiche in sospeso, eseguire la procedura seguente:

1. Passare a **Distribuisci > Distribuzione**.
2. Selezionare tutti i dispositivi nell'elenco e fare clic su **Distribuisci**.

Attenzione: La colonna Ispect Interruption indica l'interruzione del traffico



Verifica dell'installazione dell'ultimo database delle impronte digitali e delle vulnerabilità

Per verificare la versione corrente dell'impronta digitale (VDB), attenersi alla seguente procedura:

1. Selezionare **? > Informazioni su**.
2. Verificare la **versione VDB**.

Per scaricare gli aggiornamenti VDB direttamente da cisco.com, è necessario essere raggiungibili dal FMC a cisco.com.

1. Selezionare **Sistema > Aggiornamenti > Aggiornamenti prodotti**.
2. Scegliere **Scarica aggiornamenti**.
3. Installare la versione più recente disponibile.
4. Dovete riposizionare i sensori dopo.

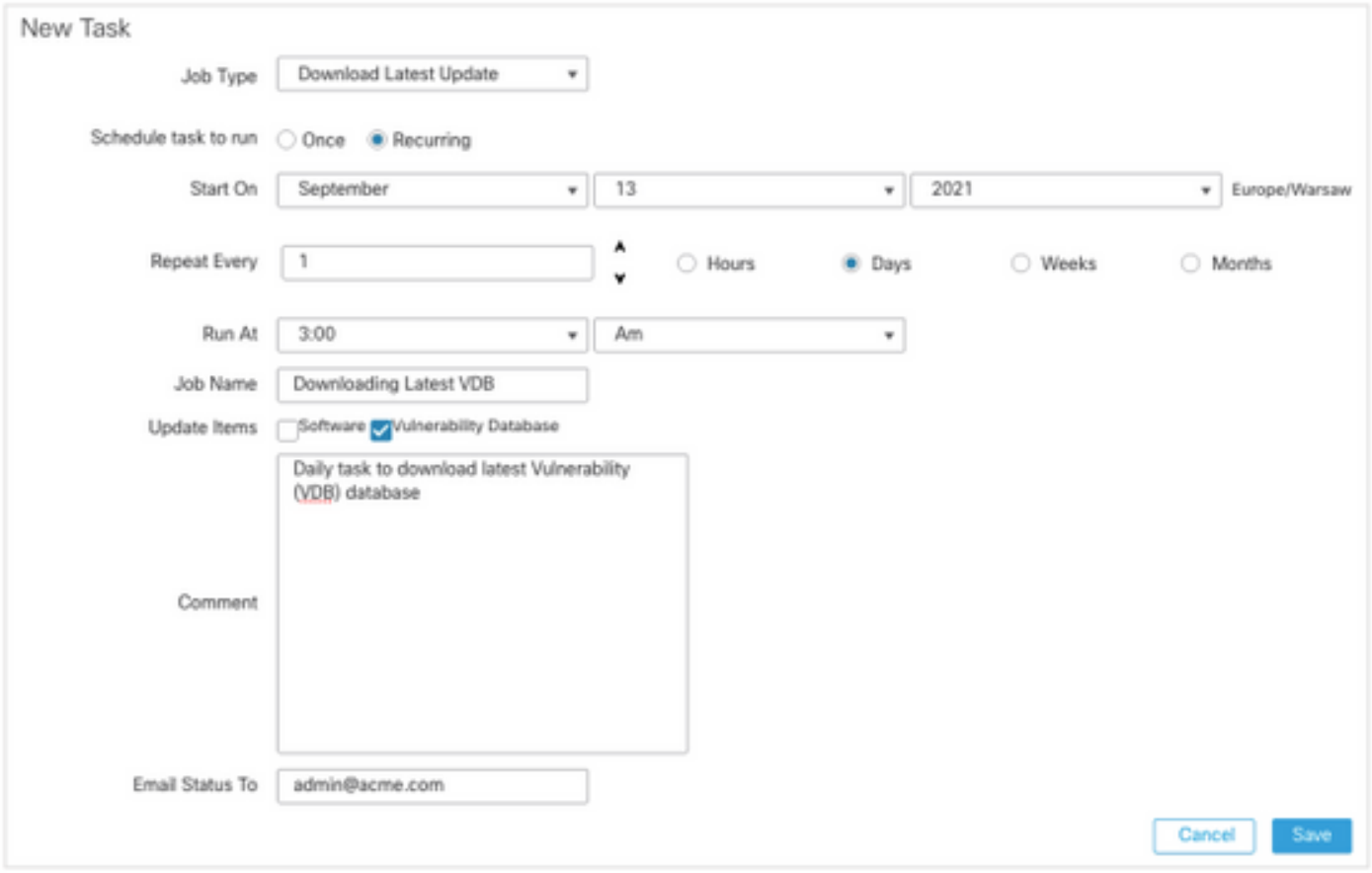
> **Nota:** Se la console centrale di gestione connessione Desktop remoto non dispone di accesso a Internet, è possibile scaricare il pacchetto VDB direttamente da software.cisco.com.

Èconsigliabile pianificare le attività per eseguire download e installazioni automatiche di pacchetti VDB.

Èbuona norma verificare ogni giorno la disponibilità di aggiornamenti VDB e installarli nel FMC durante i fine settimana.

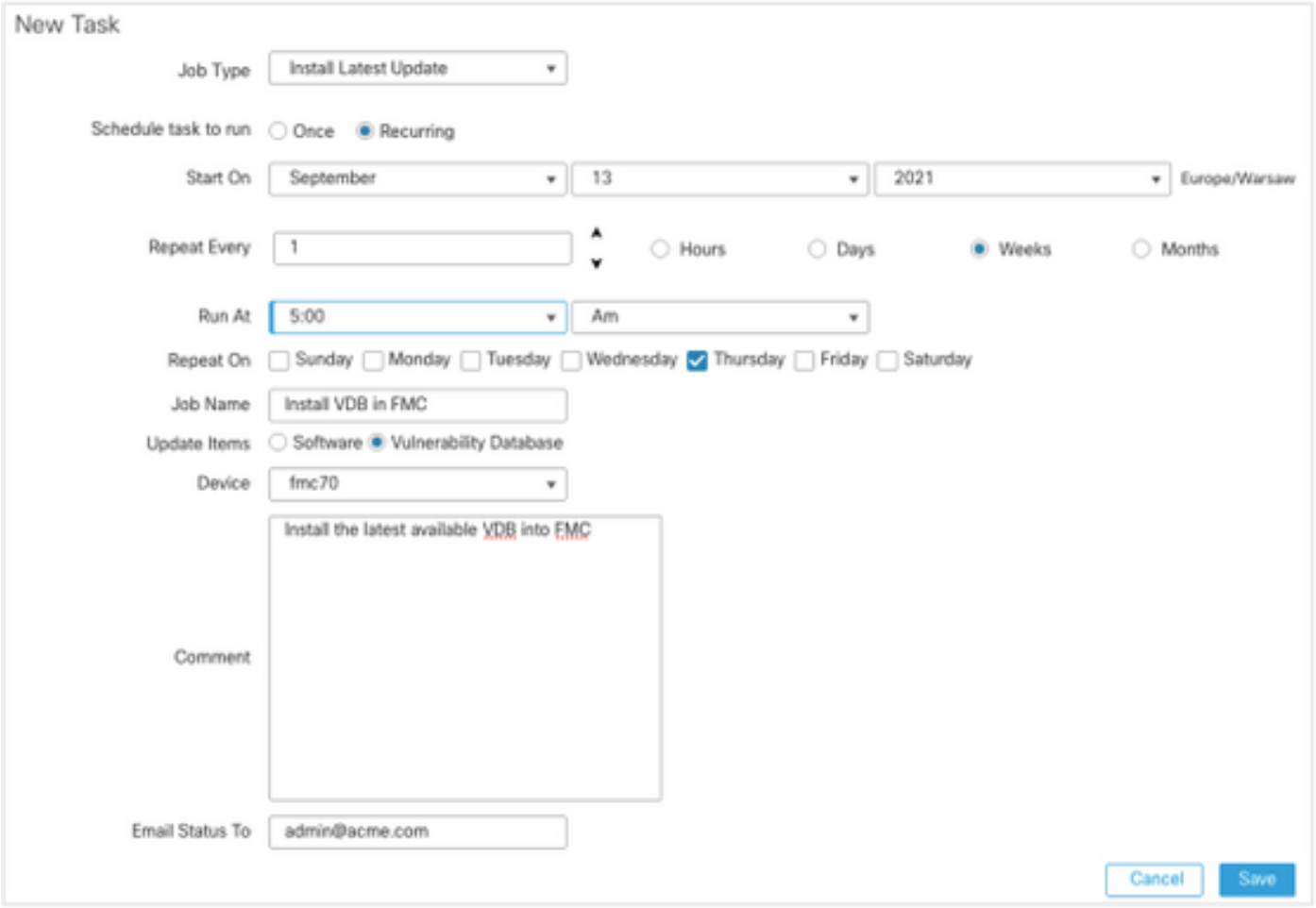
Per controllare quotidianamente il database VDB da www.cisco.com, attenersi alla seguente procedura:

1. Selezionare **Sistema > Strumenti > Programmazione**.
2. Fare clic su **Aggiungi attività**.
3. Dall'elenco a discesa **Tipo di job**, scegliere **Scarica ultimo aggiornamento.**
4. Per **eseguire l'attività Pianificazione**, fare clic sul pulsante di opzione **Periodica.**
5. Ripetere l'attività ogni giorno ed eseguirla alle 3.00 o al di fuori dell'orario di lavoro.
6. Per **Aggiorna elementi**, selezionare la casella di controllo **Database vulnerabilità.**



Per installare l'ultimo VDB nel FMC, impostare l'attività periodica settimanale:

1. Selezionare **Sistema > Strumenti > Programmazione**.
2. Fare clic su **Aggiungi attività**.
3. Dall'elenco a discesa **Tipo di job**, scegliere **Installa ultimo aggiornamento**.
4. Per **eseguire Pianifica attività**, fare clic sul pulsante di opzione **Periodica**.
5. Ripetere l'attività ogni 1 settimana ed eseguirla alle 5.00 o al di fuori dell'orario di lavoro.
6. Per **Aggiorna elementi**, selezionare la casella di controllo **Database vulnerabilità.**



Per ulteriori informazioni, vedere la guida alla configurazione di Firepower Management Center, versione 7.0 - Update the Vulnerability Database (VDB)

Verifica della regola di ordinamento e della versione corrente del pacchetto di protezione Lightweight

Per verificare le versioni SRU (Snort Rule), LSP (Lightweight Security Package) e geolocalizzazione correnti, attenersi alla seguente procedura:

1. Selezionare **? > Informazioni su**.
2. Verificare la **versione di aggiornamento** della **regola** e la **versione LSP**.

Per scaricare l'SRU e l'LSP direttamente dal sito www.cisco.com, è necessario che il FMC raggiunga www.cisco.com.

1. Passare a **Sistema > Aggiornamenti > Aggiornamenti regole**.
2. Dalla scheda **Aggiornamento unico regole/Importazione regole**, scegliere **Scarica nuovo aggiornamento regole dal sito di supporto**.
3. Scegliere **Importa**.
4. Distribuire la configurazione sui sensori in seguito.

Nota: Se il CCP non dispone di accesso a Internet, i pacchetti SRU e LSP possono essere scaricati direttamente da software.cisco.com.

Gli aggiornamenti delle regole di intrusione sono cumulativi ed è consigliabile importare sempre l'ultimo aggiornamento.

Per attivare il download e l'installazione settimanale degli aggiornamenti delle regole di snort (SRU/LSP), attenersi alla seguente procedura:

1. Passare a **Sistema > Aggiornamenti > Aggiornamenti regole**.
2. Nella scheda **Importazioni aggiornamento regole ricorrenti** selezionare la casella di controllo **Abilita importazioni aggiornamento regole ricorrenti dal sito di supporto**.
3. Scegliere la frequenza di importazione come settimanale, scegliere un giorno della settimana e nel tardo pomeriggio per il download e la distribuzione dei criteri.
4. Fare clic su **Salva**.

Per ulteriori informazioni, vedere [Firepower Management Center Configuration Guide, Version 7.0 - Update Intrusion Rules].

Verifica la versione corrente dell'aggiornamento della georilevazione

Per verificare la versione corrente della georilevazione, attenersi alla seguente procedura:

1. Selezionare **? > Informazioni su**.
2. Verificare la **versione di aggiornamento della georilevazione**.

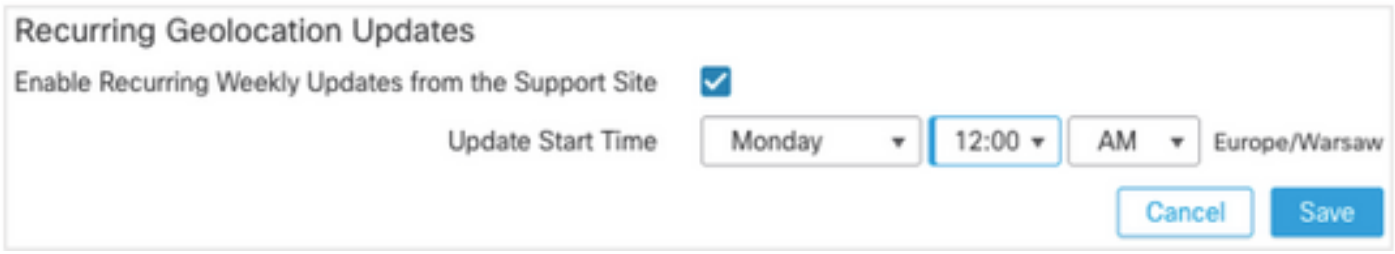
Per scaricare gli aggiornamenti di geolocalizzazione direttamente da www.cisco.com, è necessario essere raggiungibili dal FMC a www.cisco.com.

1. Passare a **Sistema > Aggiornamenti > Aggiornamenti posizione geografica**.
2. Dalla scheda **One-Time Geolocation Update**, scegliere **Download e installare l'aggiornamento della geolocalizzazione dal sito di supporto**.
3. Fare clic su **Import** (Importa).

Nota: Se il CCP non dispone di accesso a Internet, è possibile scaricare il pacchetto Aggiornamenti geolocalizzazione direttamente da software.cisco.com.

Per attivare gli aggiornamenti automatici della georilevazione, attenersi alla seguente procedura:

1. Passare a **Sistema > Aggiornamenti > Aggiornamenti posizione geografica**.
2. Nella sezione Aggiornamenti periodici geolocalizzazione selezionare la casella di controllo **Abilita aggiornamenti settimanali periodici dal sito di supporto**.
3. Scegliere la frequenza di importazione come settimanale, scegliere lunedì a mezzanotte.
4. Fare clic su **Salva**.

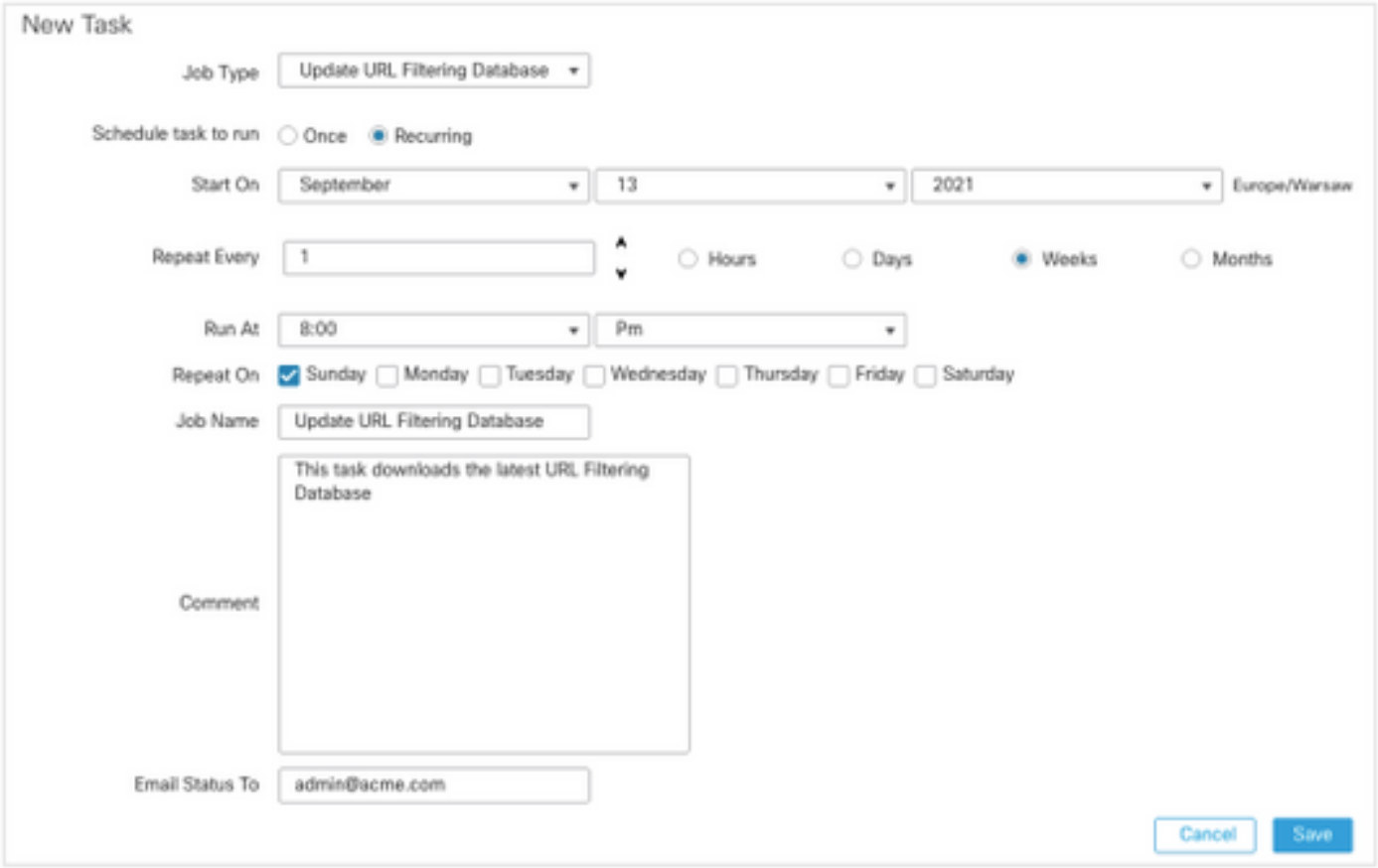


Per ulteriori informazioni, vedere Firepower Management Center Configuration Guide, versione 7.0 - Update the Geolocation Database (GeoDB).

Aggiornamento automatico del database con filtro URL e attività pianificata

Per garantire che i dati della minaccia per il filtro URL siano aggiornati, il sistema deve ottenere gli aggiornamenti dei dati dal cloud Cisco Collective Security Intelligence (CSI). Per automatizzare questo processo, eseguire la procedura seguente:

1. Selezionare **Sistema > Strumenti > Programmazione**.
2. Fare clic su **Aggiungi attività**.
3. Dall'elenco a discesa **Tipo di job**, scegliere **Aggiorna database filtro URL.**
4. Per **eseguire l'attività Pianificazione**, fare clic sul pulsante di opzione **Periodica**.
5. Ripetere l'attività ogni settimana ed eseguirla alle 20.00 la domenica o fuori dall'orario di lavoro.
6. Fare clic su **Salva**.

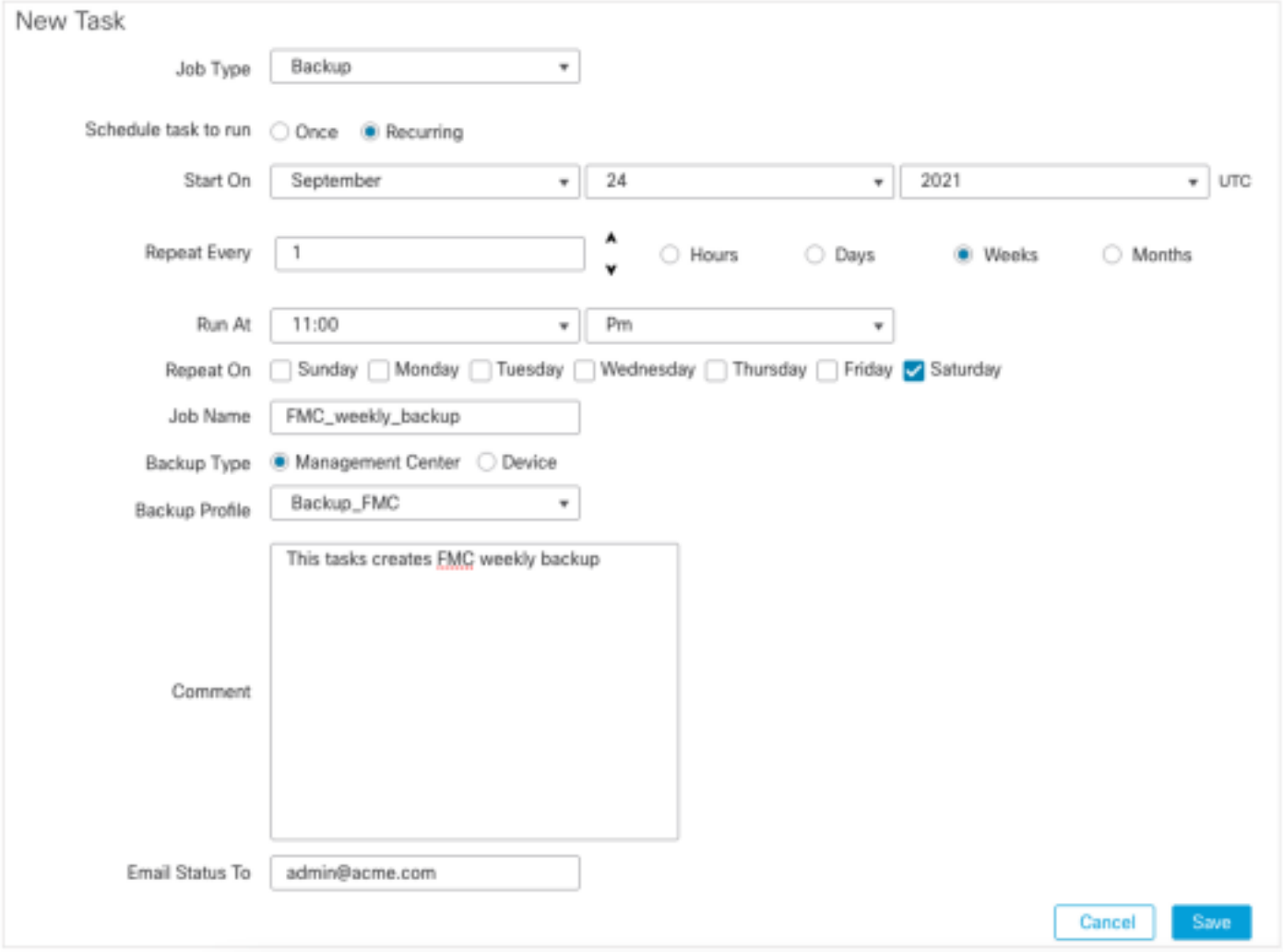


Per ulteriori informazioni, vedere la guida alla configurazione di Firepower Management Center, versione 7.0 - Automazione degli aggiornamenti del filtro URL tramite un'attività pianificata.

Configura backup periodici

Nell'ambito del piano di disaster recovery, è consigliabile eseguire backup periodici.

1. Assicurarsi di appartenere al **dominio globale**.
2. Creare il profilo di backup FMC. Per ulteriori informazioni, vedere la sezione **Creazione del backup di FMC**.
3. Selezionare **Sistema > Strumenti > Programmazione**.
4. Fare clic su **Aggiungi attività**.
5. Dall'elenco a discesa **Tipo di job**, scegliere **Backup.**
6. Per **eseguire l'attività Pianificazione**, fare clic sul pulsante di opzione **Periodica**.
   La frequenza di backup deve essere adattata alle esigenze dell'organizzazione. È consigliabile creare backup durante un intervento di manutenzione o in altri periodi di scarso utilizzo.
7. Per **Tipo di backup**, fare clic sul pulsante di opzione **Centro di gestione**.
8. Dall'elenco a discesa **Profilo di backup**, scegliere il Profilo di backup.
9. Fare clic su **Salva**.

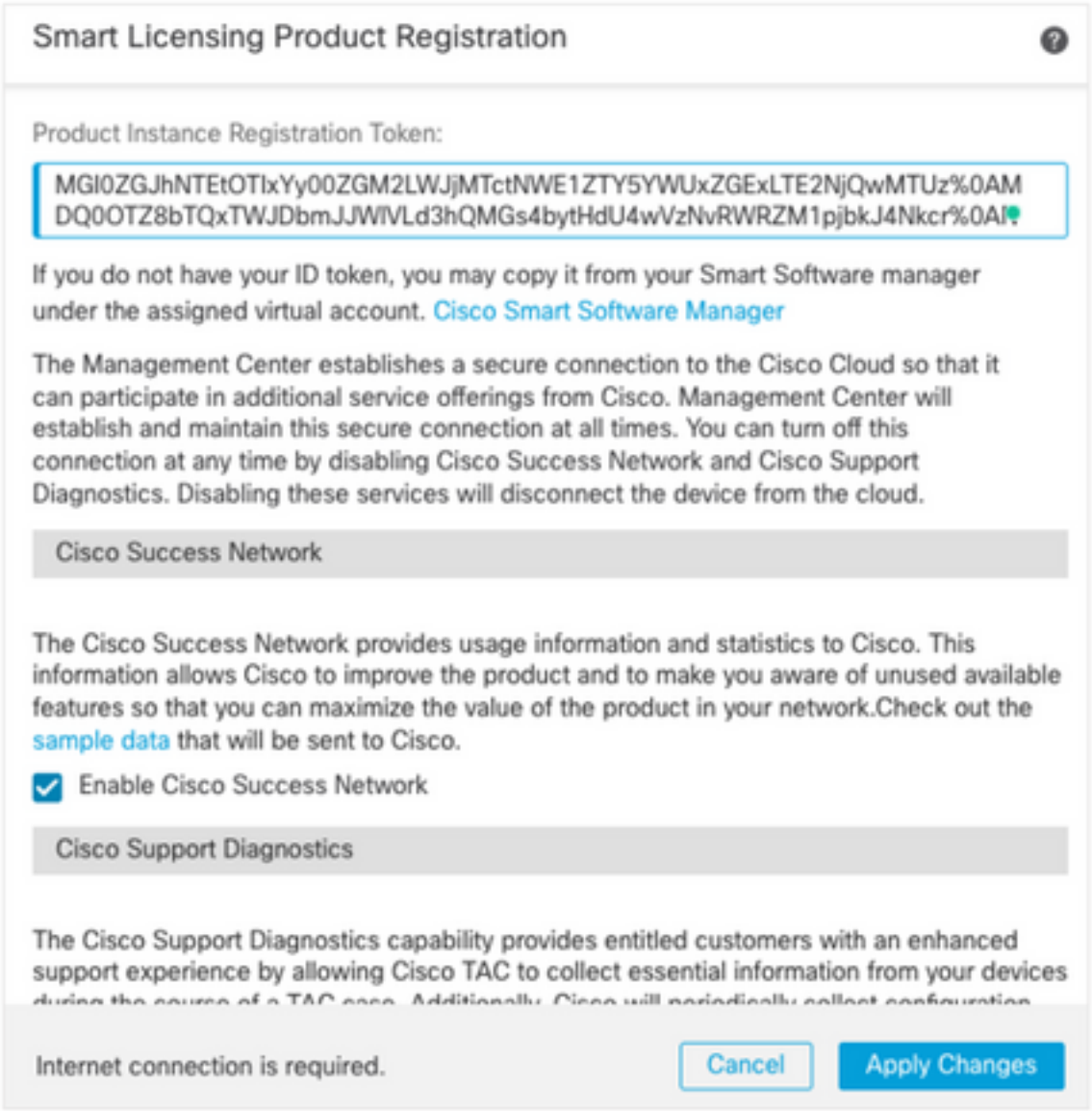


Per ulteriori informazioni, vedere la [guida alla configurazione di Firepower Management Center, versione 7.0 - capitolo: Backup e ripristino].

Verificare che la Smart License sia registrata

Per registrare Cisco Firewall Management Center con Cisco Smart Software Manager, attenersi alla seguente procedura:

1. In https://software.cisco.com, selezionare **Smart Software Manager > Manage licenses**.
2. Passare alla scheda **Magazzino > Generale** e creare un **nuovo token**.
3. Nell'interfaccia utente di FMC, selezionare **Sistema > Licenze > Licenze Smart**.
4. Fare clic su **Registra**.
5. Inserire il token generato nel portale delle licenze Cisco Smart Software.
6. Verificare che **Cisco Success Network sia abilitato**.
7. Fare clic su **Applica modifiche**.
8. Verificare Lo Stato Della Licenza Smart.



Per ulteriori informazioni, vedere la guida alla configurazione di Firepower Management Center, versione 7.0 - Registrazione di licenze Smart.

Esaminare la configurazione degli insiemi di variabili

Assicurarsi che la variabile HOME_NET contenga solo le reti/subnet interne all'organizzazione. Una definizione errata dell'insieme di variabili influisce negativamente sulle prestazioni del firewall.

1. Passare a **Oggetti > Insieme variabili**.
2. Modificare il set di variabili utilizzato dai criteri per le intrusioni. È consentito avere un set di variabili per criterio intrusione con impostazioni diverse.
3. Regolare le variabili in base all'ambiente e fare clic su **Salva**.

Altre variabili di interesse sono DNS_SERVERS O HTTP_SERVERS.

Per ulteriori informazioni, vedere Firepower Management Center Configuration Guide, versione 7.0 - Variable Sets (Guida alla configurazione di Firepower Management Center, versione 7.0 - Set di variabili).

Verifica abilitazione servizi cloud

Per trarre vantaggio dai diversi servizi cloud, npassare a **Sistema > Integrazione > Servizi cloud**.

Filtro URL

1. Abilitare il filtro URL e consentire gli aggiornamenti automatici; attivare Query su Cisco Cloud per URL sconosciuti.
   Una scadenza URL cache più frequente richiede un numero maggiore di query nel cloud, con conseguente rallentamento dei carichi Web.
2. **Salvare le modifiche.**

Suggerimento: Per la scadenza dell'URL della cache, lasciare il valore predefinito **Mai**. Se è necessaria una riclassificazione Web più rigorosa, questa impostazione può essere modificata di conseguenza.

AMP for Networks

1. Verificare che entrambe le impostazioni siano attive: **Abilita gli aggiornamenti automatici del rilevamento malware locale** e **condividi l'URI dagli eventi malware con Cisco**.
2. In FMC 6.6.X, disabilitare l'uso della porta legacy 32137 per AMP for Networks in modo che la porta TCP utilizzata sia 443.
3. **Salvare le modifiche.**

Nota: Questa impostazione non è più disponibile in FMC 7.0+ e la porta è sempre 443.

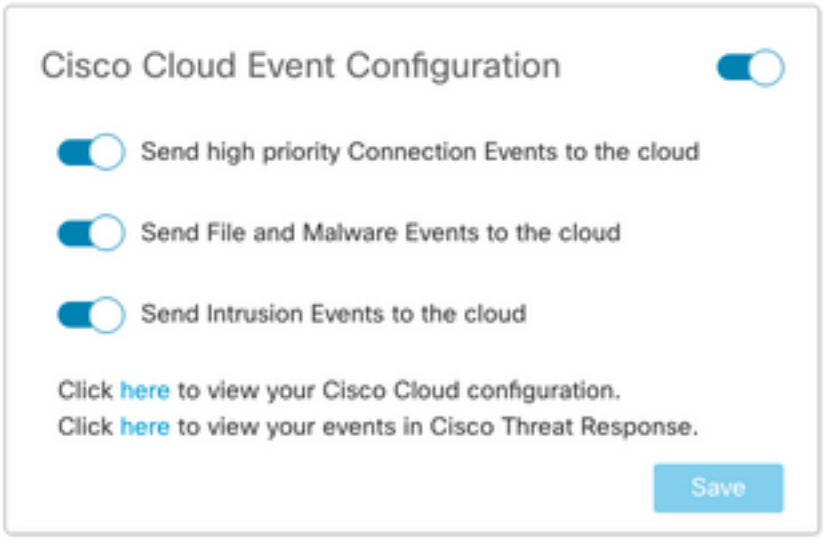
Area Cisco Cloud

1. L'area cloud deve corrispondere all'area organizzazione SecureX. Se l'organizzazione SecureX non viene creata, scegliere la regione più vicina all'installazione di FMC: Area APJ, area UE o area USA.
2. **Salvare le modifiche.**

Cisco Cloud Event Configuration

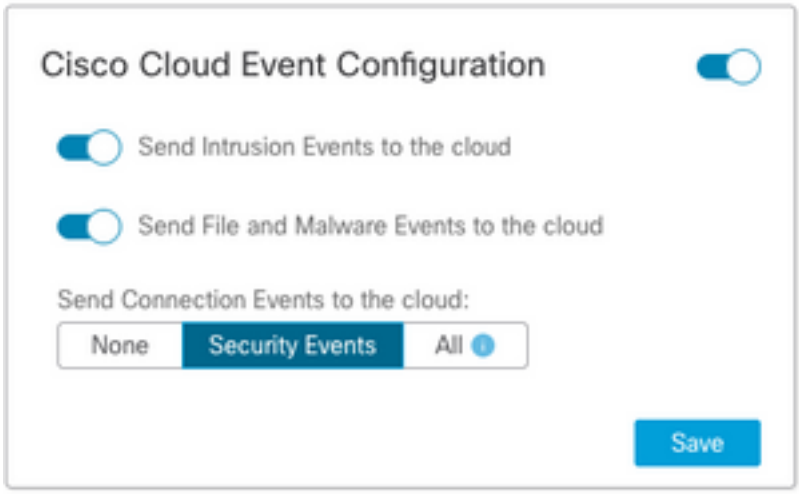
Per FMC 6.6.x

1. Verificare tutte e tre le opzioni: Vengono scelti **l'invio di eventi di connessione ad alta priorità al cloud**, l'**invio di eventi di file e malware al cloud** e l'**invio di eventi di intrusione al cloud**.
2. **Salvare le modifiche.**



Per FMC 7.0+

1. Accertarsi che siano selezionate entrambe le opzioni: **Invia eventi intrusione al cloud** e **invia eventi file e malware al cloud**.
2. Per il tipo di eventi di connessione, scegliere **All** se la soluzione di analisi e registrazione della sicurezza è in uso. Per SecureX, scegliere solo **Eventi protezione**.
3. **Salvare le modifiche.**



Abilita integrazione SecureX

L'integrazione SecureX fornisce visibilità istantanea dello scenario delle minacce tra i prodotti di sicurezza Cisco. Per connettere SecureX e abilitare la barra multifunzione, eseguire la procedura seguente:

Integrazione della barra multifunzione SecureX

> **Nota:** Questa opzione è disponibile per FMC versione 7.0+.

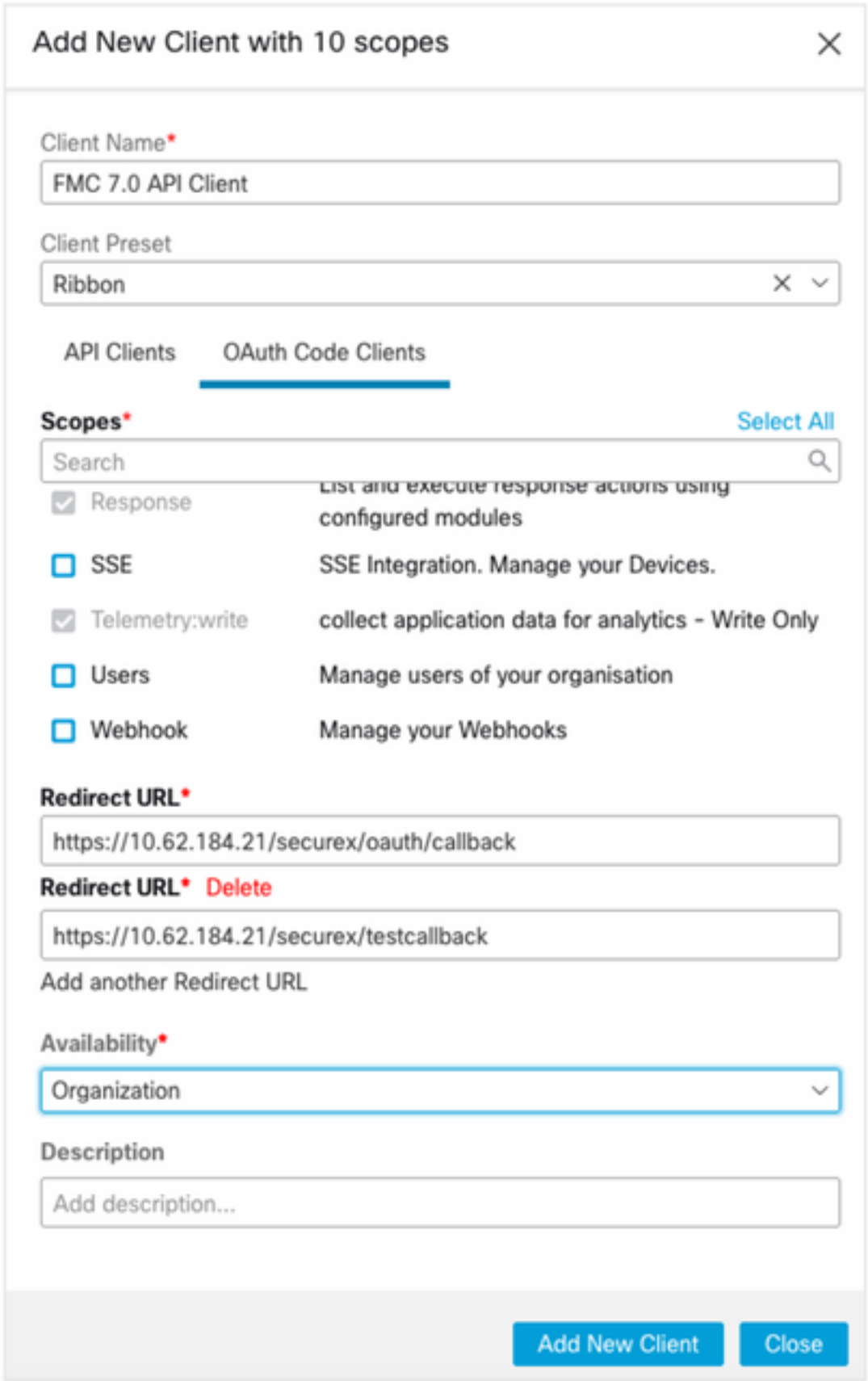
1. Accedere a SecureX e creare un client API: Nel campo **Nome client** immettere un nome descrittivo del CCP. Ad esempio, Client API FMC 7.0.Fare clic sulla scheda **Client codice Oauth**.Nell'elenco a discesa **Client Preset**, scegliere **Barra multifunzione**. Vengono scelti gli ambiti: Casebook, Enrich:read, Global Intel:read, Inspect:read, Notification, Orbital, Private

Intel, Profile, Response, Telemetry:write.Aggiungere i due URL di reindirizzamento presentati nel FMC:

URL di reindirizzamento: <URL_FMC>/securex/oauth/callback

Secondo URL di reindirizzamento: <URL_FMC>/securex/testcallback

1. Nell'elenco a discesa **Disponibilità** scegliere **Organizzazione**.Fare clic su **Aggiungi nuovo client**.



2. Dalla FMC, selezionare **System > SecureX** (Sistema > SecureX).

3. Attivare l'interruttore nell'angolo superiore destro e verificare che l'area visualizzata corrisponda all'organizzazione SecureX.

4. Copiare l'**ID** e la **password client** e incollarli nel CCP.

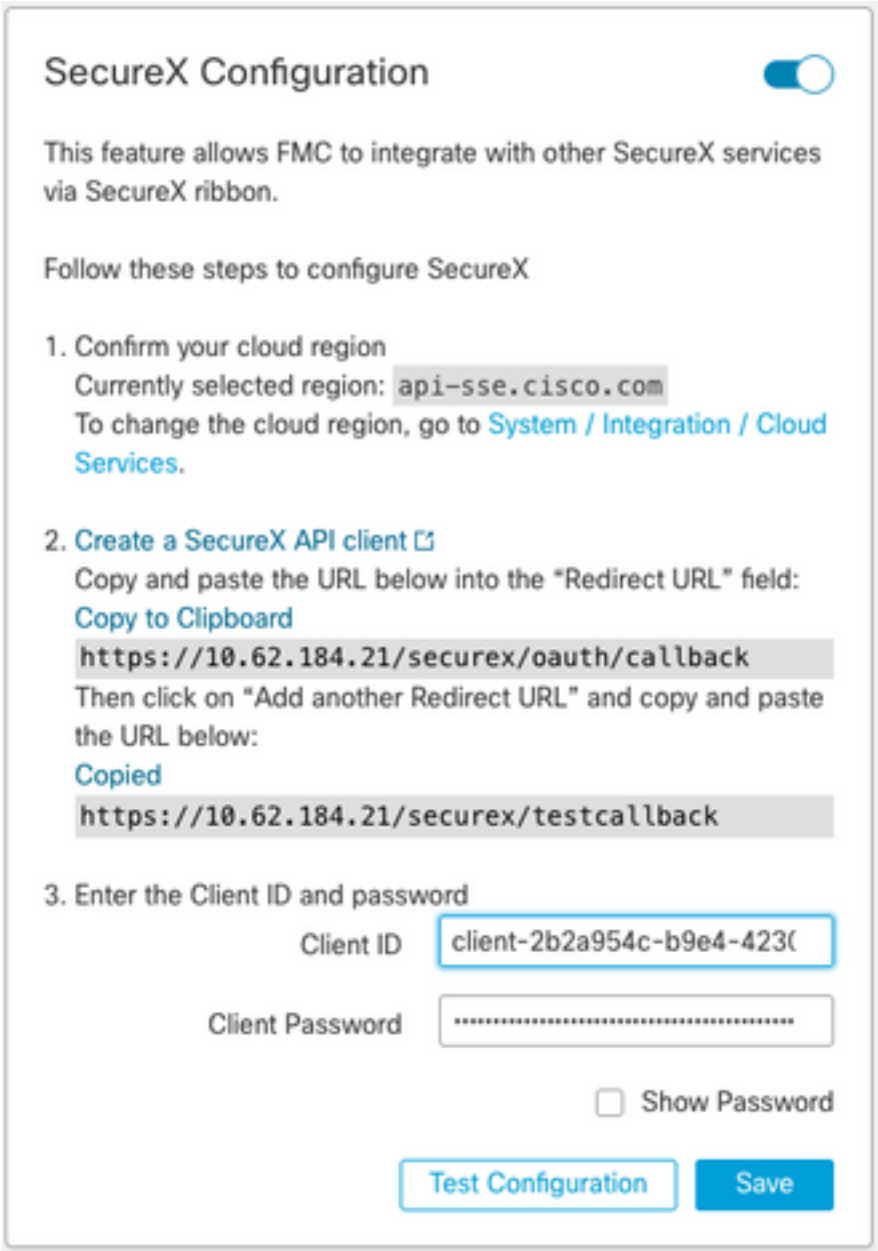
5. Scegliere **prova configurazione**.

6. Accedere a SecureX per autorizzare il client API.

7. Salvare le modifiche e aggiornare il browser per visualizzare la barra multifunzione nella parte inferiore.

8. Espandere la barra multifunzione e scegliere **Ottieni SecureX**. Se richiesto, immettere le credenziali SecureX.

9. La barra multifunzione SecureX è ora completamente funzionale per l'utente FMC.

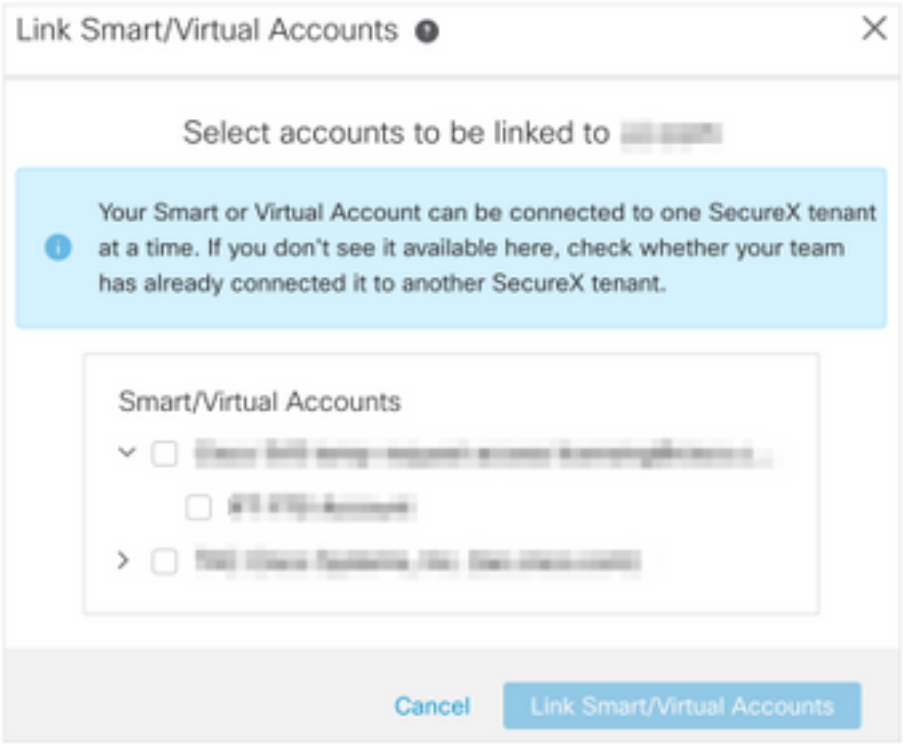


5YVPsGdzrkX8q8q0yYl-tDitezO6p_17MtH6NATx68fUZ5u9T3qOEQ

> **Nota:** Se un altro utente FMC richiede l'accesso alla barra multifunzione, tale utente deve accedere alla barra multifunzione con le credenziali SecureX.

Invia eventi connessione a SecureX

1. Nel FMC, selezionare **System > Integration > Cloud Services** (Sistema > Integrazione > Servizi cloud) e accertarsi che **Cisco Cloud Event Configuration (Configurazione eventi cloud Cisco)** invii eventi Intrusion, File e Malware come spiegato nella sezione **Turn on Cloud Services** (Attiva servizi cloud).
2. Verificare che il CCP sia registrato con una Smart License come spiegato nella sezione **Registrazione delle Smart Licenses**.
3. Prendere nota del nome dell'**account virtuale assegnato** visualizzato in FMC in **Sistema > Licenze > Smart Licenses**.
4. Registrare il CCP in SecureX: In SecureX, selezionare **Amministrazione > Dispositivi**.Scegliere **Gestisci dispositivi**.Verificare che nel browser siano consentite finestre popup.Accedere a Security Services Exchange (SSE).Selezionare **Menu Strumenti > Collega account Smart/virtuali**.Scegliere **Collega altri account**.Selezionare l'account virtuale assegnato al CCP (passaggio 3).Scegliere **Collega account Smart/virtuali.**



- Verificare che il dispositivo FMC sia elencato in Dispositivi.
- Passare alla scheda **Cloud Services**, quindi attivare le funzionalità **Cisco SecureX threat response** e **Eventing**.
- Scegliere le **Impostazioni di servizio aggiuntive** (icona a forma di ingranaggio) accanto alla funzione Eventi.
- Nella scheda Generale, scegliere **Condividi dati evento con Talos**.
- Nella sezione Per tipo di evento della scheda Promozione automatica eventi scegliere tutti i tipi di evento disponibili e **Salva**.

5. Nel portale principale di SecureX, passare a **Integration Modules > Firepower** e aggiungere il modulo di integrazione Firepower.

6. Creare un nuovo dashboard.

7. Aggiungere le tessere relative a Firepower.

Integrate Secure Endpoint (AMP for Endpoints)

Per abilitare l'integrazione di Secure Endpoint (AMP for Endpoints) con l'implementazione di Firepower, eseguire la procedura seguente:

1. Passare a **AMP > Gestione AMP**.
2. Scegliere **Aggiungi connessione cloud AMP**.
3. Scegliere il cloud e **Registrarsi**.

Nota: Lo stato **Abilitato** indica che la connessione al cloud è stata stabilita.

Integrazione Analisi malware sicuro (Threat Grid)

Per impostazione predefinita, Firepower Management Center può connettersi al cloud pubblico Cisco Threat Grid per l'invio di file e il recupero di report. Impossibile eliminare la connessione. Tuttavia, si consiglia di scegliere la soluzione più vicina al cloud di distribuzione:

1. Passare a **AMP > Connessioni analisi dinamica**.
2. Fare clic su **Modifica** (icona a forma di matita) nella sezione Azione.
3. Scegliere il nome del cloud corretto.
4. Per associare l'account Threat Grid per funzionalità di reporting dettagliate e sandbox avanzate, fare clic sull'icona **Associa**.

Per ulteriori informazioni, vedere Firepower Management Center Configuration Guide, versione 7.0 - Enabling Access to Dynamic Analysis Results in the Public Cloud (Guida alla configurazione di Firepower Management Center, versione 7.0 - Abilitazione dell'accesso ai risultati dell'analisi dinamica nel cloud pubblico).

Per l'integrazione in sede dell'appliance Thread Grid, vedere la guida alla configurazione di Firepower Management Center, versione 7.0 - Dynamic Analysis On-Premises Appliance (Cisco Threat Grid) .