Configurare la disponibilità elevata in FMC

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Premesse

Operazioni preliminari

Configurazione

- Configura FMC secondario
- Configura FMC primario

Verifica

Introduzione

In questo documento viene descritto un esempio di configurazione dell'alta disponibilità (HA, High Availability) su un centro di gestione dei firewall (FMC, Firewall Management Center).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Secure FMC per VMware v7.2.5.

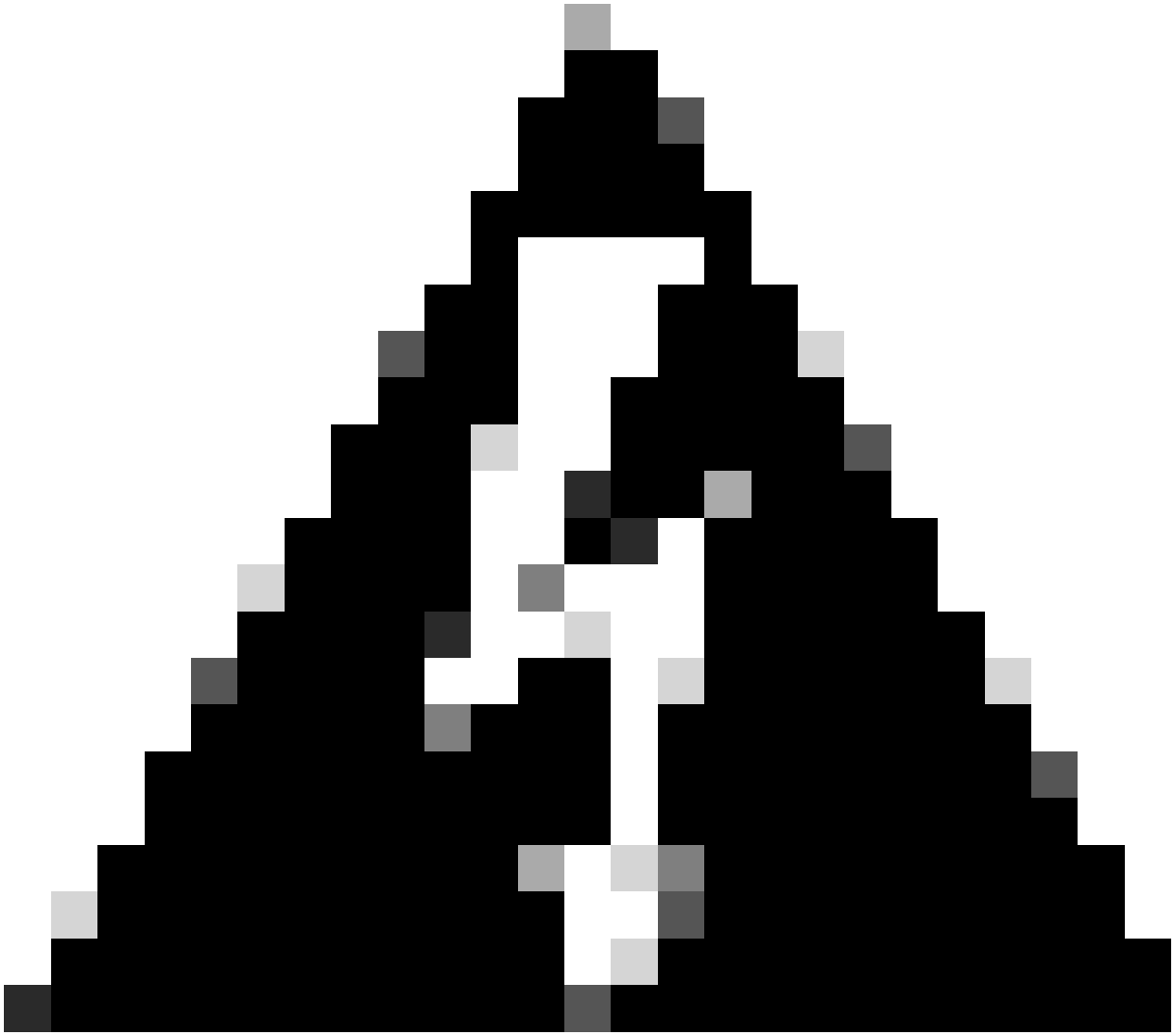
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I requisiti specifici per questo documento includono:

- Entrambi i peer FMC devono trovarsi sulla stessa versione del software, sull'aggiornamento delle regole di intrusione, sul database delle vulnerabilità e sul Lightweight Security Package
- Entrambi i peer FMC devono avere la stessa capacità o versione hardware
- Entrambi i CCP richiedono una licenza separata

Per una serie completa di requisiti, è possibile consultare la Guida all'amministrazione.



Avviso: In caso di mancata corrispondenza tra i requisiti elencati, non è possibile configurare HA.

Questa procedura è supportata su tutti gli accessori hardware.

Operazioni preliminari

- Garantire l'accesso degli amministratori a entrambi i CCP
- Connettività tra le interfacce di gestione
- Esaminare le versioni del software e verificare che siano stati eseguiti tutti gli aggiornamenti necessari

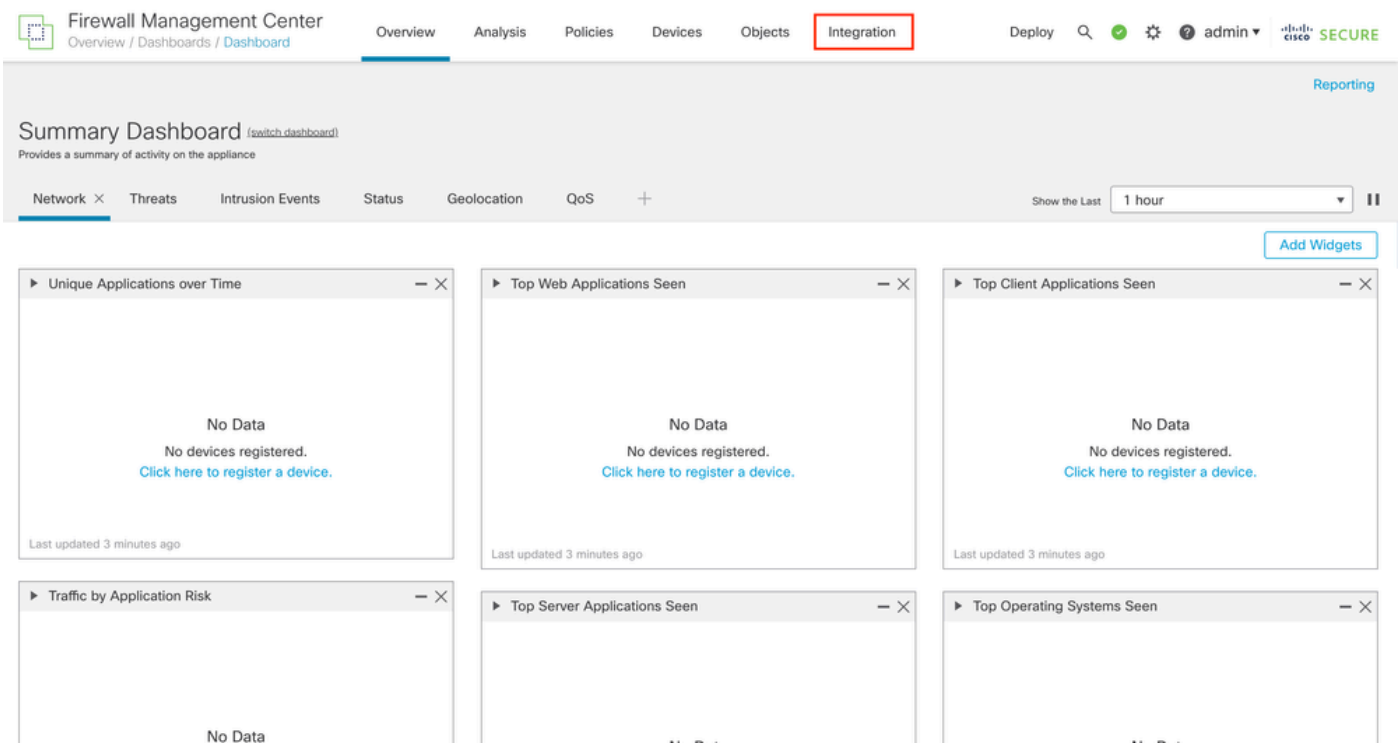
Configurazione

Configura FMC secondario

Passaggio 1. Accedere all'interfaccia utente grafica (GUI) del dispositivo del FMC che assumerà il ruolo di database secondario/standby.

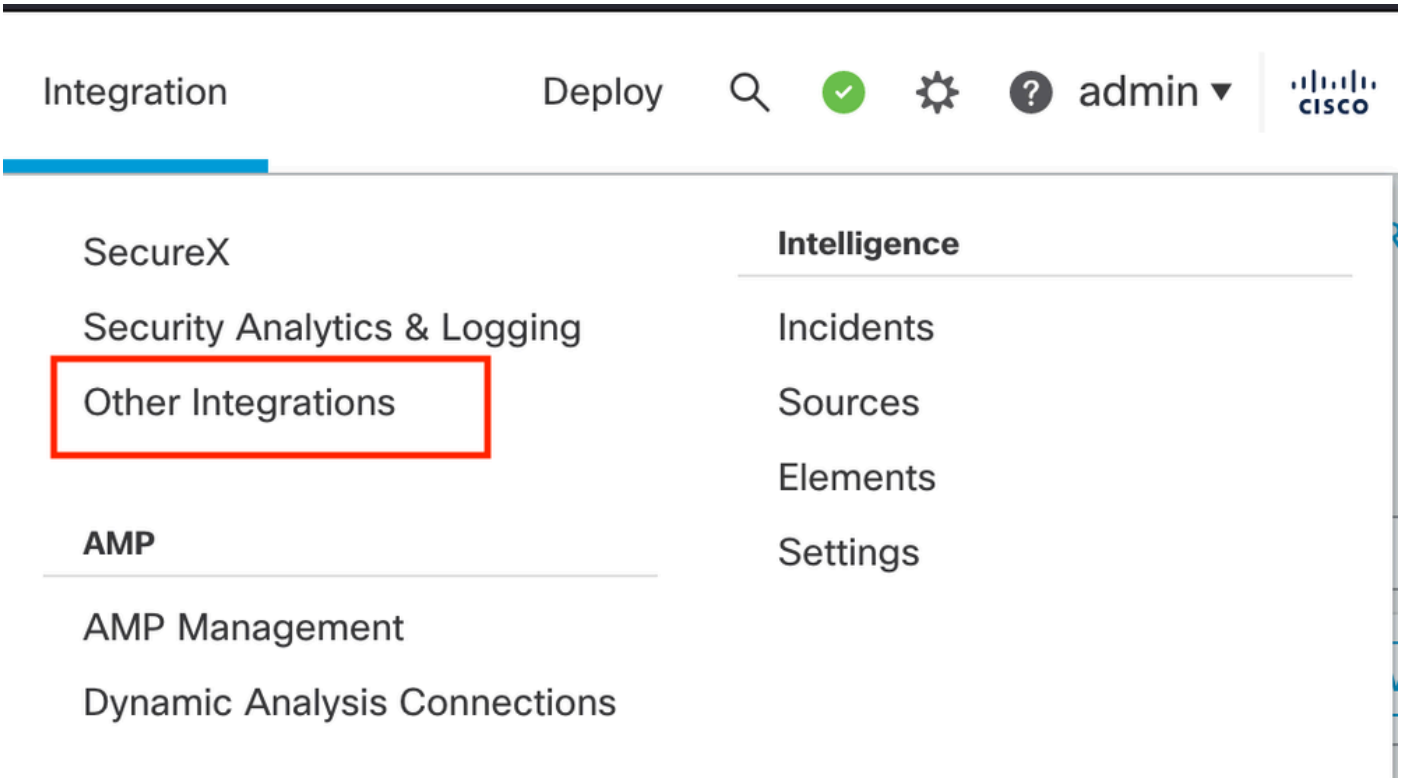
Accedere a FMC

Passaggio 2. Passare alla scheda Integrazione.



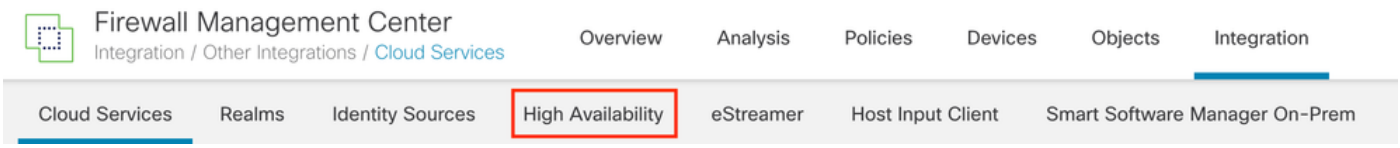
Passa all'integrazione

Passaggio 3. Fare clic su Altre integrazioni.



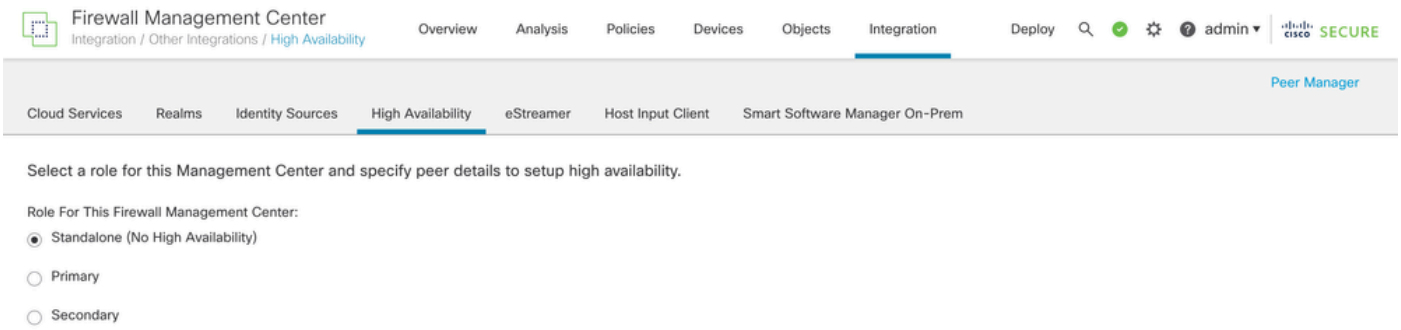
Passa ad altra integrazione

Passaggio 4. Passare alla scheda Alta disponibilità.



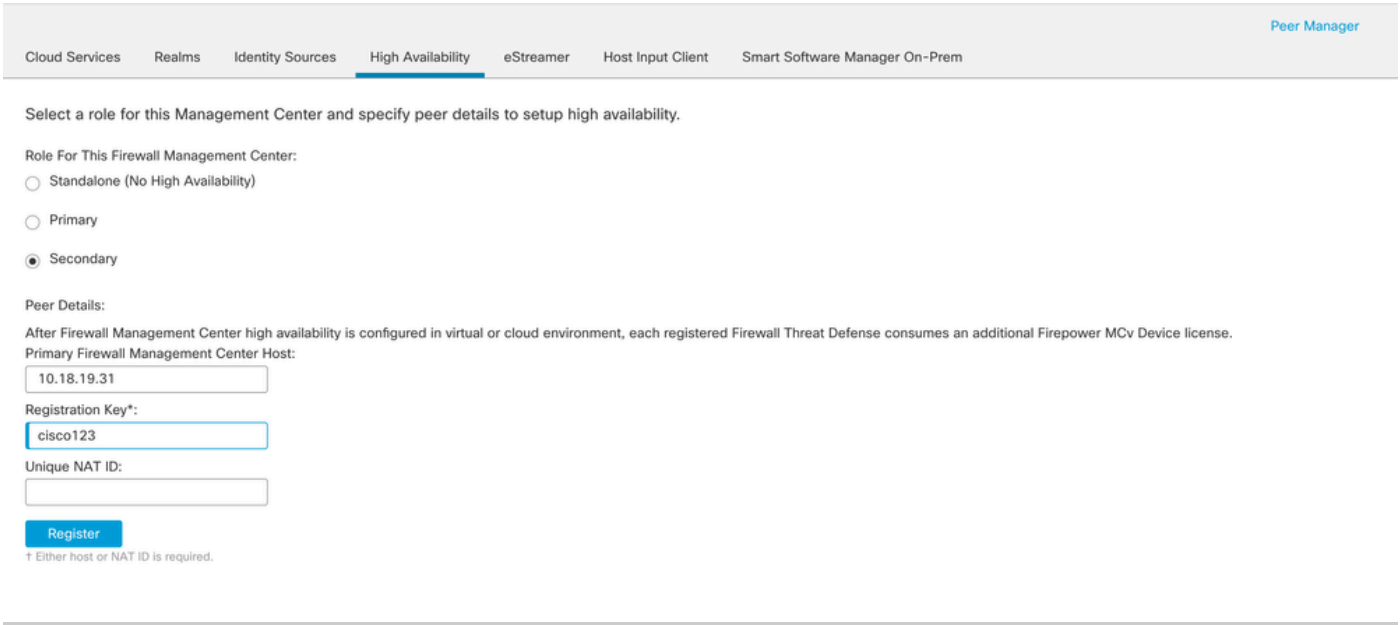
Passa a Alta disponibilità

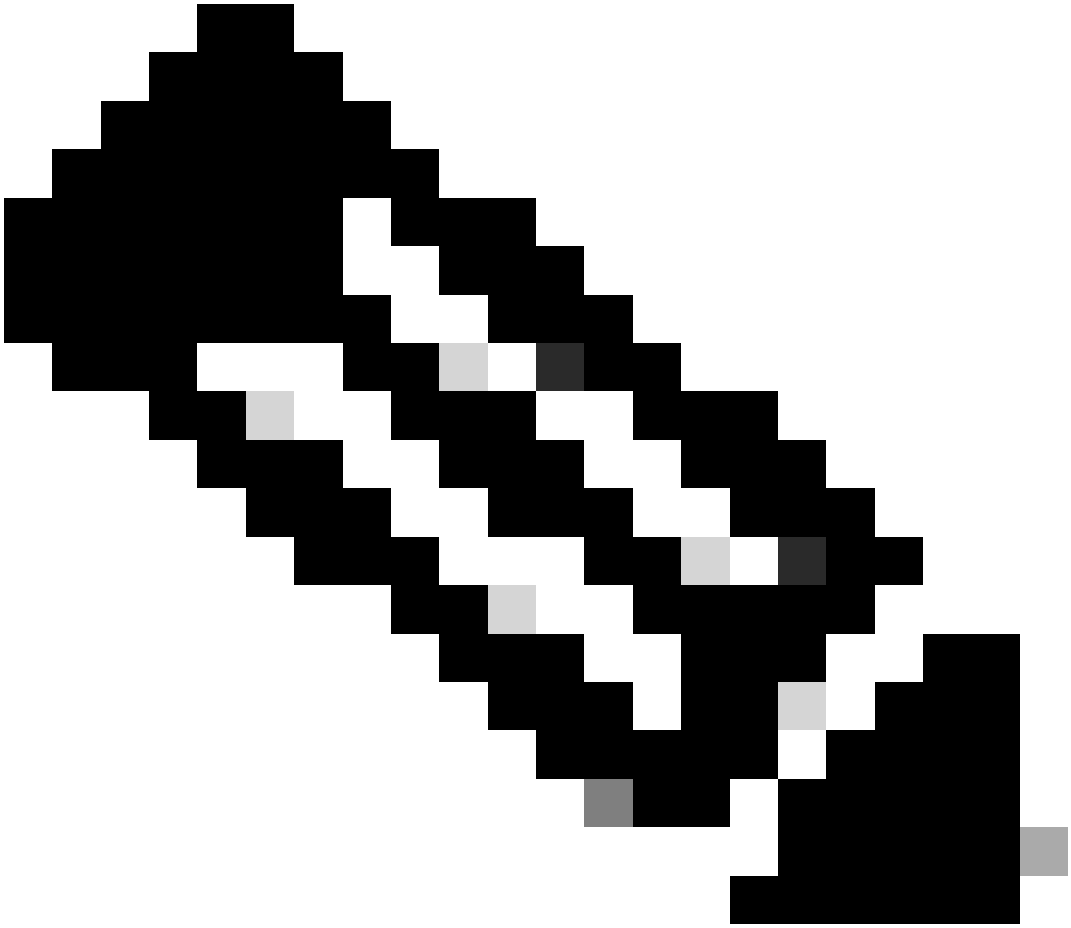
Passaggio 5. Fare clic su Secondario.



Immettere le informazioni e selezionare il ruolo desiderato per il CCP corrente

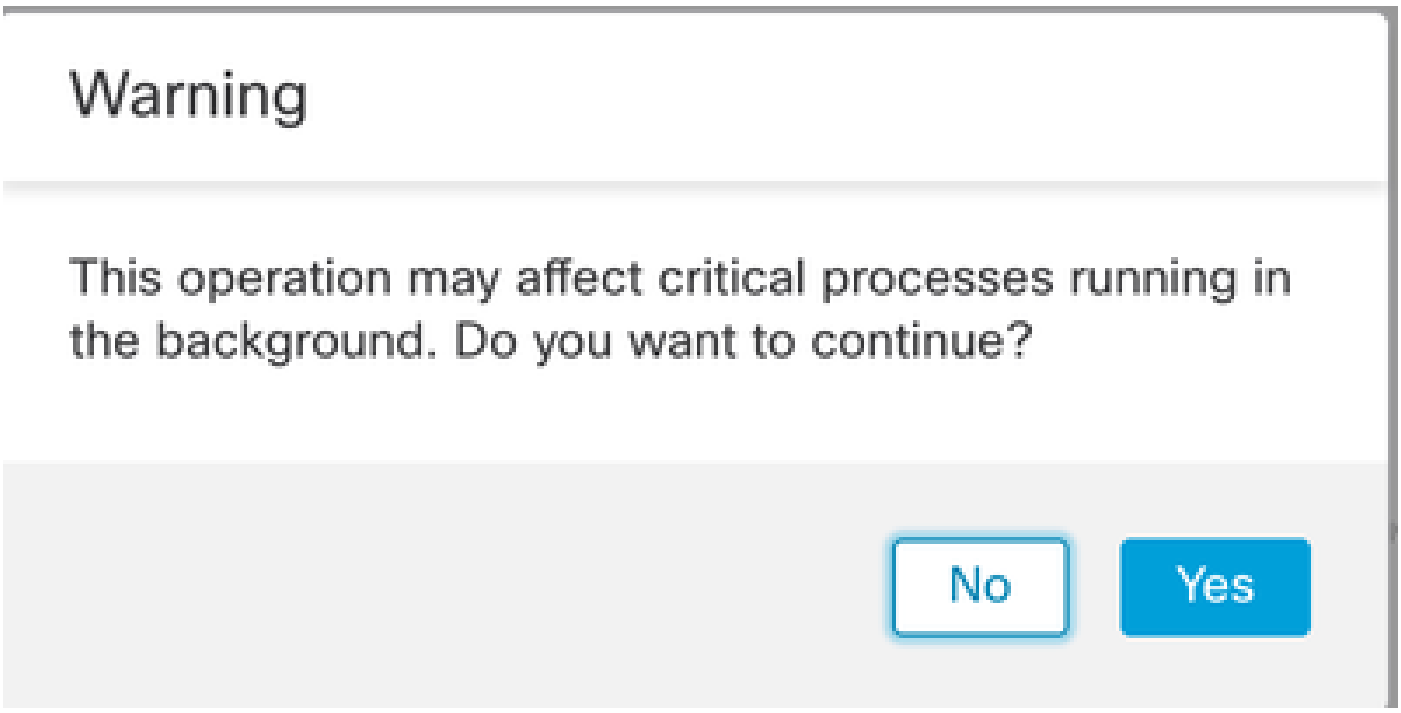
Passaggio 6. Immettere le informazioni sul peer primario/attivo e fare clic su **Register**.

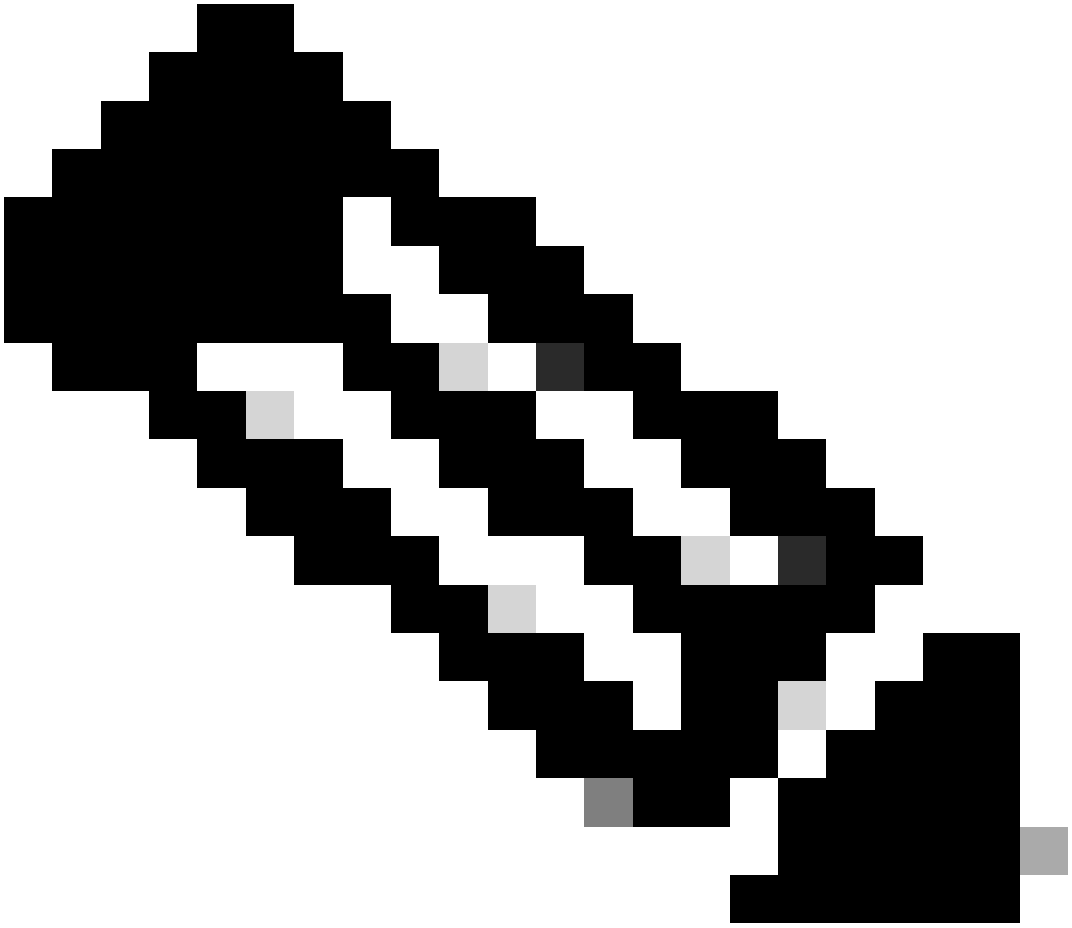




Nota: Prendere nota della chiave di registrazione, in quanto verrà utilizzata sul CCP attivo.

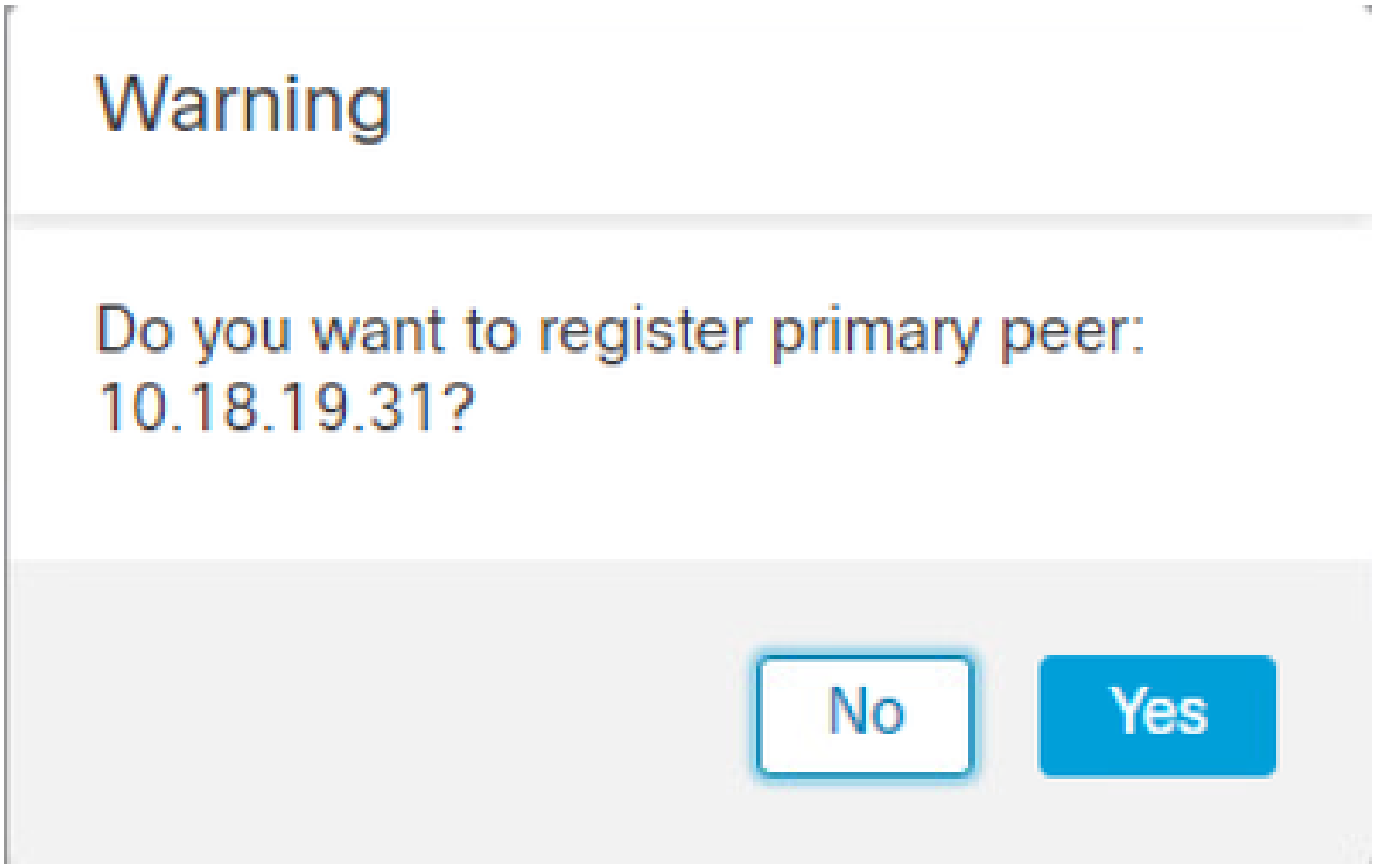
Passaggio 7. Questo avviso richiede di confermare, fare clic su **Yes**.

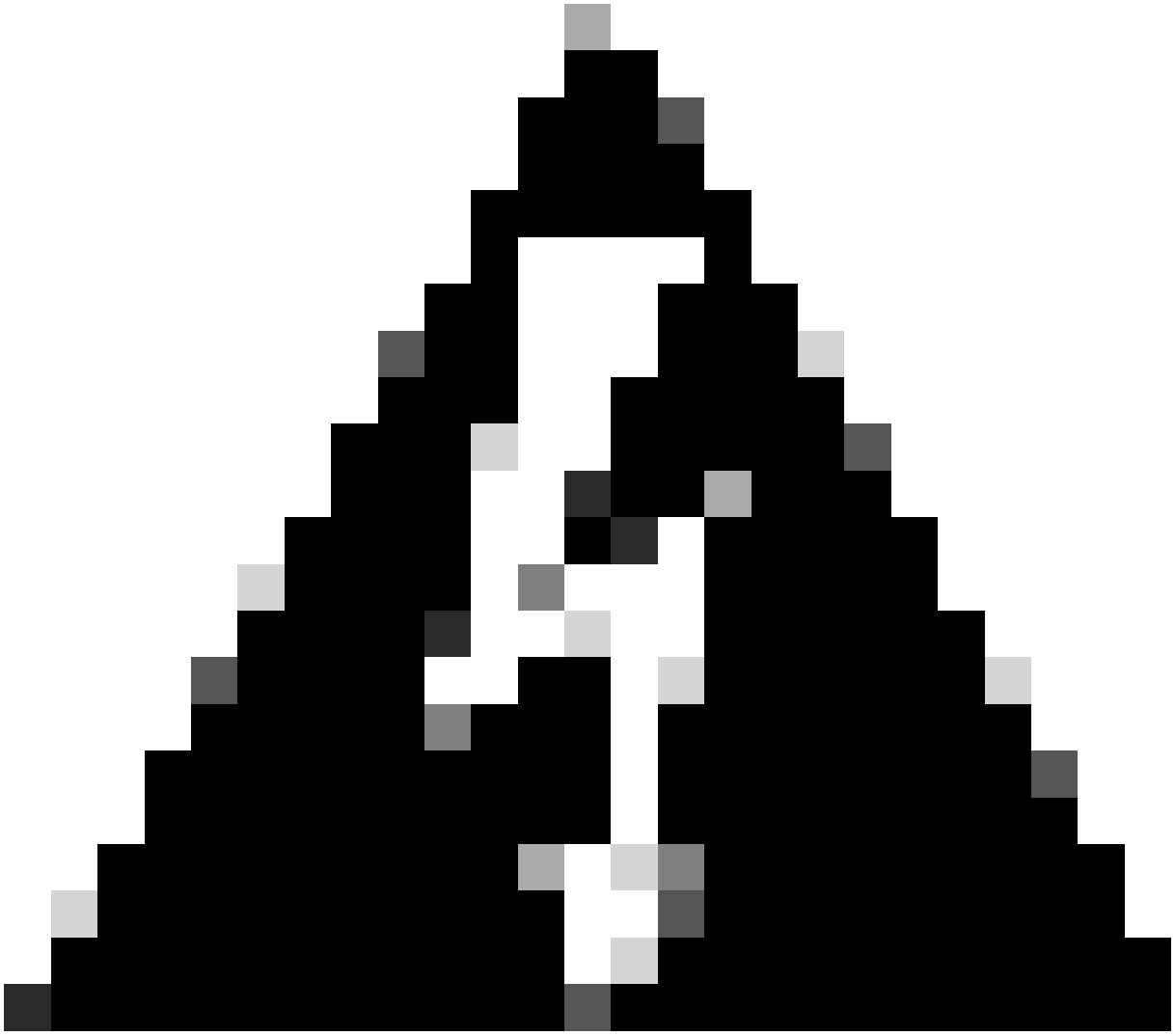




Nota: Verificare che non vi siano altre attività in esecuzione mentre è in corso la creazione di HA, la GUI viene riavviata.

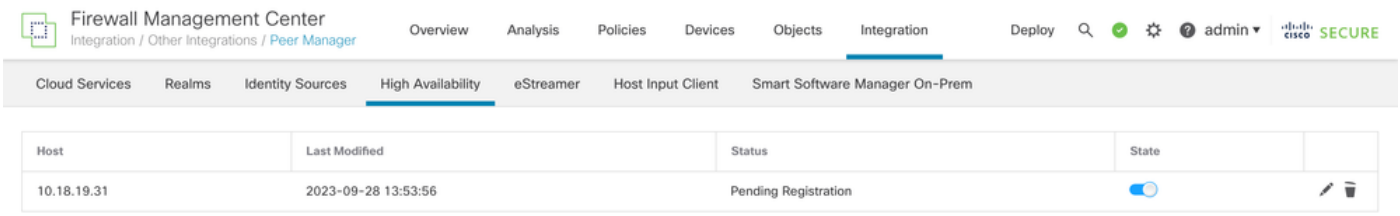
Passaggio 8. Confermare che si desidera registrare il peer primario.


Warning
Do you want to register primary peer:
10.18.19.31?
No
Yes



Avviso: Tutte le informazioni su Dispositivi/Criteri/Configurazione verranno rimosse dal FMC secondario dopo la creazione di HA.

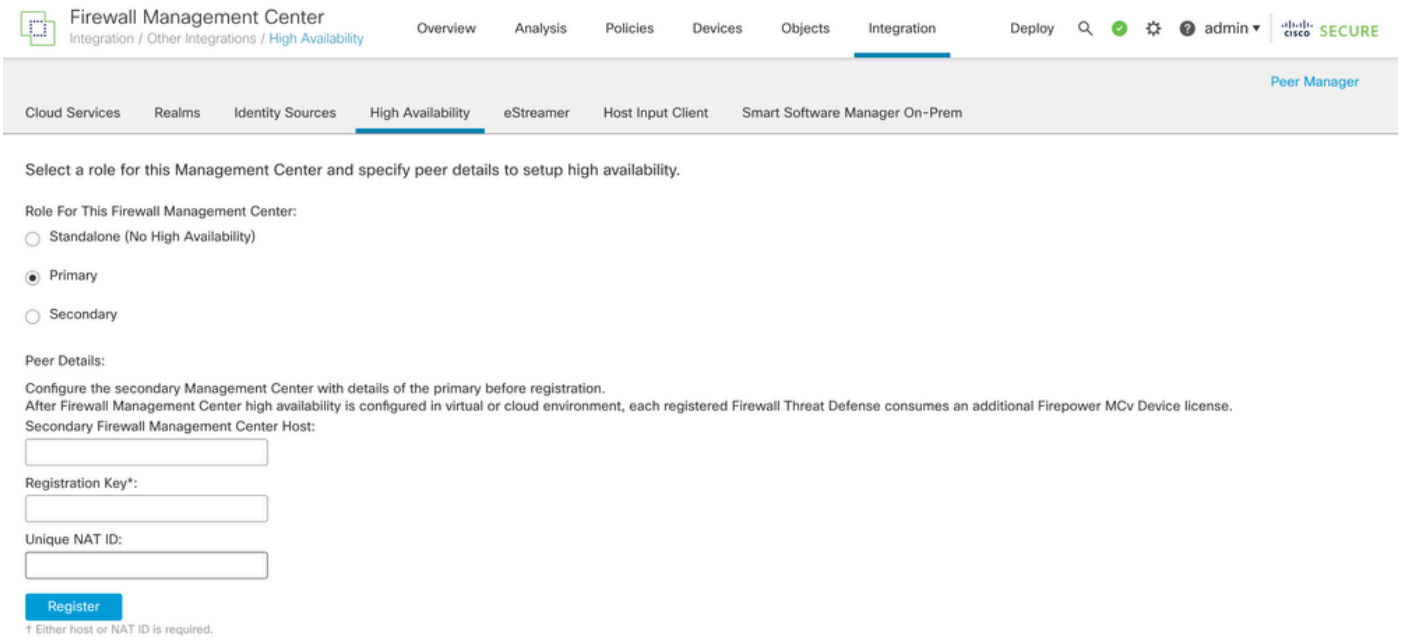
Passaggio 9. Verificare che lo stato del CCP secondario sia in sospeso.



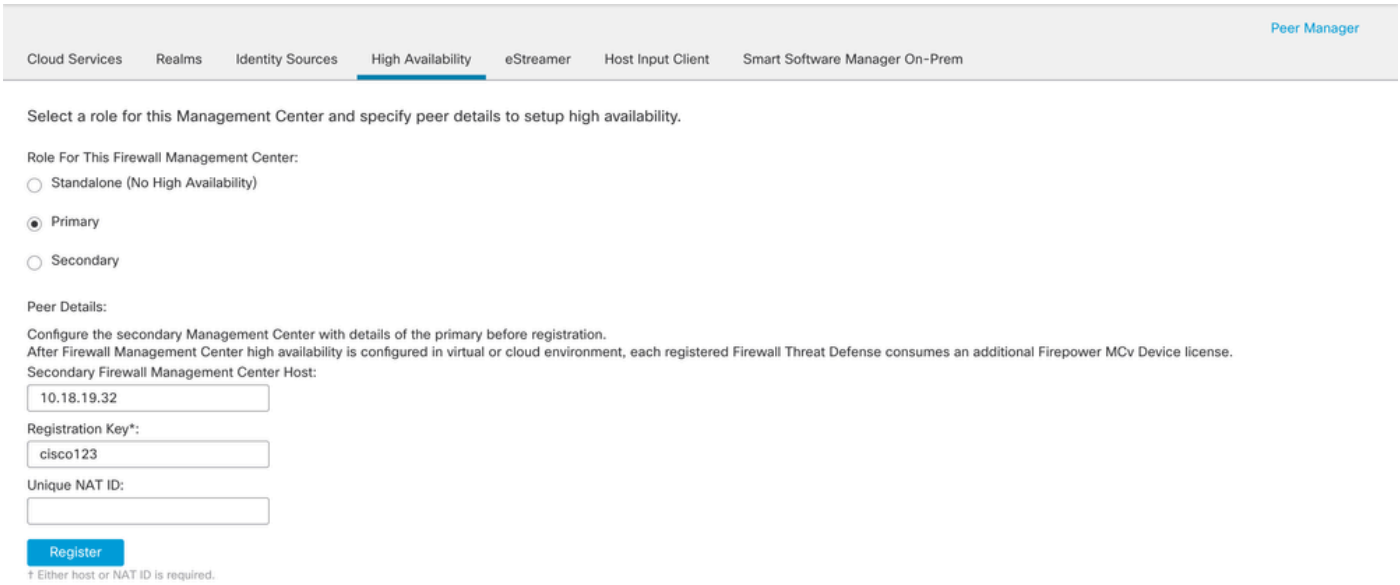
Configura FMC primario

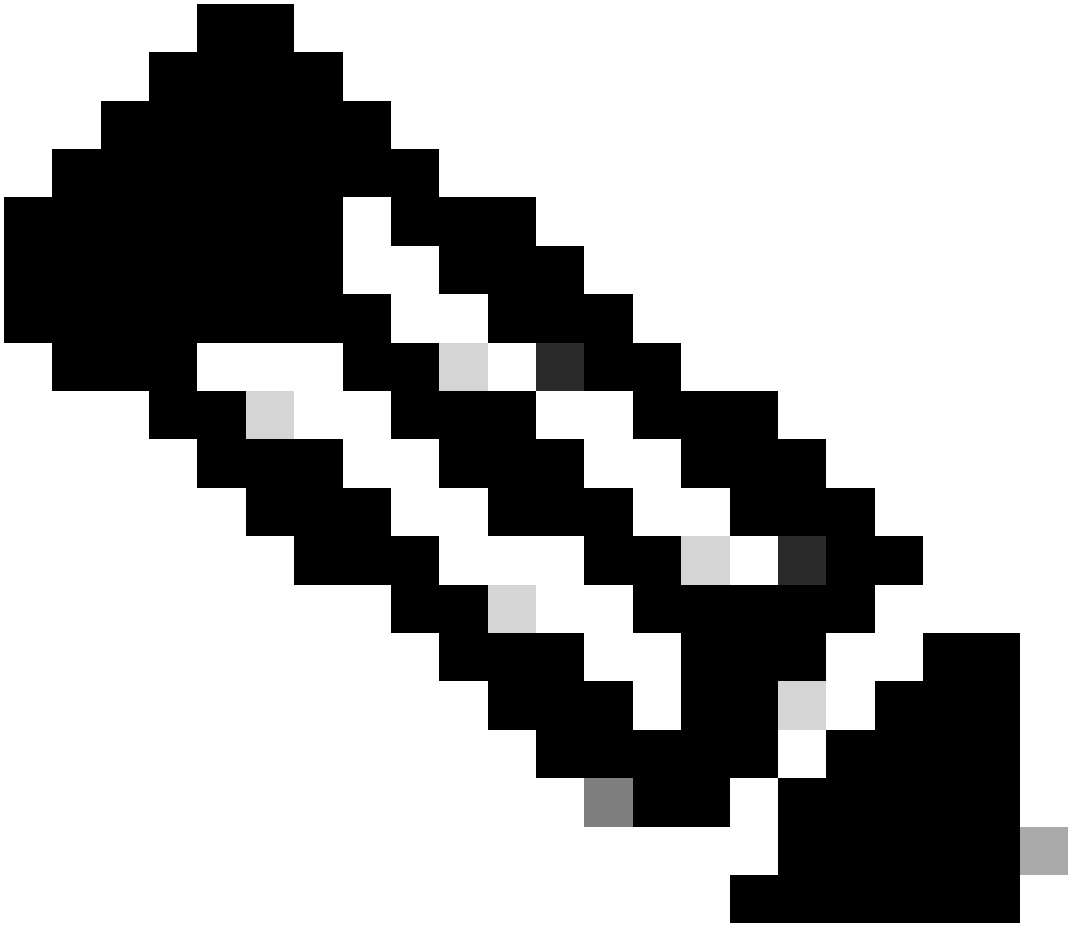
Ripetere i passaggi da 1 a 4 sul CCP primario/attivo.

Passaggio 5. Fare clic su Principale.



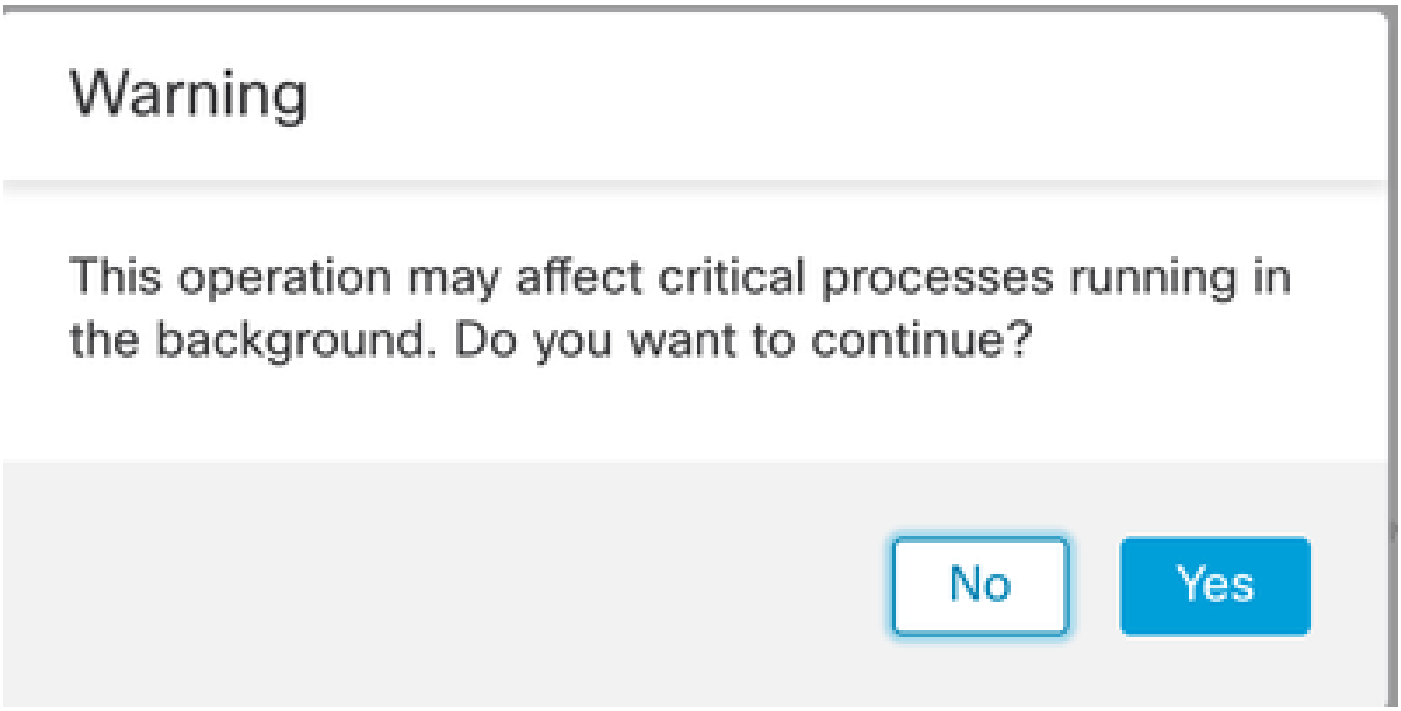
Passaggio 6. Immettere le informazioni relative al CCP secondario e fare clic su Registra.

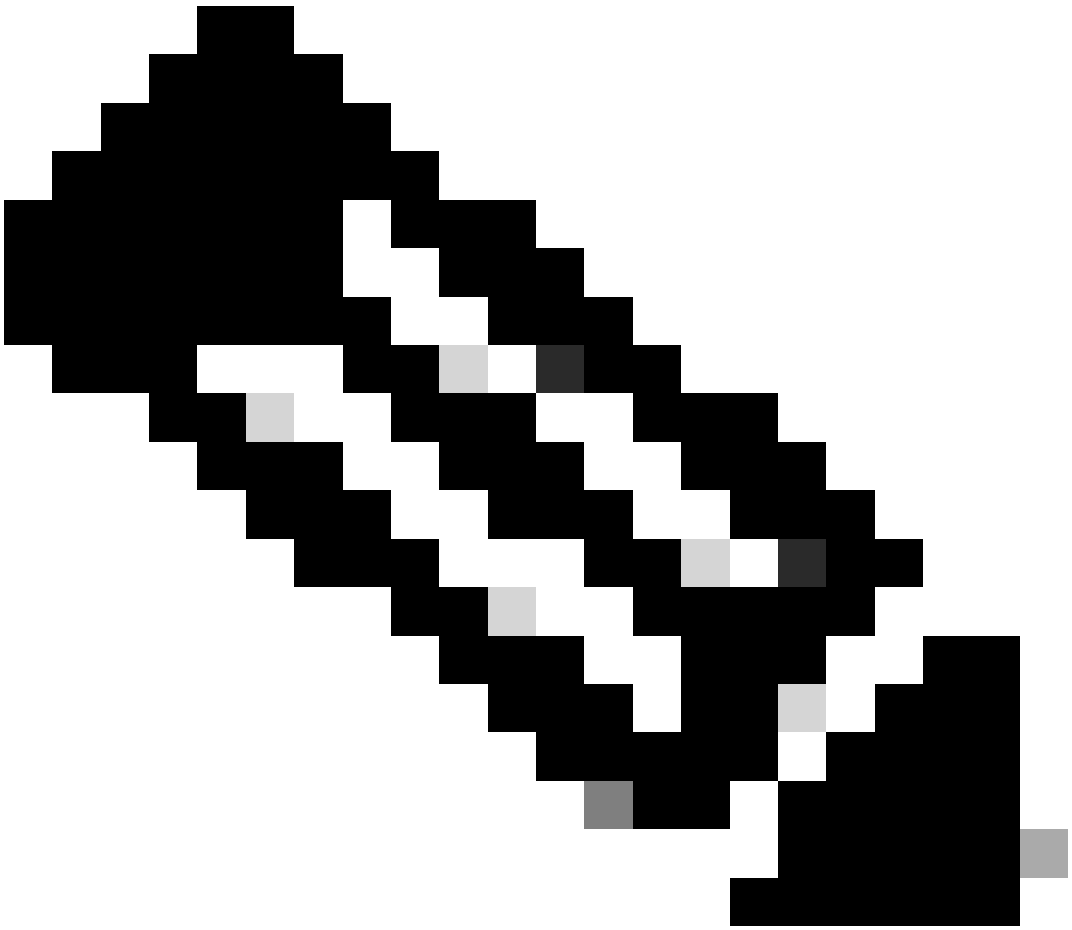




Nota: Utilizzare la stessa chiave di registrazione utilizzata come CCP secondario.

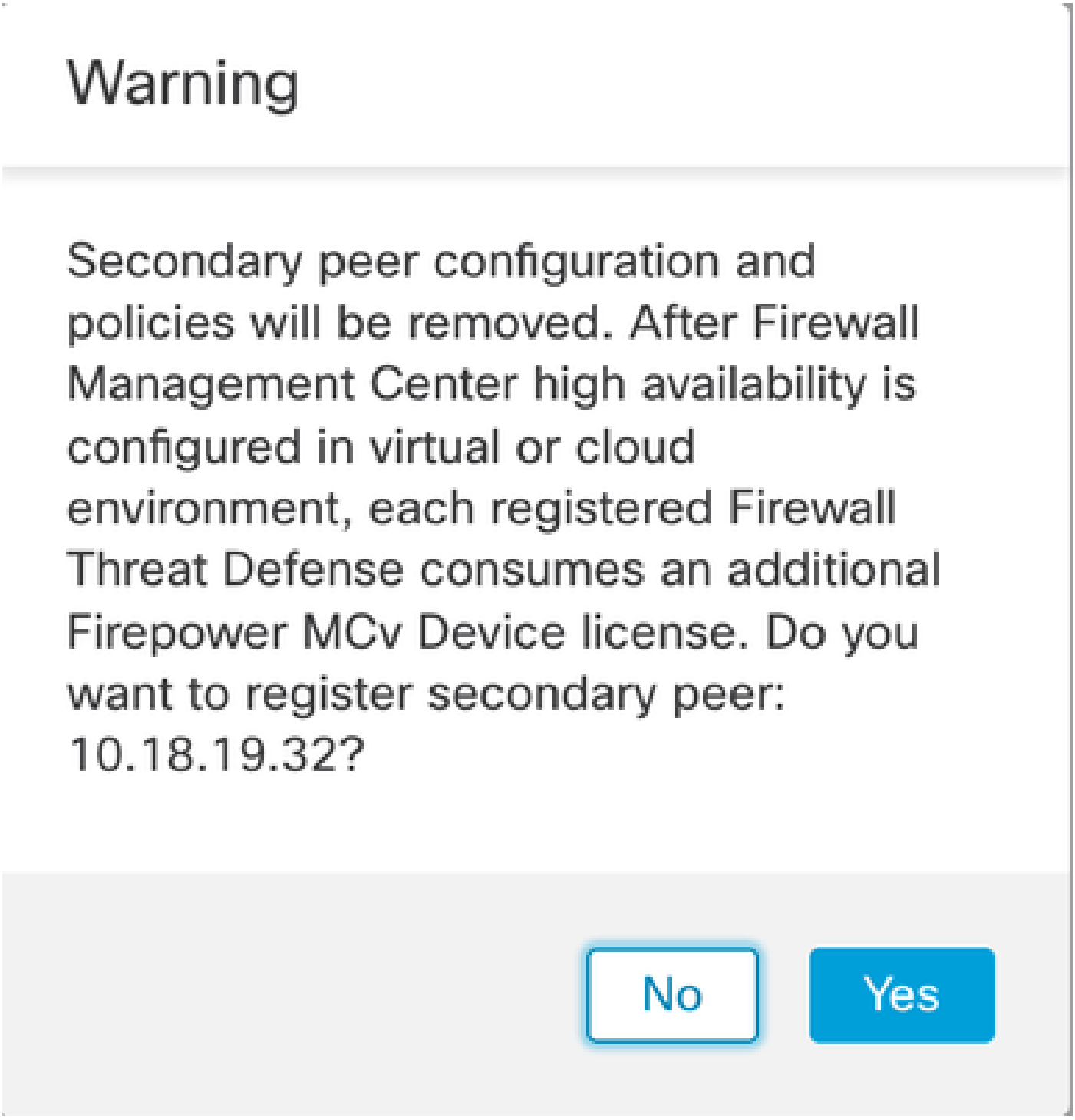
Passaggio 7. Questo avviso richiede di confermare, fare clic su **Yes**.

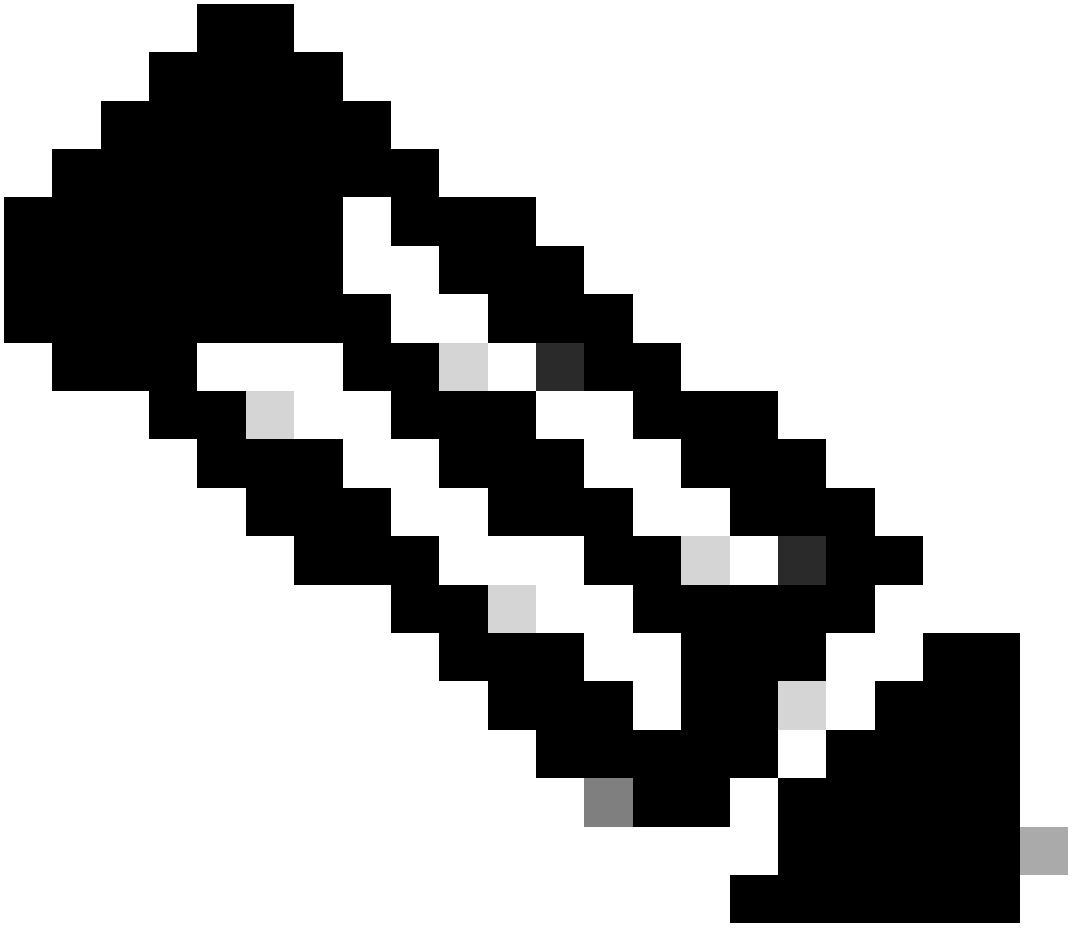

Warning
This operation may affect critical processes running in the background. Do you want to continue?
No
Yes



Nota: Verificare che non siano in esecuzione altre attività.

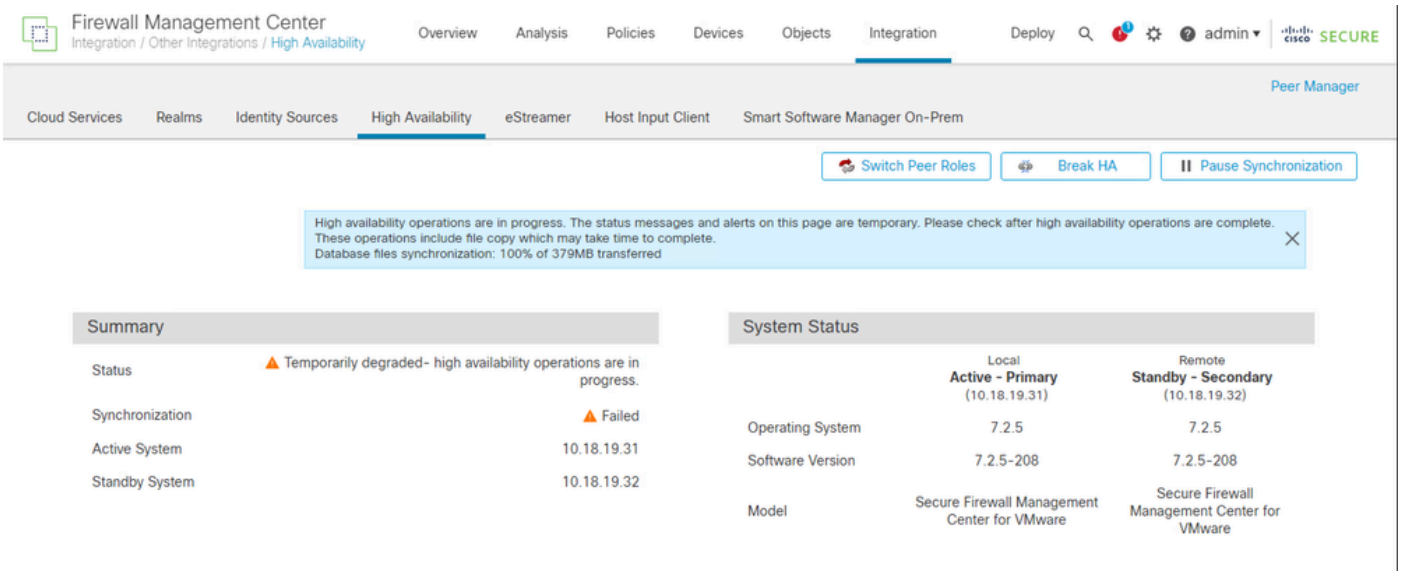
Passaggio 8. Confermare la registrazione per il CCP secondario.

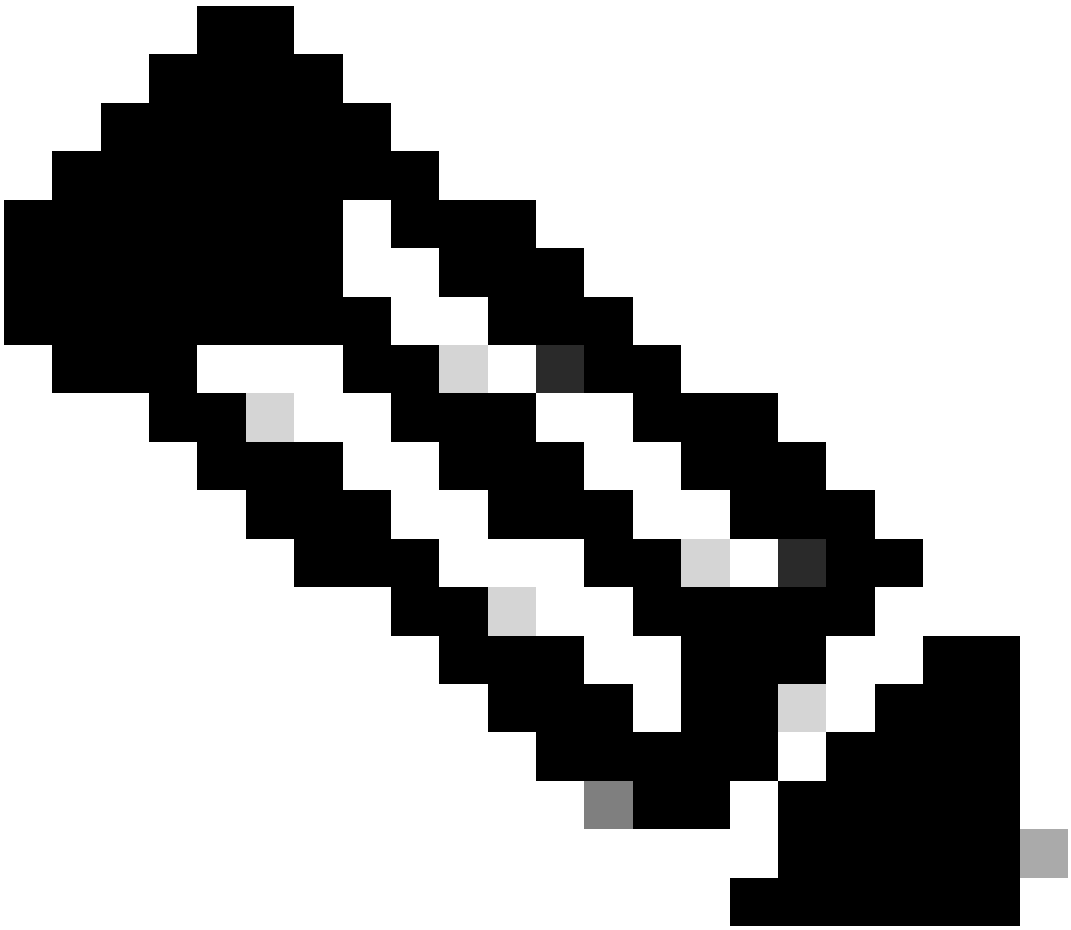




Nota: Accertarsi che il CCP secondario non contenga informazioni critiche, in quanto l'accettazione di questa richiesta comporta la rimozione di tutte le configurazioni dal CCP.

Sincronizzazione tra gli avvii primario e secondario; la durata dipende dalla configurazione e dai dispositivi. Questo processo può essere monitorato da entrambe le unità.

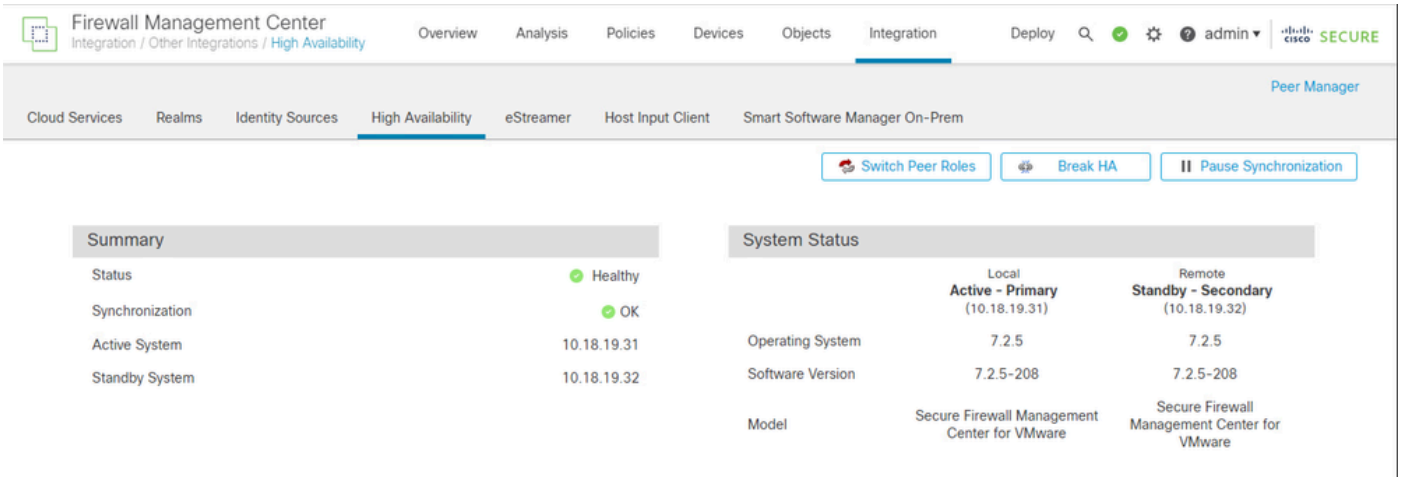




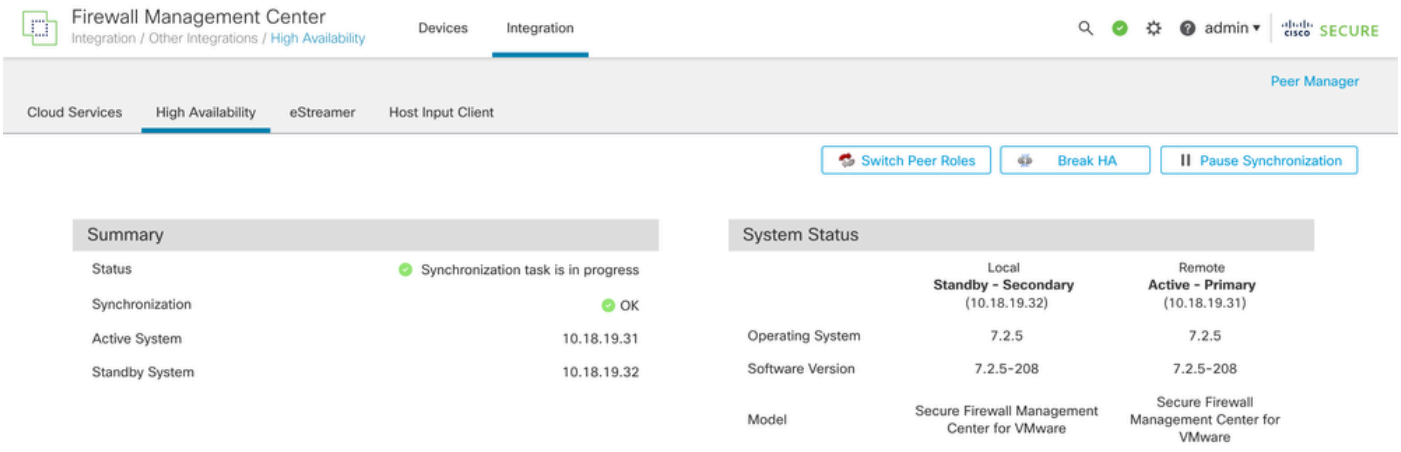
Nota: Durante la sincronizzazione, lo stato previsto sarà Non riuscito e Temporaneamente danneggiato. Questo stato viene visualizzato fino al completamento del processo.

Verifica

Una volta completata la sincronizzazione, l'output previsto sarà Stato integro e Sincronizzazione OK.



La sincronizzazione principale e secondaria continua; si tratta di un comportamento normale.



È importante verificare che i dispositivi siano visualizzati correttamente sia sul dispositivo principale che su quello secondario.

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).