Aggiornamento di Secure Firewall Threat Defense Fusing Firewall Device Manager

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Operazioni preliminari](#)
[Configurazione](#)
[Convalida](#)

Introduzione

Questo documento descrive un esempio di aggiornamento di Cisco Secure Firewall Threat Defense (FTD) con Firewall Device Manager (FDM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Nessun requisito specifico previsto per questa guida

Componenti usati

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

- Cisco Firepower 4125 con FTD versione 7.2.3

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:

- Connettività all'IP di gestione dell'FTD
- Il pacchetto di aggiornamento FTD (**.REL.tar**) precedentemente scaricato dal portale Cisco del software

Questa procedura di aggiornamento è supportata sugli accessori:

- Qualsiasi modello Cisco Firepower con software FTD configurato con gestione locale.

Operazioni preliminari

1. Creare e scaricare un backup delle configurazioni FTD.
2. Convalidare il percorso di aggiornamento per la versione di destinazione.
3. Scaricare il pacchetto di aggiornamento da Cisco Software Central.

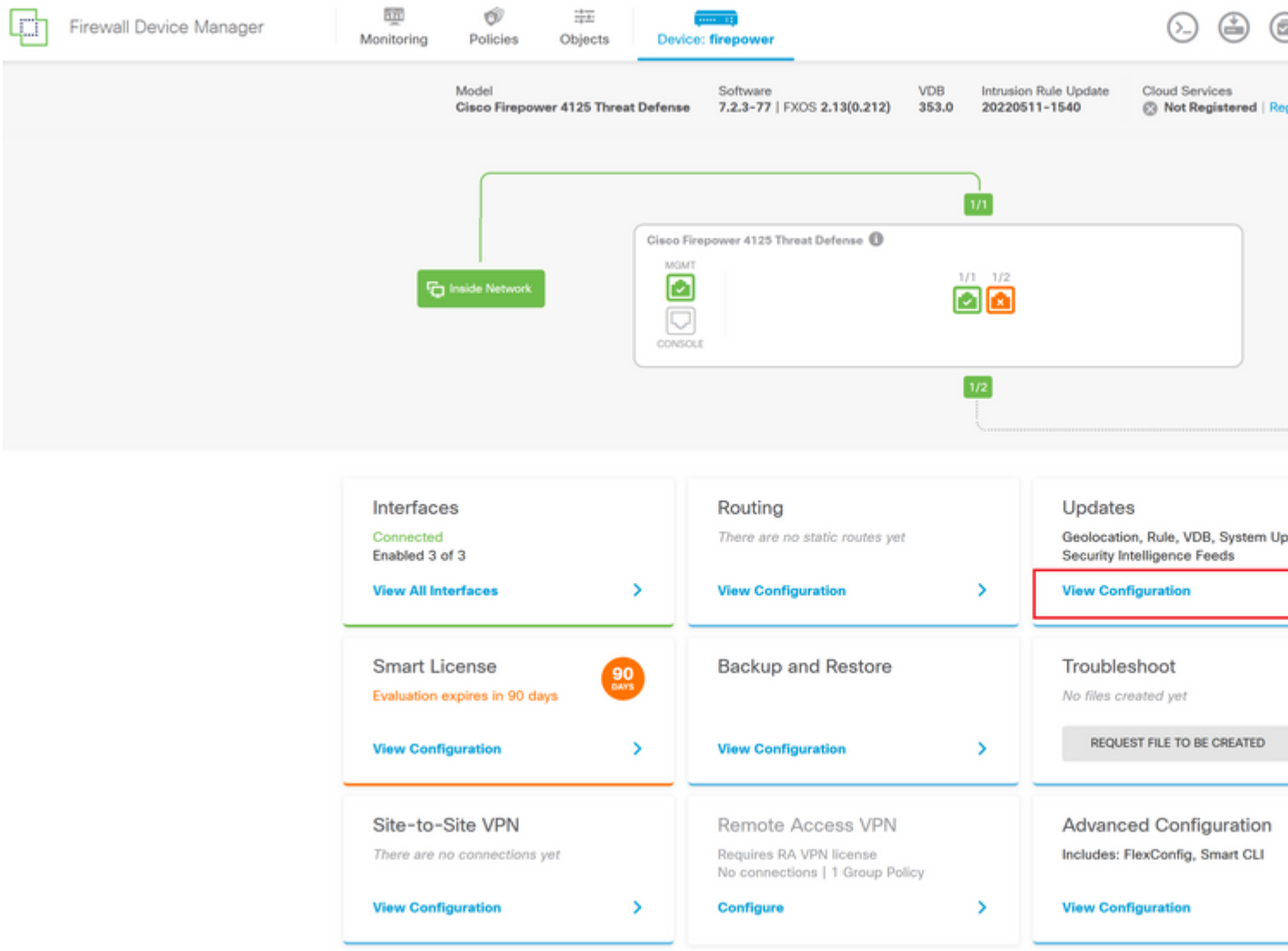
4. Non rinominare il file di aggiornamento. Il sistema considera i file rinominati non validi.

5. Pianificare una finestra di manutenzione per la procedura di aggiornamento in quanto il traffico è interessato.

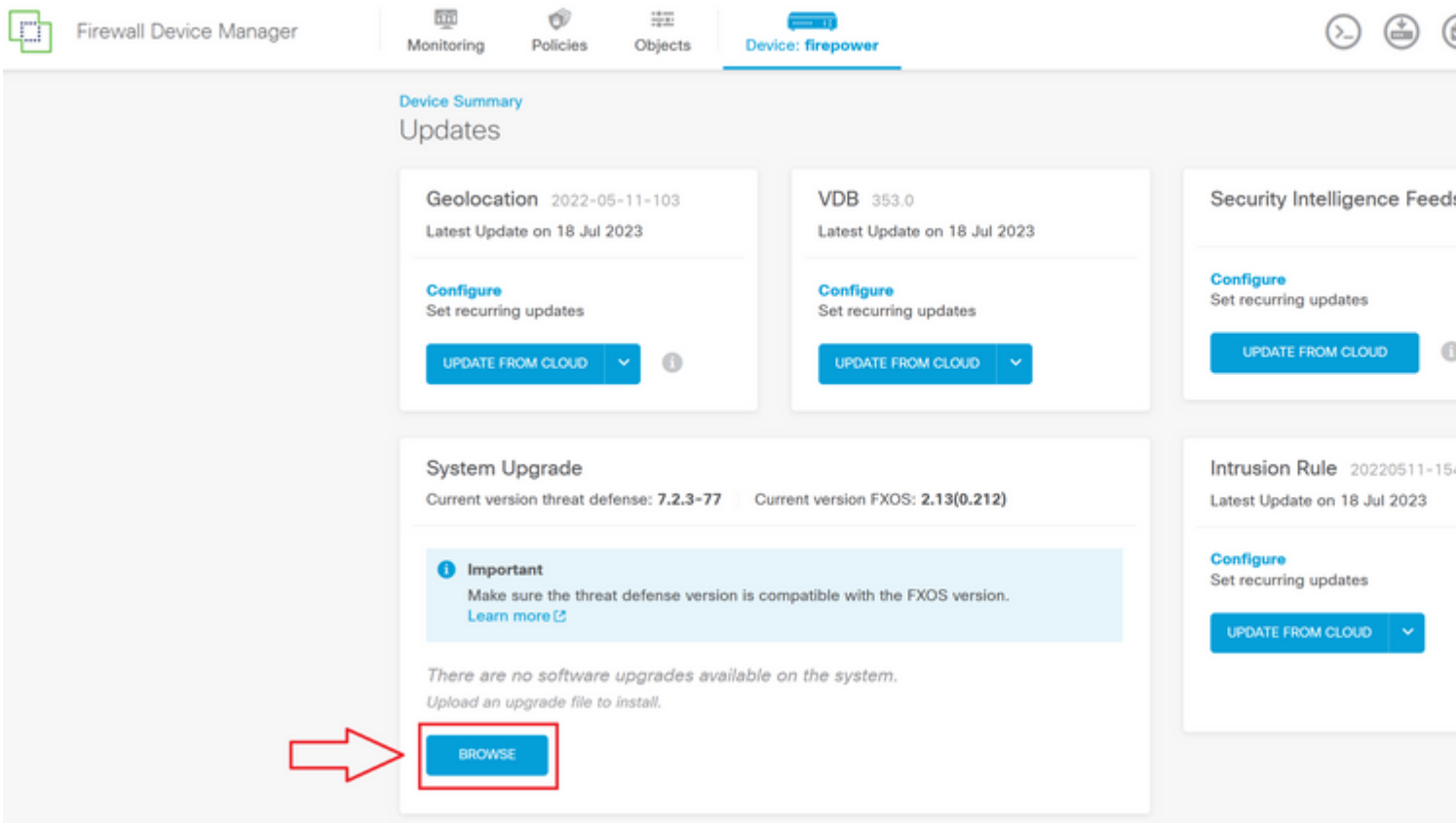
Configurazione

Passaggio 1. Accedere a Gestione periferiche firewall utilizzando l'IP di gestione dell'FTD:

Passaggio 2. Fare clic su View Configuration (Visualizza configurazione) nel dashboard di Gestione periferiche firewall:

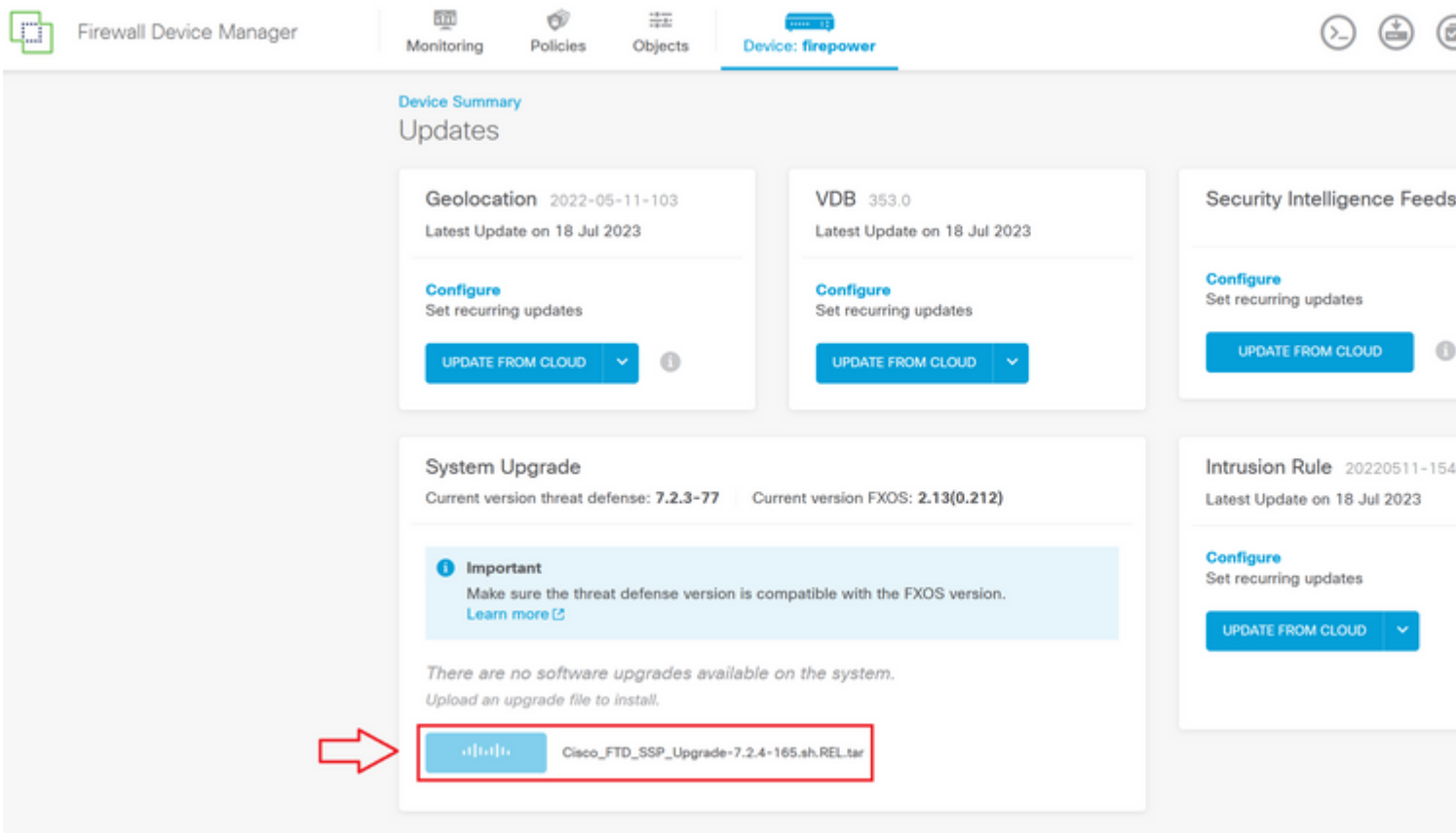


Passaggio 3. Fare clic sul pulsante Browse (Sfoglia) nella sezione System Upgrade (Aggiornamento del sistema) per caricare il pacchetto di installazione:

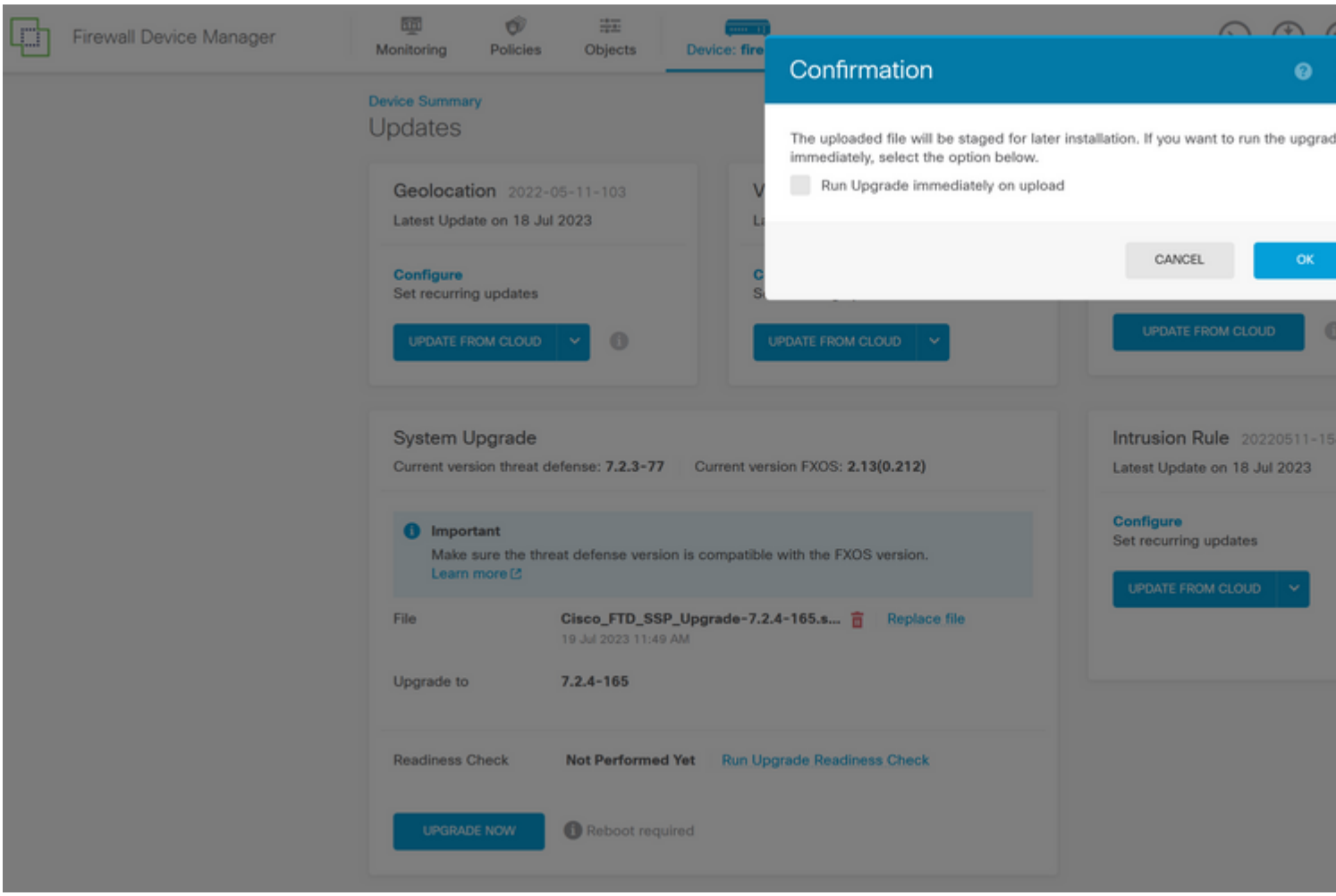


Attenzione: una volta caricato il pacchetto di aggiornamento, **BROWSE** visualizzerà un'animazione mentre il file è ancora in fase di caricamento. Non aggiornare la pagina Web fino al termine del caricamento.

Esempio di pagina di avanzamento del caricamento:

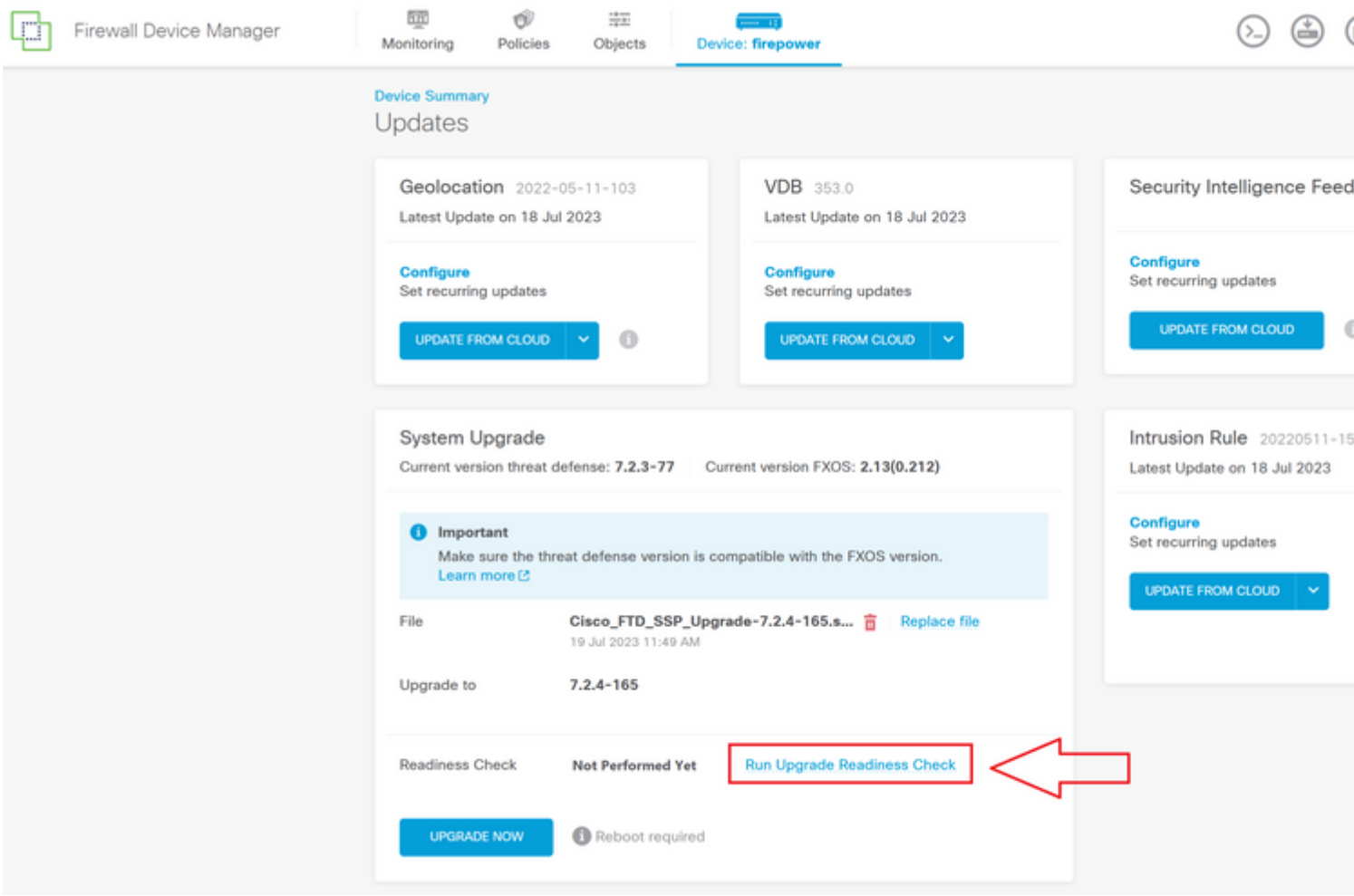


Passaggio 4. Al termine del caricamento, viene visualizzata una finestra popup che richiede di confermare:



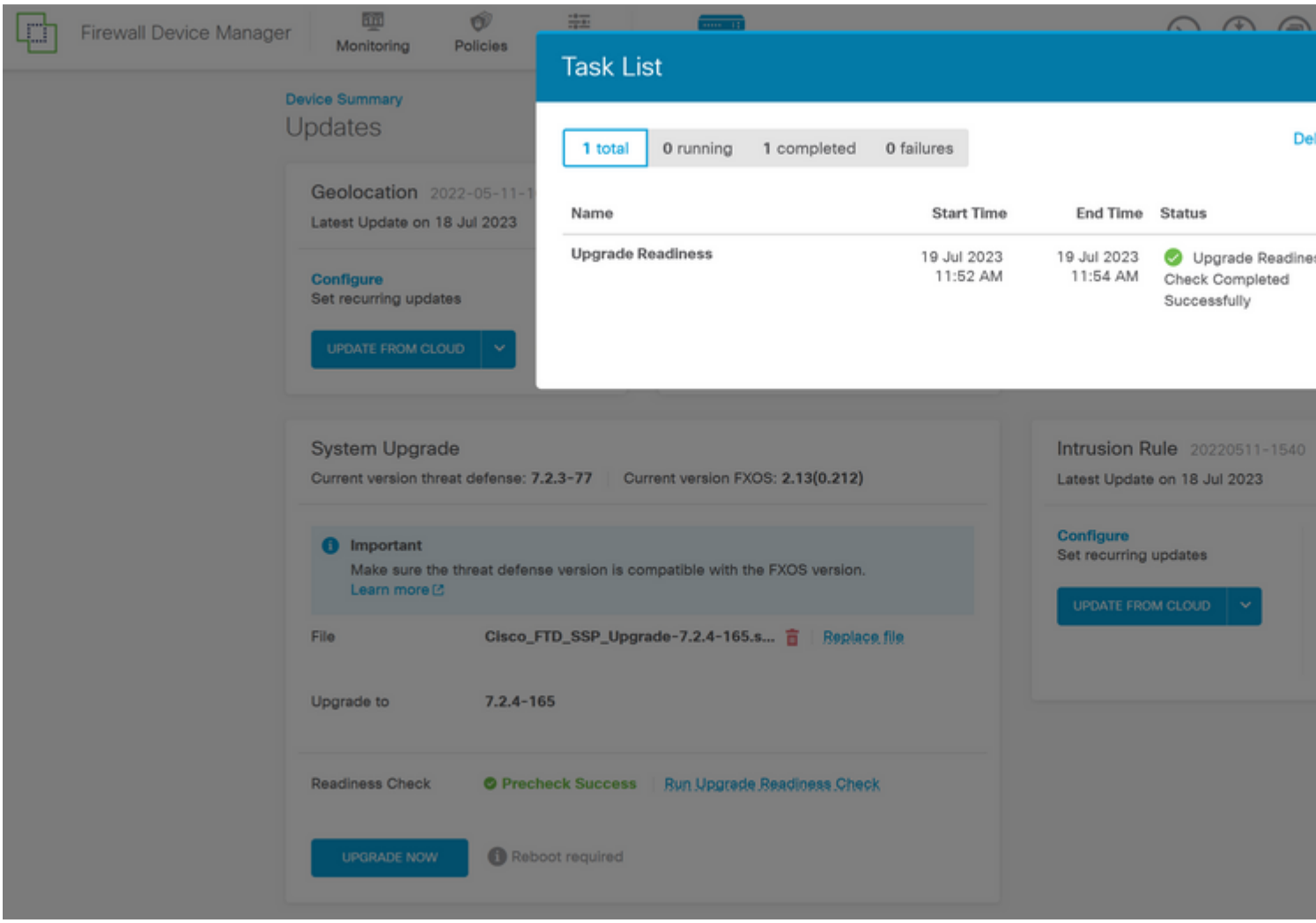
Nota: è possibile selezionare l'opzione **Esegui aggiornamento immediatamente al caricamento** se si desidera procedere direttamente con l'aggiornamento. Tuttavia, questa opzione salterà il **Controllo preparazione** che può fornire informazioni dettagliate sui conflitti nell'aggiornamento che impediscono un errore.

Passaggio 5. Fare clic su Esegui controllo preparazione aggiornamento per eseguire una preconvalida dell'aggiornamento per evitare errori:

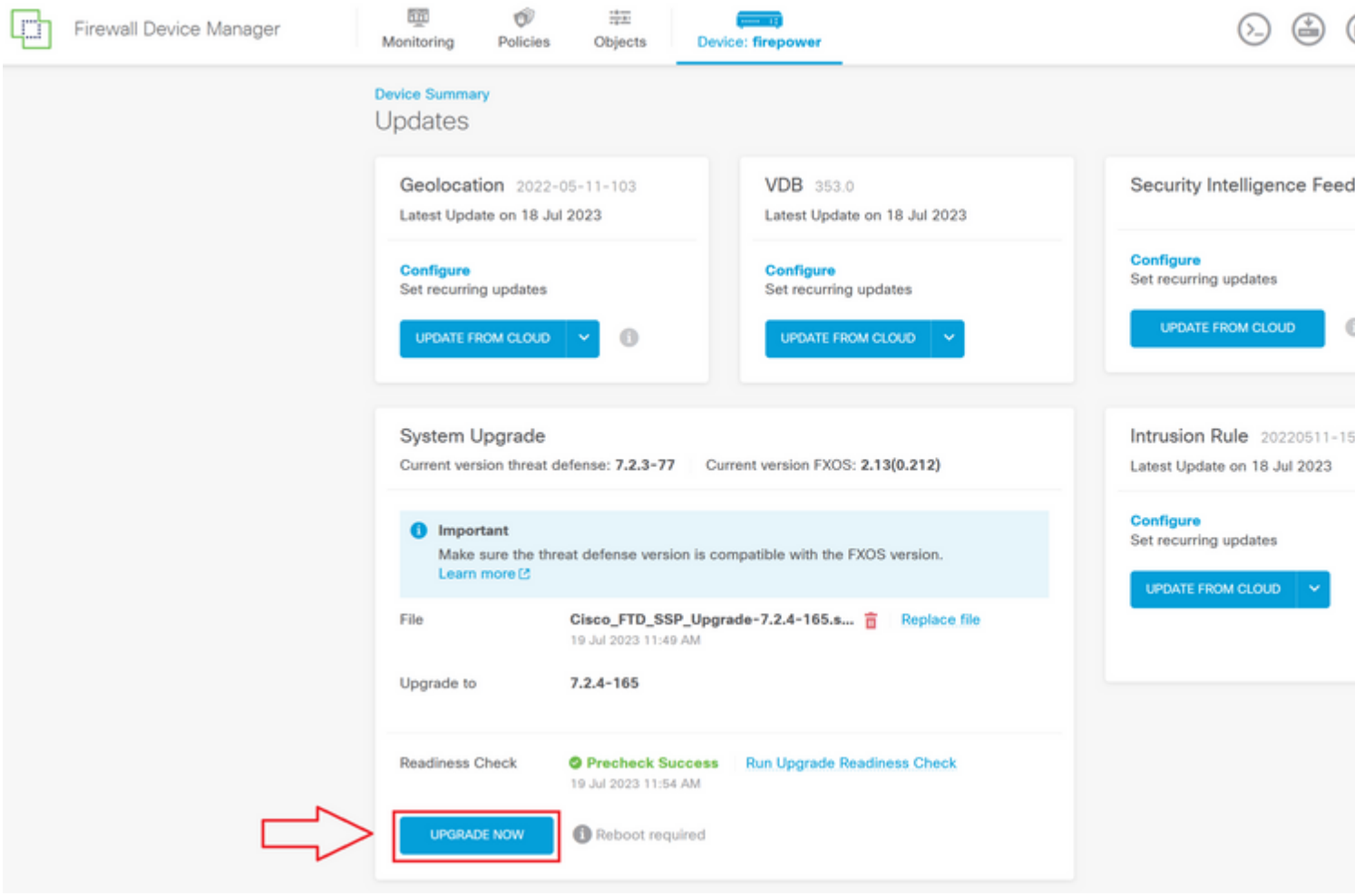


Nota: è possibile verificare che il controllo di idoneità sia stato completato correttamente dall'Elenco task.

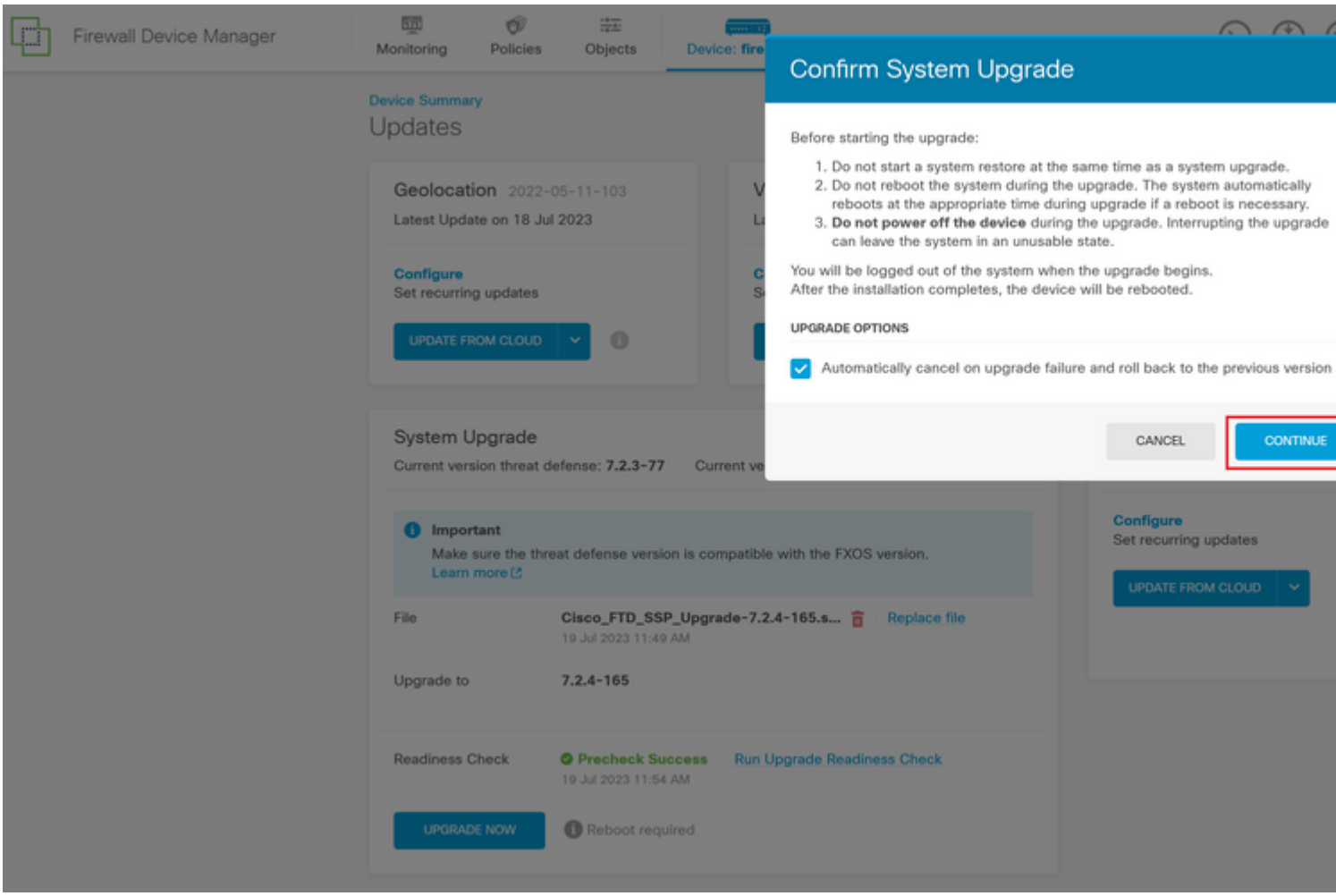
Esempio di verifica di fattibilità completata:



Passaggio 6. Fare clic sul pulsante UPGRADE NOW per procedere con l'aggiornamento del software:

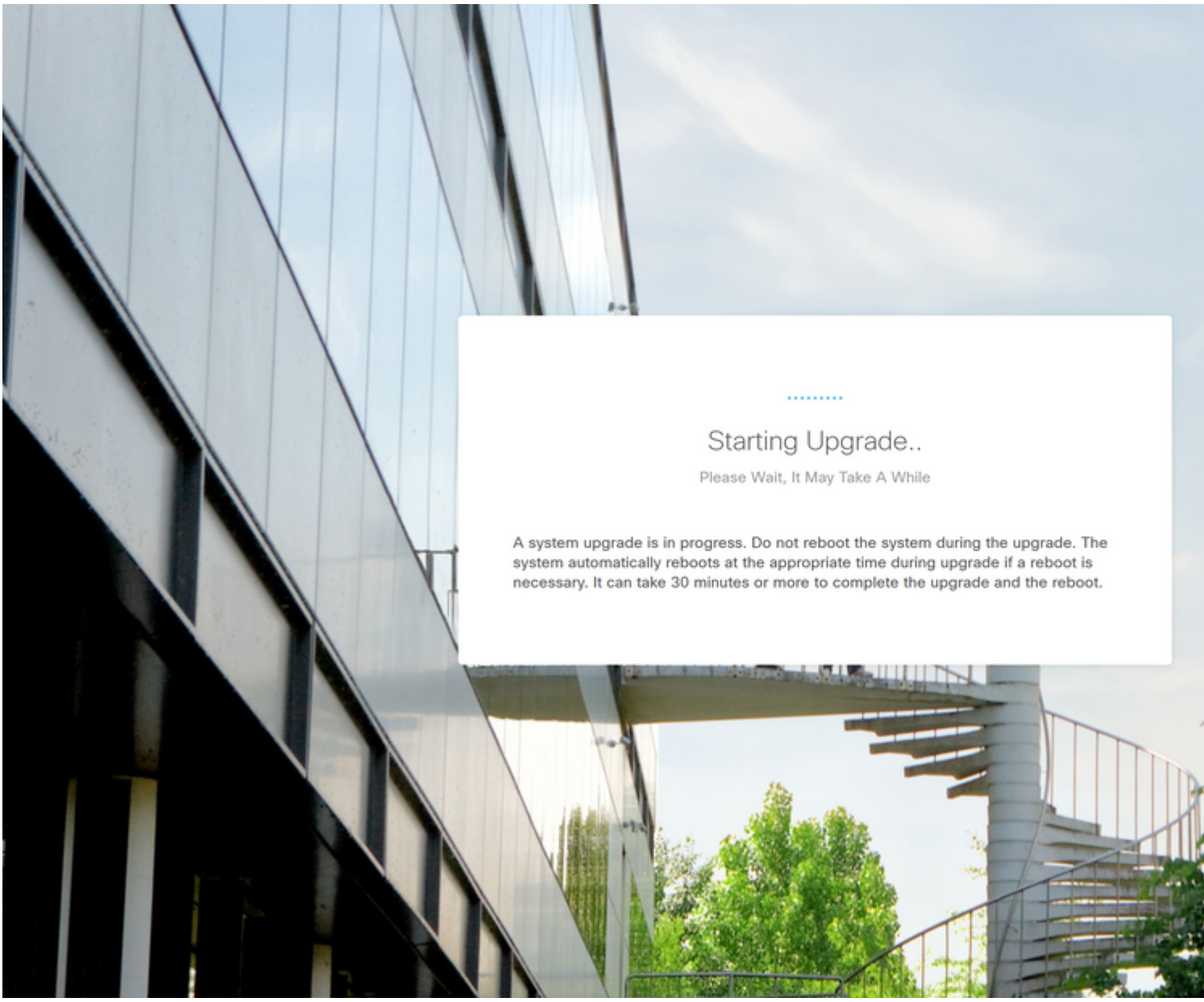


Passaggio 7. Nella finestra popup selezionare CONTINUE (CONTINUA) per procedere con l'aggiornamento:

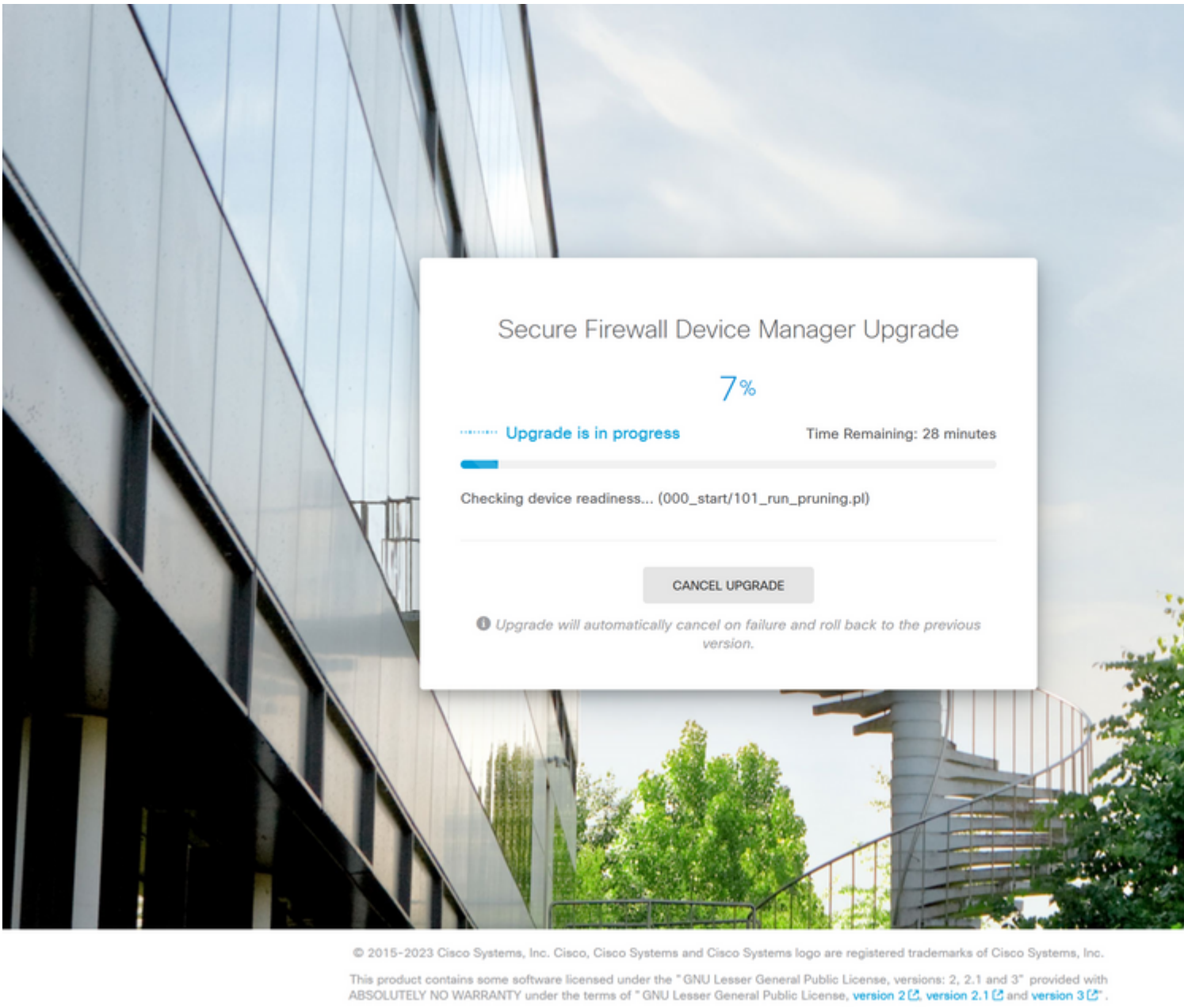


Nota: l'opzione di rollback è abilitata per impostazione predefinita. Si consiglia di mantenere questa opzione per ripristinare qualsiasi configurazione di aggiornamento in caso di problemi durante l'aggiornamento.

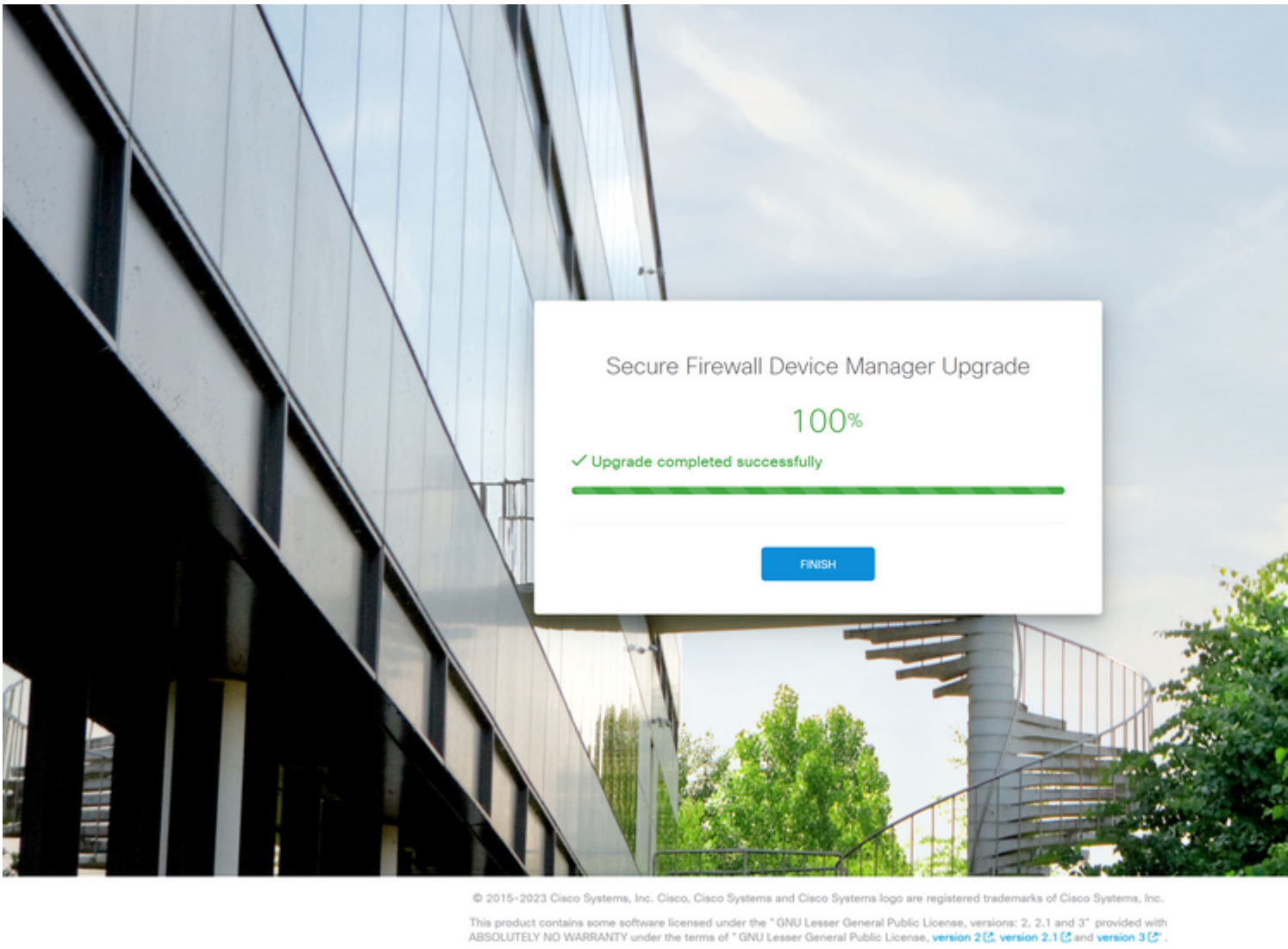
Passaggio 8. Viene visualizzata una pagina in cui verrà visualizzato lo stato dell'aggiornamento:



Esempio di pagina di avanzamento:

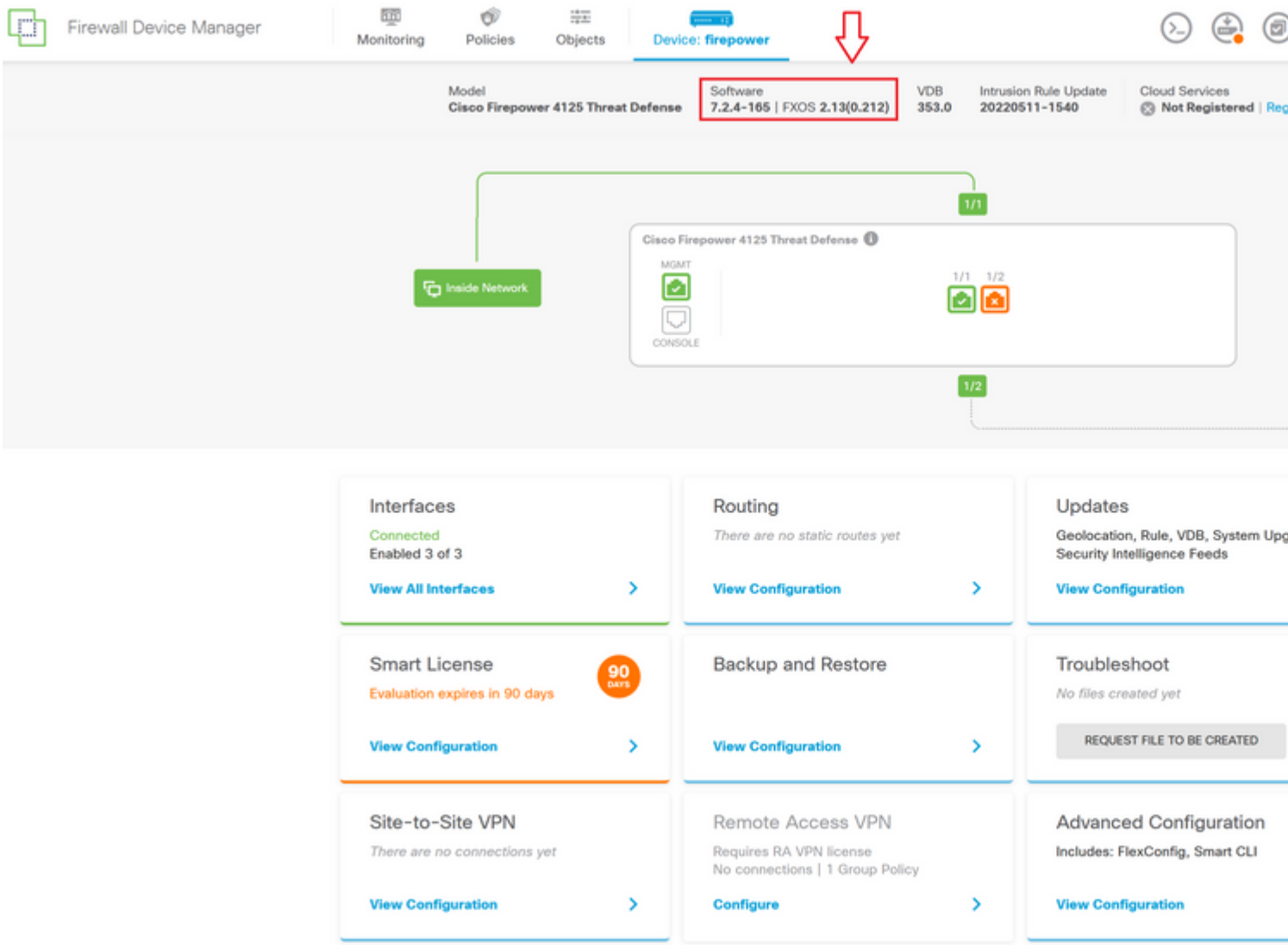


Passaggio 9. Fare clic sul pulsante FINISH al termine dell'aggiornamento per tornare alla schermata di accesso:



Convalida

Al termine dell'aggiornamento, è possibile accedere a Gestione periferiche di Firepower per convalidare la versione corrente, che viene visualizzata nel dashboard Panoramica:



Per eseguire una convalida di aggiornamento tramite CLI, è possibile utilizzare i seguenti passaggi:

I. Creare una sessione SSH usando l'IP di gestione dell'FTD.

II. Usare il comando **show version** per convalidare la versione corrente sullo chassis.

Esempio della procedura suggerita:

```
Copyright 2004-2023, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 499)
Cisco Firepower 4125 Threat Defense v7.2.4 (build 165)

> show version
-------------------[ firepower ]---------------------
Model                     : Cisco Firepower 4125 Threat Defense (76) Ve
UUID                      : e55a326e-25cd-11ee-b261-8d0ffe6dde59
LSP version               : lsp-rel-20220511-1540
VDB version               : 353
-----------------------------------------------------

>
```

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).