Recupera password dispositivo logico da Gestione chassis

Sommario

Introduzione

Questo documento descrive come recuperare la password di una periferica logica da Secure Firewall Chassis Manager (FCM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Sistema operativo FXOS (Secure Firewall eXtensible Operating System)
- Cisco Adaptive Secure Appliance (ASA)
- Secure Firewall Threat Defense (FTD)

Componenti usati

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

- Dispositivi Secure Firewall 4100/9300.
- Dispositivo logico, ASA o FTD, già creato e in stato online.

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

La password di un dispositivo logico viene configurata al momento della creazione e può essere modificata anche dopo la distribuzione della configurazione bootstrap dalla CLI.

Procedura

In questa procedura viene descritto come modificare la password dall'interfaccia utente di Chassis Manager dopo la creazione di una periferica logica. Ciò si applica alle periferiche logiche ASA e FTD.

Avviso: la procedura per il recupero della password sovrascrive la configurazione del bootstrap da FCM. Ciò significa che vengono ripristinate anche tutte le modifiche all'IP di gestione eseguite dalla CLI del dispositivo logico dopo la creazione del dispositivo.

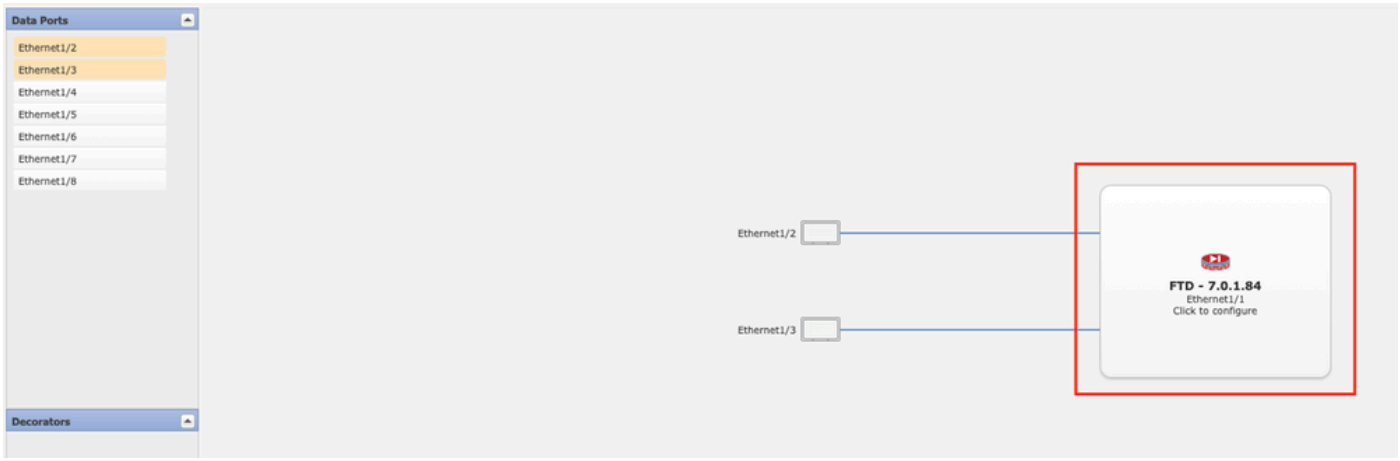
Configurazioni

1. Accedere a Secure Firewall Chassis Manager.

2. Per modificare la password della periferica logica, selezionare Periferica logica > Modifica.

Menu Periferica logica

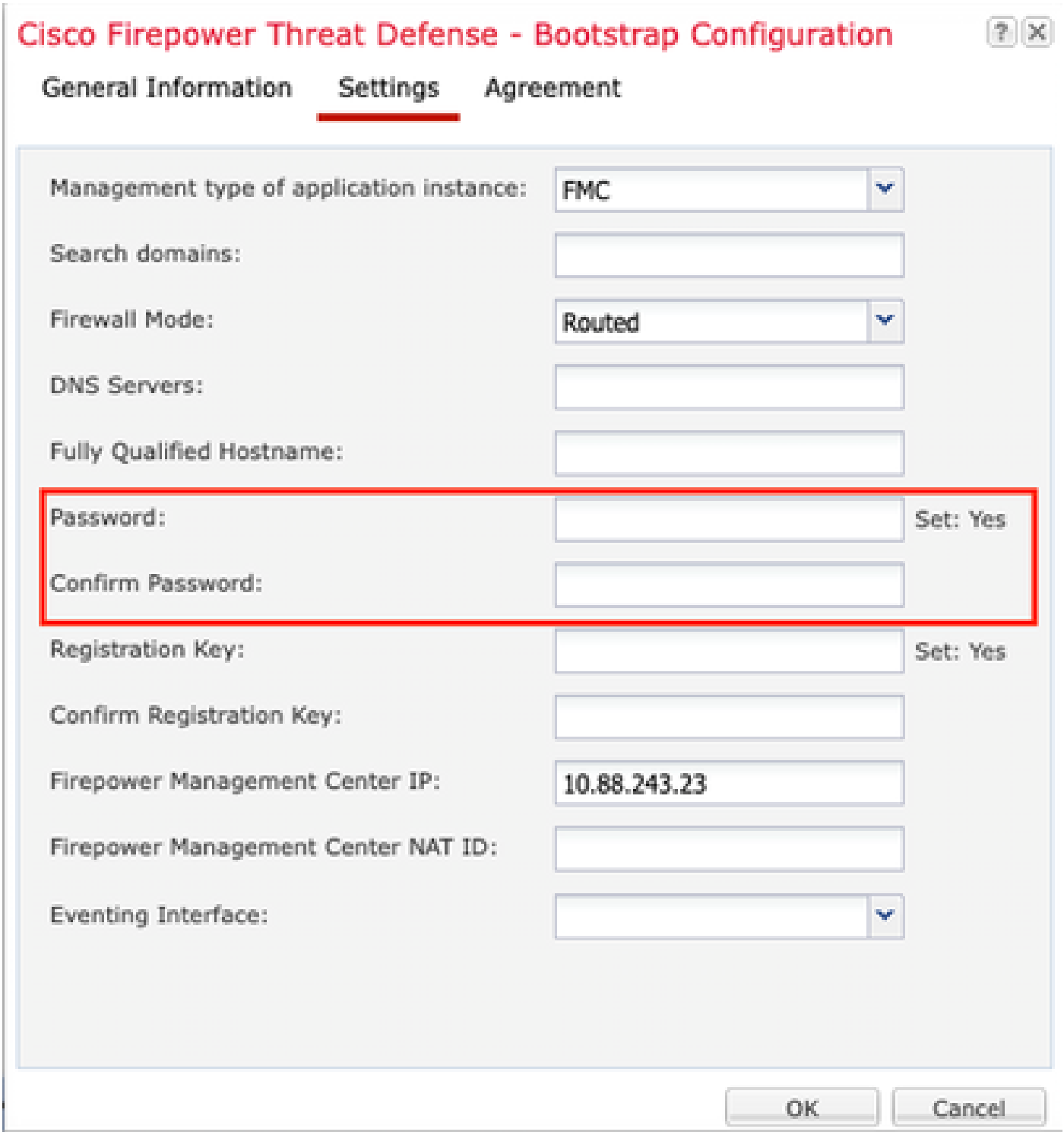
3. Accedere alla configurazione del bootstrap facendo clic sul pulsante del dispositivo.



Configurazione bootstrap

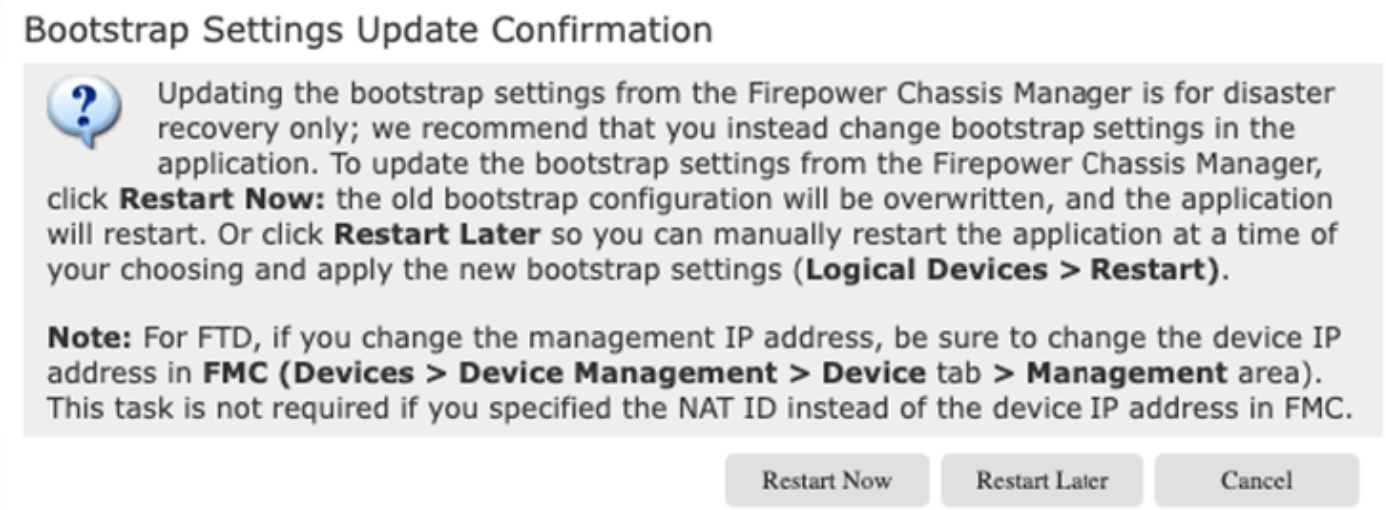
4. Fare clic su Settings (Impostazioni). La password è già impostata. Immettere la nuova password e confermarla.

Questa azione consente di modificare la password, ma è necessario riavviare il computer per eseguire le modifiche.



Campo password

5. Quando si salvano le modifiche, viene visualizzato un messaggio di conferma. È possibile scegliere di riavviare il dispositivo ora o in seguito in Dispositivi logici > Riavvia.



Avviso salvataggio modifiche

6. Dopo il riavvio del dispositivo logico, è possibile eseguire il protocollo SSH sul dispositivo e accedere alla modalità Expert con le nuove credenziali.

Informazioni correlate

- Supporto tecnico Cisco e download

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).