Distribuire il modulo di sicurezza in roaming AnyConnect Umbrella con FMC

Sommario

Introduzione

In questo documento viene descritto come distribuire il modulo di sicurezza AnyConnect Umbrella Roaming utilizzando Cisco Firewall Management Console (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso a Cisco Umbrella Dashboard
- Accedere a Cisco Firewall Management Console (FMC) versione 6.7 o successive, perché questa versione aggiunge il supporto per altri moduli AnyConnect. Per le versioni precedenti alla 6.7, FlexConfig può essere utilizzato per distribuire il modulo. Per ulteriori informazioni, consultare la documentazione di Cisco.
- Profilo del modulo AnyConnect Umbrella (orginfo.json)
- La configurazione della VPN AnyConnect è già completa e funzionante sul FMC/FTD

Componenti usati

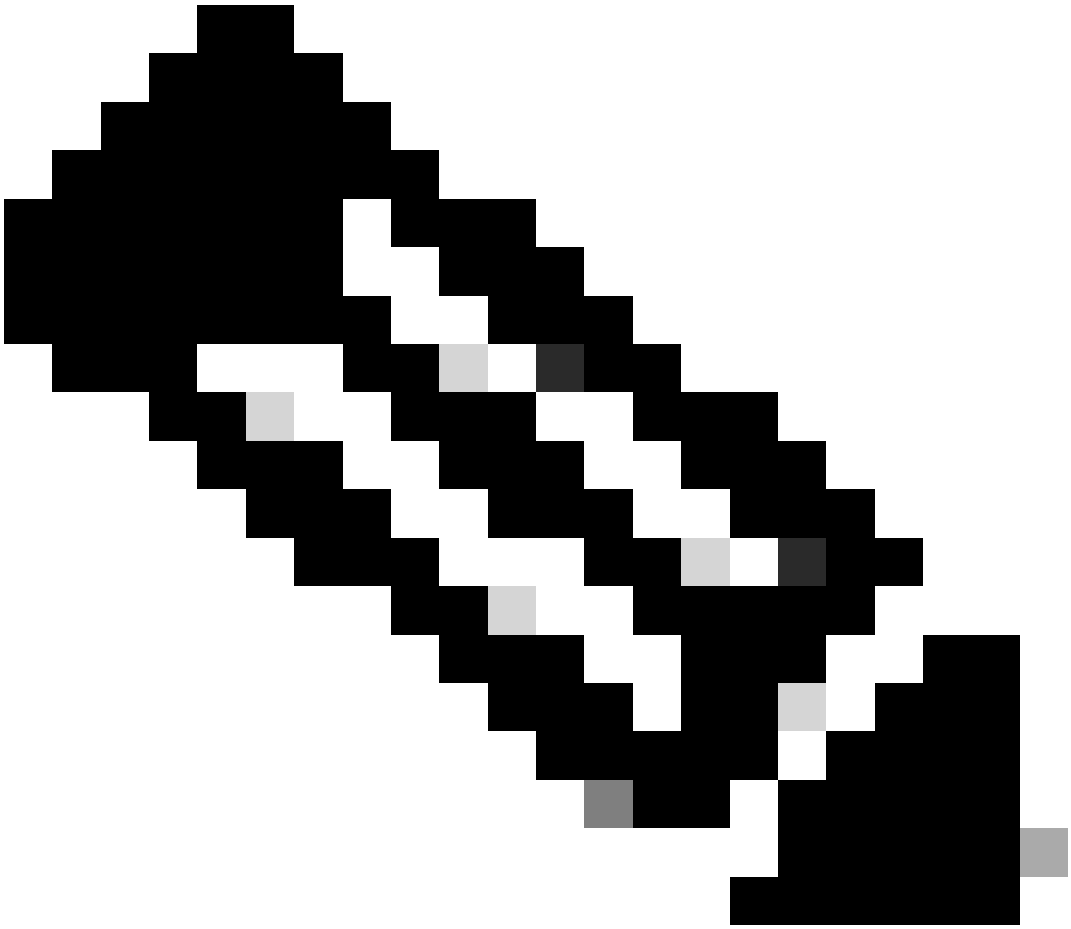
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AnyConnect Umbrella Roaming Security Module
- Cisco Firewall Management Console (FMC) per le versioni 6.7 o successive

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.

Panoramica



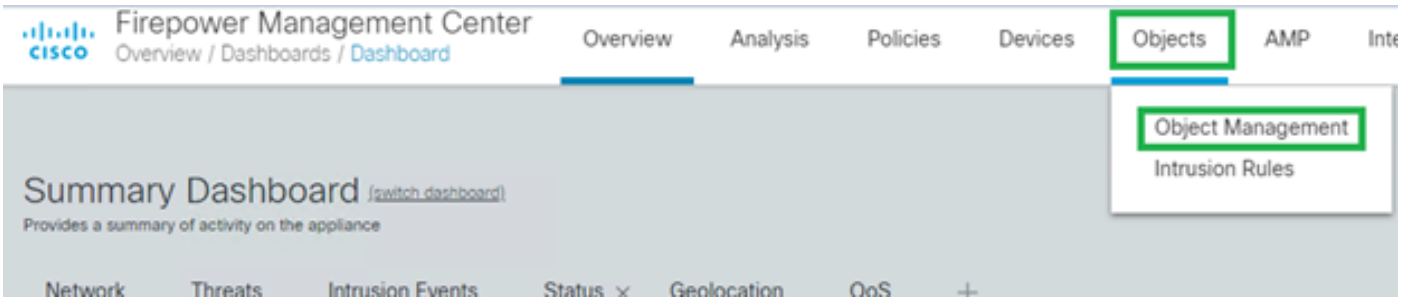
> Nota: Cisco ha annunciato il termine del ciclo di vita di Cisco AnyConnect nel 2023. Cisco ha annunciato la fine del ciclo di vita per Umbrella Roaming Client il 2 aprile 2024, e l'ultima data di supporto è il 2 aprile 2025. Molti clienti Cisco Umbrella stanno già beneficiando della migrazione a Cisco Secure Client e si è incoraggiati ad avviare la migrazione il prima possibile per ottenere un'esperienza di roaming migliore. Ulteriori informazioni in questo articolo della Knowledge Base: Come installare Cisco Secure Client con il modulo Umbrella?

La presente guida alla configurazione descrive la procedura per effettuare il provisioning del modulo di sicurezza AnyConnect Umbrella Roaming tramite Cisco Firewall Management Console (FMC) per le versioni 6.7 o successive.

Installazione e download di AnyConnect Umbrella Module dal FMC:

Completare questa procedura per abilitare l'installazione/il download del modulo AnyConnect Umbrella dal FMC:

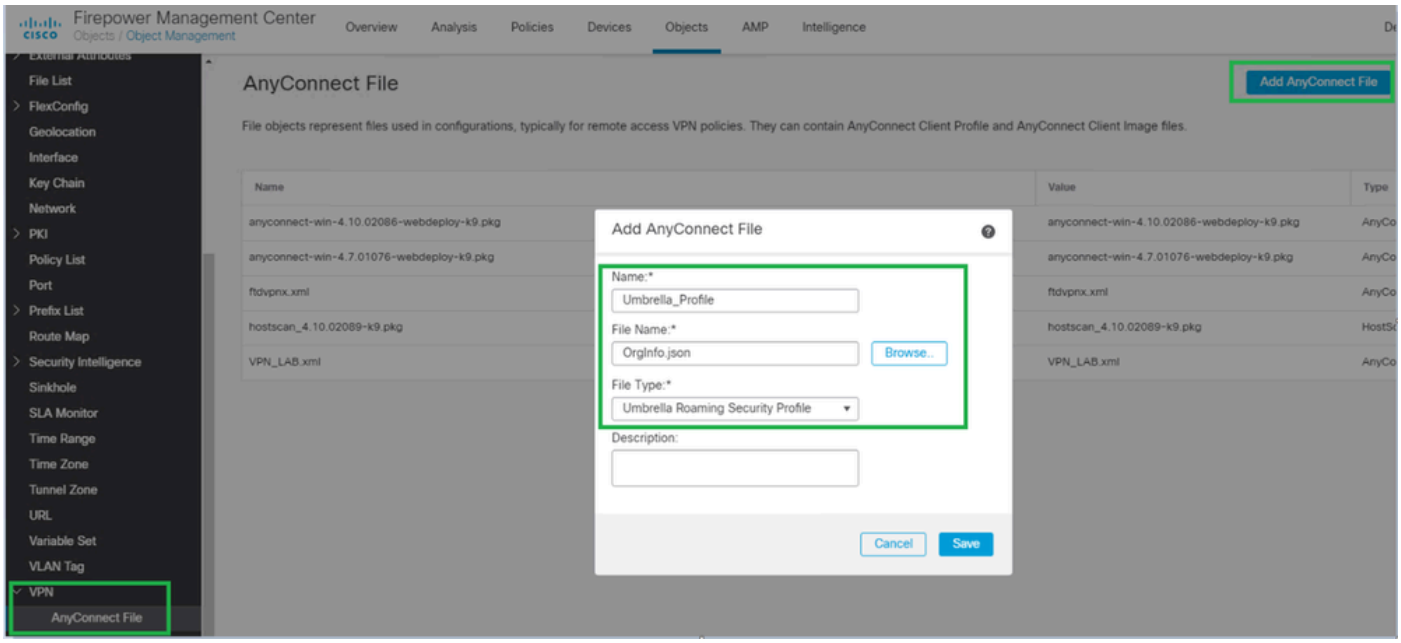
1. Selezionare Oggetti > Gestione oggetti:



8178144512532

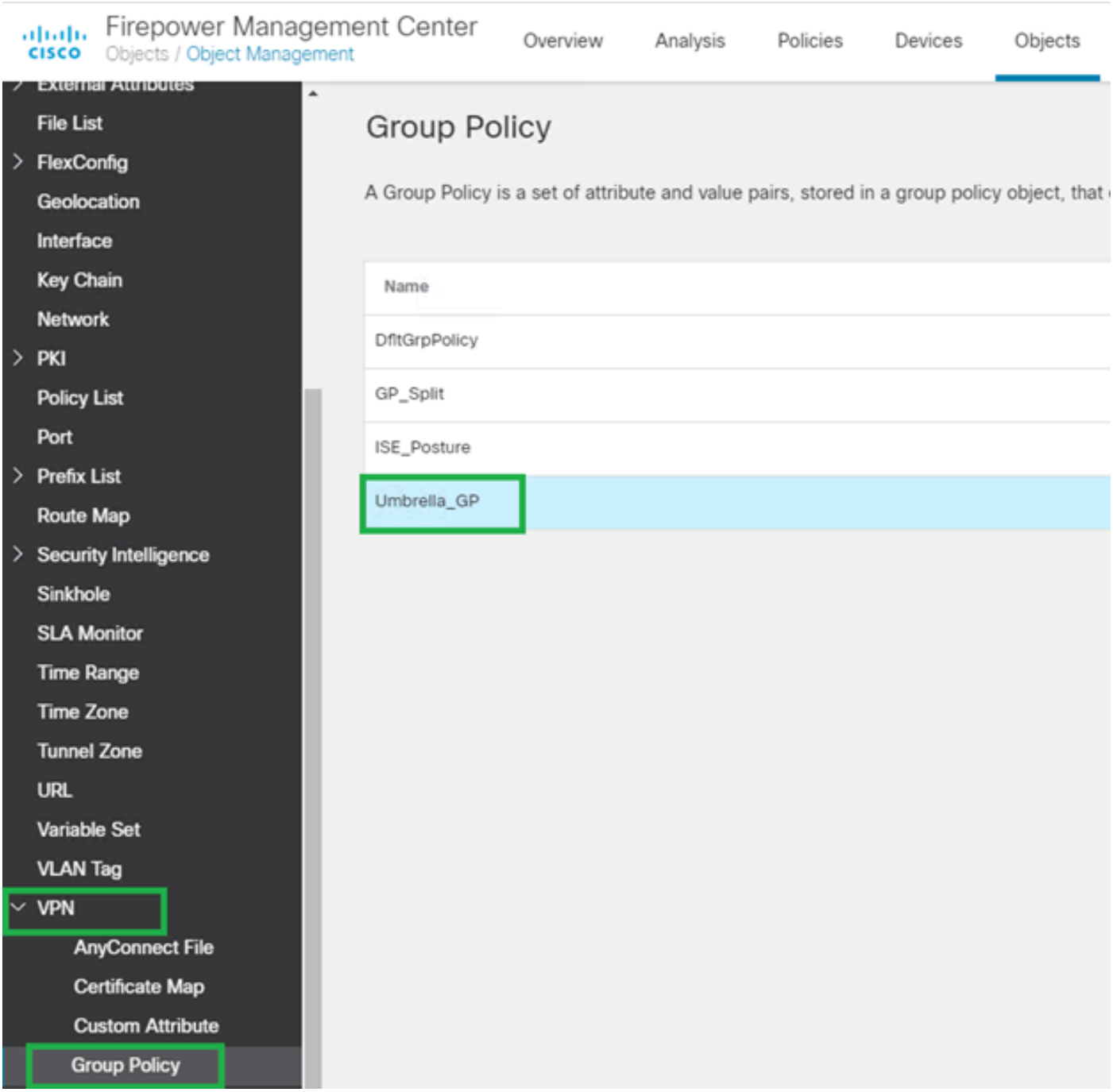
2. Selezionare VPN > AnyConnect File > Add AnyConnect File. Impostare un nome per il profilo (significativo a livello locale).

- Cerca il file JSON scaricato dal tuo dashboard Cisco Umbrella.
- In Tipo di file, selezionare Umbrella Roaming Security Profile e quindi Salva.



8178144531860

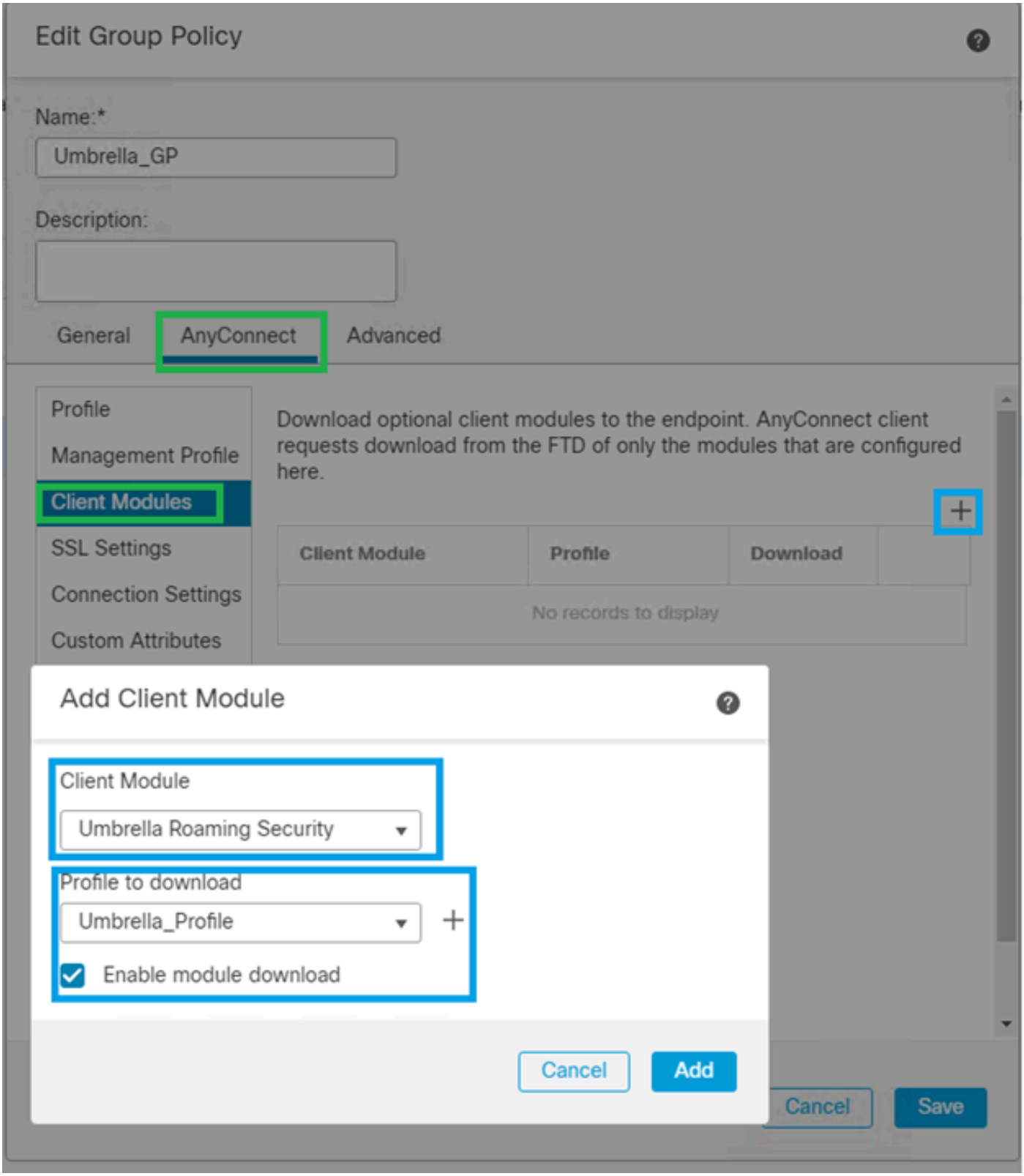
3. In seguito, selezionare Criteri di gruppo, quindi selezionare i Criteri di gruppo utilizzati per distribuire Umbrella ("Umbrella_GP" in questo caso):



8178147609492

4. Selezionare AnyConnect > Moduli client > Aggiungi modulo client.

- In Modulo client, selezionare Umbrella Roaming Client, quindi Profilo per scaricare il profilo definito al punto 2.
- Verificare che il download del modulo abilitato sia selezionato in modo che gli utenti che si connettono tramite AnyConnect possano scaricare automaticamente il profilo JSON di Umbrella.



8178147636628

Facoltativo: Autenticazione locale VPN (richiesto FMC 7.0 o versione successiva)

Se si desidera testare un profilo separato con l'autenticazione locale sul FMC/FTD, è possibile completare i seguenti passaggi (è richiesto FMC 7.0 o versione successiva):

1. Creare un realm locale.

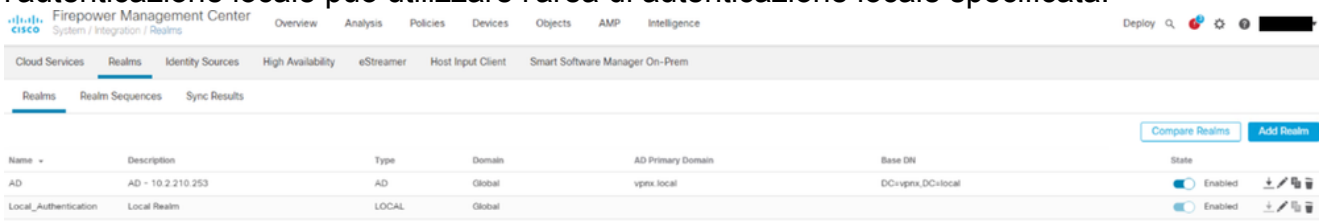
- I nomi utente e le password locali vengono archiviati nei realm locali.
- Quando create un realm (**Sistema > Integrazione > Realm**) e selezionate il nuovo tipo di realm **LOCALE**, il sistema chiede di aggiungere uno o più utenti locali.

2. Configurare la VPN per l'Autorità registrazione per l'utilizzo dell'autenticazione locale.

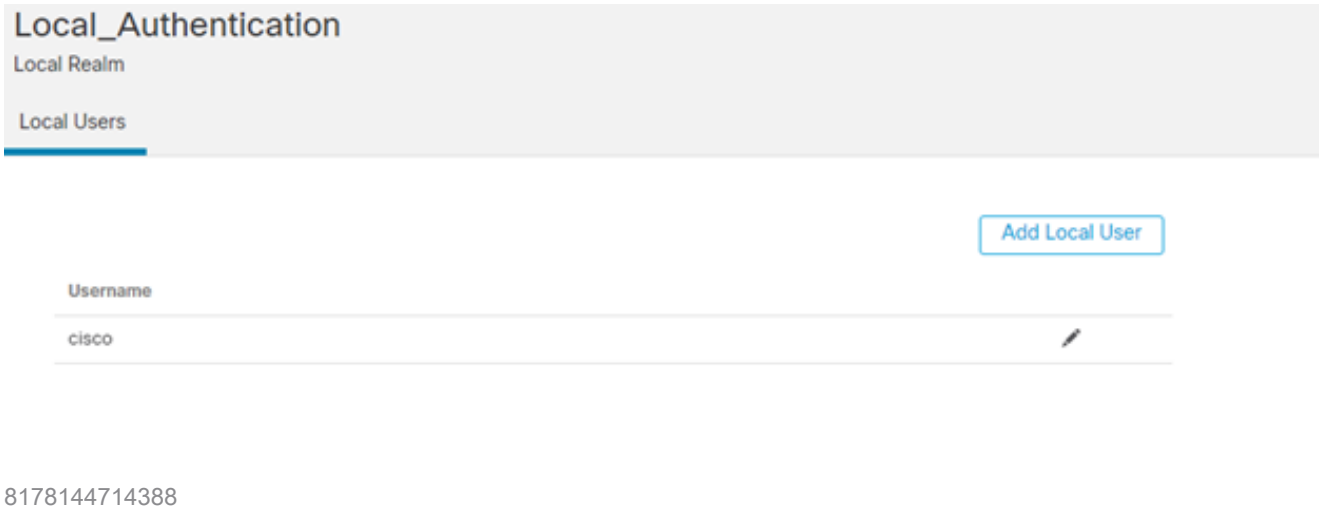
- Creare o modificare un criterio VPN per l'Autorità registrazione (**Dispositivi > VPN > Accesso remoto**).
- Creare un profilo di connessione all'interno del criterio.
- Specificare **LOCAL** come server di autenticazione primario, secondario o di fallback nel profilo di connessione.

3. Associare l'area di autenticazione locale creata a un criterio VPN RA.

- Nell'editor dei criteri VPN per l'Autorità registrazione, utilizzare la nuova impostazione **Realm locale**. Ogni profilo di connessione nel criterio VPN Autorità registrazione che utilizza l'autenticazione locale può utilizzare l'area di autenticazione locale specificata.



8178273923732



8178144714388

Ulteriori informazioni

[Note sulla versione di Cisco Firewall (in precedenza Firepower), versione 7.0.x]

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).