Ripristino di SD-WAN vSmart e vBond Access

Sommario

Introduzione

Questo documento descrive come recuperare l'accesso SD-WAN vSmart e vBond dopo la perdita delle credenziali.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Problema

L'accesso a vBonds e vSmarts è stato perso. Ciò si verifica quando non si conoscono o si ricordano le credenziali oppure quando l'accesso viene bloccato dopo un numero eccessivo di

tentativi di accesso non riusciti a entrambe le interfacce. Allo stesso tempo, le connessioni di controllo tra vManage, vSmarts e vBonds sono ancora stabilite.

Soluzione

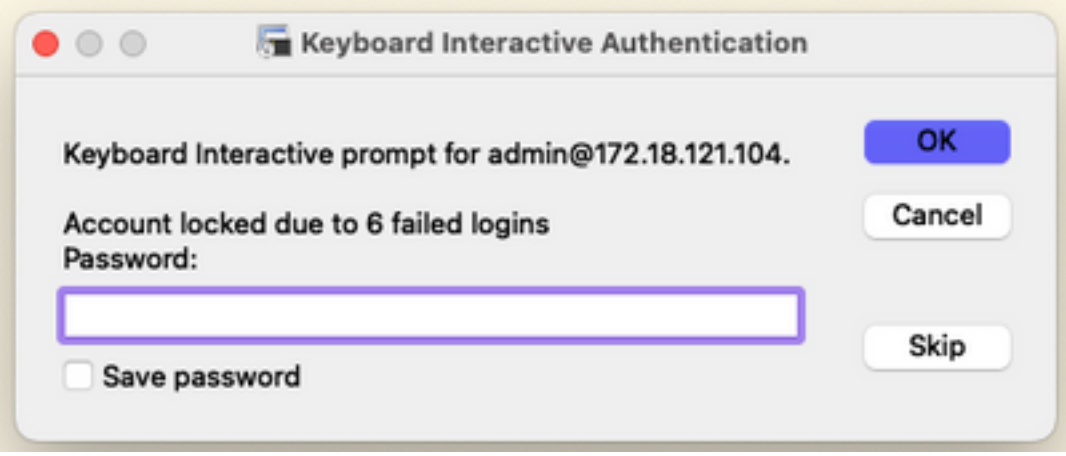
Passaggio 1. Sbloccare le credenziali, se necessario

Questa procedura consente di identificare un nome utente bloccato e di sbloccarlo.

- Se l'account è stato bloccato a causa di un numero eccessivo di tentativi di accesso non riusciti, è possibile visualizzare il messaggio 'Account bloccato a causa di X accessi non riusciti' ogni volta che si digita il nome utente.

```
host:~pc-host$ ssh admin@172.18.121.104 -p 22255
viptela 20.6.3

(admin@172.18.121.105) Account locked due to 6 failed logins <<<
```

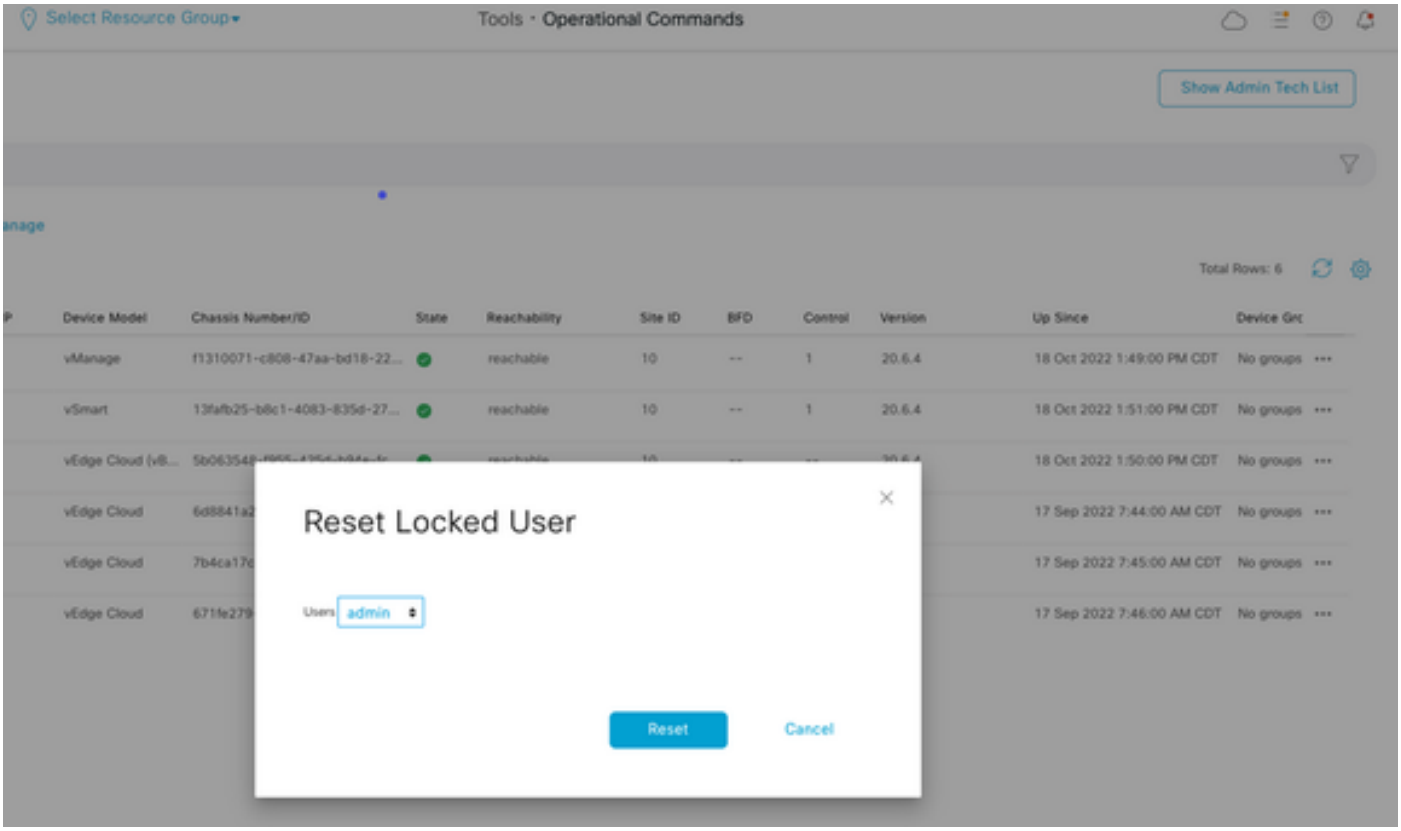


Opzione A. Sblocco delle credenziali dalla GUI vManage

Dopo aver confermato che le credenziali sono bloccate, è necessario sbloccarle. vManage consente di eseguire facilmente questa operazione.

- Èpossibile sbloccare manualmente le credenziali dall'interfaccia grafica di vManage per qualsiasi dispositivo.

Selezionare **vManage > Tools > Operational Commands > Device > ... > Reset Locked User > Select User > Reset**



Opzione B. SSH sul dispositivo che ha configurato una credenziale aggiuntiva

Se si dispone di una connettività SSH con una credenziale Netadmin aggiuntiva nel dispositivo in cui si conferma che le credenziali bloccate sono, è comunque possibile sbloccarle dalla CLI.

- Èpossibile eseguire il comando:

```
request aaa unlock-user username
```

- Se le credenziali sono state sbloccate e l'accesso non riesce, è necessario modificare la password.

Passaggio 2. Ripristino dell'accesso con un modello CLI

Ènecessario creare i modelli CLI che consentono di modificare la password dei dispositivi. Se un modello CLI è già stato creato e associato al dispositivo, è possibile andare al passo 3.

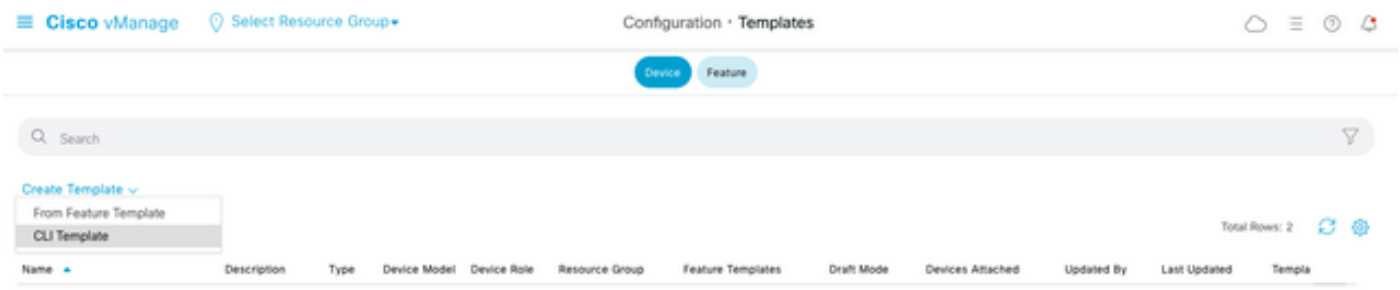
Opzione A. Caricare la configurazione in esecuzione direttamente nel modello CLI

vManage consente di caricare facilmente la configurazione in esecuzione dai dispositivi nel modello CLI.

> **Nota**: questa opzione non può essere disponibile in base alla versione di vManage. È possibile esaminare l'opzione B.

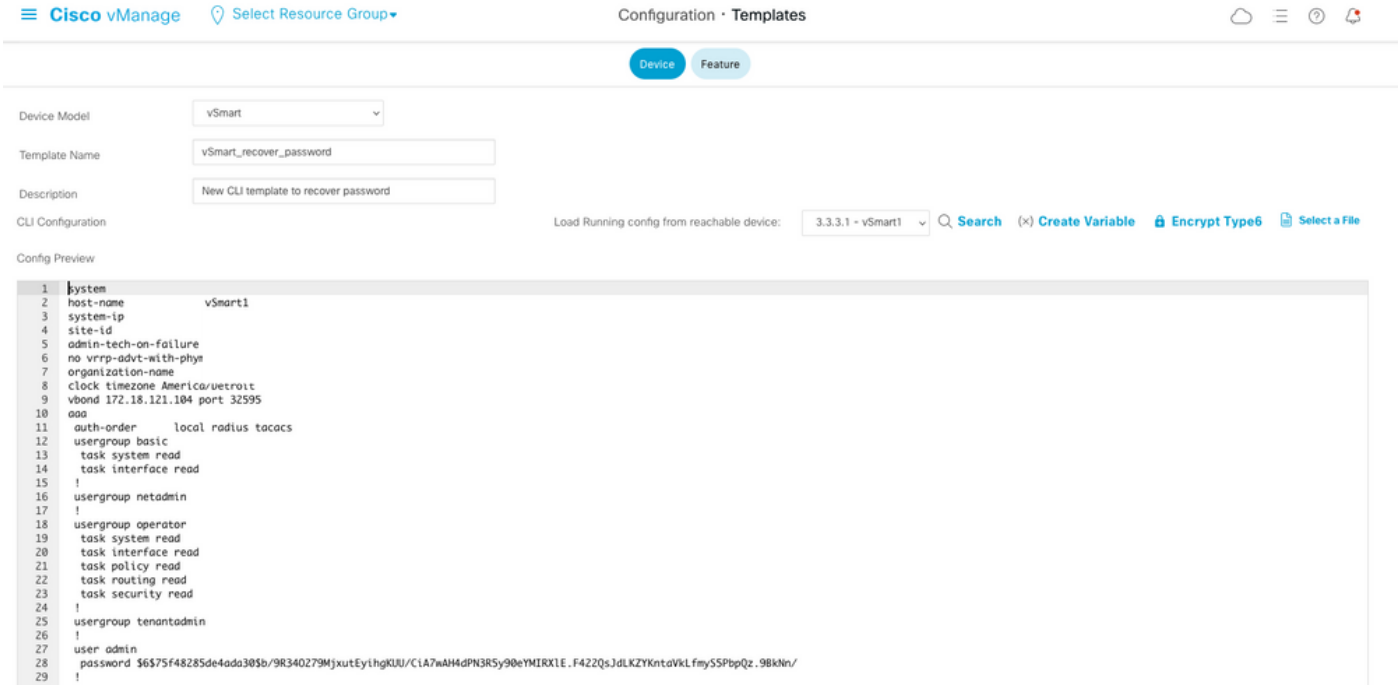
- Crea un nuovo modello CLI

Selezionare **vManage > Configuration > Templates > Create Template > CLI template**



- In base al modello di dispositivo selezionato, è possibile scegliere tra quale dispositivo vManage carica la configurazione in esecuzione.

- Per creare il modello, è necessario immettere i valori Modello dispositivo, Nome modello e Descrizione.



- Non appena la configurazione viene generata nel modello CLI, è possibile rivedere il passo 4 per modificare la password.

Opzione B. Caricamento della configurazione dal database vManage

Nel caso in cui non sia possibile caricare la configurazione automaticamente nella CLI, è comunque possibile ottenere manualmente la configurazione del dispositivo e creare il modello CLI da tali informazioni.

- vManage dispone sempre di una configurazione di backup da tutti i dispositivi archiviati nel relativo database.

Selezionare **vManage>Configuration>Controllers>Device> ... >Running Configuration vManage>Configuration>Controllers>Device> ... >Local Configuration**.

> **Nota**: esecuzione rispetto alla configurazione locale. Se si esegue Configuration, vManage deve richiedere le informazioni di configurazione per il dispositivo. Configurazione locale

indica che vManage visualizza le informazioni già archiviate nel relativo database.

- Dopo la visualizzazione della configurazione locale, è possibile copiare l'intera configurazione in un Blocco note.

Local Configuration

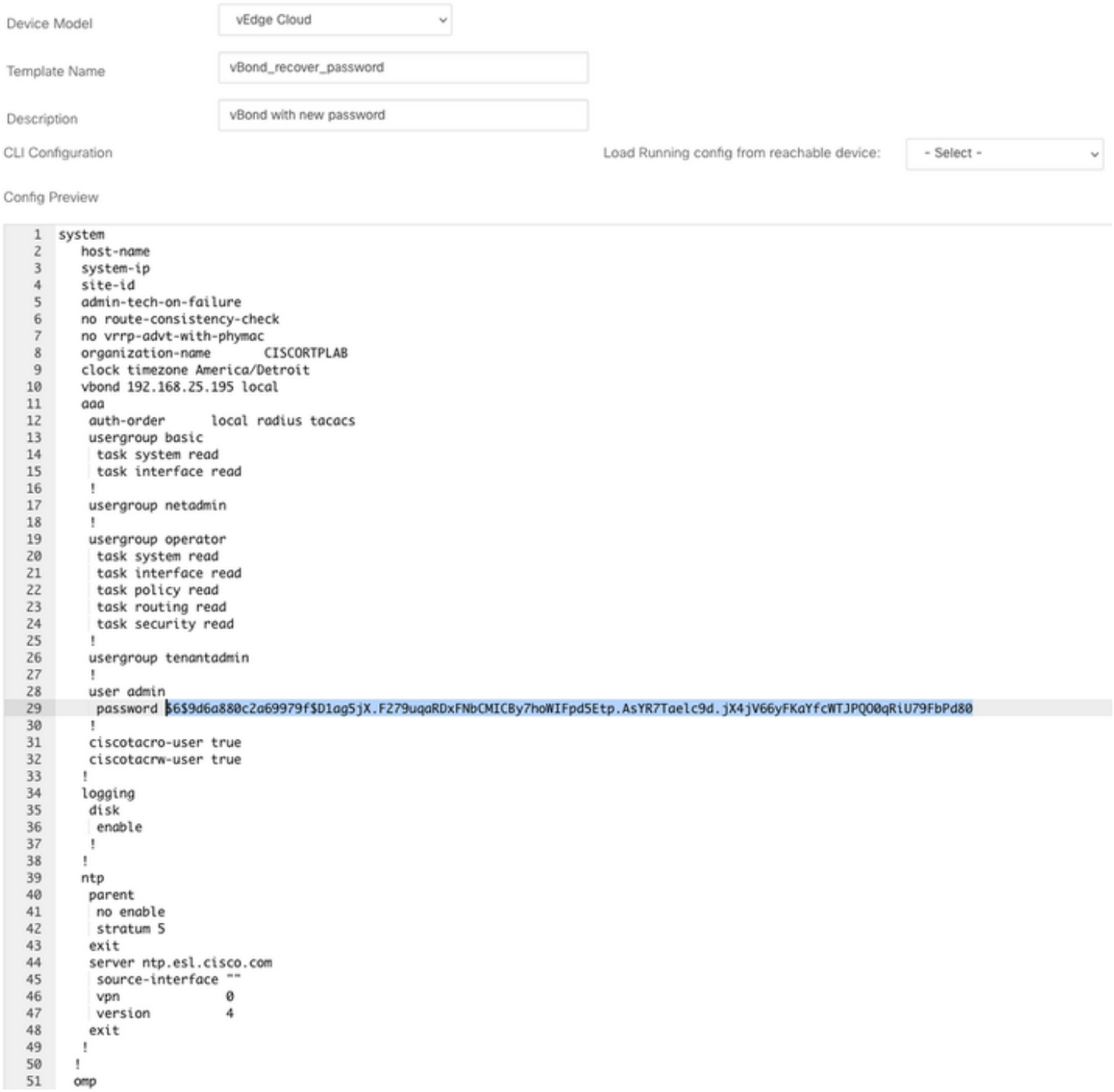
```
no config
config
 system
  host-name
  system-ip
  site-id              1
  admin-tech-on-failure
  no route-consistency-check
  no vrrp-advt-with-phymac
  organization-name       CISCORTPLAB
  clock timezone America/Detroit
  vbond 192.168.25.195 local
  aaa
   auth-order      local radius tacacs
   usergroup basic
    task system read
    task interface read
   !
   usergroup netadmin
   !
   usergroup operator
    task system read
    task interface read
    task policy read
    task routing read
    task security read
   !
   usergroup tenantadmin
   !
   user admin
    password $6$9d6a880c2a69979f$D1ag5jX.F279uqaRDxFNbCMlCBy7hoWlFpd5Etp.AsYR7Taelc9d.jX4jV66yFKaYfcWTJPQO0qRiU79FbPd80
   !
   ciscotacro-user true
   ciscotacrw-user true
  !
  logging
   disk
    enable
   !
  !
  ntp
   parent
    no enable
```

- ènecessario creare un nuovo modello CLI.

Passare a **vManage>Configuration>Templates>Create Template>CLI template (Configurazione>Modelli>Crea modello>Modello CLI).**

- Per creare il modello, è necessario immettere i valori Modello dispositivo, Nome modello, Descrizione e Anteprima configurazione. La configurazione copiata dalla configurazione locale deve essere incollata nell'anteprima della configurazione.

  Attenzione: per vBond è necessario selezionare vEdge cloud. Ogni altro dispositivo ha il proprio modello specifico.



Passaggio 3. Nuove credenziali

Dopo aver creato il modello, è possibile sostituire la password crittografata o aggiungere nuove credenziali.

Opzione A. Modifica della password persa

Èpossibile modificare la configurazione per assicurarsi di utilizzare una password nota.

- Èpossibile evidenziare e sostituire la password crittografata con una password in testo normale.

```
!
user admin
 password Cisc0123
!
```

Nota: questa password in testo normale viene crittografata dopo il push del modello.

Opzione B. Aggiungere un nuovo nome utente e password con privilegi Netadmin

Se le modifiche alla password non sono consentite, è possibile aggiungere nuove credenziali per garantire l'accessibilità.

```
user admin
 password $6$9d6a880c2a69979f$D1ag5jX.F279uqaRDxFNbCMICBy7hoWIFpd5Etp.AsYR7Taelc9d.jX4jV66yFKaYfcWTJPQO0qRiU79FbPd80
!
user admin2
 password Cisc0123
 group netadmin
!
```

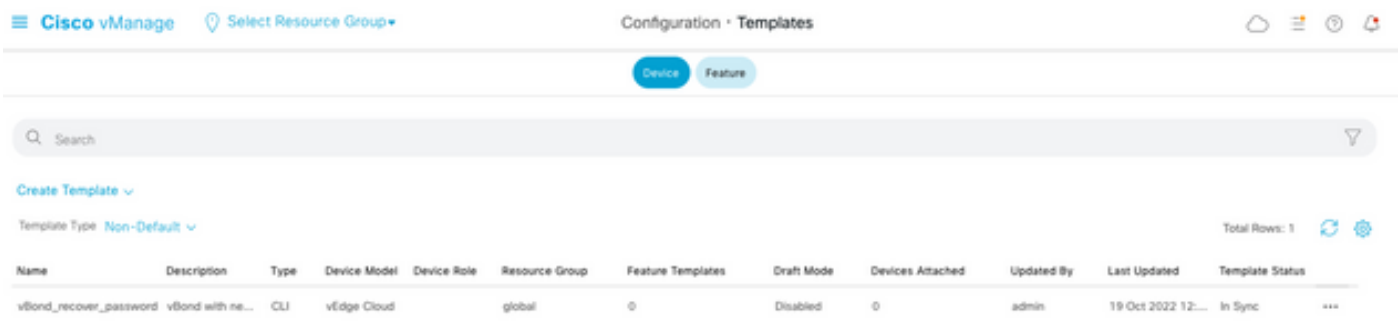
```
user newusername < Creates username
password password < Creates the password
group netadmin < Assigns read-write privileges
```

- Fare clic su **Add** per **salvare** il modello.

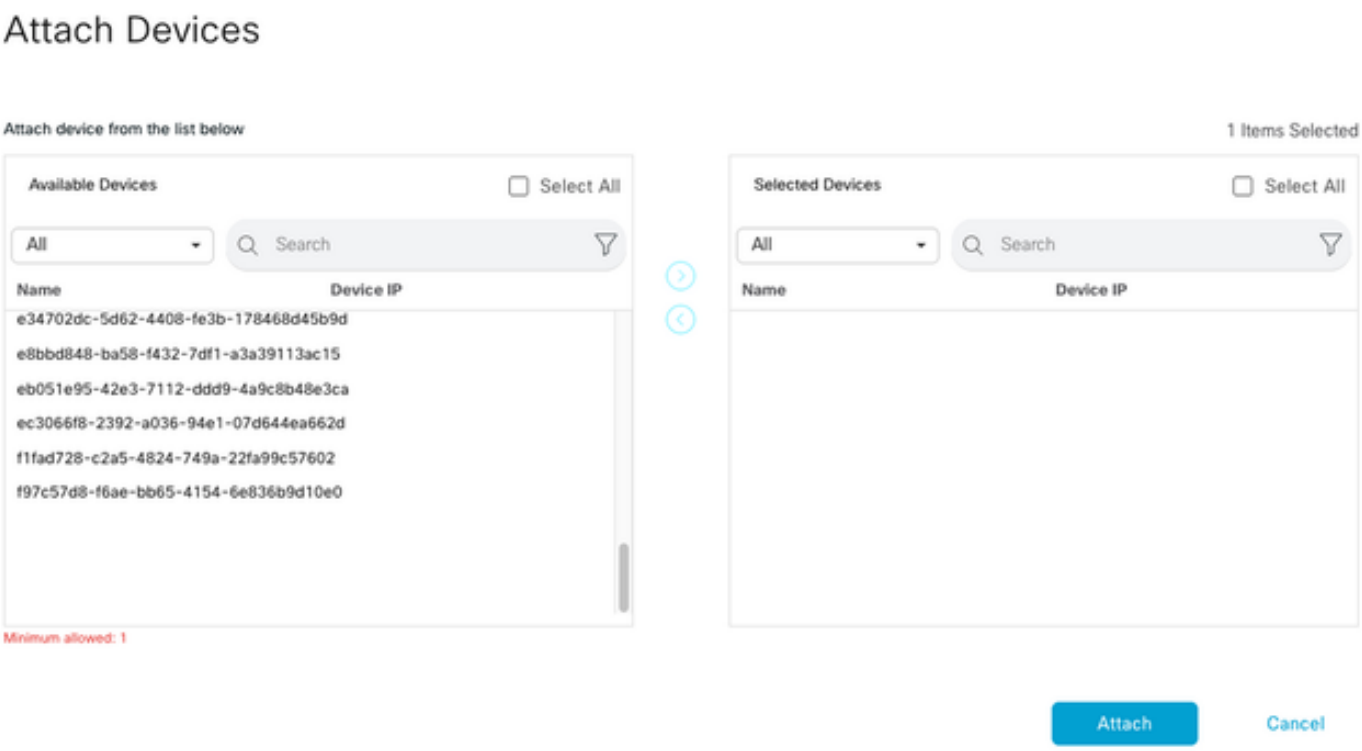
Passaggio 4. Push del modello sul dispositivo

Il passaggio successivo consiste nel spingere il modello CLI sul dispositivo per modificare la configurazione in esecuzione.

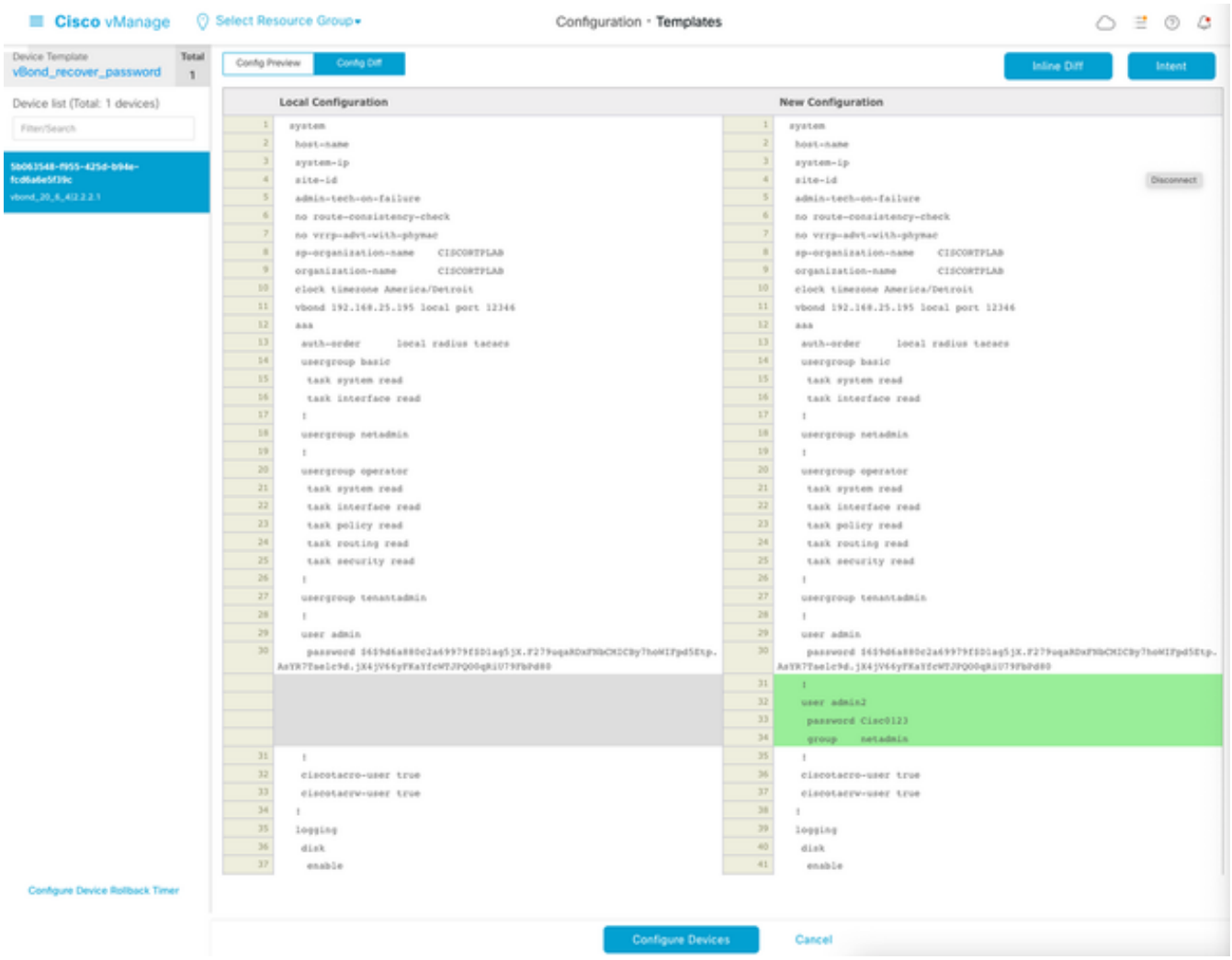
- Dopo aver salvato il modello, è possibile collegarlo al dispositivo.



Passare a **vManage>Configuration>Templates> Select the Template>... >Select the device > Attach (vManage>Configurazione>Modelli> Selezionare il modello >... >Selezionare il dispositivo > Connetti).**



- Fare clic su **Attach (Allega) per esaminare l'anteprima della configurazione.**
- Se si seleziona l'opzione di configurazione Diff, è possibile verificare se la password è stata modificata o se sono state aggiunte nuove credenziali.



- Per eseguire il push del modello, fare clic su **Configura dispositivi**.
- Dopo la conferma da parte di vManage del completamento del push di Ttemplate, è possibile usare le nuove credenziali per accedere al dispositivo tramite SSH.

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).