

Ripristino di SD-WAN vSmart e vBond Access

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Soluzione](#)

[Passaggio 1. Sbloccare le credenziali, se necessario](#)

[Opzione A. Sblocco delle credenziali dalla GUI vManage](#)

[Opzione B. SSH sul dispositivo che ha configurato una credenziale aggiuntiva](#)

[Passaggio 2. Ripristino dell'accesso con un modello CLI](#)

[Opzione A. Caricare la configurazione in esecuzione direttamente nel modello CLI](#)

[Opzione B. Caricamento della configurazione dal database vManage](#)

[Passaggio 3. Nuove credenziali](#)

[Opzione A. Modifica della password persa](#)

[Opzione B. Aggiungere un nuovo nome utente e password con privilegi Netadmin](#)

[Passaggio 4. Push del modello sul dispositivo](#)

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

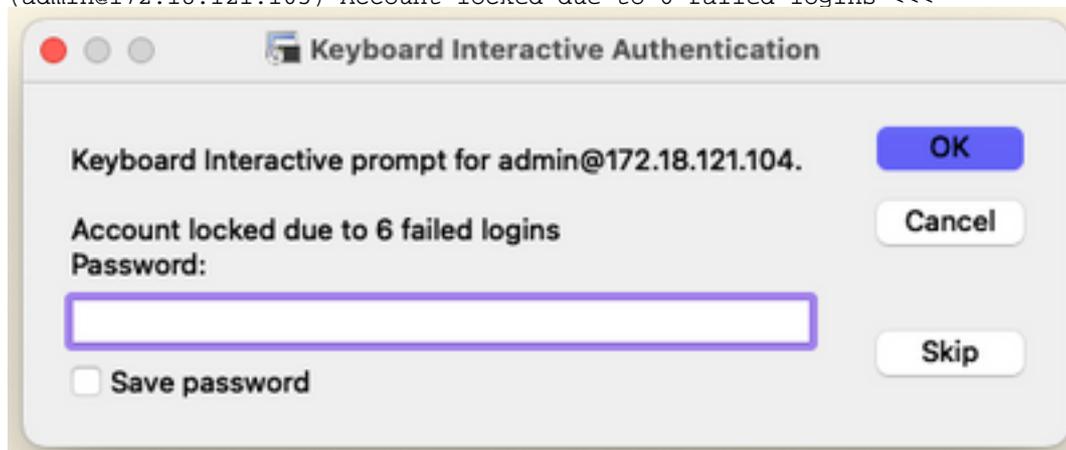
Passaggio 1. Sbloccare le credenziali, se necessario

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 <<<
```

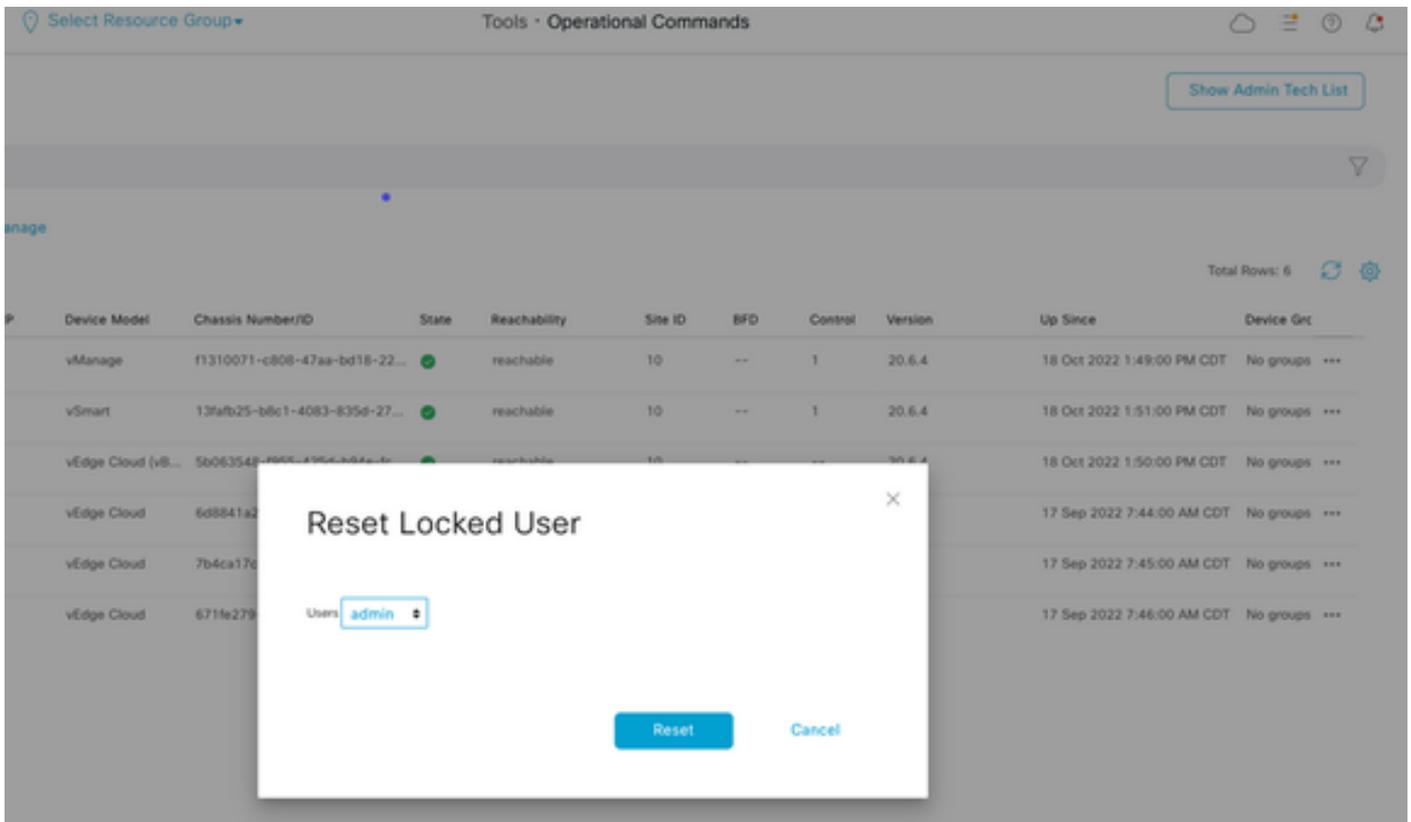


Opzione A. Sblocco delle credenziali dalla GUI vManage

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

- È possibile 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.

- È possibile 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

È necessario 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.

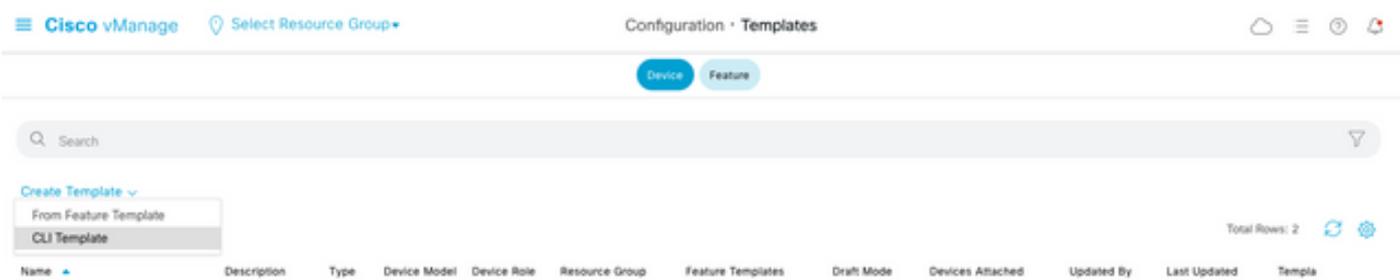
Opzione A. Caricare la configurazione in esecuzione direttamente nel modello CLI

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

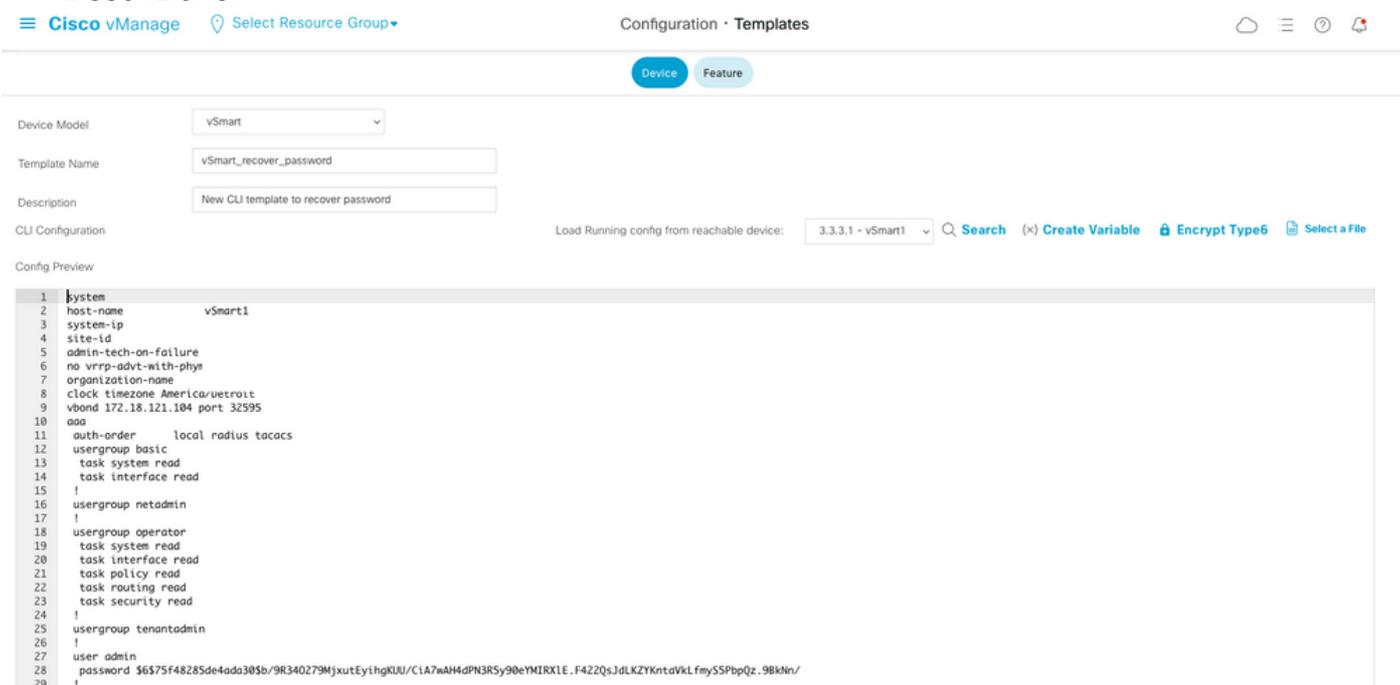
Selezionare **vManage > Configuration > Templates > Create Template > CLI template**



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

Load Running config from reachable device: 10.2.2.1 vSmart1

- 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.

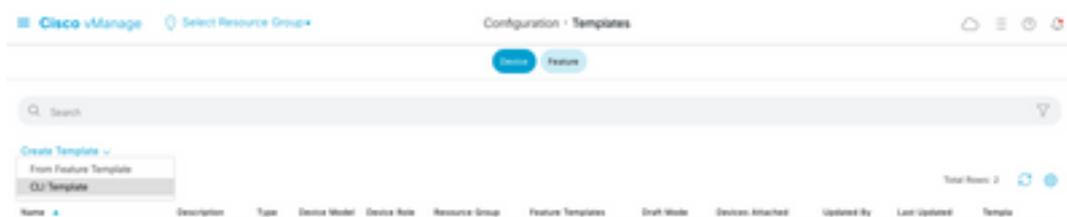
- Dopo la visualizzazione della configurazione locale, è possibile copiare l'intera configurazione in un Blocco note.

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.F279uqaRDxFNbCMICBy7hoWIFpd5Etp.AsYR7Taelc9d.jX4jV66yFKaYfcWTJPQO0qRiU79FbPd80
!
ciscotacro-user true
ciscotacrw-user true
!
logging
disk
enable
!
!
ntp
parent
no enable
```

- è necessario 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.

Device Model:

Template Name:

Description:

CLI Configuration:

Config Preview

```

1 system
2 host-name
3 system-ip
4 site-id
5 admin-tech-on-failure
6 no route-consistency-check
7 no vrrp-advt-with-phymac
8 organization-name CISCORDPLAB
9 clock timezone America/Detroit
10 vbond 192.168.25.195 local
11 aaa
12 auth-order local radius tacacs
13 usergroup basic
14 | task system read
15 | task interface read
16 |
17 usergroup netadmin
18 |
19 usergroup operator
20 | task system read
21 | task interface read
22 | task policy read
23 | task routing read
24 | task security read
25 |
26 usergroup tenantadmin
27 |
28 user admin
29 password $6$9d6a880c2a69979f$D1ag5jX.F279uqaRDxFNbCMICBy7hoWIFpd5Etp.AsYR7Taelc9d.jX4jV66yFKaYfcWTJPQ00qRiU79FbPd80
30 |
31 ciscotacro-user true
32 ciscotacrw-user true
33 |
34 logging
35 disk
36 | enable
37 |
38 |
39 ntp
40 parent
41 | no enable
42 | stratum 5
43 | exit
44 | server ntp.esl.cisco.com
45 | source-interface ""
46 | vpn 0
47 | version 4
48 | exit
49 |
50 |
51 omp

```

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

È possibile modificare la configurazione per assicurarsi di utilizzare una password nota.

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

```
27      !
28      user admin
29      password Cisc0123
30      !
```

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.

```
28      user admin
29      password $6$9d6a880c2a69979f$D1ag5jX.F279uqaRDxFNbCMICBy7hoWIFpd5Etp.AsYR7Tae1c9d.jX4jV66yFKaYfcWTJJPQ00qRiU79FbPd80
30      !
31      user admin2
32      password Cisc0123
33      group netadmin
34      !
```

```
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.

The screenshot shows the Cisco vManage interface for Configuration Templates. The page title is "Configuration · Templates". There are tabs for "Device" and "Feature". A search bar is present. Below the search bar, there is a "Create Template" dropdown and a "Template Type" dropdown set to "Non-Default". A table lists the templates:

Name	Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	Template Status
vBond_recover_password	vBond with ne...	CLI	vEdge Cloud		global	0	Disabled	0	admin	19 Oct 2022 12:...	In Sync

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

Attach Devices

Attach device from the list below

1 Items Selected

Available Devices Select All

All

Name	Device IP
e34702dc-5d62-4408-fe3b-178468d45b9d	
e8bbd848-ba58-f432-7df1-a3a39113ac15	
eb051e95-42e3-7112-ddd9-4a9c8b48e3ca	
ec3066f8-2392-a036-94e1-07d644ea662d	
f1fad728-c2a5-4824-749a-22fa99c57602	
f97c57d8-f6ae-bb65-4154-6e836b9d10e0	

Selected Devices Select All

All

Name	Device IP



Minimum allowed: 1

Attach

Cancel

- 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.

Cisco vManage Select Resource Group Configuration - Templates

Device Template: vBond_recover_password Total: 1

Device list (Total: 1 devices)

96083548-8955-4256-8946-fc046e5f39c

vbond_20_6_43.2.2.1

Config Preview
Config Diff

Inline Diff
Intent

Local Configuration		New Configuration	
1	system	1	system
2	host-name	2	host-name
3	system-ip	3	system-ip
4	site-id	4	site-id
5	admin-tech-on-failure	5	admin-tech-on-failure
6	no route-consistency-check	6	no route-consistency-check
7	no vrrp-advt-with-physac	7	no vrrp-advt-with-physac
8	sp-organization-name CISCOPTLAB	8	sp-organization-name CISCOPTLAB
9	organization-name CISCOPTLAB	9	organization-name CISCOPTLAB
10	clock timezone America/Detroit	10	clock timezone America/Detroit
11	vbond 192.168.25.195 local port 12344	11	vbond 192.168.25.195 local port 12344
12	aaa	12	aaa
13	auth-order local radius tacacs	13	auth-order local radius tacacs
14	usergroup basic	14	usergroup basic
15	task system read	15	task system read
16	task interface read	16	task interface read
17	!	17	!
18	usergroup netadmin	18	usergroup netadmin
19	!	19	!
20	usergroup operator	20	usergroup operator
21	task system read	21	task system read
22	task interface read	22	task interface read
23	task policy read	23	task policy read
24	task routing read	24	task routing read
25	task security read	25	task security read
26	!	26	!
27	usergroup tenantadmin	27	usergroup tenantadmin
28	!	28	!
29	user admin	29	user admin
30	password \$6596a880c2a6997fE01ag5JX.F279qa8Dx79bCKCBy7hW17pd5Etp.AuTR7TaeLc9d.Jk4jY6y7FA7Yc97J900q8L1U79bnd80	30	password 165hdta880c2a6997fE01ag5JX.F279qa8Dx79bCKCBy7hW17pd5Etp.AuTR7TaeLc9d.Jk4jY6y7FA7Yc97J900q8L1U79bnd80
31	!	31	!
32	!	32	user admin2
33	!	33	password C1ac0123
34	!	34	group netadmin
35	!	35	!
36	ciscotacro-user true	36	ciscotacro-user true
37	ciscotacrv-user true	37	ciscotacrv-user true
38	!	38	!
39	logging	39	logging
40	disk	40	disk
41	enable	41	enable

Configure Devices Cancel

- 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).