

Recuperación de vSmart SD-WAN y vBond Access

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

[Paso 1. Desbloquee las credenciales si es necesario](#)

[Opción A. Desbloquear credenciales de la GUI de vManage](#)

[Opción B. SSH al dispositivo que ha configurado una credencial adicional](#)

[Paso 2. Recuperar el acceso con una plantilla CLI](#)

[Opción A. Cargue la configuración en ejecución directamente en la plantilla CLI](#)

[Opción B. Cargue la configuración desde vManage Database](#)

[Paso 3. Nuevas credenciales](#)

[Opción A. Cambie la contraseña perdida](#)

[Opción B. Agregue un nombre de usuario y una contraseña nuevos con privilegios Netadmin](#)

[Paso 4. Inserción de plantilla en el dispositivo](#)

Introducción

Este documento describe cómo recuperar su acceso vSmart SD-WAN y vBond después de que se pierdan sus credenciales.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Se ha perdido el acceso a vBonds y vsmarts. Esto sucede cuando no conoce o no recuerda sus credenciales o cuando el acceso se bloquea después de intentos excesivos e infructuosos de iniciar sesión en cualquiera de las interfaces. Al mismo tiempo, las conexiones de control entre vManage, vsmarts y vBonds aún están establecidas.

Solución

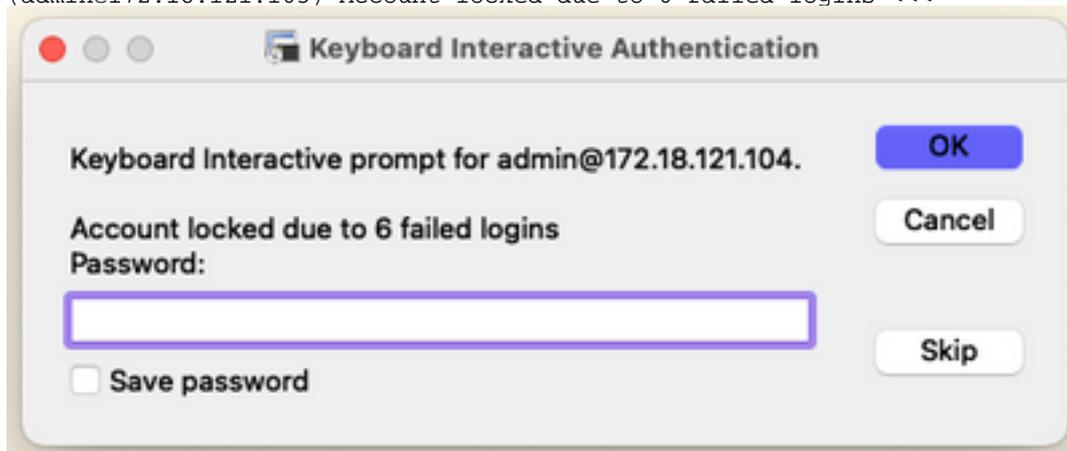
Paso 1. Desbloquee las credenciales si es necesario

Estos pasos le ayudan a identificar un nombre de usuario bloqueado y cómo desbloquearlo.

- En caso de que la cuenta se haya bloqueado debido a un número excesivo de intentos de inicio de sesión fallidos, puede ver el mensaje "Cuenta bloqueada debido a X inicios de sesión fallidos" cada vez que escribimos el nombre de usuario.

```
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 <<<
```

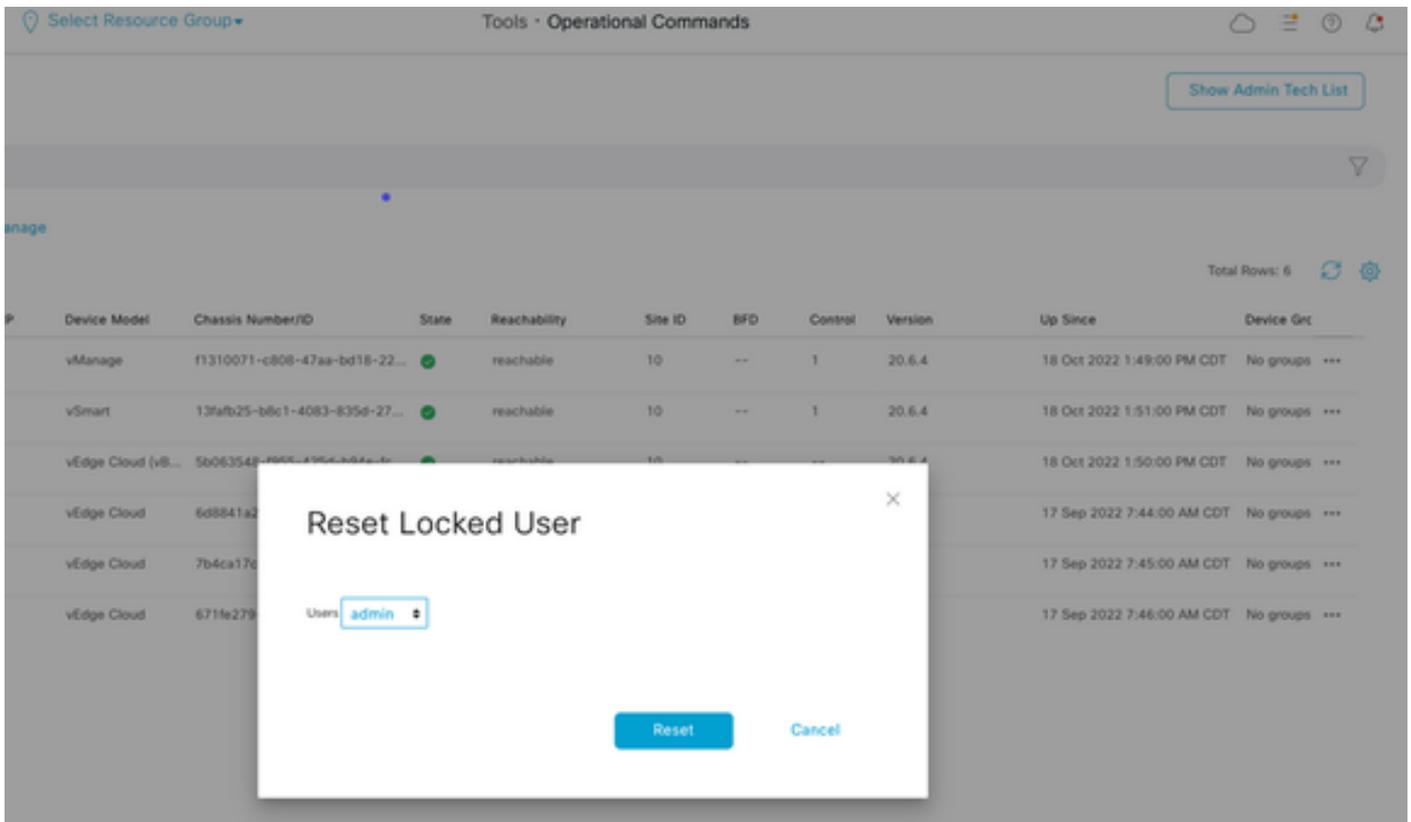


Opción A. Desbloquear credenciales de la GUI de vManage

Después de confirmar que las credenciales están bloqueadas, debe desbloquearlas. vManage puede ayudarle a realizar esta operación fácilmente.

- Puede desbloquear manualmente las credenciales de la GUI de vManage para cualquier dispositivo.

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



Opción B. SSH al dispositivo que ha configurado una credencial adicional

En caso de que tenga conectividad SSH con una credencial Netadmin adicional en el dispositivo en el que confirma que las credenciales bloqueadas están bloqueadas, aún puede desbloquearlas desde CLI.

- Puede ejecutar el comando:

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

- En caso de que desbloquee las credenciales y siga fallando el inicio de sesión, deberá cambiar la contraseña.

Paso 2. Recuperar el acceso con una plantilla CLI

Debe crear las plantillas de CLI que le ayudarán a modificar la contraseña de los dispositivos. En caso de que ya se haya creado una plantilla CLI y esté conectada al dispositivo, puede ir directamente al paso 3.

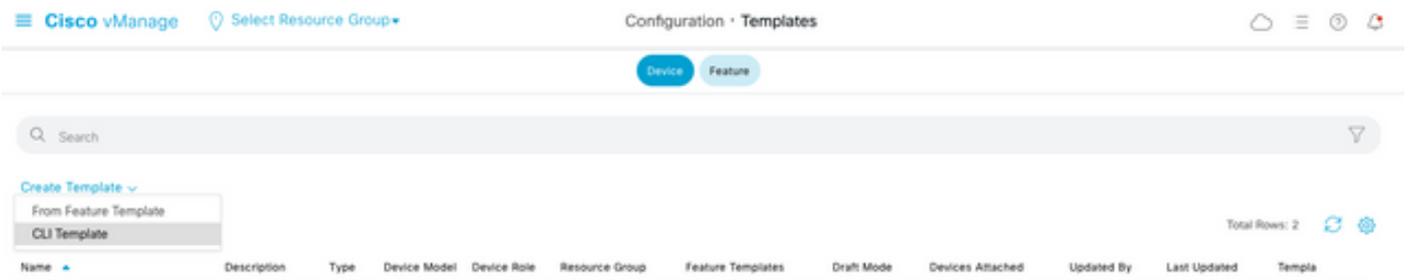
Opción A. Cargue la configuración en ejecución directamente en la plantilla CLI

vManage cuenta con una forma sencilla de cargar la configuración en ejecución desde los dispositivos en la plantilla de CLI.

Nota: Esta opción no puede estar disponible en función de la versión de vManage. Puede revisar la opción B.

- Crear una plantilla CLI nueva

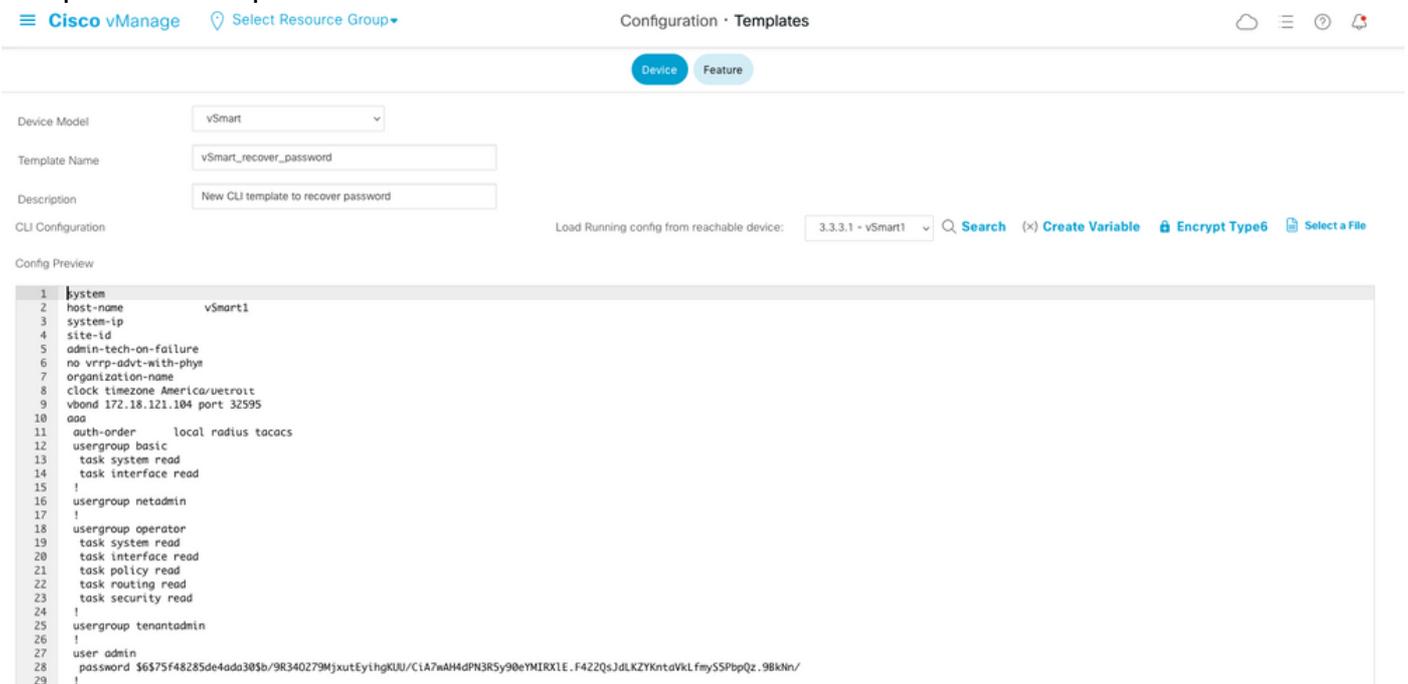
Vaya a vManage > Configuration > Templates > Create Template > CLI template



- Según el modelo de dispositivo seleccionado, puede elegir el dispositivo desde el que vManage carga la configuración en ejecución.

Load Running config from reachable device: 10.2.2.1 vSmart1

- Es necesario introducir los valores Modelo de dispositivo, Nombre de plantilla y Descripción para crear la plantilla.



- Tan pronto como se genere la configuración en la plantilla CLI, puede revisar el paso 4 para modificar la contraseña.

Opción B. Cargue la configuración desde vManage Database

En caso de que no pueda cargar la configuración automáticamente en la CLI, puede obtener manualmente la configuración del dispositivo y crear la plantilla de CLI a partir de esa información.

- vManage siempre tiene una configuración de copia de seguridad de todos los dispositivos almacenados en su base de datos.

Vaya a vManage>Configuración>Controladores>Dispositivo> ... >Configuración en ejecución>vManage>Configuración>Controladores>Dispositivo> ... >Configuración local.

Nota: Ejecución frente a configuración local. La ejecución de la configuración significa que

vManage necesita solicitar la información de configuración para el dispositivo. Configuración local significa que vManage muestra la información ya almacenada en su base de datos.

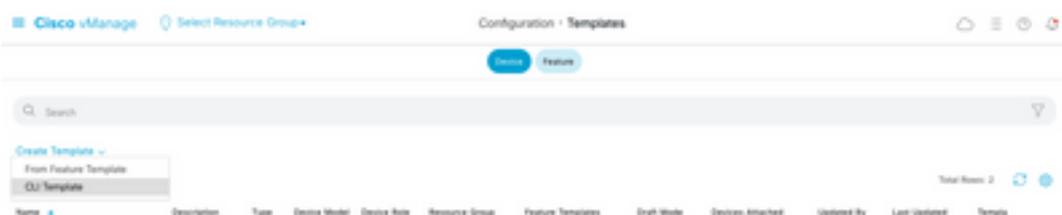
- Después de que aparezca la configuración local, puede copiar toda la configuración en un Bloc de notas.

Local Configuration

```
no config
config
system
  host-name
  system-ip
  site-id 1
  admin-tech-on-failure
  no route-consistency-check
  no vrrp-advt-wth-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
```

- Debe crear una nueva plantilla CLI.

Vaya a **vManage>Configuration>Templates>Create Template>CLI template**.



- Es necesario introducir los valores Modelo de dispositivo, Nombre de plantilla, Descripción y Vista previa de configuración para crear la plantilla. La configuración copiada de Configuración local debe pegarse en la vista previa de la configuración.

Precaución: para vBond, debe seleccionar nube de vEdge. Los demás dispositivos tienen su propio modelo específico.

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 CISCORTPLAB
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.AsYR7Tae1c9d.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

```

Paso 3. Nuevas credenciales

Una vez creada la plantilla, puede reemplazar la contraseña cifrada o agregar nuevas credenciales.

Opción A. Cambie la contraseña perdida

Puede modificar la configuración para asegurarse de que utiliza una contraseña conocida.

- Puede resaltar y reemplazar la contraseña cifrada por una de texto sin formato.

```

27      !
28      user admin
29      password Cisc0123
30      !

```

Nota: Esta contraseña de texto sin formato se cifra después de enviar la plantilla.

Opción B. Agregue un nombre de usuario y una contraseña nuevos con privilegios Netadmin

Si no se permiten los cambios en la contraseña, puede agregar nuevas credenciales para garantizar la accesibilidad.

```

28      user admin
29      password $6$9d6a880c2a69979f$D1ag5jX.F279uqaRDxFNbCMICBy7hoWIFpd5Etp.AsYR7Taelc9d.jX4jV66yFKaYfcWTJPQ00qRiU79FbPd80
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

- Haga clic en **Agregar** para **guardar** la plantilla.

Paso 4. Inserción de plantilla en el dispositivo

El siguiente paso consiste en insertar la plantilla CLI en el dispositivo para cambiar la configuración en ejecución.

- Una vez guardada la plantilla, puede conectarla 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 menu. The "Template Type" is 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

Vaya a vManage>Configuration>Templates> Select the Template>... >Select the device > Attach.

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

- Haga clic en **Attach** para revisar la previsualización de la configuración.
- Al marcar Config Diff, puede ver que la contraseña ha cambiado o que se han agregado las nuevas credenciales.

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_40.2.2.1

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-phymac	7	no vrrp-advt-with-phymac
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 \$6596a880c2a6997f501ag5JX.F279qa8Dx9BCKCBy7hW1Zpd5Eg.AuTR7Tae1c96.Jk4jY6GyF8aY2c97J900q8L1U798ad80	30	password 165hdta880c2a6997f501ag5JX.F279qa8Dx9BCKCBy7hW1Zpd5Eg.AuTR7Tae1c96.Jk4jY6GyF8aY2c97J900q8L1U798ad80
31	!	31	!
32	!	32	!
33	!	33	!
34	!	34	!
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 Device Rollback Timer

Configure Devices Cancel

- Para insertar la plantilla, haga clic en **Configure Devices**.
- Una vez que vManage confirme que la inserción de plantilla ha finalizado correctamente, puede utilizar sus nuevas credenciales para acceder al dispositivo mediante SSH.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).