

Recover SD-WAN vSmart and vBond Access

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Problem](#)

[Solution](#)

[Step 1. Unlock the Credentials if necessary](#)

[Option A. Unlock Credentials from vManage GUI](#)

[Option B. SSH to the device which has configured an additional credential](#)

[Step 2. Recover the Access with a CLI template](#)

[Option A. Load the Running Configuration directly in the CLI template](#)

[Option B. Load the Configuration from vManage Database](#)

[Step 3. New Credentials](#)

[Option A. Change the lost password](#)

[Option B. Add a new username and password with Netadmin privileges](#)

[Step 4. Template Push to the Device](#)

Introduction

This document describes how to recover your SD-WAN vSmart and vBond access after your credentials are lost.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

Access to vBonds and vSmarts has been lost. This happens when you do not know or remember your credentials or access is locked after excessive and unsuccessful attempts to log into either interface. At the same time, the Control Connections between vManage, vSmarts, and vBonds are

still established.

Solution

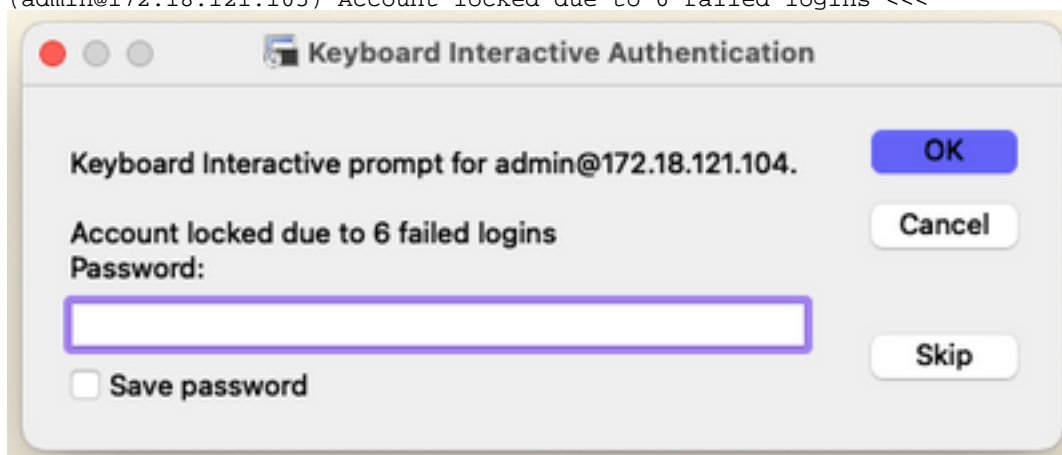
Step 1. Unlock the Credentials if necessary

These steps help you to identify a locked username and how to unlock them.

- In case the account has been locked due to excessive failed login attempts you can see the 'Account locked due to X failed logins' message every time we type the username.

```
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 <<<
```

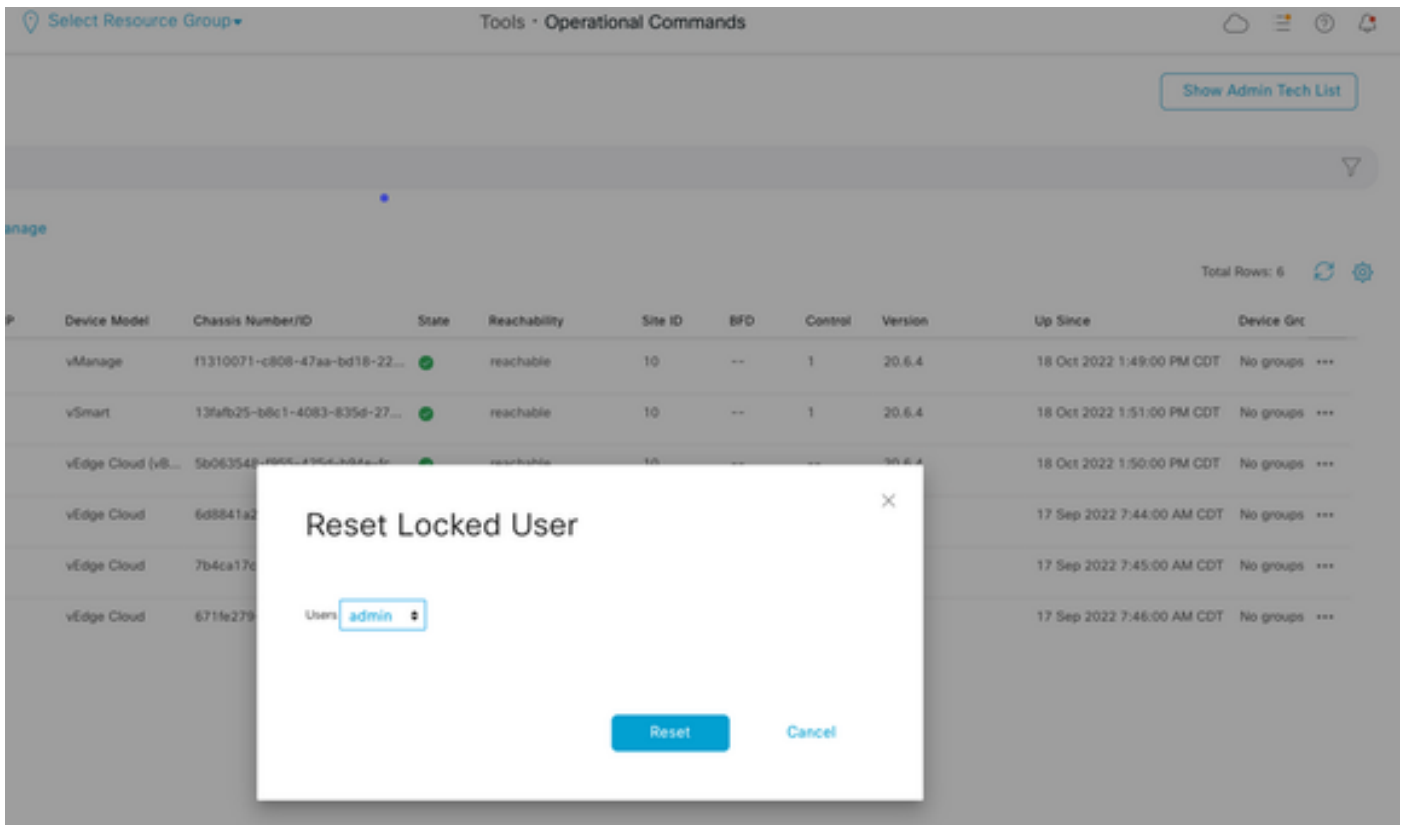


Option A. Unlock Credentials from vManage GUI

After you confirm the credentials are locked, you need to unlock them. vManage can help you to perform this operation easily.

- You can manually unlock the Credentials from vManage GUI for any device.

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



Option B. SSH to the device which has configured an additional credential

In case you have SSH connectivity with an additional Netadmin credential in the device where you confirm the locked credentials are, you can still unlock them from CLI.

- You can run the command:

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

- In case you unlocked the credentials and the log in still fails, you need to change the password.

Step 2. Recover the Access with a CLI template

You need to create the CLI templates that help you to modify the password for the devices. In case a CLI template is already created and attached to the Device, you can skip to Step 3.

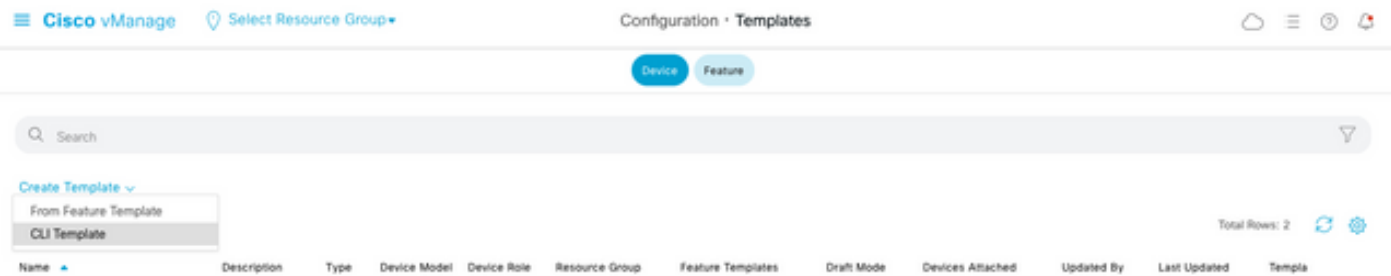
Option A. Load the Running Configuration directly in the CLI template

vManage has an easy way to load the Running Configuration from the devices into the CLI template.

Note: This option cannot be available based on the vManage Version. You can review Option B.

- Create a new CLI template

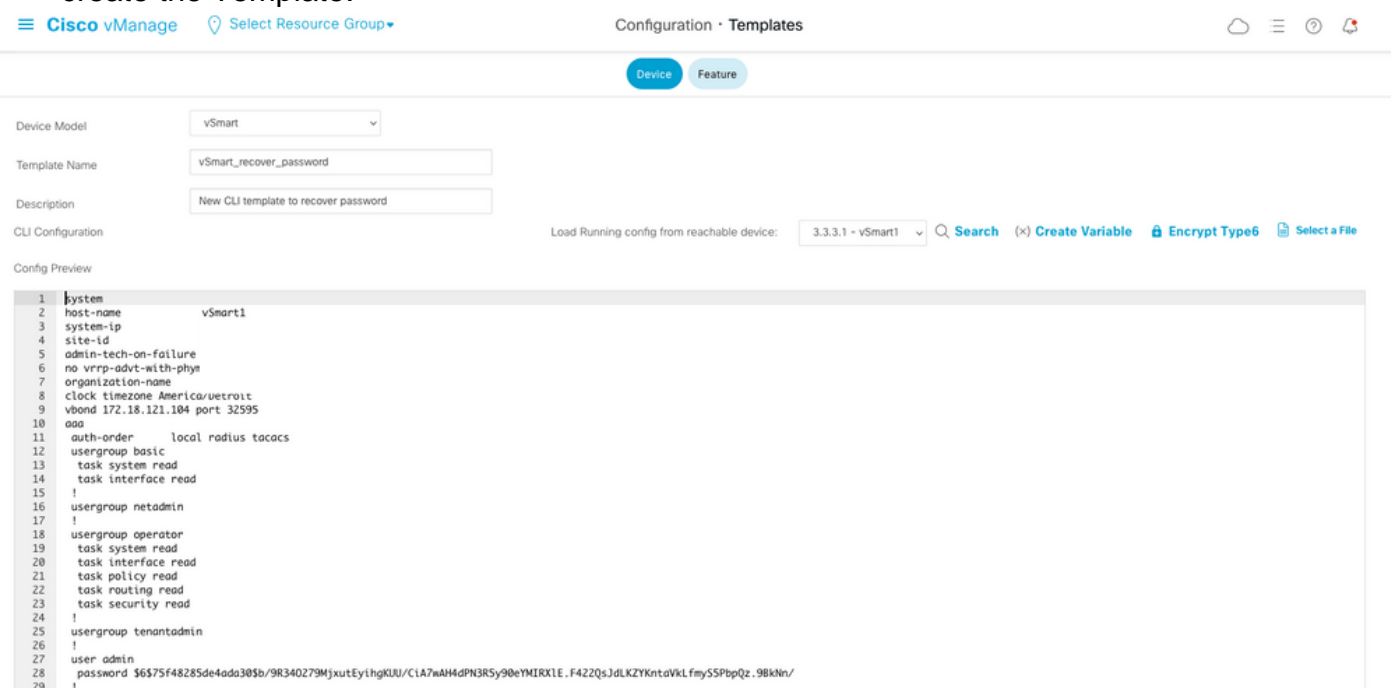
Navigate to **vManage > Configuration > Templates > Create Template > CLI template**



- Based on the device model selected, you can choose from which device the vManage loads the Running Configuration.

Load Running config from reachable device:

- The Device Model, Template Name, and Description values need to be entered in order to create the Template.



- As soon as the configuration is generated in the CLI template, you can review Step 4 to modify the password.

Option B. Load the Configuration from vManage Database

In case you cannot load the configuration automatically in the CLI, you can still manually obtain the configuration of the device and create the CLI Template from that information.

- vManage always has a backup configuration from all devices stored in its Database. Navigate to **vManage>Configuration>Controllers>Device> ... >Running Configuration** **vManage>Configuration>Controllers>Device> ... >Local Configuration**.

Note: Running vs Local Configuration. Running Configuration means that the vManage needs to request the configuration information for the device. Local Configuration means the vManage shows the information already stored in its Database.

- After the Local Configuration pops up, you can copy the whole configuration into a NotePad.

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

```

- You need to create a new CLI template.

Navigate to **vManage>Configuration>Templates>Create Template>CLI template.**



- The Device Model, Template Name, Description, and Config Preview values need to be entered in order to create the template. The configuration copied from Local Configuration needs to be pasted into config preview.

Caution: For vBond, you must select vEdge cloud. Every other device has its own specific model.

Device Model: vEdge Cloud

Template Name: vBond_recover_password

Description: vBond with new password

CLI Configuration: Load Running config from reachable device: - Select -

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
```

Step 3. New Credentials

After the template is created, you can replace the encrypted password or add new credentials.

Option A. Change the lost password

You can modify the configuration to ensure you use a known password.

- You can highlight and replace the encrypted password with a plain text one.

```

27      !
28      user admin
29      password Cisc0123
30      !

```

Note: This plain-text password is encrypted after the template push.

Option B. Add a new username and password with Netadmin privileges

If the changes to the password are not allowed, you can add new credentials to ensure accessibility.

```

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

- Click **Add** to **Save** the Template.

Step 4. Template Push to the Device

The next step is to push the CLI template to the device to change the Running Configuration.

- After the template has been saved, you can attach it to the device.

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

Navigate to **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

- **Click Attach** to review the config preview.
- When you check the Config Diff, you can see either the password has changed or the new credentials were added.

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-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 \$6596a880c2a6997f501ag5JX.F279qa8Dx9BCKCBy7hW17pd5Ep.AsTR7TaeLc9d.Jk4jY6y7FA7Yc97J900q8L0798ad80	30	password 165hdta880c2a6997f501ag5JX.F279qa8Dx9BCKCBy7hW17pd5Ep.AsTR7TaeLc9d.Jk4jY6y7FA7Yc97J900q8L0798ad80
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

Disconnect

Configure Device Rollback Timer

Configure Devices Cancel

- To push the Template, click **Configure Devices**.
- After the vManage confirms the Ttemplate push ended successfully, you can use your new credentials to access the device via SSH.