

Récupérer SD-WAN vSmart et vBond Access

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Problème](#)

[Solution](#)

[Étape 1. Déverrouillez les informations d'identification si nécessaire](#)

[Option A. Déverrouiller les informations d'identification de l'interface graphique vManage](#)

[Option B. Envoyez une requête SSH au périphérique qui a configuré une information d'identification supplémentaire](#)

[Étape 2. Récupérer l'accès avec un modèle CLI](#)

[Option A. Charger la configuration en cours directement dans le modèle CLI](#)

[Option B. Charger la configuration à partir de la base de données vManage](#)

[Étape 3. Nouvelles informations d'identification](#)

[Option A. Modifier le mot de passe perdu](#)

[Option B. Ajouter un nouveau nom d'utilisateur et un nouveau mot de passe avec les privilèges Netadmin](#)

[Étape 4. Diffusion du modèle vers le périphérique](#)

Introduction

Ce document décrit comment récupérer votre accès SD-WAN vSmart et vBond après la perte de vos informations d'identification.

Conditions préalables

Exigences

There are no specific requirements for this document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Problème

L'accès à vBonds et vSmarts a été perdu. Cela se produit lorsque vous ne connaissez pas ou ne

vous souvenez pas de vos informations d'identification ou lorsque l'accès est verrouillé après des tentatives excessives et infructueuses de connexion à l'une ou l'autre interface. Parallèlement, les connexions de contrôle entre vManage, vSmarts et vBonds sont toujours établies.

Solution

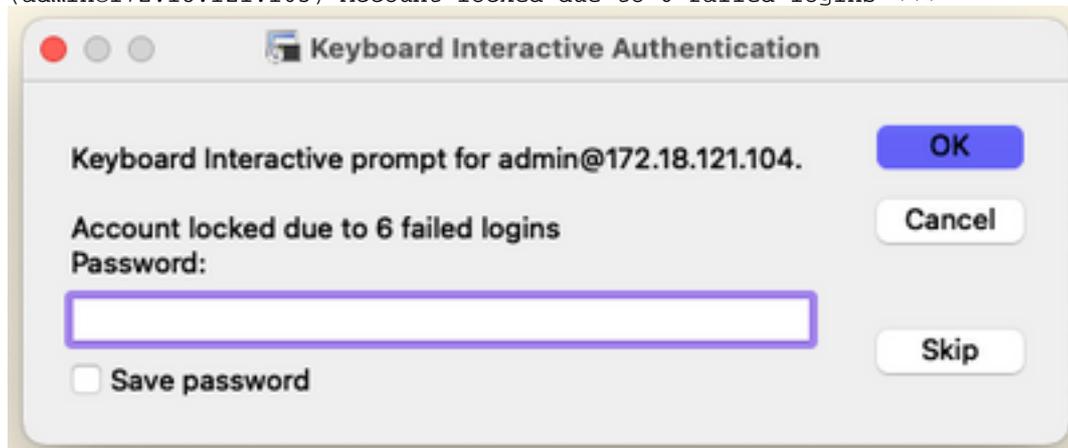
Étape 1. Déverrouillez les informations d'identification si nécessaire

Ces étapes vous aident à identifier un nom d'utilisateur verrouillé et comment les déverrouiller.

- Si le compte a été verrouillé en raison d'un nombre excessif de tentatives de connexion infructueuses, vous pouvez voir le message « Compte verrouillé en raison de X échecs de connexion » chaque fois que nous tapons le nom d'utilisateur.

```
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 <<<
```

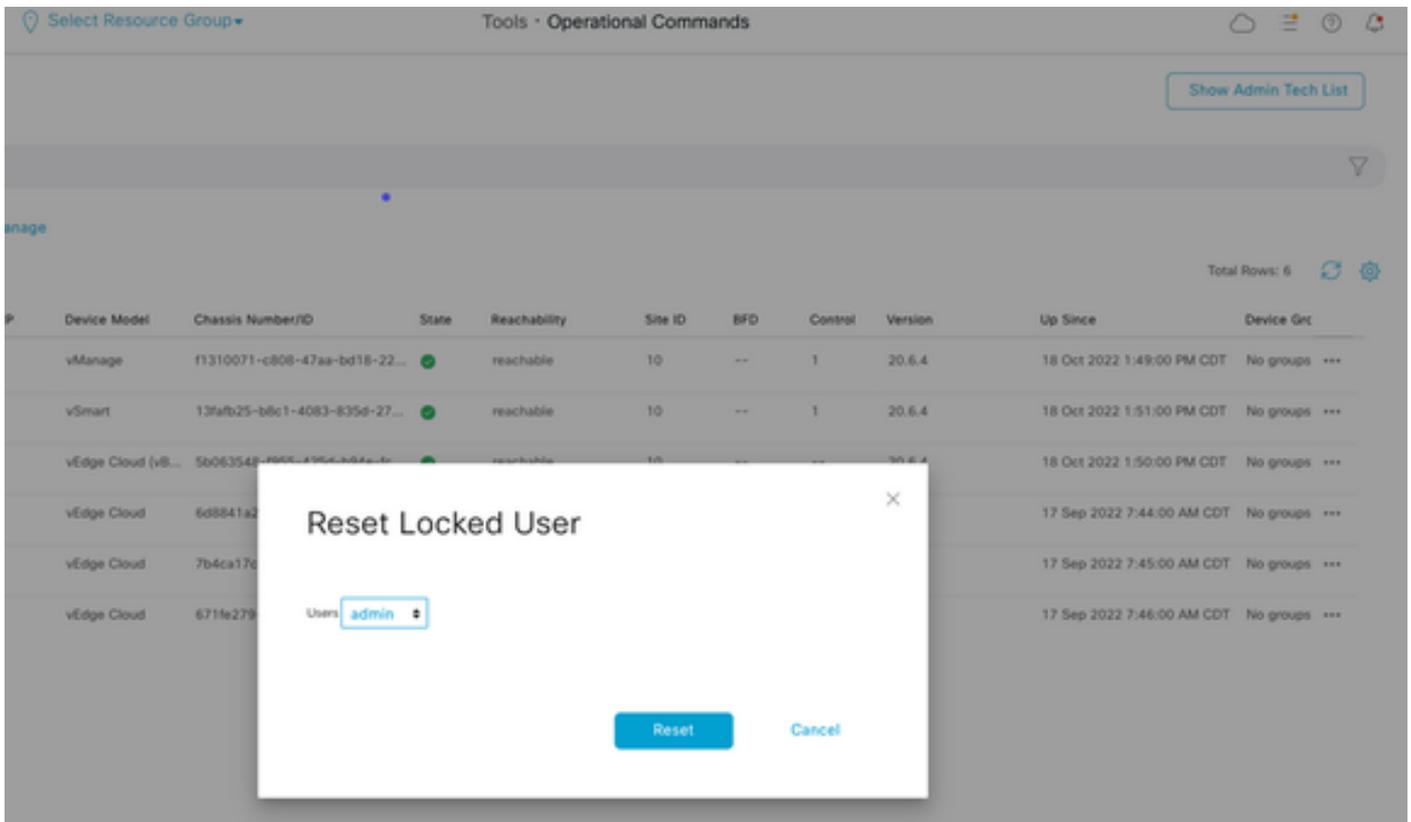


Option A. Déverrouiller les informations d'identification de l'interface graphique vManage

Après avoir confirmé que les informations d'identification sont verrouillées, vous devez les déverrouiller. vManage peut vous aider à effectuer cette opération facilement.

- Vous pouvez déverrouiller manuellement les informations d'identification depuis l'interface graphique utilisateur vManage pour tout périphérique.

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



Option B. Envoyez une requête SSH au périphérique qui a configuré une information d'identification supplémentaire

Si vous disposez d'une connectivité SSH avec des informations d'identification Netadmin supplémentaires dans le périphérique où vous confirmez que les informations d'identification sont verrouillées, vous pouvez toujours les déverrouiller de l'interface de ligne de commande.

- Vous pouvez exécuter la commande suivante :

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

- Si vous avez déverrouillé les informations d'identification et que la connexion échoue toujours, vous devez modifier le mot de passe.

Étape 2. Récupérer l'accès avec un modèle CLI

Vous devez créer les modèles CLI qui vous aident à modifier le mot de passe des périphériques. Si un modèle CLI est déjà créé et connecté au périphérique, vous pouvez passer à l'étape 3.

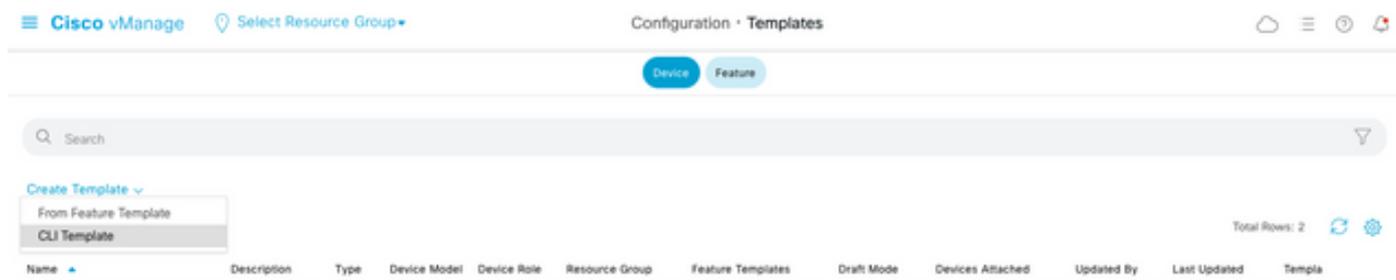
Option A. Charger la configuration en cours directement dans le modèle CLI

vManage permet de charger facilement la configuration en cours à partir des périphériques dans le modèle CLI.

Remarque : cette option ne peut pas être disponible en fonction de la version vManage. Vous pouvez consulter l'option B.

- Créer un nouveau modèle CLI

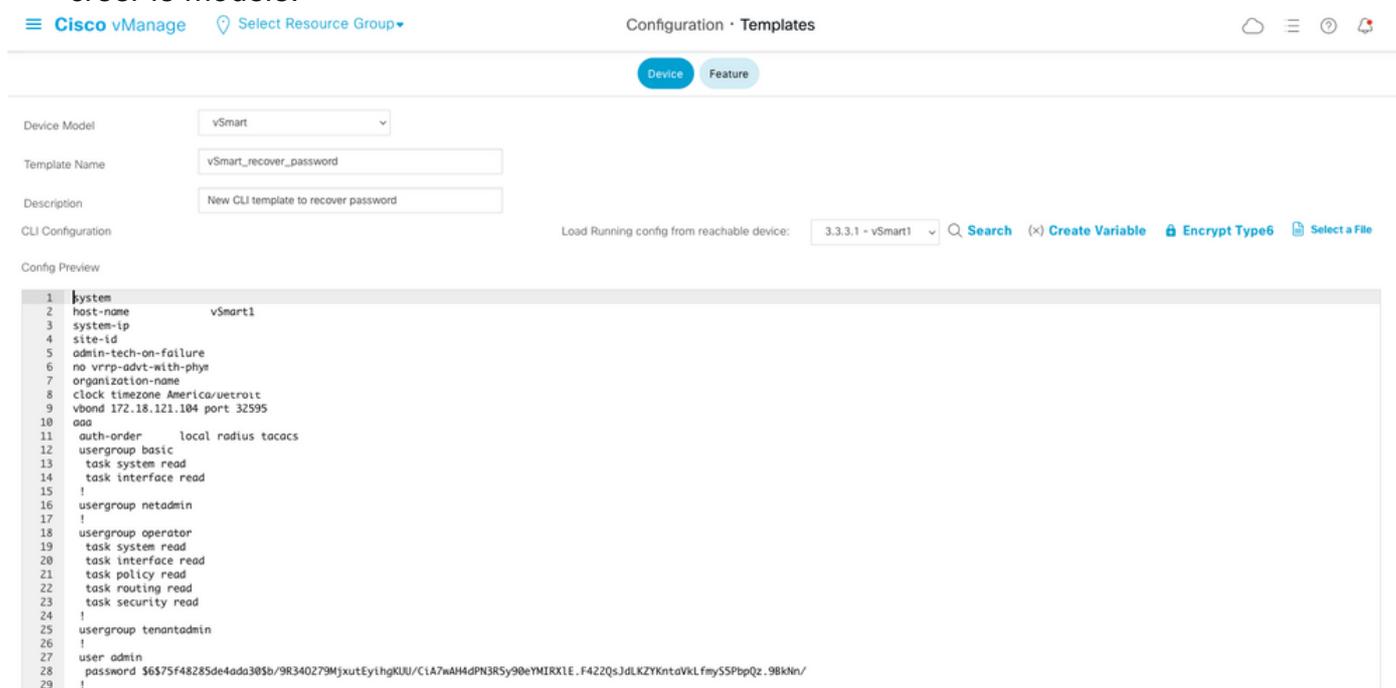
Naviguez jusqu'à vManage > Configuration > Templates > Create Template > CLI template



- En fonction du modèle de périphérique sélectionné, vous pouvez choisir à partir de quel périphérique le vManage charge la configuration en cours.

Load Running config from reachable device: 10.2.2.1 vSmart1

- Les valeurs Modèle de périphérique, Nom du modèle et Description doivent être saisies pour créer le modèle.



- Dès que la configuration est générée dans le modèle CLI, vous pouvez passer en revue l'étape 4 pour modifier le mot de passe.

Option B. Charger la configuration à partir de la base de données vManage

Si vous ne pouvez pas charger la configuration automatiquement dans l'interface de ligne de commande, vous pouvez toujours obtenir manuellement la configuration du périphérique et créer le modèle d'interface de ligne de commande à partir de ces informations.

- vManage dispose toujours d'une configuration de sauvegarde de tous les périphériques stockés dans sa base de données.

Accédez à vManage>Configuration>Controllers>Device> ... >Running Configuration>vManage>Configuration>Controllers>Device> ... >Local Configuration.

Remarque : exécution et configuration locale. L'exécution de la configuration signifie que vManage doit demander les informations de configuration du périphérique. Configuration locale signifie que vManage affiche les informations déjà stockées dans sa base de données.

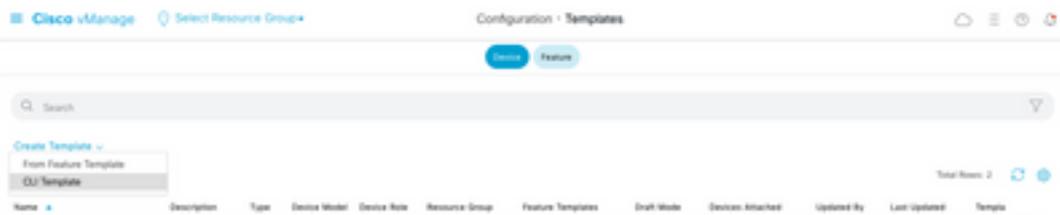
- Une fois la configuration locale affichée, vous pouvez copier toute la configuration dans un Bloc-notes.

Local Configuration

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

- Vous devez créer un nouveau modèle CLI.

Accédez à **vManage>Configuration>Templates>Create Template>CLI template.**



- Les valeurs Modèle de périphérique, Nom du modèle, Description et Aperçu de la configuration doivent être saisis pour créer le modèle. La configuration copiée à partir de la configuration locale doit être collée dans l'aperçu de la configuration.

Attention : pour vBond, vous devez sélectionner le cloud vEdge. Chaque autre périphérique a son propre modèle spécifique.

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-advrt-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

```

Étape 3. Nouvelles informations d'identification

Une fois le modèle créé, vous pouvez remplacer le mot de passe chiffré ou ajouter de nouvelles informations d'identification.

Option A. Modifier le mot de passe perdu

Vous pouvez modifier la configuration pour vous assurer d'utiliser un mot de passe connu.

- Vous pouvez mettre en surbrillance et remplacer le mot de passe chiffré par un mot de passe en clair.

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

Remarque : ce mot de passe en texte clair est chiffré après la diffusion du modèle.

Option B. Ajouter un nouveau nom d'utilisateur et un nouveau mot de passe avec les privilèges Netadmin

Si les modifications apportées au mot de passe ne sont pas autorisées, vous pouvez ajouter de nouvelles informations d'identification pour garantir l'accessibilité.

```
28      user admin
29      password $6$9d6a880c2a69979f$D1ag5jX.F279uqaRDxFNbCMICBy7hoWIFpd5Etp.AsYR7Taelc9d.jX4jV66yFKaYfcWTJPQ00qRiU79FbPd80
30      !
31      user admin2
32      password Cisc0123
33      group netadmin
34      !
```

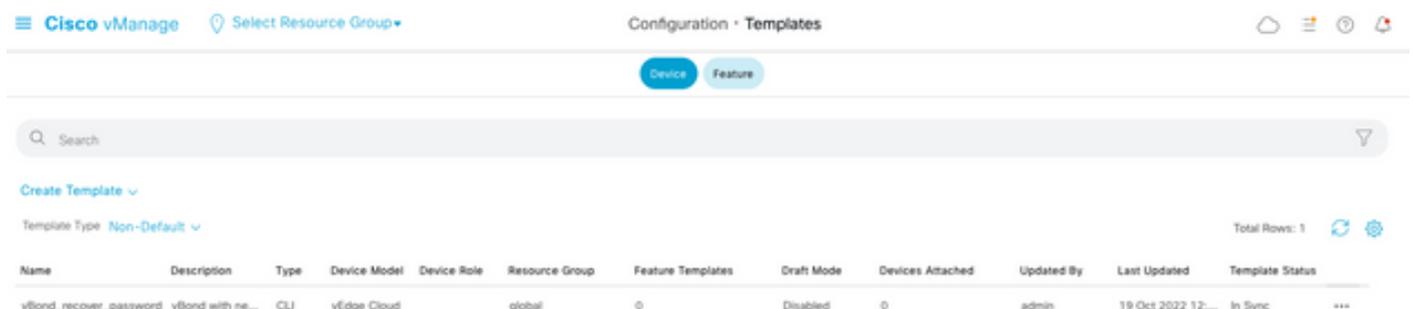
`user newusername < Creates username`
`password password < Creates the password`
`group netadmin < Assigns read-write privileges`

- Cliquez sur **Ajouter** pour **enregistrer** le modèle.

Étape 4. Diffusion du modèle vers le périphérique

L'étape suivante consiste à envoyer le modèle CLI au périphérique pour modifier la configuration en cours.

- Une fois le modèle enregistré, vous pouvez le joindre au périphérique.



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. The table has columns: Name, Description, Type, Device Model, Device Role, Resource Group, Feature Templates, Draft Mode, Devices Attached, Updated By, Last Updated, and Template Status. One template is listed: "vBond_recover_password" with description "vBond with ne...", type "CLI", device model "vEdge Cloud", resource group "global", feature templates "0", draft mode "Disabled", devices attached "0", updated by "admin", last updated "19 Oct 2022 12:...", and template status "In Sync".

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

Accédez à 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	

Minimum allowed: 1

Selected Devices Select All

All

Name	Device IP
------	-----------

- Cliquez sur **Attach** pour passer en revue l'aperçu de configuration.
- Lorsque vous cochez la case Config Diff, vous pouvez voir que le mot de passe a changé ou que les nouvelles informations d'identification ont été ajoutées.

Cisco vManage Select Resource Group Configuration - Templates

Device Template: vBond_recover_password Total: 1

Device list (Total: 1 devices)

Filter/Search

10043148-0910-4256-b94e-fc066e2f1c
vbond_20_8_A12.2.2.1

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-ghymae	7	no vrrp-advt-with-ghymae
8	sp-organization-name CISCOFTPLAB	8	sp-organization-name CISCOFTPLAB
9	organization-name CISCOFTPLAB	9	organization-name CISCOFTPLAB
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 1459d6a880c1a9979f01ag5jX.F279uqahDx7WbCK1Cy7h0WIFpd5EtP.AaYR7Tae1c9d.jK4jV6yFkaYicW7JpQ00gR1U79fhd80	30	password 1459d6a880c1a9979f01ag5jX.F279uqahDx7WbCK1Cy7h0WIFpd5EtP.AaYR7Tae1c9d.jK4jV6yFkaYicW7JpQ00gR1U79fhd80
		31	!
		32	user admin2
		33	password C1ae0123
		34	group netadmin
		35	!
31	!	36	ciscotacro-user true
32	ciscotacro-user true	37	ciscotacrv-user true
33	ciscotacrv-user true	38	!
34	!	39	logging
35	logging	40	disk
36	disk	41	enable
37	enable		

Configure Device Rollback Timer

Configure Devices Cancel

- Pour diffuser le modèle, cliquez sur **Configurer les périphériques**.
- Une fois que vManage a confirmé que la diffusion du modèle s'est terminée avec succès, vous pouvez utiliser vos nouvelles informations d'identification pour accéder au périphérique via SSH.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.