

# Wiederherstellung von SD-WAN vSmart und vBond Access

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem](#)

[Lösung](#)

[Schritt 1: Entsperren Sie ggf. die Anmeldeinformationen.](#)

[Option A. Entsperren von Anmeldeinformationen in der vManage-Benutzeroberfläche](#)

[Option B. SSH für das Gerät, das zusätzliche Anmeldeinformationen konfiguriert hat](#)

[Schritt 2: Wiederherstellen des Zugriffs mit einer CLI-Vorlage](#)

[Option A. Laden der aktuellen Konfiguration direkt in die CLI-Vorlage](#)

[Option B. Laden der Konfiguration aus der vManage-Datenbank](#)

[Schritt 3: Neue Anmeldeinformationen](#)

[Option A. Ändern des verlorenen Kennworts](#)

[Option B. Fügen Sie einen neuen Benutzernamen und ein neues Kennwort mit Netadmin-Berechtigungen hinzu.](#)

[Schritt 4: Template Push-to-Device](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Sie Ihren SD-WAN vSmart- und vBond-Zugriff wiederherstellen, nachdem Ihre Anmeldeinformationen verloren gegangen sind.

## Voraussetzungen

### Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Problem

Der Zugriff auf vBonds und vSmarts wurde unterbrochen. Dies geschieht, wenn Sie Ihre Anmeldeinformationen nicht kennen oder sich nicht daran erinnern, oder wenn der Zugriff nach überzogenen und erfolglosen Versuchen, sich bei einer der Schnittstellen anzumelden, gesperrt wird. Gleichzeitig sind die Steuerungsverbindungen zwischen vManage, vSmarts und vBonds weiterhin hergestellt.

## Lösung

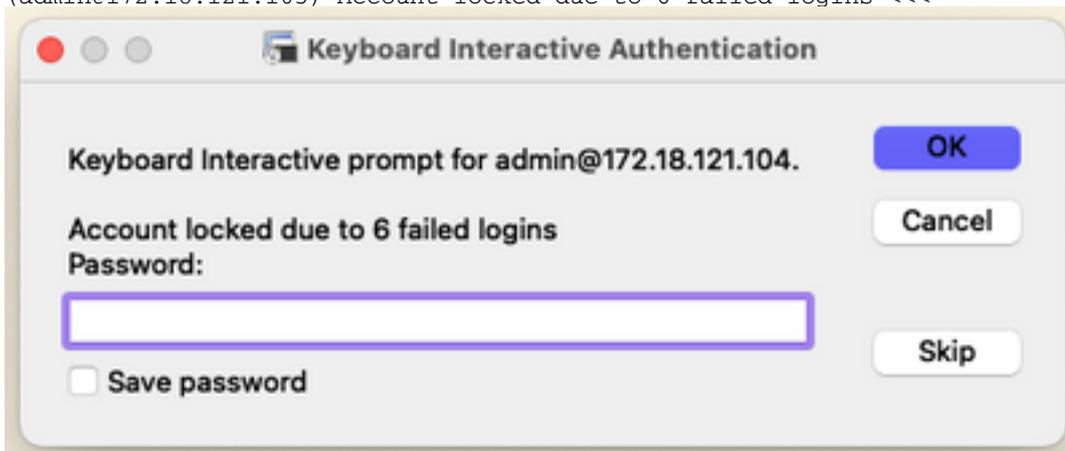
### Schritt 1: Entsperren Sie ggf. die Anmeldeinformationen.

Diese Schritte helfen Ihnen, einen gesperrten Benutzernamen zu identifizieren und diesen zu entsperren.

- Falls das Konto aufgrund übermäßiger fehlgeschlagener Anmeldeversuche gesperrt wurde, wird Ihnen bei jeder Eingabe des Benutzernamens die Meldung "Konto gesperrt aufgrund von X fehlgeschlagenen Anmeldungen" angezeigt.

```
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 <<<
```

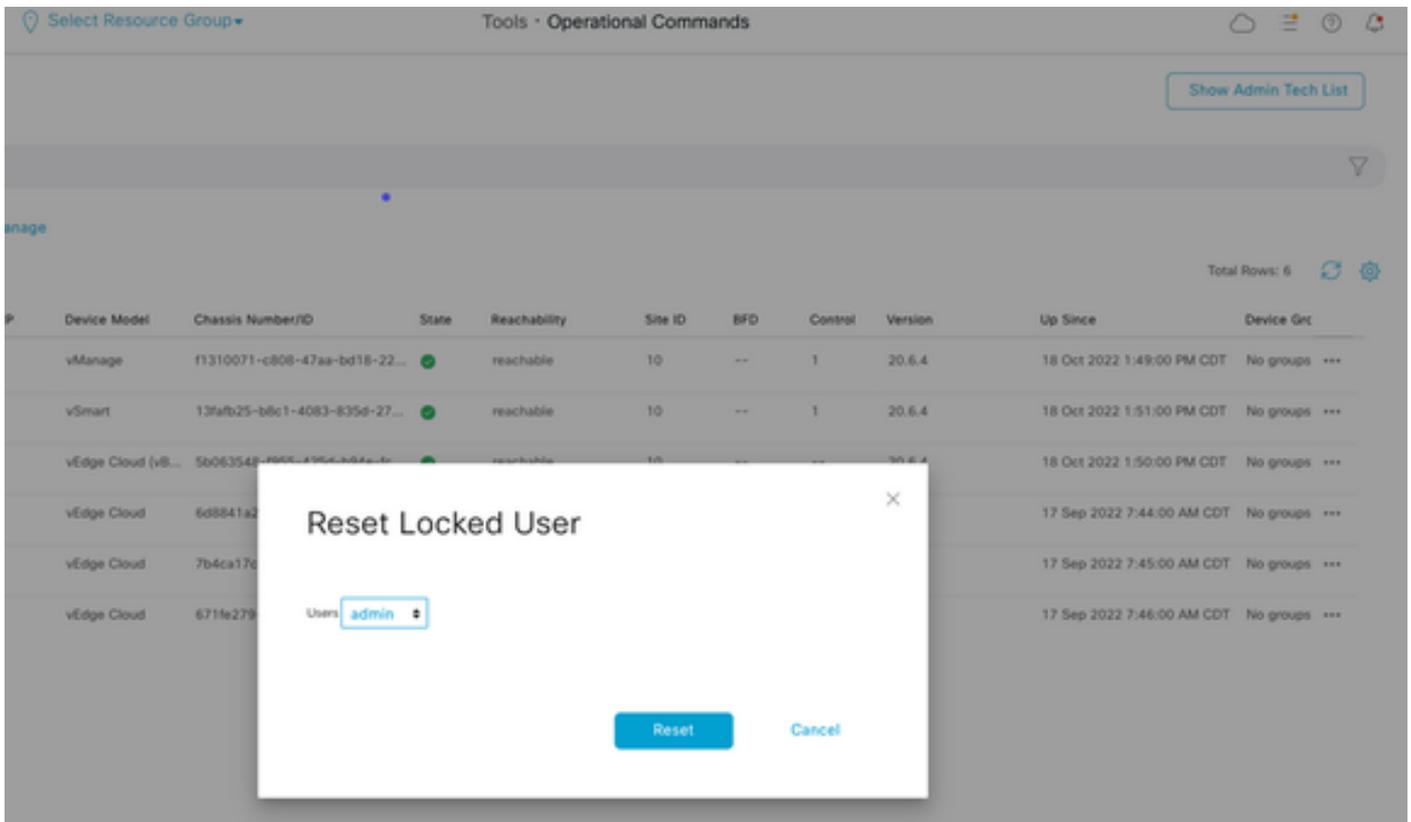


### Option A. Entsperren von Anmeldeinformationen in der vManage-Benutzeroberfläche

Nachdem Sie bestätigt haben, dass die Anmeldeinformationen gesperrt sind, müssen Sie sie entsperren. vManage kann Ihnen dabei helfen, diesen Vorgang einfach durchzuführen.

- Sie können die Anmeldeinformationen in der vManage-Benutzeroberfläche für jedes Gerät manuell entsperren.

Navigieren Sie zu **vManage > Tools > Operational Commands > Device > Reset Locked User > Select User > Reset**



## Option B. SSH für das Gerät, das zusätzliche Anmeldeinformationen konfiguriert hat

Falls Sie über SSH-Verbindungen mit zusätzlichen Netadmin-Anmeldeinformationen auf dem Gerät verfügen, auf dem Sie die gesperrten Anmeldeinformationen bestätigen, können Sie diese weiterhin über die CLI entsperren.

- Sie können den folgenden Befehl ausführen:

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

- Falls Sie die Zugangsdaten entsperren und die Anmeldung weiterhin fehlschlägt, müssen Sie das Kennwort ändern.

## Schritt 2: Wiederherstellen des Zugriffs mit einer CLI-Vorlage

Sie müssen die CLI-Vorlagen erstellen, mit denen Sie das Kennwort für die Geräte ändern können. Wenn bereits eine CLI-Vorlage erstellt und an das Gerät angehängt wurde, können Sie mit Schritt 3 fortfahren.

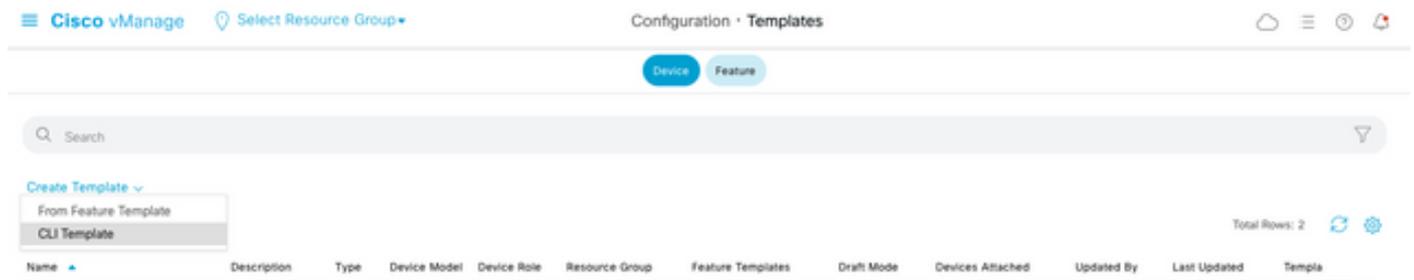
### Option A. Laden der aktuellen Konfiguration direkt in die CLI-Vorlage

In vManager kann die aktuelle Konfiguration ganz einfach von den Geräten in die CLI-Vorlage geladen werden.

**Hinweis:** Diese Option kann nicht basierend auf der vManage-Version verfügbar sein. Sie können Option B überprüfen.

- Erstellen einer neuen CLI-Vorlage

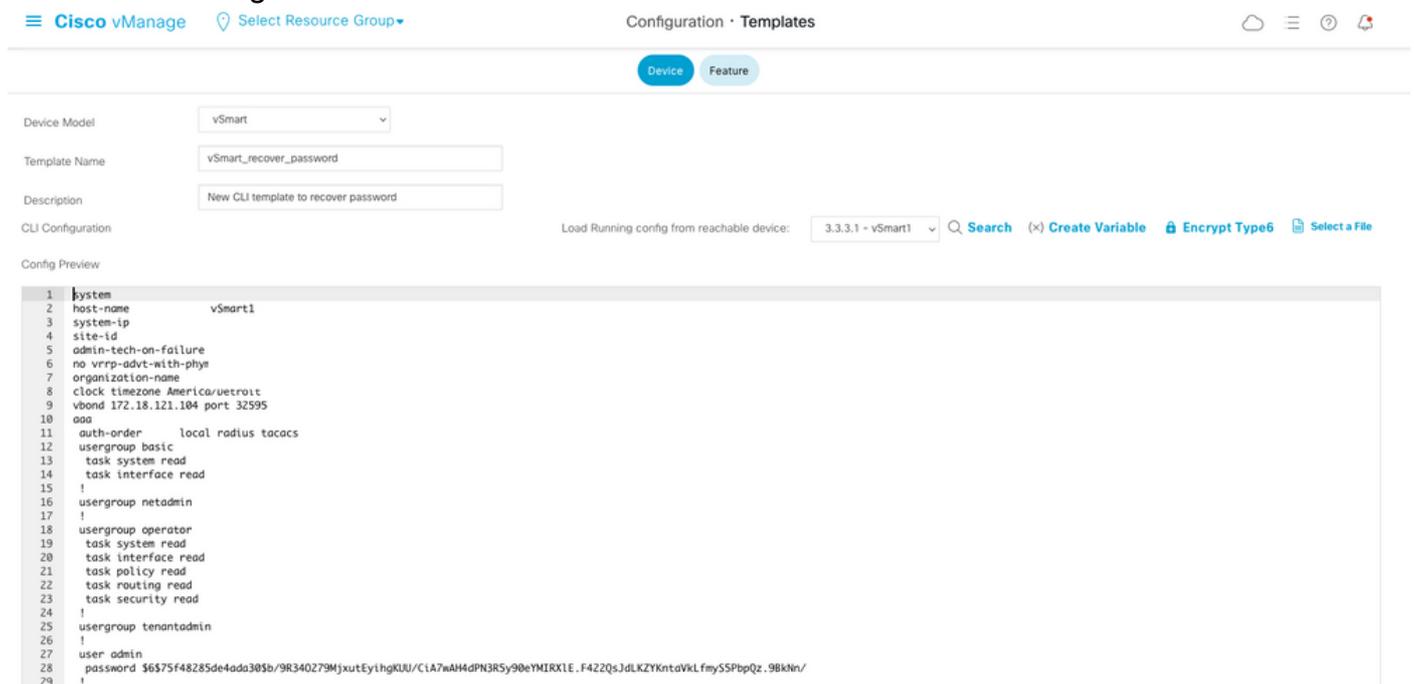
Navigieren Sie zu **vManage > Configuration > Templates > Create Template (vManage > Konfiguration > Vorlagen > Vorlage erstellen > CLI-Vorlage)**.



- Je nach gewähltem Gerätemodell können Sie auswählen, von welchem Gerät vManage die aktuelle Konfiguration lädt.

Load Running config from reachable device: 10.2.2.1 vSmart1

- Die Werte für Gerätemodell, Vorlagenname und Beschreibung müssen eingegeben werden, um die Vorlage zu erstellen.



- Sobald die Konfiguration in der CLI-Vorlage generiert wurde, können Sie Schritt 4 überprüfen, um das Kennwort zu ändern.

## Option B. Laden der Konfiguration aus der vManage-Datenbank

Falls Sie die Konfiguration nicht automatisch in die CLI laden können, können Sie die Konfiguration des Geräts trotzdem manuell abrufen und die CLI-Vorlage auf der Grundlage dieser Informationen erstellen.

- vManage verfügt immer über eine Backup-Konfiguration von allen Geräten, die in seiner Datenbank gespeichert sind.

Navigieren Sie zu **vManage>Configuration>Controllers>Device> ... >Running Configuration**  
**vManage>Configuration>Controllers>Device> ... >Local Configuration**.

**Hinweis:** Ausführen oder lokale Konfiguration "Konfiguration ausführen" bedeutet, dass der vManager die Konfigurationsinformationen für das Gerät anfordern muss. Lokale Konfiguration bedeutet, dass vManage die bereits in seiner Datenbank gespeicherten Informationen anzeigt.

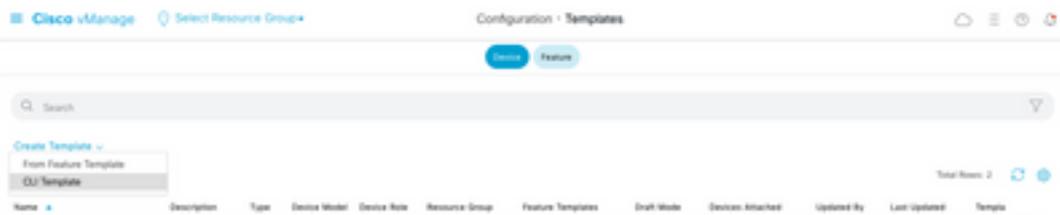
- Wenn die lokale Konfiguration angezeigt wird, können Sie die gesamte Konfiguration in ein NotePad kopieren.

## 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.jX4jV66yFKaYfcWTJPQ00qRiU79FbPd80
  !
  ciscotacro-user true
  ciscotacrw-user true
  !
logging
  disk
  enable
  !
  !
ntp
  parent
  no enable
```

- Sie müssen eine neue CLI-Vorlage erstellen.

Navigieren Sie zu **vManage>Configuration>Templates>Create Template>CLI template**.



- Die Werte für das Gerätemodell, den Vorlagennamen, die Beschreibung und die Konfigurationsvorschau müssen eingegeben werden, um die Vorlage zu erstellen. Die aus der lokalen Konfiguration kopierte Konfiguration muss in die Konfigurationsvorschau eingefügt werden.

**Achtung:** Für vBond müssen Sie vEdge cloud auswählen. Jedes andere Gerät hat sein eigenes spezifisches Modell.

Device Model:

Template Name:

Description:

CLI Configuration:

Load Running config from reachable device:

#### 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.F279uqaRDxFNbCMICBy7hoWIFpdSEtp.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

```

### Schritt 3: Neue Anmeldeinformationen

Nachdem die Vorlage erstellt wurde, können Sie das verschlüsselte Kennwort ersetzen oder neue Anmeldeinformationen hinzufügen.

### Option A. Ändern des verlorenen Kennworts

Sie können die Konfiguration ändern, um sicherzustellen, dass Sie ein bekanntes Kennwort verwenden.

- Sie können das verschlüsselte Kennwort markieren und durch ein unverschlüsseltes ersetzen.

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

**Hinweis:** Dieses unverschlüsselte Kennwort wird nach dem Push der Vorlage verschlüsselt.

### Option B. Fügen Sie einen neuen Benutzernamen und ein neues Kennwort mit Netadmin-Berechtigungen hinzu.

Wenn die Änderungen am Kennwort nicht zulässig sind, können Sie neue Anmeldeinformationen hinzufügen, um den Zugriff sicherzustellen.

```
28      user admin
29      password $6$9d6a880c2a69979f$D1ag5jX.F279uqaRDxFNBcMICBy7hoWIFpd5Etp.AsYR7Taelc9d.jX4jV66yFKaYfcWTJPQ00qRiU79FbPd80
30      !
31      user admin2
32      password Cisc0123
33      group netadmin
34      !
```

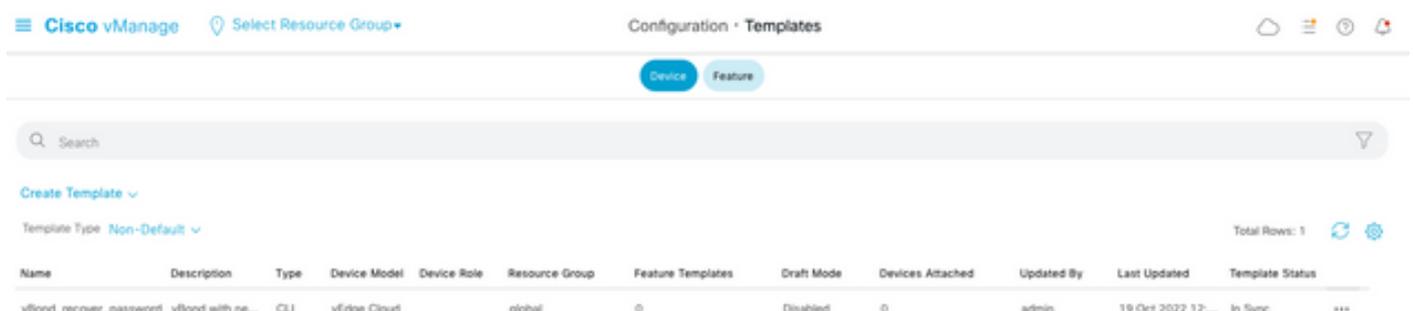
```
user newusername < Creates username
password password < Creates the password
group netadmin < Assigns read-write privileges
```

- Klicken Sie auf **Hinzufügen**, um die Vorlage zu **speichern**.

## Schritt 4: Template Push-to-Device

Der nächste Schritt besteht darin, die CLI-Vorlage an das Gerät zu senden, um die aktuelle Konfiguration zu ändern.

- Nachdem die Vorlage gespeichert wurde, können Sie sie an das Gerät anhängen.



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

Navigieren Sie zu **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
------	-----------

- **Klicken Sie auf Anfügen**, um die Konfigurationsvorschau anzuzeigen.
- Wenn Sie Config Diff (Konfigurationsdiff) überprüfen, sehen Sie, ob sich das Kennwort geändert hat oder ob die neuen Anmeldeinformationen hinzugefügt wurden.

Cisco vManage Select Resource Group Configuration - Templates

Device Template: vBond\_recover\_password Total: 1

Device list (Total: 1 devices)

10043148-0910-4256-b94e-fc066e2f1c  
vBond\_20\_8\_A12.2.2.1

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.F279uqahDx7WbCKICBy7h0WIFpd5EtP.AaYR7Tae1c9d.jK4jV6yFKaYicW7JPO0gR1U79FbD80	30	password 1459d6a880c1a9979f01ag5jX.F279uqahDx7WbCKICBy7h0WIFpd5EtP.AaYR7Tae1c9d.jK4jV6yFKaYicW7JPO0gR1U79FbD80
		31	!
		32	user admin2
		33	password C1ae0123
		34	group netadmin
31	!	35	!
32	ciscotacro-user true	36	ciscotacro-user true
33	ciscotacrv-user true	37	ciscotacrv-user true
34	!	38	!
35	logging	39	logging
36	disk	40	disk
37	enable	41	enable

Configure Device Rollback Timer

Configure Devices Cancel

- Klicken Sie auf **Geräte konfigurieren**, um die Vorlage zu **übertragen**.
- Nachdem vManage bestätigt hat, dass der Ttemplate-Push erfolgreich beendet wurde, können Sie Ihre neuen Anmeldeinformationen verwenden, um über SSH auf das Gerät zuzugreifen.

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.