

Récupération de mot de passe avec un modèle sur SD-WAN

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Étapes de récupération de mot de passe avec un modèle](#)

[Scénario 1. Périphérique avec connexions de contrôle actives et modèle joint](#)

[Scénario 2. Périphérique avec connexions de contrôle activées et sans modèle attaché](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes pour la récupération de mot de passe d'un périphérique avec un modèle dans un environnement de réseau étendu défini par logiciel (SD-WAN) de Cisco.

Conditions préalables

Exigences

Cisco vous recommande de connaître la solution SD-WAN de Cisco.

Composants utilisés

Les informations contenues dans ce document sont basées sur la version logicielle et matérielle suivante :

- vManage 20.6.4

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.

Informations générales

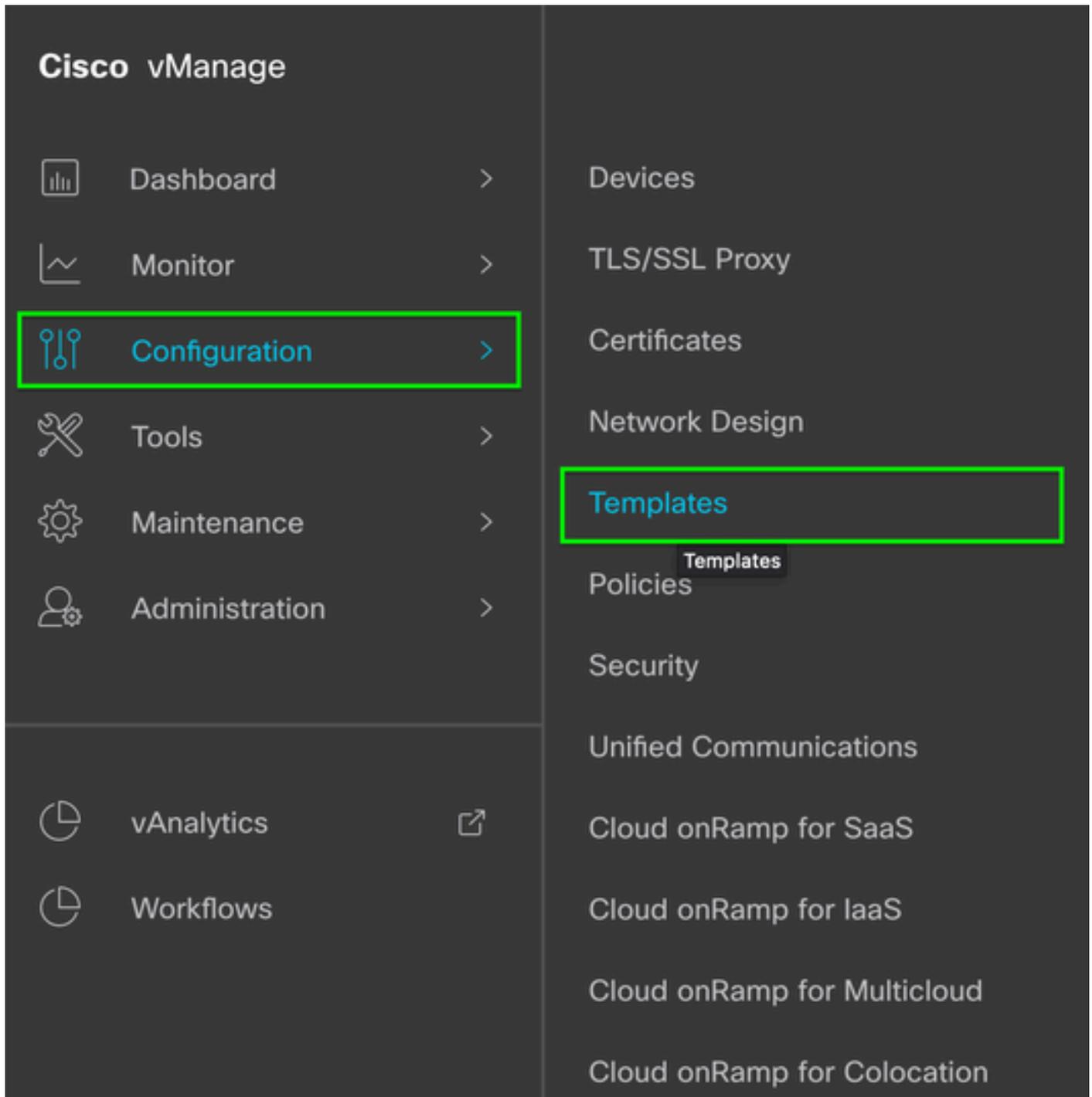
Le périphérique a été verrouillé après plusieurs tentatives de connexion infructueuses et reçoit le message indiquant que le compte est verrouillé.

Étapes de récupération de mot de passe avec un modèle

Voici deux scénarios qui peuvent être utilisés pour récupérer le mot de passe pour le ou les périphériques lorsque le compte est verrouillé.

Scénario 1. Périphérique avec connexions de contrôle activées et modèle joint

Étape 1. Dans le tableau de bord de l'interface graphique utilisateur vManage, accédez à Configuration > Templates.



Étape 2. Accédez à Device Template qui est connecté au périphérique.

Cisco vManage Select Resource Group Configuration · Templates

Device Feature

Search

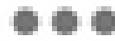
Create Template

Template Type Non-Default Total Rows: 20

Name	Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode	Devices
Basic_vEdge_Cloud_Template	This is a basic ...	Feature	vEdge Cloud	SDWAN Edge	global	16	Disabled	3

Étape 3. Sélectionnez ... à droite de la page, puis Afficher.

3



Edit

View

Delete

Copy

Attach Devices

Change Resource Group

Detach Devices

Export CSV

Change Device Values

Étape 4. Sous Informations de base, faites défiler la liste jusqu'à AAA. Copiez le nom du modèle de fonction. En haut de l'écran, cliquez sur Feature (Fonction).

The screenshot shows the Cisco vManage interface for configuring templates. At the top, the breadcrumb is 'Configuration > Templates'. There are two tabs: 'Device' and 'Feature', with 'Feature' selected. Below the tabs, there are four sub-sections: 'Basic Information', 'Transport & Management VPN', 'Service VPN', and 'Additional Templates'. The 'Basic Information' section is expanded, showing a list of templates. The 'AAA' template is highlighted with a green box. The 'Feature' tab is also highlighted with a green box. The 'Basic Information' section contains several dropdown menus for System, Logging, NTP, BFD, OMP, and Security.

Étape 5. Dans la zone de recherche, collez le nom du modèle de fonctionnalité AAA de l'étape 4 et entrez. Sélectionnez ... à droite de la page.

The screenshot shows the search results for the AAA template. The search bar contains the text 'Base_vEdge_AAA_Template'. Below the search bar, there is a table of results. The first row is highlighted, showing the details for the 'Base_vEdge_AAA_Template'.

Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated By	Last Updated
Base_vEdge_AA...	This is a base template fo...	AAA	vEdge Cloud	1	global	3	cofowler	19 Aug 2022 11:...

Étape 6. Dans la liste déroulante, sélectionnez Modifier.

19 Aug 2022 11: ...

View

Edit

Change Device Models

Change Resource Group

Delete

Copy

Étape 7. Sélectionnez Local, recherchez le nom d'utilisateur et cliquez sur l'icône Edit pour modifier le mot de passe.

Device Feature

Feature Template > AAA > Base_vEdge_AAA_Template

1.

Authentication Authorization Accounting Local RADIUS TACACS

USER		USER GROUP				
Cisco Tac Enable		<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write			
New User						
Optional	Username	Password	Description	Groups	Pubke	Action
<input type="checkbox"/>	<input type="text" value="admin"/>	<input type="password" value="....."/>	<input type="text"/>		<input checked="" type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="test"/>	<input type="password" value="....."/>	<input checked="" type="checkbox"/>	<input type="text" value="netadmin"/>	<input checked="" type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="test2"/>	<input type="password" value="....."/>	<input checked="" type="checkbox"/>	<input type="text" value="operator"/>	<input checked="" type="checkbox"/>	<input type="text"/>

Étape 8. Mettez à jour les informations de mot de passe, sélectionnez Save Changes, puis Update en bas de l'écran.

 Remarque : si un point d'exclamation est utilisé dans le mot de passe, le mot de passe entier doit être entouré de guillemets.

Update User

✕

 Mark as Optional Row ⓘName Password Description User Groups SSH RSA Key(s) (Maximum: 10) [+ Add](#)[Save Changes](#)[Cancel](#)

Device Feature

Feature Template > AAA > Base_vEdge_AAA_Template

Authentication Authorization Accounting Local RADIUS TACACS

USER USER GROUP

Cisco Tac Enable

 Read Write

New User

Optional	Username	Password	Description	Groups	Pubke	Action
<input type="checkbox"/>	admin			✓	✎
<input type="checkbox"/>	test	✓	netadmin	✓	✎ 🗑️
<input type="checkbox"/>	test2	✓	operator	✓	✎ 🗑️

RADIUS

Cancel

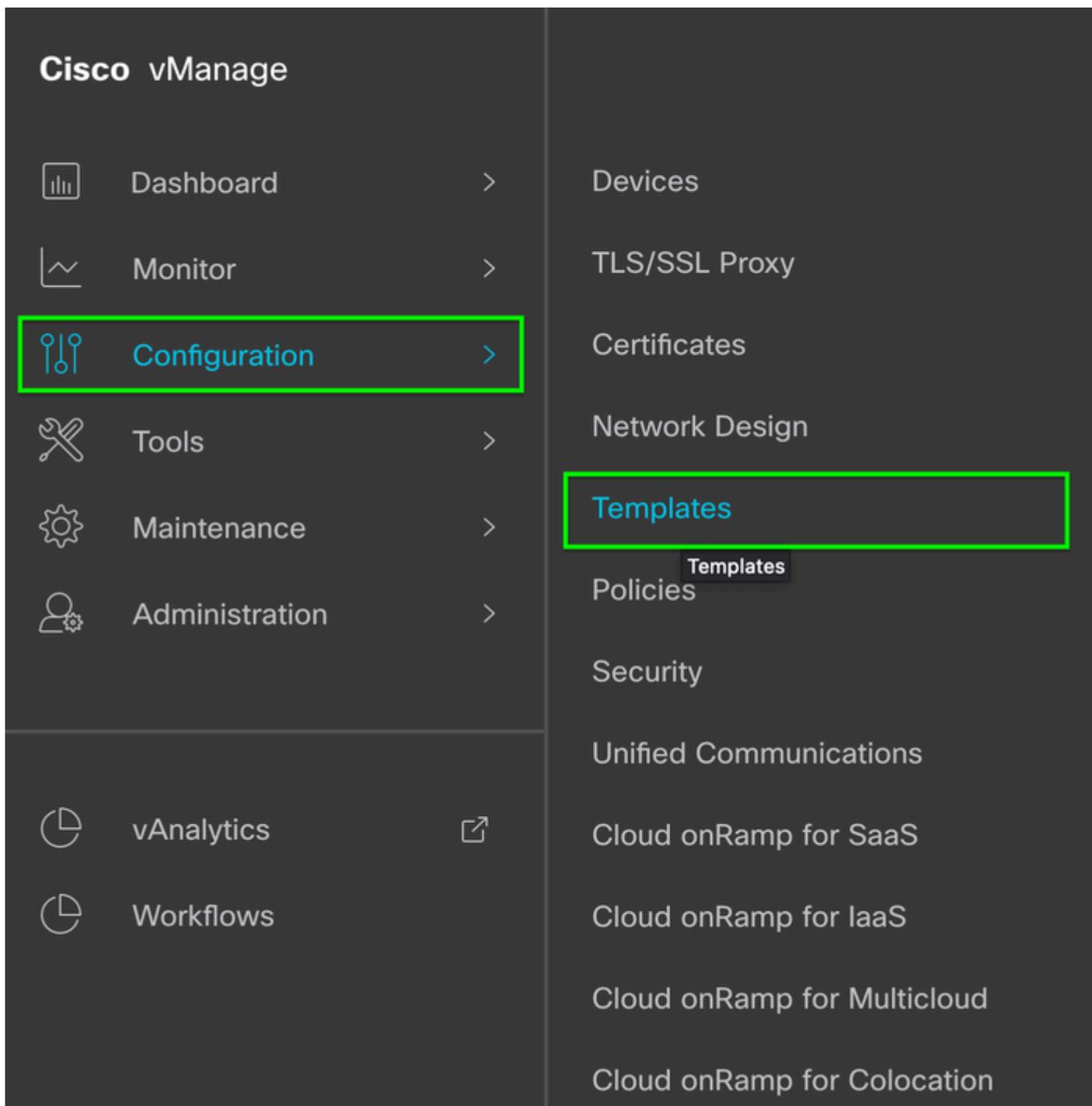
Update

Étape 9. Joignez le modèle mis à jour au périphérique.

Étape 10. Connectez-vous au périphérique avec le nouveau mot de passe créé à l'étape 8.

Scénario 2. Périphérique avec connexions de contrôle activées et sans modèle attaché

Étape 1. Dans le tableau de bord de l'interface graphique utilisateur vManage, accédez à Configuration > Templates.



Étape 2. Sélectionnez Fonction. Cliquez sur Ajouter un modèle.

Device Feature

Search

Add Template

Template Type Non-Default

Total Rows: 101



Name	Description	Type	Device Model	Device Templates	Resource Group	Devices Attached	Updated
------	-------------	------	--------------	------------------	----------------	------------------	---------

Étape 3. Sélectionnez le ou les modèles de périphériques. Sous Informations de base, sélectionnez AAA.

Feature Template > Add Template

Select Devices

vedge

- vEdge 100
- vEdge 100 B
- vEdge 100 M
- vEdge 100 WM
- vEdge 1000
- vEdge 2000
- vEdge 5000
- vEdge Cloud

Select Template

BASIC INFORMATION

AAA	Archive	BFD
NTP	OMP	Security
System		

Étape 4. Renseignez le Nom du modèle et la Description. Accédez à Local.

Device Type vEdge 100,vEdge 100 B,vEdge 100 M,vEdge 100 WM,vEdge 1000,vEdge 2000,vEdge 5000,vEdge Cloud

Template Name	vEdge_AAA_Template
Description	This is a basic AAA template for all vEdge Devices

Authentication Authorization Accounting **Local** RADIUS TACACS

✓ AUTHENTICATION

Étape 5. Cliquez sur Nouvel utilisateur, complétez les champs Nom, Mot de passe et Groupes d'utilisateurs. Cliquez sur Add.

 Remarque : si vous utilisez un point d'exclamation dans votre mot de passe, le mot de passe entier doit être entouré de guillemets.

LOCAL

USER USER GROUP

Cisco Tac Enable Read Write

1. [New User](#)

2.

Name	test
Password	*****
Description	
User Groups	Select groups... netadmin basic operator

SSH RSA Key(s) (Maximum: 10)

Mark as Optional Row ⓘ

3. [Add](#) [Cancel](#)

Étape 6. Vérifiez le nouvel utilisateur créé à l'étape 5. Cliquez sur Save.

The screenshot shows the Cisco vManage Configuration - Templates interface. The breadcrumb trail is: Feature Template > Add Template > AAA. The main navigation tabs are Authentication, Authorization, Accounting, Local, RADIUS, and TACACS. The 'LOCAL' section is expanded, showing a 'USER' table with columns: Optional, Username, Password, Description, Groups, Pubkey Chain, and Action. Two users are listed: 'admin' and 'test'. The 'test' user row is highlighted with a green border. Below the LOCAL section is the 'RADIUS' section, which includes input fields for 'Retransmit Count' and 'Timeout', both set to '5'. A 'New RADIUS Server' button is present. Below the RADIUS section is a table with columns: Optional, Tag, IP Address, Accounting Port, Authentication Port, Key (Deprecated), Secret Key, Source Interface, VPN, Priority, and Action. The table is currently empty, with the text 'No data available' displayed. At the bottom of the RADIUS section are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted in green.

Étape 7. Fixez le modèle AAA à un modèle de périphérique et poussez le modèle.

Étape 8. Pour créer le reste du modèle de périphérique, accédez à Cisco SD-WAN Release 20.x - Configure devices.

Étape 9. Connectez-vous au périphérique avec le nouveau nom d'utilisateur et le nouveau mot de passe de l'étape 5.

Informations connexes

- [Guide de configuration des interfaces et systèmes SD-WAN Cisco, Cisco IOS XE version 17.x](#)
- [Guide de configuration des systèmes et des interfaces, Cisco SD-WAN version 20.x](#)
- [Assistance et documentation techniques - Cisco Systems](#)

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.