

# Perform Password Recovery with a Template on SD-WAN

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Password Recovery Steps with a Template](#)

[Scenario 1. Device with Control Connections Up, and an Attached Template](#)

[Scenario 2. Device with Control Connections Up, and no Attached Template](#)

[Related Information](#)

## Introduction

This document describes the steps for password recovery of a device with a template in a Cisco Software Defined Wide Area Network (SD-WAN) environment.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of the Cisco SD-WAN solution.

### Components Used

The information in this document is based on this software and hardware version:

- 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. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

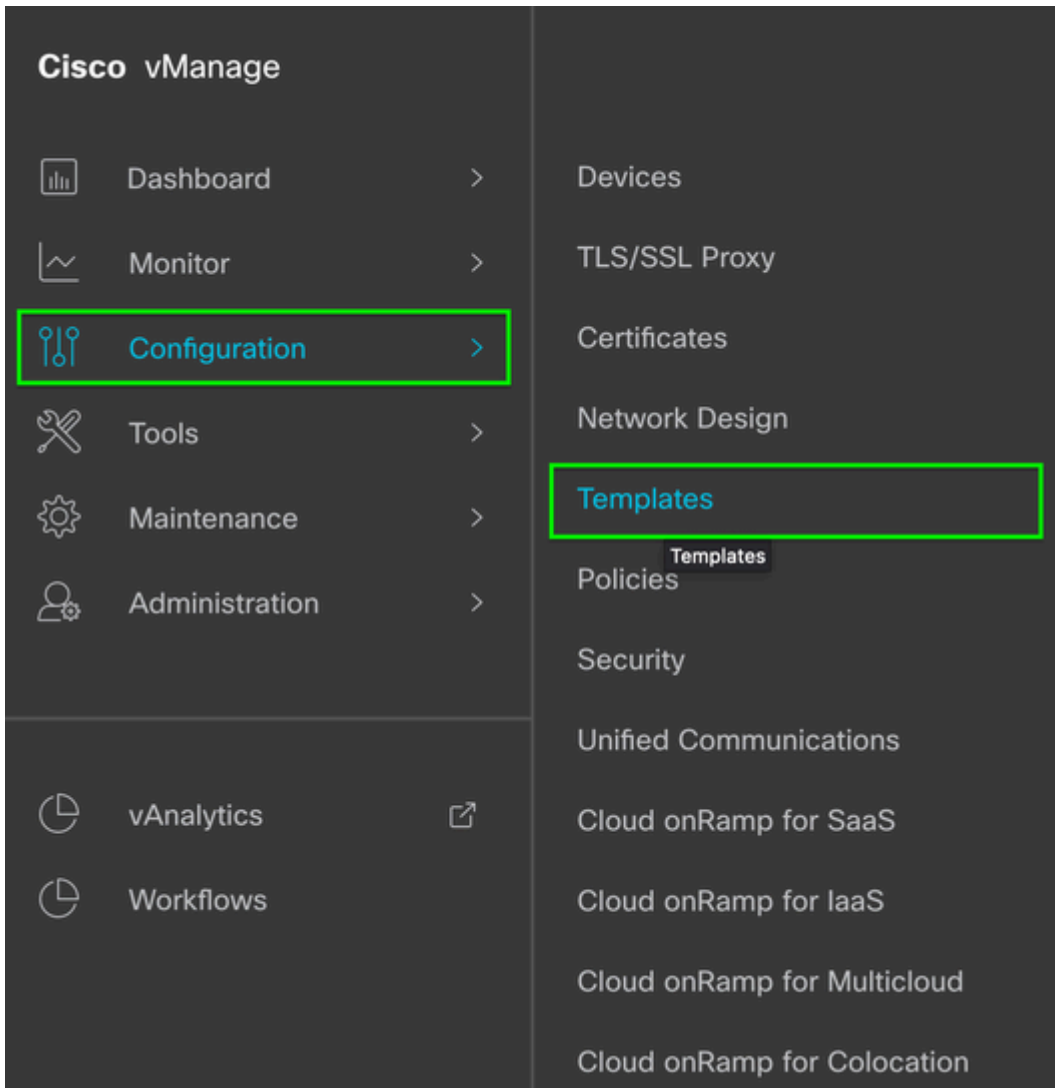
Device has been locked out after multiple failed login attempts and receives the message that the account is locked.

## Password Recovery Steps with a Template

Here are two scenarios that can be utilized to recover the password for the device(s) when the account is locked out.

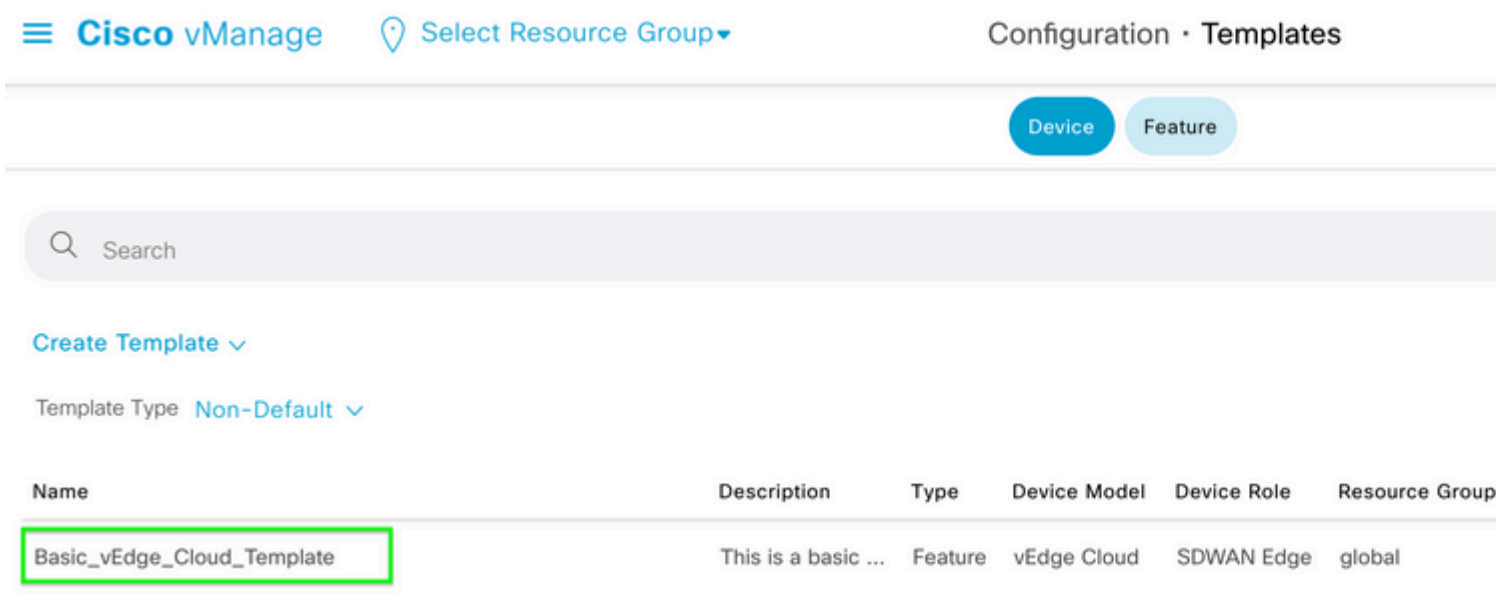
### Scenario 1. Device with Control Connections Up, and an Attached Template

Step 1. From the vManage GUI Dashboard, navigate to **Configuration > Templates**.



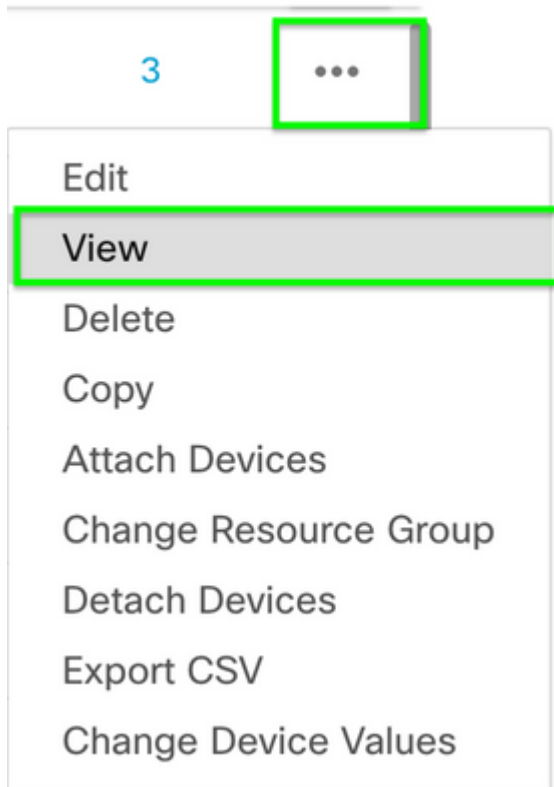
â€f

Step 2. Navigate to **Device Template** that is attached to the device.



â€f

Step 3. Select ... on the right side of the page and then select **View**.



â€f

Step 4. Under **Basic Information**, scroll down until you see **AAA**. Copy the **Feature Template** name. At the top of the screen, click **Feature**.

Device

Feature

1.

Basic Information

Transport & Management VPN

Service VPN

Additional Templates

### Basic Information

System \*

System\_Template

Logging\*

Factory\_Default\_Logging\_Template\_V01

NTP

NTP\_Server\_Template

2.

AAA

Base\_vEdge\_AAA\_Template

BFD \*

OMP \*

Factory\_Default\_vEdge\_OMP\_Template

Security \*

â€f

Step 5. In the **Search** box, paste the **AAA Feature Template** name from **Step 4** and **Enter**. Select **...** on the right side of the page.

Device

Feature

Base\_vEdge\_AAA\_Template × Search

## Add Template

Template Type Non-Default

Name	Description	Type	Device Model	Device Templates	Resource Group
Base_vEdge_AA...	This is a base template fo...	AAA	vEdge Cloud	1	global

â€f

Step 6. From the drop down, select **Edit**.

19 Aug 2022 11: ...

View

Edit

Change Device Models

Change Resource Group

Delete

Copy

â€f

Step 7. Select **Local**, locate the **Username**, and click the **Edit Icon** to edit the password.

Device

Feature

Feature Template &gt; AAA &gt; Base\_vEdge\_AAA\_Template

1.

Authentication

Authorization

Accounting

Local

RADIUS

TACACS

USER

USER GROUP

Cisco Tac Enable



Read



Write

New User

Optional	Username	Password	Description	Groups
<input type="checkbox"/>	<input type="text" value="admin"/>	<input type="password"/>		
<input type="checkbox"/>	<input type="text" value="test"/>	<input type="password"/>	<input checked="" type="checkbox"/>	<input type="text" value="netad"/>
<input type="checkbox"/>	<input type="text" value="test2"/>	<input type="password"/>	<input checked="" type="checkbox"/>	<input type="text" value="oper"/>

2.

â€f

Step 8. Update the **Password** information, select **Save Changes**, and then **Update** at the bottom of the screen.

**Note:** If an exclamation point is used in the password, the entire password must be surrounded by quotation marks.

# Update User

Name

Password

Description

User Groups

SSH RSA Key(s) (Maximum: 10)

[+ Add](#)

â€f

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
<input type="checkbox"/>	<input type="text" value="admin"/>	<input type="password"/>		
<input type="checkbox"/>	<input type="text" value="test"/>	<input type="password"/>	<input checked="" type="checkbox"/>	<input type="text" value="netadmin"/>
<input type="checkbox"/>	<input type="text" value="test2"/>	<input type="password"/>	<input checked="" type="checkbox"/>	<input type="text" value="operator"/>

✓ RADIUS

Cancel

Update

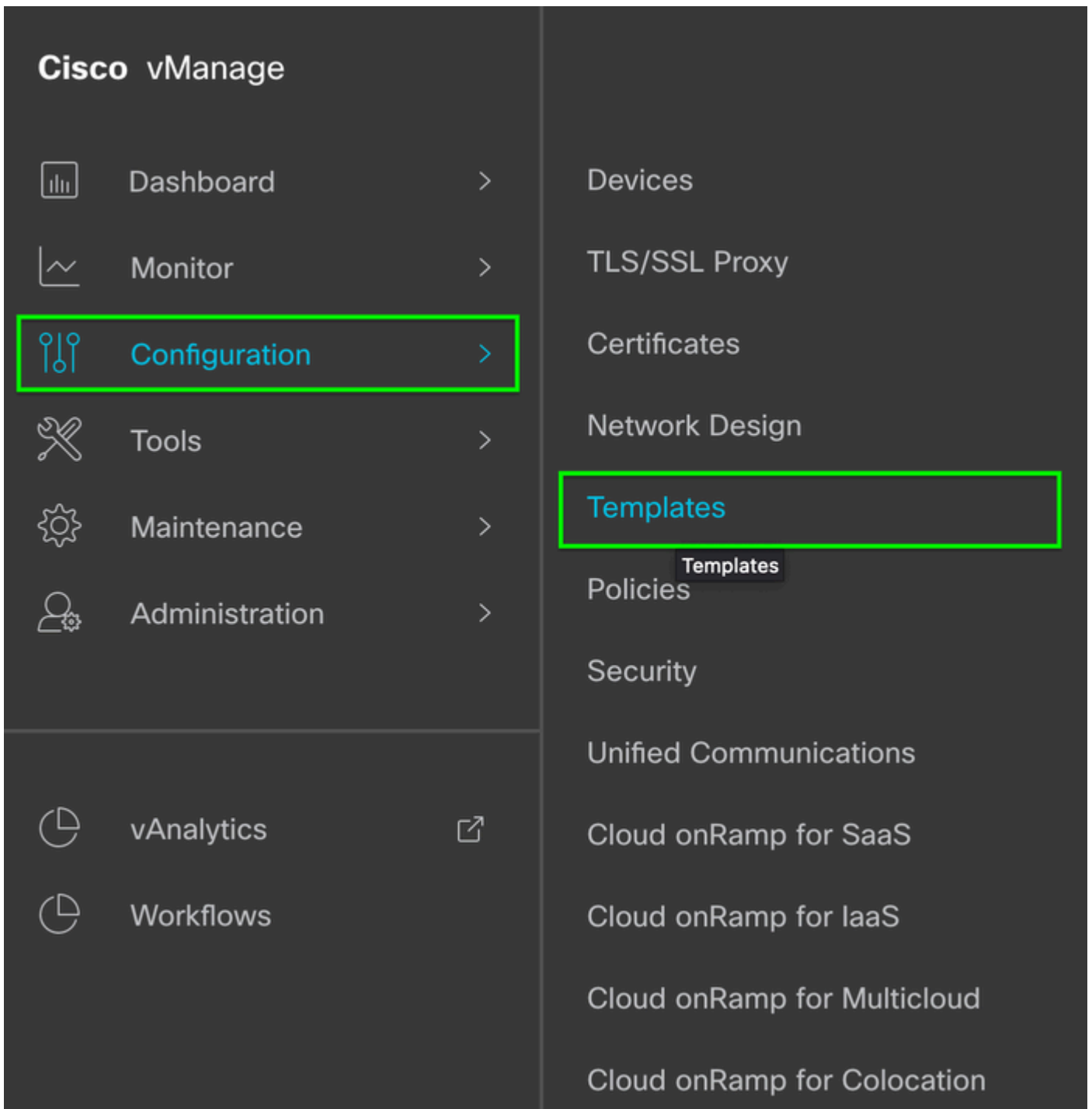
Step 9. Proceed to attach the updated template to the device.

Step 10. Login to the device with the new password created in Step 8.

### Scenario 2. Device with Control Connections Up, and no Attached Template

Step 1. From the vManage GUI Dashboard, navigate to Configuration > Templates.





â€f

â€f

Step 2. Select **Feature**. Click **Add Template**.

Device

Feature

🔍 Search

Add Template

Template Type Non-Default ▾

Name

Description

Type

Device Model

Device Templates

Resource Group

D

â€f

Step 3. Select the **Device Model(s)**. Under **Basic Information**, select **AAA**.

Select Devices

Q 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
NTP	OMP
System	

Step 4. Fill in the **Template Name** and **Description**. Navigate to **Local**.

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

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

Authentication

Authorization

Accounting

Local

RADIUS

TACACS

∨ AUTHENTICATION

Step 5. Click **New User**, fill in the **Name**, **Password**, and **User Groups**. Click **Add**.

â€f

**Note:** If you use an exclamation point in your password, the entire password must be surrounded by quotation marks.

∨ 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)

Step 6. Verify the **New User** created in **Step 5**. Click **Save**.

Device Feature

Feature Template &gt; Add Template &gt; AAA

Authentication Authorization Accounting Local RADIUS TACACS

LOCAL

USER USER GROUP

Cisco Tac Enable

Read Write

New User

Optional	Username	Password	Description	Groups
<input type="checkbox"/>	<input type="text" value="admin"/>	<input type="password" value=""/>		
<input type="checkbox"/>	<input type="text" value="test"/>	<input type="password" value=""/>	<input type="text" value=""/>	<input type="text" value="netadmin"/>

RADIUS

Retransmit Count

Timeout

New RADIUS Server

Optional	Tag	IP Address	Accounting Port	Authentication Port	Key (Deprecated)	Secret Key
No data available						

Cancel

Save

â€f

Step 7. Attach the **AAA Template** to a **Device Template** and push the template.

Step 8. To create the rest of the device template, navigate to [Cisco SD-WAN Release 20.x - Configure devices](#).

Step 9. Login to the device with the new username and password from Step 5.

## Related Information

- [Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x](#)
- [Systems and Interfaces Configuration Guide, Cisco SD-WAN Release 20.x](#)
- [Technical Support & Documentation - Cisco Systems](#)