

# Troubleshoot vSmart Policy Push Activation Errors

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[vManage Mode](#)

[Solution](#)

[Site-IDs Overlap](#)

[Solution](#)

[Add VPN List or Site List](#)

[Solution](#)

[SLA Class](#)

[Solution](#)

[Related Defects](#)

## Introduction

This document describes some common errors seen during the activation of a vSmart Policy from vManage in a Software Device Wide Area Network (SD-WAN).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of Cisco Software Defined Wide Area Network (SDWAN) solution.

### 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.

## vManage Mode

During the activation of a vSmart policy, a pop-up shows this error, where the x.x.x.x represents the vSmart system-ip:

### Failed to activate policy

vSmarts x.x.x.x are not in vManage mode

## Solution

All vSmarts in the overlay (reachable and unreachable) need to be on a template (vManage mode) in order to apply a centralized policy from the vManage Graphical User Interface (GUI). Cisco advises the vSmarts to have the same configuration with the exception of device specific details, such as system-ip, hostname, and site-id. Therefore, a simple solution to this error is to create a CLI template and make the few device specific details into variables. This ensures the vSmarts always have same configuration with the exception of those device specific variables.

## Site-IDs Overlap

After the Save **Policy** button or the **Preview** button is clicked, this error is seen:

```
Invalid policy: Assembly failed. Duplicate mapping detected on site#type#direction  
Branch#control#out
```

OR

During the activation and push of the vSmart policy, this error is seen:

```
15-Aug-2022 20:12:11 EDT] Failed to apply policy - Failed to process device request -  
Error type : application  
Error tag : operation-failed  
Error Message : /apply-policy/site-list[name='All-Site']: Overlapping apply-policy site-list Hub  
site id 200-299 with site-list All-Site  
Error info : <error-info>  
  <bad-element>site-list</bad-element>  
</error-info>
```

## Solution

If the same policy type is applied to two site-lists that contain any of the same site IDs, then this error is seen. Only one type of policy can be applied per direction to a specific site. Ensure that the site IDs across the site lists are unique.

- For Application-Aware Routing (AAR) policies, there is no direction. Only one AAR policy can be applied to a specific site.
- For Centralized Control policies, there are two possible directions, **in** and **out**. Two control policies can be applied to a specific site-id as long as one is applied in the **out** direction, and the second is applied in the **in** direction.
- For Centralized Data policies, there are three direction options, **all**, **from-service** and **from-tunnel**. Two data policies can be applied to a specific site-id as long as one is applied in the **from-tunnel** direction and the second is applied in the **from-service** direction. If the **all** direction is used to apply one data policy, then a second data policy cannot be applied to that

site. In some use cases, some sequences need to be applied both **from-service** and **from-tunnel**, but others need to be only applied in one direction. For these use cases, create a policy for all common sequences, and make a copy of it. Add direction specific sequences to the copy. Then apply the original policy in one direction and the copy with addition sequences in the other direction.

## Add VPN List or Site List

After a new policy type is added to a current Centralized policy, this error is seen after Save Policy Changes button is selected:

```
Invalid policy:Cannot save policy. Add VPN List or Site List to component Generic_Policy in Policy Application
```

### Solution

The policy needs to be applied to a specific site list in order to save the policy.

- For Centralized Control policies, only a direction and site list are required during the apply-policy section.
- For AAR policies, site list and vpn list are required during the apply-policy section.
- For Centralized Data policies, site list and vpn list are required during the apply-policy section.

## SLA Class

During the activation or removal of a vSmart policy, this error is seen. The numbers in the error message can vary based on the code version.

```
too many /ncs:devices/device{vsmart-}/config/policy/sla-class, 5 configured, at most 4 must be configured
```

### Solution

The number of SLA classes supported varies between different releases. If the vManage and vSmart are on a higher release train than the edge device, its possible that they allow the configuration of more than the edge device can support. The application of more SLA classes than the edge device supports can have unintended consequences.

Ensure that the number configured are within the confines of the allowed number of SLA classes for the code version the device is on.

The respective documentation can be found:

[vEdge Documentation](#)

[Cisco IOS-XE Controller Mode \(cEdge\) Documentation](#)

## Related Defects

Cisco bug ID [CSCwc08313](#) - System does not throw an error message for the policies that overlap in some cases.