Configure and Verify DIA NAT Tracker and Fallback

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Restrictions for NAT DIA Tracker
  - Restrictions forCisco IOS XE Catalyst SD-WAN Release 17.10.1a and Earlier Releases
  - Restrictions forCisco IOS XE Catalyst SD-WAN Release 17.11.1a
  - Restrictions forCisco IOS XE Catalyst SD-WAN Release 17.13.1a
- Supported Interfaces for NAT DIA Tracker

Configure

- Network Diagram
- Configurations
- Step 1. Configure NAT DIA Tracker
- Step 2. Bind the Tracker to Transport Interface
- Step 3. Enable NAT Fallback on Existing DIA Policy

Verify

Troubleshooting Tracker

Related Information

Introduction

This document describes how to configure and verify DIA NAT Tracker and Fallback on CIsco IOS® XE routers using Cisco Catalyst Manager GUI.

Prerequisites

Requirements

Cisco SD-WAN NAT DIA policy must be configured on branch devices. Please check the Related Information section for instructions on how to Implement Direct Internet Access (DIA) for SD-WAN.

Components Used

This document is based on these software and hardware versions:

- Cisco Catalyst SD-WAN Manager version 20.14.1
- Cisco Catalyst SD-WAN Controller version 20.14.1
- Cisco Edge Router version 17.14.01a

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.

Restrictions for NAT DIA Tracker

Restrictions for Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Earlier Releases

- In Cisco IOS XE Release 17.6.x and earlier, the NAT DIA tracker is not supported on dialer interfaces. From Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, subinterfaces and dialer interfaces support single endpoint and dual endpoint trackers.
- DNS URL endpoint is not supported on Cisco IOS XE Catalyst SD-WAN devices.
- You can only apply one tracker or tracker group to an interface.
- The NAT fallback feature is supported only from Cisco IOS XE Catalyst SD-WAN Release 17.3.2.
- The IP address of the tunnel with address 169.254.x.x is not supported to track the zScaler endpoint on manual tunnels.
- You must configure a minimum of two single endpoint trackers to configure a tracker group.
- A tracker group can incorporate only a maximum of two single endpoint trackers.
- In Cisco IOS XE Release 17.10.1 and previous releases, you cannot configure IPv4 tracker on a IPv6 interface or vice versa. The tracker wont be active.

Restrictions for Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

- API URL endpoint is supported only on IPv6 DIA tracker and not supported on IPv4 DIA tracker.
- Both IPv4 and IPv6 trackers cannot be used in the same tracker group.
- You must configure the **allow service all** command under the TLOC tunnel interface for IPv6 trackers to work with a TLOC tunnel interface.
- Multiple NAT66 DIA interfaces are not supported.

Restrictions for Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

- Name resolution process is not bond to the ET interface. Name resolution is using VPN 0 routing table. It can exit any active interface with proper routing.

Supported Interfaces for NAT DIA Tracker

You can configure the NAT DIA tracker for the these interfaces:

- Cellular Interfaces

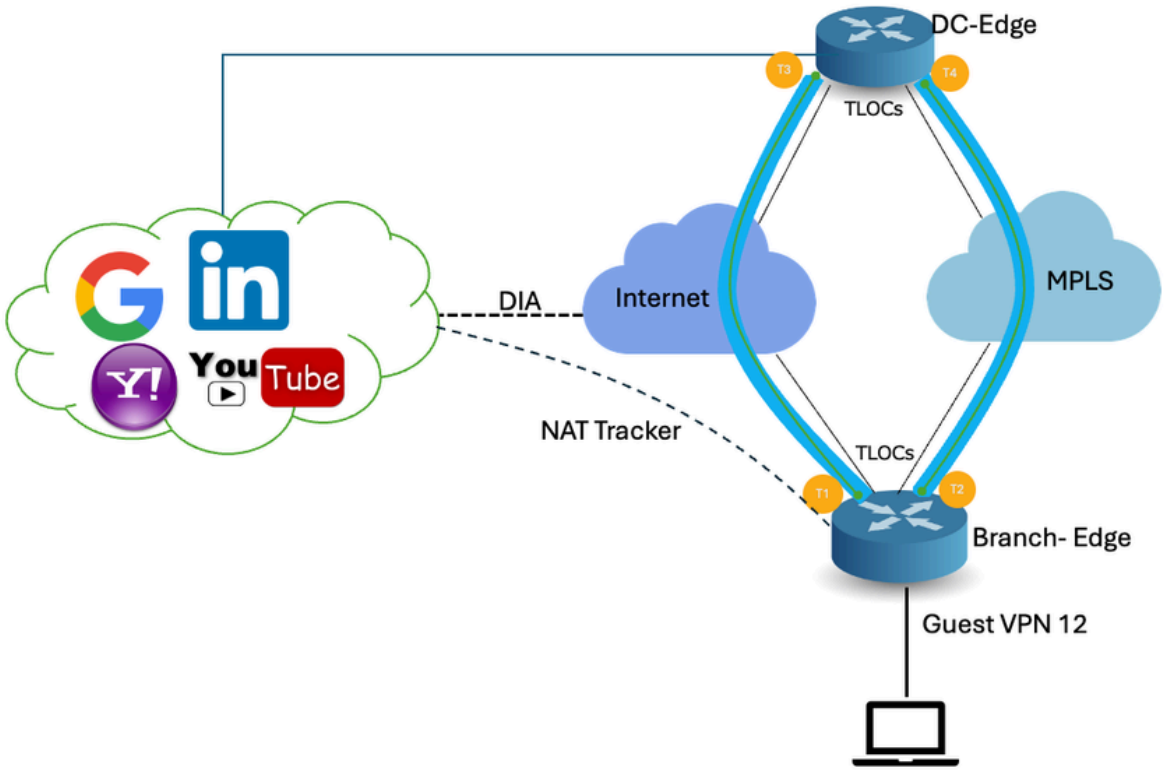
Note: Cellular interfaces do not support negotiated IP addresses.

- Ethernet Interfaces
- Ethernet (PPPoE) Interfaces
- Subinterfaces
- DSL Dialer Interfaces (PPPoE and PPPoA)

Note: IPv6 NAT DIA tracker is supported only on physical and subinterfaces of Ethernet interfaces.

Configure

Network Diagram



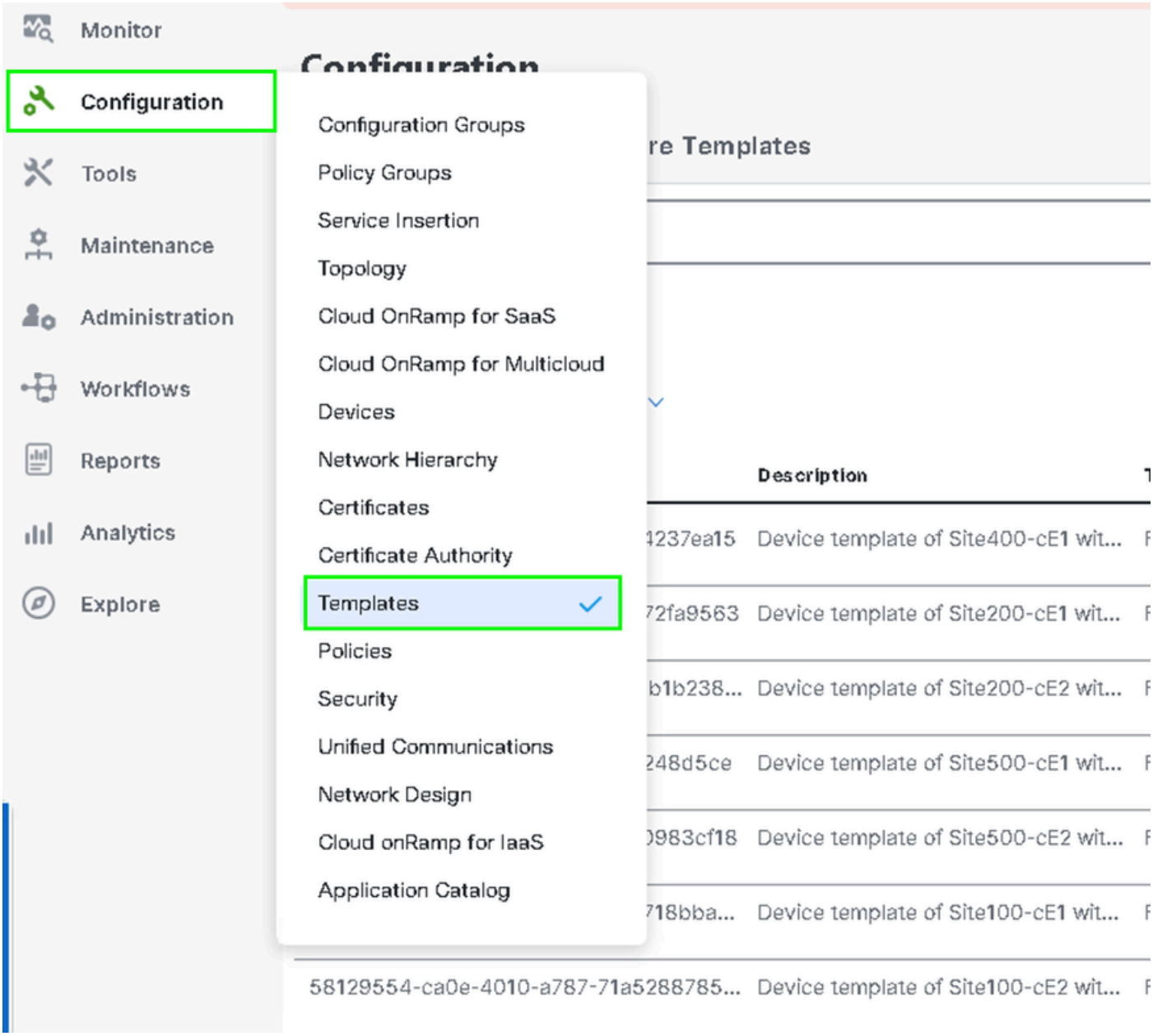
Configurations

The DIA tracker helps determine if the internet or external network has become unavailable. The NAT DIA Tracking feature is useful when NAT is enabled on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet.

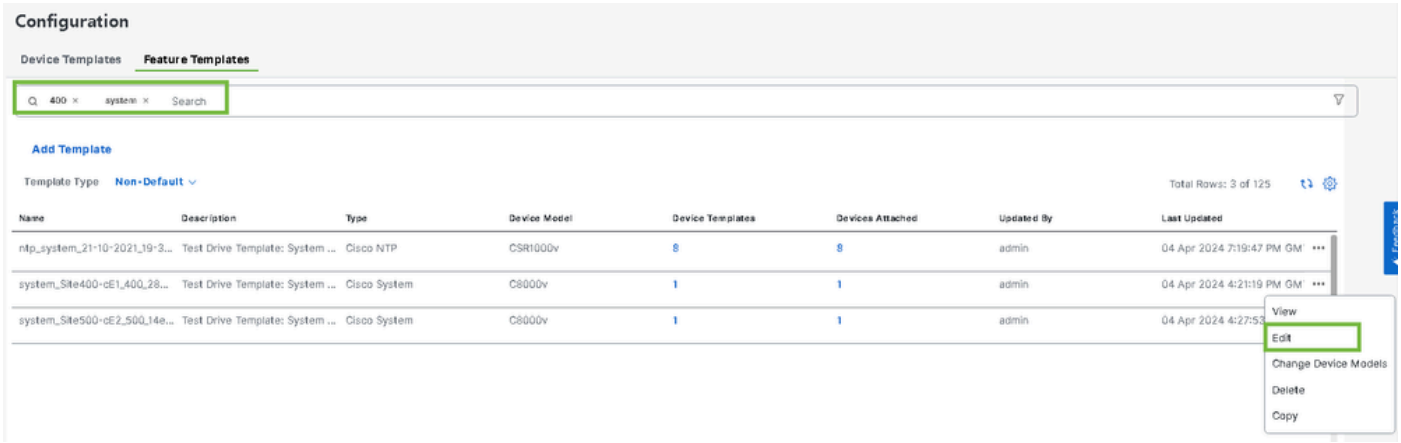
If the internet or external network becomes unavailable, the router continues to forward traffic based on the NAT route in the service VPN. Traffic that is forwarded to the internet gets dropped. To prevent the internet-bound traffic from being dropped, configure the DIA tracker on the edge router to track the status of the transport interface. The tracker periodically probes the interface to determine the status of the internet and return the data to the attach points that are associated with the tracker.

Step 1. Configure NAT DIA Tracker

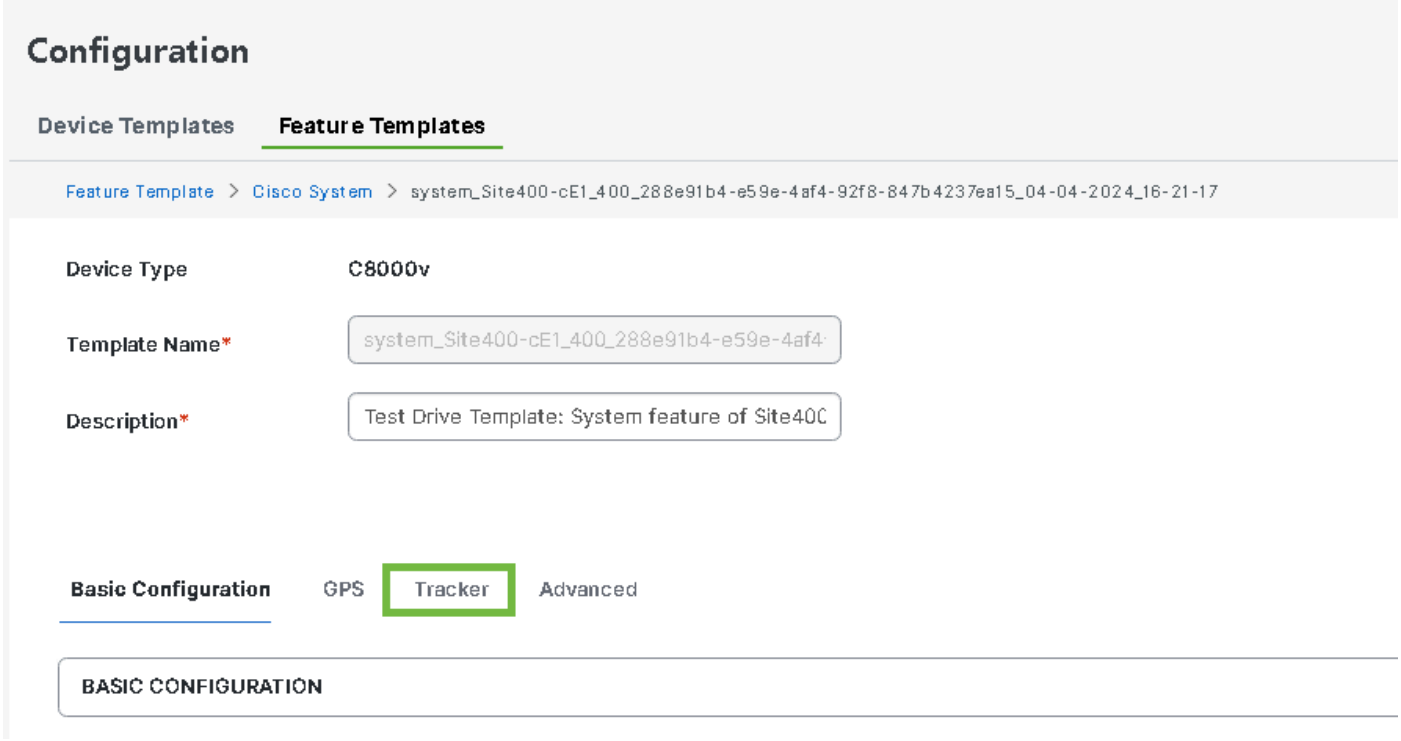
On the Cisco SD-WAN Manager menu, navigate to **Configuration > Templates**.



Click **Feature Templates**. Search for the **Cisco System feature template** in the search bar, click the **three dots (...)**, and click **Edit** to modify.



In the System feature template, click **Tracker**.



Click **New Endpoint Tracker** to configure the tracker parameters.



Enter the tracker parameters and click **Add**.

Name: Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.

Threshold: Duration to wait for the probe to return a response before declaring that the transport interface is down. Range: 100 to 1000 milliseconds. Default: 300 milliseconds.

Interval: Frequency at which a probe is sent to determine the status of the transport interface. Range: 20 to 600 seconds. Default: 60 seconds (1 minute).

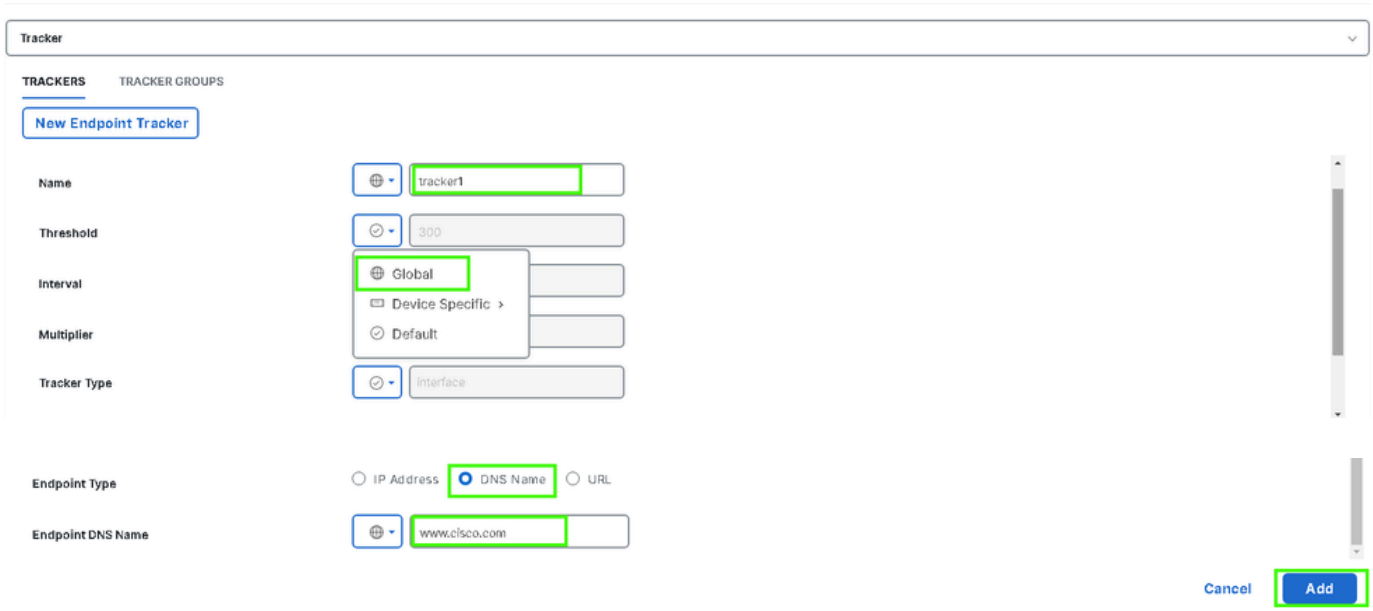
Multiplier: Number of times a probe can be resent before declaring that the transport interface is down. Range: 1 to 10. Default: 3.

Tracker Type: Choose Interface to configure the DIA tracker.

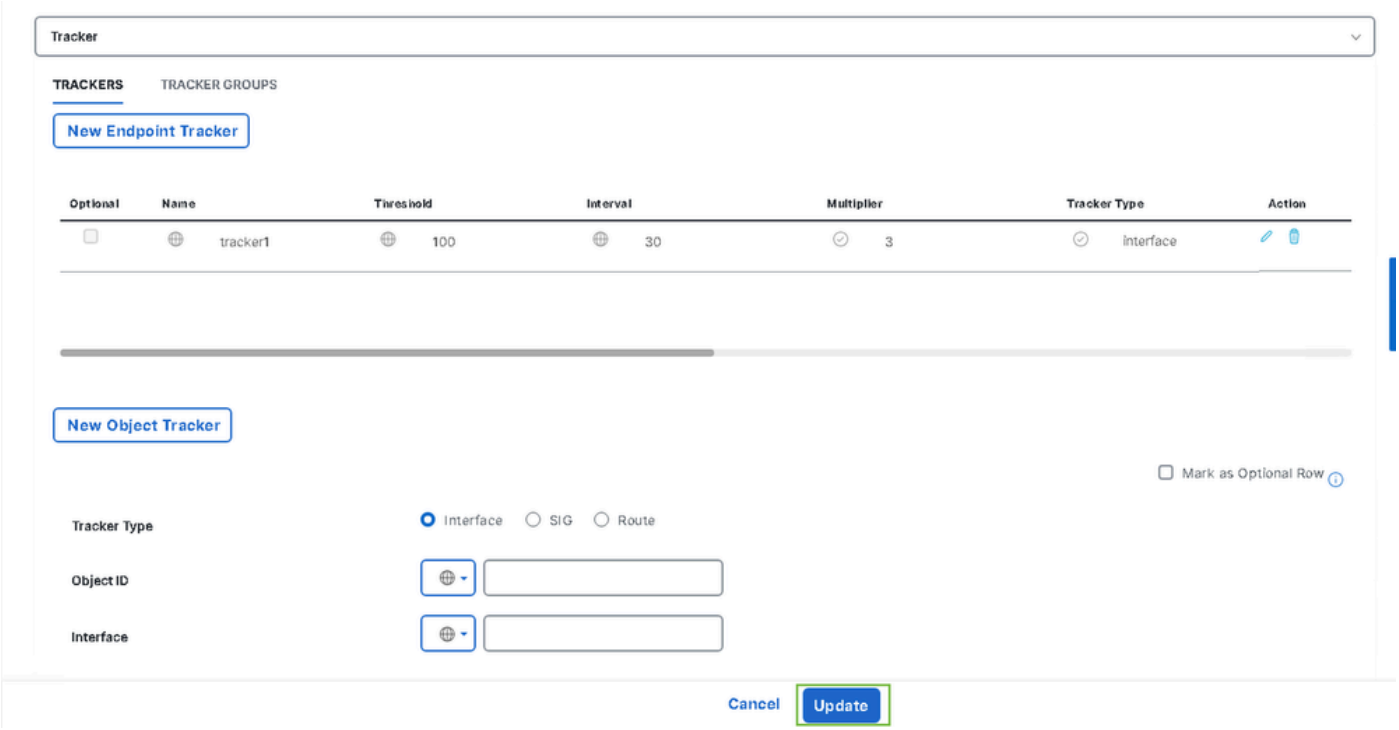
End Point Type: You can select IP address or DNS Name or URL.

End Point DNS Name: DNS name of the end point. This is the destination in the internet to which the router sends probes to determine the status of the transport interface.

Click **drop-down** and select **Global** to change any default value.

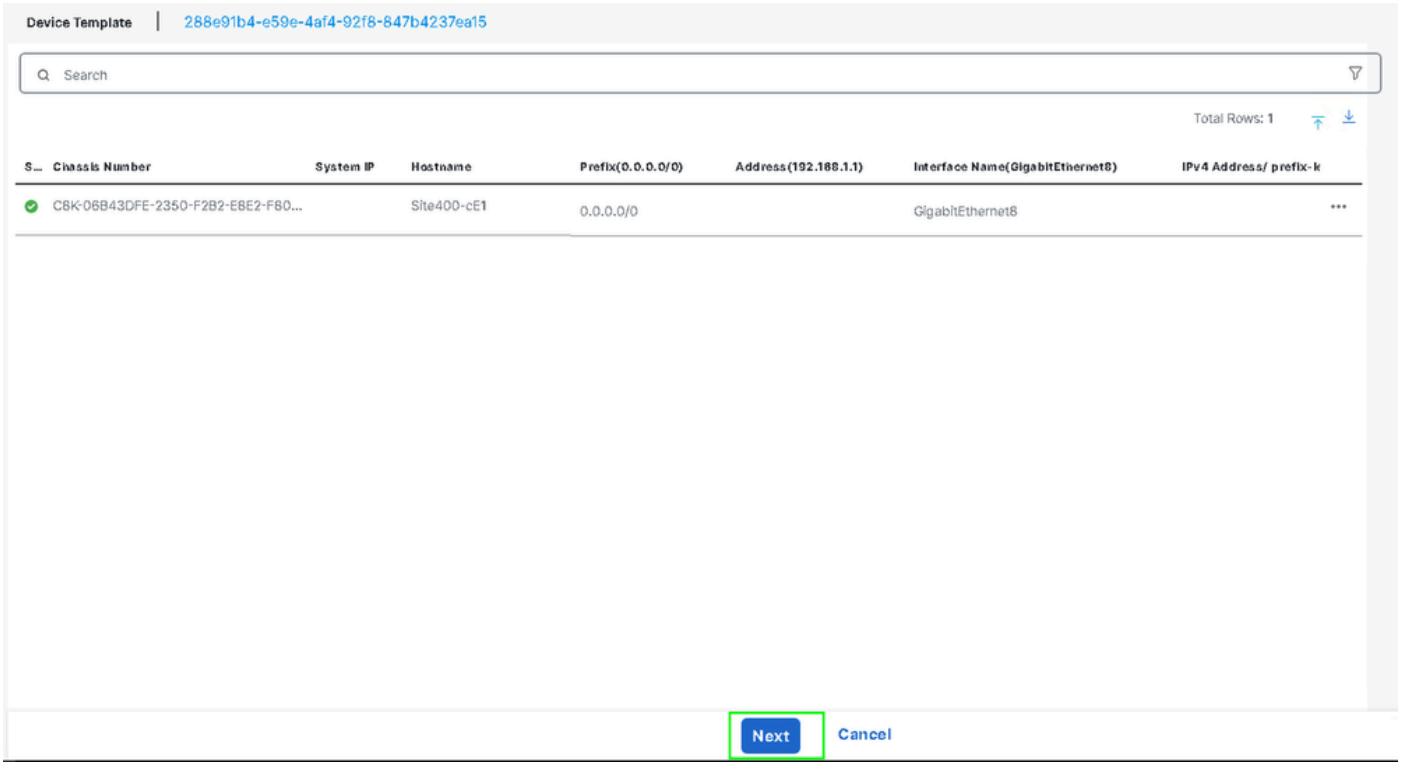


Click **Update**.

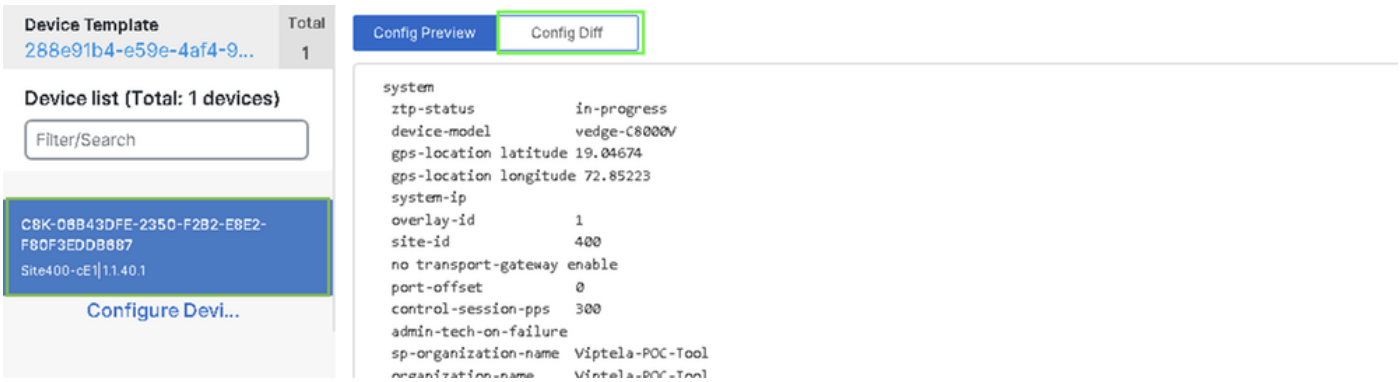


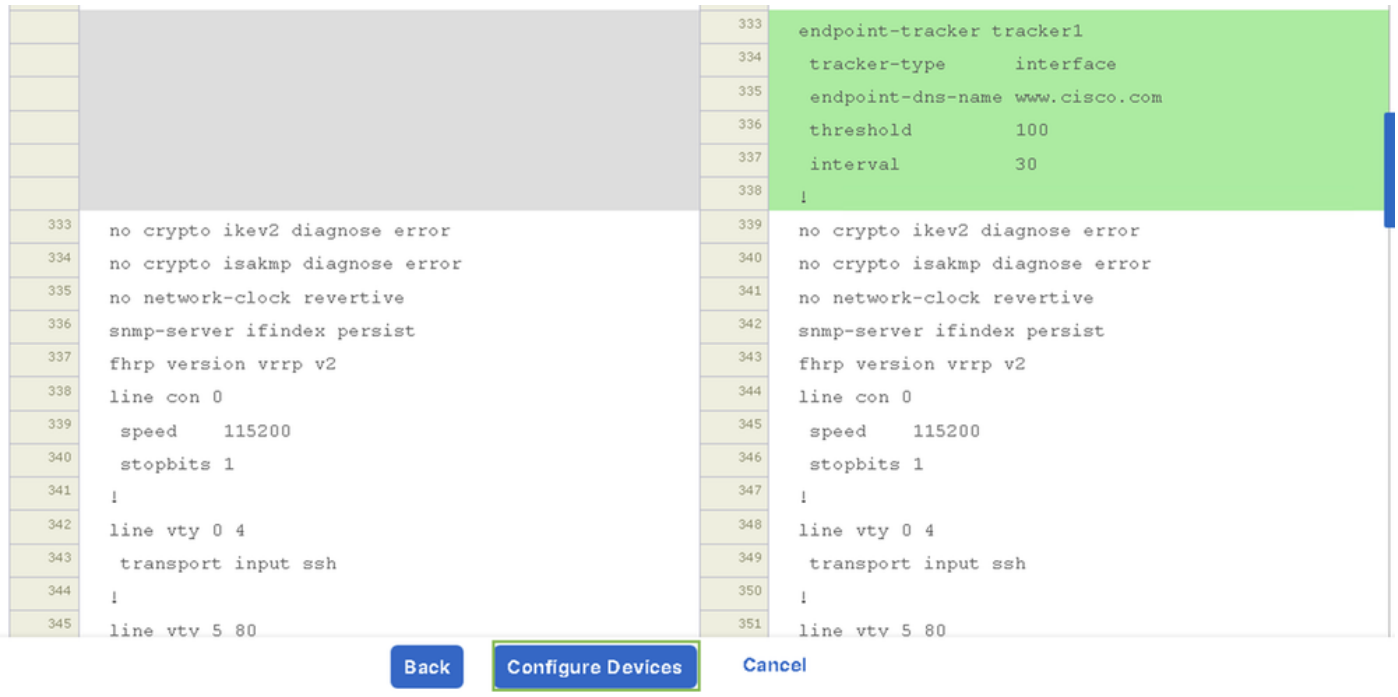
Note: Ensure that you have configured two single endpoint trackers before configuring a tracker group.

Click **Next**.

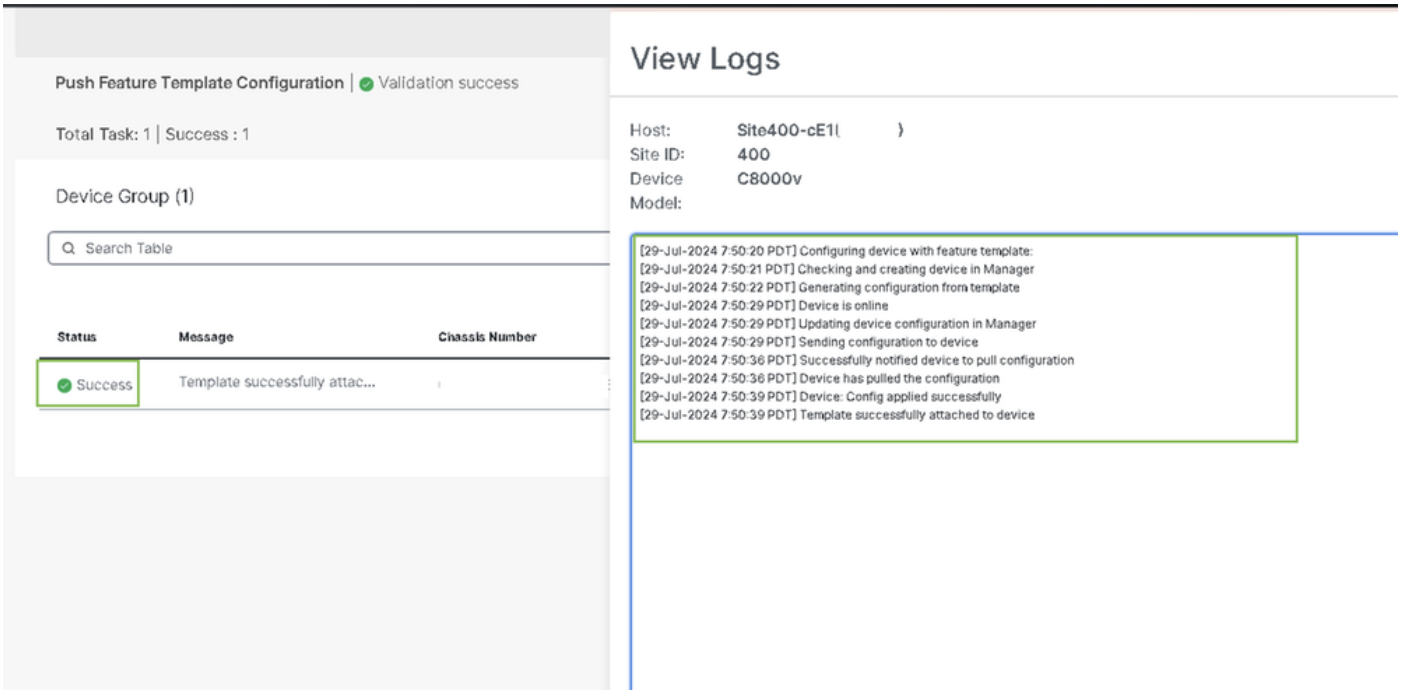


Click **devices**, and make sure the config is correct. Click **Config Diff** and **Side by Side Diff**.
Click **Configure Devices**.



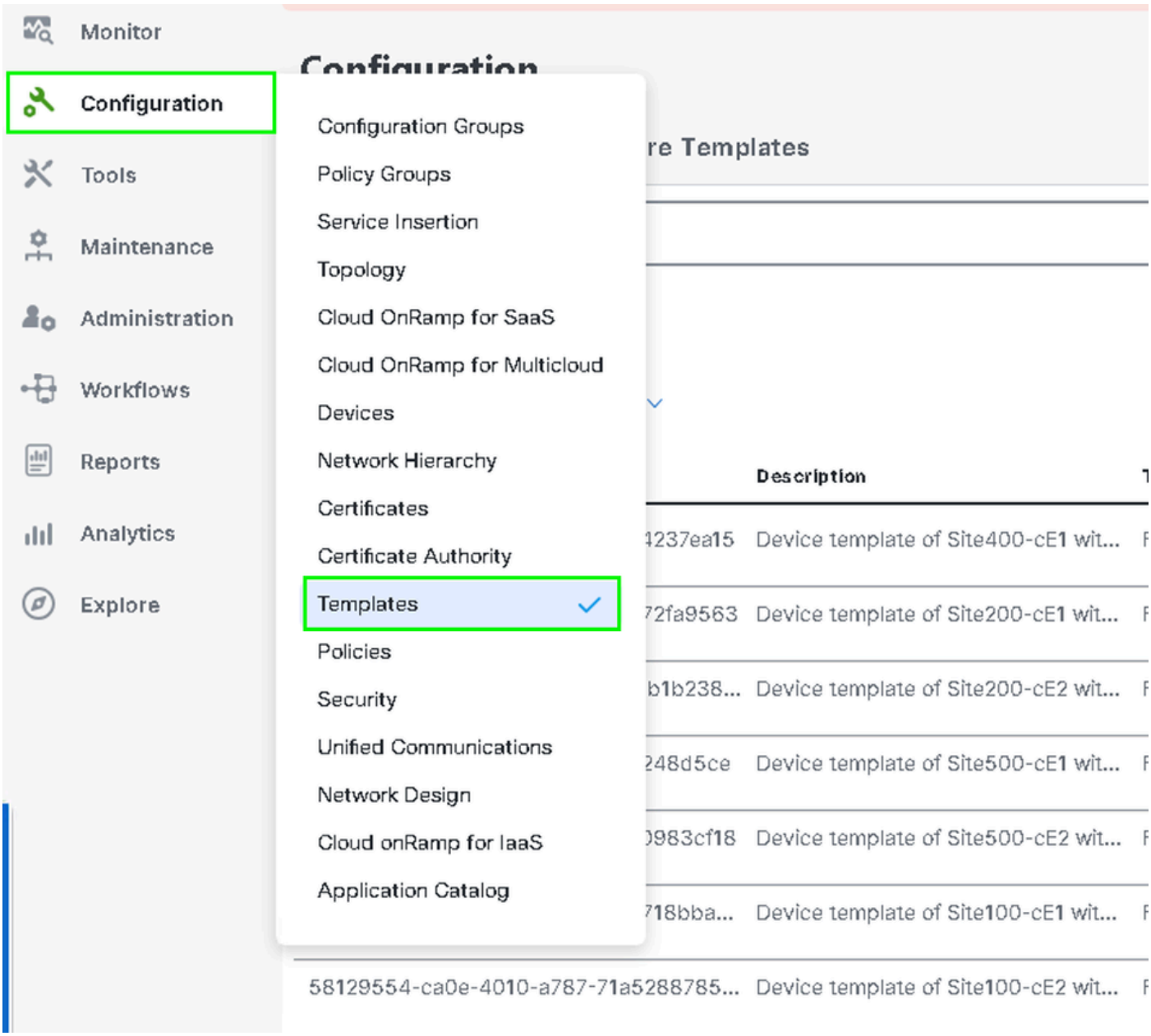


vManage successfully configured the device template with the tracker configuration.

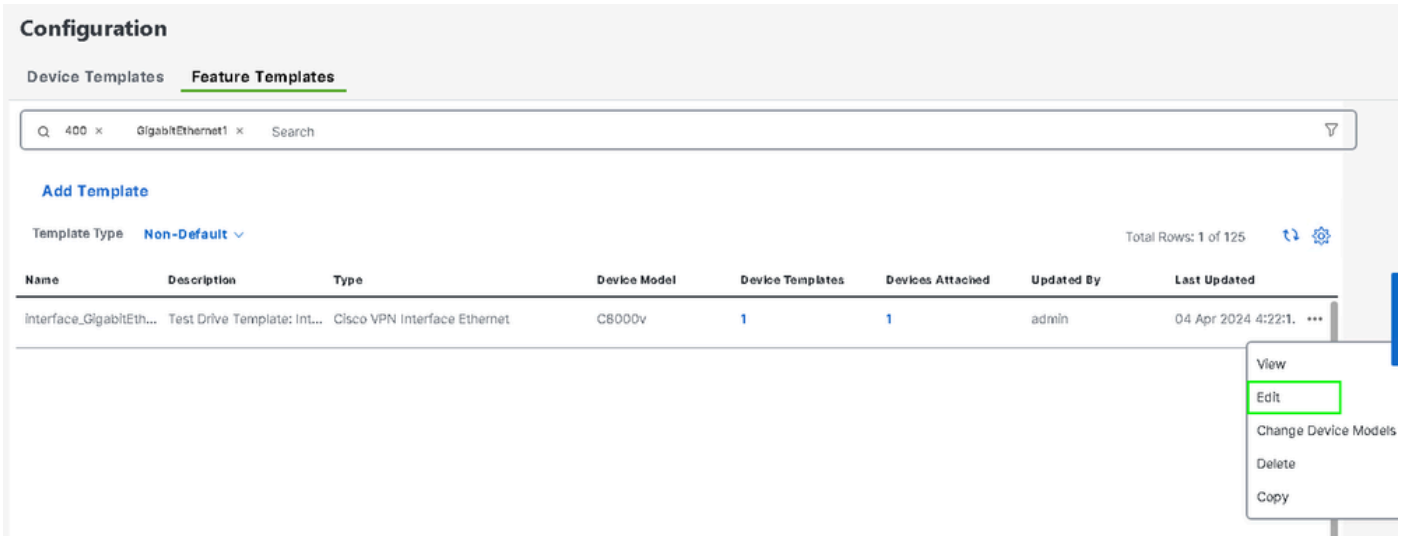


Step 2. Bind the Tracker to Transport Interface

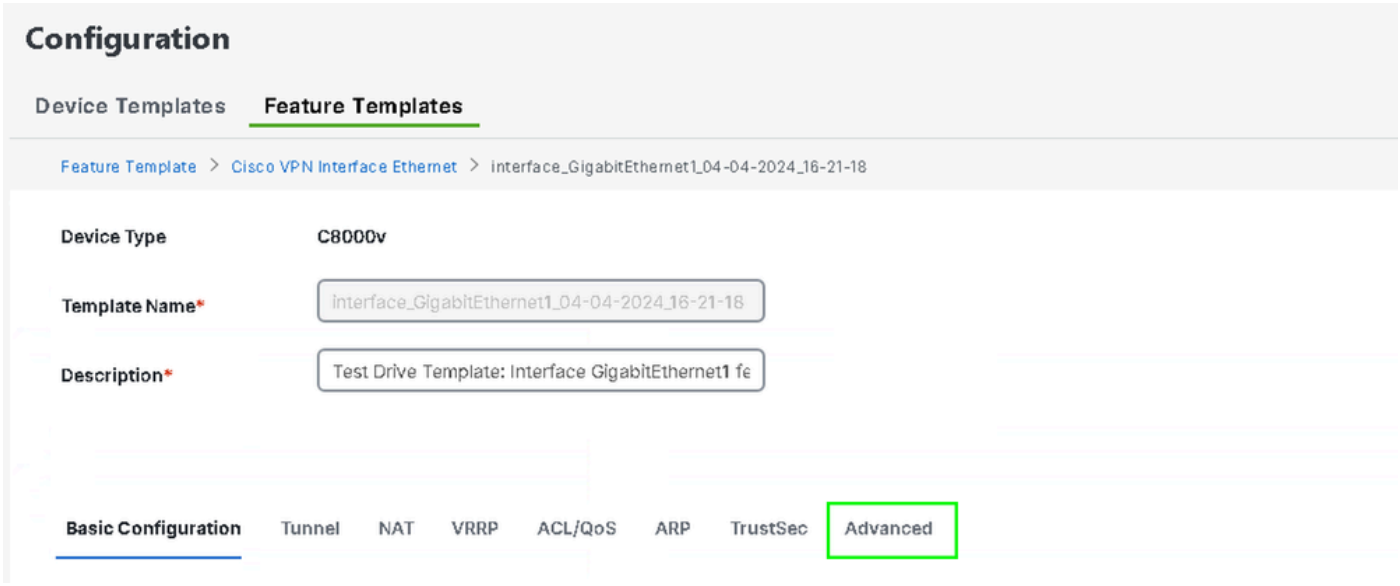
On the Cisco SD-WAN Manager menu, navigate to **Configuration > Templates**.



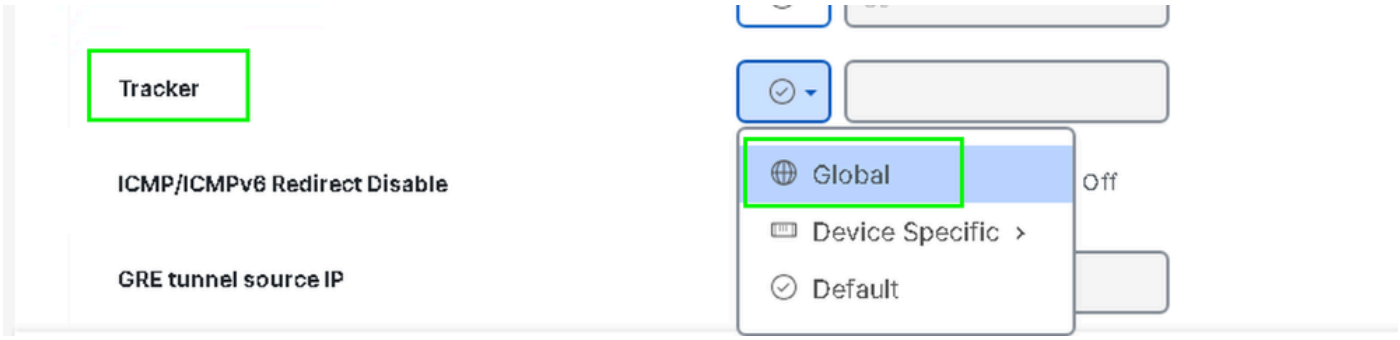
Search for the **NAT Transport Interface feature template** in the search bar, click the **three dots (...)**, and click **Edit** to modify.



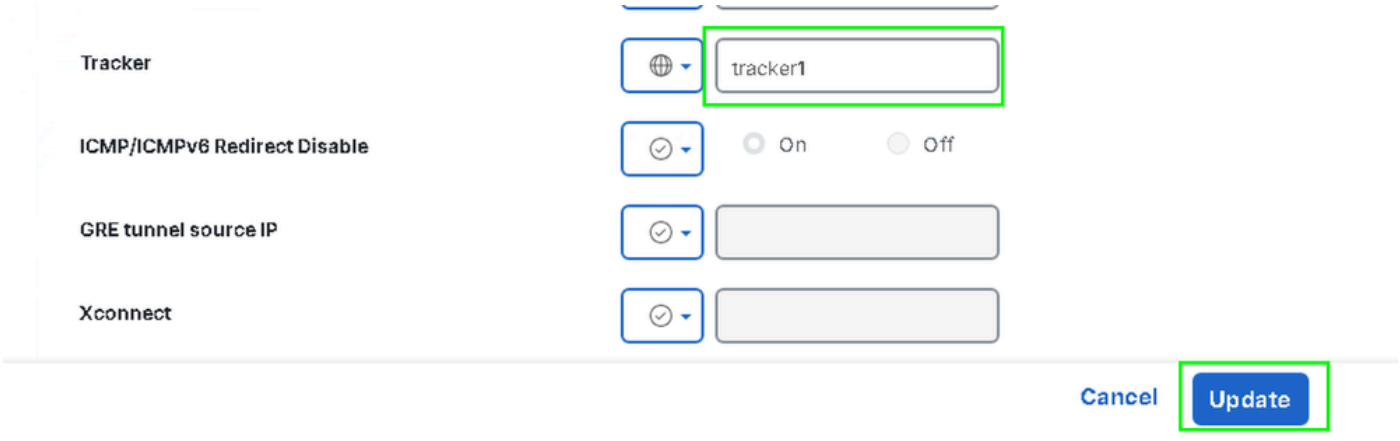
Click the **Advanced** tab.



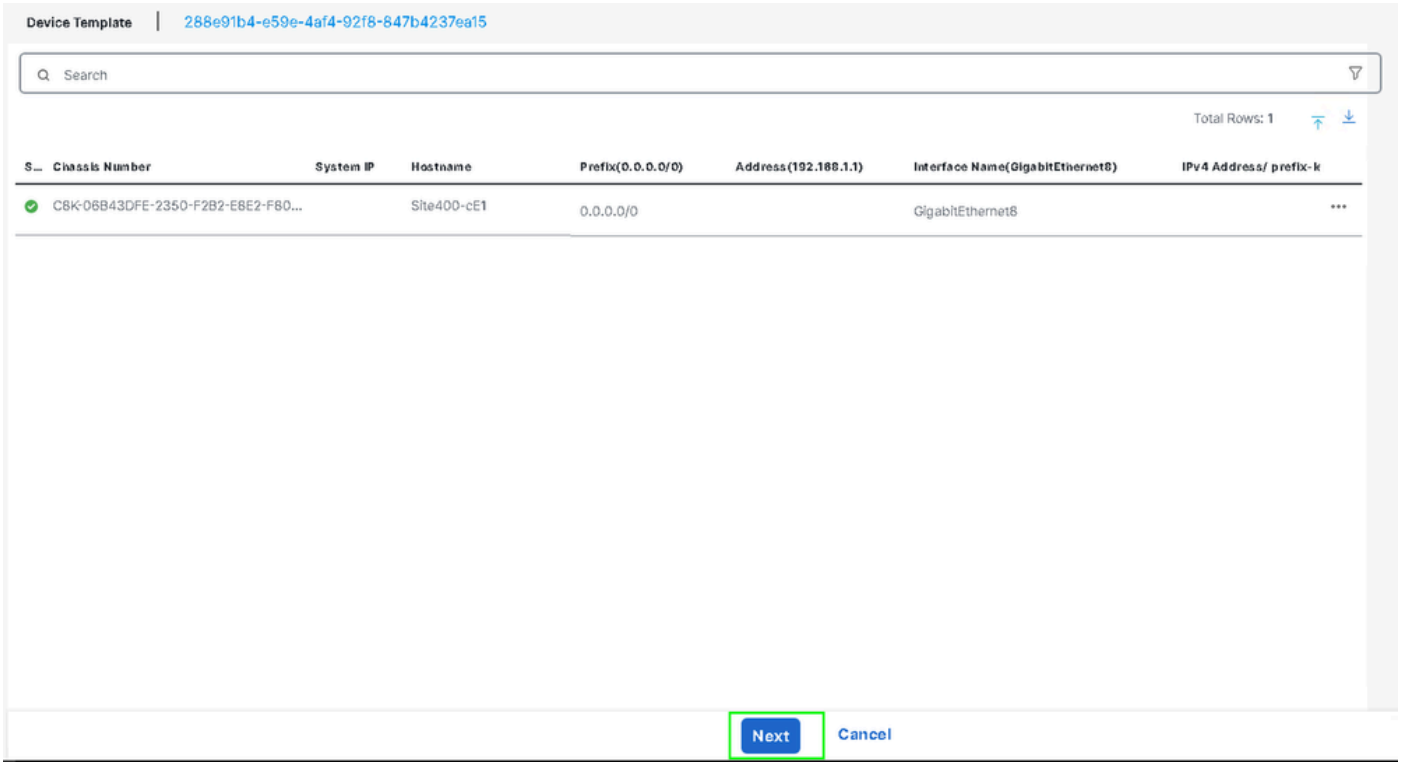
To add the tracker name on the Tracker, select **Global** from the drop-down menu.



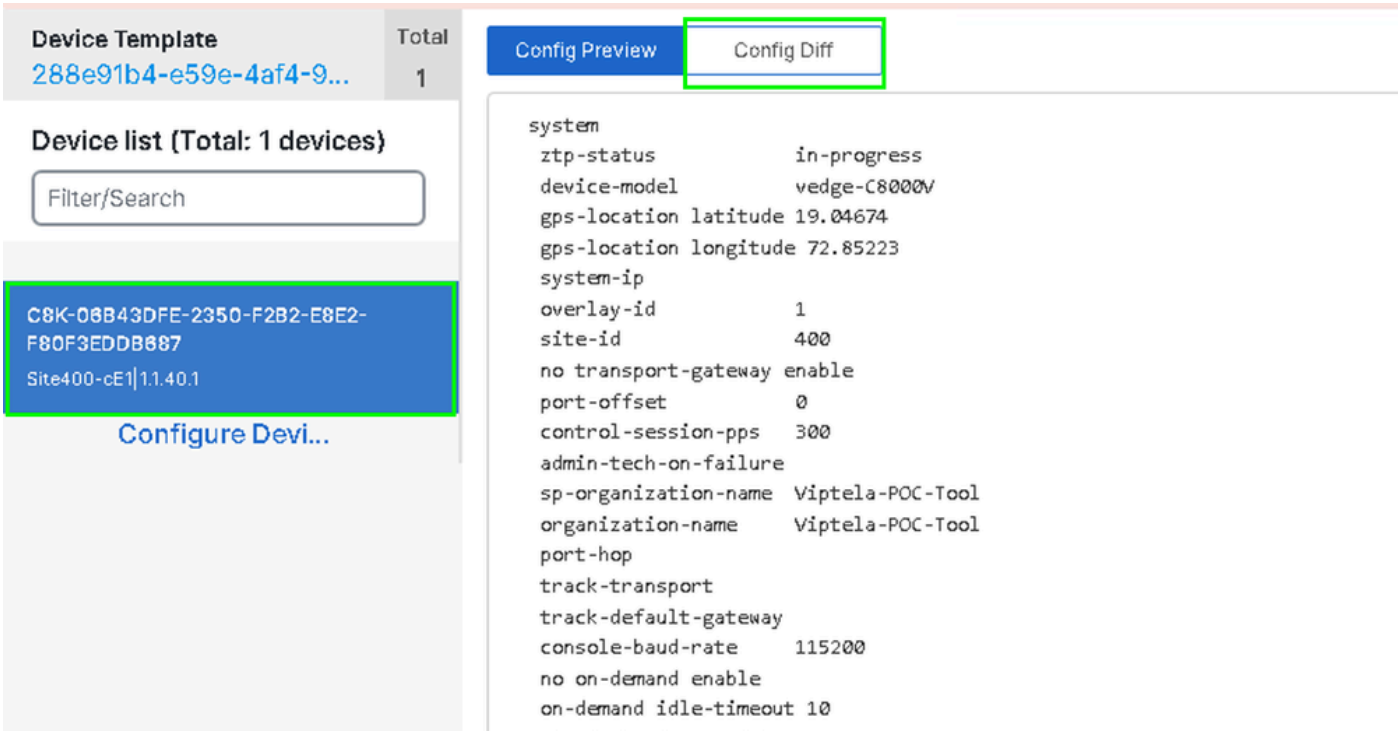
Enter the **tracker name** that you created in the system template and click **Update**.

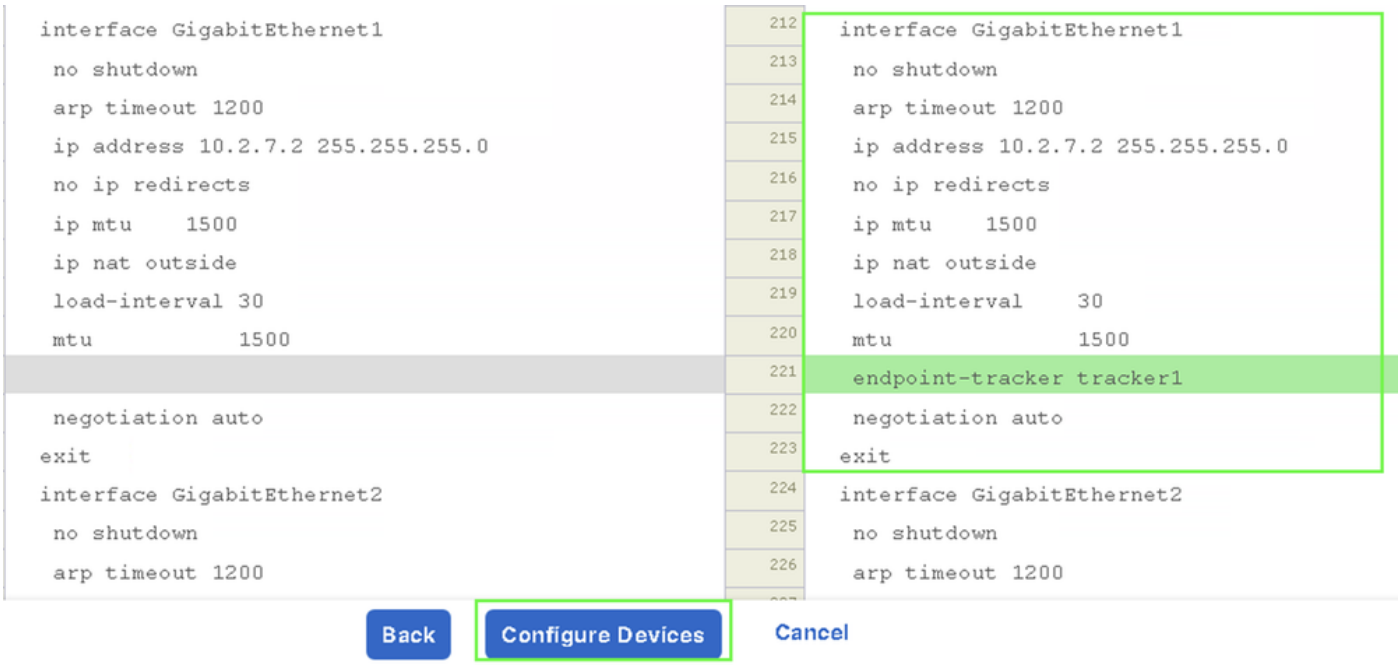


Click **Next**.

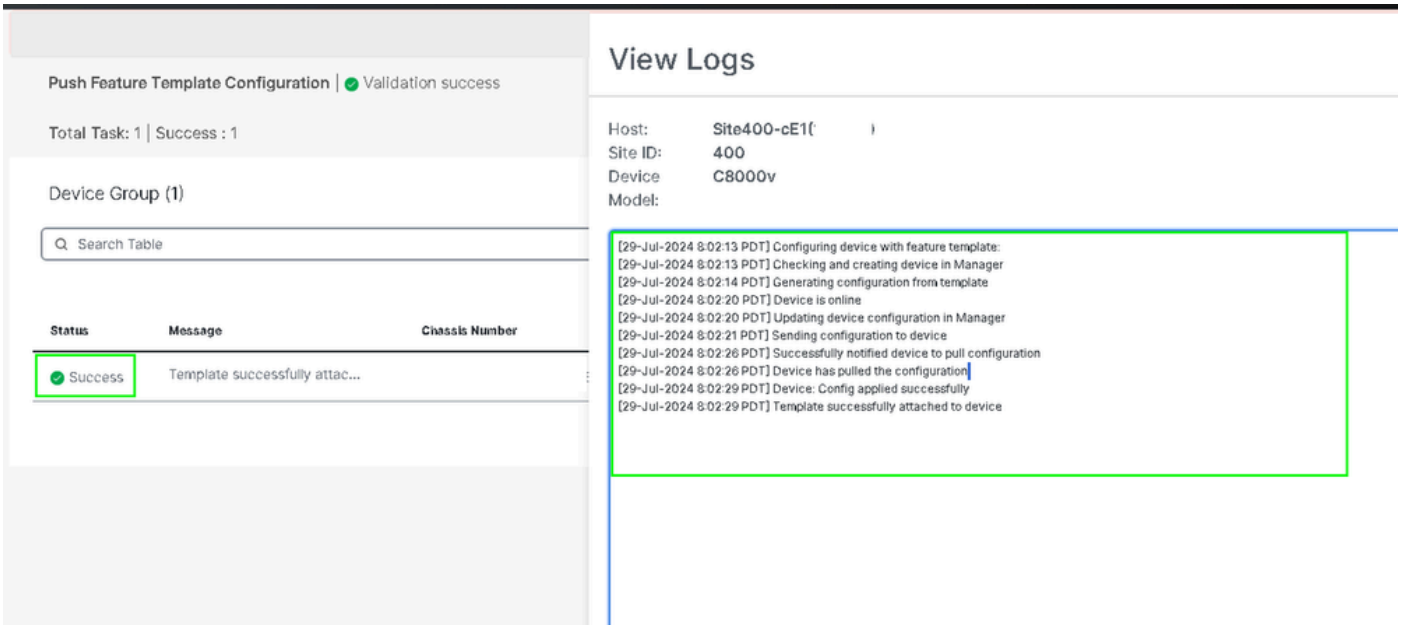


Click **devices**, and make sure the config is correct. Click **Config Diff** and **Side by Side Diff**.
Click **Configure Devices**.





vManage has successfully configured the device template.

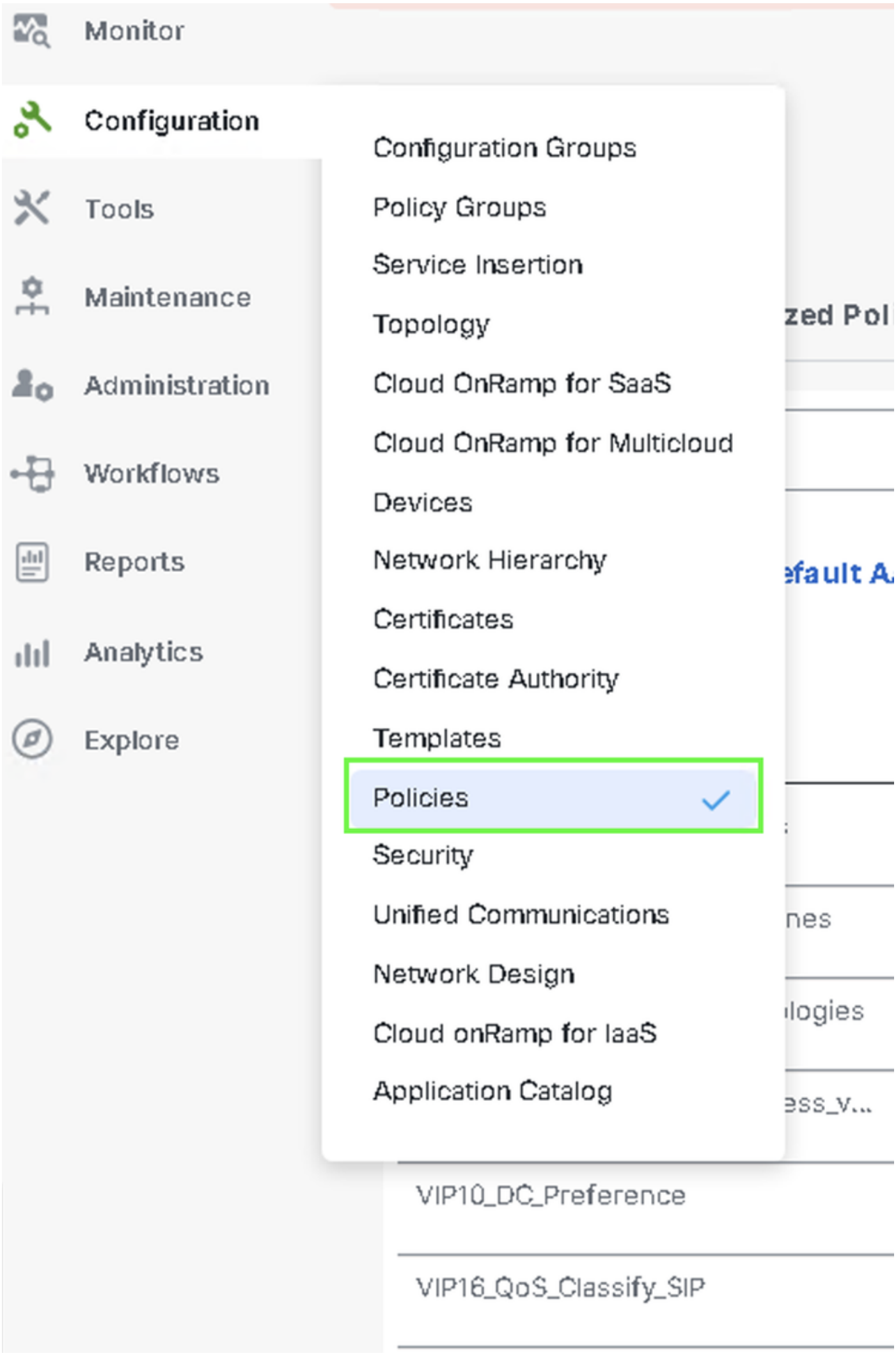


Step 3. Enable NAT Fallback on Existing DIA Policy

Cisco IOS XE Catalyst SD-WAN devices support the NAT fallback feature for Direct Internet Access (DIA). NAT fallback feature allows traffic to use an alternative path if the primary NAT path fails. This ensures continuous connectivity even if there are issues with the primary NAT configuration.

To enable NAT fallback using Cisco SD-WAN Manager:

From the Cisco SD-WAN Manager menu, navigate to **Configuration > Policy**.


Monitor
Configuration
Tools
Maintenance
Administration
Workflows
Reports
Analytics
Explore
Configuration Groups
Policy Groups
Service Insertion
Topology
Cloud OnRamp for SaaS
Cloud OnRamp for Multicloud
Devices
Network Hierarchy
Certificates
Certificate Authority
Templates
Policies
Security
Unified Communications
Network Design
Cloud onRamp for IaaS
Application Catalog
VIP10_DC_Preference
VIP16_QoS_Classify_SIP

```
interface GigabitEthernet1
ip address 10.2.7.2 255.255.255.0
no ip redirects
ip nat outside
load-interval 30
negotiation auto
```

endpoint-tracker tracker1

```
arp timeout 1200
end
```

```
Site400-cE1#show sdwan running-config | sec endpoint
endpoint-tracker tracker1
tracker-type interface
endpoint-dns-name www.cisco.com
threshold 100
interval 30
```

The output shows how to verify the tracker status using the commands **show endpoint-tracker** and **show endpoint-tracker GigabitEthernet1**.

```
Site400-cE1#show endpoint-tracker
Interface         Record Name   Status   Address Family   RTT in msecs   Probe ID  Next Hop
GigabitEthernet1    tracker1     Up      IPv4              8              6       10.2.7.1

Site400-cE1#show endpoint-tracker interface GigabitEthernet1
Interface          Record Name    Status    Address Family   RTT in msecs   Probe ID  Next Hop
GigabitEthernet1    tracker1       Up        IPv4                8          6        10.2.7.1
```

The output shows timer-related information about the tracker to help debug tracker-related issues, if any:

```
Site400-cE1#show endpoint-tracker records
Record Name    Endpoint        EndPoint Type    Threshold(ms)  Multiplier   Interval(s)  Tracker-Type
tracker1       www.cisco.com    DNS_NAME           100            3            30         interface
```

The output of**show ip sla summary**command.

```
Site400-cE1#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID  Type  Destination    Stats  Return   Last
                         Code     Run
```

```
------------------------------------------------------------------------
*5  dns    8.8.8.8       RTT=16  OK    16 seconds ago
*6  http   x.x.x.x       RTT=15  OK    3 seconds ago
```

Verify the fallback configuration applied on the device using the command **show sdwan policy from-vsmart**.

<#root>

```
Site400-cE1#show sdwan policy from-vsmart
from-vsmart data-policy _VPN12_VPN12_DIA
direction from-service
vpn-list VPN12
sequence 1
match
source-data-prefix-list Site400_AllVPN_Prefixes
action accept
nat use-vpn 0
```

nat fallback

```
no nat bypass
default-action drop
```

Troubleshooting Tracker

Enable these debugs on the edge device to check how the router sends probes to determine the status of the transport interface.

- To monitor how the router sends probes and determines the status of the transport interfaces use the **debug platform software sdwan tracker** command which is supported until the 17.12.x release.
- From 17.13.x onwards, to monitor the probes logs, enable these debugs.
  - set platform software trace ios R0 sdwanrp-tracker debug
  - set platform software trace ios R0 sdwanrp-cfg debug

- To check the logs related to IP SLA operations error and trace, enable these debugs. These logs show if IP SLA operations are failing.
  - debug ip sla trace
  - debug ip sla error

Run these show and monitor commands to check the debug logs:

- **show logging profile sdwan internal**
- **monitor logging profile sdwan internal**

```
Site400-cE1#show logging profile sdwan internal
Logging display requested on 2024/08/13 08:10:45 (PDT) for Hostname: [Site400-cE1], Model: [C8000V], Ve

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis local ...
Unified Decoder Library Init .. DONE
```

```
Found 1 UTF Streams

2024/08/13 08:02:28.408998337 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 s
2024/08/13 08:02:28.409061529 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.409086404 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE: Sla sync
2024/08/13 08:02:28.409160541 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE: Sla sync
2024/08/13 08:02:28.409182208 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Sta
2024/08/13 08:02:28.409197024 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Que
2024/08/13 08:02:28.409215496 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 DNS
2024/08/13 08:02:28.409242243 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Sou
2024/08/13 08:02:28.409274690 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Des
2024/08/13 08:02:28.409298157 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Sou
2024/08/13 08:02:28.409377223 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Nex
2024/08/13 08:02:28.409391034 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Rea
2024/08/13 08:02:28.409434969 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 act
2024/08/13 08:02:28.409525831 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Pro
2024/08/13 08:02:28.426966448 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Que
2024/08/13 08:02:28.427004143 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Rec
2024/08/13 08:02:28.427029754 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 RTT
2024/08/13 08:02:28.427161550 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427177727 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427188035 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427199147 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427208941 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 IPS
2024/08/13 08:02:28.427219960 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427238042 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427301952 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427316275 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427326235 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): Received IPSLA sta
2024/08/13 08:02:28.427328425 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS status callbac
2024/08/13 08:02:28.427341452 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS query valid TRU
2024/08/13 08:02:28.427343152 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS resolved addre
2024/08/13 08:02:28.427344332 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS probe handler
2024/08/13 08:02:28.427349194 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427359268 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427370416 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427555382 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427565670 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427577691 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427588947 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427600567 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427611465 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427620724 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427645035 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:55.599896668 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 sla
2024/08/13 08:02:55.599966240 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sta
2024/08/13 08:02:55.599981173 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Sta
2024/08/13 08:02:55.600045761 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Nex
2024/08/13 08:02:55.600111585 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 DNS
2024/08/13 08:02:55.600330868 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 sla
2024/08/13 08:02:55.610693565 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Soc
2024/08/13 08:02:55.610717011 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Wai
2024/08/13 08:02:55.610777327 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Sen
2024/08/13 08:02:55.610788233 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Wai
2024/08/13 08:02:55.618534651 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Soc
2024/08/13 08:02:55.618685838 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 HTT
2024/08/13 08:02:55.618697389 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618706090 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618714316 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618723915 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618732815 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 IPS
2024/08/13 08:02:55.618821650 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
```

```
2024/08/13 08:02:55.618833396 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:55.618857012 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
```

Related Information

Implement Direct Internet Access (DIA) for SD-WAN

Cisco Catalyst SD-WAN NAT Configuration Guide

NAT Fallback on Cisco IOS XE Catalyst SD-WAN Devices

Technical Support & Documentation - Cisco Systems