Configure Data-Driven SLA Monitoring

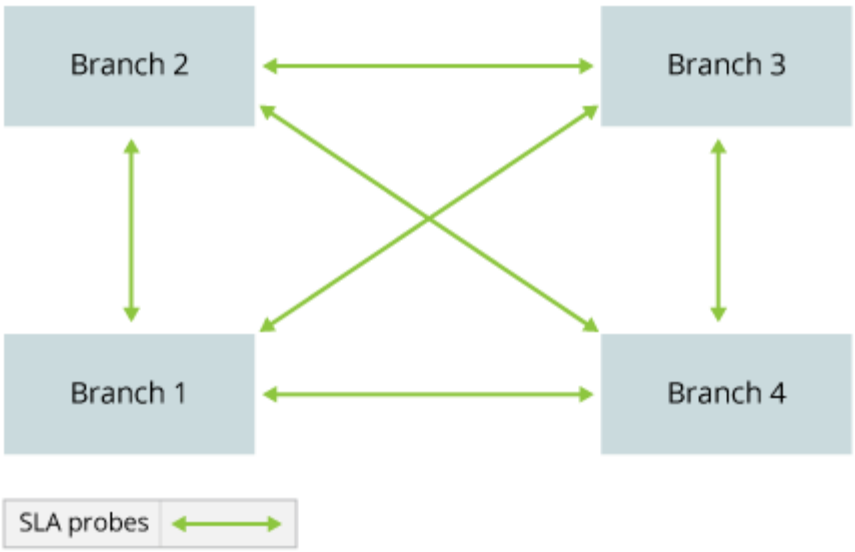
For supported software information, click here.

Data-driven SLA monitoring allows you to regulate the amount of monitoring traffic between branches by creating and deleting SLA-monitoring contexts based on whether traffic is flowing towards a remote site. SLA monitoring can generate a very large amount of SLA traffic when you enable it in large, full-mesh topologies. Also, customers who use certain high-cost links (such as LTE) might want to limit SLA monitoring traffic on those links to reduce link utilization. Data-driven SLA monitoring addresses both issues by eliminating excessive traffic that is sent over WAN links and by limiting the amount of traffic sent over higher-cost links.

With data-driven SLA monitoring, when no traffic is detected between two branches for a configured time interval, the monitoring context between the two branches is deleted. If the SLA monitoring module subsequently detects new traffic flowing towards a remote site, it creates a new SLA monitoring context between the branches and begins monitoring the path.

Data-Driven SLA Monitoring Components

The following figure show four branches in a full-mesh topology. With data-driven SLA monitoring, each branch monitors the paths to the other branches in the mesh.

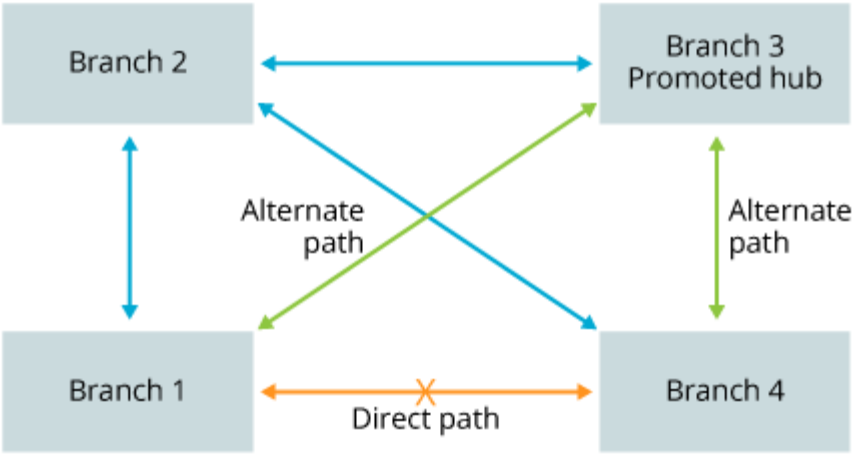


Alternate Path

When you enable data-driven SLA monitoring, you must specify an alternate path to a destination branch. To enable an alternate path, you promote one branch device to be a hub that can forward traffic between branches. While a new SLA monitoring context is being created on the direct path between two branches, the alternate path through the promoted hub is used to send the initial packets of a flow towards the destination branch.

Note: To ensure that an alternate path is available, you must enable continuous SLA monitoring toward the next-hop promoted hub on the alternate path so that the source branch knows whether the alternate path through the next hop is available.

For example, in the figure below, no traffic has been detected during the configured interval on the direct path between Branch1 and Branch4, which causes the direct path to be deleted. When there is new traffic from Branch1 to Branch4, the initial packets of the flow are sent from Branch1 to Branch3, the promoted hub, which then forwards the packets to Branch4. SLA monitoring is also restarted on the direct path from Branch1 to Branch4. As soon as the new SLA context becomes active, the data flow shifts from the alternate path to the direct path between Branch1 and Branch4.



Branches Behind NAT Devices

When a destination branch is located behind an endpoint-dependent network address translation (ED-NAT) device, sending SLA monitoring packets helps keep the NAT pinhole open so that traffic can be sent directly to the destination branch. However, because data-driven SLA monitoring deletes the monitoring context if it does not detect activity on a link, the NAT pinhole may not remain open. To address this issue, the source branch sends unicast IP SLA monitoring packets toward the destination branch behind the ED-NAT device using the alternate path. When the destination branch receives these IP SLA monitoring packets, it creates an SLA monitoring context towards the source branch on a direct path, which opens up the pinhole for data traffic flows. As soon as an SLA monitoring context between the source branch and the destination branch has been created, SLA monitoring between the source and the destination branch resumes using the direct path.

IP SLA Monitoring

As previously described, an IP SLA monitoring packet is a unicast SLA monitoring packet sent from a source branch toward a destination branch using an alternate path. The IP SLA monitoring packet is used to enable SLA monitoring from the destination branch towards the source branch on a direct link. Each branch selects a local IP address that is used in two ways:

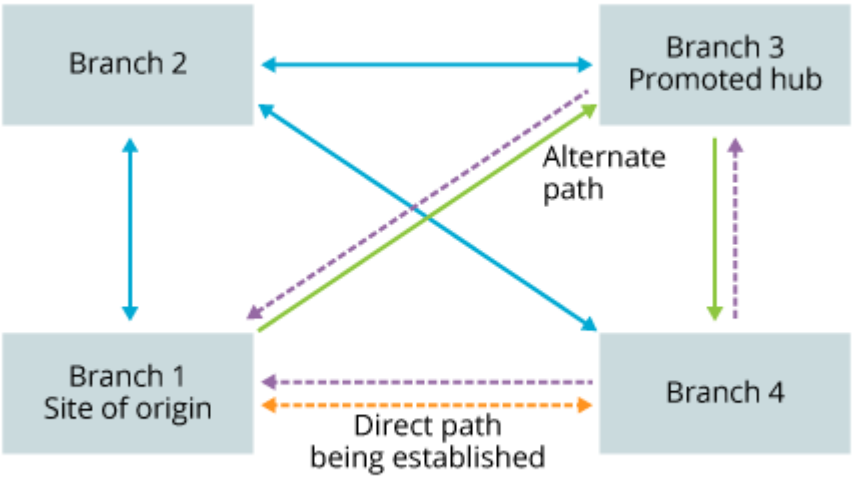
- As the source IP address when sending IP SLA monitoring packets
- As the destination IP address when receiving IP SLA monitoring packets

This local IP address is announced in MP-BGP as a /32 route along with the SLA-Community string. The SLA-Community string is common to all instances of MP-BGP for a given tenant.

Site-of-Origin Community String

A site-of-origin (SoO) community string is attached to all routes that are redistributed using MP-BGP and helps identify the site that originates a route. When an SLA context between two branches does not exist or needs to be rebuilt, IP SLA monitoring packets with the SoO string enabled are sent from a source branch to a receiving branch through the promoted hub. When the receiving branch gets the packet, it reads the SoO string to identify the source branch. The receiving branch then sends traffic back to the SoO branch, and in the process becomes the source for the traffic it sends back to the SoO.

In the figure below, Branch1 is the SoO sending traffic (green lines) to Branch4 using the alternate path through the promoted hub. Branch4 receives the traffic, identifies Branch1 as the SoO, and sends traffic back to Branch1 (dotted purple lines) through the promoted hub while the new SLA context (direct path) is being created. If the direct path is available, Branch4 sends the traffic back to Branch1 using the direct path.



The SoO community string is generated from the combination of an Encapsulating Security Payloads (ESP)-IP and a site ID. Both values are generated automatically.

Configure Data-Driven SLA Monitoring Configuration Overview

You can configure data-driven SLA monitoring in either a full-mesh or a hub-and-spoke topology. When you configure data-driven SLA monitoring in a full-mesh topology, you need to configure one of the spokes to act as a hub device. This spoke is called a promoted hub.

The following sections describe how to configure data-driven SLA monitoring on hubs and promoted hubs, and on spoke devices.

For data-drive SLA monitoring, you can configure SD-WAN path policies to direct traffic to the direct and alternate paths used to reach a destination. For more information, see Configure SD-WAN Path Policies.

Configure Data-Driven SLA Monitoring on Hubs and Promoted Hubs

If you configure multiple promoted hubs, one of the promoted hubs should act as the main hub and it should reject routes learned from the other promoted hubs.

To configure data-driven SLA monitoring on hub devices, do the following:

1. Configure a group membership for hubs and promoted hubs.
2. Check the global tenant ID screen and note the ID number of the tenant on which you will configure one or more hubs.
3. Associate an SLA community string under the Tenant-Control-VR.
4. Specify a static route for the spoke LAN routes and add it to the Redistribution policy before the WildCard-Allow-All term. (If you configure more than two hubs in the network, you must specify the 9008:9008 community string.

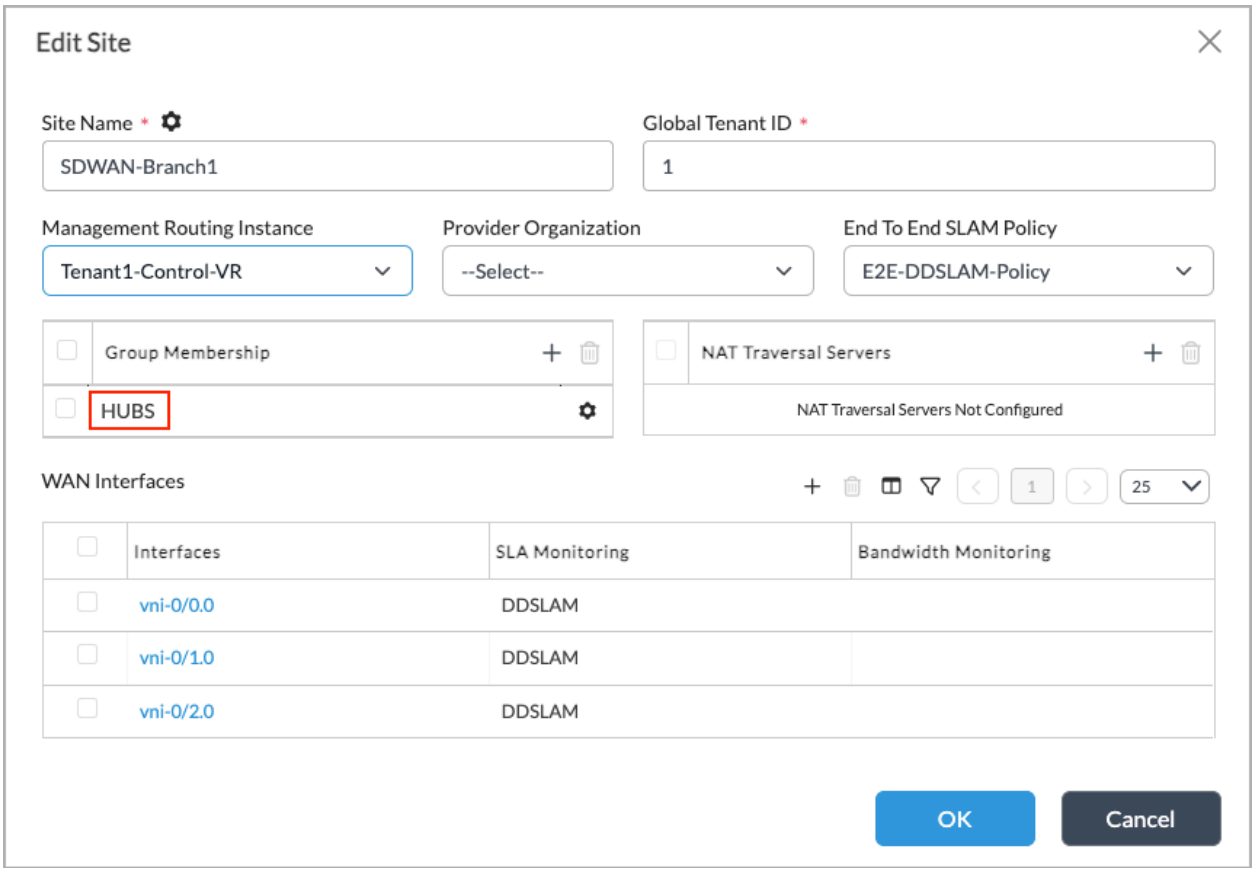
The following sections describe how to configure SLA monitoring on hub devices.

Configure a Hub Group Membership

When configuring SLA monitoring on a hub device, you first configure the group that the hub is a member of. Later, when you configure a path policy for hubs and promoted hubs, you specify this group membership.

To configure a hub group membership:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a post-staging template from the main panel. The view changes to Appliance view.
2. Select Configuration > Services > SD-WAN > Site.
3. Click the Edit icon. The Edit Site popup window displays.

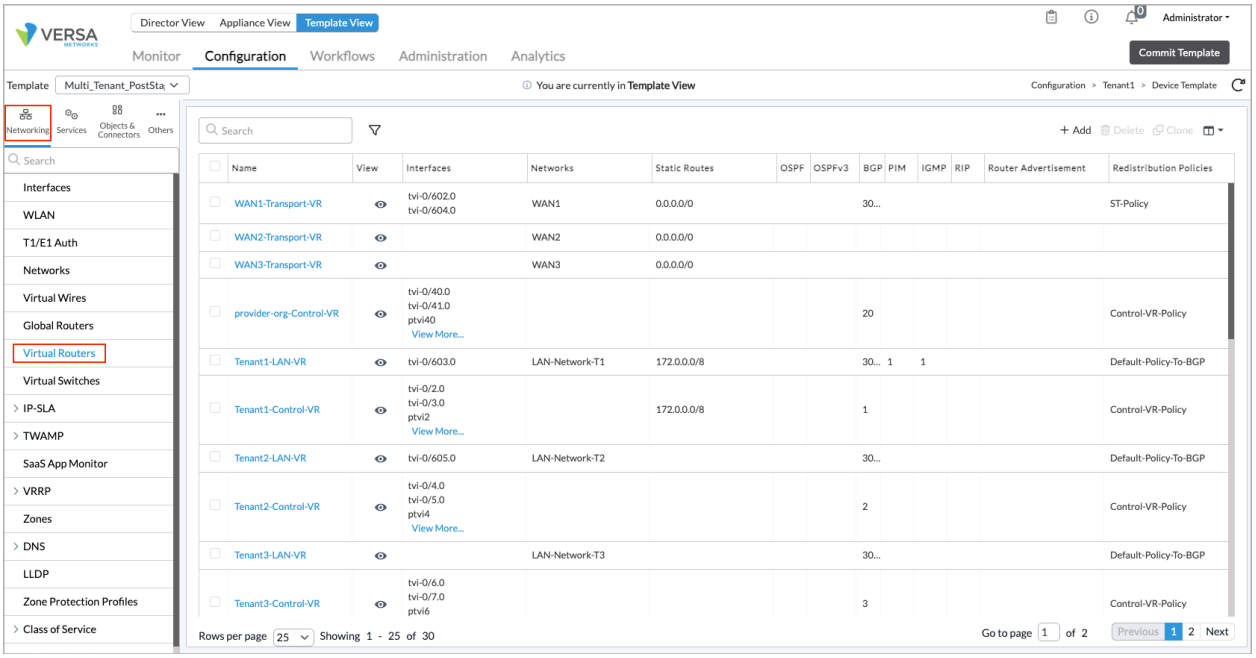


4. Enter HUBS in the Group Membership field.
5. Make a note of the Global Tenant ID shown in the Edit Site screen above. You need to this ID later when you configure the SLA community string, as described in the next section.
6. Click OK.

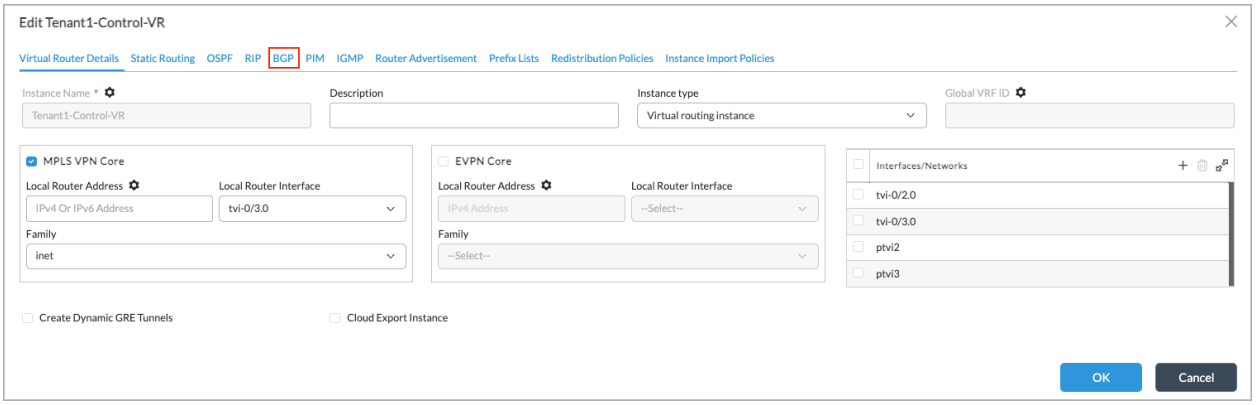
Associate an SLA Community String and Site of Origin with a Tenant Control VR

To configure the SLA community string and enable the BGP site-of-origin (SoO) extended community attribute in a tenant control VR:

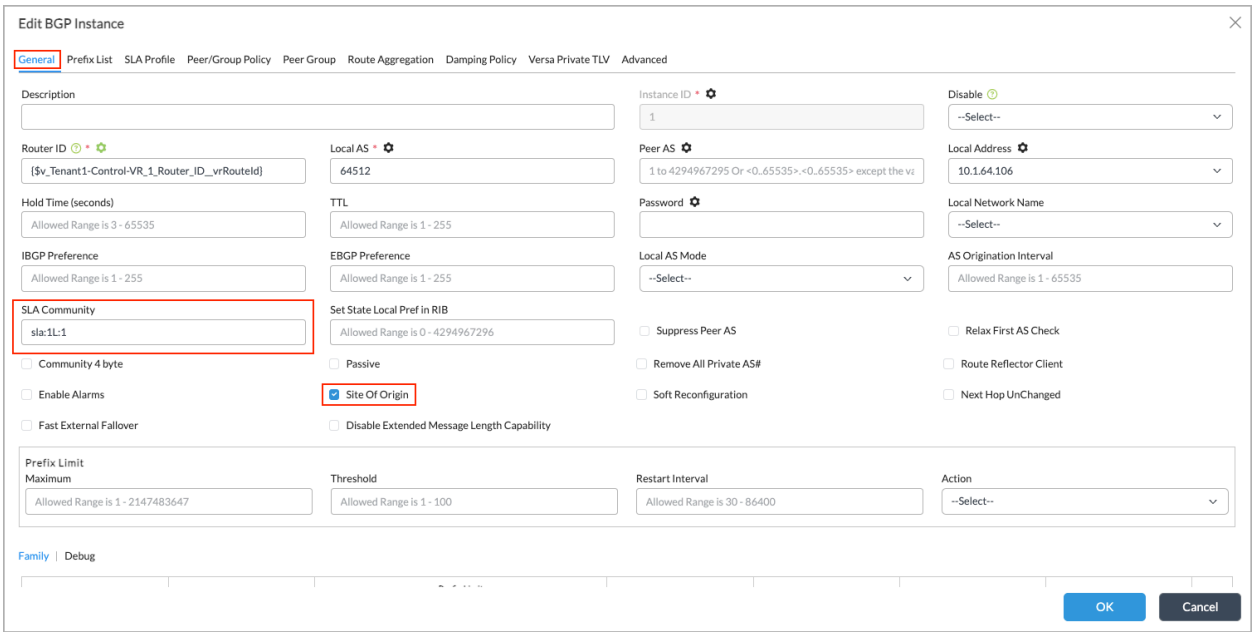
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates >Device Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a post-staging template in the main panel. The view changes to Appliance view.
2. Select Configuration > Networking > Virtual Routers. The main pane displays a list of virtual routers.



3. Select the name of a tenant control virtual router. The Edit-*Tenant*-VR popup window displays.



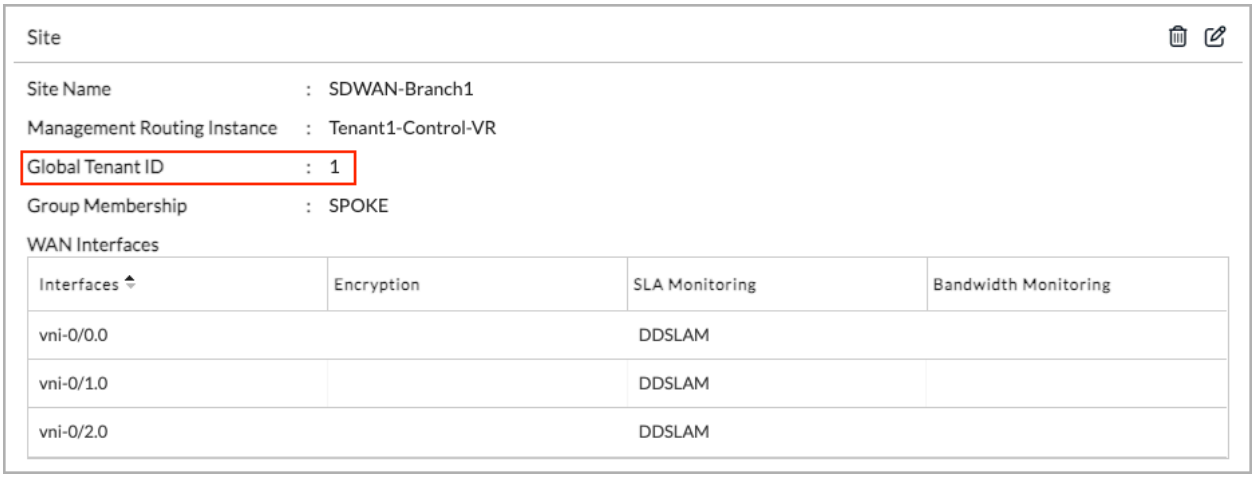
4. Select BGP. The BGP Instances screen displays.
5. Select an Instance ID number. The Edit BGP Instance popup window displays.



6. Select the General tab.
7. In the SLA Community field, enter the SLA community string in the format sla:*tenant-ID*L:*tenant-ID.* For the global tenant ID 1, which is the ID shown in the screenshot in Step 3 in the previous section, the community string is sla:1L:1. Note that the global tenant ID appears twice in the SLA community string.

   If you do not know the global tenant ID number, locate it on the Site popup window:

   a. In Appliance view, select the Configuration tab in the top menu bar, and select Services > SD-WAN > Site in the left menu bar. The main pane displays the site information. In the example screen below, the global tenant ID is 1.

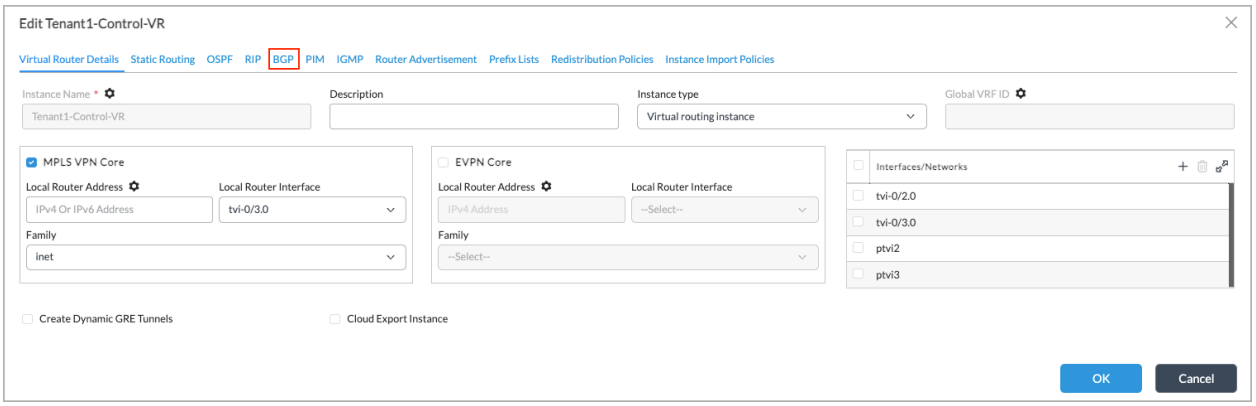


8. In the Edit BGP Instance window, under the General tab, click Site of Origin.
9. Click OK.

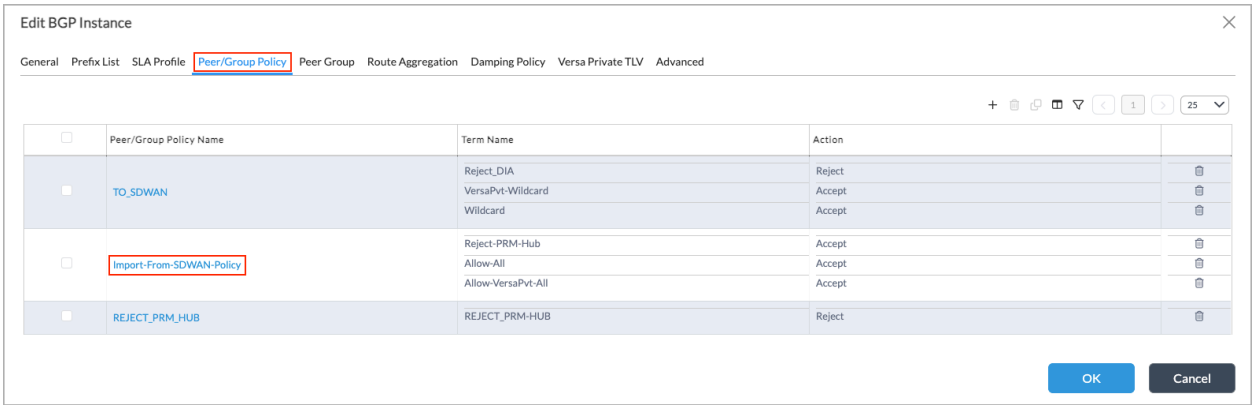
If there are more than two promoted hubs in the network, you need to reject routes learned from the additional promoted hubs to prevent those hubs from advertising the static LAN route. This configuration is applied to the existing peer policy Import_From_SDWAN_Policy on all hubs, and it is associated with the existing peer group Controllers-Group. You should add only the policy Reject-PRM-HUB, with a specified community string, to the Controllers-Group peer group.

To specify the Reject-PRM-HUB policy match condition and action to reject routes learned from additional promoted hubs:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a post-staging template in the main panel. The view changes to Appliance view.
2. Select Configuration > Networking > Virtual Routers. The main pane displays a list of virtual routers.
3. Select a Control-VR routing instance in the main pane. The Edit-*Tenant*-Control-VR screen displays.

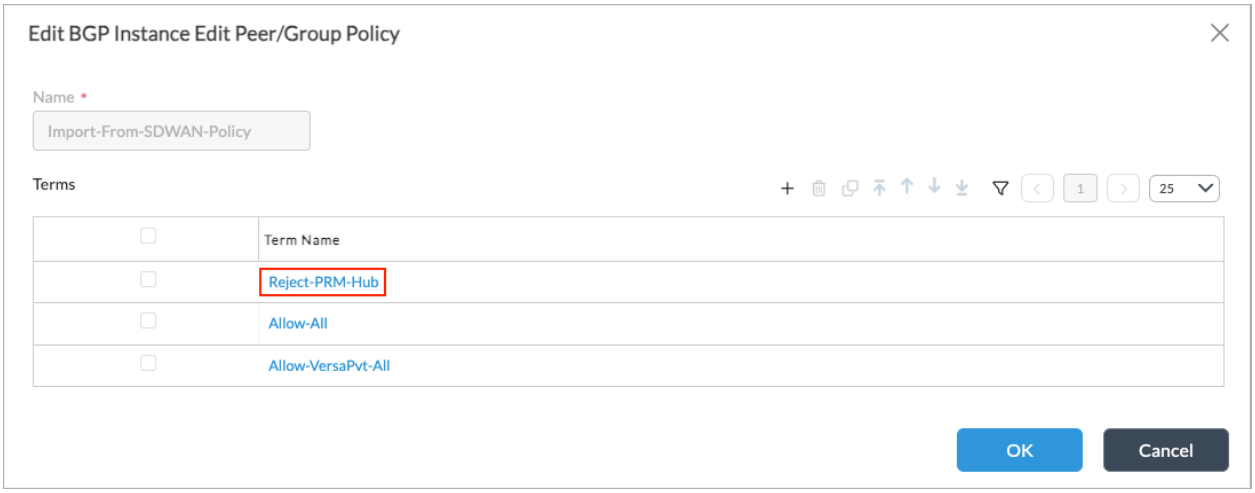


4. Select BGP in the horizontal menu bar.
5. In the main pane, click the instance ID. The Edit BGP Instance screen displays.

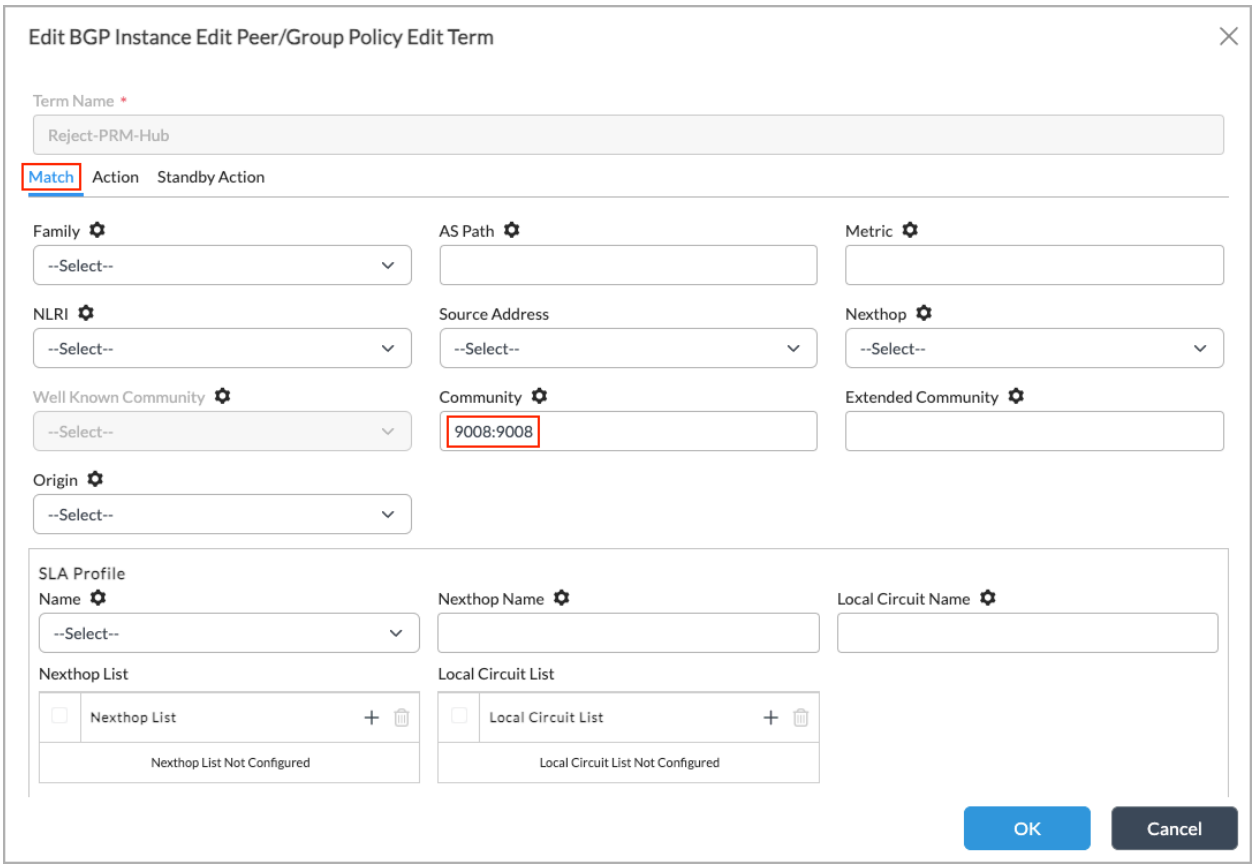


6. Select the Peer/Group Policy tab and click Import-From-SDWAN-Policy. The Edit BGP Instance > Edit Peer/Group

Policy screen displays.

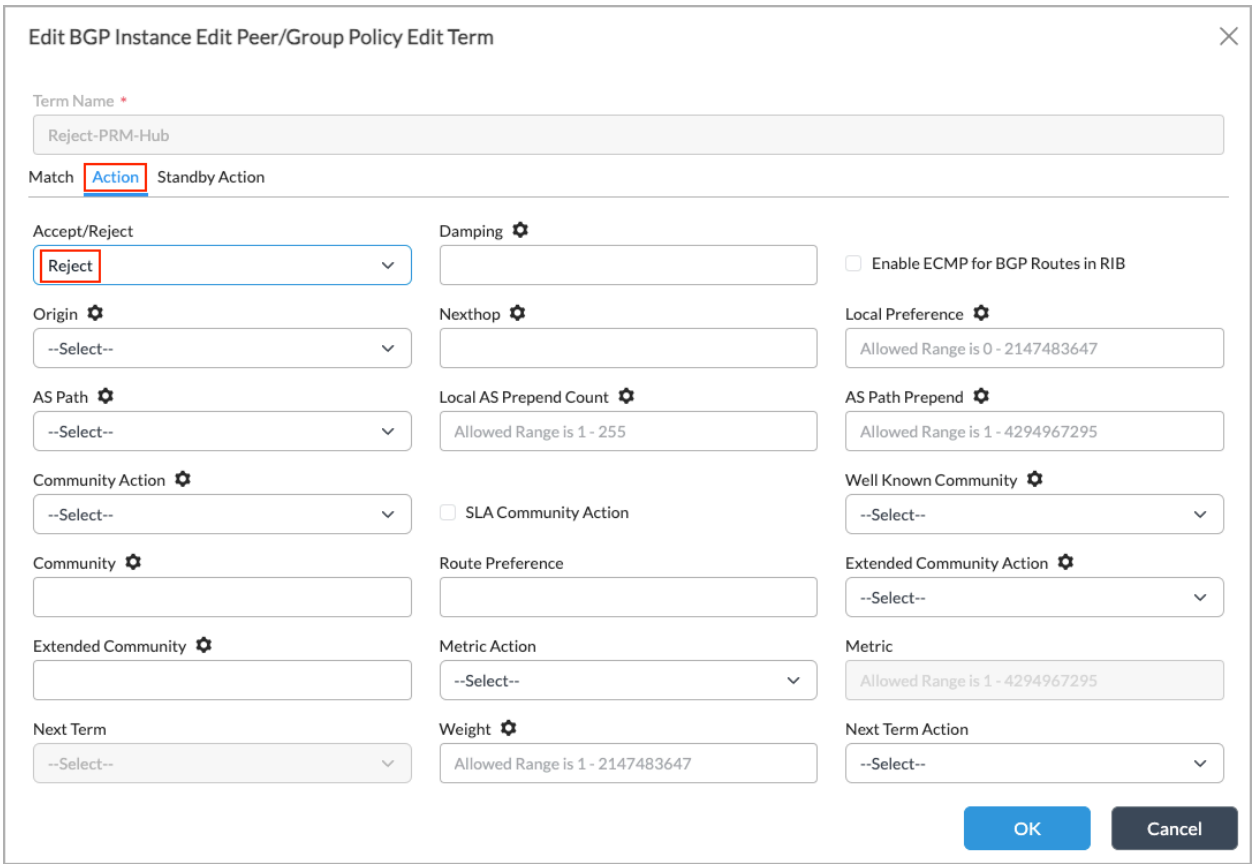


7. Select the Reject-PRM-HUB term. The Edit BGP Instance > Edit Peer/Group Policy > Edit Term window displays and the Match tab is selected.

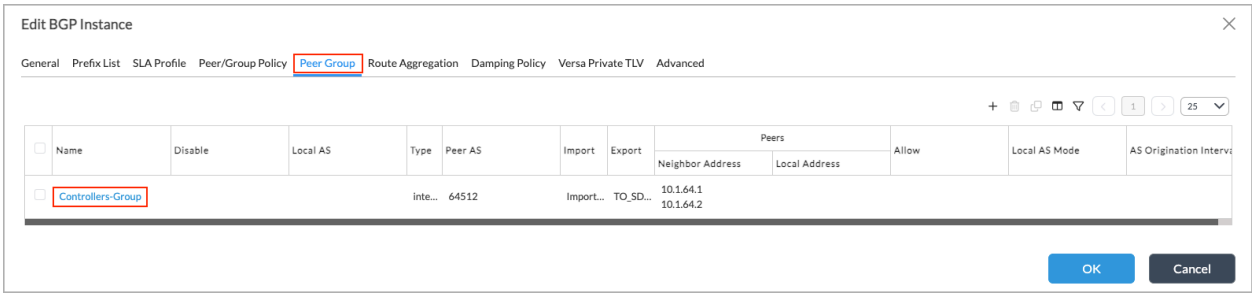


8. In the Community field, enter the community value. The community value should be a unique number. The numbers on either side of the colon do not need to be the same.

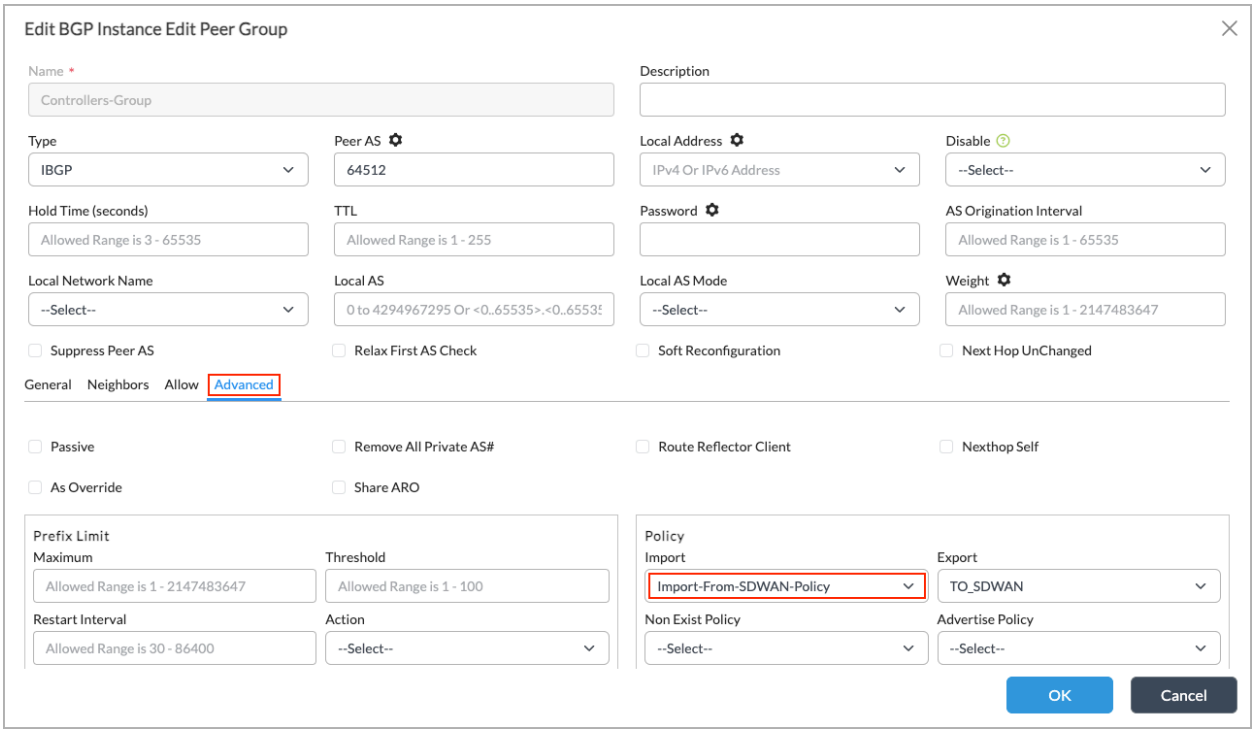
9. Select the Action tab.
10. In the Accept/Reject field, select Reject, to reject routes from the additional promoted hubs.



11. Click OK in the Edit BGP Instance > Edit Peer/Group Policy > Edit Term window and in the Edit BGP Instance > Edit Peer/Group Policy window.
12. In the Edit BGP Instance screen, select the Peer Group tab. The screen displays a table of BGP peer groups that are already configured.



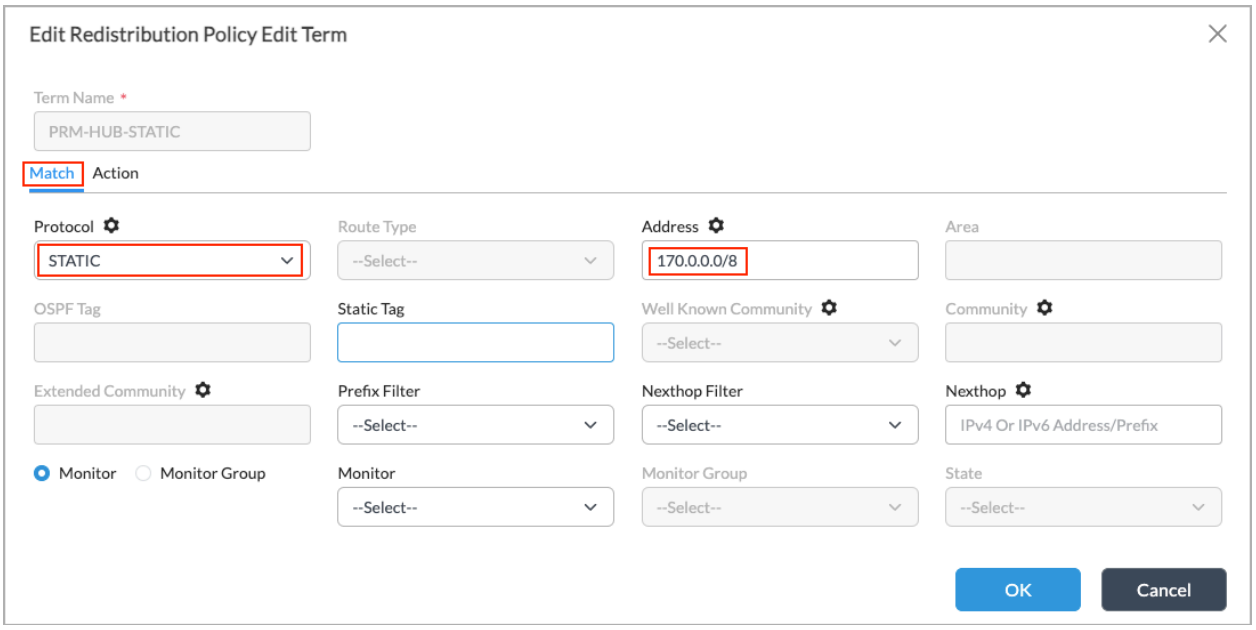
13. Click Controllers-Group. The Edit BGP Instance Edit Peer Group popup window displays.
14. Click the Advanced tab.



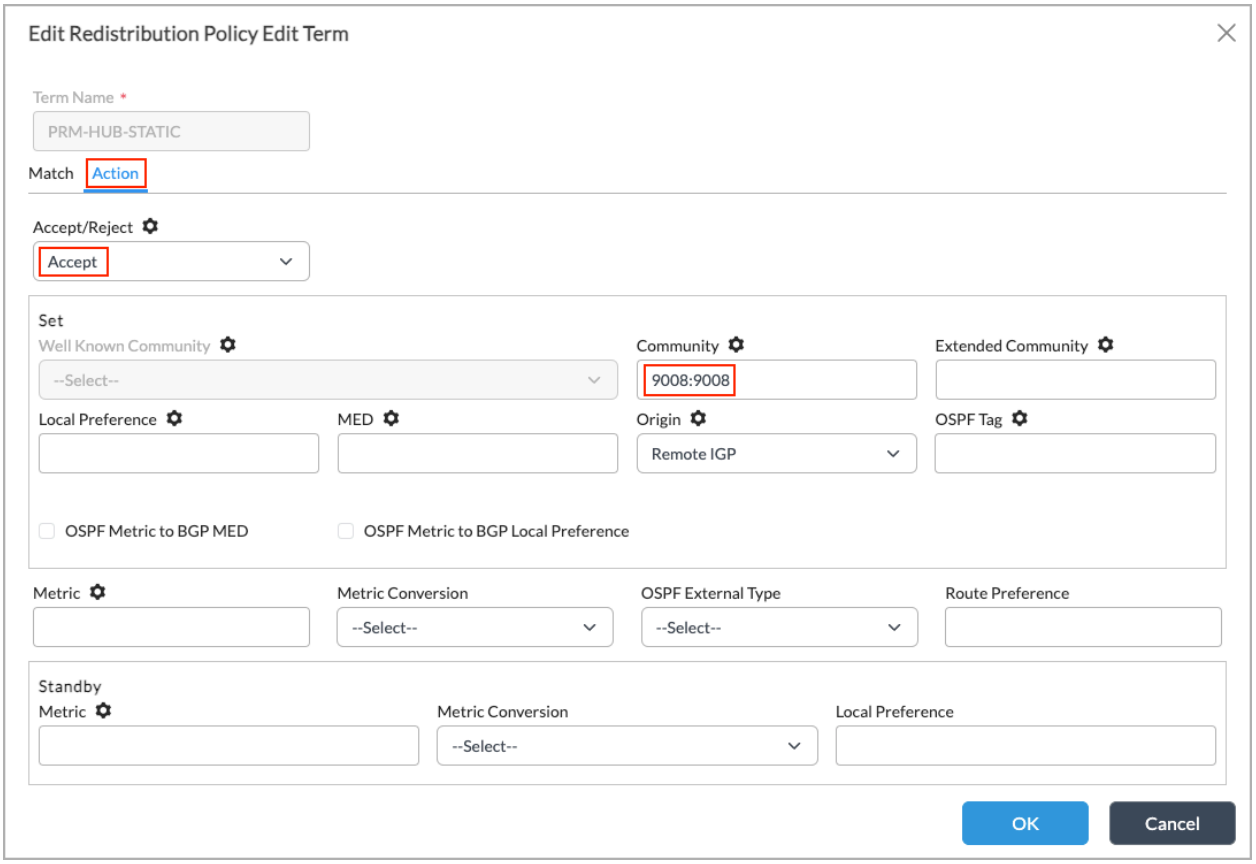
15. In the Policy group of fields, in the Import field, select Import-From-SDWAN-Policy.
16. Click OK.

Then, you specify the LAN redistribution policy match condition and the LAN redistribution policy action to enable data-driven SLA monitoring on all branches. This procedure creates a static route to the promoted hub so that all branches advertise their routes to the hub. The IP addresses for all the branches should be in the same range as the IP address of the promoted hub (which, here, is 172.0.0.0/8).

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the horizontal menu bar.
   d. Select a post-staging template in the main panel. The view changes to Appliance view.
2. Select Configuration > Networking > Virtual Routers. The main pane displays a list of virtual routers.
3. Select a Control-VR routing instance in the main pane. The Edit-VR screen displays.
4. Select Redistribution Policies in the left menu.
5. Select the name of the redistribution policy. The Edit Redistribution Policy popup window displays.
6. Select the term name. The Edit Redistribution Policy Edit Term popup window displays.
7. Select the Match tab.
8. In the Protocol field, select STATIC.
9. In the Address field, enter the aggregated IP address of the promoted hub's LAN routing instance.



10. Select the Action tab.



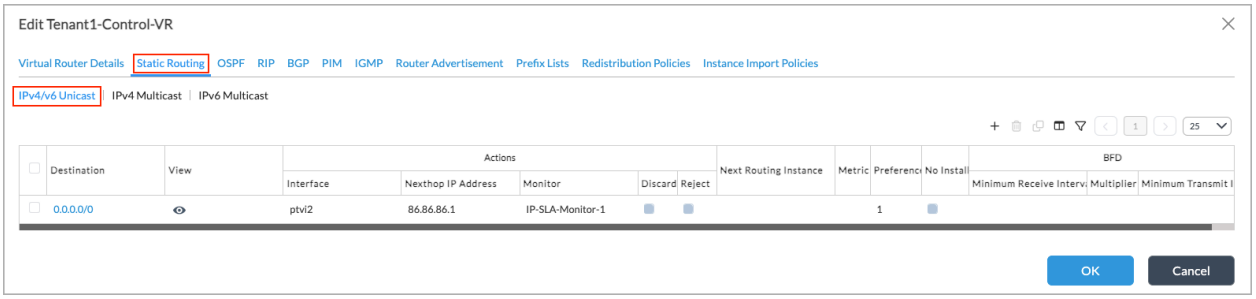
11. In the Accept/Reject field, select Accept.

12. In the Community Field, enter a unique community string.
13. Click OK.

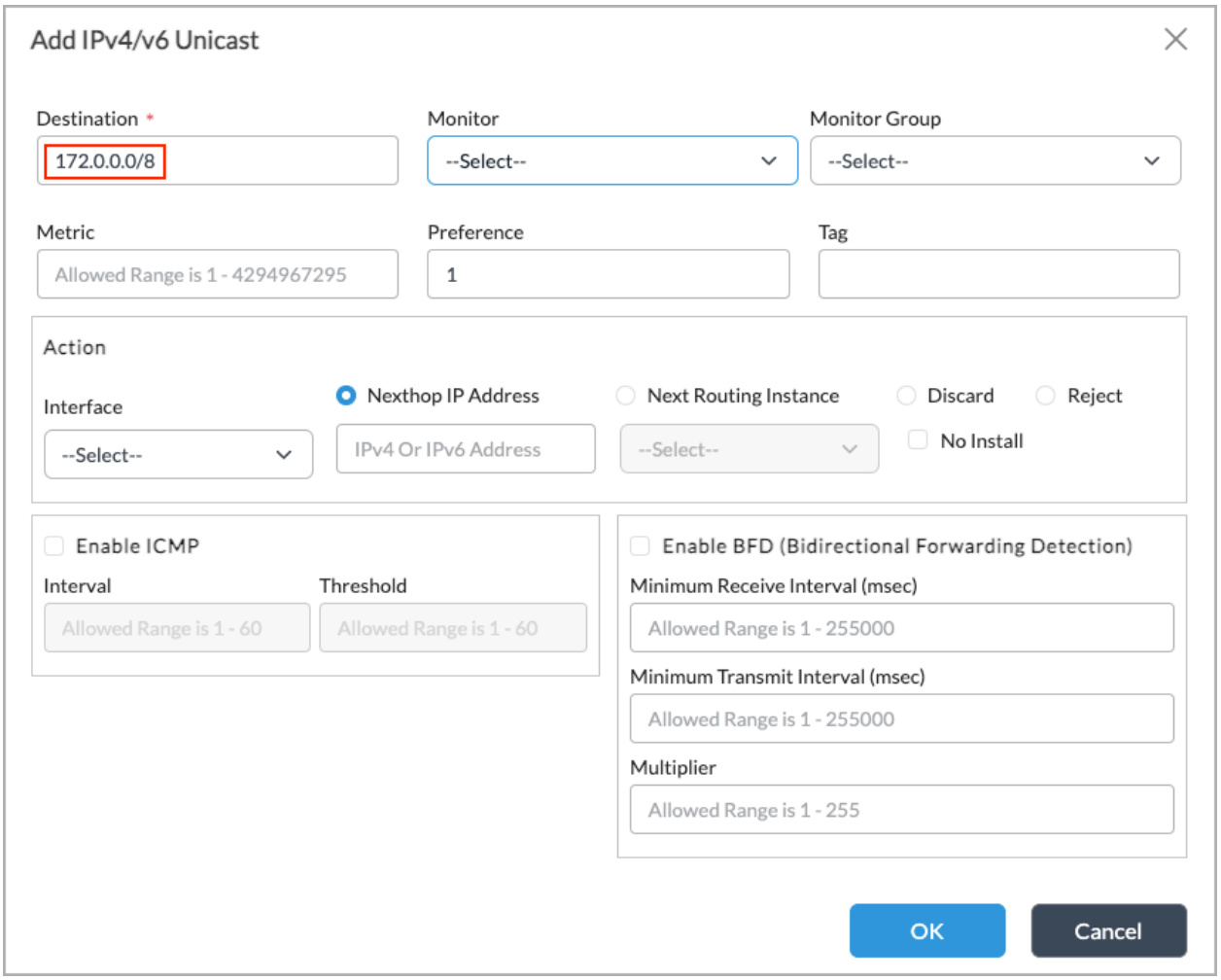
Add an Aggregate Static Route for Spoke LAN Routes

You can add an aggregate static route to create an alternate path through a hub:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a post-staging template in the main panel. The view changes to Appliance view.
2. Select Configuration > Networking > Virtual Routers. The main pane displays a list of virtual routers.
3. Click the name of a virtual router in the main pane. The Edit <*Tenant*>-VR screen displays.
4. Select Static Routing in the left menu bar. The Static Routing screen displays.



5. Select the IPv4/v6 Unicast tab, and then click + the Add icon. The Add IPv4/v6 Unicast popup window displays.



6. Enter the IP address in the Destination field.
7. Click OK.

Configure Data-Driven SLA Monitoring on Spoke Devices

To configure data-driven SLA monitoring on spoke devices, you do the following:

1. Configure a LAN interface as the SLA endpoint.
2. Configure group membership for spokes.
3. Configure a data-driven SLA monitoring path policy for spokes.
4. Add terms (such as To-Controllers, To-Hubs, and To-Spokes) to the data-driven SLA monitoring path policy.
   Note : Move the HUB term configuration above "All spokes" if it has only match with remote-site-type "branch" as match condition.
5. Configure an end-to-end SLA monitoring policy for branches (spokes) located behind NAT devices.
6. Associate an end-to-end policy and also a data-driven SLA monitoring policy with WAN interfaces.

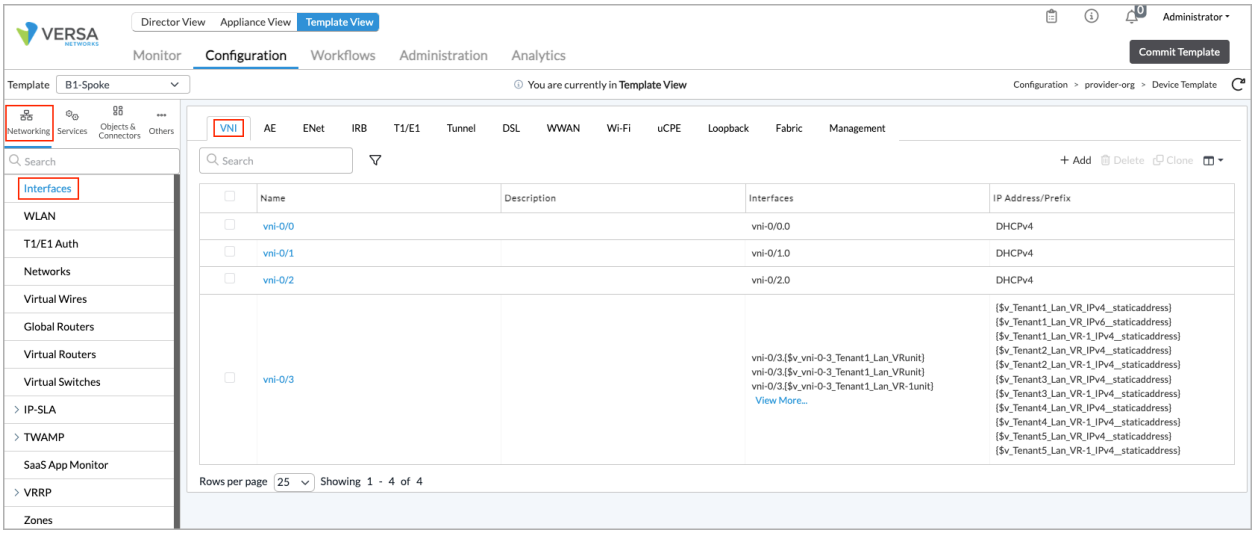
7. Associate the SLA-Community with the Tenant-Control-VR.

Configure a LAN Interface as the SLA Endpoint

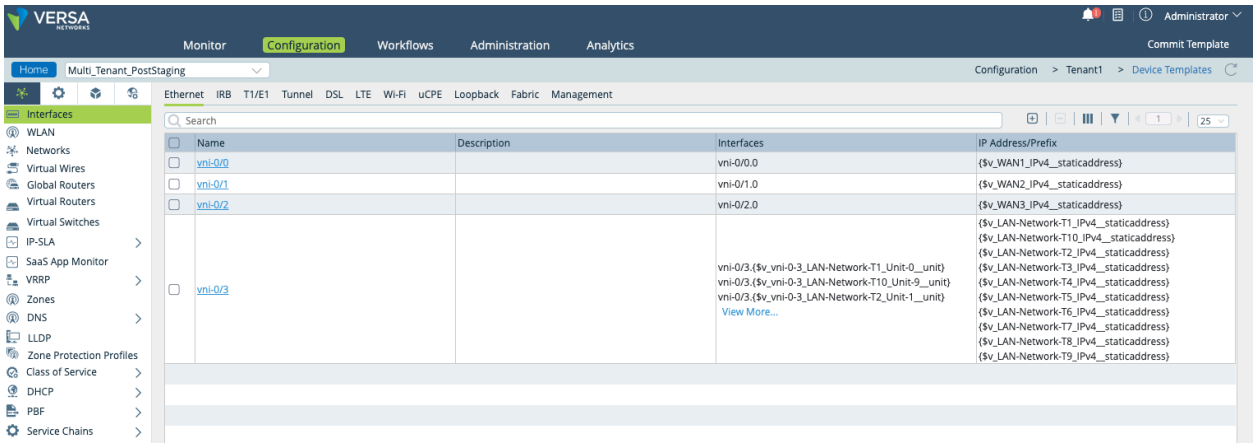
Specify a LAN interface as an SLA endpoint on each branch device on which data-driven SLA monitoring will be enabled:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a post-staging template from the main panel. The view changes to Appliance view.
2. Select Configuration > Networking > Interfaces. The Interfaces dashboard displays. In Release 22.1.3, the VNI tab selected by default. In Releases 21.2.2 and earlier, the Ethernet tab is selected by default.

   For Releases 22.1.3 and later:

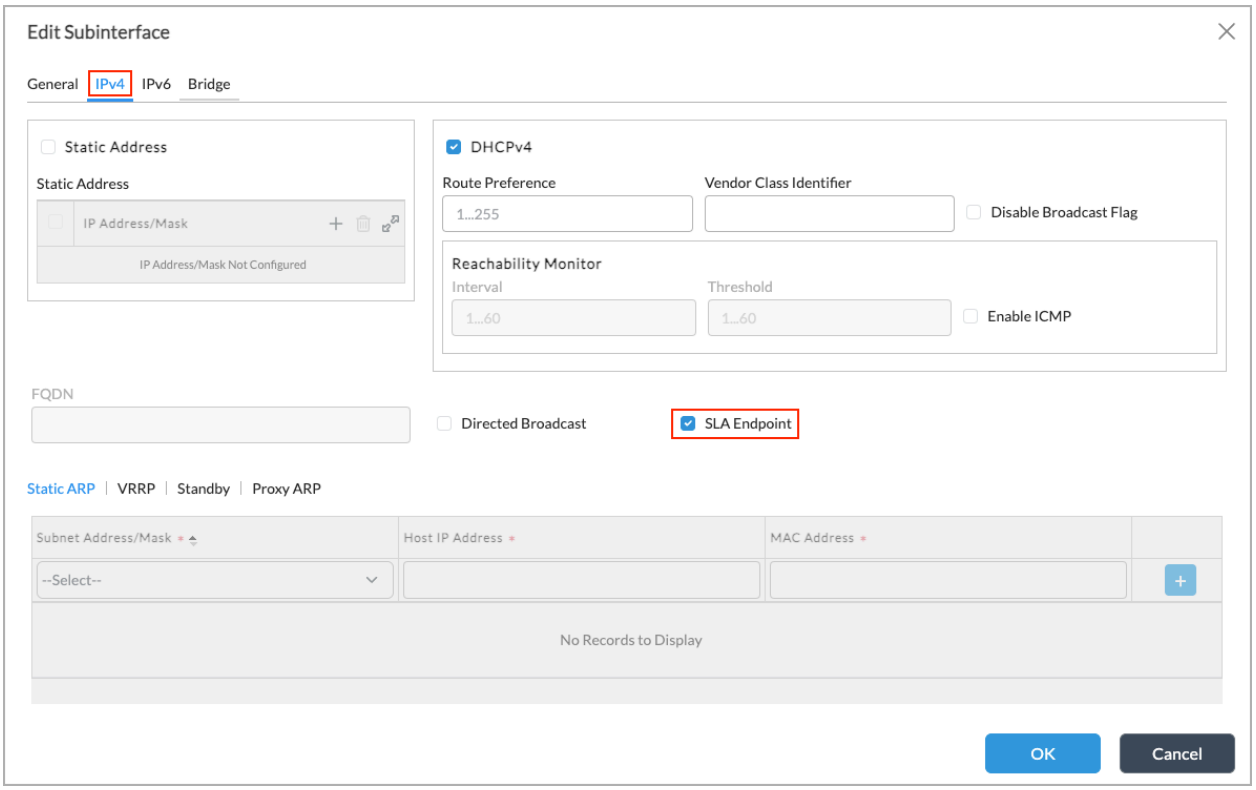


   For Releases 22.1.2 and earlier:



3. Select the appropriate interface from the list of interfaces on the Ethernet tab in the main panel. The Edit Ethernet Interface screen displays.

4. Click Subinterfaces on the Ethernet tab, and select the unit number. The Edit Subinterface screen displays.



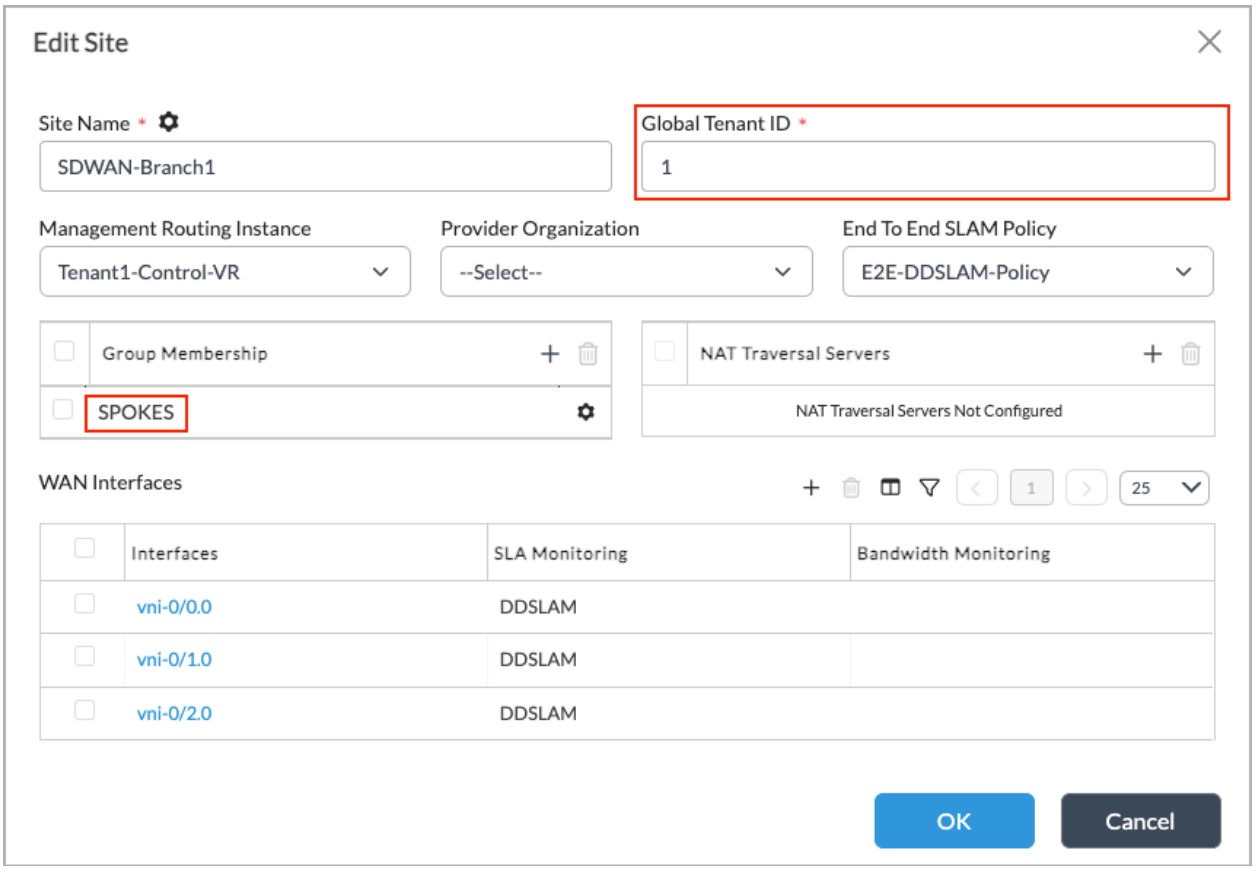
5. Select the SLA Endpoint checkbox.
6. Click OK.

Configure a Group Membership for Spoke Devices

When configuring a LAN interface as an SLA endpoint on each branch device, you configure a group membership that will apply to all spoke devices. Later, when you configure an SD-WAN path policy for spoke devices, you specify this group membership.

To configure a spoke group membership:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a post-staging template from the main panel. The view changes to Appliance view.
2. Select Configuration > Services > SD-WAN > Site. The Site dashboard displays.
3. Click the Edit icon in the Site table. The Edit Site screen displays.



4. Note the Global Tenant ID number of the site. You will use this ID number later in the procedure.

5. Click the + Add icon in the Group Membership table and enter a name for the spoke group. In the example above, the group is called SPOKES.
6. Click OK.

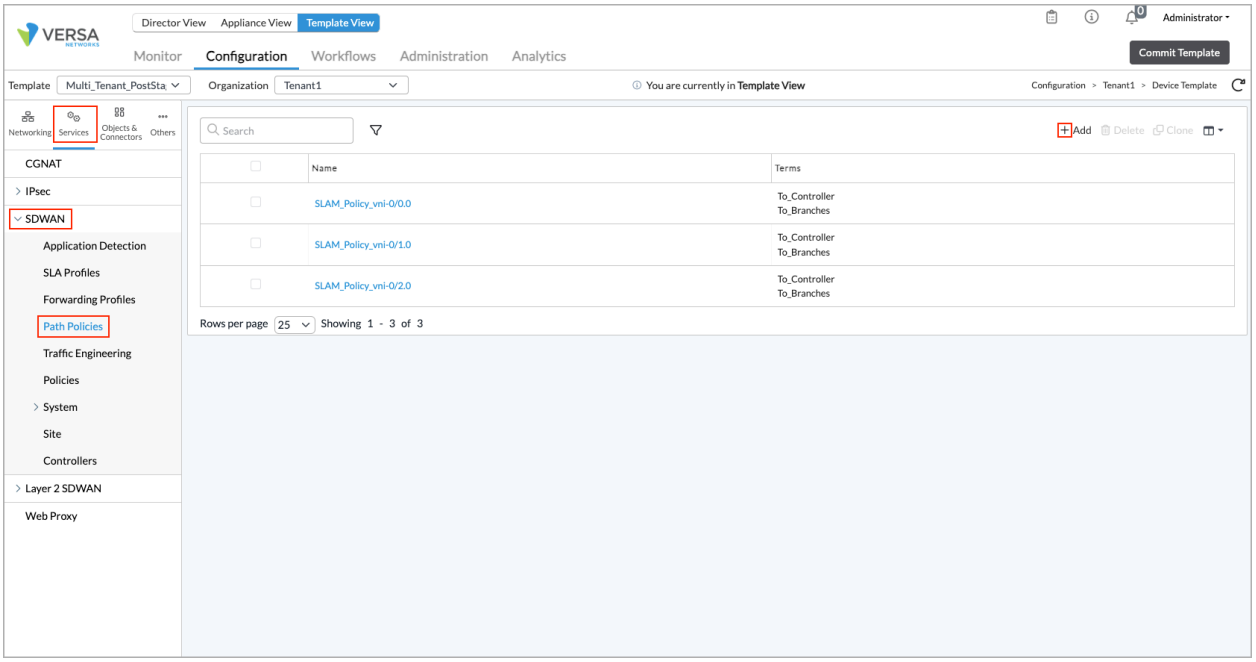
Configure an Data-Driven SLA Monitoring Path Policy for Spokes

To configure a data-driven SLA monitoring path policy for spoke devices, do the following:

1. In Director view:
    1. Select the Configuration tab in the top menu bar.
    2. Select Templates > Device Templates in the horizontal menu bar.
    3. Select an organization in the left navigation bar.
    4. Select a post-staging template from the main panel. The view changes to Appliance view.
2. Select Configuration > Services > SD-WAN > Path Policies. The Path Policies dashboard displays.

    Note that when you upgrade the software from Release 16.1R2 to Release 20.2, the VOS device preserves the path policies were present before the upgrade. For example, in the following screenshot, the SLAM_Policy_vni-0/0.0, SLAM_Policy_vni-0/1.0, and SLAM_Policy_vni-0/2.0 policies were configured previously and were preserved

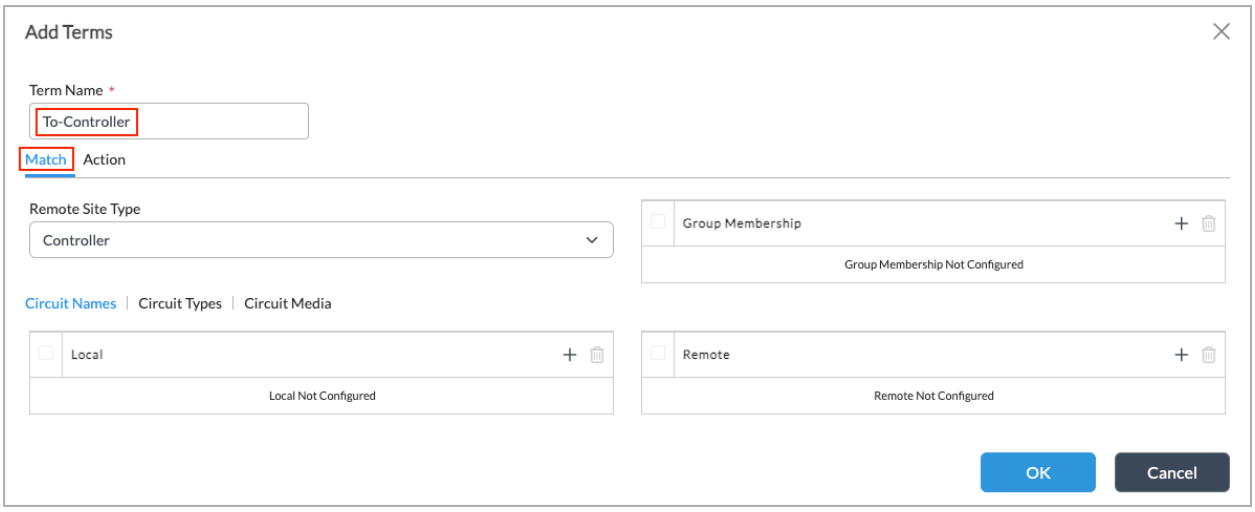
during a software upgrade. While you can configure data-driven SLA monitoring by editing these previously configured policies, it is recommended that you create a new path policy.



3. Click the Add icon to create a new path policy. The Add Path Policy popup window displays.
4. In the Policy Name field, enter a new for the new path policy. Here, the name is DDSLAM. In this policy, you define three terms, To Controllers, To Promoted Hubs, and To All Other Spokes, as described in the following steps.

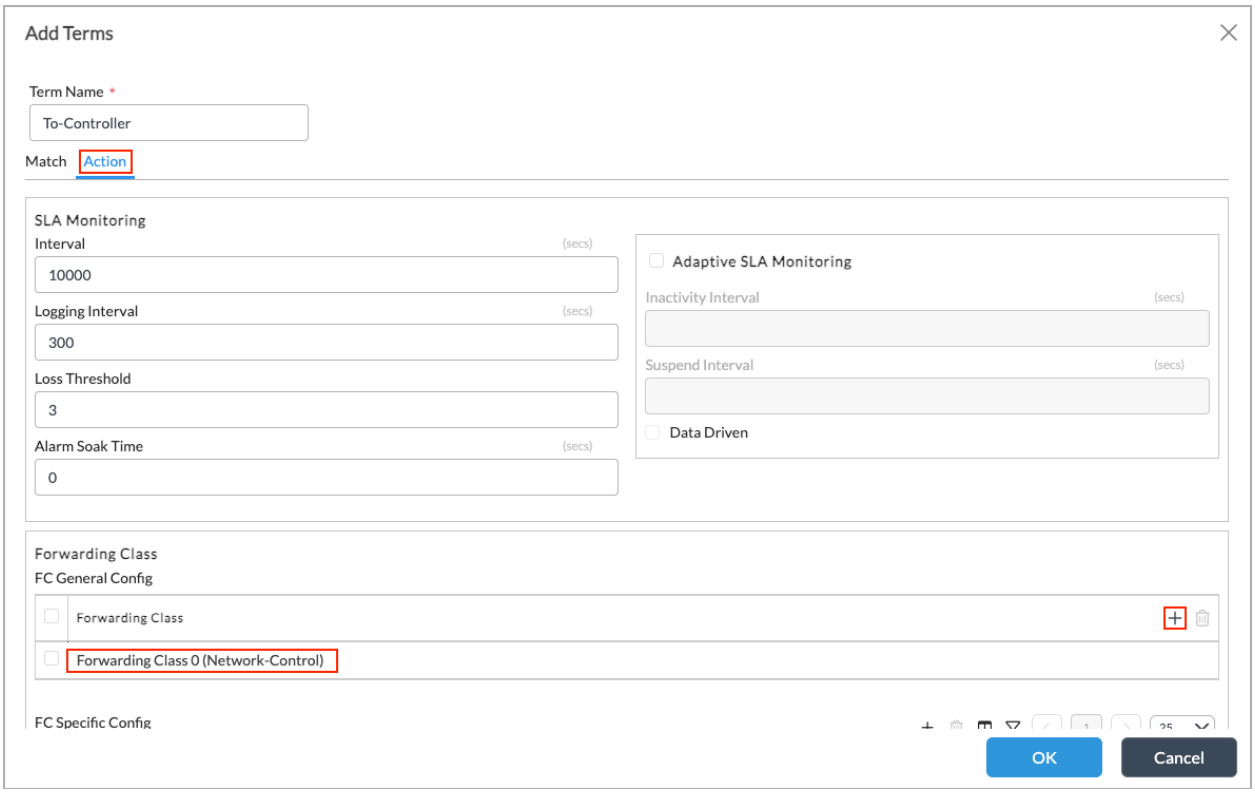
5. Define a match term and an action for Controller nodes to take based on forwarding class:

   a. Click the Add icon to create a new term. The Add Terms popup window displays, and the Match tab selected. Enter information for the following fields.



Field	Description
Term Name (Required)	Enter a name for a term. In the screenshot, the name is To-Controller.
Remote Site Type (Required)	Select Controller.
Circuit Names (Tab)	Configure the WAN circuits to match, by circuit name.
▪ Local	Click the + Add icon, and then select a WAN circuit name on the local branch. Circuits typically have names such as WAN1 and WAN2.
▪ Remote	Click the + Add icon, and then select a WAN circuit name on the remote branch.
Circuit Types (Tab)	Configure the circuits to match, by circuit type.
▪ Local	Click the + Add icon, and then select a WAN circuit type on the local branch. Circuits typically have types such as broadband, IP, and MPLS
▪ Remote	Click the + Add icon, and then select a WAN circuit type on the remote branch.
Circuit Media (Tab)	Configure the circuits to match, by circuit media.
▪ Local	Click the + Add icon, and then select a WAN circuit media on the local branch. Circuits typically have media such as cable, DSL, Ethernet, LTE, T1, and T3.
▪ Remote	Click the + Add icon, and then select a WAN circuit type on the remote branch.

b. Select the Action tab, and enter information for the following fields.

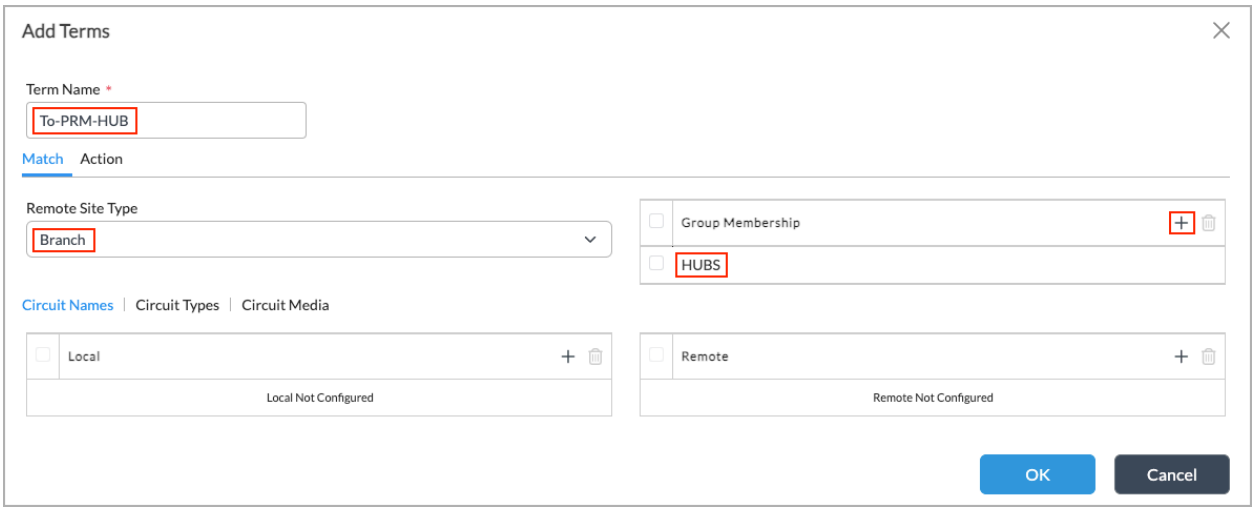


Field	Description
Forwarding Class (Group of Fields)	
▪ FC General Configuration	Click the + Add icon, and select a forwarding class.

c. Click OK.

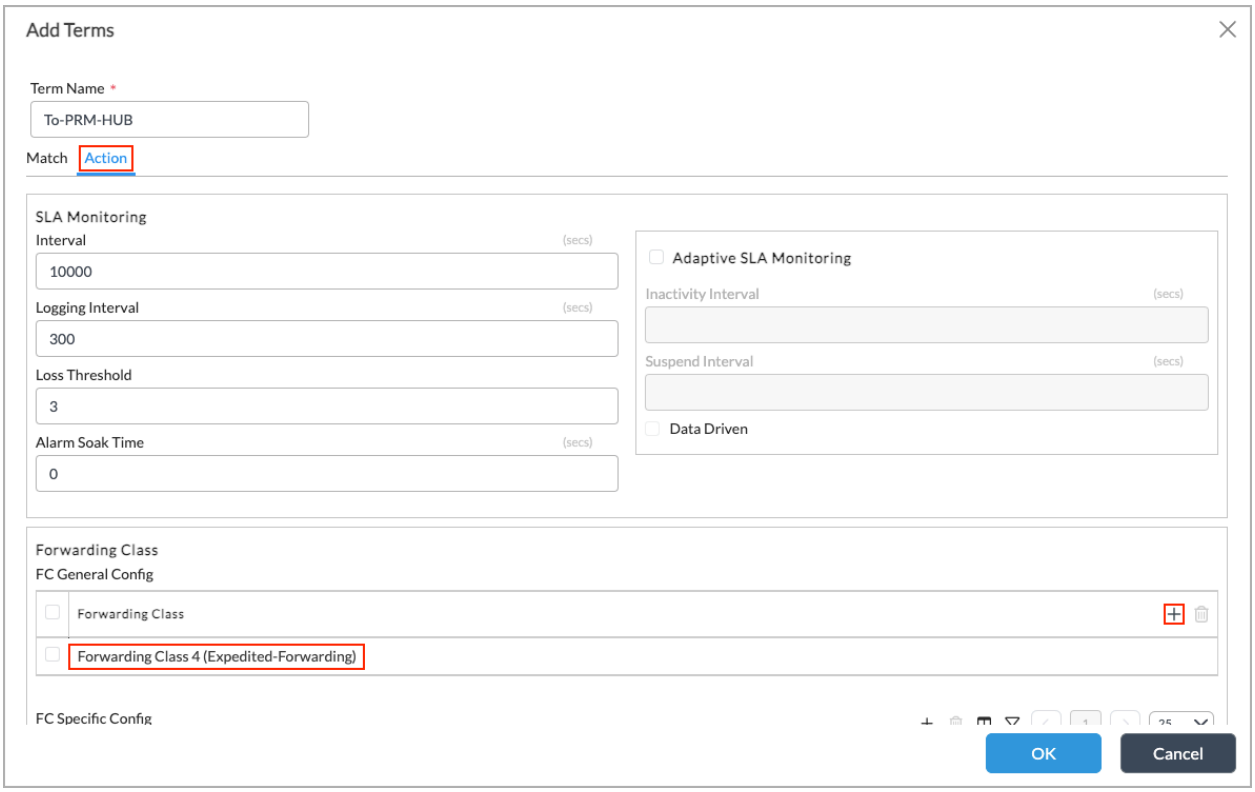
6. Define a match term and an action for promoted hubs to take based on forwarding class:

a. Click the + Add icon to create a new term. The Add Terms popup window displays, and the Match tab selected. Enter information for the following fields.



Field	Description
Term Name (Required)	Enter a name for a term. In the screenshot, the name is To-PRM-HUB.
Remote Site Type (Required)	Select Branch. If the only match criteria in the term is Branch, the term must be the first term in the path policy.
Group Member (Table) (Required)	Click the + Add icon, and select the name of the remote hub group that you created when configuring the hub device.

b. Select the Action tab, and enter information for the following fields.

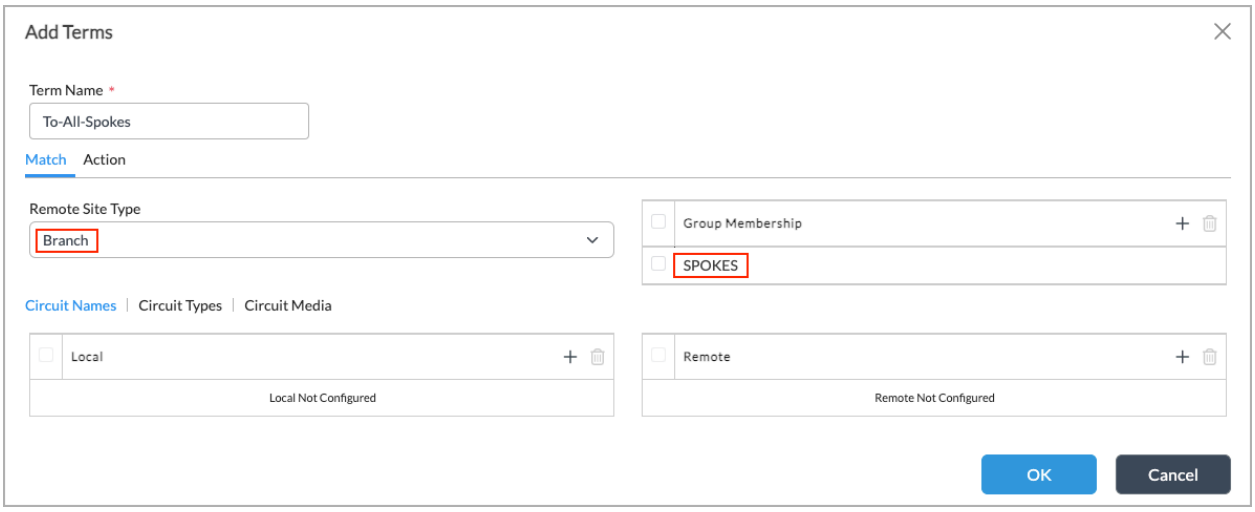


Field	Description
Forwarding Class (Group of Fields)	
▪ FC General Configuration	Click the + Add icon, and then select a forwarding class.

c. Click OK.

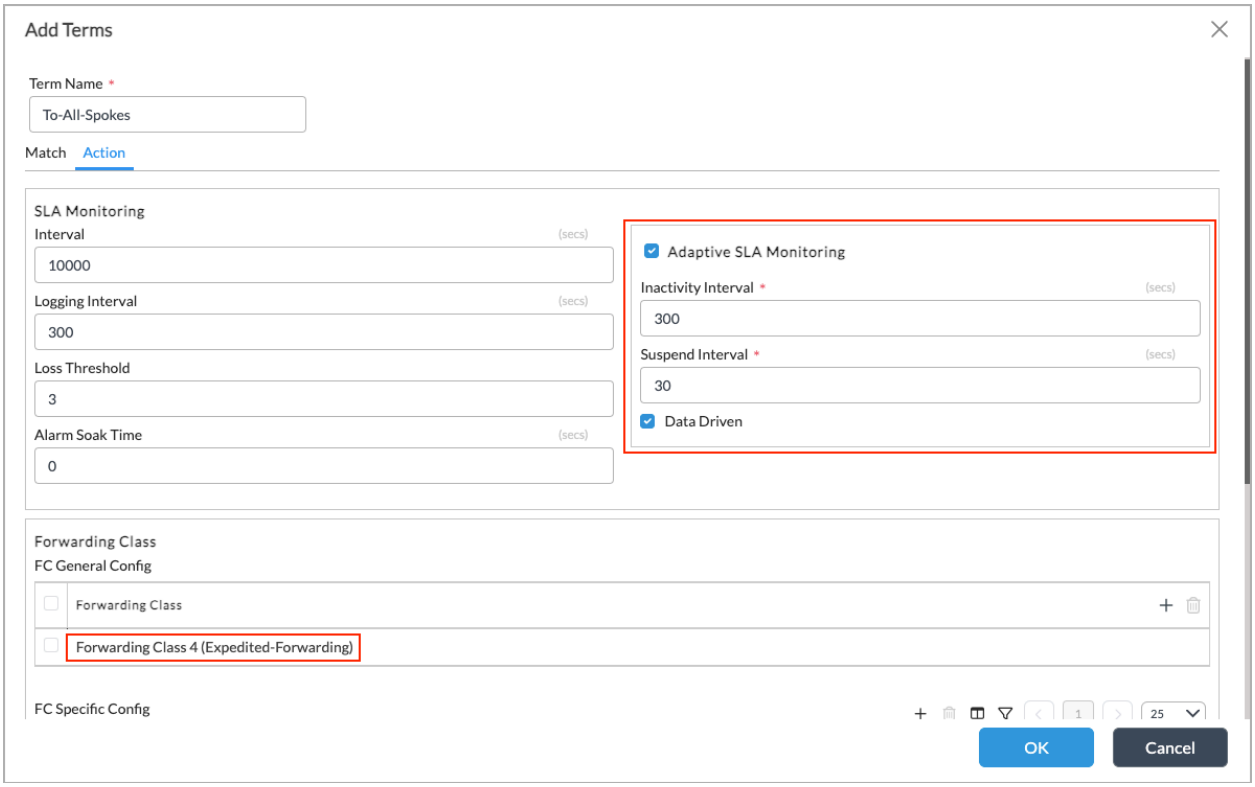
7. Define a match term or all other spokes, and in the action, apply a forwarding class to all matching spokes and enable data-driven SLA monitoring:

   a. Click the + Add icon to create a new term. Th Add Terms popup window displays, and the Match tab selected. Enter information for the following fields.



Field	Description
Term Name (Required)	Enter a name for a term. In the screenshot, the name is To-All-Spokes.
Remote Site Type (Required)	Select Branch. If the only match criteria in the term is Branch, the term must be the first term in the path policy.
Group Member (Table) (Required)	Click the + Add icon, and select a group name.

b. Select the Action tab, and enter information for the following fields.



Field	Description
Adaptive SLA Monitoring (Group of Fields)	
▪ Inactivity Interval	Enter the inactivity time interval for adaptive SLA monitoring. *Range*: 1 through 9000 seconds *Default*: 300 seconds
▪ Suspend Interval	Enter the suspend time interval for adaptive SLA monitoring. *Range*: 1 through 9000 seconds *Default*: 30 seconds
▪ Data Driven	Select to enable data-driven SLA monitoring.
Forwarding Class (Group of Fields)	
▪ FC General Configuration	Click the + Add icon, and then select a forwarding class.

c. Click OK.

Create an End-to-End Path Policy

Branches (spokes) that are located behind a NAT device may require an alternate path to ensure reachability. To create an alternate path, you configure a path policy that sends IP SLA packets on an end-to-end path over an alternate path that passes through a hub. The IP SLA packets are also used to trigger SLA monitoring probes from the destination site towards the source site. Therefore, you must create an end-to-end policy for all SD-WAN branches that use data-driven SLA monitoring.

To create an end-to-end path policy:

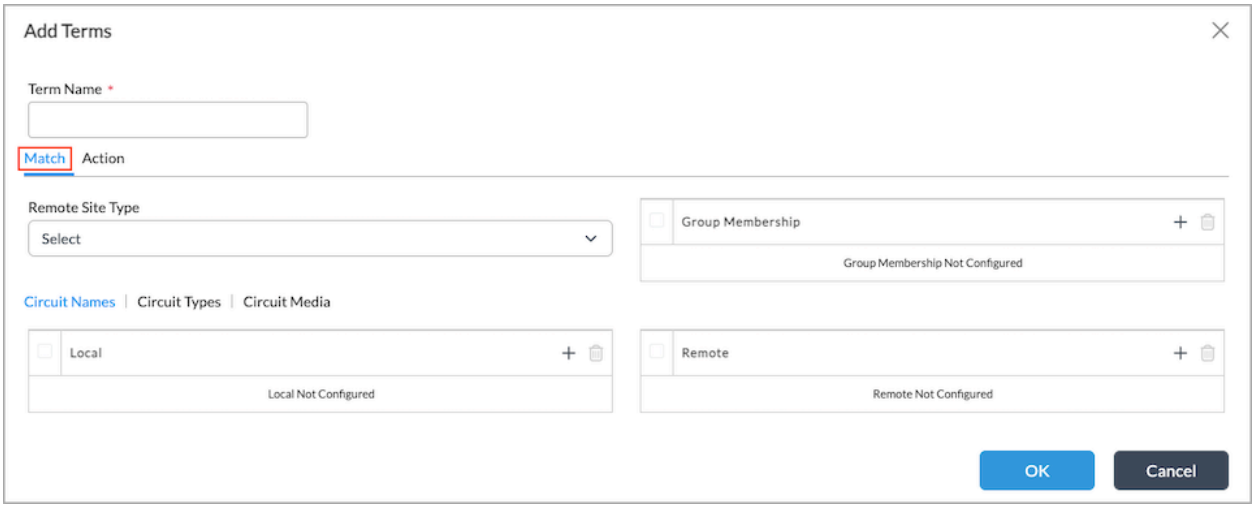
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.

c. Select an organization in the left navigation bar.

d. Select a post-staging template in the main pane. The view changes to Appliance view.

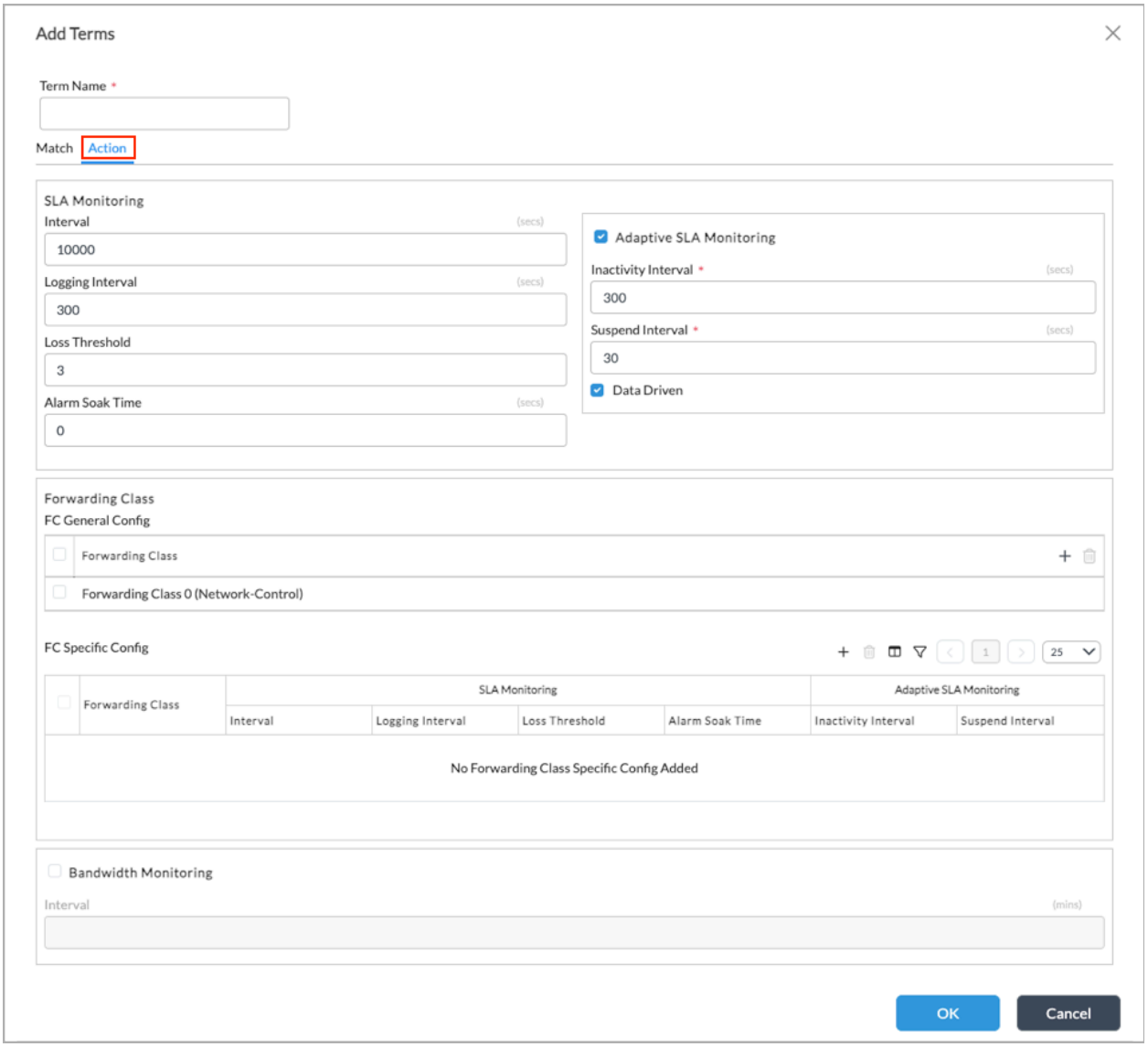
2. Select the Configuration tab in the top menu bar.
3. Select Services > SD-WAN > Path Policies in the left menu bar.
4. Click the + Add icon to create a new path policy. In the Add Path Policy popup window, enter a name for the policy in the Policy Name field.

5. Click the + Add icon to create a new term. The Add Term popup window displays, and the Match tab is selected. Enter information for the following fields.



Field	Description
Term Name (Required)	Enter a name for a term. In the screenshot, the name is To-All-Remote-Spokes.
Remote Site Type (Required)	Select Branch.

6. Select the Action tab, and enter information for the following fields.



Field	Description
Adaptive SLA Monitoring (Group of Fields)	
◦ Inactivity Interval	Enter the inactivity time interval for adaptive SLA monitoring. *Range*: 1 through 9000 seconds *Default*: 300 seconds
◦ Suspend Interval	Enter the suspend time interval for adaptive SLA monitoring. *Range*: 1 through 9000 seconds *Default*: 30 seconds
◦ Data Driven	Select to enable data-driven SLA monitoring.
Forwarding Class (Group of Fields)	
◦ FC General Configuration	Click the + Add icon, and select a forwarding class.
Bandwidth Monitoring	Click to enable bandwidth monitoring. Enter how often to monitor the link bandwidth, in minutes. *Range*: 10 to 300 minutes *Default*: None

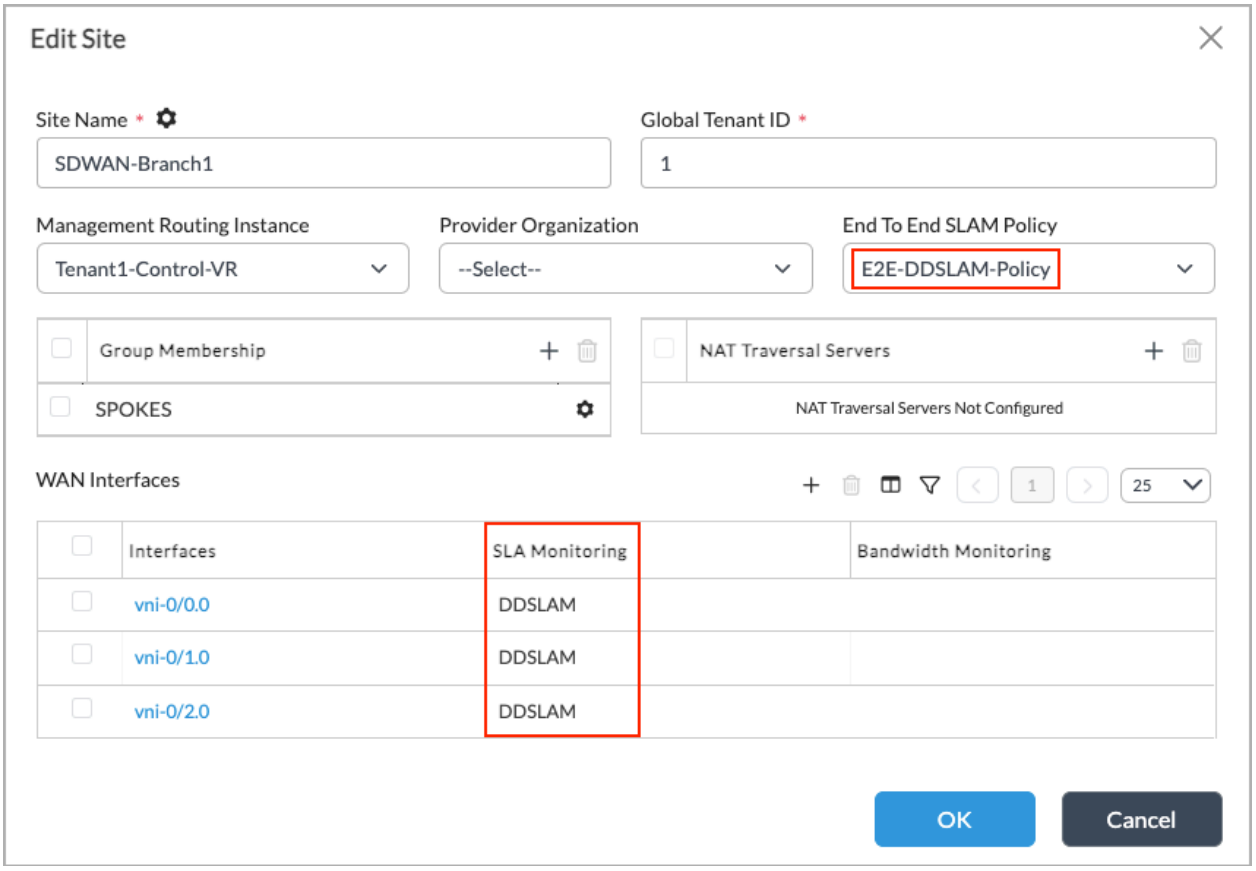
7. Click OK.

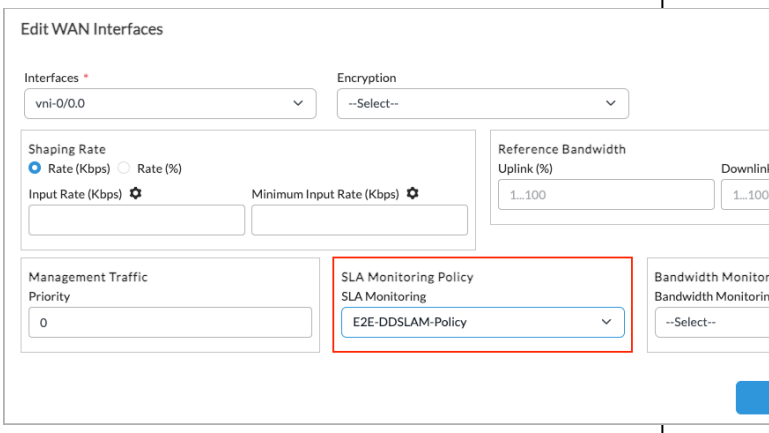
Associate the End-to-End and Data-Driven SLA Monitoring Path Policies with a WAN Interface

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.

d. Select a post-staging template in the main pane. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Services > SD-WAN > Site. The main pane displays the Site pane.
4. Click the Edit icon. In the Edit Site popup window, enter information for the following fields.



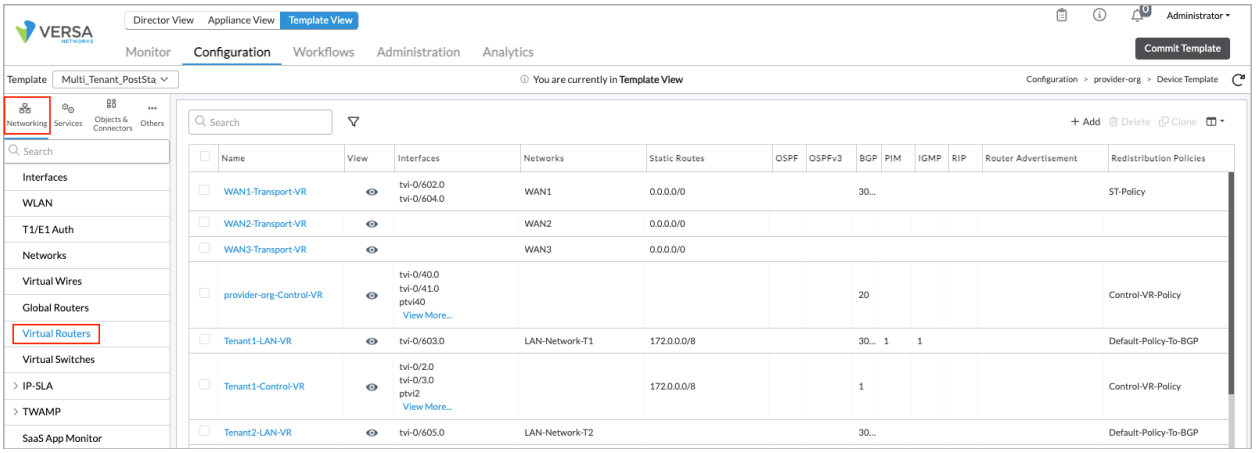
Field	Description
End-to-End SLAM Policy (Required)	Select the policy to use for the end-to-end path policy.
Group Membership (Required)	Select the SPOKES group.
WAN Interfaces (Table)	Select an interface name. The Edit WAN Interfaces popup window displays. In the SLA Monitoring Policy field, select the name of the policy to apply to the interface. 

5. Click OK.

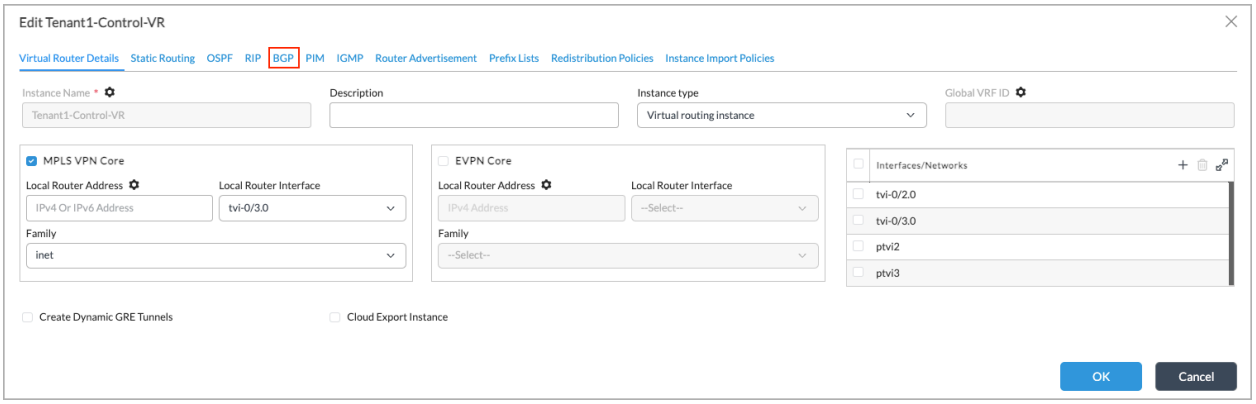
Configure SLA Community and Site of Origin

To configure the SLA community string and enable the site-of-origin (SoO) community string on the tenant's control VR:

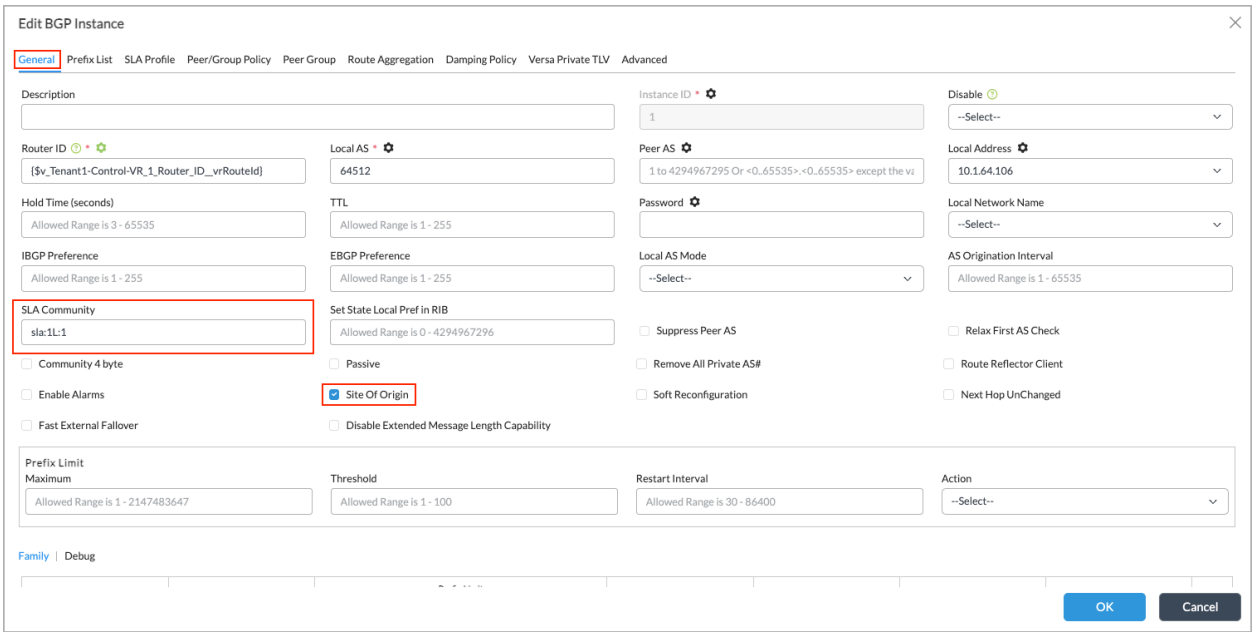
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates >Device Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a post-staging template in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar. The main pane displays a list of the virtual routers that are already configured.



4. Select the name of a tenant control virtual router. The Edit-VR popup window displays.



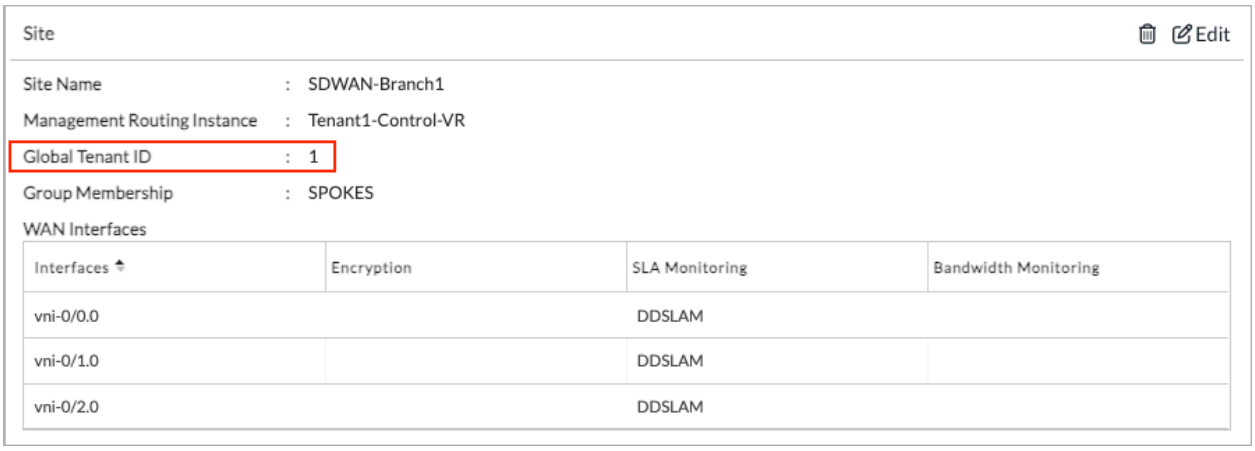
5. Select BGP. The main pane displays the BGP instances.
6. Select an Instance ID number. The Edit BGP Instance popup window displays.



7. Enter the SLA community string in the SLA Community field on the General tab. The SLA community string has format sla:*tenant-ID*L:*tenant-ID.* In the community string shown above, sla:1L:1, the global-tenant ID is 1, and it appears twice in the string.

   If you do not know the global-tenant ID number, you can find it on the Site dashboard:

   a. In Appliance view, go to Configuration > Services > SD-WAN > Site. The global tenant ID dipslays in the box labeled Site. In the example screen below, the Global Tenant ID is 1.



8. Click Site of Origin in the Edit BGP Instance screen.
9. Click OK.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Configure Automatic Bandwidth Monitoring
Configure SD-WAN Path Policies
Configure SD-WAN Traffic Steering
Configure SLA Monitoring for SD-WAN Traffic Steering