



# SonicOS and SonicOSX 7

## SD-WAN

### Administration Guide

SONICWALL®

# Contents

<b>About SD-WAN</b> .....	<b>4</b>
<b>SD-WAN Groups</b> .....	<b>5</b>
About SD-WAN Groups .....	5
Configuring SD-WAN Groups .....	6
Creating an SD-WAN Group .....	6
Editing an SD-WAN Group .....	7
Deleting an SD-WAN Group .....	7
Deleting Multiple SD-WAN Groups .....	8
<b>Performance Probes</b> .....	<b>9</b>
About Performance Probes .....	9
Configuring Performance Probes .....	10
Adding SD-WAN Performance Probes .....	11
Editing an SD-WAN Performance Probe .....	12
Deleting an SD-WAN Performance Probe .....	12
Deleting Multiple SD-WAN Performance Probes .....	13
<b>Performance Class Objects</b> .....	<b>14</b>
About Performance Class Objects .....	14
Configuring SD-WAN Performance Class Objects .....	15
Adding an SD-WAN Performance Class object .....	16
Editing an SD-WAN Performance Class Object .....	17
Deleting an SD-WAN Performance Class Object .....	17
Deleting Multiple SD-WAN Performance Class Objects .....	17
<b>Path Selection Profiles</b> .....	<b>18</b>
About Path Selection Profiles .....	18
Configuring Path Selection Profiles .....	19
Adding Path Selection Profile .....	19
Editing a Path Selection Profile .....	20
Deleting a Path Selection Profile .....	20
Deleting Multiple Path Selection Profiles .....	21
<b>SD-WAN Route Policies</b> .....	<b>22</b>
About SD-WAN Route Policies .....	22
Configuring SD-WAN Route Policies .....	23
Adding SD-WAN Route Policies .....	24
Editing SD-WAN Route Policies .....	25
Deleting SD-WAN Route Policies .....	25
Deleting Multiple SD-WAN Route Policies .....	26

<b>Monitoring SD-WAN</b> .....	<b>27</b>
<b>Viewing SD-WAN Route Policy Connections</b> .....	<b>28</b>
<b>SonicWall Support</b> .....	<b>30</b>
About This Document .....	31

# About SD-WAN

SD-WAN (Software-Defined Wide Area Network) provides software-based control over wide area network (WAN) connections. SonicOS SD-WAN offers these features:

- SD-WAN Interface Groups
  - WAN and VPN
  - Scalable from one to N interfaces
- Dynamic path selection based on:
  - Latency, jitter, and/or packet loss
  - User-defined thresholds for quality assessments
- Application-aware routing
- Path Performance Probes for metrics
- Connection-based traffic distribution
- Automatic connection failover over VPN
- Provisioning and management (GMS and Capture Security Center)

SD-WAN is best used for specific traffic types and/or applications requiring dynamically chosen optimal destination interfaces depending on how the network paths are behaving. To operate well, each application has a certain requirement from the network path. For example, the network quality for VoIP to operate well requires the optimal latency be 100 ms or less while a latency of 150 ms or higher results in choppy calls. SD-WAN helps in such scenarios by first dynamically measuring the various network performance metrics, such as latency, jitter and packet loss, on multiple network paths. SD-WAN then compares these metrics with the performance threshold for a particular traffic flow and determines the optimal network that meets the flow's network quality accordingly.

# SD-WAN Groups

## Topics:

- [About SD-WAN Groups](#)
- [Configuring SD-WAN Groups](#)

## About SD-WAN Groups

SD-WAN supports physical and virtual WAN interface types as well as VPN Numbered and Unnumbered Tunnel Interface instances, all choices provided while creating SD-WAN group.

Numbered Tunnel Interface groups are more evolved versions of the route-based implementations, and they are also far more intuitive to work with. However, they do scale poorly as they borrow from other actual entries in the interface table. Unnumbered Tunnel Interface configurations can meet the necessary scalability requirements because they are not tied to an interface table entry.

SD-WAN Groups are logical groups of interfaces that can be used for load-balancing as well as dynamic path selection based on the performance criterion through each interface path. You can create your own custom groups. For a description of SonicOS SD-WAN and its features, see [About SD-WAN](#).

The **SD-WAN Groups** page displays the custom pool of interfaces used for optimized and resilient traffic flow.

#	NAME	ZONE	IP ADDRESS	LINK STATUS	PRIORITY
1	U0	WAN	0.0.0.0	↓	1
	X1	WAN	10.203.28.158	↑	2

<b>Name</b>	Name of the SD-WAN group.
<b>Zone</b>	The zone of the interface member: <ul style="list-style-type: none"> <li>• WAN</li> <li>• VPN</li> </ul>
<b>IP Address</b>	IP address of the interface.

<b>Link Status</b>	Indicates whether the link is: <ul style="list-style-type: none"> <li>• <b>Link Up</b> (green)</li> <li>• <b>Link Down</b> (red)</li> </ul>
<b>Priority</b>	Priority of the interface in the group.

## Configuring SD-WAN Groups

### Topics:

- [Creating an SD-WAN Group](#)
- [Editing an SD-WAN Group](#)
- [Deleting an SD-WAN Group](#)
- [Deleting Multiple SD-WAN Groups](#)

## Creating an SD-WAN Group

You can create multiple SD-WAN Groups to meet your requirements.

### To add an SD-WAN group:

1. Navigate to **Network | SDWAN > Groups**. Note the Unnumbered Tunnel Interfaces included as an interface configuration option in an SD-WAN group.
2. Click the **Add** icon.  
The **Add SD-WAN Group** dialog displays.



3. Enter a descriptive name in the **Name** field.

4. Select one or more interfaces from the **Not in Group** list. Member interfaces can be only WAN, Numbered or Unnumbered Tunnel Interfaces.
  - ① | **IMPORTANT:** An interface cannot be a member of more than one SD-WAN group.
  - ① | **IMPORTANT:** The maximum number of interfaces that can be added in an SD-WAN group is 10.
5. Click the **Right Arrow** to move the selected interfaces to the **In Group** column.
6. To change the priority of the selected group members:
  - a. Select the interface.
  - b. Click the **Up Arrow** or **Down Arrow**.
7. Repeat Step 6 for each interface to prioritize.
8. Click **Add**.  
If the group is created, a confirmation message is displayed.
9. Click **Close**.

## Editing an SD-WAN Group

### To edit an SonicOS/X group:

1. Navigate to **Network | SDWAN > Groups**.
2. Hover over an SD-WAN group, click the **Edit** icon of the group to edit.



The **Edit SD-WAN group dialog** is displayed.

3. Make required changes as described in [Creating an SD-WAN Group](#).
4. Click **Save**.

## Deleting an SD-WAN Group

### To delete an SD-WAN group:

1. Navigate to **Network | SDWAN > Groups**.
2. Hover over an SD-WAN group, click the **Delete** icon.
3. Click **Confirm**.  
The message confirming the deletion of SD-WAN group is displayed.

# Deleting Multiple SD-WAN Groups

## *To delete SD-WAN groups:*

1. Navigate to **Network | SDWAN > Groups**.
2. Select the groups to delete.  
① | **NOTE:** To select all the groups, select the checkbox in the header row of the SD-WAN Groups table.
3. Click **Delete** icon at the upper-right corner of the page.
4. Click **Confirm**.



# Performance Probes

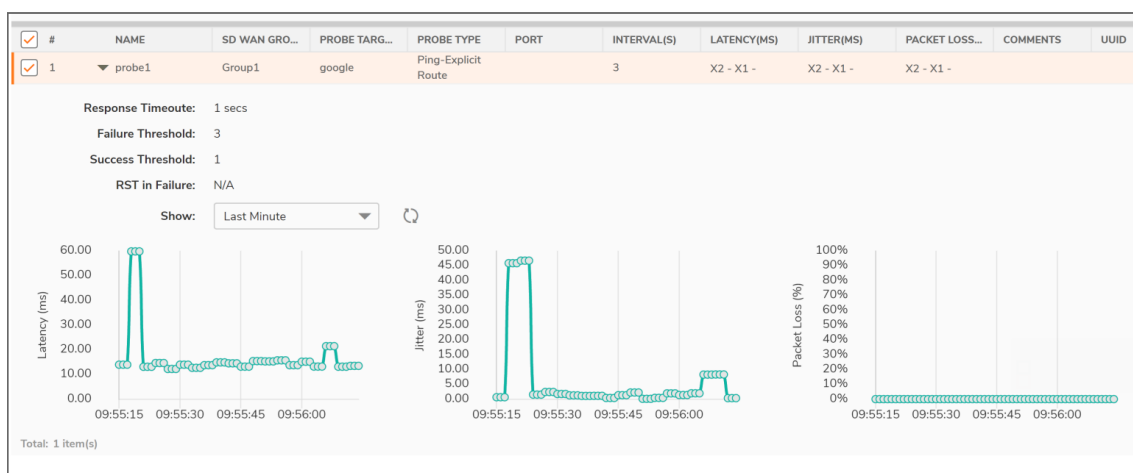
## Topics:

- [About Performance Probes](#)
- [Configuring Performance Probes](#)

## About Performance Probes

Network path performance metrics are determined using SD-WAN performance probes, which are similar to Network Monitor Probes. SonicOS supports ICMP and TCP probe types. An SD-WAN performance probe can be used by multiple Path Selection profiles (for further information, see [About Path Selection Profiles](#); for a description of SonicOS SD-WAN and its features, see [About SD-WAN](#)).

The **Network | SD-WAN > SLA Probes** page shows the dynamic performance data (latency/jitter/packet loss) and probe status for each path (interface) in the SD-WAN group, in both tabular and graphic displays. The display can show data for the last minute (default), last day, last week, or last month.



<b>#</b>	Number of the probe. The Collapse/Expand icon toggles the display of the graphs.
<b>NAME</b>	Name of the SD-WAN performance probe.
<b>SD-WAN GROUP</b>	Name of the SD-WAN group associated with the SD-WAN performance probe. Mousing over the entry displays properties about the SD-WAN group.
<b>PROBE TARGET</b>	Target address object of the SD-WAN performance probe. Mousing over the

	entry displays the host address.
<b>PROBE TYPE</b>	Type of performance probe: <ul style="list-style-type: none"> <li>• <b>Ping–Explicit Route</b></li> <li>• <b>TCP–Explicit Route</b></li> </ul> <p>ⓘ <b>NOTE:</b> When - TCP – Explicit Route is selected along with the RST Response Counts as Miss field, the Port field also becomes available.</p>
<b>PORT</b>	Port for the SD-WAN performance probe. The minimum/maximum values are 1 to 65535. <p>ⓘ <b>NOTE:</b> Ports are displayed only for TCP - Explicit Route probe types. A hyphen (-) displays for Ping - Explicit Route probe types.</p>
<b>INTERVAL (S)</b>	Time between SD-WAN performance probes, in seconds.
<b>LATENCY (MS)</b>	Round trip delay for the probes sent through a particular path/interface to reach the probe target and acknowledge back, in milliseconds. This is also displayed as a graph below the probe's entry in the <b>Performance Probe</b> table.
<b>JITTER (MS)</b>	Variation in the latency measurements for the probes through a particular path/interface, in milliseconds. This is also displayed as a graph below the probe's entry in the Performance Probe table.
<b>PACKET LOSS (%)</b>	Percentage of probes that are missed of the probes sent through a particular path/interface. This is also displayed as a graph below the probe's entry in the Performance Probe table.
<b>ADDITIONAL INFO</b>	When you hover over the icon, you can view the data for the following: <b>Response timeout, Success Threshold, Failure Threshold, &amp; RST in Failure.</b>
<b>COMMENTS</b>	Displays the comment entered when the performance probe was configured.

## Configuring Performance Probes

### Topics:

- [Adding SD-WAN Performance Probes](#)
- [Editing an SD-WAN Performance Probe](#)
- [Deleting an SD-WAN Performance Probe](#)
- [Deleting Multiple SD-WAN Performance Probes](#)

# Adding SD-WAN Performance Probes

① **IMPORTANT:** A performance Probe is created automatically for an SD-WAN Group containing a VPN numbered tunnel interface/unnumbered tunnel interface. You do not need to create an additional performance probe.

## To add a performance probe for non-VPN SD-WAN Groups:

1. Navigate to **Network | SDWAN > SLA Probes**.
2. Click the **Add** icon.  
The **Add SD-WAN Performance Probe** dialog is displayed.

The screenshot shows the 'Add SD-WAN Performance Probe' dialog box. It contains the following fields and options:

- Name: test1
- SD-WAN Group: test
- Probe Target: X0 IP
- Probe Type: Ping-Explicit Route
- Port: (empty)
- Probe hosts every: 3 seconds
- Reply time out: 1 seconds
- Probe state is set to DOWN after: 3 missed intervals
- Probe state is set to UP after: 1 successful intervals
- RST Response Counts As Miss: (unchecked)
- Comment: (empty)

Buttons: Cancel, Add

3. Enter a meaningful name in the **Name** field.
4. Select an SD-WAN group from **SD-WAN Group** drop-down menu.
5. Select an address object from **Probe Target**.
6. From **Probe Type**, select:
  - **Ping (ICMP)** - Explicit Route (default); go to Step 8.
  - **TCP** - Explicit Route; the **Port** field becomes available.
7. Enter the port number of the explicit route in the **Port** field.
8. Enter the interval between probes in the **Probe hosts every** field. The minimum is 1 second, the maximum is 3600 seconds, and the default is 3 seconds.  
① | **TIP:** The probe interval must be greater than the reply timeout.
9. Enter the maximum delay for a response in the **Reply time out ... seconds** field. The minimum is 1 second, the maximum is 60 seconds, and the default is 1 second.
10. Enter the maximum number of missed intervals before the performance probe is set to the DOWN state in the **Probe state is set to DOWN after ... missed intervals** field. The minimum number is 1, the maximum is 100, and the default is 3.
11. Enter the maximum number of successful intervals before the performance probe is set to the UP state in the **Probe state is set to UP after ... successful intervals** field. The minimum number is 1, the maximum is 100, and the default is 1.
12. If you selected TCP - Explicit Route for Probe Type, the RST Response Counts As Miss option becomes available. Select the option to count RST responses as missed intervals. This option is not selected by default.

13. Optionally, enter a comment in the `Comment` field.
14. Click **Add**.  
A confirmation message is displayed.

## Editing an SD-WAN Performance Probe

### To edit an SD-WAN performance probe:

1. Navigate to **Network | SDWAN > SLA Probes**.
2. Hover over the SD-WAN performance probe and click the **Edit** icon that appears.



3. The **Edit SD-WAN Performance Probe** dialog displays.
4. Make changes as described in [Adding SD-WAN Performance Probes](#).
5. Click **Save**.

## Deleting an SD-WAN Performance Probe

### To delete an SD-WAN performance probe:

1. Navigate to **Network | SD-WAN > SLA Probes**.
2. Hover over the SD-WAN performance probe and click the **Delete** icon that appears.



A confirmation message is displayed.

3. Click **Confirm**.

# Deleting Multiple SD-WAN Performance Probes

## *To delete multiple SD-WAN performance probes:*

1. Navigate to **Network | SDWAN > SLA Probes**.
2. Select the performance probes to delete.  
To delete all the performance probes, select the checkbox in the header row.
3. Click **Delete** icon above the table.
4. Click **Confirm**.

# Performance Class Objects

## Topics:

- [About Performance Class Objects](#)
- [Adding an SD-WAN Performance Class object](#)

## About Performance Class Objects

A Performance Class specifies the performance criterion for selecting the optimal path. It could be the:

- Best latency/jitter/packet loss among the existing paths.
- Performance Class Object that defines the metric thresholds for latency, jitter and packet loss.

You use SD-WAN Performance Class Objects to configure the desired performance characteristics for the application/traffic categories. These objects are used in the Path Selection Profile to automate the selection of paths based on these metrics. (For a description of SonicOS SD-WAN and its features, see [About SD-WAN](#).)

These are the default Performance Class Objects:

- **Lowest Jitter**
- **Lowest Latency**
- **Lowest Packet Loss**

① | **NOTE:** These default Performance Class Objects cannot be edited or deleted.

You can configure custom performance thresholds that best meet the needs of your application/traffic categories with custom Performance Class Objects. You can include or exclude the Latency, Jitter, or Packet Loss attributes in your custom object, although you cannot exclude all three attributes in the same object. When excluded, the value of that attribute is not used as a criterion or threshold when determining whether a particular path is qualified or not. For example, if you want to evaluate a particular path only on the Latency attribute but you don't care about the other attributes, you can include Latency and exclude Jitter and Packet Loss in your custom object.

① | **NOTE:** When SonicOS is upgraded to 7.0 from a previous version, all existing custom performance class objects are upgraded with the Include option enabled for Latency, Jitter, and Packet Loss.

VIEW		All			
#	NAME	LATENCY (MS)	JITTER (MS)	LOSS (%)	COMMENTS
1	Lowest Latency	LOWEST	-	-	Auto-added Perf Class Obj
2	Lowest Jitter	-	LOWEST	-	Auto-added Perf Class Obj
3	Lowest Packet Loss	-	-	LOWEST	Auto-added Perf Class Obj

<b>NAME</b>	Name of the Performance Class Object
<b>LATENCY (MS)</b>	Threshold time for the round trip delay for the probes sent through a particular path/interface to reach the probe target and acknowledge back, in milliseconds, in milliseconds. For the <b>Lowest Latency</b> Performance Class Object, the time is always <b>LOWEST</b> ; for the other default Performance Class Objects, a hyphen (–) displays.
<b>JITTER (MS)</b>	Threshold variation in the latency measurements for the probes through a particular path/interface, in milliseconds. For the <b>Lowest Jitter</b> Performance Class Object, the time is always <b>LOWEST</b> ; for the other default Performance Class Objects, a hyphen (–) displays.
<b>LOSS (%)</b>	Threshold percentage of probes that are missed of the probes sent through a particular path/interface. For the <b>Lowest Packet Loss</b> Performance Class Object, the percentage is always <b>LOWEST</b> ; for the other default Performance Class Objects, a hyphen (–) displays.
<b>COMMENT</b>	Displays the comment entered when the Performance Class Object was configured.

## Configuring SD-WAN Performance Class Objects

### Topics:

- [Adding an SD-WAN Performance Class object](#)
- [Editing an SD-WAN Performance Class Object](#)
- [Deleting an SD-WAN Performance Class Object](#)
- [Deleting Multiple SD-WAN Performance Class Objects](#)

# Adding an SD-WAN Performance Class object

## To add a Performance Class Object:

1. Navigate to **Network | SDWAN > SLA Class Objects**.
2. Click the **Add** icon.  
The **Add Performance Class** Object dialog appears.

The screenshot shows a dialog box titled "Add Performance Class Object". It contains the following fields and controls:

- Name:** A text input field containing "FTP\_per\_class\_obj".
- Include Latency:** A toggle switch that is turned on.
- Latency (ms):** A numeric input field containing "0".
- Include Jitter:** A toggle switch that is turned on.
- Jitter (ms):** A numeric input field containing "0".
- Include Loss:** A toggle switch that is turned on.
- Loss (%):** A numeric input field containing "0".
- Comment:** An empty text input field.
- Buttons:** "Cancel" and "OK" buttons at the bottom right.

3. Enter a meaningful name in the `Name` field.
4. Enable **Include Latency** to include the performance class latency attribute for this object, or clear the checkbox to exclude the latency attribute. This option is selected by default.
5. If **Include Latency** is enabled, enter the acceptable latency, in milliseconds, in the `Latency (ms)` field. The minimum is 0 milliseconds, the maximum is 1000 milliseconds, and the default is 0 milliseconds.
6. Enable **Include Jitter** to include the performance class jitter attribute for this object, or clear the checkbox to exclude the jitter attribute. This option is selected by default.
7. If **Include Jitter** is enabled, enter the acceptable jitter, in milliseconds, in the `Jitter (ms)` field. The minimum is 0 milliseconds, the maximum is 1000 milliseconds, and the default is 0 milliseconds.
8. Enable **Include Loss** to include the performance class packet loss attribute for this object, or clear the checkbox to exclude the packet loss attribute. This option is selected by default.
9. If **Include Loss** is enabled, enter the acceptable percentage of packet loss in the `Loss (%)` field. The minimum is 0, the maximum is 100, and the default is 0.  
**ⓘ | NOTE:** You cannot exclude all three attributes (Latency, Jitter, Packet Loss) in the same object.
10. Optionally, enter a comment in the `Comment` field.
11. Click **OK**.



# Editing an SD-WAN Performance Class Object

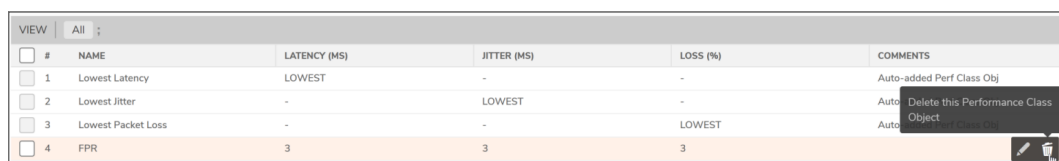
**To edit an SD-WAN performance class object:**

1. Navigate to **Network | SDWAN > SLA Class Objects**.
2. Hover over a performance class object, click the **Edit** icon. The **Edit SD-WAN Performance Class Object** dialog appears, make required changes as described in [Adding an SD-WAN Performance Class object](#).
3. Click **OK**.

# Deleting an SD-WAN Performance Class Object

**To delete an SD-WAN Performance Class Object:**

1. Navigate to **Network | SDWAN > SLA Class Objects**.
2. Hover over an object and click the **Delete** icon.



VIEW	All					
#	NAME	LATENCY (MS)	JITTER (MS)	LOSS (%)	COMMENTS	
<input type="checkbox"/>	1	Lowest Latency	LOWEST	-	-	Auto-added Perf Class Obj
<input type="checkbox"/>	2	Lowest Jitter	-	LOWEST	-	Auto
<input type="checkbox"/>	3	Lowest Packet Loss	-	-	LOWEST	Auto
<input type="checkbox"/>	4	FPR	3	3	3	Auto

3. Click **Confirm** in the confirmation prompt that is displayed.

# Deleting Multiple SD-WAN Performance Class Objects

**To delete multiple SD-WAN Performance Class Objects:**

1. Navigate to **Network | SDWAN > SLA Class Objects**.
2. Select the Performance Class Objects to delete.
3. Click **Delete** icon at the top of the Performance Class Object table. A confirmation message is displayed.  
① | **NOTE:** To delete all the performance class objects, click **Delete All** icon.
4. Click **Confirm**.

# Path Selection Profiles

## Topics:

- [About Path Selection Profiles](#)
- [Configuring Path Selection Profiles](#)

## About Path Selection Profiles

Path Selection Profiles (PSPs) are the settings that help to determine the network path or interface that satisfies a specific network performance criteria, from a pool of available network paths/interfaces. A qualified path or interface meets the performance class criteria.

The dynamic path selection mechanism is implemented using the PSP settings when associated with Policy-based Routes (PBR). When more than one network path meets the criterion (as per the performance class in the PSP), then traffic is load balanced among the qualified network paths/interfaces. When associated with a policy-based routing policy, a path selection profile helps select the optimal path among the SD-WAN interfaces for the application/service.

#	NAME	SD WAN GROUP	INTERFACE STATUS	SLA PROBE	SLA CLASS OBJECT	BACKUP INTERFACE	PROBE DEFAULT UP
1	test	tun1	UI - Qualified X1 - Qualified	test	TEST	None	✓

<b>Name</b>	Name of the Path Selection Profile.
<b>SD-WAN Group</b>	SD-WAN interface group to which the profile applies.
<b>Interface Status</b>	Status of the members of the SD-WAN interface group: <ul style="list-style-type: none"> <li>• <b>Qualified</b> (green)</li> <li>• <b>Not Qualified</b> (red)</li> </ul>
<b>Performance Probe</b>	Performance Probe used by the Path Selection Profile.
<b>Performance Class Object</b>	Performance Class Object used by the Path Selection Profile: <ul style="list-style-type: none"> <li>• <b>Lowest Latency</b></li> <li>• <b>Lowest Jitter</b></li> <li>• <b>Lowest Packet Loss</b></li> <li>• Custom Performance Class Object</li> </ul>

<b>Backup Interface</b>	Indicates the interface chosen when none of the SD-WAN group interfaces meet the performance criteria. If a backup interface was not chosen, <b>None</b> displays.
<b>Probe Default UP</b>	Indicates whether the default state of the performance probe is: <ul style="list-style-type: none"> <li>• <b>UP</b> (Checkmark icon)</li> <li>• <b>DOWN</b> (Crossmark icon)</li> </ul>

## Configuring Path Selection Profiles

### Topics:

- [Adding Path Selection Profile](#)
- [Editing a Path Selection Profile](#)
- [Deleting a Path Selection Profile](#)
- [Deleting Multiple Path Selection Profiles](#)

## Adding Path Selection Profile

### To add a Path Selection Profile:

1. Navigate to **Network | SDWAN > Path Selection Profiles**.
2. Click the **Add** icon above the table.

The **Add SD-WAN Path Selection Profile** dialog is displayed.

3. Add a meaningful name in the **Name** field.
4. From **SD-WAN Group**, select the SD-WAN interface group to which the profile applies. You have an option to create a new SD-WAN group from this dialog and then select the newly created group.
5. From **Performance Probe**, select the probe to use in the profile. A probe, if added for the SD wan group you selected, is displayed by default. Otherwise, select the appropriate probe.
6. From **Performance Class**, select the Performance Class Object for the dynamic selection of the optimal network path:

- **Lowest Latency**
- **Lowest Jitter**
- **Lowest Packet Loss**
- Custom Performance Class Object

You have an option to create a New Performance Class Object from the drop-down menu.

7. From Backup Interface, select the interface to use when all the SD-WAN Group interfaces fail to meet the performance criteria specified in **Performance Class**:
  - **None** (default)
  - Individual interface
  - VPN Tunnel Interface (if any)
8. To specify whether the default state of the performance probe should be treated as DOWN, disable **SLA Probe default state is UP**. This option is enabled by default and is treated as UP.
9. For path selection profiles with Non-VPN SD-WAN groups, if existing connections on the path should be reset when the path does not meet the performance criteria any more, select **Reset conditions if path does not meet the performance criteria**. This option is disabled by default.
10. Click **Save**.  
A confirmation message is displayed.

## Editing a Path Selection Profile

### *To edit a Path Selection Profile:*

1. Navigate to **Network | SDWAN > Path Selection Profiles**.
2. Hover over a path selection profile, click the **Edit** icon. The **Edit SD-WAN Path Selection Profile** dialog is displayed.
3. Make changes as described in [Adding Path Selection Profile](#).
4. Click **Save**.

## Deleting a Path Selection Profile

### *To delete an SD-WAN Path Selection Profile:*

1. Navigate to **Network | SDWAN > Path Selection Profiles**.
2. Hover over a path selection profile, click the **Delete** icon.
3. Click **OK** to confirm deletion.

# Deleting Multiple Path Selection Profiles

## To delete multiple Path Selection Profiles:

1. Navigate to **Network | SDWAN > Path Selection Profiles**.
2. Select the profiles that you want to delete.  
**NOTE:** To select all the profiles, click the checkbox in the header row of the **Path Selection Profiles** table.
3. Click the **Delete** icon above the Path Selection Profiles table.

<input checked="" type="checkbox"/>	#	NAME	SD WAN GROUP	INTERFACE STATUS	PERFORMANCE PROBE	PERFORMANCE CLASS	BACKUP INTERFACE	PROBE DEFAULT UP
<input checked="" type="checkbox"/>	1	FTP	test	X1 Not Qualified	test1	Lowest Jitter	Drop_Tunnelf	✓
<input checked="" type="checkbox"/>	2	WANGroup1_FTP_Paths	test	X1 Not Qualified	testt	Lowest Packet Loss	Drop_Tunnelf	✓
<input checked="" type="checkbox"/>	3	test	test	X1 Not Qualified	testt	FTP	None	✓

Total: 3 item(s)

4. Click **OK** to confirm deletion.

# SD-WAN Route Policies

## Topics:

- [About SD-WAN Route Policies](#)
- [Configuring SD-WAN Route Policies](#)

## About SD-WAN Route Policies

Dynamic Path selection for specific traffic flows uses Policy-based Routes. A SD-WAN Policy-based Route is used to configure the route policy for the specific source/destination service/app combination, with a corresponding Path Selection Profile that determines the outgoing path dynamically based on the Path Selection Profile. If there is more than one path qualified by the Path Selection Profile, the traffic is automatically load balanced among the qualified paths. If none of the paths are qualified by the path selection profile and the backup interface in the profile is not configured or is down, the route is disabled. For information about SonicOS SD-WAN, see [About SD-WAN](#).

**TIP:** SD-WAN routing can be configured from the **Network | System > Dynamic Routing** page. The **Network | SDWAN > Rules** page, however, only shows the SD-WAN Routes and only allows configuration of SD-WAN-type routes.

#	NAME	SOURCE	DESTINATION	SERVICE	APP	TOS / MASK	PATH PROFILE	INTERFACE	METRIC	PRIORITY	COMMENT
1	teswt	WAN Subnets	Firewalled Subnets	N	-appname= AlienBlue+ Jumpshare+00umblock	0x00/0x00	test	tun1	25	1	

<b>NAME</b>	Name of the SD-WAN Route Policy. The IP version is shown by an icon showing whether the Route Policy is for IPv4 and/or IPv6.
<b>SOURCE</b>	Source address object for the SD-WAN route.
<b>DESTINATION</b>	Destination address object for the SD-WAN route.
<b>SERVICE</b>	Service object for the for the SD-WAN route. If <b>App</b> was selected instead of Service for the type of route policy, <b>N/A</b> appears.
<b>APP</b>	App object for the for the SD-WAN route. If <b>Service</b> was selected instead of <b>App</b> for the type of route policy, <b>N/A</b> appears.
<b>TOS/Mask</b>	Hexadecimal TOS and TOS Mask. If these options were not configured, you will see this field as blank.

<b>PATH PROFILE</b>	Path Selection Profile for the SD-WAN route.
<b>INTERFACE</b>	SD-WAN interface group associated with the SD-WAN route.
<b>METRIC</b>	Metric used for the SD-WAN route.
<b>PRIORITY</b>	Priority of the Route Policy.
<b>COMMENT</b>	When you hover over the comment icon, the comment entered when the SD-WAN route policy was configured is displayed.

## Configuring SD-WAN Route Policies

### Topics:

- [Adding SD-WAN Route Policies](#)
- [Editing SD-WAN Route Policies](#)
- [Deleting SD-WAN Route Policies](#)
- [Deleting Multiple SD-WAN Route Policies](#)

# Adding SD-WAN Route Policies

To add an SD-WAN route policy:

1. Navigate to **Network | SDWAN > Rules**.
2. Click the **Add Route Policy** icon. The **Add Route Policy** dialog is displayed.

The screenshot shows the 'Add Route Policy' dialog box with the 'General' tab selected. The 'ROUTE POLICY SETTINGS' section includes the following fields and options:

- Name:** Text input field.
- Source:** Dropdown menu with 'Any' selected.
- Destination:** Dropdown menu with 'Any' selected.
- Service:** Radio button selected.
- App:** Radio button unselected.
- Service Object:** Dropdown menu with 'Any' selected.
- Path Profile:** Dropdown menu with 'Select a Path Selectio...' selected.
- Interface:** Dropdown menu with 'Select an Interface' selected.
- Metric:** Text input field.
- Comment:** Text input field.
- Disable route when the interface is disconnected:** Toggle switch (checked).
- Permit Acceleration:** Toggle switch (unchecked).

At the bottom right, there are 'Cancel' and 'Add' buttons.

① **NOTE:** The Interface and Disable route when the interface is disconnected options are dimmed and cannot be edited. The Interface option is populated with the SD-WAN group name associated with the Path Selection Profile (PSP) you select.

3. Enter a meaningful name in the **Name** field.
4. From **Source**, select the source address object for the static route or select **Create new address object** to dynamically create a new address object. The default is **Any**.
5. From **Destination**, select the destination address object or select **Create new address object** to dynamically create a new address object. The default is **Any**.
6. Choose the type of route policy:
  - **Service** (default)
  - **App**

① | **IMPORTANT:** Application Control Licensing is required for application-based routing.



7. If you selected **Service**, select a **Service Object**. For a generic static route that allows all traffic types, simply select Any (the default).
8. If you selected **App**, select an **App Object**.
9. From **Path Profile**, select a Path Selection Profile.
10. Enter the **Metric** (weighted cost) for the route. The minimum is 1, and the maximum is 254.  
 ⓘ | **TIP:** Lower metrics are considered better and take precedence over higher metrics (costs).
11. Optionally, enter a **Comment** for the route policy. This field allows you to enter a descriptive comment for the new static route policy.
12. To permit acceleration on the route policy, enable **Permit Acceleration**.
13. Click **Advanced**.
14. Enter a TOS value in the **TOS (Hex)** field. The maximum value is FF. If the TOS and TOS Mask fields are not configured, a value of 0 is used.
15. Enter the same value in the **TOS Mask (Hex)** field.
16. To manually specify an administration distance:
  - a. Deselect **Auto**. This option is selected by default.  
 The **Admin Distance** field becomes available.
  - b. Enter the administration distance in the **Admin Distance** field.
17. Click **Add**.

## Editing SD-WAN Route Policies

### To edit a route policy:

1. Navigate to **Network | SDWAN > Rules**.
2. Hover over a policy and click the **Edit** icon.

#	NAME	SOURCE	DESTINATION	SERVICE	APP	TOS / MASK	PATH PROFILE	INTERFACE	METRIC	PRIORITY	COMMENT
1	FTP_Test	Any	Any	HTTPSname	N/A		test2/test	test	3		

3. The **Update Route Policy** dialog is displayed.
4. Make changes as described in [Adding SD-WAN Route Policies](#).
5. Click **Update**.

## Deleting SD-WAN Route Policies

### To delete a route policy:

1. Navigate to **Network | SDWAN > Rules**.
2. Hover over a policy and click the **Delete** icon.
3. Click **Confirm**.

# Deleting Multiple SD-WAN Route Policies

## To delete multiple SD-WAN Route Policies:

1. Navigate to **Network | SDWAN > Rules**.
2. Select the Path Selection Profiles to delete.

To select all the policies, click the checkbox in the header row of the **SD-WAN Route Policies** table.

3. Click **Delete** icon above the **SD-WAN Rout Policies** table.



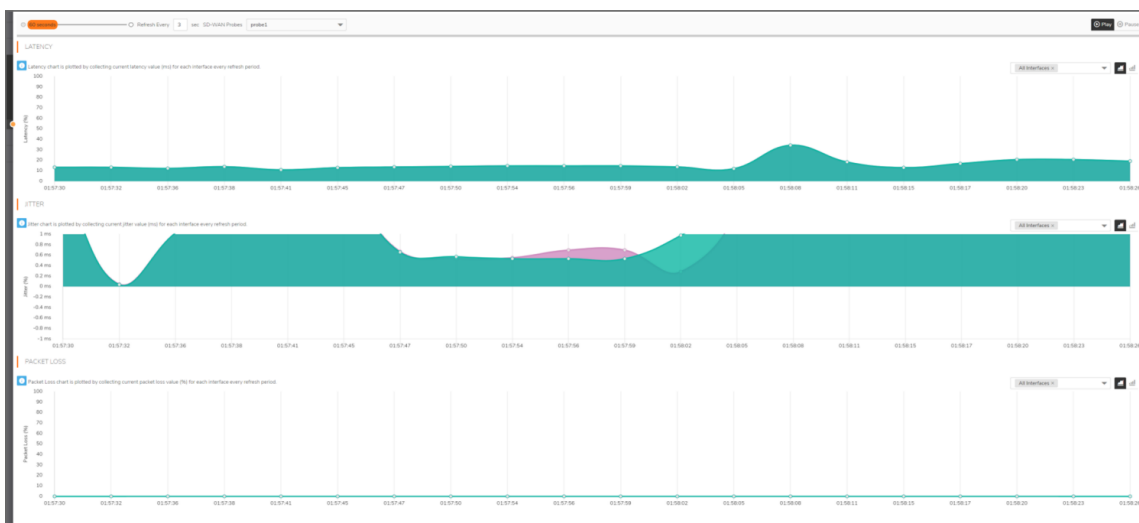
The screenshot shows a table with columns: #, NAME, SOURCE, DESTINATION, SERVICE, APP, TOS / MASK, PATH PROFILE, INTERFACE, METRIC, PRIORITY, COMMENT, and UUID. Two rows are visible, both with checkboxes in the # column checked. Above the table, there are buttons for '+ Add Route Policy', 'Delete' (highlighted with a yellow box), and 'Refresh'.

#	NAME	SOURCE	DESTINATION	SERVICE	APP	TOS / MASK	PATH PROFILE	INTERFACE	METRIC	PRIORITY	COMMENT	UUID
<input checked="" type="checkbox"/>	1	FTP_Test	Any	Any	HTTPSname	N/A	test2/test	test	3			00000000-0000-0003-0900-004010350940
<input checked="" type="checkbox"/>	2	FTP	Any	Any	HTTPname	N/A	test3/test	test	30			00000000-0000-0004-0900-004010350940

4. Click **Confirm**.

# Monitoring SD-WAN

① **NOTE:** A chart may be empty or blank if there are no recent data entries received within the viewing range.



## To monitor SD-WAN performance:

1. Navigate to **Monitor | SD-WAN > SDWAN Monitor**.
2. From **SD-WAN Probes** drop-down box, select the performance probe you would like to use to monitor.
3. Indicate the Refresh rate, in seconds, in the `Refresh Every` field.
4. Select a View Range:
  - **60 seconds** (default)
  - **2 minutes**
  - **5 minutes**
  - **10 minutes**
5. Choose an interface to track or select **All Interfaces** from the drop-down menu on the right side.
6. The two small icons on the right allow you to toggle between line and block displays.

# Viewing SD-WAN Route Policy Connections

You can view the connections that have been associated with SD-WAN Route Policies on the **Monitor | SDWAN > SD-WAN Connections** page.

- To view the activities associated with IPv4 SD-WAN Route Policies, click **IPv4**.
- To view the activities associated with IPv6 SD-WAN Route Policies, click **IPv6**.

## SD-WAN CONNECTION DETAILS

<b>SRC MAC</b>	MAC address of the appliance that is the source of the connection.
<b>SRC VENDOR</b>	Name of the vendor of the appliance that is the source of the connection.
<b>SRC IP</b>	IP address of the appliance that is the source of the connection.
<b>SRC PORT</b>	Port on the appliance that is the source of the connection.
<b>DST MAC</b>	MAC address of the appliance that is the destination of the connection.
<b>DST VENDOR</b>	Name of the vendor of the appliance that is the destination of the connection.
<b>DST IP</b>	IP address of the appliance that is the destination of the connection.
<b>DST PORT</b>	Port on the appliance that is the destination of the connection.
<b>PROTOCOL</b>	Protocol used for the connection.
<b>SRC IFACE</b>	Interface on the appliance that is the source of the connection.
<b>DST IFACE</b>	Interface on the appliance that is the destination of the connection.
<b>SRC ROUTE</b>	Source route of the connection.
<b>DST ROUTE</b>	Destination route of the connection.
<b>FLOW TYPE</b>	Type of data flow control, such as FTP Control.
<b>IPS CATEGORY</b>	Internet Provider Security (IPS) category. If this information is not available or relevant, the column displays N/A.
<b>ABR APP ID</b>	App-Based Routing Application ID.
<b>ABR CATEGORY ID</b>	App-Based Routing Category ID.
<b>EXPIRY (SEC)</b>	Number of seconds until the connection expires.
<b>TX BYTES</b>	Number of bytes transmitted on the connection.
<b>RX BYTES</b>	Number of bytes received on the connection.
<b>TX PKTS</b>	Number of packets transmitted on the connection.

---

<b>Rx PKTS</b>	Number of packets received on the connection.
<b>Flush</b>	Displays the Flush icon. Clicking the icon flushes the connection.
<b>Total</b>	Total number of entries on the page. This is displayed at the bottom of the page.

---

You can perform the following actions on the SD-WAN Connections page:

- To search a log, enter a keyword related to an activity in the `Search` bar
- To filter the logs, click **Filter** icon, select the appropriate filter options, and then click **APPLY FILTERS**.
- To clear the filters applied, click **Clear Filter** icon
- To export the logs in CSV or TEXT files, click **Export** icon and select the required format
- To refresh the page, click **Refresh** icon

# SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

# About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

SonicOS and SonicOSX SD-WAN Administration Guide

Updated - May 2021

Software Version - 7

232-005344-00 Rev B

Copyright © 2021 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

## Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request

Attn: Jennifer Anderson

1033 McCarthy Blvd

Milpitas, CA 95035