
Configure the Versa SASE Client To Select the Best Gateway

 For supported software information, click [here](#).

The Versa SASE client can connect to multiple secure access gateways. The client can connect to a specific gateway or it can determine the best available Versa cloud gateway. To have the client select the best gateway, you can configure one or more groups of gateways based on FQDN to use for selection of the best gateway.

When a user selects a gateway group for the Versa SASE client to connect to, the client selects the best gateway based on the following criteria:

- Distance of the Versa SASE client from the gateway. The default distance is less than 1000 kilometers (625 miles).
- CPU load of the gateway is less than a threshold value. The default threshold is 75 percent.
- Memory load of the gateway is less than a threshold value. The default threshold is 75 percent.

When a Versa SASE client makes a connection request to a best gateway group, one of the gateways in the group, called the landing gateway, performs the best-gateway calculations and returns a maximum of four gateways to the Versa SASE client. For example, if a best-gateway group consists of eight gateways and five match the distance, CPU, and memory load criteria, the landing gateway rates these five gateways based on the matching criteria, assigns each a value between 1 and 100, and then shares the four gateways with the highest value with the Versa SASE client. (The best-gateway calculation ignores the gateways that do not match the selection criteria.) The Versa SASE client then pings these gateways and connects to the gateway that has the lowest round-trip time (RTT) value.

To configure the Versa SASE client to select the best gateway, you do the following:

1. Enable Versa BGP TLV site information.
2. Configure FQDNs for gateway.
3. Configure FQDNs for gateway groups.
4. Associate gateway servers with the server group.
5. Configure a gateway profile to set the best gateway.

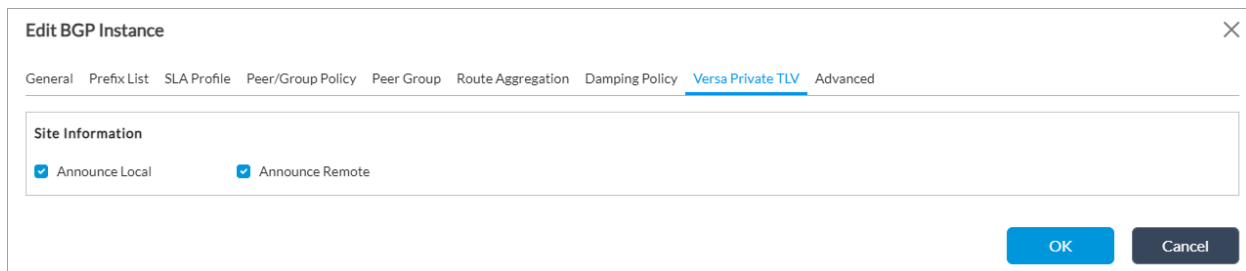
Enable Versa BGP TLV Site Information

On the provider's virtual router, you enable the BGP Versa private type-length-value (TLV) site information. Doing this distributes the gateway and group FQDNs to all the other gateways so that each gateway can learn which gateways are part of a group.

Note that in a multitenant deployment (that is, a deployment with a provider plus additional tenants), you enable the Versa Private TLV configuration in the multiprotocol BGP (MP-BGP) instance associated with the provider organization (provider control VR), not in tenant's control VRs.

To enable Versa BGP TLV site information:

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 pane. 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.
4. Click the + Add icon. The Configure Virtual Router popup window displays.
5. Select the BGP tab in the left menu bar. The Edit BGP Instance window displays.
6. Select the Versa Private TLV tab.
7. Click Announce Local to enable gateways or hub-controller nodes (HCN) to support best-gateway selection. If all SASE gateways (HCN, hub, or spoke) are in a full-mesh topology, enabling Announce Local is sufficient for gateways and HCNs to handle SASE client requests.
8. Click Announce Remote only if your gateways and HCNs are not in a full-mesh topology. If there are SASE gateways in spoke topology behind HCNs, you must enable Announce Remote on HCNs so that the spokes can handle SASE client requests.



The screenshot shows the 'Edit BGP Instance' window with the 'Versa Private TLV' tab selected. Under the 'Site Information' section, both 'Announce Local' and 'Announce Remote' are checked. The window has tabs for General, Prefix List, SLA Profile, Peer/Group Policy, Peer Group, Route Aggregation, Damping Policy, Versa Private TLV, and Advanced. At the bottom right are 'OK' and 'Cancel' buttons.

9. For information about configuring other BGP parameters, see [Configure BGP](#).
10. Click OK.

Configure FQDNs for Gateways

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in left navigation panel.
 - d. Select a tenant or Controller node in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Configure_...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Configure_...)

Updated: Wed, 23 Oct 2024 08:43:38 GMT

Copyright © 2024, Versa Networks, Inc.

3. Select Others > Organization > Limits in the left menu bar. The main pane displays the organizations associated with the Controller node.
4. Click an organization name. The Edit Organization Limit popup window displays.
5. Add the gateway FQDN (here, sase.pkversa.local). Note that the gateway FQDN must be unique for each gateway, and you can add only one gateway FQDN for an organization.
6. Add the gateway group FQDN (here, us-eu.pkversa.local). Note that you must use the same FQDN when you create a server group in [Configure FQDNs for Gateway Groups](#), below. To place gateways into the same group, use the same the FQDN for all gateways. For more information, see [Configure Organization Limits](#).

Edit Organization Limit - Tenant3

General Traffic Identification Resources Services QoS

Organization Name: Tenant3

Description:

DHCP Profile: dhcp-limits

Session Rate: Limit: 1000000

☒ Fragment Reassembly

☐ Enterprise Names Enterprise Names Not Configured

☐ Domain Names Domain Names Not Configured

☐ Gateway FQDN sase.pkversa.local

☐ Group FQDN us-eu.pkversa.local

OK Cancel

7. Click OK.

Configure FQDNs for Gateway Groups

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 template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > Gateway Groups in the left menu bar (In Releases 21.2.3 and earlier, gateway groups are called server groups).
4. Click the + Add icon. The Add Gateway Groups popup window displays.

Add Gateway Groups ✕

Name *

Description

FQDN *

OK


Cancel

5. Enter a name for the gateway group (here, US-Europe).
6. Enter the group FQDN that you specified in Step Step 6 of [Configure FQDNs for Gateways](#), above (here, us-eu.pkversa.local).
7. Click OK.

Associate Gateways with the Gateway Group

To associate gateways with the gateway group:

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 template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > Gateway in the left menu bar.
4. Click the Add icon. The Add Gateways popup window displays.
 - a. Enter a name for the gateway (here, SASE-GW).
 - b. Click FQDN and then enter the host server address as a fully qualified domain name. Note that the FQDN you configured in Step 5 of [Configure FQDNs for Gateways](#), above, is added here (here, sase-pkversa.local). The FQDN must be unique for all gateways.
 - c. Enter the IPsec profile identifier of the secure access server profile. You must use the same ID for all gateways in a gateway group.
 - d. In the Server Groups field, select the server group that you added in [Configure FQDNs for Gateway Groups](#),

above, (here, US-Europe) to associate with the server, and then click the  Add icon. You can add a gateway can be added to multiple groups, and multiple gateways can be part of the same group.

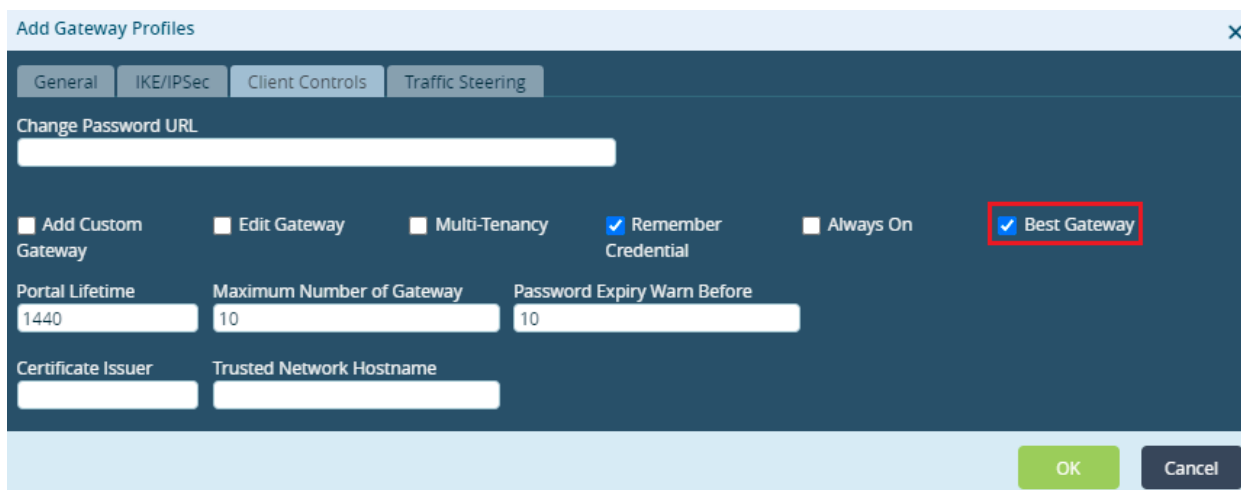
e. Click OK.

- Repeat Steps 1 through 4 to associate other gateway servers with the group. Ensure that the gateway server certificate works with both the gateway FQDN and group FQDN. It is recommended that, for compatibility, you use wildcard certificates such as, *.versa-test.net.

Configure a Gateway Profile To Set the Best Gateway

To configure a gateway profile that sets a VPN connection to be the best gateway among the available gateways:

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Templates > Device Templates in the horizontal menu bar.
 - Select an organization in the left menu bar.
 - Select a template in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Services > Secure Access > Portal > Gateway Profiles in the left menu bar.
- Click the + Add icon. The Add Profiles popup window displays.
- Select the Client Controls tab.



The screenshot shows the 'Add Gateway Profiles' dialog box with the 'Client Controls' tab selected. The 'Change Password URL' field is empty. Below it, there are several checkboxes: 'Add Custom Gateway' (unchecked), 'Edit Gateway' (unchecked), 'Multi-Tenancy' (unchecked), 'Remember Credential' (checked), 'Always On' (unchecked), and 'Best Gateway' (checked and highlighted with a red box). Below these are three input fields: 'Portal Lifetime' (1440), 'Maximum Number of Gateway' (10), and 'Password Expiry Warn Before' (10). At the bottom, there are two more input fields: 'Certificate Issuer' and 'Trusted Network Hostname'. The 'OK' and 'Cancel' buttons are at the bottom right.

- Click Best Gateway.
- For information about configuring the other fields, see [Configure a Secure Access Gateway](#).
- Click OK.

Supported Software Information

Releases 21.2.1 and later support all content described in this article.

Additional Information

[Configure Organization Limits](#)

[Configure the Versa Secure Access Service](#)

[Configure Virtual Routers](#)

[Configure Versa SASE Clients](#)

[Use the Versa SASE Client Application](#)