
Configure SASE Secure Client Access Rules

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

You use secure client access rules and profiles to manage Versa Secure Private Access (VSPA) client applications running on personal computers and mobile phones. You configure secure client access rules and apply them to secure access clients.

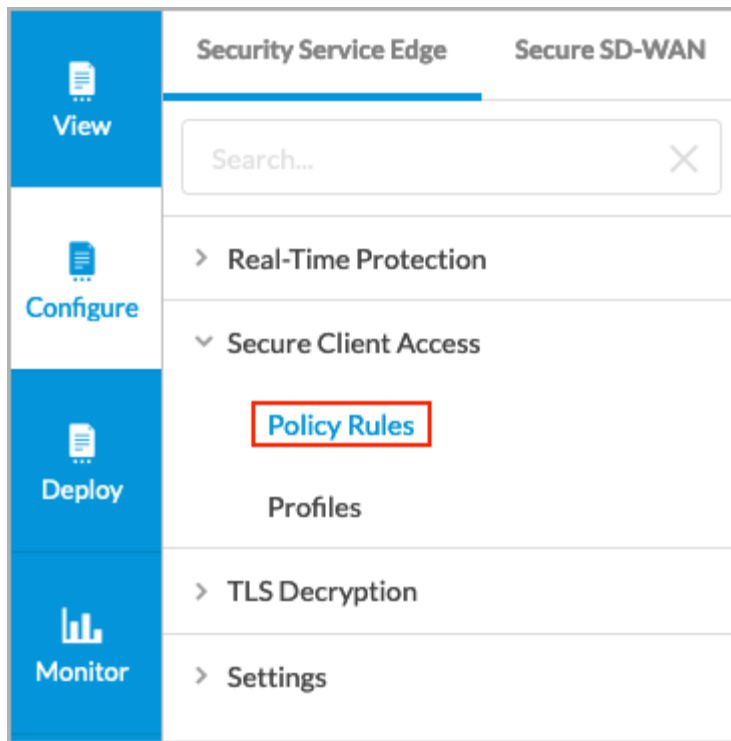
Note: You must configure the following SASE rules, profiles, and settings in the following order:

1. Configure users and user groups first, and then publish them to the gateway. For more information, see [Configure Users and Device Authentication](#) and [Publish a SASE Gateway](#).
2. Configure site-to site tunnels. For more information, see [Configure SASE Site-to-Site Tunnels](#).
3. Configure secure client access profiles. For more information, see [Configure SASE Secure Client Access Profiles](#).
4. Configure secure client access rules, as described in this article.

You do not need to configure the remaining SASE rules, profiles, and settings in any particular order.

To configure secure client access rules:

1. Go to Configure > Secure Services Edge > Secure Access Client > Policy Rules.



The Secure Client Access Rule List screen displays all configured secure access client rules.

| Rule Name | Operating System Versions | Users | EIP | Device Compliance Status | Source Geo Locations | Traffic Action | VPN & Gateway Groups | Profile Name | Enabled | Pre-Login Configuration |
|---------------------|--|-----------|---|--|---------------------------------------|--|--|--------------|---------|-------------------------|
| Unmanaged-Devices | Apple macOS | All Users | Predefined elp-profile-general-windows-11 elp-profile-general-windows-10 elp-profile-general-linux | Compliance Non Compliant | All Source Geo locations are selected | No Client Applications selected No Predefined Applications selected | VPN Name ACME-Enterprise Gateway Groups USA-West USA-East Gateways USA-West-GW-1 USA-West-GW-2 USA-East-GW-1 | SCA01 | Enabled | Download JSON file |
| Managed-Devices | Windows 10 Windows 10 Mobile Windows 7 | All Users | | Compliance Non Compliant In-Grace Period | All Source Geo locations are selected | Custom Applications kasun_sample_2 kasun_sample Predefined Applications Rally Software PingOne for Enterprise | VPN Name ACME-Enterprise Gateway Groups USA-East USA-West Gateways USA-West-GW-1 USA-West-GW-2 USA-East-GW-1 | WestCoast | Enabled | Download JSON file |
| Embargoed-Countries | Android | All Users | | No Device Compliance options | Source Geo Locations | No Client | VPN Name | RichanthRo | Enabled | Download JSON file |

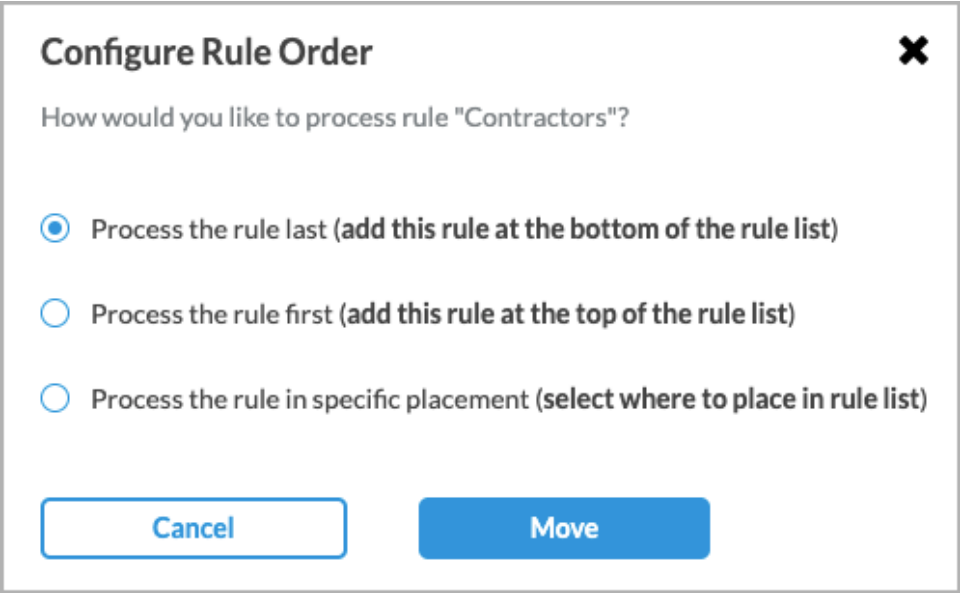
2. In the horizontal menu bar, you can perform the following operations.




[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...)

Updated: Wed, 23 Oct 2024 08:38:20 GMT

Copyright © 2024, Versa Networks, Inc.

| Operation | Description |
|-----------|--|
| Add | Create a new internet protection rule. This button is active when no existing rule is selected. |
| Clone | Clone the selected internet protection rule. When you select this option, the configuration window displays the default name of the cloned rule, if desired, then click Save. |
| Reorder | <p>Reorder the selected internet protection rule. A popup window similar to the following displays:</p>  <p>1. Select one of the three options:</p> <ul style="list-style-type: none"> ◦ Process the rule last ◦ Process the rule first ◦ Process the rule in specific placement—A list of the existing rules displays. Click the position where you want to place the rule. <p>2. Click Move.</p> |
| Delete | Delete the selected internet protection rule. A popup window similar to the following displays: |

| Operation | Description |
|-----------|--|
| | <div> <div>  Delete Rule </div> <div> <p>You are about to delete the following rule: Contractors</p> <div> <div>No</div> <div>Yes</div> </div> </div> </div> <p>Click Yes to delete the internet protection rule, or click No to retain the rule.</p> |
| Refresh | Refresh the list of existing rules. |

- To customize which columns display, click Select Columns and then select or deselect the columns you want to display. Click Reset to return to the default columns settings.

Select Columns

☒ Operating System Versions

☒ Users

☒ EIP

☒ Device Compliance Status

☒ Source Geo Locations

☐ Source IP Address

☒ Traffic Action

☒ VPN & Gateway Groups

☒ Profile Name

☐ EIP Agent


☒ Enabled

☒ Pre-Logon Configuration

Reset

Note that the Pre-Logon Configuration column only appears if you have enabled pre-logon in the tenant

configuration. See [Configure SASE Tenants](#) for more information.

4. Click the  Add icon to configure the policy rule. The Create Secure Client Access Rule screen displays. There are nine elements for each secure client Access Rule.
 - Match Criteria:
 - Operating System—Select the operating system to use with the rule.
 - Users/User Groups—Define the users and user groups to which the secure client access rules apply.
 - Dev Risk Info—Select which devices managed by the enterprise and which unmanaged devices are allowed to access the network.
 - Source Geolocation and Source IP Address—Define which geographic locations and IP addresses can access the network.
 - Actions:
 - Traffic Action—Select which traffic to send to the Versa Cloud Gateway or directly to the internet, and which traffic to block and not sent to the Versa Cloud Gateway.
 - Gateways—Select which gateway groups VSPA clients can use.
 - Client Configuration—Configure multifactor authentication (MFA) and other client parameters.
 - Agent Profile from EIP—Define the conditions that the SASE client uses to filter information from endpoint devices.
 - Review & Configure—Review the new rule configuration, edit it if needed, and save the new rule.

See the sections below to configure the nine elements of the policy rule.

Configure Operating Systems for a Secure Client Access Rule

You can choose among four operating systems to be used in a given secure client access rule. Within each operating system, you can choose different versions of operating systems, as follows:

- Android
- Apple
 - MacOS
 - Mac OS X Server
 - OS X
 - iOS
 - iPadOS
- Linux
 - Cent OS
 - Fedora
 - FreeBSD
 - Gentoo
 - Linux Mint

- Open SUSE
- Slackware Linux
- Ubuntu
- Windows
 - Windows 10
 - Windows 10 Mobile
 - Windows 7
 - Windows 8
 - Windows 8.1
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016
 - Windows Server 2019
 - Windows Vista
 - Windows XP

You can choose only one type of OS, either Android, Apple, Linux, or Windows. When you select an OS type, you must select at least one version of that OS.

To configure operating systems for a secure client access rule:

1. In the Create Secure Client Access Rule screen, select Operating System. The following screen displays.

Configure > SASE > Secure Client Access > Policy Rules

Create Secure Client Access Rule

1 OPERATING SYSTEM 2 USERS/USER GROUPS 3 DEVICE RISK INFO 4 SOURCE GEO LOCATION & SOURCE IP ADDRESS 5 TRAFFIC ACTION 6 GATEWAYS 7 CLIENT CONFIGURATION 8 AGENT PROFILE FROM EIP 9 REVIEW & CONFIGURE

Choose the operating system for this rule below.

If you prefer, you can customize which operating system options you would like to enable for the rule.

Windows

☐ All Windows Operating Systems

- ☐ Windows 10
- ☐ Windows 10 Mobile
- ☐ Windows 7
- ☐ Windows 8
- ☐ Windows 8.1
- ☐ Windows Server 2012
- ☐ Windows Server 2012 R2
- ☐ Windows Server 2016
- ☐ Windows Server 2019
- ☐ Windows Vista
- ☐ Windows XP

Apple

☐ All Apple Operating Systems

- ☐ Mac OS
- ☐ Mac OS X Server
- ☐ OS X

☐ All Apple Mobile

- ☐ iOS
- ☐ iPadOS

Android

☐ All Android Mobile


- ☐ Android

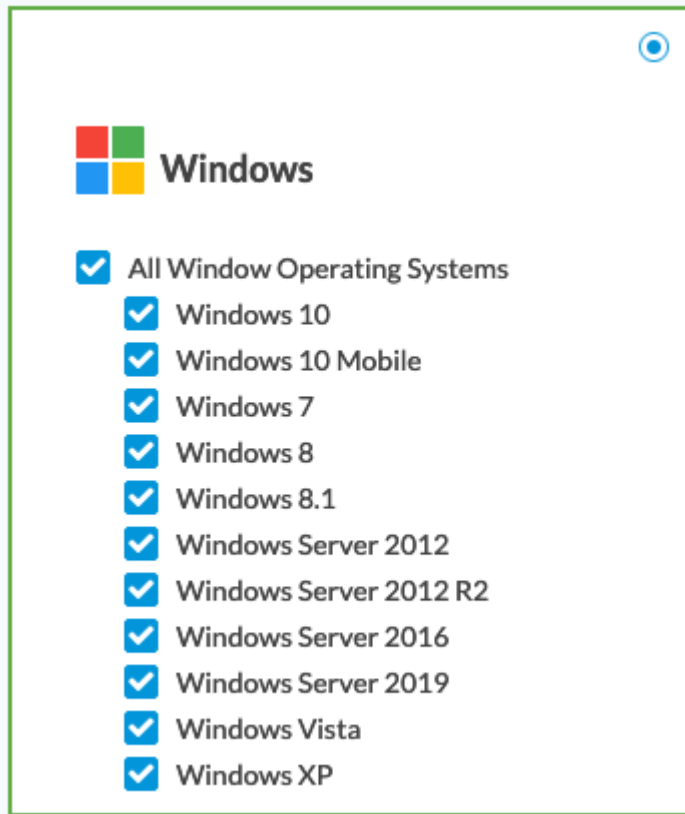
Linux

☐ All Linux Operating Systems

- ☐ Fedora
- ☐ Red Hat Enterprise Linux
- ☐ Ubuntu

Cancel Back Skip to Review Next

2. Click the  Circle icon in one of the operating system cards to choose an operating system. By default, all versions of the operating systems are selected. For example, if you click the Circle icon in the Windows box, the screen displays the following:



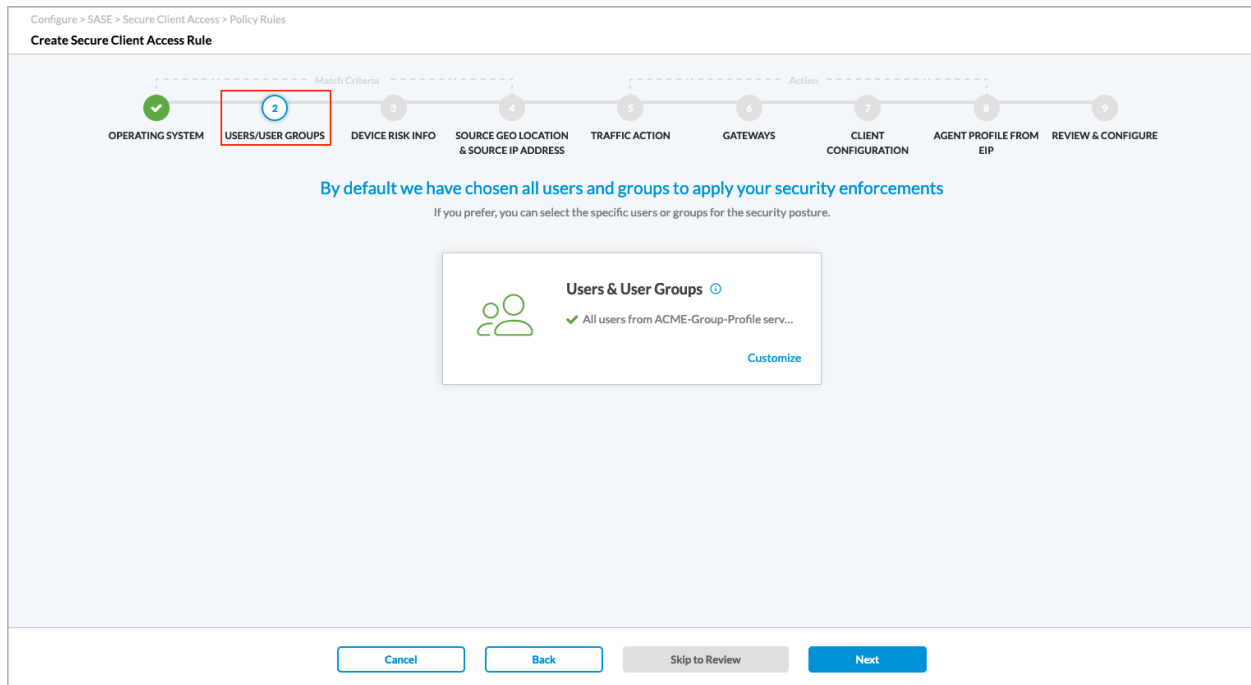
3. To deselect one or more Windows versions, click the boxes next to those versions. You can also click the box next to All Windows Operating Systems to deselect all versions, then you can click one or more versions to be used in the rule.
4. Click Next to go to the Users/User Groups screen.

Configure SASE Users and User Groups for Secure Client Access

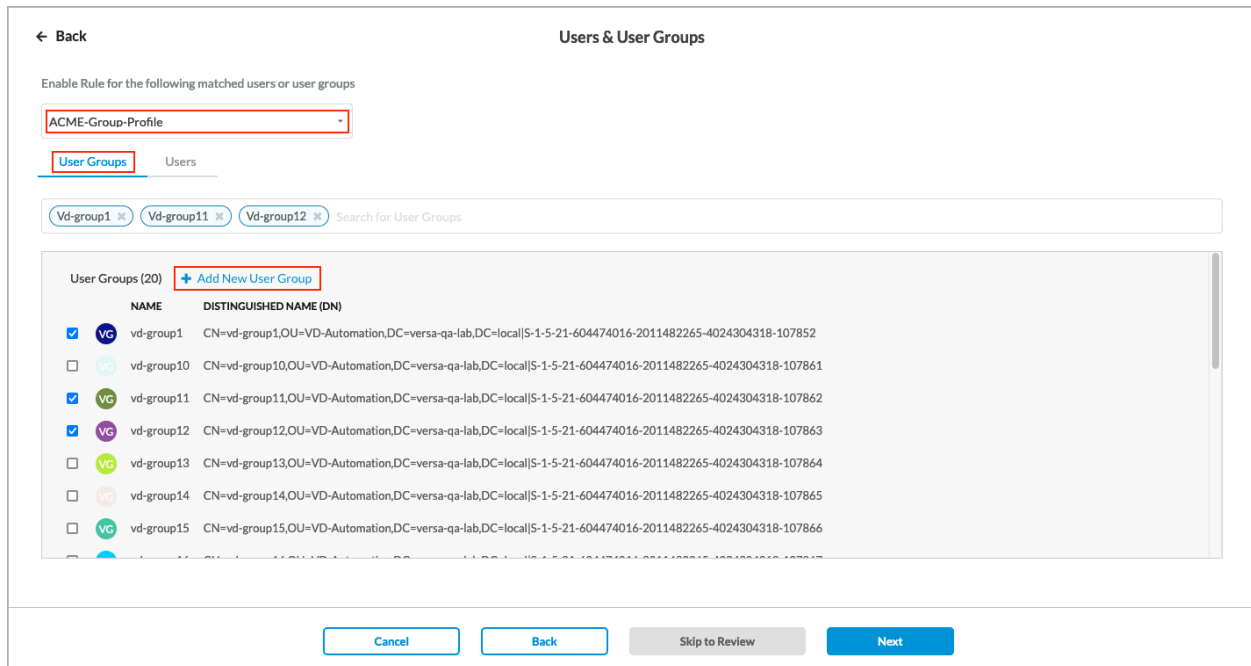
By default, secure client access rules are applied to all users and user groups. You can customize the users and user groups to which the secure client access rule is applied.

To customize the users and user groups to which you apply a secure client access rule:

1. In the Create Secure Client Access Rule screen, select Users/User Groups. By default, security enforcement rules are applied to all users and user groups.



2. To select specific users and/or user groups, click Customize. The Users & Groups screen displays.



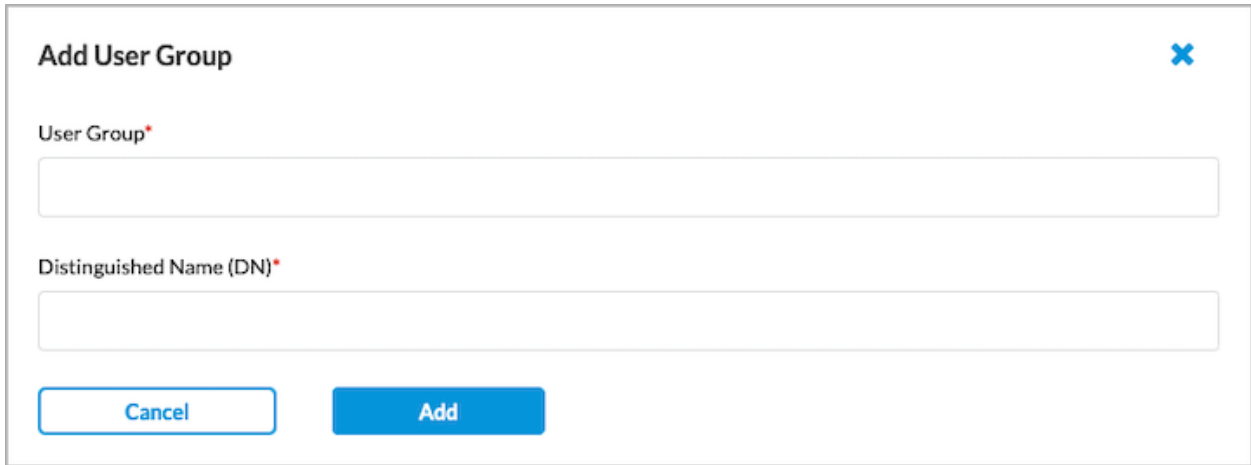
3. Select the User Groups tab, and then select the group profile to which to apply the rule.
4. Select the User Groups tab, and then select the user groups that you want to include in the match list, or type the name of a user group in the search box and then select it from the search results.
5. To create a new user group based on LDAP authentication, select an LDAP group profile, and then click + Add

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...)

Updated: Wed, 23 Oct 2024 08:38:20 GMT

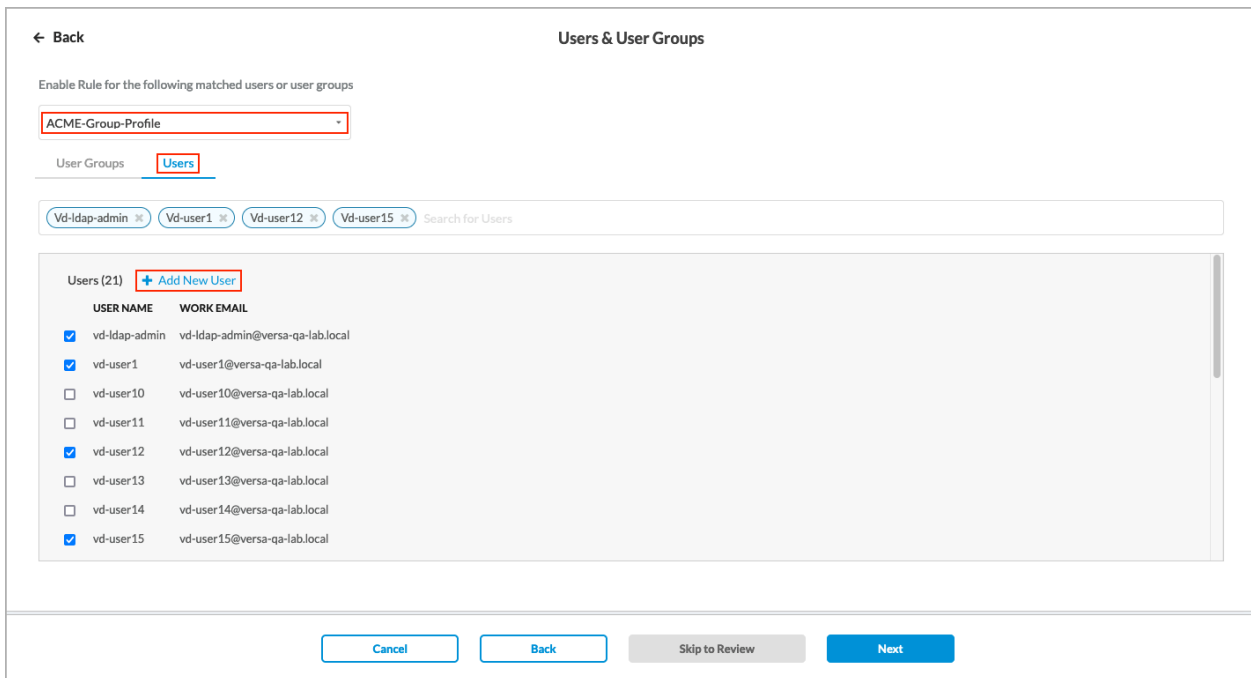
Copyright © 2024, Versa Networks, Inc.

New User Group. In the Add User Group window, enter a user group name and a distinguished name (DN) in the fields provided.



The 'Add User Group' dialog box contains two text input fields. The first field is labeled 'User Group*' and the second is labeled 'Distinguished Name (DN)*'. At the bottom of the dialog are two buttons: 'Cancel' and 'Add'.

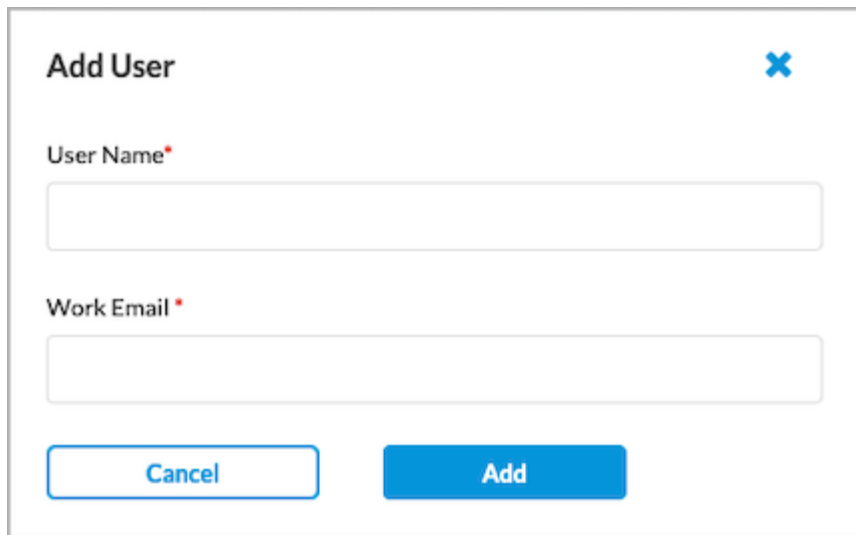
6. Click Add.
7. To select specific users, select the Users tab. The following screen displays.



The 'Users & User Groups' screen shows a dropdown menu for 'ACME-Group-Profile' and tabs for 'User Groups' and 'Users'. The 'Users' tab is active, displaying a list of users with checkboxes. The list includes 'vd-ldap-admin', 'vd-user1', 'vd-user10', 'vd-user11', 'vd-user12', 'vd-user13', 'vd-user14', and 'vd-user15'. The 'vd-user12' checkbox is checked. At the bottom are buttons for 'Cancel', 'Back', 'Skip to Review', and 'Next'.

| | USER NAME | WORK EMAIL |
|-------------------------------------|---------------|----------------------------------|
| <input checked="" type="checkbox"/> | vd-ldap-admin | vd-ldap-admin@versa-qa-lab.local |
| <input checked="" type="checkbox"/> | vd-user1 | vd-user1@versa-qa-lab.local |
| <input type="checkbox"/> | vd-user10 | vd-user10@versa-qa-lab.local |
| <input type="checkbox"/> | vd-user11 | vd-user11@versa-qa-lab.local |
| <input checked="" type="checkbox"/> | vd-user12 | vd-user12@versa-qa-lab.local |
| <input type="checkbox"/> | vd-user13 | vd-user13@versa-qa-lab.local |
| <input type="checkbox"/> | vd-user14 | vd-user14@versa-qa-lab.local |
| <input checked="" type="checkbox"/> | vd-user15 | vd-user15@versa-qa-lab.local |

8. Select the group profile to use.
9. Select the Users tab, and then select the users to include in the match list, or type the name of a user in the search box and then select it from the search results.
10. To create a new user based on LDAP authentication, select an LDAP group profile, and then click + Add New User. In the Add User window, enter a username and the user's work email in the fields provided.

A modal dialog box titled "Add User" with a blue close button (X) in the top right corner. It contains two text input fields: "User Name*" and "Work Email*", both with red asterisks indicating required fields. Below the fields are two buttons: "Cancel" (outlined in blue) and "Add" (solid blue).

11. Click Add.
12. Click Next to continue to the Device Risk Information screen.

Configure SASE Device Risk Information for Secure Client Access

On the Device Risk Information screen, you can configure an Endpoint Information Profile (EIP) and Device Compliance Status options to select devices that exhibit specific attributes that are used to determine the risk status of the device.

EIPs ensure that the endpoint devices that access the enterprise network maintain and adhere to enterprise security standards before they access enterprise network resources. EIPs collect information about the security status of the endpoint devices connecting to your networks. You then classify endpoints based on multiple types of endpoint posture information, defining rules to extract information from endpoint devices and then match the information to enforce security policy.

You can select existing user-defined or predefined EIPs, and you can also create new EIP profiles from this screen.

To configure device risk information:

1. In the Create Secure Client Access Rule screen, select Device Risk Info. The screen contains two sections, Endpoint Information Profile (EIP) and Device Compliance Status. If you are using third-party mobile device management (MDM), use the Device Compliance Status options to select one or more compliance statuses for a device.

Configure > SASE > Secure Client Access > Policy Rules

Create Secure Client Access Rule

OPERATING SYSTEM

USERS/USER GROUPS

DEVICE RISK INFO

SOURCE GEO LOCATION & SOURCE IP ADDRESS

TRAFFIC ACTION

GATEWAYS


CLIENT CONFIGURATION

AGENT PROFILE FROM EIP

REVIEW & CONFIGURE

Choose Your Device Risk Information

Use Endpoint Information Profile (EIP) and Device Compliance Status options to select devices exhibiting specific attributes that determine the risk status of the device


 **Endpoint Information Profile (EIP)**

Select an existing profile or create a new profile with the values for the different EIP attributes collected by the Versa Client. This can be used by the Versa Cloud Gateways for granular policy enforcement based on the end user's device risk.

User Defined Predefined

[+ Add Existing EIP Profile](#) [Delete](#) [+ Create New EIP Profile](#) [Select Columns](#)

| <input type="checkbox"/> | NAME | DESCRIPTION | RULES |
|------------------------------------|------|-------------|-------|
| No User Defined EIP Profiles Added | | | |

 **Device Compliant Status**

If 3rd party MDM is used, select one or more device compliance status below

☐ Compliance
☐ Non-Compliant
☐ In-Grace-Period
☐ Error
☐ Unknown

[Cancel](#) [Back](#) [Skip to Review](#) [Next](#)

Select or Create an EIP Profile

1. To customize which columns display, click Select Columns and then select or deselect the columns you want to display. Click Reset to return to the default columns settings.
2. To select an existing user-defined EIP, click the User Defined tab.
3. Click [+ Add Existing EIP Profile](#).

Add User Defined EIP Profiles

EIP-Custom-Profile

EIP-Prof-1

[Cancel](#) [Add](#)

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...)

Updated: Wed, 23 Oct 2024 08:38:20 GMT

Copyright © 2024, Versa Networks, Inc.

5. To create a new EIP profile, click  Create New EIP Profile. The Create EIP Profile screen displays.

[Configure](#) > [SASE](#) > [Settings](#) > [Endpoint Information Profile \(EIP\)](#) > [EIP Profiles](#)

Create EIP Profile

1

2

RULESREVIEW & SUBMIT

+ Add

⇅ Reorder

🗑 Delete

Select Columns ▾

| NAME | DESCRIPTION | MATCH CATEGORIES |
|---------|-------------|------------------|
| No Data | | |

6. To customize which columns display, click **Select Columns** and then select or deselect the columns you want to display. Click **Reset** to return to the default columns settings.

Select Columns 

☒ Description

☒ Match Categories

Reset

- Click the  Add icon in the Rules screen to add a new rule.

Add Rules

Name*

Description

+ Add

Delete

Select Columns

| | CATEGORY | OBJECTS | USER DEFINED OBJECTS | PREDEFINED OBJECTS |
|---------|----------|---------|----------------------|--------------------|
| No Data | | | | |

Cancel

Add

8. To customize which columns display, click Select Columns and then select or deselect the columns you want to display. Click Reset to return to the default columns settings.



9. Click the **+** Add icon. In the Add EIP Object screen, enter information for the following fields.

| Field | Description |
|--------------------------|----------------------------------|
| Category | Select an EIP object category. |
| User Defined EIP Objects | Select a user-defined EIP object |
| Predefined EIP Objects | Select a predefined EIP object. |


10. Click Add to add the new EIP object.
11. In the Create EIP Profile screen, click Next.
12. In the Review & Configure screen, review the configuration details, click the Edit icon to make any need changes, then click Save to save the EIP profile.

Select the Device Compliance Status

To select a device's compliance status:

1. Go to the Device Risk Info screen.

2. In the Device Compliance Status section, select one or more of the compliance status boxes.



Device Compliant Status

If 3rd party MDM is used, select one or more device compliance status below

- ☐ Compliance
- ☐ Non-Compliant
- ☐ In-Grace-Period
- ☐ Error
- ☐ Unknown

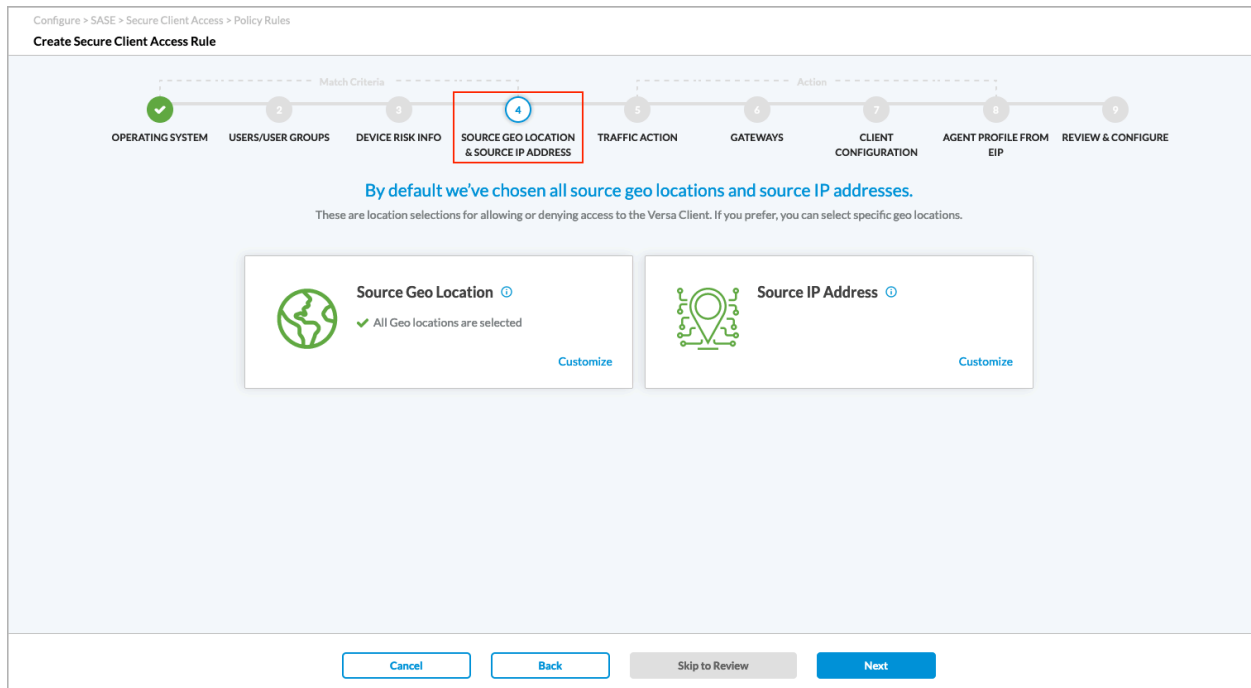
3. Click Next to go to the Source Geolocation & Source IP Address screen.

Configure SASE Source Geolocations and Source IP Addresses for Secure Client Access

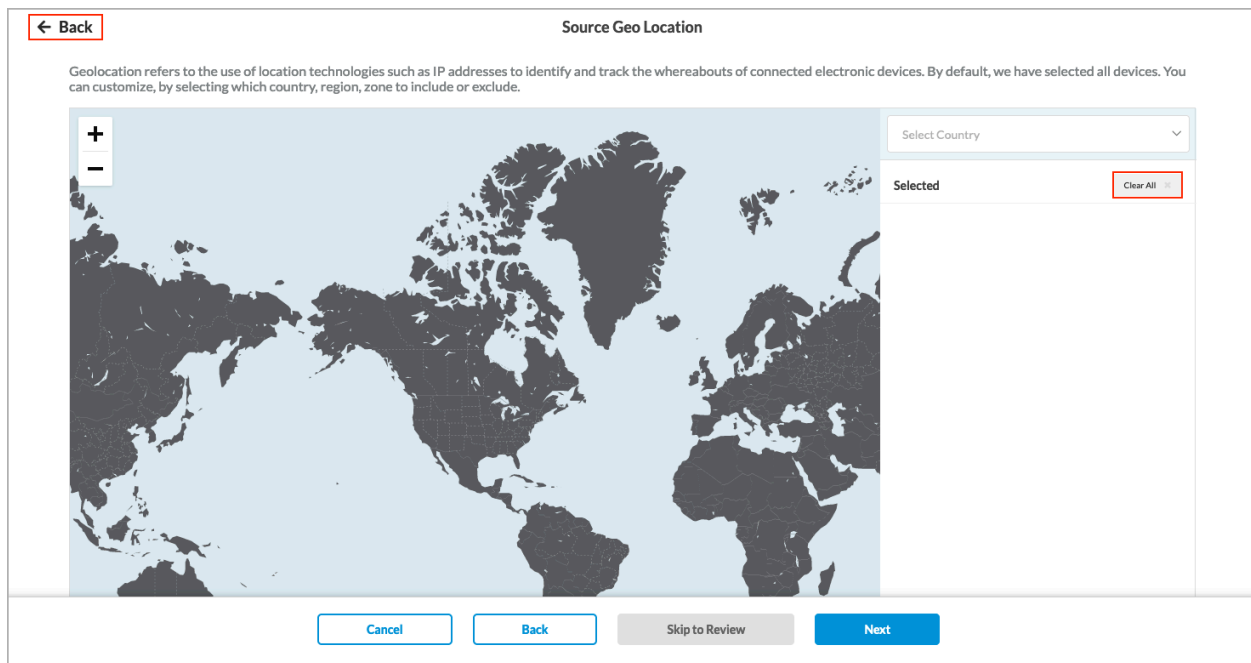
By default, VSPA clients from all source geolocations and all source IP addresses are allowed network access. You can also specify which VSPA client geolocations and source IP addresses are allowed access.

To customize VSPA client access based on source geolocation and source IP address:

1. In the Create Secure Client Access Rule screen, select Source Geolocation and Source IP Address. By default, all geographical locations are allowed access to the Versa secure client access.



2. To allow access to the Versa secure client access from specific source locations, click Customize. The Source Geolocation screen displays.



3. Click Clear All to remove all of the default source locations.
4. Click in the Select Country box, and then select one or more countries. After selecting the countries, click the down-arrow again. The selected countries are displayed.

Select Country

Selected

Clear All

Afghanistan

Australia

Hungary

Sweden

- To remove a country from the list, click X next to the country name.
- To remove all countries from the list, click Clear All.
- Click Back to customize the source IP addresses. The Source Geolocation & Source IP Address screen displays again. Note that to accept the default source IP addresses, click Next at the bottom of the screen.
- To change the source IP addresses to include, click Customize under Source IP Address. In the Source Traffic screen, enter information for the following fields.

← Back

Source Traffic

The Source Destination section represents Layer 3 of the network layer traffic. Layer 3 transmits data segments between networks in the form of packets. When you message your friend, this layer assigns source and destination IP addresses to the data segments Your IP address is the source, and your friend's is the destination.

More Information

Source Address

Address Group

+ Add New

Select 1 or more Address Groups

IP Subnet

IP Range

IP WildCard

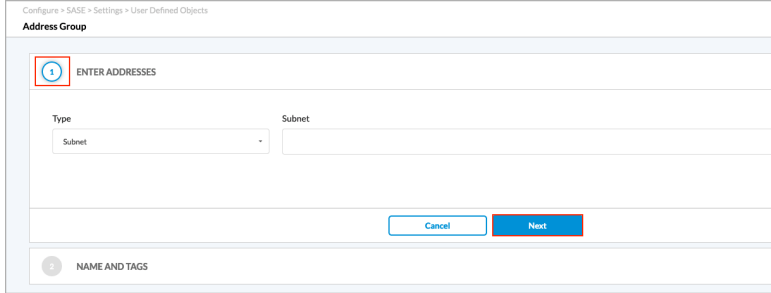


☐ Source Address Negate

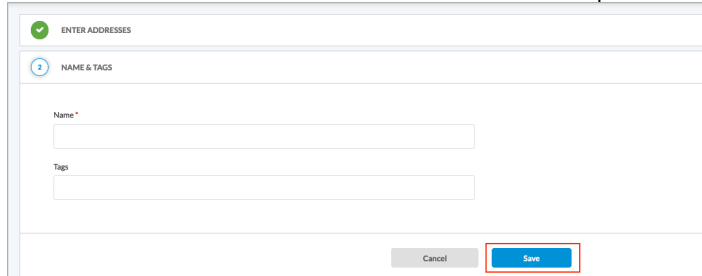
Cancel

Back

Skip to Review

Next

| Field | Description |
|---|---|
| Source Address (Group of Fields) | |
| <ul style="list-style-type: none"> Address Group | <p>Click in the box, and then select one or more address groups. The address groups in the list are those defined in the User Defined Objects section.</p> <p>If you want to provide one or more specific source IP addresses, you do not need to select an address group. Instead, use the IP Wildcard field to enter the IP address.</p> <p>To create a new address group, click + Add New, and then enter information for the following fields:</p>  <ol style="list-style-type: none"> Click the Enter Addresses section and select the group Type. The type can be Subnet, IP range, IP wildcard, or IPv6 subnet. Based on the type selected, enter one of the following and press Return: <ul style="list-style-type: none"> —Subnet: An IP address and subnet mask, for example, 10.2.1.0/24 —IP range: An IP address range, for example, 10.2.1.1-10.2.2.2 —IP wildcard: A specific IP addresses, for example, 192.68.0.56/255.255.0.255 —IPv6 subnet: A valid IPv6 subnet —FQDN: A fully qualified domain name (FQDN) —Dynamic Address: One or more address object names To add additional address group types, click the  Plus icon. To remove an address group type, click the  Minus icon. |

| Field | Description |
|-----------------------|--|
| | <p>4. Click Next.</p> <p>5. In the Name & Tags section, enter a name for the address group and any tags you want to associate with the group.</p>  <p>6. Click Save.</p> |
| IP Subnet | Enter an IP subnet to include in the match list (for example, 10.0.0.0/24), then press Return. You can add additional IP subnets by entering the subnet and pressing Return for each one. |
| IP Range | Enter an IP address ranges to include in the match list (for example, 10.2.1.1-10.2.2.2), then press Return. You can add additional IP address ranges by entering the range and pressing Return for each one. |
| IP Wildcard | Enter an IP address and mask to include in the match list (for example, 192.68.0.56/255.255.0.255), then press Return. You can add additional IP addresses and masks by entering the it and pressing Return for each one. |
| Source Address Negate | Select to apply the rule to any source addresses except the ones in the Source Address field. |

9. Click Next to go to the Traffic Action screen.

Configure SASE Traffic Action Rules for Secure Client Access

For rules used with the Apple, Android, and Linux operating systems, you use traffic action rules to select whether users that match the profile allowed to access to the internet or are denied access.

For rules used with the Windows operating system, you can used traffic-action rules that specify whether application-specific traffic should be sent to the Versa Cloud Gateway or directly to the internet, or whether the traffic should be blocked from being sent to the Versa Cloud Gateway.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...)

Updated: Wed, 23 Oct 2024 08:38:20 GMT

Copyright © 2024, Versa Networks, Inc.

Configure Traffic-Steering Rules for the Android, Apple, and Linux Operating Systems

1. In the Secure Client Access Rule List screen, click + Add to create a new rule. The Create Secure Client Access Rule screen displays.
2. Select Traffic Action. The following screen displays. Enter information for the following fields.

Configure > SASE > Secure Client Access > Policy Rules

Create Secure Client Access Rule

1

Operating System

2

Users/User Groups

3

Device Risk Info

4

Source Geo Location & Source IP Address

5

Traffic Action

6

Gateways

7

Client Configuration

8

Agent Profile From EIP

9

Review & Configure

Based on the most common secure enterprise settings, we've chosen the traffic steering below.

If you prefer, you can customize which traffic steering option you would like to enable for the rule.

Select subscription type for users matching this rule.

Versa Secure Private Access (VSPA) & Versa Secure Internet Access (VSIA)

Deny

Drop all traffic that matches the rule

Display Message after Connection is Blocked

You are not allowed to connect to the enterprise VPN, please contact administrator

Allow

With this option, the default behavior is to send all traffic from the user device to the Versa Cloud Gateway.

Display Message after Successful Connection

Welcome to ACME

Trusted Routes (0)

Excluded Routes (0)

Cancel

Back

Skip to Review

Next

| Field | Description |
|---|---|
| Select subscription type for users matching this rule | <div>Click and then select a subscription type. Note that this option is visible only if you select the Allow traffic action below. It is not visible f you select the Deny traffic action.</div> <div><div><div></div><div>Versa Secure Internet Access (VSIA)</div></div><div><div></div><div>Versa Secure Private Access (VSPA)</div></div><div><div></div><div>Versa Secure Private Access (VSPA) & Versa Secure Internet Access (VSIA)</div></div></div> |
| Deny | Click to drop all traffic that matches the rule. |

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...)
Updated: Wed, 23 Oct 2024 08:38:20 GMT
Copyright © 2024, Versa Networks, Inc.

19

| Field | Description |
|---|--|
| ◦ Display Message after Connection is Blocked | Enter the message to display after the connection is blocked. |
| Allow | Click to send all traffic from the user device to the Versa Cloud Gateway. |
| ◦ Display Message after Successful Connection | Enter the message to display after the connection is successful. |
| ◦ Trusted Routes | (For Releases 11.4.3 and later.) To add routes that are trusted, click the down arrow, and then enter one or more route prefixes. If you select Send Apps to Versa Cloud Gateway, which is a forced tunnel, all traffic is sent to the gateway. |
| ◦ Excluded Routes | <p>(For Releases 11.4.3 and later.) If you do not want to send specific traffic to the gateway, you can specify routes to exclude. Traffic that uses an excluded route is not sent to the gateway, even if you select Send Apps to Versa Cloud Gateway. To add routes to exclude, click the down arrow, and then enter one or more route prefixes.</p> <p>This field displays if you choose one of the following subscription types:</p> <ul style="list-style-type: none"> ◦ Versa Secure Internet Access (VSIA) ◦ Versa Secure Private Access (VSPA) & Versa Secure Internet Access (VSIA) |

3. Click Next to go to the Review and Configure screen. See [Review and Enable SASE Secure Client Access Rules](#).

Configure Traffic-Steering Rules for Windows Operating Systems

1. In the Secure Client Access Rule List screen, click + Add to create a new rule. The Create Secure Client Access Rule screen displays.
2. Select Traffic Action, and then select the Send Applications to Versa Cloud Gateway tab. Enter information for the following fields.

Configure > SASE > Secure Client Access > Policy Rules

Create Secure Client Access Rule

1

Operating System

2

Users/User Groups

3

Device Risk Info

4

Source Geo Location & Source IP Address

5

Traffic Action

6

Gateways

7

Client Configuration

8

Agent Profile From EIP

9

Review & Configure

Based on the most common secure enterprise settings, we've chosen the traffic steering below.

If you prefer, you can customize which traffic steering option you would like to enable for the rule.

Select subscription type for users matching this rule.

Versa Secure Private Access (VSPA) & Versa Secure Internet Access (VSIA)

Deny

Drop all traffic that matches the rule

Display Message after Connection is Blocked

You are not allowed to connect to the enterprise VPN, please contact administrator

Allow

Allow all traffic that matches the rule to pass

Send Apps to Versa Cloud Gateway

Breakout To Internet

With this option, the default behavior is to send all traffic from the user device to the Versa Cloud Gateway. Select applications below to bypass the tunnel and be sent out directly to the Internet from the user device.

Display Message after Successful Connection

Welcome to ACME

Search for Applications

+ Add New

Custom Applications (Selected: 0 of 4)

tag-1 tag-2 tag-3 tag-4

Predefined Applications (Selected: 0 of 54)

Bitcasa

Druva

Rally Software

Citrix Workspace

Rescue Remote S...

Microsoft Intune ...

Apple App Store

DocuSign

Microsoft Skype F...

Amazon Kindle

Planview Project...

PingOne For Ente...

Google Play Store

Facebook

Trusted Routes (0)

Trusted Routes

Press Enter to add

Excluded Routes (0)

Excluded Routes


Press Enter to add

Cancel

Back

Skip to Review

Next

| Field | Description |
|---|--|
| Select subscription type for users matching this rule | <p>Click and then select a subscription type. Note that this option is visible only if you select the Allow traffic action below. It is not visible if you select the Deny traffic action.</p> <ul style="list-style-type: none"> ◦ Versa Secure Internet Access (VSIA) ◦ Versa Secure Private Access (VSPA) ◦ Versa Secure Private Access (VSPA) & Versa Secure Internet Access (VSIA) |
| Deny | Click to drop all traffic that matches the rule. |
| ◦ Display Message after Blocked Connection | Enter the message to display after the connection is blocked. |
| Allow | Click to allow all traffic that matches the rule to pass. |
| ◦ Send Apps to Versa Cloud Gateway tab | Click to send all traffic from a user device to the Versa Cloud Gateway. Select applications below to bypass the tunnel and to send out directly to the internet from a user device. |
| ◦ Breakout to Internet tab | Click to send all private traffic over the tunnel to the Versa Cloud Gateway and all internet-bound traffic from the user device to the internet directly (Split Tunnel/Direct Internet Access). Select applications below to send traffic for those applications over the tunnel to the Versa Cloud Gateway. |
| ◦ Display Message after Successful Connection | Enter the message to display when the connection is successful. |
| ◦ Search | Enter an application name to search for in the list of all applications. |
| ◦  Add New | Click to add a new user-defined application. See Step 3 below. |
| ◦ Custom Applications | Select one or more custom applications to send traffic for those applications over the tunnel to the VCG. |
| ◦ Predefined Applications | Select one or more predefined applications to send traffic for those applications over the tunnel to the VCG. |

| | |
|---|--|
| <ul style="list-style-type: none"> Trusted Routes | <p>(For Releases 11.4.3 and later.) To add routes that are trusted, click the down arrow, and then enter ;one or more route prefixes. If you select Send Apps to Versa Cloud Gateway, which is a forced tunnel, all traffic is sent to the gateway.</p> |
| <ul style="list-style-type: none"> Excluded Routes | <p>(For Releases 11.4.3 and later.) If you do not want to send specific traffic to the gateway, you can specify routes to exclude. Traffic that uses an excluded route is not sent to the gateway, even if you select Send Apps to Versa Cloud Gateway. To add routes to exclude, click the down arrow, and then enter one or more route prefixes.</p> <p>This field displays if you choose one of the following subscription types:</p> <ul style="list-style-type: none"> Versa Secure Internet Access (VSIA) Versa Secure Private Access (VSPA) & Versa Secure Internet Access (VSIA) |

3. To add a new application, click **+** Add New. In the Enter Application Details section, enter information for the following fields.

Configure > SASE > Settings > User Defined Objects

Application

1 ENTER APPLICATION DETAILS

Application Type

Client Native Application

☒ File Path ☐ FQDN

Upload Application Image (Optional)

+

Add

File formats: png & svg

Cancel Next

2 NAME AND TAGS

| Field | Description |
|--------------------------|---|
| Application Type | Client Native Application |
| File Path | Enter the path to the application file. |
| FQDN | Enter the fully qualified domain name for the application file. |
| Upload Application Image | Click to upload an image for the application. |

- Click Next. In the Name and Tags section, enter a name for the application and enter any tags that you want to associate with the application.

The screenshot shows a web form titled 'ENTER APPLICATION DETAILS'. It has two main sections: 'ENTER APPLICATION DETAILS' (top) and 'NAME AND TAGS' (bottom). The 'NAME AND TAGS' section is highlighted with a red box and a blue circle containing the number 2. This section contains two input fields: 'Name' (with a red asterisk indicating it is required) and 'Tags'. At the bottom of the form are two buttons: 'Cancel' and 'Save' (which is highlighted with a red box).

- Click Save. The Traffic Action screen displays again.
- Click Next to go to the Gateways screen.

Configure SASE Gateways for Secure Client Access

By default, VSPA clients can use all available gateway groups to access the enterprise network. You can also customize the configuration to choose which gateway groups the VSPA clients can use.

To configure SASE gateway groups:

- In the Create Secure Client Access Rule screen, select Gateways. The following screen displays:

Configure > SASE > Secure Client Access > Policy Rules

Create Secure Client Access Rule

1

OPERATING SYSTEM

2

USERS/USER GROUPS

3

DEVICE RISK INFO

4

SOURCE GEO LOCATION & SOURCE IP ADDRESS

5

TRAFFIC ACTION

6

GATEWAYS

7

CLIENT CONFIGURATION

8

AGENT PROFILE FROM EIP

9

REVIEW & CONFIGURE

By default all gateway groups have been selected.
If you prefer, you can select a specific gateway to allow access.

Gateway Groups

☒ All Selected | 2

- ☒ USA-West
- ☒ USA-East

Gateways

Select VPN

ACME-Enterprise

Selected | 0

| GATEWAY | GATEWAY GROUP | CLIENT ADDRESS POOL NAME |
|--|---------------|--------------------------|
| <input type="checkbox"/> USA-West-GW-1 | USA-West | |
| <input type="checkbox"/> USA-West-GW-2 | USA-West | |
| <input type="checkbox"/> USA-East-GW-1 | USA-East | |

Cancel

Back

Skip to Review

Next

- In the Gateway Groups box, select one or more gateway groups. Note that you must select at least one gateway group. The gateways belonging to the gateway group display in the Gateways box to the right.
- In the Gateways box:
 - Select a VPN. The screen then displays the available gateways for that VPN.
 - Select one or more of the gateways, and then select a client address pool name. Each drop-down list contains the client IP address pools that are configured on the selected gateway.
- Click Next to go to the Client Configuration screen.

For information about configuring multiple VPNs and multiple client address pools, see [Configure SASE Tenants](#).

Create a SASE Client Configuration for Secure Client Access

By default, a SASE client is configured using the most common enterprise settings. You can also customize the client configuration in the following ways:

- Choose a different secure client access profile or create a new secure client access profile.
- Enable/disable and configure multifactor authentication (MFA).
- Select the type of VPN to use, IPsec VPN or SSL VPN (for Releases 12.1.1 and later).
- Choose which controls are available to SASE client users.

To customize a client configuration:

- In the Create Secure Client Access Rule screen, select Client Configuration. By default, the most common secure enterprise settings are selected.

Configure > SASE > Secure Client Access > Policy Rules

Create Secure Client Access Rule

✓

Operating System

✓

Users/User Groups

✓

Device Risk Info

✓

Source Geo Location & Source IP Address

✓

Traffic Action

✓

Gateways

7

Client Configuration

8

Agent Profile From EIP

9

Review & Configure

Based on the most common secure enterprise settings, we have defined your client configuration.
If you prefer, you can customize the client configuration setting for the rule.

Secure Client Access Profile ⓘ

Use the following Secure Client Access profile for this rule.

SCA-Profile

+ Add New Profile

Profile Details

+ Routes And DNS Resolvers

MFA ⓘ

☐ MFA is switched off

VPN Type ⓘ

☒ IPsec ☒ SSL

Select SSL Protocol
☒ TLS ☐ DTLS

Select the Primary VPN Type
☒ IPsec ☐ SSL

Client Controls ⓘ

☒ Always On
☒ Remember Credentials
☒ Allow Client Customization

Customize

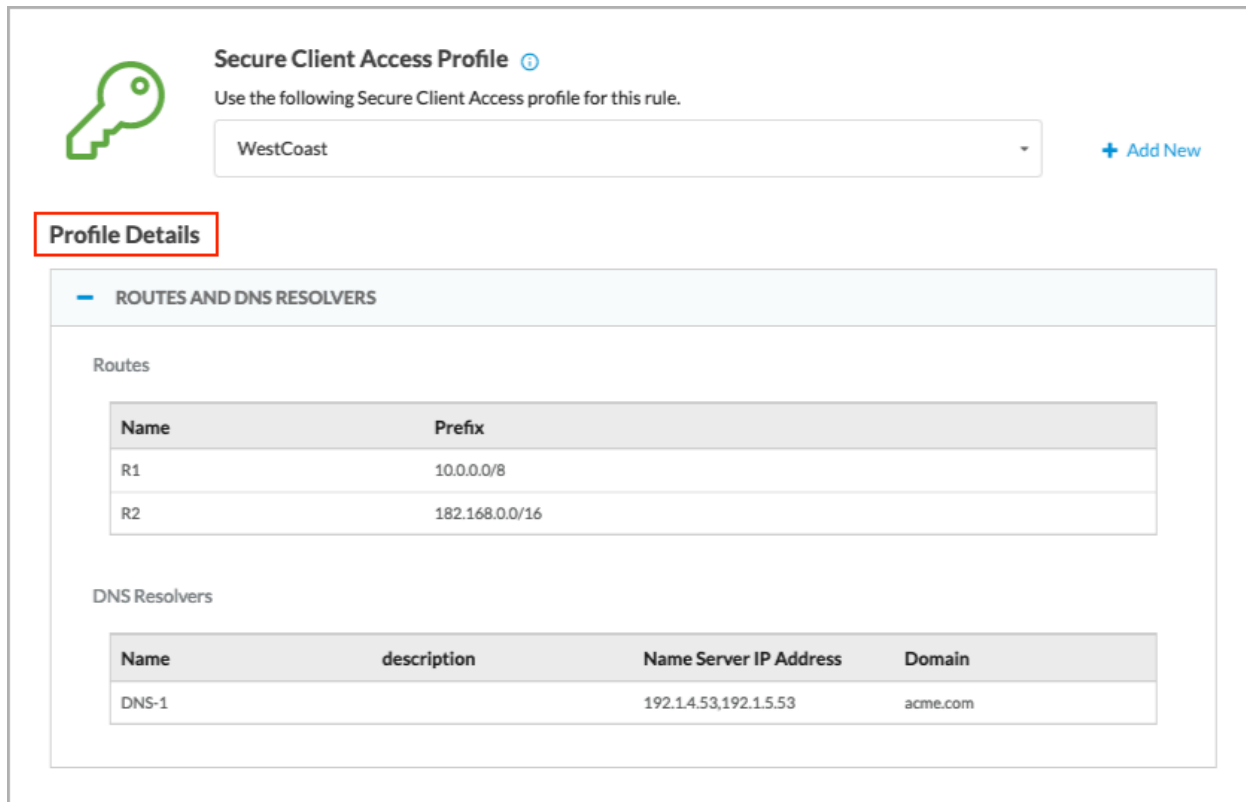
Cancel

Back

Skip to Review

Next

- To specify a secure client access profile for the rule, click the down-arrow in the Secure Client Access Profile box, and then choose a profile. The Profile Details table displays.
- In the Profile Details table, click the Plus icon to view information about the route and DNS resolvers defined in the profile.



Secure Client Access Profile ⓘ

Use the following Secure Client Access profile for this rule.

WestCoast + Add New

Profile Details

— ROUTES AND DNS RESOLVERS

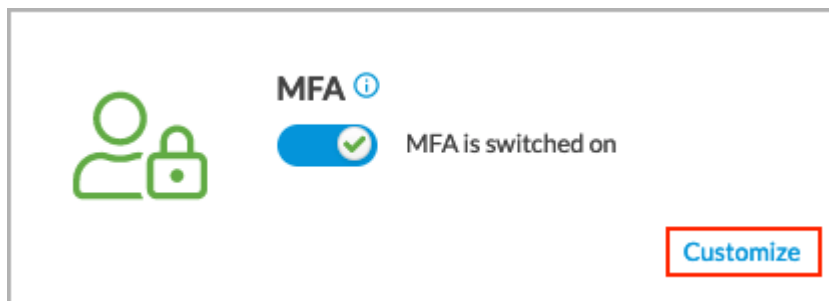
Routes

| Name | Prefix |
|------|----------------|
| R1 | 10.0.0.0/8 |
| R2 | 182.168.0.0/16 |



DNS Resolvers

| Name | description | Name Server IP Address | Domain |
|-------|-------------|------------------------|----------|
| DNS-1 | | 192.14.53,192.15.53 | acme.com |

4. To add a new profile, click + Add New. For more information, see [Configure SASE Secure Client Access Profiles](#).
5. By default, MFA is disabled. To enable MFA, in the Create Secure Client Access Rule screen, click the slider. When MFA is enabled, the Customize option displays.



MFA ⓘ

  MFA is switched on

Customize

6. Click Customize to change the MFA settings. In the Configure MFA screen, enter information for the following fields.
 - a. Select Email OTP Authentication Service to enable one-time password authentication using email, and then enter information for the following fields.

← Back

Configure MFA

☒ Email OTP Authenticator Service
 ☐ Time based OTP Authenticator Service

Message

OTP Format

One-time Password length

Password Valid(in seconds)

| Field | Description |
|--------------------------|---|
| Message | Enter a message to send using the email OTP authentication service. |
| OTP Format | Select a format for the one-time password: <ul style="list-style-type: none"> ▪ Alphabetic, ▪ Alphanumeric ▪ Numeric |
| One-time Password Length | Enter the length of the password. <i>Default: 6</i> <i>Range: 6 through 14</i> |
| Password Valid | Enter how long the password is valid, in seconds <i>Default: 3 seconds</i> <i>Range: 1 through 3600 seconds</i> |

- b. Select Time-Based OTP Authentication Service to enable time-based authentication.

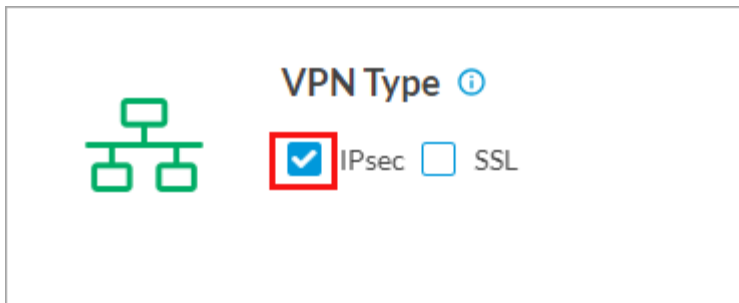
← Back

Configure MFA

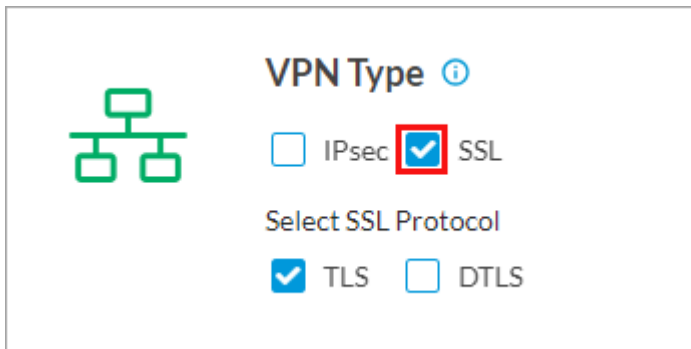
☐ Email OTP Authenticator Service
 ☒ Time based OTP Authenticator Service

- Click ← Back to return to the Client Configuration screen.
- (For Releases 12.1.1 and later.) By default, Concerto uses IPsec as the VPN type. You can select IPsec VPN or SSL VPN, or you can use both as the VPN type. IPsec VPN defines the properties of the IPsec and IKE tunnels between tenants (organizations) and SD-WAN network devices. SSL VPN allows remote users to connect to

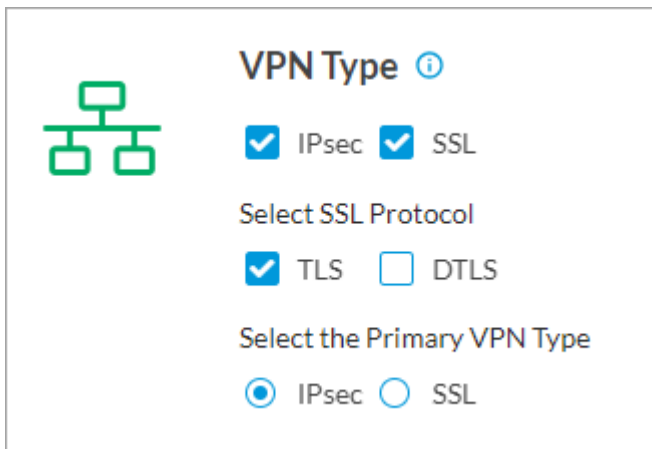
Versa gateways using the Versa SASE client. The Versa proprietary SSL VPN protocol is based on Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). The following screenshot shows the default VPN type selection (IPsec).



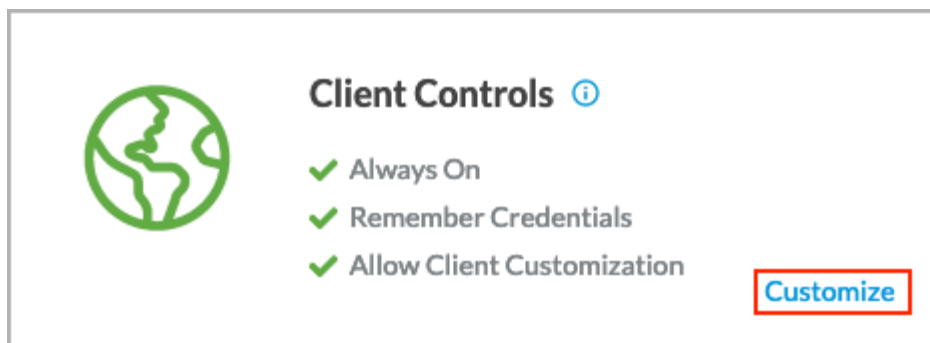
- a. To use only SSL VPN, select SSL and unselect IPsec. The following options display, with TLS selected by default. You can use TLS or DTLS, or both.



- b. To use both types of VPNs, click IPsec and SSL. The following options display.



- c. Select the VPN type to use as the primary VPN.
9. By default, you have full control of the secure client gateways. Client controls are the configurations that control the Versa Client Application's (also called the SASE Client Application) behavior and permissions. Click Customize in the Client Controls box to change the the secure client gateway settings.



10. In the Configure Client Controls screen, enter information for the following fields.

Configure > SASE > Secure Client Access > Policy Rules

Create Secure Client Access Rule

✓

Operating System

✓

Users/User Groups

✓

Device Risk Info

✓

Source Geo Location & Source IP Address

✓

Traffic Action

✓

Gateways

7

Client Configuration

8

Agent Profile From EIP

9

Review & Configure

Based on the most common secure enterprise settings, we have defined your client configuration.

If you prefer, you can customize the client configuration setting for the rule.

← Back

Configure Client Controls

By default, we have provided full control of the secure client gateways. You can customize, by selecting which settings to use for your organization.

What client controls do you have

☒ Allow Client Customization ⓘ

☒ Remember Credentials ⓘ

☐ Auto Update ⓘ

Preferred Client Version: Mac OS 7.5.3 | Windows OS 7.8.0

[Edit Preferred Client Version](#)

Client Logo URL ⓘ

Portal Lifetime (in Minutes) ⓘ

1440

Certificate Issuer

Trusted Network Hostname ⓘ

Advanced Settings

☐ Tamper Protection(Supported only on Windows client from version 7.8) ⓘ

☐ Strict Tunnel Mode

☐ AutoDisconnect

☒ Always On

Disconnect

☐ Never
 ☒ Interval (Seconds)

120

Override

Interval (Seconds)

120

Fall

☐ Close
 ☒ Open

☐ Display Gateway (Enable/disable displaying of gateways in Versa Client application)

☐ Tunnel Monitoring (Supported from Windows client version 7.6 and Mac client version 7.5)

☐ Registration with Domain Name System(DNS) (Supported only on Windows client from version 7.6)

☐ Reconnect (Supported from Windows client version 7.6 and Mac client version 7.5)

☐ IP Address Stickiness (Supported from Windows client version 7.6 and Mac client version 7.5)

☐ Two-Way Active Measurement Protocol (TWAMP) (Supported from Windows client version 7.6 and Mac client version 7.5)

Password Expiry Warn Before (in Days) ⓘ

10

User's View of Client

Secure Access Client

VERSANETWORKS

Versa Networks

Secure Access Servers >

Reregister >

Reset Password >

Remember Credentials ☒

Always On ☒

Clear Data

Delete Account

Cancel

Back

Skip to Review

Next

https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Secure_Clie...


Updated: Wed, 23 Oct 2024 08:38:20 GMT

Copyright © 2024, Versa Networks, Inc.

31

| Field | Description |
|--|--|
| What client controls do you have | <p>Select one or more client controls:</p> <ul style="list-style-type: none"> ◦ Allow Client Customization—Enable or disable the Edit Gateway tab. ◦ Remember Credentials—Enable or disable the remembering or credentials. ◦ Auto Update—(For Releases 11.4.1 and later.) Enable or disable automatic updating of the client. If enabled, the client automatically updates to the version you select. Click Edit Preferred Client Version to change the software version to which to automatically update the client. The Preferred Client Version window displays. For more information, see Select Preferred SASE Client Version, below. |
| Client Log URL | Enter the URL to reach the client logo. |
| Portal Lifetime (in Minutes) | <p>Enter the desired registration lifetime of the portal.</p> <p><i>Default:</i> 300 minutes</p> <p><i>Range:</i> 1 through 1440 minutes</p> |
| Certificate Issuer | Enter the name of the entity that issued the certificate. |
| Trusted Network Hostname | Enter the hostname of the trusted accessible network. This option determines whether a SASE client is already behind a trusted VPN network. If so, connecting to the SASE gateway is bypassed. |
| Advanced Settings (Group of Fields) | |
| <ul style="list-style-type: none"> ◦ Tamper Protection | (For Releases 11.4.1 and later.) If enabled from the server side, you cannot uninstall the client, delete the client account, or delete any files from the installation directory. To disable, click the Tamper Protection toggle button in the Account Details window and then enter the tamper protection authentication key. |
| <ul style="list-style-type: none"> ◦ Strict Tunnel Mode | (For Releases 11.4.1 and later.) Redirect all traffic through the tunnel. If disabled, specific traffic is routed through a tunnel and the rest is sent directly onto a WiFi or Ethernet interface. |

| | |
|--|--|
| <ul style="list-style-type: none"> ◦ Autodisconnect | <p>(For Releases 11.4.1 and later.) Automatically disconnect tunnel after the configured autodisconnection interval.</p> |
| <ul style="list-style-type: none"> ◦ Always On | <div> <div> <input checked="" type="checkbox"/> Always On </div> <div> <div> Disconnect <input type="radio"/> Never <input checked="" type="radio"/> Interval 120 </div> <div> Override Interval 120 </div> <div> Fail <input type="radio"/> Close <input checked="" type="radio"/> Open </div> </div> </div> <p>Enter information for the following fields:</p> <ul style="list-style-type: none"> ◦ Disconnect—Enter a disconnect interval time. <ul style="list-style-type: none"> ▪ <i>Range:</i> 1 through 65535 ▪ <i>Default:</i> 120 ◦ Override Interval—Enter an override interval time. <ul style="list-style-type: none"> ▪ <i>Range:</i> 1 through 65535 ▪ <i>Default:</i> 120 ◦ Fail—Choose the action to take when the connection fails <ul style="list-style-type: none"> ▪ Close ▪ Open (default) |
| Display Gateway | Click to enable display of gateways on the SASE client UI. |

| | |
|---|--|
| <ul style="list-style-type: none"> ◦ Tunnel Monitoring (Supported on Windows client version 7.6 and Mac client version 7.5) | <div data-bbox="857 207 1622 470"> <input checked="" type="checkbox"/> Tunnel Monitoring <small>(Supported from Windows client version 7.6 and Mac client version 7.5)</small> <div> <div>Hosts ⓘ</div> <div>Interval (seconds) ⓘ</div> </div> <div> <input type="text"/> <input type="button" value="+"/> <input type="text" value="60"/> </div> <div> <div>Interval Retry ⓘ</div> <div>Connection Retry ⓘ</div> </div> <div> <input type="text" value="10"/> <input type="text" value="5"/> </div> </div> <p>Enter information for the following fields:</p> <ul style="list-style-type: none"> ◦ Hosts—Enter one or more hosts to use for tunnel monitoring. Click the  Add icon to add additional hosts. ◦ Interval—Enter the tunnel monitoring interval, in seconds. <ul style="list-style-type: none"> ▪ <i>Range:</i> 1 through 255 seconds ▪ <i>Default:</i> 60 seconds ◦ Interval Retry—Enter the interval between tunnel monitoring retry attempts, in seconds. <ul style="list-style-type: none"> ▪ <i>Range:</i> 1 through 255 seconds ▪ <i>Default:</i> 10 seconds ◦ Connection Retry—Enter the number of connection retry attempts before concluding that the tunnel is down. <ul style="list-style-type: none"> ▪ <i>Range:</i> 1 through 255 ▪ <i>Default:</i> 5 |
| <ul style="list-style-type: none"> ◦ Registration with Domain Name System (DNS) (Supported on Windows client versions 7.6 and later) | <div data-bbox="857 1323 1622 1564"> <input checked="" type="checkbox"/> Registration with Domain Name System(DNS) <small>(Supported only on Windows client from version 7.6)</small> Enter DNS name ⓘ <input type="text"/> </div> <p>Enter a DNS suffix to enable or disable DNS.</p> <p><i>Range:</i> 1 through 255</p> <p><i>Default:</i> None</p> |

| | |
|--|--|
| <ul style="list-style-type: none"> ◦ Reconnect (Supported on Windows client version 7.6 and Mac client version 7.5) | <div data-bbox="857 210 1624 705"> <input checked="" type="checkbox"/> Reconnect <i>(Supported from Windows client version 7.6 and Mac client version 7.5)</i> <div> Interval ⓘ <div>10</div> </div> <div> Retry Count ⓘ <div>5</div> </div> </div> <p>Enter information for the following fields</p> <ul style="list-style-type: none"> ◦ Interval—Interval between autoreconnect attempts, in seconds. <ul style="list-style-type: none"> ▪ <i>Range:</i> 1 through 255, in seconds ▪ <i>Default:</i> 10 seconds ◦ Retry Count—Number of autoreconnect retry attempts. <ul style="list-style-type: none"> ▪ <i>Range:</i> 1 through 255 ▪ <i>Default:</i> 5 |
| <ul style="list-style-type: none"> ◦ IP Address Stickiness (Supported on Windows client version 7.6 and Mac client version 7.5) | Click to enable IP address stickiness, which stores the tunnel IP address provided during a connection and requests the same IP address for subsequent connections to the same gateway. |
| <ul style="list-style-type: none"> ◦ Two-Way Active Measurement Protocol (TWAMP) (Supported on Windows client version 7.6 and Mac client version 7.5) | Click to enable TWAMP. |
| Password Expiry Warn Before | <p>Enter the number of days before a password expiration warning is displayed.</p> <p><i>Default:</i> 10 days</p> <p><i>Range:</i> 1 through 255 days</p> |

11. Click Next to go to the Agent Profile from EIP screen.

Configure EIP Agent Profiles for Secure Client Access

EIP agent profiles define when the SASE client extracts information from endpoint devices. You associate predefined or custom EIP agents with secure client access rules to enforce EIP security. For more information, see [Configure a Custom EIP Agent Profile](#).

To configure EIP agent profiles for Secure Client Access rules:

1. In the Create Secure Client Access Rule screen, select the Agent Profile from EIP tab.

Configure > SASE > Secure Client Access > Policy Rules

Create Secure Client Access Rule

1 OPERATING SYSTEM 2 USERS/USER GROUPS 3 DEVICE RISK INFO 4 SOURCE GEO LOCATION & SOURCE IP ADDRESS 5 TRAFFIC ACTION 6 GATEWAYS 7 CLIENT CONFIGURATION 8 AGENT PROFILE FROM EIP 9 REVIEW & CONFIGURE

EIP Agent Profile

Type EIP Agent Profiles

Cancel Back Skip to Review Next

2. To associate an existing custom EIP agent profile with the Secure Client Access rule:
 - a. Select User Defined in the Type field.
 - b. Select a custom profile in the EIP Agent Profiles.
 - c. To add a new EIP Agent Profile, click + Create New. The Create EIP Agent Profile screen displays. For more information, see [Configure a Custom EIP Agent Profile](#).

EIP Agent Profile

Type EIP Agent Profiles

User Defined + Create New

3. To associate a predefined EIP agent profile with the Secure Client Access rule, select Predefined in the Type field, and then select a profile in the EIP Agent Profiles field.

EIP Agent Profile

Type: Predefined EIP Agent Profiles: AntiMalware_category_all

| CATEGORY | MATCH CATEGORIES |
|-------------|---|
| AntiMalware | Installed : True Configured : True Running : True Realtime : True Last Definition Update Time(in hours) : True Show More |

- Click Next to go to the Review & Configure screen.

Review and Enable SASE Secure Client Access Rules

The final step in configuring secure client access rules is to review the choices you have made, edit them if needed, and then deploy the new rule.

- In the Create Secure Client Access Rule screen, select Review and Configure, and then enter information for the following fields.

Configure > SASE > Secure Client Access > Policy Rules

Create Secure Client Access Rule

Progress: 1. OPERATING SYSTEM (✓) 2. USERS/USER GROUPS 3. DEVICE RISK INFO 4. SOURCE GEO LOCATION & SOURCE IP ADDRESS 5. TRAFFIC ACTION 6. GATEWAYS 7. CLIENT CONFIGURATION 8. AGENT PROFILE FROM EIP 9. REVIEW & CONFIGURE (selected)

Please give your rule a name:

General

Name * Description

Tags

☒ Rule is enabled

Device Risk Info [Edit](#)

[Device Compliance Status](#)


No Device Compliance options selected


[EIP Information Profile](#)

No EIP Information Profile Details selected

EIP Agent Profile [Edit](#)

Cancel Back Save

| Field | Description |
|-----------------|---|
| Name (Required) | Enter a name for the rule. |
| Description | Enter a text description for the rule. |
| Tags | Enter one or more tags to help identify the rule. A tag is an alphanumeric text descriptor with no white spaces or special characters that you can use to search objects. You can specify multiple tags. |
| Rule is enabled | Click the slider to enable the rule.  |

2. If required, edit the configuration for a given section by clicking the  **Edit** Edit icon.
3. Click Save to save the new secure client access rule.

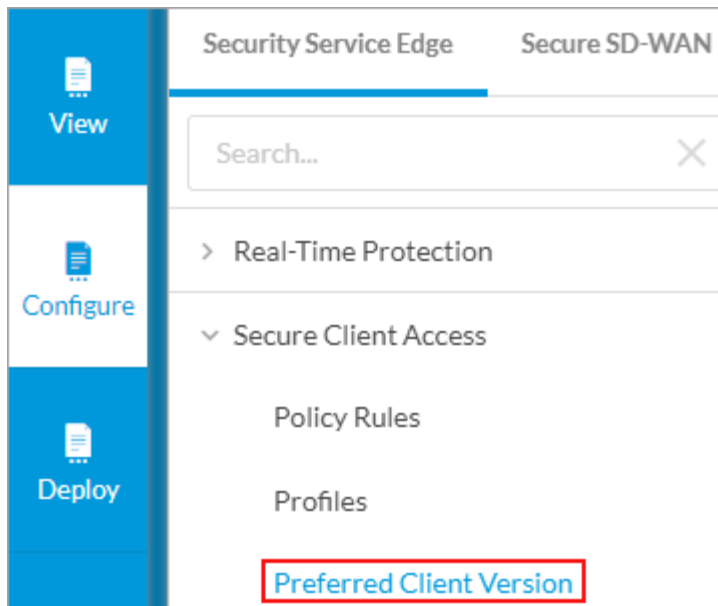
Select the Preferred SASE Client Version

For Releases 11.4.1 and later.

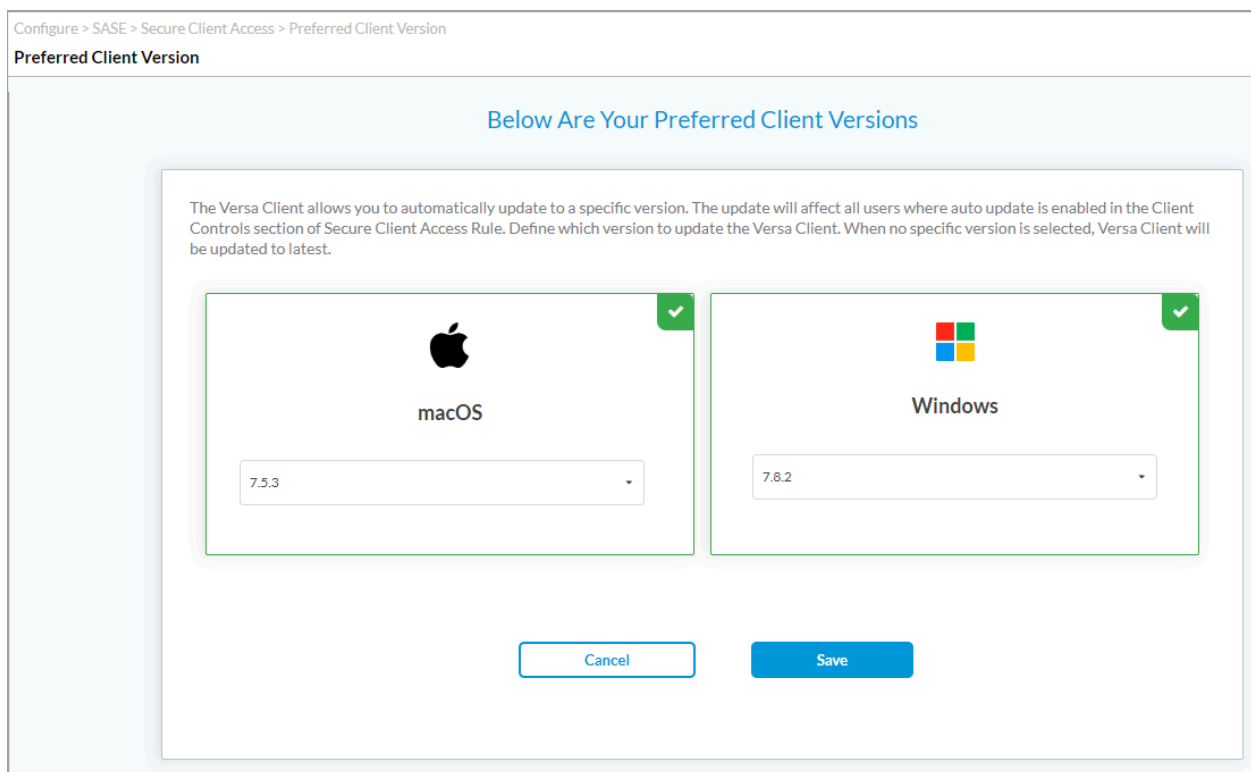
You can automatically update the Versa SASE client for MacOS and Windows OS to a specific version. If you enable Auto Update on the Configure Client Controls screen, as described in [Create a SASE Client Configuration for Secure Client Access](#), above, you can select the preferred software version to use when updating the client. If you do not select a preferred software version, the client software is updated to the latest version.


To select the preferred SASE client version to use during an automatic update:

1. Go to Configure > Secure Client Access > Preferred Client Version.



The Preferred Client Version window displays.



2. Click the  Select icon to select MacOS or Windows OS, and then select the SASE client software version.
3. Click Save.

Supported Software Information

Releases 11.1.1 and later support all content described in this article, except:

- Release 11.4.1 adds support for the Auto Update, Tamper Protection, Strict Tunnel Mode, and Autodisconnect fields in Configure Client Controls screen; and Preferred Client Version under Secure Client Access menu.
- Release 11.4.3 adds support for specifying trusted and excluded routes when you configure traffic actions, supports SSL VPN, and allows you to download a pre-logon configuration file in secure client access policy rules.

Additional Information

[Configure Endpoint Information Profiles](#)

[Configure SASE Secure Client Access Profiles](#)

[Configure SASE Internet Protection Rules](#)

[Configure SASE Private Application Protection Rules](#)

[Configure SASE Tenants](#)