

---

## Configure SASE Secure Client Access Profiles

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

Secure client access profiles define the application monitors, browser access, DNS resolvers, and routes that are used to bind public keys to the client. A DNS resolver is a server that determines which DNS name server the client uses to perform DNS lookups for all traffic. You can configure DNS resolvers that are then shared with the clients when they register.

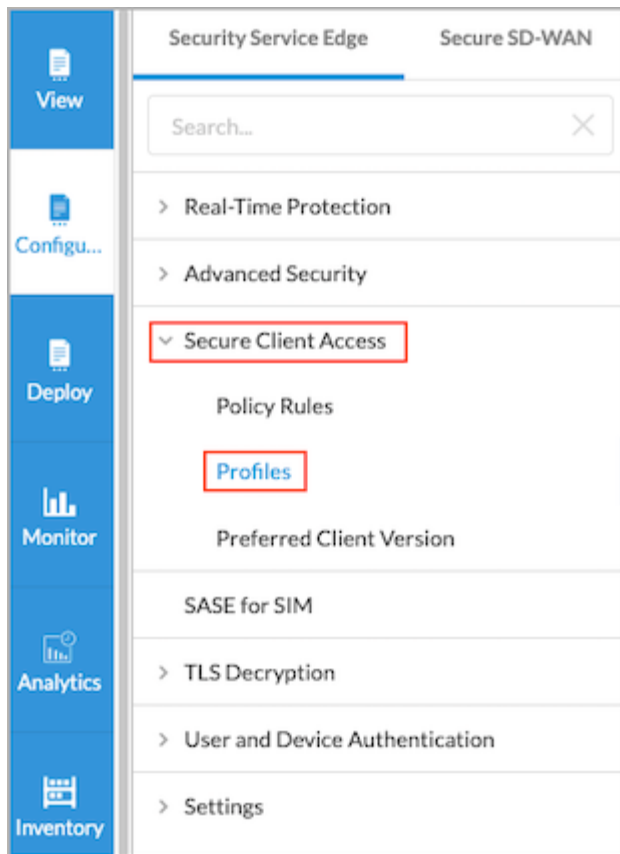
To periodically monitor end-to-end network and application performance for a user device, you can enable Digital Experience Monitoring (DEM) on SASE clients. To do this, you add an application monitor when configuring a secure client access profile. The SASE client receives the settings listed in the application monitor when it registers with the SASE portal. The SASE client collects DEM statistics based on these settings and periodically forwards them to its currently connected SASE gateway. For information about viewing DEM statistics, see the Digital Experience section in [View Integrated Monitoring and Analytics](#).

---

## Configure Secure Client Access Profiles

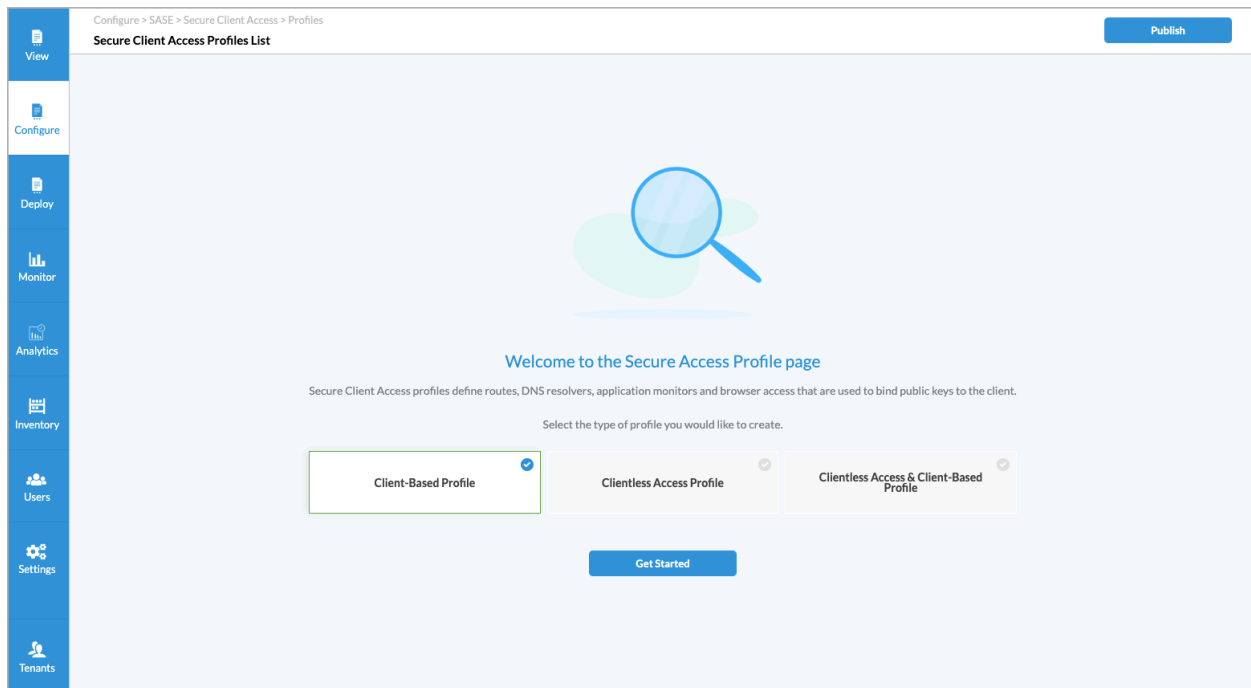
To configure SASE secure client access application monitors, browser access, DNS resolvers, and routes:

1. Go to Configure > Security Service Edge > Secure Client Access > Profiles.

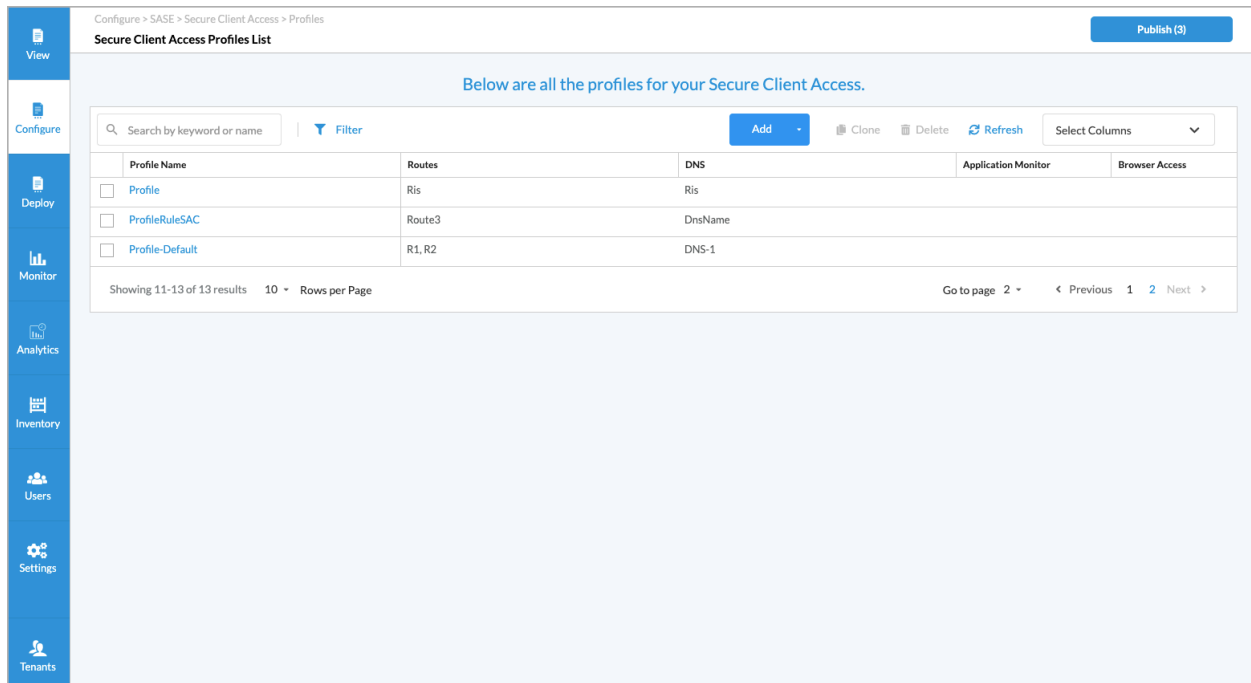


If you have not configured a secure access client profile, the Welcome to the Secure Access Profile page displays. On this page, you can choose to configure one of the following types of profiles:

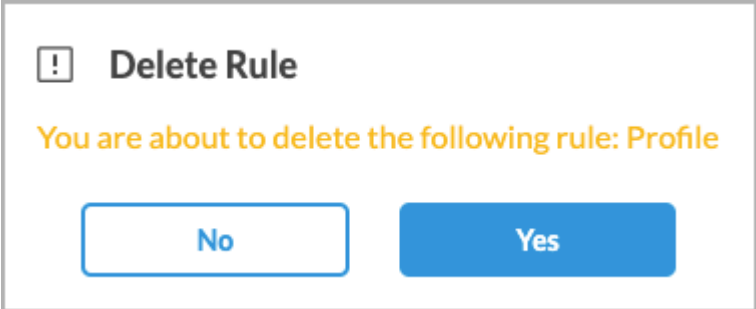
- Client-based profile
- Clientless access profile
- Both client-based and clientless access profile



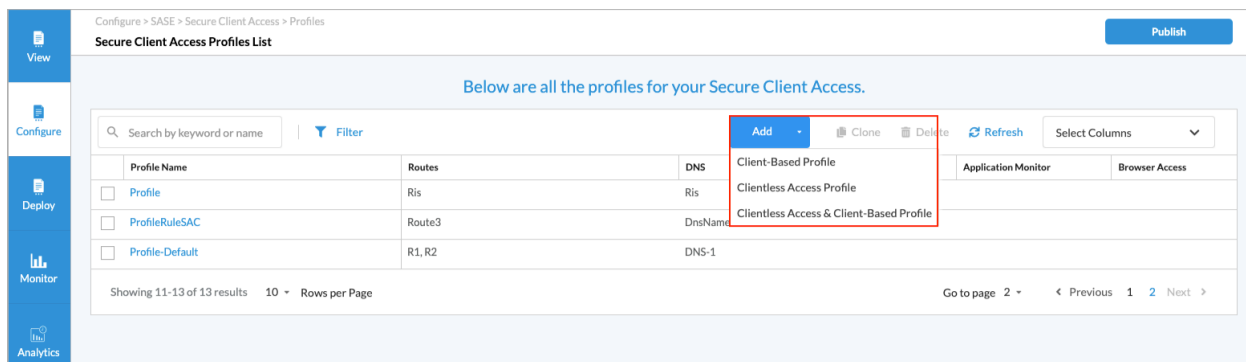
If you have configured one or more secure access client profiles, the Secure Client Access Profile List screen displays the profiles that are already configured.



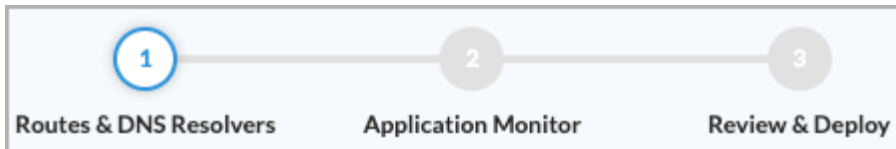
2. In the horizontal menu bar, you can select one of the following operations.

Operation	Description
Add	Create a new secure client access profile. This button is active when no existing
Clone	Clone the selected secure client access profile. When you click Clone, the confi configuration. In the Review & Deploy screen, rename the default name of the c
Delete	<p>Delete the selected access control policy. A popup window similar to the followin</p>  <p>Click Yes to delete the profile, or click No to retain the profile.</p>
Refresh	Refresh the list of existing policies.
Select Columns	To select the columns that you want to display, click the down arrow. To return t

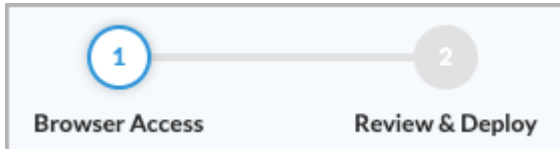
- To edit an existing profile, click the profile name, edit the entries as needed, and then click Save.
- To configure a new profile, click the **+ Add** icon, then select a type of profile to create, and then click Next.



- Client-Based Profile—You are then prompted to configure routes, DNS resolvers and applications for monitoring. Then you are prompted to review and deploy the profile.



- Clientless Access Profile—For browser access, you are prompted to select custom and predefined applications for clientless VPN access. Then you are prompted to review and deploy the profile.



- Clientless Access & Client-Based Profile—You are prompted to configure routes, DNS resolvers, applications for monitoring, and custom and predefined applications for clientless VPN access. Then you are prompted to review and deploy the profile.

The screenshot shows the 'Create Secure Client Access' configuration page. At the top, there's a breadcrumb trail: 'Configure > SASE > Secure Client Access > Profiles'. Below it, the title is 'Create Secure Client Access'. A progress bar shows four steps: 1. Routes & DNS Resolvers (highlighted with a red box), 2. Application Monitor, 3. Browser Access, and 4. Review & Deploy. Below the progress bar, the text says 'Add which routes and DNS resolvers to use.' and 'If you prefer, you can customize which routes and DNS resolvers to use for the client profile.' There are two main panels: 'Routes' and 'DNS Resolvers'. The 'Routes' panel has a green location pin icon, a blue info icon, and the text 'No Routes have been added'. Below it is a red 'Add Routes' button. The 'DNS Resolvers' panel has a green server icon, a blue info icon, and the text 'No DNS Resolvers have been added'. Below it is a red 'Add DNS Resolvers' button. At the bottom of the page, there are four buttons: 'Cancel', 'Back', 'Skip to Review', and 'Next'.

Note: The remaining steps in this procedures show how to configure both a client-based and a clientless access profile. To configure only a client-based or only a clientless access profile, follow the same procedure, performing only the relevant steps.

5. In Step 1, Routes and DNS Resolvers, click Customize in the Routes pane to add routes to the profile. Routes are prefixes that can be reached over the remote access VPN. The Routes pane displays the routes that are already configured.

Configure > SASE > Secure Client Access > Profiles

### Create Secure Client Access

1

2

3

4

Routes & DNS ResolversApplication MonitorBrowser AccessReview & Deploy

Add which routes and DNS resolvers to use.

If you prefer, you can customize which routes and DNS resolvers to use for the client profile.

← Back

Routes

+ Add

Delete

Select Columns

Name	Prefix	Metric	Encrypted
No Data			

Cancel

Back

Skip to Review

Next

- Click + Add to add a new route. In the Add Route popup window, enter information for the following fields.

Add Route

✕

Name\*

Description

Prefix\* ⓘ

Metric



Encryption is enabled

✓

Cancel

Add

Field	Description
Name Required)	Enter a name for the route.
Description	Enter a text description for new route.
Prefix (Required)	Enter a prefix for the route. By default, if you are using Versa Secure Internet Access (VSIA), the 0.0.0.0/0 subnet is advertised to the client. If you are using Versa Secure Private Access (VSPA), the prefix must be in the private access subnet range as defined in RFC 1918 (10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16 ).
Metric	Enter a value for the route metric.

Field	Description
	<p><i>Range:</i> 0 through 4294967295</p> <p><i>Default:</i> None</p>
Encryption	<p>Select to encrypt the route and to route the traffic for applications and domains to an encrypted tunnel. By default, encryption is enabled.</p> <div data-bbox="859 636 1149 758"> <p>Encryption is enabled</p>  </div> <p>To disable encryption, click the slider.</p> <div data-bbox="859 926 1115 1029"> <p>Encryption is disabled</p>  </div> <p>If you disable encryption, traffic is routed on an encrypted or non-encrypted (clear-text) route, depending on the configuration, for applications and domains. If the route is not encrypted, the Versa secure client access creates two tunnels, encrypted and clear text, and then routes traffic. In this case, you might consider securing the application using a different method, such as SSL/TLS.</p>

7. Click Add. The Routes screen displays the new route.
8. Click Back. The Routes and DNS resolvers screen displays.
9. To add DNS resolvers to the profile, click Customize in the DNS Resolvers pane. The DNS Resolvers screen displays the DNS resolvers that are already configured.



Configure > SASE > Secure Client Access > Profiles

### Create Secure Client Access

1

2

3

4

Routes & DNS ResolversApplication MonitorBrowser AccessReview & Deploy

Add which routes and DNS resolvers to use.

If you prefer, you can customize which routes and DNS resolvers to use for the client profile.

← Back

DNS Resolvers

+ AddDeleteSelect Columns

Name	Description	DNS server IP Address	Domain
No Data			

Cancel

Back

Skip to Review

Next

- Click + Add to add a new DNS resolver. In the Add DNS Resolver popup window, enter information for the following fields.

## Add DNS Resolver ✕

Name\*

Description

Domain

DNS Server IP Address

− +

Cancel

Add

Field	Description
Name	Enter a name for the DNS resolver.
Description	Enter a text description for the DNS resolver.
Domain	Enter a valid domain name for the DNS resolver to send to the client. The client uses the DNS resolver to perform DNS lookups for all traffic.
DNS Server IP Address	Enter a valid IP address for the DNS server. To enter additional addresses, click the <span>+</span> Plus icon.

- Click Add to add the new DNS resolver to the secure client access profile. The DNS Resolvers screen displays the new DNS resolver.
- Click Back. The Routes and DNS resolvers screen displays the routes and DNS resolvers that you added.

Configure > SASE > Secure Client Access > Profiles

### Create Secure Client Access

1 Routes & DNS Resolvers
 2 Application Monitor
 3 Browser Access
 4 Review & Deploy

Add which routes and DNS resolvers to use.

If you prefer, you can customize which routes and DNS resolvers to use for the client profile.

**Routes**

Name	Prefix
✓ R1	10.1.1.0/24
✓ R2	10.2.2.0/24

Customize

**DNS Resolvers**

Name	DNS server IP Address
✓ DNS-1	10.3.3.1
✓ DNS-2	10.3.3.2

Customize

Cancel
 Back
 Skip to Review
 Next

- Click Next to continue to Step 2, Application Monitor. To configure DEM, click Customize in the Application Monitor pane.

Configure > SASE > Secure Client Access > Profiles

### Create Secure Client Access

✓ Routes & DNS Resolvers
 2 Application Monitor
 3 Browser Access
 4 Review & Deploy

Add applications you want to include for monitoring at selected network segments.

If you prefer, you can customize which application to include for monitoring for the client profile.

**Application Monitor**

No Application have been selected for monitoring.

Add Application Monitor

Cancel
 Back
 Skip to Review
 Next

- In the Application Monitor screen, enter information for the following fields. These parameters are downloaded to

[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 08:38:27 GMT

Copyright © 2024, Versa Networks, Inc.

the SASE client when a user registers the client with the SASE client portal.

Configure > SASE > Secure Client Access > Profiles

Create Secure Client Access

← Back

Application Monitor

Network Segments

☒ Device Monitoring

☒ Internet Monitoring

☒ Local Network Monitoring

Interval (seconds)

CustomApp1

GMAIL

GOOGLE DOCS

GOOGLE CALENDAR

GOOGLE PHOTOS

GMAIL DRIVE

Search for Application

Clear All

Custom Applications (Selected: 1 of 4)

CustomApp1

Host-Pattern-1

sdsadsd

sf

Predefined Applications (Selected: 5 of 4018)

114LA

115COM

118114CN

11ST

123PEOPLE

1337X

139MAIL

Cancel

Back

Skip to Review

Next

Field	Description
Network Segments (Group of Fields)	
◦ Device Monitoring	Click to monitor the health of devices, including memory, CPU, disk utilization, and battery life.
◦ Internet Monitoring	Click to monitor internet performance, including delay, hops, hop-by-hop latency, jitter, and packet loss.
◦ Local Network Monitoring	Click to monitor the performance of the local network, including latency, jitter, packet loss, WiFi SSID, and signal strength.
◦ Interval	Enter how often to monitor an application, in seconds.
Application Monitoring (Group of Fields)	
◦ Custom Applications	Select one or more user-defined applications.
◦ Predefined Application	Select one or more predefined applications.

15. Click Back. The Application Monitor screen displays the applications that you added.

[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 08:38:27 GMT  
Copyright © 2024, Versa Networks, Inc.


12

Configure > SASE > Secure Client Access > Profiles

**Create Secure Client Access**

Routes & DNS Resolvers Application Monitor Browser Access Review & Deploy

Add applications you want to include for monitoring at selected network segments.  
If you prefer, you can customize which application to include for monitoring for the client profile.



**Application Monitor**

- CustomApp1
- GMAIL
- GOOGLE\_DOCS
- GOOGLE\_CALENDAR
- GOOGLE\_PHOTOS
- GMAIL\_DRIVE

Customize

Cancel Back Skip to Review Next


- Click Next to continue to Step 3, Browser Access. To select custom and predefined applications for clientless VPN access, click Customize in the Browser Access pane.

Configure > SASE > Secure Client Access > Profiles

**Create Secure Client Access**

Routes & DNS Resolvers Application Monitor Browser Access Review & Deploy

Select custom and/or predefined applications for your Clientless VPN access  
If you prefer, you can customize which application to include to allow to the client profile.



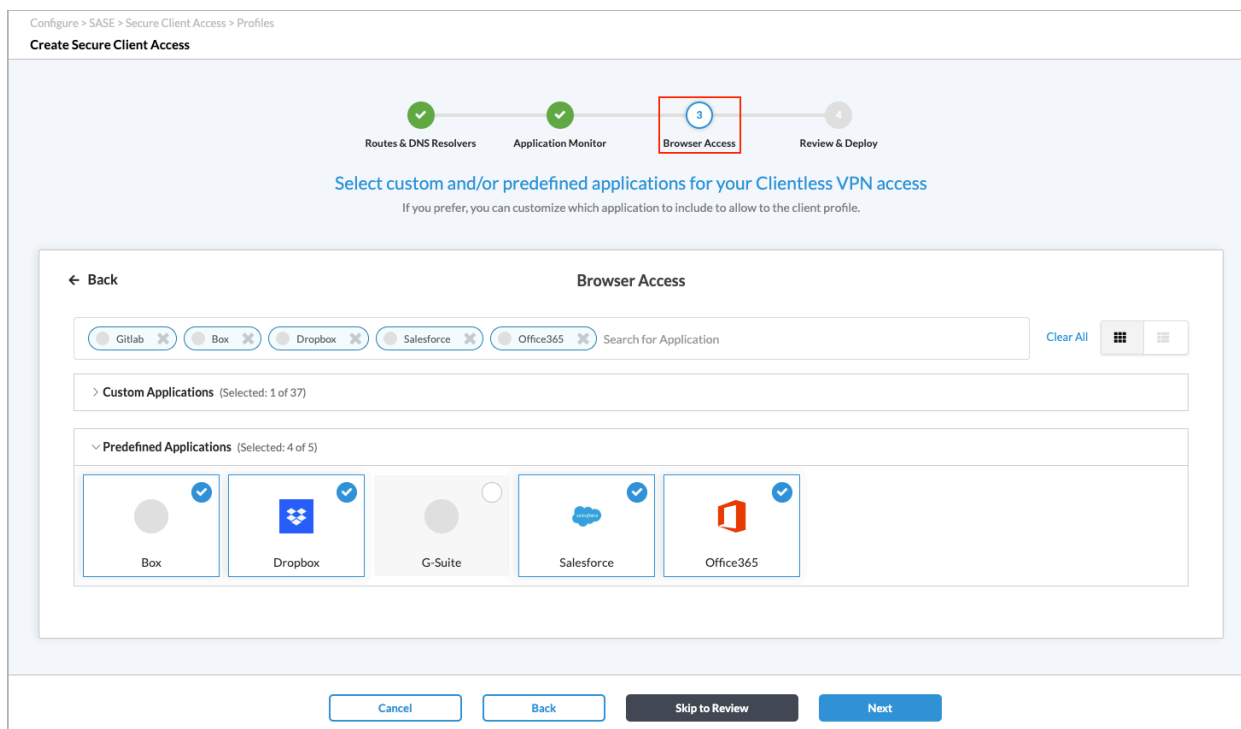
**Browser Access**

No Application have been selected for access

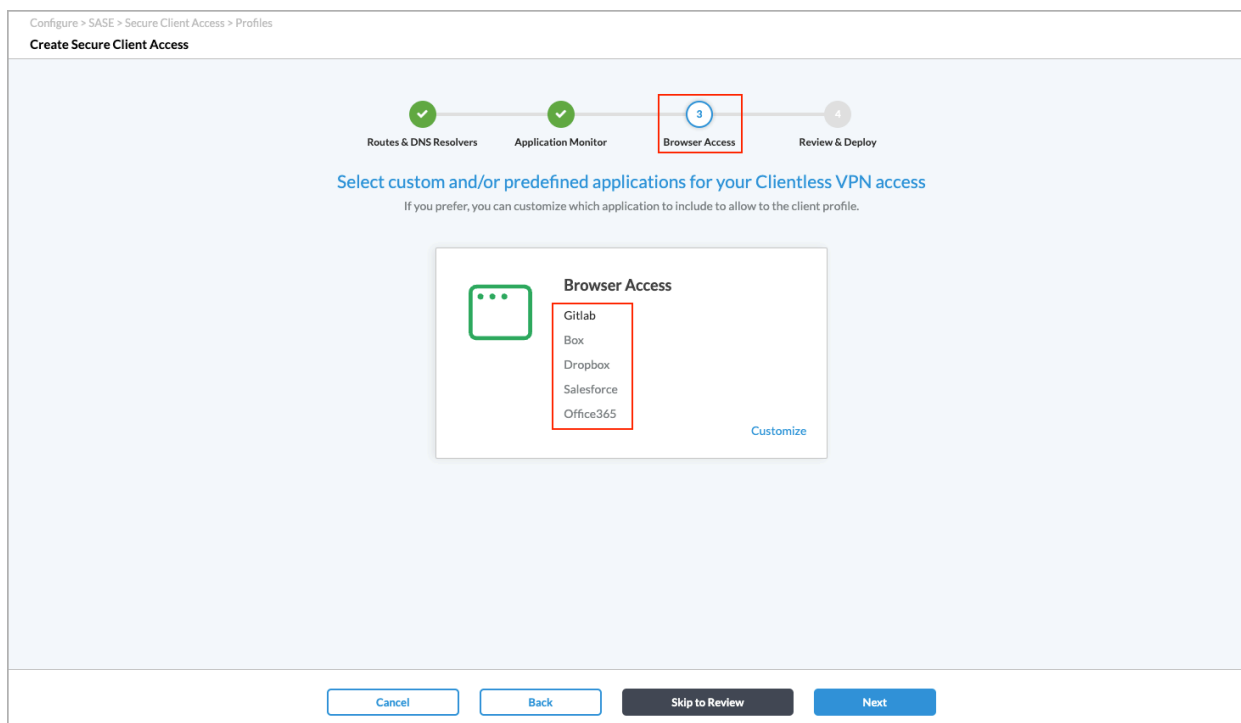
Add Browser Access

Cancel Back Skip to Review Next

17. In the Browser Access screen, select custom applications or predefined applications, or both.



18. Click Back. The Browser Access screen displays with custom and predefined applications that you added.



19. Click Next. In the Review & Submit screen, enter information for the following fields.

Configure > SASE > Secure Client Access > Profiles

Create Secure Client Access

✓

Routes & DNS Resolvers

✓

Application Monitor

✓

Browser Access

4

Review & Deploy

Please give your profile a name:

General

Name \* ⓘ

Description

Tags

Press Enter to add

Routes & DNS Resolvers ⓘ Edit

Routes2 Added

Name	IP Address
R1	10.1.1.0/24
R2	10.2.2.0/24

DNS Resolvers2 Added

Name	Description	DNS server IP Address	Domain
DNS-1		10.3.3.1	
DNS-2		10.3.3.2	

Application Monitor Edit

Network Segments

Device Monitoring: Enabled

Internet Monitoring: Enabled

Local Network Monitoring: Enabled

Interval (seconds): 300

Predefined Applications

GMAIL

GOOGLE\_DOCS

GOOGLE\_CALENDAR

GOOGLE\_PHOTOS

GMAIL\_DRIVE

Custom Applications

CustomApp 1

Browser Access Edit

Predefined Applications

Box

Dropbox

Salesforce

Office365

Custom Applications

Gitlab

Cancel

Back

Save

Field	Description
Name (Required)	Enter a name for the profile.
Description	Enter a text description for the profile.

https://docs.versa-networks.com/Security\_Service\_Edge\_(SSE)/Configuration\_from\_Concerto/Configure\_SASE\_Secure\_Clie...  
Updated: Wed, 23 Oct 2024 08:38:27 GMT  
Copyright © 2024, Versa Networks, Inc.

15

Field	Description
Tags	Enter one or more tags. A tag is an alphanumeric text descriptor with no spaces or special characters. You can specify multiple tags added for the same object. The tags are used for searching the objects.

20. Review the remaining information. Click the  Edit icon to make changes to any of the sections.

21. Click Submit.

---

## Supported Software Information

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

- Release 12.1.1 allows you to clone Private Application Protection Profiles; supports Digital Experience Monitoring (DEM).

---

## Additional Information

[Configure SASE Secure Client Access Rules](#)