Configure SaaS Tenant Control Profiles

For supported software information, click here.

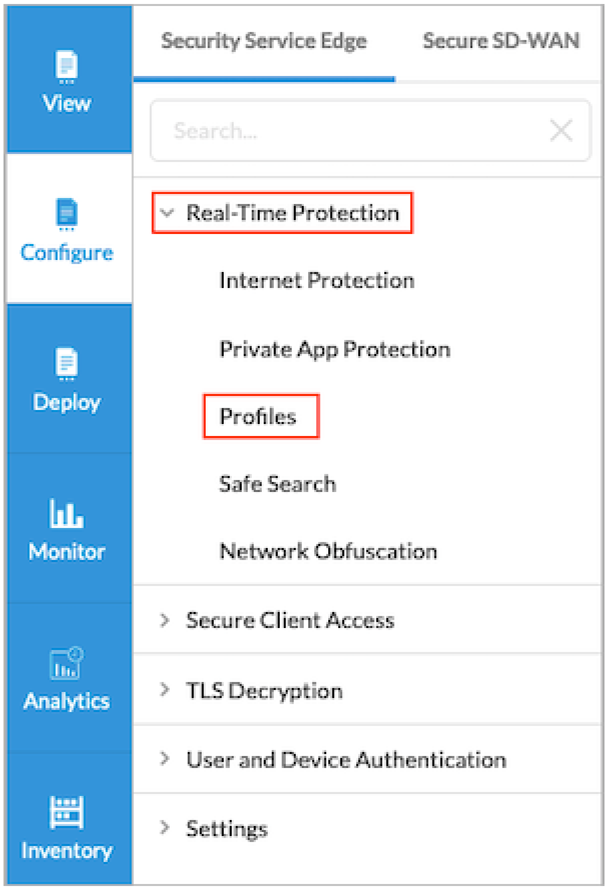
You use SaaS tenant control profiles to block users from directly accessing select services, such as web-based Office365, without going through a Versa gateway. When you configure a SaaS tenant control profile, the tenant control profile inserts fields and values in the HTTP header when traffic goes through the gateway. The headers come from the SaaS application vendors, such as YouTube or Office365. The profile is automatically inserted into all a tenant's TLS decryption profiles.

For a SaaS tenant control configuration to take effect, you must configure a TLS decryption profile that refers to the SaaS tenant control profile, and you must configure policy rules. For more information, see Configure SASE TLS Decryption.

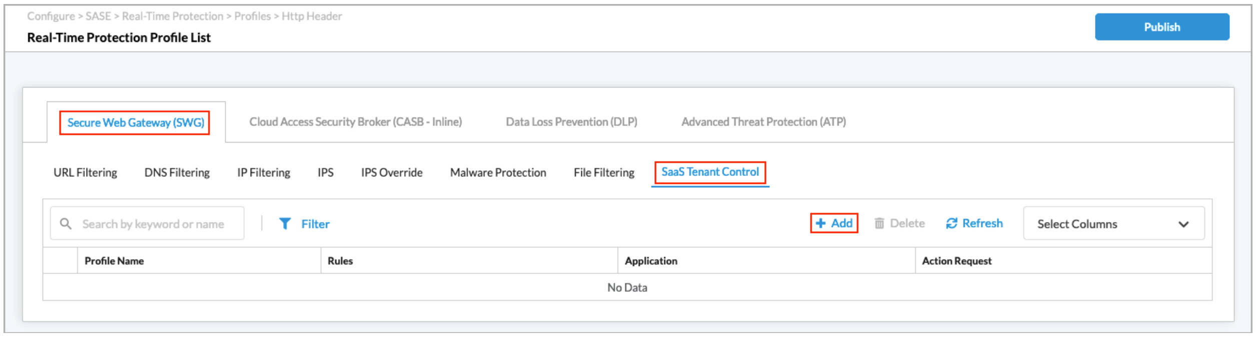
You can configure only one SaaS tenant control profile for each tenant.

To configure SaaS a tenant control profile:

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.

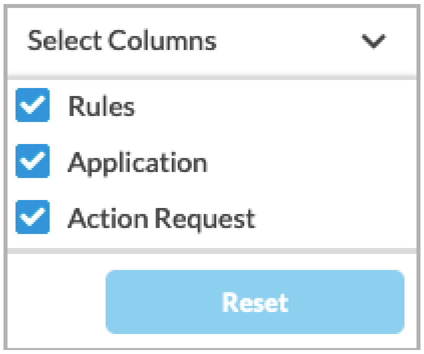


The following screen displays.


Configure > SASE > Real-Time Protection > Profiles > Http Header
Real-Time Protection Profile List
Publish
Secure Web Gateway (SWG)
Cloud Access Security Broker (CASB - Inline)
Data Loss Prevention (DLP)
Advanced Threat Protection (ATP)
URL Filtering
DNS Filtering
IP Filtering
IPS
IPS Override
Malware Protection
File Filtering
SaaS Tenant Control
Search by keyword or name
Filter
Add
Delete
Refresh
Select Columns

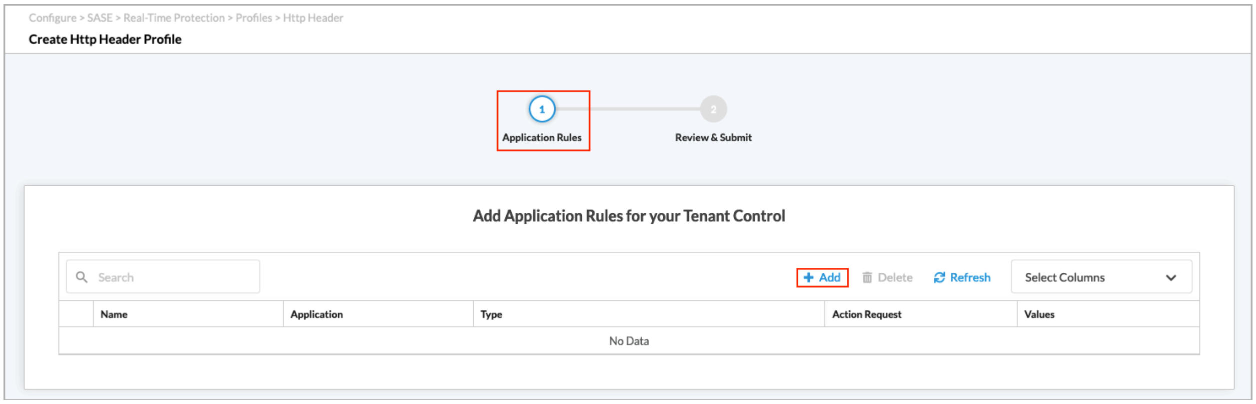
Profile Name	Rules	Application	Action Request
	No Data		

2. Select the Secure Web Gateway (SWG) tab, and then select the SaaS Tenant Control tab.
3. To customize which columns display, click Select Columns, and then click the columns to select or deselect the one you want to display. Click Reset to return to the default column display settings.



☑ Rules
☑ Application
☑ Action Request

4. Click the ✚ Add icon to create a profile. The Create HTTP Header Profile screen displays.

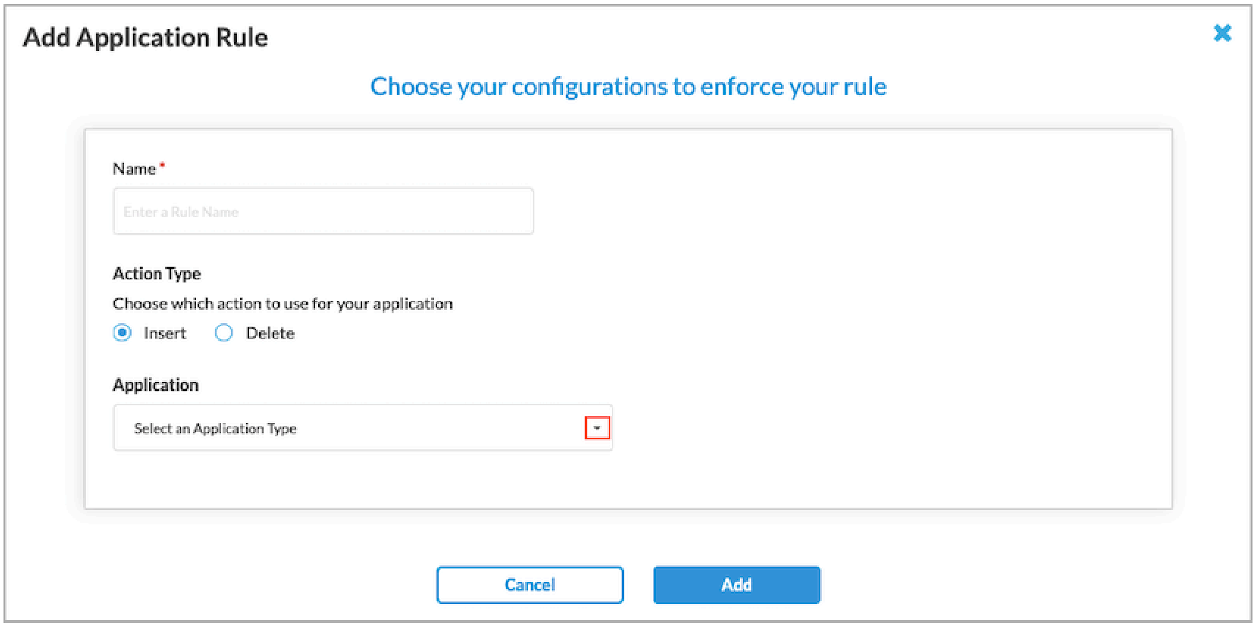


Create Http Header Profile

Add Application Rules for your Tenant Control

	Name	Application	Type	Action Request	Values
	No Data				

5. In Step 1, Application Rules, click the ✚ Add icon. In the Add Application Rule screen, enter information for the following fields.



Add Application Rule

Choose your configurations to enforce your rule

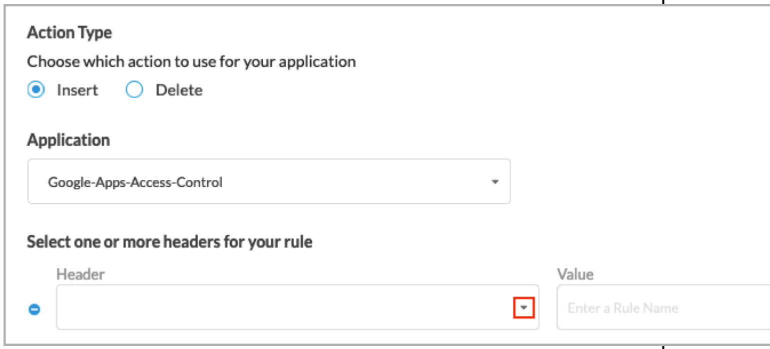
Name *

Action Type

Choose which action to use for your application

● Insert ○ Delete

Application

Field	Description
Name	Enter a name for the application rule.
Action Type	Click to choose the action to use for the application: ◦ Delete ◦ Insert
Application	Select an application. For applications that have predefined headers, the following fields display. Enter information for the following fields.  Action Type Choose which action to use for your application ● Insert ○ Delete Application Google-Apps-Access-Control Select one or more headers for your rule Header Value Enter a Rule Name ◦ Header—Select a header for the application. ◦ Value—Enter a value. You can enter multiple values, each one separated by a comma. To delete the header, click Delete Existing.

6. Click Add.

Supported Software Information

Releases 11.4.1 and later support all content described in this article.

Additional Information

Configure SASE TLS Decryption