Configure HTTP Header Profiles

For supported software information, click here.

Some SaaS application that are generally available to users are also available in an enterprise-specific version. However, users may not be able to easily distinguish between the two versions, and so may access the generally available version of a SaaS application instead of the enterprise version and may accidentally transmit sensitive information outside the enterprise. To allow users to access the enterprise version of a SaaS application while at the same time blocking access to the generally available version of that application, you can create HTTP header profiles to manage the information in the HTTP headers. Many SaaS applications control access to the application based on information contained in the HTTP headers.

You can use predefined header insertion profiles to manage access to common SaaS applications, including Dropbox, Google, Microsoft 365, and YouTube. You can also create custom header insertion profiles for other SaaS applications. In both the predefined and custom profiles, you create rules for matching the headers and values in HTTP requests. Then, you associate the profile with an SSL decryption profile, which inspects the SSL certificate transmitted as part of an HTTP or HTTPS session.

This article describes how to configure HTTP header insertion and modification profiles to control access to SaaS applications.

Configure an HTTP Header Profile

To configure a profile to use for inserting or modifying the information in an HTTP header:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliance in the left menu bar.
   c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Services > Next-Gen Firewall > Security > Profiles > HTTP Header Profile in the left menu bar.
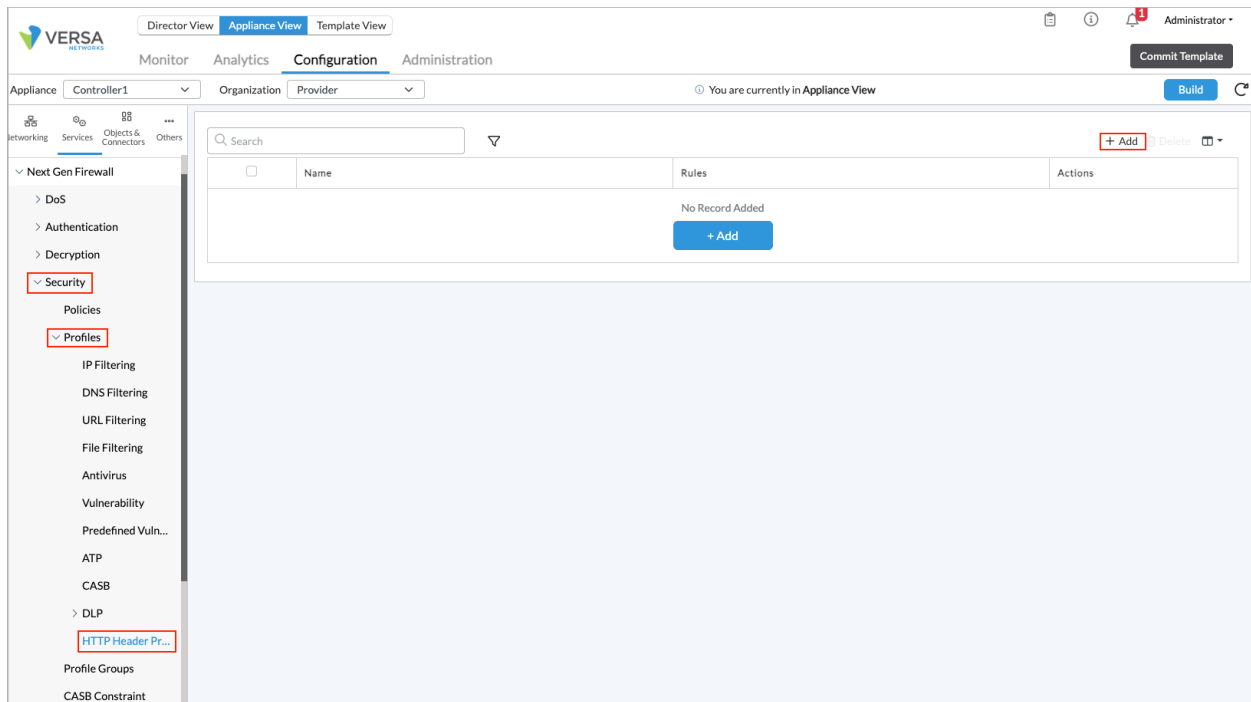
5. Click the ✛ Add icon. The HTTP Header Profile popup window displays. In the Name field, enter a name for the header profile.

6. In the Rules section, click the ✛ Add icon. In the Add Rule popup window, enter information for the following fields.

   For Releases 22.1.3 and later:

Add Rule   ✕

Name *

[_____]

Type	Domain Patterns * ⇕	⤢
● Insert ○ Delete	[Enter value or Select option ⌄] [+]	
Application	No Records to Display	
[Custom ⌄]		

Headers

Name * ⇕	Value *	Delete Existing	⤢
[Enter value or Select option ⌄]	[_____]	☑	[+]
No Records to Display			

Queries

Name * ⇕	Value *	Delete Existing	⤢
[_____]	[_____]	☑	[+]
No Records to Display			

[OK]   [Cancel]

For Releases 22.1.2 and earlier:

Add Rule

Name *

_____

Type

○ Insert   ● Delete

Application

Custom

Domain Patterns *

Enter value or Select option   ▽   [+]

No Records to Display

Headers

Name *	Value *	Delete Existing	
Enter value or Select option ▽		☑	[+]
No Records to Display			

[OK]   [Cancel]

Field	Description
Name	Enter a name for the rule.

Type	Select the rule type. Note that the you can configure queries for Release 22.1.3 and later.
	
	◦ Insert—Click to insert the list of headers into the Headers field of the HTTP request and to insert the list of queries in the Queries field of the HTTP request.
	
	  ▪ If you click Delete Existing for a line, the existing value is deleted and the new value is inserted into the HTTP request header or query.
	
	  ▪ If you do not click Delete Existing for a line, the existing value remains in the HTTP request header or query and the new header value is added to the HTTP request header or query.
	
	◦ Delete—Click to delete the list of headers in the Headers field and the list of queries in the Queries field in the HTTP request.
	
	  ▪ If you enter a value in the Value field, only that value is deleted from the HTTP request header or query.
	
	  ▪ If you do not enter a value in the Value field, the entire header or query is deleted from the HTTP request header.

Application	Select the application to which to apply the rule: ◦ Custom—Configure a custom header insertion rule to use for an SaaS application that is not predefined. ◦ Dropbox Network Control ◦ Google Apps Access Control ◦ Microsoft Office 365 Block Consumer Account ◦ Microsoft Office 365 Tenant Restrictions ◦ YouTube Safe Search
Domain Patterns	Select or enter the hostname to match the domain pattern of HTTP header profile rule, and then click the Add icon.

Headers	Enter the information to use to modify the HTTP request header, and then click the ➕ Add icon: ◦ Delete Existing—Click to delete the existing header value. For more information, see the [Type field](#), above. ◦ Name—Select or enter a name for the header. ◦ Value—Enter a value for the header. To enter multiple values, separate them with commas.
Queries	Enter information to use to modify the HTTP query, and then click ➕ Add icon: ◦ Delete Existing—Click to delete the existing query value. For more information, see the [Type field](#), above. ◦ Name—Select or enter a name for the query. ◦ Value—Enter a value for the query. To enter multiple values, separate them with commas.

7. Click OK.

Apply an HTTP Header Profile

To apply an HTTP header profile, you select it when you configure an SSL decryption profile. For more information, see [Configure HTTP/HTTPS Proxy](#).

Supported Software Information

Releases 22.1.3 and later support all content described in this article.

Additional Information

[Configure HTTP/HTTPS Proxy](#)