Configure Security Profile Groups
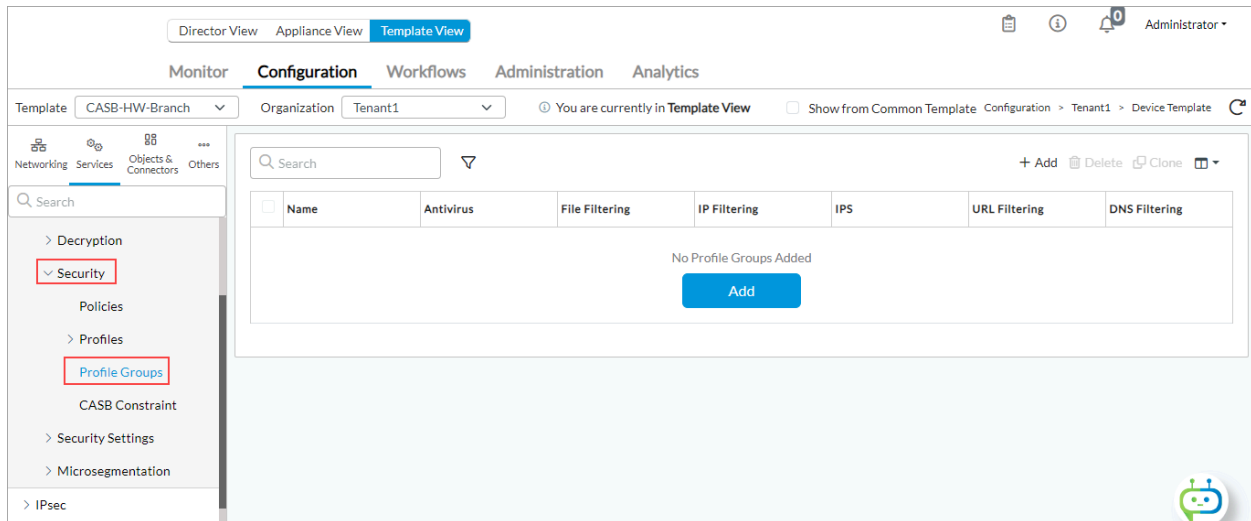
For supported software information, click here.

You create a security profile group to combine two or more security profiles—such as file filtering, URL filtering, antivirus, and IP filtering profiles—into a single group, which you can then associate with one or more security rules. A security profile group can either contain only predefined security profiles, or it can contain both predefined and user-defined security profiles. Note that a rule in a security profile group can contain either individual profiles or profile groups, but not both.

To create a security profile group:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template from the dashboard. The view changes to Appliance view.
2. Or, in Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliance in the left menu bar.
   c. Select the device from the main pane. The view changes to Appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Services > Next-Gen Firewall > Security > Profile Groups in the left menu bar.

5. Click the **+** Add icon. In the Add Profile Groups popup window, enter information for the following fields.

Field	Description
Name (Required)	Enter a name for the security profile group.
Description	Enter a text description for the security profile group.
IP Filtering	Select a predefined or custom IP filtering profile to include in the profile group. For more information, see Configure IP Filtering.
File Filtering	Select a predefined or custom file filtering profile to include in the profile group. For more information, see Configure File Filtering.
Antivirus	Select a predefined or custom antivirus profile to include in the profile group. For more information, see Configure Antivirus.
URL Filtering	Select a predefined or custom URL filtering profile to include in the profile group. For more information, see Configure URL Filtering.
Vulnerability	Select a predefined or custom vulnerability profile to include in the profile group. For more information, see Configure Intrusion Detection and Prevention.
DNS Filtering	Select a predefined or custom DNS filtering profile to include in the profile group. For more information, see Configure DNS Filtering.
Predefined Vulnerability Profile Override	If you select a predefined profile in the Vulnerability field, the vulnerability profile performs the default action associated with the profile. To use a predefined vulnerability but to take an action other than the default action, select a profile to use to override the default action. For example, by default, the Versa Recommended Profile rejects all packets that are suspected to be malicious. If you want to use this profile but do not want to reject all packets, you can choose an override profile that logs occurrences of the malicious activity so that you can investigate the activity later. To override the default action of a predefined vulnerability profile, select an existing override profile

or click + Add New to add a profile override.

Add Profile Groups

Name *

Description

IP Filtering

--Select-- ⌄

File Filtering

--Select--

Antivirus

--Select-- ⌄

URL Filtering

--Select--

Vulnerability

Versa Recommended Profile ⌄

DNS Filtering

--Select--

Predefined Vulnerability Profile Override

--Select--

--Select--
+ Add New

OK

The Create Predefined Vulnerability Profile Override
window displays. For more information, see& Create
Custom Vulnerability Profiles.

6. Click OK.

Supported Software Information

Releases 20.2.1 and later support all content described in this article.

Additional Information

[Configure Antivirus](#)
[Configure DNS Filtering](#)
[Configure File Filtering](#)
[Configure Intrusion Detection and Prevention](#)
[Configure IP Filtering](#)
[Configure NGFW](#)
[Configure URL Filtering](#)
[Configure Vulnerability Rules](#)