


Configure Schedule Objects

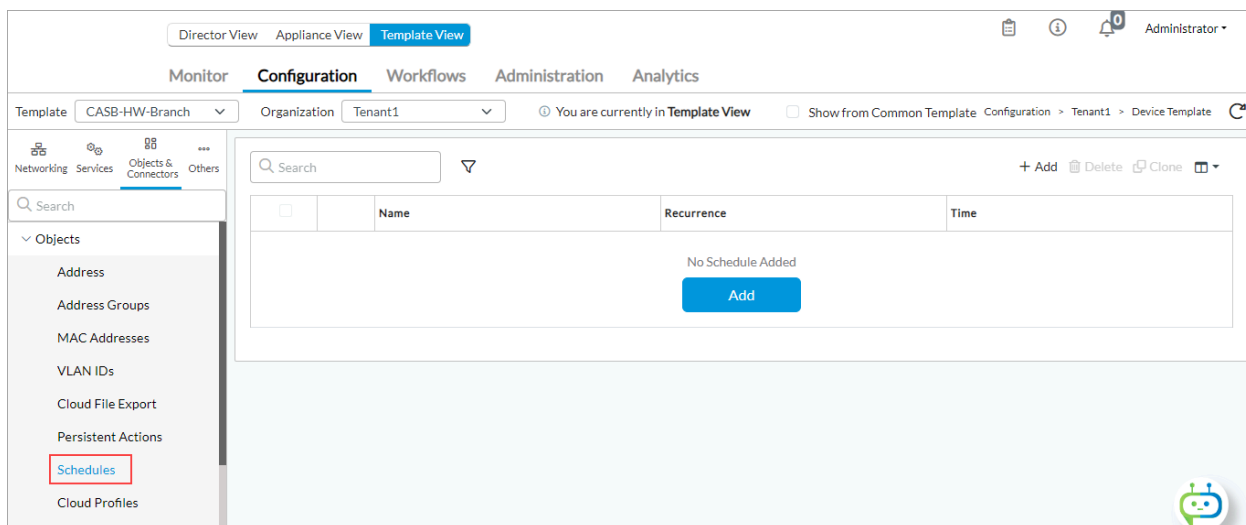
 For supported software information, click [here](#).


Security policy rules work at all dates and times. You can define a schedule to limit a security policy to specific times and then apply it to a policy. Versa Operating System™ (VOS™) schedule objects can match criteria based on time of day. For example, you can define a policy rule that is effective only during certain times of the day such as lunch hours or after standard working hours. You can specify schedule objects for a fixed date and time range or a recurring daily or weekly schedule.

Schedule objects that you configure for a tenant are applicable for that tenant only, and they are not visible to other tenant in the system.

Configure Schedule Objects

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Schedules in the left menu bar.



4. Click the  Add icon in the dashboard to add a new schedule. In the Add Schedule window, enter information for the following fields:

Add Schedule

Name *

Description

Tags

Recurrence

Non-Recurring

<




>

Start Date *	Start Time *	End Date *	End Time *	
yyyy/mm/dd	--Select--	yyyy/mm/dd	--Select--	<div>+</div>

No records added

OK

Cancel

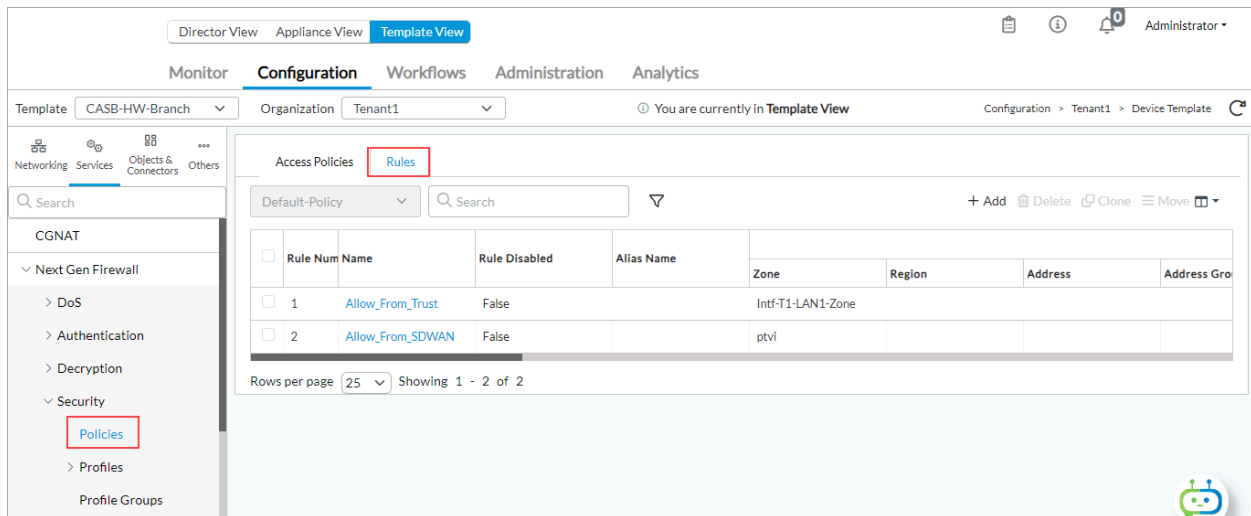
Field	Description
Name	Enter a name for the custom schedule object.
Description	Enter a text description for the custom schedule object.
Tags	Enter a keyword or phrase that allows you to filter the custom schedule object. This is useful when you have many objects and want to view those that are tagged with a particular keyword.
Recurrence	<p>Select the type of schedule:</p> <ul style="list-style-type: none"> Non-Recurring—Specify a start and end date and time. Click the  Add icon to add another row. Daily—Specify a start and end time in 24-hour format (HH:MM). Click the  Add icon to add another row. Weekly—Select a day of the week, and specify the start and end time in 24-hour format (HH:MM). Click the  Add icon to add another row.

5. Click OK.

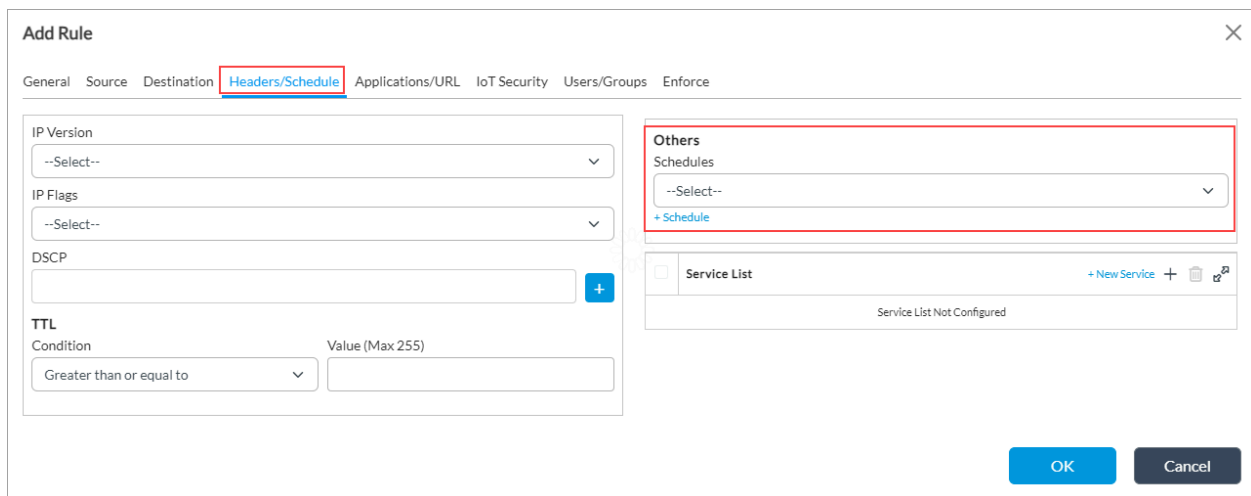
Apply a Schedule Object to an Access Policy

You can apply a schedule object to a security access policy to define a security policy. To define and configure a security access policy, see [Configure Security Access Policy Rules](#).

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Services > Next-Gen Firewall > Security > Policies in the left menu bar, and then select the Rules tab.



4. Select a security access policy rule. The Add Rule popup window displays.



5. Select the Headers/Schedule tab:
6. In the Others group of fields, in the Schedules field, select a schedule object to apply to the rule.
7. To add a schedule object, click +Schedule. The Add Service popup window displays. For more information about a service object, see [Configure Custom Service Objects](#).
8. Click OK.

Configuration Example

The following example shows how to deny traffic based on a schedule object and how to monitor the effects of the object.

To configure the schedule object:

1. In the Add Schedule popup window, add a schedule object. For more information, see [Configure Schedule](#)

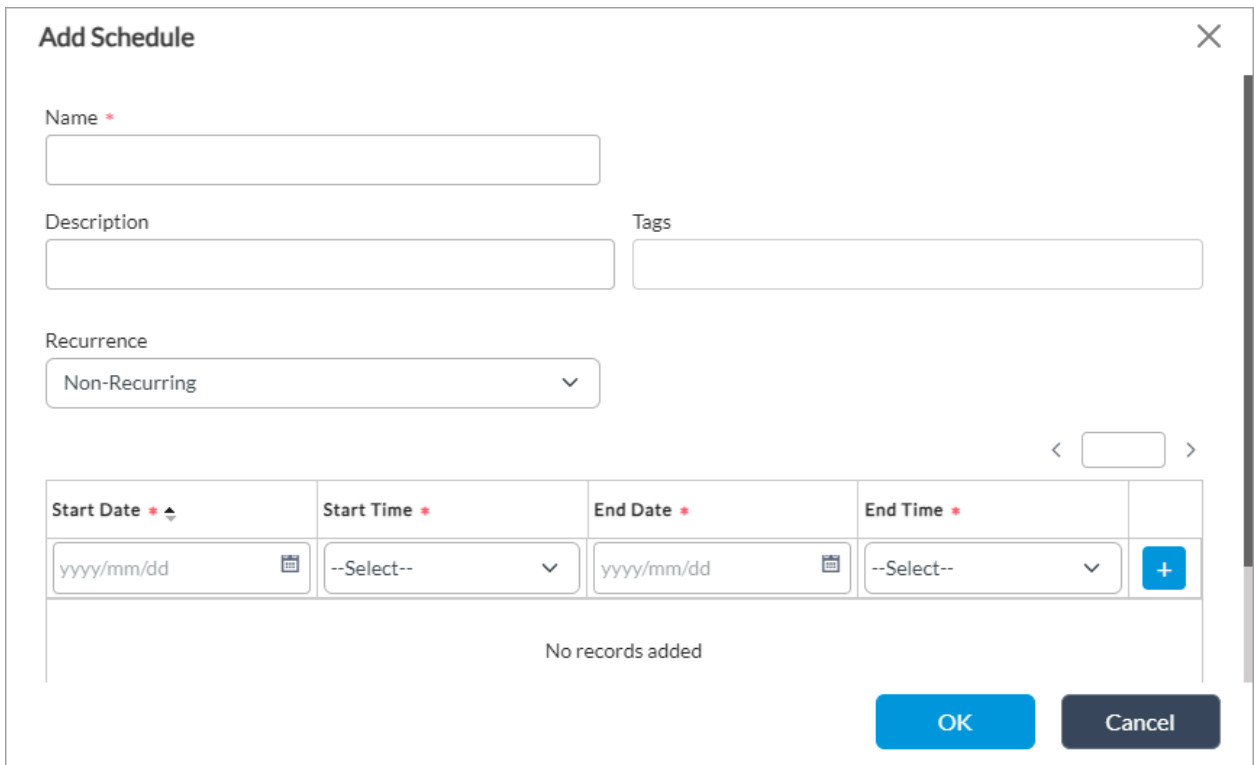
https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_Sched...

Updated: Wed, 23 Oct 2024 08:19:24 GMT

Copyright © 2024, Versa Networks, Inc.

[Objects](#), above.

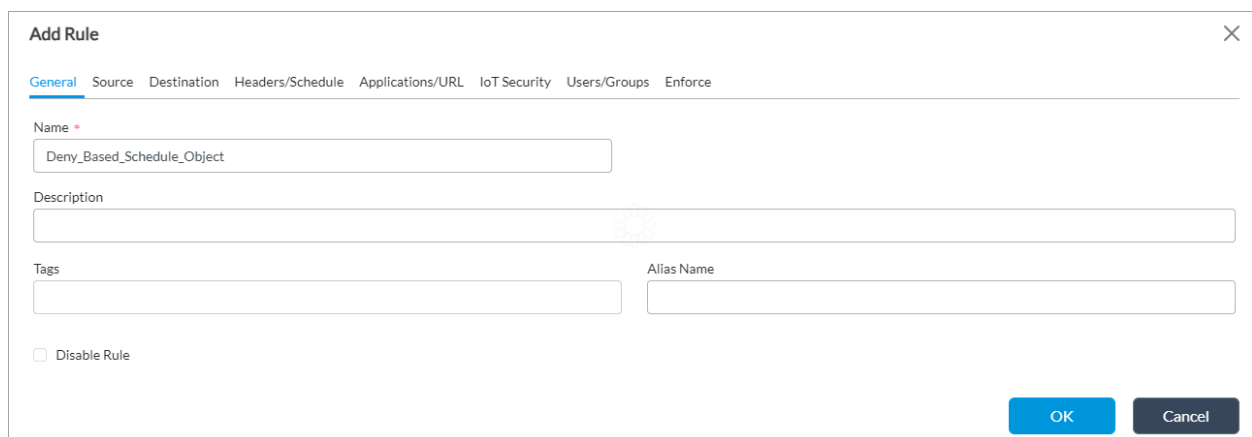
- a. Enter a name for the schedule object. In the example here, the name is `Schedule_Object_Daily`.
- b. Select the time frequency (recurrence) for running the schedule object. In this example, the recurrence is `Daily`.
- c. Enter the start and end times during which to apply the schedule object.
- d. Click OK.



The 'Add Schedule' dialog box contains the following fields and controls:

- Name ***: A text input field.
- Description**: A text input field.
- Tags**: A text input field.
- Recurrence**: A dropdown menu currently set to 'Non-Recurring'.
- Start Date ***: A date picker showing 'yyyy/mm/dd'.
- Start Time ***: A time picker showing '--Select--'.
- End Date ***: A date picker showing 'yyyy/mm/dd'.
- End Time ***: A time picker showing '--Select--'.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.
- Footer**: 'No records added' text in the center.

2. Create an access policy rule that includes the scheduled object. For more information, see [Apply a Schedule Object to an Access Policy](#).
 - a. In the General tab, enter a name for access policy rule. In our example, the name is `Deny_Based_Schedule_Object`.



The 'Add Rule' dialog box features a tabbed interface with the following elements:

- Tabs**: General (selected), Source, Destination, Headers/Schedule, Applications/URL, IoT Security, Users/Groups, Enforce.
- Name ***: A text input field containing 'Deny_Based_Schedule_Object'.
- Description**: A text input field.
- Tags**: A text input field.
- Alias Name**: A text input field.
- Disable Rule**: A checkbox.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.

- b. In the Headers/Schedule tab, select the schedule you created in Step 1, here, Schedule_Object_Daily.

The screenshot shows the 'Add Rule' dialog box with the 'Headers/Schedule' tab selected. The 'General' tab is also visible. The 'IP Version' dropdown is set to '--Select--'. The 'IP Flags' dropdown is set to '--Select--'. The 'DSCP' field is empty. The 'TTL' section has a 'Condition' dropdown set to 'Greater than or equal to' and a 'Value (Max 255)' field. The 'Others' section has a 'Schedules' dropdown set to 'Schedule_Object_Daily'. The 'Service List' section is empty with a '+ New Service' button. The 'OK' and 'Cancel' buttons are at the bottom right.

- c. In the Application/URL tab, select an application (for example, Facebook) from the Application List.

The screenshot shows the 'Add Rule' dialog box with the 'Applications/URL' tab selected. The 'General' tab is also visible. The 'Application List' section has a dropdown menu open showing 'Advertising', 'Application Filter', 'Predefined Filters', 'Advertising', 'Applications', and 'ADVERTISING_COM'. The 'URL Category List' section is empty with a '+ New URL Category' button. The 'OK' and 'Cancel' buttons are at the bottom right.

- d. In the Enforce tab, select Deny under Actions and click OK. This action creates a rule that denies users from accessing Facebook during the time specified in the scheduled object.

Add Rule [X]

General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups **Enforce**

Actions | Log

Actions
☐ Allow ☒ Deny ☐ Reject ☐ Apply Security Profile

Set-Type
☒ Public ☐ Private ☐ None

Synced Flow: --Select-- Session Timeout (secs): [] ☐ Send TCP Keep Alive at Session Timeout

☒ Profiles ☐ Profile Groups

☐ IP Filtering --Select--
 ☐ Antivirus --Select--
 ☐ File Filtering --Select--
☐ Vulnerability --Select--
 ☐ URL Filtering --Select--
 ☐ DNS Filtering --Select--
☐ Predefined Vulnerability Profile Override --Select--
 ☐ CASB Profile --Select--
 ☐ DLP Profile --Select--
☐ ATP Profile --Select--

OK Cancel

To see how the schedule object associated with a policy affects the traffic flow, you monitor the policy. For more information, see [Monitor Device Services](#).

To monitor the policy:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select a provider organization in the left menu bar.
4. Select the Services tab in the horizontal menu bar.
5. Select NGFW > Policies. The NGFW policy statistics display, and you can view the access policy rule you created under Rule Name.

Director View
Appliance View
Template View

Administrator

Monitor
Analytics
Configuration
Administration

Organization: Tenant1
You are currently in Appliance View
Build
OUT OF SYNC

Summary
Devices
Cloud Workload

Total Appliances: 9
SDLAN-Branch1

SDLAN-Branch1 | 1 Hacker Way Menlo Park, CA, USA 94025
Mgmt. Address: 10.0.0.12
System Bridge Address:

Reachable | SYNC: OUT_OF_SYNC Up since: Wed Apr 17 14:22:52 2024

Summary
Services
Networking
System
Tools

Configuration
Shell
Config Status*
Upgrade
Subscription

SDWAN
NGFW
CGNAT
SDLAN
IPsec
Sessions
SCI
Secure Access
APM

Decryption
DLP
DNS Filtering
DoS Policies
File Filtering
IP Filtering
Microsegmentation Policies
Microsegmentation Statistics
Persistent Action
Policies
Se
<
>

Default-policy

Search
Clear

Rule Name	Hit Count	Forward Packet Count	Forward Byte Count	Reverse Packet Count	Reverse Byte Count	Hit Rate	Inactive Session Count
ALLOW-ALL	15345	25422	6324702	18911	22699889	0	15344
QUIC_DROP	30	30	38340	2	2456	0	30
DNS_Rule	177665	178280	12010057	177594	40204262	0	177665
CASB_Policy	202329	3258137	576936721	3758682	3146510147	0	202325
allow_all	270	38195	2773147	127601	183291801	0	270

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure Stateful Firewall](#)

[Monitor Device Services](#)