

Configure Antivirus



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

You enable unified threat management (UTM) capabilities on Versa Operating System™ (VOS™) devices by configuring threat profiles in security access policy rules. VOS devices support the following threat profiles:

- Antivirus
- Vulnerability (IDS/IPS)

This article discusses how to configure antivirus threat profiles.

The VOS antivirus software scans files received or transmitted in live traffic. When the last byte of a file is transmitted, the antivirus software extracts the file and scans it for viruses.

You can scan the following types of traffic:

- Web traffic sent using FTP and HTTP
- Email traffic sent use IMAP, MAPI, POP3, and SMTP

The following table lists the types of files that the antivirus software can scan.

7zip	cpp	html	mp3	ppt	tif
android	dll	jar	mpeg	ppptx	torrent
appleplist	doc	jpeg	msi	psd	txt
avi	docx	lha	msoffice	rar	wav
bat	dwg	lnk	pdf	reg	wmf
bmp	elf	lzh	pgp	rm	wmv
c	exe	mach_o	php	rtf	xls
cab	flv	mdb	pif	sh	xlsx
class	gif	mdi	pl	tar	xml

coff	gzip	mov	png	targa	zip
------	------	-----	-----	-------	-----

To enable VOS devices to scan files for viruses, you must configure at least one antivirus profile and then associate it with a rule in an NGFW policy. The antivirus profile is then applied to all traffic that matches the policy rule. The VOS software provides predefined antivirus profiles, and you can configure custom antivirus profiles. For predefined antivirus profiles, the maximum scannable file size is 512 KB. For custom antivirus profiles, you can configure the maximum scannable file size.

To scan files larger than 512 KB, you must create a custom antivirus profile and associate it with a storage profile created for that purpose. The files can be stored, or buffered, on either hard disk or RAM disk (if supported by the hardware) before they are processed, to provide for faster processing times.

When the antivirus software extracts a file from a live flow and buffers it, the file data is forwarded to the destination except for the last data packet, and then the antivirus software scans the file for viruses based on the configured antivirus profile. If the file contains a virus, the action in the antivirus profile is enforced on the packet or session. If no virus is detected, the last data packet held by the VOS device is forwarded to the destination. After the antivirus scans the file, the file is automatically deleted from the storage space.

The antivirus software follows these rules when scanning extracted files for viruses:

- If the file type matches a file type in the antivirus profile, the entire file is extracted and buffered on the VOS device.
- If the file type does not match any configured file type, the file extraction is aborted.
- If the file is less than 512 KB, the file is buffered in memory.
- If the file is more than 512 KB, or if not enough RAM is available, the file is stored on the hard disk or RAM disk depending on the configured storage profile.
- If the storage is full and a file cannot be saved on the storage device, the file extraction is aborted. In such a scenario, the action specified for the antivirus profile for disk full is considered.

Configure Storage for Antivirus Files

For custom antivirus profiles that scan files larger than 512 KB, you must configure storage for the files. The files are then buffered on either hard disk or RAM disk before they are processed, to provide for faster processing times. Note that if you want to scan files larger than 512 KB, you must configure a custom antivirus profile, because predefined antivirus profiles scan files only up to 512 KB.

You can configure the antivirus file storage at the system and organization level:

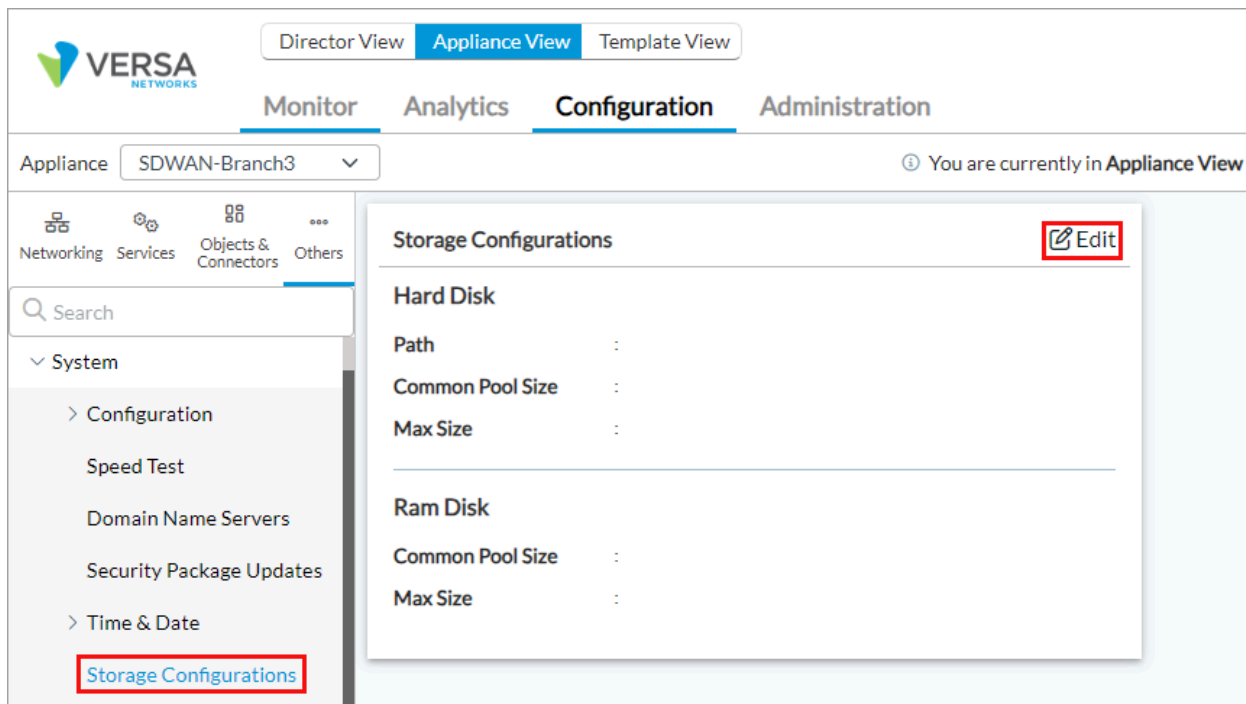
- **System level**—You configure the hard disk and RAM disk storage for the entire VOS device. All storage profiles that you create at the organization level are allocated hard disk and RAM disk from this single pool of hard disk and RAM disk on an as-needed basis. With system-level storage, if one organization is consuming a large amount of hard disk or RAM disk, storage space for other organizations might be limited or unavailable.
- **Organization level**—You configure storage profiles for the hard disk and RAM disk storage for each organization. The amount of storage space that you allocate for an organization can be used only by that organization. This

means that if the antivirus software is scanning large amounts of traffic such that the organization might temporarily need more hard disk or RAM disk storage, no additional storage is available to the organization even though the VOS device might have storage space that is not being used by other organizations.

The total amount of hard disk and RAM disk configured for all organizations on a VOS device must be less than or equal to the total hard disk and RAM disk space configured for the VOS devices at the system level.

Configure System-Level File Storage

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 Others > System > Storage Configurations in the left menu bar.



4. Click the  Edit icon. The Edit Storage Configuration Setting popup window displays.

Edit Storage Configuration Setting

×

Hard Disk

Ram Disk

Path

/tmp

Common Pool Size

512

Max Size

4096

OK

Cancel

5. Select the Hard Disk tab and enter information for the following fields.

Field	Description
Path	Enter the path to the file storage directory. <i>Default: /tmp</i>
Common Pool Size	Enter the size of the common memory pool available for all tenants, in megabytes. The space for the common pool is taken from the maximum disk size.
Maximum Size	Enter the maximum size of the hard disk, in megabytes. <i>Range: 256 through 131072 MB</i> <i>Default: 256 MB</i>

6. Select the RAM Disk tab and enter information for the following fields.

Edit Storage Configuration Setting

Hard Disk

Ram Disk

Common Pool Size

Max Size

OK

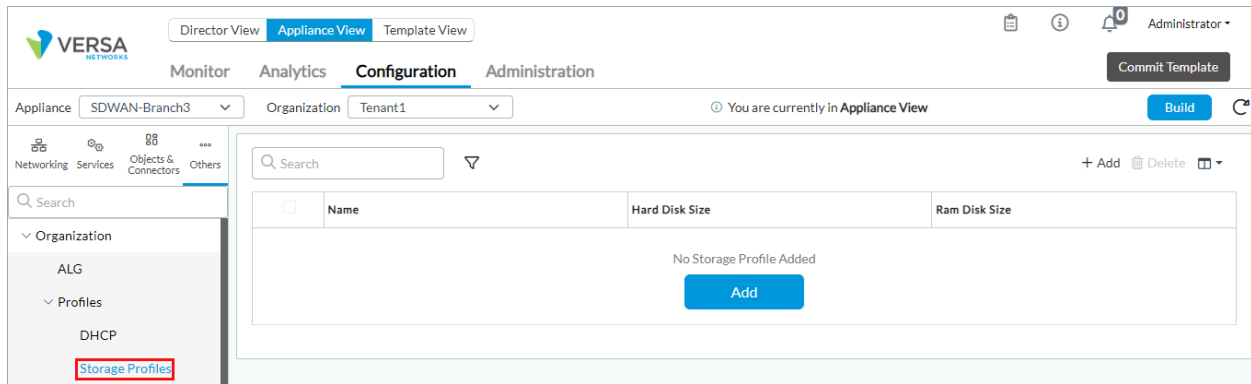
Cancel


Field	Description
Common Pool Size	Enter the size of the common RAM disk memory pool for all tenants, in megabytes.
Maximum Size	Enter the maximum size of the RAM disk, in megabytes. <i>Range:</i> 0 through 32768 MB <i>Default:</i> 0 MB

7. Click OK.

Configure Organization-Level Storage

- 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 Others > Organization > Profiles > Storage Profiles in the left menu bar.



- Click the  Add icon. In the Add Storage Profile popup window, enter information for the following fields.

Add Storage Profile ✕

Name *

Description

Hard Disk Size

Ram Disk Size

OK

Cancel

Field	Description
Name	Enter a name for the storage profile.
Description	Enter a text description for the storage profile.
Hard Disk Size	Enter the size of the guaranteed hard disk, in megabytes. <i>Range:</i> 256 through 131072 MB <i>Default:</i> 256 MB
RAM Disk Size	Enter the size of the guaranteed RAM disk, in megabytes. <i>Range:</i> 0 through 32768 MB <i>Default:</i> 0

5. Click OK.

View Predefined Antivirus Profiles

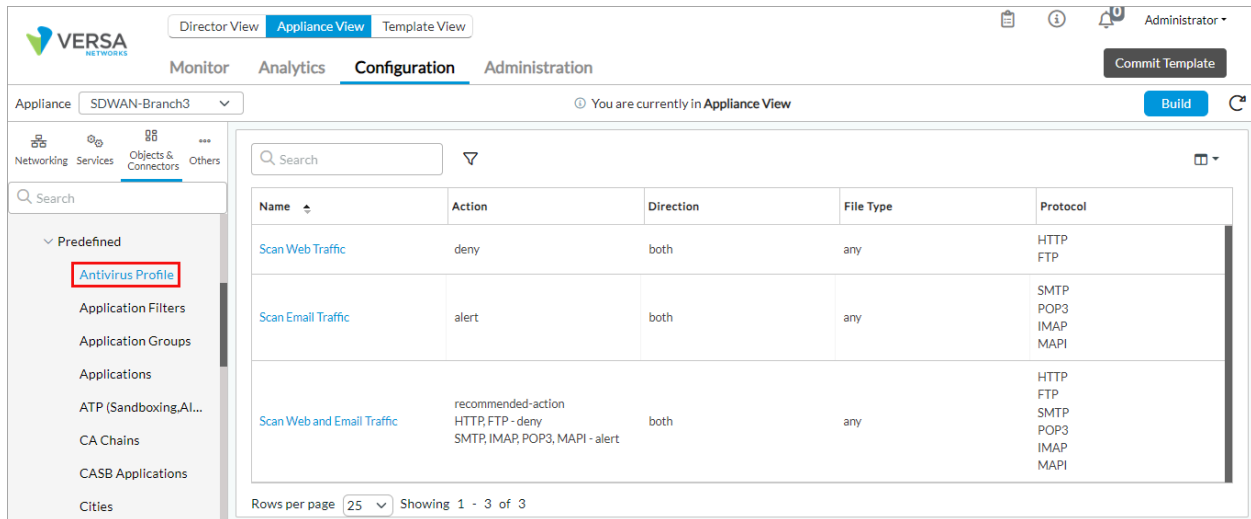
The antivirus software provides the following predefined antivirus profiles:

- Scan web traffic
- Scan email traffic
- Scan web and email traffic

Note that for antivirus profiles, Versa does not provide a predefined profile called Versa Recommended profile.

To view predefined antivirus profiles:

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 and Connectors > Objects > Predefined > Antivirus Profile in the left menu bar. The table in the main pane lists the predefined antivirus profiles. The following table describes each profile.



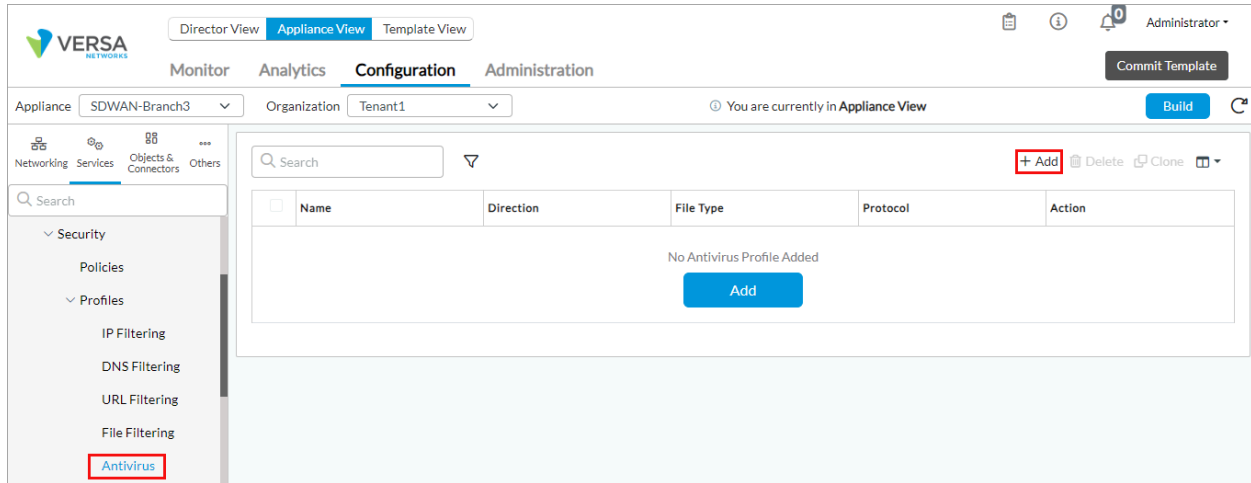
Field	Description
Scan Web Traffic	Scan all web traffic sent using the HTTP and FTP protocols. The Action column shows the "deny" action, which is the default action for web traffic
Scan Email Traffic	Scan all email traffic sent using the IMAP, MAPI, POP3, and SMTP protocols. The Action column shows the "alert" action, which is the default action for email traffic.
Scan Web and Email Traffic	Scan all web and email traffic. The Action column shows the "recommended-action" action, which takes the default actions listed above for web traffic (deny) and email traffic (alert).

Note that if you want to scan files larger than 512 KB, you must configure a custom antivirus profile, because predefined antivirus profiles scan files only up to 512 KB. If you want to use a predefined profile and scan files larger than 512 KB, because you cannot associate a storage profile with a predefined antivirus profile, you must create a custom profile that clones the configuration of predefined profile with then storage profile associated with it and then use that customer profile in your security rule.

Configure Custom Antivirus Profiles

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 Services > Next-Gen Firewall > Security > Profiles > Antivirus in the left menu bar, and select an organization in the horizontal menu bar.





4. Click the  Add icon. In the Add Antivirus Profile window, enter information for the following fields.

The 'Add Antivirus Profile' window contains the following fields and controls:

- Name ***: A text input field.
- Description**: A text input field.
- Tags**: A text input field.
- Direction**: A dropdown menu with 'Both' selected.
- LEF Profile**: A dropdown menu with '--Select--' selected.
- Default Profile**: A checkbox.
- Action**: A dropdown menu with 'Deny' selected.
- Storage Profile**: A dropdown menu with '--Select--' selected.
- Action on Disk Full**: A dropdown menu with 'Deny' selected.
- File Type ***: A section with a table header and a row labeled 'File Type Not Configured'.
- Protocol ***: A section with a table header and a row labeled 'Protocol Not Configured'.
- OK** and **Cancel** buttons at the bottom right.

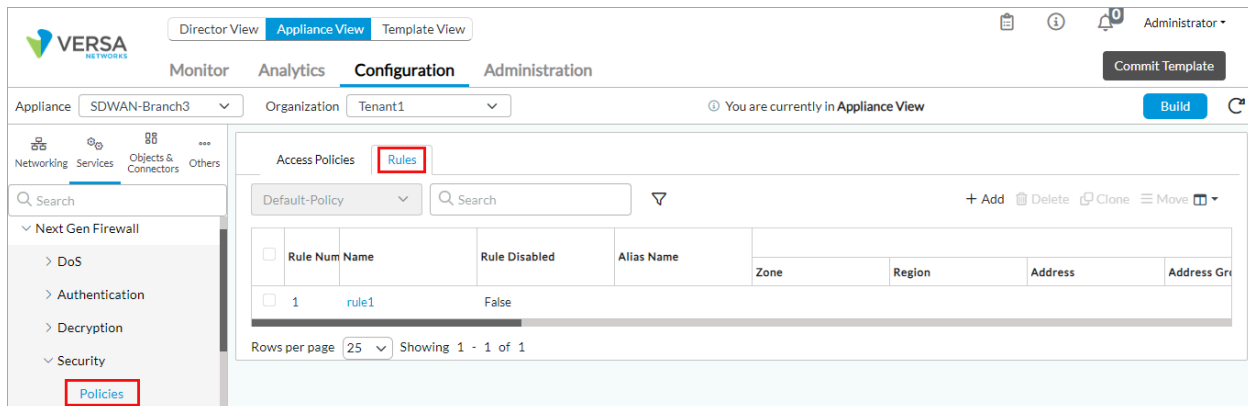
Field	Description
Name	Enter a name for the antivirus profile.
Description	Enter a text description of the antivirus profile.
Direction	<p>Select the direction of the traffic on which to perform the antivirus scan:</p> <ul style="list-style-type: none"> ◦ Both (download and upload) ◦ Download ◦ Upload
LEF Profile	<p>Select a LEF profile to use to register logs for the antivirus profile. For information about configuring a LEF profile, see Configure Log Export Functionality. For information associating a LEF profile to the configuration of a feature or service, see Apply Log Export Functionality.</p>
Action	<p>Select an enforcement action to take when traffic matches the profile:</p> <ul style="list-style-type: none"> ◦ Alert—Allow the file to pass and, if a LEF profile is configured, log the action. ◦ Allow—Allow the file to pass without logging the action. ◦ Deny— Do not allow the file to pass and, if a LEF profile is configured, log the action ◦ Reject—Reset the connection to the server and client and, if a LEF profile is configured, log the action.
Storage Profile	Select the storage profile to use to determine where to store files that are being scanned for viruses.
Action on Disk Full	<p>Select an action to take if the file storage area is full:</p> <ul style="list-style-type: none"> ◦ Alert—Allow the file to pass and, if a LEF profile is configured, log the action. ◦ Allow—Allow the file to pass without logging the action. ◦ Deny—Do not allow the file to pass and, if a LEF profile is configured, log the action ◦ Reject—Reset the connection to the server and

	client and, if a LEF profile is configured, log the action.
File Type	Select the type of file to scan for viruses. Click the  Add icon, and in the subsequent table row, select the file type from the drop-down list. To scan all file types, select the file type "any".
Protocol	Select the type protocol whose files you want to scan for viruses. Click the  Add icon, and in the subsequent table row, select the protocol from the drop-down list..

- Click OK.

Apply an Antivirus Profile to an Access Policy

- 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.



- Click the Rules tab to view the security policy access rules.
- Select an access policy rule. The Edit Rule popup window displays.
- Select the Enforce tab, and enter information for the following fields.

Edit Rule - rule1

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

AV-Office

View Antivirus Profile

☐ 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

Field	Description
Actions (Group of Fields)	Click Apply Security Profile.
Profiles	Click to select a single antivirus profile
<ul style="list-style-type: none"> Antivirus 	Click and then select the antivirus profile to use for the access policy rule. The list displays the predefined and custom antivirus profiles.
Profile Groups	Click to select a profile group.
<ul style="list-style-type: none"> Antivirus 	Click and then select the antivirus profile to use for the access policy rule. The list displays the predefined and custom antivirus profiles. For more information, see Configure Security Profile Groups .

7. Click OK.

Monitor Antivirus Profile Statistics

You monitor antivirus profiles to view the antivirus scan reports when a profile is used. For more information, see [Monitor Device Services](#).

To monitor antivirus profiles:

1. Select the Administration tab in the top menu bar.
 - a. Select Appliances in the left menu bar.
 - b. 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 the Provider Organization > Services tab.
4. Select NGFW > Antivirus, and then select Predefined Profile or User Defined Profile from the drop-down list. The antivirus profile statistics display.

The screenshot shows the Versa Networks Appliance View interface. The top navigation bar includes 'Director View', 'Appliance View' (selected), and 'Template View'. The left sidebar shows 'Monitor', 'Analytics', 'Configuration', and 'Administration'. The main panel displays the 'Antivirus' section for 'SDWAN-Branch3'. The 'Antivirus' tab is selected, showing a table of file types and their scan/block counts.

File Type	Scan Count	Block Count
Unknown	0	0
avi	0	0
bat	0	0
bmp	0	0
cab	0	0
c	0	0

The following screenshots provide examples of the antivirus statistics that are displayed.

When you select Predefined Profile from the left drop-down, the Scan Web and Email Traffic profile from the middle drop-down, and Predefined Protocol from the right drop-down, the following information displays. Similar information displays when you select the Scan Web Traffic or Scan Email Traffic profile.

SDWAN

NGFW

CGNAT

SDLAN

IPsec

Sessions

SCI

Secure Access

APM

Antivirus

ATP

Authentication Policies

CASB

Cloud File Export

Decryption

DLP

DNS Filtering

DoS Policies

File Filtering

IP Filtering

Microsegmentati

<

>

Predefined Profile

Scan Web Traffic

Predefined Protocol

Search

↺

📄

⌵

Clear

Protocol	Flows Blocked	Flows Allowed	Number of Context Switch
http	0	905	0
ftp	0	0	0
smtp	0	0	0
imap	0	0	0
pop3	0	0	0
mapi	0	0	0

Field	Description
Protocol	List of predefined protocols scanned for antivirus.
Flows Blocked	Number of protocols flows blocked by the antivirus software.
Flows Allowed	Number of protocols flows allowed by the antivirus software.

When you select Predefined Profile from the left drop-down, the Scan Web and Email Traffic profile from the middle drop-down, and Predefined File Type from the right drop-down, the following information displays. Similar information displays when you select the Scan Web Traffic or Scan Email Traffic profile.

SDWAN

NGFW

CGNAT

SDLAN

IPsec

Sessions

SCI

Secure Access

APM

Antivirus

ATP

Authentication Policies

CASB

Cloud File Export

Decryption

DLP

DNS Filtering

DoS Policies

File Filtering

IP Filtering

Microsegmentati

<

>

Predefined Profile

Scan Web Traffic

Predefined File Type

Search

🔄

📄

🔍

Clear

File Type	Scan Count	Block Count
Unknown	707	0
avi	0	0
bat	0	0
bmp	0	0
cab	0	0
c	0	0

Field	Description
File Type	Type of file scanned by the antivirus software.
Scan Count	Total number of antivirus scans for the file type.
Block Count	Total number of files blocked by the antivirus software.

When you select Predefined Profile from the left drop-down, the Scan Web and Email Traffic profile from the middle drop-down, and Predefined Statistics from the right drop-down, the following information displays. Similar information displays when you select the Scan Web Traffic or Scan Email Traffic profile.

SDWAN

NGFW

CGNAT

SDLAN

IPsec

Sessions

SCI

Secure Access

APM

Antivirus

ATP

Authentication Policies

CASB

Cloud File Export

Decryption

DLP

DNS Filtering

DoS Policies

File Filtering

IP Filtering

Microsegmentation

<

>

Predefined Profile

Scan Web Traffic

Predefined Statistics

Search

🔍

📄

📉

Clear

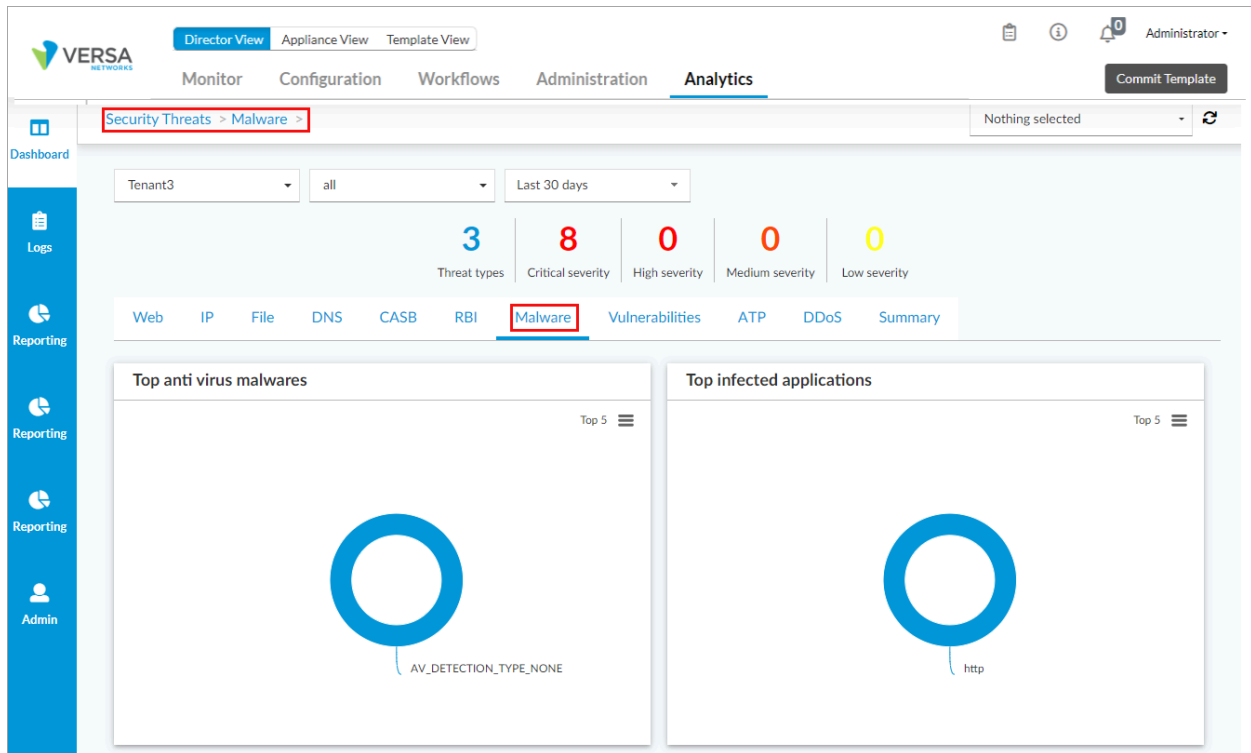
Profile Name	Profile Hit Count	Action Allow Count	Action Alert Count	Action Reject Count	Action Block Count	Action On Disk Full	File In Queue Count	EOF Received Count	Flow Bypass Count	Filetype Mismatch
Scan Web Traffic	905	905	0	0	0	0	0	905	0	0

Field	Description
Name	<p>Name of the statistics record:</p> <ul style="list-style-type: none"> Action alert count—Number of flows for which an alert was sent. Action allow count—Number of flows allowed. Action block count—Number of flows blocked. Action on disk full count—Number of actions performed when the disk was full. Action reject count—Number of flows rejected. EOF received count—Number of end-of-file (EOF) markers received. File in queue count—Number of files in the queue. Filetype mismatch count—Number of flows with a file type mismatch. Flow bypass count—Number of bypassed flows. Profile hit count—Number of times an antivirus profile matched.
Value	Statistics value for the record.

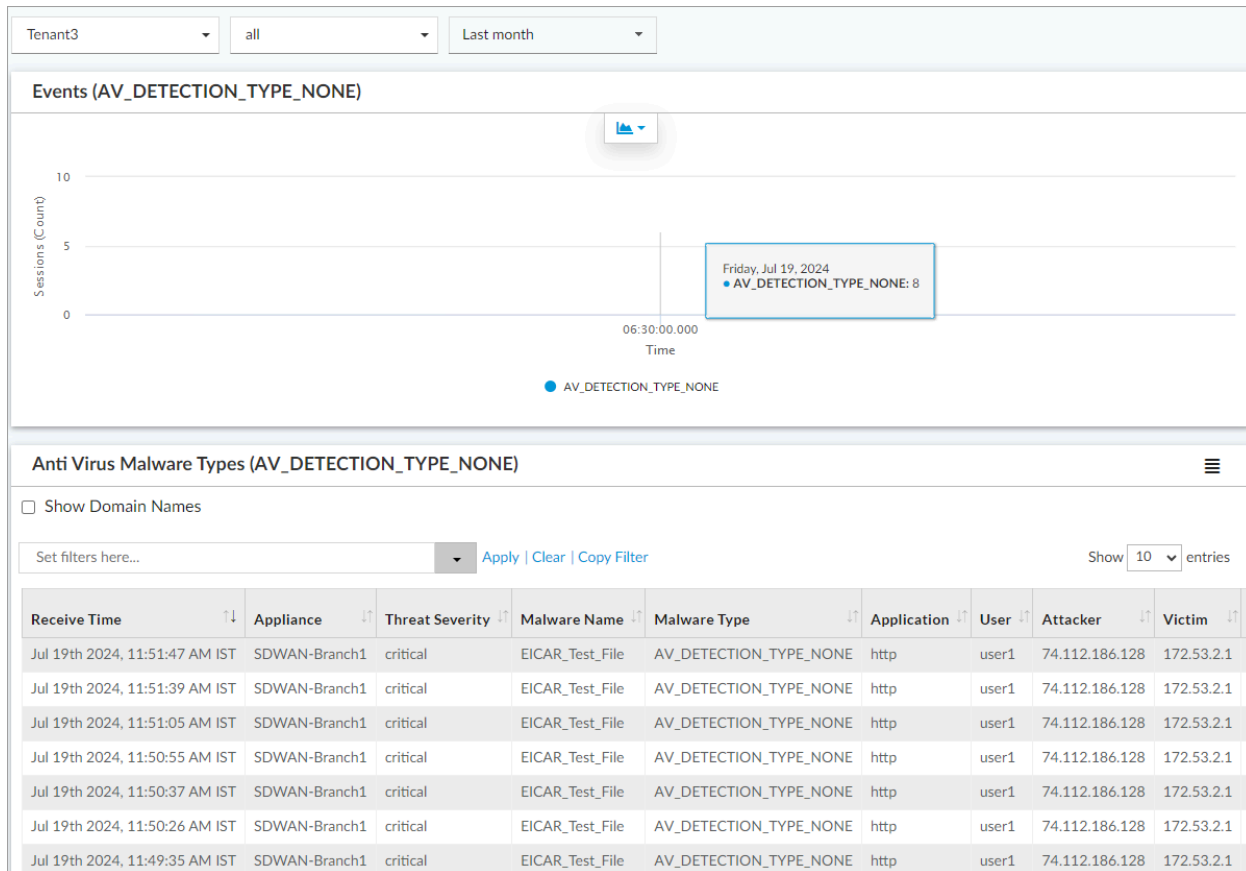
Display Antivirus Threat Logs

To monitor the antivirus threats that are occurring in your network, view malware threat monitoring reports:

1. In Director view, select the Analytics tab from the top menu bar. The view changes to Analytics view.
2. Select Home > Security > Threats in the left menu bar to view the security threats dashboard. For more information, see [Security Dashboards](#).
3. Select the Malware tab to display information about top antivirus malware and infected applications.



4. Drill down to display detailed antivirus logs matching the drill key.



5. Select Home > Logs > Threat Detection in the left menu bar to view logs. Select the Antivirus tab in the main pane.

VERSA NETWORKS Director View Appliance View Template View

Monitor Configuration Workflows Administration **Analytics** Commit Template

Threat Detection Logs > Anti Virus > Nothing selected

Tenant3 all Last month

Anti Virus IDP IPGuard DDoS RBI VFP ATP

Anti virus log

☐ Show Domain Names

Set filters here... Apply | Clear | Copy Filter Show 10 entries

Receive Time	Appliance	Threat Severity	Malware Name	Malware Type	Application	User	Attacker	Victim
Jul 19th 2024, 11:51:47 AM IST	SDWAN-Branch1	critical	EICAR_Test_File	AV_DETECTION_TYPE_NONE	http	user1	74.112.186.128	172.53.2.1
Jul 19th 2024, 11:51:39 AM IST	SDWAN-Branch1	critical	EICAR_Test_File	AV_DETECTION_TYPE_NONE	http	user1	74.112.186.128	172.53.2.1
Jul 19th 2024, 11:51:05 AM IST	SDWAN-Branch1	critical	EICAR_Test_File	AV_DETECTION_TYPE_NONE	http	user1	74.112.186.128	172.53.2.1
Jul 19th 2024, 11:50:55 AM IST	SDWAN-Branch1	critical	EICAR_Test_File	AV_DETECTION_TYPE_NONE	http	user1	74.112.186.128	172.53.2.1

Troubleshoot Antivirus

To troubleshoot antivirus-based security issues, such as disk full, run the **show orgs org-services *tenant-name* security profiles av statistics** CLI command.

To view storage details such as RAM disk and hard disk allocation, run the **show orgs org-services *tenant-name* security profiles storage statistics** CLI command.

Supported Software Information

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

Additional Information

[Apply Log Export Functionality](#)

[Configure Intrusion Detection and Prevention](#)

[Configure Log Export Functionality](#)

[Configure Security Profile Groups](#)

[Configure NGFW](#)

[Monitor Device Services](#)

[Security Dashboard](#)