
Apply Log Export Functionality



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

By default, Versa Operating System™ (VOS™) devices do not export log information. To have a VOS device send logs to an Analytics cluster, syslog server, or Netflow collector so that these devices can perform data analysis and generate reports and data visualization, you configure a log export functionality (LEF) profile. Among other things, the LEF profiles specify the destinations for the logs. One or two destinations can be active at any time, and this is known as the active collector or collectors of the LEF profile. For information about configuring LEF profiles, see [Configure Log Export Functionality](#).

To export logs to the active collector or collectors specified in the LEF profile, you associate the LEF profile with the configuration of a feature or service. You can apply the LEF profile in one of the following ways:

- Associate the LEF profile with a feature or service.
- Associate the LEF profile with a traffic-monitoring policy rule.
- Associate the LEF profile with the logging control configuration.
- Assign a LEF profile to be the default.

The method you use depends on the type of logs you are exporting.

This article describes how to send various types of logs to the active collector specified in a LEF profile. For logs sent to Analytics clusters, this article describes how to access the Analytics dashboards and log screens that correspond to the feature or service sending the logs.

Configure VOS Devices To Export Logs

When you configure a feature or service and associate a LEF profile with the feature or service, the VOS device generates logs for the feature or service. Logs are generated in syslog format and include a label, called the syslog identifier, identifying the log type. Each feature or service has one or more associated syslog identifiers. For logs sent to Analytics clusters and Netflow collectors, LEF adds an IPFIX overhead.

When you associate a LEF profile with a traffic-monitoring policy rule, the VOS device generates syslog messages for selected types of traffic monitoring flows.

When you associate a LEF with the logging control configuration, the VOS device generates syslog messages globally for all traffic-monitoring flows.

Configuring a default LEF profile automatically sends logs of the following types to the active collector specified in the profile. The syslog identifier or identifiers corresponding to each log type are displayed in parentheses.

- Alarm logs (alarmLog), unless a separate LEF profile is designated as the default for alarms
- LTE summary logs (lteEventLog, lteStatsLog)
- MOS summary logs (sdwanPathMosLog)
- SD-WAN SLA metrics logging (sdwanB2BSlamLog)
- SD-WAN traffic-conditioning logs (sdwanPathCondLog)

For Releases 22.1.1 and later, you can select a LEF profile to use for alarm logs.

For a list of all syslog identifiers, see [Analytics Log Collector Log Types Overview](#).

You can set LEF monitoring controls on VOS devices, such as maximum number of source IP addresses to export. For more information, see [Configure Firewall and SD-WAN Usage Monitoring Controls](#).

Access Analytics Dashboards and Log Screens

For logs that are forwarded to Versa Analytics clusters, the log data and data derived from the logs are incorporated into cluster datastores. This data maps to two areas under the Analytics tab:

- Log screens—These screens are accessible when you select Dashboard (Home)  > Logs in the left menu bar.
- Analytics dashboards—These screens are accessible when you select Dashboard (Home)  > Dashboards in the left menu bar.

Data on Analytics dashboards and log screens reflects the current contents of cluster datastores. Data in datastores is automatically deleted when it passes its retention time. Logs received by an Analytics cluster are incorporated into datastores only when the cluster has not surpassed its daily or total log storage limit. For information about setting log storage limits and retention times, see [Versa Analytics Scaling Recommendations](#).

Configure Log Export for Features and Services

This section describes how to configure features and services so that they send logs to a Versa Analytics cluster, syslog server, or Netflow collector. For Analytics clusters, the log data is used to populate the Analytics dashboards and log

screens on the Analytics Dashboard (Home)  screen.

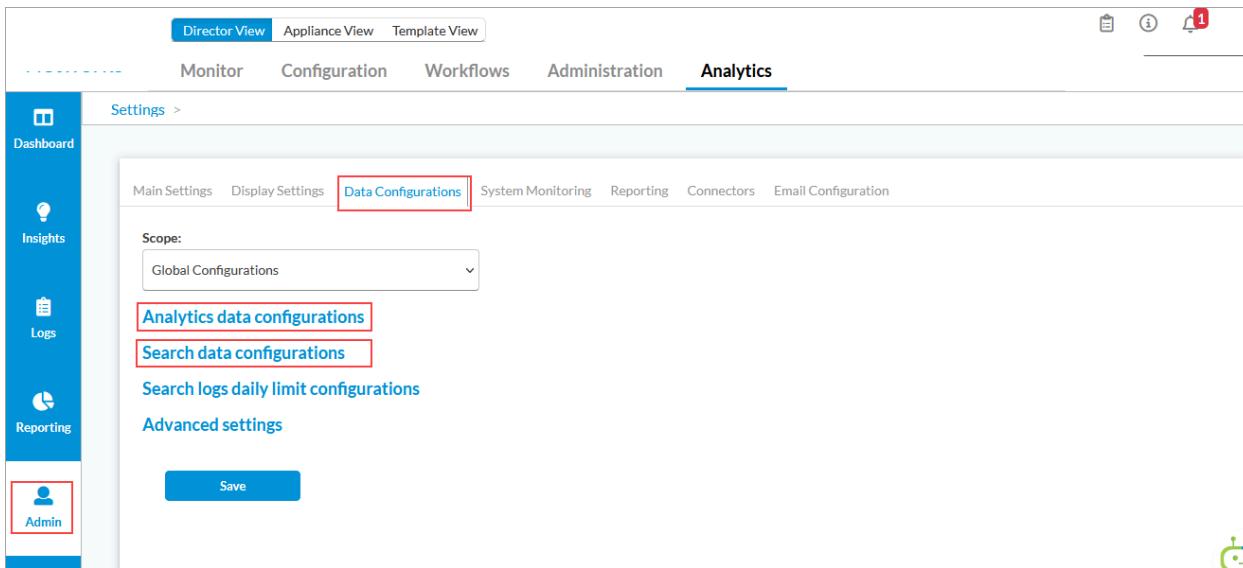
This section provides the GUI navigation instructions and field values for configuring only logs. In addition to configuring logs, you must also do the following:

- Configure the feature or service. Each section below provides links to the appropriate configuration article.
- Configure the LEF profiles on the VOS device. For more information, see [Configure Log Export Functionality](#).

- For logs sent to Analytics clusters, configure the Analytics cluster.

Each section below lists the following information for the types of logs discussed in the section:

- Syslog identifier—Name of the syslog identifier or identifiers included in the logs.
- Path to the configuration screen—(Applies to logs sent to Analytics clusters only.) Path to the Analytics Data Configurations or Search Data Configurations screen for the feature or service. This is the screen on which you configure log retention and Analytics data retention times. These screens are located under the Analytics tab, at Administration > Configuration > Settings > Data Configurations, as shown in the following figure.



Configure Alarm Logging

- Syslog identifier—alarmLog
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > Alarm Logs

To export alarms for an organization on a VOS device to an Analytics cluster, configure a default LEF profile for the organization. Alarm logs are automatically exported to the destination of the default LEF profile. For Releases 22.1.1 and later, you can designate a LEF profile to be used for alarms. If none is designated, then alarms are exported to the default LEF profile. For information about configuring a default LEF profile and designating a LEF profile for alarms, see [Configure a LEF Profile](#) in [Configure Log Export Functionality](#).

Alarm logs are maintained in Analytics clusters for correlation and diagnostics. Analytics clusters do not perform alarm management. Alarms can be streamed from Analytics nodes to Versa Director or third-party fault-monitoring systems for management and ticketing purposes.

For logs sent to Analytics clusters, to display Alarm logs, select the Analytics tab in the top menu bar and then select Logs > Alarms in the left menu bar.

Receive Time	Severity	Appliance	Alarm Type	Description	Class	Key
Oct 6th 2023, 10:34:02 AM +0530	warning	Bangalore-ECT-DC-Active	duplicate-ip	Duplicate IP detected 169.254.0.3 MAC-address 06:8fc3:eb:30:01 interface vni-0/3.100, destination 172.10.3.3. Packet dropped	new	VSNO
Oct 6th 2023, 10:34:02 AM +0530	warning	Bangalore-ECT-DC-Active	duplicate-ip	Duplicate IP detected 169.254.0.3 MAC-address 06:8fc3:eb:30:01 interface vni-0/3.100, destination 172.10.3.3. Packet dropped	new	VSNO
Oct 6th 2023, 10:34:02 AM +0530	warning	Bangalore-ECT-DC-Active	duplicate-ip	Duplicate IP detected 169.254.0.3 MAC-address 06:8fc3:eb:30:01 interface vni-0/3.100, destination 172.10.3.3. Packet dropped	new	VSNO
Oct 6th 2023, 10:34:01 AM +0530	warning	Bangalore-ECT-DC-Active	duplicate-ip	Duplicate IP detected 169.254.0.3 MAC-address 06:8fc3:eb:30:01 interface vni-0/3.100, destination 172.10.3.3. Duplicate demand	new	VSI

This article describes how to send various types of logs to the active collector specified in a LEF profile. For logs sent to Analytics clusters, this article describes how to access the Analytics dashboards and log screens that correspond to the feature or service sending the logs.

Configure ATP Logging

For Releases 22.1.4 and later.

- Syslog identifiers—[sandboxLog](#)
- Path to the configuration screen—Search Data Configurations > Security > ATP Logs

When you configure ATP on a VOS gateway device, the device reassembles files from incoming traffic to determine if the files are malicious. When required, the gateway checks file reputations with the cloud-based file reputation service, and submits files to the cloud-based file submission and sandbox service for analysis. Based on reputation and analysis, these services return a verdict for each file, which ATP uses to determine what action to take on the file. The gateway collects the verdicts and file status information into logs and forwards them to the destination of the LEF profile associated with the ATP configuration. To export ATP logs, ensure that a LEF profile is associated with the ATP profile used to configure ATP.

For a list of verdicts, see [ATP Logs](#).

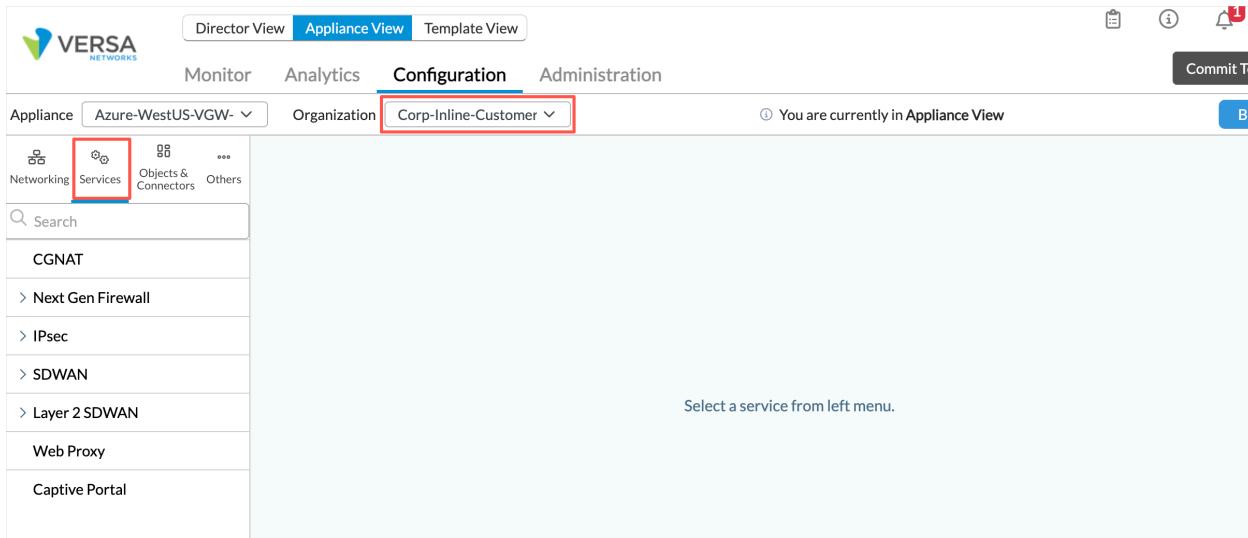
To configure ATP logging:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select the gateway in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services in the left menu bar. The following screen displays.

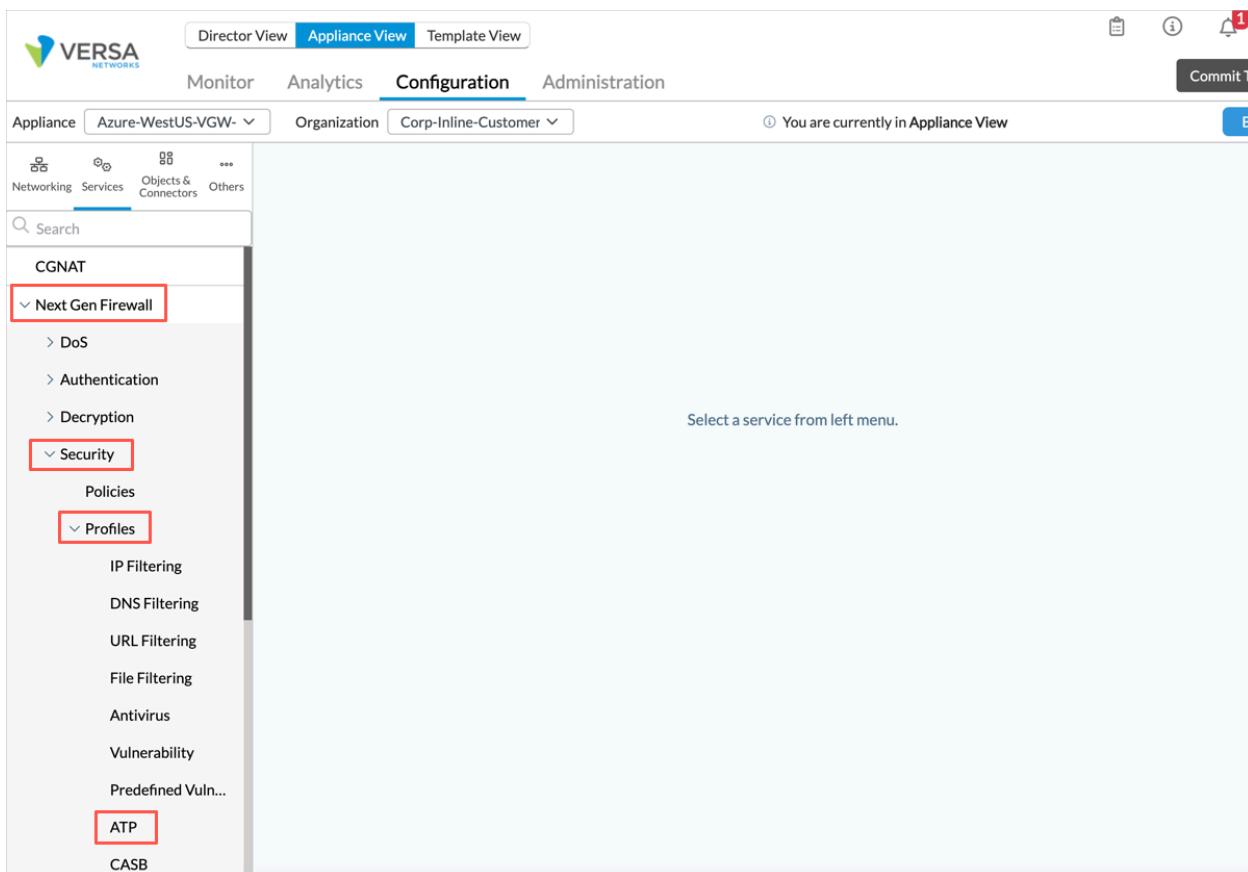
https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.



4. Select an organization in the Organization field in the top menu bar.



5. Select Next-Gen Firewall > Security > Profiles > ATP in the left menu bar.
6. In the main pane, select +Add. The Edit ATP Profile window displays.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

Edit ATP profile

[General](#) [Action Profiles](#) [ATP Rules](#) [Reputation Based Actions](#)

Name *

Description

Timeout Action

---Please Select---

Default Action *

---Please Select---

Lef Profile

---Please Select---

Default LEF Profile

OK Cancel

7. In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile.
8. Click OK.

To view ATP logs, select Analytics > Logs > Threat Detection, and then select the ATP tab.

Threat Detection Logs > ATP >

America/Los_Angeles

Corp-Inline-Customer-1 all Last day

Anti Virus IDP IPGuard DDoS RBI VFP **ATP**

ATP Logs (ALS Powered)

Show Domain Names

Set filters here... [Apply](#) | [Clear](#) | [Copy Filter](#)

Show 10 entries

Receive Time	Report	Appliance	Application	User	Action	Verdict	Profile	File Name	File Type	File Size (B)
May 13th 2024, 1:06:21 PM PDT		Bangalore-New-DC-Active	http	Unknown	allow	SandBoxDynamicAnalysisFileIsUnknown	sb		html	1.83 K
May 13th 2024, 1:06:20 PM PDT		Bangalore-New-DC-Active	http	Unknown	allow	SandBoxDynamicAnalysisFileIsUnknown	sb		html	1.57 K
May 13th 2024, 1:06:16 PM PDT		Bangalore-New-DC-Active	http	Unknown	allow	SandBoxDynamicAnalysisFileIsUnknown	sb	Case_119455	html	327
May 13th 2024, 1:06:15 PM PDT		Bangalore-New-DC-Active	http	Unknown	allow	SandBoxDynamicAnalysisFileIsUnknown	sb		html	7.64 K
May 13th 2024, 1:06:12 PM PDT		Bangalore-New-DC-Active	http	Unknown	allow	SandBoxMultiAVFilesClean	sb		html	1.83 K
May 13th 2024, 1:06:04 PM PDT		Bangalore-New-DC-Active	http	Unknown	allow	SandBoxStaticAnalysisFileIsClean	sb		html	1.83 K
May 13th 2024, 1:06:03 PM PDT		Bangalore-New-DC-Active	http	Unknown	allow	SandBoxMultiAVFilesClean	sb		html	1.57 K
May 13th 2024, 1:06:02 PM PDT		Bangalore-New-DC-Active	http	Unknown	allow	SandBoxAIMLAnalysisFileIsUnknown	sb		html	7.64 K
May 13th 2024, 1:06:02 PM PDT		Bangalore-New-DC-Active	http	Unknown	allow	SandBoxStaticAnalysisFileIsClean	sb		html	7.64 K
May 13th 2024, 1:06:02 PM PDT		Bangalore-New-DC-Active	http	Unknown	allow	SandBoxMultiAVFilesClean	sb		html	7.64 K

Showing 1 to 10 of 27,662 entries

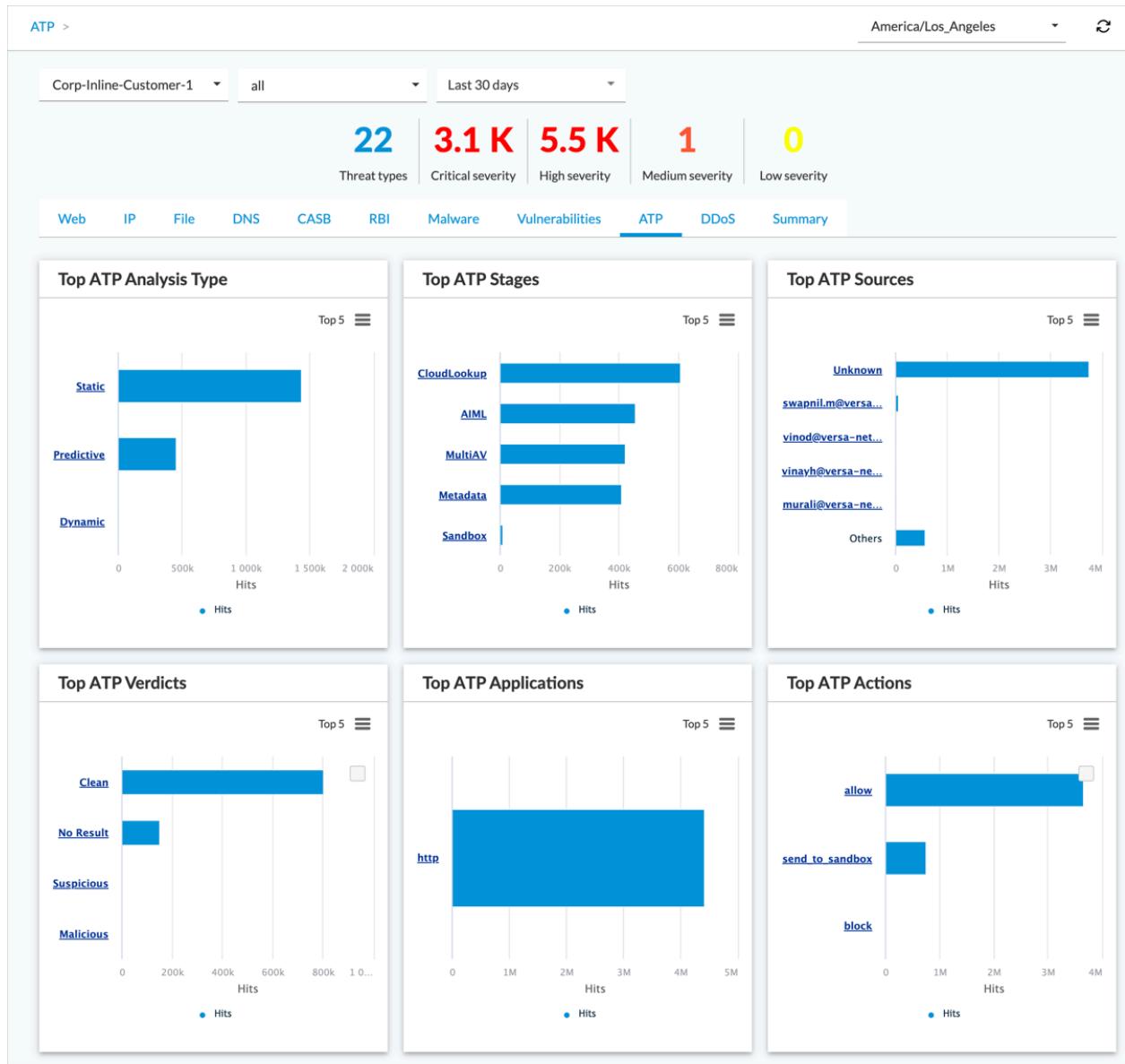
Previous [1](#) [2](#) [3](#) [4](#) [5](#) ... [2767](#) Next

To view ATP dashboards, select Analytics > Dashboards > Security > Threats, and then select the ATP tab.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.



Configure CGNAT Logging

- Syslog identifier—[cgnatLog](#)
- Path to the configuration screen—Search Data Configurations > CGNAT Logs

To export CGNAT logs, enable CGNAT logging per flow by associating a LEF profile with a CGNAT rule. For information about configuring CGNAT, see [Configure CGNAT](#).

To export CGNAT logs:

- In Director view:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

- a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To have the menu display tenant organizations, double-click the provider organization.
 - d. 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 Services > CGNAT in the left menu bar.
 4. Select the Rules tab in the horizontal menu bar. The following screen displays.

Name	Precedence	NAT Mode	Source IP	Destination IP	Source Pool	Destination Pool	LEF Profile
DIA-Rule-Provider-OR...		napt-44			DIA-Pool-BR-WAN		
RFC_1918_NoTranslate	100		10.0.0/8 172.16.0.0/12 192.168.0.0/16	10.0.0/8 172.16.0.0/12 192.168.0.0/16			
Speed-Test-BR-WAN		napt-44			Pool-BR-WAN		
Speed-Test-BR-WAN-R...		napt-44			Pool-BR-WAN-RAS		

5. Click the Add icon, or click an existing rule name. In the Add/Edit CGNAT Rule popup window, select the Action tab.

Add CGNAT Rule

General Match **Action**

Disable Translation

NAT Mode *

Source Pool

Destination Pool

LEF Profile Default Profile

Endpoint Independent Mapping Endpoint Independent Filter Address Pooling Paired

OK **Cancel**

6. In the LEF Profile field, select a LEF profile to use for logging, or click Default Profile to use the default LEF profile.
7. Click OK.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

For logs sent to Analytics clusters, to display CGNAT logs, select the Analytics tab in the top menu bar and then select Logs > CGNAT in the left menu bar, and select the Logs tab in the horizontal menu bar.

The screenshot shows the Director View interface with the Analytics tab selected. In the left sidebar, the Logs icon is highlighted. The main content area displays the 'CGNAT log' table. The table has columns for Receive Time, Appliance, Event, Source Address, Destination Address, Post NAT Source Address, Post NAT Destination Address, Source Port, and Destination Port. A filter bar at the top of the table allows setting filters, applying them, or copying the current filter. The table shows 0 entries.

Configure Digital Experience Monitoring Logging

For Releases 22.1.3 and later.

- Path to configuration screen—
 - Analytics > Administration > Settings > Data Configurations > Search Data Configurations > Digital Monitoring Experience User Data
 - Analytics > Administration > Settings > Data Configurations > Search Data Configurations > Secure Access Application Experience Metrics
 - Analytics > Administration > Settings > Data Configurations > Search Data Configurations > Secure Access User Connectivity Log
 - Analytics > Administration > Settings > Data Configurations > Search Data Configurations > Secure Access User Experience Metrics

Versa SASE clients collect digital experience monitoring (DEM) data on end-user devices and forward the data to their currently connected secure access gateway. The gateway assembles DEM data from all its clients into DEM logs and forwards them to the destination of its associated LEF profile. To export DEM logs, associate LEF profiles with all secure access gateways that receive DEM data from SASE clients. For information about configuring DEM, see [Configure Digital Experience Monitoring](#).

Note that you can export DEM logs only to Analytics nodes. You cannot export them to third-party logging systems, because the logs are in a proprietary format that may not be compatible with the third-party systems.

To associate a LEF profile with a secure access gateway:

1. In Director view, select Appliance View. The Select Appliance popup window displays.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

2. Click the secure access gateway. The view changes to appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Services > Secure Access > Gateway > General in the left menu bar. The following screen displays.

The screenshot shows the Versa Networks Director View interface. The top navigation bar includes tabs for Director View, Appliance View (which is selected), and Template View. Below the tabs are icons for Monitor, Analytics, Configuration (selected), and Administration. A status message indicates "You are currently in Appliance View". On the right side, there are buttons for Commit Template, Build, and a status indicator showing "OUT OF SYNC". The left sidebar has a tree structure: Appliance > Bangalore-ECT-DC-Ac > Organization > Corp-Inline-Provider > Secure Access > General. The "General" tab is selected. The main pane displays the "General" configuration settings, which include fields for URI, Service Type, Authentication, Authenticator Profile, LEF Profile, Default LEF Profile, Device Authentication Profile, Query MDM, MDM Profile, Trusted Network Detection, Prelogon Device Auth Profile, and Authentication Order. An "Edit" button is located in the top right corner of this pane, with a red box drawn around it.

5. In the General pane, click the Edit icon. The Add Services popup window displays.

Add Services

URI *

Service Type

Authenticator Profile

Authentication

Device Authentication Profile

Prelogin Device Auth Profile

Query MDM

Authentication Order

No Records to Display

LEF Profile

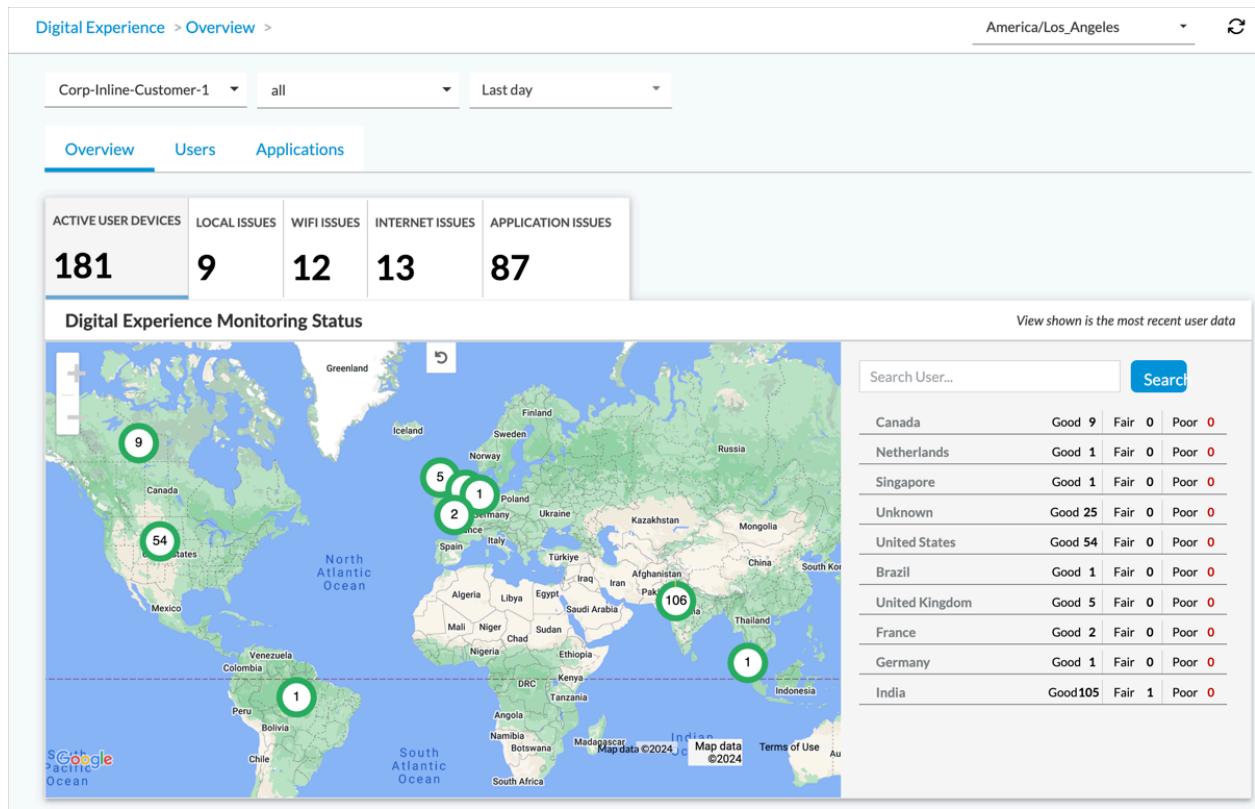
Default LEF Profile

Trusted Network Detection

OK Cancel

6. Select a LEF profile in the LEF Profile drop-down menu, or click Default LEF Profile to use the default. The LEF profile destination must be a Versa Analytics node or an ADC service on a Versa Controller node that relays the logs to a Versa Analytics node.
7. Click OK.

To display digital experience monitoring dashboards, select the Analytics tab in the top menu bar, and then select Dashboard > Secure Access > Digital Experience in the left menu bar. For information about the digital experience dashboard, see [View Digital Experience Monitoring Dashboards](#).



Configure DHCP Logging

- Syslog identifiers—[dhcpRequestLog](#), [dhcpResourceLog](#)
- Path to the configuration screen—Search Data Configurations > DHCP Logs

To export DHCP Global V4 and DHCP Global V6 information, select a LEF profile when you configure DHCP. For information about configuring DHCP, see [Configure DHCP](#).

To export DHCP logs to an Analytics cluster, syslog server, or Netflow collector:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Networking > DHCP > Global. The following screen displays.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

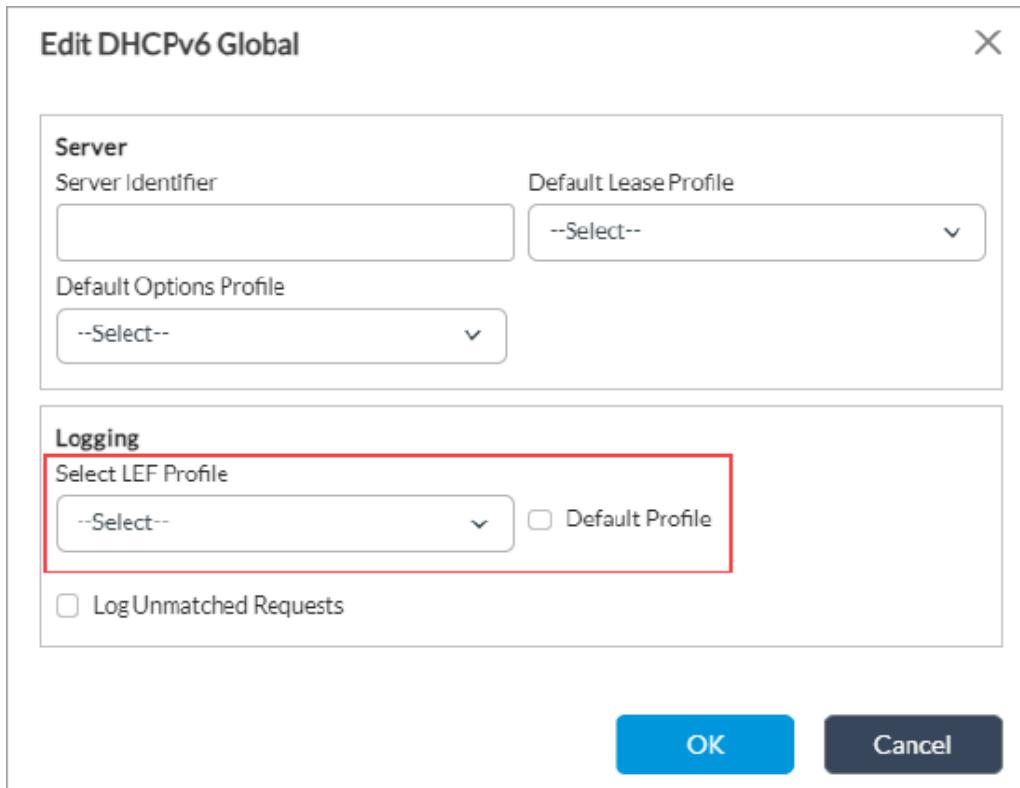
Copyright © 2024, Versa Networks, Inc.

4. To send DHCP V4 logs to the active collector for a LEF profile:

- In the main pane, click the Edit icon in the DHCP Global V4 area. The Edit DHCP v4 Global screen displays.

- Select a LEF profile, or click Default Profile to use the default LEF profile.
- Click OK.

5. To send DHCP V6 logs to the active collector of a LEF profile, select the  Edit icon in the DHCP Global V6 area, select a LEF profile or click Default Profile.



- a. Click OK.

For logs sent to Analytics clusters, to display DHCP logs, select Analytics > Logs > DHCP in the left menu bar.

The screenshot shows the Director UI's Analytics section. The left sidebar has icons for Dashboard, Insights, Logs (which is highlighted with a red box), Reporting, and Admin. The main content area is titled 'DHCP Logs >' and shows a table with the following columns: Receive Time, Appliance, DHCP Request Type, Hostname, Ingress interface, Ethernet Address, Pool Name, Client Address, Profile, and Expiration Time. There is a checkbox for 'Show Domain Names' and a 'Set filters here...' input field with 'Apply | Clear | Copy Filter' buttons. A 'Show 10 entries' dropdown is also present. The table body says 'No data available in table'. At the bottom, it shows 'Showing 0 to 0 of 0 entries' and 'Previous Next' buttons.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

Configure DLP Logging

For Releases 22.1.3 and later.

- Syslog identifier—[dlpLog](#)
- Path to the configuration screen—Search Data Configurations > DLP Logs

To export DLP logs, associate a LEF profile when configuring the DLP profile.

To export DLP logs:

1. In Director view:
 1. Select the Administration tab in the top menu bar.
 2. Select Appliances in the left menu bar.
 3. 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 > DLP > DLP Profile in the left menu bar. The following screen displays.

The screenshot shows the Director View interface. The top navigation bar has tabs for Director View, Appliance View (selected), and Template View. Below the tabs are sub-tabs: Monitor, Analytics, Configuration (selected), and Administration. The left sidebar shows an Appliance dropdown set to BR1, an Organization dropdown set to Provider-ORG, and a message: "You are currently in Appliance View". The main pane displays a table with columns: Name, Default Action, and Rules. A message "No Record Added" is shown above the table, and a blue "+ Add" button is at the bottom. The left sidebar has sections for Networking (IP Filtering, DNS Filtering, URL Filtering, File Filtering, Antivirus, Vulnerability, Predefined Vuln...), ATP, CASB, and DLP. The DLP section is expanded, and the "DLP Profile" item is highlighted with a red box.

4. Select the tenant from the Organization drop-down list.
5. In the main pane, select an existing DLP profile, or else click the + Add icon to add a new profile and select Actions tab. The following screen displays.

Add DLP profile

General Actions Exclusions Applications & Groups Reputation Rules

Actions

Default Action *

---Please Select---

LEF Profile

---Please Select--- Default LEF Profile

Storage Profile

---Please Select--- Exit On First Rule Match

Secondary DLP

---Please Select---

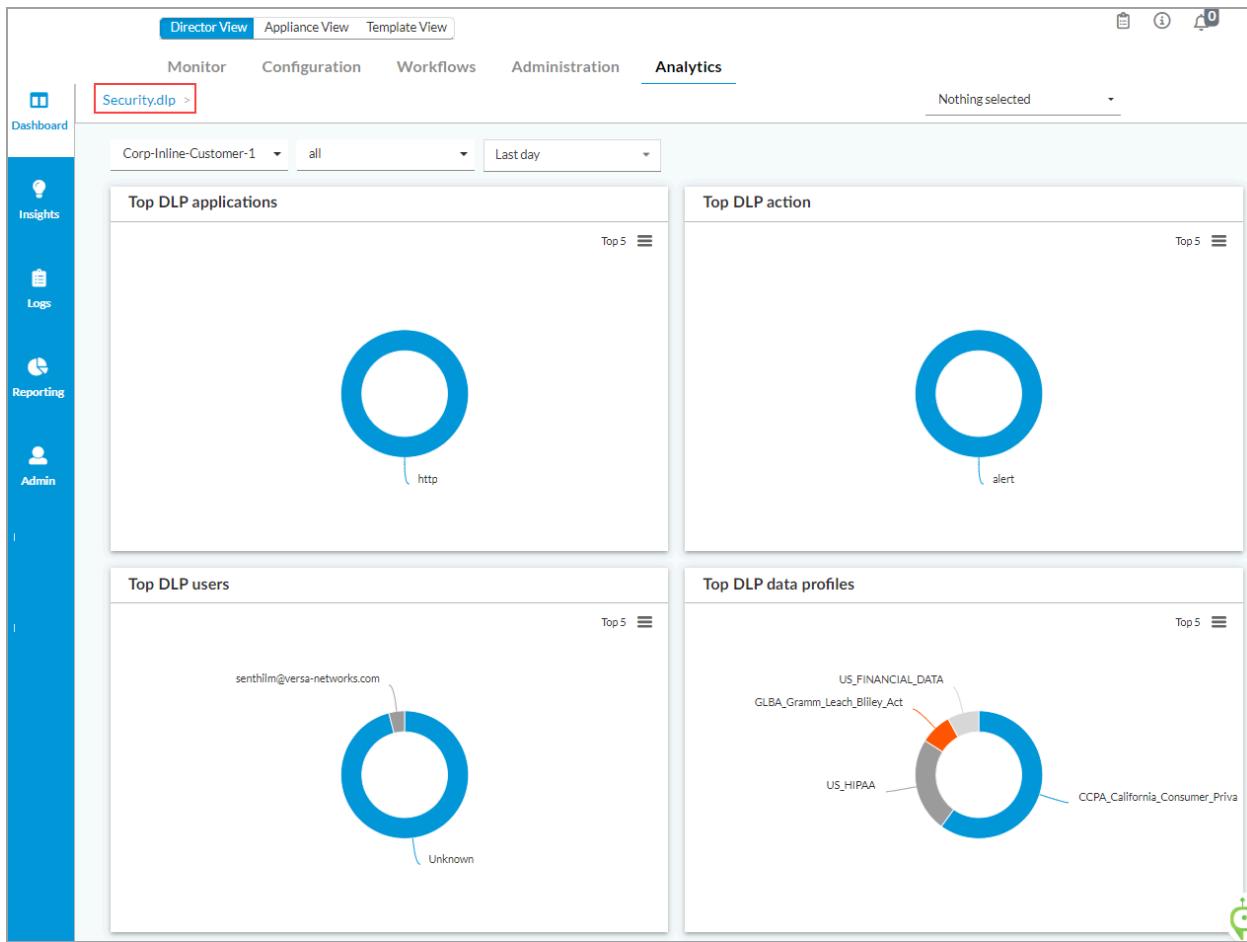
RSA Public Key (.pem) Path

OK Cancel

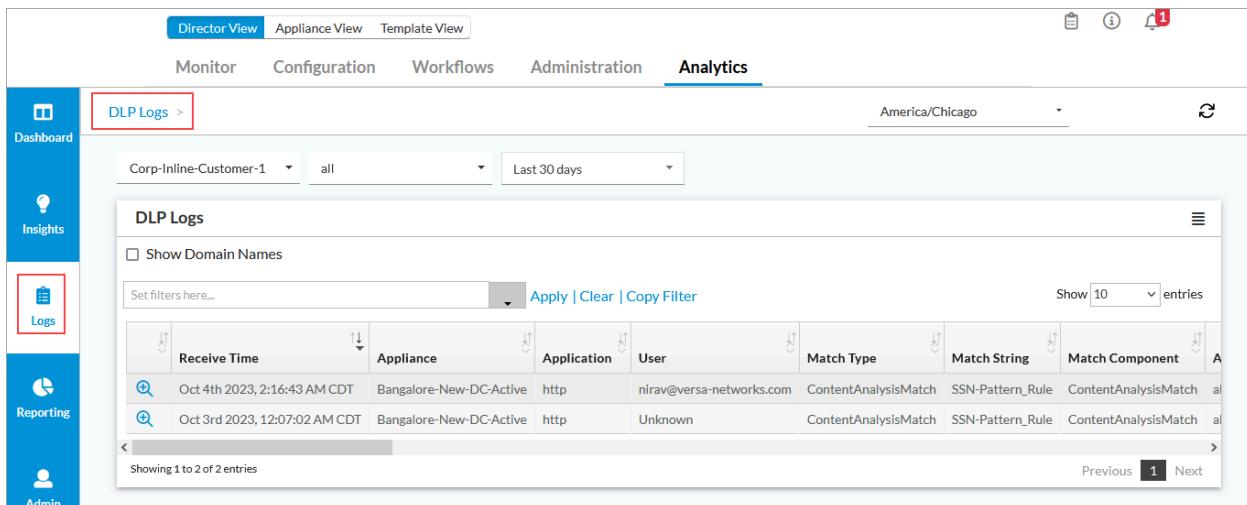
The screenshot shows the 'Add DLP profile' dialog box. The 'Actions' tab is active. In the 'Actions' section, there is a 'Default Action' dropdown set to '---Please Select---'. Below it is a 'LEF Profile' section with a dropdown set to '---Please Select---' and a checkbox for 'Default LEF Profile' which is unchecked. There are also sections for 'Storage Profile' and 'Secondary DLP' with dropdowns set to '---Please Select---' and checkboxes for 'Exit On First Rule Match' and 'RSA Public Key (.pem) Path' respectively. At the bottom are 'OK' and 'Cancel' buttons.

6. In the LEF Profile field, select a LEF profile. Or, click Default LEF Profile to use the default LEF profile.
7. Click OK.

For logs sent to Analytics clusters, to display the DLP dashboard, select the Analytics tab in the top menu bar and then select Dashboards > Security > DLP in the left menu bar.



For logs sent to Analytics clusters, to display DLP logs, select the Analytics tab in the top menu bar and then select Logs > DLP in the left menu bar, and select the Logs tab in the horizontal menu bar.



https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

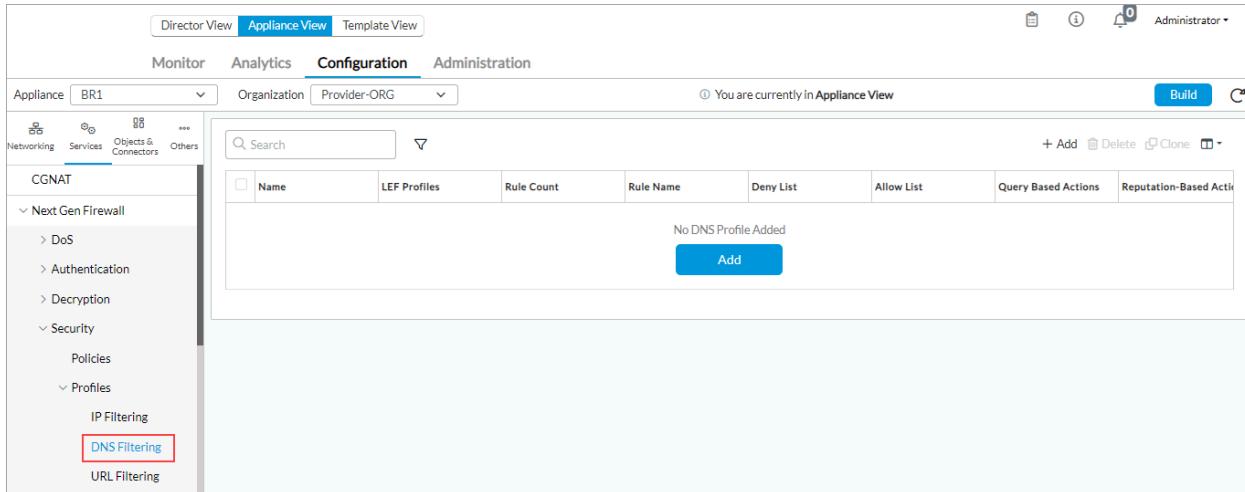
Configure DNS Filtering Logging

- Syslog identifier—[dnsfLog](#)
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > DNS Filtering Logs

To export DNS filtering logs, select a LEF profile when configuring a DNS-filtering profile. When you apply this DNS-filtering profile to an access policy, DNS filtering logs are forwarded to the active collector of the LEF profile. For information about configuring DNS filtering, see [Configure DNS Filtering](#).

To associate a LEF profile with a DNS-filtering profile:

1. In Director view:
 1. Select the Configuration tab in the top menu bar.
 2. Select Devices > Devices in the horizontal menu bar.
 3. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 4. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Profiles > DNS Filtering in the left menu bar.



4. Click the + Add icon. The Add DNS Filter popup window displays.

Add DNS Filter

Name *

Description

Tags

LEF Profile

Default Profile

Deny List Allow List Query Based Actions Reputation-Based Actions Tunnel Detection

Deny List Action

<input type="checkbox"/> Pattern ?	+	Delete	Edit
Pattern Not Configured			

<input type="checkbox"/> Strings	+	Delete	Edit
Strings Not Configured			

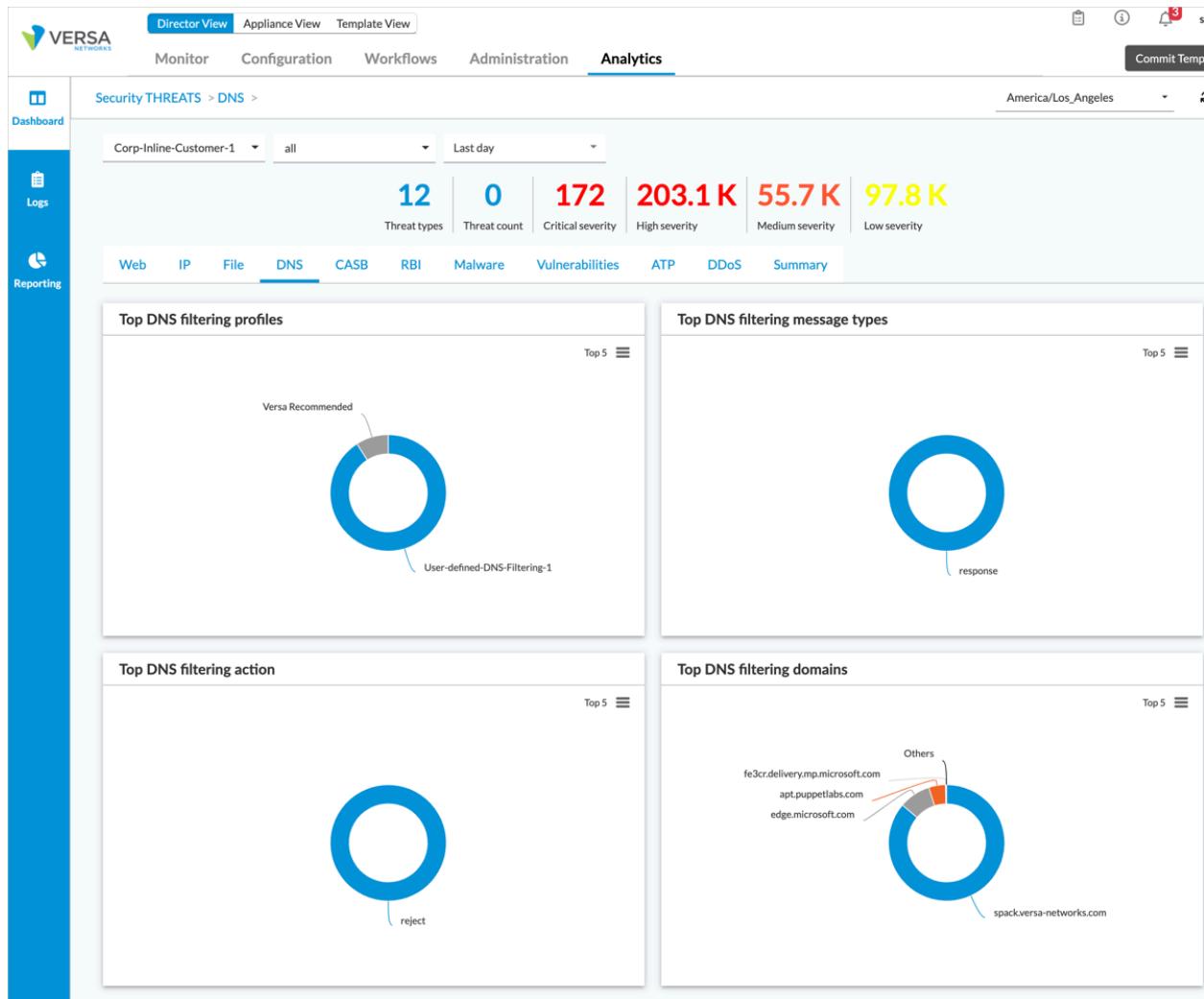
5. In the LEF Profile field, select a LEF profile to use for logging, or click Default Profile to use the default LEF profile.
6. Click OK.

For logs sent to Analytics clusters, to display DNS-filtering logs, select the Analytics tab in the top menu bar, select Logs > DNS in the left menu bar, and then select the DNS Filtering tab in the main pane.

The screenshot shows the VERSA Director View interface. The top navigation bar includes Director View, Appliance View, Template View, Monitor, Configuration, Workflows, Administration, and Analytics. The Analytics tab is selected. The main pane is titled "DNS Logs > DNS Filtering >" and shows a table of "DNS Filtering Logs". The table has columns: Receive Time, Appliance, Profile Name, Msg Type, EV Type, Action, Domain, Rule Name, Bad Resolved Addr, and Bad C Nam. There are 10 entries listed, all from Feb 9th 2024, 1:56:51 PM PST, on Colovore-DC-Branch-1, with various combinations of profile names, msg types, and actions like ip-filter reject.

Receive Time	Appliance	Profile Name	Msg Type	EV Type	Action	Domain	Rule Name	Bad Resolved Addr	Bad C Nam
Feb 9th 2024, 1:56:51 PM PST	Colovore-DC-Branch-1	User-defined-DNS-Filtering-1	response	ip-filter	reject	spack.versa-networks.com		192.55.83.30	spack.versa
Feb 9th 2024, 1:56:51 PM PST	Colovore-DC-Branch-1	User-defined-DNS-Filtering-1	response	ip-filter	reject	spack.versa-networks.com		192.55.83.30	spack.versa
Feb 9th 2024, 1:56:51 PM PST	Colovore-DC-Branch-1	User-defined-DNS-Filtering-1	response	ip-filter	reject	spack.versa-networks.com		192.55.83.30	spack.versa
Feb 9th 2024, 1:56:51 PM PST	Colovore-DC-Branch-1	User-defined-DNS-Filtering-1	response	ip-filter	reject	spack.versa-networks.com		192.55.83.30	spack.versa
Feb 9th 2024, 1:56:51 PM PST	Colovore-DC-Branch-1	User-defined-DNS-Filtering-1	response	ip-filter	reject	spack.versa-networks.com		192.55.83.30	spack.versa
Feb 9th 2024, 1:56:51 PM PST	Colovore-DC-Branch-1	User-defined-DNS-Filtering-1	response	ip-filter	reject	spack.versa-networks.com		192.55.83.30	spack.versa
Feb 9th 2024, 1:56:50 PM PST	Colovore-DC-Branch-1	User-defined-DNS-Filtering-1	response	ip-filter	reject	spack.versa-networks.com		192.55.83.30	spack.versa
Feb 9th 2024, 1:56:50 PM PST	Colovore-DC-Branch-1	User-defined-DNS-Filtering-1	response	ip-filter	reject	spack.versa-networks.com		192.55.83.30	spack.versa
Feb 9th 2024, 1:56:50 PM PST	Colovore-DC-Branch-1	User-defined-DNS-Filtering-1	response	ip-filter	reject	spack.versa-networks.com		192.55.83.30	spack.versa
Feb 9th 2024, 1:56:50 PM PST	Colovore-DC-Branch-1	User-defined-DNS-Filtering-1	response	ip-filter	reject	spack.versa-networks.com		192.55.83.30	spack.versa

For logs sent to Analytics clusters, to display DNS-filtering charts, select the Analytics tab in the top menu bar, select Dashboards > Security > Threats in the left menu bar, and then select the DNS tab in the main pane.



Configure DNS Monitoring Logging

For Releases 22.1.1 and later.

- Syslog identifier—[flowMonDNSLog](#)
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > DNS Monitoring Logs

To export DNS monitoring logs, select the Send DNS Metadata option and an LEF profile when configuring a traffic monitoring policy rule. For information about configuring a traffic monitoring rule, see Configure Traffic Monitoring Policy in [Configure Log Export Functionality](#).

To export DNS monitoring logs:

1. In Director view:
 1. Select the Configuration tab in the top menu bar.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

2. Select Devices > Devices in the horizontal menu bar.
 3. Select an organization in the left menu bar.
 4. Select a branch in the main pane. The view changes to Appliance view.
2. Select Objects & Connectors > Connectors > Reporting > Traffic Monitoring Policy in the left menu bar. The following screen displays, with the Policies tab selected by default.

3. Select the Rules tab in the main pane.
4. Click the Add icon or select an existing rule. The Add/Edit Rules popup window displays.
5. If you are adding a new rule, select the General tab, enter a rule name in the Name field, then click OK.
6. Select the Enforce tab and in the DNS Monitoring pane, enter information for the following fields.

Field	Description
Send DNS Metadata	Click to send DNS monitoring logs to the devices associated with the LEF profile.
LEF Profile	Select a LEF profile, or click Default Profile to use the default LEF profile.

7. Click OK.

For logs sent to Analytics clusters, to display DNS monitoring logs, select the Analytics tab in the top menu bar, select Logs > DNS in the left menu bar, and then click the DNS Monitoring tab:

Configure DNS Proxy Logging

- Syslog identifier—dnsPChildSessLog, dnsPParentSessLog
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > DNS Proxy Logs

To export DNS proxy logs, select a LEF profile when configuring DNS redirection rules. For information about configuring DNS redirection rules, see Configure DNS Redirection Rules in [Configure a DNS Proxy](#).

1. In Director view:
 1. Select the Configuration tab in the top menu bar.
 2. Select Devices > Devices in the horizontal menu bar.
 3. Select an organization in the left menu bar.
 4. Select a Controller in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > DNS > Policies in the left menu bar.

4. Select the Rules tab in the main pane.
5. Select an existing rule or click Add icon. The Add Redirection Rules popup window displays.
6. Select the Proxy Setting tab. The following screen displays.

Add Redirection Rules

General Source/Destination DNS Headers Match Users/Groups Proxy Setting

Actions

Proxy Setting Server Setting None

Proxy Setting

Proxy Profile	Number of Domains to Cache	DNS64 Prefix
--Select--		
+ Proxy Profile		
Override Question		
<input type="text"/>		
<input type="checkbox"/> Only IPv4 WAN Available <input type="checkbox"/> Apply Policy Based Forwarding <input checked="" type="checkbox"/> Network Obfuscation <input type="checkbox"/> Unique IP Per Client Dynamic Destination IP Pool Cache TTL Upper Limit (seconds) --Select-- 100		

Server Setting

Address	Monitor Object	
<input type="text"/>	--Select--	+
No Records to Display		

Logging Setting

LEF Profile

--Select--	<input type="checkbox"/> Default Profile
+ LEF Profile	

[OK](#) [Cancel](#)

- In the Logging Setting area, select an LEF profile or click Default Profile to use the default LEF profile.
- Click OK.

For logs sent to Analytics clusters, to display DNS proxy logs, select the Analytics tab in the top menu bar, select Logs > DNS in the left menu bar, and then select the DNS Proxy tab in the main pane.

Configure EIP Logging

For Releases 22.1.3 and later.

- Syslog identifier—eipLog
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > EIP User Profile Logs

To export endpoint information profile (EIP) logs from a VOS device, you do the following:

- Associate a LEF profile with predefined and custom EIP profiles.
 - For predefined EIP profiles, select a LEF profile in logging control settings for NGFW. This setting applies to all predefined EIP profiles.
 - For custom EIP profiles, select a LEF profile when configuring the profiles. You select a LEF profile for each custom EIP profile separately.
- Select an EIP profile when you configure rules for the following types of policies:
 - Decryption.
 - Microsegmentation.
 - SD-WAN .
 - Secure access gateway.
 - Security.

To associate a LEF profile with all predefined EIP profiles:

1. In Director view:
 1. Select the Configuration tab in the top menu bar.
 2. Select Devices > Devices in the horizontal menu bar.
 3. Select an organization in the left menu bar.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

4. Select a branch in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security Settings > Logging Control in the left menu bar.

The screenshot shows the Versa Networks Director View interface. The top navigation bar includes Director View, Appliance View (which is selected), and Template View. Below the navigation bar are tabs for Monitor, Analytics, Configuration (selected), and Administration. The main content area shows the 'Appliance' section with 'SDWAN-Branch1' selected. A message indicates 'You are currently in Appliance View'. On the left, a sidebar lists categories like Networking, Services (highlighted with a red box), Objects & Connectors, and Others. Under 'Services', 'Next Gen Firewall' is expanded, showing sub-options like DoS, Authentication, Decryption, Security, and Security Settings (also highlighted with a red box). Under 'Security Settings', 'Logging Control' is selected (highlighted with a red box). The main pane displays the 'Logging Control' configuration page with sections for Default, Sessions, PCAP, and Predefined Override Profile. A red box highlights the 'Edit' icon in the top right corner of the main pane.

4. Click the Edit icon. In the Edit Logging Control popup window, enter information for the following fields.

Edit Logging Control

Default

LEF Profile

--Select--

All Stats

X

Sessions

All Explicit

Implicit both

both both

LEF Profile

--Select-- Default Profile

PCAP

Limit

20000

Timeout (min)

600

Predefined Override Profile

URL Filtering

LEF Profile

--Select-- Default Profile

Endpoint Information

LEF Profile

--Select-- Default Profile

DNS Filtering

LEF Profile

--Select-- Default Profile

IP Filtering

LEF Profile

--Select-- Default Profile

Antivirus

LEF Profile

--Select-- Default Profile

DLP

LEF Profile

--Select-- Default Profile

File Filtering

LEF Profile

--Select-- Default Profile

Sandboxing

LEF Profile

--Select-- Default Profile

Field	Description
Endpoint Information (Group of Fields)	
◦ LEF Profile	Select the LEF profile to associate with the EIP profile rule.
◦ Default Profile	Click to associate the rule with the default LEF profile.

5. Click OK.

To associate a LEF profile with a custom EIP profile:

1. In Director view:
 1. Select the Configuration tab in the top menu bar.
 2. Select Templates > Device Templates in the horizontal menu bar.
 3. Select an organization in the left menu bar.
 4. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > EIP Profiles in the left menu bar.

4. Click an EIP profile name or click Add to add new profile. In the Edit/Add EIP Profiles popup window, enter information for the following fields.

Add EIP Profiles

Name*	Description		
<input type="text"/>	<input type="text"/>		
LEF Profile <div style="border: 1px solid red; padding: 5px;"> --Select-- + Create Log Profile <input type="checkbox"/> Default Profile </div>			
+ - ↑ ↓ ← → 1 25 ▼			
<input type="checkbox"/>	Name	Description	Match Categories
No Rules Added			

Field	Description
LEF Profile	Select the LEF profile to associate with the EIP profile rule.
Default Profile	Click to associate the rule with the default LEF profile.

5. Click OK

For logs sent to Analytics clusters, to display EIP logs, select the Analytics tab in the top menu bar and then select Logs > EIP in the left menu bar.

Configure File-Filtering Logging

- Syslog identifier—[fileFilterLog](#)
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > File Filtering Logs

To export file filtering logs, select a LEF profile when configuring a file-filtering profile. When you apply this file-filtering profile to an access policy, file-filtering logs are forwarded to the active collector of the LEF profile. For information about configuring file filtering, see [Configure File Filtering](#).

To associate a LEF profile with a file-filtering profile:

1. In Director view:
 1. Select the Configuration tab in the top menu bar.
 2. Select Devices > Devices in the horizontal menu bar.
 3. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 4. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Profiles > File Filtering in the left menu bar. The main pane displays the configured file-filtering profiles.

The screenshot shows the Versa Director View interface. The top navigation bar includes 'Director View', 'Appliance View' (which is selected), and 'Template View'. Below the navigation is a menu bar with 'Monitor', 'Analytics', 'Configuration' (selected), and 'Administration'. The left sidebar has sections for 'Networking', 'Services', 'Objects & Connectors', and 'Others', with 'File Filtering' under 'Services' highlighted with a red box. The main content area shows a table titled 'Deny List' with columns for 'Name', 'Default Action', 'LEF Profile', 'Deny List', 'Allow List', and 'Reputation'. The 'Deny List' column contains SHA256 and SHA384. A large blue 'Add' button is at the bottom of the table. The status bar at the bottom right shows a green robot icon.

- Click the Add icon. The Add File Filter popup window displays.

The 'Add File Filter' dialog box is shown. It includes fields for 'Name' (with a required asterisk), 'Description', and 'Tags'. Under 'Default Action', there is a dropdown set to 'Alert' and a 'LEF Profile' dropdown set to '--Select--'. A checkbox for 'Default Profile' is also present. The 'File Decompression' section includes 'Max Level' (set to 1) and 'Limit Reach Action' (set to 'Allow'). The 'Protocol' section shows a table with one row and a note 'Protocol Not Configured'. At the bottom, tabs for 'Deny List' (selected), 'Allow List', 'File-Based Actions', and 'Reputation-Based Actions' are available. Action options include 'Alert' (selected), 'Enable Logging', and 'Enable'. Buttons for 'OK' and 'Cancel' are at the bottom right.

- In the LEF Profile field, select a LEF profile to use for logging, or click Default Profile to use the default LEF profile

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

For logs sent to Analytics clusters, to display file-filtering logs, select the Analytics tab in the top menu bar, select Logs > Threat Filtering in the left menu bar, and then select the File Filtering tab in the main pane.

The screenshot shows the Director View interface with the Analytics tab selected. The left sidebar features a vertical navigation bar with icons for Dashboard, Insights, Logs (which is highlighted with a red box), Reporting, and Admin. The main content area displays 'Threat Filtering Logs > File Filtering >'. It includes filters for Organization (Corp-Inline-Customer-1), Type (all), and Time (Last 30 days). Below these are tabs for URL Filtering, IP Filtering, File Filtering (which is also highlighted with a red box), DNS Filtering, and CASB. A section titled 'File Filtering Logs (ALS Powered)' contains a checkbox for 'Show Domain Names' and a search bar with 'Apply | Clear | Copy Filter' buttons. The table header includes columns for Receive Time, Appliance, Threat Severity, Application, User, Profile, File Name, File Type, File Transfer Direction, File Filter Action, and File Found. At the bottom, it shows 'Showing 0 to 0 of 0 entries' and navigation buttons for Previous and Next.

Configure Firewall Logging

- Syslog identifiers—[accessLog](#), sfwAccessLog, denyLog
- Path to the configuration screen—Search Data Configurations > Access Logs

To export DHCP Global V4 and DHCP Global V6 logs, select a LEF profile when you configure DHCP. For information about configuring DHCP, see [Configure DHCP](#).

Configure Global Firewall Per-Flow Logging

For information about configuring NGFW, see [Configure NGFW](#).

To enable global firewall per-flow logging, for all flows:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Services > Next-Gen Firewall > Security Settings > Logging Control in the left menu bar.

The screenshot shows the Versa Director configuration interface. At the top, there are tabs for Director View, Appliance View (which is selected), and Template View. Below the tabs, there are navigation links for Monitor, Analytics, Configuration (selected), and Administration. The main area displays 'Logging Control' settings. On the left, a sidebar lists various appliance components like Networking, Services, Objects & Connectors, and Others, with 'Next Gen Firewall' expanded to show sub-options like DoS, Authentication, Decryption, Security, and Security Settings. Under Security Settings, 'Logging Control' is highlighted with a red box. Other options in the sidebar include URL Filtering and Application Identification. The main panel shows sections for Default (LEF Profile, All Stats), Sessions (All, Explicit, Implicit, LEF Profile), PCAP (Limit, Timeout (min)), and Predefined Override Profile (URL Filtering, Endpoint Information, DNS Filtering, IP Filtering, Antivirus, DLP). A status message at the top right says 'You are currently in Appliance View'. A 'Build' button and a refresh icon are also present.

- Click the Edit icon to enable firewall per-flow logs for all flows (both allow and deny) globally. The Edit Logging Control popup window displays.

Edit Logging Control

Default

LEF Profile
 All Stats

Sessions

All Explicit Implicit

LEF Profile
 Default Profile

PCAP

Limit
 Timeout (min)

Predefined Override Profile

URL Filtering LEF Profile <input type="button" value="--Select--"/> <input type="checkbox" value="Default Profile"/> Default Profile	Endpoint Information LEF Profile <input type="button" value="--Select--"/> <input type="checkbox" value="Default Profile"/> Default Profile
DNS Filtering LEF Profile <input type="button" value="--Select--"/> <input type="checkbox" value="Default Profile"/> Default Profile	IP Filtering LEF Profile <input type="button" value="--Select--"/> <input type="checkbox" value="Default Profile"/> Default Profile
Antivirus LEF Profile <input type="button" value="--Select--"/> <input type="checkbox" value="Default Profile"/> Default Profile	DLP LEF Profile <input type="button" value="--Select--"/> <input type="checkbox" value="Default Profile"/> Default Profile
File Filtering LEF Profile <input type="button" value="--Select--"/> <input type="checkbox" value="Default Profile"/> Default Profile	Sandboxing LEF Profile <input type="button" value="--Select--"/> <input type="checkbox" value="Default Profile"/> Default Profile

5. Click All, select a LEF profile, and then click All Stats.
6. Click OK.

Configure Firewall Per-Flow Logging by Firewall Rule

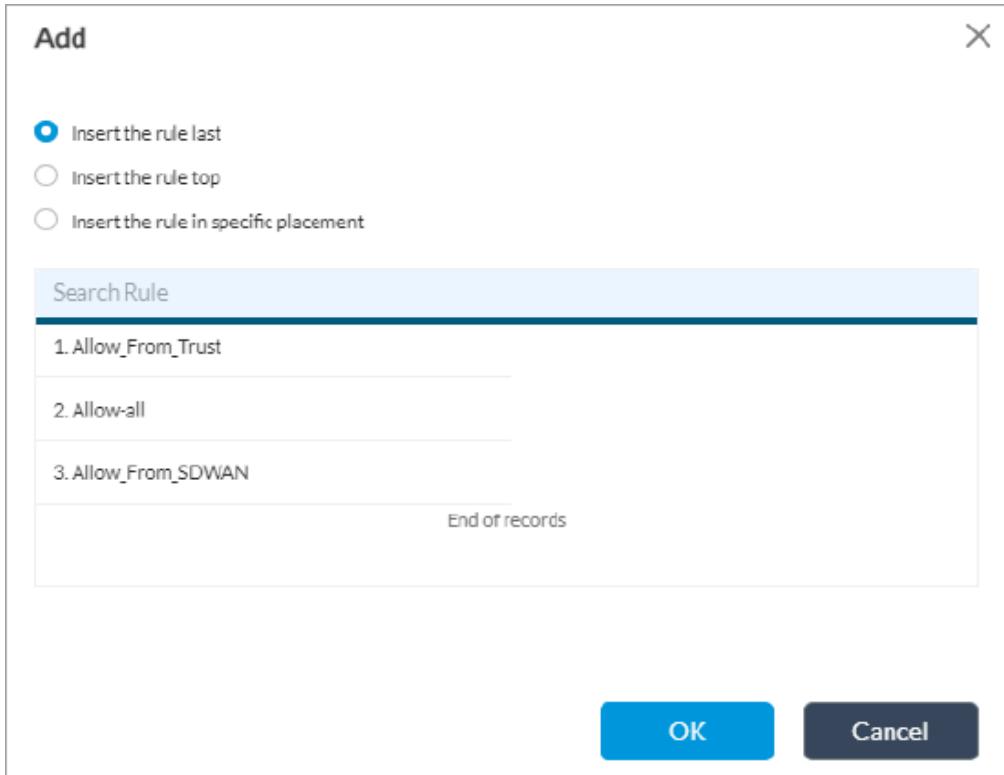
For information about configuring NGFW, see [Configure NGFW](#).

To enable firewall per-flow logging by firewall rule:

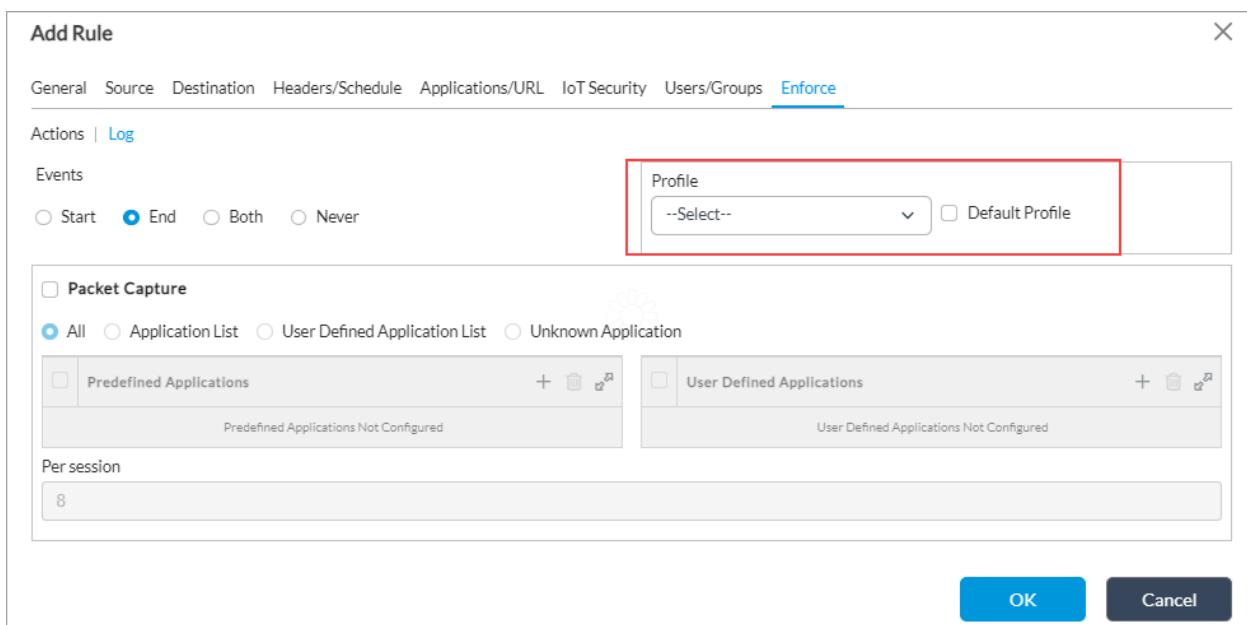
1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Services > Next-Gen Firewall > Security > Policies in the left menu bar.
4. Select the Rules tab in the horizontal menu bar.

Rule Num	Name	Rule Disabled	Alias Name	Zone	Region	Address	Address Group	Site Name
1	Allow_From_Trust	False		Intf-Provider-ORG-LA...	W-ST-Provider-ORG-L...			
2	Allow-all	False						
3	Allow_From_SDWAN	False		ptvi				

5. Click the + Add icon to define rules for the policy. The Add Rule popup window displays.
6. (For Releases 21.2.1 and later.) If rules already exist, the Configure Rule Order popup window displays.
 - a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.



- b. Select the order to insert the rule (at the top or end of the existing rules, or before or after the selected rule).
 - c. Click OK.
7. Select the Enforce tab, and then select the Log tab on the Enforce tab screen. The following screen displays.



8. In the Events group of fields, click End.
9. In the Profile group of fields, select a LEF profile or click Default Profile to use the default LEF profile.
10. Click OK.

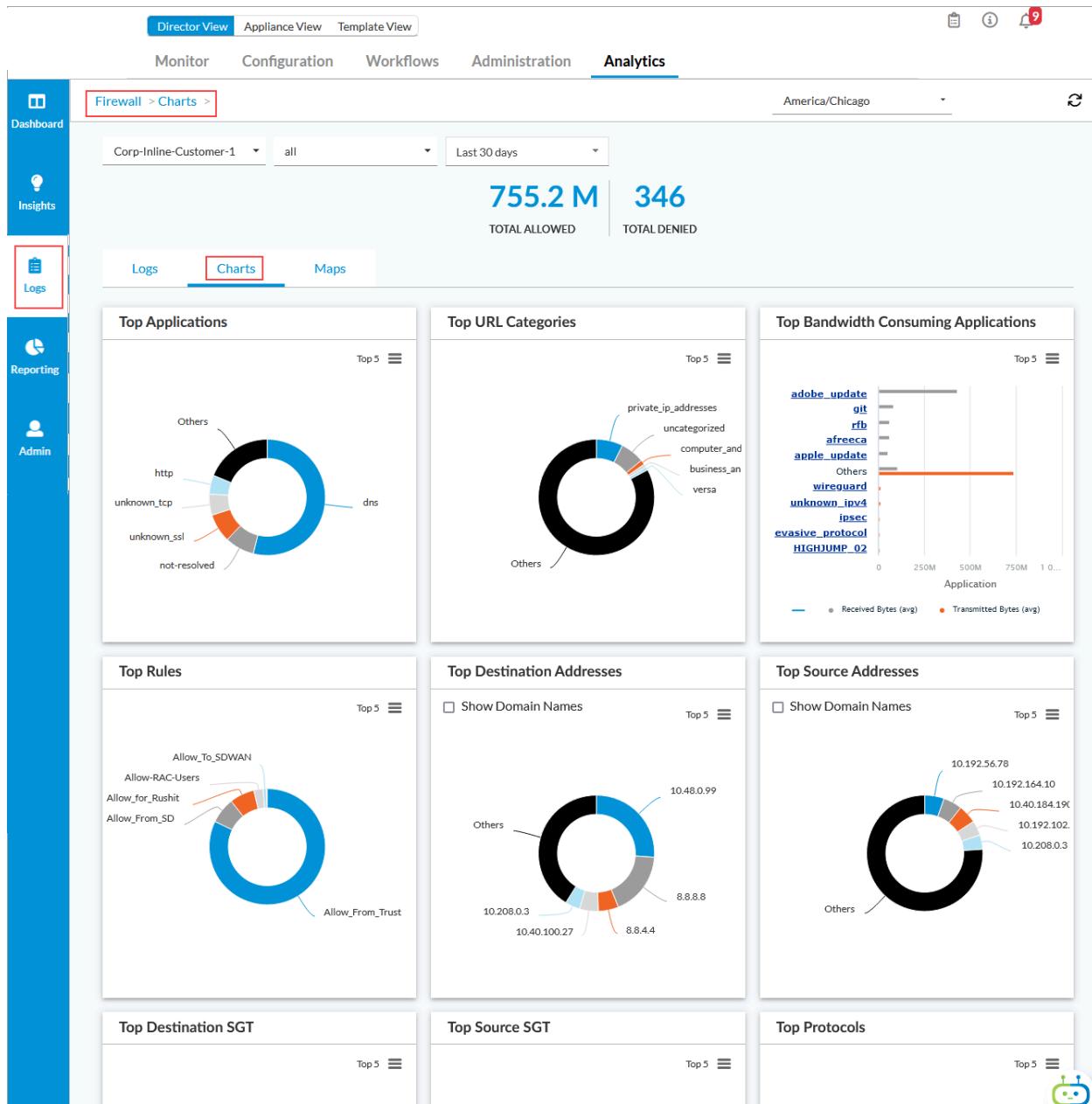
Firewall logs sent to Analytics clusters display on the following three screens:

- Analytics > Logs > Firewall > Logs
- Analytics > Logs > Firewall > Charts
- Analytics > Dashboards > Security

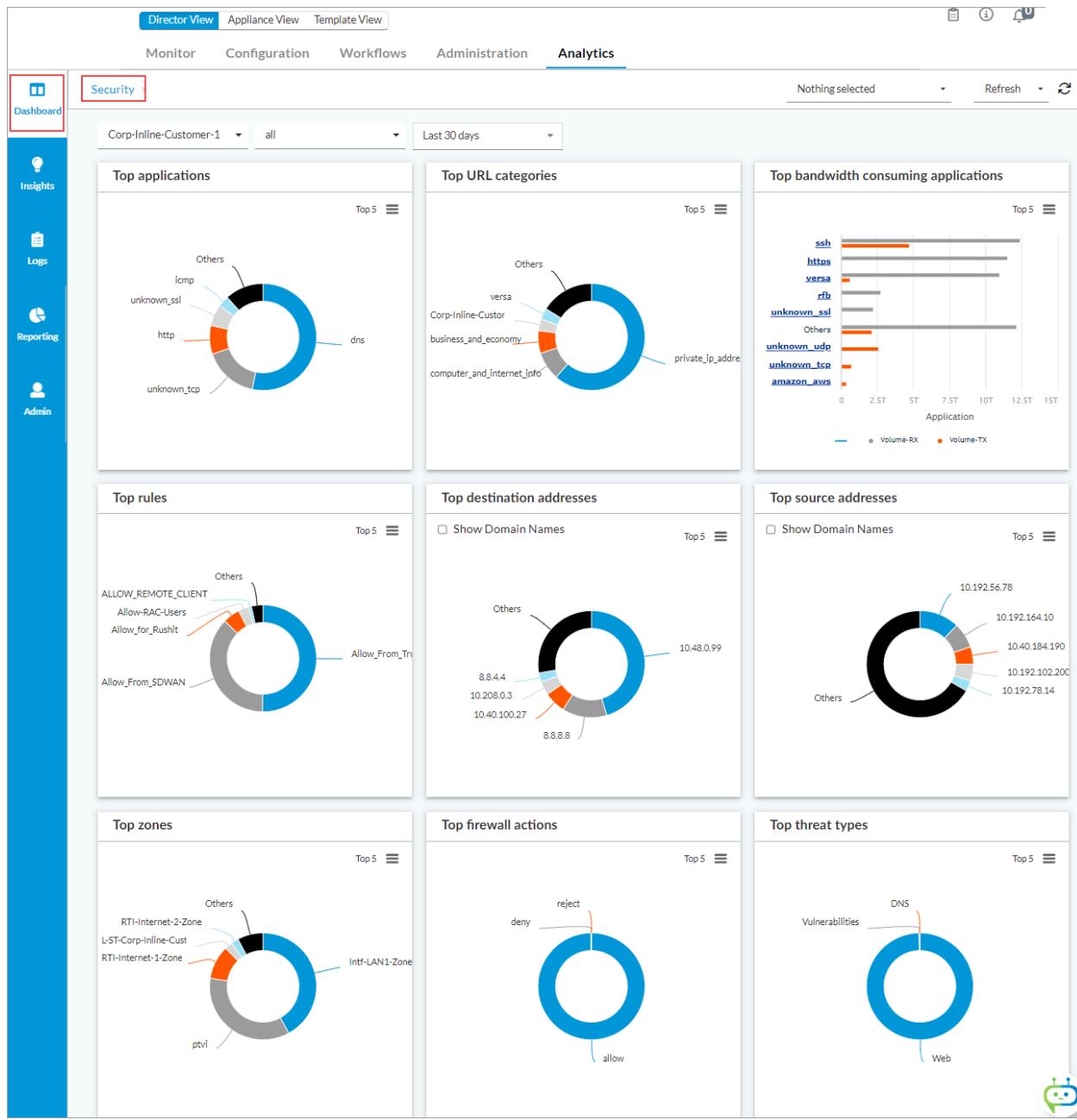
To display Firewall logs sent to Analytics clusters, select Analytics > Logs > Firewall in the left menu bar, and then select the Logs tab in the horizontal menu bar.

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Application	User	UR
Oct 5th 2023, 5:45:31 PM CDT	Bangalore-ECT-DC-Active	10.208.0.3	8.8.8	35386	53	dns	Unknown	
Oct 5th 2023, 5:45:31 PM CDT	Bangalore-ECT-DC-Active	10.192.159.103	8.8.8	56074	53	dns	Unknown	
Oct 5th 2023, 5:45:31 PM CDT	Bangalore-ECT-DC-Active	10.208.0.3	8.8.8.8	50457	53	dns	Unknown	
Oct 5th 2023, 5:45:31 PM CDT	Bangalore-ECT-DC-Active	10.192.159.103	8.8.8.8	50079	53	dns	Unknown	

To display Firewall charts sent to Analytics clusters, select Analytics > Logs > Firewall in the left menu bar, and then select the Charts tab in the horizontal menu bar.



To display Security dashboards sent to Analytics clusters, select Analytics > Dashboards > Security in the left menu bar.



Configure Firewall Summary Logging

- Syslog identifier—[monStatsLog](#)

To export firewall summary statistical logs, select a LEF profile and select the All Stats option when you configure logging control for NGFW. For information about configuring NGFW, see [Configure NGFW](#).

To export firewall summary statistical logs:

- In Director view:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

- a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Services > Next-Gen Firewall > Security Settings > Logging Control in the left menu bar.

The screenshot shows the Director View interface with the Configuration tab selected. The left sidebar has a tree structure with 'Networking' and 'Services' expanded. Under 'Services', 'Logging Control' is highlighted with a red box. The main pane shows the 'Logging Control' configuration page with sections for Default, Sessions, PCAP, and Predefined Override Profile. The 'Default' section includes LEF Profile and All Stats settings. The 'Sessions' section includes All, Explicit, and Implicit settings. The 'PCAP' section includes Limit and Timeout (min) settings. The 'Predefined Override Profile' section contains four profiles: URL Filtering, Endpoint Information, DNS Filtering, IP Filtering, Antivirus, and DLP, each with their own LEF Profile and Default Profile settings.

4. In the main pane, click the Edit icon. The Edit Logging Control popup window displays.

Edit Logging Control

Default

LEF Profile
--Select-- All Stats

Sessions

All Explicit Implicit
both both both

LEF Profile
--Select-- Default Profile

PCAP

Limit 20000 Timeout (min) 600

Predefined Override Profile

URL Filtering LEF Profile --Select-- <input type="checkbox"/> Default Profile	Endpoint Information LEF Profile --Select-- <input type="checkbox"/> Default Profile
DNS Filtering LEF Profile --Select-- <input type="checkbox"/> Default Profile	IP Filtering LEF Profile --Select-- <input type="checkbox"/> Default Profile
Antivirus LEF Profile --Select-- <input type="checkbox"/> Default Profile	DLP LEF Profile --Select-- <input type="checkbox"/> Default Profile
File Filtering LEF Profile --Select-- <input type="checkbox"/> Default Profile	Sandboxing LEF Profile --Select-- <input type="checkbox"/> Default Profile

OK **Cancel**

5. Select a LEF profile, and then click All Stats.
6. Click OK.

For firewall summary statistical logs sent to Analytics clusters, the logs display as aggregate statistics on the following

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

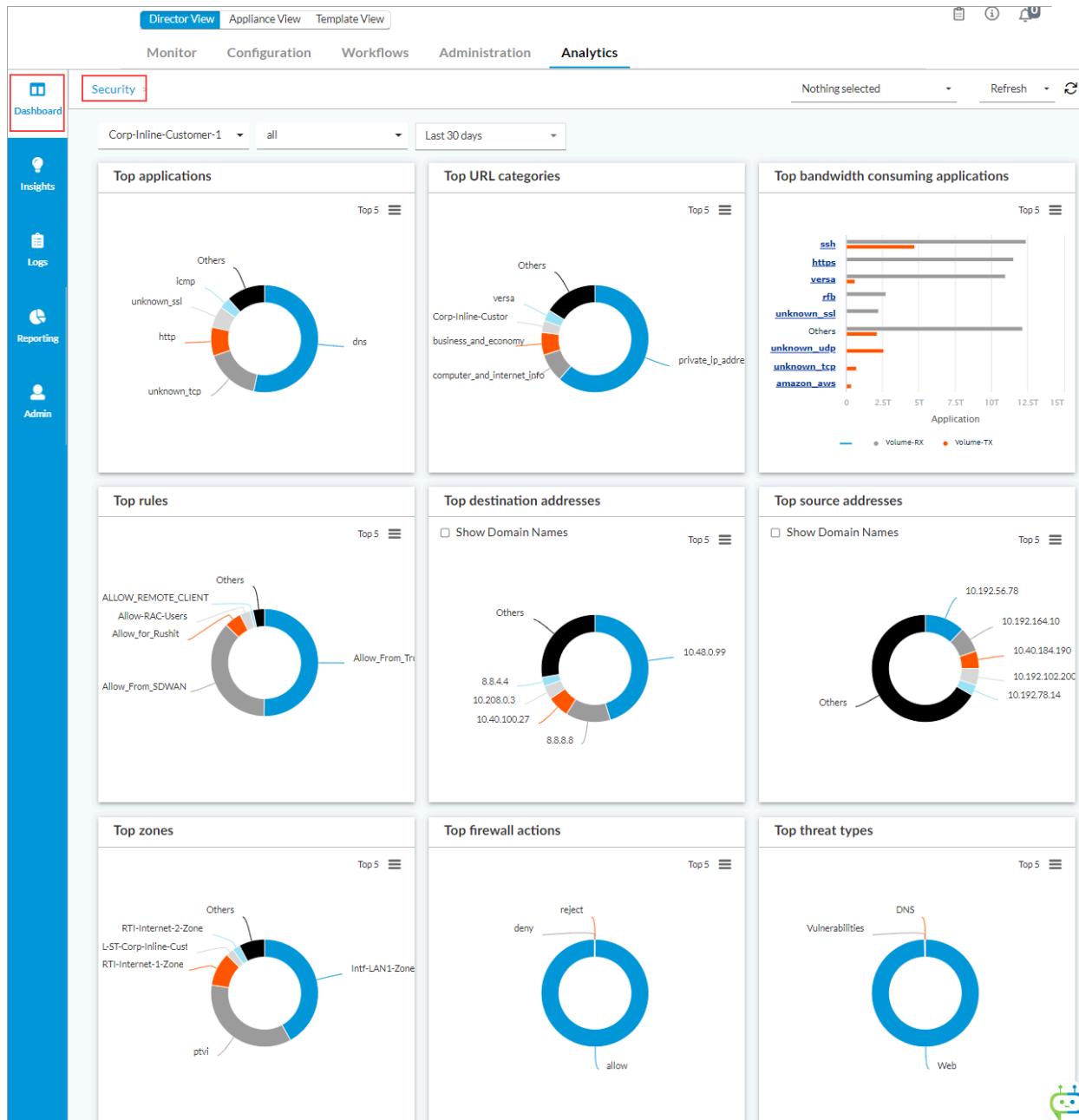
Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

screens:

- Analytics > Dashboards > Security
- Analytics > Dashboard > Security > Applications
- Analytics > Dashboards > Security > Web
- Analytics > Dashboards > Security > Firewall

For logs sent to Analytics clusters, to display the firewall summary dashboards, select Analytics > Dashboards > Security in the left menu bar.

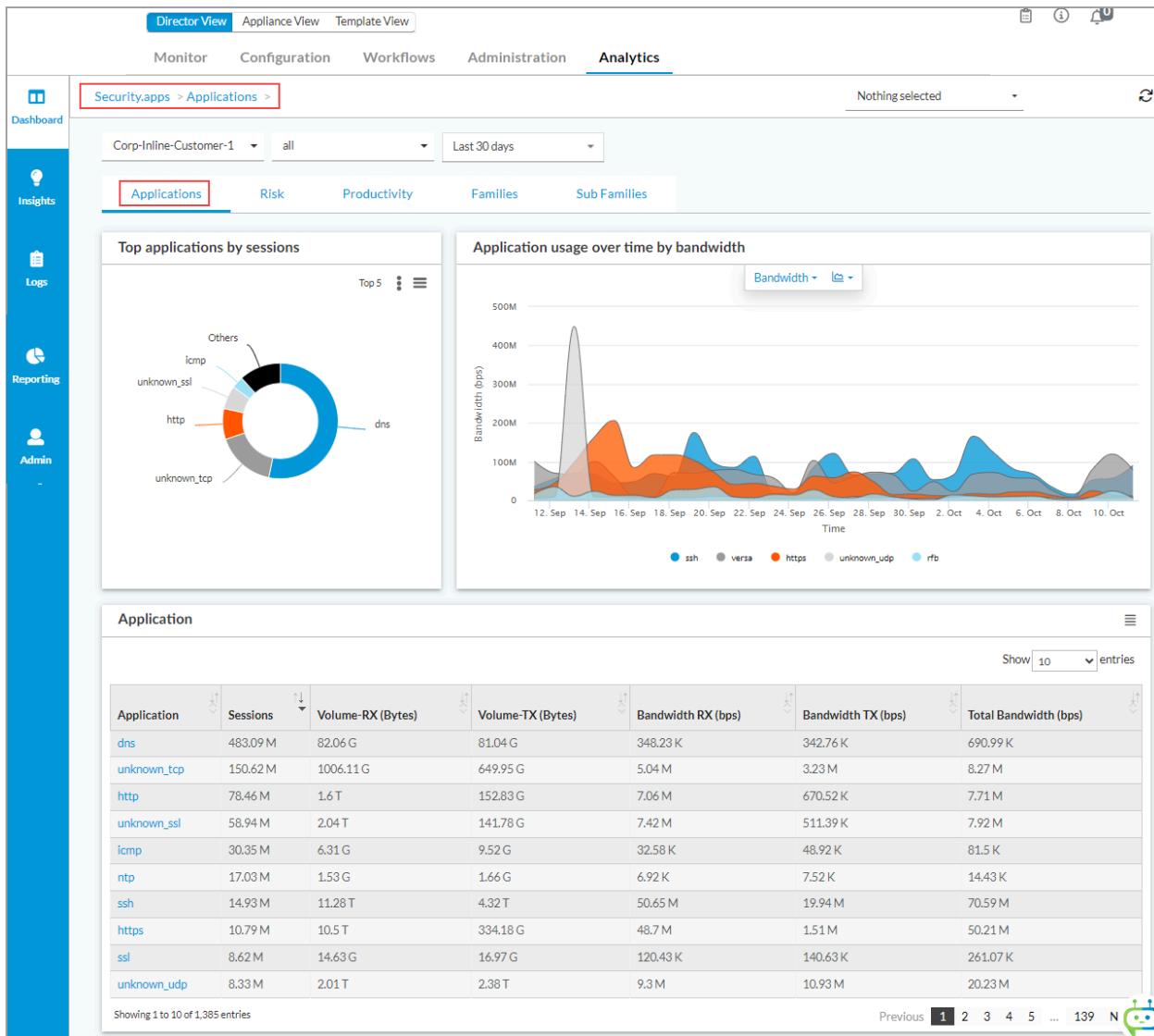


https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Export.html

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

For logs sent to Analytics clusters, to display the applications dashboards, select Analytics > Dashboards > Security in the left menu bar, and then select the Applications tab in the horizontal menu bar.

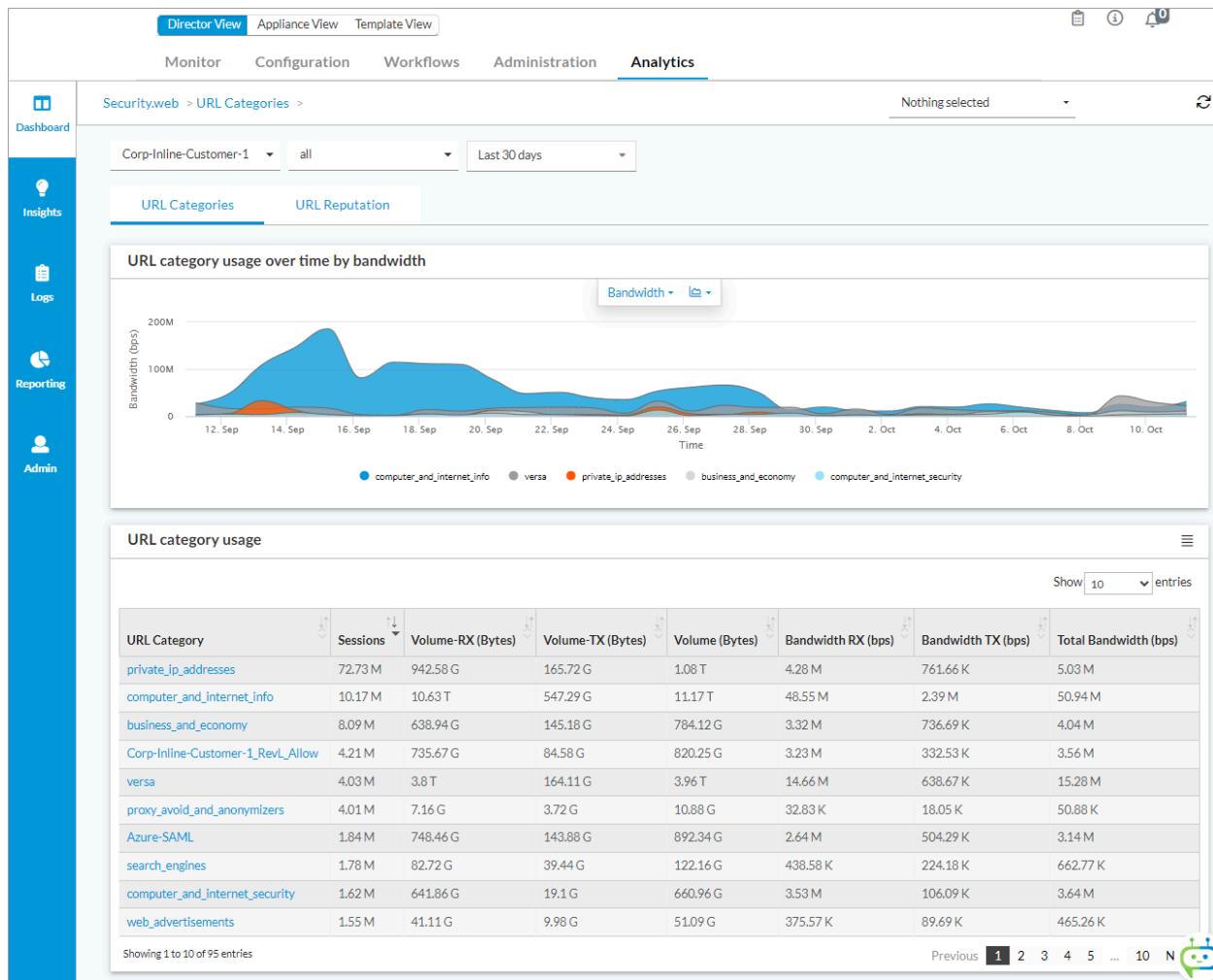


For logs sent to Analytics clusters, to display the web dashboards, select Analytics > Dashboards > Security > Web in the left menu bar.

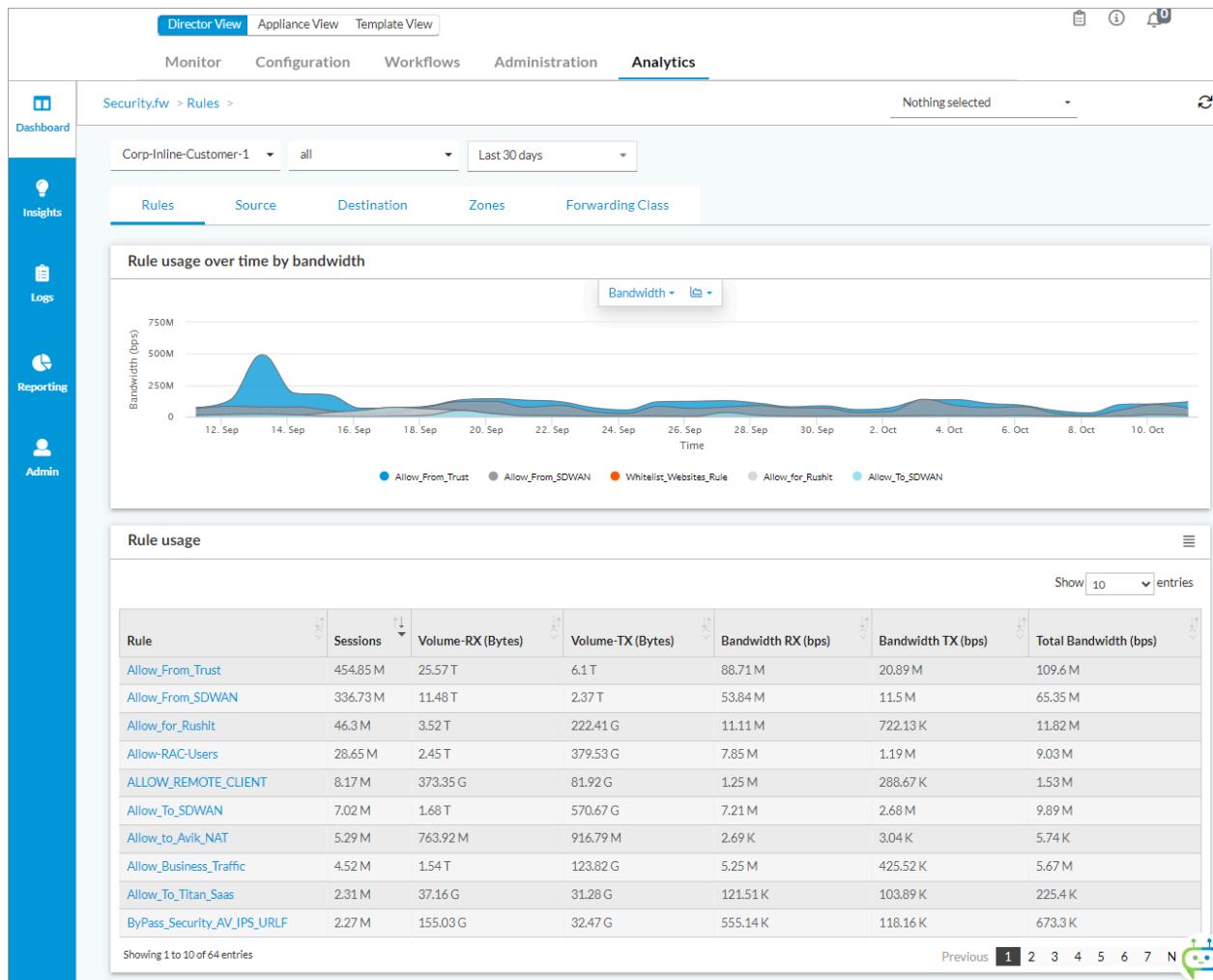
https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.



For logs sent to Analytics clusters, to display firewall dashboards, select Analytics > Dashboards > Security > Firewall in the left menu bar.



Configure LTE Summary Logging

- Syslog identifiers—`IteEventLog`, `IteStatsLog`
- Path to the configuration screen—Search Data Configurations > LTE Events Logs, Search Data Configurations > LTE Stats Logs, Analytics Data Configurations > LTE Stats

If you configure a default logging profile for LEF, LTE summary logs are generated automatically without needing further configuration, and the logs are exported. For a multitenant device, the data is sent in the provider–tenant context. For information about configuring a default LEF profile, see [Configure Log Export Functionality](#).

For logs sent to Analytics clusters, to display the LTE summary dashboards, select Analytics > Dashboards > System > Interfaces in the left menu bar, and select the LTE Interfaces tab in the horizontal menu bar.

The screenshot shows the Director View Analytics interface. The top navigation bar includes Director View, Appliance View, Template View, Monitor, Configuration, Workflows, Administration, and Analytics. The Analytics tab is active. The left sidebar has links for Dashboard, Insights, Logs, Reporting, and Admin. The main content area shows 'SYSTEM.interfaces > LTE >' and a search bar for 'Corp-Inline-Customer-1' with filters 'all' and 'Last 30 days'. Below this are tabs for WAN, LTE (selected), WIFI, and Tunnels. A section titled 'LTE Statistics' displays a table with columns: Appliance, Interface, Avg Duration (ms), Volume-RX (Bytes), Volume-TX (Bytes), Volume (Bytes), Bandwidth RX (bps), Bandwidth TX (bps), and Total Bandwidth (bps). A message says 'No data available in table'. At the bottom, it shows 'Showing 0 to 0 of 0 entries' and 'Previous' and 'Next' buttons.

Configure Packet Capture Logging

- Syslog identifier—pcapLog
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > Packet Captures

You can enable packet capture logging for the following features and services:

- IDP
- NGFW
- Traffic monitoring

You enable packet capture using policy rules for the feature or service. The VOS device exports packet capture logs to the active collector configured in the LEF profile associated with the rule. It is recommended that you enable packet capture logging only for diagnostics, because packet capture is very resource intensive on both VOS and Analytics devices.

Configure IDP Packet Capture

For IDP, you enable packet capture in a vulnerability profile rule. Packet capture logs are sent to the active collector configured in the LEF profile associated with the vulnerability profile. For more information, see [Configure IDP Threat Detection Vulnerability Logging](#), below.

To enable packet capture for IDP in a predefined vulnerability profile:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To have the menu display tenant organizations, double-click the provider organization.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

- d. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
 3. Select Services > Next-Gen Firewall > Security > Profiles > Predefined Vulnerability Profile Override in the left menu bar.

4. Click the **+ Add** icon. The Add Predefined Vulnerability Profile Override popup window displays with the Rule tab selected by default.

5. Ensure that a LEF profile is selected or that Default Profile is checked, and then enter information for the following fields:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

Field	Description
Packet Capture (Group of Fields)	Click to enable packet capture. When enabled, packet capture logs are selected LEF profile.
◦ Pre-window	Enter the number of packets immediately preceding the attacked packet.
◦ Post-window	Enter the number of packets immediately following the attacked packet.

6. Click OK.

To enable packet capture for IDP in a custom vulnerability profile:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To have the menu display tenant organizations, double-click the provider organization.
 - d. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Profiles > Vulnerability in the left menu bar. The following screen displays.

4. Either Click the Add icon to create a new vulnerability profile or select an existing profile in the main pane. The Add Vulnerability Profile or Edit Vulnerability Profile popup window displays.

Add Predefined Vulnerability Profile Override

Name *

Description

Tags

LEF Profile

--Select--

Default Profile

Rule Exceptions

Action

--Select--

Packet Capture

Pre-window Post-window

1	1
---	---

OK **Cancel**

5. Ensure that a LEF profile is selected or that Default Profile is selected.
6. Click the Add icon. The Add Rule popup window displays.
7. Select the Enforce tab, and enter information for the following fields.

Add Rule

Name *

Description

Tags

CVE Year +
 CVE Year Not Configured

Signature Set +
 Signature Set Not Configured

Enable

General OS/Product Application Reference/Severity **Enforce**

Action

--Select--

Packet Capture

Pre-window	Post-window
1	1

OK **Cancel**

Field	Description
Packet Capture (Group of Fields)	Click to enable packet capture. Packet capture logs are sent to the active collector of the LEF profile associated with the policy rule.
◦ Pre-window	Enter the number of packets immediately preceding the attacked packet that are captured.
◦ Post-window	Enter the number of packets immediately following the attacked packet that are captured.

- Click OK.

Configure NGFW Packet Capture

For NGFW, you enable packet capture in an access policy rule, and logs are sent to the active collector of the LEF profile associated with the policy rule. For packet capture logs, you can also set a default packet capture limit and timeout. When you enable packet capture logging in an access policy rule, these packet capture settings are used by default. For more information, see [Configure a Security Access Policy](#) in [Configure NGFW](#).

To set the default packet capture limit and timeout for NGFW packet capture logs:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To have the menu display tenant organizations, double-click the provider organization.
 - d. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security Settings > Logging Control in the left menu bar.
4. Select an organization in the Organization drop-down menu in the horizontal menu bar. The following screen displays.

The screenshot shows the Director View Appliance View interface. The Configuration tab is selected in the top navigation bar. The left sidebar shows a tree structure with 'Networking', 'Services', 'Objects & Connectors', and 'Others'. Under 'Services', 'CGNAT' is selected. Under 'Services', 'Next Gen Firewall' is expanded, showing 'DoS', 'Authentication', 'Decryption', 'Security', and 'Security Settings'. 'Logging Control' is highlighted with a red box under 'Security Settings'. The main pane displays the 'Logging Control' configuration page. It includes sections for 'Default' (LEF Profile, All Stats), 'Sessions' (All, Explicit, Implicit, LEF Profile), 'PCAP' (Limit, Timeout (min)), and 'Predefined Override Profile' (URL Filtering, Endpoint Information, DNS Filtering, IP Filtering, Antivirus, DLP). A status message at the top right says 'You are currently in Appliance View'.

5. Click the Edit icon. In the Edit Logging Control popup window, enter information for the following fields.

Edit Logging Control

Default

LEF Profile
--Select-- All Stats

Sessions

All Explicit Implicit
both both both

LEF Profile
--Select-- Default Profile

PCAP

Limit: 20000 Timeout (min): 600

Predefined Override Profile

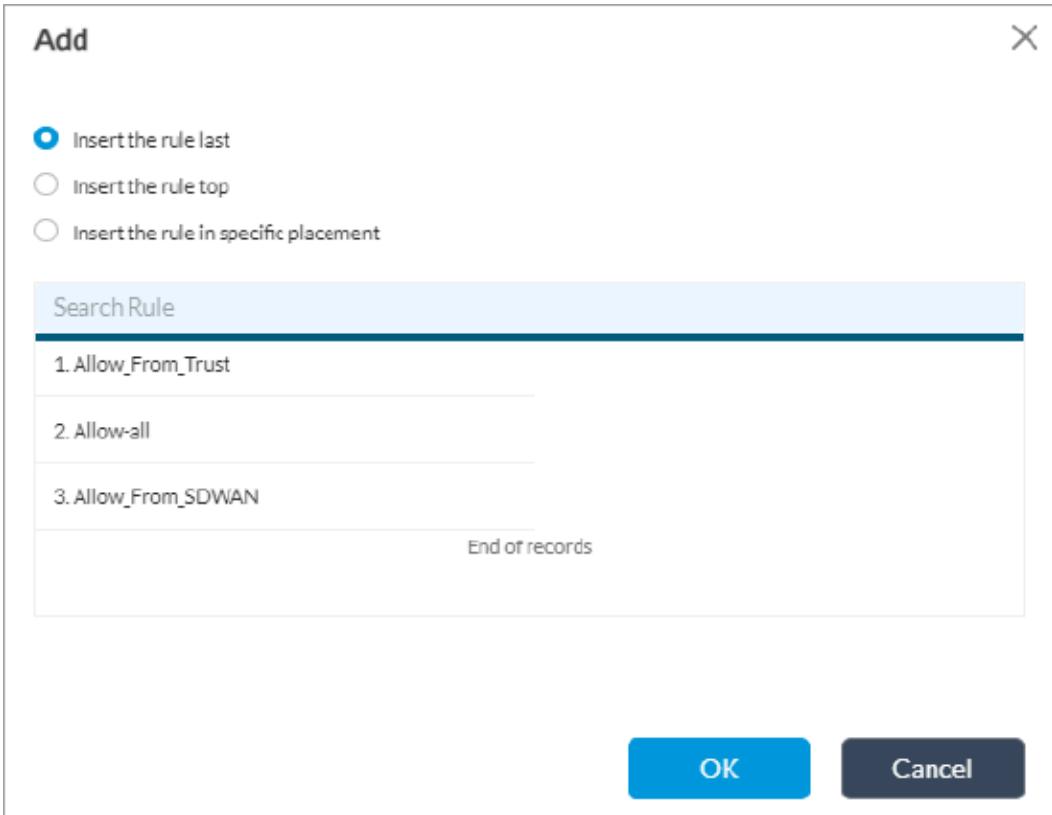
URL Filtering LEF Profile --Select-- <input type="checkbox"/> Default Profile	Endpoint Information LEF Profile --Select-- <input type="checkbox"/> Default Profile
DNS Filtering LEF Profile --Select-- <input type="checkbox"/> Default Profile	IP Filtering LEF Profile --Select-- <input type="checkbox"/> Default Profile
Antivirus LEF Profile --Select-- <input type="checkbox"/> Default Profile	DLP LEF Profile --Select-- <input type="checkbox"/> Default Profile
File Filtering LEF Profile --Select-- <input type="checkbox"/> Default Profile	Sandboxing LEF Profile --Select-- <input type="checkbox"/> Default Profile

OK **Cancel**

Field	Description
PCAP (Group of Fields)	Configure packet capture parameters.
◦ Limit	<p>Enter the number of packets to capture across the sessions. <i>Range:</i> 1000 through 50000 <i>Default:</i> 20000</p>
◦ Timeout	<p>Enter the time, in seconds, after which packet capture resumes. <i>Range:</i> 300 through 6000 seconds <i>Default:</i> 600 seconds</p>

To enable packet capture in an access policy rule:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To have the menu display tenant organizations, double-click the provider organization.
 - d. Select the device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Policies in the left menu bar, and select the Rules tab.
4. Click the  Add icon to define rules for the policy. The Add Rule popup window displays.
5. (For Releases 21.2.1 and later.) If you already added one or more rules, the Configure Rule Order popup window displays.
 - a. Select where you want to insert the policy rule, either at the beginning or end of the existing rules.
 - b. If you select a rule and then click the  Add icon, the Configure Rule Order popup window displays the following options:



- c. Select the order to insert the rule (at the beginning or end bottom of the existing rules, or before or after the selected rule).
6. Click OK. The Add Rule popup window displays.

The screenshot shows the 'Add Rule' dialog. At the top, there are tabs for 'General' (selected), 'Source', 'Destination', 'Headers/Schedule', 'Applications/URL', 'IoT Security', 'Users/Groups', and 'Enforce'. The 'General' tab contains fields for 'Name *' (with a red asterisk), 'Description', 'Tags', 'Alias Name', and a 'Disable Rule' checkbox. At the bottom right are 'OK' and 'Cancel' buttons.

7. Select the Enforce tab, and enter information for the following fields. For log collection recommendations, see [Versa Analytics Scaling Recommendations](#).

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

Add Rule

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

Actions | Log

Events

Start End Both Never

Profile
--Select-- Default Profile

Packet Capture

All Application List User Defined Application List Unknown Application

Predefined Applications + User Defined Applications +
Predefined Applications Not Configured User Defined Applications Not Configured

Per session
8

OK Cancel

The screenshot shows the 'Add Rule' dialog box with the 'Enforce' tab selected. Under 'Actions', 'Log' is chosen. In the 'Events' section, 'Start' is selected. A 'Profile' dropdown is set to '--Select--' and has a 'Default Profile' checkbox. The 'Packet Capture' section is expanded, showing 'All' selected. Below it are two lists: 'Predefined Applications' and 'User Defined Applications', both currently empty. The 'Per session' field is set to 8. At the bottom are 'OK' and 'Cancel' buttons.

Field	Description
Log (Group of Fields)	
<ul style="list-style-type: none"> ◦ Events 	<p>Select an option for logging the data:</p> <ul style="list-style-type: none"> ◦ Start—Log data at the start of each session. ◦ End—Log data at the end of each session. ◦ Both—Log data at the start and end of each session. ◦ Never—Never log data.
<ul style="list-style-type: none"> ◦ LEF Profile 	<p>Select the LEF profile to associate with the policy, or click Default Profile to use the active collector of the LEF profile. For information about configuring a LEF profile and Log Export Functionality. For information about associating a LEF profile with a feature, see Associate a LEF Profile with a Feature.</p>
Packet Capture (Group of Fields)	
<ul style="list-style-type: none"> ◦ Packet Capture 	<p>Click, and then select the application type of the packets to capture:</p> <ul style="list-style-type: none"> ◦ All ◦ Application List ◦ Unknown Application ◦ User-Defined Application List <p>For each category, select one of the following options:</p> <ul style="list-style-type: none"> ◦ Predefined Applications—Click to select a predefined application. ◦ User-Defined Applications—Click to select a custom-defined application. <p>Packet capture logs are sent to the active collector of the LEF profile.</p>
<ul style="list-style-type: none"> ◦ Per Session 	<p>Enter the number of sessions allowed per log.</p> <p><i>Default:</i> 8 sessions</p>

Configure Packet Capture for Traffic Monitoring Flows

To export packet capture logs for selected types of traffic monitoring flows, you enable packet capture in a traffic-monitoring policy rule. The packet capture logs are sent to the active collector configured in the LEF profile associated with the policy rule. For information about configuring traffic-monitoring policy, see [Configure Log Export Functionality](#).

To enable packet capture in a traffic-monitoring policy rule:

1. In Director view:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

- a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a branch in the main pane. The view changes to Appliance view.
2. Select Objects & Connectors > Connectors > Reporting > Traffic Monitoring Policies in the left menu bar. The following screen displays, with the Policies tab selected by default.

Name	Description	Tag
Default-Policy		

3. If no policy is listed in the main pain, add a policy by doing the following:

- a. Click the Add icon.
- b. In the Add/Edit Policies popup window, enter information for the following fields and then click OK.

Edit Policies - Default-Policy

Name *

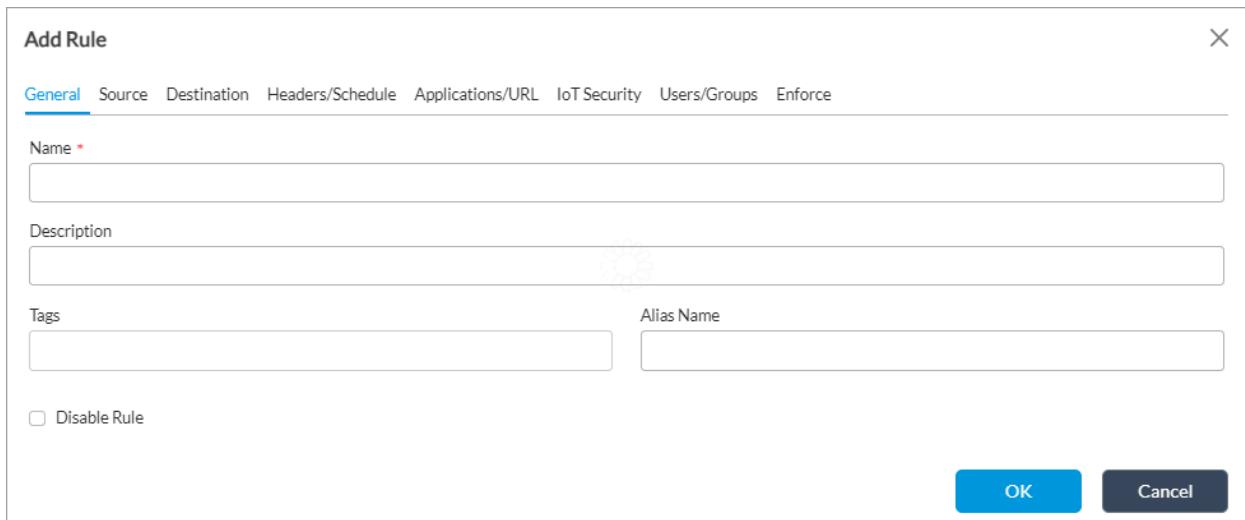
Description

Tags

OK Cancel

Field	Description
Name	Enter a name for the traffic monitoring policy.
Description	Enter a text description for the policy.
Tag	Enter a keyword or phrase that allows you to filter the policy name. Tagging is useful when you have many policies and want to view those that are tagged with a particular keyword.

- c. Click OK.
4. Select the Rules tab in the main pane.
5. Click the  Add icon or select an existing rule. The Add/Edit Rules popup window displays.



The screenshot shows the 'Add Rule' dialog box. At the top, there is a title bar with 'Add Rule' and a close button. Below the title bar is a horizontal navigation bar with tabs: General (which is selected and underlined in blue), Source, Destination, Headers/Schedule, Applications/URL, IoT Security, Users/Groups, and Enforce. The main area contains several input fields and controls:

- Name:** A text input field with a red asterisk indicating it is required. It is currently empty.
- Description:** A text input field. It is currently empty.
- Tags:** A text input field. It is currently empty.
- Alias Name:** A text input field. It is currently empty.
- Disable Rule:** A checkbox labeled 'Disable Rule'. It is currently unchecked.

At the bottom right of the dialog box are two buttons: 'OK' (highlighted in blue) and 'Cancel'.

6. If you are adding a new rule:
- Select the General tab, and in the Name field enter a name for the rule name.
 - Select one or more the following tabs to define the policy rule. For information about the fields on these tabs, see [Configure Policy-Based Forwarding](#).
 - **Source/Destination Addresses**—Enable log export based on the source or destination IP address of the traffic or the zone of the traffic.
 - **Header/Schedule**—Enable log export based on specific header information.
 - **Application/URL**—Enable log export for specific applications or URL.
7. Select the Enforce tab and enter information for the following fields.

Add Rules

General Source Destination Headers/Schedule Applications/URL **Enforce**

Flow Logging Setting

- Start
- End
- Start and End
- Interim
- Never

LEF Profile

Default Profile

[+ LEF Profile](#)

Send to Netflow Collector

Web Monitoring

LEF Profile

Default Profile

[+ LEF Profile](#)

Send SASE Web Data

DNS Monitoring

LEF Profile

Default Profile

[+ LEF Profile](#)

Send DNS Metadata

Performance Monitoring

LEF Profile

Default Profile

[+ LEF Profile](#)

TCP Monitoring

OK **Cancel**

Field	Description
LEF Profile	Select the LEF profile to associate with the traffic monitoring rule, or click Default LEF profile.
LEF Options (Group of Fields)	
◦ Send Packet Capture Data	Select to send packet capture logs for the items selected on the Source/Destination tabs to the active collector configured in the selected LEF profile.
◦ Count	Enter the number of packets to capture.
◦ Match	Select a match option: ◦ All ◦ Unclassified App ID ◦ Unknown App ID

8. Click OK.

For logs sent to Analytics nodes, to display packet capture logs, select the Analytics tab in the top menu bar, and then select Logs > Packet Captures in the left menu bar.

Configure SASE for SIM Logging

For Releases 22.1.4 and later.

- Syslog identifiers—priMobActivityLog, priMobExceptionLog, IAEEEntitlementLog
- Paths to the configuration screen:

[https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Export)

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

- Analytics > Administration > Settings > Data Configurations > Search Data Configurations > Secure Access > SASE-on-SIM activity logs
- Analytics > Administration > Settings > Data Configurations > Search Data Configurations > Secure Access > SASE-on-SIM exception logs
- Analytics > Administration > Settings > Data Configurations > Search Data Configurations > Secure Access > IAE entitlement logs

SASE for SIM performs passive authentication through a Versa Messaging Service (VMS) cluster, and the cluster generates the log types listed above. To enable SASE for SIM logging, you configure VMS log export and the VMS cluster automatically exports the logs to Analytics.

Configure VMS Log Export

To configure VMS log export, you do the following:

- Identify the IP address and port number for the local collector on each Analytics node that collects logs.
- Configure an ADC service to distribute VMS log connections to the local collectors. The ADC service provides a TCP port that listens for incoming connections. VMS cluster nodes establish connections to this port and export their logs to the ADC. The ADC uses network address translation (NAT) to map the connections, using a load-balancing algorithm, to receiving ports on Analytics nodes. Local collectors on Analytics nodes listen at the receiving ports and process the incoming logs.
- Ensure the IP address and port number of the ADC service are associated with a VMS connector. For information about configuring a VMS connector, see [Configure a VMS Connector](#).

To identify the IP addresses and port numbers for local collectors:

- In Director view, select Analytics > Administration > Configuration > Log Collector Exporter. The Log Collector Configuration screen displays.

#	Name	Address	Protocol	Clients (IP/prefix)	Port	Categories
<input type="checkbox"/>	lc1	10.40.24.141	ipfix		1234	flow
<input type="checkbox"/>	lc2	10.40.24.141			5678	flow
<input type="checkbox"/>	lc3	10.40.24.141	ipfix		1235	

Driver hosts are Analytics nodes with at least one configured local collector. Driver hosts are typically log-forwarder type Analytics nodes, although database-type and search-type nodes can also be configured with local collectors.

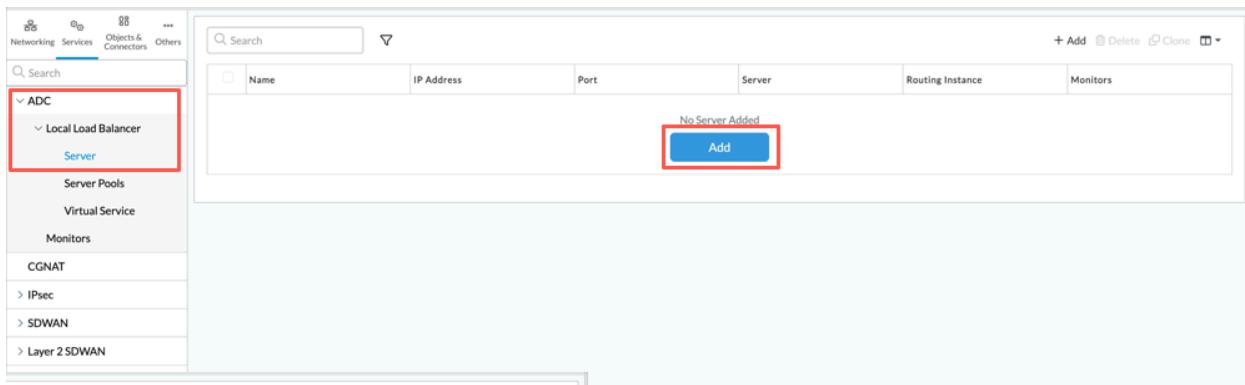
- If the Analytics cluster contains driver hosts that are not listed in the Driver Hosts field, add them to the driver hosts

list on the Analytics System Configuration screen, and then repeat Step 1. For more information, see [Configure Node Types in the Analytics Application](#).

3. In the Driver Hosts field, select a node.
4. Select the Local Collector tab. The screen displays the local collectors configured on the driver host.
5. Note the IP address and port number of the local collector that you want to receive the VMS logs.
6. Repeat Steps 3 through 5 for each driver host in the Analytics cluster.

To configure an ADC service to distribute log connections to local collectors:

1. In Director view, click Appliance view and then select a Controller node.
2. Select Configuration > Services.
3. Select the organization in the Organization drop-down list. This is typically a provider organization.
4. Select ADC > Local Load Balancer > Server in the left menu bar. If the ADC menu option does not display, enable it using the procedure in [Enable an ADC](#).



5. In the main pane, click Add. The Add Server popup window displays.

Add Server

Name *

Description

Tags

Type *

Any

 Disable Server

IP Address *

Port *

Routing Instance

--Select--

Availability Requirement

Monitors

Available	Add All
Search	Search

Selected	Remove All
Search	Search

6. Enter information for the following fields.

Field	Description
Name	Enter a name for the ADC server.
Type	Select Any.
IP Address	Enter the IP address of the local collector on the

Field	Description
	Analytics node.
Port	Enter the port number of the local collector on the Analytics node.
Routing Instance	Select a routing instance for the connection to the Analytics cluster. You typically select a provider routing instance.
Monitors	Select an ADC monitor. The monitor periodically exchanges packets with the Analytics port to determine if the port is up or down. For more information, see Configure an ADC Server Monitor .

7. Click OK.
8. Repeat Steps 5 through 7 for each local collector you noted in the previous procedure.
9. Select Server Pools in the left menu bar, and then select +Add. The Add Server Pool popup window displays.

Add Server Pool

Name *	<input type="text"/>												
Description	<input type="text"/>												
Tags	<input type="text"/>												
Availability Requirement	<input type="text"/> 1												
Type *	<input type="text"/> Any												
Load Balancing Algorithm	<input type="text"/> Round Robin												
Member	<table border="1"> <tr> <td>Name *</td> <td>Pricing</td> <td>Ratio</td> <td>Disable</td> </tr> <tr> <td>--Select--</td> <td><input type="text"/> 0...255</td> <td><input type="text"/> 0...100</td> <td><input type="checkbox"/></td> </tr> <tr> <td colspan="4"> <input type="button"/> + <input type="button"/> </td> </tr> </table>	Name *	Pricing	Ratio	Disable	--Select--	<input type="text"/> 0...255	<input type="text"/> 0...100	<input type="checkbox"/>	<input type="button"/> + <input type="button"/>			
Name *	Pricing	Ratio	Disable										
--Select--	<input type="text"/> 0...255	<input type="text"/> 0...100	<input type="checkbox"/>										
<input type="button"/> + <input type="button"/>													
<input type="button"/> OK <input type="button"/> Cancel													

10. Enter information for the following fields. For a description of all fields, see [Configure an Application Delivery Controller](#).

Field	Description
Name	Enter a name for the ADC server pool.
Type	Select Any.
Member (Group of Fields)	
<ul style="list-style-type: none"> ◦ Name 	Select an ADC server.
<ul style="list-style-type: none"> ◦ Add icons 	Click to add the ADC server to the Member table.

11. In the Member table, add an entry for each ADC server that you configured in Steps 5 through 7.
12. Click OK.
13. Select Virtual Service in the left menu bar, and then select +Add. The Add Virtual Service popup window displays.

Add Virtual Service

General Attributes Profile

Name *

Description

 Tags

Type *

--Select--

Disable Virtual Service

IP Address *

 0.0.0.0

Port *

Default Pool *

--Select--

Backup Pool

--Select--

Fallback to Active

OK Cancel

14. Click the General tab, and then enter information for the following fields.

Field	Description
Name	Enter a name for the virtual service.
Type	Select Any.
IP Address	Enter an IP address for the ADC service. This is the value for the Controller IP Address field when you verify the VMS connector, below.
Port	Enter a port number for the ADC service. The ADC service listens at this port number for connection requests initiated by VMS cluster nodes. This is the value for the Controller Port field when you verify the VMS connector, below.
Default Pool	Select the ADC pool that you configured in Step 13.

15. Click the Attributes tab.

Add Virtual Service

General Attributes Profile

NAT
 Interface NAT SNAT Pool No SNAT
 --Select--

Routing Instance **Provider Org**
 --Select-- --Select--

LEF Profile
 --Select-- Default Profile MAC Tracking

Direct Server Return **DSCP**
 --Select-- --Select--

OK **Cancel**

16. In the Routing Instance field, select a routing instance for the connection between the ADC and the VMS cluster. You typically select a provider routing instance.
17. Click OK.

To verify that the VMS cluster is configured with the correct ADC service IP address and port number:

1. In Director view, select Administration > Connectors > VMS Connector.
2. Select the VMS cluster in the main pane. The Configure VMS Cluster screen displays.
3. Click Next to go to Step 2, Authentication.

The screenshot shows the 'Configure VMS Cluster' step of a four-step wizard. The steps are: 1. VMS CONNECTION (green checkmark), 2. VMS CLUSTER (highlighted with a red box), 3. TENANTS & SERVICES, and 4. REVIEW. The title 'Configure VMS Cluster' is centered above the form. A note 'VMS Connector: VMS-Cluster-1' is in the top right. The 'Authentication' section has a 'Username' field containing 'vmsadmin'. Below it, two IP address fields are shown: 'Primary Director IP Address / Fully Qualified Domain Name (FQDN)' with '0.0.0.0' and 'Secondary Director IP Address / Fully Qualified Domain Name (FQDN)' with '0.0.0.0'. A note says 'Below are the director assigned to your VMS Cluster during high availability. If you prefer, you can change the address to your preference.' The 'VMS Interface' dropdown is set to '---Please Select---'. The 'VMS Cluster Name' field is empty. In the 'Select the VMS interface where external agents will connect' section, there are two empty input fields: 'VMS Elastic IP for Agents' and 'VMS Elastic Hostname / FQDN for Agents'. A note says 'Enter the address to the Versa Analytics Controller you want to send logs to.' The 'Controller IP Address' field contains '0.0.0.0' and the 'Controller Port' field is empty ('Enter a value'). A red box highlights both of these fields. At the bottom are 'Cancel', 'Back', and 'Next' buttons.

- Verify that the IP address and port number of the ADC service are listed in the Controller IP Address and Controller Port fields.

View SASE for SIM Logs

To display SASE for SIM logs, select Analytics > Logs > VMS. Note that SASE for SIM logs are typically assigned to a provider organization. In this case, you select the provider organization in the left drop-down list to display logs for the provider and its tenant organizations.

Select the Exceptions tab to display SASE for SIM exceptions logs.

VMS Logs > Exceptions >

Corp-Inline-Provider all Last day

Exceptions Activities IAE Entitlement

SASE-on-SIM Exceptions

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

Receive Time	Appliance	Exception Type	Description
No data available in table			

Showing 0 to 0 of 0 entries Previous Next

Select the Activities tab to display SASE for SIM activities logs.

VMS Logs > Activities >

Corp-Inline-Provider all Last day

Exceptions Activities IAE Entitlement

SASE-on-SIM Activities

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

Receive Time	Appliance	IMSI	IMEI	IP	User Group	Subscription Type
No data available in table						

Showing 0 to 0 of 0 entries Previous Next

Select the IAE Entitlement tab to display Versa identification and entitlement (IAE) logs.

VMS Logs > IAE Entitlement >

Corp-Inline-Provider all Last day

Exceptions Activities **IAE Entitlement**

Identity and Authentication Engine Entitlement logs

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

Receive Time	Appliance	IP	User	User Group	Domain	Generation Time	Type	IAE Engine
No data available in table								

Showing 0 to 0 of 0 entries Previous Next

Configure SASE Web-Monitoring Logging

For Releases 22.1.1 and later.

- Syslog identifier—[saseWebLog](#)

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > SASE Web Logs

To export SASE web-monitoring logs:

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Devices > Devices in the horizontal menu bar.
 - Select an organization in the left menu bar.
 - Select a branch in the main pane. The view changes to Appliance view.
- Select Objects & Connectors > Connectors > Reporting > Traffic Monitoring in the left menu bar. The following screen displays.

- Select the Rules tab in the main pane.
- Click the Add icon or select an existing rule. The Add/Edit Rules popup window displays.

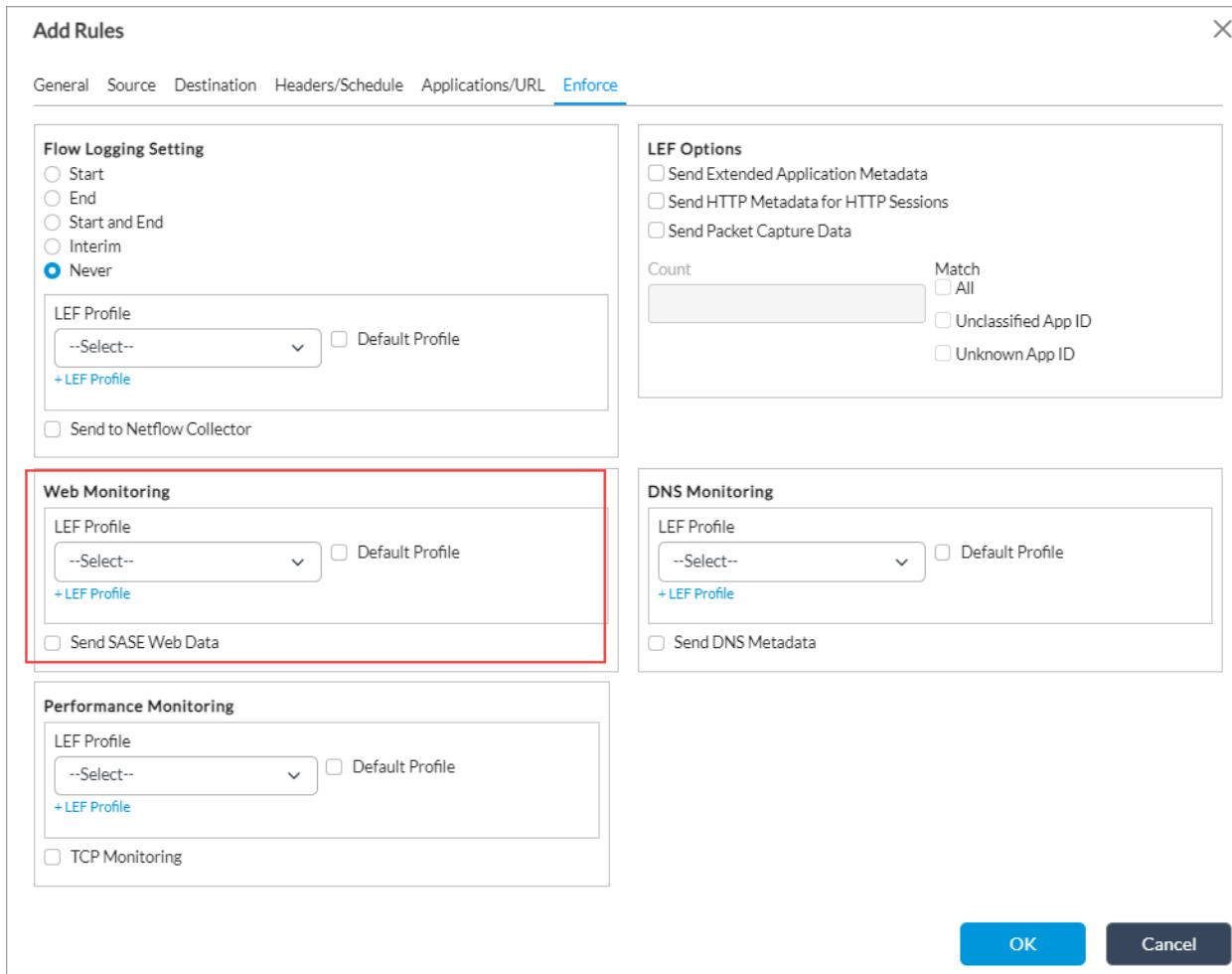
- If you are adding a new rule, select the General tab, enter a rule name in the Name field, and then click OK.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

6. Select the Enforce tab, and then enter information for the following fields.



Field	Description
Send SASE Web Data	Click to send SASE web logs to the devices associated with the LEF profile.
LEF Profile	Select a LEF profile, or click Default Profile to use the default LEF profile.

7. Click OK.

For logs sent to Analytics nodes, to display SASE web-monitoring logs, select the Analytics tab in the top menu bar, and then select Logs > SASE Web Monitoring in the left menu bar.

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Application	User	App Category
Oct 10th 2023, 11:06:52 PM PDT	CASB-Demo-Device-1	192.168.5.21	52.123.128.14	41822	443	ms_teams	Unknown	instant-messaging
Oct 10th 2023, 11:06:13 PM PDT	CASB-Demo-Device-1	192.168.5.21	8.8.8.8	58345	443	dns	Unknown	network-service
Oct 10th 2023, 11:03:56 PM PDT	CASB-Demo-Device-1	192.168.5.21	142.250.189.227	41821	443	chrome_update	Unknown	web
Oct 10th 2023, 11:02:54 PM PDT	CASB-Demo-Device-1	192.168.5.21	52.112.127.51	41820	443	ms_teams	Unknown	instant-messaging
Oct 10th 2023, 11:01:20 PM PDT	CASB-Demo-Device-1	192.168.5.21	8.8.4.4	56992	443	dns	Unknown	network-service
Oct 10th 2023, 10:54:50 PM PDT	CASB-Demo-Device-1	192.168.5.21	52.123.128.14	41819	443	ms_teams	Unknown	instant-messaging
Oct 10th 2023, 10:54:01 PM PDT	CASB-Demo-Device-1	192.168.5.21	8.8.8.8	61072	443	dns	Unknown	network-service
Oct 10th 2023, 10:52:46 PM PDT	CASB-Demo-Device-1	192.168.5.21	59.82.33.253	41818	443	wangwang	Unknown	instant-messaging
Oct 10th 2023, 10:50:35 PM PDT	CASB-Demo-Device-1	192.168.5.21	52.112.127.48	41817	443	ms_teams	Unknown	instant-messaging
Oct 10th 2023, 10:48:59 PM PDT	CASB-Demo-Device-1	192.168.5.21	8.8.8.8	63111	443	dns	Unknown	network-service

Configure SD-WAN MOS Summary Logging

- Syslog identifier—sdwanPathMosLog
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Analytics Data Configurations > SD-WAN MOS paths usage

To export mean opinion scores (MOS), you first configure MOS computation. Then you configure a default LEF profile, which forwards the computations to the active collector for the profile. For information about configuring MOS score monitoring, see [Configure MOS Score Monitoring](#). For information about configuring a default LEF profile, see [Configure Log Export Functionality](#).

To configure a VOS device to perform MOS computations for an organization:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Others > Organization > Settings in the left menu bar. The main pane displays panes related to organization settings.

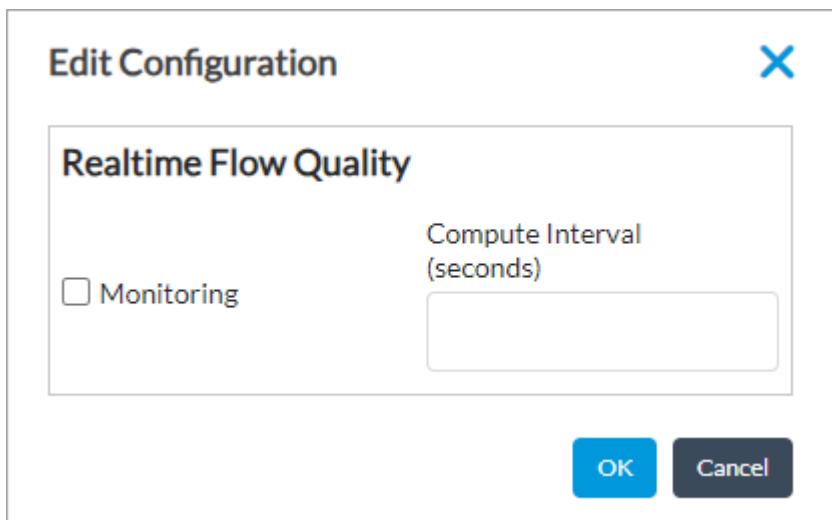
https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

The screenshot shows the Director View Configuration interface for Tenant1. The top navigation bar includes Director View, Appliance View, Template View, Tenant1-DataStore, Monitor, Configuration (selected), Workflows, Administration, Analytics, and Administrator. The Configuration menu path is Configuration > Provider1 > Common Template. On the left, there's a sidebar with links for Networking, Services, Objects & Connectors, Others, Organization (ALG, Profiles, Limits), Settings (highlighted with a red box), Messaging Service, Radius Servers, and Authentication Profile. The main pane displays configuration sections for Realtime Flow Quality, Application Generic Options, Override DF Bit, Layer2, Cloud Export Enabled, and Mip Scheduler Interval.

- In the Real-Time Flow Quality pane, click the Edit icon. The Edit Configuration popup window displays.



- Click Monitoring.
- Click OK.
- To send the MOS computations to an Analytics cluster, syslog server, or Netflow collector, configure a default LEF profile.

MOS information sent to Analytics clusters displays on the following dashboards:

- Analytics > Dashboards > SD-WAN > Top Sites by Bandwidth (choose an appliance) > MOS
- Analytics > Dashboards > SD-WAN > Top Access Circuits By Bandwidth (choose an appliance) > MOS
- Analytics > Dashboards > SD-WAN > Paths > MOS

For logs sent to Analytics nodes, to display the SD-WAN MOS top sites by bandwidth dashboards, select Analytics > Dashboards > SD-WAN in the left menu bar. In the horizontal menu bars, select a site name and then select the MOS tab.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

Screenshot of the Director View interface showing the SD-WAN Analytics dashboard for the SanJose-Office-Preferred-Standby Internet-2 MOS path.

Header: Director View, Appliance View, Template View, Monitor, Configuration, Workflows, Administration, **Analytics**.

Left Sidebar: Dashboard, Insights, Logs, Reporting, Admin.

Breadcrumbs: SDWAN > SanJose-Office-Preferred-Standby,Internet-2:MOS >

Filters: Corp-Inline-Customer-1, SanJose-Office-Preferred, Internet-2, Last 30 days.

Horizontal Menu: Access Circuit, Users, Applications, Rules, SLA Metrics, SLA Violations, VRF, QoS, APM, **MOS** (highlighted).

Left Panel: MOS scores of SanJose-Office-Preferred-Standby. Subtitle: No data to display.

Right Panel: Active sessions per MOS ranges (SanJose-Office-Preferred-Standby,Internet-2). Subtitle: All ranges. Line chart showing active sessions over time from Sep 11 to Oct 9.

Bottom Panel: MOS score of SanJose-Office-Preferred-Standby. Subtitle: Show 10 entries. Table showing MOS scores and session details for various access circuits and codecs.

Site	Access circuit	Codec	Logs count	MOS Score	Active Sessions	Active Sessions MOS 1-2	Active Sessions MOS 2-3	Active
SanJose-Office-Preferred-Standby	Internet-2	OPUS	7282	3.84	5	0	1	0
SanJose-Office-Preferred-Standby	Internet-2	AAC-LD (MPEG-4)	1735	3.61	3	1	0	0
SanJose-Office-Preferred-Standby	Internet-2	AMR-WB+	976	3.25	3	1	0	0
SanJose-Office-Preferred-Standby	Internet-2	G.711/PCMU	272	4.17	2	0	0	0
SanJose-Office-Preferred-Standby	Internet-2	H.264	187	2.59	3	1	0	0
SanJose-Office-Preferred-Standby	Internet-2	SILK	78	3.24	3	1	0	1
SanJose-Office-Preferred-Standby	Internet-2	AMR	63	1.29	3	3	0	0
SanJose-Office-Preferred-Standby	Internet-2	MSRTAudio	60	1.75	2	1	0	0
SanJose-Office-Preferred-Standby	Internet-2	H.264 SVC	27	3.76	2	0	0	0
SanJose-Office-Preferred-Standby	Internet-2	Default Codec	15	2.49	2	1	0	0

Show 1 to 10 of 12 entries. Previous 1 2 N 

For logs sent to Analytics clusters, to display the top MOS scores by path, select Analytics > Dashboards > SD-WAN > Paths in the left menu bar and then select the MOS tab in the horizontal menu bar.

The screenshot shows the Director View interface with the Analytics tab selected. The MOS tab is highlighted with a red box. The interface displays network paths, usage metrics, and QoS configurations.

Configure SD-WAN QoS Logging

- Syslog identifier—[sdwanAccCktCosLog](#)
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Analytics Data Configurations > SD-WAN QoS usage

Quality-of-service (QoS) logs are exported when shaping is configured with logging enabled on an SD-WAN link. Enable a nonzero logging interval for each WAN interface. If you set the logging interval to zero, no logs are sent. For information about configuring QoS, see [Configure CoS](#).

VOS devices aggregate all QoS queues of a traffic class (best effort [BE], expedited forwarding [EF], network control [NC], or assured forwarding [AF]) to the corresponding traffic class before exporting to the LEF profile destination.

For Releases 22.1.1 and later, you can also export QoS status logs by forwarding class, which is the combination of traffic class and queue. There are up to four traffic classes and four queues for a maximum of 16 forwarding classes, which are exported simultaneously.

To configure a VOS device to export QoS logs:

1. In Director view, select Appliance view. The Select Appliance popup window displays.
2. Select an organization from the drop-down menu in the Organization field, and then click an appliance name. The view changes to Appliance View.
3. Select the Configuration tab in the top menu bar.
4. Select Networking > Class of Service > Associate Interface/Network. The following screen displays.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

- Choose an existing interface or network, or click the Add icon to add a new interface. The Associate Interface/Network popup window displays.

Associate Interface/Network

Interface Network

Name *
--Select--

Description Tags

Shaping ?

Burst Size (Bytes) Rate (Kbps)

1000 .. 4294967295 8 .. 10000000

DSCP Rewrite Rule DSCP6 Rewrite Rule

--Select-- --Select--

802.1p Rewrite Rule Scheduler Map

--Select-- --Select--

Logging Interval(seconds)
2 .. 300

Bandwidth Sharing Off

Logging CoS FC Stats

OK **Cancel**

6. In the Logging Interval field, enter a logging interval, in seconds. Setting this field to 0 disables logging. Setting to any other value enables QoS logging by traffic class. Logs are forwarded to the default LEF profile destination.
7. For Releases 22.1.1 and later, enter a nonzero logging interval and also click Logging CoS FC Statistics to export QoS logs by forwarding class (queue).
8. Click OK.

For logs sent to Analytics clusters, to display SD-WAN QoS dashboards:

1. In Director view, select Analytics > Dashboard > SD-WAN.
2. In the second drop-down menu in the main pane, select a VOS device to display the device details dashboard.
3. Select the QoS tab in the horizontal menu bar. By default, the sum of all forwarding class statistics display in the following items:
 - Traffic Volume from *device* (chart)
 - Traffic Bandwidth from *device* (chart)

- Volume Dropped at *device* (chart)
- QoS of *device* (table)

The screenshot shows the VERSA Director View Analytics page for SDWAN-Branch1. The top navigation bar includes Director View, Appliance View, Template View, Monitor, Configuration, Workflows, Administration, and Analytics. The Analytics tab is selected. The left sidebar has links for Dashboard, Logs, Reporting, and Admin.

SDWAN > SDWAN-Branch1:QoS >

Filter options: provider-org (SDWAN-Branch1), All, Last 7 days. Location: America/Los_Angeles, Refresh, Commit Template.

Metrics tabs: Usage, Availability, Access Circuits, Users, Applications, Rules, SLA Metrics, SLA Violations, VRF, QoS (selected), APM, MOS.

Traffic volume from SDWAN-Branch1 by all forwarding classes: A stacked area chart showing traffic volume (Bytes) over time (30 Mar to 6 Apr). Legend: All Forwarding Classes (Auto), WAN1 (red), WAN2 (blue), WAN3 (grey).

Traffic bandwidth from SDWAN-Branch1 by all forwarding classes: A stacked area chart showing bandwidth (Mbps) over time (30 Mar to 6 Apr). Legend: All Forwarding Classes (Auto), WAN1 (red), WAN2 (blue), WAN3 (grey).

Volume dropped at SDWAN-Branch1 by all forwarding classes: A line chart showing dropped volume (Bytes) over time (30 Mar to 6 Apr). Legend: WAN1 (blue), WAN2 (grey), WAN3 (red). A tooltip for Thursday, Mar 30, 08:00 shows WAN2: 0 and WAN3: 0.

QoS of SDWAN-Branch1: A table showing QoS metrics for SDWAN-Branch1 across three access circuits (WAN1, WAN2, WAN3).

Site	Access circuit	Volume-TX (Bytes)	Total Tx Drops (Bytes)
SDWAN-Branch1	WAN2	2.8 G	2.24 M
SDWAN-Branch1	WAN3	2.64 G	874.54 K
SDWAN-Branch1	WAN1	1.79 M	3.11 M

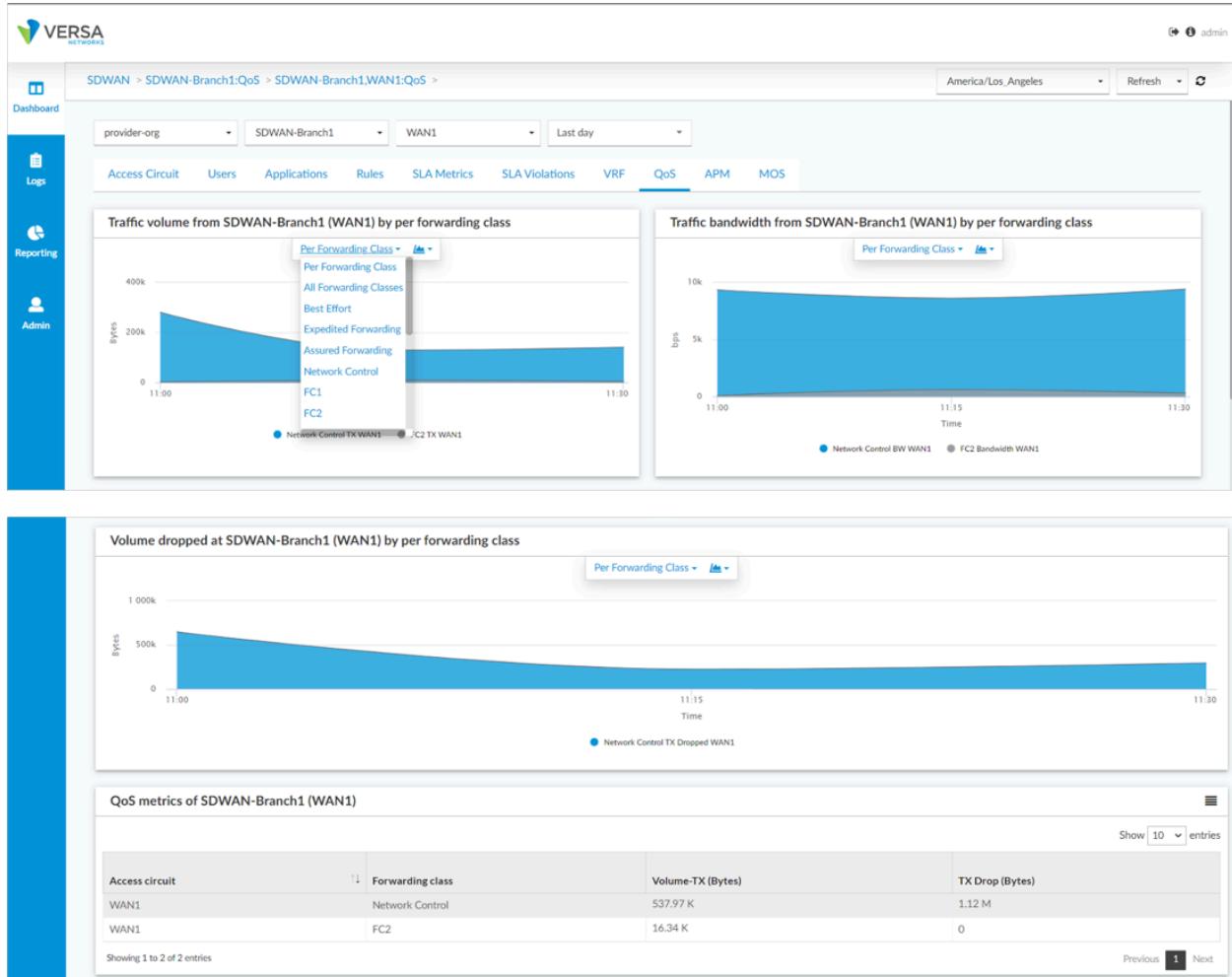
Show 10 entries, Previous, Next.

- Select a metric from the drop-down menu in a chart to display the chart by all forwarding classes or a specific forwarding class. If you did not select Log COS FC Stats on the Associate Interface/Network popup window in Step 5 of the previous procedure, then only forwarding classes EF, AF, NC, and RE are available.
- To display QoS information for a specific WAN link, select a link from the third drop-down menu. The following items display:
 - Traffic Volume from *device* (*WAN*) (chart)
 - Traffic Bandwidth from *device* (*WAN*) (chart)
 - Traffic Dropped at *device* (*WAN*) (chart)
 - QoS Metrics of *device* (*WAN*) (table)

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.



Configure SD-WAN SLA Metrics Logging

- Syslog identifier—[sdwanB2BSlamLog](#)
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Analytics Data Configurations > SD-WAN SLAM usage

To export SLA metrics logs, configure a default LEF profile. SD-WAN SLA metrics logs are then generated automatically without needing further configuration.

By default, SLA metrics logs are sent every 5 minutes for each SD-WAN path. You can change the default logging interval setting by modifying a path policy associated with a WAN interface. SLA metrics are exported from VOS devices only if the path is in active state. If it is in suspend or suspend-retry state, no logs are sent as these paths are not actively carrying traffic. For information about configuring SLA monitoring, see [Configure SLA Monitoring for SD-WAN Traffic Steering](#).

SD-WAN SLA metrics logs can exhaust cluster disk storage, especially for tenants running large full-mesh topologies. It

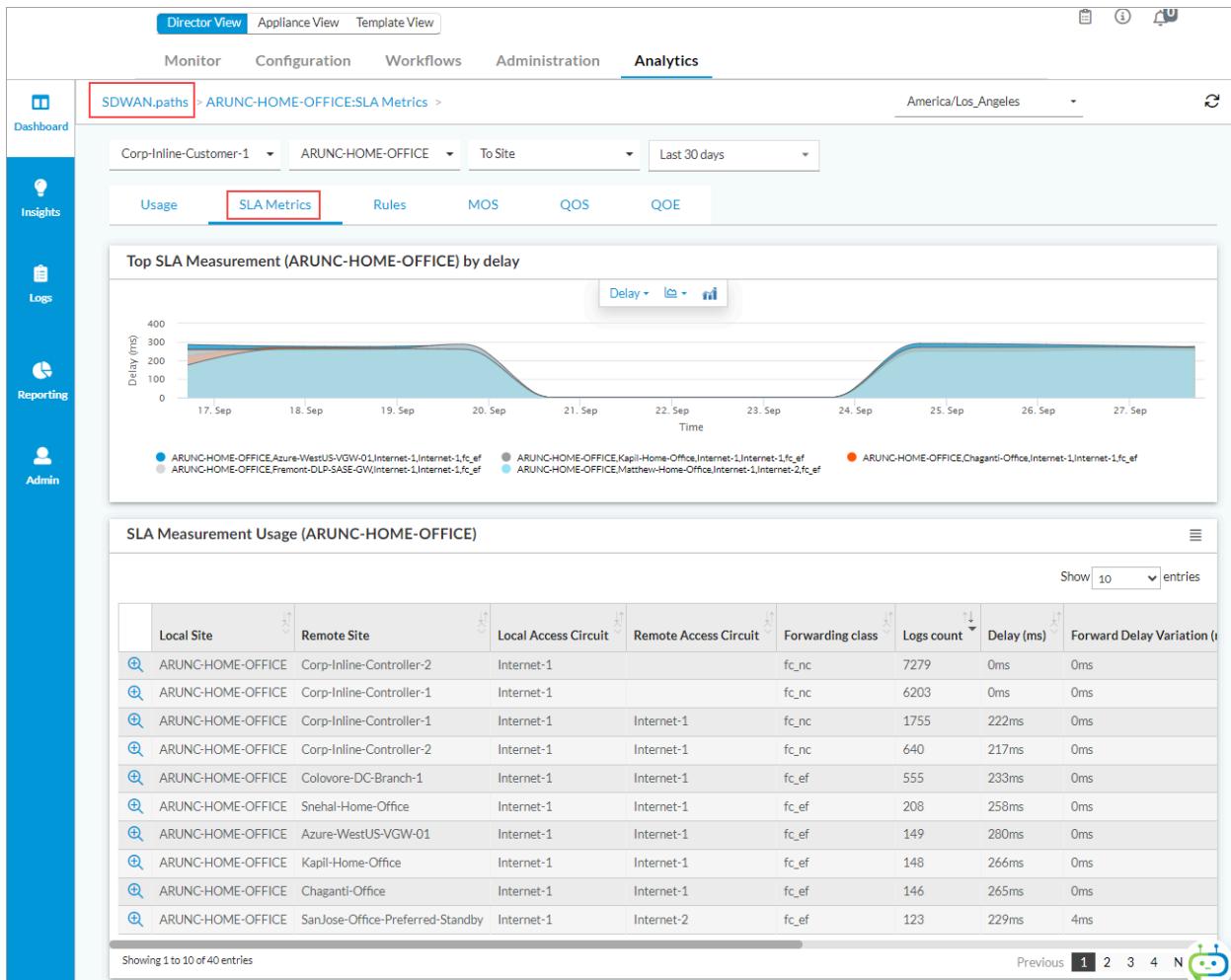
https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

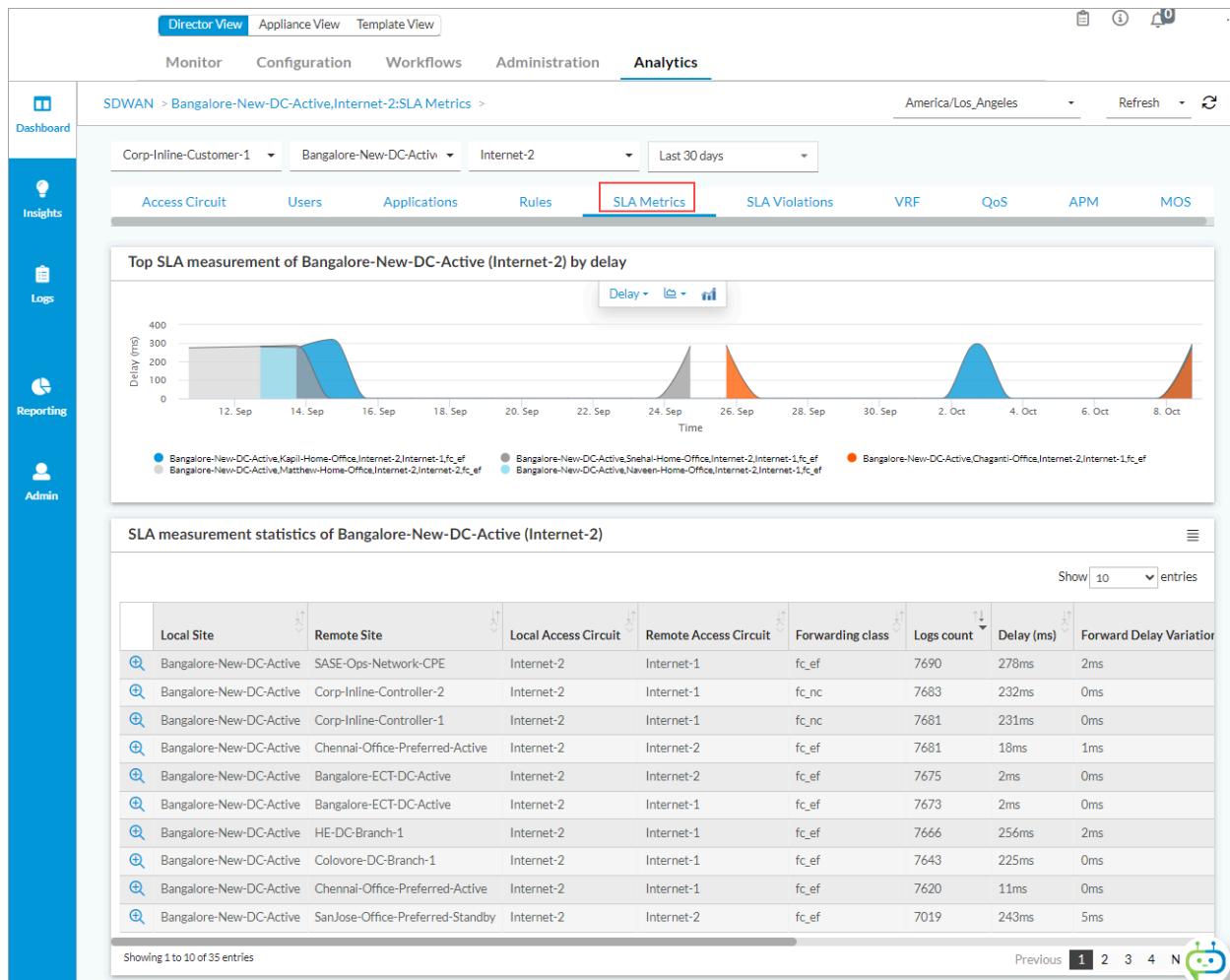
Copyright © 2024, Versa Networks, Inc.

is recommended that this data be periodically removed from database storage by configuring datastore retention times. For more information, see the [Analytics Datastore Limits](#) section in the [Versa Analytics Scaling Recommendations](#) article.

For logs sent to Analytics clusters, to display the SD-WAN SLA path metrics dashboards, select Analytics > Dashboards > SD-WAN > Paths in the left menu bar, and then select the SLA Metrics tab in the horizontal menu bar.



For logs sent to Analytics clusters, to display the SD-WAN SLA metrics by site, select Analytics > Dashboards > SD-WAN > Sites in the left menu bar. In the Sites table, select a VOS device and then select the SLA Metrics tab in the horizontal menu bar.



Configure SD-WAN SLA Violations Logging

- Syslog identifier—[sdwanSlaPathViolLog](#)
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > SD-WAN SLA Path Violation Logs

To export SLA violation logs, select a LEF profile in a traffic-steering policy rule. Log are generated based on the SLA violation events on the customer's traffic flows. If you enable SLA violation logging for all traffic, too many logs may be generated. Therefore, it is recommended that you enable log export on business-critical traffic only. For information about configuring SD-WAN traffic-steering policies, see [Configure SD-WAN Policy](#).

To export SLA violation logs:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.

- d. 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 Services > SD-WAN > Policies in the left menu bar.
4. Select the Rules tab in the horizontal menu bar. The following screen displays.

The screenshot shows the Director View interface. The top navigation bar includes 'Director View', 'Appliance View', 'Template View' (selected), 'Monitor', 'Configuration' (selected), 'Workflows', 'Administration', and 'Analytics'. The left sidebar has sections for 'Networking', 'Services', 'Objects & Connectors', and 'Others'. Under 'SDWAN', 'Application Detection', 'SLA Profiles', 'Forwarding Profiles', 'Path Policies', 'Traffic Engineering', and 'Policies' are listed, with 'Policies' highlighted by a red box. The main content area shows a table for 'Rules' under 'Default-Policy'. The table columns include 'Rule Num', 'Name', 'Rule Disabled', 'Zone', 'Address', 'Address Group', 'Address Region', 'Site Name', and 'User Defined'. A message at the bottom says 'No Rules Added'. Below the table is a blue 'Add' button.

5. Click the + Add icon, or click an existing rule. The Add/Edit Rules window displays.
6. Select the Enforce tab. The following window displays.

The screenshot shows the 'Add Rules' dialog box. The tabs at the top are 'General', 'Source', 'Destination', 'Headers/Schedule', 'Applications', 'URL', 'IoT Security', 'Users/Groups', 'Forwarding Class', and 'Enforce' (selected). The 'Forwarding' section contains fields for 'Action' (Allow Flow, Nexthop IP Address, Enable Symmetric Forwarding of Return Traffic) and 'Forwarding Profile'. The 'Monitor' section contains fields for 'Address' (IP Address), 'Action' (Select), and 'Threshold(Events)'. The 'Logging' section (highlighted with a red box) contains fields for 'LEF Profile' (Select, Default Profile checked) and 'Event' (Never, Rate Limit 10). The 'TCP Optimization' section contains fields for 'Bypass Latency Threshold (msec)', 'Mode' (Select), 'LAN Profile' (Select), and 'WAN Profile' (Select). At the bottom are 'OK' and 'Cancel' buttons.

7. In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile.
8. In the Event field, select All SLA Violated.
9. Click OK.

For logs sent to Analytics clusters, to display SLA violations by site, select Analytics > Dashboards > SD-WAN > Sites in the left menu bar and then select the Usage tab. In the Sites table, select a VOS device and then select the SLA Violations tab in the horizontal menu bar.

The screenshot shows the SD-WAN Analytics Dashboard with the following details:

- Top Remote Sites:** A donut chart titled "Top remote sites of Bangalore-New-DC-Active (Internet-2) seeing path ...". The segments represent different sites:
 - SanJose-Office-Preferred-Active (large blue segment)
 - Santa-Clara-Office-AP2 (orange segment)
 - Matthew-Home-Office (red segment)
 - Chennai-Office-Preferred-Active (light blue segment)
 - Santa-Clara-Office-AP-1 (light grey segment)
 - Others (black segment)
- SLA Alarms:** A table titled "SLA alarms of Bangalore-New-DC-Active (Internet-2)". The table has columns for Receive Time, Severity, Appliance, Alarm Type, Description, Class, Key, Event Type, Kind, Clearable, Cause, Generation Time, Serial Number, and Alarm Key. It displays "No data available in table".

Configure SD-WAN TCP Performance-Monitoring Logging

- Syslog identifier—[tcpAppMonLog](#)
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Analytics Data Configurations > TCP App Monitoring

To export TCP monitoring logs, select a LEF profile and select TCP performance monitoring in a traffic-monitoring policy rule. TCP performance monitoring is referred to as Passive APM on Analytics dashboards.

To export TCP performance monitoring logs:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

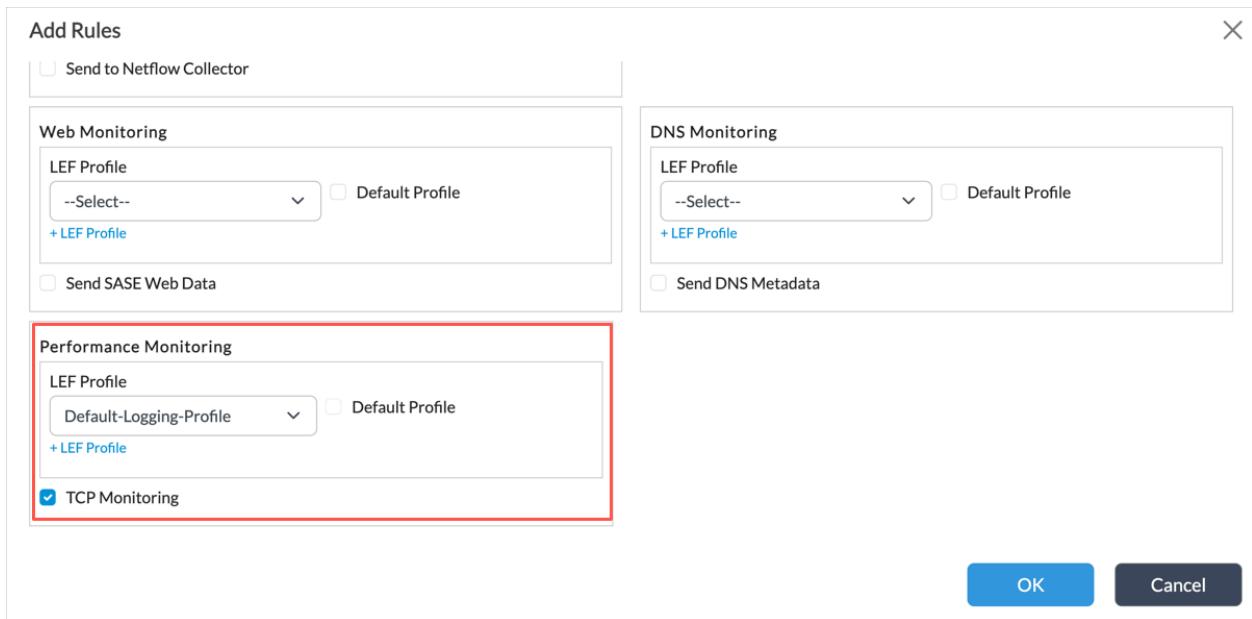
- b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar. The following screen displays.

Name	Description	Interfaces	IP Address/Prefix
vni-0/0		vni-0/0.0	192.168.30.2/24
vni-0/1		vni-0/1.0	10.192.13.251/16
vni-0/2		vni-0/2.0 vni-0/2.101 vni-0/2.401 View More...	192.168.10.251/24 192.168.1.1/32 192.168.14.252/24 192.168.15.251/24
vni-0/3		vni-0/3.0	192.168.12.251/24

3. Select Objects & Connectors > Connectors > Reporting > Traffic Monitoring Policies in the left menu bar.
4. Select the Rules tab in the horizontal menu bar. The following screen displays.

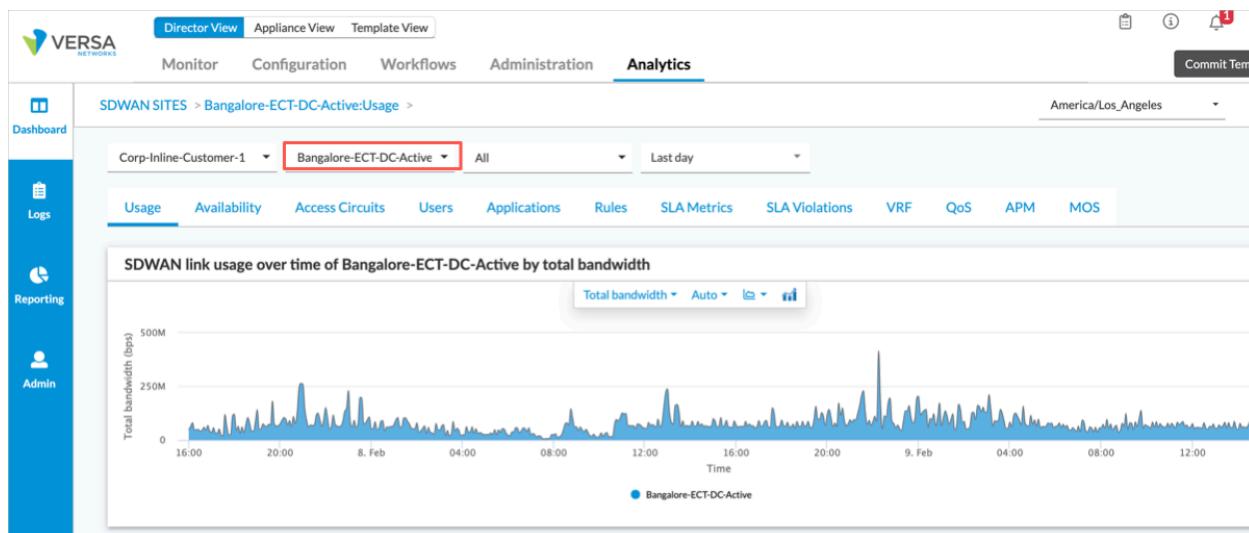
Rule Num	Name	Rule Disabled	Source	Destination
No Rules Added				

5. Click an existing rule or click + Add. The Add/Edit Rules popup window displays.
6. Select the Enforce tab. The following screen displays.



7. Scroll down to the Performance Monitoring pane and select a LEF profile from the drop-down menu to associate it with the policy rule, or click Default Profile to use the default LEF profile.
8. Click TCP Monitoring.
9. Click OK.

For logs sent to Analytics clusters, to display the Passive APM dashboard, select Analytics > Dashboards > Sites in the left menu bar. Then, in the main pane, select a VOS device from the second drop-down menu to display the site details dashboard for the selected VOS device.



On the site details dashboard, select the APM tab and then select the Passive APM tab.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

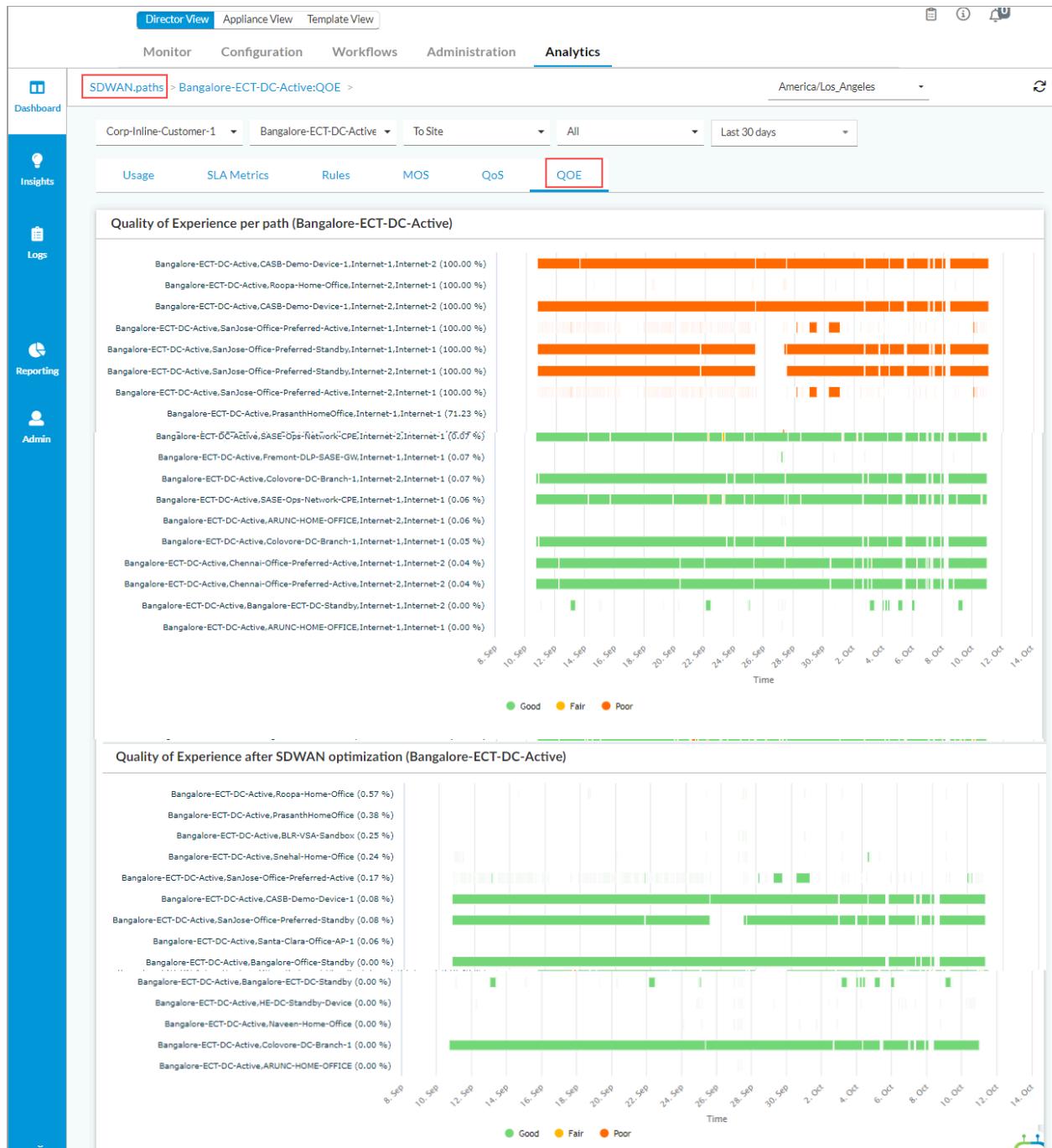
The screenshot shows the Versa Director View interface with the Analytics tab selected. The left sidebar includes Dashboard, Logs, Reporting, and Admin sections. The main content area displays two charts: a donut chart titled "Application performance of Bangalore-ECT-DC-A..." and a bar chart titled "Application performance over time of Bangalore-ECT-DC-Active by network response time". The APM tab is highlighted with a red box.

Configure SD-WAN Traffic-Conditioning Logging

- Syslog identifier—sdwanPathCondLog
- Path to the configuration screen—Analytics Data Configurations > SD-WAN Traffic Condition

SD-WAN path-conditioning logs are used to determine the quality of experience after SD-WAN optimization. To export SD-WAN path-conditioning logs, configure a default LEF profile.

For logs sent to Analytics clusters, to display the SD-WAN path conditioning dashboards, select Analytics > Dashboards > SD-WAN > Path in the left menu bar, and then select the QoE tab in the horizontal menu bar.



Configure SD-WAN Traffic and Web-Monitoring Logging

- Syslog identifiers—[flowIdLog](#), flowMonLog, flowMonHttpLog
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > Traffic Monitoring Logs, Search Data Configurations > HTTP Traffic Monitoring Logs:

You can export traffic-monitoring logs in two ways. To configure globally for all flows (both allow and deny flows), you

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

select parameters in the LEF logging control configuration; otherwise, you configure by traffic-monitoring policy rule. For more information about configuring logging control and traffic monitoring policy, see [Configure Log Export Functionality](#).

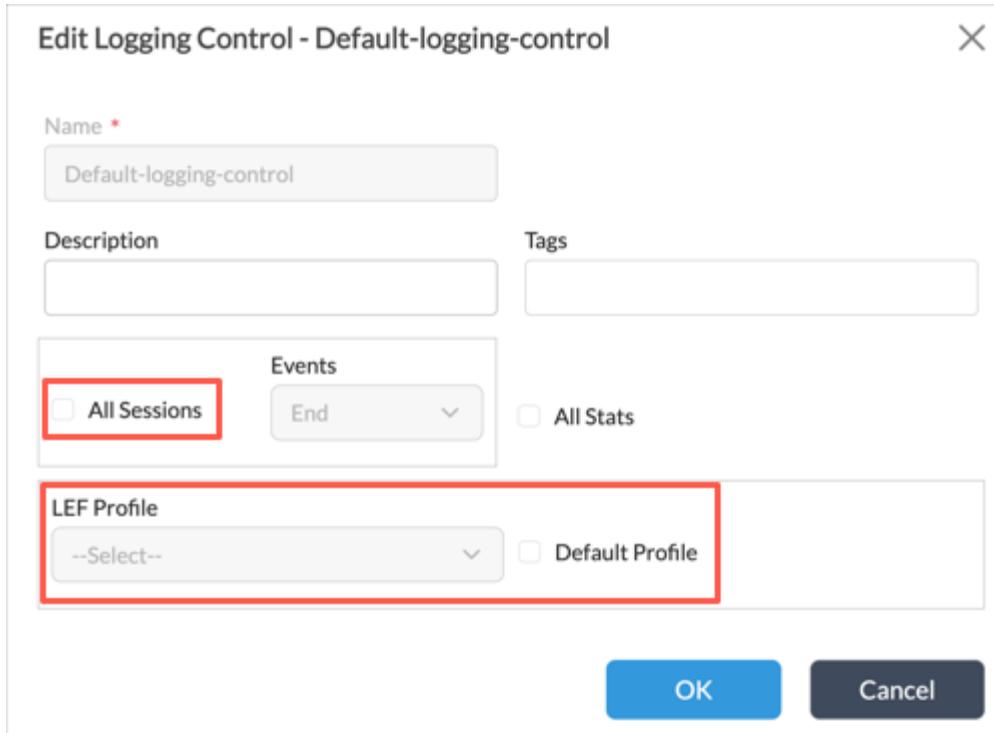
To export web-monitoring logs, select the Send HTTP Metadata for HTTP Sessions option when you configure traffic-monitoring policy.

To export traffic-monitoring logs globally for all flows:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Objects & Connectors > Connectors > Reporting > Logging Control in the left menu bar. The following screen displays.

Name	All Sessions	All Stats	LEF Profile
Default-Logging-Control	Active	Enabled	Default-Logging-Profile

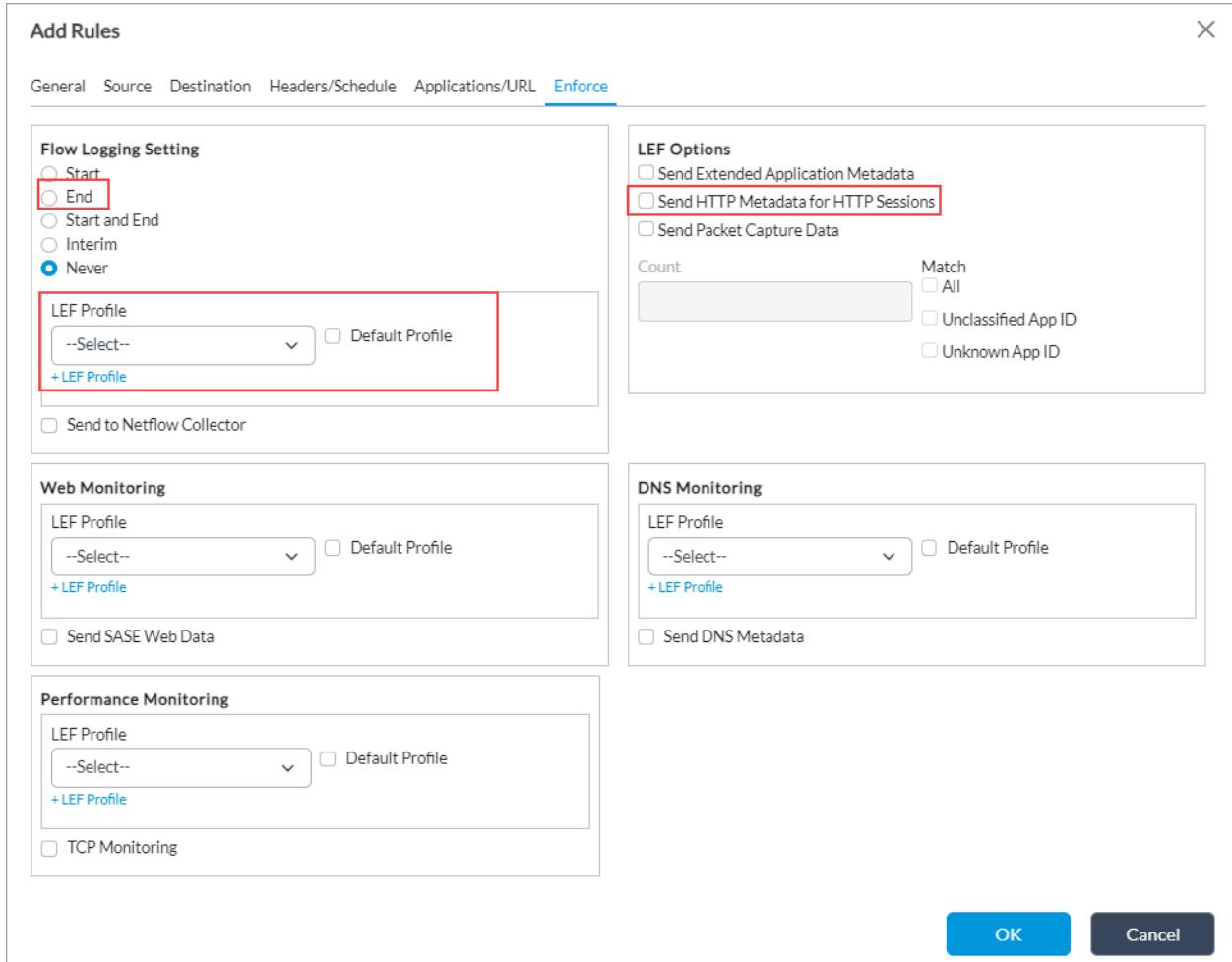
4. In the main pane, if a logging control entry exists click the name of the entry. If no entry exists, click +Add. The Edit/Add Logging Control popup window displays.



5. Click All Sessions and then either select a LEF profile or click Default Profile to use the default LEF profile. If adding a new logging control entry, enter a name in the Name field.
6. Click OK.

To export traffic-monitoring and web-monitoring logs using a traffic-monitoring policy rule:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Objects & Connectors > Connectors > Reporting > Traffic Monitoring Policy in the left menu bar
4. Select the Rules tab in the horizontal menu bar.
5. Select an existing rule, or select Add to add a new rule. The Add/Edit Rules popup window displays.
6. Select the Enforce tab. The following screen displays.



7. To send traffic-monitoring logs to the active collector for a LEF profile:
 - a. In the Flow Logging Setting group of fields, select End.
 - b. Select a LEF profile, or click Default Profile to use the default LEF profile.
8. To include application metadata, such as application risk, productivity, family, and subfamily, in traffic-monitoring logs click Send Extended Application Metadata.
9. To send web-monitoring logs to the active collector for a LEF profile:
 - a. In the LEF Options group of fields, click Send HTTP Metadata for HTTP Sessions.
 - b. Select a LEF profile, or click the Default Profile to use the default LEF profile.
10. Click OK.

For logs sent to Analytics clusters, to display the SD-WAN traffic-monitoring logs, select Analytics > Logs > Traffic Monitoring in the left menu bar.

Screenshot of the Director View interface showing the Analytics section for Traffic Monitoring. The left sidebar includes Dashboard, Insights, Logs, Reporting, and Admin sections. The main content area shows a table of generic traffic monitoring logs from Colovore-DC-Branch-1 over the last 30 days.

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Protocol	Application	User
Oct 11th 2023, 12:29:27 AM PDT	Colovore-DC-Branch-1	10.192.121.239	10.100.228.46	40306	2222	tcp	unknown_tcp	Unknown
Oct 11th 2023, 12:29:27 AM PDT	Colovore-DC-Branch-1	10.192.121.239	10.100.227.184	42458	2222	tcp	unknown_tcp	Unknown
Oct 11th 2023, 12:29:26 AM PDT	Colovore-DC-Branch-1	10.192.121.239	10.100.230.62	39080	2222	tcp	unknown_tcp	Unknown
Oct 11th 2023, 12:29:26 AM PDT	Colovore-DC-Branch-1	10.192.121.239	10.100.228.4	48023	2222	tcp	unknown_tcp	Unknown
Oct 11th 2023, 12:29:26 AM PDT	Colovore-DC-Branch-1	172.30.60.249	10.48.94.250	51017	3080	tcp	http	gustavo@versa-net
Oct 11th 2023, 12:29:26 AM PDT	Colovore-DC-Branch-1	10.100.100.6	10.100.100.8	58510	2222	tcp	unknown_tcp	Unknown
Oct 11th 2023, 12:29:26 AM PDT	Colovore-DC-Branch-1	10.40.24.3	10.100.1.105	36490	8020	tcp	unknown_tcp	Unknown
Oct 11th 2023, 12:29:26 AM PDT	Colovore-DC-Branch-1	10.192.121.239	10.100.228.216	45996	2222	tcp	unknown_tcp	Unknown
Oct 11th 2023, 12:29:26 AM PDT	Colovore-DC-Branch-1	10.40.24.3	10.100.1.105	56298	8010	tcp	unknown_tcp	Unknown
Oct 11th 2023, 12:29:26 AM PDT	Colovore-DC-Branch-1	172.30.60.32	10.48.0.99	63941	53	udp	dns	ayush.lohiya@versa

For logs sent to Analytics clusters, to display the SD-WAN web-monitoring logs, select Analytics > Logs > Web Monitoring in the left menu bar.

Screenshot of the Director View interface showing the Analytics section for Web Monitoring. The left sidebar includes Dashboard, Insights, Logs, Reporting, and Admin sections. The main content area shows a table of HTTP traffic monitoring logs from Colovore-DC-Branch-1 over the last 30 days.

Receive Time	Appliance	Application	User	URL Category	Source Address	Destination Address	Source Port
Oct 11th 2023, 12:34:24 AM PDT	Colovore-DC-Branch-1	http	kyle.murray@versa-networks.com	private_ip_addresses	172.30.60.151	10.43.4.34	50350
Oct 11th 2023, 12:34:24 AM PDT	Colovore-DC-Branch-1	http	kyle.murray@versa-networks.com	private_ip_addresses	172.30.60.151	10.43.4.34	50351
Oct 11th 2023, 12:34:23 AM PDT	Colovore-DC-Branch-1	http	kyle.murray@versa-networks.com	private_ip_addresses	172.30.60.151	10.43.4.34	50346
Oct 11th 2023, 12:34:23 AM PDT	Colovore-DC-Branch-1	http	kyle.murray@versa-networks.com	private_ip_addresses	172.30.60.151	10.43.4.34	50347
Oct 11th 2023, 12:34:19 AM PDT	Colovore-DC-Branch-1	http	kyle.murray@versa-networks.com	private_ip_addresses	172.30.60.151	10.43.4.34	50340
Oct 11th 2023, 12:34:19 AM PDT	Colovore-DC-Branch-1	http	kyle.murray@versa-networks.com	private_ip_addresses	172.30.60.151	10.43.4.34	50341
Oct 11th 2023, 12:34:19 AM PDT	Colovore-DC-Branch-1	http	kyle.murray@versa-networks.com	private_ip_addresses	172.30.60.151	10.43.4.34	50344
Oct 11th 2023, 12:34:19 AM PDT	Colovore-DC-Branch-1	http	kyle.murray@versa-networks.com	private_ip_addresses	172.30.60.151	10.43.4.34	50345
Oct 11th 2023, 12:34:18 AM PDT	Colovore-DC-Branch-1	http	kyle.murray@versa-networks.com	private_ip_addresses	172.30.60.151	10.43.4.34	50339
Oct 11th 2023, 12:34:17 AM PDT	Colovore-DC-Branch-1	http	kyle.murray@versa-networks.com	private_ip_addresses	172.30.60.151	10.43.4.34	50332

[https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Export)

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

Configure SD-WAN Traffic-Monitoring Summary Logging

- Syslog identifiers—[bwMonLog](#), eventLog

To export traffic-monitoring summary logs, click All Stats in the logging control configuration. For information about configuring logging control, see [Configure Log Export Functionality](#).

To export traffic monitoring summary logs:

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Devices > Devices in the horizontal menu bar.
 - Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - Select a VOS device in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.,
- Select Objects & Connectors > Connectors > Reporting > Logging Control in the left menu bar. The following screen displays.

The screenshot shows the Director View Appliance View interface. The Configuration tab is selected in the top navigation bar. The left sidebar shows the navigation path: Objects & Connectors > Connectors > Reporting > Logging Control. The 'Logging Control' link is highlighted with a red box. The main pane displays a table with columns: Name, All Sessions, All Stats, and LEF Profile. A message 'No Logging Control Added' is shown above the table, and a blue 'Add' button is at the bottom.

- Click a logging control entry in the main pane. The Edit Logging Control window displays.

Add Logging Control

X

Name *

Description

Tags

Events

All Sessions

All Stats

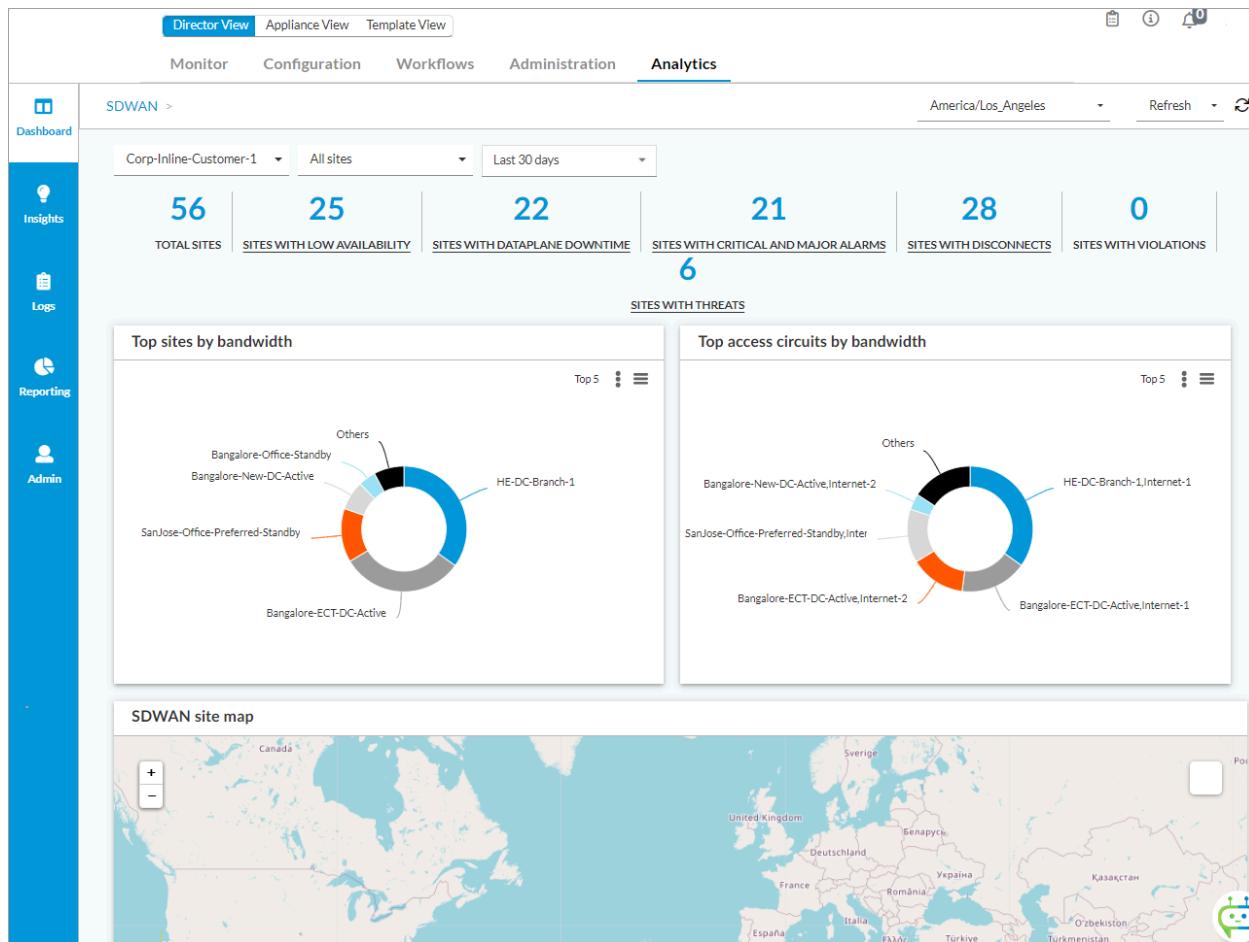
LEF Profile

--Select-- Default Profile

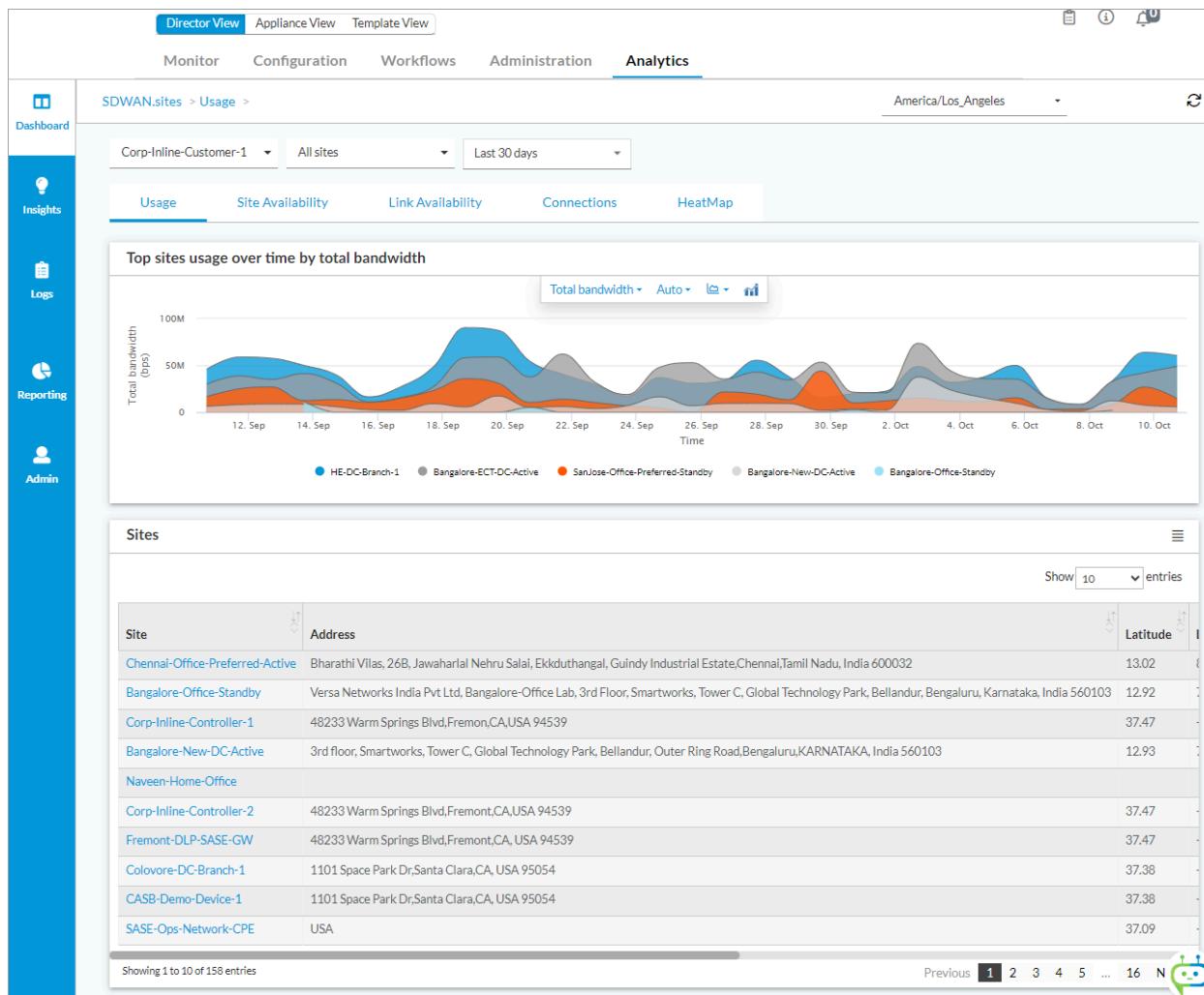
OK Cancel

5. Click All Stats, and then either select a LEF profile or click Default Profile to use the default LEF profile.
6. Click OK.

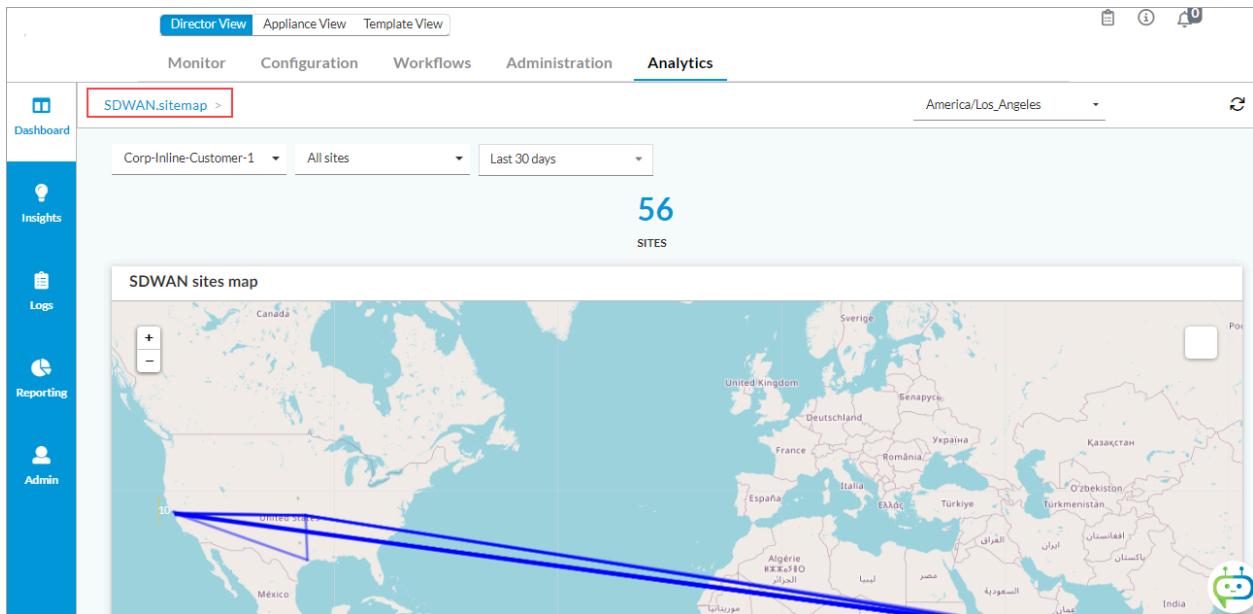
For logs sent to Analytics clusters, to display the SD-WAN traffic-monitoring summary dashboards, select Analytics > Dashboards > SD-WAN in the left menu bar.



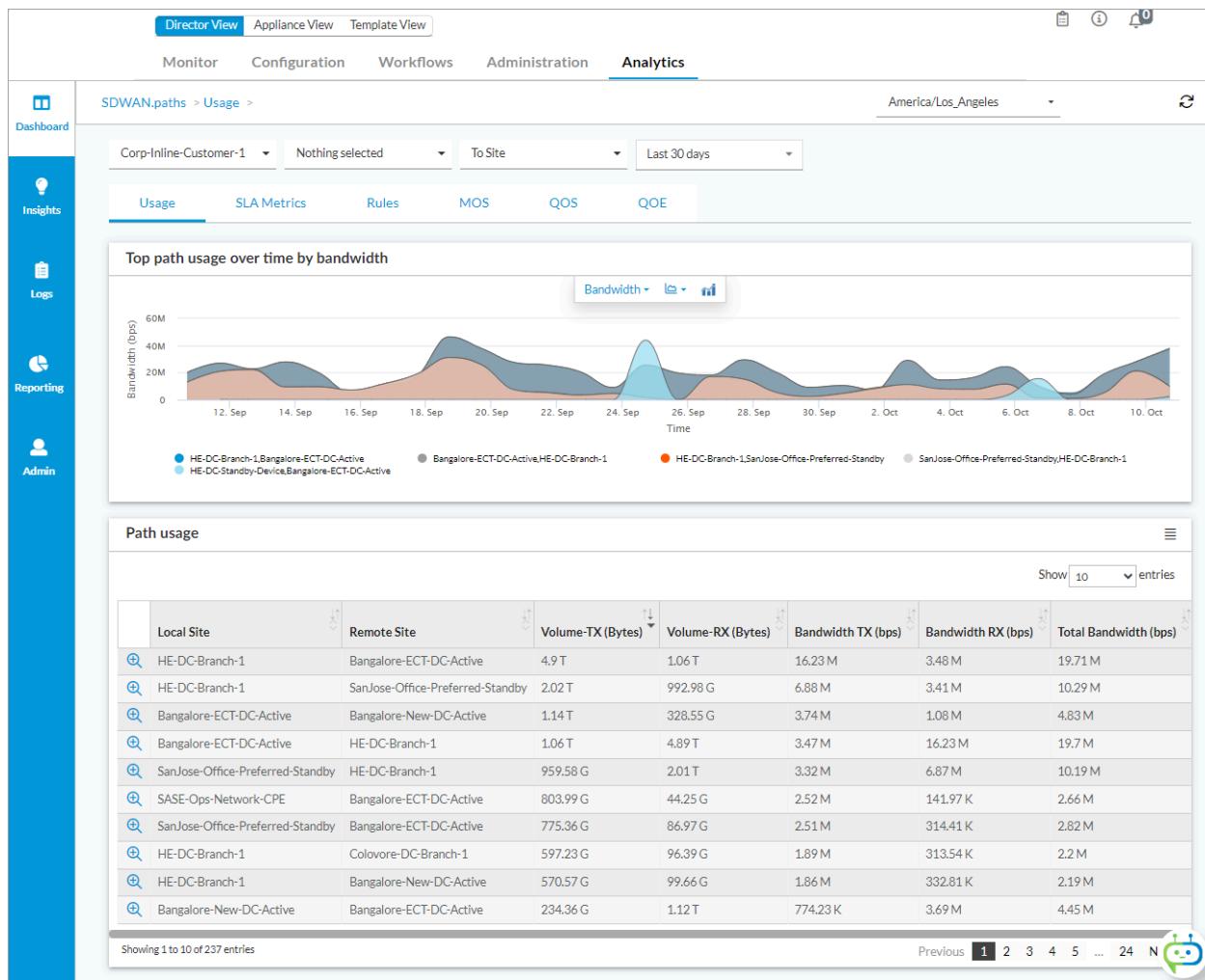
For logs sent to Analytics clusters, to display the SD-WAN traffic monitoring by sites, select Analytics > Dashboards > SD-WAN > Sites in the left menu bar.



For logs sent to Analytics clusters, to display the SD-WAN traffic monitoring by site map, select Analytics > Dashboards > SD-WAN > Sites Map in the left menu bar.



For logs sent to Analytics clusters, to display the SD-WAN traffic monitoring by path, select Analytics > Dashboards > SD-WAN > Paths in the left menu bar, and then select the Usage tab in the horizontal menu bar.



Configure System Load Logging

- Syslog identifier—`systemLoadLog`
- Path to the configuration screen—Analytics Data Configurations > System load

To export VOS device load logs, configure a default LEF profile. A system health log is exported from each VOS device every 5 minutes. These logs are exported in provider organization (appliance owner) context on multi-tenant VOS devices.

For logs sent to Analytics clusters, to display the appliance health-monitoring dashboard, select Analytics > Dashboards > System in the left menu bar, and then select the Appliance Health tab in the horizontal menu bar. For multi-tenant VOS devices, select the provider organization from the drop-down menu in the main pane.

The screenshot shows the Director View interface with the Analytics tab selected. The left sidebar has sections for Dashboard, Insights, Logs, Reporting, and Admin. The main pane is titled "SYSTEM.interfaces > Appliance health >" and shows a table of appliance health monitoring data. The table has columns for Appliance, CPU Load (%), Memory Load (%), Disk Load (%), and Sessions Load. Two entries are listed: Chaganti-Office and PrasanthiHomeOffice.

Appliance	CPU Load (%)	Memory Load (%)	Disk Load (%)	Sessions Load
Chaganti-Office	2.00%	59.00%	8.00%	39
PrasanthiHomeOffice	2.00%	50.00%	9.00%	7

Configure Threat Logging

- Syslog identifiers—[avLog](#), [dosThreatLog](#), [idpLog](#), ipfLog, urlfLog
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > Antivirus logs, Search Data Configurations > DoS threat logs, Search Data Configurations > IDP logs, Search Data Configurations > URL filtering logs

Threat logs include logs for antivirus, DoS, IDP, IP filtering, and URL filtering. All the threat logs are per-flow logs. If you enable threat events, the threat logs are only a small percentage of the actual traffic. Threat logs sent to Analytics clusters can be kept in the database for a configurable number of days; the default is 30 days.

To export threat logs, associate a LEF profile with the antivirus, DoS, IDP, IP-filtering, and URL-filtering configurations.

Configure Antivirus (Malware) Logging

For information about configuring antivirus, see [Configure Antivirus](#).

To configure antivirus (malware) logging:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Services > Next-Gen Firewall > Security > Profiles > Antivirus in the left menu bar. The following screen displays.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

4. Select an existing profile, or click the Add icon to add a new profile. The Add/Edit Antivirus Profile popup window displays.

	Name	Severity	OS	Product	Application	Action
No Rule Added						

5. In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...
 Updated: Wed, 23 Oct 2024 08:27:55 GMT
 Copyright © 2024, Versa Networks, Inc.

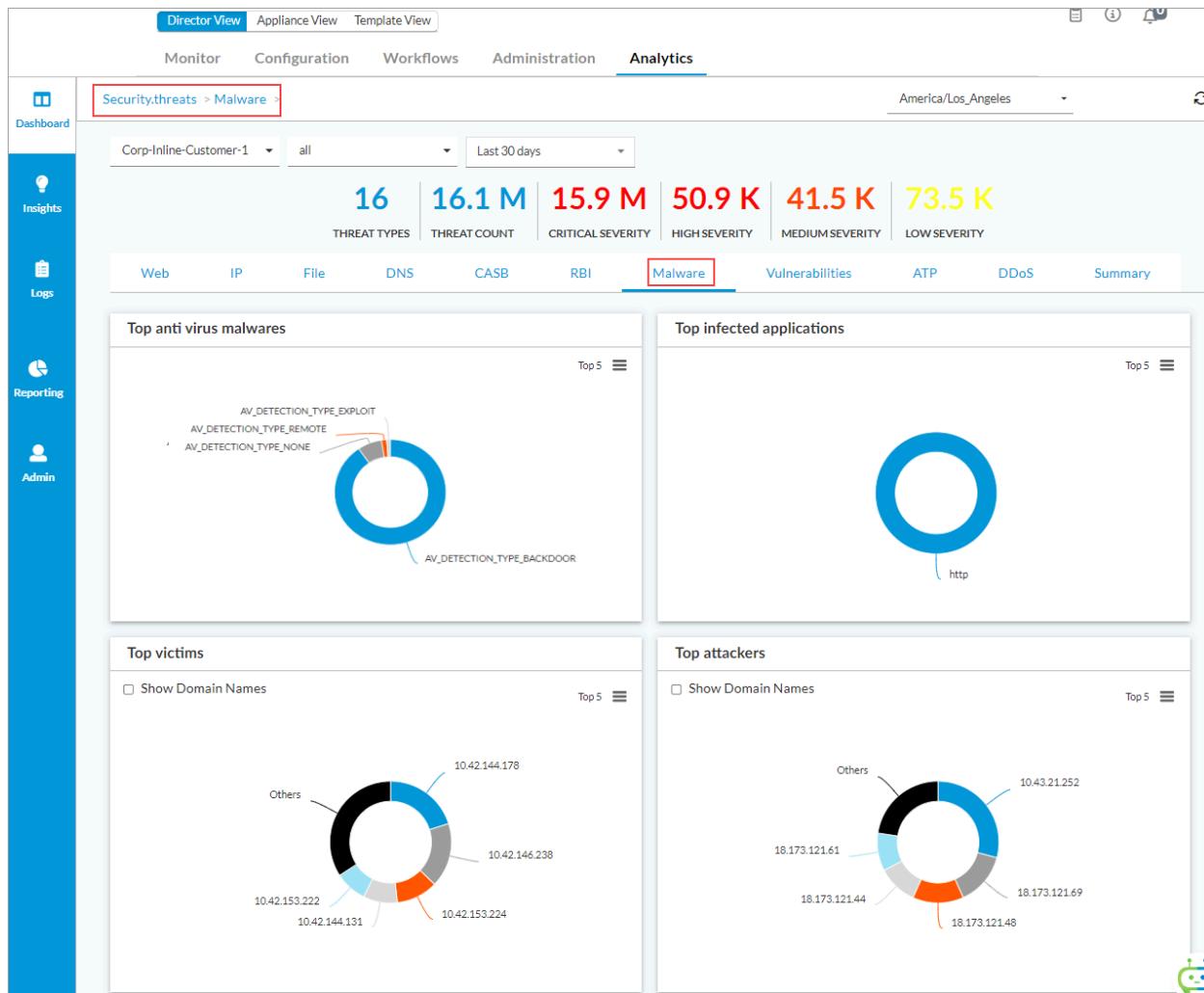
6. Click OK.

For logs sent to Analytics clusters, to display the antivirus (malware) threats log screen, select Analytics > Logs > Threat Detection in the left menu bar, and then select the Antivirus tab in the horizontal menu bar.

The screenshot shows the Versa Director interface with the following details:

- Left Sidebar:** Includes icons for Dashboard, Insights, Logs (highlighted with a red box), Reporting, and Admin.
- Top Navigation:** Director View, Appliance View, Template View, Monitor, Configuration, Workflows, Administration, and Analytics (highlighted with a blue underline).
- Sub-Header:** Threat Detection Logs > Anti Virus > (highlighted with a red box).
- Region Selection:** America/Los_Angeles.
- Filter Options:** Corp-Inline-Customer-1, all, Last 30 days.
- Tab Selection:** Anti Virus (highlighted with a red box), IDP, IPGuard, DDoS, CASB, RBI, VFP, ATP.
- Section Title:** Anti virus log.
- Filtering:** Show Domain Names, Set filters here..., Apply | Clear | Copy Filter.
- Table Headers:** Receive Time, Appliance, Threat Severity, Malware Name, Malware Type, Application, User, Attacker.
- Table Data:** A list of log entries showing detections from Oct 9th to Oct 10th, 2023, across various appliances and threat types (critical, Archive Bomb, EICAR_Test_File). The table includes columns for Application, User, and Attacker, with some entries showing Unknown values.

For logs sent to Analytics clusters, to display the Antivirus (Malware) Threats dashboard, select Analytics > Dashboards > Security > Threats in the left menu bar, and then select the Malware tab:



Configure DDoS Threats Logging

For information about configuring DoS, see [Configure DoS Protection](#).

To configuration DDoS threat logging:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Services > Next-Gen Firewall > DoS > Policies in the left menu bar. The following screen displays.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

The screenshot shows the Director View Configuration interface. The top navigation bar includes tabs for Director View, Appliance View (selected), and Template View. Below the navigation is a sub-navigation bar with Monitor, Analytics, Configuration (selected), and Administration. The main area shows an Appliance named BR1 and an Organization named Provider-ORG. A message indicates the current view is Appliance View. On the left, a sidebar lists Networking, Services, Objects & Connectors, and Others, with CGNAT selected. Under CGNAT, the Next Gen Firewall section is expanded, showing DoS, Authentication, Decryption, and Security. The DoS section is selected, and its Policies tab is highlighted with a red box. The main content area displays a table for Default-Policy rules, with columns for Rule Num, Name, Rule Disabled, Source (Zone, Region, Address, Address Group, Zone, Region), and an Add button. A search bar and a dropdown menu are also present.

4. Click the Add icon. The Add DoS Rule popup window displays.
5. Select the Enforce tab. The following window displays.

The screenshot shows the Add DoS Rule dialog box. The Enforce tab is selected. The Action Setting section contains radio buttons for Allow (selected), Deny, and Protect. The Logging Setting section contains a dropdown menu for LEF Profile (with options --Select-- and Default Profile) and a checkbox for Default Profile, which is checked. The DDoS Profile section contains dropdown menus for Aggregate Profile (with option --Select--) and Classified Profile (with option --Select--). At the bottom are OK and Cancel buttons.

6. In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile.
7. Click OK.

For logs sent to Analytics clusters, to display the DDoS threats log screen, select Analytics > Logs > Threat Detection in the left menu bar, and then select the DDoS tab in the horizontal menu bar.

For logs sent to Analytics clusters, to display the DDoS threats dashboard, select Analytics > Dashboards > Security > Threats in the left menu bar, and then select the DDoS tab in the horizontal menu bar.

Configure IP Threats Logging

To reduce the number of logs generated, you can enable only deny-listed IP filters. You cannot enable all IP addresses.

For information about configuring IP filtering, see [Configure IP Filtering](#).

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Apply_Log_Expo...

Updated: Wed, 23 Oct 2024 08:27:55 GMT

Copyright © 2024, Versa Networks, Inc.

name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.

- d. 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 Services > Next-Gen Firewall > Security > Profiles > IP Filtering in the left menu bar. The following screen displays.

The screenshot shows the Versa Director View interface. The top navigation bar includes Director View, Appliance View (selected), Template View, and various status icons. The main menu tabs are Monitor, Analytics, Configuration (selected), and Administration. The left sidebar shows the appliance selection (BR1) and organization (Provider-ORG). The configuration path is: CGNAT > Next Gen Firewall > Security > Profiles > IP Filtering. The 'IP Filtering' link is highlighted with a red box. The main pane displays a table with columns: Name, Deny List, Deny List Action, Allow List, LEF Profile, GeoIP Based Actions, Reputation-Based Action, and Address Reverse Looku. A message indicates 'No IP Filter Added'. A large blue 'Add' button is centered at the bottom of the table area.

4. Click the + Add icon. The Add IP Filter popup window displays.

Add IP Filter

Name *

Description

Tags

Default Action

--Select-- Prioritize URL Reputation

Allow URL Reputation *

--Select--

LEF Profile

--Select-- Default Profile

Deny List [Allow List](#) [GeoIP Based Actions](#) [Reputation-Based Actions](#) [Address Reverse Lookup](#)

Deny List Action

--Select--

Match Type

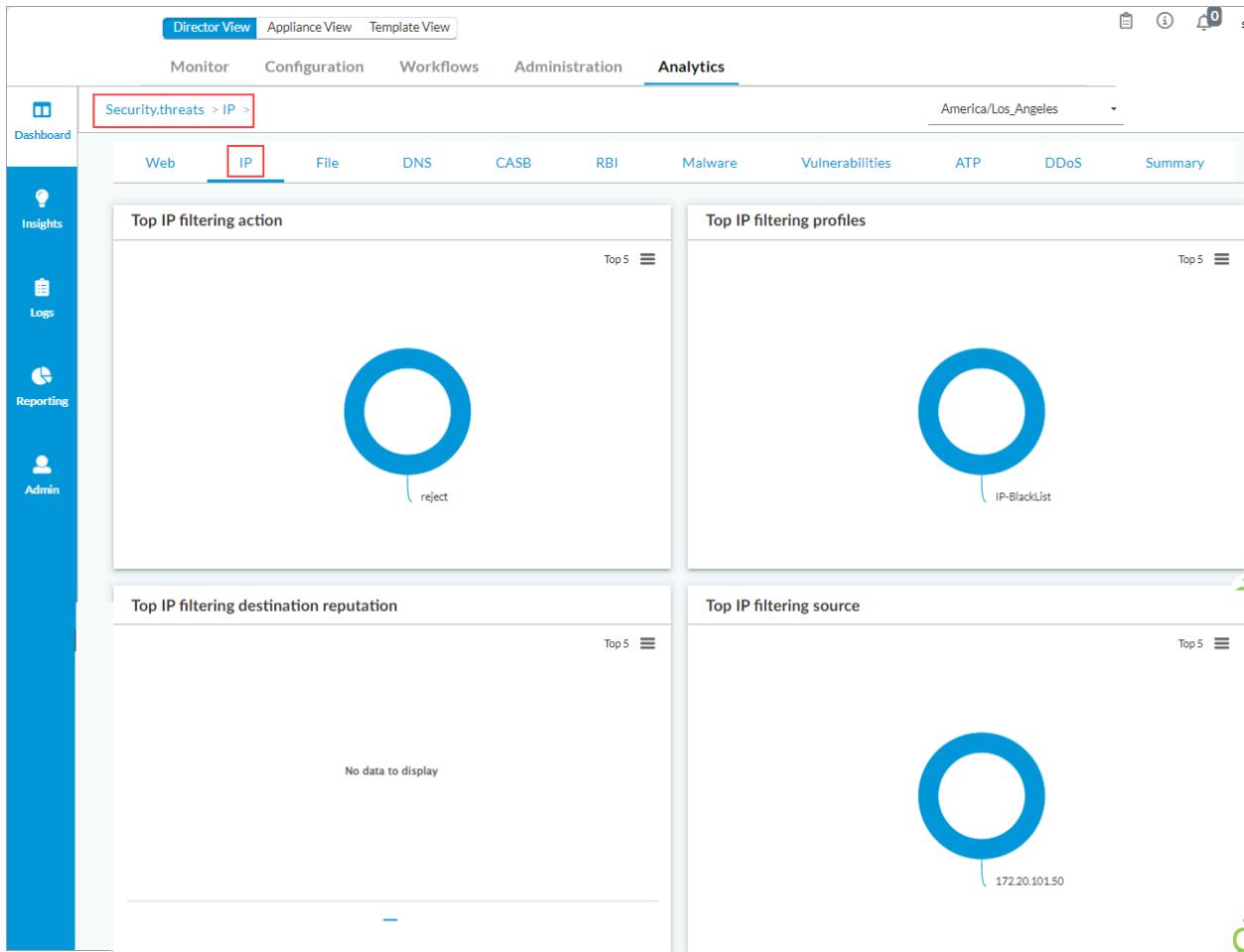
--Select--

IP Address IP Address Group

OK **Cancel**

5. In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile.
6. Click OK.

To display the IP threats dashboard, select Analytics > Dashboard > Security > Threats in the left menu bar, and then select the IP tab in the horizontal menu bar.



Configure IDP Threat Detection Vulnerability Logging

For information about configuring IDP, see [Configure Intrusion Detection and Prevention](#).

To enable vulnerability (IDP) logging:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Services > Next-Gen Firewall > Security > Profiles > Vulnerability in the left menu bar. The following screen displays.

The screenshot shows the 'Configuration' tab selected in the top navigation bar. Under 'Appliance' (BR1) and 'Organization' (Provider-ORG), the 'Vulnerability' profile is highlighted. A search bar and a table for managing vulnerability profiles are visible. The table has columns: Name, Rule Count, Exception Count, Name, Direction, Action, Severity, and OS. A blue 'Add' button is located at the bottom right of the table area.

- Click the Add icon. The Add Vulnerability Profile popup window displays.

The dialog box is titled 'Add Vulnerability Profile'. It contains fields for 'Name' (with a red asterisk), 'Description', and 'Tags'. A dropdown menu for 'LEF Profile' is shown, with an option '--Select--' highlighted by a red box. A checkbox for 'Default Profile' is also present. Below this, there are tabs for 'Rule' (selected) and 'Exceptions'. The 'Rule' tab shows a table with columns: Name, Severity, OS, Product, Application, and Action. A message 'No Rule Added' is displayed. At the bottom are 'OK' and 'Cancel' buttons.

- In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile.
- Click OK.

For logs sent to Analytics clusters, to display the IDP threat detection vulnerability dashboard, select Analytics > Logs > Threat Detection in the left menu bar, and then select the IDP tab in the horizontal menu bar.

The screenshot shows the Director View interface with the following details:

- Top Navigation:** Director View, Appliance View, Template View, Monitor, Configuration, Workflows, Administration, **Analytics** (selected).
- Left Sidebar:** Dashboard, Insights, **Logs** (selected), Reporting, Admin.
- Current Path:** Threat Detection Logs > IDP > IDP log.
- Filter Bar:** Anti Virus, **IDP** (selected), IPGuard, DDoS, CASB, RBI, VFP, ATP.
- Log Table Headers:** Receive Time, Appliance, Threat Severity, Threat Type, Application, User, Signature Message, Class.
- Log Data:** A table showing 10 entries of IDP logs from Oct 5th 2023, 12:09:59 PM PDT, categorized by Threat Type (e.g., web-application-attack, attempted-recon) and Application (e.g., linkedin, nationalgeographic, nfl, skype).

Configure URL-Filtering Threats Logging

To reduce the number of URL-filtering logs generated, you can enable only deny-listed URL profile logging. You cannot enable logging for all URLs. For information about configuring URL filtering, see [Configure URL Filtering](#).

To enable URL-filtering logging:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.
 - d. 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 Services > Next-Gen Firewall > Security > Profiles > URL Filtering in the left menu bar. The following screen displays.

The screenshot shows the Versa Networks Appliance View Configuration interface. The top navigation bar includes Director View, Appliance View (selected), and Template View. On the right, there are icons for file operations (New, Open, Save, Delete, Copy, Paste) and a notification bell with 0 messages. The main content area has tabs for Monitor, Analytics, Configuration (selected), and Administration. A sub-header indicates the current view is Appliance View for SDWAN-Branch1, with an Organization set to provider-org. A message says "You are currently in Appliance View". Below this, a search bar and a table list URL filter profiles. The table columns are Name, Deny List, Deny List Action, Allow List, and Category Based Action. One row is selected, labeled "URL-filter-profile-1" with "Predefined: block". Navigation controls at the bottom include "Rows per page" (set to 25) and "Showing 1 - 1 of 1". The left sidebar contains a tree view of Next Gen Firewall settings, including DoS, Authentication, Decryption, Security (Policies and Profiles), IP Filtering, DNS Filtering, and URL Filtering.

- Click the Add icon. The Add URL Filter popup window displays.

The screenshot shows the "Add URL Filter" dialog box. It includes fields for Name (mandatory), Description, Tags, Default Action (dropdown menu with options like --Select--), and checkboxes for Decrypt Bypass and Cloud Lookup State. A section for LEF Profile is highlighted with a red box; it contains a dropdown menu with options like --Select-- and a checkbox for Default Profile. Below this are tabs for Deny List, Allow List, Category Based Action, and Reputation Based Action. The Deny List tab is selected. The Action section includes a dropdown menu for Action (with --Select-- option) and a checkbox for Evaluate Referrer. Below the Action section are two sections for Pattern and Strings, each with a table header and a "Not Configured" message. At the bottom are OK and Cancel buttons.

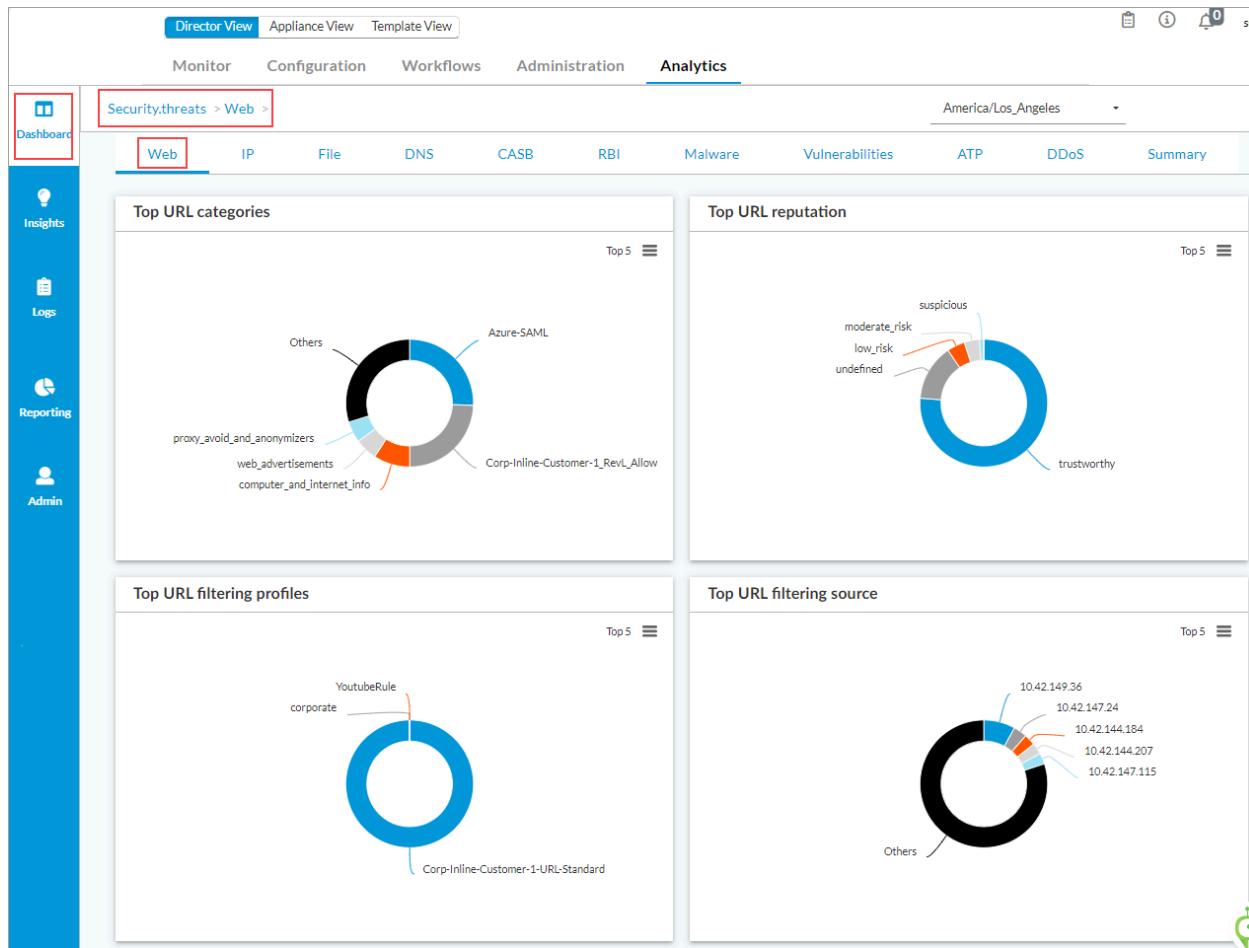
- In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile. This exports logs for URLs that match the deny list, category action , or reputation action.
- To also export logs for URLs that match the allow list , select the Allow List tab and then click Enable Logging.

Add URL Filter

Description	Tags
<input type="text"/>	
Default Action	
--Select--	<input type="checkbox"/> Decrypt Bypass <input type="checkbox"/> Cloud Lookup State
LEF Profile	
--Select--	<input type="checkbox"/> Default Profile
<input type="radio"/> Deny List <input checked="" type="radio"/> Allow List <input type="radio"/> Category Based Action <input type="radio"/> Reputation Based Action	
<input type="checkbox"/> Enable Logging <input checked="" type="checkbox"/> Evaluate Referrer	
<input type="checkbox"/> Pattern <small>①</small> <small>Pattern Not Configured</small>	<input type="checkbox"/> Strings <small>Strings Not Configured</small>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- Click OK.

For logs sent to Analytics clusters, to display the URL-filtering dashboard, select Analytics > Dashboards > Security > Threats in the left menu bar, and then select the Web tab in the horizontal menu bar.



For logs sent to Analytics clusters, to display the URL-filtering logs dashboard, select Analytics > Logs > Threat Filtering in the left menu bar, and then select the URL Filtering tab in the horizontal menu bar.

The screenshot shows the Director View interface with the Analytics tab selected. The URL Filtering Log table is displayed, listing various log entries. The columns in the table are: Receive Time, Appliance, Threat Severity, Application, User, URL Category, URL Reputation, and HTTP U. The table contains six rows of data, each with a timestamp from Oct 11th 2023, an appliance name (Bangalore-ECT-DC-Active), informational threat severity, and user details like darahas.k@versa-networks.com or masaru@versa-networks.com.

Configure TWAMP Logging

For Releases 21.2.1 and later.

- Syslog identifier—[twampSenderSessLog](#)
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Analytics Data Configurations > Measurement Stats

You can use the Two-Way Active Measurement Protocol (TWAMP) to measure metrics such as delay, delay variation, and loss between two IP endpoints that support the TWAMP sender and receiver functionality. TWAMP logs include these metrics, which are recorded by IP session.

To export TWAMP logs, select a LEF profile when configuring TWAMP sessions. For information about configuring TWAMP, see [Configure Two-Way Active Measurement Protocol](#).

To export TWAMP logs from a VOS device:

1. In Appliance view, select Networking > TWAMP > Light.
2. In the main pane, click the Edit icon in the LEF pane.

The screenshot shows the Versa Director View interface. At the top, there are tabs for Director View, Appliance View (which is selected), and Template View. Below the tabs, there are sections for Monitor, Analytics, Configuration (selected), and Administration. Under Configuration, there are sub-sections for Appliance (set to Bangalore-ECT-DC-Ac) and Organization (set to Corp-Inline-Provider). A message at the top right says "You are currently in Appliance View". On the left, there's a sidebar with icons for Networking, Services, Objects & Connectors, and Others, followed by a search bar and a list of virtual routers, switches, and other network components. The main area shows a sub-menu for 'LEF' with three tabs: LEF, Session Sender, and Session Reflector. The 'Edit' button in the LEF sub-menu is highlighted with a red box.

3. Click Enable, and then select a LEF profile, or click Profile Default to use the default LEF profile.

This is a configuration dialog box for the LEF tab. It contains three fields: 'Enable' with a checked checkbox, 'Profile' with a dropdown menu showing '---Please Select---', and 'Profile Default' with an unchecked checkbox. At the bottom are two buttons: 'Cancel' and 'Confirm', with 'Confirm' being highlighted in blue.

4. Click Confirm.

For logs sent to Analytics clusters, to display TWAMP logs, select the Analytics tab in the top menu bar, and then select Dashboards > System > Measurements in the left menu bar.

The screenshot shows the Versa Director View interface. The top navigation bar includes Director View, Appliance View, Template View, Monitor, Configuration, Workflows, Administration, and Analytics. The Analytics tab is selected. On the left, there's a vertical sidebar with icons for Dashboard, Logs, Reporting, and Admin. The main content area displays a table titled 'Two Way Active Measurements Protocol' with columns for Appliance, Source Address, Destination Address, DSCP, VRF Name, Packets Size (Bytes), Packets Count, Packets Loss, TX Packets, RX Packets, and TX. A dropdown menu at the top left shows 'Corp-Inline-Customer-1' and 'Last day'. A dropdown menu at the top right shows 'America/Los_Angeles'. A 'Commit Tem' button is in the top right corner.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 21.1.1 adds support for ADC logging.
- Release 21.2.1 adds support for TWAMP logging.
- Release 22.1.1 adds support for DNS-monitoring logs, QoS monitoring logs by forwarding class, and SASE web-monitoring logs. You can select a LEF profile to be used for alarms.
- Release 22.1.3 adds support for DEM, DLP, and EIP logging.
- Release 22.1.4 adds support for ATP and SASE-for-SIM logging.

Additional Information

[Analytics Dashboards by Title](#)

[Analytics Log Screens by Title](#)

[Analytics Log Collector Log Types Overview](#)

[Configure Antivirus](#)

[Configure CGNAT](#)

[Configure CoS](#)

[Configure DHCP](#)

[Configure Digital Experience Monitoring](#)

[Configure DNS Filtering](#)

[Configure DoS Protection](#)

[Configure Microsegmentation](#)

[Configure File Filtering](#)

[Configure Firewall and SD-WAN Usage Monitoring Controls](#)

[Configure Intrusion Detection and Prevention](#)

[Configure IP Filtering](#)

[Configure Log Export Functionality](#)
[Configure MOS Score Monitoring](#)
[Configure NGFW](#)
[Configure SD-WAN Policy](#)
[Configure SLA Monitoring for SD-WAN Traffic Steering](#)
[Configure the Versa Advanced Logging Service](#)
[Configure URL Filtering](#)
[Configure TWAMP Control Client and Server Sessions](#)
[Versa Analytics Configuration Concepts](#)
[View Digital Experience Monitoring Dashboards](#)