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.

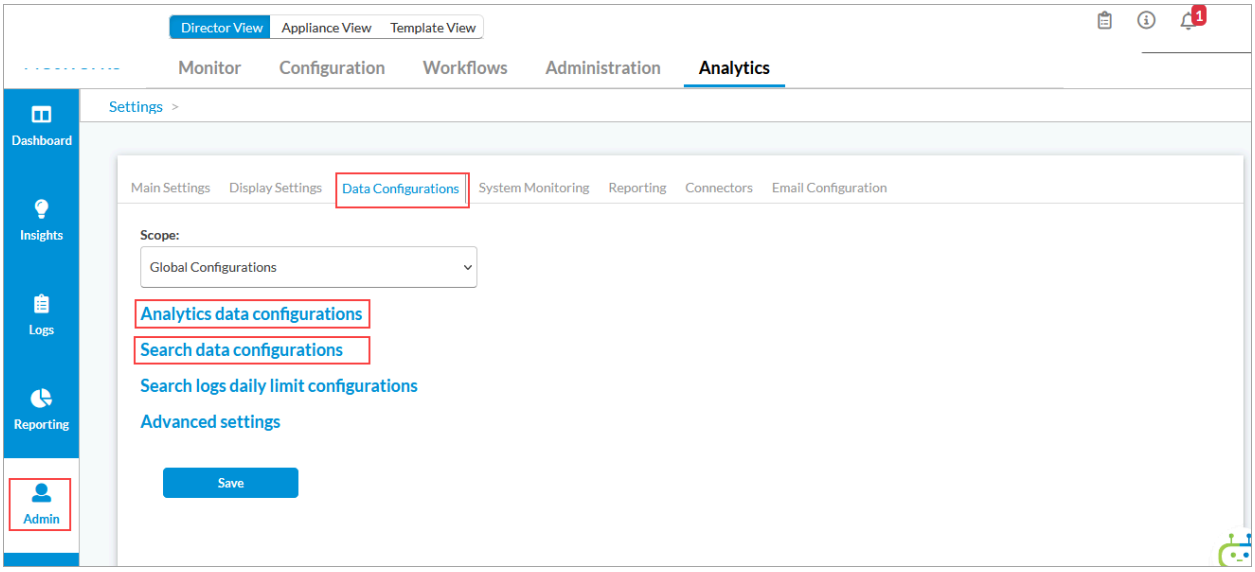
This section provides the GUI navigation instructions and field values for configuring only logs. In addition to configuring logs, you must also do the following:

- 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.



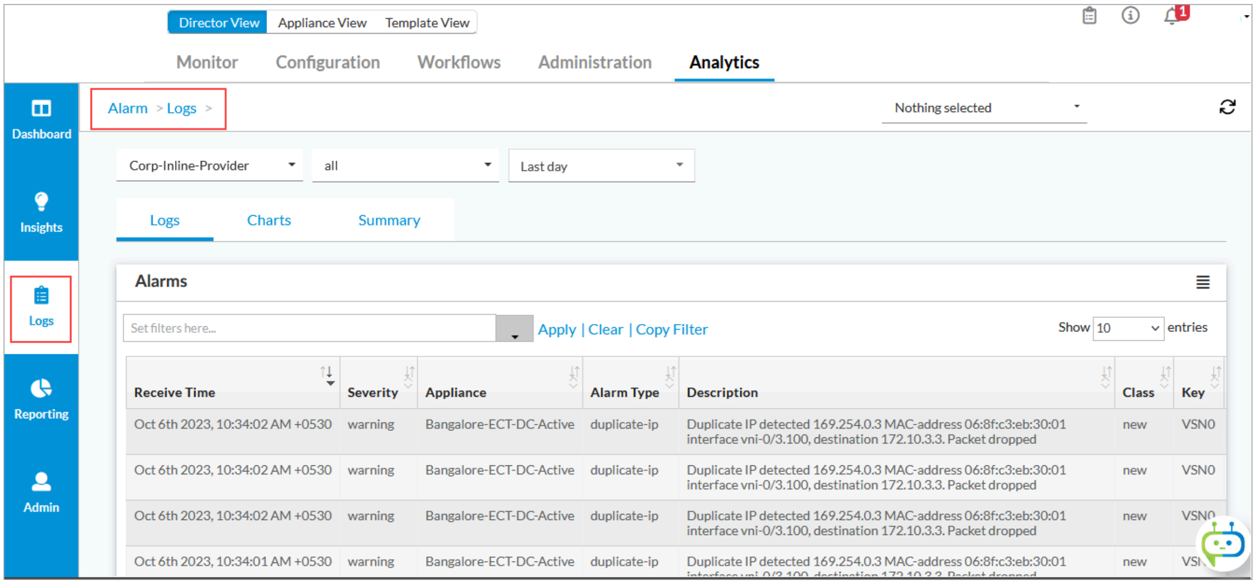
Configure Alarm Logging

- 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.



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.

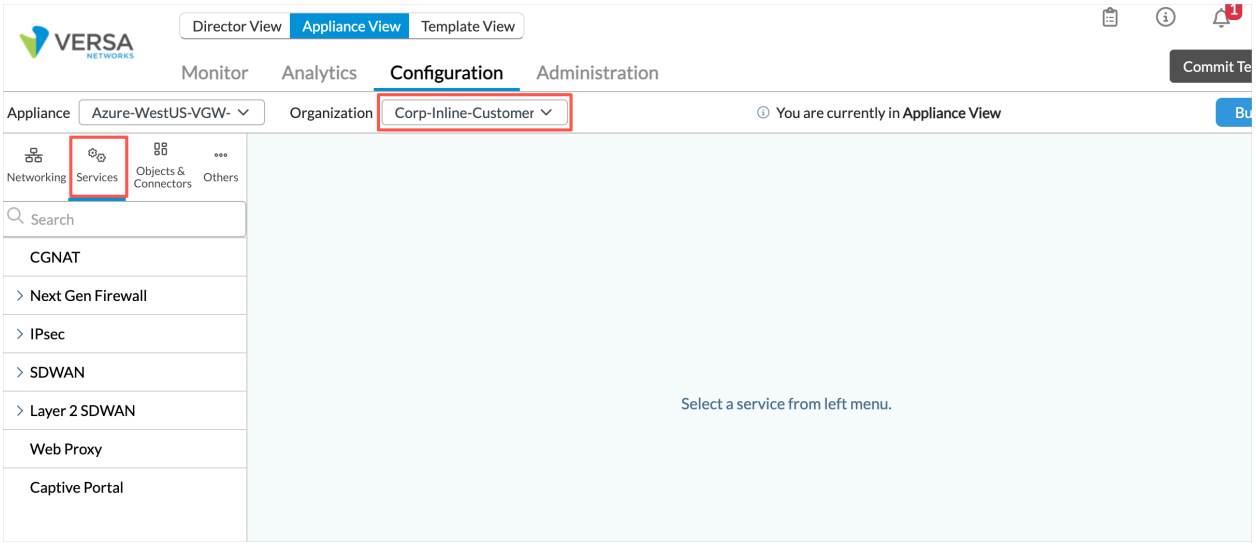
- Syslog identifiers—sandboxLog
- Path to the configuration screen—Search Data Configurations > Security > ATP Logs

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.

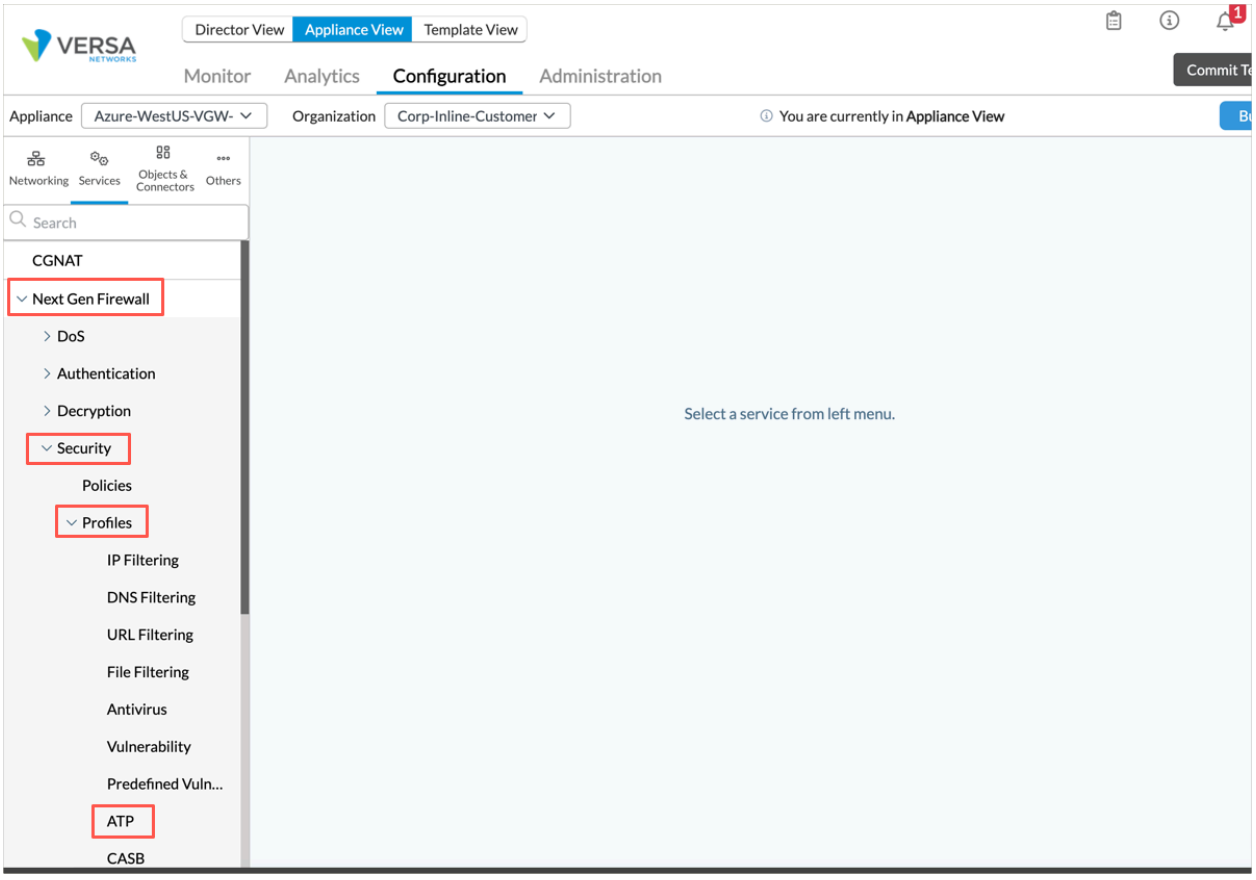
For a list of verdicts, see ATP Logs.

To configure ATP logging:

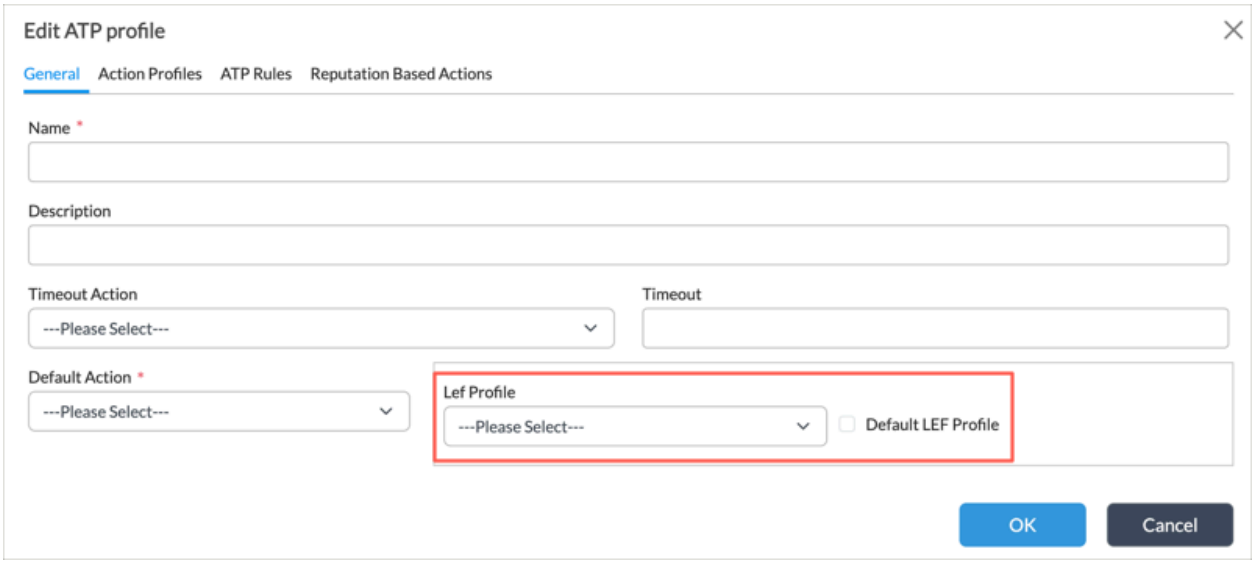
1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select the gateway in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services in the left menu bar.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



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

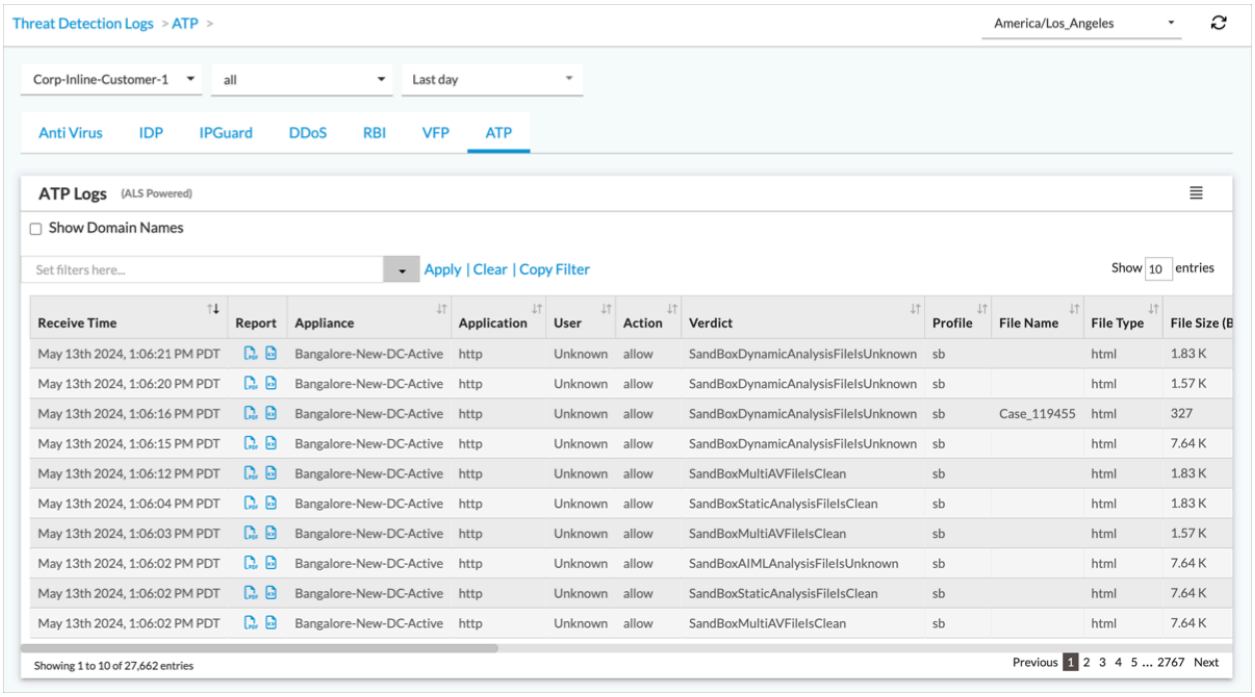


5. Select Next-Gen Firewall > Security > Profiles > ATP in the left menu bar.
6. In the main pane, select +Add. The Edit ATP Profile window displays.

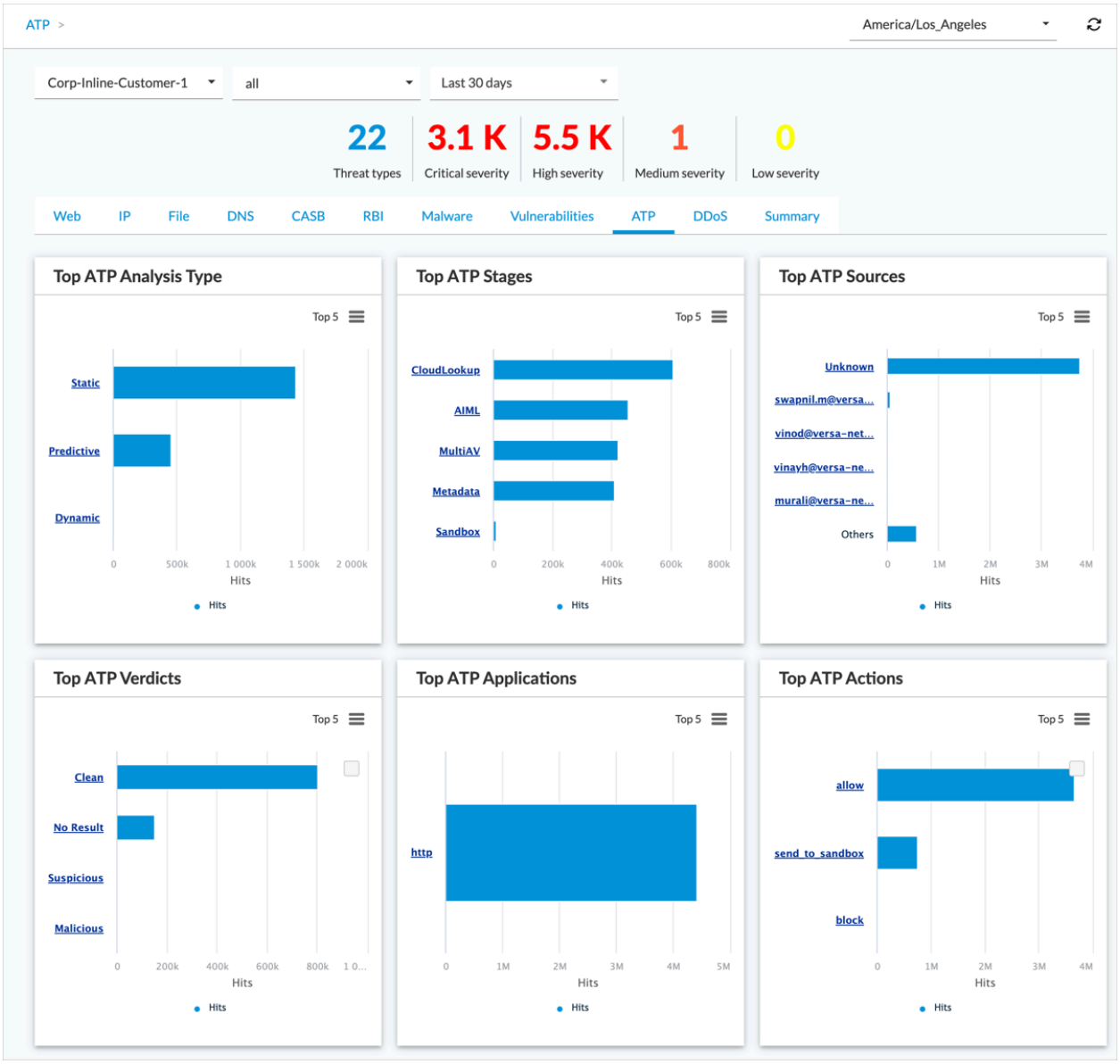


7. In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile.
8. Click OK.

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



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



Configure CGNAT Logging

- Syslog identifier—cgnatLog
- Path to the configuration screen—Search Data Configurations > CGNAT Logs

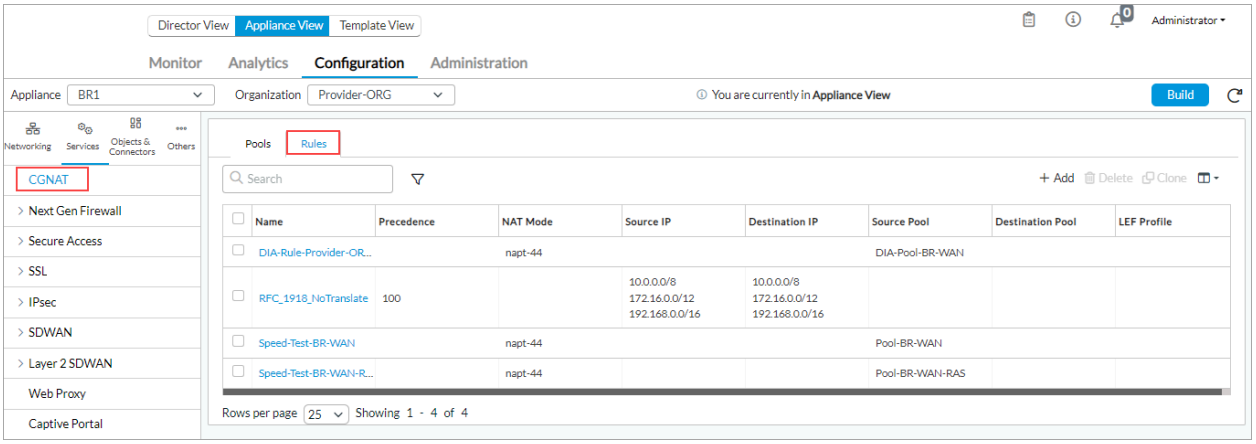
To export CGNAT logs, enable CGNAT logging per flow by associating a LEF profile with a CGNAT rule. For information about configuring CGNAT, see Configure CGNAT.

To export CGNAT logs:

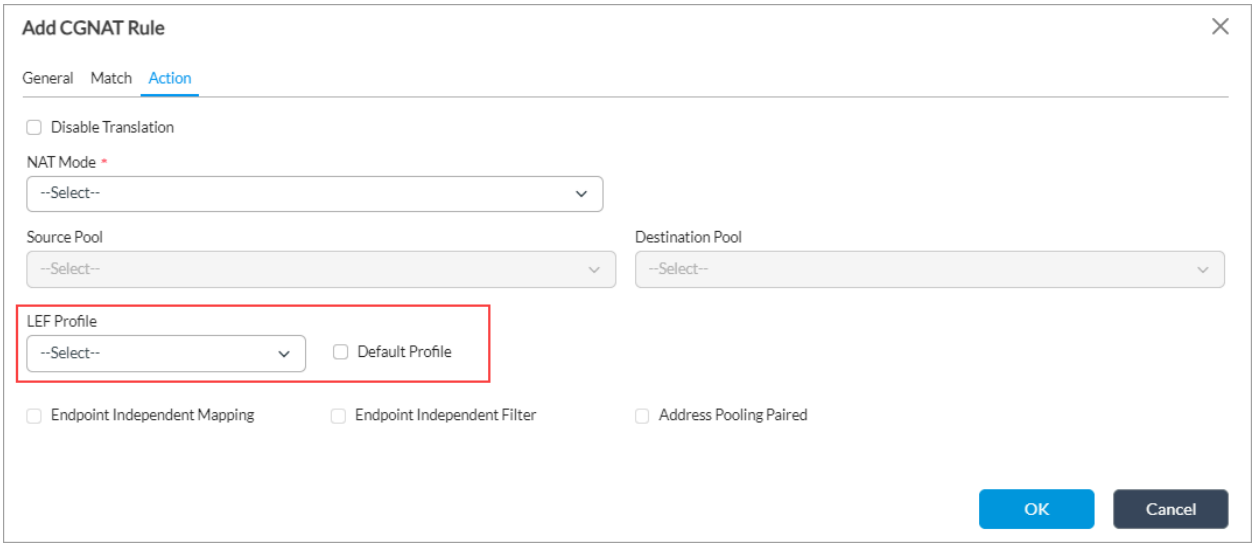
1. In Director view:

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 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.

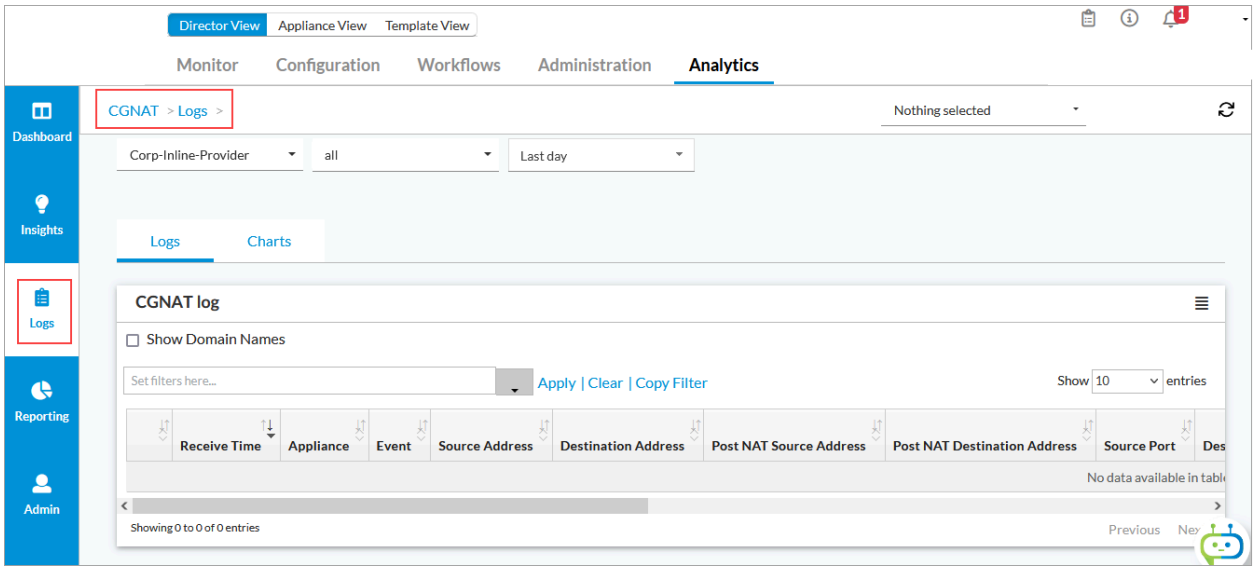


5. Click the + Add icon, or click an existing rule name. In the Add/Edit CGNAT Rule popup window, select the Action tab.



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.

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.



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

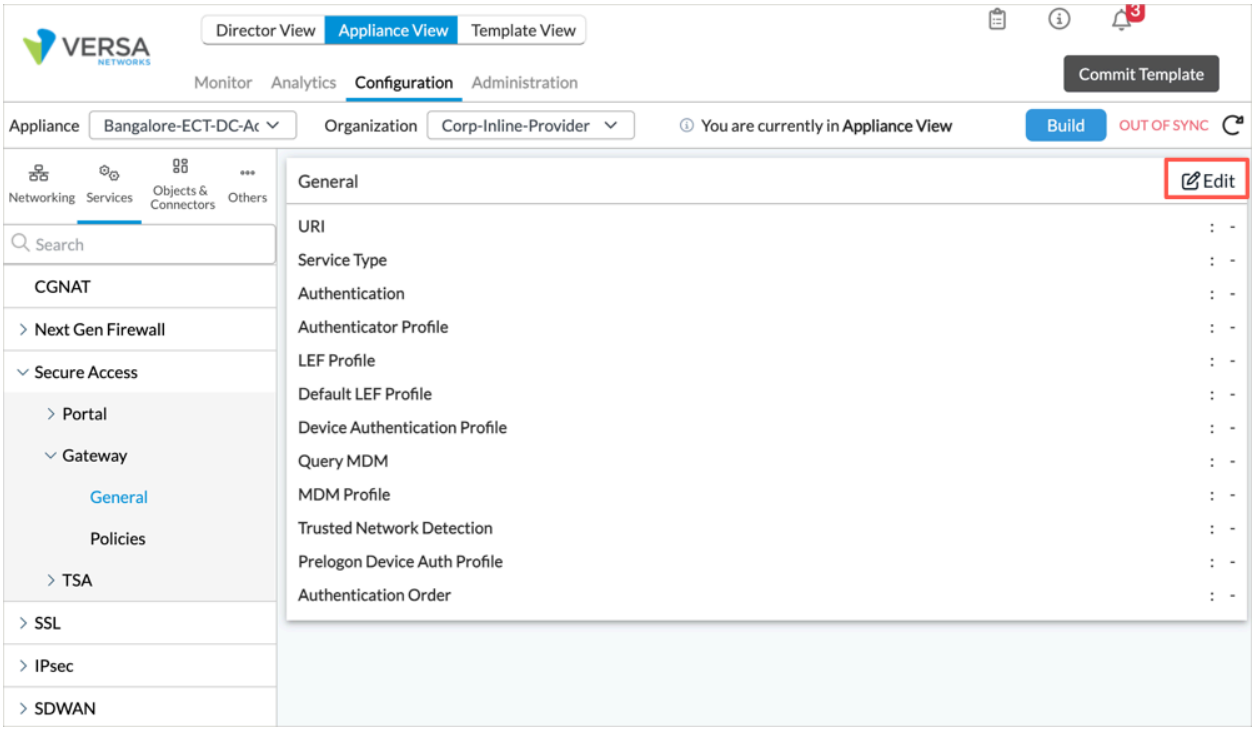
Versa SASE clients collect digital experience monitoring (DEM) data on end-user devices and forward the data to their currently connected secure access gateway. The gateway assembles DEM data from all its clients into DEM logs and forwards them to the destination of its associated LEF profile. To export 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.

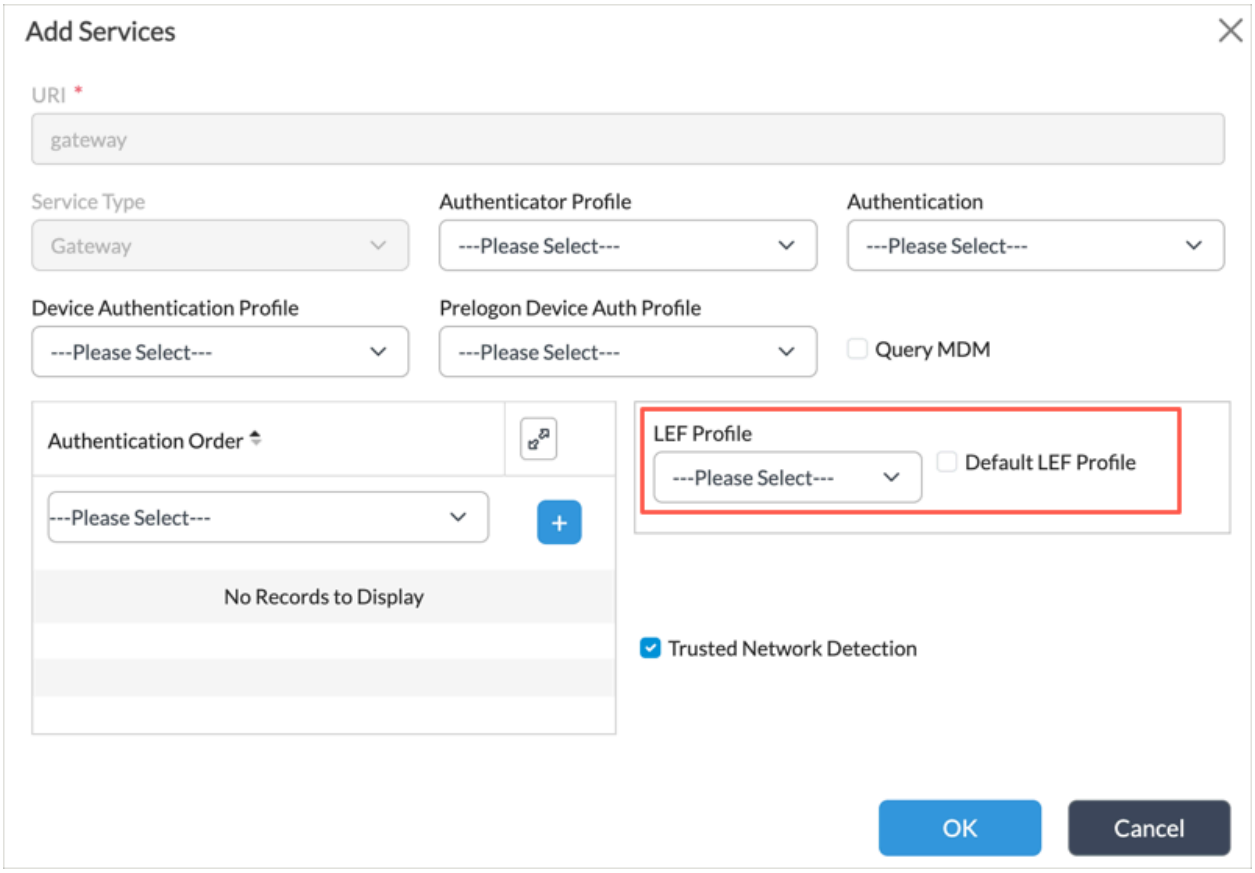
To associate a LEF profile with a secure access gateway:

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

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.

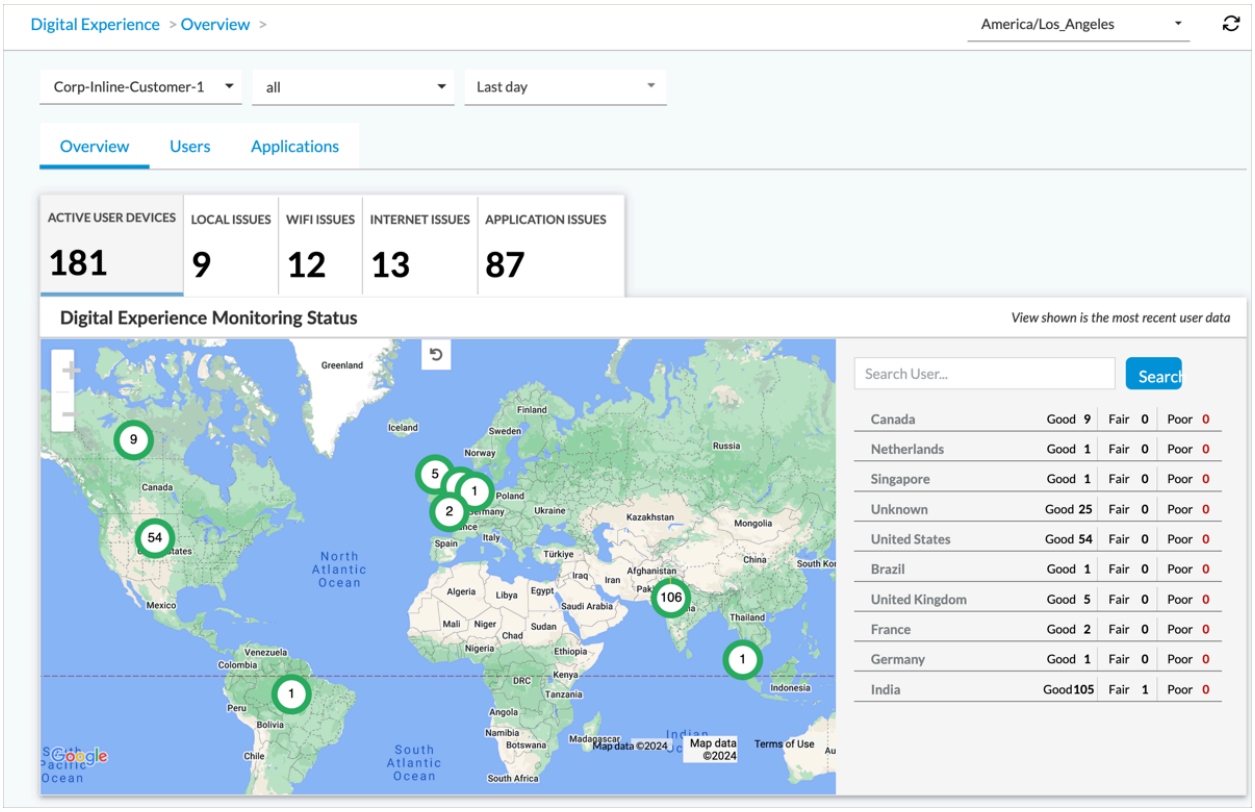


5. In the General pane, click the Edit icon. The Add Services popup window displays.



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.



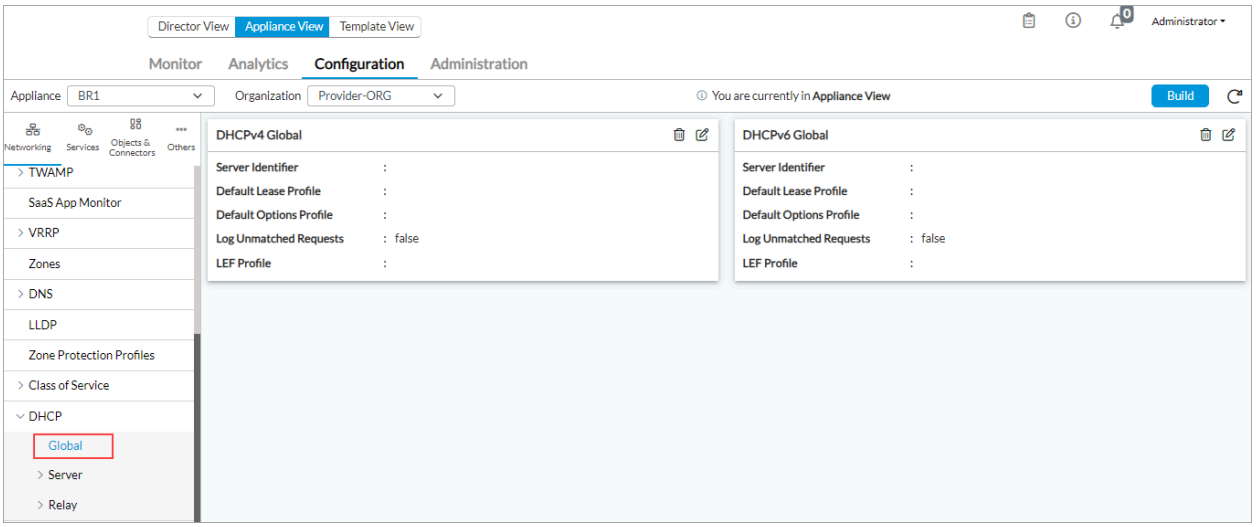
Configure DHCP Logging

- 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.

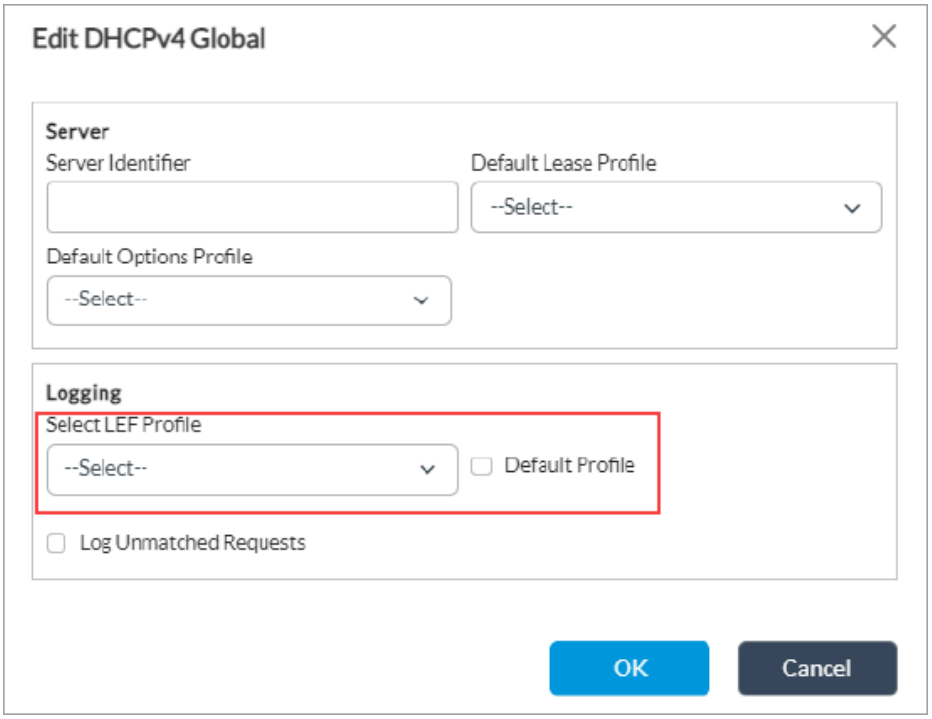
To export DHCP logs to an Analytics cluster, syslog server, or Netflow collector:

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.



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

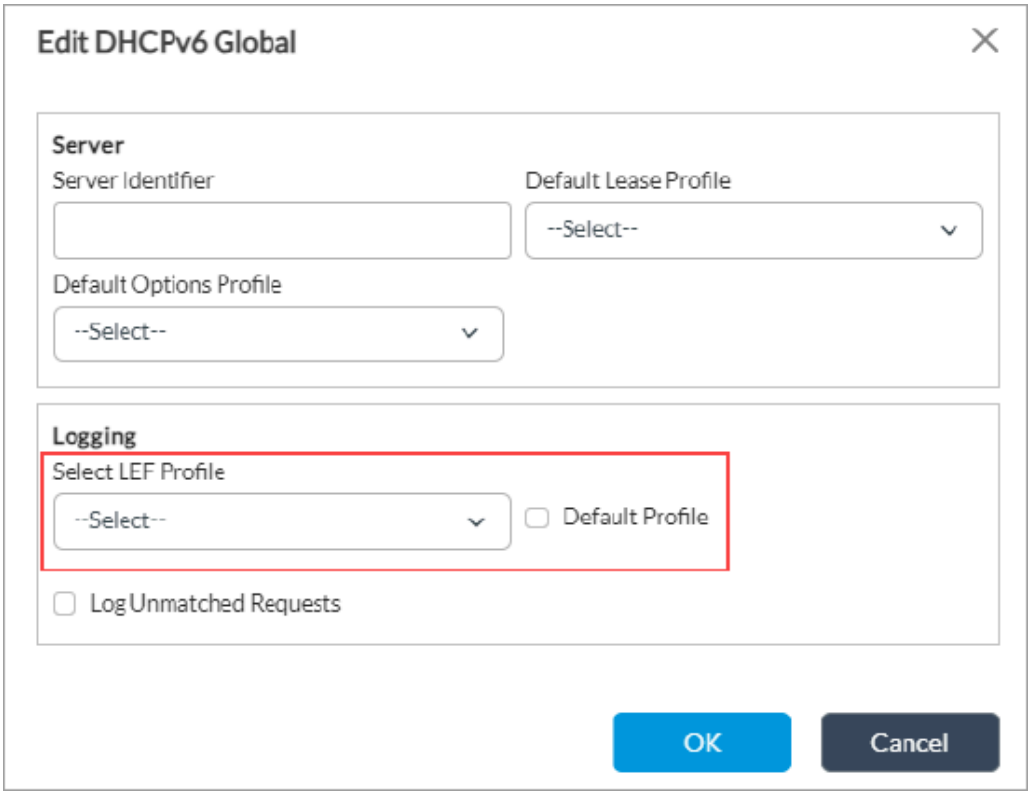
   a. In the main pane, click the Edit icon in the DHCP Global V4 area. The Edit DHCP v4 Global screen displays.



   b. Select a LEF profile, or click Default Profile to use the default LEF profile.

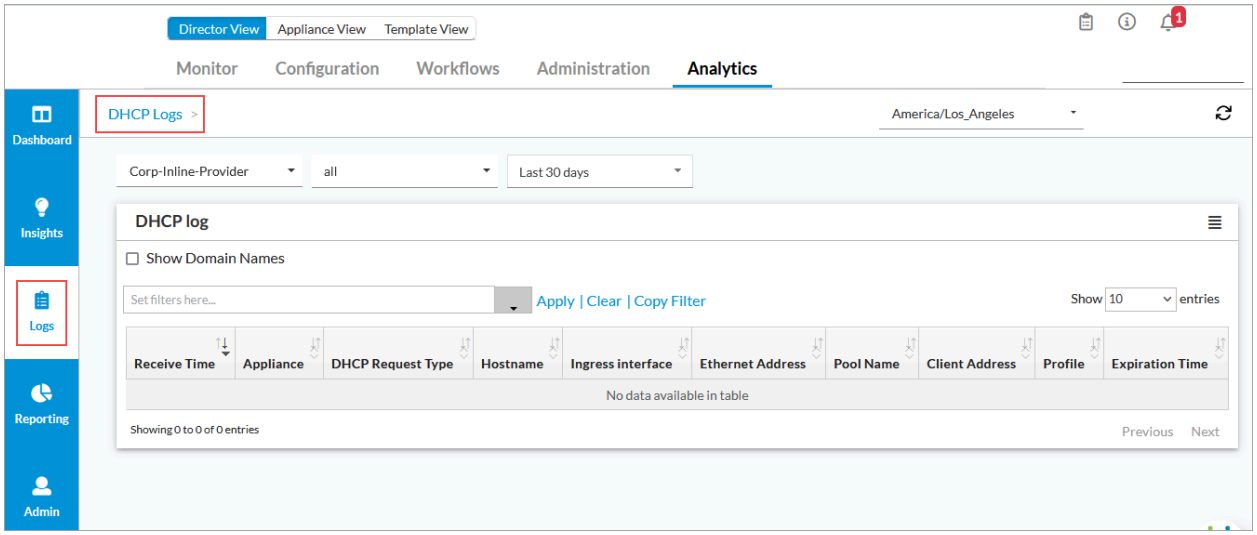
   c. Click OK.

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.



Configure DLP Logging

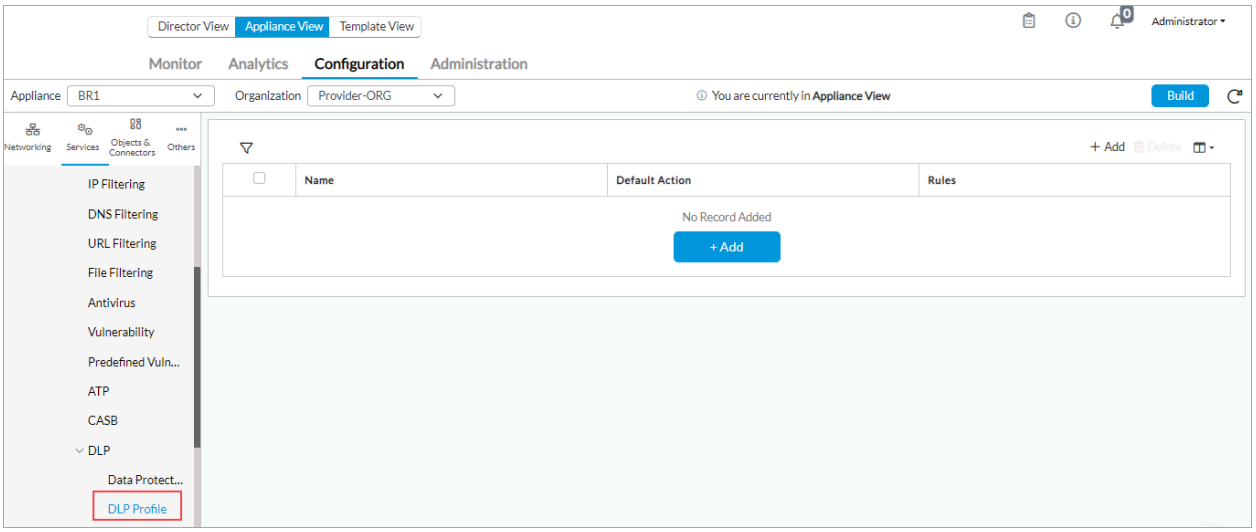
For Releases 22.1.3 and later.

- 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.

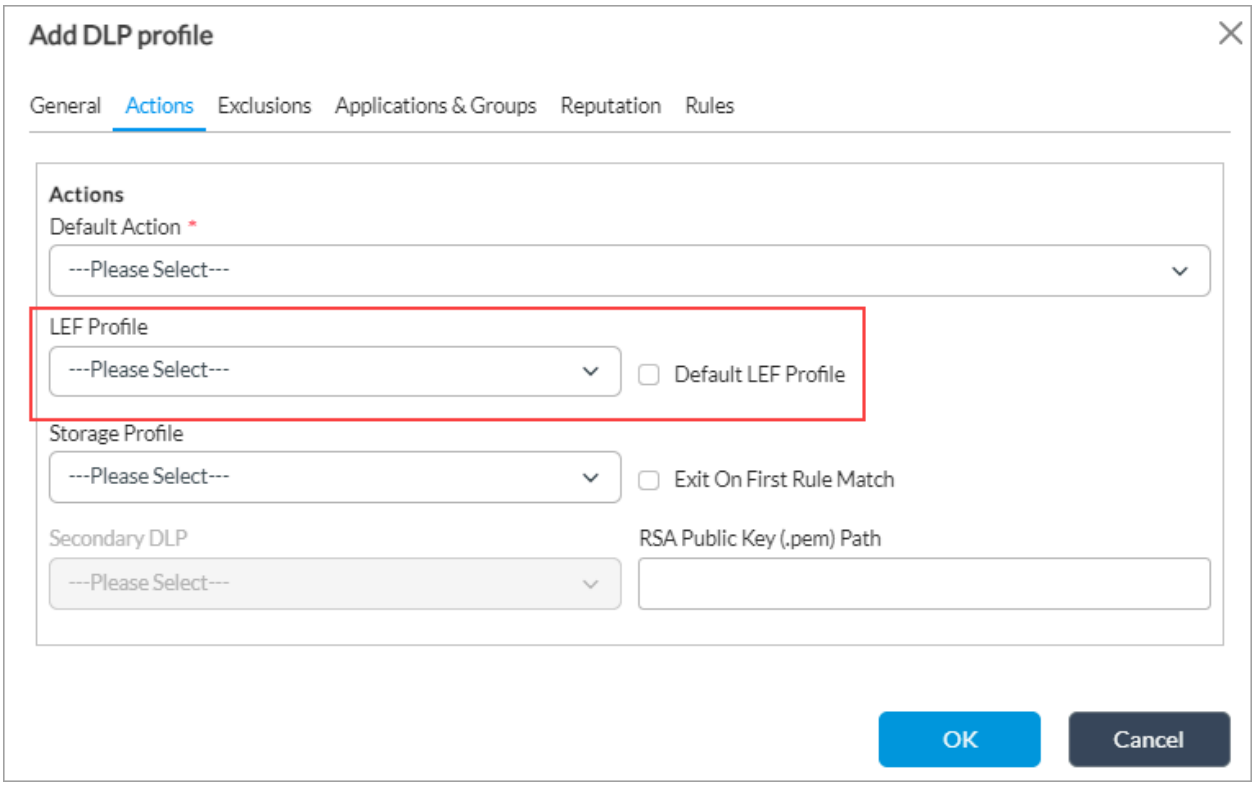
To export DLP logs:

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.



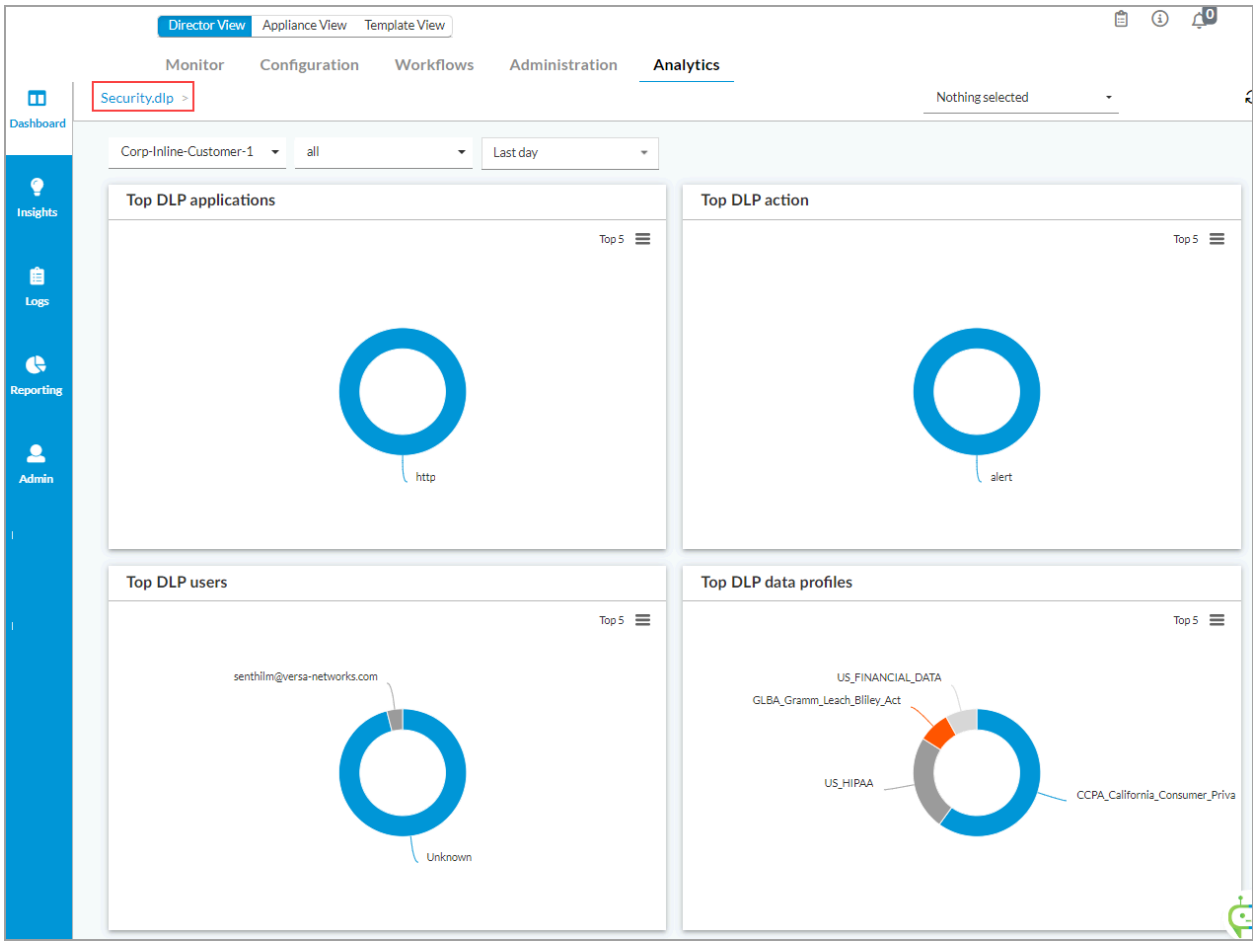
4. Select the tenant from the Organization drop-down list.

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.

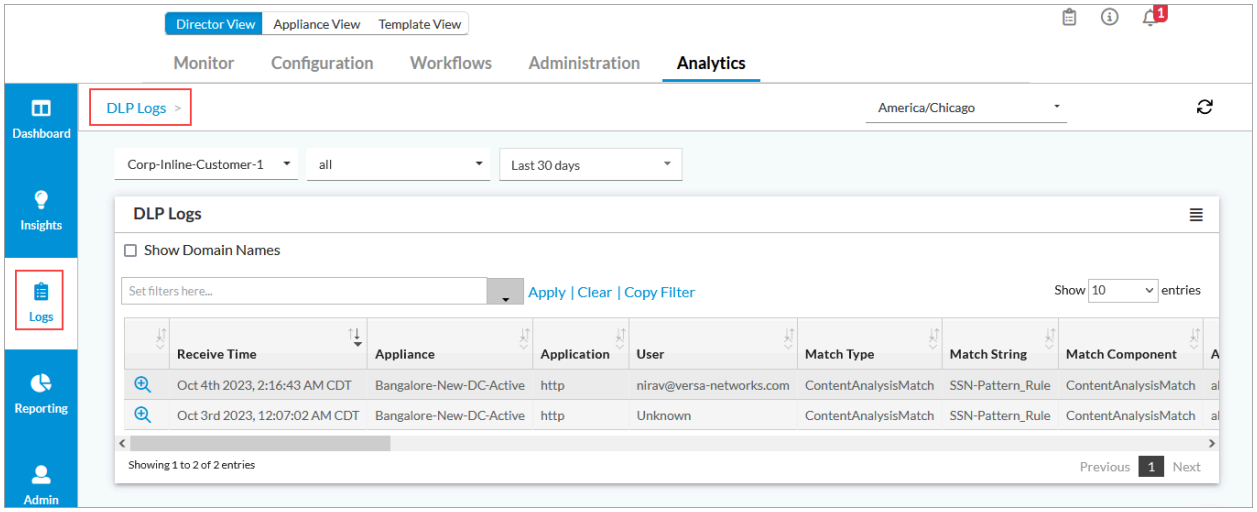


6. In the LEF Profile field, select a LEF profile. Or, click Default LEF Profile to use the default LEF profile.
7. Click OK.

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.



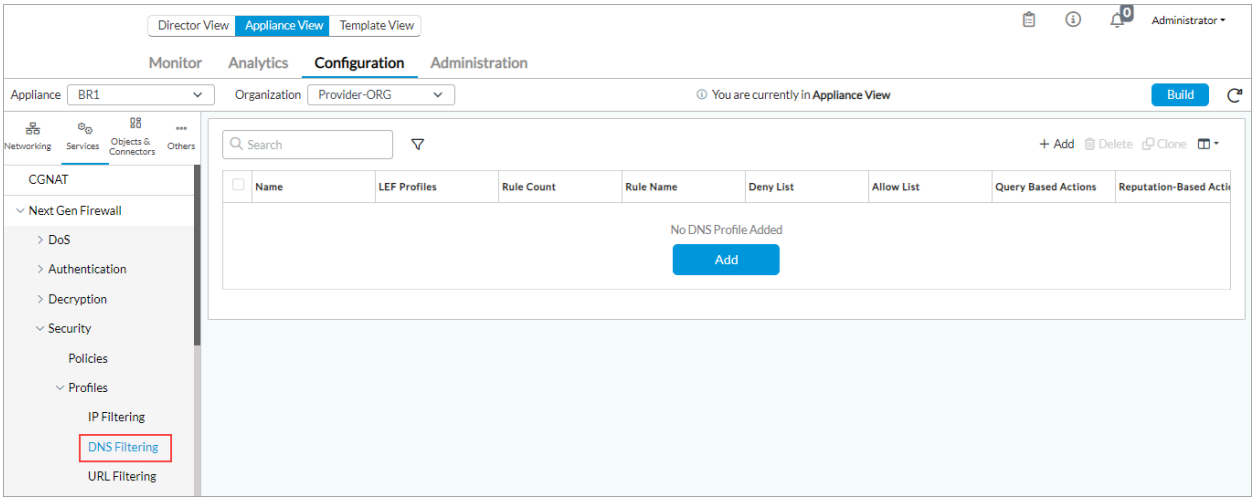
Configure DNS Filtering Logging

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

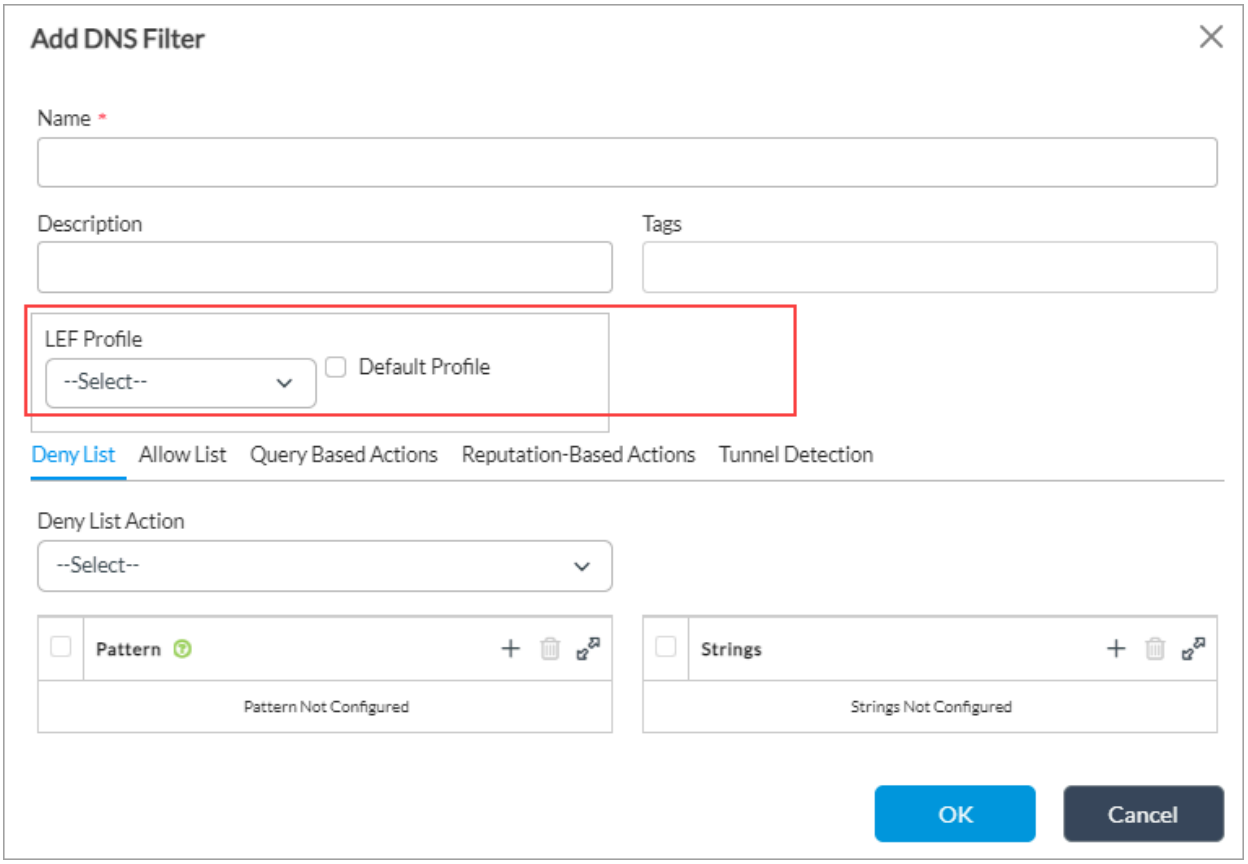
To export DNS filtering logs, select a LEF profile when configuring a DNS-filtering profile. When you apply this DNS-filtering profile to an access policy, DNS filtering logs are forwarded to the active collector of the LEF profile. For information about configuring DNS filtering, see Configure DNS Filtering.

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.

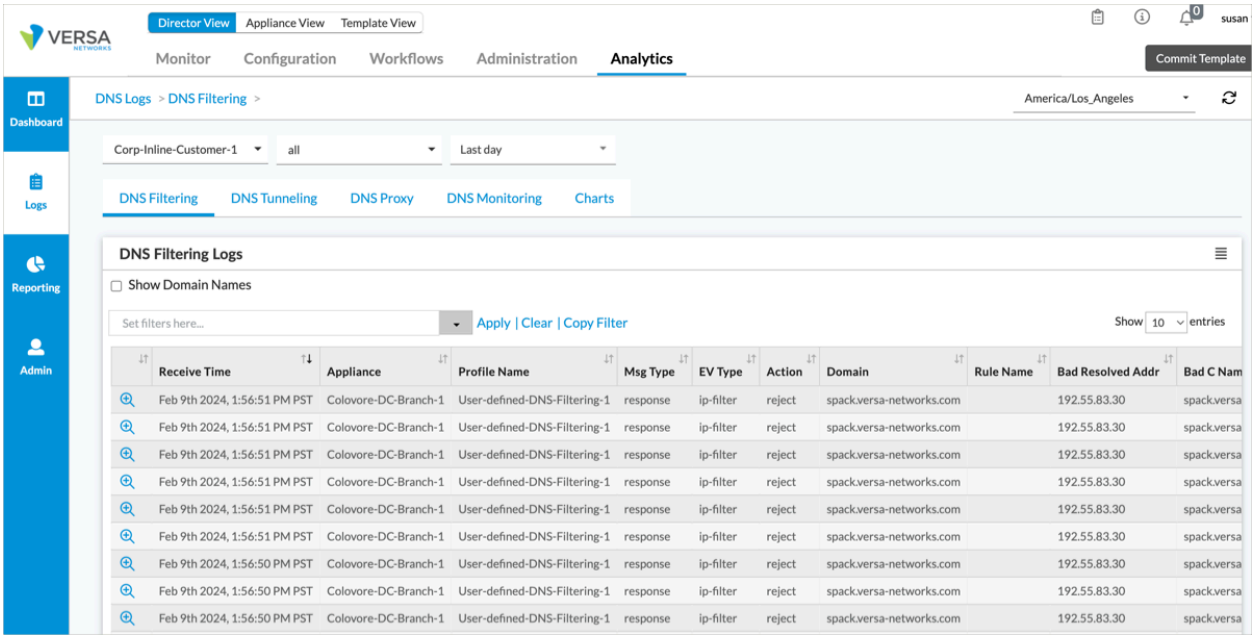


4. Click the + Add icon. The Add DNS Filter popup window displays.

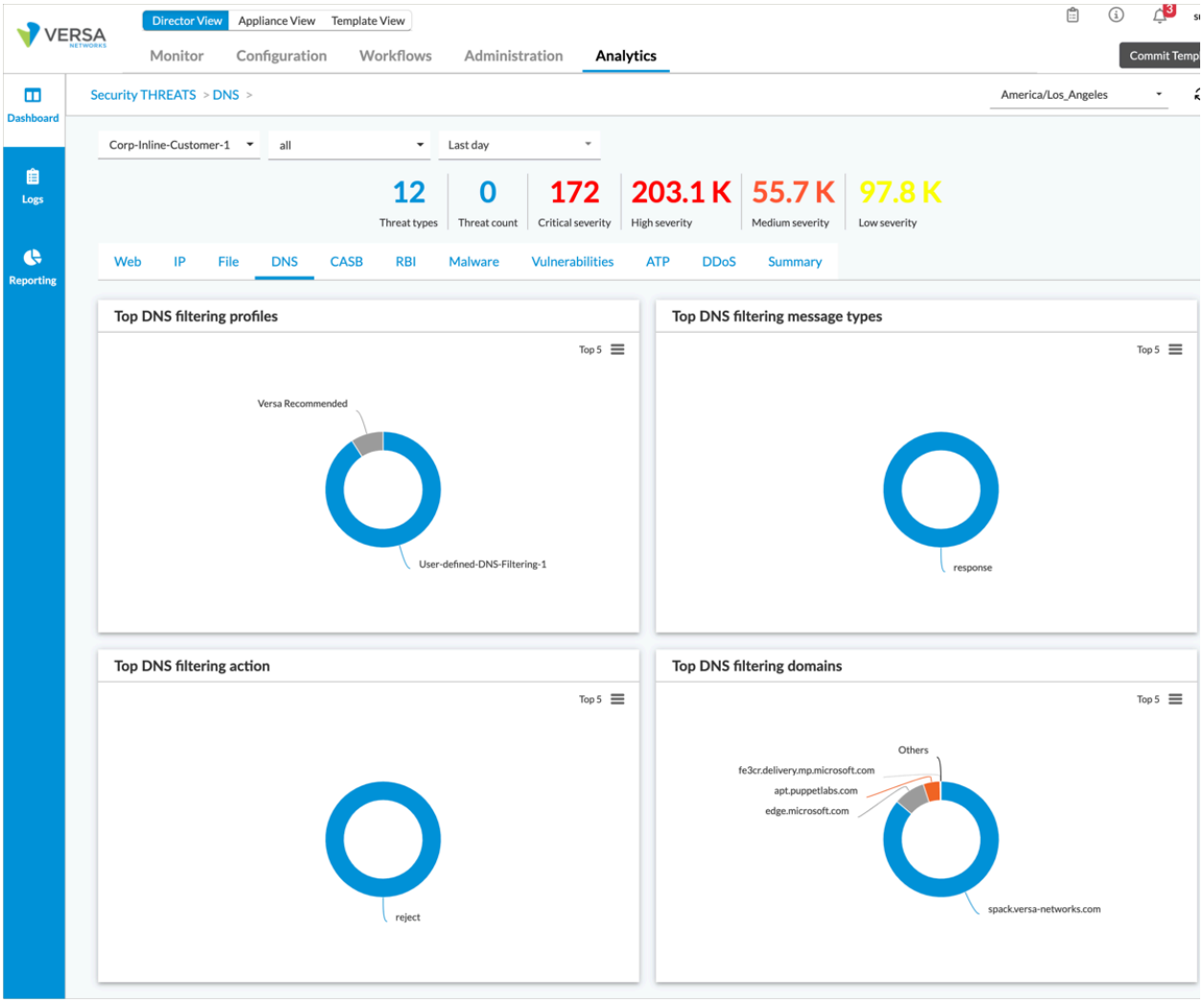


5. In the LEF Profile field, select a LEF profile to use for logging, or click Default Profile to use the default LEF profile.
6. Click OK.

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.



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

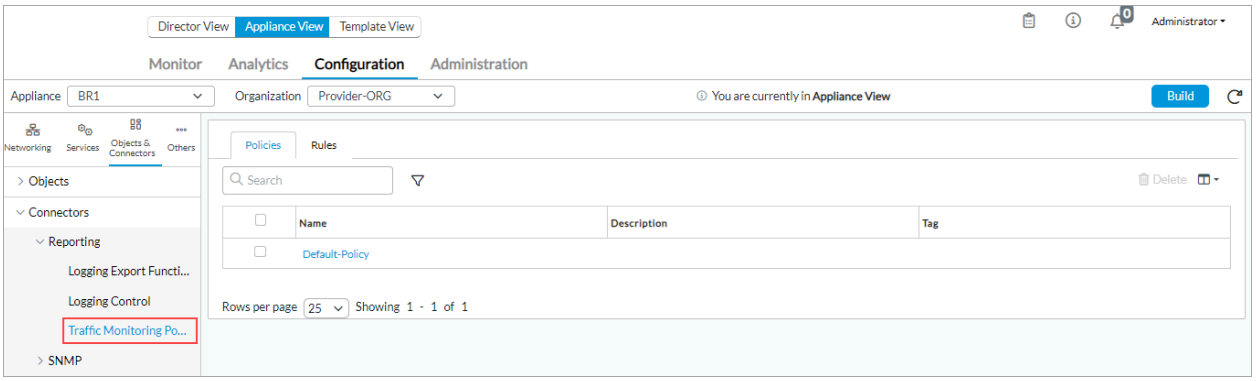
To export DNS monitoring logs, select the Send DNS Metadata option and an LEF profile when configuring a traffic monitoring policy rule. For information about configuring a traffic monitoring rule, see Configure Traffic Monitoring Policy in Configure Log Export Functionality.

To export DNS monitoring logs:

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

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.



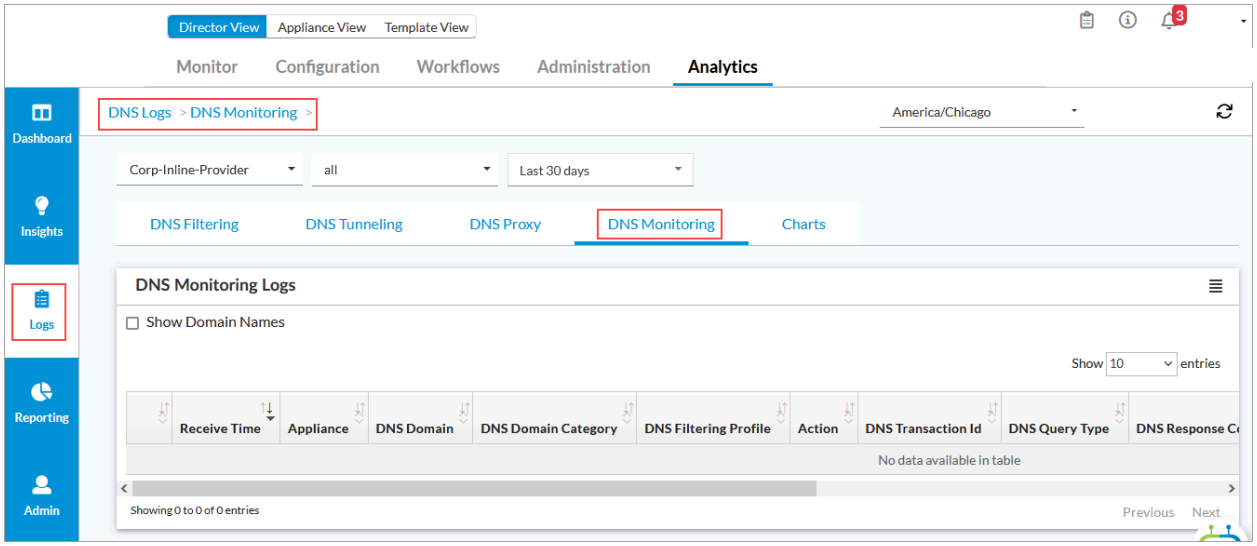
3. Select the Rules tab in the main pane.

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 p
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:

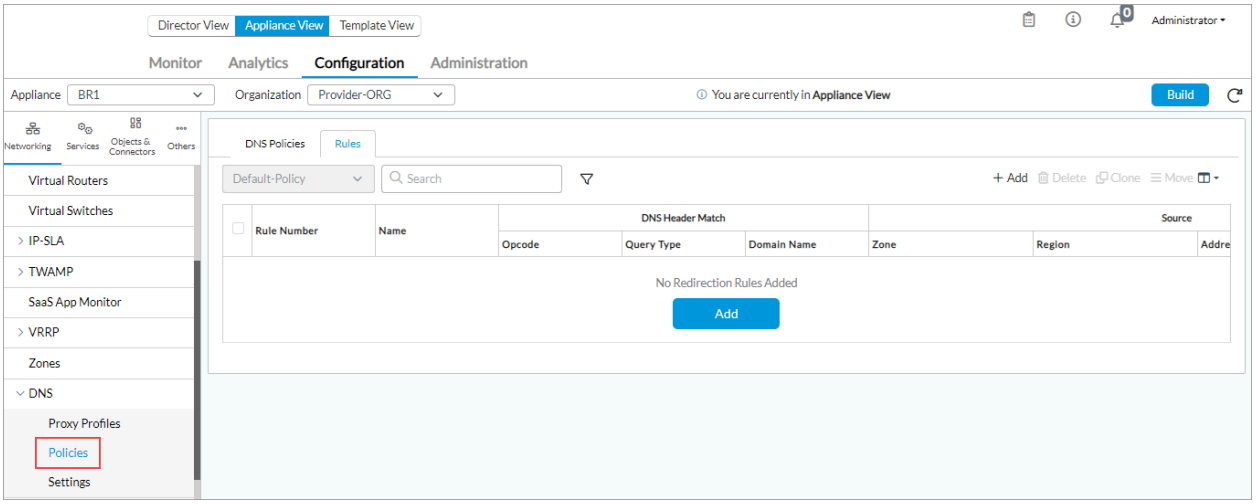


Configure DNS Proxy Logging

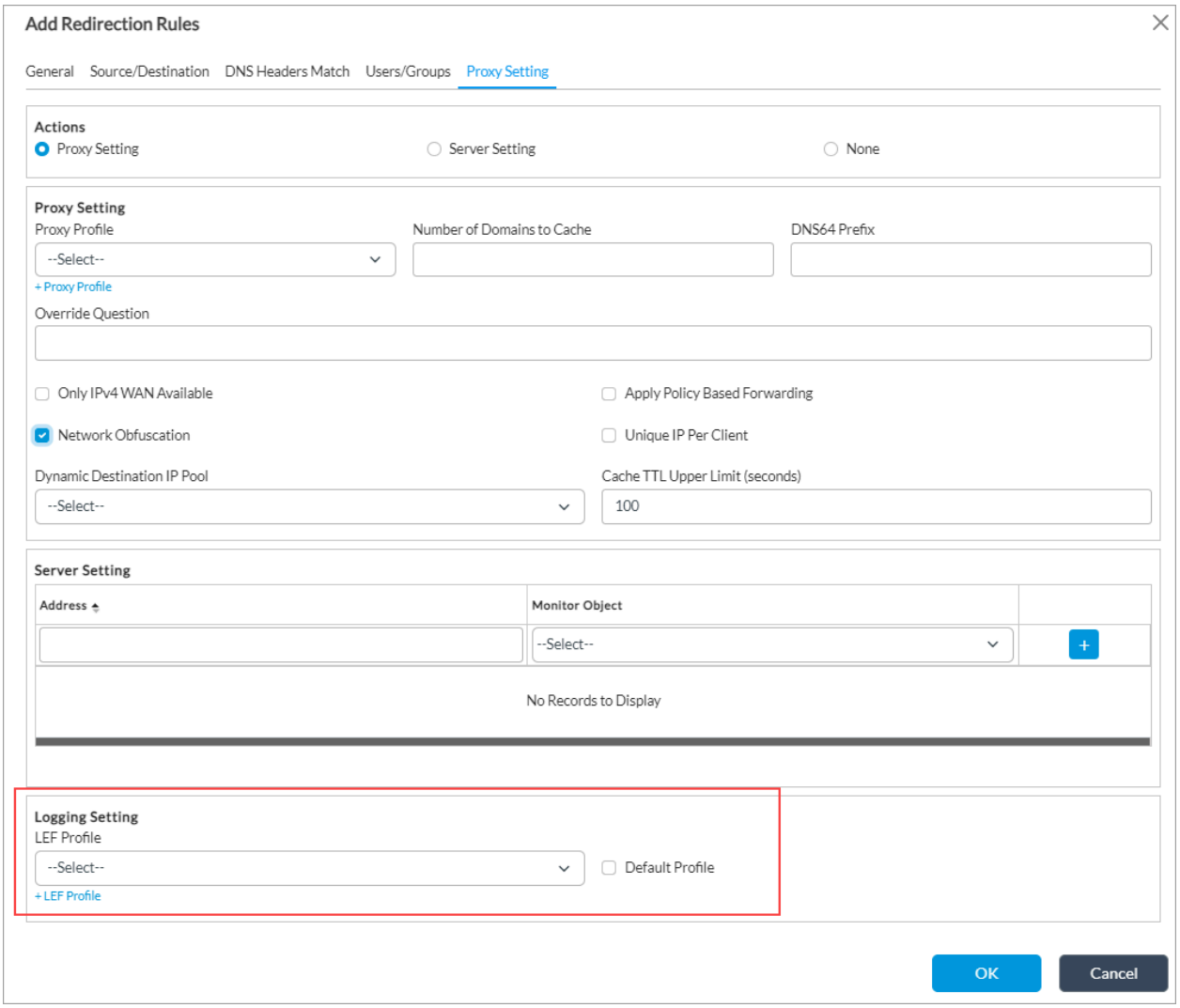
- Syslog identifier—dnspChildSessLog, dnspParentSessLog
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Search Data Configurations > DNS Proxy Logs

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.

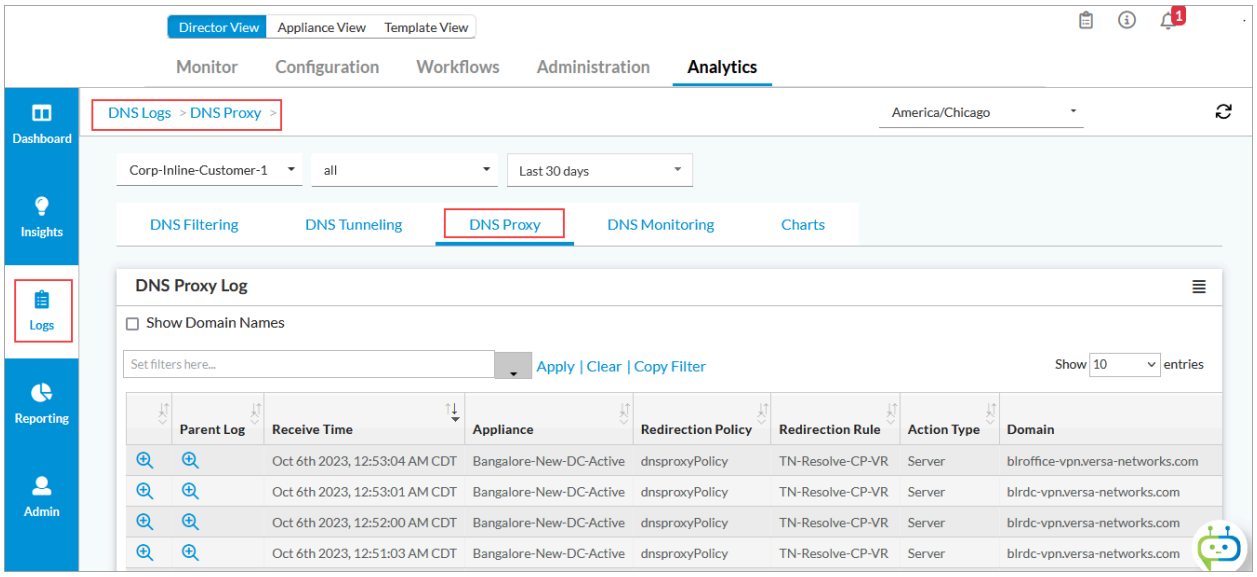


4. Select the Rules tab in the main pane.
5. Select an existing rule or click + Add icon. The Add Redirection Rules popup window displays.
6. Select the Proxy Setting tab. The following screen displays.



7. In the Logging Setting area, select an LEF profile or click Default Profile to use the default LEF profile.
8. 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:

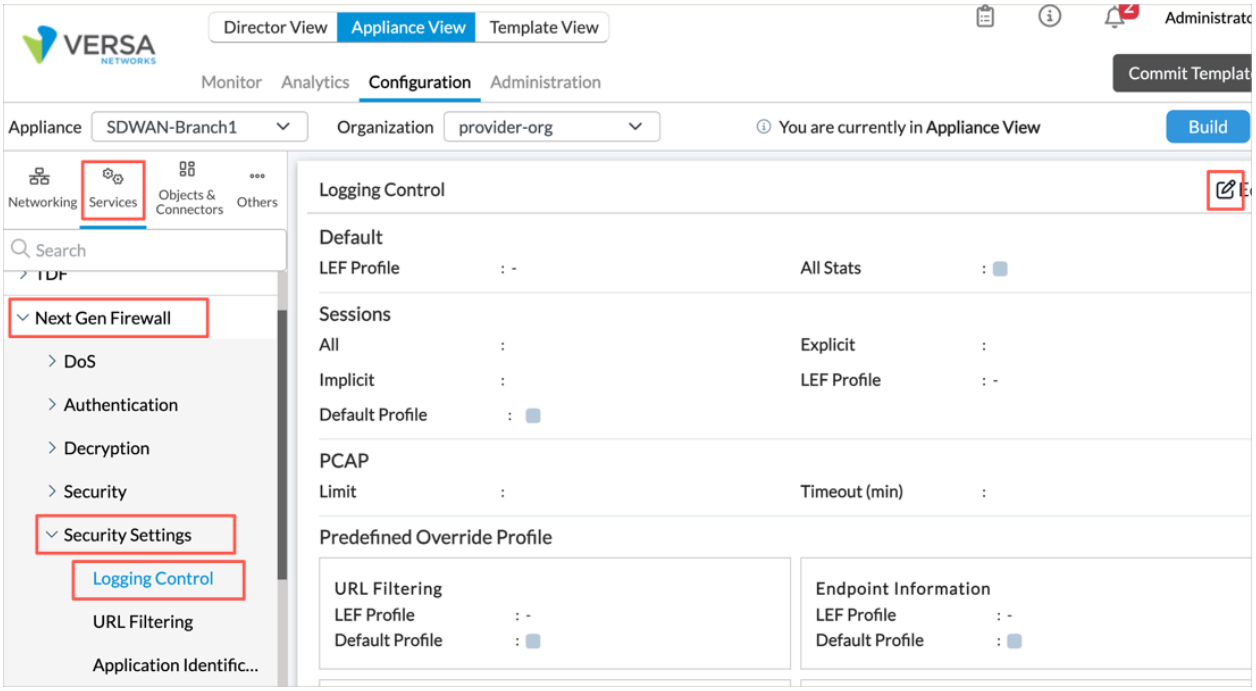
- Associate a LEF profile with predefined and custom EIP profiles.
  - For predefined EIP profiles, select a LEF profile in logging control settings for NGFW. This setting applies to all predefined EIP profiles.
  - For custom EIP profiles, select a LEF profile when configuring the profiles. You select 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:

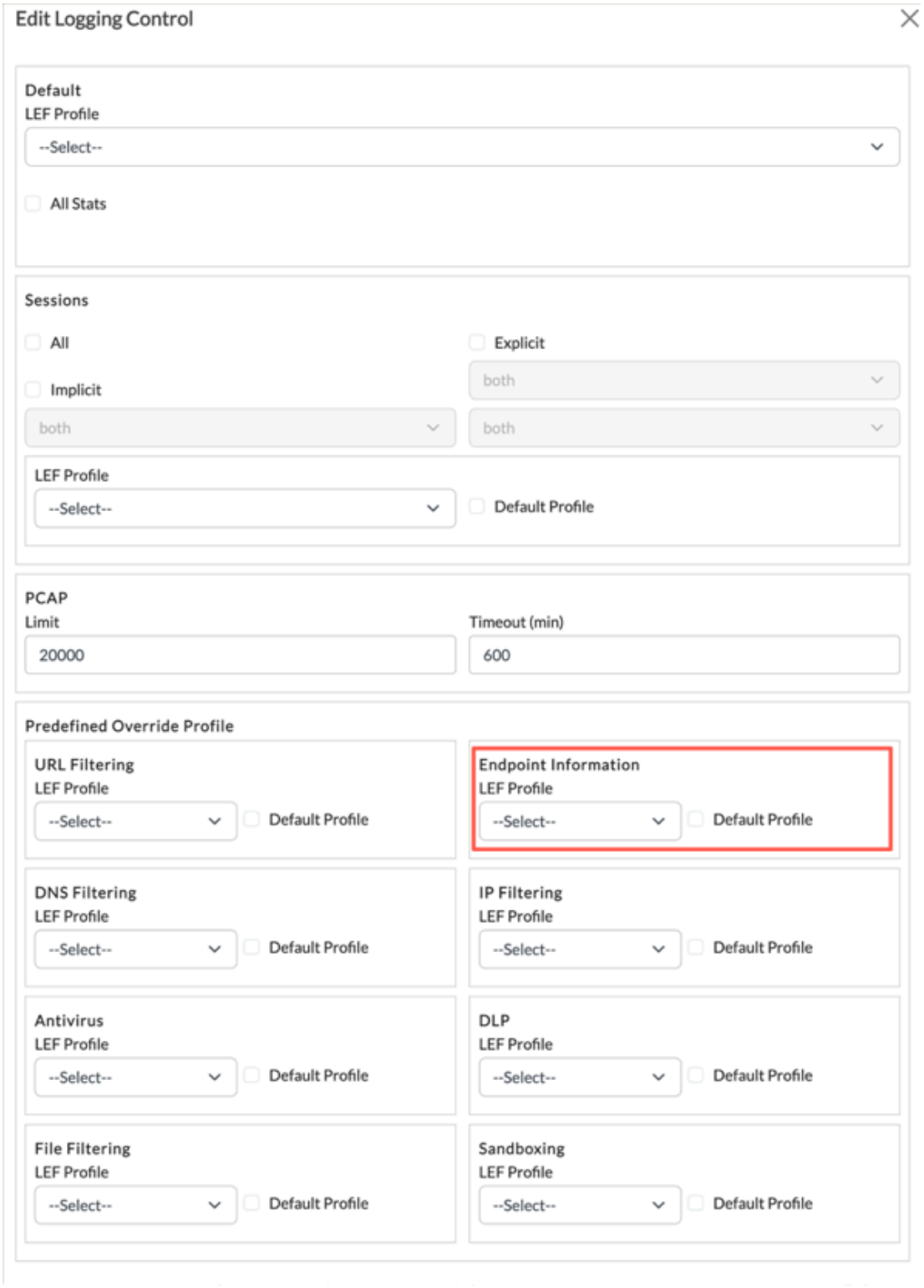
1. In Director view:
   1. Select the Configuration tab in the top menu bar.
   2. Select Devices > Devices in the horizontal menu bar.
   3. Select an organization in the left menu bar.

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.



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

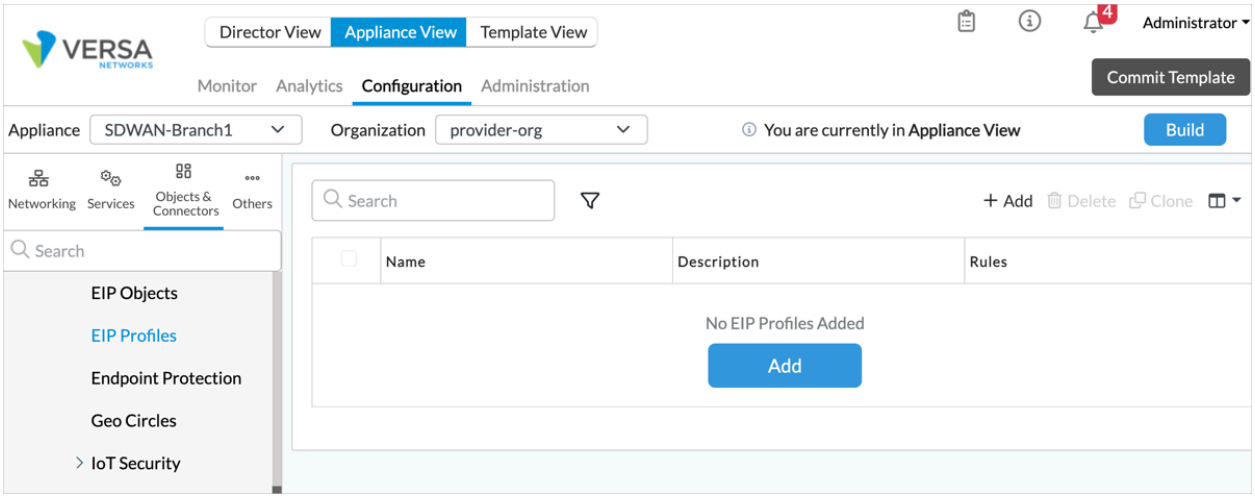


Field	Description
Endpoint Information (Group of Fields)	
◦ LEF Profile	Select the LEF profile to associate with the EIP profile rule.
◦ Default Profile	Click to associate the rule with the default LEF profile.

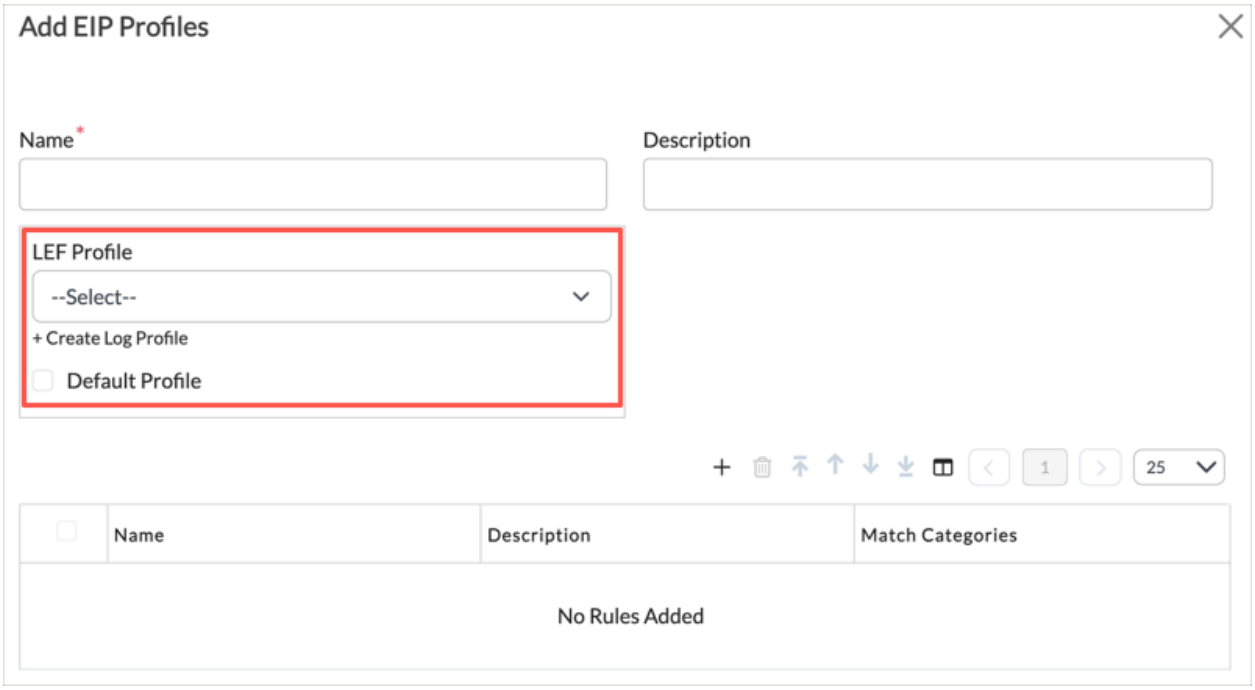
5. Click OK.

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.



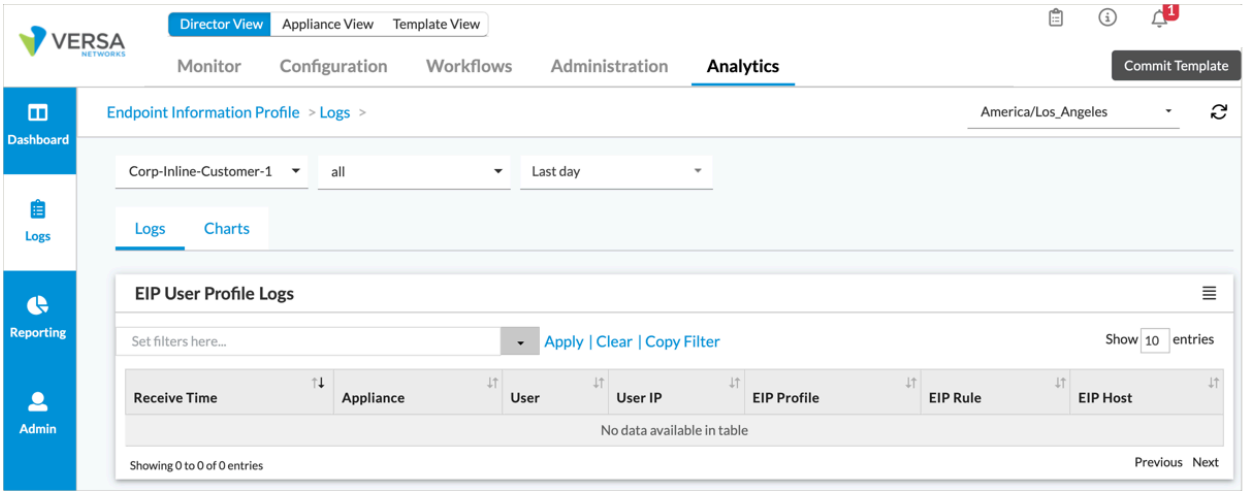
4. Click an EIP profile name or click Add to add new profile. In the Edit/Add EIP Profiles popup window, enter information for the following fields.



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.



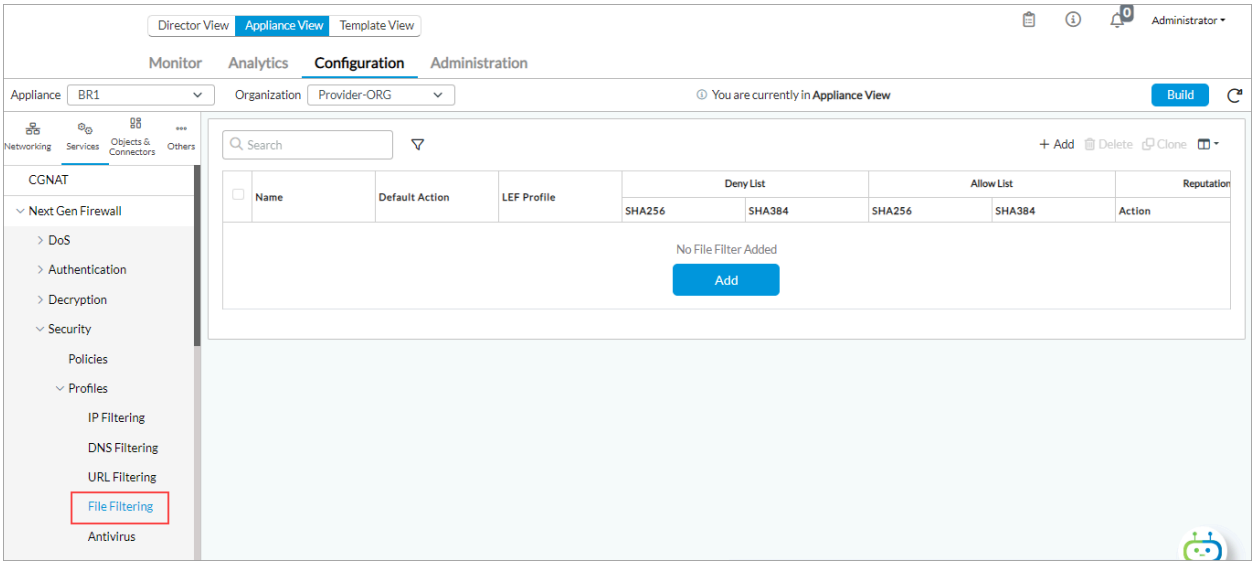
Configure File-Filtering Logging

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

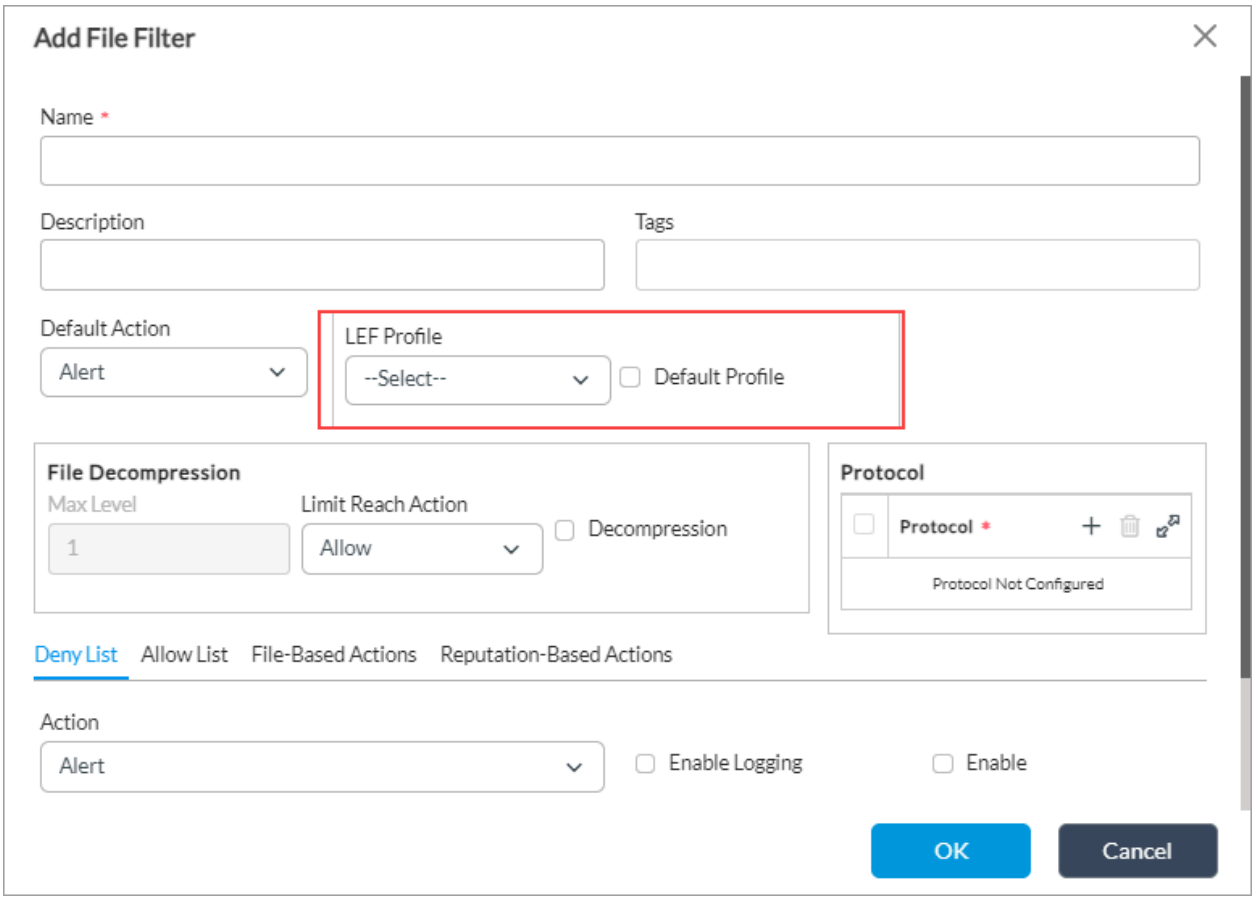
To export file filtering logs, select a LEF profile when configuring a file-filtering profile. When you apply this file-filtering profile to an access policy, file-filtering logs are forwarded to the active collector of the LEF profile. For information about configuring file filtering, see Configure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

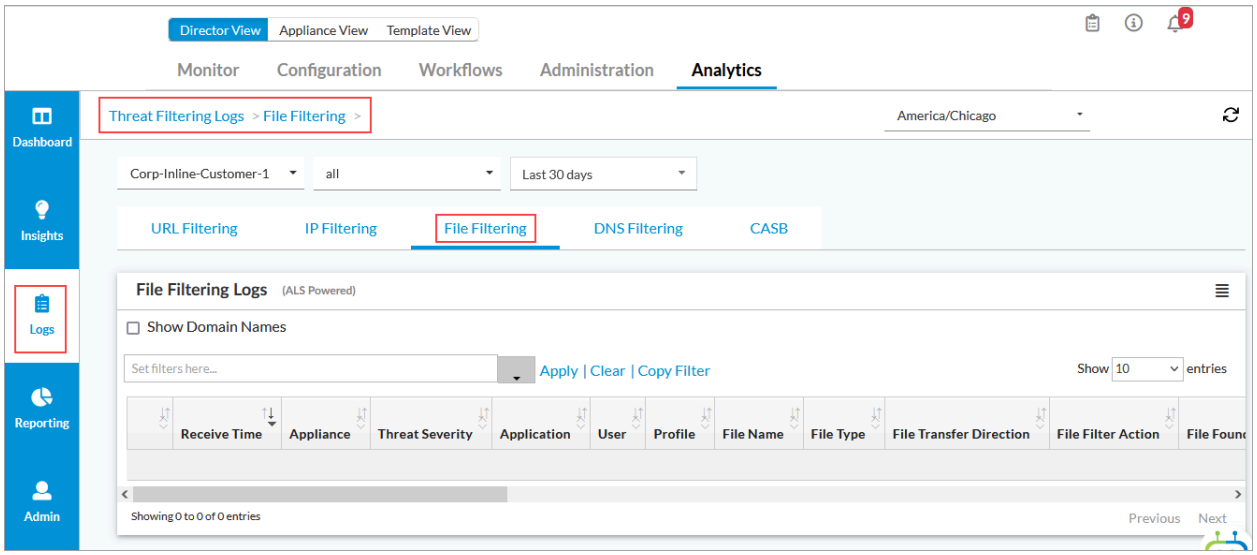


4. Click the + Add icon. The Add File Filter popup window displays.



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

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.



Configure Firewall Logging

- Syslog identifiers—accessLog, sfwAccessLog, denyLog
- Path to the configuration screen—Search Data Configurations > Access Logs

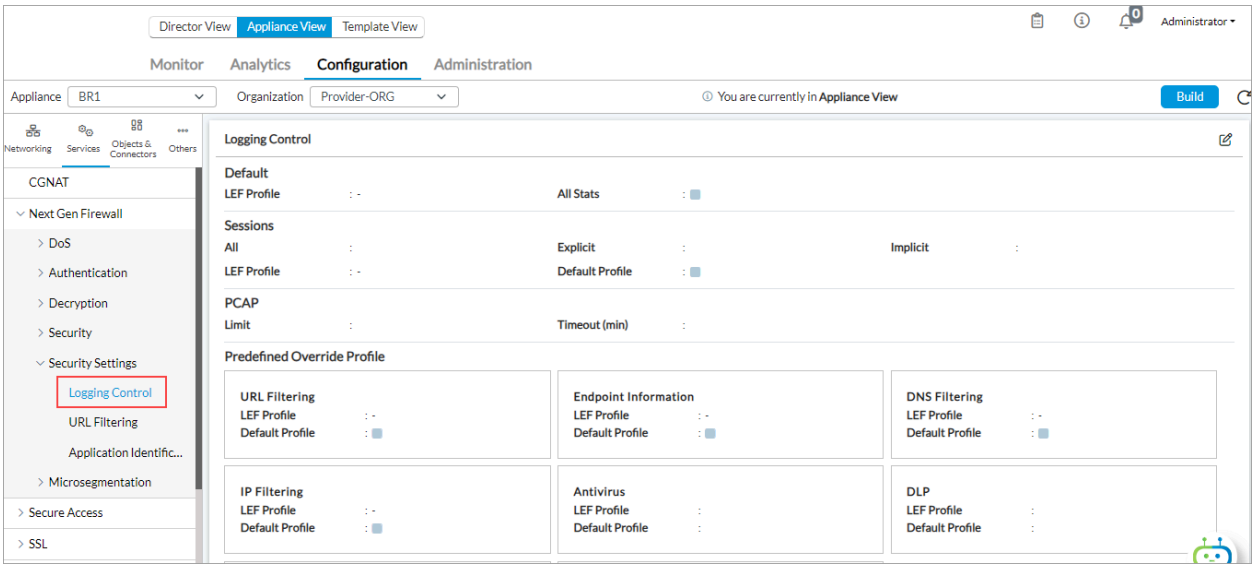
To export DHCP Global V4 and DHCP Global V6 logs, select a LEF profile when you configure DHCP. For information about configuring DHCP, see Configure DHCP.

Configure Global Firewall Per-Flow Logging

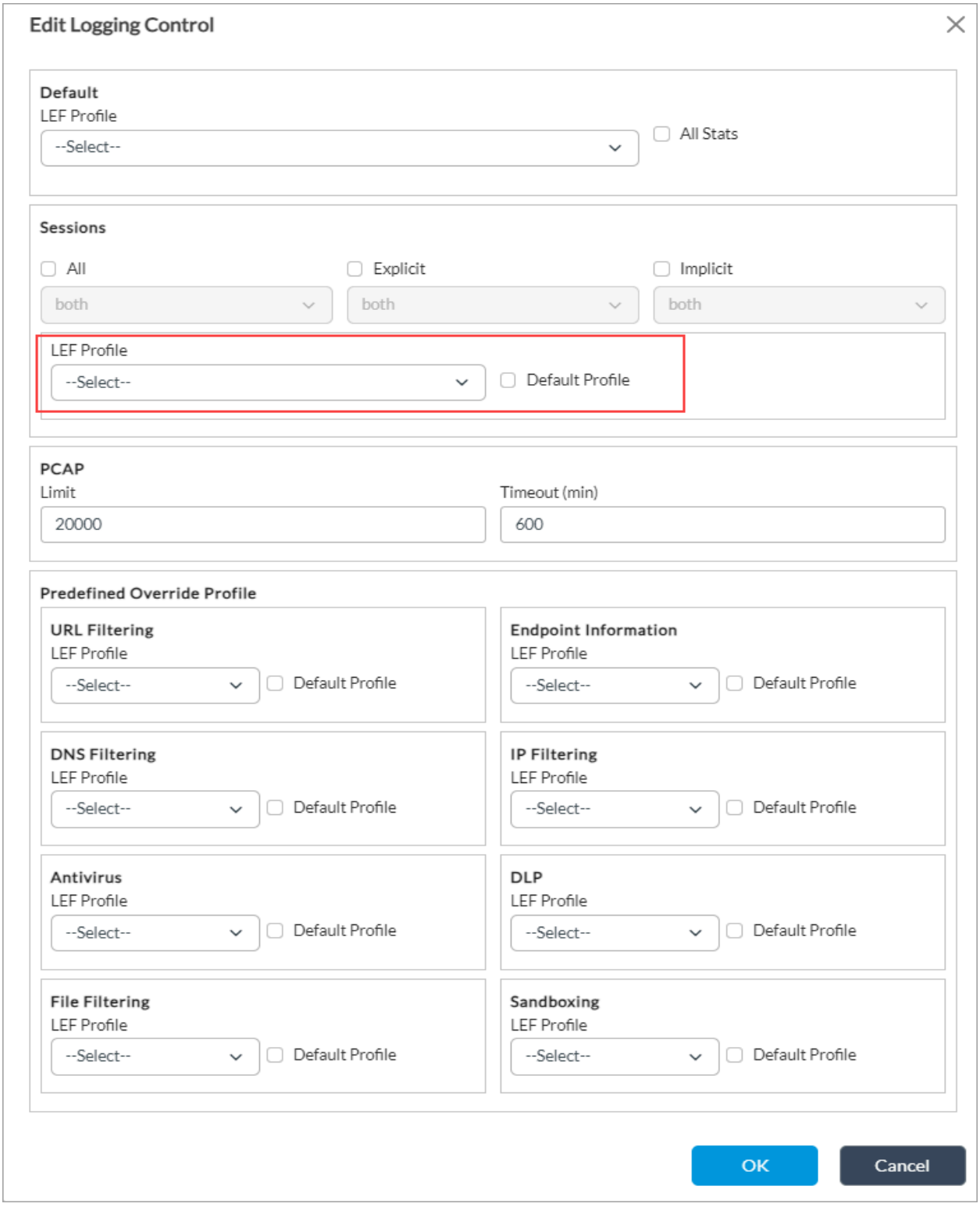
For information about configuring NGFW, see Configure NGFW.

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.



4. 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.



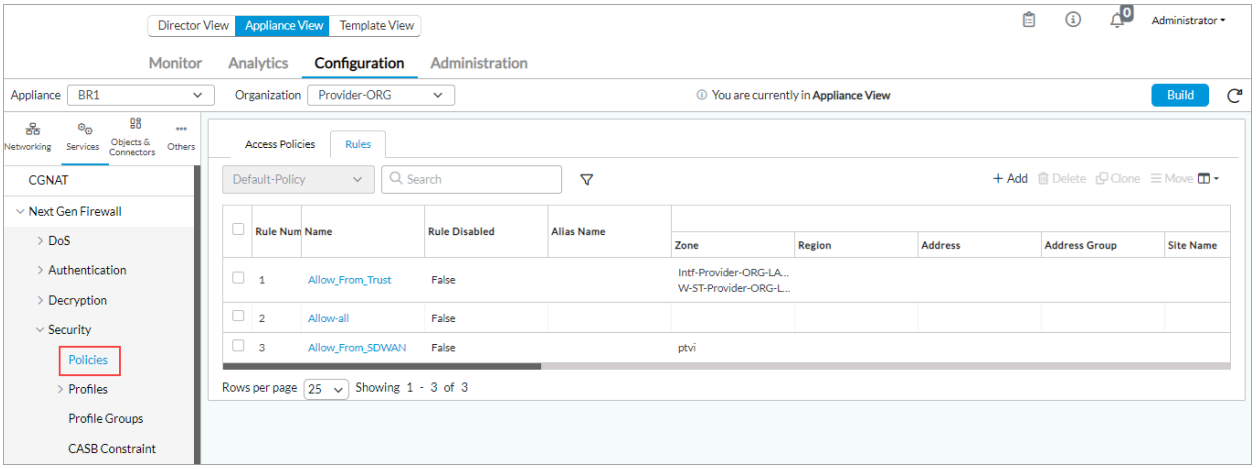
5. Click All, select a LEF profile, and then click All Stats.
6. Click OK.

Configure Firewall Per-Flow Logging by Firewall Rule

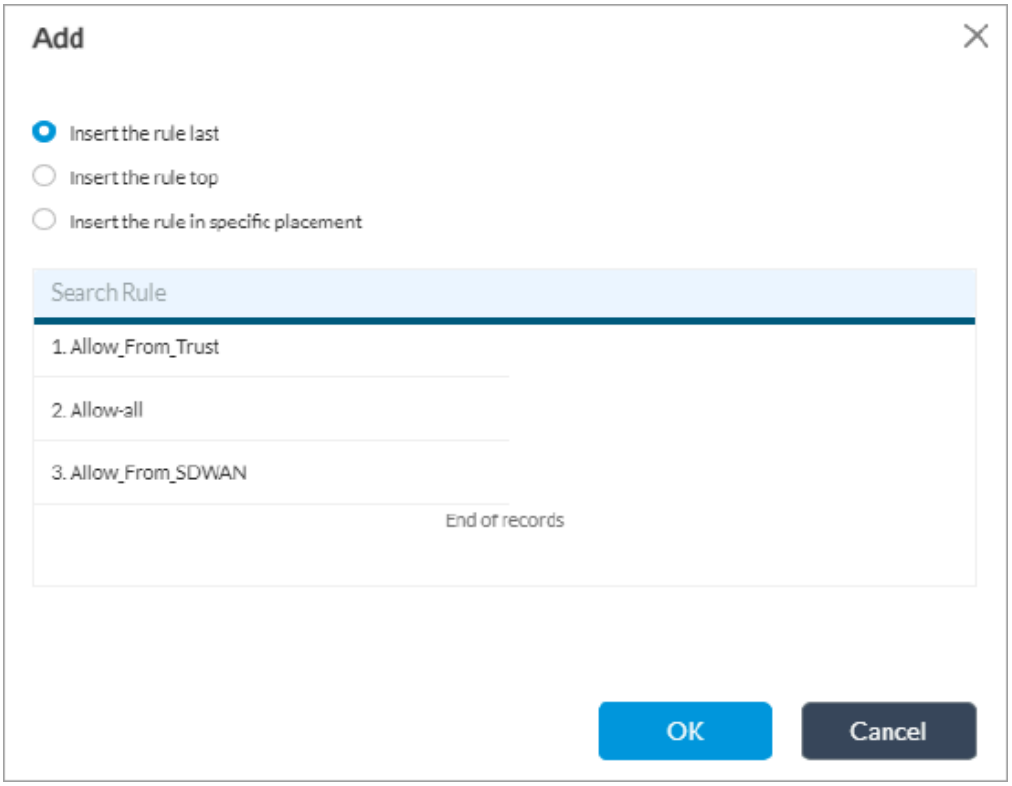
For information about configuring NGFW, see Configure NGFW.

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.

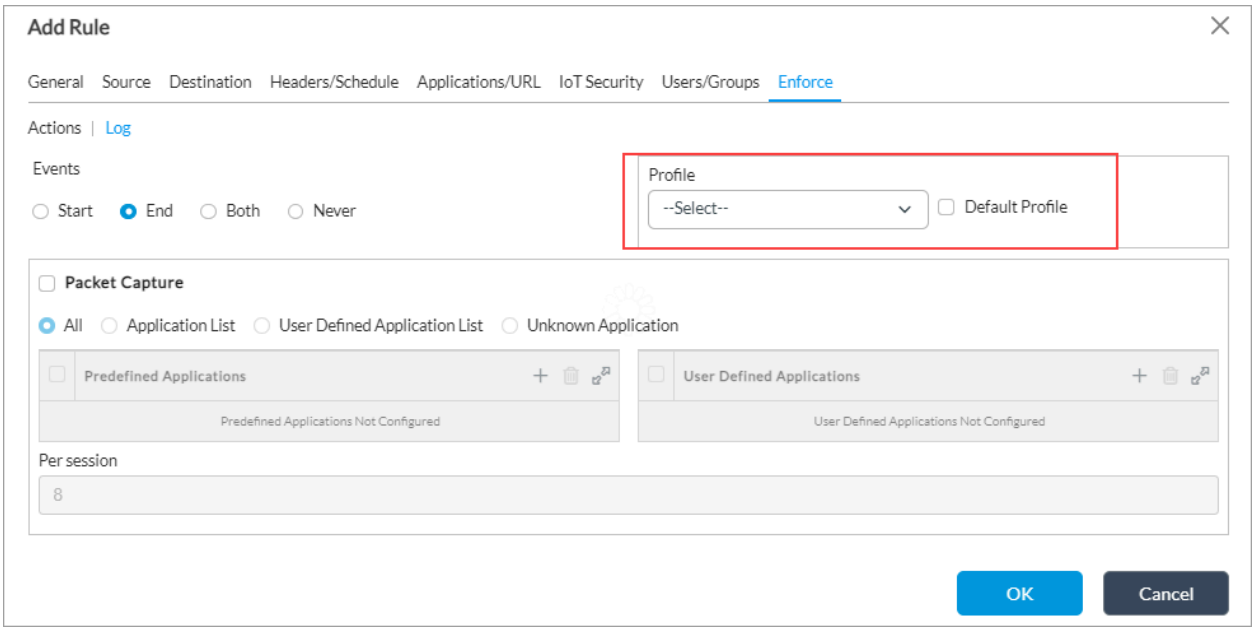


5. Click the + Add icon to define rules for the policy. The Add Rule popup window displays.
6. (For Releases 21.2.1 and later.) If rules already exist, the Configure Rule Order popup window displays.
   a. Select where you want to insert the policy rule, either at the beginning or end of the existing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

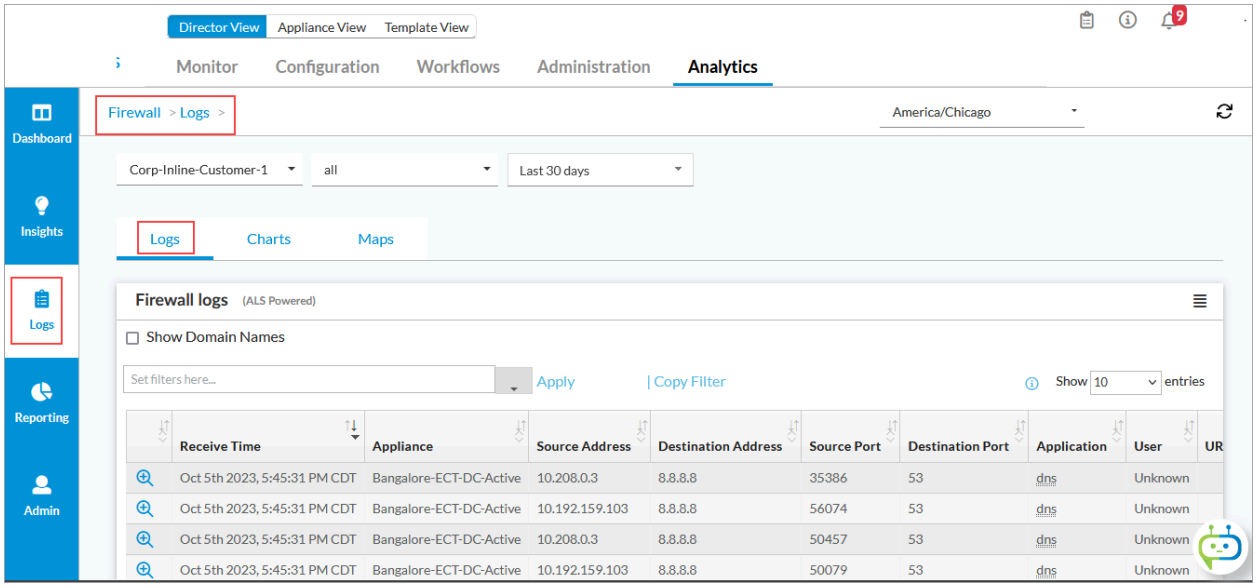


8. In the Events group of fields, click End.
9. In the Profile group of fields, select a LEF profile or click Default Profile to use the default LEF profile.
10. Click OK.

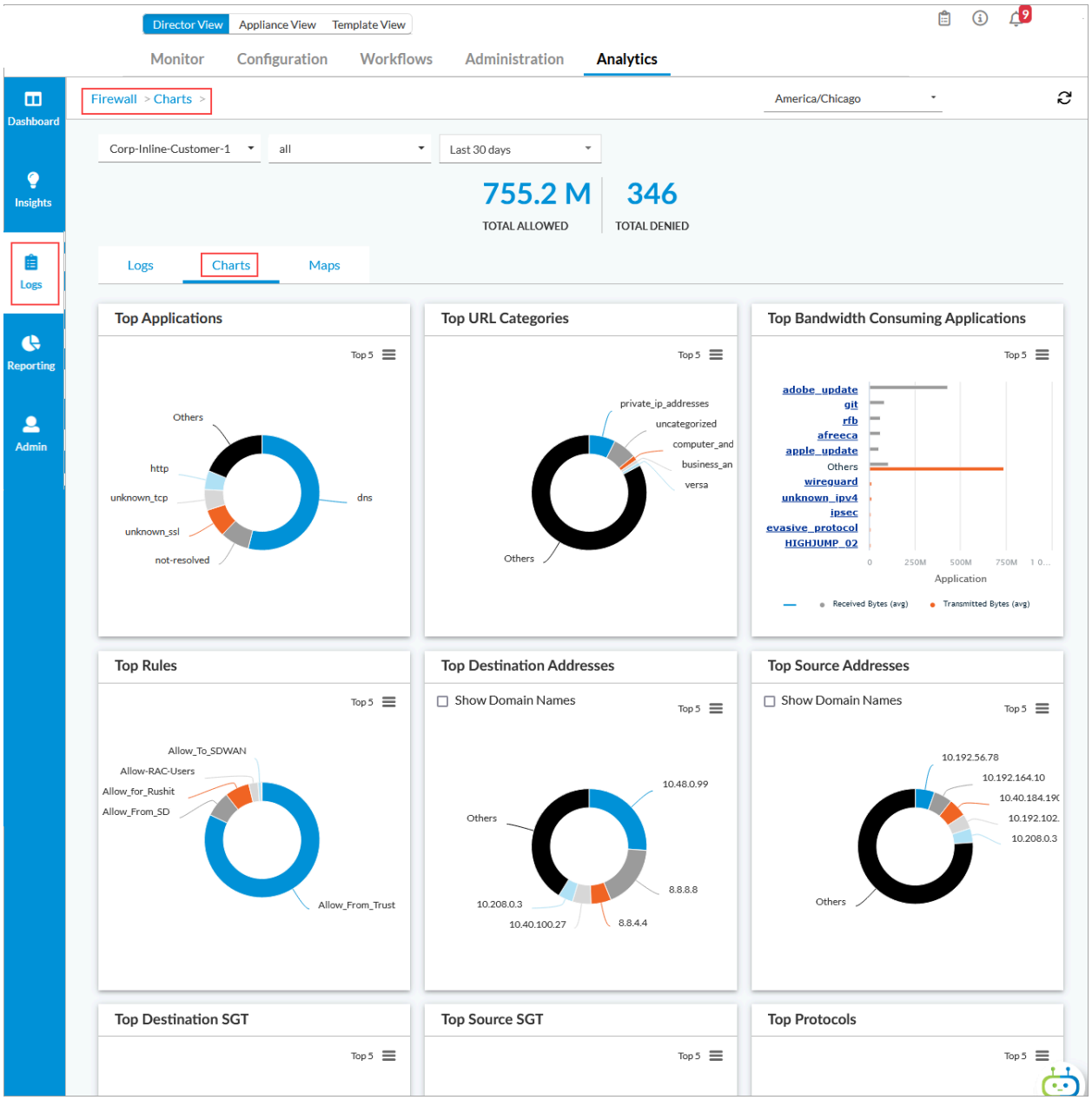
Firewall logs sent to Analytics clusters display on the following three screens:

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

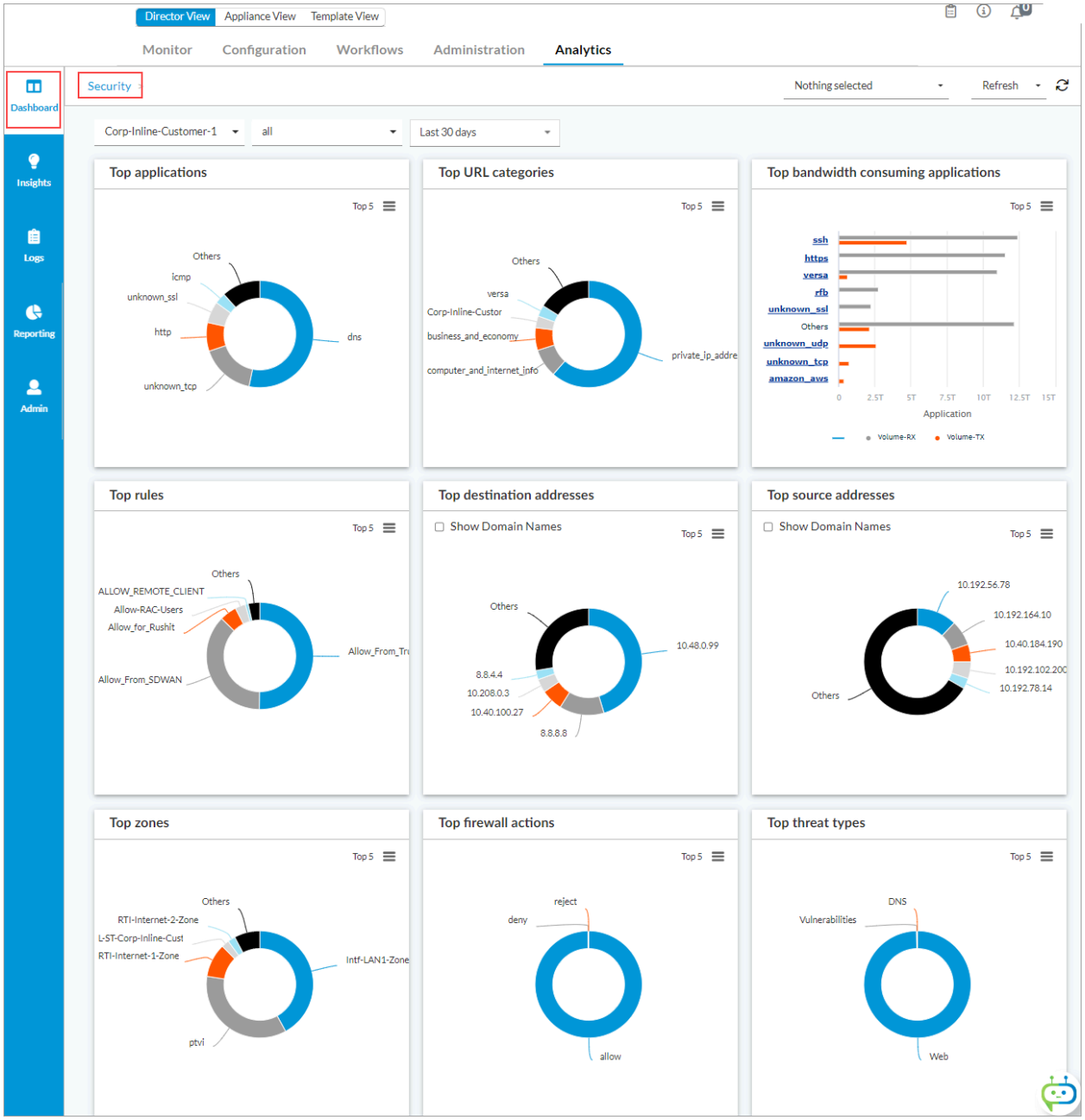
To display Firewall logs sent to Analytics clusters, select Analytics > Logs > Firewall in the left menu bar, and then select the Logs tab in the horizontal menu bar.



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

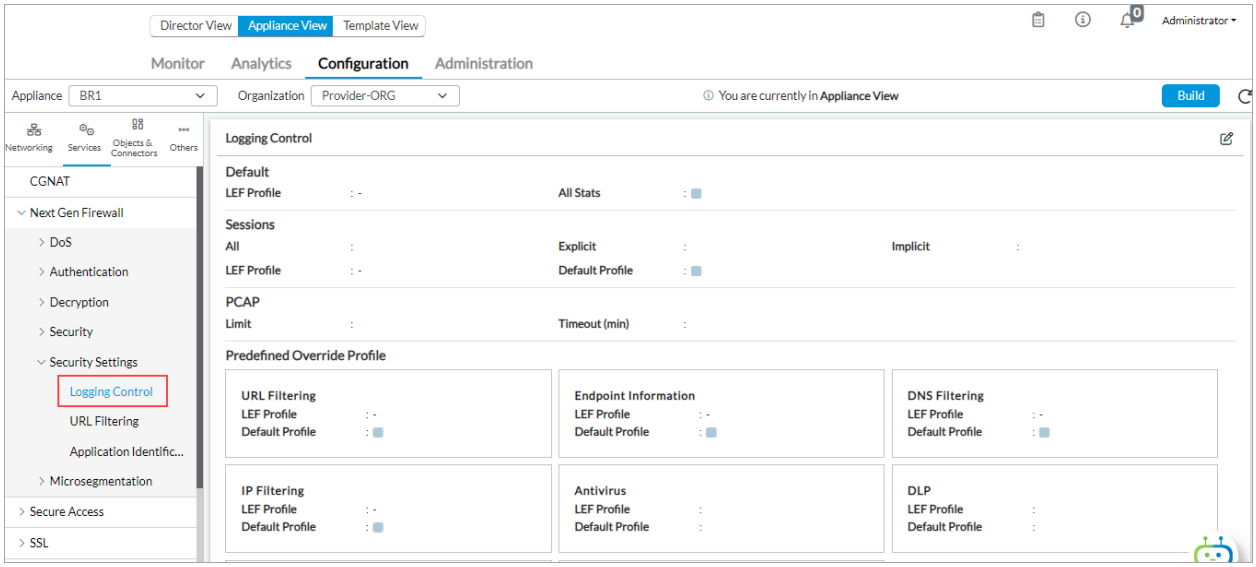
To export firewall summary statistical logs, select a LEF profile and select the All Stats option when you configure logging control for NGFW. For information about configuring NGFW, see Configure NGFW.

To export firewall summary statistical logs:

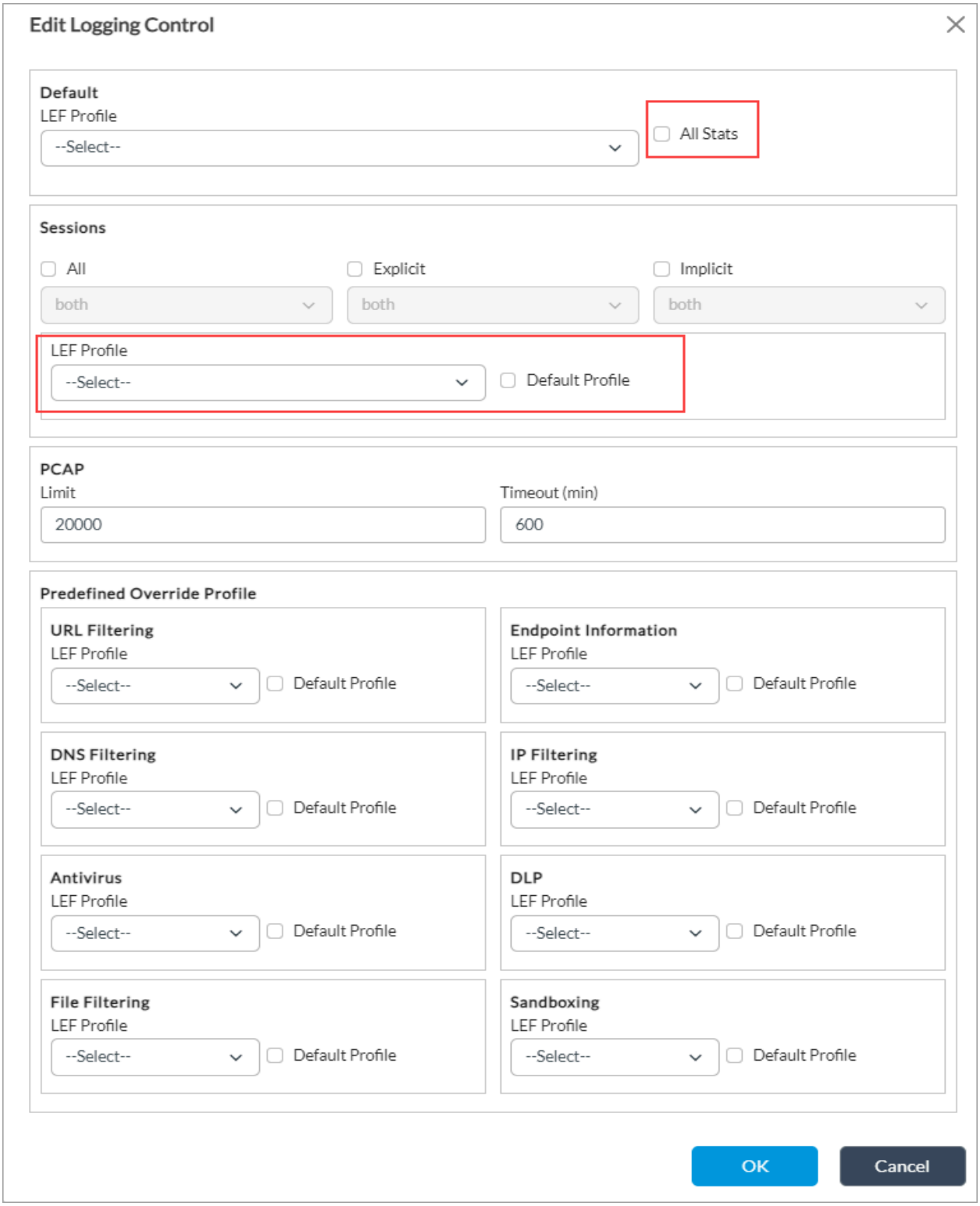
1. In Director view:

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.



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



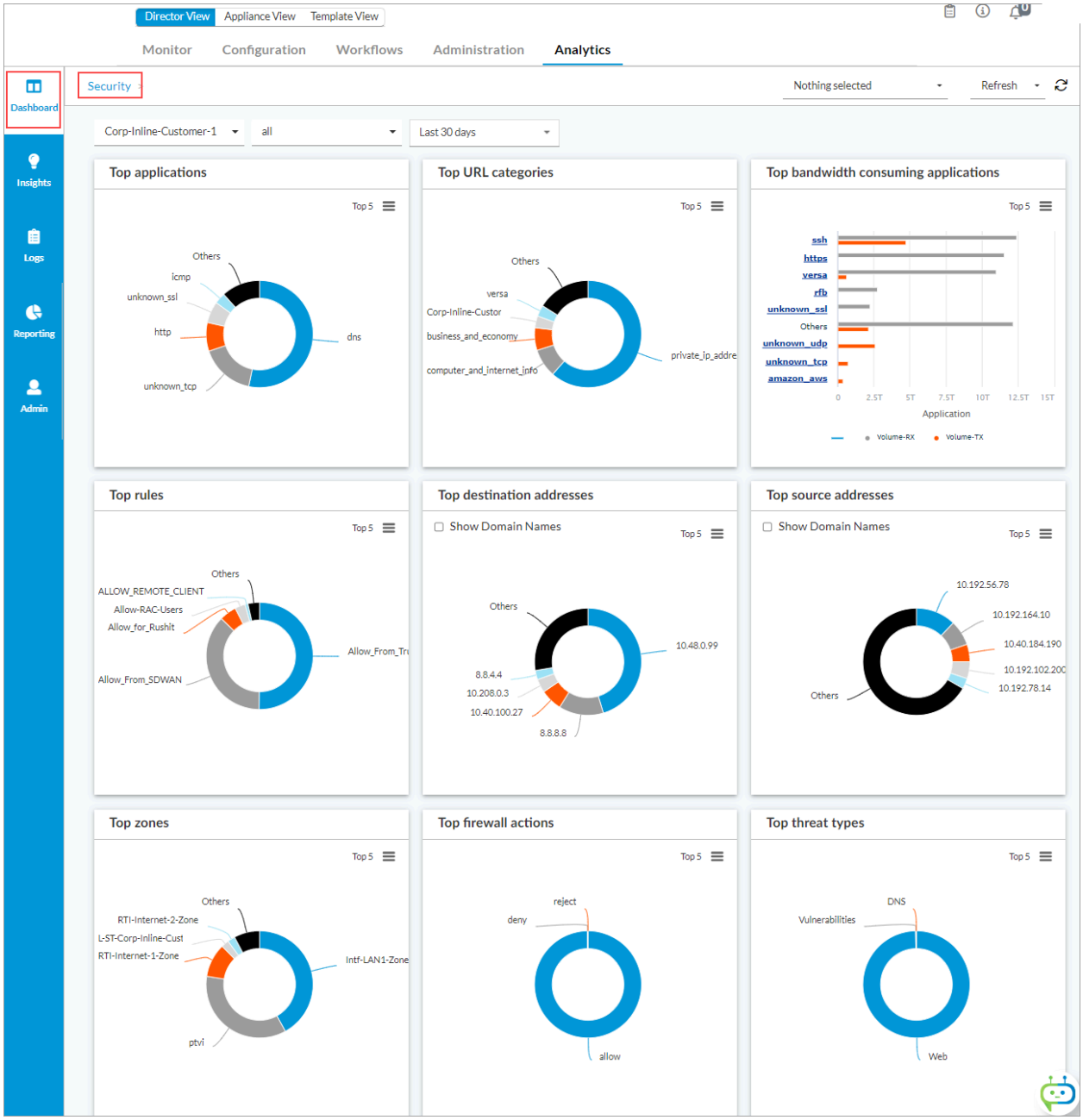
5. Select a LEF profile, and then click All Stats.
6. Click OK.

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

screens:

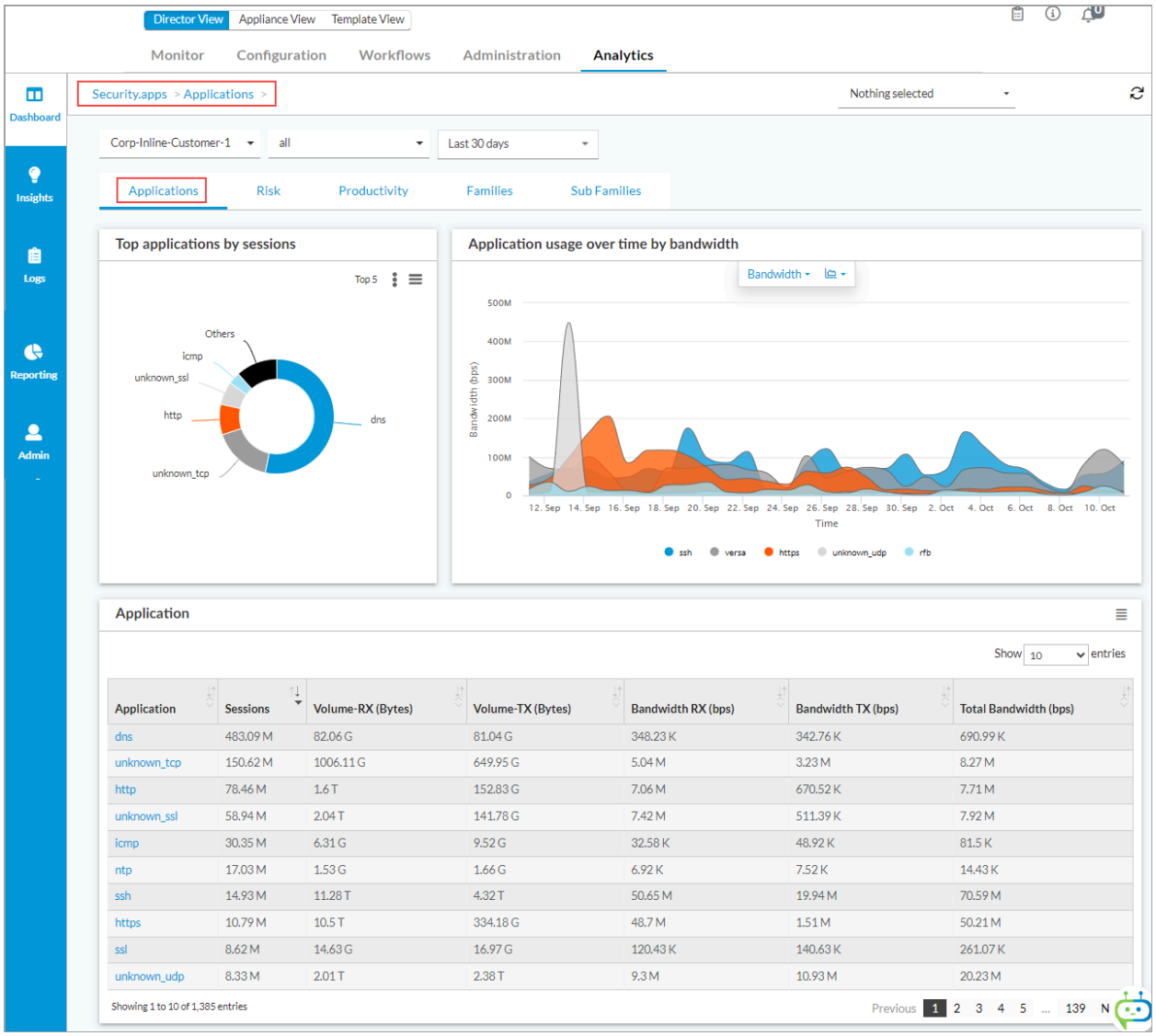
- Analytics > Dashboards > Security
- Analytics > Dashboard > Security > Applications
- Analytics > Dashboards > Security > Web
- Analytics > Dashboards > Security > Firewall

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

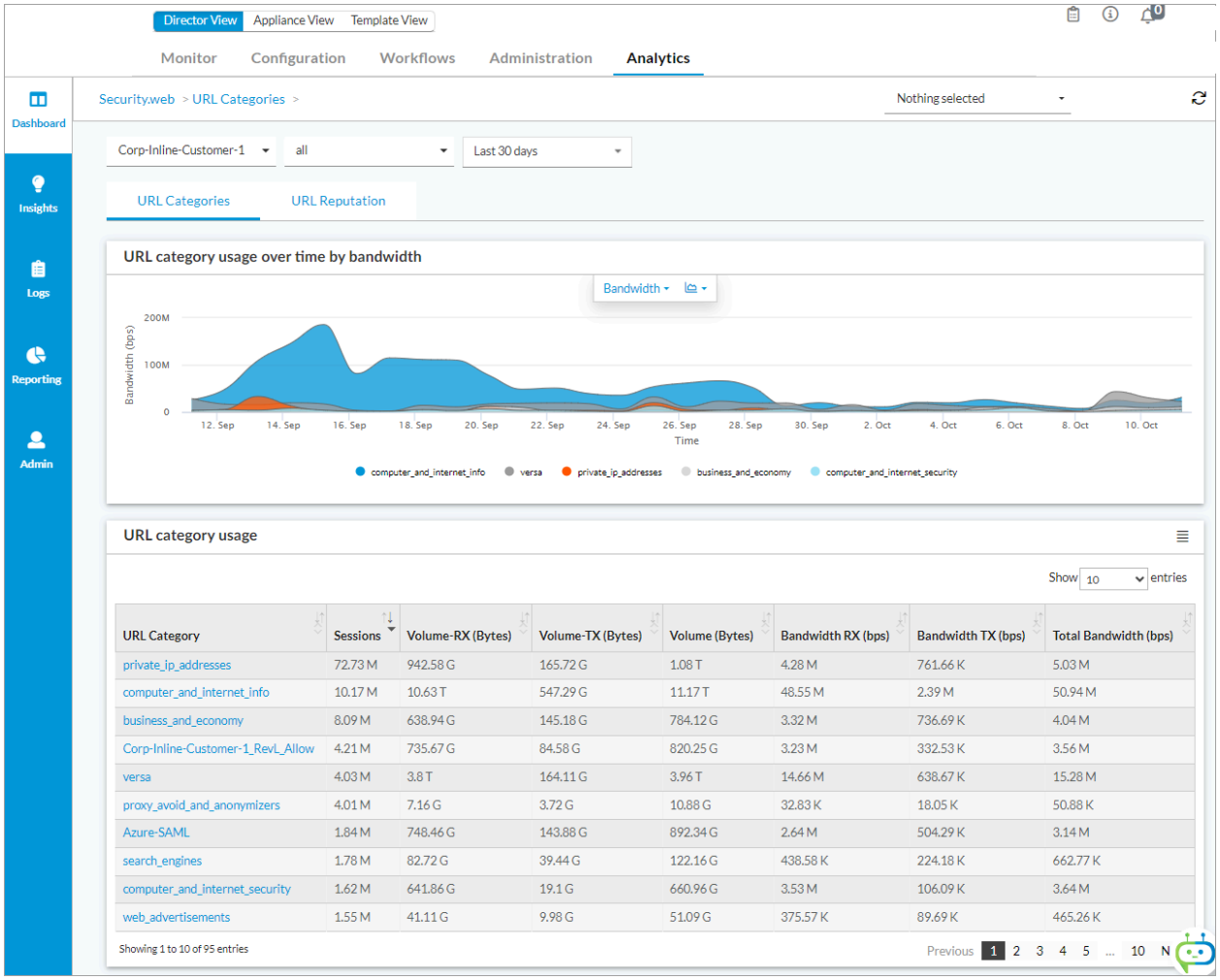


Updated: Wed, 23 Oct 2024 08:27:55 GMT

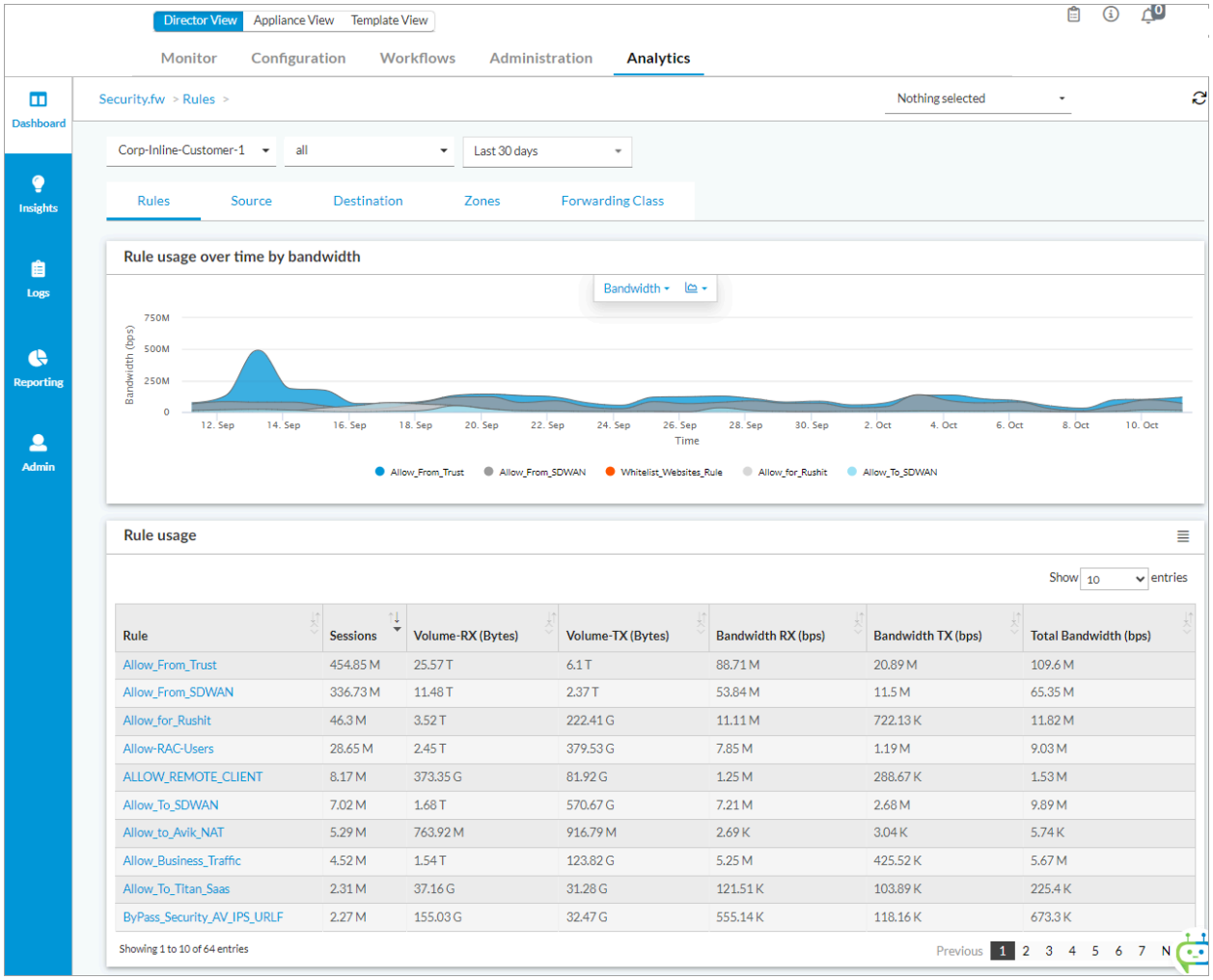
For logs sent to Analytics clusters, to display the applications dashboards, select Analytics > Dashboards > Security in the left menu bar, and then select the Applications tab in the horizontal menu bar.



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



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

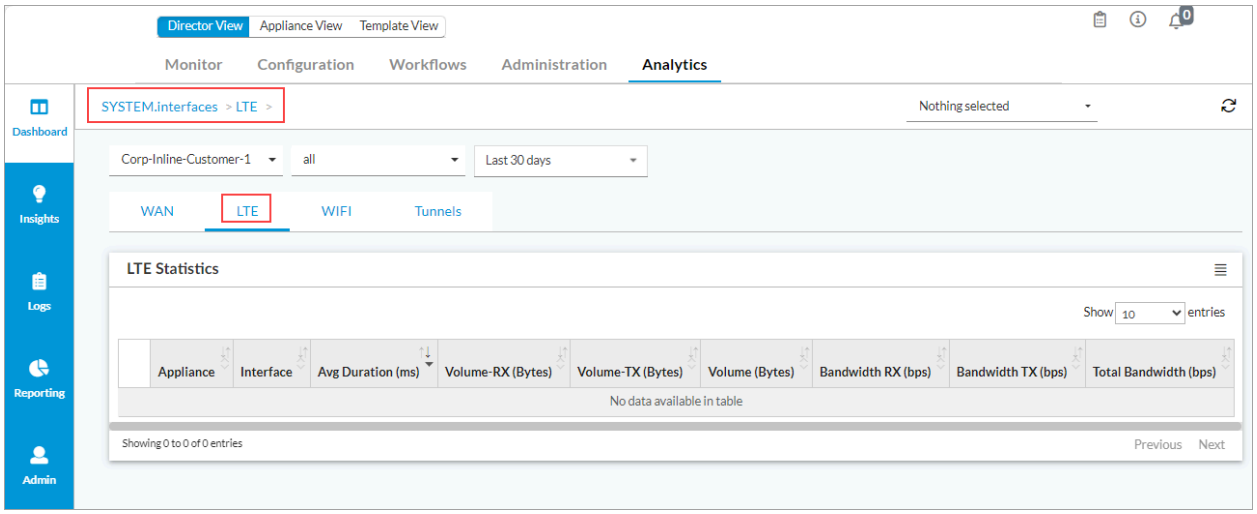


Configure LTE Summary Logging

- Syslog identifiers—lteEventLog, lteStatsLog
- 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.



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

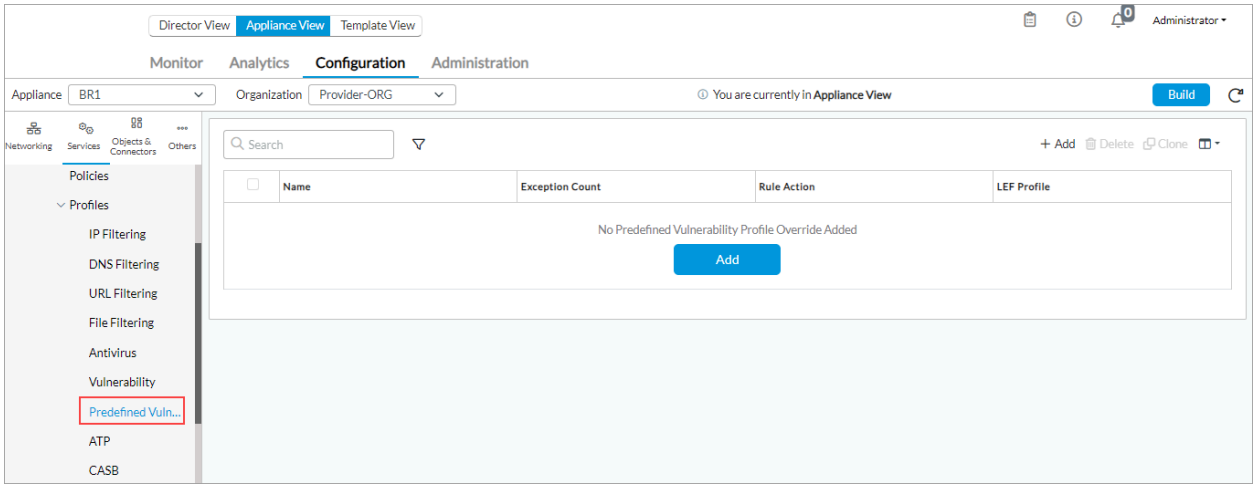
For IDP, you enable packet capture in a vulnerabilty profile rule. Packet capture logs are sent to the active collector configured in the LEF profile associated with the vulnerability profile. For more information, see Configure IDP Threat Detection Vulnerability Logging, below.

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

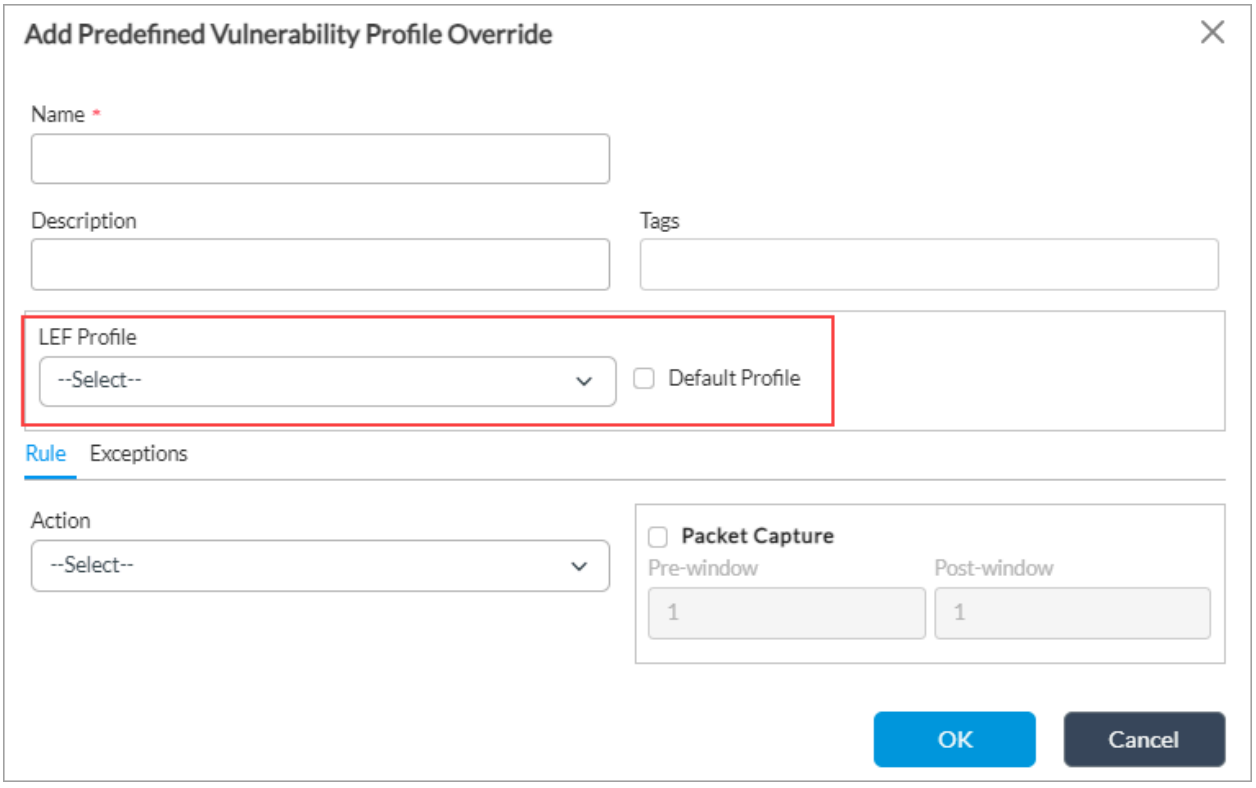
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select an organization in the left menu bar. To have the menu display tenant organizations, double-click the provider organization.

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.



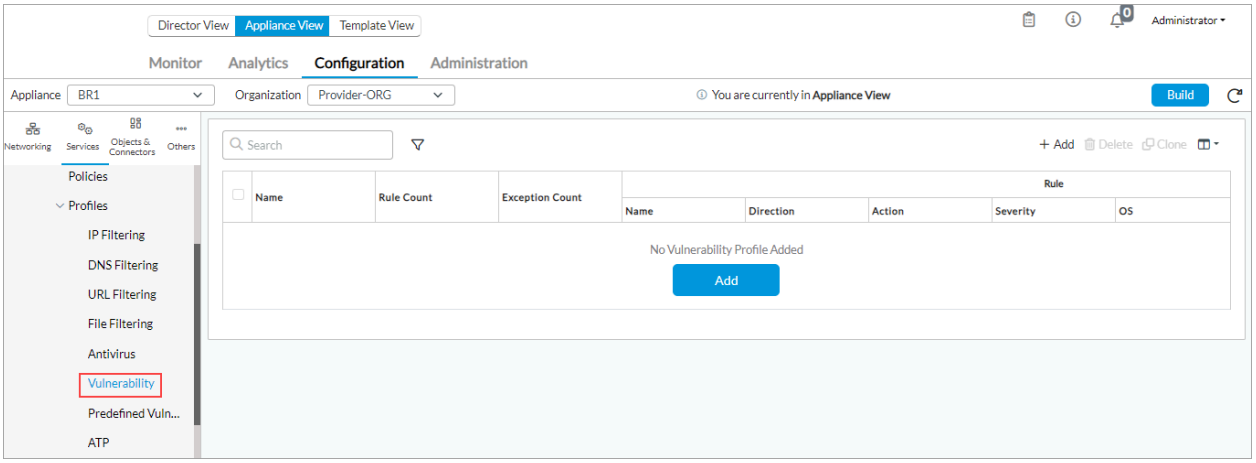
5. Ensure that a LEF profile is selected or that Default Profile is checked, and then enter information for the following fields:

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

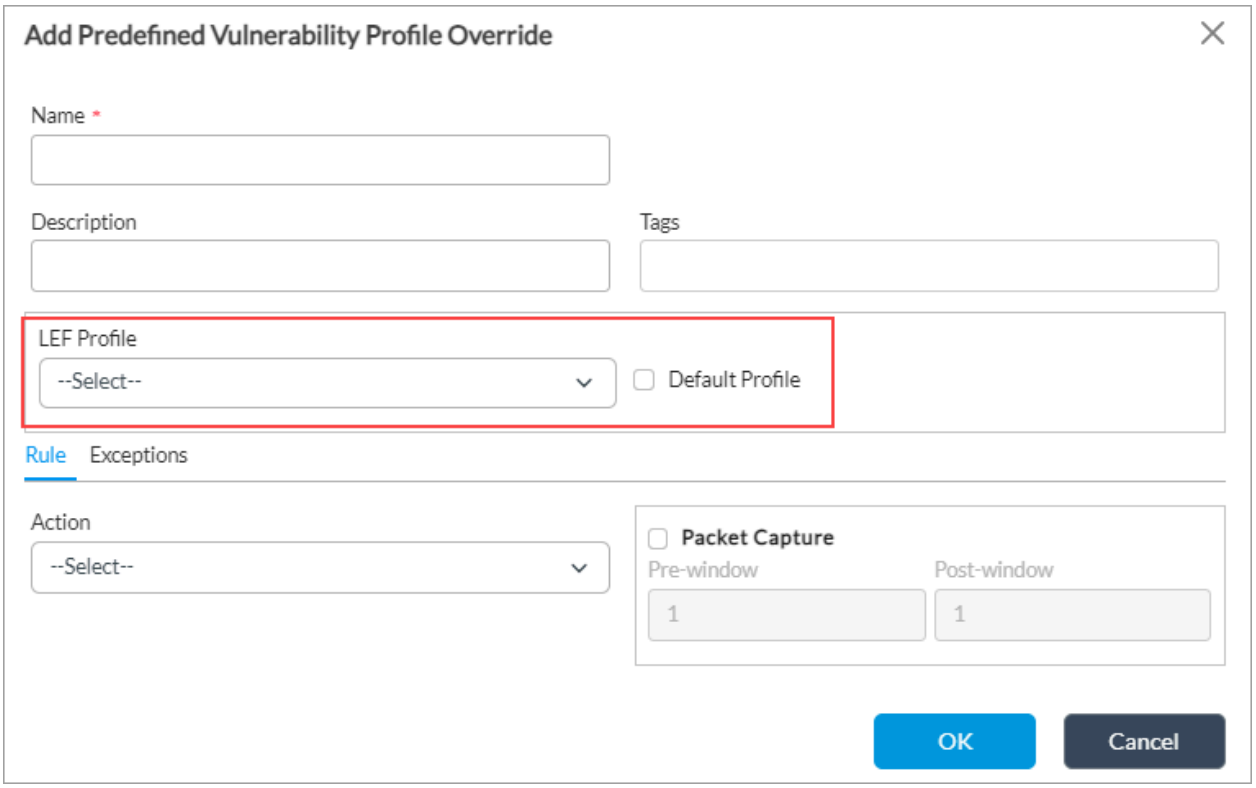
6. Click OK.

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

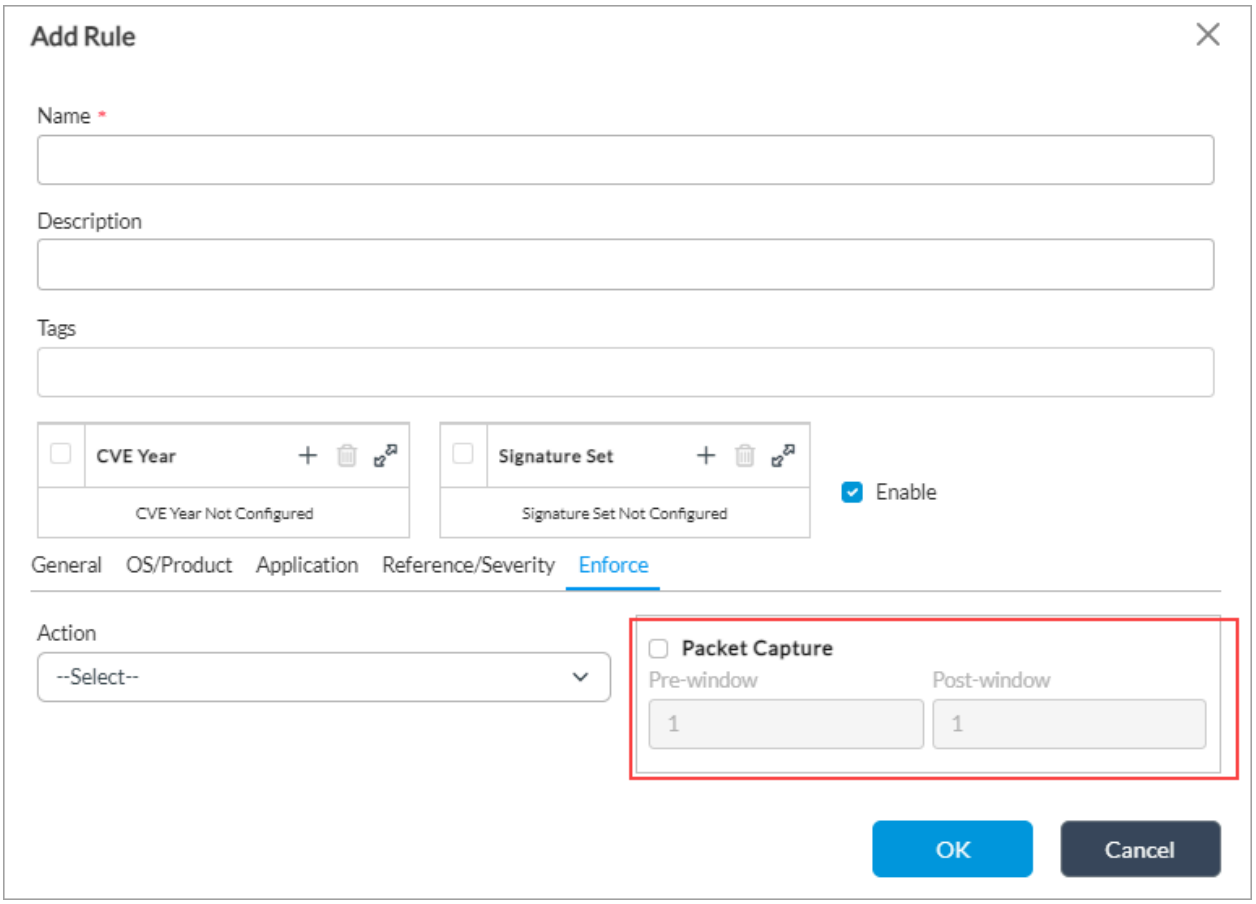
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select an organization in the left menu bar. To have the menu display tenant organizations, double-click the provider organization.
   d. Select the device in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



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.



Field	Description
Packet Capture (Group of Fields)	Click to enable packet capture. Packet capture logs are sent to the active c
◦ Pre-window	Enter the number of packets immediately preceding the attacked packet th
◦ Post-window	Enter the number of packets immediately following the attacked packet tha

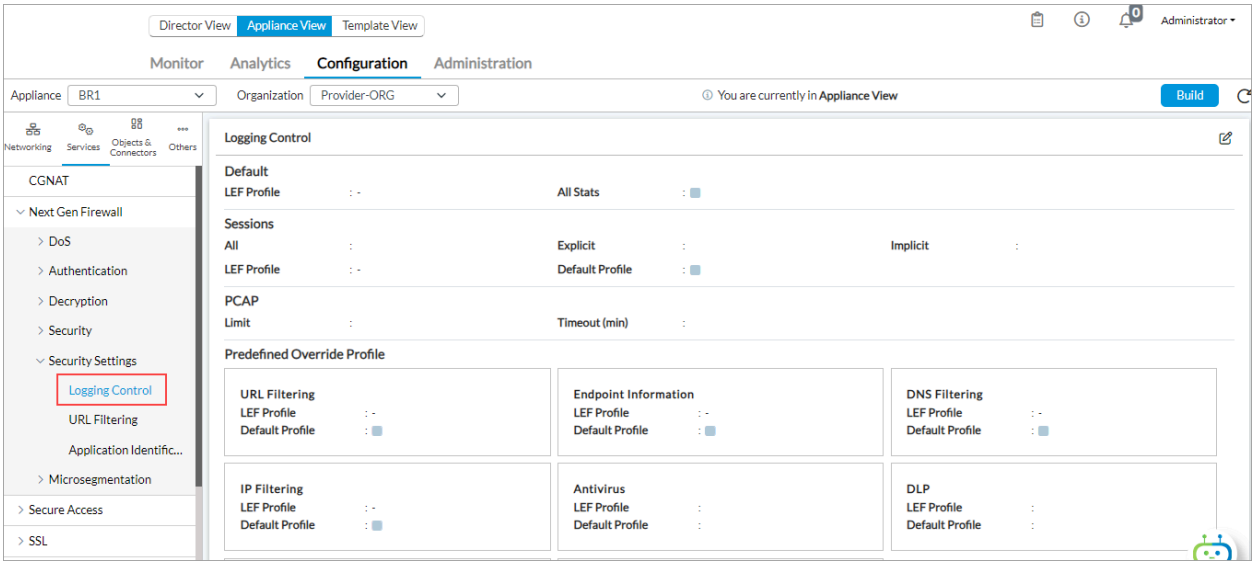
8. Click OK.

Configure NGFW Packet Capture

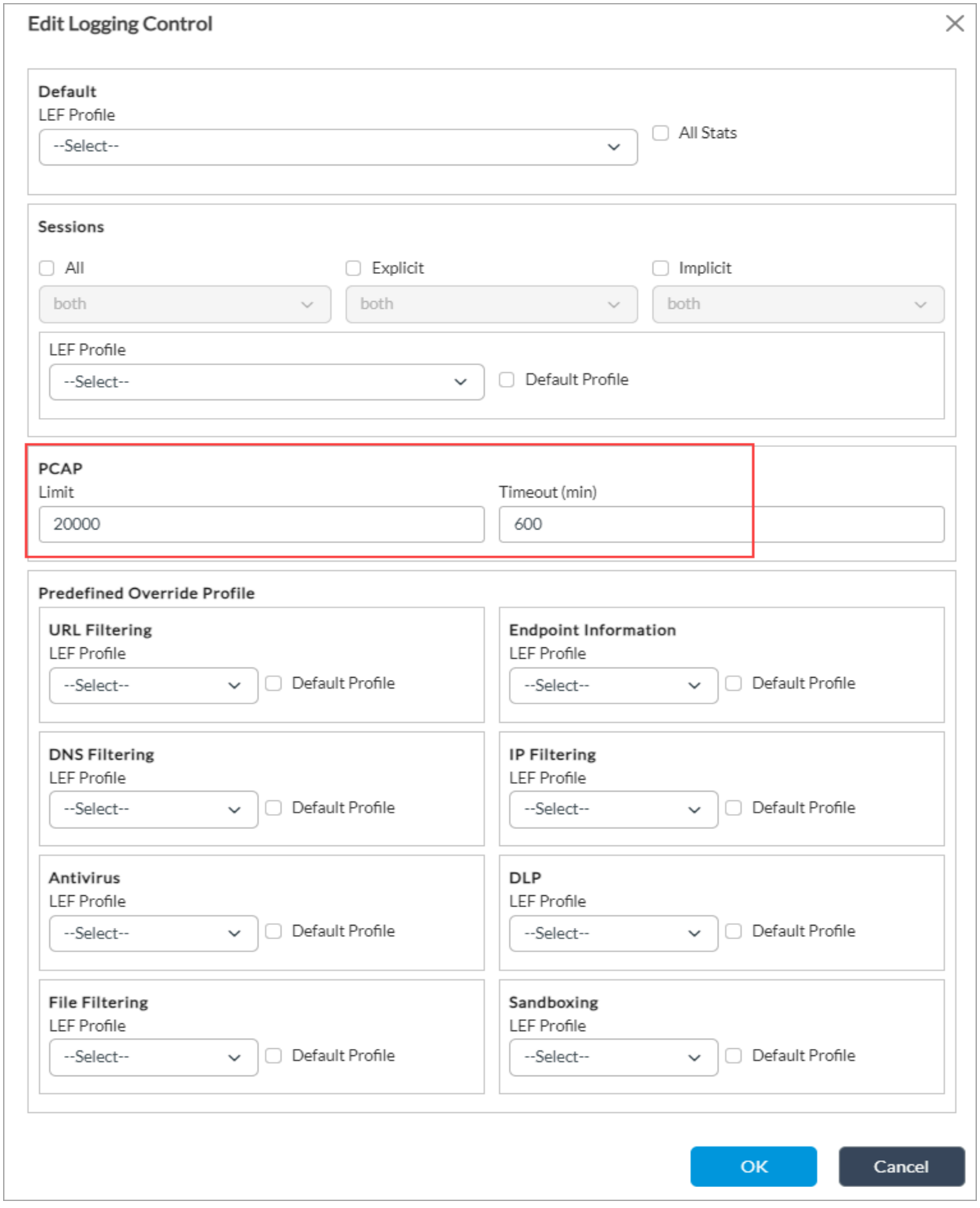
For NGFW, you enable packet capture in an access policy rule, and logs are sent to the active collector of the LEF profile associated with the policy rule. For packet capture logs, you can also set a default packet capture limit and timeout. When you enable packet capture logging in an access policy 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.



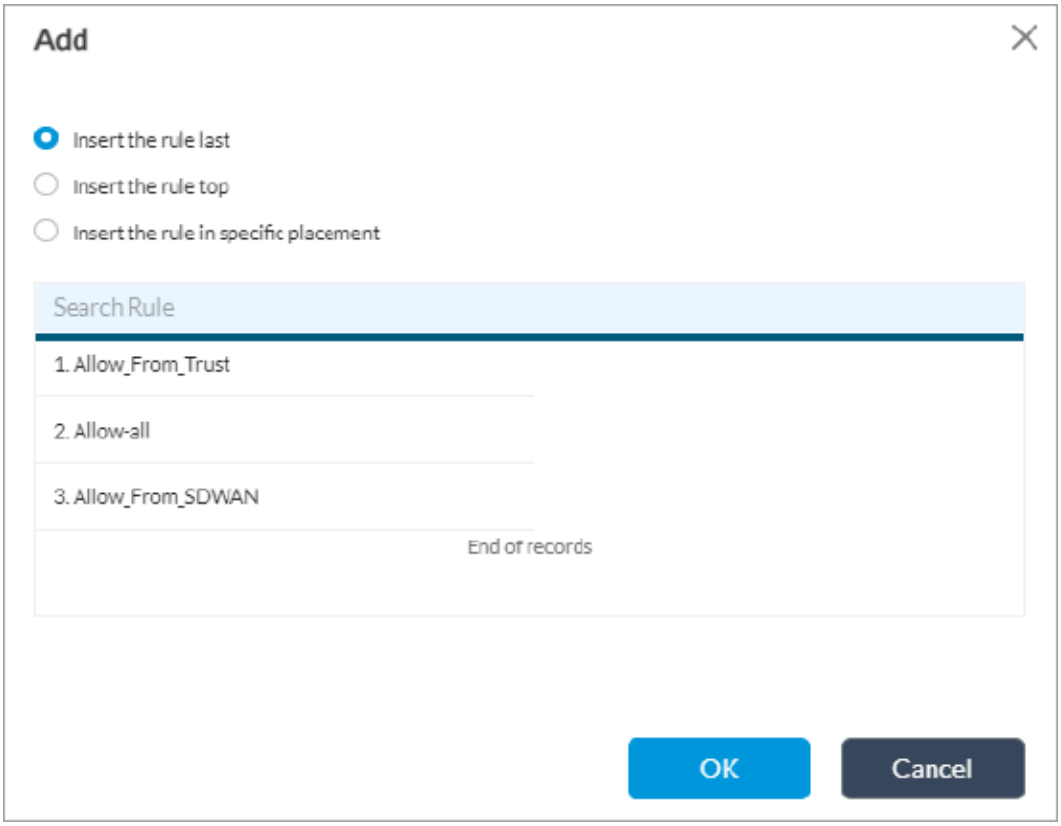
5. Click the Edit icon. In the Edit Logging Control popup window, enter information for the following fields.



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

To enable packet capture in an access policy rule:

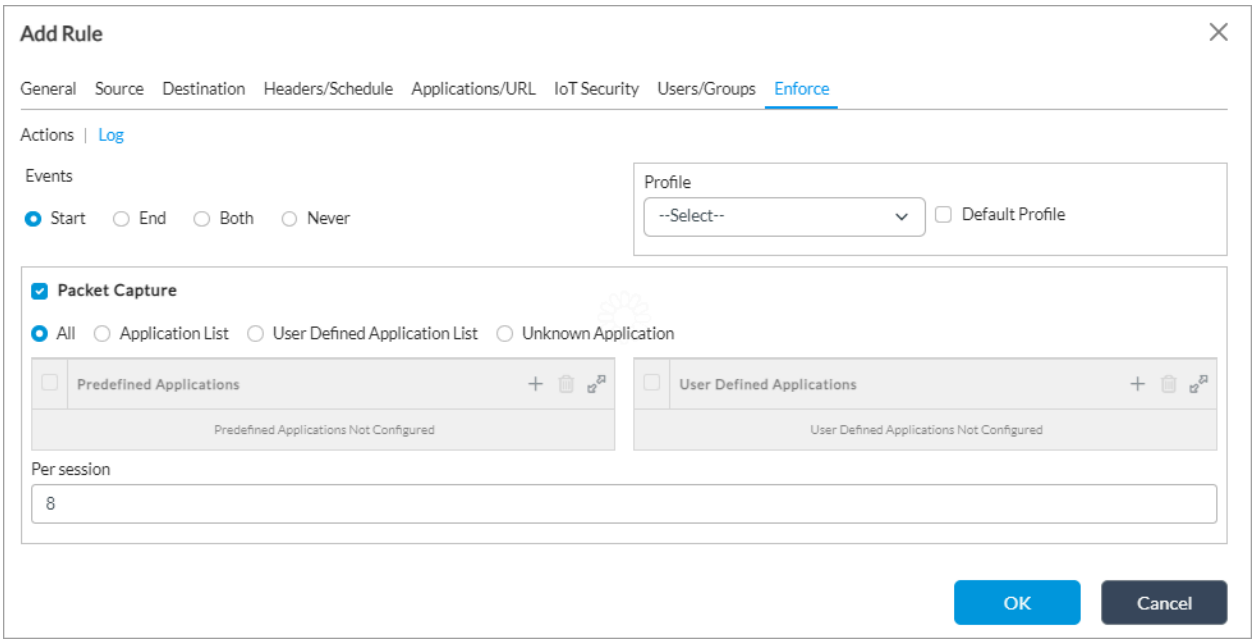
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select an organization in the left menu bar. To have the menu display tenant organizations, double-click the provider organization.
   d. Select the device in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

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



Field	Description
Log (Group of Fields)	
◦ Events	Select an option for logging the data: ◦ 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.
◦ LEF Profile	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 an Log Export Functionality. For information about associating a LEF profile with a featu Functionality.
Packet Capture (Group of Fields)	
◦ Packet Capture	Click, and then select the application type of the packets to capture: ◦ All ◦ Application List ◦ Unknown Application ◦ User-Defined Application List For each category, select one of the following options: ◦ Predefined Applications—Click to select a predefined application. ◦ User-Defined Applications—Click to select a custom-defined application. Packet capture logs are sent to the active collector of the LEF profile.
◦ Per Session	Enter the number of sessions allowed per log. *Default:* 8 sessions

Configure Packet Capture for Traffic Monitoring Flows

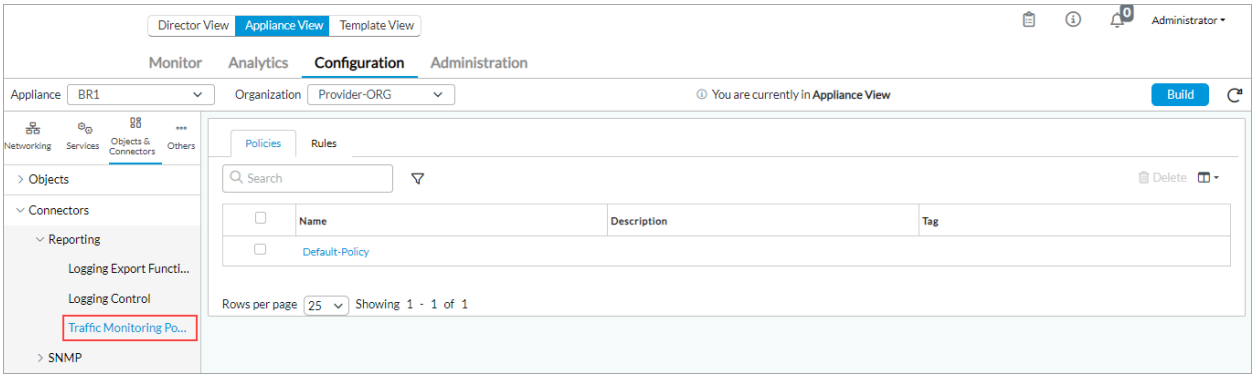
To export packet capture logs for selected types of traffic monitoring flows, you enable packet capture in a traffic-monitoring policy rule. The packet capture logs are sent to the active collector configured in the LEF profile associated with the policy rule. For information about configuring traffic-monitoring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

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

1. In Director view:

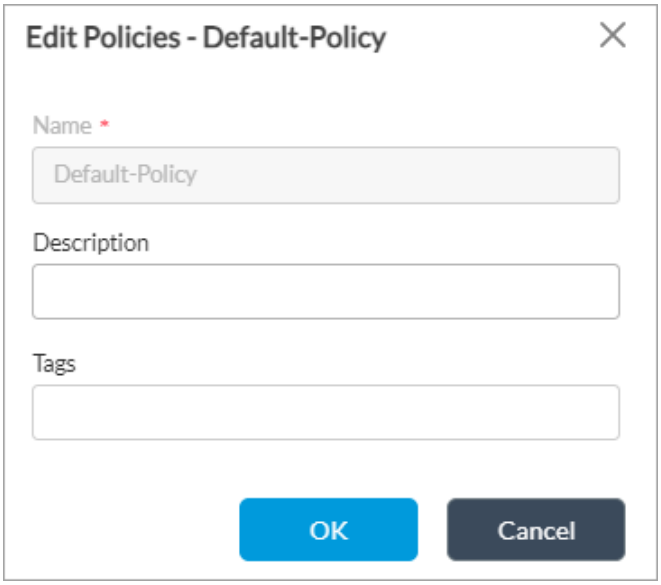
a. Select the Configuration tab in the top menu bar.
b. Select Devices > Devices in the horizontal menu bar.
c. Select an organization in the left menu bar.
d. Select a branch in the main pane. The view changes to Appliance view.

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.



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.

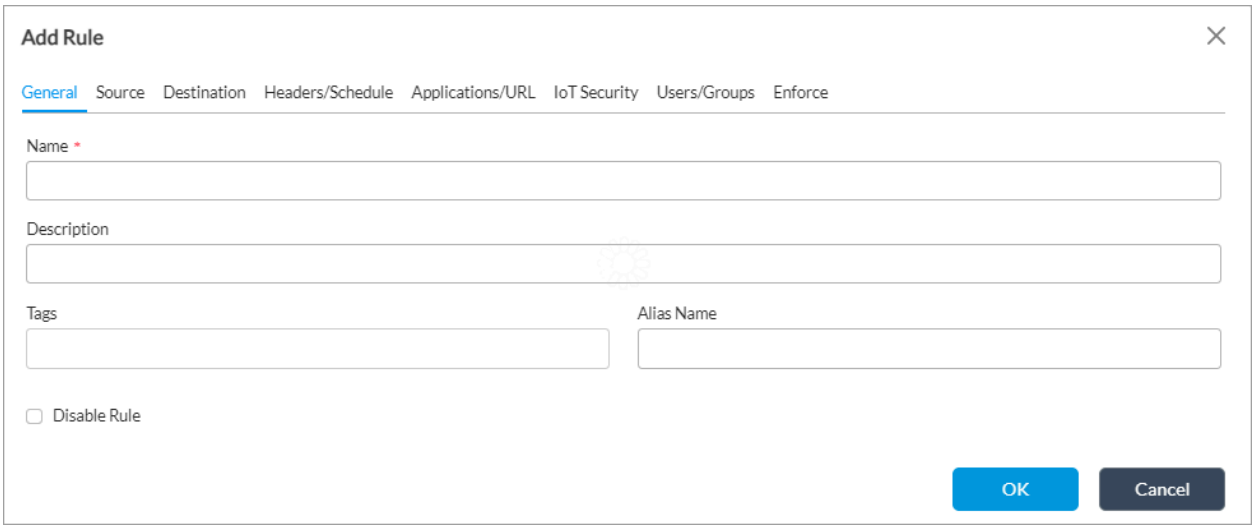


Field	Description
Name	Enter a name for the traffic monitoring policy.
Description	Enter a text description for the policy.
Tag	Enter a keyword or phrase that allows you to filter the policy name. Tagging is useful when you have many policies and want to view those that are tagged with a particular keyword.

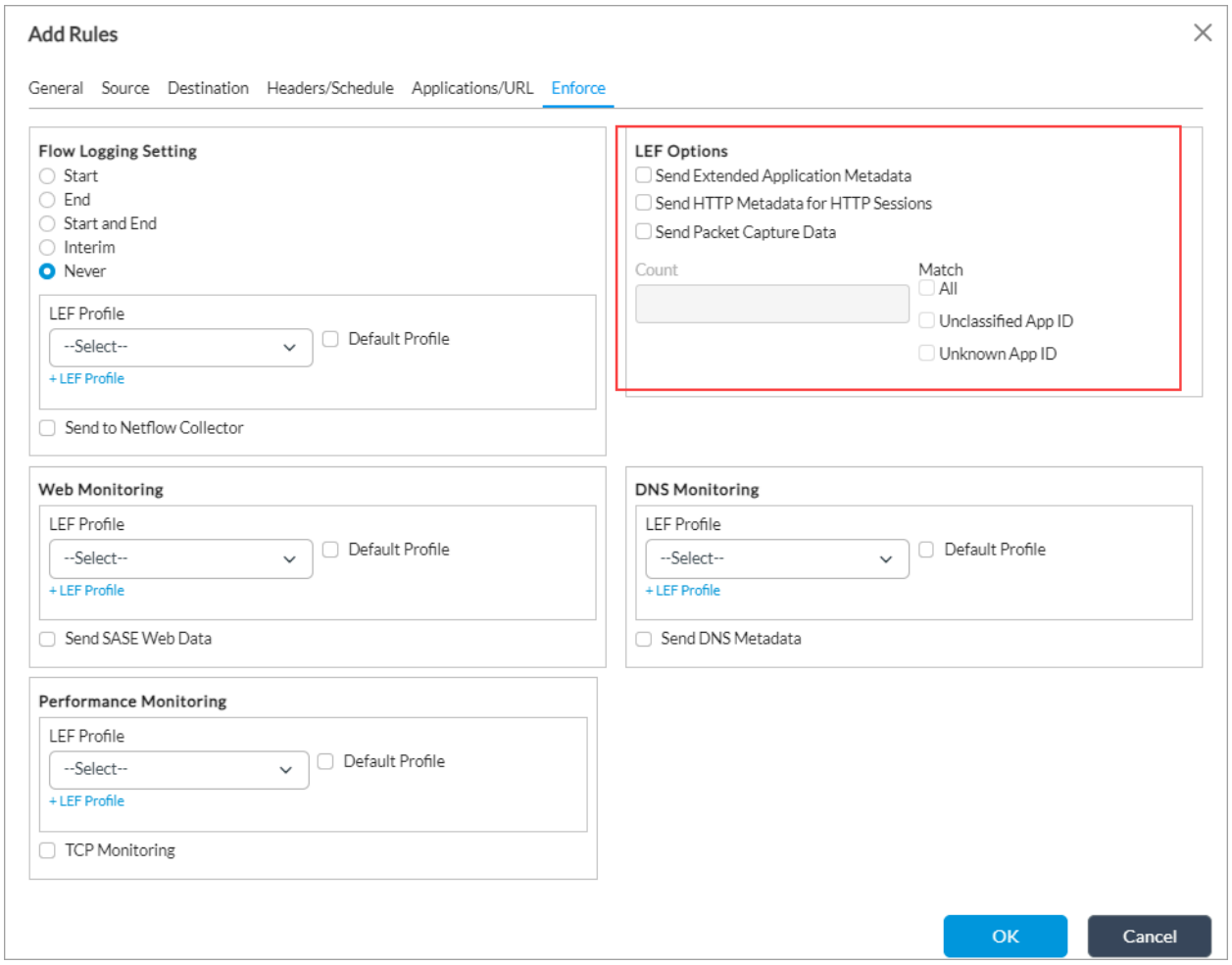
c. Click OK.

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.



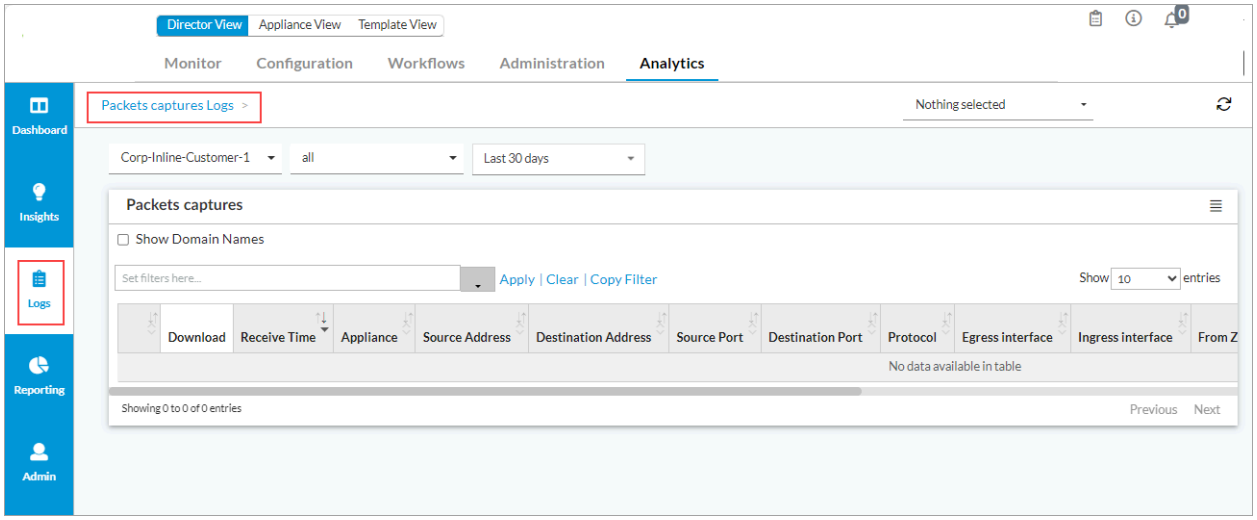
6. If you are adding a new rule:
   a. Select the General tab, and in the Name field enter a name for the rule name.
   b. Select one or more the following tabs to define the policy rule. For information about the fields on these tabs, see Configure Policy-Based Forwarding.
      - Source/Destination 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.



Field	Description
LEF Profile	Select the LEF profile to associate with the traffic monitoring rule, or click Defaul LEF profile.
LEF Options (Group of Fields)	
◦ Send Packet Capture Data	Select to send packet capture logs for the items selected on the Source/Destina 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. IAEEntitlementLog
- Paths to the configuration screen:

- 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.

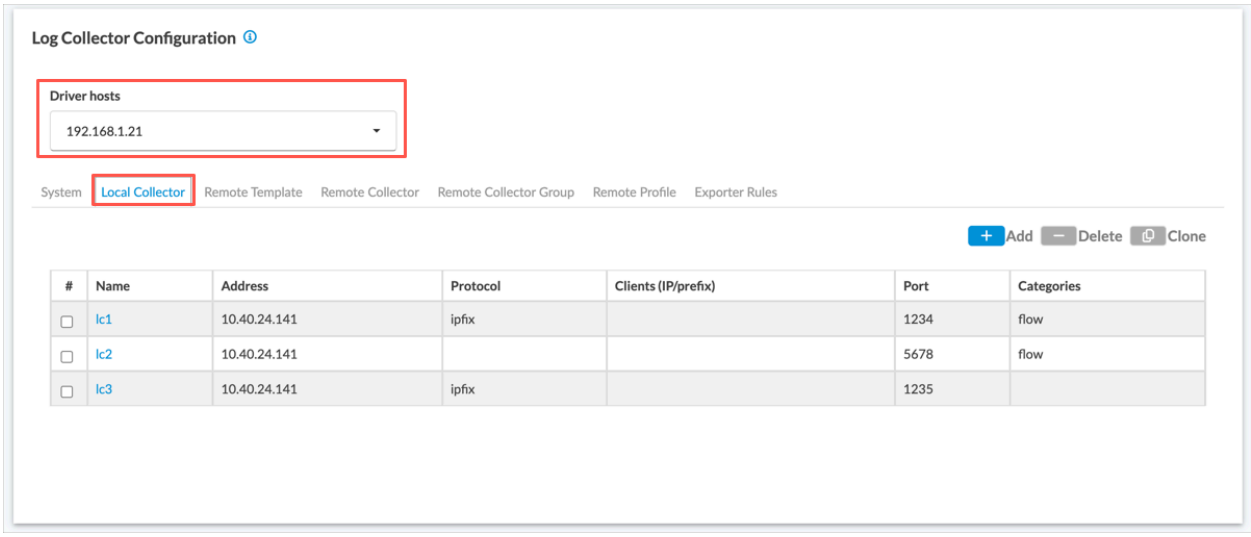
Configure VMS Log Export

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:

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



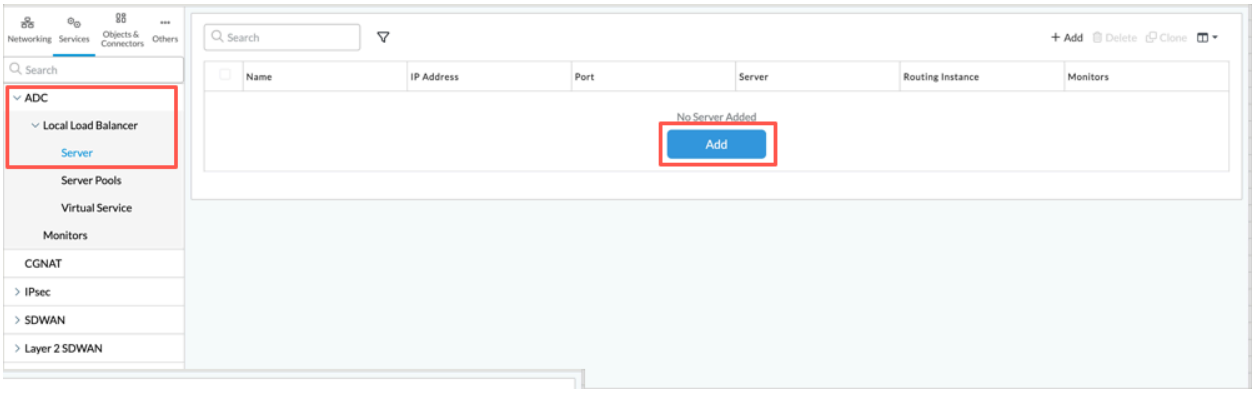
   Driver hosts are Analytics nodes with at least one configured local collector. Driver hosts are typically log-forwarder type Analytics nodes, although database-type and search-type nodes can also be configured with local collectors.
2. If the Analytics cluster contains driver hosts that are not listed 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.

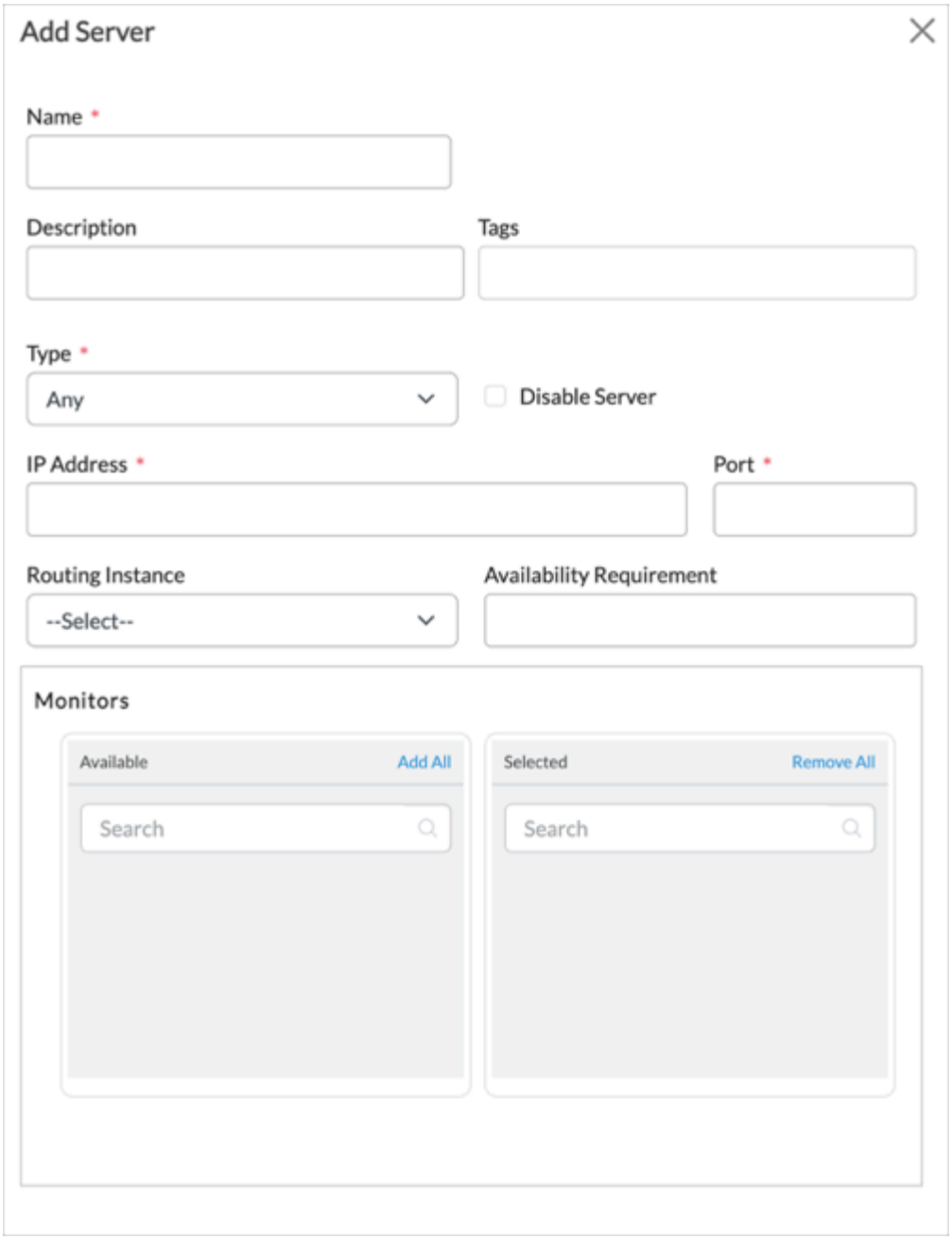
3. In the Driver Hosts field, select a node.
4. Select the Local Collector tab. The screen displays the local collectors configured on the driver host.
5. Note the IP address and port number of the local collector that you want to receive the VMS logs.
6. Repeat Steps 3 through 5 for each driver host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

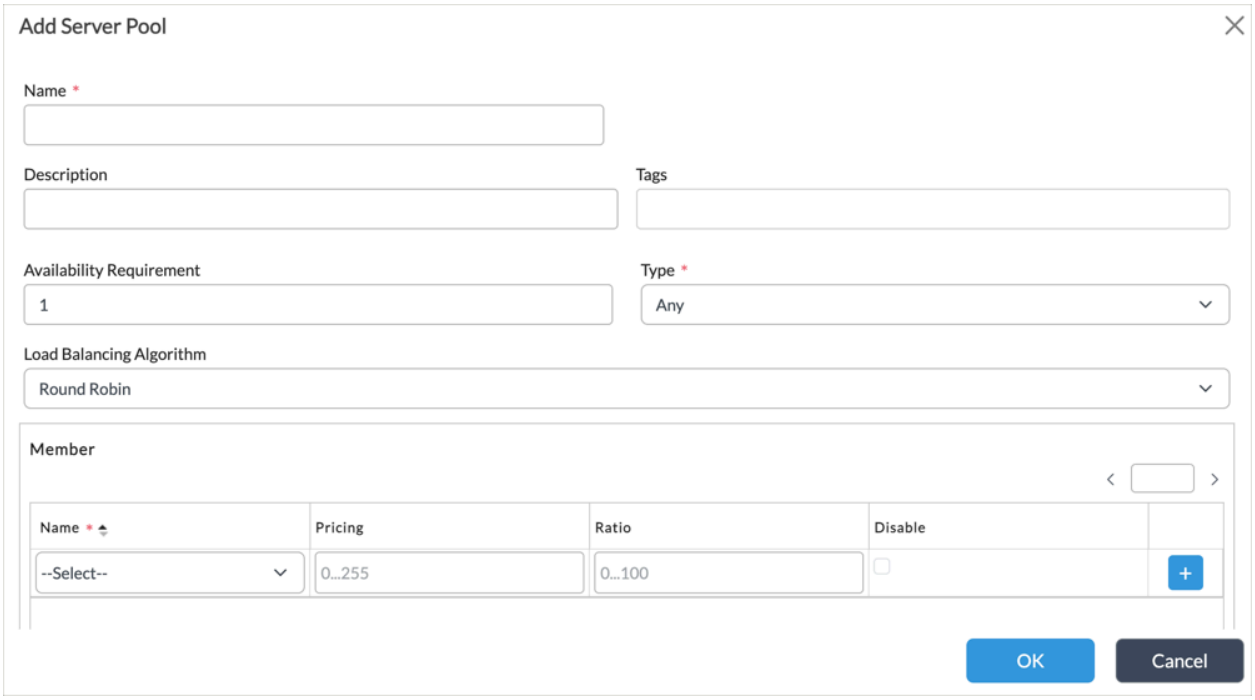


6. Enter information for the following fields.

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.

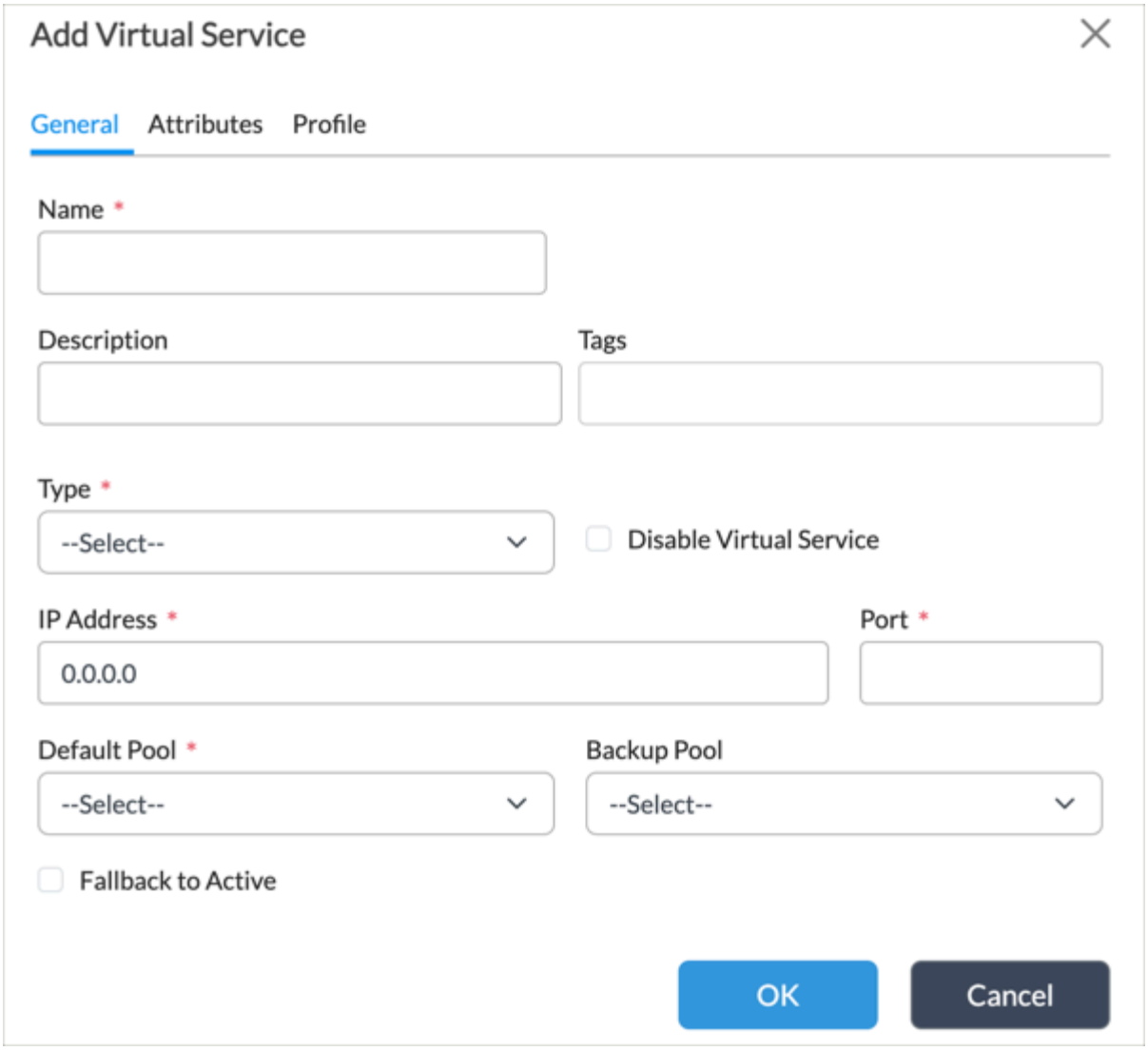
7. Click OK.
8. Repeat Steps 5 through 7 for each local collector you noted in the previous procedure.
9. Select Server Pools in the left menu bar, and then select +Add. The Add Server Pool popup window displays.



10. Enter information for the following fields. For a description of all fields, see Configure an Application Deliver Controller.

Field	Description
Name	Enter a name for the ADC server pool.
Type	Select Any.
Member (Group of Fields)	
◦ Name	Select an ADC server.
◦ Add icons	Click to add the ADC server to the Member table.

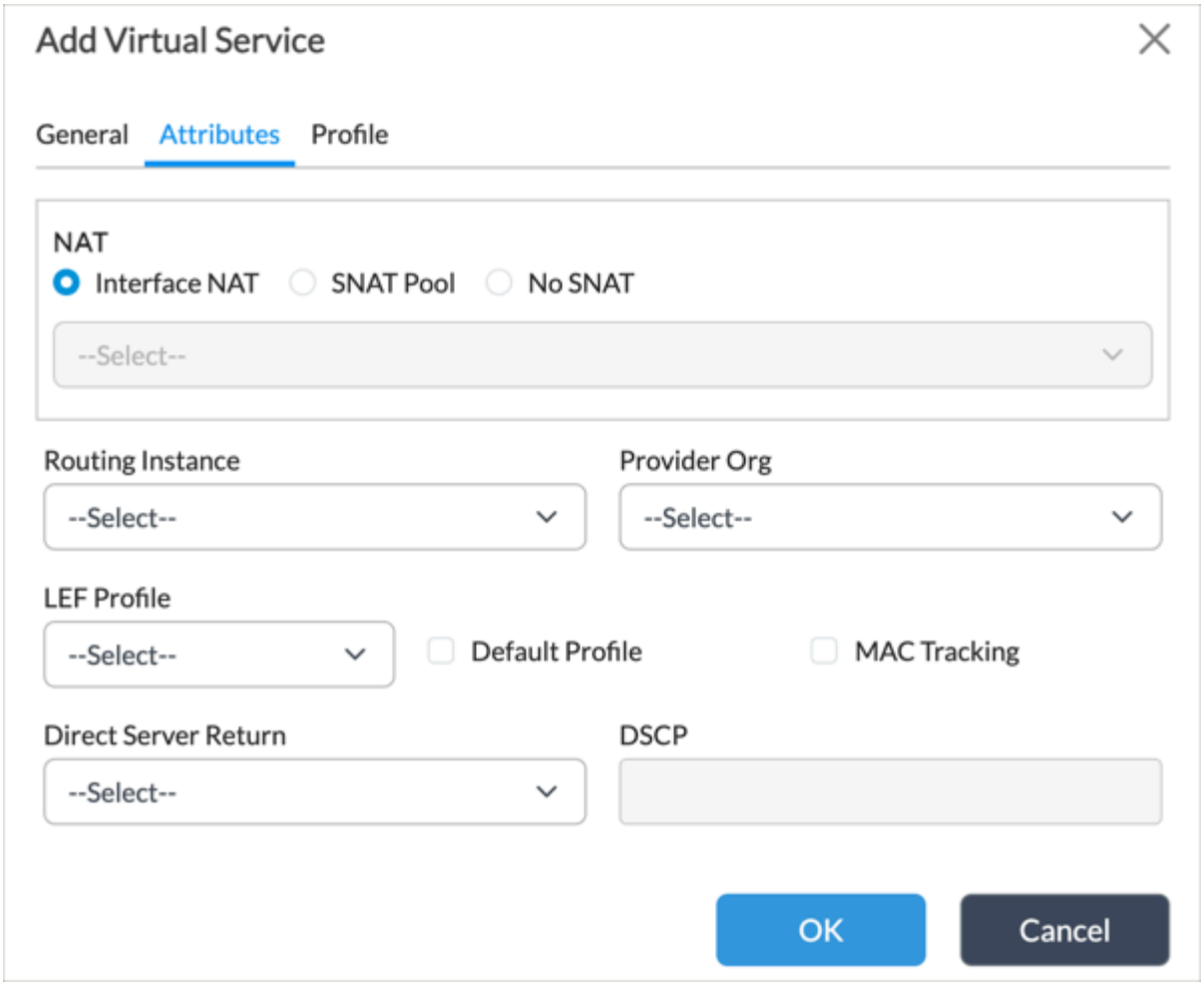
11. In the Member table, add an entry for each ADC server that you configured in Steps 5 through 7.
12. Click OK.
13. Select Virtual Service in the left menu bar, and then select +Add. The Add Virtual Service popup window displays.



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.

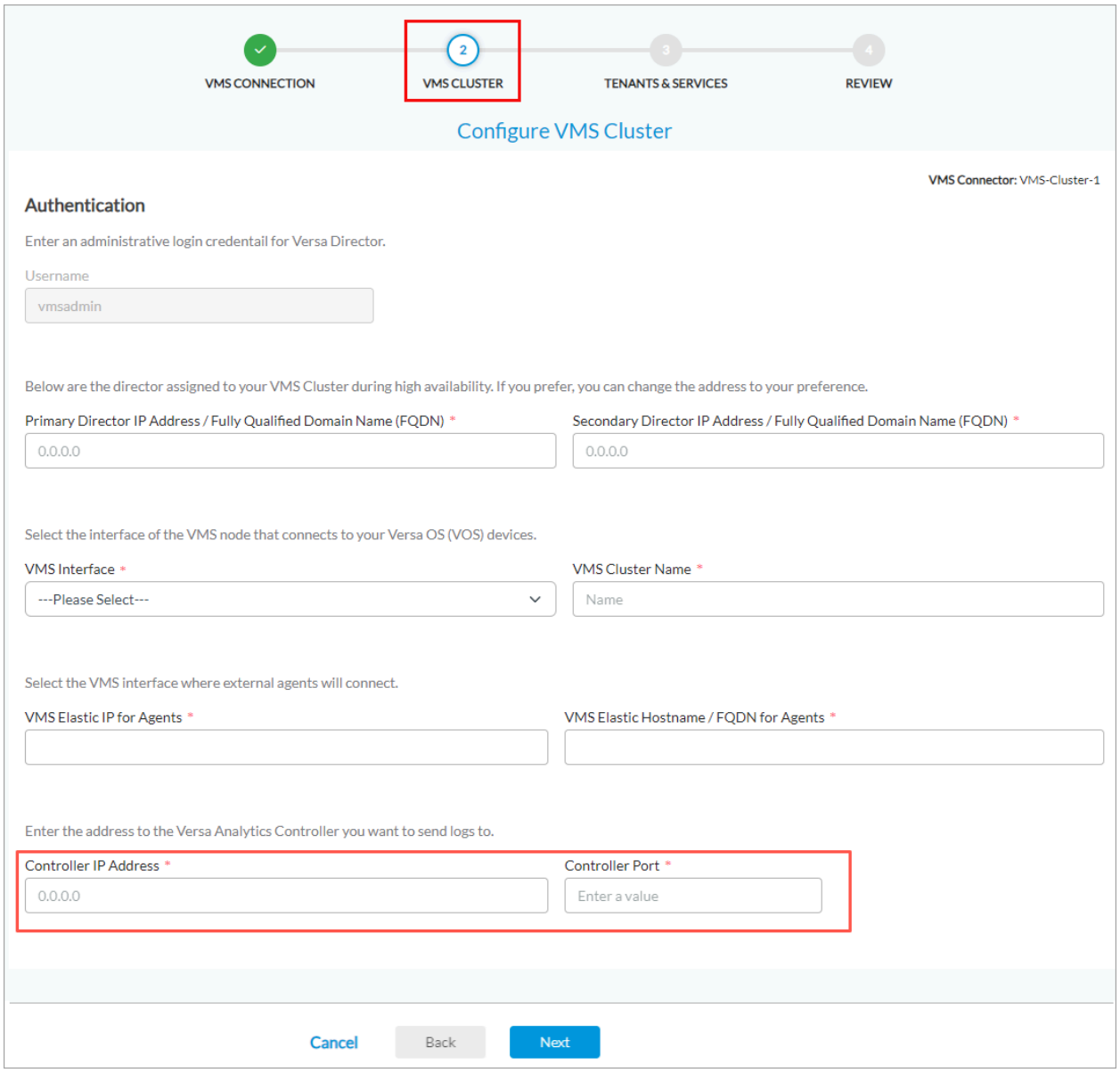
15. Click the Attributes tab.



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.

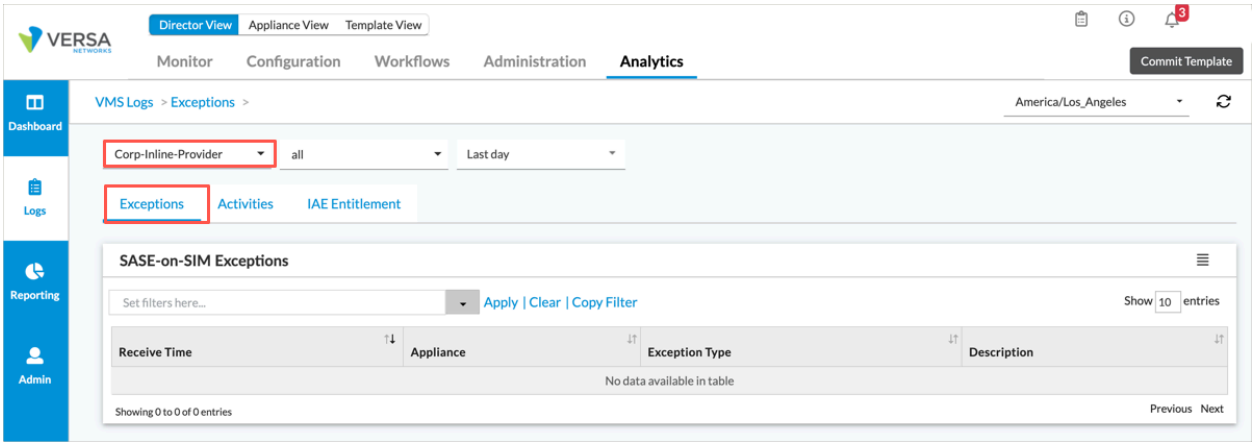


4. Verify that the IP address and port number of the ADC service are listed in the Controller IP Address and Controller Port fields.

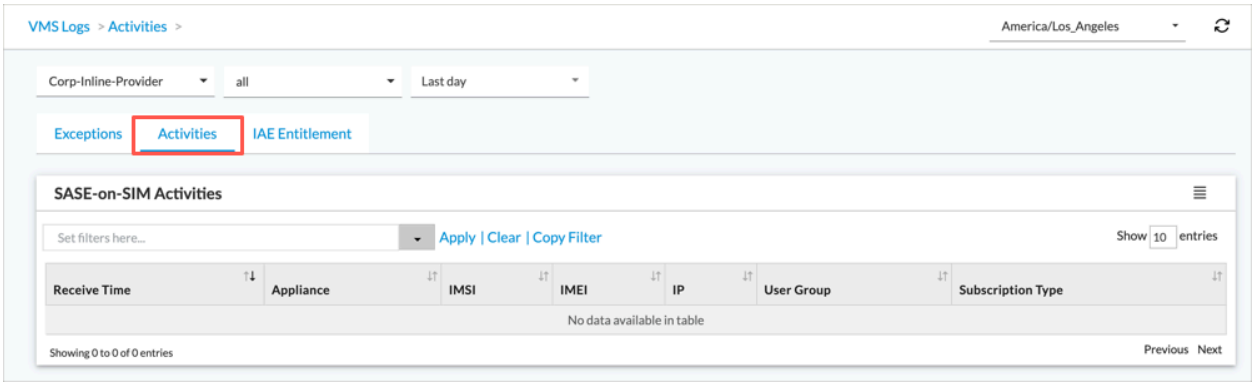
View SASE for SIM Logs

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.

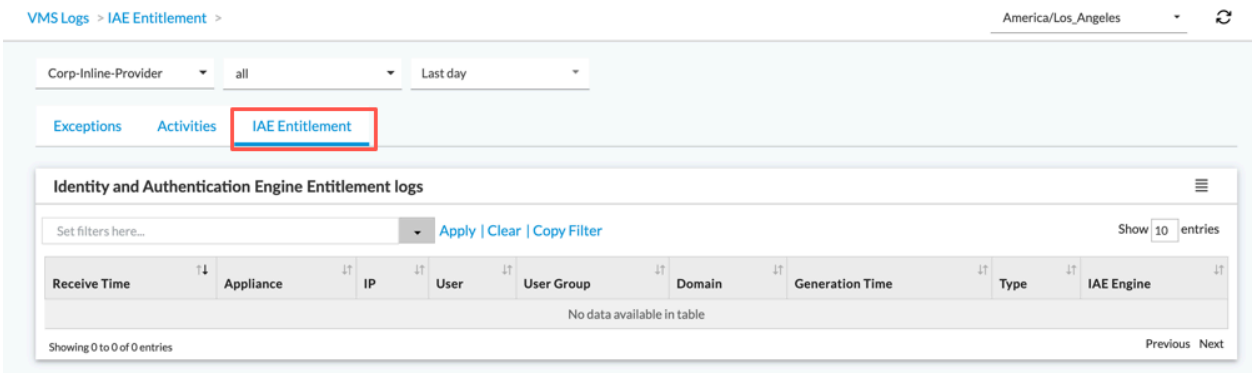
Select the Exceptions tab to display SASE for SIM exceptions logs.



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



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



Configure SASE Web-Monitoring Logging

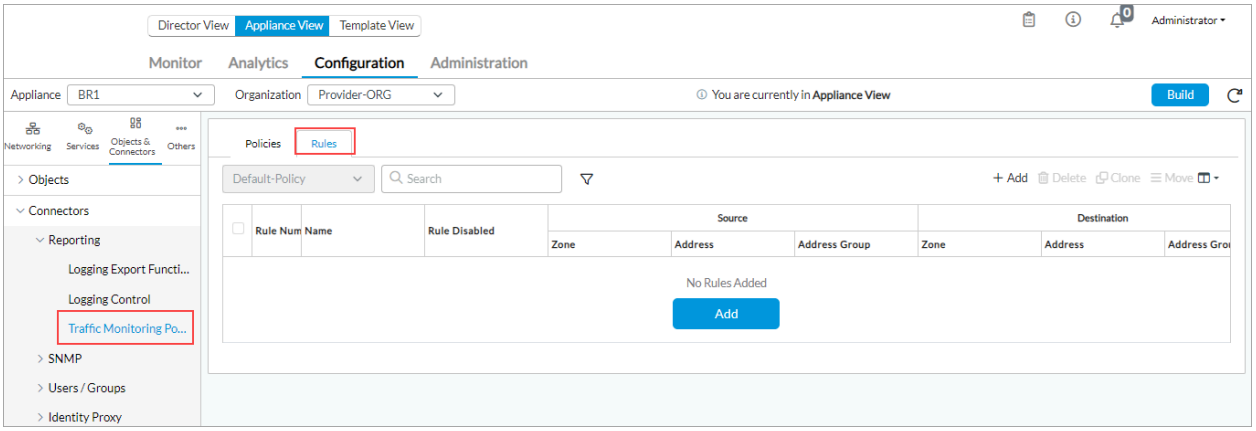
For Releases 22.1.1 and later.

- Syslog identifier—saseWebLog

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

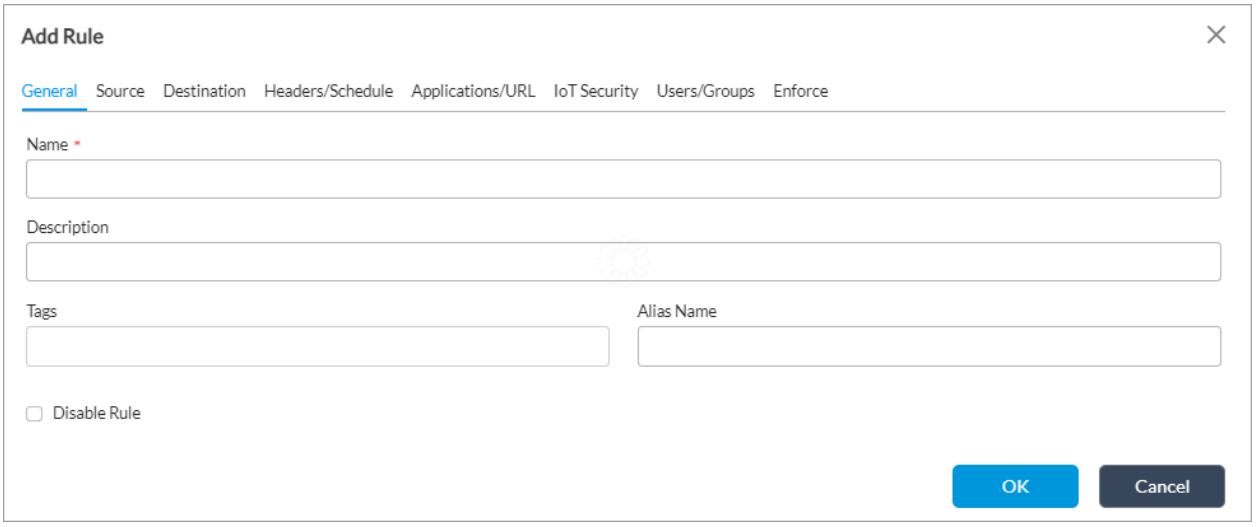
To export SASE web-monitoring logs:

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.
   d. Select a branch in the main pane. The view changes to Appliance view.
2. Select Objects & Connectors > Connectors > Reporting > Traffic Monitoring in the left menu bar. The following screen displays.



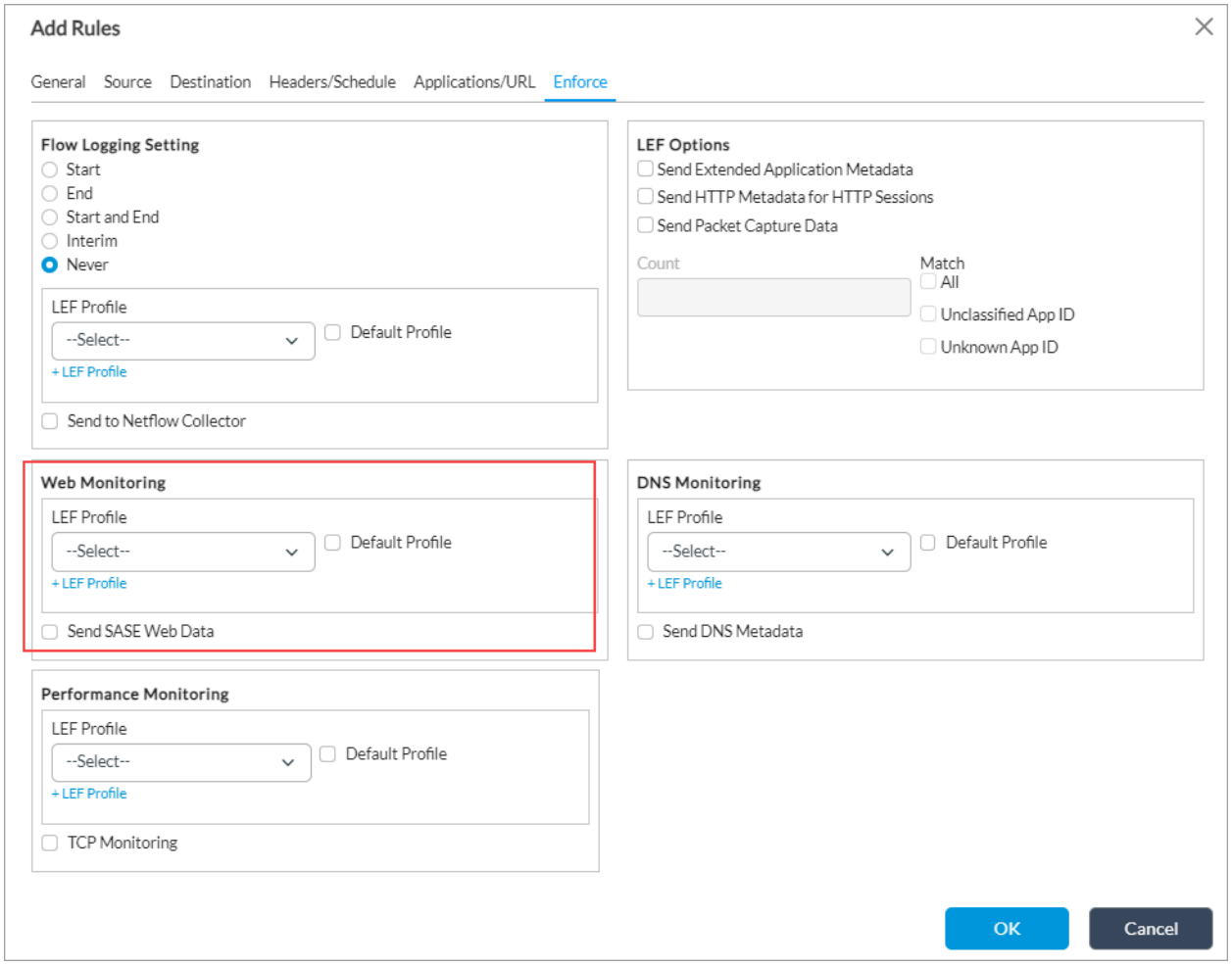
3. Select the Rules tab in the main pane.

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, and then click OK.

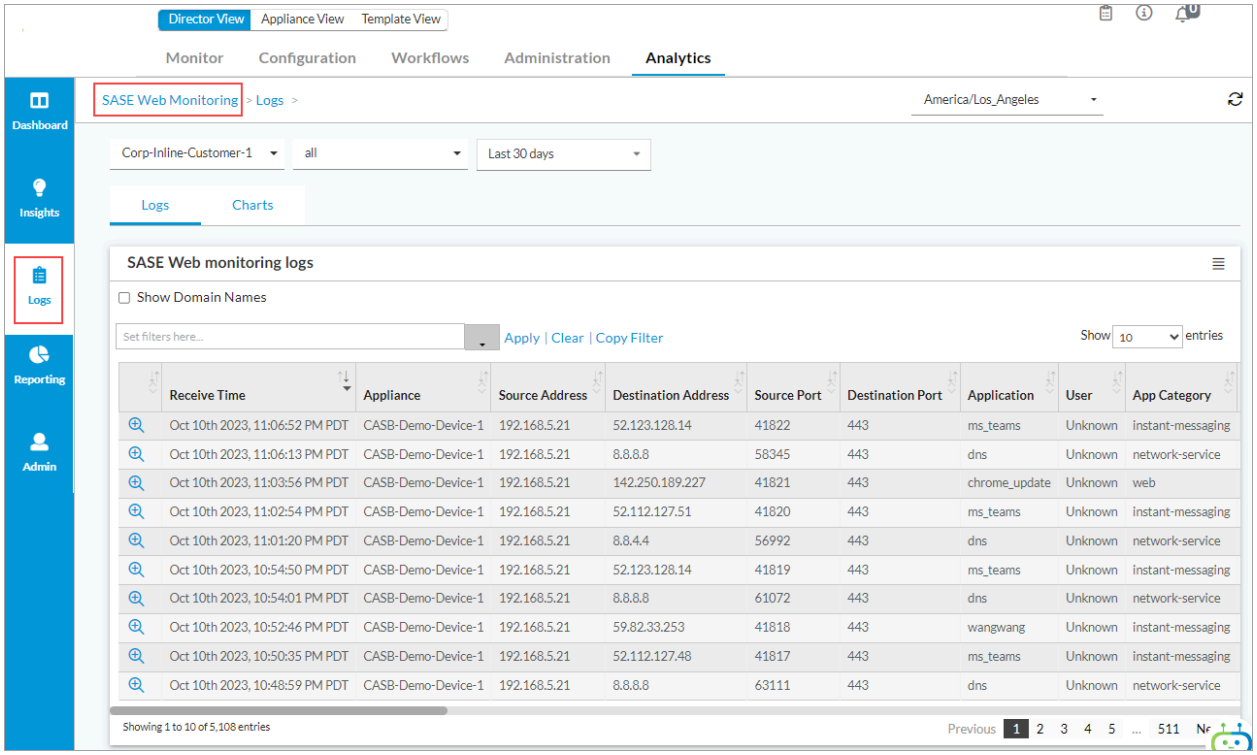
6. Select the Enforce tab, and then enter information for the following fields.



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.



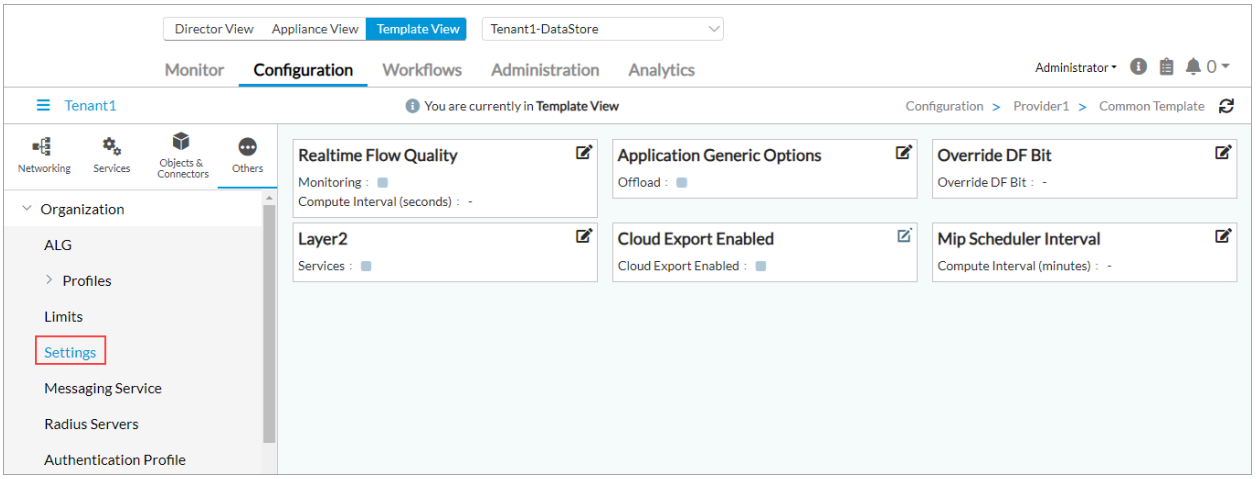
Configure SD-WAN MOS Summary Logging

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

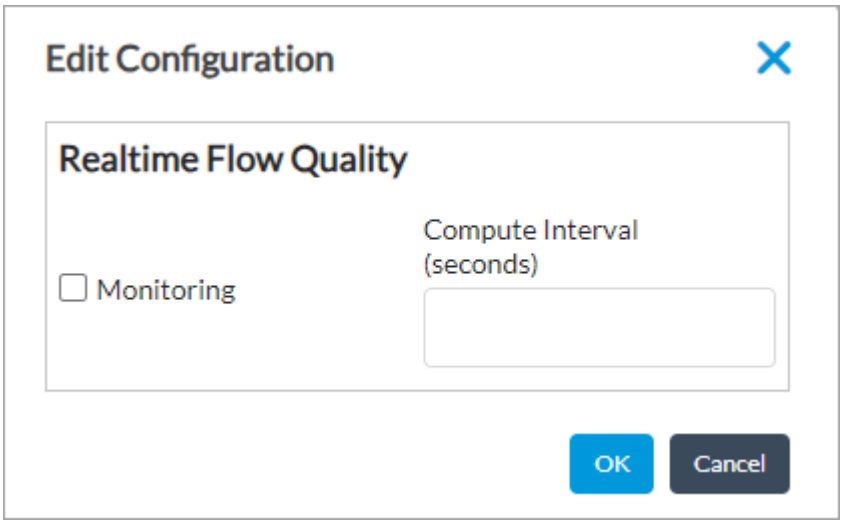
To export mean opinion scores (MOS), you first configure MOS computation. Then you configure a default LEF profile, which forwards the computations to the active collector for the profile. For information about configure MOS score monitoring, see Configure MOS Score Monitoring. For information about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



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

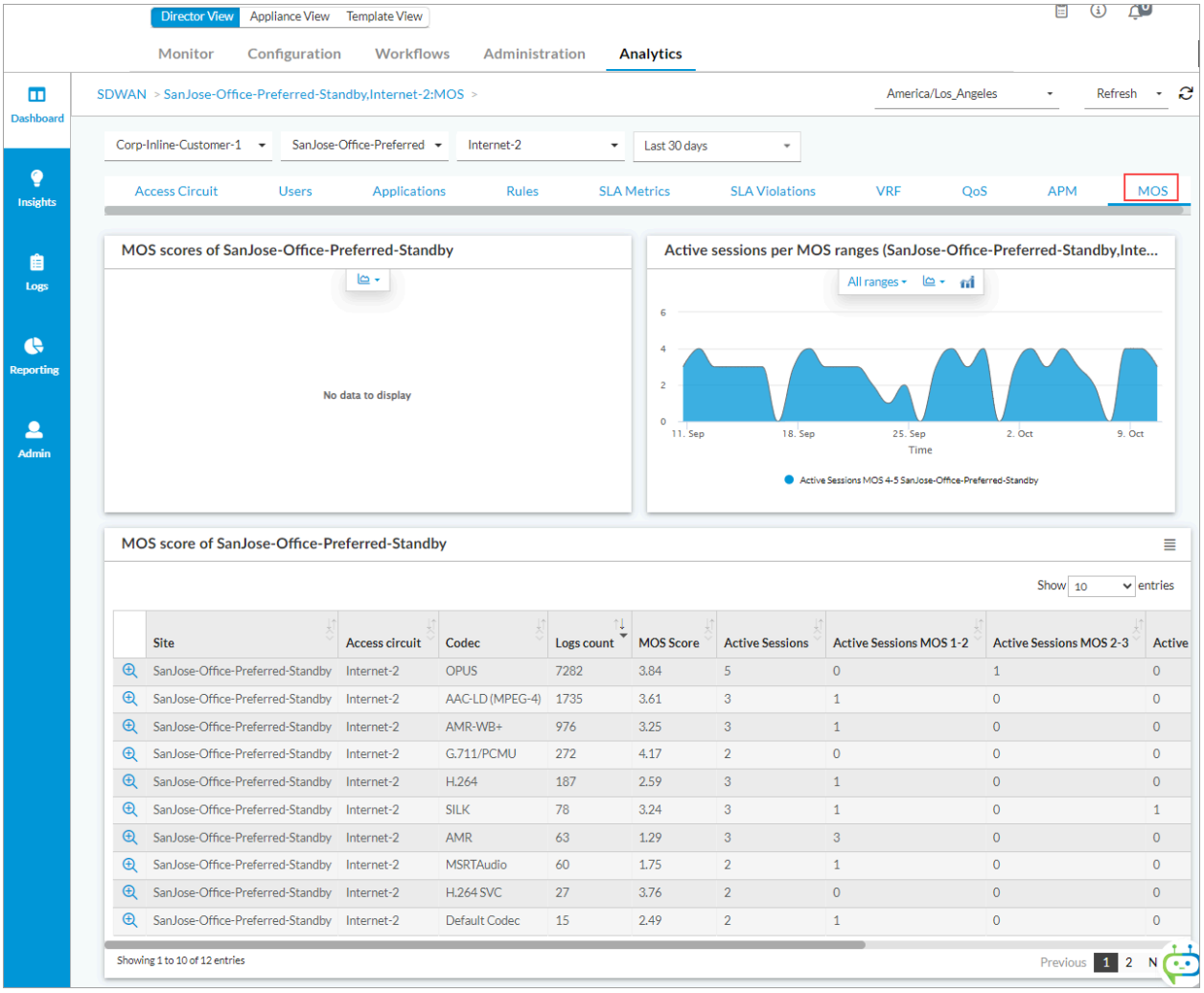


5. Click Monitoring.
6. Click OK.
7. To send the MOS computations to an Analytics cluster, syslog server, or Netflow collector, configure a default LEF profile.

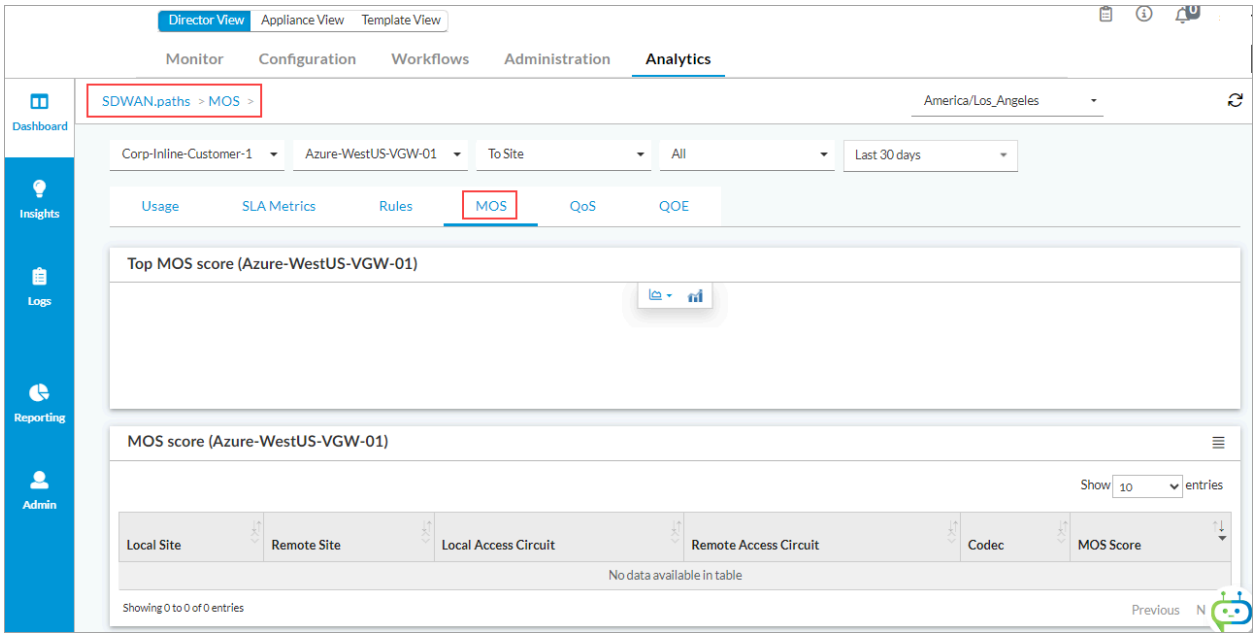
MOS information sent to Analytics clusters displays on the following dashboards:

- 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.



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.



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

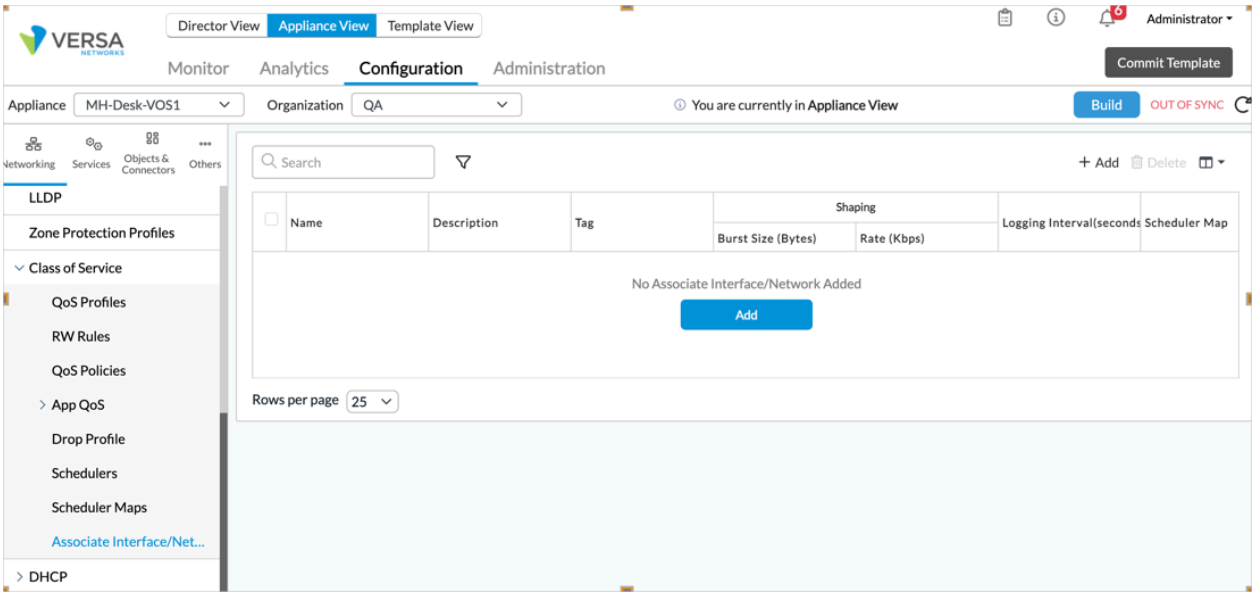
Quality-of-service (QoS) logs are exported when shaping is configured with logging enabled on an SD-WAN link. Enable a nonzero logging interval for each WAN interface. If you set the logging interval to zero, no logs are sent. For information about configuring QoS, see Configure CoS.

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.

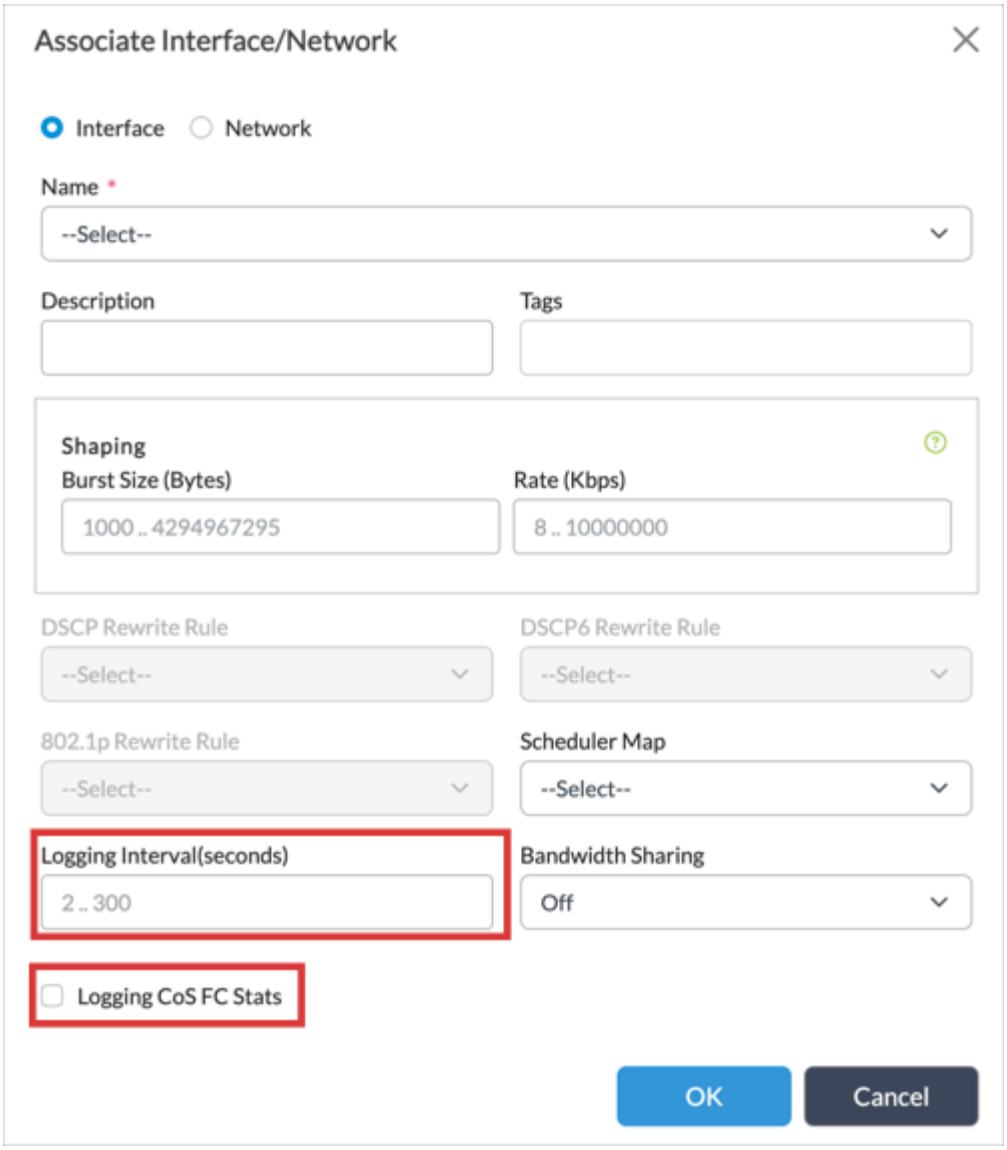
For Releases 22.1.1 and later, you can also export QoS status logs by forwarding class, which is the combination of traffic class and queue. There are up to four traffic classes and four queues for a maximum of 16 forwarding classes, which are exported simultaneously.

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.



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

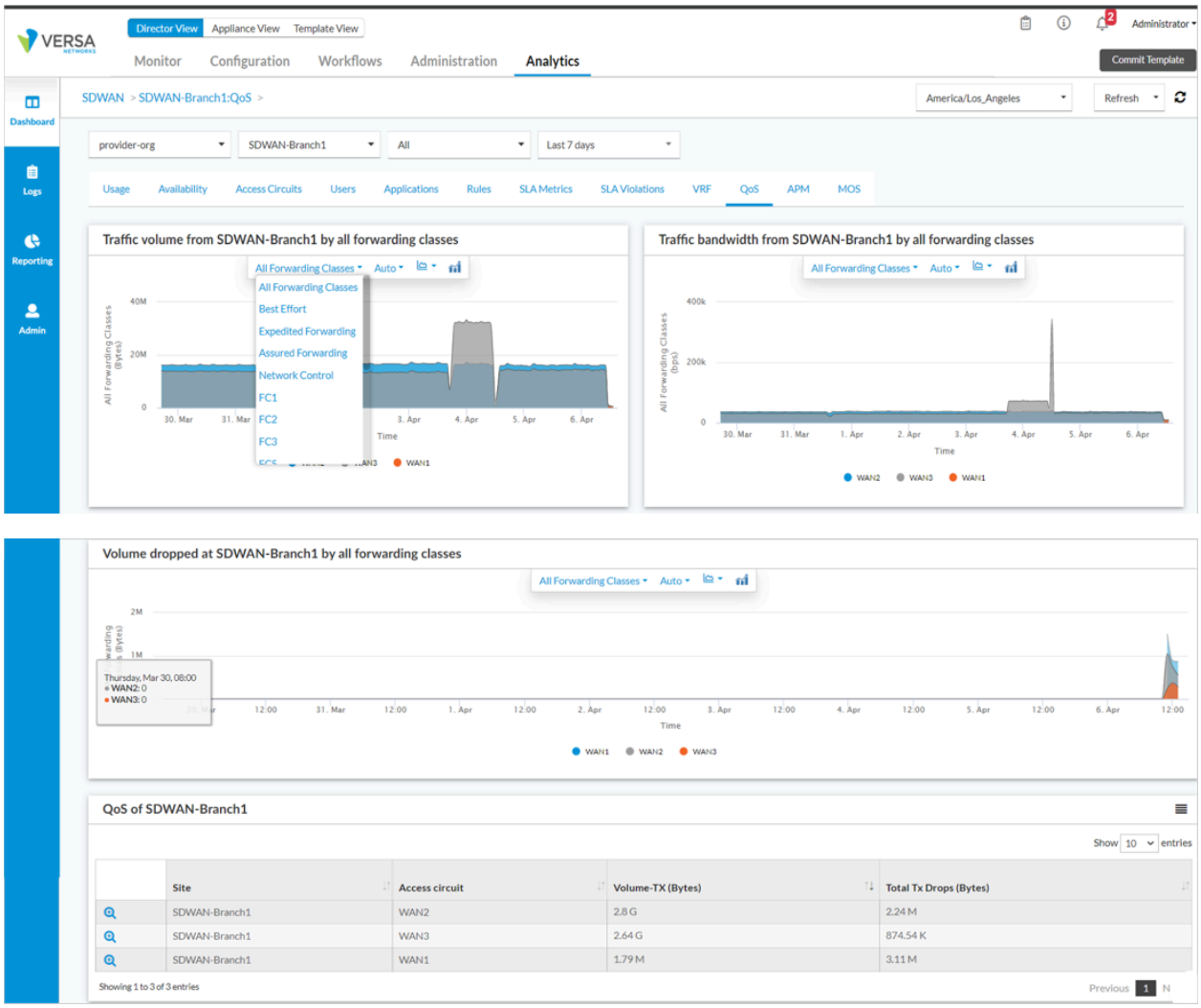


6. In the Logging Interval field, enter a logging interval, in seconds. Setting this field to 0 disables logging. Setting to any other value enables QoS logging by traffic class. Logs are forwarded to the default LEF profile destination.
7. For Releases 22.1.1 and later, enter a nonzero logging interval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

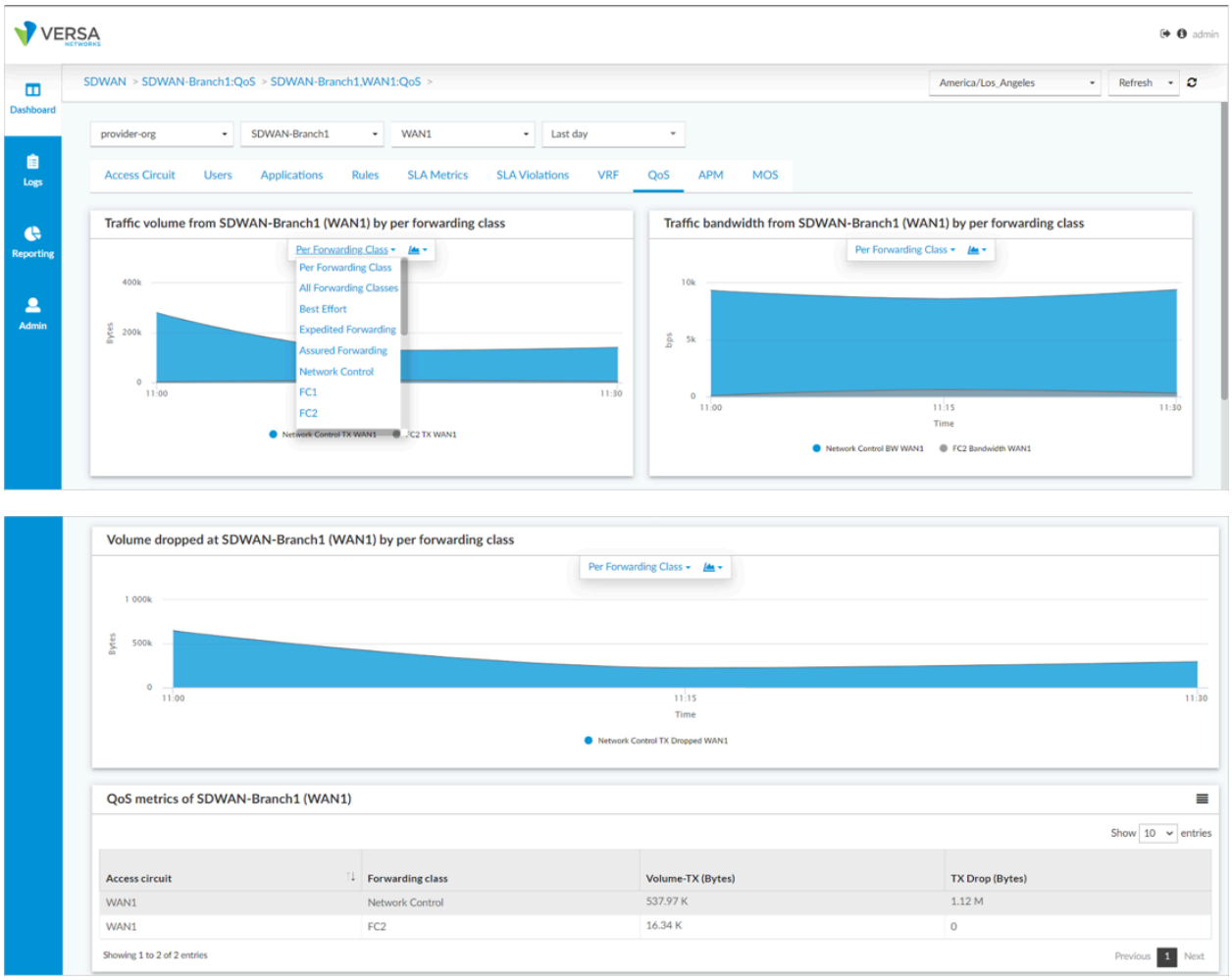
For logs sent to Analytics clusters, to display SD-WAN QoS dashboards:

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)



4. 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.
5. 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)



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

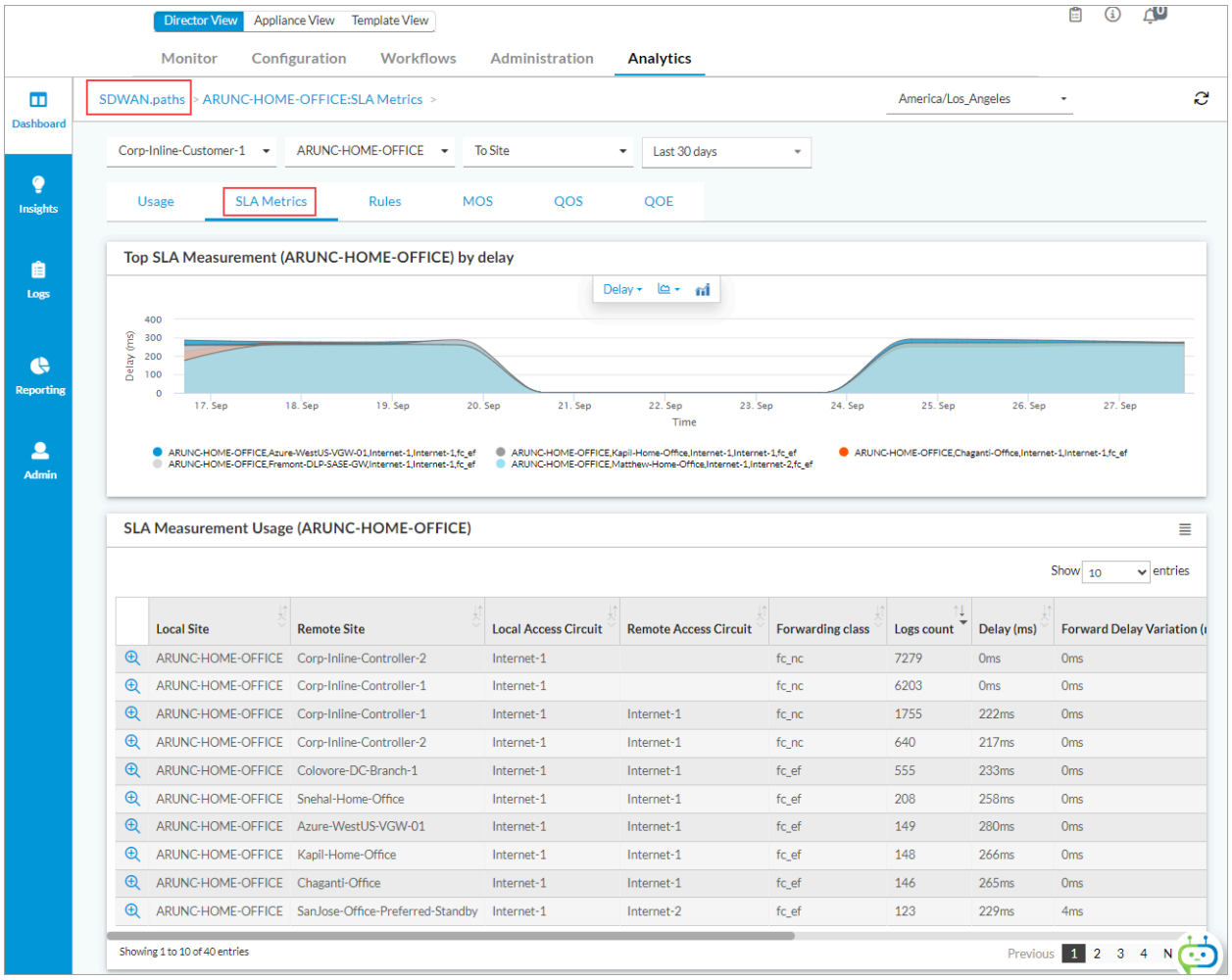
To export SLA metrics logs, configure a default LEF profile. SD-WAN SLA metrics logs are then generated automatically without needing further configuration.

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.

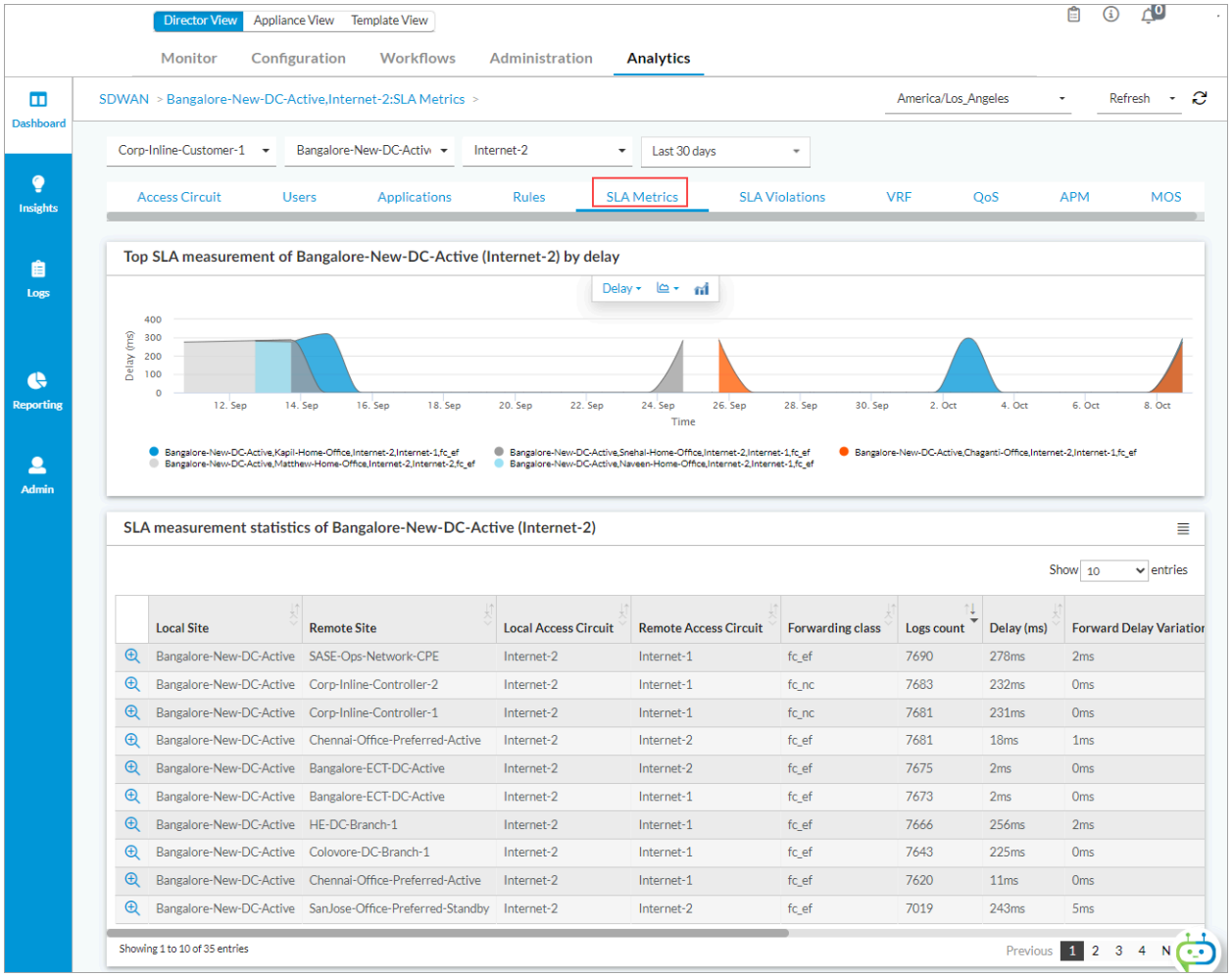
SD-WAN SLA metrics logs can exhaust cluster disk storage, especially for tenants running large full-mesh topologies. It

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.

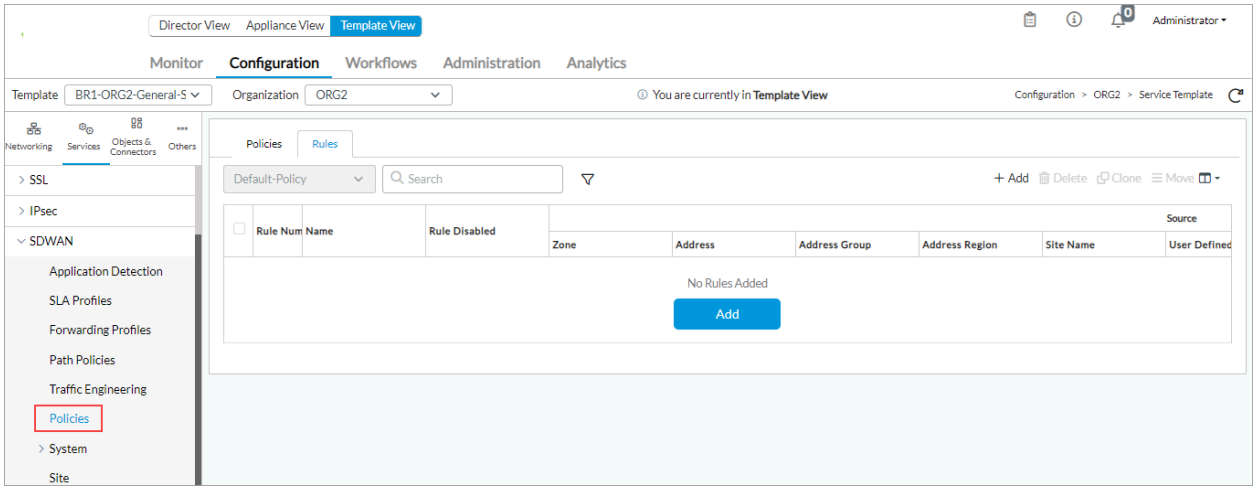
To export SLA violation logs:

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

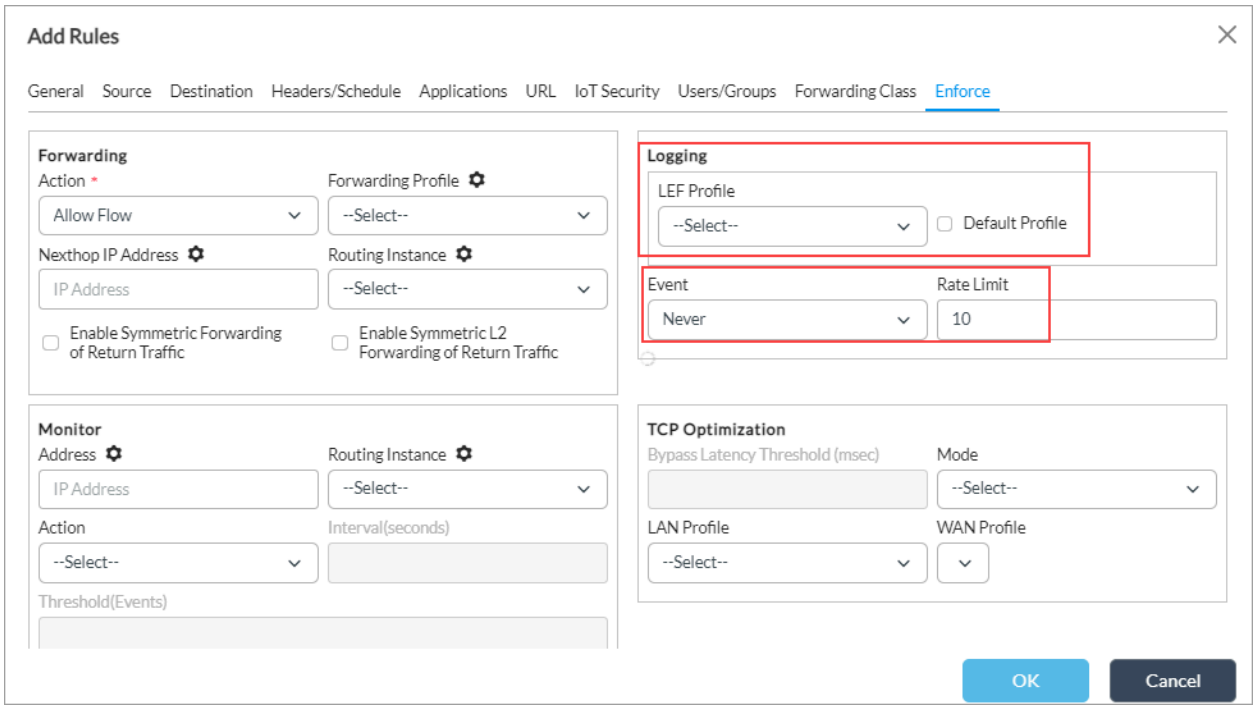
name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.

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.

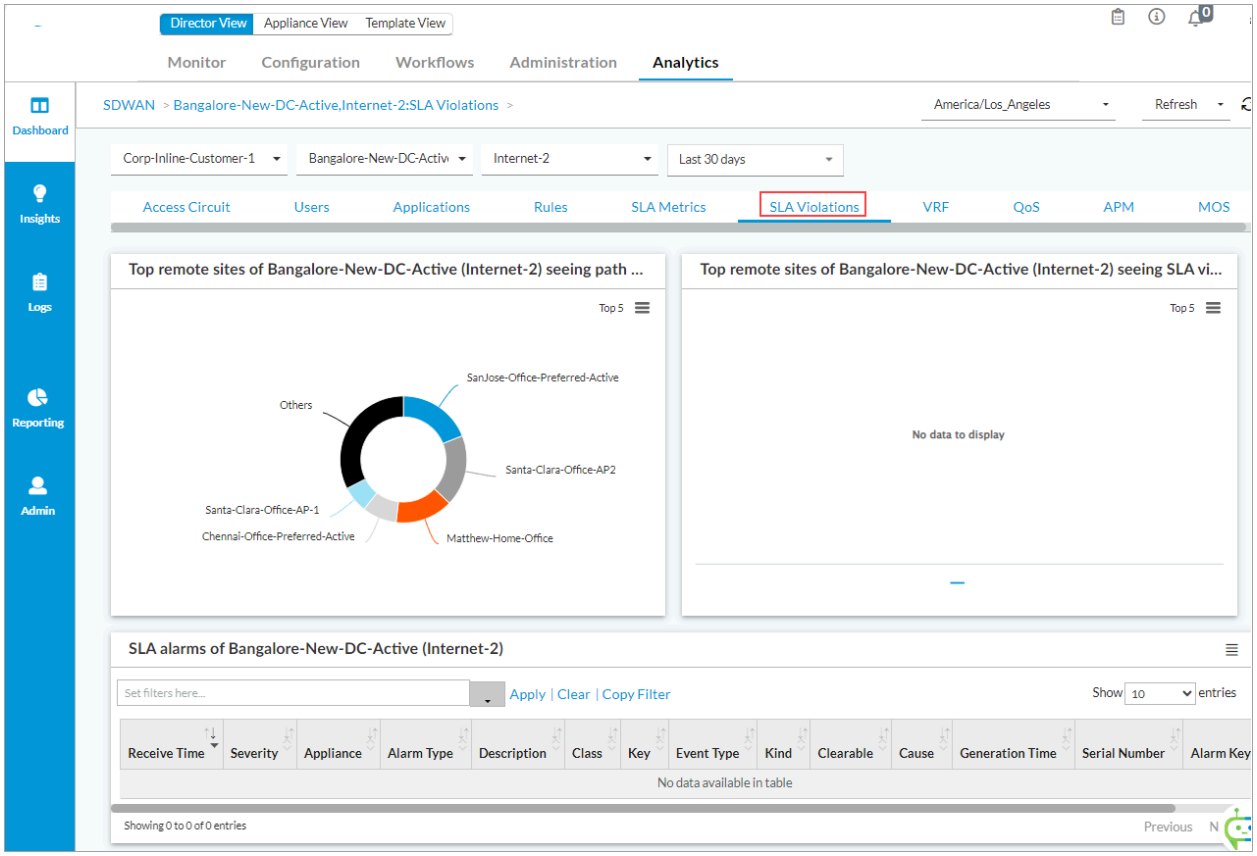


5. Click the + Add icon, or click an existing rule. The Add/Edit Rules window displays.
6. Select the Enforce tab. The following window displays.



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.



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:

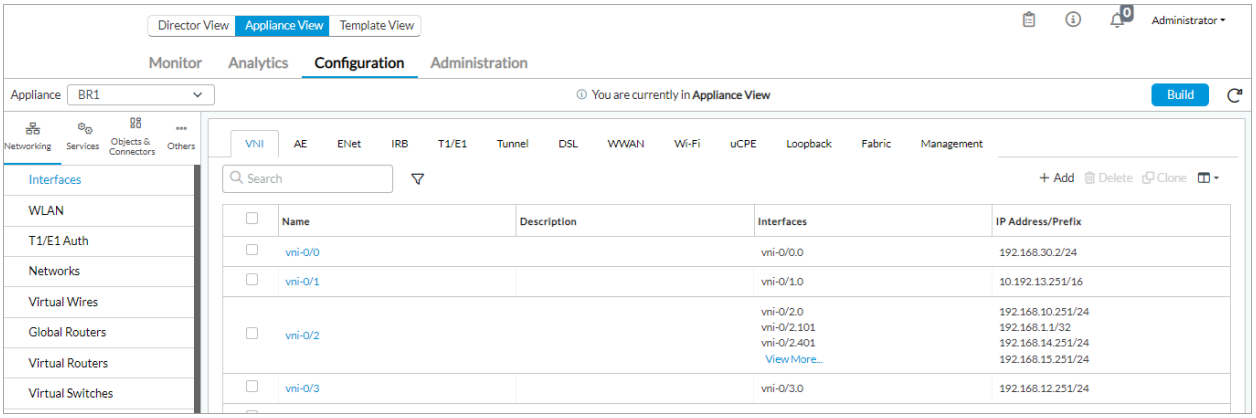
1. In Director view:
    a. Select the Configuration tab in the top menu bar.

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.

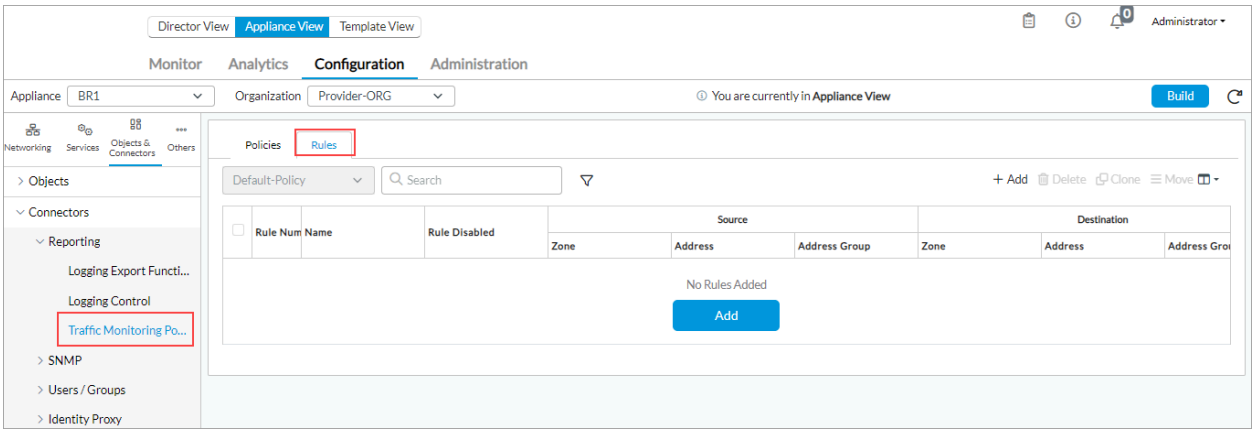
d. Select a VOS device in the main pane. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar. The following screen displays.



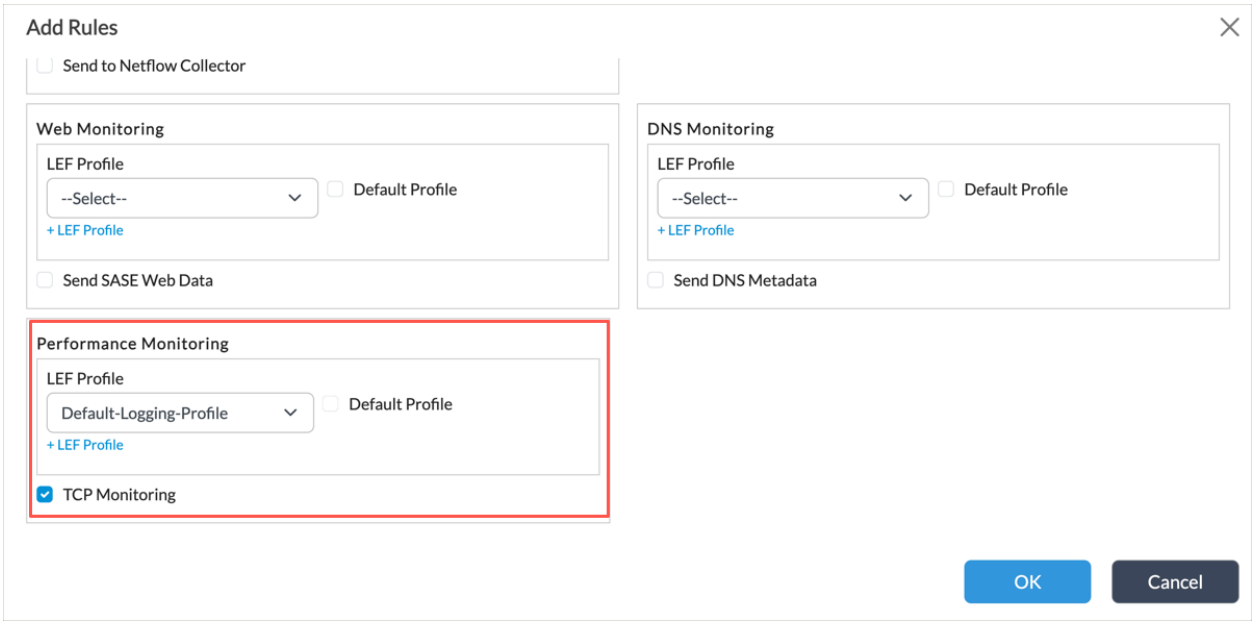
3. Select Objects & Connectors > Connectors > Reporting > Traffic Monitoring Policies in the left menu bar.

4. Select the Rules tab in the horizontal menu bar. The following screen displays.



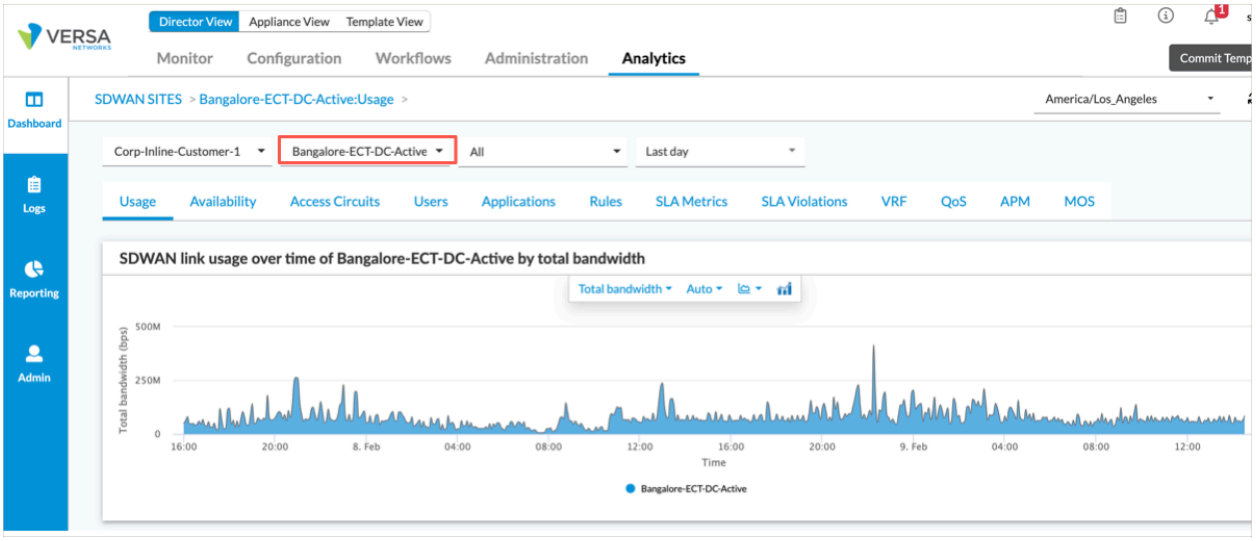
5. Click an existing rule or click + Add. The Add/Edit Rules popup window displays.

6. Select the Enforce tab. The following screen displays.

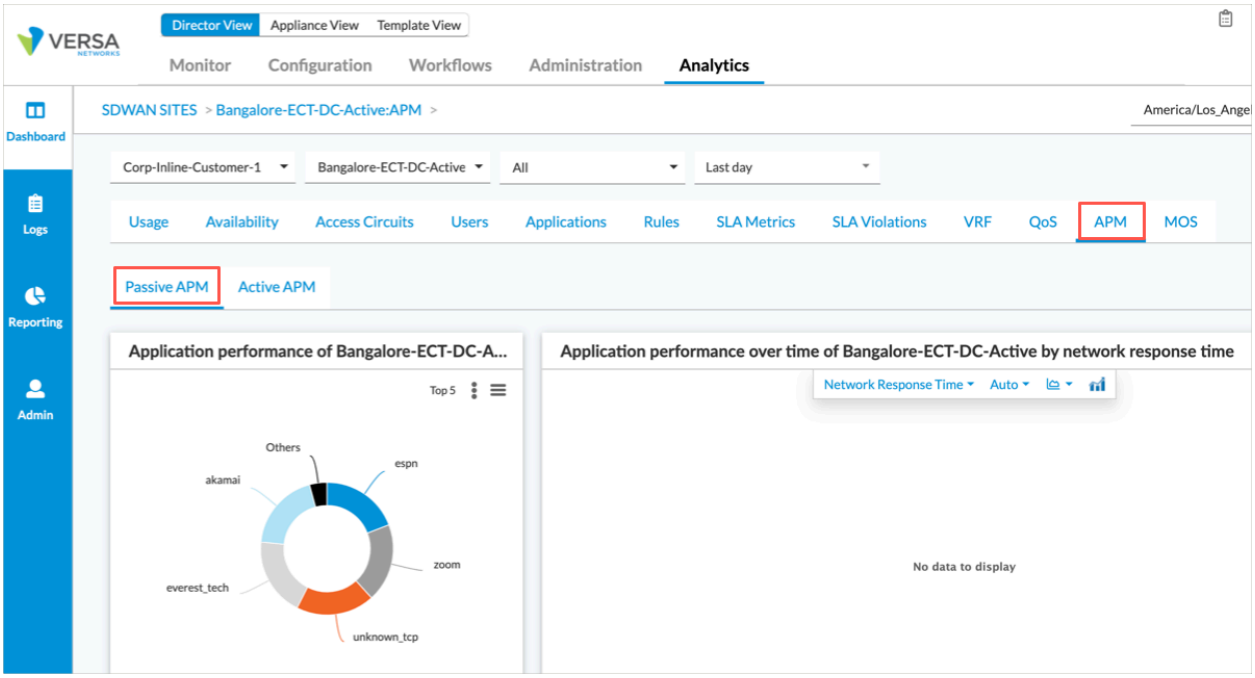


7. Scroll down to the Performance Monitoring pane and select a LEF profile from the drop-down menu to associate it with the policy rule, or click Default Profile to use the default LEF profile.
8. Click TCP Monitoring.
9. Click OK.

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.

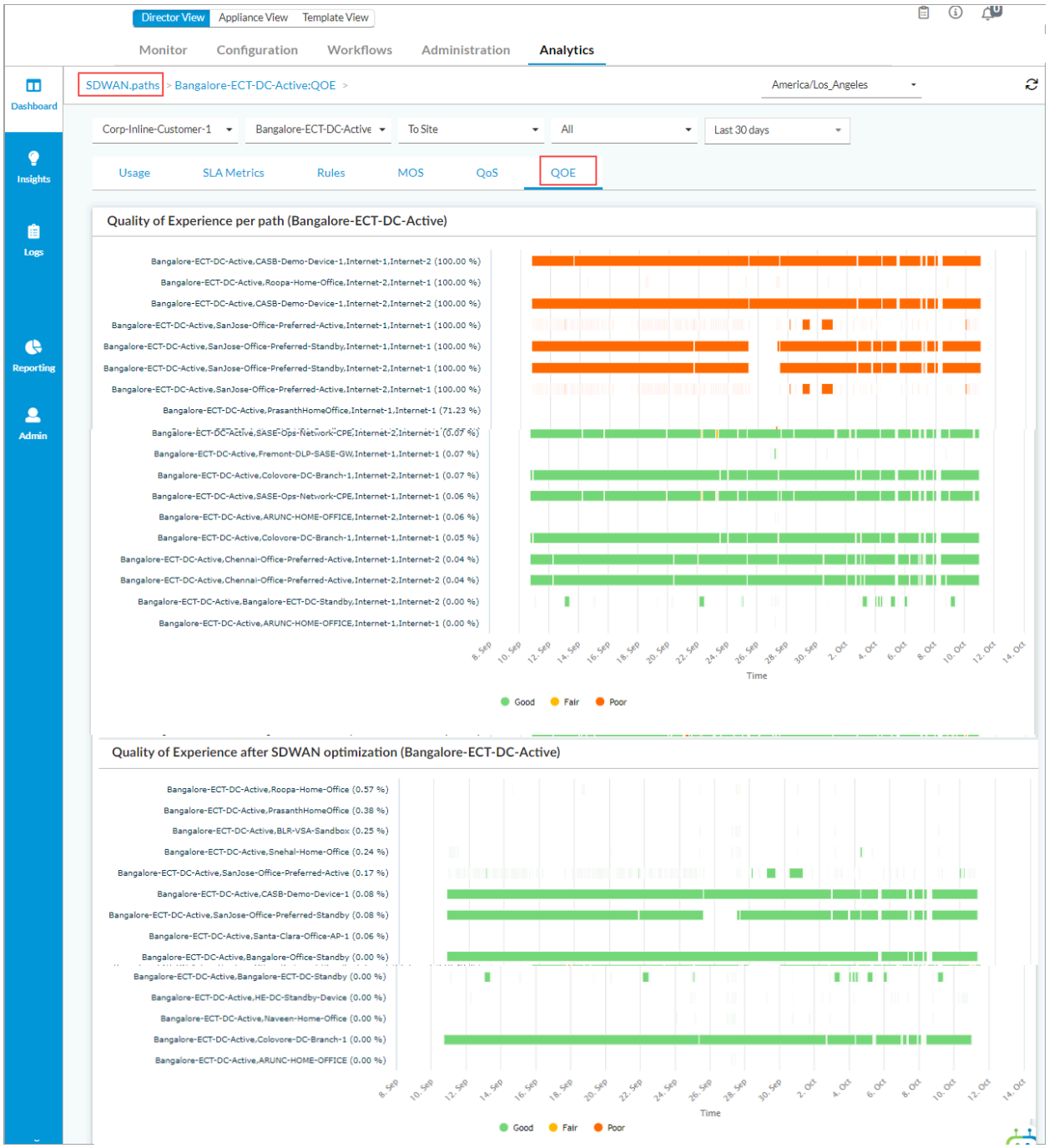


Configure SD-WAN Traffic-Conditioning Logging

- 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:

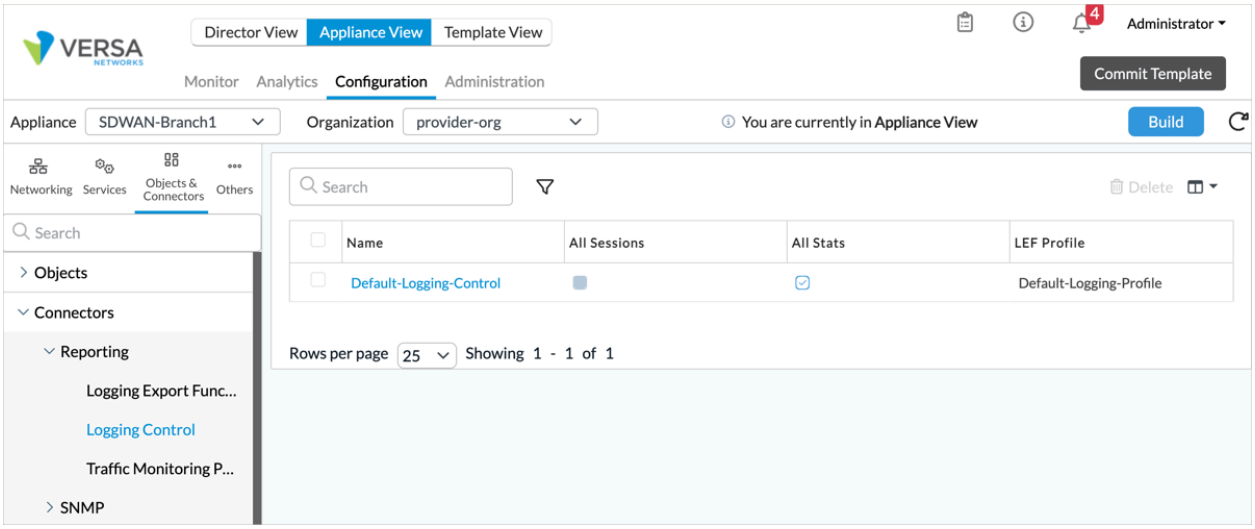
You can export traffic-monitoring logs in two ways. To configure globally for all flows (both allow and deny flows), you

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.

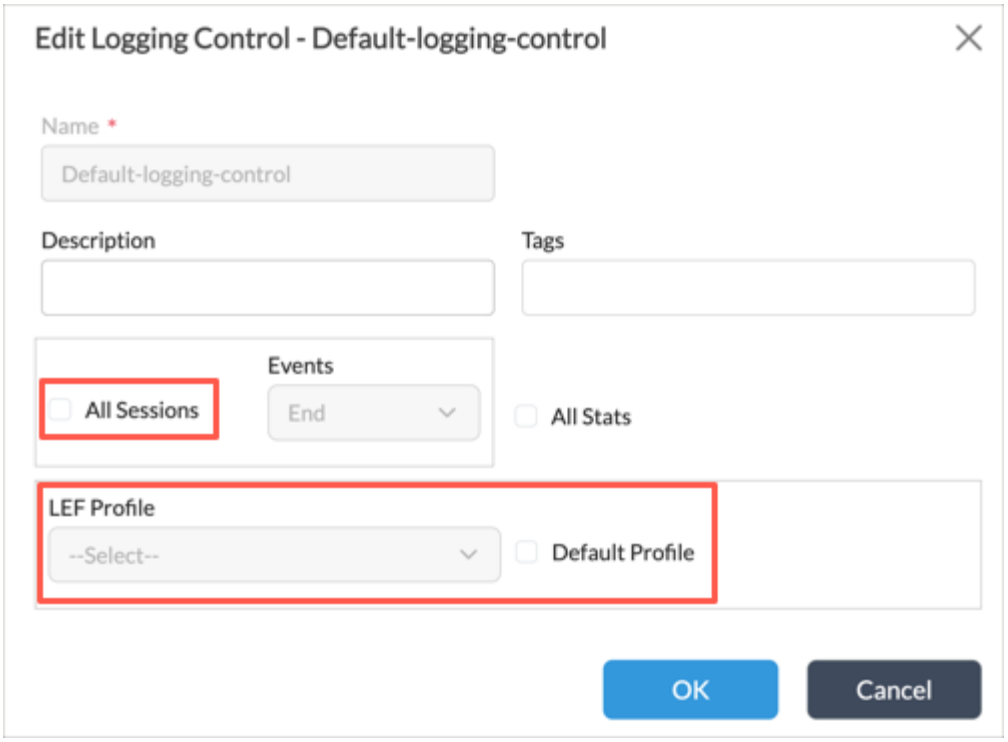
To export web-monitoring logs, select the Send HTTP Metadata for HTTP Sessions option when you configure traffic-monitoring policy.

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.



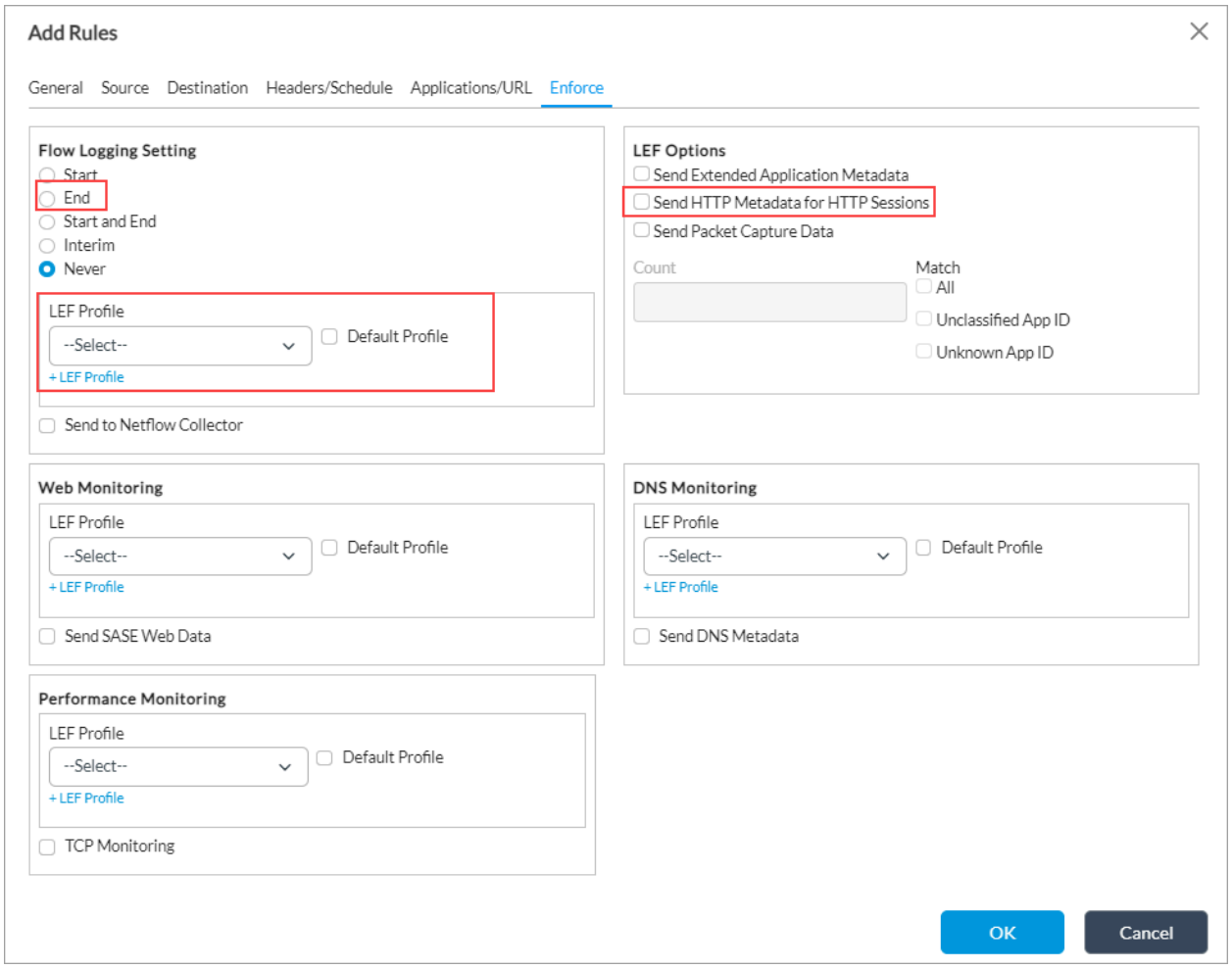
4. In the main pane, if a logging control entry exists click the name of the entry. If no entry exists, click +Add. The Edit/Add Logging Control popup window displays.



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.

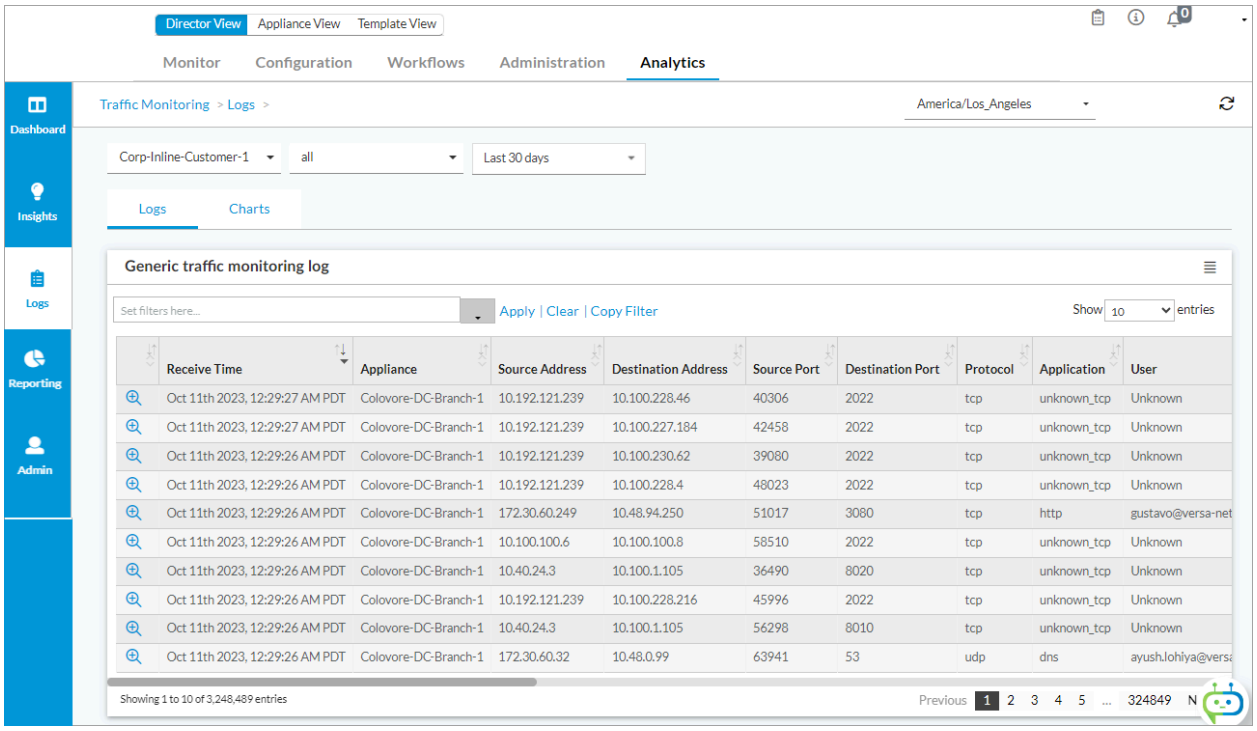
To export traffic-monitoring and web-monitoring logs using a traffic-monitoring policy rule:

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.

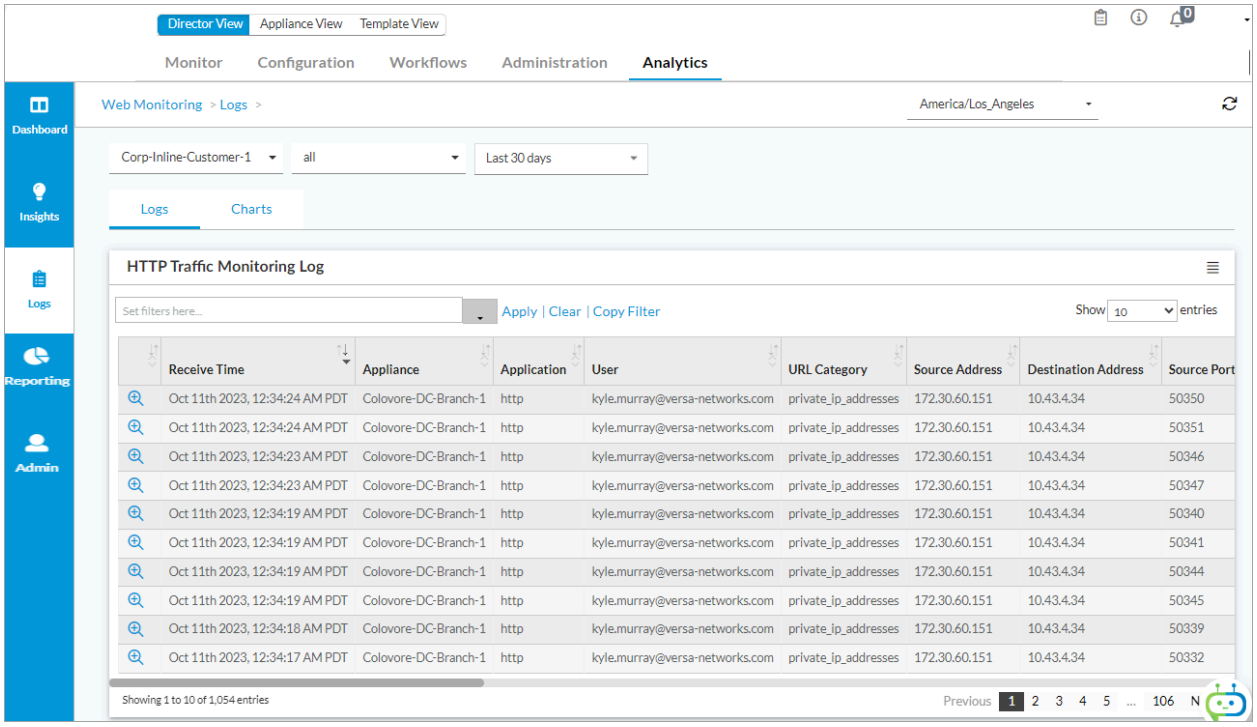


7. To send traffic-monitoring logs to the active collector for a LEF profile:
   a. In the Flow Logging Setting group of fields, select End.
   b. Select a LEF profile, or click Default Profile to use the default LEF profile.
8. To include application metadata, such as application risk, productivity, 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.



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

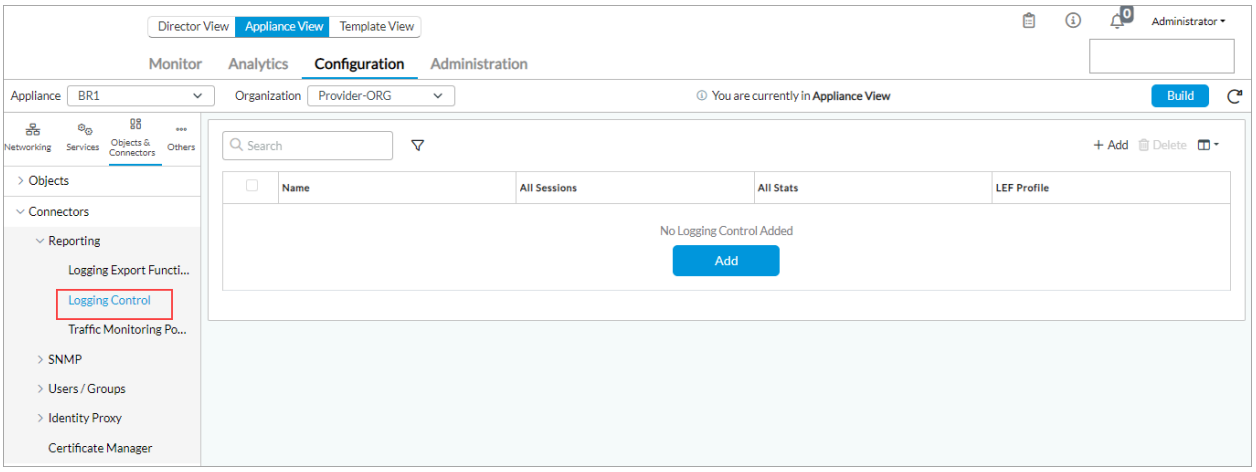


- Syslog identifiers—bwMonLog, eventLog

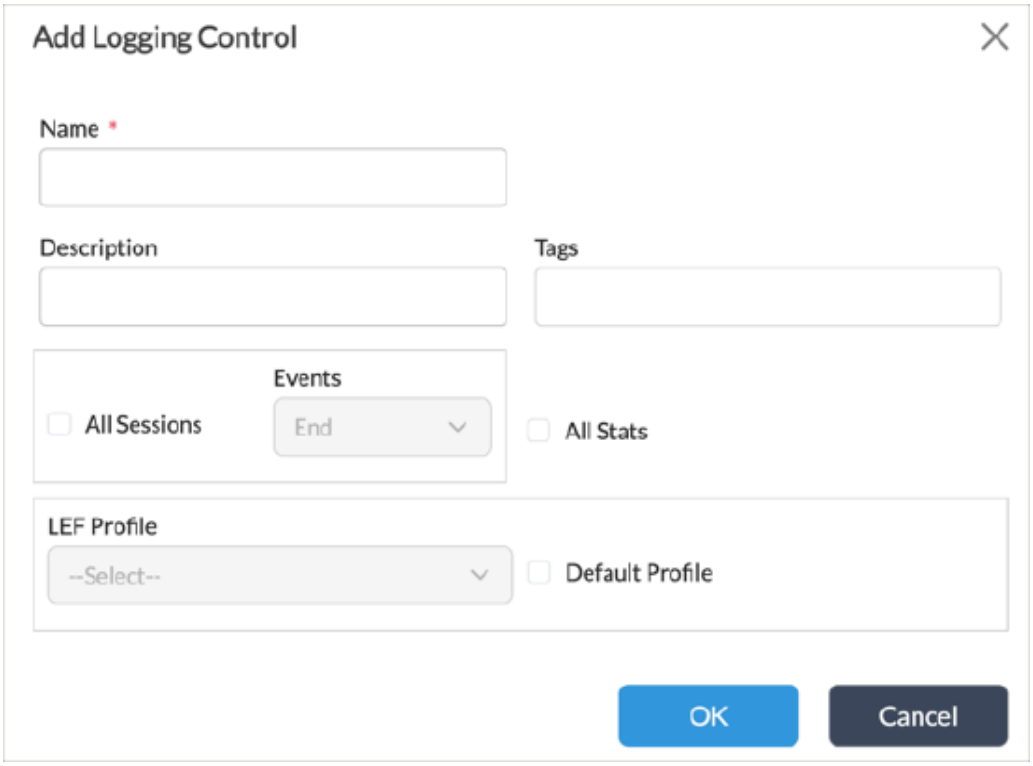
To export traffic-monitoring summary logs, click All Stats in the logging control configuration. For information about configuring logging control, see Configure Log Export Functionality.

To export traffic monitoring summary logs:

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.

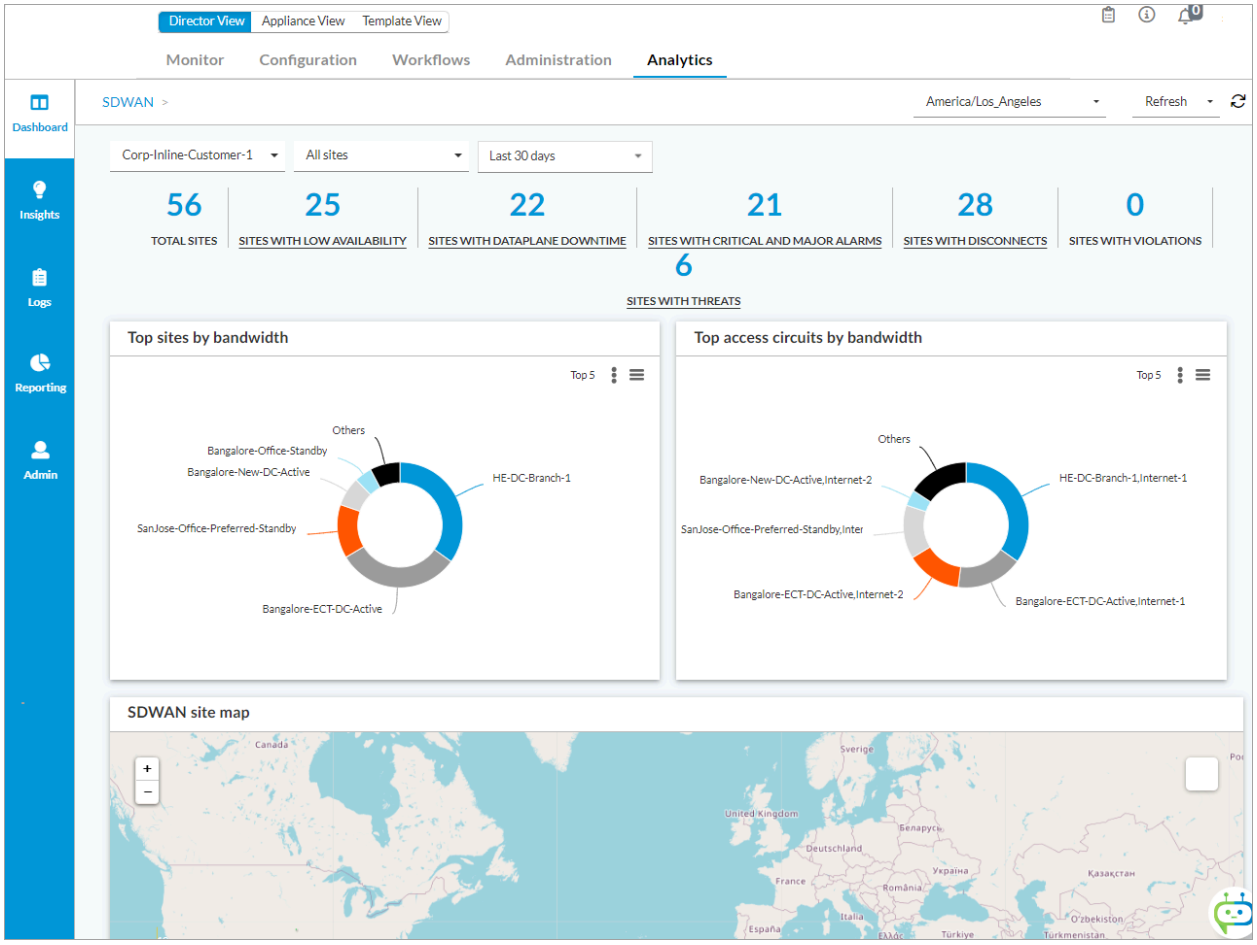


4. Click a logging control entry in the main pane. The Edit Logging Control window displays.

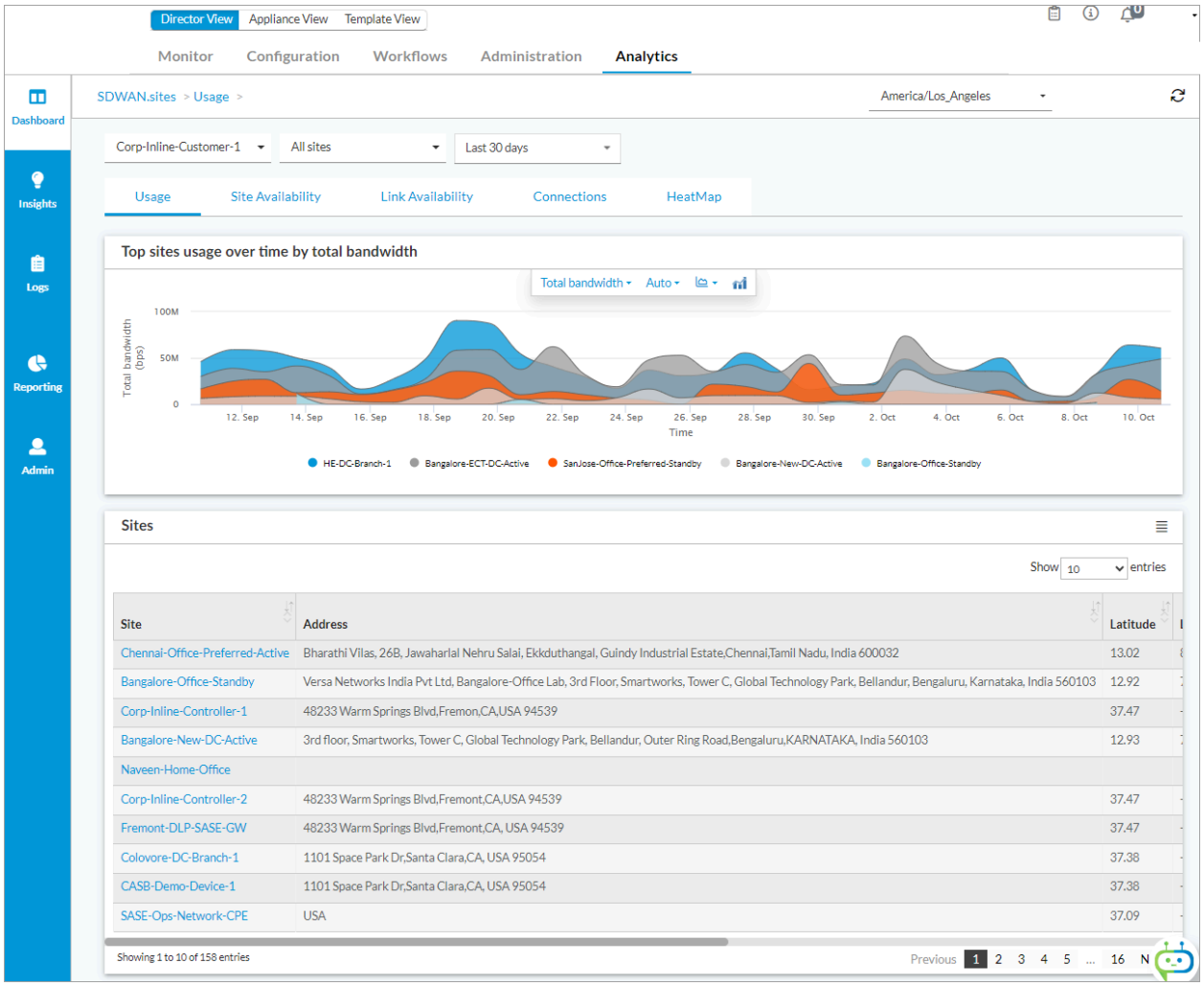


5. Click All Stats, and then either select a LEF profile or click Default Profile to use the default LEF profile.
6. Click OK.

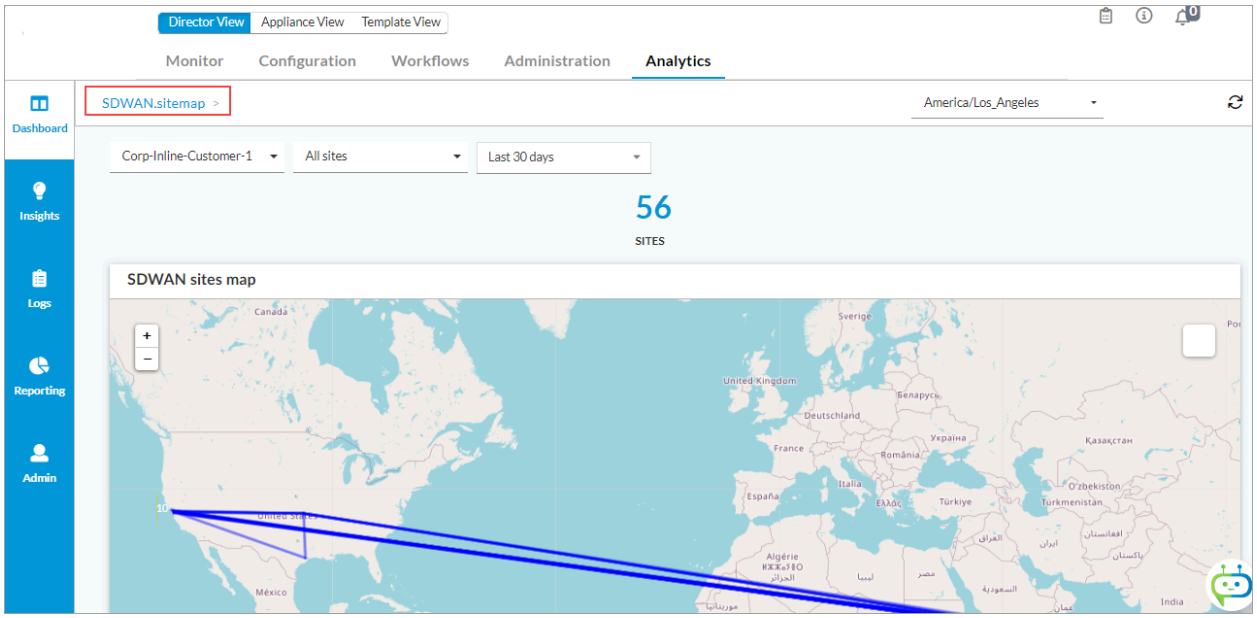
For logs sent to Analytics clusters, to display the SD-WAN traffic-monitoring summary dashboards, select Analytics > Dashboards > SD-WAN in the left menu bar.



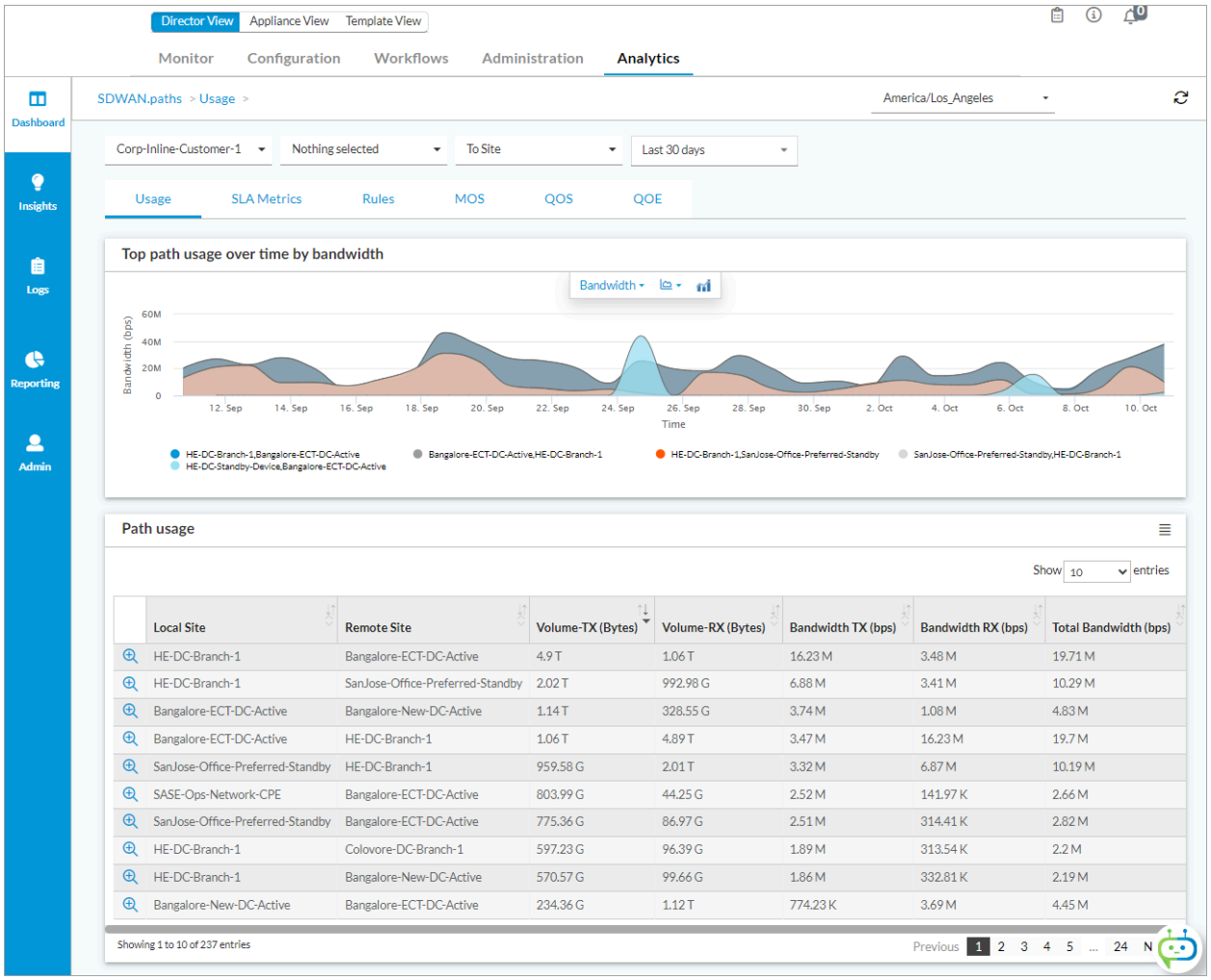
For logs sent to Analytics clusters, to display the SD-WAN traffic monitoring by sites, select Analytics > Dashboards > SD-WAN > Sites in the left menu bar.



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.

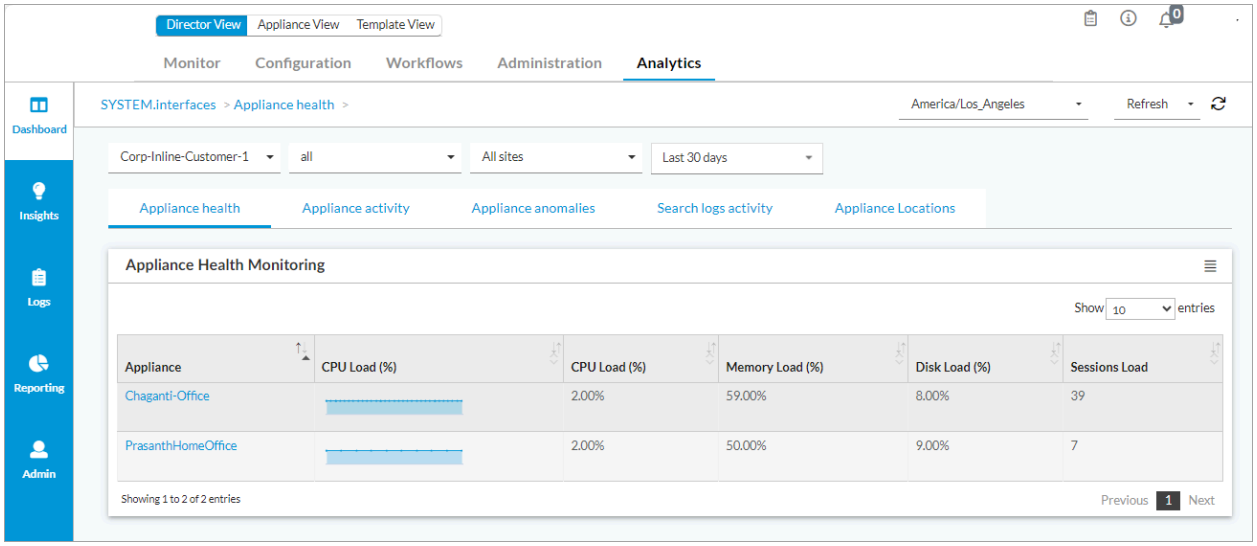


Configure System Load Logging

- 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.



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.

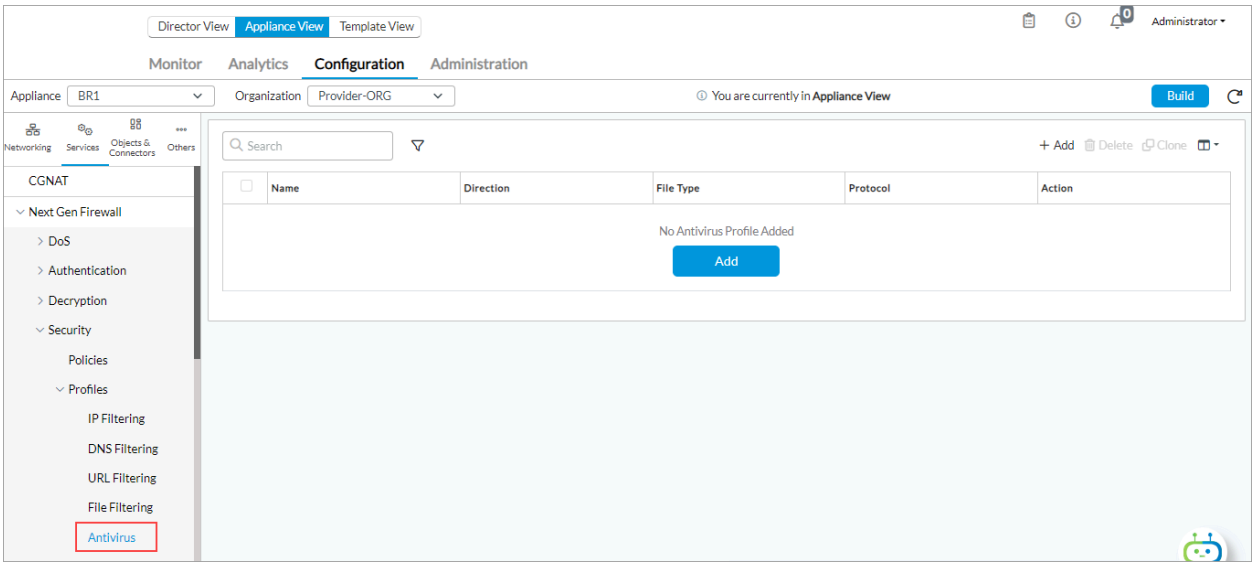
To export threat logs, associate a LEF profile with the antivirus, DoS, IDP, IP-filtering, and URL-filtering configurations.

Configure Antivirus (Malware) Logging

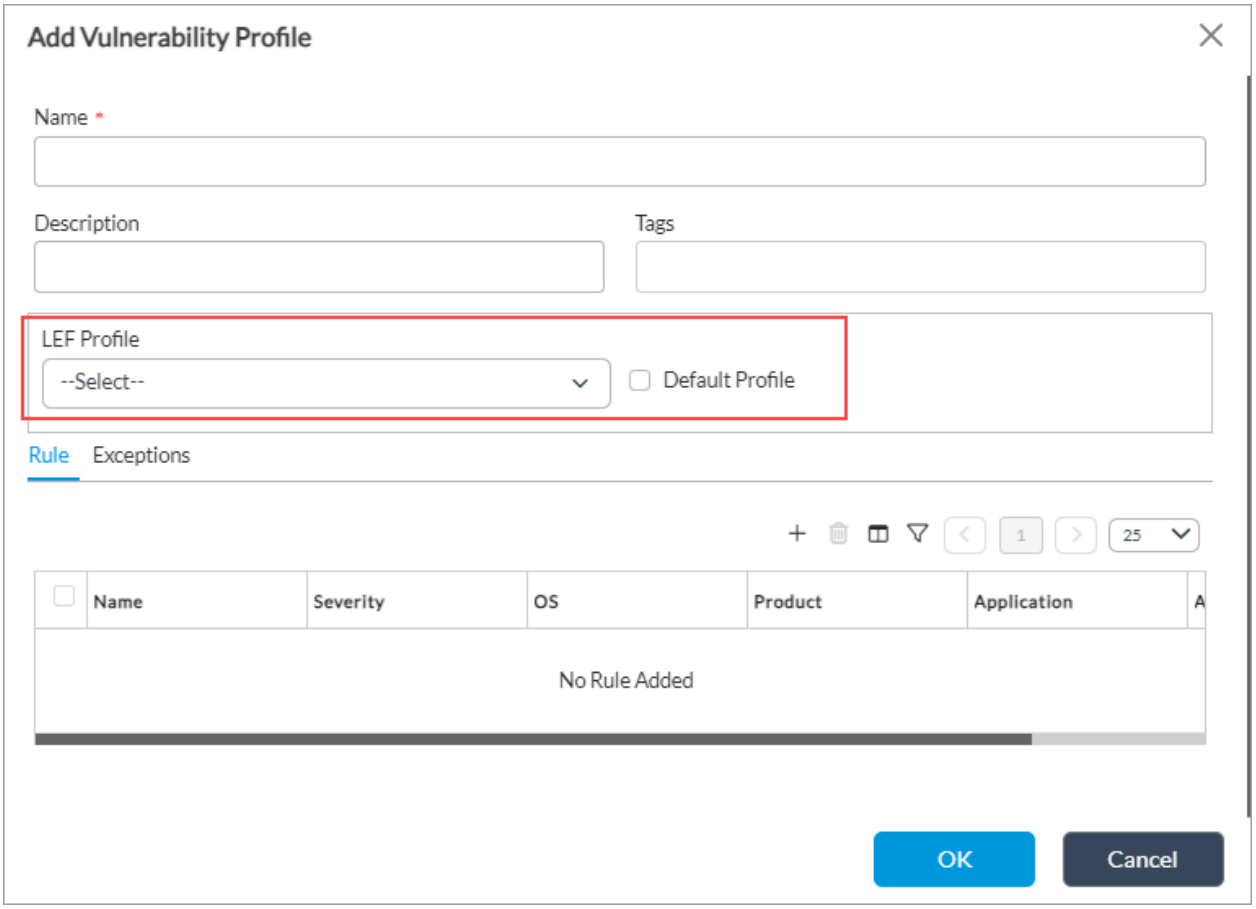
For information about configuring antivirus, see Configure Antivirus.

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.



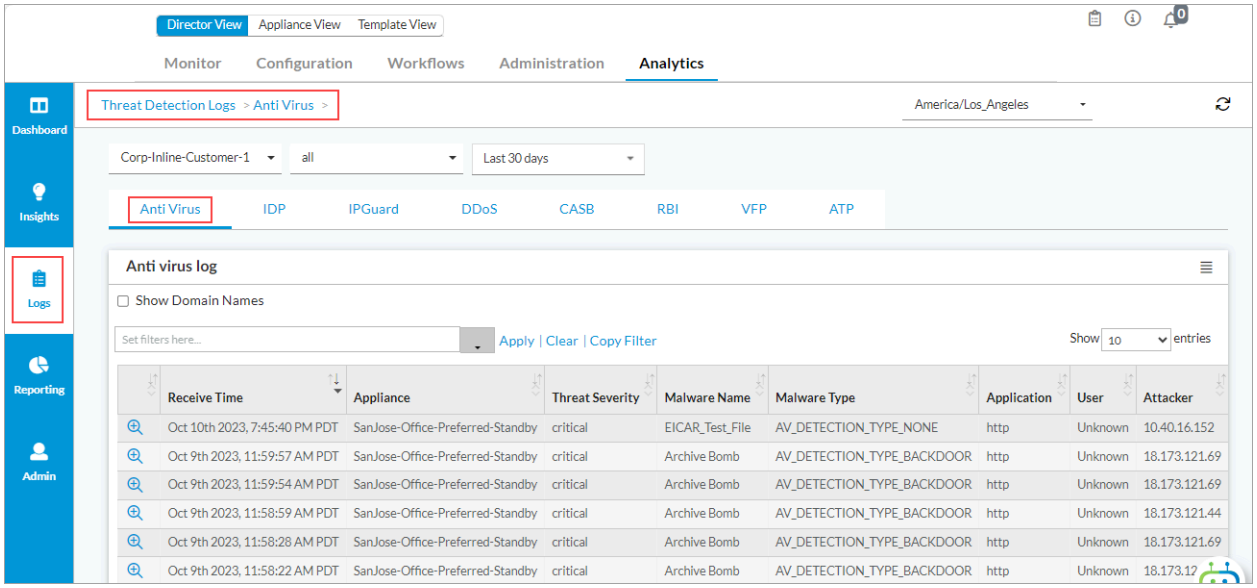
4. Select an existing profile, or click the + Add icon to add a new profile. The Add/Edit Antivirus Profile popup window displays.



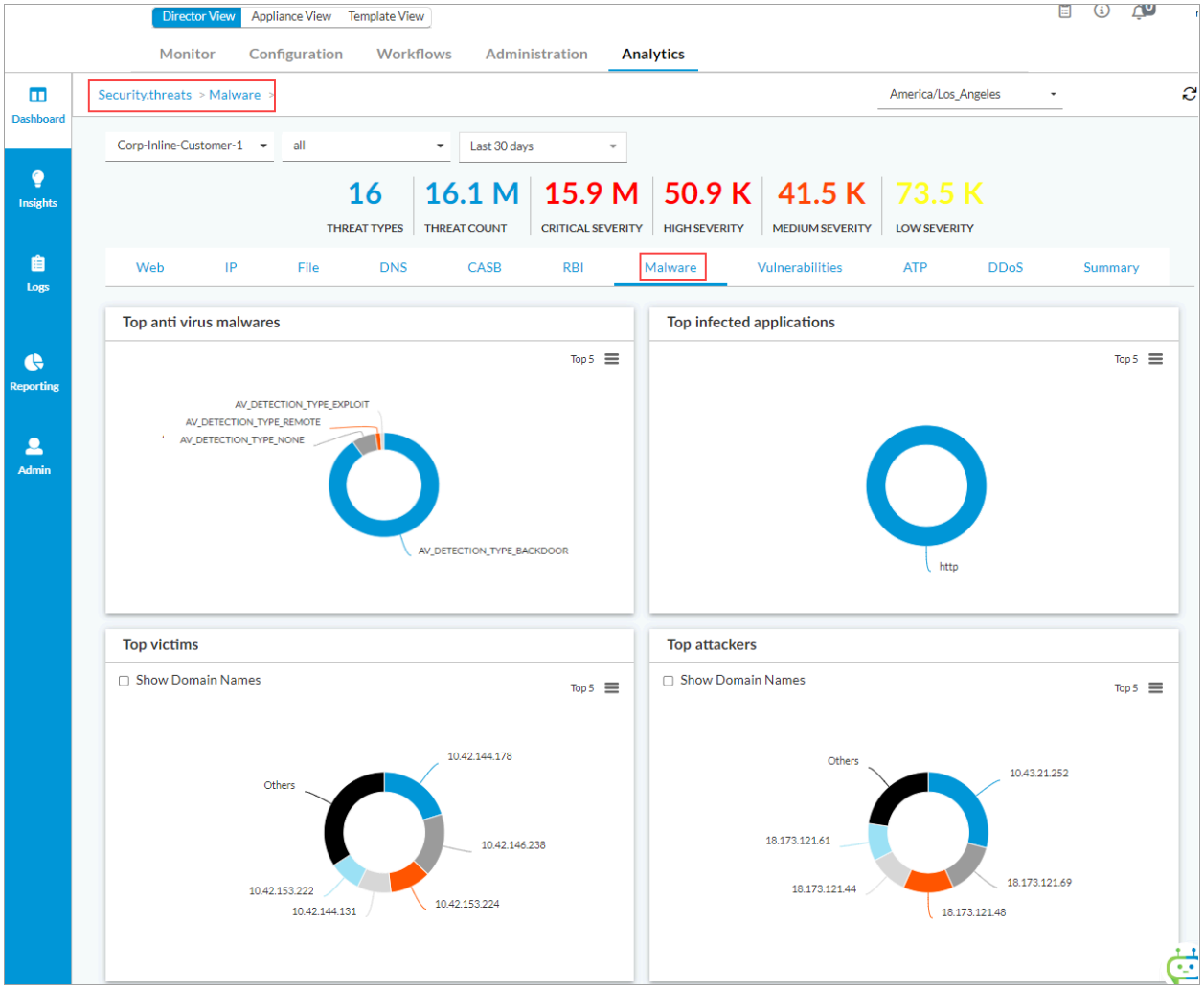
5. In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile.

6. Click OK.

For logs sent to Analytics clusters, to display the 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.



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:

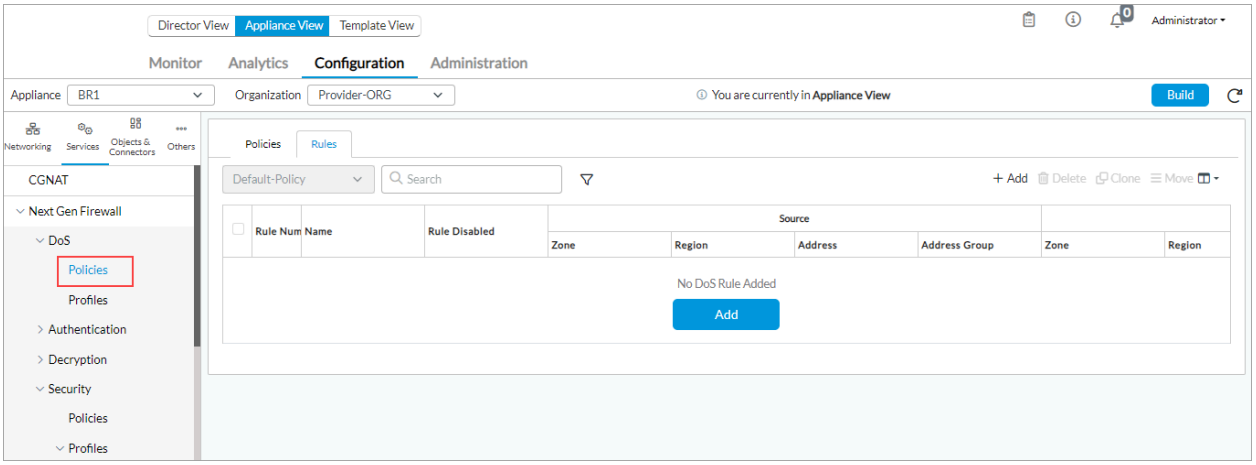


Configure DDoS Threats Logging

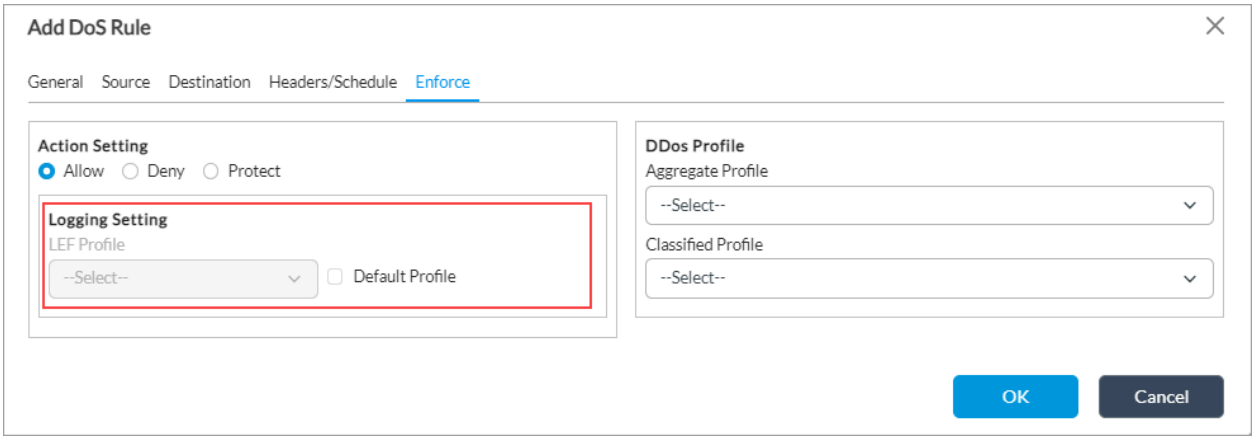
For information about configuring DoS, see Configure DoS Protection.

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.

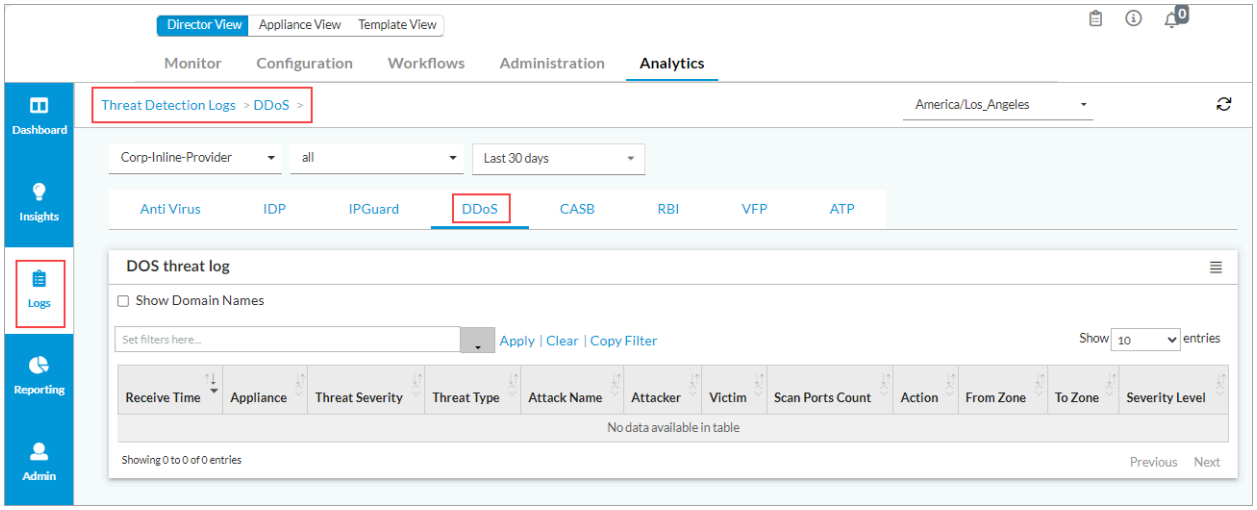


4. Click the + Add icon. The Add DoS Rule popup window displays.
5. Select the Enforce tab. The following window displays.

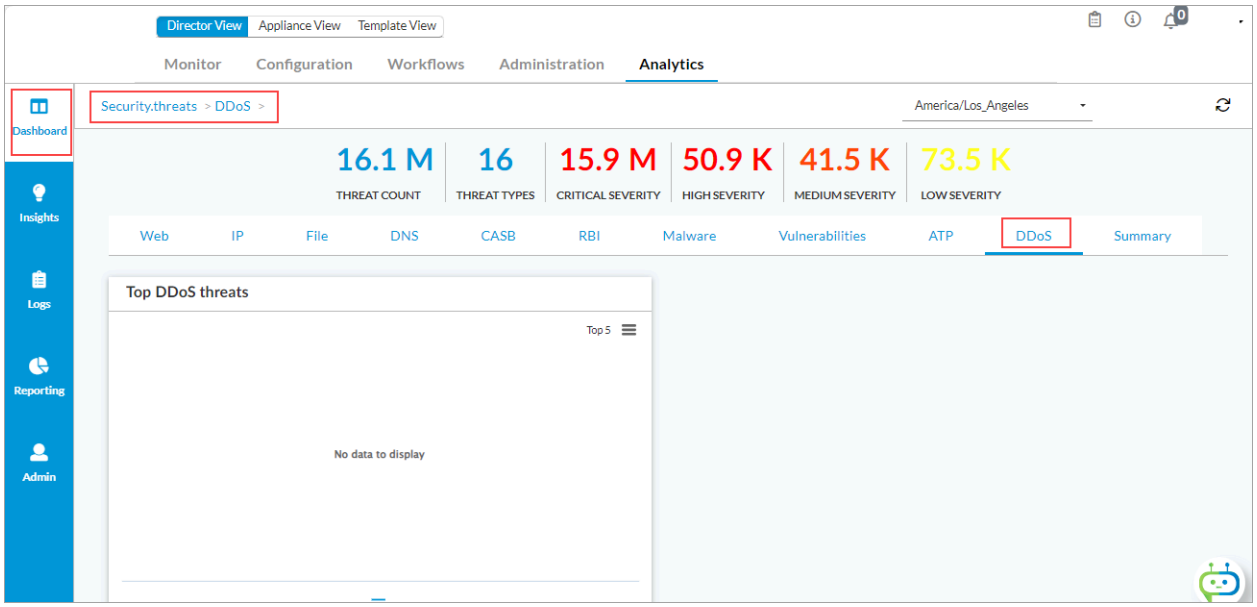


6. In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile.
7. Click OK.

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.

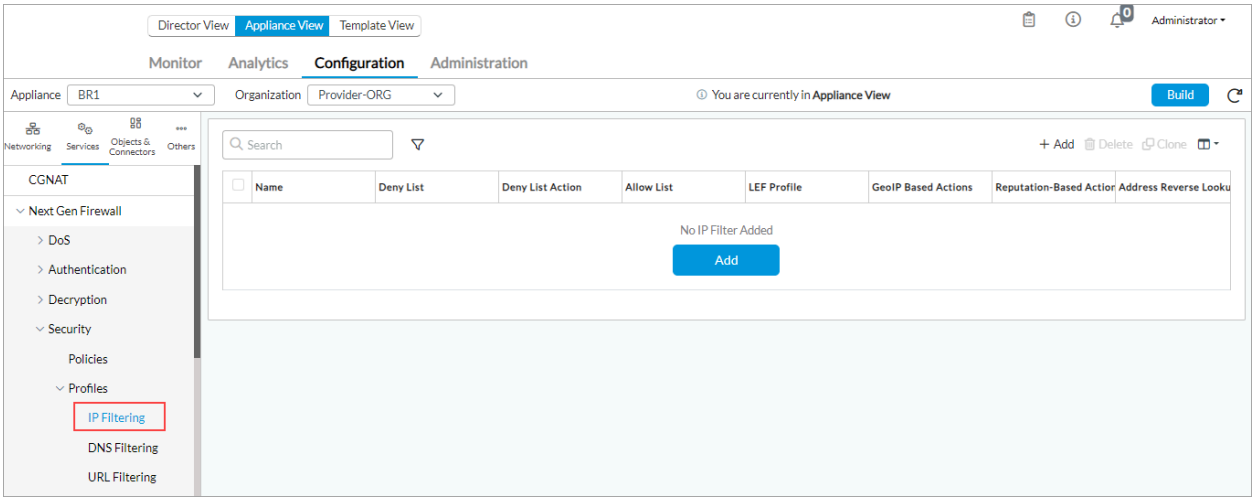
For information about configuring IP filtering, see Configure IP Filtering.

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

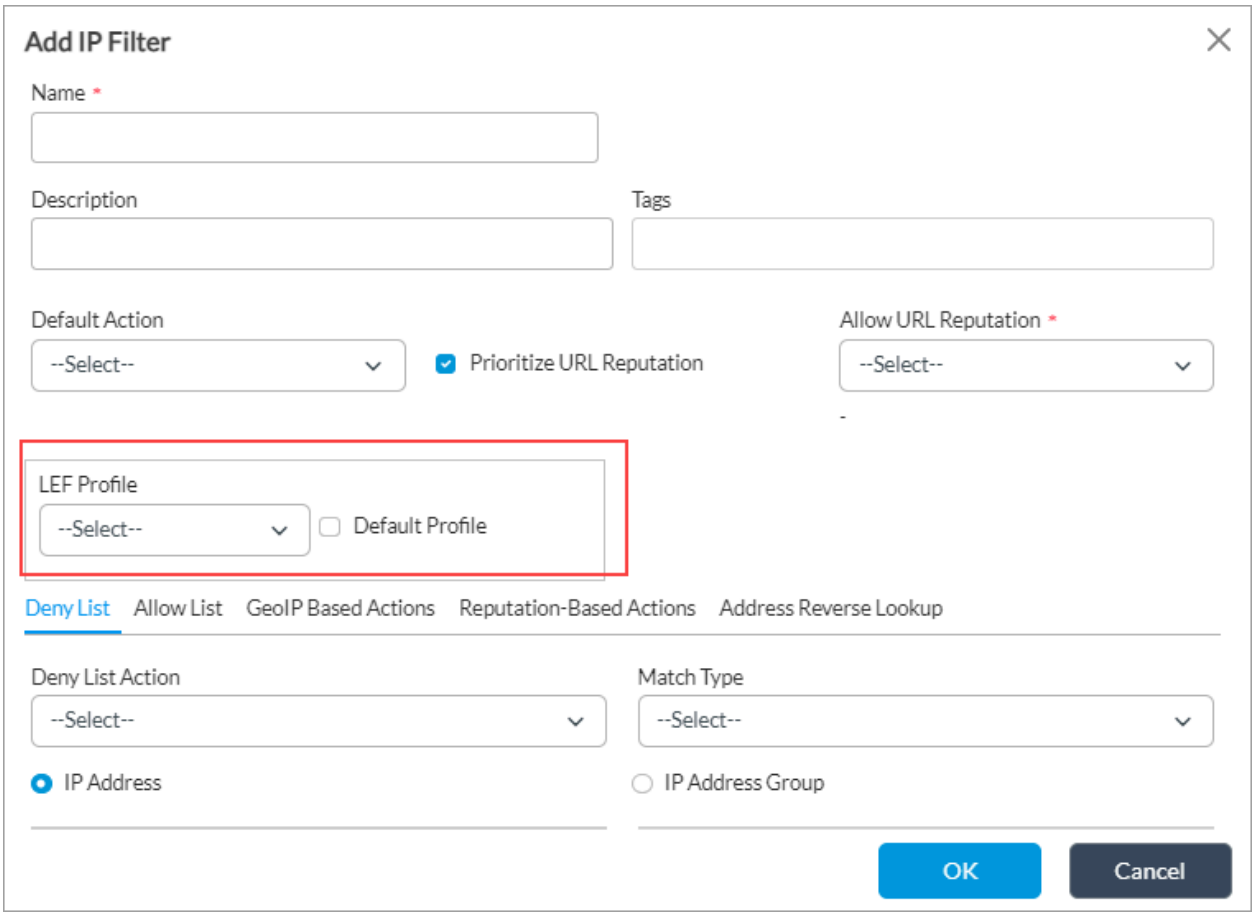
name of the provider organization or click the ► next to the organization's name. Then, select a tenant organization.

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.

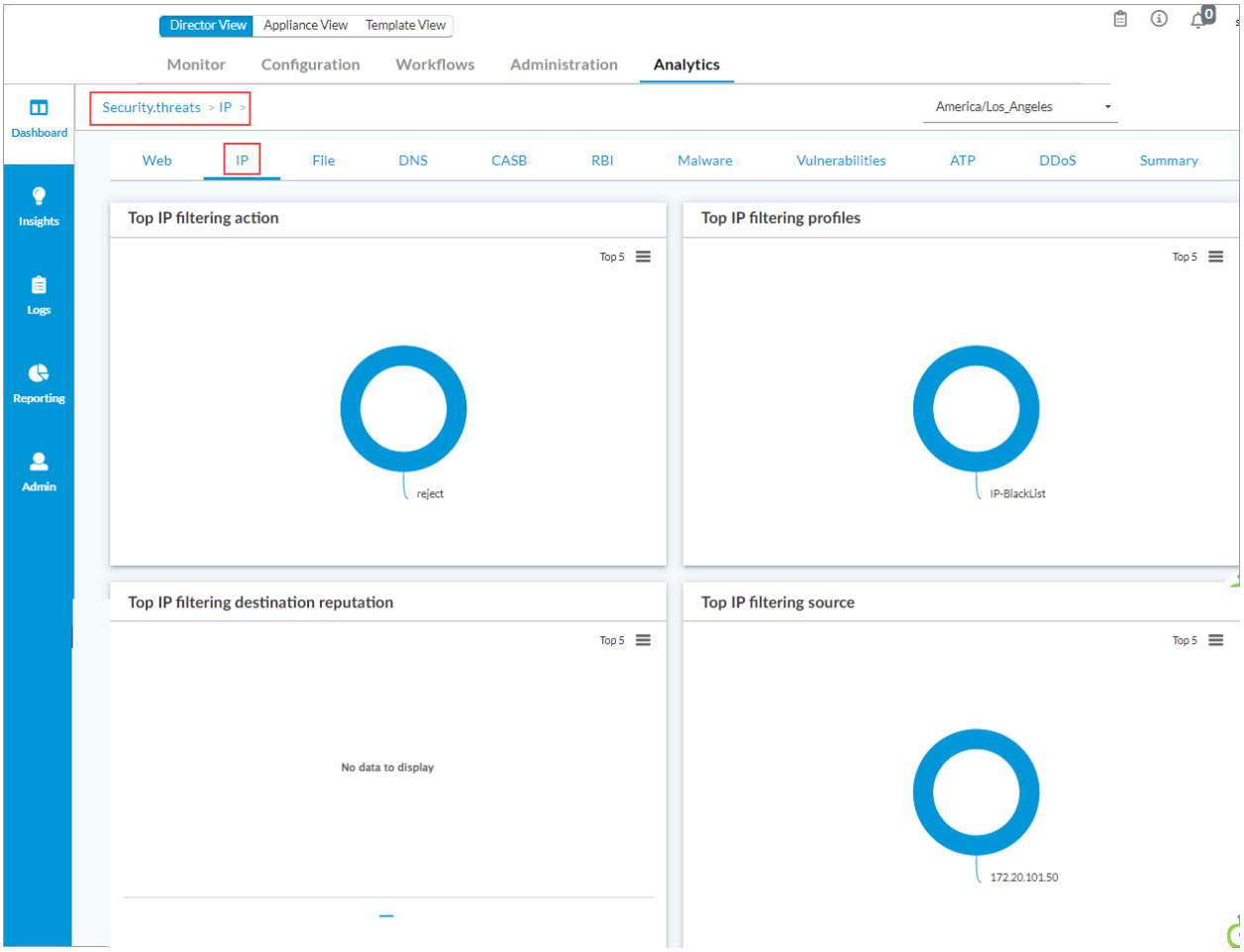


4. Click the + Add icon. The Add IP Filter popup window displays.



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.

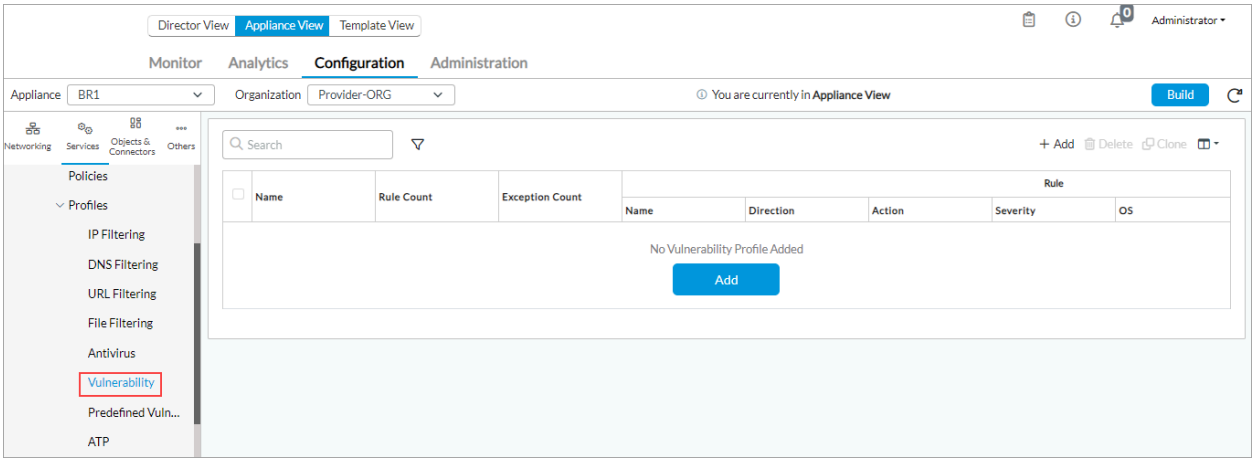


Configure IDP Threat Detection Vulnerability Logging

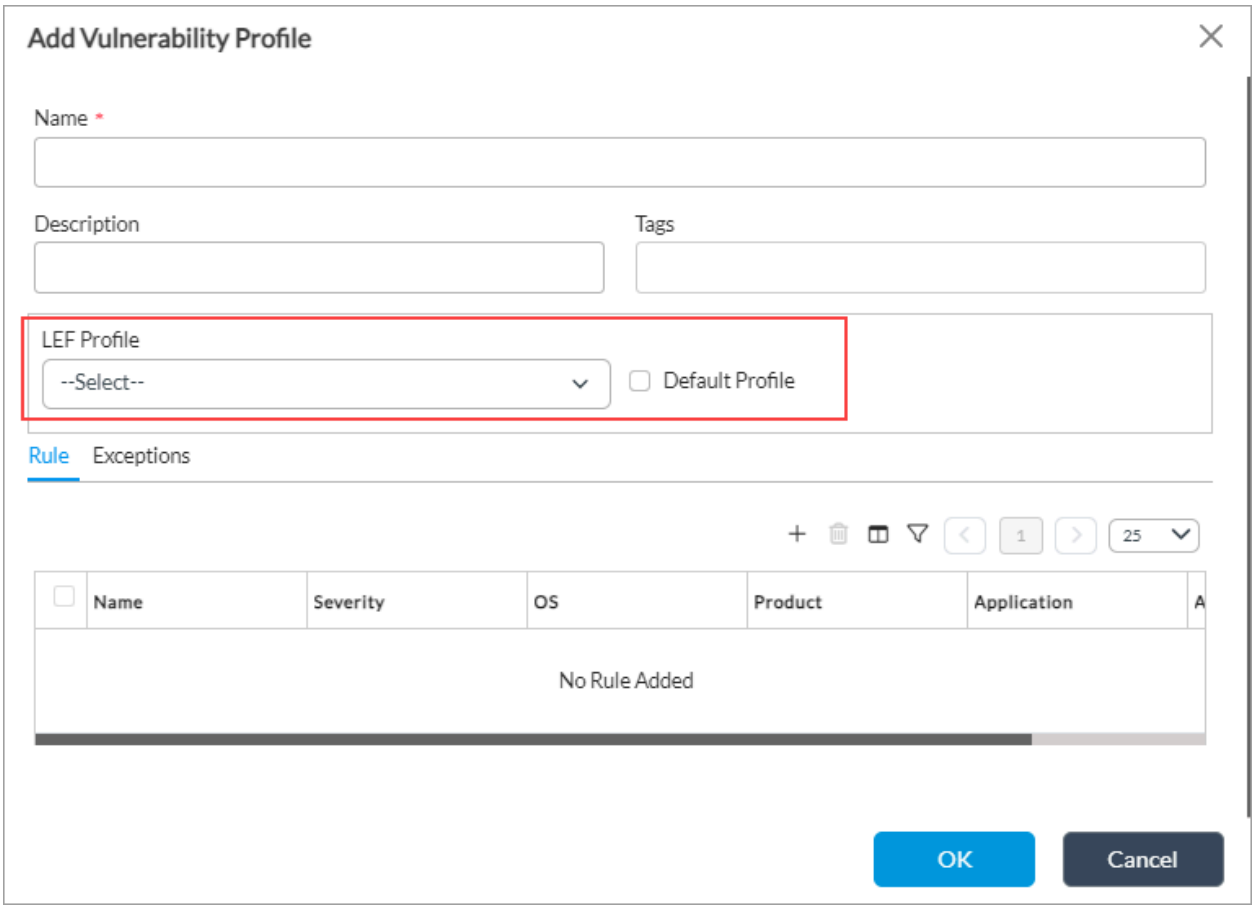
For information about configuring IDP, see Configure Intrusion Detection and Prevention.

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.

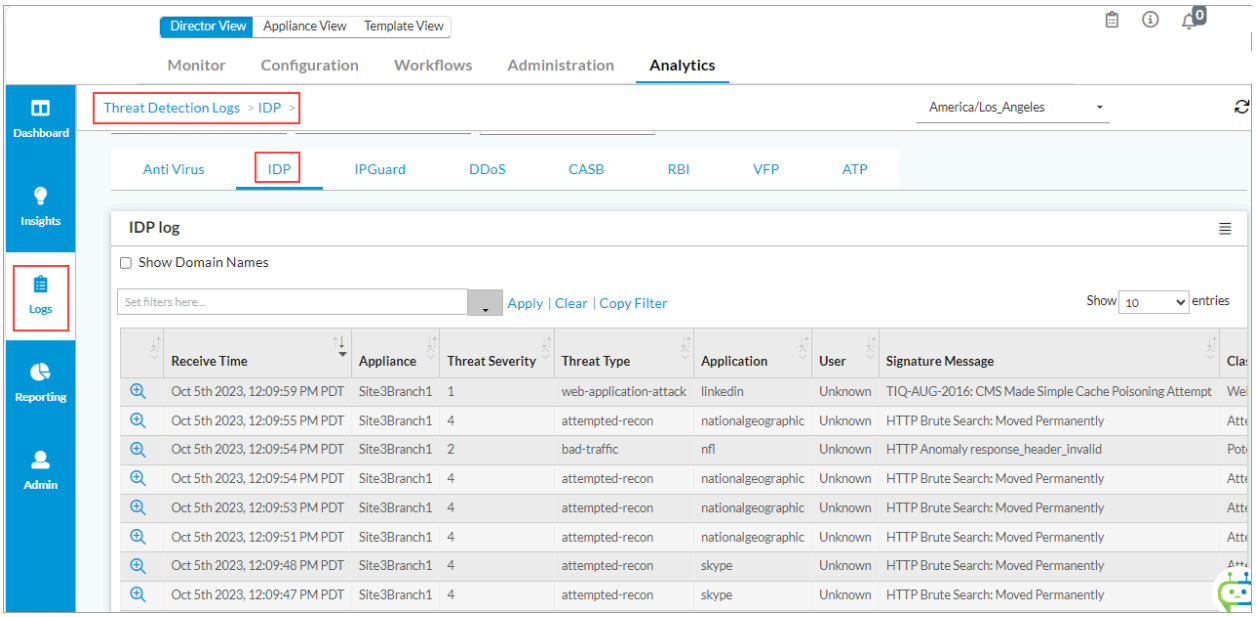


4. Click the + Add icon. The Add Vulnerability Profile popup window displays.



5. In the LEF Profile field, 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 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.

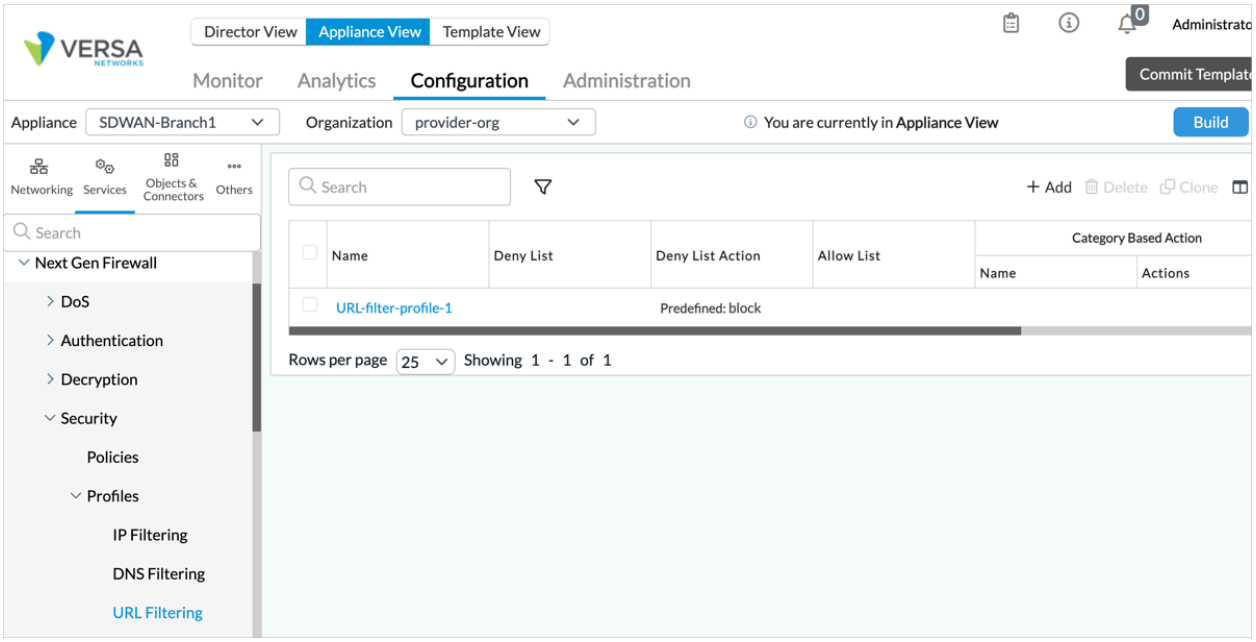


Configure URL-Filtering Threats Logging

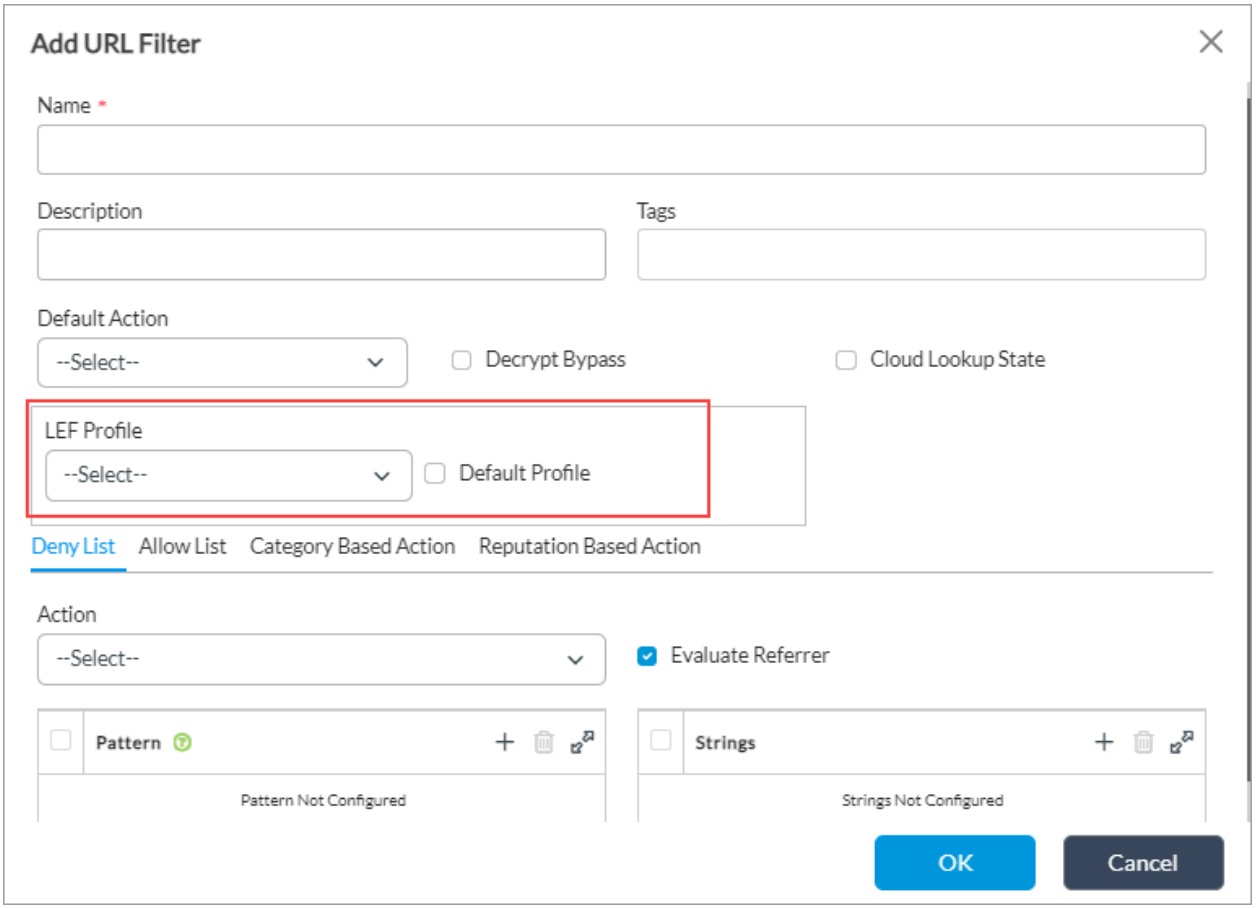
To reduce the number of URL-filtering logs generated, you can enable only deny-listed URL profile logging. You cannot enable logging for all URLs. For information about configuring URL filtering, see Configure URL Filtering.

To enable URL-filtering logging:

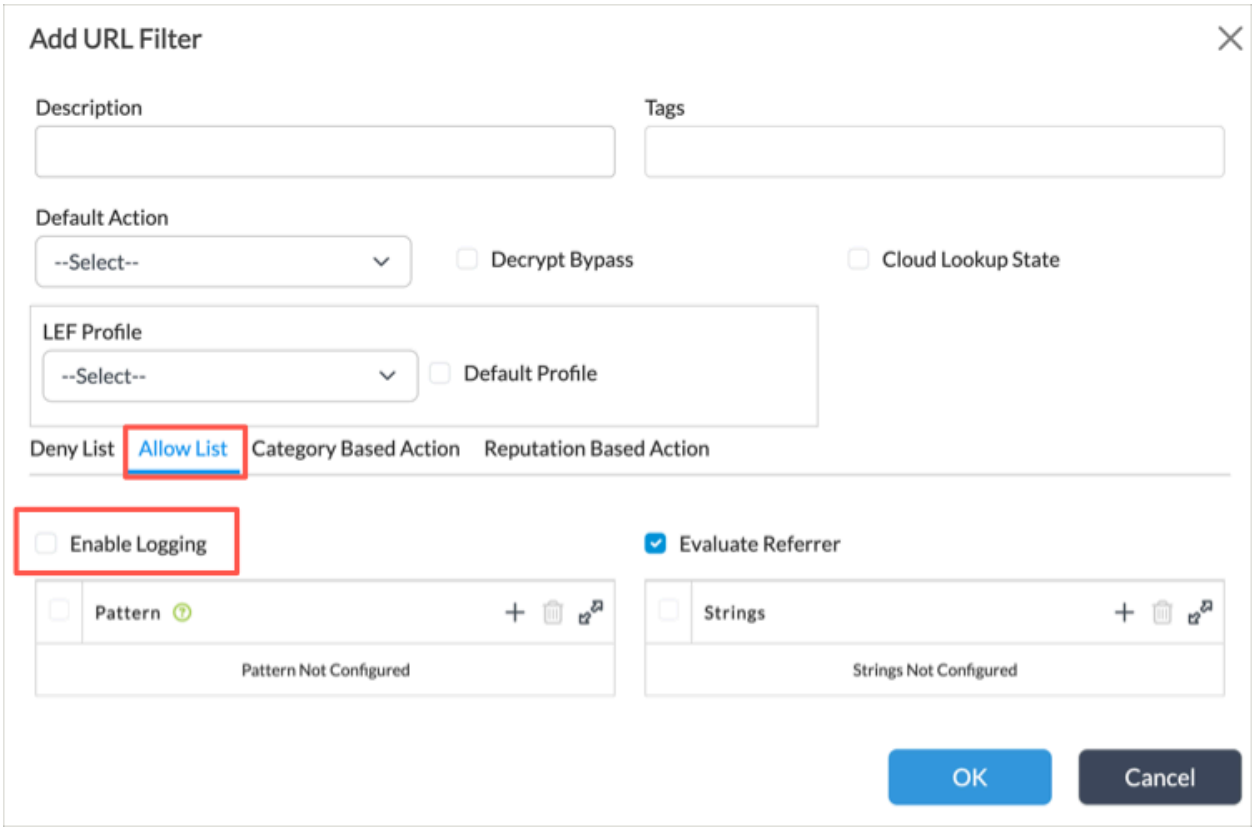
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select an organization in the left menu bar. To display the tenants in a provider organization, double-click the name of the provider organization or click the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



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

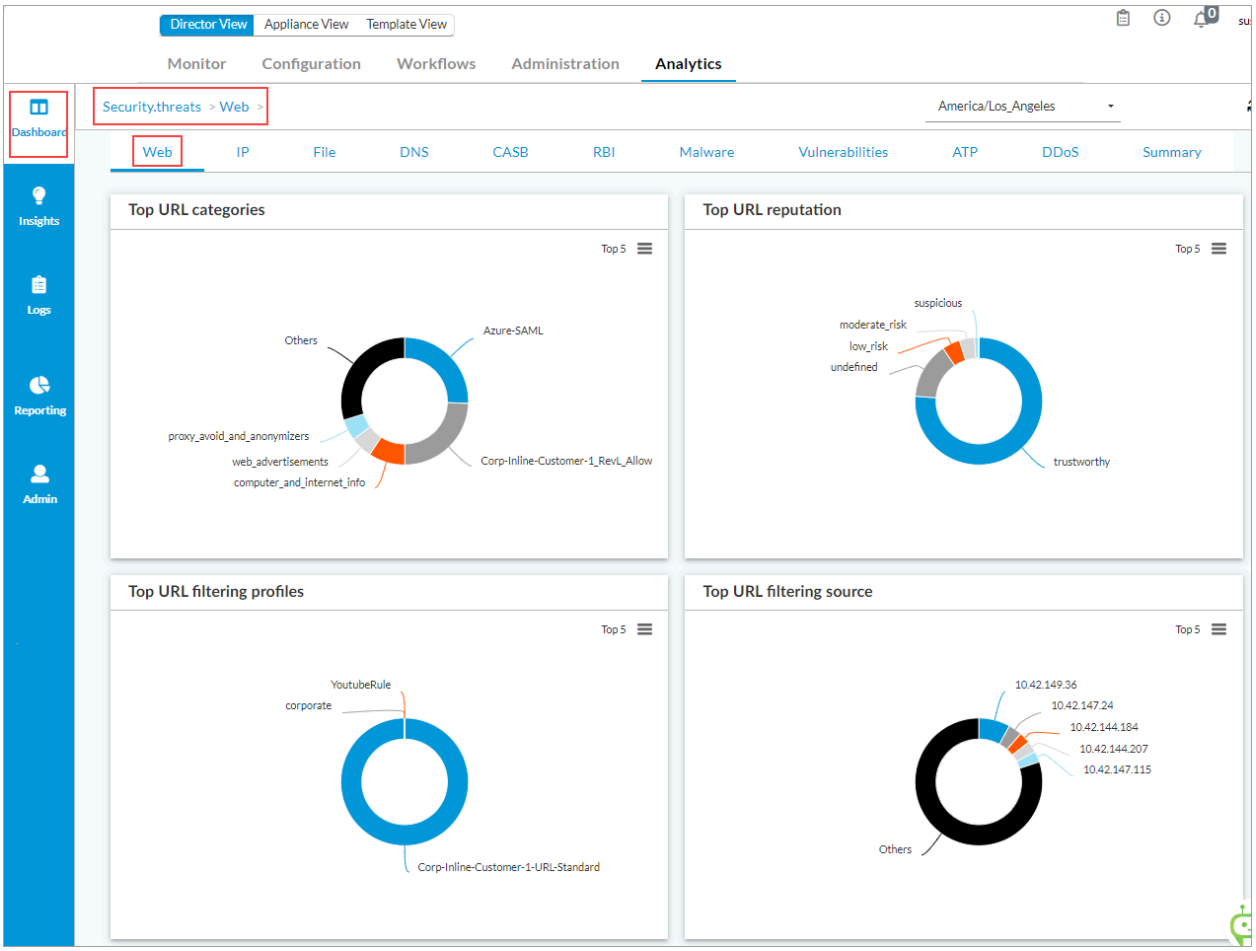


5. In the LEF Profile field, select a LEF profile, or click Default Profile to use the default LEF profile. This exports logs for URLs that match the deny list, category action , or reputation action.
6. To also export logs for URLs that match the allow list , select the Allow List tab and then click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

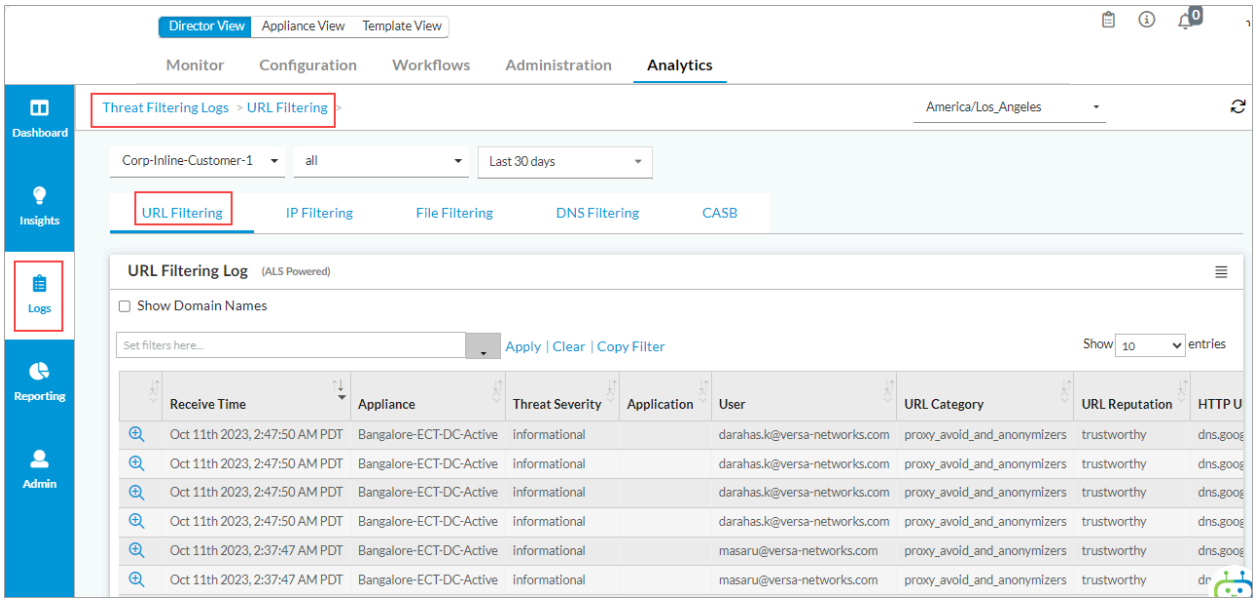


7. Click OK.

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.



Configure TWAMP Logging

For Releases 21.2.1 and later.

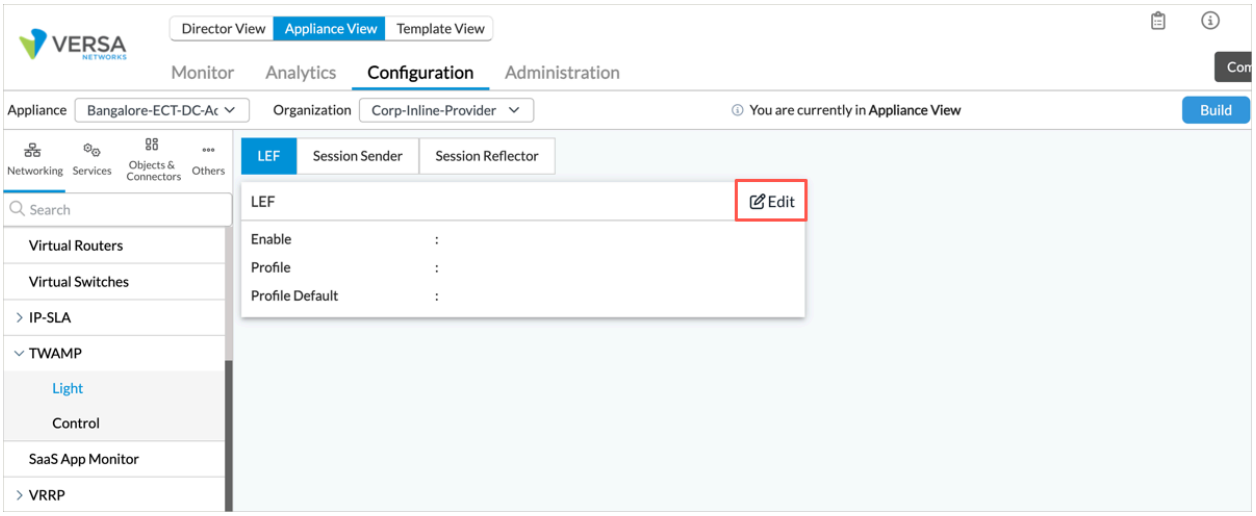
- Syslog identifier—twampSenderSessLog
- Path to the configuration screen—Administration > Configuration > Settings > Data Configurations > Analytics Data Configurations > Measurement Stats

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.

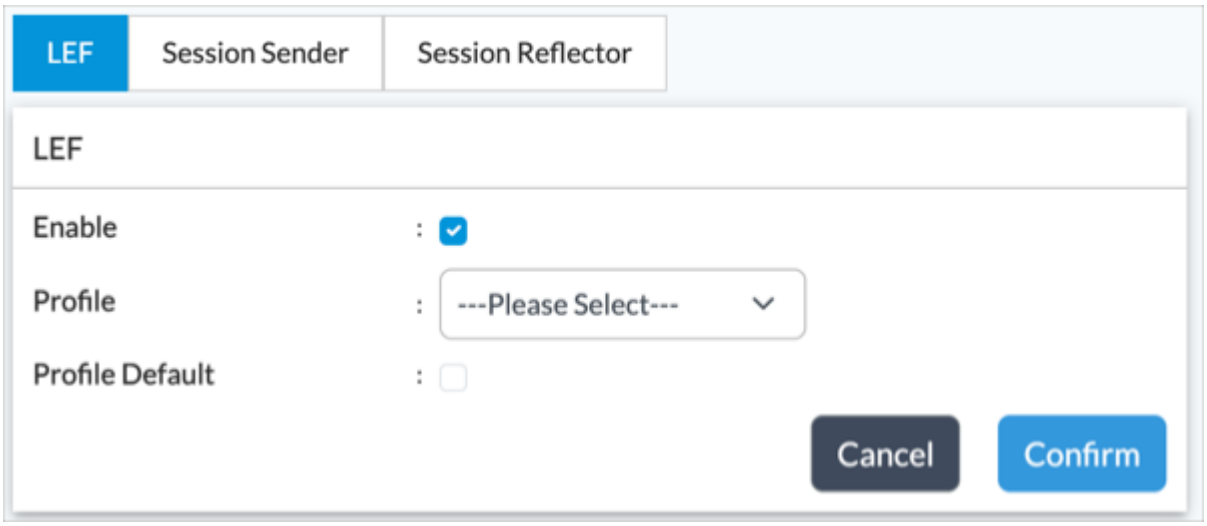
To export TWAMP logs, select a LEF profile when configuring TWAMP sessions. For information about configuring TWAMP, see Configure Two-Way Active Measurement Protocol.

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.

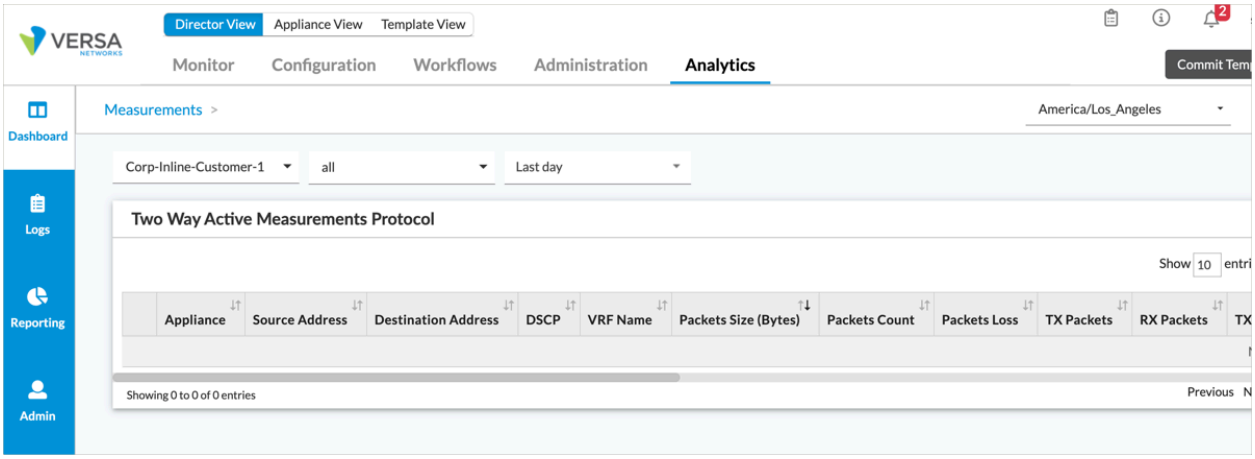


3. Click Enable, and then select a LEF profile, or click Profile Default to use the default LEF profile.



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.



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