

---

## Configure the Exporting of Session Log Records

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

When a Versa Operating System™ (VOS™) device sends session (flow) log messages for services, each flow is identified by a number of parameters, including the tenant ID, source IP address, destination IP address, source port number, destination port number, and protocol. Because these parameters are common to all the log messages generated during the duration of a flow, the VOS software optimizes the logging process by sending a flow identification log that includes all common parameters, followed by feature-specific logs. Correlation of the logs belonging to a specific flow is done using a combination of the (tenantId, applianceId, flowId, flowCookie, vsnId) fields, which are present in each of the flow logs. However, many third-party collectors and log message implementations cannot perform this correlation, because it requires state management.

To make it simpler for third-party collectors and log message implementations to process VOS flow logs, for Releases 20.2.2 and later, you can configure flow logging to also include tuple information (source IP address, destination IP address, source port, destination port) in each flow log. To do this, you click (enable) the Include Session ID Logging field for Firewall and SD-WAN when you configure the parameters for exporting log records. For Releases 21.1.1 and later, sending the session identification is enabled by default.

When you include the session ID logging information, the log messages include the following session identification parameters:

- For IPv4 flows—sourceIPv4Address=<>, destinationIPv4Address=<>, sourceTransportPort=<>, destinationTransportPort=<>
- For IPv6 flows—sourceIPv6Address=<>, destinationIPv6Address=<>, sourceTransportPort=<>, destinationTransportPort=<>

When you enable session ID logging information for SD-WAN logs, the session identification parameters are appended to the accessLog, avLog, fileFilterLog, idpLog, ipfLog, and urlfLog log messages.

When you enable session ID logging information for firewall logs for SD-WAN logs, the session identification parameters are appended to the flowMonLog, flowMonHttpLog, and sdwanFlowMonLog log messages.

For descriptions of the log fields, see [Flow Logs](#).

Note that whether you enable session ID logging information or not, a flowIdLog log message is sent for all flows.

To illustrate the different log message formats, the following is an example of the default firewall log message format,

without the session identification parameters:

```
2020-05-27T23:47:42+0000 accessLog, applianceName=SDWAN-Branch1, tenantName=Tenant1,
flowId=2181768529, flowCookie=1590623217, flowStartMilliseconds=2148889852,
flowEndMilliseconds=2148889875, sentOctets=589, sentPackets=7, recvdOctets=671,
recvdPackets=6, appld=298, eventType=end, tenantId=2, urlCategory=social_network,
action=allow, vsnId=0, applianceId=1, appRisk=3, appProductivity=4, appldStr=linkedin,
appFamily=collaboration, appSubFamily=forum, rule=linkedin, forwardForwardingClass=fc_be,
reverseForwardingClass=fc_be, host=www.linkedin.com, deviceKey=, deviceName=,
```


The following shows the firewall log message format that includes the session identification parameters. The bolded text highlights the fields that are added to the log message.

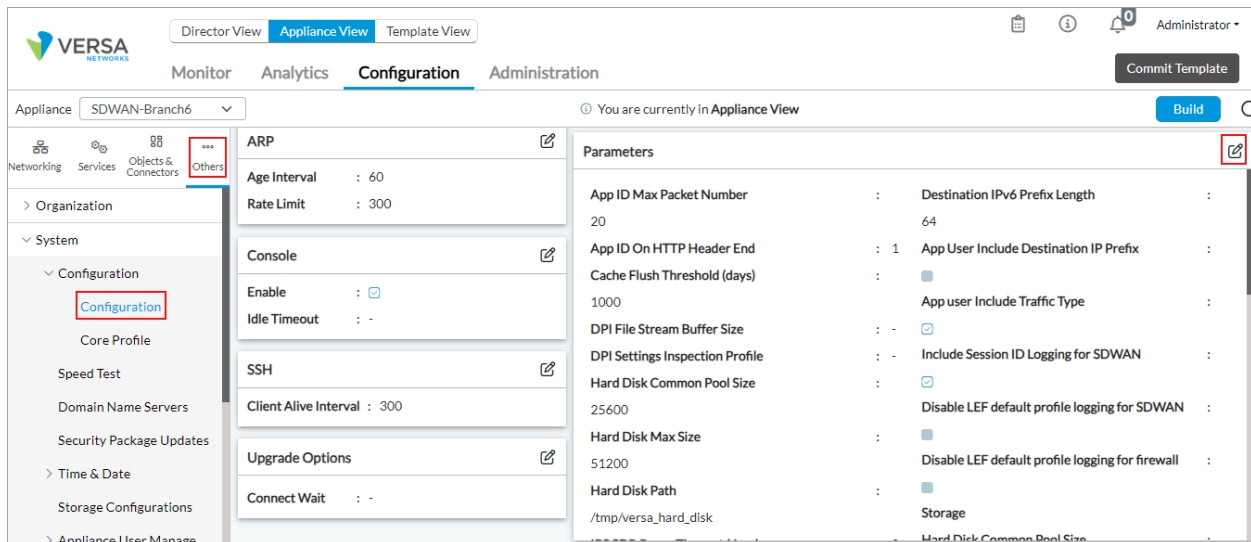
```
05-27T23:46:35+0000 accessLog, applianceName=SDWAN-Branch1, tenantName=Tenant1,
flowId=2181767937, flowCookie=1590623141, flowStartMilliseconds=2148813878,
flowEndMilliseconds=2148813963, sentOctets=589, sentPackets=7, recvdOctets=671,
recvdPackets=6, appld=298, eventType=end, tenantId=2, urlCategory=social_network,
action=allow, vsnId=0, applianceId=1, appRisk=3, appProductivity=4, appldStr=linkedin,
appFamily=collaboration, appSubFamily=forum, rule=linkedin, forwardForwardingClass=fc_be,
reverseForwardingClass=fc_be, host=www.linkedin.com, deviceKey=, deviceName=,
sourceIPv4Address=172.16.11.110, destinationIPv4Address=172.16.21.10, sourceTransportPort=34653,
destinationTransportPort=80
```

---

## Configure the Exporting of Session Log Records

To configure the exporting of log records for statistics related to firewall and SD-WAN operations:

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 a tenant in the left menu bar.
  - d. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Configuration > Configuration in the left menu bar.
4. In the Parameters pane, click the  Edit icon.



5. In the Edit Parameters popup window, select the LEF tab and then enter information for the following fields.

Edit Parameters

×

General

Storage

LEF

Dynamic Scale

DPI / IPS Custom Config

Disable LEF Session Logging

Firewall

Source IP Count

50

Destination IP Count

50

Include Session ID Logging

SDWAN

App User Count

100

Destination IPv4 Prefix Length

24

Destination IPv6 Prefix Length

64

App User Include Destination IP Prefix

Include Session ID Logging

Include Private App User

OK

Cancel

Field	Description
Firewall (Group of Fields)	
<ul style="list-style-type: none"> <li>Include Session ID Logging</li> </ul>	<p>(For Releases 21.1.1 and later.) Click to include session (flow) identification parameters in the exported firewall statistics log. By default, sending the session identification is enabled.</p> <p>(For Releases 20.2.2 and 21.1.0.) Click to include</p>

Field	Description
	session (flow) identification parameters in the exported firewall statistics log. Each log contains a flow identifier, common parameters (such as tenant ID, source and destination addresses, and source and destination ports), and feature-specific logs, if any. For third-party implementations or collectors, however, it can be difficult to correlate these parameters.
SD-WAN (Group of Fields)	Configure the SD-WAN user application statistics logs to export from the VOS device to the Analytics node.
<ul style="list-style-type: none"> <li>Include Session ID Logging</li> </ul>	(For Releases 21.1.1 and later.) Click to include session (flow) identification parameters in the exported SD-WAN statistics log. By default, sending the session identification is enabled.

- Configure the remaining fields, as described in [Configure Firewall and SD-WAN Usage Monitoring Controls](#).
- Click OK.
- Click Home to return to Director view.

---

## Supported Software Information

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

- Releases 21.1.1 changes the allowable range and adds default values for the Firewall Source IP Count and Destination IP Count fields, and for the SD-WAN Application User Count field. Adds support for including session ID parameters in SD-WAN logs.

---

## Additional Information

[Configure Application Performance Monitoring](#)

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

[Configure Log Export Functionality](#)

[Flow Logs](#)