

Cisco NetFlow

To get routers and switches that support NetFlow IP traffic statistics (version 9), configure XpoLog to listen on a network port for incoming NetFlow data:

1. Go to Manager > Administration > Listeners. The Listeners management console opens.
2. Add NetFlow account, for each account the following should be configured:
 - a. **Name:** the name of the Listener account
 - b. **Description:** the description of the Listener account
 - c. **Listening Node:** the node in the cluster which will listen to the Syslog messages (appears only if a XpoLog cluster is deployed)
 - d. **Port:** the port which will be used on the XpoLog machine to receive Syslog messages of this Listener account (usually 2055)

e. **Advanced Settings:**

General Information:

Enabled: determine whether this account is enabled or not

Listening Interface: the network interface (IP address) on which the XpoLog listener instance is listening

Dynamic Log Creation Configuration:

Parent Folder: the parent folder which all logs from this listener will be placed under in XpoLog Folders and Logs tree

Collection Policy: the [collection policy](#) which will be associated to all logs from this listener (used mainly for storage location and data retention)

AppTags: the [AppTags](#) which will be associated to all the logs from this listener (used mainly for data enrichment)

Log Name Prefix: a prefix which will be added to any of the logs from this listener (used to easily distinguish between multiple listener accounts logs)

Split by Source Device:

- i. Do not split - by default, XpoLog will not split the incoming data. All data will be stored under a single log in XpoLog.
- ii. Create log by unique IP / host name - XpoLog will split the incoming data based on the source that sends it to different logs, the log name structure will be "Log_Name_Prefix Source_IP/Name"
- iii. Create log by IP mask - XpoLog will split the incoming data based on matched source to the configured IP mask that sends it to different logs, the log name structure will be "Log_Name_Prefix IP_Mask"
- iv. Create log with Regular expression - XpoLog will split the incoming data to different logs based on a regular expression that will be applied on the Message field. The part in the regular expression that will be used to determine the split should be in (round parentheses).
Records that the regular expression does not return a value will be directed to the global NetFlow log.

Listener Data:

Listener Data Location: the location which data will be stored to, by default XpoLog stores it in its data directory

Indexing Node: the node in the cluster which will index the received Syslog messages (appears only if a XpoLog cluster is deployed)

Indexing Interval: the frequency in which received Syslog messages are indexed

3. Save the account.
4. Data received to the NetFlow listener account will be created under the configured parent folder and will be available for searching, reporting and alerting.

Note: multiple listeners accounts may be configured. However, listeners which run on the same machine must listen on a different network port.