Log Processing

Logline Filters are employed to ensure only relevant human activity is stored in the DrawBridge web activity database.

Log Servers + **Log Sender Batches** together are an optional function used for export of DrawBridge filtering logs to an external web traffic log analysis service.

When configured: a device is filtered by the DrawBridge, which logs all the web traffic of that device. Then, on a schedule, the DrawBridge uploads those web traffic logs to a separate log analysis/Reporter server for additional operations to be performed.

Important Note: The Log Server/Sender system is inactive unless the following two conditions are met:

- A Log Server is configured. (See below)
- A Log Server Account Number is configured on one or more Company records. See **Accounts: Companies** for more information.

Logline Filters

Remove unwanted Log Lines before saving them to Reporter database.

Displays a list view of rulesets which apply to loglines prior saving them in the DrawBridge log database.

List view displays:

Column	About
Sequence	Priority of rule when processing is performed
Filter	Name of rule
Scope	Defines operations of the rule
Field	Parameter of Logline database field to which the rule applies
Operator	Data matching parameter (In , Contains , Starts With , and so forth)

Logline Filter Record view

Parameter	About
Name Details	Name of the rule
Notes	Comments about the rule, where applicable
Matches If	Expressions which trigger the rule
data list	Exact text that is referenced in the expression.

Logline Filter Record header buttons:

- **Add** a Logline Filter record with the blue **+** Create Logline Filter button
- **Edit** this Logline Filter record with the green pencil Update Logline Filter button
- **Delete** this Logline Filter record with the red trashcan Delete Logline Filter button
- Sync menu (**blue chainlink icon**)
  - **2 Way - Push / Pull from Server:** call a sync run for this record
  - **Push to Sync Publisher:** send this record to the sync server
  - **Pull from Sync Publisher:** fetch this record from the sync server
  - **Mark to Resync:** flag this record for inclusion in the next sync server run

Scope options:

A rule can apply with the following scope of action:

- Skip All Logging -- Discard/Don't Save or Upload traffic matching this rule
- Log Summary Details Only -- Skip detailed logging data for traffic matching this rule
- DNS Log Lines -- Discard/Don't Save or Upload traffic containing these domain names

Log Servers

Uploaded Log Lines to compatible Report Server for further processing.

Displays a list view of configured Log Servers.

List View displays:

Column	About
Name	Display name of the log server
URL	Web address of the log server

Log Server Record View

Parameter	About
Name	Display name of the Log Server
Status	This record is `Active` or `Inactive`
URL	Web address of the log server

Log Server Record header buttons:

- **Add** a Log Server record with the blue **+** Create Log Server button
- **Edit** this Log Server record with the green pencil Update Log Server button
- **Delete** this Log Server record with the red trashcan Delete Log Server button
- **Bookmark** this record with the blue ribbon Bookmark This Page button
- Sync menu (**blue chain icon**)
  - **Create on Sync Publisher:** Push this record to the Sync Server

Log Sender Batches

Log Sender Batch Details

Displays a list view of all configured Log Sender batches for Company records which have a Log Server Account number specified.

Filter the data with the following Select field:

- Company

List View displays:

Column	About
Name	Display name of batch job
Company	Associated company of the batch job
Date	Timestamp of last batch job run event
Uploaded To	Timestamp of most recent data uploaded
Results	What the Log Processor job did

Log Sender Batches is informational-only and does not have a record view.

FAQ:

- **Q:** Why does the Log Sender Batch indicate 0 lines uploaded, even though devices on the Company are being used?

A: Either the devices are not properly connecting to the DrawBridge, or, any data that was recorded was considered system activity, not human activity, and was therefore discarded. See **Logline Filters** above for more information.

Revision #3
Created 6 December 2022 14:24:02 by Marvin M.
Updated 6 December 2022 15:32:14 by Marvin M.