

Collect Host Based Logs through the Armor Agent

Armor Knowledge Base

Topics Discussed

- [Log Relay](#)
- [Order Log Relay for Host Log Collection](#)
- [Review Additional Agent-Related Commands](#)



In order to use this document, you must have the **Write LogManagement** permission assigned to your account.

You can use the **Log Relay** add-on product to securely store file-based application logs with Armor for 30 days or 13 months, based on your log retention plan.

Log Relay

- Collects only single-line log formats.
- Does not provide security analysis, parsing, or awareness of log content.
- Can store up to 10,000 logs

At a high-level, to use Log Relay, you must:

- Order Host Log Collector
- Send logs to Armor



In some cases, the terms **Log Depot**, **Host Log Collector**, or **Log Relay** may be used interchangeably.



For pricing information, please contact your account manager.

Order Log Relay for Host Log Collection

Step 1: Add Log Relay

Use the **Post Host Log Collector (Activate) API** to add Host Log Collector to your account.

Method / Type	POST
API call / URL	/log-management/log-depot/activate
Parameters	There are no parameters for this API call.
Full API call / URL	POST <code>https://api.armor.com/log-management/log-depot/activate</code>

Sample 200 return

```
{
  "accountId": 0,
  "modifiedByUserId": 0,
  "modifiedDate": "2017-10-23T16:35:13.540Z",
  "isEnabled": true
}
```



To learn more about this API call, see [Post Host Log Collector \(Activate\)](#).

Step 2: Send Logs to Armor

1. Contact Armor Support to add a custom file path via a host log collector.

Review Additional Agent-Related Commands

Review the following table to better understand how to interact with the agent via the command line:

Command	Description
<code>armor -h</code>	Displays the agent's help dialog
<code>armor policy -h</code>	Displays the agent's policy help dialog
<code>armor policy filelog -h</code>	Displays the agent's policy filelog help dialog
<code>armor policy filelog add -h</code>	Displays the agent's policy filelog add help dialog
<code>armor policy filelog --add [path]</code>	Adds a filebeat logging policy with the user-defined path, category, and tag(s).
<code>armor policy add eventlog [name]</code>	Adds a (Windows) eventlog logging policy with the user-defined path, category, and tag(s).
<code>armor policy show</code>	Displays command functionality and syntax available at the command line. "show" can be added to any level of command to help drive user input
<code>armor policy sync</code>	Synchronizes the local Armor CORE Agent with API services to pull down the latest policy version

Troubleshooting

If you do not see any data in the **Search** section of the **Log & Data Management** screen, consider that

- You did not order Log Relay.
- You did not properly sync Log Relay to collect logs.
- The selected date range does not contain any data.
- You do not have permission to view log data.
 - You must have the **Write LogManagement** permission enabled to access the **Search** section. Contact your account administrator to enable this permission. To learn how to update your permissions, see [Roles and Permissions](#)



Was this helpful? *

Your Rating:

Results: 11 rates