

Log Management

Home > Armor Complete - Product User Guide > Log Management

This topic only applies to **Armor Complete** users.

To fully use this screen, you must add the following permissions to your account:

- Read LogManagement
- Write LogManagement
- Read Log Management Plan Selection
- Write Log Management Plan Selection

Overview

You can use the **Log & Data Management** screen to:

- View collected logs in the **Search** section
- View the status of the logging subagent in the **Sources** section

By default, Armor collects and retains the following log types for 30 days:

CentOS/RHEL	Ubuntu/Debian	Windows
/var/log/secure	/var/log/auth.log	System Event Log
/var/log/messages	/var/log/syslog	Security Event Log
/var/log/audit.log		
/var/log/audit/audit.log		
/var/log/yum.log		

Search for collected logs

The Armor Management Portal (AMP) only displays logs from the previous 30 days.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Search**.
 - Enter separate search terms within quotation marks.
 - Enter exact search terms, including letter capitalization.

Column	Description
Date	This column displays the date and time when Armor received the corresponding log.
Source	This column displays the name of the virtual machine that generated the log.
Message	This column displays the specific log message.

To better understand how to perform successful searches, consider the following sample log message: **2019-04-08T18:46:09Z INFO No non-zero metrics in the last 30s**

In a log message, spaces between words indicates a separate search term. For instance, there are no spaces in **2019-04-08T18:46:09Z**. As a result, **2019-04-08T18:46:09Z** is considered one search term. In this example, to search for dates, you must enter the complete and exact date; you cannot perform searches with partial search terms, such as 2019-04.

Successful search parameters	Unsuccessful search parameters	Description
<ul style="list-style-type: none"> "2019-04-08T18:46:09Z" 	<ul style="list-style-type: none"> 2019 2019-04-08T18:46:09Z 	<p>If the search term contains special characters, such as a colon, then you must perform the search with quotation marks (" ").</p> <p>Also, in this example, the complete search term is 2019-04-08T18:46:09Z. You cannot perform a search on partial search terms, such as 2019.</p>
<ul style="list-style-type: none"> "INFO" 	<ul style="list-style-type: none"> INF 	<p>You cannot perform a search on partial search terms. In this example, the complete search term is INFO, not INF.</p>
<ul style="list-style-type: none"> "metrics" "30s" 	<ul style="list-style-type: none"> "metrics" "30" 	<p>You can search for different search terms by separating terms with quotation marks.</p> <p>In this example, the complete search term is 30s, not 30. You cannot perform searches with partial search terms.</p>
<ul style="list-style-type: none"> *zero *30 	<ul style="list-style-type: none"> *zero 30 	<p>Similar to the use of quotation marks, you can also use an asterisk (*) to perform a wildcard search for strings.</p> <p>A wildcard search may take a few more seconds to complete.</p>

View logging subagent status

You can use these instructions to review the logging status of your virtual machines. Specifically, you can verify if your virtual machine is sending logs to Armor.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Sources**.

Column	Description
VM	<p>This column displays the name of the instance that contains the Armor agent.</p> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>You can click a specific virtual machine to access the Virtual Machines screen.</p> </div>
Last Log Received	<p>This column displays the date and time when Armor last received a log.</p>

Retention Type	<p>This column displays the length of time that Armor keeps logs.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>By default, the Armor Management Portal (AMP) retains log status and details for the previous 30 days. To review logs older than 30 days for a specified instance, see Review log retention plans.</p> </div>
Average Size	This column displays the average size of the collected logs.
Log Status	<p>This column displays the status of the logging subagent.</p> <ul style="list-style-type: none"> • Online indicates the agent has sent logs within the past hour. • Warning indicates the agent in the past 24 hours has sent logs that exceeds the 7-day moving average by 10% or more. • Critical indicates the agent has not sent logs within the past hour. • Offline indicates the agent (or the instance) is offline.

View log collections projections

You can use these instructions to review AMP's prediction regarding future log collection. You can use this information to estimate log collection cost.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Retention Plan**.
4. Review the **Total Log Storage** graph.
 - The dotted line indicates AMP's prediction for your future log collections.

Export log service status

You can export the logs that are displayed in the Armor Management Portal (AMP) to analyze offline or to provide to an auditor.

This file export will only contain logs from the previous 30 days.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **Log Sources**.
4. (Optional) Use the filter function to customize the data displayed.
5. Under the table, click **CSV**.
6. You have the option to export all data (**All**) or only the data that appears on the current screen (**Current Set**).

Data Type	Data Detail
Vm Name	This data shows the name of the Armor Agent.
Last Log Date	This data shows the last date that Armor received logs. A blank entry indicates that the action has never taken place.
Vm Provider	This data shows if you are an Anywhere or Complete user. If Armor cannot determine your specific environment, such as AWS or Azure, then by default, this entry will say Anywhere .
Vm Location	This data shows the virtual data center that hosts your data.
Retention	This data shows how long the logs are stored in the Armor user interface.
Average Size	This data shows the average log size.

Agent Status	<p>This data shows the status of your Armor Agent.</p> <p>Online - This status means the Armor Agent is active and has sent logs within the last hour.</p> <p>Warning - This status means the previous 24-hour log volume has exceeded the 7-day moving average by 10% or more.</p> <p>Critical - This status means the Armor Agent has not sent logs within the last hour.</p> <p>Offline - This status means that the Armor Agent, and possibly the virtual machine, is offline.</p>
--------------	--

Troubleshoot Log Management screen

Search section or Sources section

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

- The selected date range does not contain any data.
- The virtual machine may be powered off.
- You do not have permission to view log data.
 - You must have the **ReadLogManagement** permission enabled to view log data. Contact your account administrator to enable this permission. To learn how to update your permissions, see [Roles and Permissions \(Armor Complete\)](#).

Retention Plan section

If you cannot add or update your plan, consider that you do not have permission to update your plans. You must have the following permissions enabled:

- **Read Log Management Plan Selection**
 - **Write Log Management Plan Selection**
 - **Read LogManagement**
 - **Write LogManagement**
-

Review API calls

- [Get Log Entries](#)
 - [Get Log Event Types](#)
 - [Get Log Management List](#)
 - [Get OS Log Graph](#)
 - [Get OS Log Details](#)
 - [Upgrade Log Retention Plan](#)
 - [Get Log Management Products](#)
 - [Post Log Depot \(Activate\)](#)
 - [Post Log Depot \(Deactivate\)](#)
 - [Search Log Events](#)
 - [Get Log Retention Types](#)
 - [Get Log Sources](#)
 - [Get Log Storage](#)
 - [Get Log Storage Totals](#)
-

Related documentation

To enhance the default **Log and Data Management** services, you can:

- Collect **host-based logs**.

- To learn more, see [Collect host-based logs through Log Relay \(Armor Complete\)](#) or [Collect host-based logs through Log Relay \(Armor Anywhere\)](#).
 - Convert your virtual machine into a log collector to collect **additional log types**.
 - To learn more, see [Convert a virtual machine into a log collecting device through Log Relay \(Armor Complete\)](#) or [Convert a virtual machine into a log collecting device through Log Relay \(Armor Anywhere\)](#).
-