Convert a virtual machine into a log collecting device through Log Relay (Armor Complete)

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

Overview

You can use the **Log Relay** feature to convert your virtual machines into a log collecting device, which will forward logs to the Armor Management Portal (AMP). Within AMP, Armor will securely store, review, and analyze supported log types.

In some cases, the terms **Log Collection** or **Log Collector** may be used instead of **Log Relay**.

Add Log Relay

Step 1: Review requirements

Support Devices	You can only convert Linux machines that are in an **OK** state. To learn more about the health status of a virtual machine, see Health Overview Dashboard (Armor Complete).
Pricing information	While log collection is available to all Armor Complete users, there is a cost associated with sending and storing logs. For pricing information, please contact your Account Manager.
Permissions	You must have the **Write Virtual Machine** permission included in your account in order to use **Log Relay**. To learn more about permissions, see Roles and Permissions (Armor Complete).
Log retention plan	Virtual machines that are converted to a log relay device will be automatically enrolled in the Compliance Professional plan. This plan: • Collects and stores your logs for 13 months at an additional cost. • Provides certain HIPAA and PCI compliance. For pricing information, please contact your Account Manager.

Step 2: Configure your virtual machine

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Virtual Machines**.
3. Locate and hover over the desired virtual machine.
4. Click the vertical ellipses.
5. Click **Convert to Log Relay**.
6. Review the product information, and then click **Convert VM to Log Relay**.
    - By default, the Armor agent will update the virtual machine within 15 minutes.

Step 3 Create a firewall rule for ingress

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. Click **Service Groups**.
4. Click the plus (+) icon.
5. In **Service Group Name**, enter a descriptive name, such as **Log Relay (ingress)**.
6. In **Add Members to Group**, enter:
    - tcp/5141
    - udp/5140
7. Click **Apply**.
8. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
9. Click **Firewall**.
10. Click **Rules**.
11. Click the plus (+) icon.
12. In **Name**, enter a descriptive name, such as **Log Relay (ingress)**.
13. In **Action**, select **Allow**.
14. In **Source**, enter the IP address of the application server that will send the logs.
15. In **Destination**, enter the IP address of the log collecting virtual machine.
16. Click **Save Rule**.

Step 4: Create a firewall rule for egress

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Firewall**.
3. Click **Service Groups**.
4. Click the plus (+) icon.
5. In **Service Group Name**, enter a descriptive name, such as **Log Relay (egress)**.
6. In **Add Members to Group**, enter **tpc/5443**.
7. Click **Apply**.
8. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
9. Click **Firewall**.
10. Click **Rules**.
11. Click the plus (+) icon.
12. In **Name**, enter a descriptive name, such as **Log Relay (egress)**.
13. In **Action**, select **Allow**.
14. In **Source**, enter the IP address of the log collecting device.
15. In **Destination**, enter **1c.log.armor.com**.
16. In **Services**, select the service group you created earlier (**Log Relay (egress)**).
17. Click **Save Rule**.

Step 5: Validate log collection in AMP

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log Management**.
3. Click **Sources**.
4. Search for the virtual machine that is sending logs.
5. Click **Search**.
6. Search for a log message from the application server.

Remove Log Relay

If you remove the log relay feature from a virtual machine, Armor will still retain the collected logs.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Virtual Machines**.
3. Locate and hover over the desired virtual machine.
4. Click the vertical ellipses.
5. Click **Remove Log Relay**.
6. Click **Remove Log Relay Services**.

Troubleshoot Log Relay

If you do not see any data in the **Log Collection** screen for **Log Relay**, consider that:

- Your instance is powered off.
    - To review the status of your instance, in the left-side navigation, click **Infrastructure**, and then click **Virtual Machines**.
    - For more information, see Virtual Machines (Armor Complete).
- You do not have permission to view and configure this screen.
    - You must have the **Write Virtual Machine** permission enabled. Contact your account administrator to enable these permissions. To learn how to update you permissions, see Roles and Permissions (Armor Complete).
