



**Hewlett Packard**  
Enterprise

# **HPE Security ArcSight Logger for AWS**

Software Version: 6.2

## Setup Guide

January 19, 2017

## Legal Notices

### Warranty

The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

### Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notice

© Copyright 2017 Hewlett Packard Enterprise Development, LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the HPE ArcSight Technical Support Page: <a href="https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list">https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.hpe.com">https://softwaresupport.hpe.com</a>
<b>Protect 724 Community</b>	<a href="https://www.protect724.hpe.com">https://www.protect724.hpe.com</a>

# Contents

Setting Up Logger for AWS .....	4
Launching an Instance of Logger for AWS .....	4
Configuring Logger for AWS .....	4
Additional Information .....	5
Send Documentation Feedback .....	6

# Setting Up Logger for AWS

Logger for AWS is available as an Amazon Machine Image (AMI) on the AWS Marketplace. It contains an operating system with Logger for AWS software pre-installed. You can launch an instance of this AMI to create a virtual machine (Elastic Cloud 2 instance) on the AWS cloud.

## Launching an Instance of Logger for AWS

This procedure assumes that you already have Amazon Web Services account.

1. Browse to the [AWS Marketplace](#) and login with your existing AWS account credentials.
2. In the AWS Marketplace section search for "Logger". Then, click **Select**.
3. On the next screen, in the **Filter by** field, select "Memory optimized" and "m3.2xlarge".
4. Click **Next: Configure Instance Details**. Skip this procedure, as there is no need to modify any setting on the Instance Details screen.
5. Click **Next: Add Storage**. There is no need to modify any setting on the **Add Storage** screen. If you choose to increase the capacity of secondary storage (EBS volume), follow the Amazon procedure to extend the EBS volume once the instance is launched. Refer to the AWS User's Guide topic on expanding the storage space of an EBS volume on Linux.
6. Click **Next: Tag Instance**. Then, in **Value**, enter a name for the instance.
7. Click **Next: Configure Security Group**. Then add any custom rules required for your environment.
8. Open port 9000 to access the Logger for AWS web interface.
9. Click **Review and Launch**. Review the configuration selections. Correct any incorrect settings by clicking **Previous** to return to the proper screen for editing. When the settings are correct, click **Launch**.
10. Create a new key pair and click **Download Key Pair**. Follow the instructions on screen to download the key pair. (The key pair is required for connecting to the instance remotely.)
11. Click **Launch Instances**. The Logger for AWS EC2 instance should be ready in few minutes. You can monitor the progress by visiting the EC2 dashboard and clicking the **Instances** link on the left panel.

Once the instance is in a running state, you can continue with the configuration of Logger for AWS.

## Configuring Logger for AWS

Perform the following steps to set a new password for the admin account, and then update the license key.

1. Locate the public or private IP address assigned to the Logger for AWS EC2 instance. Then,  
`ssh -i <private_key> <user>@<aws-assigned-address>`
2. Using sudo access, change the user to 'arcsight' user.
3. Start the application by running the following  
command: `/opt/arcsight/current/arcsight/logger/bin/loggerd start`
4. Execute '`tail /var/log/boot.log`' to view the initial admin password.
5. Set a new password for the admin account. Browse to the web UI at: `https://<aws-assigned-ip-or-hostname>:9000/`

Username: admin

Password: (Note that a password change is forced on first login)

6. Update the license key of the Logger for AWS instance.
7. Continue product configuration as described in the Logger for AWS documentation.

## Next Steps

Send logs to HPE ArcSight Logger and search for events.

1. The ArcSight Logger instance has 2 Syslog SmartConnectors listening on UDP 514 and 515. Configure your devices and applications to send Syslog events to the IP or Hostname of the ArcSight Logger instance.
2. Use ArcSight Logger to search for events.
3. If needed, deploy more SmartConnectors by launching the ArcMC image from the Marketplace.

## Additional Information

For additional information on the use and operation of Logger for AWS, see the HPE ArcSight product documentation, available from HPE ArcSight Product Documentation:

<https://www.protect724.hpe.com/community/arcsight/productdocs>.

You can also reach HPE ArcSight Software Support at: <https://softwaresupport.hpe.com>

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Setup Guide (Logger for AWS 6.2)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [arc-doc@hpe.com](mailto:arc-doc@hpe.com).

We appreciate your feedback!