



Hewlett Packard
Enterprise

HPE Security ArcSight ESM for Azure

Software Version: 6.9.1

Setup Guide

January 20, 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

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

Contents

Launching an Instance of ESM on the Azure Cloud Platform	4
Next Steps	5
Additional Information	6
Send Documentation Feedback	7

Launching an Instance of ESM on the Azure Cloud Platform

HPE ArcSight ESM is available for deployment in Azure Marketplace. It is designed as a virtual appliance containing required operating system and ESM software pre-installed.

This procedure assumes you have an Azure portal account setup.

1. Log in to [Azure Marketplace](#) with your Azure account credentials.
2. Click **New**, and type ArcSight ESM in the search box.
3. Select HPE ArcSight ESM from the search results.
4. Select a Deployment Model and click **Create** button. These are Azure options that do not apply to ESM.
5. Enter basic details about the virtual machine on the next screen such as:
 - Virtual Machine Name: any alphanumeric string)
 - User Name: this **must** be "centos"
 - Password or SSH public key
 - Resource Group: any alphanumeric string
 - Location: select a region from the list

When complete, click **OK**.

6. Choose the size and click **Select**. We recommend DS13 Standard.
7. Optionally, on the next screen, you may change Settings if desired. When complete, click OK.
8. All the inputs will be validated. If the validation is passed, click OK to continue. If it fails, an explanation is provided. Correct the indicated problem and redeploy.
9. On the next screen, accept the Purchase agreement and click OK to start the virtual machine deployment.
10. Once the virtual machine is ready (in the running state), connect via SSH as centos user with the password or ssh key provided during the deployment of this virtual machine.
11. Upon successful SSH login, the ESM First Boot Wizard launches automatically. Complete the ESM configuration as described in Chapter 2, "Installing on an Appliance," in the ESM Installation Guide.
12. Copy your ESM license to the /tmp directory on the virtual machine before you get to the step where you are prompted for the path and file name of the license file. You can access the ArcSight Command Center after configuration wizard completes successfully.

Next Steps

Send logs to HPE ArcSight ESM and search for events.

1. The ArcSight ESM 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 ESM instance.
2. Use the ArcSight Command Center or the ArcSight ESM Console to view events.
3. If needed, deploy more SmartConnectors by launching the ESM AMI.

Additional Information

For additional information on the use and operation of ESM for Azure, 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 (ESM for Azure 6.9.1)

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.

We appreciate your feedback!