opentext™

ArcSight ESM

Software Version: 7.7

ESM Technical Requirements

Document Release Date: January 2024
Software Release Date: January 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2001 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

ArcSight Enterprise Security Manager (ESM) Technical Requirements 4
End of Product Support Notices 4
ESM 7.7 Supported Upgrade Paths, Platforms, and Products 4
Supported Upgrade Paths 4
Supported Platforms and Products 7
Support for Patched and Upgraded Operating Systems 9

Publication Status 10

Send Documentation Feedback 11

ArcSight Enterprise Security Manager (ESM) Technical Requirements

This document describes current platform support for ArcSight Enterprise Security Manager (ESM) and its components. The components include:

- ArcSight Manager
- ArcSight Console
- Correlation Optimized Retrieval and Retention Engine (CORRE)
- ArcSight Command Center
- Active Passive High Availability module

Note: The term **supported** indicates that the product has been sanity-tested on the indicated platform. Micro Focus will accept support calls and address issues with the product and the platform on which it runs.

End of Product Support Notices

For updated end-of-life schedules for all ArcSight products, including ESM, see the Product Support Lifecycle page.

ESM 7.7 Supported Upgrade Paths, Platforms, and Products

Supported upgrade paths, platforms, and products are described below.

Supported Upgrade Paths

Note: These upgrade paths do not apply to ESM with the Active Passive High Availability (APHA) Module. Supported upgrade paths for the APHA module are described in Upgrade Paths for ESM with the Active Passive High Availability (APHA) Module.

For ESM 7.5, 7.6, 7.6.4 and release patches, you can upgrade directly to ESM 7.7.

Upgrade paths for earlier versions are as follows:

- 7.4:
  a. Upgrade to ESM 7.5.
  b. Upgrade to ESM 7.6.
  c. Upgrade to ESM 7.6.4.
  d. Upgrade to ESM 7.7
- 7.3:
  a. Upgrade to ESM 7.5.
  b. Upgrade to ESM 7.6.
  c. Upgrade to ESM 7.6.4.
  d. Upgrade to ESM 7.7
- 7.2 Service Pack 1:
  a. Upgrade to ESM 7.3.
  b. Upgrade to ESM 7.5.
  c. Upgrade to ESM 7.6.
  d. Upgrade to ESM 7.6.4.
  e. Upgrade to ESM 7.7
- 7.0 Patch 1 and Patch 2:
  a. Upgrade to ESM 7.2.
  b. Upgrade to ESM 7.4.
  c. Upgrade to ESM 7.5.
  d. Upgrade to ESM 7.6.
  e. Upgrade to ESM 7.6.4.
  f. Upgrade to ESM 7.7
- ESM 7.0:
  a. Apply ESM 7.0 Patch 2.
  b. Upgrade to ESM 7.2.
  c. Upgrade to ESM 7.4.
  d. Upgrade to ESM 7.5.
  e. Upgrade to ESM 7.6.
  f. Upgrade to ESM 7.6.4.
  g. Upgrade to ESM 7.7

- ESM 6.11, with or without patches:
  a. Upgrade to ESM 7.0 Patch 1.
  b. Upgrade to ESM 7.2.
  c. Upgrade to ESM 7.4.
  d. Upgrade to ESM 7.5.
  e. Upgrade to ESM 7.6.
  f. Upgrade to ESM 7.6.4.
  g. Upgrade to ESM 7.7

Upgrade Paths for ESM with the Active Passive High Availability (APHA) Module

For ESM 7.5, 7.6, 7.6.4 and release patches, you can upgrade directly to ESM 7.7.

Upgrade paths for earlier versions are as follows:

- Version 7.4 of ESM and the APHA module:
  a. Upgrade ESM and the APHA module to version 7.5.
  b. Upgrade ESM and the APHA module to version 7.6.
  c. Upgrade ESM and the APHA module to version 7.6.4.
  d. Upgrade ESM and the APHA module to version 7.7
- Version 7.3 of ESM and the APHA module:
  a. Upgrade ESM and the APHA module to version 7.5.
  b. Upgrade ESM and the APHA module to version 7.6.
  c. Upgrade ESM and the APHA module to version 7.6.4.
  d. Upgrade ESM and the APHA module to version 7.7
- Version 7.2 Service Pack 1 of ESM and the APHA module:
  a. Upgrade ESM and the APHA module to version 7.3.
  b. Upgrade ESM and the APHA module to version 7.5.
  c. Upgrade ESM and the APHA module to version 7.6.
  d. Upgrade ESM and the APHA module to version 7.6.4.
  e. Upgrade ESM and the APHA module to version 7.7
- Version 7.0 of ESM and the APHA module:
  a. Upgrade ESM and the APHA module to version 7.0 Patch 2.
  b. Upgrade ESM and the APHA module to version 7.2.
  c. Upgrade ESM and the APHA module to version 7.4.
  d. Upgrade ESM and the APHA module to version 7.5.

e. Upgrade ESM and the APHA module to version 7.6.
f. Upgrade ESM and the APHA module to version 7.6.4.
g. Upgrade ESM and the APHA module to version 7.7

- Version 7.0 of the APHA module:
  a. Upgrade the APHA module to version 7.2.
  b. Upgrade the APHA module to version 7.4.
  c. Upgrade ESM and the APHA module to version 7.5.
  d. Upgrade ESM and the APHA module to version 7.6.
  e. Upgrade ESM and the APHA module to version 7.6.4.
  f. Upgrade ESM and the APHA module to version 7.7

Supported Platforms and Products

GA date	January 2024
Operating systems and browsers:	
Supported operating systems for software ESM -Active Passive High Availability module	• Red Hat Enterprise Linux (RHEL) 7.9, 8.8, and 9.2 with or without FIPS enabled • Community Enterprise Operating System (CentOS) 7.9 with or without FIPS enabled • SUSE Linux Enterprise Server (SLES) 15 Service Pack 3, with or without FIPS enabled • Rocky Linux 8.8 and 9.2 with or without FIPS enabled
Supported operating systems for software ESM (compact mode and distributed mode) **Note:** In distributed mode, all cluster nodes must be on the same operating system version.	• Red Hat Enterprise Linux (RHEL) 7.9, 8.8, and 9.2 with or without FIPS enabled • Community Enterprise Operating System (CentOS) 7.9 with or without FIPS enabled • SUSE Linux Enterprise Server (SLES) 15 Service Pack 3 and 5, with or without FIPS enabled • Rocky Linux 8.8 and 9.2 with or without FIPS enabled
Supported operating systems for the ArcSight Console	• RHEL 7.9, 8.8, and 9.2 • CentOS 7.9 • SUSE Linux Enterprise Desktop 15 Service Pack 5 • Rocky Linux 8.8 and 9.2 • macOS Monterey, Ventura, Sonoma • Windows Server 2022 • Windows 10 Enterprise (including patches)

Supported browsers for ArcSight Command Center	The latest version of Chrome, Firefox Extended Support Release, or Microsoft Edge (chromium-based only)
Related components:	
Forwarding Connector	8.4.4.9249.0 You can install the Forwarding Connector on any operating system and version that the ESM 7.7 ArcSight Manager supports.
Active Directory (Actor) Model Import Connector	8.4.4.9244.0 This connector supports the following operating systems: • CentOS Linux 7.9 • Microsoft Windows Server 2022 Standard 64-bit • Microsoft Windows Server 2019 Standard 64-bit • SUSE Linux Enterprise Server (SLES) 15 SP 2
Asset Model Import Flex Connector	8.4.4.9245.0 This connector supports the following operating systems: • RHEL 8.6, 8.8, 9.0, 9.1, and 9.2 • Rocky Linux 8.6, and 8.8 • CentOS Linux 7.9 • Microsoft Windows Server 2022 Standard 64-bit • Microsoft Windows Server 2019 Standard 64-bit • SUSE Linux Enterprise Server (SLES) 15 SP 2
ArcSight Platform	2024.1 **Note:** To use Command Center from the ArcSight Platform, ESM and the ArcSight Platform must run the same version of Command Center.
Transformation Hub	3.7.3
Recon	1.5.6
Miscellaneous:	
Federal Information Processing Standards (FIPS)	140-2
Suite B	128-bit and 192-bit
Common access card (CAC)	Yes
Third-party products:	
ServiceNow®	Quebec version ServiceNow API

Support for Patched and Upgraded Operating Systems

We recommend the fully tested operating systems defined above. However, the ArcSight Product Management team approves the use of vendor-supported and newly patched versions of operating systems and minor releases that are not explicitly defined above. For example, we will support minor releases between RHEL 8.6 and RHEL 8.8. Although we might not have tested ArcSight components on a new minor or patched release, we will provide support on a "best effort" basis for ArcSight products and components that you run on these upgraded operating systems.

If we cannot fix or provide a workaround in a timely manner for an issue between the newer OS minor release and an ArcSight component, we might ask you to revert to one of the operating systems listed above until the problem can be fixed or the newer OS minor release level has passed our product testing.

If you choose to run ArcSight components on other platforms or with uncertified configurations, we will provide support until the point that we determine that the root cause is the uncertified platform or configuration. Issues that can be reproduced on the certified platforms will be prioritized and fixed according to standard defect-handling policies.

We do not implicitly support major changes for an operating system, such as a new release for RHEL. As a best practice, the ArcSight product team must test ArcSight functionality on new major operating systems before we list the operating system as supported or certified.

Publication Status

Released: January 2024

Updated: Wednesday, May 22, 2024

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 computer, click the link above and an email window opens with the following information in the subject line:

Feedback on ESM Technical Requirements (ESM 7.7)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!