
Micro Focus Security ArcSight ESM

Software Version: 4.0

ESM Default Content 4.0 Release Notes



Legal Notices

Copyright Notice

© Copyright 2001-2023 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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

| | |
|--|----|
| What's New | 4 |
| Security Threat Monitoring | 4 |
| Threat Intelligence Platform | 4 |
| Updated Content | 6 |
| Security Threat Monitoring | 6 |
| Threat Intelligence Platform | 6 |
| Package Requirements | 8 |
| ESM Requirements | 8 |
| Log Source Requirements | 8 |
| Deployment | 9 |
| Install the 4.0 Package | 9 |
| Uninstallation Process | 10 |
| Verifying the Downloaded Installation Software | 10 |
| PublicationStatus | 11 |
| Send Documentation Feedback | 12 |

What's New

ESM Default Content 4.0's primary focus has been to support [CyberRes Galaxy Threat Acceleration Program \(GTAP\) 2.0](#). The most significant change has been the introduction of 22 additional fields to the Threat Intelligence Platform active lists hosting the real-time IoC information received from the threat-intelligence feed.

 **Important:** ESM Default Content 4.0 has new installation instructions that you can see [here](#).

- [Security Threat Monitoring](#)
- [Threat Intelligence Platform](#)

Security Threat Monitoring

4.0 includes two new rules to help you detect attacks in Windows, Sysmon, and Powershell.

| Rule Name | Tactic/Technique | Description | Log Source | Events Monitored |
|---|--------------------------------|--|-----------------|---|
| Credentials in Group Policy Preferences | Credential Access T1552.006 | Detects attempts on unsecured credentials in Group Policy Preferences (GPP) that allow administrators to create domain policies with embedded credentials. | Windows, Sysmon | Microsoft-Windows-Sysmon:1 Microsoft-Windows-Security-Auditing: 4688 |
| Mark-of-the-Web Bypass Using PowerShell | Defense Evasion T1553.005 | Detects abuse of specific file formats to subvert Mark-of-the-Web (MOTW) controls. | Powershell | Microsoft-Windows-PowerShell: 4104 |

Threat Intelligence Platform

All ten /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/ active lists have been updated with the 22 new GTAP fields to allow more IoC data feed storage. You can see the new fields [here](#). Additionally, 4.0 includes three new dashboards to help you monitor your environment.

What's New

| Dashboard Name | Description | Location |
|---|---|---|
| Data Feed Overview | Allows you to monitor data feeds by attribute type, confidence, and CreatorOrg, as well as the most active threat actors. | /All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview |
| Top Malware and CVE | Allows you to monitor datafeeds sorted by malware, AV signature, and CVE. | /All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Top Malware and CVE |
| TI Confidence Comparison- Open Source vs Galaxy-curated | Allows you to monitor the confidence comparison between CyberRes and open-source TI feeds | /All Dashboards/ArcSight Foundation/Threat Intelligence Platform/TI Confidence Compariso- Open Source vs Galaxy-curated |

4.0 also includes a new rule for the Threat Intelligent Platform.

| Rule Name | Description | Log Source | Events Monitored |
|-----------------------------------|--|--------------------------|------------------|
| Track GTAP Connector Update Count | This rule tracks GTAP connector update count, and write to an active list. | ArcSight Internal Events | agent:050 |

Updated Content

ESM Default Content 4.0 includes updated content for Security Threat Monitoring and Threat Intelligence Platform.

- [Security Threat Monitoring](#)
- [Threat Intelligence Platform](#)

Security Threat Monitoring

The following rules have been updated for Security Threat Monitoring 4.0.

| Tactic/Technique | Rule Name | What Changed |
|------------------------------------|---|--|
| Data Encrypted for Impact T1486 | Possible Ransomware Detected | Fixed a bug related to local variable GetSizeOfList. |
| Data Encrypted for Impact T1486 | Large amounts of file modifications in user directories | Updated aggregation tab. |

Threat Intelligence Platform

In addition to the new fields added to the active list, the following resources have been updated for Threat Intelligence Platform 4.0.

| Resource Type | Name | Location | What Changed |
|---------------|---|--|---|
| Dashboard | Threat Intelligence Security Incidents Overview | /All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Security Incidents Overview | Name change from "Alerts" to "Security Incidents." |
| Dashboard | GTAP Health Status | /All Dashboards/ArcSight Foundation/Threat Intelligence Platform/GTAP Health Status | Added a new chart that shows the TI data feeds and updates hourly. |
| Dashboard | TI Confidence Details | /All Dashboards/ArcSight Foundation/Threat Intelligence Platform/TI Confidence Details | Added a Data Field Overview by Confidence chart that shows confidence categories by high, medium, low, and unknown. |

| Resource Type | Name | Location | What Changed |
|---------------|--|---|--|
| Dashboard | Top Malware Type | /All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Top Malware Type | Added a Top Data Feed Overview by Malware Type chart. |
| Rule | Malware Activity to a Suspicious Address | /All Rules/ArcSight Foundation/Threat Intelligence Platform/Malware/Malware Activity to a Suspicious Address | Updated rule conditions to check that the malware name is not null. |
| Rule | Malware Activity to a Suspicious Domain | /All Rules/ArcSight Foundation/Threat Intelligence Platform/Malware/Malware Activity to a Suspicious Domain | Updated rule conditions to check that the malware name is not null. |
| Rule | High Confidence Alerts to Suspicious Source | /All Rules/ArcSight Foundation/Threat Intelligence Platform/High Confidence Alerts/High Confidence Alerts to Suspicious Source | The confidence value is now extracted directly from a new field: "confidence." |
| Rule | High Confidence Alerts with Suspicious File Hash | /All Rules/ArcSight Foundation/Threat Intelligence Platform/High Confidence Alerts/High Confidence Alerts with Suspicious File Hash | The confidence value is now extracted directly from a new field: "confidence." |
| Active List | Suspicious Indicator Types | /All Active Lists/ArcSight Foundation/Common/Suspicious Indicator Types | Added new indicator types. |

Package Requirements

This package has ESM and Log Source requirements.

ESM Requirements

Requires ArcSight 7.2 or later.

Log Source Requirements

This package requires the following log sources:

| Log Source | Requirement |
|----------------------|---|
| AWS Security Hub | ArcSight Security Hub SmartConnector |
| GTAP | CyberRes Galaxy Threat Acceleration Program 2.0 |
| Linux Audit | ArcSight Linux Audit File SmartConnector |
| Microsoft Office 365 | ArcSight Microsoft 365 Defender SmartConnector |
| Microsoft Windows | ArcSight Windows Connector SmartConnector |

Deployment

The .zip file contains three files:

- package .arb file
- signature .arb file
- Readme

Install the 4.0 Package



Important: ESM Default Content 4.0 has new specific instructions that must be completed to install the new package.

1. [Uninstall /ArcSight Foundation/Threat Intelligence Platform.](#)
 - a. Make sure all resources, especially active lists, have been removed from /ArcSight Foundation/Threat Intelligence Platform.
2. Restart the ESM Manager (/opt/arcsight/services/init.d/arcsight_services stop manager, then start manager).



Note: If you do not restart the Manager, you will receive the following error: :Install Failed: invalid field name: creatorOrg".

3. Go to the ArcSight Console.
4. Click **Packages**.
5. Click **Import**.
6. Select the package .arb from the .zip file.
7. Follow the prompts to import and install this package.
8. After the initial install finishes, right-click **Threat Intelligence Platform** and click **Install Package**.



Note: If you get the error message below during installation, please select "Always skip DrilldownLists" and continue the installation. Some drilldown functions might not work properly.

Error:

/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Top Threat Intelligence Security Incidents by Attacker
Not Enough Privileges
Not enough privileges to modify '/All Drilldown Lists/Attachments/loP7xRXABABCr+s40+xvZQ==/Drilldown List for Top Threat Intelligence Alerts by Attacker

Uninstallation Process

Right-click the package from the ArcSight Console, then select **Uninstall Package**.

Verifying the Downloaded Installation Software

Micro Focus provides a digital public key to enable you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

<https://support.microfocus.com/kb/doc.php?id=7025140>

PublicationStatus

Released: NOT RELEASED

Updated: Monday, March 13, 2023

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 Default Content 4.0 Release Notes (ESM 4.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!