OpenText Enterprise Security Manager

Software Version: 4.7

ESM Default Content 4.7 Release Notes

Document Release Date: June 2025
Software Release Date: June 2025

Legal Notices

Open Text Corporation

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

Copyright Notice

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

What's New

ESM Default Content 4.7 introduces six new detection rules across three MITRE ATT&CK Techniques, strengthening visibility into Initial Access, Defense Evasion, and Lateral Movement Tactics. These rules enhance detection in both network and endpoint environments.

Summary of additions

- Six new detection rules implemented
- MITRE ATT&CK Techniques introduced
  - T1566 - Phishing
  - T1036.005 - Masquerading: Match Legitimate Resource Name or Location
  - T1127.002 - Trusted Developer Utilities Proxy Execution: ClickOnce **(New)**

Security Threat Monitoring

Version 4.7 adds six new rules to the Security Threat Monitoring package, adding rules to the Network Monitoring, Vulnerability Monitoring, and Application Monitoring use cases.

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	DKIM Based Attack Detected	Initial Access (T1566)	Detects DomainKeys Identified Mail (DKIM)-related attacks	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring	ArcSight Categorization
Rule	SPF-Based Attack Detected	Initial Access T1566	Detects Sender Policy Framework protocol (SPF)-related attacks	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring	ArcSight Categorization
Rule	Okta FastPass Phishing Detection	Initial Access T1566	Detects when Okta FastPass prevents a user from authenticating to a phishing website.	/All Rules/ArcSight FoundationSecurity Threat Monitoring/Network Monitoring	Okta

Resource Type	Rule Name	Tactic (Technique)	Description	Rule Path	Data Source
Rule	DMARC Weakness Detected	Initial Access T1566	Detects DMARC protocol-related vulnerabilities.	All Rules/ArcSight Foundation/Security Threat Monitoring/Vulnerability Monitoring	Vulnerability Scanner (Nessus, Qualys)
Rule	Process Executed with Whitespace Special Characters	Defense Evasion (T1036.005)	Detects processes executed with file paths that contain any of the following special characters: U+2000 (En Quad), U+2001 (Em Quad), U+2002 (En Space), and U+200A (Hair Space)	/All Rules/Real-time Rules/Security Threat Monitoring/Application Monitoring	Windows Process Creation Event
Rule	Possible Abnormal Use of ClickOnce	Defense Evasion (T1127.002)	This rule identifies suspicious activity involving ClickOnce applications by detecting the usage of specific command line parameters: dfshim.dll, ShOpenVerbApplication1, and abnormal process name. These parameters could be associated with attempts to circumvent standard application behavior, potentially indicating malicious intent or misuse.	/All Rules/Arcsight Foundation/Security Threat Monitoring/Application Monitoring	Windows Process Creation Event

Deprecated Rules

The legacy detection rule "Juicy-Rotten-Rogue Potato Exploitation" found under the folder “/All Rules/Arcsight Foundation/Security Threat Monitoring/Host Monitoring” has been deprecated due to outdated detection logic and limited relevance in modern environments.

ESM Requirements

Requires OpenText Enterprise Security Manager 7.2 or later.

Log Source Requirements

Security Threat Monitoring and Threat Intelligence Platform require the use of SIEM SmartConnectors.

ArcSight Threat Acceleration Program Connector

Arcsight Threat Acceleration Program Connector is essential for the Threat Intelligence Platform's capabilities.

Other Log Source Requirements

Log Source	Requirement
Amazon Web Services	SmartConnector for Amazon Web Services CloudTrail
Linux Audit	OpenText Linux Audit File SIEM SmartConnector
Microsoft IIS File	SmartConnector for Microsoft IIS File
Microsoft Office 365	OpenText Microsoft 365 Defender SIEM SmartConnector
Microsoft Windows	OpenText Microsoft Windows Connector SIEM SmartConnector

Security Threat Monitoring and Threat Intelligence Platform have rules and other resources that require SmartConnectors to catch and provide information about events. Information about the log sources associated with each rule are listed in the rule's documentation. You can find the relevant SmartConnector in the SmartConnector Grand List (A-Z).

Note: For log sources like IDS, Proxy, and Firewall, there are a range of SmartConnectors available. You can choose the connectors that best suite your environment from the SmartConnector Grand List.

Verifying the Downloaded Installation Software

ArcSight Marketplace has two .zip files for the ESM 4.7 Default Content release:

- Security_Threat_Monitoring4.7.zip
  - Security_Threat_Monitoring4.7.arb
  - ESM4.7DefaultContentReleaseNotes.pdf
  - Security_ThreatMonitoring4.7.arb.sig
- Threat_Intelligence_Platform4.7.zip
  - Threat_Intelligence_Platform4.7.arb
  - ESM4.7DefaultContentReleaseNotes.pdf
  - Threat_Intelligence_Platform4.7.arb.sig

Verifying the Downloaded Installation Software

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

> ✓ **Tip:** Evolving security needs imply the renewal of certificates for the signature verification procedure. To ensure a successful verification of your product signature, download the latest public keys file before proceeding with the verification process (step 1 of the Get the Public Keys procedure).

Visit the following site for information and instructions:

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

Installing and Updating Default Content 4.7

The following section contains instructions for you to install, update, or uninstall your STM and TIP packages.

- Installing STM
- Installing TIP
- Updating STM
- Updating TIP
- Uninstalling the Packages

Installing Security Threat Monitoring

1. Download Security_Threat_Monitoring4.7.zip.
2. Extract the zipped files.
3. Go to the ArcSight Console.
4. Click **Packages**.
5. Click **Import**.
6. Select the corresponding .arb.
7. Follow the prompts to install or update this package.

Installing Threat Intelligence Platform

Installing Threat Intelligence Platform 4.7

1. Download Threat_Intelligence_Platform4.7.zip.
2. Extract the zipped files.
3. Go to the ArcSight Console.
4. Click **Packages**.
5. Click **Import**.
6. Select the corresponding .arb.
7. Follow the prompts to import and install this package.

Upgrading Security Threat Monitoring

Important: If you previously customized standard resources in the resource's original location, back up the resources to an .arb file (exclude related resources) before you upgrade. If you copied the resources to a custom group and then customized them, the upgrade does not impact the custom group.

1. Download Security_Threat_Monitoring4.7.zip.
2. Extract the zipped files.
3. Go to the ArcSight Console.
4. Click **Packages**.
5. Click **Import**.
6. Select the corresponding .arb.
7. Follow the prompts to install or update this package.

Upgrading Threat Intelligence Platform

This section contains *two* sets of instructions for updating the Threat Intelligence Platform 4.7 package. Choose the option that applies to you.

> **Important:** Customizations to the Threat Intelligent Platform package (TIP) v3.x to v4.x are not supported.
>
> Export any custom packages created for TIP v3.x and then delete the original. This allows the upgrade process to cleanly uninstall TIP v3.x package.
>
> Do not import custom packages created for TIP v3.x after the upgrade, as they can create resource conflicts with new version of Threat Intelligent Platform. You can manually add your customizations back once this upgrade is complete.

- Updating TIP version 3.x to 4.7
- Updating TIP version 4.0 to 4.7

Updating TIP version 3.x to 4.7

1. Uninstall /ArcSight Foundation/Threat Intelligence Platform.

   Make sure all resources, especially active lists, have been removed from /ArcSight Foundation/Threat Intelligence Platform.

   Active Lists must be deleted manually since they might not uninstall automatically for many reasons like being part of other packages. You can find them under /All Active Lists/ArcSight Foundation/Threat Intelligence Platform.
2. Stop the ESM Manager, `/opt/arcsight/services/init.d/arcsight_services stop manager`.
3. Restart the manager.

   > **Note:** If you do not restart the Manager, you will receive the following error: :Install Failed: invalid field name: creatorOrg".
4. Download Threat_Intelligence_Platform4.7.zip.
5. Extract the zipped files.
6. Go to the ArcSight Console.
7. Click **Packages**.
8. Click **Import**.
9. Select the corresponding .arb.
10. Follow the prompts to install this package.

11. 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/IoP7xRXABABCrr+s40+xvZQ==/Drilldown List for Top Threat Intelligence Alerts by Attacker

Updating TIP version 4.0 to 4.7

1. Download Threat_Intelligence_Platform4.7.zip.
2. Extract the zipped files.
3. Go to the ArcSight Console.
4. Click **Packages**.
5. Click **Import**.
6. Select the corresponding .arb.
7. Follow the prompts to import and install this package.

Important: All Threat Intelligence Platform resources have been rebranded from Galaxy Threat Acceleration Program (GTAP) to ArcSight Threat Acceleration Program (ATAP) with the exception of the column names in these active lists:

- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Addresses List
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain List
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email List
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash List
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL List
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Additional Suspicious Addresses
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform//Additional Suspicious Domain
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Additional Suspicious Email
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Additional Suspicious Hash
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Additional Suspicious URL
- /All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Track ATAP Connector Type

Uninstalling the Packages

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