opentext™

ArcSight ESM

Software Version: 4.4

ESM Default Content 4.4 Release Notes

Document Release Date:
Software Release Date:

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

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 4.4 adds new content to the Security Threat Monitoring package to help you monitor your Windows, Linux, Google, and Amazon environments.

Security Threat Monitoring

4.4 includes six new rules to help you detect unwanted processes, Wi-Fi and device driver discovery, and Network Provider DLL modifications.

Resource Type	Rule Name	Technique	Description	Location	Log Source	Events Monitored
Rule	Suspicious Powercfg Execution To Change Lock Screen Timeout	Power Settings T1653	Detects suspicious powercfg execution to change lock screen timeout.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Suspicious Powercfg Execution To Change Lock Screen Timeout	Windows	Microsoft-Windows-Security-Auditing: 4688
Rule	Potential Distributed DoS	Network Denial of Service T1498	Detects potential Distributed Denial of Service (DDoS) activity.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/Potential Distributed DoS	Snort ArcSight Categorization	N/A

Resource Type	Rule Name	Technique	Description	Location	Log Source	Events Monitored
Dashboard	DoS Activity	Network Denial of Service T1498	Provides the relationship between attacker and target machines and ports as they appear in DoS attack events. **Note:** Before running this dashboard, enable the data monitors which are under All Data Monitors/ArcSight Foundation/Security Threat Monitoring/DoS Activity.	/All Dashboards/Security Threat Monitoring/Network Monitoring/DoS Activity	Snort ArcSight Categorization	N/A
Use Case	DoS Activity	Network Denial of Service T1498	Provides resources to monitor DoS activity reported by ArcSight Connectors based on ArcSight categorization.	All Use Cases/ArcSight Foundation/Security Threat Monitoring/Network Monitoring	Snort ArcSight Categorization	N/A
Rule	Logs Enumerated in Windows	Log Enumeration T1654	Detects attempts to enumerate logs on a victim host.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Logs Enumerated in Windows	Windows PowerShell Sysmon	PowerShell: 800 Microsoft-Windows-PowerShell: 4104 Microsoft-Windows-Security-Auditing: 4688 Microsoft-Windows-Sysmon: 1

Resource Type	Rule Name	Technique	Description	Location	Log Source	Events Monitored
Rule	Google Cloud Services Accessed Remotely	Remote Services T1021	Detects possible adversary connections to available cloud services (in this case Google Cloud) through the Web console or through the cloud command line interface to perform anomalous activity.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Cloud Monitoring/Google Cloud Services Accessed Remotely	Google Cloud - Security Command Center	N/A
Rule	Cloud Services Accessed Remotely	Remote Services T1021	Detects possible adversary connections to available cloud services through the Web console or through the cloud command line interface to perform anomalous activity.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Cloud Monitoring/Cloud Services Accessed Remotely	Windows PowerShell	Microsoft-Windows-PowerShell: 4104 PowerShell: 800
Rule	Cloud Administration Commands Executed	Cloud Administration Command T1651	Detects possible abuse of cloud management services by adversaries to execute commands within virtual machines or hybrid-joined devices.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Cloud Monitoring/Cloud Administration Commands Executed	Amazon - Cloud Trail Logs	N/A

Updated Content

ESM Default Content 4.4 includes updated content for Security Threat Monitoring.

Security Threat Monitoring

The following rules have been updated for Security Threat Monitoring 4.4.

Tactic/Technique	Rule Name	What Changed
Discovery T1217-Browser Information Discovery	Browser Information Discovery	Name change. Browser Bookmark Discovery has been renamed to Browser Information Discovery
Exfiltration T1567.003	Possible Exfiltration to Text Storage Sites	Improved rule performance.

ESM Requirements

Requires ArcSight ESM 7.2 or later.

Log Source Requirements

Security Threat Monitoring and Threat Intelligence Platform require the use of ArcSight 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	ArcSight Linux Audit File SmartConnector
Microsoft IIS File	SmartConnector for Microsoft IIS File
Microsoft Office 365	ArcSight Microsoft 365 Defender SmartConnector
Microsoft Windows	ArcSight Microsoft Windows Connector 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 4.4 Default Content release:

- Security_Threat_Monitoring4.4.zip
  - Security_Threat_Monitoring4.4.arb
  - ESM4.4DefaultContentReleaseNotes.pdf
  - Security_ThreatMonitoring4.4.arb.sig
- Threat_Intelligence_Platform4.4.zip
  - Threat_Intelligence_Platform4.4.arb
  - ESM4.4DefaultContentReleaseNotes.pdf
  - Threat_Intelligence_Platform4.4.arb.sig

Verifying the Downloaded Installation Software

Open Text provides a digital public key to enable you to verify that the signed software you received is indeed from Open Text 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 4.4

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

Installing Security Threat Monitoring 4.4

1. Download Security_Threat_Monitoring4.4.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 4.4

1. Download Threat_Intelligence_Platform4.4.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 4.4

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_Monitoring4.4.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 4.4 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 4.4

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_Platform4.4.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 4.4

1. Download Threat_Intelligence_Platform4.4.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**.

PublicationStatus

Released: NOT RELEASED

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 4.4 Release Notes (ESM 4.4)

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!