



ArcSight ESM

Software Version: 4.5

ESM Default Content 4.5 Release Notes

Document Release Date: July 2024

Software Release Date: July 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 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

- What's New 4
- Updated Content 5
 - ArcSight Foundation Package 5
- ESM Requirements 6
- Log Source Requirements 7
 - ArcSight Threat Acceleration Program Connector 7
 - Other Log Source Requirements 7
- Verifying the Downloaded Installation Software 8
 - Verifying the Downloaded Installation Software 8
- Installing and Updating Default Content 4.5 9
- Installing Security Threat Monitoring 10
- Installing Threat Intelligence Platform 11
 - Installing Threat Intelligence Platform 4.5 11
- Upgrading Security Threat Monitoring 12
- Upgrading Threat Intelligence Platform 13
 - Updating TIP version 3.x to 4.5 13
 - Updating TIP version 4.0 to 4.5 14
- Uninstalling the Packages 16
- Publication Status 17
- Send Documentation Feedback 18

What's New

ESM Default Content 4.5 adds five new active lists that have a new, optional customer name and customer URI fields optimized for MSSP users to support entries tailored to specific customers. These active lists are located in the ArSight Foundation/Common folder.

The new fields help MSSP environments distinguish between similar IDs and usernames across multiple customers. For example, Customer 1 and Customer 2 are concerned with suspicious countries. With the new customer field in the Risky Countries active list, MSSP users can use the new field to specify which countries each customer would like to monitor.

These upgraded active lists have similar names to their predecessors. However, the original active lists have been renamed to show their deprecated status, and they will be removed completely in the future ESM Default Content 4.7 release. This allows time for users to move any customizations to the new active lists.



Note: Any content included in the Default Content packages that required the original active lists, has been updated to require the new active lists. Users only need to ensure that any personal customizations, such as self-built rules that require the original active lists, are switched to require the new active lists before the Default Content 4.7 release. See [Updated Content](#) for a list of Rules that have been updated to depend on the new active lists.

Original Active List (4.4)	Deprecated Active List (4.5)	New Active List (4.5)
Default Accounts	Default Accounts Deprecated	Default User Accounts
Privilege User Account	Privilege User Account Deprecated	Privileged User Accounts
Privilege User Groups	Privilege User Groups Deprecated	Privileged User Groups
Suspicious Countries	Suspicious Countries Deprecated	Risky Countries
Uncommonly Used Ports	Uncommonly Used Ports Deprecated	Uncommon Ports

Updated Content

ESM Default Content 4.5 includes updated rules in the ArcSight Foundation package.

ArcSight Foundation Package

The following rules have been updated to depend on the new active lists instead of the original active lists.

Active List Name (New)	Dependent Rule Name	Rule Location
Risky Countries	Egress Communications to Suspicious Country	/All Rules/ArcSight Foundation/Security Threat Monitoring/Perimeter Monitoring
Privileged User Groups	A Member was Added into a Privileged Group	/All rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring
Privileged User Accounts	SharePoint Activity by Privileged User	/All rules/ArcSight Foundation/Security Threat Monitoring/Cloud Monitoring
Privileged User Accounts	Consecutive Unsuccessful Logins to Administrative Account	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring
Privileged User Accounts	Privileged Account Locked Out	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring
Default User Accounts	Default Account Enabled	All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring

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 4.5 Default Content release:

- Security_Threat_Monitoring4.5.zip
 - Security_Threat_Monitoring4.5.arb
 - ESM4.5DefaultContentReleaseNotes.pdf
 - Security_ThreatMonitoring4.5.arb.sig
- Threat_Intelligence_Platform4.5.zip
 - Threat_Intelligence_Platform4.5.arb
 - ESM4.5DefaultContentReleaseNotes.pdf
 - Threat_Intelligence_Platform4.5.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 4.5

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_Monitoring4.5.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 4.5

1. Download [Threat_Intelligence_Platform4.5.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_Monitoring4.5.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 4.5 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 4.5](#)
- [Updating TIP version 4.0 to 4.5](#)

Updating TIP version 3.x to 4.5

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_Platform4.5.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/loP7xRXABABCr+s40+xvZQ==/Drilldown List for Top Threat Intelligence Alerts by Attacker

Updating TIP version 4.0 to 4.5

1. Download [Threat_Intelligence_Platform4.5.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**.

Publication Status

Released: July 2024

Updated: Friday, July 12, 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 Default Content 4.5 Release Notes (ESM 4.5)

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!