opentext™

OpenText ArcSight ESM

Software Version: 4.3
The following line is optional. Use it for PDF targets if there are different versions of the

ESM Default Content 4.3 Release Notes

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

Acknowledgements

REQUIRED: Do not change the name of your copy of the `_MFc_AcknowledgementsSnip.flsnp` file. Copy this file to your `<FlareProject>/Content/Resources/Snippets/Required/_MFc_AcknowledgementsSnip.flsnp`.

Adding text to this section is optional. If the product team receives permission from the Legal Department to acknowledge third-party software used in the product, they must let you know of that permission.

If the product team receives permission to publish the *full* third-party licenses, they must give you the text, and *you must create a separate document for it*. If you are asked to publish the licenses for the open source and third-party software used in your product, use a template from the Information Engineering web site (Word, html, or Flare). See the templates for more instructions about publishing such licenses.

If your product team receives instructions *to provide Acknowledgements*:

1. Open this Snippet file.
2. In Flare's XML Editor, right-click the [h3] and the last [p] three blocks in this snippet file.
3. Select the Conditions menu item.
4. Remove the `_MF_Conditions.Internal`.
5. Modify the example Acknowledgements text to meet the requirements for the licenses of any open source or third-party software in the product.

   Tip: Perhaps the text you need already exists in another file if you are migrating to the Standard Flare File-Set.

If your product *does not require any Acknowledgements*, leave the heading and text in this file set to `_MF_Conditions.Internal`.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes code licensed from RSA Data Security.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information

Contact Information, continued

Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

What's New 5

ESM Requirements 18

Downloading and Verifying the Installation Files 19

Publication Status 20

Contact Information 20

Send Documentation Feedback 21

What's New

ArcSight Compliance Pack for NERC 24.2 (1.0) for ESM supports latest version of NERC standards. New Active Channels, Active Lists, Dashboards, Filters, and Rules have been added to help monitor compliance of CIP 012, CIP 013, and CIP 014, in addition to existing CIPs.

In addition to ESM, this new package is also a requirement for Compliance Insight Pack for Recon, which is being released as part of the ArcSight Platform 24.2. There are three NERC Compliance Overview dashboards in Recon NERC that draw on correlation events that are created by the ArcSight Compliance Pack for NERC for ESM.

Details of the new resources are below:

Resource Type	NERC Control Number	Resource Name	Description	Location
Dashboard	N/A	Risk Score Overview Dashboard	Monitors the risk score to every PCI requirement. Additionally, you can drilldown to viewers that show all NERC correlation trigger events. From there you can drilldown further by: • Hostname • IP Address • User • Hostname and NERC CIP • IP Address and NERC CIP • User and NERC CIP • Specific NERC CIP • Specific Rule Name • Agent Severity • Specific Customer • Source IP	/All Dashboards/ArcSight Solutions/NERC/CIPS Overview/Risk Score Overview Dashboard

Resource Type	NERC Control Number	Resource Name	Description	Location
			• Asset Location • Asset Location and CIP	
Rule	CIP-007	Anti-Virus Failed Update	Detects anti-virus update failures.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/Anti-Virus Failed Update
Rule	CIP-007	Default Account Detected	Detects default accounts.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/Default Account Detected
Rule	CIP-007	Default Password Detected	Detects default passwords.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management /Default Password Detected
Rule	CIP-007	Minimum Password History Set to Less than Policy Standard (default 5)	Detects when minimum password history is set to less than standard policy defined in the organization. The default is 5.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/Minimum Password History Set Less than Policy Standard
Rule	CIP-007	Minimum Password Length Changed to Less than Policy	Detects whenever the minimum password length is set to less than the standard policy defined in the organization.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/Minimu

Resource Type	NERC Control Number	Resource Name	Description	Location
		Standard		m Password Length Set Less than Policy Standard
Rule	CIP-007	Password Spray Attack	Detects password spray attacks on Windows systems.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/Password Spray Attack
Rule	CIP-007	Shellcode Execution Detected	Detects shellcode execution.	/All Rules/ArcSight Solutions/NERC/CIP-007 System Security Management/Shellcode Execution Detected
Dashboard	CIP-008	Threat Overview	Provides a geo overview of threat activity reported on the organization.	/All Dashboards/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/Threat Overview
Filter	CIP-008	SQL Injection Attack Detected	Identifies SQL Injection attacks.	/All Filters/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/SQL Injection Attack Detected
Rule	CIP-008	Attacks Increased Exponenti	Detects exponential increases of attacks and suspicious events.	/All Rules/ArcSight Solutions/NERC/CIP-008 Incident

Resource Type	NERC Control Number	Resource Name	Description	Location
		ally in less than 10 Minutes		Reporting and Response Planning/Attacks Increased Exponentially in less than 10 minutes
Rule	CIP-008	Exploit Executed on Database Asset	Detects exploits executed against database assets. To trigger this rule, the database assets should be categorized with this category: Asset Categories/Site Asset Categories/Application/Type/Database.	/All Rules/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/Exploit Executed on Database Asset
Rule	CIP-008	High Risk Events Increased Exponentially in less than 10 Minutes	Detects exponential increases of high risk events. Before deploying this rule make sure the High Risk Events per 10 Minutes data monitor is enabled.	/All Rules/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/High Risk Events Created Increased Exponentially in less than 10 Minutes
Use Case	CIP-008	Threat Overview	Provides geographical view of events that identified as threats against the organization.	/All Use Cases/ArcSight Solutions/NERC/Threat Overview
Rule	CIP-008	Multiple MITRE ATT&CK Techniques Detected on the	Triggers when multiple MITRE techniques are detected on the same asset in a short period of time.	/All Rules/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/Multiple

Resource Type	NERC Control Number	Resource Name	Description	Location
		Same Asset		MITRE ATT&CK Techniques detected on the Same Asset
Rule	CIP-008	SQL Injection Attack Detected	Detects SQL Injection attacks.	/All Rules/ArcSight Solutions/NERC/CIP-008 Incident Reporting and Response Planning/SQL Injection Attack Detected
Active Channel	CIP-010	Removable Media Activity	Looks for events that indicate a removable media activity.	/All Active Channels/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability Assessments/Removable Media Activity
Active List	CIP-010	Missing Security Patches	Stores all the missing security patches reported on the environment. By default, the active list TTL is set to 30 days, which means it will hold all of the unfixed security patches until 30 days. **Note:** Users can manually remove the fixed issues or set a custom reasonable TTL so that the removal is automated.	/All Active Lists/ArcSight Solutions/NERC/Missing Security Patches
Active List	CIP-010	Vulnerability	Stores all the assets that scanned by vulnerability	All Active Lists/ArcSight

Resource Type	NERC Control Number	Resource Name	Description	Location
		Scanned Assets	scanners on the last x days. The default is 90 days. Do not manually update this active list.	Solutions/NERC/Vulnerability Scanned Assets
Rule	CIP-010	Anti-Virus Software Disabled	Detects when anti-virus software is disabled.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability Assessments/Anti-Virus Software Disabled
Filter	CIP-010	SQL Injection Vulnerability Detected	Identifies SQL Injection vulnerabilities	/All Filters/ArcSight Solutions/NERC/CIP-010 Configuration Change management and vulnerability Assessments/SQL Injection Vulnerability Detected
Rule	CIP-010	Asset not Scanned for Longer than Policy Standard	Detects when an entry expires out of the referenced active list, signifying that asset didn't scanned within the prescribed time. Time limit is defined by the TTL in the active list (default 90 days). Before deploying this rule make sure the Asset Scanned rule is enabled and	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability Assessments/Asset not Scanned for Longer than Policy Standard

Resource Type	NERC Control Number	Resource Name	Description	Location
			deployed.	
Rule	CIP-010	Asset Scanned	Detects vulnerability scans against a specific asset and adds the asset to the active list.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability Assessments/Asset Scanned
Rule	CIP-010	Database Vulnerabilities	Detects database vulnerabilities. Note: Before deploying this rule, make sure your database assets are categorized within this category: /All Asset Categories/Arcsight Solutions/Compliance Insight Package/Application/Type/Database	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability Assessments/Database Vulnerabilities
Rule	CIP-010	Removable Media Plugged In Multiple Assets in Short Period of Time	Detects removable media plugged into multiple assets in a short period of time.	/All Rules/ArcSight Solutions/NERC/CIP-010Configuration Change Management and Vulnerability Assessments/Removable Media Plugged In Multiple Assets in Short Period of Time
Rule	CIP-010	Security Patch Not Fixed	Triggers when security patch released but not fixed in the system is detected.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change

Resource Type	NERC Control Number	Resource Name	Description	Location
			In order to make this rule work, please ensure that the rule "Security Patch Missing" is present and enabled.	Management and Vulnerability Assessments/Security Patch Not Fixed
Rule	CIP-010	SQL Injection Vulnerabilities	Detects SQL Injection vulnerabilities.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability Assessments/SQL Injection Vulnerabilities
Rule	CIP-010	USB Rubber Ducky Detected	Triggers when rubber ducky USBs are detected.	/All Rules/ArcSight Solutions/NERC/CIP-010 Configuration Change Management and Vulnerability Assessments/USB Rubber Ducky Detected
Use Case	CIP-010	SQL Injection	Provides information about SQL injection vulnerabilities and attacks.	/All Use Cases/ArcSight Solutions/NERC/SQL Injection
Rule	CIP-011	Encrypted Communication Information Leaks	Detects encrypted communication leaks on the network.	/All Rules/ArcSight Solutions/NERC/CIP-011 Information Protection/Encrypted Communication Information Leaks
Active Chann	CIP-012	Audit Data Tampered	Shows a real-time feed of events with modified audit	/All Active Channels/ArcSight

Resource Type	NERC Control Number	Resource Name	Description	Location
el		Events	data.	Solutions/NERC/CIP-012 Communications between Control Centers/Audit Data Tampered Events
Filter	CIP-012	Assets in Control Centers	Selects events showing unauthorized data access to assets in control centers.	/All Filters/ArcSight Solutions/NERC/CIP-012 Communications between Control Centers/Assets in Control Centers
Filter	CIP-012	Data Modification	Selects events with data modification.	/All Filters/ArcSight Solutions/NERC/CIP-012 Communications between Control Centers/Data Modification
Filter	CIP-012	Unauthorized Data Access	Identifies events with unauthorized data access during its transfer between the control centers.	/All Filters/ArcSight Solutions/NERC/CIP-012 Communications between Control Centers/Unauthorized Data Access
Rule	CIP-012	Data Modified During Transfer between Control Centers	Detects data modification during its transfer between the control centers.	/All Rules/ArcSight Solutions/NERC/CIP-012 Communications between Control Centers/Data Modified During Transfer between Control Centers

Resource Type	NERC Control Number	Resource Name	Description	Location
Rule	CIP-012	Unauthorized Data Access during Transfer between Control Centers	Detects any unauthorized data access during its transfer between the control centers.	/All Rules/ArcSight Solutions/NERC/CIP-012 Communications between Control Centers/Unauthorized Data Access during Transfer between Control Centers
Use Case	CIP-012	Data Transfer between Control Centers	Provides the all resources of data transfer between control centers.	/All Use Cases/ArcSight Solutions/NERC/Data Transfer Control Centers
Dashboard	CIP-012	CIP-012 Overview	Displays high-level information around NERC standard CIP-012.	ArcSight/Solutions/NERC/CIPS Overview
Data Monitor	CIP-012	Last 20 Rules Fired	Displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-012 Overview/
Data Monitor	CIP-012	Top 20 Targets in Rule Firings	Displays which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-012 Overview/
Data Monitor	CIP-012	Rules Attackers and Targets	Shows attacker-target pair relationships for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-012 Overview/
Data Monitor	CIP-012	CIP-012 Most Fired	Shows the rule that fired most in CIP-012 in the last	/All Data Monitors/ArcSight

Resource Type	NERC Control Number	Resource Name	Description	Location
		Rule Top 20 Rules Fired	hour.	Solutions/NERC/CIPS Overview/CIP-012 Overview/
Data Monitor	CIP-012	Top 20 Rules Fired	Displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-012 Overview/
Rule	CIP-013	Integrity Check Failed in Systems	Detects failed integrity checks in the systems.	/All Rules/ArcSight Solutions/NERC/CIP-013 Supply Chain Risk Management/Integrity Check Failed in Systems
Rule	CIP-013	Unauthorized Access to Applications by a Third-Party	Detects any unauthorized access to applications by third party vendors.	/All Rules/ArcSight Solutions/NERC/CIP-013 Supply Chain Risk Management/Unauthorized Access to Applications by a Third-Party
Rule	CIP-013	Updates and Patches Failed in Systems	Detects when the latest patches or updates are not installed or failed.	/All Rules/ArcSight Solutions/NERC/CIP-013 Supply Chain Risk Management/Updates and Patches Failed in Systems
Dashboard	CIP-013	CIP-013 Overview	Displays high-level information around NERC standard CIP-013.	ArcSight/Solutions/NERC/CIPS Overview
Data	CIP-013	Last 20	Displays a graphic	/All Data

Resource Type	NERC Control Number	Resource Name	Description	Location
Monitor		Rules Fired	distribution of the last 20 correlation rules fired from this section.	Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-013 Overview/
Data Monitor	CIP-013	Top 20 Targets in Rule Firings	Displays which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-013 Overview/
Data Monitor	CIP-013	Rules Attackers and Targets	Shows attacker-target pair relationships for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-013 Overview/
Data Monitor	CIP-013	CIP-013 Most Fired Rule	Shows the rule that fired most in CIP-013 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-013 Overview/
Data Monitor	CIP-013	Top 20 Rules Fired	Displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-013 Overview/
Dashboard	CIP-014	CIP-014 Overview	Displays high-level information around NERC standard CIP-014.	ArcSight/Solutions/NERC/CIPS Overview
Data Monitor	CIP-014	Last 20 Rules Fired	Displays a graphic distribution of the last 20 correlation rules fired from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIPS Overview/CIP-014 Overview/
Data	CIP-014	Top 20	Displays which targets are	/All Data

Resource Type	NERC Control Number	Resource Name	Description	Location
Monitor		Targets in Rule Firings	most frequently involved in rule firings for that section. This may reveal a trend about certain targets.	Monitors/ArcSight Solutions/NERC/CIP S Overview/CIP-014 Overview/
Data Monitor	CIP-014	CIP-014 Most Fired Rule	Shows the rule that fired most in CIP-014 in the last hour.	/All Data Monitors/ArcSight Solutions/NERC/CIP S Overview/CIP-014 Overview/
Data Monitor	CIP-014	Rules Attackers and Targets	Shows attacker-target pair relationships for the various rule firings from this section.	/All Data Monitors/ArcSight Solutions/NERC/CIP S Overview/CIP-014 Overview/
Data Monitor	CIP-014	Top 20 Rules Fired	Displays a graphic distribution of the 20 most frequently firing correlation rules of this section.	/All Data Monitors/ArcSight Solutions/NERC/CIP S Overview/CIP-014 Overview/

ESM Requirements

Requires ArcSight ESM 7.2 or later.

Downloading and Verifying the Installation Files

To download and verify the signature of your downloaded files:

1. Log in to the host where you want to begin the installation process.
2. Change to the directory where you want to download the installer files.
3. Download the product solution package .arb file: ArcSight-ComplianceInsightPackage-NERC.1.0.0.0.47.arb. from the OpenText Downloads website along with their associated signature files (*.sig).

   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).

   Open Text provides a digital public key that is used to verify that the software you downloaded from the Open Text software entitlement site is indeed from Open Text and has not been tampered with by a third party. For more information and instructions on validating the downloaded software, visit the Open Text Code Signing site. If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please contact Open Text Customer Support.
4. Begin the installation.

Publication Status

Released: June 5, 2024

Updated: Tuesday, June 4, 2024

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact OpenText Customer Care.

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 4.3 Release Notes (ESM 4.3)

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!