



ArcSight Compliance Insight Package GDPR

Software Version: 1.0.0.1

Solutions Guide for ArcSight Compliance Insight Package

Document Release Date: October 2023

Software Release Date: October 2023

Contents

Solutions Guide for ArcSight Compliance Insight Pack for NERC	2
Additional Documentation	3
Contact Information	3
About this Compliance Insight Pack	4
How Events Flow to this Compliance Insight Pack	4
Supported Devices	5
Adding and Removing the Compliance Pack	6
Downloading this Pack	6
Installation	6
Adding Content	6
Uninstalling	6
Removing Dashboard Content	6
Viewing Dashboard Details	7
Known Issues	7
Issue with Report Formatting	7
Publication Status	7
Send Documentation Feedback	8
Additional Documentation	9

Solutions Guide for ArcSight Compliance Insight Pack for NERC

Version 1.0.0.0

To use this compliance pack, you must have, at a minimum, either ArcSight Platform 24.2 with Recon deployed or the Log Management & Compliance service in ArcSight SaaS.

The [North American Electric Reliability Corporation \(NERC\) Critical Infrastructure Protection](#) sets the standards for monitoring, detecting, and responding to various cyberattacks and threats to the electric power industry to ensure the reliability and

security of the bulk power industry. NERC standards require that owners, operators, and users of bulk power systems in the United States and Canada comply with NERC standards.

To help you comply or prove compliance with NERC, we provide the **Compliance Insight Pack for NERC**. This Solutions Guide is designed to help you understand and add the NERC Compliance Insight Pack to your ArcSight Platform instance.

- [About this Compliance Insight Pack](#)
- [Adding and Removing the Compliance Insight Pack](#)
- [Viewing Dashboard and Report Details](#)
- [Known Issues](#)

Additional Documentation

The [ArcSight Platform documentation library](#) includes the following resources:

- ***User's Guide for ArcSight Platform***, which is embedded in the product to provide both context-sensitive Help and conceptual information. In the guide, you can find descriptions of the dashboards and reports that come with this compliance pack.
- ***Administrator's Guide for ArcSight Platform***, which contains installation, user, and deployment guidance for the ArcSight software products and components that you deploy in the containerized platform.

Contact Information

We designed this product in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope that you continue to help us ensure that our products meet all your needs.

The documentation for this product is available on the Documentation website in HTML and PDF formats. If you have suggestions for documentation improvements, click **comment** or **support** on this topic at the bottom of any page in the HTML version of the documentation posted at the [ArcSight Platform Documentation](#) page or the documentation pages for the included products.

We want to hear your comments and suggestions about this document and the other documentation included with this product. You can use the **comment** or **support** 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 [Open Text Customer Care](#).

About this Compliance Insight Pack

Open Text solutions help manage and protect your bulk power system in accordance with NERC enabling you to grow your business with confidence. The Compliance Insight Package (CIP) for NERC, coupled with Recon and optimized to work with ESM events, provides a security framework for monitoring, detecting, and responding to various cyber attacks and threats using the Defense Monitoring in Depth Model. This CIP also helps satisfy auditor expectations and to demonstrate compliance with the NERC standards.

The CIP for NERC can assist you in complying with the NERC CIP Standards, by:

- Providing an overview of the current status of the organization's infrastructure with quick access to alert information
- Monitoring and notifying when potentially hazardous events happen
- Providing real-time monitoring of risks and threats by correlating security events
- Monitoring actions, operations and processes on the network
- Displaying security events graphically which allows analysts to quickly analyze situations
- Tracking potentially harmful users and machines
- Adhering to security policies and best practices
- Monitoring of vulnerabilities, and configuration changes on critical BES Cyber assets

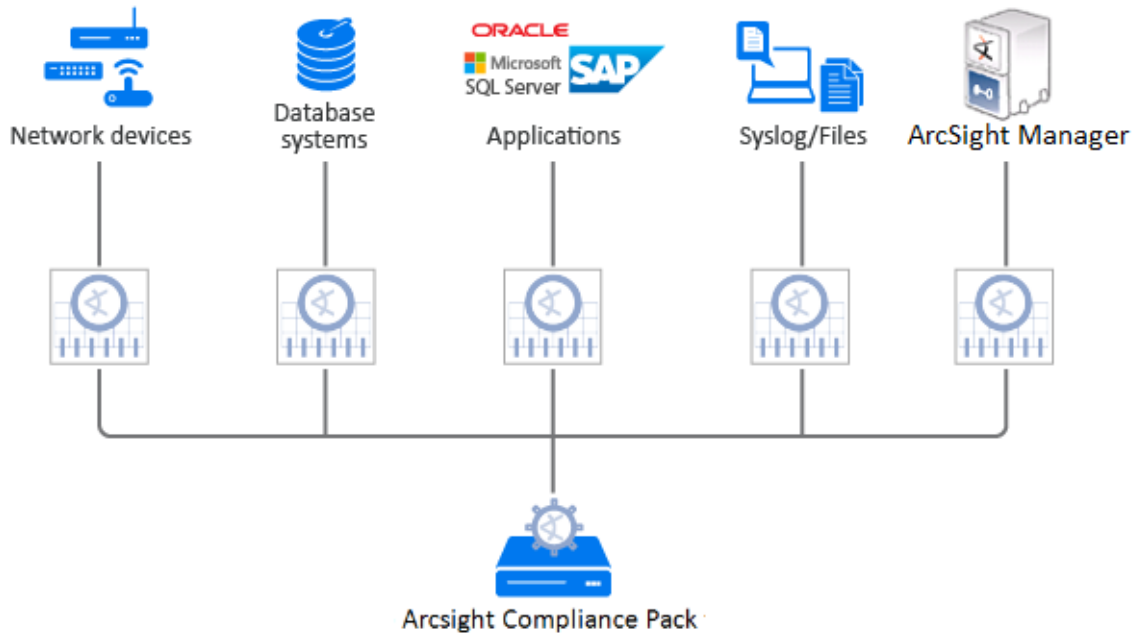
For more information on the available dashboards and reports in this compliance pack, see the Help in the ArcSight Platform. If you have enabled multi-tenancy for your system, you must first choose your tenant before you access the content. To access the content, select Reports > Portal > Repository > Data Compliance > NERC.

How Events Flow to this Compliance Insight Pack

The dashboards available with this ArcSight Compliance Insight Pack operate on events in Common Event Format (CEF), which is an industry standard for the interoperability of event or log-generating devices. CEF events can come from a device that is already configured to post events in CEF. For devices in your network that are not already CEF-ready, the events must run through an ArcSight SmartConnector. Some dashboards, such

as those under the CIP Overview dashboard, visualize ESM correlation Alerts, which must be forwarded from ESM through the ArcSight Forwarding Connector.

For more information about CEF events and how they are used, see the [Administrator's Guide for ArcSight Platform](#).



Supported Devices

The following devices could generate events used by this compliance pack.

- Anti-virus solutions and EDR products
- Databases
- Content Security and Web Filtering systems
- Operating systems
- Physical Security systems
- Host and network-based IDS
- Firewalls
- Wireless systems
- Vulnerability and assessment tools

Adding and Removing the Compliance Pack

This section describes adding and removing the compliance pack.


Downloading this Pack

To purchase this pack, please contact your account or sales representative.

After you purchase this pack, you can download the package from the [Software Licenses and Downloads \(SLD\)](#) portal. Log in to the portal using your active service contract ID.

Installation

Adding Content

1. Select **Reports > Content**.
2. Click the **Import Asset**  icon.
3. Select the zip file for the compliance pack from the stored location.
4. Click **Next**.
5. Follow the prompt to import and continue with the installation.
6. To verify the installation is complete, locate the compliance pack folder under the Data Compliance folder.

Uninstalling

Removing Dashboard Content

1. Select **Dashboards > Portal**.
2. Select **Repository > Data Compliance Content**.
3. Select the content, such as **NERC**, right-click, and select **Delete**.
A confirmation pop-up window displays.
4. Click **OK**.

Viewing Dashboard Details

For more information on the available dashboards and reports in this compliance pack, see the *Help* in the ArcSight Platform or "[Ensuring NERC Compliance](#)" in the *User's Guide for the ArcSight Platform*.

Known Issues

We are currently researching the following issues that are common to all capabilities that you can deploy in the Compliance Packs.

Open Text strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit [Open Text Support](#), then select the appropriate product category.

Issue with Report Formatting

Issue: When using the **Export Asset** feature, the formatting for the reports might have issues such as:

- Dark backgrounds
- Dark fonts
- Dark table cells

Workaround: Currently, no workaround is available. (OCTCR33I186007)

Publication Status

Released: June 5, 2024

Updated: Tuesday, June 4, 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 Solutions Guide for ArcSight Compliance Insight Package (Compliance Insight Package GDPR 1.0.0.1)

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@Openext.com.

We appreciate your feedback!

Additional Documentation

The ArcSight Platform documentation library includes the following resources.

- [Administrator's Guide for ArcSight Platform](#), which contains installation, user, and deployment guidance for the ArcSight software products and components that you deploy in the containerized platform.
- [User's Guide for Fusion 1.3 in the ArcSight Platform](#), which is embedded in the product to provide both context-sensitive Help and conceptual information.
- [Product Support Lifecycle Policy](#), which provides information on product support policies.

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2001 - 2023 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

"Openext" 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.