



Help

Download

Admin

Reports

Change

Manage

Operations

Home

NERC CIP

INTELLIGENT EVENT MODULE

Copyright 2006–2007 by TECSys Development, Inc. All rights reserved.

The information in this document is provided by TECSys Development, Inc. as is without warranty of any kind and is subject to change without notice.

Console*Works* is a registered trademark of TECSys Development, Inc. HP-UX is a registered trademark of Hewlett-Packard, Inc. or its subsidiaries in the United States and other countries. IBM and AIX are registered trademarks of International Business Machines Corporation in the United States, other countries, or both. Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Microsoft, Windows, Windows 2000, Windows Server, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries. Novell is a registered trademark of Novell, Inc., in the United States and other countries. Red Hat is a registered trademark of Red Hat, Inc. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Sun, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. SUSE is a registered trademark of SUSE LINUX Products GmbH. UNIX is a registered trademark of The Open Group in the U.S. and other countries. All other product or company names mentioned in this document are trademarks or registered trademarks of their respective owners. Portions of the technology within the Console*Works* server are protected under US Patent number 6,505,245.

Console*Works* JavaTerminal Emulator Applet makes use of the public domain Java Telnet Applet. TDi did not write the Java Telnet Applet nor does it claim any particular license to the applet excepting those rights given by the GNU Library General Public License.

The Java Telnet Applet credits are listed below:

The Java Telnet Applet

Copyright © 1996–98 Matthias L. Jugel, Marcus Meibner. All Rights Reserved.

<http://www.mud.de/se/jta/>

On RegEx

Copyright 1992, 1993, 1994 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

The SSL features of Console*Works* include OpenSSL software that is covered by Terms and Conditions that are available at the OpenSSL web site, <http://www.openssl.org>. Source code copyright © 1995–1998 Erick Young (eay@cryptsoft.com).

CUSTOMER CARE

To connect with TDi Support:

Email: support@tditx.com
Voice: +1.800.695.1258
Fax: +1.972.424.9181
Post: Support
TECSys Development, Inc.
1600 10th Street
Suite B
Plano, Texas, U.S.A. 75074

Tip: When requesting customer care, ensure you have within easy reach an active Service Agreement and the following information:

- Name and contact information
- Company name
- Make and model of host running *Console Works*
- Host operating system version and patch level
- *Console Works* version
- Description of problem

Some of this information is available in the Software Product Report (SPR). You can generate an SPR from the *Console Works* main menu:

» Click **Help** > **Run SPR**

DEMONSTRATIONS, DOCUMENTATION & DOWNLOADS

To register for a free demonstration of *Console Works*, view company and product information, and obtain documentation and downloads, visit <http://www.tditx.com>

CUSTOMER CARE SUPPORT LEVELS AND FEATURES

	Active Care	Platinum	Gold	Silver
Telephone Support	24x7*	24x7*	07:00 to 19:00* Every Day	08:00 to 17:00† Monday through Friday
Email Support (support@tditx.com)	24x7*	24x7*	07:00 to 19:00* Every Day	08:00 to 17:00† Monday through Friday
Fax Support		08:00 to 17:00‡ Monday through Friday	08:00 to 17:00‡ Monday through Friday	08:00 to 17:00‡ Monday through Friday
TDi Support Engineer Assigned	Y	Optional		
Maintenance Support	Y	Y	Y	Y
2-Hour Response§	Y	Y	Y	
4-Hour Response§				Y
Support During TDi Holidays	Y	Y	Y	

*Primary local time zone (North America only) / Includes holidays

†Primary local time zone (North America only) / Excludes holidays

‡CST = UTC -6 / CDT = UTC -5

§Next day response when support requested after posted hours.

CONTENTS

Chapter 1. NERC CIP IEM	1
CIP Cyber Security Standards	1
ABOUT IEMS	2
QUICK START	3
ASSUMPTIONS	4
Chapter 2. Installing the NERC CIP IEM License	5
Before You Begin	5
INSTALLING THE LICENSE (OPENVMS)	6
INSTALLING THE LICENSE (UNIX)	8
INSTALLING THE LICENSE (MS WINDOWS)	9
Chapter 3. Installing the NERC CIP IEM	11
Download IEM	11
Import IEM	12
Post-Install Tasks (optional)	13
Chapter 4. Associating Scans	15
Scans	15
Scan Associations	15
More About Associations	18
Chapter 5. Confirming Event Correlation	19
REGULATORY CORRELATION TEMPLATE	20
Automatic Policy Application	20
Confirm Event Correlation	20
Modify Regulatory Events	23
Next Steps	24

Chapter 6. Generating Regulatory Reports25

REGULATORY REPORTS26
 Creating Regulatory Reports 26
 Relative Time Frames 30
 REPORT REUSE32
 Saved Report Access 32

**Appendix A. Regulatory Events
 and NERC CIP StandardsA-1**

CIP-005-1 R2.1 A-1
 CIP-005-1 R2.2 A-1
 CIP-005-1 R2.4 A-2
 CIP-005-1 R3 A-6
 CIP-005-1 R3.2 A-8
 CIP-007-1 R2.1 A-11
 CIP-007-1 R2.2 A-11
 CIP-007-1 R2.3 A-12
 CIP-007-1 R3.1 A-12
 CIP-007-1 R5.1 A-12
 CIP-007-1 R5.1.1 A-13
 CIP-007-1 R5.1.2 A-14
 CIP-007-1 R5.2 A-15
 CIP-007-1 R5.2.1 A-16
 CIP-007-1 R5.2.2 A-18
 CIP-007-1 R5.3 A-21
 CIP-007-1 R5.3.3 A-21
 CIP-007-1 R6.1 A-21
 CIP-007-1 R6.2 A-21
 CIP-007-1 R6.3 A-22
 CIP-007-1 R6.4 A-30

How-To

INSTALLING THE NERC CIP IEM LICENSE

OpenVMS	
To register license	6
To load license	6
UNIX	
To load license	8
To install license	8
MS Windows	
To install license	9

INSTALLING THE NERC CIP IEM

To download NERC CIP IEM	11
To import NERC CIP IEM	12

ASSOCIATING SCANS

To associate Scan to Consoles	17
-------------------------------------	----

CONFIRMING EVENT CORRELATION

To access Regulatory Correlation Template	20
To modify Regulatory Correlation Template	23
To enable Regulatory Result Event to trigger Event	24

GENERATING REGULATORY REPORTS

To create Regulatory report	26
To save report configuration	32
To load saved Regulatory report	32
To show saved report	32

**This Page Intentionally Left Blank
(except for what you've just read)**

NERC CIP IEM

CIP CYBER SECURITY STANDARDS

The NERC CIP cyber security standards require that those entities responsible for North America's bulk energy systems identify and protect their critical cyber assets. These standards define the minimum requirements for security controls for 8 major areas across 41 topics, including asset identification and monitoring, systems access, user account management, incident reporting and documentation, and security procedures, policies, and plans. The complex interrelationships among the requirements, not to mention the legal and national security implications of not complying with these now-mandatory standards, means you face bigger challenges to managing infrastructure than ever before.

ConsoleWorks CIP Solution

ConsoleWorks[®] by TDi can play a key role in your CIP compliance solution. TDi has engineered an Intelligent Event Module (IEM) specifically for CIP Standards CIP-002 through CIP-009. Integrating the robust standard features of ConsoleWorks with this CIP-specific IEM enables you to take advantage of a powerful and comprehensive compliance package.

Install the NERC CIP IEM into Console *Works* and you instantly enhance your compliance solution with such features as:

- Real-time monitoring and management of critical cyber assets
- Audit-quality, tamper-sensitive logs for all system events and user activity
- Data-rich reports and documentation for reviews, audits, and adherence to standards
- Support for security policies, response and recovery plans, and change control programs

What is an IEM? A Console*Works* Intelligent Event Module (IEM) enables you to automate real-time monitoring of your infrastructure and capture the critical cyber security information you need for effective enterprise management and regulatory compliance.

An IEM provides Console*Works* with a watch-list of all the text messages, including error codes, system warnings, security incidents, and status alerts, produced by any application, system, device, or database. Console*Works* watches for these messages, called Events, in the data streams of your managed Consoles.

Note

Console*Works* logs all the messages to and from a managed Console, regardless of whether they contain Events.

Events

When Console*Works* detects an Event, it alerts you to the Event as it is happening, captures the state of the Console before and after the Event, and automatically performs the default or customer-configured responses associated with that Event.

Scans

IEMs come with Events pre-arranged in logical groupings called Scans. By using a Scan—or a combination of Scans—instead of hundreds of individual Events, you can simplify the tasks of configuring Consoles, monitoring Events, and managing your enterprise. By consolidating Events into Scans and then associating these Scans with the Consoles you want to monitor for those Events, you streamline your network management efforts and standardize the coverage of Console messages throughout your site. This standardization ensures Event monitoring and remediation that is compliant, comprehensive, and auditable.

Typically, a Scan is designed to listen for any of the hundreds of messages, such as error codes, system warnings, and status alerts, coming from a specific networked asset or asset type. The Scans in the NERC CIP IEM, though, are specially designed to focus on cyber security incident messages and match those messages to one or more CIP standards.

What is the NERC CIP IEM?

The NERC CIP IEM contains a knowledge base of NERC CIP standards, a watch-list of over 400 cyber security-related Events for 10 industry-leading operating systems, servers, and applications, plus the technology necessary to link each Event to its corresponding standard(s). This correlation technology enables you to configure Scans to support compliance policies.

QUICK START

This section provides an overview of the tasks you need to complete to take advantage of all the features in the NERC CIP IEM. If you are familiar with IEMs and *Console Works*, you can use this overview as a checklist and guide to installing, configuring, and using the NERC CIP IEM. If you are unfamiliar with *Console Works* and its operations, use the overview to preview the tasks involved and then move to page 5 to begin the process.

Tip

If you are using the online version of this book, click the page number displayed for each quick start step to move to that page.

► **To use the NERC CIP IEM**

1. **Install the NERC CIP IEM license page 5**
Obtain access to all of the features of the NERC CIP IEM.
2. **Install the NERC CIP IEM page 11**
Load close to 600 cyber security Events, including security incident alerts and their corresponding NERC CIP standards, into the *Console Works* knowledge base.
3. **Associate Scans to managed Consoles page 15**
Initiate real-time monitoring of the data streams of associated Consoles.
4. **Customize Regulatory Events. page 19**
Define policies that coordinate responses to a security-related Event.
5. **Run Regulatory Reports page 25**
Customize reports to give you the data you need to secure your critical cyber assets and manage your compliance initiatives.

ASSUMPTIONS

The information presented in this guide was developed under the following assumptions:

- You are familiar with the concepts, terminology, features, and functionality of your host operating system and platform.
- You know how to perform basic actions, such as managing files, using a mouse or on-screen pointer, and operating menu commands, in a graphical user interface (GUI) environment.
- You are familiar with the concepts, terminology, features, and functionality of a web browser GUI. For example, you understand that *to select a check box* means to click a check box so as to make a check mark appear in the check box; whereas *to clear a check box* means to click the check box so as to make the check mark displayed in the check box disappear.
- You are familiar with the concepts, terminology, features, and functionality of *Console Works*.
- You have installed and started *Console Works*, have accessed it through a web browser, and have it displayed on the screen in front of you.

Note

For information about using the NERC CIP IEM with CWCLient™, the command line interface for *Console Works*, contact TDi Support (support@tditx.com).

Installing the NERC CIP IEM License

This chapter contains the procedures for installing the *Console Works* license for the NERC CIP IEM. You must install the NERC CIP license before you can install the NERC CIP IEM.

Note

The regulatory compliance features in *Console Works* also require installation of the Regulatory license (CONWRKS-FE-REGUL). Typically, this license is purchased in combination with the NERC CIP IEM license and both licenses are sent to you in a single kit. To install this kit, use the following procedures. To purchase and install only the Regulatory license, contact TDi Support.

BEFORE YOU BEGIN

- Install and configure *Console Works*. For information and installation instructions, refer to the *Console Works* installation guide for your site's operating system.
- Have ready access to the NERC CIP IEM license. If you require a license, contact TDi Support at support@tditx.com.
- (*HP® OpenVMS®*) Ensure that you have logged into an account with full privileges, such as **SYSTEM**.
- (*UNIX®*) Ensure that you have logged into an account with full privileges, such as **root**.
- (*Microsoft® Windows®*) Ensure that you have logged into a fully privileged account, such as **ADMINISTRATOR** or a member of the **ADMINISTRATOR** group.

INSTALLING THE LICENSE (OPENVMS)

For information about trouble-shooting license issues, refer to the section, *Trouble-Shooting Installation*, in the *Console Works* installation guide for OpenVMS.

LICENSE FORMATS

The NERC CIP IEM license is available in the following formats:

- .pdf
- .PAK
- **XXX_COM.TXT** or **XXX.COM.TXT**, where **XXX** represents a combination of your company code and the license creation date.

Tip

When you extract **XXX_COM.TXT** or **XXX.COM.TXT**, rename it with an informative name, such as **CIP_LICENSE.COM**.

Registering the license

► **To register license**

```
$ @XXX.COM
```

Example

To register the license file you have named **CIP_LICENSE.COM**:

```
$ @CIP_LICENSE.COM
```

Loading the license

You have to manually load the license only once. OpenVMS automatically loads the license the next time it starts.

► **To load license**

```
$ LICENSE LOAD
```

NERC CIP IEM LICENSE

After you install the license, open and review the file. It should resemble the license in the following example.

Example

```
ISSUER: TECSYS-DEVELOPMENT
AUTHORIZATION: 123456-7890-1234567-8901
PRODUCT: CONWRKS-DB-CIP
PRODUCER: TECSYS-DEVELOPMENT
UNITS: 0
VERSION: 3.99
TERMINATION: 22-APR-2007
ACTIVITY: CONSTANT=1
PRODUCT TOKEN: 098765-4321-098765-0000
HARDWARE ID: Z43HOCK2B45G0
CHECKSUM: 871B8818 U291055Y 34078835 T974D9I9
```

INSTALLING THE LICENSE (UNIX)

For information about trouble-shooting license issues, refer to the section, *Trouble-Shooting Installation*, in the *Console Works* installation guide for UNIX.

Loading the license

► **To load license**

1. Open the TDi email attachment containing the NERC CIP IEM license.
2. From the attachment, extract the compressed shell script—shipped in the format: `xxx_sh.zip`—to the installation directory (typically, `/tmp/conwrks`).

Installing the license

► **To install license**

To install the license, run the shell script.

NERC CIP IEM LICENSE

After you install the license, open and review the file. It should resemble the license in the following example.

Example

```
ISSUER: TECSYS-DEVELOPMENT
AUTHORIZATION: 123456-7890-1234567-8901
PRODUCT: CONWRKS-DB-CIP
PRODUCER: TECSYS-DEVELOPMENT
UNITS: 0
VERSION: 3.99
TERMINATION: 22-APR-2007
ACTIVITY: CONSTANT=1
PRODUCT TOKEN: 098765-4321-098765-0000
HARDWARE ID: Z43HOCK2B45G0
CHECKSUM: 871B8818 U291055Y 34078835 T974D9I9
```

INSTALLING THE LICENSE (MS WINDOWS)

For information about trouble-shooting license issues, refer to the section, *Trouble-Shooting Installation*, in the *Console Works* installation guide for Windows.

Installing the license

► **To install license**

Copy or extract the .LIC file(s) to the following folder:

`C:\Program Files\TDi\ConsoleWorks Server\LMF\TDI_Licenses`

NERC CIP IEM LICENSE

After you install the license, open and review the file. It should resemble the license in the following example.

Example

```
ISSUER: TECSYS-DEVELOPMENT
AUTHORIZATION: 123456-7890-1234567-8901
PRODUCT: CONWRKS-DB-CIP
PRODUCER: TECSYS-DEVELOPMENT
UNITS: 0
VERSION: 3.99
TERMINATION: 22-APR-2007
ACTIVITY: CONSTANT=1
PRODUCT TOKEN: 098765-4321-098765-0000
HARDWARE ID: Z43HOCK2B45G0
CHECKSUM: 871B8818 U291055Y 34078835 T974D9I9
```

NOTES

CHAPTER

3

Installing the NERC CIP IEM

After installing the license for the NERC CIP IEM, you need to install the IEM itself.

This chapter contains the information on the following topics:

- Instructions for installing the IEM onto the Console *Works* server
- Post-installation tasks
- Information about new regulatory-related Severities

The process for installing the NERC CIP IEM has two parts:

1. Download the IEM.
2. Import the IEM.

DOWNLOAD THE IEM

► To download NERC CIP IEM

1. Move to the TDi web site (www.tditx.com/support_iemdownloads.asp).
2. On the Product Downloads page, click **NERC Critical Infrastructure Protection (CIP)**.

3. In the Connect to support2.tditx.com dialog box, enter your User name and Password, and click **OK**. To obtain a User name and Password, contact TDi Support (support@tditx.com).
4. On the File Download dialog box, click **Open**.
5. Extract the IEM (`cw_iem-nerc_cip-0006.xml`) to a directory accessible from your client workstation.

IMPORT THE IEM

For more information about importing IEMs or XML files, refer to the user guide for *ConsoleWorks*.

► To import NERC CIP IEM

1. On the *ConsoleWorks* main menu, click **Admin > Database > Import XML**.
2. On the Import XML page, complete the following tasks:
 - On the Correction Level drop-down list, select **None**.
 - For Replace records, click **No**.

3. Click **Browse**.

The Choose file dialog box appears.

4. On the Choose file dialog box, locate and double-click `cw_iem-nerc_cip-0006.xml`.

The Import XML page appears, with the file name displayed in the XML File box.

5. On the Import XML page, click **Import XML**.

A dialog box appears.

6. Review the message on the dialog box, and click **OK**.

ConsoleWorks imports the file to the Data Store. The results of the validation appear.

7. To complete the import, review the results, remediate any issues, and click **Commit Store**.

The NERC CIP IEM is saved to the ConsoleWorks configuration database.

Tip

To cancel the import and delete the Import XML file, click **Delete Store**. This action does not delete the IEM.

POST-INSTALL TASKS (OPTIONAL)

After you have imported the NERC CIP IEM, review the Events to ensure that their default settings and configuration match your compliance requirements. For example, the NERC CIP IEM ships with two new Severities: *Actionable* and *Reportable* (refer to Figure 3.1 on this page). These Severities, which you can use to classify cyber security incidents, come with pre-assigned colors (red and yellow) and priority ratings (30 and 70). You should check whether these defaults conform to your company's compliance policies. For information about changing an Event's configuration, refer to the user guide for *Console Works*.

You can view all of the Events on the Show Events page (refer to Figure 3.1). To display the Show Events page, click **Manage > Events > Show Events** on the *Console Works* main menu.

Figure 3.1 CIP EVENT SEVERITIES

Prio	Event	Description	Severity
30	CIP-006-1-R2_3	CIP-006-1 R2.3: Physical Access Controls: Security Personnel	ACTIONABLE
30	CIP-006-1-R2_4	CIP-006-1 R2.4: Physical Access Controls: Other Authentication Devices	ACTIONABLE
70	CIP-006-1-R3	CIP-006-1 R3: Monitoring Physical Access	REPORTABLE
30	CIP-006-1-R3_1	CIP-006-1 R3.1: Monitoring Physical Access: Alarm Systems	ACTIONABLE
30	CIP-006-1-R3_2	CIP-006-1 R3.2: Monitoring Physical Access: Human Observation of Access Points	ACTIONABLE
30	CIP-006-1-R4	CIP-006-1 R4: Logging Physical Access	ACTIONABLE
30	CIP-006-1-R4_1	CIP-006-1 R4.1 Logging Physical Access: Computerized Logging	ACTIONABLE
30	CIP-006-1-R4_2	CIP-006-1 R4.2: Logging Physical Access: Video Recording	ACTIONABLE
30	CIP-006-1-R4_3	CIP-006-1 R4.3: Logging Physical Access: Manual Logging	ACTIONABLE
30	CIP-006-1-R5	CIP-006-1 R5: Access Log Retention	ACTIONABLE
70	CIP-006-1-R6	CIP-006-1 R6: Maintenance and Testing	REPORTABLE
30	CIP-006-1-R6_1	CIP-006-1 R6.1: Maintenance and Testing: Cycle	ACTIONABLE
70	CIP-006-1-R6_2	CIP-006-1 R6.2: Maintenance and Testing: Retention of Testing Records	REPORTABLE
70	CIP-006-1-R6_3	CIP-006-1 R6.3: Maintenance and Testing: Retention of Outage Records	REPORTABLE
70	CIP-007-1-R1	CIP-007-1 R1: Test Procedures	REPORTABLE

NOTES

Associating Scans

After installing the NERC CIP IEM, you need to associate Scans from the IEM to critical cyber assets in your *Console Works*-managed environment. This chapter contains the procedures for associating the Scans. For more information about Scans and about strategies for managing infrastructures effectively using Scans and rules-based policies, refer to the user guide for *Console Works*.

SCANS

Scans are a convenient tool for managing the capture, classification, notification, and resolution of cyber security incidents in your infrastructure. Such incidents are communicated as text messages among your networked assets (*Consoles*). These messages are known to *Console Works* as *Events*.

To have *Console Works* scan for Events on a Console, you must associate the Scan containing those Events with that Console. As soon as you do, *Console Works* begins using that Scan to sift through all the chatter in your managed infrastructure, looking for security, availability, and regulatory-related Events.

SCAN ASSOCIATIONS

Although you can associate any Scan with any class of Console, only associate a Scan with the class of Console appropriate for that Scan. For instance, associate Cisco® PIX® Firewall Scans with only PIX firewalls and HP Scans with only HP systems. Table 4.1 on page 16 contains a list of the Scans in the NERC CIP IEM and their corresponding class of Console.

Table 4.1 NERC CIP IEM Scans and Console Classes

SCAN	CLASS OF CONSOLE
CIP	All. Scan contains NERC CIP Standards CIP-002-1-R1 through CIP-009-R5
CIP_AIX	IBM® AIX® 4.3
CIP_CISCO	Cisco IOS® v12.3
CIP_CONWRKS	ConsoleWorks server
CIP_HPUX11	HP-UX® 11 and later
CIP_LNX26	Linux® kernel 2.6
CIP_PIX	Cisco PIX Firewall 6.3
CIP_SOLARIS	Sun™ Solaris™ 7 and 8
CIP_T64U	HP Tru64® UNIX 5.1
CIP_VMS	HP OpenVMS v7.2
CIP_WIN	Microsoft® Windows 2000® Server and Windows Server 2003®

Tip

Select the **Require Exclusive Connect** check box for the Consoles you are monitoring for regulatory compliance. For information about Require Exclusive Connect, refer to the user guide for ConsoleWorks.

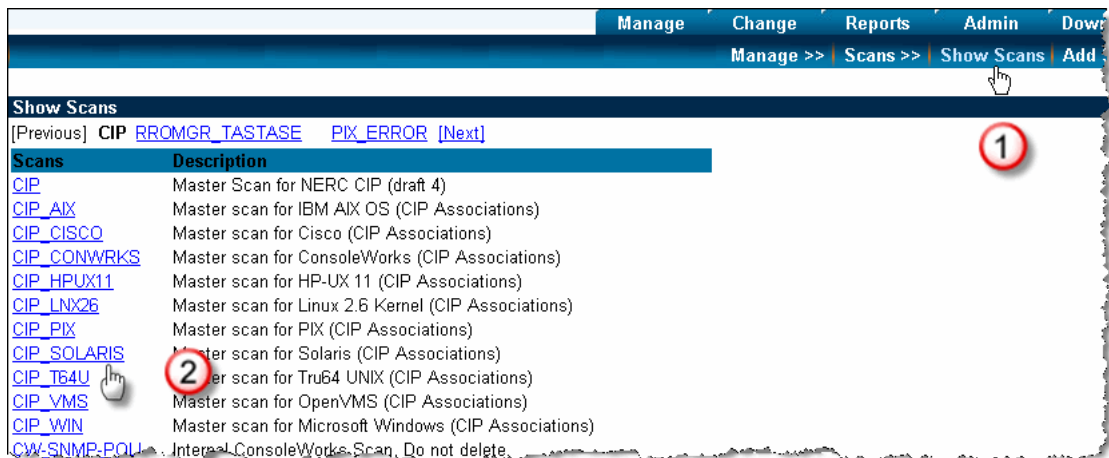
Associating Scans

You must have Admin Write privileges to associate Scans.

► To associate Scan to Consoles

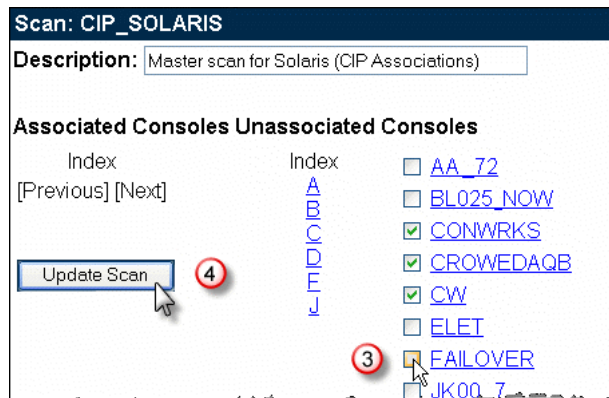
1. On the ConsoleWorks main menu, click **Manage > Scans > Show Scans**.

The Show Scans page appears.



2. In the Scans column, click the Scan of interest.

The Scan page for that Scan appears.



3. On the Scan page, in the Unassociated Consoles column, select the check boxes next to the Consoles you want to associate with the Scan. Click **Update Scan**.

A dialog box appears, specifying the number of Regulatory Seed Events now correlated to Regulatory Resulting Events. For information about Regulatory Seed Events or Regulatory Resulting Events, refer to “Regulatory Correlation Template” on page 20.

4. On the dialog box, click **OK**.

The Scan page appears, displaying the associated Consoles.

MORE ABOUT ASSOCIATIONS

While this chapter provides instructions for associating a single Scan with one or more Consoles, you have two more options for associating Scans with Consoles:

- Associate groups of Scans with one or more Consoles
- Create a Scan containing only the Events you want monitored and associate this customized Scan with one or more Consoles

This flexibility enables you to build and manage an enterprise solution for real-time monitoring, incident notification, and regulatory compliance.

Additionally, you can associate a Console to one or more Scans, associate Scans to Scans, and even associate Scans to Events.

To learn more about these and other association options, refer to the user guide for *Console Works*.

Warning

Do not associate any Scan displayed in Table 4.1 on page 16 with any other Scan displayed in that table.

Confirming Event Correlation

After associating the Scans in the NERC CIP IEM with the Consoles you want monitored, you should review the Event correlations found in the Regulatory Correlation Template (RCT).

Note

A correlated Event is a monitored-for incident that, when triggered, causes another Event to happen. The correlation is the set of configurable circumstances that must occur for the one Event to trigger the other Event.

This chapter contains the procedures for accessing, reviewing, and tailoring, Event configurations and correlations to meet the specific needs of your CIP compliance policies.

REGULATORY CORRELATION TEMPLATE

The RCT controls the relationship between a cyber security Event (Seed Event) and the CIP standard Event (Regulatory Result Event) that it references. The RCT is a part of every Seed Event's configuration.

AUTOMATIC POLICY APPLICATION

The RCT enables you to configure *Console Works* to trigger a CIP standard Event after a cyber security Event has occurred a set number of times within a given time period. You can even link several correlations to create a chain of Events that only trigger for very specific circumstances. Used this way, the RCT enables you to construct rule-based policies that automate policy application and support your compliance initiatives.

Tip

The RCT default is for every occurrence of a Seed Event to trigger its corresponding Regulatory Resulting Event. Before adjusting this default or any Regulatory Event correlation configuration, consult with your company's compliance monitor or their equivalent.

CONFIRM EVENT CORRELATION

To confirm that the correlation configurations for Regulatory Events supports your compliance policies, complete the following tasks:

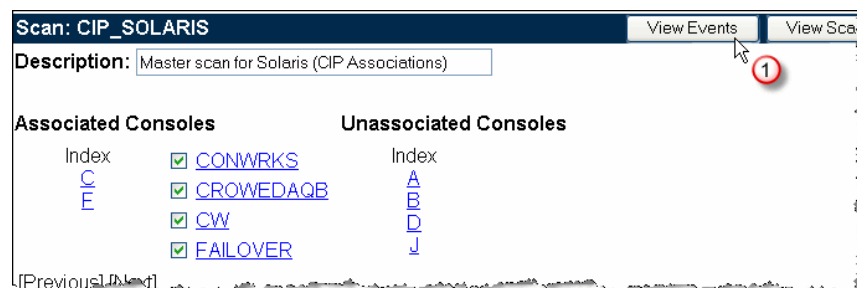
1. Access the Seed Event's configuration and the RCT.
2. Review its RCT.
3. (optional) Modify the correlation configuration.

Accessing THE RCT

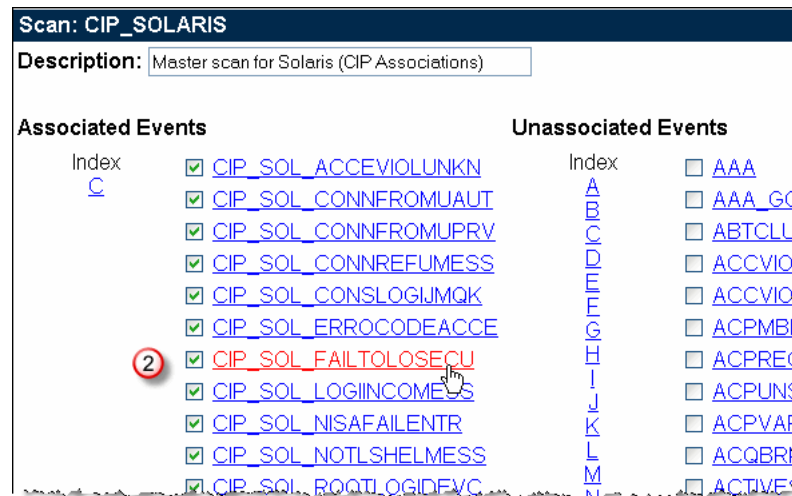
You do not need Admin privileges to view an Event's configuration, including its RCT.

► To access Regulatory Correlation Template

1. On the Scan page, click **View Events**.

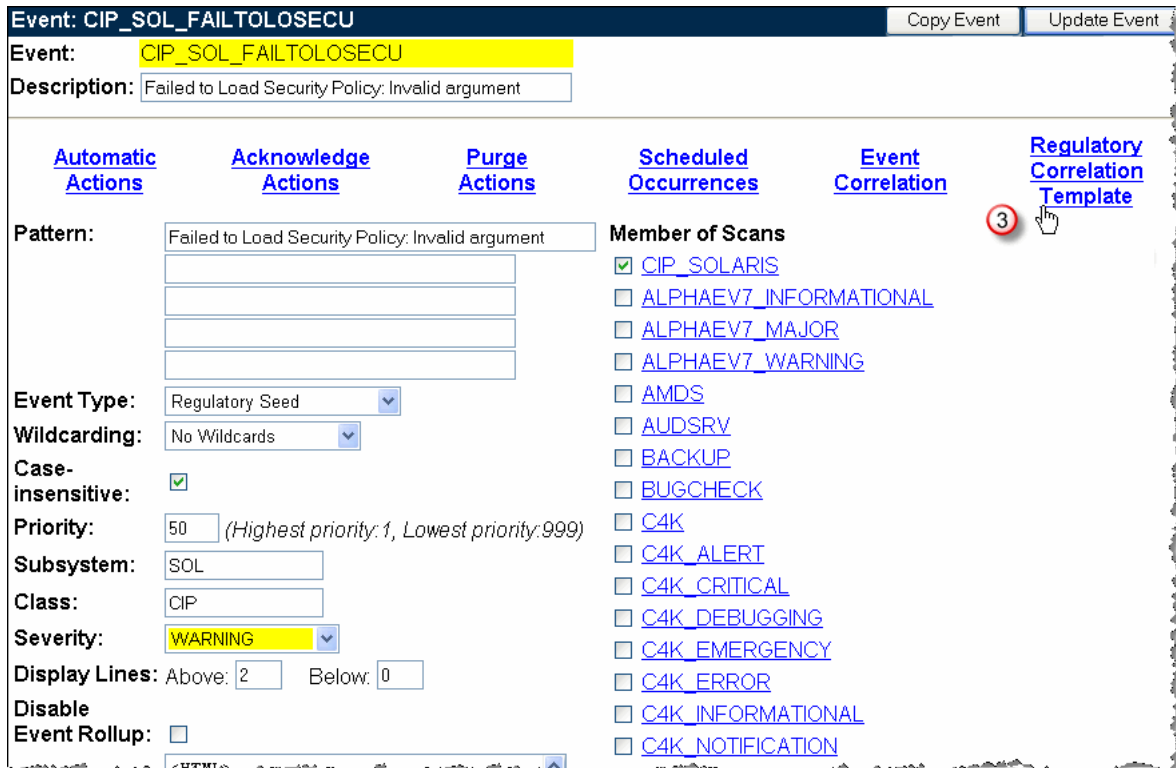


The associated and unassociated Events for the Scan appear.



2. Click an associated Event.

The Event configuration page for that Event appears.



3. Click **Regulatory Correlation Template**.

The RCT for the Event appears.

Regulatory Correlation Template: CIP_SCL_FAILTOLOSECU		Update
Originating Event Occurs		Resulting Event
<input type="text" value="1"/> Times in	<input type="text" value="1"/> Seconds	<input type="text" value="CIP-007-1-R5_2"/>
<input type="button" value="Update"/>		Event Search

Reviewing the RCT

The RCT displays the following elements:

Originating Event Occurs

Specifies the correlation criteria.

The first box specifies the number of times a Seed Event has to occur before triggering the correlated Resulting Event. You can specify from 1 to 1000 times. The default is 1.

The second box specifies the number of seconds within which the originating Seed Event has to occur before triggering the correlated Resulting Event. You can specify from 1 to 86400 seconds (1 day). The default is 1 second.

Resulting Event

Specifies the Event (also called the Regulatory Result Event) you want to occur after the Originating Event criteria have been met.

The CIP standard that deals with the incident that triggered the Seed Event appears in this box by default.

Event Search

Enables you to search for Events by name, description, priority, and Severity and enter the found Event into the Resulting Event text box.

For more information about Event Search, click **Event Search**, and then click **Search Help** on the Event Search window.

Tip

To return to the Event configuration page from the RCT, click the Event name in the title bar.



Regulatory Correlation Template: CIP_SQL_FAILTOLOSECU

Modifying the RCT configuration

You must have Admin Write privileges to change RCT configurations.

Warning

Consult with your company's compliance monitor or their equivalent before adjusting Event configurations.

► To modify Regulatory Correlation Template

1. Make changes directly to the values in the RCT.
2. Click **Update**.

Note

Any changes made to the RCT take effect the next time the Scan containing the changed Event is associated with a Console. Changes are not applied to existing associations. To apply RCT changes to a currently associated Console, unassociate the Console, clear the web browser cache, and re-associate the Console.

MODIFY REGULATORY EVENTS

Console *Works* enables you to modify and reconfigure Events to custom-fit your compliance efforts. This section provides procedures for changing Event types (Regulatory Seed, Regulatory Result, Regulatory Seed & Result, Non-Regulatory), enabling the RCT for a Regulatory Result Event, and creating a cascade of correlated Regulatory Events.

Changing Event types

To change an Event's type, on the Event configuration page for the Event, select a type from the Event Type drop-down list, and click **Update Event**.

Note

The RCT is not available for Non-Regulatory Events and Regulatory Result Events.

Turning Regulatory Result Events into Seed Events

By default, the Regulatory Result Events, the CIP standards, are strictly Resulting Events; they are not correlated to trigger an Event themselves. However, you can reconfigure a Regulatory Result Event to make it a Seed Event, and then set up an RCT for that new Seed Event.

► To enable Regulatory Result Event to trigger Event

1. On the Console *Works* main menu, click **Manage > Scans > Show Events**.

The Show Events page appears.

2. On the Show Events page, locate and click the Event you want to change.

The Event configuration page for that Event appears.

3. On the Event page, select **Regulatory Seed** or **Regulatory Seed and Result** on the Event Type drop-down list.

4. Click **Update Event**.

The Event page appears, displaying the RCT.

5. Click **Regulatory Correlation Template**.

The RCT for the Seed Event appears, with the Resulting Event box empty.

6. Configure the RCT for the Seed Event. For information about the elements in the RCT, refer to “Reviewing the RCT” on page 22.

Linking Event correlations

To configure multiple Event triggers and occurrences, repeat the procedure in “To enable Regulatory Result Event to trigger Event” to link Event correlations. These links result in Seed Events triggering Regulatory Result Events that, in turn, trigger other Regulatory Result Events.

NEXT STEPS

After you have confirmed the RCT configurations, you can specify the actions you want Console *Works* to take when a cyber security incident occurs. Console *Works* offers a range of options, from just logging the Event to issuing an ever-escalating series of emails and pages to running remediation scripts to resolve the incident.

For information and procedures for configuring incident responses through Console *Works*, refer to the user guide or contact TDi Support at support@tditx.com.

Generating Regulatory Reports

This chapter contains the instructions for building, running, and displaying regulatory-related reports.

The Console *Works* reporting feature enables you to tailor regulatory reports to fit the perspective you need: from reports that compile all cyber security Event activity across the entire monitored infrastructure to reports detailing the occurrence of a single Event on a single Console at a specific date and time.

REGULATORY REPORTS

Regulatory reports contain tallies of regulatory-related Events occurring on your managed infrastructure, as well as details about each Event and the governing regulations that make the Event relevant to your compliance initiatives. Use this information to spot overall trends or pinpoint and resolve regulatory issues across your enterprise.

Tip

Because the reports provide detailed, time-stamped data for each incident, they could help you meet some of your compliance challenges. You should review the reports with your company's compliance monitor or their equivalent to discern whether the reports can play a part in your regulatory compliance solution.

CREATING REGULATORY REPORTS

You must have Admin Control privileges to create, modify, or view reports in *Console Works*.

► **To create Regulatory report**

1. On the *Console Works* main menu, click **Reports**.


The Reports page appears (refer to Figure 6.1).

Figure 6.1 Reports Page

Reports		Show Saved Reports	
• Configuration Reports		Type	Name
○ Users		Summary	BOQSUMM1
○ Profiles		Detail	BOQDETAILRPT LOGFILEDETAIL1
○ Severities		Console Messages	CONSMESSAGES1
○ Scans		Regulatory	REGT1 REGT2
○ Events		Report Wizard	BLATES
○ Consoles			
• Log File Reports			
○ Console Messages			
○ Detail			
○ Summary			
• Regulatory Report			
• Tools			
○ Report Wizard			
○ Rename Saved Reports			
○ Delete Saved Reports			

2. Click **Regulatory Report**.

The Regulatory Report page appears.

3. Specify a time frame for the report. Enter a start date in the From box and an end date in the To box. Use one of the following methods:
 - Type the time frame in the format: DD-MMM-YYYY.
 - Type the time frame as a phrase (refer to “Relative Time Frames” on page 31).
 - Click the pop-up calendar () , and then click the date you want.

Note

Time is not a required parameter. The From default time is 00:00.
The To default time is 23:59.

4. In the Consoles column, select the check boxes next to the Consoles you want to include in the report.
5. In the Events column, select the check boxes next to the Events you want to include in the report.
6. (optional) To save the report’s configuration, in the Save Current Parameters As text box, type a name for the current report, and click **Save** (refer to “Report Reuse” on page 33).

7. Run the report by using one of the following methods:

- To run and display the report in new browser window:

Click .

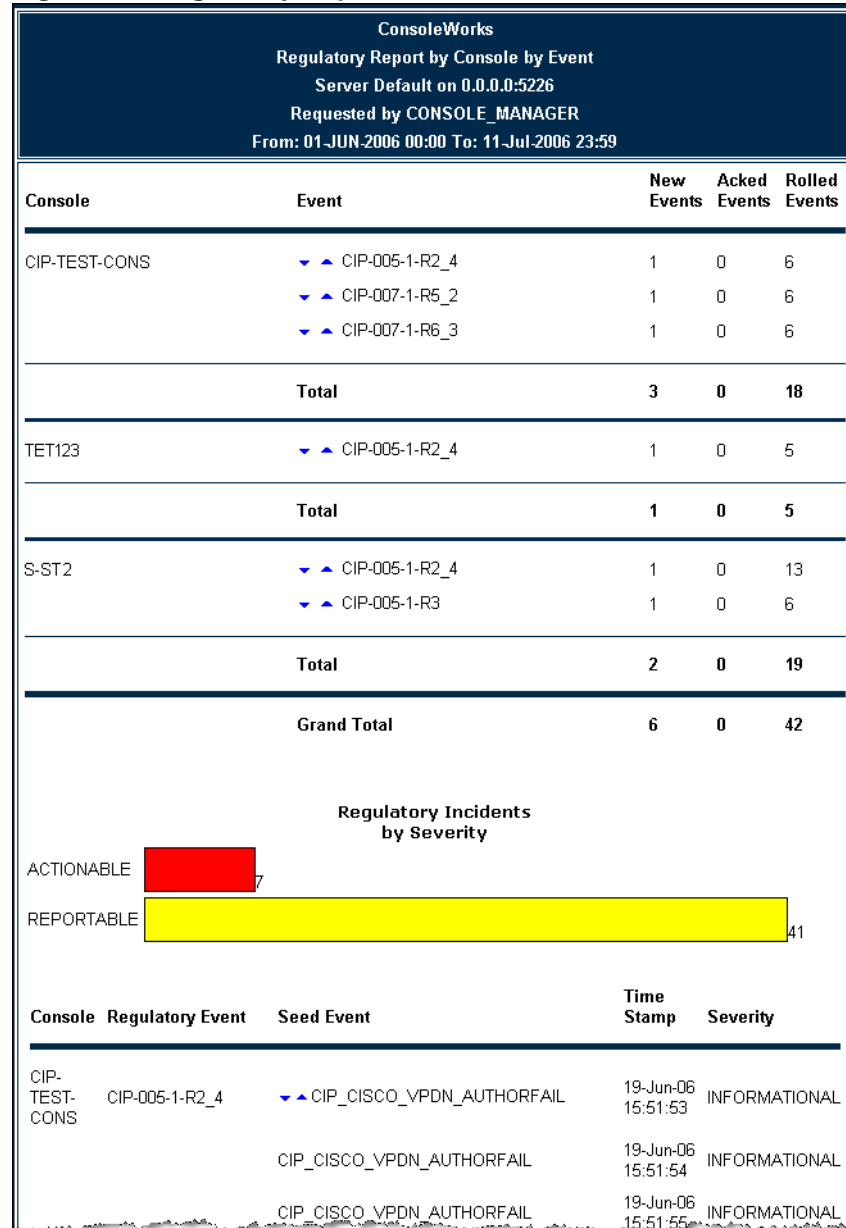
The Regulatory report appears in a new window. Refer to Figure 6.2 on page 29 for an example of a Regulatory report.

- To run and display report in the current browser window:

Click .

The Regulatory report appears in the current window. Refer to Figure 6.2 on page 29 for an example of a Regulatory report.

Figure 6.2 Regulatory Report



Tip

Click the down arrow (▼) to display the NERC CIP standard associated with a specific Event (refer to Figure 6.3). Click the up arrow (▲) to hide the standard.

Figure 6.3 NERC CIP Regulation in Regulatory Report

ConsoleWorks
Regulatory Report by Console by Event
 Server Default on 0.0.0.0:5226
 Requested by CONSOLE_MANAGER
 From: 01-JUN-2006 00:00 To: 11-Jul-2006 23:59

Console	Event	New Events	Acked Events	Rolled Events
CIP-TEST-CONS	▼ ▲ CIP-005-1-R2_4	1	0	6
	▼ ▲ CIP-007-1-R5_2	1	0	6

NERC CIP draft4 Event CIP-007-1-R5_2

Source

Standard:	Cyber Security -- Systems Security Management
Number:	CIP-007-1
Release:	Draft 4 (May 2, 2006)
Effective Date:	June 1, 2006

Requirement Text

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

- **R5.2.1.** The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.
- **R5.2.2.** The Responsible Entity shall identify those individuals with access to shared accounts.
- **R5.2.3.** Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

RELATIVE TIME FRAMES

You can specify a report's time frame relative to the day you run that report. Table 6.1 displays the words or phrases you can use as the time frame's From and To dates.

Table 6.1 Phrases And Meanings For Relative Time Frames

PHRASE	WHEN USED IN	MEANS
TODAY	From:	Today at midnight
	To:	Tonight at 11:59 PM
YESTERDAY	From:	Yesterday at midnight
	To:	Last night at 11:59 PM
BOM	From:	Beginning of the current month
BOQ	From:	Beginning of the current calendar quarter
BOY	From:	Beginning of the current calendar year
LAST WEEK	From:	Sunday at midnight (00:00) of the last calendar week
	To:	Saturday at 23:59 of the last calendar week
LAST MONTH	From:	Midnight (00:00) of the first day of last month
	To:	23:59 of the last day of last month
LAST YEAR	From:	Midnight (00:00) of January 1st of last year
	To:	23:59 of December 31st of last year
<i>n</i> HOURS AGO	From:	<i>n</i> hours from the time the report is run
	To:	<i>n</i> hours from the time the report is run

Table 6.1 Phrases And Meanings For Relative Time Frames (continued)

PHRASE	WHEN USED IN	MEANS
<i>n</i> DAYS AGO	From:	<i>n</i> days from the time the report is run
	To:	<i>n</i> days from the time the report is run
<i>n</i> WEEKS AGO	From:	<i>n</i> weeks from the time the report is run
	To:	<i>n</i> weeks from the time the report is run
<i>n</i> MONTHS AGO	From:	<i>n</i> months from the time the report is run
	To:	<i>n</i> months from the time the report is run

For more information about the Console *Works* reporting feature and for detailed instruction on its use, refer to the user guide for Console *Works* or contact TDi Support (support@tditx.com).

REPORT REUSE

Console *Works* enables you to save a report's configuration so that you can run it again and again, as well as use it as a model for other reports. Reports saved by one User account may be seen and used by all sufficiently privileged User accounts on the same Console *Works* invocation.

► To save report configuration

1. In the Save Current Parameters As text box, type a name for the report's configuration. You can use the same name for reports of different types.
2. Click **Save**.

SAVED REPORT ACCESS

You can access saved reports in either of two ways:

- Load Saved Report drop-down list
- Show Saved Reports page (refer to "Reports Page" on page 26)

Using Load Saved Report

The Load Saved Report drop-down list displays only configurations for the type of report specified on the current Report page. For example, on the Regulatory Report page, the list displays only saved Regulatory reports. On another Report page (Summary, Scans, Console Messages, and so on), it displays only the saved reports of that report type.

► To load saved Regulatory report

1. On the Console *Works* main menu, click **Reports**.
2. On the Reports page, click **Regulatory Report**.
3. On the Load Saved Report drop-down list, click the name of the report you want to appear.

Using Show Saved Reports

Use the following procedure to view all saved reports.

► To show saved report

1. On the Console *Works* main menu, click **Reports**.
2. On the Show Saved Reports page, click the report of interest.

The report page for the report appears, displaying the report's configuration.

NOTES

A

Regulatory Events and NERC CIP Standards

Appendix A lists the NERC CIP Standards and their associated Regulatory Events. Use the list to help you correlate Events and build Scans that can detect and remediate security incidents and enforce compliance adherence in accordance with your policies.

CIP-005-1 R2.1: Electronic Access Controls: Explicit Access Permissions

AIX

- CIP_AIX_REQUTOCHSECU4476: 2521-050 Request to change security state to new group security state is rejected (current security state is current group security state).

CIP-005-1 R2.2: Electronic Access Controls: Enable Required Ports/ Services Only

CISCO

- CIP_CISCO_URLF_SITE_ALLOWED: %URLF-6-SITE_ALLOWED: Client <IP_address>:<dec> accessed server <IP_address>:<dec>
- CIP_CISCO_URLF_SITE_BLOCKED: %URLF-4-SITE_BLOCKED: Access denied for the site '<chars>', client <IP_address>:<dec> server <IP_address>:<dec>
- CIP_CISCO_URLF_URL_ALLOWED: URLF-6-URL_ALLOWED: Access allowed for URL '<chars>', client <IP_address>:<dec> server <IP_address>:<dec>
- CIP_CISCO_URLF_URL_BLOCKED: URLF-4-URL_BLOCKED: Access denied URL '<chars>', client <IP_address>:<dec> server <IP_address>:<dec>
- CIP_CISCO_URLF_URL_TOO_LONG: URLF-3-URL_TOO_LONG: URL sent from <IP_address> is too long (more than <dec> bytes), possibly a fake packet?

CISCO PIX

- CIP_PIX_106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID
- CIP_PIX_106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name/ source_address(source_port) -> interface_name/ dest_address(dest_port) hit-cnt number ({first hit | number-second interval})
- CIP_PIX_304002: Access denied URL url SRC IP_address DEST IP_address: url

CIP-005-1 R2.4: Electronic Access Controls: External Access

CISCO

- CIP_CISCO_CRYPTOCERTREJECT: CRYPTO-6-CERTREJECT: Certificate enrollment request was rejected by Certificate Authority
- CIP_CISCO_CRYPTOCERTRET: %CRYPTO-6-CERTRET: Certificate received from Certificate Authority
- CIP_CISCO_CRYPTOCERTRETFAIL: %CRYPTO-3-CERTRETFAIL: Certificate enrollment failed.
- CIP_CISCO_CRYPTOKMP_AUTHFAIL: %CRYPTO-6-
IKMP_AUTH_FAIL: Authentication method <dec> failed with host <IP_address>
- CIP_CISCO_DBCONN_PWDEXPIRED: %DBCONN-5-PWDEXPIRED: APPC security failed, client <IP_address> using userid '<chars>' for server <chars>
- CIP_CISCO_DBCONN_PWDINVALID: %DBCONN-5-PWDINVALID: APPC security failed, client <IP_address> using userid '<chars>' for server <chars>
- CIP_CISCO_DBCONN_PWDMISSING: %DBCONN-5-PWDMISSING: APPC security failed, client <IP_address> using userid '<chars>' for server <chars>
- CIP_CISCO_DBCONN_SECFAIL: %DBCONN-5-SECFAIL: APPC security failed, client <IP_address> using userid '<chars>' for server <chars>
- CIP_CISCO_DBCONN_SECUNKNOWN: %DBCONN-5-SECUNKNOWN: APPC security failed, client <IP_address> using userid '<chars>' for server <chars>
- CIP_CISCO_DBCONN_UIDINVALID: %DBCONN-5-UIDINVALID: APPC security failed, client <IP_address> using userid '<chars>' for server <chars>
- CIP_CISCO_DBCONN_UIDMISSING: %DBCONN-5-UIDMISSING: APPC security failed, client <IP_address> using userid '<chars>' for server <chars>
- CIP_CISCO_DBCONN_UIDREVOKED: %DBCONN-5-UIDREVOKED: APPC security failed, client <IP_address> using userid '<chars>' for server <chars>

- CIP_CISCO_ENVM_NOACK: %ENVM-3-NOACK: Access to <chars> failed
- CIP_CISCO_FTSP_FMAIL_FAIL_AUTH: %FTSP-4-FMAIL_FAILED_AUTHENTICATION: Authentication for > <chars> < failed
- CIP_CISCO_FW_FTP_SESS_NOT_AU: FW-3-FTP_SESSION_NOT_AUTHENTICATED: Command issued before the session is authenticated -- FTP client <IP_address> FTP server <IP_address>
- CIP_CISCO_GLBP_BDAUTH: %GLBP-4-BDAUTH: Bad authentication received from <IP_address>, group <dec>
- CIP_CISCO_HSRP_BDAUTH: %HSRP-4-BDAUTH: Bad authentication from <IP_address>, group <dec>, remote state <chars>
- CIP_CISCO_RSVP_MSG_BADLEN: RSVP-3-BAD_RSVP_MSG_RCVD_LEN: RSVP Message had a bad length ip len: <dec> rsvp len: <dec>
- CIP_CISCO_RSVP_MSG_BADOBJ: RSVP-3-BAD_RSVP_MSG_RCVD_OBJ_LEN: Received a bad RSVP message, num objs: <dec> obj len: <dec> msg_len: <dec>
- CIP_CISCO_RSVP_MSG_BADTYPE: %RSVP-3-BAD_RSVP_MSG_RCVD_TYPE: RSVP Message had a bad type: <dec>
- CIP_CISCO_RSVP_MSG_BADVER: %RSVP-3-BAD_RSVP_MSG_RCVD_VER: RSVP Message had a bad version: <dec>
- CIP_CISCO_RSVP_MSG_CKSUM: %RSVP-3-BAD_RSVP_MSG_RCVD_CHECKSUM: RSVP Message had a bad checksum: <dec> foo: <dec>
- CIP_CISCO_RSVP_MSG_DIGEST: RSVP-3-BAD_RSVP_MSG_RCVD_AUTH_DIGEST: <chars> message from <IP_address> discarded - incorrect message digest
- CIP_CISCO_RSVP_MSG_RCV_COOK: RSVP-3-BAD_RSVP_MSG_RCVD_AUTH_COOKIE: <chars> message from <IP_address> discarded - challenge failed for key ID <chars>

- CIP_CISCO_RSVP_MSG_RCV_DUP:RSVP-3-
BAD_RSVP_MSG_RCVD_AUTH_DUP: <chars> message from
<IP_address> discarded - authentication seq #<int> is a
duplicate
- CIP_CISCO_RSVP_MSG_RCV_NOSA:RSVP-3-
BAD_RSVP_MSG_RCVD_AUTH_NO_SA: <chars> message from
<IP_address> discarded: no security association for
<IP_address> - no RSVP security key configured or no
memory left.
- CIP_CISCO_RSVP_MSG_RCV_WIN:RSVP-3-
BAD_RSVP_MSG_RCVD_AUTH_WIN:<chars> message from
<IP_address> discarded - seq #<int> outside
authentication window
- CIP_CISCO_SGBP_AUTHFAILED:%SGBP-1-AUTHFAILED: Member
<chars> failed authentication
- CIP_CISCO_SHELF_AUTH_FAILED:%SHELF-5-AUTH_FAILED: MD5
digest does not match, SDP packet received from,
<IP_address> rejected
- CIP_CISCO_SNASW_RM_LOG_48:SNASW-3-RM_LOG_48: PROBLEM
- <int> - Attach rejected because security information
invalid <chars>
- CIP_CISCO_SNASW_RM_LOG_53:SNASW-3-RM_LOG_53: PROBLEM
- <int> - Attach rejected because security information
not specified <chars>
- CIP_CISCO_SNMP_AUTHFAIL:%SNMP-3-AUTHFAIL:
Authentication failure for SNMP req from host
<dec>.<dec>.<dec>.<dec>
- CIP_CISCO_SNMP_MGR_BADAUTHTYPE:%SNMP_MGR-4-
BADAUTHTYPE: Unsupported SNMP authorization type: <int>
- CIP_CISCO_SONET_BADAUTH:%SONET-3-BADAUTH: APS Bad
authentication from <IP_address>
CIP_CISCO_STANDBY_BADAUTH: %STANDBY-3-BADAUTH: Bad
authentication from <IP_address>, remote state <chars>
- CIP_CISCO_SYSCTLR_AUTH_FAILED:%SYSCTLR-5-AUTH_FAILED:
MD5 digest does not match, SDP packet received from,
<IP_address> rejected
- CIP_CISCO_TCP_BADAUTH:%TCP-6-BADAUTH: <chars> MD5
digest from <chars>(<dec>) to <chars>(<dec>)<chars>

- CIP_CISCO_TN_BADLOGIN: %TN-2-BADLOGIN: Bad login string pointer <hex>
- CIP_CISCO_TXCONN_SECFAIL: %TXCONN-5-SECFAIL: APPC security failed, client <IP_address> using userid '<chars>' for server <chars>
- CIP_CISCO_UBR7200_AUTHFAIL: %UBR7200-5-AUTHFAIL: Authorization failed for Cable Modem <enet> on interface <chars>
- CIP_CISCO_VPDN_AUTHENERR: %VPDN-6-AUTHENERR: <chars> <chars> <chars> cannot authenticate for <chars> <chars> <chars><chars><chars>
- CIP_CISCO_VPDN_AUTHENFAIL: %VPDN-6-AUTHENFAIL: <chars> <chars> <chars>, <atalk_address>authentication failure <chars>for <chars> <chars> <chars><chars><chars>
- CIP_CISCO_VPDN_AUTHORERR: %VPDN-6-AUTORERR: <chars> <chars> <chars> cannot authorize for <chars> <chars> <chars><chars><chars>
- CIP_CISCO_VPDN_AUTHORFAIL: VPDN-6-AUTORFAIL: <chars> <chars> <chars>, <atalk_address> authorization failure for <chars> <chars> <chars><chars><chars>

LINUX

- CIP_LNX26_NET_CLNT_01026: call_verify: unknown auth error: [0-9a-f]+
- CIP_LNX26_NET_CLNT_01034: call_verify: auth check failed CIP_PIX_107001: RIP auth failed from IP_address: version=number, type=string, mode=string, sequence=number on interface interface_name

CISCO PIX

- CIP_PIX_107002: RIP pkt failed from IP_address: version=number on interface interface_name
- CIP_PIX_109006: Authentication failed for user user from inside_address/inside_port to outside_address/ outside_port on interface interface_name.

- CIP_PIX_109008: Authorization denied for user user from outside_address/outside_port to inside_address/inside_port on interface interface_name.
- CIP_PIX_109009: Authorization denied from inside_address/inside_port to outside_address/outside_port (not authenticated) on interface interface_name.
- CIP_PIX_109013: User must authenticate before using this service
- CIP_PIX_109015: Authorization denied (acl=acl_ID) for user 'user' from source_address/ source_port to dest_address/dest_port on interface interface_name
- CIP_PIX_610002: NTP daemon interface interface_name: Authentication failed for packet from IP_address
- CIP_PIX_610101: Authorization failed: Cmd: command Cmdtype: command_modifier
- CIP_PIX_611102: User authentication failed: Uname: user
- CIP_PIX_611311: VNPClient: XAUTH Failed: Peer: IP_address

CIP-005-1 R3: Monitoring Electronic Access

AIX

- CIP_AIX_ADDPPRINYOUR3603: 2502-032 add_principal: Principal your-login-name.admin@realm-name does not exist.
- CIP_AIX_CANNEXECCOMM4246: 2515-017 Cannot execute command for subscription Subscription handle name, because login restrictions prevent the target AIX user AIX user name from running: AIX system error message.
- CIP_AIX_LOGIFAILEVEN1559: 0018-276 Login failed.
- CIP_AIX_PLEALOGIASRO3301: 0037-607 Please login as root to execute this program.
- CIP_AIX_YOUEANINLOGIO205: 3004-007 You entered an invalid login name or password

CISCO

- CIP_CISCO_LOGIN_TOOMANY_AUTHF: LOGIN-3-TOOMANY_AUTHFAILS: Too many Login Authentication failures have occurred in the last one minute on the line <dec>.

CONSOLEWORKS SERVER

- CIP_CONWRKS-EAAUTHDENY: Login denied - external authentication authoritatively denied a user.
- CIP_CONWRKS-EANOVALIDPROFILES: Login denied - external authentication validated a user and profiles were returned but none of the profiles were valid.
- CIP_CONWRKS-LOSTCOMM: Lost communication with console

LINUX

- CIP_LNX26_DRV_CPQFCTSWORK_01916: ERROR: Login Payload unacceptable!
- CIP_LNX26_DRV_QLOGICFC_01058: qllogicfc[- 0-9]+ : Error performing port login [0-9a-f]+

SOLARIS

- CIP_SOL_CONSLOGIJMQK: console login: JMQKKP
- CIP_SOL_SUSUROOTSUCC: su: 'su root' succeeded for login on /dev/pts/ int CIP_T64U_BADLOGIN: Login incorrect

OPENVMS

- CIP_VMS_LOGIN-RESTRICT: RESTRICT, you are not authorized to login from this source

WINDOWS

- CIP_WIN_100_MSFTPSVC: The server was unable to logon the Windows NT account 'anonymous@ftp.microsoft.
- CIP_WIN_1012_TERMSERVICE: Remote session from client name %COMPUTERNAME% exceeded the maximum allowed failed logon attempts.
- CIP_WIN_5516_NETLOGON: The computer or domain <domain1> trusts domain <domain2>. This may be an indirect trust.
- CIP_WIN_610_SECURITY: New Trusted Domain:
- CIP_WIN_611_SECURITY: Removing Trusted Domain:
- CIP_WIN_680_SECURITY: Account Used for Logon by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Account Name: Derek Workstation: DESKTOP01

CIP-005-1 R3.2: Monitoring Electronic Access: Unauthorized Access

CISCO

- CIP_CISCO_FW_TCP_MJRDOMO_EXEC: %FW-4- TCP_MAJORDOMO_EXEC_BUG: Majordomo Execute Attack - from <IP_address> to <IP_address>
- CIP_CISCO_FW_TCP_SENDEM_BAD_CMD: %FW-4- TCP_SENDMAIL_INVALID_COMMAND: Invalid SMTP command - <IP_address> to <IP_address>
- CIP_CISCO_FW_TCP_SENDEM_BAD_F: %FW-4- TCP_SENDMAIL_BAD_FROM_SIG: Sendmail Invalid Sender - from <IP_address> to <IP_address>
- CIP_CISCO_FW_TCP_SENDEM_BAD_TO: %FW-4- TCP_SENDMAIL_BAD_TO_SIG: Sendmail Invalid Recipient - from <IP_address> to <IP_address>
- CIP_CISCO_FW_TCP_SENDEM_DECODE: %FW-4- TCP_SENDMAIL_DECODE: Sendmail Decode Alias - from <IP_address> to <IP_address>
- CIP_CISCO_FW_TCP_SENDEM_OLD_SIG: %FW-4- TCP_SENDMAIL_OLD_SIG: Archaic Sendmail Attacks - from <IP_address> to <IP_address>

- CIP_CISCO_IDS_HTTP_BASIC_AUTH: IDS-4-
HTTP_BASIC_AUTH_OVFLOW_SIG: Sig:5055:HTTP Basic Authentication Overflow - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_IIS_DOTDOT: %IDS-4-
HTTP_IIS_DOTDOT_EXE_SIG: Sig:3215:IIS DOT DOT EXECUTE Attack - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_ACDSDDL: IDS-4-
HTTP_WWW_MSACSDLL_SIG: Sig:5071:WWW msacds.dll Attack - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_ANYFORM: %IDS-4-
HTTP_WWW_ANYFORM_SIG: Sig:5041:WWW anyform attack - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_COLDFUS: %IDS-4-
HTTP_WWW_COLDFUSION_SIG: Sig:5043:WWW Cold Fusion Attack - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_CTCGI: %IDS-4-
HTTP_WWW_COUNT_CGI_OVFLOW_SIG: Sig:3233:WWW count-cgi Overflow - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_FLD_OF: %IDS-4-
HTTP_WWW_HOST_FIELD_OVFLOW_SIG: Sig:5123:WWW Host Field overflow - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_FRONTTPG: %IDS-4-
HTTP_WWW_FRONTPAGE_HTIMAGE_SIG: Sig:5090:WWW FrontPage htimage.exe Access - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_IIS_HTR: %IDS-4-
HTTP_WWW_IIS_HTR_OVFLOW_SIG: Sig:5050:WWW IIS .htr Overflow Attack - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_IIS_NEW: %IDS-4-
HTTP_WWW_IIS_NEWSN_SIG: Sig:5034:WWW IIS newdsn attack - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_IIS_UNI: %IDS-4-
HTTP_WWW_IIS_UNICODE_SIG: Sig:5114:WWW IIS Unicode Attack - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_WEBCOM: IDS-4-
HTTP_WWW_WEBCOMSE_GUESTBOOK_SIG: Sig:5044:WWW Webcom.se Guestbook Attack - from <IP_address> to <IP_address>

- CIP_CISCO_IDS_HTTP_WWW_WINNTCM: %IDS-4-
HTTP_WWW_WINNT_CMDEXE_SIG: Sig:5081:WWW WinNT cmd.exe
Access - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_HTTP_WWW_XTM_DI: %IDS-4-
HTTP_WWW_XTERM_DISP_SIG: Sig:5045:WWW xterm display
attack - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_ICMP_PING_OF_DTH: %IDS-4-
ICMP_PING_OF_DEATH_SIG: Sig:2154:ICMP Ping of Death
Attack - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_IPFRAG_ATTACK: %IDS-4-IPFRAG_ATTACK_SIG:
Sig:1100:IP Fragment Attack - from <IP_address> to
<IP_address>
- CIP_CISCO_IDS_TCP_MAJORDOMO: %IDS-4-
TCP_MAJORDOMO_EXEC_BUG: Sig:3107:Majordomo Execute
Attack - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_TCP_SENDMAIL_BN: %IDS-4-
TCP_SENDMAIL_BOUNCE_SIG: Sig:3100:Smail Attack - from
<IP_address> to <IP_address>
- CIP_CISCO_IDS_TCP_SENDMAIL_SIG: %IDS-4-
TCP_SENDMAIL_OLD_SIG: Sig:3104:Archaic Sendmail
Attacks - from <IP_address> to <IP_address>
- CIP_CISCO_IDS_TCP_SYN_ATTACK: %IDS-4-
TCP_SYN_ATTACK_SIG: Sig:3050:Half-Open Syn Flood - from
<IP_address> to <IP_address>
- CIP_CISCO_SSH_DEATTACK: %SSH-4-DEATTACK: CRC-32
compensation attack detected src <IP_address> dst
<IP_address>, attack thwarted. Connection is closed.

CISCO PIX

- CIP_PIX_106017: Deny IP due to Land Attack from
IP_address to IP_address
- CIP_PIX_400007: IP Fragment Attack (signature 1100 -
Attack)
- CIP_PIX_400008: IP Impossible Packet (signature 1102 -
Attack)

- CIP_PIX_400009: IP Fragments Overlap (signature 1103 - Attack)
- CIP_PIX_400023: Fragmented ICMP Traffic (signature 2150 - Attack)
- CIP_PIX_400024: Large ICMP Traffic (signature 2151 - Attack)
- CIP_PIX_400025: Ping of Death Attack (signature 2154 - Attack)
- CIP_PIX_400026: TCP NULL flags (signature 3040 - Attack)
- CIP_PIX_400027: TCP SYN+FIN flags (signature 3041 - Attack)
- CIP_PIX_400028: TCP FIN only flags (signature 3042 - Attack)
- CIP_PIX_400031: UDP Bomb attack (signature 4050 - Attack)

CIP-007-1 R2.1: Ports and Services: Enabled Ports

AIX

- CIP_AIX_RESTROOTREMO2073: 0022-383 Restricted root remote command mode must be enabled before choosing secrshell as a remote command method.

WINDOWS

- CIP_WIN_11001_MICROSOFT: Microsoft Firewall failed. The failure occurred during Initialization of reverse Network Address Translation (NAT).

CIP-007-1 R2.2: Ports and Services: Disabled Ports

CISCO

- CIP_CISCO_SSH_DISABLED: %SSH-5-DISABLED: SSH <dec>.<dec> has been disabled CIP_PIX_605004: Login denied from {source_address/source_port | serial} to {interface_name:dest_address/service | console} for user "user"

CISCO PIX

- CIP_PIX_605005: Login permitted from {source_address/source_port | serial} to {interface_name:dest_address/service | console} for user "user"
- CIP_PIX_710002: {TCP|UDP} access permitted from source_address/source_port to interface_name:dest_address/service
- CIP_PIX_710003: {TCP|UDP} access denied by ACL from source_address/source_port to interface_name:dest_address/service

SOLARIS

- CIP_SOL_ACCEVIOLUNKN: access violation unknown host IP address
- CIP_SOL_CONNFROMUAUT: connect from hostIP to request from unauthorized host
- CIP_SOL_CONNFROMUPRV: connect from hostIP to request from unprivileged port
- CIP_SOL_CONNREFUMESS: Connection refused

OPENVMS

- CIP_VMS_LOGIN-NOEXTAUTH: NOEXTAUTH, external authentication service disabled or unavailable
- CIP_VMS_SYSTEM-IVACMODE: IVACMODE, invalid access mode specified

CIP-007-1 R2.3: Ports and Services: Exceptions

CISCO PIX

- CIP_PIX_400032:UDP Snork attack (signature 4051 - Attack)
- CIP_PIX_400033:UDP Chargen DoS attack (signature 4052 - Informational)
- CIP_PIX_400041:Proxied RPC Request (signature 6103 - Attack)
- CIP_PIX_400050:statd Buffer Overflow (signature 6190 - Attack)

TRU64

- CIP_T64U_NFSUNPRIV:NFS request from unprivileged port, source IP address = n

CIP-007-1 R3.1: Security Patch Management: Applicability

WINDOWS

- CIP_WIN_59_LIVEUPDATE:Error 6004: Internal Authentication Failed for the <path>\luadmin\temp

CIP-007-1 R5.1: Account Management: User Accounts

HPUX

- CIP_HPUX11_PRM-409:User <string> does not have permission to move process <num>.
- CIP_HPUX11_PRM-411:User <string> does not have permission to move user <string>.
- CIP_HPUX11_PRM-412:User <string> does not have permission to use group <string>.

OPENVMS

- CIP_VMS_SYSTEM-NOENTRY:NOENTRY, access control entry not found
- CIP_VMS_SYSTEM-NOEXQUOTA:NOEXQUOTA, operation requires EXQUOTA privilege
- CIP_VMS_SYSTEM-NOPRIV:NOPRIV, insufficient privilege or object protection violation
- CIP_VMS_SYSTEM-NORDACC:NORDACC, read access denied
- CIP_VMS_SYSTEM-NOSECURITY:NOSECURITY, operation requires SECURITY privilege
- CIP_VMS_SYSTEM-NOSUCHUSER:NOSUCHUSER, login information not recognized at remote node
- CIP_VMS_SYSTEM-NOWRTACC:NOWRTACC, write access denied
- CIP_VMS_SYSTEM-PROTVIO:PROTVIO, file protection prohibits the type of access requested
- CIP_VMS_SYSTEM-WRONGACMODE:WRONGACMODE, operation attempted from insufficiently privileged access mode

CIP-007-1
R5.1.1:

Account Management: User Accounts: Implementation

CONSOLEWORKS SERVER

- CIP_CONWRKS-EAUSRCREFAIL: External authentication tried to create a new user but failed.

OPENVMS

- CIP_VMS_LOGIN-BADDAY:BADDAY, you are not authorized to login today
- CIP_VMS_LOGIN-BADHOUR:BADHOUR, you are not authorized to login at this time
- CIP_VMS_LOGIN-DEFCLI:DEFCLI, you are not authorized to specify CLI parameters

- CIP_VMS_LOGIN-DISRECONNECT: DISRECONNECT, you are not authorized to do reconnections
- CIP_VMS_LOGIN-DISUSER: DISUSER, account is disabled
- CIP_VMS_LOGIN-FRCPWDERR: FRCPWDERR, error changing expired password
- CIP_VMS_SECSRV-BADLOCALUSERLEN: BADLOCALUSERLEN, local user name length is out of range
- CIP_VMS_SECSRV-BADNODENAMELEN: BADNODENAMELEN, remote node name length is out of range
- CIP_VMS_SECSRV-BADREMUSERLEN: BADREMUSERLEN, remote user name length is out of range
- CIP_VMS_SECSRV-DUPLICATEUSER: DUPLICATEUSER, username already exists in the proxy record

**CIP-007-1
R5.1.2:**

Account Management: User Accounts: Audit Trails

SOLARIS

- CIP_SOL_ROOTLOGIDEVC: ROOT LOGIN /dev/console
- CIP_SOL_ROOTLOGIDEVP: ROOT LOGIN /dev/pts/ int FROM string
- CIP_SOL_SUSUROOTFAIL: su: 'su root' failed for login on /dev/pts/ int

TRU64

- CIP_T64U_CATFTPALI: ANONYMOUS FTP LOGIN FROM <node>, id=<uid>
- CIP_T64U_NFSAUTHGET: authget: unknown authflavor nauthflavor
- CIP_T64U_SUSUSU: su: SU <Username> on <terminal>
- CIP_T64U_UUCPBLIMCMB: BAD LOGIN/MACHINE COMBINATION
- CIP_T64U_UUCPLGINFL: LOGIN FAILED
- CIP_T64U_UUCPRMRJCAL: REMOTE REJECT AFTER LOGIN

OPENVMS

- CIP_VMS_AUDSRV-NEWSERVERDB:NEWSERVERDB, new audit server database created
- CIP_VMS_AUDSRV-NEW_FILE:NEW_FILE, now analyzing file 'file-name'
- CIP_VMS_AUDSRV-OBSERVERDB:OBSERVERDB, obsolete audit server database 'n.n' encountered
- CIP_VMS_AUDSRV-ODB_NAC:ODB_NAC, cannot access object database
- CIP_VMS_AUDSRV-OLDPURGE:OLDPURGE, security auditing resources exhausted; oldest message purged
- CIP_VMS_AUDSRV-PEXFULL:PEXFULL, process exclusion list full; requestor PID: 'pid'
- CIP_VMS_AUDSRV-REMARCEST:REMARCEST, remote archive link established ('n' messages 'n' lost)
- CIP_VMS_RMS-ACC:ACC, ACP file access failed
- CIP_VMS_RMS-DEL:DEL, RFA-accessed record was deleted
- CIP_VMS_RMS-FAC:FAC, record operation not permitted by specified file access (FAC)
- CIP_VMS_RMS-PRV:PRV, insufficient privilege or file protection violation
- CIP_VMS_SYSTEM-NOAUDIT:NOAUDIT, operation requires AUDIT privilege
- CIP_VMS_SYSTEM-NOCMKRNL:NOCMKRNL, operation requires CMKRNL privilege

WINDOWS

- CIP_WIN_576_SECURITY:Special privileges assigned to ew logon:
- CIP_WIN_608_SECURITY:User Right Assigned:
- CIP_WIN_681_SECURITY:The logon to account: <account name>

- CIP_WIN_7013_SERVICE: Logon attempt with current password failed with the following error: Logon failure: unknown user name or bad password.

CIP-007-1 R5.2: Account Management: Acceptable Use

AIX

- CIP_AIX_EFFEUSERIDMU4204: 2511-206 Effective user id must be root to execute.
- CIP_AIX_INSTMUSTBERU1523: 0018-231 Install must be run with root authority.
- CIP_AIX_OFFLMUSTBERU1525: 0018-233 Offline must be run with root authority.
- CIP_AIX_ONLIMUSTBERU1526: 0018-234 Online must be run with root authority.
- CIP_AIX_ONLYTHERUSER0177: 0821-058 Only the root user can set network options
- CIP_AIX_PERMDENIYOU2482: 0027-113 Permission denied; you must be the root user to execute.
- CIP_AIX_PERMDENIYOU3971: 2509-001 Permission denied. You must be the root user to set the virtual host name.
- CIP_AIX_PERMDENIYOU3976: 2509-032 Permission denied. You must be the root user to run this command.
- CIP_AIX_REMOMUSTBERU1528: 0018-236 Remove must be run with root authority.
- CIP_AIX_REQUOPERREQU4229: 2511-514 Requested operation requires authority type authority, or the effective user id of the client must be root.

CISCO

- CIP_CISCO_APAUPROXY_RETR_0205: %AP-1-AUTH_PROXY_RETRIES_EXCEEDED: IP-address <IP_address> has exceeded the maximum retry limit

SOLARIS

- CIP_SOL_FAILTOLOSECU: Failed to Load Security Policy: Invalid argument

WINDOWS

- CIP_WIN_2_IAS: User <username> was denied access.
- CIP_WIN_3036_MRXSMB: The redirector detected a security signature mismatch. The connection has been disconnected.
- CIP_WIN_3210_NETLOGON: Failed to authenticate with \

**CIP-007-1
R5.2.1:**

Account Management: Acceptable Use: Policy

HPUX

- CIP_HPUX11_PRM-402: <string> not a recognized user name.
- CIP_HPUX11_PRM-403: Could not find access list for user <string>.
- CIP_HPUX11_PRM-818: Could not find user <string> in the configuration file.
- CIP_HPUX11_SNAP3270-NOCFGUSRID: User ID userid not found in configuration file

SOLARIS

- CIP_SOL_LOGIINCOMESS: Login incorrect

OPENVMS

- CIP_VMS_JBC-DELACCESS: DELACCESS, file protection does not allow delete access
- CIP_VMS_LOGIN-NOSUCHUSER: NOSUCHUSER, no such user

- CIP_VMS_LOGIN-NOTVALID:NOTVALID, user authorization failure
- CIP_VMS_LOGIN-USERAUTH:USERAUTH, error accessing authorization record
- CIP_VMS_SECSRV-INVALIDDELETE:INVALIDDELETE, you cannot delete the only user in a record; you must delete the entire record
- CIP_VMS_SECSRV-NOSUCHUSER:NOSUCHUSER, no user matches your specification
- CIP_VMS_SECSRV-TOOMANYUSERS:TOOMANYUSERS, proxy already has the maximum number of associated users

WINDOWS

- CIP_WIN_100_W3SVC:The server was unable to logon the Windows NT account '<user name>' due to the following error: <error description>.
- CIP_WIN_624_SECURITY:Description: User Account Created:
- CIP_WIN_625_SECURITY:Description: User Account Type Change:
- CIP_WIN_626_SECURITY:User Account Enabled:
- CIP_WIN_629_SECURITY:User Account Disabled:
- CIP_WIN_630_SECURITY:User Account Deleted:
- CIP_WIN_631_SECURITY:Global Group Created:
- CIP_WIN_632_SECURITY:Global Group Member Added:
- CIP_WIN_633_SECURITY:Global Group Member Removed:
- CIP_WIN_634_SECURITY:Global Group Deleted:
- CIP_WIN_635_SECURITY:Local Group Created:
- CIP_WIN_642_SECURITY:User Account Changed:
- CIP_WIN_646_SECURITY:Computer Account Changed: -

**CIP-007-1
R5.2.2:**

**Account Management: Acceptable Use: Shared
Account Access**

AIX

- CIP_AIX_ASECSERVCONF3649: 2502-624 A security services configuration file contains erroneous data. filename -- line number
- CIP_AIX_RECEPROPTOCH4475: 2521-049 Received proposal to change group security state to new group security state from provider EM daemon provider ID but local methods do not match. The local methods are local methods.
- CIP_AIX_RESEMUSTBERU1527: 0018-235 Reset must be run with root authority.
- CIP_AIX_ROPTREQUROOT4942: 2523-734 -r option requires root privilege.
- CIP_AIX_SCANMUSTBERU1529: 0018-237 Scan must be run with root authority.
- CIP_AIX_SECUFUNCFAIL4217: 2511-502 Security function() failing security function failed on host hostname - information about the failure.
- CIP_AIX_SPNATHISPROG3884: 2505-277 (sp_name) This program can only be run as root.
- CIP_AIX_THEEUSERIDOF4226: 2511-511 The effective user id of the client must be root.
- CIP_AIX_THESFUNCNAME4473: 2521-047 The security function name security function was unsuccessful.
- CIP_AIX_THESSERVENVI3645: 2502-620 The security services environment is damaged.
- CIP_AIX_TOSUCOMPTHIS3267: 0037-220 To successfully complete this test, it must be run as root.
- CIP_AIX_UPDAMUSTBERU1532: 0018-240 Update must be run with root authority.
- CIP_AIX_YOUMBEROTORU1574: 0018-291 You must be root to run this command.
- CIP_AIX_YOUMBEROTORU1597: 0019-017 You must be root to run this command.

- CIP_AIX_YOUMBEROTOUS0179:0821-073 You must be root to use the -f option
- CIP_AIX_YOUMHAVEROOT2878:0034-180 You must have root authority to run this command.

CISCO

- CIP_CISCO_CASA_SECURITY_FAIL:%CASA-4-SECURITY_FAIL:
<chars> security information in CASA packet.
- CIP_CISCO_CRYPTOA_IA_ENABLE:%CRYPTO-4-IA_ENABLE:
Security warning: crypto ipsec optional is configured
- CIP_CISCO_IPMOBILE_SECURE:%IPMOBILE-6-SECURE: Security violation on <chars> from <chars> <chars> - errcode <chars> (<dec>), reason <chars> (<dec>)

HPUX

- CIP_HPUX11_PRM-1522:illegal user <string>
- CIP_HPUX11_PRM-1601:error: must be root to execute
- CIP_HPUX11_PRM-228:You must be superuser to use -d, -e, -i, -k,-r, -u, -I, -L. or -M.

LINUX

- CIP_LNX26_DRV_OSST_04847:osst[- 0-9]+:W:
MTSETDRVBUFFER only allowed for root\.
- CIP_LNX26_DRV_ST_03157:st[- 0-9]+:MTSETDRVBUFFER only allowed for root\.

CISCO PIX

- CIP_PIX_106101:The number of ACL log deny-flows has reached limit (number).

SOLARIS

- CIP_SOL_ERROCODEACCE: error code 2: access violation
- CIP_SOL_NISAFILENTR: NIS+ authentication failure
- CIP_SOL_NOTLSHELMESS: Not login shell
- CIP_SOL_SECUEXCEONHO: security exception on host string . USER ACCESS DENIED.
- CIP_SOL_SECUSERVFAIL: 550 Security server failed to perform requested command

OPENVMS

- CIP_VMS_AMDS-ACCVIO: ACCVIO, access violation executing program 'string' request for node 'string'
- CIP_VMS_AMDS-NOSECACC: NOSECACC, insufficient privilege to access security file
- CIP_VMS_AMDS-RMSNOPRIV: RMSNOPRIV, insufficient privilege to access program library AMDS\$'string'VMS-'string'.LIB
- CIP_VMS_AUDSRV-NEWIGNORE: NEWIGNORE, security auditing resources exhausted; new message ignored
- CIP_VMS_AUDSRV-NOOPCOM: NOOPCOM, OPCOM not running at 'time'; security alarms may be lost
- CIP_VMS_AUDSRV-NORESTART: NORESTART, error 'status' attempting to restart server
- CIP_VMS_AUDSRV-RESUME: RESUME, system operation resumed; security auditing resources available
- CIP_VMS_ECSRV-ASSIGNFAILED: ASSIGNFAILED, security server failed to assign a channel to a client reply mailbox
- CIP_VMS_JBC-RESTRICT: RESTRICT, UAF restricts access at this time, please log out immediately
- CIP_VMS_SECSRV-QIOFAILED: QIOFAILED, security server QIO on client mailbox failed

- CIP_VMS_SYSTEM-ACLEEMPTY:ACLEEMPTY, access control list is empty
- CIP_VMS_SYSTEM-ACLFULL:ACLFULL, ACL is full
- CIP_VMS_SYSTEM-INVLOGIN:INVLOGIN, login information invalid at remote node

WINDOWS

- CIP_WIN_636_SECURITY:Local Group Member Added:
- CIP_WIN_637_SECURITY:Local Group Member Removed:
- CIP_WIN_638_SECURITY:Local Group Deleted:
- CIP_WIN_639_SECURITY:Local Group Changed:
- CIP_WIN_641_SECURITY:Global Group Changed:
- CIP_WIN_7005_SERVICE:The RpcImpersonateClient call failed with the following error: No security context is available to allow impersonation.

CIP-007-1 R5.3: Account Management: Password Use

AIX

- CIP_AIX_CANNEXECCOMM4247:2515-018 Cannot execute command for subscription Subscription handle name, because the subscription owner is not authorized to run as the target AIX user AIX user name.

OPENVMS

- CIP_VMS_LOGIN-INVPWD: INVPWD, invalid password

CIP-007-1 R5.3.3:

Account Management: Password Use: Expiration

OPENVMS

- CIP_VMS_LOGIN-PWDEXPIR:PWDEXPIR, your password has expired - contact your system manager

CIP-007-1 R6.1: Security Status Monitoring: Process

OPENVMS

- CIP_VMS_AUDSRV-RESCRASH: RESCRASH, resources exhausted; server restarting
- CIP_VMS_AUDSRV-RESCRITICAL: RESCRITICAL, security auditing resources exhausted on journal 'name'

CIP-007-1 R6.2: Security Status Monitoring: Alerts

AIX

- CIP_AIX_CANNSTOROOT0217: 3004-501 Cannot su to root: Authentication is denied - or Account has expired?
- CIP_AIX_PERMISDEEVEN0183: 0821-233 Permission is denied

HPUX

- CIP_HPUX11_PRM-401: Warning! All root processes with pid > 0 have been moved to group <string>.

SOLARIS

- CIP_SOL_SUNOSHELMESS: su: No shell

OPENVMS

- CIP_VMS_SECSRV-NOSUCHPROXY: NOSUCHPROXY, no proxy record matches your specification

WINDOWS

- CIP_WIN_3224_NETLOGON: Changing machine account password for account <computer name>\$ failed with the following error: The system # See INFO file #

- CIP_WIN_34_TERMSERVICE: {Access Denied} A process has requested access to an object, but has not been granted those access rights.
- CIP_WIN_40960_LSASRV: The Security System detected an attempted downgrade attack for server <server name>.
- CIP_WIN_40961_LSASRV: The Security System could not establish a secured connection with the server <server name>.
- CIP_WIN_5000_LSASRV: The security package <security package name> generated an exception. The package is now disabled.
- CIP_WIN_517_SECURITY: The audit log was cleared Primary User Name: SYSTEM Primary Domain: NT AUTHORITY Primary Logon ID: # See INFO file #
- CIP_WIN_5705_NETLOGON: The change log cache maintained by the Netlogon service for database changes is corrupted.
- CIP_WIN_5723_NETLOGON: The session setup from the computer <computer name> failed because there is no trust account in the security # See INFO file #
- CIP_WIN_617_SECURITY: Kerberos Policy Changed: Changed By: User Name: APPSERVER\$ Domain Name: ALTDOMAIN Logon ID: (0x0,0x3E7) # See INFO file #
- CIP_WIN_627_SECURITY: Change Password Attempt: Target Account Name: mshino Target Domain: CORPDOM Target Account ID: # See INFO file #
- CIP_WIN_628_SECURITY: User Account password set: Target Account Name: CORPSMTP01\$ Target Domain: CORP Target Account ID: # See INFO file #
- CIP_WIN_640_SECURITY: General Account Database Change:
- CIP_WIN_643_SECURITY: Domain Policy Changed:

CIP-007-1 R6.3: Security Status Monitoring: Security Logs

AIX

- CIP_AIX_USERCANNBEAU2350:0026-412 User cannot be authenticated on hostname. SP Security Services error code: error code SP Security Services error message: error message

CISCO

- CIP_CISCO_AAAA_BADAUTHENSTR: %AAA-3-BADAUTHENSTR: Bad authentication data: <chars>
- CIP_CISCO_APAUPROXY_DDOS_ATTK: %AP-1-AUTH_PROXY_DDOS_ATTACK: Distributed DOS attack
- CIP_CISCO_APAUPROXY_DOS_ATTK: %AP-1-AUTH_PROXY_DOS_ATTACK: Possible DOS attack from source IP-address <IP_address>
- CIP_CISCO_SNASW_DS_LOG_26: SNASW-3-DS_LOG_26: PROBLEM - <int> - Unable to register resources because this node is not authorised at the network node server <chars>
- CIP_CISCO_SNASW_DS_LOG_33: SNASW-3-DS_LOG_33: PROBLEM - <int> - Unable to delete resources because this node is not authorised at the network node server <chars>

CISCO PIX

- CIP_PIX_109010: Auth from inside_address/inside_port to outside_address/outside_port failed (too many pending auths) on interface interface_name.

OPENVMS

- CIP_VMS_AUDSRV-REMARCFAIL: REMARCFAIL, remote archive link failure; archive messages will be lost (status: 'status')
- CIP_VMS_AUDSRV-REMARCNVL: REMARCNVL, remote archive link not available; archive messages will be lost

- CIP_VMS_AUDSRV-REMARCASTS:REMARCASTS, remote archive link not available ('n' messages lost)
- CIP_VMS_AUDSRV-REMDISABLED:REMDISABLED, resource monitoring disabled for journal 'name'
- CIP_VMS_AUDSRV-REMENABLED:REMENABLED, resource monitoring enabled for journal 'name'
- CIP_VMS_AUDSRV-REMNOTENAB:REMNOTENAB, resource monitoring not enabled for journal 'name'
- CIP_VMS_AUDSRV-RESDISMISS:RESDISMISS, resource exhaustion condition dismissed on journal 'name'
- CIP_VMS_AUDSRV-RESINFO:RESINFO, resource information: 'n' blocks needed, 'n' blocks available
- CIP_VMS_AUDSRV-RESNOTDISK:RESNOTDISK, resource monitoring ignored for journal 'name'; journal is directed to an invalid device type
- CIP_VMS_AUDSRV-RESOKAY:RESOKAY, free resources available on journal 'name'
- CIP_VMS_AUDSRV-RESTART:RESTART, audit server restart requested
- CIP_VMS_AUDSRV-RESUMEFAIL:RESUMEFAIL, system operation not resumed; resource condition still exists on journal 'name'
- CIP_VMS_AUDSRV-RESUMEWARN:RESUMEWARN, resource exhaustion condition dismissed (with resources still low) on journal 'name'
- CIP_VMS_AUDSRV-RESWARNING:RESWARNING, resource warning condition exists on journal 'name'
- CIP_VMS_AUDSRV-SERVEREXIT:SERVEREXIT, requested audit server shut down
- CIP_VMS_AUDSRV-SNDOPRERR:SNDOPRERR, error (%X'hex-value') returned from \$SNDOPR; alarm may not be received on remote nodes
- CIP_VMS_AUDSRV-SUSPEND:SUSPEND, system operation suspended; security auditing resources exhausted

- CIP_VMS_AUDSRV-SYSJNLFULL:SYSJNLFULL, device full error on journal SECURITY; automatic server restart suppressed
- CIP_VMS_AUDSRV-SYSJNLNAC:SYSJNLNAC, cannot access system audit journal 'name'
- CIP_VMS_CAF-NEEDBOTH:NEEDBOTH, no authorization file - need both a password and group number
- CIP_VMS_CAF-NONEXIST:NONEXIST, authorization file does not exist
- CIP_VMS_CAF-NOPRIV:NOPRIV, operation requires SYSPRV privilege
- CIP_VMS_LAT-LRJACCESSDENIED:LRJACCESSDENIED, access denied
- CIP_VMS_LAT-LRJACCESSREJECT:LRJACCESSREJECT, immediate access is rejected
- CIP_VMS_LOGIN-ACNTEXC:ACNTEXC, you are at maximum allowed processes for your account name
- CIP_VMS_LOGIN-EVADE:EVADE, breakin evasion in effect
- CIP_VMS_LOGIN-FILEACC:FILEACC, error accessing system authorization file
- CIP_VMS_LOGIN-INVINPUT:INVINPUT, invalid SYS\$INPUT for interactive login
- CIP_VMS_LOGIN-NETUAFACC:NETUAFACC, error accessing network authorization file
- CIP_VMS_LOGIN-NOLOCAUTH:NOLOCAUTH, not authorized to override external authentication
- CIP_VMS_SECAUDEXH:Security auditing shutdown due to resource exhaustion
- CIP_VMS_SECAUDTCB:Security auditing failure reported by TCB
- CIP_VMS_SECIPLHIGH:Security subsystem detected IPL too high
- CIP_VMS_SECREFNAG:Section reference count went negative

- CIP_VMS_SECSRV-AUDITFAILED: AUDITFAILED, security server failed to audit an event because of the following error:
- CIP_VMS_SECSRV-BADJOBTYPE: BADJOBTYPE, an invalid job type was used to audit a login failure or breakin attempt
- CIP_VMS_SECSRV-CIADBEMPTY: CIADBEMPTY, no intruders or suspects currently exist
- CIP_VMS_SECSRV-CIASHUTDOWN: CIASHUTDOWN, breakin detection and evasion processing is shutting down
- CIP_VMS_SECSRV-CIASTARTINGUP: CIASTARTINGUP, breakin detection and evasion processing now starting up
- CIP_VMS_SECSRV-CIATERMINATED: CIATERMINATED, an error caused breakin detection and evasion processing to terminate
- CIP_VMS_SECSRV-CONSTERROR: CONSTERROR, security server experienced a CONSTRAINT_ERROR exception
- CIP_VMS_SECSRV-CONVERT: CONVERT, converting proxy database to new format
- CIP_VMS_SECSRV-CONVERT_SUCCESS: CONVERT_SUCCESS, conversion of proxy database to new format was successful
- CIP_VMS_SECSRV-COULDNTRESTART: COULDNTRESTART, security server cannot restart because of the following error:
- CIP_VMS_SECSRV-COULDNTSTART: COULDNTSTART, security server cannot start functioning properly
- CIP_VMS_SECSRV-CREATEPROXYDB: CREATEPROXYDB, attempting to create proxy database
- CIP_VMS_SECSRV-CREMBXFAILED: CREMBXFAILED, security server failed to create input mailbox
- CIP_VMS_SECSRV-DASSGNFAILED: DASSGNFAILED, security server could not deassign a channel to a client reply mailbox
- CIP_VMS_SECSRV-DBALREADYEXISTS: DBALREADYEXISTS, proxy database already exists

- CIP_VMS_SECSRV-INSUFINFO: INSUFINFO, not enough information to produce a breakin record
- CIP_VMS_SECSRV-INTRUDER: INTRUDER, matching intruder found
- CIP_VMS_SECSRV-INVALIDTERMNAME: INVALIDTERMNAME, received invalid terminal name for intruder/suspect
- CIP_VMS_SECSRV-NOPROXYDB: NOPROXYDB, cannot find proxy database file NET\$PROXY.DAT
- CIP_VMS_SECSRV-NORDPROXYREC: NORDPROXYREC, proxy record is internally inconsistent; cannot read it
- CIP_VMS_SECSRV-NOSCANNEDINTRUDE: NOSCANNEDINTRUDER, no matching intruder or suspect found
- CIP_VMS_SECSRV-NOSUCHINTRUDER: NOSUCHINTRUDER, no intruder or suspect matches your specification
- CIP_VMS_SECSRV-OUTCOMTERMINATED: OUTCOMTERMINATED, security server's outgoing message mechanism failed and is exiting
- CIP_VMS_SECSRV-PROXYACTIVE: PROXYACTIVE, proxy processing is active; you must shut down proxy processing to perform this action
- CIP_VMS_SECSRV-PROXYMODIFIED: PROXYMODIFIED, existing proxy entry modified
- CIP_VMS_SECSRV-PROXYNOTACTIVE: PROXYNOTACTIVE, proxy processing is not currently active
- CIP_VMS_SECSRV-PROXYNOTOPEN: PROXYNOTOPEN, cannot open proxy database
- CIP_VMS_SECSRV-PROXYSHUTDOWN: PROXYSHUTDOWN, proxy processing is shutting down
- CIP_VMS_SECSRV-PROXYSTARTINGUP: PROXYSTARTINGUP, proxy processing now starting up
- CIP_VMS_SECSRV-PROXYTERMINATED: PROXYTERMINATED, an error caused proxy processing to terminate
- CIP_VMS_SECSRV-RUNNING: RUNNING, security server is already running; it will not be restarted

- CIP_VMS_SECSRV-SERVERNOTACTIVE: SERVERNOTACTIVE, security server is not active
- CIP_VMS_SECSRV-SERVERRESTART: SERVERRESTART, security server restarting
- CIP_VMS_SECSRV-SERVERSHUTDOWN: SERVERSHUTDOWN, security server shutting down
- CIP_VMS_SECSRV-SERVERSTARTINGUP: SERVERSTARTINGUP, security server starting up
- CIP_VMS_SECSRV-SERVERTERMINATED: SERVERTERMINATED, an error caused the security server to terminate
- CIP_VMS_SECSRV-SRVREPLYTIMEOUT: SRVREPLYTIMEOUT, timed out waiting for reply from security server
- CIP_VMS_SECSRV-SUSPECT: SUSPECT, matching suspect found
- CIP_VMS_SECSRV-TASKERROR: TASKERROR, security server experienced a TASKING_ERROR exception
- CIP_VMS_SECSRV-VERIFY_CONVERSIO: VERIFY_CONVERSION, verifying that proxy database conversion is correct
- CIP_VMS_SMI-NOOPER: NOOPER, OPER privilege required on all nodes, access rejected
- CIP_VMS_SYSTEM-EVTNOTENAB: EVTNOTENAB, security auditing event not enabled
- CIP_VMS_SYSTEM-INVAJLNAM: INVAJLNAM, invalid security audit journal name
- CIP_VMS_SYSTEM-MMATORB: MMATORB, selected security object mismatch
- CIP_VMS_SYSTEM-OBJNOTLOCKED: OBJNOTLOCKED, security object context is not write-locked
- CIP_VMS_SYSTEM-OVRMAXAUD: OVRMAXAUD, maximum security audit message size exceeded
- CIP_VMS_SYSTEM-TOOMANYAJL: TOOMANYAJL, too many security audit journals encountered

WINDOWS

- CIP_WIN_1202_SCECLI: Security policies are propagated with warning. <error code>: <error description>.
- CIP_WIN_14_IAS: A request was received with an authenticator that is not valid from client <friendly client name>
- CIP_WIN_1508_USERENV: windows was unable to load the registry. This is often caused by insufficient memory or insufficient security rights.
- CIP_WIN_2044_MSMQ: The Message Queuing service has insufficient privileges to create audit log messages.
- CIP_WIN_3051_NETLOGON: The registry or the information you just typed includes an illegal value for "DBFlag";.
- CIP_WIN_514_SECURITY: An authentication package has been loaded by the Local Security Authority.
- CIP_WIN_515_SECURITY: A trusted logon process has registered with the Local Security Authority.
- CIP_WIN_516_SECURITY: Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
- CIP_WIN_518_SECURITY: A notification package has been loaded by the Security Account Manager.
- CIP_WIN_528_SECURITY: Successful Logon:
- CIP_WIN_529_SECURITY: Logon Failure:
- CIP_WIN_530_SECURITY: Logon Failure:
- CIP_WIN_531_SECURITY: Logon Failure:
- CIP_WIN_532_SECURITY: Logon Failure:
- CIP_WIN_533_SECURITY: Logon Failure:
- CIP_WIN_534_SECURITY: Logon Failure:
- CIP_WIN_535_SECURITY: Logon Failure:
- CIP_WIN_536_SECURITY: Logon Failure:

- CIP_WIN_537_SECURITY: Logon Failure:
- CIP_WIN_538_SECURITY: User Logoff:
- CIP_WIN_539_SECURITY: Logon Failure:
- CIP_WIN_540_SECURITY: Successful Network Logon:
- CIP_WIN_5722_NETLOGON: The session setup from the computer TEST_COMP1 failed to authenticate.
- CIP_WIN_577_SECURITY: Privileged Service Called:
- CIP_WIN_612_SECURITY: Audit Policy Change:
- CIP_WIN_644_SECURITY: User Account Locked Out
- CIP_WIN_672_SECURITY: Authentication Ticket Granted:
- CIP_WIN_675_SECURITY: Pre-authentication failed: User Name: Administrator User ID: <user sid> Service Name: krbtgt/ALTDOMAIN.
- CIP_WIN_676_SECURITY: Authentication Ticket Request Failed: User Name: 248b-277-4\$ Supplied Realm Name: <domain name> Service Name: # See INFO file #
- CIP_WIN_8112_MSADC: The authentication package value (<value>) is not supported on server <server name>.

CIP-007-1 R6.4: Security Status Monitoring: Log Retention

CONSOLEWORKS SERVER

- CIP_CONWRKS-ALTLOGFAIL: Alternate logging directory invoked, but not valid.