



# Intellitactics SAFE LP

NERC CIP Report List



[www.intellitactics.com](http://www.intellitactics.com)

## **Copyright Information**

© 1998-2009 Intellitactics Inc. All rights reserved.

No part of this document may be reproduced in any form by any photographic, electronic, mechanical or other means, or used in any information storage and retrieval system, without prior written permission from Intellitactics Inc.

All other product and brand names in this document are trademarks or registered trademarks of their respective owners.

# NERC CIP Compliance Reports

## Access Control (CIP-003-1 R5)

Reports and Event Views supporting compliance with requirement R5 of NERC Standard CIP-003-1.

### Administration Access

#### Account Management by Selected Users

This report shows all management events performed against accounts or groups by the selected or excluded user within a specified time period. It is essential to enter a user value or select a list of users for the report to return data.

#### Administrative Users List

This report shows all administrative event activity, grouped by administrator, within a specified time period.

### DB Access

#### All Denied DB Login Attempts

This report shows all failed login attempts to database services within a specified time period. Any failed login attempts should be considered suspicious. This report is sorted by data module, and the number of attempts is also shown.

### **Logon to Selected DB Server by Selected Users**

This report shows hosts accessed by users within a specified time period. Although users have the system level access to sensitive databases, they should not be accessing them. Entering host or user values is optional.

### **New Users Accessing Databases**

This report shows users accessing a database server within a specified time period. Few users directly access databases, so any occurrences of this are worth reviewing.

### **Users Connecting to DB from New Sources**

This report shows users accessing a database server from a new client address within a specified time period.

## **File Access**

### **Denied File Access Summary**

This report shows a detailed summary of denied attempts, grouped by user, to access files within a specified time period. The objective is to find users who are attempting to misuse or exceed their rightful access.

### **Denied Files List**

This report shows files that users have unsuccessfully attempted to access, grouped by the originating IP address, within a specified time period. Files with very high numbers of attempts may be accessed by automated tools.

### **New Users of Selected Files**

This report shows users accessing selected files for the first time, within a specified time period. It is essential to enter a file name or select a list of files for the report to return data.

### **Selected File Accessed by New Program**

This report shows the access of selected files by new programs within a specified time period. Highly sensitive files are usually accessed in a limited number of ways, and any access by a new program should be reviewed. It is essential to enter a file name or select a list of files for the report to return data.

### **Selected Users Accessing Selected Files**

This report shows any users who accessed the selected files, within a specified time period. The report can be used to identify access to business files by privileged system users (such as administrators). It is essential to enter a file name or select a list of files for the report to return data. The report results are grouped by user.

### **Users Accessing Selected Files**

This report shows all users who have accessed the specified file(s) (which are usually sensitive resources) for the specified time period. It is essential to enter a file name or select a list of files for the report to return data. The results are grouped by file.

### **Users Accessing Selected Files (Detail)**

This report shows all users who have accessed the specified file(s) (which are usually sensitive resources) for the specified time period. It is essential to enter a file name or select a list of files for the report to return data. The results are grouped by file.

## **Login Access**

### **Authentication Failure for Selected Users**

This report shows files that users have unsuccessfully attempted to access within a specified time period. Files with very high numbers of attempts may be accessed by automated tools. It is essential to enter a user value, or select a list of users, for the report to return data.

### **Local Login to Selected Hosts**

This report shows local login attempts to selected hosts, such as critical servers, within a specified time period. It is essential to enter a host value or select a list of hosts for the report to return data.

### **Top Accounts Authenticating**

This report shows users with the highest successful login rates for the specified time period.

### **Top Accounts Failing to Authenticate**

This report shows the users with the highest rate of failed logins within a specified time period.

## **Account Management (CIP-007-1 R5)**

Reports and Event Views supporting compliance with requirement R5 of NERC Standard CIP-007-1.

### **Account Management by Selected Users**

This report shows all management events performed against accounts or groups by the selected or excluded user within a specified time period. It is essential to enter a user value or select a list of users for the report to return data.

### **Accounts Created**

This report shows all accounts created within a specified time period.

### **Accounts Deleted**

This report shows all accounts deleted within a specified time period.

### **Accounts Disabled**

This report shows all accounts disabled within a specified time period.

**Accounts Enabled**

This report shows all accounts enabled within a specified time period.

**Accounts Locked Out**

This report shows all accounts locked out within a specified time period.

**Accounts Modified**

This report shows all accounts modified within a specified time period.

**Accounts Modified by Owner**

This report shows all modification events performed by the selected account within a specified time period. It is essential to enter an account value or select a list of accounts for the report to return data.

**Accounts Unlocked**

This report shows all accounts unlocked within a specified time period.

**Group Members Added**

This report shows all groups that had members added within a specified time period.

**Group Members Removed**

This report shows all groups that had users removed within a specified time period.

**Groups Created**

This report shows all groups created within a specified time period.

## **Groups Deleted**

This report shows all groups deleted within a specified time period.

## **Groups Modified**

This report shows all groups modified within a specified time period.

## **Change and Configuration (CIP-003-1 R6)**

Reports and Event Views supporting compliance with requirement R6 of NERC Standard CIP-003-1.

## **Account Management by Selected Users**

This report shows all management events performed against accounts or groups by the selected or excluded user within a specified time period. It is essential to enter a user value or select a list of users for the report to return data.

## **Administrative Users List**

This report shows all administrative event activity, grouped by administrator, within a specified time period.

## **Critical Cyber Asset Identification (CIP-002-1 R3)**

Reports and Event Views supporting compliance with requirement R3 of NERC Standard CIP-002-1.

## **Asset Configuration for Selected Zone**

This report shows the assets and asset groups associated with the selected zone. User data restrictions are applied to this report by zone only.

## Entries in Selected List

This report shows the current contents of a selected dynamic list.

User data restrictions are not applied to this report.

## Electronic Security Perimeter (CIP-005-1 R1-R5)

Reports and Event Views supporting compliance with requirements of NERC Standard CIP-005-1.

## Network Traffic Analysis

### Connections to Services

This report shows the top client/server connections, such as the relationship between source, target host and port, within a specified time period.

### Denied Connections from Selected Hosts

This report shows all sources and ports that attempted to connect to selected hosts, within a specified time period. The report also shows any denied connections for the host. It is essential to enter a host or select a list of hosts for the report to return data.

### Event Type Sources

This report shows top source/event ID combinations of the selected events within a specified time period.

### Event Type Targets

This report shows the top targets/event IDs of the selected events within a specified time period.

### **Port Traffic Control**

This report shows events (by target port) to indicate which ports are blocking or allowing events, within a specified time period. This provides an overview of the types of applications that are allowed by the firewall, and which ones are denied.

### **Proxy Use by Selected Hosts**

This report shows selected hosts or users of the proxy within a specified time period. It is essential to enter a host or user value or select a list of hosts or list of users for the report to return data.

### **Source Analysis**

This report shows the top sources of the selected events within a specified time period.

### **Target Analysis**

This report shows the top targets of the selected events within a specified time period.

### **Top Targeted Services**

This report shows the top services reported in the selected events within a specified time period.

### **Top Traffic Sources**

This report shows the top sources of the selected events within a specified time period.

### **Top Traffic Targets**

This report shows the top targets of the selected events within a specified time period.

### **Top Zone Relationships**

This report shows the connections between source and target zones, which can indicate abnormal connection patterns, within a specified time period.

## Traffic Control Summary

This report shows granted and denied connections for firewall devices within a specified time period.

## VPN Access

### Failed VPN Logins by Selected Users

This report shows failed VPN login activity for sensitive accounts within a specified time period. Accounts that should never be used for VPN (such as service accounts) are also identified. The report shows the first and last time the activity occurred; the VPN gateway; the source address and zone; the assigned address; and the number times the user logged in. It is essential to enter a user value or select a list of users for the report to return data.

### New VPN Client Sources for Selected Users

This report shows new sources of connections, grouped by user, for sensitive user accounts (such as administrators) within a specified time period. Unauthorized use of these accounts is identified. The report shows the first and last time the connection was made; the VPN gateway; the source address; the assigned network address; and the number of successful and unsuccessful login attempts. It is essential to enter a user value or select a list of users for the report to return data.

### New VPN Users

This report shows new users of a VPN service within a specified time period. The report shows the users; the first time the usage was noticed; the number of sources from which logins were made; the number of failed logins; and the number of successful logins.

### VPN Gateways

This report shows hosts reporting VPN logins within a specified time period. This report shows the detector; detector zone; number of users; number of sources from which logins were made; and the number of successful and unsuccessful logins.

### **VPN Login Attempts Without Eventual Success**

This report shows users and sources who unsuccessfully attempted to log in to the VPN within a specified time period. These cases most likely represent truly unauthorized attempts, as opposed to failure due to misconfiguration. This report shows users; source addresses and zones; the first and last time the attempt occurred; the number of sources from which logins were made; and the number of login attempts.

### **VPN Logins by Selected Users**

This report shows the VPN login activity of the selected user within a specified time period. All VPN activity for sensitive accounts is presented, to enable identification of accounts that should never be used for VPN, such as service accounts. This report shows the first and last time the activity occurred; the VPN gateway; the user; the source address and zone; the assigned IP address; and the number of times the user logged in. It is essential to enter a user value or select a list of users for the report to return data.

### **VPN Users List**

This report shows all active users of the VPN service, grouped by the device and detector, within a specified time period. The report shows users; the first and last time the user logged in; the number of sources from which logins were made; and the number of successful and unsuccessful logins.

## **Information Classification (CIP-003-1 R4)**

Reports and Event Views supporting compliance with requirement R4 of NERC Standard CIP-003-1.

### **Denied Files List**

This report shows files that users have unsuccessfully attempted to access, grouped by the originating IP address, within a specified time period. Files with very high numbers of attempts may be accessed by automated tools.

### **Entries in Selected List**

This report shows the current contents of a selected dynamic list.

User data restrictions are not applied to this report.

## **Logging Physical Access (CIP-006-1 R4)**

Reports and Event Views supporting compliance with requirement R4 of NERC Standard CIP-006-1.

### **Local Login to Selected Hosts**

This report shows local login attempts to selected hosts, such as critical servers, within a specified time period. It is essential to enter a host value or select a list of hosts for the report to return data.

## **Malicious Software Prevention (CIP-007-1 R4)**

Reports and Event Views supporting compliance with requirement R4 of NERC Standard CIP-007-1.

### **Active Malware**

This report shows all active malware detected within a specified time period.

### **Exposure of Selected Hosts to Malware**

This report shows the exposure of selected hosts to malware within a specified time period. It is essential to enter a user value or select a list of users for the report to return data.

### **Hosts Exposed to Selected Malware**

This report shows hosts exposed to selected malware within a specified time period. It is essential to enter a malware or select a list of malware for the report to return data.

## **Least Common Malware**

This report shows the least common malware detected within a specified time period.

## **Most Infected Hosts**

This report list the most infected hosts within a specified time period.

## **Scans Disabled on Selected Hosts**

This report shows the scans disabled on selected hosts within a specified time period. It is essential to enter a host or select a list of hosts for the report to return data.

## **Top Malware**

This report shows the top malware within a specified time period.

## **Users Most Frequently Disabling Protection**

This report shows users who have frequently disabled system protection within a specified time period.

## **Personnel Access (CIP-004-1 R4)**

Reports and Event Views supporting compliance with requirement R4 of NERC Standard CIP-004-1.

## **Local Login to Selected Hosts**

This report shows local login attempts to selected hosts, such as critical servers, within a specified time period. It is essential to enter a host value or select a list of hosts for the report to return data.

## **New Users Accessing Databases**

This report shows users accessing a database server within a specified time period. Few users directly access databases, so any occurrences of this are worth reviewing.

## **New Users of Selected Files**

This report shows users accessing selected files for the first time, within a specified time period. It is essential to enter a file name or select a list of files for the report to return data.

## **Users Accessing Selected Files**

This report shows all users who have accessed the specified file(s) (which are usually sensitive resources) for the specified time period. It is essential to enter a file name or select a list of files for the report to return data. The results are grouped by file.

## **Users Accessing Selected Files (Detail)**

This report shows all users who have accessed the specified file(s) (which are usually sensitive resources) for the specified time period. It is essential to enter a file name or select a list of files for the report to return data. The results are grouped by file.

## **Users Connecting to DB from New Sources**

This report shows users accessing a database server from a new client address within a specified time period.

## **Policy Exceptions (CIP-003-1 R3)**

Reports and Event Views supporting compliance with requirement R3 of NERC Standard CIP-003-1.

## **Local Login to Selected Hosts**

This report shows local login attempts to selected hosts, such as critical servers, within a specified time period. It is essential to enter a host value or select a list of hosts for the report to return data.

## **Notifications by Policy**

This report summarizes notifications according to policy tag within the specified time period.

User data restrictions are not applied to this report.

## **Users Authenticating from Multiple Sources**

This report shows the users who successfully and unsuccessfully attempt to authenticate from many sources during a specified time period.

## **Ports and Services (CIP-007-1 R2)**

Reports and Event Views supporting compliance with requirement R2 of NERC Standard CIP-007-1.

## **Port Traffic Control**

This report shows events (by target port) to indicate which ports are blocking or allowing events, within a specified time period. This provides an overview of the types of applications that are allowed by the firewall, and which ones are denied.

## **Top Targeted Services**

This report shows the top services reported in the selected events within a specified time period.

## Security Status Monitoring (CIP-007-1 R6)

Reports and Event Views supporting compliance with requirement R6 of NERC Standard CIP-007-1.

### Automated Notification

#### Notification Summary

This report shows the defined notification types and how many notifications have been sent within the specified time period.

User data restrictions are not applied to this report.

#### Notifications by Policy

This report summarizes notifications according to policy tag within the specified time period.

User data restrictions are not applied to this report.

#### Notifications by Process

This report summarizes notifications by process tag within the specified time period.

User data restrictions are not applied to this report.

#### Notifications by Target

This report shows the defined notification types and how many notifications were sent within the specified time period.

User data restrictions are not applied to this report.

### Event Management

## **Data Sources**

This report shows details of the status and operation of SAFE and of the data sources providing logs to SAFE within a specified time period. This report may also reveal spikes in event rates. The parameters within the report can also list the detectors associated with various types of events.

## **Top Acting Users**

This report shows the most active users, grouped by event type, within a specified time period.

## **Top Detectors**

This report shows the top detectors, determined by the highest event count within a specified time period.

## **Top Event Types**

This report shows the top event types within a specified time period.

## **System Events**

### **Administration Activity**

This report shows all administration events within a specified time period.

### **Administrative Users List**

This report shows all administrative event activity, grouped by administrator, within a specified time period.

### **Audit Subsystem Events**

This report shows the summarized events related to auditing information received from data sources within a specified time period.

## **Summary of Errors and Availability Events**

This report shows all events related to error and availability activities, determined by highest count, within a specified time period.

## **Vulnerability Assessment (CIP-007-1 R8)**

Reports and Event Views supporting compliance with requirement R8 of NERC Standard CIP-007-1.

### **Asset Vulnerabilities**

This report shows the asset vulnerabilities within a specified time period.

### **Asset Vulnerability History**

This report shows the asset vulnerability history within the specified time period.

### **Assets with Selected Vulnerability**

This report shows assets and their related vulnerability ID within a specified time period.

### **Most Common Vulnerabilities**

This report shows the most common vulnerabilities with a specified time period.

### **Most Severe Vulnerabilities**

This report shows the most severe vulnerabilities within a specified time period.

### **Most Vulnerable Assets**

This report shows the most vulnerable assets within the specified time period.

## **Most Vulnerable Zones**

This report shows the most vulnerable zones within a specified time period.