FORTRA™

GUIDE (TRIPWIRE)

Tripwire NERC CIP Report Catalog

Fortra's Tripwire NERC CIP Solution Suite is an advanced offering that augments Tripwire's tools for meeting 23 of NERC CIP's 44 requirements. The Tripwire NERC CIP Solution Suite allows you to achieve and maintain NERC CIP compliance with high efficacy and reduced effort. This suite includes continuous monitoring of cyber assets, automated assessment of security, and audit-ready evidence with quick generation of reports or dashboards.

The reports shown here start with those produced in Tripwire® Enterprise with our Allowlisting solution, but also include examples of broader reporting capabilities. The reports in this document are a partial listing of what is available as part of the NERC CIP Solution Suite. Customers can implement some or all of the solutions according to their needs.

TRIPWIRE COVERAGE OF NERC CIP REQUIREMENTS

13 Standards & 44 Requirements – Tripwire Solutions Cover 23

	CIP-002 BES Cyber System Identification and Categorization	CIP-003 Security Management Controls	CIP-004 Training and Personnel Security	CIP-005 Electronic Security Perimeter	CIP-006 Physical Security of BES Cyber Systems	CIP-007 Systems Security Management	CIP-008 Incident Reporting and Response Planning	CIP-009 Recovery Plans for BES Cyber Systems	CIP-010 Configuration Change Management and Vulnerability Assessments	CIP-011 Information Protection	CIP-012 Control Center Communication Network	CIP-013 Supply Chain Management	CIP-014 Physical Security
1	BES Cyber System Identification Tripiwire IP360	Cyber Security Policy for High/ Medium Systems Tripwire Enterprise	Awareness	Electronic Security Perimeter Tripwire Enterprise	Physical Security Plan Tripwire LogCenter	Ports and Services Tripwire Enterprise	Cyber Security Incident Response Plan Tripwire LogCenter	Recovery Plan Specifications Tripwire Enterprise & Tripwire LogCenter	Configuration Change Management Tripwire Enterprise	Information Protection Tripwire Enterprise & Tripwire LogCenter	Physical & Logical Risk Mitigation for Data	Risk Management Plan	Transmission Station Physical Security
2	Regular Approval	Cyber Security Policy for Low Systems Tripwire Enterprise	Training	Interactive Remote Access Management Tripwire Enterprise	Visitor Control Program Tripwire LogCenter	Security Patch Management Tripwire Enterprise	Cyber Security Incident Response Plan Implementation and Testing	Recovery Plan Implementation and Testing Tripwire Enterprise & Tripwire LogCenter	Configuration Monitoring Tripwire Enterprise	BES Cyber Asset Reuse and Disposal	Proof of Implementation	Proof of Implementation Tripwire Enterprise	Third Party Verification of Physical Security
3		Identification of Senior Manager	Personnel Risk Assessment Program		Maintenance and Testing Program	Malicious Code Prevention Tripwire Enterprise	Cyber Security Incident Response Plan Review, Update, Communication	Recovery Plan Review, Update and Communication	Vulnerability Assessments Tripiwire IP360			CIP Senior Manager Approval	Primary Control Center
4		Delegation of Authority	Access Management Program Tripwire LogCenter			Security Event Monitoring Tripwire LogCenter			Transient Cyber Assets and Removable Media Tripwire Enterprise & Tripiwire IP360				Evaluate Potential Threats & Vulnerabilities
5			Access Revocation Program Tripwire Enterprise & Tripwire LogCenter			System Access Controls Tripwire Enterprise							Physical Security Plan
6													Third Party Review of Plans

Example: Tripwire Reports Based on Ports Control

Tripwire 's Allowlisting provides core assessment and reporting capability on key NERC CIP requirements. The example reports below highlight ports reporting. The same reports can be generated for all of the other Allowlisting supported controls listed below.

Ports (CIP-007 R1 and CIP-010 R1)

Available reports support several use cases:

- Evidence reporting
- Manager level review of compliance status
- Ports needing remediation (add justification or close port)
- CIP baseline – Allowed ports for an asset
- Allowed but not used CIP baseline ports

Ports listening on a given asset are identified and justifications supplied by the Responsible Entitle are recorded for evidence reporting. The solution for ports also covers ephemeral ports, port ranges as well as use of asset groups for scalable assignment of justification. Customer defined fields like review, review date, or TFE can easily be included.

Note: *Port justification data is supplied and maintained by the customer.*

Example: Evidence Report for Ports

Report by asset	**tlc (Windows Server)** **Open Ports (External Rule)** **Open Ports - All**
Summary header	**Version :** 2/24/23 10:47 AM **Type :** Modified **Content** ********** ** OPEN PORTS ALLOWLIST RESULTS ** ********** Report Type: Documentation Format: Text Node Name: tlc Total Open Ports Found: 30 Unauthorized Open Ports: 0
Details for each port, including justification	Protocols: TCP Port Numbers: 135 Service Names: RpcSs Process Names: svchost.exe Justification: Remote Procedure Call (RPC) (RpcSs) Service Defaults in Windows 10. The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activations requests, object exporter resolutions and distributed garbage collection for COM and DCOM servers. Protocols: TCP Port Numbers: 139 Process Names: System Justification: Port 139 is utilized by NetBIOS Session service. Enabling NetBIOS services provide access to shared resources like files and printers not only to your network computers but also to anyone across the internet. Protocols: TCP Port Numbers: 445 Process Names: System Justification: The system process is responsible for the system memory and compressed memory in the NT kernel. This system process is a single thread running on each processor. It is the host of all kind of drivers (network, disk, USB). Protocols: TCP Port Numbers: 1468 Process Names: Tlc.LogManager.Svc.exe Justification: TLC Server - TLC application port and service allowed. Protocols: TCP Port Numbers: 3306 Process Names: mysqld.exe Justification: mysql DB installed for TLC event database use.
Custom fields easily added (Documentation, Reviewer, Review Date, etc.)	

Example: Summary View of Compliance Status

This example shows an environment with seven servers, for which there is one unjustified port on the second server in the sequence. Therefore, the pie chart is red for that server.

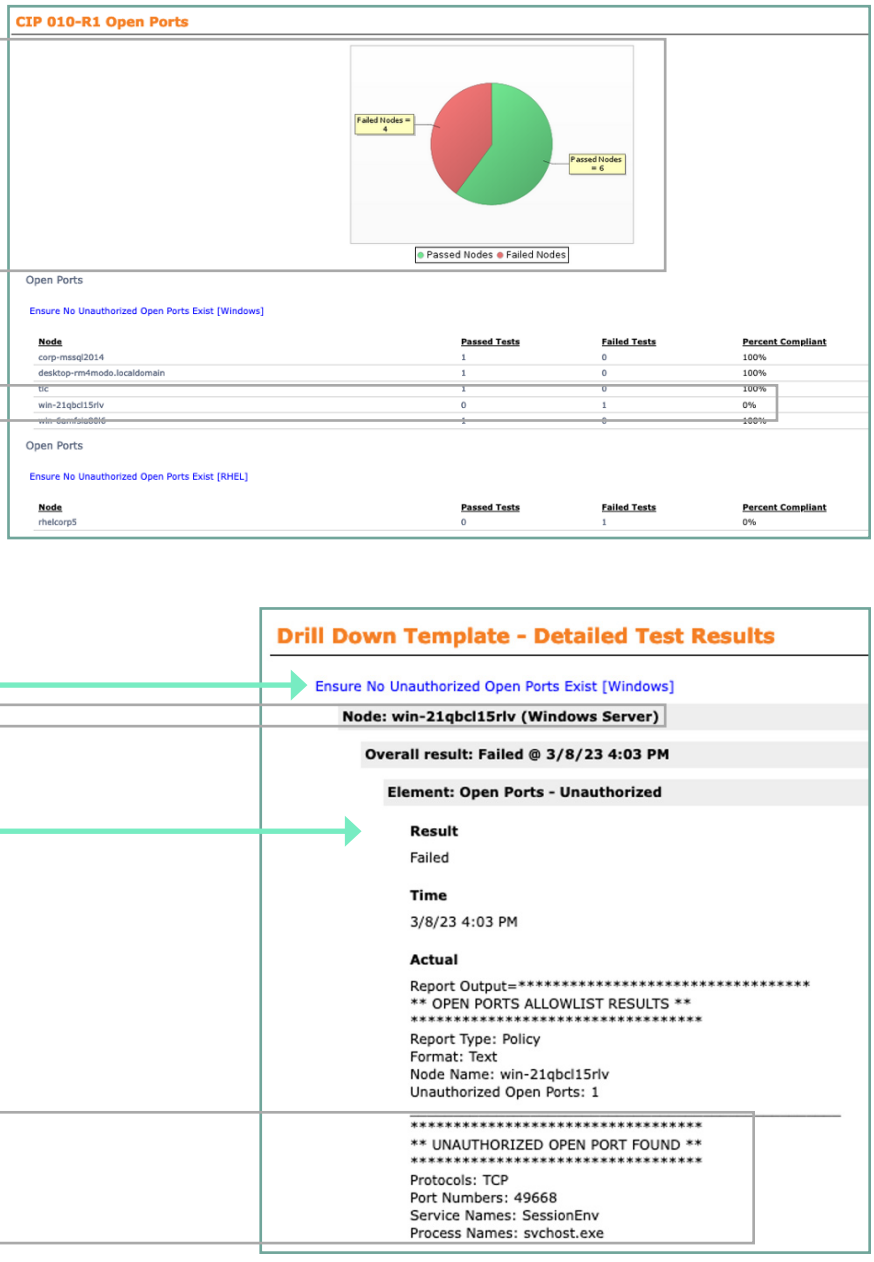
Summary of red/green view of compliance

Reporting includes justification

Report by asset

Drill-down report only lists exceptions needing to be addressed in order to focus engineering efforts on remediation

Unjustified port
Note: Svchost is resolved down to the underlaying process

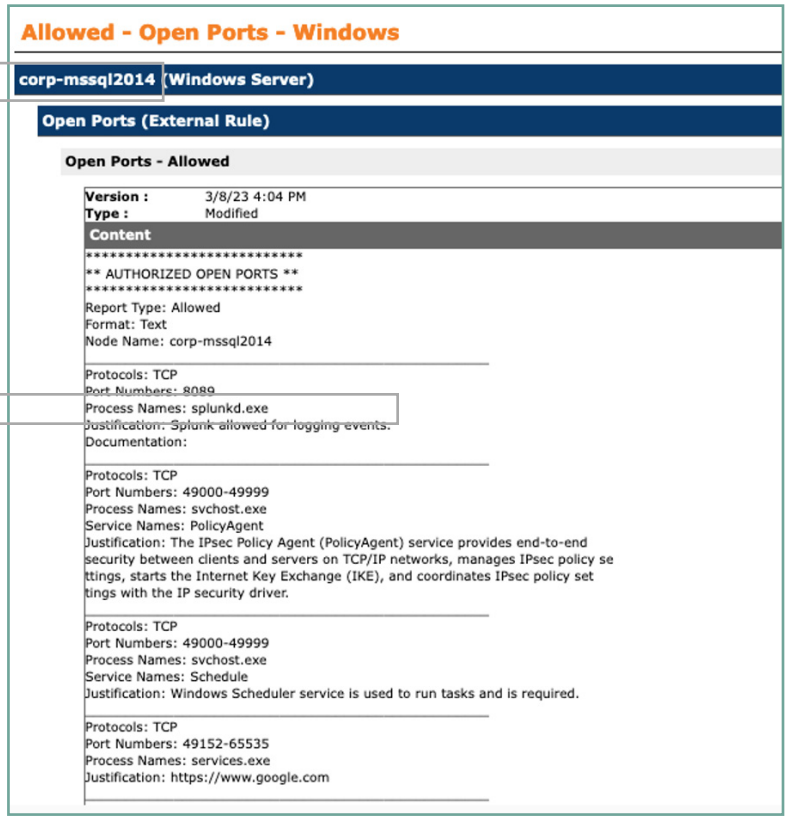


Example: CIP Baseline Report – Allowed Ports

This report provides documentation of allowed ports (as CIP baseline) and tracking of changes to an asset's CIP baseline over time with Tripwire Enterprise's built-in review and approval features.

Report by asset

Optionally match by regular expression



Allowed - Open Ports - Windows

corp-mssql2014 (Windows Server)

Open Ports (External Rule)

Open Ports - Allowed

Version : 3/8/23 4:04 PM
Type : Modified

Content

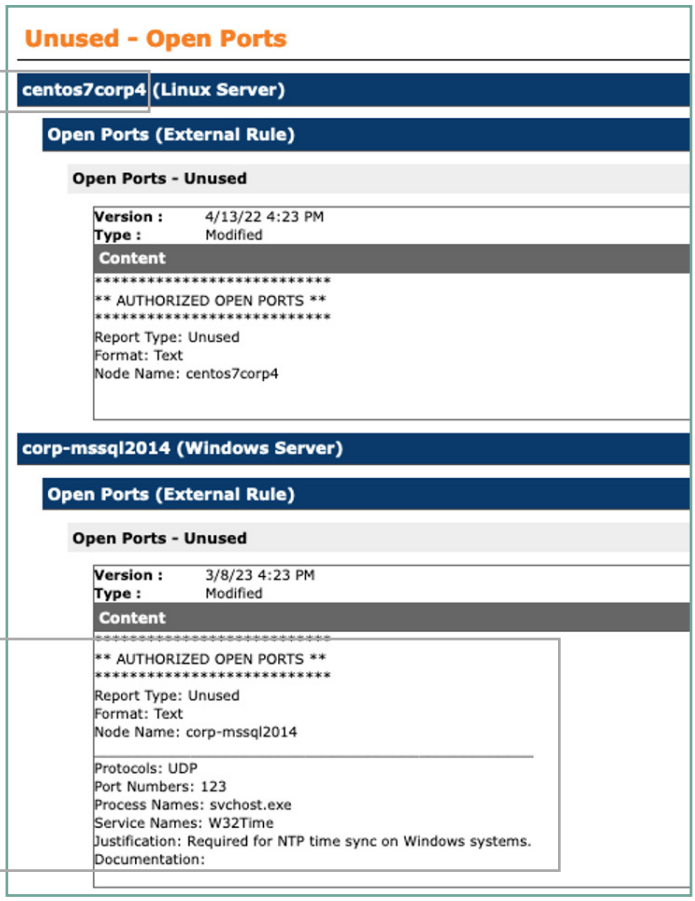
```
****************************
** AUTHORIZED OPEN PORTS **
****************************
Report Type: Allowed
Format: Text
Node Name: corp-mssql2014

Protocols: TCP
Port Numbers: 8089
Process Names: splunkd.exe
Justification: Splunk allowed for logging events.
Documentation:

Protocols: TCP
Port Numbers: 49000-49999
Process Names: svchost.exe
Service Names: PolicyAgent
Justification: The IPsec Policy Agent (PolicyAgent) service provides end-to-end
security between clients and servers on TCP/IP networks, manages IPsec policy se
ttings, starts the Internet Key Exchange (IKE), and coordinates IPsec policy set
tings with the IP security driver.

Protocols: TCP
Port Numbers: 49000-49999
Process Names: svchost.exe
Service Names: Schedule
Justification: Windows Scheduler service is used to run tasks and is required.

Protocols: TCP
Port Numbers: 49152-65535
Process Names: services.exe
Justification: https://www.google.com
```

Example: Allowed But Not Used Ports

This report lists allowed (i.e., expected) allowlist items that were not observed in the last scan. This is used to identify over-allowlisting for any allowlist control, and thus provides a means for ensuring precisely scoped allowlisting. This report is most often used with the software control.

Report by asset

Example port not found in use



Additional Tripwire Allowlisting Supported Controls

All of the reports shown for ports are available for all of the other six Allowlisting controls listed below.

1. Software

   Used to list commercially available software, custom software and OS patches. Even software that does not register on installation can be allowlisted, e.g., PuTTY, OSI monarch, and Oracle on Linux.

2. Services

   This control provides for allowlisting by service/daemon in supported systems. This control also includes capability for:

   - Identifying root processes under SVCHOST instances
   - Pattern match names of services for dynamically named services

3. Users and password age

   The User control allowlists local or domain users. Additionally, it checks the age of passwords and can alert if password are approaching a threshold age (e.g., 80% of allowed age).

4. Groups

   The Allowlisting control for Groups is usually used related to access management. This control provides for allowlisting of local groups. Alerting on this control is especially helpful on administrative groups.

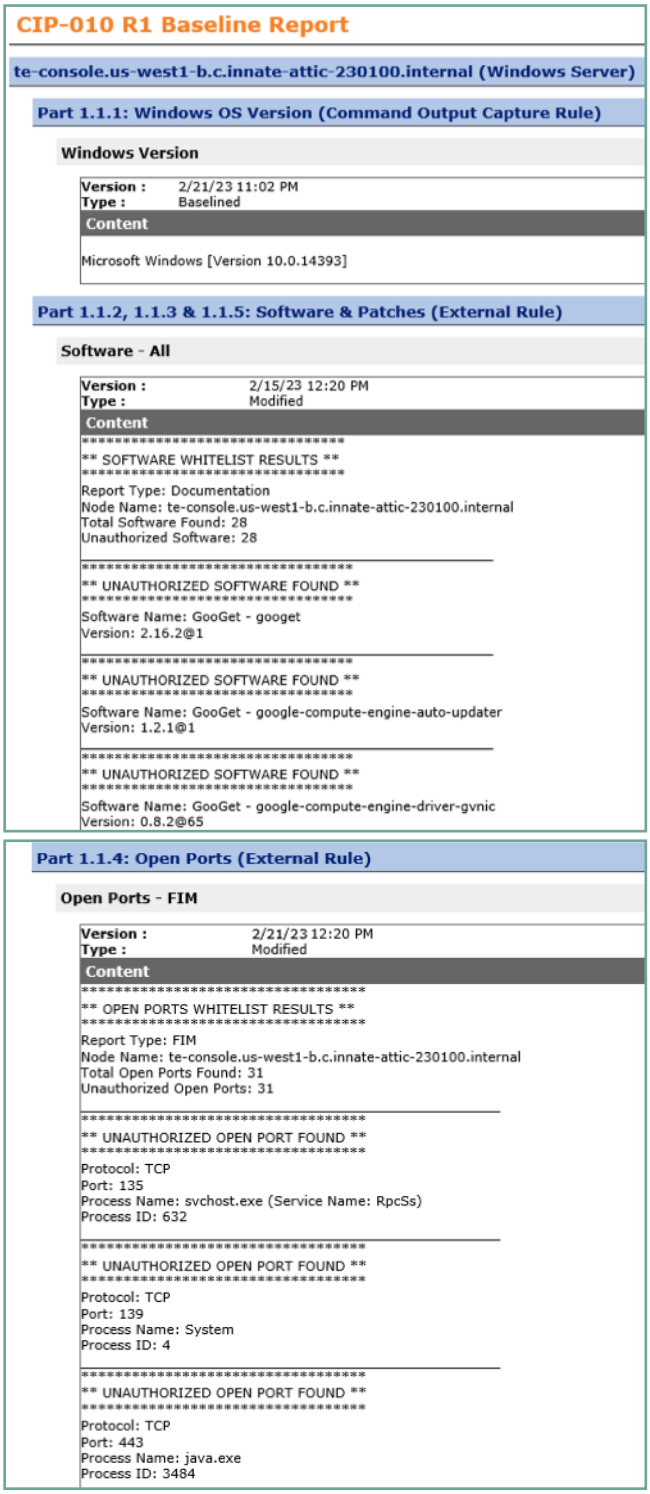
5. Shares

   This control allowlists Windows shares, including permissions on those shares. Alerting occurs when unexpected shares appear, or unexpected access is granted.

6. Routes

   The routes control generates evidence that the Electronic Security Perimeter is maintained by allowlisting based on allowed network, netmask, and gateway.

Example: CIP-010 Baseline Report



CIP-010 R1 Baseline Report

te-console.us-west1-b.c.innate-attic-230100.internal (Windows Server)

Part 1.1.1: Windows OS Version (Command Output Capture Rule)

Windows Version

Version : 2/21/23 11:02 PM
Type : Baselined

Content

Microsoft Windows [Version 10.0.14393]

Part 1.1.2, 1.1.3 & 1.1.5: Software & Patches (External Rule)

Software - All

Version : 2/15/23 12:20 PM
Type : Modified

Content

****
** SOFTWARE WHITELIST RESULTS **
****
Report Type: Documentation
Node Name: te-console.us-west1-b.c.innate-attic-230100.internal
Total Software Found: 28
Unauthorized Software: 28

****
** UNAUTHORIZED SOFTWARE FOUND **
****
Software Name: GooGet - googet
Version: 2.16.2@1

****
** UNAUTHORIZED SOFTWARE FOUND **
****
Software Name: GooGet - google-compute-engine-auto-updater
Version: 1.2.1@1

****
** UNAUTHORIZED SOFTWARE FOUND **
****
Software Name: GooGet - google-compute-engine-driver-gvnic
Version: 0.8.2@65

Part 1.1.4: Open Ports (External Rule)

Open Ports - FIM

Version : 2/21/23 12:20 PM
Type : Modified

Content

****
** OPEN PORTS WHITELIST RESULTS **
****
Report Type: FIM
Node Name: te-console.us-west1-b.c.innate-attic-230100.internal
Total Open Ports Found: 31
Unauthorized Open Ports: 31

****
** UNAUTHORIZED OPEN PORT FOUND **
****
Protocol: TCP
Port: 135
Process Name: svchost.exe (Service Name: RpcSs)
Process ID: 632

****
** UNAUTHORIZED OPEN PORT FOUND **
****
Protocol: TCP
Port: 139
Process Name: System
Process ID: 4

****
** UNAUTHORIZED OPEN PORT FOUND **
****
Protocol: TCP
Port: 443
Process Name: java.exe
Process ID: 3484

Other Reports Supporting NERC CIP

Tripwire's Allowlisting capabilities provide the keystone to most utilities' CIP programs. Typically, high priority controls are addressed per the priorities of the Registered Entity. As time and resources permit, additional controls can be addressed, including, but not limited to:

- **CIP-002** – Asset reconciliation with actual assets vs. declared assets in the system of record
- **CIP-007 R4** – Reports on log requirements (successful logins, unsuccessful logins, etc.)
- **CIP-007** – Security controls
- **CIP-010 R3** – Vulnerability assessments
- **CIP-013 R2** – Software integrity

Tripwire: Platform Coverage

Platform	Open Ports	Services	Users	Group Memberships	Software	Shares	Routes
AIX	×	×	×		×		
Debian	×	×	×		×		
RHEL	×	×	×		×		×
Solaris	×	×	×		×		
Ubuntu	×	×	×		×		
Windows	×	×	×	×	×	×	×
Agentless Devices	×						

A complete list of platform versions supported and additional requirements can be found in the current version of the Tripwire Whitelist Profiler Implementation Guide. Additional platforms can be supported through a custom engagement with Tripwire Professional Services. Agentless devices would be scanned by Nmap or Tripwire IP360™ for listening ports.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.