ConsoleWorks

Cybersecurity Operations Platform

Configuration Port Security with ConsoleWorks

REFERENCE: CIP-007-5 R1

INTRODUCTION

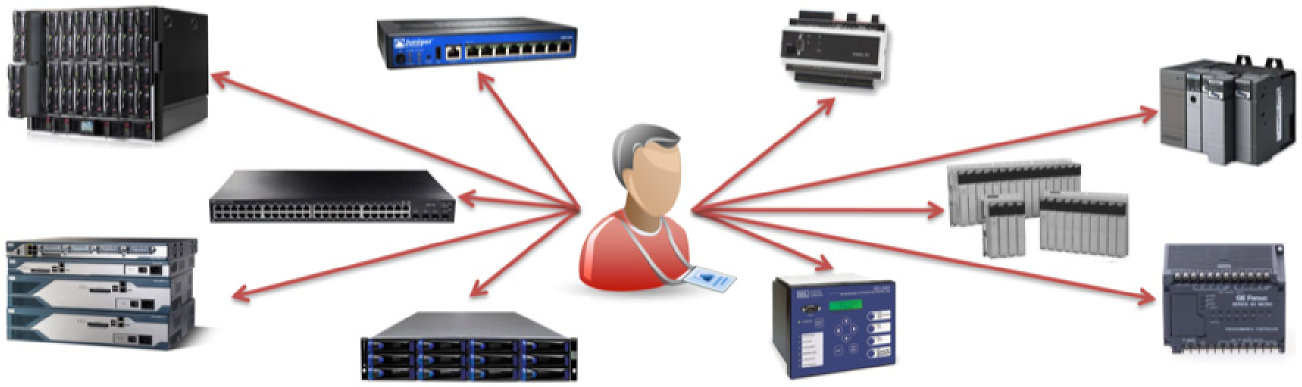
Configuration ports on critical and non-critical cyber assets must be secured and managed. Per CIP-007-5, all ports should be either secured or disabled. This obviously includes configuration ports. However, most IT devices do not allow the disabling of these ports nor should these ports be disabled as they serve important purposes, including being the primary emergency access port. Instead, these ports must be secured.

Configuration ports exist on almost every IT device used in Utility operations. From the control room to the sub-station to the “pole,” these physical ports provide a special level of privileged access that can be used to:

1. Change Bios
2. Upgrade Firmware
3. Set Baseline Configuration
4. Build-out devices that have components (like servers)
5. Perform a variety of Administrative functions
6. Perform emergency repair or failure recovery when no other port is accessible

ConsoleWorks provides a means to secure these ports, helping Utility providers meet NERC CIP requirements and pass NERC CIP audits. This solution also helps Utility providers improve the efficiency of day-to-day operations. Business value is a combination of NERC CIP compliance, reduced operating cost (man-power) and improved service.

ConsoleWorks Configuration Port Security



There's a back door into every Bulk Energy System. It's called the configuration port. Own the port and you own the device – period. ConsoleWorks secures configuration ports no matter what device they are on or where the device is located. From the EMS to the Control Room to the Substation to the Pole – we've got you covered.

SECURING CONFIGURATION PORTS WITH CONSOLEWORKS

In order to effectively secure configuration ports while meeting NERC CIP requirements access to all configuration ports must be controlled and all activity over these ports must be automatically logged to provide a forensic record of this activity. These are both requirements of CIP-007-05.

For a more detailed discussion on Configuration Port Security in respect to CIP-007-5 R1 please see the whitepaper at: http://www.tditechnologies.com/whitepaper-nerc-cip-007-5-r1

ConsoleWorks solves this problem by establishing and maintaining persistent connections to all configuration ports and then logging all user activity over these ports down to the keystroke. Port management in ConsoleWorks includes a comprehensive security model with granular permissions for access control and enforcement of least privilege. NERC CIP port access security events (log on, log off, failed log on, etc.) are automatically detected, alerted on, and logged per NERC CIP requirements in the current version through CIP version 5. Persistent connections can be setup to deny any other connections to managed ports, ensuring that any backdoors to these ports are eliminated.

WHAT DEVICES HAVE CONFIGURATION PORTS?

Virtually all electronic devices with communication capability have configuration ports. For modern servers, baseboard management controllers[1] that are networkable are the common configuration port technology. Older servers, routers, switches, firewalls, SANs, appliances, etc. have serial privileged configuration ports, often network-enabled with terminal servers.

Control systems and control devices have configuration ports. Virtually every PLC, RTU, and IED has a configuration port (usually a privileged serial port with command and control access to the device's core program and operating system functions). In remote locations, such as substations and endpoints ("poles") there are found many devices that have configuration ports. These are often a mix of traditional IT devices and control system devices.

[1] Baseboard management controllers include the iLo2 (HP), DRAC (DELL), and ALOM, ILOM (SUN/ORACLE).

This diversity of devices and geographical locations is a significant part of the challenge in securing these configuration ports. Many of these devices do not allow or support the installation of a local software agent to help logically secure them, and virtually all software agents cannot effectively manage the actual configuration ports themselves. Because of this most control devices are only secured through physical security (locks, gates, walls, doors).

ConsoleWorks: Agent-less and Agnostic

ConsoleWorks addresses this challenge with a unique method for controlling configuration ports. With ConsoleWorks, communication connections are initiated to each configuration port and then they are persistent, resulting in always up connections that are monitored at all times (in real-time). There is no agent software installed and no vendor-specific connection paradigm used, which is the key to delivering a solution that can secure configuration ports of all types regardless of geographical location. For all command-line access to configuration ports, ConsoleWorks automatically logs all activity down to the keystroke. This provides a comprehensive forensic record over all configuration port access (change management, change alerts, activity reports, etc.)

PERFORMANCE & PRODUCTIVITY IMPACTS

There are two other important considerations that must be taken into account when establishing a successful configuration port security strategy. These considerations are: 1) physical performance of devices and 2) performance impacts on people.

Device performance in control systems can be a critical factor for any deployed solution. Many control systems are designed to operate within very specific parameters that include running programs, processing sensor input, and generating control commands in a given time usually defined in milliseconds. Even very small performance impacts can disrupt control mechanisms and trigger negative impacts. For IT systems, device performance is generally more of a cost issue where each “hit” on processing capability increases the total computing required – which means more hardware and software must be purchased, installed, and maintained to met the demand.

For people, the primary performance challenge stems from the fact that most security solutions introduce additional steps into existing work requirements. That slows things down, makes them more complex, and requires new training and support. None of these are desirable as this obviously increases the cost and manpower required by the Utility to perform daily activities.

ConsoleWorks resolves these challenges by eliminating the vast majority of performance consumption on devices where configuration ports are managed. The typical performance impact of ConsoleWorks ranges from negligible to about 3% - low enough that there are rarely any negative effects experienced on the devices themselves.

From the people perspective, ConsoleWorks actually simplifies the work that people must do to perform their daily activities. Operations support in the product simplifies and automates many tasks that exist today in performing daily work activities, yielding a net increase in productivity and a net decrease in response time. In many ways, ConsoleWorks turns the traditional security paradigm upside-down by addressing security from the perspective of Operations as an integrated function that does not impede work activity.

DESIGNED FOR NERC CIP

ConsoleWorks does the heavy-lifting for you when it comes to NERC CIP. The solution captures the data and produces the documentation you need to 'prove-the-practice.' Covering all major components in existing and proposed NERC CIP regulations, ConsoleWorks provides a highly secure solution that can meet even the most demanding requirements of Utility organizations. The solution includes:

- Appropriate, customizable, log-on splash screen
- All Log-ons, log-offs, and failed log-on attempts captured, logged, and alerted
- All changes—down to the keystroke (by user) captured, logged, and alerted
- Event Detection, Alerts, and Acknowledgements
- All records digitally signed
- Built-in reporting
- Archiving controls ensure records are retained as needed
- No buffers, no polling cycles—nothing is EVER 'missed'
- Comprehensive—coverage over all monitored devices (IT, IED, RTU)
- Password management (rules, change frequency, no-reuse, etc.)
- Two-factor authentication
- End-to-end Encryption
- Nothing to install on managed devices (agent-less)
- Directly supports NERC CIP versions 3, 4, 5 and 6

SOLUTION BENEFITS

The benefits of security, compliance, and performance improvement in one solution are an important part of the unique value offered by the ConsoleWorks solution for configuration port security. Performance improvement is driven by the work-centric design of ConsoleWorks, where many of the activities users perform over configuration ports are simplified and optimized within the ConsoleWorks product. This approach has the unique benefits of:

- Achieving security goals without negatively impacting performance
- Protecting against code-based exploits (malware, viruses)
- Restricting access and assigning least privilege for all (local and remote) users
- Recording of user activity (command, control and response) down to the keystroke
- Event management automation: alerting, response, best-practice, remediation
- Bi-directional data capture and logging (all system messages, all user activity)
- Configurable alerting-alarming for oversight and proactive security event notification

Additional compliance benefits include:

1. Comprehensive Logging
2. User Activity (keystroke)
3. Event Detection
4. Event Alerting
5. Transparency
6. Packaged Reports
7. Custom Reports

Logging, event detection, and alerting provide security event notification that support (and automatically document) key components of compliance business processes. User activity captured down to the keystroke (bi-directional logging) further facilitates compliance business processes and enhances security oversight by building forensic records for all actions taken for every configuration port access through ConsoleWorks to the BES.

FULL SUPPORT FOR UTILITY PROVIDER REQUIREMENTS

Monitoring Electronic Access

The ConsoleWorks solution for configuration port security provides monitoring and logging of access all configuration ports that it manages, 24-hours a day, seven days a week in all modes of operation including normal, maintenance, single-user, operating system absent modes. It monitors, detects, logs, and alerts all access attempts, and then notifies the designated response personnel through various means (e.g. email, text message, etc.). All data collected by ConsoleWorks is exportable to SIEM tools (and other aggregation products). Available export methods include e-mail, Syslog, SNMP, SFTP, SCP, and XML.

Downstream Device Integration

ConsoleWorks is designed for communication integration with devices[2] having a routable protocol. ConsoleWorks is commonly used to manage a very broad spectrum of traditional IT devices (routers, switches, servers, firewalls, appliances, etc.) virtual machines, applications, networks, IEDs, RTUs and other industrial control systems.

SCADA Devices

SCADA systems operate in a mission-critical, real-time environment. ConsoleWorks meets the demands of the SCADA environment by brokering sessions to configuration ports in true real-time limited only by existing network latency.

Legacy Protocols

ConsoleWorks can support virtually all devices that are managed with a Command Line Interface (CLI). This includes routers, console servers, terminal servers, and other like devices (telnet, ssh, etc.) For special purpose IEDs and RTUs where vendor-specific clients (Graphical User Interfaces – GUI) and specialized protocols (DNP3, Modbus, IEC61850, UCA2 MMS, etc.) are used, the end user application(s) are moved onto the ConsoleWorks Server where they are then managed by the ConsoleWorks pseudo console technology.

[2] The hardware and firmware capabilities of remote devices determine what degree of communication ConsoleWorks can support. In the vast majority of cases, ConsoleWorks can manage all downstream devices.

Audit Support

ConsoleWorks produces, aggregates, and summarizes audit logs that record user activities, exceptions, and information security events. This information includes:

- user IDs
- dates, times, and details of key events, e.g. log-on and log-off
- records of successful and rejected configuration port access attempts
- records of successful and rejected data and other resource access attempts
- changes to system configuration
- use of privileges
- alarms raised by the access control system
- system admin and system operator activities

ConsoleWorks uses a common timestamp and digital signing on all logs (each line) to produce the most accurate forensic record possible. All alarms are logged by ConsoleWorks as well as all system configuration changes.

In addition, ConsoleWorks:

- Protects logs with line-by-line digital signatures
- Tracks individual HTTP requests/responses with a unique ID
- Includes prebuilt reports
- Supports custom report generation

AN EXPANDABLE SOLUTION

The ConsoleWorks solution for conifguration port security is delivered on the ConsoleWorks Security and Operations Platform and can be expanded to meet additional security, compliance, and operational requirements.

Applicable to the Utility market and NERC CIP, the primary capabilities that are supported by the ConsoleWorks server platform are:

1. Secure Remote Access and Configuration Port Security
2. Baseline Configuration Management (Asset, Configuration, Patch and Firmware Management)
3. Endpoint Password Management
4. NERC CIP Event Monitoring and Detection, Processing, and Reporting
5. Automated data collection (logs, Syslog, SNMP), data consolidation, reporting, alerting, and process automation to support compliance business processes.

ABOUT TDI TECHNOLOGIES

TDi Technologies is the leader in IT/OT Cybersecurity, delivering solutions to a global customer base with key verticals including Utilities, Financial Services, Telecommunications, Health-care, and Government. The company's solutions help customers reduce operating costs, meet foundational compliance requirements, secure IT/OT assets, and improve IT/OT service delivery..

The TDi Technologies Utility practice is focused on delivering solutions that meet existing and future NERC CIP requirements without disrupting existing IT investments or burdening operations. In most cases, our NERC CIP solutions yield significant cost reductions through performance improvements that often provide solution payback in less than a year.

TDi Technologies, the TDi Technologies logo and the ConsoleWorks logo are registered trademarks of TDi Technologies, LLC.