

02 · ELIMINATE — CONFIGURATION & CHANGE MANAGEMENT

What Changed. When It Changed. Who Changed It.

Before a vendor accesses your device, ConsoleWorks captures the approved configuration. After they leave, it collects it again and compares. Every change is documented. Every deviation is scored. The forensic record is generated automatically — tied to the session, the identity, and the device.

THE CHALLENGE

Configuration Drift Is a Security Event

Most organizations have no authoritative record of device configuration state — before or after anyone touches it.

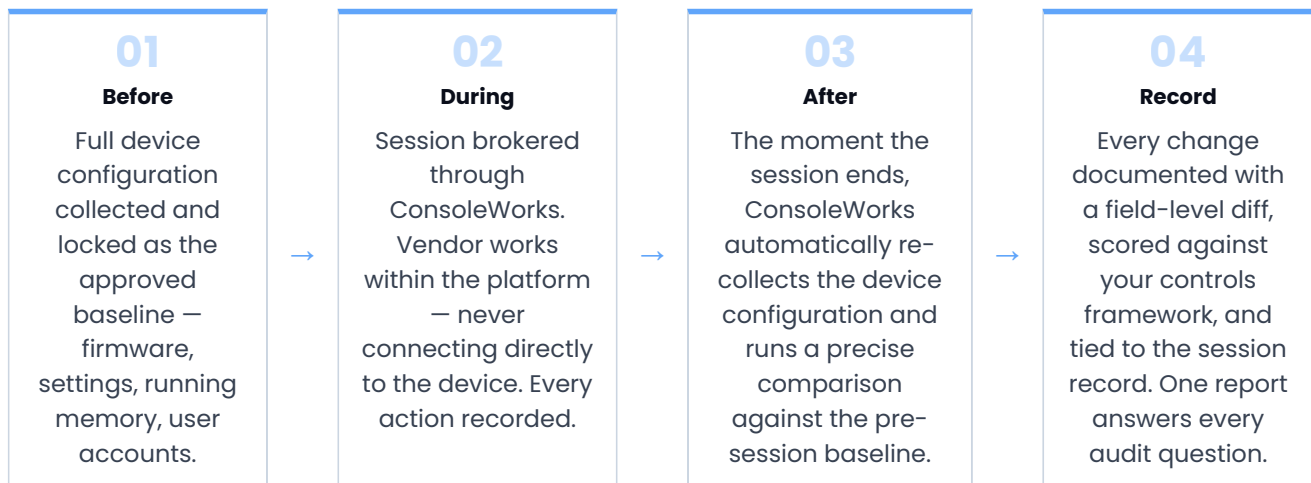
- Vendors make changes — firmware updates, settings, emergency fixes — with no automated record of device state beforehand.
- File integrity monitoring tells you a file changed — not what the device’s running configuration actually is.
- Change attribution requires access and collection to run through the same platform.
- NERC CIP-010, NIST 800-53, CMMC, and IEC 62443 require baseline documentation and change attribution — evidence that takes weeks to assemble manually.

The risk isn't just that vendors have access to your critical devices. It's that you have no way to prove what they changed — or that the device is in the state they said they left it in.

THE SOLUTION

The Vendor Access Story — Closed Loop, Every Time

ConsoleWorks addresses this directly. Because CCM operates through the same SRA connection that manages vendor access, every session automatically triggers a before-and-after configuration collection. The vendor never touches the device directly. ConsoleWorks brokers the connection, records every command, and the moment the session ends, re-collects the full device configuration and runs a precise field-level comparison. No manual steps. No gaps in the record.



No other configuration management tool can tie configuration state to a specific vendor session. ConsoleWorks can — because access and collection are managed through the same platform.

WHAT THIS DELIVERS

Complete Visibility Into Every Configuration Event

The result is a single, unbroken record that answers every question an operations team, security team, or auditor could ask — generated automatically, without manual collection steps, for every managed device in your environment.

Question	ConsoleWorks Answer
Who	MFA-authenticated vendor identity tied to every session record — no shared credentials
When	Exact session window logged — baseline captured before, configuration re-collected after
What they did	Every CLI command logged keystroke-by-keystroke. Every GUI action screen-recorded.
What changed	Field-level diff — every deviation from the approved baseline identified, scored, and reportable for audit

HOW CONFIGURATION & CHANGE MANAGEMENT WORKS

Collect. Compare. Act. Continuously.

Configuration & Change Management is not a snapshot tool. It is a continuous cycle — collect, compare, alert, remediate, verify — running against every managed device without manual intervention. Collection happens through the same active SRA connection ConsoleWorks establishes to the device — whether that's a server, a network appliance, or a field controller — retrieving actual running configuration state directly from the endpoint, not inferred from network traffic, not estimated from file signatures.

01 · Collect
Active Configuration Collection

ConsoleWorks connects directly to each device through SRA and retrieves the actual running configuration — firmware, settings, running memory, software inventory, and user accounts. Scheduled, on-demand, or session-triggered.

- Scheduled collection per device type
- On-demand or event-triggered
- SSH, Telnet, Serial, RDP — no agents

02 · Compare
Baseline Comparison & Drift Detection

Every collected configuration is compared against the approved baseline — field by field, value by value. ConsoleWorks surfaces exactly what changed, what was added, and what was removed. Not a flag. A diff.

- Field-level diff on every comparison
- Authorized vs unauthorized classification
- Multi-version history — compare any snapshot

03 · Act
Alert, Remediate & Verify

Drift doesn't just raise a flag — it initiates action. The deviation is scored, the asset is surfaced in risk posture, and SRA puts the right person on the device. After the fix, CCM re-collects and verifies. The loop closes itself.

- Immediate alert on unauthorized deviation
- SRA session opened directly to affected device
- Post-remediation collection confirms baseline

CONFIGURATION & CHANGE MANAGEMENT IN THE PLATFORM

Configuration Data That Feeds Everything Downstream

Configuration & Change Management doesn't operate in isolation. Every configuration collected feeds the Asset Inventory, scores risk measurements, and generates compliance evidence. When drift is detected, risk scores update continuously. When remediation finishes, CCM re-collects, verifies return to baseline, and closes the gap in the audit record — automatically.

The connection to Asset Inventory is what makes configuration data meaningful. When CCM collects from a device, it isn't just capturing a snapshot — it's enriching a structured asset record that already contains the device's classification, criticality, ownership, and compliance obligations. Firmware versions, software state, active user accounts, and running configuration are written directly into that record. Every asset in the inventory reflects its actual current state, not what was last scanned or manually entered.

The connection to Risk Analysis is what makes drift actionable. ConsoleWorks evaluates every managed asset against a configurable set of measurement questions — each one mapped to one or more controls across your compliance frameworks. When CCM detects a configuration deviation, it triggers an immediate measurement failure against the relevant

controls. That failure updates the asset's risk score, which rolls up through site, region, organization, and fleet – so leadership sees posture changes as they happen, not in the next scheduled report.

Together, these three capabilities – configuration collection, asset context, and risk scoring – form a closed loop that no standalone configuration tool can replicate. The data is collected once and serves every downstream purpose simultaneously: operational visibility, security posture, and audit evidence.

CCM CONNECTS TO THE FULL CONSOLEWORKS PLATFORM

Feeds Asset Inventory

Configuration data collected by CCM enriches the Inventory Asset record – firmware versions, software state, active accounts, and settings – providing the most accurate and current device profile in the platform.

Drives Risk Analysis & Scoring

Configuration drift triggers a measurement failure, which immediately updates the risk score for the affected asset – rolling up through site, region, org, and fleet. Posture reflects reality the moment drift is detected.

Produces Compliance Evidence

Every collection, every change, and every remediation generates evidence mapped to SCF controls – NERC CIP-010, NIST 800-53, CMMC, IEC 62443, SOC 2, and 100+ other frameworks. Audit-ready on demand. No manual assembly.

Reaches Every Device – Servers to Field Controllers

ConsoleWorks CCM collects from servers, network devices, workstations, and field controllers alike – because collection happens through the same active SRA connection, not passive network inference. Most tools stop at the IT/OT boundary. ConsoleWorks doesn't. If SRA can reach it, CCM can collect from it.

Compliance Evidence. Generated Automatically.

NERC CIP-010, NIST 800-53, CMMC, IEC 62443, SOC 2 – all require baseline documentation and change monitoring. ConsoleWorks automates the entire requirement across every framework – baseline captured, changes detected, evidence generated, every deviation tied to a session record and a verified identity. When the auditor asks, you report.

Configuration data without access is guesswork. CCM with SRA is truth – pulled directly from the device, not inferred, not estimated. And when drift is detected, the remediation path is already built in. No ticket. No separate tool. No waiting.

HOW WE COMPARE

Not All Configuration Monitoring Is Built the Same

Most configuration monitoring tools were designed for a specific environment or use case – file integrity for servers, passive collection for network visibility, or manual baselines for compliance. ConsoleWorks CCM was built to cover the full environment, tie collection to access, and close the loop from detection to remediation without switching tools.

Capability	Standard Configuration Tools	ConsoleWorks CCM
Collection Method	File integrity monitoring or passive network inference – does not retrieve actual running device configuration	✓ Active collection through SRA – actual running state pulled directly from the device
Device Coverage	Strong on servers and workstations – limited visibility into network devices and field controllers	✓ Servers, network devices, workstations, and field controllers – full environment coverage
Vendor Session Tie-in	No session awareness – configuration changes cannot be tied to a specific vendor access event	✓ Pre/post collection on every session – baseline before, comparison the moment the session ends
Change Attribution	What and when – change detected, but not tied to a specific user or session	✓ Who, when, and what – every change tied to a verified identity and session record