Configuration audit

Evaluate required and forbidden configuration conditions with repeatable audit policies and evidence.

The business requirement

A saved configuration is useful evidence, but it does not establish that the device meets the required standards. Engineers need a repeatable way to evaluate installed configuration against company policy. Gluware connects defined audit rules to captured results, findings, and corrective work.



HOW THE CAPABILITY WORKS

Define the controls

Config Drift & Audit owns audit policies and rules for required or forbidden conditions. Use captured configuration output, regular expressions, and installed modeling Concept Items where appropriate.

Capture and run the audit

Capture the relevant device configuration and evaluate the policy. Run on demand, on a schedule with email notification, from a syslog event, or through a Network RPA workflow.

Inspect findings and preserve evidence

Review rule results, execution detail, logs, and audit reporting. Export detailed audit evidence or use Data Explorer templates for reusable reporting. Optional Git integration synchronizes and backs up/restores audit policies.

Correct and reassess

Network RPA can coordinate the corrective process. Config Model Editor applies modeled CLI/API configuration changes and separate state assessments; a subsequent audit evaluates whether the defined controls now pass.

Configuration audit

Connect the operating process to defined component responsibilities.

COMPONENTS DELIVERING THE CAPABILITY

Config Drift & Audit	Owns capture, audit rules, policy execution, results, and detailed evidence.
Config Model Editor	Performs modeled CLI/API corrective provisioning and separate assessments.
Network RPA	Coordinates audit, corrective tasks, and reassessment.
Data Explorer	Provides reusable reporting from stored fields.
Version Control	Provides optional Git-based policy synchronization and artifact restore.

OPERATING SCOPE

Config Drift & Audit: capture and evaluation

Capture configuration and operational command results, compare snapshots to identify drift, and evaluate audit policies for required or forbidden conditions. Installed modeling Concept Items can scope the audit inputs.

Config Model Editor: modeled correction

Validate the model, preview proposed differences, and provision the modeled configuration through declarative execution. Connected Preview reads the current device state without writing changes; provisioning is a separate operation.

Data Explorer: reports and evidence

View report results and history, download reports, or email them to the people who need them. The underlying applications supply the data being reported.

Business value and measurement

Measure covered policies and devices, recurring failures, exceptions, and time to resolution. Configuration audit checks required controls; snapshot comparison detects change. Together, they support sustained compliance and consistent network standards.

Technical documentation | Request a demo

Configuration audit background