Config Drift & Audit

Capture actual configuration and operational state, compare it with baselines, and audit the controls required by your enterprise.



Controls need to hold between audits.

Configurations change as teams operate the network, deploy software, and respond to incidents. Departures from approved state can introduce security exposure or disrupt services long before the next formal audit. Config Drift & Audit provides a repeatable way to identify those departures and feed corrective processes.

CORE FUNCTIONALITY

Capture, compare, and audit

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.

Choose how assessments run

Run drift comparisons or audits on demand, on a schedule with email notification, from a syslog event, or through a Network RPA workflow.

Manage audit revisions in Git

Use Git integration to synchronize and back up or restore audit policies. Restoring a policy is distinct from changing a device.

Review logs, report, and correct

Integrated logging and reporting support investigation and evidence. Network RPA can connect findings to corrective tasks; Config Model Editor performs modeled configuration changes and separate node state assessments.

> **Business contribution**
>
> Visible business value comes from maintaining controls and reducing the time that failures remain unresolved. Teams can track recurring drift, audit coverage, and corrective work, then use Compliance Reporting to present that evidence for review.

Config Drift & Audit

Functions, dependencies, and operating boundaries.

RELATED FUNCTIONS AND OPERATING SCOPE

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.

Network RPA: process coordination

Connect targets, tasks, variables, conditions, scheduling, triggers, and notifications across Gluware applications and external systems. Each task uses its supported application or execution mechanism.

Data Explorer: reusable reports

Create reusable report templates and run them on demand or on a schedule. Templates can serve as default exports in Device Manager, Config Drift & Audit, and OS Manager.

Version Control: automation artifacts

Back up and restore Config Drift & Audit policies, Config Model Editor construct instances, and Network RPA process versions.

> **Working with the wider platform**
>
> Config Drift & Audit owns snapshot capture and comparison, audit evaluation, integrated logging, and audit reporting. Git integration supports audit-policy synchronization and backup/restore. Config Model Editor owns configuration intent models, provisioning, and node state assessments. Network RPA coordinates corrective tasks, and Data Explorer supplies reusable reports from stored data.

Supports: Configuration intent & drift management; Continuous compliance & reporting; Configuration audit; Network state audit; Git integration; Backup & restore.

Technical documentation | Request a demo