Backup & restore

Back up supported device configurations and preserve the model, policy, and process artifacts needed to operate them.

The business requirement

Recovery requires more than a saved text file. Teams need a usable device configuration backup, a supported restore path, and recoverable automation definitions. Gluware provides device configuration backup/restore through Device Manager and separate artifact recovery through Git integration.



HOW THE CAPABILITY WORKS

Define backup scope and cadence

Use Device Manager to back up a single device, a selected device group, or scheduled targets. Site organization helps teams apply backup coverage to the required fleet.

Capture, store, and retain backups

Backups are pulled off devices and stored centrally in the Gluware file system. Gluware keeps the latest backup and records changed content; unchanged captures do not create duplicate backup files. Retained backup history and logs follow configured retention policies.

Restore devices and replacements

Restore a known-good backup to the original device or a replacement of the same vendor and model, after establishing the required basic connectivity. Verify the device operating state after restoration. Network RPA can invoke the documented backup task; Device Manager owns the supported restore path.

Preserve automation artifacts separately

Enable Git integration for supported Config Model Editor constructs, audit policies, and Network RPA artifacts. Restore an artifact revision, review it, and use its owning runtime application when execution is required.

Backup & restore

Connect the operating process to defined component responsibilities.

COMPONENTS DELIVERING THE CAPABILITY

Device Manager	Owns device configuration backup, scheduling, status, and supported restore operations.
Network RPA	Invokes supported backup tasks and coordinates surrounding checks and records.
Version Control	Provides Git-based backup/restore for supported automation artifacts.
Config Model Editor	Owns model artifacts, CLI/API state checks, and modeled provisioning.
Config Drift & Audit	Owns audit-policy artifacts and separate snapshot comparison.

OPERATING SCOPE

Device Manager: storage, latest backup and recovery

Backups are pulled off devices and kept centrally in the Gluware file system. Changed content updates the latest backup without duplicate unchanged files; history and logs follow retention policies. Restore to the original device or a replacement of the same vendor/model.

Version Control: supported automation artifacts

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

Config Model Editor: separate provisioning

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.

Business value and measurement

Measure backup coverage, successful captures, failed jobs, and the time required to recover the appropriate configuration or artifact. Keep recovery procedures tied to the target and operation, and verify the device's operating condition after a restore.

Technical documentation | Request a demo
Full vendor and OS coverage

Full vendor and OS coverage