

GLUWARE & CISCO ARE BETTER TOGETHER!

*Automate and Orchestrate your Network
and Data Center with Gluware's Multi-Vendor,
Multi-Platform, and Multi-Domain Pre-Built
Network Hyperautomation Suite*

Consolidate, Simplify & Accelerate Network Automation with Gluware

Gluware delivers the only pre-built network hyperautomation suite in the industry, and is a long-standing Cisco partner. **Gluware is complementary to Cisco DNA Center and offers pre-built API integrations for Cisco Meraki, SD-WAN, ACI and more.**

10 Reasons to Automate Your Cisco Network with Gluware

- 1 Immediately detect configuration drift with the ability to remediate – regardless of platform
- 2 View your global inventory and leverage Cisco Support integration for Cisco EoX API, PSIRTs and SmartNet status
- 3 Automate the process of Operating System (OS) Upgrades
- 4 Run daily compliance audit checks across global networks
- 5 Run daily cross-platform vulnerability checks leveraging Cisco PSIRT and NIST CVEs
- 6 Automate operational state checks for assessment and/or troubleshooting
- 7 Unify islands of automation management across multi-vendor platforms
- 8 View actionable insights from your network using customizable dashboards
- 9 Reduce security vulnerabilities through auditing, OS upgrades, and enforcing config policy
- 10 Eliminate repetitive tasks and evolve from task to process automation

“

*Gluware is a long-standing
Cisco partner. Their automation
suite is optimized for Cisco and
proven to deliver superior
customer outcomes.*

Charles Duffy
Distinguished Systems
Engineer, Cisco Systems, Inc.



Lifecycle Management Benefits & Use Cases

Maintain an Accurate Inventory of Network Devices

Gluware provides a unified inventory through network and device discovery. This allows enterprises to have visibility and a single pane of glass view into what is on the network, across vendors and domains. Gluware provides a view into Cisco legacy devices and Cisco's current product portfolio, and supports organizations with complex networks resulting from M&A activity and best-of-breed approaches. Gluware spans multi-vendor, multi-platform, and multi-domain, and includes built-in integrations for Cisco Meraki, ASA, ACI, SD-WAN (vManage) and more. With this, organizations are able to view a single source of truth and integrate with Configuration Management Databases (CMDBs) and IT Service Management (ITSMs). Using this functionality, teams can easily generate reports on-demand or set up reports as part of scheduled workflows.

Inventory Management

Once Gluware discovers the network devices across the LAN, WAN, Campus and Data Center, a critical first step in automating a network infrastructure is knowing exactly what is connected to the network and the details about each platform, operating system and operational state.

Unknown devices and devices that are End-of-Life/End-of-Support can expose significant security risks. Through integration with the Cisco Support API, you can determine the status of devices for their End-of-Life/End-of-Sale/End-of Support, SmartNet status and security advisories through PSIRTs. Gluware provides NIST integration for multi-vendor CVEs. Having clear visibility into End-of-Support dates and migration paths in one view enables better network planning.

Audit

Execute audits for 3rd party compliance such as PCI-DSS, SOX and HIPPA. Leverage example CIS audits for security standards. Use Gluware to perform initial and ongoing audits to establish and maintain compliance, simplifying audits and reviews with regulators.

Enhance Security and Detect and Remediate Drift for Brownfield and Greenfield Environments

Detecting configuration drift is essential. Remediating it efficiently is vital. With Gluware, our pre-built intelligent out-of-the-box applications enable you to auto-remediate:

- Audit violations
- Misconfigurations
- Configuration drift

Gluware provides greenfield and brownfield support for your configuration and design automation, including the ability to import and manage your current network configurations and designs to prevent network downtime.

*Adding Gluware
Intelligent Network
Automation to your Cisco
Network and Data Center
reduces network outages
by 95% and ensures
100% policy compliance.*

Automating Configuration Policy

- Implement configuration standardization.
 - Standard configurations for AAA, AUX ports, banner, DHCP, DNS, NTP, SNMP and other protocols should be well-defined and implemented consistently across all network devices.
- Implement and automate standard configuration changes.
 - Add VLAN, change QoS policies, and update ACLs.
 - Make changes across authentication configurations like AAA, TACACS, user credentials and password rotations.
 - Ensure accurate monitoring for policies including SNMP and NetFlow.
 - Enable deployment of Cisco Network Access Control (NAC) on campus switches to enhance edge security.
 - Enable automation of data center solutions including EVPN-VXLAN and Cisco ACI.
- Implement and automate changes through Cisco SDN controllers.
 - Make changes to Orgs, Networks and Device settings for Cisco Meraki deployments.
 - Address changes to tenants on a Cisco ACI data center fabric.
 - Use feature-based templates through vManage for SD-WAN.

Maintain Compliance

With pre and post check validation of network changes, Gluware enables you to conduct recurring audit / compliance checks, and even automates remediation approvals with ServiceNow Service Connector. Audits can be OS-specific or work across operating systems with rules defined for each OS. We make regulatory compliance easy by providing:

- Compliance audits and policy enforcement
- Configuration drift detection and auto-remediation
- Inventory assessments
- Site documentation

Remain Agile

Use Gluware to define configuration policy and easily make changes to your infrastructure reliably and at scale. Gluware's declarative behavior makes only the necessary changes and can remove configuration statements that are not part of the policy, providing ongoing cleanup.

OS Version Enforcement

Putting off OS upgrades and security patches puts your network at great risk. But what if you could automate network OS changes and security patches at scale to reduce risk, minimize network downtime, save time and resources, and enable greater agility?

Gluware provides intelligent out-of-the-box OS management across complex multi-vendor, multi-platform environments, with dashboard views of all current OS versions, so you can achieve OS upgrades 300X faster with 0% defects.

Gluware provides broad patching and OS management support, complementing the platforms supported in Cisco DNA Center today.

Automation and Orchestration

Gluware Network RPA brings together pre-built network automation tasks into a single workflow with easy, drag-and-drop navigation. Network RPA allows you to orchestrate tasks and 3rd party API's so you can build, test, deploy, operate and monitor no-code process automation to further accelerate your automation efforts. Network engineers and operations can build processes related to moves, adds, changes, deletes, troubleshooting, assessment and more. Using workflows for process automation in Network RPA ensures the process is followed every time. This can include pre-checks, post-checks, notifications, reporting and integrations with 3rd party systems for data collection and reporting, including the popular ServiceNow ITSM, which uses the pre-built Gluware Service Connector. Integration with StackStorm provides nearly 200 additional API integrations.

Example use cases include:

- Perform a configuration audit and remediate the configuration if there are audit violations.
- Perform a set of assessments including drift, audit and operational state checks to minimize troubleshooting time.
- Perform a configuration drift check before a configuration change to ensure the device is in a known good config state prior to a change.
- Perform state assessments pre/post Operating System upgrades to ensure the devices are in the proper operational state.
- Incorporate email messages, 3rd party messages (like Slack notifications) and send reports as part of automated processes.

IN SUMMARY: Here's Why Enterprises Choose to Add Gluware to Cisco DNA Center

- Device lifecycle management with inventory, EoX, security reports, audit, moves, adds and changes
- Pre-built Cisco integrations for ACI, AireOS, ASA, CatOS, FXOS, IOS/IOS XE, Meraki, NXOS, and SD-WAN (vManage)
- Pre-built ServiceNow integration
- Support for Cisco legacy devices that complement what's available in Cisco DNA Center
- Brownfield and greenfield support for configuration/design automation
- Broad patching and OS management support, including OS upgrade support beyond platforms available with Cisco DNA Center today, which include Cisco Catalyst 9000, Cisco ASR 1000, and Cisco ISR 4000 product families
- Ability to import and manage your current network configuration and design
- Unified suite of award-winning pre-built, intent-based, data model driven, out-of-the-box applications to automate and orchestrate inventory discovery, OS and patch management, audit and compliance, config drift detection and remediation – and more. No programming skills are required, enabling fastest implementation and time to value/ROI in the industry
- Support for multi-vendor networks, enabling enterprises to reduce network management tool sprawl, and use Gluware as the single pane of glass for discovery, assessment, configuration and upgrade management
- A customer success team dedicated to excellence

Ready to Dig Deeper? Schedule a [private executive briefing](#) or [demo](#) now!



sales@gluware.com

www.gluware.com