Device Manager

Discover and inventory devices, inspect configuration and software state, and maintain the fleet information that network automation depends on.



Fleet management should not start with another custom collector.

Acquisitions, new locations, and infrastructure changes continually alter the device fleet. When inventory and device interrogation depend on separate scripts and manual reconciliation, every new automation outcome begins with more foundation work. Device Manager supplies the discovery and inventory constructs teams can apply to their own fleet.

CORE FUNCTIONALITY

Plan and run network discovery

Build and run discovery plans using seeded-device discovery with ARP and CDP/LLDP, or subnet crawling. Discover hardware, software, and configuration information for the fleet.

Organize devices in Site Explorer

Create sites and assign devices. Site context is available to other applications, including Config Drift & Audit and Network RPA.

Manage the fleet in Device Explorer

Add devices manually, import/export devices, or add them through the API. Run device discovery and use multi-edit, grouping, search, filtering, and sorting for fleet operations.

Inspect and protect device configurations

Search configurations, capture snapshots, reboot devices, and review logs. Backups are stored centrally, changed content is recorded without duplicate files, and retention is configurable. Restore to the original device or the same vendor/model replacement.

Connect lifecycle and security intelligence

Gluware uses API integration with NIST/NVD for multi-vendor CVE information and Cisco Support API integration for Cisco PSIRT advisories, including their CVEs. Cisco CVE information comes from Cisco, not NIST/NVD. Cisco Support API also provides EoL/EoS and SmartNet status.

> **Business contribution**
>
> A usable device inventory gives teams a starting point for OS upgrades, configuration standardization, and exposure assessment. Teams can focus on fleet coverage and the changes required by the business, while using built-in discovery and inventory capabilities.

Device Manager

Functions, dependencies, and operating boundaries.

RELATED FUNCTIONS AND OPERATING SCOPE

Central backup storage and device 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.

Vendor and OS coverage

Inventory and discovery cover Cisco IOS/IOS XE, IOS XR, NX-OS, ACI and Meraki; Juniper Junos; Arista EOS; HPE Aruba; Palo Alto PAN-OS; Fortinet FortiOS; F5 TMOS; and additional vendor platforms. Operation coverage varies.

OS Manager: software deployment

Use OS catalogs and deployment plans to select approved images, validate readiness, schedule upgrades or downgrades, and review execution results on supported devices.

Config Model Editor: configuration intent

Model multi-vendor CLI and API intended configuration state with declarative enforcement.

> **Working with the wider platform**
>
> Device Manager owns inventory, discovery, ad hoc inspection, and supported device backup/restore and reboot. Config Model Editor owns configuration intent models and provisioning. Config Drift & Audit owns snapshot comparisons and policy checks; OS Manager owns software deployment plans. NetBox and/or ServiceNow CMDB sync can connect discovered fleet information to mapped external records.

Supports: Network discovery & onboarding; Device & OS lifecycle management; Configuration intent & drift management; Network exposure management; Network discovery; Network state assessments; Device inventory; NIST & Cisco CVE/PSIRT integrations; Network state audit; OS management & patching; Backup & restore.

Technical documentation | Request a demo
Full vendor and OS coverage