

stella

STANDARDISE, CENTRALISE,
AUTOMATE



Stella Central

Your portfolio of
networks securely
managed,
documented,
and without
human error.

Stella is an industry-specific platform that has been built to eliminate labour-based challenges. In full implementation, Stella Central is your single network operating platform, allowing you to automatically discover, audit, configure, manage, and document your portfolio of networks.

Stella Central

Stella Central delivers Discovery, Compliance and Configuration modules with Monitoring and Reconfiguration functionality.

Why Stella Central

- Network documentation is always up to date
- Network risk profile is identified in minutes, not months
- Baseline network performance enables fact-based troubleshooting
- Lower mean time to resolution with an integrated Stella deployment
- Critical equipment performance monitoring supports proactive engineering
- Stella supports a clear demarcation of accountabilities for field and network engineers

- Stella frees your high-value engineers to focus on network performance exceptions and orchestration improvements
- With Stella Monitoring, only your most senior network engineers require direct network access permissions, dramatically reducing error rates and escalations
- The Primary Customer can extract their own network reports
- Service Providers can be limited to the networks that they manage
- Stella interfaces with several authentication gateways

Stella Satellite deployment

The Stella Satellite can be deployed on dedicated Stella-certified hardware or using an OVF image on your existing on-premises virtualisation infrastructure.

Human engineer vs Stella



Human Network Engineer



Stella

	Human Network Engineer	Stella
Discovery	9.3 hours	90 seconds
Compliance	9.8 hours	11.5 minutes
Configuration	4 hours	30 minutes
Documentation		✓
Accuracy		100%

Based on an average network with 12-edge switches, core switch, firewall and wireless controller

FAQs

What is included with Stella Central?

Stella Central comes with orchestration modules designed specifically to the network standard.

Stella Central starts with Discovery of your network then checks the Compliance against specific brand standards. For new installations, the Configuration module takes your requirements and configures the network according to the given standard. For existing equipment, Stella Central holds Reconfiguration to those same standards and documentation is updated automatically. Any performance or configuration problems on your network are highlighted by Stella Central in the Monitoring module.

How is Stella Central different to what I already use?

Stella is a curated collection of high-quality automated orchestration playbooks that remove the need for network engineers to directly access active equipment. All changes are aligned by Stella to a Network Standard for configuration and reporting, enabling the network operator to run specific reports and the Primary Customer to draw their own reports.

How do I get my network on Stella Central?

Our onboarding specialists will walk you through the process to ensure all your networks are imported error-free into Stella Central and can be managed to the appropriate network standards.

Who owns the data?

The Primary Customer owns all data relating to the networks stored in their instance of Stella Central. Service Providers to the Primary Customer will have access to the Primary Customer's Stella Central instance.

Where is the data kept?

All Stella Central data resides in the Primary Customer's instance of Stella Central, hosted in AWS.

What does Stella Central give me?

Your license enables you to operate Stella Central over your specified networks and their active equipment. Any bespoke report and its output remain your property.

- **Discovery** reports the equipment details on your network.
- **Compliance** gives a score card for configuration, including VLANs and IP addresses, according to the provided network standards.
- **Configuration** configures your equipment correctly from the start according to your design and the provided network standards, and provides detailed, accurate documentation.
- **Reconfiguration** ensures your changes are correct and according to your network standards, then shows the changes made and who authorised the change.
- **Monitoring** indicates any problems with performance on critical equipment or equipment that is down, and interfaces to your incident response system to create tickets.

Is Stella Central secure?

Stella takes security seriously and does not hold personal or financial information. We present a minimal attack surface and use AWS-managed services where possible. Our architecture and configuration are built to AWS best practices.

What technologies does Stella Central leverage?

Stella Central is built on AWS infrastructure and many mature technologies such as Linux, SSH, Python, Ansible, and OpenVPN.

How is Stella Central supported?

Stella Central customer support is available via email, chat, and phone, 24x7x365.

Supported equipment

Switches

OEM	Models
Aruba/HP	25xx, 26xx, 29xx, 38xx, 54xxRzl2, 6xxx, 83xx, 84xx
Cisco	29xx, 35xx, 37xx, 38xx, 45xx
Ruckus	71xx, 72xx, 74xx, 76xx, 78xx

Firewalls (documentation only)

OEM	Models
Cisco	ASA 55xx
Fortinet	Fortigate 50E, Fortigate 60E
Juniper	SRX100, SRX300, SRX320, SRX340

Wireless Controllers

Alcatel-Lucent	OAW-4650
Aruba	7200 Series Mobility Controllers
Cisco	5500 Series
HP	MSM760
Ruckus	SmartZone 100 Series, Zone Director, Virtual SmartZone

Supported services

- Automated documentation of hardware and versions
- Compliance checks against given network standards
- Base configuration using given network standards
- Templated layered-services configuration using given network standards
- Firmware upgrades
- Performance monitoring of critical equipment and status monitoring of non-critical equipment

Outputs

- Inventory report of network devices discovered, including OEM, model, hostname, serial number, firmware version, EOSL date, approved-hardware status, and warranty status
- Unidentified active device report
- Report the results of all compliance checks against the documented configuration standard, EOSL and approved-hardware list
- Audit logging of actions including report runs and change to sites, device configuration, and standards
- Details of configuration changes that were made and who committed the change
- Notifications (email/Slack/SMS/Teams)
- Point-in-time reporting including Asset Inventory, Port Mapping, and Cabling Matrix documents
- Monitoring alerts via tickets in your incident response system
- Monitoring status dashboard and diagnostics reporting

To find out more, email us at info@stellanetworks.io
www.stellanetworks.io

