

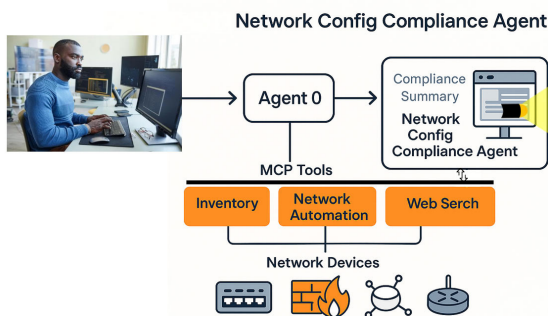
Agentic NetOps

Network Config Compliance Agent



Autonomous, multi-vendor network configuration validation - without writing a single device command

The Network Config Compliance Agent logs directly into network devices, intelligently determines the right vendor-specific commands to issue, and validates every configuration control point against industry best practices or your organization's custom policies - with no manual command specification required. Supports on-demand, scheduled, and event-triggered operation across any multi-vendor environment including Cisco, Juniper, Arista, Palo Alto, Fortinet, and more.



Fabrix.ai Copilot

8:42 PM show me the network config compliance of device 10.95.140.21

I'll help you check the network configuration compliance for device 10.95.140.21. Let me first gather the necessary context and then retrieve the compliance information.

History Summary: User is requesting network configuration compliance check for device 10.95.140.21. Active Template: network-config-compliance-template. Justification: The conversation history shows this is the first request for compliance analysis of a specific device, and the template provides the exact workflow for network compliance validation.

Network Configuration Compliance Report

Executive Summary:

Device: 10.95.140.21

- Total Policies Evaluated: 20/20
- Overall Compliance Rate: 35%
- Critical Issues: 12
- Compliant Systems: 7
- Non-Compliant Systems: 12
- Unable to Assess: 1

Detailed Compliance Analysis:

ID	Compliance Rule	Check Performed	Result	Details
1	No default or weak enable passwords	Look for 'enable password' or 'enable secret'	NON_COMPLIANT	Device lacks enable password/secret configuration entirely
2	Use enable secret instead of enable password	Ensure 'enable secret' is configured	NON_COMPLIANT	Device lacks enable secret configuration
3	AAA authentication is enabled	Presence of 'aaa new-model'	NON_COMPLIANT	AAA is explicitly disabled with 'no aaa new-model'

Enter a prompt

Key Features & Highlights

- **Natural Language Compliance Queries:** Ask Fabrix.ai Copilot to run a compliance check on any device in plain English - no CLI or query syntax required.
- **Custom & Industry Standard Policies:** Apply CIS benchmarks, NIST SP 800-53, PCI-DSS, or define your own organizational compliance rules without writing device commands.
- **On-Demand, Scheduled, or Event-Triggered:** Run ad-hoc via Copilot, on a recurring schedule, or automatically triggered by configuration changes or incident alerts.
- **Detailed Per-Device Compliance Reports:** Full audit report with pass/fail per rule, raw evidence, compliance rate, and actionable remediation steps per device.
- **MCP Tool Integration:** Works with Inventory, Network Automation, and Web Search MCP tools - giving the agent complete network environment context.

Technical Outcomes & Benefits

- **Zero Manual Command Specification:** Agent autonomously determines the correct commands per vendor and OS. Network admins define policies, not device syntax.
- **Agentless, Non-Intrusive Device Access:** Connects over SSH, NETCONF, or REST APIs. No software installed on devices, no disruption to live network operations.
- **Uniform Coverage Across Heterogeneous Networks:** A single policy framework enforced uniformly across Cisco, Juniper, Arista, Palo Alto, and Fortinet - no vendor lock-in.
- **Faster Incident Response & Audit Readiness:** Event-triggered checks surface config risks immediately - reducing MTTR and keeping compliance teams audit-ready.
- **Reduced Compliance Overhead & Human Error:** Eliminates manual audit processes and operator errors in command selection - freeing network teams for higher-value work.