

Agentic Actions: Resolve Issues Faster, Build Worry-Free Networks



What if your network could detect, investigate, and resolve issues before users feel impact? Agentic Actions transforms fragmented troubleshooting into AI-powered, outcome-driven operations turning telemetry into fast, validated action aligned to business priorities.

Benefits

Agentic Actions helps NetOps teams move faster with less effort, reducing operational overhead while improving user experience and application performance.

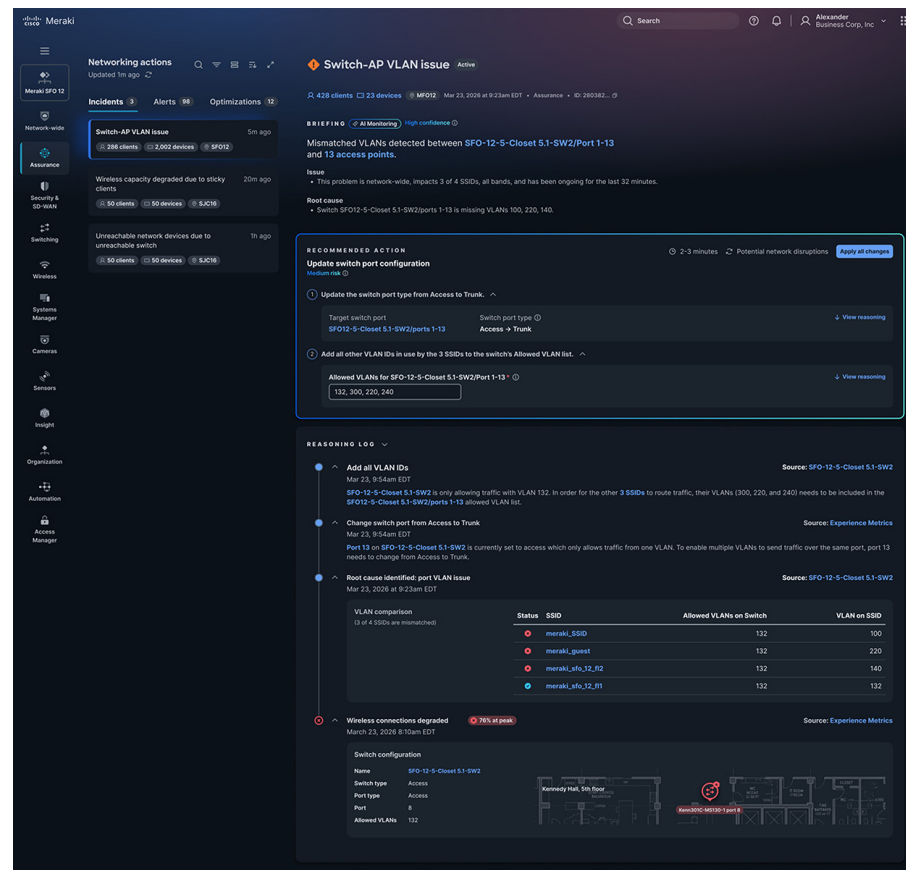
- Accelerate resolution with AI-powered root cause analysis and guided remediation
- Eliminate manual triage with prioritized incidents and high-confidence actions
- Prevent recurring issues through automation and agentic execution
- Scale operations with repeatable workflows and built-in validation
- Resolve issues before users are impacted with continuous assurance

By connecting signals, decisions, actions, and validation, Agentic Actions transforms reactive troubleshooting into fast, predictable, outcome-driven operations.

Overview

Drowning in alerts but still missing what matters? Modern networks generate endless signals, but most don't tell you what's actually impacting users or how to fix it. Agentic Actions cuts through the noise, correlating events, pinpointing root cause, and driving remediation in a single workflow.

From a single place, you can act instantly or enable agentic agents to operate within defined policies and guardrails. Start building worry-free networks that detect issues earlier, respond faster, and scale operations with confidence.



Switch-AP VLAN issue Active

428 clients 23 devices MFO12 Mar 23, 2026 at 9:23am EDT • Assurance • ID: 280382...

BRIEFING All Monitoring High confidence

Mismatched VLANs detected between SFO-12-5-Closet 5.1-SW2/Port 1-13 and 13 access points.

Issue

- This problem is network-wide, impacts 3 of 4 SSIDs, all bands, and has been ongoing for the last 52 minutes.

Root cause

- Switch SFO12-5-Closet 5.1-SW2/ports 1-13 is missing VLANs 100, 220, 140.

RECOMMENDED ACTION 2-3 minutes Potential network disruptions [Apply all changes](#)

Update switch port configuration Medium risk

- Update the switch port type from Access to Trunk.

Target switch port	Switch port type
SFO12-5-Closet 5.1-SW2/ports 1-13	Access → Trunk
- Add all other VLAN IDs in use by the 3 SSIDs to the switch's Allowed VLAN list.

Allowed VLANs for SFO-12-5-Closet 5.1-SW2/Port 1-13
132, 300, 220, 240

REASONING LOG

- Add all VLAN IDs** (Source: SFO-12-5-Closet 5.1-SW2)

Mar 23, 9:54am EDT

SFO-12-5-Closet 5.1-SW2 is only allowing traffic with VLAN 132. In order for the other 3 SSIDs to route traffic, their VLANs (300, 220, and 240) needs to be included in the SFO12-5-Closet 5.1-SW2/ports 1-13 Allowed VLAN list.
- Change switch port from Access to Trunk** (Source: Experience Metrics)

Mar 23, 9:54am EDT

Port 13 on SFO-12-5-Closet 5.1-SW2 is currently set to access which only allows traffic from one VLAN. To enable multiple VLANs to send traffic over the same port, port 13 needs to change from Access to Trunk.
- Root cause identified: port VLAN issue** (Source: SFO-12-5-Closet 5.1-SW2)

Mar 23, 2026 at 9:23am EDT

VLAN comparison	Status	SSID	Allowed VLANs on Switch	VLAN on SSID
13 of 4 SSIDs are mismatched	🔴	meraki_guest	132	100
	🔴	meraki_sfs_12_62	132	220
	🔴	meraki_sfs_12_81	132	140
	🟢	meraki_sfs_12_81	132	132
- Wireless connections degraded** (Source: Experience Metrics)

March 23, 2026 8:10am EDT

76% at peak

Switch configuration

Name	Switch type	Port type	Port	Allowed VLANs
SFO-12-5-Closet 5.1-SW2	Access	Access	13	132

Trends and challenges

Rising complexity. Slower resolution.

Enterprise networks are more distributed, dynamic, and dependent on infrastructure outside IT's control. Cloud, SaaS, hybrid work, and AI applications have increased operational complexity, while most NetOps teams still rely on fragmented tools and reactive workflows to keep up. As a result, users often experience issues before IT is aware.

At the same time, expectations for always-on digital experiences continue to rise. But siloed monitoring tools, alert storms, and manual correlation slow root cause analysis and delay resolution, forcing teams to navigate disconnected data across multiple interfaces.

The result:

- Too many alerts with little actionable context
- Slow, manual troubleshooting across siloed tools
- Limited ability to automate and scale with confidence
- Increased risk of downtime and poor user experience

Organizations need more than visibility. They need systems that can prioritize, decide, act, and validate outcomes in real time.

How Agentic Actions Works

Agentic Actions operates within a closed-loop operational system that connects signals, root cause analysis, automation, and validation across the network lifecycle.

Unify and prioritize signals

Aggregates incidents, alerts, and optimization opportunities across assurance, performance, and security domains, surfacing what matters most based on user impact, blast radius, and operational priority. Real-time detections and proactive recommendations help teams focus on the issues that require immediate attention.

AI-driven correlation and RCA

Correlates telemetry, topology, configuration changes, and experience data to transform fragmented signals into clear, explainable troubleshooting workflows. Agentic Actions identifies root cause with confidence scoring and supporting evidence, prioritizing issues based on business impact and delivering actionable next steps, not just insights.

Trusted action and automation

Enables guided remediation, repeatable automation, and agentic execution with human oversight and built-in governance. Teams can

accelerate resolution through step-by-step workflows while reducing manual intervention and operational inconsistency at scale.

Embedded operational workflows

Integrates directly into operator workflows with embedded entry points across devices, topology views, and experience dashboards. Teams can move seamlessly from detection to RCA to remediation without switching tools, while integrations with IT service management (ITSM) platforms help align operations across teams.

Centralized configuration and control

Provides unified management for alerts, thresholds, notifications, automation policies, and execution controls. Smart thresholds reduce false positives and alert fatigue, while policy-driven governance, approval workflows, and audit trails help teams automate with confidence.

Continuous validation

Closes the loop by validating every action against live telemetry, testing, and real user experience. Agentic Actions confirms whether remediation improved outcomes, detects regressions or instability, and helps ensure every action is safe, effective, and repeatable at scale.

Cisco Capital

Financing to help you achieve your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more.](#)

Use cases

Table 1. Industry use cases

Industry	Agentic Actions use case
Retail	Detect and prioritize storewide connectivity or point-of-sale degradation as incidents. Correlate WAN, Wi-Fi, and SaaS signals to isolate root cause, then execute remediation or delegate to agents to restore service and validate impact before revenue is affected.
Healthcare	Identify degradation in clinical applications or device connectivity across hospital networks. Use AI-driven RCA to pinpoint issues and trigger guided or agentic remediation workflows, helping ensure rapid recovery and validated user experience for patient-critical systems.
Financial services	Correlate performance issues across trading platforms, branches, and cloud apps. Prioritize by business impact, execute controlled remediation with policy guardrails, and validate outcomes to maintain uptime, compliance, and transaction integrity.
Manufacturing/ industrial	Detect anomalies impacting production systems and connected devices. Correlate signals across IT/OT boundaries, automate remediation for recurring issues, and validate recovery to prevent downtime and maintain operational continuity.
Public sector/ education	Surface high-impact connectivity issues across campuses and distributed users. Enable centralized teams to diagnose root cause, execute fixes, or delegate to agents, helping ensure consistent access to learning platforms and public services.

The Cisco Advantage

Only Cisco delivers a true closed-loop, agentic system for worry-free network operations, connecting signals, root cause analysis, automation, and validation across the entire digital ecosystem.

Cisco uniquely provides:

- End-to-end visibility across enterprise, internet, cloud, SaaS, and third-party networks
- A unified workflow that moves from detection to RCA, action, and validation
- Explainable, correlated RCA with confidence scoring and actionable guidance
- Built-in automation and agentic execution with governance and human oversight
- Continuous validation tied directly to real user experience outcomes
- A unified platform combining Cisco networking, Cisco ThousandEyes, and cross-domain intelligence

Unlike siloed or domain-specific solutions, Cisco enables teams to operate across the full digital experience with speed, precision, and validated outcomes at scale.

Table 2. Operational use cases

Operational area	Agentic Actions use case
Incident detection and triage	Aggregate incidents, alerts, and optimizations into a prioritized queue. Automatically correlate signals to identify root cause and accelerate triage, reducing time spent navigating tools and focusing teams on high-impact issues.
Root Cause Analysis (RCA)	Correlate events, configuration changes, topology, and experience signals to isolate root cause with confidence. Provide explainable RCA and recommended next best actions to eliminate guesswork and speed resolution.
Guided and agentic remediation	Execute fixes directly through guided workflows, or delegate to agentic agents to investigate and remediate within defined policies, thresholds, and approvals, enabling consistent, scalable operations.
Automation at scale	Convert repeatable fixes into automated workflows. Define guardrails for agent execution, allowing the system to resolve recurring issues autonomously while maintaining governance and control.
Outcome validation	<p>Validate every action with before-and-after analysis tied to user experience.</p> <p>Detect regression, confirm recovery, and help ensure that actions are effective, closing the loop between detection, action, and outcome.</p>

Learn more

Start building worry-free networks, with confidence.

See how Agentic Actions helps you cut through alert noise, pinpoint root cause instantly, and automate remediation at scale. Unify operations and reduce MTTR across your entire environment. Learn more and request a [demo](#).