CASE STUDY

compucom
Technology Driven.
People Powered.

Cisco Identity Service Engine (ISE)

Fixing What Hardware Checks Miss:

The Root Causes Behind a Year of Wireless Disruption

SNAPSHOT

A large Canadian regional hospital network had been experiencing persistent instability in its Cisco ISE deployment, including recurring SEV1 outages tied to authentication delays and 802.1X failures. A standard Cisco ISE Health Check provided baseline data, but it did not uncover the underlying issues. Cisco brought in our experts to extend the investigation beyond the initial hardware-focused review, revealing and correcting deep configuration, policy, and architectural problems that had gone unresolved for more than a year.

This healthcare provider's environment spans 17 hospitals and clinics, all funneled through two wireless LAN controllers and a single ISE deployment. When authentication latency spiked, every hospital experienced a multi-hour wireless outage — impacting clinical operations across the entire region.

Challenges: Chronic Instability Meets Clinical Operations

Loose policies, unmanaged configuration drift, and years of inconsistent maintenance were beginning to affect both security and patient care. During outages, critical medical devices — dialysis machines, glucose monitors, diagnostic imaging equipment, and mobile ultrasound units — would drop off the network for hours at a time.

Although the customer's basic Cisco ISE Health Check outputs appeared largely "green," the report did not connect warnings (such as certificate issues and high swap utilization) to real-world impact. In practice, the organization continued to experience repeated, hours-long wireless outages each quarter. A pass/fail report could not explain why 802.1X users could not reliably connect.

Service Impacting Performance Failures

- High-latency RADIUS responses causing authentication delays and outages
- Recurring SEV1 incidents tied to unpredictable performance spikes

Misconfiguration and Policy Design Issues

- High-resource operations triggered on every RADIUS request
- Poorly constructed and poorly ordered policy rules
- Deviation from Cisco best practices for NAD integration

Infrastructure and Architecture Gaps

- Improper infrastructure sizing
- Backend services consuming excessive resources
- No clear correlation between configuration issues and service impact

These were not hardware failures. They were rooted in policy logic, system design, and operational configuration — precisely the areas where our expertise goes beyond the scope of a standard Cisco health check.

Action: Root Cause Analysis at the Policy Layer

We started with our own comprehensive health check, which then evolved into a structured, multi-phase remediation program focused on stabilizing authentication services and eliminating the root causes of latency and outages. We applied a three-phase, architecture-driven methodology to correct the issues that had eluded traditional Cisco TAC/BU case-based troubleshooting.

Key Actions:

Phase 1 — Immediate Stabilization

- Reordered and optimized RADIUS policies
- Removed unnecessary, resource-intensive operations
- Tuned backend services to reduce processing overhead
- Applied Cisco best practices for NAD integration

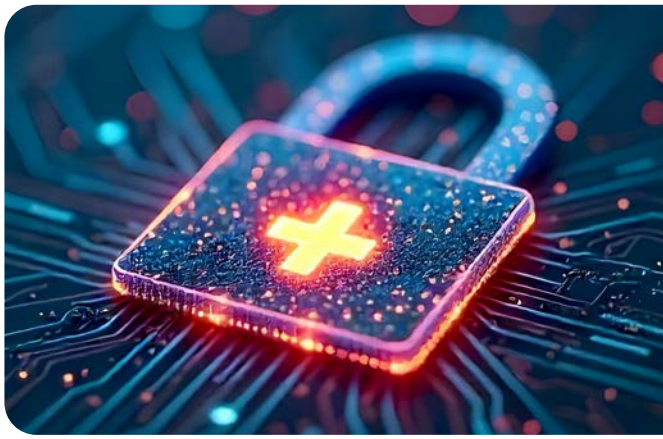
Phase 2 — Infrastructure Optimization

- Right-sized ISE personas and resources
- Redistributed load across nodes
- Improved redundancy and failover behavior

Phase 3 — Policy and Architecture Modernization (In Progress)

- Rationalized and simplified policy sets
- Strengthened governance and operational alignment
- Prepared the environment for future certificate-based authentication

Results: Stability Restored. Latency Eliminated.



Dramatic Performance Improvement Even After Phase 1

- RADIUS latency reduced by over 93% — from 840 ms to 50 ms
- Significant reduction in SEV1 outages and authentication failures

Operational Stability

- Wireless 802.1X services stabilized across the environment
- Predictable, reliable authentication performance restored

Clear Path Forward

- A structured roadmap now guides long-term architectural improvements
- Remaining phases will strengthen scalability, governance, and security posture

Looking to the Future

Our goal is to move the customer beyond basic stability and into a performance tier capable of supporting real-time mobility — such as VoIP roaming and wireless video conferencing — while maintaining strong access control through RADIUS and 802.1X, including certificate-based authentication.

Phase 1 restored stability; the remaining phases will drive latency toward the threshold required for real-time services (approximately 50 ms or below) and establish a foundation for long-term scalability.

Cisco Partner
Security Preferred

Key Outcomes

This engagement demonstrates that "green" infrastructure metrics do not equal operational health. By focusing on *how policies are built, ordered, and maintained,* we delivered measurable business outcomes:

1 Stability Restored, Risk Reduced
Chronic authentication outages were eliminated through architecture-led policy redesign, restoring reliable access across all hospitals.

2 Built to Scale, Ready for What's Next
Modernized infrastructure and policy foundations now support certificate-based authentication and future growth without added complexity.

3 Governance That Performs
Clear, enforceable policies improved operational consistency, accelerated troubleshooting, and strengthened confidence at both IT and executive levels.

compucom
Technology Driven.
People Powered.

Learn more about Compucom and how we source, integrate, and support your technology needs at compucom.com

05.8889578.26