CASE STUDY

compucom
Technology Driven.
People Powered.

Cisco Identity Service Engine (ISE)

Enhanced ISE Health Check Reveals Hidden Risks Across Five Continents

SNAPSHOT

A multinational mining corporation operating across North America, the United Kingdom, South America, the Caribbean, and Africa initiated a Cisco ISE upgrade that included a standard Cisco ISE Health Check. While the check provided a useful baseline, Compucom's experts went far beyond its hardware-centric scope — uncovering deep configuration and policy issues affecting more than 60,000 endpoints worldwide.

The customer's environment is exceptionally large and complex: over 60,000 endpoints, global offices and mines, and roughly 20 ISE servers distributed in data centers across North America, South America, the Caribbean, and the UK. Years of admin turnover and incremental changes had created significant policy bloat, conflicting rules, and widespread misconfigurations.

Recognizing the growing operational challenges, we encouraged the customer to proceed with a comprehensive health check — one that goes well beyond Cisco's standard hardware based review. The result was a long-overdue, in-depth assessment that finally exposed the root causes impacting their global access infrastructure.

Challenges: Configuration Chaos Meets Global Operations

Policy and Access Control Issues

- Policies misaligned with actual business services
- Conflicting rules allowed endpoints with incorrect credentials to access services

Uncontrolled Device Access

- Widespread associate abuse of mobile and BYOD access on corporate WLANs
- Unauthorized devices consuming bandwidth in remote mines and regional offices
- Corporate endpoint configuration standards and practices inconsistently followed across different regions

Lack of Visibility

- No reliable method to audit which endpoints were trusted managed assets and which were not when they were connecting to services, with valid credentials

Action: Modern Authentication. Clean Policies. Full Control.

The engagement evolved from a routine Cisco ISE Health Check into a full-scale policy and access control remediation initiative. We collaborated with the customer's mobile and endpoint teams across North America, South America, and Europe to identify certificate usage, validate endpoint profiles. Cisco ISE rules were rebuilt to not only confirm trusted asset access but to also provide complete visibility into endpoint configuration shortcomings that could be displayed from country down to site level resolution.

We applied a two phase, use-case–driven methodology designed to uncover and correct the configuration and policy issues.

Key Actions:

Audit and Visibility Enhancements

- Created a global audit framework to map endpoints, credentials, and service access
- Audited and corrected service account usage

Policy and Authentication Modernization

- Removed MSCHAPv2 and all password-based authentication from corporate laptop SSIDs
- Restricted mobile WLAN access to MDM-managed devices using EAP-TLS

Endpoint Compliance Improvements

- Identified/remediated misconfigured laptops (missing GPOs)
- Identified/remediated mobile devices missing MDM profiles

Policy Simplification and Governance

- Reduced wireless access policy rules from **70 to 9**, dramatically improving clarity and maintainability
- Drove global organizational adoption of tighter, certificate-based network access control
- Drove tighter alignment and documented points of dependencies between internal IT teams of Cyber Security, Network Infrastructure, Endpoint and Mobile management

Results: Cleaner Policies, Stronger Security, Less Disruption Risk

Rebuilt ISE rules provided the customer with critical visibility. For example, they had planned to disable the mobile SSID entirely. Our analysis revealed that nearly 600 corporate devices, in just one region, were incorrectly using that SSID. Disabling it would have caused widespread disruption across global sites. Our visibility prevented that outcome and enabled a controlled, informed remediation process.

Through this engagement, the customer achieved real stability. Policies were reduced from roughly 70 to just 9, each aligned to a clear use case — corporate laptops, managed mobile devices, guest access, and more. The environment became understandable, predictable, and supportable.

Just as importantly, the health check exposed areas of the organization that were not adhering to their own standards. This shifted the narrative for the network team, who had long been blamed for issues they could not control. Our findings showed that endpoint and device-management gaps, not network failures, were undermining the access strategy.

By clarifying where compliance was breaking down, we helped establish accountability across teams. Had every team followed established standards, remediation would have been a simple three-minute configuration change. Instead, years of unmanaged drift had turned it into a five-month project.

Across all global locations, the customer achieved:

Stronger, Certificate-Based Access Controls

- Corporate WLAN restricted to corporate laptops using EAP-TLS only
- Mobile WLAN restricted to MDM-managed devices using EAP-TLS only

Improved Network Hygiene

- All BYOD/unmanaged devices removed and migrated to a redesigned guest network
- Guest access modernized with self-sponsorship

Operational and Security Gains

- Policies fully aligned with production services
- Reduced threat vectors and bandwidth abuse
- Significant improvement in service quality at remote mines and regional offices

CISCO Partner
Security Preferred

Enhanced Cisco ISE Health Check: The Compucom Advantage

1 Global Access Control, Realigned
A simplified, use-case–driven policy architecture restored clarity, consistency, and predictable access across all regions.

2 A Modern, Certificate Driven Identity Framework
Password-based authentication was eliminated, enabling a secure, scalable foundation for long-term growth and operational resilience.

3 Governance That Drives Accountability
Clear visibility, stronger policy discipline, and cross-team alignment reduced operational risk and ensured every team understood its role in maintaining a secure access environment.

compucom
Technology Driven.
People Powered.

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

05.8889818.26