



Cisco SDA **Health Check by** **WhiteSpider**

WhiteSpider is an industry expert in enabling business transformation through the power of digital technologies.

Working across the globe, we design, deliver, and manage Software Defined technologies that transform IT operations, secure business infrastructure, and enhance user experience.

Service overview

Cisco Software Defined Access (SDA) provides a secure, automated, policy-driven network fabric that simplifies enterprise LAN operations. Deployments can range from a single-site fabric using Catalyst Centre (formerly DNAC) to large multi-site, multi-fabric architectures with thousands of endpoints.

SDA provides segmentation, automated provisioning, rich analytics, and consistent identity-based access policies. As deployments grow, configuration drift, overlooked warnings, and unnoticed performance issues can accumulate. While these may not immediately cause outages, they can eventually impact stability, user experience, and security posture.

WhiteSpider's SDA Health Check reduces the likelihood of future issues and strengthens operational readiness by validating the fabric against best practice, performance baselines, and Cisco platform guidance.

What we do

The SDA Health Check assesses a single-fabric or multi-fabric environment, reviewing Catalyst Centre, border/edge nodes, control-plane nodes, policy configurations, and integrations such as ISE.

Using a combination of Catalyst Centre automation, API-driven data collection, and expert manual analysis, WhiteSpider engineers create a detailed picture of the SDA environment. Findings and remediation recommendations are delivered in a comprehensive report.

Benefits

A WhiteSpider SDA Health Check enables you to:

- ✓ **Increase policy assurance:**
Validate that identity-based and segmentation policies are operating as intended.
- ✓ **Improve stability:**
Detect misconfigurations, redundant fabric constructs, or performance issues before they cause user impact.
- ✓ **Enhance security posture:**
Identify gaps in macro/micro segmentation, SGT usage, and ISE integration.
- ✓ **Optimise fabric performance:**
Review underlay health, wireless fabric integration, scale limits, and endpoint behaviour.
- ✓ **Ensure best practice design:**
Confirm that your fabric design aligns with Cisco recommended architecture and current operational demands.

Typical activities

Catalyst Center (DNAC)

- Appliance health, CPU, memory, disk utilisation
- Software version/EoL status
- Cluster health (3-node/4-node)
- Telemetry ingestion & assurance data

Outcome:

Ensures Catalyst Center is healthy and capable of delivering accurate insights.

Fabric Infrastructure

- Underlay routing health
- Border/control-plane node availability
- Anycast gateways configuration
- Fabric site connectivity
- Scale checks (VN limits, endpoint limits, transit control-plane capacity)

Outcome:

Validates core fabric services and scalability.

Policies & Segmentation

- VN and SGT design correctness
- Policy matrix consistency
- Contract/SGT mappings
- Border handoff policies

Outcome:

Ensures segmentation is predictable and secure.

Access Layer (Edge Nodes)

- Interface utilisation and errors
- PoE status
- Host-onboarding consistency
- Authentication/ISE integration checks

Outcome:

Identifies physical or policy-driven access issues.

Wireless (if fabric-enabled)

- Fabric-enabled wireless settings
- WLC to Catalyst Center integration
- AP fabric roles and onboarding

Outcome:

Verifies wireless fabric alignment and user experience.

Operations & Security

- Alarms and events review
- Backups and disaster recovery processes
- AAA, SNMP, Syslog, NTP/DNS validation
- Vulnerability checks against DNAC/SDA images

Outcome:

Ensures ongoing operational readiness.



Telephone: +44 20 3773 2380
E-mail: info@whitespider.com
Website: www.whitespider.com

