Service Brief

Guardian Support

majentai

Cisco Identity Services Engine (ISE) Guardian Support

Cisco Identity Services Engine (ISE) Guardian Support is a support engagement designed to keep your ISE environment stable and aligned to evolving security and business requirements. Majentai provides health oversight, incident triage, change advisory, and policy optimization so teams can sustain access services with lower risk and better continuity.

Overview

The ISE Guardian Support service sustains Cisco ISE after deployment through structured monitoring, guided troubleshooting, governed changes, and repeatable operational practices that protect authentication, authorization, guest access, profiling, and segmentation-related services while establishing the operating model needed to improve resilience, reduce disruption, and scale support with confidence.

- ISE health and integration monitoring
- Incident triage and troubleshooting guidance
- Policy and change advisory support
- Runbooks, reporting, and service reviews
- Ongoing optimization and roadmap input

Business Outcomes

This engagement reduces operational risk by combining structured support and controlled change practices into a sustainable operating model that protects critical access services. It gives stakeholders clearer visibility, ownership, and a path to improve resilience, supportability, and future ISE expansion.

- Reduce access service disruption and outage risk
- Improve confidence in policy and platform changes
- Strengthen visibility into ISE operational health
- Accelerate steady-state maturity and optimization

At a Glance

Objectives

- Maintain stable and resilient ISE day-2 operations
- Reduce disruption across access and policy services
- Establish governed support and change workflows

Scope

- Support for defined ISE nodes, personas, and services
- Coverage across identity, network, and security integrations
- Recurring health checks, incident support, and review cadence

Deliverables

- Guardian Support model and operating workflows
- ISE monitoring, runbook, and reporting structure
- Ongoing recommendations and optimization summary

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders, confirm in-scope ISE functions, sites, services, and support expectations, then review current architecture, integrations, ticketing workflows, recurring issues, and operational priorities that will shape the Guardian Support model.

Phase 2: Solution Design and Planning

Define service components, roles, responsibilities, severity model, communication cadence, health indicators, runbook requirements, and reporting structure needed to support ISE consistently across incidents, changes, and steady-state operations.

Phase 3: Build, Implement and Validate

Onboard Cisco ISE into agreed monitoring, escalation, and support workflows, document environment-specific knowledge, validate incident and communication runbooks, and tune the model through early-life support and real-world process feedback.

Phase 4: Operations & Recommendations

Transition the service into steady-state operations through recurring health checks, incident support, advisory input for planned changes and upgrades, scheduled service reviews, and a roadmap for ongoing optimization and future ISE enhancements.

Majentai is a world-class Cybersecurity services provider, dedicated to implement, integrate and operate the most resilient Cybersecurity platforms using proven state-of-the-art technologies. With a team of seasoned experts and cutting-edge technology, we deliver comprehensive solutions tailored to our clients' unique needs, ensuring their digital assets remain secure in an increasingly complex cyber landscape.

For more information or to engage our services, please contact us at info@majentai.com or visit https://majentai.com