Service Brief

Implementation

majentai

Cisco Identity Services Engine (ISE) Implementation

Cisco Identity Services Engine (ISE) Implementation is a greenfield engagement designed to deploy Cisco ISE as the customer's primary policy and access control platform for wired, wireless, remote access, guest workflows, and segmentation readiness. Majentai aligns stakeholders, integrates, validates, and transitions the platform into day-2 operations.

Overview

The ISE Implementation is a focused greenfield engagement designed to establish a scalable identity and access control foundation with controlled rollout risk and a clear path to broader Zero Trust adoption. The engagement deploys, integrates core identity and network systems, and validates policy enforcement while establishing the operational model for expand access control and segmentation with confidence.

- Wired and wireless NAC foundation
- Centralized AAA and policy control
- Identity, profiling, and posture visibility
- Guest and contractor access workflows
- Segmentation readiness and operational handoff

Business Outcomes

The ISE Implementation reduces access control risk by aligning policy design, platform integration, and phased enforcement before broader rollout begins. It gives stakeholders stronger visibility, cleaner governance, and a practical foundation to expand segmentation, posture, and Zero Trust controls across the environment.

- Reduce rollout risk with phased enforcement
- Improve visibility into users and devices
- Strengthen governance for access changes
- Create foundation for future segmentation

At a Glance

Objectives

- Deploy Cisco ISE aligned to topology and security goals
- Validate access policies with manageable rollout risk
- Prepare operations teams for sustained day-2 ownership

Scope

- Greenfield ISE implementation for customer-defined pilot and production phases
- Integrations with identity stores, NADs, and logging platforms
- Wired, wireless, guest, contractor, and device access use cases

Deliverables

- ISE strategy, design, and pilot plan
- Platform build, policy, and validation artifacts
- Operations runbook and knowledge transfer materials

Engagement Phases

Phase 1: Strategy and Discovery

Majentai aligns stakeholders, defines access control and segmentation use cases, inventories the current network, identity, and endpoint landscape, and documents constraints, risk boundaries, and success criteria for a safe Cisco ISE rollout.

Phase 2: Solution Design and Planning

Majentai defines the target ISE architecture, integrations, certificate strategy, policy model, and pilot onboarding plan, producing the design and rollout approach needed to implement Cisco ISE with clarity and operational control.

Phase 3: Build, Implement and Validate

Majentai deploys and configures ISE, integrates identity stores and pilot NADs, implements baseline authentication and authorization policies, and validates access outcomes, logging, fail-safe behavior, and controlled enforcement across pilot scope.

Phase 4: Operations & Recommendations

Document operating procedures, deliver knowledge transfer, and provide recommendations to expand Cisco ISE across additional sites, devices, and segmentation use cases.

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