Service Brief

Migration

majentai

Cisco Identity Services Engine (ISE) Migration

Cisco Identity Services Engine (ISE) Migration is designed to transition legacy NAC, AAA, or fragmented access control environments into Cisco ISE with controlled risk and operational readiness. Majentai guides discovery, policy translation, coexistence planning, phased cutover, validation, and handoff so teams can modernize access control with less disruption.

Overview

This Cisco Identity Services Engine (ISE) Migration is a structured engagement designed to move a legacy access control environment into Cisco ISE with low risk and a path to production adoption. The ISE Migration aligns authentication, profiling, and policy workflows, maps legacy controls into the target architecture, and establishes the validation and cutover model needed to scale confidently.

- Legacy-to-ISE migration strategy
- Identity and policy translation
- Profiling and access workflow migration
- Coexistence and phased cutover
- Operations handoff and governance

Business Outcomes

This engagement reduces risk by moving legacy access controls into Cisco ISE through phased validation, coexistence planning, and controlled rollout. It gives stakeholders clearer operational visibility, stronger confidence in policy outcomes, and a practical foundation for broader Zero Trust and segmentation initiatives.

- Reduce user and device migration risk
- Improve confidence in target-state controls
- Strengthen ownership after phased cutover
- Create a scalable identity control foundation

At a Glance

Objectives

- Translate current access controls into an ISE-aligned target state
- Migrate authentication and policy workflows with controlled risk
- Deliver a phased path to production readiness

Scope

- Migration from legacy NAC, AAA, or fragmented policy environments
- Identity, network device, profiling, and policy workstreams within agreed scope
- Pilot, coexistence, cutover, and operational transition support

Deliverables

- Migration design and rollout plan
- Policy mapping and validation evidence
- Runbook, closeout, and roadmap package

Engagement Phases

Phase 1: Strategy and Discovery

Stakeholders align on migration scope while the current environment is assessed across legacy authentication methods, identity sources, access workflows, policy constructs, PKI dependencies, and constraints to define risks and cutover needs.

Phase 2: Solution Design and Planning

The target ISE architecture, policy mapping approach, identity and profiling model, onboarding sequence, validation criteria, and phased migration plan are defined to move users, devices, and workflows into Cisco ISE safely.

Phase 3: Build, Implement and Validate

Majentai configures the ISE baseline, supports identity and policy setup, enables migration workstreams across access and profiling use cases, executes pilot and cutover waves, captures evidence, and tunes exceptions for readiness.

Phase 4: Operations & Recommendations

Majentai delivers runbooks, knowledge transfer, governance guidance, legacy decommission recommendations, and next-step priorities so customer teams can assume ownership and continue hardening and expanding Cisco ISE after migration.

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

© 2026 Majentai Inc. All rights reserved. Unauthorized duplication or distribution is prohibited.