Service Brief

Proof of Value

majentai

Cisco Identity Services Engine (ISE) PoV

This Cisco Identity Services Engine (ISE) PoV is a focused engagement designed to validate secure network access controls in your environment before a broader rollout. Majentai deploys a limited pilot, integrates core infrastructure, tests real use cases, and delivers the evidence, findings, and recommendations needed for a confident go or no-go decision.

Overview

This Cisco Identity Services Engine (ISE) PoV is a focused engagement designed to prove value quickly with controlled scope and limited production risk, with a clear path to broader rollout after pilot validation. The PoV validates identity-based access control, endpoint visibility, policy behavior, and core infrastructure integrations while establishing the operational foundation required to expand ISE with confidence.

- Identity-based access control validation
- Wired and wireless authentication testing
- Role-based policy enforcement
- Endpoint profiling and visibility
- Pilot evidence and next-step guidance

Business Outcomes

The ISE PoV reduces deployment risk by proving policy behavior, infrastructure integration, and operational impact in a controlled pilot before wider rollout begins. It gives stakeholders stronger evidence, clearer visibility into gaps, and a more confident path toward production deployment and future expansion.

- Reduce risk before full deployment
- Improve visibility across users and devices
- Validate access controls with real evidence
- Prepare teams for broader rollout decisions

At a Glance

Objectives

- Validate Cisco ISE outcomes in the customer environment
- Confirm authentication, policy, and visibility capabilities work as designed
- Deliver a clear recommendation for broader rollout

Scope

- Limited pilot across selected switches, WLCs, and identity stores
- Validation of 802.1X, MAB, profiling, and role-based access
- Optional guest access and SIEM integration where applicable

Deliverables

- PoV scope and objectives summary
- Use case and test plan
- Results, findings, and recommendations pack

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders on business goals, technical priorities, pilot scope, success criteria, sites, VLANs, SSIDs, user groups, devices, and early risks so the PoV starts with clear constraints and a shared definition of success.

Phase 2: Solution Design and Planning

Define the PoV use cases, expected authentication behavior, access outcomes, infrastructure integrations, and test approach, then finalize participant roles, timeline, and the evidence that will be captured during validation.

Phase 3: Build, Implement and Validate

Configure Cisco ISE in the agreed pilot environment, integrate in-scope switches, wireless controllers, identity stores, and logging platforms, then execute testing to validate authentication flows, policy behavior, endpoint visibility, and user experience.

Phase 4: Operations & Recommendations

Consolidate results, document what worked, identify issues or limitations, map findings to business impact, and deliver a go or no-go recommendation with prerequisites, improvement areas, and a high-level roadmap for next phases.

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