

# Cisco Identity Services Engine (ISE) Assessment

The Cisco Identity Services Engine (ISE) Assessment is a structured engagement designed to evaluate current-state access control, identity, and network readiness before deployment or expansion. Majentai identifies technical gaps, operational risks, and integration dependencies, delivering a prioritized roadmap for phased adoption with lower risk and clearer stakeholder alignment.

## Overview

The ISE Assessment is a focused readiness engagement designed to clarify whether the environment, teams, and dependencies are prepared for a successful ISE rollout or expansion, with a clear path to phased implementation. The assessment validates network access controls, identity infrastructure, capabilities, and readiness while establishing the foundation required to move into pilot, design, and deployment.

- Network access and identity review
- ISE prerequisite and dependency analysis
- Integration and policy readiness validation
- Risk, gap, and constraint identification
- Phased deployment roadmap development

## Business Outcomes

This engagement reduces deployment risk and accelerates planning by identifying technical, operational, and governance gaps before implementation begins. It gives stakeholders clearer visibility into prerequisites, sequencing, and quick wins so broader rollout decisions can be made with stronger confidence.

- Reduce risk before enforcement begins
- Improve readiness across teams and platforms
- Clarify dependencies and remediation priorities
- Create a lower-risk path to deployment

## Engagement Phases

### Phase 1: Strategy and Discovery

Align stakeholders on business drivers, scope, success criteria, and target outcomes, then review current-state network access, identity, security, guest access, and compliance requirements that will shape the readiness assessment.

### Phase 2: Solution Design and Planning

Define the target ISE role, conceptual architecture, priority use cases, and technical prerequisites, then establish the readiness framework, scoring model, and interview plan needed for structured gap analysis.

### Phase 3: Build, Implement and Validate

Execute technical deep dives across switching, wireless, VPN, identity, PKI, and security operations, validate readiness against the agreed framework, and document per-domain findings, risks, and deployment constraints.

### Phase 4: Operations & Recommendations

Translate findings into a phased roadmap with remediation priorities, quick wins, operational readiness recommendations, and clear next steps that guide pilot planning, deployment sequencing, and future optimization.

## At a Glance

### Objectives

- Assess readiness for Cisco ISE deployment or expansion
- Identify risks, gaps, and technical dependencies early
- Deliver a practical roadmap for phased adoption

### Scope

- Workshops and assessment sessions across network, identity, and security teams
- Review of switching, wireless, VPN, identity, and security integrations
- No production deployment, policy enforcement, or cutover changes performed

### Deliverables

- Readiness scorecard and findings summary
- Gap analysis and risk register
- Phased roadmap and recommendations

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](mailto:info@majentai.com) or visit <https://majentai.com>