Service Brief

Workshop

majentai

Cisco Secure Access (CSA) Workshop

This Cisco Secure Access (CSA) Workshop is a structured engagement designed to align business and technical stakeholders, validate current-state readiness, and define a phased deployment path for Secure Internet Access (SIA) and Secure Private Access (SPA). Majentai clarifies architecture, integrations, and governance needed to move to controlled enforcement.

Overview

This CSA Workshop is a focused planning engagement designed to define a low-risk path to deployment with clear stakeholder alignment and practical next steps. The workshop validates current-state realities, target architecture decisions, and rollout assumptions while establishing the design, governance, and operating model required to move toward implementation with more confidence.

- Stakeholder alignment and decision rights
- SIA, SPA and RAVPN use case planning
- Current-state readiness assessment
- Deployment roadmap and rollout controls
- Operating model and governance design

Business Outcomes

The CSA Workshop reduces early deployment risk by aligning stakeholders, validating dependencies, and defining a practical implementation path before rollout begins. It gives teams a clearer foundation for phased rollout decisions, governance, and controlled enforcement at scale.

- Reduce implementation risk before enforcement starts
- Improve readiness across teams and platforms
- Clarify ownership, approvals, and exception handling
- Create a controlled path to scale

At a Glance

Objectives

- Establish a standardized greenfield approach for CSA adoption
- Align business, IT, and security requirements and constraints
- Define a phased, low-risk deployment roadmap for CSA

Scope

- Workshop for SIA, SPA, RAVPN or combined use cases
- Current-state review across identity, endpoints, and network readiness
- Planning engagement only with no production changes performed

Deliverables

- Strategy and use case matrix
- High-level design and implementation plan
- Operating model and governance workflow

Engagement Phases

Phase 1: Strategy and Discovery

Align stakeholders, confirm scope and success criteria, and assess current-state identity, endpoint, and network readiness for SIA, SPA, and RAVPN adoption, including governance expectations for monitoring, staged enforcement, and rollback.

Phase 2: Solution Design and Planning

Define the target CSA architecture, integration approach, policy baseline, connector strategy, and rollout plan needed to deploy Secure Access safely across the agreed pilot scope.

Phase 3: Build, Implement and Validate

Produce an execution-ready blueprint covering Secure Client rollout, SIA steering, SPA/PSA connector readiness, validation gates, and pilot controls so implementation teams can confirm feasibility before delivery begins.

Phase 4: Operations & Recommendations

Define the operating model, policy governance workflow, escalation paths, and knowledge transfer outputs required to support post-implementation adoption and a controlled path toward broader enforcement.

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