Service Brief

Implementation

majentai

Cisco Secure Access (CSA) Implementation

This Cisco Secure Access (CSA) Implementation takes customers from readiness and design through build, pilot validation, phased rollout, and operational handoff. Majentai establishes the tenant baseline, integrates identity and policy controls, enables SIA and/or SPA capabilities, and delivers runbooks and knowledge transfer required to support CSA in production.

Overview

This CSA Implementation is a focused engagement designed to deliver a validated, supportable Secure Service Edge foundation with controlled risk and a clear path to broader enforcement. The CSA implementation establishes core SIA and SPA capabilities, identity and endpoint alignment, and the operational framework required to deploy, administer, and scale Secure Access with confidence.

- Tenant baseline and RBAC setup
- SSO and group mapping alignment
- SIA policy configuration and tuning
- SPA connector and app onboarding
- Runbooks and operational handoff

Business Outcomes

This CSA implementation reduces deployment risk and accelerates time to value by aligning architecture, identity, policy, and rollout controls before broader enforcement. It gives stakeholders stronger operational visibility, validated access outcomes, and a clear foundation for future expansion across users, applications, and locations.

- Reduce risk before broad enforcement
- Improve confidence in access controls
- Strengthen support and operational readiness
- Create a scalable Secure Access foundation

At a Glance

Objectives

- Establish a validated CSA architecture and implementation baseline
- Enable SIA and/or SPA capabilities aligned to confirmed scope
- Deliver a supportable path to enforcement and operations

Scope

- Greenfield CSA deployment for SIA, SPA, or both
- Identity, policy, endpoint, and network readiness alignment
- Pilot rollout, phased enforcement, and operational transition

Deliverables

- High-level design and rollout plan
- As-built configuration and validation results
- Operations runbook and knowledge transfer

Engagement Phases

Phase 1: Strategy and Discovery

Majentai aligns stakeholders, confirms whether the engagement covers SIA, SPA, or both, and assesses identity, endpoint, network, and application readiness so the deployment scope, pilot population, risks, and success criteria are clearly defined.

Phase 2: Solution Design and Planning

Majentai defines the target CSA architecture, RBAC model, SSO and group-mapping approach, policy framework, connector strategy, rollout sequencing, and dependencies needed to support a controlled implementation.

Phase 3: Build, Implement and Validate

Majentai provisions the tenant baseline, configures identity and access controls, enables SIA and/or SPA services, supports pilot execution, validates outcomes, tunes approved policy sets, and guides phased rollout toward production readiness.

Phase 4: Operations & Recommendations

Majentai delivers the runbooks, knowledge transfer, governance guidance, and closeout recommendations required to transition ownership to customer operations and support the next stage of CSA maturity.

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