Service Brief

Implementation

majentai

Cisco SD-Access Implementation

Cisco SD-Access Implementation is a structured engagement designed to transition networks from manual VLAN operations to an automated, identity-based fabric. Majentai guides teams through readiness, design, implementation, and Day 2 handoff using Cisco Catalyst Center (DNA Center) and Cisco ISE to deliver consistent segmentation and a scalable Zero Trust model.

Overview

This Cisco SD-Access Implementation is a guided deployment engagement designed to deliver an automated campus fabric with governance and operational readiness, with a clear path to expand across additional sites. It aligns networking and security teams around intent-based policy, validating a repeatable migration approach that reduces complexity and improves control.

- SDA readiness and lighthouse site strategy
- Fabric underlay/overlay and transit blueprint
- Virtual Networks and SGT-based policy model
- Catalyst Center provisioning and automation
- ISE integration and Day 2 handoff

Business Outcomes

This engagement reduces operational and security risk by replacing manual VLAN and ACL workflows with identity-based automation and a repeatable fabric operating model. Majentai delivers centralized policy, improved visibility, and a practical Day 2 foundation that accelerates expansion while improving troubleshooting and control.

- Consistent segmentation across wired and wireless
- Faster changes through intent-based policy
- Improved visibility via assurance telemetry
- Reduced troubleshooting time and complexity

At a Glance

Objectives

- Establish an SDA architecture aligned to business outcomes
- Define identity-based segmentation using VNs and SGTs
- Deploy and migrate users with minimal disruption

Scope

- Pilot lighthouse site selection and migration methodology
- Catalyst Center + ISE integration for identity-to-fabric exchange
- Wired and wireless onboarding using Dot1x/MAB and policy

Deliverables

- SDA fabric blueprint and design package
- Group-based policy matrix (SGTs/SGACLs)
- Integration guide and operational runbooks

Engagement Phases

Phase 1: Strategy and Discovery

Assess infrastructure and licensing readiness, define the identity strategy between Active Directory and Cisco ISE, and select a lighthouse site to confirm scope, success criteria, and a repeatable migration approach.

Phase 2: Solution Design and Planning

Design the fabric architecture and high availability model, define Virtual Networks for macro-segmentation, and build the group-based policy matrix using SGTs and SGACLs to establish intent-based access rules.

Phase 3: Build, Implement and Validate

Configure Catalyst Center hierarchy and automation, orchestrate pxGrid integration with ISE for identity propagation, and onboard hosts using Dot1x/MAB while transitioning ports and users into the SDA fabric with minimal disruption.

Phase 4: Operations & Recommendations

Enable assurance dashboards and health telemetry, refine policies using endpoint analytics for unknown devices, complete operational handoff with runbooks and knowledge transfer, and provide a prioritized roadmap for fabric expansion.

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