SERVICE OVERVIEW

Perform SD-Access installation and configuration for the following components:

- Identify Services Engine (ISE) (if not using customer instance): a) Configure ISE bootstrapping; b) Configure system administrators and accounts; c) Configure certificates; d) Configure ISE deployment; e) Configure network resources; f) Configure users and identity stores; g) Authentication configuration; h) Authorization configuration; I) Guest configuration; j) integrate with up to one (1) Active Directory domain.
- Identify Services Engine (ISE) (if using Customer instance): a) Review and verify ISE minimum requirements b) provide notification of identified deficiencies.
- Cisco DNA Center: a) Set up and install the latest version of Cisco DNA-Center on Customer's Cisco DNA Center appliance; b) Integrate Cisco DNA Center with ISE instance being leveraged for this infrastructure; c) Discover and inventory the infrastructure as defined in Section 3.3.
- SD-Access Fabric Provisioning (Underlay): a) Manual Setup, including: i) Cisco DNA Center Discovery, Inventory & Topology App, ii) If not using automated underlay, create and deploy manual underlay templates; b) Automated Setup – Cisco DNA Center Design App – Switching Profile.
- SD-Access Fabric Provisioning (Overlay): a) Assign devices to site; b) Create Fabric domain(s); c) Add devices to a Fabric domain – i) Set up Control Plane, ii) Set up Border Nodes (internal and/or external).
- SD-Access Address Pools and Host Onboarding: a) Assign IP pools (wired and wireless); b) Dynamic device authentication – i) 802.1X, MAB; c) Static device pool assignment.
- SD-Access Policy Administration: a) Create Virtual Network(s); b) Group creation and/or import from ISE; c) Group policy definition.
- SD-Access Fabric Enabled Wireless (FEW): a) IP Pool assignment for APs and clients; b) Add wireless controller to Fabric; c) Configure campus Fabric for wireless integration; d) Configure up to two (2) wireless SSIDs for

Migration Support:

- Validate user profiles for those users/devices to be migrated
- Validate current user/device configurations.
- Plan user/device migration from existing to SD-Access infrastructure.
- Execute physical and software configuration changes to infrastructure and policies to enable migration from existing environment to the SD-Access fabric.
- Configure WAN access on the SD-Access Border/Control Node to enable migration from existing environment to the SDA fabric.
- Configure up to twenty (20) access policies using Cisco DNA Center for SD-Access Policy Administration.
- Test connectivity and access of user profiles.
- Assist in troubleshooting of migrated user connectivity and access.

WHAT YOU GET

- Up to 5-days of support (on-site or remote)
- Whiteboard design session with DNAC/SDA Expert including knowledge transfer throughout the project on topics related to the proposed network design, configuration, and management concerns.
- Day 2 operations training