

CISCO ISE MENTORED INSTALL

Service Overview:

At Netnology, we specialize in Cisco Identity Services Engine (ISE) implementation services as part of the Cisco TrustSec security solution to help enable your compliance needs, enhance security and streamline operations. As part of the Mentored Install service offer, our subject matter experts (SME) partner with your team to ensure a smooth deployment of the ISE solution and provide knowledge transfer to equip your staff with the necessary skills to configure and manage the ISE environment.

Cisco ISE Solution:

Cisco ISE is designed to help organizations to gain enterprise wide visibility into their network; allowing authentication, authorization, accounting, posture profiling gathering real-time contextual information from network, users, and devices; and making proactive governance decisions by enforcing policy across the network infrastructure. Cisco ISE performs the following functions:

- Provides context-aware identity-based network access
- Manages various deployment scenarios across enterprise infrastructure, supporting 802.1X wired, wireless, and virtual private networks (VPN)
- Provides basic authentication and authorization
- Enforces endpoint compliance by providing comprehensive client provisioning measures and accessing device posture for all endpoints that access the network, including 802.1X environments
- Provides comprehensive guest access management
- Provides support for discovery, profiling, policy-based placement and monitoring of endpoint devices on the network
- Enables consistent policy in centralized and distributed deployments that allow services to be delivered where they are needed
- Employs advanced enforcement capabilities including security group access (SGA) through the use of security group tags (SGTs) and security group access control lists (SGACLs)

Service Benefits:

Netnology has a team of world class engineers who specialize in Cisco ISE solution and are passionate about customer success. Netnology will partner with you to provide:

- Step-by-step guidance from an SME on solution deployment
- Configuration and documentation of Cisco ISE solution
- Knowledge transfer to ensure customer is ready to configure and manage the lab environment

Scope of Services:

As part of the 10-day (up to 80 hours) engagement, Netnology will help with the following:

- ISE Architecture Design
 - Review existing network, identity infrastructure, and security policies
 - Design Cisco ISE deployment architecture
 - Define node roles (PAN, PSN, MnT)
 - Define high-availability and redundancy model
 - Define integration points with network infrastructure and identity sources

- ISE Node Installation and Setup
 - Install Cisco ISE nodes
 - Configure node roles and deployment setup
 - Apply and configure Cisco ISE licensing
 - Verify deployment health and node communication

- ISE Upgrade (if required)
 - Review current ISE version and upgrade path
 - Validate compatibility with network devices and integrations
 - Perform Cisco ISE upgrade to the recommended version
 - Validate services post-upgrade

- MAB (MAC Authentication Bypass) Implementation
 - Configure MAB authentication for non-802.1X devices
 - Create policies for IoT, printers, cameras, and legacy devices
 - Configure profiling policies for device identification
 - Validate access behavior for MAB devices

- Wired 802.1X Rollout
 - Configure wired network authentication using 802.1X
 - Configure switch AAA and RADIUS integration with ISE
 - Implement authentication policies for wired users
 - Configure fallback mechanisms such as MAB where required

- Wireless 802.1X Rollout
 - Integrate Wireless LAN Controllers with Cisco ISE
 - Configure secure wireless authentication using 802.1X
 - Configure SSID authentication policies
 - Validate user authentication workflows

- ISE Posture / Profiling / Device Visibility
 - Configure endpoint profiling policies
 - Enable device discovery and classification
 - Configure posture policies for endpoint compliance
 - Provide visibility into user and device identity

- ISE Guest Services Configuration
 - Configure Cisco ISE Guest Portal
 - Configure guest authentication workflows
 - Define guest access policies and session duration
 - Validate guest access functionality

- TrustSec Enforcement
 - Setting-up optional enforcement for North South Micro segmentation use cases i.e. User accessing resources in Data Center.
 - Enabling micro-segmentation on supported Cisco network access devices

- Network Infrastructure Integration
 - Integrate Cisco switches with Cisco ISE
 - Integrate Wireless LAN Controllers with Cisco ISE
 - Configure RADIUS and AAA settings
 - Integrate Microsoft Active Directory with Cisco ISE

- Meraki Integration (if applicable)
 - Integrate Cisco Meraki wireless networks with Cisco ISE
 - Configure RADIUS authentication for Meraki SSIDs
 - Enable identity-based access control for Meraki users
 - Configure Meraki group policies mapped to ISE authorization results

- Testing and Validation
 - Validate wired authentication workflows
 - Validate wireless authentication workflows
 - Validate guest access services
 - Perform end-to-end access control testing

- Knowledge Transfer

Target Audience:

This service is designed for Security Architects, Network Security Engineers, Network Architects, Network Engineers and Administrators, configuring, deploying and managing the ISE environment.

Pre-requisites:

Customer needs to ensure that Virtual Machines are provisioned for ISE based on the specifications provided prior to the kick-off. Also, customer needs to ensure they have identified the necessary switches and Wireless LAN Controller going to be used in the Mentored Install. Customer needs to acquire the necessary software licenses and download the latest version of Cisco ISE ISO from Cisco site.

Service Deliverables:

No	Deliverable	Service Details
1.	Project Kickoff	<ul style="list-style-type: none"> Project Overview Solution Overview
2.	ISE Architecture Design	<ul style="list-style-type: none"> Work with customer to design suitable Cisco ISE architecture Define node roles (PAN, PSN, MnT) Define redundancy and high availability
3.	ISE Node Setup	<ul style="list-style-type: none"> Install and configure Cisco ISE nodes Configure node roles and deployment Apply and configure ISE licensing
4.	ISE Upgrade	<ul style="list-style-type: none"> Review current ISE version and upgrade path Perform upgrade to recommended Cisco ISE version Validate services after upgrade
5.	MAB (MAC Authentication Bypass)	<ul style="list-style-type: none"> Configure MAB authentication for non-802.1X devices Create policies for printers, IoT devices, and legacy systems Validate MAB device access behavior
6.	Wired 802.1X Rollout	<ul style="list-style-type: none"> Configure wired authentication using 802.1X Configure switch AAA and RADIUS integration Implement authentication and authorization policies
7.	Wireless 802.1X Rollout	<ul style="list-style-type: none"> Integrate Wireless LAN Controller with Cisco ISE Configure secure wireless authentication using 802.1X Validate wireless authentication workflows
8.	ISE Posture / Profiling / Device Visibility	<ul style="list-style-type: none"> Configure endpoint profiling policies Enable device discovery and classification Configure posture policies for endpoint compliance
9.	Integrate and Configure	<ul style="list-style-type: none"> Integrate switches with Cisco ISE Integrate Wireless LAN Controllers with Cisco ISE Configure network devices for ISE authentication Integrate Microsoft Active Directory
10.	ISE Guest Services ⁽¹⁾	<ul style="list-style-type: none"> Setup Cisco ISE Guest portal for Wireless Guest Users. Setup ISE Sponsor portal for creating and managing Guest Accounts
11.	TrustSec Enforcement ⁽¹⁾	<ul style="list-style-type: none"> Setting-up optional enforcement for North South Micro segmentation use cases i.e. User accessing resources in Data Center. Enabling micro-segmentation on supported Cisco network access devices This will ONLY include devices which are capable of in-line SGT enforcement. This will not include SXP (security exchange protocols), pxGrid and 3rd party NAD's will be out of scope for this engagement https://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/trustsec/trustsec_platform_support.pdf
12.	Meraki Integration	<ul style="list-style-type: none"> Integrate Cisco Meraki wireless network with Cisco ISE Configure RADIUS authentication for Meraki SSIDs Map Meraki group policies with ISE authorization policies
13.	Test Customer Endpoints/users	<ul style="list-style-type: none"> Test customer's computers Test IP phones Test printers Test other IoT devices on customer's network

		<ul style="list-style-type: none"> • Test various access for users
14.	Knowledge Transfer	<ul style="list-style-type: none"> • Explain to the customer how to configure and manage the solution in the lab environment • A walkthrough of the customer's environment

- (1) **Note: Additional Services is an add-on service, not included in the ISE Mentored Install scope. Additional charges will apply for deploying Advanced Services in addition to ISE Mentored Install engagement.**
- (2) **Note: Integration with any supported security solution (McAfee, Qualys, etc.) is not included in the ISE Mentored Install scope. Additional Charges will apply for integration in addition to ISE Mentored Install engagement.**