Cisco Identity Service Engine (ISE) Mentored Implementation Service

Delivery Type: Mentored Installation

Why Skyline?

Skyline Advanced Technology Services (ATS) offers Professional Services for a variety of Cisco-centric solutions. From inception to realization, our senior staff of engineers is available for any size project or duration for the following services:

- Consulting Services
- Installation Services
- Network Design
- Staff Augmentation

For an in-depth discussion regarding your technical and staffing needs, our team is with you every step of the way.

Contact your Skyline-ATS representative today.

Are you deploying a Cisco Identity Service Engine (ISE) solution?

Contact your Skyline Account Manager today for more information on how we can help.

800.375.9546
info@skyline-ats.com

Description

The Cisco Identity Services Engine (ISE) Mentored Install is a unique engineering enablement offering designed to assist Cisco partners/customers in building service offerings around the ISE solution. This offering is designed for partners/customers who are selling, designing, and deploying Cisco ISE solutions and require assistance with and training on design and deployment.

The engagement consists of a design and readiness review followed by engineering support during the mentored install. During the design phase, a Skyline-ATS Security Solutions Architect will work with the partner/customer to complete a High Level Design (HLD), assess the readiness of the network, provide recommendations for IOS upgrades and/or equipment replacement and/or configuration changes to make the network ISE ready. The mentored installation is focused around installation and deployment of an operational ISE system while providing the partner/customer deployment experiences as well as a well-defined knowledge transfer on design, installation, and deployment.

This mentored installation assumes that all relevant use cases will be designed, implemented and tested specific to a limited number of end points and users. The Mentored Install will cover wired and wireless network access control, BYOD, Profiling, Posture Assessment, TACACS+ and VPN. The objective of this Mentored Install is to educate the partner/customer to enable them to complete pushing the solution out to all endpoints/end-users without the need for Skyline-ATS' assistance.

The engagement is expected to take between one and three weeks depending on the services required.

Overall Objectives

1. Collaborate with key personnel to design and determine functionality goals.

2. Interactive training and design sessions geared to educate the partner/customer and finalize the design.

3. Provide interactive training to partner/customer personnel throughout the selling, designing, and deployment process focusing on those areas the partner/customer feels they need assistance with.

Partner/Customer Responsibilities

- Participate in a high level design workshop via WebEx pre-installation.

- Provide proper rack and other supporting infrastructure, such as power, HVAC etc.

- System must be racked and powered prior to Skyline arriving onsite.

- Partner/customer must provide adequate resources to perform the implementation with Skyline providing Interactive training and guidance.

- Partner/customer will assist with all testing scenarios.

Statement of Work (SOW)

After the Skyline-ATS ISE Engineer thoroughly qualifies the partner/customer's SDA requirements, a detailed Statement of Work (SOW) will be submitted for partner/customer approval prior to the implementation engagement.

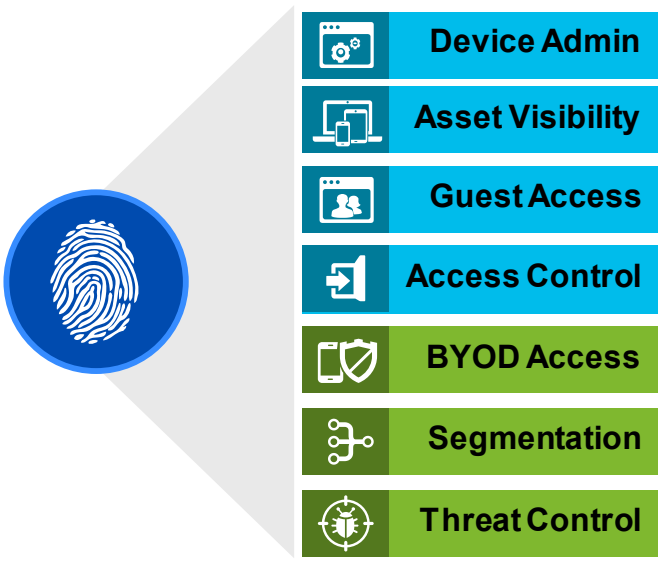
Instructor Led Training (ILT)

Instructor Led Training is also available for those partners/ customers that want to increase their knowledge of Cisco Identity Services Engine technology beyond what is provided in this mentored implementation.

Cisco Identity Services Engine (ISE) Mentored Install Summary

Cisco ISE is a security policy management platform that provides secure access to network resources. Cisco ISE functions as a policy decision point and enables enterprises to ensure compliance, enhance infrastructure security, and streamline service operations. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make governance decisions by tying identity to various network elements, including access switches, wireless LAN controllers (WLCs), Virtual Private Network (VPN) gateways, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

Not all partners/customers will want to deploy all ISE capabilities at once and may opt for more of a phased approach. Because of that, this service is broken out into multiple options. Options may be combined into a single deployment or any number of options may be combined to support the phased approach.



Cisco Identity Services Engine Mentored Install Options

A Mentored Install can include one or more of following options as applicable:

OPTION 1: Cisco Identity Services Engine (ISE) High Level Design (HLD)

Skyline will interview the partner/customer engineers in order to complete a HLD. Design discussions will include but are not limited to:

1. Business objectives
2. Timelines
3. Customer environment
4. Physical network topology details
5. Deployment details
   a. Operations
   b. Unknowns
   c. High Availability (HA)
   d. Migration
   e. ISE node details
   f. Certificate options
6. Build of Materials (BOM)
7. Performance specifications

Wired/Wireless Network Analysis

1. Perform a review of the models and code revisions of network devices involved in current deployment.
2. Review network support capabilities for requested features.

VPN Analysis

1. Perform a review of the models and code revisions of network devices involved in current deployment. Identify models requiring:
   a. a code upgrade.
   b. replacement.
2. Review network support capabilities for requested features.

OPTION 2: Cisco Identity Services Engine (ISE) Base Implementation Services (Wired/Wireless)

Review High Level Design

1. Review the high level design and proposed policies.
2. Discuss with Client and make recommendations for changes if applicable.

ISE Node Implementation

1. Deploy two (2) ISE Appliances (virtual or physical) as all-in-one nodes configured for High Availability (HA) in the client's wired production environment in support of the proof of concept. Each node will be configured as an:
   a. Admin node
   b. Monitor node
   c. Policy Service Node (PSN).
2. Integrate ISE nodes with existing Active Directory.
3. Set up process for ISE management access as follows:
   a. Administration access and policies
   b. Install licenses
   c. Discuss certificate options and install certificates.
4. Create users and end user portals.

Configure Policies

Skyline will consider scenarios such as user versus endpoint authentication (certificate or non-certificate based), role-based identification and segmentation (e.g., employees, contractors, guests,etc.), or endpoint-based differentiation (corporation asset vs. non-corporation asset). These unique security policies will map directly to the final ISE policy sets.

1. Configure policy sets:
   a. Create up to five (5) policy sets that indicate the allowed protocol and/or server sequence (RADIUS or TACACS) as applicable based on design discussions.
2. Configure authentication policies
   a. Create up to five (5) authentication policy use cases to show partner/customer how to create and deploy

authentication policies.
b. 802.1x will be used for any compliant endpoints - configure standard authentication policy to authenticate against corporate AD.
c. Discuss 802.1x authentication policy protocols and configure the appropriate protocols for the use cases (e.g., EAP-Chaining/EAP-FAST).
d. Configure Centralized Web Authentication Guest Access Lifecycle.
e. MAC Authentication Bypass (MAB) will be used for Apple devices and devices that are not 802.1x compliant.
f. Configure authentication policy to authenticate against MAC list - ISE Local.

3. Configure authorization policies:
   a. Create up to five (5) authorization policy use cases to show partner/customer how to create and deploy authorization policies (e.g., corporate assets, corporate users, phones, WAPs, and printers).
   b. Some of the use cases will fall under the MAC list for authorization.
   c. Partner/customer will create and deploy any additional policies.
4. Create two (2) MAC lists in ISE to show partner/customer how to create and populate MAC lists.
   a. Partner/customer will create and deploy any additional MAC lists.

Configure Network Access Devices

1. Configure ISE for network access devices.
2. Deploy Network Access Device (NAD) configuration templates to a sampling of devices (e.g., three (3) to four (4) NADs). After that, partner/customer will deploy to the remaining NADs.

Configure Endpoint Devices

1. Discuss/Advise endpoint device configuration steps and implementation guidelines.
2. Creation and deployment of an 802.1x supplicant; native or Cisco AnyConnect Network Access Manager (NAM) configuration template for multiple endpoint types.
3. Document endpoint device implementation. Demonstrate the deployment of a few endpoints for each use case such as:
   a. Desktop/Laptop (Windows/Apple)
   b. Printers
   c. IP phones
   d. Other endpoints as required.

Test and Remediate

1. Test all use cases deployed and remediate as necessary.

As-Built Documentation Creation and Delivery

1. Skyline will provide as-built documentation to partner/customer prior to the project closeout and acceptance. The as-built documentation will provide partners/customers a record of the baseline configuration settings as applied by the Skyline engineers through the execution of the project.

OPTION 3: Cisco Identity Services Engine (ISE) Profiling

Implementation Services

Using the ISE Profiler to provide dynamic detection and classification of endpoints connected to the network using standard extensive library of profiles and use that classification for authorizing it to connect to the network and granted access based on their profile.

1. Configure Profiling based on default policies for the following:
   a. WAPs
   b. Printers
   c. IP phones
   d. Other devices, up to four (4) additional device types.

Test and Remediate

1. Test all use cases deployed and remediate as

necessary.

As-Built Documentation Creation and Delivery

1. Skyline will provide as-built documentation to partner/customer prior to the project closeout and acceptance. The as-built documentation will provide partner/customer a record of the baseline configuration settings as applied by the Skyline engineers through the execution of the project.

OPTION 4: Cisco Identity Services Engine (ISE) BYOD Implementation Services

Implementation

Creation of Bring Your Own Device (BYOD) policies to allow or restrict access to internet, corporate LANs etc.

1. 1. Configure ISE to support corporate BYOD policies.
   a. Access to intranet.
   b. Limited access to other corporate network services to be defined.
2. Configure BYOD guest access.

Test and Remediate

1. Test all use cases deployed and remediate as necessary.

As-Built Documentation Creation and Delivery

1. Skyline will provide as-built documentation to partner/customer prior to the project closeout and acceptance. The as-built documentation will provide partner/customer a record of the baseline configuration settings as applied by the Skyline engineers through the execution of the project.

OPTION 5: Cisco Identity Services Engine (ISE) Posture Assessment/Remediation Implementation Services

Posture Assessment

Configuring ISE to assess the posture of endpoint devices by analyzing factors such as anti-virus, antispyware, personal FW processes to allow access or quarantine a device and/or process for remediation services.

1. Configure two (2) to three (3) posture policies based on partner/customer requirements (e.g., Anti-Virus validations, MS Windows version assessment, etc.
2. Configure standard posture authorization policies for non-compliant, compliant, quarantined workstations.

Test and Remediate

1. Test all use cases deployed and remediate as necessary.

As-Built Documentation Creation and Delivery

1. Skyline will provide as-built documentation to partner/customer prior to the project closeout and acceptance. The as-built documentation will provide partner/customer a record of the baseline.
2. Configuration settings as applied by the Skyline engineers through the execution of the project.

OPTION 6: Cisco Identity Services Engine (ISE) VPN Authentication/Authorization - RADIUS

Configuration

1. Add/Modify AAA device information in ISE for RADIUS on ASA 5500-x series security appliance.
2. Create VPN policy set.
3. Configure ISE authentication policy - VPN users.
4. Configure ISE authorization polices - VPN users up to two (2) (eg., employees and contractors).
5. Create/Deploy AAA-RADIUS configuration templates for ASA 5500-x security appliance.
6. Configure/Deploy Cisco AnyConnect - up to five (5) endpoints.

Test and Remediate

1. Test all use cases deployed and remediate as necessary.

As-Built Documentation Creation and Delivery

1. Skyline will provide as-built documentation to partner/ customer prior to the project closeout and acceptance. The as-built documentation will provide partner/ customer a record of the baseline configuration settings as applied by the Skyline engineers through the execution of the project.

OPTION 7: Cisco Identity Services Engine (ISE) TACACS

ISE - Device Management - TACACS+Configuring ISE for Device Management using TACACS+

1. Add AAA Device information in ISE for TACACS+ on ASA 5500-x series security appliances and network devices - up to five (5).
2. Configure ISE device management + TACACS+ authentication policy.
3. Configure ISE device management + TACACS+ authorization polices - up to two (2):
   a. (eg., Net_Engineers, NOC_Engineers).
4. Configure ISE Device Management Command Set policies - up to two (2):
   a. (example: Net_Engineer_Command_Set, NOC_ Engineers_Command_Set).
5. Create/Deploy AAA-TACACS+ configuration templates for ASA 5500-x series.
6. Create/Deploy AAA-TACACS+ configuration for corporate network devices - up to five (5).

Test and Remediate

1. Test all use cases deployed and remediate as necessary.

As-Built Documentation Creation and Delivery

1. Skyline will provide as-built documentation to partner/ customer prior to the project closeout and acceptance. The as-built documentation will provide the partner/ customer a record of the baseline configuration settings as applied by the Skyline engineers through the execution of the project.