

The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

# ISE Design, Deploy & Best Practices

## BRKSEC-2091

Pavan Gupta – Technical Marketing Engineer  
BRKSEC-2091



# Cisco Webex App

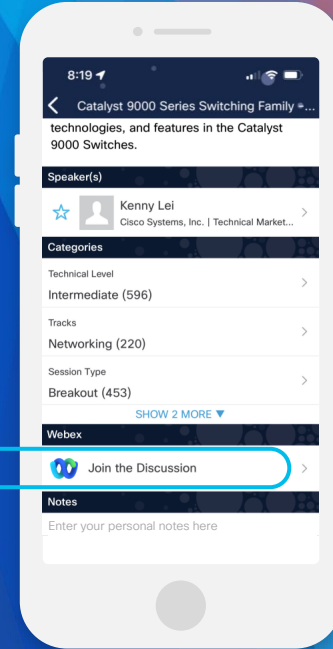
## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this **BRKSEC-2091** in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

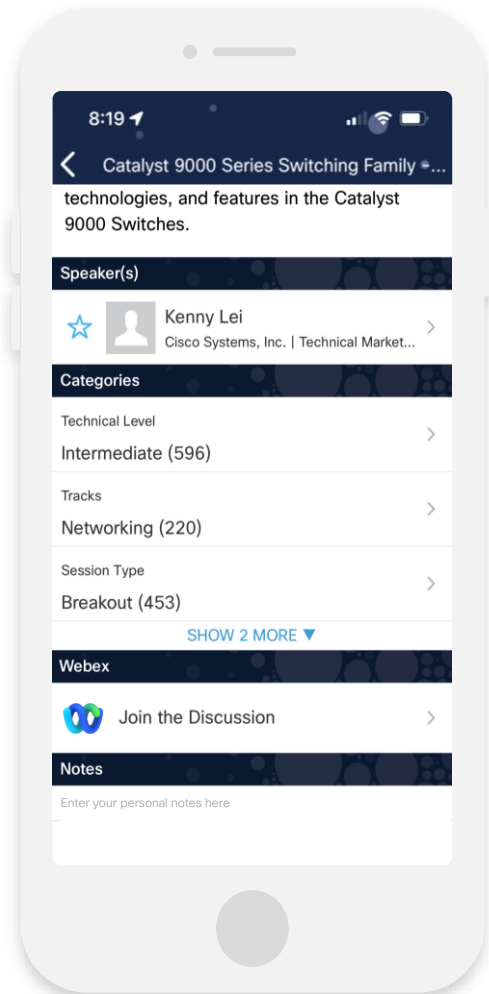
Webex spaces will be moderated by the speaker until June 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2091>

# Cisco Webex Space for Q&A

<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2091>





**Join at  
slido.com**

**#BRKSEC-2091**

# A Word About Myself



Pavan Gupta

- 10+ years of experience in Network & Security
- Different Roles in ISE Team
- Been with ISE team from beginning
- 2+ years in TME Role

## Zero Trust principles

- ▶ Never assume trust
- ▶ Always verify
- ▶ Enforce least privilege

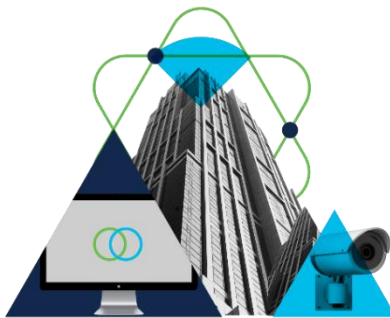
# Cisco Secure Zero Trust

A comprehensive approach to securing all access across your people, applications, and environments.



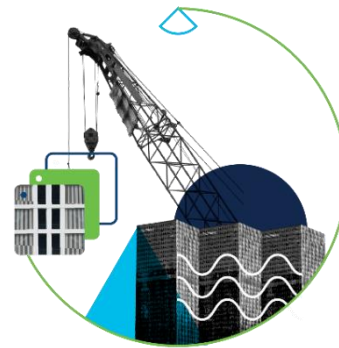
## Workforce

Ensure only the right users and secure devices can access applications.



## Workplace

Secure all user and device connections across your network, including IoT.



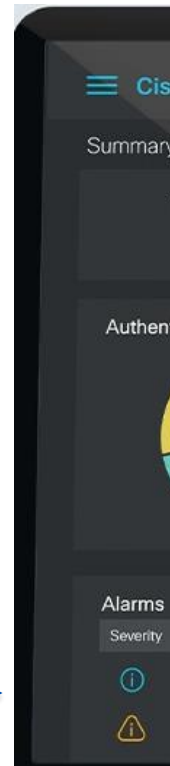
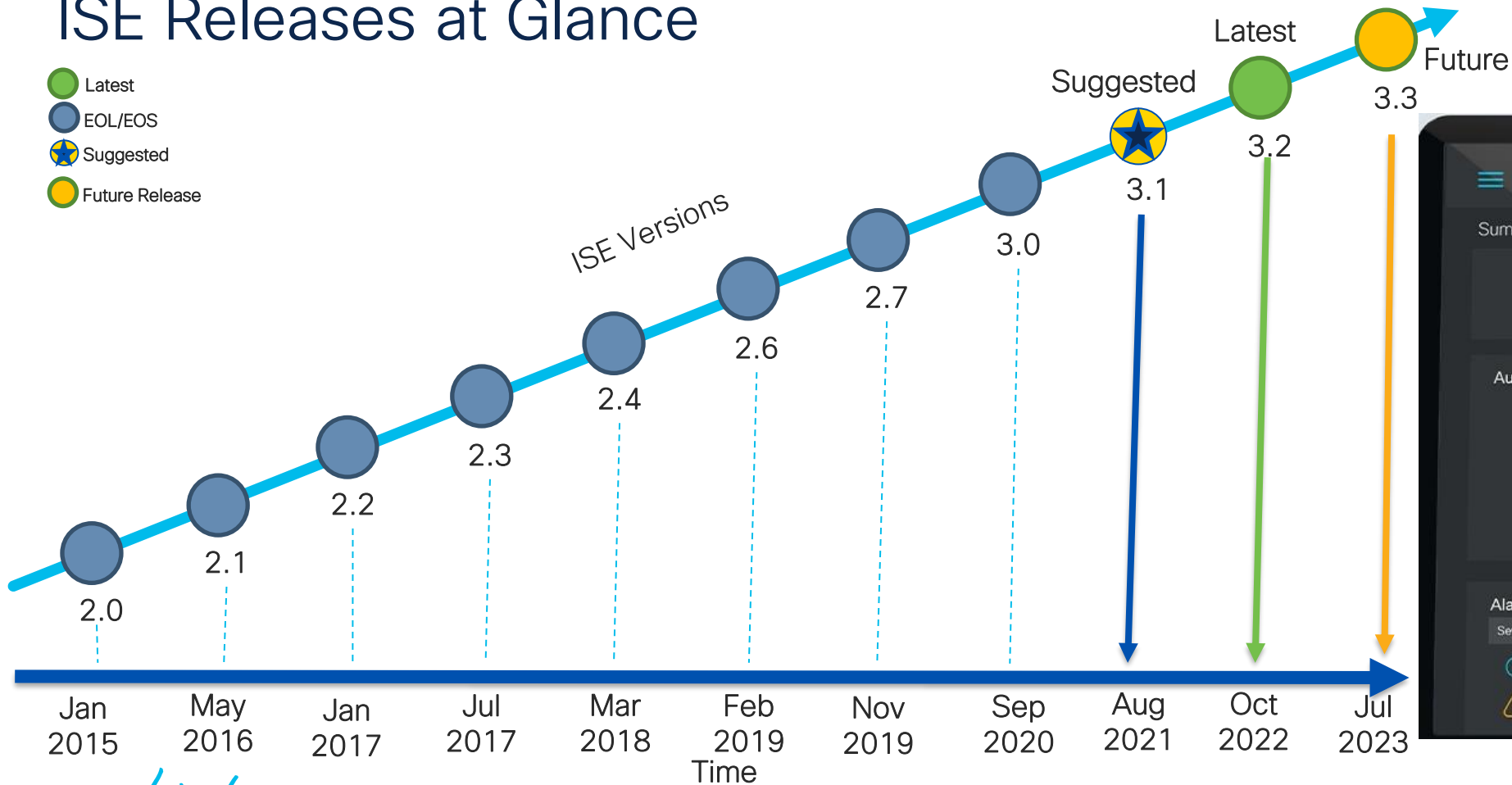
## Workloads

Secure all connections within your apps, across multi-cloud.



# ISE Releases at Glance

- Latest
- EOL/EOS
- Suggested
- Future Release



# Why ISE?



## Enhanced UX



ISE 3.X UI navigation and UX was revamped. The Navigation is aligned with other cisco products to give same kind of experience across all cisco products.

## Device Administration



**TACACS+** Migrating from Cisco Secure ACS or building a new Device Administration Policy Server, this allows for secure, identity-based access to the network devices

## Secure Access



Allow wired, wireless, or VPN access to network resources based upon the identity of the user and/or endpoint. Use **RADIUS** with **802.1X**, **MAB**, **Easy Connect**, or **Passive ID**

## Guest Access



Differentiate between **Corporate** and **Guest** users and devices. Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options

## Asset Visibility



Use the probes in ISE and Cisco network devices to classify endpoints and authorize them appropriately with **Device Profiling**. Automate access for many different IoT devices

## Compliance & Posture



Use **agentless posture**, **AnyConnect**, **MDM**, or **EMM** to check endpoints to verify compliance with policies (Patches, AV, AM, USB, etc.) before allowing network access

## Context Exchange



**pxGrid** is an ecosystem that allows any application or vendor to integrate with ISE for endpoint identity and context to increase **Network Visibility** and facilitate automated Enforcement.

## Segmentation



**Group-based Policy** allows for segmentation of the network through the use of Scalable Group Tags (SGT) and Scalable Group ACLs (SGACL) instead of VLAN/ACL segmentation.

## Cisco SDA/DNAC



ISE integrates with **DNA Center** to automate the network fabric and enforces the policies throughout the entire network infrastructure using Software-Defined Access (SDA)

## BYOD



Allow **employees** to use **their own devices** to access network resources by registering their device and downloading certificates for authentication through a simple **onboarding** process

## Threat Containment



Using a **Threat Analysis tool**, such as Cisco Cognitive **Threat Analytics**, to grade an endpoints threat score and allow network access based upon the results

## Enhanced Reporting



Finally, ISE **provides enhanced reporting** capabilities inhouse for better operations and reporting purposes. Cisco ISE provides you log analytics and infrastructure monitoring and connecting to operational DB and create your dashboards

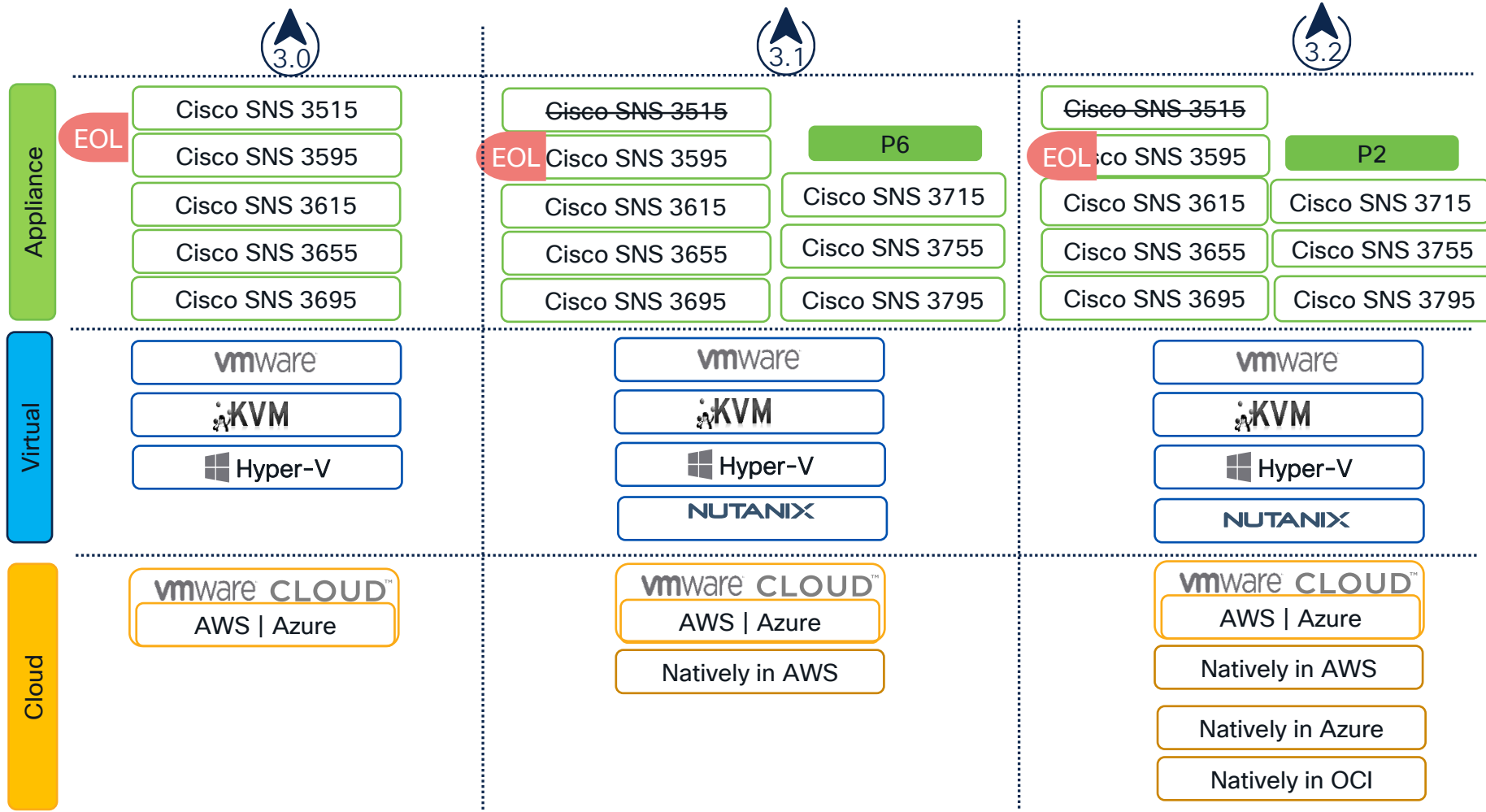
Deploying any Network Access Control requires proper Design, Planning and phased approach.

# Cisco ISE Deployment

# *ISE Deployment*

## Supported Platforms

# ISE 3.X Platforms - At Glance



# Free, 90-day ISE Evaluation License

☰ Cisco ISE

Administration • System

Evaluation Mode 89 Days

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreAdmin AccessSettings

UDI Details

Product Identifier (PID)ISE-VM-K9

Version Identifier (VID)V01

Serial Number (SN)6IM0FCCEC

License Type

Choose Registration Details to acquire pre-purchased license entitlements. Choose Permanent License Reservation to enable all Cisco ISE licenses. Enter the required details to enable Cisco ISE licenses. When you click Register, you agree to the terms and conditions detailed in [Smart Licensing Resources](#).

☒ Smart Licensing Registration

☐ Permanent License Reservation

☐ Specific License Reservation

[Registration Details](#)

Licenses

Select relevant licenses and click Enable to acquire the pre-purchased license's entitlements. Select relevant licenses and click Disable to release unused entitlements. Click Refresh to reauthorize the enabled licenses.

☒ Enable

☒ Disable

☒ Refresh

	License	Status	Compliance	Consumption	Days Out of Compliance	Last Authorization
▼ T						
<input type="checkbox"/>	Essential	Enabled	Evaluation	0	-	-
<input type="checkbox"/>	Advantage	Enabled	Evaluation	0	-	-
<input type="checkbox"/>	Premier	Enabled	Evaluation	0	-	-
<input type="checkbox"/>	Device Admin	Enabled	Evaluation	1	-	-

100 x

1 x

Premier

Advantage

Essentials

Device Admin Appliance License

TACACS+

#CiscoLive

BRKSEC-2091

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

15



# Which ISE Version are you using?

Join at [slido.com](https://slido.com)

#BRKSEC-2091



# *ISE Deployment*

Personas

# ISE Personas

Max 2

## Policy Administration Node (PAN)

- Administrative GUI
- Policy configuration
- Policy replication
- Deployment Management
- Configuration REST APIs

Max 2

## Monitoring & Troubleshooting Node (MNT)

- Receives logs from all nodes
- Handles remote logging targets
- Generates summary Dashboard Views
- Performs scheduled reports
- Handles reporting and operations



## Policy Service Node (PSN)

- TACACS requests
- RADIUS requests
- Endpoint profiling probes
- Identity store queries
- Hosts Guest/BYOD/CP portals
- MDM/Posture queries
- TC-NAC & SXP services

## Platform Exchange Grid Node (PXG)

- Runs pxGrid controller
- Authorizes pxGrid Pubs/Subs
- Publishes pxGrid topics to subscribers
- Handles ANC/EPS requests
- REST APIs

Max 50

Max 4

# *ISE Deployment*

Models

# ISE Deployment Scale

No. of Endpoints Support - Deployment Wise

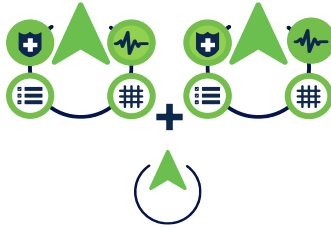
 [cs.co/ise-scale](https://cs.co/ise-scale)

Lab and  
Evaluation



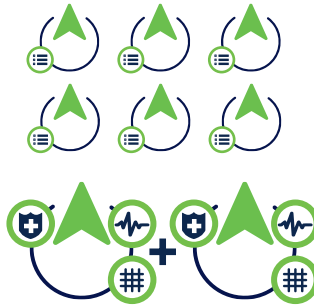
1 x (PAN + MNT + PSN + PXG)

Small



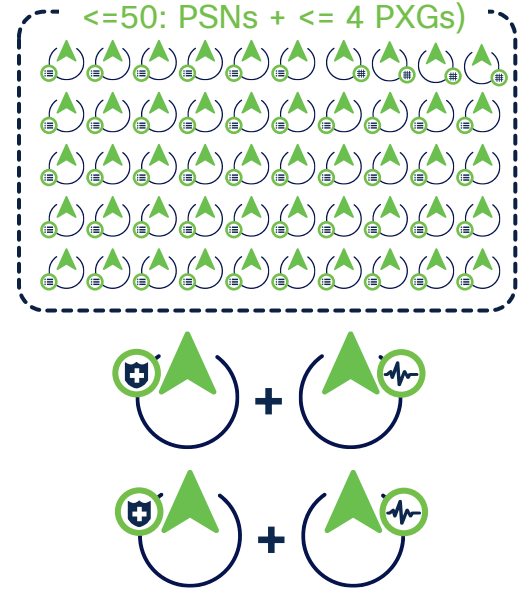
2 x (PAN+MNT+PSN)

Medium



2 x (PAN+MNT+PXG), <= 6 PSN

Large



2 PAN, 2 MNT, <=50: PSNs + <= 4 PXGs

# *ISE Deployment*

Standalone

# ISE Deployment – Standalone



(Demos & Testing!)

# *ISE Deployment*

Small

# ISE Deployment - Small



2 x (PAN+MNT+PSN+PXG) + 1 x PSN/PXG



# ISE Small Deployment Scale

 [cs.co/ise-scale](https://cs.co/ise-scale)



Deployment Scale (PAN/MnT)	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3595	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Small	10,000	25,000	20,000	25,000	50,000	50,000	50,000

# ISE Deployment

## Configuring ISE Small Deployment – Primary Node

Role STANDALONE

Make Primary



General Settings | Profiling Configuration

Hostname: ise-server  
FQDN: ise-server.aws.local  
IP Address: 172.31.2.15  
Node Type: Identity Services Engine (ISE)

Role: STANDALONE [Make Primary](#)

☒ Administration

☒ Monitoring

Role: PRIMARY

Other Monitoring Node:

☐ Dedicated Mnt

☒ Policy Service

☒ Enable Session Services

Include Node in Node Group: None

☒ Enable Profiling Service

☐ Enable Threat Centric NAC Service

☐ > Enable SXP Service

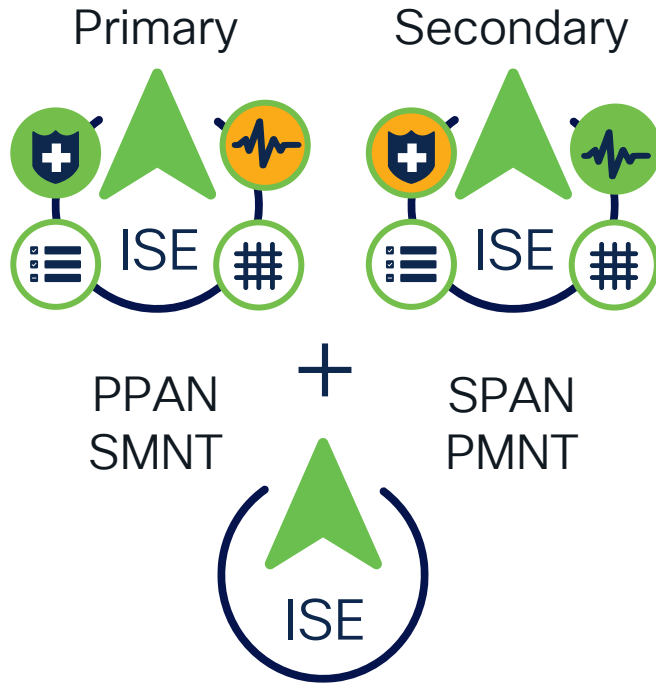
☐ Enable Device Admin Service

☐ Enable Passive Identity Service

☐ > pxGrid

# ISE Small Deployment

## Configuring ISE Small Deployment



The screenshot shows the ISE configuration interface. At the top, there are buttons for "Edit", "Register", "Syncup", and "Deregister". The "Register" button is highlighted with an orange box. Below the buttons, there is a table with two columns: "Hostname" and "Personas". The table has two rows: one with "ise-server" in the "Hostname" column and "Administration, Monitoring, Policy Serv..." in the "Personas" column. An orange line connects the "Register" button to the "Personas" column of the table. Below the table, there is a form with the following fields: "Host FQDN\*" (with the value "ise2.domain.com"), "User Name\*" (with the value "admin"), and "Password\*" (with a masked value "\*\*\*\*\*").

# *ISE Deployment*

Medium



# ISE Deployment: Medium



2 x (PAN+MNT+PXG), <= 6 PSN

# ISE Medium Deployment Scale

 [cs.co/ise-scale](https://cs.co/ise-scale)



Deployment Scale (PAN/MnT)	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3595	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Medium	10,000	75,000	20,000	25,000	150,000	50,000	150,000

# ISE Medium Deployment

## Small to Medium Deployment Transition

From Small to Medium



# ISE Medium Deployment

Small to Medium Deployment Transition(Contd.)

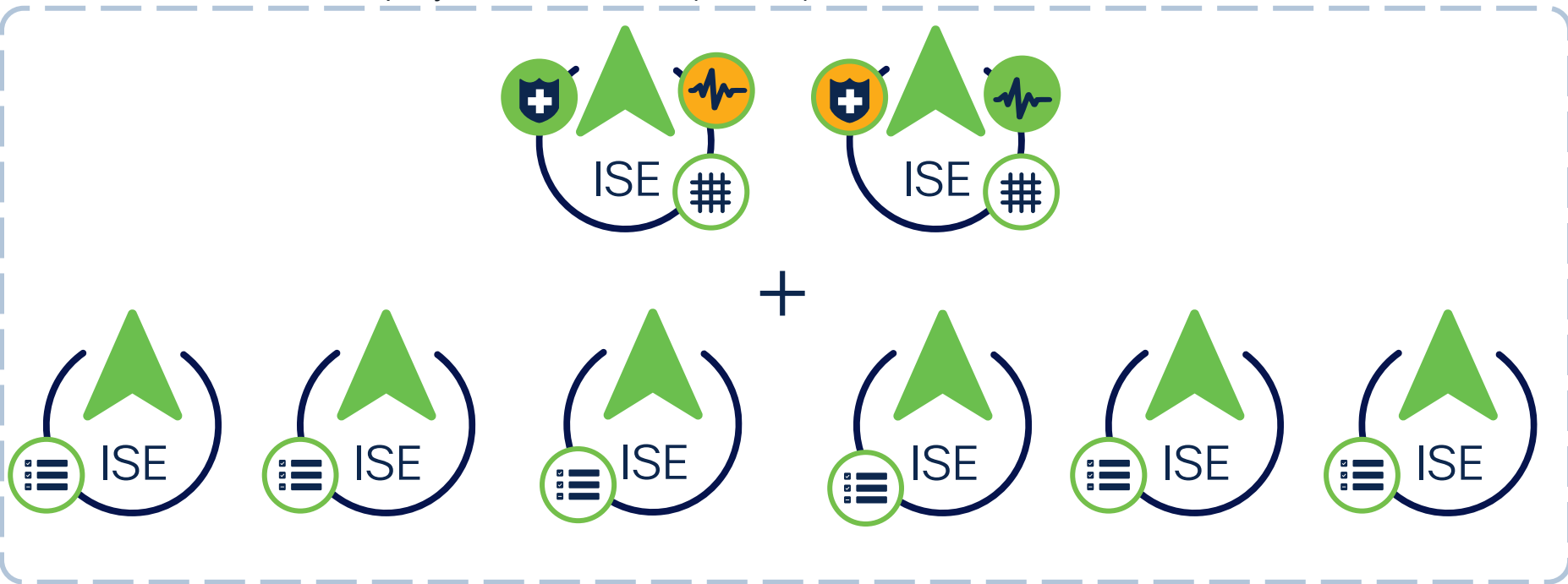


2 x (PAN+MNT+PXG), <= 6 PSN



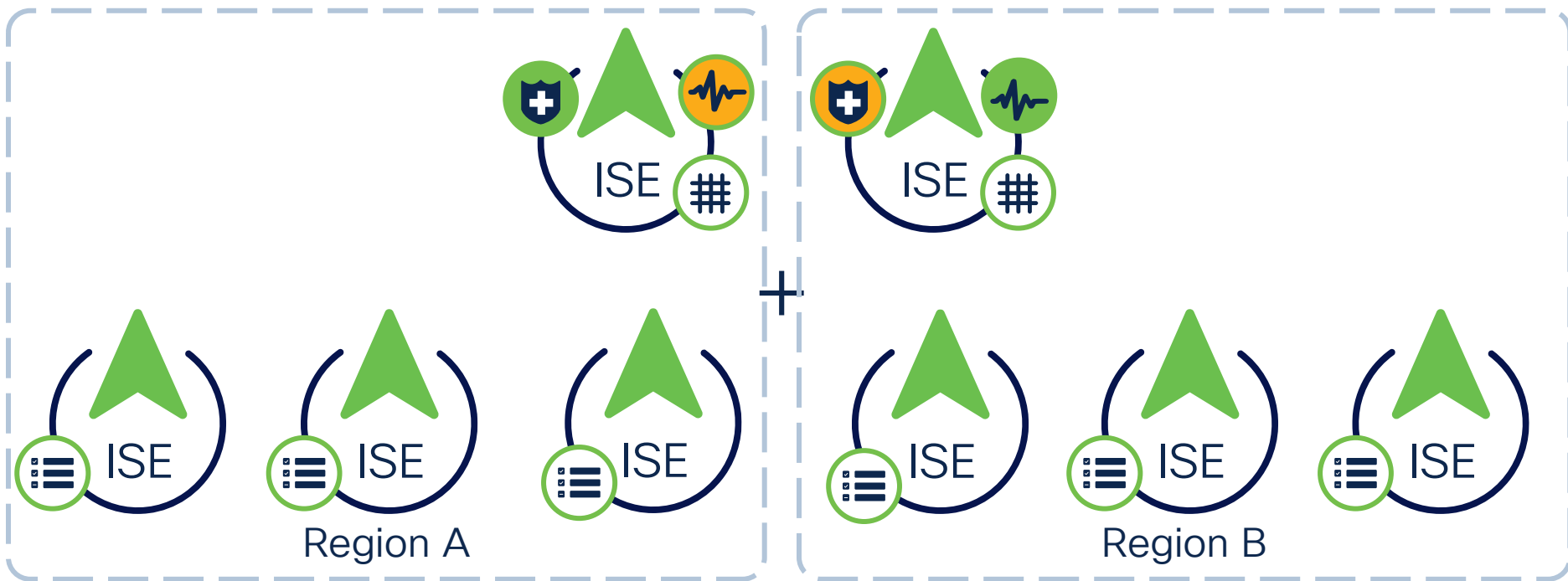
# ISE Medium Deployment

Small to Medium Deployment Transition(Contd.)



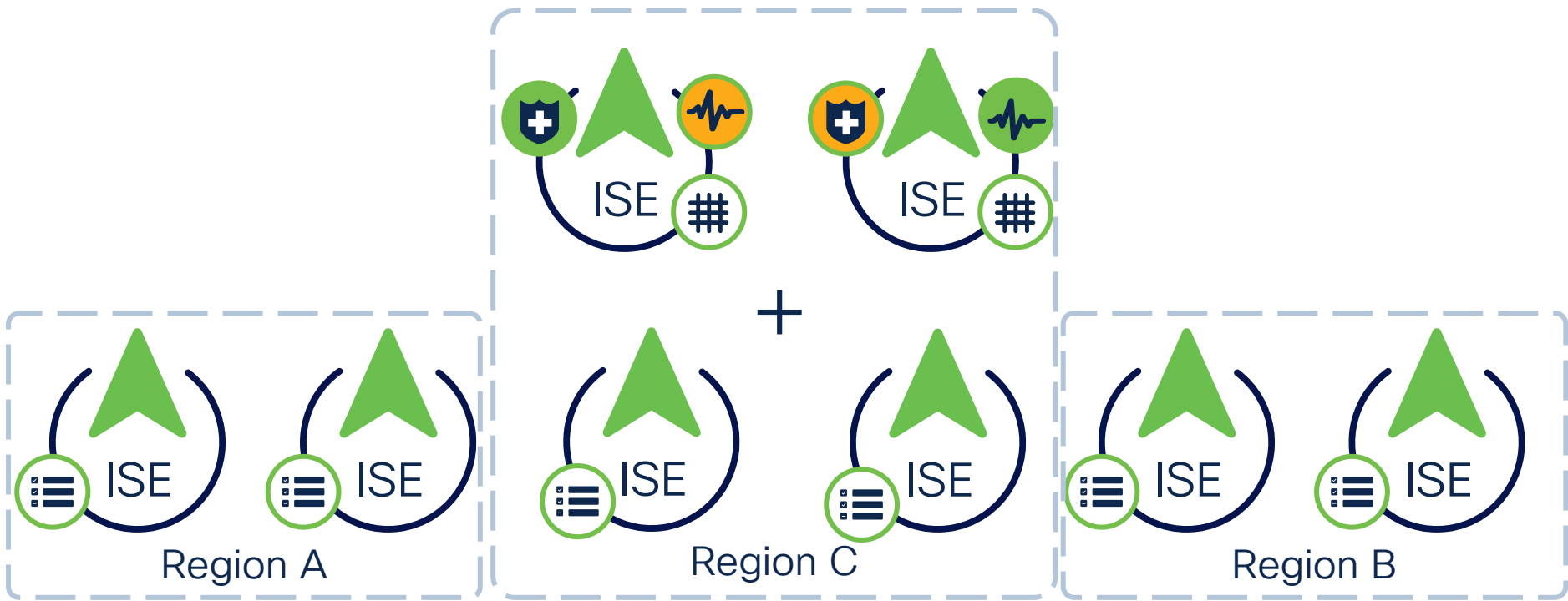
2 x (PAN+MNT+PXG), <= 6 PSN

# ISE Medium Deployment - Models



2 x (PAN+MNT+PXG), <= 6 PSN

# ISE Medium Deployment - Models



2 x (PAN+MNT+PXG), <= 6 PSN

# *ISE Deployment*

Large



# ISE Deployment: Large

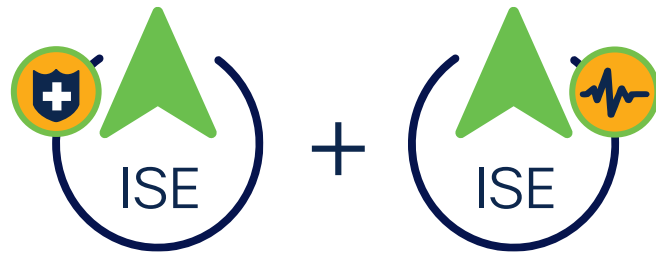
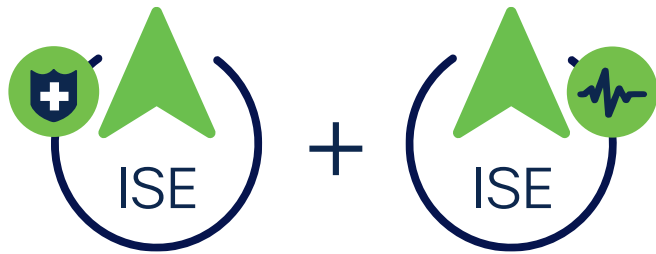
2 PAN, 2 MNT, <=50: PSNs + <= 4 PXGs



# ISE Large Deployment Scale

2 PAN, 2 MNT, <=50: PSNs + <= 4 PXGs

 [cs.co/ise-scale](https://cs.co/ise-scale)



Deployment Scale (PAN/MnT)	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3595	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Large	Unsupported	Unsupported	500,000	500,000	750,000	2,000,000	2,000,000

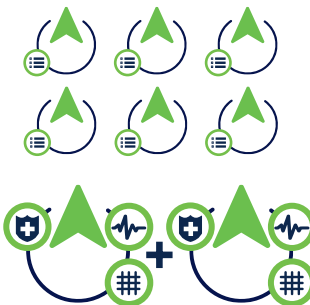
# ISE Deployment Scale

No. of Endpoints Support - Deployment Wise

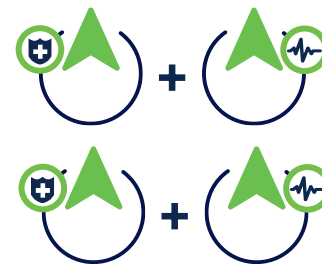
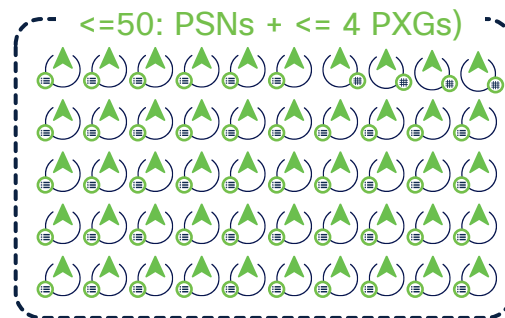
 [cs.co/ise-scale](https://cs.co/ise-scale)



Small HA Deployment



Medium Deployment



Large Deployment

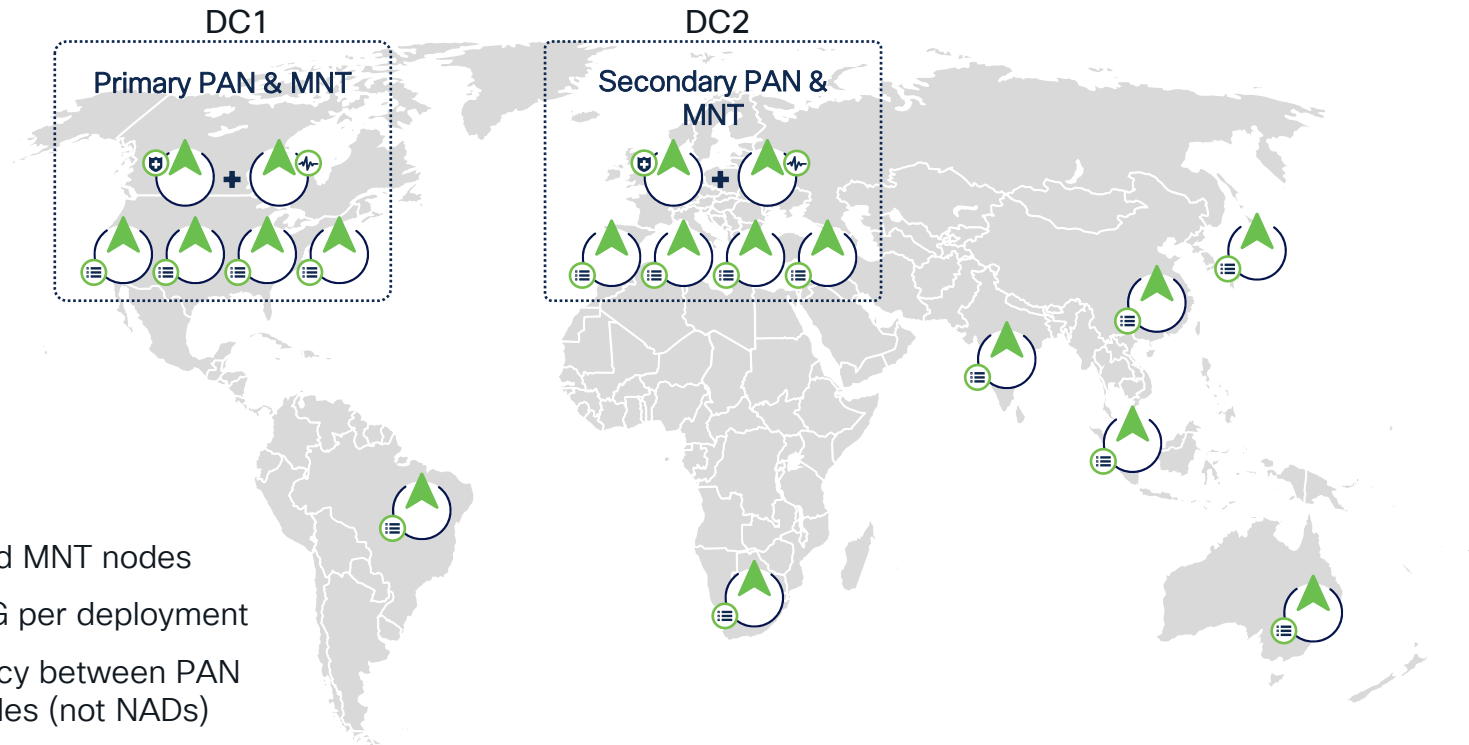
Deployment	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3595	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Large	Unsupported	Unsupported	500,000	500,000	750,000	2,000,000	2,000,000
Medium	10,000	75,000	20,000	25,000	150,000	50,000	150,000
Small	10,000	25,000	20,000	25,000	50,000	50,000	50,000

# *ISE Deployment*

Centralized or Distributed



# Large Deployment: Centralized or Distributed



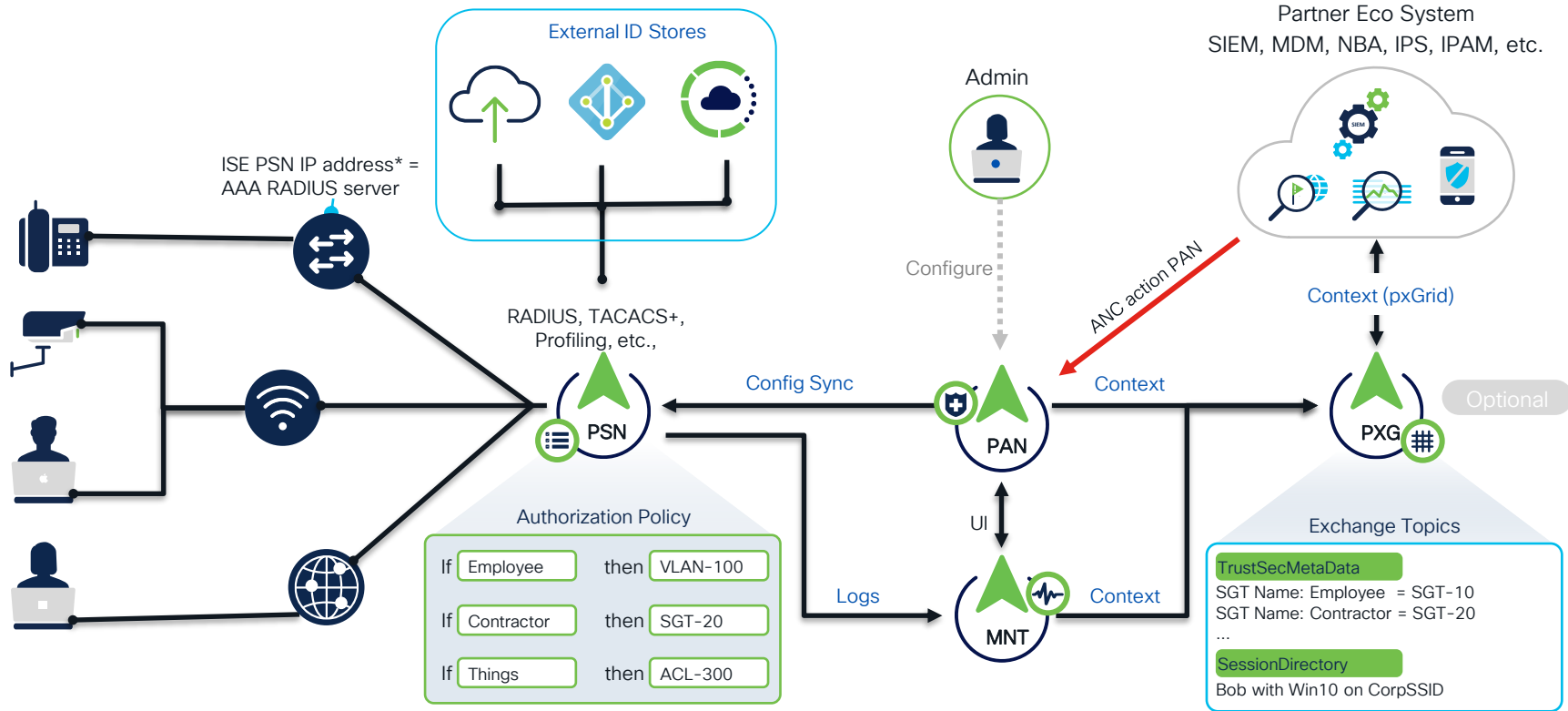
- Separate PAN and MNT nodes
- Max 50 PSN+PXG per deployment
- Max 300ms latency between PAN and other ISE nodes (not NADs)
- Co-locate PSNs with AD or other dependencies

# *ISE Deployment*

Services



# ISE Node Services



\*PSNs can optionally be behind a load-balancer and can be accessed via Load Balancer Virtual IP address (VIPs)

# *ISE Deployment*

Automation

# ISE Policy Management & Lifecycle Orchestration



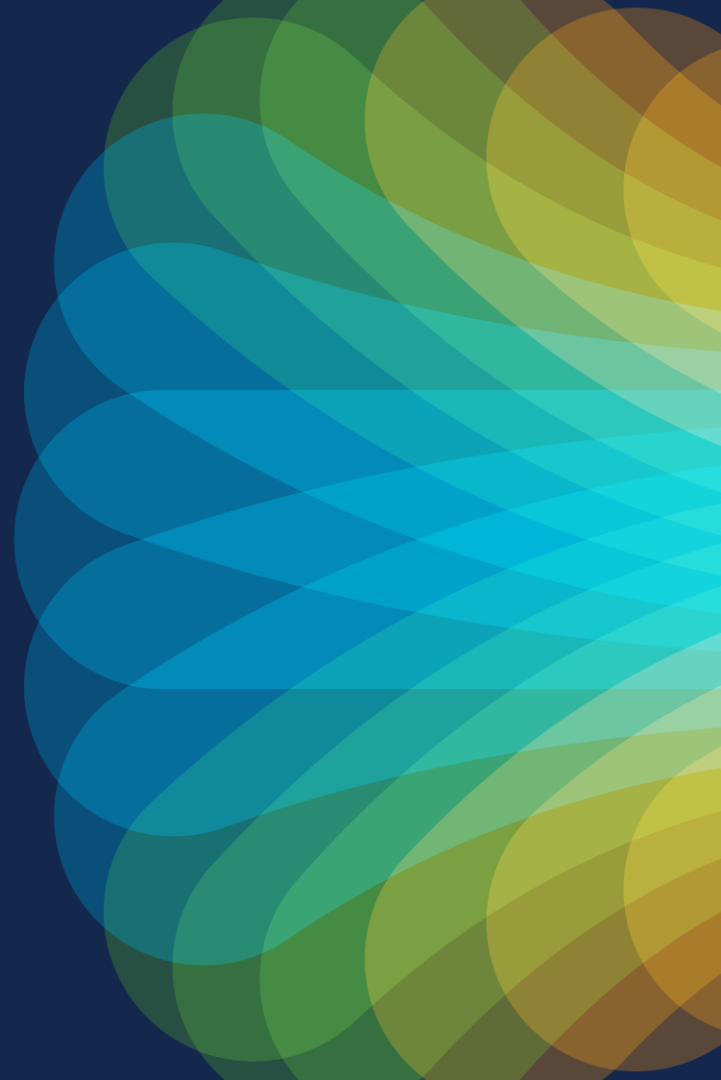
Diagram illustrating the integration of various tools and services with Cisco ISE:

- Tools/Services on the left:** OpenAPIs, Postman, and a combination of `cisco.ise` and `ciscoesdk`.
- Central Component:** ISE (Cisco Identity Services Engine).
- Cloud Services on the right:** internaluser, certificate, sgt, sgadm, endpoint, policy, identitygroup, node, portal, activedirectory, and guestuser.
- Connections:** Green arrows indicate data flow from the tools/services on the left to ISE, and from ISE to the cloud services on the right.

The diagram illustrates the integration of three tools in an AWS environment. On the left is the CloudFormation logo (a green arrow pointing up inside a white circle). In the center is a green plus sign. To the right of the plus sign is the Terraform logo (a purple 3D cube icon above the word "Terraform" in black text). Further right is the Ansible logo (a white letter 'A' inside a dark blue circle). Below the Terraform and Ansible logos, the text "(in AWS!)" is written in white.



# Cisco ISE Design



# ISE Design

- Considerations & Approach
- NDGs & NADs
- Certificates
- Network Access
- Guest
- BYOD
- Profiling
- Compliance





Which Cisco ISE Services  
do you use?



Join at [slido.com](https://slido.com)

#BRKSEC-2091

# ISE Design



- Considerations & Approach
- NDGs & NADs
- Certificates
- Network Access
- Guest
- BYOD
- Profiling
- Compliance

# ISE Capabilities

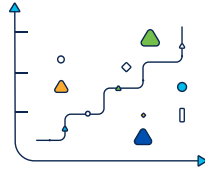


# Everyone Has Different Needs

Government



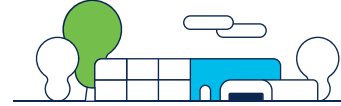
Financials



Healthcare



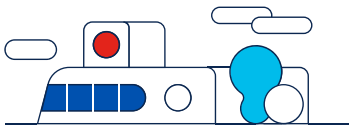
Retail



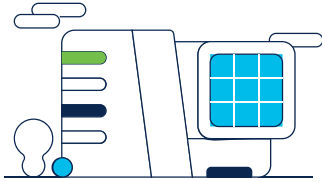
Education



Transportation



Services



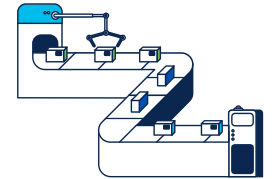
Utilities



Technology



Manufacturing



# Cisco ISE High Level Design (HLD)



- ✓ Business Objectives
- ✓ Environment
- ✓ Scenarios
- ✓ Policy Details
- ✓ Operations & Management
- ✓ Scale & High Availability

## ISE High Level Design (HLD)

AAA AnyConnect Identity Services Engine (...)  
Policy and Access TrustSec VPN

48001 77 0  
VIEWS HELPFUL COM



thomas

05-07-2018 09:40 AM

Edited On: 02-04-2021 01:42 PM

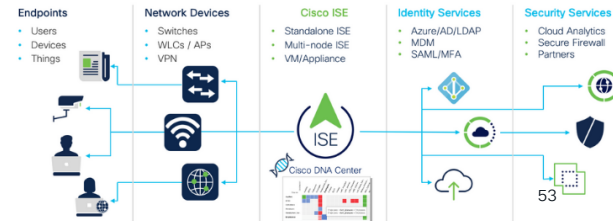


### Introduction

An ISE High Level Design (HLD) is recommended to assist you with the design and planning of your ISE deployment. Having a clearly written security policy - whether aspirational or active - is the first step in assessing, planning and deploying network access security. Without this, it is hard to break down the deployment into phases by location or capabilities. When seeking outside help, the HLD provides a huge time savings for education other teams, partners, Cisco Sales representative, Technical Assistance Center (TAC) representative or even the ISE product and engineering teams. Clearly state the desired solution capabilities, hardware and software environment and integrations can quickly allow people to understand what you want and how to configure it or troubleshoot it.

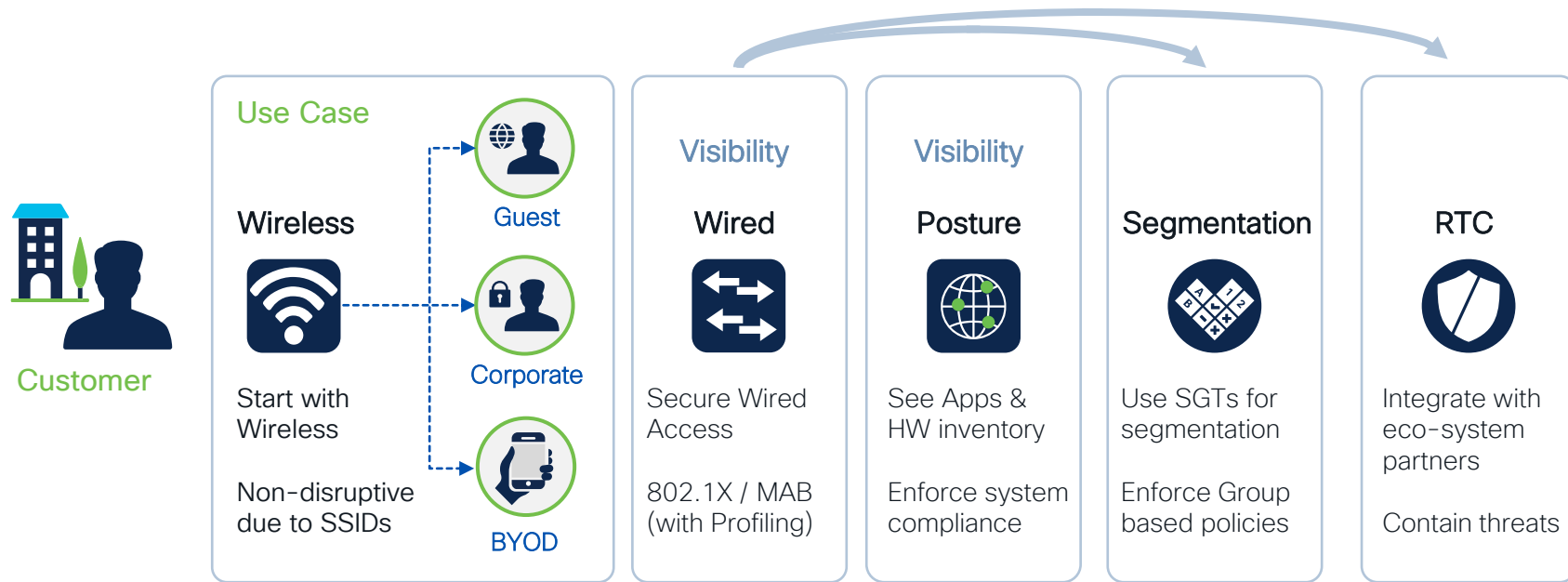
### Enterprise

### Security



# A Typical Customer Journey

No standard or required approach – each use case may be the end goal



# ISE Design



- Considerations & Approach
- NDGs & NADs
- Certificates
- Network Access
- Guest
- BYOD
- Profiling
- Compliance

# Default Network Device Groups (NDGs)

## Network Device Groups

All Groups

Choose group ▾

🔄 Refresh + Add 📄 Duplicate ✎ Edit 🗑 Trash 👁 Show group members 📥 Import 📤 Export ▾ 📄 Flat Table ↗ Expand All ↖ Collapse All ⚙

<input type="checkbox"/>	Name	Description	No. of Network Devices
<input type="checkbox"/>	All Device Types	All Device Types	--
<input type="checkbox"/>	All Locations	All Locations	--
<input type="checkbox"/>	Is IPSEC Device	Is this a RADIUS over IPSEC Device	--
<input type="checkbox"/>	No	Device is not IPSEC Type	0
<input type="checkbox"/>	Yes	Device is IPSEC Type	0

} Default NDGs



# Organizing Your Network Devices by Groups



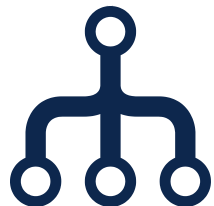
## Network Access Type

- Wired
- Wireless
- VPN
- Branch



## Location

- Theaters
- Country
- City
- Building / Floor / Room



## Organization

- Regions
- Line of Business
- Departments
- IT / OT



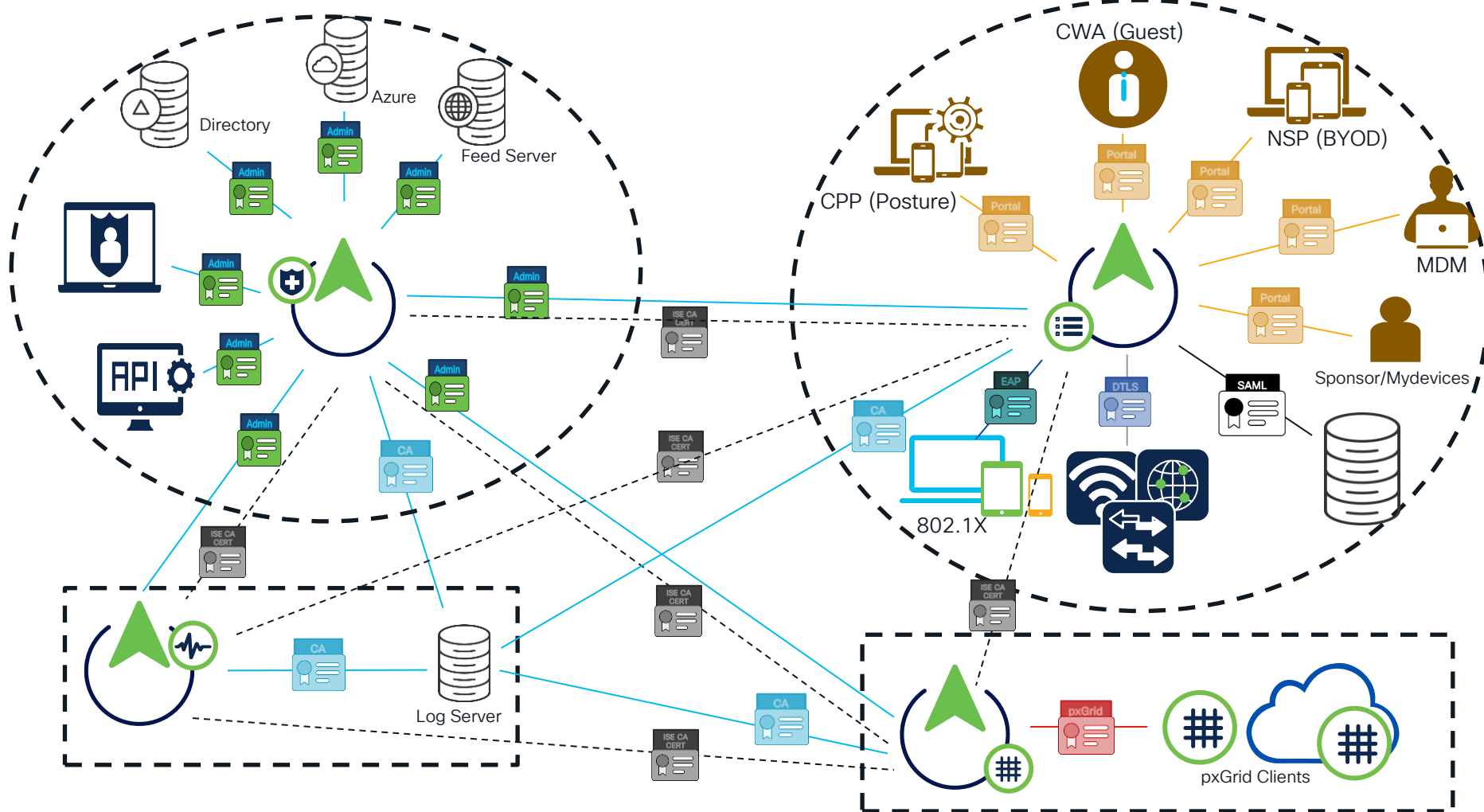
## Vendor / Model

- Cisco
  - Catalyst
  - Meraki
- Aruba
- Juniper

# ISE Design

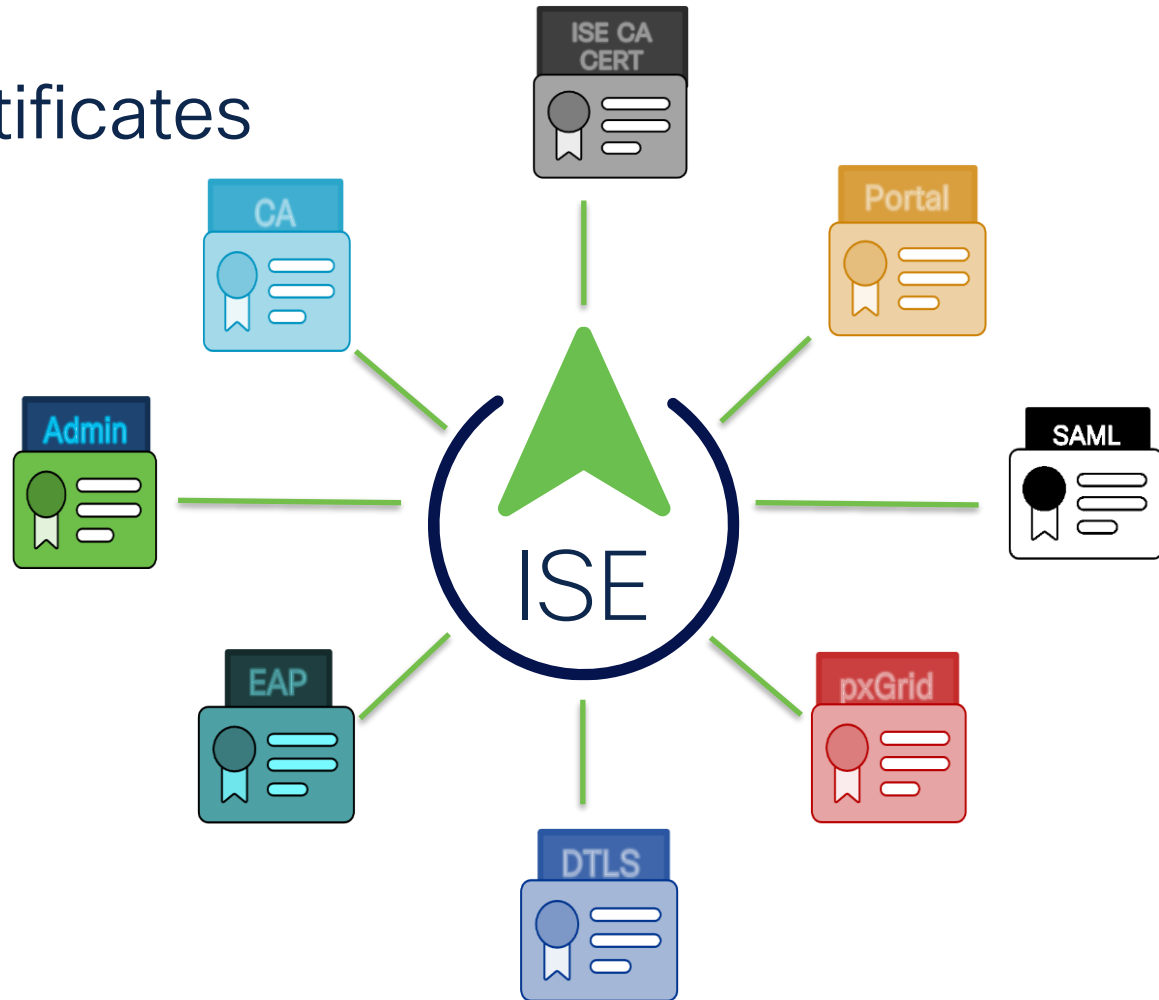


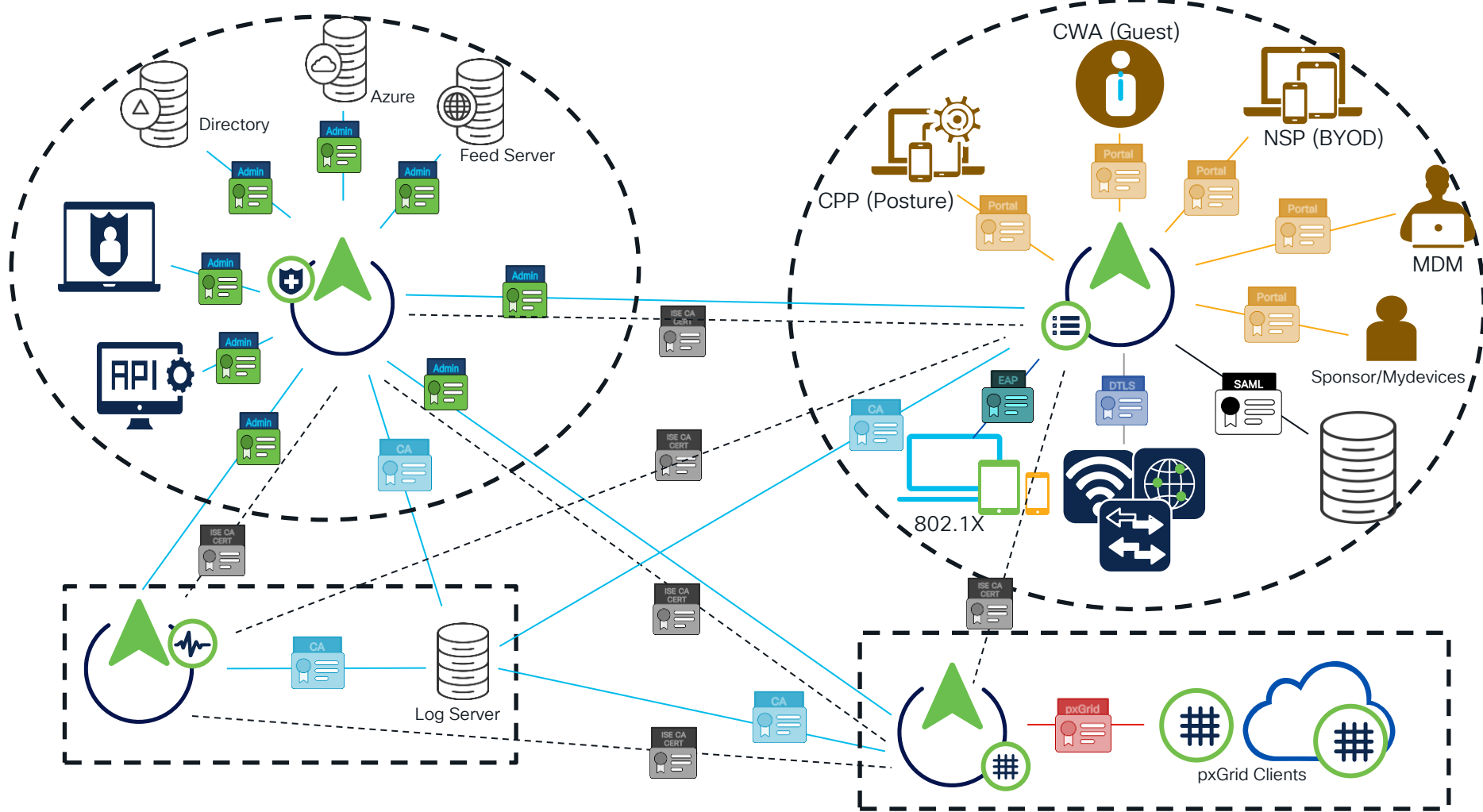
- Considerations & Approach
- NDGs & NADs
- **Certificates**
- Network Access
- Guest
- BYOD
- Profiling
- Compliance



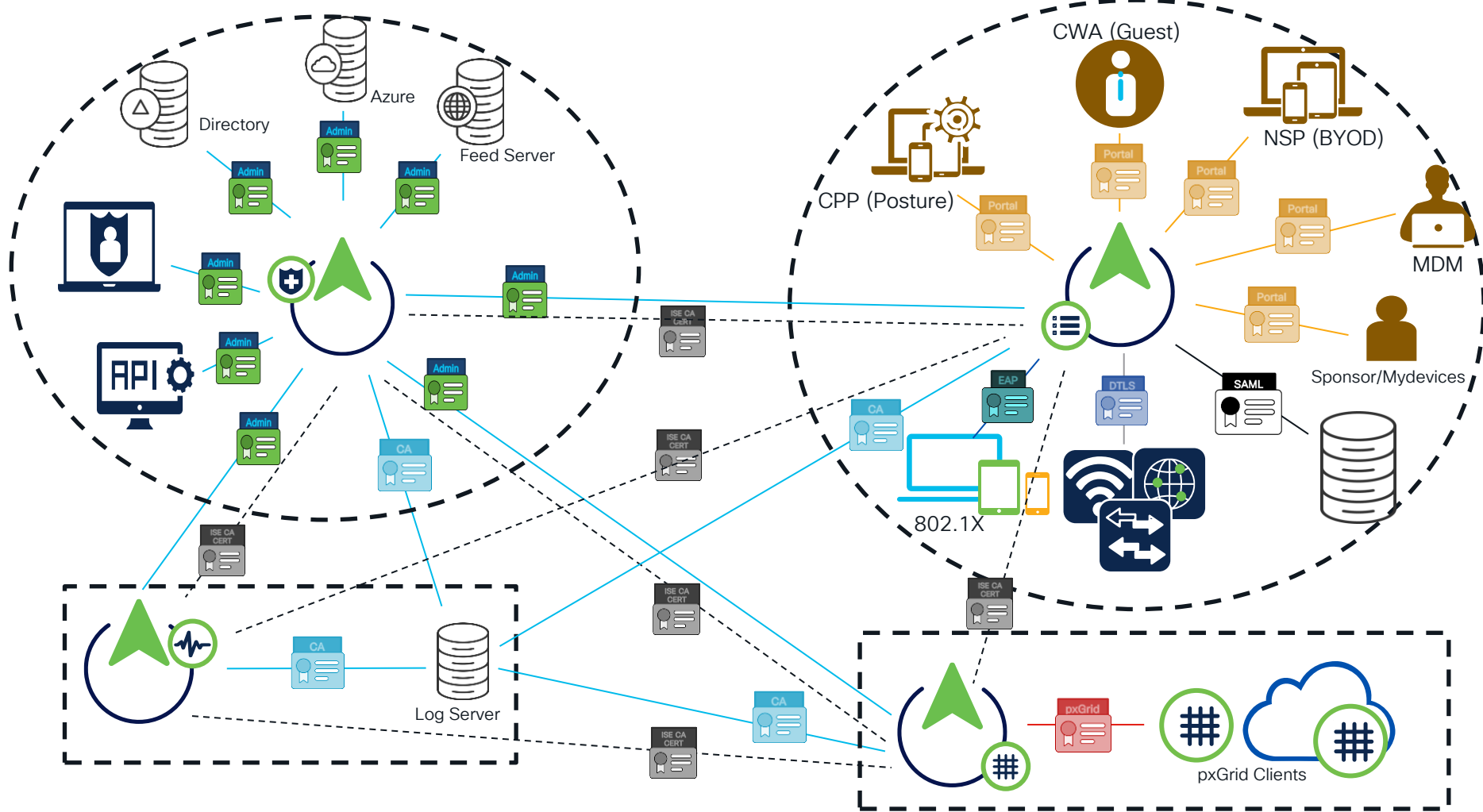
# ISE Certificate architecture

# ISE Certificates





# ISE Certificate architecture



# ISE Certificate architecture

# ISE Design



- Considerations & Approach
- NDGs & NADs
- Certificates
- Network Access
- Guest
- BYOD
- Profiling
- Compliance

# Access Control Context



**Who** ... is requesting access?

---



**What** ... is their role, profile, compliance?

---



**Where** ... are they attempting access from?

---



**When** ... are they allowed access?

---



**Why** ... are they allowed access?

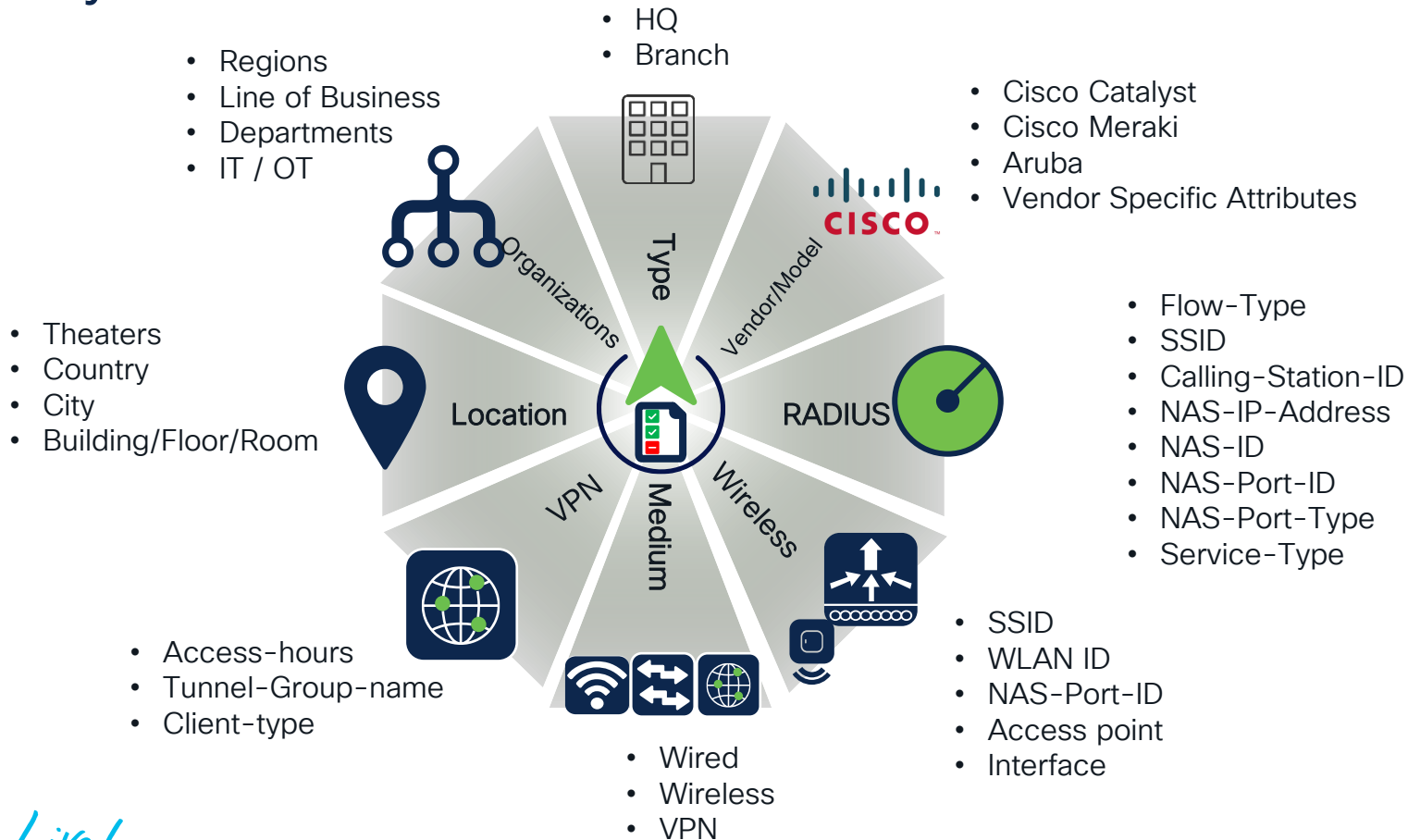
---



**How** ... much access are they allowed?



# Policy Sets Conditions



# Example ISE Policy Sets

## Policy Sets

[Reset](#)
[Reset Policyset Hitcounts](#)
[Save](#)

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
				<input type="text" value="Search"/>				
	✓	Secure Access.		<div>OR</div> <div> <div> </div> <div>                     DEVICE-Location EQUALS All Locations#My-Territory#UK-region                 </div> </div> <div> <div> </div> <div>                     DEVICE-Location EQUALS All Locations#My-Territory#US                 </div> </div>	TEAP Network Access	0		
	✓	Wireless.		<div>AND</div> <div> <div> </div> <div>                     DEVICE-Device Type EQUALS All Device Types#Wireless#WLC9800                 </div> </div> <div> <div> </div> <div>                     Radius-Called-Station-ID CONTAINS Secure-SSID                 </div> </div>	Default Network Access	0		
	✓	Guest Access.		<div>OR</div> <div> <div> </div> <div>                     Radius-Service-Type EQUALS Call Check                 </div> </div> <div> <div> </div> <div>                     Radius-Called-Station-ID CONTAINS .employee-mab                 </div> </div>	Default Network Access	0		
	✓	VPN.		<div> <div> </div> <div>                     DEVICE-Device Type EQUALS All Device Types#VPN-Concentrators                 </div> </div>	Default Network Access	0		

# ISE Policy evaluation



RADIUS  
Access-Request

PSN

## ▼ RADIUS Protocol

Code: **Access-Request** (1)

Packet identifier: x0 (0)

Length: 153

Authenticator:29eb293b3a40ea740a8fd33bdb18f1d7

## ▼ Attribute Value Pairs

> AVP: t=User-Name (1) 1=8 val=**pavan**

> AVP: t=NAS-IP-Address (4) (=6 val=**6.86.227.108**

> AVP: t=Calling-Station-Id (31) 1=19 val=**02-00-00-00-00-01**

> AVP: t=Called-Station-Id (30) 1=27 val=**2C-3F-0B-56-E3-6C: Employee**

> AVP: t=Framed-MTU (12) (=6 val=**1400**

> AVP: t=NAS-Port-Type (61) (=6 val=**Wireless-802.11 (19)**

> AVP: t=Service-Type (6) 1=6 val=Framed (2)

> AVP: t=Connect-Info (77) (=24 val=**CONNECT 11Mbps 802.11b**

> AVP: t=EAP-Message (79) 1=13 Last Segment [1]

> AVP: t=Message-Authenticator (80) 1=18

val=26f047af6a9a82279dfd6d19b477c31b

> AVP: t=Vendor-Specific (26) 1=36 vnd=ciscoSystems (9)

> AVP: t=EAP-Message (79) 1=6 Last Segment [1]

> AVP: t=Message-Authenticator (80) (=18 val=1cb417480820021d54882fcaea90308c

> AVP: t=Tunnel-Private-Group-Id (81) (=7 Tag=0x01 val=**DATA**

▼ AVP: t=Vendor-Specific (26) 1=36 vnd=ciscoSystems (9)

Type: 26

Length: 36

Vendor ID: ciscoSystems (9)

> VSA: t=Cisco-AVPair (1) (=30 val=**linksec-policy=should-secure**

▼ AVP: t=Vendor-Specific (26) 1=80 vnd=ciscoSystems (9)

Type: 26

Length: 80

Vendor ID: ciscoSystems (9)

> VSA: t=Cisco-AVPair (1) (=74 val=**ACS: CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT-ALL-IPV4 TRAFFIC-57f6b0d3**

▼ AVP: t=Vendor-Specific (26) (=38 vnd=ciscoSystems (9)

NAD Evaluation



failed

Request Drop

Pass

Policy sets  
evaluation  
based on  
conditions

Policy  
set  
match

> Authentication Policy (

Send RADIUS  
Access-Accept  
using authz profile

Send RADIUS  
Access-Reject

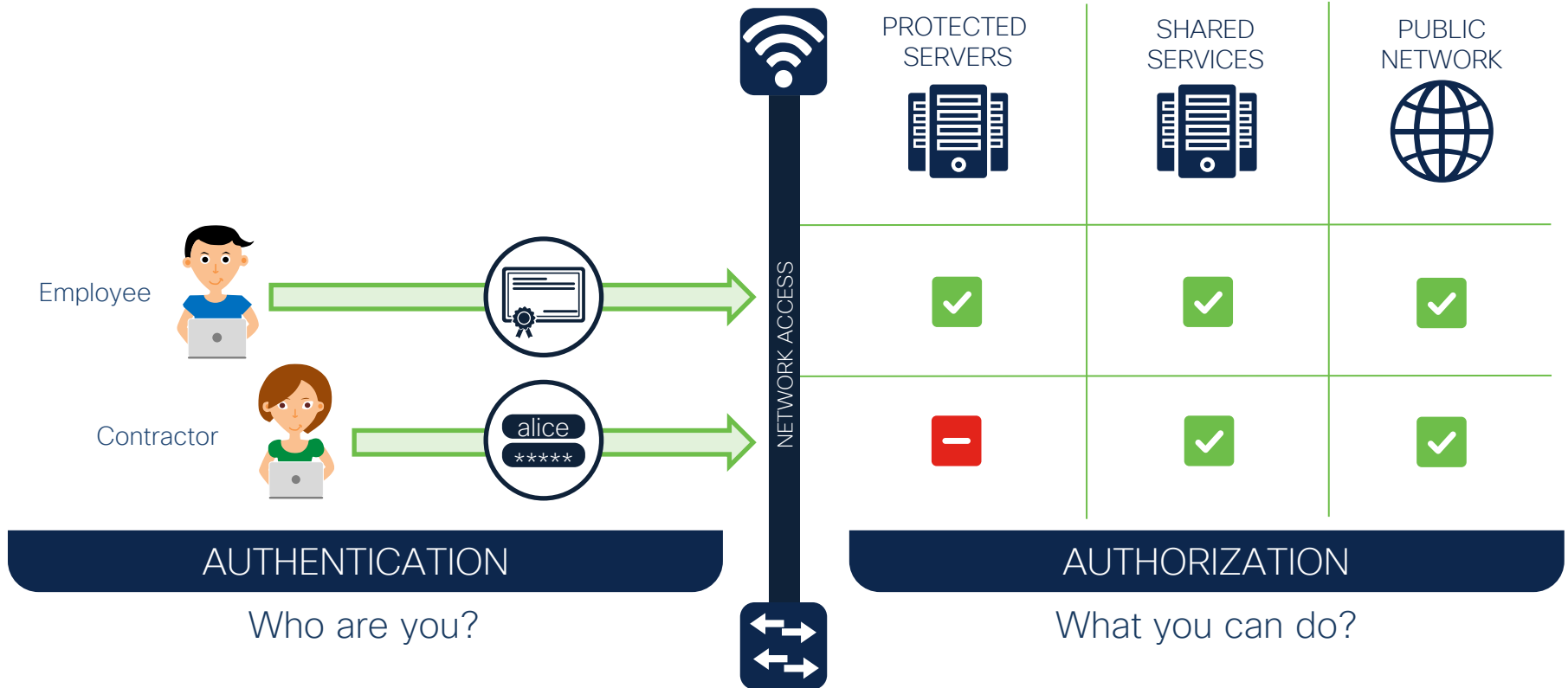
> Authorization Policy - Local Exception

> Authorization Policy - Global Exception

> Authorization Policy (13)

11007 Could not locate Network Device or AAA Client  
5405 RADIUS Request dropped  
5413 RADIUS Accounting-Request dropped

# Authentication and Authorization



# Enforce Trust-Based Access: Authorization

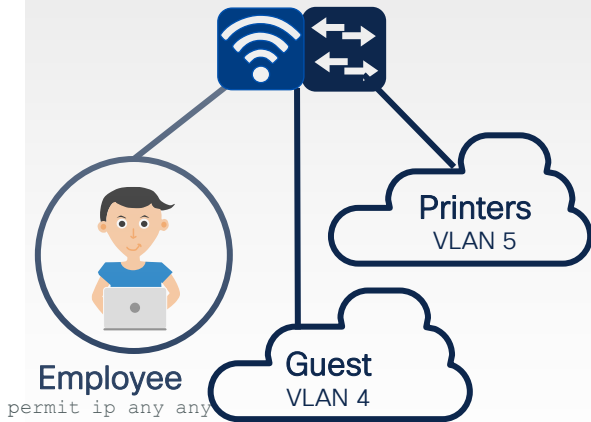
Beyond RADIUS Access-Accept / Access-Reject



VLANs Dynamic VLANs

ACLs Downloadable

ACL(Wired), Named ACL(Wired + Wireless)



Per port / Per Domain /  
Per MAC

CISCO *Live!*

Security Group Tags

Cisco Group-Based Policy

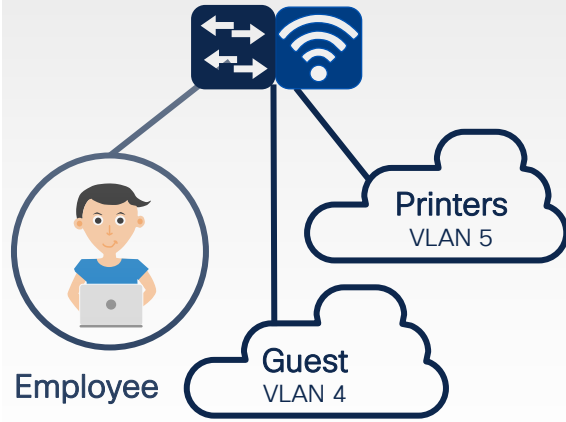


16-bit SGT assignment and  
SGT based Access Control



Named/Group VLANs

Named ACLs



[cs.co/trustsec-compatibility](https://cs.co/trustsec-compatibility)

# *ISE Design*

Other Factors

# ISE Compatibility



RFC2865 : RADIUS  
RFC2866 : Accounting  
RFC3579 : EAP Support  
RFC5176 : CoA Support

Cisco ISE supports protocol standards like RADIUS, its associated RFC Standards, and TACACS+. For more information, see the [ISE Community Resources](#).

Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior for standards-based authentication.

Cisco ISE interoperates fully with third-party TACACS+ client devices that adhere to the governing protocols. Support for TACACS+ functions depends on the device-specific implementation.



[cs.co/ise-compatibility](https://cs.co/ise-compatibility)

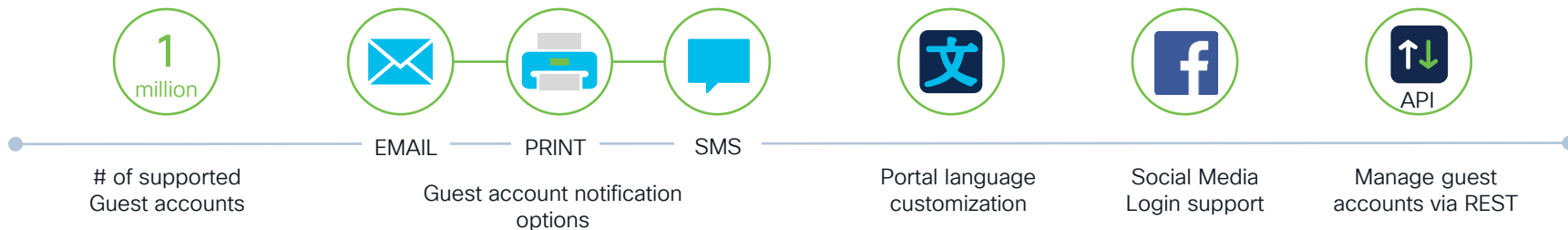
# ISE Design



- Considerations & Approach
- NDGs & NADs
- Certificates
- Network Access
- Guest
- BYOD
- Profiling
- Compliance

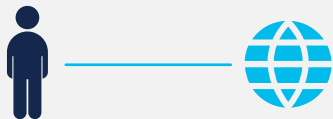


# Guest Solution Overview



## The 3 types of guest access

### Hotspot



Immediate, un-credentialed Internet access

### Self Registered



Self-registration by guests, Sponsors may approve access

### Sponsored Guest Access



Authorized sponsors create account and share credentials

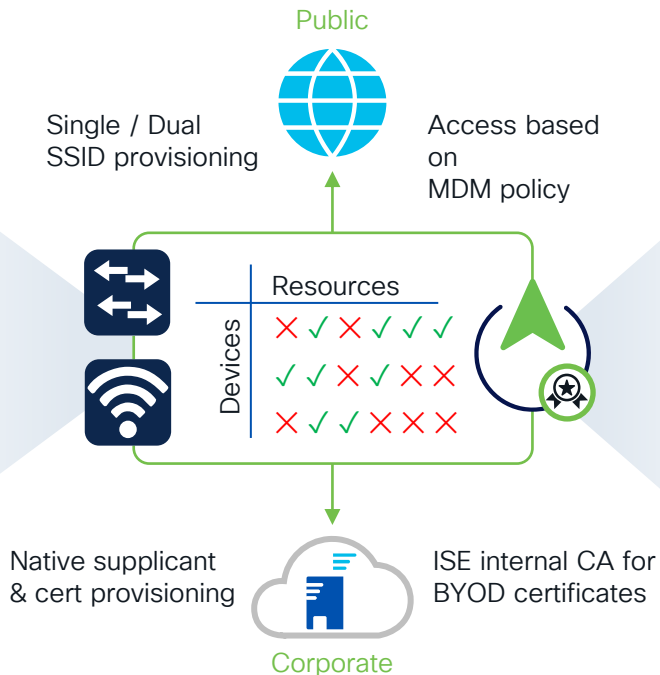
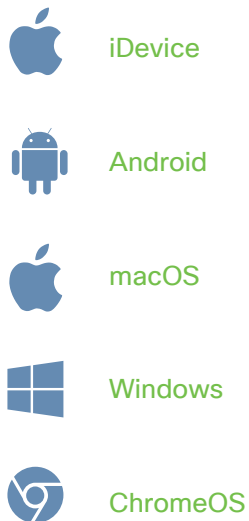
# ISE Design



- Considerations & Approach
- NDGs & NADs
- Certificates
- Network Access
- Guest
- BYOD
- Profiling
- Compliance

# ISE BYOD Solution

## Device Support



## EMM/MDM Integrations



EMM: Enterprise Mobility Management | MDM: Mobile Device Management

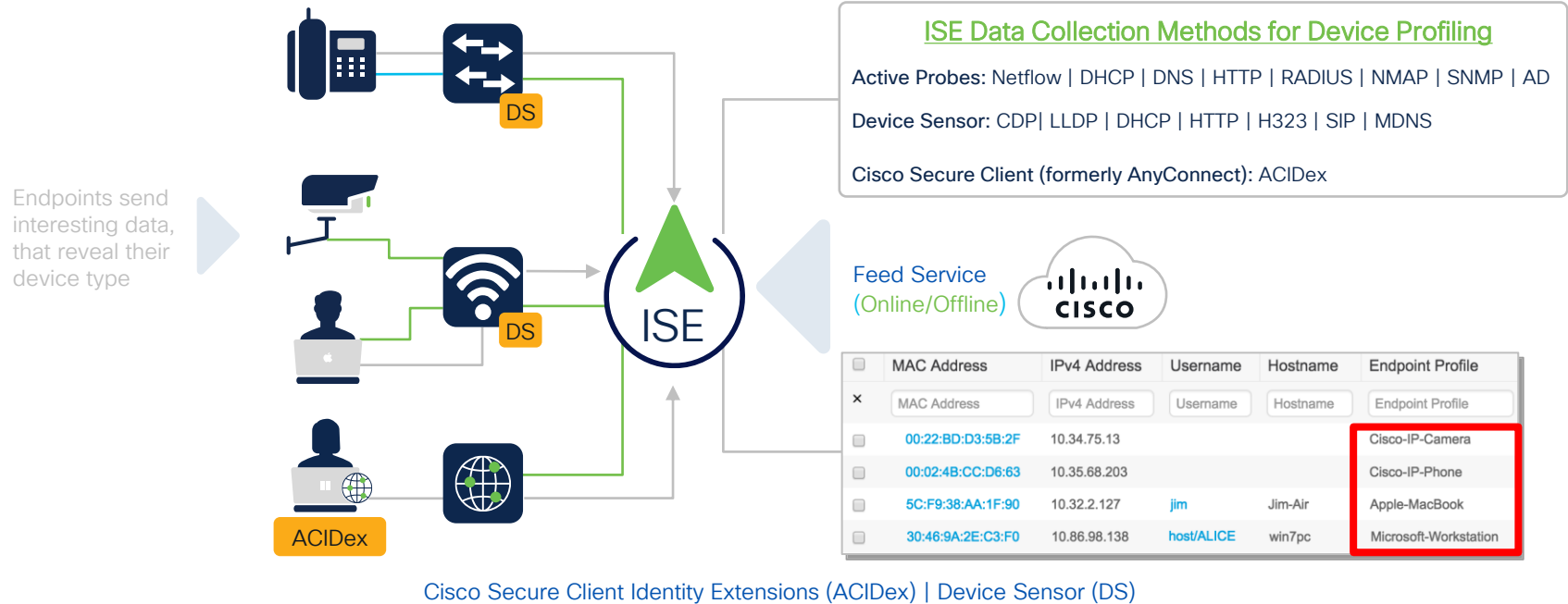
# ISE Design



- Considerations & Approach
- NDGs & NADs
- Certificates
- Network Access
- Guest
- BYOD
- Profiling
- Compliance

# Endpoint Profiling

The profiling service in Cisco ISE identifies the devices that connect to your network



# Profiling Packages and Integrations

## Medical Devices



Hospital



250+ Medical device profiles

Pharma-Smart-Device
Philips-Analytical-X-Ray-Device
Philips-CareServant-Device
Philips-Healthcare-PCCI-Device
Philips-Medical-Systems-Device
Philips-Oral-Healthcare-Device
Philips-Patient-Monitoring-Device
Philips-Personal-Health-Device
Philips-Respironics-Device
Phonak-Communications-Device

## IOT Building & Automation

Library



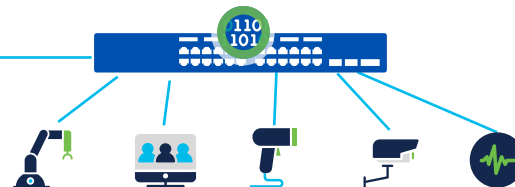
Siemens-Device
Siemens-Automation-Drives-Device
Siemens-Building-Device
Siemens-Building-Technologies-Device
Siemens-Convergence-Device
Siemens-Digital-Factory-Device
Siemens-Energy-Automation-Device
Siemens-Energy-Management-Device
Siemens-Home-Office-Device
Siemens-Industrial-Automation-Device

# pxGrid



Cisco  
CyberVision

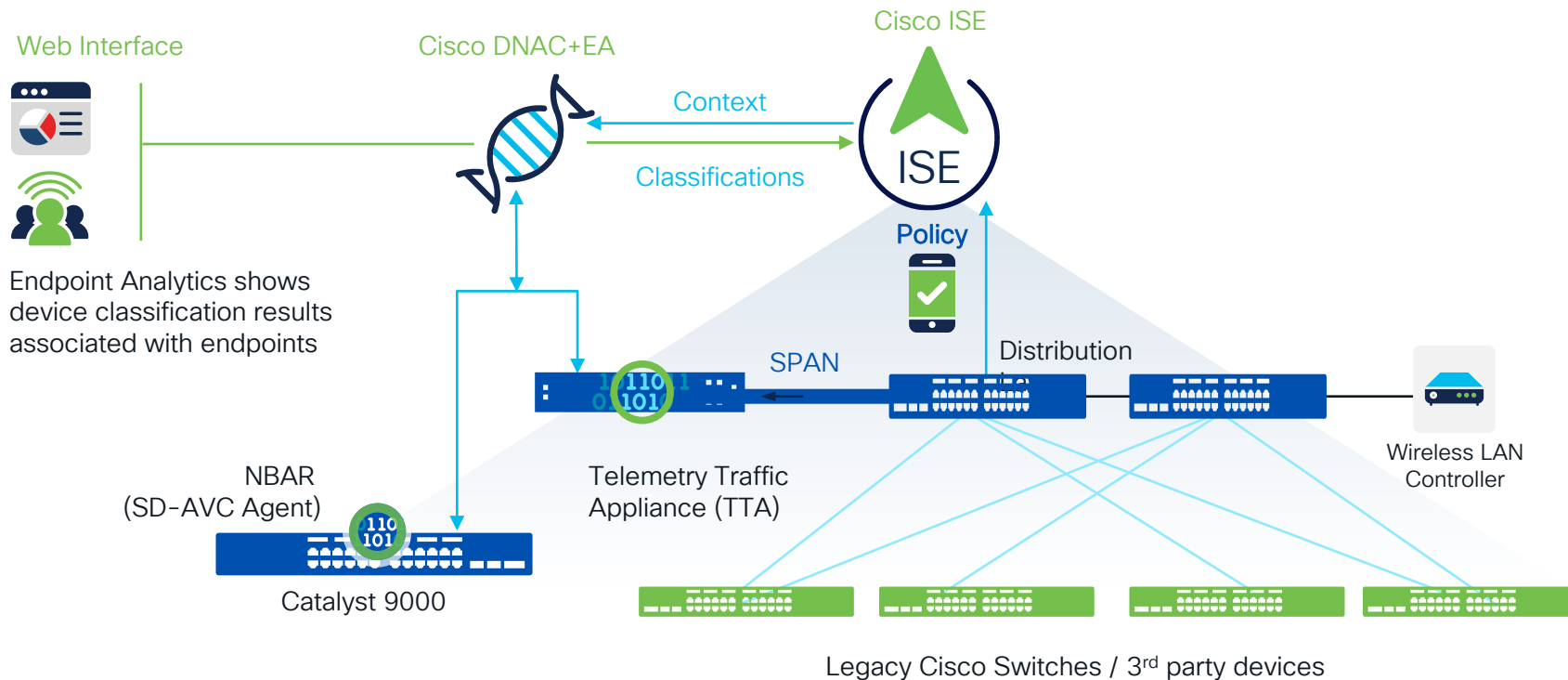
# pxGrid



## Cisco AI Endpoint Analytics

Profiles IOT devices and sends endpoint labels via pxGrid to ISE for authorization

# Cisco AI Endpoint Analytics and ISE

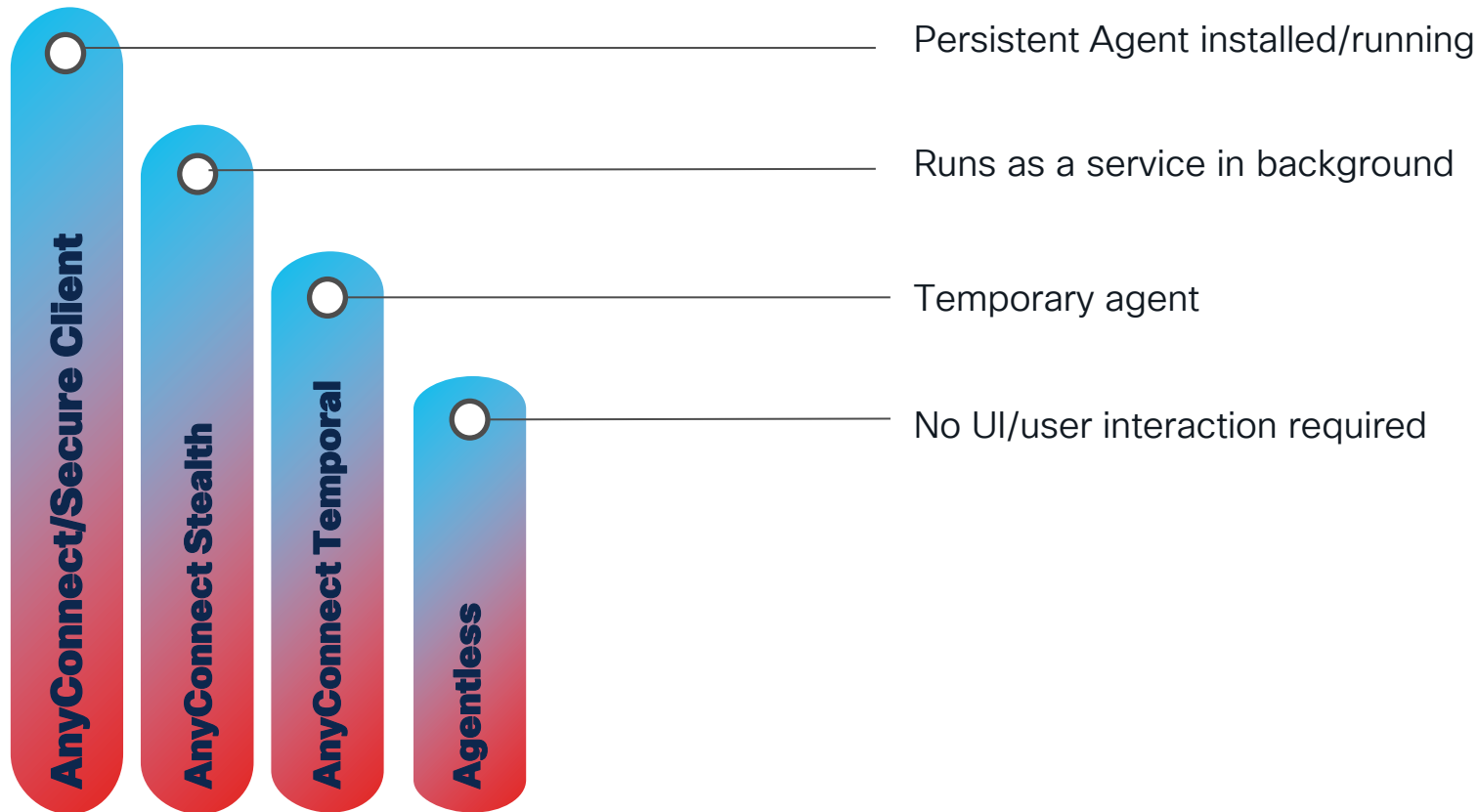


# ISE Design




- Considerations & Approach
- NDGs & NADs
- Certificates
- Network Access
- Guest
- BYOD
- Profiling
- Compliance












# Agent Types












# Agent & Agentless Posture Options

 Supported  
 Limitations  
 Not Supported

Capability	AnyConnect			AC Stealth		Temporal		Agentless	
									
Anti-Malware Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Firewall Installation Checks	✓	✓	✗	✓	✓	✓	✓	✓	✓
Application Inventory	✓	✓	✗	✓	✓	✓	✓	✓	✓
Hardware Inventory	✓	✓	✗	✓	✓	✓	✓	✓	✓
Process Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dictionary Conditions	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application Checks	✓	✓	✗	✓	✓	✓	✓	✓	✓
File Checks	✓	✓	!	✓	✓	✓	✓	!	✓
Service Checks	✓	✓	✗	✓	✓	✓	!	✓	!
Disk Encryption	✓	✓	✗	✓	✓	!	!	!	!
Patch Management	✓	✓	!	✓	✓	!	!	!	!
Registry Checks	✓	N/A	N/A	✓	N/A	✓	N/A	!	N/A
USB Checks	✓	✗	✗	✓	✗	✓	✗	✓	✗
WSUS remediation (legacy)	✓	N/A	N/A	✓	N/A	✗	✗	✗	✗
Remediation	Auto, Manual	Partial	Partial	Part Auto	Partial	Text	Text	✗	✗
Reassessment	✓	✓	✓	✓	✓	✗	✗	✗	✗

# Posture Deployment Options

- ✓ Supported
- ⚠ Limitations
- ✗ Not Supported

Capability	AnyConnect			AC Stealth		Temporal		Agentless	
									
Anti-Malware Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Firewall Installation Checks	✓	✓	✗	✓	✓	✓	✓	✓	✓
Application Inventory	✓	✓	✗	✓	✓	✓	✓	✓	✓
Hardware Inventory	✓	✓	✗	✓	✓	✓	✓	✓	✓
Process Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dictionary Conditions	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application Checks	✓	✓	✗	✓	✓	✓	✓	✓	✓
File Checks	✓	✓	⚠	✓	✓	✓	✓	⚠	✓
Service Checks	✓	✓	✗	✓	✓	✓	⚠	✓	⚠
Disk Encryption	✓	✓	✗	✓	✓	⚠	⚠	⚠	⚠
Patch Management	✓	✓	⚠	✓	✓	⚠	⚠	⚠	⚠
Registry Checks	✓	N/A	N/A	✓	N/A	✓	N/A	⚠	N/A
USB Checks	✓	✗	✗	✓	✗	✓	✗	✓	✗
WSUS remediation (legacy)	✓	N/A	N/A	✓	✗	✗	✗	✗	✗
Remediation	Auto Manual	Partial	Partial	Part Auto	Part Auto	Text	Text	✗	✗
Reassessment	✓	✓	✓	✓	✓	✗	✗	✗	✗

Visibility (Effort)

Experience (Time)

Security (Protection)

# Posture/MDM Compliance



 [cisco.com/go/csta](https://cisco.com/go/csta)

**CISCO** *Live!*

**Absolute**Software

**SOPHOS**

 **GLOBO**

 IBM Security

 Microsoft

**SOTI**

**tangoe**

 Meraki

 XenMobile

 jamf

 SAP

 MobileIron

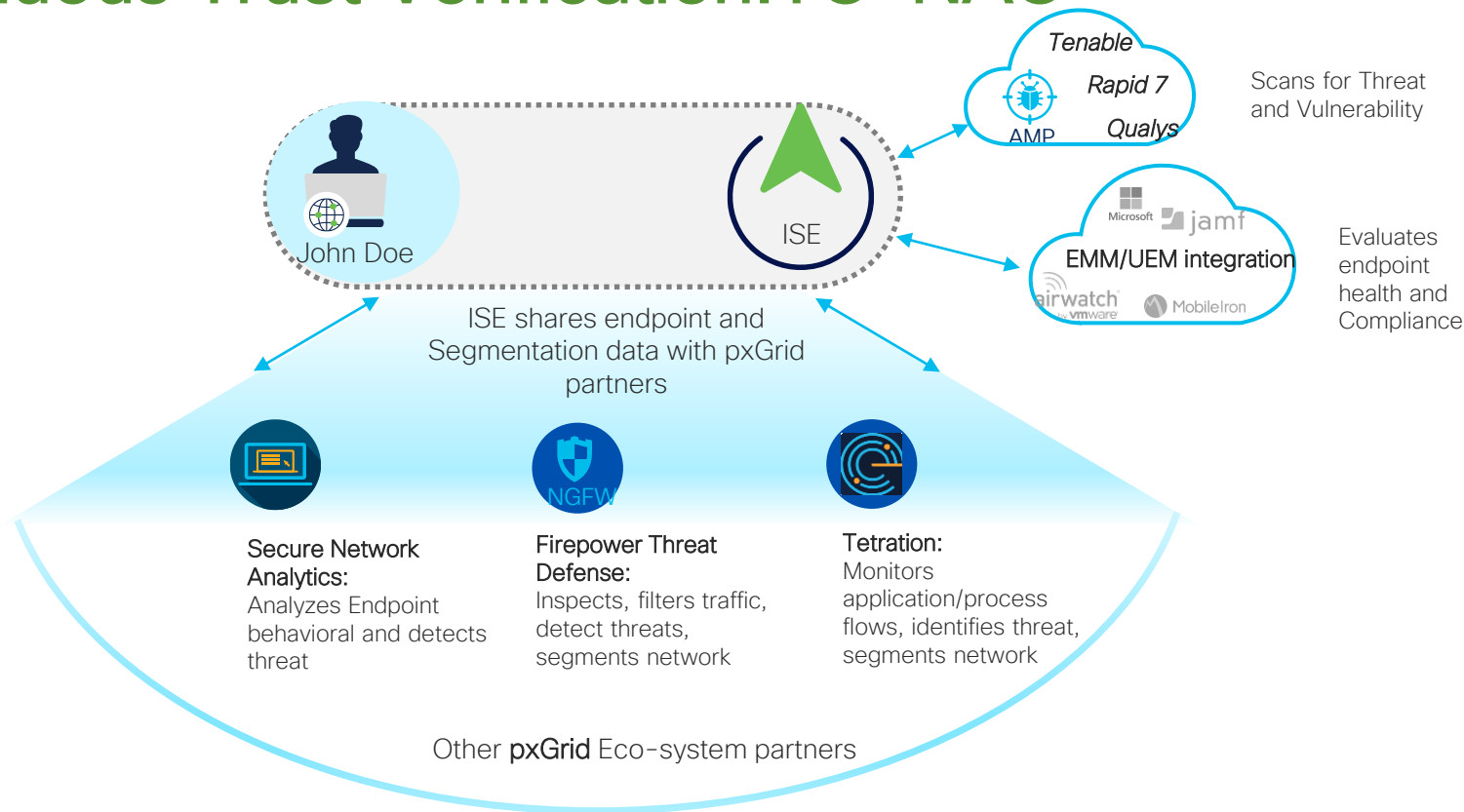
 Symantec

 airwatch  
by vmware

## MDM Attributes

ActivityType  
AdminAction  
AdminActionUUID  
AnyConnectVersion  
DaysSinceLastCheckin  
DetailedInfo  
DeviceID  
DeviceName  
DeviceType  
DiskEncryption  
EndPointMatchedProfile  
FailureReason  
IdentityGroup  
IMEI  
IpAddress  
JailBroken  
LastCheckInTimeStamp  
MacAddress  
Manufacturer  
MDMCompliantStatus  
MDMFailureReason  
MDMServerName  
MEID  
Model  
OperatingSystem  
PhoneNumber  
PinLock  
PolicyMatched  
RegisterStatus  
SerialNumber  
ServerType  
SessionId  
UDID  
UserName  
UserNotified

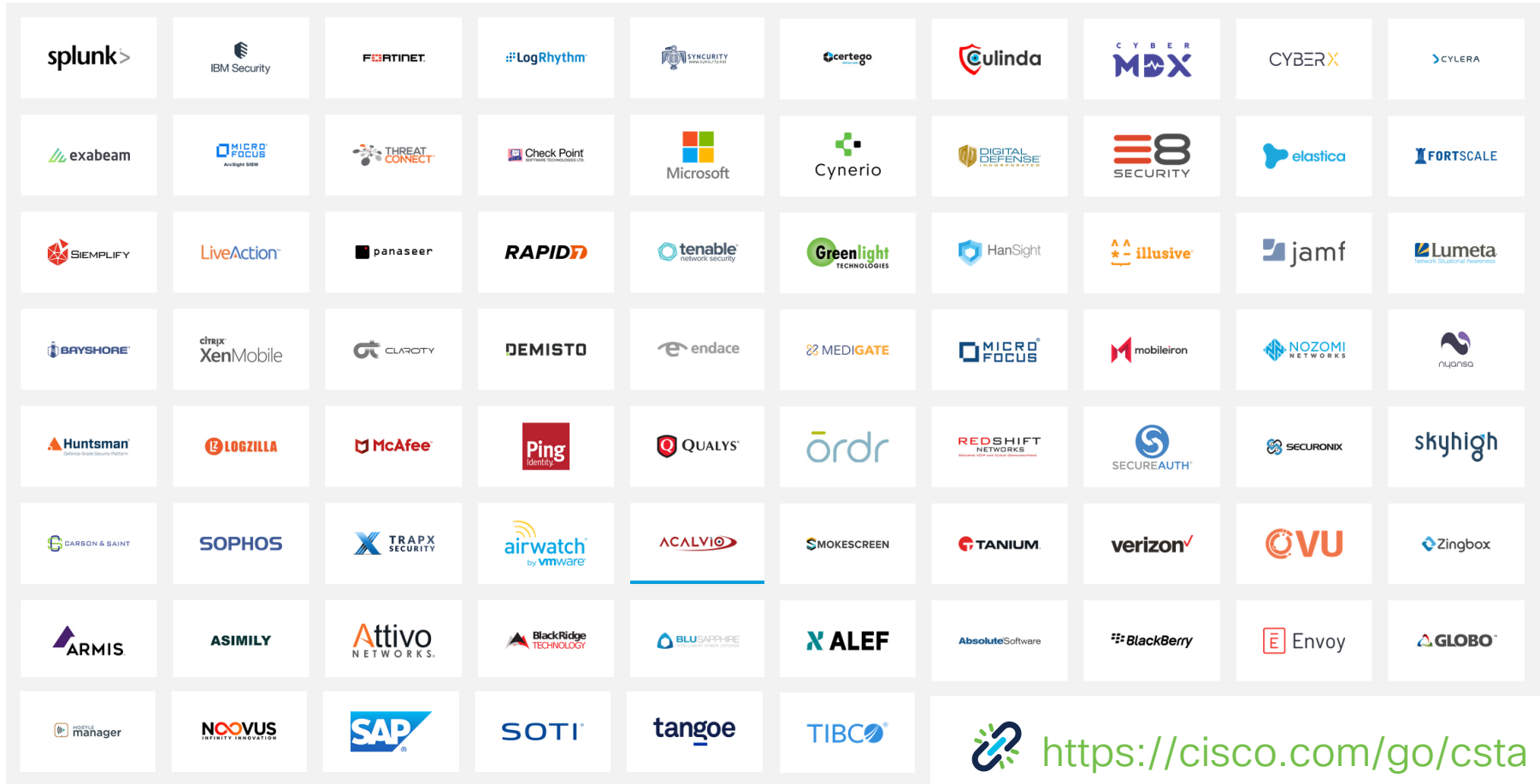
# Continuous Trust Verification:TC-NAC



# *ISE Design*

## Integrations

# Cisco Security Technical Alliance Partners



# Cisco ISE Best Practices

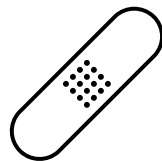


# *Cisco ISE Best Practices*

Recommended Release & Patches

# ISE Recommended Release

## Patches



Apply Latest Patches



[cs.co/ise-software](https://cs.co/ise-software)

CISCO *Live!*



[cs.co/ise-eol](https://cs.co/ise-eol)



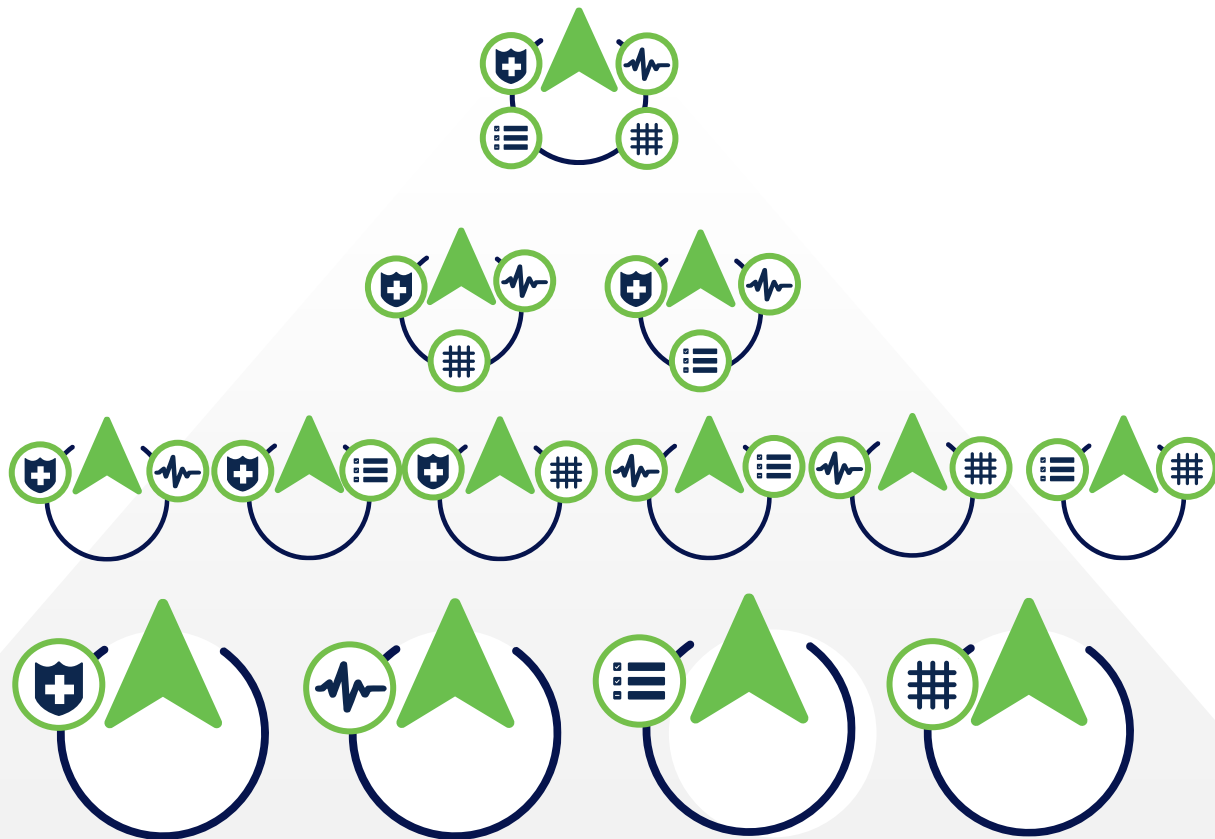
[cs.co/ise-rn](https://cs.co/ise-rn)

# *Cisco ISE Best Practices*

## Performance and Scale Considerations

# Shared vs Dedicated ISE Persona

Shared



Dedicated

CISCO *Live!*

# Shared vs Dedicated ISE PSN



Performance increases if dedicated

# Steady State versus Peak Demand

- You have a mix of **Static** Endpoints and **Mobile** Endpoints
- Some Endpoints are always on with long (8+ hours) session expirations
- Mobile endpoints **hibernate & roam causing a 3-10X+ larger load**
- **Misconfigured devices** can have **100-1000X larger than average auth load**

# *Cisco ISE Best Practices*

3<sup>rd</sup> Party NADs

# ISE Compatibility



RFC2865 : RADIUS  
RFC2866 : Accounting  
RFC3579 : EAP Support  
RFC5176 : CoA Support

Cisco ISE supports protocol standards like RADIUS, its associated RFC Standards, and TACACS+. For more information, see the [ISE Community Resources](#).

Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior for standards-based authentication.

Cisco ISE interoperates fully with third-party TACACS+ client devices that adhere to the governing protocols. Support for TACACS+ functions depends on the device-specific implementation.



[cs.co/ise-compatibility](https://cs.co/ise-compatibility)

Products and Services Solutions Support Learn Partners Explore Cisco Search

Support / Product Support / Security / Cisco Identity Services Engine / Compatibility Information

## Cisco Identity Services Engine Network Component Compatibility

Updated: August 11, 2021

Download Print

### Contents

#### Overview

- Supported Protocol Standards, RFCs, and IETF Drafts
- AAA Attributes for RADIUS Proxy Service
- AAA Attributes for Third-Party VPN Concentrators
- System Requirements
- Supported Hardware
- Supported Virtual Environments
- Federal Information Processing Standard Mode Support
- Validated Browsers
- Validated External Identity Sources
- Supported Unified Endpoint Management and Mobile Device Management Servers
- Supported Antivirus and Antimalware Products
- Supported Ciphers
- Validated OpenSSL Version
- Validated Client Machine Operating Systems, Suppliants, and Agents
- Google Android
- Apple iOS
- Apple macOS
- Microsoft Windows
- Google Chromebook
- Validated Operating Systems and Browsers for Sponsor, Guest, and My Devices Portals
- Validated Devices for On-Boarding and Certificate Provisioning
- Validated Cisco Digital Network Architecture Center Release
- Validated Cisco Prime Infrastructure Release
- Validated Cisco Firepower Management Center Release
- Validated Cisco Stealthwatch Management Release
- Validated Cisco WAN Service Administrator Release
- Support for Threat Centric NAC

#### Overview

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

**Note**

Cisco ISE supports protocol standards like RADIUS, its associated RFC Standards, and TACACS+. For more information, see the [ISE Community Resources](#).

Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior for standards-based authentication.

Cisco ISE interoperates fully with third-party TACACS+ client devices that adhere to the governing protocols. Support for TACACS+ functions depends on the device-specific implementation.



# *Cisco ISE Best Practices*

## Policies

# Policies

- Provide **Deny Access to unknown** endpoints in closed environment
- Provide **highest privileges based on Granular policies**
- Provide **least privileges for general access**

# *Cisco ISE Best Practices*

Operations

# Optimization

## Suppress Successful Reports

















Suppress repeated successful authentications 



Enable to Suppress Repeated AAA Records

 [Reset Repeat Counts](#) [Export To](#) 

Time	Status	Details	Identity	Repeat Count	Authentication Pr...
×			▼ Identity		Authentication Protocc
Apr 24, 2023 01:55:20.4...			azureuser@iseiscool.onmicro...	14	EAP-TLS
Apr 24, 2023 01:32:41.0...			14:16:9D:86:D7:3E	13	Lookup
Apr 24, 2023 01:31:52.0...			00:50:56:8E:85:F0	13	Lookup
Apr 24, 2023 01:31:50.6...			00:50:56:8E:70:06	13	Lookup
Apr 24, 2023 01:31:47.5...			00:50:56:8E:C1:38	13	Lookup
Apr 24, 2023 01:31:42.0...			00:50:56:8E:6A:67	13	Lookup
Apr 24, 2023 01:31:41.9...			00:50:56:8E:A9:F6 BRKSEC-2091	13	Lookup

# Optimization

- Enable to Identify Misconfigured Supplicants
- Enable to Suppress Repeated Failed Endpoints

- Rejects Repeated Failed Endpoints

Live Logs   Live Sessions

---

Misconfigured Supplicants ⓘ

1

Rejected Endpoints ⓘ

1

Cisco ISE Work Centers · Network Access

Overview Identities Id Groups Ext Id Sources Network Resources Policy Elements Policy

Client Provisioning

Protocols

EAP-FAST

EAP TLS

PEAP

RADIUS

Collection Filters

Proxy Settings

## RADIUS Settings

Suppression & Reports UDP Ports DTLS

### Suppress Repeated Failed Clients

☒ Suppress Repeated Failed Clients ⓘ

Detect two failures within 5 Minutes ⓘ

Report failures once every 15 minutes (15-60) ⓘ

☒ Reject RADIUS requests from clients with repeated failures ⓘ

Failures prior to automatic rejection 5 (2-100) ⓘ

Continue rejecting requests for 60 minutes (5-180) ⓘ

Ignore repeated accounting updates within 5 seconds (1 - 86,400) ⓘ

### Suppress Successful Reports

☒ Suppress repeated successful authentications ⓘ

# Schedule Your Backup Regularly

☰ Cisco ISE

Administration · System

Evaluation Mode 85 Days 🔔 🔍 ⓘ 🖨 ⚙

DeploymentLicensingCertificatesLoggingMaintenanceUpgradeHealth ChecksBackup & RestoreMore ▾

Backup & Restore

Policy Export

Backup & Restore

Backup Now ⓘ

☒ Configuration Data Backup

☐ Operational Data Backup

Backup Now

Schedule Backup

		Frequency	Start End Date	Execute At	Schedule Status
Configuration Data Backup	Edit	MONTHLY	04/21/2023 - 04/30/2024	1:00 AM	<input checked="" type="checkbox"/>
Operational Data Backup	Edit	MONTHLY	04/21/2023 - 04/25/2024	4:00 AM	<input checked="" type="checkbox"/>

# Operational Data Purging

- By **default**, Data Retention Period is **30 Days**
- Adjust with caution based on the Disk Space availability
- **Export to external Repositories** for your old data before it gets purged.

The screenshot displays the Cisco ISE Administration console interface. The top navigation bar includes 'Cisco ISE' and 'Administration · System'. Below this, a secondary navigation bar contains tabs for 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance' (which is selected), 'Upgrade', 'Health Checks', and 'Backup & Restore'. On the left side, a sidebar menu lists 'Patch Management', 'Repository', 'Operational Data Purging' (which is selected), and 'Localdisk Management'. The main content area is titled 'Database Utilization' and shows a database icon with the text '310 GB Total DB Space'. Below this, there are two rows of data for 'isenode23.dominion.in' and 'isenode24.dominion.in', each with a progress bar. The 'Operational Data Purging' section is highlighted with a dashed blue border and contains a 'Data Retention Period' table with columns for 'RADIUS', 'TACACS', and 'Days'. The table shows '30' days for both. Below the table are 'Save' and 'Reset' buttons. To the right of the retention period settings is a 'Repository' section with a checkbox for 'Enable Export Repository', a dropdown for 'Select a Repository', a 'Create Repository' link, and an 'Encryption Key' field.

Database Utilization		
isenode23.dominion.in		
isenode24.dominion.in		

Data Retention Period		
RADIUS	30	Days
TACACS	30	Days

Repository

☐ Enable Export Repository

Select a Repository

Create Repository

Encryption Key

# RADIUS Logs Data Retention



**Cisco ISE** Administration • System

Deployment Licensing Certificates Logging **Maintenance** Upgrade Health Checks Backup & Restore

Patch Management  
Repository  
Operational Data Purging  
Localdisk Management

## Database Utilization

310 GB Total DB Space

isenode23.dominion.in [ ]  
isenode24.dominion.in [ ]

**Data Retention Period**

RADIUS 30 Days  
TACACS 30 Days

**Repository**

☐ Enable Export Repository

Select a Repository

Create Repository

Encryption Key

Reset

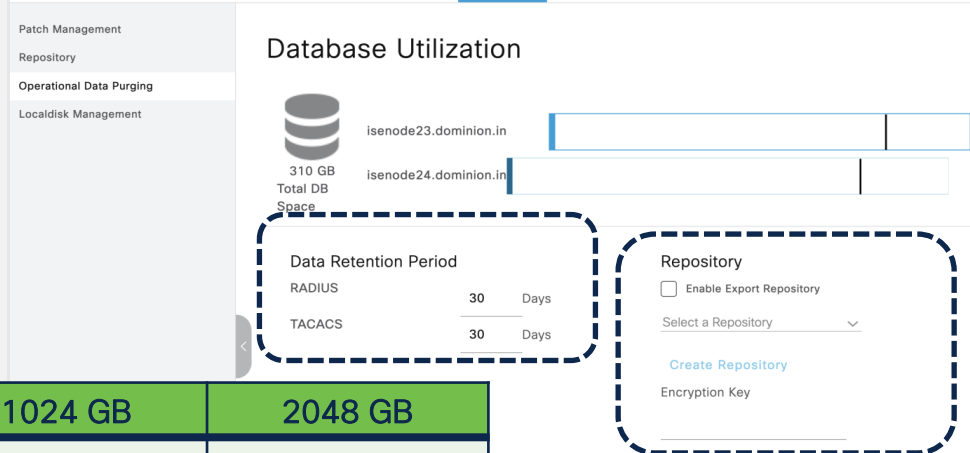
No. of Endpoints	300 GB	600 GB	1024 GB	2048 GB
5,000	504	1510	2577	5154
10,000	252	755	1289	2577
25,000	101	302	516	1031
50,000	51	151	258	516
100,000	26	76	129	258
150,000	17	51	86	172
200,000	13	38	65	129
250,000	11	31	52	104
500,000	6	16	26	52

ISE 3.2

\*The numbers are based on the following assumptions: Ten or more authentications per day per endpoint with logging suppression enabled.



# TACACS Logs Data Retention



No. of Authc	300 GB	600 GB	1024 GB	2048 GB
100	12,583	37,749	64,425	128,850
500	2,517	7,550	12,885	25,770
1,000	1,259	3,775	6,443	12,885
5,000	252	755	1,289	2,577
10,000	126	378	645	1,289
25,000	51	151	258	516
50,000	26	76	129	258
75,000	17	51	86	172
100,000	13	38	65	129

ISE 3.2

\*Assumption: The script runs against all NADs, 4 sessions per day, and 5 commands per session.

# Endpoint Purge Policies

Configure Policies that **you don't want to purge** eg., BYOD

Configure Policies that **you want to purge** eg., Guest, Inactive Endpoints

**Schedule** the Purge Policies

## Endpoint Purge

Define the EndPoint Purge Policy by configuration rules based on identity groups and/or other conditions. Drag and drop rules to the list below. The first matched rule applies.

### Never Purge

Status	Rule Name	Conditions (identity groups and/or other conditions)	
<input type="checkbox"/>	EnrolledRule	if DeviceRegistrationStatus Equals Registered	<a href="#">Edit</a> <span>▼</span>

### Purge

Status	Rule Name	Conditions (identity groups and/or other conditions)	
<input checked="" type="checkbox"/>	GuestEndpointsPurgeRule	if GuestEndpoints AND ElapsedDays Greater than 30	<a href="#">Edit</a> <span>▼</span>
<input checked="" type="checkbox"/>	RegisteredEndpointsPurgeRule	if RegisteredDevices AND ElapsedDays Greater than 30	<a href="#">Edit</a> <span>▼</span>

### Schedule

Purge endpoints from the identity table at a specific time

Schedule : Every

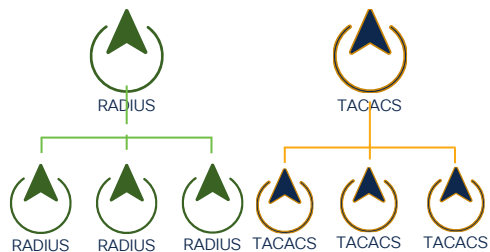
Everyday ▼

at 03 ▼ 00 ▼

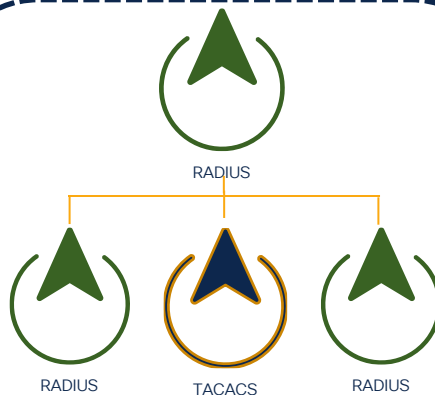
# *Cisco ISE Best Practices*

Device Administration – RADIUS & TACACS

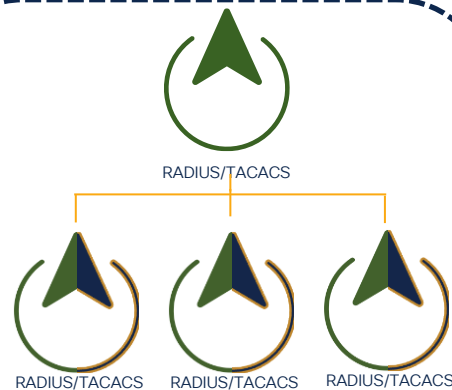
# RADIUS & TACACS Deployment Options



Separate ISE  
Cubes for RADIUS  
& TACACS

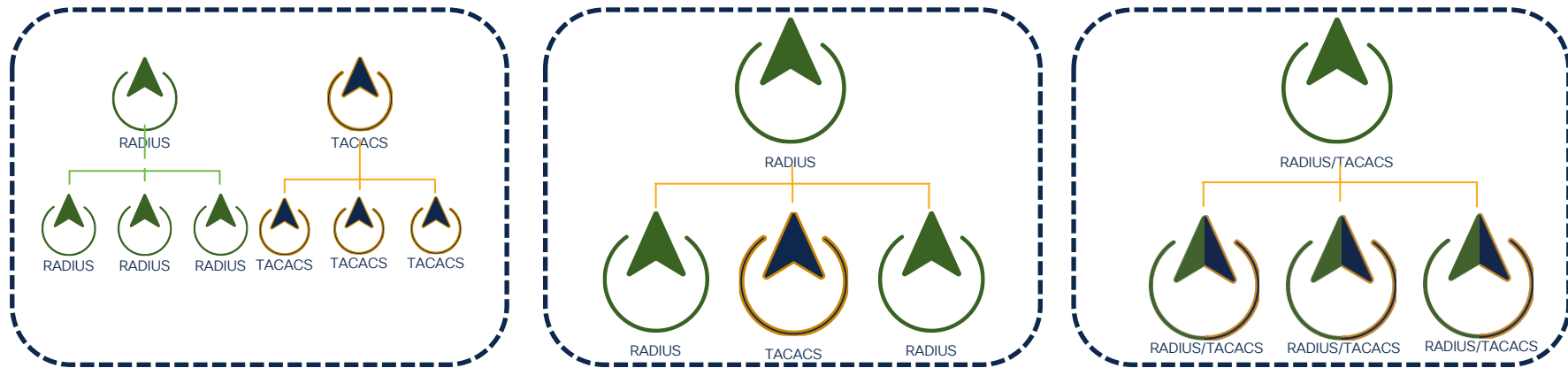


Mixed ISE Cube  
with separate  
PSNs for RADIUS  
and TACACS+



Mixed ISE Cube  
where PSNs are  
not dedicated to  
either

# When do we separate TACACS+ and RADIUS?



1. How many network devices?
2. Number of TACACS+ & RADIUS sessions
3. Scripts?
4. Network Management Tools
5. Increased log retention on both Deployments
6. Per-PSN utilization and load



What features would you like to see in ISE future releases?



Join at [slido.com](https://slido.com)

#BRKSEC-2091

# Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



**These points** help you get on the leaderboard and increase your chances of winning daily and grand prizes

# Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



# References

- ISE YouTube Channel  
[cs.co/ise-videos](https://www.cisco.com/go/ise-videos)
- ISE Resources  
[cs.co/ise-resources](https://www.cisco.com/go/ise-resources)
- ISE Webinars  
[cs.co/ise-webinars](https://www.cisco.com/go/ise-webinars)
- ISE Community  
[cs.co/ise-community](https://www.cisco.com/go/ise-community)
- ISE Integration Guides  
[cs.co/ise-guides](https://www.cisco.com/go/ise-guides)
- Network Access Device Capabilities  
[cs.co/nad-capabilities](https://www.cisco.com/go/nad-capabilities)
- ISE
- ISE Licensing & Evaluations  
[cs.co/ise-licensing](https://www.cisco.com/go/ise-licensing)

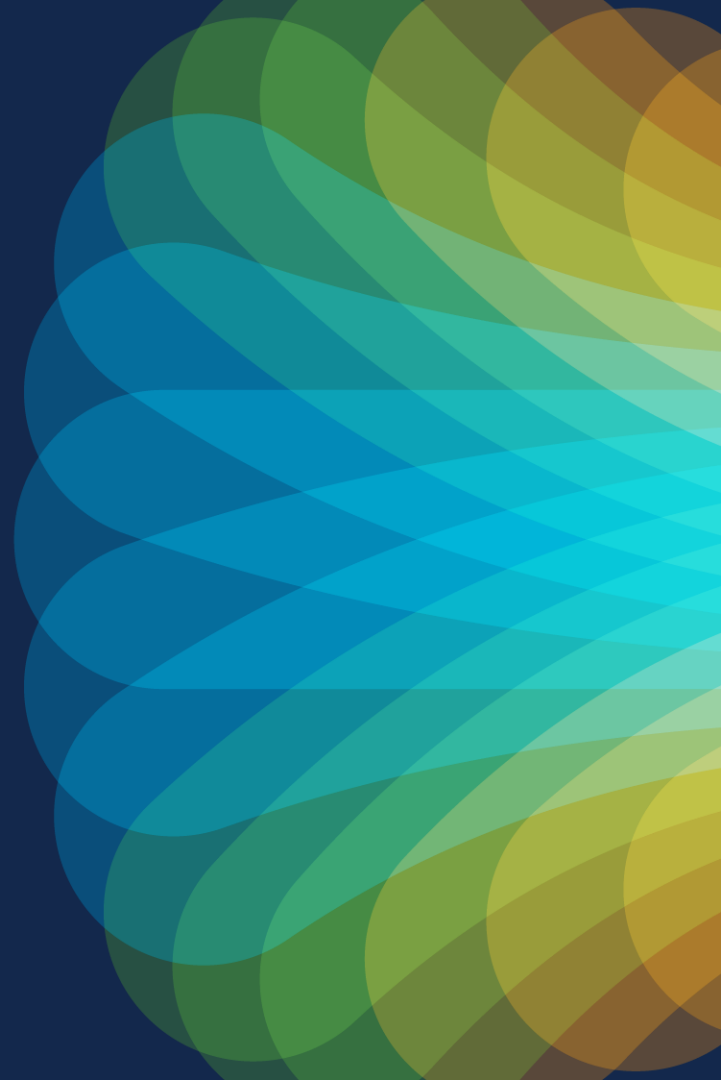


The bridge to possible

# Thank you



#CiscoLive

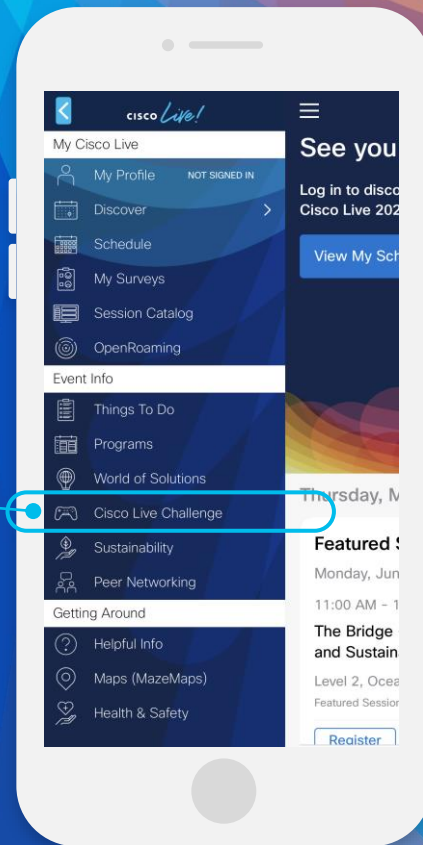
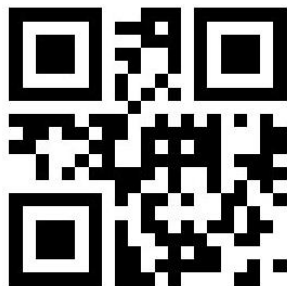


# Cisco Live Challenge

Gamify your Cisco Live experience!  
Get points for attending this session!

## How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive