
cisco Live!
Let's go
#CiscoLiveAPJC

The bridge to possible

ISE Deployment Staging and Planning

Thomas Howard, Technical Marketing Engineer (TME)
thomas@cisco.com
BRKSEC-2705

Cisco Live!

“Reconciliation” - Dustin Koa Art

cisco

Cisco Webex App

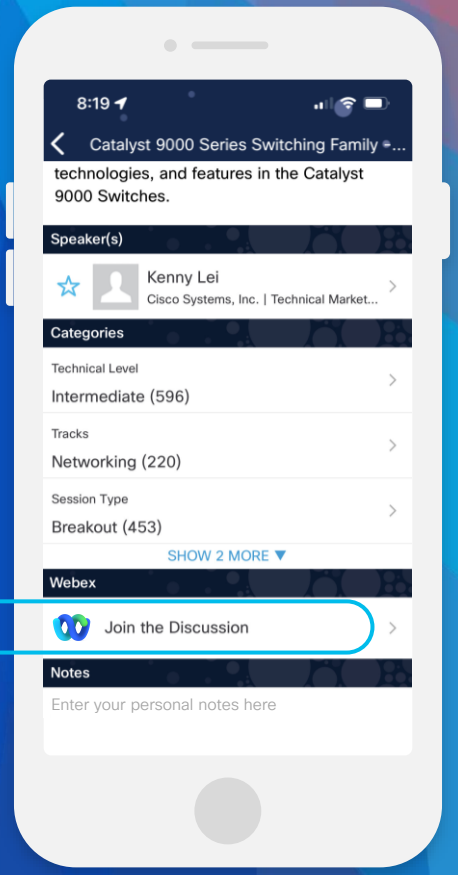
Questions?

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

How

1. Find this session 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 December 22, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2705

Agenda

- **Introduction**
- **Challenges**: Organizations, Endpoints, Network Devices, Policy
- **Planning**: Platforms, Sizing & Scale, Lab, Monitor => Enforced
- **Staging**: Nodes, Certificates, Patching, Policy
- **Operations**: Automation, Monitoring, Backups
- **Resources**

ISE Webinars

cs.co/ise-webinars

MAC Authentication Bypass (MAB)

youtu.be/OKPGBEMb0w4

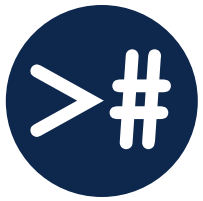
Getting Started with ISE Profiling

youtu.be/xoTwxlDux8Y

ISE Etern

ISE Deployment Challenges

Why Customers Buy ISE

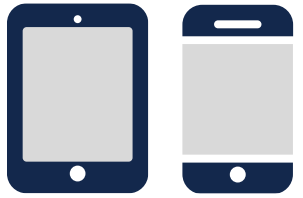


TACACS+ Migrating from Cisco Secure ACS or building a new Device Administration Policy Server, this allows for secure, identity-based access to the network devices

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

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

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.



Allow employees to Bring their Own Devices to access network resources by registering their device and downloading certificates for authentication through a simple onboarding process

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

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

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.

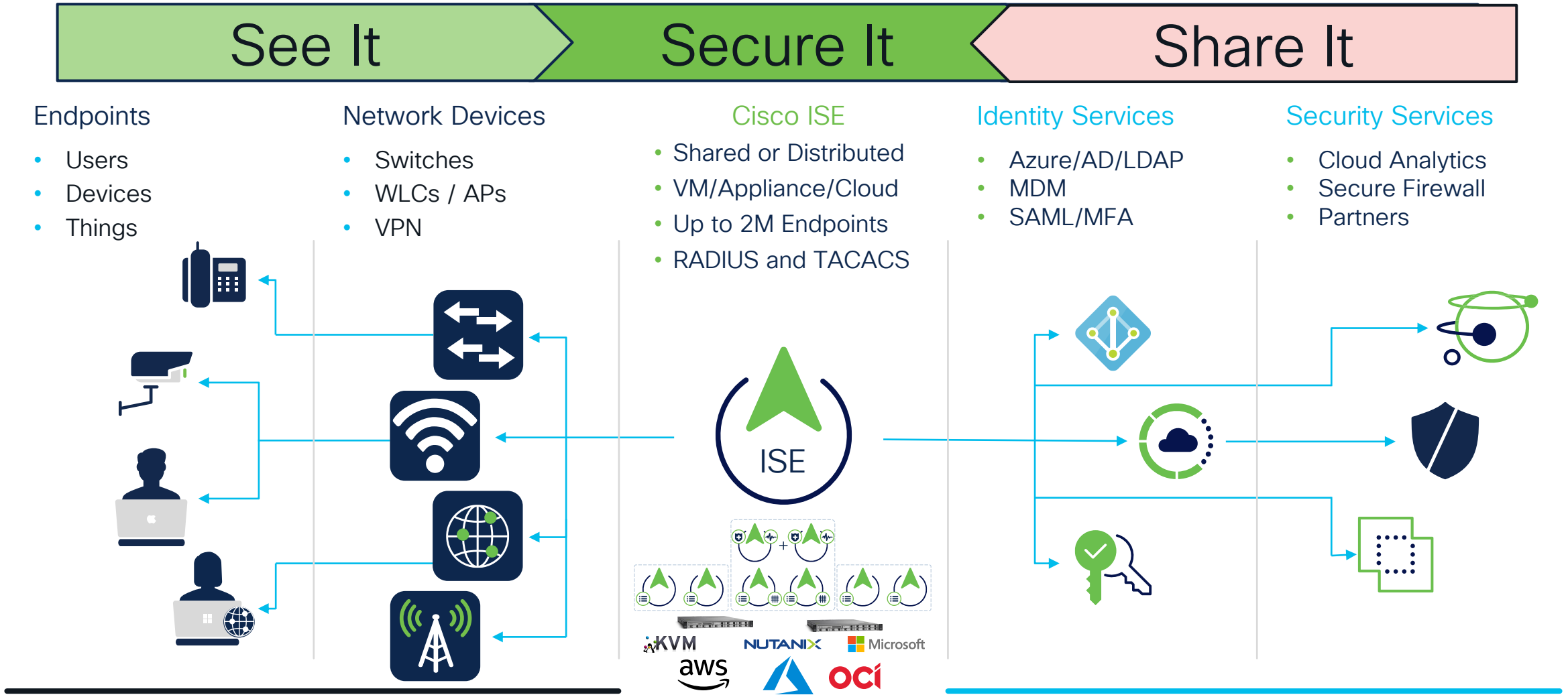
ISE integrates with DNA Center to automate the network fabric and enforces the policies throughout the entire network infrastructure using Software-Defined Access (SDA)

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

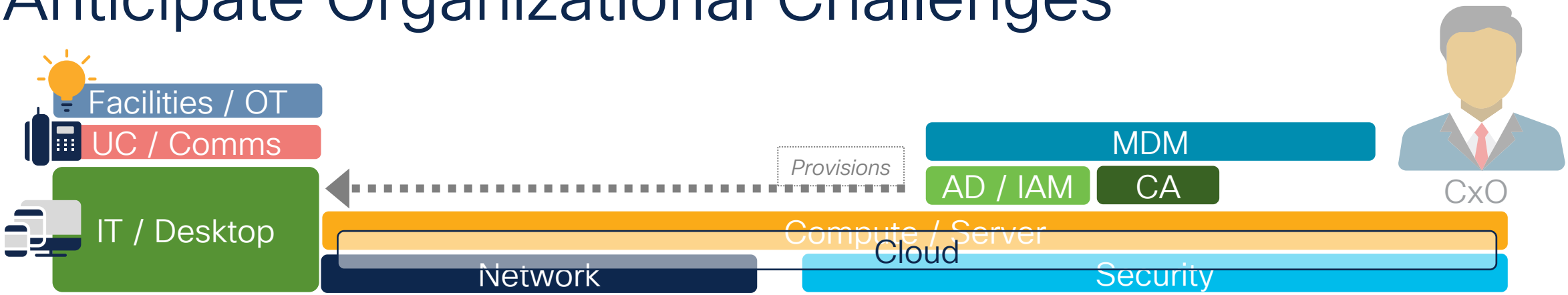
“ISE is complex.”

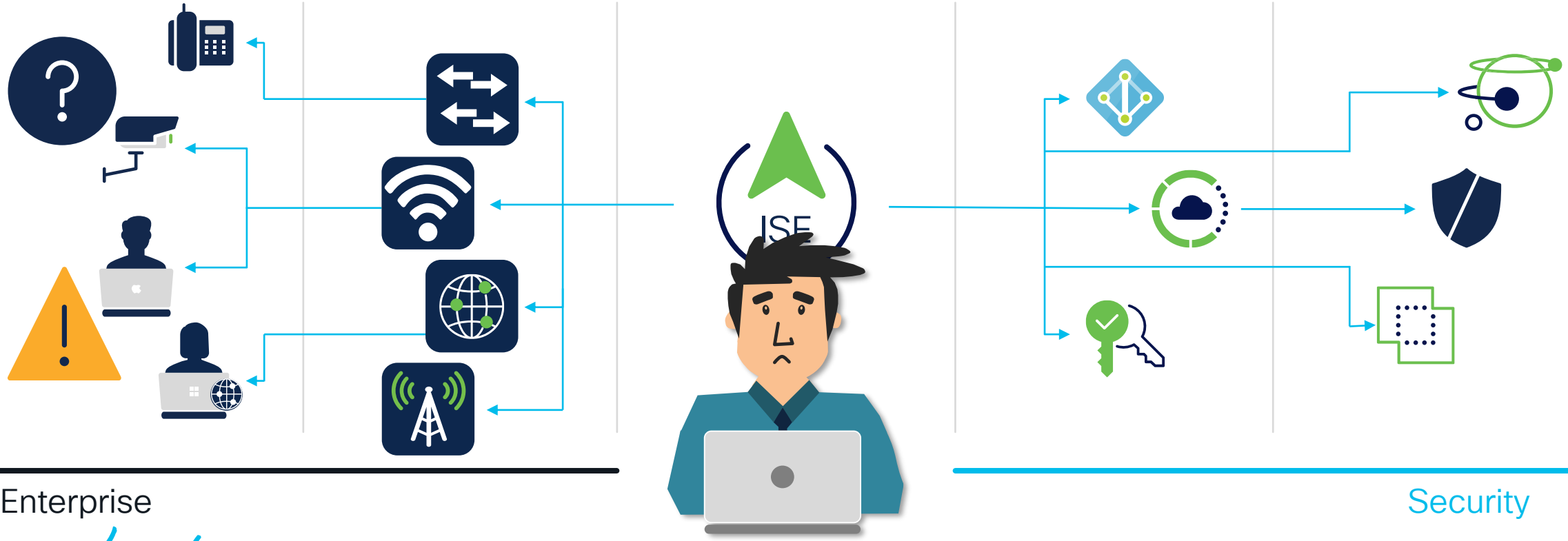
Every ISE Customer

ISE Provides Zero Trust for the Workplace



Anticipate Organizational Challenges





Enterprise

Security

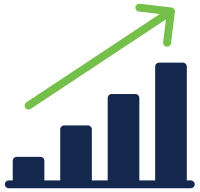
Understand Your Needs and Situation

Objectives / Risk / Priorities

- Brand Trust
- Customer/Patient Data
- Hospitality: Fast & Easy
- IT/OT Segmentation
- Protect Intellectual Property

Environment

- Wired / Wireless / VPN
- Multi-Vendor
- Hardware & Software
- Network Device Capabilities



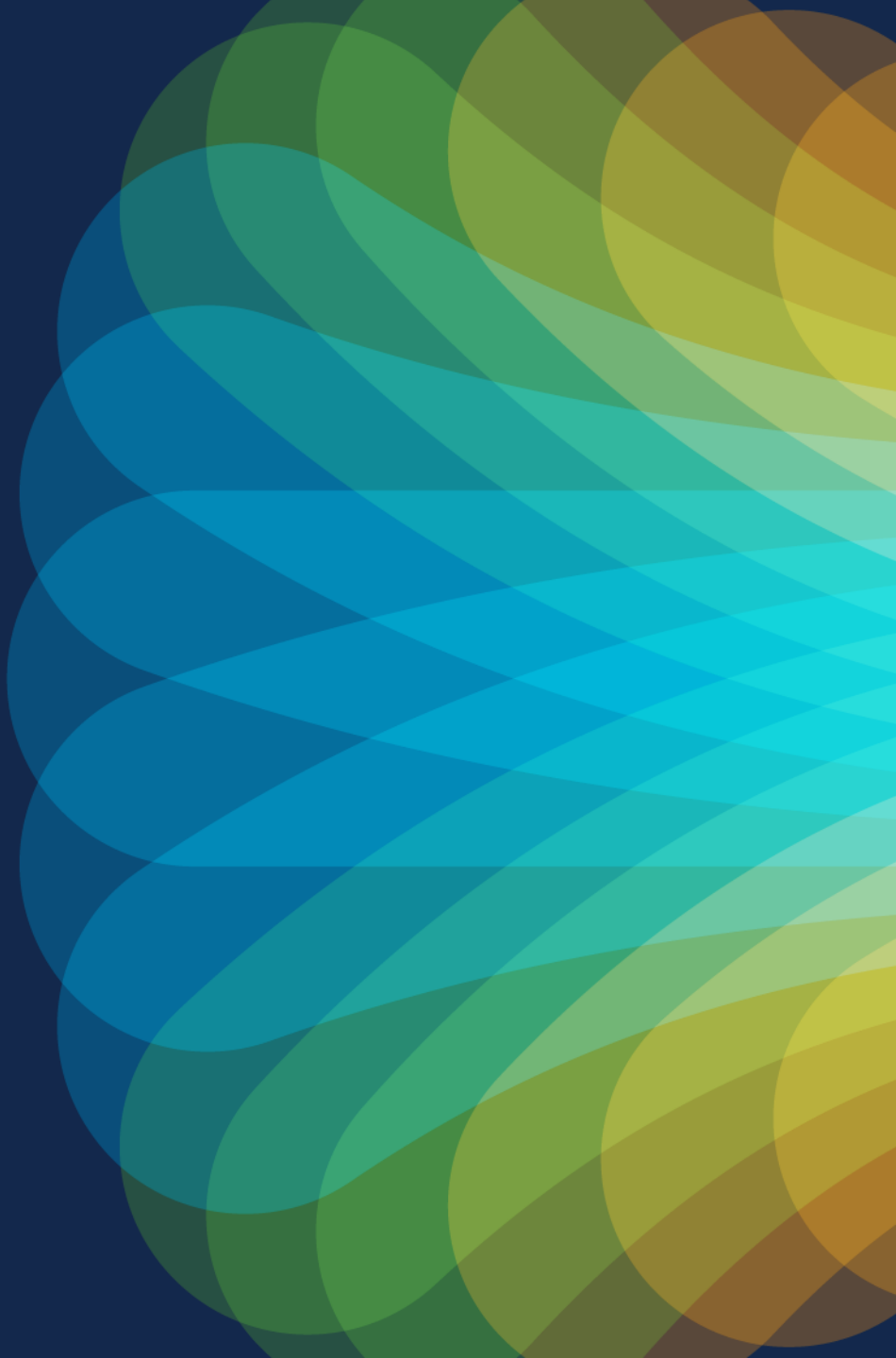
Scaling

- Concurrent Active Endpoints
- Network Devices
- Scale Horizontally (discovery)
- Scale Vertically (user+device)
- Geography

Management & Operations

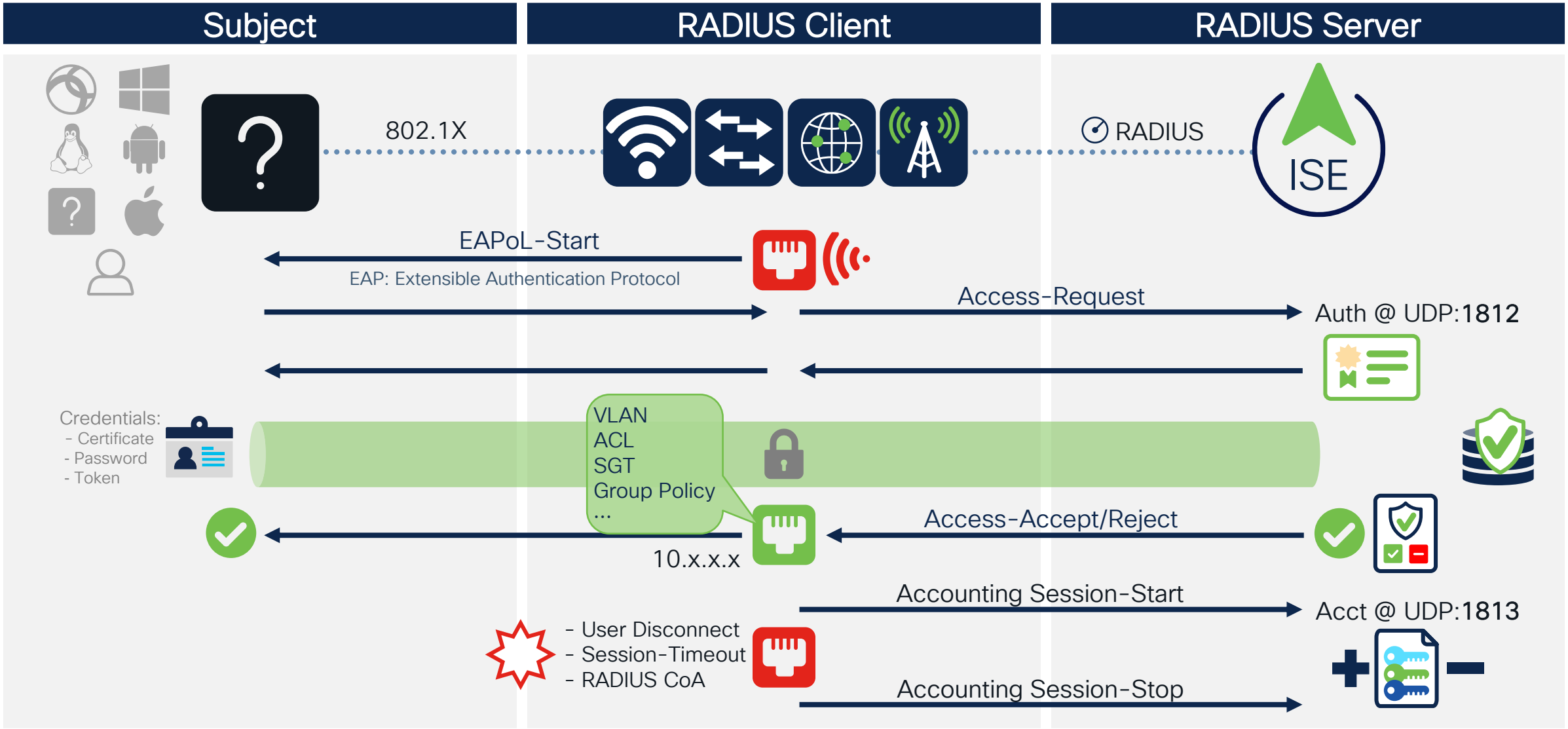
- Top Down / Bottom Up?
- Orgs / Regions / Departments
- Collaboration or Siloes
- Scheduling Config Changes
- Tooling & Automation

Challenges: Endpoints

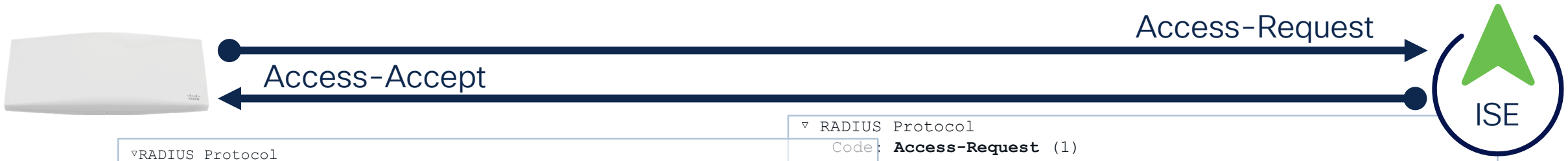


RADIUS : 802.1X

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



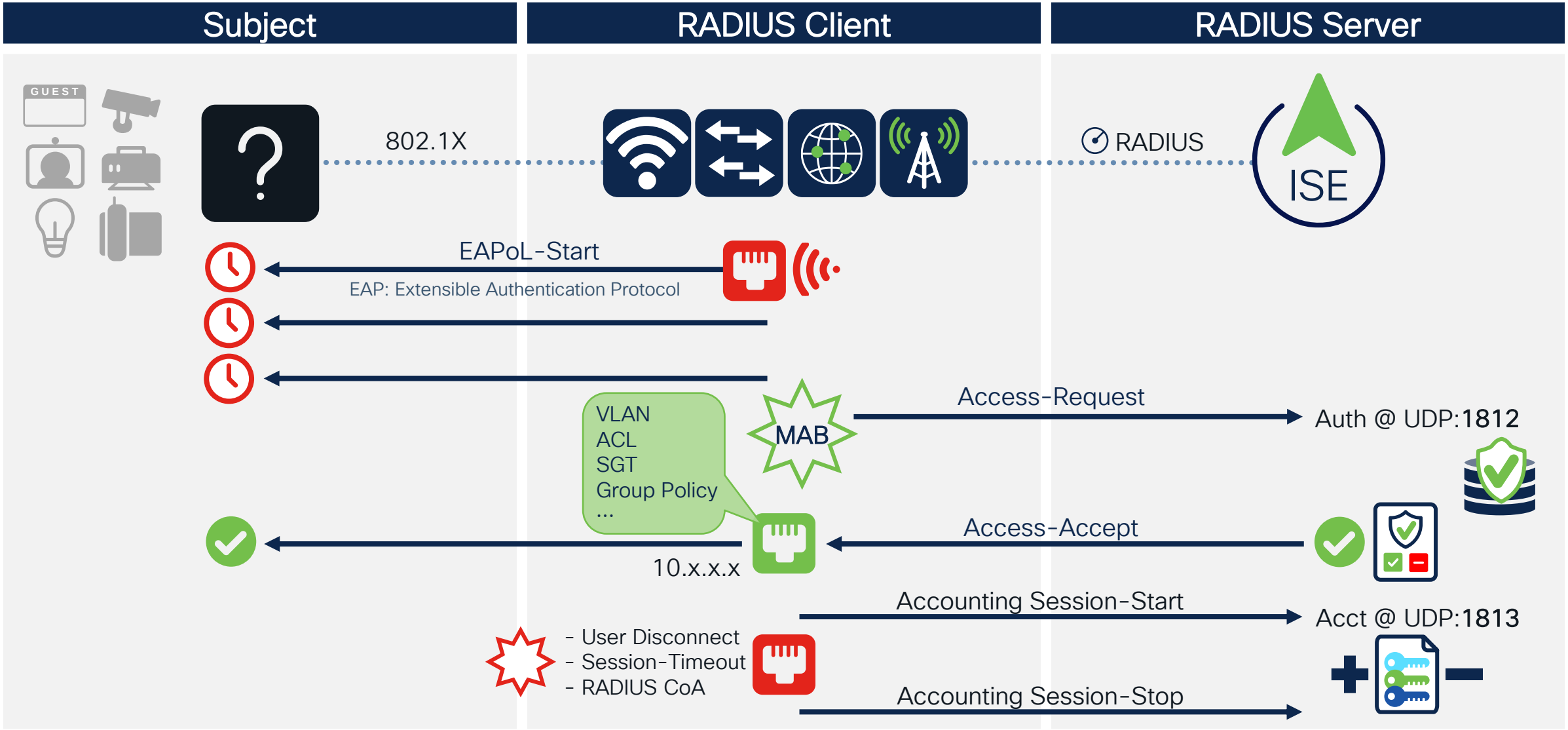
RADIUS : Access-Request + Access-Accept



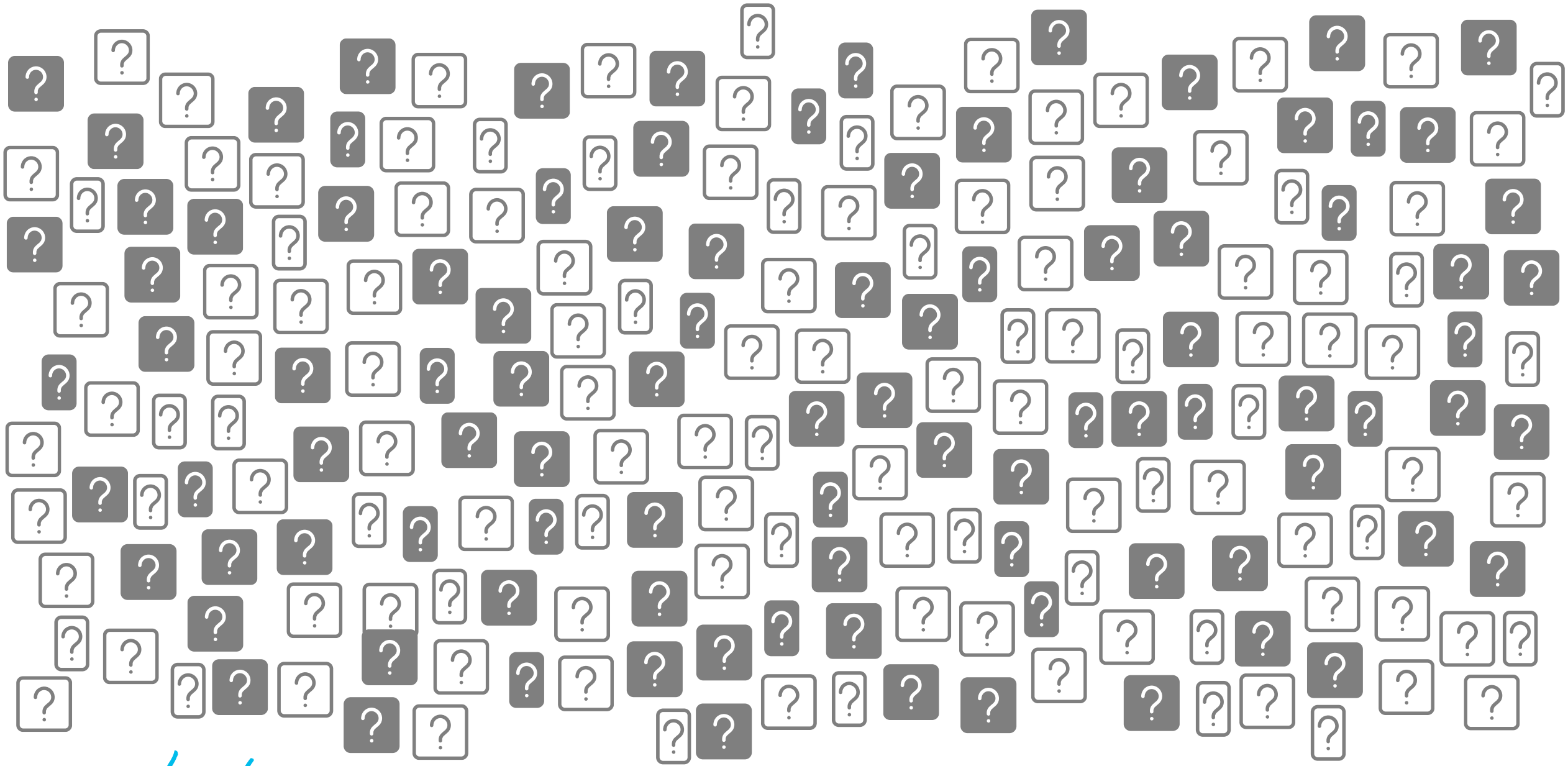

```
▿RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: Oxd (13)
  Length: 428
  Authenticator: 66403608336c3e77859116d46cd0d65f
 ▿Attribute Value Pairs
  › AVP: t=User-Name (1) l=8 val=thomas
  › AVP: =Class (25) l=75 val=434143533a6336313238353162724344a2f7767443633147…
  › AVP: t=Session-Timeout (27) l=6 val=1800
  › AVP: t=Termination-Action(29) (=6 val=RADIUS-Request(1)
  › AVP: t=Tunnel-Type (64) (=6 Tag=0x01 val=VLAN(13)
  › AVP: t=Tunnel-Medium-Type(65) l=6 Tag=0x01 val=IEEE-802(6)
  › AVP: t=EAP-Message (79) l=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) l=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) l=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)
     Type: 26
     Length: 38
     Vendor ID: ciscoSystems (9)
    › VSA: t=Cisco-AVPair(1) (=32 val=cts:security-group-taq=0004-00
  › AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft (311)
```

```
▿ RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: x0 (0)
    Length: 153
    Authenticator:29eb293b3a40ea740a8fd33bdb18f1d7
   ▿Attribute Value Pairs
    › AVP: t=User-Name (1) l=8 val=thomas
    › AVP: t=NAS-IP-Address(4) (=6 val=6.86.227.108
    › AVP: t=Calling-Station-Id(31) l=19 val=02-00-00-00-00-01
    › AVP: t=Called-Station-Id(30) l=27 val=2C-3F-0B-56-E3-6C: Corp
    › 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) l=6 val=Framed (2)
    › AVP: t=Connect-Info(77) (=24 val=CONNECT 11Mbps 802.11b
    › AVP: t=EAP-Message (79) l=13 Last Segment [1]
    › AVP: t=Message-Authenticator(80) l=18
val=26f047af6a9a82279dfd6d19b477c31b
```

RADIUS : MAC Authentication Bypass (MAB)

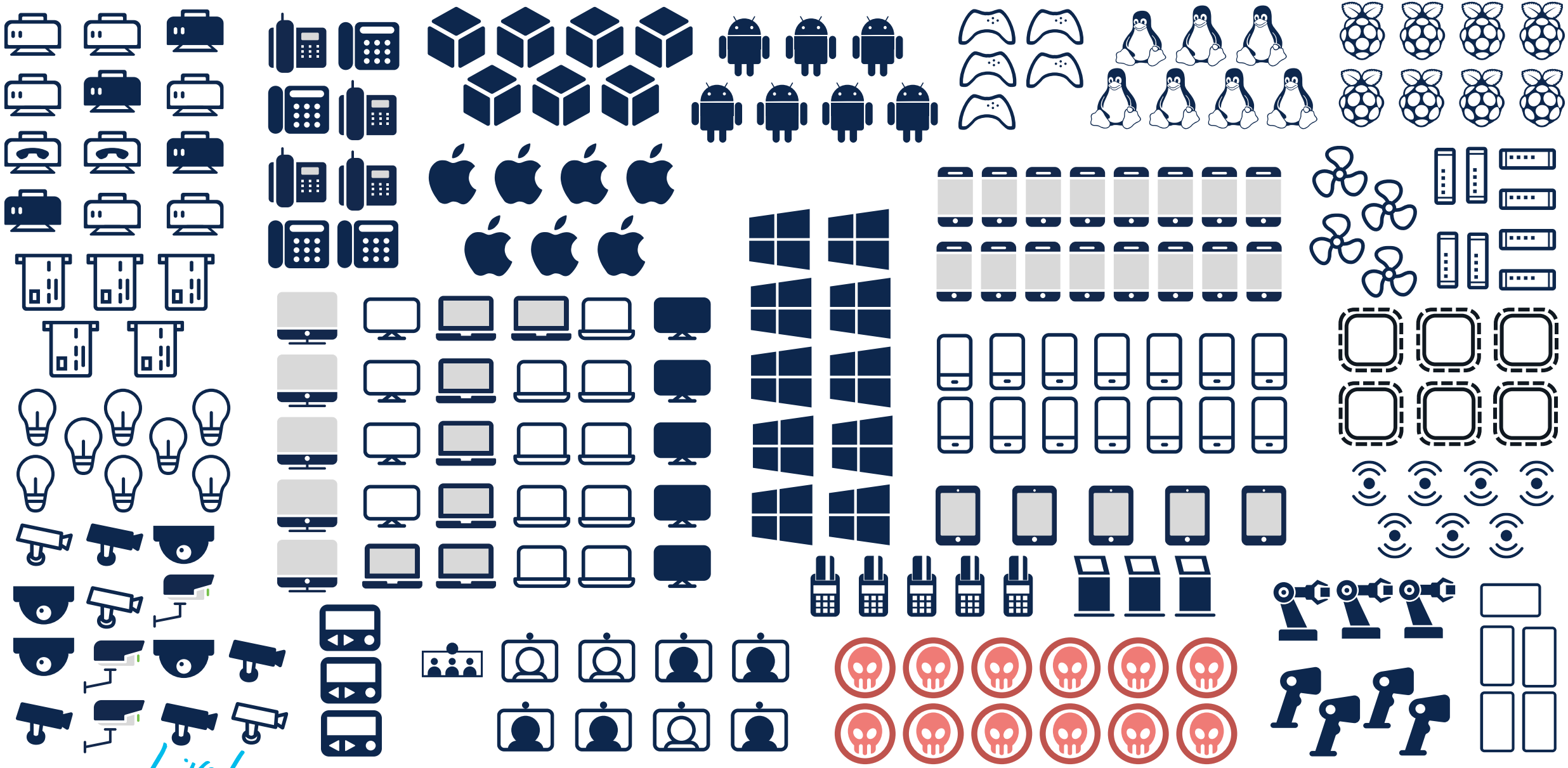


Unknowns



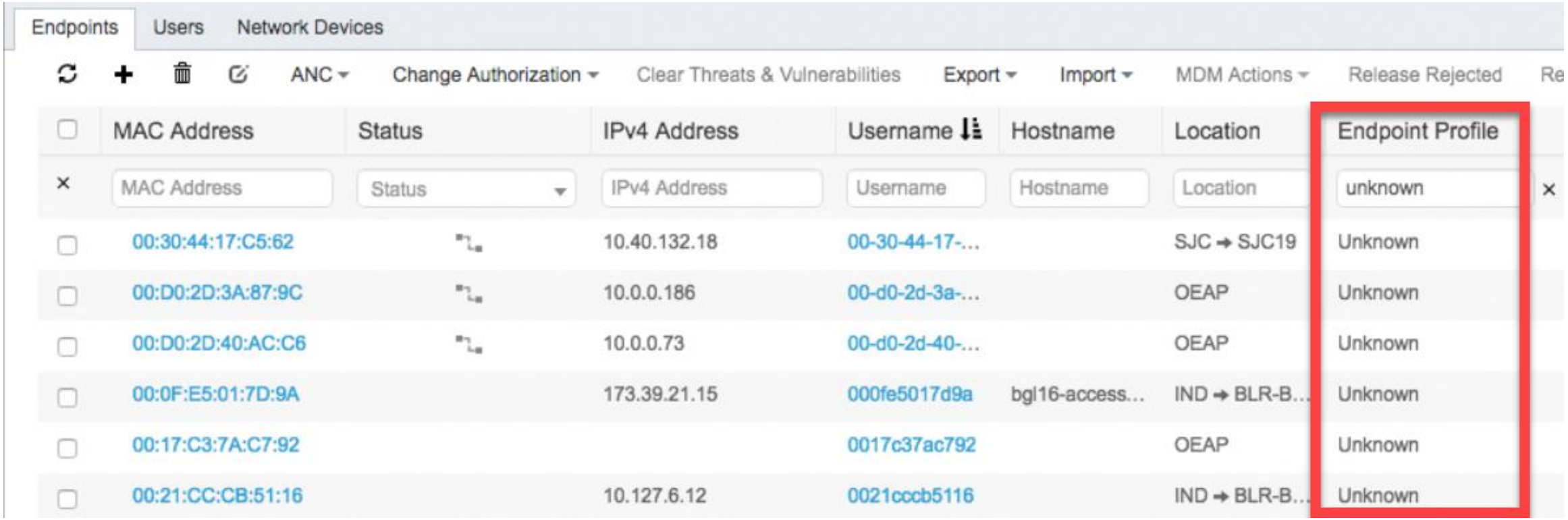
Unknowns... to Knowns

Unknowns... to Knowns... to Classified



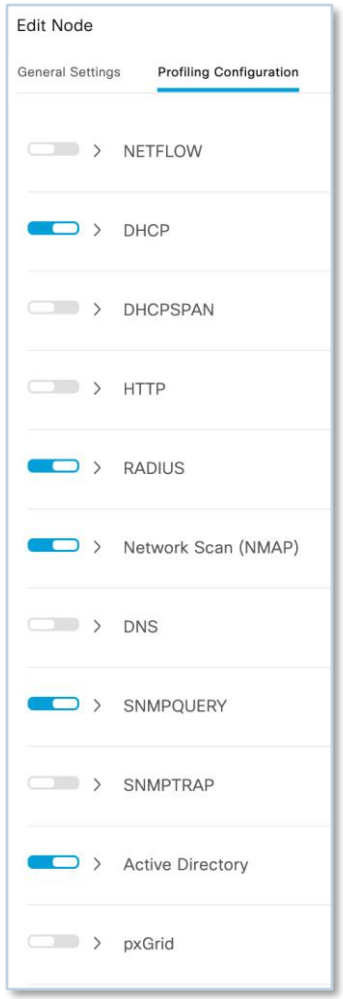
What about Unknowns?

- There will be endpoints that don't have pre-built profiles
- Endpoint profiles will show as "Unknown"
- View your unknown endpoints under Context Visibility>Endpoints

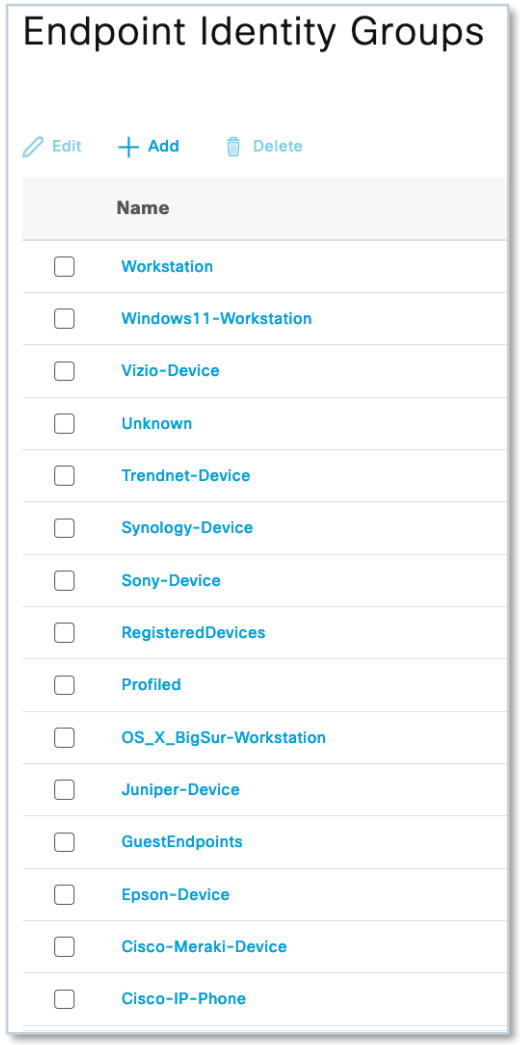


Classifying Endpoints without Authentication

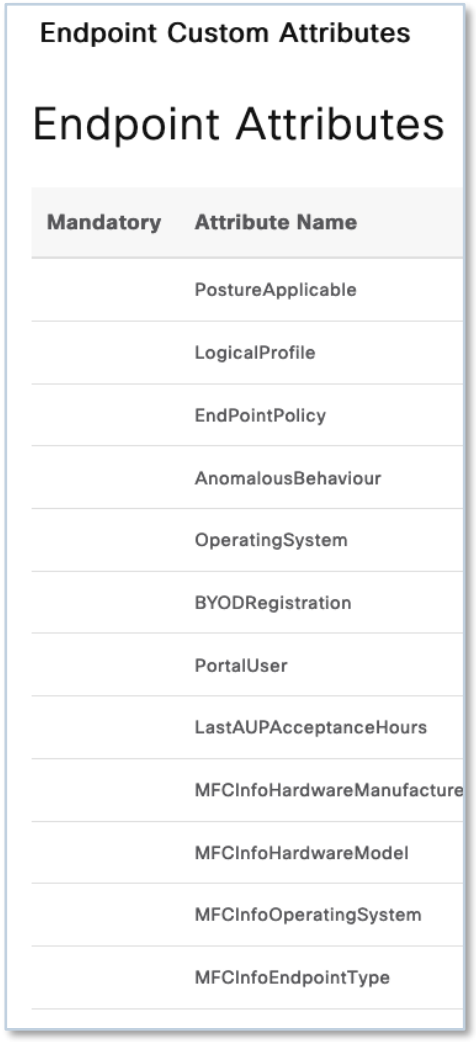
Profiling



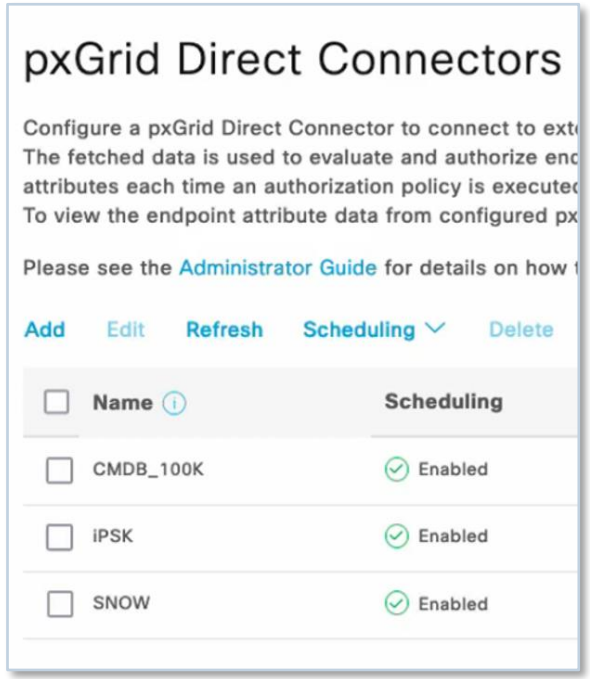
Static Groups



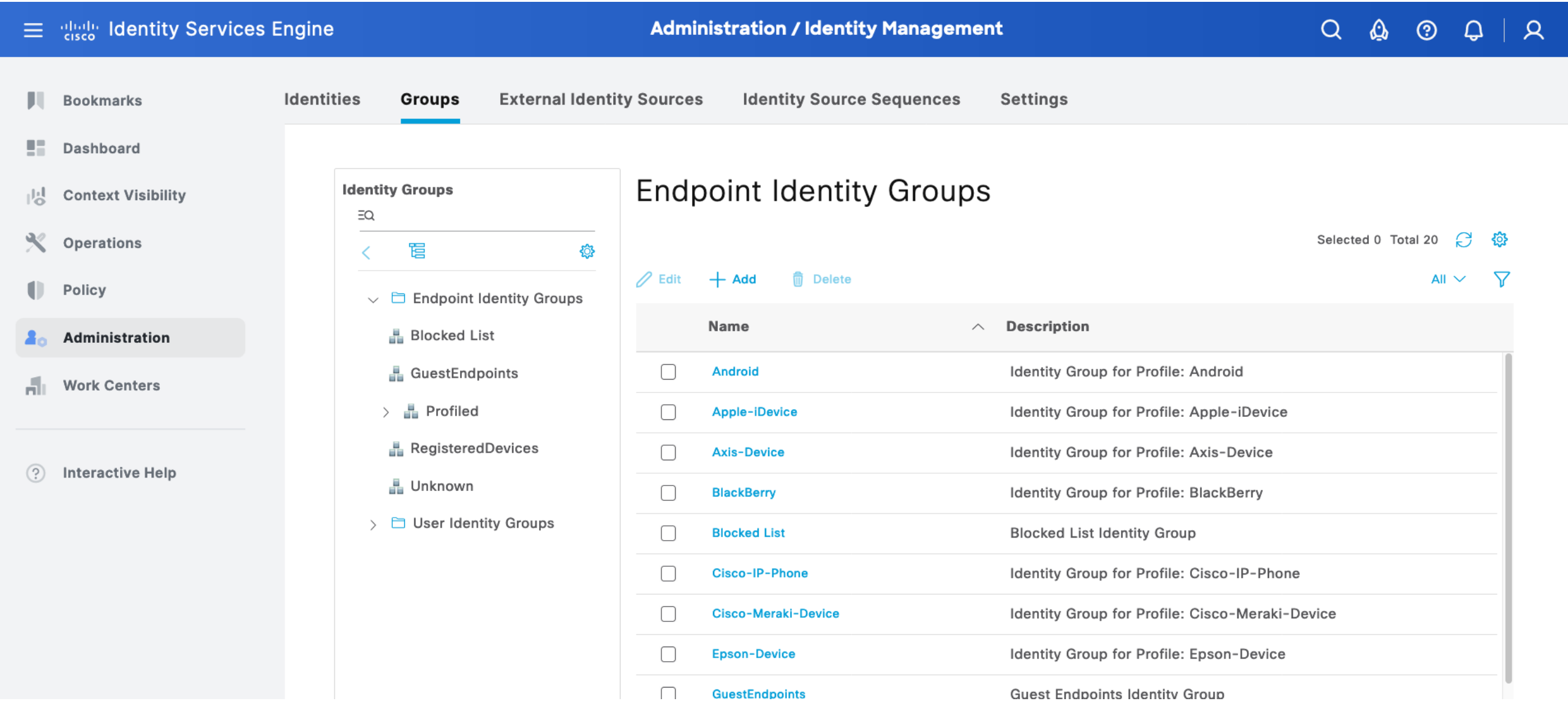
Custom Attributes



CMDBs



Static Endpoint Groups from MAC Inventories



Endpoint Custom Attributes

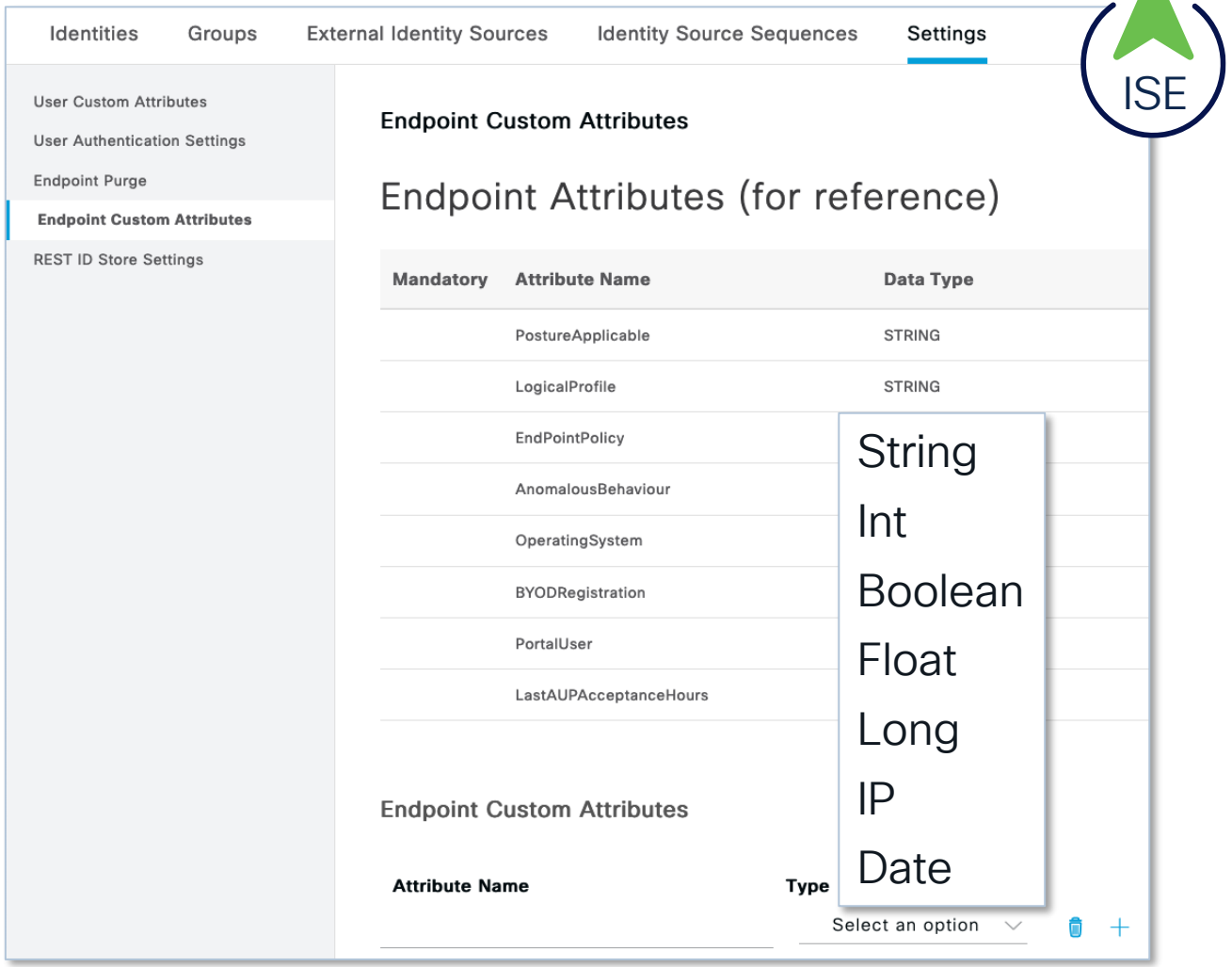
Administration > Identity Management > Settings > Endpoint Custom Attributes

cs.co/ise-api#endpoint

cs.co/ise-api#custom-attributes-openapi

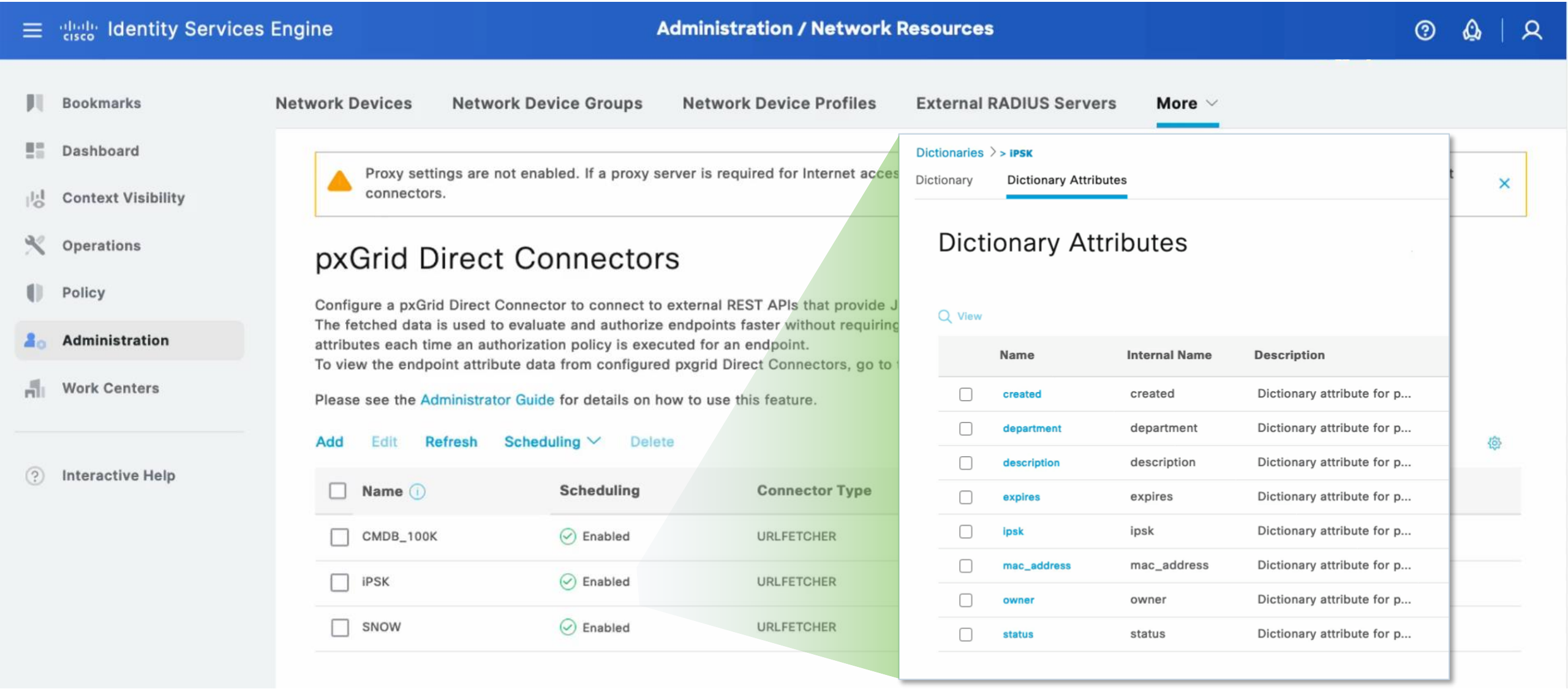
Examples

Attribute Name	Type
Created	Date
Expires	Date
Owner	String
Department	String
iPSK	String
Authorization	String
DeviceType	String
Manufacturer	String
Model	String
...	...

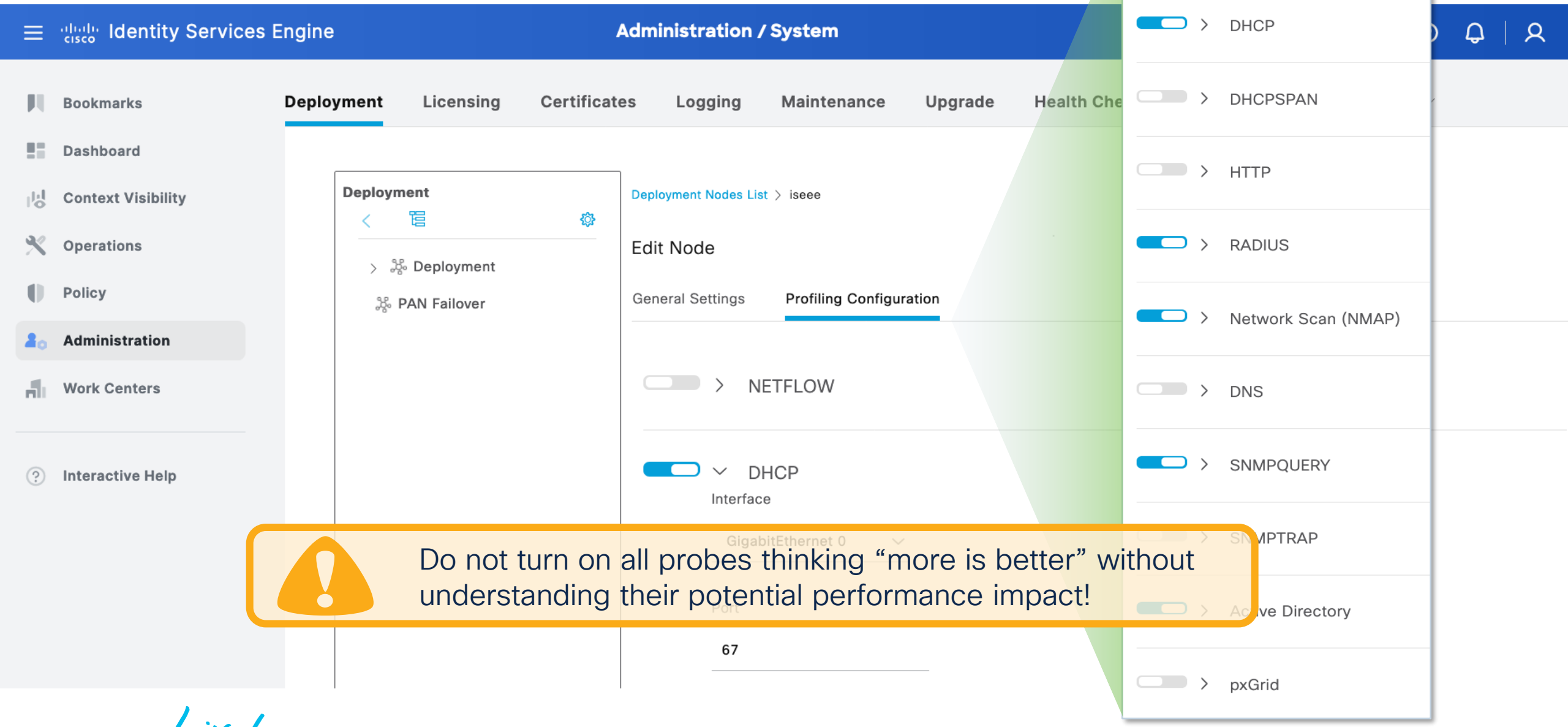


ISE pxGrid Direct with CMDBs

ISE 3.2P2 / 3.3

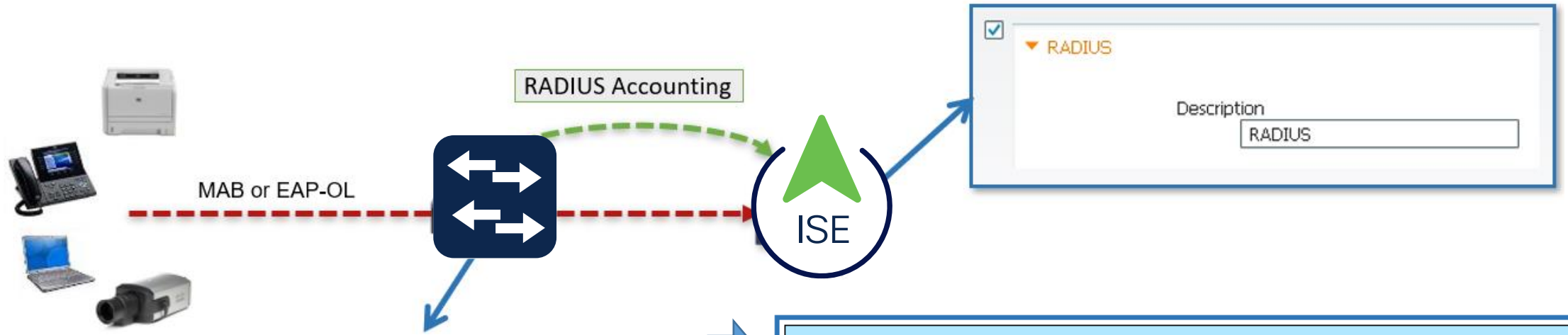


ISE Profiling Probes



Do not turn on all probes thinking “more is better” without understanding their potential performance impact!

Device Sensor for Wired



1) Filter DHCP, CDP, and LLDP options/TLVs

```
device-sensor filter-list cdp list my_cdp_list
 tlv name device-name
 tlv name platform-type
device-sensor filter-spec cdp include list my_cdp_list
```

```
device-sensor filter-list lldp list my_lldp_list
 tlv name system-name
 tlv name system-description
device-sensor filter-spec lldp include list my_lldp_list
```

```
device-sensor filter-list dhcp list my_dhcp_list
 option name host-name
 option name class-identifier
 option name client-identifier
device-sensor filter-spec dhcp include list my_dhcp_list
```

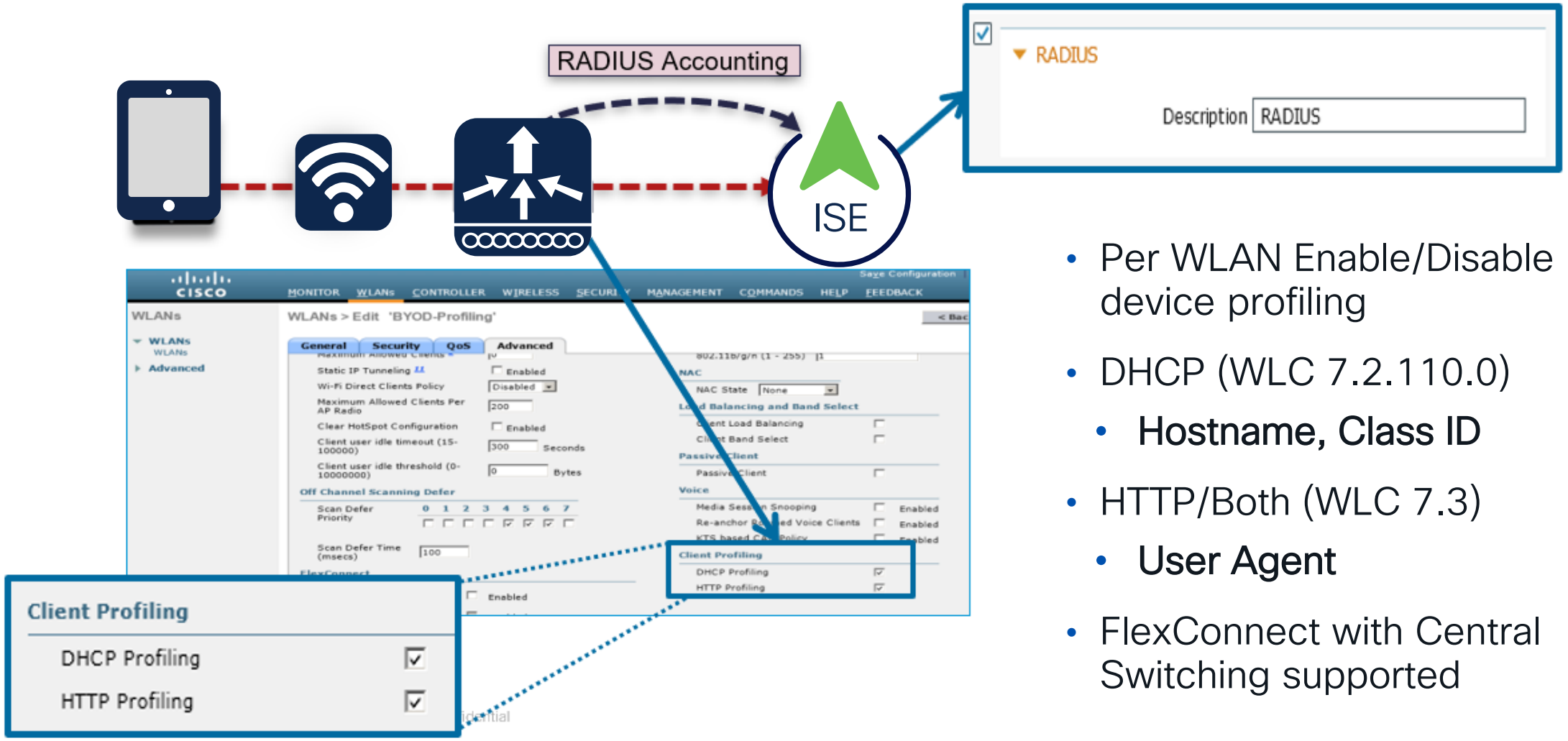
2) Enable sensor data to be sent in RADIUS Accounting including all changes

```
device-sensor accounting
device-sensor notify all-changes
```

3) Disable local analyzer if sending sensor updates to ISE (central analyzer)

```
no macro auto monitor
access-session template monitor
```

Wireless Device Sensor



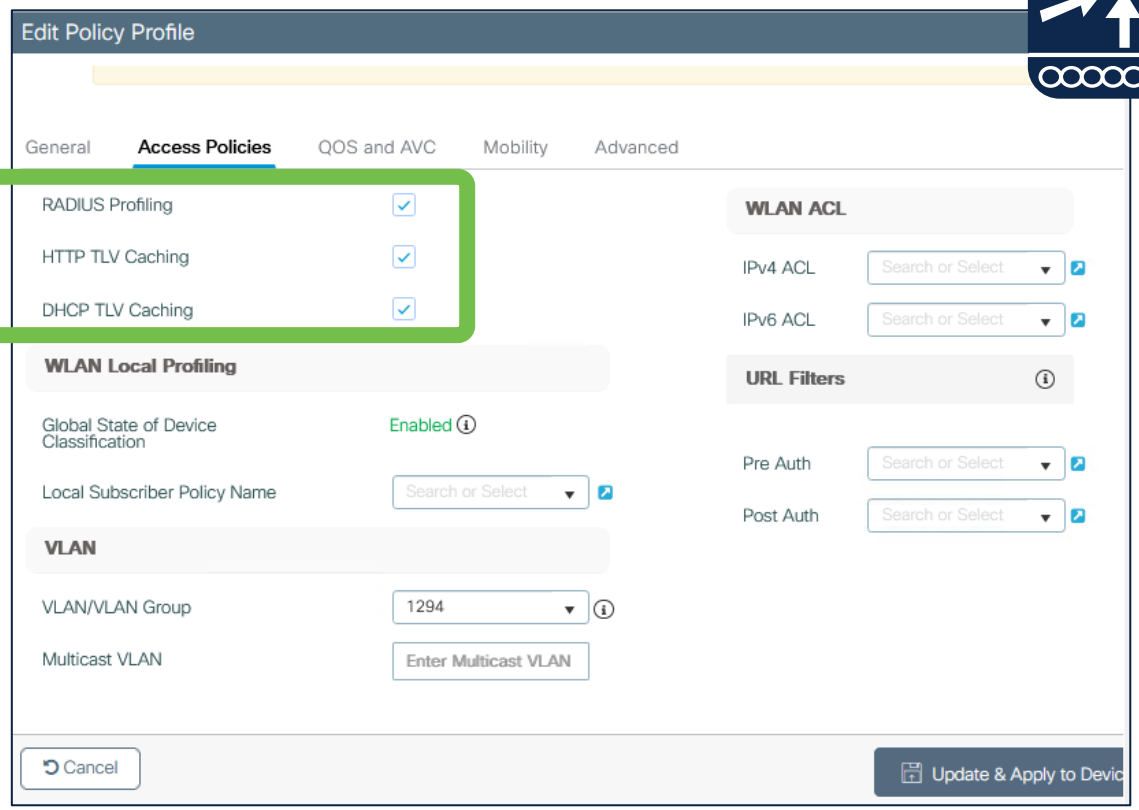
- Per WLAN Enable/Disable device profiling
- DHCP (WLC 7.2.110.0)
  - **Hostname, Class ID**
- HTTP/Both (WLC 7.3)
  - **User Agent**
- FlexConnect with Central Switching supported

WiFi Device Analytics

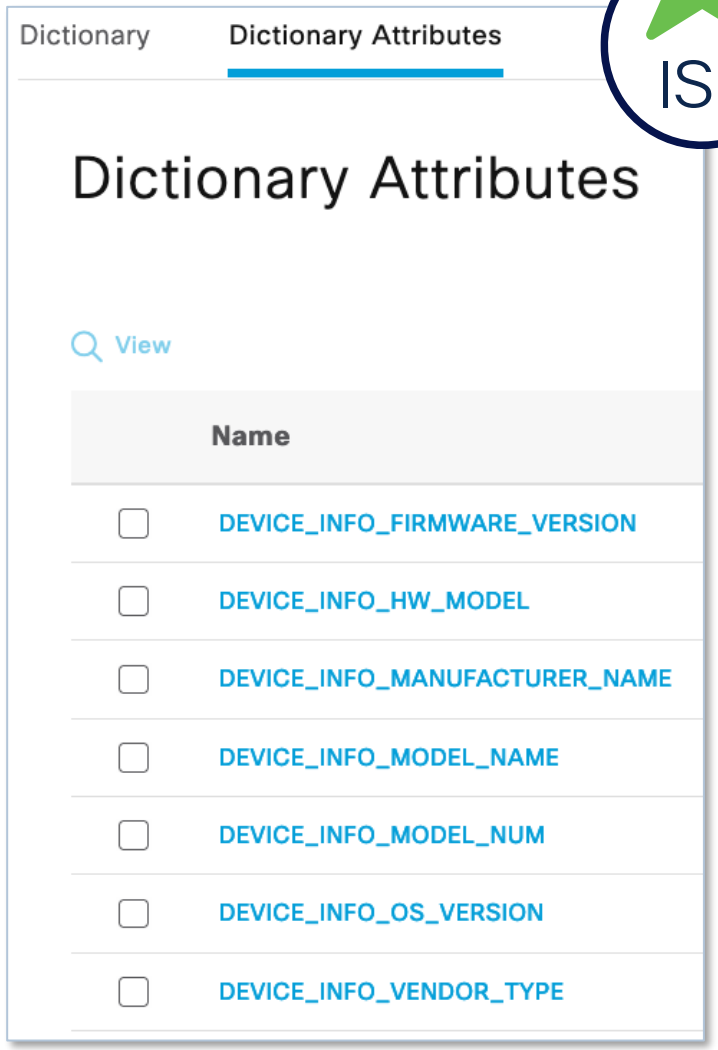
ISE 3.3

IOS-XE 17.10+

Enable



Wifi_Device_Analytics



Creating a Custom Profile

Under Attributes, you can see all the attributes for the unknown endpoint

Other Attributes	
5060-tcp	sip
80-tcp	http
AAA-Server	ise
AuthenticationIdentityStore	Internal Endpoints
AuthenticationMethod	Lookup
AuthenticationStatus	AuthenticationPassed
AuthorizationPolicyMatchedRule	Default
BYODRegistration	Unknown
Called-Station-ID	C0-67-AF-EE-09-AB
Calling-Station-ID	00-14-48-00-30-8C
DTLSSupport	Unknown
DestinationIPAddress	10.1.100.21
DestinationPort	1812
Device IP Address	10.1.100.75
Device Type	Device Type#All Device Types#Switches
DeviceRegistrationStatus	NotRegistered
ElapsedDays	0
EndPointMACAddress	00-14-48-00-30-8C
EndPointPolicy	Unknown
EndPointProfilerServer	ise.securitydemo.net
EndPointSource	SNMPQuery Probe
FailureReason	-
Framed-IP-Address	10.1.100.103
IPSEC	IPSEC#Is IPSEC Device#No
IdentityGroup	Unknown
IdentityPolicyMatchedRule	MAB
InactiveDays	0

OUI	Inventec Multimedia & Telecom Corporation
OriginalUserName	00144800308c
PolicyVersion	8
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	WiredMAB
SSID	C0-67-AF-EE-09-AB
SelectedAccessService	PEAP-EAP
SelectedAuthenticationIdentityStores	Internal Endpoints
SelectedAuthorizationProfiles	PermitAccess
Service-Type	Call Check
StaticAssignment	false
StaticGroupAssignment	false
StepData	5= DEVICE.Location, 6= DEVICE.Device Type, 7= DEVICE.Mode, 8= DEVICE. Radius.RadiusFlowType, 11=Internal Endpoints, 17= Session.ANCPolicy, 18= S
Total Certainty Factor	0
TrustSec-Enabled	TrustSec-Enabled#TrustSec-Enabled#Non-TrustSec
UseCase	Host Lookup
User-AD-Last-Fetch-Time	1543131931802
User-Fetch-User-Name	00144800308c
User-Name	00144800308c
UserType	Host
allowEasyWiredSession	false
chaddr	00:14:48:00:30:8c
ciaddr	0.0.0.0

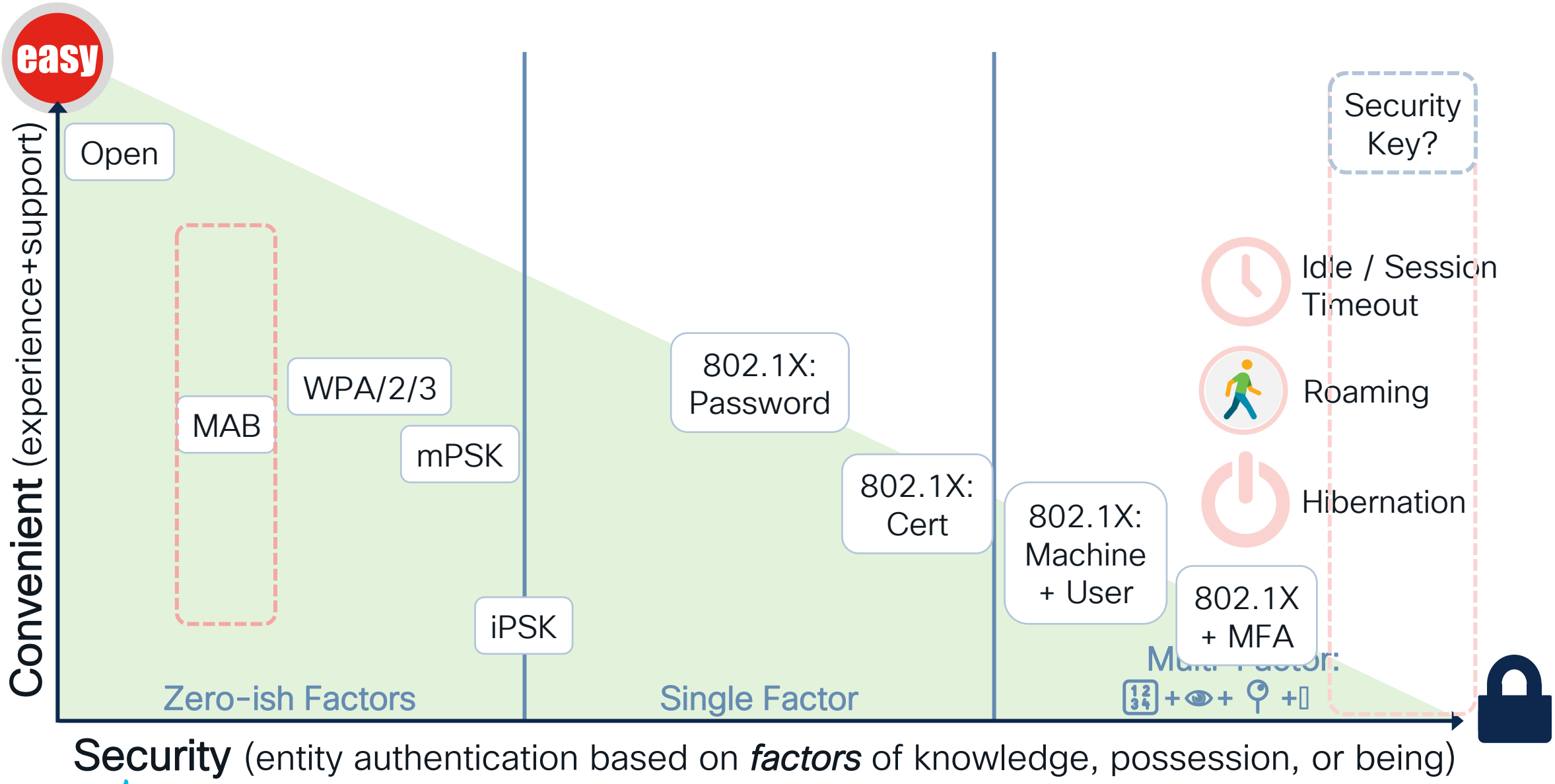
dhcp-class-identifier	udhcp 0.9.7
dhcp-client-identifier	01:00:14:48:00:30:8c
dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 3, 6, 12, 15, 28
dhcp-requested-address	10.1.100.103
dot1xAuthAuthControlledPortControl	2
dot1xAuthAuthControlledPortStatus	2
dot1xAuthSessionUserName	00-14-48-00-30-8C
flags	0x0000
giaddr	10.1.100.75
hlen	6
htype	Ethernet (10Mb)
ifDescr	GigabitEthernet1/0/43
ifIndex	50
ifOperStatus	1
ip	10.1.100.103
op	BOOTREQUEST
operating-system	Linux 2.4.9 - 2.4.18 (likely embedded)
operating-system-result	Linux 2.4.9 - 2.4.18 (likely embedded)
yiaddr	0.0.0.0

Profiling Probe Selection Best Practices

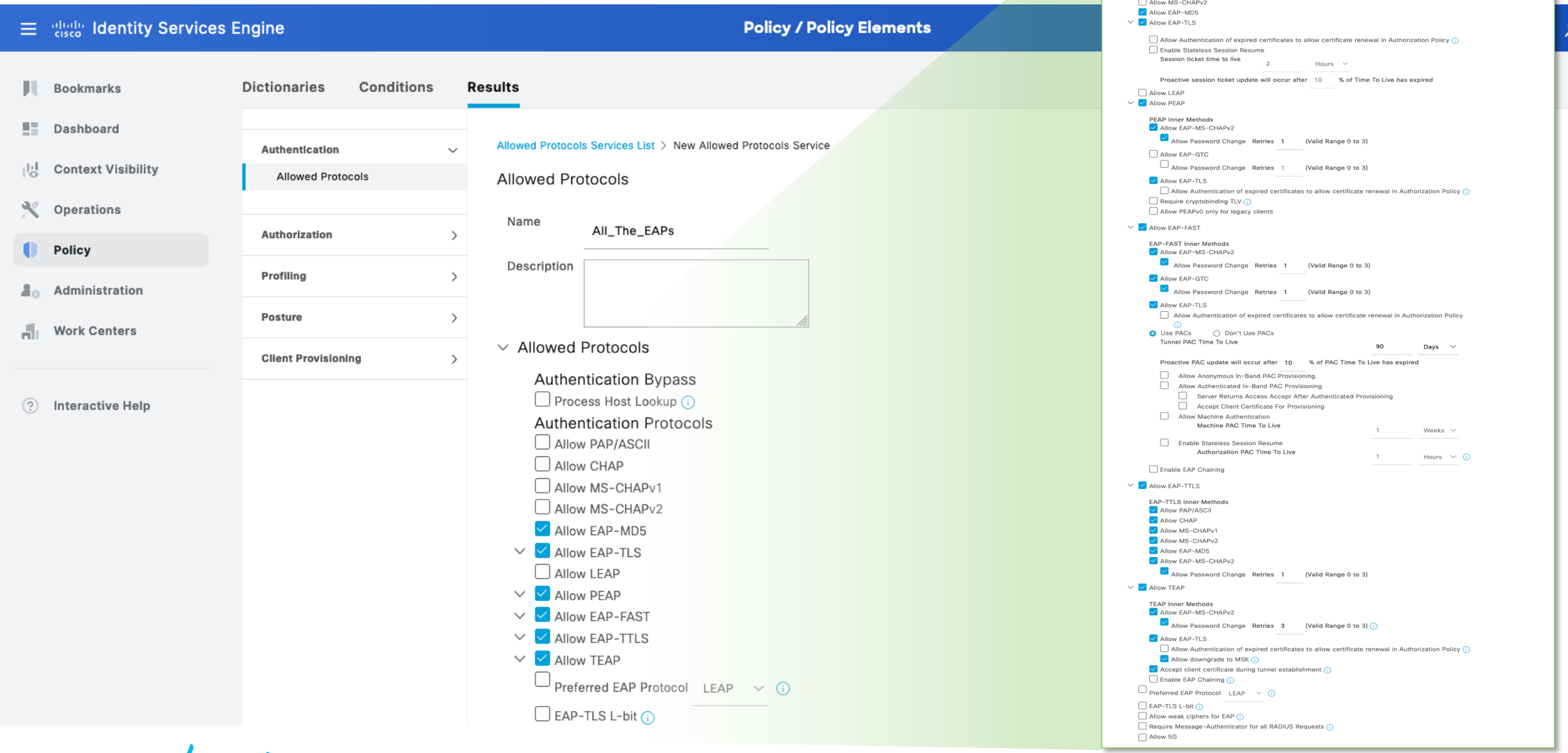
Probe	Key Profiling Attributes
RADIUS	MAC Address (OUI), IP Address, NDG values
RADIUS w/Device Sensor	CDP/LLDP, DHCP, User-Agent, mDNS, H323/SIP
RADIUS w/ACIDex	MAC Address (OUI), UDID, Operating System, Platform/Device Type
SNMP	MAC Address (OUI), CDP/LLDP, ARP tables
DHCP	DHCP
DNS	FQDN
HTTP	User-Agent
NetFlow	Protocol, Source/Dest IP, Source/DestPorts
NMAP	OS, Common and custom ports, Service Version Info, SMB & SNMP data
AD	Operating System and Version, AD Domain
pxGrid	IoT Asset, Custom Attributes
Endpoint Custom Attributes	*Customer defined*

ISE Profiling Design Guide cs.co/ise-profiling

Network Access Authentication is a Spectrum



ISE Supported EAP Methods



Federal Information Processing Standard (FIPS) Mode

cs.co/ise-fips

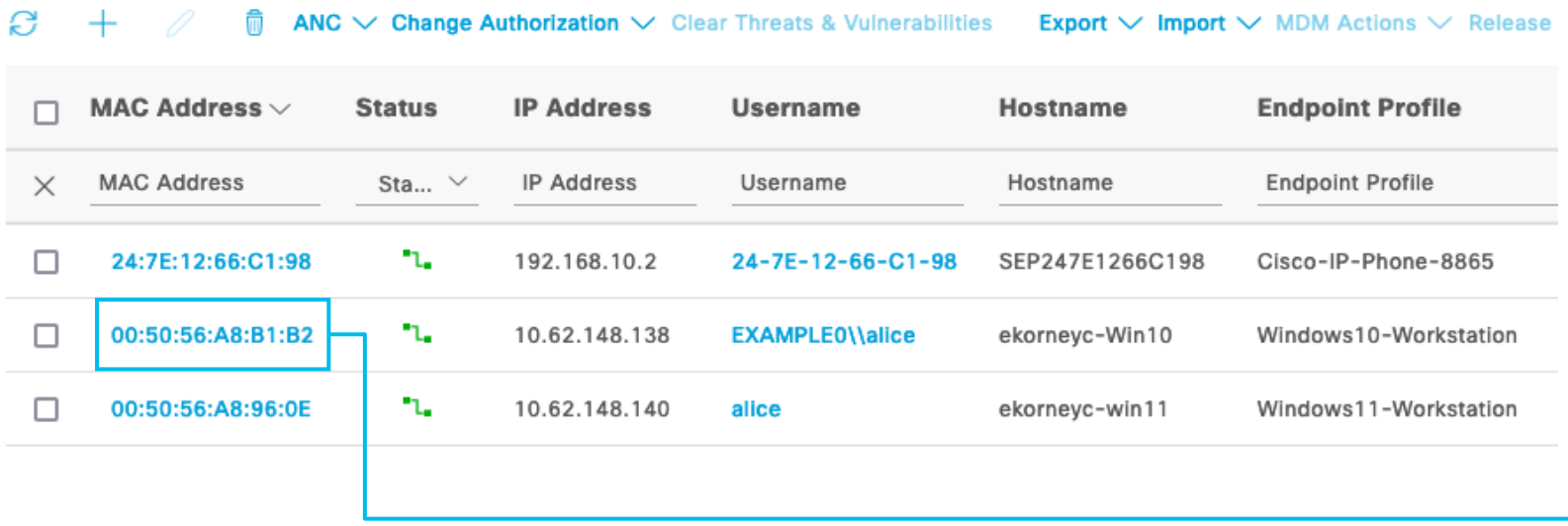
FIPS mode configures ISE to use only FIPS approved cryptographic modules

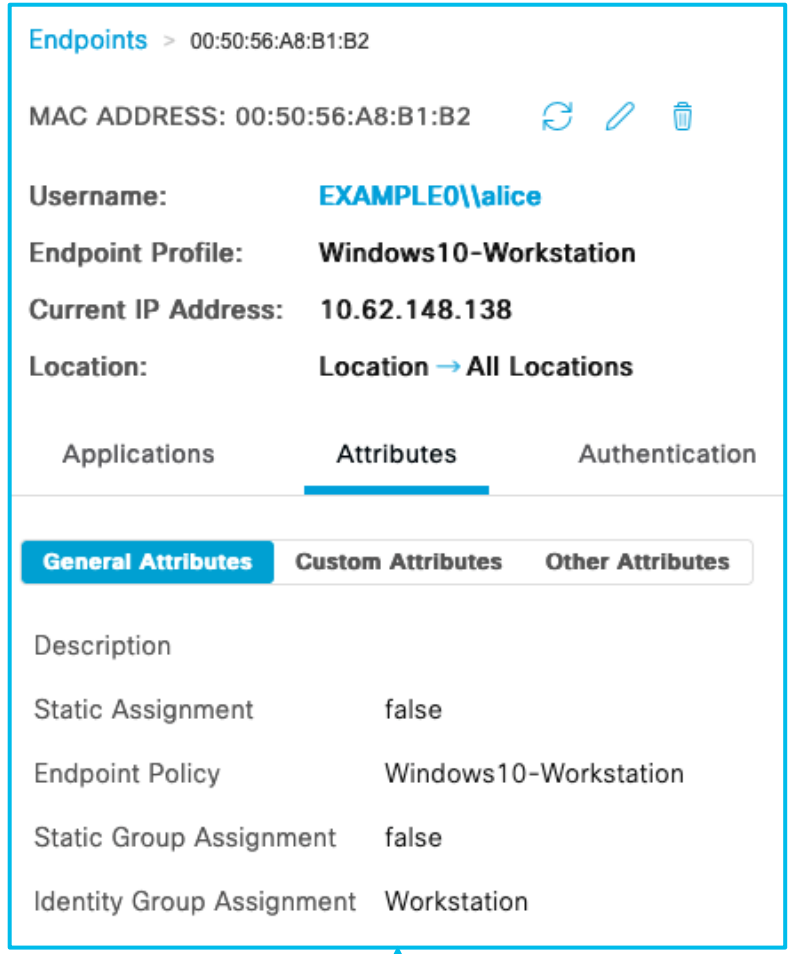
- All non-FIPS compliant cipher suites will be disabled in EAP-TLS, PEAP and EAP-FAST
- Certificates and private keys must use only FIPS compliant hash and encryption algorithms
  - RSA Private keys must be of 2048 bits or greater
  - ECDSA Private keys must be of 224 bits or greater
  - DHE ciphers work with DH param of 2048 bits or greater
  - SHA1 is not allowed to generate ISE local server certificates
  - The anonymous PAC provisioning option in EAP-FAST is disabled
- Local SSH server will operate in FIPS mode
- The following protocols are ***not supported*** in FIPS mode for RADIUS:
  EAP-MD5, PAP, CHAP, MS-CHAPv1, MS-CHAPv2, LEAP

FIPS mode changes require a restart of all ISE nodes in the deployment

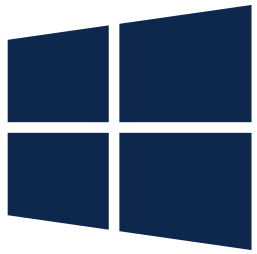
Context Visibility

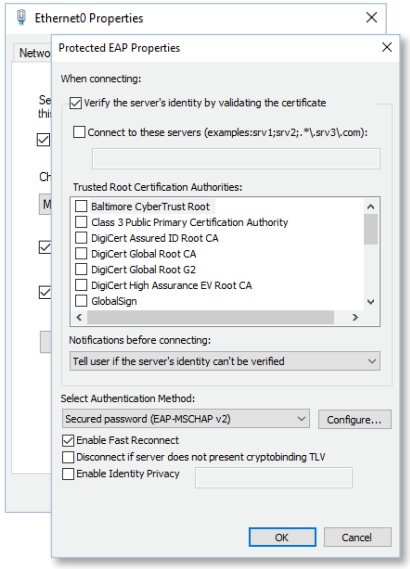
- Single pane for all endpoints:
  - Which endpoints are connected
  - Which profiles are assigned to which endpoints
  - IP to Mac address associations
  - Attributes, attributes, attributes!

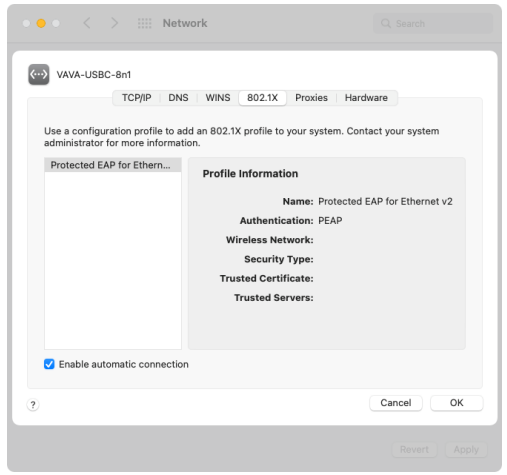


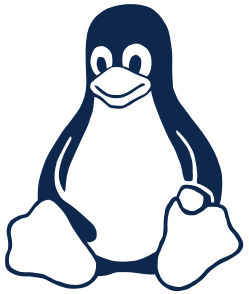


Endpoint 802.1X Supplicant Configuration







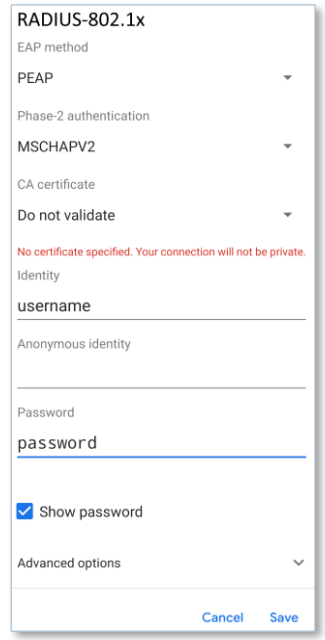


```
wpa_supplicant

NAME
wpa_supplicant - Wi-Fi Protected Access client and IEEE
802.1X supplicant

SYNOPSIS
wpa_supplicant [ -BddfhKLqqsTtuvW ] [ -iifname ] [ -
cconfig file ] [ -Ddriver ] [ -PPID_file ] [ -foutput
file ]

OVERVIEW
Wireless networks do not require physical access to the
network equipment in the same way as wired networks.
This makes it easier for unauthorized users to passively
monitor a network and capture all transmitted frames.
In addition, unauthorized use of the network is much
easier. In many cases, this can happen even
without user's explicit knowledge since the wireless
LAN adapter may have been configured to automatically
join any available network.
Link-layer encryption can be used to provide a layer of security
for wireless networks. The original wireless LAN standard,
```



BYOD / EMM / MDM

For Provisioning and Compliance

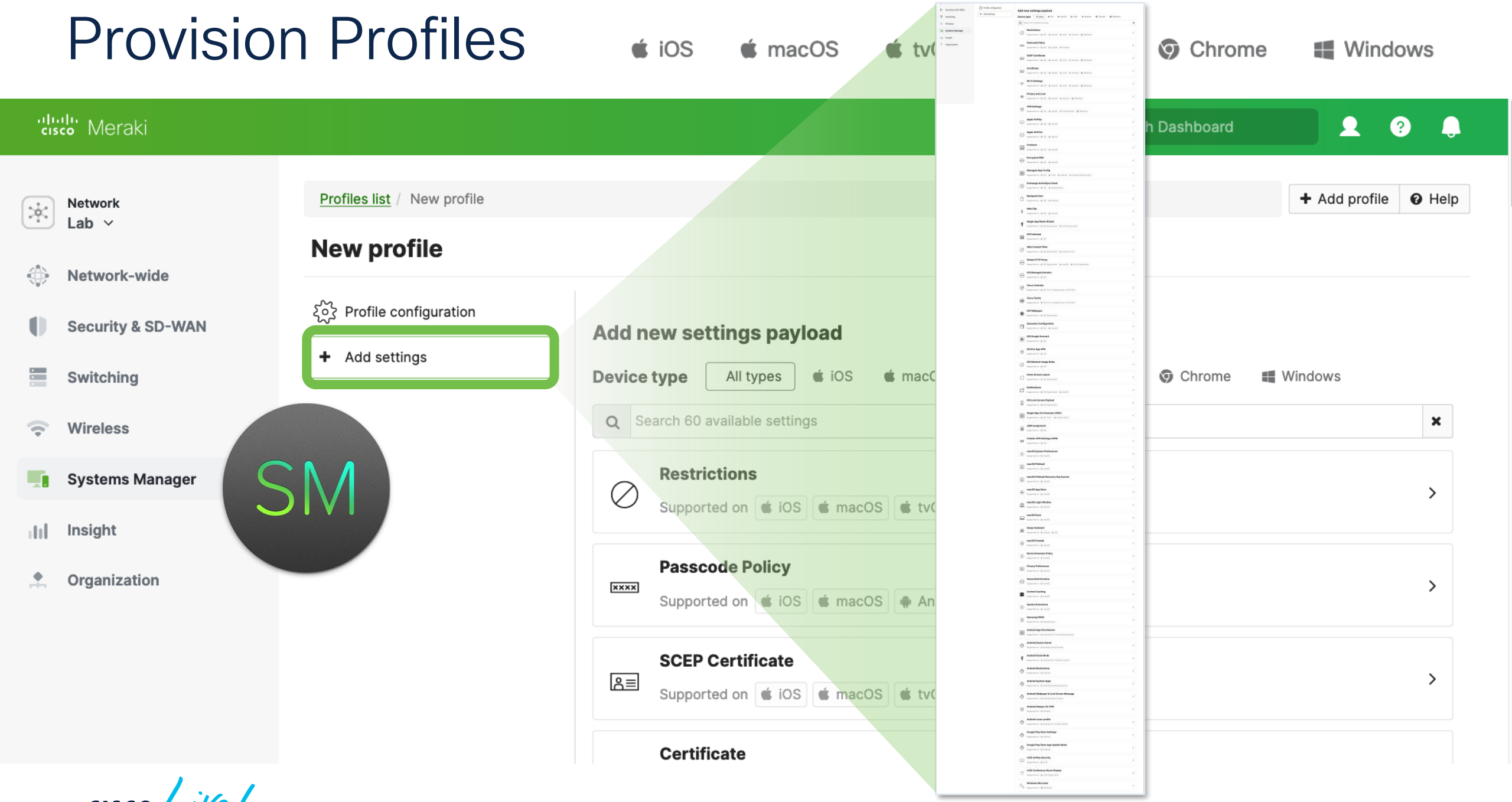
cisco.com/go/csta

AbsoluteSoftware
SOPHOS
GLOBO
IBM Security
Microsoft
SOTI
tangoe
cisco Meraki
CITRIX XenMobile
jamf
SAP
MobileIron
Symantec.
airwatch by vmware

MDM Attributes

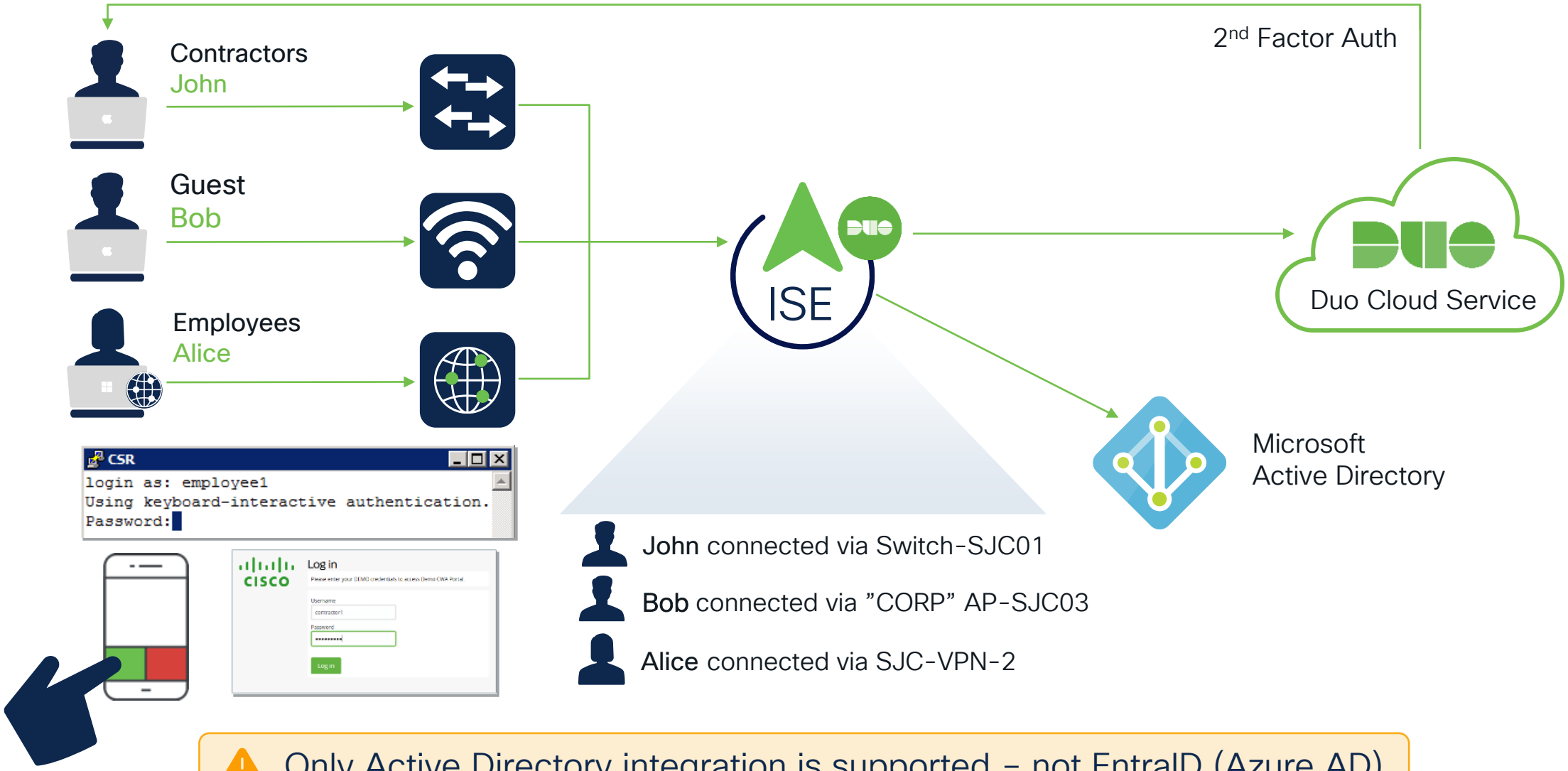
ActivityType
AdminAction
AdminActionUUID
AnyConnectVersion
DaysSinceLastCheckin
DetailedInfo
DeviceID
DeviceName
DeviceType
DiskEncryption
EndPointMatchedProfile
FailureReason
IdentityGroup
IMEI
IpAddress
JailBroken
LastCheckInTimeStamp
MacAddress
Manufacturer
MDMCompliantStatus
MDMFailureReason
MDMServerName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

Provision Profiles



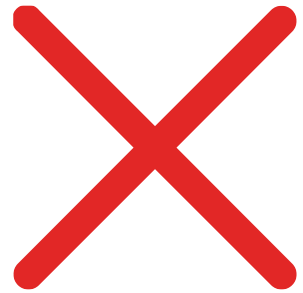
Enhanced ISE + Duo Integration for MFA

ISE 3.3.1



⚠ Only Active Directory integration is supported – not EntraID (Azure AD)

MFA Requires a Finger and a Phone



Solve Identity for Zero Trust with Duo *and* ISE

Access Problem	Cisco ISE	Cisco Duo	Cisco ISE + Duo
User + Device (On-Premise) → On-Premise Applications	No MFA	Web Only	○
IOT Device (On-Premise) → On-Premise Applications	○		○
User + Device (Off-Premise) → On-Premise Applications	VPN Based	Web Only	○
User / Device (On-Premise) → User / Device (On-Premise)	○		○
User + Device (On-Premise) → Cloud Applications	No MFA	No network security	○
User + Device (Off-Premise) → Cloud Applications		○	○

Challenges: Network Devices

ISE Compatibility

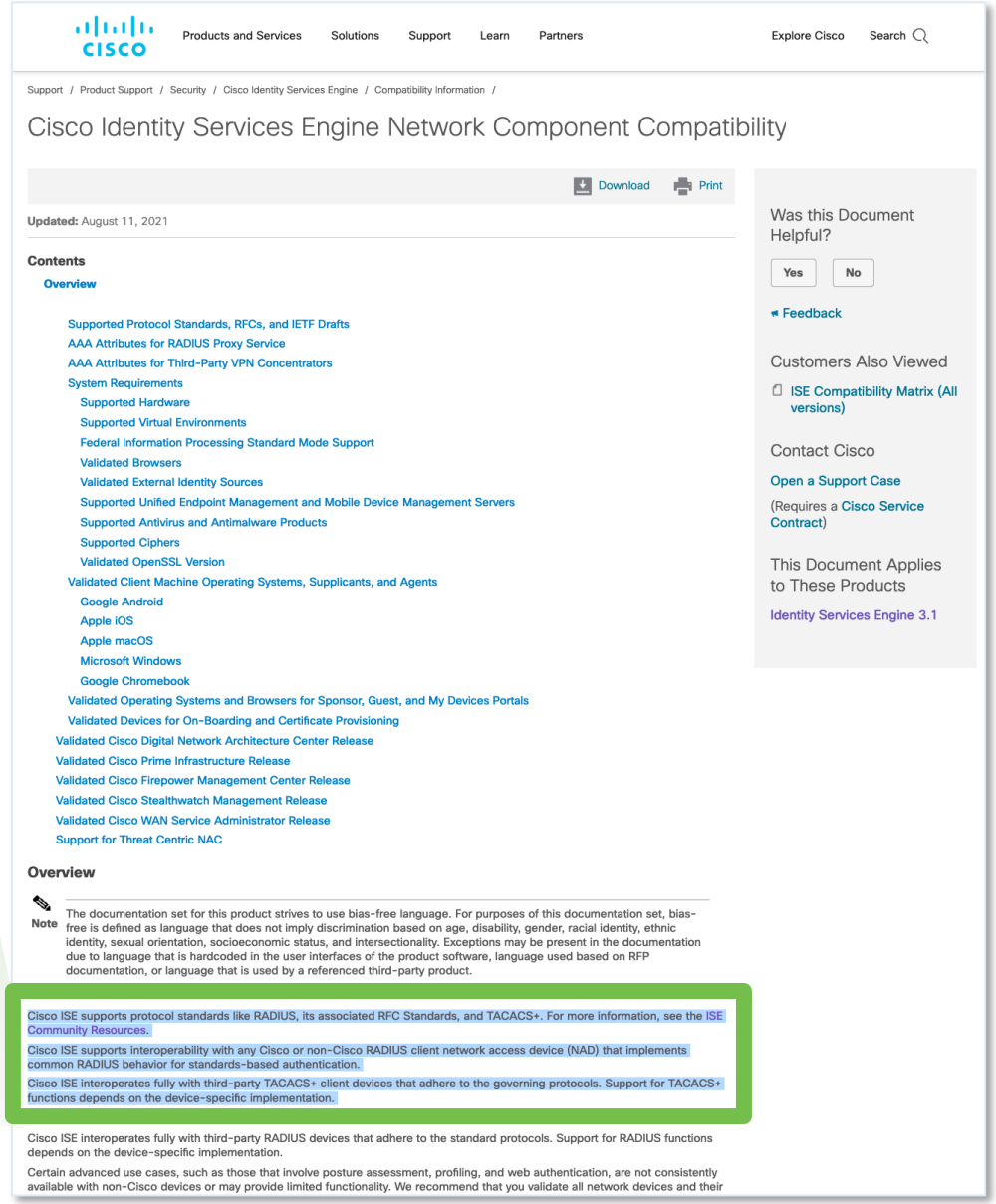
cs.co/ise-compatibility

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.

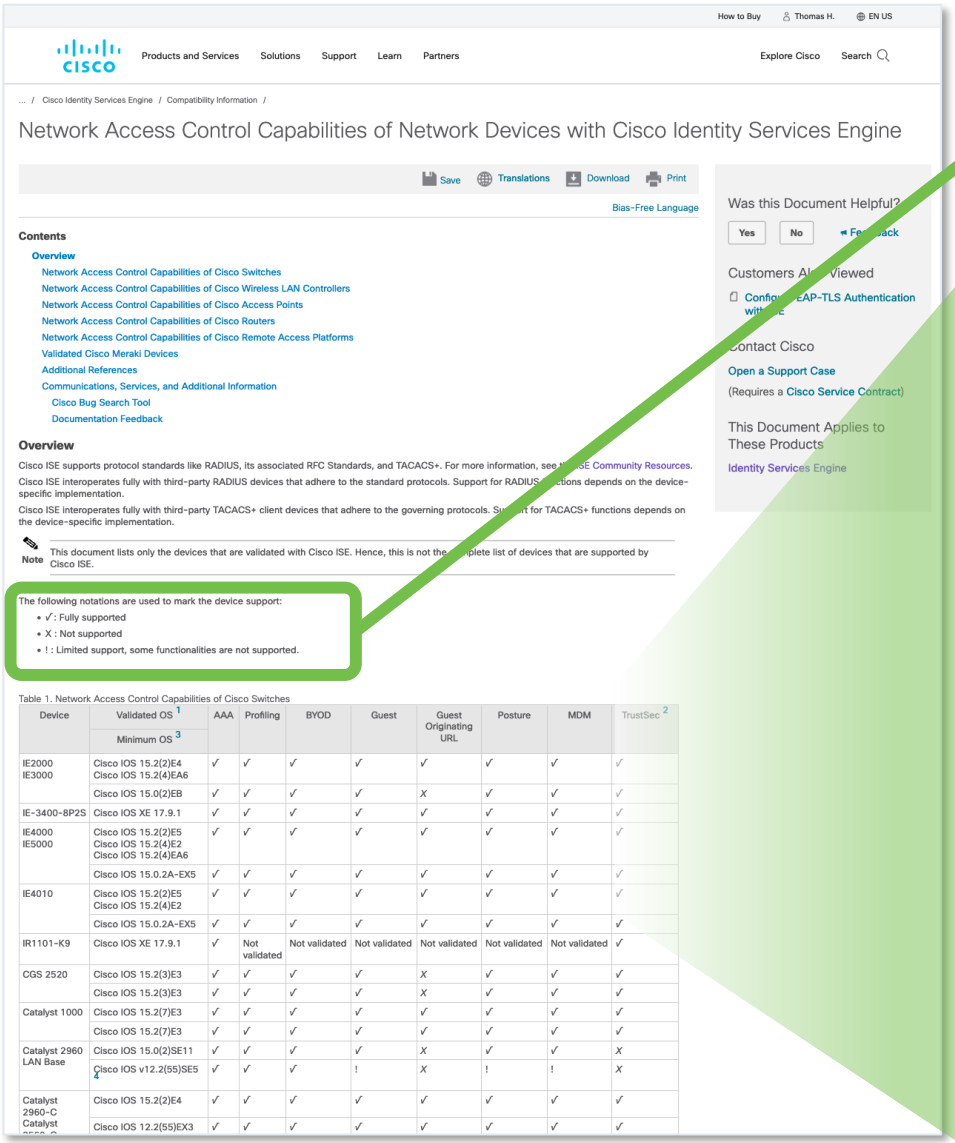
Cisco ISE supports interoperability with **any Cisco or non-Cisco RADIUS client network access device (NAD)** that implements common RADIUS behavior for standards-based authentication.

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.



Network Device Capabilities

cs.co/nad-capabilities



Network Access Control Capabilities of Network Devices with Cisco Identity Services Engine

Contents

- Overview
  - Network Access Control Capabilities of Cisco Switches
  - Network Access Control Capabilities of Cisco Wireless LAN Controllers
  - Network Access Control Capabilities of Cisco Access Points
  - Network Access Control Capabilities of Cisco Routers
  - Network Access Control Capabilities of Cisco Remote Access Platforms
  - Validated Cisco Meraki Devices
  - Additional References
  - Communications, Services, and Additional Information
    - Cisco Bug Search Tool
    - Documentation Feedback

Overview

Cisco ISE supports protocol standards like RADIUS, its associated RFC Standards, and TACACS+. For more information, see ISE Community Resources.

Cisco ISE interoperates fully with third-party RADIUS devices that adhere to the standard protocols. Support for RADIUS functions depends on the device-specific implementation.

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.

Note: This document lists only the devices that are validated with Cisco ISE. Hence, this is not the complete list of devices that are supported by Cisco ISE.

The following notations are used to mark the device support:

- ✓ : Fully supported
- X : Not supported
- ! : Limited support, some functionalities are not supported.

Table 1. Network Access Control Capabilities of Cisco Switches

Device	Validated OS [1] / Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
IE2000 IE3000	Cisco IOS 15.2(2)E4 Cisco IOS 15.2(4)EA6	✓	✓	✓	✓	✓	✓	✓	✓
	Cisco IOS 15.0(2)EB	✓	✓	✓	✓	X	✓	✓	✓
IE-3400-8P2S	Cisco IOS XE 17.9.1	✓	✓	✓	✓	✓	✓	✓	✓
IE4000 IE5000	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2(4)EA6	✓	✓	✓	✓	✓	✓	✓	✓
	Cisco IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✓
IE4010	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2	✓	✓	✓	✓	✓	✓	✓	✓
	Cisco IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✓
IR1101-K9	Cisco IOS XE 17.9.1	✓	Not validated	Not validated	Not validated	Not validated	Not validated	Not validated	✓
CGS 2520	Cisco IOS 15.2(3)E3	✓	✓	✓	✓	X	✓	✓	✓
	Cisco IOS 15.2(3)E3	✓	✓	✓	✓	X	✓	✓	✓
Catalyst 1000	Cisco IOS 15.2(7)E3	✓	✓	✓	✓	✓	✓	✓	✓
	Cisco IOS 15.2(7)E3	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 2960 LAN Base	Cisco IOS 15.0(2)SE11	✓	✓	✓	✓	X	✓	✓	X
	Cisco IOS v12.2(55)SE5 [4]	✓	✓	✓	!	X	!	!	X
Catalyst 2960-C Catalyst	Cisco IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓	✓
	Cisco IOS 12.2(55)EX3	✓	✓	✓	✓	✓	✓	✓	✓

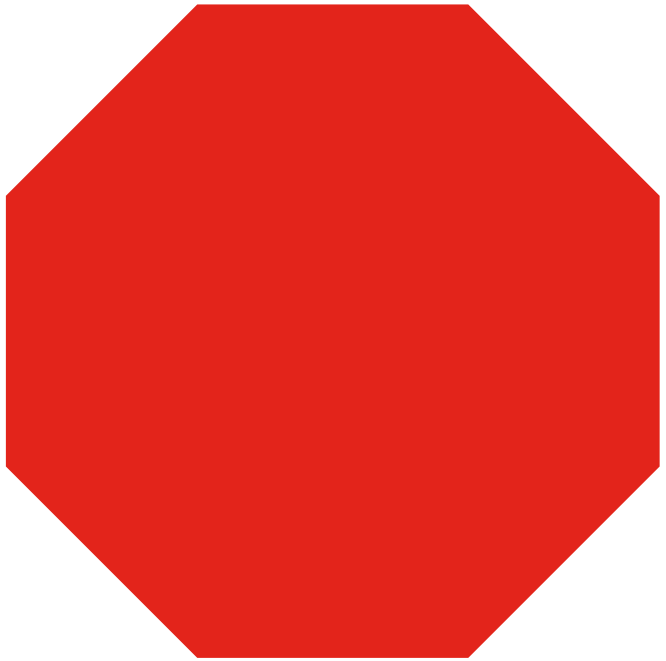
✓ : Fully supported
X : Not supported
! : Limited support, some functionalities are not supported

Device	Validated OS [1] / Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
IE2000 IE3000	Cisco IOS 15.2(2)E4 Cisco IOS 15.2(4)EA6	✓	✓	✓	✓	✓	✓	✓	✓
	Cisco IOS 15.0(2)EB	✓	✓	✓	✓	X	✓	✓	✓
IE-3400-8P2S	Cisco IOS XE 17.9.1	✓	✓	✓	✓	✓	✓	✓	✓
IE4000 IE5000	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2(4)EA6	✓	✓	✓	✓	✓	✓	✓	✓
	Cisco IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✓
IE4010	Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2	✓	✓	✓	✓	✓	✓	✓	✓
	Cisco IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✓
IR1101-K9	Cisco IOS XE 17.9.1	✓	Not validated	Not validated	Not validated	Not validated	Not validated	Not validated	✓

Cisco Meraki Access Control Capabilities with ISE

Model	802.1X	MAB	VLAN	GPACL	Adaptive Policy	URL Redirect	CoA	Profiling
Wireless								
MR20, MR70, MR28, MR78	☑	☑	☑	☑	–	☑	☑	–
MR30H, MR36, MR42/E, MR44, MR45, MR46/E, MR52, MR53E, MR56, MR57, MR74, MR76, MR86, CW916x	☑	☑	☑	☑	☑ 802.11ac Wave2 or higher. Min 27.6	☑	☑	–
Teleworker								
Z3/C	☑	☑	–	–	☑ Transport MX18.1+	–	–	–
Switching								
MS120, MS125, MS130	☑	☑	☑	–	–	–	☑	CDP+LLDP
MS210, MS225, MS250	☑	☑	☑	☑	–	☑	☑	CDP+LLDP
MS350, MS355	☑	☑	☑	☑	–	☑	☑	CDP+LLDP
MS390, 9300-M	☑	☑	☑	☑	☑ 14.2+	☑	☑	Device Sensor CDP/LLDP/ DHCP/HTTP
MS410, MS425, MS450 (aggregation)	☑	☑	☑	☑	–	☑	☑	CDP+LLDP
Security & SD-WAN								
MX64/W, MX67/C/W, MX68/CW/W, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX450	☑ 802.1X *or* MAB	☑ 802.1X *or* MAB	–	–	☑ Transport MX18.1+	–	–	–
vMX, vMX100	–	–	–	–	–	–	–	–

No/Missing Network Device(s)?



A network device that is not defined in ISE will not receive AAA services from ISE!

Relevant Errors in Syslogs or ISE LiveLogs :

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

ISE Network Device Groups (NDGs)

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | More

Network Device Groups

Refresh | Add | Duplicate | Edit | Trash | Show group members | Import | Export | Flat Table | Expand All | Collapse All

Name	Description	No. of Network Devices
All Device Types	All Device Types	--
All Locations	All Locations	--
AMER		0
US		0
San Jose		0
Building		0
Floor		0
Countries		--
Departments		--

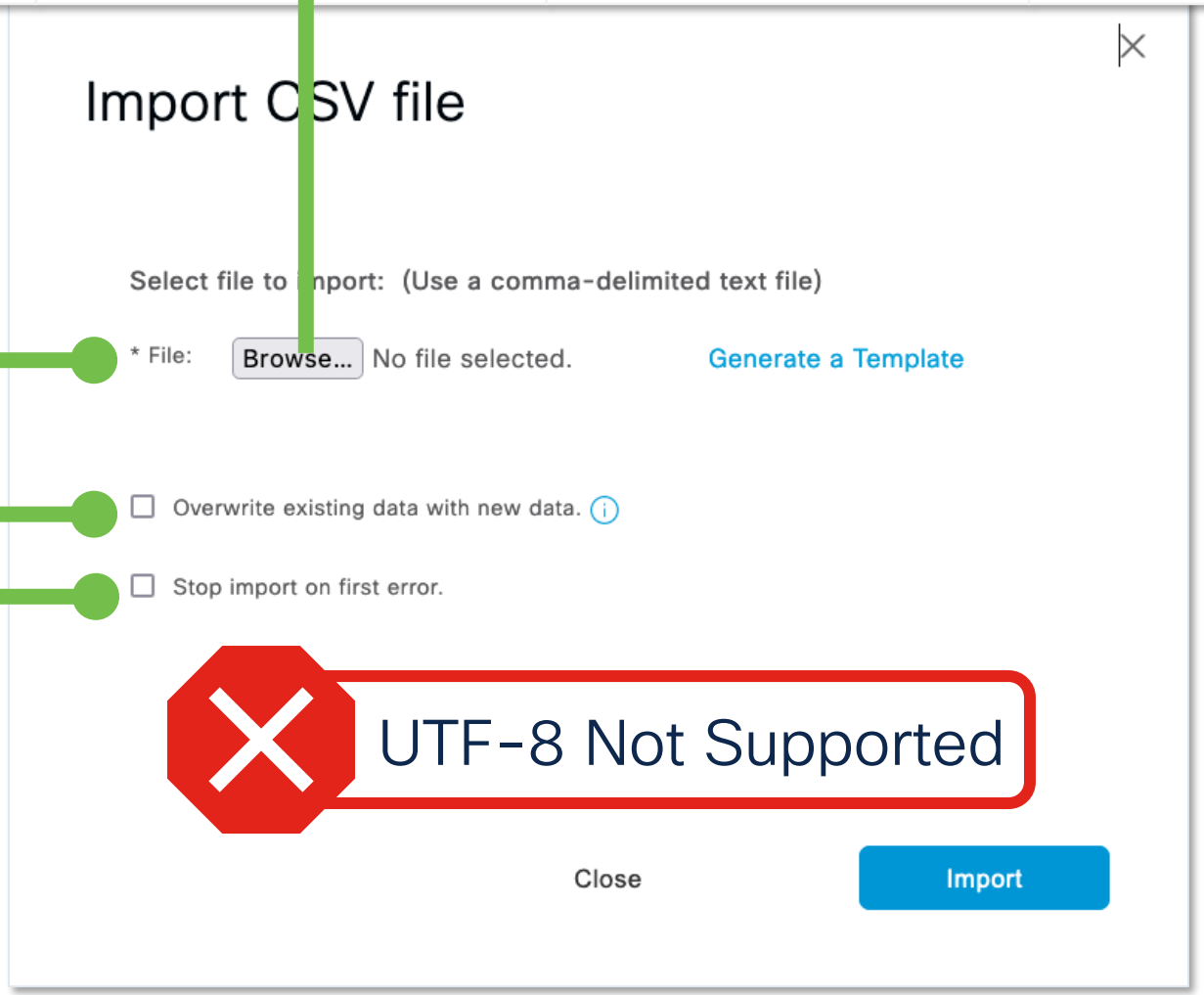
Maximum 6 NDG Levels

Create Your Own Root NDGs!

Network Device Group: Import from CSV

template.csv

Name:String(100):Required	Description:String(1024)	Type:String(64):Required	Is Root:Boolean(true|false):Required



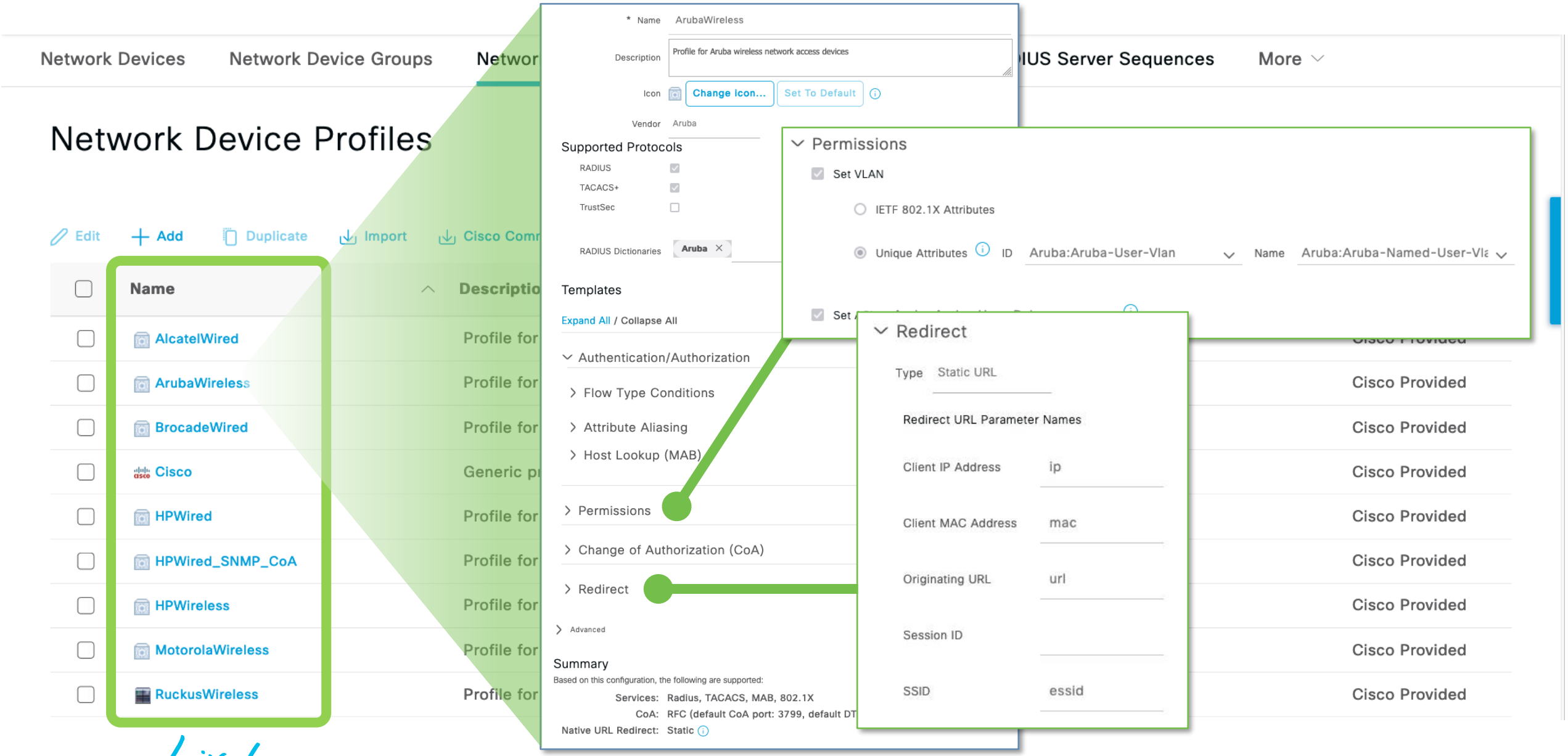
Choose File

Missing NDGs Deleted

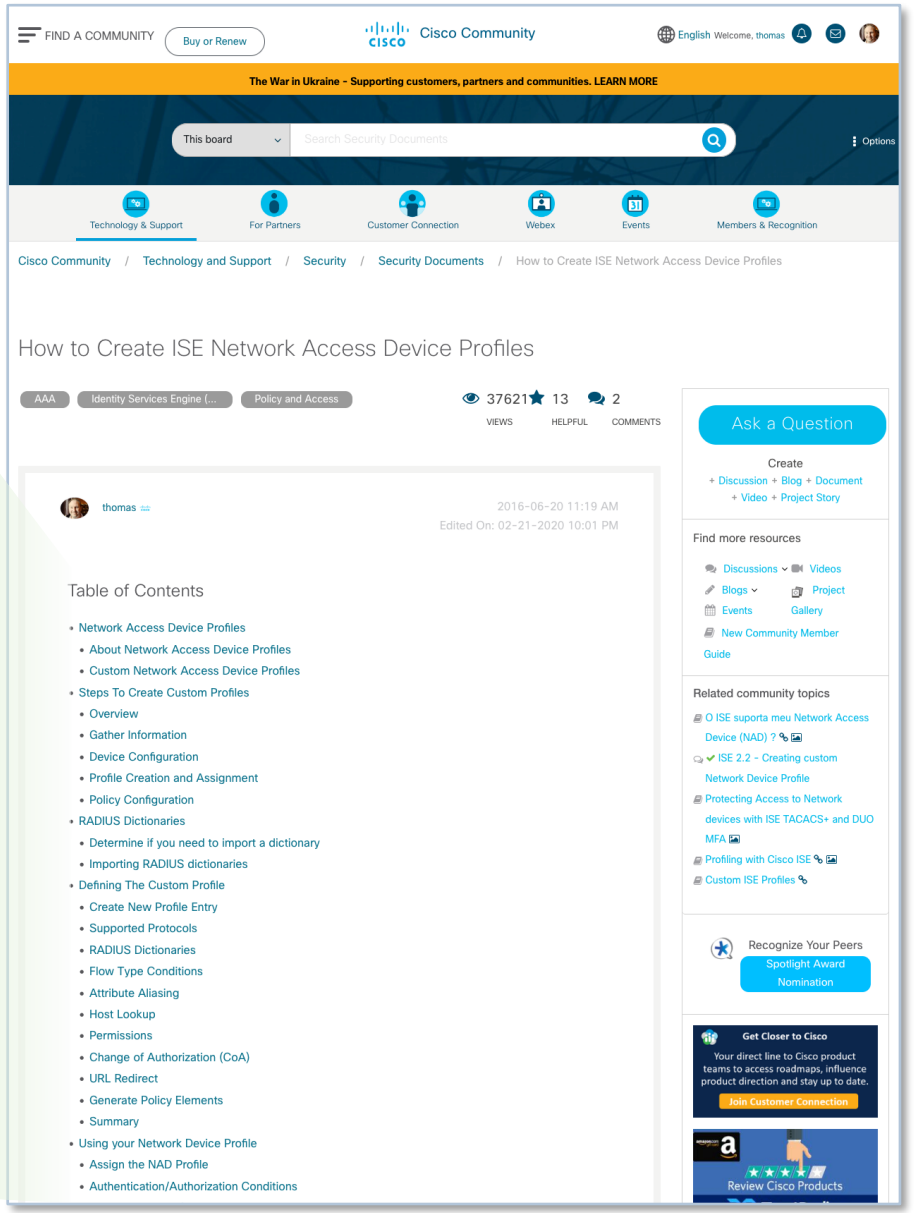
Choose File

UTF-8 Not Supported

Network Device Profiles



Create ISE Network Access Device Profiles

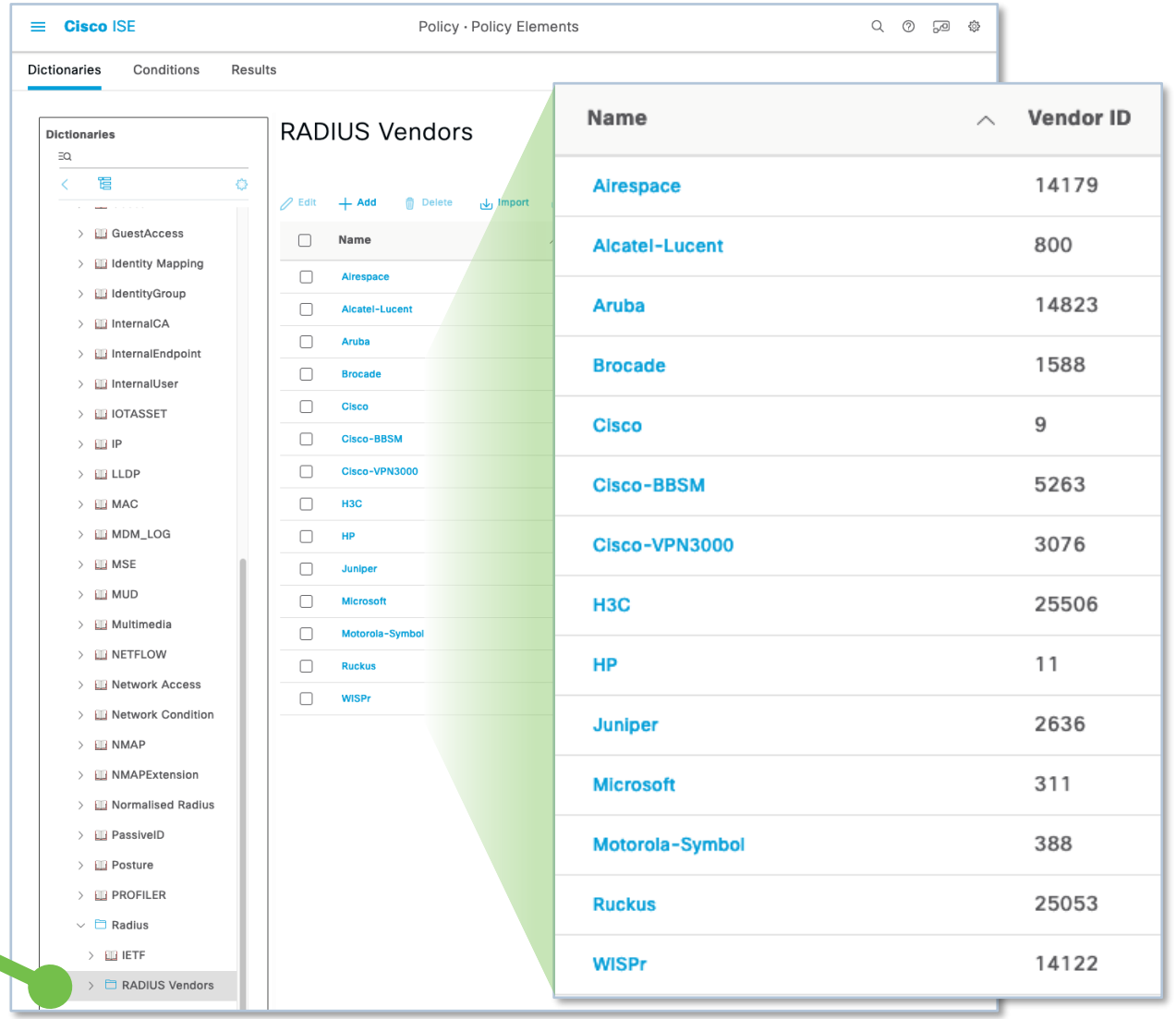


RADIUS Vendor Specific Attributes (VSAs)

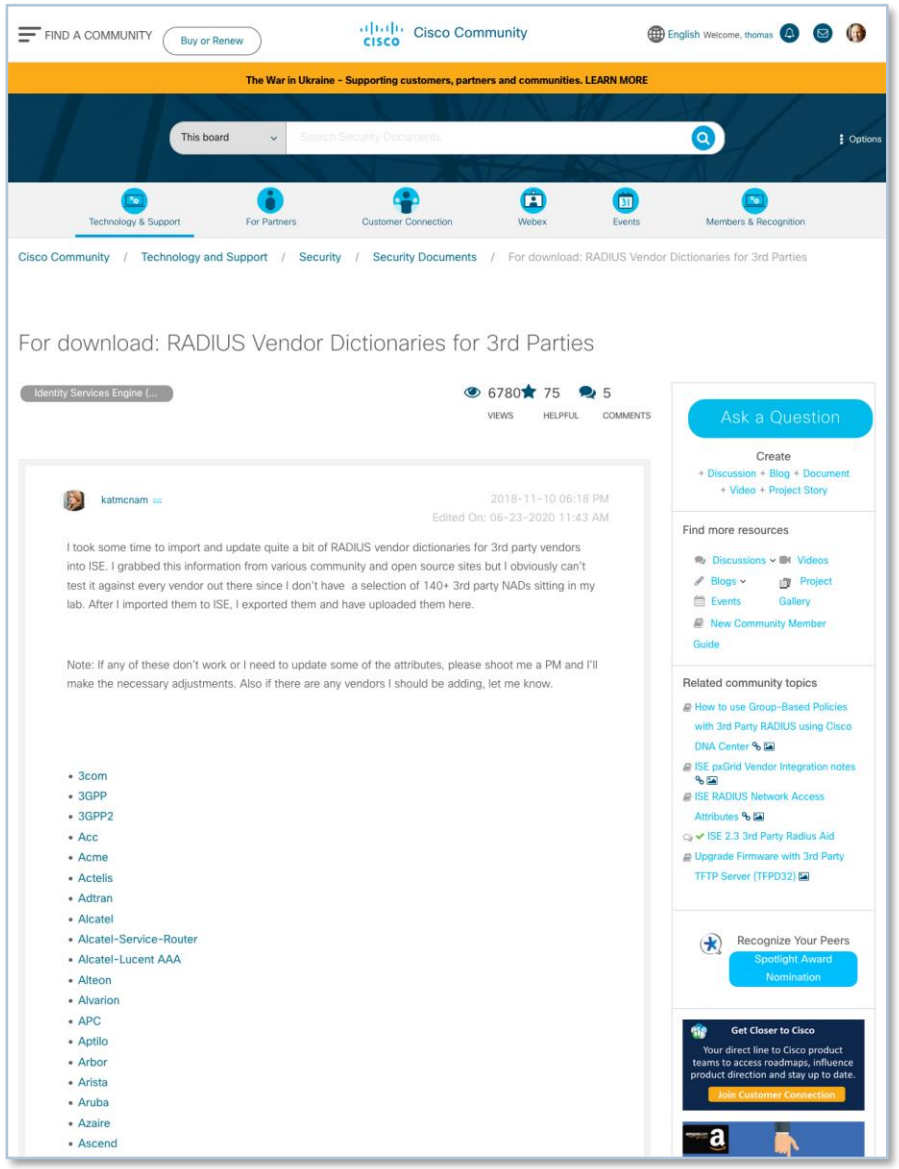
RFC 2865 **RADIUS** **June 2000**

Table of Contents

≡ > Policy > Policy Elements > Dictionaries



RADIUS Vendor Dictionaries for 3rd Parties



- 3com
- 3GPP
- 3GPP2
- Acc
- Acme
- Actelis
- Adtran
- Alcatel
- Alcatel-Service-Router
- Alcatel-Lucent AAA
- Alteon
- Alvarion
- APC
- Aptilo
- Arbor
- Arista
- Aruba
- Azaire
- Ascend
- Bay Networks
- BinTec
- Bluecoat
- Boingo
- Broadsoft
- Brocade
- British Sky Broadcasting Group
- British Telecom
- Cablelabs
- Cabletron
- Camiant
- Checkpoint
- Chillispot
- Citrix
- Clavister
- Cnergee Access Server
- Colubris
- Compatible Systems Corporation
- Cosine
- Dante
- Dell EMC
- Dlink
- Digium
- Dragonwave
- Efficient IP
- Eltex
- Epygi
- ERX
- EqualLogic
- Ericsson
- Ericsson-AB
- Ericsson Packet Core Networks
- Extreme
- F5
- FdXtended
- FreeRADIUS
- FreeSwitch
- Fortinet
- Foundry
- Gandalf
- Gemtek
- H3C
- Hillstone
- HP
- Huawei
- IEA Software
- Infonet
- Issanni
- ITK
- IP Unplugged
- Juniper
- Karlnet
- Kineto
- Lancom
- Lantronix
- Livingston
- Local Web
- Lucent
- Manzara
- Meinberg
- Meraki
- Merit
- Meru
- Microsemi
- Microsoft
- Mikrotik
- Mimosa
- Motorola
- Motorola-Symbol
- Navini
- NetBorder
- Netscreen
- Network Physics
- Nexans
- NTUA
- Nokia
- Nomadix, Inc
- Nortel
- Packeteer (Later acquired by Blue Coat)
- Palo Alto Networks
- Patton IADs
- Perle Systems
- Propel
- Prosoft
- Proxim Wireless
- Purewave Networks Base Station
- Quiconnect
- Quintum
- Redcreek
- Riverbed
- Riverstone Networks
- Roaring Penguin
- RuggedCom
- Ruckus
- Shasta
- SG-1 Systems by Runcom Technologies
- Siemens
- Slipstream
- Softbank
- SonicWall
- SpringTide
- Starent
- SurfNet
- Telebit
- Terena
- Trapeze/Juniper
- Travelping
- Tropos
- T-Systems-Nova
- Ukerna
- Unix
- USR Robotics
- UT Starcom
- Valemount Networks
- VersaNet Communications
- Waverider
- Walabi
- Wichorus
- WiFi-Alliance
- WiMAX
- WISPr
- Xedia
- Yubico
- Zeus Packet
- ZTE
- Zyxel

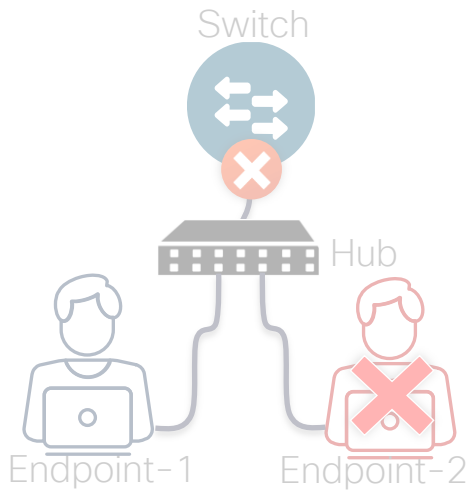
Endpoint Host Modes

cs.co/ise-wired

Single Host Mode

Only 'one' MAC Address is allowed. Second MAC Address causes Security Violation

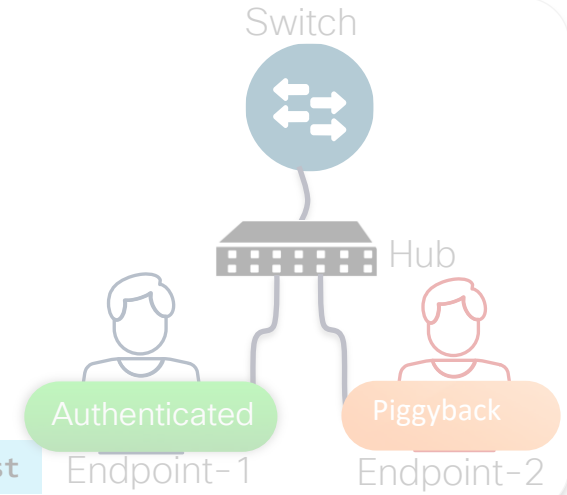
```
authentication host-mode single-host
```



Multi-Host Mode

1st MAC Address is authenticated. 2nd endpoint piggybacks on 1st MAC Address authentication and bypasses authentication

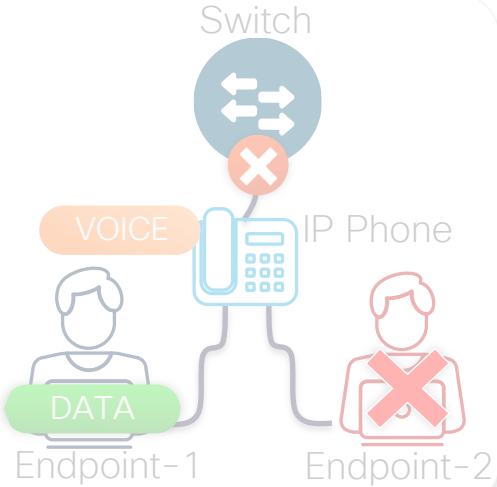
```
authentication host-mode multi-host
```



Multi-Domain Mode

Each domain (Voice or Data) authenticates one MAC address. 2nd MAC address on each domain causes security violation

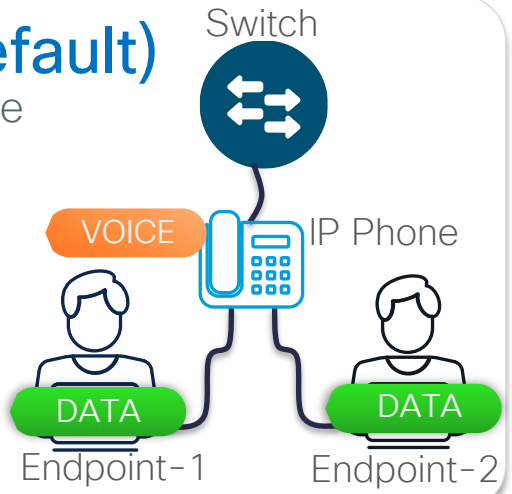
```
authentication host-mode multi-domain
```



Multi-Auth Mode(Default)

Voice domain authenticates one MAC address. Data domain authenticates multiple MAC addresses. dACL or single VLAN Assignment for all devices are supported

```
authentication host-mode multi-auth
```

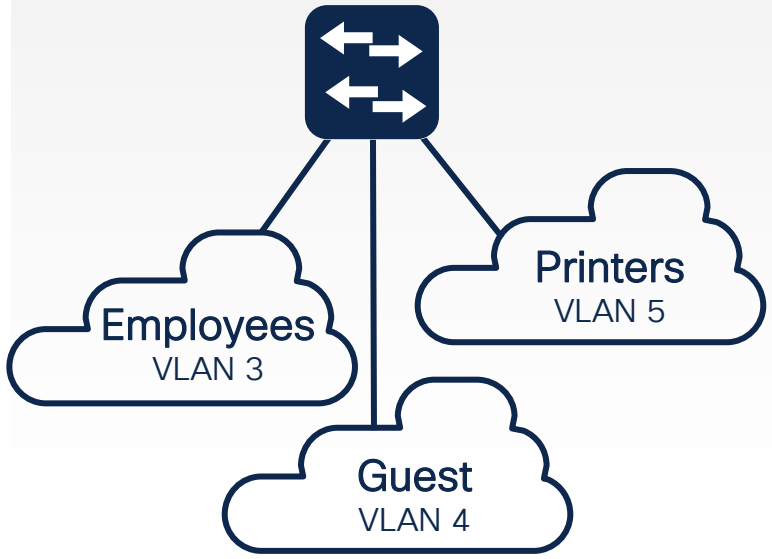


Authorization Enforcement Options

Beyond RADIUS Access-Accept / Access-Reject

VLANs

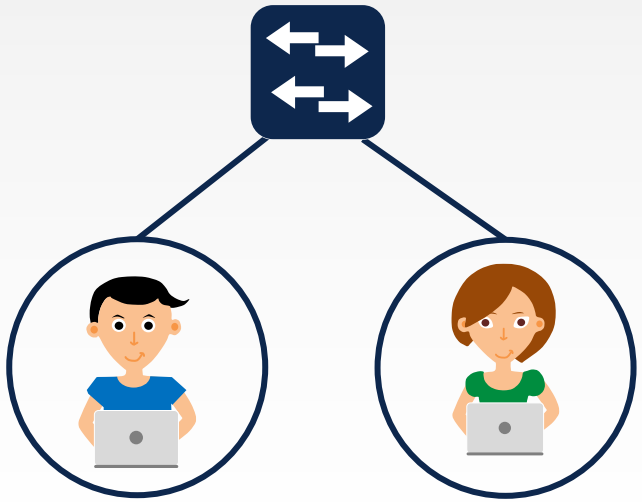
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless)



Employee
permit ip any any

Contractor
deny ip host <critical>
permit ip any any

Scalable Group Tags

Cisco Group-Based Policy

16-bit SGT assignment and
SGT based Access Control

cs.co/trustsec-compatibility

ISE Secure Wired Access Prescriptive Deployment Guide

cs.co/ise-wired

- Define
  - AAA Components & Terminology
- Design
  - Phased Deployments
- Deploy
  - Monitoring (Open Mode)
  - Low Impact (Pre-Authentication)
  - Restricted (Closed Mode)
- Operate
  - Troubleshooting

ISE Secure Wired Access Prescriptive Deployment Guide

hariholla Cisco Employee

on 2021-01-21 12:41 PM - edited on 2021-09-10 03:06 PM by hslai

Cisco ISE Secure Wired Access Prescriptive Deployment Guide

Cisco ISE Deployment Guides

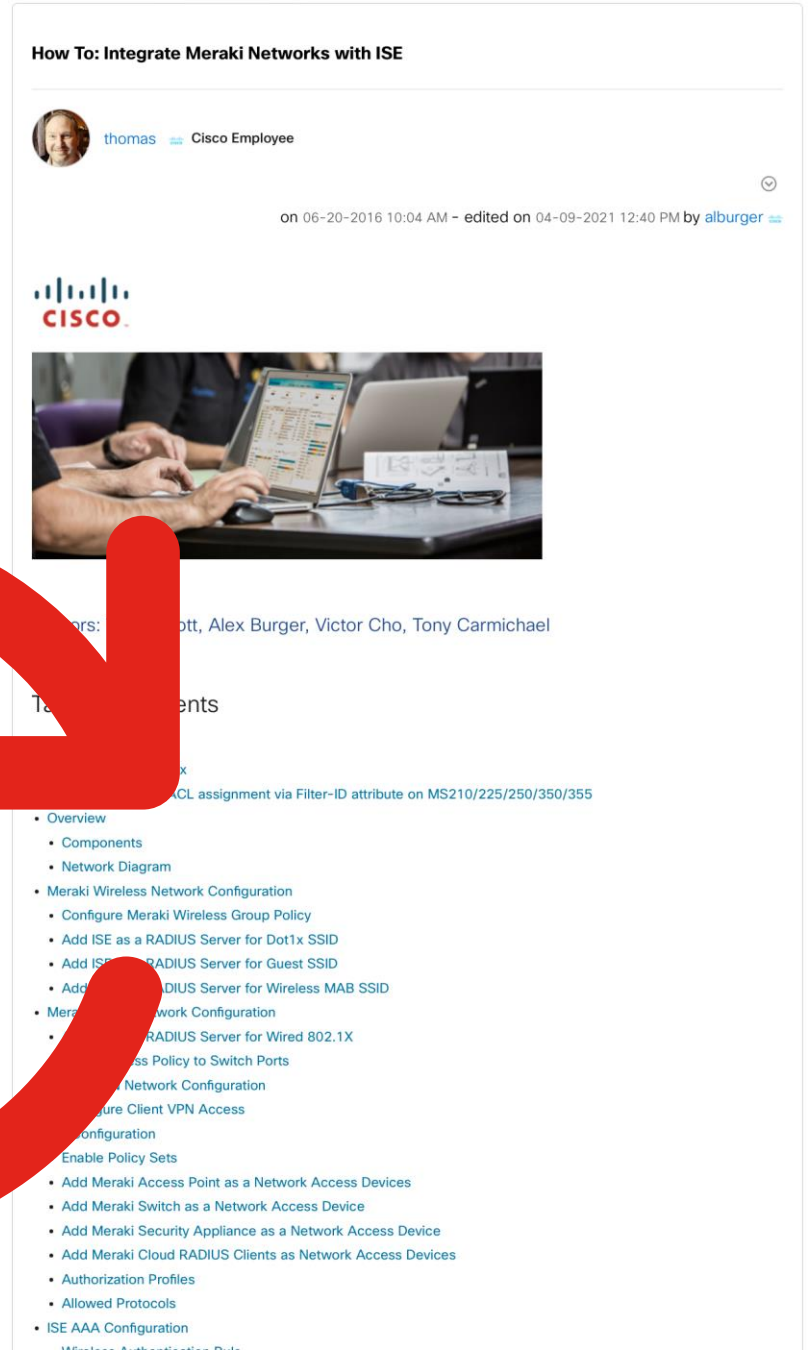
Authors: Hariprasad Holla (until June 2018), Mahesh Nagireddy (until Dec 2018)

For an offline or printed copy of this document, simply choose ⋮ **Options > Printer Friendly Page**. You may then Print, Print to PDF or copy and paste to any other document format you like.

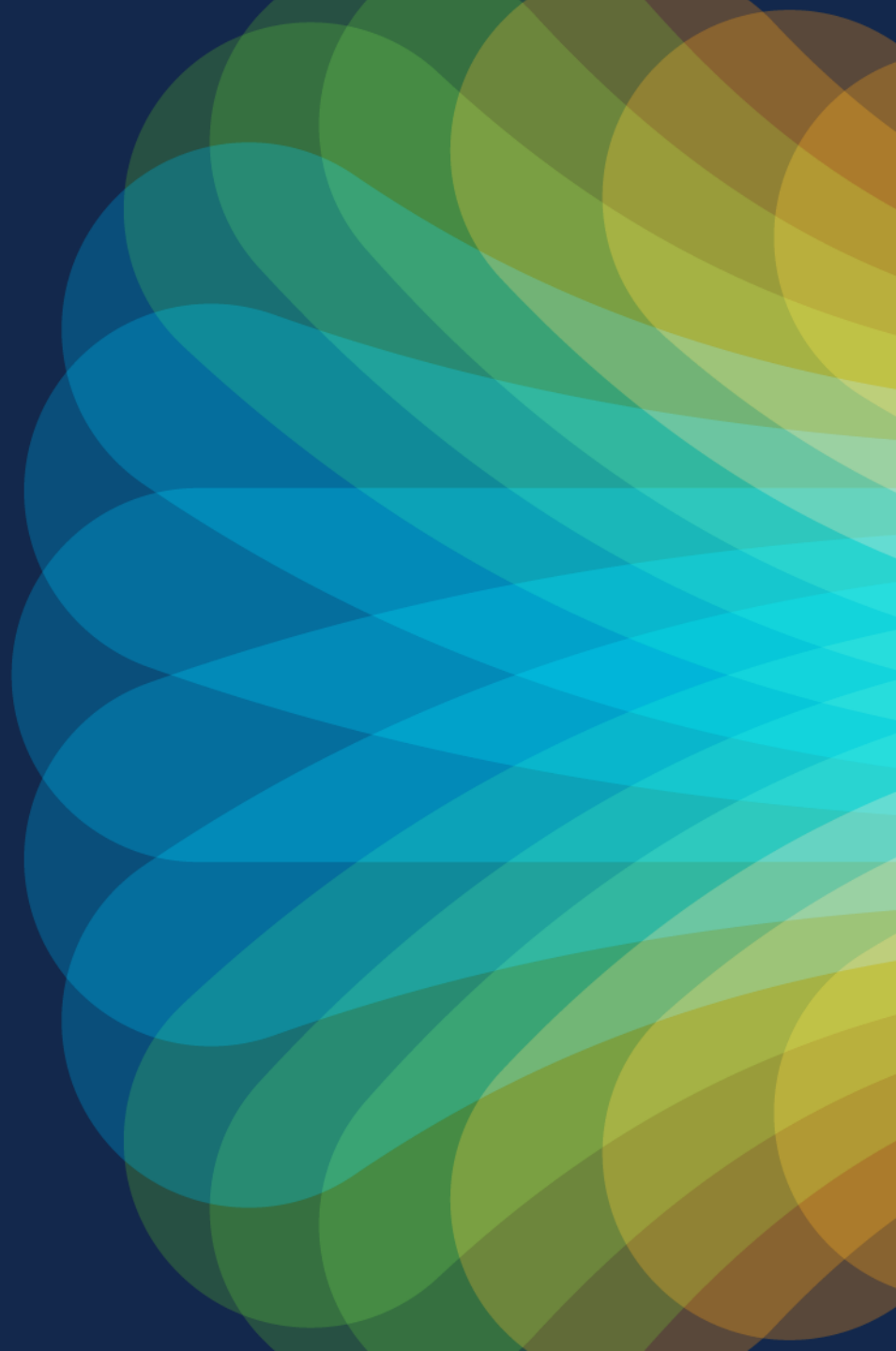
Table of Contents

How To: Integrate Meraki Networks with ISE

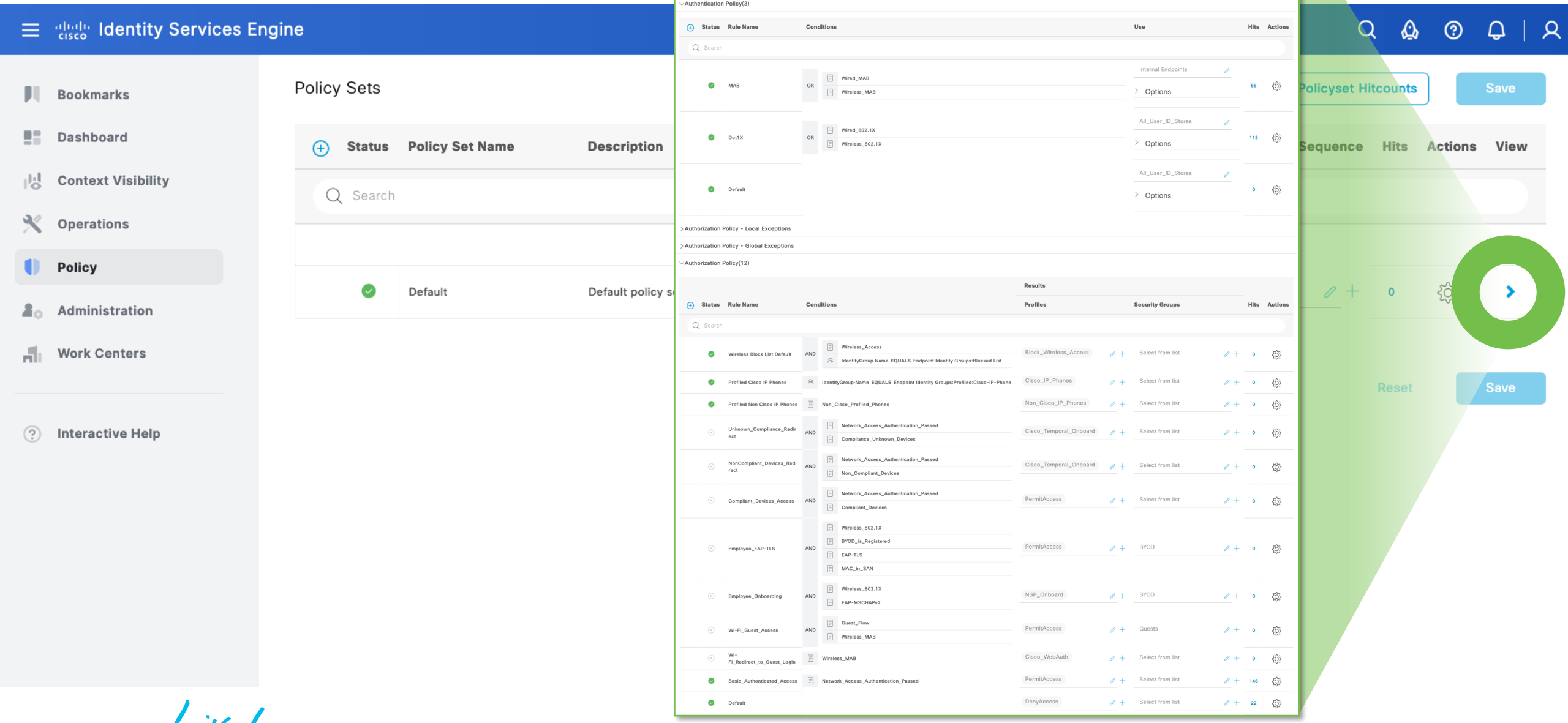
cs.co/ise-meraki



Challenges: Policy



Default Policy Set



Policy Set Authorization Rules

Status	Rule Name	Conditions	Profiles
☑	Lobby_Ambassadors	*domain.com*:ExternalGroups EQUALS *domain.com*/Users/Ambassadors AND Work_Hours	PermitAccess & Ambassadors
☑	Engineers	*domain.com*:ExternalGroups EQUALS *domain.com*/Users/Engineering	PermitAccess & Engineering
☑	HR	*domain.com*:ExternalGroups EQUALS *domain.com*/Users/HR	PermitAccess & HR
☑	radius_test	Network Access:Username EQUALS radius_test	DenyAccess
☑	Blocklist	IdentityGroup-Name EQUALS Endpoint Identity Groups:Blocklist	DenyAccess
☑	Employee+Machine	Network Access:EAP Tunnel EQUALS TEAP AND *domain.com*:ExternalGroups EQUALS *domain.com*/Users/Domain Users AND Network Access EapChainingResult EQUALS User and machine both succeeded	PermitAccess
☑	Domain_Computer_Compliant	*domain.com*:ExternalGroups EQUALS *domain.com*/Users/Domain Computers AND Session:PostureStatus == Compliant	Domain_Computer
☑	Domain_Computer_Unknown	*domain.com*:ExternalGroups EQUALS *domain.com*/Users/Domain Computers AND Session:PostureStatus == Unknown	Quarantine
☑	Phones	IdentityGroup·Name == Endpoint Identity Groups:Cisco-IP-Phone	one & Phone
☑	Cameras	Wireless_MAB AND IdentityGroup-Name EQUALS Endpoint Identity Groups:Cameras	Surveillance
☑	Guest_Wireless	RADIUS:Called-Station-ID ENDS_WITH Guest AND Guest_Flow	Internet_Only & Guest
☑	VPN_Employees	Radius:NAS-Port-Type EQUALS Virtual	PermitAccess
☑	Fabrication_Plant	Device:Location EQUALS All Locations:Fabrication	Manufacturing
☑	Default		DenyAccess

Why

When

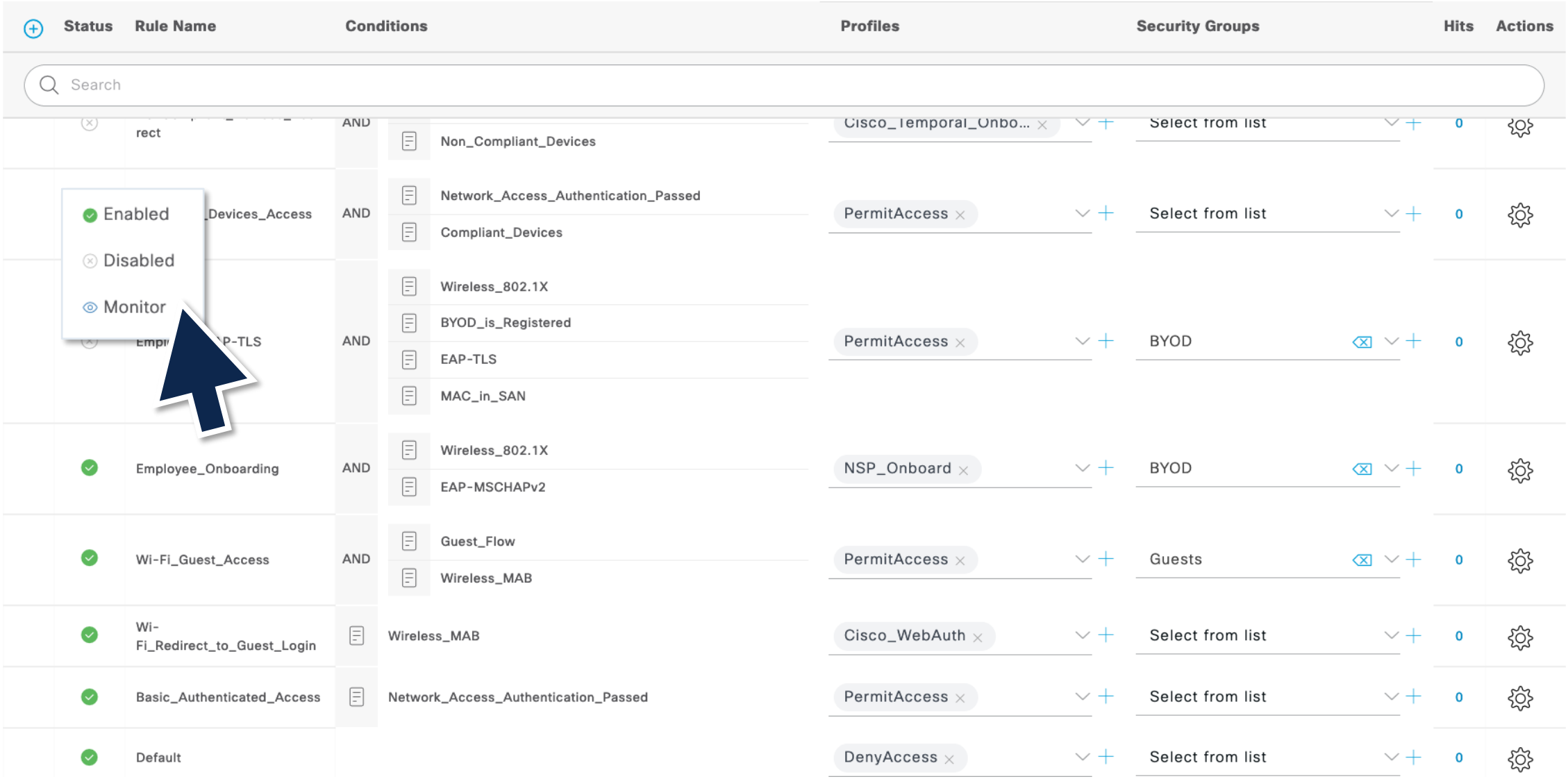
Who

What

Where

How Much

Monitoring Authorization Rules



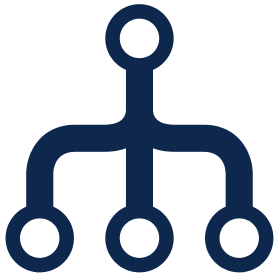
Organizing Your Network Devices and Policies

Network Access Type

- Wired
- Wireless
- VPN
- Branch

Location

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



Organization

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

Vendor / Model

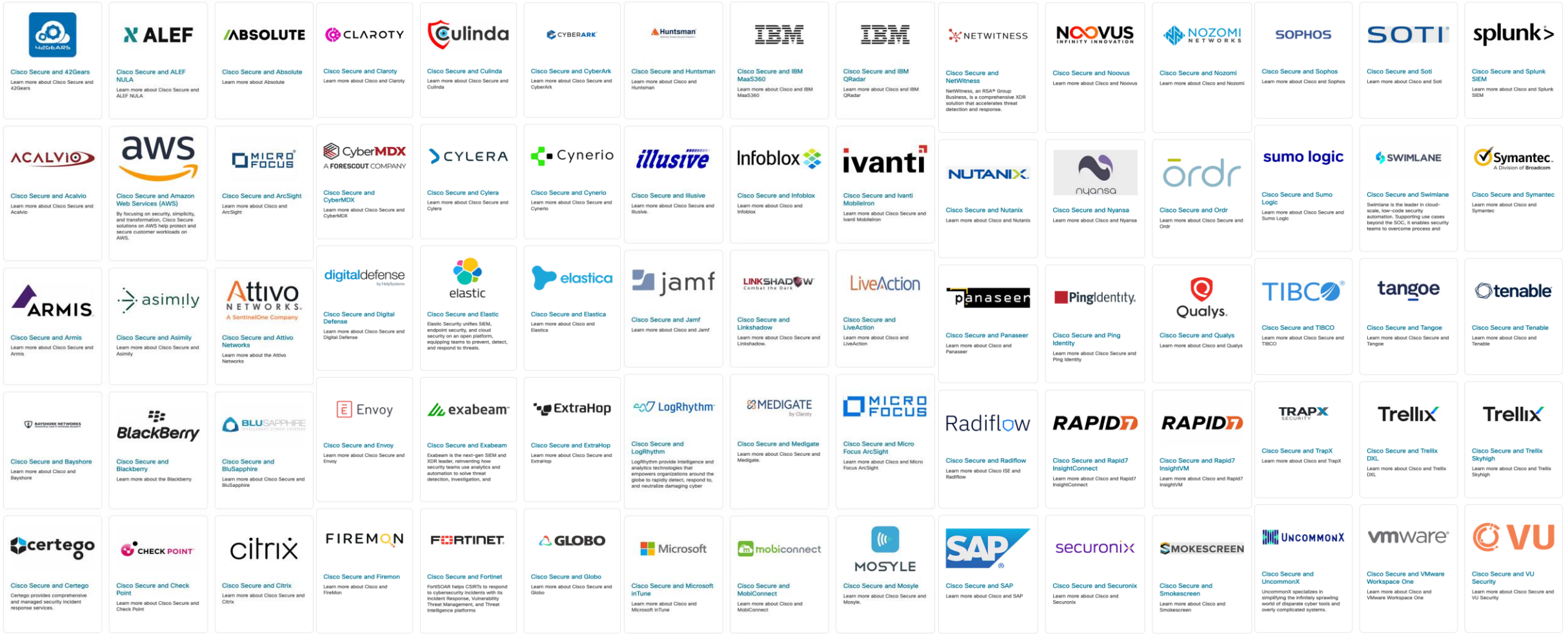
- Cisco
  - Catalyst
  - Meraki
- Aruba
- Juniper

“Always be labbing.”

Katherine McNamara

ISE Cisco Security Technical Alliance (CSTA)

Dec 2023



cisco.com/go/csta

pxGrid | pxGrid Cloud | pxGrid Direct

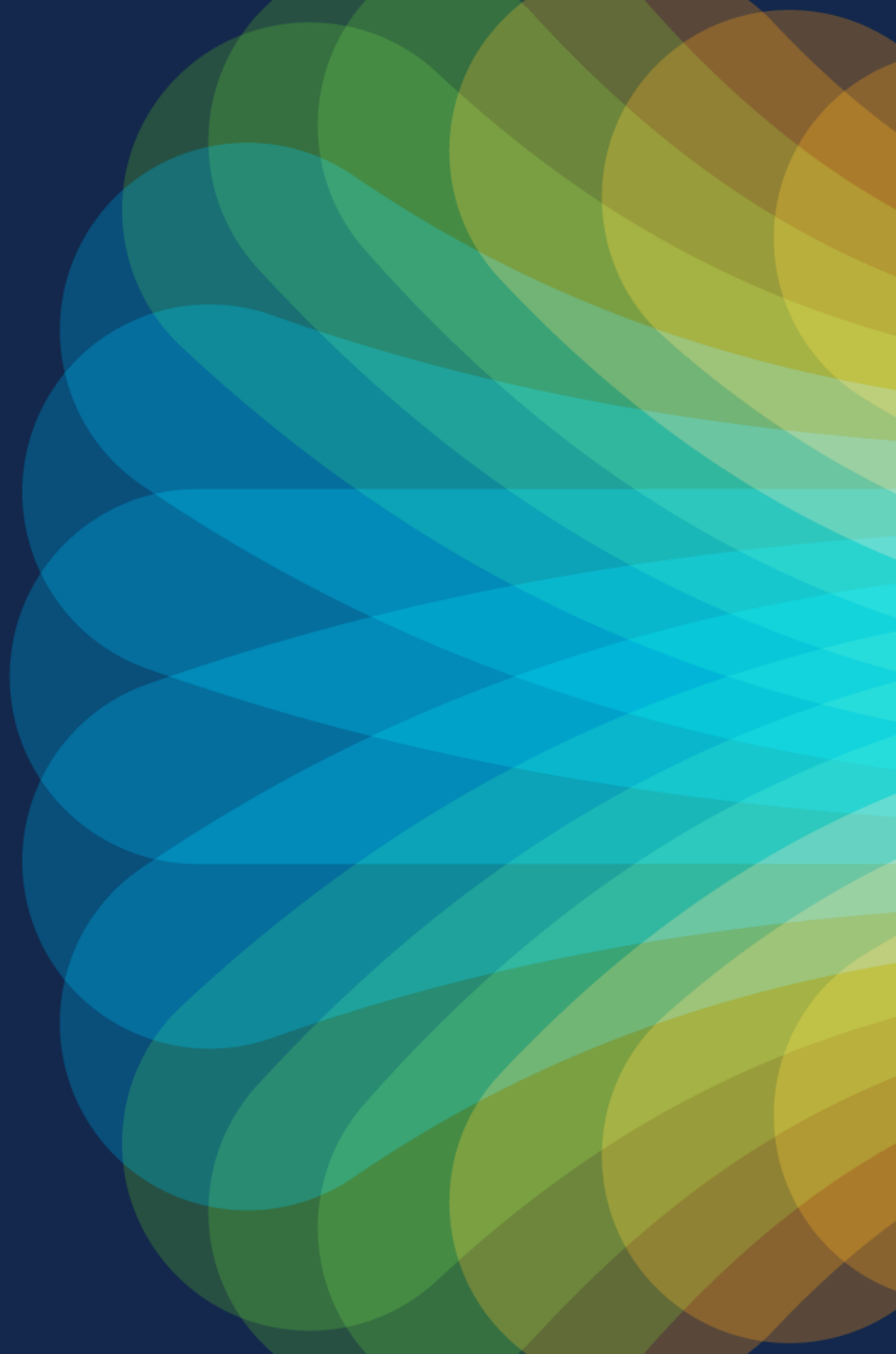
ISE Security Ecosystem Integration Guides

Dec 2023

Tags: cs.co/ise-guides#*tag*

42Gears | AAD | AD | Acalvio | ACI | Active-Directory | ANC | adaptive-network-control | adaptive-policy | AIEA | AirWatch | Alef | Amazon | AMP | analytics | Android | Ansible | AnyConnect | API | APIs | APIC-DC | APIC | APICDC | Apple | appliance | Arista | Armis | Aruba | ASA | Asimily | ASR | Avaya | AWS | Azure | AzureAD | Bayshore | Blusapphire | Brocade | BYOD | CAIEA | Catalyst | Catalyst-Center | CC | CCC | CCV | Certego | certificate | certificates | certs | Checkpoint | Chromebook | CIMC | Cisco | Claroty | Cognitive | compliance | CSC | CSE | CSM | CTA | CyberArk | CyberObserver | CyberVision | Cylera | Cynerio | data-connect | DataConnect | DeceptionGrid | deployment | developer | DevNet | DFLabs | DNA | DNAC | Duo | EA | EAP-FAST | EAP-TLS | EAP | eduroam | ELK | EntraID | Envoy | errors | ExtraHop | Extreme | F5 | FAST | features | Firepower | FMC | Firewall | FTD | Forescout | Fortinet | FTD | FW | Good | Google | guides | HP | Huawei | Hyper-V | IBM | IBNS | icons | Incman | IND | InfoBlox | instance | intro | introduction | Intune | iPad | iPadOS | iPhone | ip-phones | ipsec | ipsk | ISE | Ivanti | JAMF | JumpCloud | Juniper | Kibana | KVM | labs | LDAP | LinkShadow | LiveAction | lb | load-balancing | log-analytics | logging | logs | Logzilla | MaaS360 | macOS | MAB | McAfee | MDM | Medigate | MEM | Meraki | Microsoft | EntraID | MicroTik | MobileIron | mobility | Motorola | MR | MS | MX | MySQL | Nessus | NetScaler | network-analytics | NGFW | Nozomi | Nutanix | OCI | ODBC | Okta | operations | Oracle | OracleCloud | ORDR | PAN | Palo-Alto | partners | passive | passive-id | PEAP | pfSense | phones | PI | PIC | Ping | PKI | PNG | Postman | posture | prescriptive | Prime | products | proxy | PXG | PXGC | PXGD | pxgrid-cloud | pxgrid-direct | pxGrid | QRadar | Qualys | Radiflow | RADIUS_CLI | RADIUS_Proxy | radius-simulation | RADIUS | Rapid7 | REST | Rockwell | RSA | Ruckus | SCCM | sd-access | SD-Access | SDA | secure-access | secure-client | secure-endpoint | secure-network-analytics | secure-workload | security | Securonix | segmentation | ServiceNow | simulation | SM | Smokescreen | SMS | SMTP | SNA | SOTI | Splunk | Stealthwatch | stencils | SVG | SWA | switch | switches | switching | Symantec | syslogs | Systems-Manager | TACACS | | Tanium | TEAP | Tenable | Terraform | Tetration | third-party | ThreatConnect | TLS | TrapX | troubleshoot | troubleshooting | trustsec | TrustSec | UCS | Umbrella | upgrade | split-upgrade | vCenter | Visio | VM | VMware | VOIP | web-appliance | Webex | WebexRoomNavigator | windows | wireless | WLC | Workload | WSA | WSUS | XenMobile | XTENDISE | zero-touch | ZTP

Planning: Platforms



ISE Nodes – Mix and Match

cs.co/ise-scale

Physical Appliances	Virtual Machines	Cloud Instances

SNS-3795
SNS-3755
SNS-3715
SNS-3695
SNS-3655
SNS-3615
SNS-3595

KVM

Microsoft

NUTANIX

vmware

aws

Azure

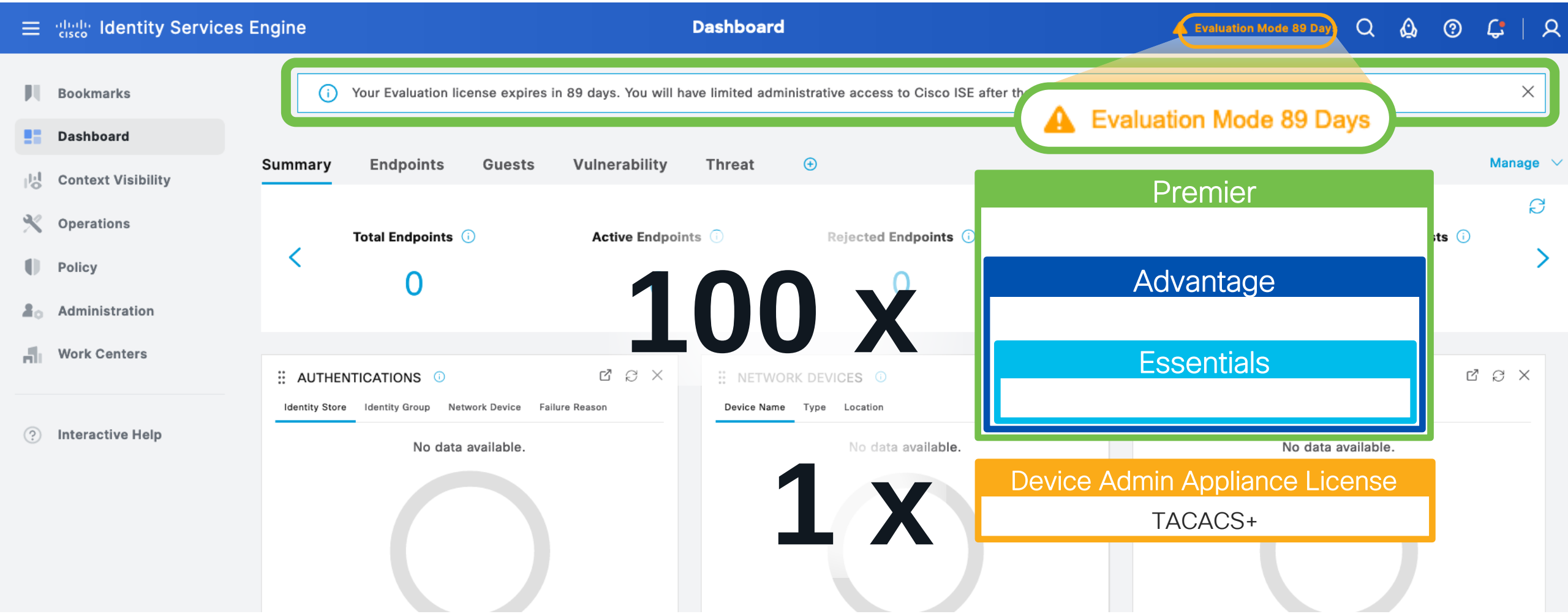
ORACLE

Future

Google

Free, 90-day ISE Evaluation Licenses!

cs.co/ise-licensing



Appliance versus VM

	Appliance	Virtual Machine
Pros	• Dedicated HW Resources • “Network Device” vs Compute	• Rapid deployment • Flexible HW resources • 10X+ R/W with SSD for MnT • MnT Storage up to 2.4TB
Cons	• Static HW Resources • No SSD – spinning disks only • Ordering, Shipping, Racking • Remote management	• Resource Reservation Failure!!

ISE Appliances vs VMs vs Cloud Deployment Comparison

On-Premises versus Cloud

	On-Premises	Cloud
Pros	• Control	• Rapid deployment • Flexible HW resources • Simple, pay-as-you-go billing • Automation
Cons	• Plan ahead • Procurement • Automation?	• Learning curve • Security • Surprise bills

ISE Appliances vs VMs vs Cloud Deployment Comparison

ISE Architecture

cs.co/ise-scale

Standalone ISE

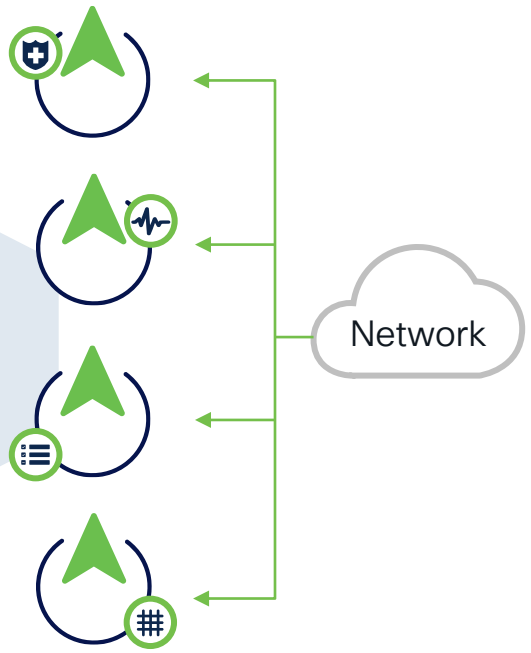
Policy Administration Node (PAN)
- Single plane of glass for ISE admin
- Replication hub for all config changes

Monitoring & Troubleshooting Node (MnT)
- Reporting and logging node
- Syslog collector from ISE Nodes

Policy Services Node (PSN)
- Makes policy decisions
- RADIUS / TACACS+ Servers

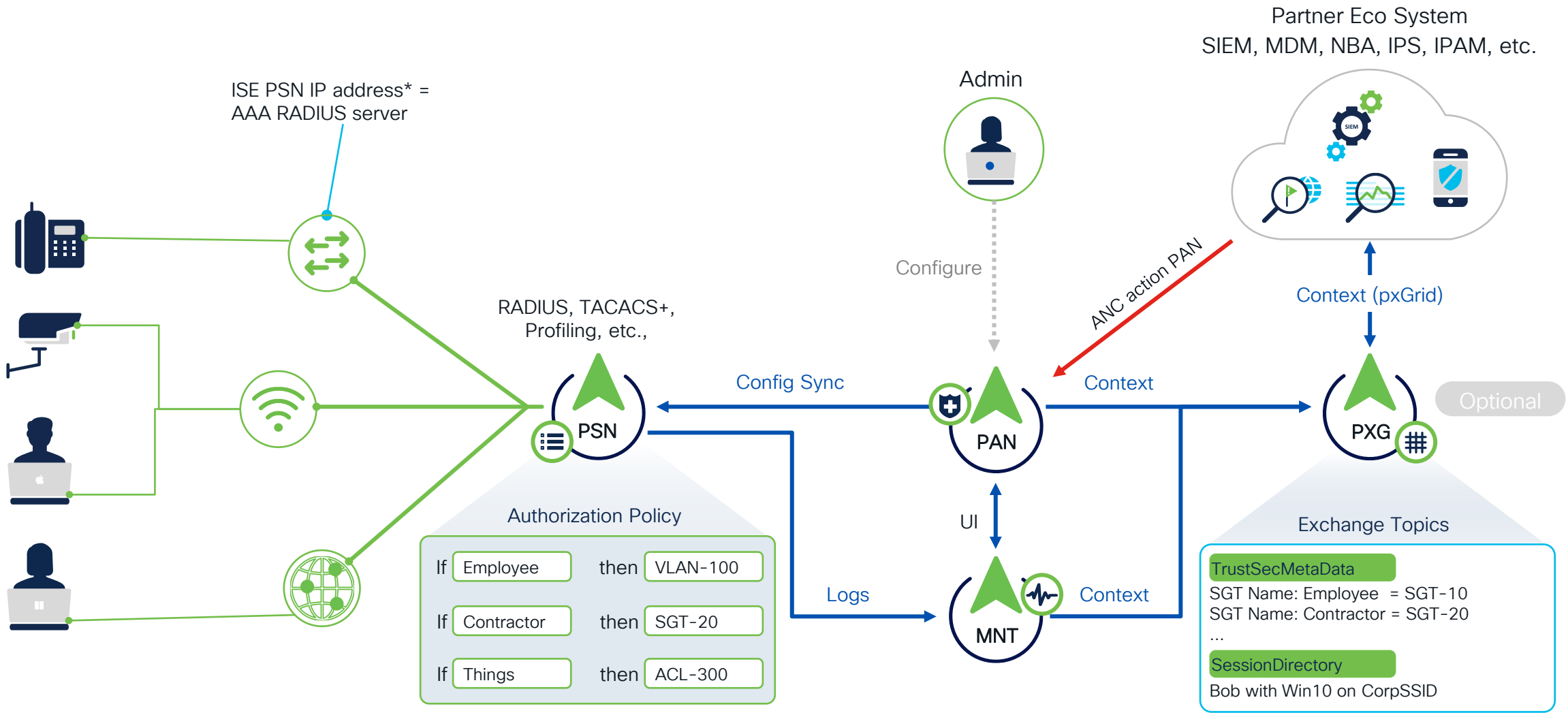
pxGrid Controller (PXG)
- Facilitates sharing of context

Distributed ISE



Single Node (Virtual/Appliance)		Multiple Nodes (Virtual/Appliance)
Up to 50,000 concurrent endpoints	3700	Up to 2,000,000 concurrent endpoints
Up to 50,000 concurrent endpoints	3600	Up to 2,000,000 concurrent endpoints
Up to 20,000 concurrent endpoints	3500	Up to 500,000 concurrent endpoints

ISE Node Personas... Explained

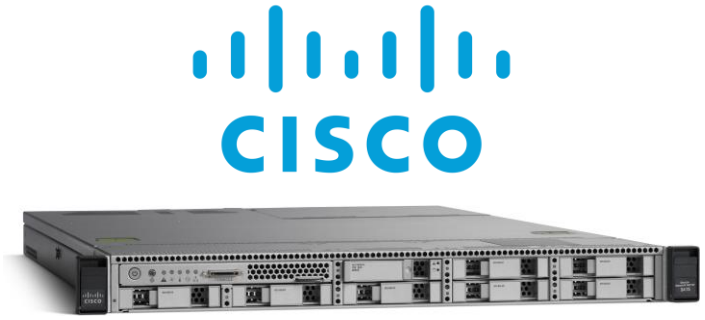


*PSNs can optionally be behind a load-balancer and can be accessed via Load Balancer Virtual IP address (VIPs)

Zero Touch Provisioning

cs.co/ise-ztp

ISE 3.1



SNS Appliances
w/ CIMC

ESXi

Cloud

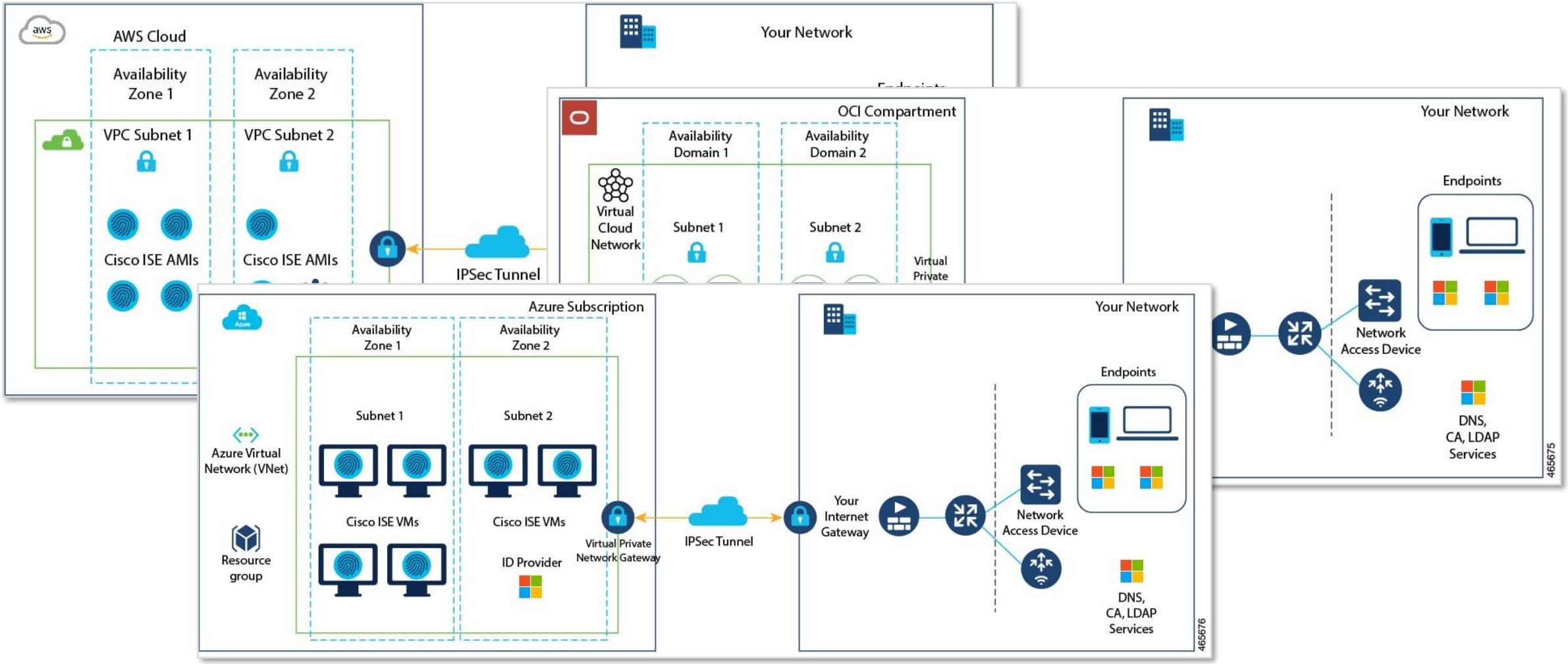
Use configuration
ISO/IMG file mount

Native APIs

CIMC – Cisco Integrated Management Controller

Deploy Cisco ISE Natively on Cloud Platforms

cs.co/ise-on-cloud

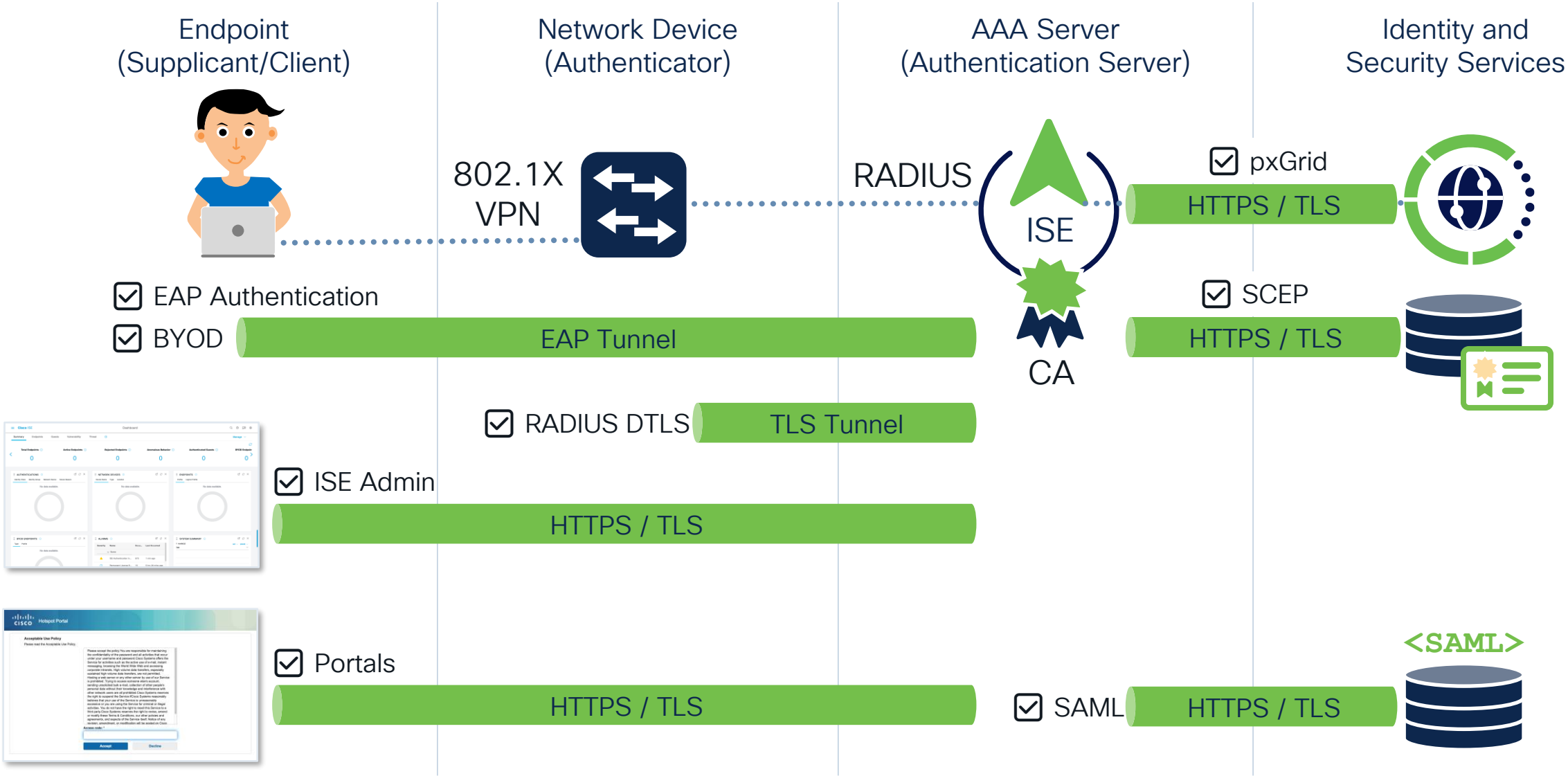


Enforcement Options

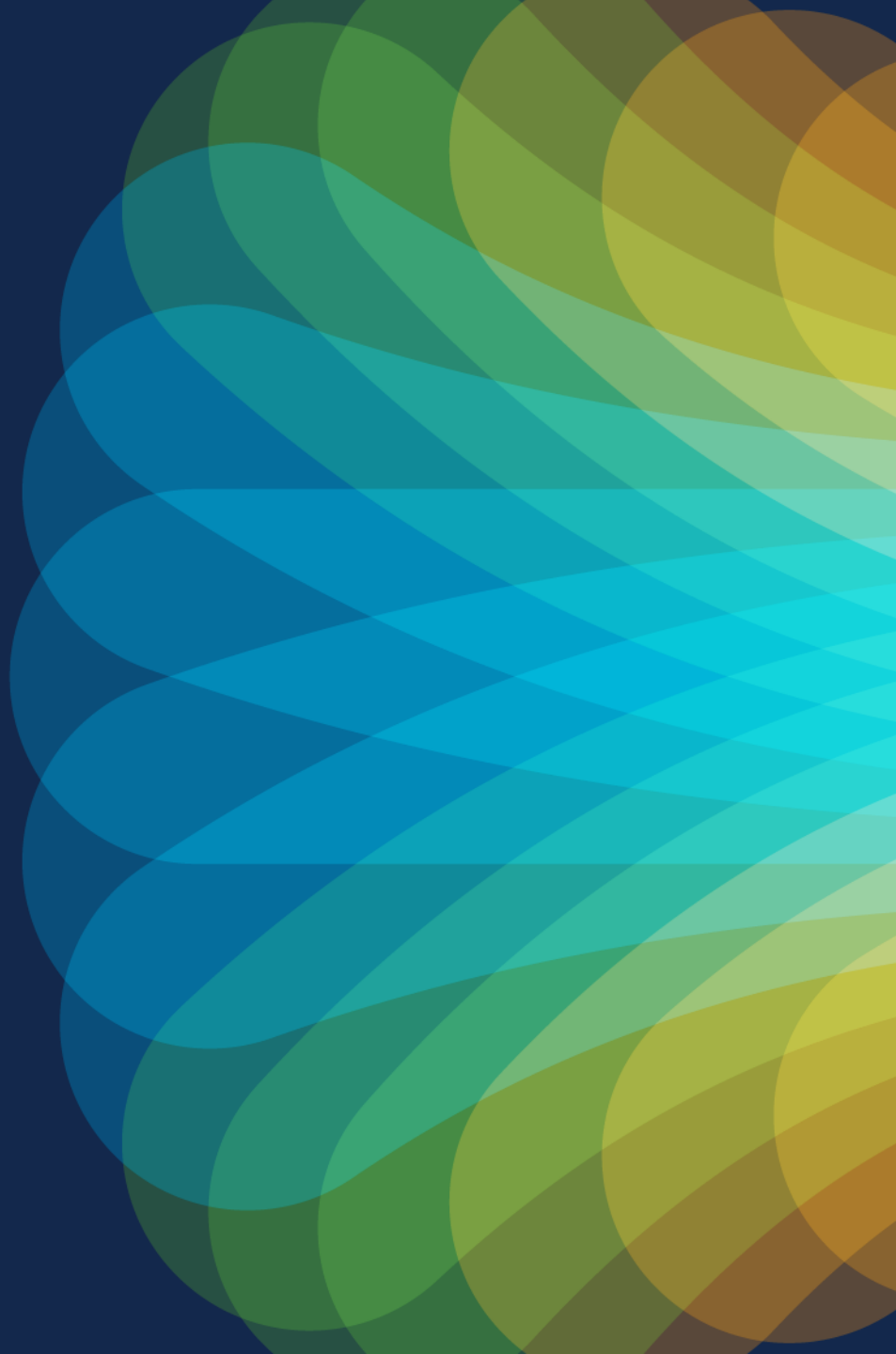
cs.co/ise-wired

	Monitor	Low-Impact	Closed
Why?	Visibility: profiling, supplicant configuration, bad credentials, certs	Differentiate access with ISE authorization policy	IEEE 802.1X specification
Switchport	authentication host-mode multi-auth authentication open	authentication host-mode multi-auth	authentication host-mode multi-auth
Before Authentication	Port Open Unconditionally	Traffic subject to Pre-Auth ACL: DNS, DHCP, PXE, etc.	EAP Only
After Authentication	Port Open Unconditionally (Access-Reject ignored)	ISE response	ISE response
Profiling?	Yes	Yes	After Authentication
Guests?	Yes	Yes, redirect to hotspot or self-registration	Requires Sponsor

Digital Certificates are ⚠ CRITICAL ⚠



Planning: Sizing & Scale



ISE Deployment Scale

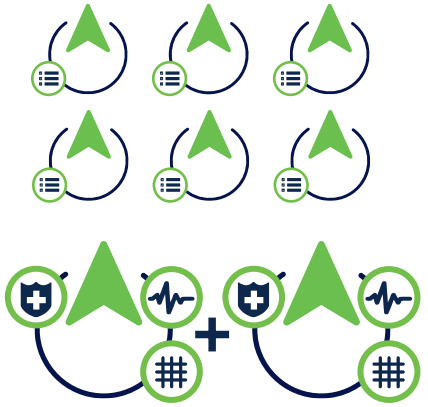
cs.co/ise-scale

Standalone to Distributed

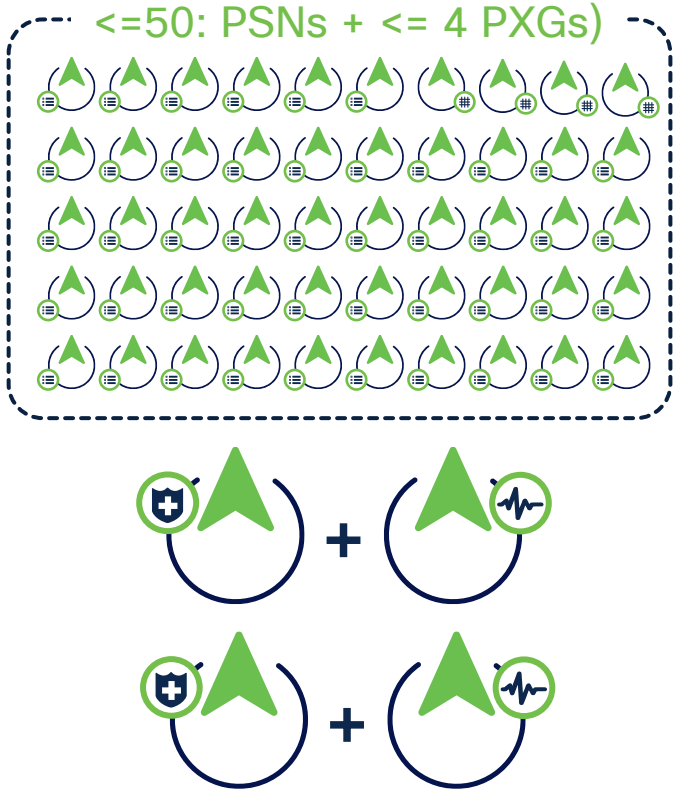
- Same for physical and virtual deployments
- Compatible with load balancers
- No changes to current Licensing Model

Eval / Demo / Lab

Small HA Deployment
2 x (PAN+MNT+PSN) + 1 x PSN



Medium Multi-node Deployment
2 x (PAN+MNT+PXG), <= 6 PSN



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

3700	100 Endpoints	Up to 50,000 Endpoints	Up to 2,000,000 Endpoints
3600	100 Endpoints	Up to 50,000 Endpoints	Up to 2,000,000 Endpoints
3595	100 Endpoints	Up to 20,000 Endpoints	Up to 500,000 Endpoints

ISE Performance & Scale

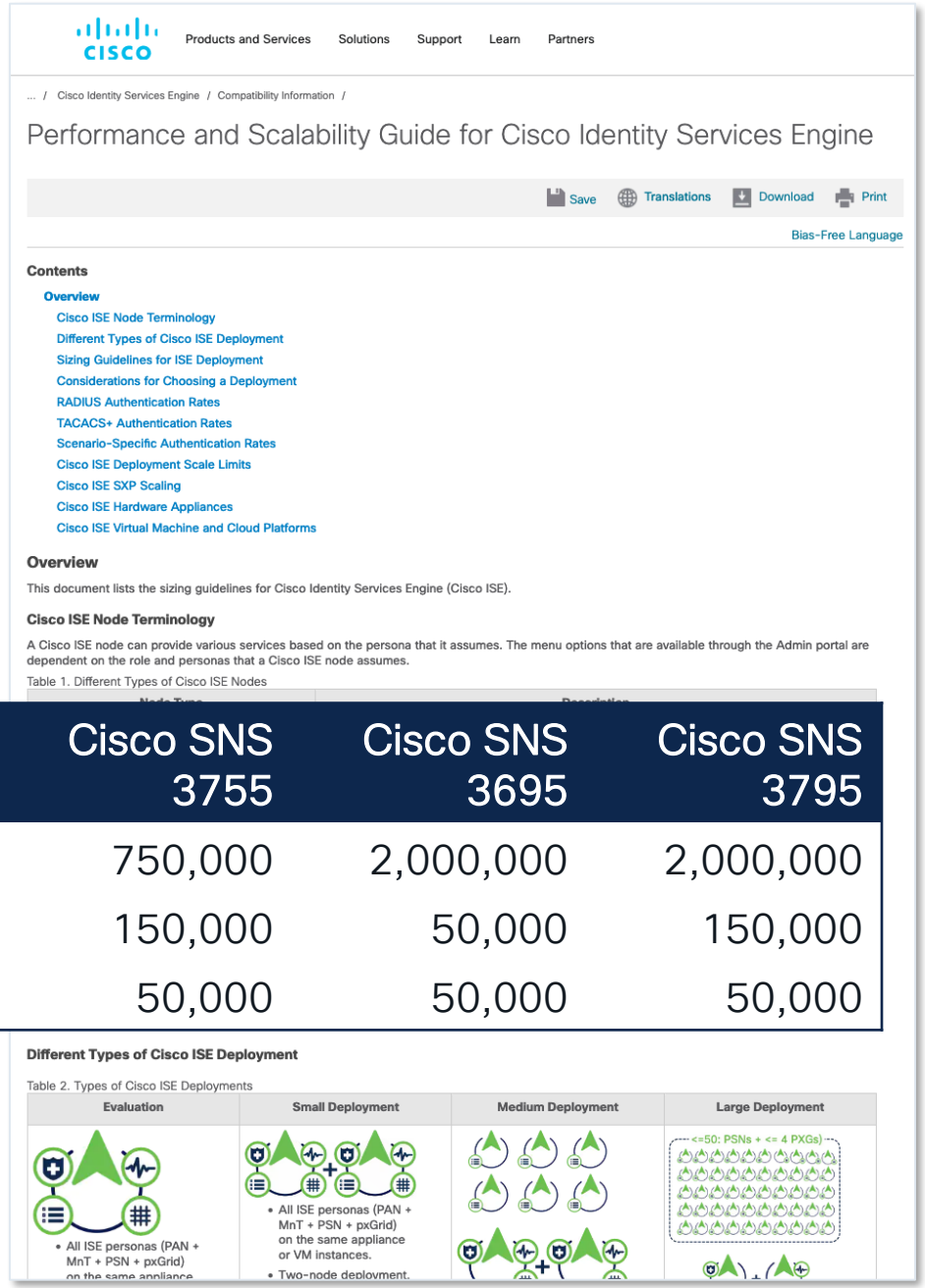
Maximum Concurrent Active Sessions

- ISE Licensing counts *active endpoint sessions*
- RADIUS Accounting defines session Start & Stop events
- Sessions **Start** upon RADIUS Authorization
- Sessions **Stop** upon :
  1) Disconnect 2) Session Expiration 3) Idle Timeout

Table 3. Maximum Concurrent Active Sessions for Deployments

Deployment	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Large	500,000	Unsupported	Unsupported	500,000	750,000	2,000,000	2,000,000
Medium	20,000	12,500	75,000	25,000	150,000	50,000	150,000
Small	20,000	12,500	25,000	25,000	50,000	50,000	50,000

cs.co/ise-scale



Steady State versus Peak Demand

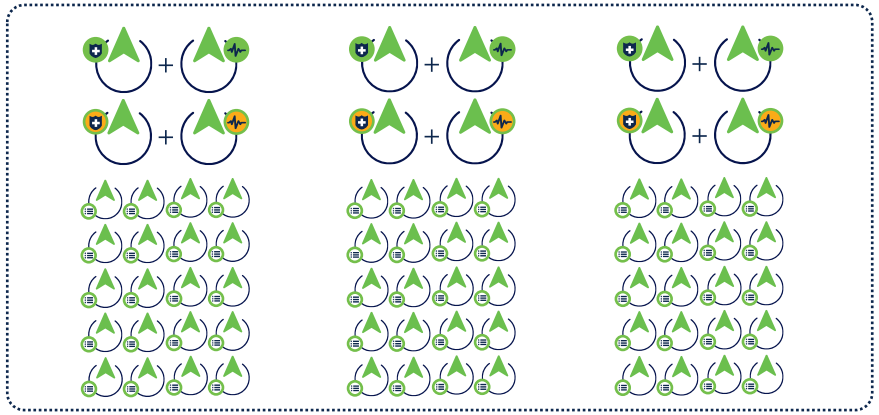
- You will have a mix of **static** and **mobile** endpoints
- Some endpoints are always on with long (8+ hours) session expirations
- Usage patterns will cause regional and periodic **ebbs, flows, and spikes**
  - Increased regional activity “follows the sun”
  - Wireless roaming spikes on the hour to change classrooms and meetings
- Mobile endpoints hibernate & roam causing a **3-10X+ larger load**
- Misconfigured devices can have **100-1000X** larger than average auth load

Table 4. Maximum Concurrent Active Sessions for Different ISE Appliances Acting as PSNs

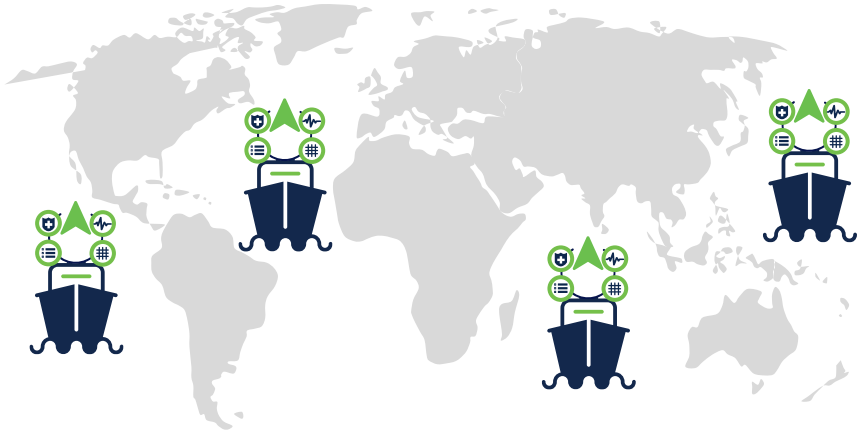
PSN Type	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Dedicated PSN (only PSN persona)	40,000	25,000	50,000	50,000	100,000	100,000	100,000
Shared PSN (multiple personas)	20,000	12,500	25,000	25,000	50,000	50,000	50,000

Multiple ISE Deployments?

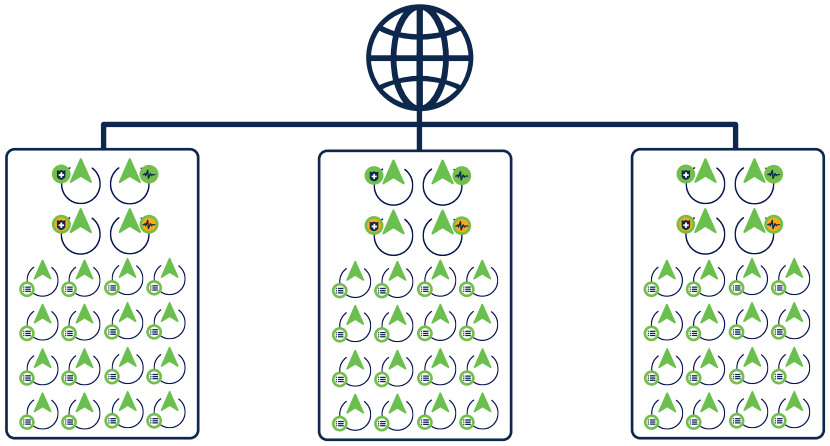
Scale (>2M endpoints)



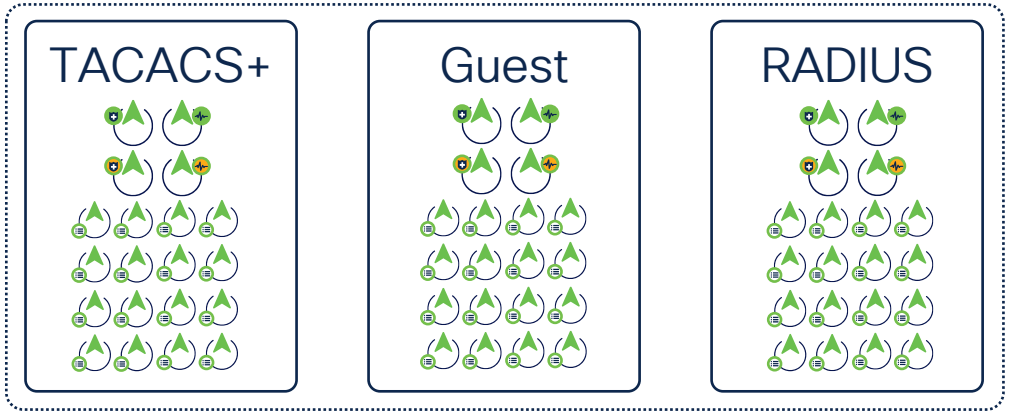
Latency (>300ms)



Regional / Organizational



Services (security / reliability)

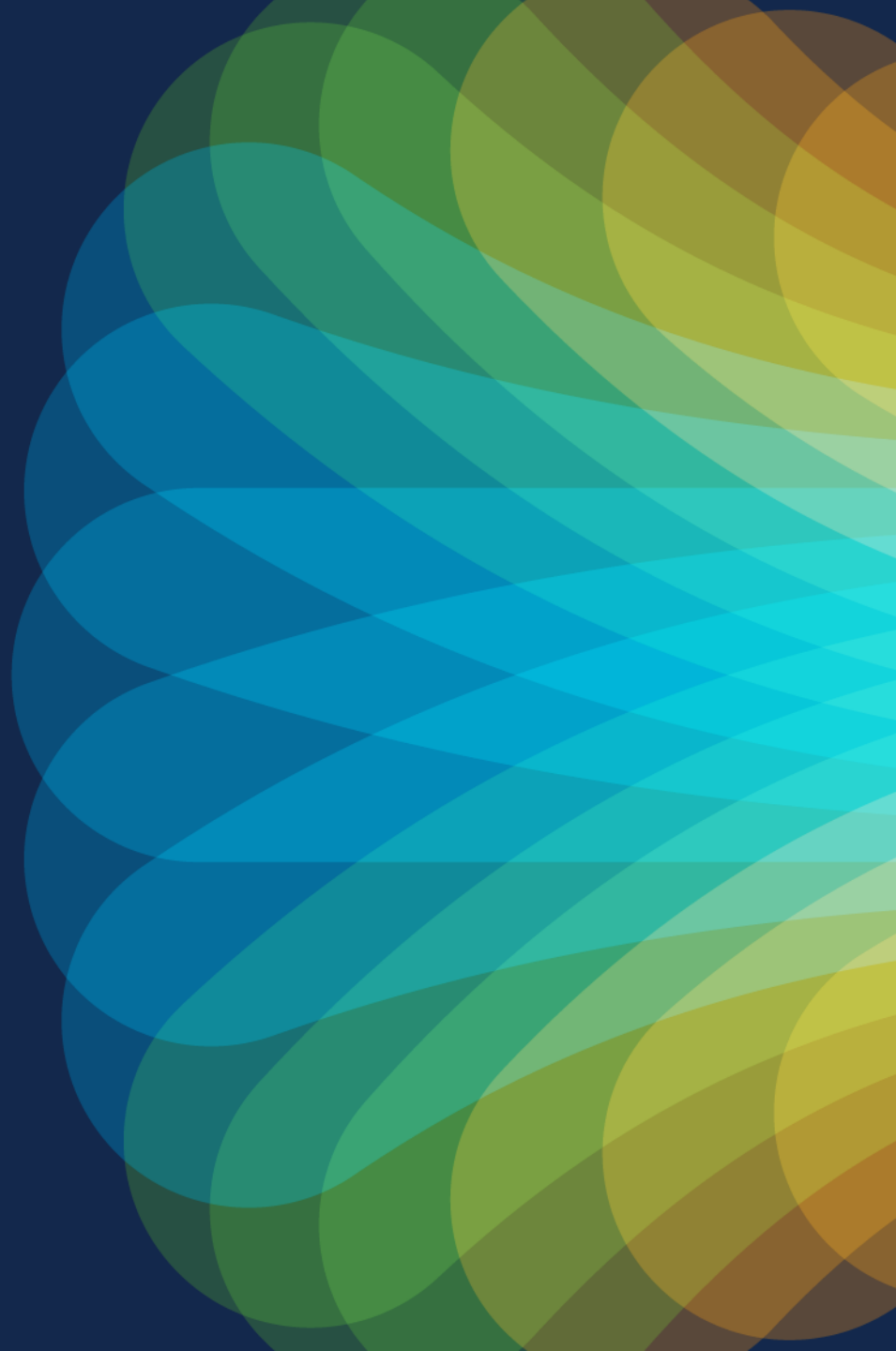


No ISE “Manager of Managers” (MOM)!

Other Scaling Considerations

- ISE PAN: Policy Sets and Authorization Rule Optimization, AuthzProfiles
- ISE MNT: Log Filtering
- ISE PSNs: EAP Protocols, Profiling Probes, Node Groups, Collection Filters
- Network Devices: Load Balancing, Identity Stores, Misconfiguration, Accounting, Timers, Timeouts, EAP/Stateless Session Resume, Fast Reconnect, ACLs, SGTs/SGACLs, Bugs
- Mobile Endpoints: High re-auth rates (hibernation and roaming), misconfigured passwords, untrusted certificates
- Automation: TACACS for Admins vs Tools
- Bugs

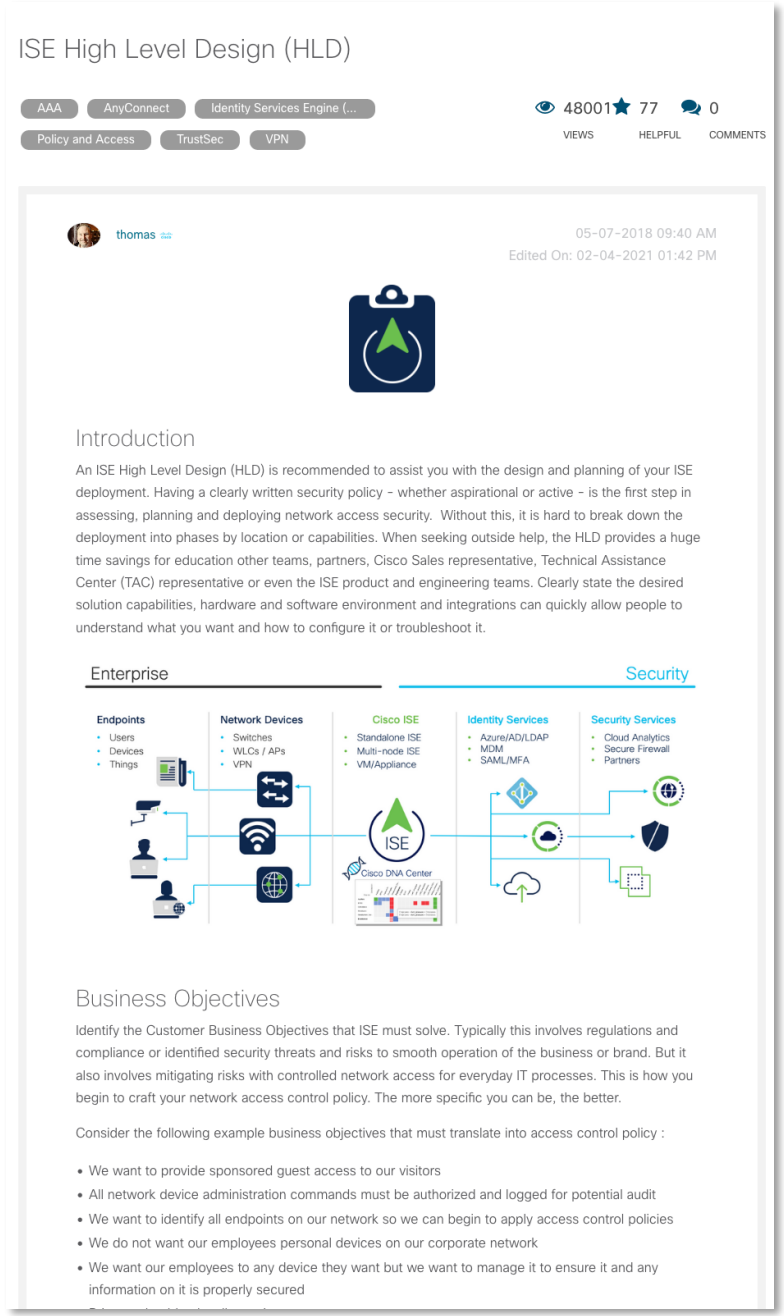
Planning: Lab



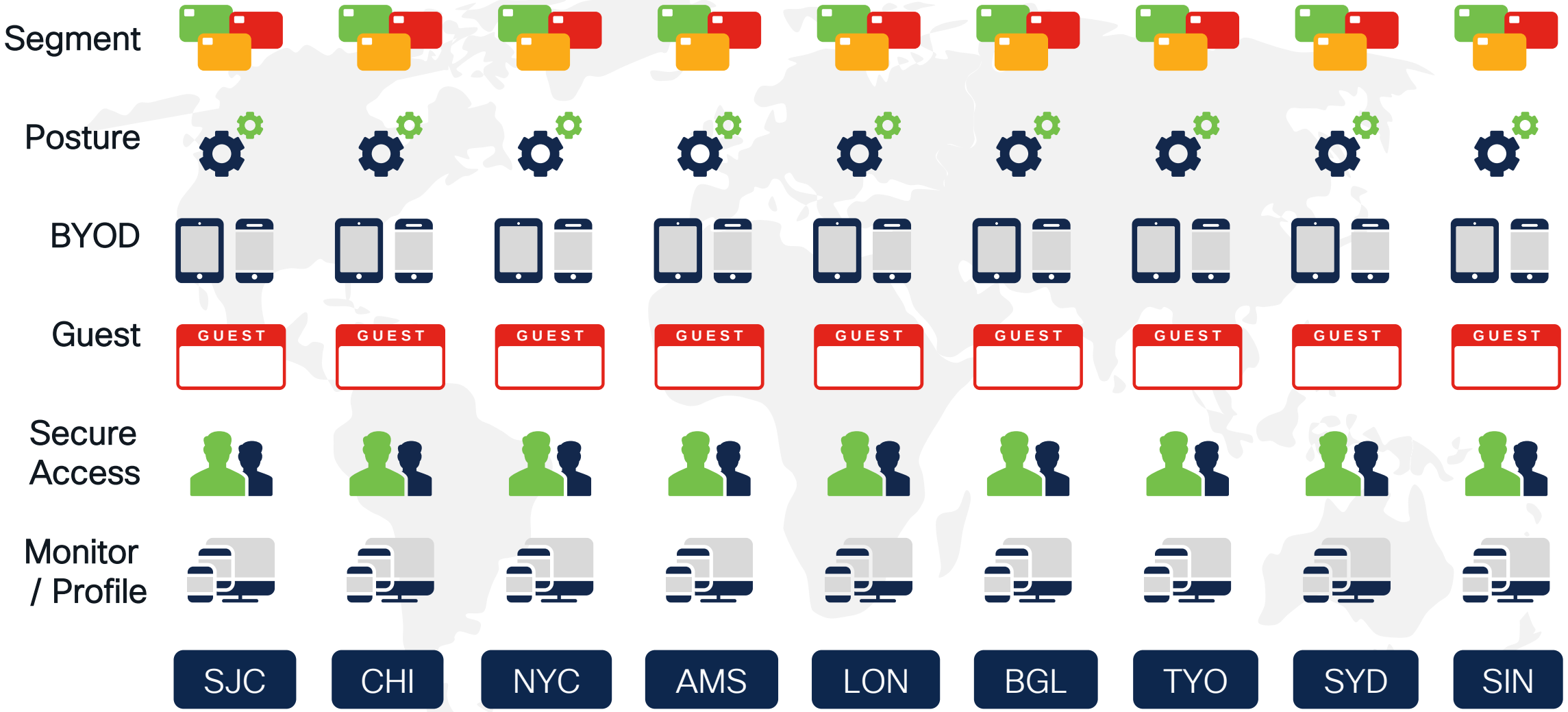
Cisco ISE High Level Design (HLD)

cs.co/ise-hld

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



Deployment by Location vs Scenario



ISE Deployment: Standalone

Role: **Standalone**

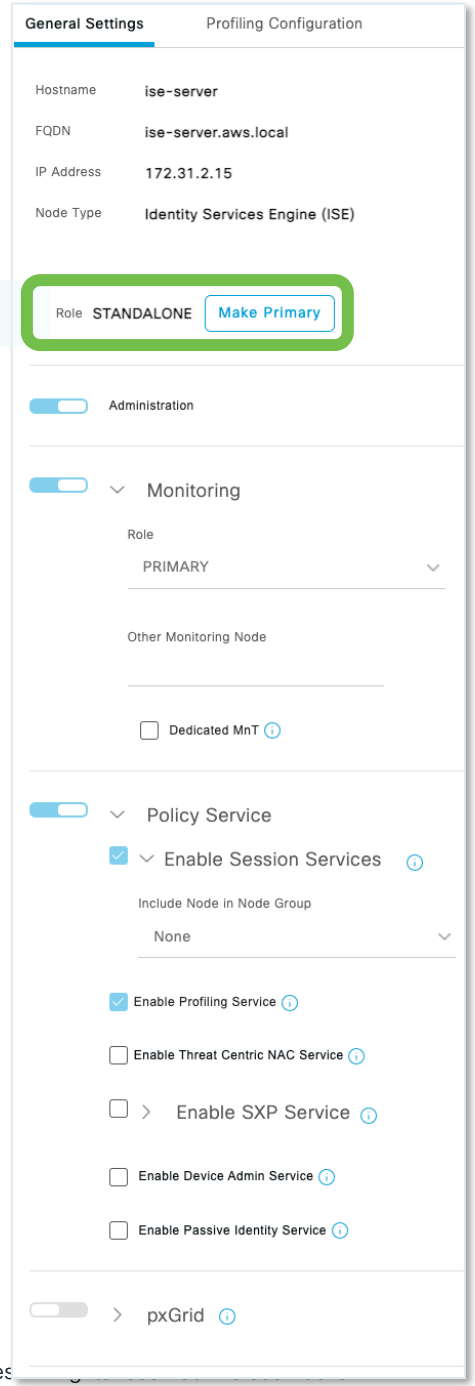
- May run *all* ISE services
- Not joined to a deployment

Demos & Labs!

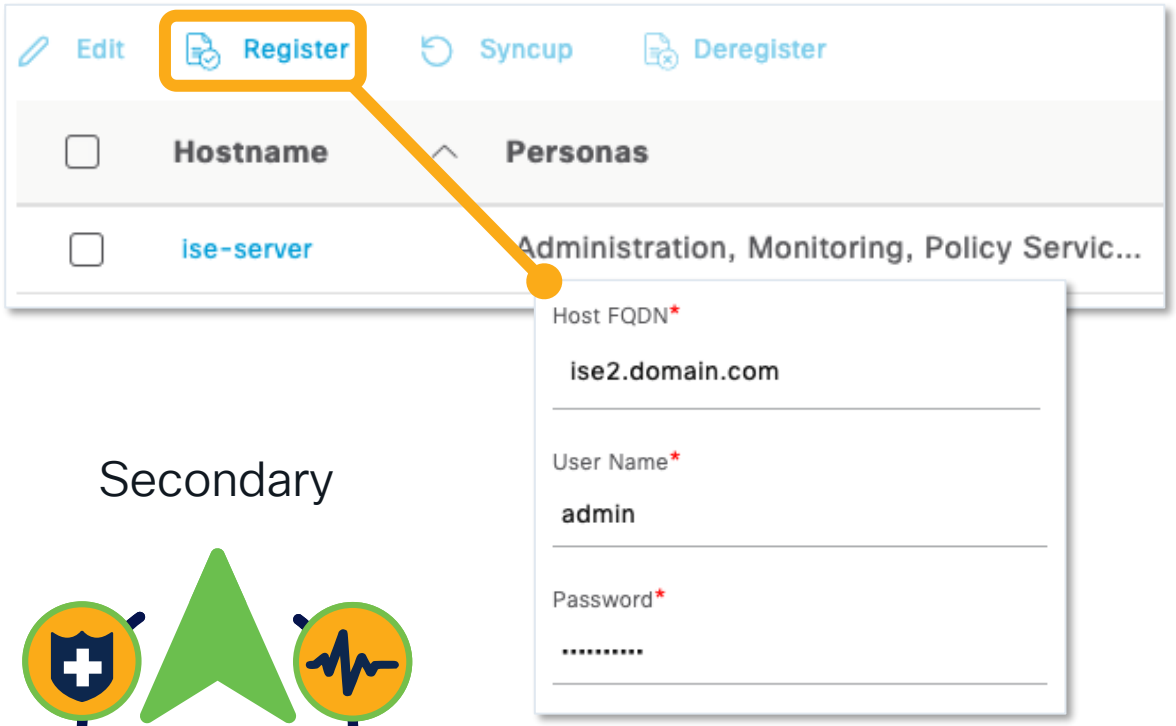
ISE Deployment: Small

Primary

PPAN
PMNT



ISE Deployment: Small



ISE Deployment: Small 3 Node

ISE Deployment: Medium

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

ISE Deployment: Medium

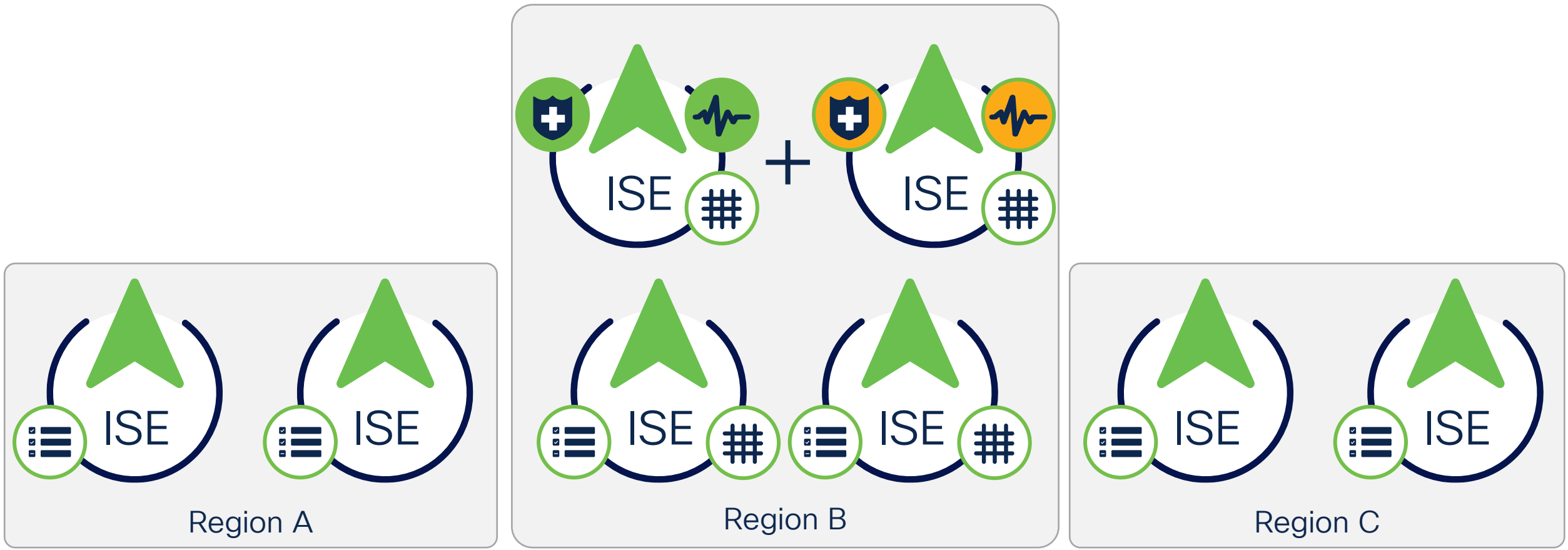
2 x (PAN+MNT+PXG), <= 6 PSN

ISE Deployment: Medium

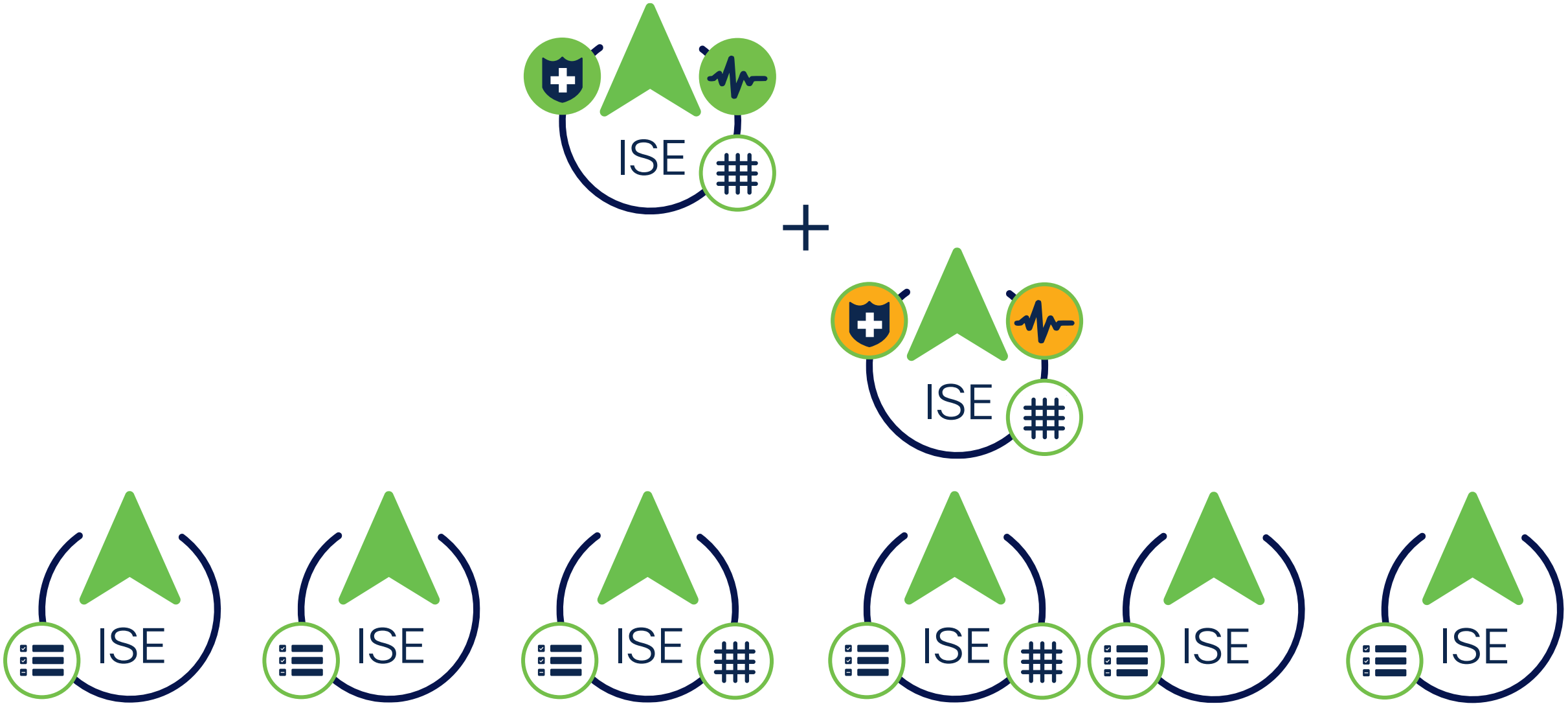
2 x (PAN+MNT+PXG), <= 6 PSN

ISE Deployment: Medium

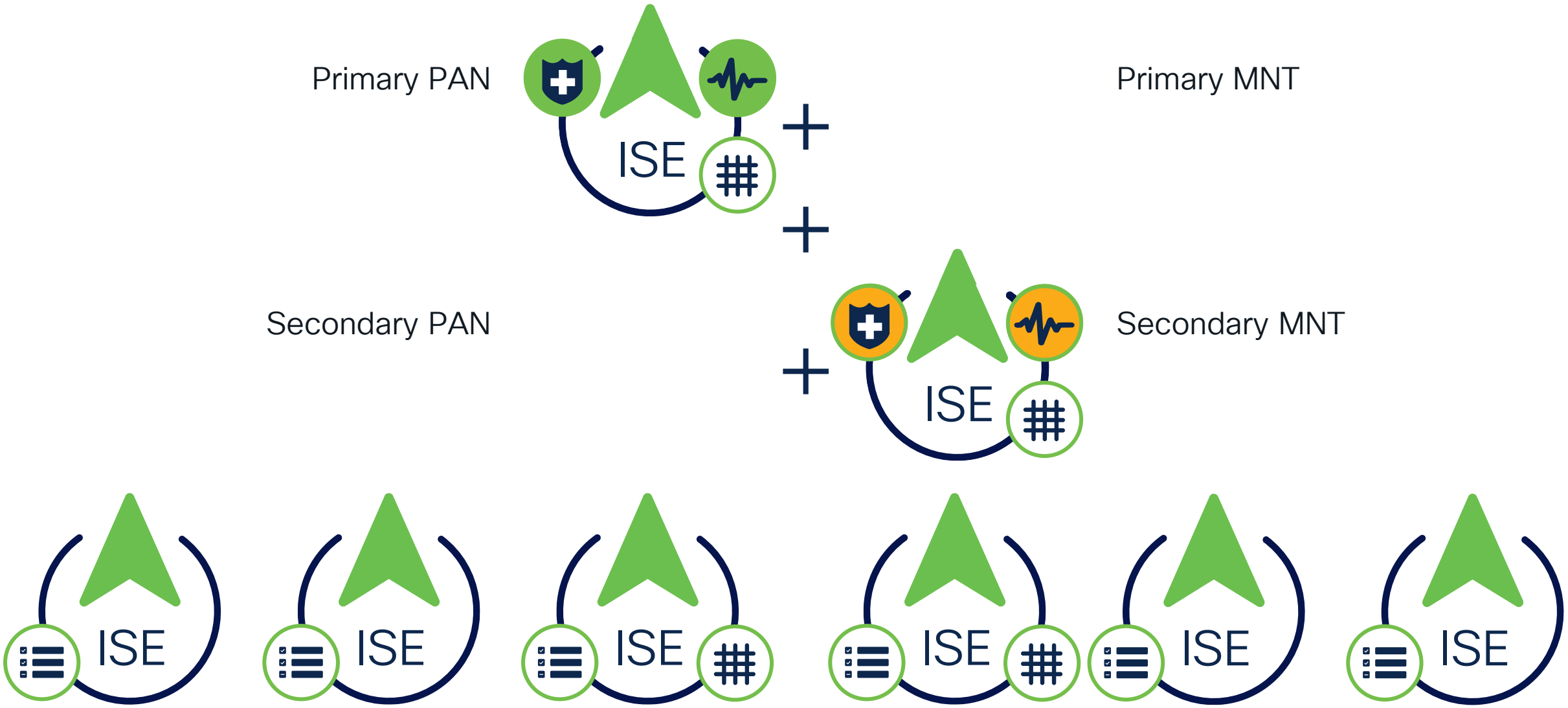
2 x (PAN+MNT+PXG), <= 6 PSN



ISE Deployment: Medium => Large

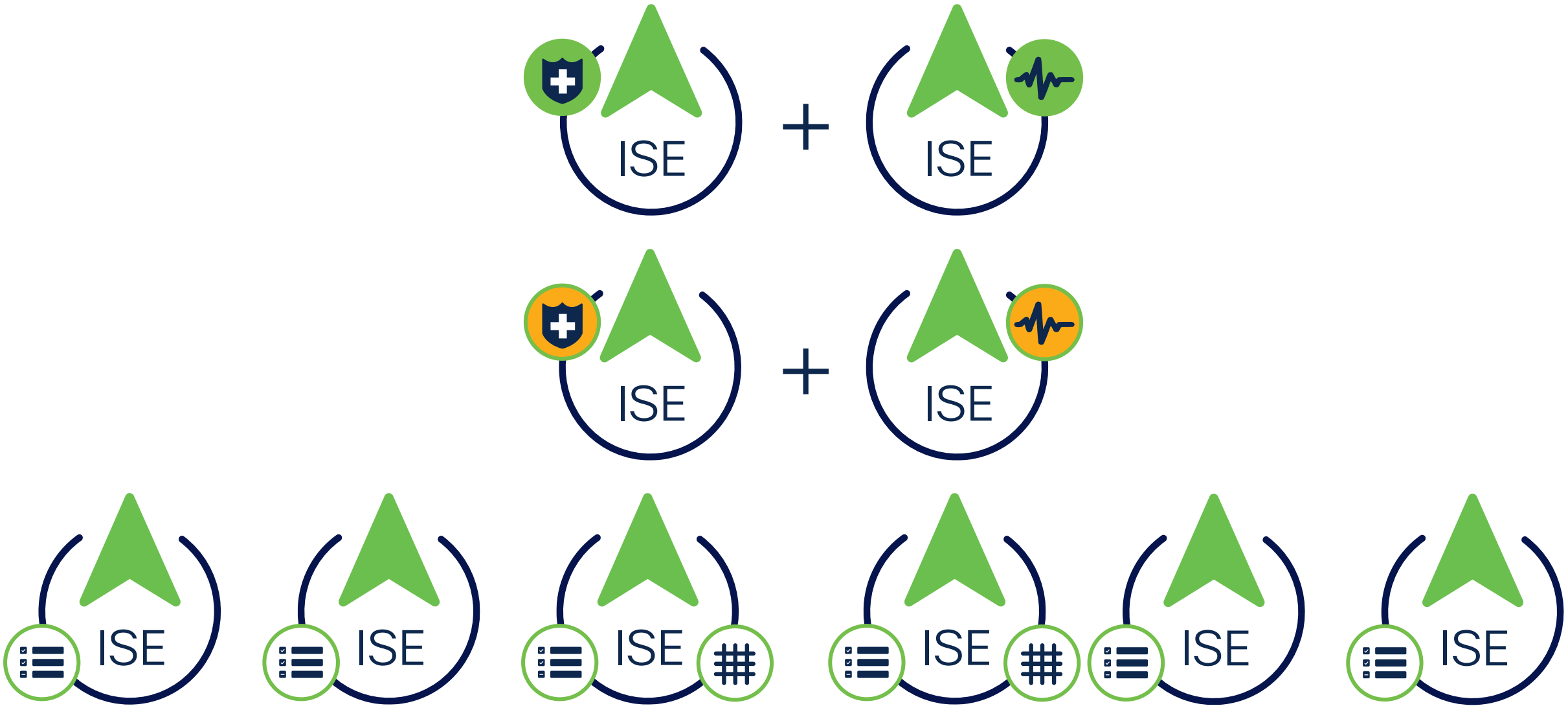


ISE Deployment: Medium => Large



ISE Deployment: Large

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

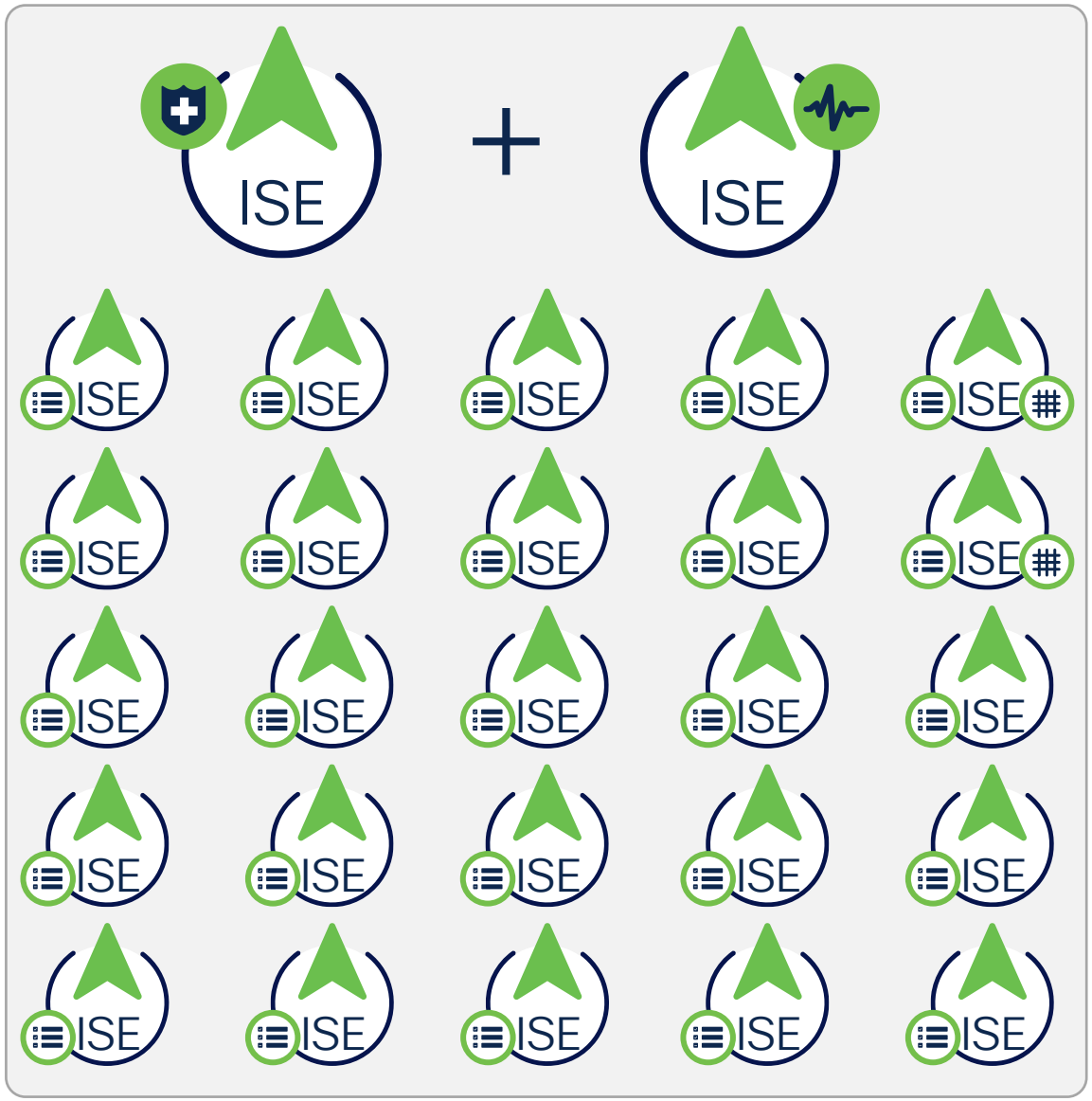


ISE Deployment: Large

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

ISE Deployment: Large

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



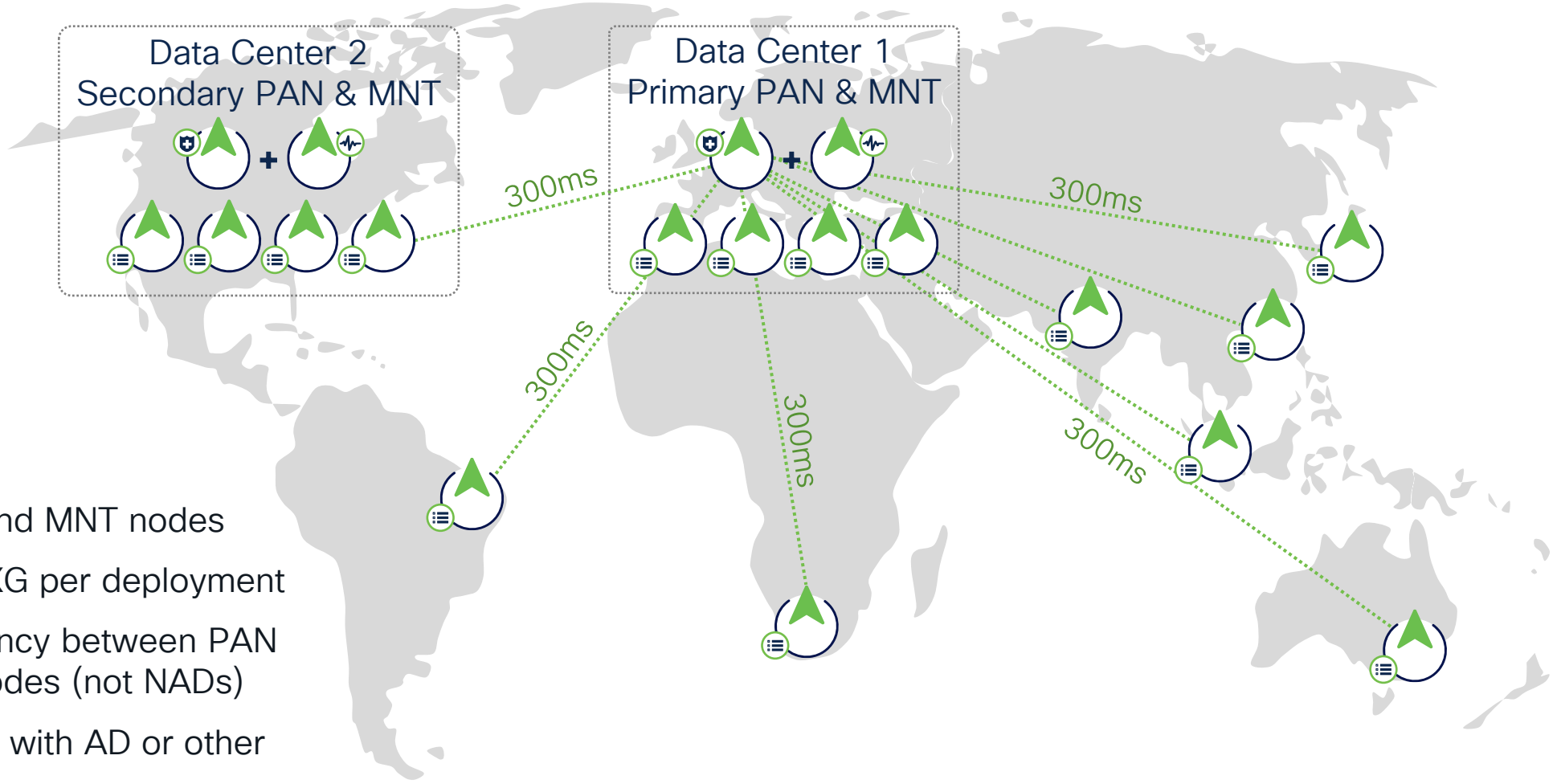
ISE Deployment: Large

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

ISE Deployment: Large

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

Large Deployment: Centralized or Distributed



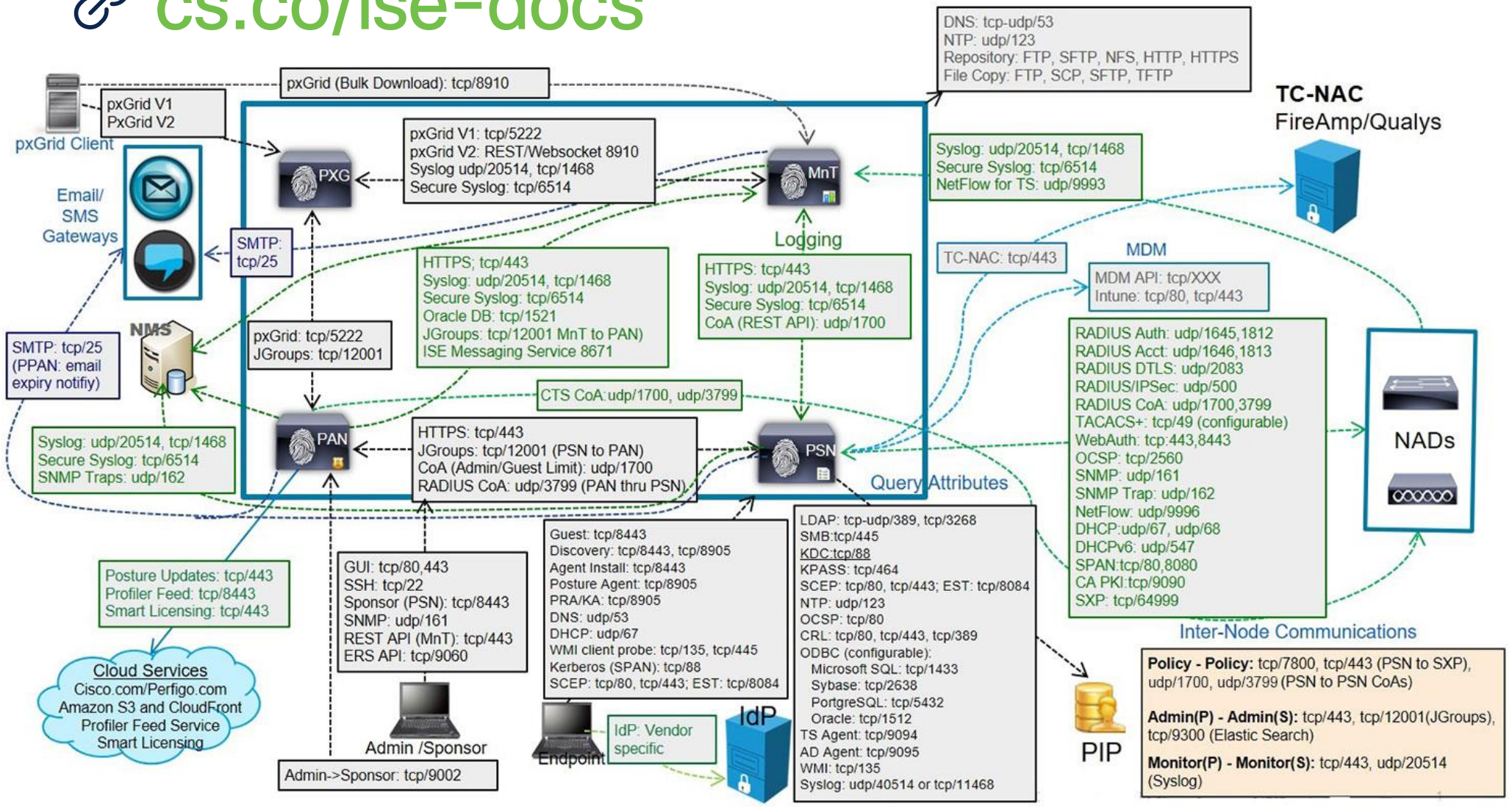
- Separate PAN and MNT nodes
- Max 50 PSN+PXG per deployment
- Max 300ms latency between PAN and other ISE nodes (not NADs)
- Co-locate PSNs with AD or other dependencies

Primary PAN is Required for Many Operations...

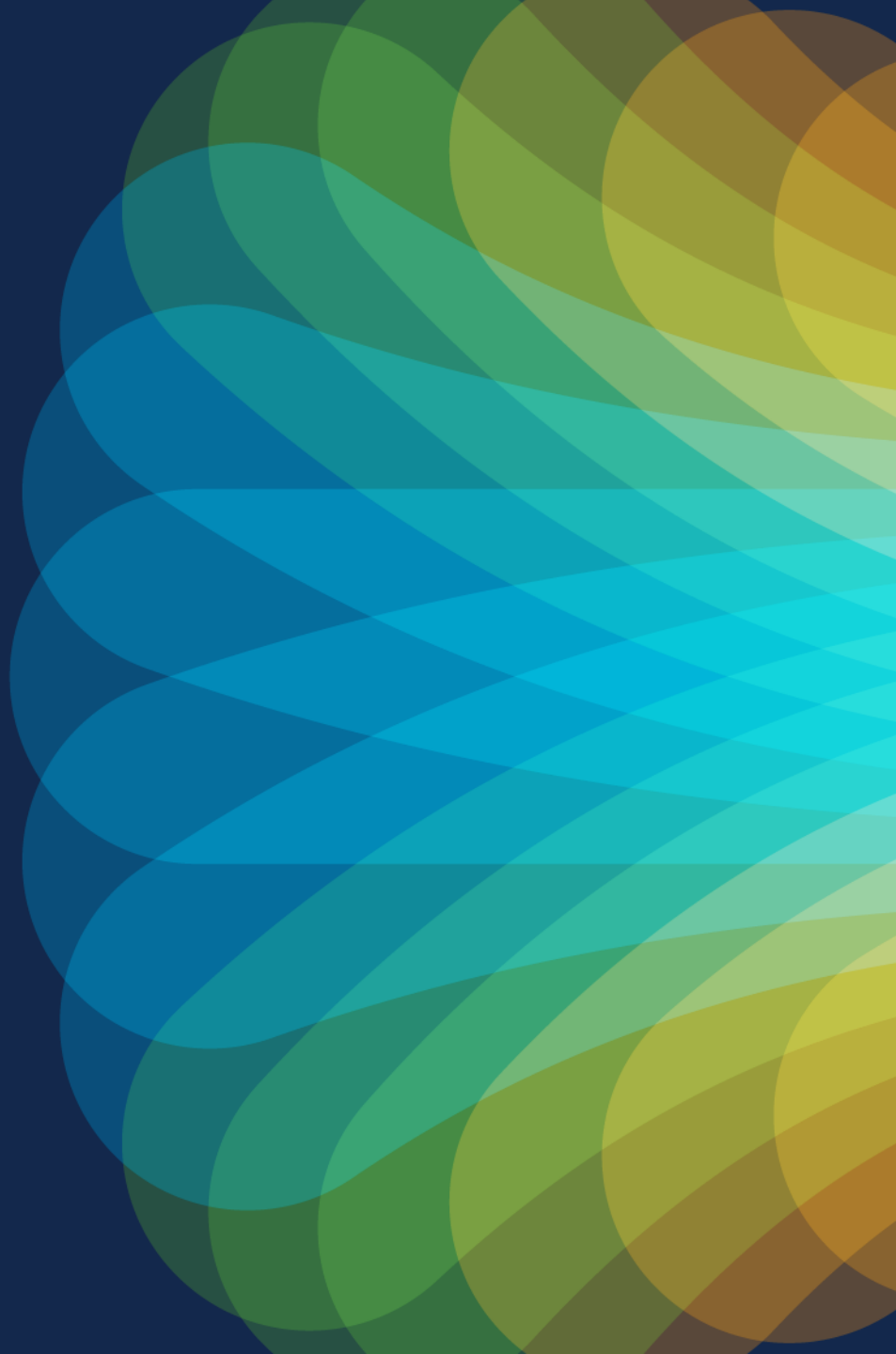
Feature	Available When Primary PAN is Down?
Internal user RADIUS authentication	☑
RADIUS authentication reliant on identity stores	☑
New endpoint learned through profiling.	✗
Existing endpoint with profile change	✗
Existing endpoint with no profile change	☑
Guest: Local Web Authentication (LWA)	☑
Guest: Central Web Authentication (CWA)	☑ Except flows with device registration: Hotspot, BYOD, and CWA
New Guest (Sponsored or Self-registered)	✗
Guest: Change password	✗
Guest: AUP	✗
Guest: Max Failed Login Enforcement	✗
Posture (lease unable to fetch timer)	☑
BYOD with Internal CA	✗
Existing Registered Devices	☑
MDM on-boarding	✗
pxGrid: New registrations or sessions	✗
Log in to GUI of secondary nodes	☑ Login *delayed* due to call to PAN for last login details

ISE Installation Guide: Node Communications

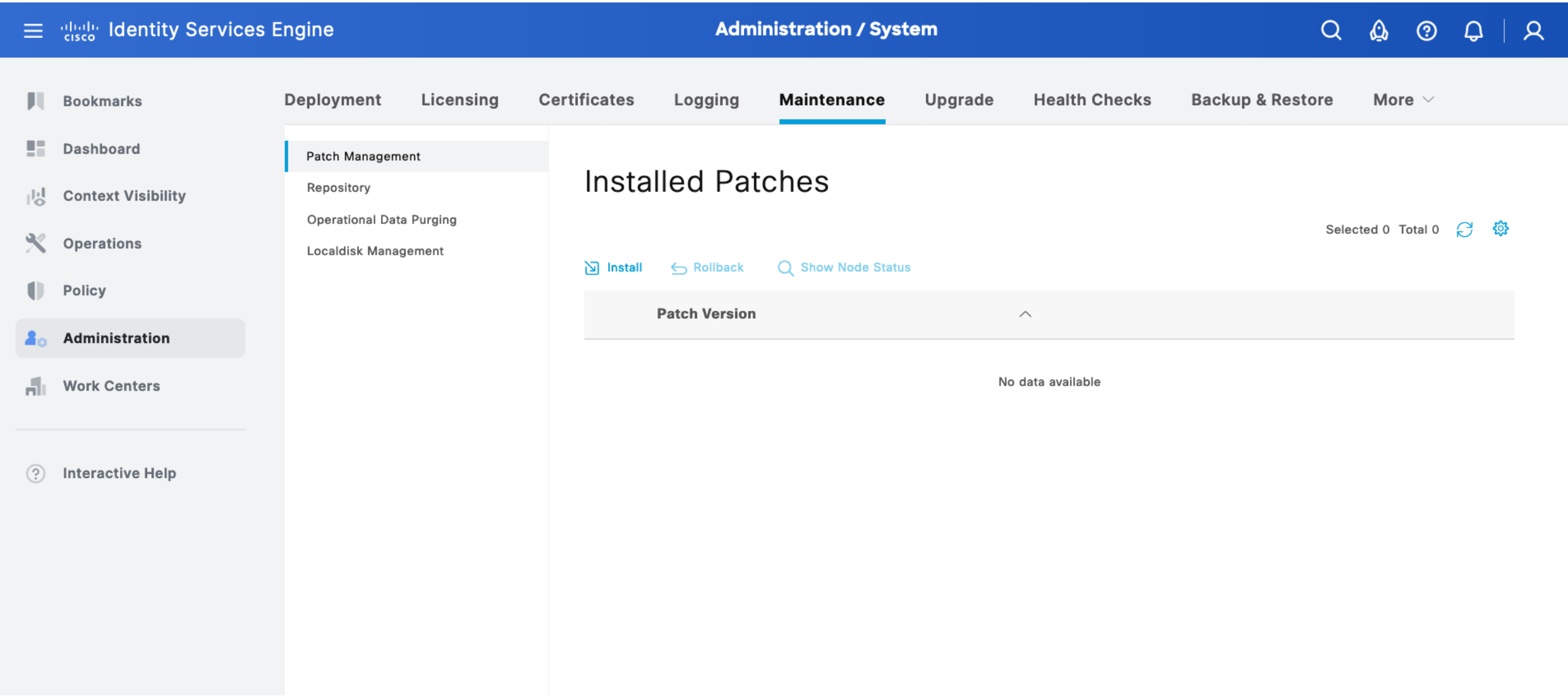
cs.co/ise-docs



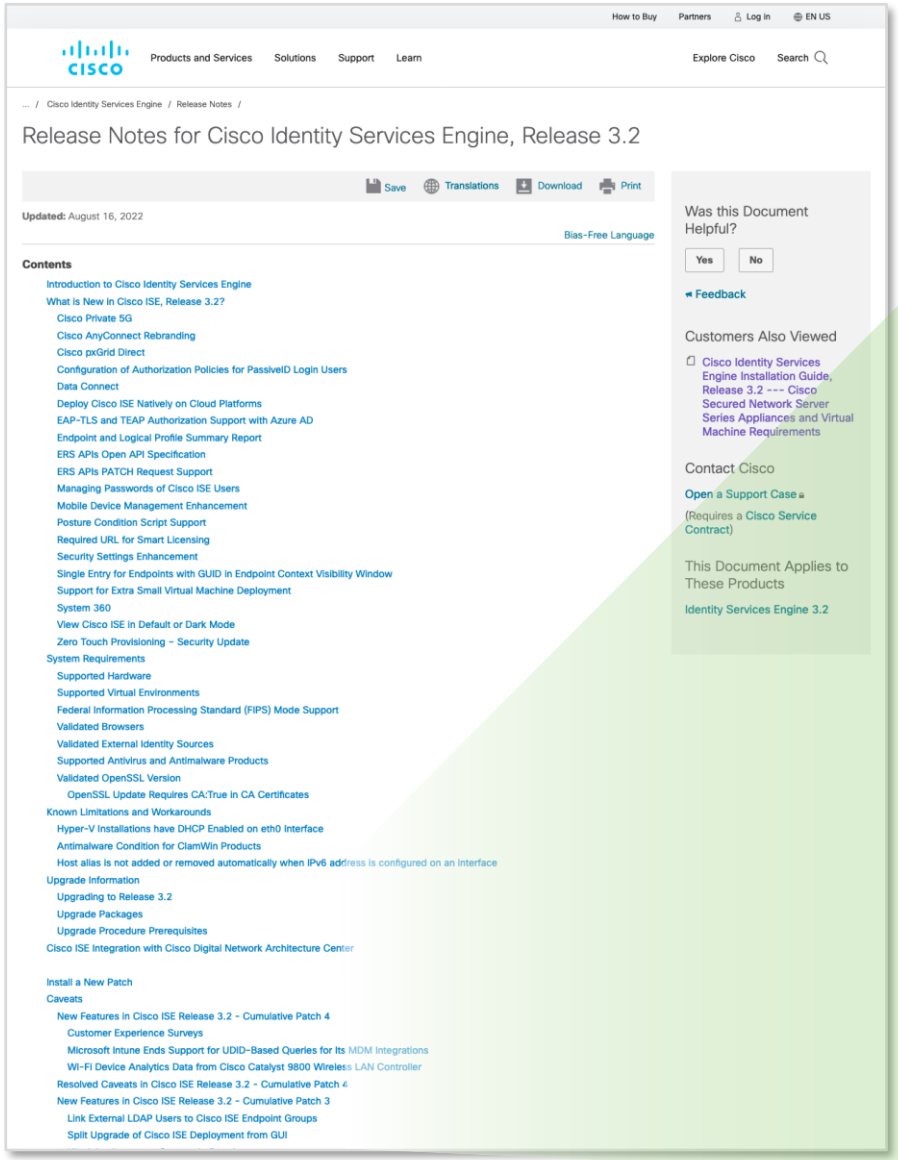
Staging: Patching



Patching



Release Notes for Patch Features & Fixes!



Release Notes for Cisco Identity Services Engine, Release 3.2

Save Translations Download Print

Updated: August 16, 2022

Bias-Free Language

Contents

- Introduction to Cisco Identity Services Engine
- What is New in Cisco ISE, Release 3.2?
  - Cisco Private 5G
  - Cisco AnyConnect Rebranding
  - Cisco pxGrid Direct
  - Configuration of Authorization Policies for PassiveID Login Users
  - Data Connect
  - Deploy Cisco ISE Natively on Cloud Platforms
  - EAP-TLS and TEAP Authorization Support with Azure AD
  - Endpoint and Logical Profile Summary Report
  - ERS APIs Open API Specification
  - ERS APIs PATCH Request Support
  - Managing Passwords of Cisco ISE Users
  - Mobile Device Management Enhancement
  - Posture Condition Script Support
  - Required URL for Smart Licensing
  - Security Settings Enhancement
  - Single Entry for Endpoints with GUID in Endpoint Context Visibility Window
  - Support for Extra Small Virtual Machine Deployment
  - System 360
  - View Cisco ISE in Default or Dark Mode
  - Zero Touch Provisioning – Security Update
- System Requirements
  - Supported Hardware
  - Supported Virtual Environments
  - Federal Information Processing Standard (FIPS) Mode Support
  - Validated Browsers
  - Validated External Identity Sources
  - Supported Antivirus and Antimalware Products
  - Validated OpenSSL Version
    - OpenSSL Update Requires CA:True in CA Certificates
- Known Limitations and Workarounds
  - Hyper-V Installations have DHCP Enabled on eth0 Interface
  - Antimalware Condition for ClamWin Products
  - Host alias is not added or removed automatically when IPv6 address is configured on an interface
- Upgrade Information
  - Upgrading to Release 3.2
  - Upgrade Packages
  - Upgrade Procedure Prerequisites
- Cisco ISE Integration with Cisco Digital Network Architecture Center
- Install a New Patch
- Caveats
  - New Features in Cisco ISE Release 3.2 – Cumulative Patch 4
    - Customer Experience Surveys
    - Microsoft Intune Ends Support for UDID-Based Queries for Its MDM Integrations
    - Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller
  - Resolved Caveats in Cisco ISE Release 3.2 – Cumulative Patch 4
  - New Features in Cisco ISE Release 3.2 – Cumulative Patch 3
    - Link External LDAP Users to Cisco ISE Endpoint Groups
    - Split Upgrade of Cisco ISE Deployment from GUI

Was this Document Helpful? Yes No

Feedback

Customers Also Viewed

Cisco Identity Services Engine Installation Guide, Release 3.2 --- Cisco Secured Network Server Series Appliances and Virtual Machine Requirements

Contact Cisco

Open a Support Case

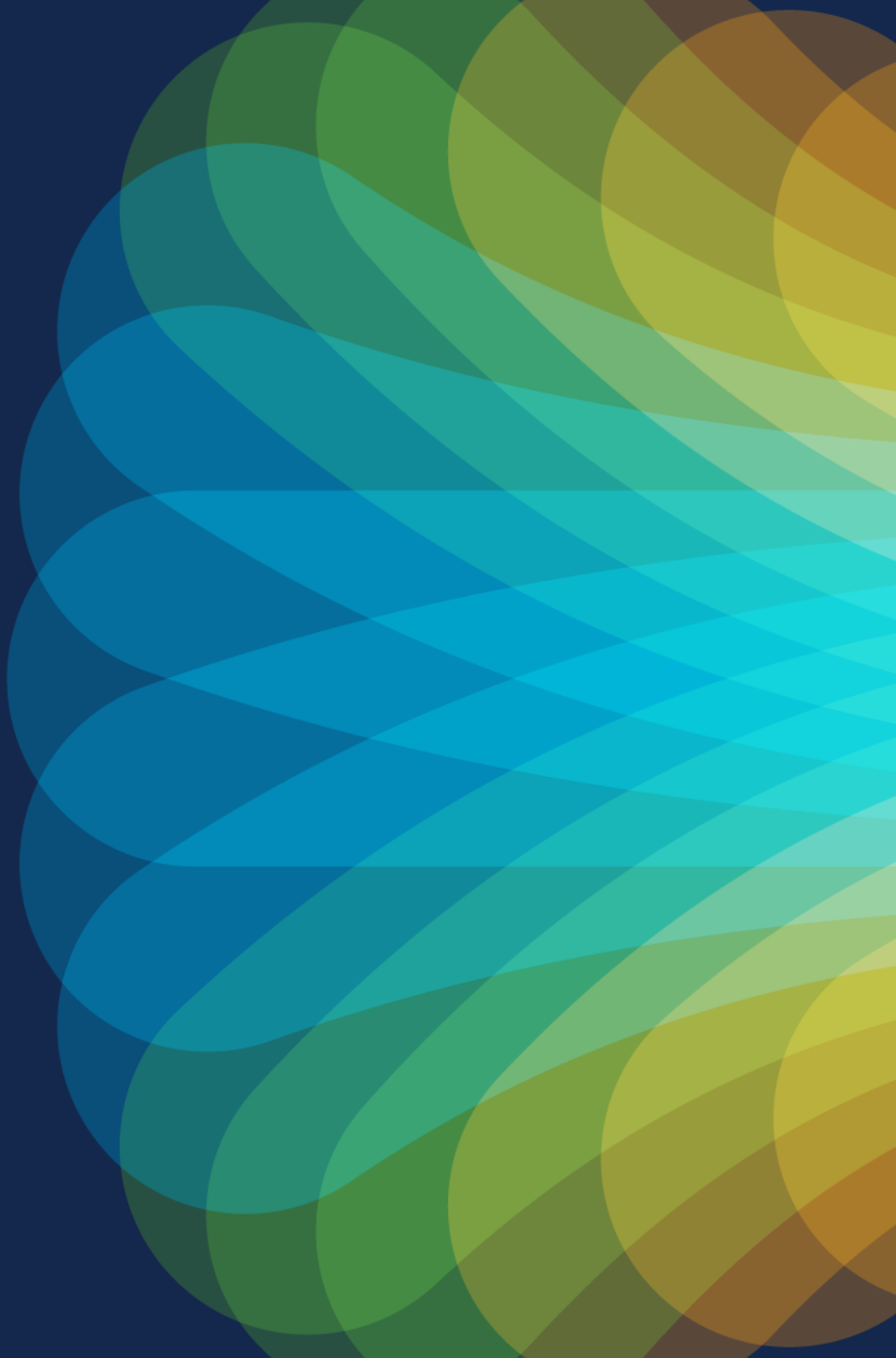
(Requires a Cisco Service Contract)

This Document Applies to These Products

Identity Services Engine 3.2

- Caveats
  - New Features in Cisco ISE Release 3.2 - Cumulative Patch 4
    - Customer Experience Surveys
    - Microsoft Intune Ends Support for UDID-Based Queries for Its MDM Integrations
    - Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller
  - Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 4
  - New Features in Cisco ISE Release 3.2 - Cumulative Patch 3
    - Link External LDAP Users to Cisco ISE Endpoint Groups
    - Split Upgrade of Cisco ISE Deployment from GUI
    - Ukrainian Language Support in Portals
  - Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 3
  - Open Caveats in Cisco ISE Release 3.2 - Cumulative Patch 3
  - New Features in Cisco ISE, Release 3.2 - Cumulative Patch 2
    - Bulk Update and Bulk Delete Support for Context-In API in pxGrid Cloud
    - pxGrid Direct Enhancements
    - Support for Cisco Secure Network Server 3700 Series Appliance
  - Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 2
  - Open Caveats in Cisco ISE Release 3.2 - Cumulative Patch 2
  - New Features in Cisco ISE, Release 3.2 - Cumulative Patch 1
    - Extended Support for Cisco Secure Client
    - Meraki Connector for Cisco ISE
    - pxGrid Cloud Support for Context-in
    - Support for Cisco AI Analytics
    - SGT Reservation using OpenAPI
  - Resolved Caveats in Cisco ISE Release 3.2 - Cumulative Patch 1

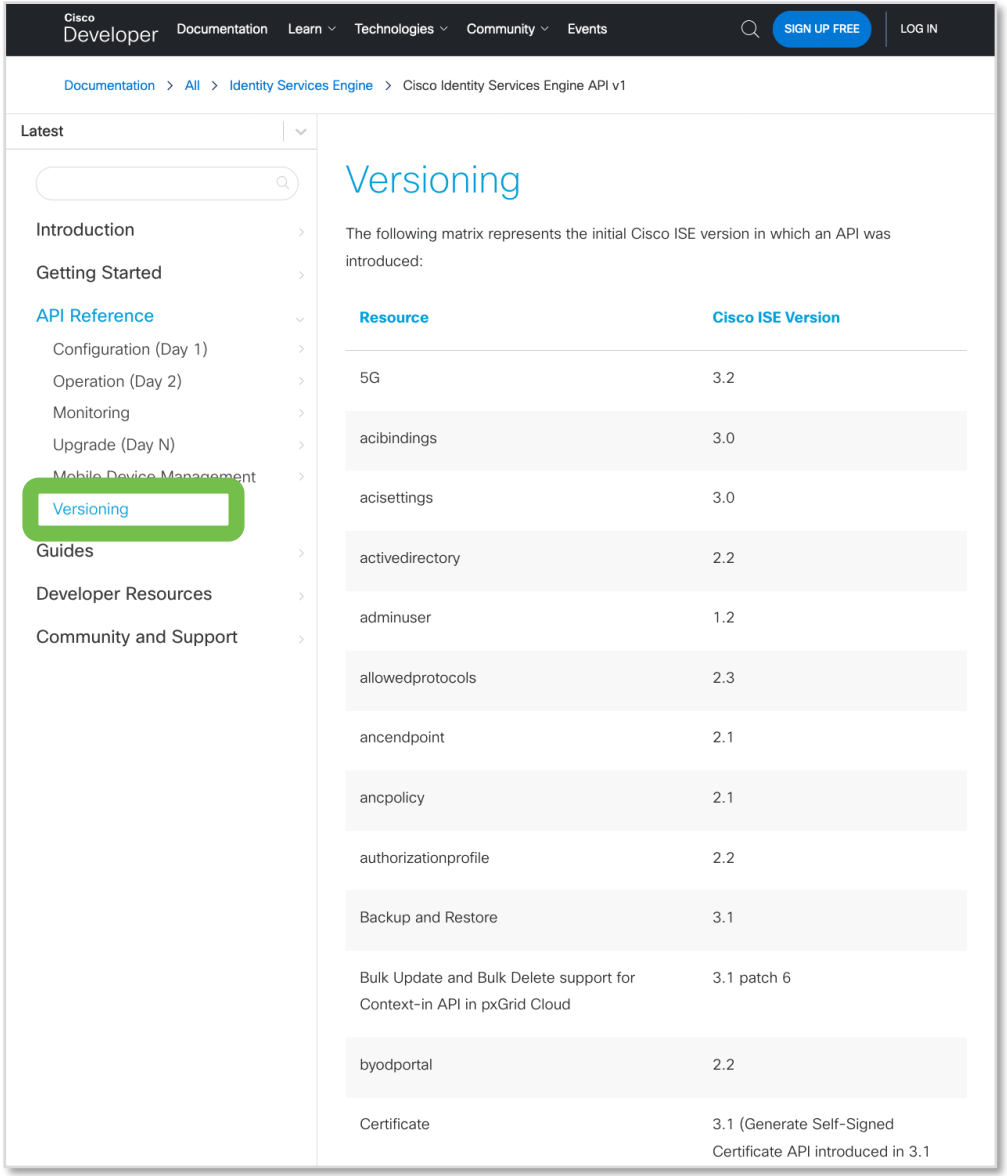
Operations: Automation



ISE 3.3 APIs on DevNet

cs.co/ise-api

5G
acibindings
acisettings
activedirectory
adminuser
allowedprotocols
ancendpoint
ancpolicy
authorizationprofile
Backup and Restore
byodportal
Certificate
certificateprofile
certificatetemplate
Custom Attributes
Data Connect
Deployment
deploymentinfo
downloadableacl
egressmatrixcell
endpoint
Endpoint Replication
endpointcert
endpointgroup
externalradiusserver
filterpolicy
guestlocation
guestsmtpnotificationsettings
guestssid
guesttype
guestuser
hotspotportal
identitygroup
idstoresequence
internaluser
Ipsec
Iseversion
LDAP
License
LSD Settings
sendmessage
mydeviceportal
networkdevice
networkdevicegroup
node
nspprofile
Patch and Hot Patch
Policy
portal
portalglobalsetting
portaltheme
profilerprofile
pxGrid Direct
pxgridnode
pxgridsettings
radiusserversequence
Repository
restidstore
selfregportal
service
sessionservicenode
sgacl
sgmapping
sgmappinggroup
Sgt
SGT Reservation
sgtvnvlan
smsprovider
sponsoredguestportal
sponsorgroup
sponsorgroupmember
sponsorportal
supportbundle
supportbundledownload
supportbundlestatus
sxpconnections
sxplocalbindings
sxpvpns
systemcertificate
System Settings
tacacscommandsets
tacacsexternalservers
tacacsprofile
tacacsserversequence
Task Service
telemetryinfo
TrustSec
Upgrade

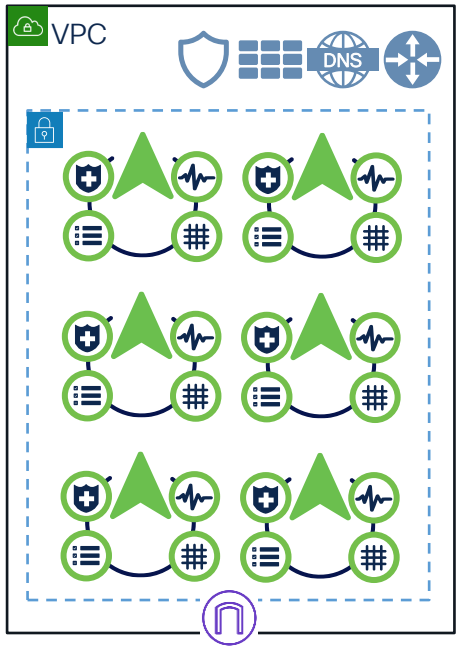


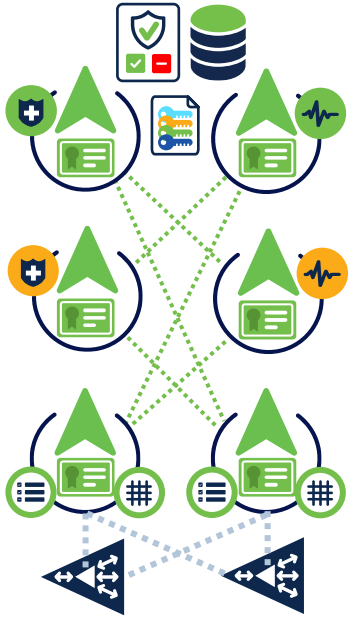
ISE Lifecycle Orchestration & Policy Management

Zero Touch Deployment | Patch Installation | License Management | Certificate Management | Configuration Management | Policy Management | Operations Automation

ISE 3.1 Patch 1 or later

ISE Deployment and Operational Lifecycle





Provision

VPC(s)
Networks
VPNs
ISE Nodes
Repository(s)
Patch + Hotpatches
...

Deploy

Certificates
Roles
Services
Licensing
Load Balancers
...

Configure

Identity Stores
Network Devices
Policy Sets
Endpoints
Portals
...

Operate

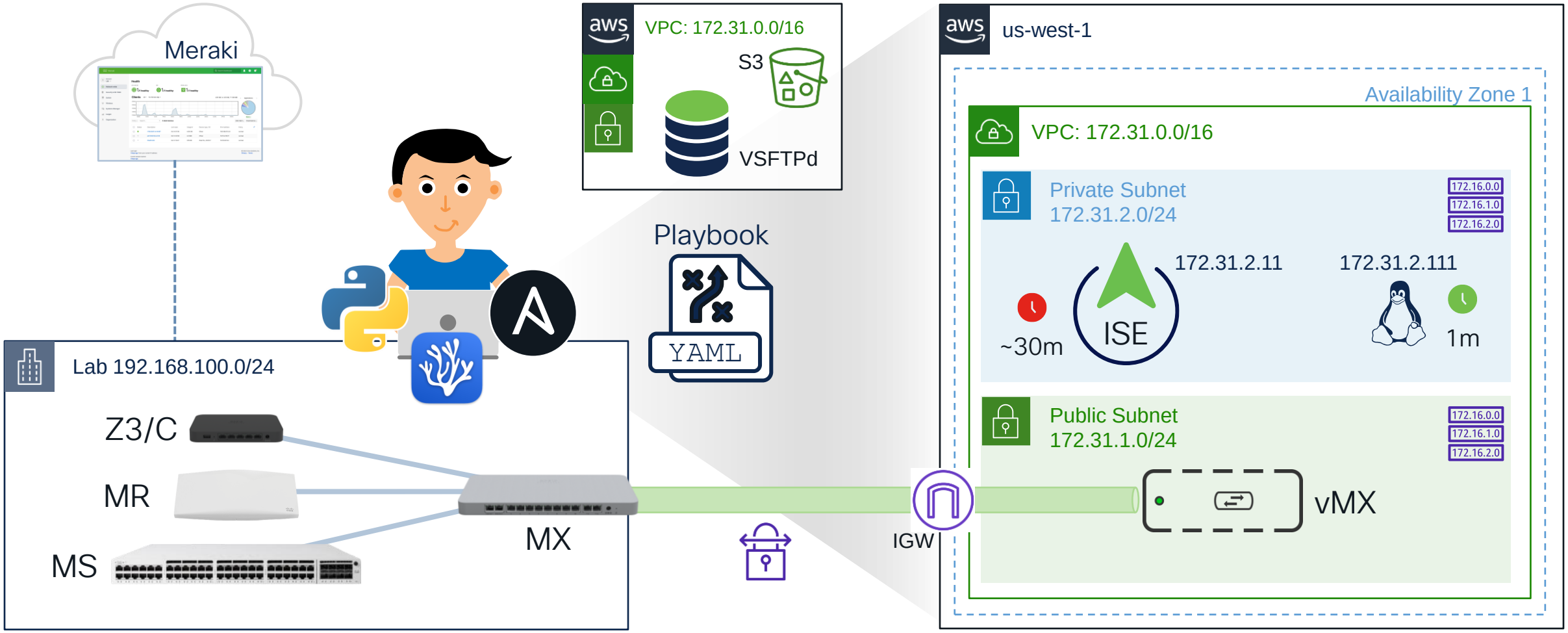
Manage Endpoints
Reporting
Performance
pxGrid / Events
Backup/Restore
Patch
...

Destroy

Terminate
...

ISE with Meraki in AWS

github.com/1homas/ISE_with_Meraki_in_AWS



DataConnect

cs.co/ise-dataconnect

ISE 3.2

cisco DevNet | Documentation | Learn | Technologies | Community | Events | SIGN UP FREE | LOG IN

Documentation > All > Identity Services Engine > Data Connect

Data Connect

- Introduction
- Getting Started
  - Requirements
  - From Java Code
  - From Python Code
  - From Oracle SQL Developer
  - From Microsoft Excel on Windows
- Guides
- Changelog

Database Views

Data Connect

- Introduction
- Getting Started
- Guides
- Changelog

Database Views

- AAA_DIAGNOSTICS_VIEW
- ADAPTER_STATUS
- ADAPTIVE_NETWORK_CONTROL
- ADMINISTRATOR_LOGINS
- ADMIN_USERS
- AUP_ACCEPTANCE_STATUS
- AUTHORIZATION_PROFILES
- CHANGE_CONFIGURATION_AUDIT
- COA_EVENTS
- **ENDPOINTS_DATA**
- ENDPOINT_IDENTITY_GROUPS
- ENDPOINT_PURGE_VIEW
- EXT_ID_SRC_ACTIVE_DIRECTORY
- EXT_ID_SRC_CERT_AUTH_PROFILE
- EXT_ID_SRC_LDAP
- EXT_ID_SRC_ODBC
- EXT_ID_SRC_RADIUS_TOKEN
- EXT_ID_SRC_REST

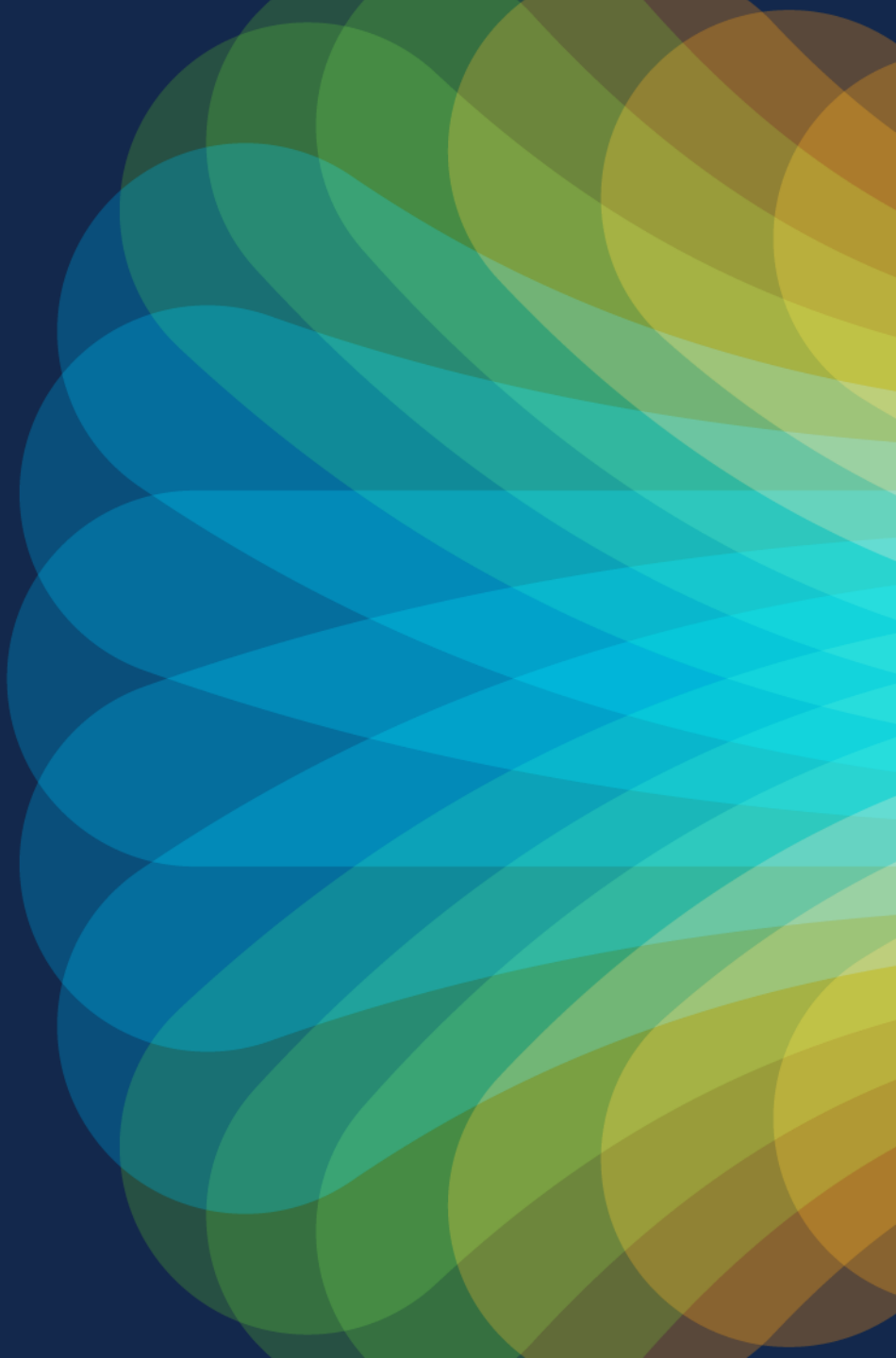
ENDPOINTS_DATA

Collection of all data related to endpoint that ISE collects

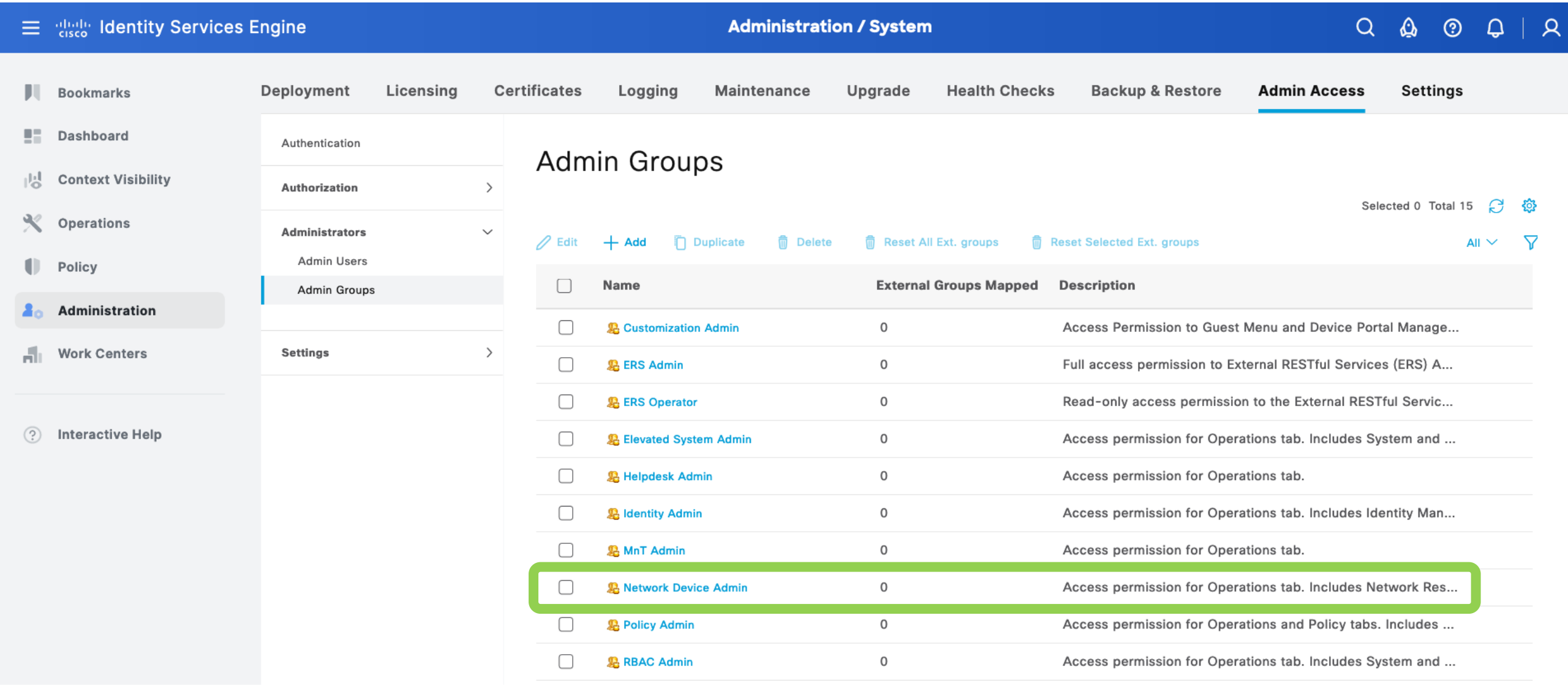
Type: View

Column name	Data Type	Column Description
ENDPOINT_POLICY_ID	VARCHAR2	Specifies the unique ID of the endpoint policy used
MATCHED_POLICY_ID	VARCHAR2	Specifies the ID of profiling used
NMAP_SUBNET_SCANID	NUMBER	NMAP subnet can ID of end points
PORTAL_USER	VARCHAR2	Specifies the portal user
AUTH_STORE_ID	VARCHAR2	Specifies the auth store ID
DEVICE_REGISTRATIONS_STATUS	NUMBER	Specifies if device is registered
REG_TIMESTAMP	NUMBER	Specifies the registered timestamp
POSTURE_APPLICABLE	NUMBER	Specifies if Posture is Applicable

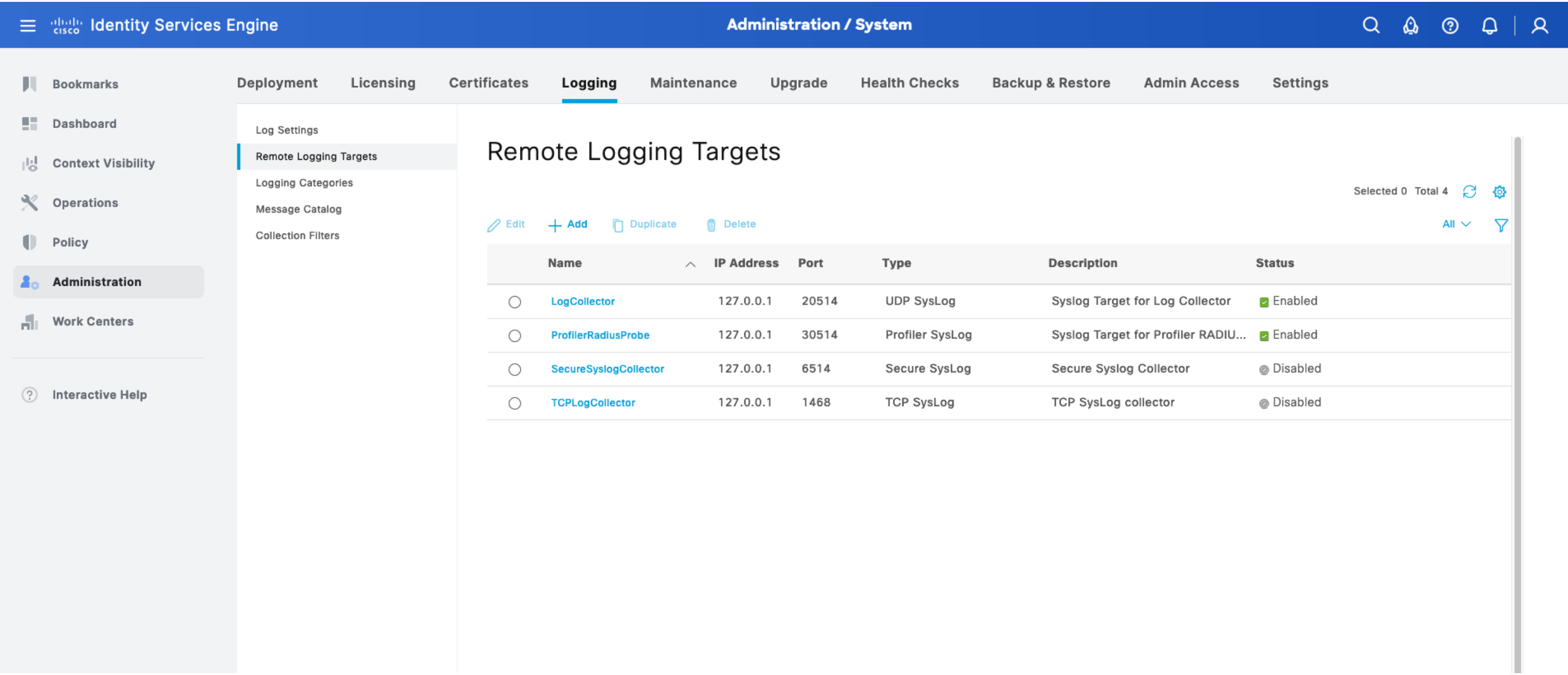
Operations: Monitoring



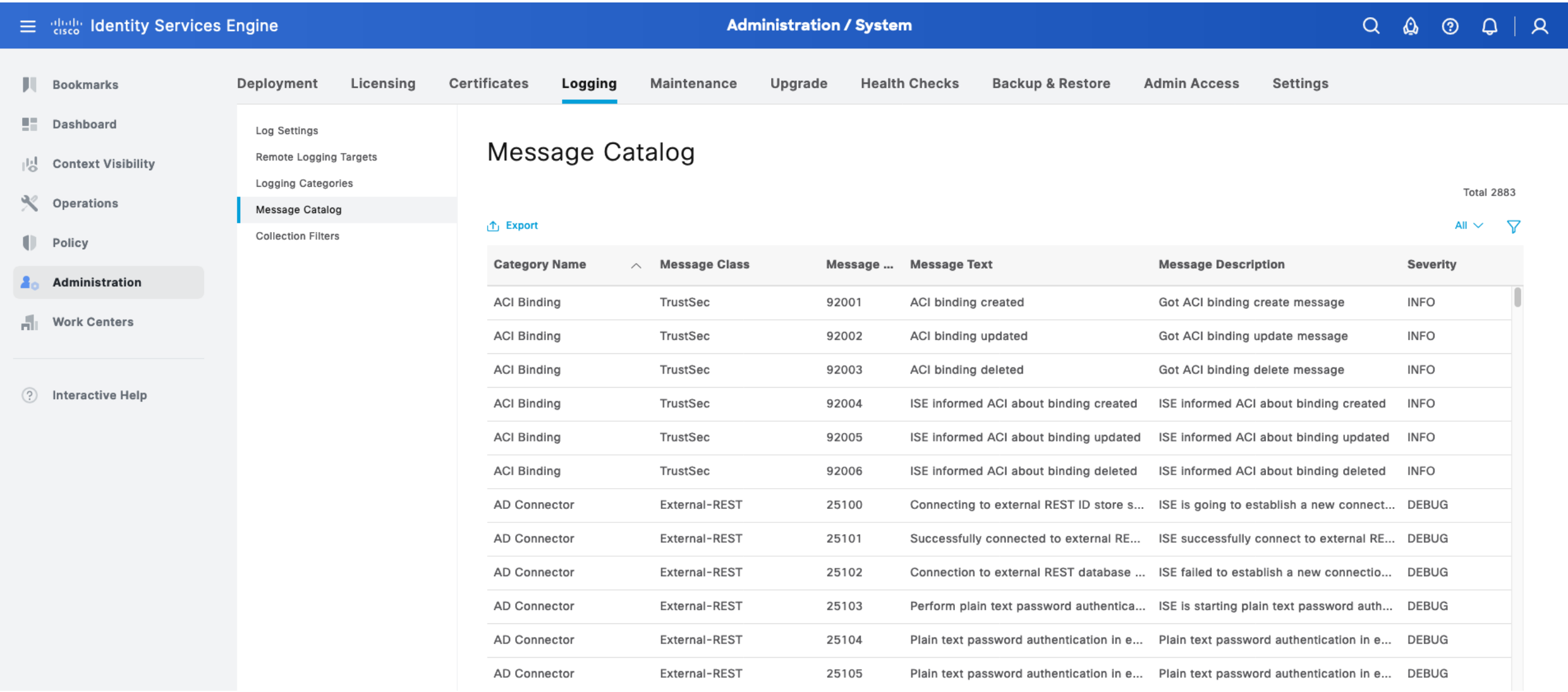
ISE Admin Role Based Access Control (RBAC)



Remote Logging Targets (Syslog Servers)



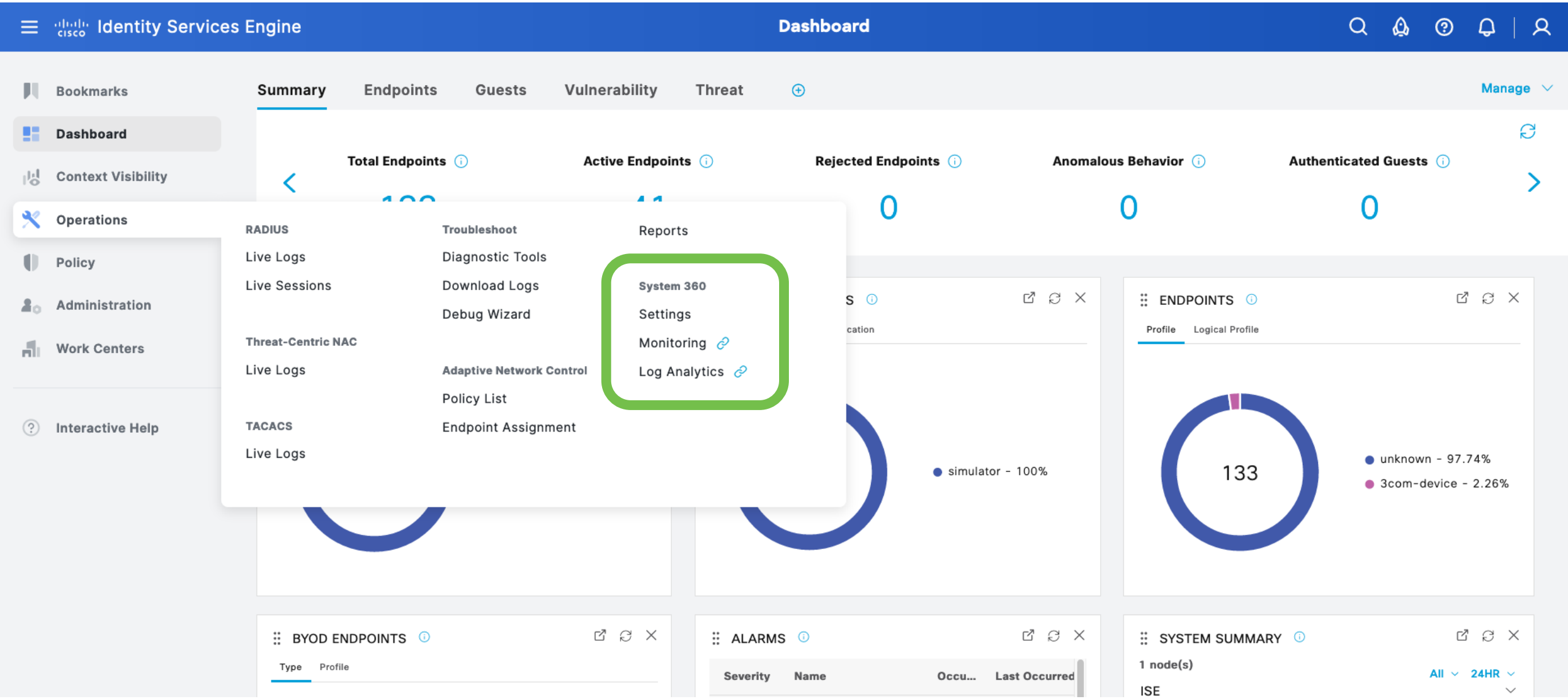
ISE Message Catalog



Category Name	Message Class	Message ...	Message Text	Message Description	Severity
ACI Binding	TrustSec	92001	ACI binding created	Got ACI binding create message	INFO
ACI Binding	TrustSec	92002	ACI binding updated	Got ACI binding update message	INFO
ACI Binding	TrustSec	92003	ACI binding deleted	Got ACI binding delete message	INFO
ACI Binding	TrustSec	92004	ISE informed ACI about binding created	ISE informed ACI about binding created	INFO
ACI Binding	TrustSec	92005	ISE informed ACI about binding updated	ISE informed ACI about binding updated	INFO
ACI Binding	TrustSec	92006	ISE informed ACI about binding deleted	ISE informed ACI about binding deleted	INFO
AD Connector	External-REST	25100	Connecting to external REST ID store s...	ISE is going to establish a new connect...	DEBUG
AD Connector	External-REST	25101	Successfully connected to external RE...	ISE successfully connect to external RE...	DEBUG
AD Connector	External-REST	25102	Connection to external REST database ...	ISE failed to establish a new connectio...	DEBUG
AD Connector	External-REST	25103	Perform plain text password authentica...	ISE is starting plain text password auth...	DEBUG
AD Connector	External-REST	25104	Plain text password authentication in e...	Plain text password authentication in e...	DEBUG
AD Connector	External-REST	25105	Plain text password authentication in e...	Plain text password authentication in e...	DEBUG

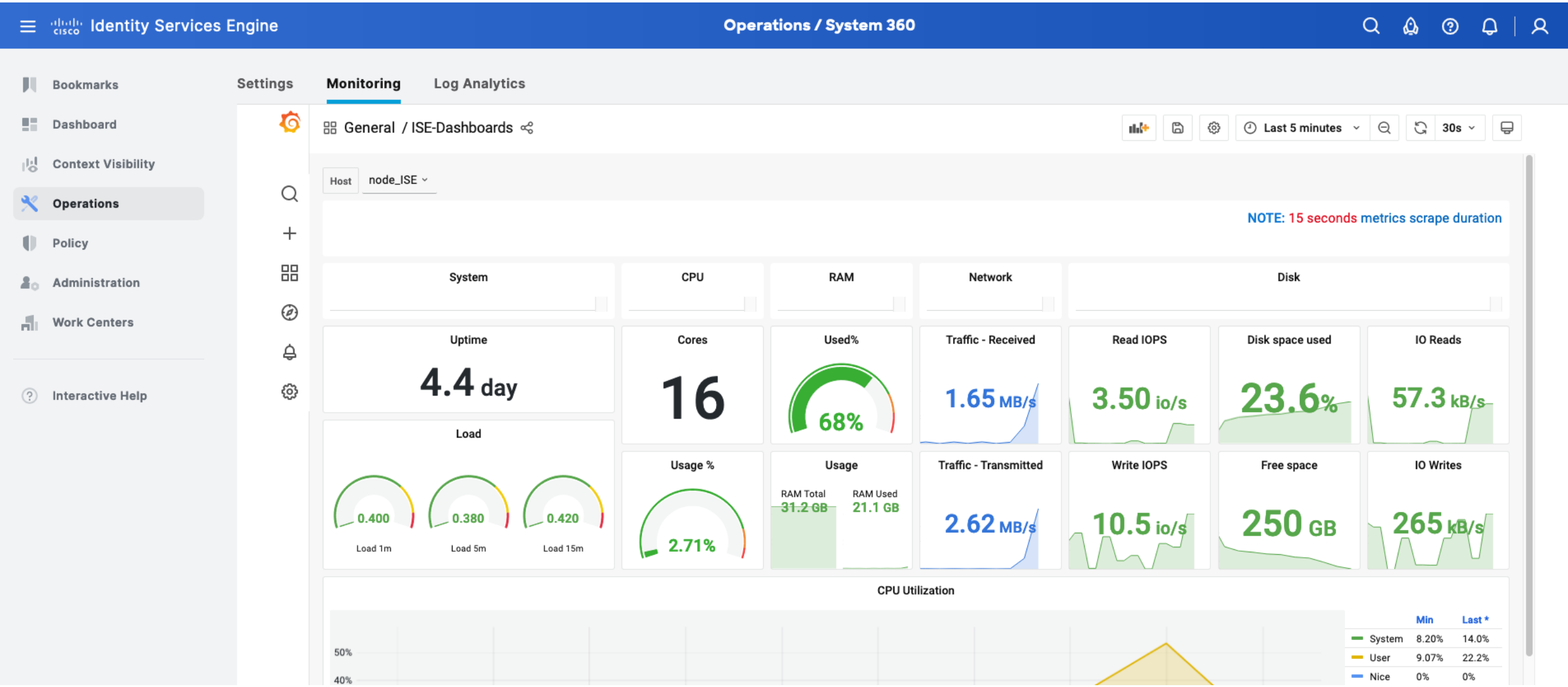
ISE System 360

ISE 3.2



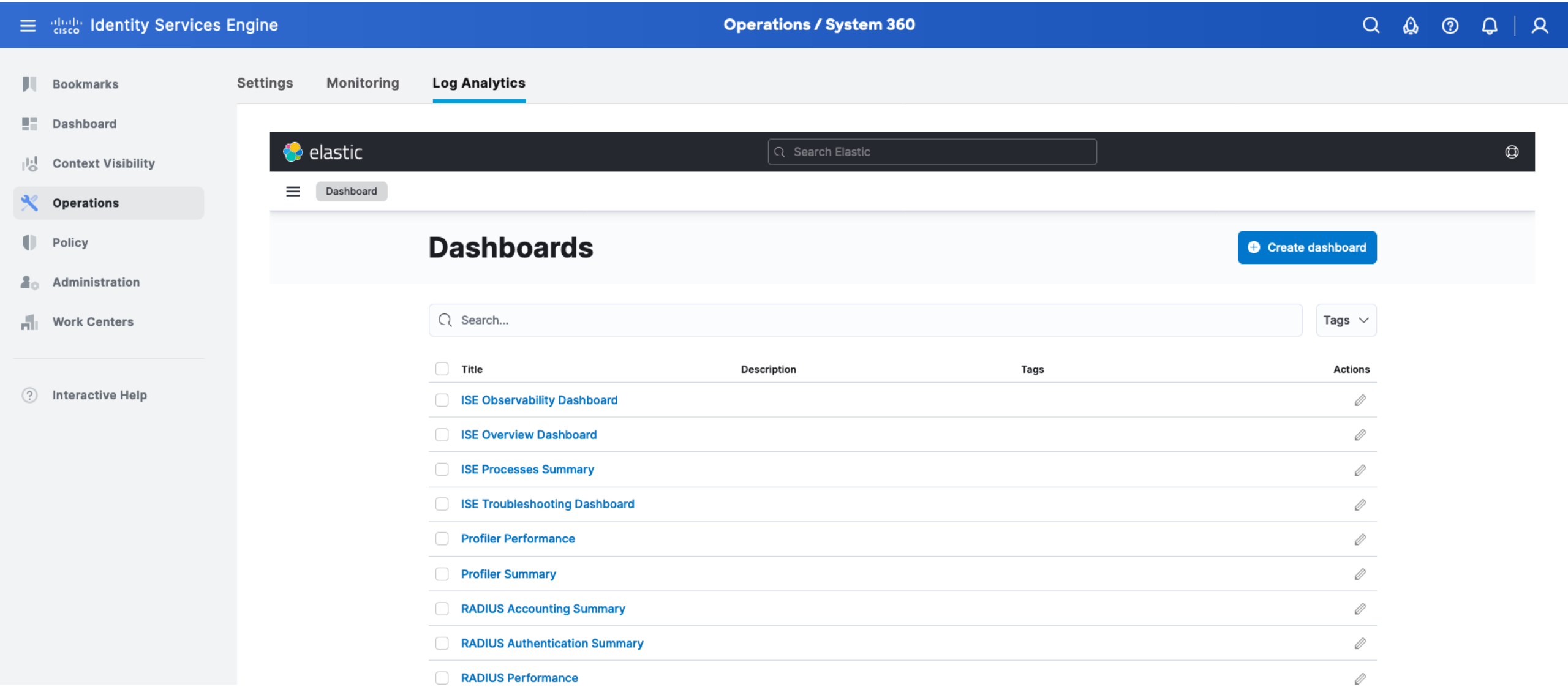
System 360: Monitoring

ISE 3.2



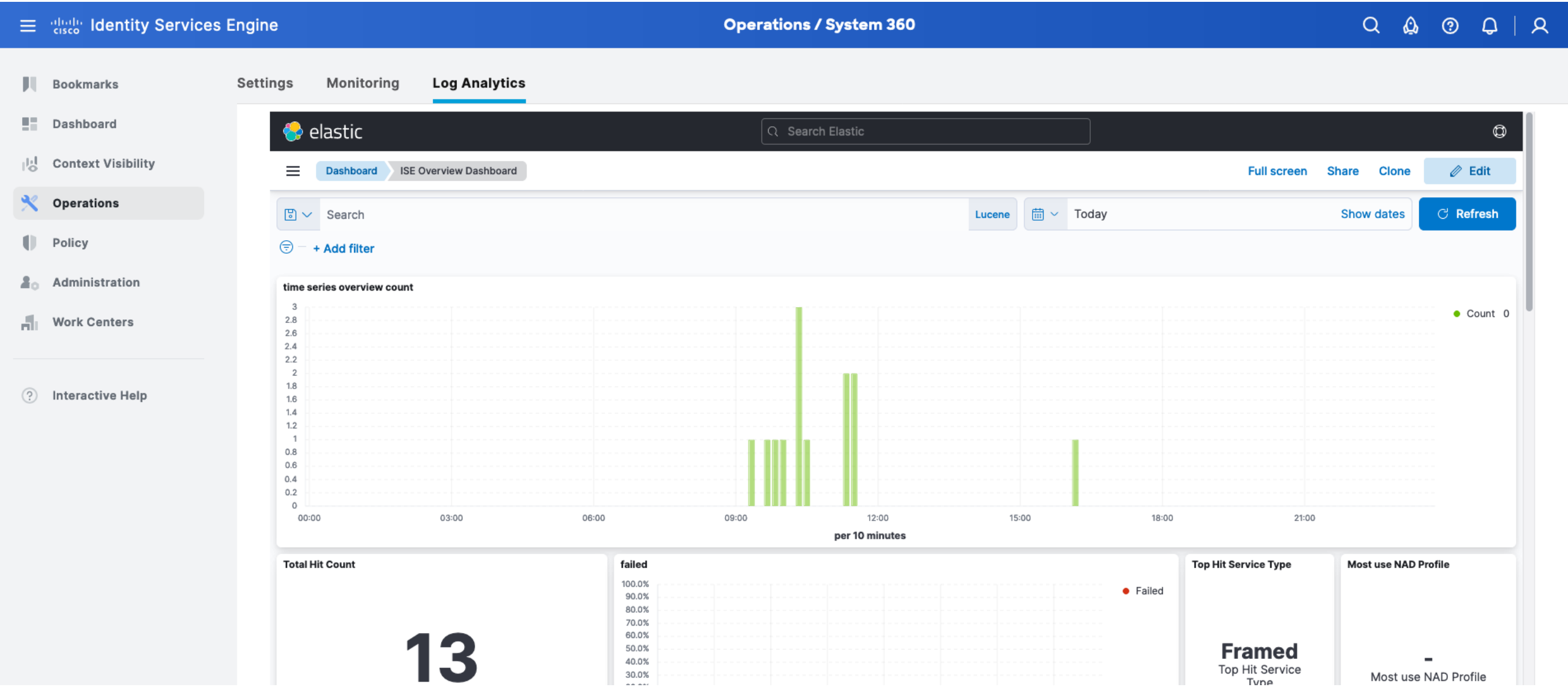
System 360: Log Analytics

ISE 3.2

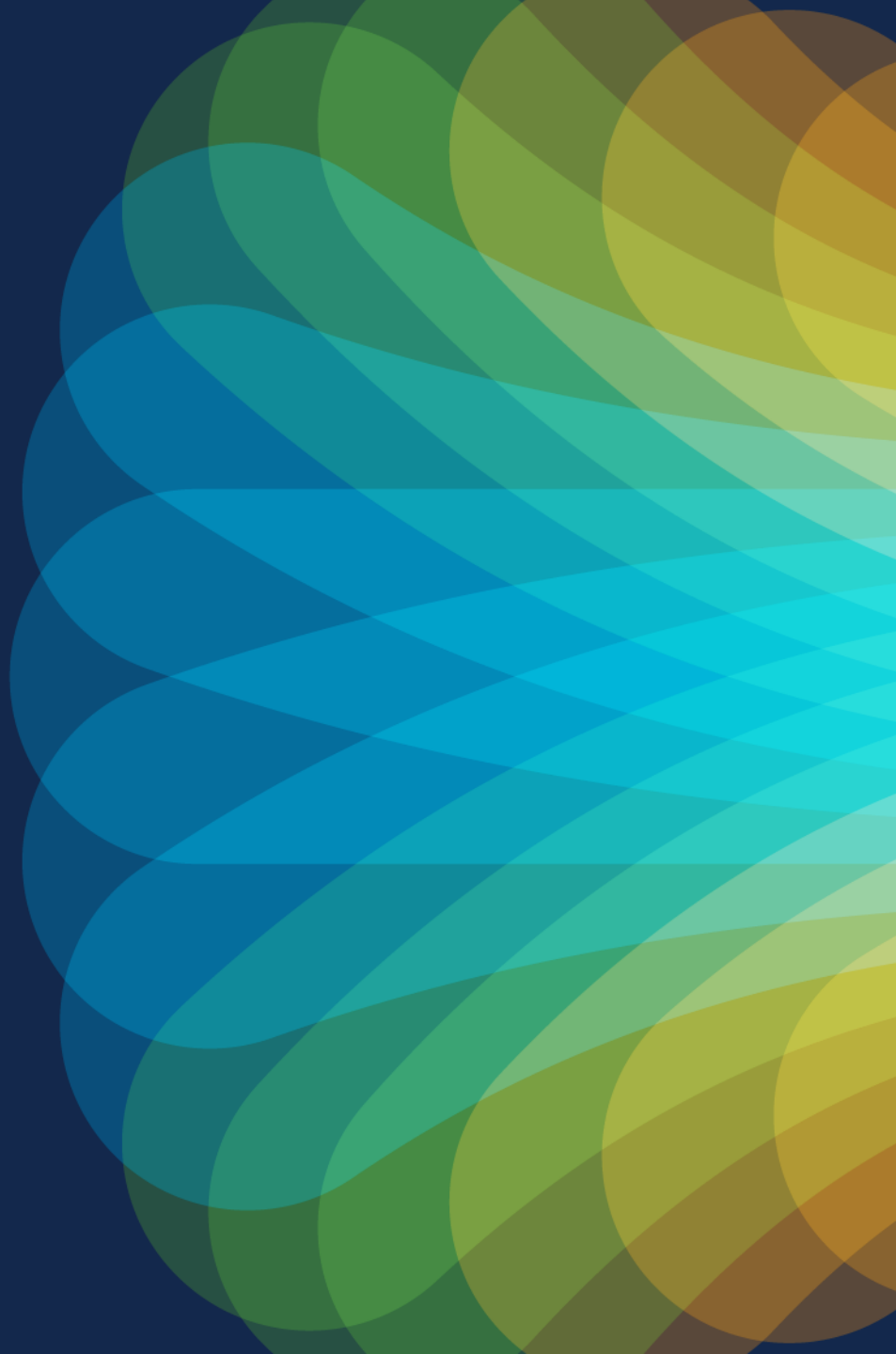


System 360: Log Analytics

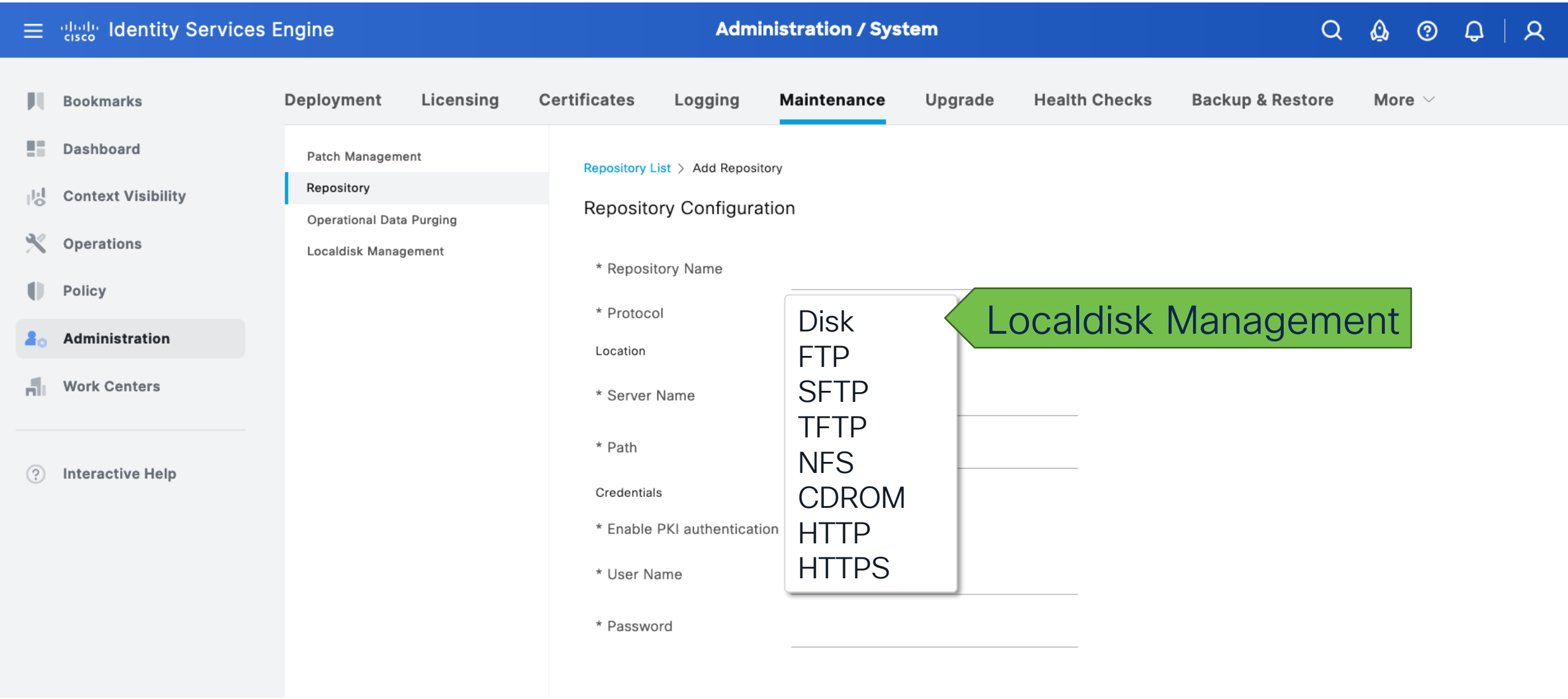
ISE 3.2



Operations: Backups

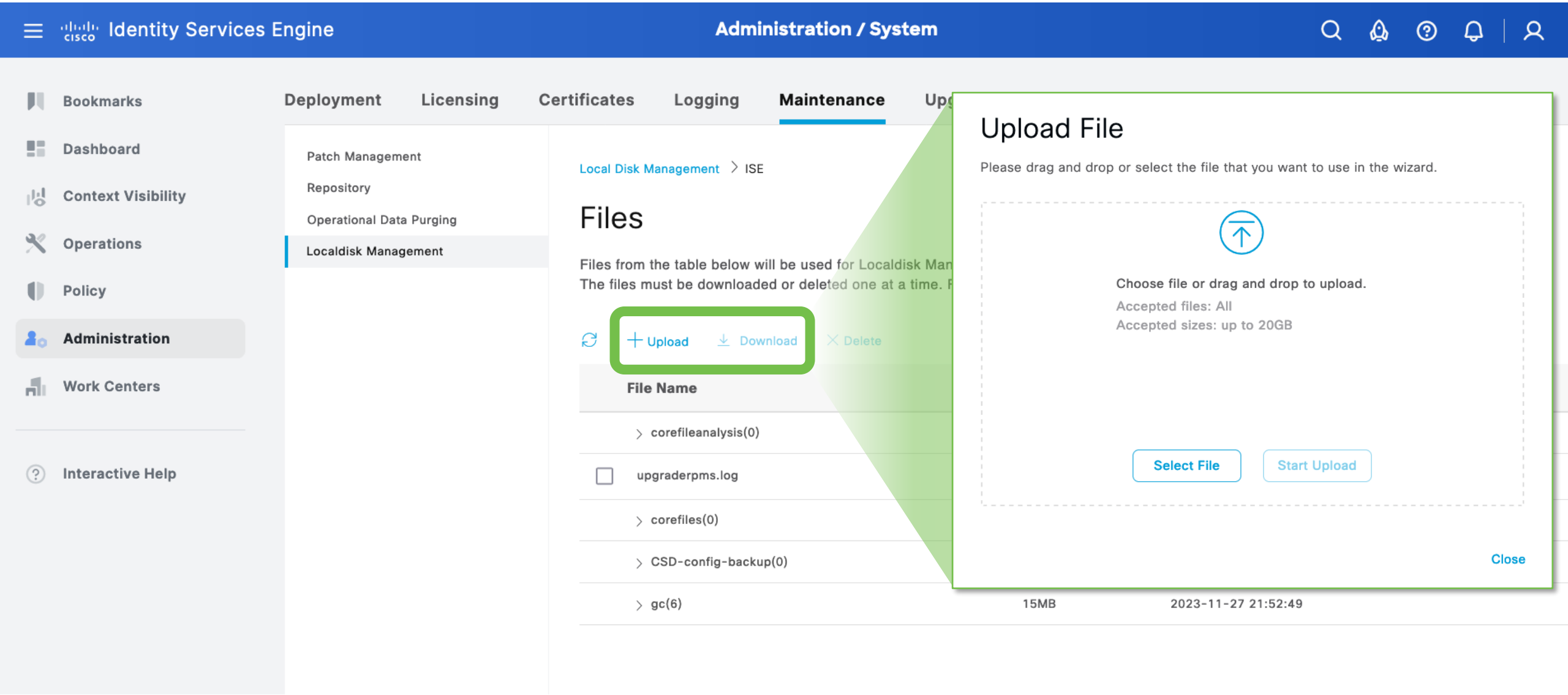


ISE Repositories

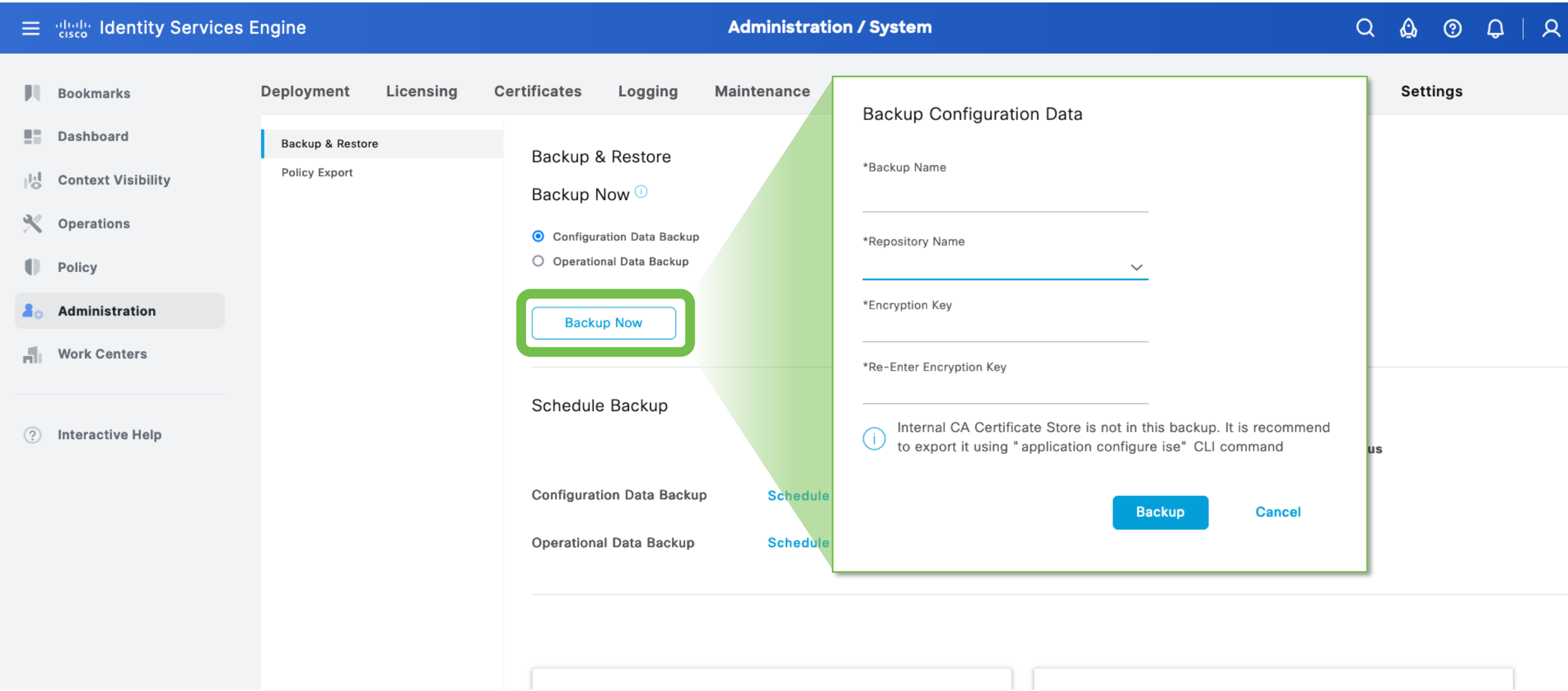


Localdisk Management

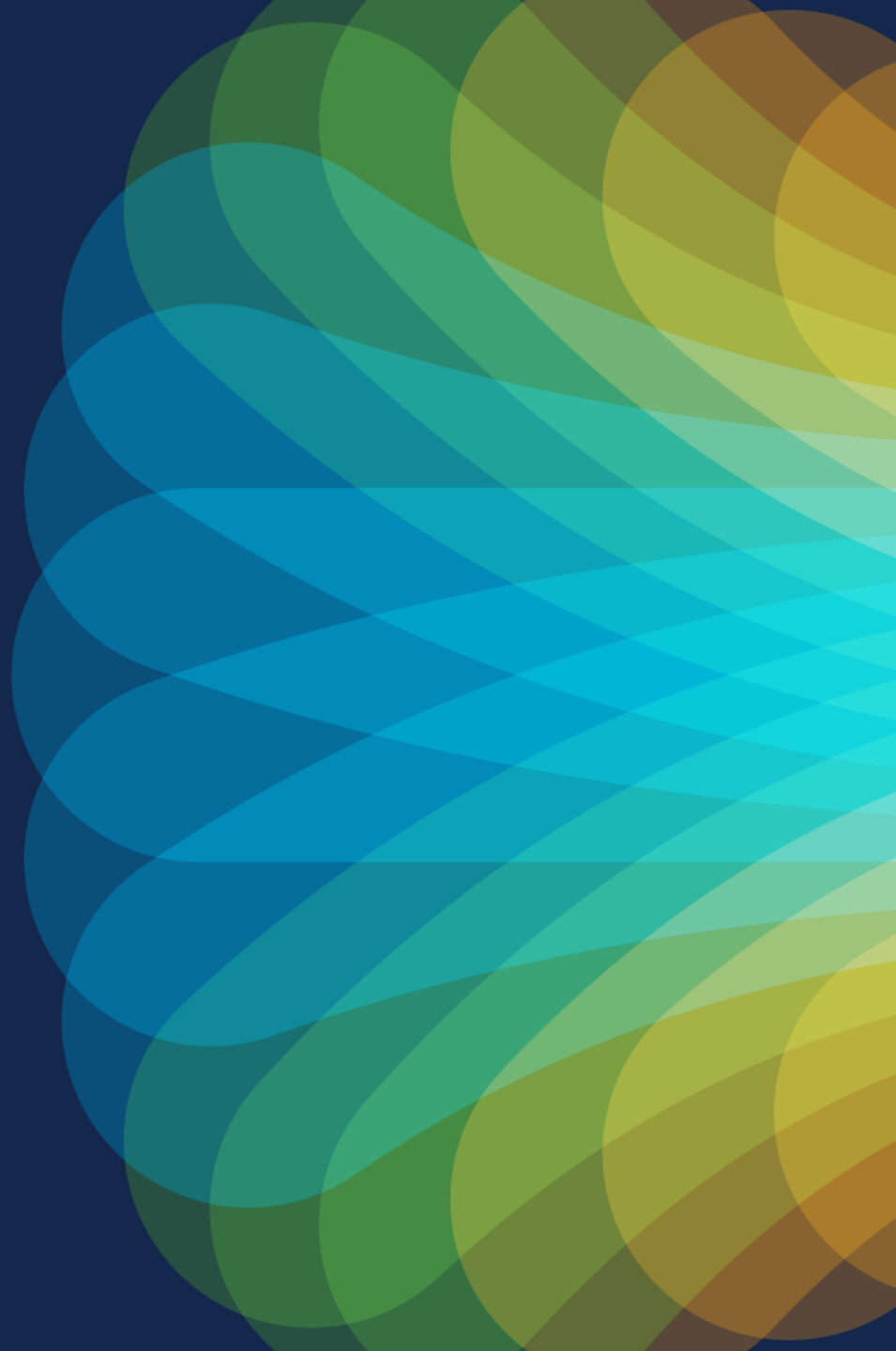
ISE 3.1



Administration > System > Backup & Restore



Conclusion

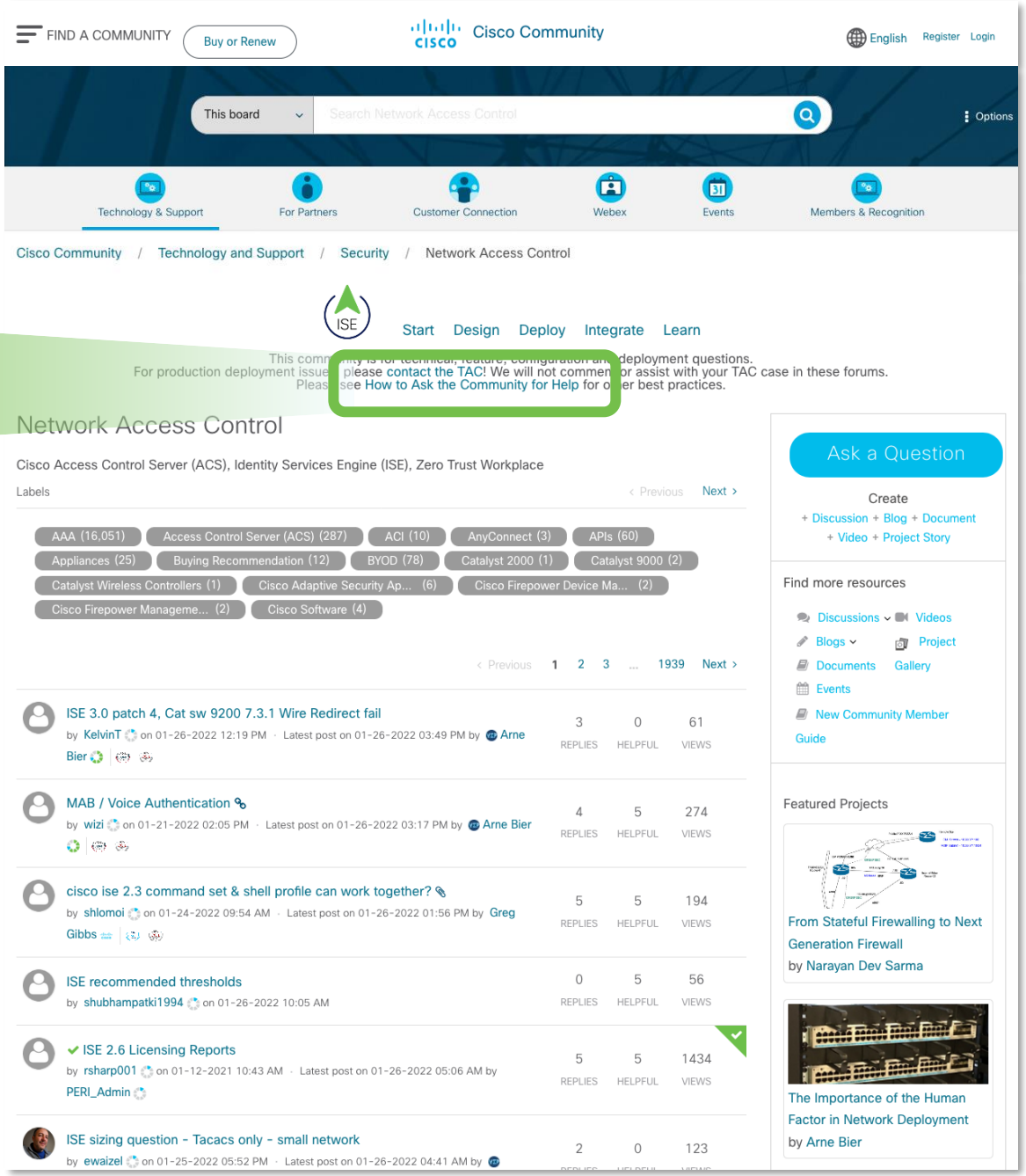


Ask The Community

cs.co/ise-community

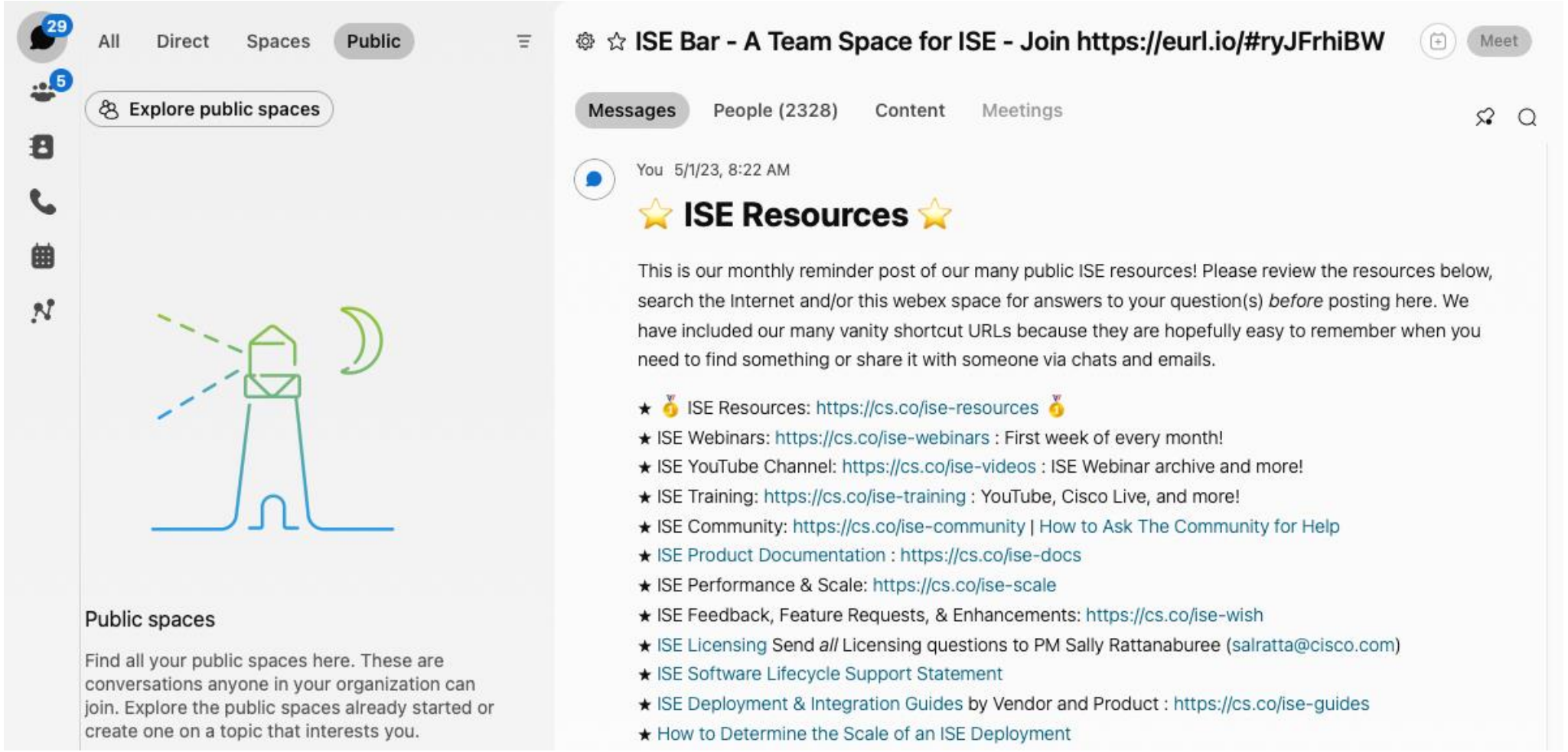
How to Ask the Community for Help

- The Community is Not TAC
- No Comment on Roadmaps or Fixes
- New Features and Feedback
- Provide Details
  - Goal/Scenario?
  - NAD Hardware & Software?
  - Endpoint OS(es)?
  - Browser(s)?
- Reproducibility (expected vs actual)
- Use Pictures or even Video!



ISE Bar: A Webex Team Space for ISE

eurl.io/#ryJFrhiBW

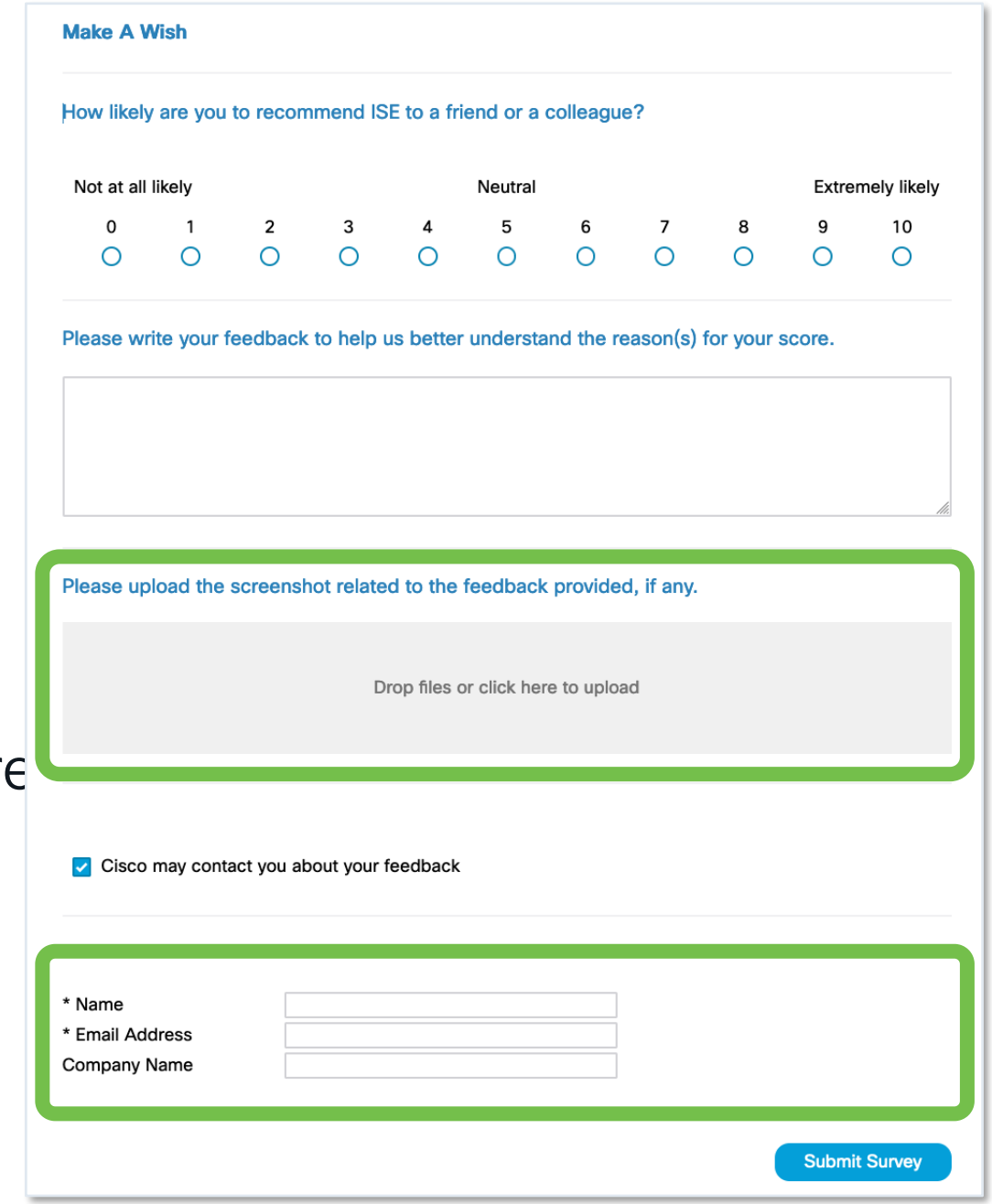


Make a Wish

Do you want a new feature in ISE?

Or an improvement in an existing feature

cs.co/ise-wish



Resources

- cs.co/ise-resources
- cs.co/ise-training
- cs.co/ise-guides***#tag***
- cs.co/ise-community
- cs.co/nad-capabilities
- github.com/1homas/
- github.com/ISEDemoLab/
- woland.com
- ise-support.com
- network-node.com
- securityccie.net/
- labminutes.com/video/sec/ISE

cisco Live!

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.

Meet the Expert Opening Hours:

Tuesday	**3:00pm – 7:00pm**
Wednesday	**11:15am – 7:00pm**
Thursday	**9:30am – 4:00pm**
Friday	**10:30am – 1:30pm**

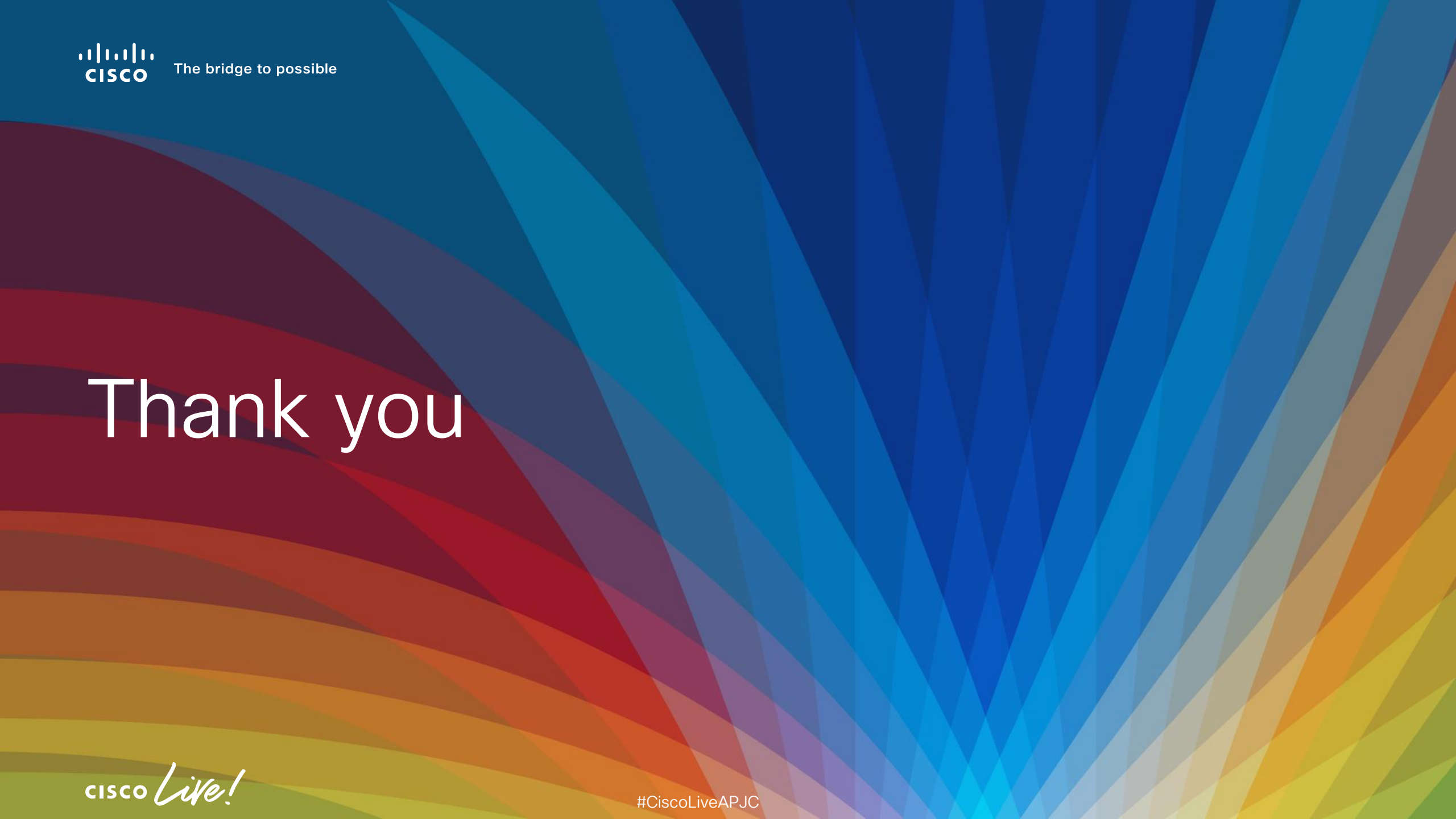
Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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


The bridge to possible
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
Let's go
#CiscoLiveAPJC