
cisco Live!
Let's go

The bridge to possible

ISE Planning, Staging and Deployment

Francesca Martucci
Technical Solutions Architect, Cybersecurity EMEA

cisco Live!

BRKSEC-2660

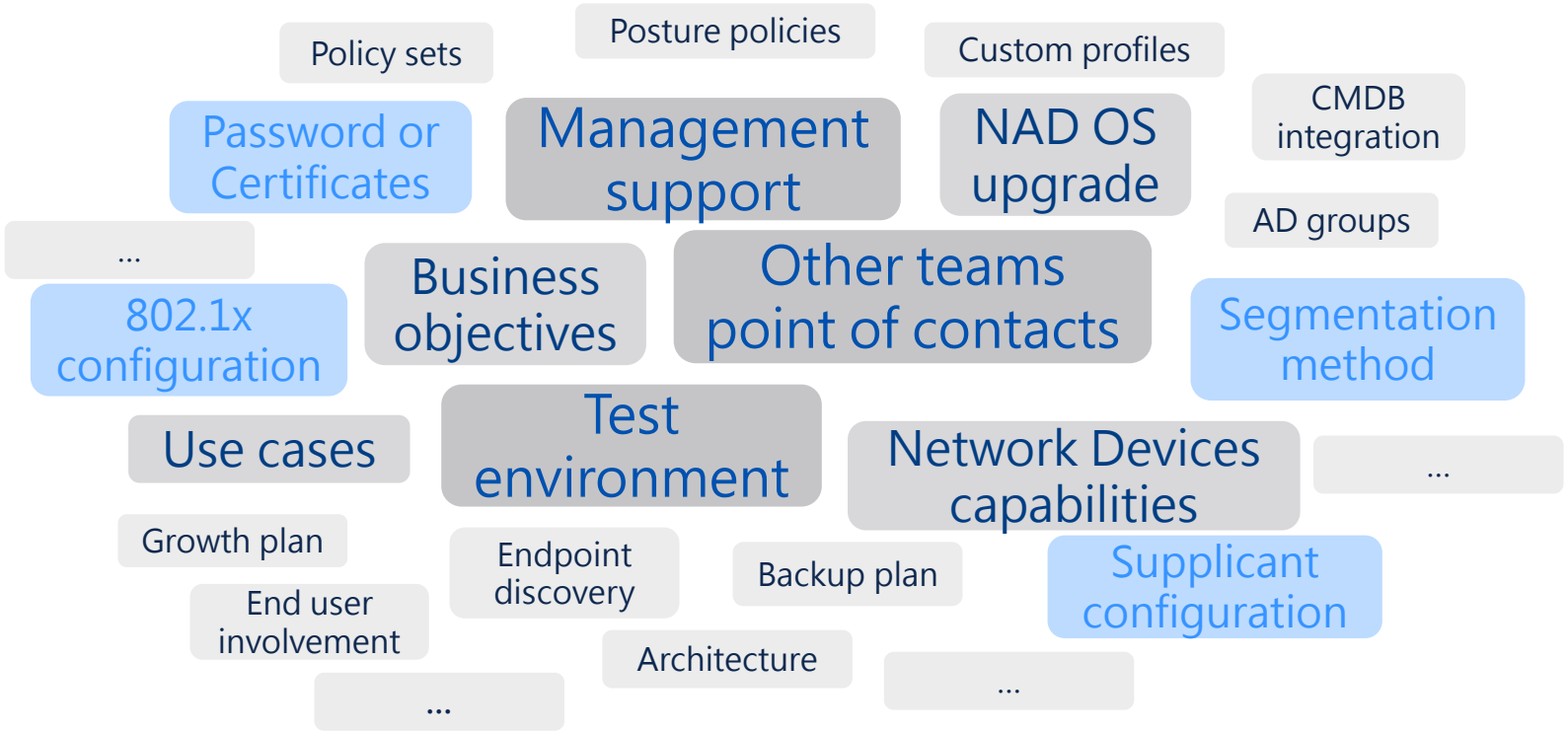
“A goal without a plan is just a wish”

Antoine de Saint-Exupéry

Deploying any network access control solution is crucial

but it isn't easy....

What needs to be included in my planning?



Deploying any network access control solution is crucial

but it isn't easy....

Proper planning is essential to a successful deployment.

Who am I?

Technical Solutions Architect

Cyber Security EMEA

In Cisco since 24 years...

... And 3 countries

Main interest on

- Policy and Access
- Segmentation
- Industrial Security

Cisco ISE High Level Design

- Business Objectives
- Environment
  (Network Device vendor, supplicants, PKI)
- Scenarios & Use Cases
  (Posture, BYOD, Device Administration)
- Policy Details
  (External Identity Sources, what type of posture what type of BYOD
- Operations & Management
- Scale & High Availability

ISE High Level Design (HLD)

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

48001 VIEWS · 77 HELPFUL · 0 COMMENTS

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.

Business Objectives

Identify the Customer Business Objectives that ISE must solve. Typically this involves regulations and compliance or identified security threats and risks to smooth operation of the business or brand. But it also involves mitigating risks with controlled network access for everyday IT processes. This is how you begin to craft your network access control policy. The more specific you can be, the better.

Consider the following example business objectives that must translate into access control policy :

- We want to provide sponsored guest access to our visitors
- All network device administration commands must be authorized and logged for potential audit
- We want to identify all endpoints on our network so we can begin to apply access control policies
- We do not want our employees personal devices on our corporate network
- We want our employees to any device they want but we want to manage it to ensure it and any information on it is properly secured
- Printers should only talk to print servers
- We need to be able to re-image our workstations over the network via PXE
- We must comply with [PCI, HIPAA, etc.] regulation
- All Windows devices must be patched within the last 30 days to minimize known vulnerabilities
- We want to automatically quarantine endpoints when [Stealthwatch, AMP, etc.] detects malicious behavior

Business Objectives

Agenda

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

What not to expect:

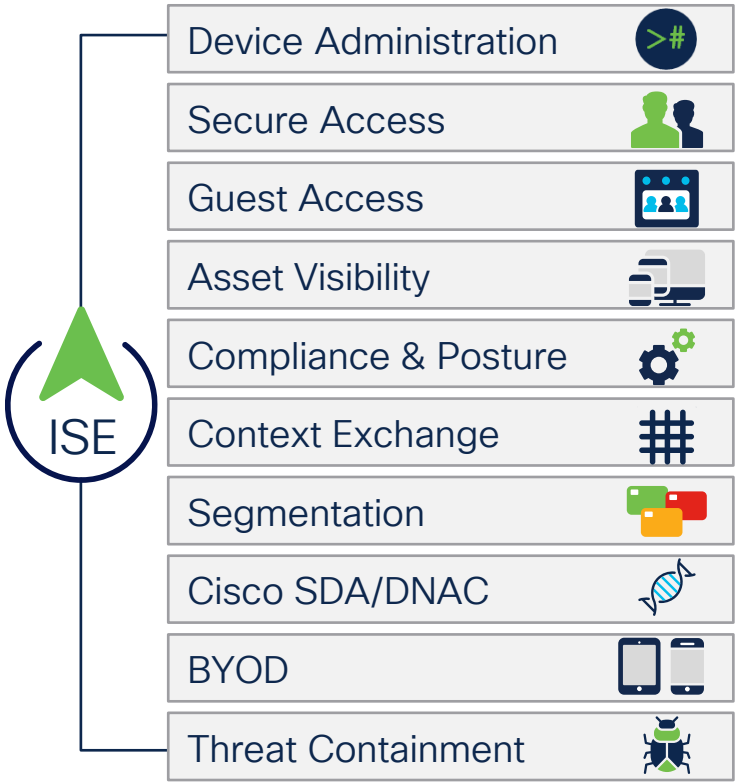
- Specific ISE use cases and their implementation
- Detailed configuration guidelines
- Troubleshooting information
- Licensing

This presentation has many links to resources helping with most of them

Agenda

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

What are your business priorities?



What is the business trying to accomplish with ISE?

Profiling is critical with today IoT proliferation

From where do you want to start?

Do you need a BYOD policy?

Which use cases could be considered for the future?

cisco Live!

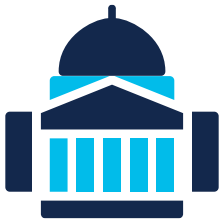
Defining your Security Policy

What is an IT security policy?

"It identifies the rules and procedures for all the individuals accessing and using an organization's IT assets and resources."

Everyone Has Different Needs

Government



Financials

Healthcare

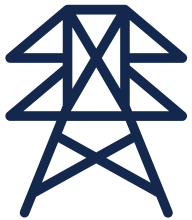
Retail

Education

Transportation

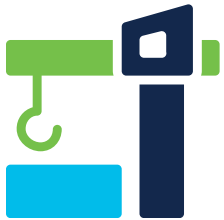
Services

Utilities



Technology

Manufacturing



Example of your ISE policy planning

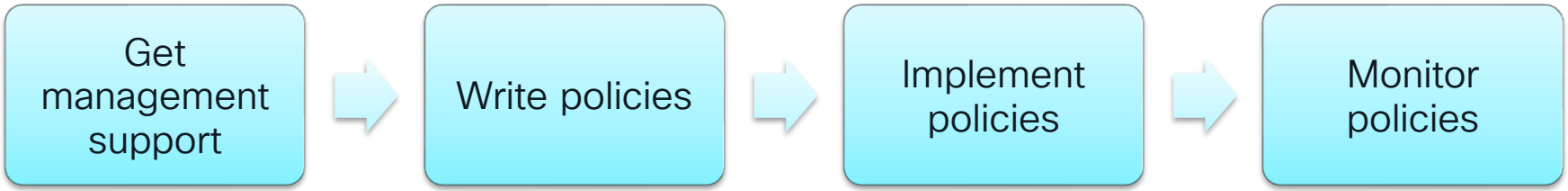
Endpoint Type	Authentication	Identity Store	Network Access	Enforcement	Staging / Provisioning
Corp PC	802.1X – Cert	ISE Cert Store	Full Access	VLAN CORP	Physical Staging Port
Guests	WebAuth	ISE Guest DB	Internet-Only	VLAN Guest	Manual Connect Sponsored account
Access Point	802.1X – User/Pass	ISE User DB	Trunk	Trunk	AP Provisioning
AP Provisioning	MAB	ISE MAC Whitelist	WLC-Only	VLAN AP	ISE Profiling
Printers	MAB	ISE MAC Whitelist	Print Servers-Only	VLAN Printers	ISE Profiling

Endpoint Team Network Team Security Team

Remember: do not think only at positive outcome.
What if a corporate PC certificate is expired?

Interoperation with other teams

- Management buy in is critical to have support of your decisions
- Get the right contacts in the other teams ahead of time
- Monitor and update polices with your IT Security Policy



Understand Your Needs and Use cases

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
- Scale Horizontally
- Scale Vertically
- Geography

Management & Operations

- Top Down / Bottom Up?
- Org(s) / Regions / Departments
- Collaboration or Siloes
- Scheduling Config Changes
- Tooling & Automation

Agenda

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

ISE Personas

Policy Administration Node (PAN)

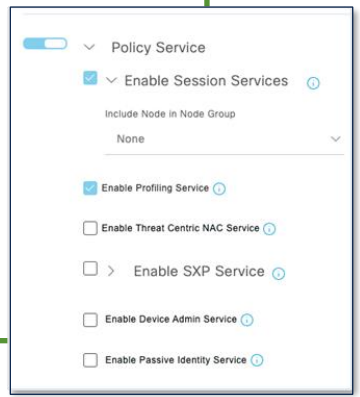
- Administrative GUI
- Policy configuration
- Policy replication
- Centralized Guest database
- Centralized BYOD database
- Configuration REST APIs

Monitoring & Troubleshooting Node (MNT)

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

Policy Service Node (PSN)

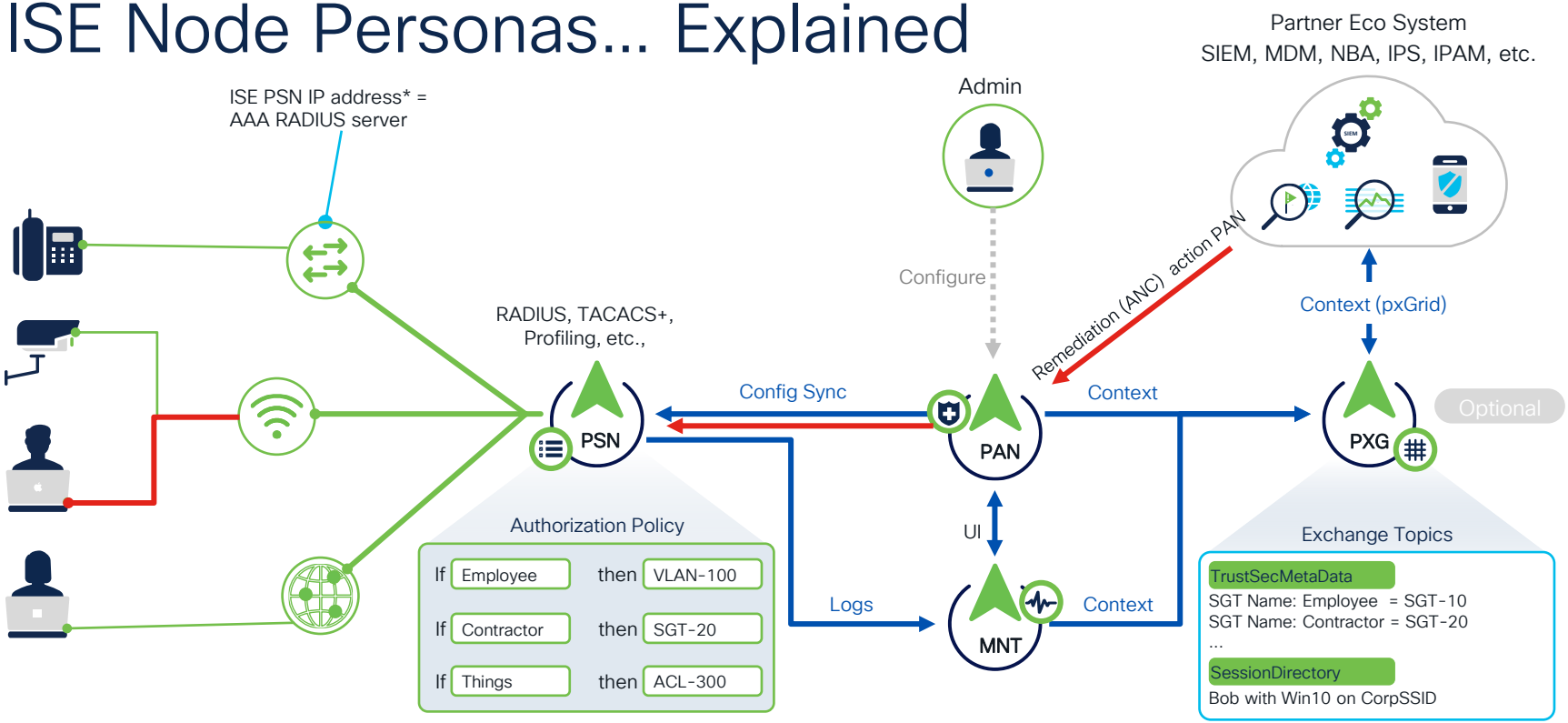
- TACACS requests
- RADIUS requests
- Endpoint profiling probes
- Identity store queries
- Hosts Guest/BYOD portals
- MDM/Posture queries
- TC-NAC & SXP services



Platform Exchange Grid Node (PXG)

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

ISE Node Personas... Explained



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

ANC = Adaptive Network Control

ISE Architecture

Standalone ISE

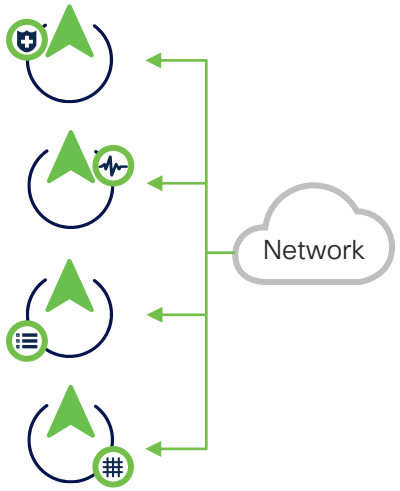
Policy Administration Node (PAN)
- Max 2 in a deployment

Monitoring & Troubleshooting Node (MnT)
- Max 2 in a deployment

Policy Services Node (PSN)
- Max 50 in a deployment

pxGrid Controller
- Max 4 in deployment

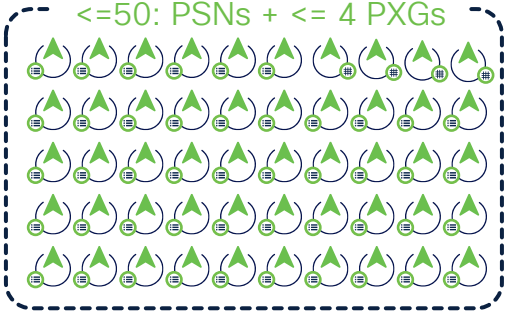
Distributed ISE



ISE Distributed Deployment Scale

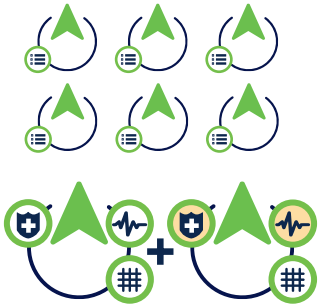
Same for physical and virtual deployments

Compatible with load balancers

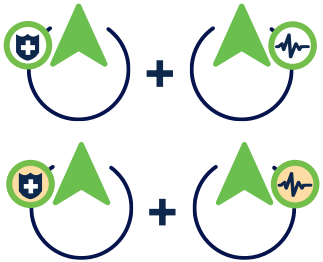


Standalone
(for Lab and
Evaluation)

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



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



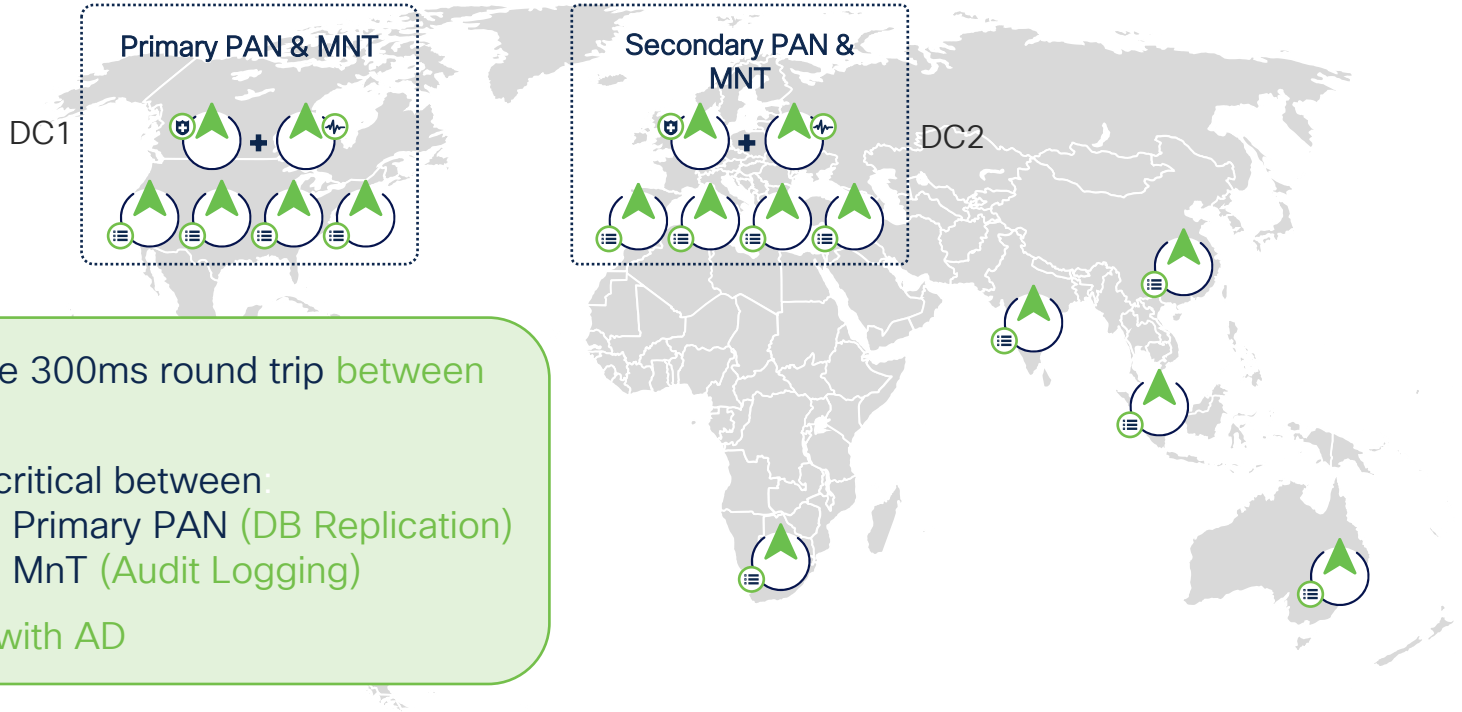
Large Deployment
2 PAN, 2 MNT, <=50: PSNs
+ <= 4 PXGs

100 Endpoints	Up to 50,000 Endpoints	Up to 150,000 Endpoints	Up to 2,000,000 Endpoints	3700
100 Endpoints	Up to 50,000 Endpoints		Up to 2,000,000 Endpoints	3600

http://cs.co/ise-scale

ISE Fully Distributed Architecture

Centralize in DCs…or Distribute PSNs across Geographies



- Latency should be 300ms round trip between PAN and PSN
- Bandwidth most critical between:
  - PSNs and Primary PAN (DB Replication)
  - PSNs and MnT (Audit Logging)
- Co-locate PSNs with AD

Maximum Concurrent Active Endpoints

- One endpoint is a unique MAC address
- ISE Licensing is counted by *active endpoint sessions*

- RADIUS Accounting defines session **Start** & **Stop** events
- Sessions **Start** upon RADIUS Authorization
- Sessions **Stop** upon :
  - Disconnect
  - Session Expiration
  - Idle Timeout

ISE Nodes – Mix and Match

Physical Appliances	Virtual Machines	Cloud Instances

SNS-3715
SNS-3755
SNS-3795

SNS-3615
SNS-3655
SNS-3695

KVM

Microsoft

NUTANIX

vmware

aws

Azure

OCI

Reminders

ISE platforms

SNS 3515
SNS 3595

EOL

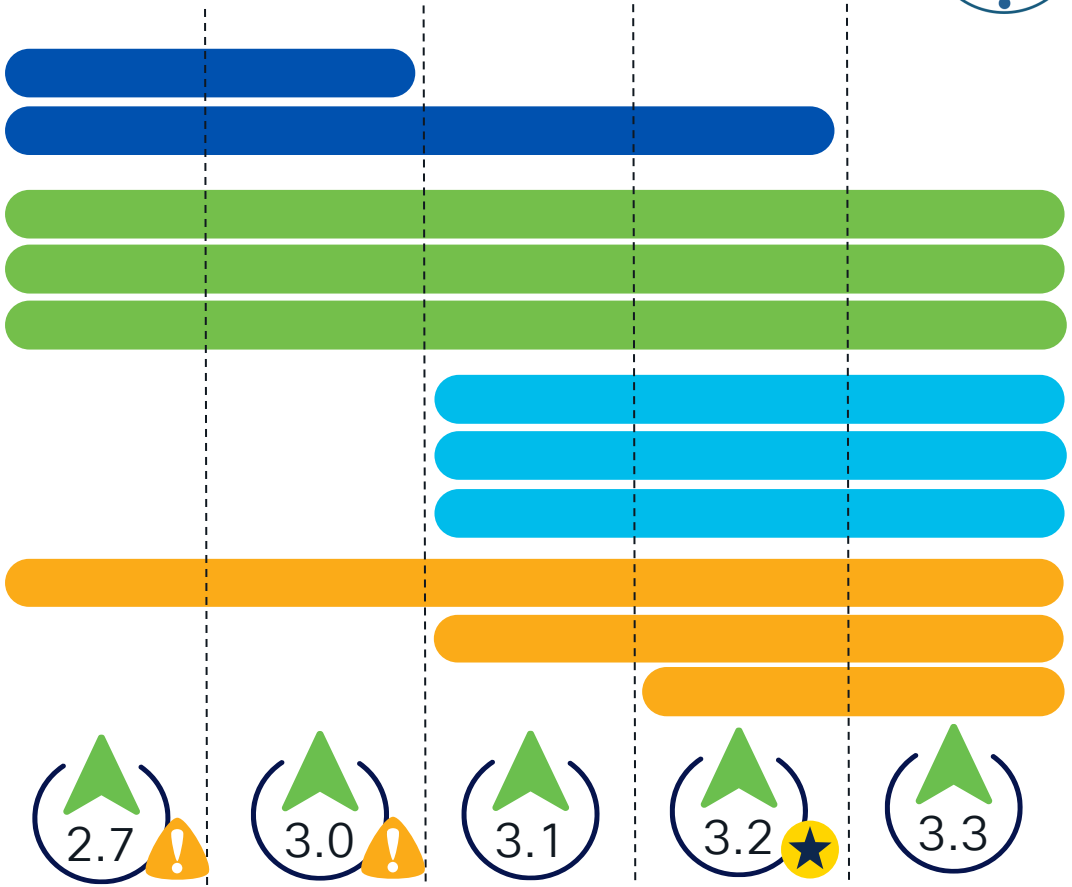
SNS 3615
SNS 3655
SNS 3695

EOL

SNS 3715
SNS 3755
SNS 3795

VM

Traditional VM
AWS
Azure & OCI



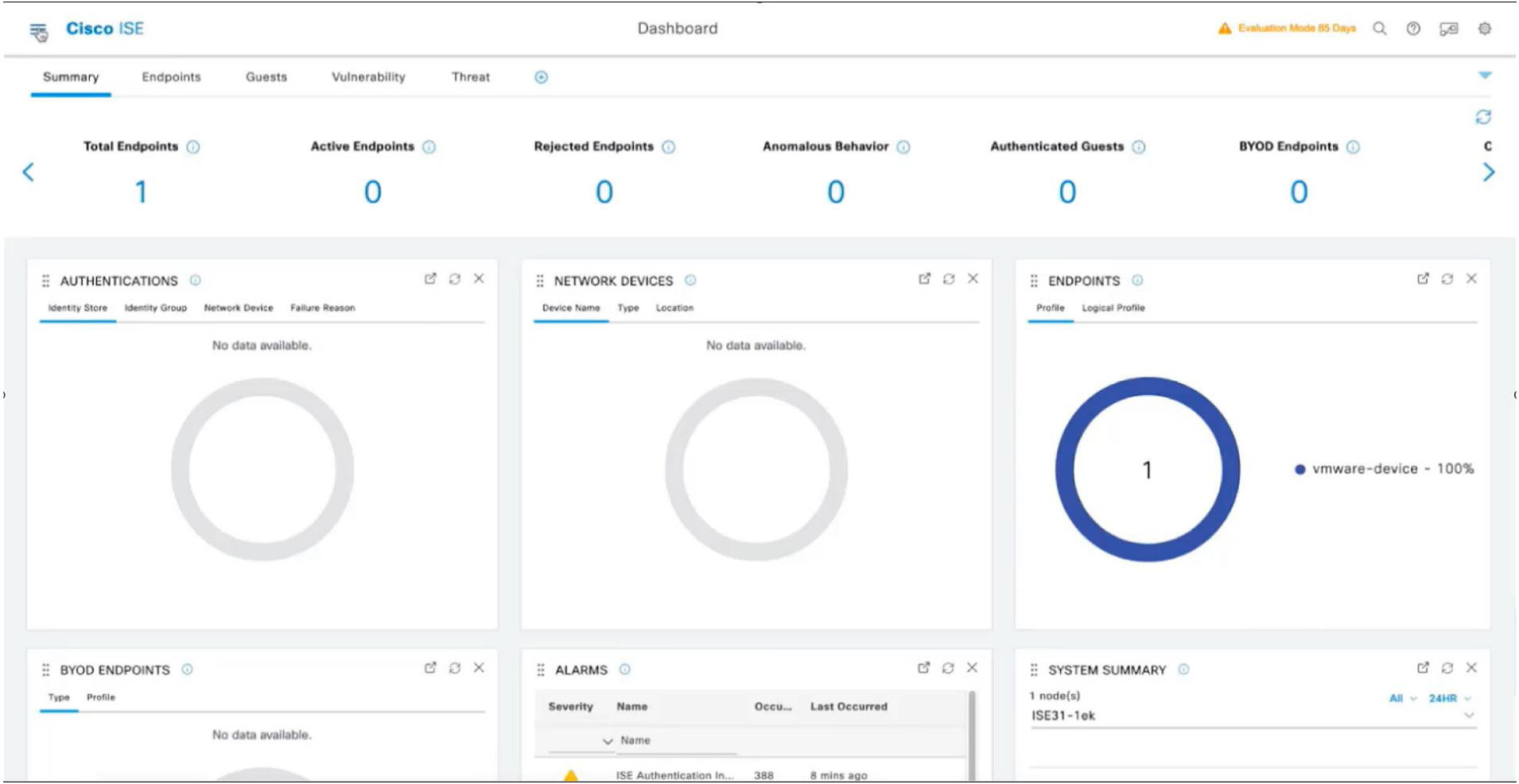
ISE Performance & Scale

- Deployment Architectures: S / M / L
- Maximum Concurrent Active Sessions
- Deployment Scale Limits
- Protocol Performance
- Scenario Performance
- PxGrid and SXP scaling
- Network Device maximum numbers

cs.co/ise-scale

Go to page to check for current numbers

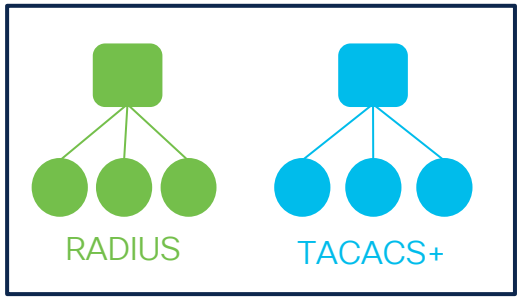
Platform	Concurrent active endpoints supported by a dedicated PSN (Cisco ISE node has only PSN persona)	Concurrent active endpoints supported by a shared PSN (Cisco ISE node has multiple personas)
Extra Small (VM only)	12.000	unsupported
SNS 3615	25,000	12.500
SNS 3715	50,000	25.000
SNS 3655	50,000	25.000
SNS 3755	100,000	50,000
SNS 3695	100,000	50,000
SNS 3795	100,000	50,000



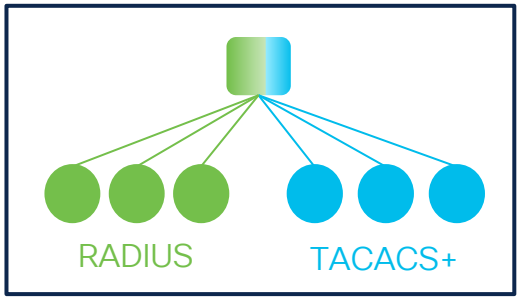
TACACS+ Deployment Models

Separating RADIUS & TACACS+ ISE Cubes?

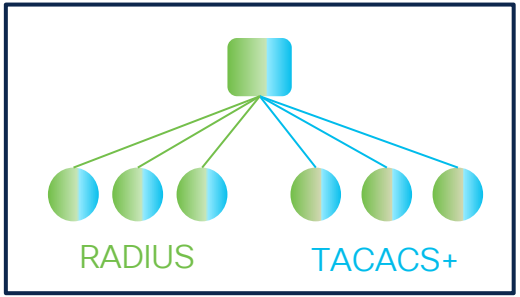
There are three different options:



Separate ISE cubes



Mixed ISE cube with separate PSNs



Mixed ISE cube with shared PSNs

- Scalability is transactions per second (TPS)
- Authentication or also Commands Authorization?
- Do you use scripts?

Agenda

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

ISE Certificates

System Certificates

- Identifies a cisco ISE node & services
- Specific to the node
- Can manage all node's system certs from PPAN

Trusted Certificates

List of CAs

- Trusts for the identities of entities interacting with ISE
- Replicated to all the nodes in deployment

ISE Issued Certificates

- Internal CA service
- Issues and manages certificates for endpoints, pxGrid and ISE messaging

Different ISE System certificates

Endpoint
(Supplicant/Client)

Network Device
(Authenticator)

AAA Server
(Authentication Server)

Identity and
Security Services

802.1X
VPN

RADIUS

ISE

CA

pxGrid

HTTPS / TLS

SCEP

HTTPS / TLS

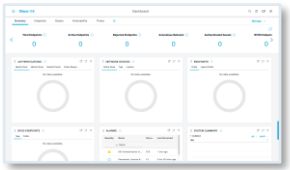
EAP Authentication

BYOD

EAP Tunnel

RADIUS DTLS

TLS Tunnel



ISE Admin (GUI plus Node communication)

HTTPS / TLS

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 10.48.26.63. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Portals

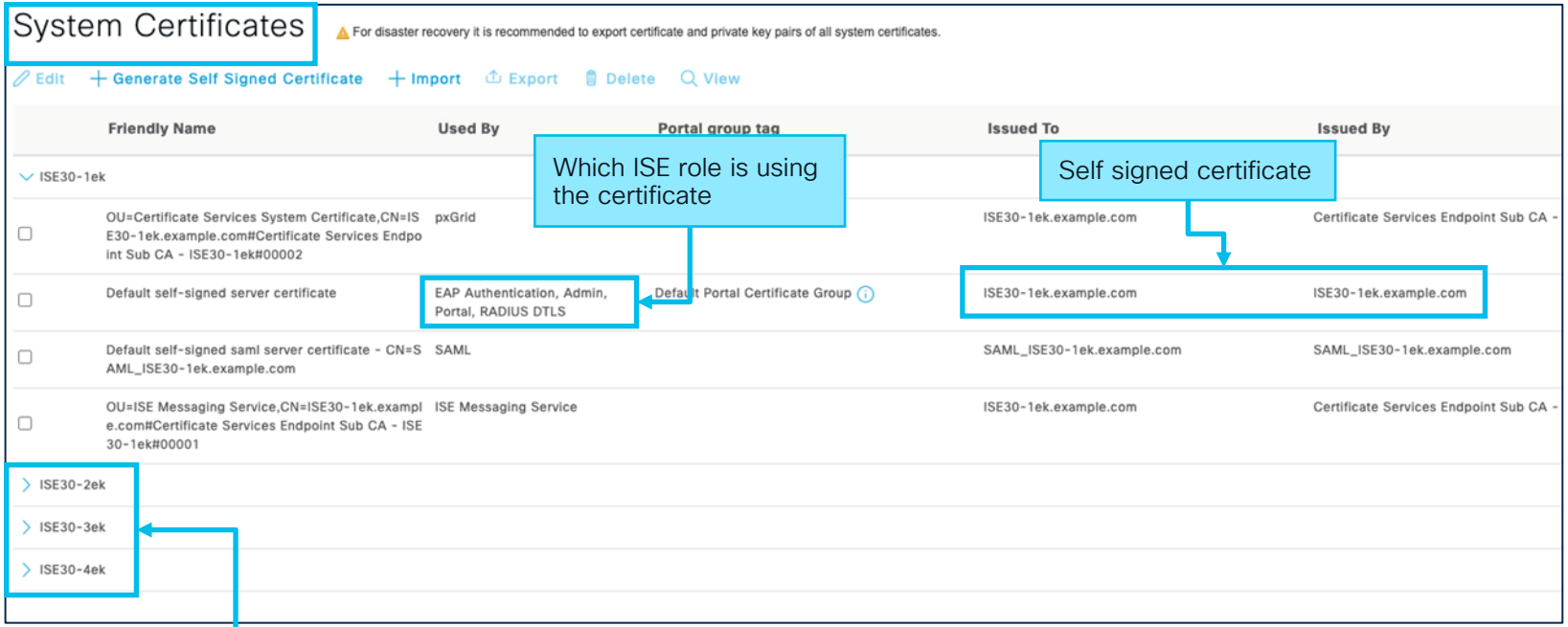
HTTPS / TLS

SAML

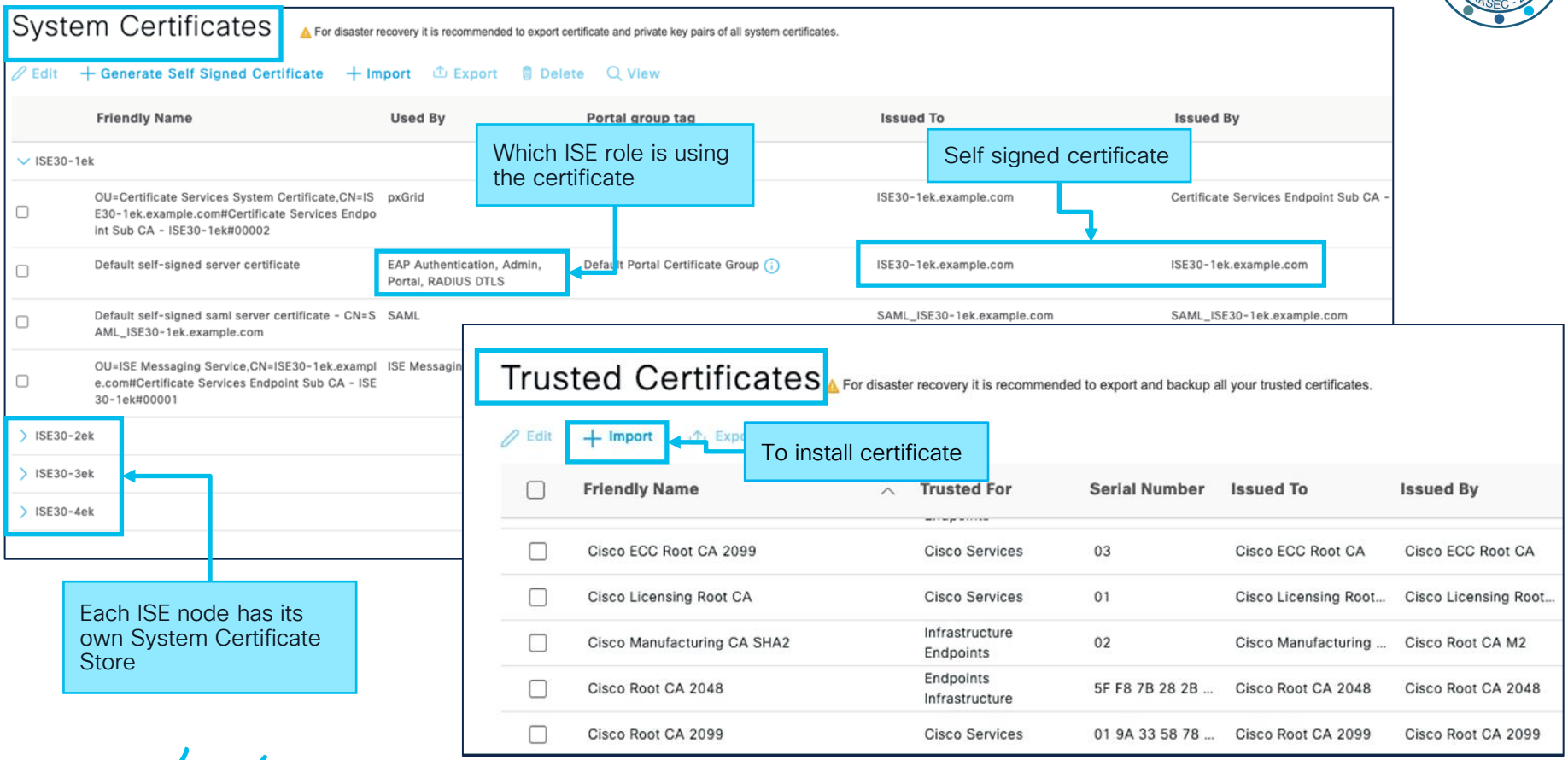
HTTPS / TLS

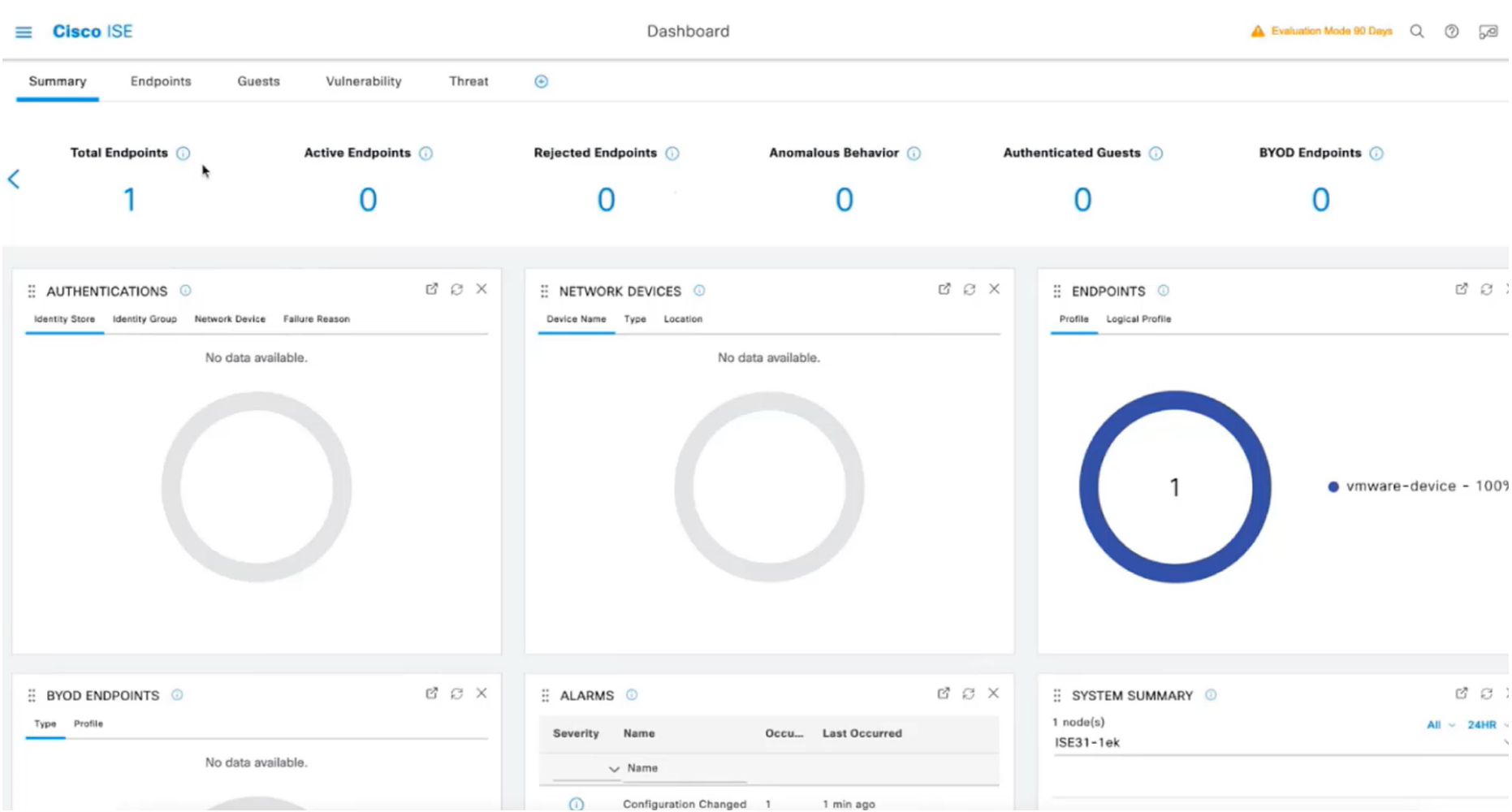
<SAML>

Systems and Trusted Certificates



Systems and Trusted Certificates



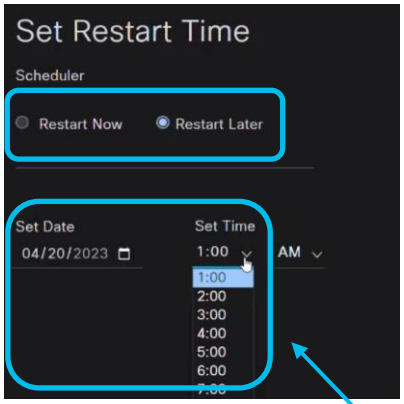


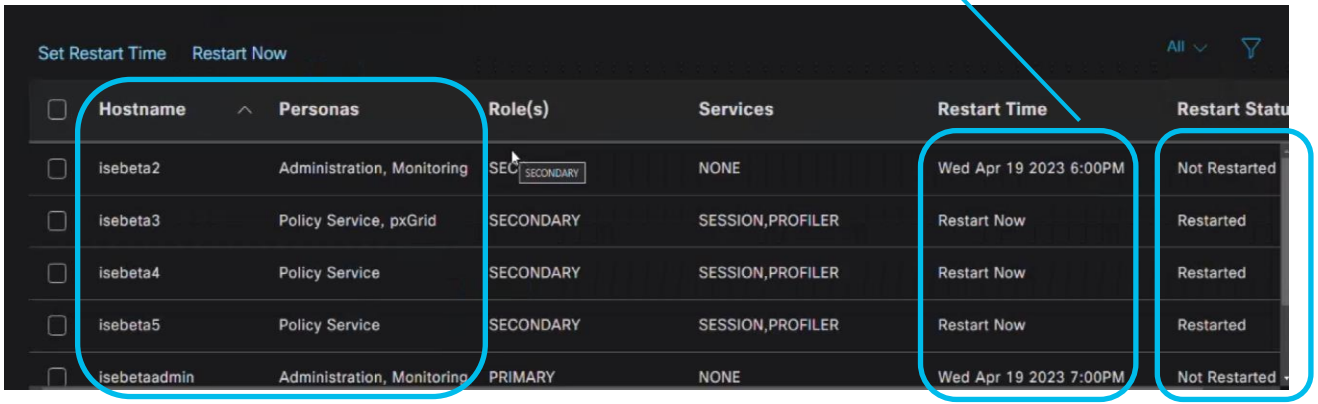
Controlled Application Restart

Up to ISE 3.2 a new ISE admin certificate requires reboot of all the nodes without any control.

From ISE 3.3, the reboot can be scheduled for each node.

Reboot must take place within 15 days

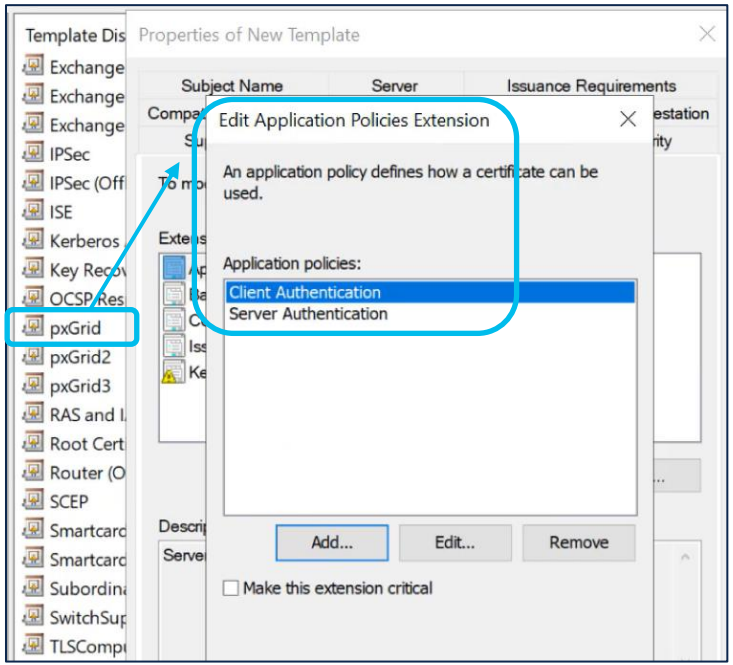




PxGrid Certificate

PxGrid certificate is built with both Client Authentication and Server Authentication extension

Need to create your template and use it for the Signing Request



Agenda

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

Network Device discovery/capabilities

- Hardware model
- IOS version
- Count
- OS Version and capabilities
- Hardware limitations

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

cs.co/nad-capabilities

[2] Refer to Cisco Compatibility Matrix

Table 1. Features and Functionalities

Feature	Functionality
AAA	802.1X, MAB, VLAN Assignment, dACL
Profiling	RADIUS CoA and Profiling Probes
BYOD	RADIUS CoA, URL Redirection and SessionID
Guest	RADIUS CoA, Local Web Auth, URL Redirection and SessionID
Guest Originating URL	RADIUS CoA, Local Web Auth, URL Redirection and SessionID
Posture	RADIUS CoA, URL Redirection and SessionID
MDM	RADIUS CoA, URL Redirection and SessionID
TrustSec	SGT Classification

Validated Cisco Access Switches

Table 2. Validated Cisco Access Switches

Device	Validated OS [1] / Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
IE2000 IE3000	IOS 15.2(2)E4 IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	IOS 15.0(2)EB	√	√	√	√	X	√	√	√
IE4000 IE5000	IOS 15.2(2)E5 IOS 15.2(4)E2 IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
IE4010	IOS 15.2(2)E5 IOS 15.2(4)E2	√	√	√	√	√	√	√	√
	IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
SMB SG500	Sx500 1.4.8.06	[4]	!	X	X	X	X	X	X
	Sx500 1.2.0.97	!	!	X	X	X	X	X	X

Does ISE Support my third-party Network device? Does my third-party Network Device Supports ISE?

Overview

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.

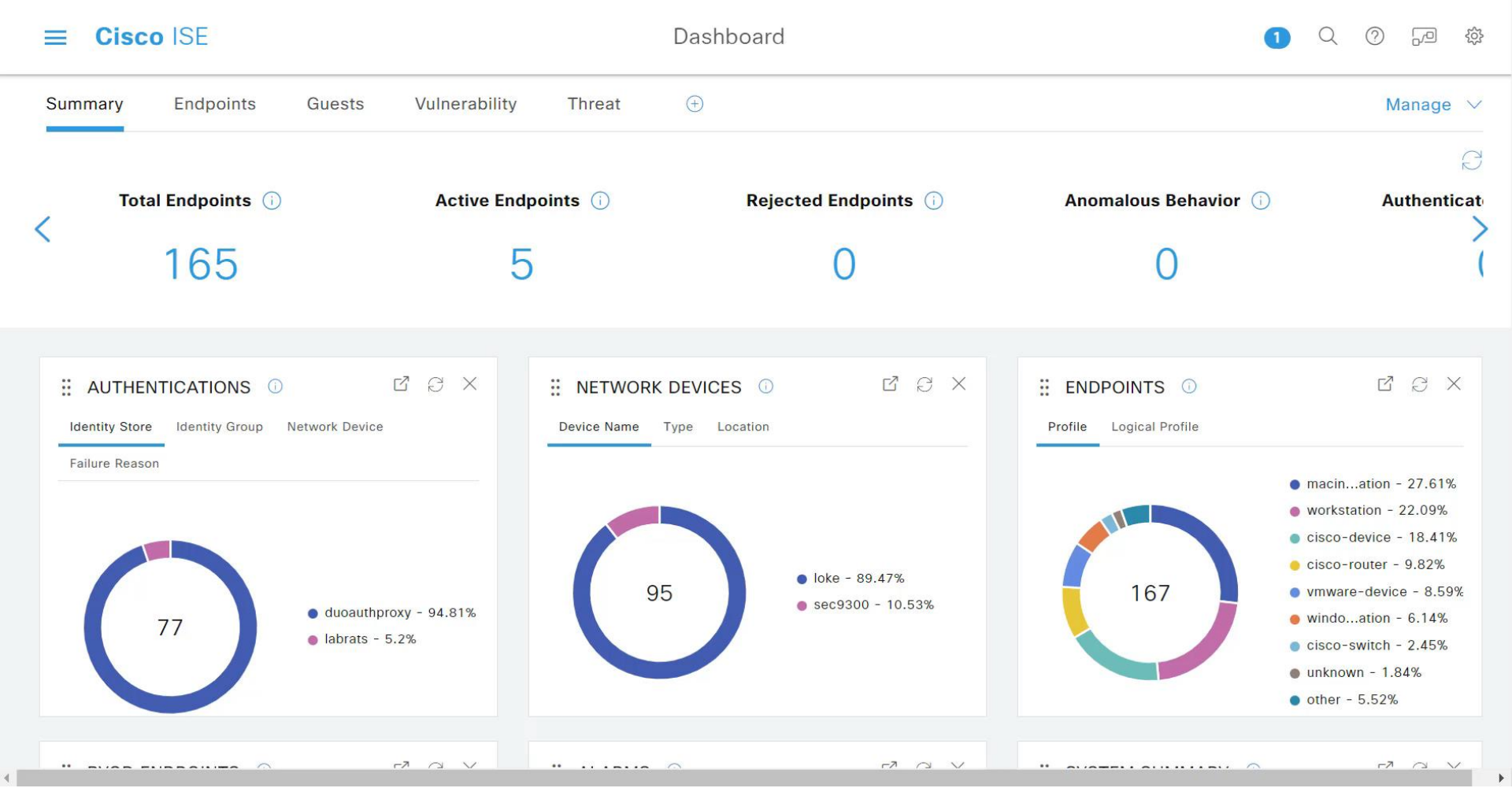
Check for Advanced capabilities support:

- CoA (RADIUS or SNMP)
- URL Redirection

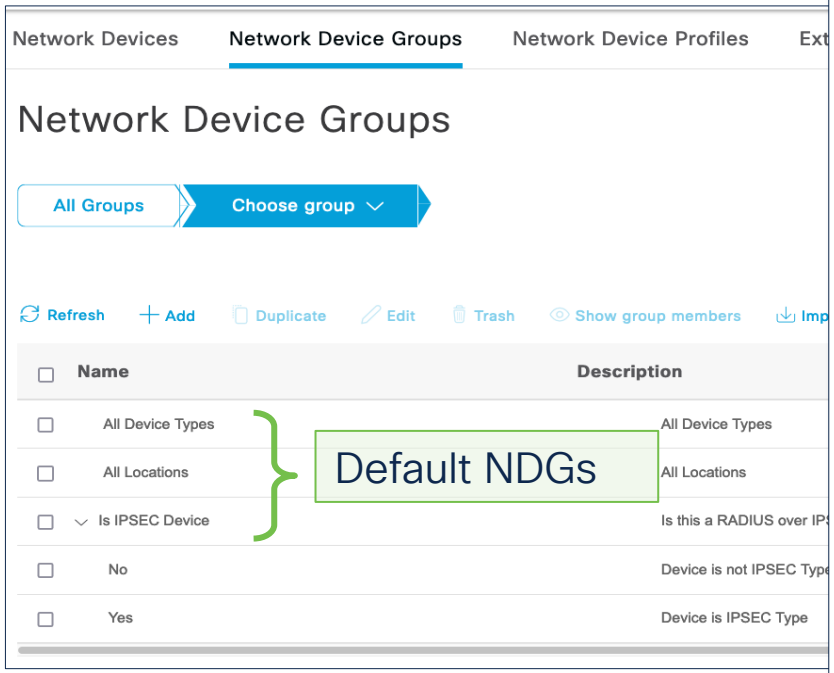
Might need to:

- Import a Vendor Specific Dictionary
- Create Network Device Profile

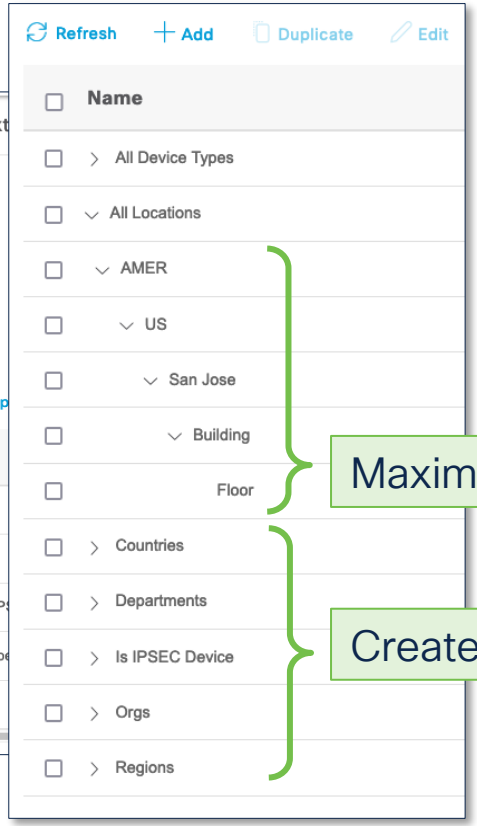
From the Network Component Compatibility, Release 3.3
https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/compatibility_doc/b_ise_sdt_33.html



Default Network Device Groups (NDGs)

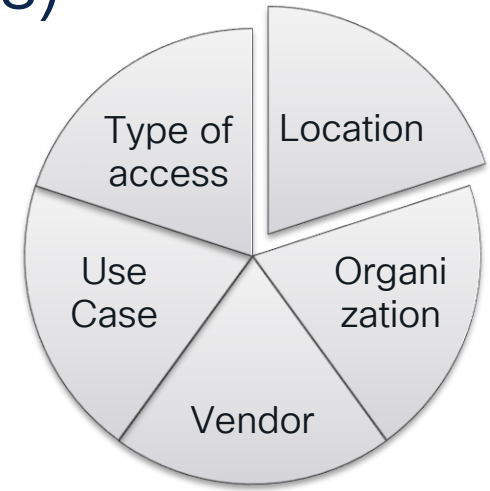


Default NDGs



Maximum 6 Levels

Create Your Own Root NDGs



Additional Tips

- Always Test before implementing!

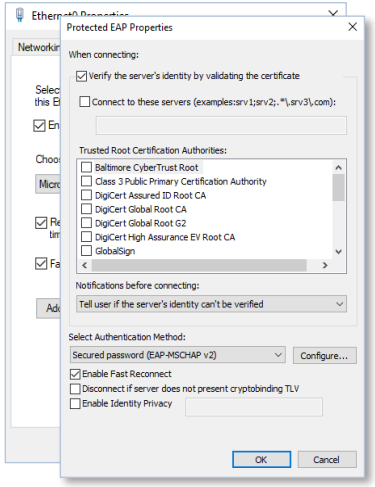
- Standardize! Standardize! Standardize!
  - IOS versions
  - AAA configuration
  - Wireless configuration
  - Profiling configuration

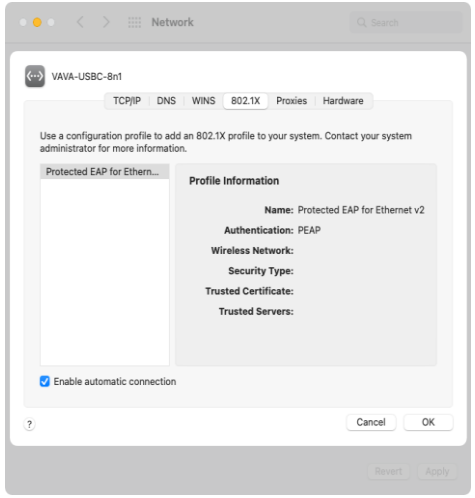
- 3rd party device documentation

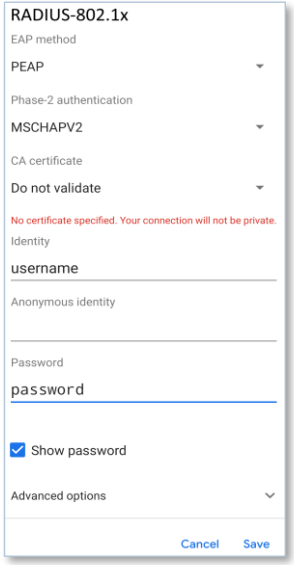
Agenda

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

Endpoints: Native 802.1X Supplicants







```
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
```

Windows 7, 8/8.1, and 10 – Native Supplicant

- Now you can do TEAP directly in Windows for Chaining (Windows 10 build 2004 and ISE 2.7 Patch 2)
- Involve the Active Directory Team
- Group Policy for:
  - Supplicant configuration
  - Pushing certificates
  - Pre-configure SSIDs – better user experience

Agenda

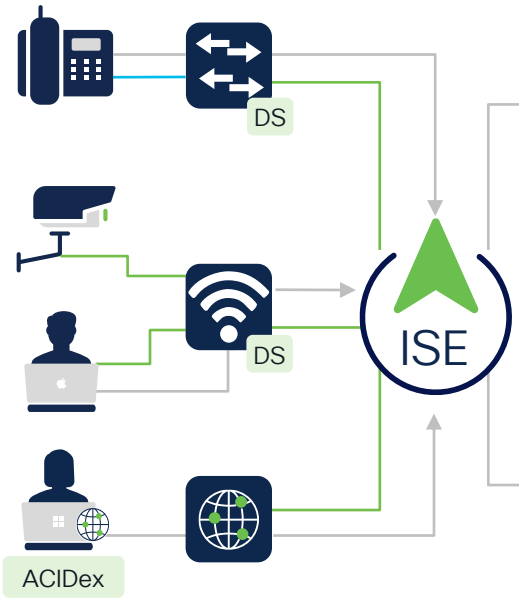
- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

Endpoints: Everything Else

Endpoint Profiling

Identifies dynamically the devices that connect to your network

Endpoints send interesting data, that reveal their device type



ISE Data Collection Methods for Device Profiling

Active Probes: Netflow | DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | AD

Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

Cisco Secure Client (formerly AnyConnect): ACIDex

Feed Service (Online/Offline)

MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

Effect of RADIUS Probe

 vendor	OUI = Vendor ID, IP = xx.xx.xx.xx
 Cisco Device	OUI = Cisco, IP = xx.xx.xx.xx
 HP Device	OUI = HP, IP = xx.xx.xx.xx
 Apple Device	OUI = Apple, IP = xx.xx.xx.xx

Effect of SNMP Probe

 Unknown	OUI = Random, IP = xx.xx.xx.xx
 Cisco Device	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971
 HP Device	OUI = HP, IP = xx.xx.xx.xx
 Apple Device	OUI = Apple, IP = xx.xx.xx.xx

Effect of DHCP Probe

 Microsoft Workstation	OUI = Random, IP = xx.xx.xx.xx, **dhcp-class-identifier CONTAINS MSFT**
 Cisco IP Phone 9971	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971, **DHCP:dhcp-class-identifier CONTAINS CP-9971**
 HP Printer	OUI = HP, IP = xx.xx.xx.xx, **DHCP:dhcp-class-identifier CONTAINS LaserJet**
 Apple Device	OUI = Apple, IP = xx.xx.xx.xx, **DHCP:dhcp-DHCP:dhcp-parameter-request-list EQUALS 1, 3, 6, 15, 119, 252**

Effect of DHCP Probe

 Microsoft Workstation	OUI = Random, IP = xx.xx.xx.xx, **dhcp-class-identifier CONTAINS MSFT**
 Cisco IP Phone 9971	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971, **DHCP:dhcp-class-identifier CONTAINS CP-9971**
 HP Printer	OUI = HP, IP = xx.xx.xx.xx, **DHCP:dhcp-class-identifier CONTAINS LaserJet**
 Apple Device	OUI = Apple, IP = xx.xx.xx.xx, **DHCP:dhcp-DHCP:dhcp-parameter-request-list EQUALS 1, 3, 6, 15, 119, 252**

Effect of HTTP Probe

 Windows10-Workstation Microsoft Workstation	OUI = Random, IP = xx.xx.xx.xx, dhcp-class-identifier CONTAINS MSFT, **IP:User-Agent CONTAINS Windows NT 10.0**
Cisco IP Phone 9971	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971, DHCP:dhcp-class-identifier CONTAINS CP-9971
 HP Printer	OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet
 Apple iDevice	OUI = Apple, IP = xx.xx.xx.xx, DHCP:dhcp-DHCP:dhcp-parameter-request-list EQUALS 1, 3, 6, 15, 119, 252 **IP:User-Agent contains iPad**

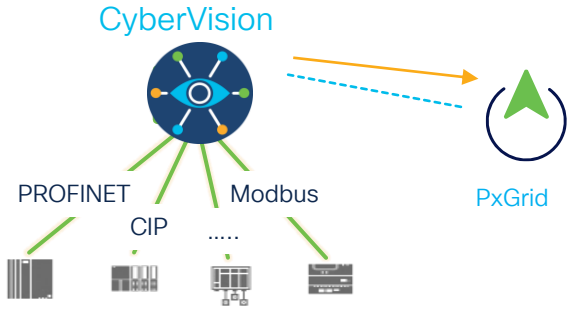
Effect of NMAP Probe

 Windows10-Workstation	OUI = Random, IP = xx.xx.xx.xx, dhcp-class-identifier CONTAINS MSFT, IP:User-Agent CONTAINS Windows NT 10.0, FQDN=test-laptop1.zero0k.org, **NMAP:SMB.operating-system CONTAINS Windows 10**
 Cisco IP Phone 9971	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971, DHCP:dhcp-class-identifier CONTAINS CP-9971, FQDN=test-phone1.zero0k.org
 HP Printer	OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet, FQDN=test-printer1.zero0k.org, **NMAP:hrDeviceDescr CONTAINS HP LaserJet P4015**
 Apple IPad	OUI = Apple, IP = xx.xx.xx.xx, IP:User-Agent contains iPad, FQDN=test-i-pad1.zero0k.org

Effect of AD Probe

 Windows10-Workstation	OUI = Random, IP = xx.xx.xx.xx, dhcp-class-identifier CONTAINS MSFT, IP:User-Agent CONTAINS Windows NT 10.0, FQDN=test-laptop1.zero0k.org, NMAP:SMB.operating-system CONTAINS Windows 10, **AD-OS = Windows 10**
 Cisco IP Phone 9971	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971, DHCP:dhcp-class-identifier CONTAINS CP-9971, FQDN=test-phone1.zero0k.org
 HP LaserJet P4015	OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet, FQDN=test-printer1.zero0k.org, SNMP:hrDeviceDescr CONTAINS HP LaserJet P4015
 Apple IPad	OUI = Apple, IP = xx.xx.xx.xx, IP:User-Agent contains iPad, FQDN=test-i-pad1.zero0k.org

PxGrid Probe Context-in



MACAddress	00:1D:9C:CA:85:8B
MatchedPolicy	Rockwell-Automation-Device
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	5
assetConnectedLinks.assetDeviceType	Switch
assetConnectedLinks.assetId	40109
assetConnectedLinks.assetIpAddress	10.195.119.22
assetConnectedLinks.assetName	IE4000-119-22
assetConnectedLinks.assetPortName	GigabitEthernet1/2
assetDeviceType	Controller
assetId	60100
assetIpAddress	10.195.119.38
assetMacAddress	00:1d:9c:ca:85:8b
assetName	10.195.119.38
assetProductId	1756-EN2TR/C 217021900
assetProtocol	CIP
assetSerialNumber	12174476
assetVendor	Rockwell Automation/Allen-Bradley

1. Profiling tool classifies the devices.
2. The attributes are then sent to ISE via pxGrid
3. ISE populates the custom attributes with the ones received via profiling pxGrid probe

Cisco EA

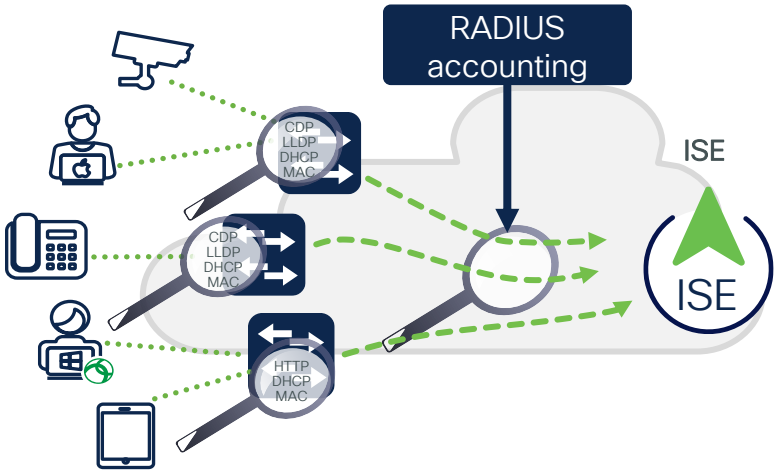
CyberVision

ARMIS

MEDIGATE by Claroty

ordr

Device Sensor to scale attribute collection



Network devices send attributes via RADIUS to ISE to optimize collection:

Attributes used:

- MAC OUI
- CDP/LLDP
- DHCP
- HTTP (WLC only)
- mDNS,
- H323,
- MSI-Proxy (4k only)

From IOS 15.0(2)SE

Meraki MS390

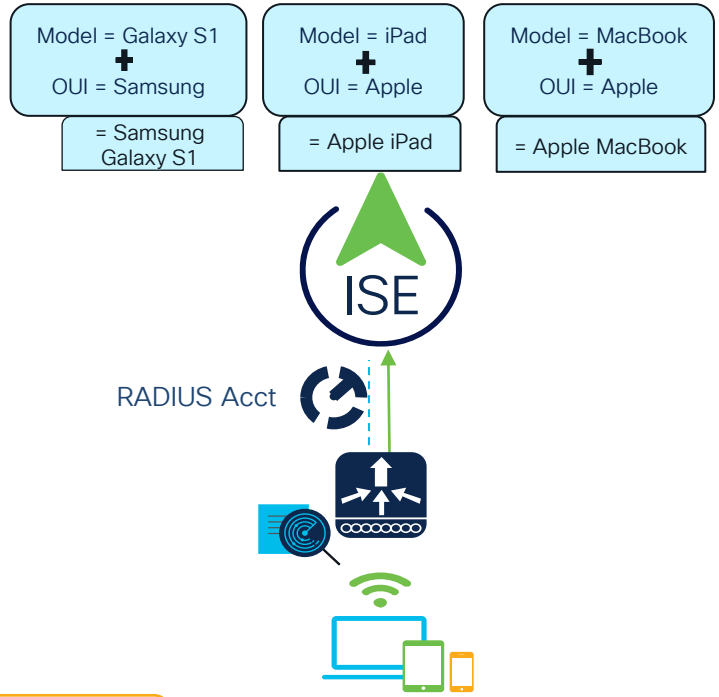
MS Switches only
CDP+LLDP

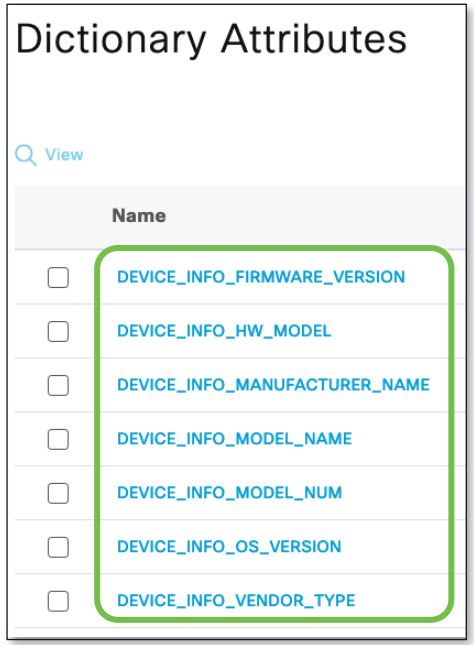
From AirOS 7.2

Wi-Fi Edge Analytics

Apple, Samsung, and Intel devices are sharing rich data with the WLCs.

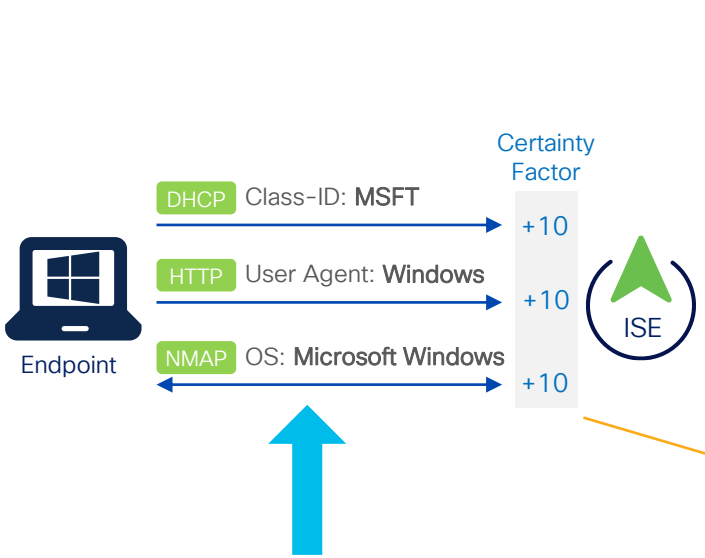
With Catalyst 9800 WLCs (IOS-XE 17.10) you can now pass those attributes to ISE within RADIUS accounting.





Disable the ISE Profiling Endpoint Attribute Filter to use WiFi Device Analytics attributes in policies

ISE profiles definition

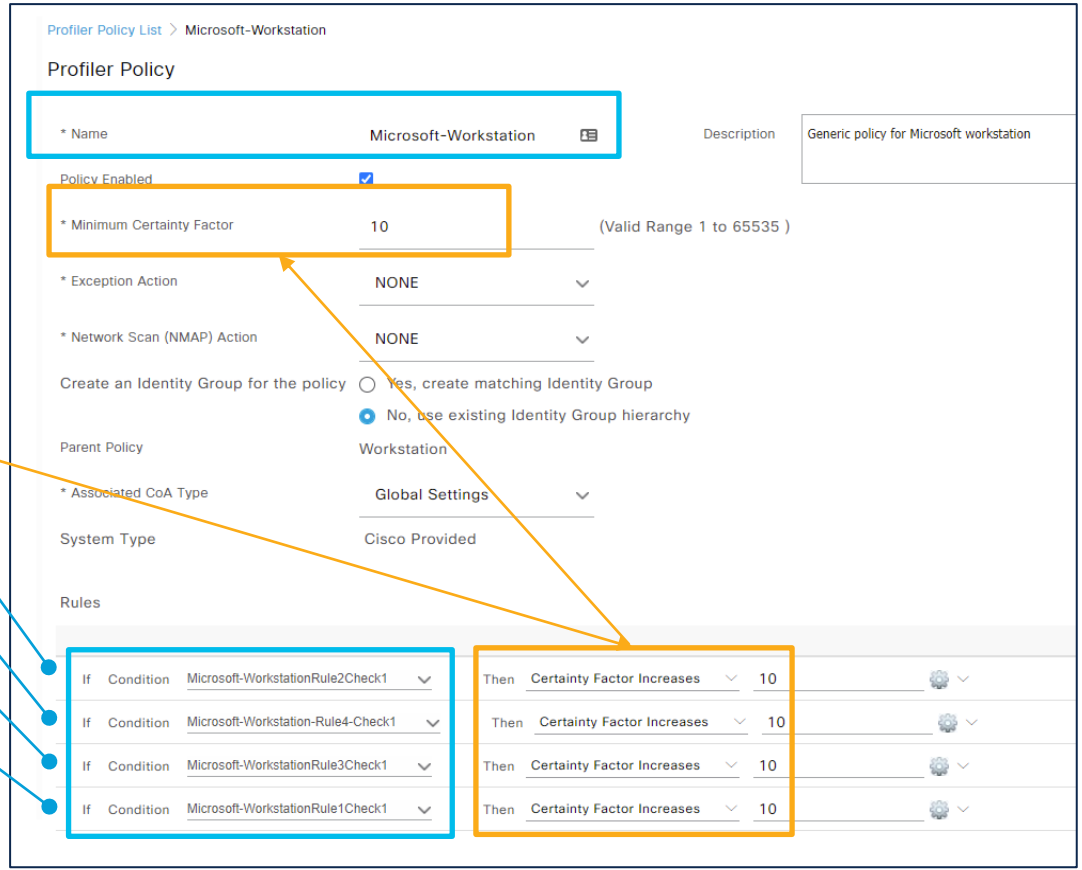


DHCP:dhcp-class-identifier CONTAINS MSFT

DHCP:dhcp-class-identifier CONTAINS MS-UC-Client

IP:User-Agent CONTAINS Windows

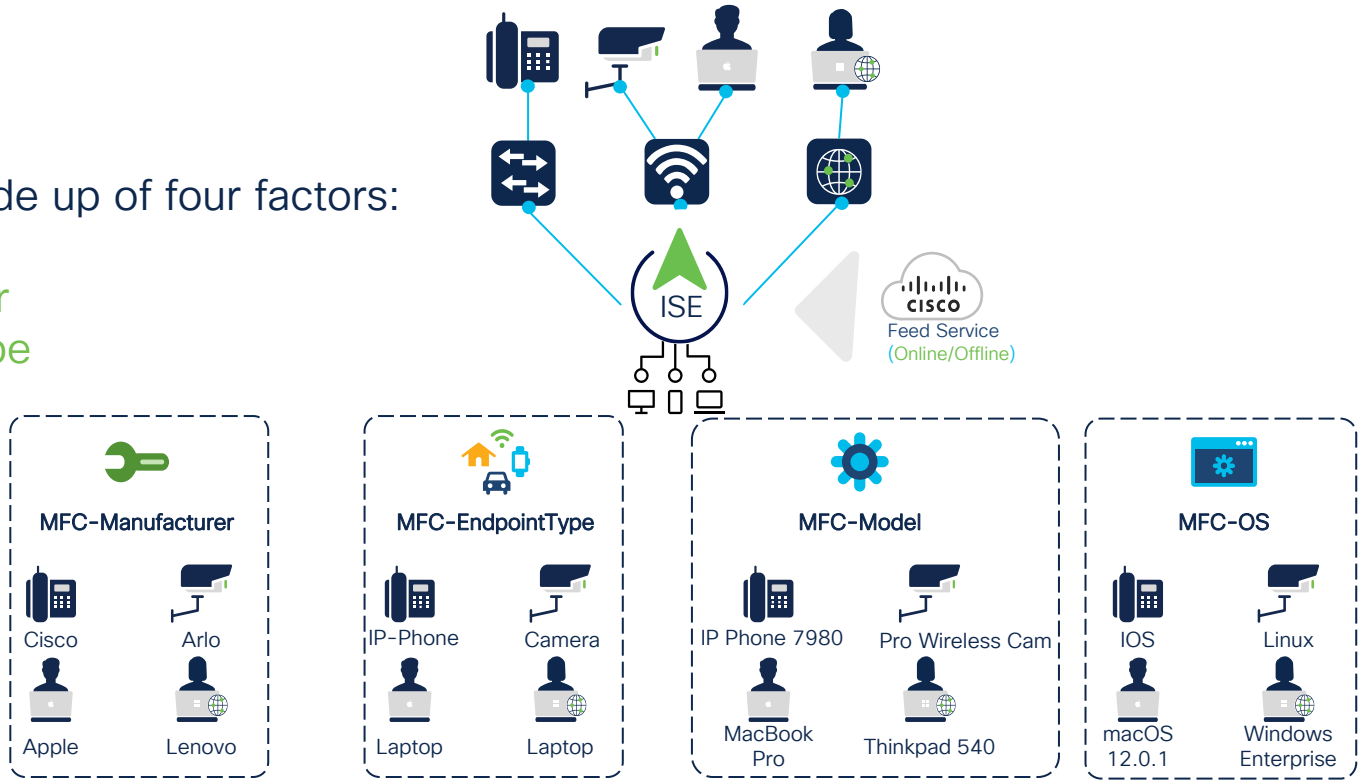
NMAP:operating-system CONTAINS Microsoft Windows



Multi-Factor Classification on ISE

Profiles are now made up of four factors:

- MFC-Manufacturer
- MFC-Endpoint Type
- MFC-Model
- MFC-OS

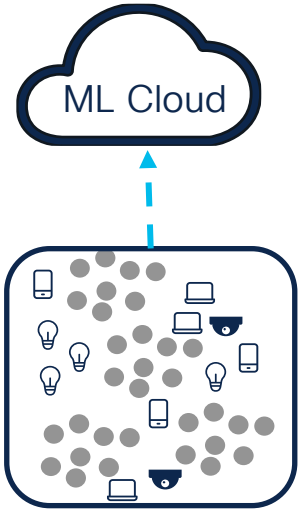


AI Proposed Profiling Policies

ISE 3.3

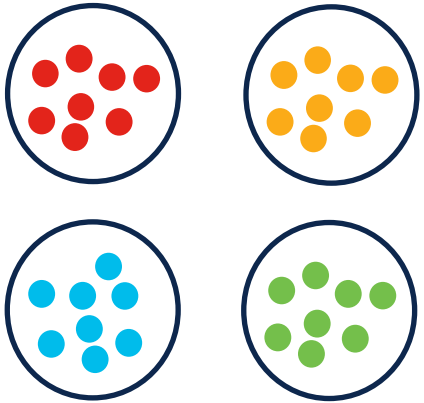
Data Forwarded to Cloud

All data on endpoints (profiled & unknown) forwarded to ML engine



ML Groups Endpoints

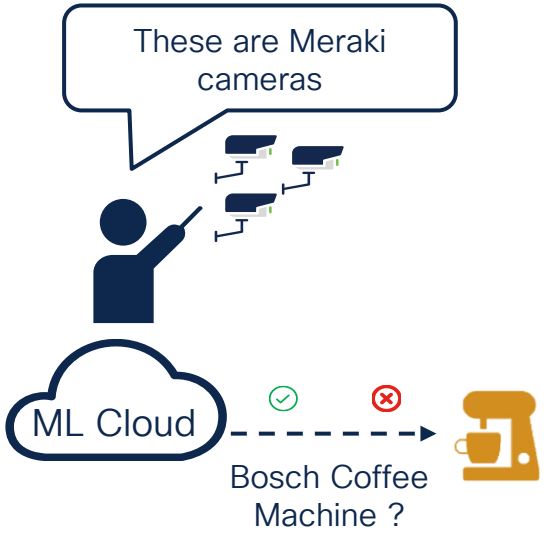
ML groups endpoints into clusters of identical of based on attribute data

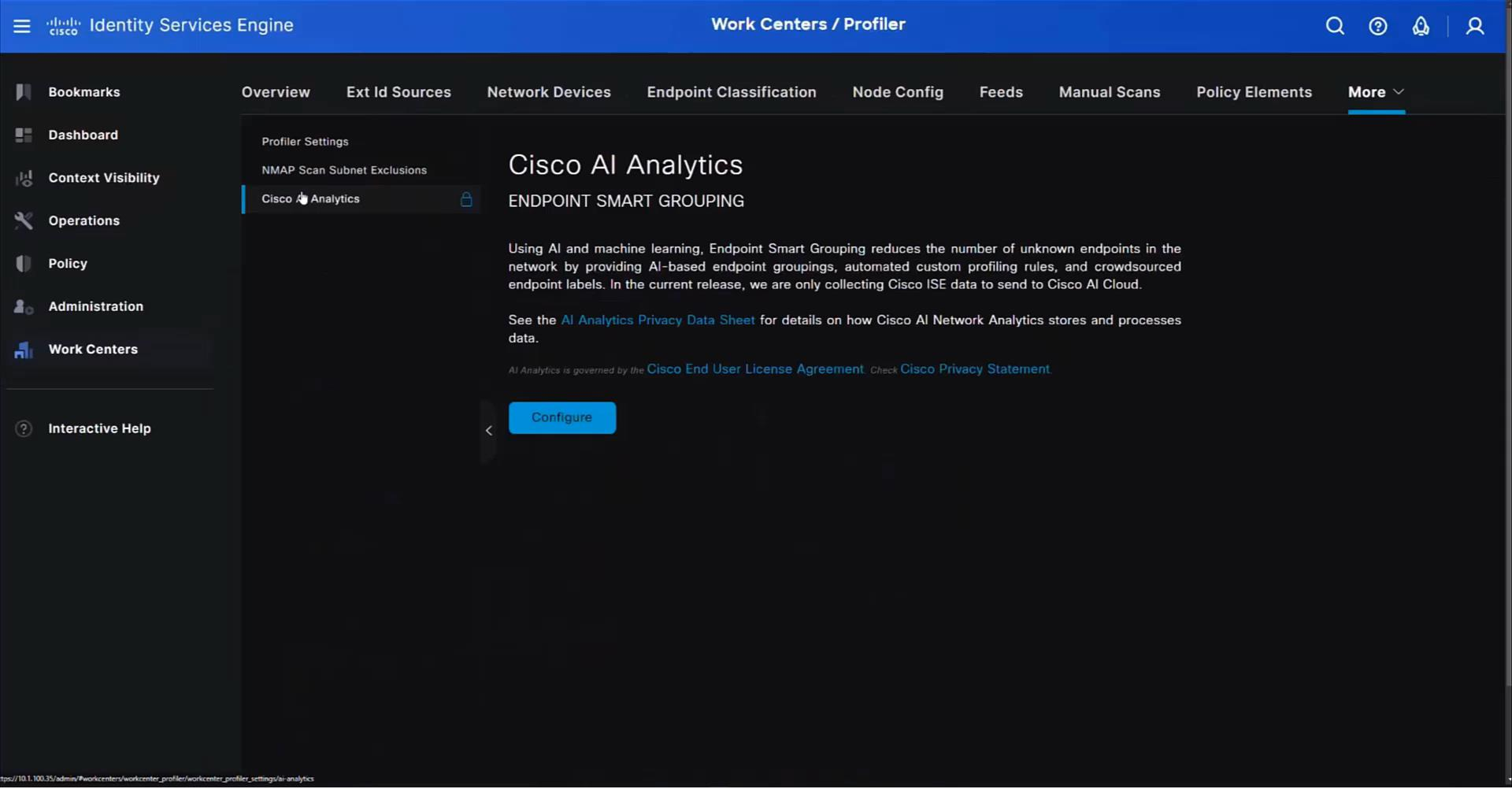


- Must forward endpoint attributes to ML cloud (available 3.2p1)
- Air gapped environments not supported

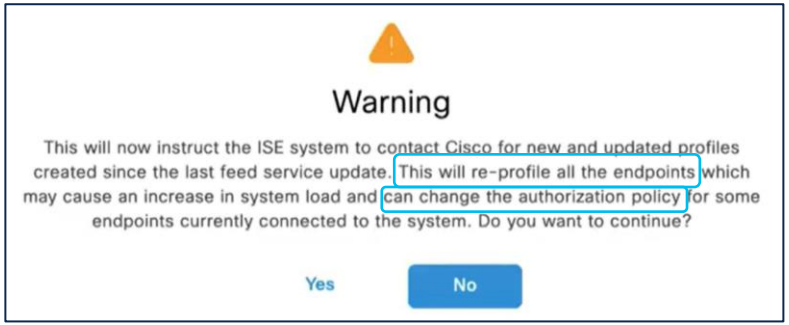
Labels Assigned

Users assign labels to unknown clusters or accept recommendations

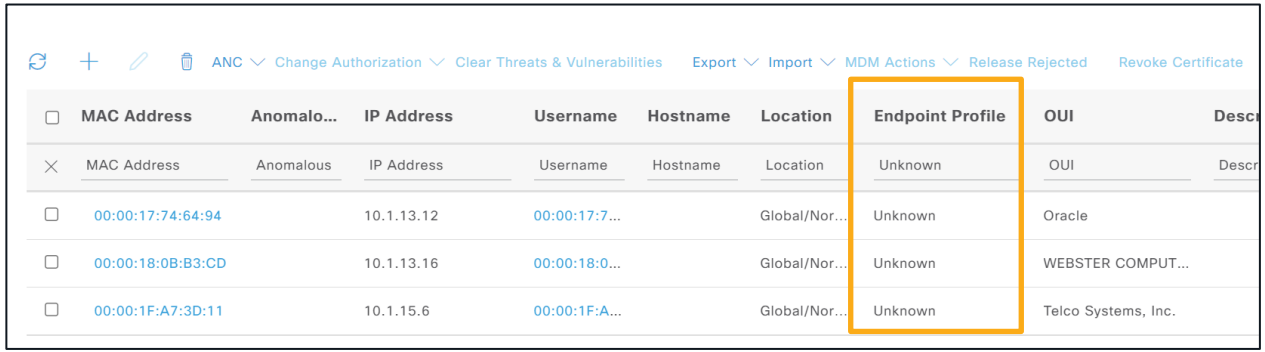




ISE Feed service Updates

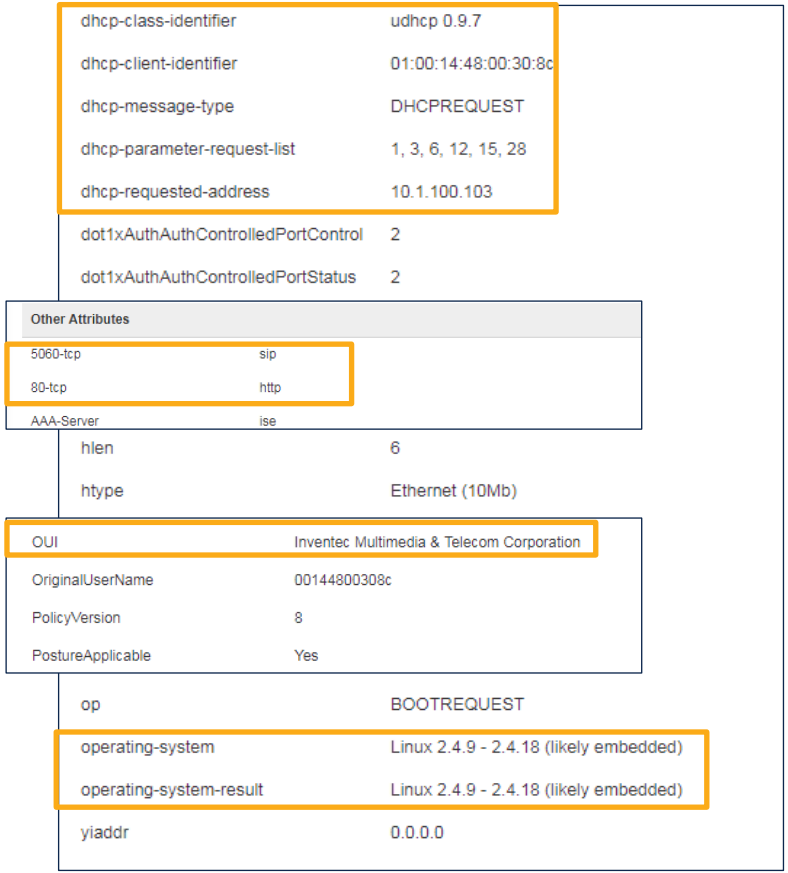


- Feed service updates MAC OUIs
- Feed service provides new and updated profiles
- Be careful when applying profile updates, check they do not interfere with the profiles you have been using and your policies
- You will still have unknowns For everything else: custom profiles



Create custom profiles

- Gather more information
  - Create more traffic from the device
  - Run an NMAP scan
  - Enable more probes
- Find attributes or combinations of attributes unique to device type
- Focus on:
  - Attributes found every time the endpoint connects
  - Attributes found very early after the endpoint connects



Profiles Precedence

Cisco Provided Profile

Existing Cisco Profile

CF = 30

Custom Profile

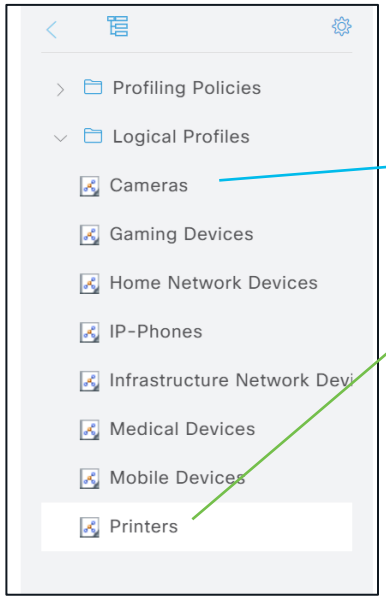
New Customer Profile

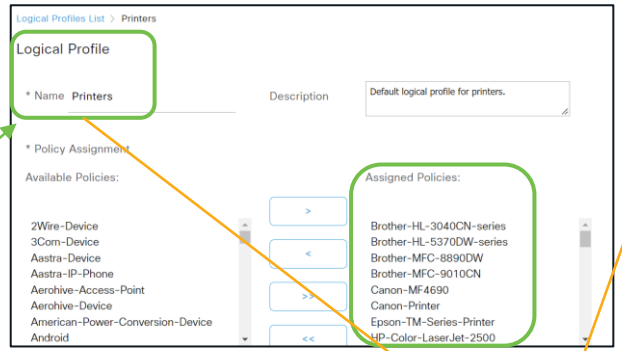
CF >= 30

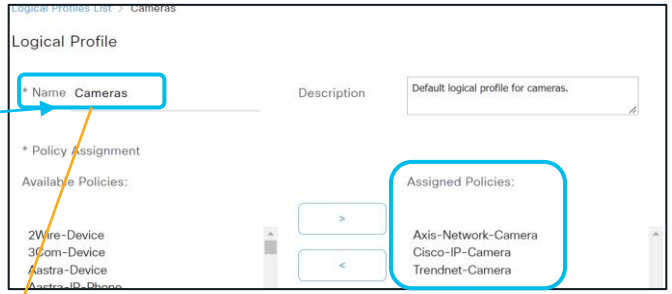
Custom profiles CF should be higher than the ones provided by Cisco. (in general low number).

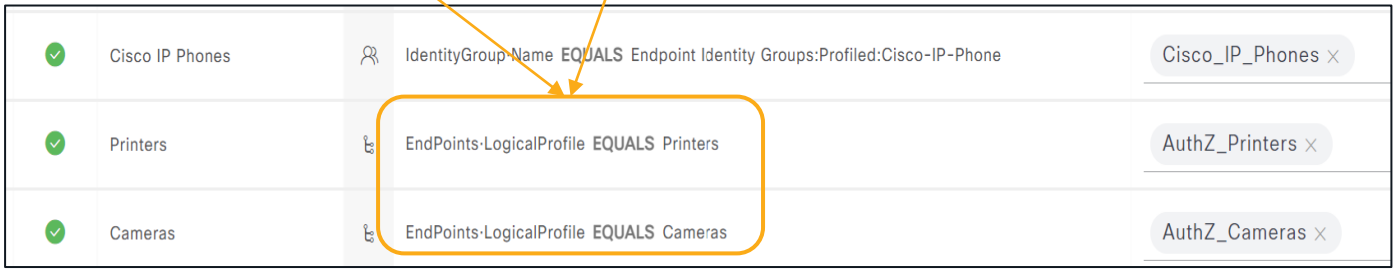
Try put custom profiles above 100

Using device profiles and logical profiles in ISE

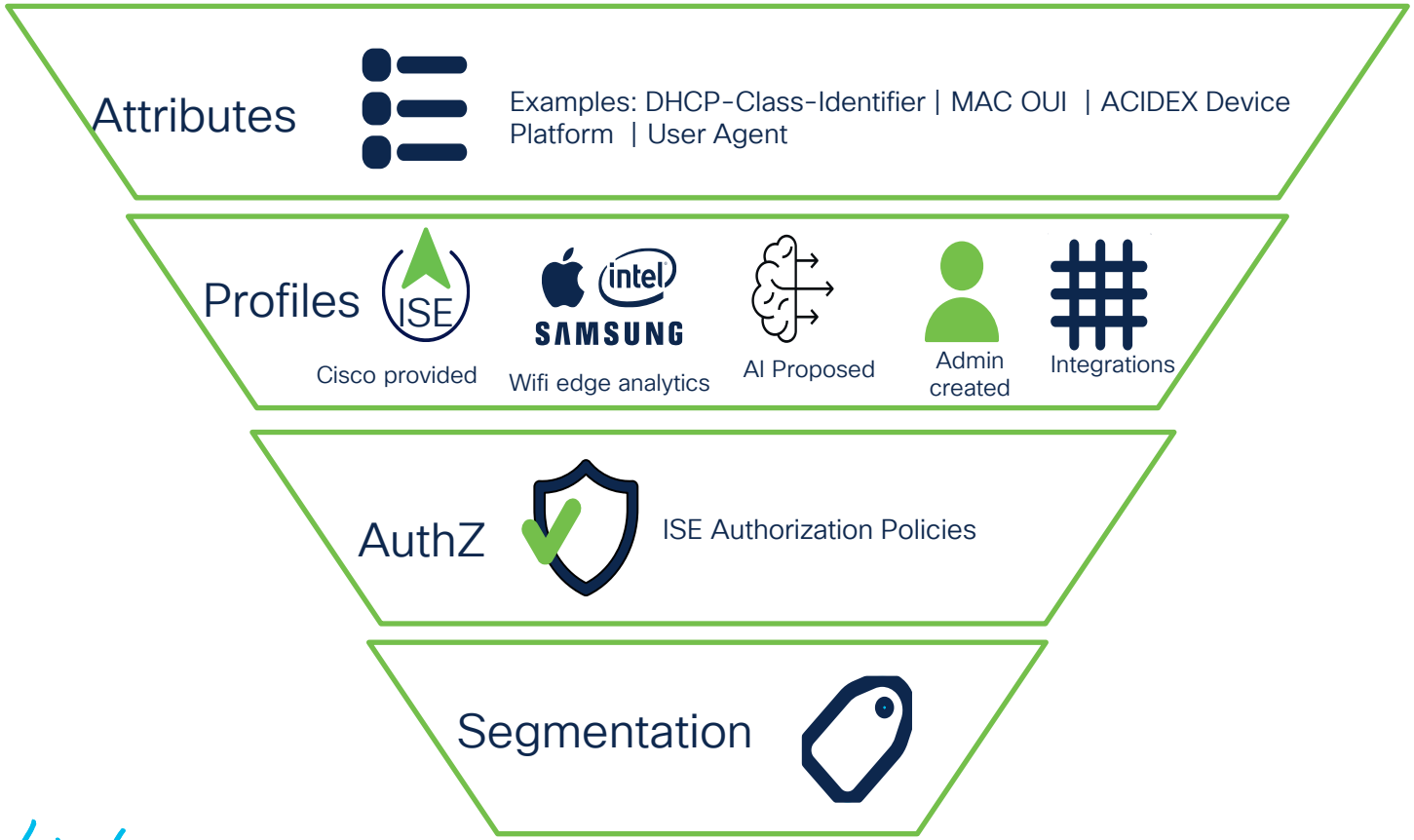








Turning Probes Into Profiles, Profiles Into Protection



Behavioral vs Organizational Endpoint Information

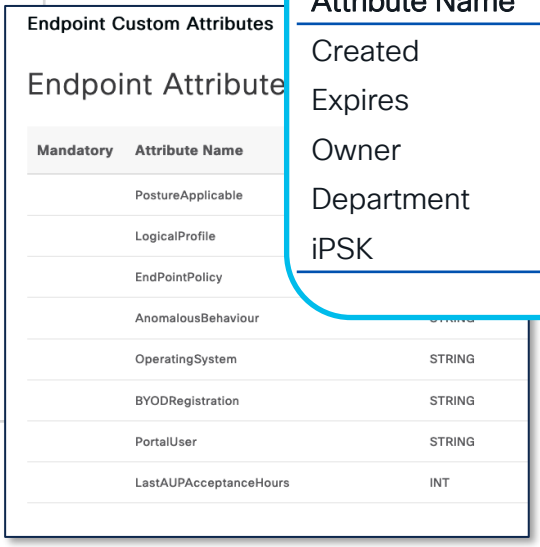
Behavioral

- Probes and profiling
- Device Sensor
- pxGrid Context-In

Organizational

- Endpoint Custom Attributes
- Context Visibility Input (GUI/CSV)
- Custom Attributes and endpoint REST API (JSON)

- External Databases (CMDBs)
- Active Directory / LDAP
- pxGrid Direct (ServiceNow, etc.)

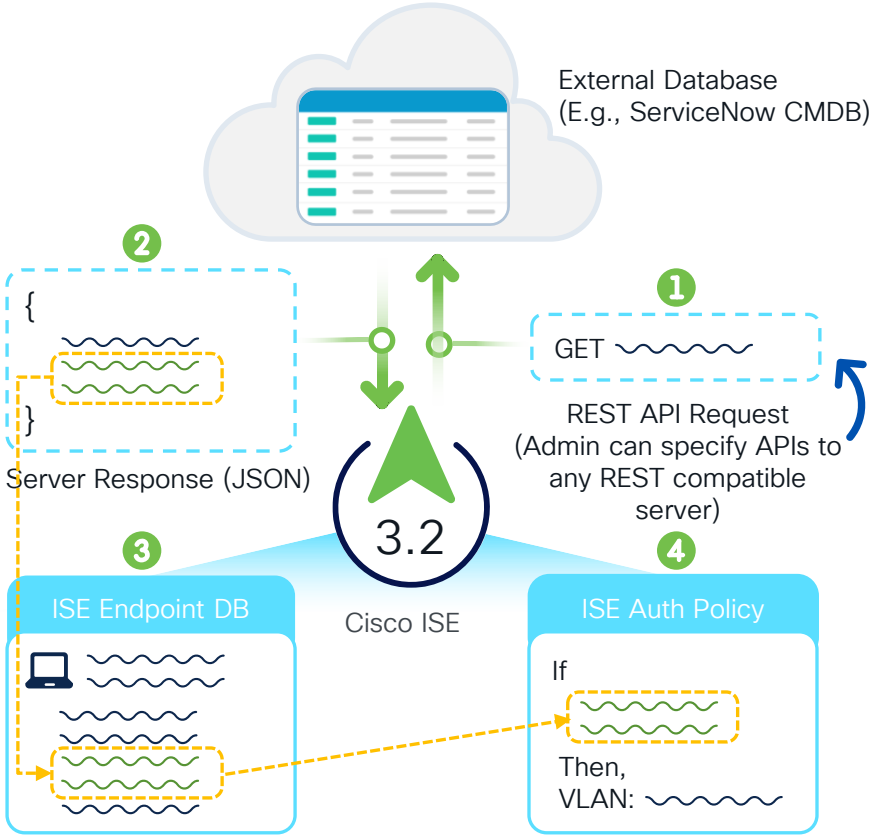


Common Uses

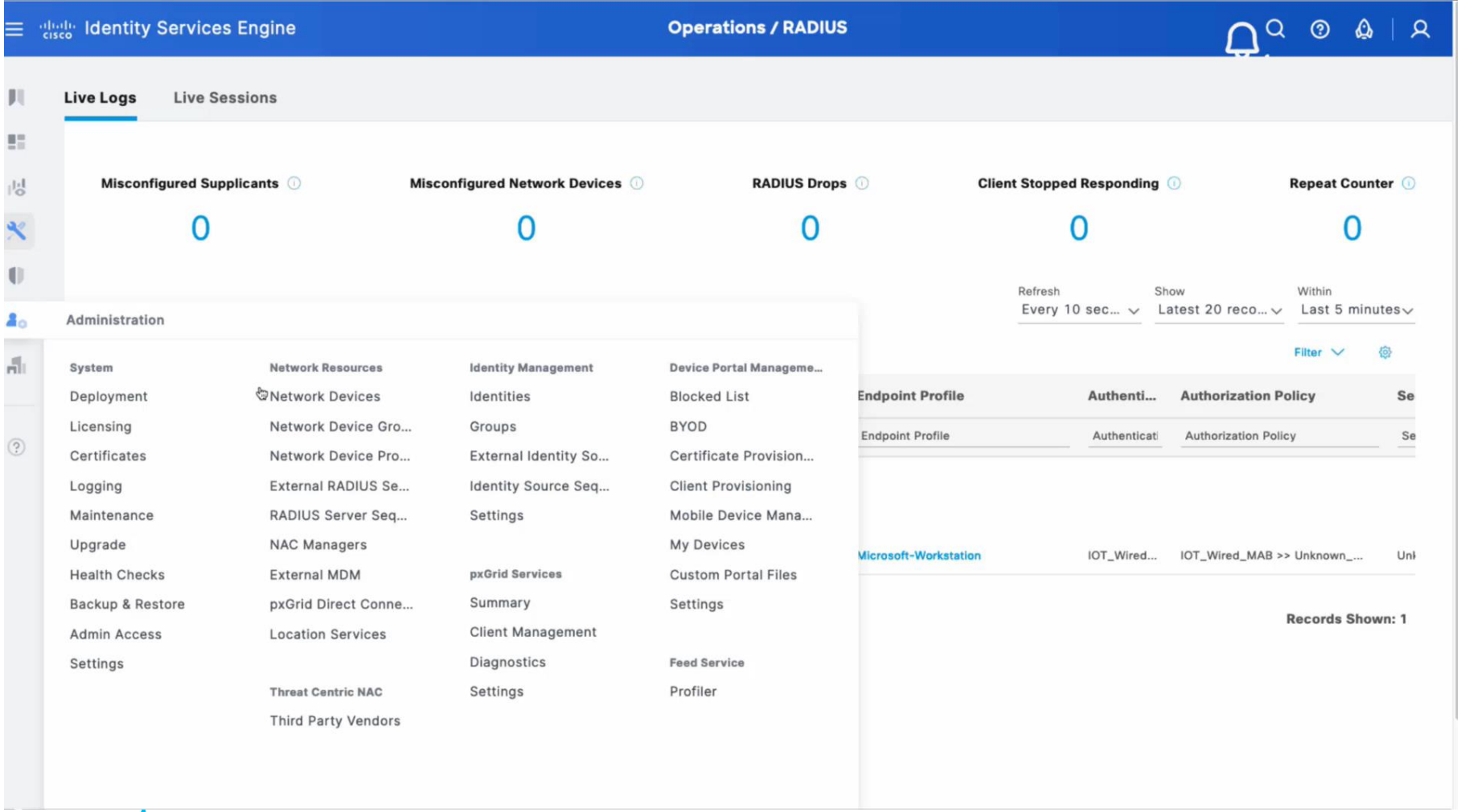
Attribute Name	Type
Created	Date
Expires	Date
Owner	String
Department	String
iPSK	String

Cisco ISE pxGrid Direct for CMDBs

ISE 3.2




```
{
  "result": [
    {
      "sys_import_state_comment": "",
      "template_import_log": "",
      "sys_updated_on": "2022-05-17 10:53:53",
      "sys_class_name": "EDDA_Demo",
      "sys_target_sys_id": "",
      "sys_id": "00021059db6b01101f0f174b13961900",
      "sys_updated_by": "aacook",
      "sys_created_on": "2022-05-17 10:53:53",
      "sys_import_set": "ISET0011307",
      "sys_transform_map": "",
      "sys_created_by": "aacook",
      "sys_import_row": "34,285",
      "u_account_name": "Holly.Allen@example.org",
      "u_macaddress": "05:0e:33:f3:2b:03",
      "sys_row_error": "",
      "group_tag": "cts:security-group-tag=2774-000",
      "sys_target_table": "",
      "sys_mod_count": "0",
      "u_hostname": "black.williams.com",
      "import_set_run": "",
      "sys_tags": "",
      "u_community_group": "Administration",
      "sys_import_state": "Pending",
      "u_config_item": "SNtoDataMartHolly.Allen",
      "u_sync": "",
      "u_ci_status": "Operational",
      "u_host_name": "black.williams.com"
    },{ … }
  ]
}
```



Agenda

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

Make use of Policy Sets

Organizations

Type

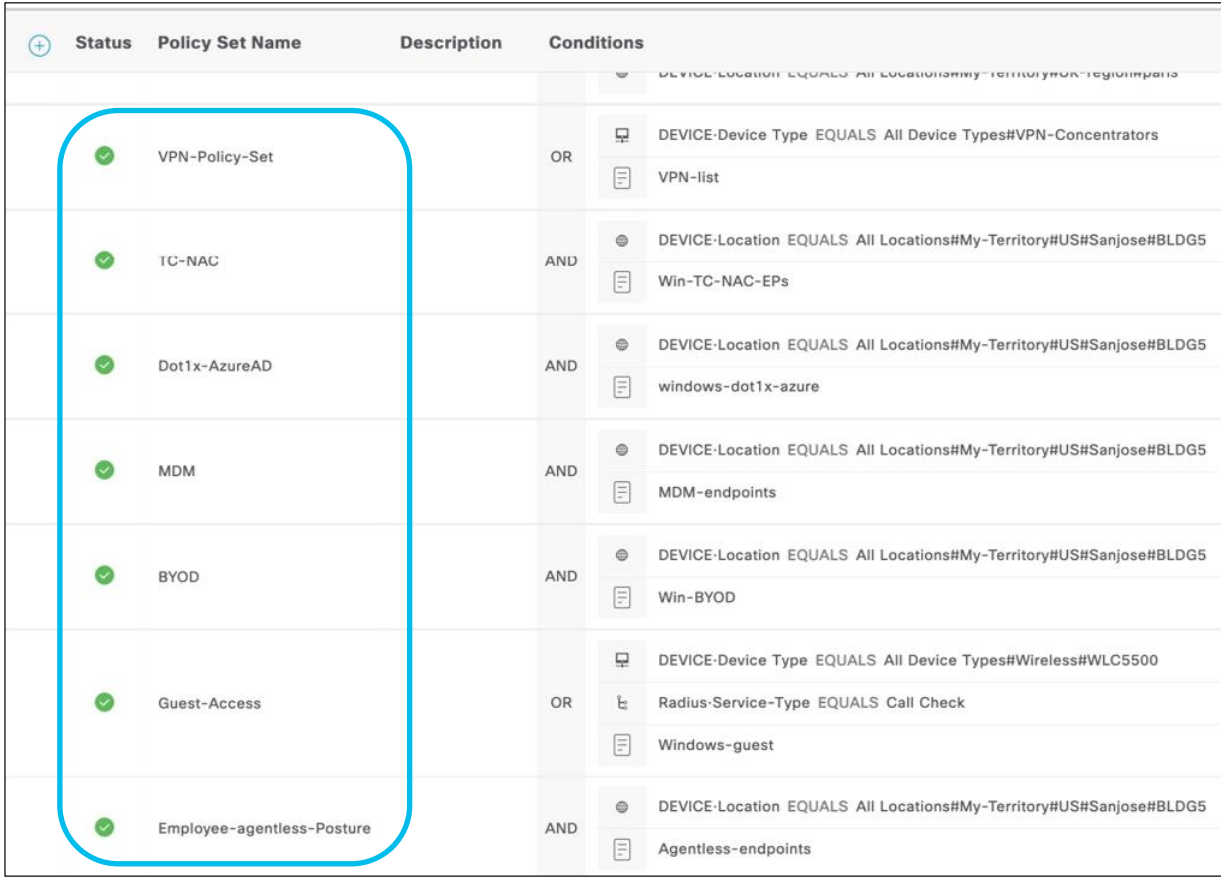
Location

Vendor/Model

Medium

Wireless

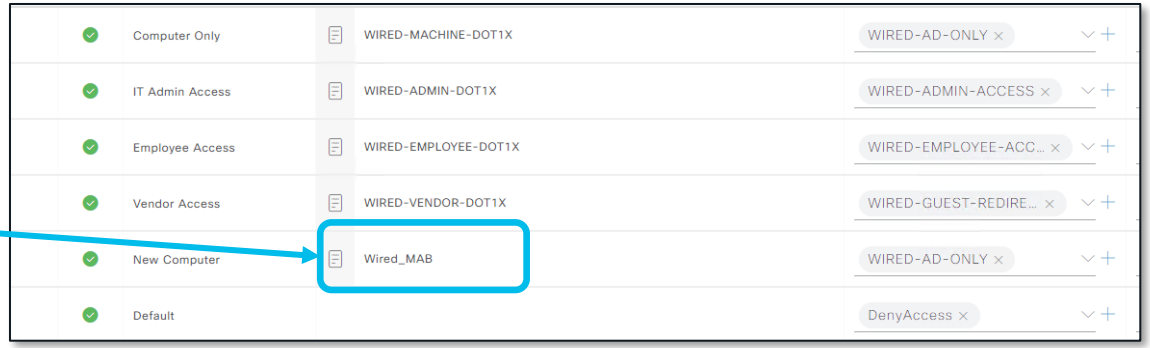
RADIUS



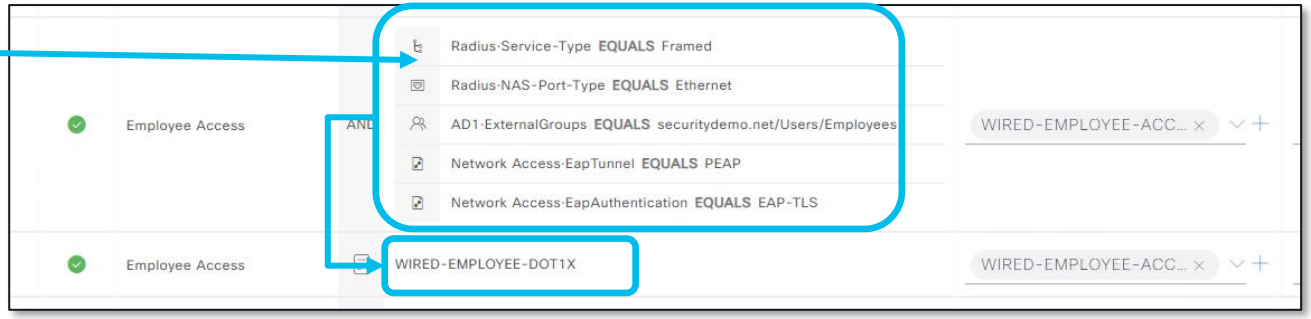
Status	Policy Set Name	Description	Conditions	
	VPN-Policy-Set		OR	DEVICE·Device Type EQUALS All Device Types#VPN-Concentrators VPN-list
	TC-NAC		AND	DEVICE·Location EQUALS All Locations#My-Territory#US#Sanjose#BLDG5 Win-TC-NAC-EPs
	Dot1x-AzureAD		AND	DEVICE·Location EQUALS All Locations#My-Territory#US#Sanjose#BLDG5 windows-dot1x-azure
	MDM		AND	DEVICE·Location EQUALS All Locations#My-Territory#US#Sanjose#BLDG5 MDM-endpoints
	BYOD		AND	DEVICE·Location EQUALS All Locations#My-Territory#US#Sanjose#BLDG5 Win-BYOD
	Guest-Access		OR	DEVICE·Device Type EQUALS All Device Types#Wireless#WLC5500 Radius·Service-Type EQUALS Call Check Windows-guest
	Employee-agentless-Posture		AND	DEVICE·Location EQUALS All Locations#My-Territory#US#Sanjose#BLDG5 Agentless-endpoints

Conditions simplification

Pre-sets Dictionary Condition are easy to read and intuitive



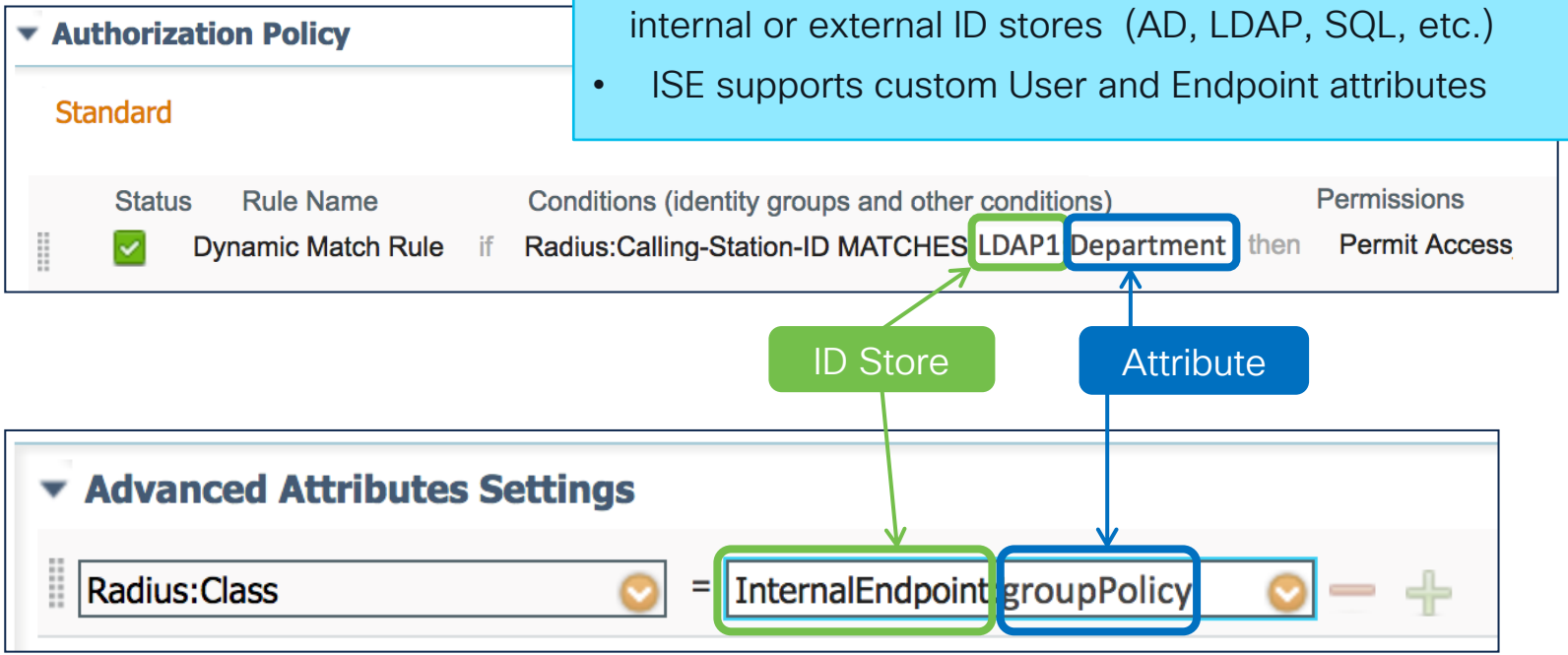
Custom created Conditions often are not as intuitive



Use Compound Conditions and for custom ones

Dynamic Variable Substitution

- Match conditions to unique values stored per- User/Endpoint in internal or external ID stores (AD, LDAP, SQL, etc.)
- ISE supports custom User and Endpoint attributes



Speed Test

Is the image matching the condition set?

- Total stars = 10
- Total Green stars = 4
- Total red stars = 2
- Outer shape = Red triangle

Auth Policy Optimization

Policy Logic:
- First Match, Top Down
- Skip Rule on first negative condition match

Employee

AND

AND

OR

AD1·ExternalGroups **EQUALS** cts.local/Users/employees

AD1·ExternalGroups **EQUALS** cts.local/Users/employees-contractors

1. AD Groups

AD1·msNPAllowDialin **EQUALS** true

2. AD Attributes

OR

MDM·DeviceRegisterStatus **EQUALS** Registered

3. MDM

CERTIFICATE·Subject - Organization Unit **CONTAINS** MyOrganization

4. Certificate

IdentityGroup·Name **EQUALS** Endpoint Identity Groups:RegisteredDevices

5. ID Group

MyCorpSQL·Asset Type **EQUALS** Corporate

6. SQL Attributes

AND

Network Access·EapAuthentication **EQUALS** EAP-TLS

7. Auth Method

OR

EndPoints·EndPointPolicy **STARTS_WITH** Windows7

EndPoints·EndPointPolicy **STARTS_WITH** Windows10

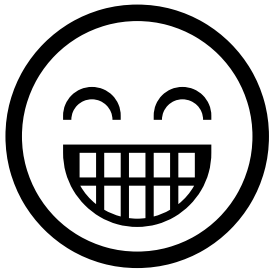
8. Endpoint Profile

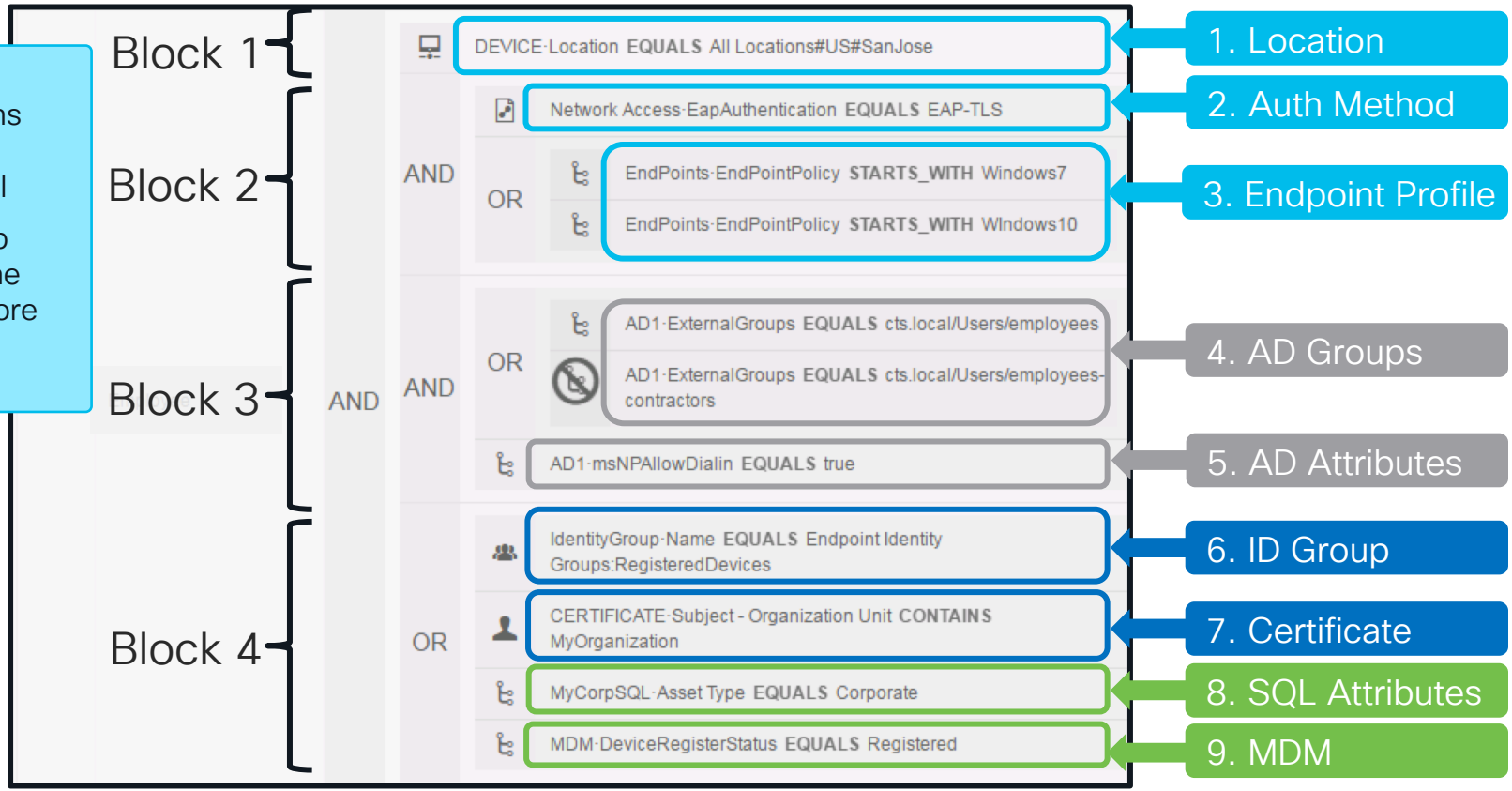
DEVICE·Location **EQUALS** All Locations#US#SanJose

9. Location

Auth Policy Optimization

- Local conditions should be put before external
- External lookup should go at the end as take more time





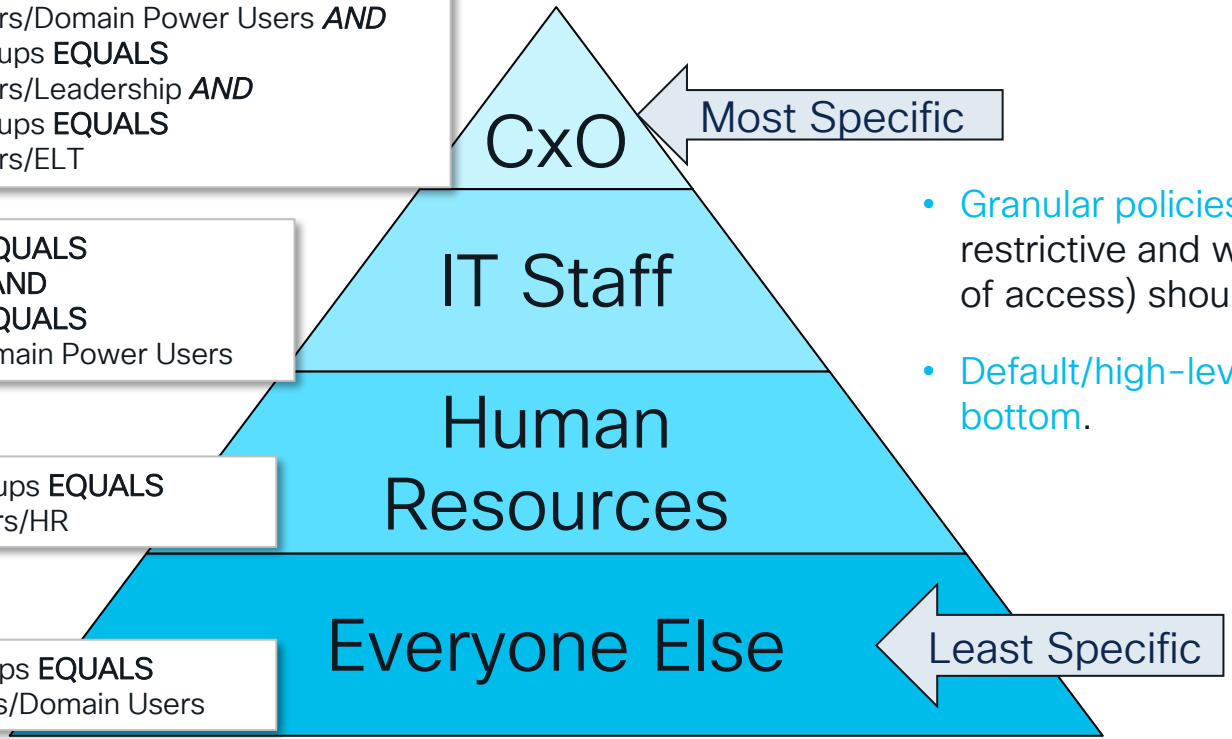
AD Policy rule optimization example

AD1·ExternalGroups **EQUALS** domain.com/users/IT ***AND*** AD1·ExternalGroups **EQUALS** domain.com/users/Domain Power Users ***AND*** AD1·ExternalGroups **EQUALS** domain.com/users/Leadership ***AND*** AD1·ExternalGroups **EQUALS** domain.com/users/ELT

AD1·ExternalGroups **EQUALS** domain.com/users/IT **AND** AD1·ExternalGroups **EQUALS** domain.com/users/Domain Power Users

AD1·ExternalGroups **EQUALS** domain.com/users/HR

AD1·ExternalGroups **EQUALS** domain.com/users/Domain Users



- Granular policies (most restrictive and with higher level of access) should go first.
- Default/high-level policies go bottom.

Agenda

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

Who Needs an ISE Lab? You do!

With ever Standalone installation :

- 90-day Evaluation license
- For 100 endpoints
- All Cisco ISE features
- 1 TACACS+ license

You can set up a limited deployment and test all the required features in your environment

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

Python

Ansible

VSCode

github.com/CiscoISE

#YAML

```
network_device:
- name: lab-mr46-1
  description: ''
  profileName: Cisco
  authenticationSettings:
    dtlsRequired: false
    enableKeyWrap: false
    enableMultiSecret: 'false'
    keyEncryptionKey: ''
    keyInputFormat: ASCII
```

ISE Deployment and Operational Lifecycle

Provision

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

Deploy

Enable APIs
Repositories
Roles
Services
Certificates
Licensing
...

Configure

Identity Stores
Network Devices
Policy Sets
Endpoints
Portals
...

Operate

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

Extend

Terminate
...

ISE Eternal Evaluation

https://github.com/1homas/ISE_Ansible_Sandbox

Cisco ISE playbooks and roles for ISE automated deployment and configuration in labs and demos, beginning with the ISE Eternal Evaluation (ISEEE)

README.md

Cisco Identity Services Engine (ISE) playbooks and roles for ISE automated deployment and configuration in labs and demos. Also featured in the Cisco ISE Webinar, **ISE Eternal Evaluation for Your Lab**.

Quick Start

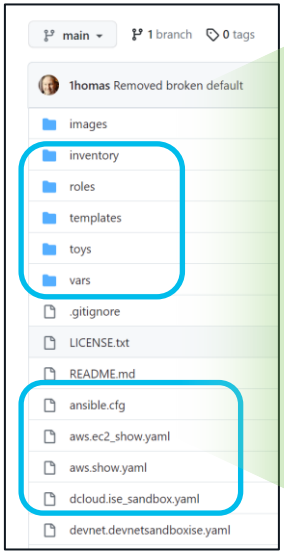
1. Clone this repository:

```
git clone https://github.com/1homas/ISE_Ansible_Sandbox.git
```

2. Install a local Python virtual environment with Ansible and other required packages:

```
python_environment_install.sh
```

> ⚠️ Installing Ansible using Linux packages (`sudo apt install ansible`) may info in a much older version of Ansible being installed. 💡 Installing Ansible with Python packages will get you the latest.
> 💡 If you have any problems installing Python or Ansible, see Installing Ansible.



iseee.yaml

- iseee.**ssh**.yaml
- iseee.**provision**.yaml
- iseee.**facts**.yaml
- iseee.**patch**.yaml
- iseee.**deploy**.yaml
- iseee.**certificates**.yaml
- iseee.**licensing**.yaml
- iseee.**configure**.yaml
- iseee.**backup**.yaml
- iseee.**restore**.yaml
- iseee.**extend**.yaml
- iseee.**password_reset**.yaml
- iseee.**destroy**.yaml

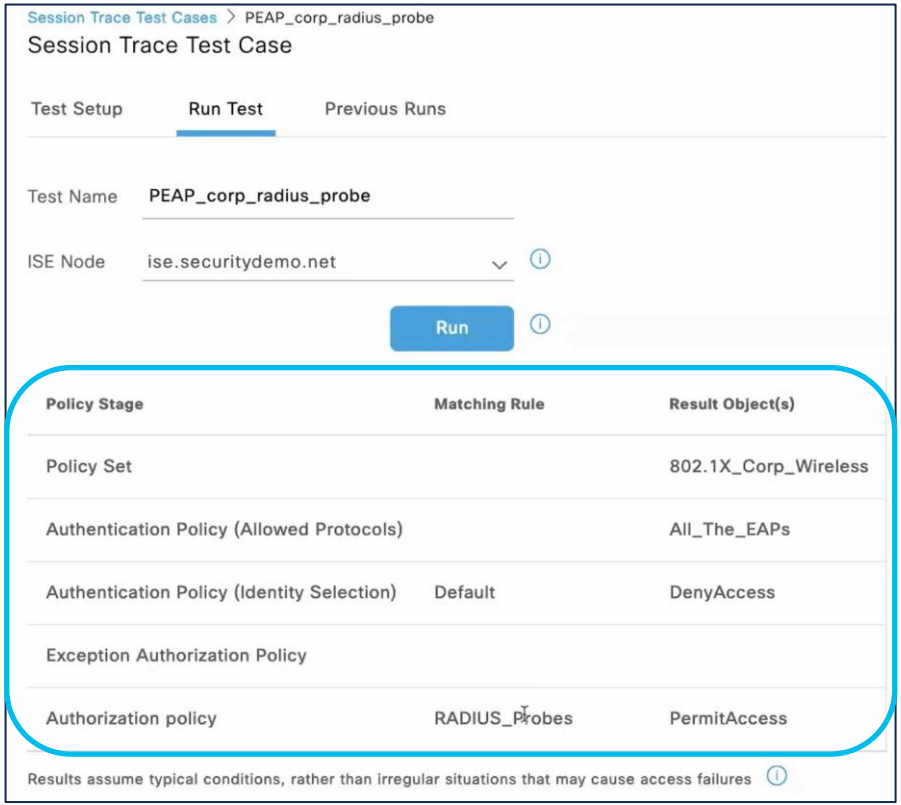
How to test your lab?

Using real devices (the one you will use in production) is always best (expecially if you test use cases like posture/profiling)

BUT...

Sometimes simulation tools are useful (policy match or simulating large number of devices).

Try the Session Trace Test tool in ISE

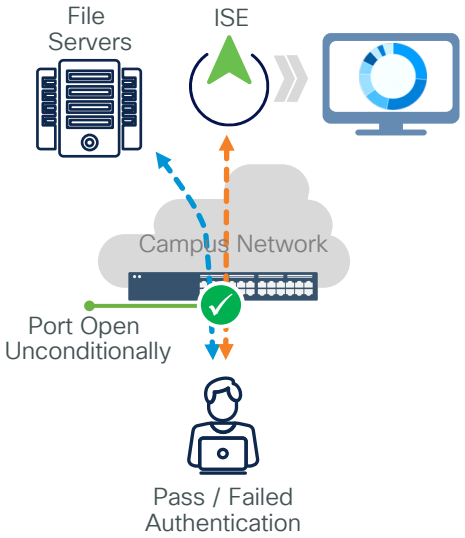


Agenda

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

Deployment Modes

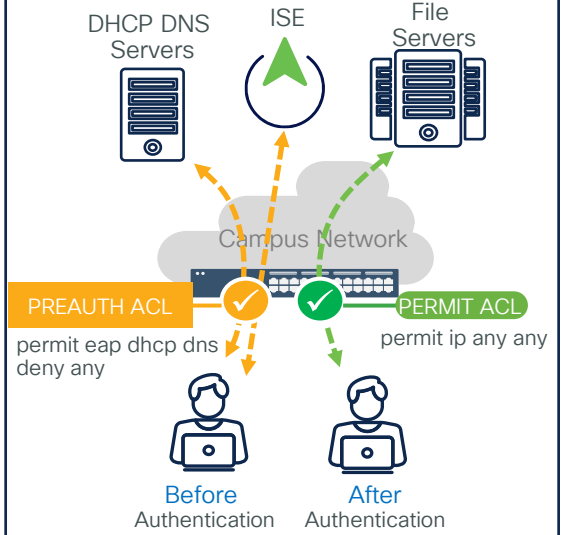
Monitor Mode (Visibility)




```
authentication open
```

No impact to existing network

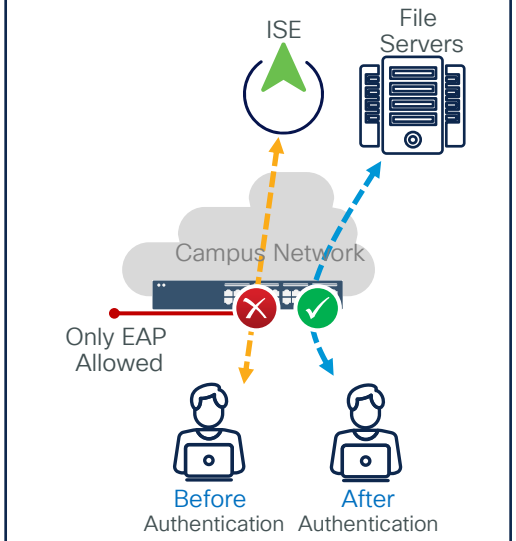
Low-Impact Mode (Visibility and Control)




```
ip access-group PRE-AUTH in
authentication open
```

Begin to control and differentiate access

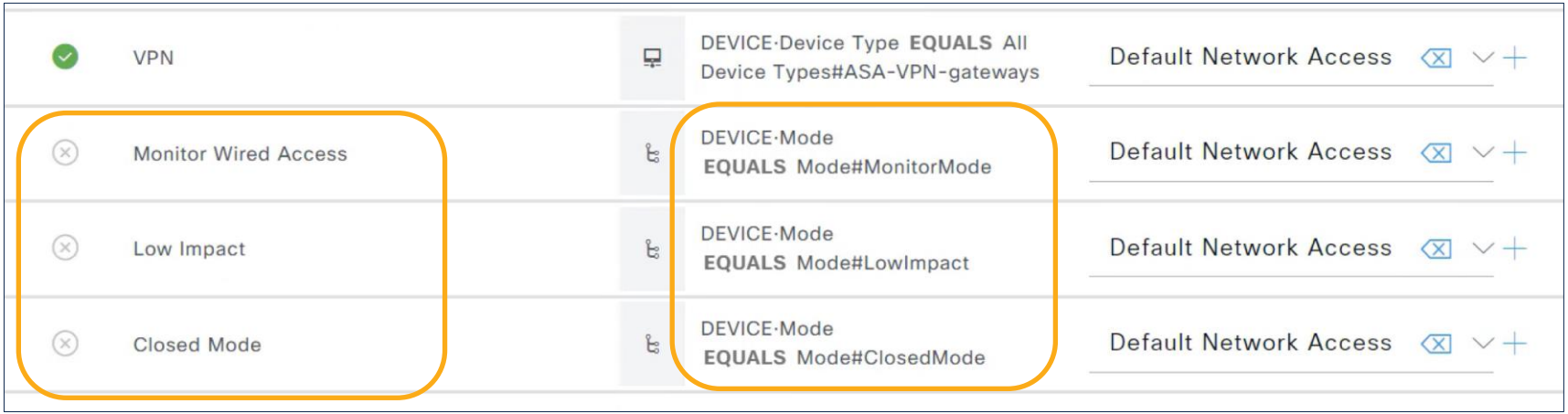
Closed Mode (Visibility and Control)



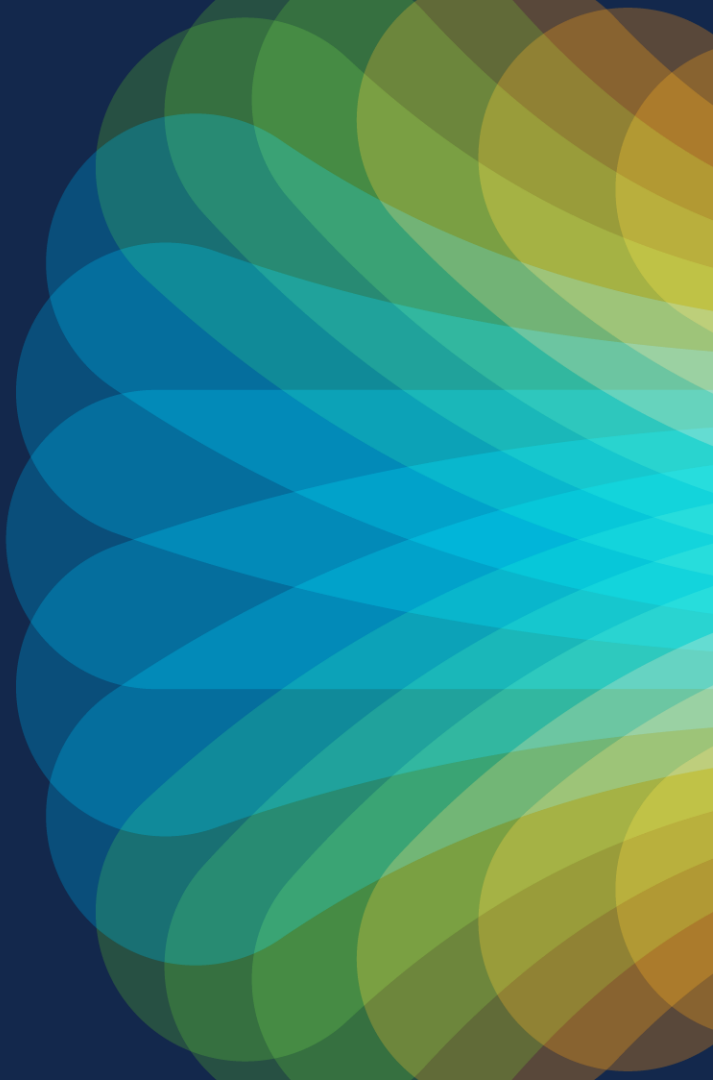
- Not everyone needs Closed Mode
- No access at all before authentication

Utilizing Policy Sets with Modes

- When deploying leverage Network Device Groups
- Move devices in and out while the deployment progresses



Day 2 Operations



User involvement

User Communication before and after ISE rollout

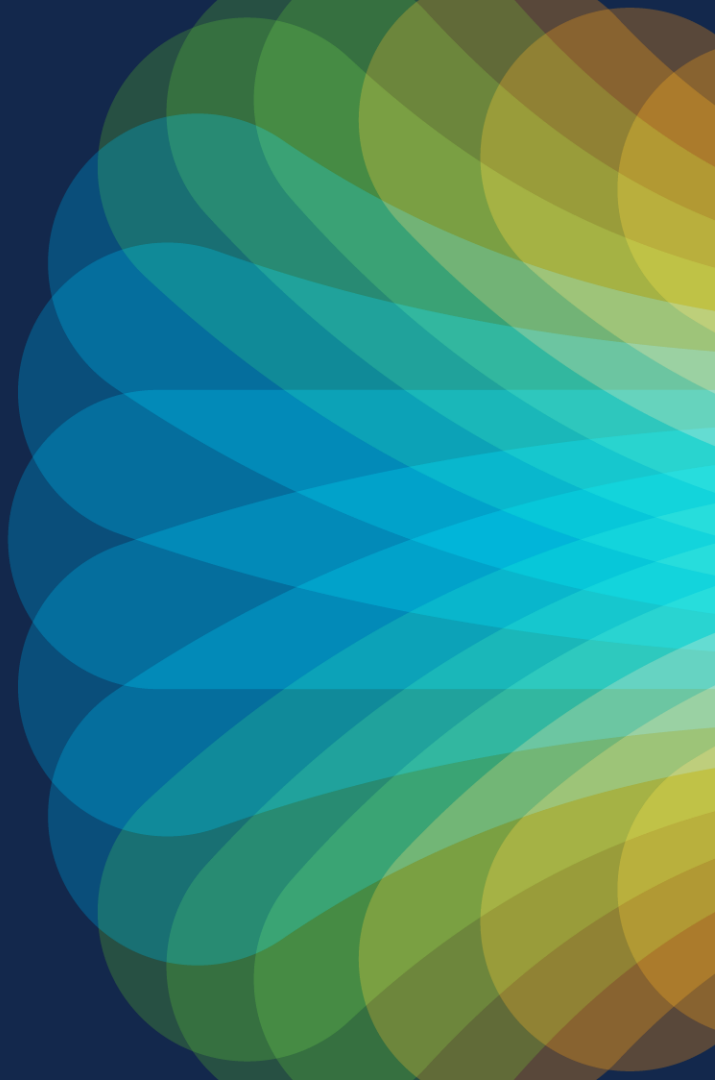
Supporting ISE After Deployment

- Train Your Support with A Playbook for common issues

- Document as much as possible!
  - ✓ Policy Configuration
  - ✓ Supplicant Configuration
  - ✓ Network Access Devices

- Many document templates available on ISE Communities

Wrap up



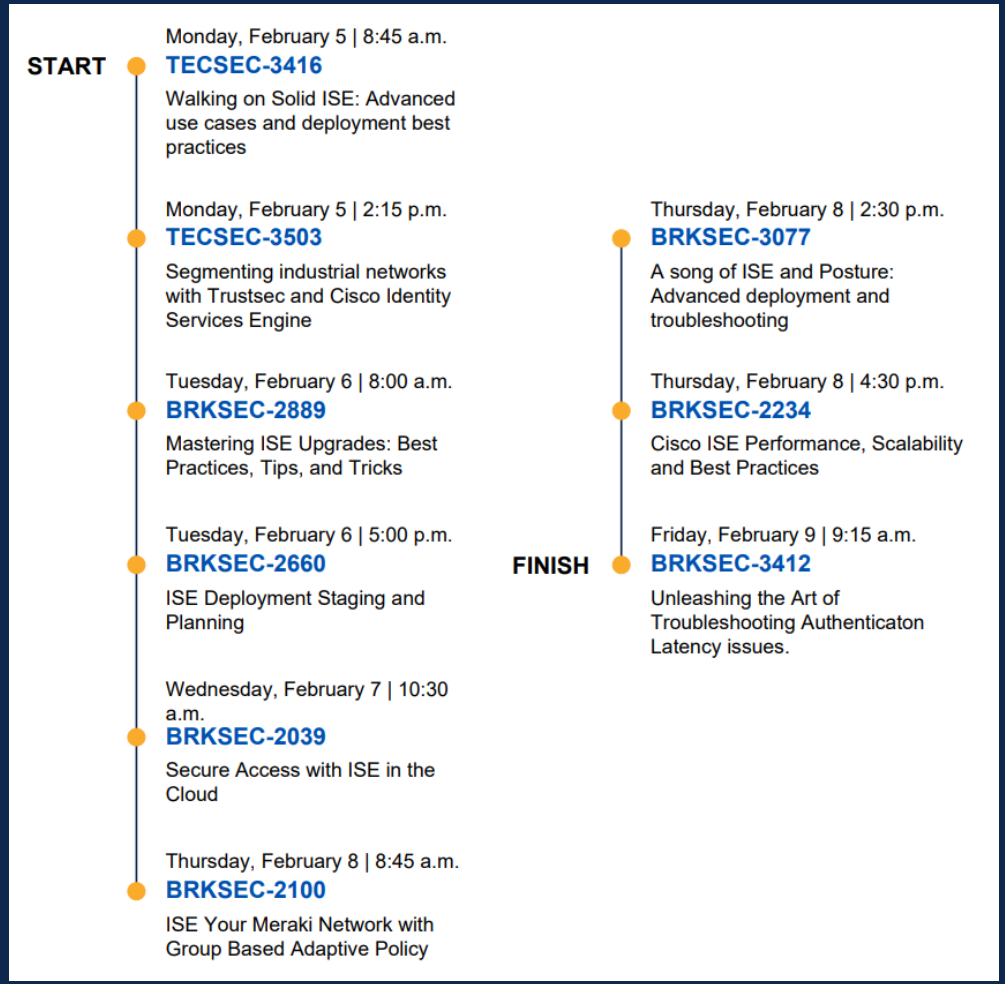
Deploying any network access control solution is crucial

but it isn't easy....

Proper planning is essential to any successful development.

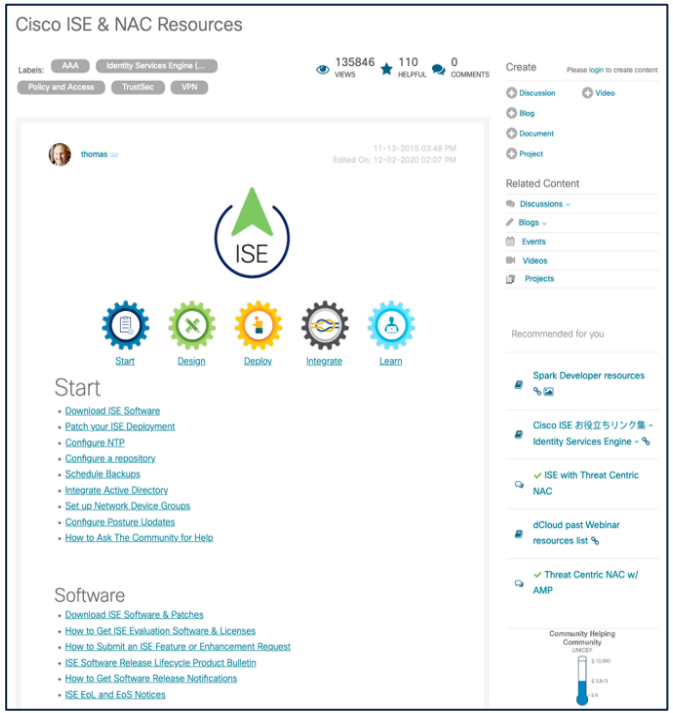
ISE learning map

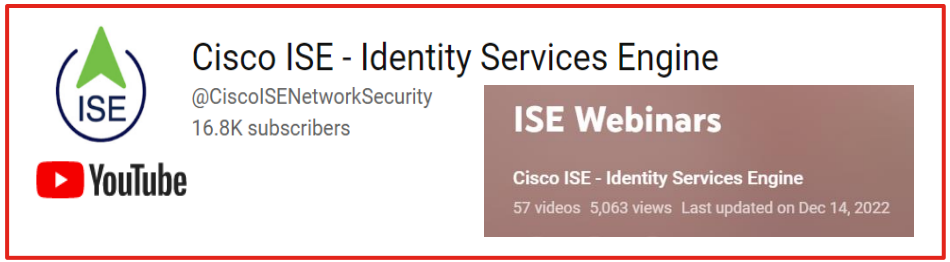
Learn how Cisco ISE will help you implement Network access Control in your campus.
Sessions will cover how to plan and deploy, how to leverage the new cloud capabilities, best practices and other topics



Cisco ISE Resources

- Consolidated list of resources
  cs.co/ise-resources
- Community Q&A
  cs.co/ise-community
- Recorded webinars and other videos
  cs.co/ise-videos
- Integration Guides
  cs.co/ise-guides
- Licensing Guide
  cs.co/ise-licensing



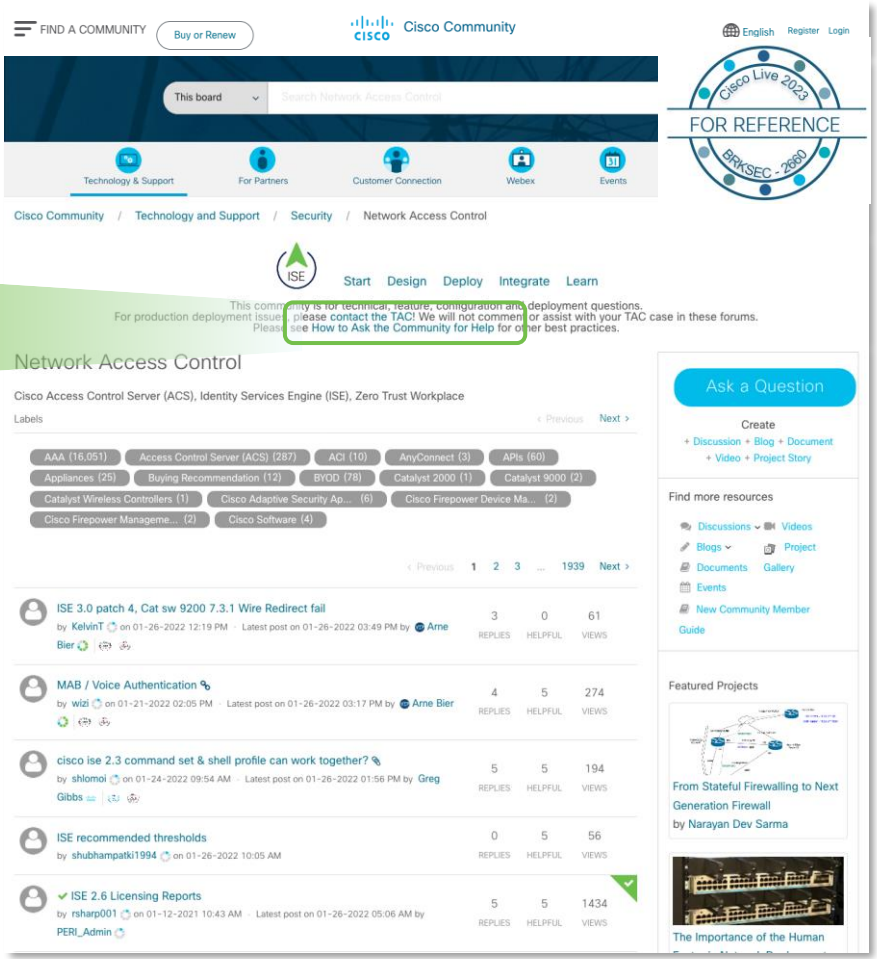


Ask The Community

cs.co/ise-community

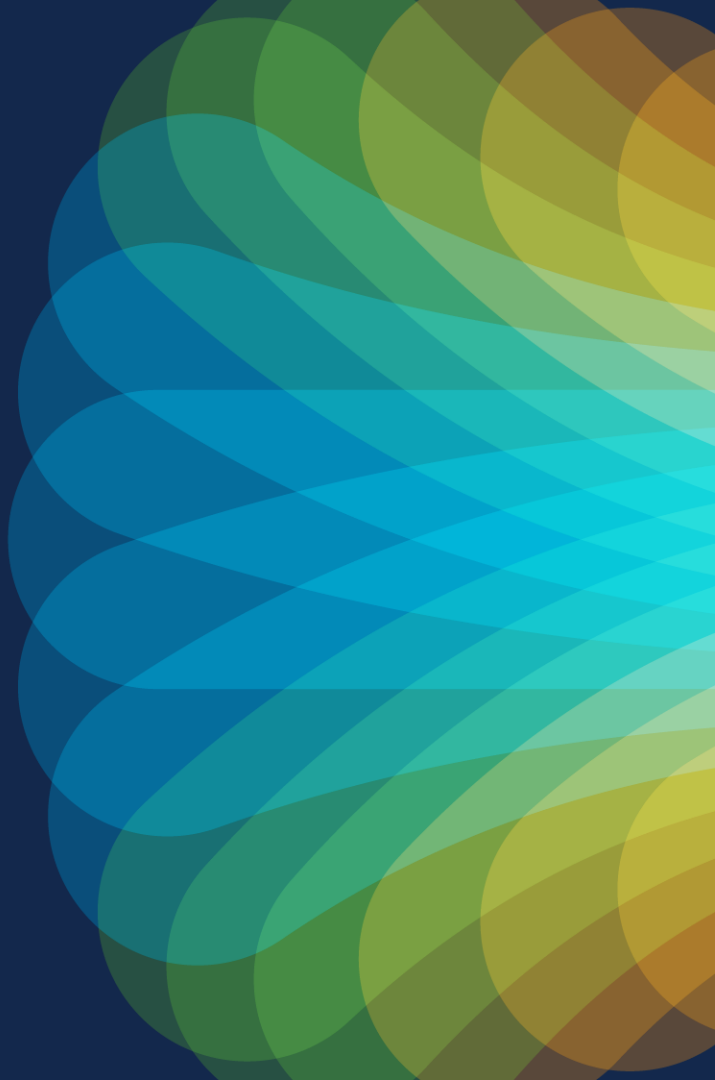
How to Ask the Community for Help

- 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)
- Pictures and Video!



The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go