The bridge to possible

ISE Deployment, Staging and Planning

Francesca Martucci, Technical Solutions Architect – Cybersecurity EMEA

cisco Live!

BRKSEC-2660

ISE Planning, Deployment and Staging

Do I really need to plan?

Need to work with other teams in the organization:

- Virtualized environment
- Active Directory
- PKI
- Endpoint team
- Desktop support
- And possibly other teams

Deploying any network access control solution is crucial

but it isn't easy....

Planning is essential to any successful development.

Who am I?

- Technical Solutions Architect
  Cyber Security EMEA
- In Cisco since 23 years...

  ... And 3 countries

Main interest on

- Policy and Access
- Segmentation
- Industrial Security

Agenda

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

What we are not covering

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

This presentation has many links at the end, to resources helping with all of them

Cisco Webex App

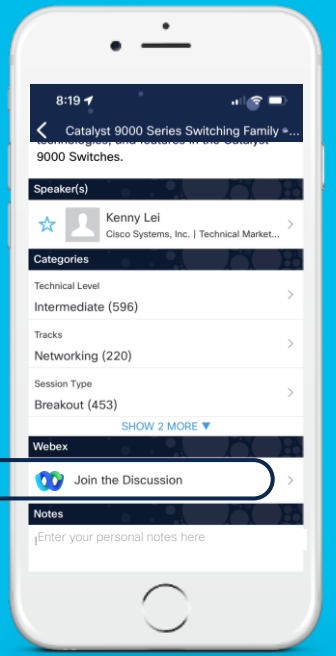
Questions?

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 until February 24, 2023.



- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases

Cisco ISE High Level Design (HLD)

- 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

cs.co/ise-hld

Use cases

What is the business trying to accomplish with ISE?
Which ones could be considered for the future?

Asset Visibility	Cisco ISE can reach deep into the network to deliver superior visibility into who and what is accessing resources.
Access Control	Consistent access control across wired, wireless and VPN Networks. 802.1X, MAC, Web Authentication and Easy connect for admission control.
Guest Access	Fully customizable branded mobile and desktop guest portals, with dynamic visual workflows to easily manage guest user experience.
BYOD Access	Simplified BYOD management with built-in CA and 3rd party MDM integration for on boarding and self-service of personal mobile devices
Segmentation	Topology independent Software-defined segmentation policy to contain network threats.
Context Exchange	Context sharing with partner eco-system to improve their overall efficacy and accelerate time to containment of network threats.
Threat Control	Protection against threats across the attack continuum, before, during and after an attack. Reduce time-to-detection from days to hours.
Device Admin	Cisco ISE supports device administration using the TACACS+ security protocol to control and audit the configuration of network devices

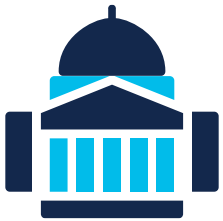
Defining your Security Policy

What is an IT security policy?

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

Everyone Has Different Needs

Government



Financials

Healthcare

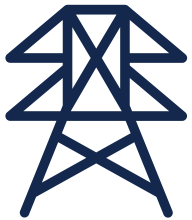
Retail

Education

Transportation

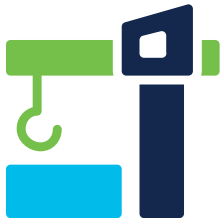
Services

Utilities



Technology

Manufacturing



Example of your ISE policy planning

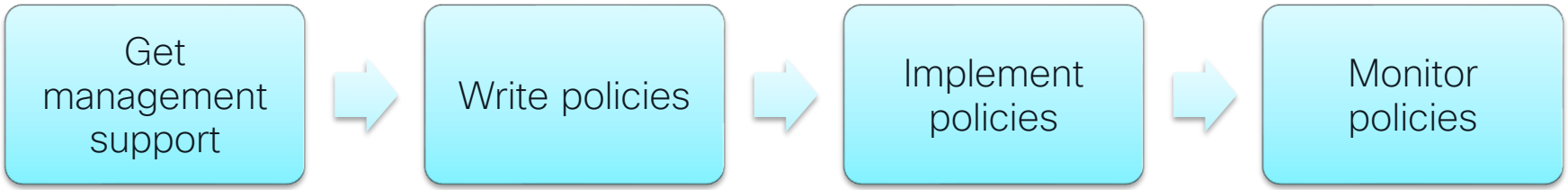
Endpoint Type	Authentication	Identity Store	Network Access	Enforcement	Staging / Provisioning
Corp PC	802.1X – Cert	ISE Cert Store	Full Access	VLAN CORP	Physical Staging Port
Guests	WebAuth	ISE Guest DB	Internet-Only	VLAN Guest	Manual Connect Sponsored account
Access Point	802.1X – User/Pass	ISE User 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 corp PC certificate is expired?

IT Security Policy important considerations

- Security Policy should not be written by “feature”
- Need to know your Security Policy prior to deploy
- Get management buy-in
- 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

ISE Deployment Planning

cs.co/ise-hld

ISE High Level Design (HLD)

- Business Objectives
- Environment
  - Physical Network Topology
  - Identity Sources
  - User Groups
  - Network Devices
  - Endpoints
  - ISE Cube
- Device Administration (TACACS+)
- Visibility
- Secure Access : Wireless / Wired / VPN
- Guest : HotSpot / Registered / Sponsored / API
- BYOD
- Integration : Context Sharing / Threat Mitigation / APIs
- Compliance
- Segmentation
- Containment
- Operations & Management
- Scale & High Availability
- Policy Details
- Resources

cs.co/ise-resources#Planning

ISE Planning & Pre-Deployment Checklists

- Planning Checklists
  - Business Objectives
  - Organizational
  - Security Policy Creation and Maintenance
  - Scale
  - Public Key Infrastructure (PKI)
  - Directory Services
  - Network Access Devices (NADs)
  - Managed Endpoints
  - Assets
  - Cisco Identity Services Engine (ISE)
  - Guest Services
  - Monitoring, Reporting, and Troubleshooting
  - Communications
  - Support Desk
- Deployment Checklists
  - Network Services
  - Digital Certificates
  - Network Devices
  - Security Policy
  - Enforcement States
  - Endpoints
  - Test Scenarios

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases

ISE Personas

Policy Administration Node (PAN)

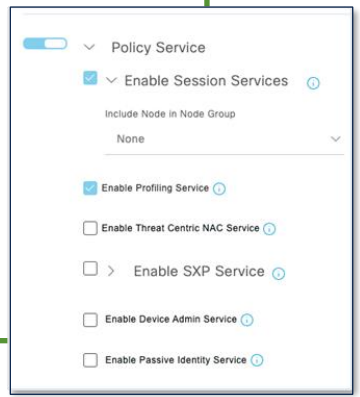
- Administrative GUI
- Policy configuration
- Policy replication
- Centralized Guest database
- Centralized BYOD database
- Configuration REST APIs

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)

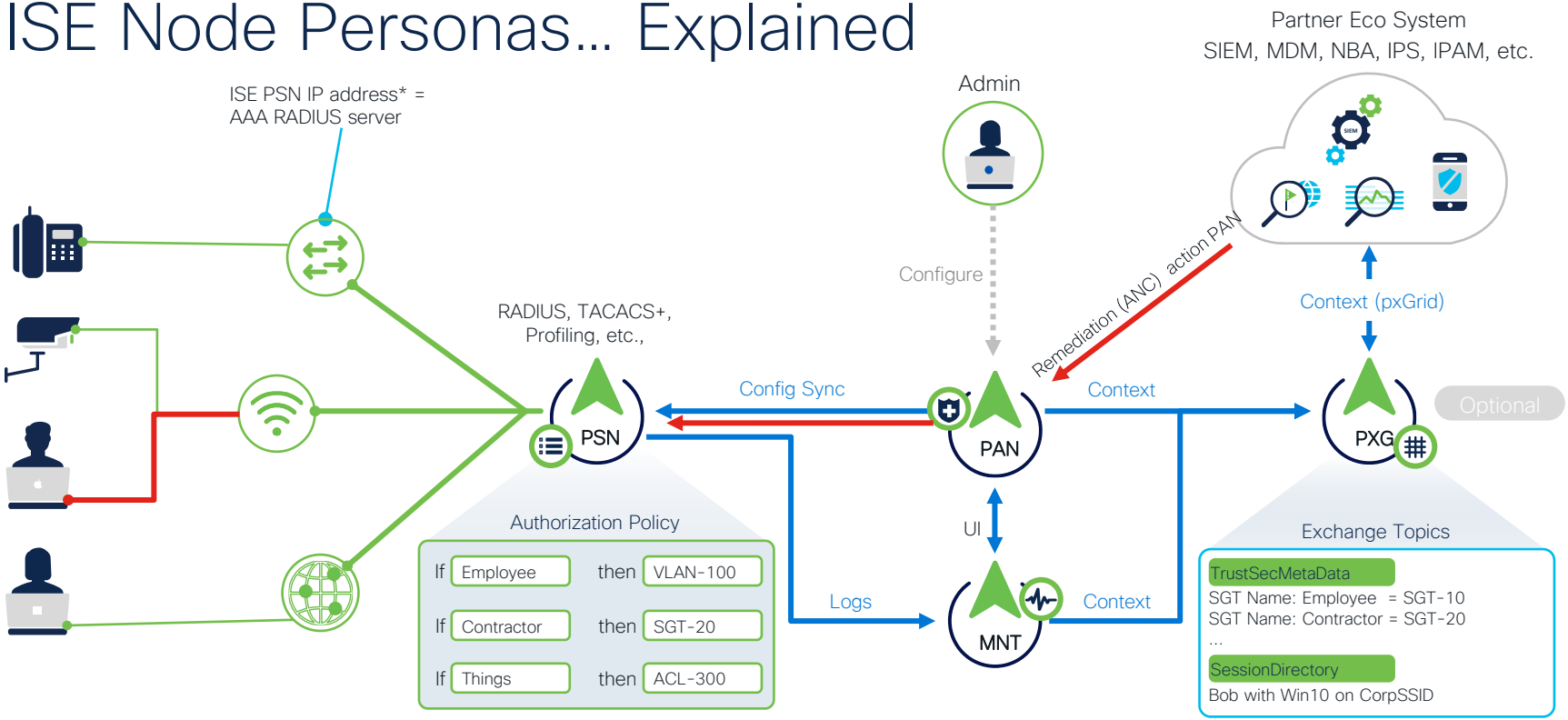
- TACACS requests
- RADIUS requests
- Endpoint profiling probes
- Identity store queries
- Hosts Guest/BYOD portals
- MDM/Posture queries
- TC-NAC & SXP services



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

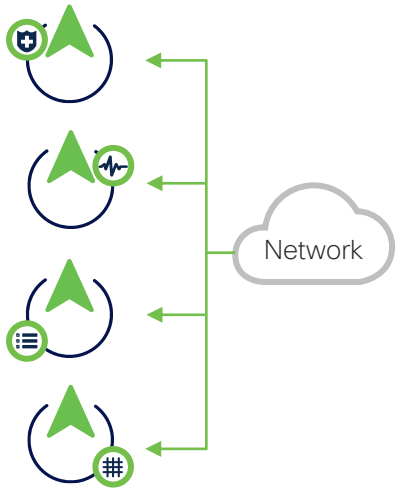
Policy Administration Node (PAN)
- Max 2 in a deployment

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

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

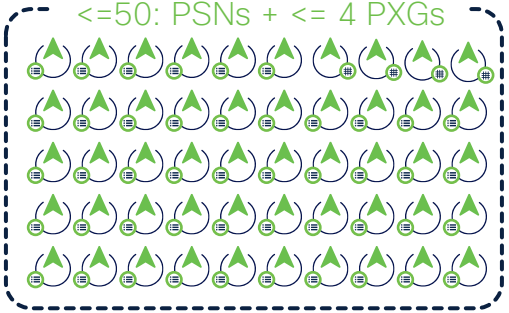
pxGrid Controller
- Max 4 in deployment

Distributed ISE



2.6+

ISE Distributed Deployment Scale

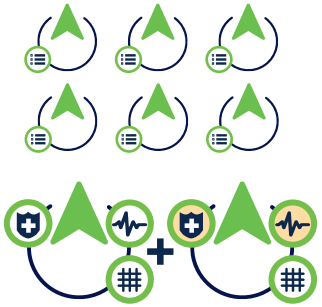


Same for physical and virtual deployments

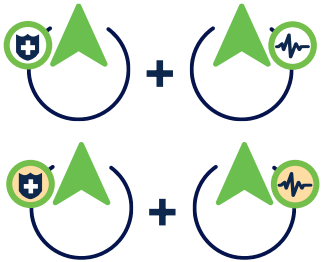
Compatible with load balancers

Standalone
(for Lab and
Evaluation)

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



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



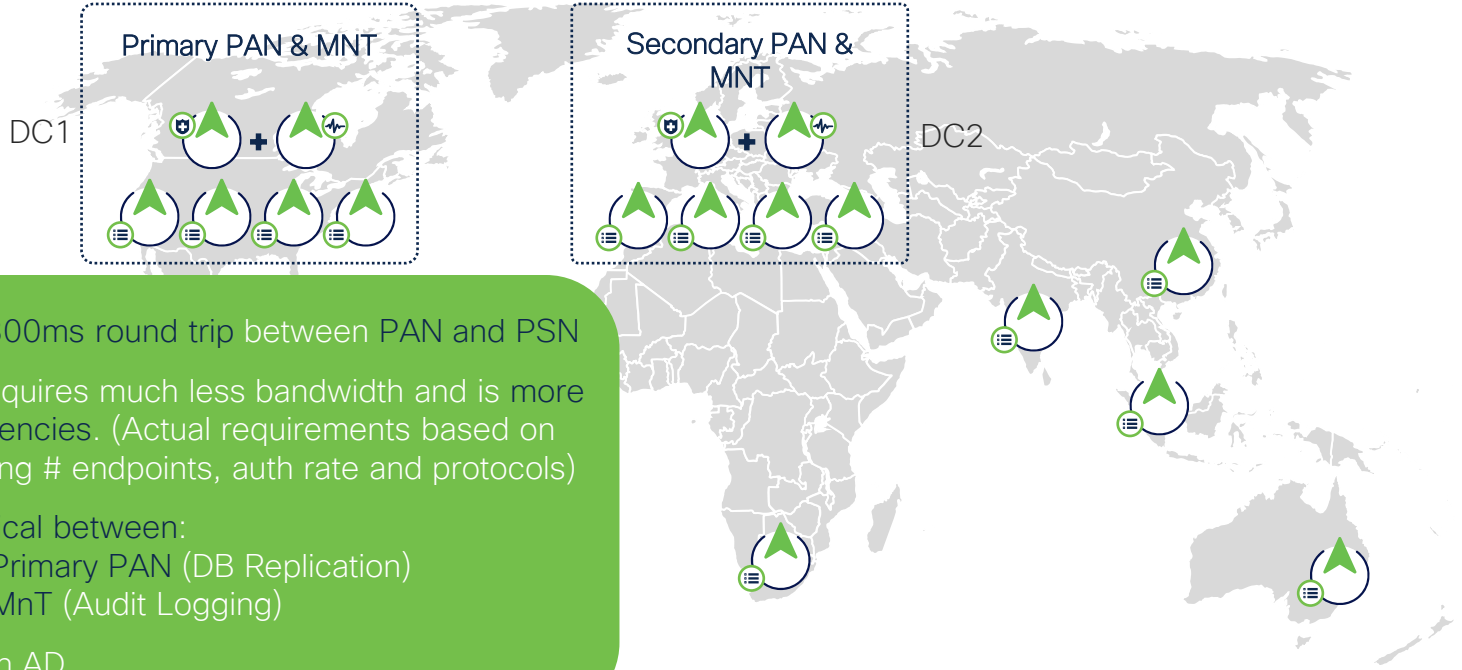
Large Deployment
2 PAN, 2 MNT, <=50: PSNs
+ <= 4 PXGs

100 Endpoints	Up to 20,000 Endpoints	Up to 500,000 Endpoints	3500
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
- RADIUS generally requires much less bandwidth and is more tolerant of higher latencies. (Actual requirements based on many factors including # endpoints, auth rate and protocols)
- Bandwidth most critical between:
  - PSNs and Primary PAN (DB Replication)
  - PSNs and MnT (Audit Logging)
- Co-locate PSNs with AD

Maximum Concurrent Active Endpoints

- 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

SNS-3595

KVM

Microsoft

NUTANIX

vmware

aws

Azure

ORACLE

- Use resource reservations (built into OVAs)
- Do NOT oversubscribe!

SNS-37xx appliances

SNS-3715		Intel 4310 2.1GHz 12 Cores	600GB HDD 800GB SSD 960GB SED [1]	32GB	2 X 1GbE 4 X 10Gb SFP	RAID0	TPM [1]
SNS-3755		Intel 4316 2.3GHz 20 Cores	4X600GB HDD 4X800GB SSD 4X960GB SED [1]	96GB	2 X 1GbE 4 X 10Gb SFP	RAID10	TPM [1]
SNS-3795		Intel 4316 2.3GHz 20 Cores	8X600GB HDD 8X800GB SSD 8X960GB SED [1]	256GB	2 X 1GbE 4 X 10Gb SFP	RAID10	TPM [1]

[1] SED to come later in Spring. TPM Chip available probably next ISE release

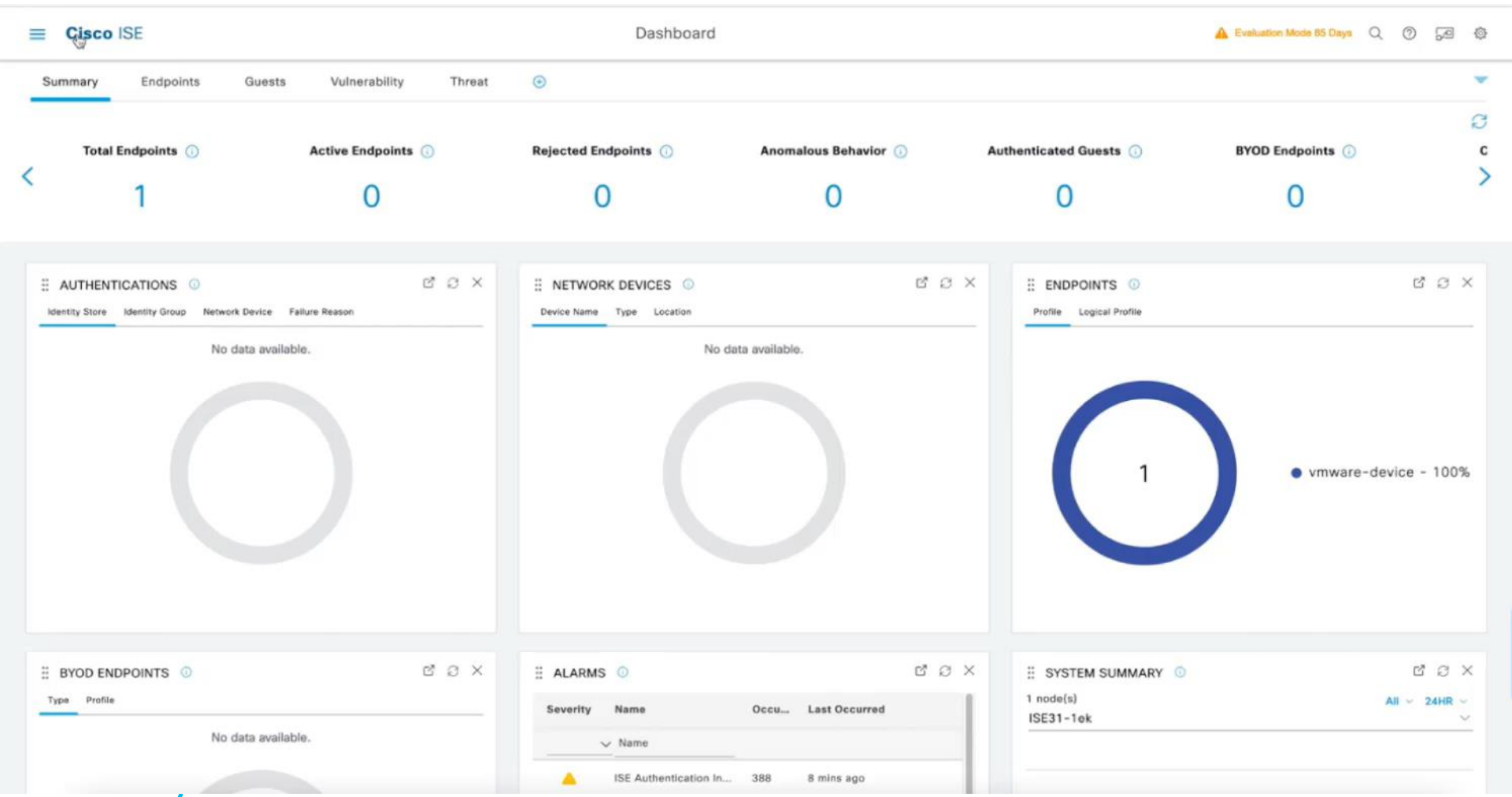
Distributed Scalability Numbers

cs.co/ise-scale

Platform	Concurrent active endpoints supported by a dedicated PSN (Cisco ISE node only has 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 3595	40,000	20.000
SNS 3695	50,000	25.000

Deployment Type	Platform	Max Concurrently Connected Endpoints in ISE Deployment
Standalone (All personas on a single node)	3615 3595 3655 3695	10.000 20.000 25.000 50.000
Small deployment (Basic 2-node)	3615 3595 3655 3695	10.000 20.000 25.000 50.000
Medium deployment (Admin + MnT; PSN dedicated)	3615 3595 3655 3695	10.000 20.000 25.000 50.000
Large deployment (PAN, MnT, PXG, and PSN Nodes)	3595 3655 3695	500.000 500.000 2.000.000

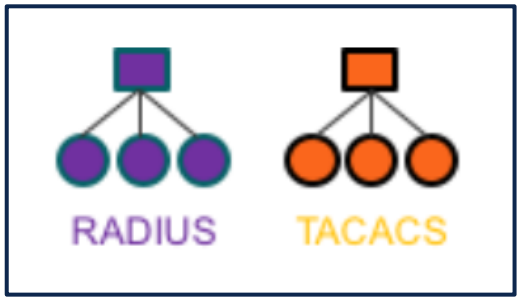
cisco Live!



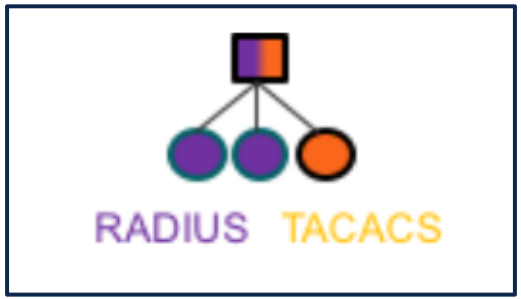
ISE RADIUS vs TACACS+ Deployment Models

Separating RADIUS & TACACS+ ISE Cubes?

There are three different options:



Separate ISE cubes for RADIUS & TACACS+



Mixed ISE cube with separate PSNs for RADIUS and TACACS+

Mixed ISE cube where PSNs are not dedicated to either

When do we separate TACACS+ and RADIUS?

Things to consider

- Device Admin service enabled per PSN
- Sizing is NOT per device count
- Scalability is transactions per second (TPS)

- Authentication? Command authorization?
- Scripts? Network management tools?

- Number of TACACS+ & RADIUS sessions if PSN is shared
- Per-PSN utilization and load

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases

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

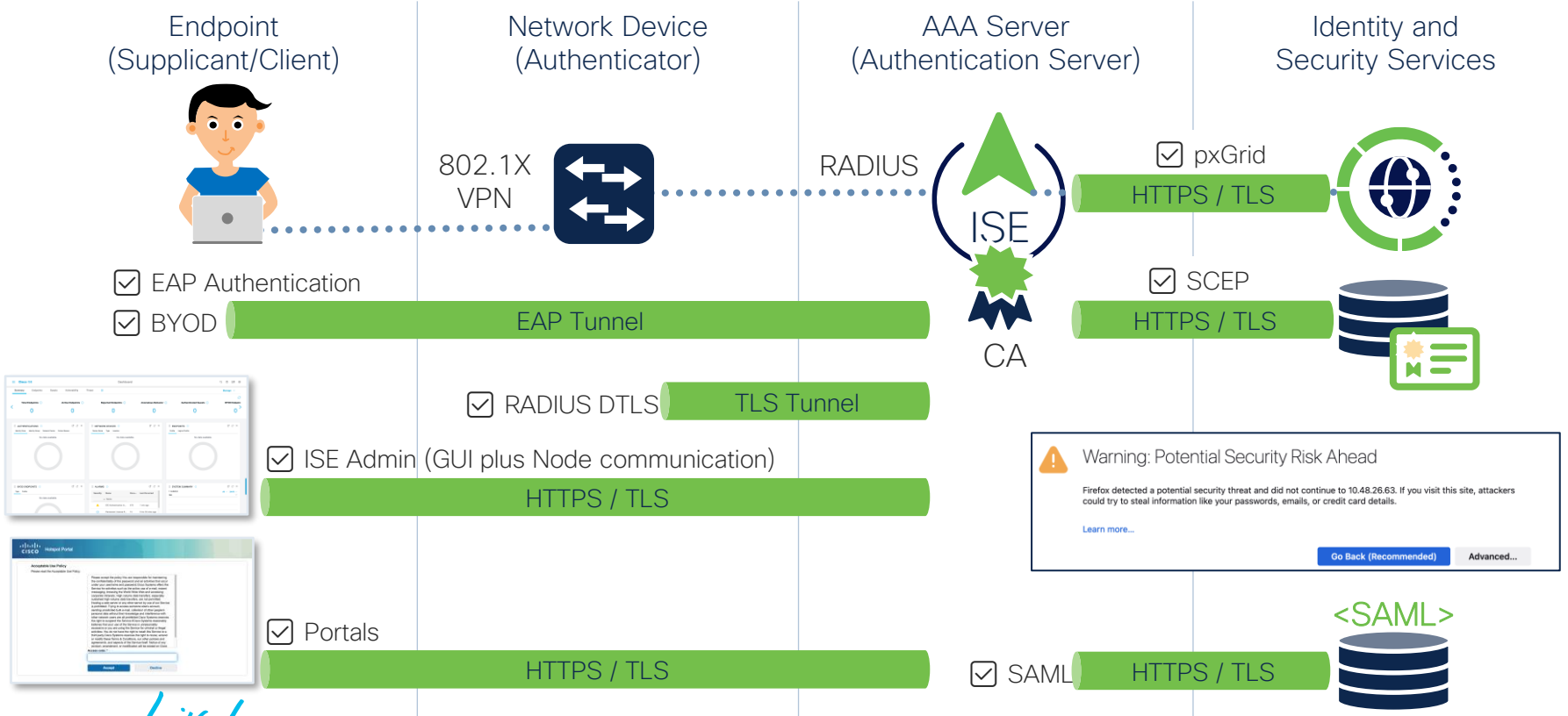
List of CAs

- from which endpoint certs are issued for cert-based authentication
- from which users' certs are issued for admin UI access
- for secure communication with external entities
- for ISE Internal services
- Replicated to all the nodes in deployment

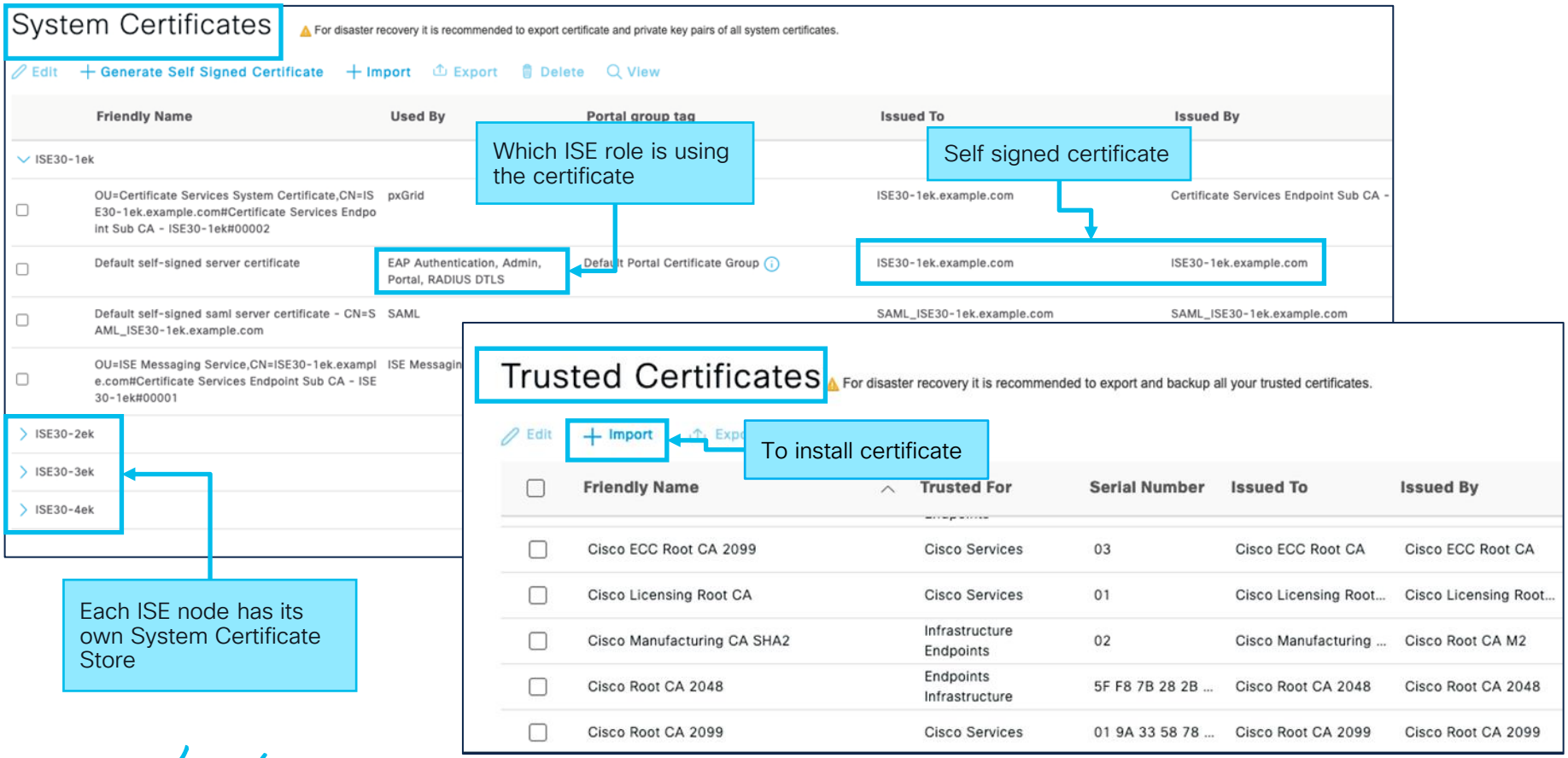
ISE Issued Certificates

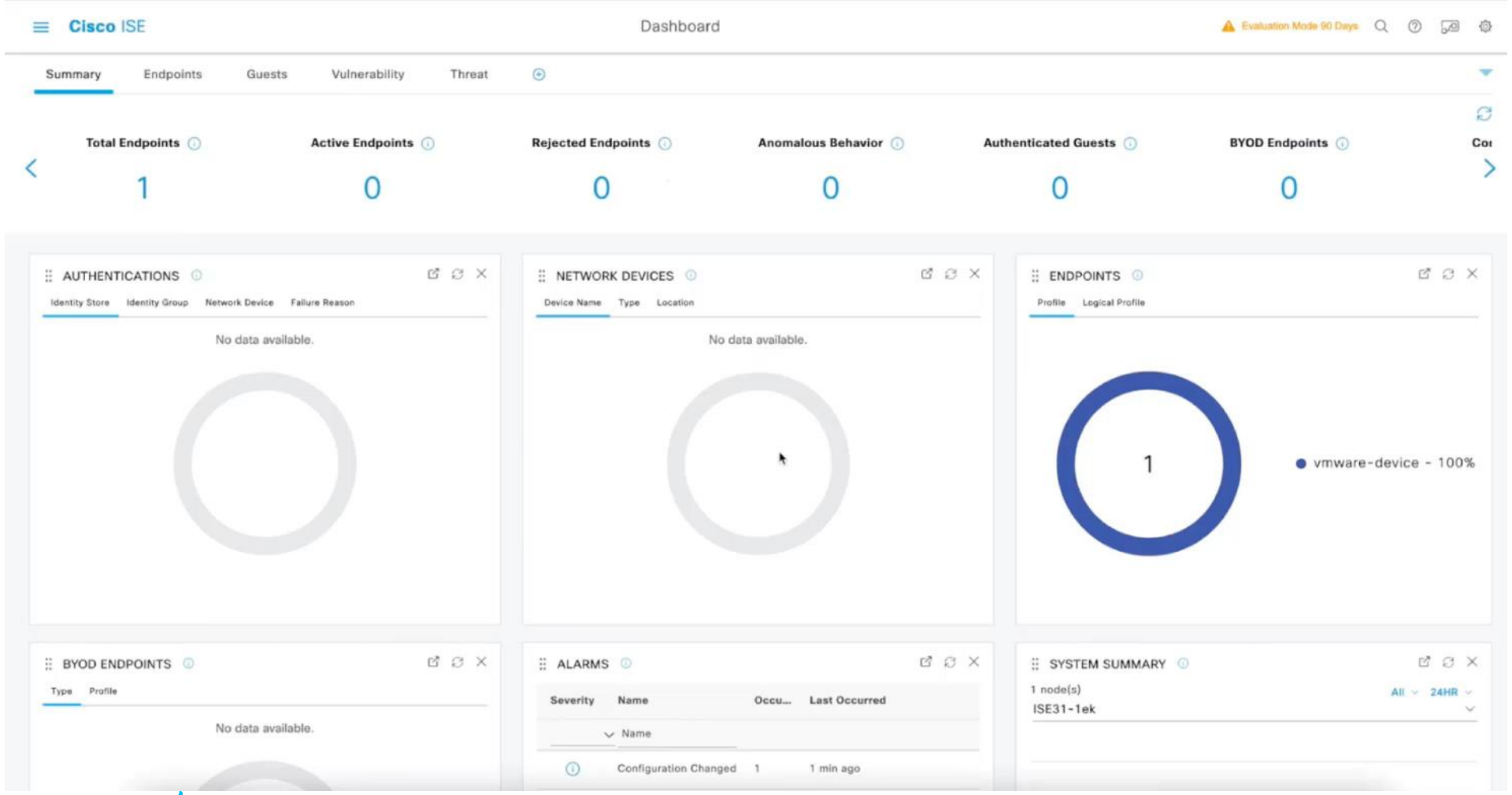
- Internal CA service, issues and manages certificates for endpoints, pxGrid and ISE messaging

Different ISE System certificates

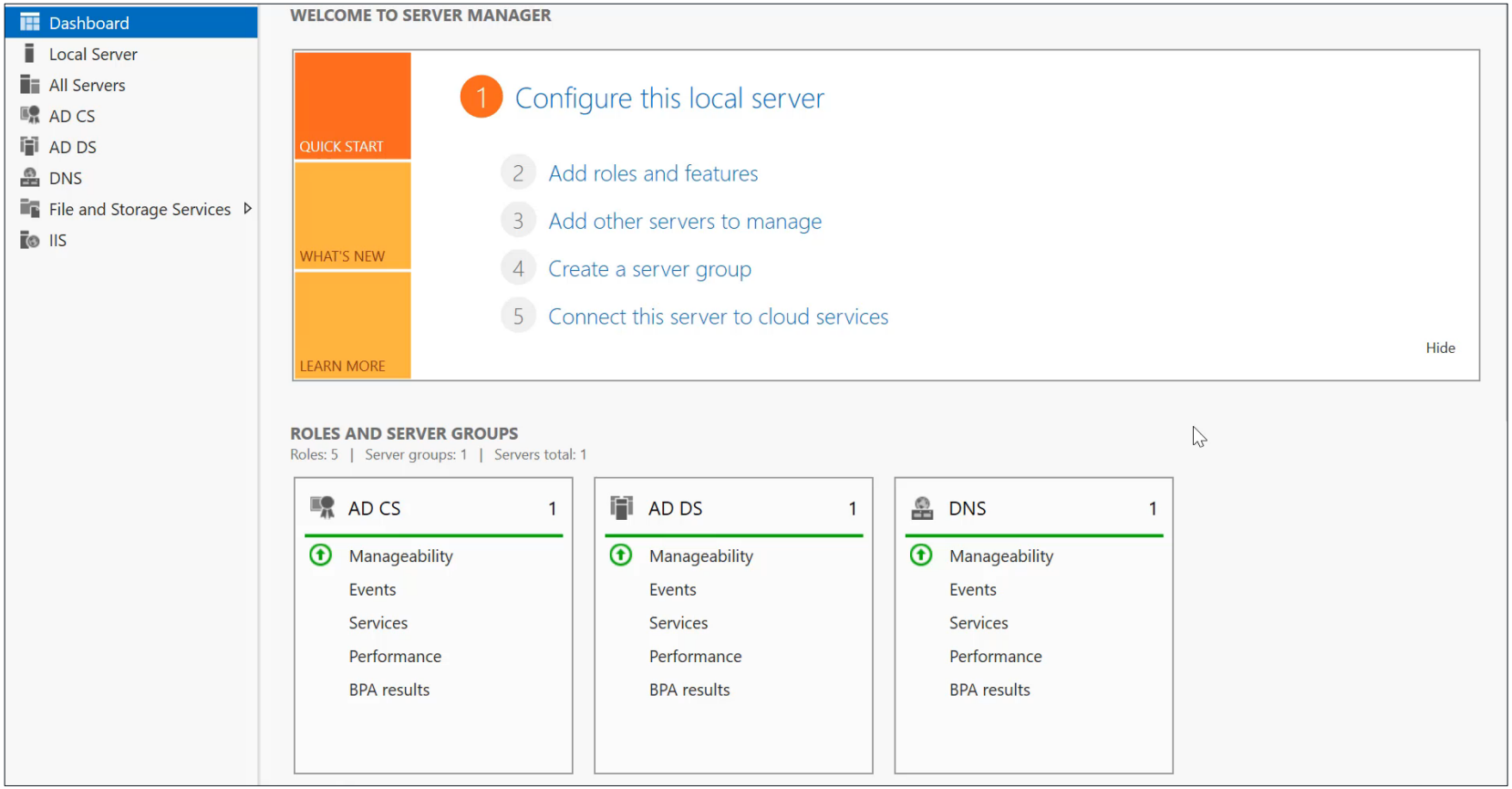


Systems and Trusted Certificates





Sample pxGrid Certificate Template



- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases

Network Device discovery

cs.co/nad-capabilities

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

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

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

Third-Party Network Device Compatibility

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.

802.1X	✓	✓	✓	✓	✓	✓
Profiling	✓	✓	✓	✓	✓	✓
Posture	✓	✓		✓	✓	✓
Guest	✓	✓		✓	✓	✓
BYOD	✓	✓		✓	✓	✓

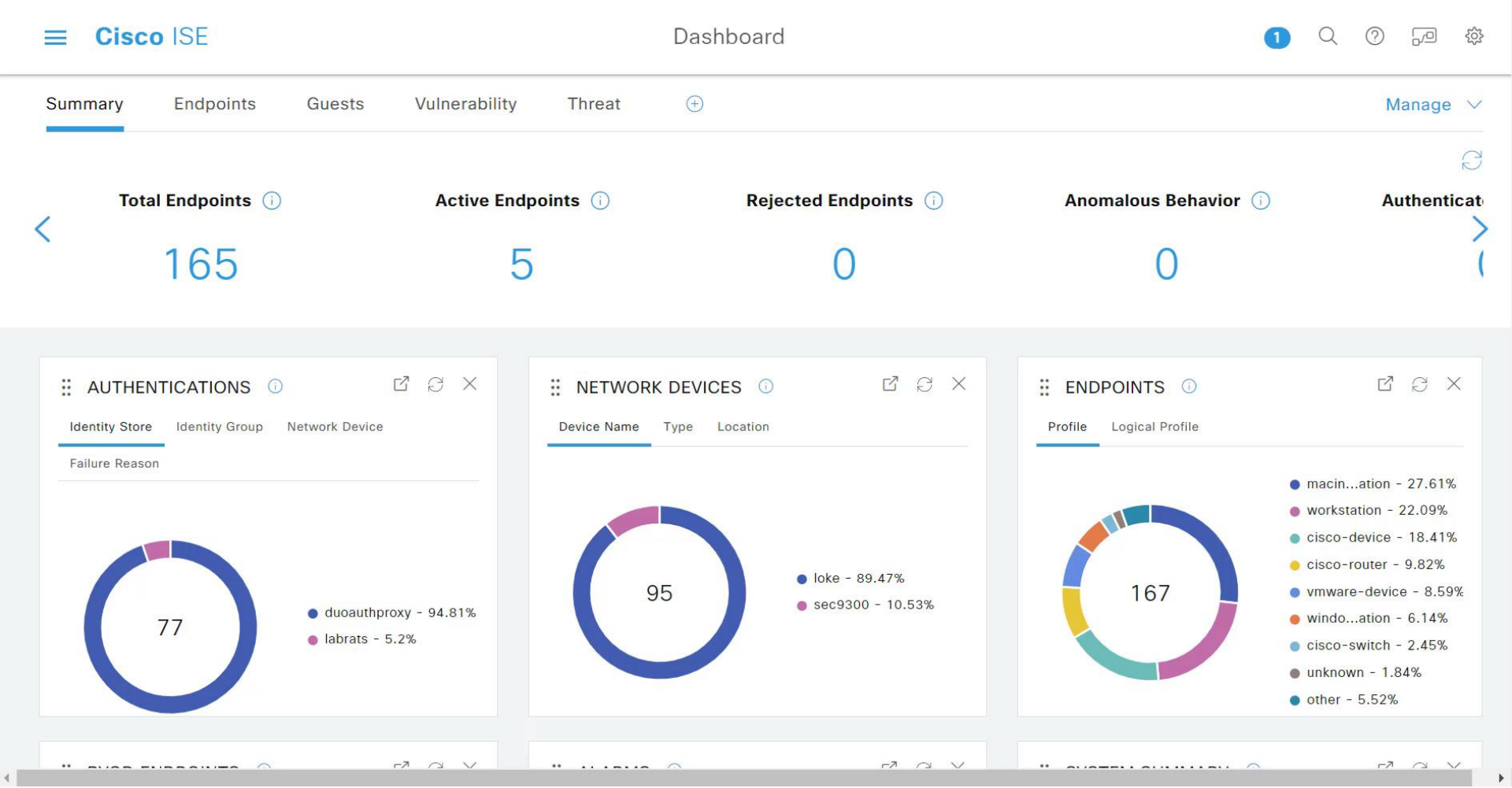
Capabilities

- Templatized MAB configuration for select non-Cisco vendor devices
- CoA and URL re-direction
- Non-Cisco NADs enabled to drive regular 802.1X operations

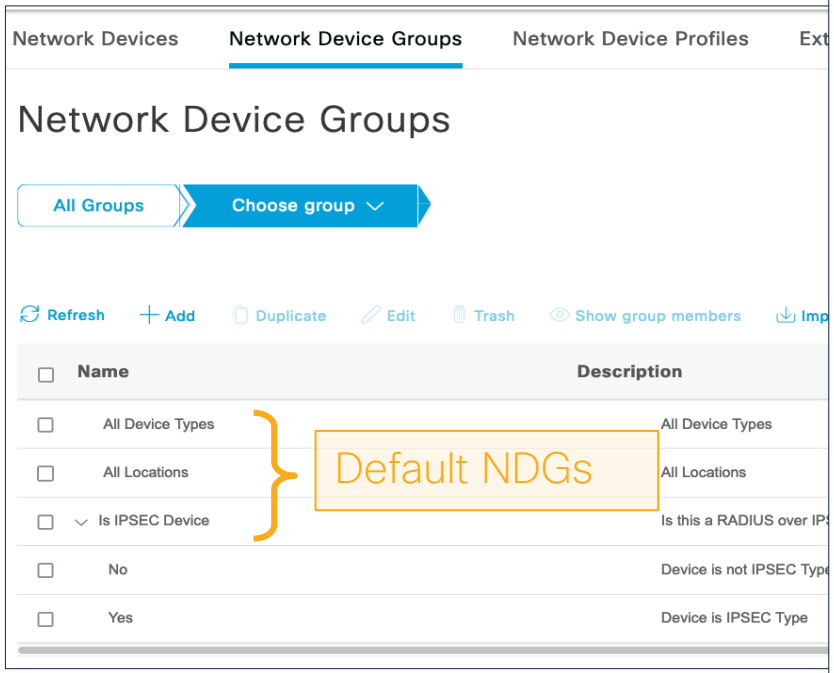
*Refer to Cisco Compatibility Matrix http://cs.co/ise-compatibility

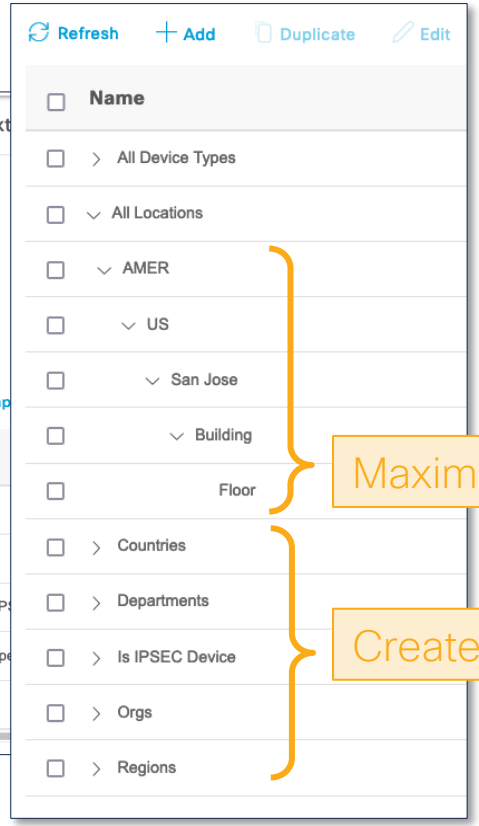
Additional Tips

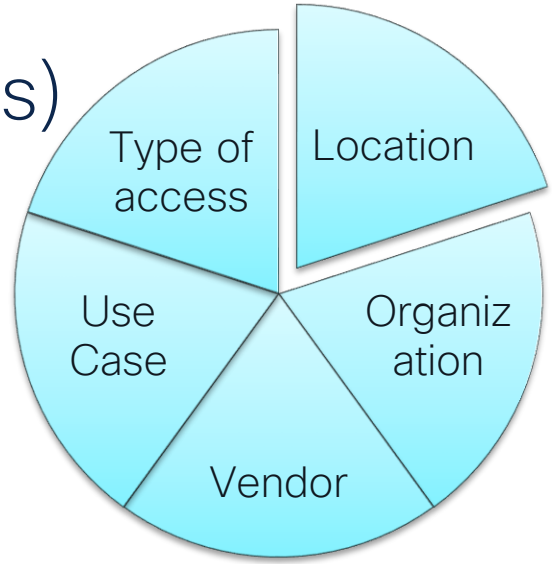
- Standardize! Standardize! Standardize!
  - IOS versions
  - AAA configuration
  - Wireless configuration
  - Profiling configuration
- Always Test before implementing!
- 3rd party device documentation
  - Vendor Specific RAIDUS dictionary needed?
  - Network Device Profile creation needed?



Default Network Device Groups (NDGs)

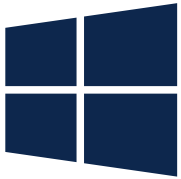


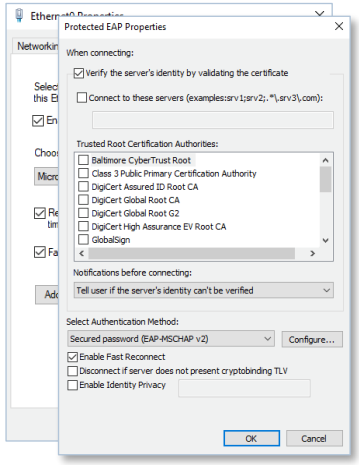


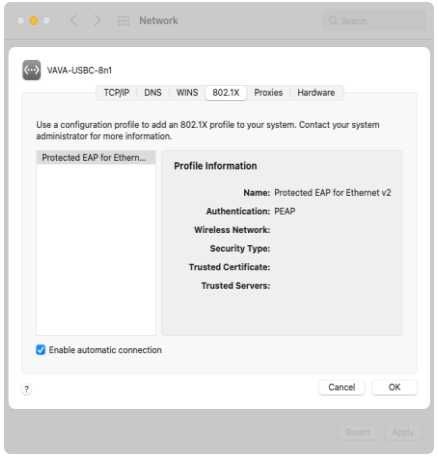


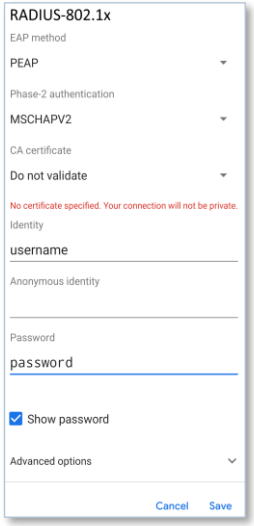
- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases

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)
- Group Policy for:
  - Supplicant configuration
  - Pushing certificates
  - Pre-configure SSIDs – better user experience
- Involve the Active Directory Team

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases

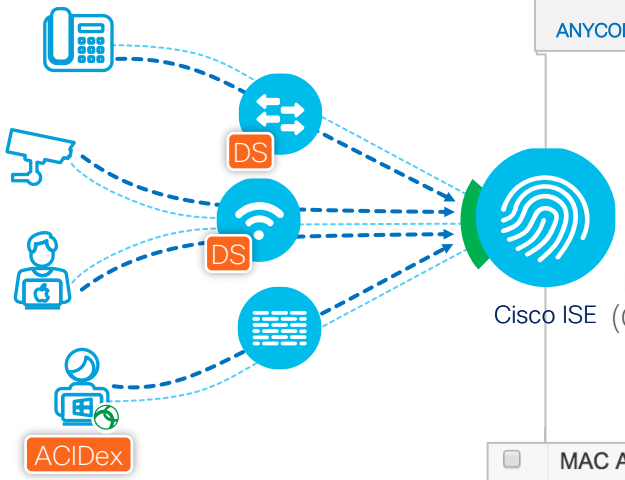
Endpoints: Everything Else

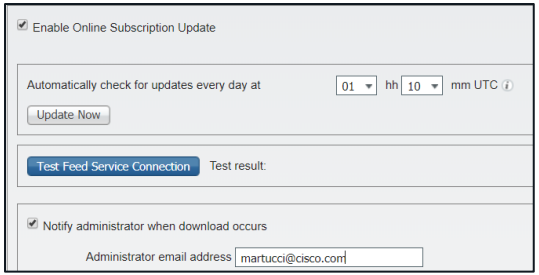
Profiling and probes

ACTIVE PROBES	Netflow	DHCP	DNS	HTTP	RADIUS	NMAP	SNMP	AD
DEVICE SENSOR	CDP	LLDP	DHCP	HTTP	H323	SIP	MDNS	
ANYCONNECT	ACIDex							

ISE data collection methods for Device profiling

Endpoints send interesting data, that reveal their device identity





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

Profling helps with differentiated access also for authenticated devices

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 HTTP Probe

 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 iPad	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

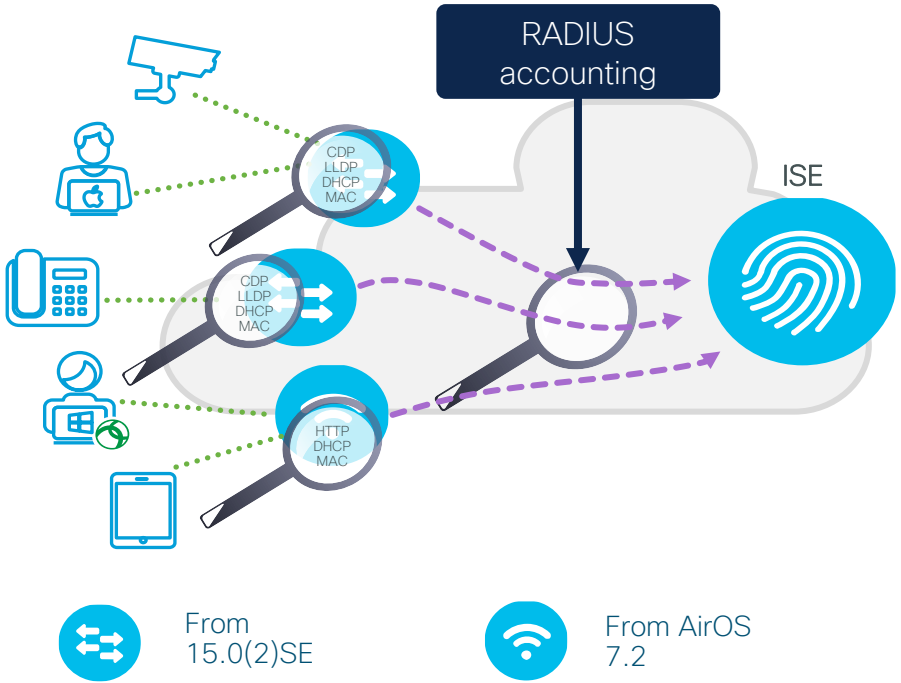
Effect of NMAP Probe

 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 LaserJet P4015	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

Device Sensor

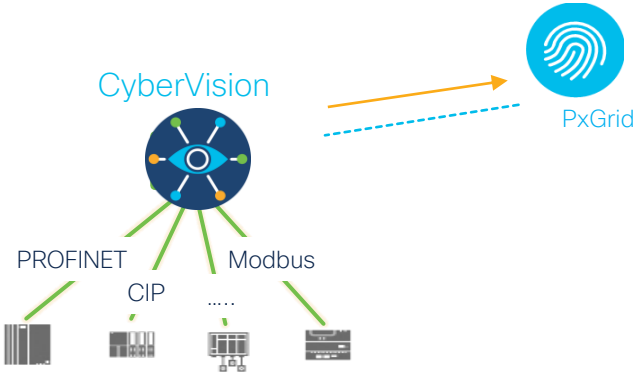


Network devices send attributes via RADIUS to ISE to optimize collection:

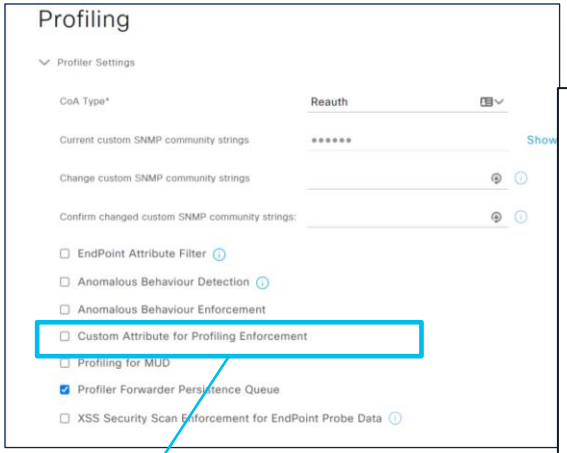
Attributes used:

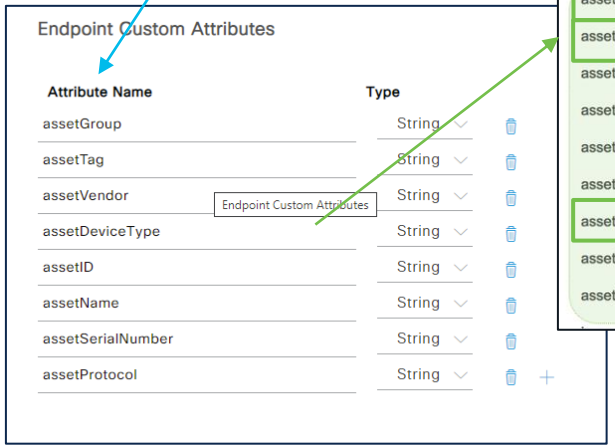
- MAC OUI
- CDP/LLDP
- DHCP
- HTTP (WLC only)
- mDNS,
- H323,
- MSI-Proxy (4k only)

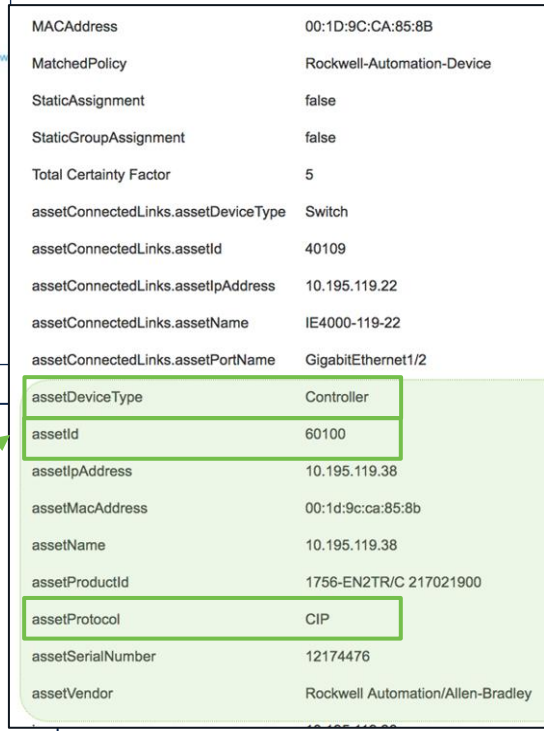
PxGrid Probe



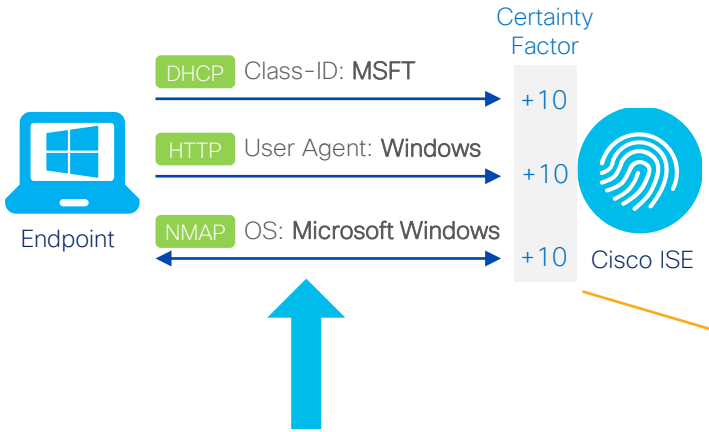
- CyberVision classifies the OT devices.
- The attributes are then sent to ISE via pxGrid
- ISE populates the custom attributes with the ones received via profiling pxGrid probe







ISE profiles definition

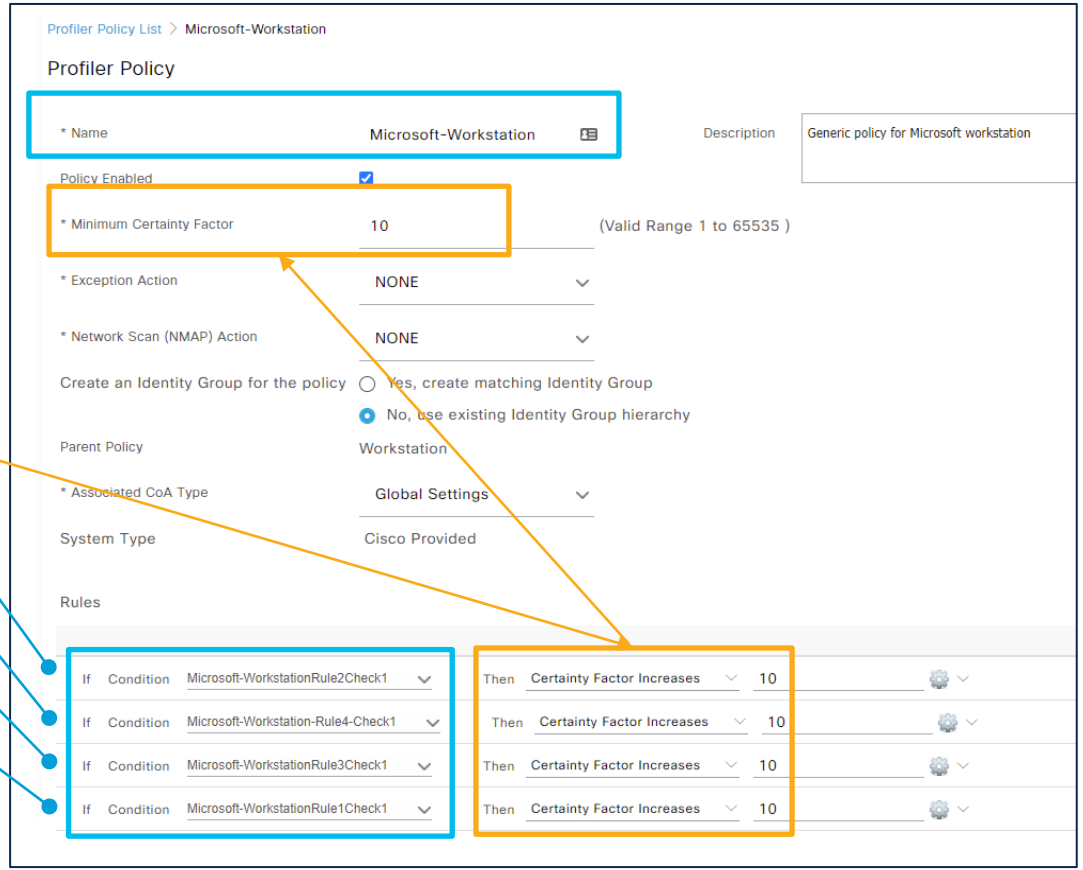


DHCP:dhcp-class-identifier CONTAINS MSFT

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

IP:User-Agent CONTAINS Windows

NMAP:operating-system CONTAINS Microsoft Windows



Profiling Packages and Integrations

Medical Devices

Hospital

250+ Medical device profiles

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

IOT Building & Automation

Library

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

Factory

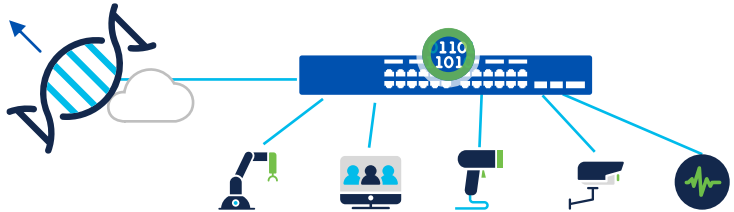
Industrial Devices

pxGrid

ISE

CyberVision

Cisco CyberVision

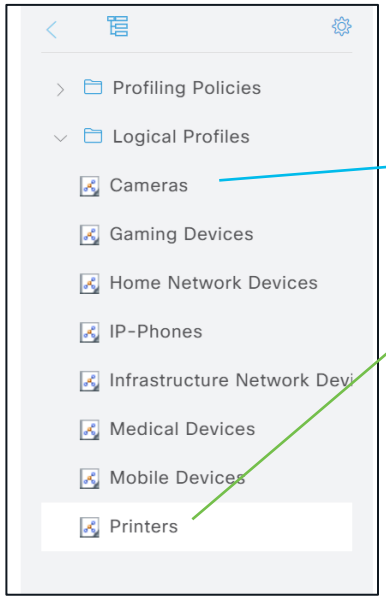


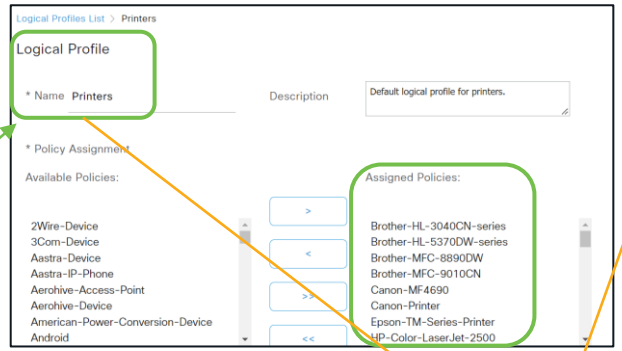
Cisco AI Endpoint Analytics

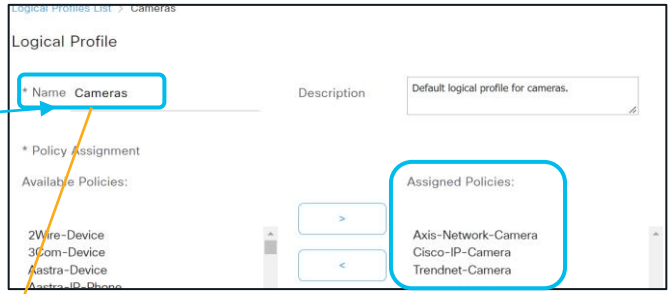
Profiles IOT devices and sends endpoint labels via pxGrid to ISE for authorization

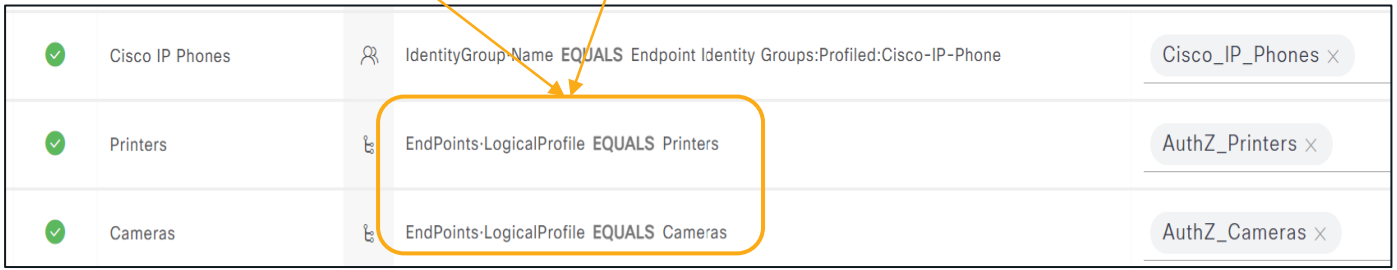
https://community.cisco.com/t5/tag/ise-endpoint-profile/tg-p/board-id/4561-docs-security

Using device profiles and logical profiles in ISE



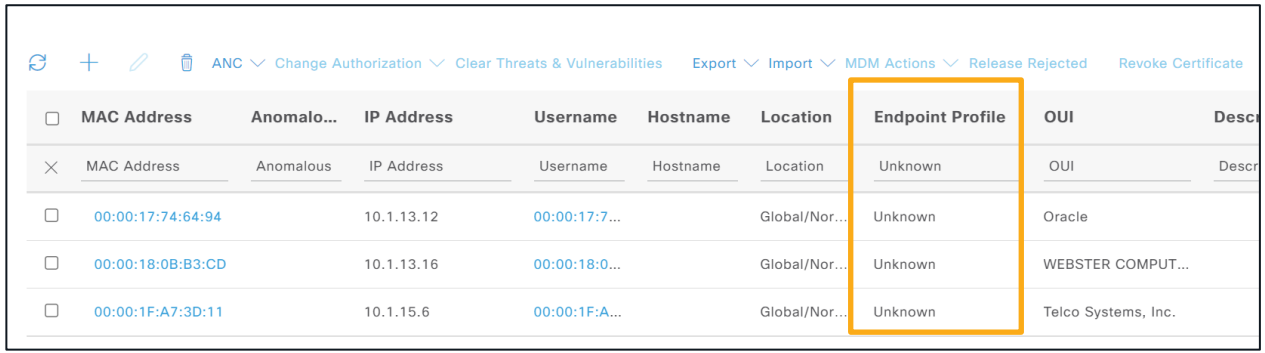






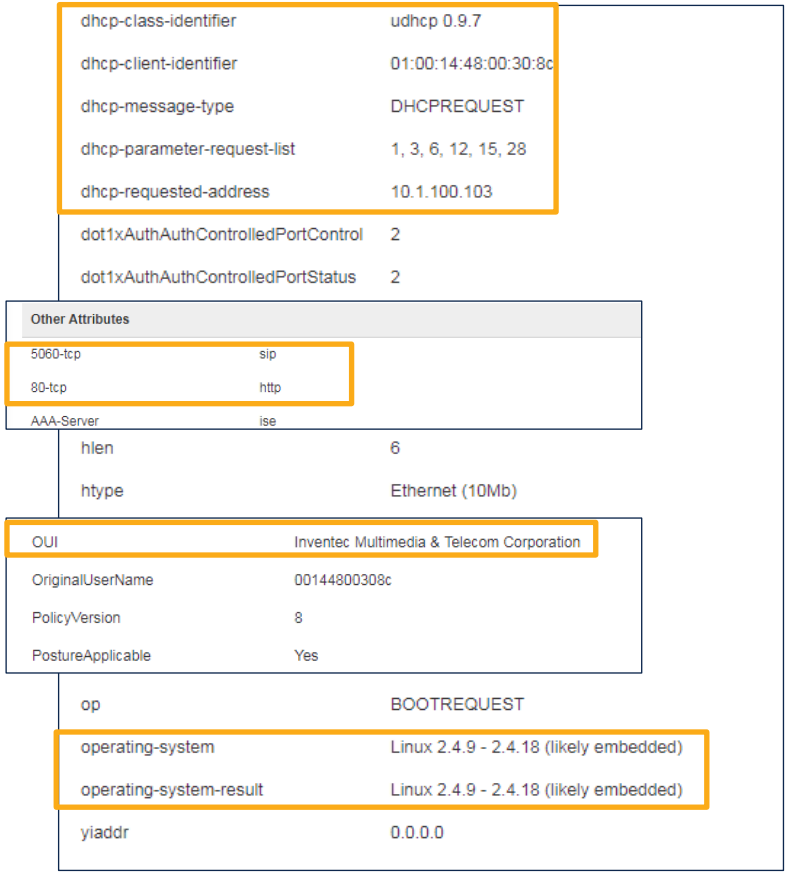
ISE Profiling Updates

- 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

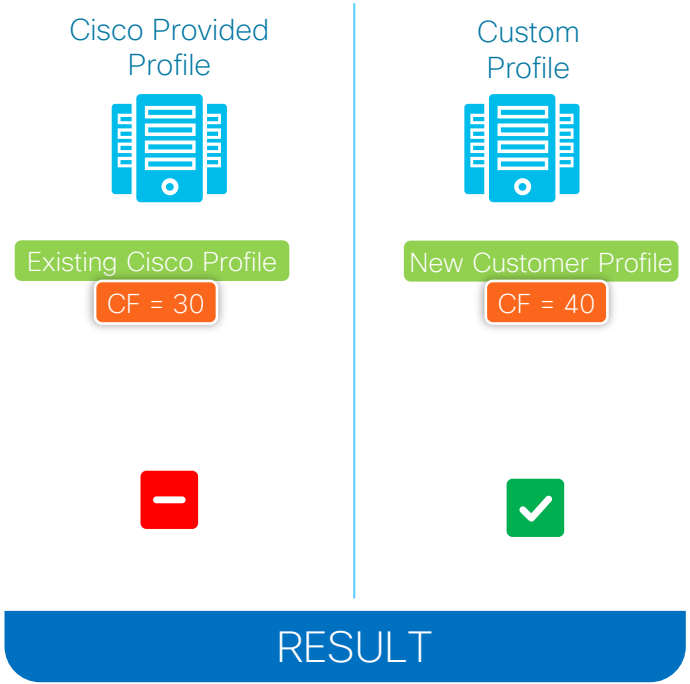


Create custom profiles

- 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



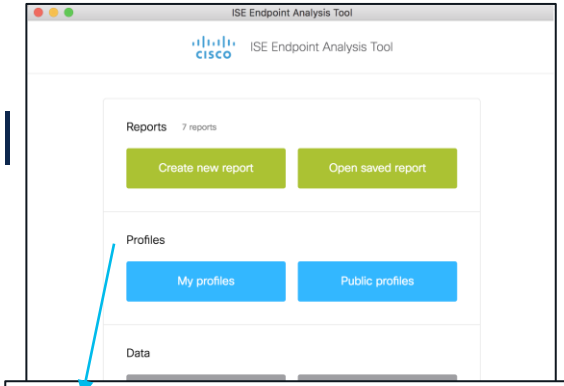
Profiles Precedence

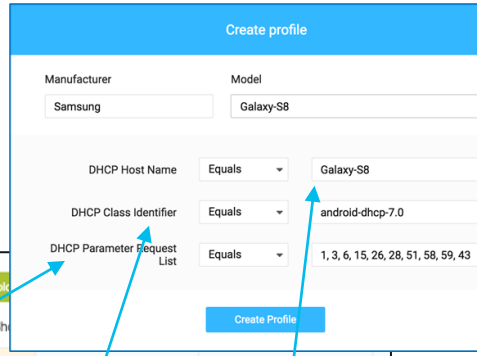


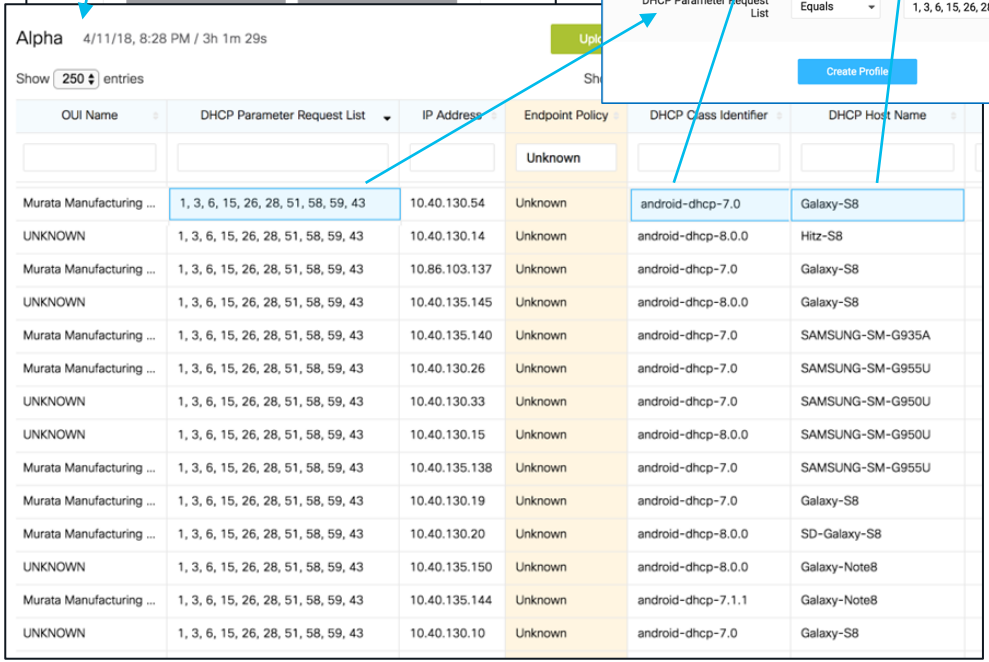
Endpoint Analysis Tool

- Collects endpoint attributes from Primary PAN database
- Select attributes to be used in new profile and click “Create Profile”
- Option to edit condition criteria before complete
- Import XML into ISE
- Advanced profile tuning can be performed inside ISE

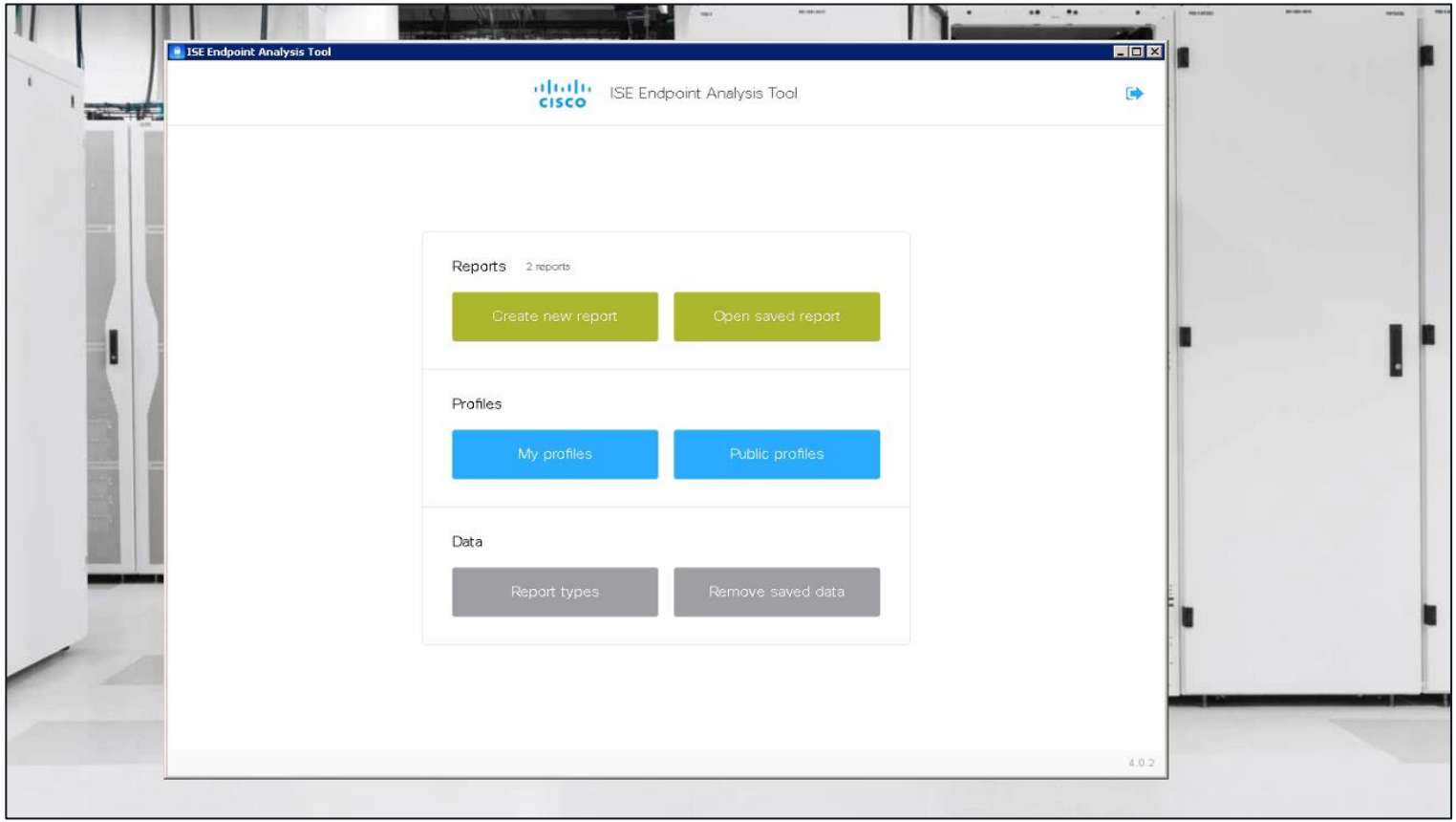
http://iseeat.cisco.com



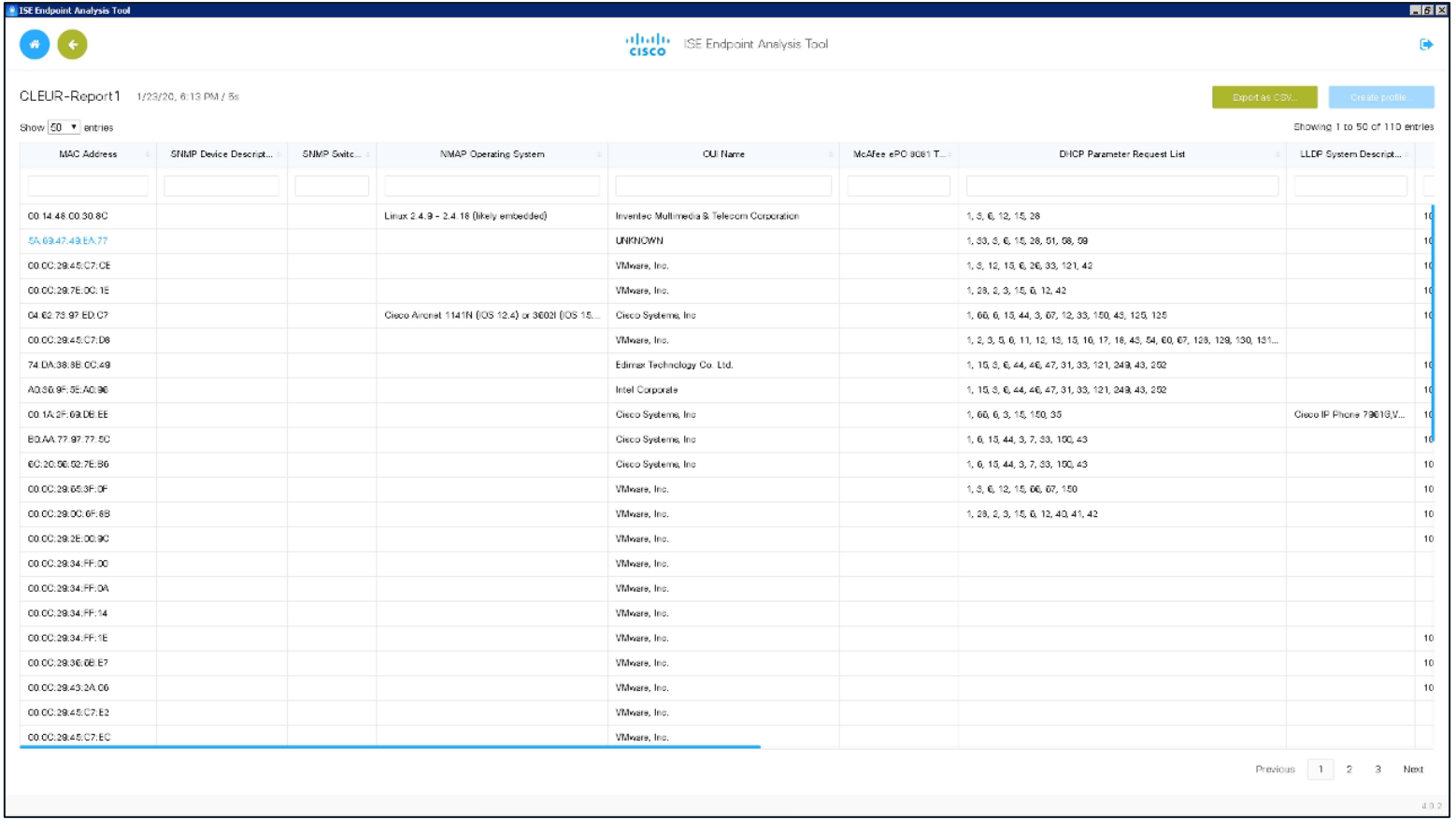




ISE Endpoint Analysis Tool –Endpoint Report



ISE Endpoint Analysis Tool – Custom Profile Creation



ISE Profiling Design Guide

This deployment guide is intended to provide the relevant design, configuration and operations-related guidance to deploy Cisco Identity Services Engine (ISE) Profiling.

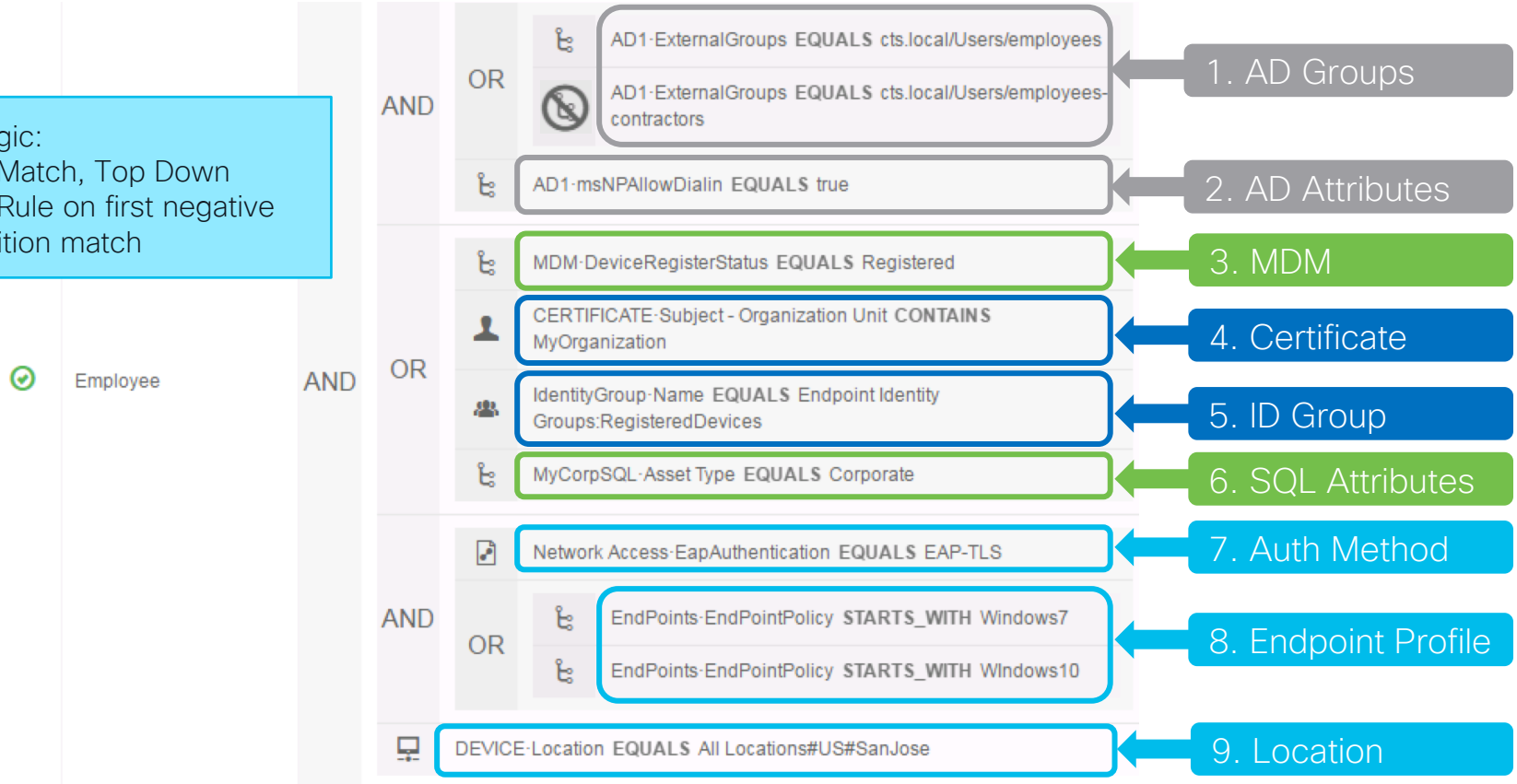
by Craig Hyps

ISE profiling design guide

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases

Auth Policy Optimization

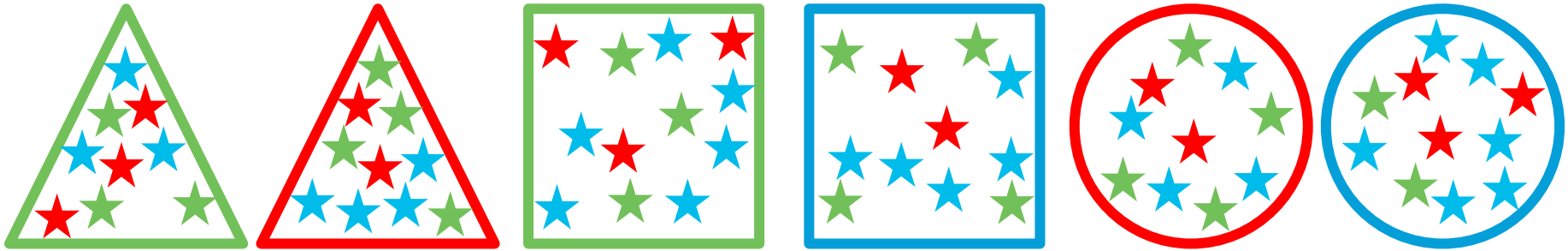
Policy Logic:
- First Match, Top Down
- Skip Rule on first negative condition match



Authorization Policy Optimization – Search Speed Test

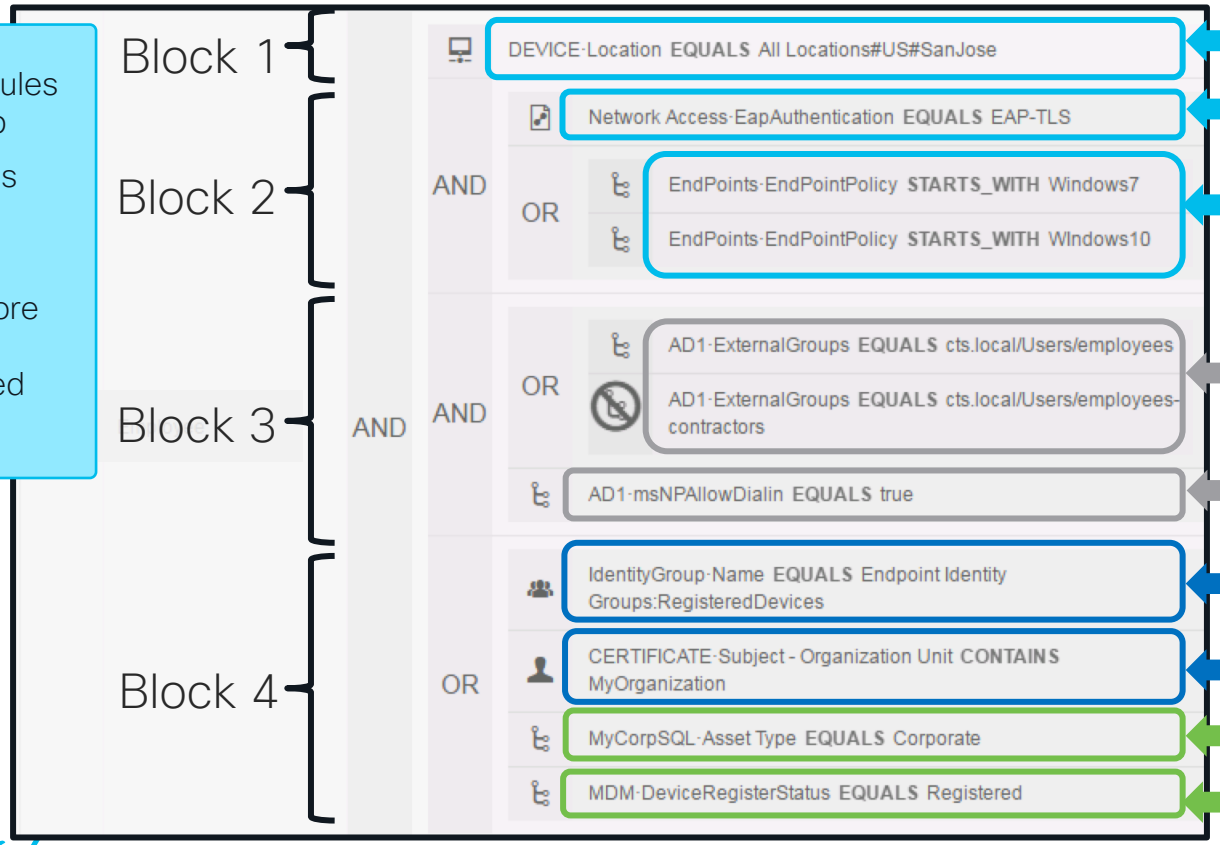
Find the object where:

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



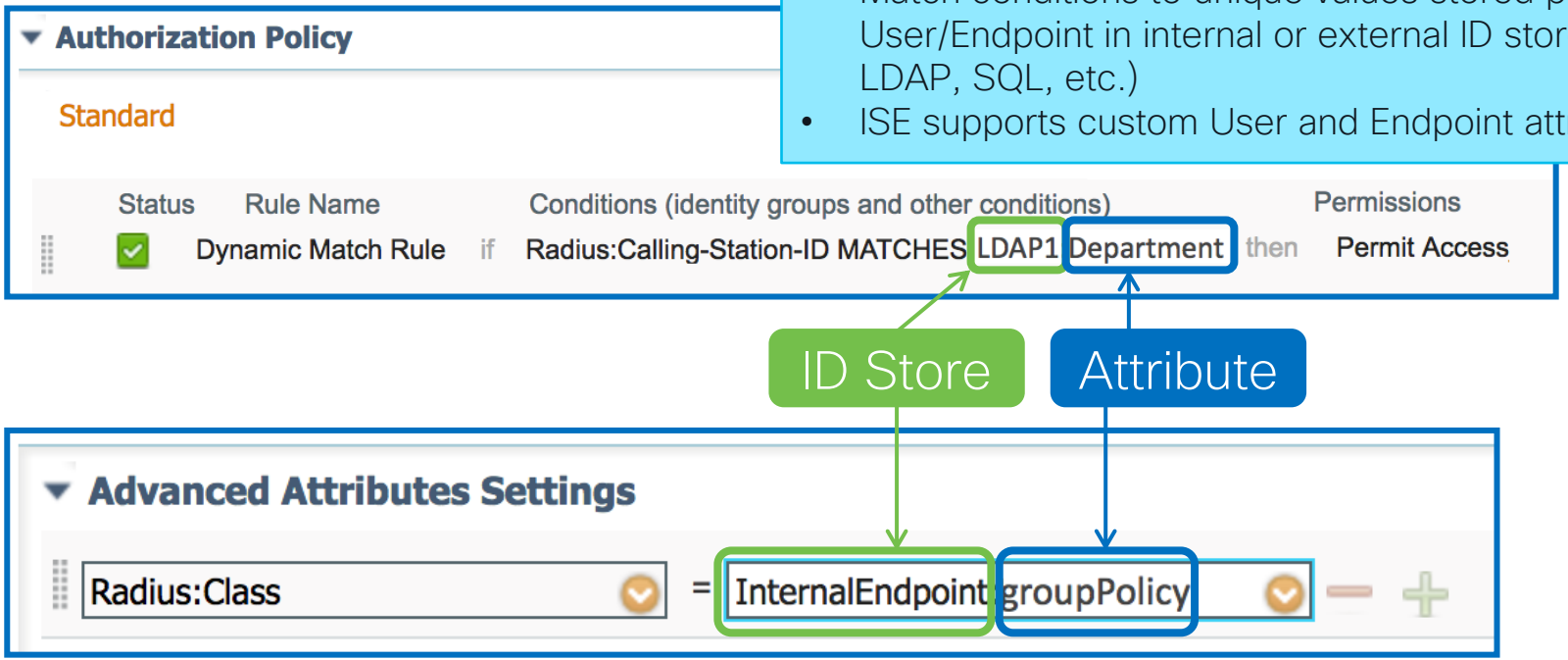
Auth Policy Optimization

- More specific rules generally at top
- Local conditions should be put before external
- Try to place more “popular” rules before less used rules



Dynamic Variable Substitution

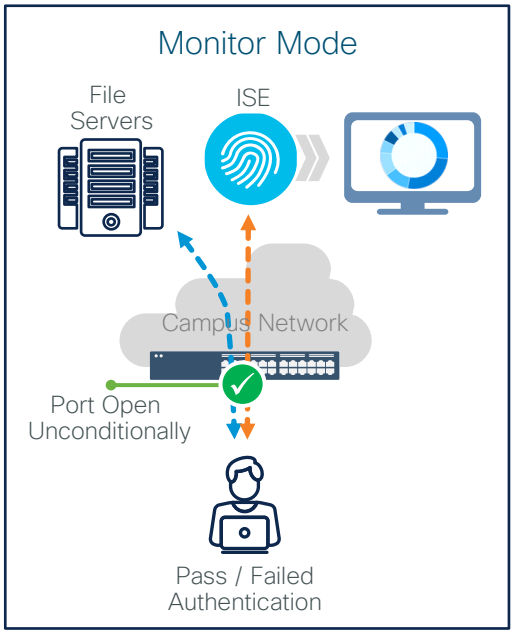
- Match conditions to unique values stored per-User/Endpoint in internal or external ID stores (AD, LDAP, SQL, etc.)
- ISE supports custom User and Endpoint attributes



- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases

Deployment Modes

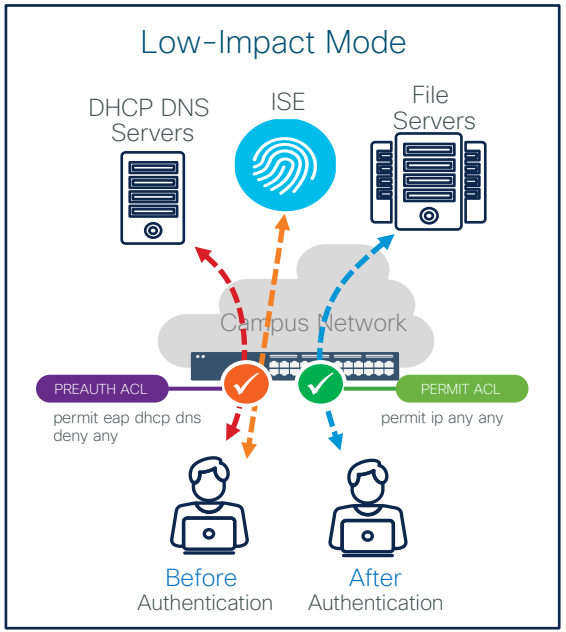
Phase I (Visibility Only)




```
authentication open
```

No impact to existing network

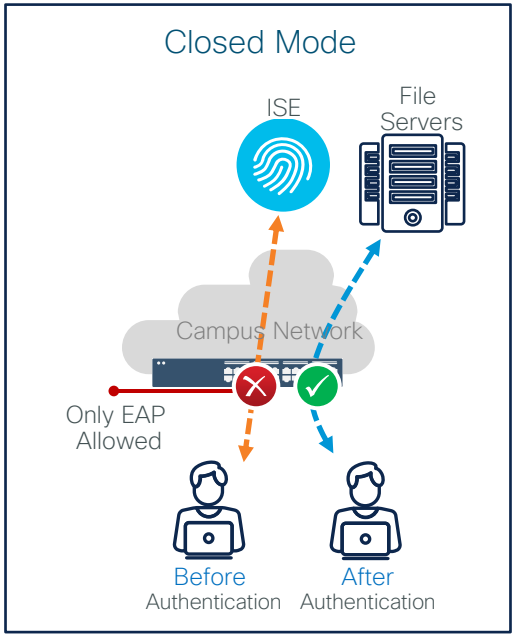
Phase II (Visibility and Control)




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

Begin to control/differentiate access

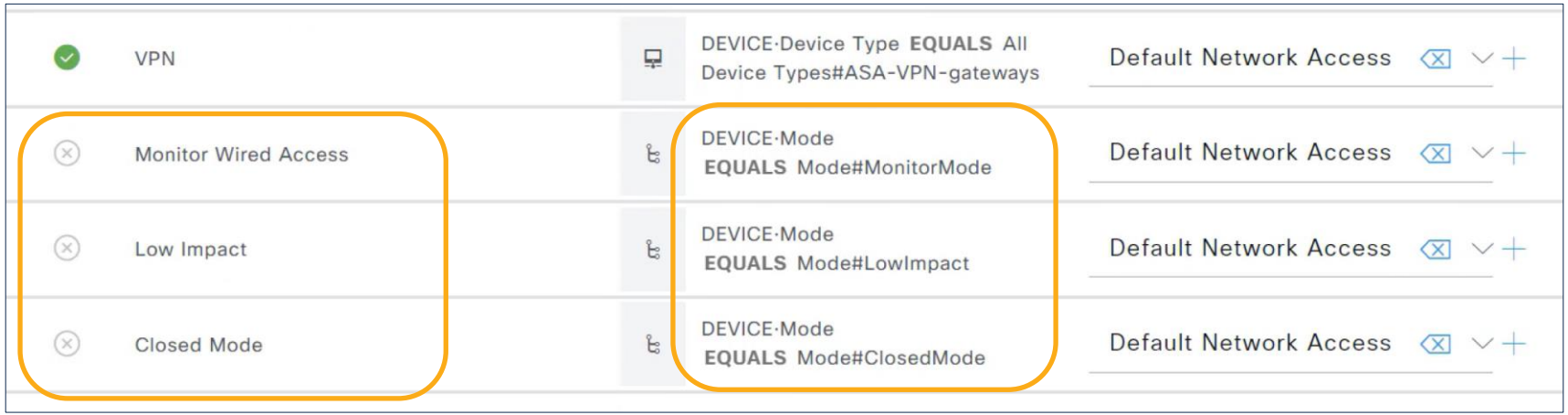
Phase III (Visibility and Control)



- Not everyone goes into 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

Supporting ISE After Deployment

- Standardize devices configuration as much as possible
- 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

User involvement

User Communication before and after ISE rollout

Wired Authentication Support Page

Your workstation is Authenticated

What are we doing ?
IT Network Services are implementing 802.1x Authentication on the Wired Network in Cisco offices to bring it in line with the Wireless and CVO networks and adhere to Cisco's Network Access Policy. So that individuals with physical access to Cisco network ports cannot access Cisco data and potentially compromise Cisco's network from inside the network perimeter.

What is 802.1x ?
IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

What do I need to do ?
Cisco IT Managed devices should have 802.1x enabled on them already. If not – please see support instructions below...

Cisco Managed Windows Laptops	Mac Laptops	Remote Desktops **Windows Only**	Linux / Unix workstations	Voice/Video Endpoints	Non IT Managed Printers
Personal devices (Apple TVs, PlayStation etc.)	Routers, Switches, ESXi, and APs	Onsite (In-Office) – Patching	Demo/Training devices	Password Management	Generic Users
802.1x exception requests					

Wrap up

Deploying any network access control solution is crucial

but it isn't easy....

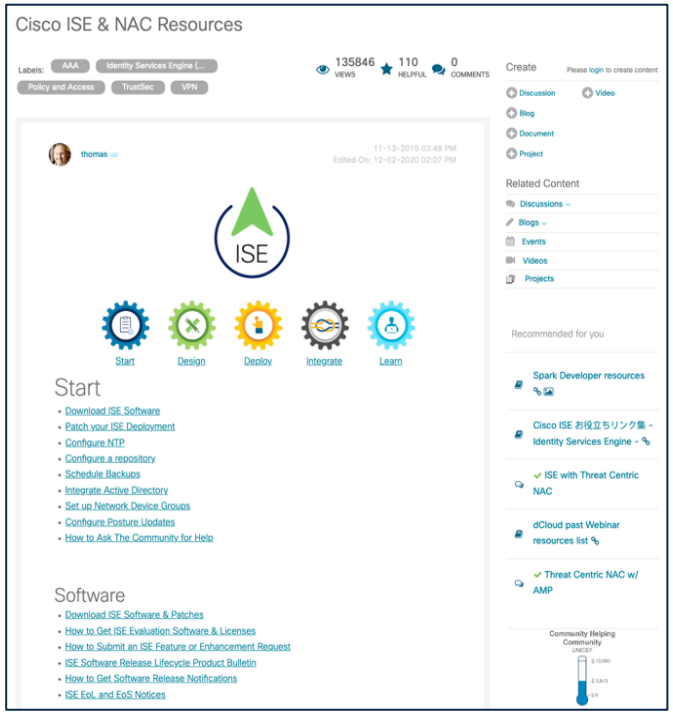
Planning is essential to any successful development.

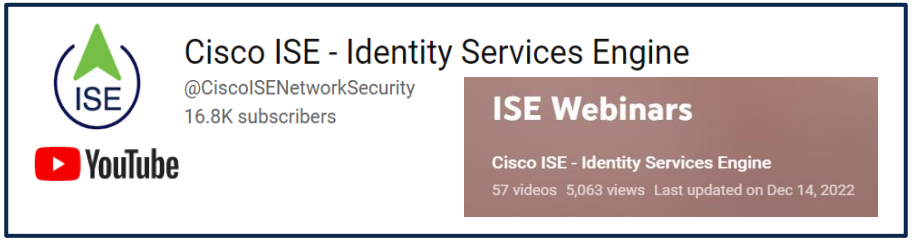
Technical Session Surveys

- Compliments ☺
- What you liked
- Suggestions?

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





Security Technologies

Zero Trust

Learn how Cisco will help you deploy a broad range of technologies in order to deploy your end to end Zero Trust strategy.

START

Feb 5 | 16:00
LABSEC-2089
Multi-factor Authentication: Integration of DUO with ISE for MFA

Feb 6 | 08:45
TECSEC-2007
Find Your Zen with Cisco Secure Workload for Zero Trust Segmentation

Feb 6 | 08:45
TECSEC-2781
Zero Trust: From understanding the risks to architecting a practical solution

Feb 6 | 15:20
PSOSEC-1210
A global view on Zero-Trust - mapping your business resilience requirements

Feb 7 | 08:45
BRKSEC-2445
The Art of ISE Posture, Configuration and Troubleshooting

Feb 7 | 16:45
BRKSEC-2053
Zero Trust: Securing the Evolving Workplace

Feb 7 | 17:00
BRKSEC-1139
Application Security - The Final Frontier

Feb 8 | 10:45
BRKSEC-2096
Securing Industrial Networks: Where do I start?

Feb 8 | 13:30
BRKSEC-2748
Taking Authentication to the Next Level with Cisco Secure Access by Duo

Feb 8 | 17:00
BRKSEC-2123
Solving the Segmentation Puzzle! Secure Workload and Secure Firewall Integration

If you are unable to attend a live session, you can watch it On Demand after the event

Feb 9 | 08:30

BRKSEC-2660

ISE Deployment Staging and Planning

Feb 9 | 13:45

BRKSEC-2834

Cisco's Unified Agent: Cisco Secure Client. Bringing AMP, AnyConnect, Orbital & Umbrella together

Feb 9 | 14:00

LTRSEC-2000 ISE

Deployments in the Cloud - Automate ISE Deployments in AWS and Integrate Them with Azure Active Directory

Feb 10 | 09:15

BRKSEC-2039

Secure Access with ISE in the Cloud

Feb 10 | 11:00

FINISH **BRKSEC-2773**

How to Build a Secure Multi-Cloud Environment with Cisco Secure Workload

If you are unable to attend a live session, you can watch it On Demand after the event

Security Technologies

Network Security

Learn about a broad range of solution and technologies which will help you better understand how to secure your network. You will find topics such as VPN, ISE, IPv6, DDoS, IoT....

START

Feb 5 | 19:00
LABSEC-2333
ISE integrations via pxGrid with FTD, WSA, StealthWatch

Feb 6 | 08:45
TECSEC-3781
Walking on solid ISE - Advanced Use Cases and Deployment Best Practices

Feb 7 | 08:45
BRKSEC-2445
The Art of ISE Posture, Configuration and Troubleshooting

Feb 7 | 11:30
BRKSEC-2037
Securing Starlink Internet Services

Feb 8 | 10:45
BRKSEC-2096
Securing Industrial Networks: Where do I start?

Feb 8 | 13:30
BRKSEC-2678
DDoS Mitigation: Introducing Radware Deployment on Firepower Appliances

Feb 9 | 08:30
BRKSEC-2660
ISE Deployment Staging and Planning

Feb 9 | 10:30
BRKSEC-2101
Malware Execution As A Service: a Deep Dive into CSMA Advanced File Analysis

Feb 9 | 15:45
BRKSEC-3058
Route based VPNs with Cisco Secure Firewall

Feb 9 | 15:45
BRKSEC-2044
Secure Operations for an IPv6 Network

Feb 10 | 09:00
BRKSEC-3019
Visibility, Detection and Response with Cisco Secure Network Analytics

If you are unable to attend a live session, you can watch it On Demand after the event

cisco Live!

Feb 10 | 09:00

LTRSEC-2381

Stronger Together: Uniting IT and OT Security with Cyber Vision

Feb 10 | 09:00

BRKIPV-3134

IPv6 Security in the Local Area with First Hop Security

Feb 10 | 11:00

FINISH

BRKSEC-2218

Cisco Secure Hybrid SWG – Your First Step to Your SASE Journey

If you are unable to attend a live session, you can watch it On Demand after the event

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

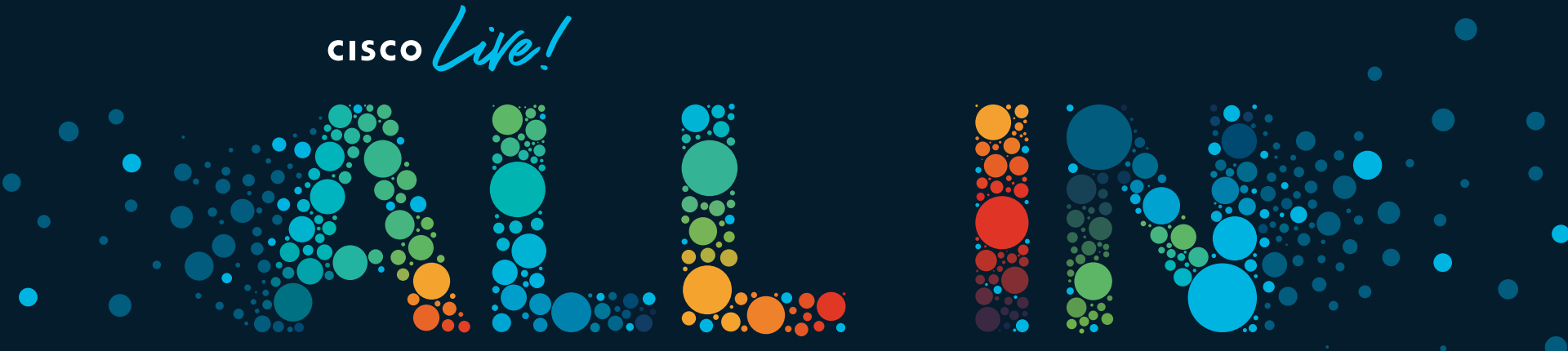
Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

The bridge to possible

Thank you

cisco Live!


CISCO Live!
ALL IN