Setting the Stage for ISE Deployment Success:

A Guide to Effective Planning

Francesca Martucci
Technical Solutions Architect –
Cybersecurity EMEA

BRKSEC-2660

Abstract

This session focuses on the preparation work that a customer should perform in order to ensure a successful ISE deployment. Like any technology, a deployment cannot be successful unless the proper planning and design isn't done first. We will examine best practices to follow in order to avoid some of the common pitfalls while preparing for an ISE deployment.

At the end of the session, attendees can expect to have a better understanding of how to prepare their environment and their staff for an ISE deployment. This session is targeted at Network and Security Engineers, who are tasked in deploying ISE successfully.

© 2025 Cisco and/or its affiliates. All rights reserved.

“A goal without a plan is just a wish”

Antoine de Saint-Exupéry

© 2025 Cisco and/or its affiliates. All rights reserved.

Deploying any network access control solution is crucial but it isn't easy....

© 2025 Cisco and/or its affiliates. All rights reserved.

What needs to be included in my planning?

© 2025 Cisco and/or its affiliates. All rights reserved.

Deploying any network access control solution is crucial

but it isn't easy....

Proper planning is essential to a successful deployment.

© 2025 Cisco and/or its affiliates. All rights reserved.

Who am I?

Technical Solutions Architect

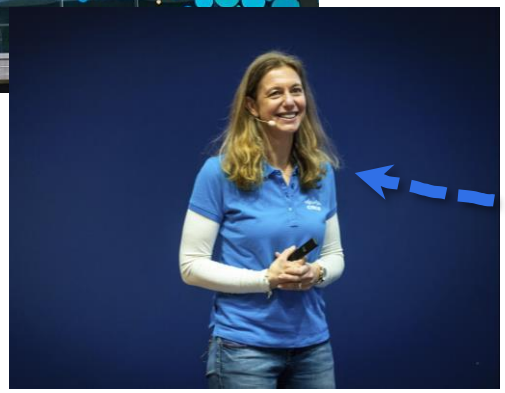
Cyber Security EMEA

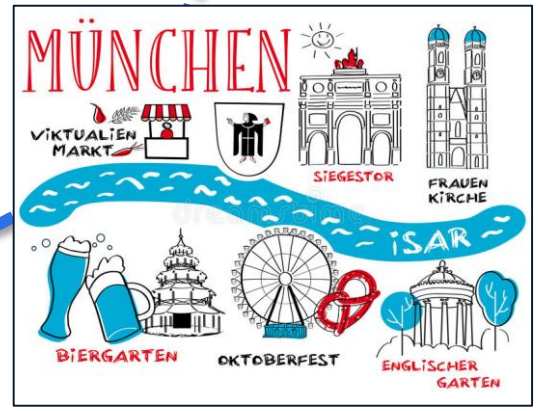
25 years of Cisco experience...

... And 3 countries

Main interest on

- Policy and Access
- Segmentation
- Industrial Security





© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

ISE High Level Design (HLD)

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

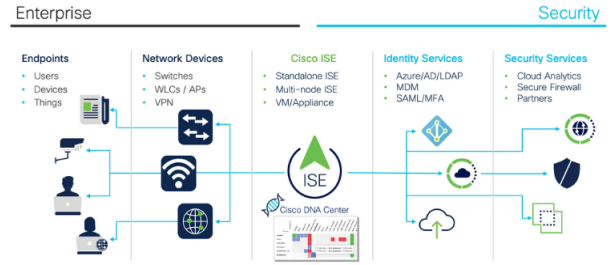
48001 VIEWS · 77 HELPFUL · 0 COMMENTS

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

01 Where To Start: planning

02 ISE Deployment Options

03 Certificates

04 Network Devices

05 Profiling

06 Policies

07 Create your own lab

08 802.1x Deployment modes

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Webex App

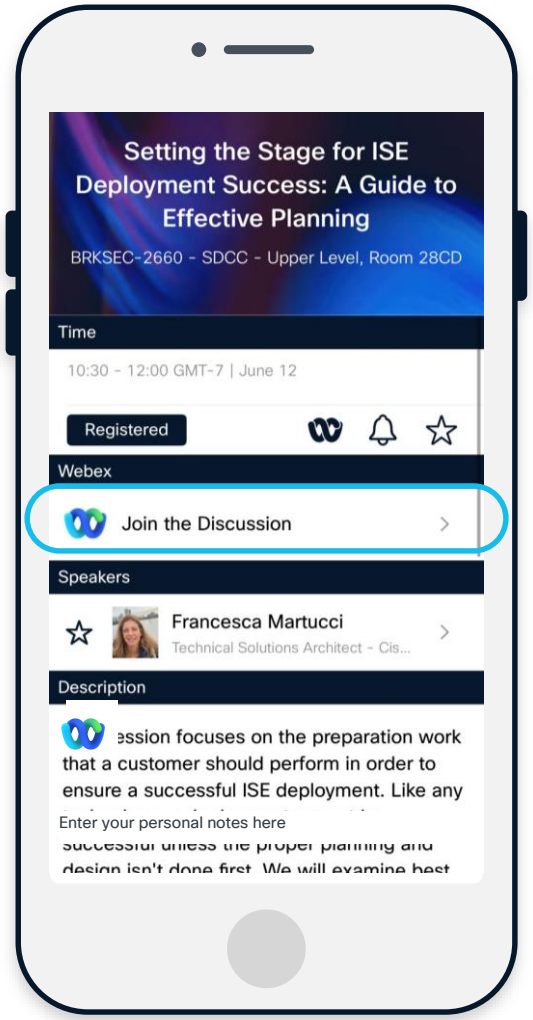
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 13, 2025.

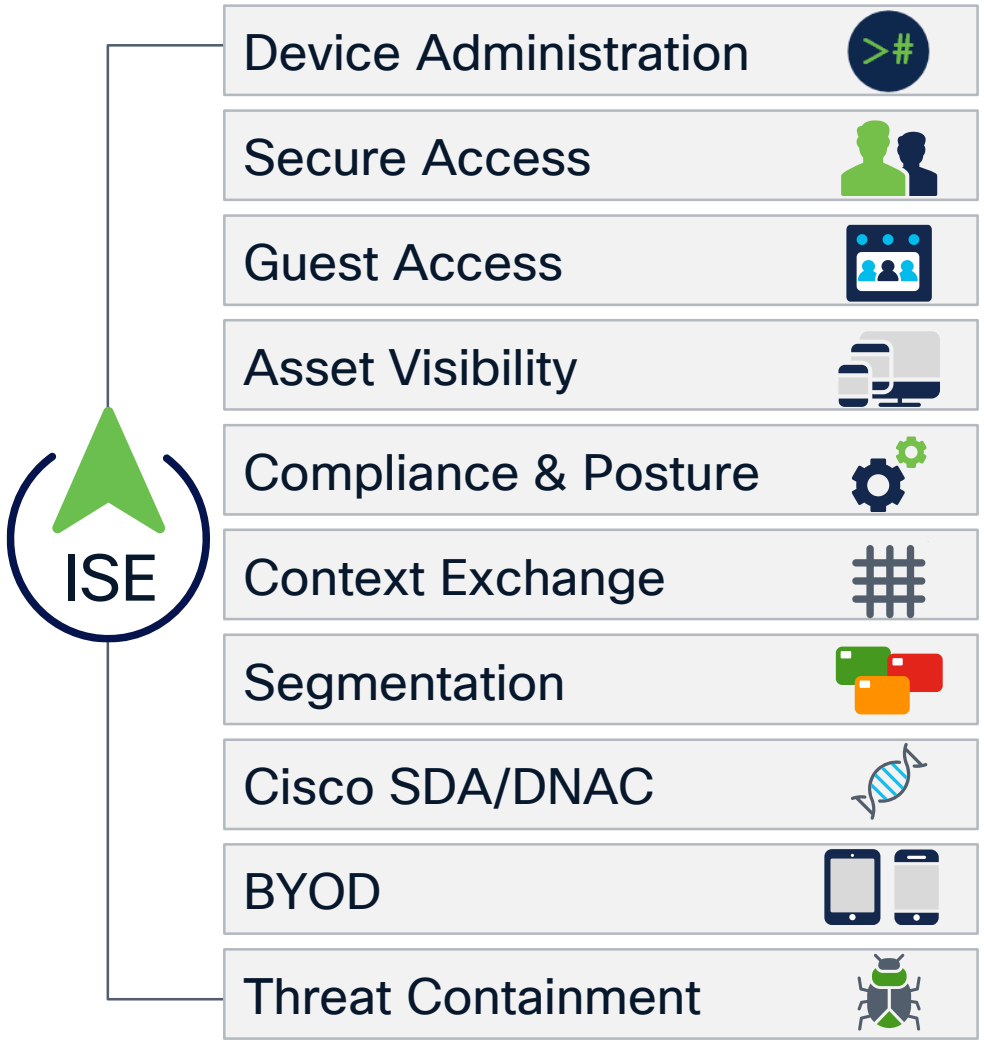


https://ciscolive.ciscoevents.com/ciscolivebot/**#BRKSEC-2660**

© 2025 Cisco and/or its affiliates. All rights reserved.

Where to start: planning

What are your business priorities?



What is the business trying to accomplish with ISE?

Profiling is critical with today IoT proliferation

Do you need a BYOD policy?

From where do you want to start?

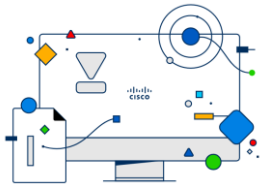
Which use cases could be considered for the future?

© 2025 Cisco and/or its affiliates. All rights reserved.

Understand Your Needs and Use cases

Objectives / Risk / Priorities

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

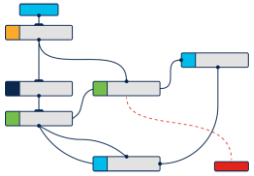


Environment

- 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

© 2025 Cisco and/or its affiliates. All rights reserved.

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."

© 2025 Cisco and/or its affiliates. All rights reserved.

Everyone Has Different Needs

Government

Financials

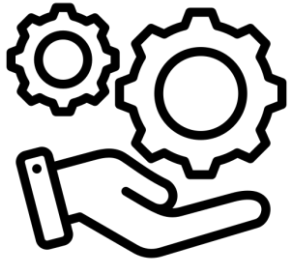
Healthcare

Retail

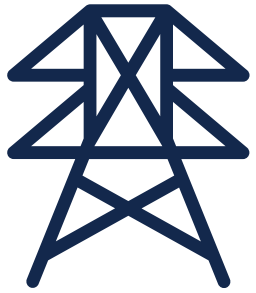
Education

Transportation

Services

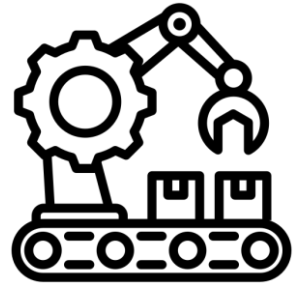


Utilities



Technology

Manufacturing



© 2025 Cisco and/or its affiliates. All rights reserved.

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

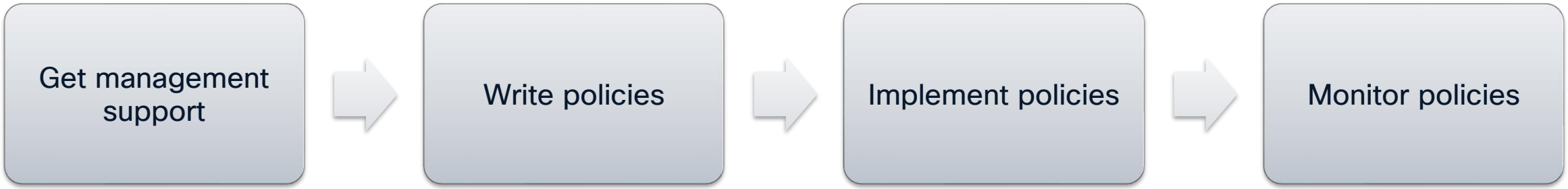
Endpoint Team Network Team Security Team

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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



© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

ISE Deployment Options

ISE Personas

Policy Administration Node (PAN)

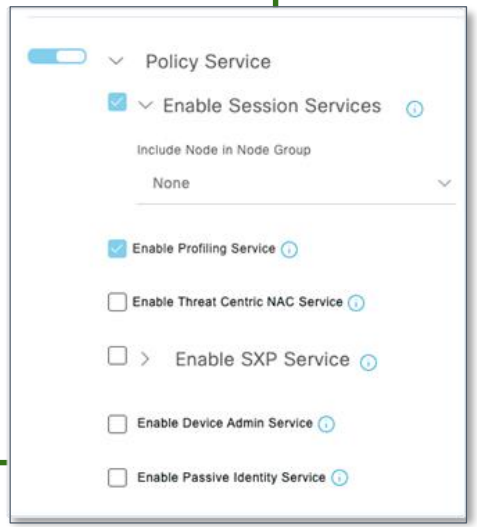
- Administrative GUI
- Policy configuration
- Policy replication
- Centralized Guest database
- Centralized BYOD database
- Configuration REST APIs

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

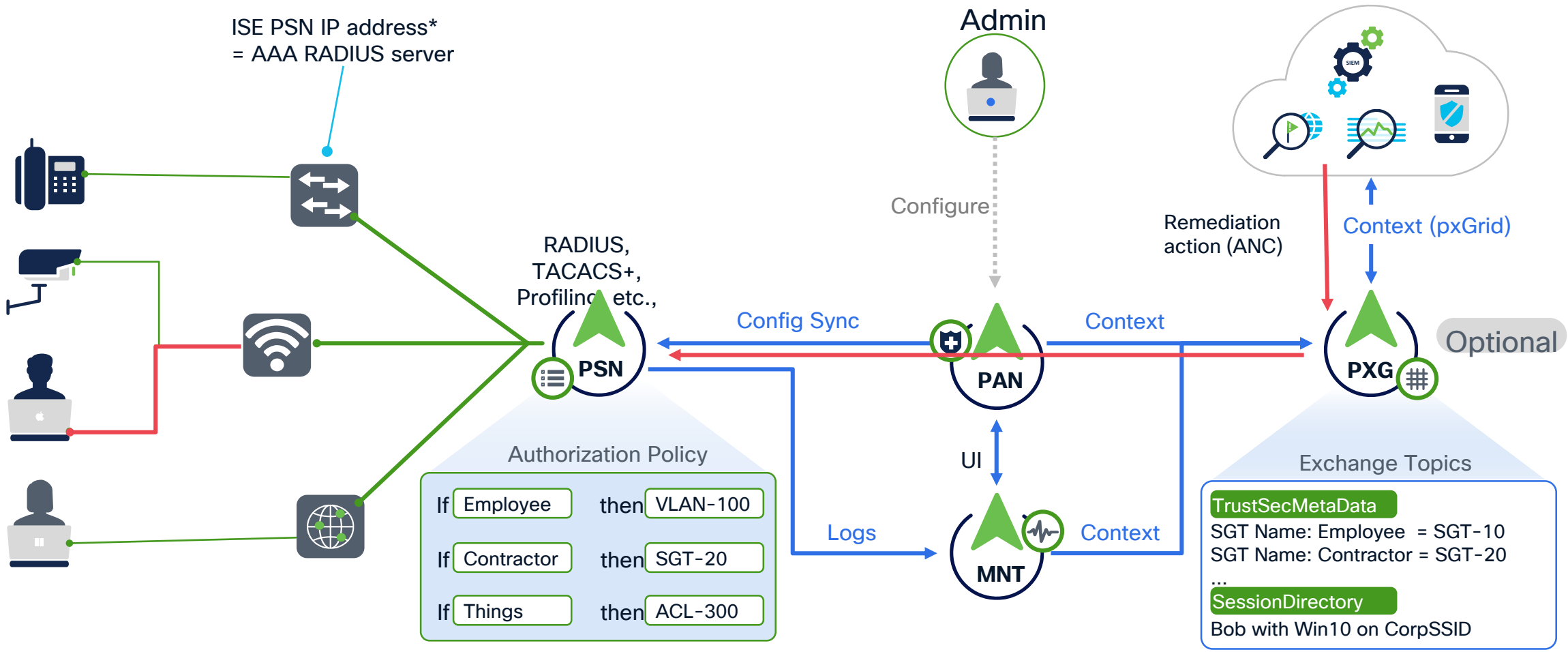


Platform Exchange Grid Node (PXG)

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

ISE Architecture and HA

Centralzed ISE

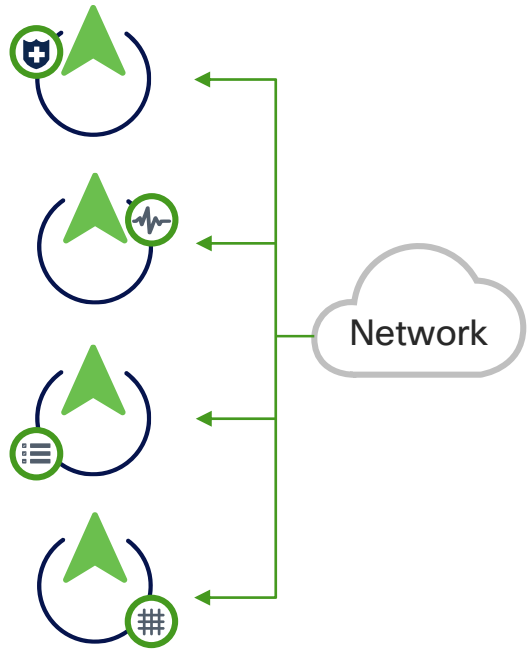
Policy Administration Node (PAN)
- Max 2 in a deployment

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



© 2025 Cisco and/or its affiliates. All rights reserved.

Maximum Concurrent Active Endpoints

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

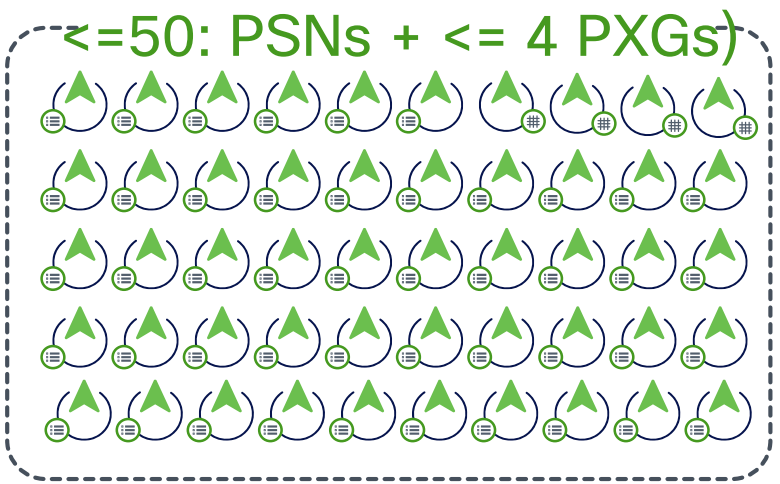
- RADIUS Accounting defines session **Start** & **Stop** events
- Sessions **Start** upon RADIUS Authorization
- Sessions **Stop** upon :
  - Disconnect
  - Session Expiration
  - Idle Timeout

© 2025 Cisco and/or its affiliates. All rights reserved.

ISE Scaling

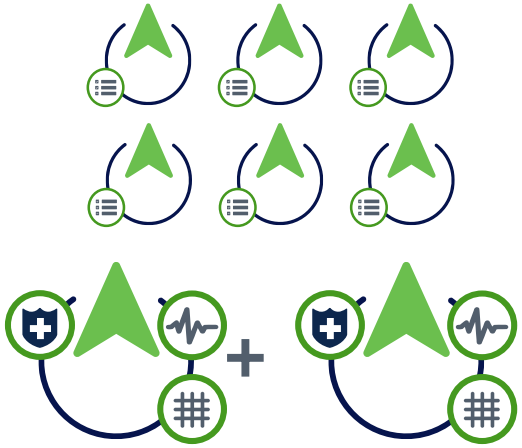
Lab and Evaluation

Standalone



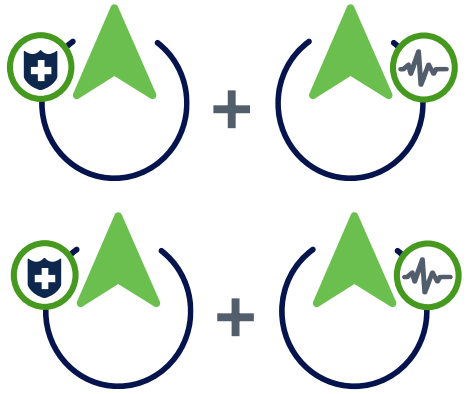
Small HA Deployment

2 x (PAN+MNT+PSN)+ Extra PSN



Medium Multi-node Deployment

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



Large Deployment

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

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Total Maximum Concurrent Active Sessions

Per whole deployment

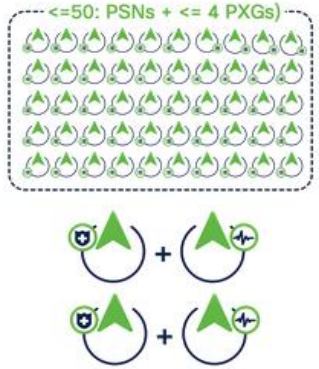
Cisco Live 2025
FOR REFERENCE
BRKSEC-2660

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

Small Deployment

Medium Deployment

Large Deployment



© 2025 Cisco and/or its affiliates. All rights reserved.

PSN Maximum Concurrent Active Sessions

Per PSN

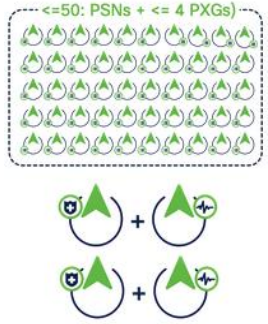
cs.co/ise-scale

PSN Type	SNS 3615	SNS 3715	SNS 3595	SNS 3655	SNS 3755	SNS 3695	SNS 3795
Concurrent active endpoints supported by a dedicated PSN (ISE node has only PSN persona)	25,000	50,000	40,000	50,000	100,000	50,000	100,000
Concurrent active endpoints supported by a shared PSN (ISE node has multiple personas)	12,500	25,000	20,000	25,000	50,000	50,000	50,000

Small Deployment

Medium Deployment

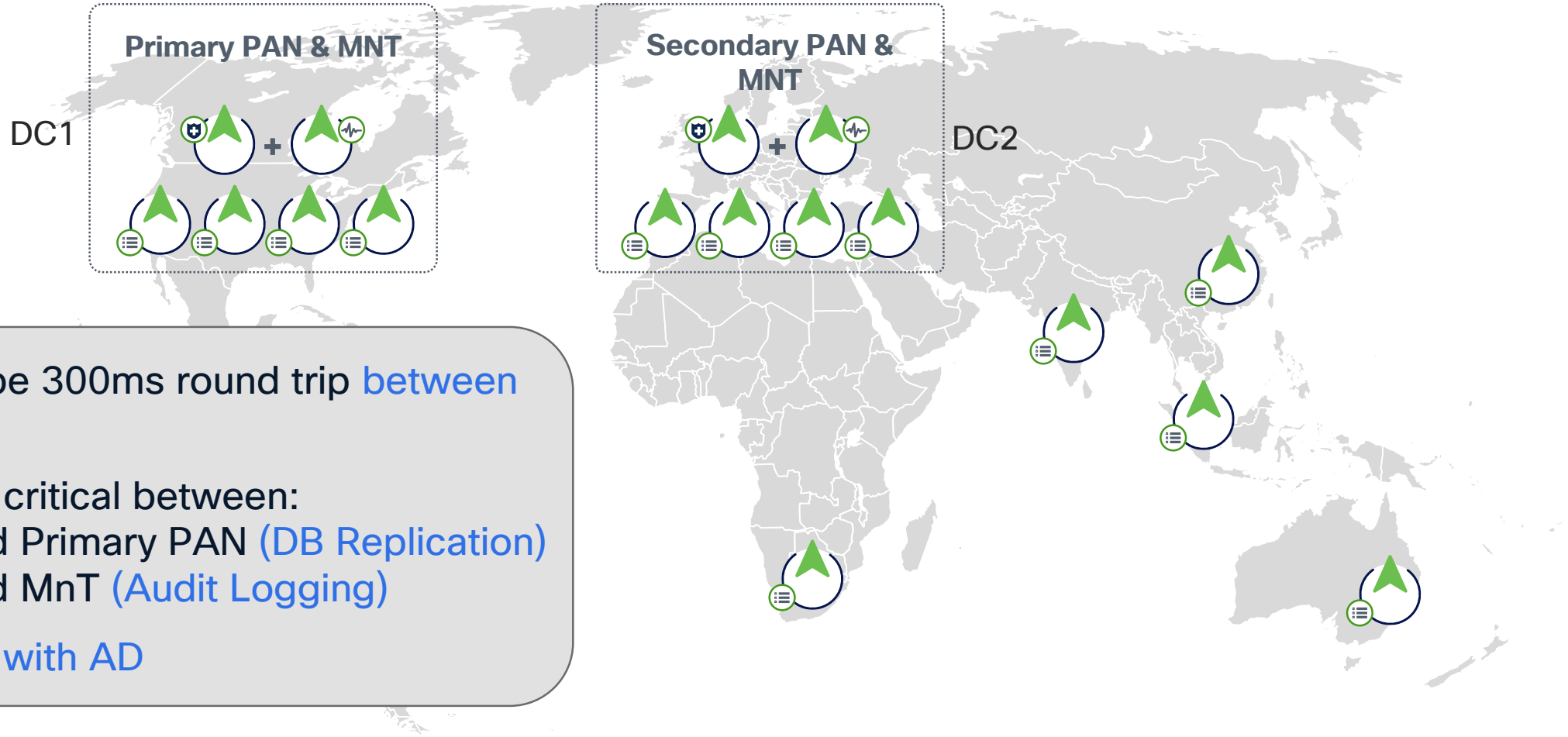
Large Deployment



© 2025 Cisco and/or its affiliates. All rights reserved.

ISE Fully Distributed Architecture

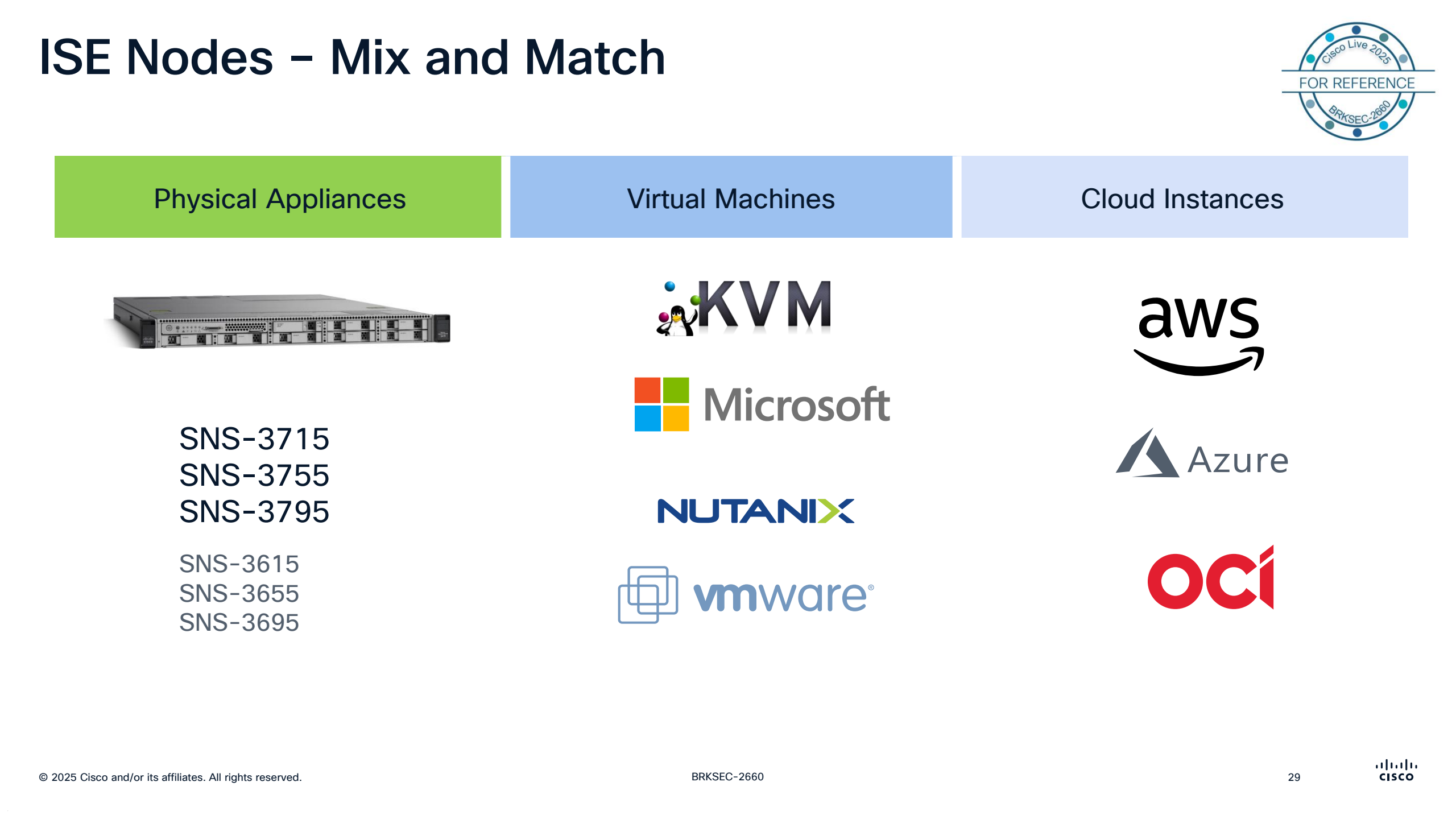
Centralize in DCs...or Distribute PSNs across Geographies



- 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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Reminders

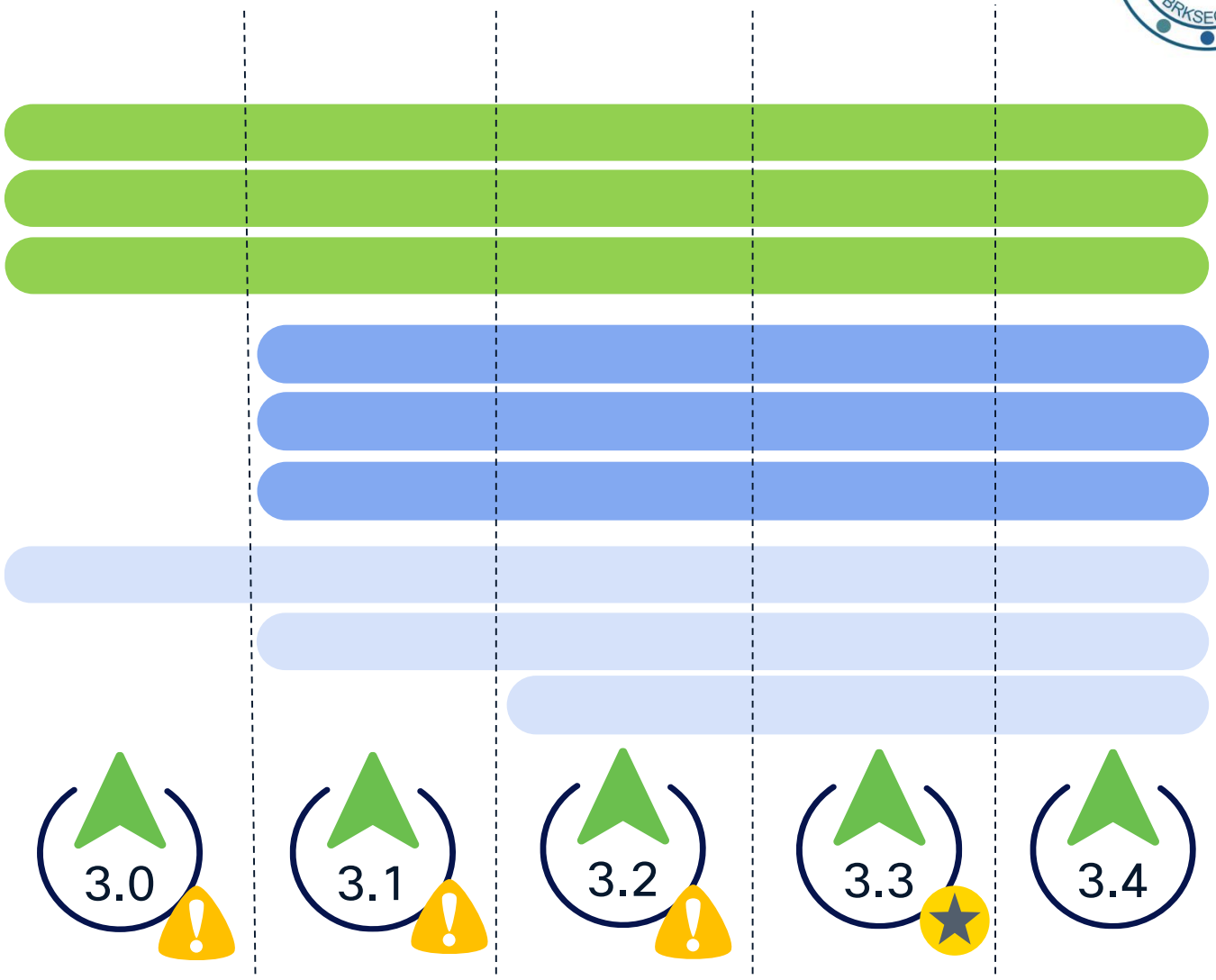
ISE platforms

SNS 3615
SNS 3655
SNS 3695

EOL

SNS 3715
SNS 3755
SNS 3795

Traditional VM
AWS
Azure & OCI



© 2025 Cisco and/or its affiliates. All rights reserved.

ISE Performance & Scale

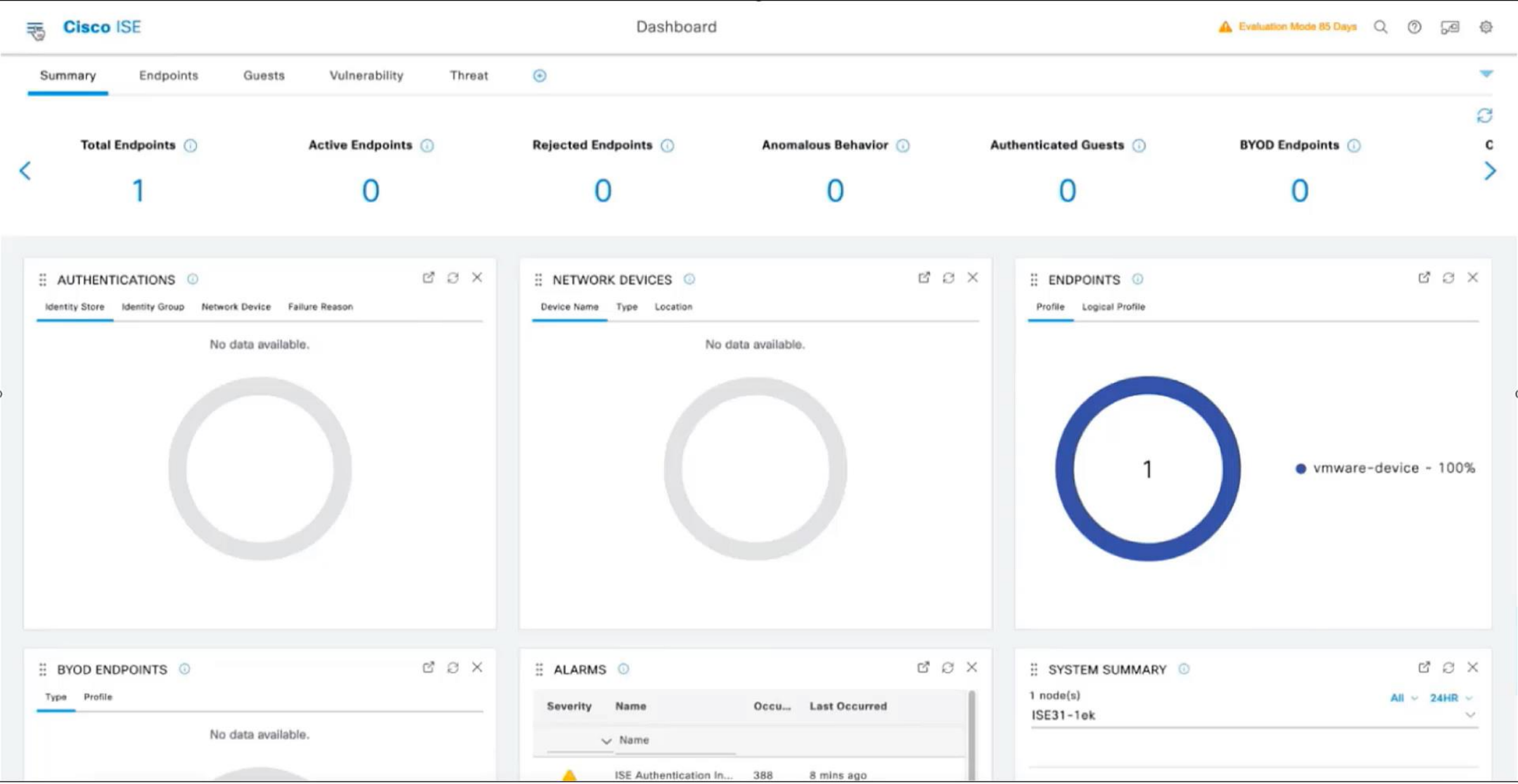
- Deployment Architectures: S / M / L
- Maximum Concurrent Active Sessions
- Deployment Scale Limits
- Protocol Performance
- Scenario Performance
- PxGrid and SXP scaling
- Network Device maximum numbers

cs.co/ise-scale

Go to page to check for current numbers

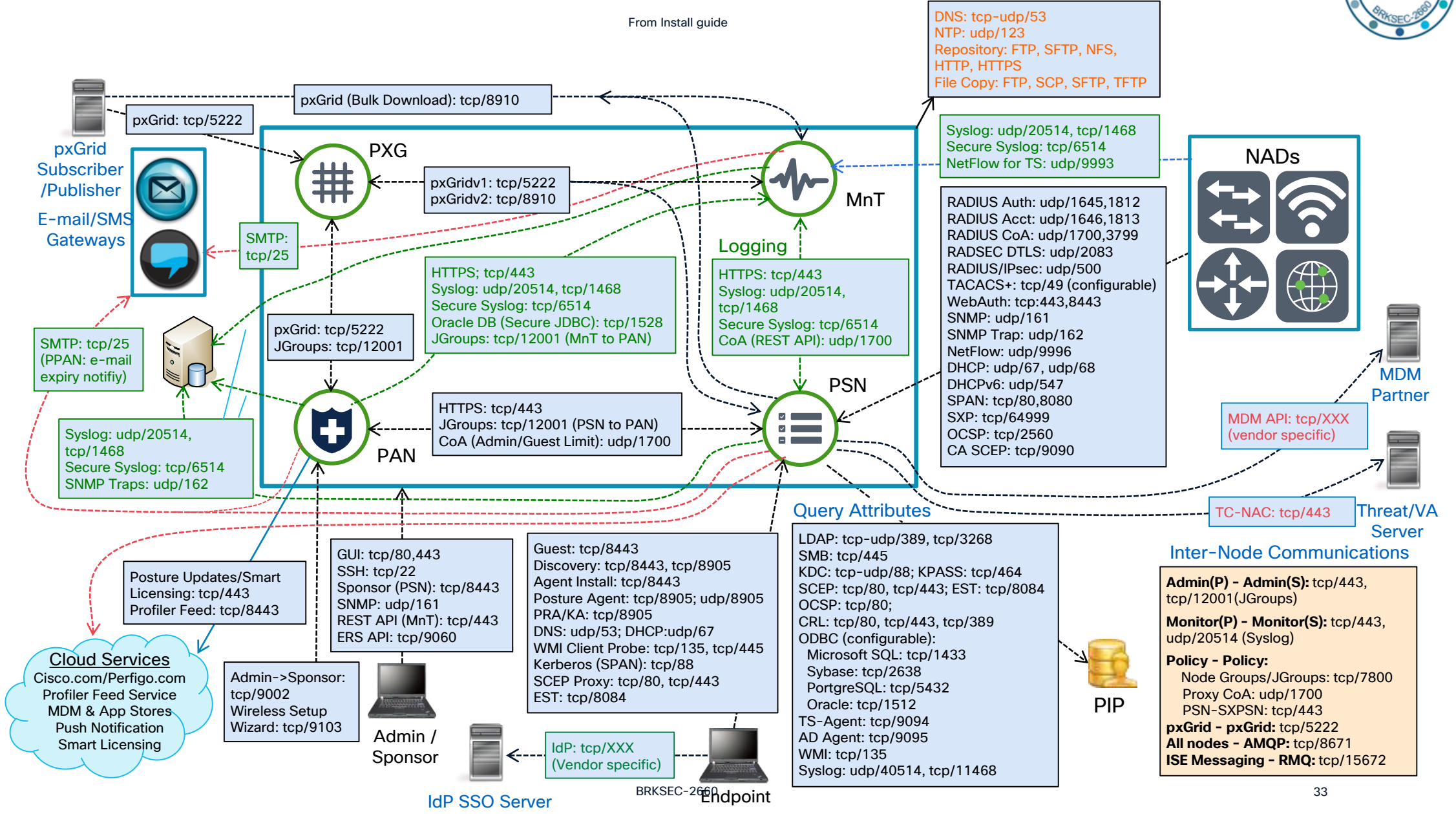
Platform	Concurrent active endpoints supported by a dedicated PSN (Cisco ISE node has only PSN persona)	Concurrent active endpoints supported by a shared PSN (Cisco ISE node has multiple personas)
Extra Small (VM only)	12.000	unsupported
SNS 3615	25,000	12.500
SNS 3715	50,000	25.000
SNS 3655	50,000	25.000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

© 2025 Cisco and/or its affiliates. All rights reserved.



© 2025 Cisco and/or its affiliates. All rights reserved.

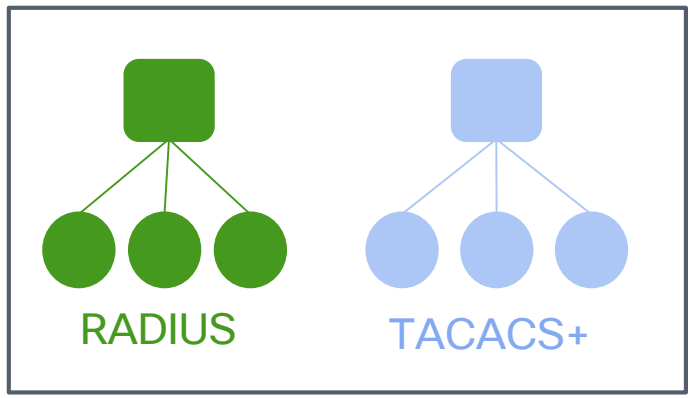
ISE Inter-Node Communications



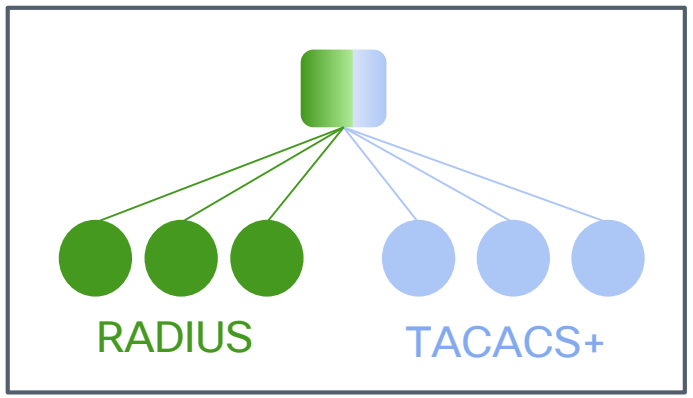
TACACS+ Deployment Models

Separating RADIUS & TACACS+ ISE Cubes?

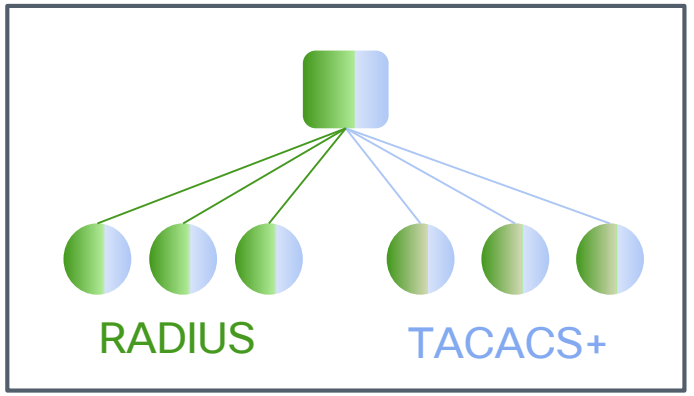
There are three different options:



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?
- How much Log Retention do you need?

© 2025 Cisco and/or its affiliates. All rights reserved.

ISE Device Administration Prescriptive Deployment Guide

cs.co/ise-tacacs

- Define
  - Components & Considerations
- Design
  - Admin Model, Scale, Logs
- Deploy
  - ISE Configuration
  - Device Administration Policy Sets
  - Network Device Configuration
- Operate
  - Settings, Logging, Reporting

Cisco ISE Device Administration Prescriptive Deployment Guide

kthiruve Cisco Employee

on 2018-11-02 07:54 PM - edited on 2023-09-26 11:54 AM by thomas

Deploying Cisco ISE for Device Administration

This deployment guide is intended to provide the relevant design, deployment, operational guidance and best practices to run Cisco Identity Services Engine (ISE) for device administration on Cisco devices and a sample non-Cisco devices.

Author: Krishnan Thiruvengadam

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

Table of Contents

© 2025 Cisco and/or its affiliates. All rights reserved.

Certificates

ISE Certificates

System Certificates

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

Trusted Certificates

List of CAs

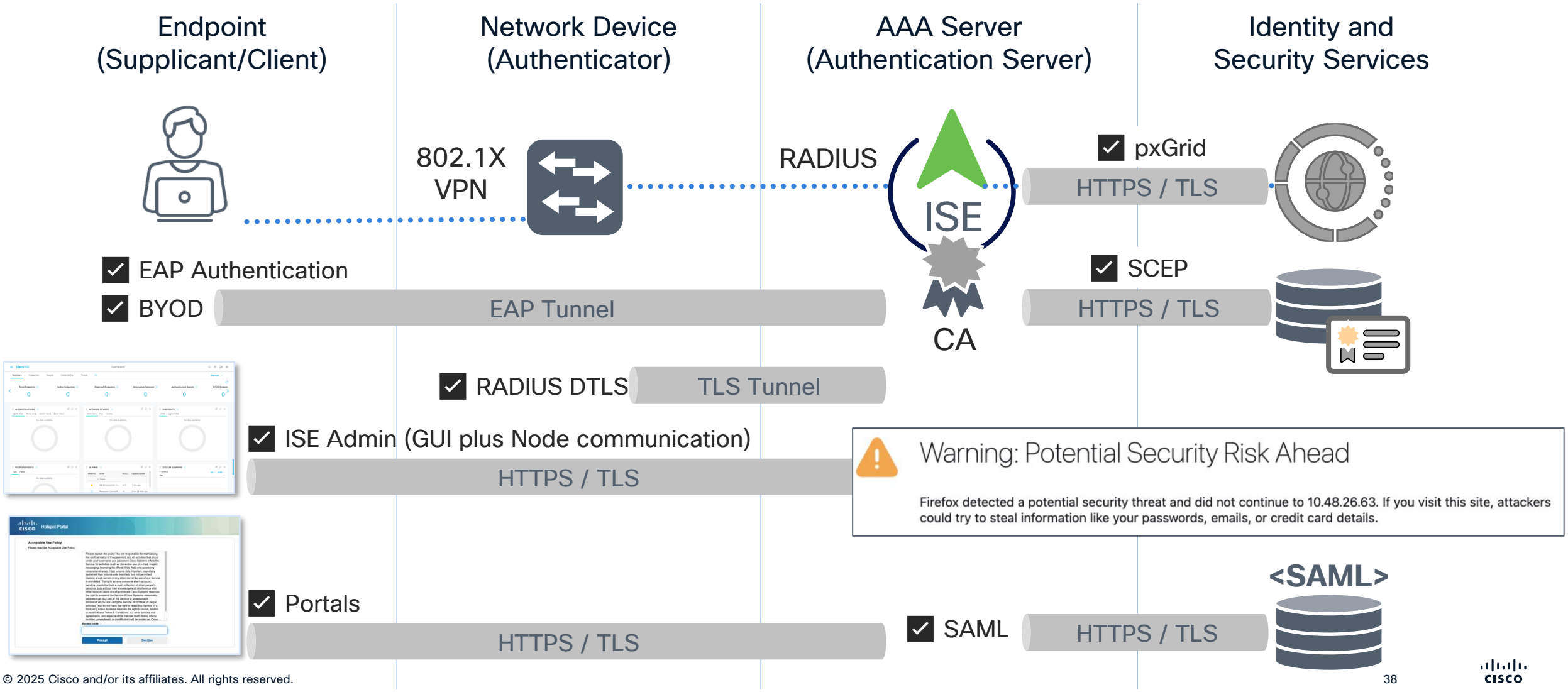
- Trusts for the identities of entities interacting with ISE
- Replicated to all the nodes in deployment

ISE Issued Certificates

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

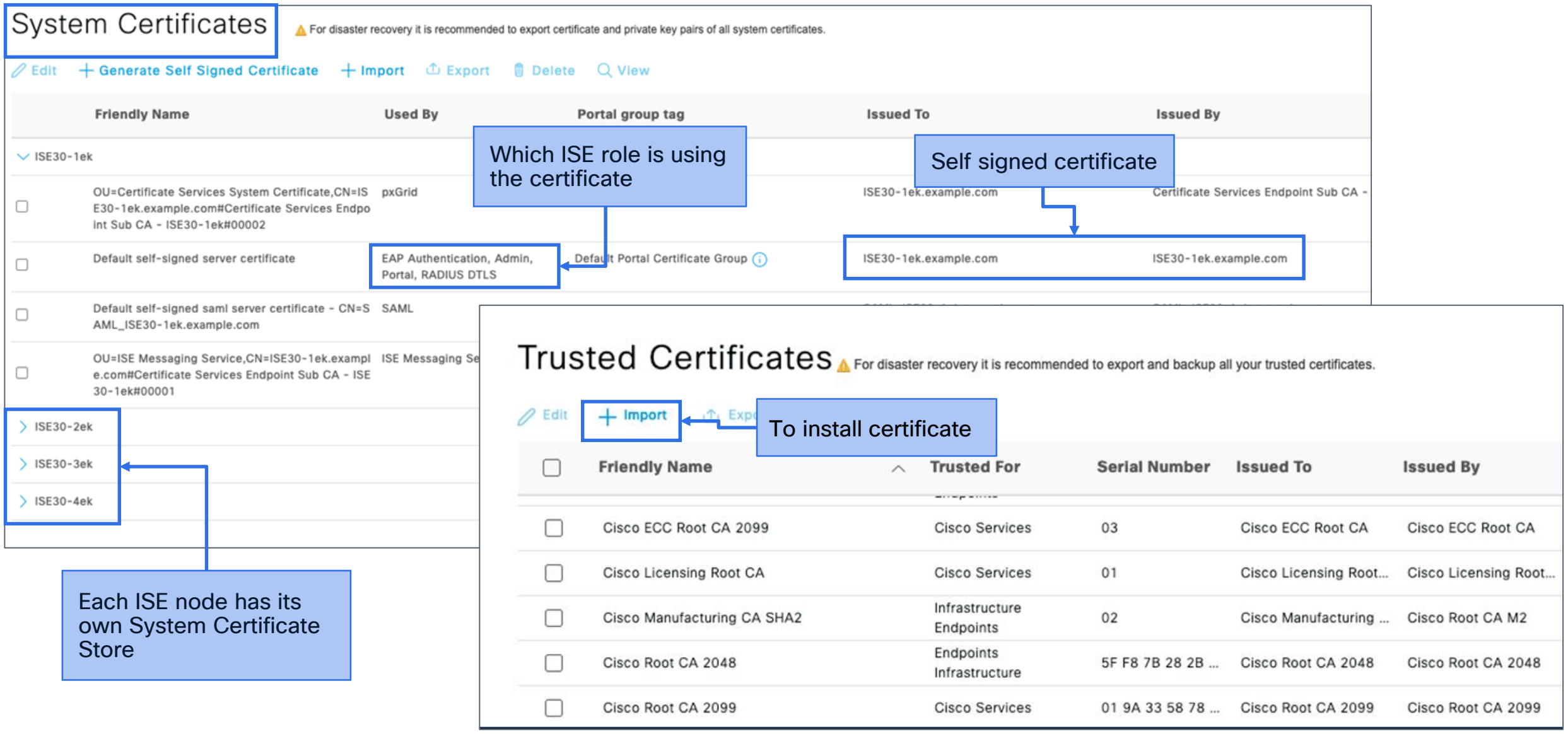
© 2025 Cisco and/or its affiliates. All rights reserved.

Different ISE System certificates

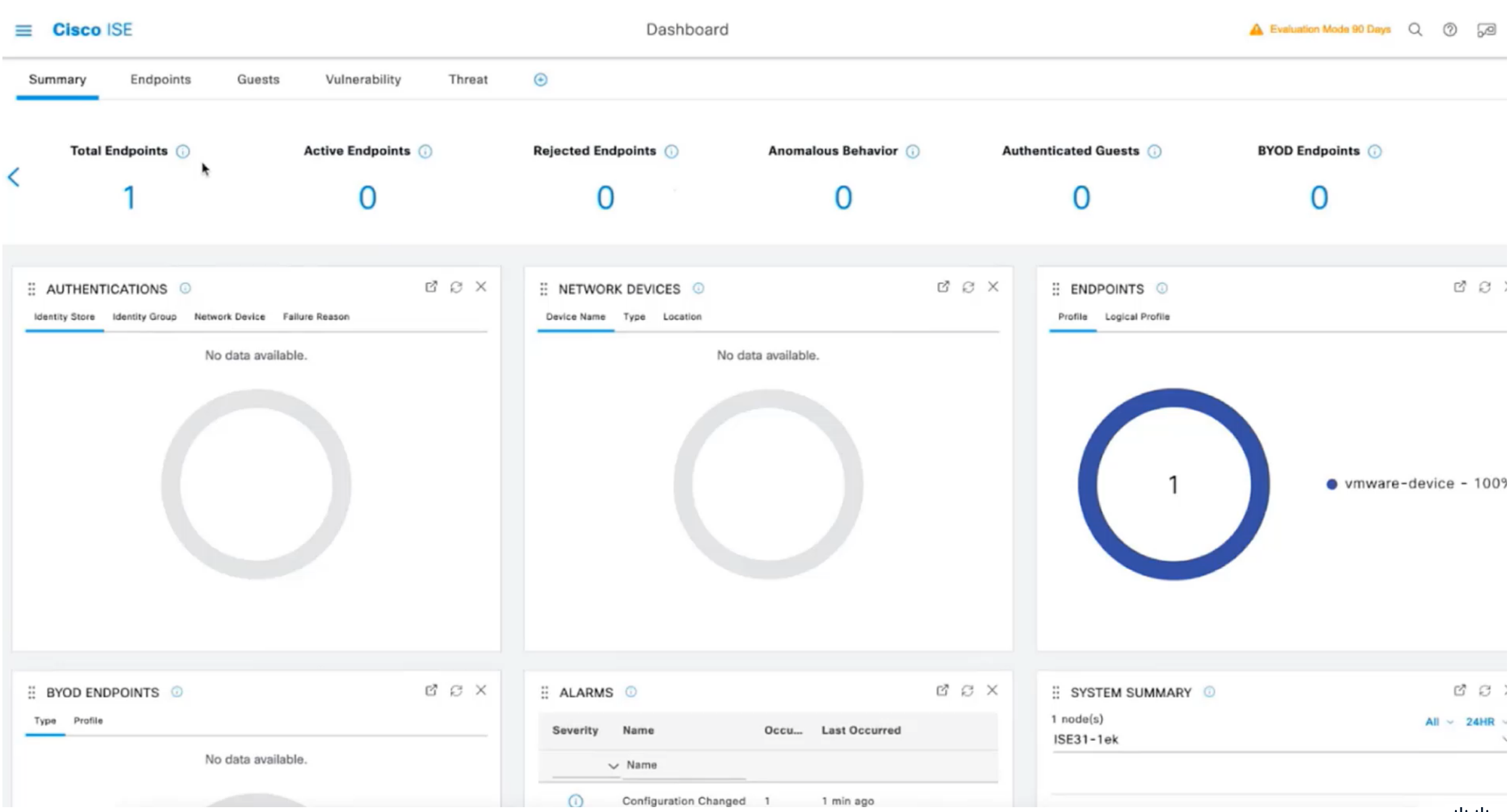


© 2025 Cisco and/or its affiliates. All rights reserved.

Systems and Trusted Certificates



© 2025 Cisco and/or its affiliates. All rights reserved.



© 2025 Cisco and/or its affiliates. All rights reserved.

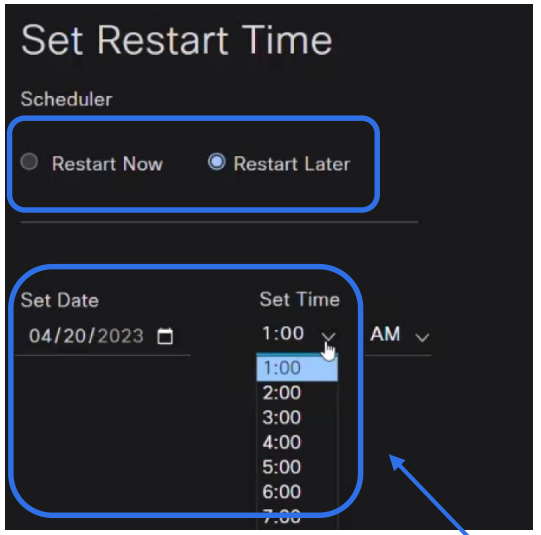
Controlled Application Restart

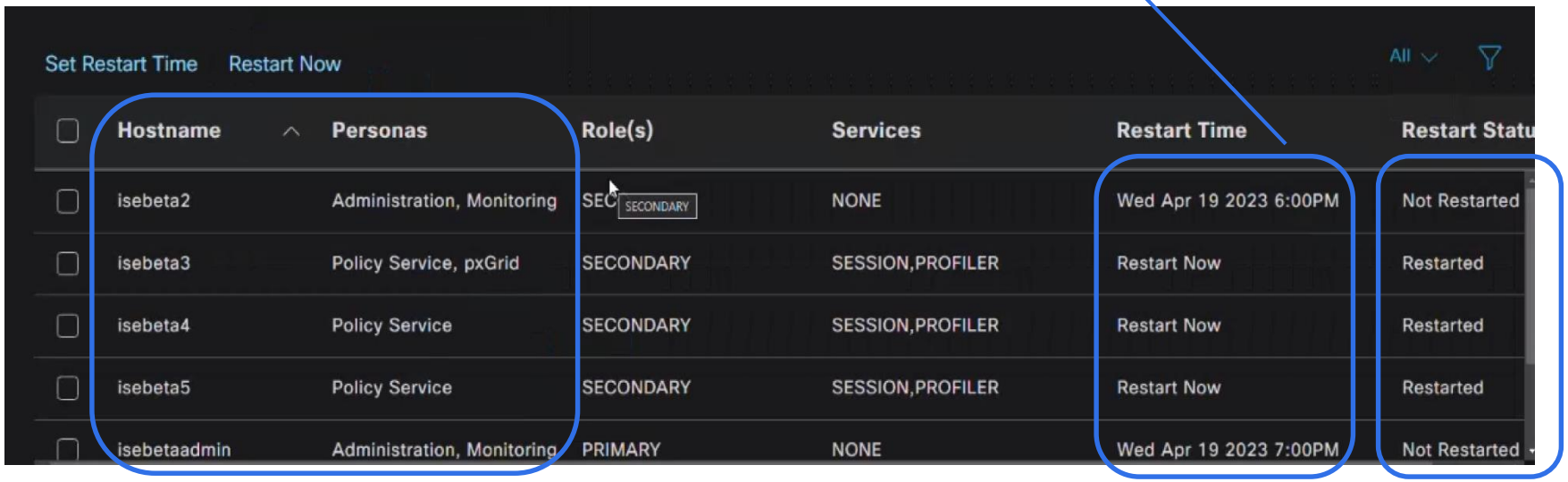
ISE 3.3.0

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





© 2025 Cisco and/or its affiliates. All rights reserved.

Improved Restart Time

ISE 3.4.0

~20 min in ISE 3.2

~16 min in ISE 3.3

~5.5 min in ISE 3.4

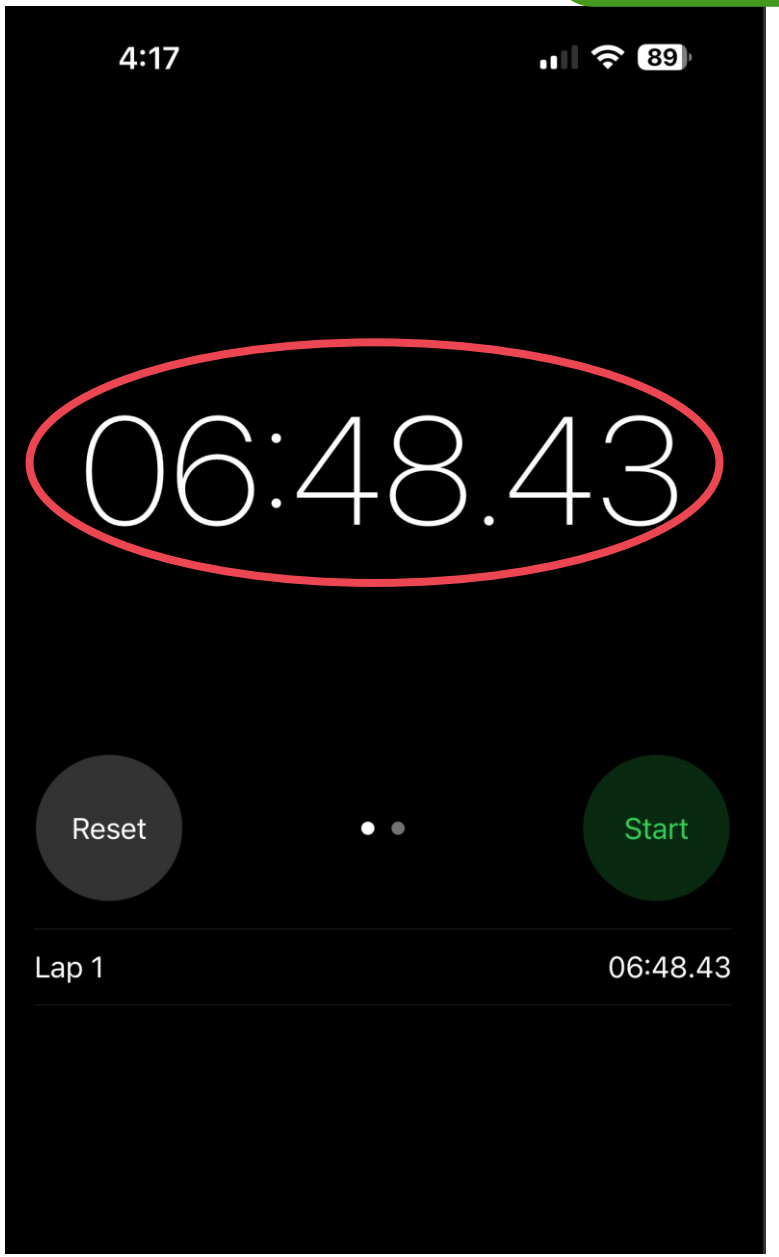
Using the commands

application stop ise
reload

~6.5 min in ISE 3.4

Using the commands

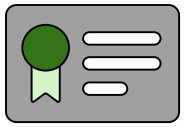
reload



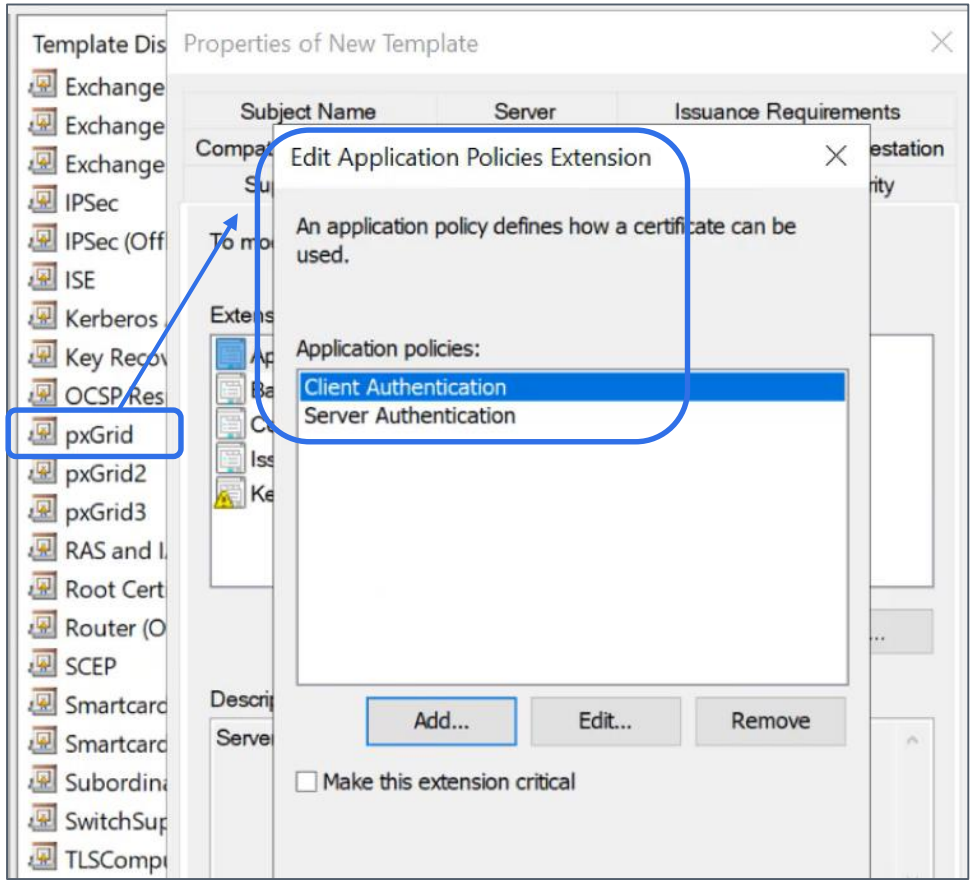
© 2025 Cisco and/or its affiliates. All rights reserved.

PxGrid Certificate

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



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



© 2025 Cisco and/or its affiliates. All rights reserved.

Network Devices

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
CGS 2520	IOS 15.2(2)E3	√	√	√	√	X	√	√	√

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Summary Endpoints Guests Vulnerability Threat Manage

Total Endpoints 165

Active Endpoints 5

Rejected Endpoints 0

Anomalous Behavior 0

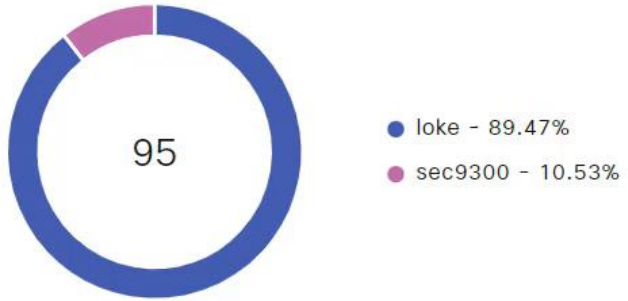
Authenticat (

AUTHENTICATIONS

Identity Store | Identity Group | Network Device | Failure Reason

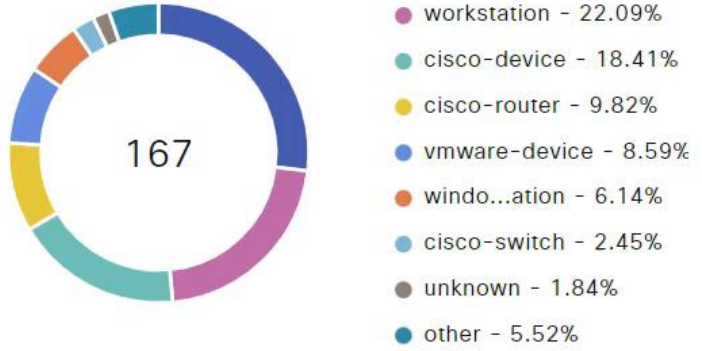
NETWORK DEVICES

Device Name | Type | Location

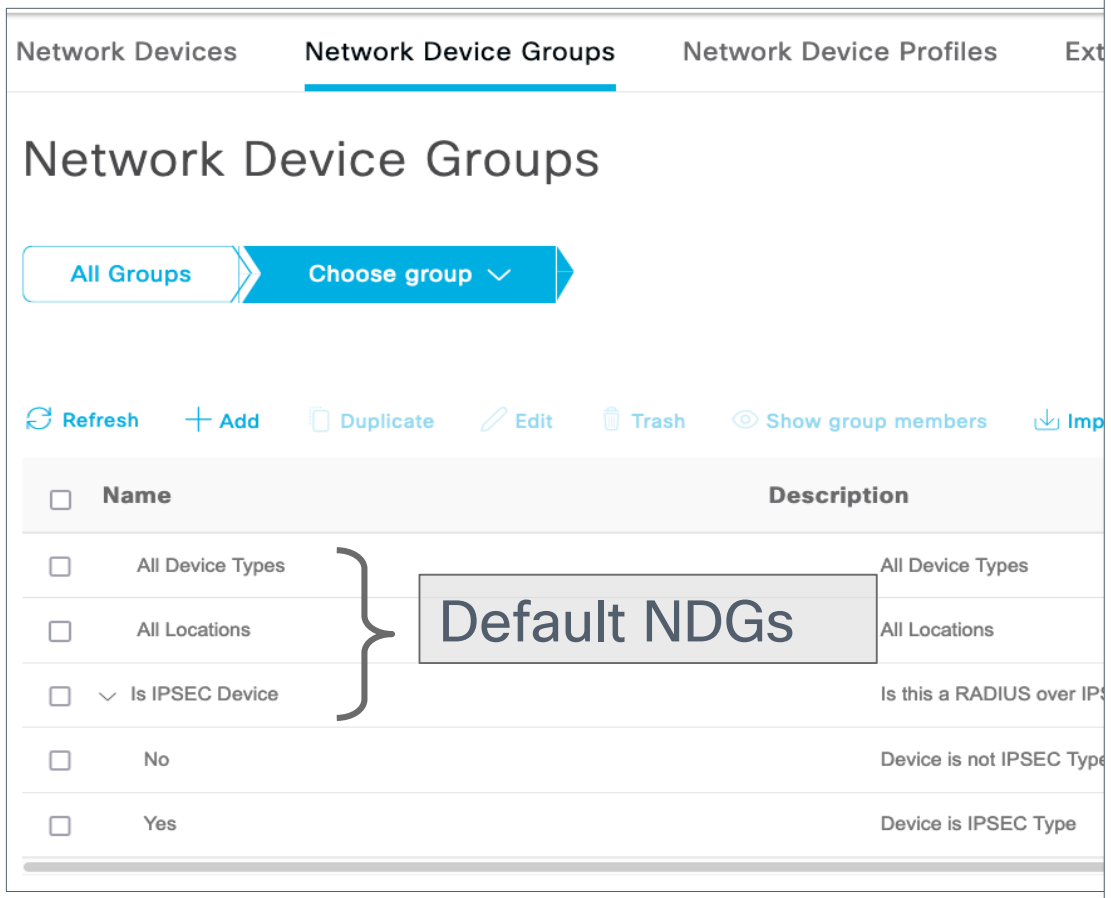


ENDPOINTS

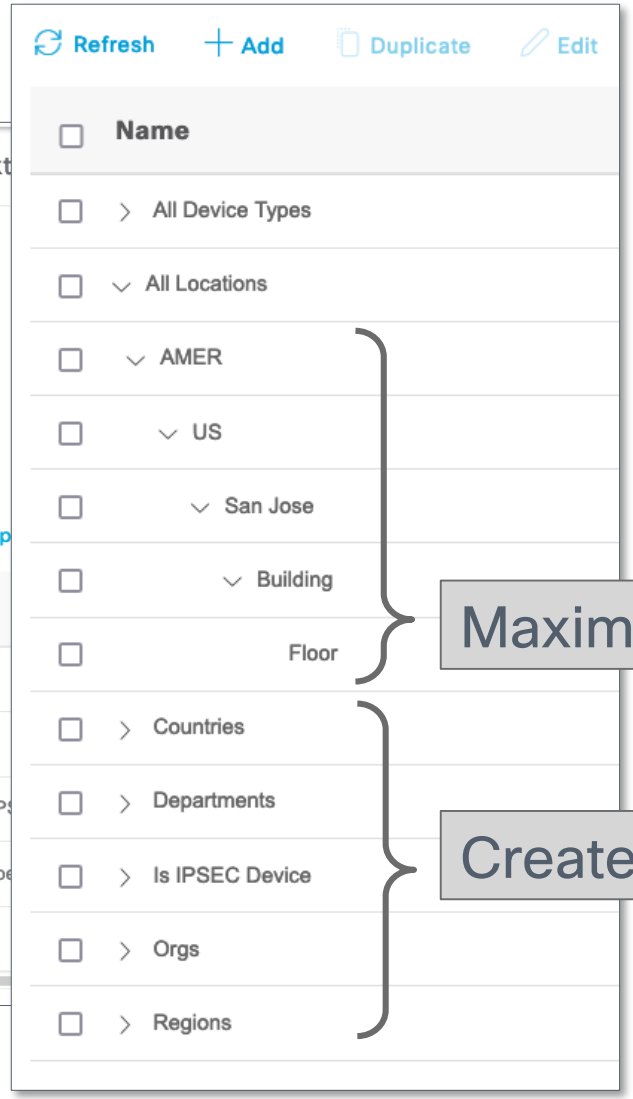
Profile | Logical Profile



Default Network Device Groups (NDGs)

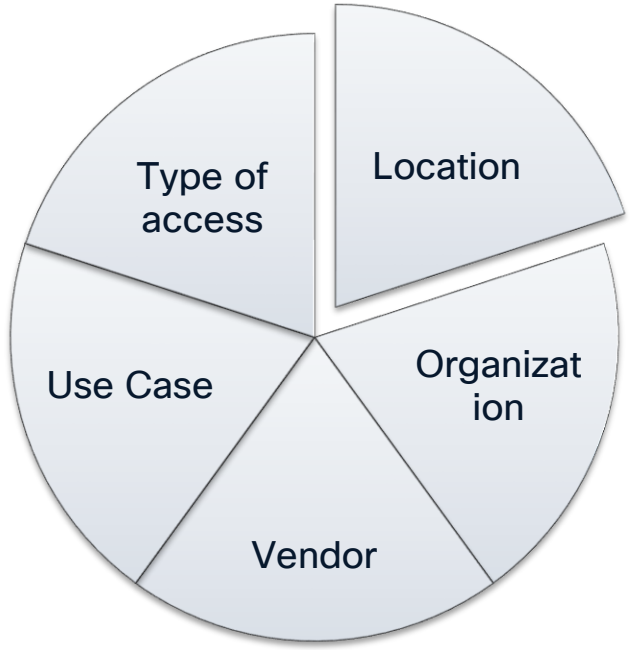


Default NDGs



Maximum 6 Levels

Create Your Own Root NDGs



© 2025 Cisco and/or its affiliates. All rights reserved.

Additional Tips

- Always Test before implementing!
- Standardize! Standardize! Standardize!
  - IOS versions
  - AAA configuration
  - Wireless configuration
  - Profiling configuration
- Document everything!

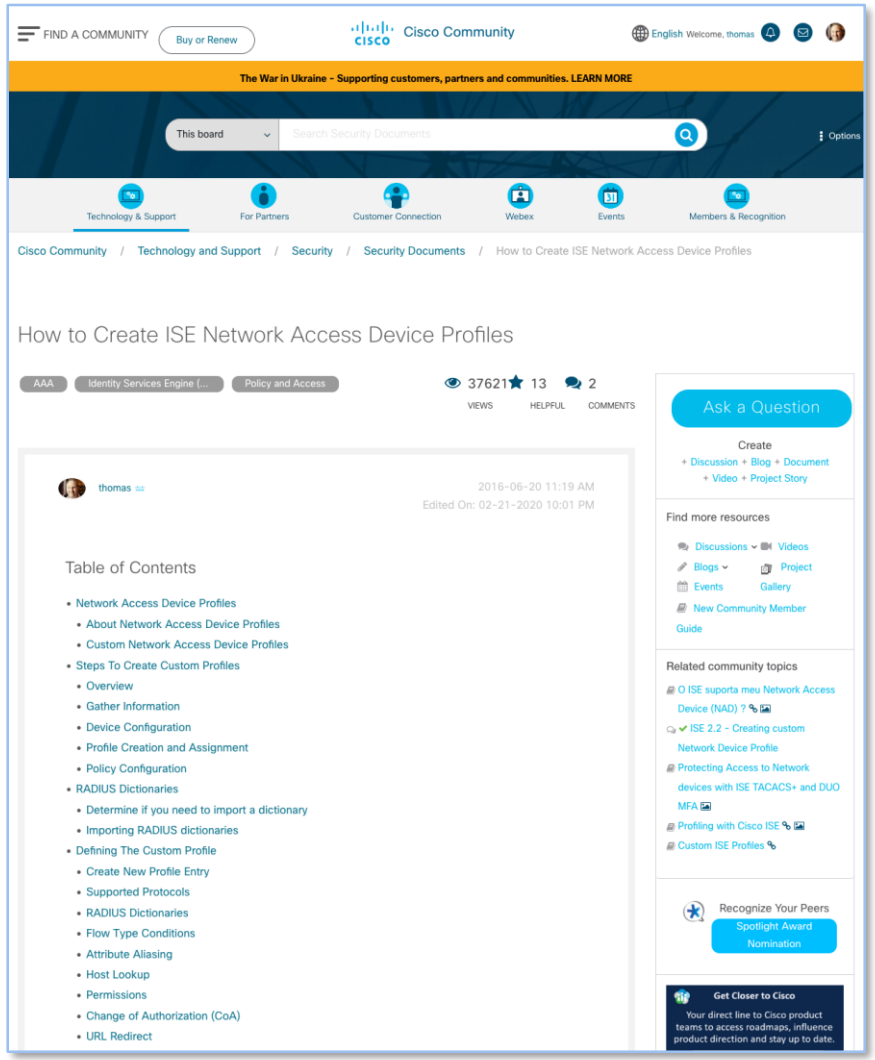
© 2025 Cisco and/or its affiliates. All rights reserved.

Create ISE Network Access Device Profiles

Cisco Live 2025
FOR REFERENCE
BRKSEC-2660

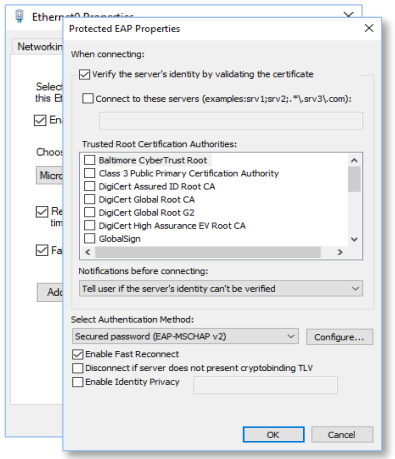
- Network Access Device Profiles
  - About Network Access Device Profiles
  - Custom Network Access Device Profiles
- Steps To Create Custom Profiles
  - Overview
  - Gather Information
  - Device Configuration
  - Profile Creation and Assignment
  - Policy Configuration
- RADIUS Dictionaries
  - Determine if you need to import a dictionary
  - Importing RADIUS dictionaries
- Defining The Custom Profile
  - Create New Profile Entry
  - Supported Protocols
  - RADIUS Dictionaries
  - Flow Type Conditions
  - Attribute Aliasing
  - Host Lookup
  - Permissions

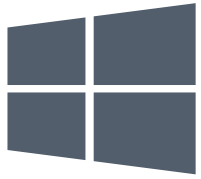
how-to-create-ise-network-access-device-profiles

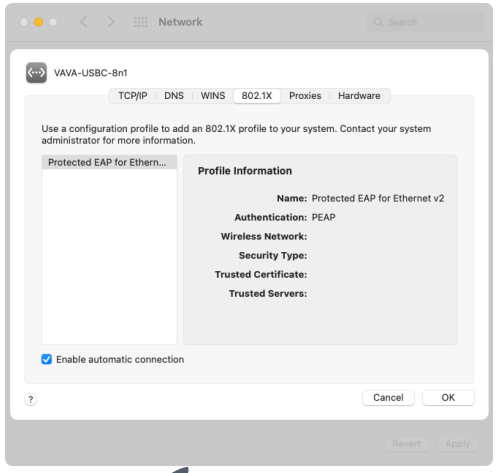


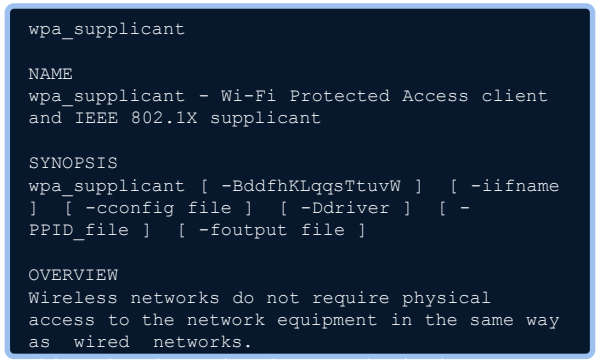
Supplicants

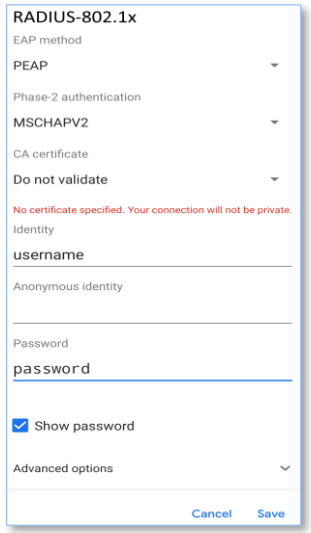
Endpoints: Native 802.1X Supplicants











- Now you can do TEAP natively in Windows for Chaining (Windows 10 build 2004 and ISE 2.7 Patch 2)

- Use Group Policies in Windows for:
  - Quick Supplicant configuration for the user
  - Certificate pushing (User and Root)
  - Pre-configure SSID

© 2025 Cisco and/or its affiliates. All rights reserved.

Profiling

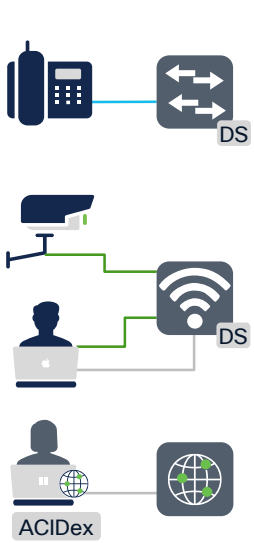
Endpoints: Everything Else

© 2025 Cisco and/or its affiliates. All rights reserved.

Endpoint Profiling

The profiling service dynamically classifies devices connected to your network

Endpoints send interesting data, that reveal their device type



ISE Data Collection Methods for Device Profiling

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

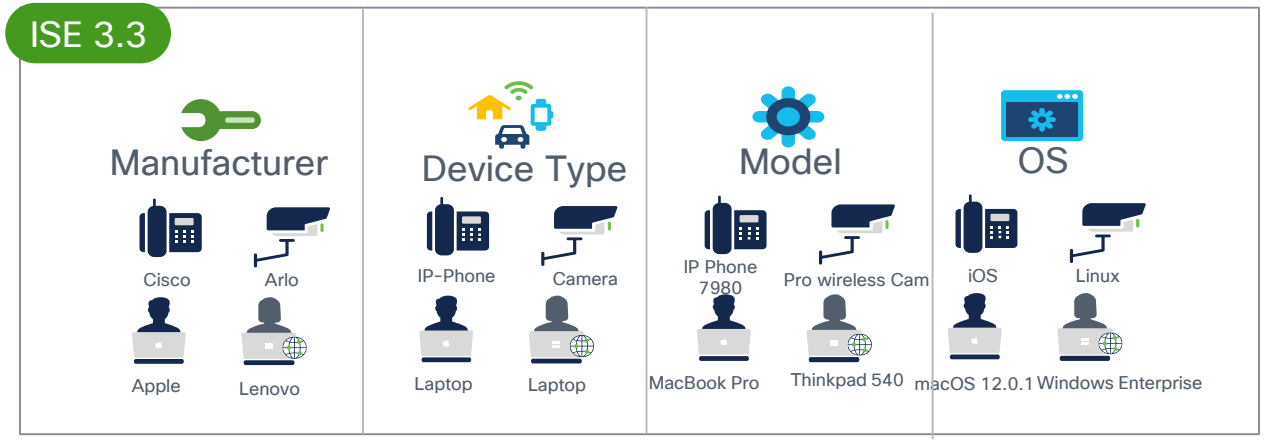
Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

AnyConnect: ACIDex

pxGrid context-in: (DNAC Endpoint Analytics, CyberVision for industrial)

WIFI Edge Analytics: Firmware_version, HW_Model, Manufacturer, Model, OS_Version, Vendor (Samsung, Apple and Intel devices)

ISE 3.3



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

© 2025 Cisco and/or its affiliates. All rights reserved.

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**

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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**

© 2025 Cisco and/or its affiliates. All rights reserved.

Effect of HTTP Probe

 Windows 10 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**

© 2025 Cisco and/or its affiliates. All rights reserved.

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

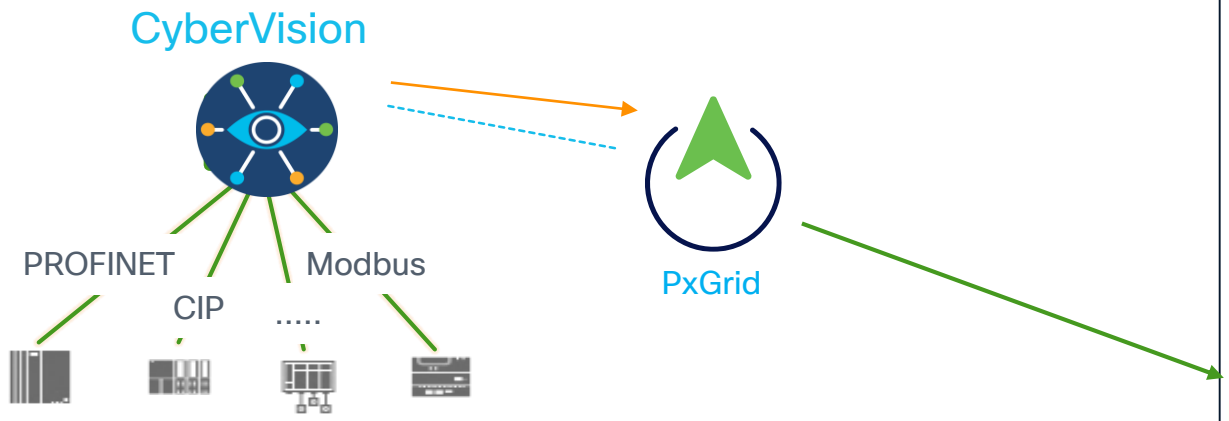
© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

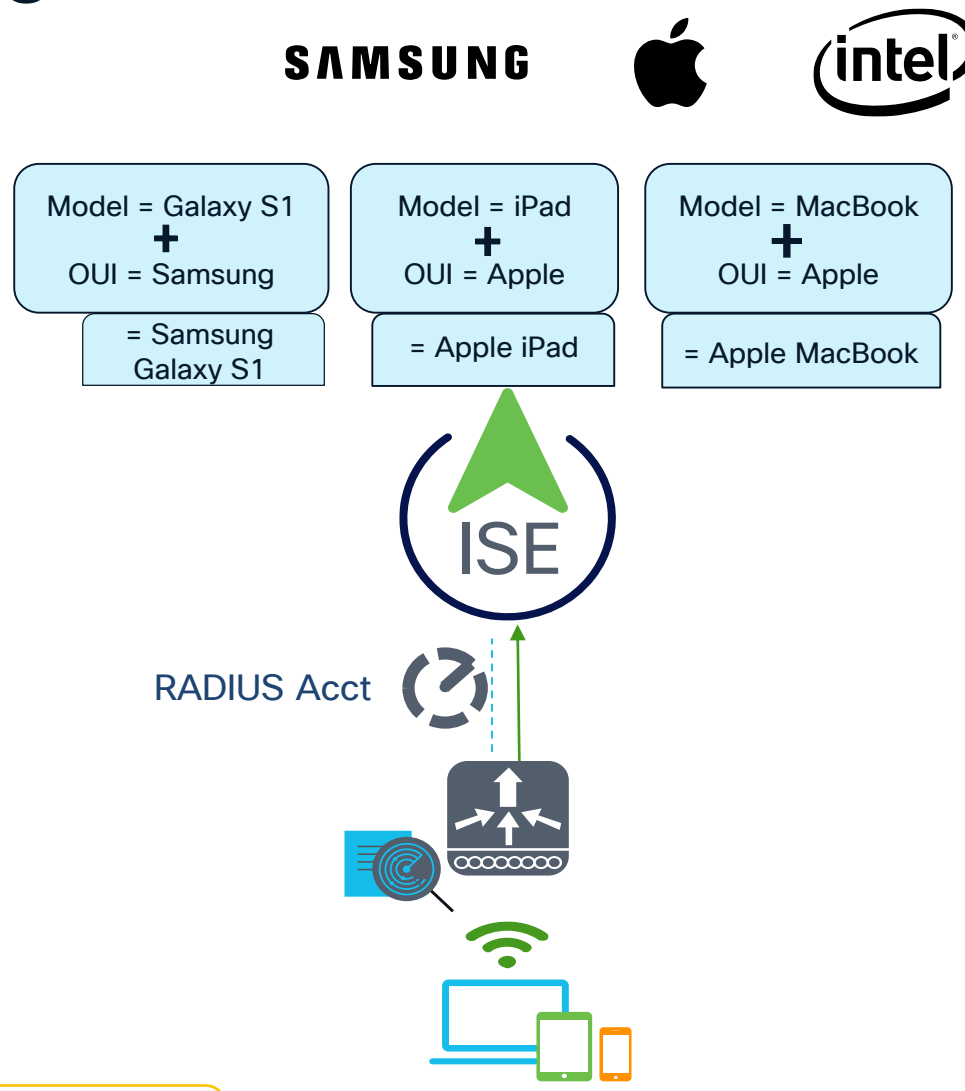
© 2025 Cisco and/or its affiliates. All rights reserved.

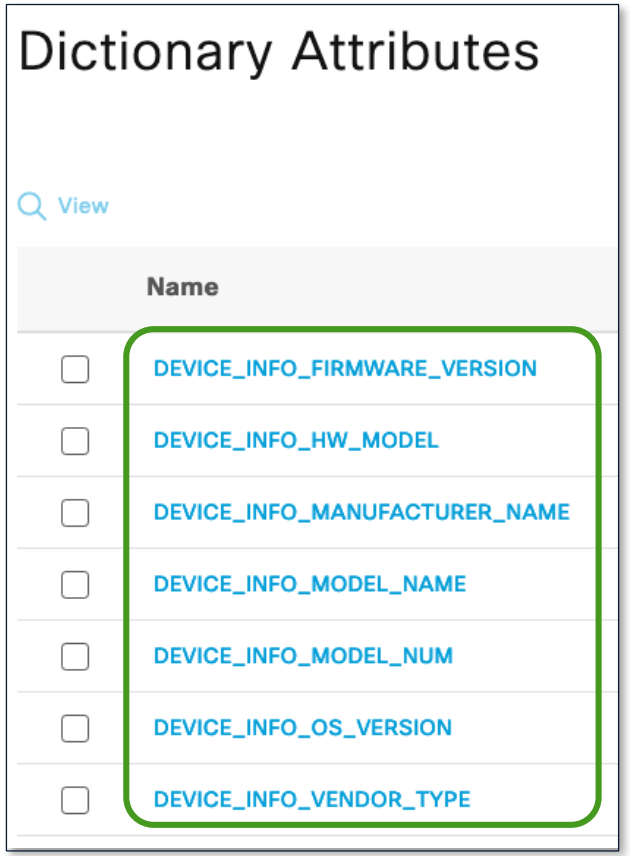
Wi-Fi Edge Analytics

ISE 3.3

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.

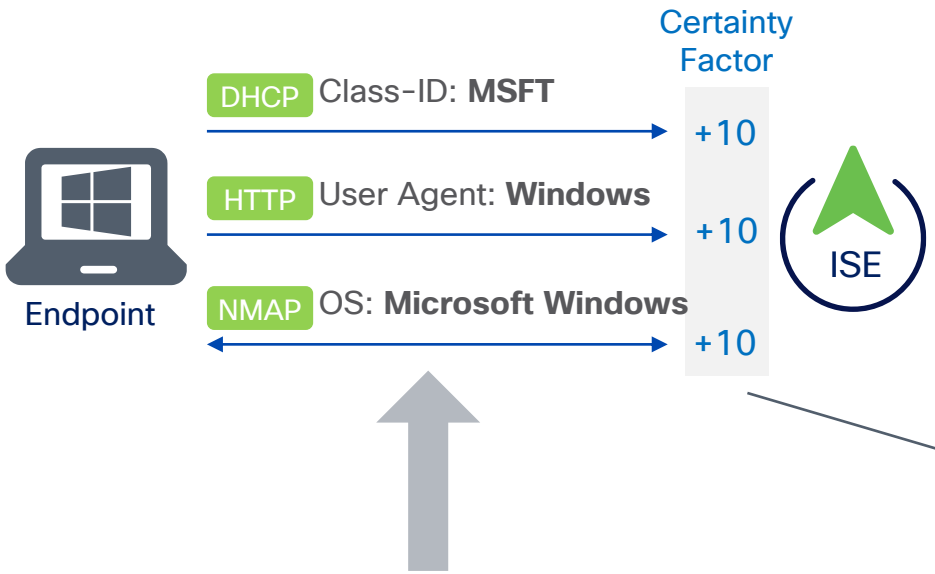




⚠ Disable the ISE Profiling Endpoint Attribute Filter to use WiFi Device Analytics attributes in policies

© 2025 Cisco and/or its affiliates. All rights reserved.

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

Profiler Policy List > Microsoft-Workstation

Profiler Policy

* Name: Microsoft-Workstation

Description: Generic policy for Microsoft workstation

Policy Enabled

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: Yes, create matching Identity Group / No, use existing Identity Group hierarchy

Parent Policy: Workstation

* Associated CoA Type: Global Settings

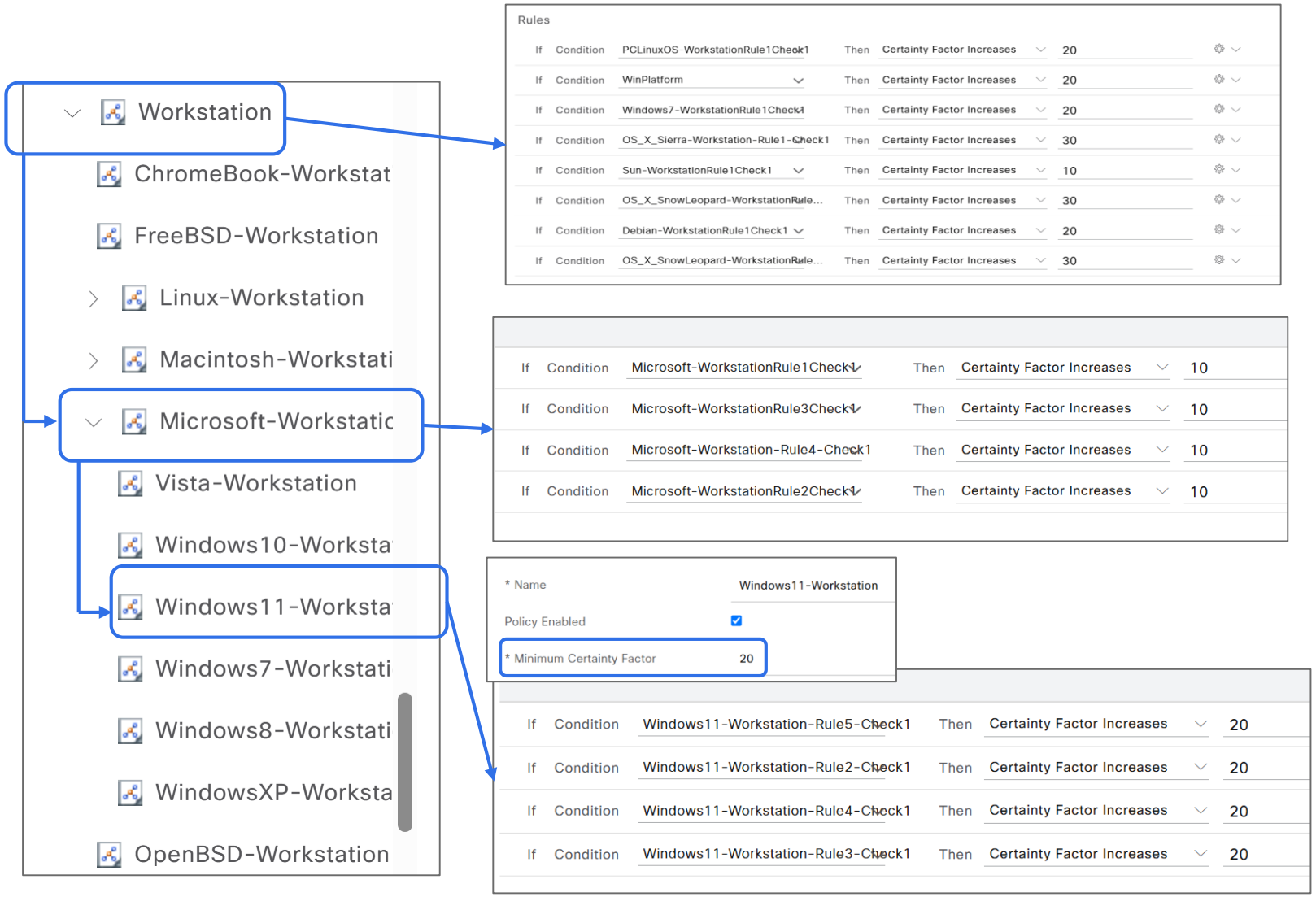
System Type: Cisco Provided

Rules

If	Condition	Microsoft-WorkstationRule2Check1	Then	Certainty Factor Increases	10
If	Condition	Microsoft-Workstation-Rule4-Check1	Then	Certainty Factor Increases	10
If	Condition	Microsoft-WorkstationRule3Check1	Then	Certainty Factor Increases	10
If	Condition	Microsoft-WorkstationRule1Check1	Then	Certainty Factor Increases	10

© 2025 Cisco and/or its affiliates. All rights reserved.

Profile hierarchy



For one profile to be matched, the endpoint has to match also the profiles of all the parents in the tree!

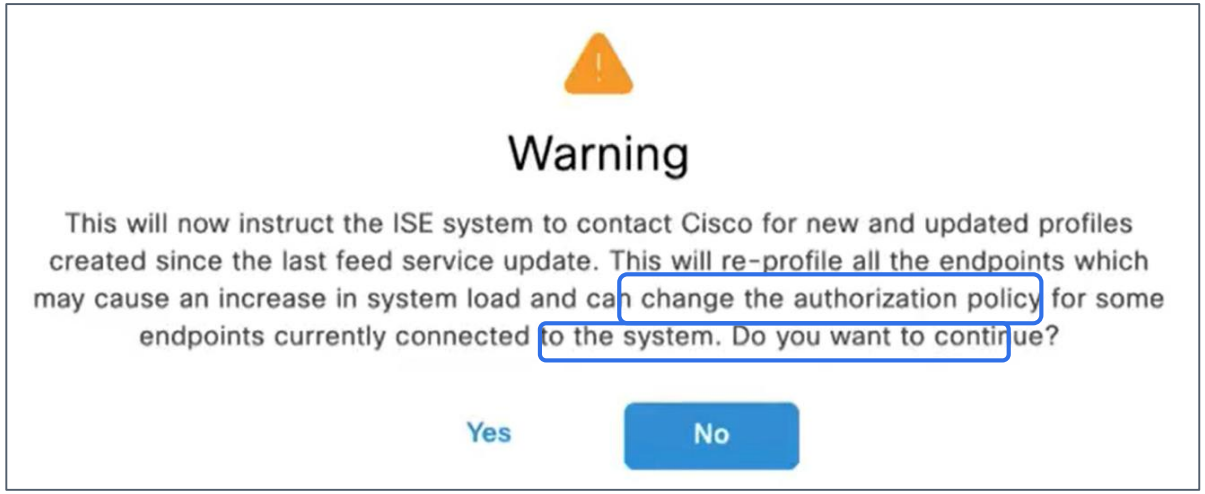
Windows 11 has to match the conditions for ALL the following profiles:

1. Workstation
2. Microsoft Workstations
3. Windows 11-Workstation

© 2025 Cisco and/or its affiliates. All rights reserved.

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
- Test and create correct Policies before implementing



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco AI Machine Learning Profiling

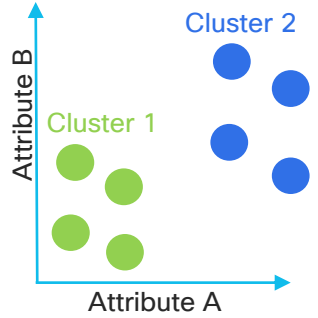
ISE 3.3

ISE

Unknown endpoints

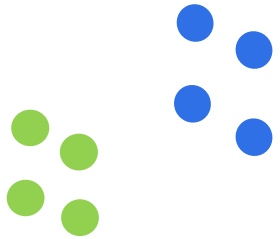
Clustering

ML groups different endpoints into clusters based on attribute data



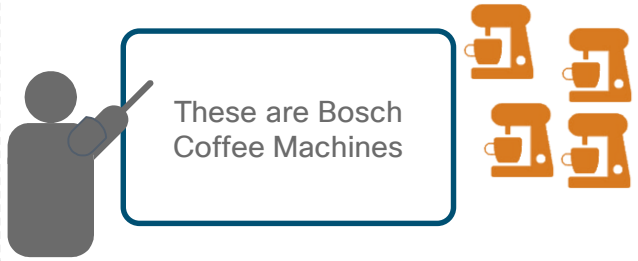
Rule Creation

Creates a rule that uniquely groups together endpoint clusters



Endpoint Labeling

System recommends labels or customer can teach ML what to label the endpoints in a cluster



Active Learning

ML learns new labels and validates existing labels

New Labels

= Bosch Coffee Machine

= Arlo Pro Wireless Cam

Label Validation

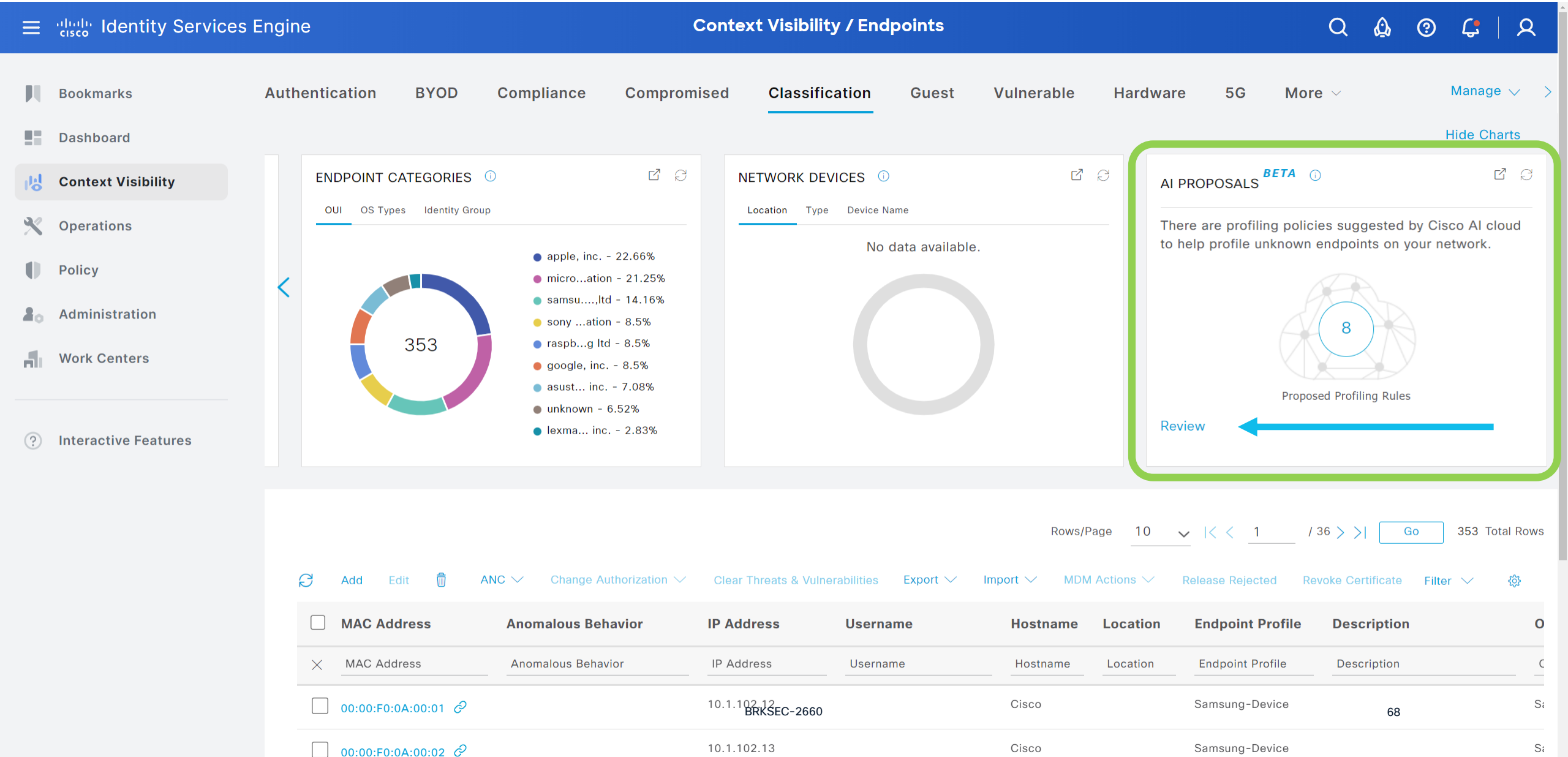
= Apple Watch

= Cisco IP Phone 7980

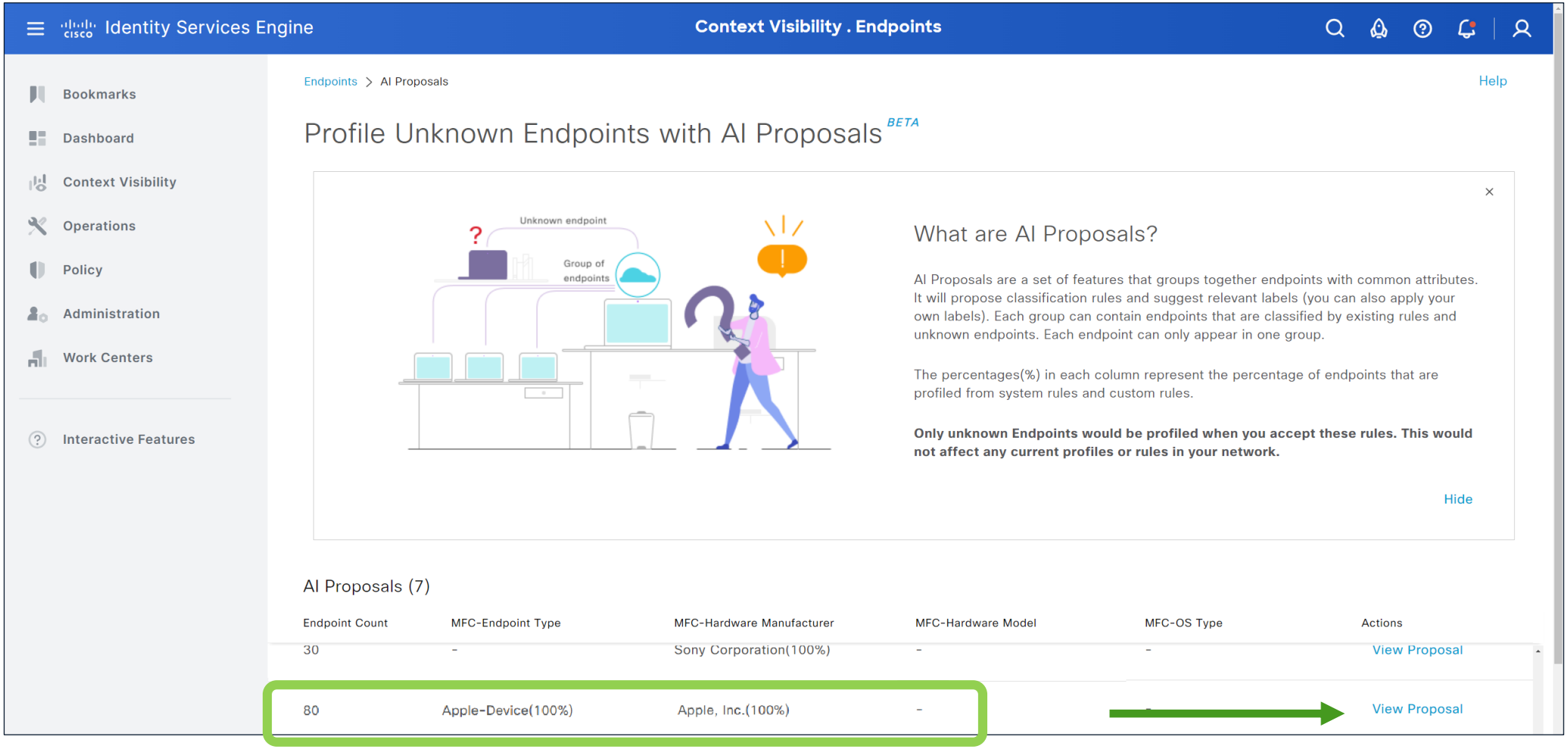
= Step done in the ML Cloud

© 2025 Cisco and/or its affiliates. All rights reserved.

Review the AI Proposals

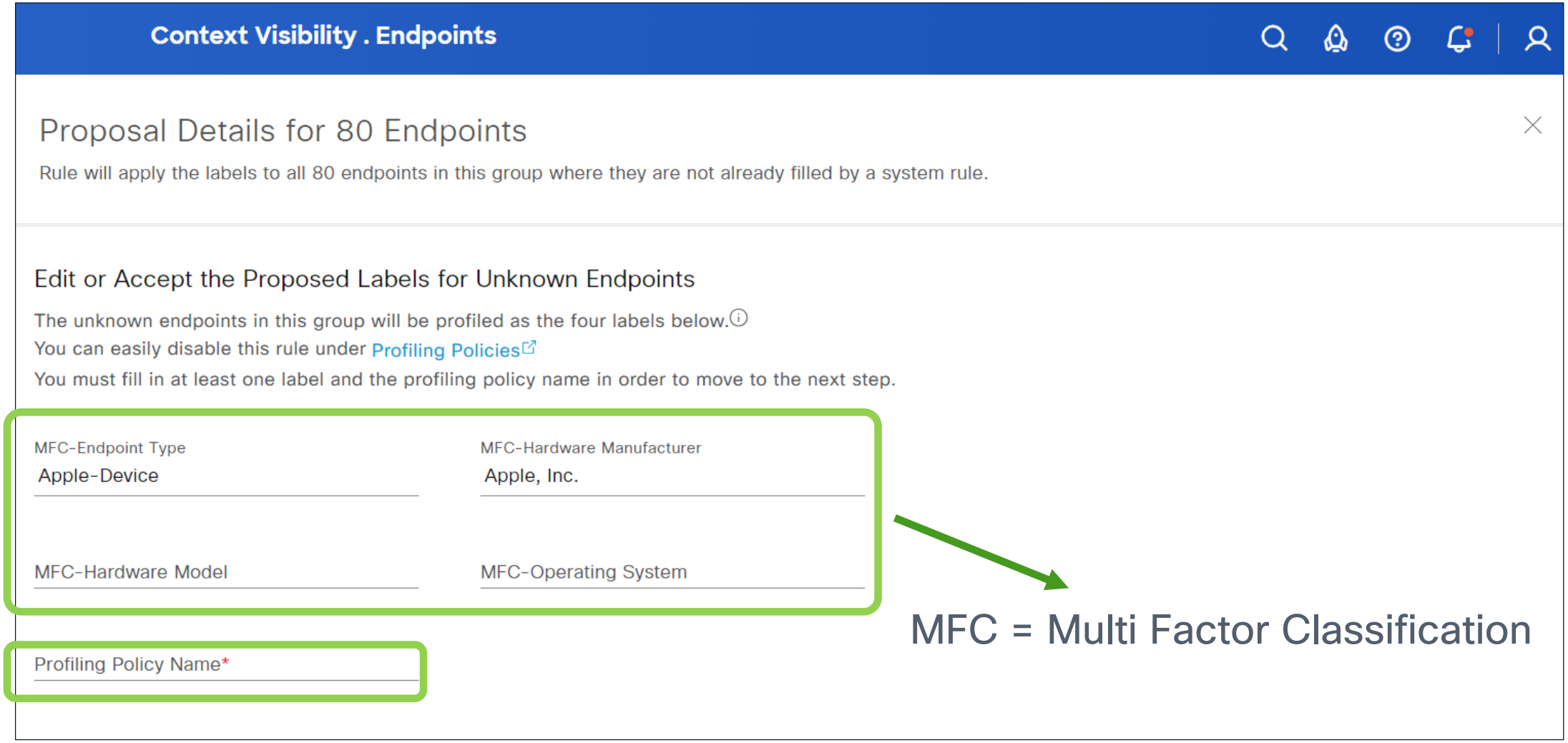


Choose the Proposal to View



© 2025 Cisco and/or its affiliates. All rights reserved.

Review the proposed labels



© 2025 Cisco and/or its affiliates. All rights reserved.

Proposed Profile Rule for Unknown

Download

	Attribute	Operator	Value
AND	oui	equals	Apple, Inc.
	dhcpParameterRequestList	equals	1, 121, 3, 6, 15, 108, 114, 119, 252
	dhcpClassIdentifier	matches	(?i)(.*[^a-zA-Z0-9]|^)apple($|[^a-zA-Z0-9].*)

ATTRIBUTE USED IN THE RULE

Percentage: % of endpoints in this group already profiled with this information

oui	Apple, Inc.	100%
dhcpParameterRequestList	1, 121, 3, 6, 15, 108, 114, 119, 252	100%
dhcpClassIdentifier	apple	100%

Close

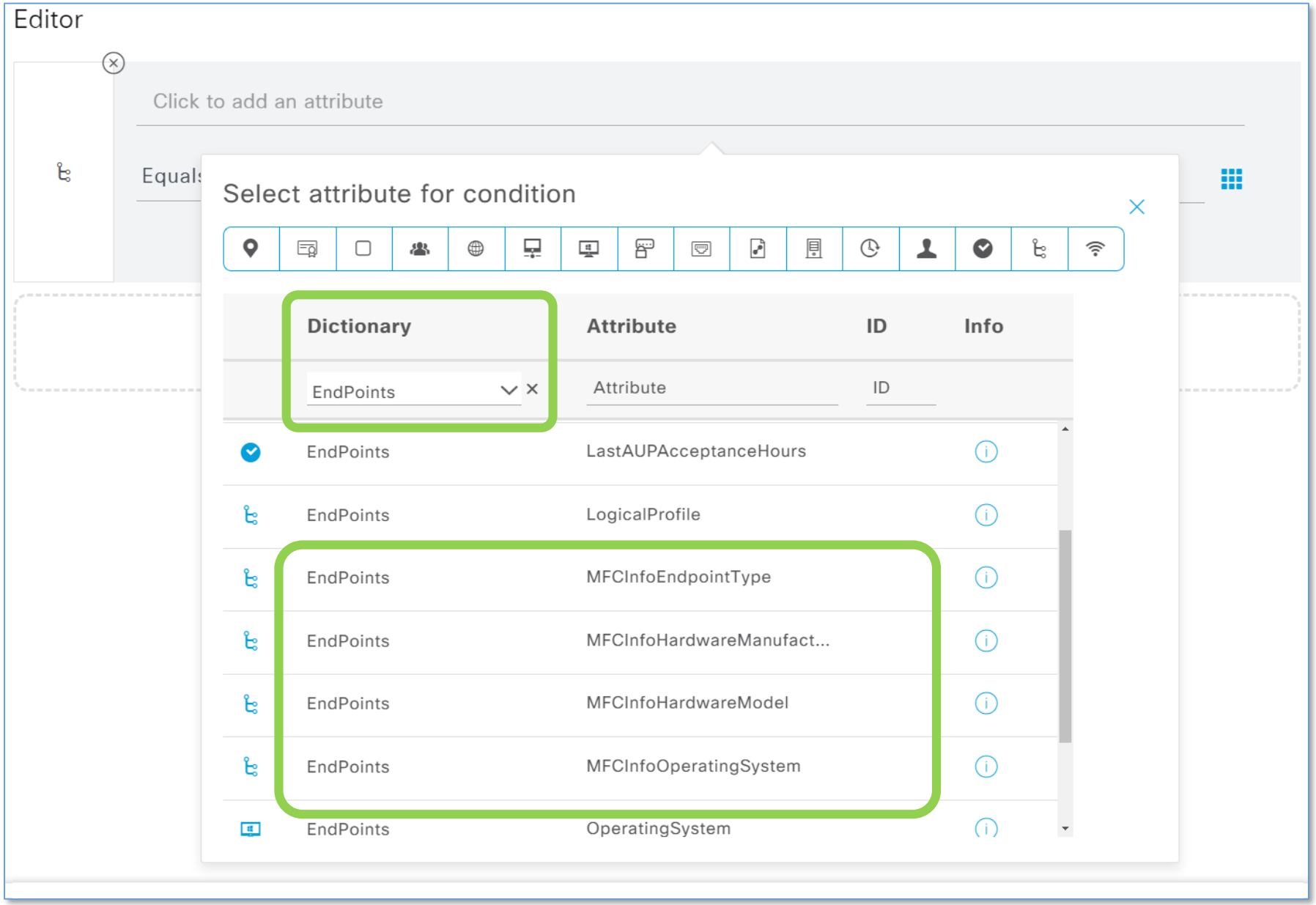
Reject Grouping

Accept Profiling Rule

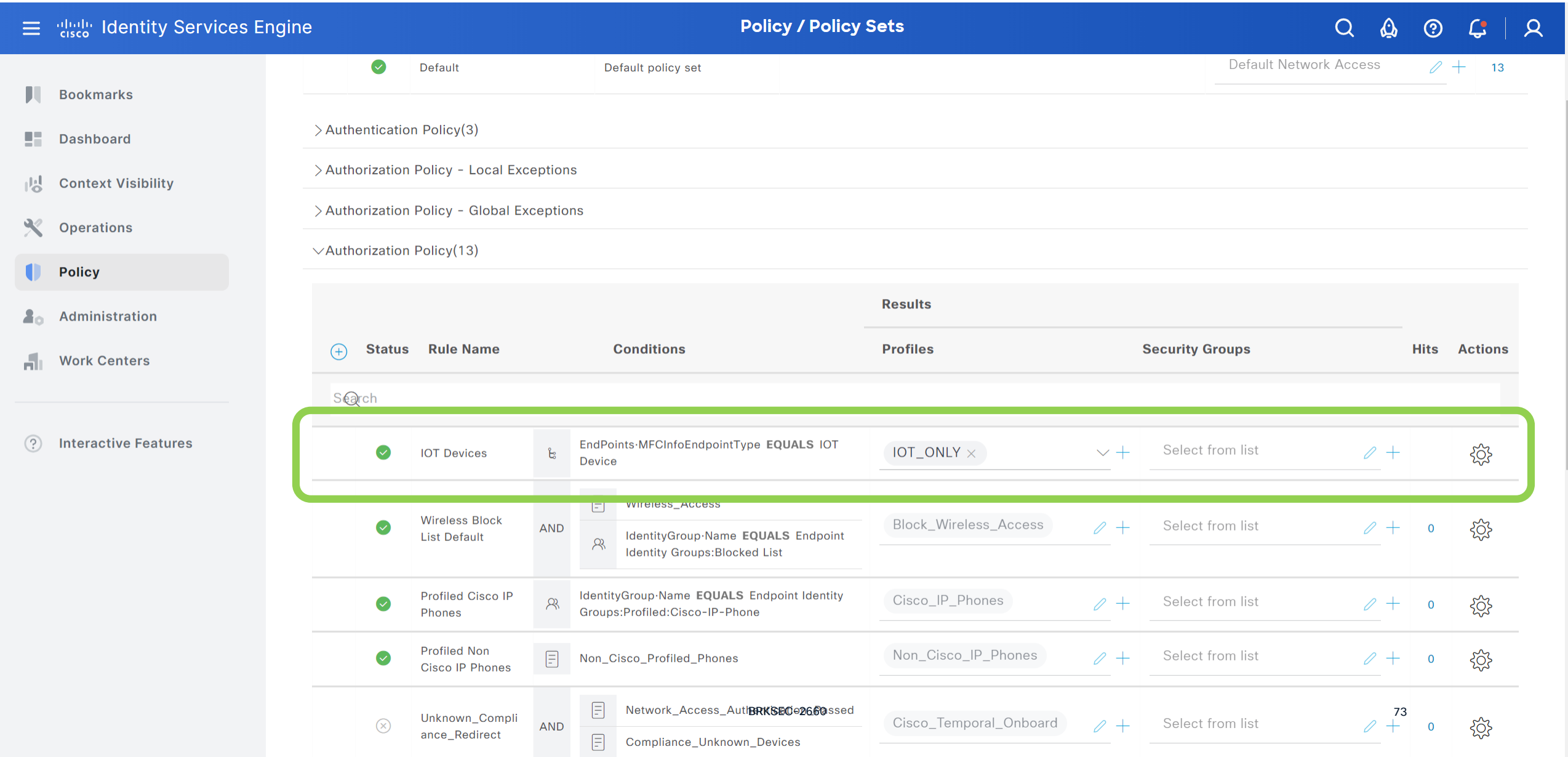
Close = cancel
no changes

© 2025 Cisco and/or its affiliates. All rights reserved.

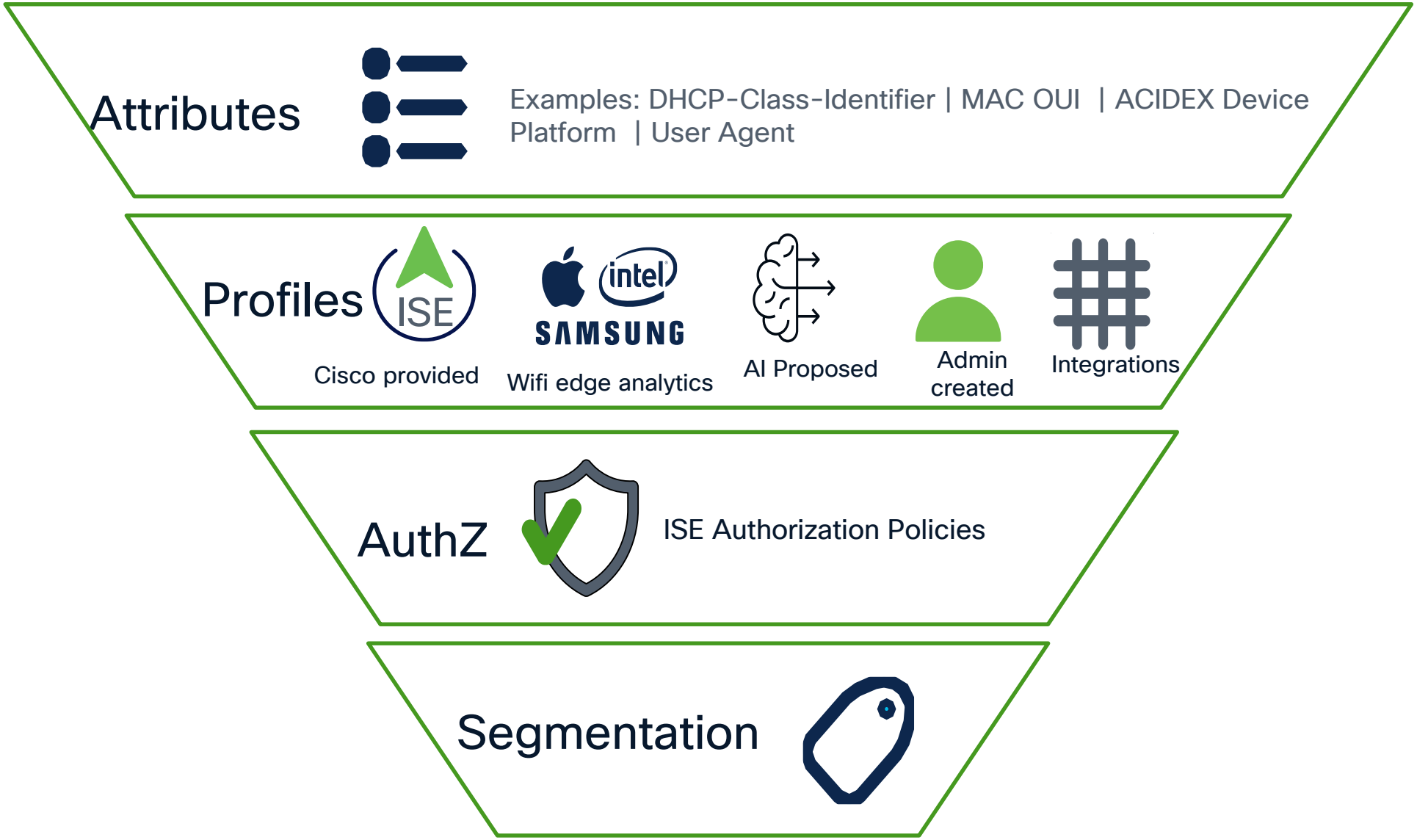
All the MFC Attributes Can Be Used



Ready to Profile!



Turning Probes Into Profiles, Profiles Into Protection



© 2025 Cisco and/or its affiliates. All rights reserved.

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

Cisco Live 2025 FOR REFERENCE BRKSEC-2660

© 2025 Cisco and/or its affiliates. All rights reserved.

Behavioral vs Organizational Endpoint Information

Behavioral

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

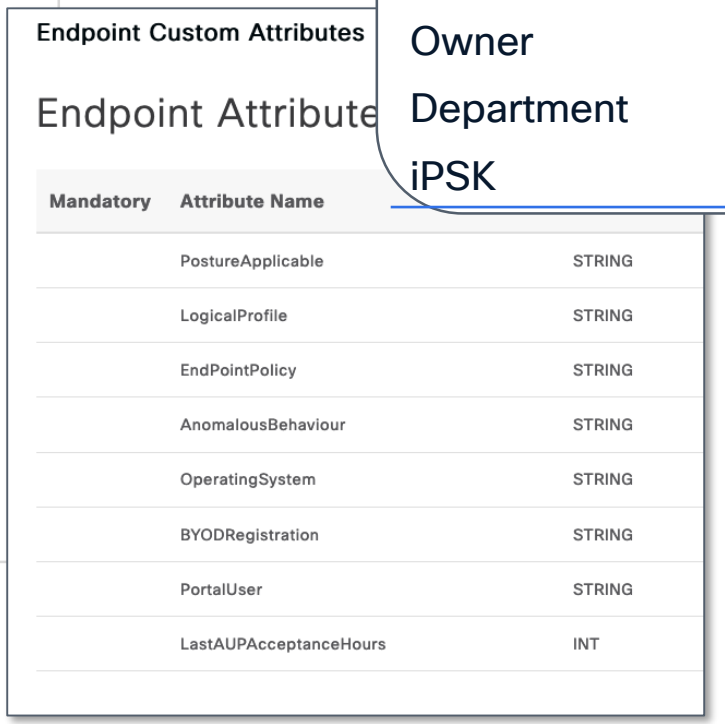
Organizational

- 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

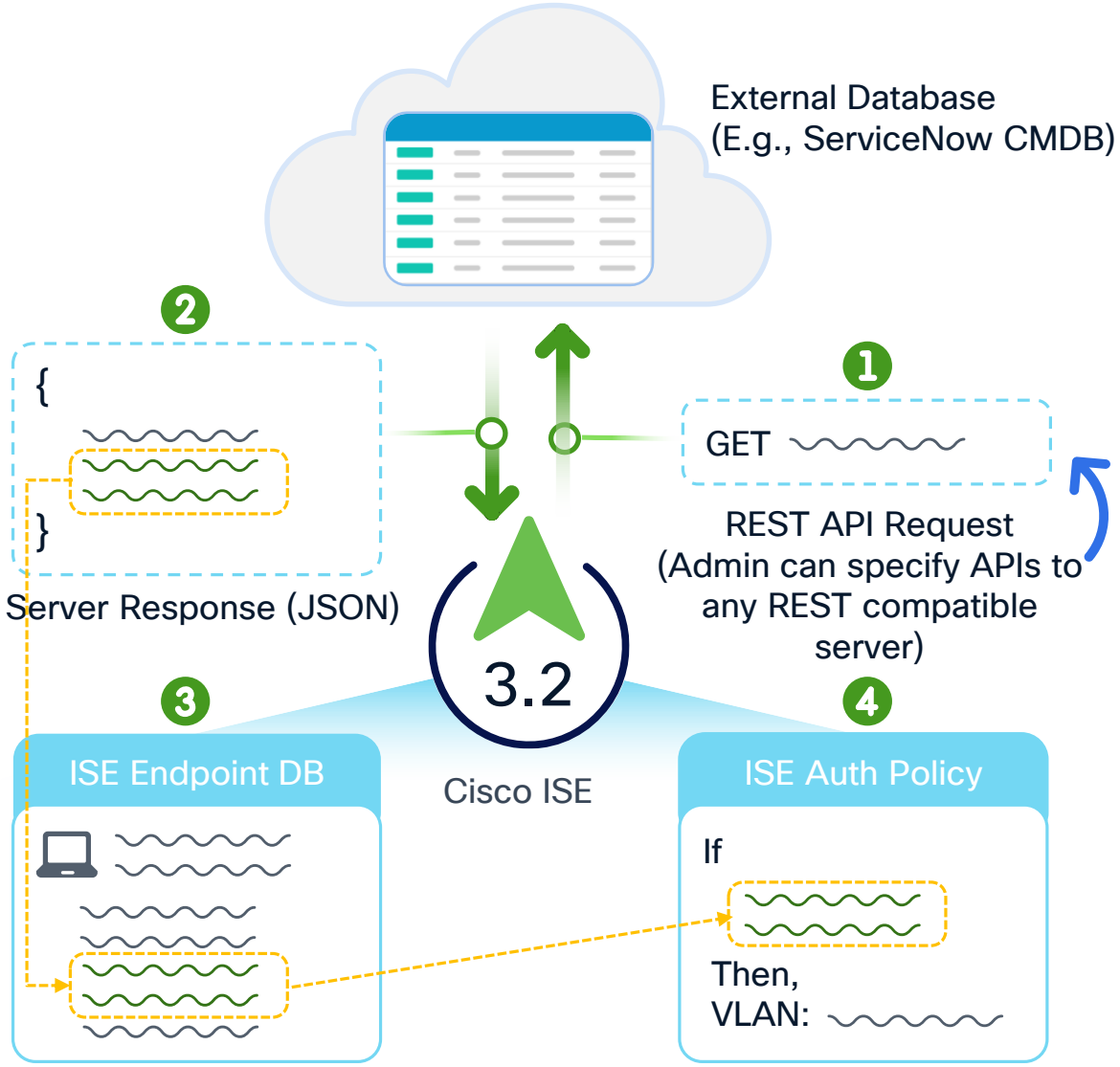
Attribute Name	Type
Created	Date
Expires	Date
Owner	String
Department	String
iPSK	String



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco ISE pxGrid Direct for CMDBs

ISE 3.2



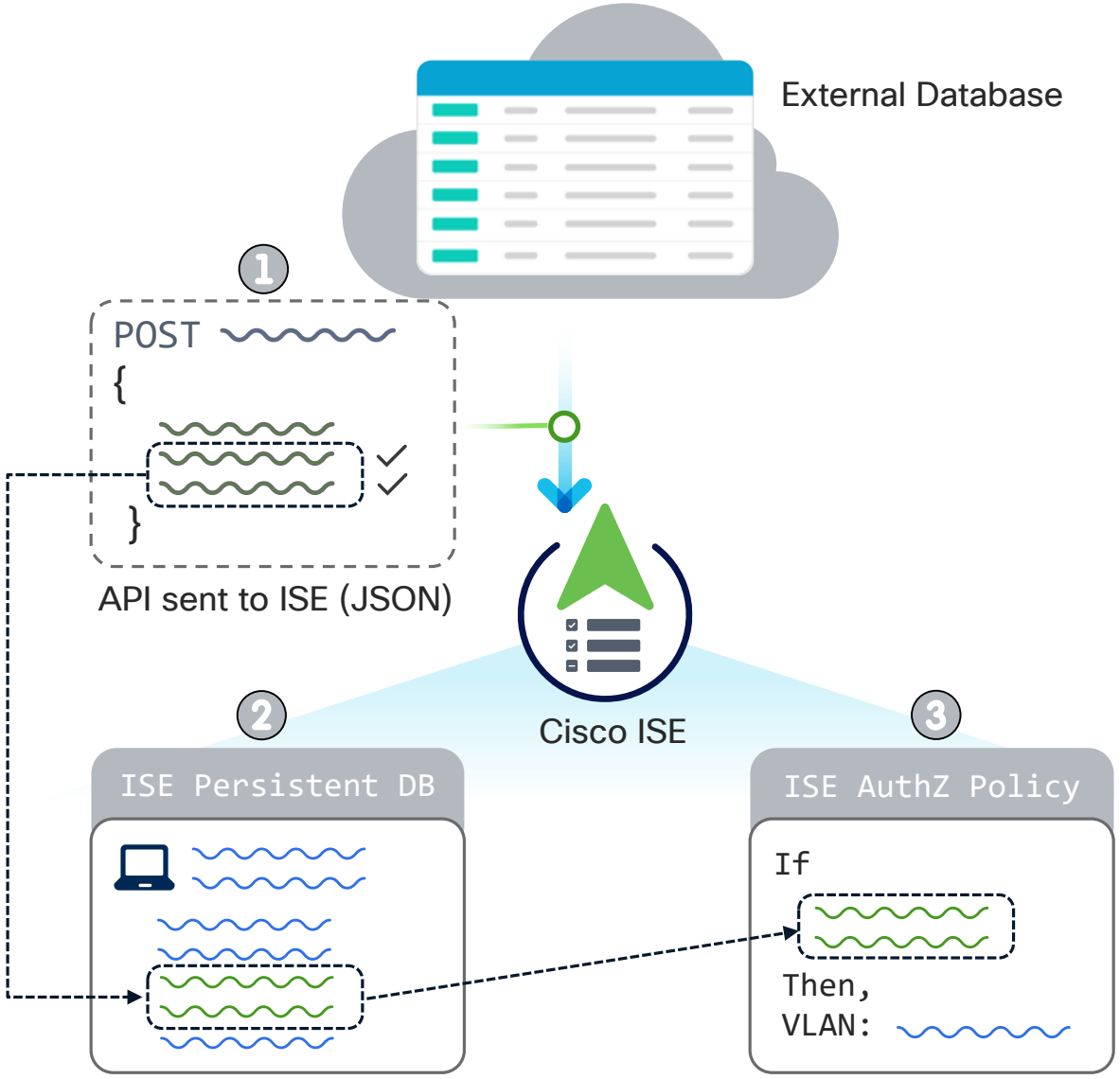

```
{
  "result": [
    {
      "sys_import_state_comment": "",
      "template_import_log": "",
      "sys_updated_on": "2022-05-17 10:53:53",
      "sys_class_name": "EDDA_Demo",
      "sys_target_sys_id": "",
      "sys_id": "00021059db6b01101f0f174b13961900",
      "sys_updated_by": "aacook",
      "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"
    },{ … }
  ]
}
```


© 2025 Cisco and/or its affiliates. All rights reserved.

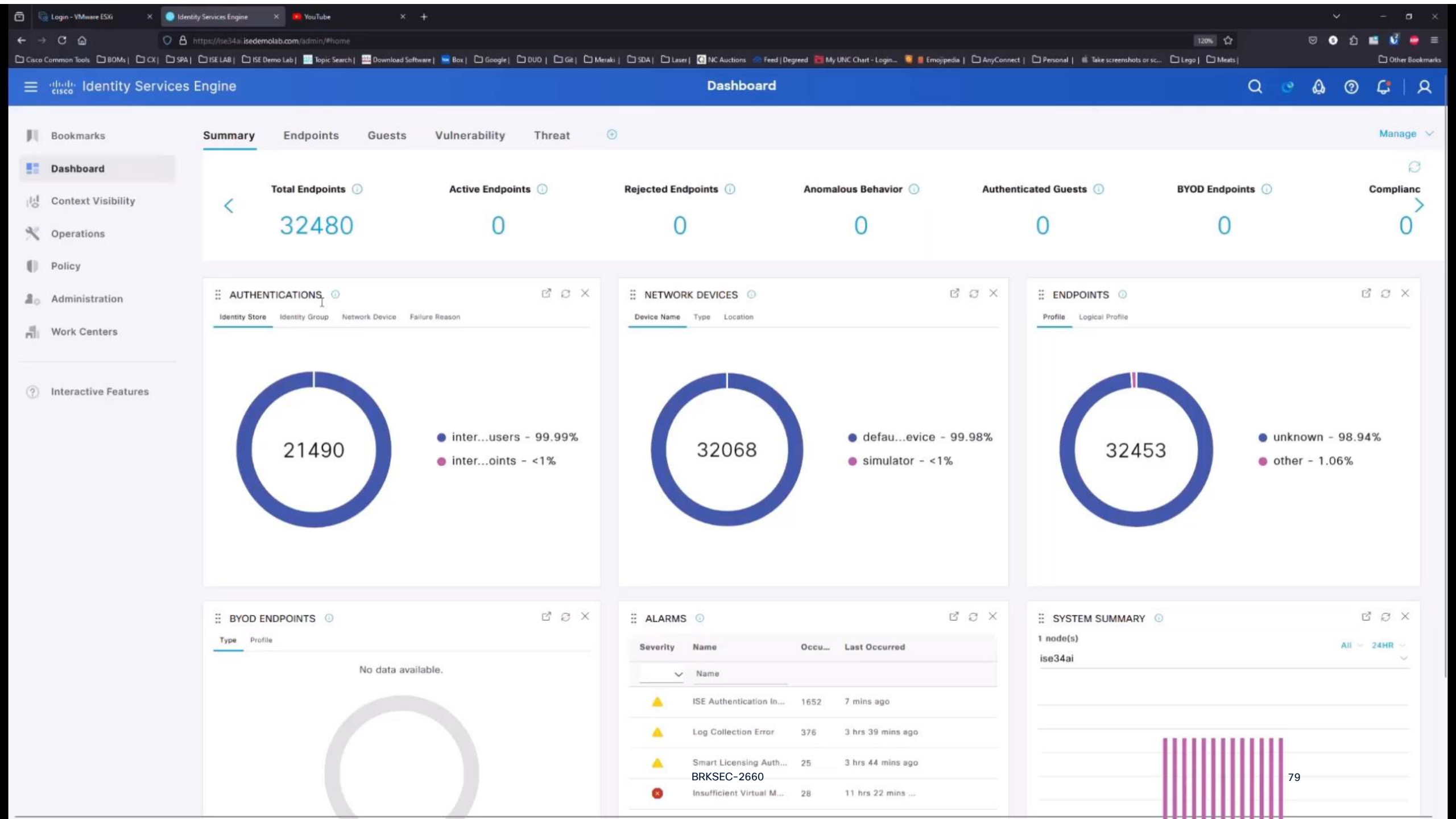
What is pxGrid Direct URL Pusher?

ISE 3.4

- The external server sends the API request to ISE in JSON format
- The attributes are stored in the persistent database, not the endpoint database (which is purged)



© 2025 Cisco and/or its affiliates. All rights reserved.

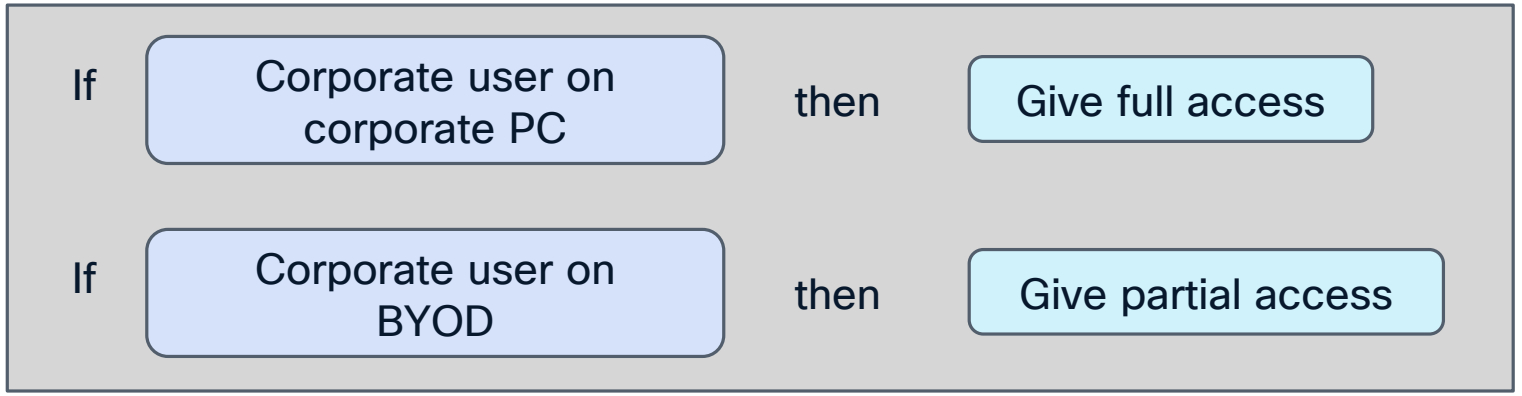

Identity Services Engine
Dashboard
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Summary
Endpoints
Guests
Vulnerability
Threat
Manage
Total Endpoints
32480
Active Endpoints
0
Rejected Endpoints
0
Anomalous Behavior
0
Authenticated Guests
0
BYOD Endpoints
0
Complianc
0
AUTHENTICATIONS
Identity Store
Identity Group
Network Device
Failure Reason
21490
inter...users - 99.99%
inter...oints - <1%
NETWORK DEVICES
Device Name
Type
Location
32068
defau...evice - 99.98%
simulator - <1%
ENDPOINTS
Profile
Logical Profile
32453
unknown - 98.94%
other - 1.06%
BYOD ENDPOINTS
Type
Profile
No data available.
ALARMS
Severity
Name
Occu...
Last Occurred
ISE Authentication In...
1652
7 mins ago
Log Collection Error
376
3 hrs 39 mins ago
Smart Licensing Auth...
25
3 hrs 44 mins ago
Insufficient Virtual M...
28
11 hrs 22 mins ...
SYSTEM SUMMARY
1 node(s)
All
24HR
ise34ai

Policies

ISE Policy Logic

- Start from logic you want to implement. Then translate it in technical language
- All ISE policies use the same format:

Examples:



Rules will be processed top to bottom, first match will be applied, (as for Firewall ACL)

© 2025 Cisco and/or its affiliates. All rights reserved.

Policy Sets

Policy sets allow to control the type of access of groups of users.

Define access policies for a specific group of users based on any attribute from the initial RADIUS packet.

Group similar rules (MAB vs. dot1x, SSID, location)

Improve rules readability

Reduces configuration mistakes

Better rule processing

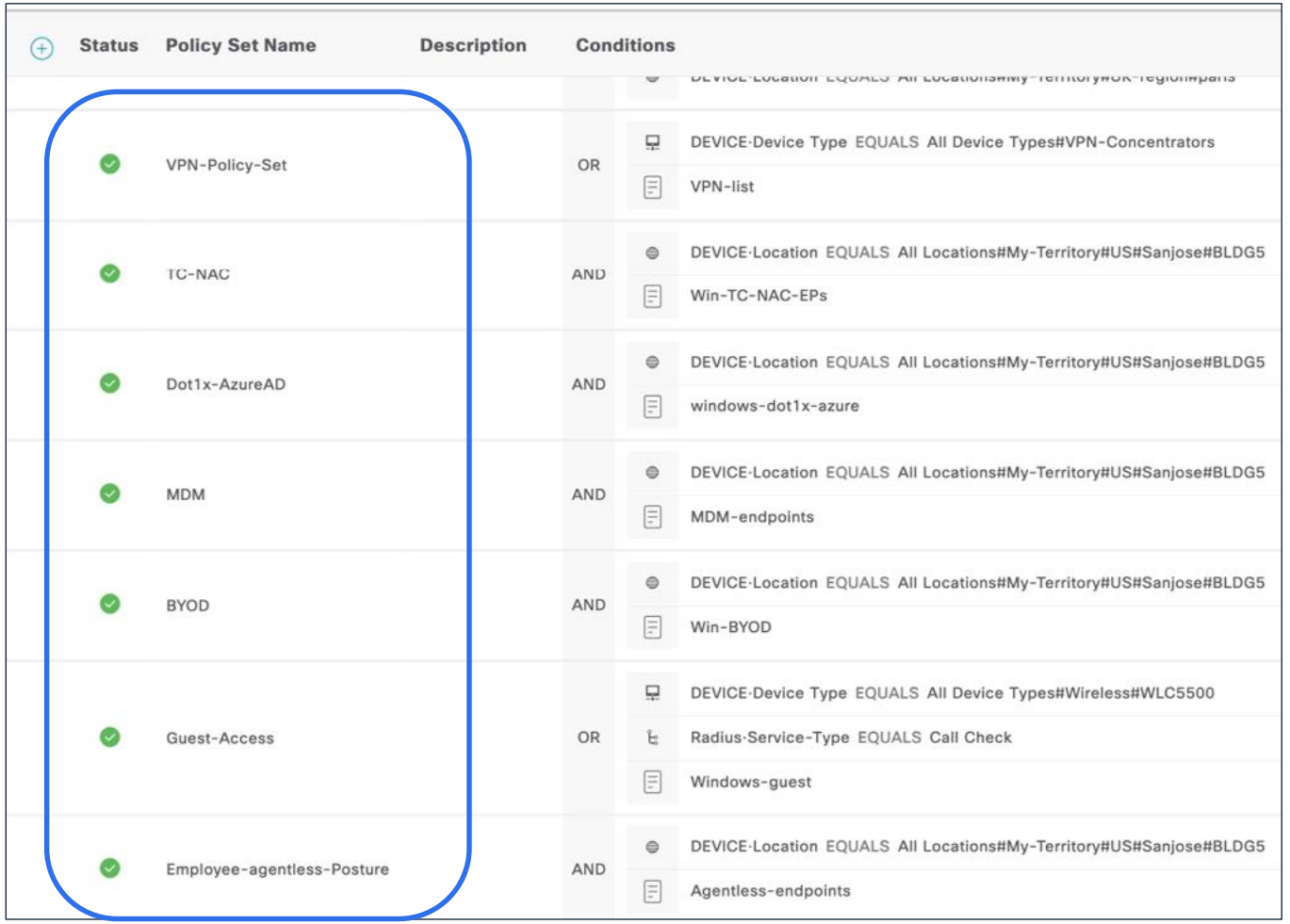
Network Device Type

Location

SSID

Vendor/Model

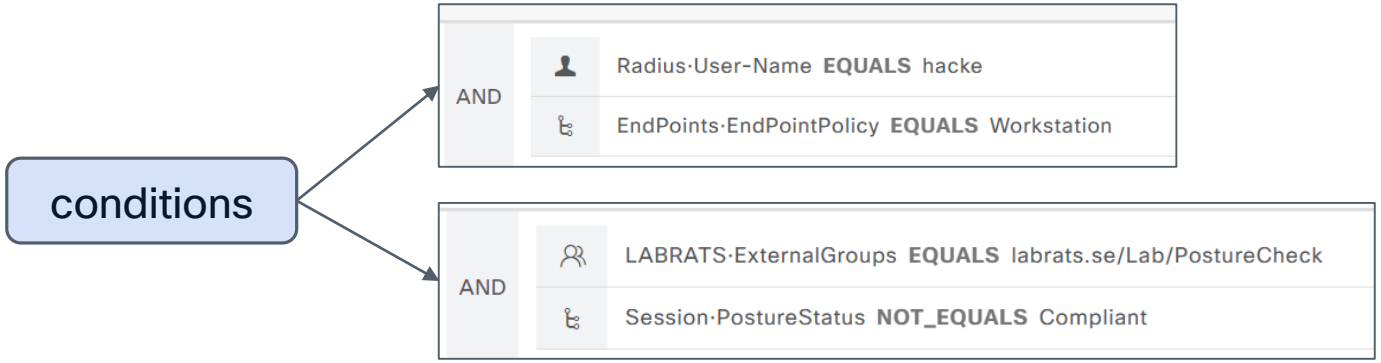
Access Type (802.1x or MAB)



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

© 2025 Cisco and/or its affiliates. All rights reserved.

ISE Conditions



Conditions can be combined with multiple logic (for example AND, OR, EQUALS, CONTAINS, IS NOT etc

Example:

The endpoint has to be

User AND machine authenticated

AND

OR

User in AD group Employee

User in AD group Corporate

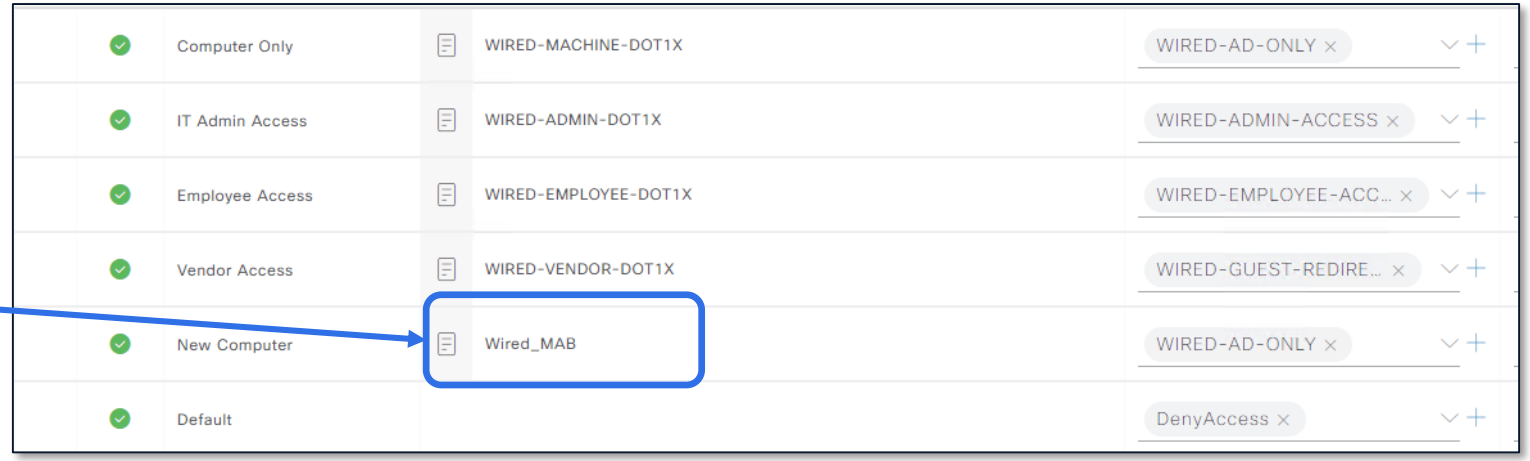
AND

User NOT in San Diego

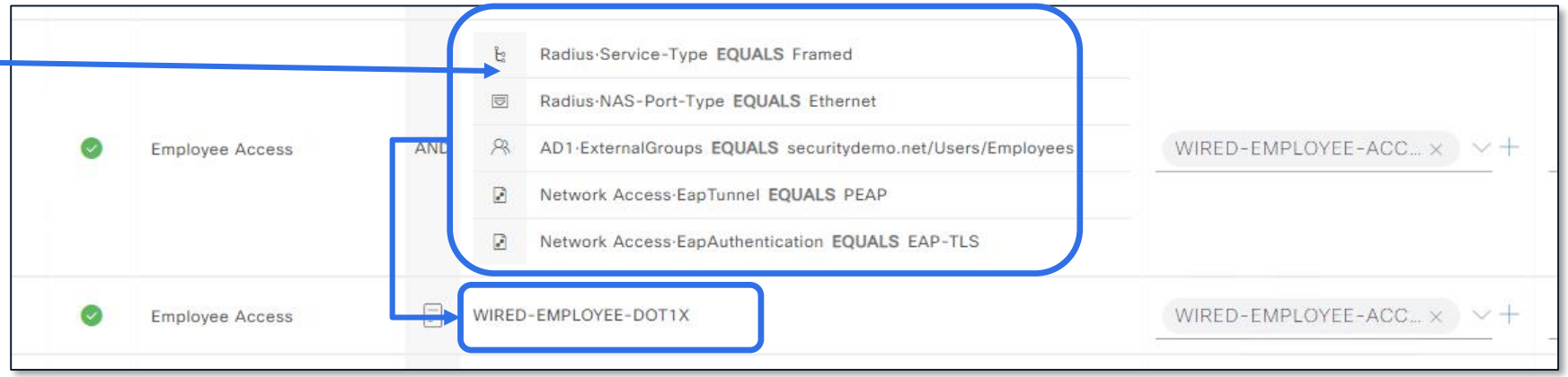
© 2025 Cisco and/or its affiliates. All rights reserved.

Conditions simplification

Pre-sets Dictionary Condition are easy to read and intuitive



Custom created Conditions often are not as intuitive

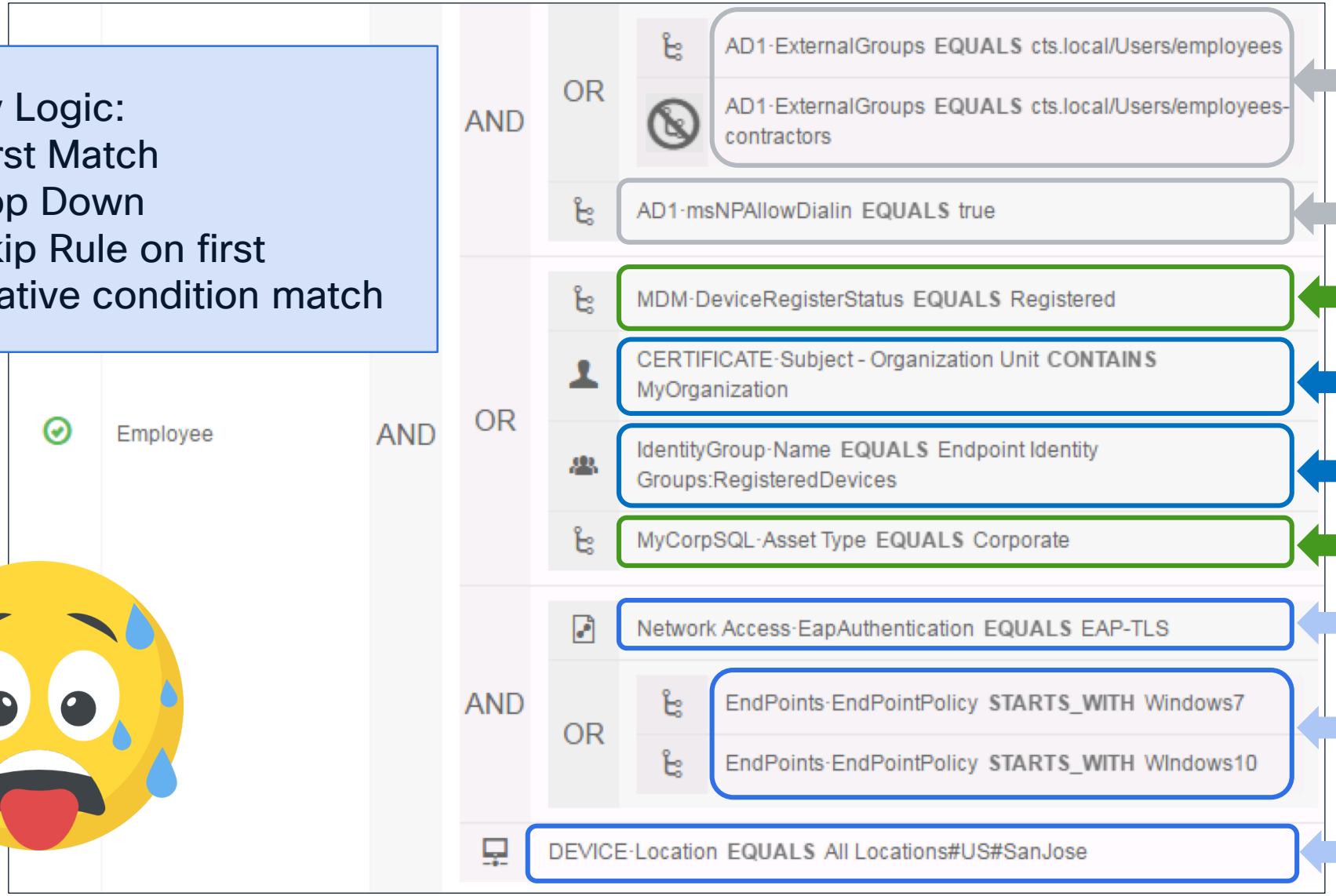


Use Compound Conditions and for custom ones

© 2025 Cisco and/or its affiliates. All rights reserved.

Auth Policy Optimization

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



Let’s make a speed Test!

Let’s process conditions in Policies as ISE does one condition after the other in order of writing

Is the image matching the condition set?

Total stars = 10

Total Green stars = 4

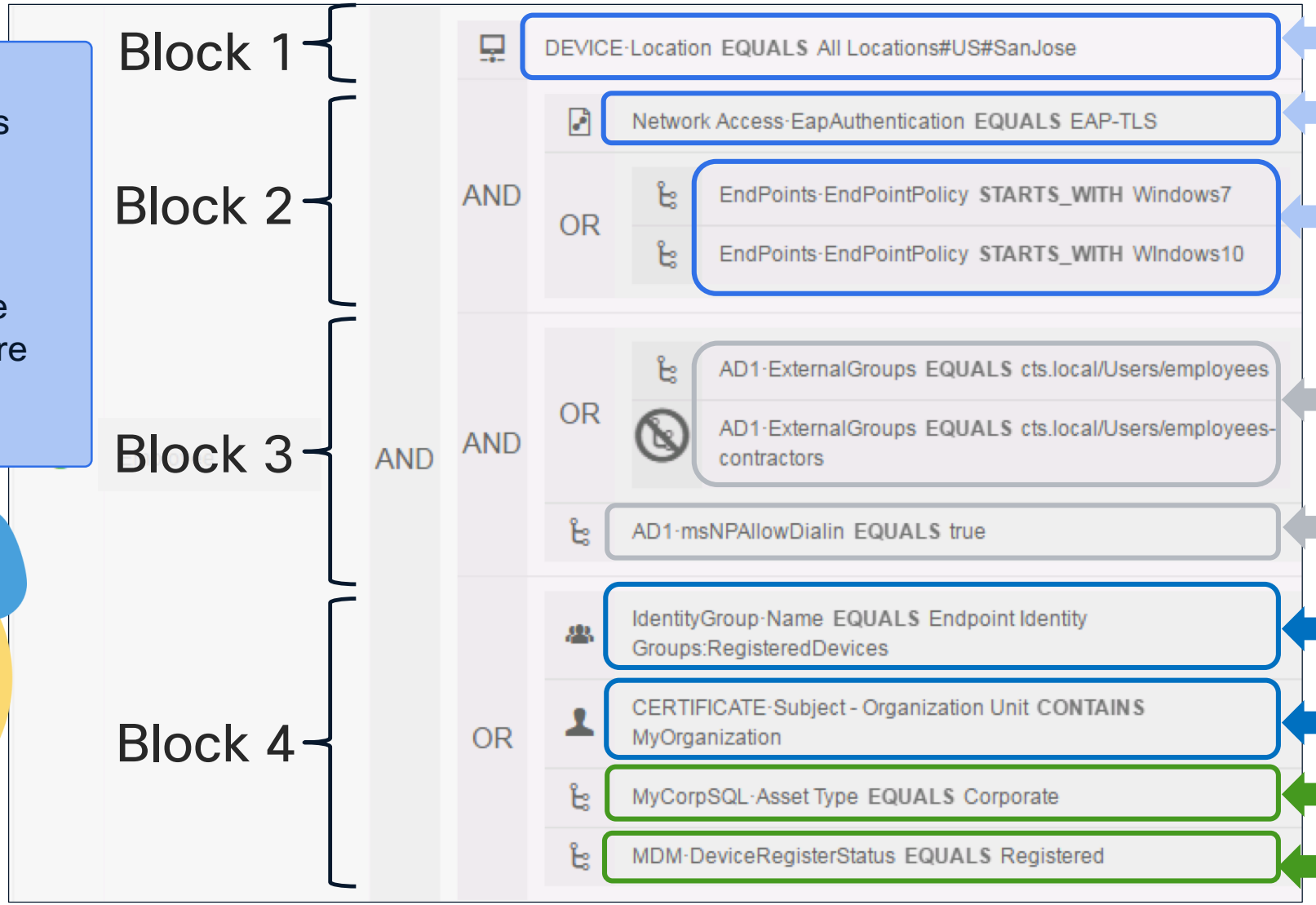
Total red stars = 2

Outer shape = Red triangle

© 2025 Cisco and/or its affiliates. All rights reserved.

Auth Policy Optimization

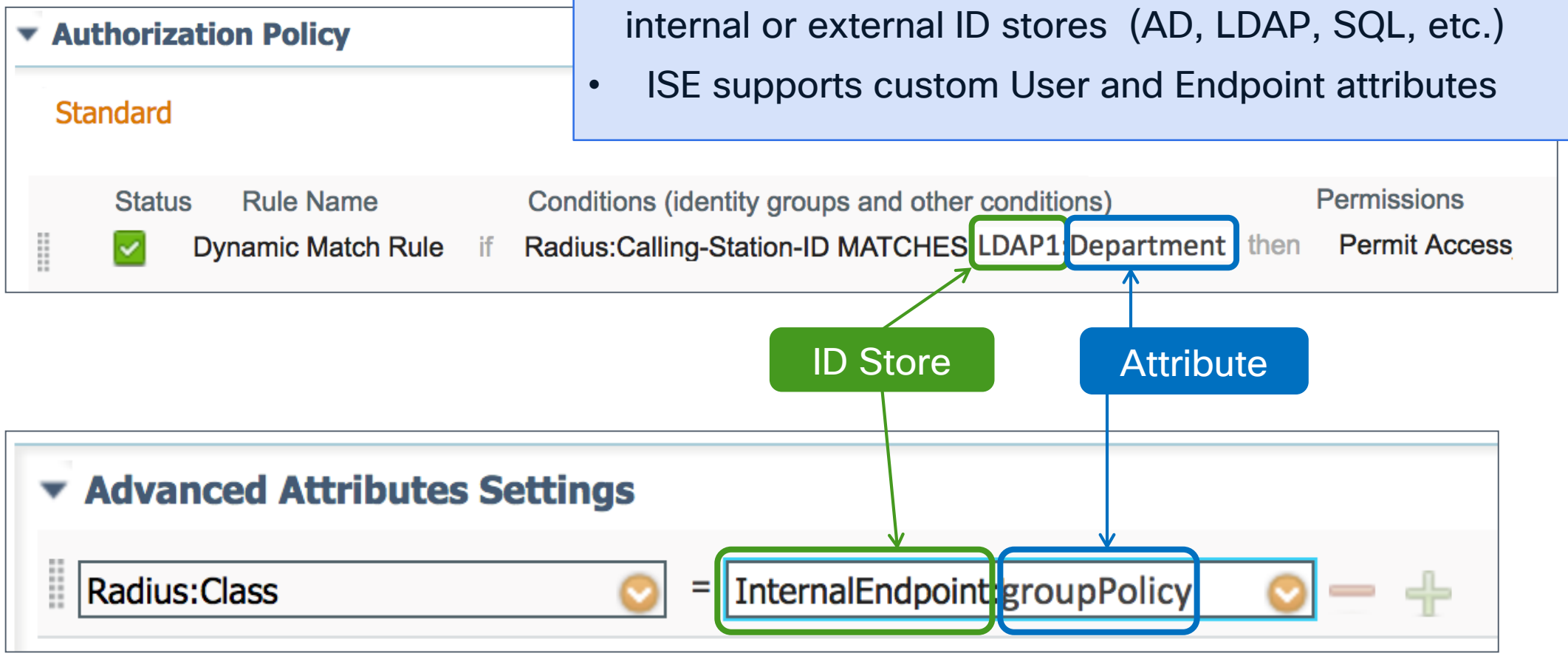
- Local conditions should be put before external
- External lookup should go at the end as take more time



© 2025 Cisco and/or its affiliates. All rights reserved.

Dynamic Variable Substitution

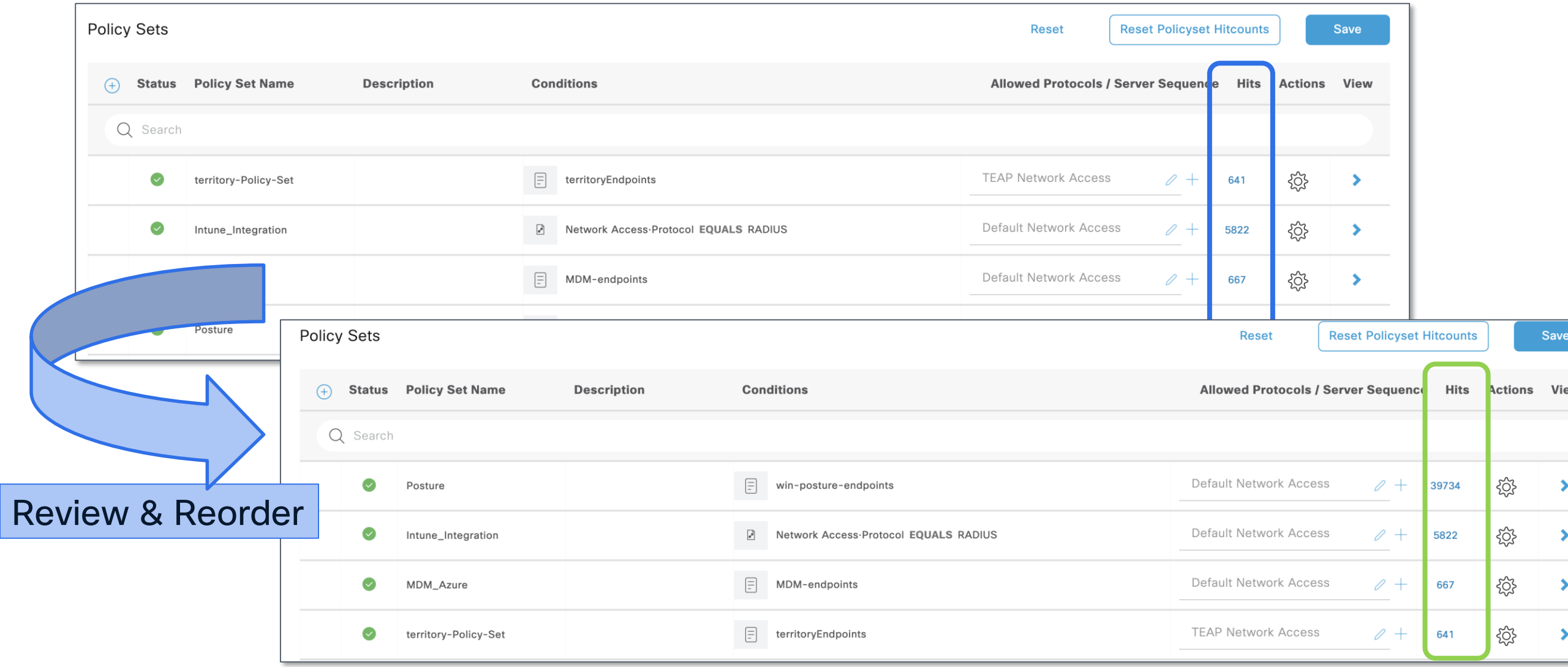
- Match conditions to unique values stored per- User/Endpoint in internal or external ID stores (AD, LDAP, SQL, etc.)
- ISE supports custom User and Endpoint attributes



© 2025 Cisco and/or its affiliates. All rights reserved.

Can you reorder some of the policy sets?

Review and Reorder



© 2025 Cisco and/or its affiliates. All rights reserved.

Create your own lab

Who Needs an ISE Lab? You do!

With every 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

© 2025 Cisco and/or its affiliates. All rights reserved.

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
...

© 2025 Cisco and/or its affiliates. All rights reserved.

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

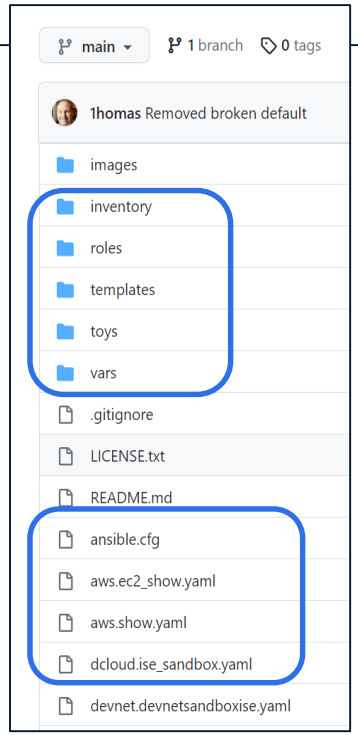
1. Clone this repository:

```
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.



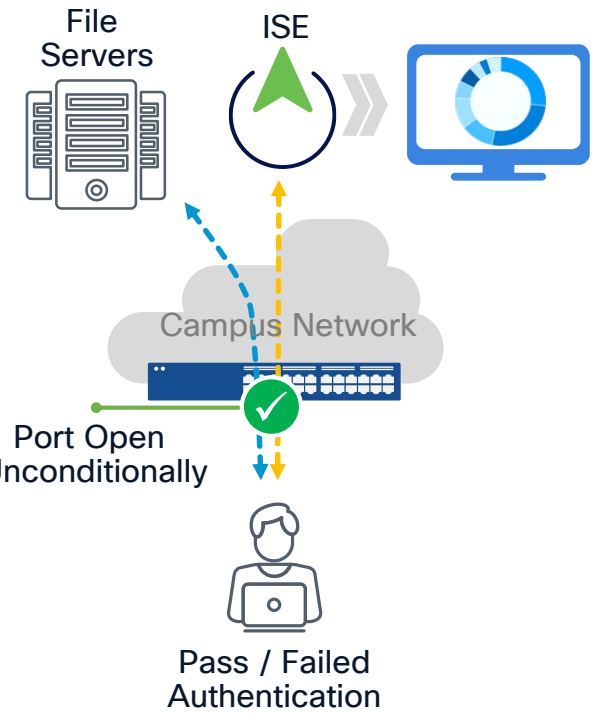
Ansible playbooks

© 2025 Cisco and/or its affiliates. All rights reserved.

802.1x Deployment Modes

Deployment Modes

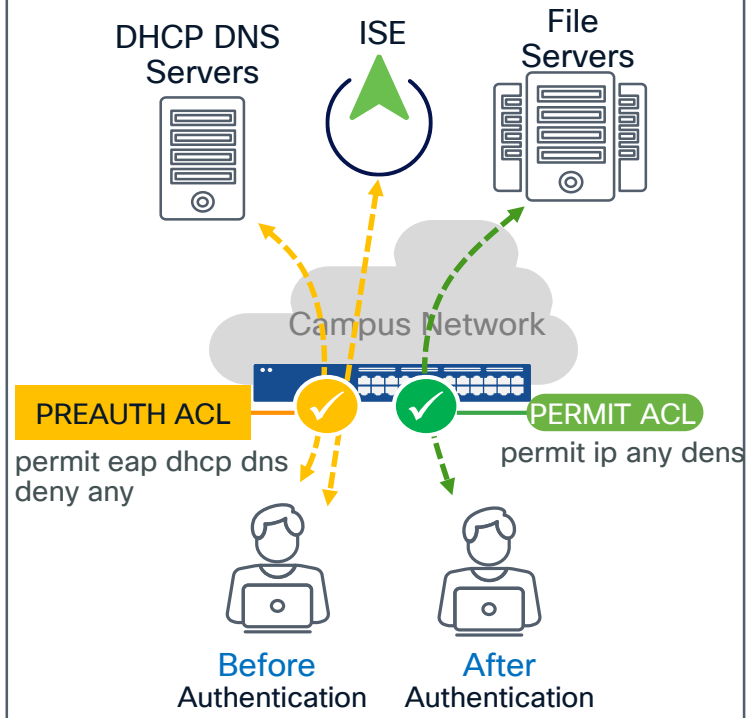
Monitor Mode (Visibility)




```
authentication open
```

No impact to existing network

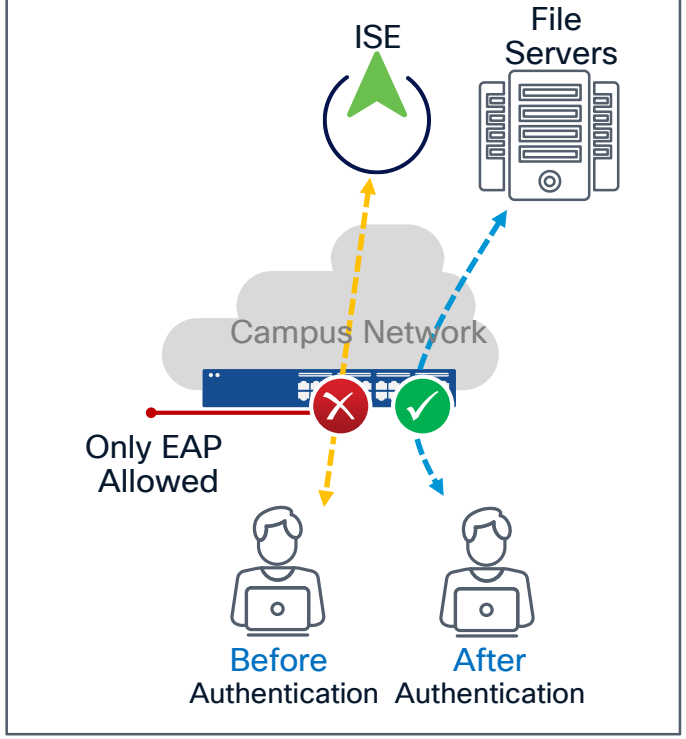
Low-Impact Mode (Visibility and Control)




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

Begin to control and differentiate access

Closed Mode (Visibility and Control)

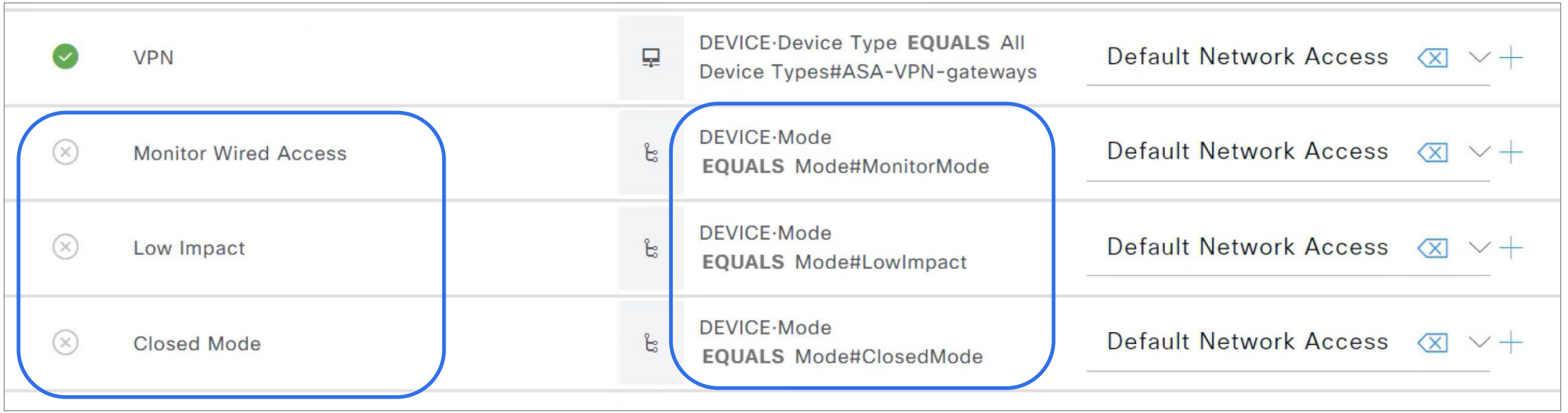


- Not everyone needs Closed Mode
- No access at all before authentication

© 2025 Cisco and/or its affiliates. All rights reserved.

Utilizing Policy Sets with Modes

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



© 2025 Cisco and/or its affiliates. All rights reserved.

Day 2 Operations

User involvement

User Communication before and after ISE rollout

cisco **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.

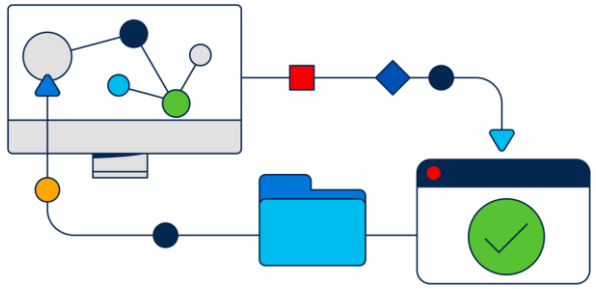
What is 802.1x ?
IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

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...

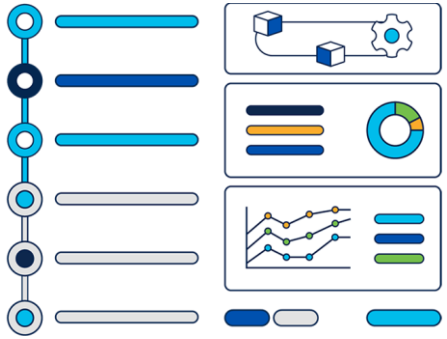
Cisco Managed Windows Laptops	Mac Laptops	Remote Desktops **Windows Only**	Linux / Unix workstations	Voice/Video Endpoints	Non IT Managed Printers
Personal devices (Apple TVs, PlayStation etc.)	Routers, Switches, ESXi, and APs	Onsite (In-Office) – Patching	Demo/Training devices	Password Management	Generic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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Wrap up

Deploying any network access control solution is crucial

but it isn't easy....

Proper planning is essential to any successful development.

© 2025 Cisco and/or its affiliates. All rights reserved.

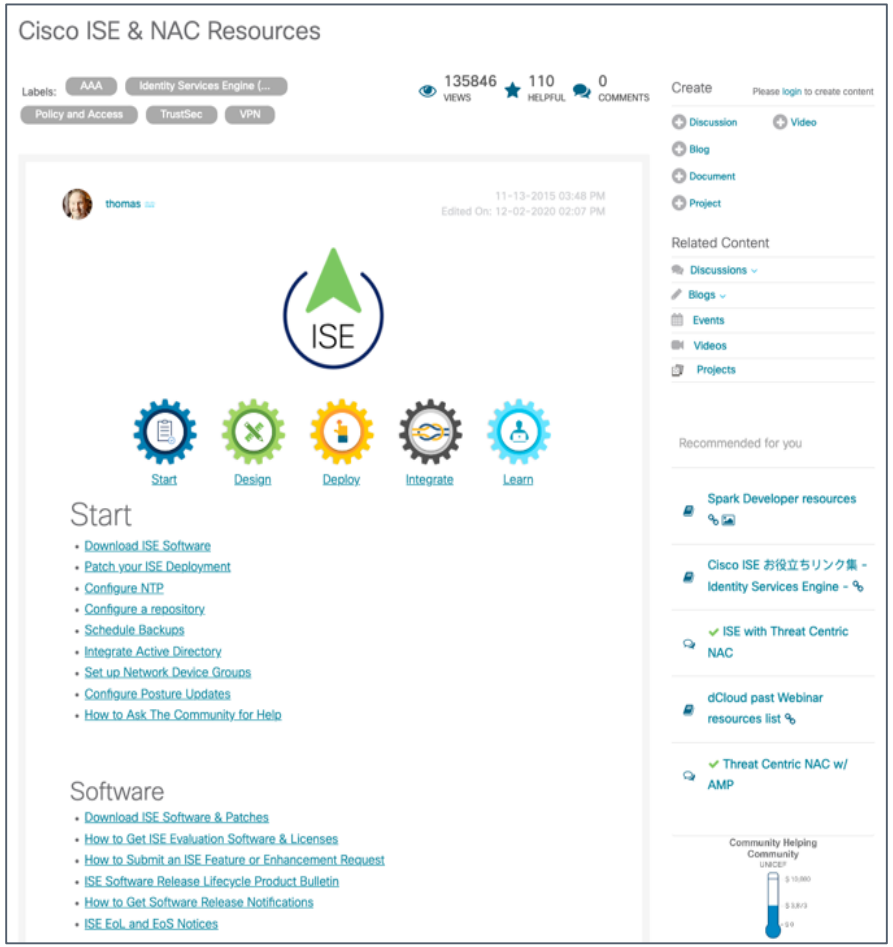
Technical Session Surveys

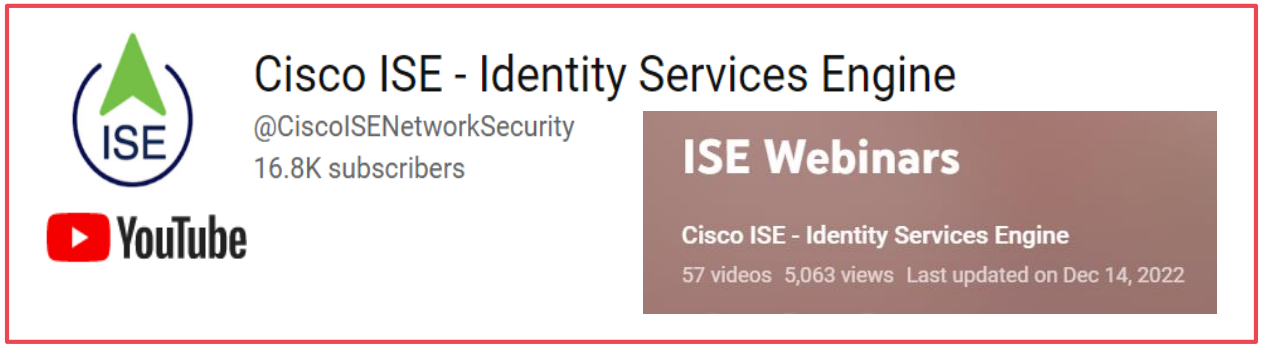
- Compliments ☺
- What you liked
- Suggestions?

© 2025 Cisco and/or its affiliates. All rights reserved.

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





© 2025 Cisco and/or its affiliates. All rights reserved.

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!

© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

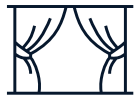
Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

cisco Live !


CISCO