

Setting the Stage for ISE Deployment Success:

A Guide to Effective Planning

Francesca Martucci
Technical Solutions Architect –
Cybersecurity EMEA

cisco Live !

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.



**“A goal
without a plan
is just a wish”**

Antoine de Saint-Exupéry



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

What needs to be included in my planning?



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

**Proper planning is
essential to a successful
deployment.**



Who am I?

Technical Solutions Architect

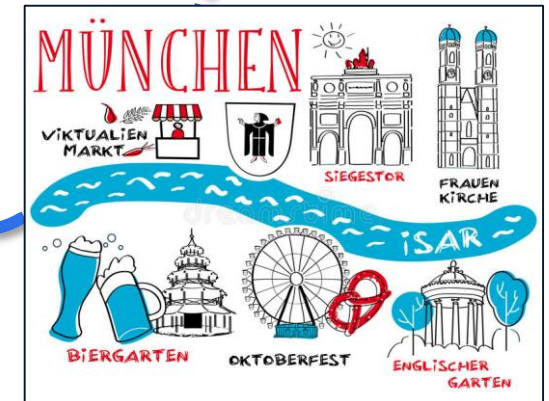
Cyber Security EMEA

25 years of Cisco experience...

... And 3 countries

Main interest on

- Policy and Access
- Segmentation
- Industrial Security



Cisco ISE High Level Design

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



thomas

05-07-2018 09:40 AM

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

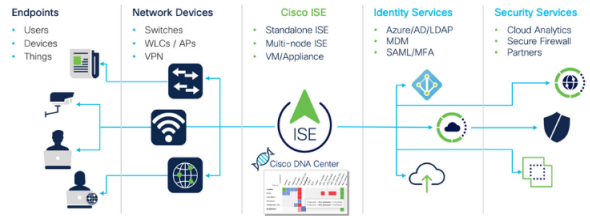


Introduction

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

Enterprise

Security



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**

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*

Cisco Webex App

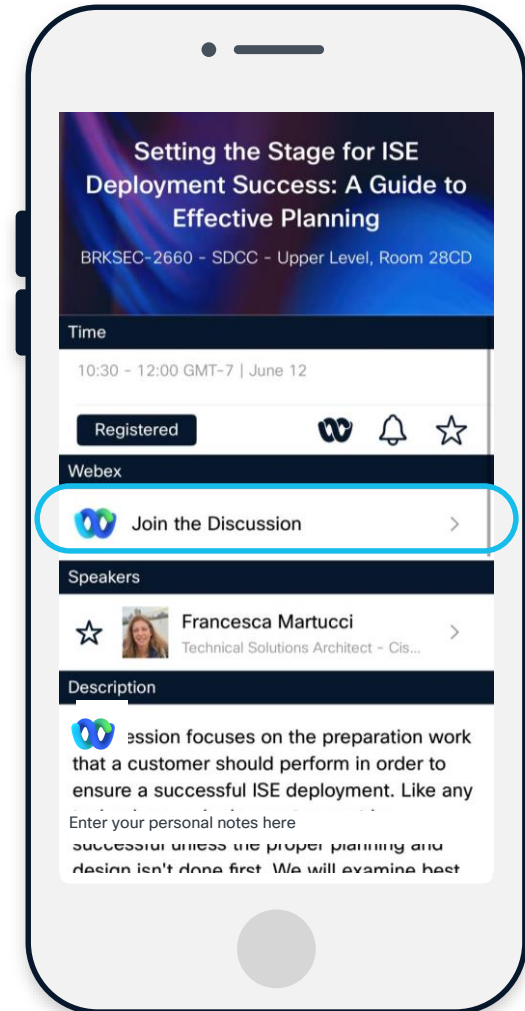
Questions?

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

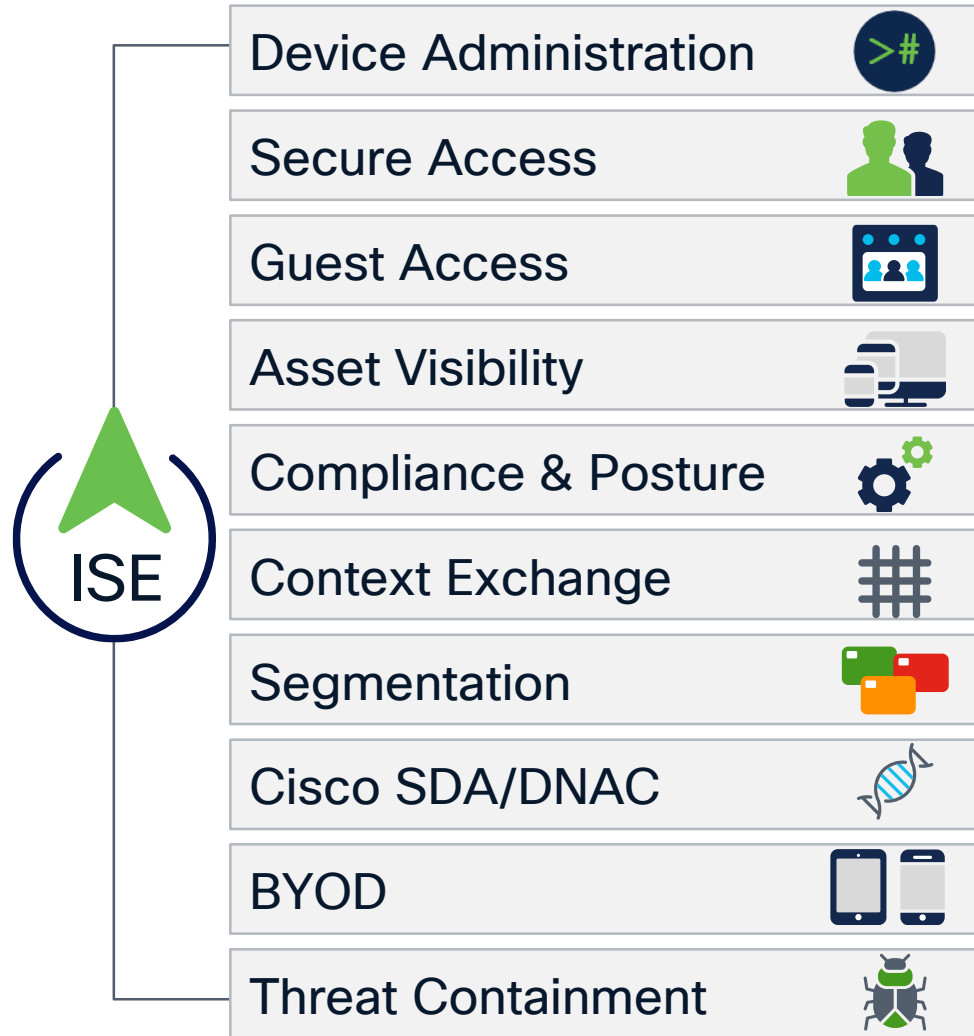
Webex spaces will be moderated by the speaker until June 13, 2025.



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

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?

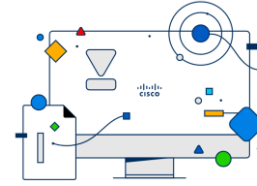
Which use cases could be considered for the future?

Understand Your Needs and Use cases



Objectives / Risk / Priorities

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



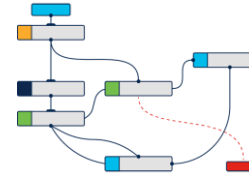
Environment

- 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

Defining your Security Policy

What is an IT security policy?

“It identifies the rules and procedures for all the individuals accessing and using an organization’s IT assets and resources.”

Everyone Has Different Needs

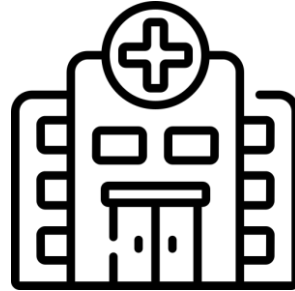
Government



Financials



Healthcare



Retail



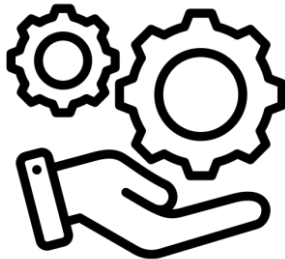
Education



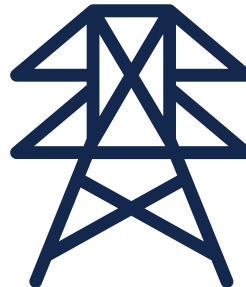
Transportation



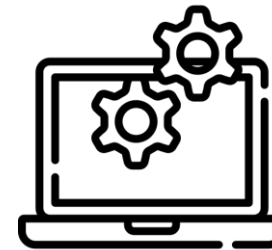
Services



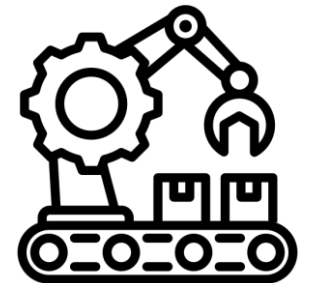
Utilities



Technology



Manufacturing



Example of your ISE policy planning

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

Endpoint Team

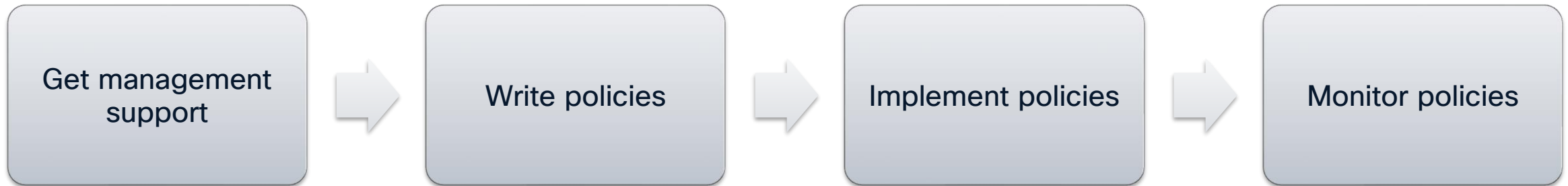
Network Team

Security Team

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

Interoperation with other teams

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



ISE Deployment Planning



cs.co/ise-hld



cs.co/ise-resources#Planning



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



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

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)

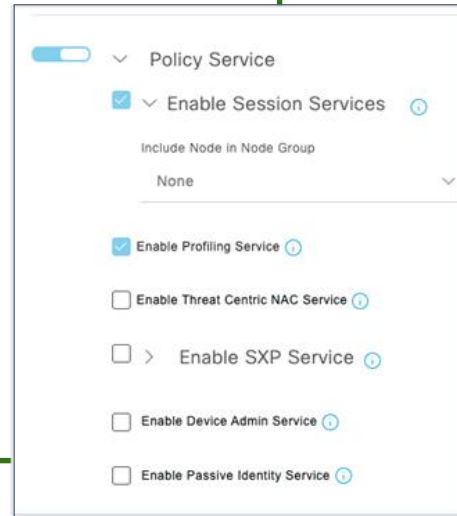
- Receives logs from all nodes
- Handles remote logging targets
- Generates summary Dashboard Views
- Performs scheduled reports
- Handles reporting and API queries

Policy Service Node (PSN)

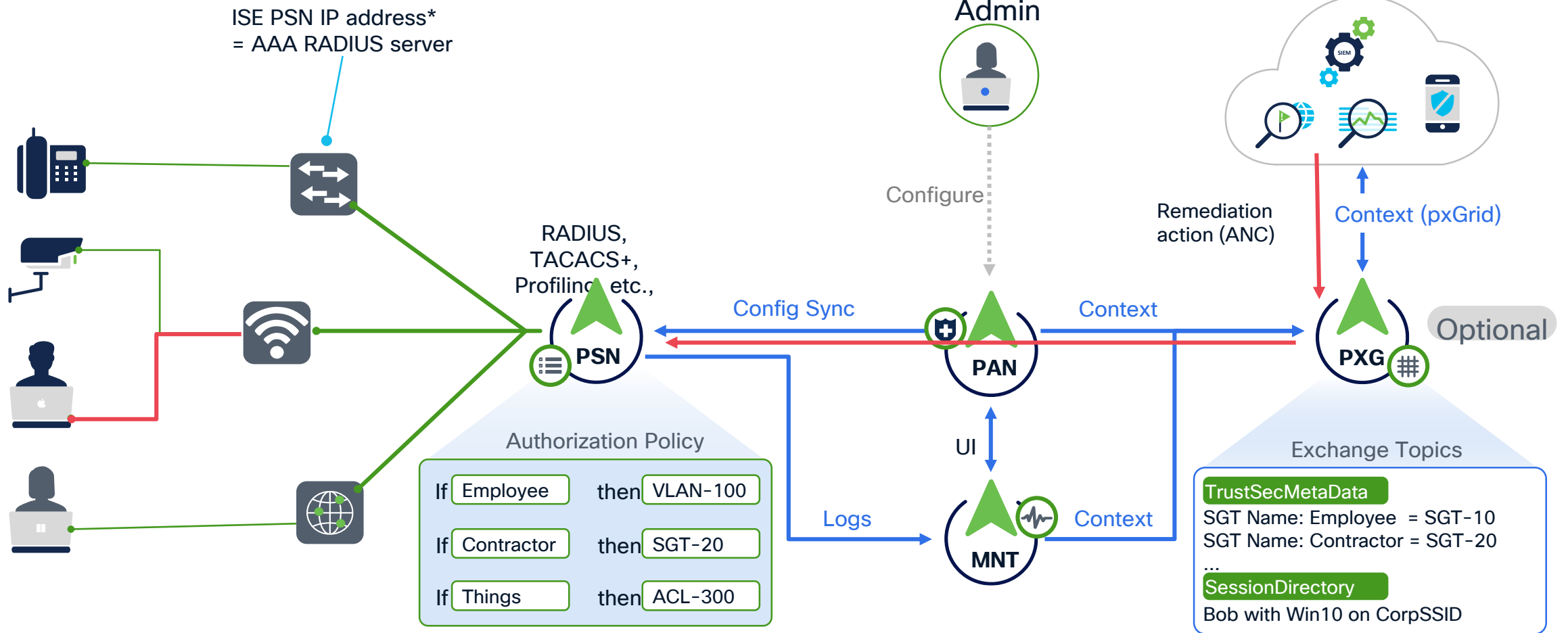
- TACACS requests
- RADIUS requests
- Endpoint profiling probes
- Identity store queries
- Hosts Guest/BYOD portals
- MDM/Posture queries
- TC-NAC & SXP services

Platform Exchange Grid Node (PXG)

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



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 and HA

Centralized ISE



Policy Administration Node (PAN)

- Max 2 in a deployment



Monitoring & Troubleshooting Node (MnT)

- Max 2 in a deployment



Policy Services Node (PSN)

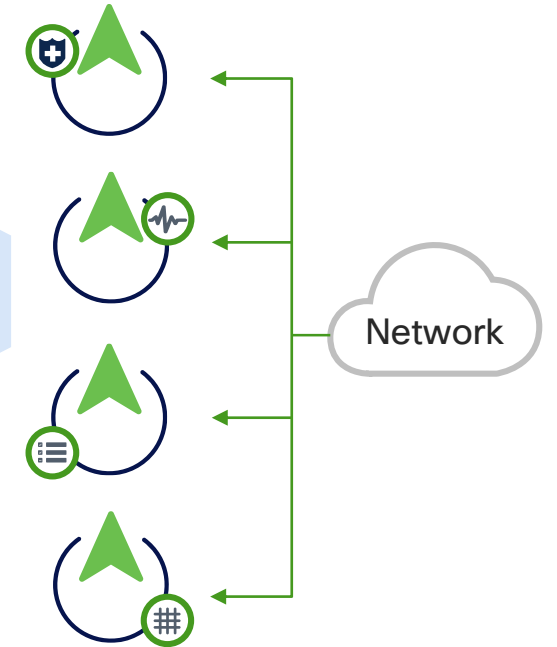
- Max 50 in a deployment



pxGrid Controller

- Max 4 in deployment

Distributed ISE



Maximum Concurrent Active Endpoints



- One endpoint is a unique MAC address
- ISE Licensing is counted by *active endpoint sessions*
- RADIUS Accounting defines session **Start & Stop** events
- Sessions **Start** upon RADIUS Authorization
- Sessions **Stop** upon :
 - Disconnect
 - Session Expiration
 - Idle Timeout

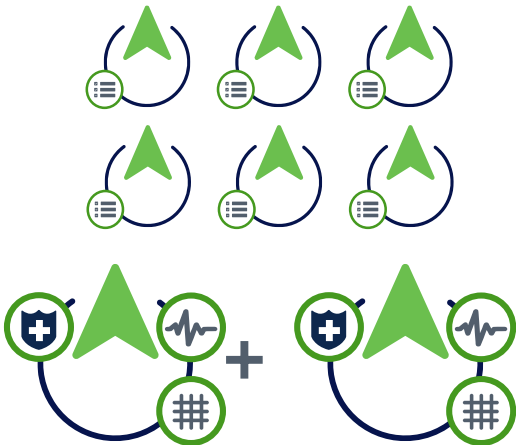
ISE Scaling



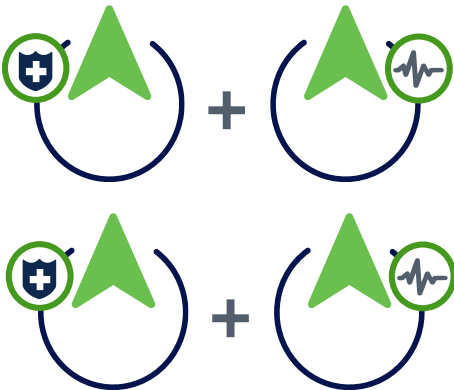
Standalone



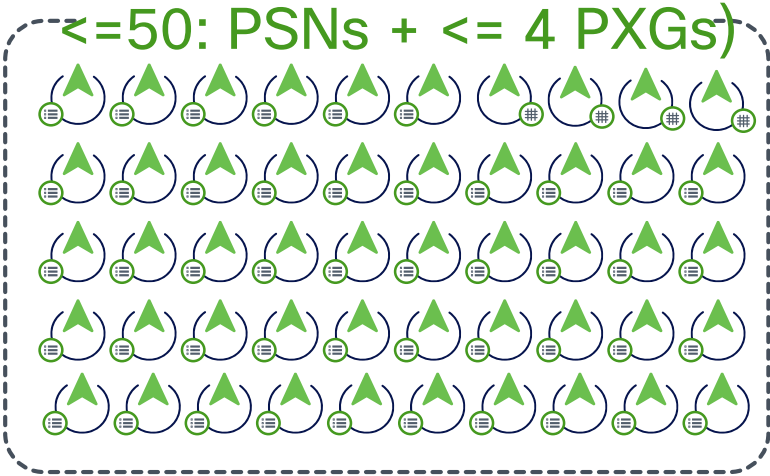
Small HA Deployment
2 x (PAN+MNT+PSN)+ Extra PSN



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

Total Maximum Concurrent Active Sessions

Per whole deployment



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

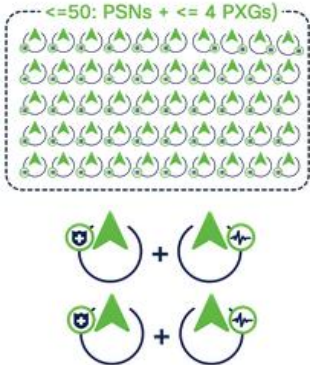
Small Deployment



Medium Deployment



Large Deployment



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

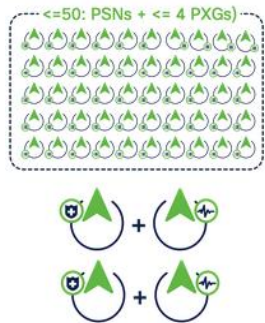
Small Deployment



Medium Deployment

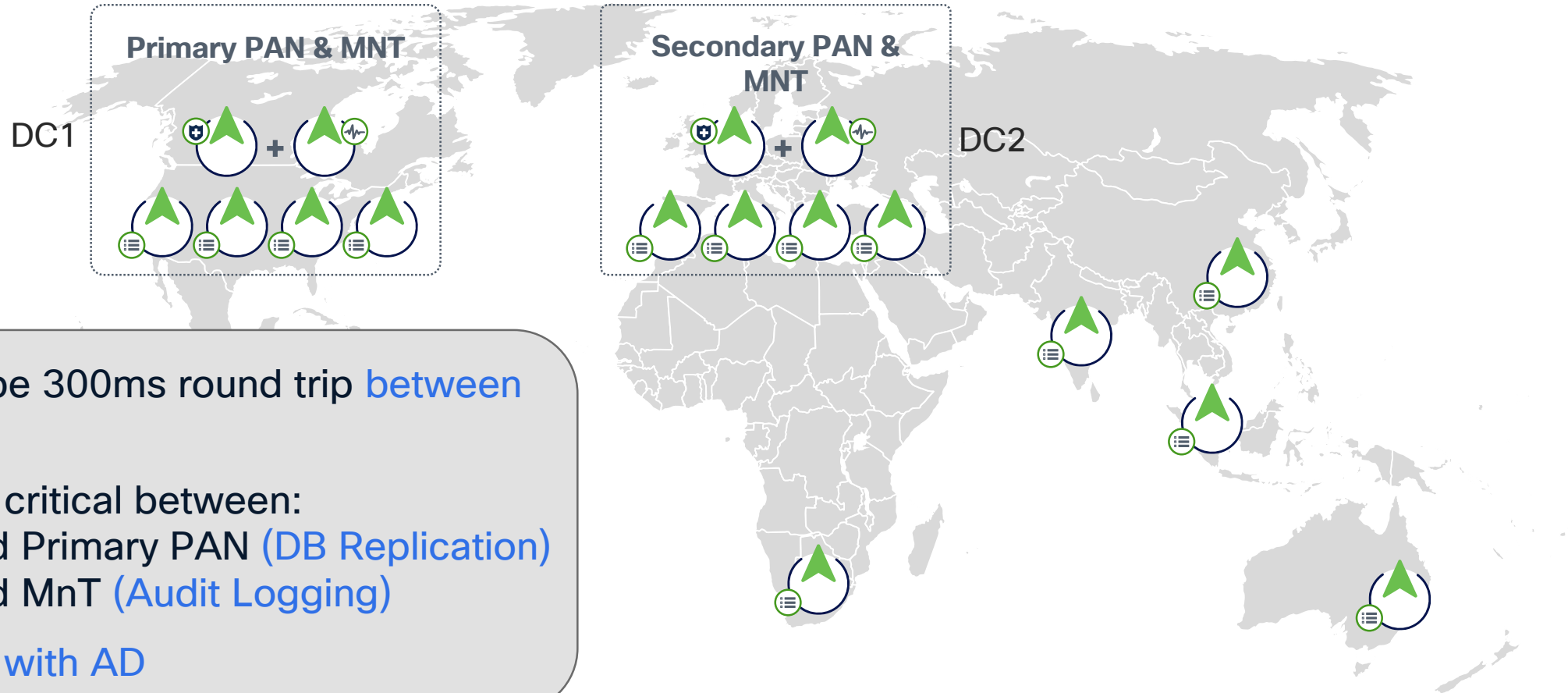


Large Deployment



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**

ISE Nodes – Mix and Match



Physical Appliances



SNS-3715
SNS-3755
SNS-3795

SNS-3615
SNS-3655
SNS-3695

Virtual Machines



Cloud Instances



Reminders

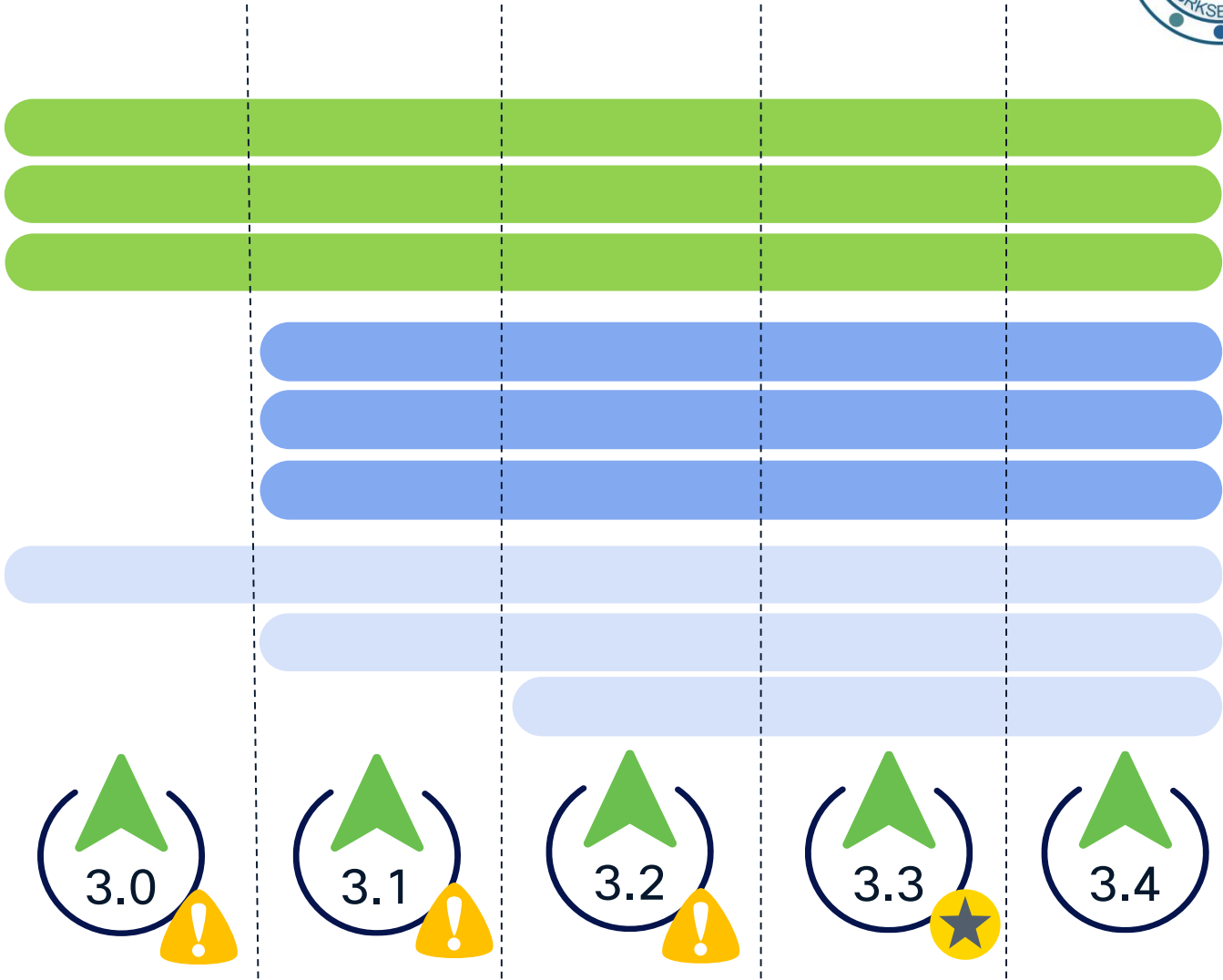
ISE platforms



SNS 3615
SNS 3655
SNS 3695

SNS 3715
SNS 3755
SNS 3795

Traditional VM
AWS
Azure & OCI



ISE Performance & Scale



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

 cs.co/ise-scale

Go to page to check for current numbers

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



Summary

Endpoints

Guests

Vulnerability

Threat



Total Endpoints ⓘ

1

Active Endpoints ⓘ

0

Rejected Endpoints ⓘ

0

Anomalous Behavior ⓘ

0

Authenticated Guests ⓘ

0

BYOD Endpoints ⓘ

0

AUTHENTIFICATIONS ⓘ



Identity Store Identity Group Network Device Failure Reason

No data available.



NETWORK DEVICES ⓘ



Device Name Type Location

No data available.



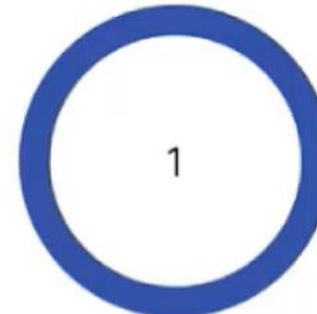
ENDPOINTS ⓘ



Profile Logical Profile

1

vmware-device - 100%



BYOD ENDPOINTS ⓘ



Type Profile

No data available.



ALARMS ⓘ



Severity Name Occu... Last Occurred

Name



ISE Authentication In... 388 8 mins ago

SYSTEM SUMMARY ⓘ



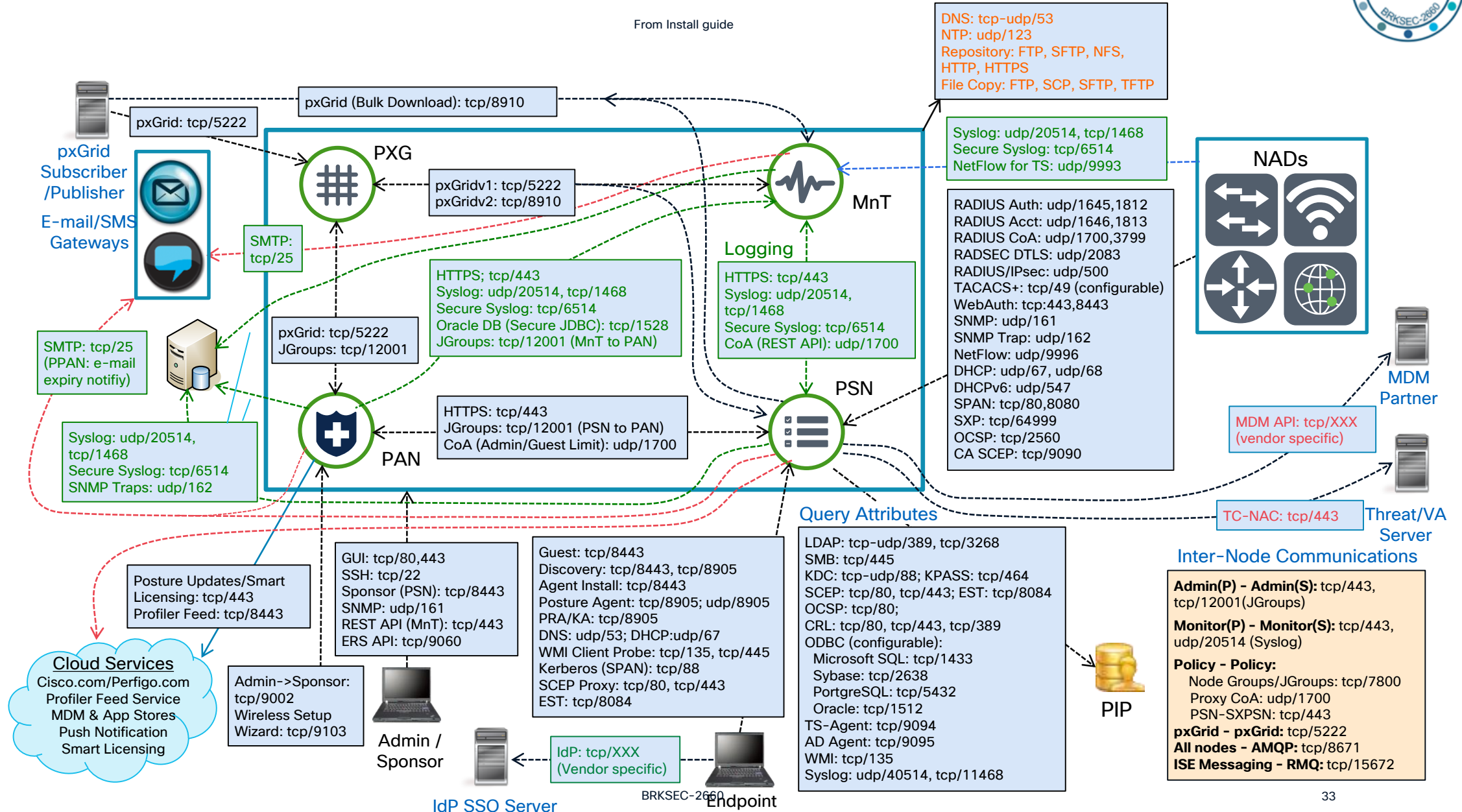
1 node(s)

All 24HR

ISE31-1ek

ISE Inter-Node Communications

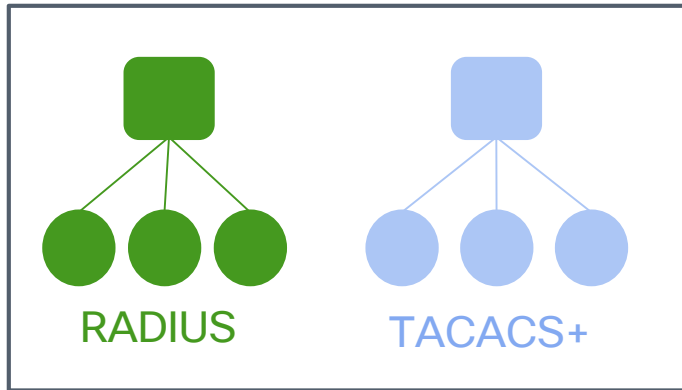
From Install guide



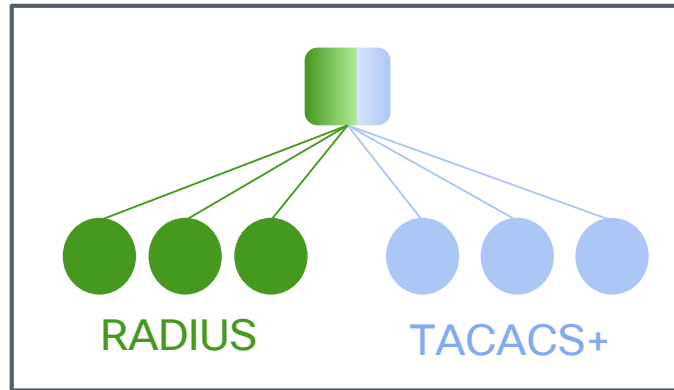
TACACS+ Deployment Models

Separating RADIUS & TACACS+ ISE Cubes?

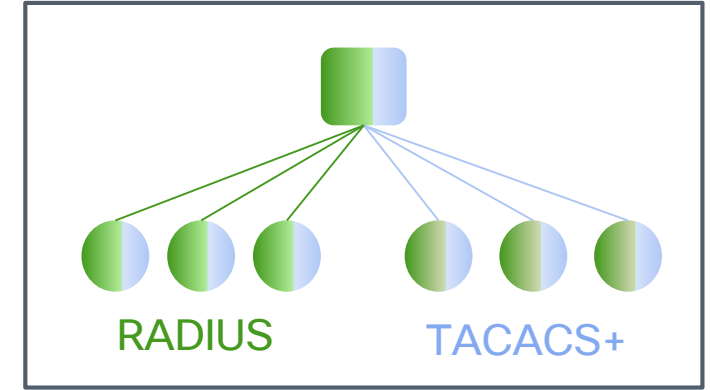
There are three different options:



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?

ISE Device Administration Prescriptive Deployment Guide



- 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

- [Introduction](#)
 - [About Cisco Identity Services Engine \(ISE\)](#)
 - [About This Guide](#)
- [Define](#)
 - [What is Device administration?](#)

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

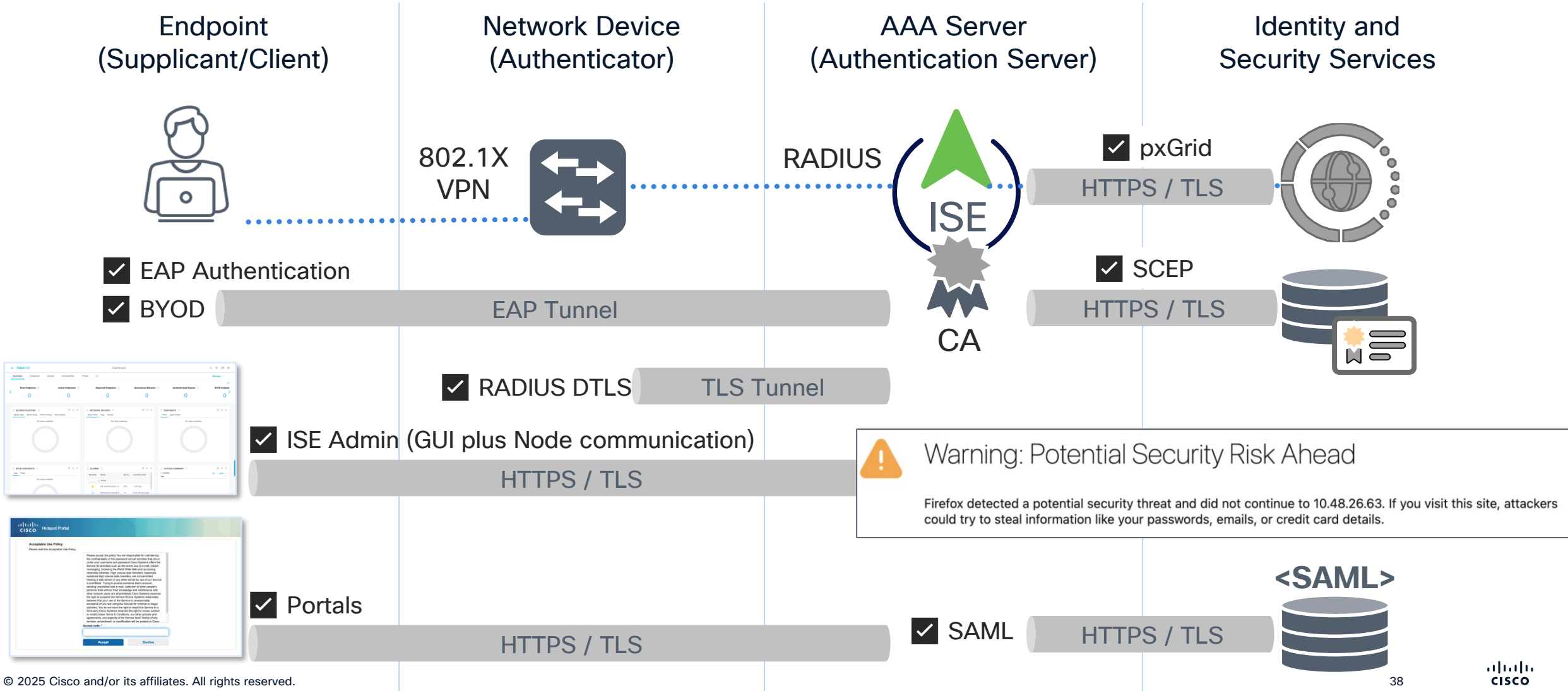
List of CAs

- 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

Different ISE System certificates



Systems and Trusted Certificates

System Certificates

⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Edit

+ Generate Self Signed Certificate

+ Import

Export

Delete

View

	Friendly Name	Used By	Portal group tag	Issued To	Issued By
✓ ISE30-1ek					
<input type="checkbox"/>	OU=Certificate Services System Certificate,CN=ISE30-1ek.example.com#Certificate Services Endpoint Sub CA - ISE30-1ek#00002	pxGrid		ISE30-1ek.example.com	Certificate Services Endpoint Sub CA -
<input type="checkbox"/>	Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ	ISE30-1ek.example.com	ISE30-1ek.example.com
<input type="checkbox"/>	Default self-signed saml server certificate - CN=SAML_ISE30-1ek.example.com	SAML			
<input type="checkbox"/>	OU=ISE Messaging Service,CN=ISE30-1ek.example.com#Certificate Services Endpoint Sub CA - ISE30-1ek#00001	ISE Messaging Se			

> ISE30-2ek

> ISE30-3ek

> ISE30-4ek

Which ISE role is using the certificate

Self signed certificate

EAP Authentication, Admin, Portal, RADIUS DTLS

ISE30-1ek.example.com

- > ISE30-2ek
- > ISE30-3ek
- > ISE30-4ek

Each ISE node has its own System Certificate Store

Trusted Certificates

⚠ For disaster recovery it is recommended to export and backup all your trusted certificates.

Edit

+ Import

Export

	Friendly Name	Trusted For	Serial Number	Issued To	Issued By
<input type="checkbox"/>	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA
<input type="checkbox"/>	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing Root...	Cisco Licensing Root...
<input type="checkbox"/>	Cisco Manufacturing CA SHA2	Infrastructure Endpoints	02	Cisco Manufacturing ...	Cisco Root CA M2
<input type="checkbox"/>	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2B ...	Cisco Root CA 2048	Cisco Root CA 2048
<input type="checkbox"/>	Cisco Root CA 2099	Cisco Services	01 9A 33 58 78 ...	Cisco Root CA 2099	Cisco Root CA 2099

To install certificate

Summary | Endpoints | Guests | Vulnerability | Threat | ➕

<

Total Endpoints ⓘ

1

Active Endpoints ⓘ

0

Rejected Endpoints ⓘ

0

Anomalous Behavior ⓘ

0

Authenticated Guests ⓘ

0

BYOD Endpoints ⓘ

0

AUTHENTICATIONS ⓘ

Identity Store | Identity Group | Network Device | Failure Reason

No data available.

NETWORK DEVICES ⓘ

Device Name | Type | Location

No data available.

ENDPOINTS ⓘ

Profile | Logical Profile

1

vmware-device - 100%

BYOD ENDPOINTS ⓘ

Type | Profile

No data available.

ALARMS ⓘ

Severity	Name	Occu...	Last Occurred
	▼ Name		
ⓘ	Configuration Changed	1	1 min ago

SYSTEM SUMMARY ⓘ

1 node(s) All 24HR

ISE31-1ek

Controlled Application Restart

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

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

Reboot must take place within 15 days

Set Restart Time

Scheduler

☐ Restart Now☒ Restart Later

Set Date

04/20/2023

Set Time

1:00

1:002:003:004:005:006:007:00

AM

Set Restart Time		Restart Now					All
<input type="checkbox"/>	Hostname	Personas	Role(s)	Services	Restart Time	Restart Status	
<input type="checkbox"/>	isebeta2	Administration, Monitoring	SECONDARY	NONE	Wed Apr 19 2023 6:00PM	Not Restarted	
<input type="checkbox"/>	isebeta3	Policy Service, pxGrid	SECONDARY	SESSION,PROFILER	Restart Now	Restarted	
<input type="checkbox"/>	isebeta4	Policy Service	SECONDARY	SESSION,PROFILER	Restart Now	Restarted	
<input type="checkbox"/>	isebeta5	Policy Service	SECONDARY	SESSION,PROFILER	Restart Now	Restarted	
<input type="checkbox"/>	isebetaadmin	Administration, Monitoring	PRIMARY	NONE	Wed Apr 19 2023 7:00PM	Not Restarted	

Improved Restart Time

~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

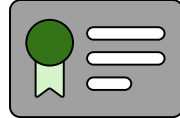
reload

ISE 3.4.0

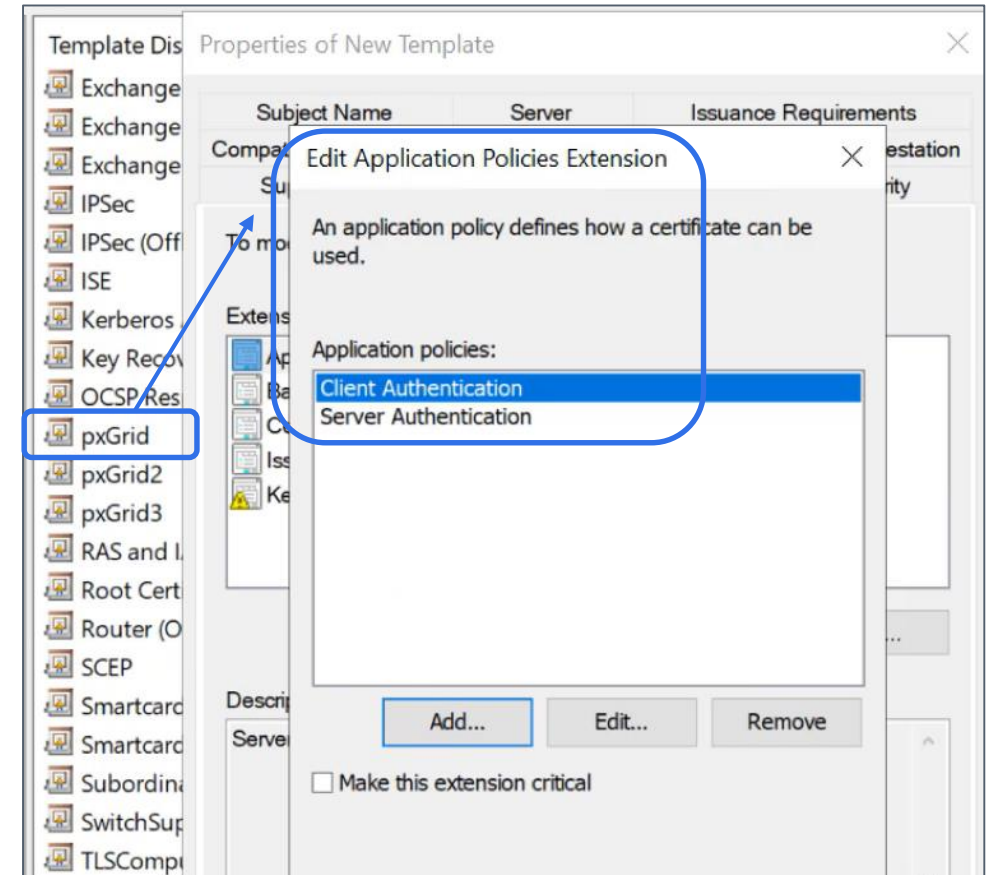


PxGrid Certificate

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



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



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	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec ²
	Minimum OS ³								
IE2000 IE3000	IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.2(4)EA6	✓	✓	✓	✓	X	✓	✓	✓
IE4000 IE5000	IOS 15.2(2)E5	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.2(4)E2	✓	✓	✓	✓	✓	✓	✓	✓
IE4010	IOS 15.2(4)EA6	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✓
SMB SG500	IOS 15.2(2)E5	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.2(4)E2	✓	✓	✓	✓	✓	✓	✓	✓
SMB SG500	IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✓
	Sx500 1.4.8.06	4	!	X	X	X	X	X	X
SMB SG500	Sx500 1.2.0.97	!	!	X	X	X	X	X	X
	IOS 15.2(2)E5	✓	✓	✓	✓	✓	✓	✓	✓

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

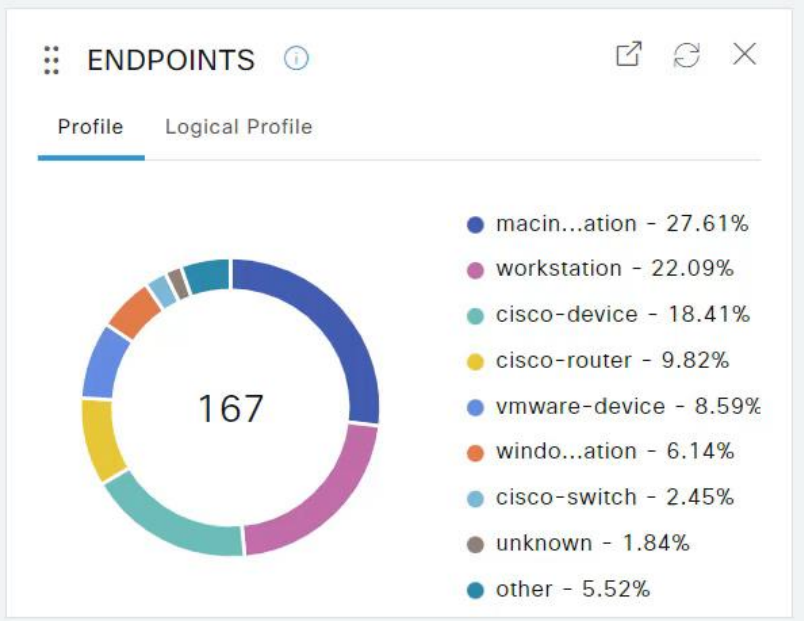
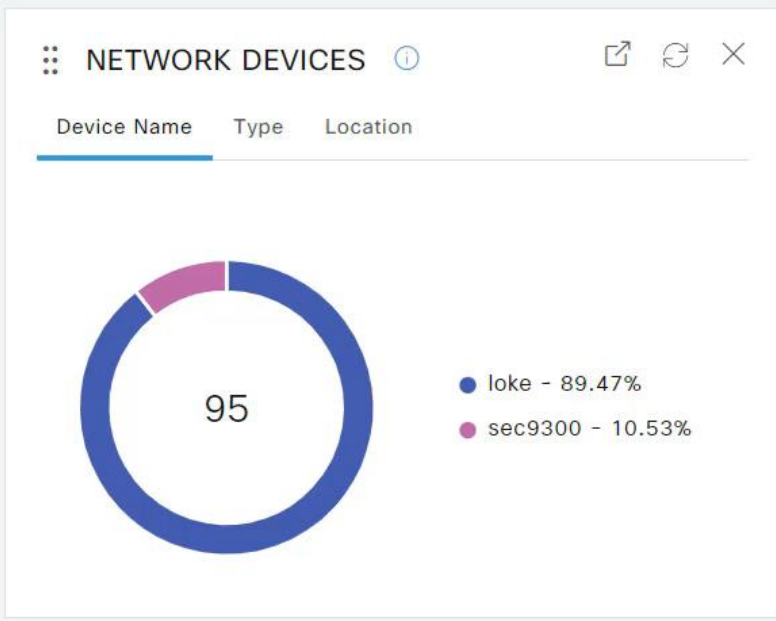
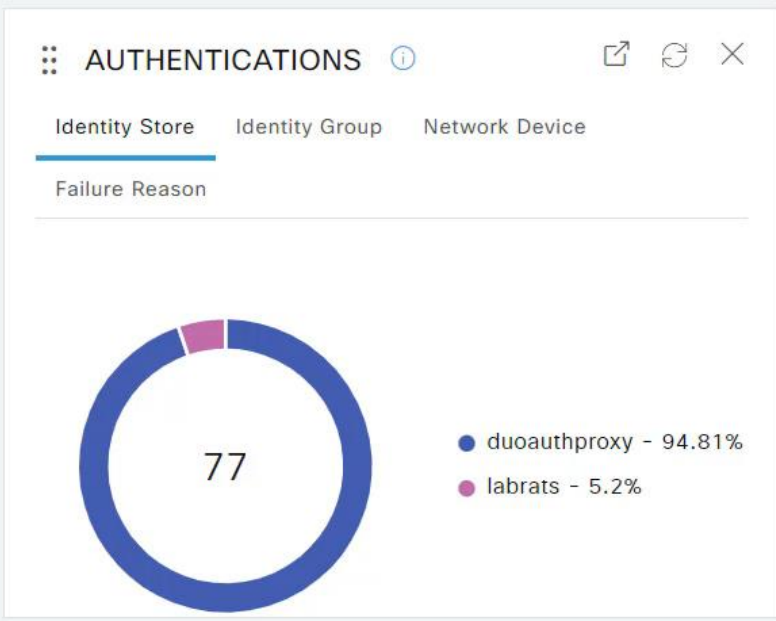
Total Endpoints 165

Active Endpoints 5

Rejected Endpoints 0

Anomalous Behavior 0

Authenticated 1



Default Network Device Groups (NDGs)

Network Devices

Network Device Groups

Network Device Profiles

Ext

Network Device Groups

All Groups

Choose group

Refresh

Add

Duplicate

Edit

Trash

Show group members

Imp

Name	Description
All Device Types	All Device Types
All Locations	All Locations
Is IPSEC Device	Is this a RADIUS over IP
No	Device is not IPSEC Type
Yes	Device is IPSEC Type

Default NDGs

Refresh

Add

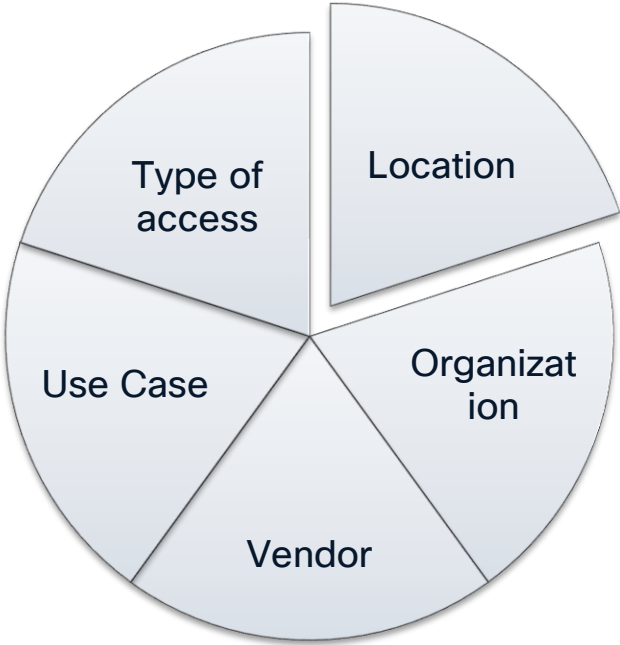
Duplicate

Edit

Name
> All Device Types
✓ All Locations
✓ AMER
✓ US
✓ San Jose
✓ Building
Floor
> Countries
> Departments
> Is IPSEC Device
> Orgs
> Regions

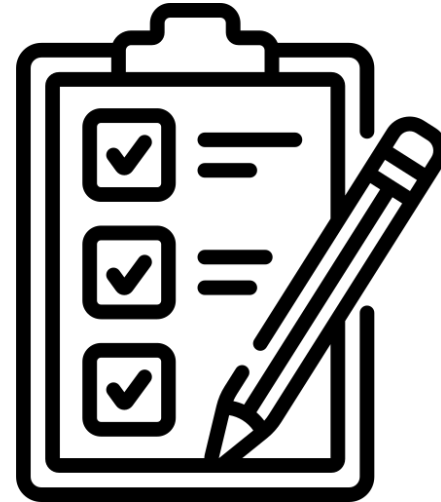
Maximum 6 Levels

Create Your Own Root NDGs



Additional Tips

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



Create ISE Network Access Device Profiles



- [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](#)

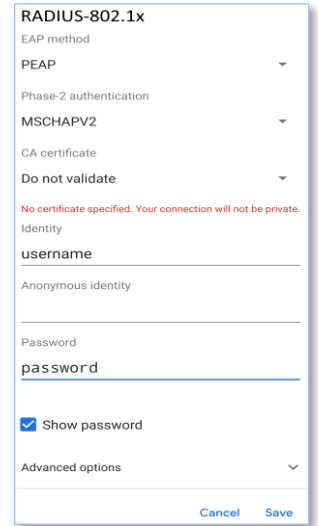
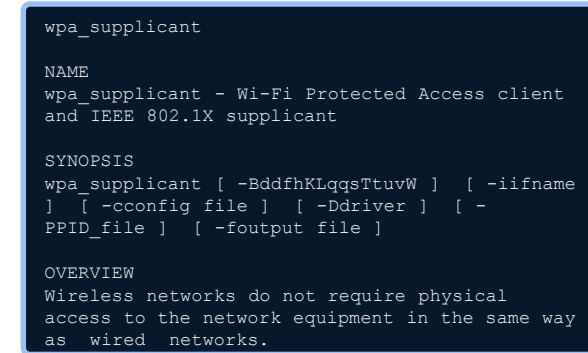
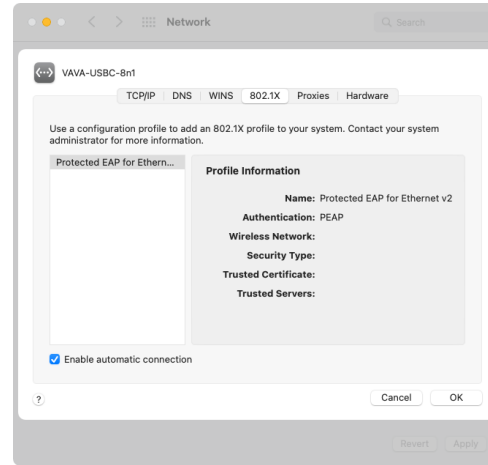
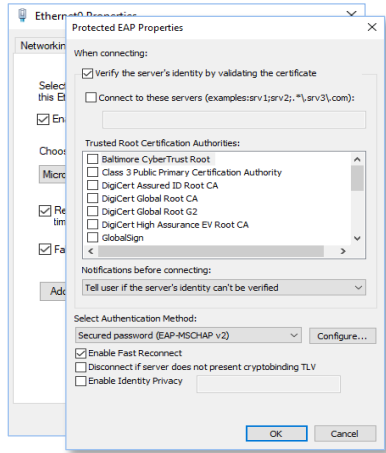


[how-to-create-ise-network-access-device-profiles](#)

The screenshot shows the Cisco Community page for the article 'How to Create ISE Network Access Device Profiles'. The page is part of the 'Security Documents' section. It features a 'Table of Contents' with links to various sections: Network Access Device Profiles, Steps To Create Custom Profiles, RADIUS Dictionaries, and Defining The Custom Profile. The 'Defining The Custom Profile' section is expanded, showing sub-links like 'Create New Profile Entry', 'Supported Protocols', 'RADIUS Dictionaries', 'Flow Type Conditions', 'Attribute Aliasing', 'Permissions', 'Change of Authorization (CoA)', and 'URL Redirect'. The page also includes a 'Find more resources' sidebar with links to discussions, blogs, events, and a 'Recognize Your Peers' section.

Supplicants

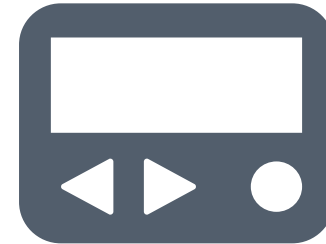
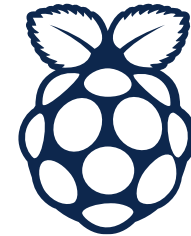
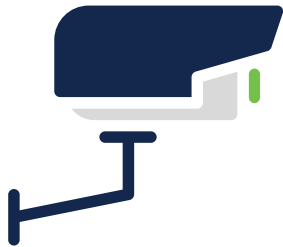
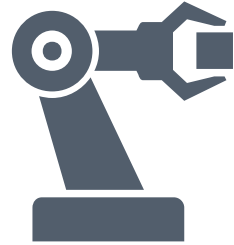
Endpoints: Native 802.1X Supplicants



- 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**

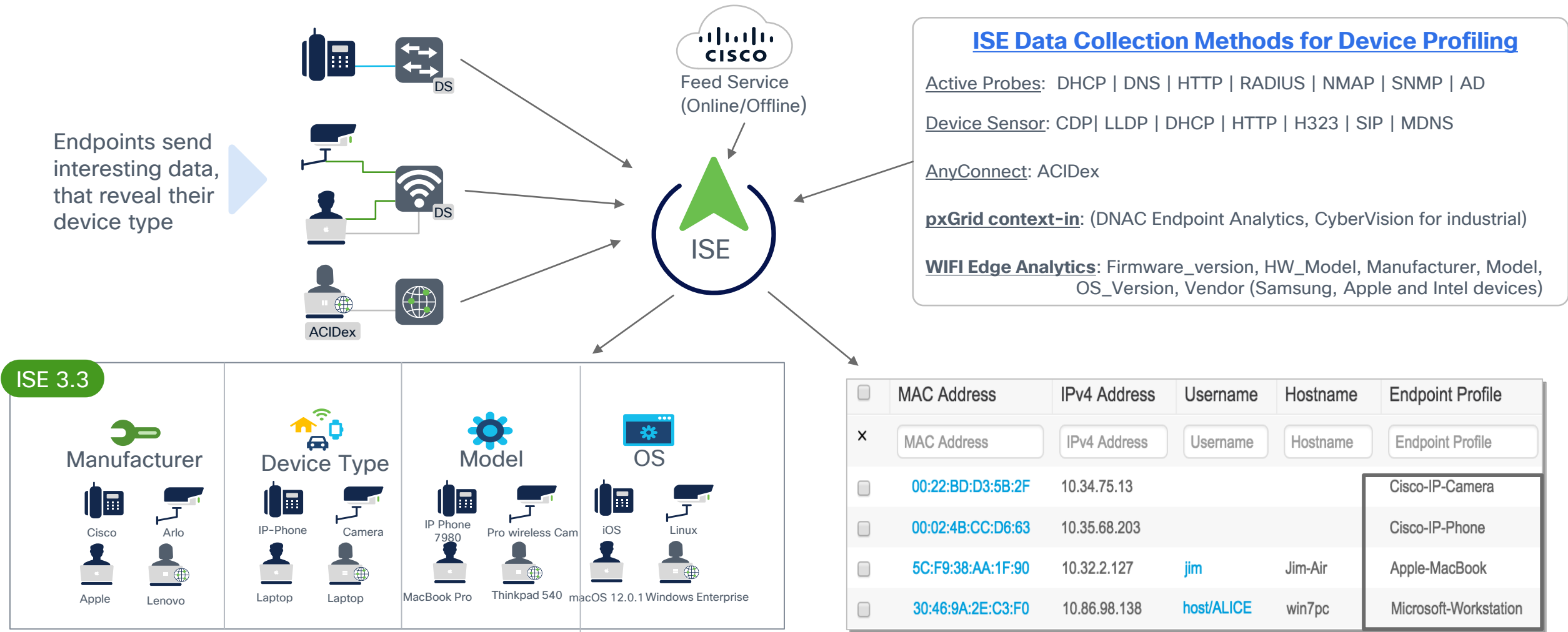
Profiling

Endpoints: Everything Else



Endpoint Profiling

The profiling service dynamically classifies devices connected to your network



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 IP Phone 9971	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



Windows 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 Device

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

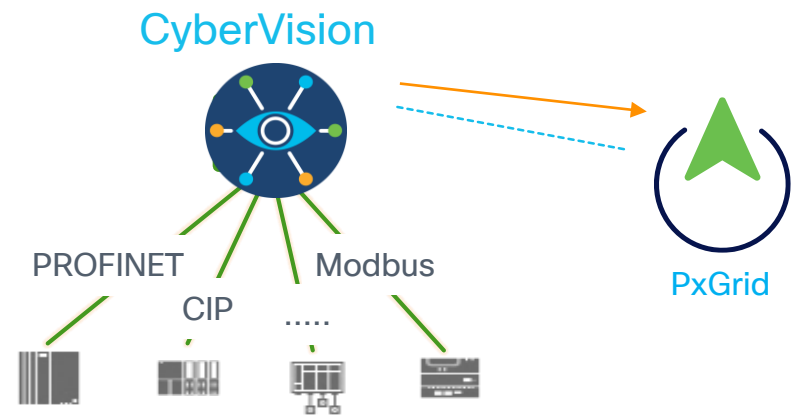
OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet, FQDN=test-printer1.zero0k.org, SNMP:hrDeviceDescr CONTAINS HP LaserJet P4015



Apple iPad

OUI = Apple, IP = xx.xx.xx.xx, IP:User-Agent contains iPad, FQDN=test-ipad1.zero0k.org

PxGrid Probe Context-in



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

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

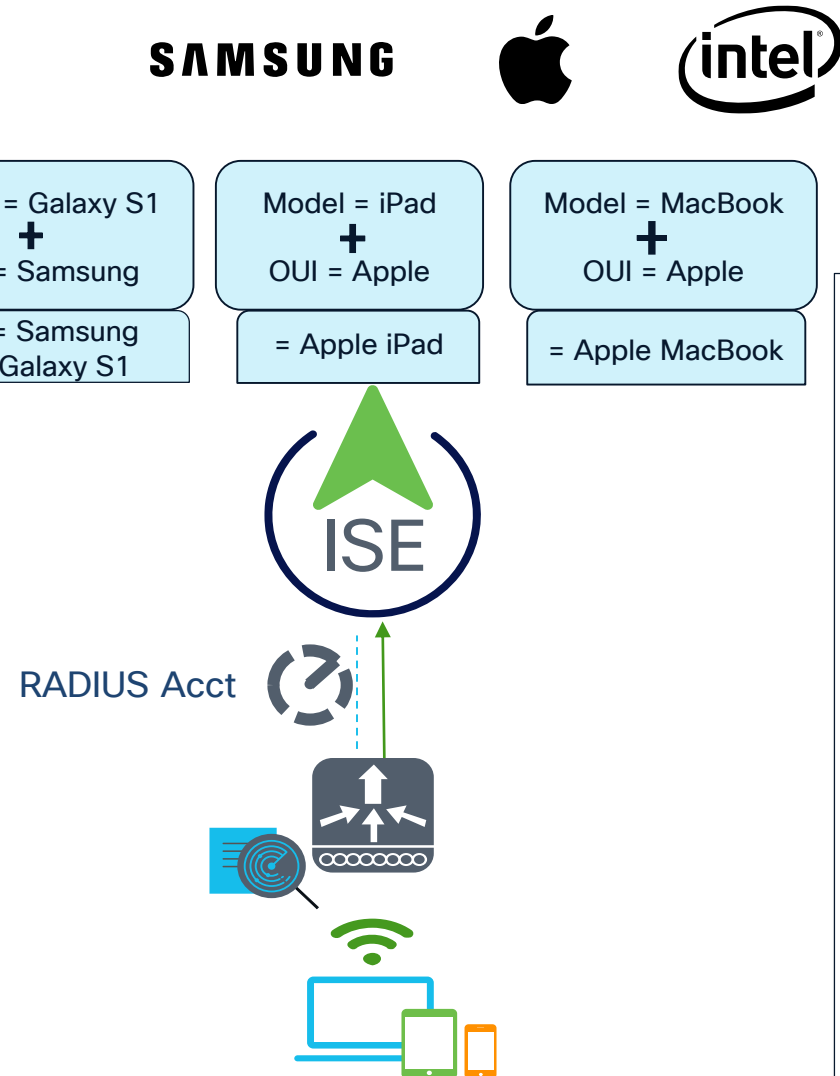


Wi-Fi Edge Analytics

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.



Dictionary Attributes

View

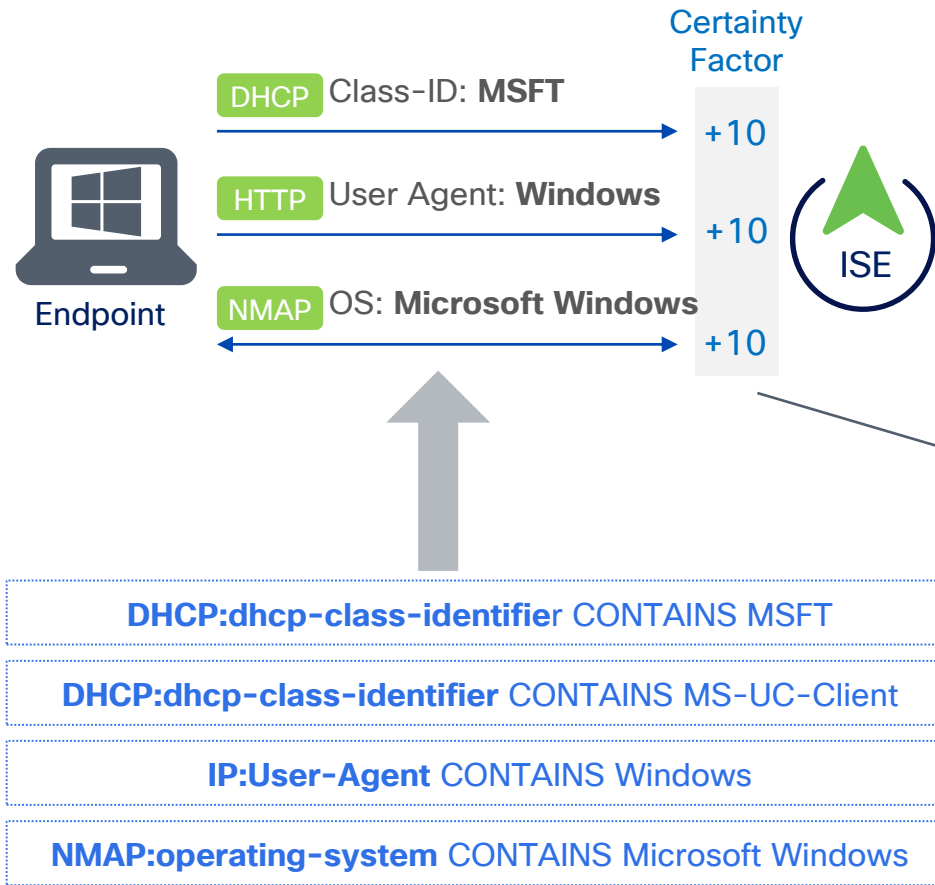
Name

- ☐ DEVICE_INFO_FIRMWARE_VERSION
- ☐ DEVICE_INFO_HW_MODEL
- ☐ DEVICE_INFO_MANUFACTURER_NAME
- ☐ DEVICE_INFO_MODEL_NAME
- ☐ DEVICE_INFO_MODEL_NUM
- ☐ DEVICE_INFO_OS_VERSION
- ☐ DEVICE_INFO_VENDOR_TYPE



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

ISE profiles definition



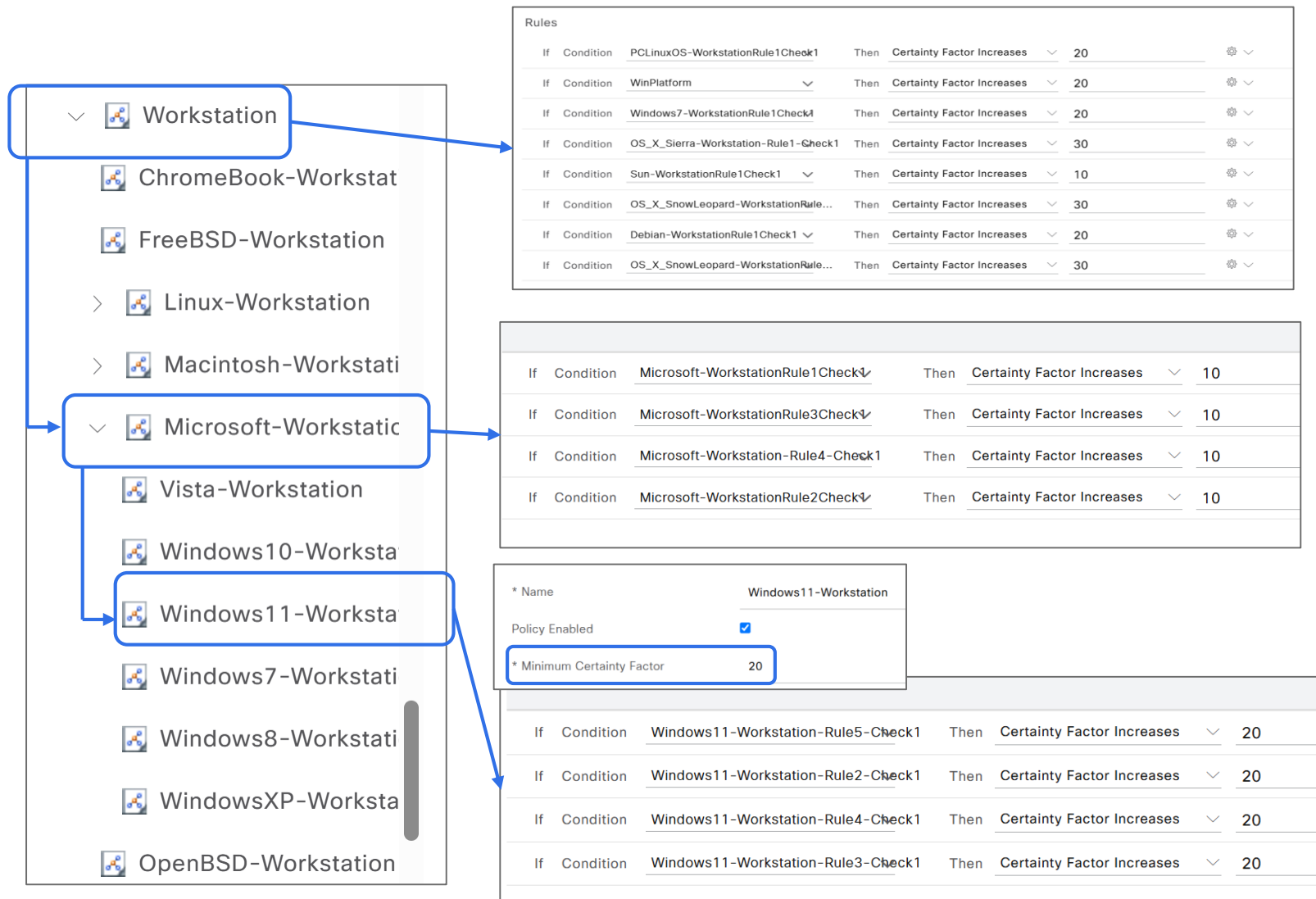
Profiler Policy List > Microsoft-Workstation

Profiler Policy

* Name	Microsoft-Workstation	Description	Generic policy for Microsoft workstation
Policy Enabled	<input checked="" type="checkbox"/>		
* Minimum Certainty Factor	10	(Valid Range 1 to 65535)	
* Exception Action	NONE		
* Network Scan (NMAP) Action	NONE		
Create an Identity Group for the policy	<input type="radio"/> Yes, create matching Identity Group <input checked="" type="radio"/> No, use existing Identity Group hierarchy		
Parent Policy	Workstation		
* Associated CoA Type	Global Settings		
System Type	Cisco Provided		
Rules			

If	Condition	Then	Value
Microsoft-WorkstationRule2Check1	Microsoft-WorkstationRule2Check1	Certainty Factor Increases	10
Microsoft-WorkstationRule4Check1	Microsoft-WorkstationRule4Check1	Certainty Factor Increases	10
Microsoft-WorkstationRule3Check1	Microsoft-WorkstationRule3Check1	Certainty Factor Increases	10
Microsoft-WorkstationRule1Check1	Microsoft-WorkstationRule1Check1	Certainty Factor Increases	10

Profile hierarchy



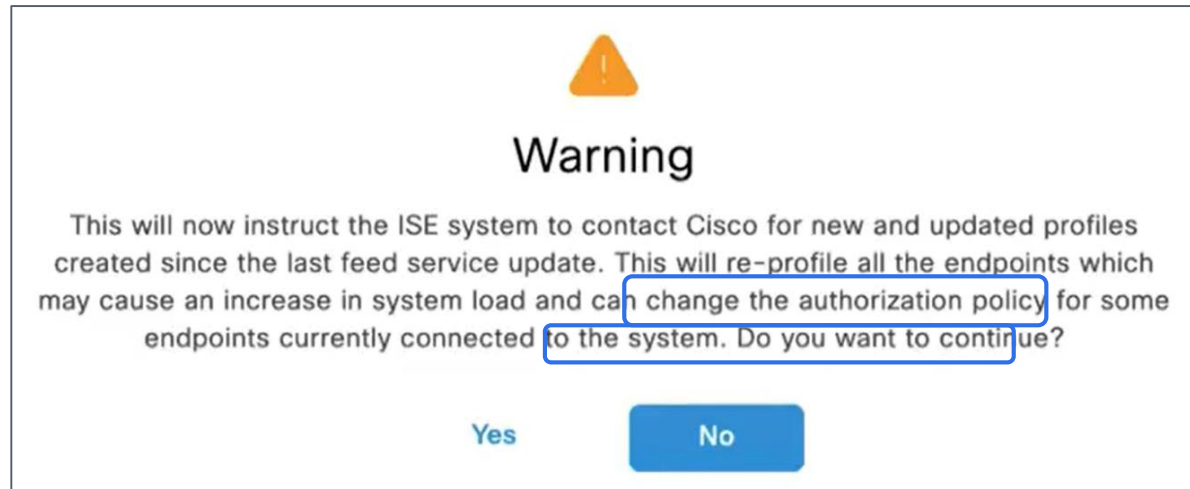
For one profile to be matched, the **endpoint** has to **match** also the profiles of **all the parents in the tree!**

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

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

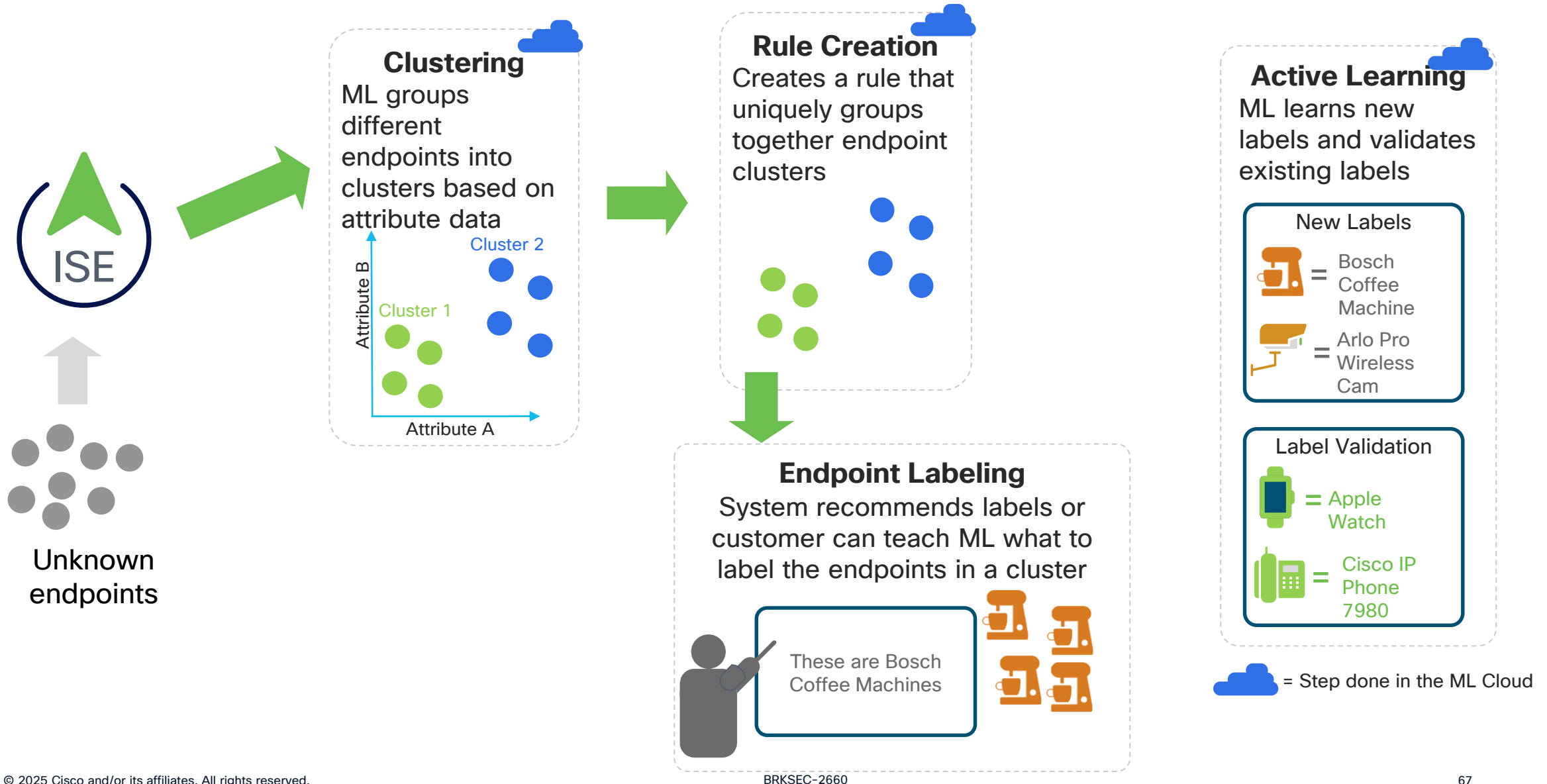
ISE Feed service Updates

- 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



Cisco AI Machine Learning Profiling

ISE 3.3



Review the AI Proposals

Identity Services Engine

Context Visibility / Endpoints

Search

Alerts

Help

Notifications

User

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Authentication

BYOD

Compliance

Compromised

Classification

Guest

Vulnerable

Hardware

5G

More

Manage

Hide Charts

ENDPOINT CATEGORIES

OUI

OS Types

Identity Group

353

apple, inc. - 22.66%

micro...ation - 21.25%

samsu...,ltd - 14.16%

sony ...ation - 8.5%

raspb...g ltd - 8.5%

google, inc. - 8.5%

asust... inc. - 7.08%

unknown - 6.52%

lexma... inc. - 2.83%

NETWORK DEVICES

Location

Type

Device Name

No data available.

AI PROPOSALS BETA

There are profiling policies suggested by Cisco AI cloud to help profile unknown endpoints on your network.

8

Proposed Profiling Rules

Review

Rows/Page

10

<<

1

/ 36 >>

Go

353 Total Rows

Refresh

Add

Edit

Trash

ANC

Change Authorization

Clear Threats & Vulnerabilities

Export

Import

MDM Actions

Release Rejected

Revoke Certificate

Filter

Settings

<input type="checkbox"/>	MAC Address	Anomalous Behavior	IP Address	Username	Hostname	Location	Endpoint Profile	Description	O
<input checked="" type="checkbox"/>	MAC Address	Anomalous Behavior	IP Address	Username	Hostname	Location	Endpoint Profile	Description	C
<input type="checkbox"/>	00:00:F0:0A:00:01		10.1.102.12	BRKSEC-2660	Cisco		Samsung-Device	68	Si
<input type="checkbox"/>	00:00:F0:0A:00:02		10.1.102.13		Cisco		Samsung-Device		Si

Choose the Proposal to View

Identity Services Engine

Context Visibility . Endpoints

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

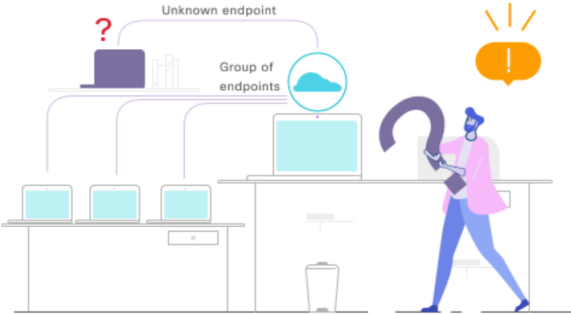
Work Centers

Interactive Features

Endpoints > AI Proposals

Help

Profile Unknown Endpoints with AI Proposals ^{BETA}



What are AI Proposals?

AI Proposals are a set of features that groups together endpoints with common attributes. It will propose classification rules and suggest relevant labels (you can also apply your own labels). Each group can contain endpoints that are classified by existing rules and unknown endpoints. Each endpoint can only appear in one group.

The percentages(%) in each column represent the percentage of endpoints that are profiled from system rules and custom rules.

Only unknown Endpoints would be profiled when you accept these rules. This would not affect any current profiles or rules in your network.

Hide

AI Proposals (7)

Endpoint Count	MFC-Endpoint Type	MFC-Hardware Manufacturer	MFC-Hardware Model	MFC-OS Type	Actions
30	-	Sony Corporation(100%)	-	-	View Proposal
80	Apple-Device(100%)	Apple, Inc.(100%)	-	-	View Proposal

Review the proposed labels

Context Visibility . Endpoints

Proposal Details for 80 Endpoints

Rule will apply the labels to all 80 endpoints in this group where they are not already filled by a system rule.

Edit or Accept the Proposed Labels for Unknown Endpoints

The unknown endpoints in this group will be profiled as the four labels below.

You can easily disable this rule under [Profiling Policies](#)

You must fill in at least one label and the profiling policy name in order to move to the next step.

MFC-Endpoint Type

Apple-Device

MFC-Hardware Manufacturer

Apple, Inc.

MFC-Hardware Model

MFC-Operating System


Profiling Policy Name*

MFC = Multi Factor Classification

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

BRKSEC-2660

70

 CISCO

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

All the MFC Attributes Can Be Used

Editor

Click to add an attribute

Equals

Select attribute for condition

Dictionary

EndPoints

▼

×

	Attribute	ID	Info
✓	EndPoints	LastAUPAcceptanceHours	i
🔗	EndPoints	LogicalProfile	i
🔗	EndPoints	MFCInfoEndpointType	i
🔗	EndPoints	MFCInfoHardwareManufact...	i
🔗	EndPoints	MFCInfoHardwareModel	i
🔗	EndPoints	MFCInfoOperatingSystem	i
🖨	EndPoints	OperatingSystem	i

Ready to Profile!

Identity Services Engine

Policy / Policy Sets

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

✓

Default

Default policy set

Default Network Access

13

> Authentication Policy(3)

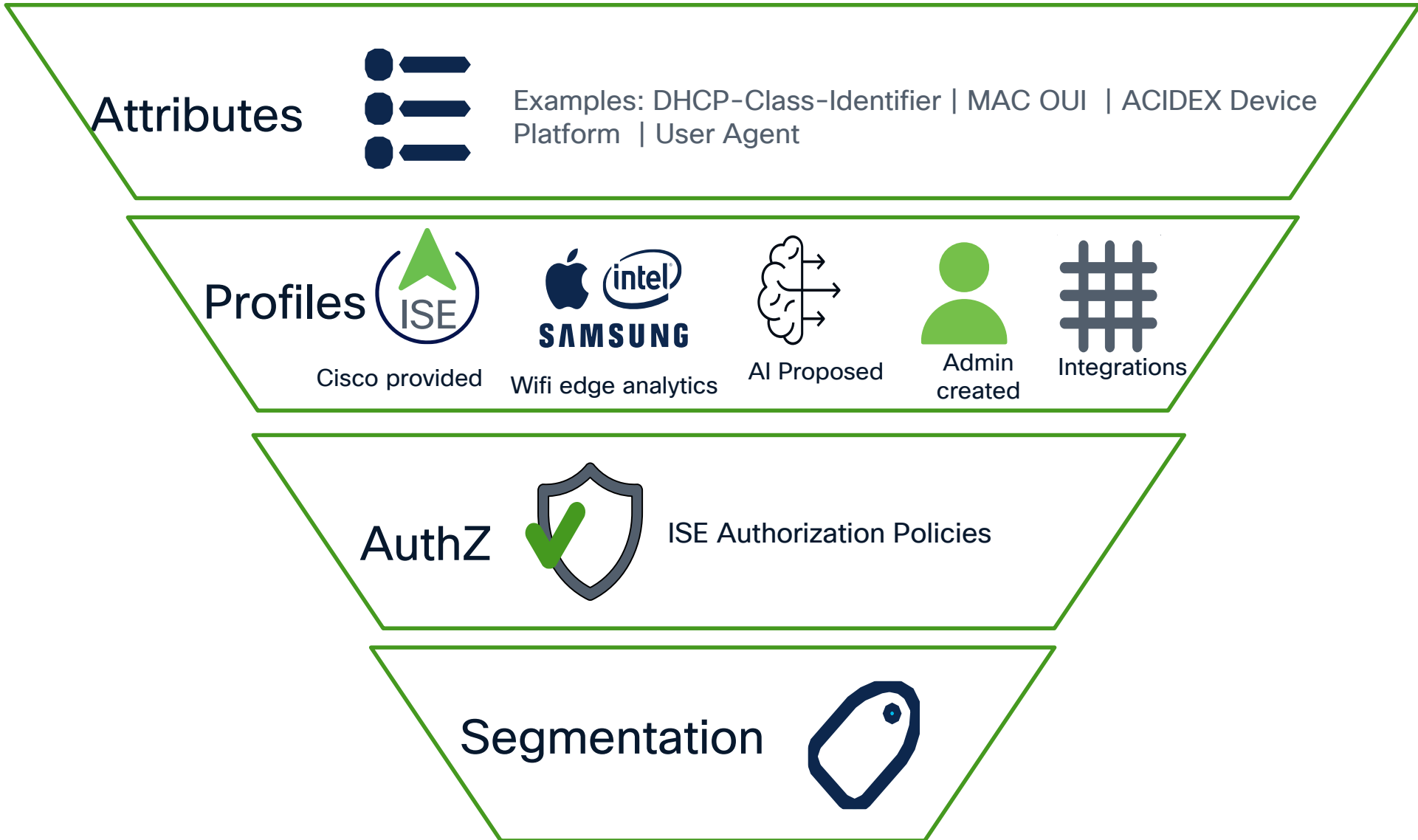
> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

∨ Authorization Policy(13)

					Results				
+	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions		
Search									
	✓	IOT Devices	EndPoints·MFCInfoEndpointType EQUALS IOT Device	IOT_ONLY ×	Select from list				
	✓	Wireless Block List Default	AND Wireless_Access IdentityGroup·Name EQUALS Endpoint Identity Groups:Blocked List	Block_Wireless_Access	Select from list	0			
	✓	Profiled Cisco IP Phones	IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Cisco_IP_Phones	Select from list	0			
	✓	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones	Select from list	0			
	×	Unknown_Compliance_Redirect	AND Network_Access_Authentication·Accessed BRKSEC-2660 Compliance_Unknown_Devices	Cisco_Temporal_Onboard	Select from list	73			

Turning Probes Into Profiles, Profiles Into Protection



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



- Introduction
 - About Cisco Identity Services Engine (ISE)
 - About this guide
- Cisco ISE Profiling Services
 - Solution Overview
 - Policy Architecture and Components
 - Scenario Overview
 - Network Topology
 - Guide Components
- Profiling Service Requirements
 - Licensing
 - Appliance Requirements
 - Network Requirements
- Profiling Services Global Configuration
 - ISE Profiling Global Configuration
 - Procedure 1 Configure Global Profiling Settings from the Policy Administration Node
 - Enable ISE Profiling Services
 - Procedure 2 Enable Profiling Services on the Policy Service Node
 - Procedure 3 Access and View the Profiling Configuration Page
- Configuring Probes
 - Probe Overview
 - Probe Configuration
- Profiling Using the RADIUS Probe
 - Configuring the RADIUS Probe
 - Procedure 4 Enable the RADIUS Probe in ISE
 - Procedure 5 Verify Access Device Is Configured in ISE
 - Procedure 6 Verify That Access Devices Are Configured to Send RADIUS to ISE PSN
 - Procedure 7 Verify RADIUS Probe Data
- Profiling Using the SNMP Trap Probe
 - Configuring the SNMP Trap Probe
 - Procedure 8 Enable the SNMP Trap Probe in ISE
 - Procedure 9 Add the Network Access Device to ISE
 - Procedure 10 Configure Access Devices to Send SNMP Traps to ISE Policy Service Node
 - Procedure 11 Verify SNMP Trap Probe Data
- Profiling Using the SNMP Query Probe

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

Endpoint Custom Attributes

Endpoint Attribute

Mandatory	Attribute Name	
	PostureApplicable	STRING
	LogicalProfile	STRING
	EndPointPolicy	STRING
	AnomalousBehaviour	STRING
	OperatingSystem	STRING
	BYODRegistration	STRING
	PortalUser	STRING
	LastAUPAcceptanceHours	INT

Cisco ISE pxGrid Direct for CMDDBs

ISE 3.2

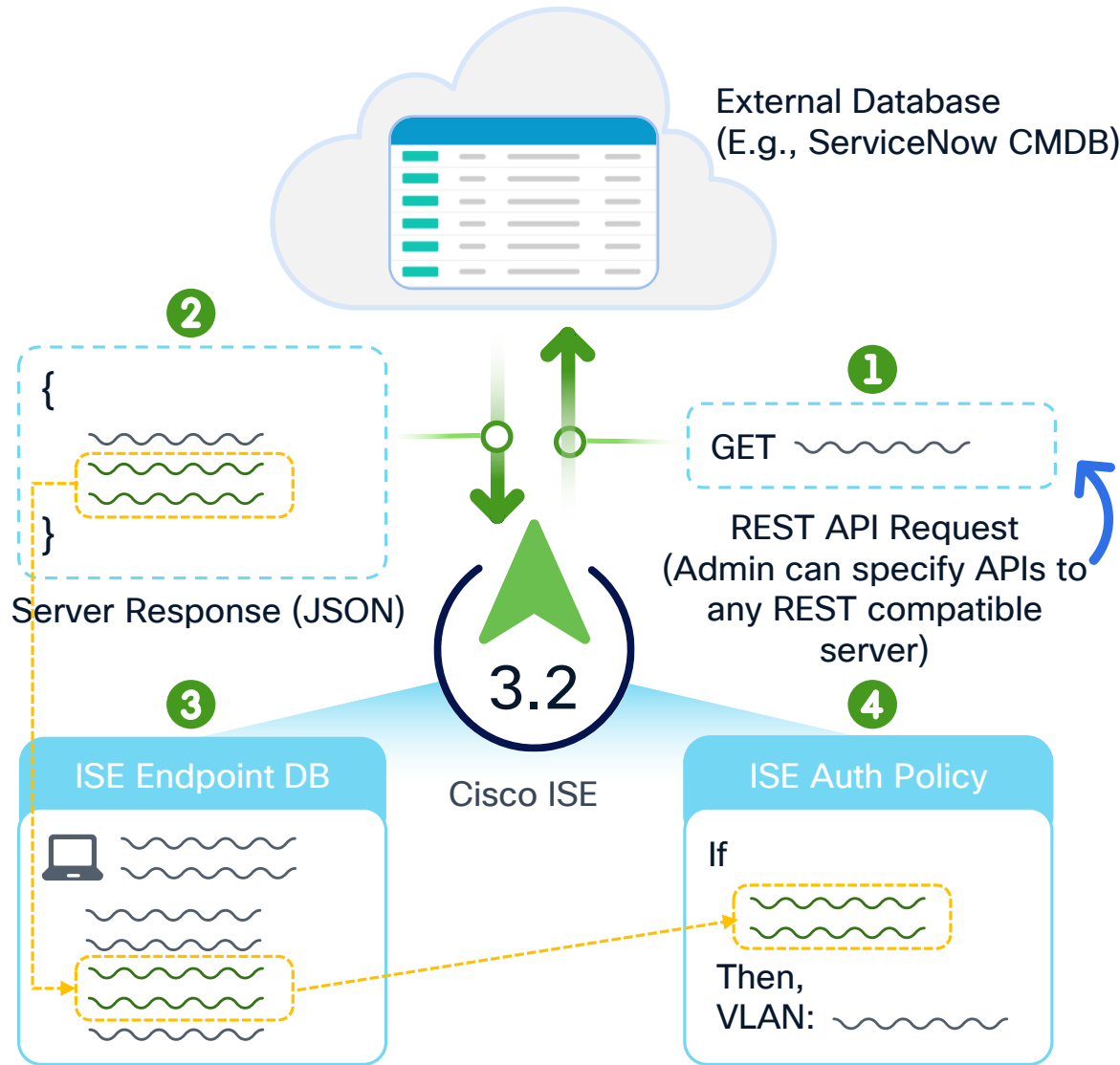


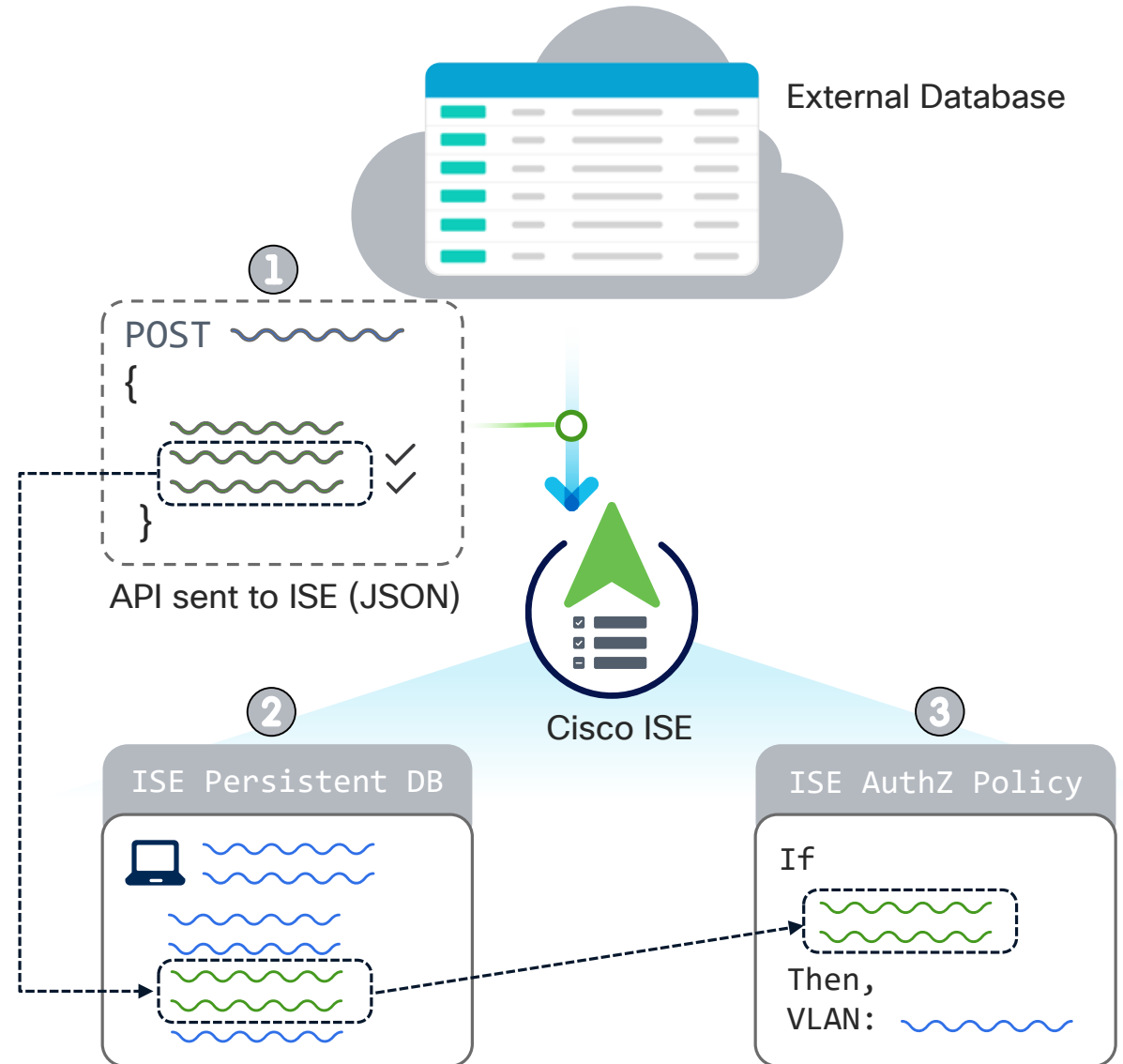
Diagram illustrating the JSON response structure for the REST API request, showing a list of system records with various attributes.

```
{
  "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"
    },
    { ... }
  ]
}
```

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)



- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration
- Work Centers
- Interactive Features

Summary

Endpoints

Guests

Vulnerability

Threat

Manage

Total Endpoints 32480

Active Endpoints 0

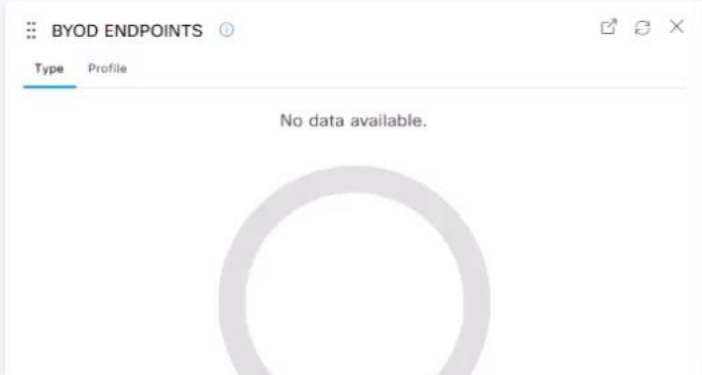
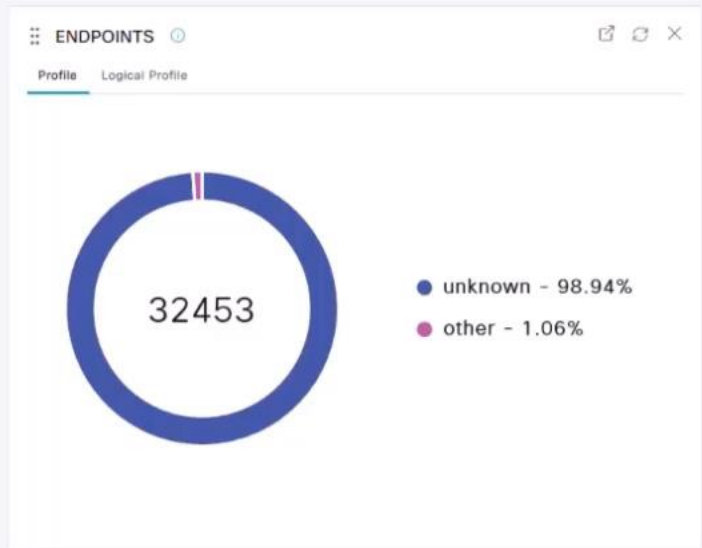
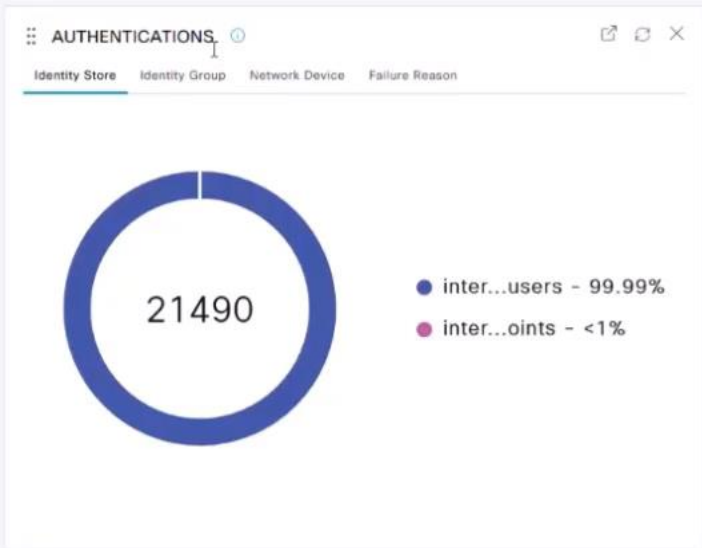
Rejected Endpoints 0

Anomalous Behavior 0

Authenticated Guests 0

BYOD Endpoints 0

Compliance 0



ALARMS

Severity	Name	Occu...	Last Occurred
	Name		
Warning	ISE Authentication In...	1652	7 mins ago
Warning	Log Collection Error	376	3 hrs 39 mins ago
Warning	Smart Licensing Auth...	25	3 hrs 44 mins ago
Error	BRKSEC-2660		
Error	Insufficient Virtual M...	28	11 hrs 22 mins ...

SYSTEM SUMMARY

1 node(s)

ise34ai

79

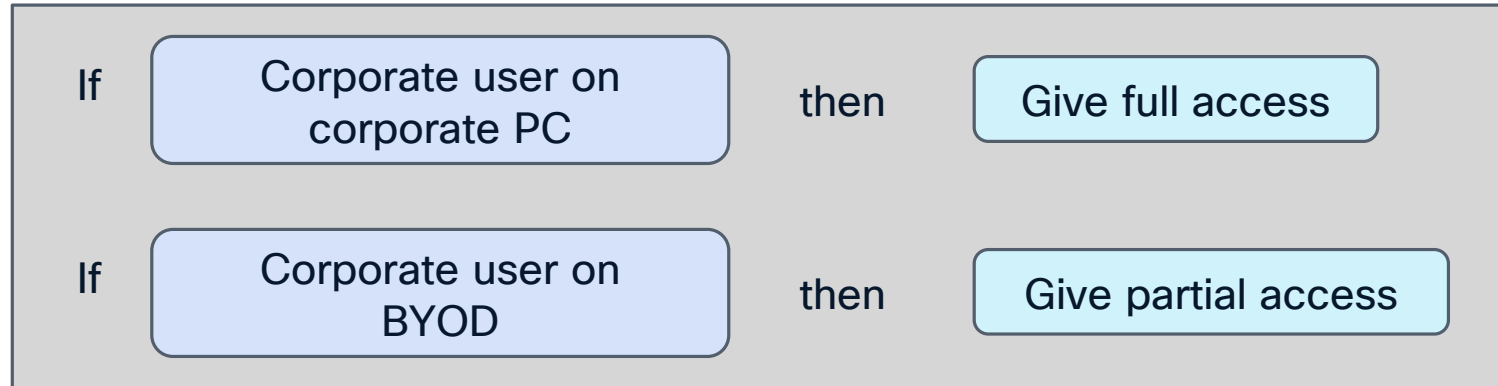
Policies

ISE Policy Logic

- Start from logic you want to implement. Then translate it in technical language

- All ISE policies use the same format: If condition then result

Examples:



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

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



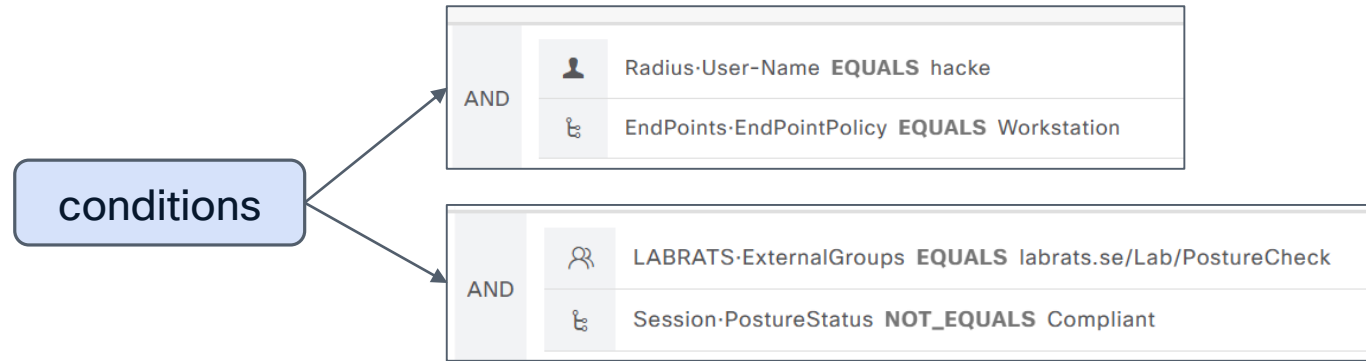
Vendor/Model



Access Type
(802.1x or MAB)

Status	Policy Set Name	Description	Conditions
			DEVICE-Location EQUALS All Locations#My-Territory#US#Sanjose#BLDG5
✓	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

ISE Conditions



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

Example:

The endpoint has to be



Conditions simplification

Pre-sets Dictionary
Condition are easy to
read and intuitive

✓	Computer Only	WIRED-MACHINE-DOT1X	WIRED-AD-ONLY x	∨ +
✓	IT Admin Access	WIRED-ADMIN-DOT1X	WIRED-ADMIN-ACCESS x	∨ +
✓	Employee Access	WIRED-EMPLOYEE-DOT1X	WIRED-EMPLOYEE-ACC... x	∨ +
✓	Vendor Access	WIRED-VENDOR-DOT1X	WIRED-GUEST-REDIRE... x	∨ +
✓	New Computer	Wired_MAB	WIRED-AD-ONLY x	∨ +
✓	Default		DenyAccess x	∨ +

Custom created
Conditions often are
not as intuitive



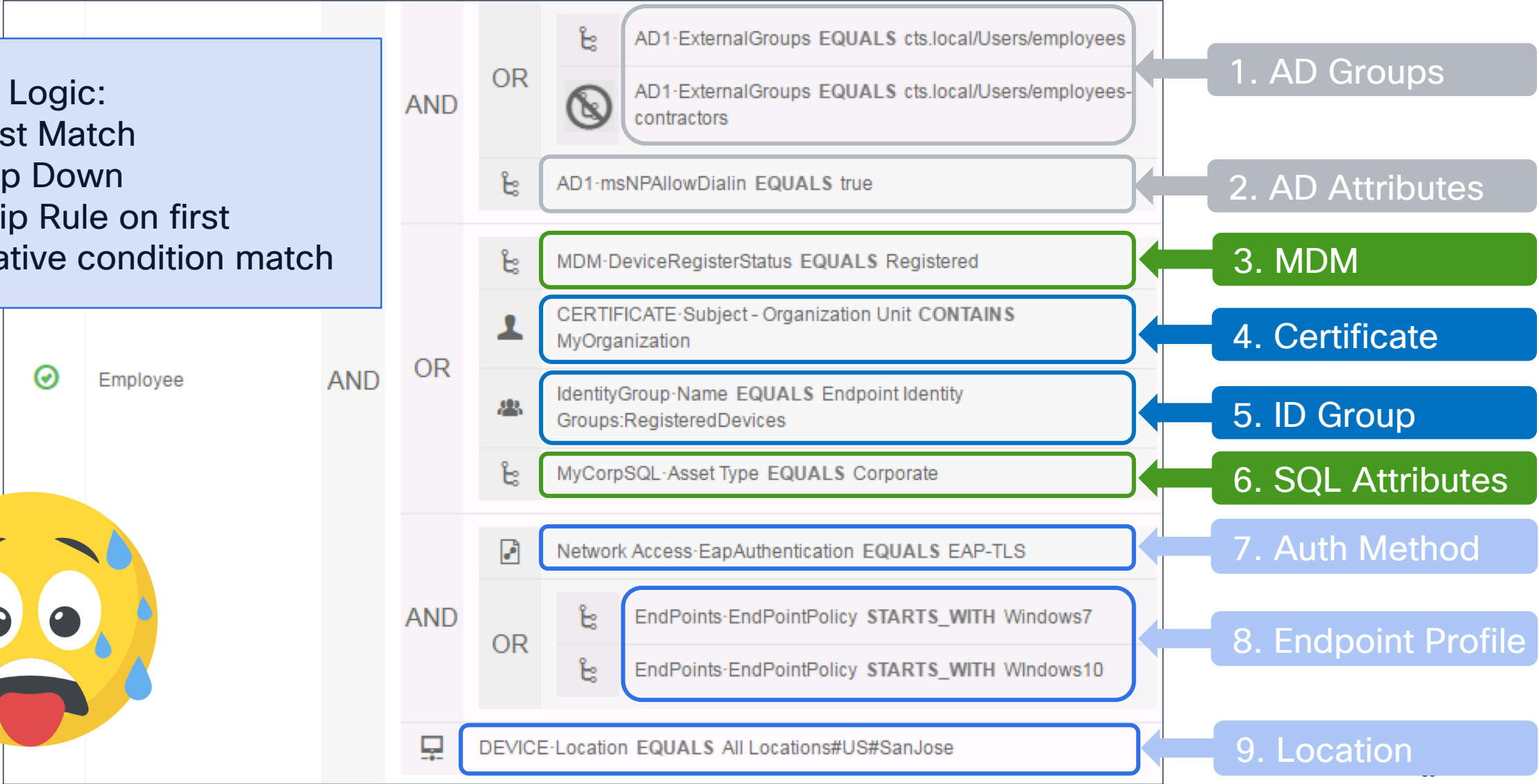
Use Compound
Conditions and
for custom ones

✓	Employee Access	AND	Radius:Service-Type EQUALS Framed		
			Radius:NAS-Port-Type EQUALS Ethernet		
			AD1:ExternalGroups EQUALS securitydemo.net/Users/Employees		WIRED-EMPLOYEE-ACC... x ∨ +
			Network Access:EapTunnel EQUALS PEAP		
			Network Access:EapAuthentication EQUALS EAP-TLS		
✓	Employee Access		WIRED-EMPLOYEE-DOT1X	WIRED-EMPLOYEE-ACC... x	∨ +

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

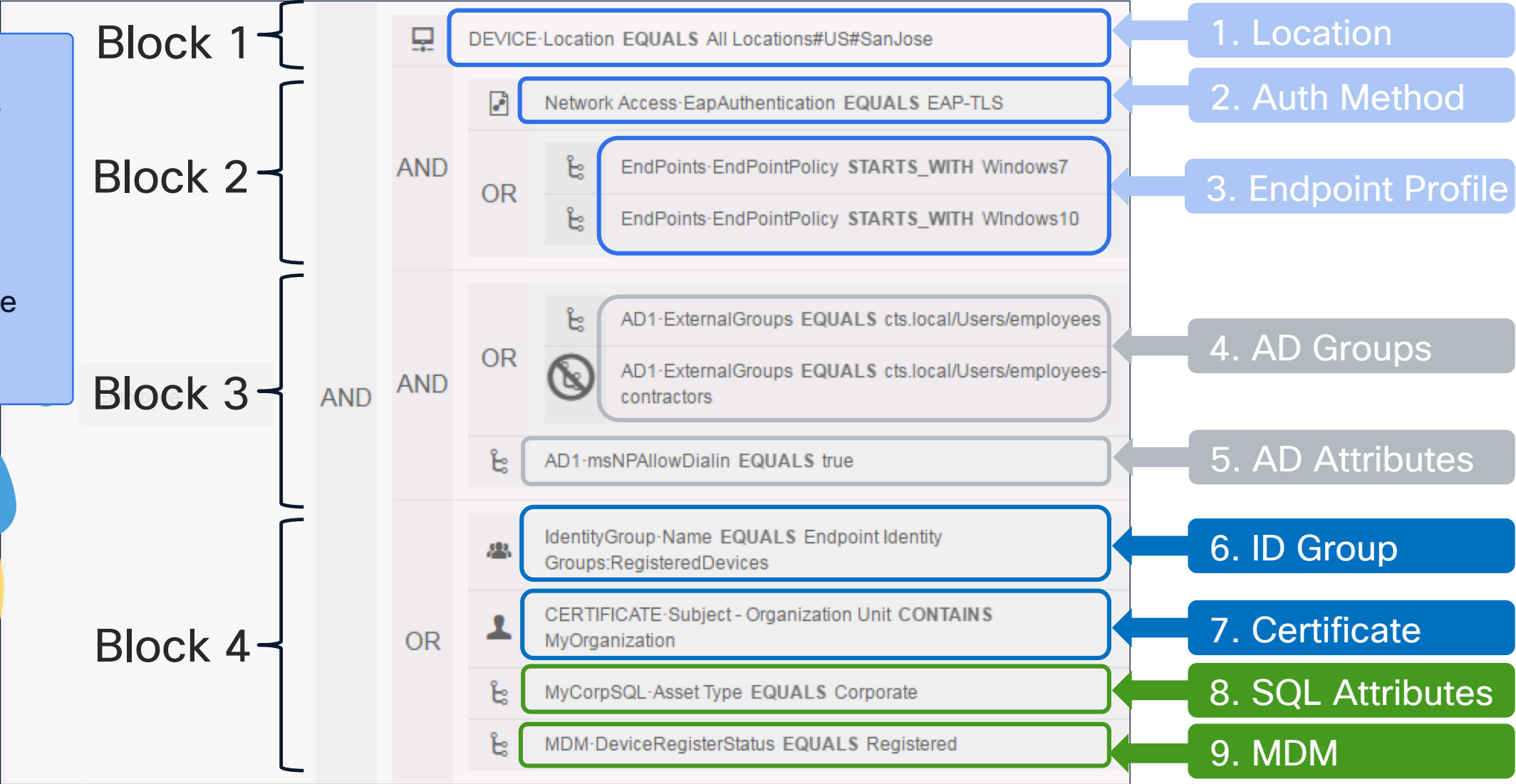
Total red stars = 2

Outer shape = Red triangle



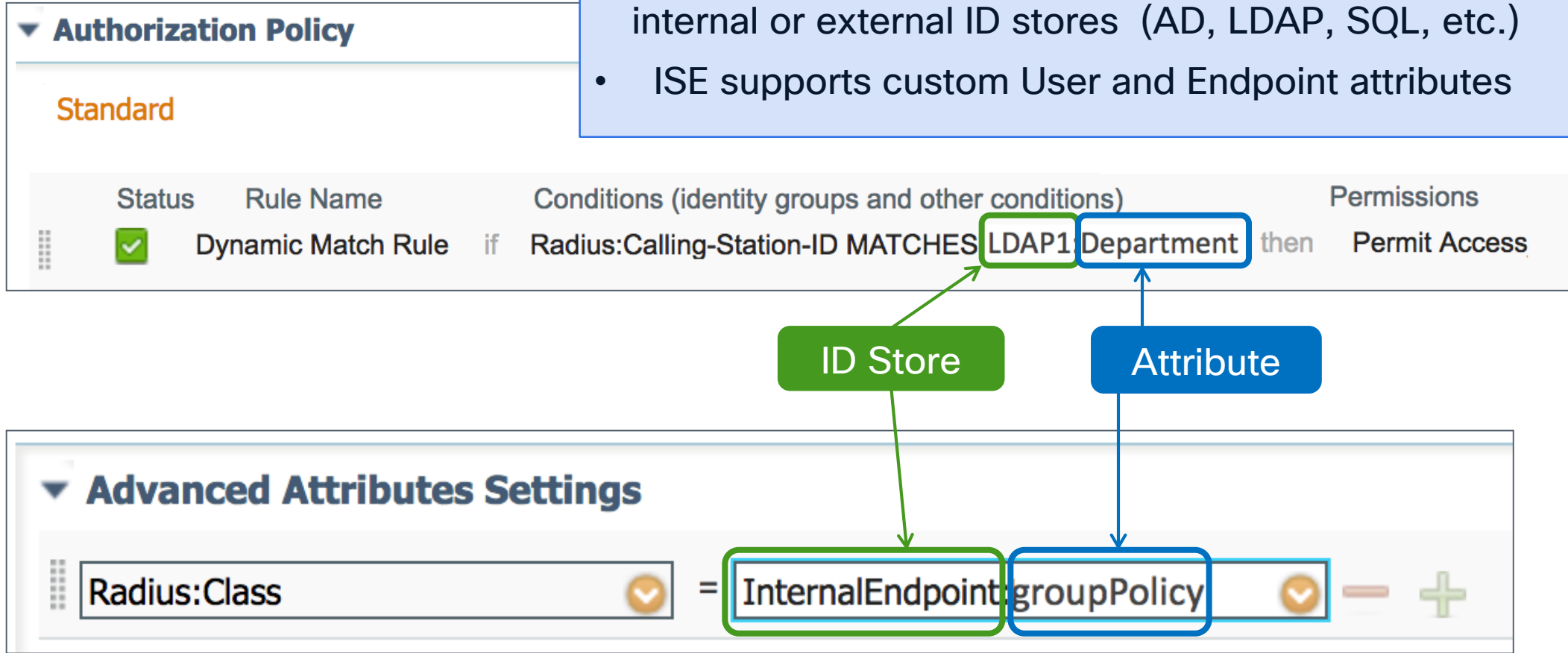
Auth Policy Optimization

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



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



Can you reorder some of the policy sets?

Review and Reorder

Policy Sets

Reset Reset Policyset Hitcounts Save

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input type="text" value="Search"/>								
	✓	territory-Policy-Set		territoryEndpoints	TEAP Network Access	641		
	✓	Intune_Integration		Network Access-Protocol EQUALS RADIUS	Default Network Access	5822		
				MDM-endpoints	Default Network Access	667		

Policy Sets									
+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View	
<input type="text" value="Search"/>									
	✓	Posture		win-posture-endpoints	Default Network Access	39734			
	✓	Intune_Integration		Network Access-Protocol EQUALS RADIUS	Default Network Access	5822			
	✓	MDM_Azure		MDM-endpoints	Default Network Access	667			
	✓	territory-Policy-Set		territoryEndpoints	TEAP Network Access	641			

Review & Reorder

The background of the slide is an abstract composition of numerous thin, flowing lines in shades of blue, yellow, orange, and purple, creating a sense of motion and energy. A large, semi-transparent white rectangle is positioned on the left side of the slide, serving as a backdrop for the main text.

Create your own lab

Who Needs an ISE Lab? You do!



Partners



Customers



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**

ISE Deployment and Operational Lifecycle



Provision

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



Deploy

Enable APIs
Repositories
Roles
Services
Certificates
Licensing 🤖
...



Configure

Identity Stores
Network Devices
Policy Sets
Endpoints
Portals
...



Operate

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



Extend

Terminate
...

ISE Eternal Evaluation

ISE Eternal Evaluation for Your Lab



https://github.com/1thomas/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](#).

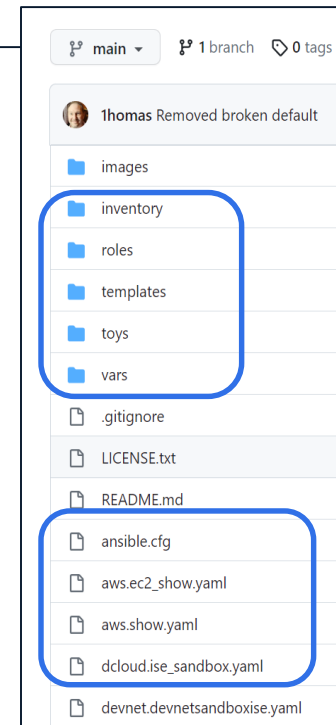
Quick Start

1. Clone this repository:

```
git clone https://github.com/1thomas/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](#).

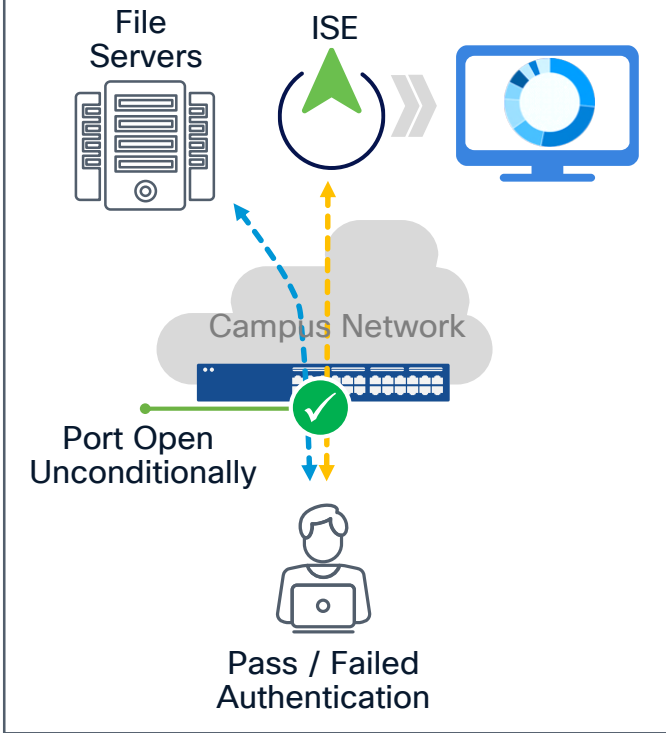


Ansible
playbooks

802.1x Deployment Modes

Deployment Modes

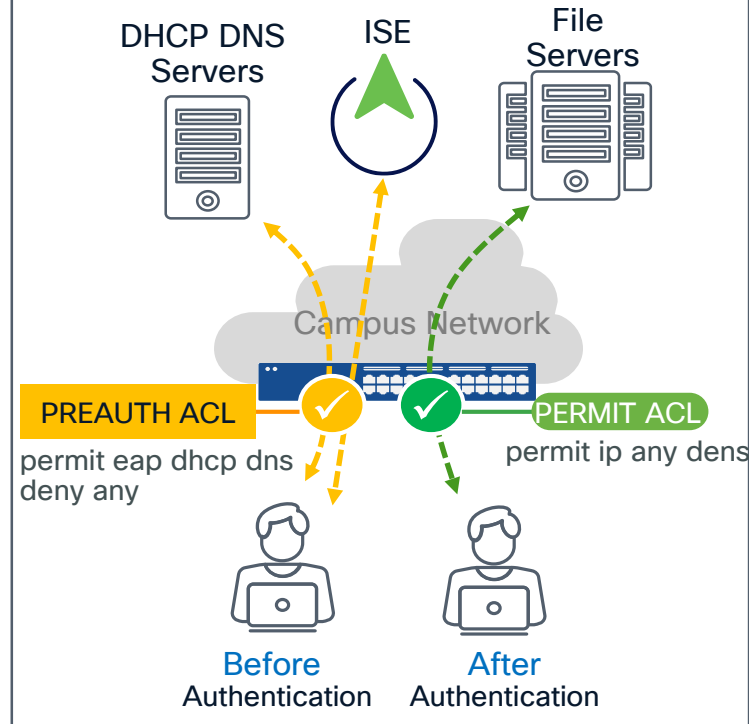
Monitor Mode (Visibility)



`authentication open`

No impact to existing network

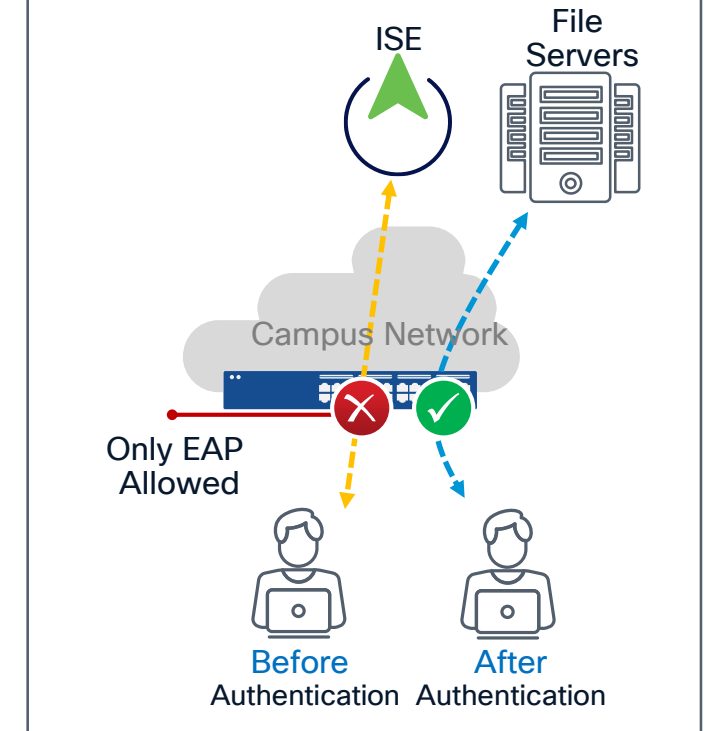
Low-Impact Mode (Visibility and Control)



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

Begin to control and differentiate access




















Closed Mode (Visibility and Control)



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

Utilizing Policy Sets with Modes

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

✓ VPN		DEVICE·Device Type EQUALS All Device Types#ASA-VPN-gateways	Default Network Access   
 Monitor Wired Access		DEVICE·Mode EQUALS Mode#MonitorMode	Default Network Access   
 Low Impact		DEVICE·Mode EQUALS Mode#LowImpact	Default Network Access   
 Closed Mode		DEVICE·Mode EQUALS Mode#ClosedMode	Default Network Access   

Day 2 Operations

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.

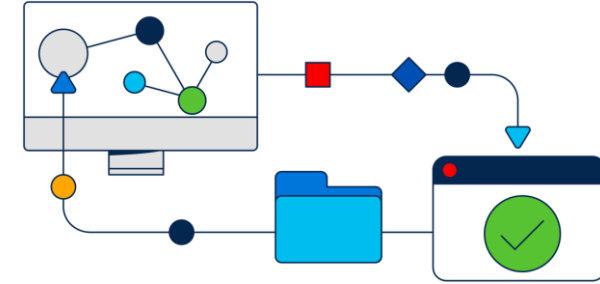
What is 802.1x ?
IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

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					

Supporting ISE After Deployment

- Train Your Support with A Playbook for common issues
- Document as much as possible!
 - ✓ Policy Configuration
 - ✓ Supplicant Configuration
 - ✓ Network Access Devices
- Many document templates available on ISE Communities



Wrap up

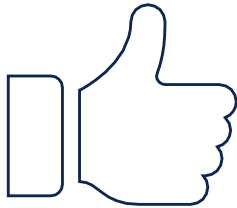
Deploying any network access control solution is **crucial** but it **isn't easy....**

Proper planning is **essential** to any **successful** development.



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

Cisco ISE & NAC Resources

Labels: AAA Identity Services Engine (I...) Policy and Access TrustSec VPN

135846 VIEWS 110 HELPFUL 0 COMMENTS

Create Please login to create content

Discussion + Video Blog Document Project

Related Content

Discussions - Blogs - Events Videos Projects

Recommended for you

Spark Developer resources Cisco ISE お役立ちリンク集 - Identity Services Engine - ISE with Threat Centric NAC dCloud past Webinar resources list Threat Centric NAC w/ AMP

Community Helping Community UNICEF

Start

- Download ISE Software
- Patch your ISE Deployment
- Configure NTP
- Configure a repository
- Schedule Backups
- Integrate Active Directory
- Set up Network Device Groups
- Configure Posture Updates
- How to Ask The Community for Help

Software

- Download ISE Software & Patches
- How to Get ISE Evaluation Software & Licenses
- How to Submit an ISE Feature or Enhancement Request
- ISE Software Release Lifecycle Product Bulletin
- How to Get Software Release Notifications
- ISE EoL and EoS Notices



Cisco ISE - Identity Services Engine

@CiscoISENetworkSecurity

16.8K subscribers

ISE Webinars

Cisco ISE - Identity Services Engine

57 videos 5,063 views Last updated on Dec 14, 2022

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!



FIND A COMMUNITY Buy or Renew Cisco Community

FOR REFERENCE BRKSEC-2660

This board Search Network Access Control

Technology & Support For Partners Customer Connection Webex Events Members & Recognition

Cisco Community / Technology and Support / Security / Network Access Control

ISE Start Design Deploy Integrate Learn

This community is for technical, feature, configuration and deployment questions. For production deployment issues, please contact the TAC! We will not comment or assist with your TAC case in these forums. Please see How to Ask the Community for Help for other best practices.

Network Access Control

Cisco Access Control Server (ACS), Identity Services Engine (ISE), Zero Trust Workplace

Labels < Previous Next >

AAA (16,051) Access Control Server (ACS) (287) ACI (10) AnyConnect (3) APIs (60) Appliances (25) Buying Recommendation (12) BYOD (78) Catalyst 2000 (1) Catalyst 9000 (2) Catalyst Wireless Controllers (1) Cisco Adaptive Security Ap... (6) Cisco Firepower Device Ma... (2) Cisco Firepower Manageme... (2) Cisco Software (4)

< Previous 1 2 3 ... 1939 Next >

 ISE 3.0 patch 4, Cat sw 9200 7.3.1 Wire Redirect fail
by KelvinT on 01-26-2022 12:19 PM · Latest post on 01-26-2022 03:49 PM by Arne Bier
3 REPLIES 0 HELPFUL 61 VIEWS

 MAB / Voice Authentication
by wizi on 01-21-2022 02:05 PM · Latest post on 01-26-2022 03:17 PM by Arne Bier
4 REPLIES 5 HELPFUL 274 VIEWS

 cisco ise 2.3 command set & shell profile can work together?
by shlomo on 01-24-2022 09:54 AM · Latest post on 01-26-2022 01:56 PM by Greg Gibbs
5 REPLIES 5 HELPFUL 194 VIEWS

 ISE recommended thresholds
by shubhampatki1994 on 01-26-2022 10:05 AM
0 REPLIES 5 HELPFUL 56 VIEWS

 ISE 2.6 Licensing Reports
by rsharp001 on 01-12-2021 10:43 AM · Latest post on 01-26-2022 05:06 AM by PERL_Admin
5 REPLIES 5 HELPFUL 1434 VIEWS

Ask a Question

Create
+ Discussion + Blog + Document
+ Video + Project Story

Find more resources

Discussions Videos
Blogs Project
Documents Gallery
Events
New Community Member
Guide

Featured Projects

From Stateful Firewalling to Next Generation Firewall
by Narayan Dev Sarma

The Importance of the Human

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.

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

Thank you

CISCO Live !

