

The background features a vibrant, abstract design with a color gradient from dark blue on the left to bright yellow and white on the right. The design consists of overlapping, wavy horizontal bands and a radial pattern of lines emanating from a bright white point on the right side, creating a sense of motion and energy.

CISCO *Live!*

Let's go



The bridge to possible

ISE Planning, Staging and Deployment

Francesca Martucci

Technical Solutions Architect, Cybersecurity EMEA



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

Antoine de Saint-Exupéry

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

What needs to be included in my planning?



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



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

Who am I?

Technical Solutions Architect

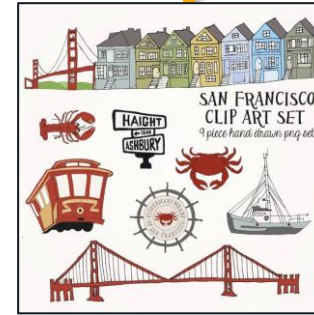
Cyber Security EMEA

In Cisco since 24 years...

... And 3 countries

Main interest on

- Policy and Access
- Segmentation
- Industrial Security



Cisco ISE High Level Design

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

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

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

What not to expect:



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

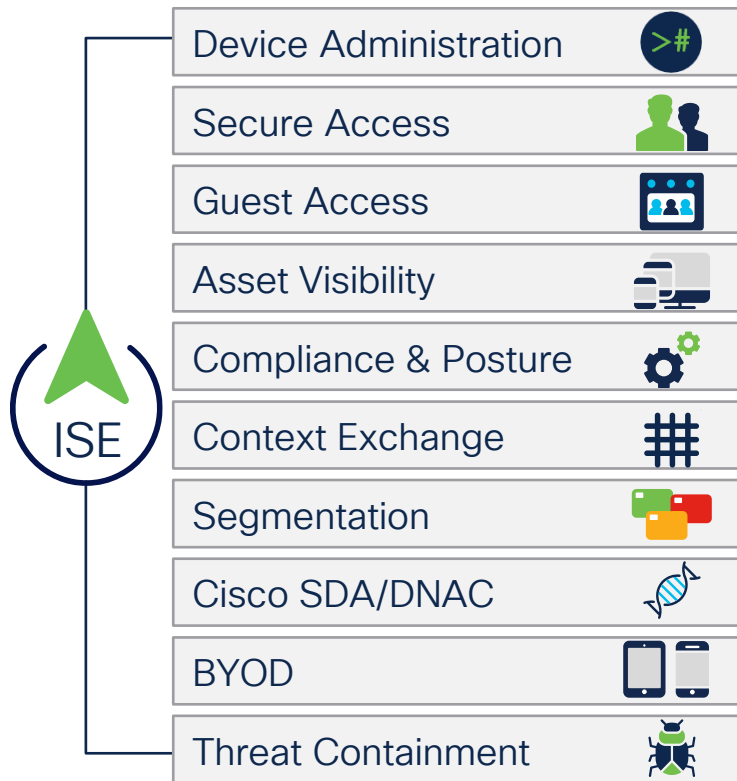


This presentation has
many links to resources
helping with most of
them

Agenda

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

What are your business priorities?



What is the business trying to accomplish with ISE?

Profiling is critical with today IoT proliferation

From where do you want to start?

Do you need a BYOD policy?

Which use cases could be considered for the future?

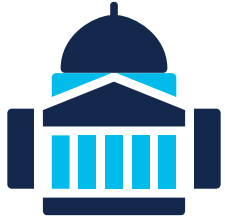
Defining your Security Policy

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

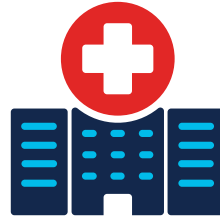
Government



Financials



Healthcare



Retail



Education



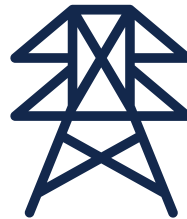
Transportation



Services



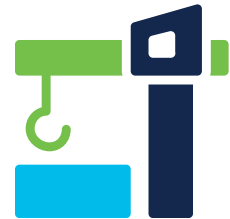
Utilities



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

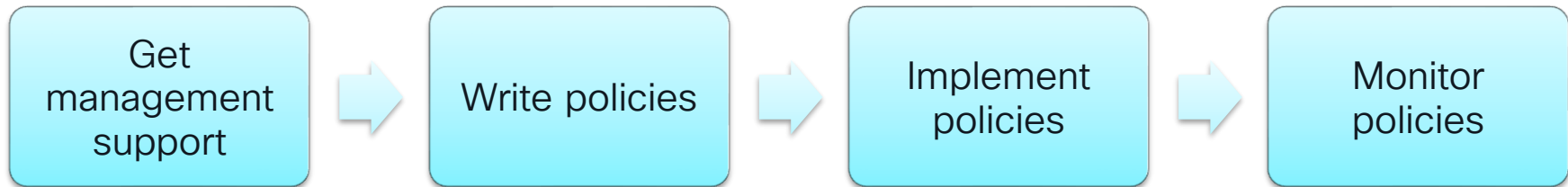
Network Team

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



Understand Your Needs and Use cases



Objectives / Risk / Priorities

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



Scaling

- Concurrent Active Endpoints
- Scale Horizontally
- Scale Vertically
- Geography



Environment

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



Management & Operations

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

Agenda

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

ISE Personas

Policy Administration Node (PAN)

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

Monitoring & Troubleshooting Node (MNT)

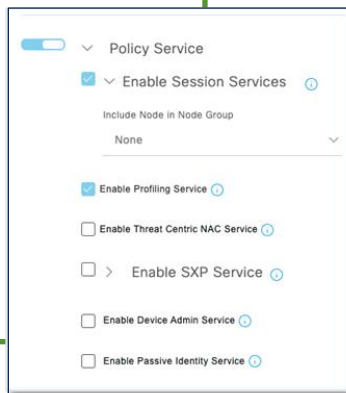
- Receives logs from all nodes
- Handles remote logging targets
- Generates summary Dashboard Views
- Performs scheduled reports
- Handles reporting and API queries

Policy Service Node (PSN)

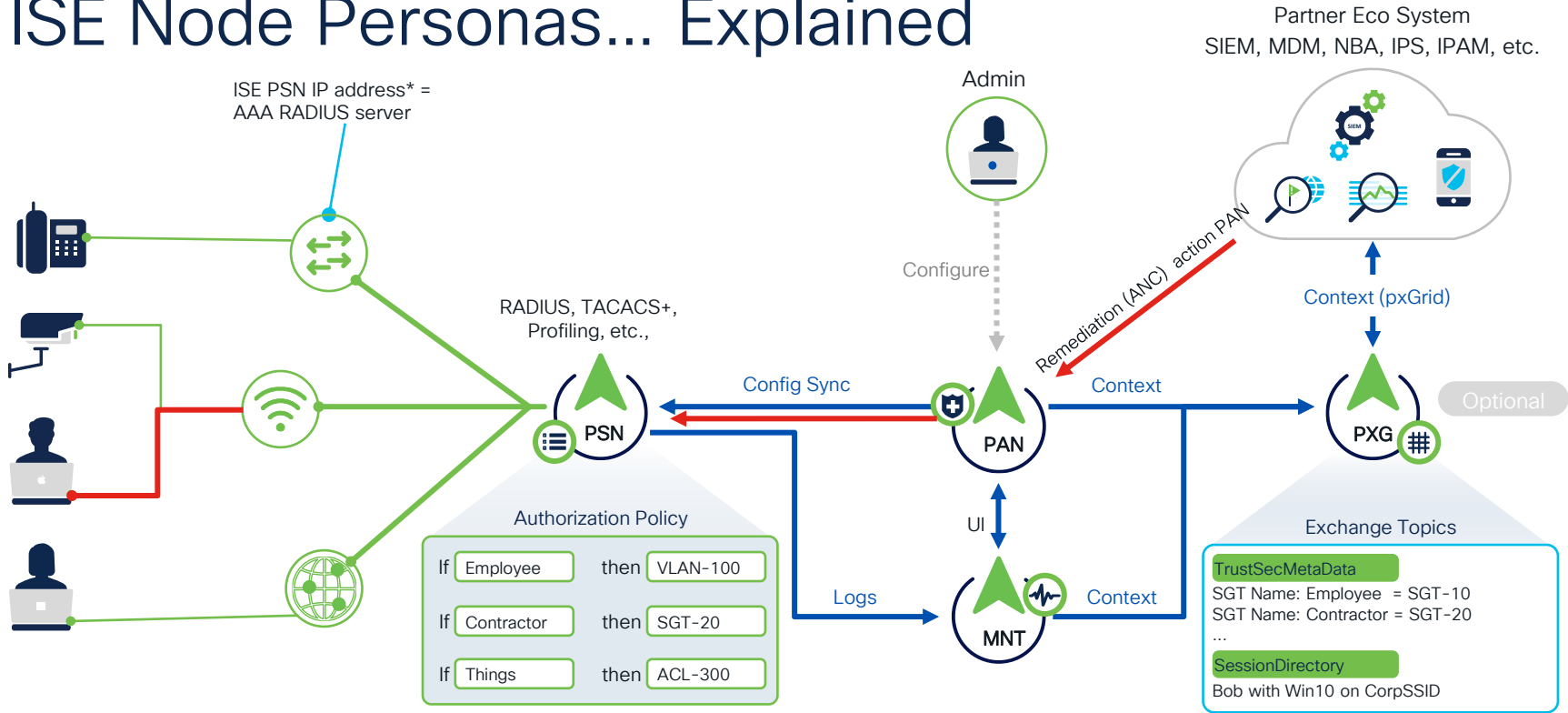
- TACACS requests
- RADIUS requests
- Endpoint profiling probes
- Identity store queries
- Hosts Guest/BYOD portals
- MDM/Posture queries
- TC-NAC & SXP services

Platform Exchange Grid Node (PXG)

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



ISE Node Personas... Explained



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

ANC = Adaptive Network Control

ISE Architecture

Standalone ISE



Policy Administration Node (PAN)

- Max 2 in a deployment



Monitoring & Troubleshooting Node (MnT)

- Max 2 in a deployment



Policy Services Node (PSN)

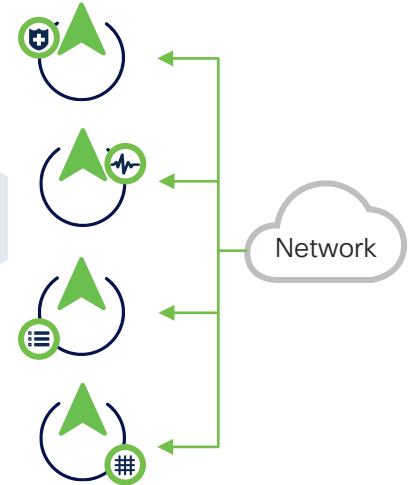
- Max 50 in a deployment



pxGrid Controller

- Max 4 in deployment

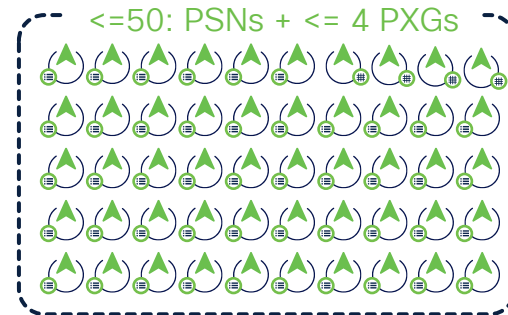
Distributed ISE



ISE Distributed Deployment Scale

Same for physical and virtual deployments

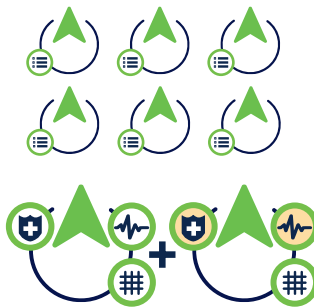
Compatible with load balancers



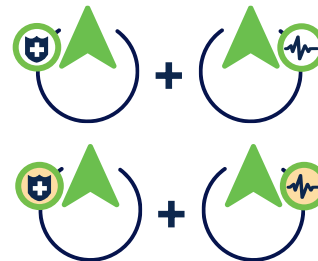
Standalone
(for Lab and
Evaluation)



Small HA
Deployment
 $2 \times (\text{PAN} + \text{MNT} + \text{PSN})$



Medium Multi-node
Deployment
 $2 \times (\text{PAN} + \text{MNT} + \text{PXG}), \leq 6 \text{ PSN}$



Large Deployment
 $2 \text{ PAN}, 2 \text{ MNT}, \leq 50: \text{PSNs}$
 $+ \leq 4 \text{ PXGs}$

100 Endpoints

Up to 50,000 Endpoints

Up to 150,000 Endpoints

Up to 2,000,000 Endpoints

3700

100 Endpoints

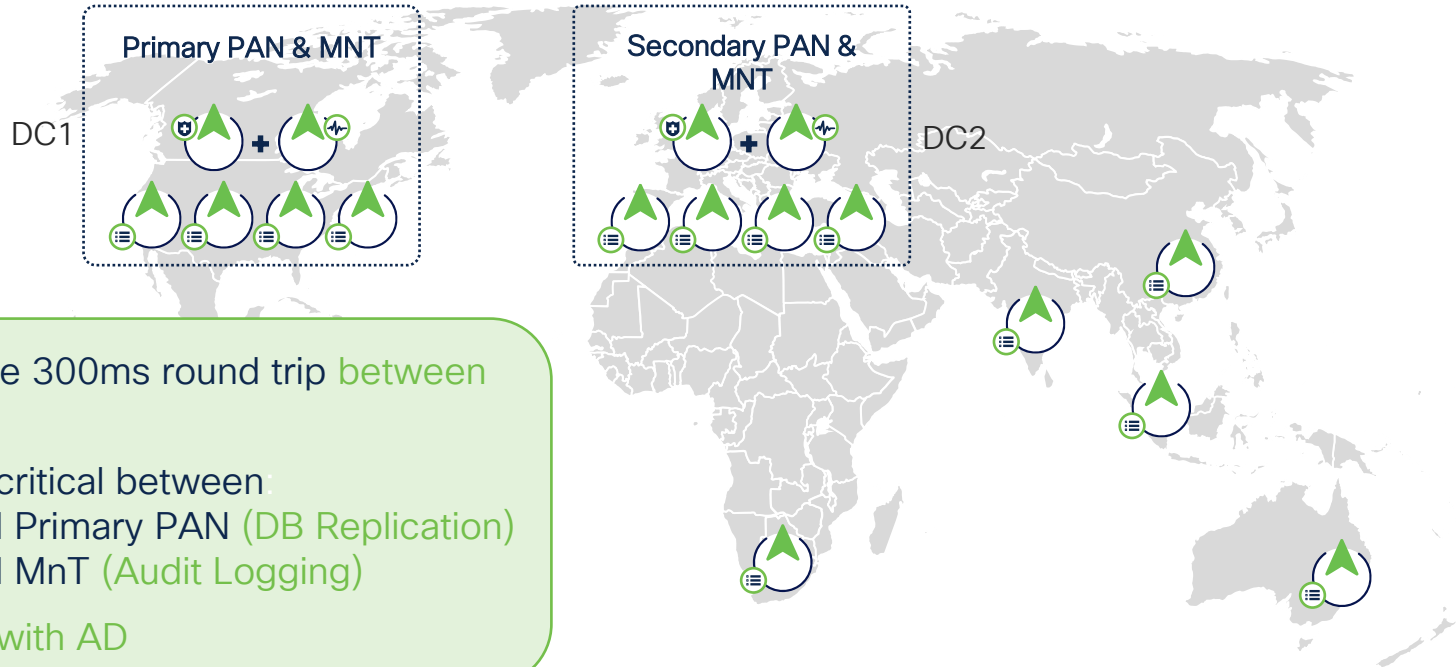
Up to 50,000 Endpoints

Up to 2,000,000 Endpoints

3600

ISE Fully Distributed Architecture

Centralize in DCs...or Distribute PSNs across Geographies



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

Maximum Concurrent Active Endpoints



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

ISE Nodes – Mix and Match

Physical Appliances



SNS-3715

SNS-3755

SNS-3795

SNS-3615

SNS-3655

SNS-3695

Virtual Machines



NUTANIX



Cloud Instances



Reminders

ISE platforms



SNS 3515

SNS 3595



EOL



SNS 3615

SNS 3655

SNS 3695



EOL



SNS 3715

SNS 3755

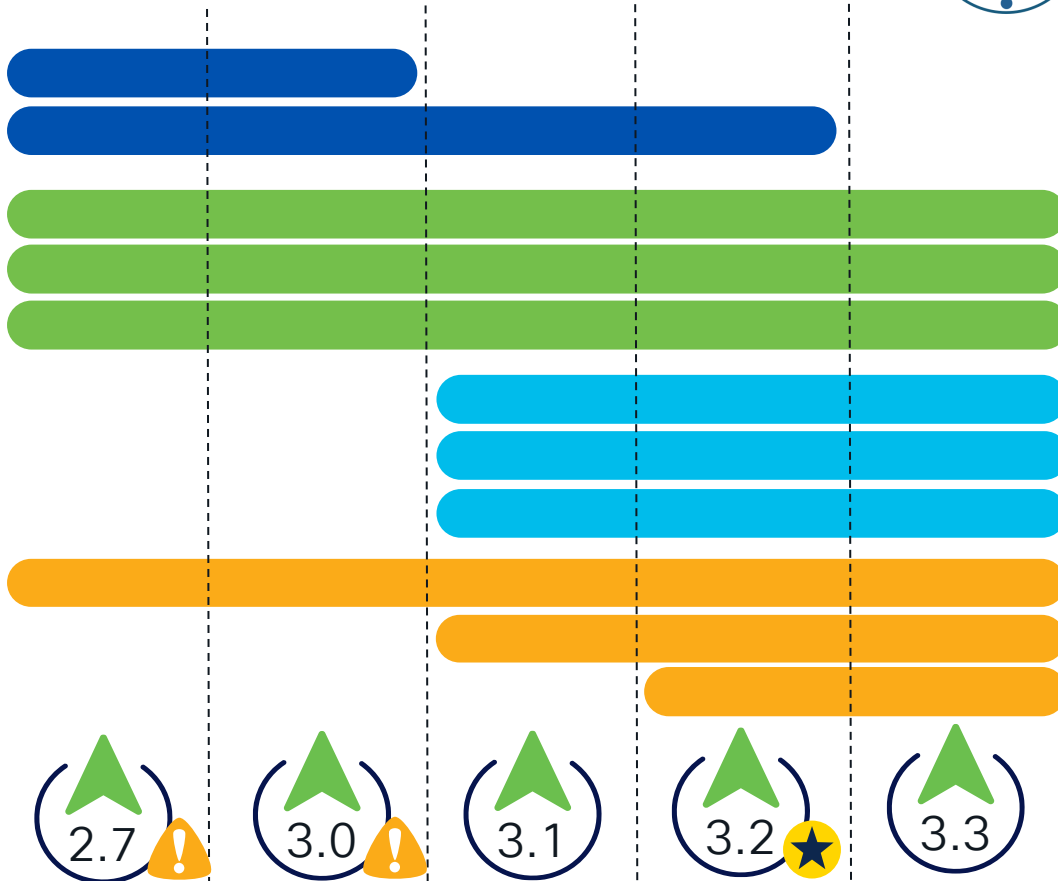
SNS 3795



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

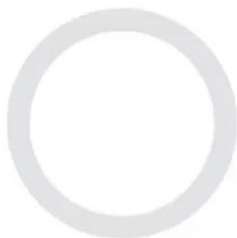
BYOD Endpoints

0

AUTHENTIFICATIONS

Identity Store Identity Group Network Device Failure Reason

No data available.



NETWORK DEVICES

Device Name Type Location

No data available.

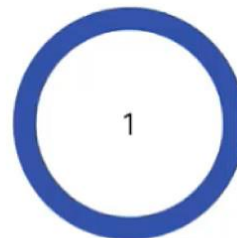


ENDPOINTS

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

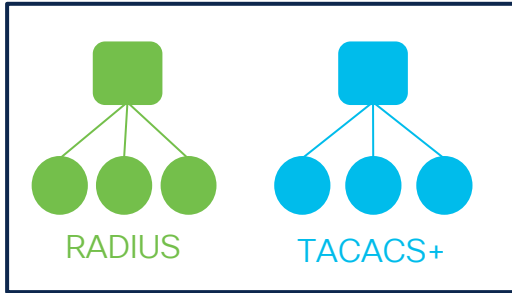
1 node(s)
ISE31-1ek

All 24HR

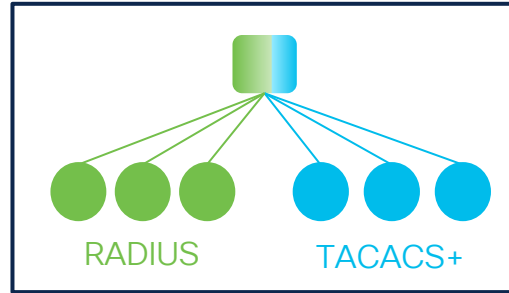
TACACS+ Deployment Models

Separating RADIUS & TACACS+ ISE Cubes?

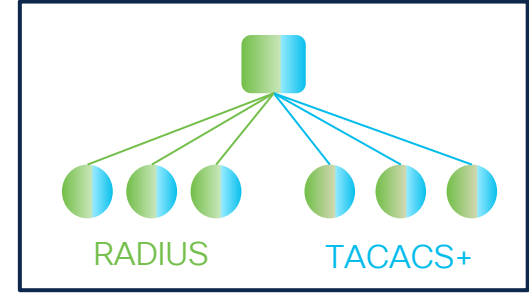
There are three different options:



Separate ISE cubes



Mixed ISE cube with
separate PSNs



Mixed ISE cube with
shared PSNs

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

Agenda

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

ISE Certificates



✓ System Certificates

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

✓ Trusted Certificates

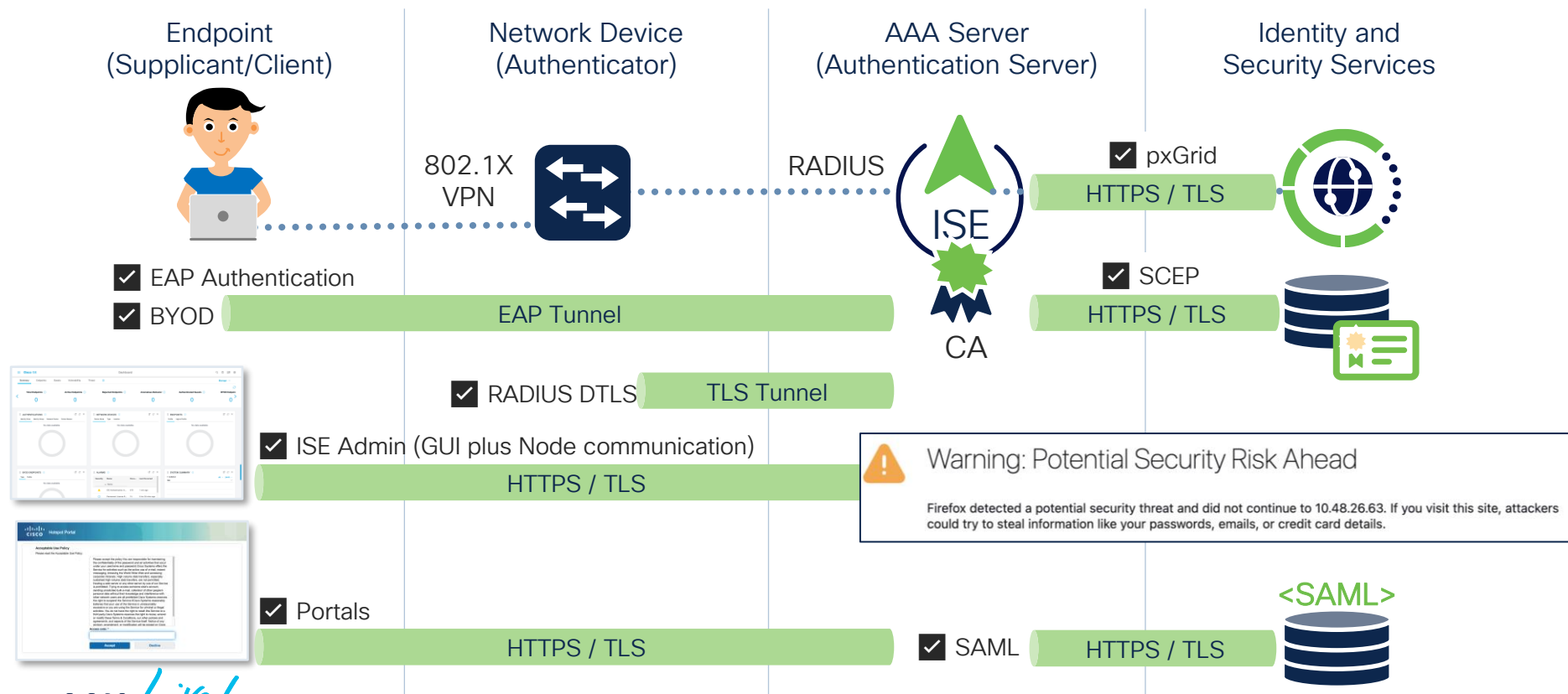
List of CAs

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

✓ ISE Issued Certificates

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

Different ISE System certificates



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_	SAML		SAML_ISE30-1ek.example.com	SAML_ISE30-1ek.example.com
<input type="checkbox"/>	OU=ISE Messaging Service,CN=ISE30-1ek.example.com#Certificate Services Endpoint Sub CA - ISE30-1ek#00001	ISE Messaging Service		ISE30-1ek.example.com	Certificate Services Endpoint Sub CA -
>	ISE30-2ek				
>	ISE30-3ek				
>	ISE30-4ek				

Which ISE role is using the certificate

Self signed certificate

Each ISE node has its own System Certificate Store

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_AME30-1ek.example.com	SAML		SAML_AME30-1ek.example.com	SAML_AME30-1ek.example.com
<input type="checkbox"/>	OU=ISE Messaging Service,CN=ISE30-1ek.example.com#Certificate Services Endpoint Sub CA - ISE30-1ek#00001	ISE Messaging			

Which ISE role is using the certificate

Self signed certificate

EAP Authentication, Admin, Portal, RADIUS DTLS

Default Portal Certificate Group ⓘ

ISE30-1ek.example.com

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

To install certificate

	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

<

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
	Configuration Changed	1	1 min ago

SYSTEM SUMMARY ⓘ

1 node(s)
ISE31-1ek

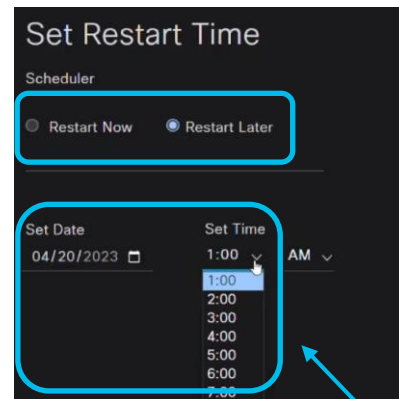
All 24HR

Controlled Application Restart

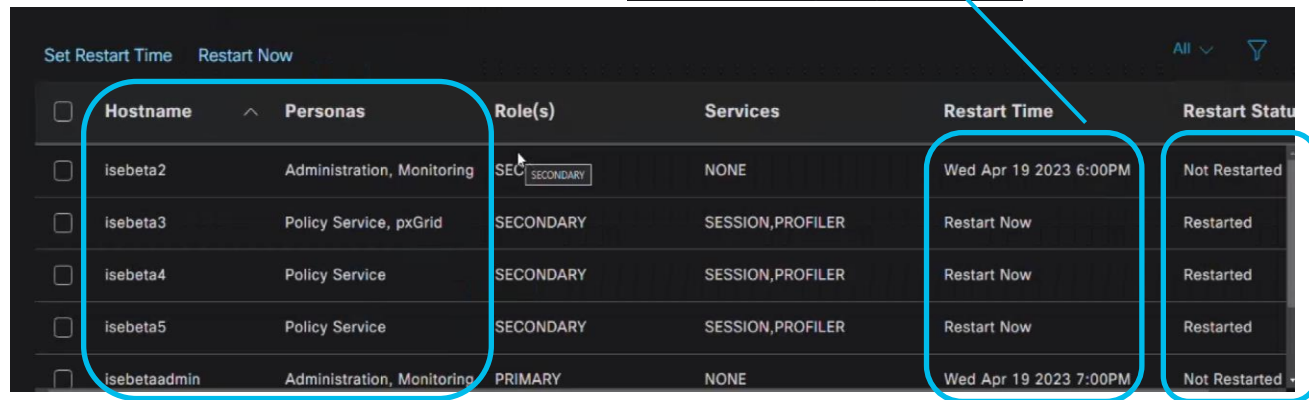
Up to ISE 3.2 a new ISE admin certificate requires reboot of all the nodes without any control.

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

Reboot must take place within 15 days



The 'Set Restart Time' dialog box shows two options: 'Restart Now' and 'Restart Later'. The 'Restart Later' option is selected. Below, the 'Set Date' is 04/20/2023. The 'Set Time' dropdown is open, showing a list of times from 1:00 to 7:00. The '1:00' time is highlighted. The 'AM' dropdown is also visible.



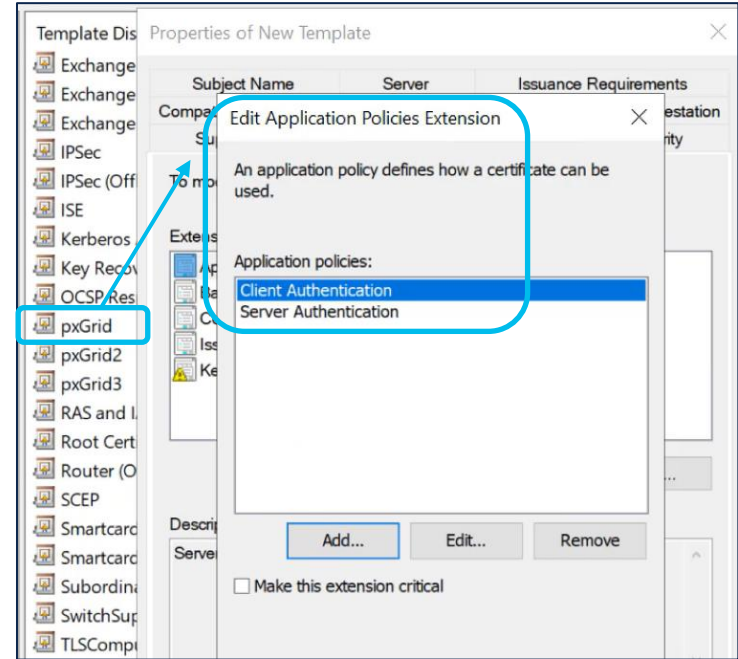
The main configuration table displays a list of ISE nodes. The 'Set Restart Time' and 'Restart Now' tabs are visible at the top. The table has columns for Hostname, Personas, Role(s), Services, Restart Time, and Restart Status. The 'isebeta2' node is highlighted with a red box. The 'Restart Time' column for 'isebeta2' is 'Wed Apr 19 2023 6:00PM'. The 'Restart Status' column for 'isebeta2' is 'Not Restarted'. A red arrow points from the 'Set Time' dropdown in the dialog box to the 'Restart Time' column in the table.

	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

PxGrid Certificate

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

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



Agenda

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

Network Device discovery/capabilities

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

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

 cs.co/nad-capabilities

² Refer to [Cisco Compatibility Matrix](#)

CISCO *Live!*

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	✓	✓	✓	✓	✓	✓	✓	✓
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 Sx500 1.2.0.97	✓ ⁴ !	✓ !	✓ X	✓ X	✓ X	✓ X	✓ X	✓ X

Does ISE Support my third-party Network device?

Does my third-party Network Device Supports ISE?

Overview

Cisco ISE supports protocol standards like RADIUS, its associated RFC Standards, and TACACS+. For more information, see the [ISE Community Resources](#).

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

Cisco ISE interoperates fully with third-party TACACS+ client devices that adhere to the governing protocols. Support for TACACS+ functions depends on the device-specific implementation.

Check for Advanced capabilities support:

- CoA (RADIUS or SNMP)
- URL Redirection

Might need to:

- Import a Vendor Specific Dictionary
- Create Network Device Profile

Summary Endpoints Guests Vulnerability Threat +

Manage ▾

Total Endpoints ⓘ

165

Active Endpoints ⓘ

5

Rejected Endpoints ⓘ

0

Anomalous Behavior ⓘ

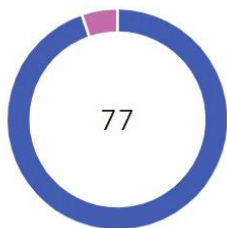
0

Authenticated ⓘ

AUTHENTIFICATIONS ⓘ

Identity Store Identity Group Network Device

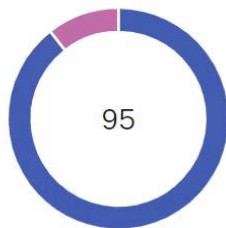
Failure Reason



- duoauthproxy - 94.81%
- labrats - 5.2%

NETWORK DEVICES ⓘ

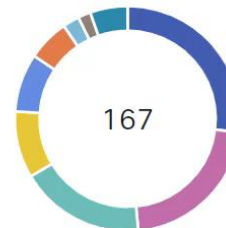
Device Name Type Location



- loke - 89.47%
- sec9300 - 10.53%

ENDPOINTS ⓘ

Profile Logical Profile



- macin...ation - 27.61%
- workstation - 22.09%
- cisco-device - 18.41%
- cisco-router - 9.82%
- vmware-device - 8.59%
- windo...ation - 6.14%
- cisco-switch - 2.45%
- unknown - 1.84%
- other - 5.52%

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 Import

<input type="checkbox"/> Name	Description
<input type="checkbox"/> All Device Types	All Device Types
<input type="checkbox"/> All Locations	All Locations
<input type="checkbox"/> ▾ Is IPSEC Device	Is this a RADIUS over IPSEC
<input type="checkbox"/> No	Device is not IPSEC Type
<input type="checkbox"/> Yes	Device is IPSEC Type

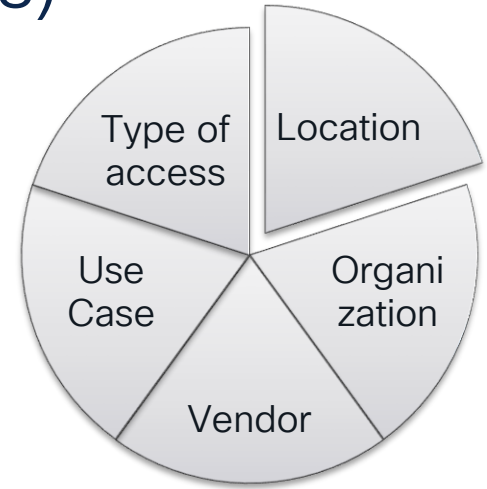
Default NDGs

Refresh Add Duplicate Edit

<input type="checkbox"/> Name
<input type="checkbox"/> > All Device Types
<input type="checkbox"/> ▾ All Locations
<input type="checkbox"/> ▾ AMER
<input type="checkbox"/> ▾ US
<input type="checkbox"/> ▾ San Jose
<input type="checkbox"/> ▾ Building
<input type="checkbox"/> Floor
<input type="checkbox"/> > Countries
<input type="checkbox"/> > Departments
<input type="checkbox"/> > Is IPSEC Device
<input type="checkbox"/> > Orgs
<input type="checkbox"/> > Regions

Maximum 6 Levels

Create Your Own Root NDGs



Additional Tips

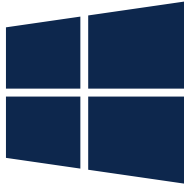
- Always Test before implementing!
- Standardize! Standardize! Standardize!
 - IOS versions
 - AAA configuration
 - Wireless configuration
 - Profiling configuration
- 3rd party device documentation



Agenda

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

Endpoints: Native 802.1X Supplicants



RADIUS-802.1x

EAP method
PEAP

Phase-2 authentication
MSCHAPV2

CA certificate
Do not validate

No certificate specified. Your connection will not be private.

Identity
username

Anonymous identity

Password
password

☒ Show password

Advanced options

Cancel Save

Ethernet Properties

Protected EAP Properties

When connecting:
☒ Verify the server's identity by validating the certificate
☐ Connect to these servers (examples: sv1;sv2; *[,sv3],com):

Trusted Root Certification Authorities:
☐ Baltimore CyberTrust Root
☐ Class 3 Public Primary Certification Authority
☐ DigiCert Assured ID Root CA
☐ DigiCert Global Root CA
☐ DigiCert Global Root G2
☐ DigiCert High Assurance EV Root CA
☐ GlobalSign

Notifications before connecting:
Tell user if the server's identity can't be verified

Select Authentication Method:
Secured password (EAP-MSCHAP v2) Configure...

☒ Enable Fast Reconnect
☐ Disconnect if server does not present cryptobinding TLV
☐ Enable Identity Privacy

OK Cancel



Network

VAVA-USBC-8n1

TCP/IP DNS WINS 802.1X Proxies Hardware

Use a configuration profile to add an 802.1X profile to your system. Contact your system administrator for more information.

Protected EAP for Ethernet...

Profile Information

Name: Protected EAP for Ethernet v2

Authentication: PEAP

Wireless Network:

Security Type:

Trusted Certificate:

Trusted Servers:

☒ Enable automatic connection

Cancel OK

Revert Apply

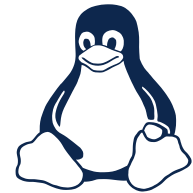


```
wpa_supplicant

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

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

OVERVIEW
Wireless networks do not require physical access to the
network equipment in the same way as wired networks.
This makes it easier for unauthorized users to passively
monitor a network and capture all transmitted frames.
In addition, unauthorized use of the network is much
```



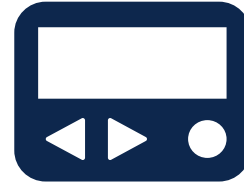
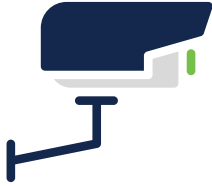
Windows 7, 8/8.1, and 10 – Native Supplicant

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

Agenda

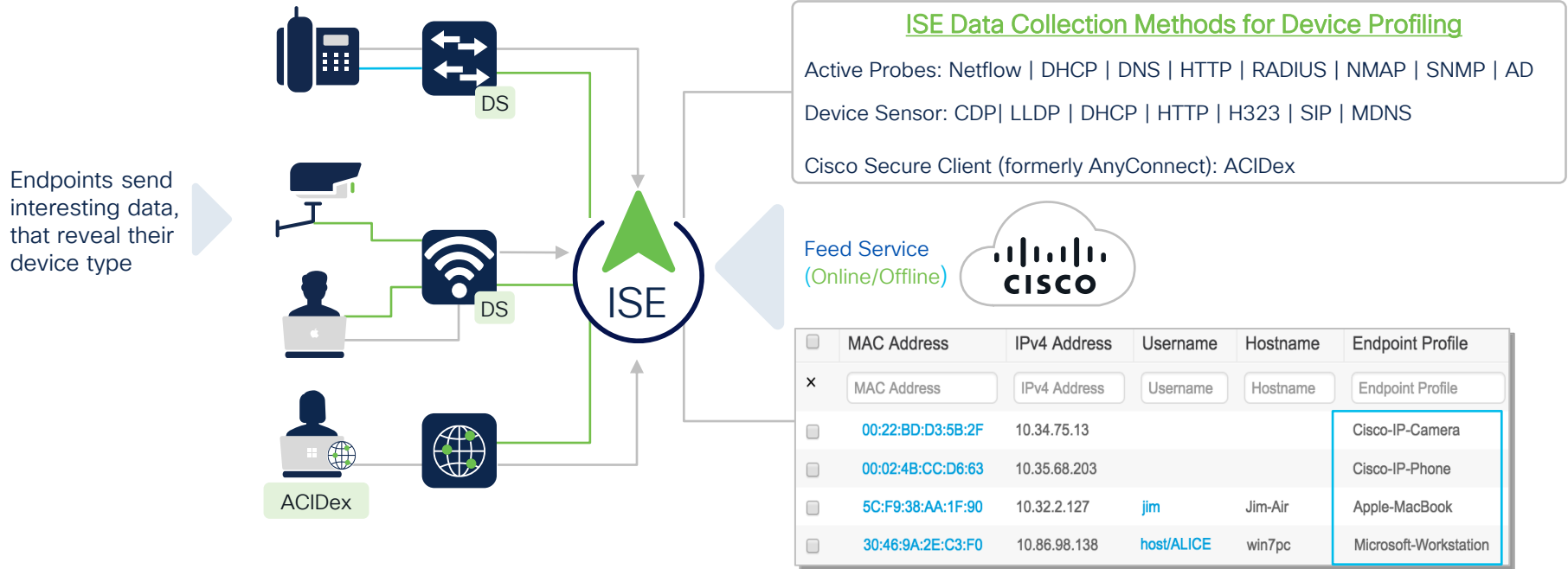
- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

Endpoints: Everything Else



Endpoint Profiling

Identifies dynamically the devices that connect to your network



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 DHCP Probe



Microsoft Workstation

OUI = Random, IP = xx.xx.xx.xx, dhcp-class-identifier CONTAINS MSFT



Cisco IP Phone 9971

OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971,
DHCP:dhcp-class-identifier CONTAINS CP-9971



HP Printer

OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet



Apple Device

OUI = Apple, IP = xx.xx.xx.xx,
DHCP:dhcp-DHCP:dhcp-parameter-request-list EQUALS 1, 3, 6, 15, 119, 252

Effect of HTTP Probe



Windows10-Workstation
Microsoft Workstation

OUI = Random, IP = xx.xx.xx.xx, dhcp-class-identifier CONTAINS MSFT,
IP:User-Agent CONTAINS Windows NT 10.0



Cisco IP Phone 9971

OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971,
DHCP:dhcp-class-identifier CONTAINS CP-9971



HP Printer

OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet



Apple iDevice

OUI = Apple, IP = xx.xx.xx.xx,
DHCP:dhcp-DHCP:dhcp-parameter-request-list EQUALS 1, 3, 6, 15, 119, 252
IP:User-Agent contains iPad

Effect of NMAP Probe



Windows10-Workstation

OUI = Random, IP = xx.xx.xx.xx, dhcp-class-identifier CONTAINS MSFT, IP:User-Agent CONTAINS Windows NT 10.0, FQDN=test-laptop1.zero0k.org,
NMAP:SMB.operating-system CONTAINS Windows 10



Cisco IP Phone 9971

OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971,
DHCP:dhcp-class-identifier CONTAINS CP-9971, FQDN=test-phone1.zero0k.org



HP Printer

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



Apple iPad

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

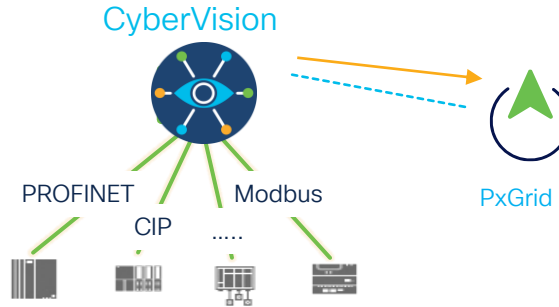
OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet, FQDN=test-printer1.zero0k.org, SNMP:hrDeviceDescr CONTAINS HP LaserJet P4015



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

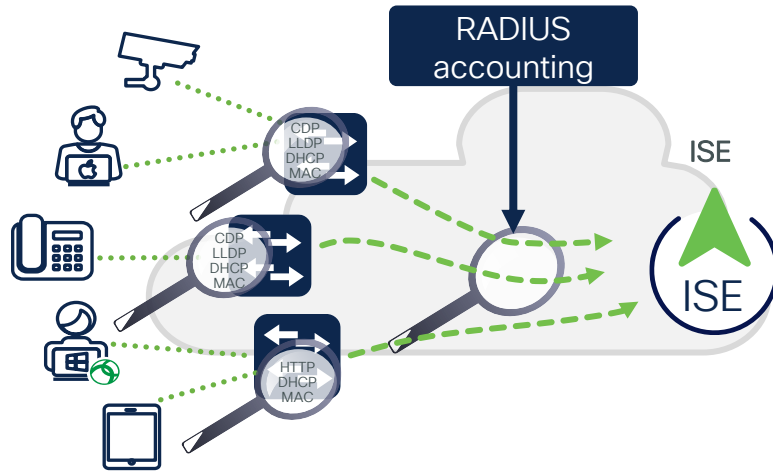


Device Sensor to scale attribute collection

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

Attributes used:

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



From IOS
15.0(2)SE



Meraki MS390
MS Switches only
CDP+LLDP



From
AirOS 7.2

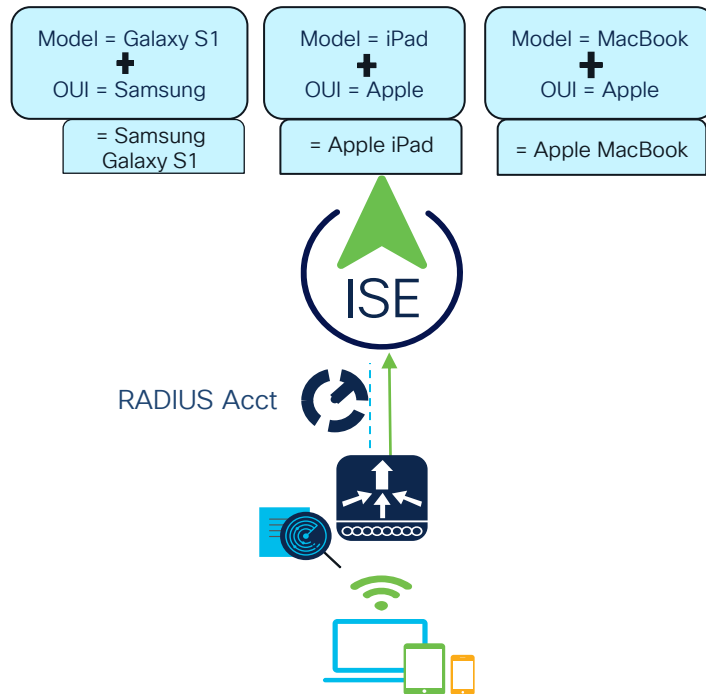
Wi-Fi Edge Analytics

SAMSUNG



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](#)

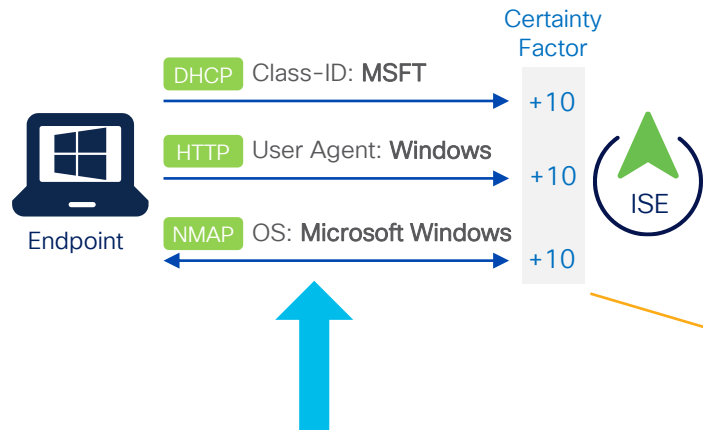
Name

- ☐ 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



- 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

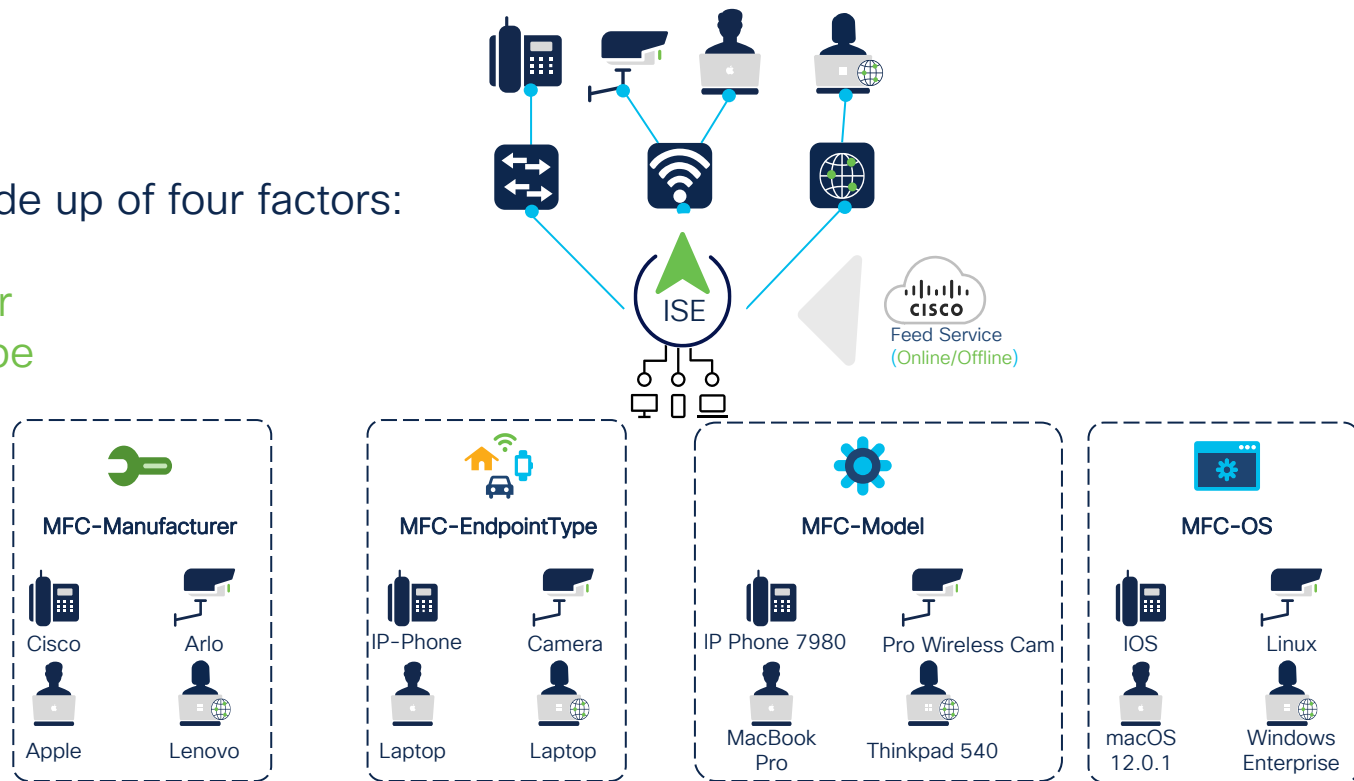
Rules

If	Condition	Then	Certainty Factor Increases	Value
If	Condition: Microsoft-WorkstationRule2Check1	Then	Certainty Factor Increases	10
If	Condition: Microsoft-WorkstationRule4-Check1	Then	Certainty Factor Increases	10
If	Condition: Microsoft-WorkstationRule3Check1	Then	Certainty Factor Increases	10
If	Condition: Microsoft-WorkstationRule1Check1	Then	Certainty Factor Increases	10

Multi-Factor Classification on ISE

Profiles are now made up of four factors:

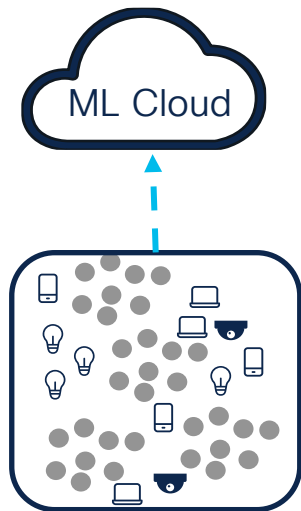
- MFC-Manufacturer
- MFC-Endpoint Type
- MFC-Model
- MFC-OS



AI Proposed Profiling Policies

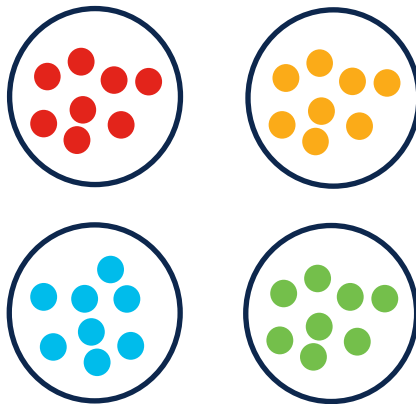
Data Forwarded to Cloud

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



ML Groups Endpoints

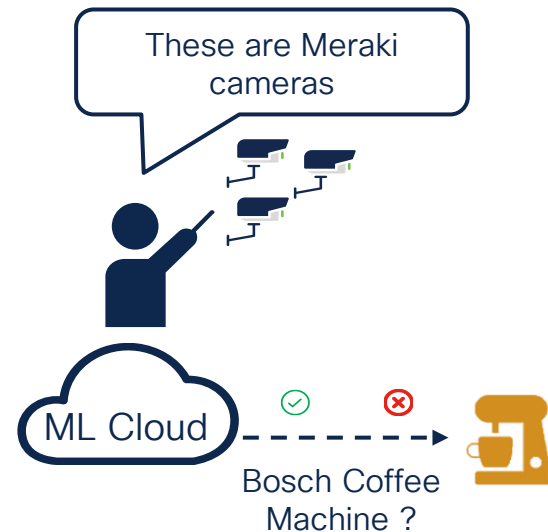
ML groups endpoints into
clusters of identical or
based on attribute data



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

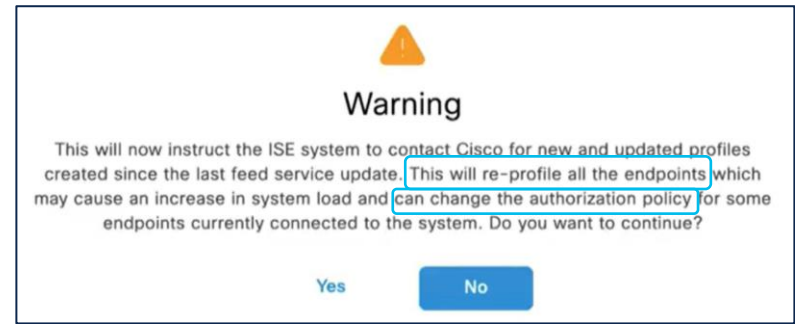
Labels Assigned

Users assign labels to
unknown clusters or
accept recommendations



ISE Feed service Updates

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



ANC

▼

Change Authorization

▼

Clear Threats & Vulnerabilities

Export

▼

Import

▼

MDM Actions

▼

Release Rejected

Revoke Certificate

<input type="checkbox"/>	MAC Address	Anomalo...	IP Address	Username	Hostname	Location	Endpoint Profile	OUI	Des
<input checked="" type="checkbox"/>	MAC Address	Anomalous	IP Address	Username	Hostname	Location	Unknown	OUI	Des
<input type="checkbox"/>	00:00:17:74:64:94		10.1.13.12	00:00:17:7...		Global/Nor...	Unknown	Oracle	
<input type="checkbox"/>	00:00:18:0B:B3:CD		10.1.13.16	00:00:18:0...		Global/Nor...	Unknown	WEBSTER COMPUT...	
<input type="checkbox"/>	00:00:1F:A7:3D:11		10.1.15.6	00:00:1F:A...		Global/Nor...	Unknown	Telco Systems, Inc.	

Create custom profiles

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

dhcp-class-identifier	udhcp 0.9.7
dhcp-client-identifier	01:00:14:48:00:30:8c
dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 3, 6, 12, 15, 28
dhcp-requested-address	10.1.100.103
dot1xAuthAuthControlledPortControl	2
dot1xAuthAuthControlledPortStatus	2
Other Attributes	
5060-tcp	sip
80-tcp	http
AAA-Server	ise
hlen	6
htype	Ethernet (10Mb)
OUI	Inventec Multimedia & Telecom Corporation
OriginalUserName	00144800308c
PolicyVersion	8
PostureApplicable	Yes
op	BOOTREQUEST
operating-system	Linux 2.4.9 - 2.4.18 (likely embedded)
operating-system-result	Linux 2.4.9 - 2.4.18 (likely embedded)
yiaddr	0.0.0.0

Profiles Precedence

Cisco Provided
Profile



Existing Cisco Profile

CF = 30



Custom
Profile



New Customer Profile

CF >= 30



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

Try put custom profiles above 100

Using device profiles and logical profiles in ISE

The image illustrates the configuration of logical profiles in Cisco ISE. It shows the navigation menu, the configuration of logical profiles for Printers and Cameras, and a table of endpoint identity groups.

Logical Profiles List > Printers

Logical Profile

- * Name: Printers
- Description: Default logical profile for printers.
- * Policy Assignment
- Available Policies:
 - 2Wire-Device
 - 3Com-Device
 - Aastra-Device
 - Aastra-IP-Phone
 - Aerohive-Access-Point
 - Aerohive-Device
 - American-Power-Conversion-Device
 - Android
- Assigned Policies:
 - Brother-HL-3040CN-series
 - Brother-HL-5370DW-series
 - Brother-MFC-8890DW
 - Brother-MFC-9010CN
 - Canon-MF4690
 - Canon-Printer
 - Epson-TM-Series-Printer
 - HP-Color-LaserJet-2500

Logical Profiles List > Cameras

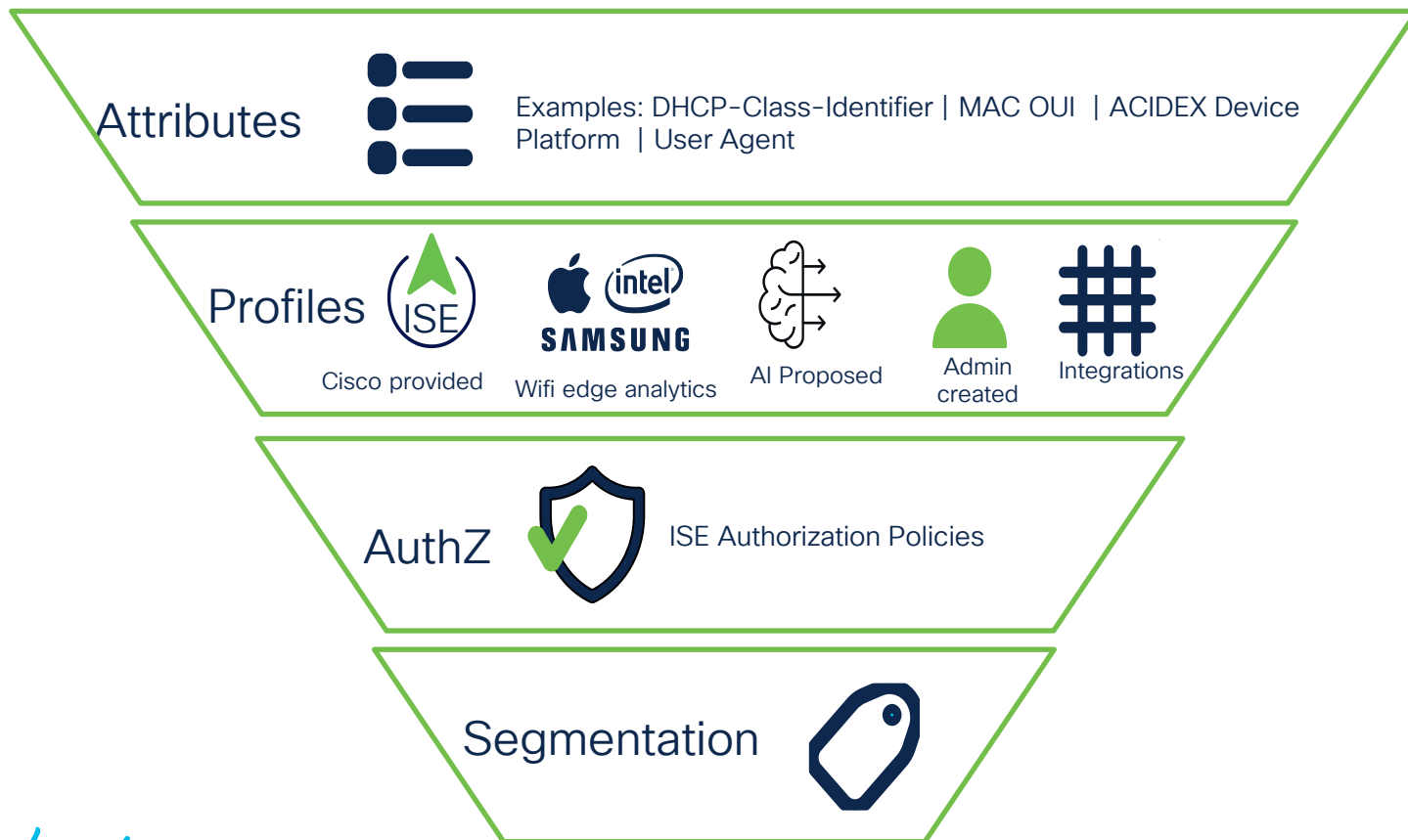
Logical Profile

- * Name: Cameras
- Description: Default logical profile for cameras.
- * Policy Assignment
- Available Policies:
 - 2Wire-Device
 - 3Com-Device
 - Aastra-Device
 - Aastra-IP-Phone
- Assigned Policies:
 - Axis-Network-Camera
 - Cisco-IP-Camera
 - Trendnet-Camera

Table of Endpoint Identity Groups:

✓	Device	IdentityGroup Name	Endpoint Identity Groups
✓	Cisco IP Phones	IdentityGroup Name EQUALS	Endpoint Identity Groups: Profiled: Cisco-IP-Phone
✓	Printers	EndPoints-LogicalProfile EQUALS	Printers
✓	Cameras	EndPoints-LogicalProfile EQUALS	Cameras

Turning Probes Into Profiles, Profiles Into Protection



Behavioral vs Organizational Endpoint Information

Behavioral

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

Organizational

- [Endpoint Custom Attributes](#)
 - Context Visibility Input (GUI/CSV)
 - Custom Attributes and endpoint REST API (JSON)
- [External Databases \(CMDBs\)](#)
 - Active Directory / LDAP
 - pxGrid Direct (ServiceNow, etc.)

Common Uses

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

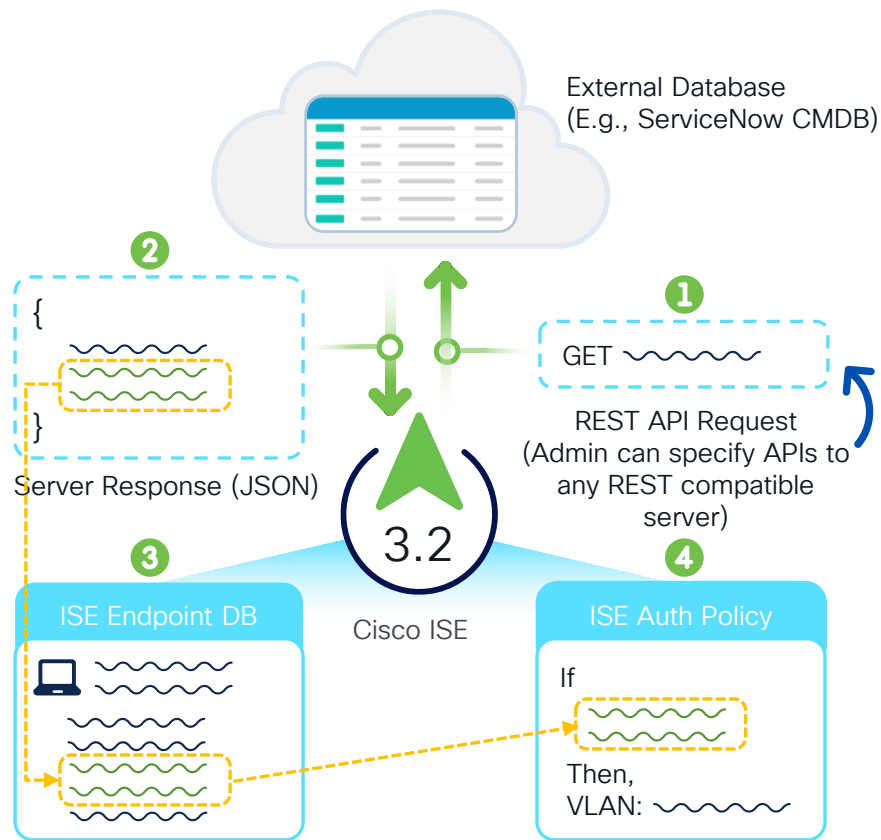
Endpoint Custom Attributes

Endpoint Attribute

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

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



Live Logs

Live Sessions



Misconfigured Supplicants ⓘ

0

Misconfigured Network Devices ⓘ

0

RADIUS Drops ⓘ

0

Client Stopped Responding ⓘ

0

Repeat Counter ⓘ

0

Refresh

Every 10 sec... ▾

Show

Latest 20 reco... ▾

Within

Last 5 minutes ▾

Filter ▾



Administration



System

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade

Health Checks

Backup & Restore

Admin Access

Settings

Network Resources

Network Devices

Network Device Gro...

Network Device Pro...

External RADIUS Se...

RADIUS Server Seq...

NAC Managers

External MDM

pxGrid Direct Conne...

Location Services

Threat Centric NAC

Third Party Vendors

Identity Management

Identities

Groups

External Identity So...

Identity Source Seq...

Settings

pxGrid Services

Summary

Client Management

Diagnostics

Settings

Device Portal Manageme...

Blocked List

BYOD

Certificate Provision...

Client Provisioning

Mobile Device Mana...

My Devices

Custom Portal Files

Settings

Feed Service

Profiler

Endpoint Profile

Authenti...

Authorization Policy

Se

Endpoint Profile

Authenticati

Authorization Policy

Se

Microsoft-Workstation

IOT_Wired...

IOT_Wired_MAB >> Unknown_...

Uni

Records Shown: 1

Agenda

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

Make use of Policy Sets

Organizations 

Type 

Location 

Vendor/Model 

Medium 

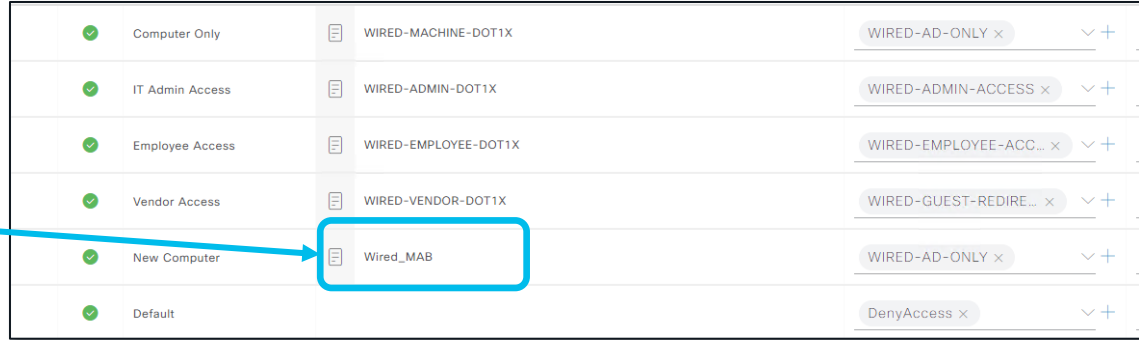
Wireless 

RADIUS 

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

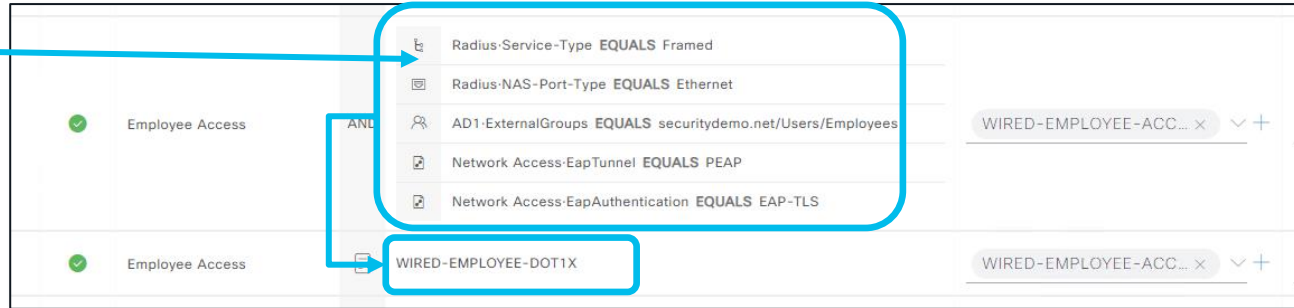
Conditions simplification

Pre-sets Dictionary
Condition are easy to
read and intuitive



✓	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



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



Use Compound
Conditions and
for custom ones

Dynamic Variable Substitution

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

▼ Authorization Policy				
Standard				
Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
✓	Dynamic Match Rule	if	Radius:Calling-Station-ID MATCHES LDAP1 Department	then Permit Access

ID Store

Attribute

▼ Advanced Attributes Settings	
Radius:Class	= InternalEndpoint groupPolicy

Speed Test

Is the image matching the condition set?

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



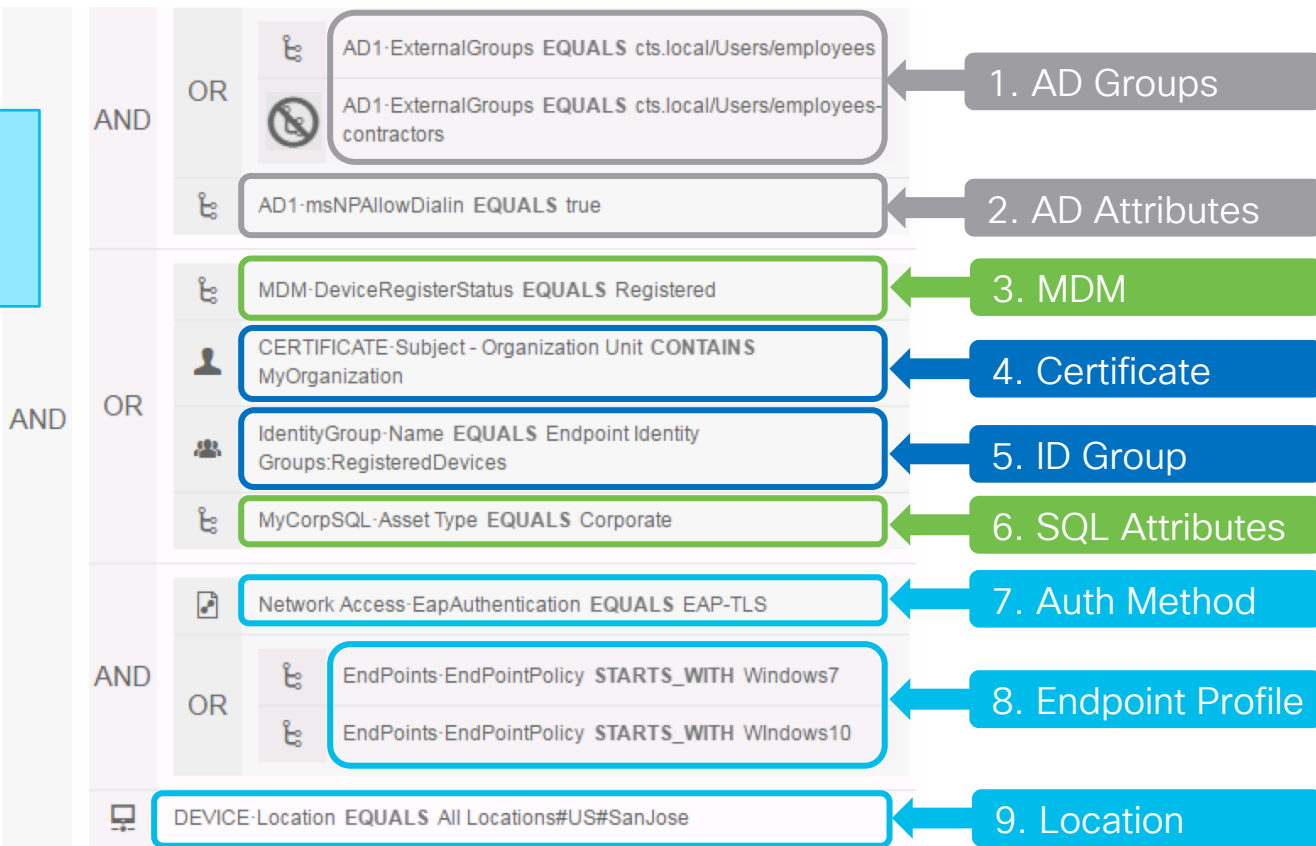
Auth Policy Optimization

Policy Logic:

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

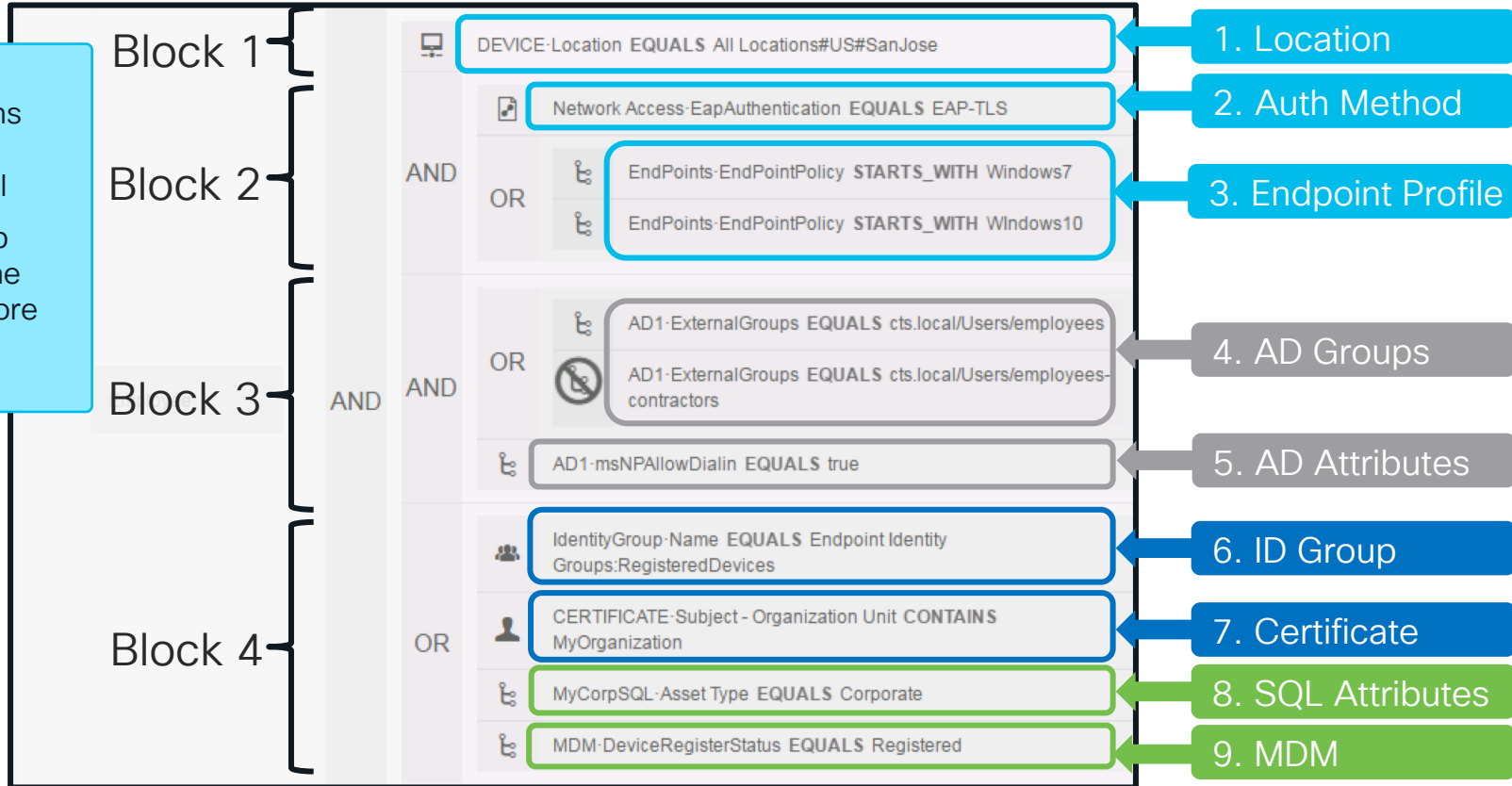
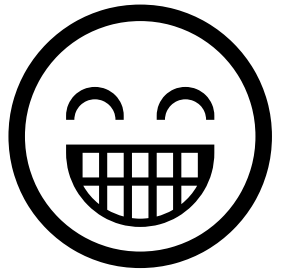


Employee

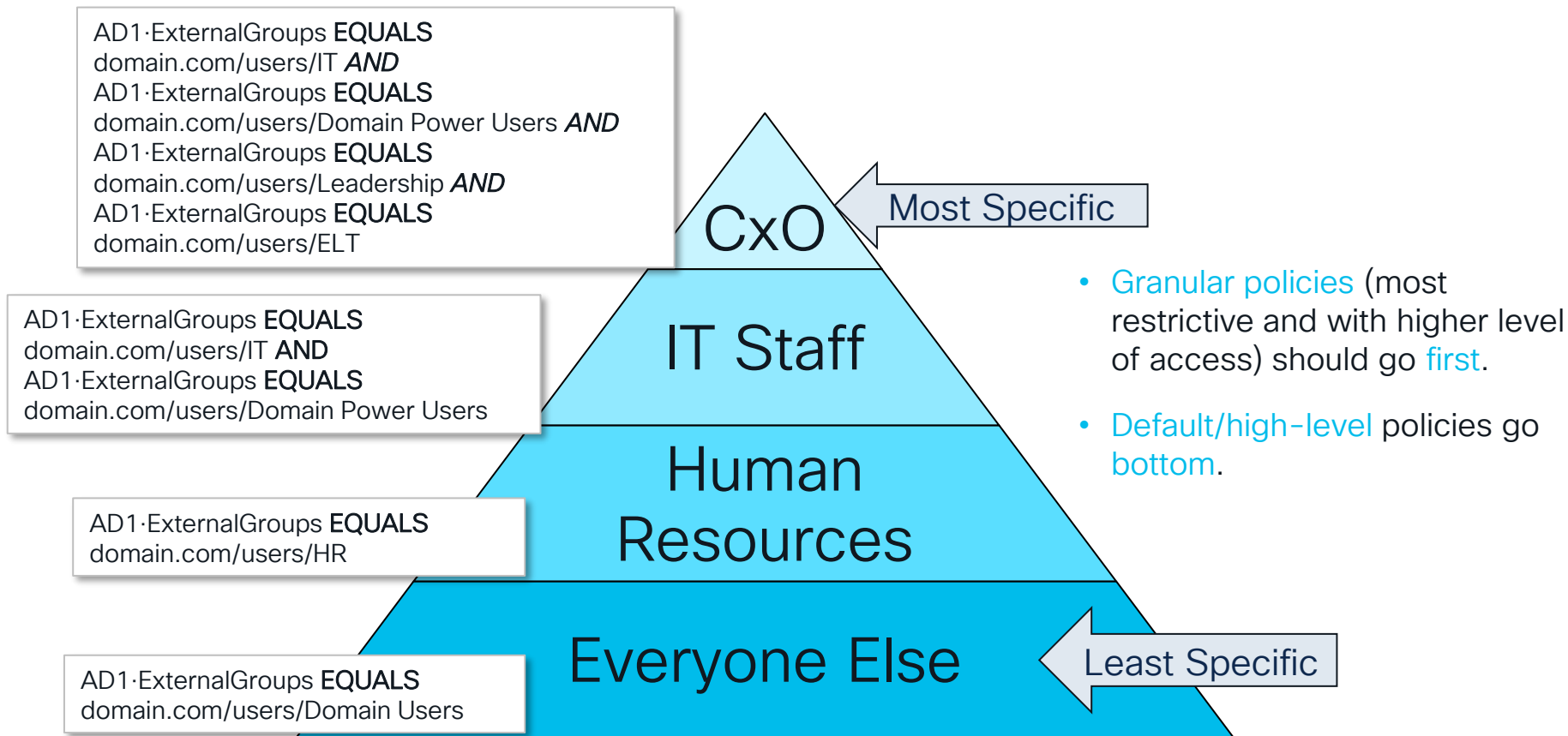


Auth Policy Optimization

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



AD Policy rule optimization example



Agenda

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

Who Needs an ISE Lab? You do!



With ever **Standalone** installation :

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

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

ISE Lifecycle Orchestration & Policy Management



Zero Touch
Deployment



Patch
Installation



License
Management



Certificate
Management



Configuration
Management



Policy
Management



Operations
Automation



ISE 3.1
Patch 1 or later



Python



Ansible



VSCode

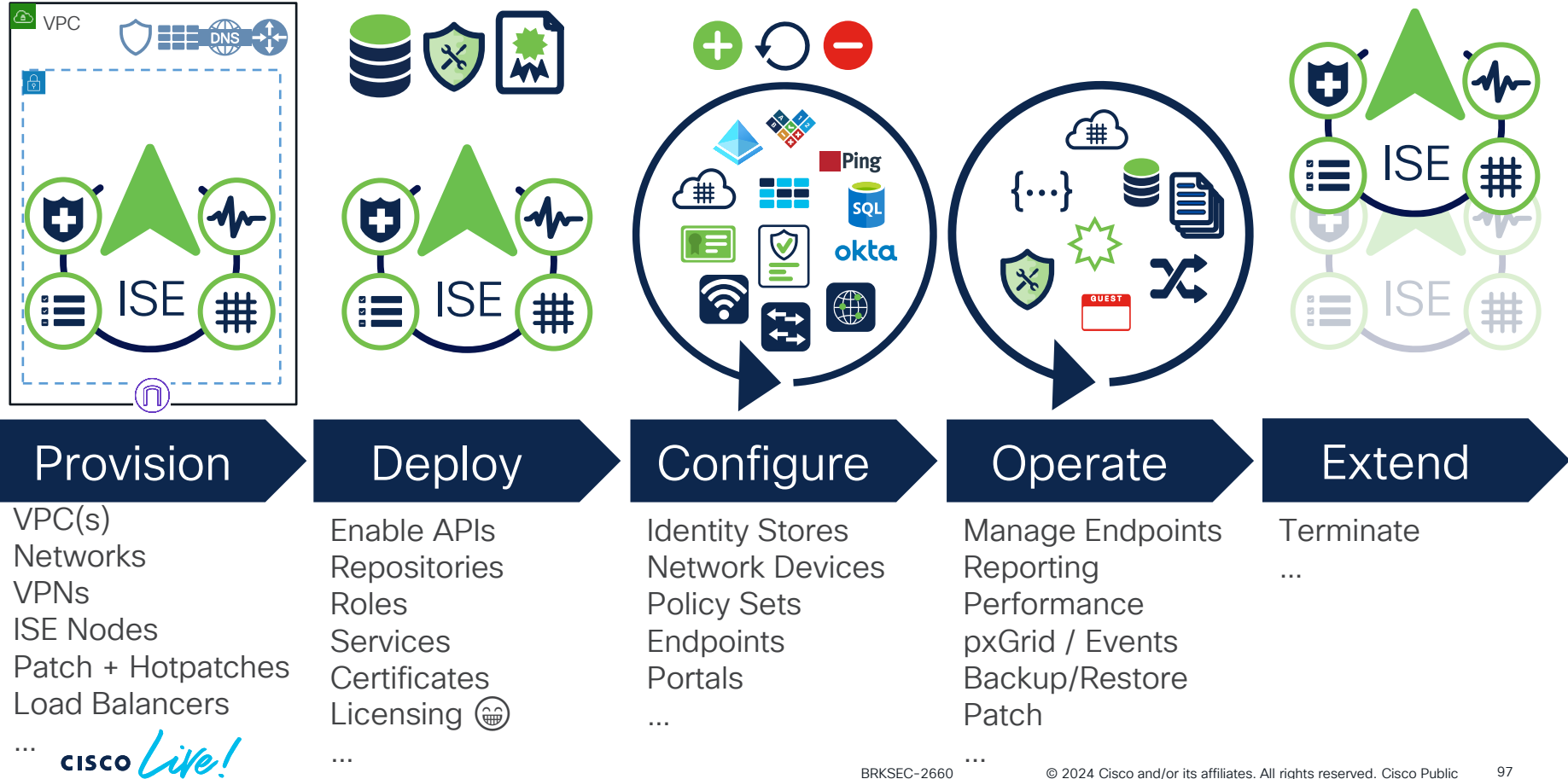


github.com/CiscoISE

#YAML

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

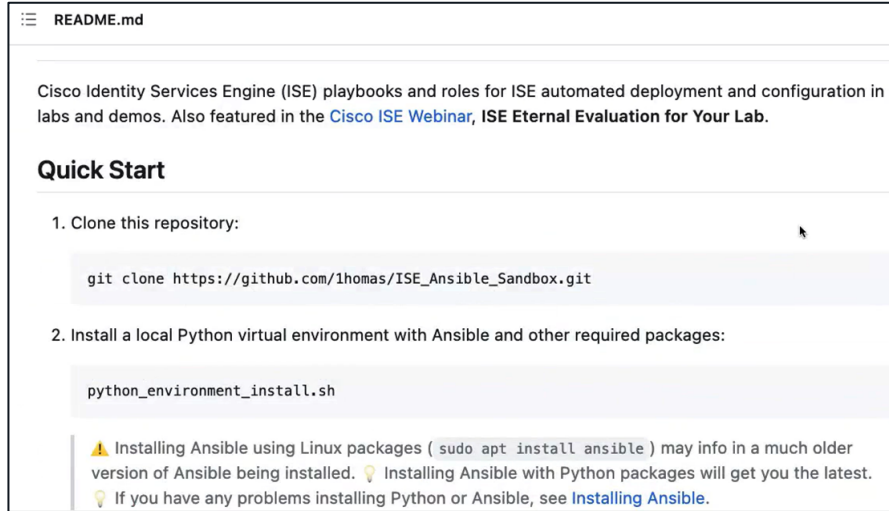
ISE Deployment and Operational Lifecycle



ISE Eternal Evaluation

 https://github.com/1thomas/ISE_An 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

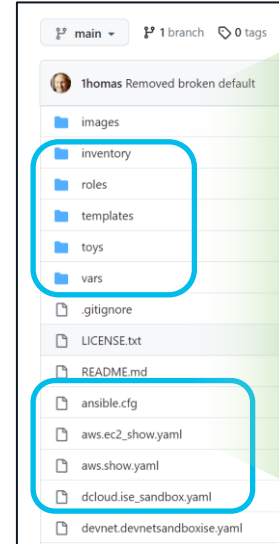
1. Clone this repository:

```
git clone https://github.com/1thomas/ISE_An ansible_Sandbox.git
```
2. Install a local Python virtual environment with Ansible and other required packages:

```
python_environment_install.sh
```

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

iseee.yaml



main 1 branch 0 tags

thomas Removed broken default

- images
- inventory
- roles
- templates
- toys
- vars
- gitignore
- LICENSE.txt
- README.md
- ansible.cfg
- aws.ec2_show.yaml
- aws.show.yaml
- dcloud.ise_sandbox.yaml
- devnet.devnetsandboxise.yaml

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

How to test your lab?

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

BUT...

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

Try the Session Trace Test tool in ISE

Session Trace Test Cases > PEAP_corp_radius_probe

Session Trace Test Case

Test Setup **Run Test** Previous Runs

Test Name

ISE Node ⓘ

ⓘ

Policy Stage	Matching Rule	Result Object(s)
Policy Set		802.1X_Corp_Wireless
Authentication Policy (Allowed Protocols)		All_The_EAPs
Authentication Policy (Identity Selection)	Default	DenyAccess
Exception Authorization Policy		
Authorization policy	RADIUS_Probes	PermitAccess

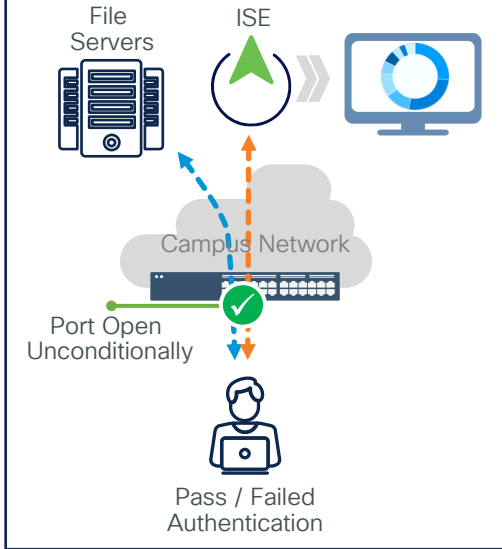
Results assume typical conditions, rather than irregular situations that may cause access failures ⓘ

Agenda

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

Deployment Modes

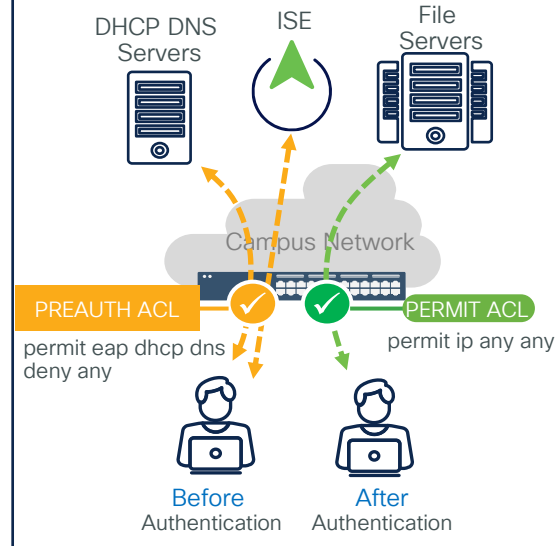
Monitor Mode (Visibility)



authentication open

No impact to existing network

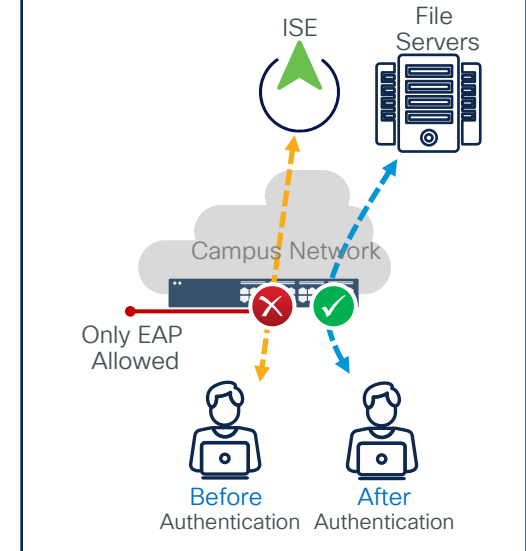
Low-Impact Mode (Visibility and Control)



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

Begin to control and differentiate access





















Closed Mode (Visibility and Control)



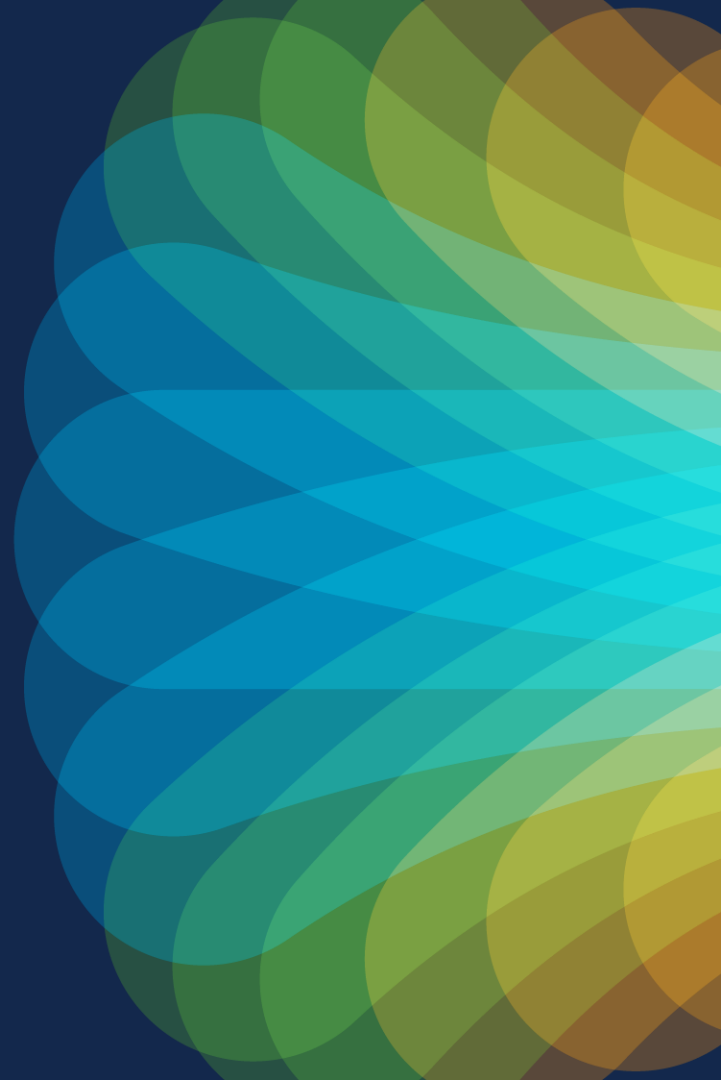
- Not everyone needs Closed Mode
- No access at all before authentication

Utilizing Policy Sets with Modes

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

 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.



ISE learning map

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

START

Monday, February 5 | 8:45 a.m.

TECSEC-3416

Walking on Solid ISE: Advanced use cases and deployment best practices

Monday, February 5 | 2:15 p.m.

TECSEC-3503

Segmenting industrial networks with Trustsec and Cisco Identity Services Engine

Tuesday, February 6 | 8:00 a.m.

BRKSEC-2889

Mastering ISE Upgrades: Best Practices, Tips, and Tricks

Tuesday, February 6 | 5:00 p.m.

BRKSEC-2660

ISE Deployment Staging and Planning

Wednesday, February 7 | 10:30 a.m.

BRKSEC-2039

Secure Access with ISE in the Cloud

Thursday, February 8 | 8:45 a.m.

BRKSEC-2100

ISE Your Meraki Network with Group Based Adaptive Policy

Thursday, February 8 | 2:30 p.m.

BRKSEC-3077

A song of ISE and Posture: Advanced deployment and troubleshooting

Thursday, February 8 | 4:30 p.m.

BRKSEC-2234

Cisco ISE Performance, Scalability and Best Practices

Friday, February 9 | 9:15 a.m.

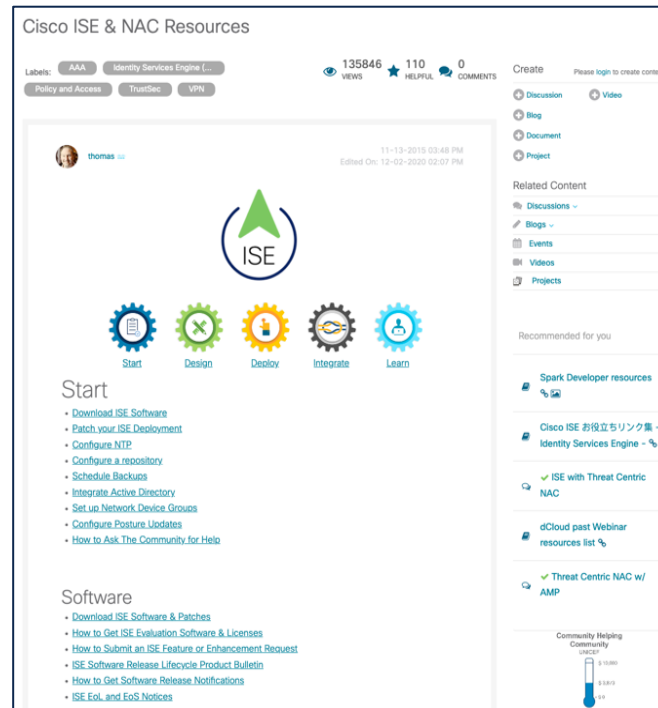
BRKSEC-3412

Unleashing the Art of Troubleshooting Authentication Latency issues.

FINISH

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 - 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!

English Register Login

Cisco Live 2022 FOR REFERENCE BRKSEC - 2660

Find A Community Buy or Renew Cisco Community

This board Search Network Access Control

Technology & Support For Partners Customer Connection Webex Events

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 our 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 Manage... (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 Ame 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 Ame Bier 4 REPLIES 5 HELPFUL 274 VIEWS

cisco ise 2.3 command set & shell profile can work together?
by shlomai 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 shubhampatk1994 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 PERI_Admin 5 REPLIES 5 HELPFUL 1434 VIEWS

Ask a Question

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

Find more resources

Discussions Videos Blogs Documents Gallery Events New Community Member Guide

Featured Projects

From Stateful Firewalling to Next Generation Firewall by Narayan Dev Sarma

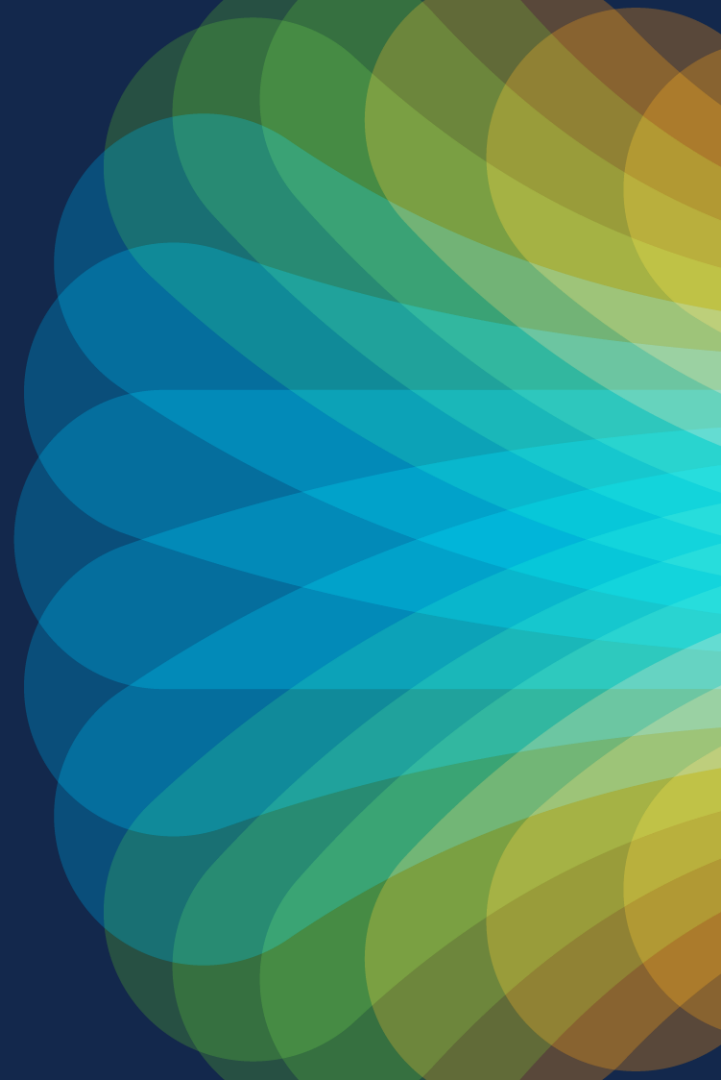
The Importance of the Human



The bridge to possible

Thank you

CISCO *Live!*



The background of the slide is a vibrant, abstract graphic. It features a large, stylized cloud on the left side, composed of overlapping, semi-transparent shapes in shades of red, orange, yellow, and green. To the right of the cloud, a bright, multi-colored sunburst or starburst pattern radiates from a central point, with rays extending towards the right edge of the frame. The colors of the sunburst transition through a spectrum from blue and purple on the left to yellow and orange on the right. The overall effect is energetic and colorful.

cisco *Live!*

Let's go