



Setting the Stage for ISE Deployment Success:

A Guide to Effective Planning

Francesca Martucci

Technical Solutions Architect – Cybersecurity EMEA

BRKSEC-2660

CISCO *Live!*

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

Antoine de Saint-Exupéry

CISCO *Live!*

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

What needs to be included in my planning?

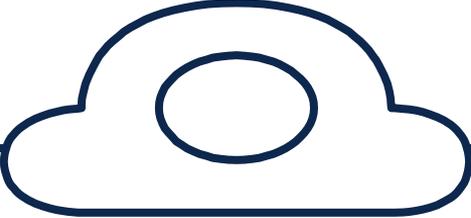


Deploying any network access control solution is **crucial** but it **isn't easy**....



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

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

Webex App

Questions?

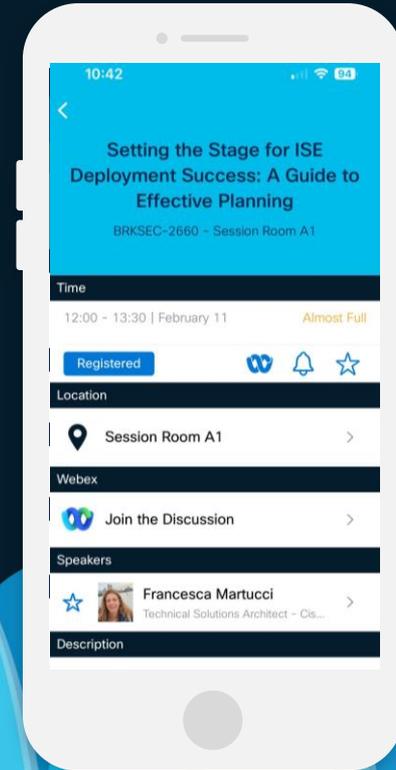
Use the Webex app to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events 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 February 28, 2025.

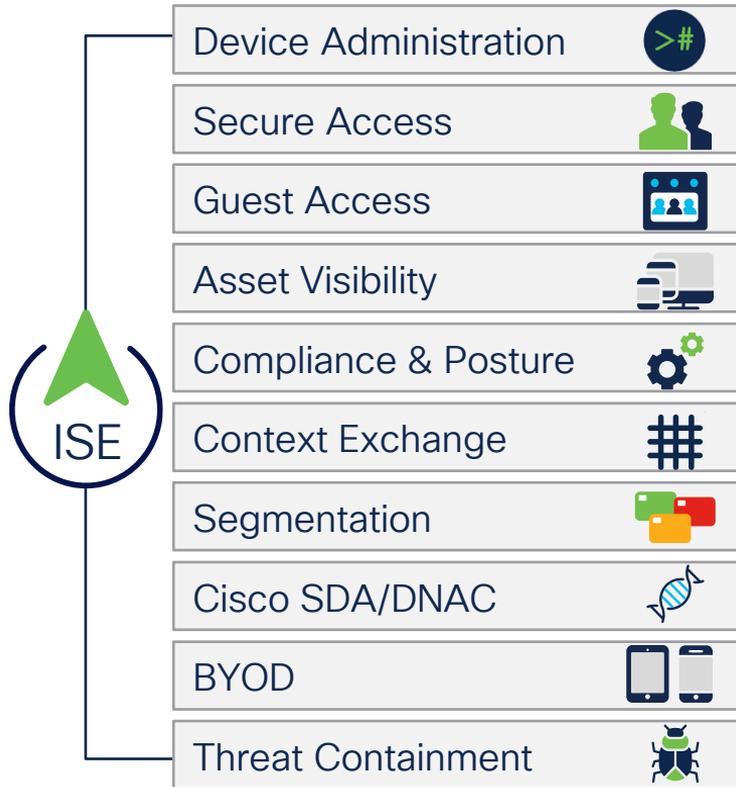
CISCO *Live!*



• 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

Do you need a BYOD policy?

From where do you want to start?

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

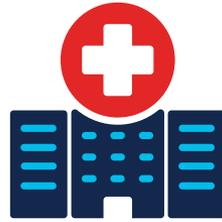
Government



Financials



Healthcare



Retail



Education



Transportation



Services



Utilities



Technology



Manufacturing

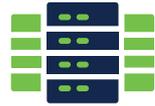


Understand Your Needs and Use cases



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

Example of your ISE policy planning

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

Endpoint Team

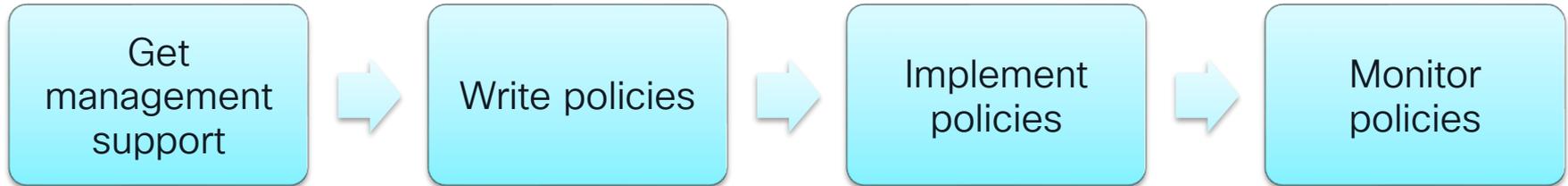
Network Team

Security Team

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

Interoperation with other teams

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



- 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)

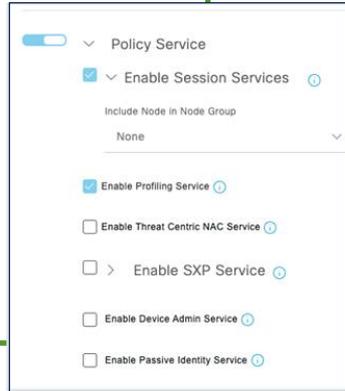
- Administrative GUI
- Policy configuration
- Policy replication
- Centralized Guest database
- Centralized BYOD database
- Configuration REST APIs

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

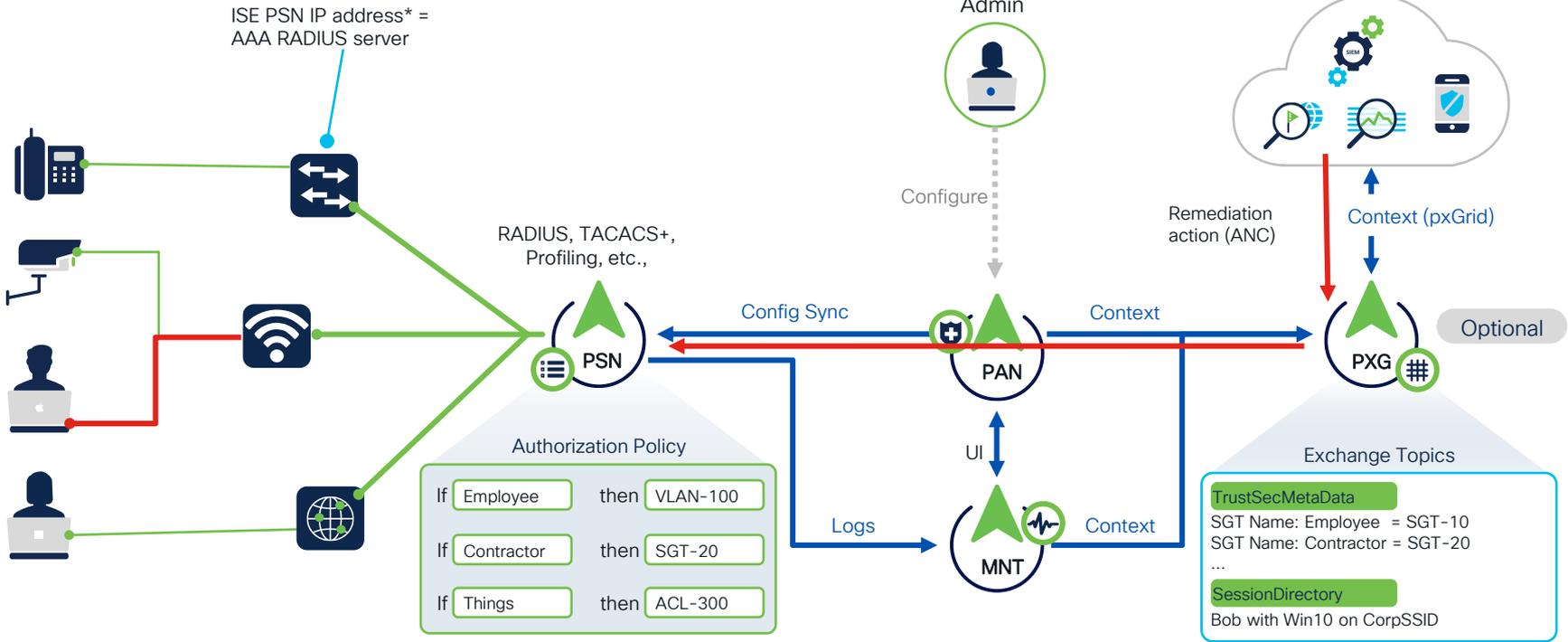


Platform Exchange Grid Node (PXG)

- 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)

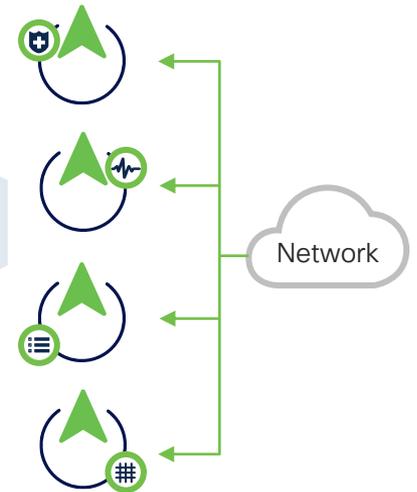
- Max 50 in a deployment



pxGrid Controller

- Max 4 in deployment

Distributed ISE



ISE Scaling



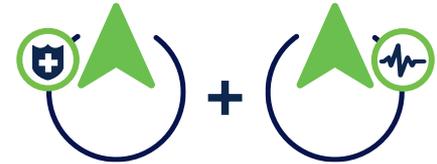
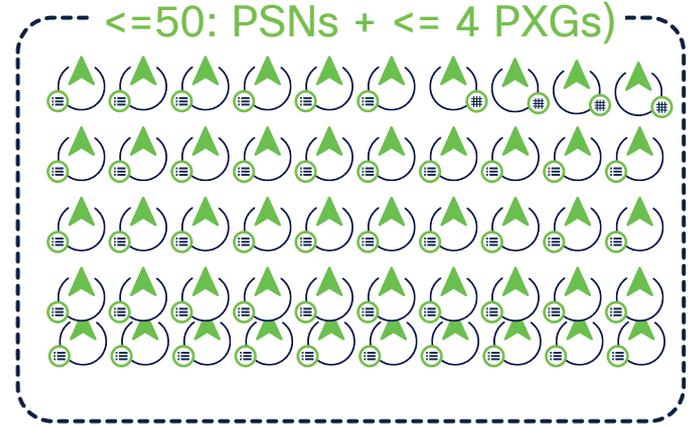
Lab and Evaluation
Only for Lab use (no HA)
Max 100 endpoint



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

Total Maximum Concurrent Active Sessions



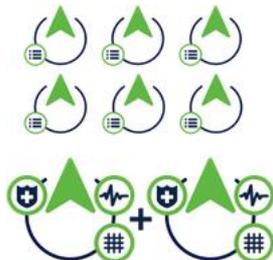
Deployment Type	SNS 3615	SNS 3715	SNS 3595	SNS 3655	SNS 3755	SNS 3695	SNS 3795
Large deployment	Unsupported	Unsupported	500,000	500,000	750,000	2,000,000	2,000,000
Medium deployment	10,000	75,000	20,000	25,000	150,000	50,000	150,000
Small deployment	10,000	25,000	20,000	25,000	50,000	50,000	50,000

Small Deployment

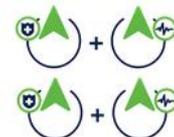


CISCO Live!

Medium Deployment



Large Deployment



PSN Maximum Concurrent Active Sessions

cs.co/ise-scale

Cisco ISE

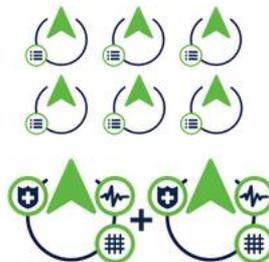


PSN Type	SNS 3615	SNS 3715	SNS 3595	SNS 3655	SNS 3755	SNS 3695	SNS 3795
Concurrent active endpoints supported by a <u>dedicated PSN</u> (ISE node has only PSN persona)	25,000	50,000	40,000	50,000	100,000	100,000	100,000
Concurrent active endpoints supported by a <u>shared PSN</u> (ISE node has multiple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

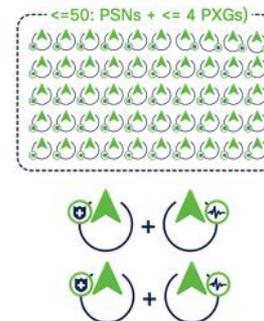
Small Deployment



Medium Deployment

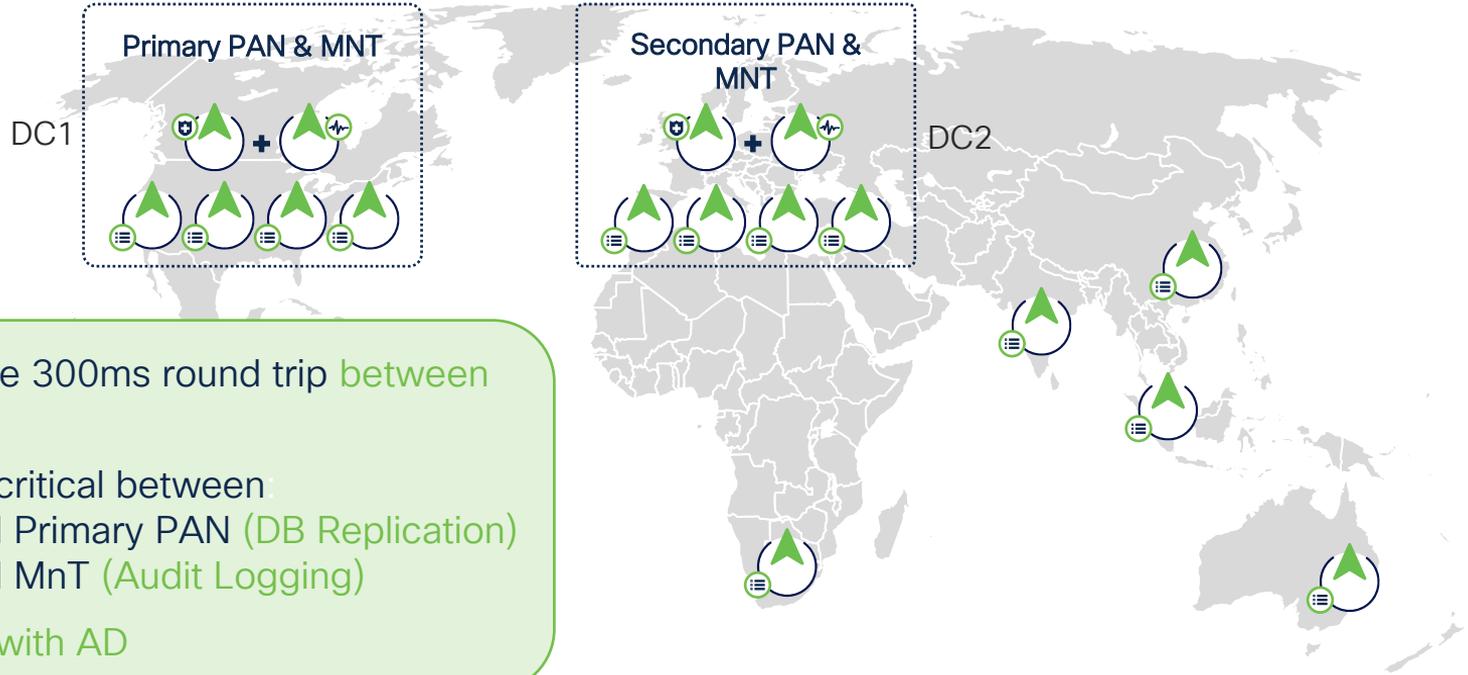


Large Deployment



ISE Fully Distributed Architecture

Centralize in DCs...or Distribute PSNs across Geographies



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



Summary Endpoints Guests Vulnerability Threat

Total Endpoints 1

1

Active Endpoints 0

0

Rejected Endpoints 0

0

Anomalous Behavior 0

0

Authenticated Guests 0

0

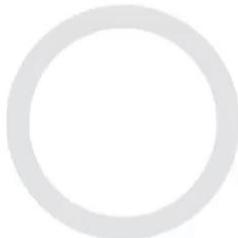
BYOD Endpoints 0

0

AUTHENTICATIONS

Identity Store Identity Group Network Device Failure Reason

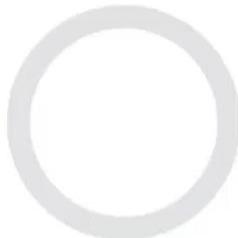
No data available.



NETWORK DEVICES

Device Name Type Location

No data available.

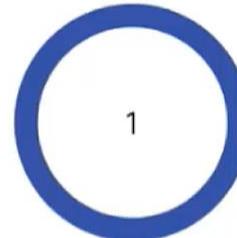


ENDPOINTS

Profile Logical Profile

1

vmware-device - 100%



BYOD ENDPOINTS

Type Profile

No data available.

ALARMS

Severity Name Occu... Last Occurred

Name

ISE Authentication In... 388 8 mins ago

SYSTEM SUMMARY

1 node(s)

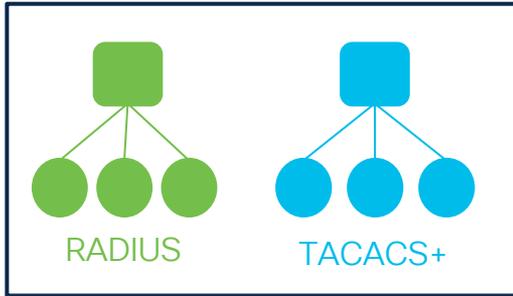
ISE31-1ek

All 24HR

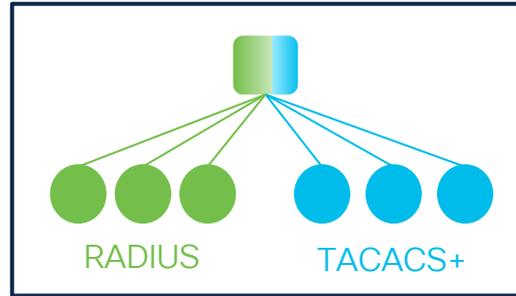
TACACS+ Deployment Models

Separating RADIUS & TACACS+ ISE Cubes?

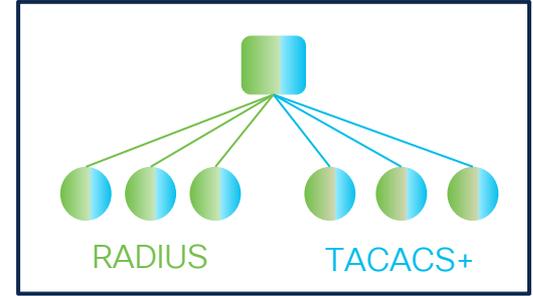
There are three different options:



Separate ISE cubes



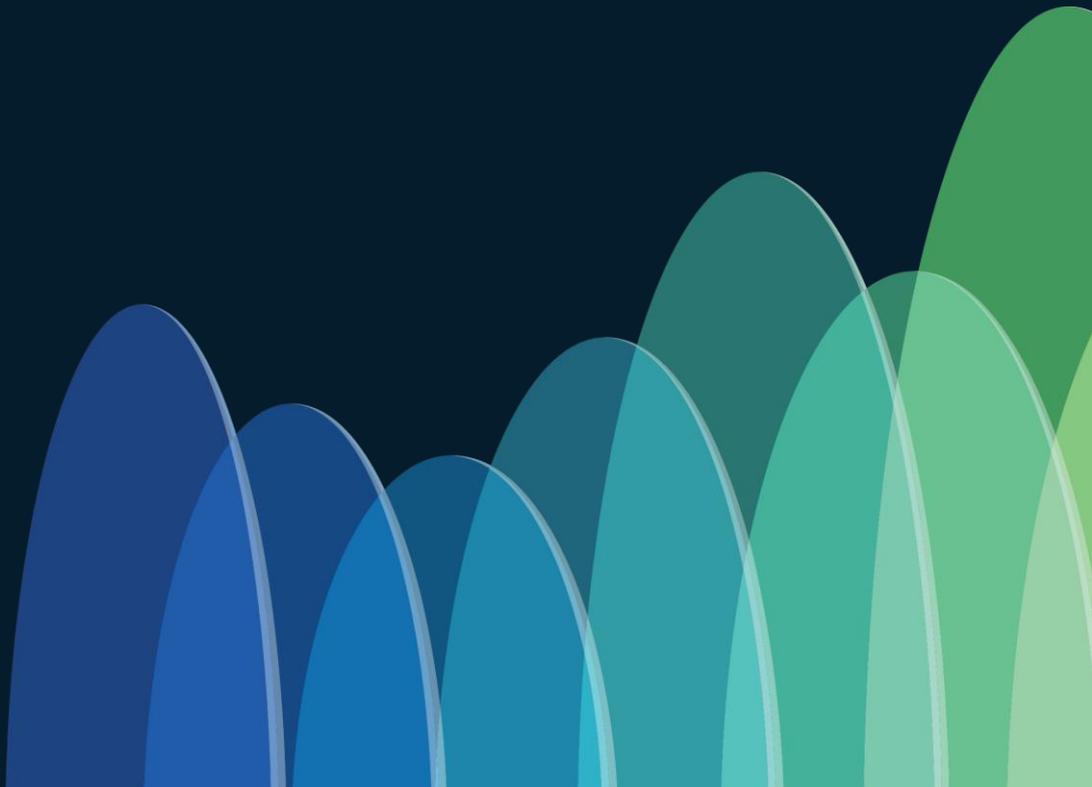
Mixed ISE cube with separate PSNs



Mixed ISE cube with shared PSNs

- Scalability is transactions per second (TPS)
- Authentication or also Commands Authorization?
- Do you use scripts?
- How much Log Retention do you need?

- 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 and service.](#)
- Can [manage](#) all node's system certs [from PPAN](#)

✓ Trusted Certificates

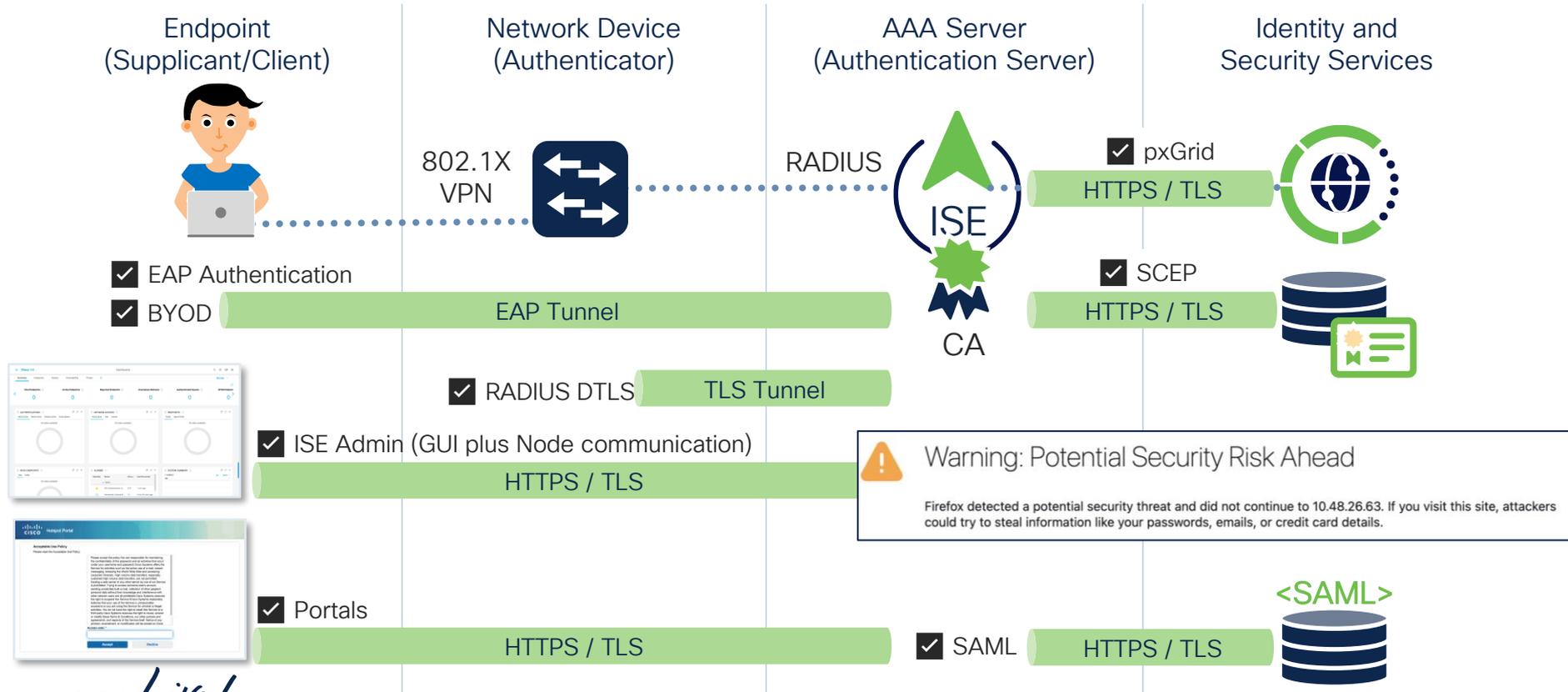
List of CAs

- 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
<input type="checkbox"/> ISE30-1ek 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_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			

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

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

Each ISE node has its own System Certificate Store



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

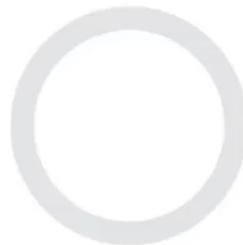
No data available.



NETWORK DEVICES

Device Name Type Location

No data available.

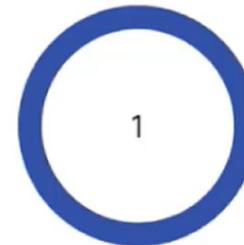


ENDPOINTS

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)

ISE31-1ek

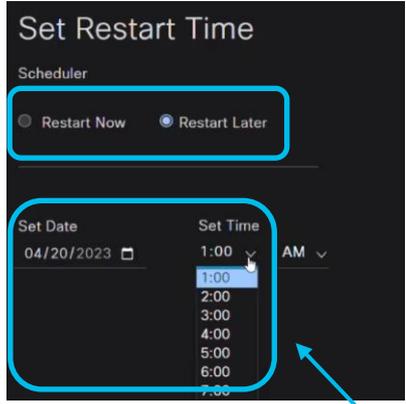
All 24HR

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



	Hostname	Personas	Role(s)	Services	Restart Time	Restart Status
<input type="checkbox"/>	isebeta2	Administration, Monitoring	SEC _{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`

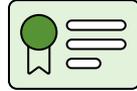
~6.5 min in ISE 3.4

Using the commands
`reload`

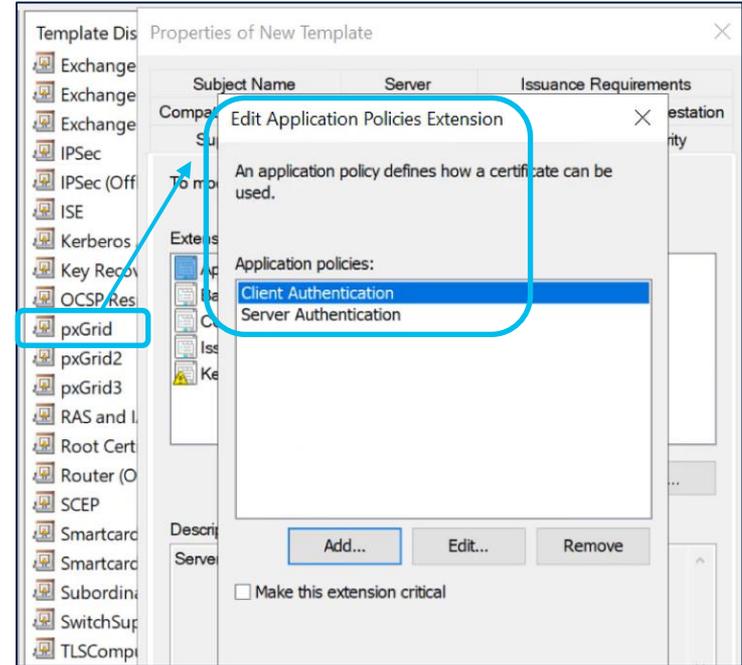


PxGrid Certificate

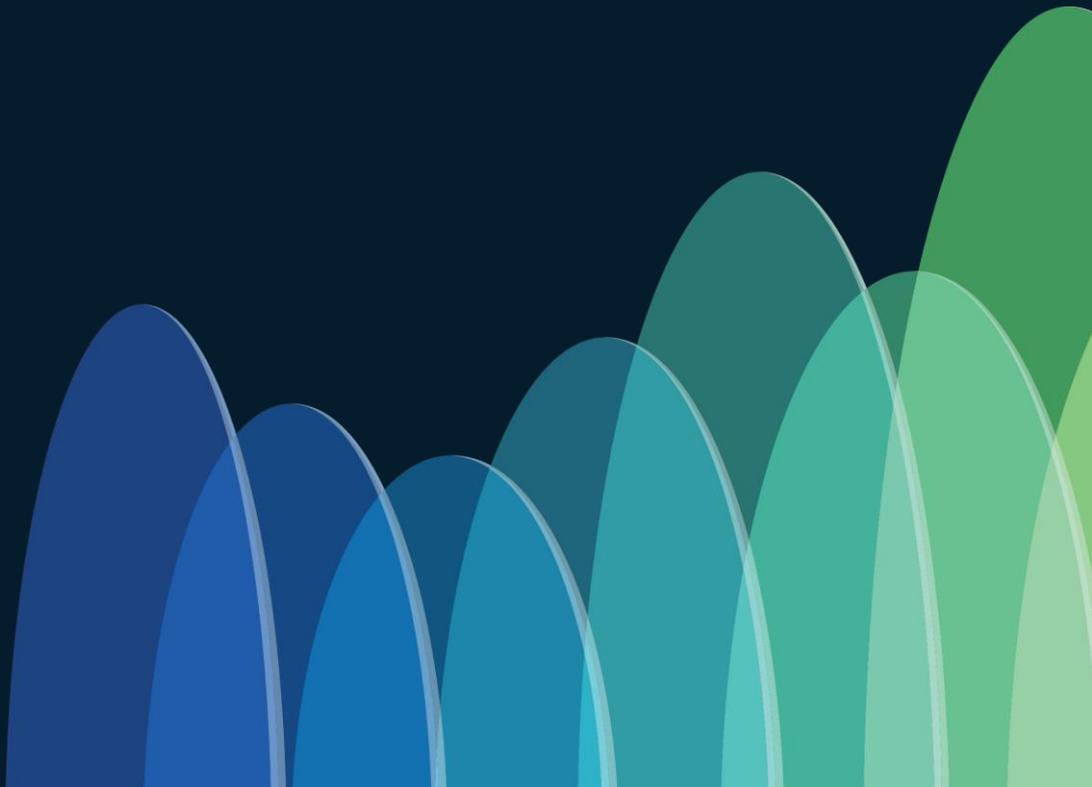
PxGrid certificate is built with both **Client Authentication** and **Server Authentication** extension



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



- 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

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								
IE4000 IE5000	IOS 15.0(2)EB	✓	✓	✓	✓	X	✓	✓	✓
	IOS 15.2(2)E5	✓	✓	✓	✓	✓	✓	✓	✓
IE4010	IOS 15.2(4)E2	✓	✓	✓	✓	✓	✓	✓	✓
	IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✓
SMB SG500	Sx500 1.4.8.06	4	!	X	X	X	X	X	X
	Sx500 1.2.0.97	!	!	X	X	X	X	X	X

 cs.co/nad-capabilities

² Refer to [Cisco Compatibility Matrix](#)

CISCO Live!

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

Total Endpoints ⓘ

165

Active Endpoints ⓘ

5

Rejected Endpoints ⓘ

0

Anomalous Behavior ⓘ

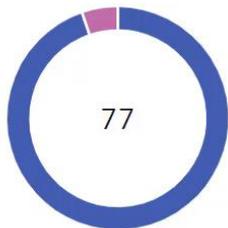
0

Authenticated

AUTHENTICATIONS ⓘ

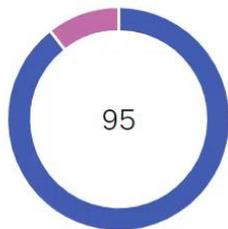
Identity Store Identity Group Network Device

Failure Reason



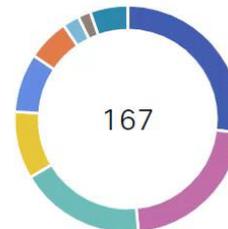
NETWORK DEVICES ⓘ

Device Name Type Location



ENDPOINTS ⓘ

Profile Logical Profile



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

Name	Description
All Device Types	All Device Types
All Locations	All Locations
Is IPSEC Device	Is this a RADIUS over IPSEC
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



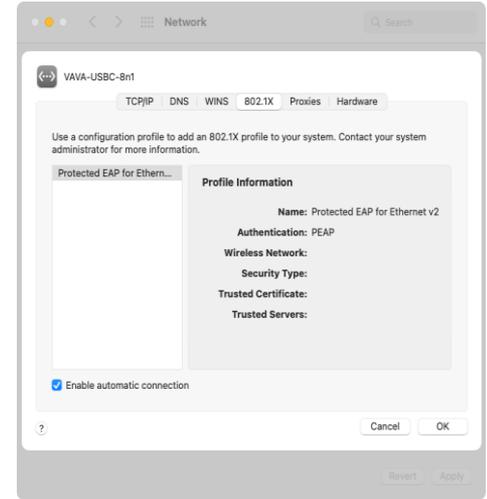
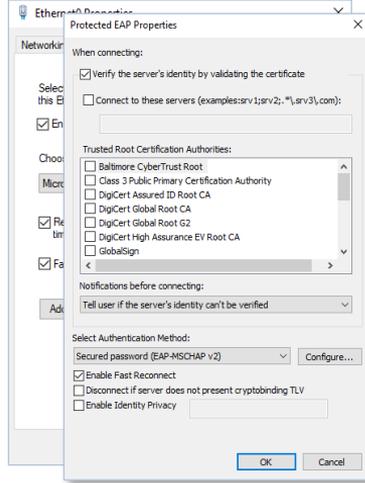
Additional Tips

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



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

Endpoints: Native 802.1X Supplicants



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



```
wpa_supplicant

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

SYNOPSIS
wpa_supplicant [ -BddfhKLqgsTtuvW ] [ -ifname ] [ -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
```

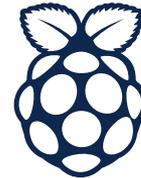


Windows 7, 8/8.1, and 10 – Native Supplicant

- 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

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

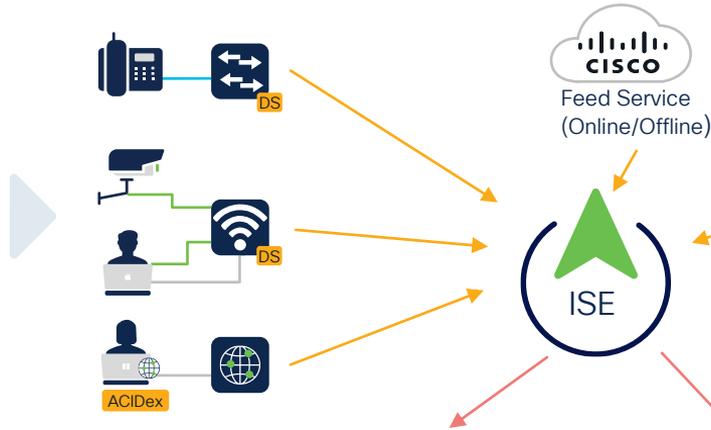
Endpoints: Everything Else



Endpoint Profiling

The profiling service dynamically classifies devices connected to your network

Endpoints send interesting data, that reveal their device type



ISE Data Collection Methods for Device Profiling

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

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

AnyConnect: ACIDex

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

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

ISE 3.3

Manufacturer	Device Type	Model	OS
 Cisco Arlo Apple Lenovo	 IP-Phone Camera Laptop Laptop	 IP Phone 7980 Pro wireless Cam MacBook Pro Thinkpad 540	 iOS Linux macOS 12.0.1 Windows Enterprise

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

Effect of RADIUS Probe



vendor

OUI = Vendor ID, IP = xx.xx.xx.xx



Cisco Device

OUI = Cisco, IP = xx.xx.xx.xx



HP Device

OUI = HP, IP = xx.xx.xx.xx



Apple Device

OUI = Apple, IP = xx.xx.xx.xx

Effect of SNMP Probe



Unknown

OUI = Random, IP = xx.xx.xx.xx



Cisco 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 iPad

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

Effect of NMAP Probe



Windows10-Workstation

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



Cisco IP Phone 9971

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



HP LaserJet P4015

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



Apple iPad

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

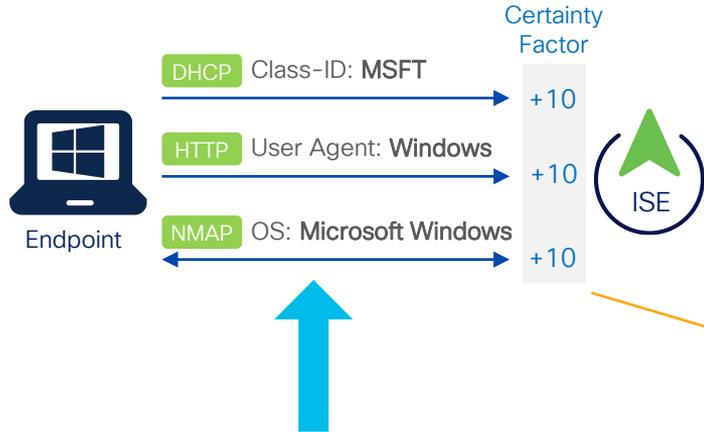
OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet, FQDN=test-printer1.zero0k.org, SNMP:hrDeviceDescr CONTAINS HP LaserJet P4015



Apple iPad

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

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	<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

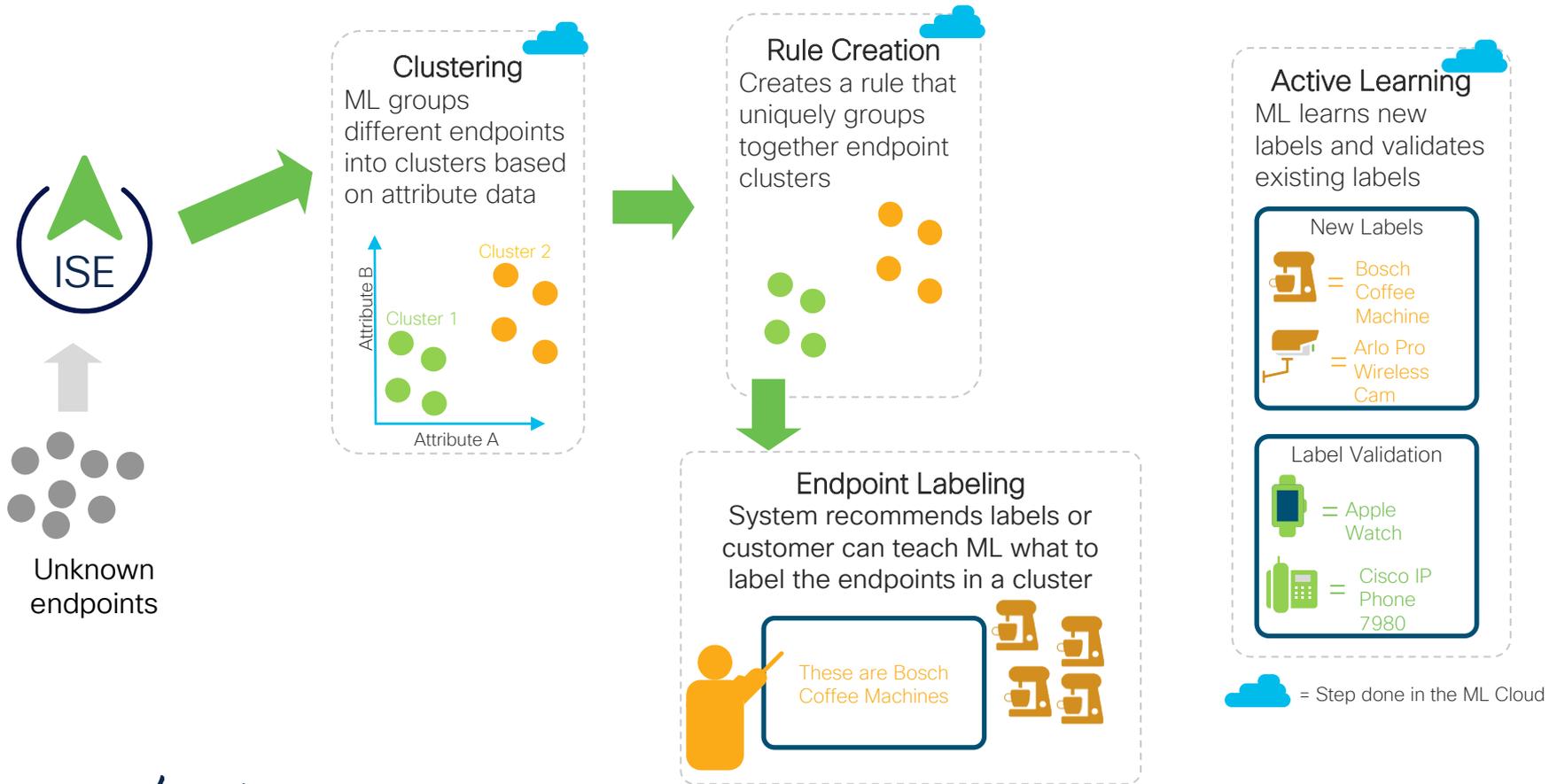
If	Condition	Then	Certainty Factor
	Microsoft-WorkstationRule2Check1	Certainty Factor Increases	10
	Microsoft-Workstation-Rule4-Check1	Certainty Factor Increases	10
	Microsoft-WorkstationRule3Check1	Certainty Factor Increases	10
	Microsoft-WorkstationRule1Check1	Certainty Factor Increases	10

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



Review the AI Proposals

Identity Services Engine Context Visibility / Endpoints

Authentication BYOD Compliance Compromised **Classification** Guest Vulnerable Hardware 5G More Manage Hide Charts

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Features

ENDPOINT CATEGORIES

OUI OS Types Identity Group

Category	Percentage
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.

Review

Rows/Page 10 / 36 1 / 36 Go 353 Total Rows

MAC Address	Anomalous Behavior	IP Address	Username	Hostname	Location	Endpoint Profile	Description
00:00:F0:0A:00:01		10.1.102.12		Cisco		Samsung-Device	
00:00:F0:0A:00:02		10.1.102.13	BRKSEC-2660				

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

Choose the Proposal to View

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Context Visibility . Endpoints'. A sidebar on the left contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area is titled 'Profile Unknown Endpoints with AI Proposals ^{BETA}'. It features an illustration of a person at a desk with a laptop, a 'Group of endpoints' diagram, and a lightbulb icon. A modal window titled 'What are AI Proposals?' is open, explaining that AI Proposals are sets of features that group endpoints with common attributes and suggest labels. Below the modal is a table of AI Proposals (7) with columns for Endpoint Count, MFC-Endpoint Type, MFC-Hardware Manufacturer, MFC-Hardware Model, MFC-OS Type, and Actions. The second row, representing Apple devices, is highlighted with a green box and a green arrow pointing to the 'View Proposal' link.

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

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

Equal:

Select attribute for condition

Dictionary

Attribute

ID

Info

EndPoints

<input checked="" type="checkbox"/>	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

Default Network Access 13

Default policy set

> Authentication Policy(3)

> Authorization Policy - Local Exceptions

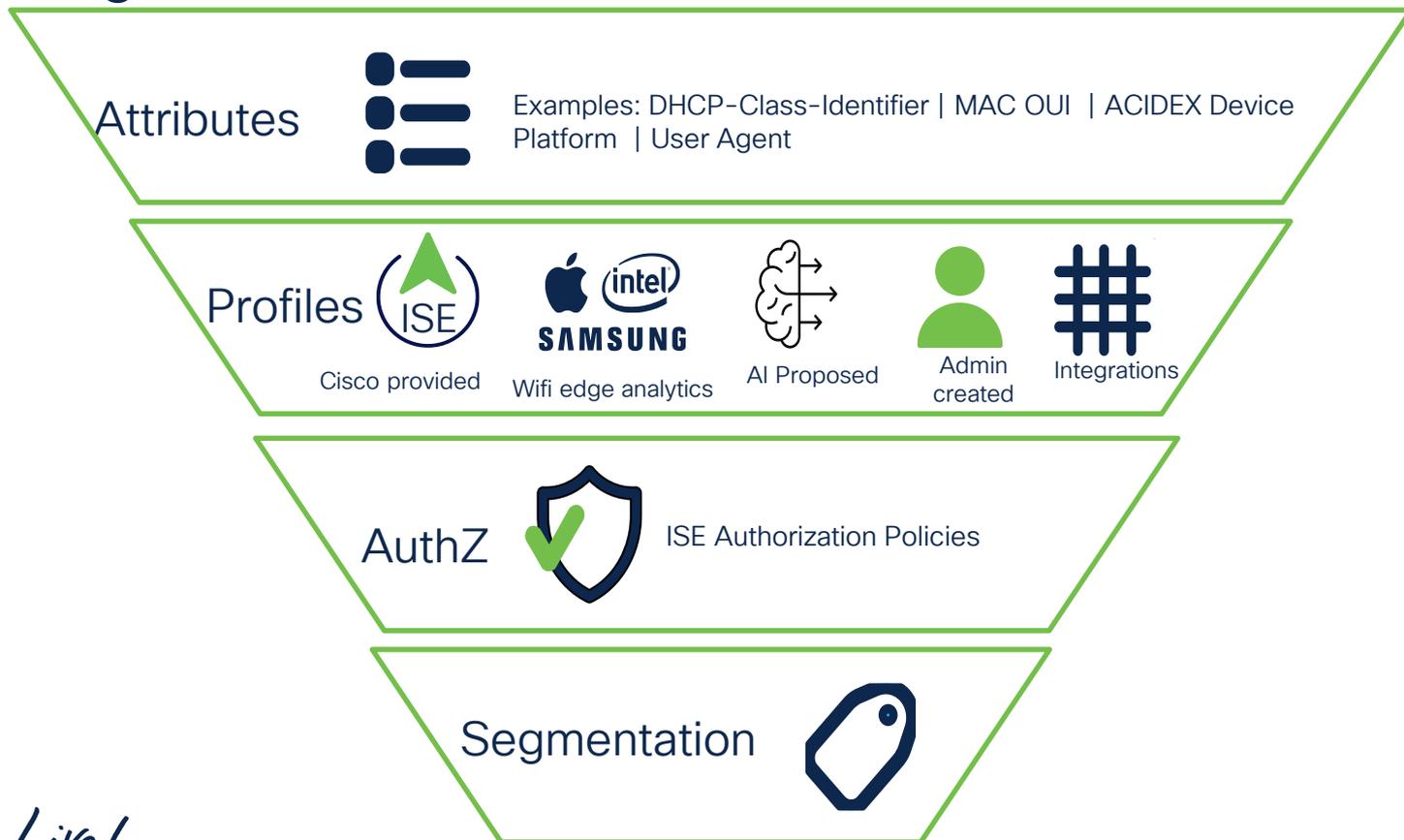
> Authorization Policy - Global Exceptions

∨ Authorization Policy(13)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	IOT Devices	EndPoints-MFCInfoEndpointType EQUALS IOT Device	IOT_ONLY x	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_Passed Compliance_Unknown_Devices	Cisco_Temporal_Onboard BRKSEC-2660	Select from list	0	

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

Turning Probes Into Profiles, Profiles Into Protection



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

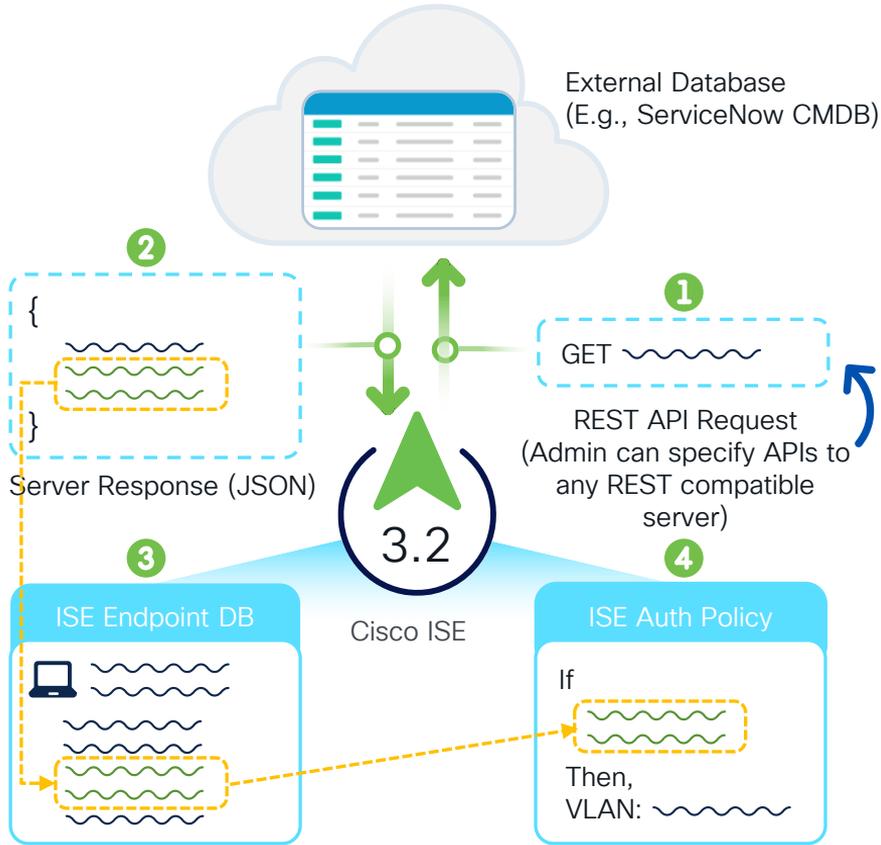
Attribute Name	Type
Created	Date
Expires	Date
Owner	String
Department	String
iPSK	String

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 CMDBs



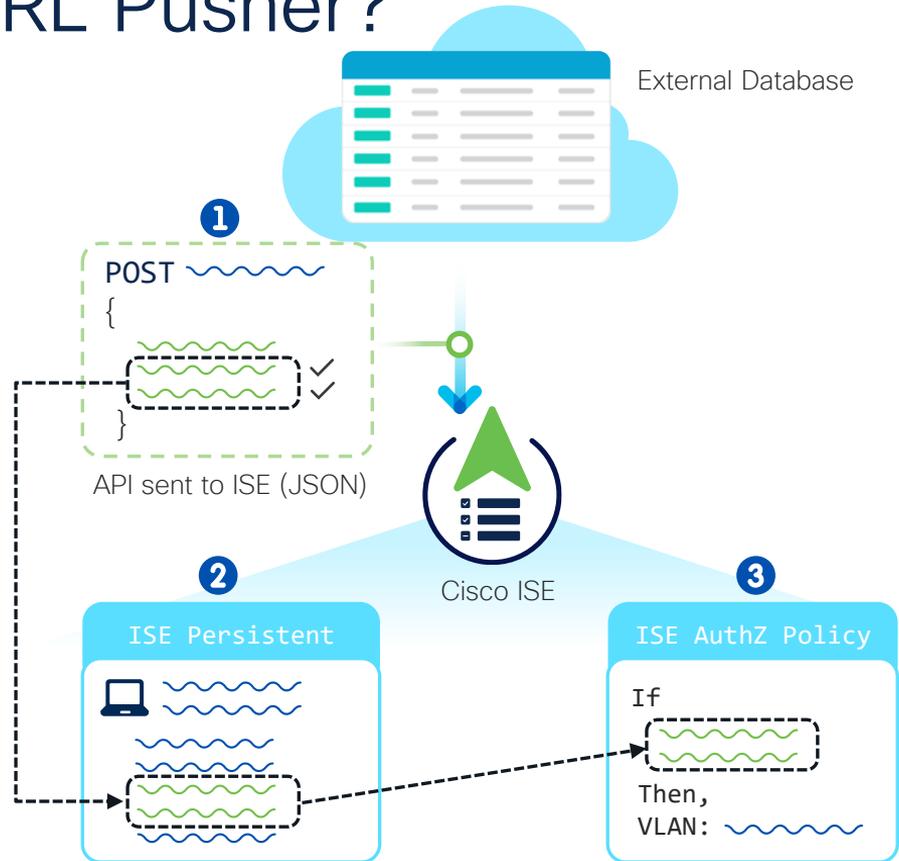
```

{
  "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?

- 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)

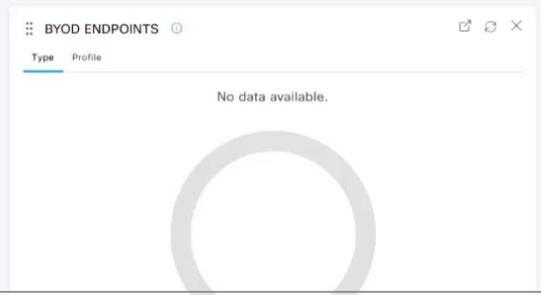
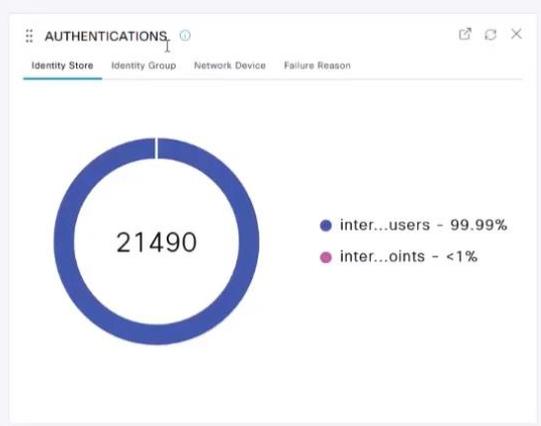


- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration
- Work Centers
- Interactive Features

Summary | Endpoints | Guests | Vulnerability | Threat | Manage

Summary Metrics:

- 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
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	Insufficient Virtual M...	28	11 hrs 22 mins ...



- 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

- Easier to read policies
- Better rule processing
- Group similar rules (MAB vs. dot1x, SSID, location)
- Conditions based on attributes from initial RADIUS packet:

Organizations



Type

Location



Vendor/Model

Medium



RADIUS



Wireless

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

Conditions simplification

Pre-sets Dictionary Condition are easy to read and intuitive

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 AND Radius-NAS-Port-Type EQUALS Ethernet AND AD1-ExternalGroups EQUALS securitydemo.net/Users/Employees AND Network Access-EapTunnel EQUALS PEAP AND Network Access-EapAuthentication EQUALS EAP-TLS	WIRED-EMPLOYEE-ACC... x
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
<input checked="" type="checkbox"/>	Dynamic Match Rule	if Radius:Calling-Station-ID MATCHES LDAP1 Department then	Permit Access



▼ **Advanced Attributes Settings**

Radius:Class = InternalEndpoint groupPolicy

Speed Test

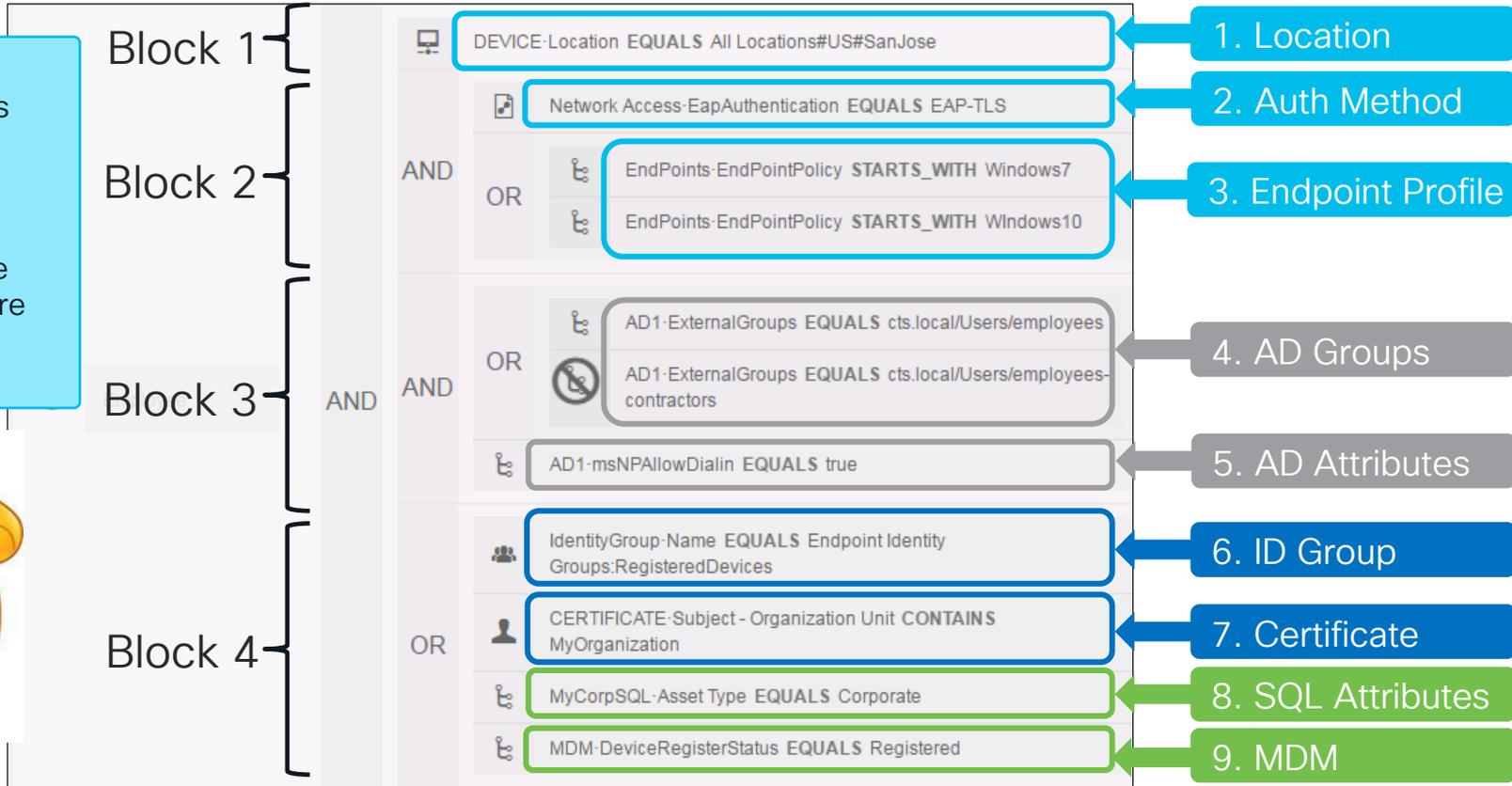
Is the image matching the condition set?

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



Auth Policy Optimization

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

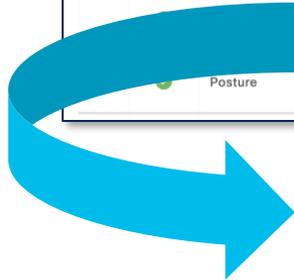


Can you reorder some of the policy sets?

Review and Reorder

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	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	⚙️	➔
	Posture		win-posture-endpoints	Default Network Access	39786	⚙️	➔



Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	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

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

Who Needs an ISE Lab? You do!



With ever **Standalone** installation :

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

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

ISE Lifecycle Orchestration & Policy Management



Zero Touch
Deployment



Patch
Installation



License
Management



Certificate
Management



Configuration
Management



Policy
Management



Operations
Automation



ISE 3.1
Patch 1 or later



Python



Ansible



VSCode



github.com/CiscoISE

#YAML

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

ISE Deployment and Operational Lifecycle



Provision

Deploy

Configure

Operate

Extend

VPC(s)
 Networks
 VPNs
 ISE Nodes
 Patch + Hotpatches
 Load Balancers
 ... **cisco Live!**

Enable APIs
 Repositories
 Roles
 Services
 Certificates
 Licensing 😊
 ...

Identity Stores
 Network Devices
 Policy Sets
 Endpoints
 Portals
 ...

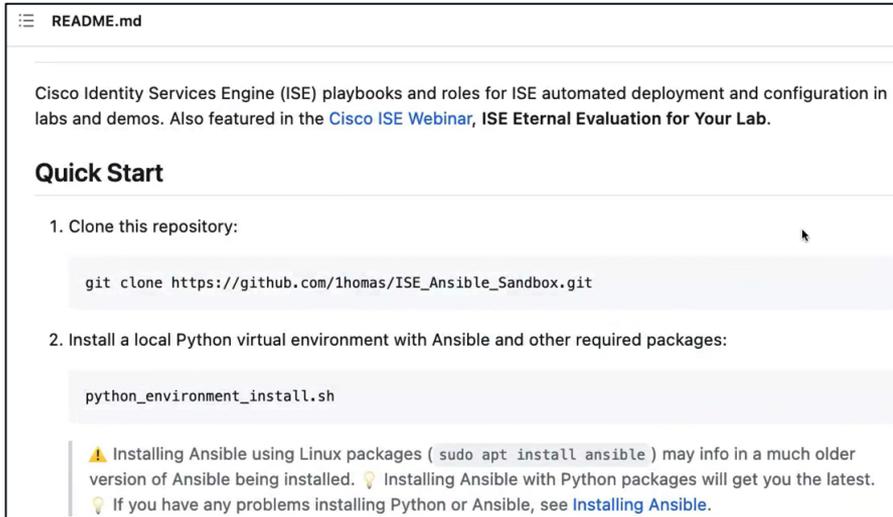
Manage Endpoints
 Reporting
 Performance
 pxGrid / Events
 Backup/Restore
 Patch

Terminate
 ...

ISE Eternal Evaluation

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

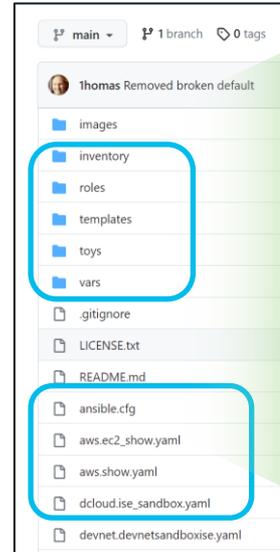
1. Clone this repository:

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

```
python_environment_install.sh
```

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

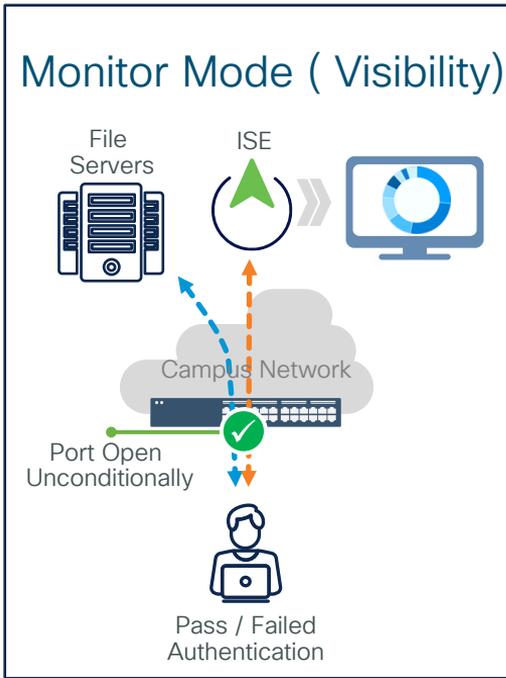
iseee.yaml



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

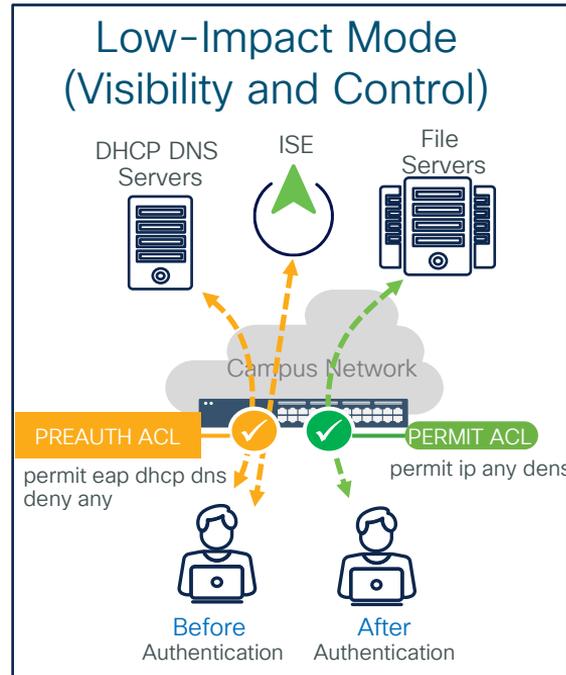
- Where to start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

Deployment Modes



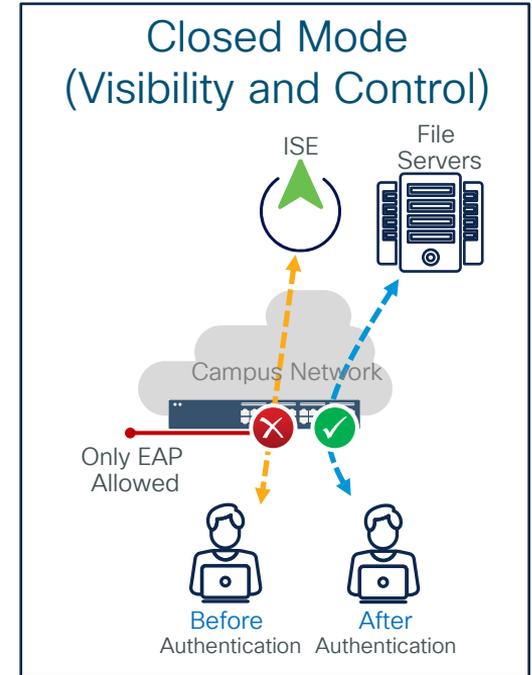
authentication open

No impact to existing network



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

Begin to control and differentiate access



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

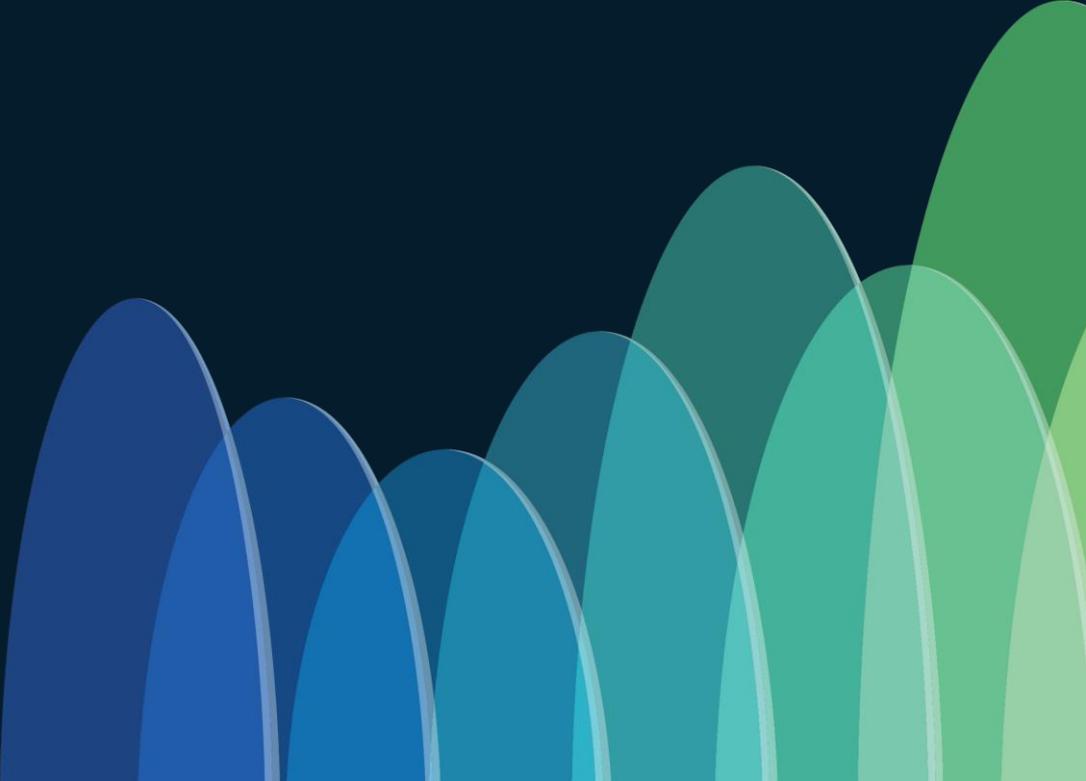
Utilizing Policy Sets with Modes

- 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

CISCO *Live!*



User involvement

User Communication before and after ISE rollout



Cisco Live!



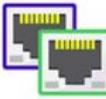
Wired Authentication Support Page

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...

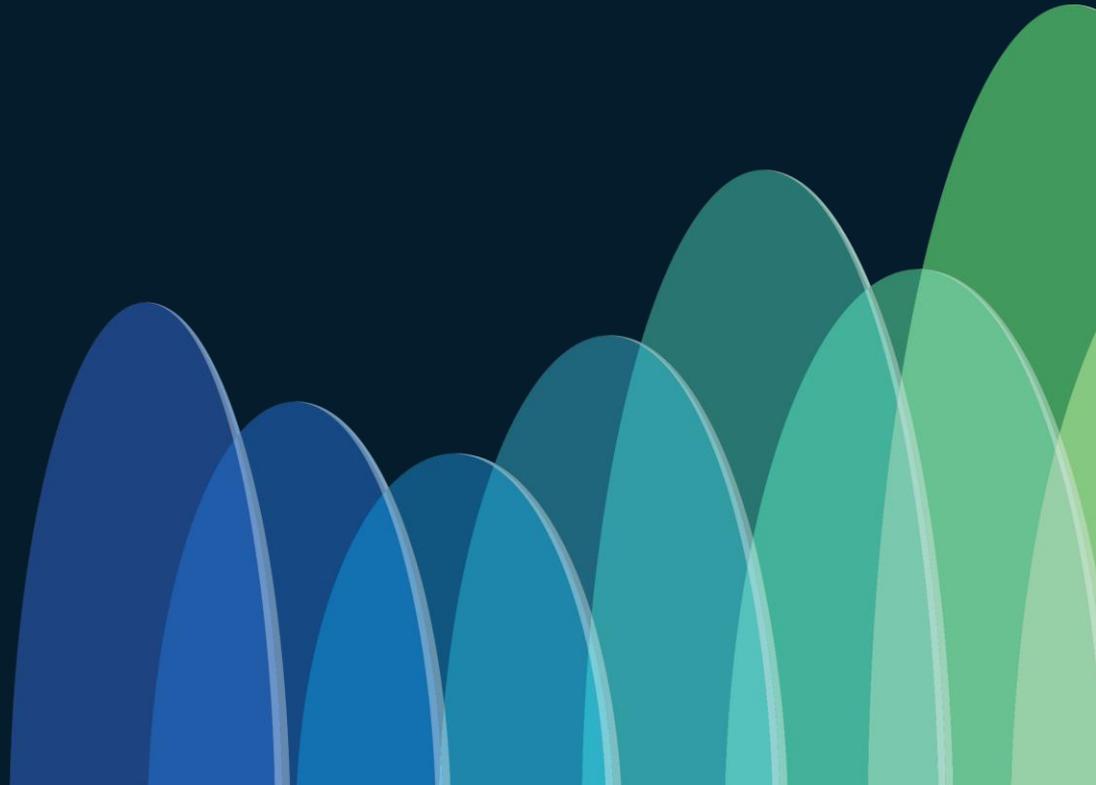
					
Cisco Managed Windows Laptops	Mac Laptops	Remote Desktops Windows Only	Linux / Unix workstations	Voice/Video Endpoints	Non IT Managed Printers
					
Personal devices (Apple TVs, PlayStation etc.)	Routers, Switches, ESXi, and APs	Onsite (In-Office) - Patching	Demo/Training devices	Password Management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



Security

ISE

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 10 | 4:00 p.m.

BRKSEC-2100

ISE Your Meraki Network with Group Based Adaptive Policy

Tuesday, February 11 | 8:00 a.m.

BRKENS-1852

TrustSec Refresh Reinforced with Common Policy Innovations

Tuesday, February 11 | 12:00 p.m.

BRKSEC-2660

Setting the Stage for ISE Deployment Success: A Guide to Effective Planning

Tuesday, February 11 | 4:30 p.m.

BRKSEC-2416

Cisco ISE Meets Azure Cloud. Deploy, Automate, Integrate with Entra ID and Intune

Wednesday, February 12 | 8:00 a.m.

BRKSEC-2889

Mastering ISE Upgrades: Best Practices, Tips, and Tricks

Wednesday, February 12 | 1:00 p.m.

BRKSEC-2053

Zero Trust: Securing the Evolving Workplace

FINISH

Thursday, February 13 | 10:45 a.m.

BRKSEC-3707

Advanced SGT - Multi Domain Context

Thursday, February 13 | 3:15 p.m.

BRKSEC-3234

Cisco ISE Performance, Scalability and Best Practices

Friday, February 14 | 9:00 a.m.

BRKSEC-3077

A Song of ISE and Posture: Advanced Deployment and Troubleshooting

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 ...

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

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!

FOR REFERENCE

BRKSEC-2660

Buy or Renew

Find A Community

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 our best practices.

Network Access Control

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

Labels

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

MAB / Voice Authentication
by wizi on 01-21-2022 02:05 PM - Latest post on 01-26-2022 03:17 PM by Ame Bier

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

ISE recommended thresholds
by shubhampatki1994 on 01-26-2022 10:05 AM

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

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

Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog

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 ciscolive.com/on-demand. Sessions from this event will be available from March 3.



Thank you

CISCO *Live!*

CISCO *Live!*

GO BEYOND

A series of overlapping, rounded, teardrop-shaped abstract forms in various shades of blue, ranging from light to dark, positioned on the right side of the image.