The bridge to possible

ISE Deployment Improvements Tips and Tricks

Katherine McNamara – Technical Solutions Architect

BRKSEC-2347

Cisco Live!

#CiscoLive

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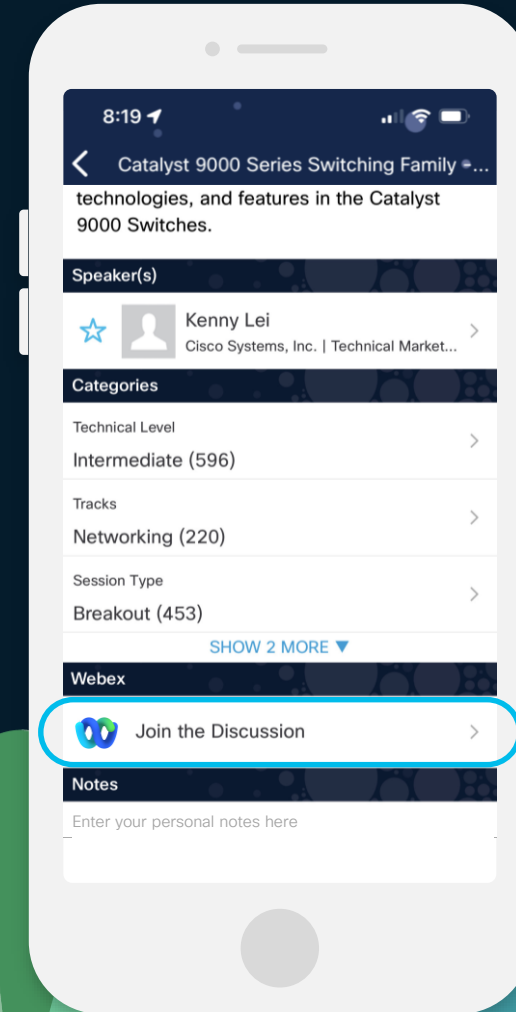
Questions?
Use Cisco Webex App to chat
with the speaker after the session

How

1 Find this session in the Cisco Live Mobile App

2 Click "Join the Discussion"

3 Install the Webex App or go directly to the Webex space

4 Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 7, 2024.

Agenda

- Where to Start
- Laying the Foundation
- A Phased Approach
- Tuning Policy Sets
- The Power of Profiling
- Integrations
- Post-Deployment
- Conclusion

A little about me...

- Started as an early ISE 1.1 customer

- 15+ years of network & security experience

- Lots of paper: BS and MS in IT Security, 2x CCIE (Data Center + Security), CISSP, and various other industry certifications

- Co-authored recent CiscoPress SISE book

- Co-organize for the largest Cisco Meetup study group – Routergods and owner of network-node blog

Where to Start

Simplifying and optimizing your deployment is how you can lower the administrative burden of managing ISE

The Swiss Army Knife of Network Access Control

ISE

Device Administration
TACACS+ Migrating from Cisco Secure ACS or building a new Device Administration Policy Server, this allows for secure, identity-based access to the network devices

Secure Access
Allow wired, wireless, or VPN access to network resources based upon the identity of the user and/or endpoint. Use **RADIUS** with **802.1X, MAB, Easy Connect, or Passive ID**

Guest Access
Differentiate between **Corporate and Guest** users and devices. Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options

Asset Visibility
Use the probes in ISE and Cisco network devices to classify endpoints and authorize them appropriately with **Device Profiling**. Automate access for many different **IoT** devices

Compliance & Posture
Use **agentless posture**, **Cisco Secure Client**, **MDM**, or **EMM** to check endpoints to verify compliance with policies (Patches, AV, AM, USB, etc.) before allowing network access

Context Exchange
pxGrid is an ecosystem that allows any application or vendor to integrate with ISE for endpoint identity and context to increase **Network Visibility** and facilitate automated Enforcement.

Segmentation
Group-based Policy allows for segmentation of the network through the use of Security Group Tags (SGT) and Security Group ACLs (SGACL) instead of VLAN/ACL segmentation.

Cisco SDA/DNAC
ISE integrates with **DNA Center** to automate the network fabric and enforces the policies throughout the entire network infrastructure using Software-Defined Access (SDA)

BYOD
Allow employees to use their own devices to access network resources by registering their device and downloading certificates for authentication through a simple **onboarding** process

Threat Containment
Using a **Threat Analysis** tool, such as Cisco Cognitive Threat Analytics, to grade an endpoints threat score and allow network access based upon the results

Where To Start...

- Define your business and security objectives
  - What is it that you want ISE to do for you?

- Determine which teams will be needed
  - Virtualization team?
  - Desktop support?
  - PKI?
  - etc

- Collaborate with those teams at the beginning of the project

- Get management buy-in early

Laying the Foundation
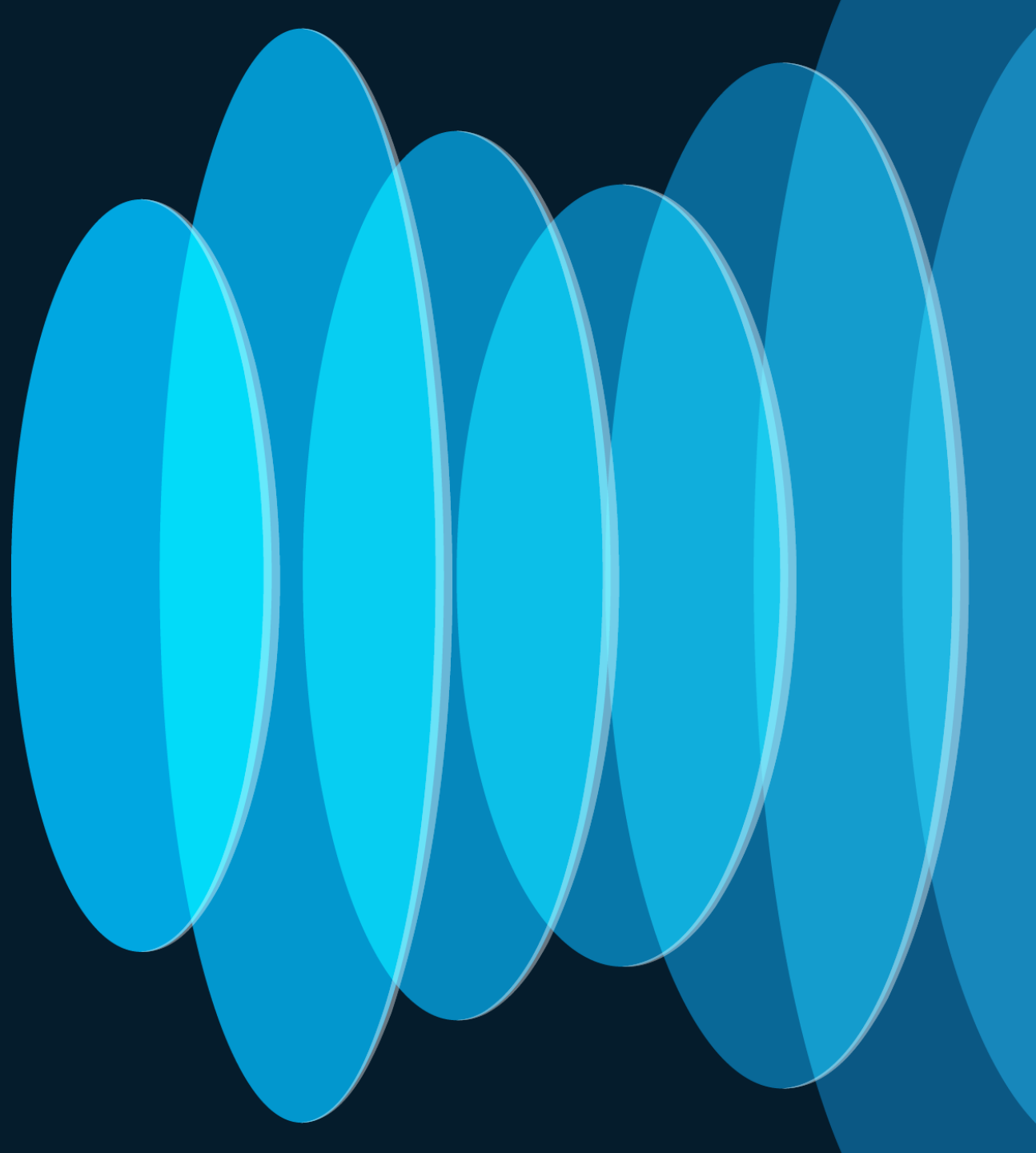
Let's Talk about ISE Personas...

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

- Monitoring Node (MNT)
  - Max 2 in a deployment

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

- pxGrid Node
  - Max 4 in a deployment

Policy Administration Node (PAN)
- Single plane of glass for ISE admin
- Replication hub for all database config changes

Monitoring and Troubleshooting Node (MnT)
- Reporting and logging node
- Syslog collector from ISE Nodes

Policy Services Node (PSN)
- Makes policy decisions
- RADIUS/TACACS+ Servers

pXGrid Controller
- Facilitates sharing of context

ISE Deployment Scale
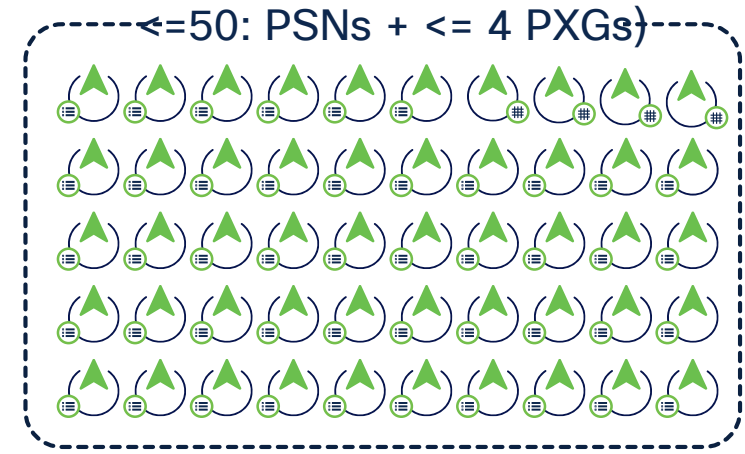
Lab and Evaluation

Small HA Deployment
2 x (PAN+MNT+PSN)
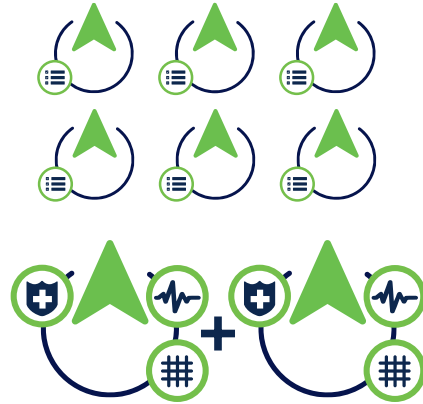
Medium Multi-node Deployment
2 x (PAN+MNT+PXG), <= 6 PSN
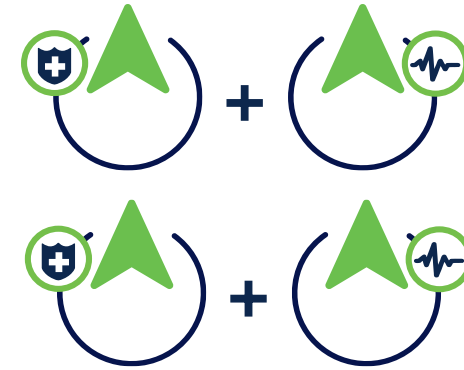
Large Deployment
2 PAN, 2 MNT, <=50: PSNs + <= 4 PXGs

| 100 Endpoints | Up to 50,000 Endpoints | Up to 2,000,000 Endpoints | 3600 |
| 100 Endpoints | Up to 100,000 Endpoints | Up to 2,000,000 Endpoints | 3700 |

ISE Node Types

Physical Appliances	Virtual Machines	Cloud Instances

Physical Appliances

SNS-3795
SNS-3755
SNS-3715
SNS-3695
SNS-3655
SNS-3615
SNS-3595

Virtual Machines

KVM

Microsoft

NUTANIX

vmware®

Cloud Instances

aws

Azure

ORACLE

Future

Google

Expanding Your ISE Deployment...

Adding an ISE Node

Changing the Persona

Recommendations

- Make your life easier: Use load balancers
  - Easier to add PSNs
  - Easier to upgrade
  - Failover is more seamless

- Scale up as you grow

- VMs or appliances? Same specs!

- Device Admin? Think about separate PSNs for TACACS+

- Use the ISE Scalability Guide as a reference

Licensing

- Endpoint licenses are based on <u>concurrently connected</u> endpoints only

- Endpoint licenses are term-based

- Endpoint licenses does not include Secure Client/AnyConnect licenses

- Other license types:
  - Virtual Machine Licenses
  - Device Admin Licenses

3.x Model

Premier (Compliance with Advantage)
- Posture
- MDM Compliance
- TC-NAC

Advantage (Context with Essentials)
- Profiling
- BYOD (+CA, MDP)
- pxGrid, pxGrid Cloud and pxGrid Direct (Context in or Out)**
- User Defined Network (Cloud)
- TrustSec (Group-Based Policy)
- Endpoint Analytics Visibility and Enforcement
- Rapid Threat Containment (Adaptive Network Control)

Essentials (User Visibility and Enforcement)
- AAA and 802.1X
- Guest (Hotspot, Self-Reg, Sponsored)
- Easy Connect (PassiveID)

Certificates

- ISE's EAP Cert is only for ISE to identify/authenticate itself endpoint

- ISE can accept certificate-based authentication issued from various Root CAs

BYOD

Employee

IP Phone
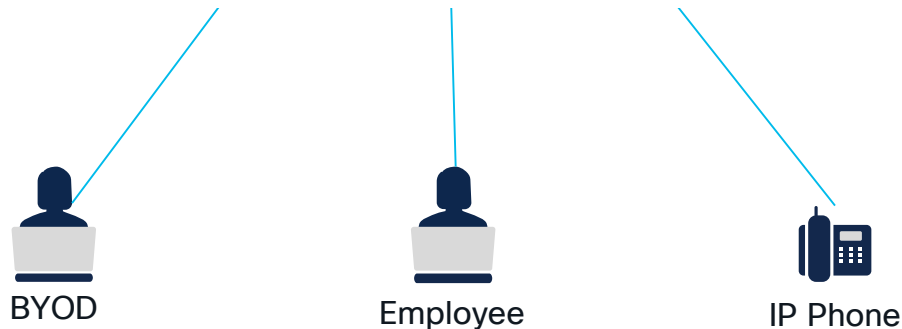
Certificates

- ISE's EAP Cert is only for ISE to identify/authenticate itself endpoint

- ISE can accept certificate-based authentication issued from various Root CAs
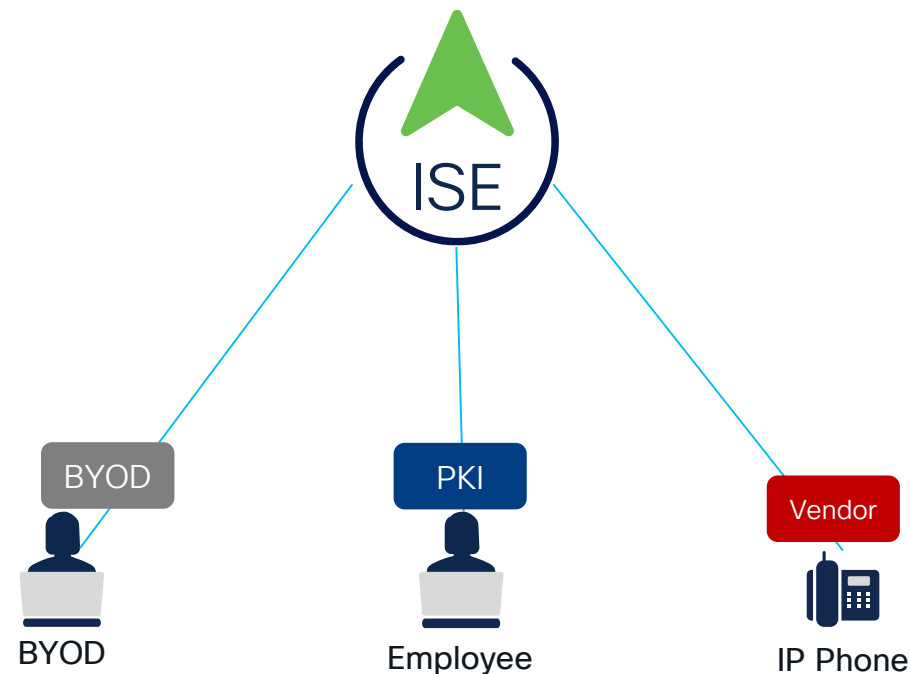
Certificates

- Pre-load trusted root certificates – including potentially:
  - Manufacturer certificates for phones, printers, etc
  - Internal PKI root certificate
  - etc

- "Trust for client authentication and Syslog"

Trusted For: ⓘ

☑ Trust for authentication within ISE

☑ Trust for client authentication and Syslog

☐ Trust for certificate based admin authentication

Reduce Chaos and Unpredictability

- As best as you can: Standardize! Standardize! Standardize!
  - Switch IOS Versions
  - Wireless Controller Versions
  - Switch and Wireless Configuration Templates

- Check the versions and capabilities against the ISE Network Component Capability Releases
  - If possible, validated OS versions

- Enable SMTP for alerts, warnings of certificates expiring, etc

Reduce Chaos and Unpredictability

- Create and deploy Active Directory GPO
  - Seamless native supplicant configuration for user
  - Seamless wired-to-wireless transition
  - Endpoint and Trusted Root Certificates

- Use SCCM or software delivery package if needed for Secure Client

- Utilize the 90 day VM evaluation – Lab It Up

Lab It Up!

A Phased Approach
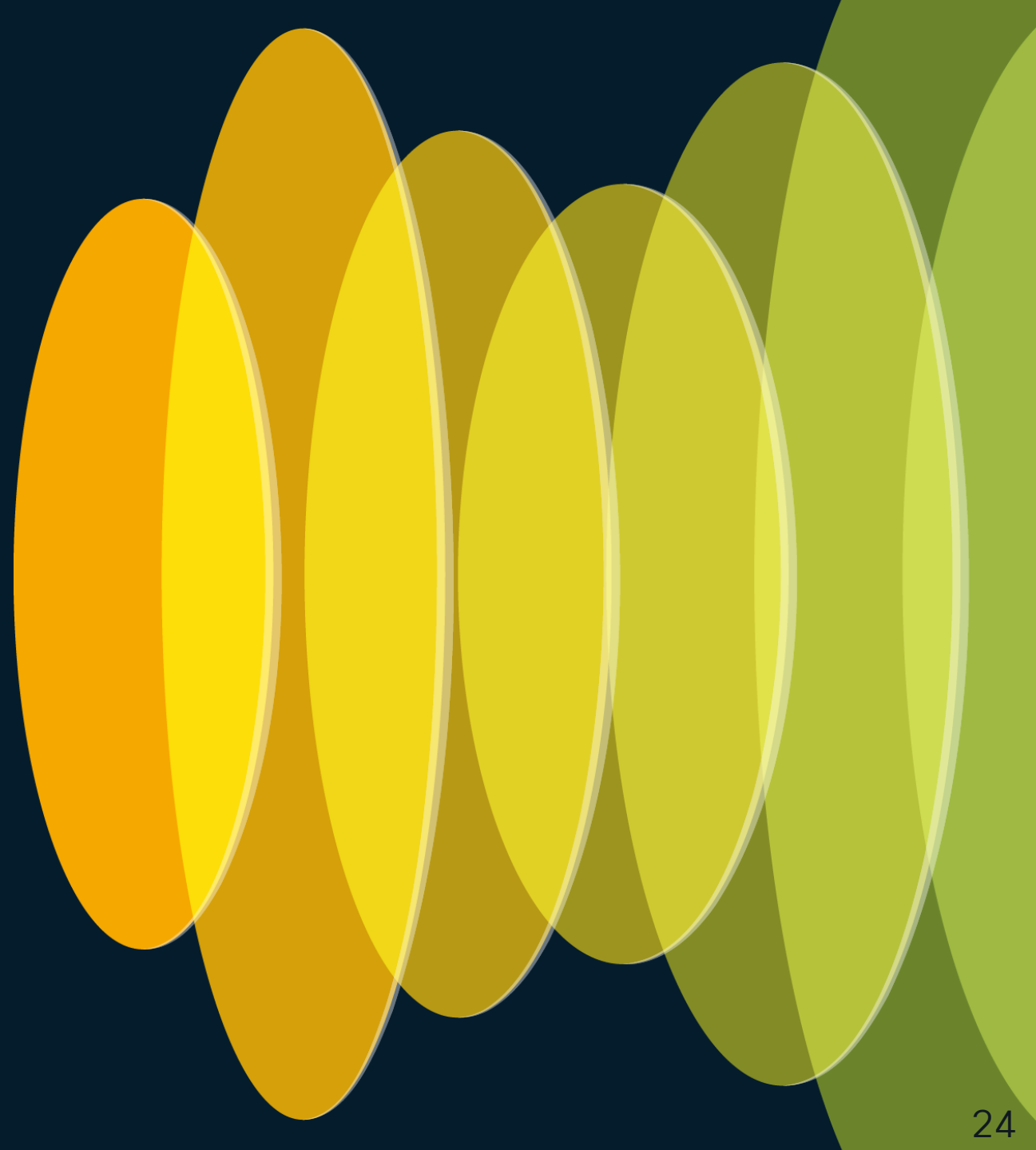
A Phased Approach to ISE…

- VPN:
  - Create a test VPN profile
  - Migrate the profile to production after testing

- Wireless:
  - Create a test SSID
  - Migrate the profile to production after testing

- But what about wired?

Wired Phases

Monitor Mode

File Servers

ISE

Campus Network

✓ Port Open Unconditionally

Pass / Failed Authentication

Low-Impact Mode

DHCP DNS Servers

ISE

File Servers

Campus Network

PREAUTH ACL ✓

`permit eap dhcp dns deny any`

PERMIT ACL

`permit ip any any`

Before Authentication

After Authentication

Closed Mode

ISE

File Servers

Campus Network

Only EAP Allowed ✗ ✓

Before Authentication

After Authentication
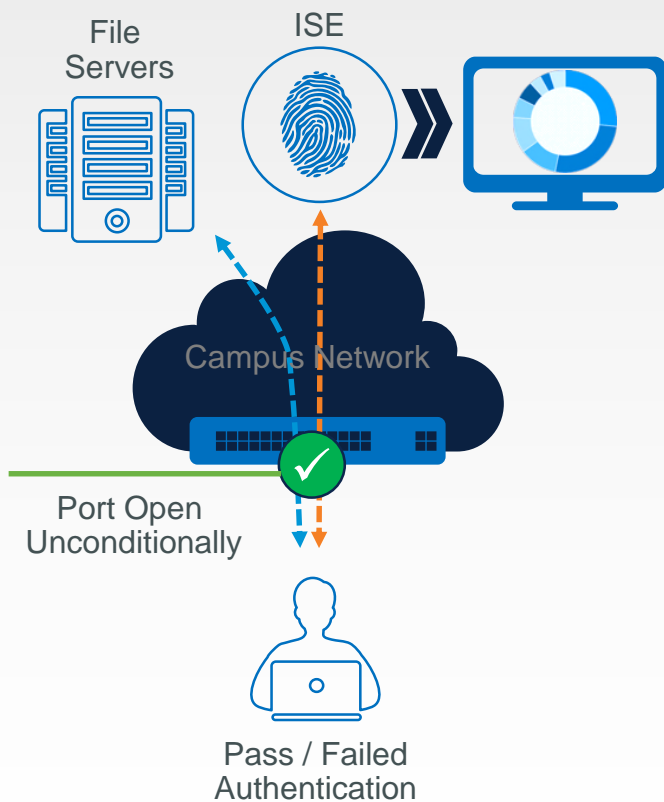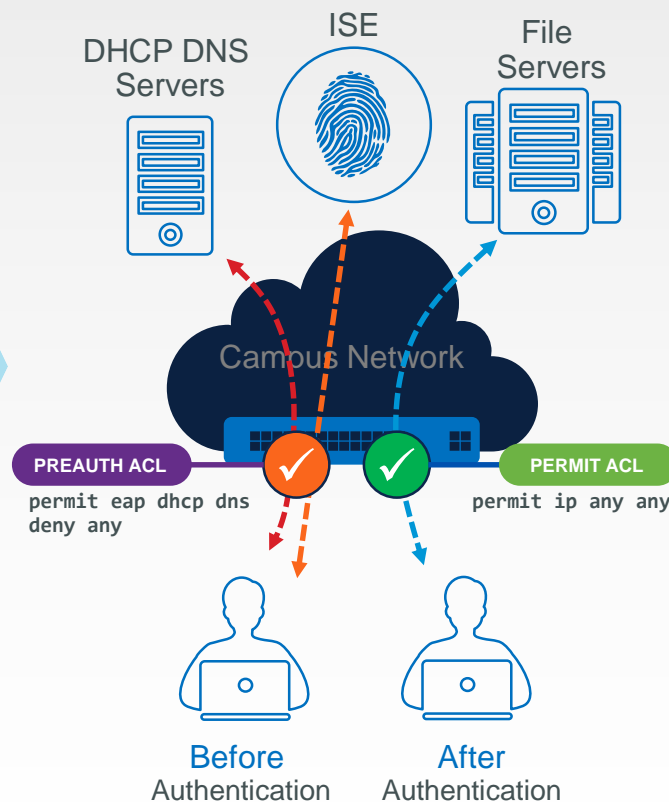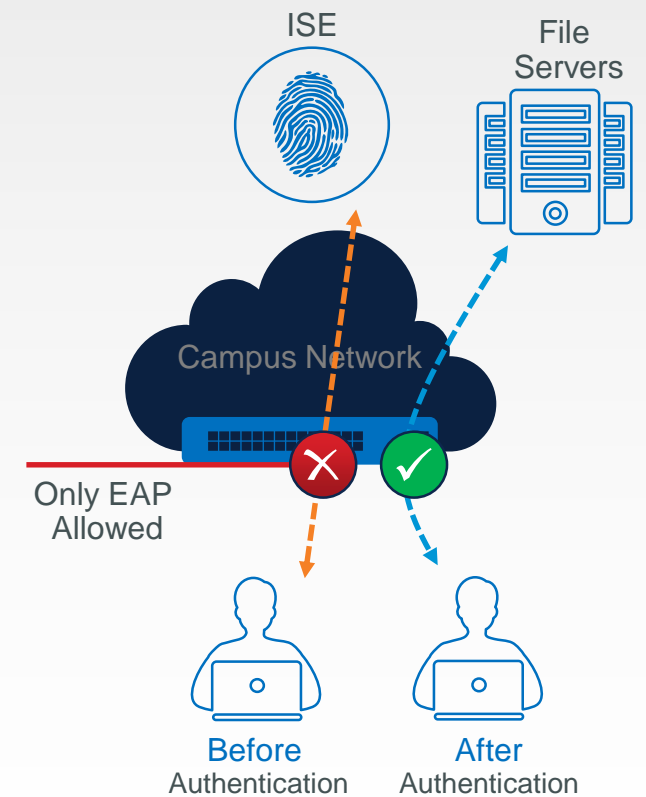
Monitor Mode

- No impact to existing network

- Prepare for enforcement

- Visibility to:
  - Endpoints on network & their supplicant configuration
  - Passed/Failed 802.1x & MAB attempts

- To configure:
  - Enable 802.1X and MAB
  - Enable Open Access
  - Enable Multi-Auth host mode
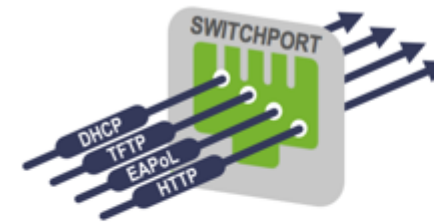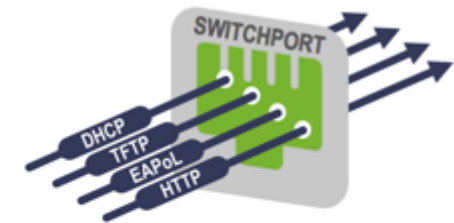
Before Authentication   **After Authentication**

Traffic always allowed irrespective of authentication status

```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
switchport voice vlan 10
authentication host-mode multi-auth
authentication open
authentication port-control auto
mab
dot1x pae authenticator
authentication violation restrict
```

Monitor Mode
Basic 1X/MAB

Low Impact Mode

- Begin to control/differentiate access

- Minimize impact to existing network while retaining visibility of Monitor Mode

- Start from Monitor Mode

- Add ACLs, dACLs, Flex-auth, etc

- Limit number of devices connecting to ports

Before Authentication   **After Authentication**

Pre-Auth and Post-Auth Access controlled by IP ACLs

```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
switchport voice vlan 10
authentication host-mode multi-auth       Low-
ip access-group PRE-AUTH in               Impact
authentication open                       Mode
authentication port-control auto          From
mab                                       Monitor
dot1x pae authenticator                   Mode
authentication violation restrict
```

Closed Mode

- Not everyone goes to Closed Mode

- No access at all before authentication

- Rapid access for non-802.1x-capable corpora assets

- Logical isolation of traffic at the access layer

- Return to default "closed" access

- Implement identity-based access assignment
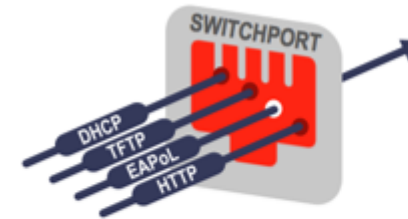
Before Authentication
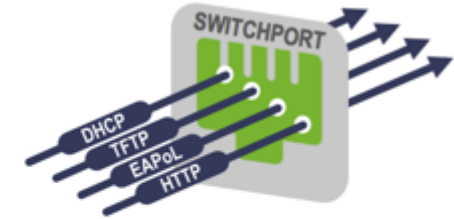
After Authentication

No access prior authentication, Specific access on Auth-success

```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
switchport voice vlan 10
no authentication open
authentication event fail authorize vlan 101
authentication event no-resp authorize vlan 101
authentication event server dead action \
   authorize vlan 101
authentication port-control auto
mab
dot1x pae authenticator
dot1x timer tx-period 10
```

More on Wired Access...

- Start as much as you can on Monitor Mode
  - Gathers contextual information about endpoints
  - Find the "Unknown" endpoints
  - What endpoints would have failed AuthC/AuthZ

- Build and test your policies in Monitor Mode
  - Note: Monitor Mode can still enforce/transition to low-impact mode if Authz is enabled/enforce

- Utilize Network Device Groups to make policy easier
  - Move switch-by-switch into low-impact mode this way

Monitor Mode for Policy Rules

Creating and Applying Network Device Groups

Policy Set Example – Monitor vs Low-Impact

Policy Sets

	Status	Policy Set Name	Description	Conditions	
⊕					
	🔍 Search				
	✅	Wired Monitor Mode		AND	🖥 DEVICE·Device Type **EQUALS** All Device Types#Switches
					⌨ DEVICE·Mode **EQUALS** Mode#Monitor
	✅	Wired Low-Impact Mode		AND	🖥 DEVICE·Device Type **EQUALS** All Device Types#Switches
					⌨ DEVICE·Mode **EQUALS** Mode#Low-Impact

Moving from Monitor to Low-Impact Mode

Wired – High Availability

- More PSNs – Up to 50x
  - Failover to another PSN – Initial delay (deadtime)
  - Failover to another PSN (Load balancer)
  - Local PSN deployed to critical sites

- Switch configuration:
  - IBNS 1.0 Pros:
    - Fail Open/VLAN/Voice Authorization
    - Reauthorize once RADIUS server available
  - IBNS 1.0 Cons:
    - Not very dynamic

Wired – High Availability

- Switch configuration:
  - IBNS 2.0 Pros:
    - Fail open/ACL/ACL with Conditions/SGT/VLAN/Voice Authorization/etc – Any number of options/conditions
    - Extremely dynamic
  - IBNS 2.0 Cons:
    - More complicated to configure
  - IBNS 1.0 is the "out-of-box" configuration style
  - Switch can be converted to IBNS 2.0 with a single command: **authentication display new-style**
    - Warning: Cannot change back to legacy style without formatting switch

IBNS 1.0: Inaccessible Authentication Bypass

Critical VLAN

WAN or PSN Down

WAN or Internet

Client   Access Switch   PSN

- Switch detects PSN unavailable

- Enables port in critical VLAN

- Existing sessions retain authorization status

- Recovery action can re-initialize port when AAA returns

Critical Data VLAN can be anything:
- Same as default access VLAN
- Same as guest/auth-fail VLAN
- New VLAN

```
authentication event server dead action authorize vlan 100
authentication event server alive action reinitialize
authentication event server dead action authorize voice
```

Critical Voice VLAN

IBNS 1.0: Critical Auth for Data and Voice

Voice VLAN Enabled

Data VLAN Enabled

```
interface GigabitEthernet 3/48
 dot1x pae authenticator
 authentication port-control auto
 authentication event server dead action authorize vlan x
 authentication event server dead action authorize voice
```

```
# show authentication sessions interface fa3/48
...
Critical Authorization is in effect for domain(s) DATA and VOICE
```
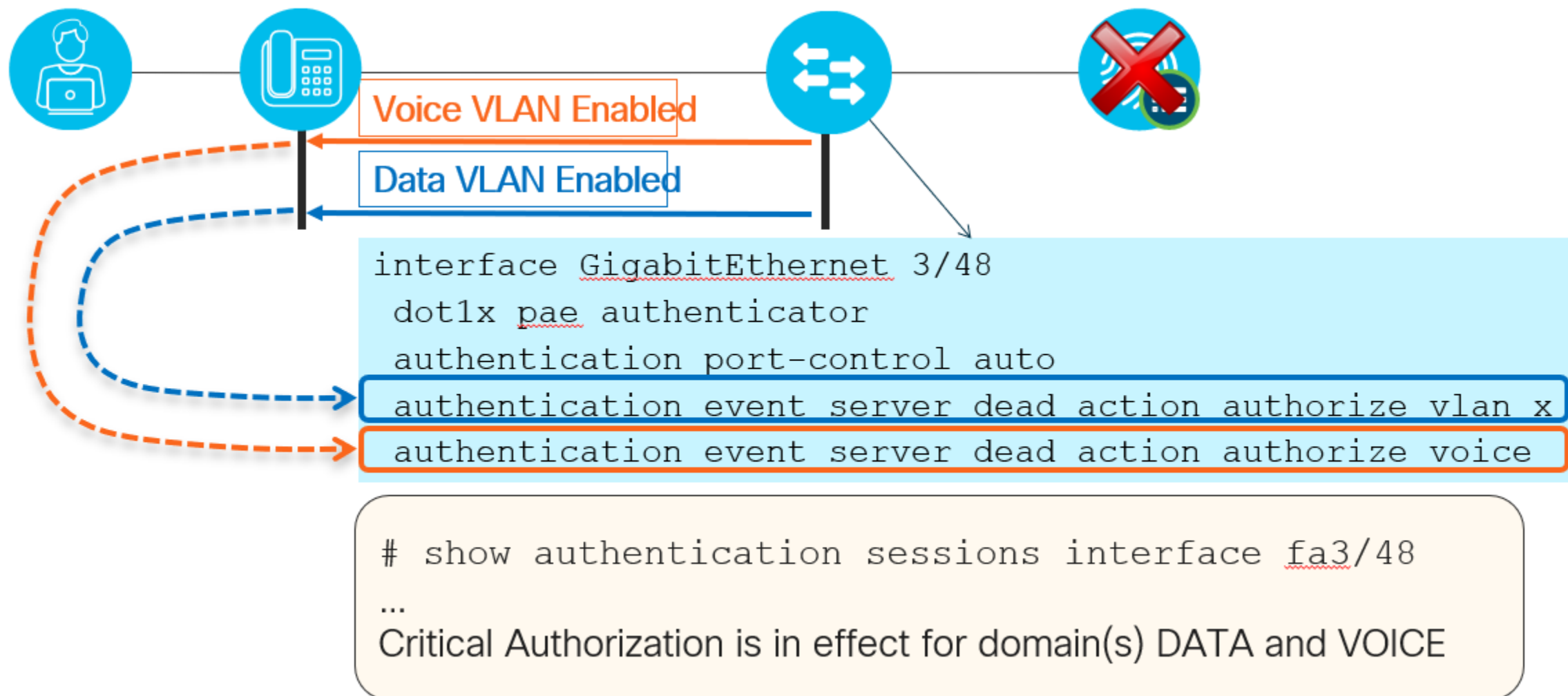
IBNS 1.0: Default Port ACL Issues with Critical VLAN
Limited Access Even After Authorization to New VLAN

- Data VLAN reassigned to critical auth VLAN, but new (or reinitialized) connections are still restricted by existing port ACL

Critical VLAN

Voice VLAN

Gi1/0/2

WAN or PSN Down

Only DHCP/DNS/PING/TFTP allowed !

Default ACL
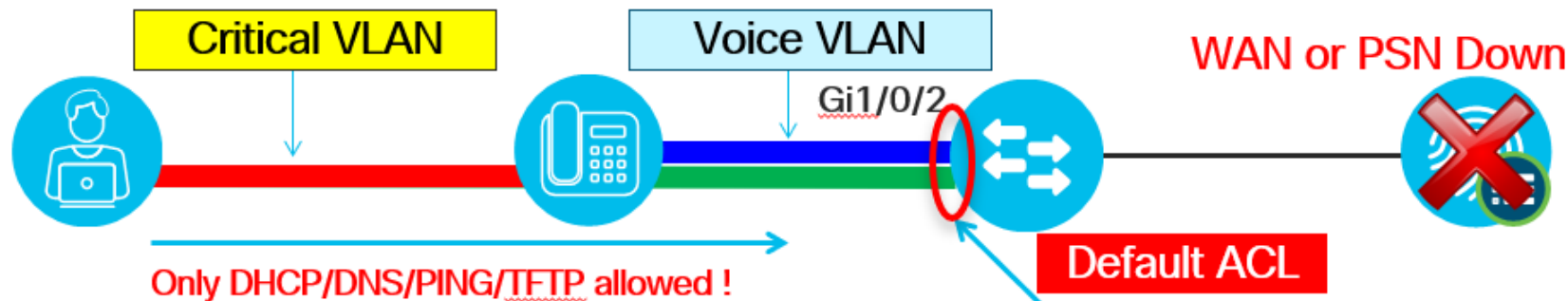
```
interface GigabitEthernet1/0/2
  switchport access vlan 10
  switchport voice vlan 13
  ip access-group ACL-DEFAULT in
  authentication event server dead action reinitialize vlan 11
  authentication event server dead action authorize voice
  authentication event server alive action reinitialize
```

```
ip access-list extended ACL-DEFAULT
  permit udp any eq bootpc any eq bootps
  permit udp any any eq domain
  permit icmp any any
  permit udp any any eq tftp
```
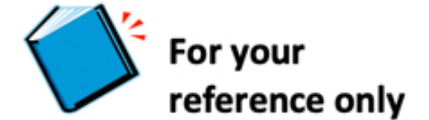
IBNS 2.0: Authorize Port if AAA Down

- Event: Session started
  - Attempt to authenticate using 802.1x until failure

- Event: Authentication failure
  - If AAA is complete down: Stop 802.1x and authorize the port
  - If no response from AAA (but not down yet), authorize to guest VLAN
  - If 802.1x authentication failure, authorize to guest VLAN

```
interface g1/0/1
dot1x pae authenticator
spanning-tree portface
switchport access vlan 100
switchport mode access
mab
access-session port-control auto
service-policy type control subscriber POLICY-A
```

```
policy-map type control subscriber POLICY-A
event session-started match-all
    10 class always do-until-failure
    10 authenticate using dot1x
event authentication-failure match-first
    10 class AAA-DOWN do-all
    10 terminate dot1x
    20 authorize
20 class DOT1X_NO_RESP do-until-failure
    10 activate service-template GUEST_VLAN
30 class 1X-FAIL do-all
    10 activate service-template GUEST_VLAN
```

IBNS 2.0: Assign Critical ACL if AAA down

- Event: Session started
  - Attempt to authenticate using 802.1x until failure

- Event: Authentication failure
  - If AAA is down, do the following:
    - Authorize the port
    - Activate service-template CRITICAL on the port which consists of a local ACL named "ACL-CRITICAL"
    - Terminate 802.1x authentication

```
interface g1/0/1
dot1x pae authenticator
spanning-tree portface
switchport access vlan 100
switchport mode access
mab
access-session port-control auto
service-policy type control subscriber POLICY-A
```

```
policy-map type control subscriber POLICY-B
event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x
event authentication-failure match-all
  10 class AAA-DOWN do-all
    10 authorize
    20 activate service-template CRITICAL
    30 terminate dot1x
```

```
service-template CRITICAL
access-group ACL-CRITICAL
```

```
ip access-list extended ACL-CRITICAL
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
…
```

IBNS 2.0: Assign VLAN if AAA down
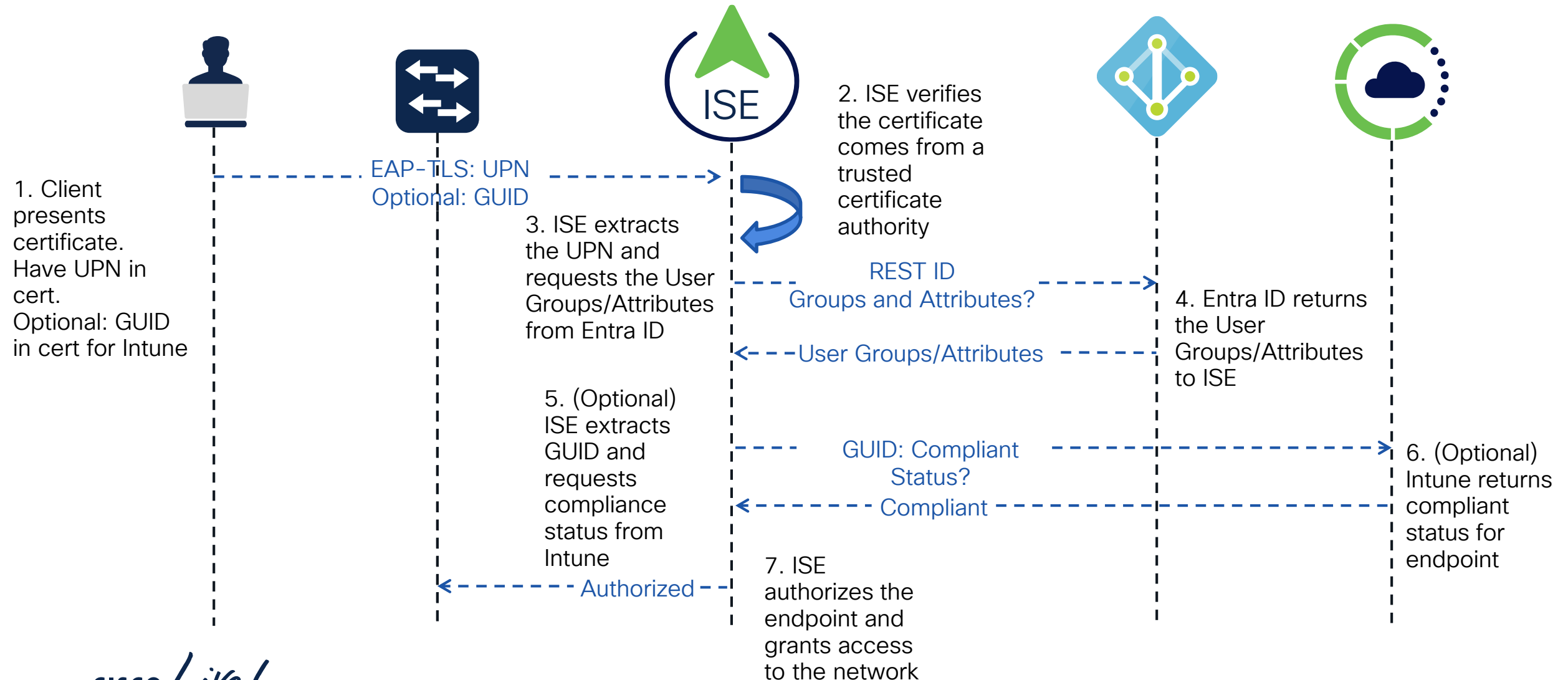
- Event: Session started
  - Attempt to authenticate using 802.1x until failure
- Event: Authentication failure
  - If AAA is down, do the following:
    - Authorize the port
    - Activate service-template CRITICAL on the port which consists of VLAN 110
    - Terminate 802.1x authentication

```
interface g1/0/1
dot1x pae authenticator
spanning-tree portface
switchport access vlan 100
switchport mode access
mab
access-session port-control auto
service-policy type control subscriber POLICY-A
```

```
policy-map type control subscriber POLICY-B
event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x
event authentication-failure match-all
  10 class AAA-DOWN do-all
    10 authorize
    20 activate service-template CRITICAL
    30 terminate dot1x
```

```
service-template CRITICAL
    vlan 110
```

IBNS 2.0: Assign Voice VLAN if AAA down

- Event: Session started
  - Attempt to authenticate using 802.1x until failure
- Event: Authentication failure
  - If AAA is down, do the following:
    - Authorize the port
    - Activate service-template CRITICAL which authorizes the voice VLAN
    - Terminate 802.1x authentication

```
interface g1/0/1
dot1x pae authenticator
spanning-tree portface
switchport access vlan 100
switchport mode access
mab
access-session port-control auto
service-policy type control subscriber POLICY-A
```

```
policy-map type control subscriber POLICY-B
event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x
event authentication-failure match-all
  10 class AAA-DOWN do-all
    10 authorize
    20 activate service-template CRITICAL
    30 terminate dot1x
```

```
service-template CRITICAL
  voice vlan
```

IBNS 2.0: Assign SGT if AAA down

- Event: Session started
  - Attempt to authenticate using 802.1x until failure

- Event: Authentication failure
  - If AAA is down, do the following:
    - Authorize the port
    - Activate service-template CRITICAL which assigns SGT 10 to the endpoint
    - Terminate 802.1x authentication

```
interface g1/0/1
dot1x pae authenticator
spanning-tree portface
switchport access vlan 100
switchport mode access
mab
access-session port-control auto
service-policy type control subscriber POLICY-A
```

```
policy-map type control subscriber POLICY-B
event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x
event authentication-failure match-all
  10 class AAA-DOWN do-all
    10 authorize
    20 activate service-template CRITICAL
    30 terminate dot1x
```

```
service-template CRITICAL
   sgt 10
```

IBNS 2.0: Assign CRITICAL ACL, Voice VLAN and VLAN if AAA down

For your reference only

- Event: Session started
  - Attempt to authenticate using 802.1x until failure

- Event: Authentication failure
  - If AAA is down, do the following:
    - Authorize the port
    - Activate service-template CRITICAL on the port which consists of a local ACL named "ACL-CRITICAL", Voice VLAN, SGT 10, and VLAN 110
    - Terminate 802.1x authentication

```
interface g1/0/1
dot1x pae authenticator
spanning-tree portface
switchport access vlan 100
switchport mode access
mab
access-session port-control auto
service-policy type control subscriber POLICY-A
```

```
policy-map type control subscriber POLICY-B
event session-started match-all
  10 class always do-until-failure
    10 authenticate using dot1x
event authentication-failure match-all
  10 class AAA-DOWN do-all
    10 authorize
    20 activate service-template CRITICAL
    30 terminate dot1x
```

```
service-template CRITICAL
    access-group ACL-CRITICAL
    vlan 110
    voice vlan
    sgt 10
```

```
ip access-list extended ACL-CRITICAL
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
…
```

Authentication

- Multiple authentication methods
  - 802.1x
    - Multiple 802.1X EAP methods simulanteously –
      - TEAP-EAP-TLS for Corporate Endpoints
      - EAP-TLS for supported printers and phones
      - PEAP-MSCHAPv2 for BYOD
  - Easy Connect
    - User authentication without 802.1x
  - Web Auth
  - MAB

Allowed Protocols

- ISE gives many options...

- Most common allowed protocols:

  - Process Host Lookup

  - EAP-TLS

  - PEAP-MSCHAPv2

  - PEAP-EAP-TLS

  - EAP-TEAP

Azure AD/Entra ID Support

EAP-TTLS and EAP-TLS currently supported

1. Client presents certificate. Have UPN in cert. Optional: GUID in cert for Intune

EAP-TLS: UPN
Optional: GUID

2. ISE verifies the certificate comes from a trusted certificate authority

3. ISE extracts the UPN and requests the User Groups/Attributes from Entra ID

REST ID Groups and Attributes?

4. Entra ID returns the User Groups/Attributes to ISE

User Groups/Attributes

5. (Optional) ISE extracts GUID and requests compliance status from Intune

GUID: Compliant Status?

Compliant

6. (Optional) Intune returns compliant status for endpoint

Authorized

7. ISE authorizes the endpoint and grants access to the network

Easy Connect

1. Endpoint initially connects to the network

Endpoint Connects

3. Endpoint is granted access to basic services to allow AD login

MAB Authentication

2. Endpoint authenticates via MAB

Authorized: AD Login Only

User logs into computer - credentials sent to Active Directory

4. User logs into computer with their AD credentials which is authenticated against Active Directory

5. Credentials successfully authenticate and the login is successful

Login Successful

Login Event for User

6. ISE receives Login event log from Active Directory with username and MAC address of endpoint. ISE binds this to the existing MAB session to determine authorization

Change of Authorization

7. ISE issues a CoA to the NAD

Full Access

8. ISE grants endpoint full access

Example of Easy Connect AD Only ACL

```
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit icmp any any
permit tcp any host <AD-DC> eq 88
permit udp any host <AD-DC> eq 88
permit udp any host <AD-DC> eq ntp
permit tcp any host <AD-DC> eq 135
permit udp any host <AD-DC> eq netbios-ns
permit tcp any host <AD-DC> eq 139
permit tcp any host <AD-DC> eq 389
permit udp any host <AD-DC> eq 389
permit tcp any host <AD-DC> eq 445
permit tcp any host <AD-DC> eq 636
permit udp any host <AD-DC> eq 636
permit tcp any host <AD-DC> eq 1025
permit tcp any host <AD-DC> eq 1026
```

Migrating to 802.1x? Make it easier with Easy Connect

Phased Posturing – Client Provisioning

- Determines which posture agent type

- Can be filtered to a test on a subset of endpoints based on:
  - Endpoint Identity Groups
  - Access Method
  - User Identity
  - etc

- Create a client provisioning policy for a test group first

- After testing, move the policy to production

Client Provisioning – Creating a Test Policy

Phased Posturing – Posture Policy

- Determines which requirements will be checked

- Conditions can be applied similar to the Client Provisioning policy

- Requirements may be added over time

- Requirements have three modes:

  - Mandatory

  - Optional

  - Audit

     54

Posture Policy – Creating a Test Policy

Tuning Policy Sets

Policy Logic

- All policies in ISE follow the same following policy logic:

    if {*condition*} then {*result*}

- Think about it in non-technical terms:
    - If {the user is in the marketing department} then {let him/her on the network}
    - If {the user is using their laptop from home} then {only give them internet access}

- Think about what you're trying to achieve in non-technical terms first, then create the policy in ISE using technical conditions/results that accomplish it

- Similar to an ACL: First matched rule

Policy Conditions

- AND – Both Conditions MUST match
  - "SSID is Corp-WiFi AND endpoint needs to be authenticating with wireless

Policy Conditions

- OR – At least one of the conditions must match
  - "Endpoint must be authenticating on the wired network with 802.1x OR MAB"
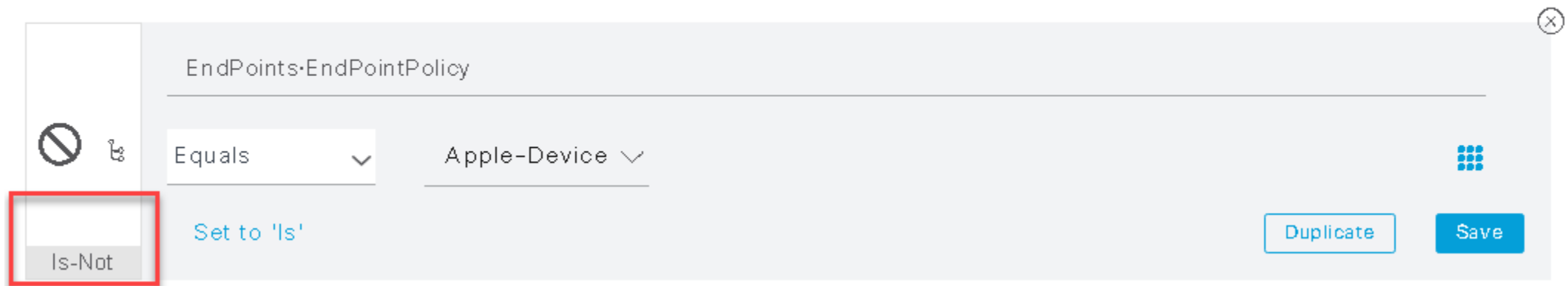
Policy Conditions

- NOT – This condition must NOT be met
  - "Endpoint should NOT be an Apple device"

Policy Conditions

- Combine them to create conditions required to meet your business use-case:

  - "The endpoint's user and machine must have both successfully authenticated AND the user must be part of the Corporate OR Enterprise AD groups and they should NOT be trying to connect to a network device in San Francisco"

Editor

Network Access·EapChainingResult

Equals   User and machine both succeeded ∨

ad-2016·ExternalGroups

Equals   dcloud.cisco.com/Builtin/Corporate ×

ad-2016·ExternalGroups

OR ∨   Equals   dcloud.cisco.com/Builtin/Enterprise ×

AND ∨

+   NEW

DEVICE·Location

Is-Not   Equals   All Locations#San Francisco ∨

A little history lesson…

Introduced in ISE 1.3: Policy Sets

- Groups of authentication and authorization policies to manage network access control

- Create segmented authorization and authorization rules for specific use cases, locations, NAD times, authentication methods, and so much more...

- No more single running list of authentication/authorization rules to manage and troubleshoot

- Reduces the fault surface if there is a misconfiguration

Policy Set Flow

Policy Sets   Reset   Re

	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Se
				Q Search		
	✓	VPN-Policy-Set		AND	🖥 DEVICE·Device Type **EQUALS** All Device Types#VPN-Concentrators 📄 VPN-list	• Default Network Access
	✓	TC-NAC		AND	🌐 DEVICE·Location **EQUALS** Location#All Locations#Global#North America#USA#California#SJC01	• Default Network Access
	✓	Dot1x-AzureAD		AN	ca#USA#California#SJC01	• Default Network Access
	✓	MDM		⅄	🌐 DEVICE·Location **EQUALS** All Locations#My-Territory#APAC-Region#India#Karnataka#Bengaluru 📄 MDM-endpoints	• Default Network Access
	✓	BYOD		AND	🌐 DEVICE·Location **EQUALS** North America#USA#California#SJC01 📄 Win-BYOD	• Default Network Access
	✓	Guest-Access		OR	🖥 DEVICE·Device Type **EQUALS** All Device Types#Wireless ⅄ Radius·Service-Type **EQUALS** Call Check 📄 Windows-guest	• Default Network Access

> Result: First policy set matched checks allows protocols and processes packet

Policy Set Flow

Policy Sets→ Dot1x-AzureAD   Reset   Reset Policyset Hitcounts

Status	Policy Set Name	Description	Conditions			Allowed Protocols / Serve
🔍 Search
✅	Dot1x-AzureAD		AND	🌐 DEVICE·Location **EQUALS** North America#USA#California#SJC01		• Default Network Access
				📄 windows-dot1x-azure		

∨ Authentication Policy (3)

⊕	Status	Rule Name	Conditions	Use
	🔍 Search
	✅	Dot1x_TLS	🔲 Network Access·EapAuthentication **EQUALS** EAP-TLS	
				• AzureAD
	✅	Dot1x-TTLS	🔲 Network Access·EapTunnel **EQUALS** EAP-TTLS	> Options

> Result: Credentials authenticated against Azure AD

Policy Set Flow

∨ Authorization Policy (3)

	Status	Rule Name	Conditions	Results Profiles
⊕				
	🔍 Search			
	✓	HR_Policy	👤 AzureAD·ExternalGroups **EQUALS** HRGroup	• Full-Access
	✓	Employee_Policy	👤 AzureAD·ExternalGroups **EQUALS** EmployeeGroup	• Full-Access
	✓	Default		• DenyAccess

Result: Endpoint is granted full access

Grouping Policy Sets

There is more than one way to make an omelette!

- Many ways to overcomplicate, but many ways to simplify

- Embrace the KISS principle!

- Commonly two trains of thought:

  1. Policy Sets based on device type, location, and/or SSID:
     - Network Device Group: Switches, Wireless Controller, VPN
     - (Optional) Network Device Group Location: HQ
     - (Optional) SSID: Corp-Guest

  2. Policy Sets based Use-Case:
     - Use-Case: Wired 802.1x, Wireless 802.1x, Wired MAB, Wireless MAB, etc
     - (Optional) Network Device Group Location: HQ
     - (Optional) SSID: Corp-Guest

Policy Sets
Option 1 Example

Policy Sets

Reset Policyset Hit

	Status	Policy Set Name	Description	Conditions			Allowed Protocols / Server Sequence
		Search					
	✓	San Francisco Wired Access		AND	🖥 DEVICE·Device Type **EQUALS** All Device Types#Switches 🌐 DEVICE·Location **EQUALS** All Locations#San Francisco		Default Network Access
	✓	San Jose Wired Access		AND	🖥 DEVICE·Device Type **EQUALS** All Device Types#Switches 🌐 DEVICE·Location **EQUALS** All Locations#San Jose		Default Network Access
	✓	Guest SSID		AND	🖥 DEVICE·Device Type **EQUALS** All Device Types#Wireless Controllers 🖥 Radius·Called-Station-ID **CONTAINS** Corp-Guest		Default Network Access
	✓	Corp 802.1x		AND	🖥 DEVICE·Device Type **EQUALS** All Device Types#Wireless Controllers 🖥 Radius·Called-Station-ID **CONTAINS** Corp-Dot1x		Default Network Access
	✓	VPN			🖥 DEVICE·Device Type **EQUALS** All Device Types#VPN		Default Network Access

Policy Sets
Option 2 Example

Policy Sets

⊕	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequence
	🔍 Search					
	✓	San Francisco Wired 802.1		AND	🌐 DEVICE·Location **EQUALS** All Locations#San Francisco 📄 Wired_802.1X	Default Network Access ✎ +
	✓	San Francisco Wired MAB		AND	🌐 DEVICE·Location **EQUALS** All Locations#San Francisco 📄 Wired_MAB	Default Network Access ✎ +
	✓	San Jose Wired 802.1X		AND	🌐 DEVICE·Location **EQUALS** All Locations#San Jose 📄 Wired_802.1X	Default Network Access ✎ +
	✓	San Jose Wired MAB		AND	🌐 DEVICE·Location **EQUALS** All Locations#San Jose 📄 Wired_MAB	Default Network Access ✎ +
	✓	Guest SSID		AND	🖥 DEVICE·Device Type **EQUALS** All Device Types#Wireless Controllers 🖥 Radius·Called-Station-ID **CONTAINS** Corp-Guest	Default Network Access ✎ +
	✓	Corp 802.1x		AND	🖥 DEVICE·Device Type **EQUALS** All Device Types#Wireless Controllers 🖥 Radius·Called-Station-ID **CONTAINS** Corp-Dot1x	Default Network Access ✎ +
	✓	VPN		🖥 DEVICE·Device Type **EQUALS** All Device Types#VPN		Default Network Access ✎ +

The Power of Profiling

CISCO *Live!*

Endpoint Profiling – Visibility Data Sources

The profiling service in Cisco ISE identifies the devices that connect to your devices

Endpoints send interesting data, that reveal their device type

DS

DS

ACIDex

ISE

ISE Data Collection Methods for Device Profiling

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

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

Cisco Secure Client (formerly AnyConnect): ACIDex

Feed Service
(Online/Offline)

CISCO

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

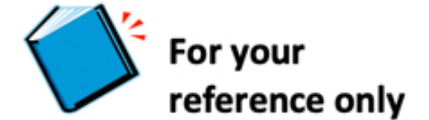Cisco Secure Client Identity Extensions (ACIDex) | Device Sensor (DS)

ISE Profiling Probes

- RADIUS
  - Collects session attributes as well as CDP, LLDP, DCHP, HTTP, and MDM from IOS Device Sensor
- SNMP Query and Traps
  - Collects information such as interface, CDP, LLDP, ARP, Linkup, Lidown, and MAC notifications
- DHCP
  - Listens for DHCP Packets
- DNS
  - Performs a DNS lookup for the FQDN
- HTTP
  - Receives and parses HTTP packets to discover the User-Agent

ISE Profiling Probes

- Netflow

  - Collects Netflow packets – Don't use this one!

- **Active Directory**

  - **Queries AD for Windows information**

- **NMAP**

  - **Scans endpoints for open ports, service information, and OS**

- **pxGrid**

  - **Fetches attributes of MAC or IP address of a subscriber**

- AnyConnect ACIDEX

 - Provides ACIDEX information to ISE over RADIUS – device public MAC and device platform

RADIUS Probe Sample Configuration

aaa authentication dot1x default group ise-group

aaa authorization network default group ise-group

aaa accounting dot1x default start-stop group ise-group

aaa accounting update newinfo periodic 2880

!

radius server ise

address ipv4 <ISE-PSN-IP> auth-port 1812 acct-port 1813

key <Shared-Secret>

aaa group server radius ise-group

server name ise

!

ip radius source-interface <Interface>

!

radius-server attribute 6 on-for-login-auth

radius-server attribute 8 include-in-access-req

radius-server attribute 25 access-request include

radius-server vsa send accounting

radius-server vsa send authentication

SNMP Probe Sample Configuration
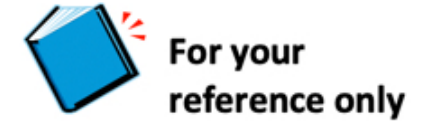
interface <interface>

snmp trap mac-notification change added

snmp trap mac-notification change removed

!

mac address-table notification change

mac address-table notification mac-move

!

snmp-server trap-source <interface>

snmp-server enable traps snmp linkdown linkup

snmp-server enable traps mac-notification change move

snmp-server host <ISE-PSN-IP> version 2c <string>

snmp-server community <string> RO

cdp run

!

interface <interface>

cdp enable

lldp run

!

interface <interface>

lldp receive

lldp transmit

HTTP Probe Sample Configuration

ip http server

ip http secure-server

ip access-list extended REDIRECT-ACL

deny ip any host <ISE-PSN-IP>
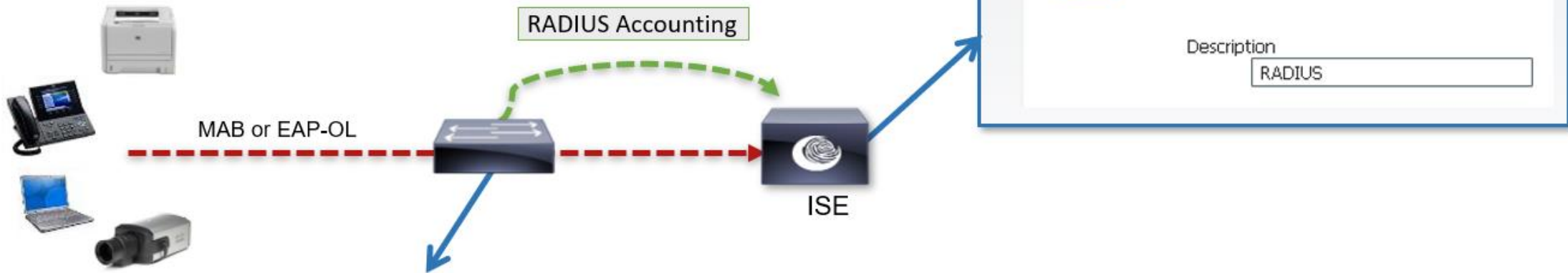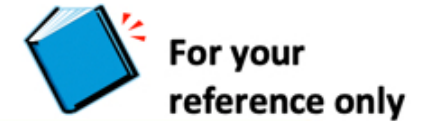
permit tcp any any eq http

permit tcp any any eq https

DHCP Probe Sample Configuration
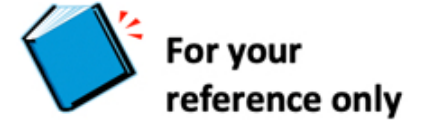
interface vlan 30

ip helper-address <PSN-IP-Address>

Device Sensor for Wired

RADIUS Accounting

MAB or EAP-OL

ISE

RADIUS

Description

RADIUS

1) Filter DHCP, CDP, and LLDP options/TLVs

```
device-sensor filter-list cdp list my_cdp_list
  tlv name device-name
  tlv name platform-type
device-sensor filter-spec cdp include list my_cdp_list
```

2) Enable sensor data to be sent in RADIUS Accounting including all changes

```
device-sensor accounting
device-sensor notify all-changes
```

```
device-sensor filter-list lldp list my_lldp_list
  tlv name system-name
  tlv name system-description
device-sensor filter-spec lldp include list my_lldp_list
```

3) Disable local analyzer if sending sensor updates to ISE (central analyzer)

```
no macro auto monitor
access-session template monitor
```

```
device-sensor filter-list dhcp list my_dhcp_list
  option name host-name
  option name class-identifier
  option name client-identifier
device-sensor filter-spec dhcp include list my_dhcp_list
```

Device Sensor for WLCs

- Per WLAN Enable/Disable device profiling

- DHCP (WLC 7.2.110.0)
  - **Hostname, Class ID**

- HTTP/Both (WLC 7.3)
  - **User Agent**

- FlexConnect with Central Switching supported

Device Sensor for Catalyst 9800s

Configuration> Tags & Profiles > Policy

Enabling Probes on ISE
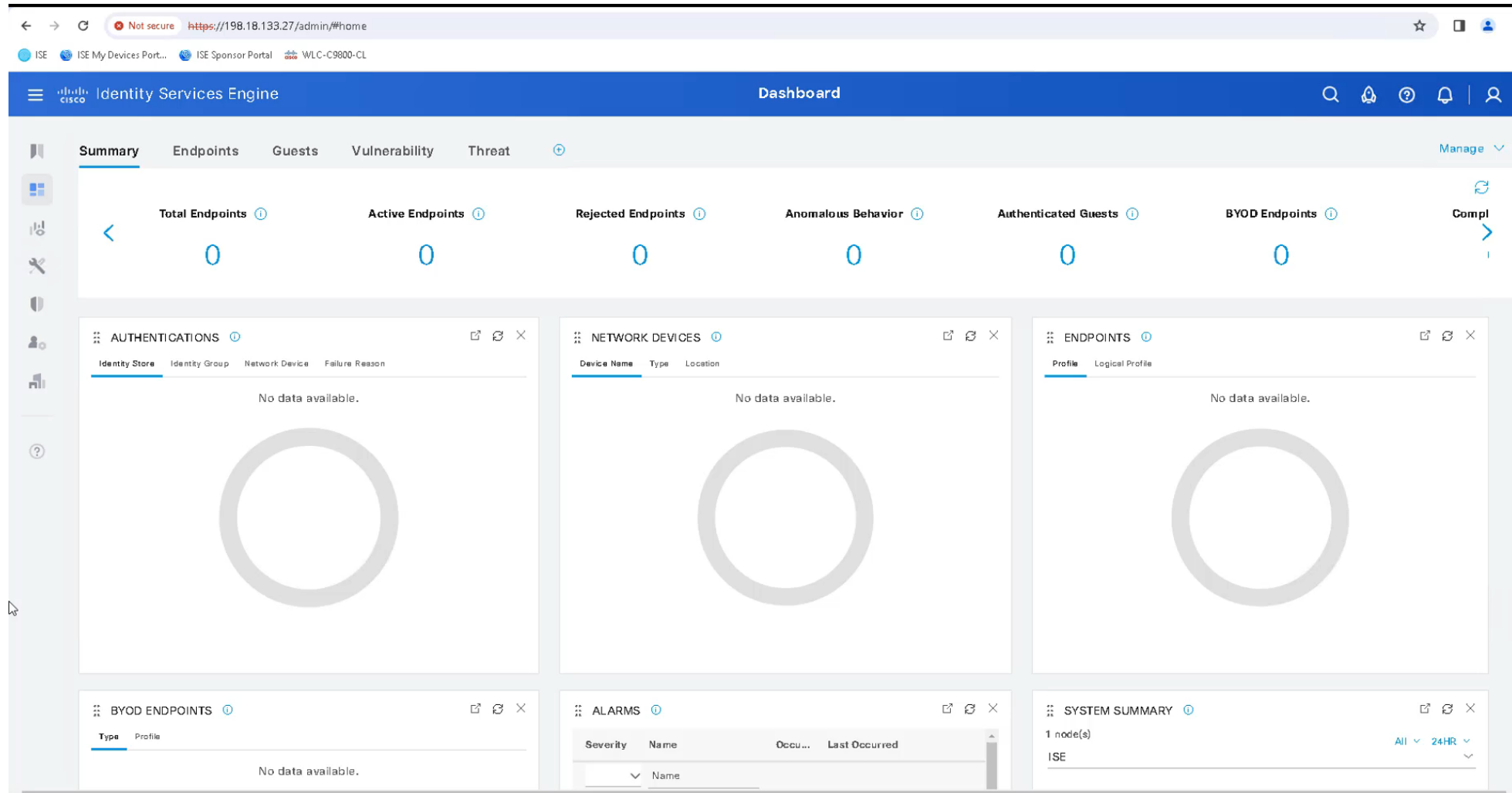
Profiling Logic

Profiler Policy

* Name	Apple-Device	Description	Generic policy for all Apple devices
Policy Enabled	☑		
* Minimum Certainty Factor	10	(Valid Range 1 to 65535)	
* Exception Action	NONE ⌄		
* Network Scan (NMAP) Action	OS-scan ⌄		
Create an Identity Group for the policy	○ Yes, create matching Identity Group		
	● No, use existing Identity Group hierarchy		
Parent Policy	***NONE***		
* Associated CoA Type	Global Settings ⌄		
System Type	Cisco Provided		

Rules

If	Condition	Apple-iPadRule4Check1 ⌄	Then	Certainty Factor Increases ⌄	10	⚙ ⌄
If	Condition	Apple-DeviceRule3check1 ⌄	Then	Certainty Factor Increases ⌄	180	⚙ ⌄
If	Condition	Apple-iPhoneRule3Check1 ⌄	Then	Certainty Factor Increases ⌄	10	⚙ ⌄
If	Condition	Apple-DeviceRule4check1 ⌄	Then	Certainty Factor Increases ⌄	180	⚙ ⌄
If	Condition	Apple-DeviceRule1Check1 ⌄	Then	Certainty Factor Increases ⌄	10	⚙ ⌄
If	Condition	Apple-iPadRule1Check1 ⌄	Then	Certainty Factor Increases ⌄	100	⚙ ⌄
If	Condition	Apple-iPhoneRule1Check1 ⌄	Then	Certainty Factor Increases ⌄	100	⚙ ⌄
If	Condition	Apple-DeviceRule1-SCAN ⌄	Then	Take Network Scan Action ⌄		⚙ ⌄

Profile Hierarchy

✓ Profile: Cisco-Device
Minimum Certainty Factor: 10
NMAP Action: OS-scan
15 Rules
Must match 1-2 rules

✓ Profile: Cisco-Access-Point
Minimum Certainty Factor: 10
6 Rules
Must match at least 1 rule

✓ Profile: Cisco-AP-Aironet-1040
Minimum Certainty Factor: 30
4 Rules
Must match at least 1 rule
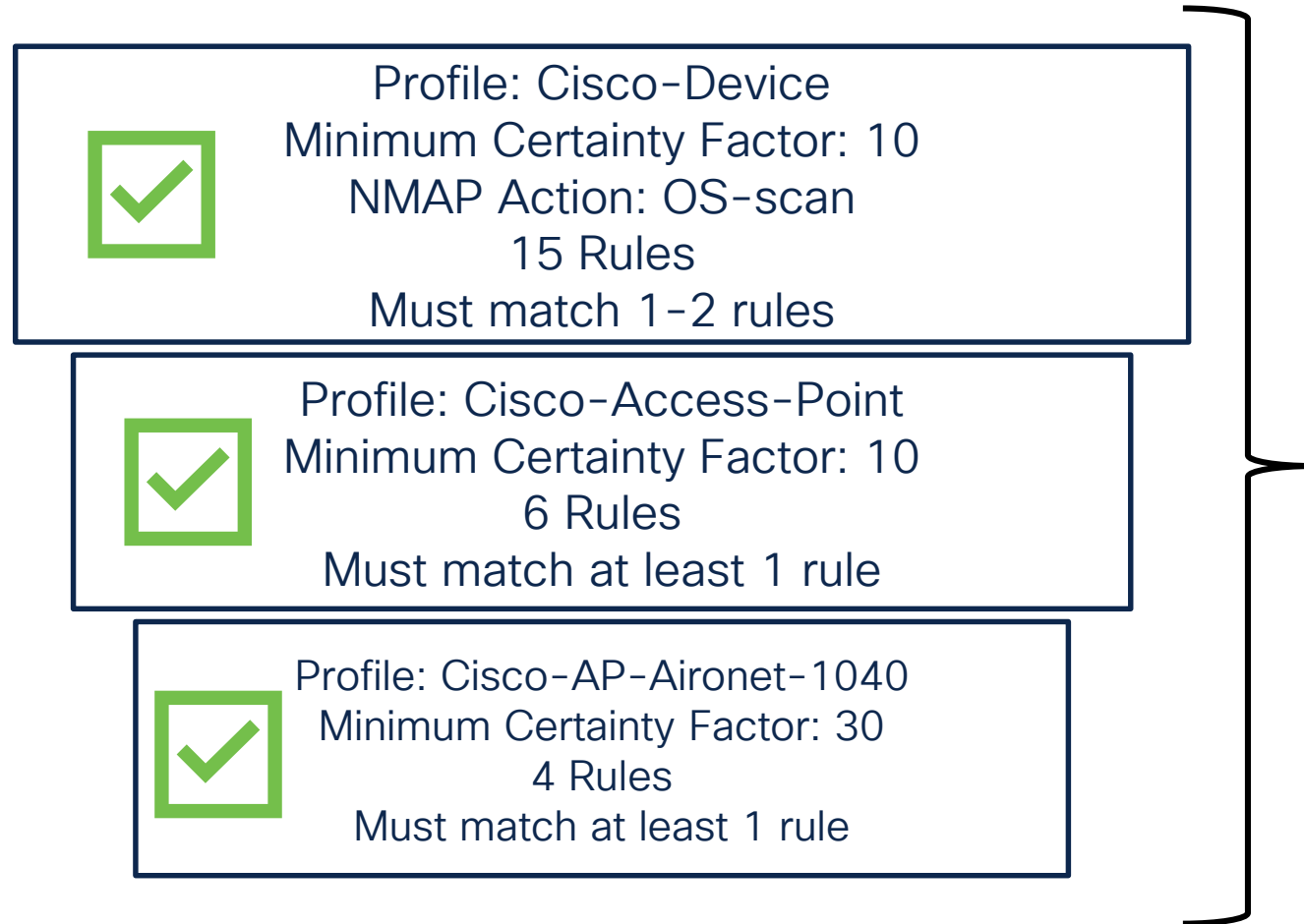
In order to profiled as a Cisco-AP-Aironet-1040, the endpoint must match 3-4 unique rules in total based on default policies built into ISE

Profile Packages and Integrations

Medical Devices

Hospital

250+ Medical device profiles

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

IOT Building & Automation

Library

XML

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

ISE

pxGrid

pxGrid

Factory

Industrial Devices

Cisco CyberVision

Cisco AI Endpoint Analytics

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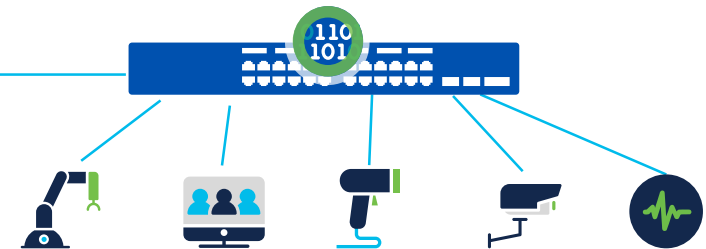
Creating Custom Profiles

- Sometimes we need to create custom endpoint profiles

- GUI does not make it easier to view collective attributes across many endpoints

- Sadly, ISE Endpoint Analytics Tool is no longer supported after ISE 2.6

- How do we make it easier to create custom profiles?

  - Answer: Endpoint export to CSV from the CLI!

- Best practices:

  - Utilize hierarchical profiles if needed

  - Minimum certainty factor should be higher than pre-built profiles (aim for 500+)

Creating Custom Profiles – Get All Endpoints

Creating Custom Hierachical Profiles

Profiling Attributes

For your reference only
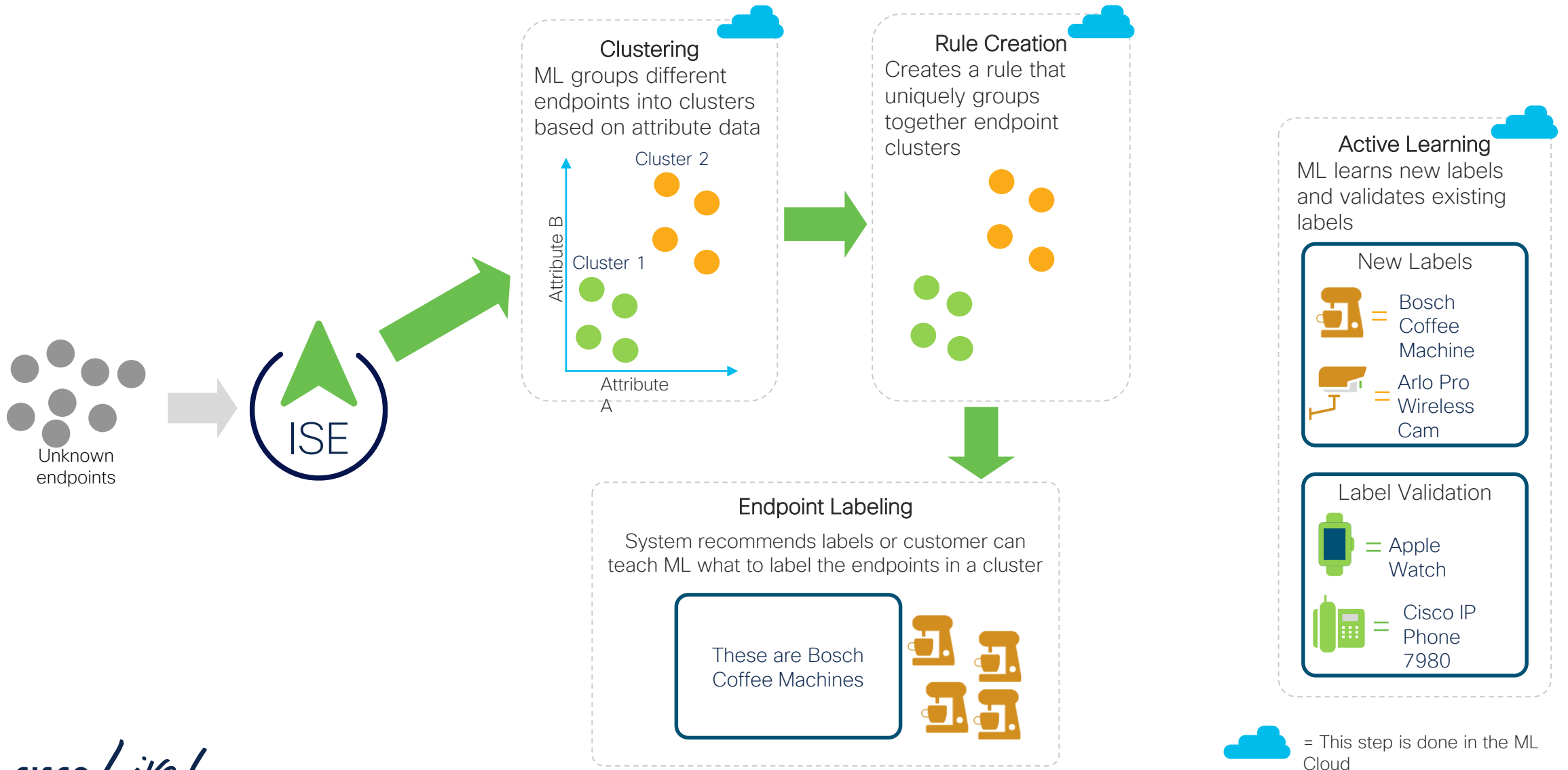
- OUI
- FQDN
- DHCP client-identifier
- DHCP class-identifier
- DHCP parameter-request-list
- DHCP host-name
- AD host-exists

- AD operating-system
- HTTP User-Agent
- CDP Cache Platform
- CDP System Name
- LLDP System Name
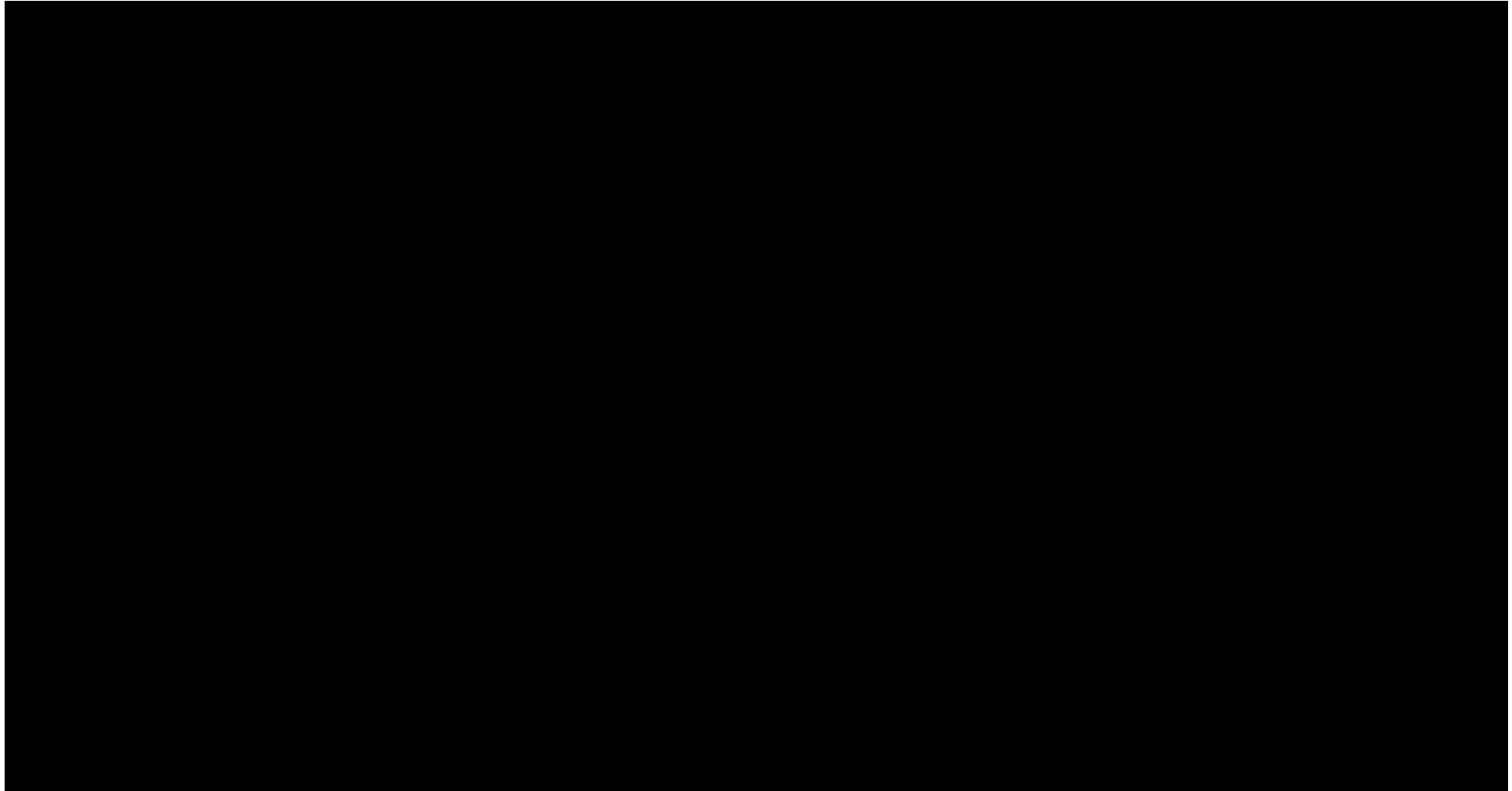- LLDP System Description
- SNMP information

Cisco AI Analytics

Web Interface

Cisco Catalyst Center

Cisco ISE

Context

Classifications

ISE

Endpoint Analytics shows device classification results associated with endpoints

Policy

SPAN

Distribution

NBAR
(SD-AVC Agent)

Telemetry Traffic
Appliance (TTA)

Wireless LAN
Controller

Catalyst 9000

Legacy Cisco Switches / 3rd party devices

Cisco AI Endpoint Analytics

Clustering
ML groups different endpoints into clusters based on attribute data

Cluster 2
Cluster 1
Attribute B
Attribute A

Rule Creation
Creates a rule that uniquely groups together endpoint clusters

Unknown endpoints

ISE

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

These are Bosch Coffee Machines

Active Learning
ML learns new labels and validates existing labels

New Labels
= Bosch Coffee Machine
= Arlo Pro Wireless Cam

Label Validation
= Apple Watch
= Cisco IP Phone 7980

= This step is done in the ML Cloud

AI Endpoint Analytics on ISE

Integrations

Platform Exchange Grid (pxGrid)

- Open and scalable Security Product Integration Framework (SPIF) that allows for bi-directional any-to-any partner platgorm integration

- Introduced in ISE 1.3

- Integrations with 100+ Cisco and non-Cisco products

- Reduces silos by integrating your security architecture together to share context, respond to threats, and ingest information

- Tons of guides on integrations at cs.co/ise-guides
  - But also check out developer.cisco.com/site/pxgrid

On-Prem pxGrid Integration

1. Both ISE and the pxGrid Client need to have an identity (pxGrid) certificate issued from a Root CA the other trusts. Note: Certificate EKU must have Client and Server Authentication

Client's pxGrid Certificate

2. The pxGrid client is configured with the IP addresses of ISE's pxGrid nodes

3. The pxGrid initiates the connection to ISE and authenticates itself with it's identity (pxGrid) certificate

ISE

ISE's pxGrid Certificate

4. ISE will authenticate itself back to the client with its own pxGrid certificate

5. ISE should now list the pxGrid client in the pxGrid dashboard and share session context with the client by default. In the pxGrid dashboard, this client can also be assigned additional permissions by being added pxGrid groups such as ANC

Note: Password-based pxGrid authentication is available but rarely used

pxGrid Cloud Integration

ISE

dna.cisco.com

Launch

OFFER
OFFER
OFFER

Subscribe ✓

Register

Partner App

App App App App App App

Connect   App Store   Activate
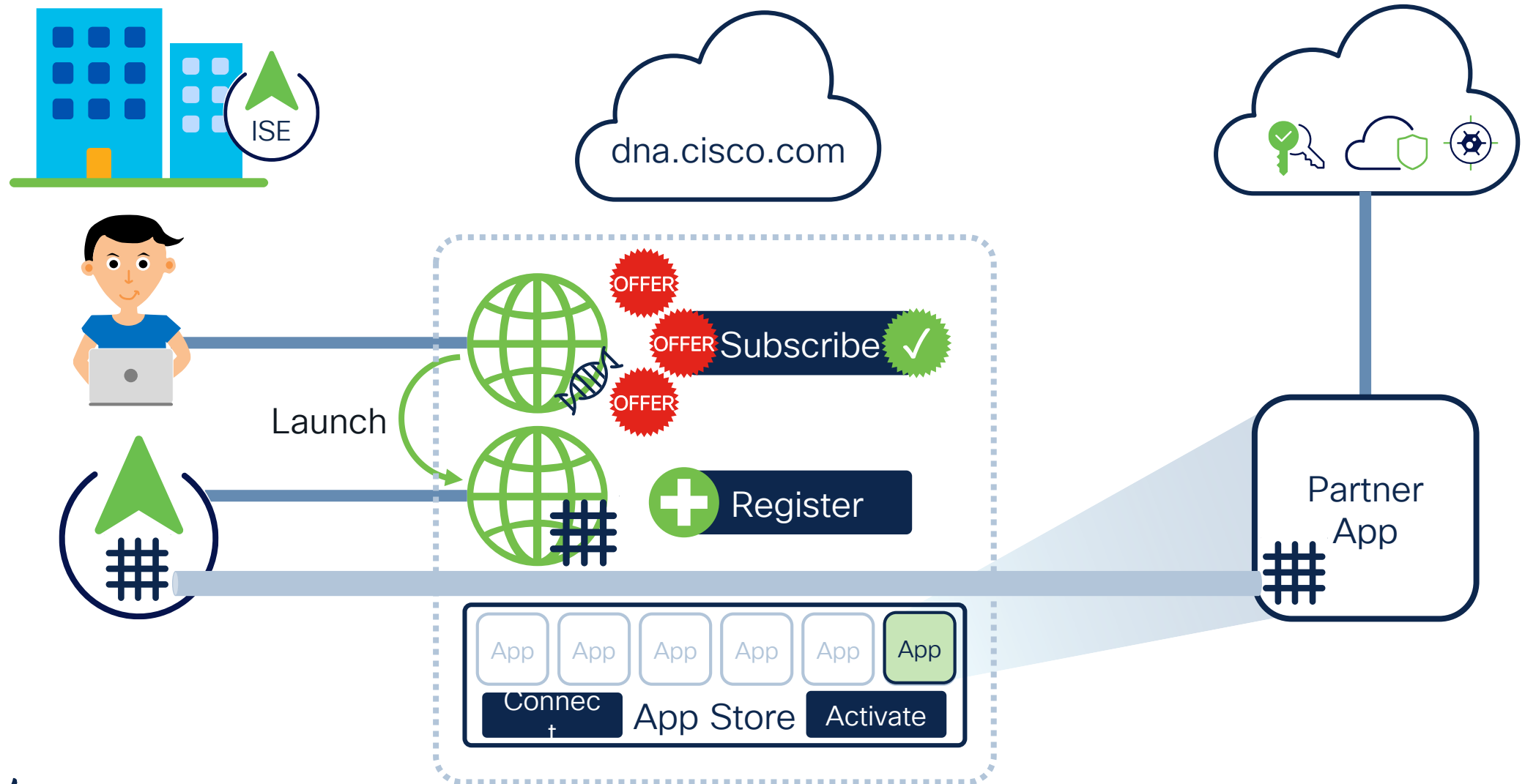
Context Sharing with pxGrid
Eco system partnership to enrich, exchange context and enact

Context to Partner

Cisco ISE   Eco-Partner

CONTEXT

ISE makes Customer
IT Platforms User/Identity,
Device and Network Aware

Enrich ISE Context

Cisco ISE   Eco-Partner

CONTEXT

Enrich ISE context. Make
ISE a better Policy
Enforcement Platform

Threat Mitigation

Cisco ISE   Eco-Partner

ACTION

MITIGATE
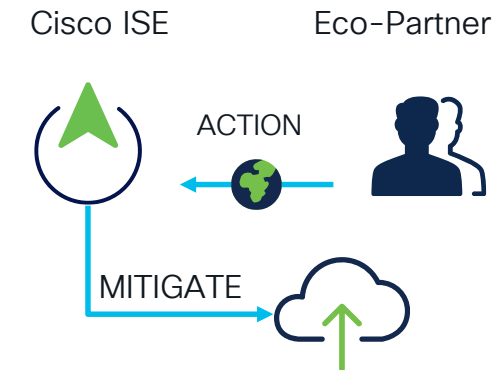
Enforce dynamic policies
into the network based on
Partner's request

Context Brokerage

Cisco ISE

Eco-Partner

ISE 2.2+

ISE brokers Customer's IT
platforms to share data
amongst themselves

PxGrid/ANC Policies in ISE
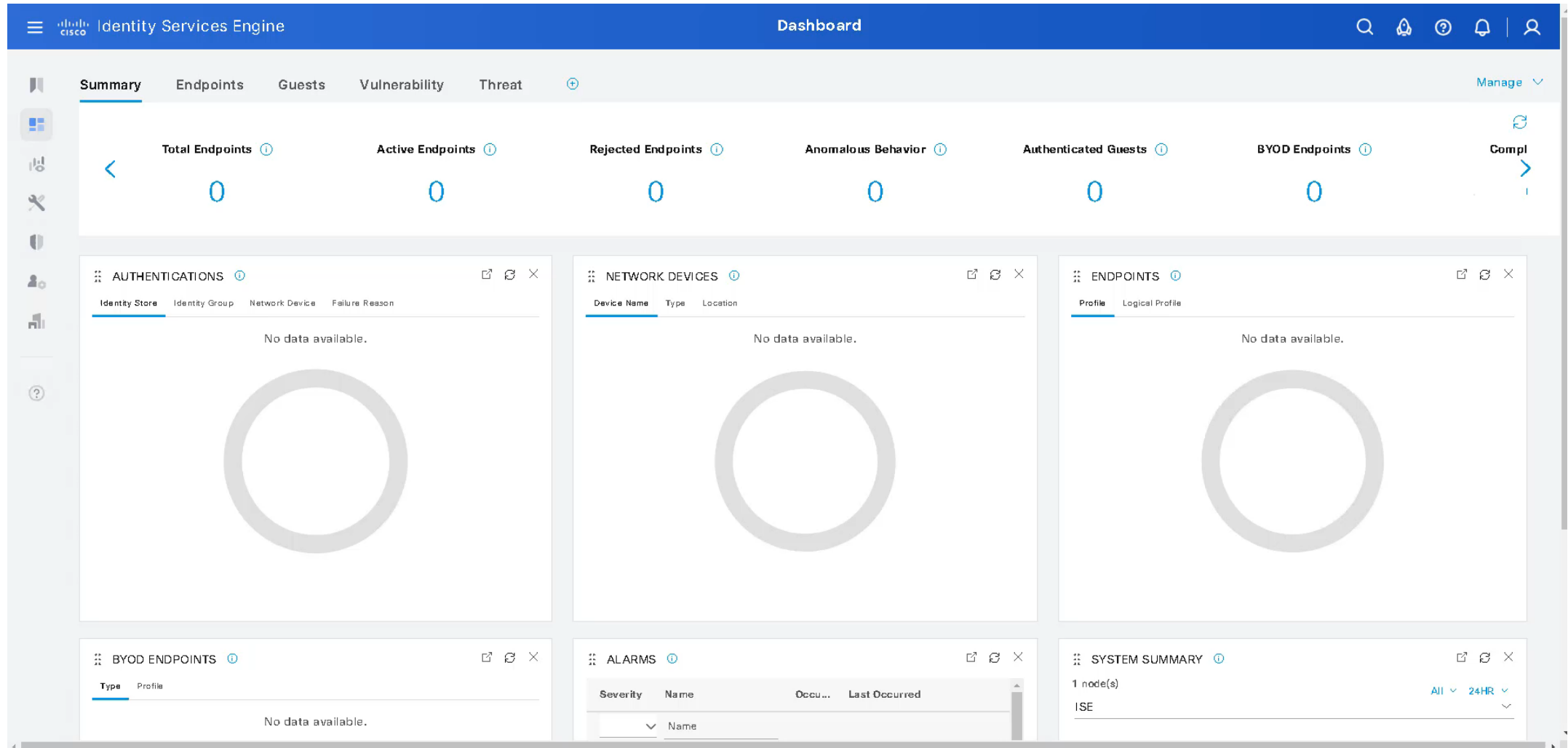
Other pxGrid Use-Case Examples

- Secure Firewall
  - Share IP-to-Username binding, SGT, and profile information with Secure Firepower
  - Create ACPs in Firepower based on profile, identity/AD Group, and SGT
  - Quarantine endpoints from ISE based on detections from Secure Firewall

- Secure Network Analytics (SNA)
  - Shares IP-to-Username binding, SGT, and profile information with SNA
  - Create network-based detection policies in SNA that will quarantine or change access endpoint access level through ISE

- And much more...

pxGrid Integration Tips

- Start with integrating to share context out:
  - Gives information to a pxGrid subscriber such as username-to-IP binding, profile, SGT, etc

- (Optional) Migrated data in for richer profiling:
  - Custom third party attributes don't build the profiles themselves
  - Will still need to build profiles
  - Leverage AI Analytics to help

- Rapid Threat Containment:
  - Automates the change of access based on a trigger from a pxGrid subscriber
  - Start with the "low hanging fruit" – Don't need to quarantine everything

Threat-Centric NAC (TC-NAC)

- Integrates with third-party vulnerability scanners such as Qualys, Rapid7, and Tenable
  - Trigger an endpoint scan
  - Ingest vulnerability information into ISE

- Integrates with Cisco Secure Endpoint and Cognitive Threat Analytics
  - Ingests threat information about an endpoint

- Contextual information stored under endpoint attributes as well as Context Visibility dashboards to see overview of the data

Vulnerability Assessment with Threat-Centric NAC

On-prem Scanner

③ Scans

Jim **❶**

⑥

Quarantine

Full Access

② Scan Jim's Endpoint

Scan report **④**

Harry

⑤

CVSS=10

RAPID7
tenable
network security

Cisco ISE

Alice
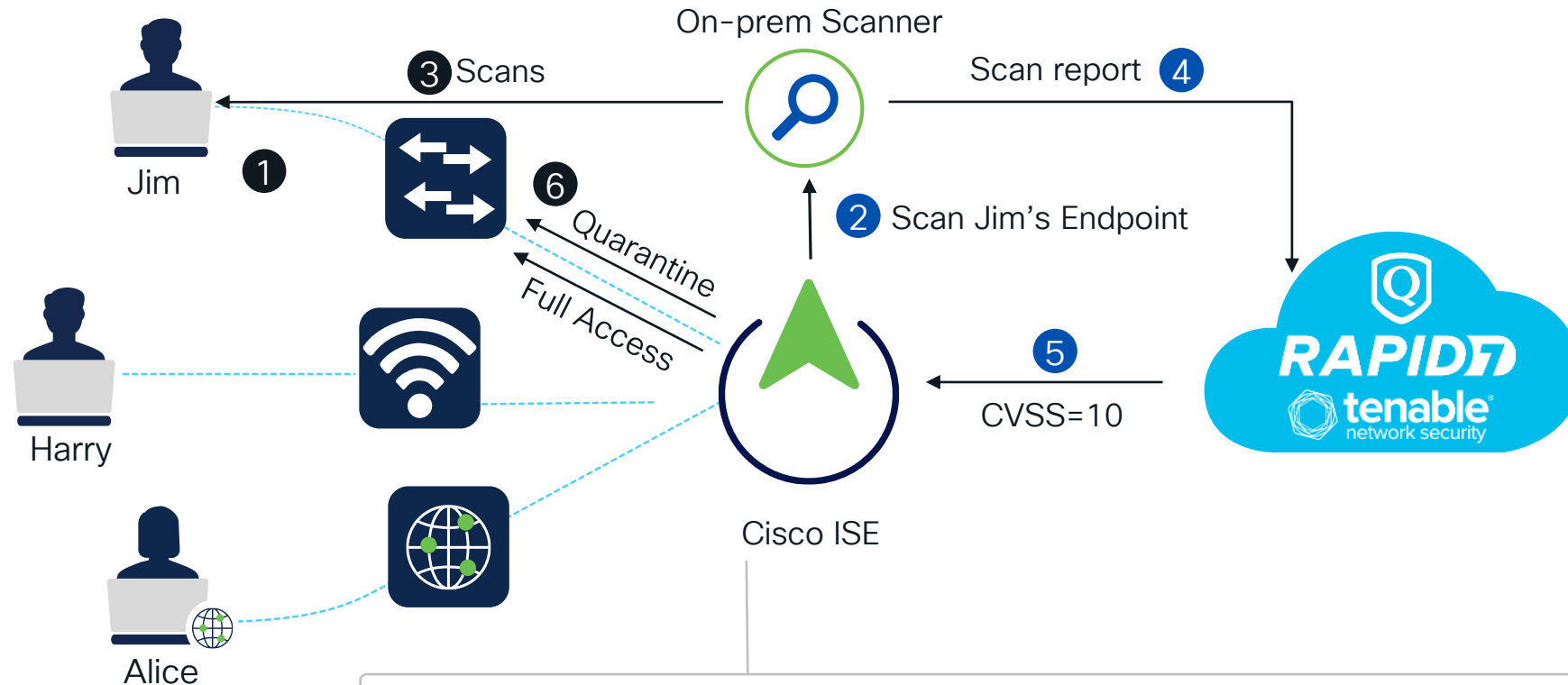
Authorization Policy

If CVSS is Greater than 5 = true, then Quarantine

CVSS: Common Vulnerability Scoring System

MDM Integrations

- Integrates with many third-party MDM vendors

- Onboard endpoints to MDM through ISE

- Control and visibility into non-corporate and mobile devices

- MDM posture checks in ISE authorization rules

Name	Internal Name	Description
DaysSinceLastCheckin	days_since_lastc...	Number of days since last checkin
DeviceCompliantStatus	compliant_status	Compliant Status of device on MDM
DeviceRegisterStatus	register_status	Status of device registration on MDM
DiskEncryptionStatus	disk_encryption_on	Device disk encryption on MDM
IMEI	imei	IMEI
JailBrokenStatus	jail_broken	Is device jail broken
Manufacturer	manufacturer	Manufacturer name
MDMFailureReason	mdm_failure_reas...	Reason for MDM Server connection failure
MDMServerName	mdmServerName	MDM server name
MDMServerReachable	MDMserverReach...	MDM server reachability
MEID	meid	MEID
Model	model	Device model
OsVersion	os_version	Device Operating System
PhoneNumber	phone_number	Phone number
PinLockStatus	pin_lock_on	Device Pin lock status
SerialNumber	serial_number	Device serial number
ServerType	server_type	Type of device management server
UDID	udid	UDID
UserNotified	user_notified	Has the user been notified

MDM Integration Example

ISE APIs and Automation

OpenAPIs

Postman

REST

ISE

internaluser

certificate

sgt   sgacl

endpoint

policy

identitygroup

node   portal

activedirectory

guestuser
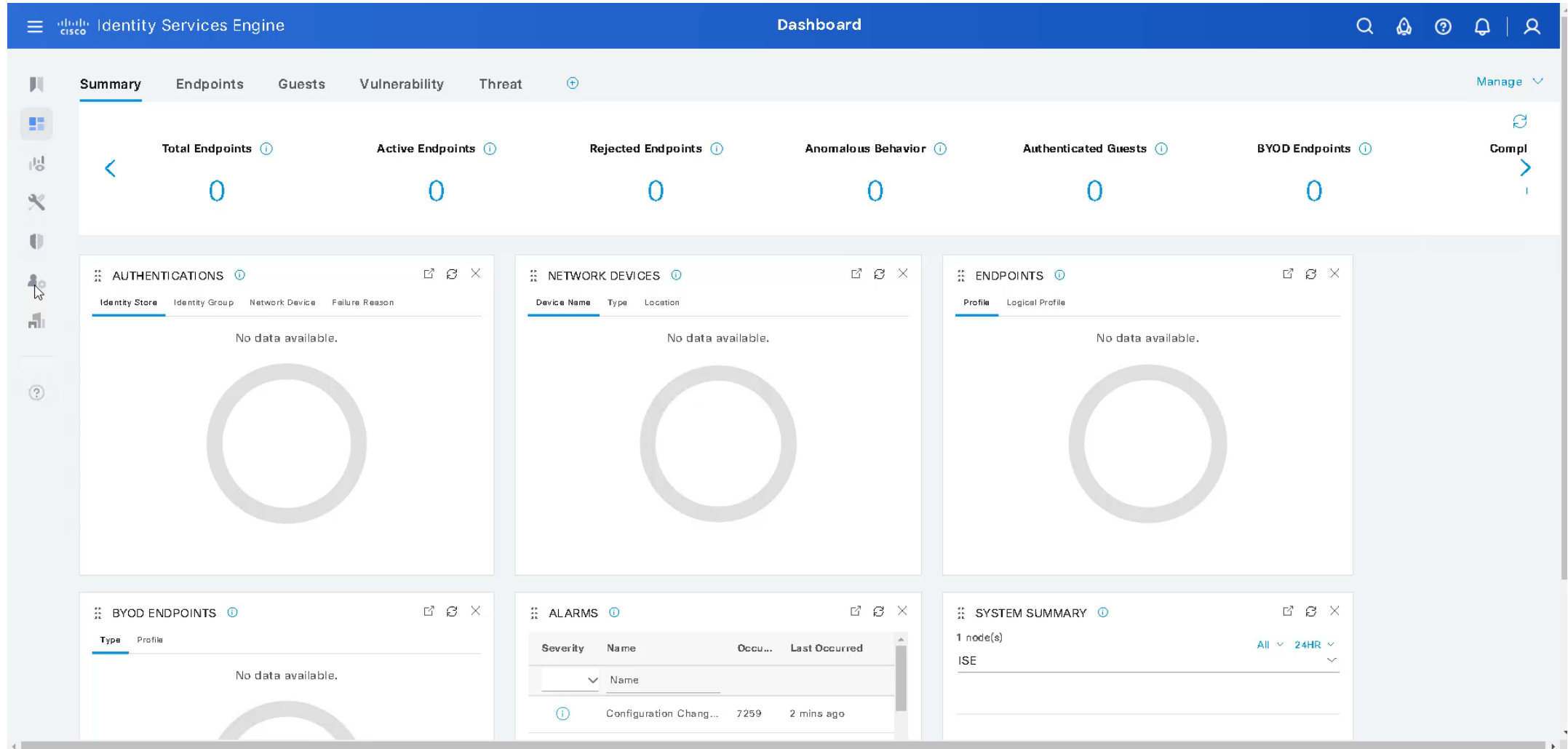
Integration Example: Catalyst Center and ISE

- Catalyst Center supercharges AI Analytics

  - Granular profile recommendations utilizing telemetry and DPI

- Zero trust: Trust Score

  - Score based on:

    - Change in profile label

    - Traffic pattern anomaly

    - Unauthorized ports and weak credentials

    - and more

  - Quarantine low scoring endpoints via ISE integration

- Configure Trustsec SGACLs and policy utilizing historic traffic patterns

Catalyst Center Trust Score and Spoofing Detection
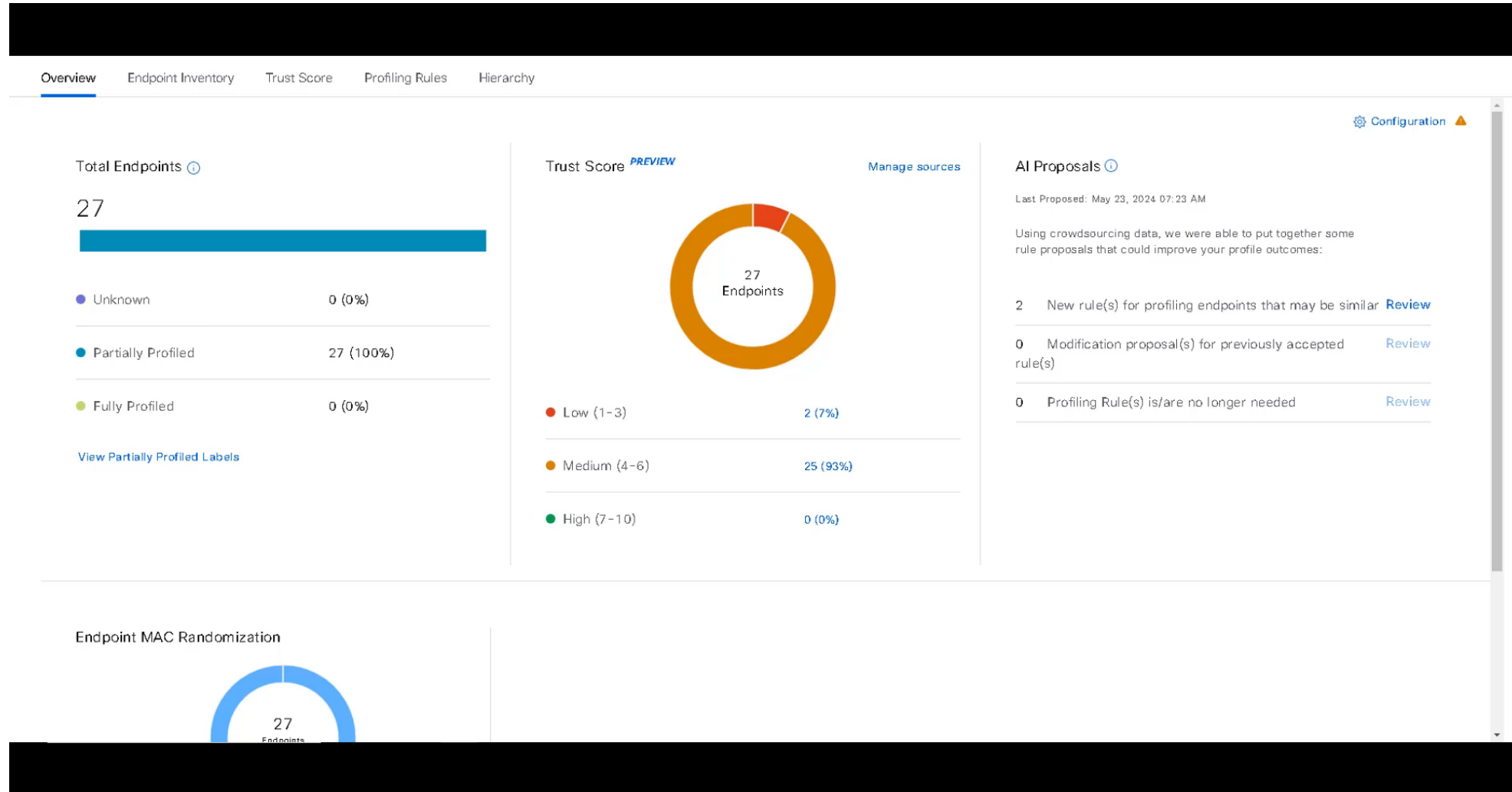
Catalyst Center AI Endpoints Telemetry
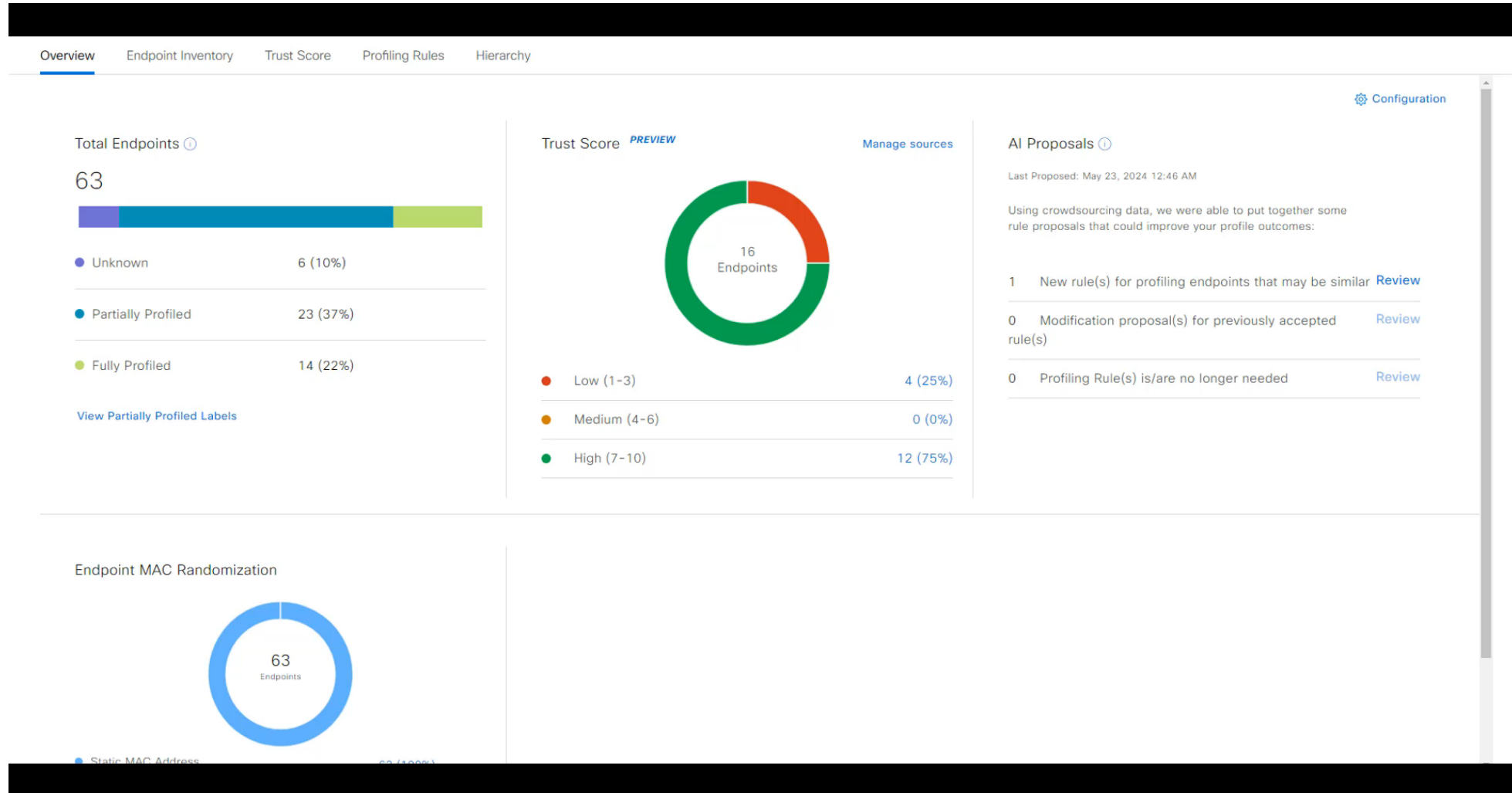
TrustSec Policies with Catalyst Center Integration
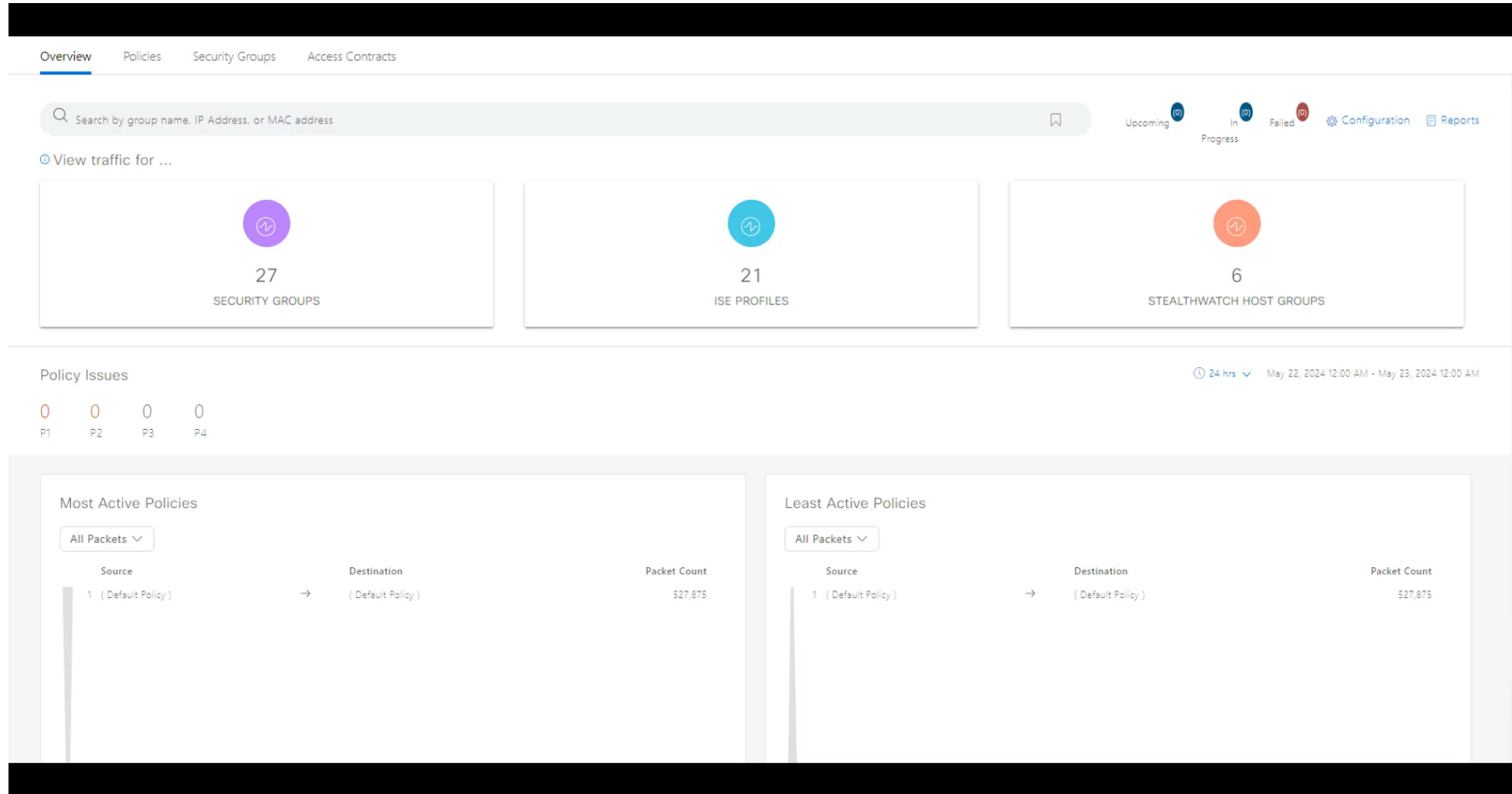
Post-Deployment

Supporting your ISE Deployment

- Document, Document Document!
  - Policy Configuration
  - Supplicant Configuration
  - Certificate Information
  - Network Access Devices
  - Network Access Device Configuration

- Standardize above Configurations

Supporting your ISE Deployment

- ISE Version
  - Patch Regularly
    - If possible, wait until patch is 1-2 weeks old
  - Upgrade when necessary
    - End of Support
    - Necessary feature
    - Preferably upgrade to gold star

- Backup Schedule
  - Operational Backup – Occasionally
  - Configuration Backup - Regularly

Supporting your ISE Deployment

- Utilized built-in ISE roles for Helpdesk, NOC, etc

- Train your support
  - Avoid being called for every issue
  - Playbook for common issues for:
    - NOC
    - Helpdesk

- Know the tools you have to troubleshoot and monitor your deployment
  - Create your playbook for your support with these tools
  - Hidden Troubleshooting slides in this presentation for the playbook

Troubleshooting Endpoint Issues

- ISE –
  - **Operations>RADIUS>Live Logs** – Click the Details for the failed authentication
  - **Operations>Troubleshooting> Diagnostic Tools>Endpoint Debug** – Add MAC address and start debug

- Endpoint –
  - Check the supplicant configuration for the endpoint
  - Check that all necessary certificates are installed on the endpoint
  - Check the OS version
  - Check if User, Computer or User and Computer authentication is picked
  - For wired access, ensure that the Wired AutoConfig service is turned on
  - Check if endpoint is joined to AD domain or BYOD onboarded

Troubleshoot Network Access Device Issues

- ISE –

  - **Administration>Network Resources>Network Devices** – Check to see if NAD exists and shared secret

  - **Operations>RADIUS>Live Logs** – Check to see alerts for Misconfigured Network Devices and RADIUS drops

- Network Access Device –

  - Check OS version/model – Are similar NADs working with same OS/model?

  - Check configuration – Is it running the same template as others with same OS/model?

  - Are only some endpoints on the device failing? Check to see if CoA is working

  - Debug commands

  - RADIUS/TACACS source interface defined?

Debugging Switches for ISE/CTS Issues

- General CTS:
  - debug cts all
  - debug cts condition level detail
  - debug cts messages
  - debug cts packets
- PAC Failure:
  - debug cts provision events
  - debug cts provision packet
  - debug cts ifc events

- AAA:
  - debug radius
  - debug radius all
  - debug cts aaa
  - debug cts ifc events
  - debug eap events
  - debug eap errors
  - debug authen event
  - debug authen error
  - debug dot1x all
  - debug authen feature all
  - debug mab all

- CTS Auth
  - debug cts authen details
  - debug cts auth
  - debug dot1x events
  - debug dot1x packets
  - debug dot1x errors
  - debug cts ifc events
- CTS Policy dnload:
  - debug cts author event
  - debug cts author
  - debug cts author aaa
  - debug cts aaa
  - debug cts ifc events

Debugging Switches for ISE/CTS Issues

For your reference only

- CTS Policy Install:
  - debug cts author event
  - debug cts autho
  - debug cts author aaa
  - debug cts author rbacl
  - debug rbm
  - debug rbm policy
  - debug rbm binding
  - debug rbm api
  - debug rbm platform
  - debug cts ifc events

- CTS Env Data:
  - debug cts environment-data all
  - debug cts env
  - debug cts aaa
  - debug radius
  - debug cts ifc events
  - debug cts authe
  - debug cts autho

- CTS L3IF & Mapping:
  - debug rbm bindings
  - debug cts ifc events
  - debug cts sgt-map

- CTS SAP:
  - debug cts sap events
  - debug cts ifc events
  - debug cts errors
  - debug cts sap packets
  - debug macsec events
  - debug cts sap pakdump
  - debug cts dp info
  - debug cts dp error
  - debug macsec
  - debug cts sap

- CTS Cache:
  - debug cts ifc events
  - debug cts cache

Debugging Switches for ISE/CTS Issues

For your reference only

- CTS HW Path:
  - debug platform cts dp api
  - debug platform cts dp event
  - debug platform cts dp error
  - debug platform cts dp redundancy

- CTS HA/Sync
  - debug cts ha core
  - debug cts ha config
  - debug cts ha infra
  - debug cts err
  - debug cts ifc ev
  - debug cts cluster
  - debug cts ha

- CTS SGT Cache:
  - debug rbm bindings
  - debug rbm api
  - debug fm rbacl caching packets
  - debug fm rbacl caching events
  - debug fm rbacl all
  - debug fm rbacl monitoring
  - debug cts sgt-caching

- SXP:
  - debug cts sxp connection
  - debug cts sxp errors
  - debug cts sxp all
  - debug cts sxp
  - debug cts sxp internal

- debug cts sxp mdb
- debug cts sxp message
- debug ip tcp trans
- debug up tcp packet

- IPv6:
  - debug ipv6 snooping binding
  - debug ipv6 snooping fsm
  - debug epm all
  - debug epm events session details
  - debug epm plugin cts error
  - debug epm plugin cts event
  - debug rbm all

Debugging Switches for ISE/CTS Issues

For your reference only
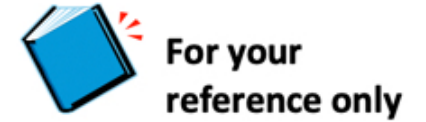
- CoA:
  - **debug cts coa event**
  - **debug aaa coa**
  - **debug radius dynamic-authorization**

- NX-OS Specific:
  - **show tech-support cts**
  - **show tech-support forward l3 unicast detail**
  - **show tech module** <mod #>
  - **show tech-support routing ip unicast**

Troubleshoot Network Access Device Issues
Operations>RADIUS>Live Logs – Check Misconfigured Network Devices

Troubleshooting Network Issues

- Check bandwidth utilization

- Check interfaces for dropped packets

- Check QoS – RADIUS being prioritized?

- IP connectivity
  - Traceroute

- Packet filtering?
  - To/from NAD PSNs to ISE
  - Ports allowed? 1812/UDP, 1813/UDP, 1700/UDP, etc

Network Ports open for ISE

DNS: tcp-udp/53
NTP: udp/123
Repository: FTP, SFTP, NFS, HTTP, HTTPS
File Copy: FTP, SCP, SFTP, TFTP

pxGrid Subscriber/Publisher

pxGrid (Bulk Download): tcp/8910

pxGrid: tcp/5222

PXG

pxGrid: tcp/5222

Email/SMS Gateways

Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
NetFlow for TS: udp/9993

NADs

MNT

SMTP:tcp/25

Logging

HTTPS; tcp/443
Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
Oracle DB (Secure JDBC): tcp/1528
JGroups: tcp/12001 (MnT to PAN)

HTTPS: tcp/443
Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
CoA (REST API): udp/1700

RADIUS Auth: udp/1645,1812
RADIUS Acct: udp/1646,1813
RADIUS CoA: udp/1700,3799
RADSEC DTLS: udp/2083
RADIUS/IPsec: udp/500
TACACS+: tcp/49 (configurable)
WebAuth: tcp:443,8443
SNMP: udp/161
SNMP Trap: udp/162
NetFlow: udp/9996
DHCP:udp/67, udp/68
DHCPv6: udp/547
SPAN:tcp/80,8080
SXP: tcp/64999
OCSP: tcp/2560
CA SCEP: tcp/9090

SMTP: tcp/25 (PPAN: email expiry notifiy)

pxGrid: tcp/5222
JGroups: tcp/12001

PSN

PAN

HTTPS: tcp/443
JGroups: tcp/12001 (PSN to PAN)
CoA (Admin/Guest Limit): udp/1700

Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
SNMP Traps: udp/162

MDM Partner

MDM API: tcp/XXX (vendor specific)

Query Attributes

TC-NAC: tcp/443

Threat/VA Server

Posture Updates/Smart Licensing: tcp/443
Profiler Feed: tcp/8443

GUI: tcp/80,443
SSH: tcp/22
Sponsor (PSN): tcp/8443
SNMP: udp/161
REST API (MnT): tcp/443
ERS API: tcp/9060

Guest: tcp/8443
Discovery: tcp/8443, tcp/8905
Agent Install: tcp/8443
Posture Agent: tcp/8905; udp/8905
PRA/KA: tcp/8905
DNS: udp/53; DHCP:udp/67
WMI Client Probe: tcp/135, tcp/445
Kerberos (SPAN): tcp/88
SCEP Proxy: tcp/80, tcp/443
EST: tcp/8084

LDAP: tcp-udp/389, tcp/3268
SMB:tcp/445
KDC:tcp-udp/88; KPASS: tcp/464
SCEP: tcp/80, tcp/443; EST: tcp/8084
OCSP: tcp/80;
CRL: tcp/80, tcp/443, tcp/389
ODBC (configurable):
  Microsoft SQL: tcp/1433
  Sybase: tcp/2638
  PortgreSQL: tcp/5432
  Oracle: tcp/1512
TS-Agent: tcp/9094
AD Agent: tcp/9095
WMI: tcp/135
Syslog: udp/40514, tcp/11468

Inter-Node Communications

Admin(P) - Admin(S): tcp/443, tcp/12001(JGroups)

Monitor(P) - Monitor(S): tcp/443, udp/20514 (Syslog)

Policy - Policy:
  Node Groups/JGroups: tcp/7800
  Proxy CoA: udp/1700
  PSN-SXPSN: tcp/443

pxGrid - pxGrid: tcp/5222

PIP

Cloud Services
Cisco.com/Perfigo.com
Profiler Feed Service
MDM & App Stores
Push Notification
Smart Licesing

Admin->Sponsor: tcp/9002
Wireless Setup
Wizard: tcp/9103

Admin / Sponsor

IdP: tcp/XXX (Vendor specific)

IdP SSO Server

Endpoint

Troubleshooting ISE Issues

- Check ISE health
  - RADIUS latency?
  - RADIUS packets on other PSNs?
  - Check load guidelines
  - ISE replication occurring?

- Certificates
  - Any expired certificates?
  - Missing trusted CAs?

Troubleshooting ISE Issues

Dashboard – Check Authentication Latency per ISE Node
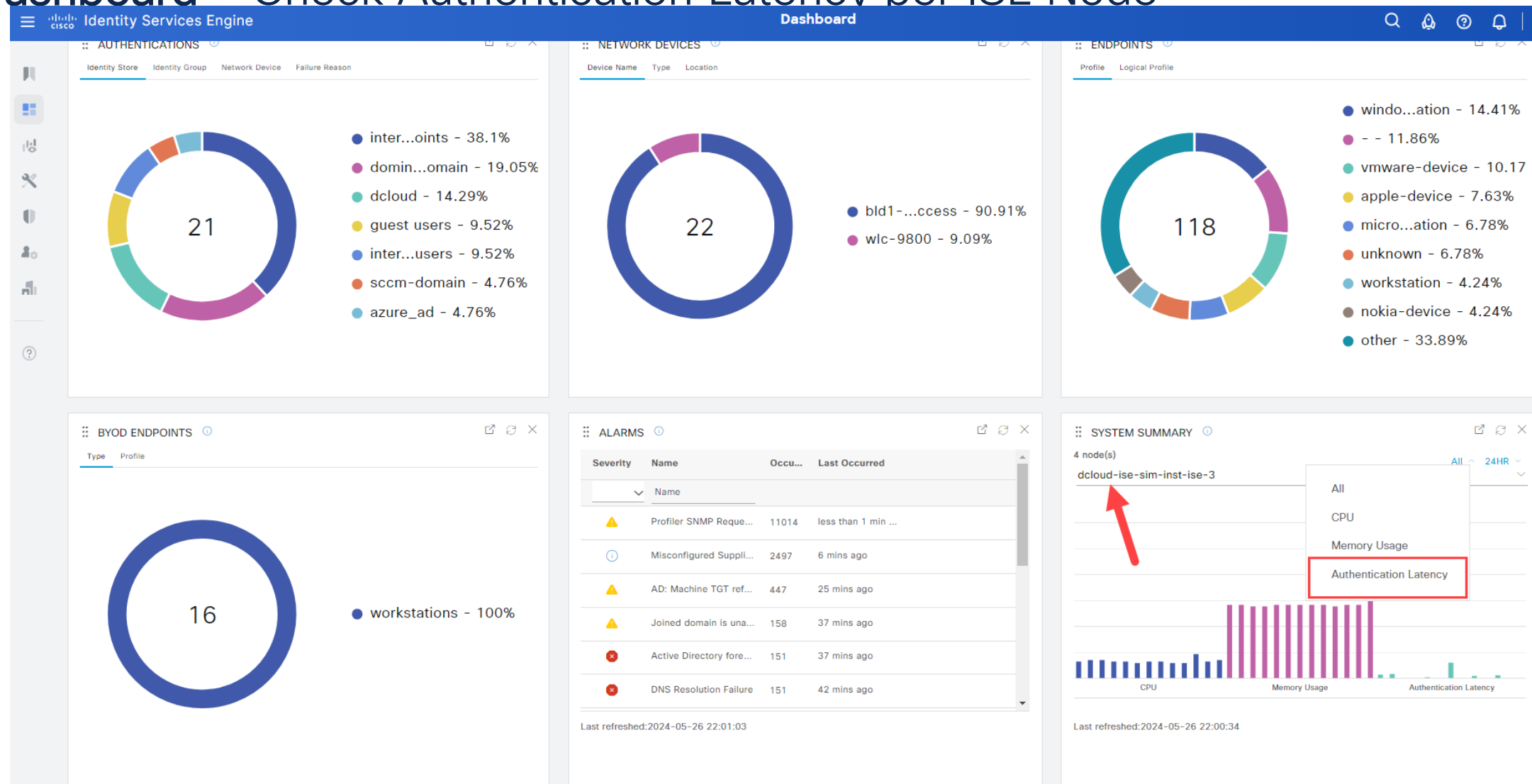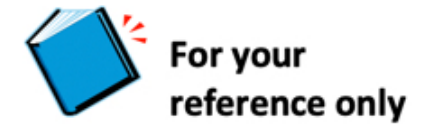
Troubleshooting ISE Issues
Administration>System>Deployment – Check Node Status for replication issues

Troubleshooting ISE Issues

Administration>System>Certificates>System Certificates – Check system

For your reference only

Troubleshooting ISE Issues
Administration>System>Certificates>Trusted Certificates – Check Trusted

For your reference only

Check for the existence of root certificates that you expect endpoints to authenticate against - could be manufacturer certificates, internal PKI, etc

Check expiration dates

Check status

Troubleshooting ISE Issues
Administration>Deployment – Check Node Status for replication issues

Troubleshooting ISE Issues
Operations>System 360>Monitoring – ISE Node Health Monitoring
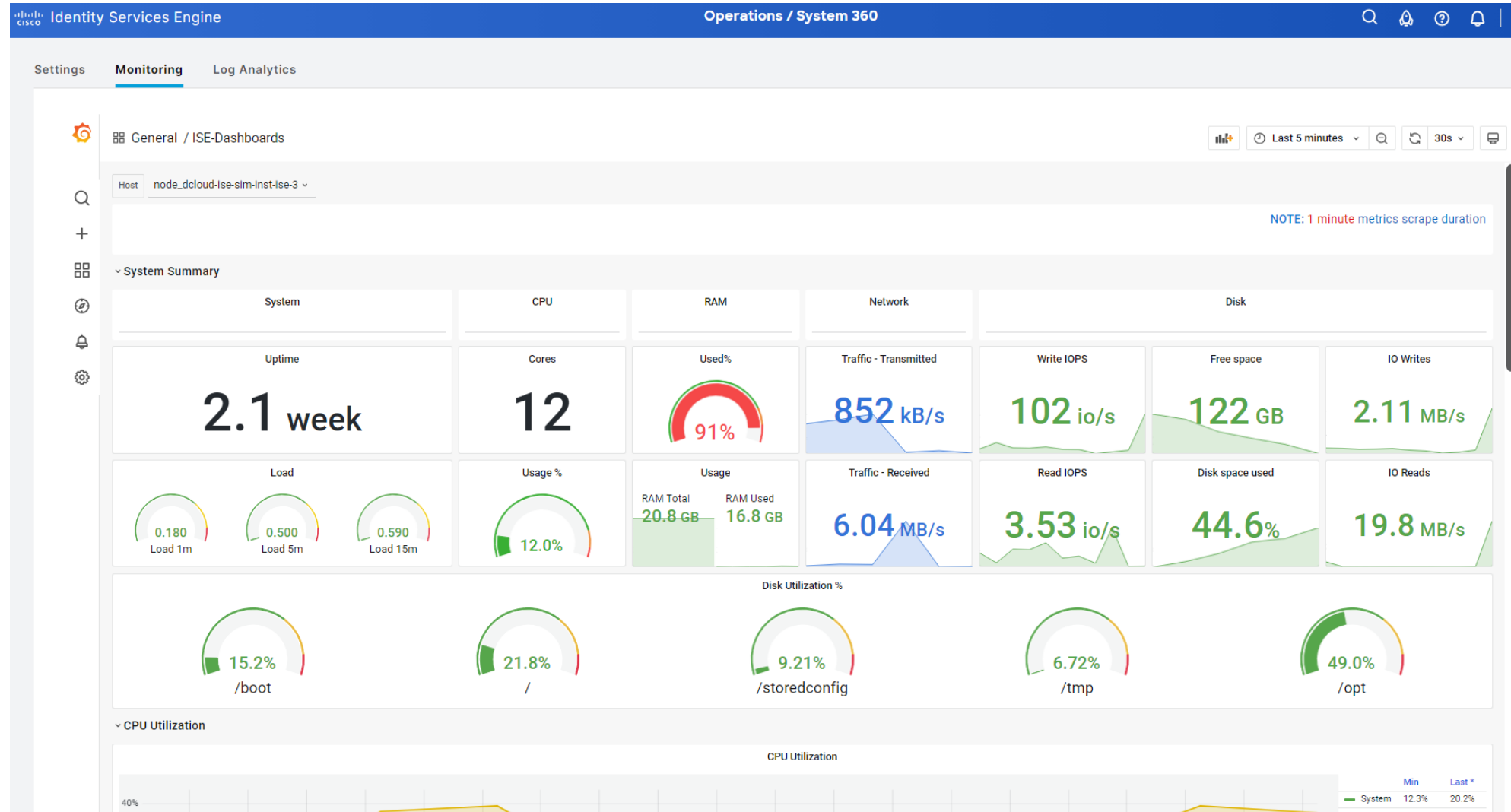
Troubleshooting ISE Issues

Administration>Network Resources>Network Devices – Check to see if NAD exis

Identity Services Engine — Administration / Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | pxGrid Direct Connectors | More

Network Devices
Default Device
Device Security Settings
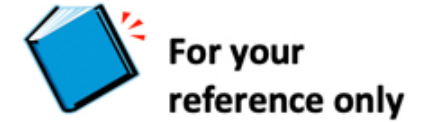
Network Devices

2. Filter by NAD IP address

Selected 0 Total 16

Edit   + Add   Duplicate   Import   Export   Generate PAC   Delete

Quick Filter

1. Quick filter

Name	IP/Mask	Profile Name	Location	Type	Description
LDN-ASA-VPN	10.10.2.1/32	Cisco	Europe#London 1	VPN Headend	
LDN1-C9200-Edge3.pseudoco.com	10.10.11.9/32	Cisco	Europe#London 1	All Device Types	
LDN1-C9300-DIST1.pseudoco.com	10.10.11.5/32	Cisco	Europe#London 1	Switch#PseudoCo-SDA-...	
LDN1-C9300-DIST2.pseudoco.com	10.10.11.6/32	Cisco	Europe#London 1	Switch#PseudoCo-SDA-...	
LDN1-C9300-Edge1.pseudoco.com	10.10.11.7/32	Cisco	Europe#London 1	Switch#PseudoCo-SDA-...	
LDN1-C9300-Edge2.pseudoco.com	10.10.11.8/32	Cisco	Europe#London 1	Switch#PseudoCo-SDA-...	
LDN1-C9300-SS.pseudoco.com	10.10.1.3/32	Cisco	Europe#London 1	Switch#PseudoCo-SDA-...	
LDN1-C9500-BC1.pseudoco.com	10.10.11.3/32	Cisco	Europe#London 1	Switch#PseudoCo-SDA-...	
LDN1-C9500-BC2.pseudoco.com	10.10.11.4/32	Cisco	Europe#London 1	Switch#PseudoCo-SDA-...	
LDN1-C9800-01.PseudoCo.com	10.10.10.42/32	Cisco	Europe#London 1	WLC#PseudoCo-SDA-W...	
LDN1-ISR4K-SS.pseudoco.com	10.10.1.2/32	Cisco	Europe#London 1	All Device Types	
MXC1-C9800-01.PseudoCo.com	10.13.12.82/32	Cisco	Americas#MXC 1	WLC#PseudoCo-nonSD...	
SJ1-C9300-BC1.pseudoco.com	10.12.11.3/32	Cisco	Americas#SJ 1	All Device Types	
SJ1-C9300-BC2.pseudoco.com	10.12.11.4/32	Cisco	Americas#SJ 1	All Device Types	
SJ1-C9300-Edge1.pseudoco.com	10.12.11.7/32	Cisco	Americas#SJ 1	All Device Types	
SJ1-C9300-Edge2.pseudoco.com	10.12.11.8/32	Cisco	Americas#SJ 1	All Device Types	

Troubleshooting ISE Issues
Operations>System 360>Log Analytics – ISE Node, RADIUS, and TACACS Health

Troubleshooting ISE Issues

Operations>Troubleshooting>Diagnostic Tools>RADIUS Authentication Troubleshooting – Troubleshoot RADIUS Authenications
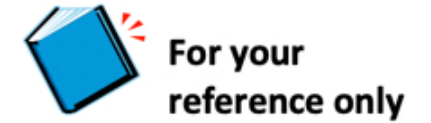
Troubleshooting ISE Issues
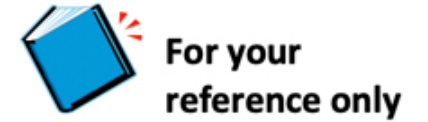
Operations>Troubleshooting>Diagnostic Tools>Posture Troubleshooting – Troubleshoot Posture Events

Troubleshooting ISE Issues

Operations>Troubleshooting>Diagnostic Tools>Agentless Posture Troubleshooting – Troubleshoot Agentless Posture Events

Troubleshooting ISE Issues

Operations>Troubleshooting>Diagnostic Tools>TCP Dump – Troubleshoot traffic a PSN is receiving

Troubleshooting ISE Issues

Operations>Troubleshooting>Diagnostic Tools>Session Trace – Test the policy flows in a predictable way without needing real traffic from a real

Identity Services Engine

Diagnostic Tools   Download Logs   Debug Wizard

General Tools

RADIUS Authentication Troubl...

Execute Network Device Com...

Evaluate Configuration Validat...

Posture Troubleshooting

Agentless Posture Troublesho...

EndPoint Debug

TCP Dump

Session Trace Tests

TrustSec Tools

Session Trace Test Cases

Add   Duplicate   Trash ⌄   Edit   ▶ Run

☐	Name	Type	Description

No data found.

Troubleshooting ISE Issues – Policy Troubleshooting 1

Operations>RADIUS>Live Logs – Check AuthC/AuthZ policy and rules the endpoint hits

Troubleshooting ISE Issues – Policy Troubleshooting 2
Operations>RADIUS Live Logs – Click Details for endpoint

Troubleshooting ISE Issues – Policy Troubleshooting 3

Detail: Check Steps on the right side to see authentication details

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD-PseudoCo	
11017	RADIUS created a new session – pseudoco.com	0
15049	Evaluating Policy Group - AD-PseudoCo	1
15008	Evaluating Service Selection Policy	0
15048	Queried PIP - DEVICE.Deployment Type	1
15048	Queried PIP - Radius.Called-Station-ID	0
15048	Queried PIP - Radius.NAS-IP-Address	0
15048	Queried PIP - DEVICE.Location	0
11507	Extracted EAP-Response/Identity	1
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	7
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	0
61025	Open secure connection with TLS peer	1
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	46
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0

PEAP successfully negotiated as outer EAP Method

Step ID	Description	Latency (ms)
12304	Extracted EAP-Response containing PEAP challenge-response	1
11808	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated	0
15041	Evaluating Identity Policy	0
25114	Number of bad password attempts for AD instance is lower than the configuration in Active Directory, Continuing to AD authentication.	5
15013	Selected Identity Source - AD-PseudoCo	1
24430	Authenticating user against Active Directory - AD-PseudoCo	0
24325	Resolving identity – Grace.Smith	1
24313	Search for matching accounts at join point - pseudoco.com	0
24319	Single matching account found in forest - pseudoco.com	0
24323	Identity resolution detected single matching account	0
24343	RPC Logon request succeeded - Grace.Smith@pseudoco.com	2
24402	User authentication against Active Directory succeeded - AD-PseudoCo	0
22037	Authentication Passed	0
11824	EAP-MSCHAP authentication attempt passed	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	4
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	0
11810	Extracted EAP-Response for inner method containing MSCHAP challenge-response	0
11814	Inner EAP-MSCHAP authentication succeeded	0
11519	Prepared EAP-Success for inner EAP method	0
12314	PEAP inner method finished successfully	0
12305	Prepared EAP-Request with another PEAP challenge	1

MSCHAP is the inner authentication method

Credentials Grace.Smith@psuedoco.com are extracted and authenticated against pseudoco.com Active Directory domain
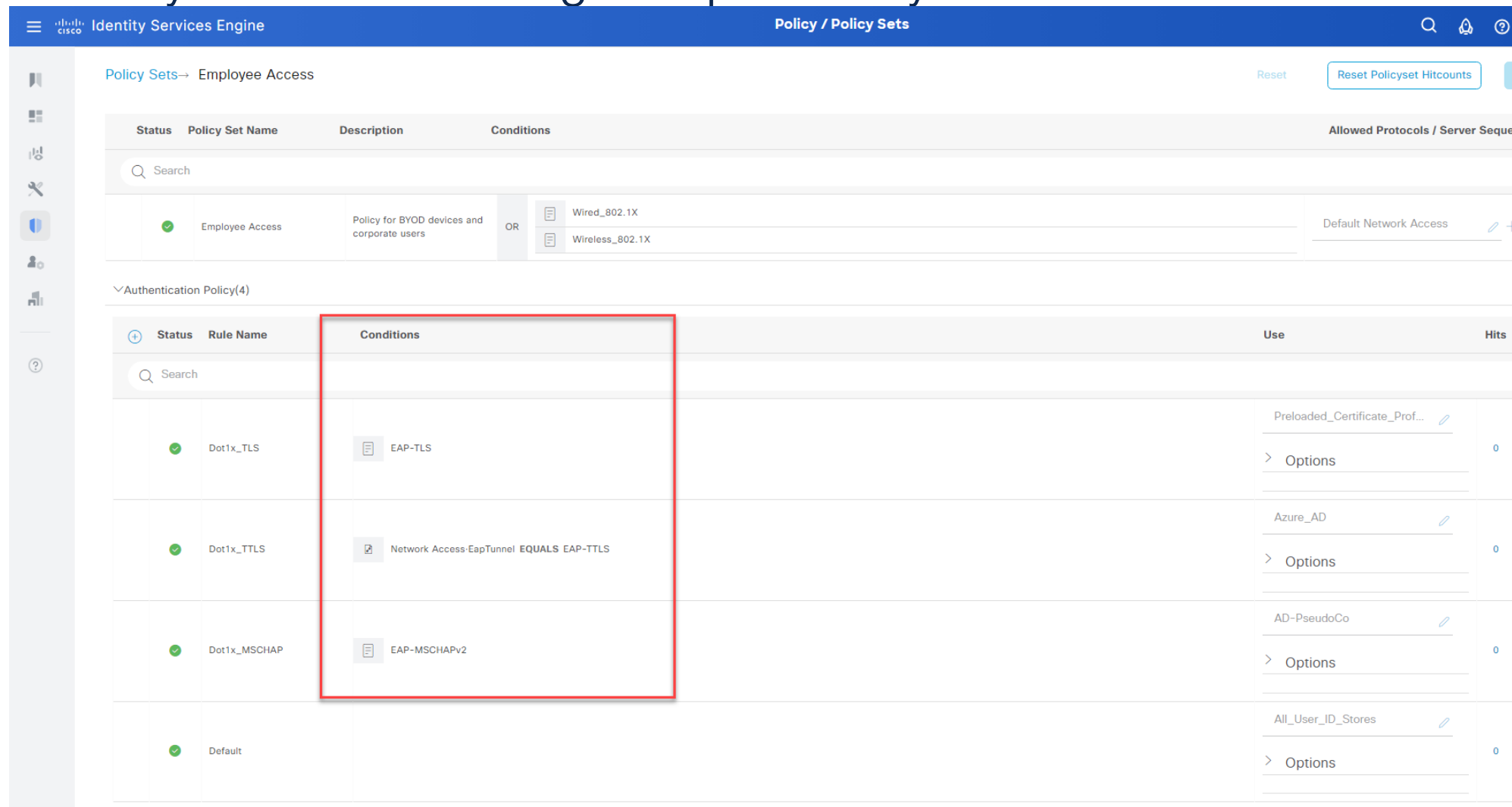
Authentication to Active Directory Successful

Troubleshooting ISE Issues – Policy Troubleshooting 4

Policy>Policy Sets – Check Conditions compared to authentication details

Troubleshooting ISE Issues – Policy Troubleshooting 5
Check Policy Set conditions against previously checked Authentication Detail

Troubleshooting ISE Issues – Policy Troubleshooting 6
Check Policy Set conditions against previously checked Authentication Detail

Conclusion
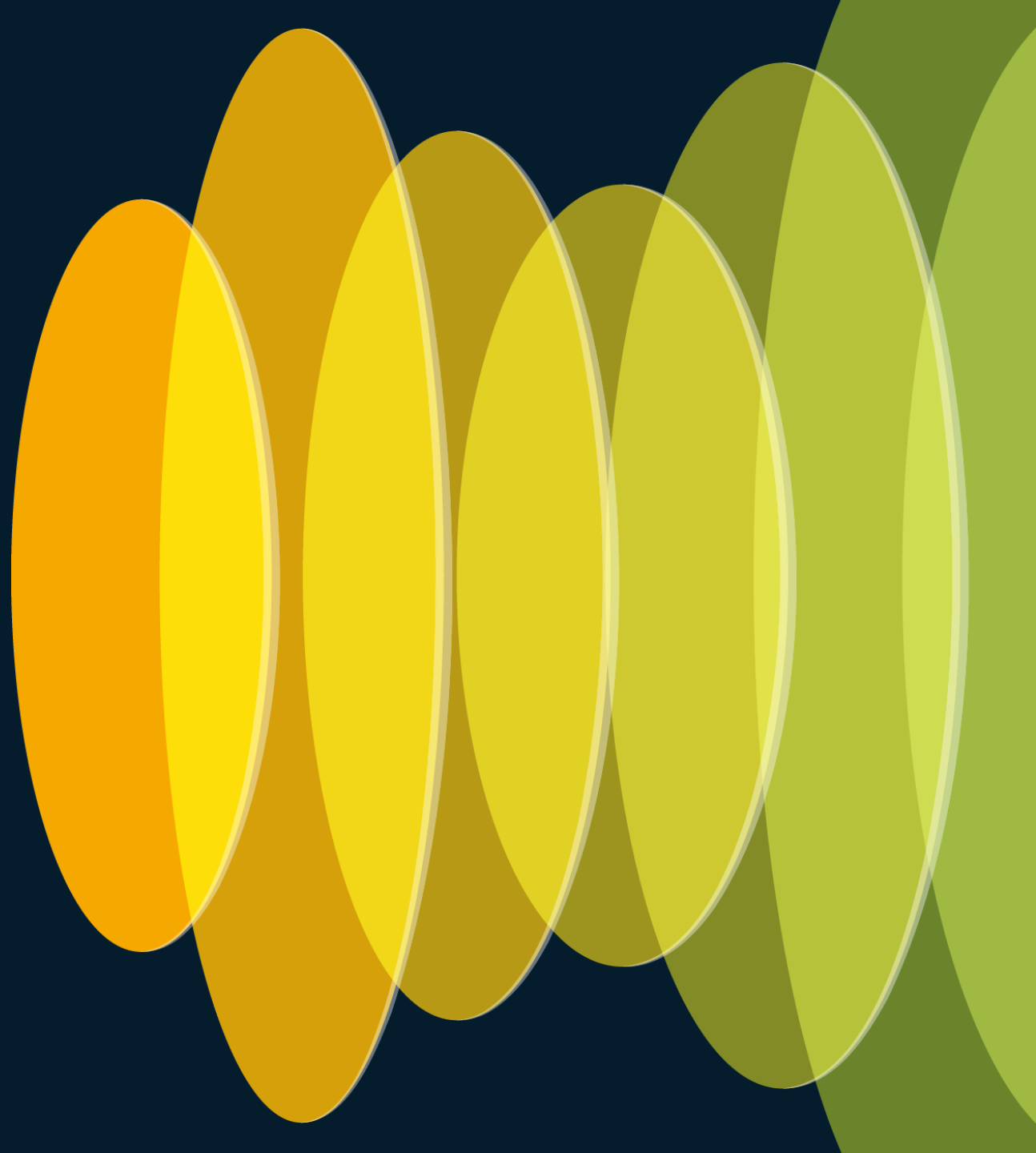
Simplifying and optimizing your deployment is how you can lower the administrative burden of managing ISE

Helpful Links and Training

- CiscoPress SISE Book – https://tinyurl.com/ciscopress-sise

- ISE Scalability Guide – https://tinyurl.com/ise-scale

- ISE Loadbalancing Guides – https://tinyurl.com/ise-loadbalancing

- ISE NAD Compatability Matrix – https://tinyurl.com/ise-compatibility

- ISE Mega-list of Integration/Configuration Guides – https://cs.co/ise-guides

- Cisco Security Technical Alliance Partners – https://cisco.com/go/csta

- Deploy ISE in Cloud – https://tinyurl.com/ise-cloud

- ISE APIs and Automation – https://github.com/CiscoISE

Helpful Links and Training

- ISE Switch Deployment Guide – https://tinyurl.com/ise-switch-guide

- ISE WLC Deployment Guide – https://tinyurl.com/ise-wlc-config

- ISE Catalyst 9800 Wireless Guide – https://tinyurl.com/ISE-9800-Guide

- Profile Packs:
  - Medical NAC 2.0 Profiles – https://tinyurl.com/ise-medical-nac-2
  - Automation and Control Profiles – https://tinyurl.com/ise-automation-library
  - Industrial Network Director IoT Profiles – https://tinyurl.com/ind-profiles
  - Windows-Embedded IoT Profiles – https://tinyurl.com/windows-embedded

- ISE Licensing – https://cs.co/ise-licensing

Helpful Links and Training

- TrustSec Troubleshooting Guide – https://tinyurl.com/TS-Troubleshooting

- ISE Webinars – https://cs.co/ise-webinars

- ISE Community – https://cs.co/ise-community

- Cisco's ISE YouTube Channel – https://cs.co/ise-videos

Helpful Links and Training

- Network-Node Blog – https://www.network-node.com

- My ISE Videos – https://tinyurl.com/KM-ISE-Videos

- Labminutes ISE Configuration Videos – https://tinyurl.com/LM-ISE

- Aaron Woland's ISE Blog Posts – https://tinyurl.com/Woland-ISE

- Brad Johnson's ISE Support Blog – https://www.ise-support.com

- Steve McNutt's Blog –
  - PKI for Network Engineers - https://tinyurl.com/PKI-for-NE
  - ISE Posts – https://tinyurl.com/McNutt-ISE

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

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

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos

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

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

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