

CISCO Live !

ISE Deployment Improvement Tips and Tricks

Katherine McNamara
Cybersecurity Solutions Engineer,
@kmcnam1

BRKSEC-2347

Cisco Webex App

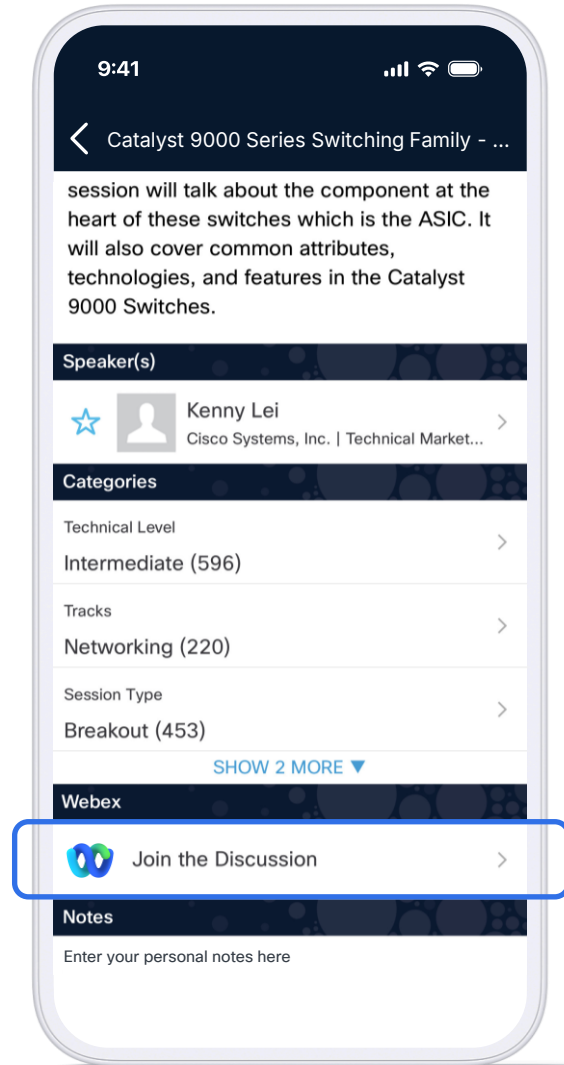
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 13, 2026.



<https://cislive.ciscoevents.com/clamer26/BRKSEC-2347>

Agenda

- 01 Where to Start
- 02 Laying the Foundation
- 03 A Phased Approach
- 04 Tuning Policy Sets
- 05 The Power of Profiling
- 06 Integrations
- 07 Post-Deployment
- 08 Conclusion

A little about me



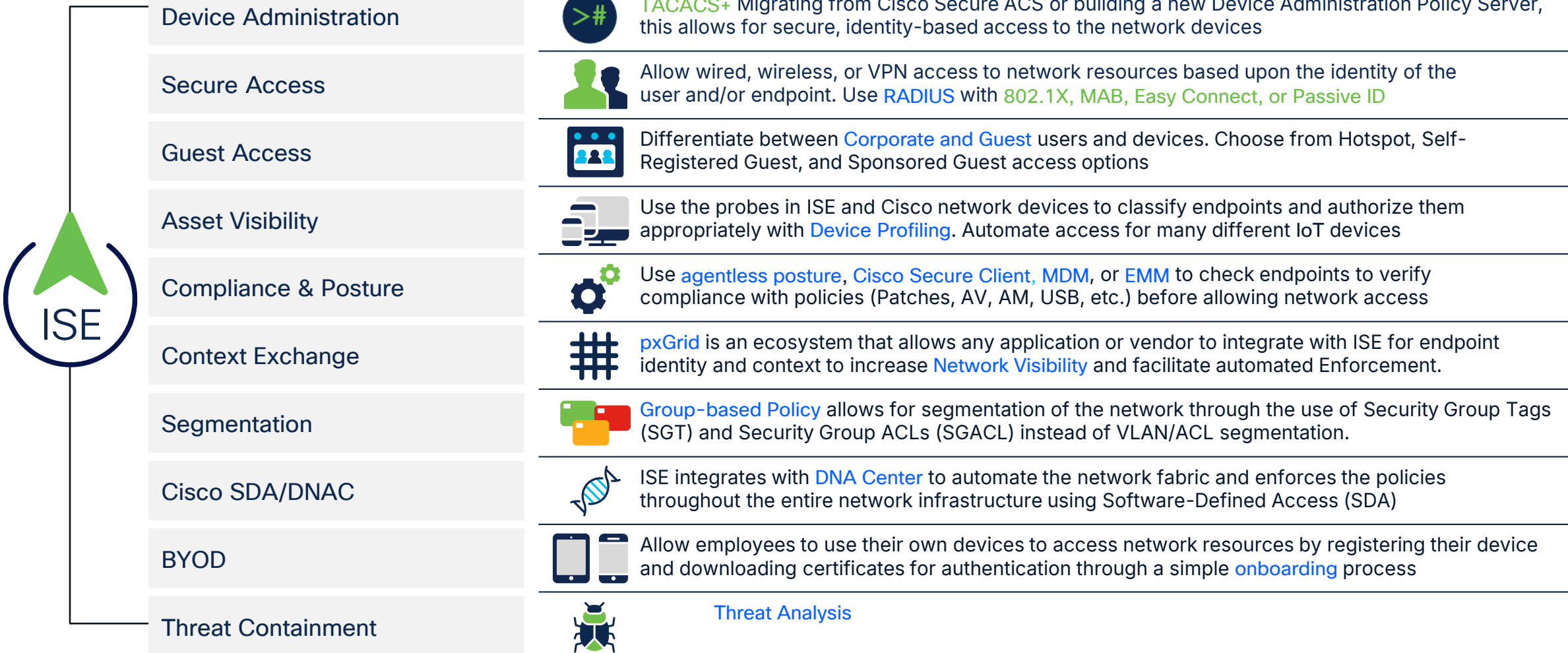
- Started as an early ISE 1.1 customer
- Almost 20 years of network & security experience
- Lots of paper: BS and MS in IT Security, 2x CCIE (Security & Data Center), GPEN, GCIH, CISSP, and various other industry certifications
- Co-authored the most recent CiscoPress SISE book
- Co-organize for the largest Cisco Meetup study group, Router gods
- Owner of network-node and sendthepayload blogs

Where to Start

The background features a light gray gradient. A prominent diagonal bar with a color gradient from red to blue is positioned in the upper right. A blue arc is visible in the bottom left corner.

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

The Swiss Army Knife of Network Access Control



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

The background features a light gray gradient. A diagonal bar with a color gradient from red to blue is positioned in the upper right. A blue arc is visible in the lower left corner.

Laying the Foundation

Where To Start...

- 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

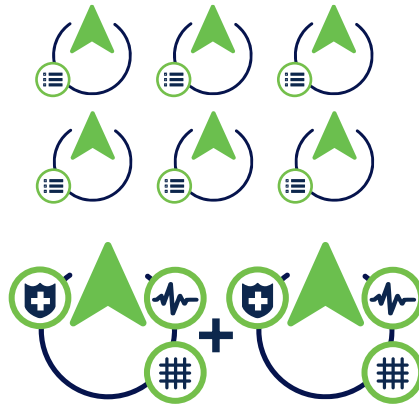
ISE Deployment Scale



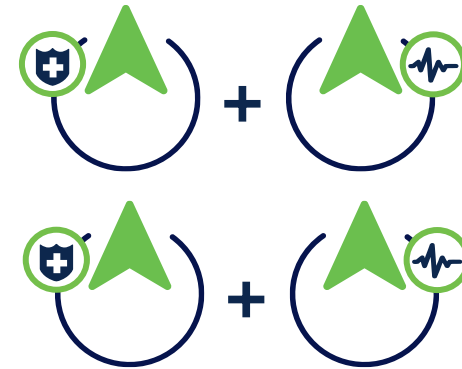
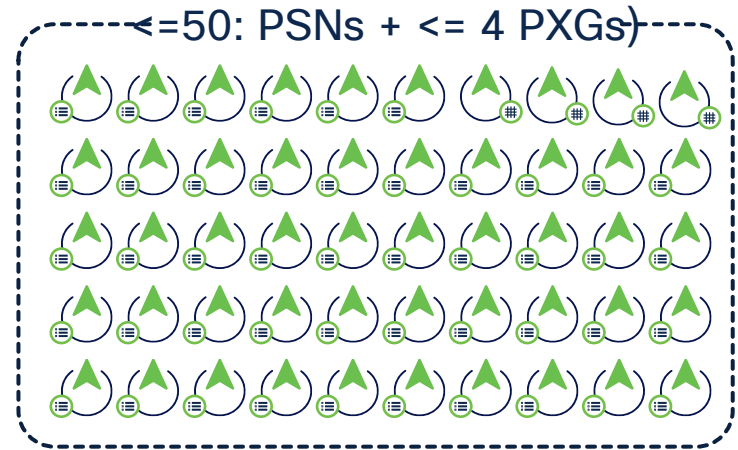
Lab and Evaluation



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 150,000 Endpoints	Up to 2,000,000 Endpoints	3700

ISE Node Types

Physical Appliances

Virtual Machines

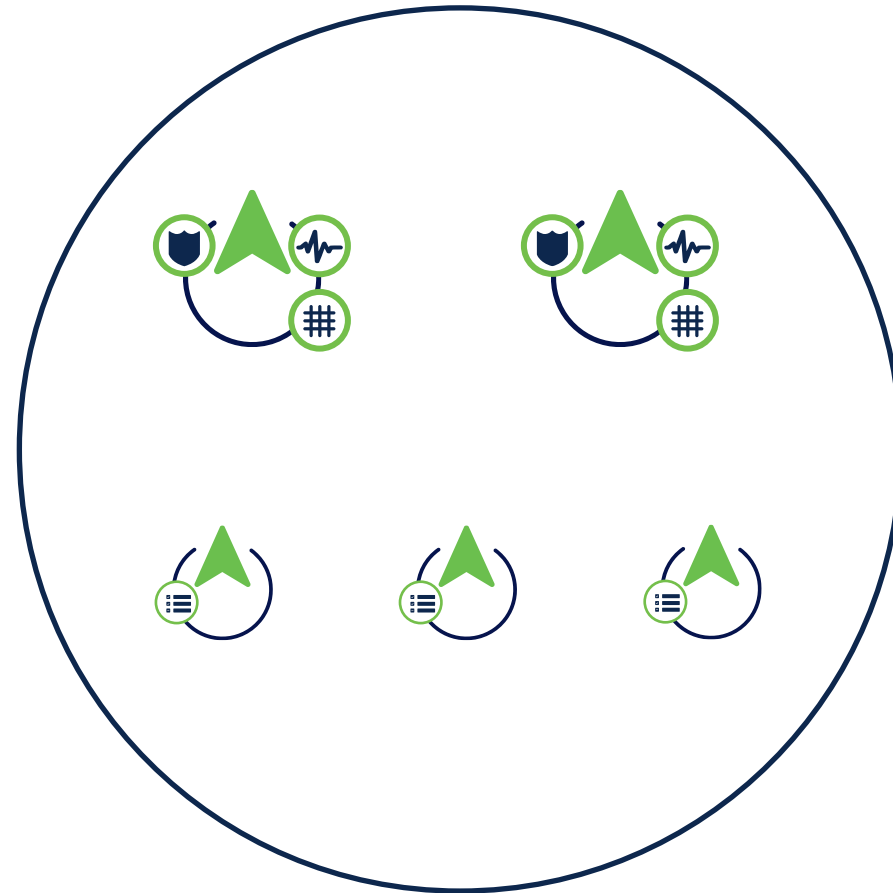
Cloud Instances



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



Expanding your ISE deployment



Add an ISE Node

The screenshot displays the Cisco Identity Services Engine (ISE) dashboard. The browser address bar shows the URL `https://198.18.133.27/admin/#/home`. The dashboard header includes the Cisco logo, the text "Identity Services Engine", and "Dashboard". A navigation menu on the left contains icons for various functions. The main content area features a "Summary" tab and several key performance indicators (KPIs) for endpoints and guests, all showing a value of 0. Below the KPIs are three data tables: "AUTHENTIFICATIONS", "NETWORK DEVICES", and "ENDPOINTS", each displaying "No data available." with a large circular placeholder. At the bottom, there are three more sections: "BYOD ENDPOINTS" (also showing "No data available."), "ALARMS" (with a table header for Severity, Name, Occu..., and Last Occurred), and "SYSTEM SUMMARY" (showing "1 node(s)" and "ISE").

Changing the Persona

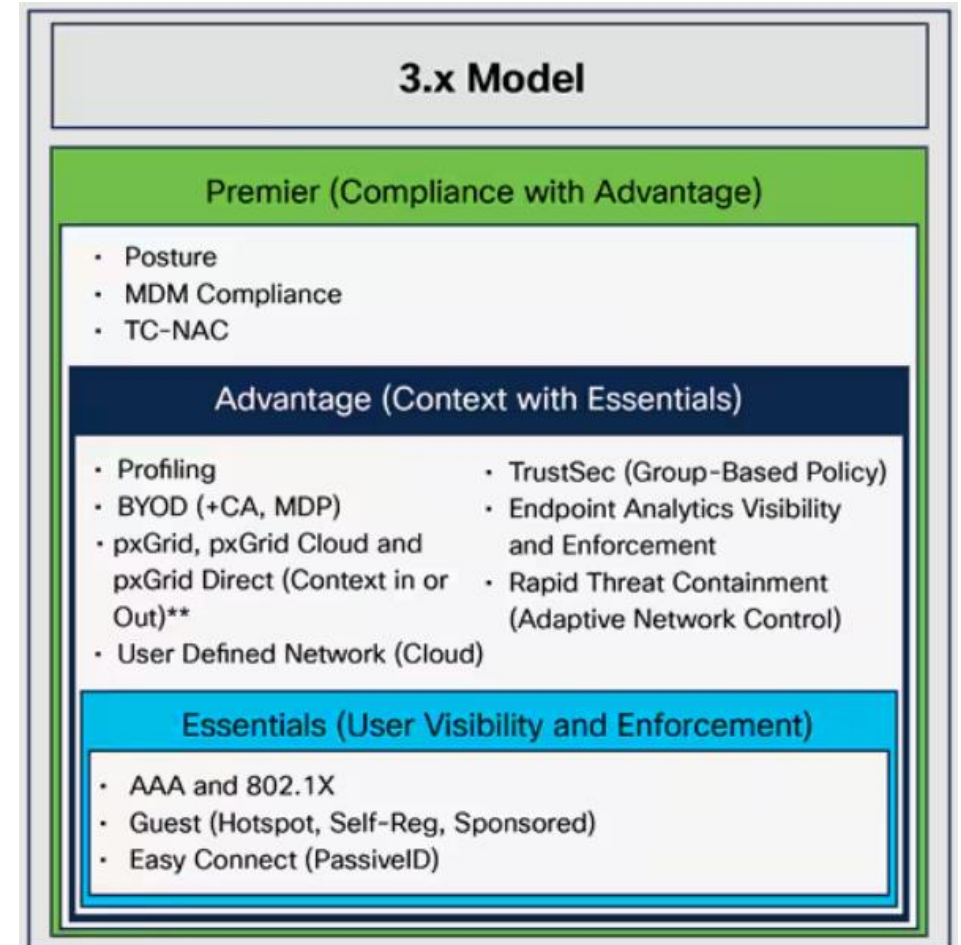
The screenshot displays the Cisco Identity Services Engine (ISE) dashboard. At the top, the browser address bar shows the URL `https://198.18.133.27/admin/#/home`. The dashboard header includes the Cisco logo, the text "Identity Services Engine", and the word "Dashboard". A navigation menu on the left contains icons for various functions. The main content area features a "Summary" tab and a row of six key metrics, each with a value of 0: "Total Endpoints", "Active Endpoints", "Rejected Endpoints", "Anomalous Behavior", "Authenticated Guests", and "BYOD Endpoints". Below these metrics are six data panels, each displaying "No data available." and a large grey circle. The panels are: "AUTHENTIFICATIONS" (with sub-headers "Identity Store", "Identity Group", "Network Device", "Failure Reason"), "NETWORK DEVICES" (with sub-headers "Device Name", "Type", "Location"), "ENDPOINTS" (with sub-headers "Profile", "Logical Profile"), "BYOD ENDPOINTS" (with sub-headers "Type", "Profile"), "ALARMS" (with sub-headers "Severity", "Name", "Occu...", "Last Occurred"), and "SYSTEM SUMMARY" (with sub-headers "1 node(s)", "ISE").

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

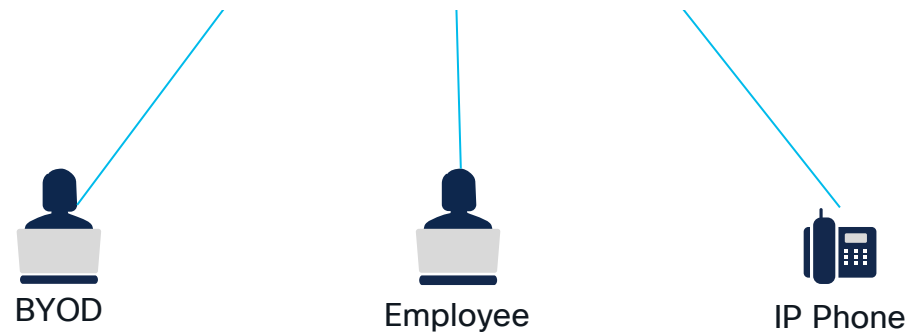
Licensing

- Endpoint licenses are based on concurrently connected 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



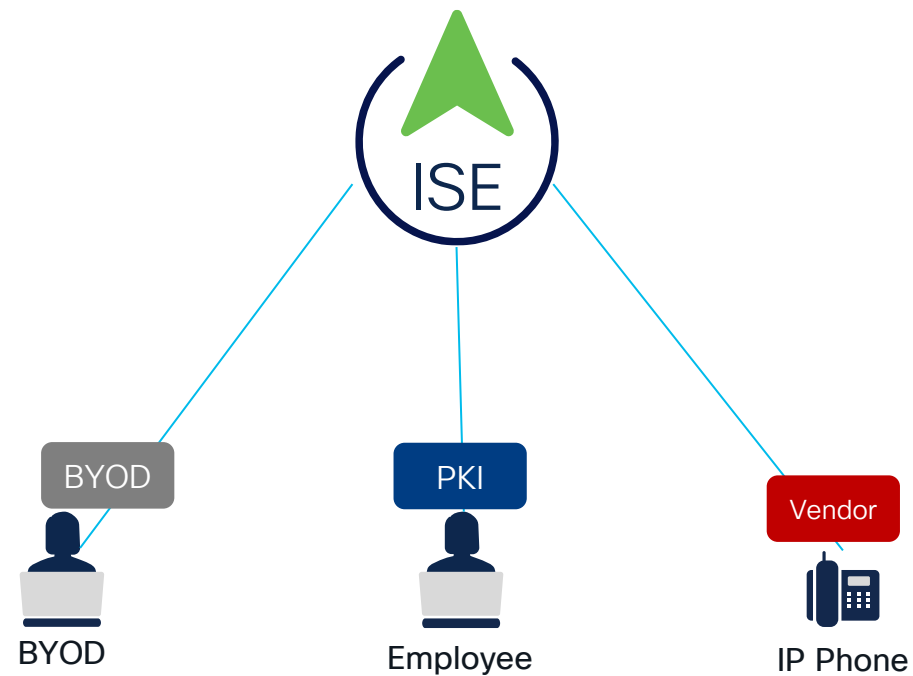
Certificates

- 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

- 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!



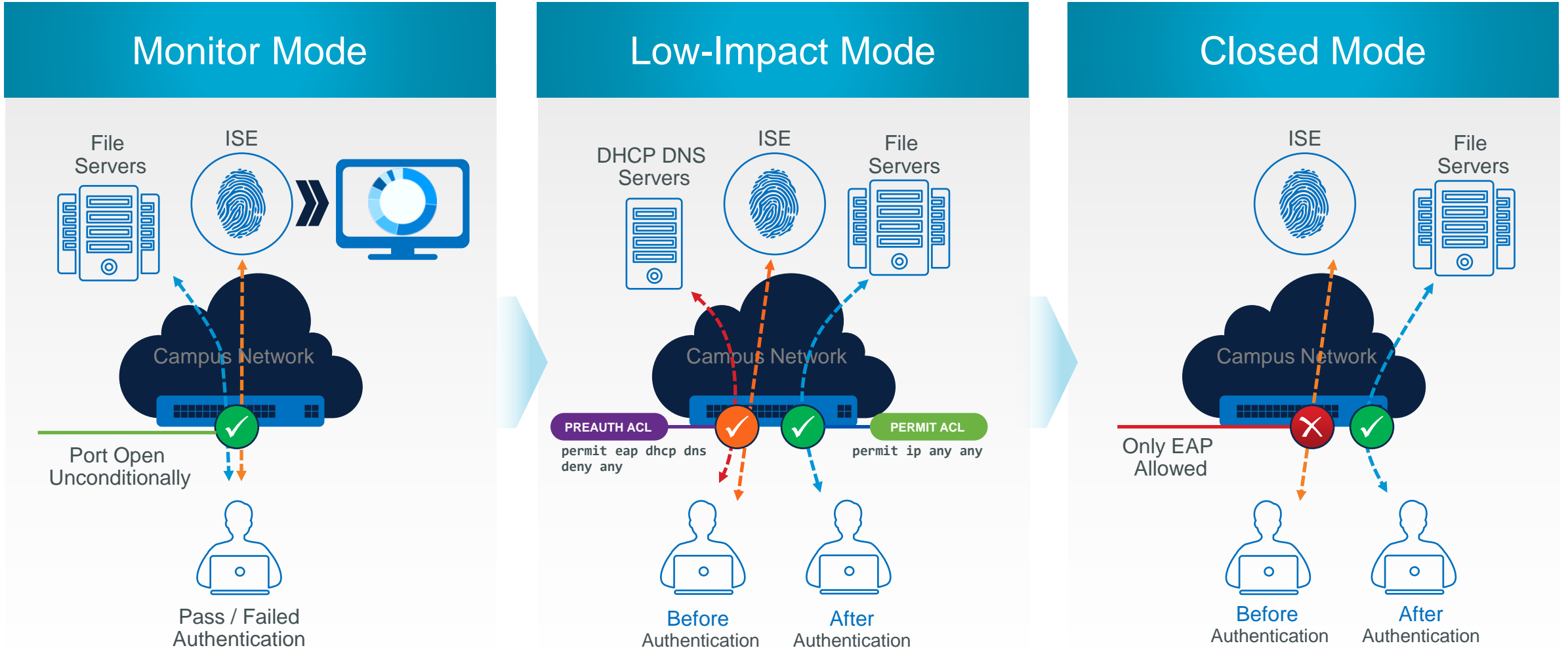


A Phased Approach

A Phased Approach to ISE

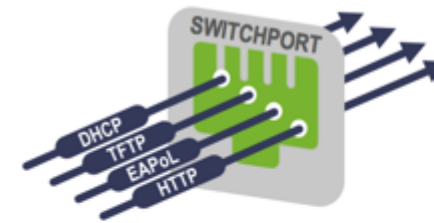
- VPN:
 - Create a test VPN profile
 - Migrate the profile to production after testing
- Wireless:
 - Create a test SSID
 - Migrate the profile to production after testing
- But what about wired?

Wired Phases

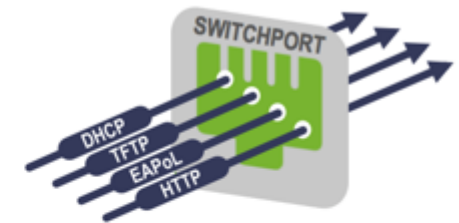


Monitor Mode

- 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

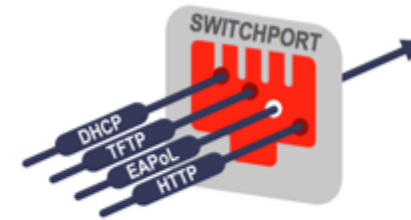
```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
switchport voice vlan 10
authentication host-mode multi-auth
ip access-group PRE-AUTH in
authentication open
authentication port-control auto
mab
dot1x pae authenticator
authentication violation restrict
```

} Low-
Impact
Mode

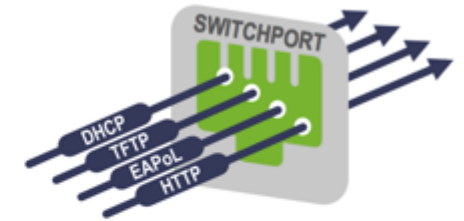
} From
Monitor
Mode

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

Creating and Apply Network Device Groups

The screenshot displays the Cisco Identity Services Engine (ISE) dashboard. The top navigation bar includes the Cisco logo, the text "Identity Services Engine", and "Dashboard". The main content area is divided into several sections:

- Summary:** A row of six cards showing key metrics: Total Endpoints (0), Active Endpoints (0), Rejected Endpoints (0), Anomalous Behavior (0), Authenticated Guests (0), and BYOD Endpoints (0).
- Authentications:** A table with columns for Identity Store, Identity Group, Network Device, and Failure Reason. It displays "No data available."
- Network Devices:** A table with columns for Device Name, Type, and Location. It displays "No data available."
- Endpoints:** A table with columns for Profile and Logical Profile. It displays "No data available."
- BYOD Endpoints:** A table with columns for Type and Profile. It displays "No data available."
- Alarms:** A table with columns for Severity, Name, Occu..., and Last Occurred. It shows one alarm: Configuration Chang... with a severity of 7267 and a last occurrence of less than 1 min ...
- System Summary:** A section showing "1 node(s)" and "ISE".

Monitor Mode for Policy Rules

Identity Services Engine Policy / Policy Sets









Reset Reset Polycyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Wired Monitor Mode		AND DEVICE-Device Type EQUALS All Device Types#Switches DEVICE-Mode EQUALS Mode#Monitor	Default Network Access	0	⚙️	➔
✓	Wired Low-Impact Mode		AND DEVICE-Device Type EQUALS All Device Types#Switches DEVICE-Mode EQUALS Mode#Low-Impact	Default Network Access	0	⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

Reset Save

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

Identity Services Engine Policy / Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Wired Monitor Mode		AND DEVICE-Device Type EQUALS All Device Types#Switches DEVICE-Mode EQUALS Mode#Monitor	Default Network Access	0	⚙️	➔
✓	Wired Low-Impact Mode		AND DEVICE-Device Type EQUALS All Device Types#Switches DEVICE-Mode EQUALS Mode#Low-Impact	Default Network Access	0	⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

Reset Save

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



- 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:

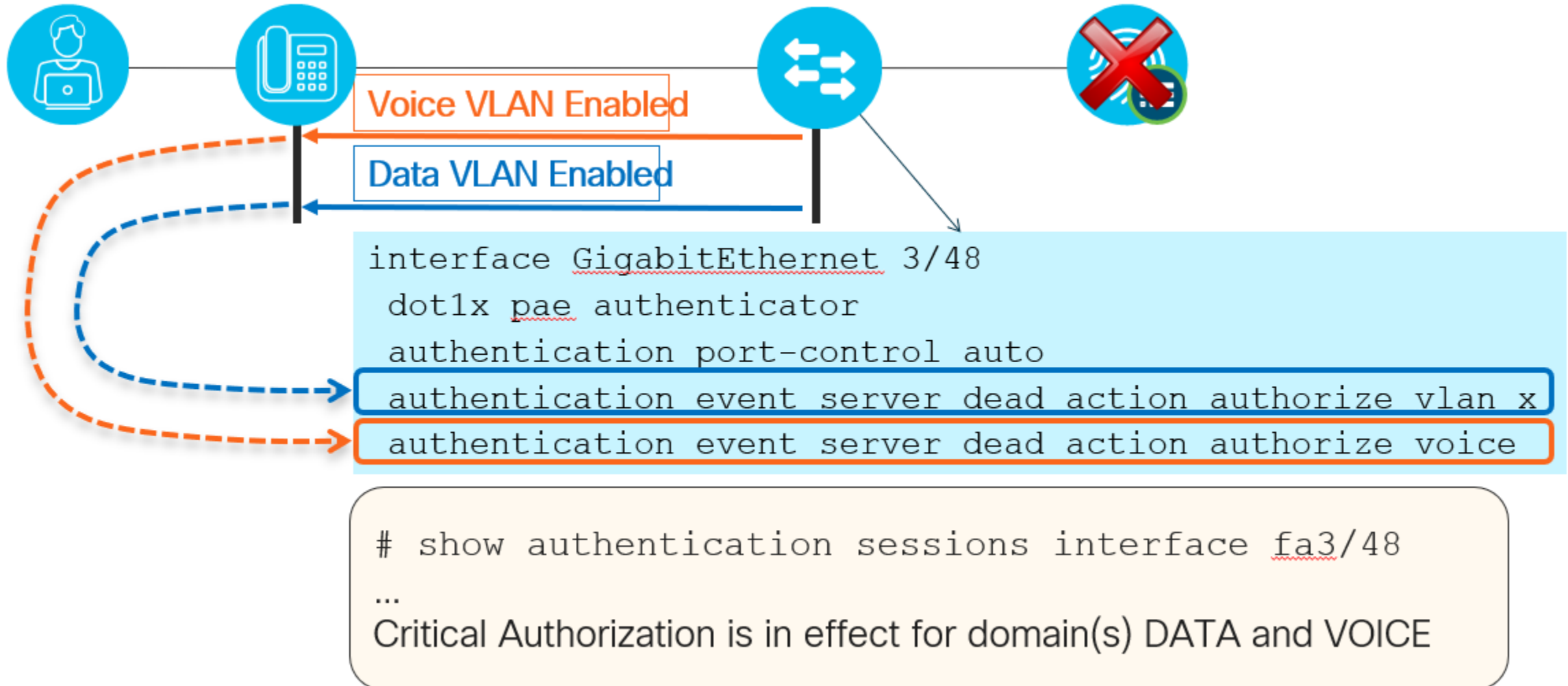
- Same as default access VLAN
- Same as guest/auth-fail VLAN
- New VLAN

```

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

Critical Voice VLAN

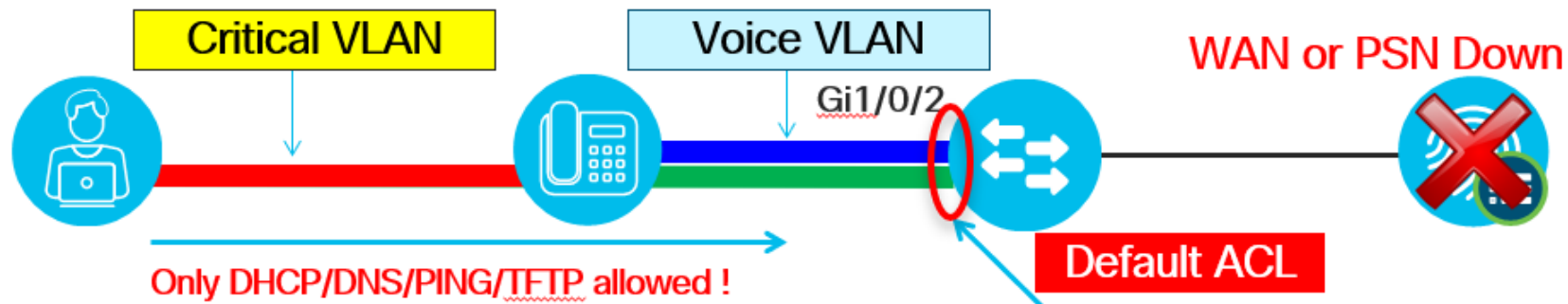
IBNS 1.0: Critical Auth for Data and Voice



IBNS 1.0: Default Port ACL Issues with Critical VLAN

Limited Access Even After Authorization to New VLAN

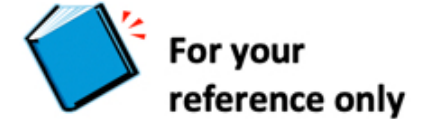
- Data VLAN reassigned to critical auth VLAN, but new (or reinitialized) connections are still restricted by existing port ACL



```
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

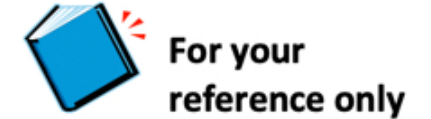


- Event: Session started
 - Attempt to authenticate using 802.1x until failure
- Event: Authentication failure
 - If AAA is complete down: Stop 802.1x and authorize the port
 - If no response from AAA (but not down yet), authorize to guest VLAN
 - If 802.1x authentication failure, authorize to guest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

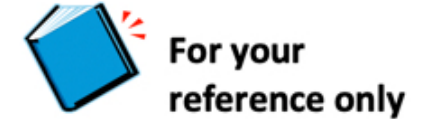
```
interface g1/0/1
dot1x pae authenticator
spanning-tree portface
switchport access vlan 100
switchport mode access
mab
access-session port-control auto
service-policy type control subscriber POLICY-A
```

```
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 portfast
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

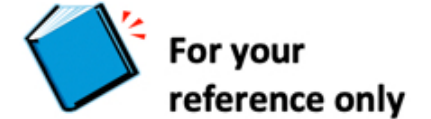
- Event: Session started
 - Attempt to authenticate using 802.1x until failure
- Event: Authentication failure
 - If AAA is down, do the following:
 - Authorize the port
 - Activate service-template CRITICAL which authorizes the voice VLAN
 - Terminate 802.1x authentication

```
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



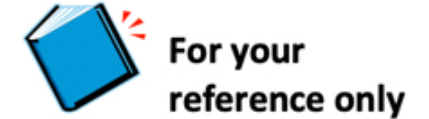
- Event: Session started
 - Attempt to authenticate using 802.1x until failure
- Event: Authentication failure
 - If AAA is down, do the following:
 - Authorize the port
 - Activate service-template CRITICAL which assigns SGT 10 to the endpoint
 - Terminate 802.1x authentication

```
interface g1/0/1
dot1x pae authenticator
spanning-tree portfast
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



- 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

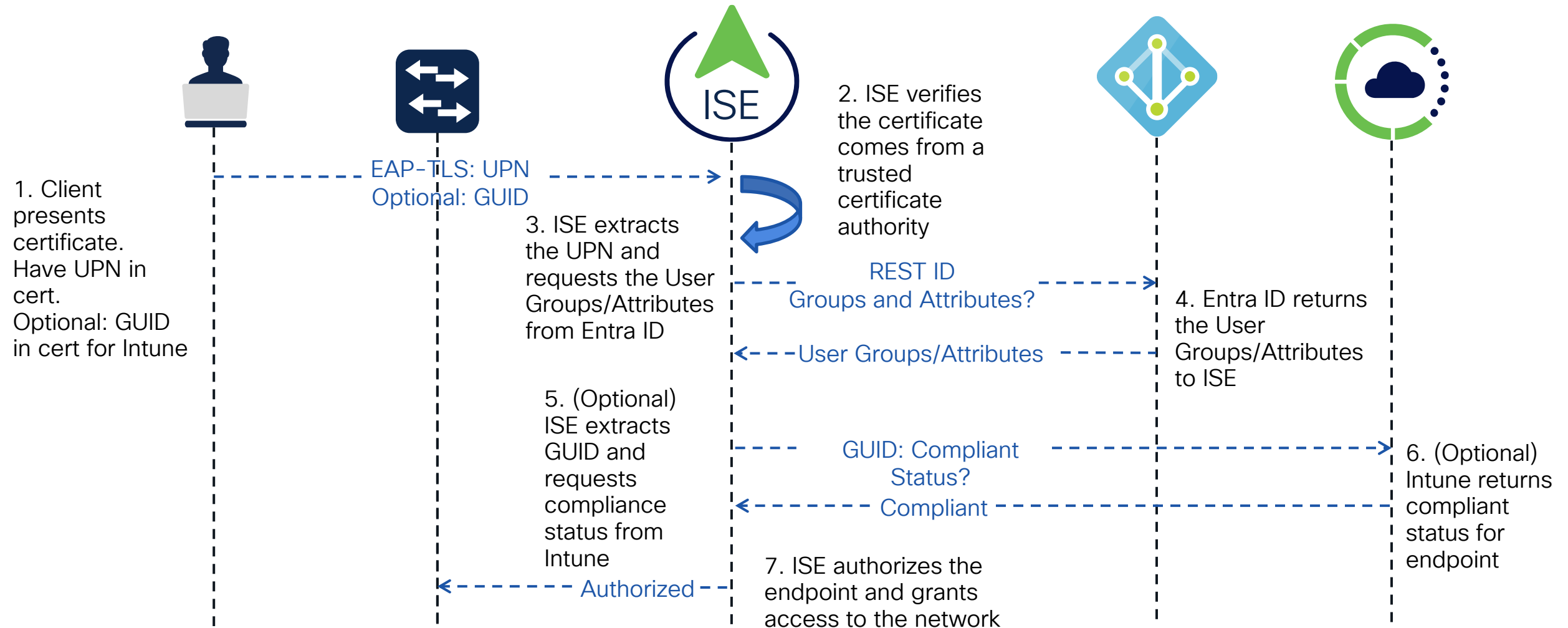
- Multiple authentication methods
 - 802.1x
 - Multiple 802.1X EAP methods simultaneously –
 - TEAP-EAP-TLS for Corporate Endpoints
 - EAP-TLS for supported printers and phones
 - PEAP-MSCHAPv2 for BYOD
 - Easy Connect
 - User authentication without 802.1x
 - Web Auth
 - MAB

Allowed Protocols

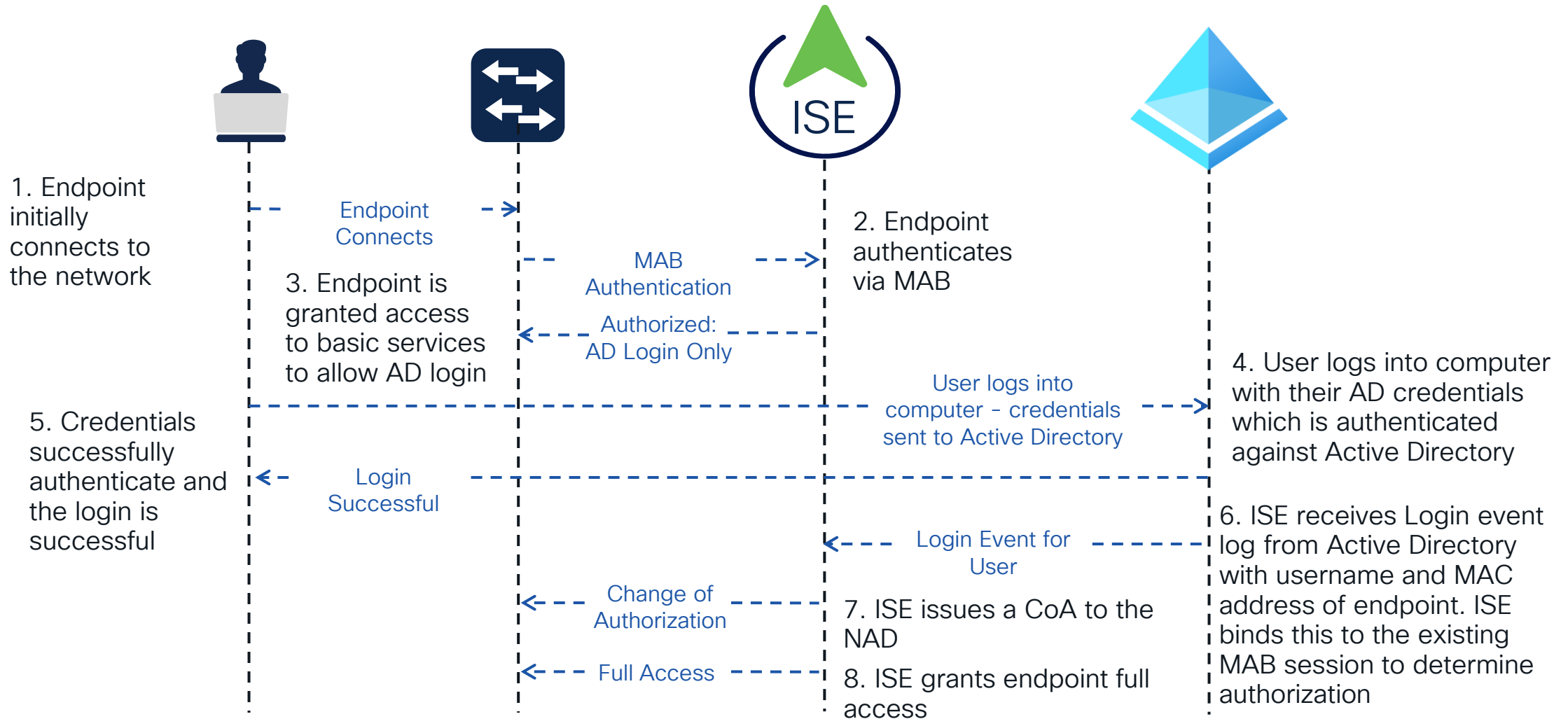
- ISE gives many options...
- Most common allowed protocols:
 - Process Host Lookup
 - EAP-TLS
 - PEAP-MSCHAPv2
 - PEAP-EAP-TLS
 - EAP-TEAP

Azure AD/Entra ID Support

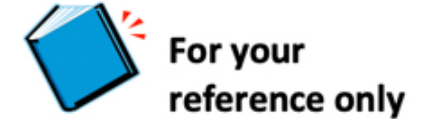
EAP-TTLS and EAP-TLS currently supported



Easy Connect



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
```

Migrate to 802.1x? Make it easier with Easy Connect!

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Wired Monitor Mode		AND DEVICE-Device Type EQUALS All Device Types#Switches DEVICE-Mode EQUALS Mode#Monitor	Default Network Access	0	⚙️	➔
✓	Wired Low-Impact Mode		AND DEVICE-Device Type EQUALS All Device Types#Switches DEVICE-Mode EQUALS Mode#Low-Impact	Default Network Access	0	⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

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

The screenshot displays the Cisco Identity Services Engine (ISE) dashboard. The top navigation bar includes the Cisco logo, the text "Identity Services Engine", and "Dashboard". The left sidebar contains a menu with items: Bookmarks, Dashboard (selected), Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area is titled "Summary" and features six large metric cards: Total Endpoints (0), Active Endpoints (0), Rejected Endpoints (0), Anomalous Behavior (0), Authenticated Guests (0), and BYOD Endpoints (0). Below these are six data tables, each with a "No data available." message and a large circular graphic: AUTHENTIFICATIONS, NETWORK DEVICES, ENDPOINTS, BYOD ENDPOINTS, ALARMS, and SYSTEM SUMMARY. The ALARMS table shows a single entry: Configuration Chang... with a severity of 7334 and a last occurrence of less than 1 min ... The SYSTEM SUMMARY table shows 1 node(s) and ISE.

Severity	Name	Occu...	Last Occurred
7334	Configuration Chang...	7334	less than 1 min ...

Type	Profile
------	---------

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

Posture Policy – Creating a Test Policy

The screenshot displays the Cisco Identity Services Engine (ISE) dashboard. The top navigation bar includes the Cisco logo, the text "Identity Services Engine", and "Dashboard". The left sidebar contains a menu with items: Bookmarks, Dashboard (selected), Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area is titled "Summary" and features six large metric cards: Total Endpoints (0), Active Endpoints (0), Rejected Endpoints (0), Anomalous Behavior (0), Authenticated Guests (0), and BYOD Endpoints (0). Below these are six data tables, each with a "No data available." message and a large circular graphic: AUTHENTIFICATIONS, NETWORK DEVICES, ENDPOINTS, BYOD ENDPOINTS, ALARMS, and SYSTEM SUMMARY. The ALARMS table shows a single entry: Configuration Chang... with a severity of 7354 and occurred 3 mins ago. The SYSTEM SUMMARY table shows "1 node(s)" and "ISE".

Identity Store	Identity Group	Network Device	Failure Reason
No data available.			

Device Name	Type	Location
No data available.		

Profile	Logical Profile
No data available.	

Type	Profile
No data available.	

Severity	Name	Occu...	Last Occurred
	Name		
	Configuration Chang...	7354	3 mins ago

SYSTEM SUMMARY	
1 node(s)	
ISE	

Tuning Policy Sets

The background features a light gray gradient. A prominent diagonal bar with a color gradient from red to blue is positioned in the upper right. A blue arc is visible in the bottom left corner.

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

Editor

Normalised Radius-SSID

Equals Corp-WiFi

AND

Wireless_802.1X

+ NEW AND OR

Set to 'Is not'

Duplicate Save

Policy Conditions

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

Editor

The screenshot shows a policy editor interface. On the left, a vertical sidebar contains a dropdown menu with 'OR' selected and highlighted by a red box. The main area displays two conditions: 'Wired_MAB' and 'Wired_802.1X', each with a list icon and a close button (X). Below the conditions is a dashed box containing a '+' sign and a menu with 'NEW', 'AND', and 'OR' options. At the bottom left, there is a link 'Set to 'Is not''. At the bottom right, there are 'Duplicate' and 'Save' buttons.

Policy Conditions

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

Editor

The screenshot shows the Cisco Policy Editor interface. The title bar reads 'EndPoints-EndPointPolicy'. The main configuration area contains two dropdown menus: 'Equals' and 'Apple-Device'. Below these is a 'Set to 'Is'' link. On the left side, there is a vertical menu with a 'No' symbol (a circle with a diagonal line) and an 'Is-Not' option, which is highlighted with a red box. On the right side, there are 'Duplicate' and 'Save' buttons. A close button (X) is in the top right corner.

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

OR

ad-2016-ExternalGroups

Equals dcloud.cisco.com/Builtin/Enterprise

AND

+ NEW

DEVICE:Location

Is-Not Equals All Locations#San Francisco

A little history lesson....

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
✓	Employee and CorpMachine	if (Network Access:EapChainingResult EQUALS User and machine both succeeded AND AD1:ExternalGroups EQUALS ise.local/Users/Employees)	then Employee Full Access
✓	Employee iDevices	if (EndPoints:LogicalProfile EQUALS iDevices AND AD1:ExternalGroups EQUALS ise.local/Users/Employees)	then Internet Only
✓	Employee Limited	if AD1:ExternalGroups EQUALS ise.local/Users/Employees	then Employee Limited
✓	Default	if no matches, then	PermitAccess

Save Reset

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 / Services
✓	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		AND • DEVICE-Location EQUALS Location#All Locations#Global#North America#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
✓	Dot1x-AzureAD		AND • DEVICE-Location EQUALS North America#USA#California#SJC01 • windows-dot1x-azure	• Default Network Access



Authentication Policy (3)

Status	Rule Name	Conditions	Use
✓	Dot1x_TLS	Network Access-EapAuthentication EQUALS EAP-TLS	
✓	Dot1x-TTLS	Network Access-EapTunnel EQUALS EAP-TTLS	• AzureAD > Options

Result: Credentials authenticated against Azure AD

Policy Set Flow

Authorization Policy (3)

				Results
+ Status	Rule Name	Conditions		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 Set – Option 1 Example

Policy Sets

Reset

Reset Polycyset Hit















+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
<input type="text" value="Search"/>					
✓	San Francisco Wired Access		AND	<ul style="list-style-type: none"> DEVICE-Device Type EQUALS All Device Types#Switches DEVICE-Location EQUALS All Locations#San Francisco 	Default Network Access ✎ +
✓	San Jose Wired Access		AND	<ul style="list-style-type: none"> DEVICE-Device Type EQUALS All Device Types#Switches DEVICE-Location EQUALS All Locations#San Jose 	Default Network Access ✎ +
✓	Guest SSID		AND	<ul style="list-style-type: none"> DEVICE-Device Type EQUALS All Device Types#Wireless Controllers Radius-Called-Station-ID CONTAINS Corp-Guest 	Default Network Access ✎ +
✓	Corp 802.1x		AND	<ul style="list-style-type: none"> DEVICE-Device Type EQUALS All Device Types#Wireless Controllers Radius-Called-Station-ID CONTAINS Corp-Dot1x 	Default Network Access ✎ +
✓	VPN			<ul style="list-style-type: none"> DEVICE-Device Type EQUALS All Device Types#VPN 	Default Network Access ✎ +

Policy Set – Option 2 Example

Policy Sets

Reset

Reset Policyset Hit

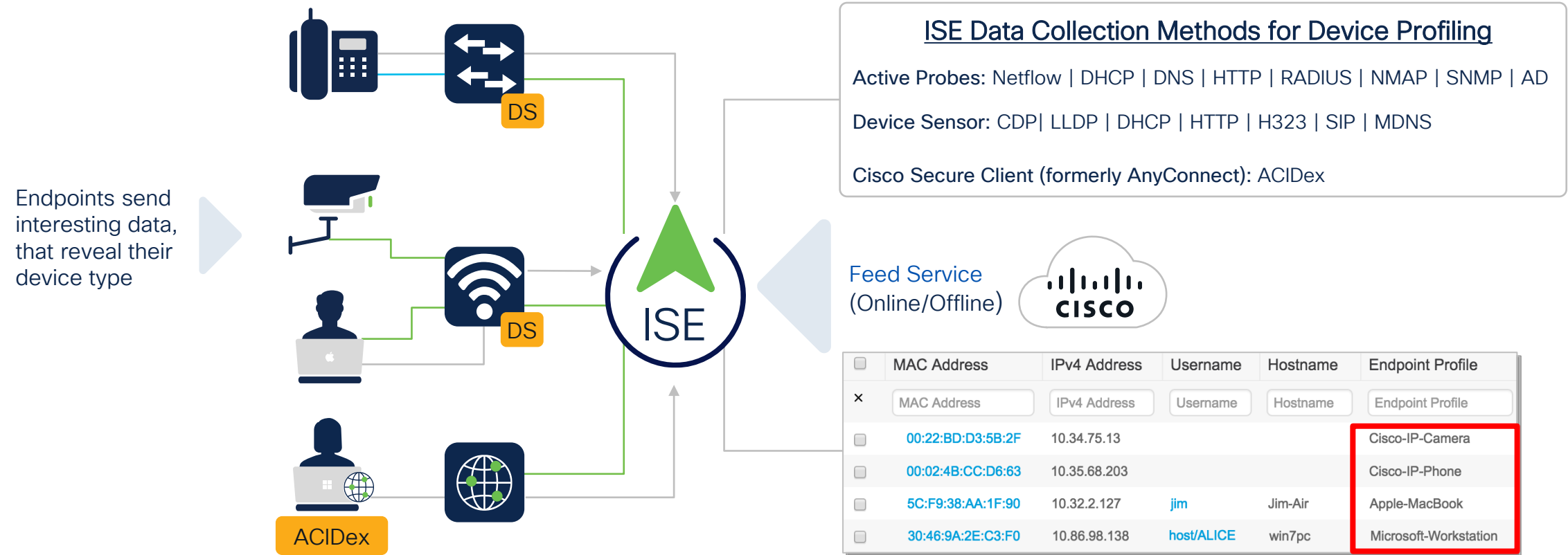
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
✓	San Francisco Wired 802.1		AND <ul style="list-style-type: none"> DEVICE-Location EQUALS All Locations#San Francisco Wired_802.1X 	Default Network Access  
✓	San Francisco Wired MAB		AND <ul style="list-style-type: none"> DEVICE-Location EQUALS All Locations#San Francisco Wired_MAB 	Default Network Access  
✓	San Jose Wired 802.1X		AND <ul style="list-style-type: none"> DEVICE-Location EQUALS All Locations#San Jose Wired_802.1X 	Default Network Access  
✓	San Jose Wired MAB		AND <ul style="list-style-type: none"> DEVICE-Location EQUALS All Locations#San Jose Wired_MAB 	Default Network Access  
✓	Guest SSID		AND <ul style="list-style-type: none"> DEVICE-Device Type EQUALS All Device Types#Wireless Controllers Radius-Called-Station-ID CONTAINS Corp-Guest 	Default Network Access  
✓	Corp 802.1x		AND <ul style="list-style-type: none"> 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 background features a light gray gradient. A prominent diagonal bar with a color gradient from red to blue is positioned in the upper right. A blue arc is visible in the bottom left corner.

The Power of Profiling

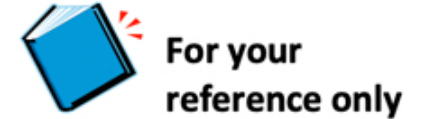
Endpoint Profiling – Visibility Data Sources

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



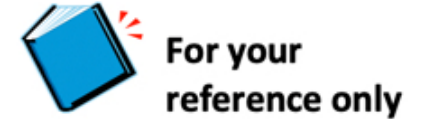
Cisco Secure Client Identity Extensions (ACIDex) | Device Sensor (DS)

ISE Profiling Probes



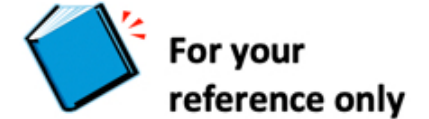
- **RADIUS**
 - **Collects session attributes as well as CDP, LLDP, DCHP, HTTP, and MDM from IOS Device Sensor**
- **SNMP Query and Traps**
 - Collects information such as interface, CDP, LLDP, ARP, Linkup, Lidown, and MAC notifications
- **DHCP**
 - **Listens for DHCP Packets**
- **DNS**
 - **Performs 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

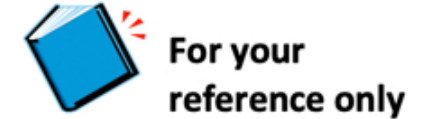
RADIUS Probe Sample Configuration



```
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
```

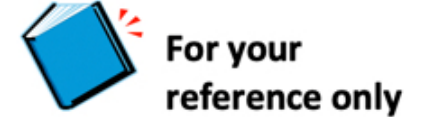
SNMP Probe Sample Configuration



```
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
```

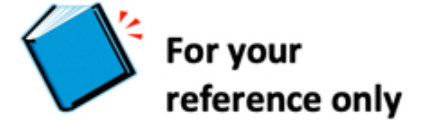
```
ip access-list extended REDIRECT-ACL
```

```
deny ip any host <ISE-PSN-IP>
```

```
permit tcp any any eq http
```

```
permit tcp any any eq https
```

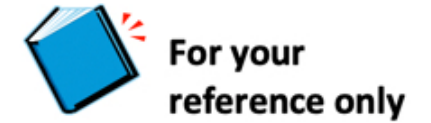
DHCP Probe Sample Configuration



```
interface vlan 30
```

```
ip helper-address <PSN-IP-Address>
```

Device Sensor for Wired



- 1) Filter DHCP, CDP, and LLDP options/TLVs
- 2) Enable sensor data to be sent in RADIUS Accounting including all changes

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

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


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

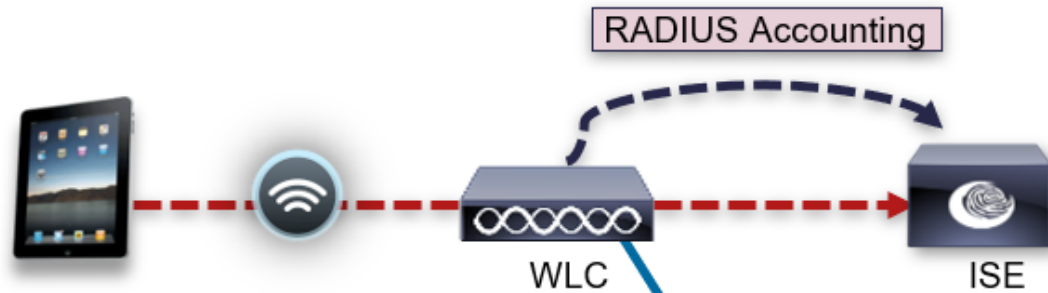
```
device-sensor filter-list cdp list my_cdp_list
tlv name device-name
tlv name platform-type
device-sensor filter-spec cdp include list my_cdp_list
```

```
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
```

```
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

 For your reference only



▼ RADIUS

Description

The screenshot shows the 'WLANs > Edit 'BYOD-Profiling'' configuration page. The 'Advanced' tab is selected, showing various settings. A blue box highlights the 'Client Profiling' section, which includes 'DHCP Profiling' and 'HTTP Profiling', both of which are checked.

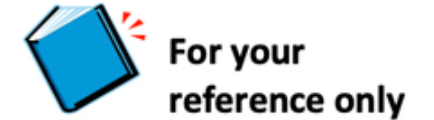
Client Profiling

DHCP Profiling

HTTP Profiling

- 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

Edit Policy Profile

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name BlockPolicy x ▼

Enabling Probes on ISE

The screenshot displays the Cisco Identity Services Engine (ISE) dashboard. At the top, the browser address bar shows the URL `https://198.18.133.27/admin/#/home`. The dashboard header includes the Cisco logo, the text "Identity Services Engine", and the word "Dashboard". A navigation menu below the header lists "Summary", "Endpoints", "Guests", "Vulnerability", and "Threat".

The main content area features a row of six summary cards, each displaying a large blue "0" and a refresh icon:

- Total Endpoints
- Active Endpoints
- Rejected Endpoints
- Anomalous Behavior
- Authenticated Guests
- BYOD Endpoints

Below these cards are three data tables, each with a "No data available." message and a large grey circle:

- AUTHENTICATIONS**: Columns include Identity Store, Identity Group, Network Device, and Failure Reason.
- NETWORK DEVICES**: Columns include Device Name, Type, and Location.
- ENDPOINTS**: Columns include Profile and Logical Profile.

At the bottom of the dashboard, there are three more sections:

- BYOD ENDPOINTS**: Columns include Type and Profile.
- ALARMS**: A table with columns for Severity, Name, Occu..., and Last Occurred.
- SYSTEM SUMMARY**: Shows "1 node(s)" and "ISE".

Profiling Logic

Profiler Policy

* Name Apple-Device Description

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

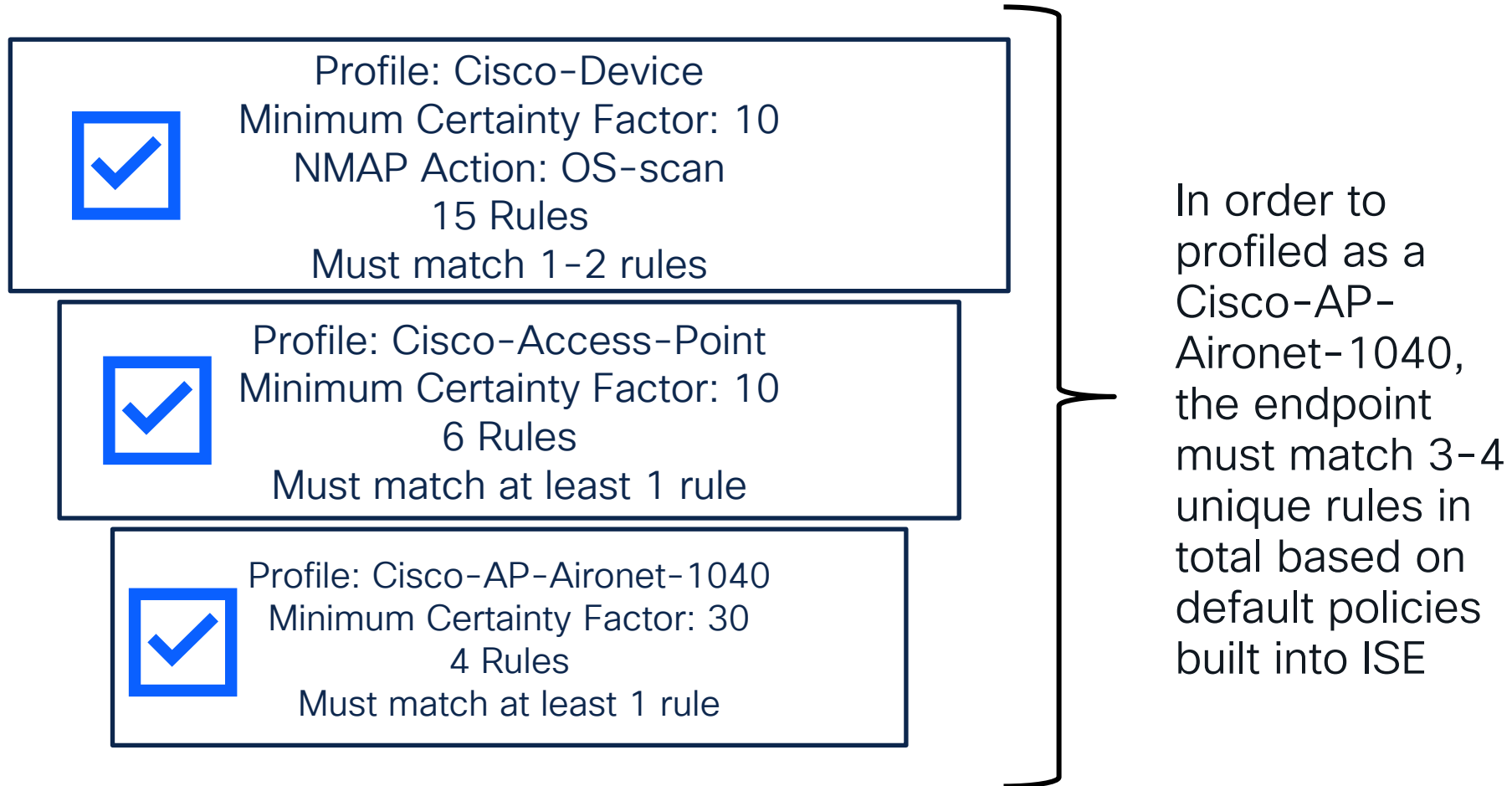
Parent Policy *****NONE*****

* Associated CoA Type Global Settings ▾

System Type Cisco Provided

Rules						
If	Condition	<u>Apple-iPadRule4Check1</u>	▾	Then	<u>Certainty Factor Increases</u>	▾ 10
If	Condition	<u>Apple-DeviceRule3check1</u>	▾	Then	<u>Certainty Factor Increases</u>	▾ 180
If	Condition	<u>Apple-iPhoneRule3Check1</u>	▾	Then	<u>Certainty Factor Increases</u>	▾ 10
If	Condition	<u>Apple-DeviceRule4check1</u>	▾	Then	<u>Certainty Factor Increases</u>	▾ 180
If	Condition	<u>Apple-DeviceRule1Check1</u>	▾	Then	<u>Certainty Factor Increases</u>	▾ 10
If	Condition	<u>Apple-iPadRule1Check1</u>	▾	Then	<u>Certainty Factor Increases</u>	▾ 100
If	Condition	<u>Apple-iPhoneRule1Check1</u>	▾	Then	<u>Certainty Factor Increases</u>	▾ 100
If	Condition	<u>Apple-DeviceRule1-SCAN</u>	▾	Then	<u>Take Network Scan Action</u>	▾

Profile Hierarchy



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

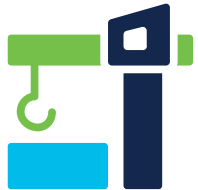


Siemens-Device
Siemens-Automation-Drives-Device
Siemens-Building-Device
Siemens-Building-Technologies-Device
Siemens-Convergence-Device
Siemens-Digital-Factory-Device
Siemens-Energy-Automation-Device
Siemens-Energy-Management-Device
Siemens-Home-Office-Device
Siemens-Industrial-Automation-Device



pxGrid

pxGrid



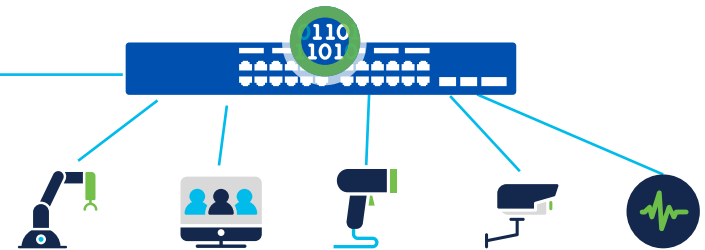
Factory



Industrial Devices



Cisco CyberVision



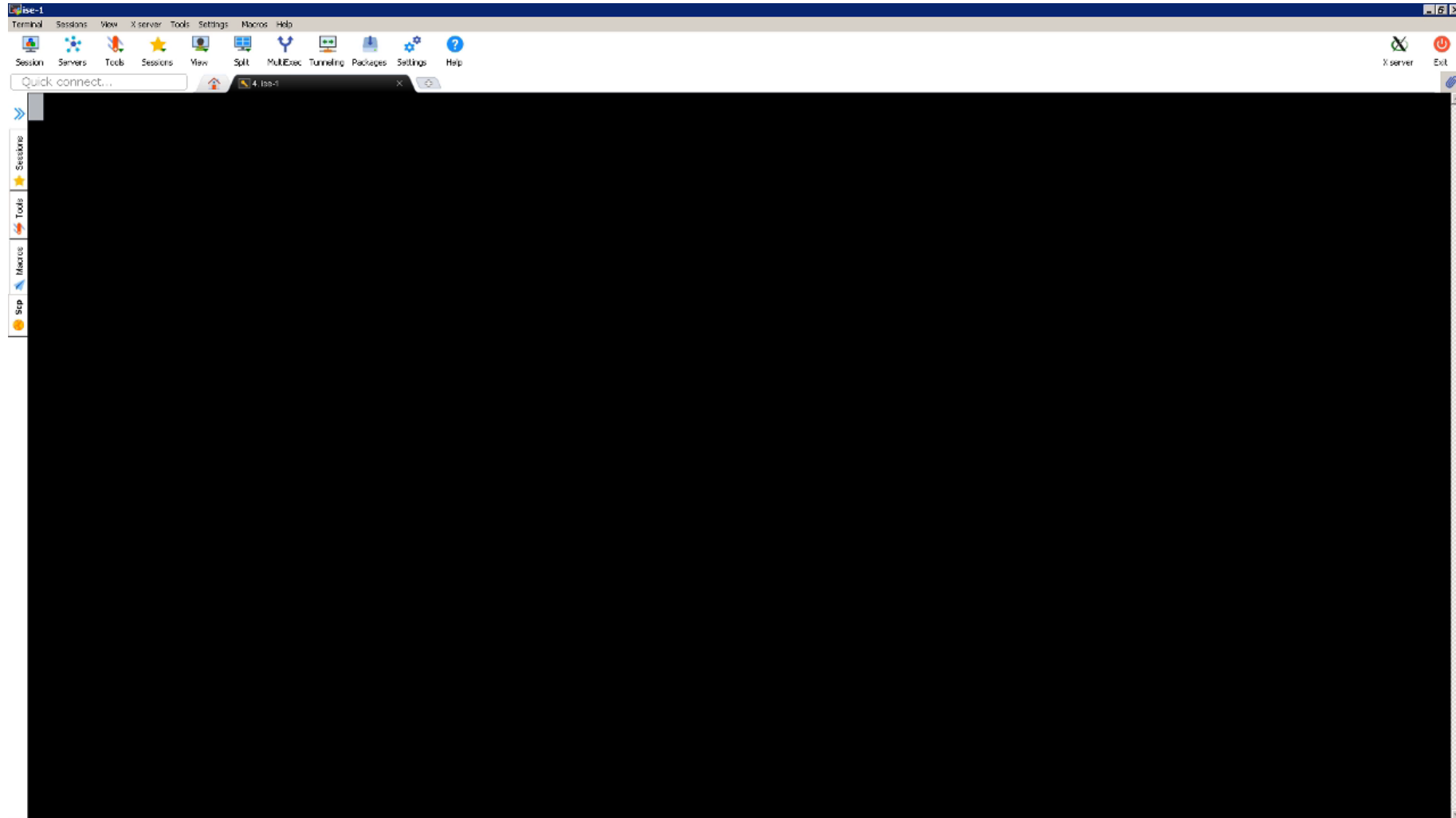
Cisco AI Endpoint Analytics

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

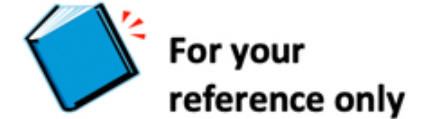


Creating Custom Hierarchical Profiles

The screenshot shows an Excel spreadsheet with the following data:

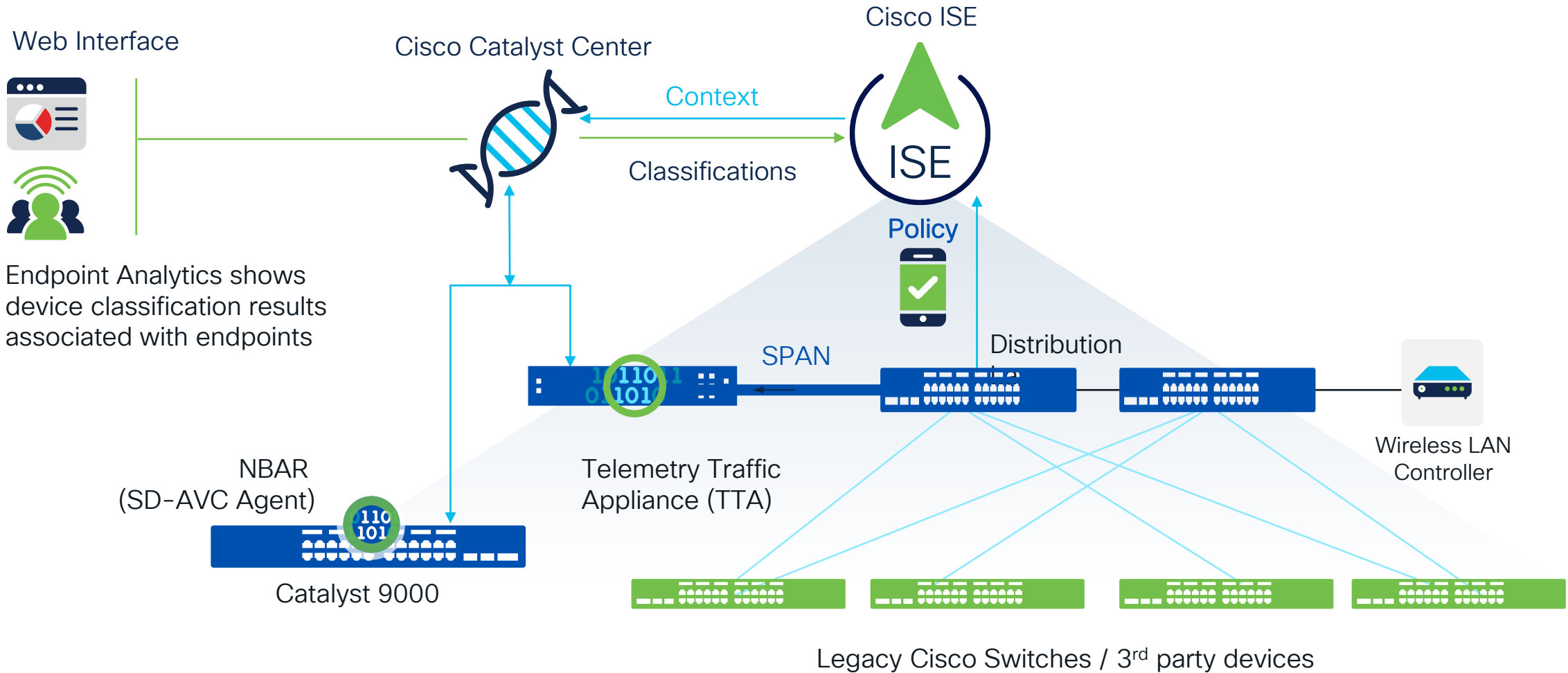
host-name	MatchedPolicy	OUI	sysContact	sysLocation	sysName	hrDeviceDescr	sysDescr	9100-
	HP-LaserJet-Printer	Hewlett Packard				HP LaserJet 400 MFP M425dn	HP ETHERNET MULTI-ENVIRONMENT,PID:HP LaserJet 400 MFP M425dn	jetdirect
	HP-LaserJet-Printer	Hewlett Packard				HP LaserJet 400 MFP M425dn	HP ETHERNET MULTI-ENVIRONMENT,PID:HP LaserJet 400 MFP M425dn	jetdirect
lw*print*server	Unknown	KCodes Corporation	Visit www.dymo.com or call 203-588-2500	www.dymo.com	LabelWriter Print Server		ucd-snmp-4.1.2/Red Hat eCos	jetdirect
lw*print*server	Unknown	KCodes Corporation	Visit www.dymo.com or call 203-588-2500	www.dymo.com	LabelWriter Print Server		ucd-snmp-4.1.2/Red Hat eCos	jetdirect

Profiling Attributes

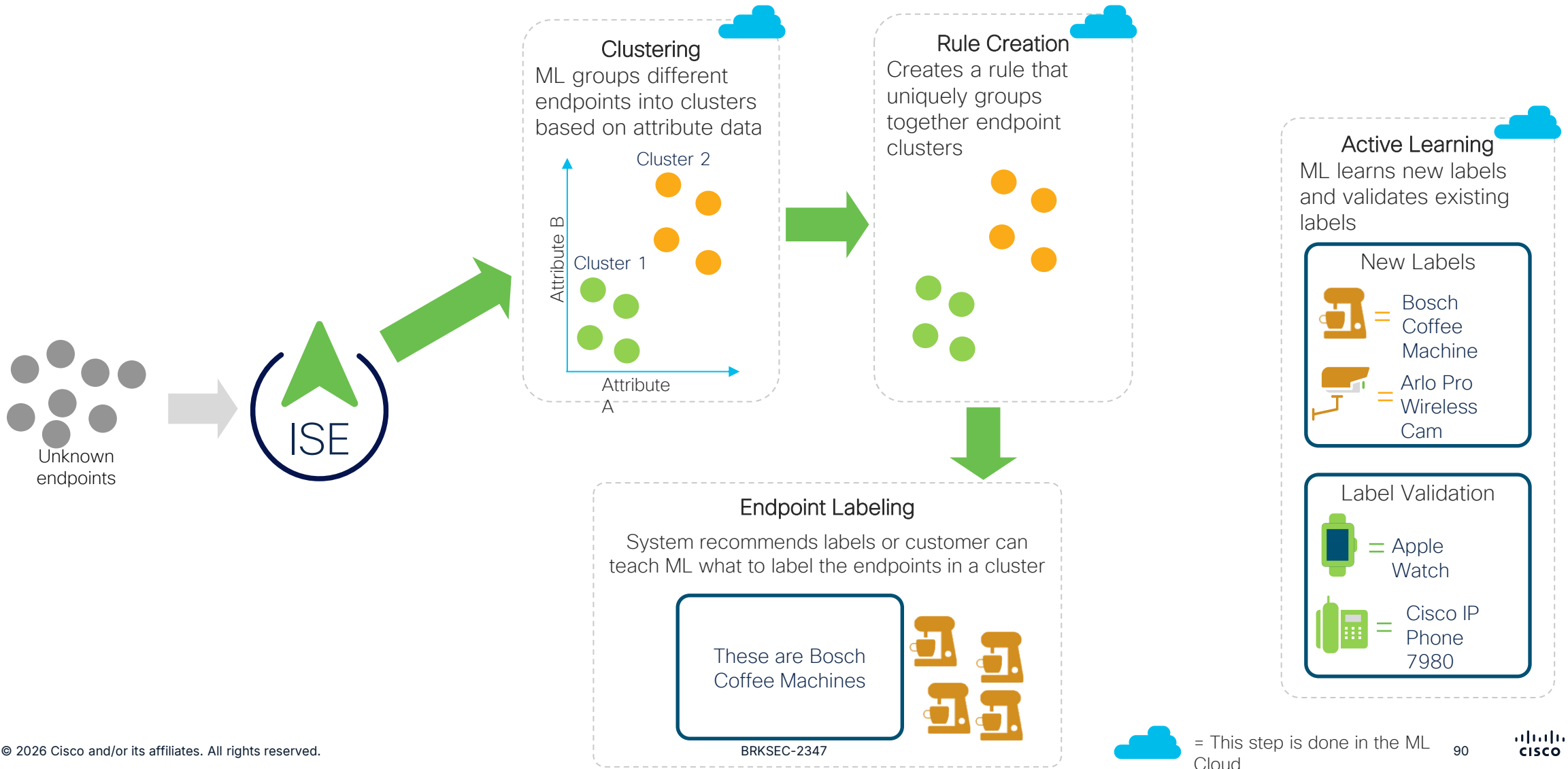


- OUI
- FQDN
- DHCP client-identifier
- DHCP class-identifier
- DHCP parameter-request-list
- DHCP host-name
- AD host-exists
- AD operating-system
- HTTP User-Agent
- CDP Cache Platform
- CDP System Name
- LLDP System Name
- LLDP System Description
- SNMP information

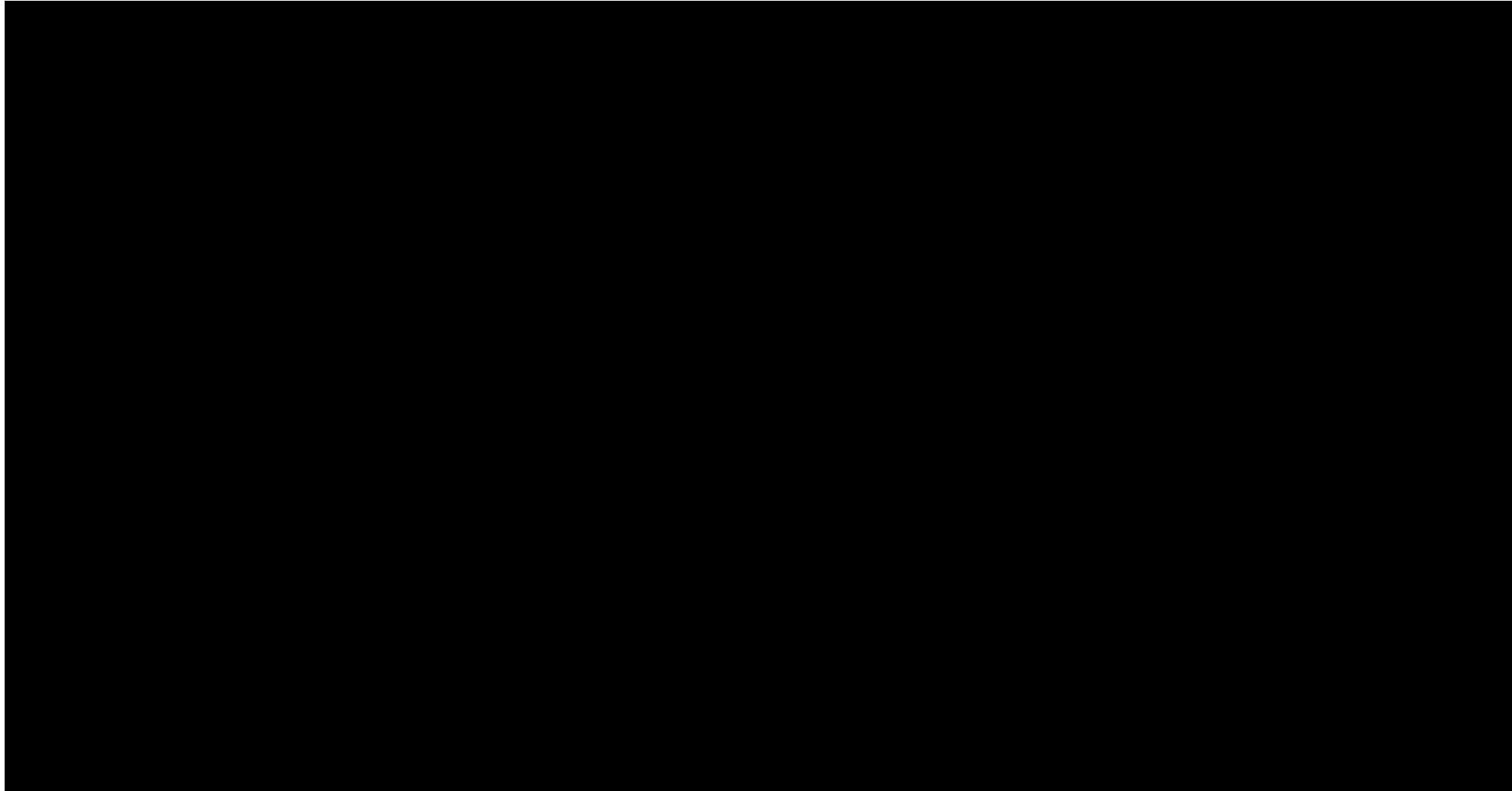
Cisco AI Analytics



Cisco AI Endpoint Analytics



AI Endpoint Analytics on ISE



Integrations

The background features a light gray gradient. A diagonal bar with a color gradient from red to blue is positioned in the upper right. A blue circular arc is visible in the lower left corner.

Platform Exchange Grid (pxGrid)

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



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 its identity (pxGrid) certificate

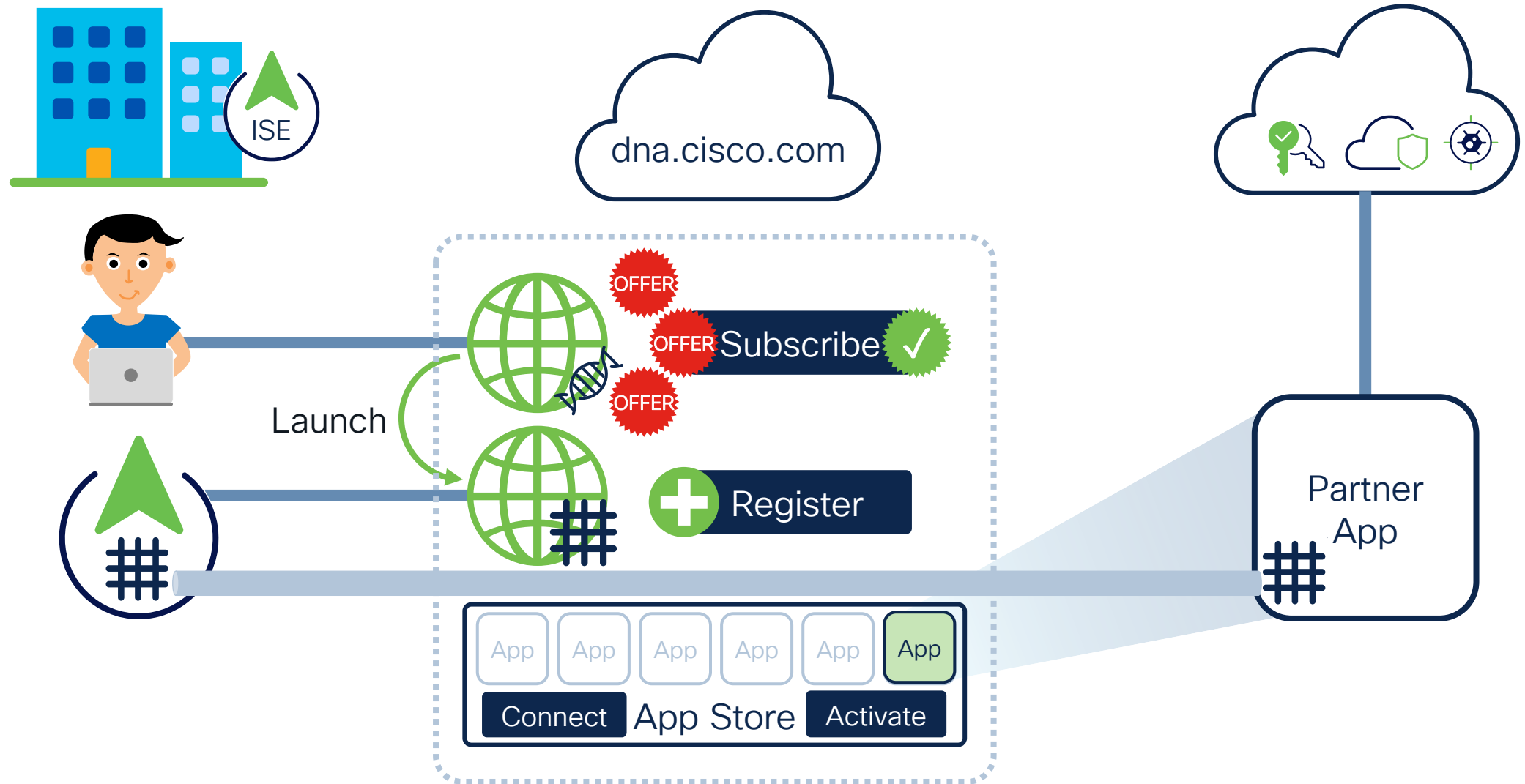


4. ISE will authenticate itself back to the client with its own pxGrid certificate

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



Context Sharing with pxGrid

Eco system partnership to enrich, exchange context and enact

Context to Partner



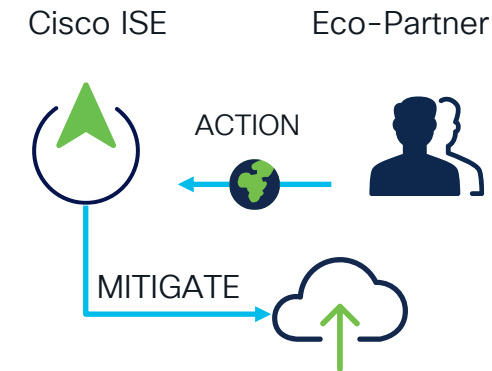
ISE makes Customer IT Platforms User/Identity, Device and Network Aware

Enrich ISE Context



Enrich ISE context. Make ISE a better Policy Enforcement Platform

Threat Mitigation



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

Context Brokerage



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

pxGrid/ANC Policies in ISE

The screenshot displays the Cisco Identity Services Engine (ISE) dashboard. The top navigation bar includes the Cisco logo, "Identity Services Engine", and "Dashboard". The main content area is divided into several sections:

- Summary:** A row of six cards showing metrics: Total Endpoints (0), Active Endpoints (0), Rejected Endpoints (0), Anomalous Behavior (0), Authenticated Guests (0), and BYOD Endpoints (0). Each card has a refresh icon and a "Compl" link.
- Authentication Section:** A card titled "AUTHENTIFICATIONS" with sub-tabs for Identity Store, Identity Group, Network Device, and Failure Reason. It displays "No data available." with a large circular graphic.
- Network Devices Section:** A card titled "NETWORK DEVICES" with sub-tabs for Device Name, Type, and Location. It displays "No data available." with a large circular graphic.
- Endpoints Section:** A card titled "ENDPOINTS" with sub-tabs for Profile and Logical Profile. It displays "No data available." with a large circular graphic.
- BYOD Endpoints Section:** A card titled "BYOD ENDPOINTS" with sub-tabs for Type and Profile. It displays "No data available." with a large circular graphic.
- Alarms Section:** A card titled "ALARMS" with a table showing Severity, Name, Occu..., and Last Occurred. The table has a dropdown menu for Name.
- System Summary Section:** A card titled "SYSTEM SUMMARY" showing "1 node(s)" and "ISE" with filters for "All" and "24HR".

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...

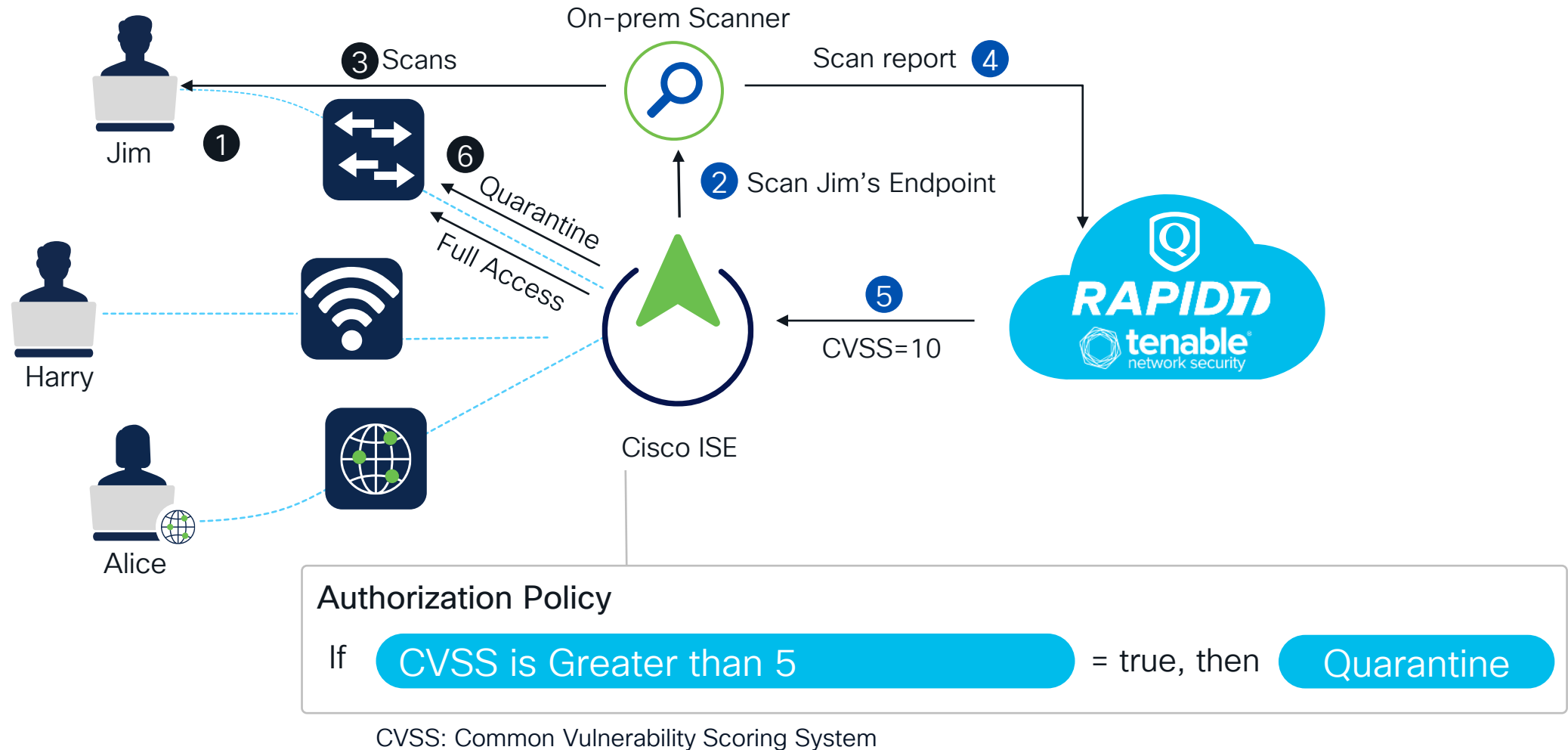
pxGrid Integration Tips

- 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



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

The screenshot displays the Cisco Identity Services Engine (ISE) Dashboard. The top navigation bar includes the Cisco logo, the text "Identity Services Engine", and "Dashboard". On the right side of the navigation bar are icons for search, notifications, help, and user profile.

Below the navigation bar is a secondary menu with tabs for "Summary", "Endpoints", "Guests", "Vulnerability", and "Threat". A "Manage" dropdown menu is visible on the right.

The main content area features a row of six summary cards, each with a title and a large blue "0" value:

- Total Endpoints
- Active Endpoints
- Rejected Endpoints
- Anomalous Behavior
- Authenticated Guests
- BYOD Endpoints

Below these cards are six data panels, each with a title and a table:

- AUTHENTICATIONS**: Table with columns "Identity Store", "Identity Group", "Network Device", and "Failure Reason". Content: "No data available."
- NETWORK DEVICES**: Table with columns "Device Name", "Type", and "Location". Content: "No data available."
- ENDPOINTS**: Table with columns "Profile" and "Logical Profile". Content: "No data available."
- BYOD ENDPOINTS**: Table with columns "Type" and "Profile". Content: "No data available."
- ALARMS**: Table with columns "Severity", "Name", "Occu...", and "Last Occurred".

Severity	Name	Occu...	Last Occurred
	Configuration Chang...	7259	2 mins ago
- SYSTEM SUMMARY**: Shows "1 node(s)" and "ISE". Includes filters for "All" and "24HR".

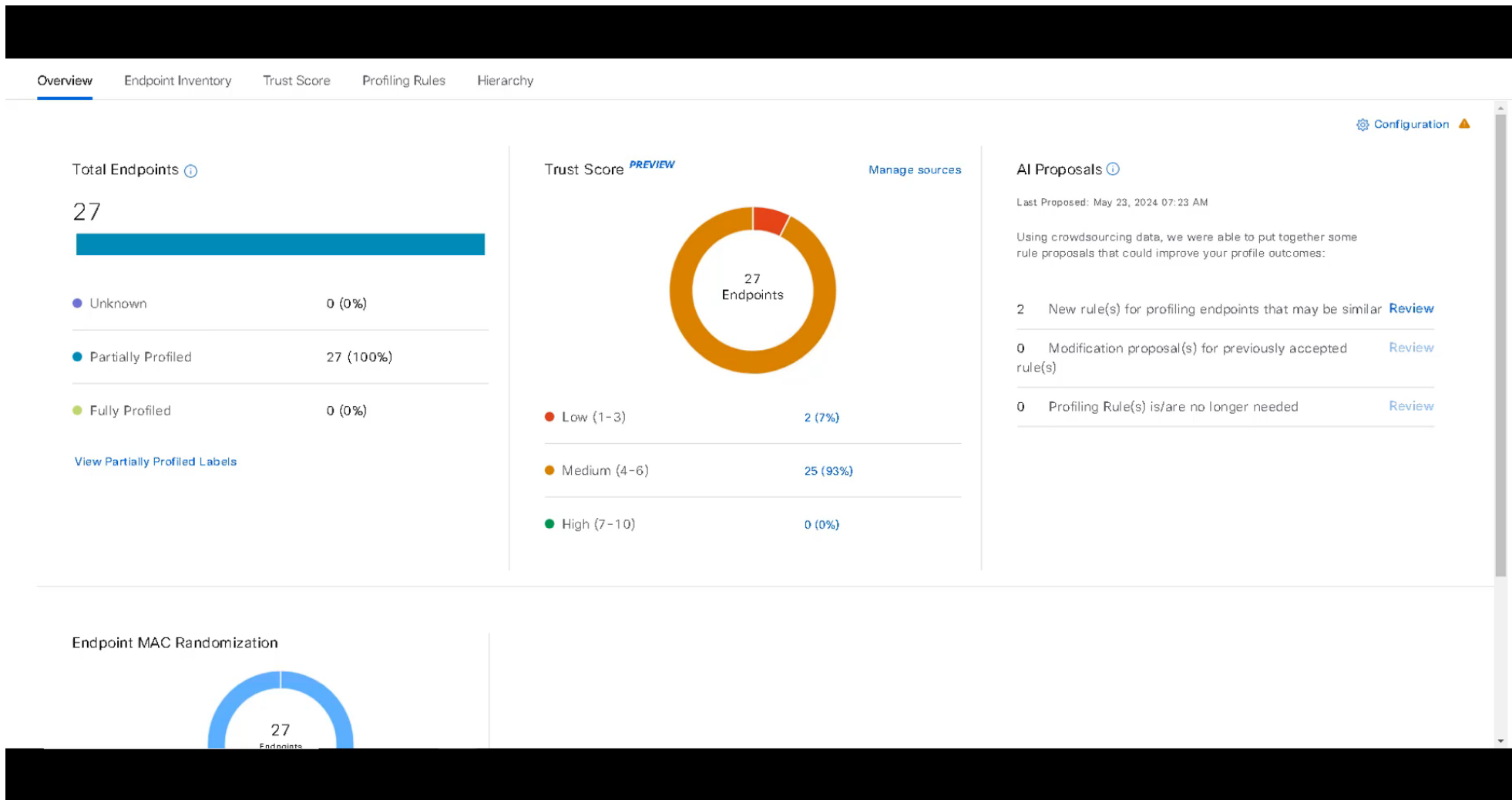
ISE APIs and Automation



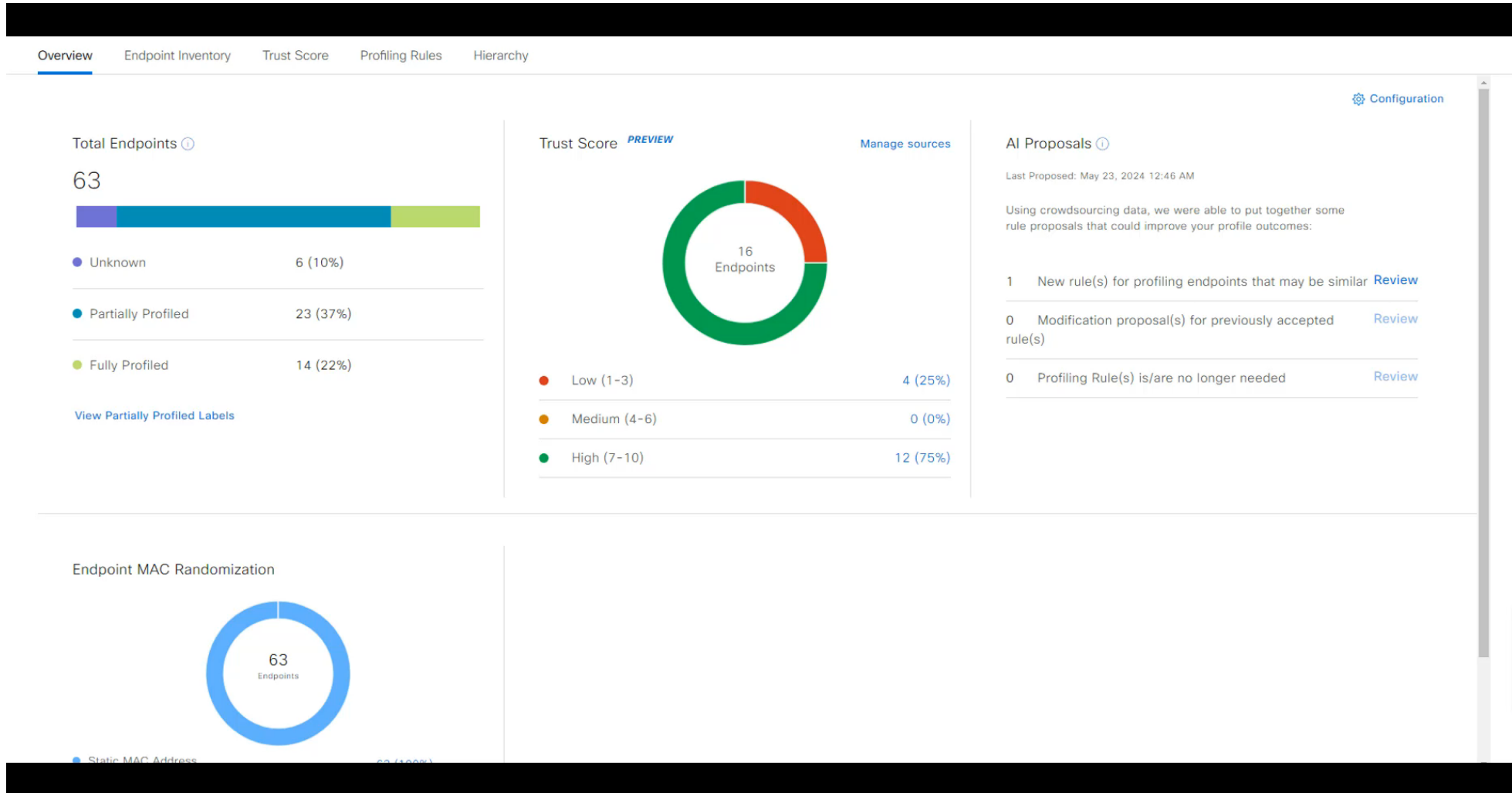
Integration Example: Catalyst Center and ISE

- 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

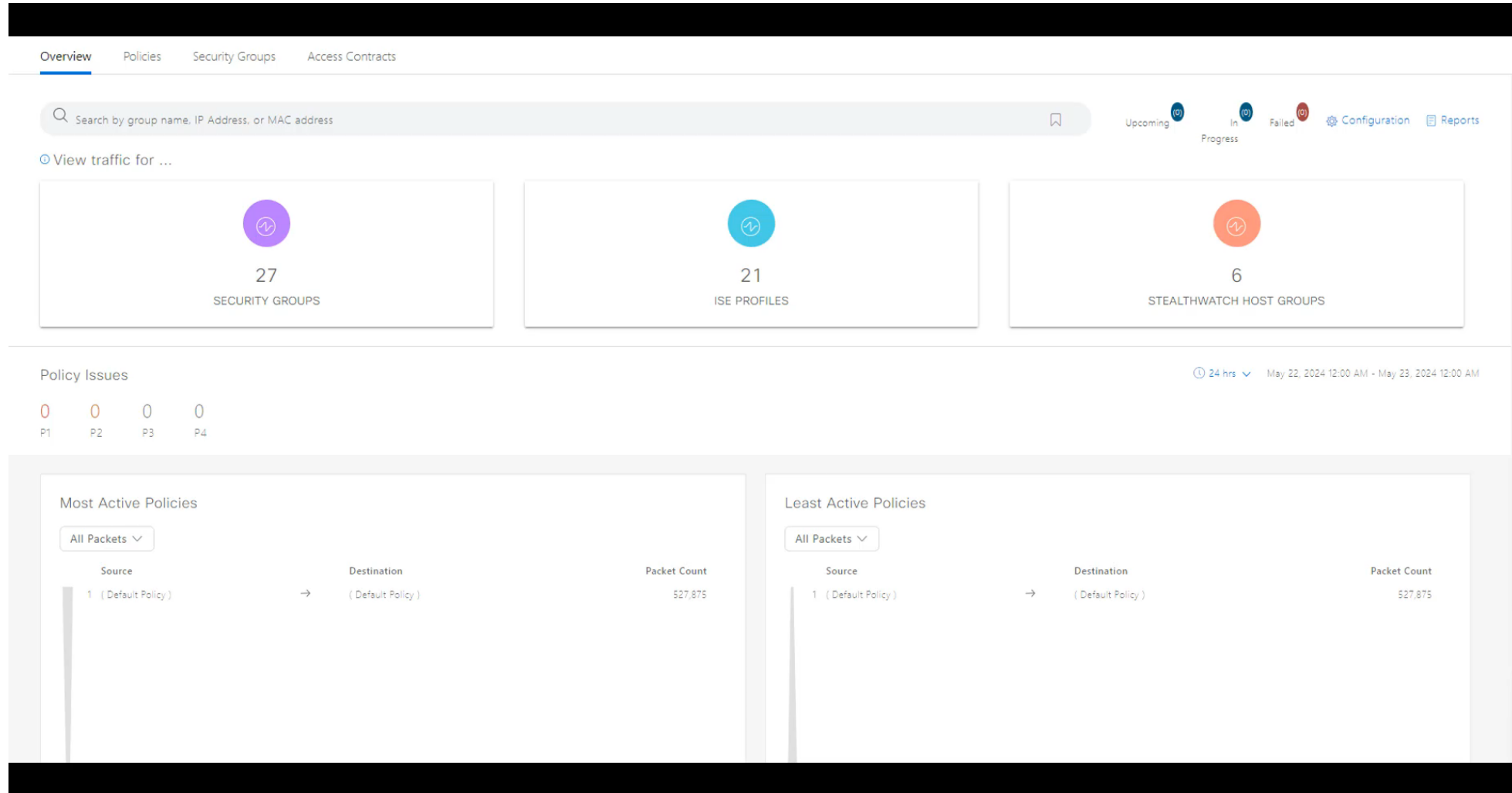
Catalyst Center Trust Score and Spoofing Detection



Catalyst Center AI Endpoint Telemetry



TrustSec Policies with Catalyst Center Integration



Post-Deployment

The background features a white tilted rectangle in the upper right quadrant, containing a smooth gradient from red to blue. A blue arc is visible at the bottom left corner of the image.

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

Troubleshooting 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



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



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:

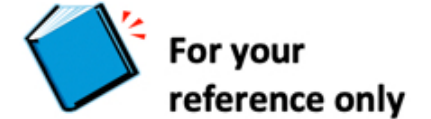
- **debug cts sxp connection**
- **debug cts sxp errors**
- **debug cts sxp all**
- **debug cts sxp**
- **debug cts sxp internal**

- **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



- CoA:
 - **debug cts coa event**
 - **debug aaa coa**
 - **debug radius dynamic-authorization**
- NX-OS Specific:
 - **show tech-support cts**
 - **show tech-support forward I3 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

Identity Services Engine Operations / RADIUS

Live Logs Live Sessions

Misconfigured Supplicants Repeat Counter

1 0 1064 0 2423096

Refresh: Never | Show: Latest 50 records | Within: Last 24 hours

Reset Repeat Counts | Export To | Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Aut
May, 25 2024 07:37:14.3...	✓			Grace.Smith	A8:8E:27:36:70:11	Mobile Devices	MDM >> User Dot1x	MDM >> MDM-Intune-Compliant	Emp
May, 25 2024 07:37:14.3...	✓			Grace.Smith	B8:27:EB:CA:AA:88	Microsoft-Workstation	Corporate Posture >> Corporate Dot1x	Corporate Posture >> Employees Compliant	Emp
May, 25 2024 07:37:14.3...	✓				B8:27:EB:CA:AA:88				
May, 25 2024 07:37:14.3...	✓			Grace.Smith	B8:27:EB:CA:AA:88	Microsoft-Workstation	Corporate Posture >> Corporate Dot1x	Corporate Posture >> Employees Posture Unknown	Post
May, 25 2024 07:37:14.3...	✓			Grace.Smith	6C:7E:67:D7:68:E9	Windows-Laptop	Employee Access >> Dot1x_TTLS	Employee Access >> Employees-Access	Emp
May, 25 2024 07:37:14.3...	✓			Michael.Chang	00:50:56:8E:90:DE	Windows10-Workstation	Remote Access VPN >> Default	Remote Access VPN >> Contractor-Access	VPN
May, 25 2024 07:37:14.3...	✓			guest	00:50:56:8E:E3:B3	Windows-Laptop	MAC Based Authentication	MAC Based Authentication >> Guest Access	GUE
May, 25 2024 07:37:14.3...	✓				00:50:56:8E:E3:B3				
May, 25 2024 07:37:14.3...	✓			guest	00:50:56:8E:E3:B3				
May, 25 2024 07:37:14.3...	✓			00:50:56:8E:E3...	00:50:56:8E:E3:B3		MAC Based Authentication >> Default	MAC Based Authentication >> Guest Redirect	GUE
May, 25 2024 07:37:14.3...	✓			A8:46:9D:2F:2...	A8:46:9D:2F:2B:3F	Cisco-Meraki-Device	MAC Based Authentication >> Default	MAC Based Authentication >> IoT_Camera	CAN

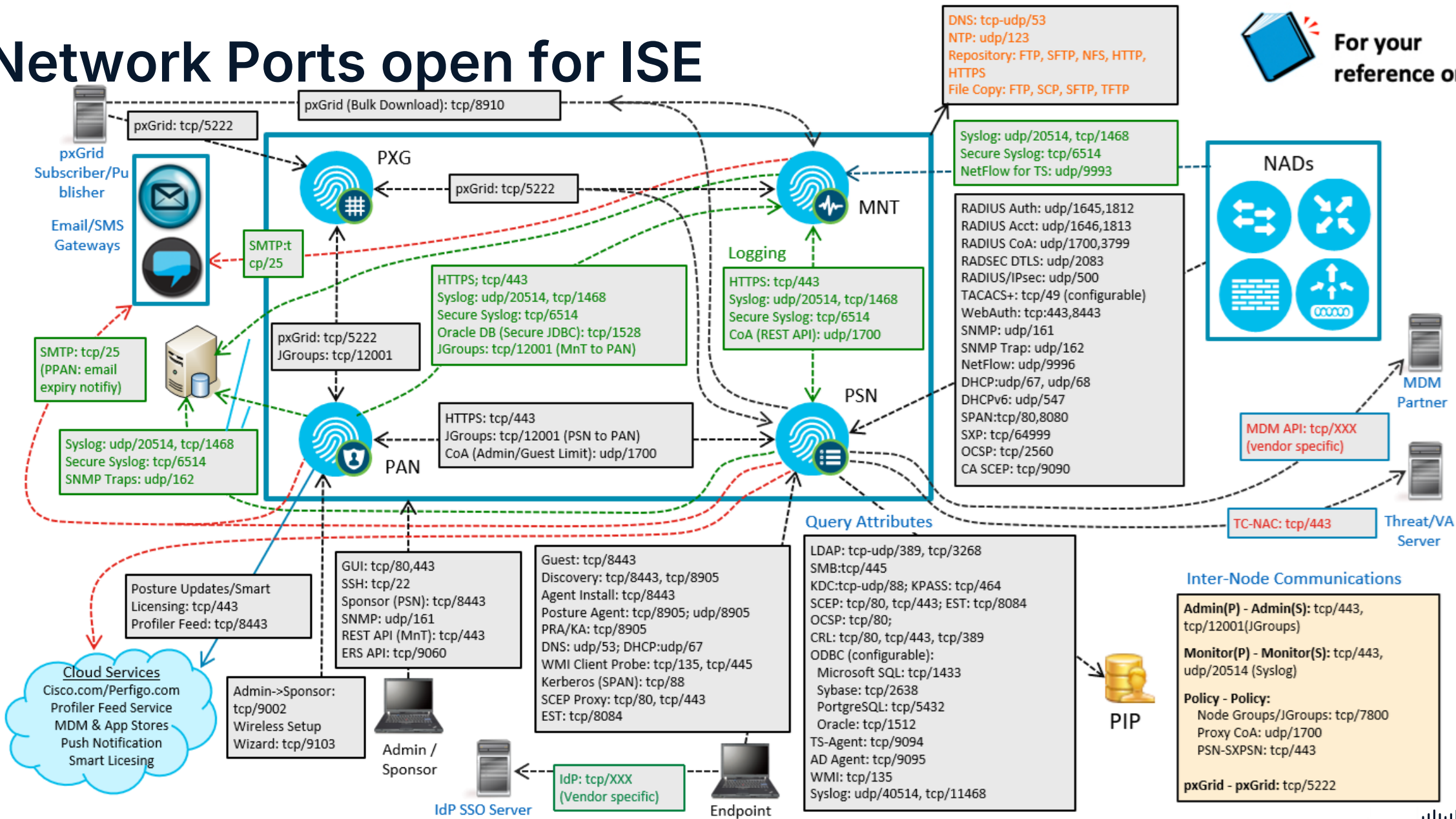
Last Updated: Sun May 26 2024 16:37:14 GMT-0700 (Pacific Daylight Time) Records Shown: 11

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

 For your reference only

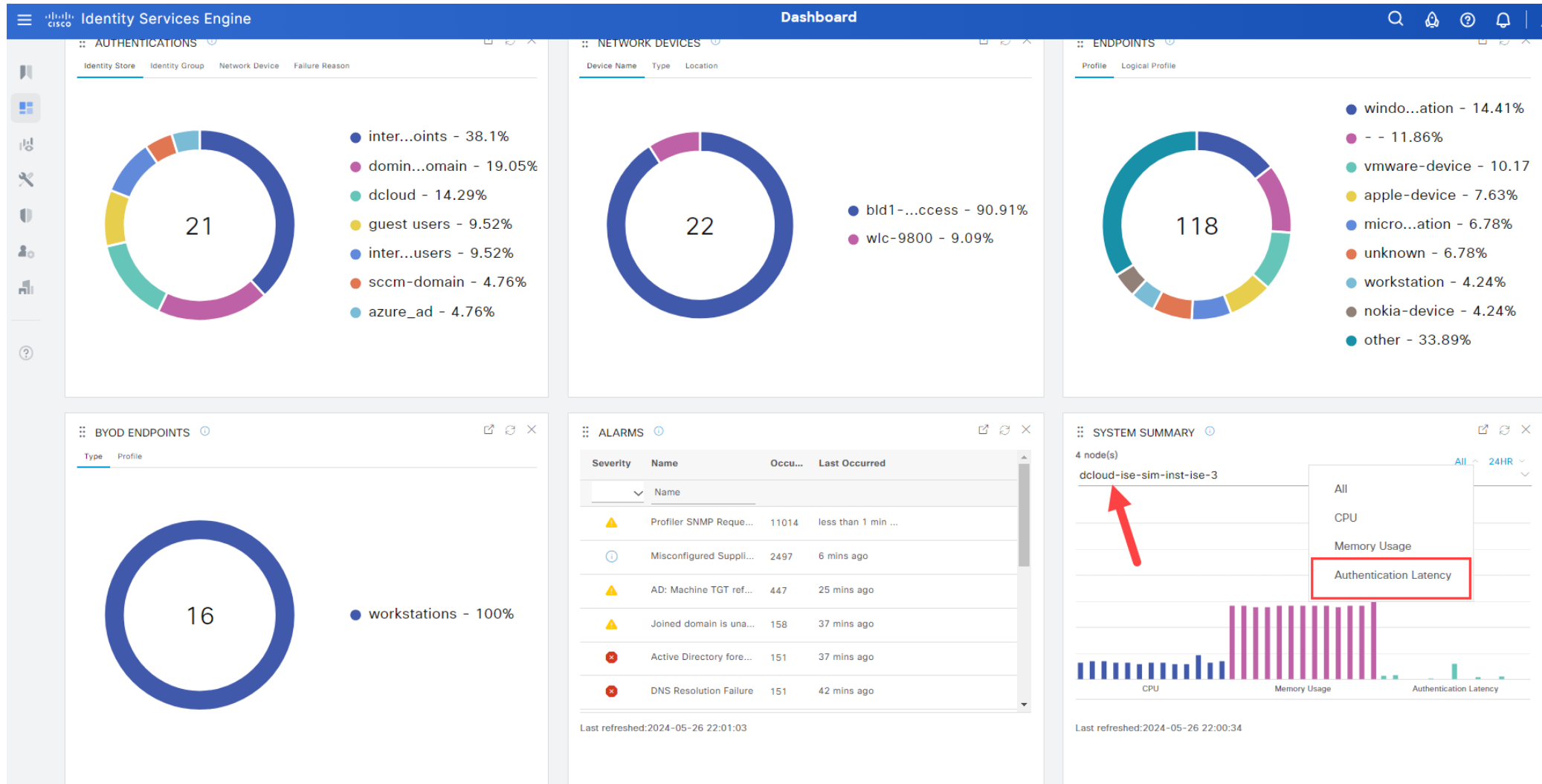


Troubleshooting ISE Issues

- 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



Troubleshoot ISE Issues

Administration>System Deployment – Check Node Status for replication issues



For your
reference only

Identity Services Engine Administration / System

Deployment Nodes

Selected 0 Total 4

Edit Register Syncup Deregister

Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/> dcloud-ise-sim-inst-ise-3	Administration, Monitoring, pxGrid	PRI(A), PRI(M)	TC-NAC,SXP	<input checked="" type="checkbox"/>
<input type="checkbox"/> dcloud-ise2-sim-inst-ise-3	Administration, Monitoring, pxGrid	SEC(A), SEC(M)	SXP	<input checked="" type="checkbox"/>
<input type="checkbox"/> dcloud-ise3-sim-inst-ise-3	Policy Service		SESSION,PROFILER,DEVICE ADMIN	<input checked="" type="checkbox"/>
<input type="checkbox"/> dcloud-ise4-sim-inst-ise-3	Policy Service		SESSION,PROFILER,DEVICE ADMIN	<input checked="" type="checkbox"/>

Troubleshooting ISE Issues

Administration>System>Certificates>System Certificates – Check System



For your reference only

Identity Services Engine Administration / System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

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	Valid From	Expiration Date	Status
<input type="checkbox"/> dcloud-ise-sim-inst-ise-3							
<input type="checkbox"/> Default self-signed saml server certificate - CN=SAML_dcloud-ise-sim-inst-ise-3.PseudoCo.com	SAML		SAML_dcloud-ise-sim-inst-ise-3.PseudoCo.com	SAML_dcloud-ise-sim-inst-ise-3.PseudoCo.com	Thu, 23 Feb 2023	Tue, 22 Feb 2028	Active
<input type="checkbox"/> CN=dcloud-ise-sim-inst-ise-3.PseudoCo.com, OU=ISE Messaging Service#Certificate Services Endpoint Sub CA - dcloud-ise-sim-inst-ise-3#00001	ISE Messaging Service		dcloud-ise-sim-inst-ise-3.PseudoCo.com	Certificate Services Endpoint Sub CA - dcloud-ise-sim-inst-ise-3	Wed, 22 Feb 2023	Wed, 23 Feb 2028	Active
<input type="checkbox"/> dcloud-ise-sim-inst-ise-3_A D_CA_Signed	Admin, Portal, EAP Authentication, pxGrid, RADIUS DTLS	Default Portal Certificate Group ⓘ	dcloud-ise-sim-inst-ise-3.PseudoCo.com	PseudoCo-AD-CA	Fri, 18 Aug 2023	Mon, 18 Aug 2025	Active
> dcloud-ise2-sim-inst-ise-3							
> dcloud-ise3-sim-inst-ise-3							
> dcloud-ise4-sim-inst-ise-3							

Check the existence of certificates, expiration date, and status on other ISE nodes

Troubleshoot ISE Issues

Administration > System > Certificates > Trusted Certificates – Check Trusted

Identity Services Engine
Administration / System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority

Trusted Certificates

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

[Edit](#)
[+ Import](#)
[Export](#)
[Delete](#)
[View](#)

	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
<input type="checkbox"/>	AD-10-10_CA_Root	Infrastructure Cisco Services Endpoints	6E 1A 9B 5D ...	PseudoCo-AD-CA	PseudoCo-AD-CA	Wed, 16 Aug ...	Sat, 16 Aug 2...	Enabled
<input type="checkbox"/>	Baltimore CyberTrust Root	Cisco Services	02 00 00 B9	Baltimore CyberT...	Baltimore CyberT...	Fri, 12 May 20...	Mon, 12 May ...	Enabled
<input type="checkbox"/>	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 20...	Mon, 7 Sep 2...	Enabled
<input type="checkbox"/>	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2...	Sun, 30 May 2...	Enabled
<input type="checkbox"/>	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov ...	Thu, 12 Nov 2...	Enabled
<input type="checkbox"/>	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 20...	Cisco Root CA 20...	Fri, 14 May 20...	Mon, 14 May ...	Disabled
<input type="checkbox"/>	Cisco Root CA 2099	Cisco Services	01 9A 33 58 ...	Cisco Root CA 20...	Cisco Root CA 20...	Tue, 9 Aug 20...	Sun, 9 Aug 20...	Enabled
<input type="checkbox"/>	Cisco Root CA M1	Cisco Services	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2...	Fri, 18 Nov 20...	Enabled
<input type="checkbox"/>	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov ...	Thu, 12 Nov 2...	Enabled
<input type="checkbox"/>	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 20...	Sun, 9 Jul 2034	Enabled

Check
expiration
dates

Check
status

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

Troubleshoot ISE Issues

Administration>Deployment – Check Node Status for replication issues



For your reference only

Identity Services Engine Administration / System

Deployment Nodes

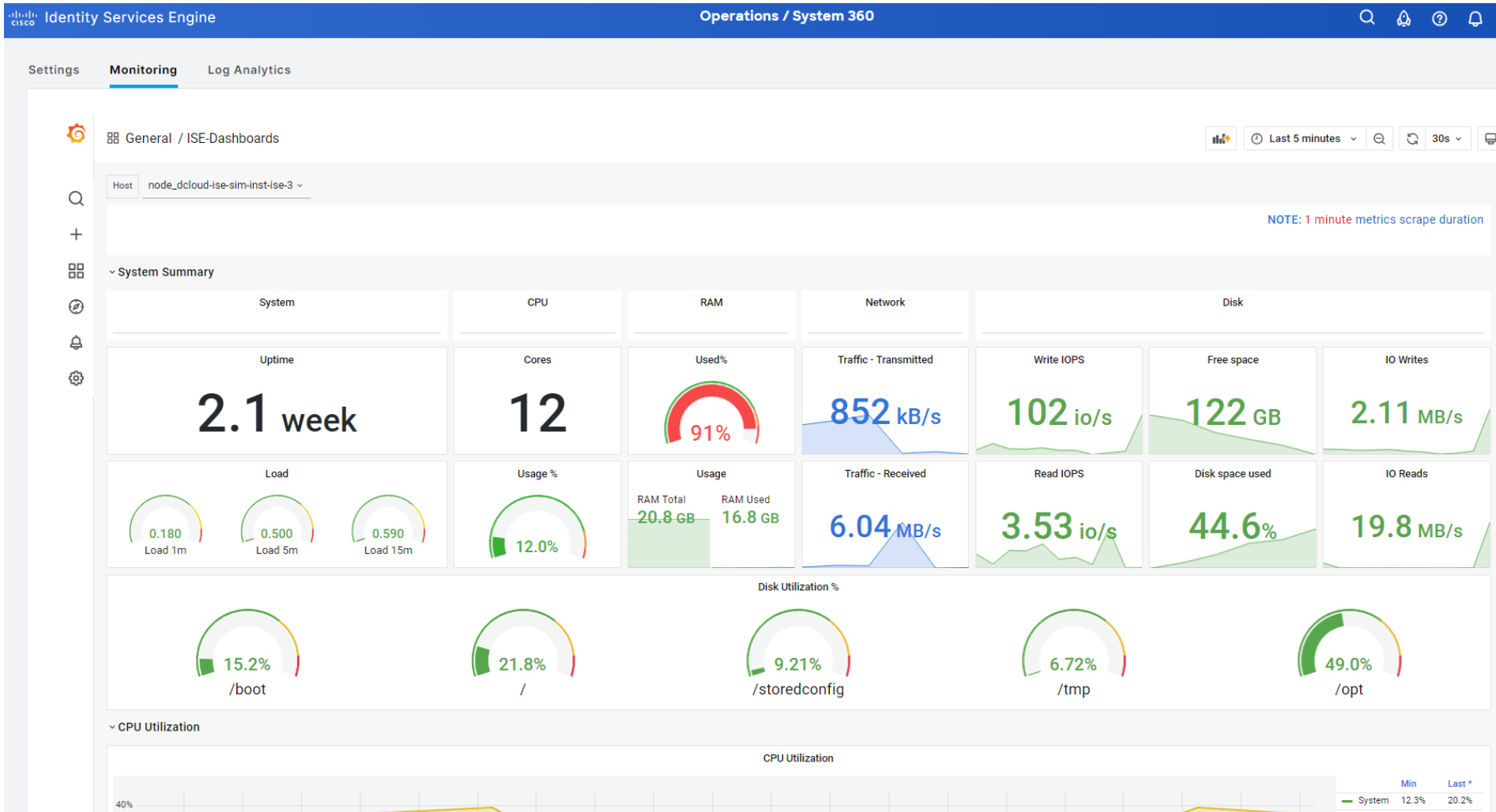
Selected 0 Total 4

Edit Register Syncup Deregister

Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/> dcloud-ise-sim-inst-ise-3	Administration, Monitoring, pxGrid	PRI(A), PRI(M)	TC-NAC,SXP	<input checked="" type="checkbox"/>
<input type="checkbox"/> dcloud-ise2-sim-inst-ise-3	Administration, Monitoring, pxGrid	SEC(A), SEC(M)	SXP	<input checked="" type="checkbox"/>
<input type="checkbox"/> dcloud-ise3-sim-inst-ise-3	Policy Service		SESSION,PROFILER,DEVICE ADMIN	<input checked="" type="checkbox"/>
<input type="checkbox"/> dcloud-ise4-sim-inst-ise-3	Policy Service		SESSION,PROFILER,DEVICE ADMIN	<input checked="" type="checkbox"/>

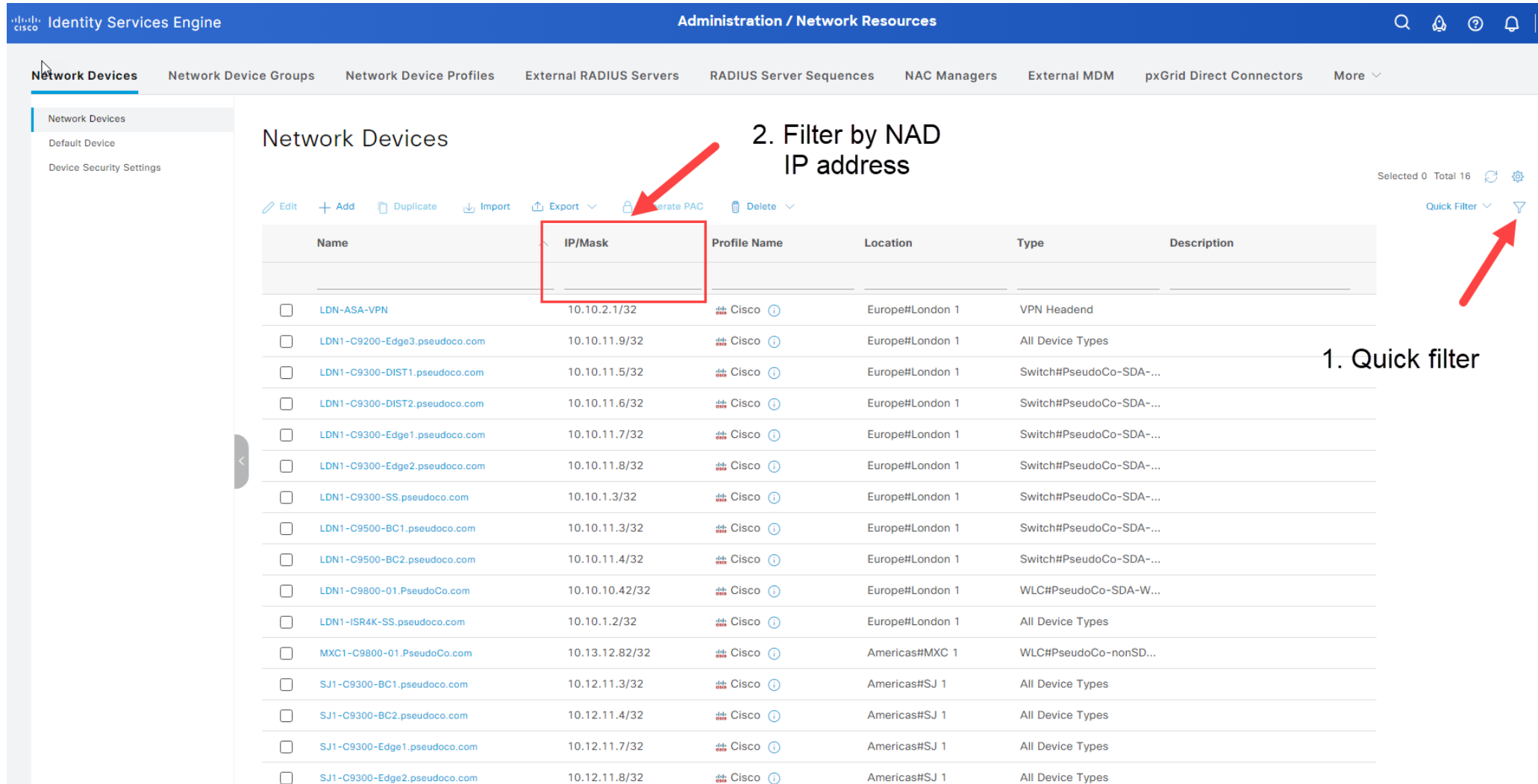
Troubleshoot ISE Issues

Operations>System 360>Monitoring – ISE Node Health Monitoring



Troubleshoot ISE Issues

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



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

Quick Filter

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

1. Quick filter



For your
reference only

Troubleshoot ISE Issues

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

Identity Services Engine Operations / System 360

Settings Monitoring Log Analytics

elastic

Dashboard

Dashboards + Create dashboard

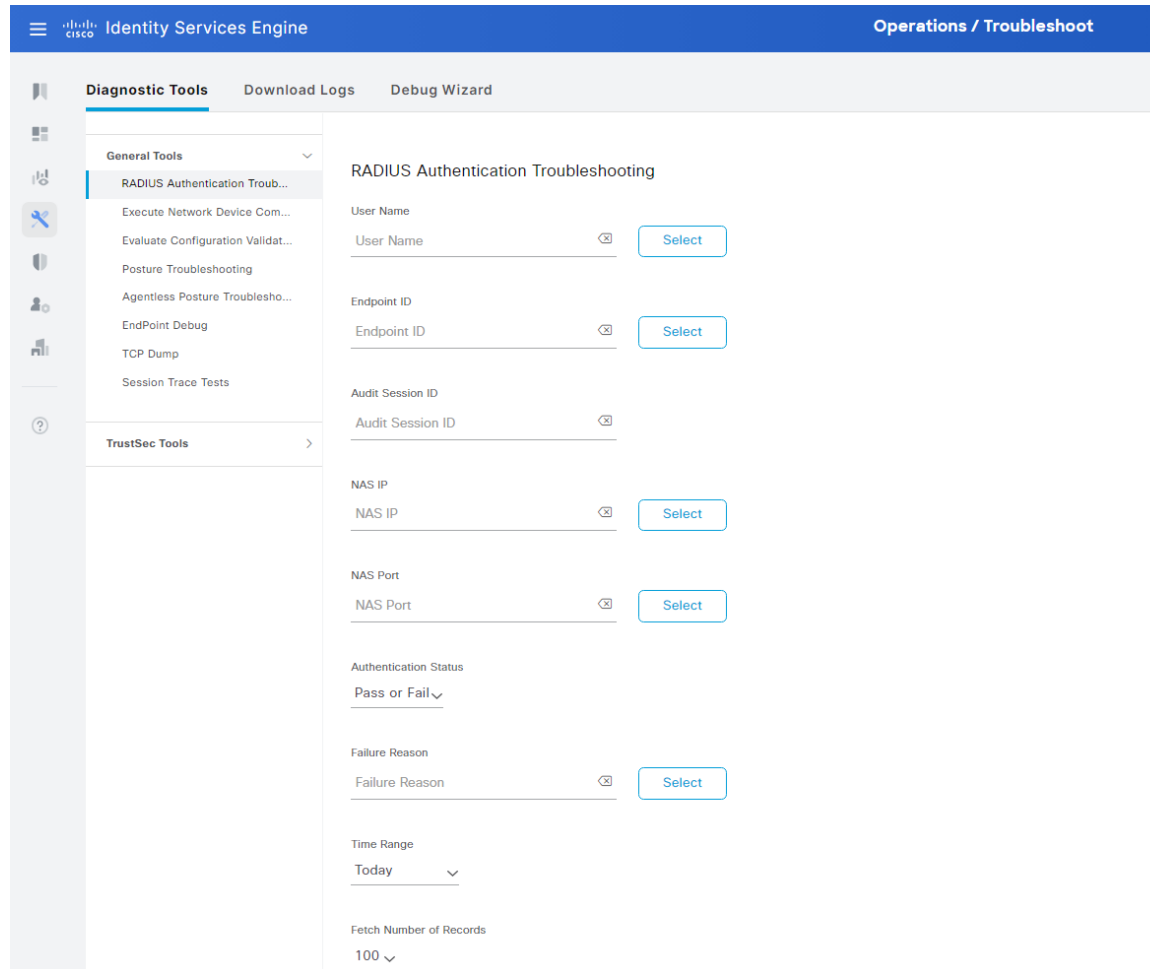
Tags ▾

<input type="checkbox"/>	Title	Description	Tags	Actions
<input type="checkbox"/>	ISE Observability Dashboard			
<input type="checkbox"/>	ISE Overview Dashboard			
<input type="checkbox"/>	ISE Processes Summary			
<input type="checkbox"/>	ISE Troubleshooting Dashboard			
<input type="checkbox"/>	Profiler Performance			
<input type="checkbox"/>	Profiler Summary			
<input type="checkbox"/>	RADIUS Accounting Summary			
<input type="checkbox"/>	RADIUS Authentication Summary			
<input type="checkbox"/>	RADIUS Performance			
<input type="checkbox"/>	TACACS Accounting Summary			
<input type="checkbox"/>	TACACS Authentication Summary			

Rows per page: 20 ▾ < 1 >

Troubleshoot ISE Issues

Operations>Troubleshooting>Diagnostic Tools>RADIUS Authentication Troubleshooting – Troubleshoot RADIUS Authentications

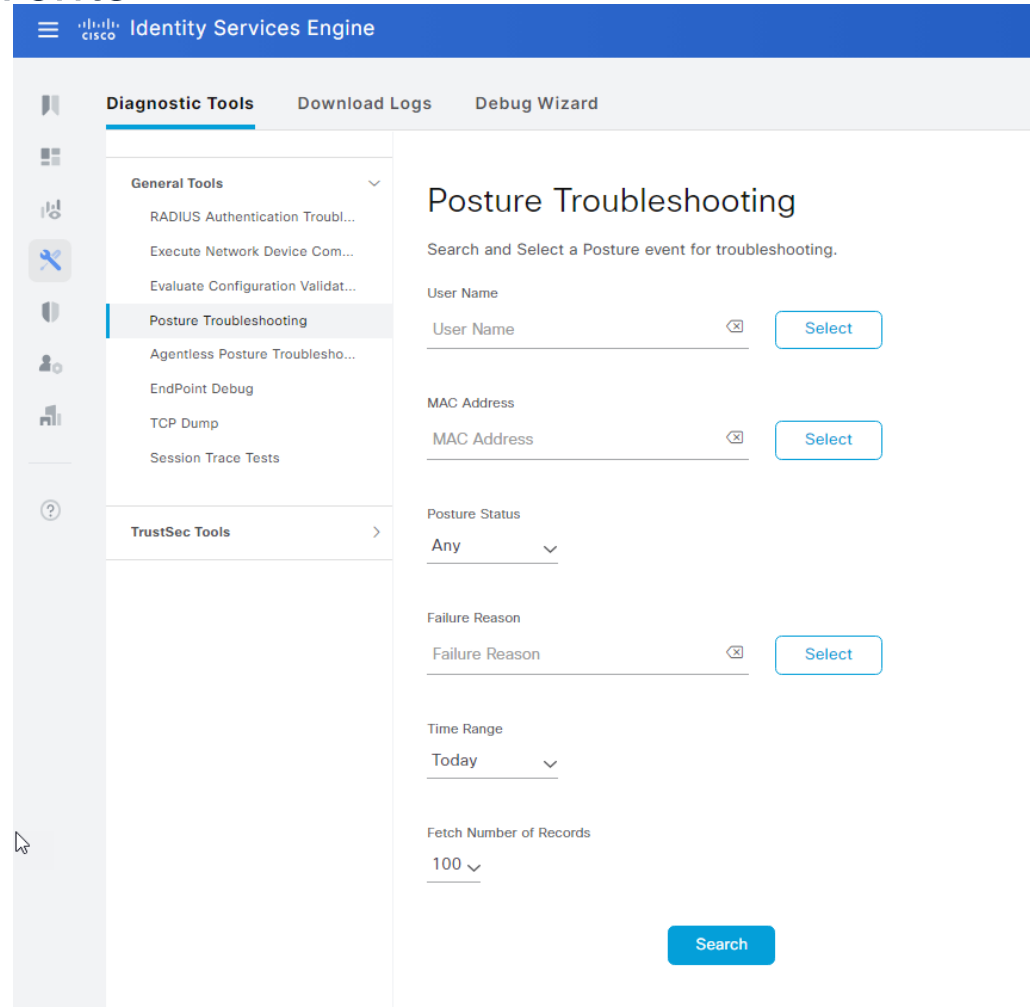


The screenshot displays the Cisco Identity Services Engine (ISE) interface for RADIUS Authentication Troubleshooting. The top navigation bar shows "Identity Services Engine" and "Operations / Troubleshoot". The left sidebar contains "Diagnostic Tools" and "TrustSec Tools". The main content area is titled "RADIUS Authentication Troubleshooting" and includes the following fields:

- User Name:
- Endpoint ID:
- Audit Session ID:
- NAS IP:
- NAS Port:
- Authentication Status:
- Failure Reason:
- Time Range:
- Fetch Number of Records:

Troubleshoot ISE Issues

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



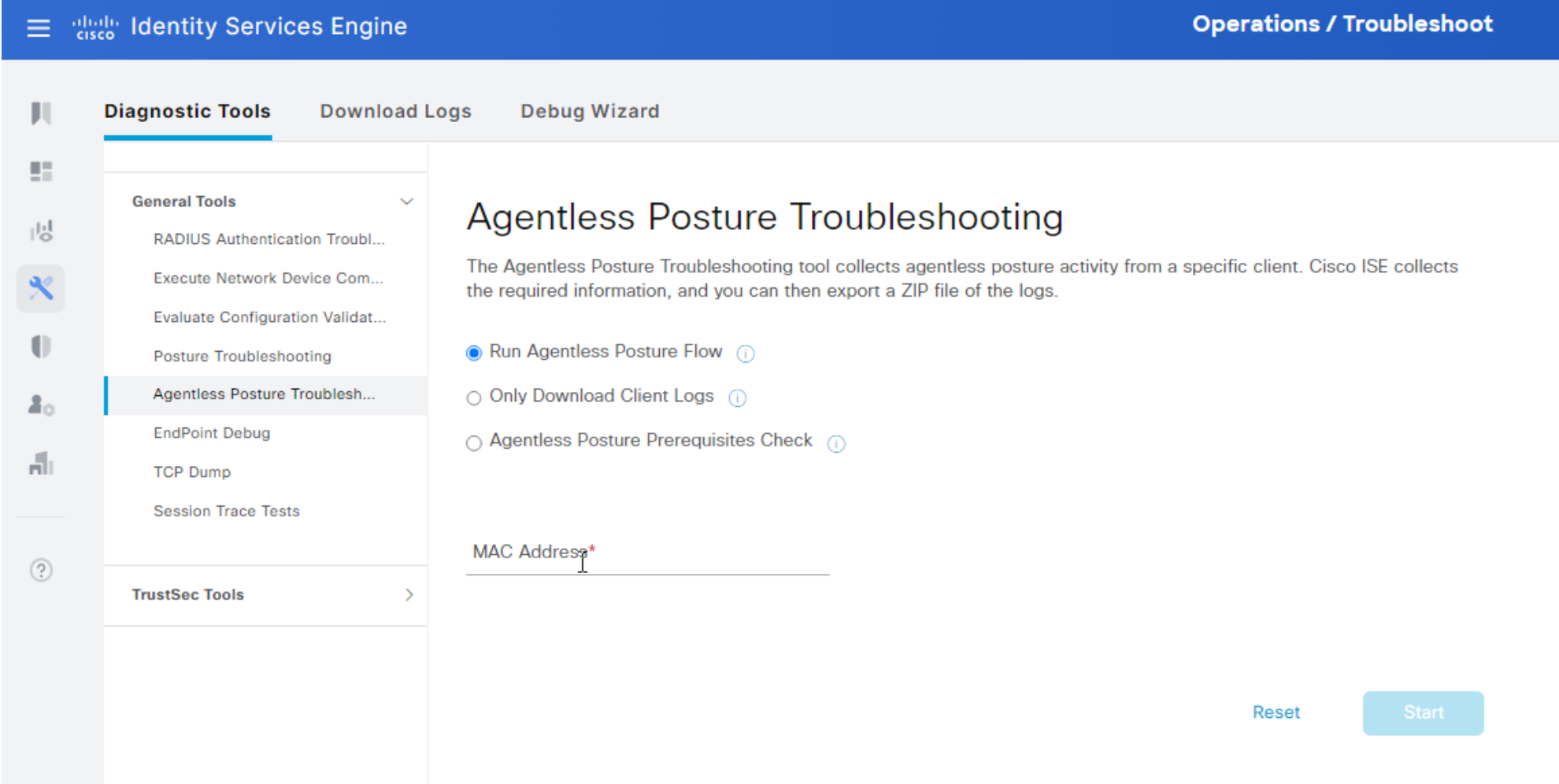
The screenshot displays the Cisco Identity Services Engine (ISE) web interface for Posture Troubleshooting. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". Below this, a secondary navigation bar contains "Diagnostic Tools", "Download Logs", and "Debug Wizard". The "Diagnostic Tools" section is expanded, showing a list of tools under "General Tools" and "TrustSec Tools". The "Posture Troubleshooting" tool is selected and highlighted. The main content area is titled "Posture Troubleshooting" and contains a search form with the following fields:

- User Name:** A text input field with a "Select" button.
- MAC Address:** A text input field with a "Select" button.
- Posture Status:** A dropdown menu currently set to "Any".
- Failure Reason:** A text input field with a "Select" button.
- Time Range:** A dropdown menu currently set to "Today".
- Fetch Number of Records:** A dropdown menu currently set to "100".

A "Search" button is located at the bottom of the form.

Troubleshoot ISE Issues

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



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar is blue with the Cisco logo and the text "Identity Services Engine" on the left, and "Operations / Troubleshoot" on the right. Below the navigation bar, there are three tabs: "Diagnostic Tools" (selected), "Download Logs", and "Debug Wizard". The "Diagnostic Tools" tab is expanded to show a list of tools under "General Tools" and "TrustSec Tools". The "Agentless Posture Troubleshooting" tool is selected. The main content area displays the "Agentless Posture Troubleshooting" tool configuration page. It includes a description: "The Agentless Posture Troubleshooting tool collects agentless posture activity from a specific client. Cisco ISE collects the required information, and you can then export a ZIP file of the logs." There are three radio button options: "Run Agentless Posture Flow" (selected), "Only Download Client Logs", and "Agentless Posture Prerequisites Check". Below these options is a text input field labeled "MAC Address*" with a red asterisk indicating it is required. At the bottom right of the page, there are two buttons: "Reset" and "Start".



Troubleshoot ISE Issues

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

Identity Services Engine Operations / Troubleshoot

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

TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

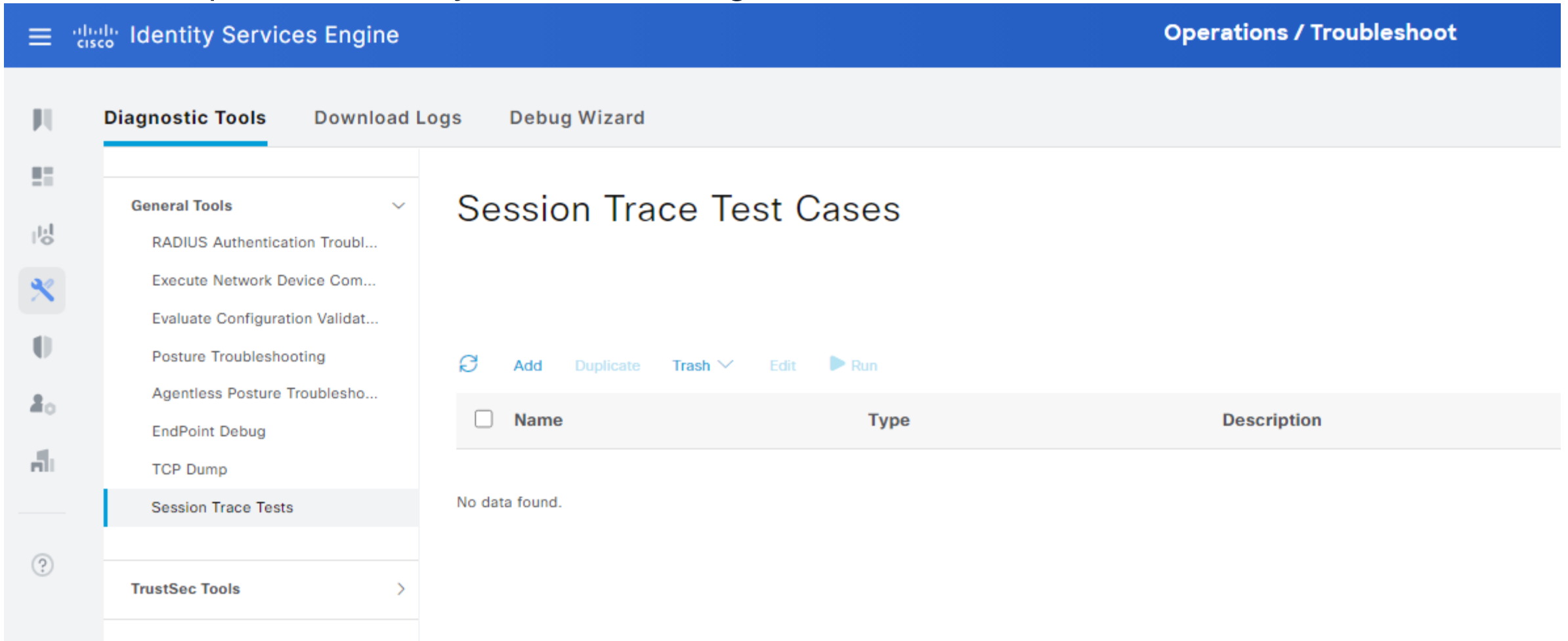
Rows/Page 0 << >> / 0 >>

Refresh Add Edit Trash Start Stop Download

<input type="checkbox"/>	Host Name	Network Interface	Filter	File Name	Repository	File S...	Number of ...	Time Limit	Promiscuous M...	Status
No data found.										

Troubleshoot ISE Issues

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



Identity Services Engine Operations / Troubleshoot

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 >

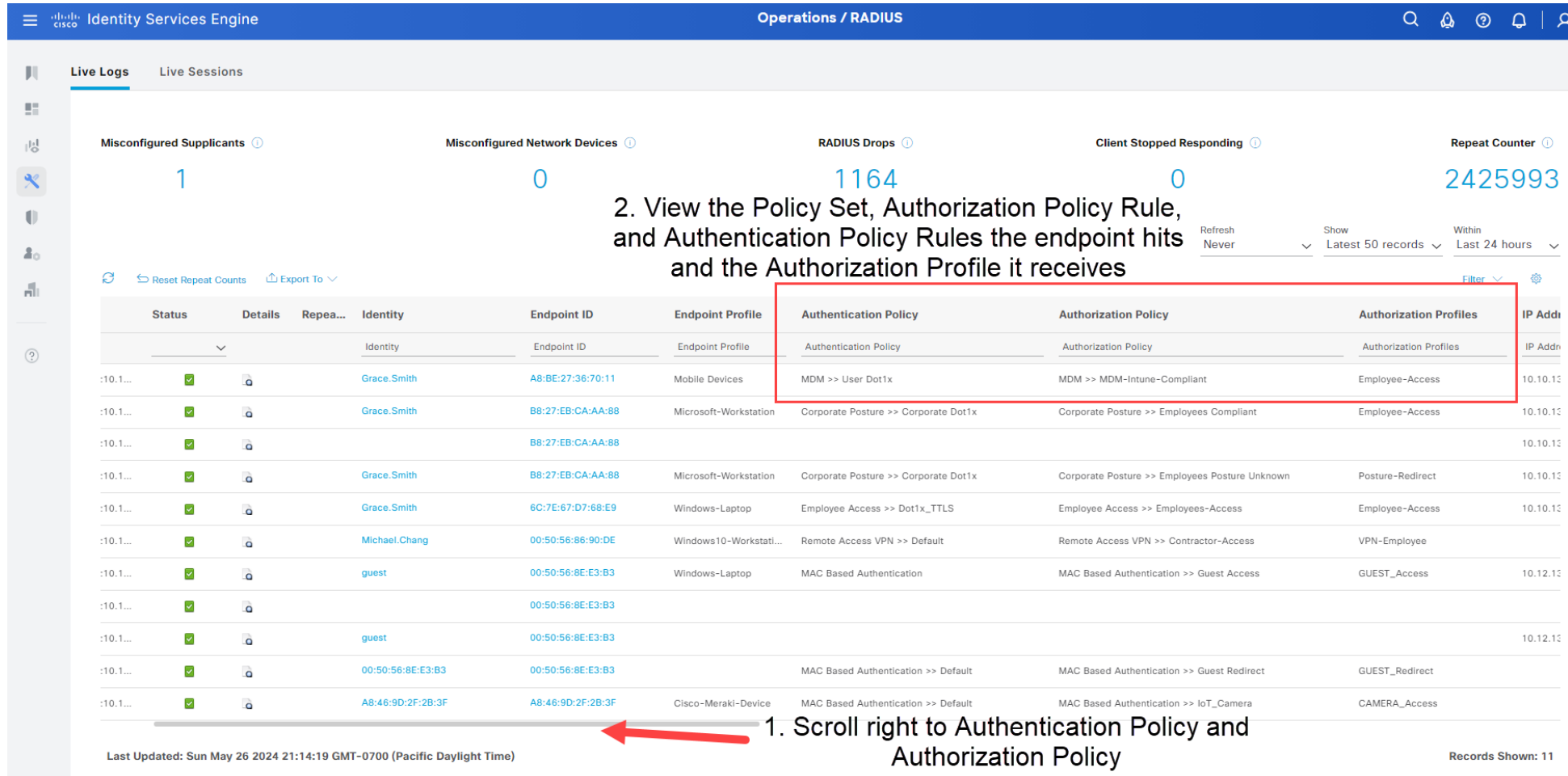
Session Trace Test Cases

↻ Add Duplicate Trash ▼ Edit ▶ Run

<input type="checkbox"/>	Name	Type	Description
No data found.			

Troubleshoot ISE Issues – Policy Troubleshooting 1

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



2. View the Policy Set, Authorization Policy Rule, and Authentication Policy Rules the endpoint hits and the Authorization Profile it receives

Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Addr
			Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	IP Addr
10.1...	✓	🔒	Grace.Smith	A8:BE:27:36:70:11	Mobile Devices	MDM >> User Dot1x	MDM >> MDM-Intune-Compliant	Employee-Access	10.10.10.10
10.1...	✓	🔒	Grace.Smith	B8:27:EB:CA:AA:88	Microsoft-Workstation	Corporate Posture >> Corporate Dot1x	Corporate Posture >> Employees Compliant	Employee-Access	10.10.10.10
10.1...	✓	🔒		B8:27:EB:CA:AA:88					10.10.10.10
10.1...	✓	🔒	Grace.Smith	B8:27:EB:CA:AA:88	Microsoft-Workstation	Corporate Posture >> Corporate Dot1x	Corporate Posture >> Employees Posture Unknown	Posture-Redirect	10.10.10.10
10.1...	✓	🔒	Grace.Smith	6C:7E:67:D7:68:E9	Windows-Laptop	Employee Access >> Dot1x_TTLS	Employee Access >> Employees-Access	Employee-Access	10.10.10.10
10.1...	✓	🔒	Michael.Chang	00:50:56:86:90:DE	Windows10-Workstati...	Remote Access VPN >> Default	Remote Access VPN >> Contractor-Access	VPN-Employee	
10.1...	✓	🔒	guest	00:50:56:8E:E3:B3	Windows-Laptop	MAC Based Authentication	MAC Based Authentication >> Guest Access	GUEST_Access	10.12.10.10
10.1...	✓	🔒		00:50:56:8E:E3:B3					10.12.10.10
10.1...	✓	🔒	guest	00:50:56:8E:E3:B3		MAC Based Authentication >> Default	MAC Based Authentication >> Guest Redirect	GUEST_Redirect	
10.1...	✓	🔒	00:50:56:8E:E3:B3	00:50:56:8E:E3:B3		MAC Based Authentication >> Default	MAC Based Authentication >> Guest Redirect	GUEST_Redirect	
10.1...	✓	🔒	A8:46:9D:2F:2B:3F	A8:46:9D:2F:2B:3F	Cisco-Meraki-Device	MAC Based Authentication >> Default	MAC Based Authentication >> IoT_Camera	CAMERA_Access	

1. Scroll right to Authentication Policy and Authorization Policy



Troubleshoot ISE Issues – Policy Troubleshooting 2

Operations>RADIUS Live Logs – Check Details for endpoint

Identity Services Engine Operations / RADIUS

Misconfigured Supplicants 1 Misconfigured Network Devices 0 RADIUS Drops 1264 Client Stopped Responding 0 Repeat Counter 2428890

Refresh Never Show Latest 50 records Within Last 24 hours

Reset Repeat Counts Export To

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization
May, 26 2024 12:34:41.1...	✓			Grace.Smith	A8:BE:27:36:70:11	Mobile Devices	MDM >> User Dot1x	MDM >> MDM-Intune-Compliant	Employee-Acces
May, 26 2024 12:34:41.1...	✓			Grace.Smith	B8:27:EB:CA:AA:88	Microsoft-Workstation	Corporate Posture >> Corporate Dot1x	Corporate Posture >> Employees Compliant	Employee-Acces

Troubleshoot ISE Issues – Policy Troubleshooting 3

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

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

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@pseudoco.com are extracted and authenticated against pseudoco.com Active Directory domain

Authentication to Active Directory Successful



For your
reference only

Troubleshoot ISE Issues – Policy Troubleshooting 4

Policy>Policy Sets – Check Conditions compared to authentication details

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+			Search				
●	PseudoCo Lab	Policy for PseudoCo Lab	AND - DEVICE-Deployment Type EQUALS Deployment Type#PseudoCo-Lab OR - RADIUS-Called-Station-ID CONTAINS @PseudoCo-Corp - RADIUS-Called-Station-ID CONTAINS @PseudoCo-Guest - RADIUS-Called-Station-ID CONTAINS @PseudoCo-Hotspot - RADIUS-Calling-Station-ID CONTAINS A8-46-9D-2F-2B-3F - RADIUS-NAS-IP-Address EQUALS 10.12.11.7	Default Network Access	8266	⚙️	➔
●	MAC Based Authentication	Policy for Hotspot, Guest, and IoT	OR - Wired_MAB - Wireless_MAB	HostLookup	1871	⚙️	➔
●	Corporate Posture	Posture policy for San Jose employees	AND - DEVICE-Location EQUALS All Locations#Americas#SJ 1 OR - Wireless_802.1X - Wired_802.1X	Default Network Access	1675	⚙️	➔
●	MDM	Posture policy using MDM/EMM	AND - DEVICE-Location EQUALS All Locations#Europe#London 1 OR - Wired_802.1X - Wireless_802.1X	Default Network Access	1978	⚙️	➔
●	Employee Access	Policy for BYOD devices and corporate users	OR - Wired_802.1X - Wireless_802.1X	Default Network Access	1356	⚙️	➔
●	Remote Access VPN	Policy for VPN users	- DEVICE-Device Type EQUALS All Device Types#VPN Headend	Default Network Access	2134	⚙️	➔
●	Default	Default policy set		Default Network Access	1015	⚙️	➔

Troubleshoot ISE Issues – Policy Troubleshooting 5

Check Policy Set conditions against previously checked Authentication Detail

Identity Services Engine Policy / Policy Sets

Policy Sets → Employee Access Reset Reset Policyset Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequ
●	Employee Access	Policy for BYOD devices and corporate users	OR <ul style="list-style-type: none"> Wired_802.1X Wireless_802.1X 	Default Network Access ✎ +

Authentication Policy(4)

Status	Rule Name	Conditions	Use	Hits
●	Dot1x_TLS	EAP-TLS	Preloaded_Certificate_Prof... ✎ > Options	0
●	Dot1x_TTLS	Network Access-EapTunnel EQUALS EAP-TTLS	Azure_AD ✎ > Options	0
●	Dot1x_MSCHAP	EAP-MSCHAPv2	AD-PseudoCo ✎ > Options	0
●	Default		All_User_ID_Stores ✎ > Options	0

Troubleshoot ISE Issues – Policy Troubleshooting 6

Check Policy Set conditions against previously checked Authentication Detail

Identity Services Engine Policy / Policy Sets

Authorization Policy(10)

Status	Rule Name	Conditions	Results	Profiles
✓	TC-NAC_NoVuln	AND <ul style="list-style-type: none"> AD-PseudoCo-ExternalGroups EQUALS PseudoCo.com/Users/GROUP_Developers Threat-Tenable Security Center-CVSS_Base_Score LESS 2 		Employee-Access
✓	TC-NAC_Scan	<ul style="list-style-type: none"> AD-PseudoCo-ExternalGroups EQUALS PseudoCo.com/Users/GROUP_Developers 		Tenable_Scan
✓	TEAP-Chain-Success	AND <ul style="list-style-type: none"> Network Access-EapTunnel EQUALS TEAP Network Access-EapChainingResult EQUALS User and machine both succeeded AD-PseudoCo-ExternalGroups EQUALS PseudoCo.com/Users/GROUP_Employees 		Employee-Access
✓	TEAP_Chain-MachineAuth	AND <ul style="list-style-type: none"> Network Access-EapTunnel EQUALS TEAP Network Access-EapChainingResult EQUALS User failed and machine succeeded 		Employee-Restricted-Access
✓	TEAP_Chain-UserAuth	AND <ul style="list-style-type: none"> Network Access-EapTunnel EQUALS TEAP Network Access-EapChainingResult EQUALS User succeeded and machine failed 		GUEST_Access
✓	BYOD-Success	AND <ul style="list-style-type: none"> Wireless_802.1X Network Access-EapAuthentication EQUALS EAP-TLS EndPoints-BYODRegistration EQUALS Yes AD-PseudoCo-ExternalGroups EQUALS PseudoCo.com/Users/GROUP_Employees 		Employee-Access
✓	BYOD-Onboarding_dot1x	AND <ul style="list-style-type: none"> Wireless_802.1X Network Access-EapAuthentication EQUALS EAP-MSCHAPv2 EndPoints-BYODRegistration EQUALS Unknown 		BYOD_Onboard
✓	Employees-Access	OR <ul style="list-style-type: none"> AD-PseudoCo-ExternalGroups EQUALS PseudoCo.com/Users/GROUP_Employees Azure_AD-ExternalGroups EQUALS Employees 		Employee-Access

Conclusion

The background features a light gray gradient. A diagonal bar with a color gradient from red to blue is positioned in the upper right. A blue circular arc is visible in the lower left corner.

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>
- Cisco U: Introduction to 802.1X – <https://u.cisco.com/paths/introduction-8021x-operations-cisco-security-professionals-20909>
- Cisco U: Implementing ISE - <https://u.cisco.com/paths/implementing-configuring-cisco-identity-services-engine-21111>

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 2027.



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

CISCO Live !

Thank you

