

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC





ISE Deployment Improvements Tips and Tricks

Katherine McNamara
@kmcnam1
BRKSEC-2347

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

Questions?

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

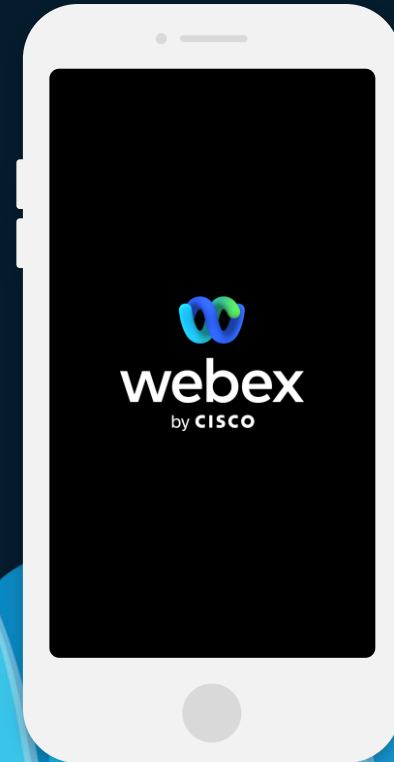
How

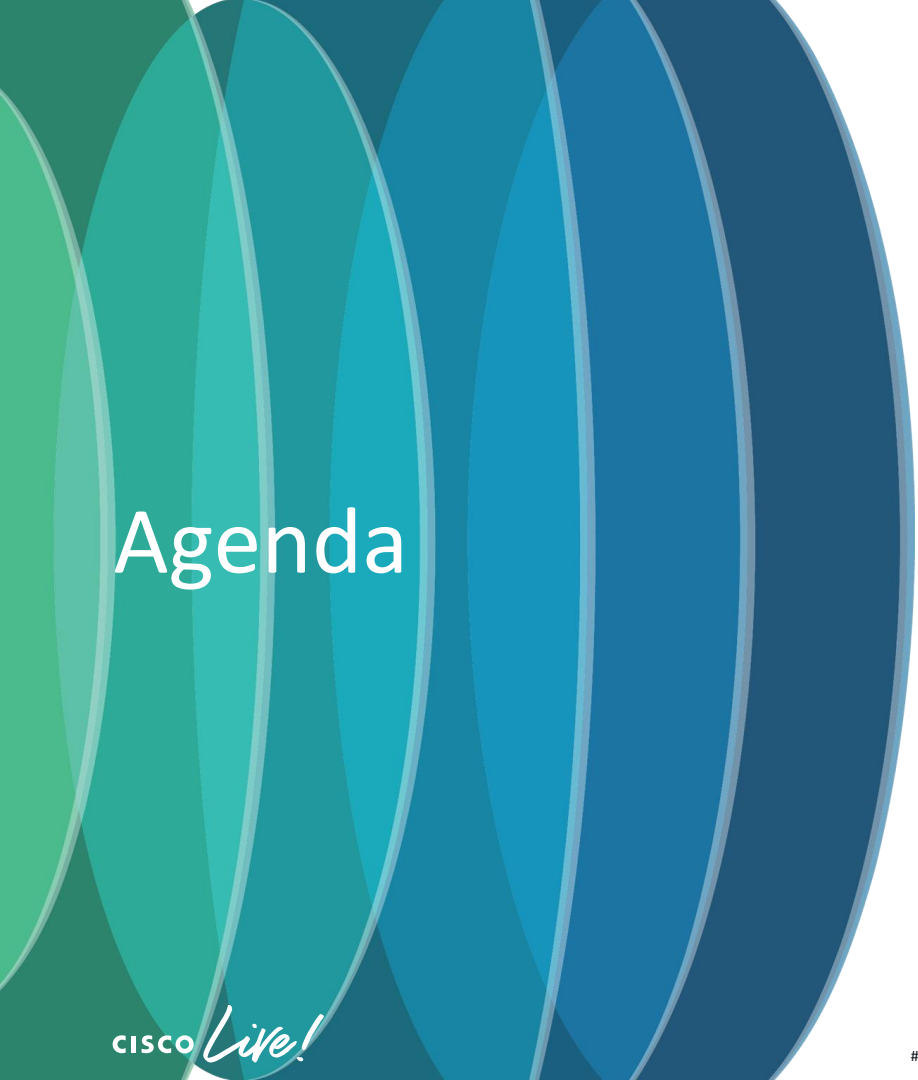
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2347>





Agenda

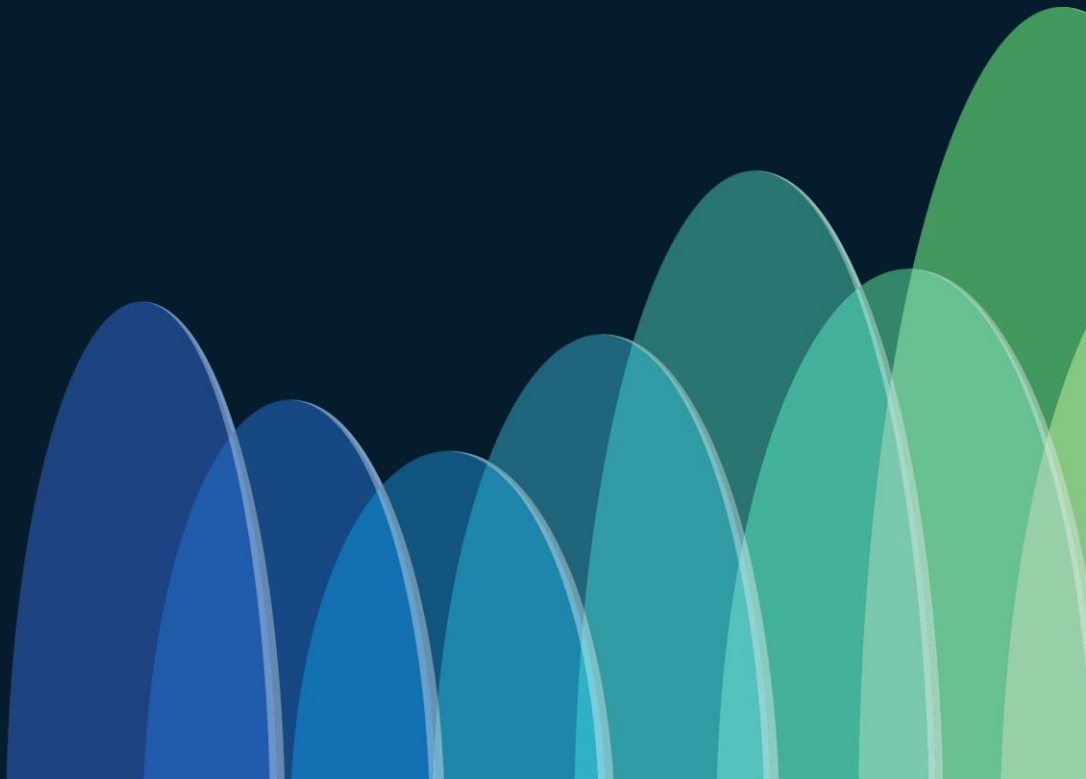
- Where to Start
- Laying the Foundation
- A Phased Approach
- Tuning Policy Sets
- The Power of Profiling
- Integrations
- Post-Deployment
- Conclusion

A little about me



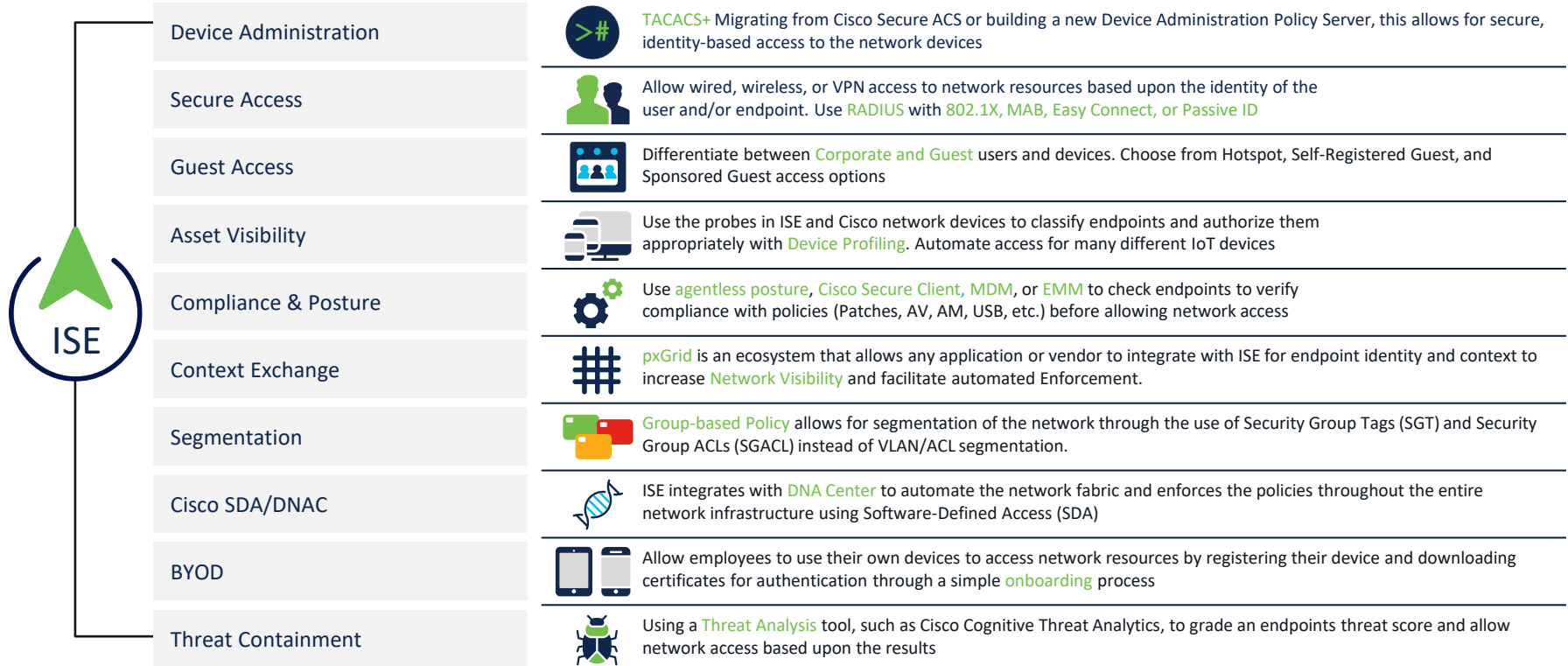
- Started as an early ISE 1.1 customer
- 15+ years of network & security experience
- Lots of paper: BS and MS in IT Security, 2x CCIE (Data Center + Security), CISSP, and various other industry certifications
- Co-authored recent CiscoPress SISE book
- Co-organize for the largest Cisco Meetup study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

Where to Start



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

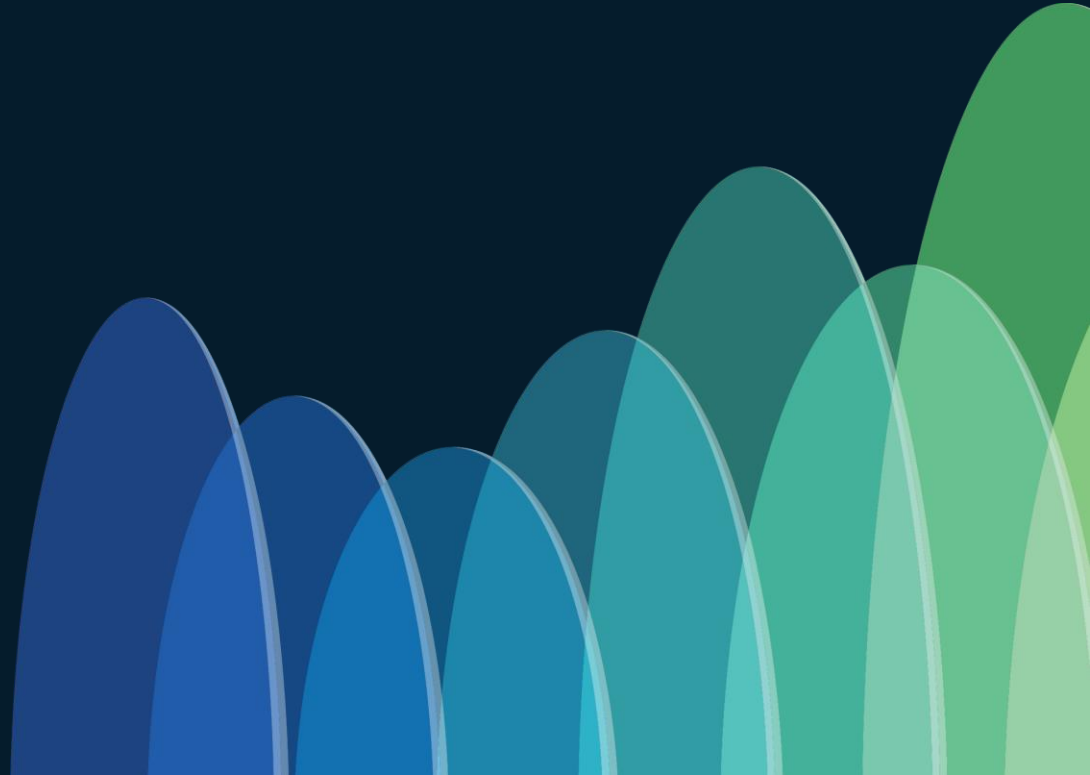
The Swiss Army Knife of Network Access Control



Where To Start...

- Define your business and security objectives
 - What is it that you want ISE to do for you?
- Determine which teams will be needed
 - Virtualization team?
 - Desktop support?
 - PKI?
 - etc
- Collaborate with those teams at the beginning of the project
- Get management buy-in early

Laying the Foundation



Let's Talk about ISE Personas...

- Administration Node (PAN)
 - Max 2 in a deployment
- Monitoring Node (MNT)
 - Max 2 in a deployment
- Policy Service Node (PSN)
 - Max 50 in a deployment
- pxGrid Node
 - Max 4 in a deployment



Policy Administration Node (PAN)

- Single plane of glass for ISE admin
- Replication hub for all database config changes



Monitoring and Troubleshooting Node (MnT)

- Reporting and logging node
- Syslog collector from ISE Nodes



Policy Services Node (PSN)

- Makes policy decisions
- RADIUS/TACACS+ Servers



pXGrid Controller

- Facilitates sharing of context

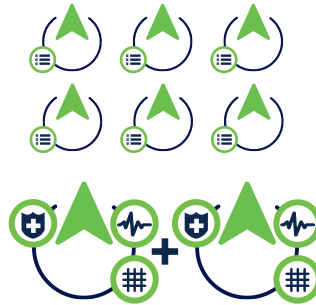
ISE Deployment Scale



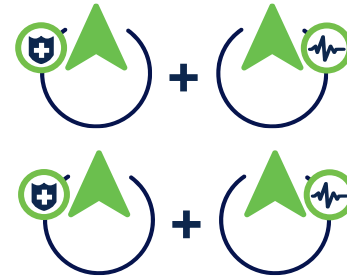
Lab and Evaluation



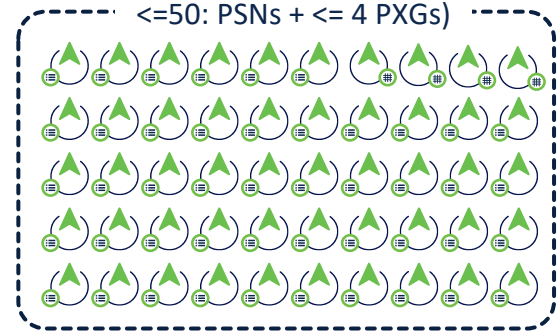
Small HA Deployment
2 x (PAN+MNT+PSN)



Medium Multi-node Deployment
2 x (PAN+MNT+PXG), <= 6 PSN



Large Deployment
2 PAN, 2 MNT, <=50: PSNs + <= 4 PXGs



100 Endpoints

Up to 50,000 Endpoints

Up to 2,000,000 Endpoints

3600

100 Endpoints

Up to 150,000 Endpoints

Up to 2,000,000 Endpoints

3700

ISE Node Types

Physical Appliances



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

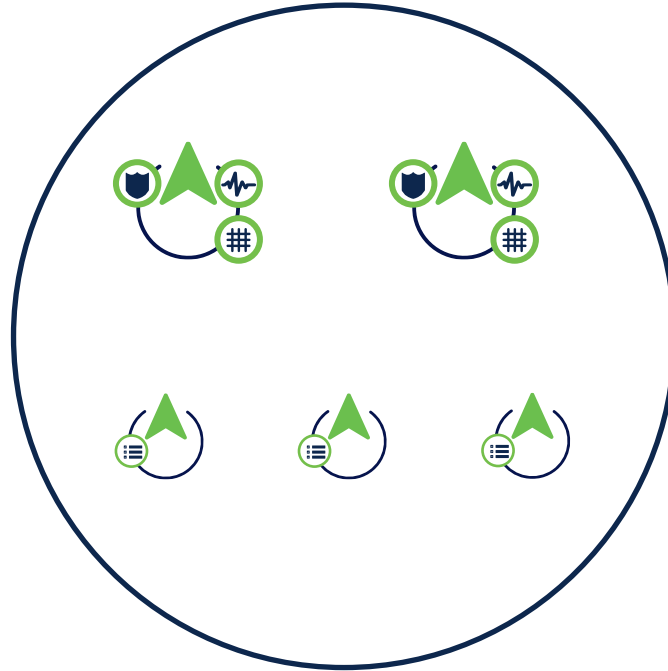
Virtual Machines



Cloud Instances



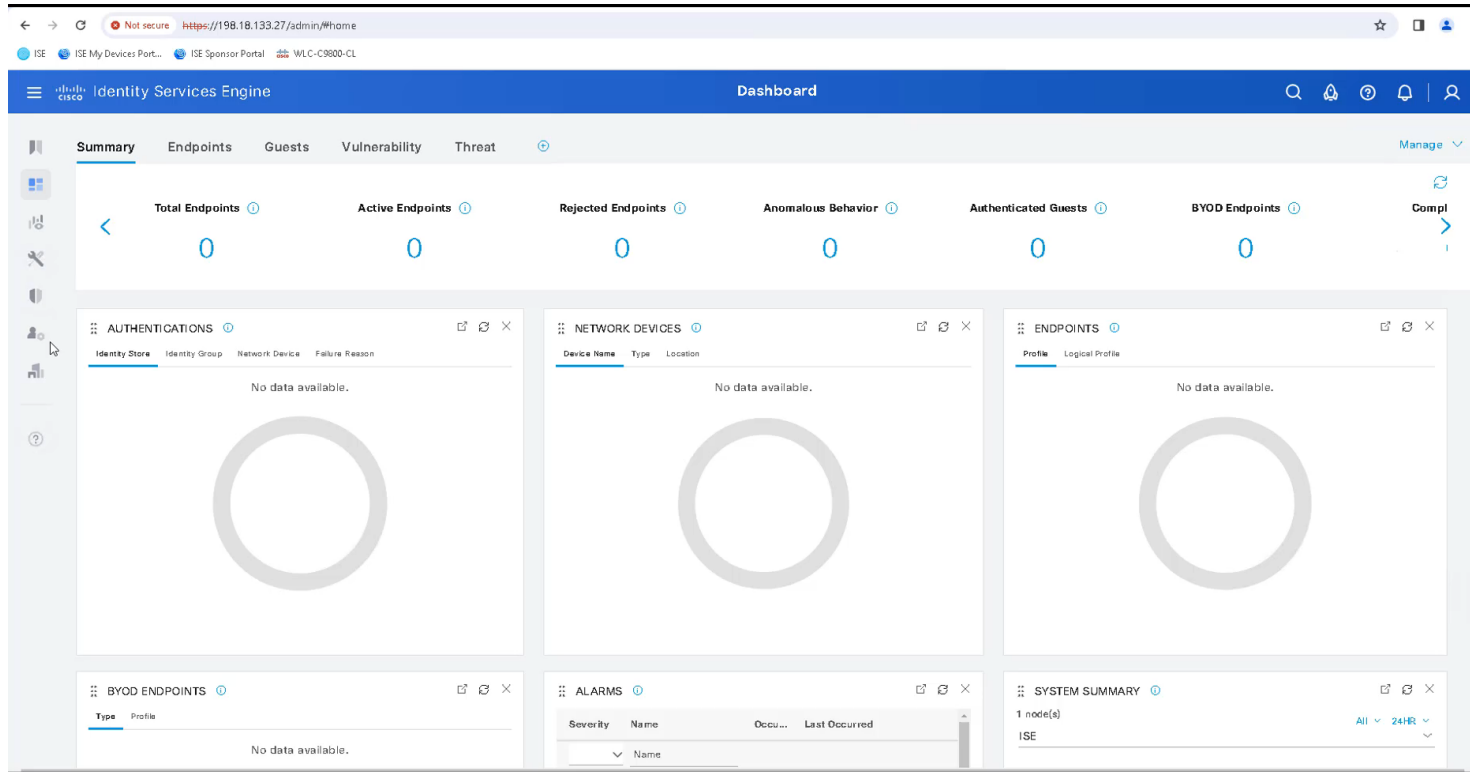
Expanding Your ISE Deployment...



CISCO *Live!*



Changing the Persona

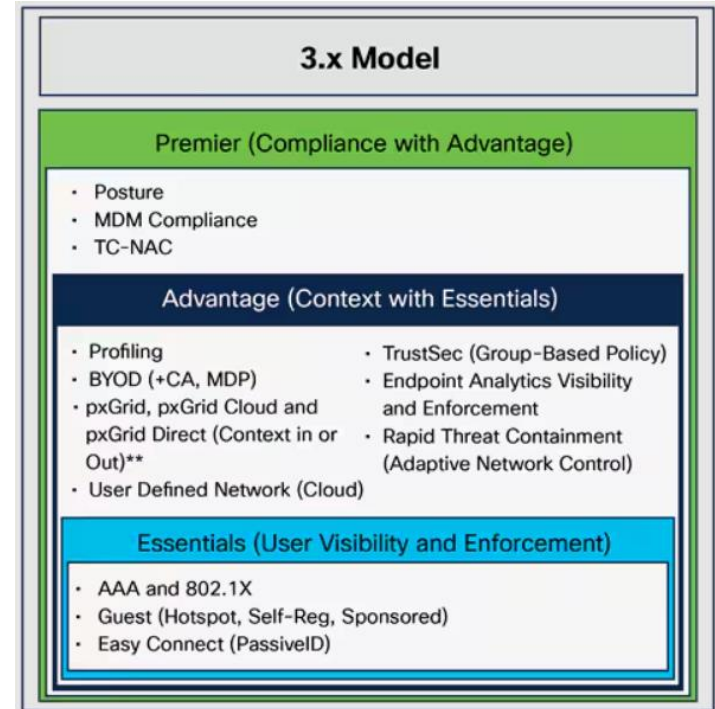


Recommendations

- Make your life easier: Use load balancers
 - Easier to add PSNs
 - Easier to upgrade
 - Failover is more seamless
- Scale up as you grow
- VMs or appliances? Same specs!
- Device Admin? Think about separate PSNs for TACACS+
- Use the ISE Scalability Guide as a reference

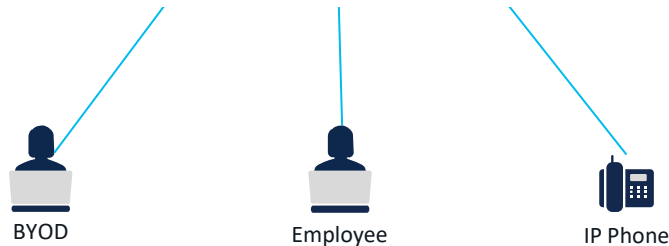
Licensing

- Endpoint licenses are based on 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



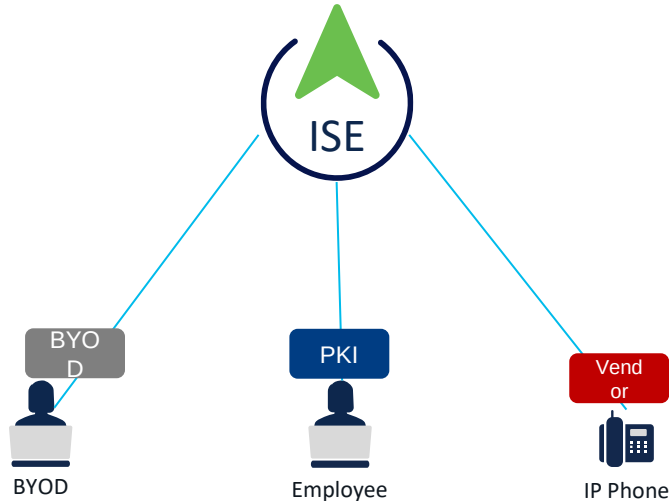
Certificates

- 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

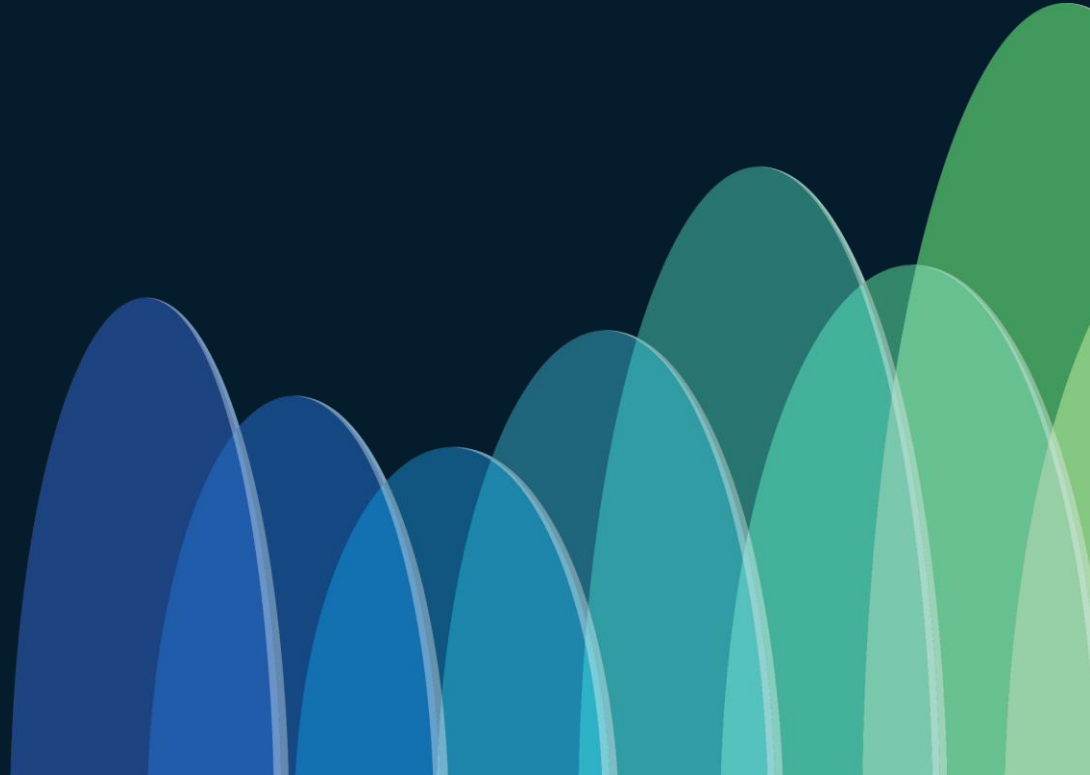
Reduce Chaos and Unpredictability

- 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

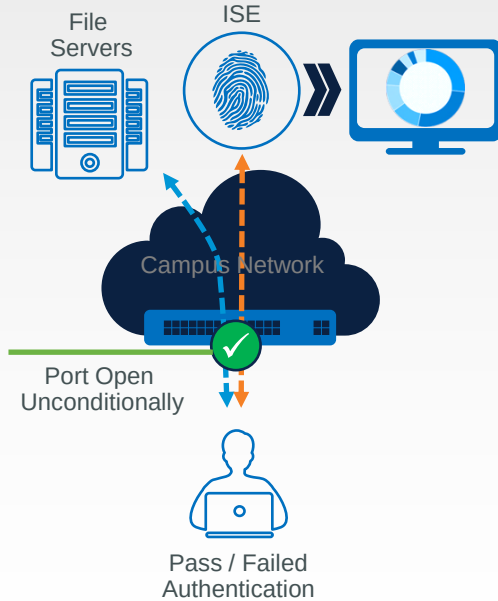


A Phased Approach to ISE...

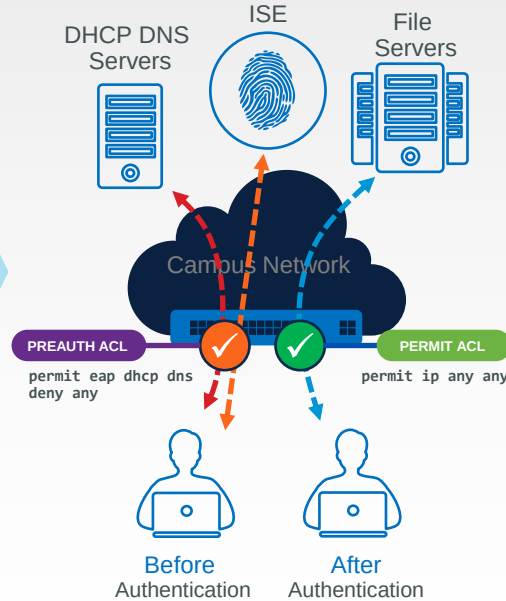
- VPN:
 - Create a test VPN profile
 - Migrate the profile to production after testing
- Wireless:
 - Create a test SSID
 - Migrate the profile to production after testing
- But what about wired?

Wired Phases

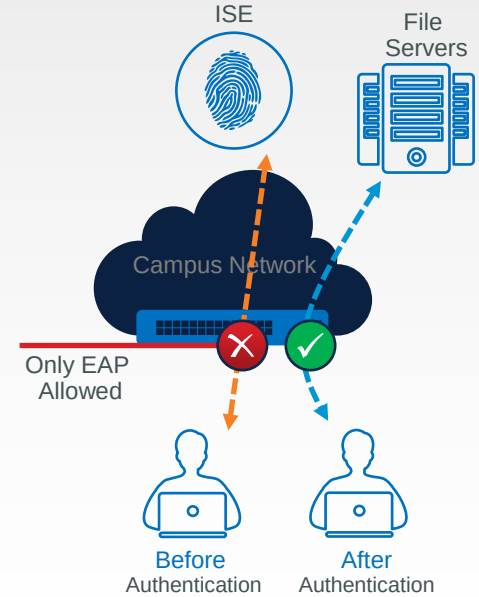
Monitor Mode



Low-Impact Mode



Closed Mode



More on Wired Access...

- Start as much as you can on Monitor Mode
 - Gathers contextual information about endpoints
 - Find the “Unknown” endpoints
 - What endpoints would have failed AuthC/AuthZ
- Build and test your policies in Monitor Mode
 - Note: Monitor Mode can still enforce/transition to low-impact mode if Authz is enabled/enforce
- Utilize Network Device Groups to make policy easier
 - Move switch-by-switch into low-impact mode this way

Monitor Mode for Policy Rules

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 TypesSwitches DEVICE-Mode EQUALS ModeMonitor	Default Network Access	0	⚙️	➔
●	Wired Low-Impact Mode		AND DEVICE-Device Type EQUALS All Device TypesSwitches DEVICE-Mode EQUALS ModeLow-Impact	Default Network Access	0	⚙️	➔
●	Default	Default policy set		Default Network Access	0	⚙️	➔

Creating and Applying 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 a "Dashboard" label. A search bar and several icons are also present. The left sidebar contains a "Bookmarks" section and a list of navigation items: "Dashboard", "Context Visibility", "Operations", "Policy", "Administration", "Work Centers", and "Interactive Features". The main content area is divided into several sections. At the top, there is a "Summary" tab with sub-tabs for "Endpoints", "Guests", "Vulnerability", and "Threat". Below this, a row of six cards displays key metrics: "Total Endpoints", "Active Endpoints", "Rejected Endpoints", "Anomalous Behavior", "Authenticated Guests", and "BYOD Endpoints", each with a value of 0. Below the metrics, there are three large cards for "AUTHENTICATIONS", "NETWORK DEVICES", and "ENDPOINTS", each showing "No data available." and a large circular graphic. At the bottom, there are two more cards: "BYOD ENDPOINTS" and "ALARMS". The "ALARMS" card shows a table with columns for "Severity", "Name", "Occu...", and "Last Occurred". The "SYSTEM SUMMARY" card shows "1 node(s)" and "ISE".

Identity Services Engine Dashboard

Summary Endpoints Guests Vulnerability Threat

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

0 0 0 0 0 0

Authentication Network Devices Endpoints

No data available. No data available. No data available.

BYOD Endpoints Alarms System Summary

No data available.

Severity	Name	Occu...	Last Occurred
Configuration Chang...	7267	less than 1 min ...	

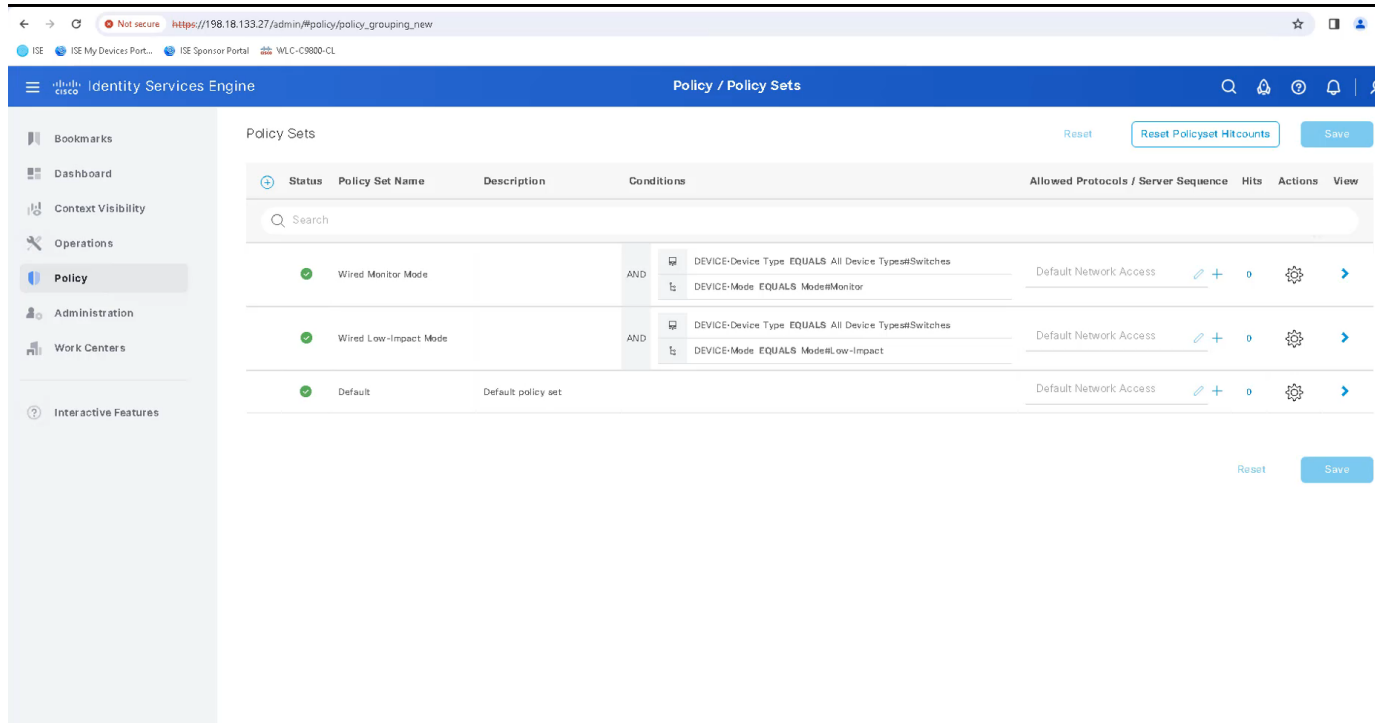
1 node(s) ISE

Policy Set Example – Monitor vs Low-Impact

Policy Sets

	Status	Policy Set Name	Description	Conditions
 Search				
		Wired Monitor Mode		AND <ul style="list-style-type: none"> DEVICE·Device Type EQUALS All Device Types#Switches DEVICE·Mode EQUALS Mode#Monitor
		Wired Low-Impact Mode		AND <ul style="list-style-type: none"> DEVICE·Device Type EQUALS All Device Types#Switches DEVICE·Mode EQUALS Mode#Low-Impact

Moving from Monitor to Low-Impact Mode



The screenshot displays the Cisco Identity Services Engine (ISE) web interface, specifically the 'Policy / Policy Sets' configuration page. The page shows a table of policy sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. Three policy sets are listed: 'Wired Monitor Mode', 'Wired Low-Impact Mode', and 'Default'. The 'Wired Low-Impact Mode' policy set is highlighted, showing its conditions and actions.

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 Model#Monitor	Default Network Access	0	⚙️	➔
✓	Wired Low-Impact Mode		AND DEVICE-Device Type EQUALS All Device Types#Switches DEVICE-Mode EQUALS Model#Low-Impact	Default Network Access	0	⚙️	➔
✓	Default	Default policy set		Default Network Access	0	⚙️	➔

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

Authentication

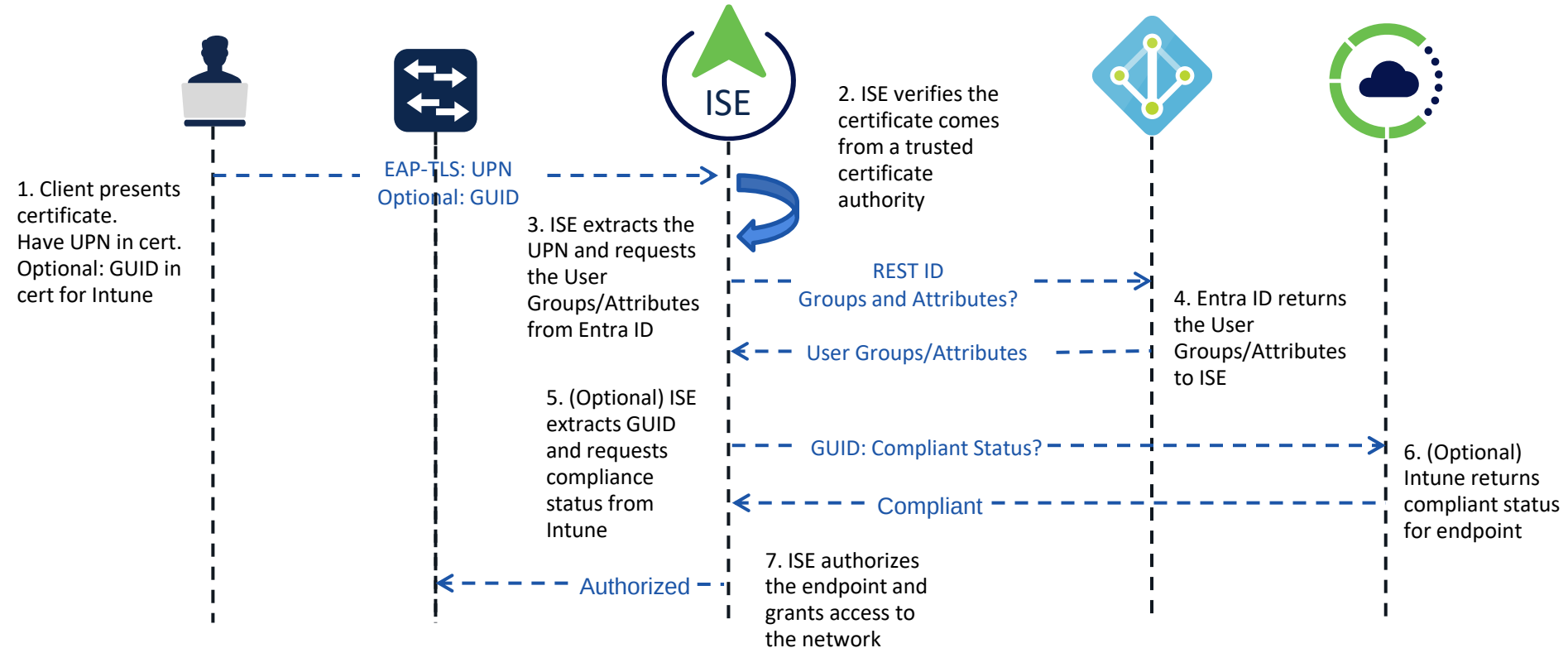
- Multiple authentication methods
 - 802.1x
 - Multiple 802.1X EAP methods simultaneously –
 - TEAP-EAP-TLS for Corporate Endpoints
 - EAP-TLS for supported printers and phones
 - PEAP-MSCHAPv2 for BYOD
 - Easy Connect
 - User authentication without 802.1x
 - Web Auth
 - MAB

Allowed Protocols

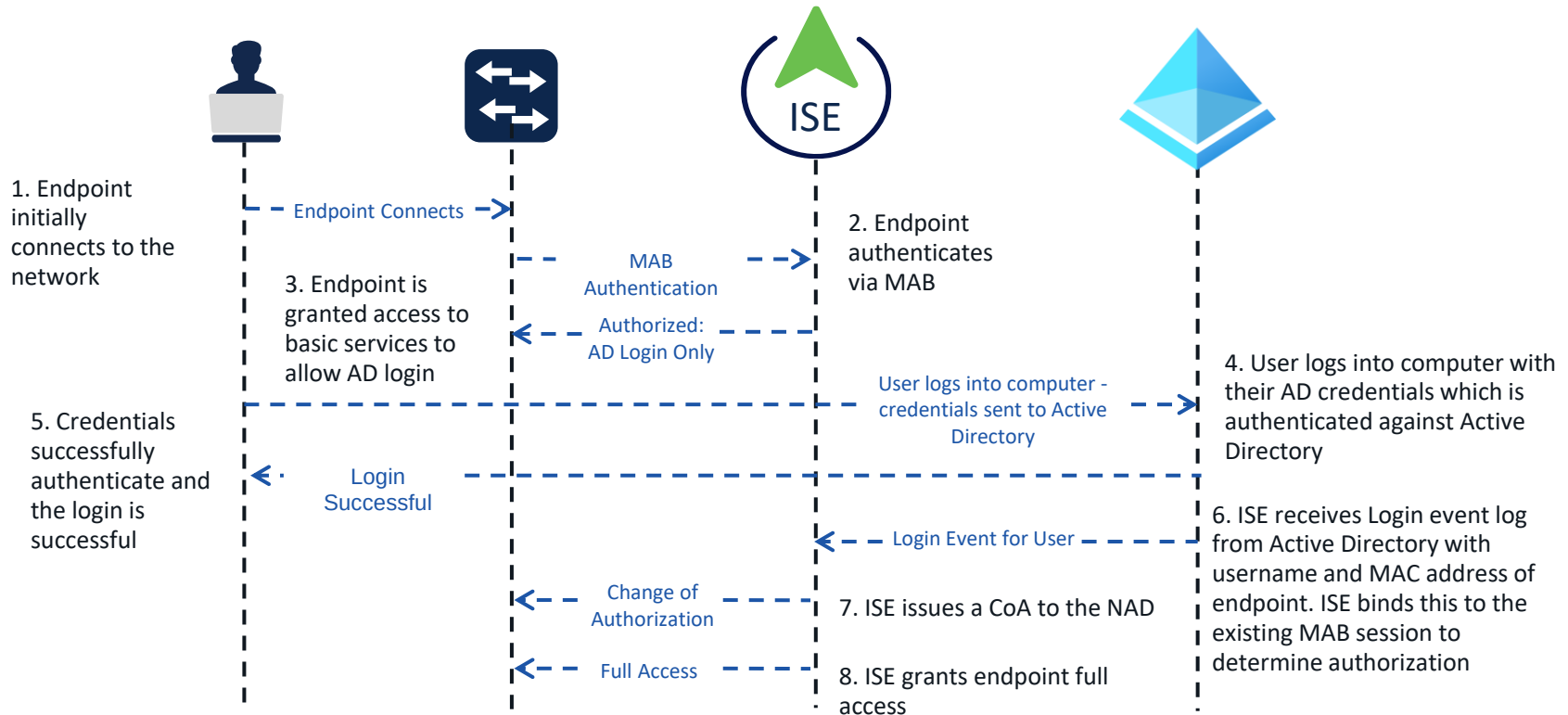
- ISE gives many options...
- Most common allowed protocols:
 - Process Host Lookup
 - EAP-TLS
 - PEAP-MSCHAPv2
 - PEAP-EAP-TLS
 - EAP-TEAP

Azure AD/Entra ID Support

EAP-TTLS and EAP-TLS
currently supported



Easy Connect



Migrating to 802.1x? Make it easier with Easy Connect

The screenshot displays the Cisco Identity Services Engine (ISE) web interface, specifically the 'Policy / Policy Sets' configuration page. The browser address bar shows the URL https://198.18.133.27/admin/#policy/policy_grouping_new. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, Work Centers, and Interactive Features. The main content area is titled 'Policy Sets' and includes a search bar and buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save'. Below these is a table listing the configured 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 TypesSwitches DEVICE-Mode EQUALS ModesMonitor	Default Network Access	0	⚙️	➔
✓	Wired Low-Impact Mode		AND DEVICE-Device Type EQUALS All Device TypesSwitches DEVICE-Mode EQUALS ModesLow-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 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 a "Dashboard" tab. A left sidebar contains navigation links: Bookmarks, Dashboard (selected), Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area features a "Summary" tab with six metrics: Total Endpoints (0), Active Endpoints (0), Rejected Endpoints (0), Anomalous Behavior (0), Authenticated Guests (0), and BYOD Endpoints (0). Below these are three sections: AUTHENTICATIONS, NETWORK DEVICES, and ENDPOINTS, each showing "No data available." with a large circular placeholder. At the bottom, there are sections for BYOD ENDPOINTS, ALARMS, and SYSTEM SUMMARY. The ALARMS section contains a table with columns for Severity, Name, Occu..., and Last Occurred. The SYSTEM SUMMARY section shows "1 node(s)" and "ISE".

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

Phased Posturing – Posture Policy

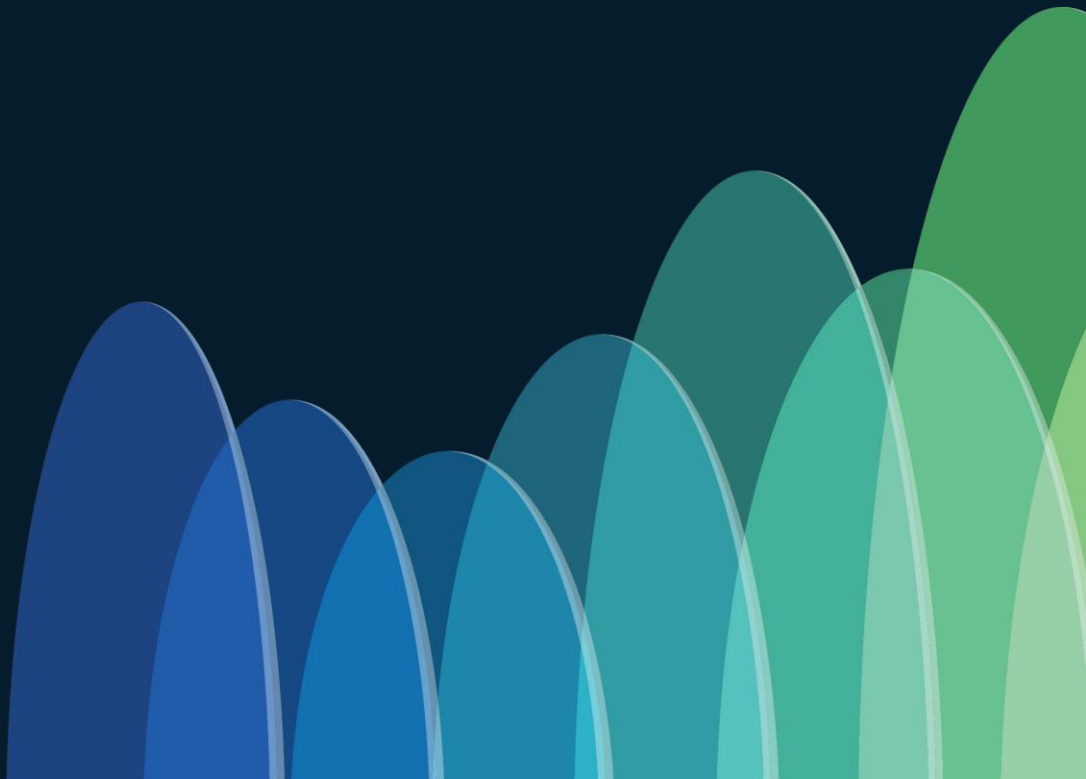
- Determines which requirements will be checked
- Conditions can be applied similar to the Client Provisioning policy
- Requirements may be added over time
- Requirements have three modes:
 - Mandatory
 - Optional
 - Audit

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 a "Dashboard" tab. The left sidebar contains a menu with options: Bookmarks, Dashboard (selected), Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area is divided into several sections:

- Summary** (selected tab): Displays a row of six metrics, each with a large blue number "0" and a circular progress indicator:
 - Total Endpoints
 - Active Endpoints
 - Rejected Endpoints
 - Anomalous Behavior
 - Authenticated Guests
 - BYOD Endpoints
- Authentications**: A section with a table showing authentication data. The table has columns for Identity Store, Identity Group, Network Device, and Failure Reason. The content area shows "No data available." and a large circular progress indicator.
- Network Devices**: A section with a table showing network device data. The table has columns for Device Name, Type, and Location. The content area shows "No data available." and a large circular progress indicator.
- Endpoints**: A section with a table showing endpoint data. The table has columns for Profile and Logical Profile. The content area shows "No data available." and a large circular progress indicator.
- BYOD Endpoints**: A section with a table showing BYOD endpoint data. The table has columns for Type and Profile. The content area shows "No data available." and a large circular progress indicator.
- Alarms**: A section with a table showing system alarms. The table has columns for Severity, Name, Occu..., and Last Occurred. The content area shows a table with one row: "Configuration Chang..." with a severity of 7354 and a time of 3 mins ago.
- System Summary**: A section showing a summary of the system. It displays "1 node(s)" and "All 24HR".

Tuning Policy Sets



Policy Logic

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

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

- Think about it in non-technical terms:
 - If {the user is in the marketing department} then {let him/her on the network}
 - If {the user is using their laptop from home} then {only give them internet access}
- Think about what you're trying to achieve in non-technical terms first, then create the policy in ISE using technical conditions/results that accomplish it
- Similar to an ACL: First matched rule

Policy Conditions

- AND – Both Conditions MUST match
 - “SSID is Corp-WiFi AND endpoint needs to be authenticating with wireless 802.1”

Editor

The screenshot shows the Cisco Policy Editor interface. On the left is a vertical sidebar with a red box highlighting the 'AND' operator. The main area contains two conditions:

- Condition 1: A wireless icon, a text field containing 'Normalised Radius:SSID', a dropdown menu set to 'Equals', and a text field containing 'Corp-WiFi'. A blue grid icon is on the right.
- Condition 2: A document icon, a text field containing 'Wireless_802.1X', and a blue grid icon on the right.

Below the conditions is a dashed box for adding new conditions, with a '+' icon on the left and 'NEW | AND | OR' options in the center. At the bottom, there is a link 'Set to 'Is not'', a 'Duplicate' button, and a 'Save' button.

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

Wired_MAB

Wired_802.1X

OR ▼

+ NEW AND OR

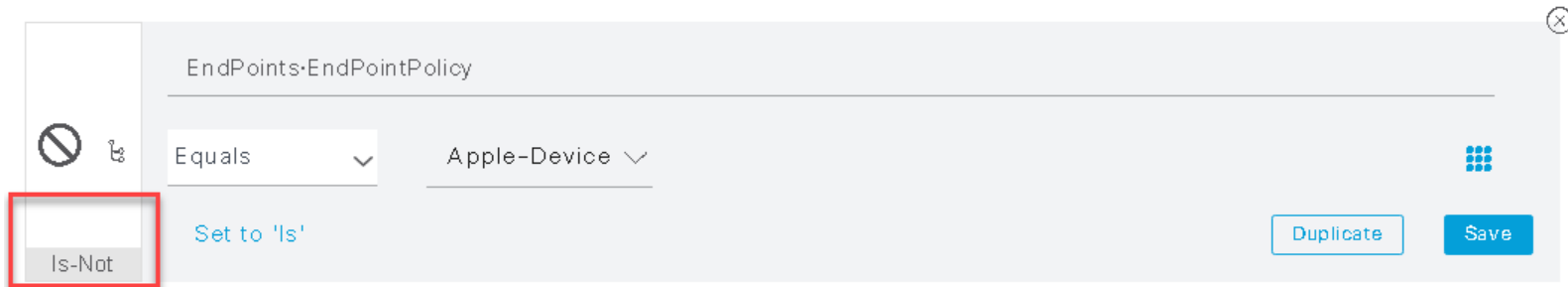
Set to 'Is not'

Duplicate Save

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. On the left is a sidebar with a 'No' icon (a circle with a diagonal line) and a red box highlighting the 'Is-Not' option. The main area is titled 'EndPoints-EndPointPolicy' and contains a configuration row with 'Equals' and 'Apple-Device' dropdown menus. Below these is a 'Set to 'Is'' link. On the right 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

The screenshot shows the Cisco Policy Editor interface with three conditions listed vertically. The first condition is highlighted with a blue box, the second with a green box, and the third with a black box. Logical operators 'AND' and 'OR' are visible between the conditions.

- Condition 1 (Blue Box):** Network Access-EapChainingResult. Operator: Equals. Value: User and machine both succeeded.
- Condition 2 (Green Box):** ad-2016-ExternalGroups. Operator: Equals. Value: dcloud.cisco.com/Builtin/Corporate. This condition is part of an OR group.
- Condition 3 (Black Box):** ad-2016-ExternalGroups. Operator: Equals. Value: dcloud.cisco.com/Builtin/Enterprise.
- Condition 4 (Black Box):** DEVICE-Location. Operator: Is-Not. Value: All Locations#San Francisco.

A little history lesson...

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes the Cisco logo, the title "Identity Services Engine", and tabs for Home, Operations, Policy (selected), and Administration. Below the navigation bar are icons for Authentication, Authorization (selected), Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The main content area is titled "Authorization Policy" and includes a description: "Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order." A dropdown menu labeled "First Matched Rule Applies" is set to "First Matched Rule Applies". Below this is a section for "Exceptions (0)" and a "Standard" section. The "Standard" section contains a table of authorization rules.

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

At the bottom of the table are "Save" and "Reset" buttons.

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
				<input type="text" value="Search"/>	
	✓	VPN-Policy-Set		AND DEVICE-Device Type EQUALS All Device Types#VPN-Concentrators VPN-list	• Default Network Access
	✓	TC-NAC		AND DEVICE-Location EQUALS Location#All Locations#Global#North America#USA#California#SJC01	• Default Network Access
	✓	Dot1x-AzureAD		AND ca#USA#California#SJC01	• Default Network Access
	✓	MDM		DEVICE-Location EQUALS All Locations#My-Territory#APAC-Region#India#Karnataka#Bengaluru MDM-endpoints	• Default Network Access
	✓	BYOD		AND DEVICE-Location EQUALS North America#USA#California#SJC01 Win-BYOD	• Default Network Access
	✓	Guest-Access		OR DEVICE-Device Type EQUALS All Device Types#Wireless Radius-Service-Type EQUALS Call Check Windows-guest	• Default Network Access

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

Policy Set Flow

Policy Sets → Dot1x-AzureAD

Reset

Reset Policyset Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Serve
Search				
✓	Dot1x-AzureAD		AND <ul style="list-style-type: none">DEVICE-Location EQUALS North America#USA#California#SJC01windows-dot1x-azure	• Default Network Access

Authentication Policy (3)

+ Status	Rule Name	Conditions	Use
Search			
✓	Dot1x-TLS	Network Access-EapAuthentication EQUALS EAP-TLS	
✓	Dot1x-TTLS	Network Access-EapTunnel EQUALS EAP-TTLS	<ul style="list-style-type: none">AzureAD> Options

Result: Credentials authenticated against Azure AD

Policy Set Flow

▼ Authorization Policy (3)

				Results
+ Status	Rule Name	Conditions		Profiles
<div>Search</div>				
✓	HR_Policy		AzureAD·ExternalGroups EQUALS HRGroup	<div>• Full-Access</div>
✓	Employee_Policy		AzureAD·ExternalGroups EQUALS EmployeeGroup	<div>• Full-Access</div>
✓	Default			<div>• DenyAccess</div>

Result: Endpoint is granted full access

Result: Endpoint is granted full access

Grouping Policy Sets

There is more than one way to make an omelette!

- Many ways to overcomplicate, but many ways to simplify
- Embrace the KISS principle!
- Commonly two trains of thought:
 1. Policy Sets based on device type, location, and/or SSID:
 - Network Device Group: Switches, Wireless Controller, VPN
 - (Optional) Network Device Group Location: HQ
 - (Optional) SSID: Corp-Guest
 2. Policy Sets based Use-Case:
 - Use-Case: Wired 802.1x, Wireless 802.1x, Wired MAB, Wireless MAB, etc
 - (Optional) Network Device Group Location: HQ
 - (Optional) SSID: Corp-Guest

Policy Sets

Option 1 Example

Policy Sets

[Reset](#)

[Reset Policyset Hits](#)

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
				<input type="text" value="Search"/>	
	✓	San Francisco Wired Access		AND <div> <div> DEVICE-Device Type EQUALS All Device Types#Switches </div> <div> DEVICE-Location EQUALS All Locations#San Francisco </div> </div>	Default Network Access ✎ +
	✓	San Jose Wired Access		AND <div> <div> DEVICE-Device Type EQUALS All Device Types#Switches </div> <div> DEVICE-Location EQUALS All Locations#San Jose </div> </div>	Default Network Access ✎ +
	✓	Guest SSID		AND <div> <div> DEVICE-Device Type EQUALS All Device Types#Wireless Controllers </div> <div> Radius-Called-Station-ID CONTAINS Corp-Guest </div> </div>	Default Network Access ✎ +
	✓	Corp 802.1x		AND <div> <div> DEVICE-Device Type EQUALS All Device Types#Wireless Controllers </div> <div> Radius-Called-Station-ID CONTAINS Corp-Dot1x </div> </div>	Default Network Access ✎ +
	✓	VPN		DEVICE-Device Type EQUALS All Device Types#VPN	Default Network Access ✎ +

Policy Sets

Option 2 Example

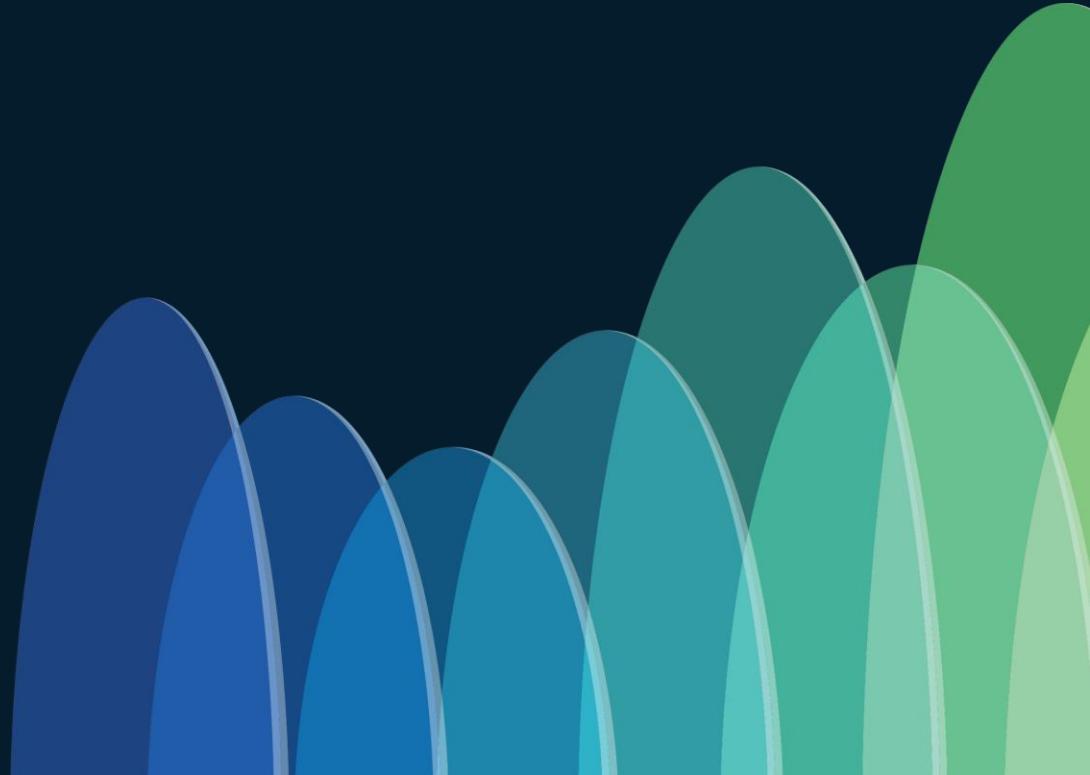
Policy Sets

[Reset](#)

[Reset Policyset Hitc](#)

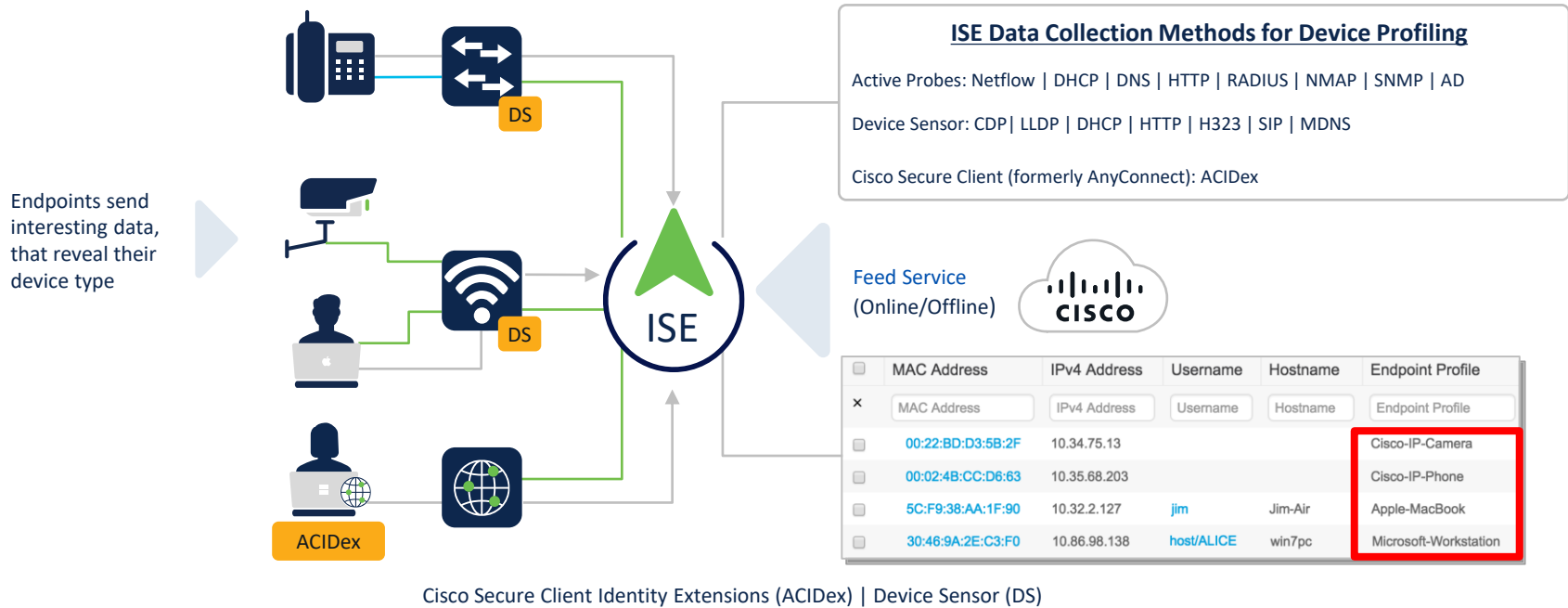
	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
				<input type="text" value="Search"/>	
	✓	San Francisco Wired 802.1		AND <div> <div> DEVICE-Location EQUALS All Locations#San Francisco </div> <div> Wired_802.1X </div> </div>	Default Network Access ✎ +
	✓	San Francisco Wired MAB		AND <div> <div> DEVICE-Location EQUALS All Locations#San Francisco </div> <div> Wired_MAB </div> </div>	Default Network Access ✎ +
	✓	San Jose Wired 802.1X		AND <div> <div> DEVICE-Location EQUALS All Locations#San Jose </div> <div> Wired_802.1X </div> </div>	Default Network Access ✎ +
	✓	San Jose Wired MAB		AND <div> <div> DEVICE-Location EQUALS All Locations#San Jose </div> <div> Wired_MAB </div> </div>	Default Network Access ✎ +
	✓	Guest SSID		AND <div> <div> DEVICE-Device Type EQUALS All Device Types#Wireless Controllers </div> <div> Radius-Called-Station-ID CONTAINS Corp-Guest </div> </div>	Default Network Access ✎ +
	✓	Corp 802.1x		AND <div> <div> DEVICE-Device Type EQUALS All Device Types#Wireless Controllers </div> <div> Radius-Called-Station-ID CONTAINS Corp-Dot1x </div> </div>	Default Network Access ✎ +
	✓	VPN		DEVICE-Device Type EQUALS All Device Types#VPN	Default Network Access ✎ +

The Power of Profiling



Endpoint Profiling – Visibility Data Sources

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



Enabling Probes on ISE

The screenshot displays the Cisco Identity Services Engine (ISE) Dashboard. The top navigation bar includes the Cisco logo, the text "Identity Services Engine", and a "Dashboard" label. A search bar and several notification icons are on the right. Below the navigation bar, a "Summary" tab is selected, showing a row of six metrics: Total Endpoints, Active Endpoints, Rejected Endpoints, Anomalous Behavior, Authenticated Guests, and BYOD Endpoints. All metrics are currently at 0. To the right of these metrics is a "Manage" dropdown and a "Compl" link. Below the metrics row are three main sections: "AUTHENTICATIONS", "NETWORK DEVICES", and "ENDPOINTS". Each section has a table with columns for "Identity Store", "Identity Group", "Network Device", and "Failure Reason" (for Authentications); "Device Name", "Type", and "Location" (for Network Devices); and "Profile" and "Logical Profile" (for Endpoints). All three sections display "No data available." and a large gray circle. At the bottom, there are three smaller sections: "BYOD ENDPOINTS", "ALARMS", and "SYSTEM SUMMARY". The "BYOD ENDPOINTS" section has columns for "Type" and "Profile" and also shows "No data available.". The "ALARMS" section has columns for "Severity", "Name", "Occu...", and "Last Occurred". The "SYSTEM SUMMARY" section shows "1 node(s)" and "ISE".

Profiling Logic

Profiler Policy

* Name Apple-Device Description Generic policy for all Apple devices

Policy Enabled ☒

* Minimum Certainty Factor 10 (Valid Range 1 to 65535)

* Exception Action NONE ▼

* Network Scan (NMAP) Action OS-scan ▼

Create an Identity Group for the policy ☐ Yes, create matching Identity Group
☒ No, use existing Identity Group hierarchy

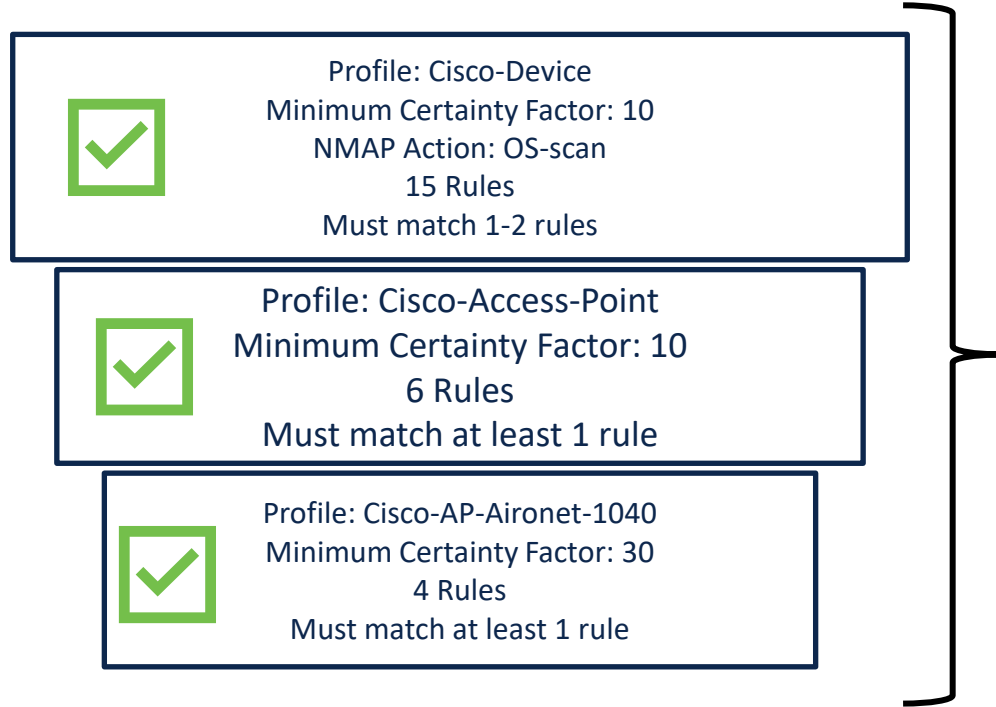
Parent Policy ***NONE***

* Associated CoA Type Global Settings ▼

System Type Cisco Provided

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

Profile Hierarchy

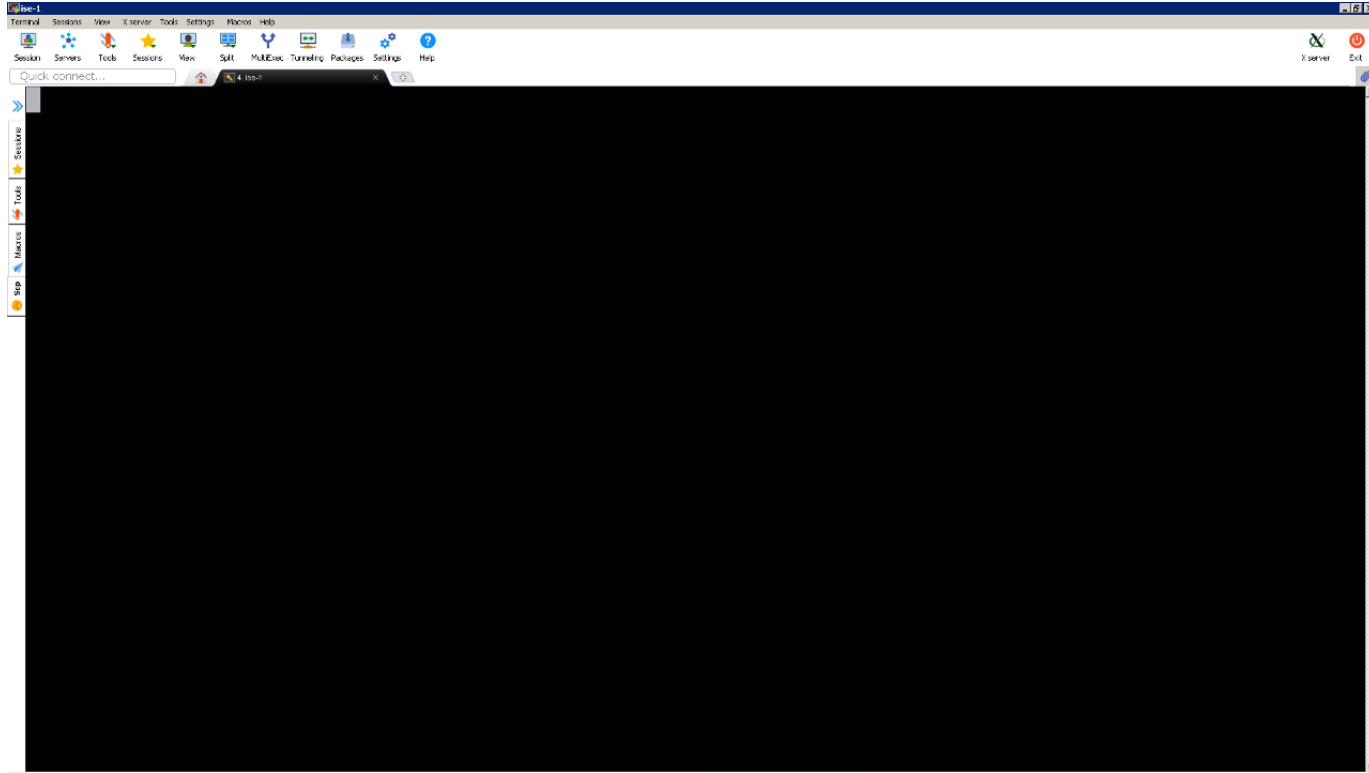


In order to profiled as a Cisco-AP-Aironet-1040, the endpoint must match 3-4 unique rules in total based on default policies built into ISE

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

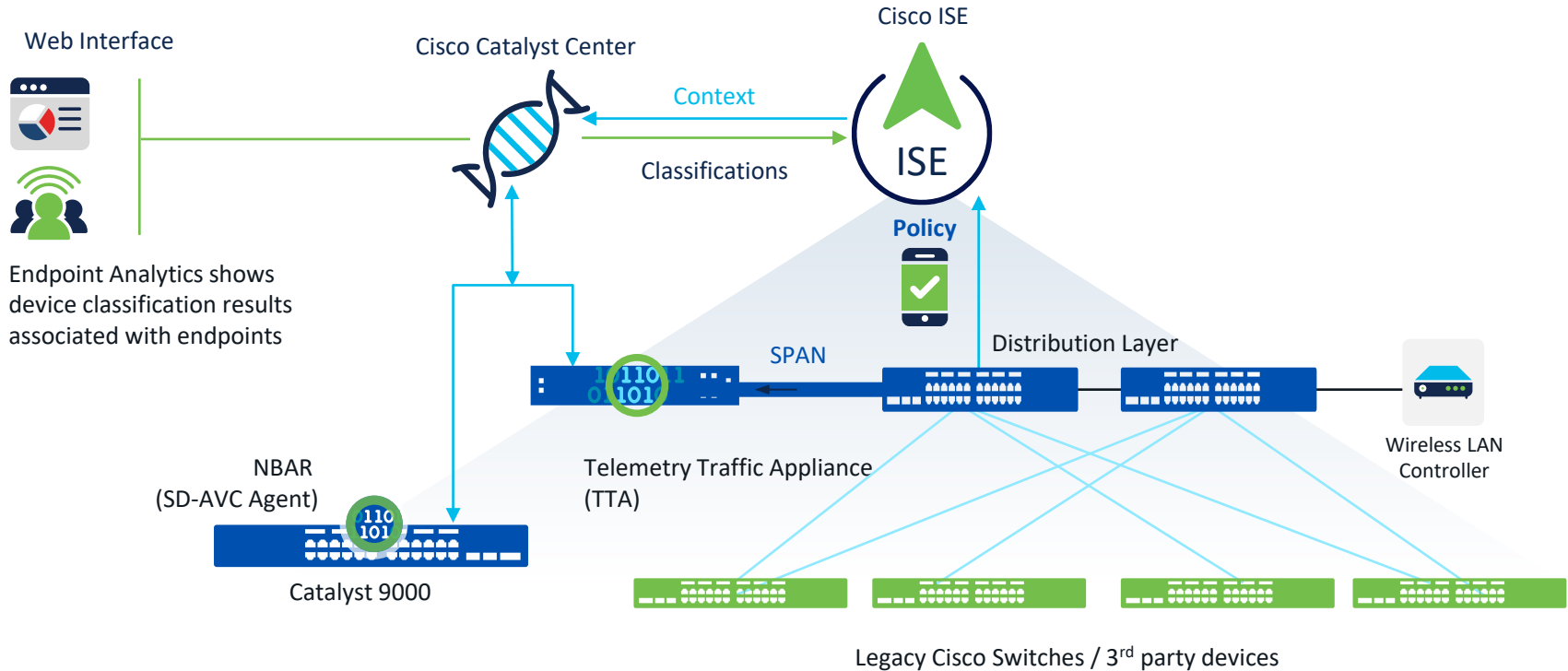
The screenshot shows an Excel spreadsheet with the following data:

	host-name	MatchedPolicy	OUI	sysContact	sysLocation	sysName	hrDeviceDescr	sysDescr	9100-
1		HP-LaserJet-Printer	Hewlett Packard				HP LaserJet 400 MFP M425dn	HP ETHERNET MULTI-ENVIRONMENT,PID:HP LaserJet 400 MFP M425dn	jetdirect
2		HP-LaserJet-Printer	Hewlett Packard				HP LaserJet 400 MFP M425dn	HP ETHERNET MULTI-ENVIRONMENT,PID:HP LaserJet 400 MFP M425dn	jetdirect
3	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
4	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

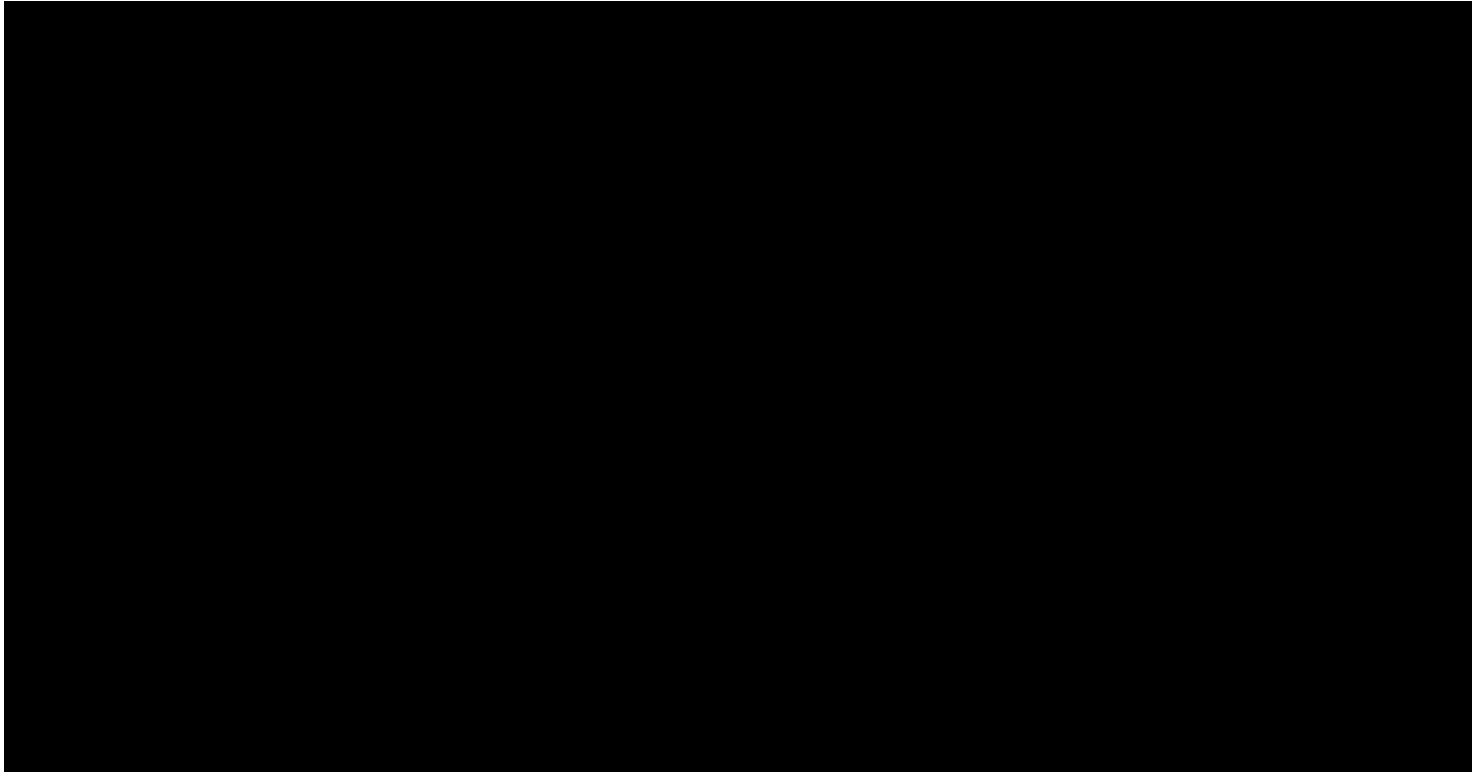
Profiling Attributes

- 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

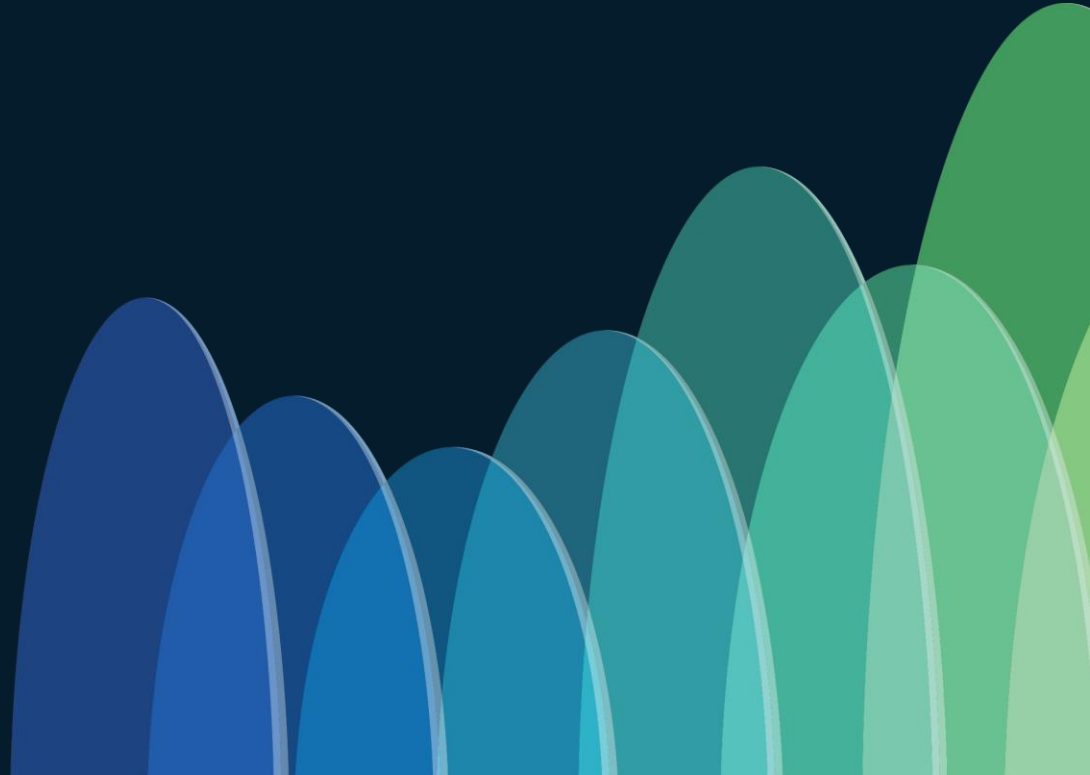
Cisco AI Analytics



AI Endpoint Analytics on ISE



Integrations



Platform Exchange Grid (pxGrid)

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



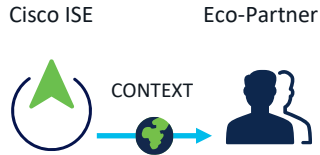
5. ISE should now list the pxGrid client in the pxGrid dashboard and share session context with the client by default. In the pxGrid dashboard, this client can also be assigned additional permissions by being added pxGrid groups such as ANC

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

Context Sharing with pxGrid

Eco system partnership to enrich, exchange context and enact

Context to Partner



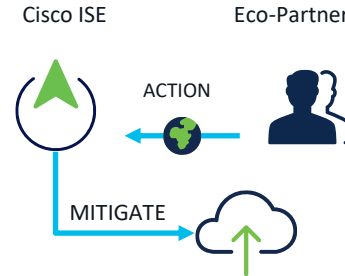
ISE makes Customer IT Platforms User/Identity, Device and Network Aware

Enrich ISE Context



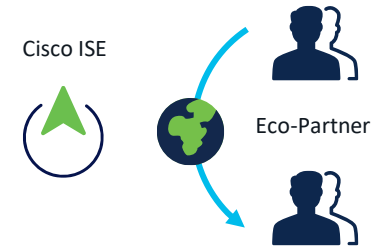
Enrich ISE context. Make ISE a better Policy Enforcement Platform

Threat Mitigation



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

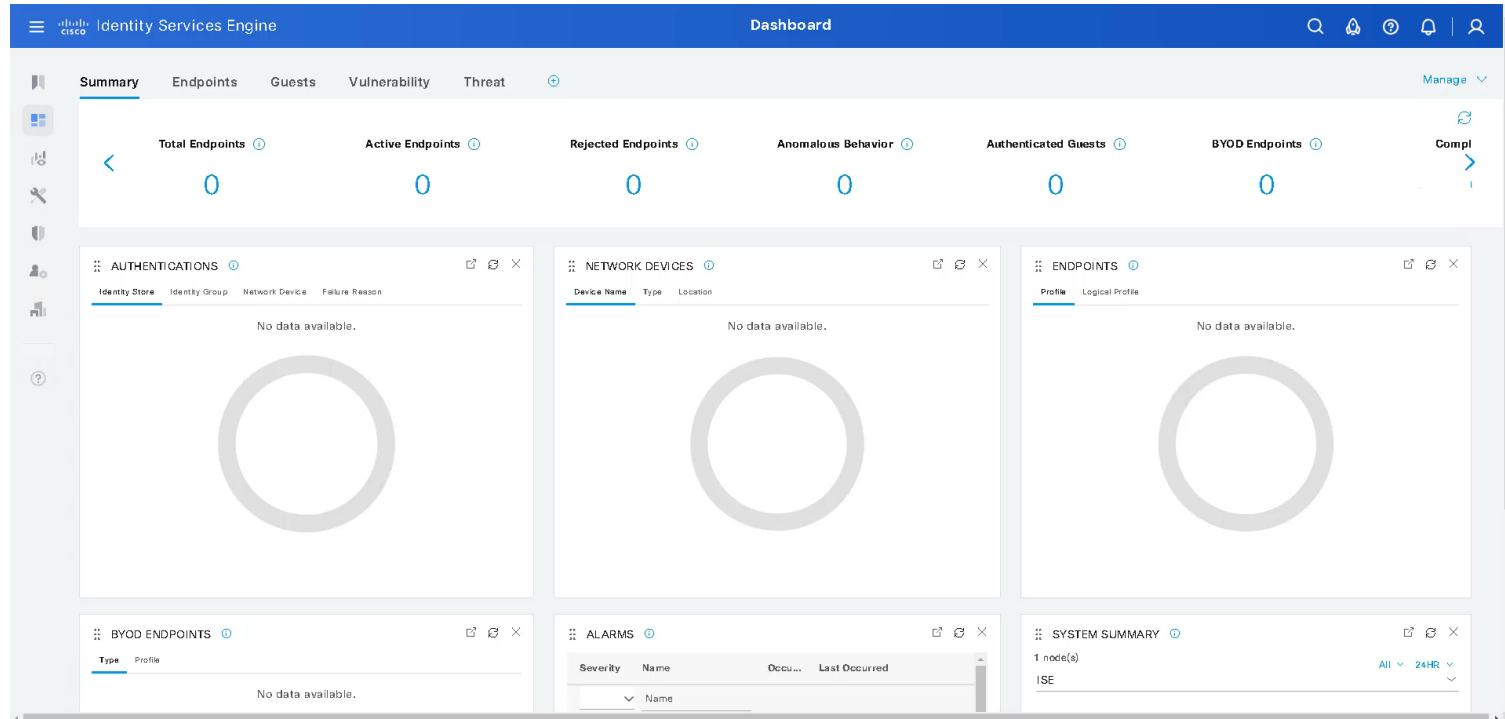
Context Brokerage



ISE 2.2+

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

PxGrid/ANC Policies in ISE



Other pxGrid Use-Case Examples

- Secure Firewall
 - Share IP-to-Username binding, SGT, and profile information with Secure Firepower
 - Create ACPs in Firepower based on profile, identity/AD Group, and SGT
 - Quarantine endpoints from ISE based on detections from Secure Firewall
- Secure Network Analytics (SNA)
 - Shares IP-to-Username binding, SGT, and profile information with SNA
 - Create network-based detection policies in SNA that will quarantine or change access endpoint access level through ISE
- And much more...

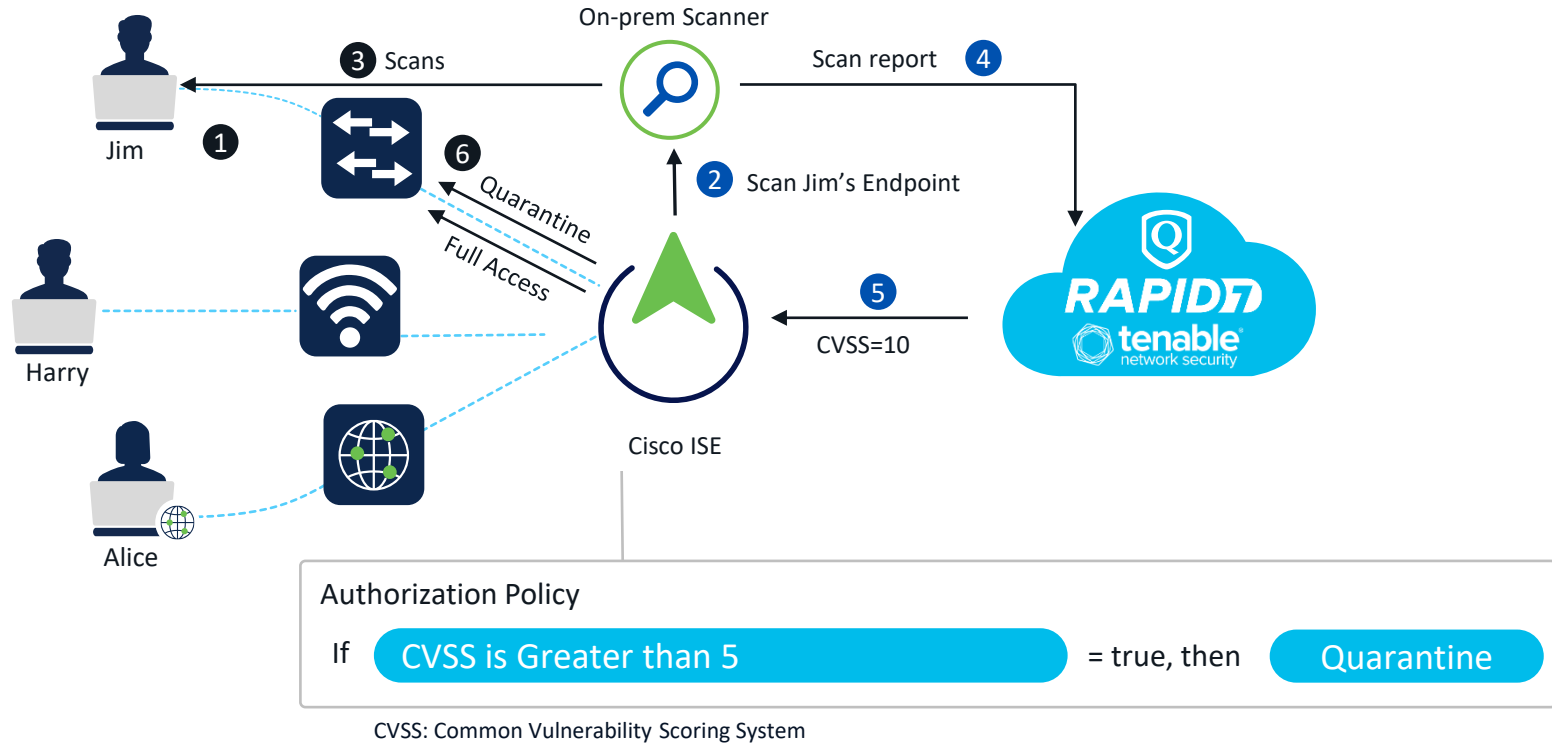
pxGrid Integration Tips

- Start with integrating to share context out:
 - Gives information to a pxGrid subscriber such as username-to-IP binding, profile, SGT, etc
- (Optional) Migrated data in for richer profiling:
 - Custom third party attributes don't build the profiles themselves
 - Will still need to build profiles
 - Leverage AI Analytics to help
- Rapid Threat Containment:
 - Automates the change of access based on a trigger from a pxGrid subscriber
 - Start with the “low hanging fruit” – Don't need to quarantine everything

Threat-Centric NAC (TC-NAC)

- Integrates with third-party vulnerability scanners such as Qualys, Rapid7, and Tenable
 - Trigger an endpoint scan
 - Ingest vulnerability information into ISE
- Integrates with Cisco Secure Endpoint and Cognitive Threat Analytics
 - Ingests threat information about an endpoint
- Contextual information stored under endpoint attributes as well as Context Visibility dashboards to see overview of the data

Vulnerability Assessment with Threat-Centric NAC

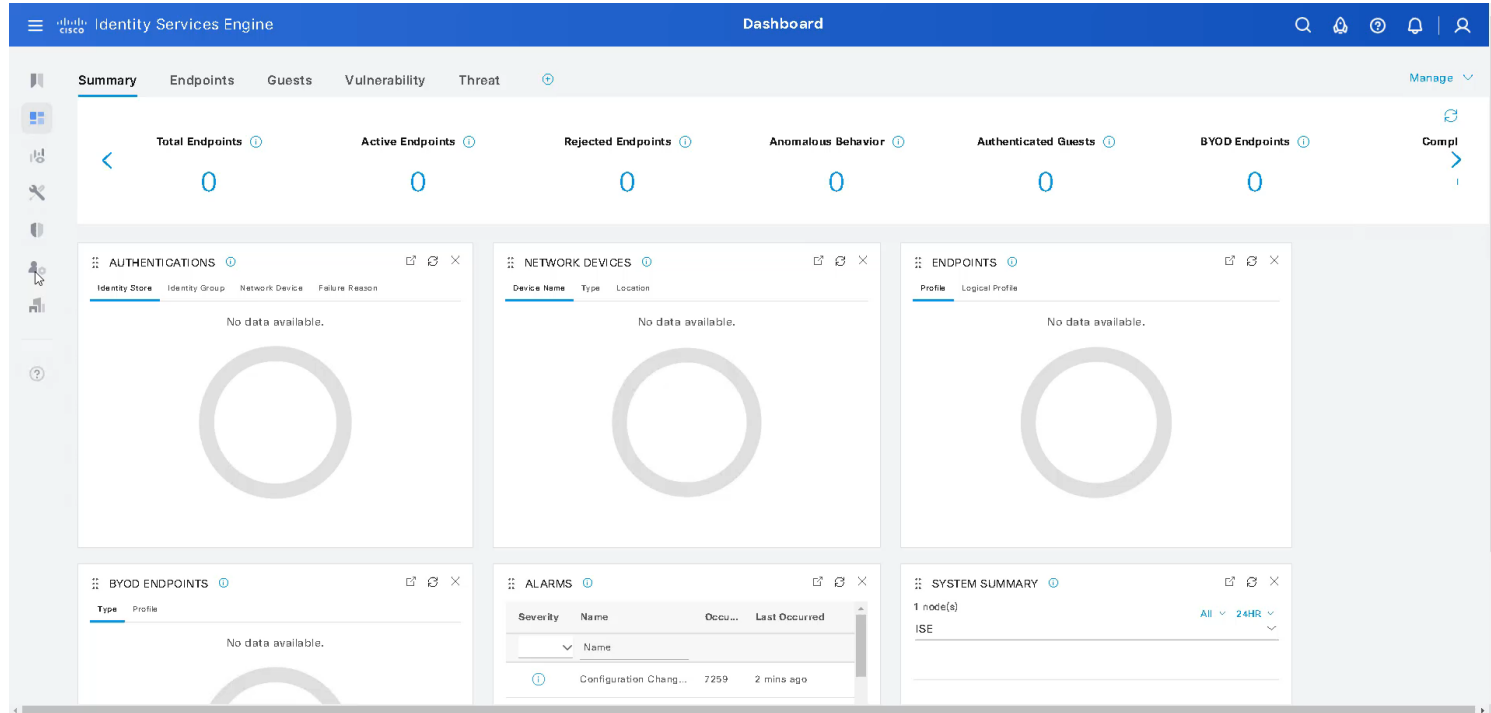


MDM Integrations

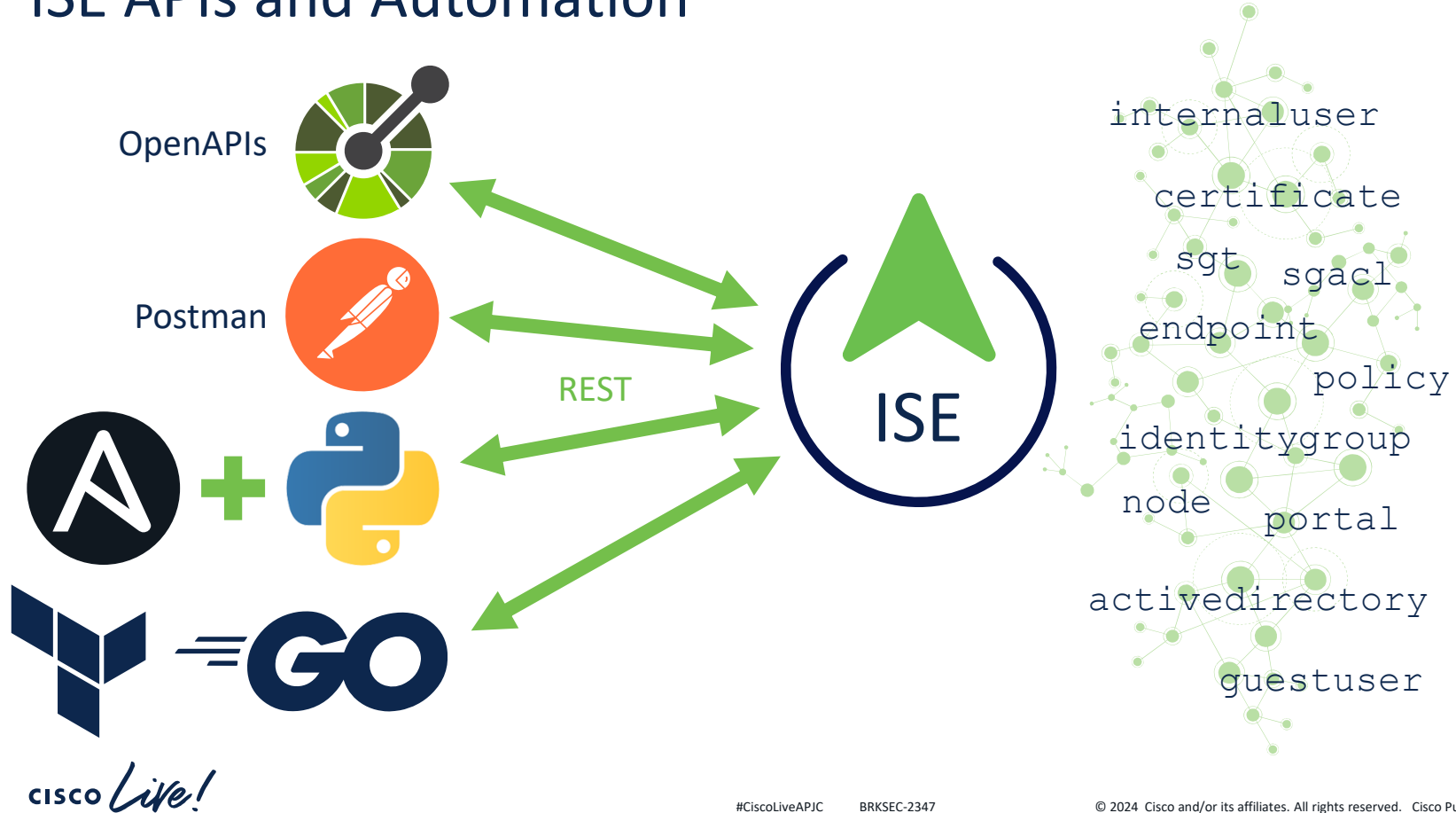
- Integrates with many third-party MDM
- Onboard endpoints to MDM through ISE
- Control and visibility into non-corporate
- MDM posture checks in ISE authorization

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

MDM Integration Example



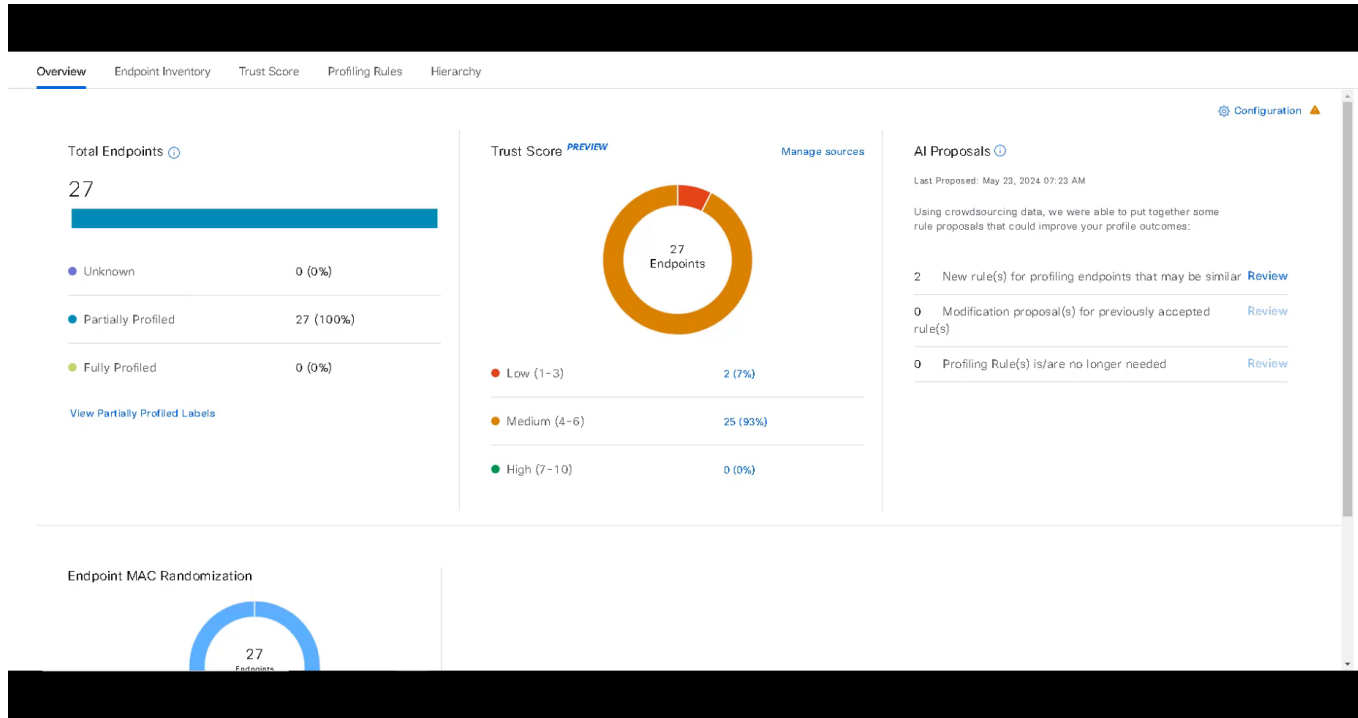
ISE APIs and Automation



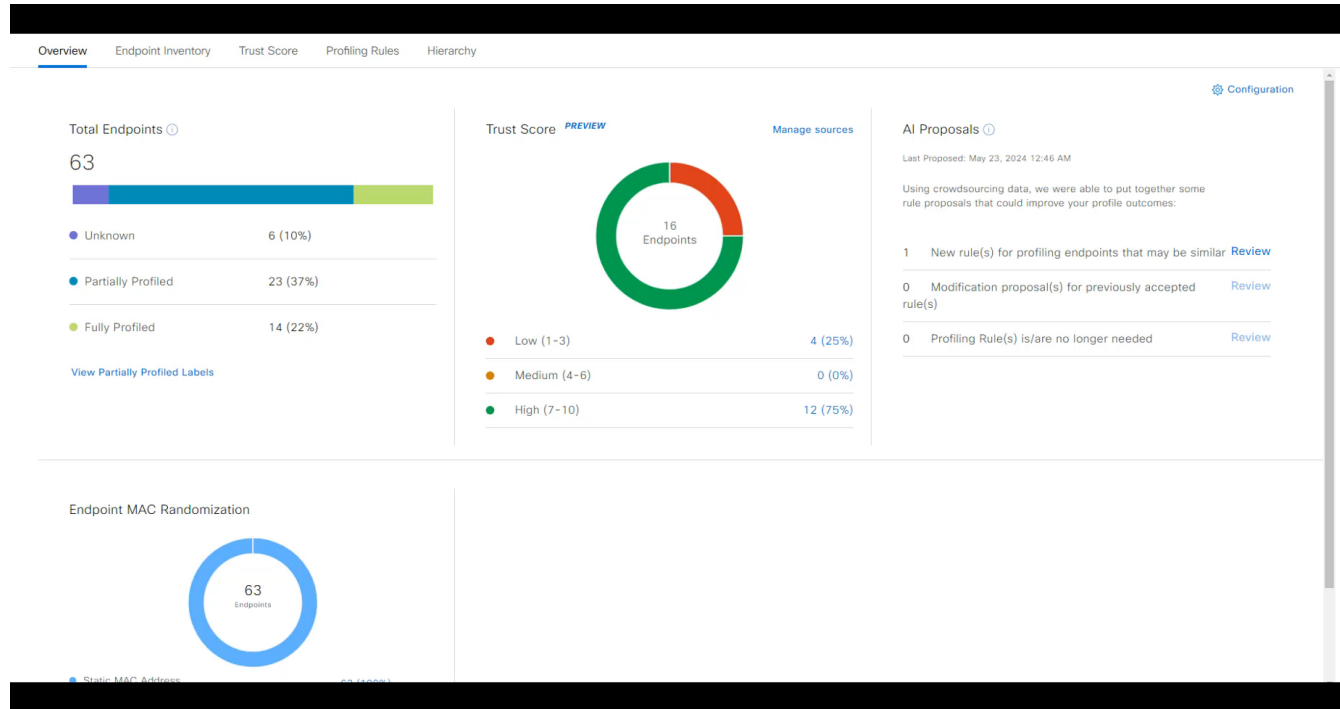
Integration Example: Catalyst Center and ISE

- Catalyst Center supercharges AI Analytics
 - Granular profile recommendations utilizing telemetry and DPI
- Zero trust: Trust Score
 - Score based on:
 - Change in profile label
 - Traffic pattern anomaly
 - Unauthorized ports and weak credentials
 - and more
 - Quarantine low scoring endpoints via ISE integration
- Configure Trustsec SGACLs and policy utilizing historic traffic patterns

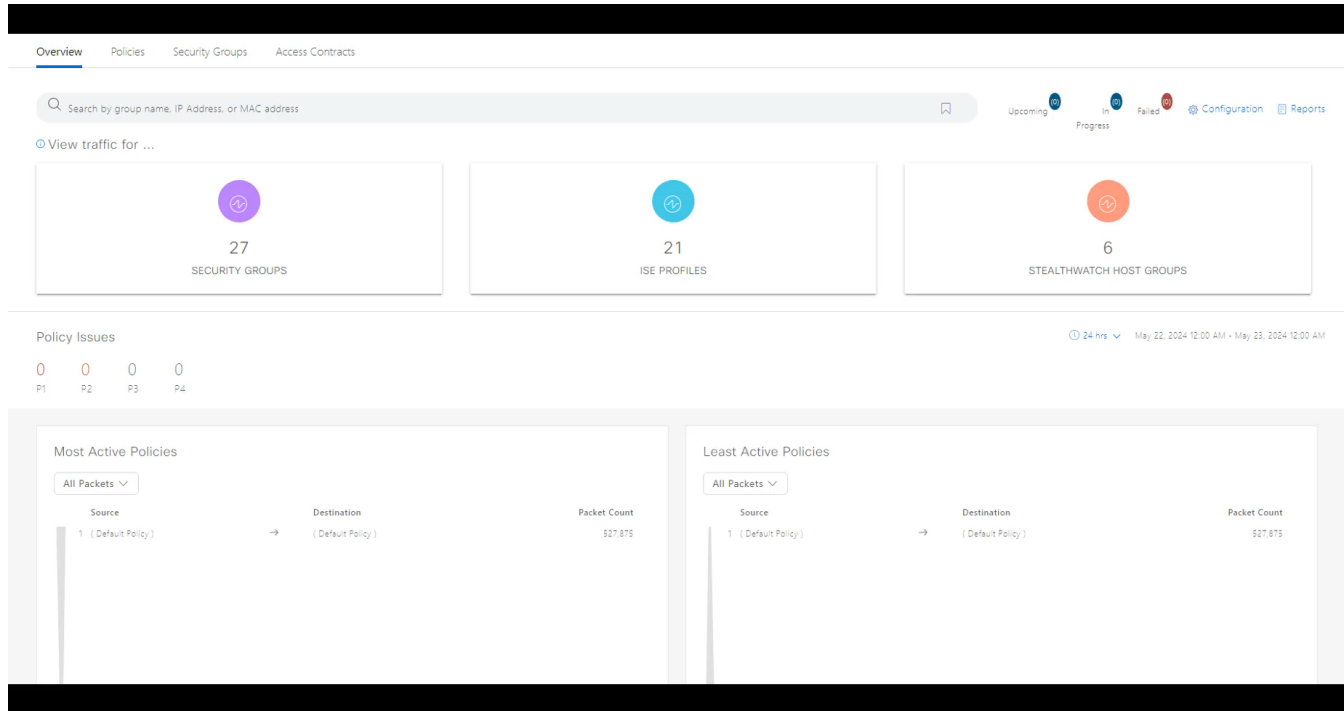
Catalyst Center Trust Score and Spoofing Detection



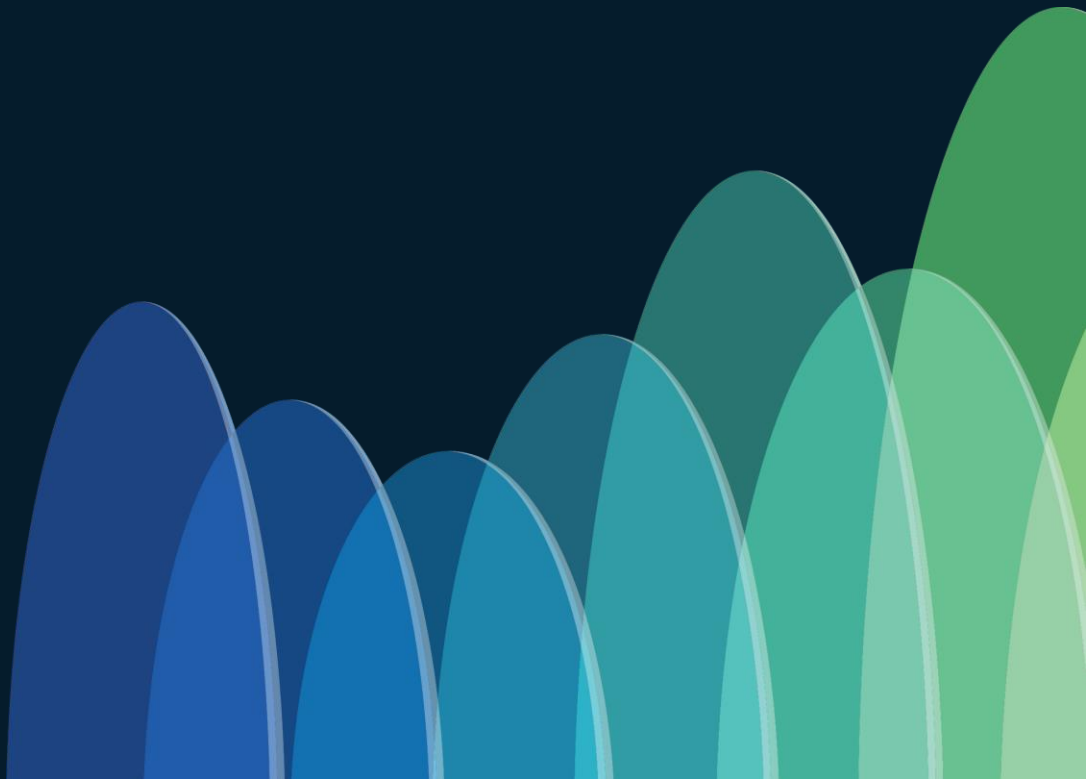
Catalyst Center AI Endpoints Telemetry



TrustSec Policies with Catalyst Center Integration



Post-Deployment



Supporting your ISE Deployment

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

Supporting your ISE Deployment

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

Supporting your ISE Deployment

- Utilized built-in ISE roles for Helpdesk, NOC, etc
- Train your support
 - Avoid being called for every issue
 - Playbook for common issues for:
 - NOC
 - Helpdesk
- Know the tools you have to troubleshoot and monitor your deployment
 - Create your playbook for your support with these tools
 - Hidden Troubleshooting slides in this presentation for the playbook

Troubleshooting Endpoint Issues

- ISE –
 - **Operations>RADIUS>Live Logs** - Click the Details for the failed authentication
 - **Operations>Troubleshooting> Diagnostic Tools>Endpoint Debug** – Add MAC address and start debug
- Endpoint –
 - Check the supplicant configuration for the endpoint
 - Check that all necessary certificates are installed on the endpoint
 - Check the OS version
 - Check if User, Computer or User and Computer authentication is picked
 - For wired access, ensure that the Wired AutoConfig service is turned on
 - Check if endpoint is joined to AD domain or BYOD onboarded

Troubleshoot Network Access Device Issues

- ISE –
 - **Administration>Network Resources>Network Devices** – Check to see if NAD exists and shared secret
 - **Operations>RADIUS>Live Logs** – Check to see alerts for Misconfigured Network Devices and RADIUS drops
- Network Access Device –
 - Check OS version/model - Are similar NADs working with same OS/model?
 - Check configuration – Is it running the same template as others with same OS/model?
 - Are only some endpoints on the device failing? Check to see if CoA is working
 - Debug commands
 - RADIUS/TACACS source interface defined?

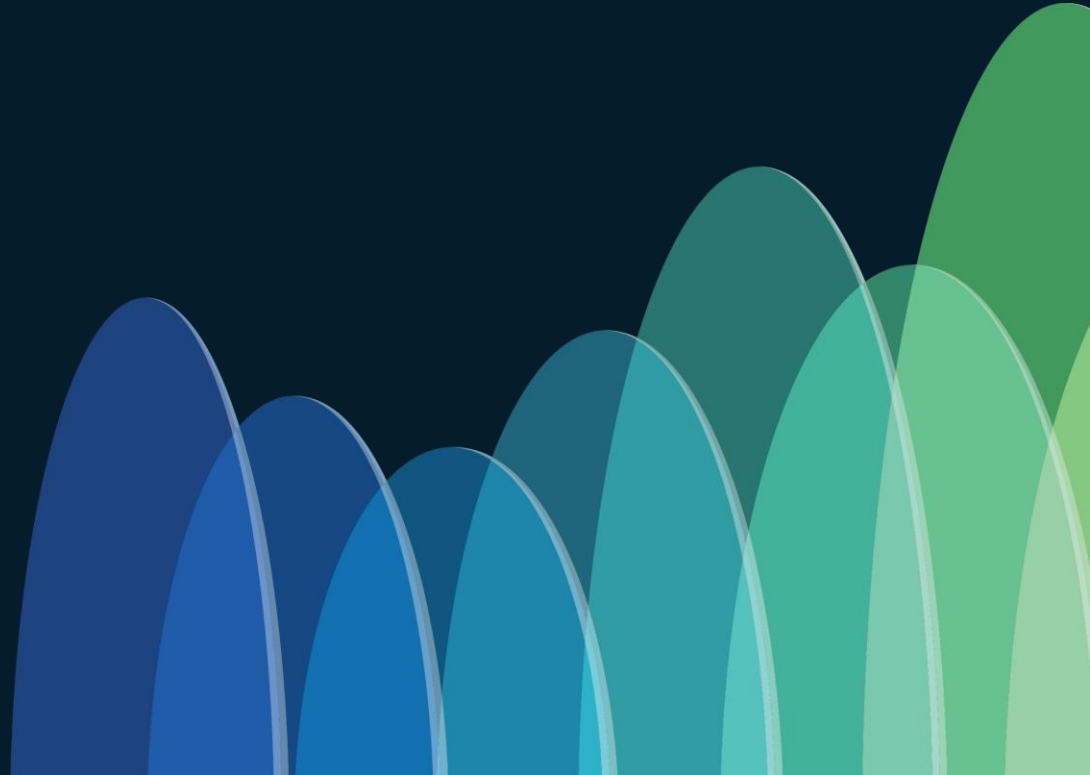
Troubleshooting Network Issues

- 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

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?

Conclusion



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

Helpful Links and Training

- CiscoPress SISE Book - <https://tinyurl.com/ciscopress-sise>
- ISE Scalability Guide - <https://tinyurl.com/ise-scale>
- ISE Loadbalancing Guides - <https://tinyurl.com/ise-loadbalancing>
- ISE NAD Compatability Matrix - <https://tinyurl.com/ise-compatibility>
- ISE Mega-list of Integration/Configuration Guides - <https://cs.co/ise-guides>
- Cisco Security Technical Alliance Partners - <https://cisco.com/go/csta>
- Deploy ISE in Cloud - <https://tinyurl.com/ise-cloud>
- ISE APIs and Automation - <https://github.com/CiscoISE>

Helpful Links and Training

- ISE Switch Deployment Guide - <https://tinyurl.com/ise-switch-guide>
- ISE WLC Deployment Guide - <https://tinyurl.com/ise-wlc-config>
- ISE Catalyst 9800 Wireless Guide - <https://tinyurl.com/ISE-9800-Guide>
- Profile Packs:
 - Medical NAC 2.0 Profiles - <https://tinyurl.com/ise-medical-nac-2>
 - Automation and Control Profiles - <https://tinyurl.com/ise-automation-library>
 - Industrial Network Director IoT Profiles - <https://tinyurl.com/ind-profiles>
 - Windows-Embedded IoT Profiles - <https://tinyurl.com/windows-embedded>
- ISE Licensing - <https://cs.co/ise-licensing>

Helpful Links and Training

- TrustSec Troubleshooting Guide - <https://tinyurl.com/TS-Troubleshooting>
- ISE Webinars - <https://cs.co/ise-webinars>
- ISE Community - <https://cs.co/ise-community>
- Cisco's ISE YouTube Channel - <https://cs.co/ise-videos>

Helpful Links and Training

- Network-Node Blog – <https://www.network-node.com>
- My ISE Videos - <https://tinyurl.com/KM-ISE-Videos>
- Labminutes ISE Configuration Videos - <https://tinyurl.com/LM-ISE>
- Aaron Woland's ISE Blog Posts – <https://tinyurl.com/Woland-ISE>
- Brad Johnson's ISE Support Blog - <https://www.ise-support.com>
- Steve McNutt's Blog –
 - PKI for Network Engineers - <https://tinyurl.com/PKI-for-NE>
 - ISE Posts - <https://tinyurl.com/McNutt-ISE>

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



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



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC