

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

ISE Deployment Staging and Planning

Katherine McNamara – Technical Solutions Architect
@kmcnam1
BRKSEC-2347

CISCO *Live!*

#CiscoLive

A little about me....



- Over 10 years in the technology field
- Bachelors of Science and Masters of Science in IT Security
- 2x CCIEs (Data Center + Security), CISSP, and various other industry certifications
- Co-organize for the largest Cisco Meetup study group – Routergods
- Network-node.com blog
- @kmcnam

Cisco Webex App

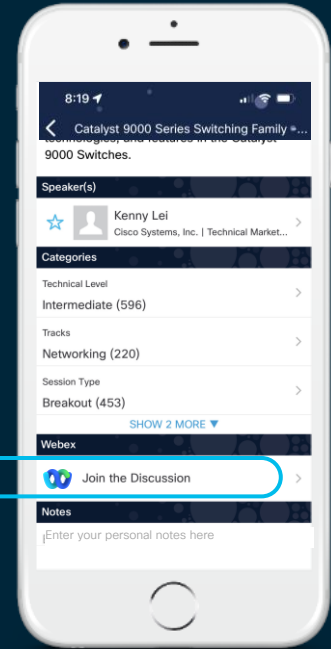
Questions?

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 17, 2022.

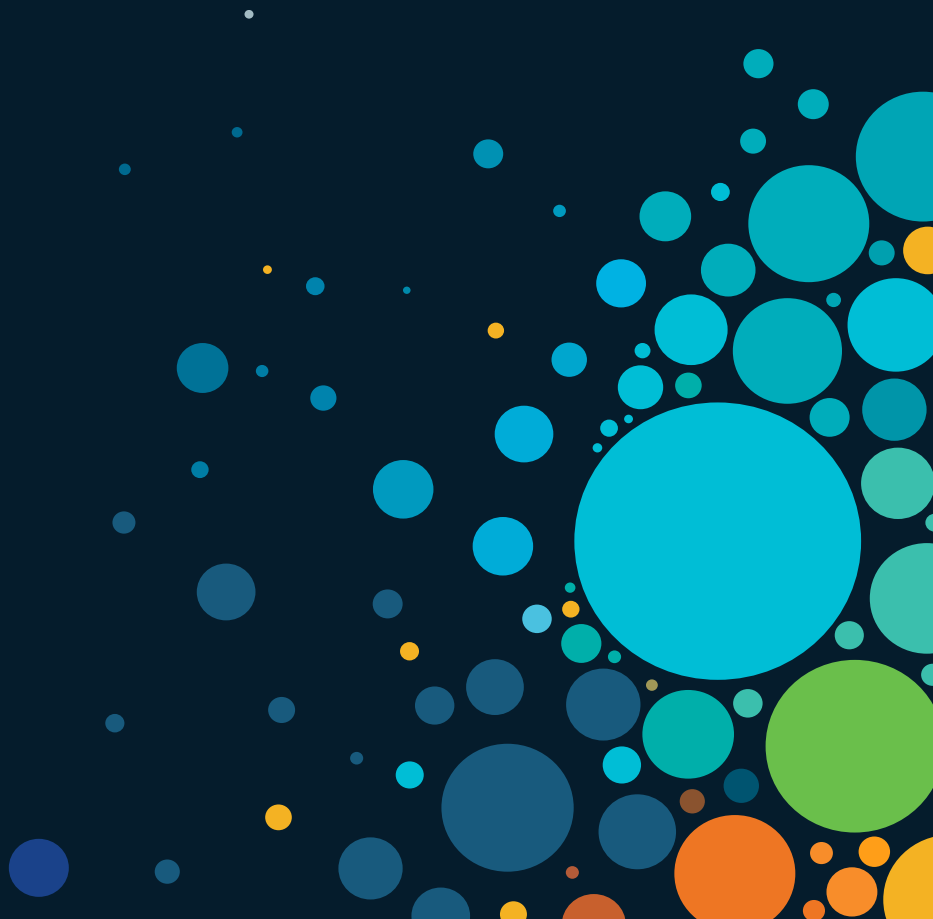


<https://cislive.ciscoevents.com/cislivebot/#BRKSEC-2347>

Agenda

- Where To Start
- ISE Appliances & Deployment Options
- Network Devices
- Identity Sources
- Enforcement
- 802.1x Deployment Phases
- Day 2 Operations
- Conclusion

Where do we start?





Deploying any network access
control isn't easy...



Why isn't there an easy button?









- There are a lot of layers to account for: Layer 1 through 8
- Discovery required
- Often need to work with other teams in the organization:
 - Active Directory
 - PKI
 - Desktop Support
 - Virtualization Team
 - Etc
- Planning & Staging



Understand the Business Objectives

What is the business trying to accomplish with ISE?



 Asset Visibility	Cisco ISE can reach deep into the network to deliver superior visibility into who and what is accessing resources.
 Access Control	Consistent access control across wired, wireless and VPN Networks. 802.1X, MAC, Web Authentication and Easy connect for admission control.
 Guest Access	Fully customizable branded mobile and desktop guest portals, with dynamic visual workflows to easily manage guest user experience.
 BYOD Access	Simplified BYOD management with built-in CA and 3rd party MDM integration for on boarding and self-service of personal mobile devices
 Segmentation	Topology independent Software-defined segmentation policy to contain network threats.
 Context Exchange	Context sharing with partner eco-system to improve their overall efficacy and accelerate time to containment of network threats.
 Threat Control	Protection against threats across the attack continuum, before, during and after an attack. Reduce time-to-detection from days to hours.
 Device Admin	Cisco ISE supports device administration using the TACACS+ security protocol to control and audit the configuration of network devices

ISE Appliances & Deployment Options

Let's talk about ISE personas...

Persona Types:

- Administrative 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 2 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)

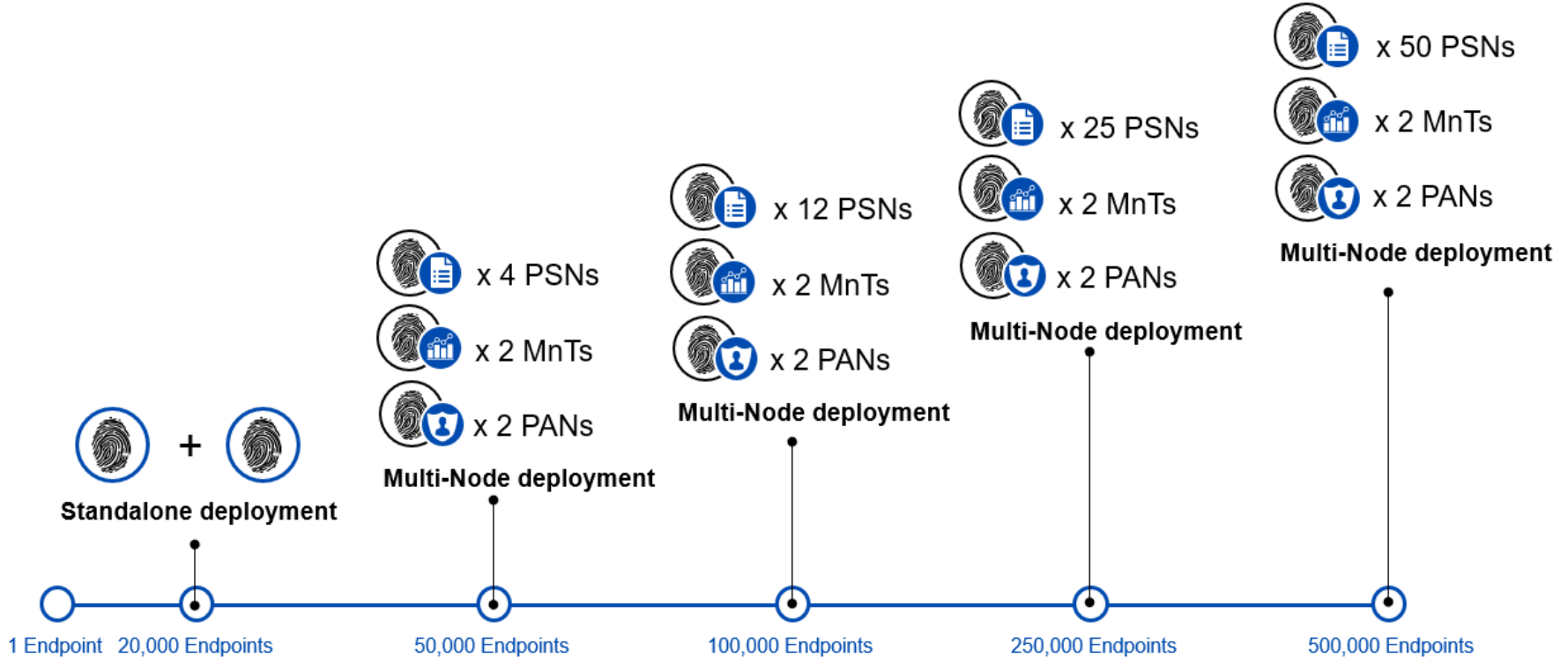
- Makes policy decisions
- RADIUS/TACACS+ Servers



pxGrid Controller

- Facilitates sharing of context

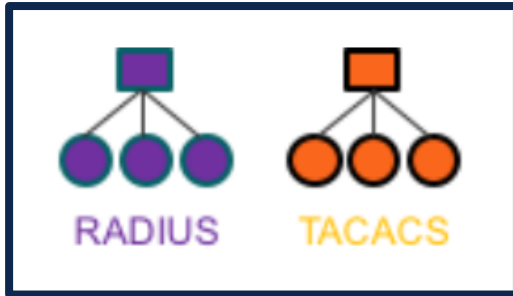
Scaling ISE



ISE Deployment Models

Separating RADIUS & TACACS+ ISE Cubes?

- Three different options:
 - Separate ISE cubes for RADIUS & TACACS+
 - Mixed ISE cube with separate PSNs for RADIUS and TACACS+
 - Mixed ISE cube where PSNs are not dedicated to either



Other Considerations

- Number of concurrently connected endpoints
- Redundancy
 - PSNs deployed to critical sites?
 - Load balancers?
- Bandwidth between ISE nodes
- Latency considerations:
 - 300 ms between PAN and PSN
 - QA-tested guardrail

Network Devices

Network Device Discovery

- Support for RADIUS and/or TACACS+
- Cisco device or third party?
 - Hardware model
 - IOS version
 - Count
 - Vendor-specific RADIUS dictionary needed?
 - Support for RADIUS CoA or SNMP CoA?
- Network Device Profile Creation
- Hardware limitations

Easy way to check hardware and OS Feature Support

ISE Network Component Compatibility Matrix

Table 1. Features and Functionalities

Feature	Functionality
AAA	802.1X, MAB, VLAN Assignment, dACL
Profiling	RADIUS CoA and Profiling Probes
BYOD	RADIUS CoA, URL Redirection and SessionID
Guest	RADIUS CoA, Local Web Auth, URL Redirection and SessionID
Guest Originating URL	RADIUS CoA, Local Web Auth, URL Redirection and SessionID
Posture	RADIUS CoA, URL Redirection and SessionID
MDM	RADIUS CoA, URL Redirection and SessionID
TrustSec	SGT Classification

Validated Cisco Access Switches

Table 2. Validated Cisco Access Switches

Device	Validated OS ¹	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec ²
	Minimum OS ³								
IE2000 IE3000	IOS 15.2(2)E4 IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	IOS 15.0(2)EB	√	√	√	√	X	√	√	√
IE4000 IE5000	IOS 15.2(2)E5 IOS 15.2(4)E2 IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
IE4010	IOS 15.2(2)E5 IOS 15.2(4)E2	√	√	√	√	√	√	√	√
	IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
SMB SG500	Sx500 1.4.8.06	⁴	!	X	X	X	X	X	X
	Sx500 1.2.0.97	!	!	X	X	X	X	X	X
IOS 15.2(2)E2	IOS 15.2(2)E2	√	√	√	√	√	√	√	√

Additional Tips

- Favorite study motto: Always Be Labbing!
- 3rd party device documentation
- Standardize! Standardize! Standardize!
 - IOS versions
 - AAA configurations
 - Wireless configurations

Identity Sources

ISE Supports a Large Number of Identity Sources

- Active Directory
- LDAP
- ODBC
- RADIUS Token Servers
- RSA SecurID
- SAMLv2 Identity Providers
- Certificate Authentication Profiles
- Social Login

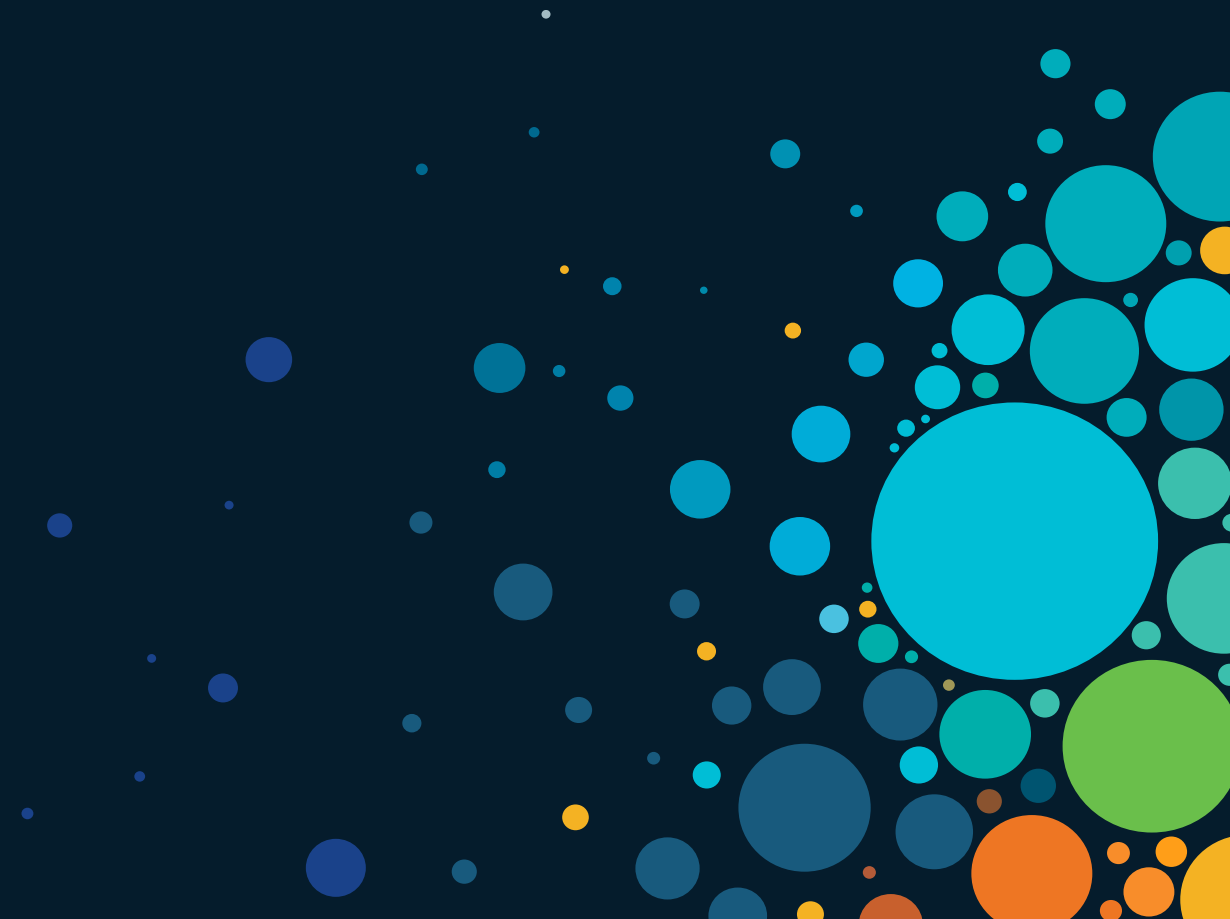
Integration with Identity Sources is Key

- Active Directory?
 - Multiple domains?
 - Multiple forests?
 - Version of AD?
- Common issues with domain join:
 - Time skew
 - AD DNS SRV records

Prepare the Certificates

- Server Certificate
- Public Certificate (Guest)
 - Cert errors if self-signed
- EAP Certificate
- pxGrid Certificate
 - Protip: EKU: Server & Client Authentication

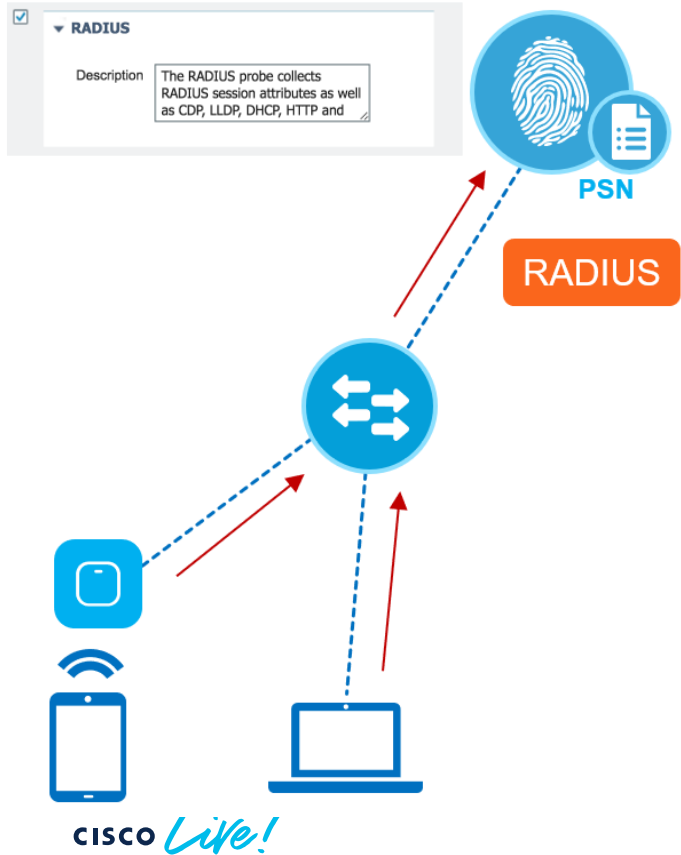
Profiling



ISE Profiling

- Pre-loaded profiles covers majority of endpoints
 - For everything else: custom profiles
- Discovery before enforcement
 - Passively discover with ISE
- Find the unique endpoints
 - Average person carries 2.9 devices
 - New device times are introduced every year

RADIUS Probes



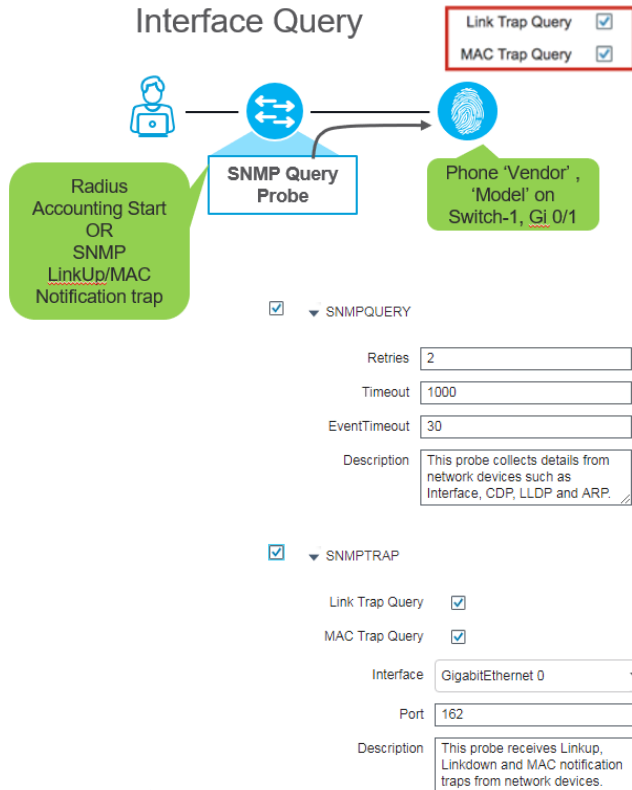
- ISE can profile endpoints based on the RADIUS attributes collected from the RADIUS request/response messages from the RADIUS Servers over standard radius ports
- UDP/1645 or UDP/1812 for Authentication
- UDP/1646 and UDP/1813 for Accounting
- Network devices must be configured for AAA
- The following are the known attributes that are collected by the RADIUS probe:

IP-MAC Bindings

User-Name	Calling-Station-Id	Called-Station-Id	Framed-IP-Address
NAS-IP-Address	NAS-Port-Type	NAS-Port-Id	NAS-Identifier
Device Type (NAD)	Location (NAD)	Authentication Policy	Authorization Policy

NDG's

SNMP Probe



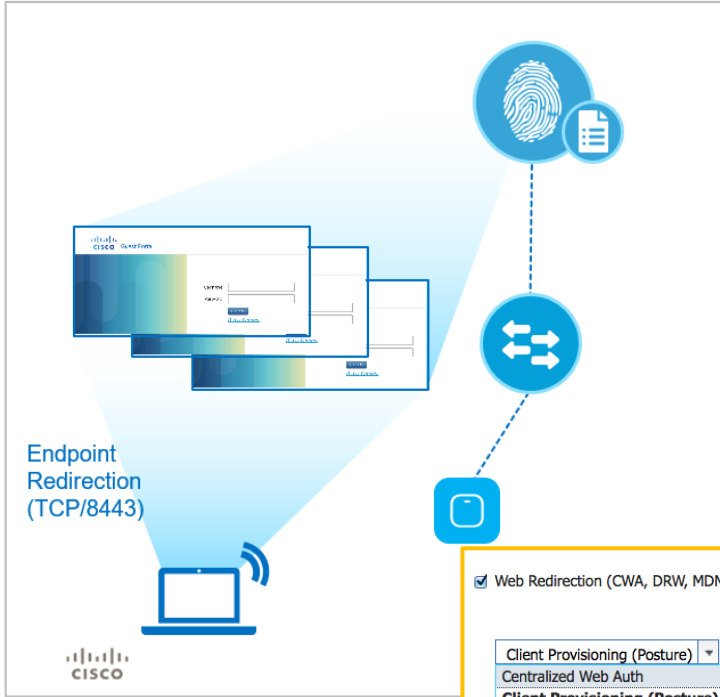
SNMP Trap Probe

- Alert ISE Profiling Services to the presence (connection or disconnection) of a network endpoint
- Trigger an SNMP Query probe
- Key attributes highlighted include **EndPointSource**, **MACAddress**, and **OUI**

SNMP Query Probe

- This probe collects details from the network devices such as Interface, CDP, LLDP, and ARP
- “Network devices” in ISE must be configured for SNMP
 - System Query (Polled) [Default 8 hours]
 - Interface Query (Triggered)
- RADIUS Accounting Start messages also trigger the SNMP Query probe

HTTP Probe



- User-agent is an HTTP request header that is sent from web browsers to web servers. **The user-agent includes application, vendor, and OS information** that can be used in profiling endpoints.
- User-agent attributes can be collected from web browser sessions redirected to ISE for existing serves such as:
 - Central Web Auth (CWA)
 - Device Registration WebAuth (DRW)
 - Native Supplicant Provisioning

Web Redirection (CWA, DRW, MDM, NSP, CPP)

Client Provisioning (Posture) ACL

Centralized Web Auth

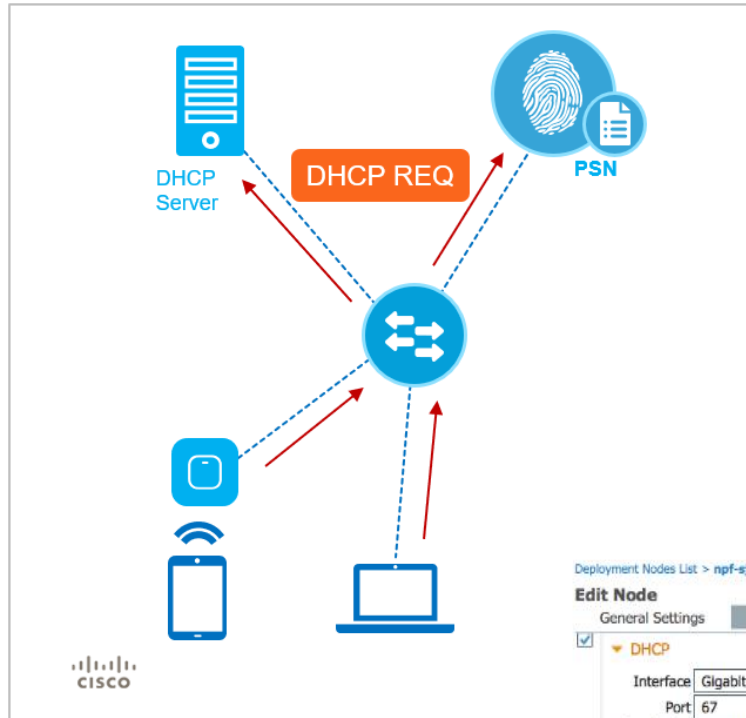
Client Provisioning (Posture)

Device Registration Web Auth

MDM Redirect

Native Supplicant Provisioning

DHCP Probe



- Simple method of getting DHCP traffic to ISE
- Requires configuration of NADs to relay DHCP packets to ISE.
- DHCP probe in ISE will collect DHCP data to use in profiling policy
- For WLCs disable DHCP proxy

Deployment Nodes List > npf-sjca-pdp01

Edit Node

General Settings

Profiling Configuration



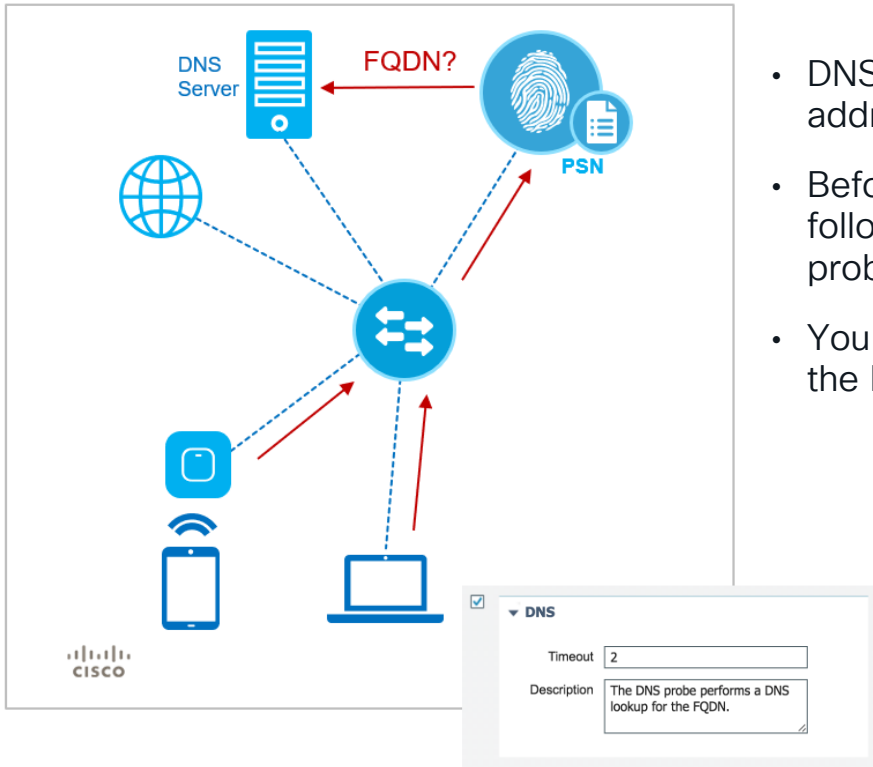
DHCP

Interface: GigabitEthernet 0

Port: 67

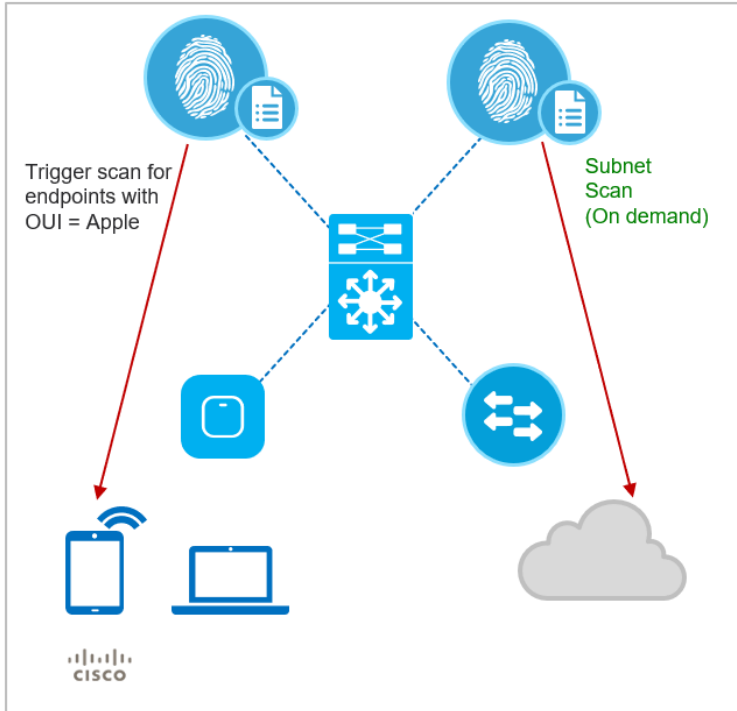
Description: The DHCP probe listens for DHCP packets from IP helper.

DNS Probe

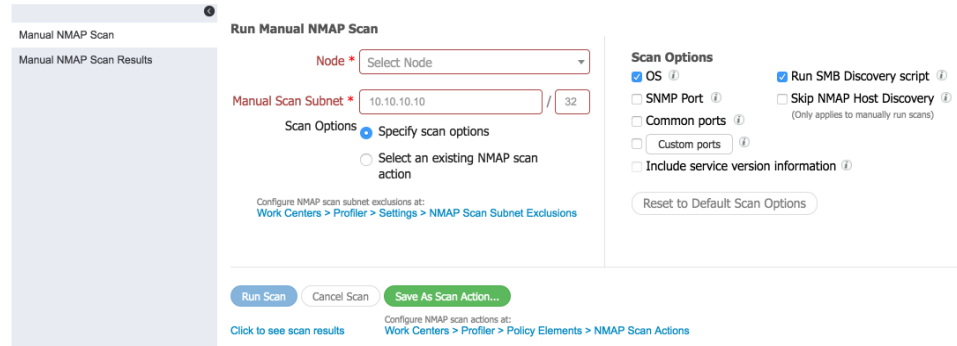


- DNS probe in the profiler does a reverse DNS lookup for IP addresses learnt by other means.
- Before a DNS lookup can be performed, one of the following probes must be started along with the DNS probe: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP.
- You can create an endpoint profiling condition to validate the FQDN attribute and its value for profiling.

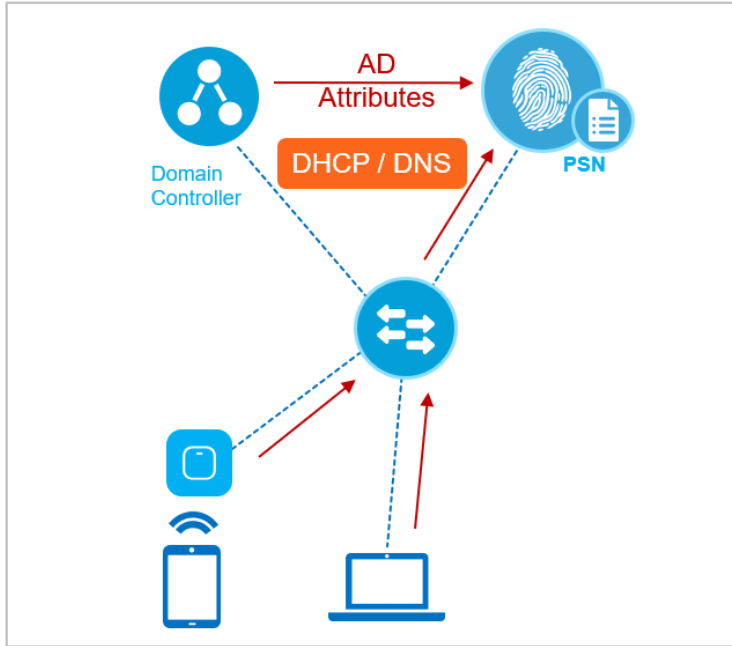
NMAP Probe



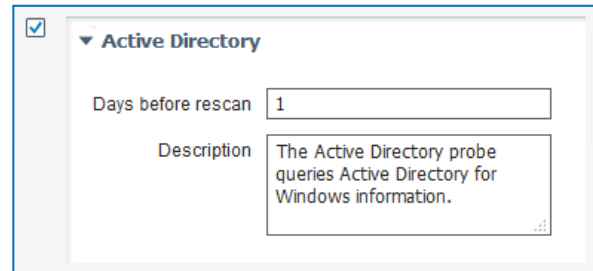
- NMAP utility incorporated into ISE allows profiler to detect new endpoints through a subnet scan and to classify endpoints based on their operating system, OS version, and services as detected by the NMAP.
- The network scan probe is considered an “active” assessment mechanism since it communicates directly with the endpoint to obtain information from the source.
- The scan can trigger dynamically based on policy.



Active Directory Probe

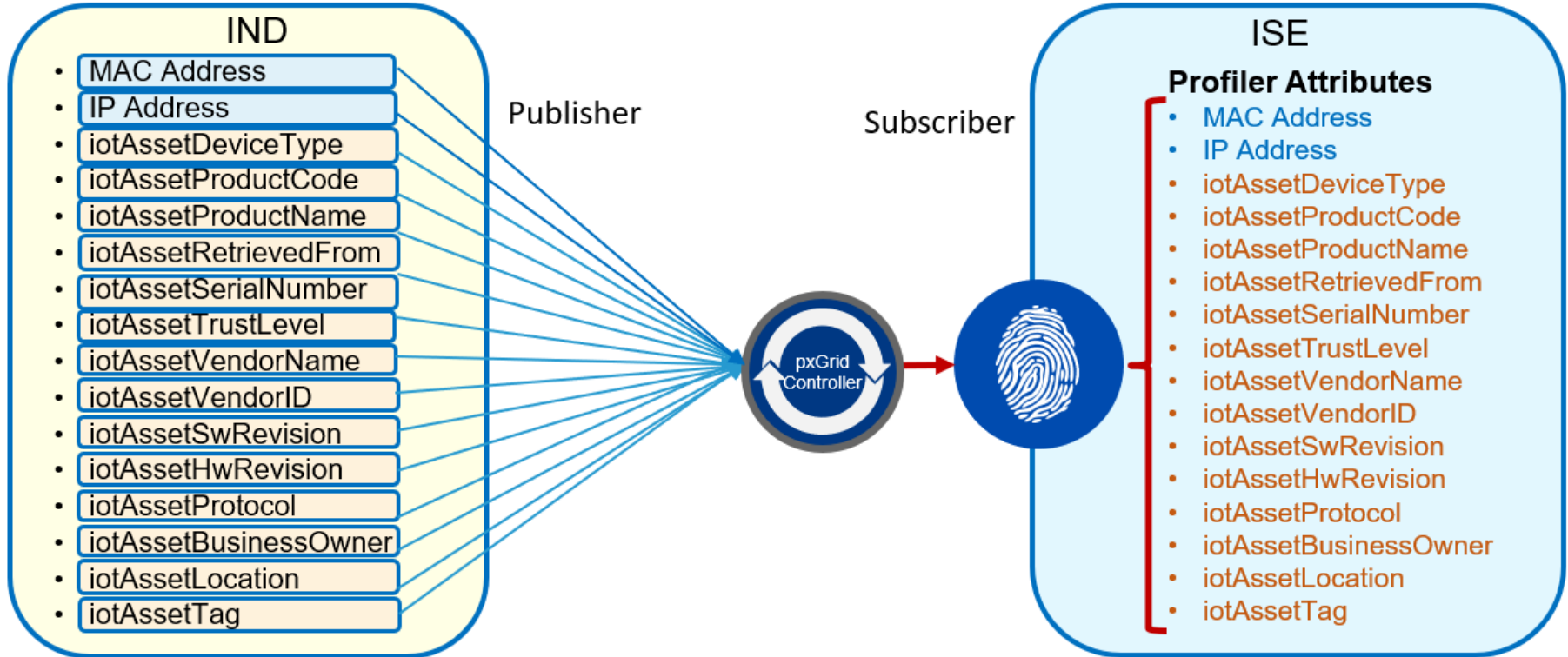


- Increases OS fidelity through detailed info extracted via AD.
- Leverages AD Runtime Connector
- Attempts to fetch AD attributes once computer hostname learned from DHCP Probe and DNS Probe
- AD queries gated by:
 - Rescan interval (default 1 day)
 - Profiler activity for endpoint



pxGrid Probe

Custom Attributes Supported !!!



Netflow Probe

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Directory', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows a tree view with 'Deployment' and 'PAN Fallover'. The main content area is titled 'Deployment Nodes List > ise-2' and 'Edit Node'. It features two tabs: 'General Settings' and 'Profiling Configuration'. The 'Profiling Configuration' tab is active, showing a list of probes. The 'NETFLOW' probe is selected and expanded, showing the following configuration:

- NETFLOW**
- Interface: GigabitEthernet 0
- Port: 9996
- Description: The Netflow probe collects Netflow packets sent to it from Routers.

The 'DHCP' probe is also visible and checked:

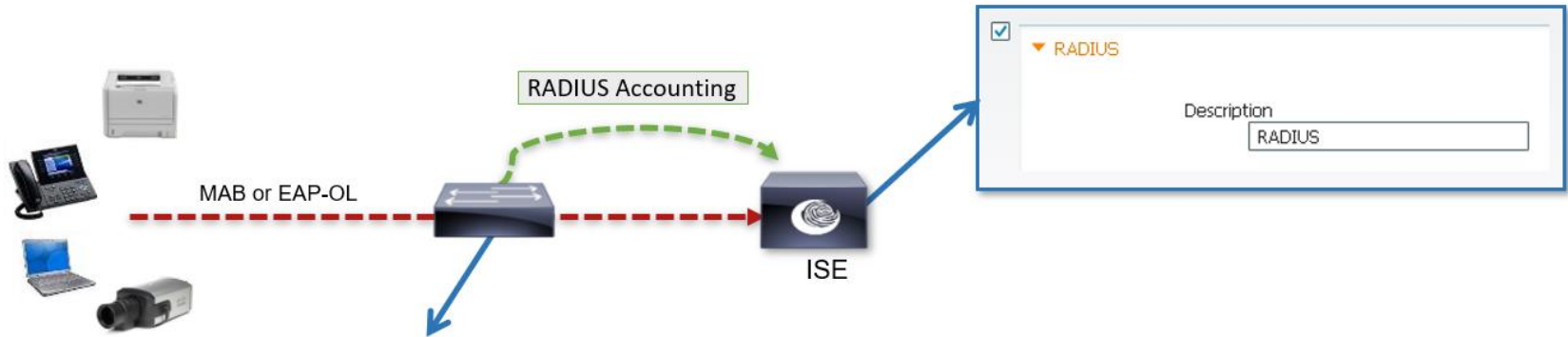
- DHCP**
- Interface: GigabitEthernet 0
- Port: 67
- Description: The DHCP probe listens for DHCP packets from IP helper.

The 'DHCPSPAN' probe is also visible but unchecked:

- DHCPSPAN**

- NetFlow vendor specific attributes reveal device identity
- Flow reception on Port # 9996/UDP
- Cisco ISE profiler implements Cisco IOS NetFlow Version 9, while backward compatible to earlier versions
- Cisco IOS NetFlow Version 5 packets do not contain MAC addresses of endpoints. Prior record on ISE via other means necessary for merging attributes.
- As a general rule, avoid this probe – only unique corner cases where this might be applicable

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)

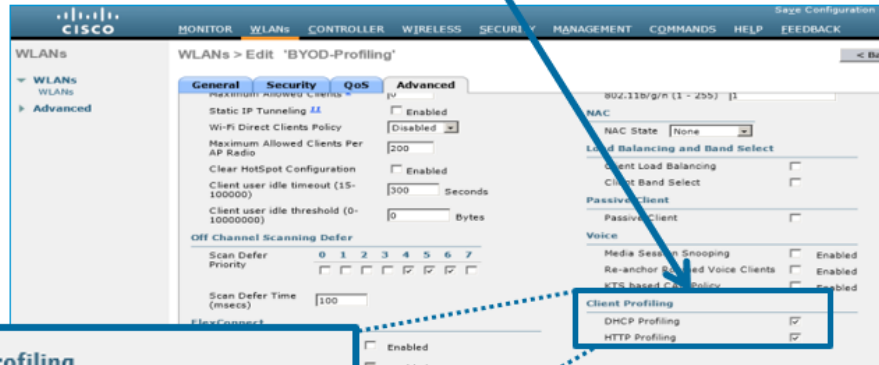
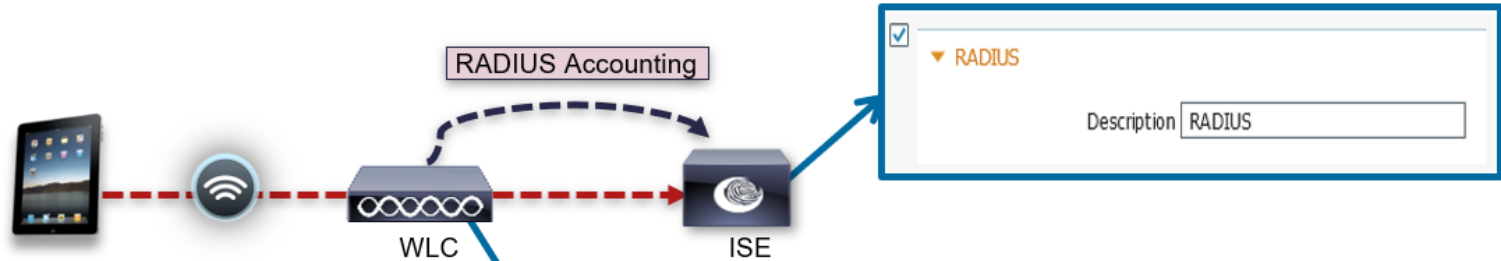
```
no macro auto monitor
access-session template monitor
```

```
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
```

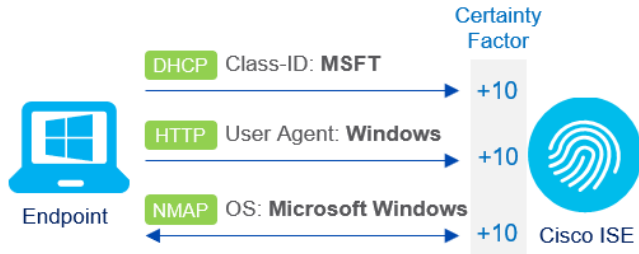
Wireless Device Sensor



- 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

Profiling Policies

The minimum 'certainty metric' in the profiling policy evaluates the matching profile for an endpoint.



DHCP:dhcp-class-identifier CONTAINS MSFT	●	If Condition	Microsoft-WorkstationRule1Check1	Then	Certainty Factor Increases	10
DHCP:dhcp-class-identifier CONTAINS MS-UC-Client	●	If Condition	Microsoft-Workstation-Rule4-Check1	Then	Certainty Factor Increases	10
IP:User-Agent CONTAINS Windows	●	If Condition	Microsoft-WorkstationRule2Check1	Then	Certainty Factor Increases	10
NMAP:operating-system CONTAINS Microsoft Windows	●	If Condition	Microsoft-WorkstationRule3Check1	Then	Certainty Factor Increases	10

Profiler Policy List > Microsoft-Workstation

Profiler Policy

* Name: Microsoft-Workstation Description: Generic policy for Microsoft workstation

Policy Enabled:

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

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

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

Parent Policy: Workstation

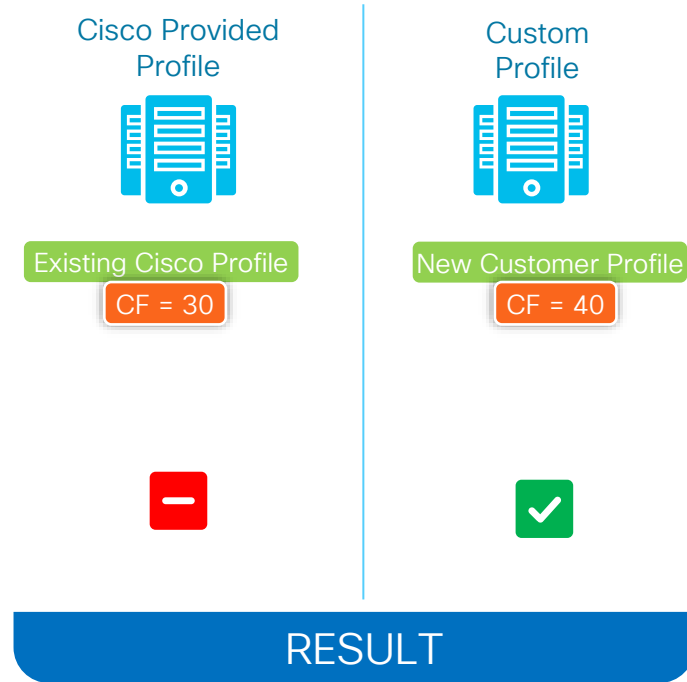
* Associated CoA Type: Global Settings

System Type: Cisco Provided

Rules

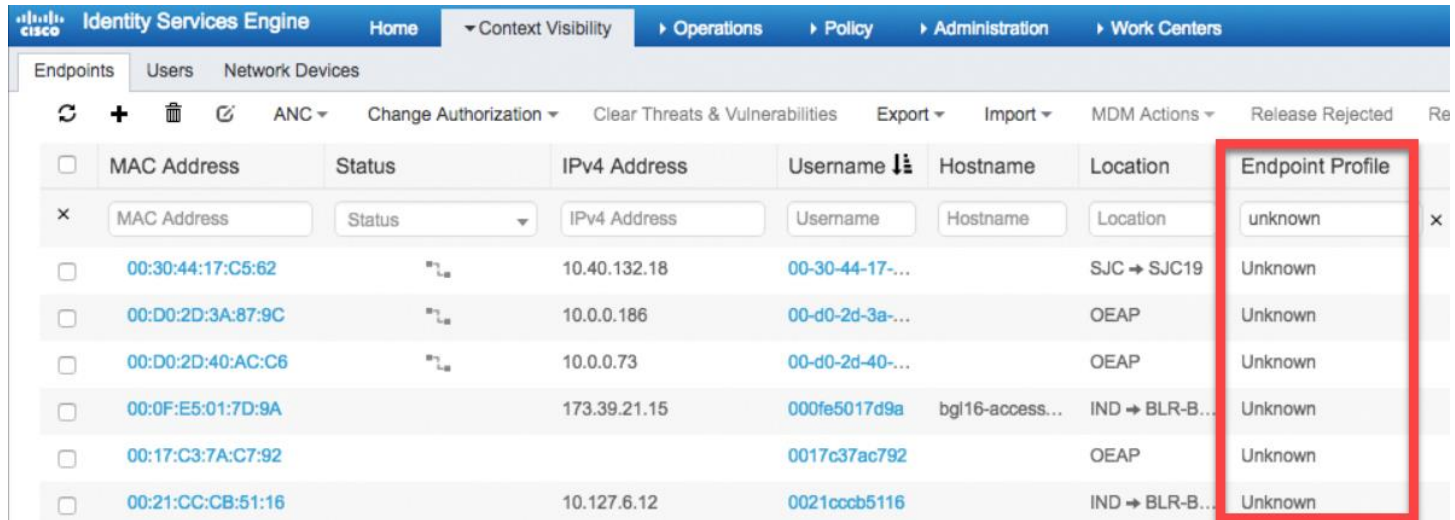
If Condition	Microsoft-WorkstationRule1Check1	Then	Certainty Factor Increases	10
If Condition	Microsoft-Workstation-Rule4-Check1	Then	Certainty Factor Increases	10
If Condition	Microsoft-WorkstationRule2Check1	Then	Certainty Factor Increases	10
If Condition	Microsoft-WorkstationRule3Check1	Then	Certainty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

Profiles Precedence



What about Unknowns?

- There will be endpoints that don't have pre-built profiles
- Endpoint profiles will show as "Unknown"
- View your unknown endpoints under Context Visibility>Endpoints



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Context Visibility' section is active, showing 'Endpoints', 'Users', and 'Network Devices'. The 'Endpoints' tab is selected, displaying a table of endpoints. The 'Endpoint Profile' column is highlighted with a red box, showing 'Unknown' for several entries.

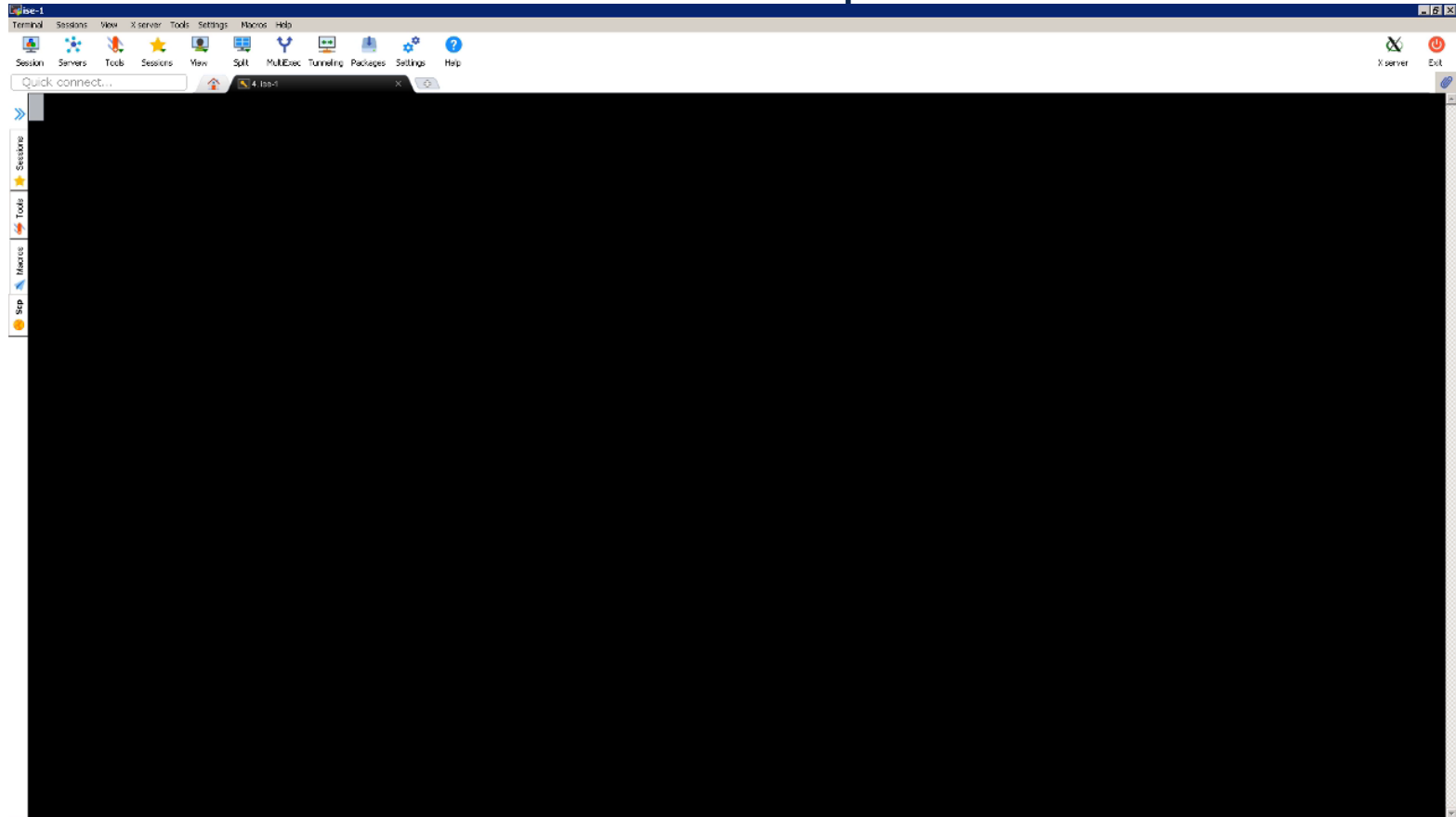
MAC Address	Status	IPv4 Address	Username	Hostname	Location	Endpoint Profile
00:30:44:17:C5:62	🔒	10.40.132.18	00-30-44-17-...		SJC → SJC19	Unknown
00:D0:2D:3A:87:9C	🔒	10.0.0.186	00-d0-2d-3a-...		OEAP	Unknown
00:D0:2D:40:AC:C6	🔒	10.0.0.73	00-d0-2d-40-...		OEAP	Unknown
00:0F:E5:01:7D:9A		173.39.21.15	000fe5017d9a	bgl16-access...	IND → BLR-B...	Unknown
00:17:C3:7A:C7:92			0017c37ac792		OEAP	Unknown
00:21:CC:CB:51:16		10.127.6.12	0021ccb5116		IND → BLR-B...	Unknown

Creating a Custom Profile

Under Attributes, you can see all the attributes for the unknown endpoint

Other Attributes					
5060-tcp	sip	OUI	Inventec Multimedia & Telecom Corporation	dhcp-class-identifier	udhcp 0.9.7
80-tcp	http	OriginalUserName	00144800308c	dhcp-client-identifier	01:00:14:48:00:30:8c
AAA-Server	ise	PolicyVersion	8	dhcp-message-type	DHCPREQUEST
AuthenticationIdentityStore	Internal Endpoints	PostureApplicable	Yes	dhcp-parameter-request-list	1, 3, 6, 12, 15, 28
AuthenticationMethod	Lookup	PostureAssessmentStatus	NotApplicable	dhcp-requested-address	10.1.100.103
AuthenticationStatus	AuthenticationPassed	RadiusFlowType	WiredMAB	dot1xAuthAuthControlledPortControl	2
AuthorizationPolicyMatchedRule	Default	SSID	C0-67-AF-EE-09-AB	dot1xAuthAuthControlledPortStatus	2
BYODRegistration	Unknown	SelectedAccessService	PEAP-EAP	dot1xAuthSessionUserName	00-14-48-00-30-8C
Called-Station-ID	C0-67-AF-EE-09-AB	SelectedAuthenticationIdentityStores	Internal Endpoints	flags	0x0000
Calling-Station-ID	00-14-48-00-30-8C	SelectedAuthorizationProfiles	PermitAccess	giaddr	10.1.100.75
DTLSSupport	Unknown	Service-Type	Call Check	hlen	6
DestinationIPAddress	10.1.100.21	StaticAssignment	false	htype	Ethernet (10Mb)
DestinationPort	1812	StaticGroupAssignment	false	ifDescr	GigabitEthernet1/0/43
Device IP Address	10.1.100.75	StepData	5= DEVICE.Location, 6= DEVICE.Device Type, 7= DEVICE.Mode, 8= DEVICE.Radius.RadiusFlowType, 11=Internal Endpoints, 17= Session.ANCPolicy, 18	ifIndex	50
Device Type	Device Type#All Device Types#Switches	Total Certainty Factor	0	ifOperStatus	1
DeviceRegistrationStatus	NotRegistered	TrustSec-Enabled	TrustSec-Enabled#TrustSec-Enabled#Non-TrustSec	ip	10.1.100.103
ElapsedDays	0	UseCase	Host Lookup	op	BOOTREQUEST
EndPointMACAddress	00-14-48-00-30-8C	User-AD-Last-Fetch-Time	1543131931802	operating-system	Linux 2.4.9 - 2.4.18 (likely embedded)
EndPointPolicy	Unknown	User-Fetch-User-Name	00144800308c	operating-system-result	Linux 2.4.9 - 2.4.18 (likely embedded)
EndPointProfilerServer	ise.securitydemo.net	User-Name	00144800308c	yiaddr	0.0.0.0
EndPointSource	SNMPQuery Probe	UserType	Host		
FailureReason	-	allowEasyWiredSession	false		
Framed-IP-Address	10.1.100.103	chaddr	00:14:48:00:30:8c		
IPSEC	IPSEC#Is IPSEC Device#No	ciaddr	0.0.0.0		
IdentityGroup	Unknown				
IdentityPolicyMatchedRule	MAB				
InactiveDays	0				

Custom Profiles: Get All Endpoints



Breaking Down Profiling Attributes

OUI	dhcp-parameter-request-list	User-Agent	AD-Operating-System	device-platform	device-type
Apple, Inc.	1, 121, 3, 6, 15, 119, 252, 95, 44, 46	Mozilla/4.0 (compatible; MAC_OSX; 2.10.13; AnyConnect Posture Agent v.4.8.00175)	Mac OS X	mac-intel	MacBook8,1
Apple, Inc.	1, 121, 3, 6, 15, 119, 252, 95, 44, 46	Mozilla/4.0 (compatible; MAC_OSX; 2.10.14; AnyConnect Posture Agent v.4.8.00175)	Mac OS X	mac-intel	MacBook8,1
Apple, Inc.	1, 121, 3, 6, 15, 119, 252, 95, 44, 46	Mac OS X/10.13.6 (17G66)		mac-intel	MacBookAir4,2
Apple, Inc.	1, 121, 3, 6, 15, 119, 252, 95, 44, 46	Mozilla/4.0 (compatible; MAC_OSX; 2.10.13; AnyConnect Posture Agent v.4.8.00175)	Mac OS X	mac-intel	MacBookAir7,2
Apple, Inc.	1, 121, 3, 6, 15, 119, 252, 95, 44, 46	Mozilla/5.0 (iPhone\; CPU iPhone OS 12_1_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1	Mac OS X	mac-intel	MacBookAir7,2
Apple, Inc.	1, 121, 3, 6, 15, 119, 252, 95, 44, 46	Mozilla/4.0 (compatible; MAC_OSX; 2.10.12; AnyConnect Posture Agent v.4.8.00175)		mac-intel	MacBookAir7,2
Apple, Inc.	1, 121, 3, 6, 15, 119, 252, 95, 44, 46	Mozilla/4.0 (compatible; MAC_OSX; 2.10.14; AnyConnect Posture Agent v.4.8.00175)		mac-intel	MacBookAir8,1
Apple, Inc.	1, 121, 3, 6, 15, 119, 252, 95, 44, 46	Mozilla/4.0 (compatible; MAC_OSX; 2.10.14; AnyConnect Posture Agent v.4.8.00175)	Mac OS X	mac-intel	MacBookPro10,1
Apple, Inc.	1, 121, 3, 6, 15, 119, 252, 95, 44, 46	Mac OS X/10.13.6 (17G8030)		mac-intel	MacBookPro10,1

Custom Profiles: Using Endpoint Attributes

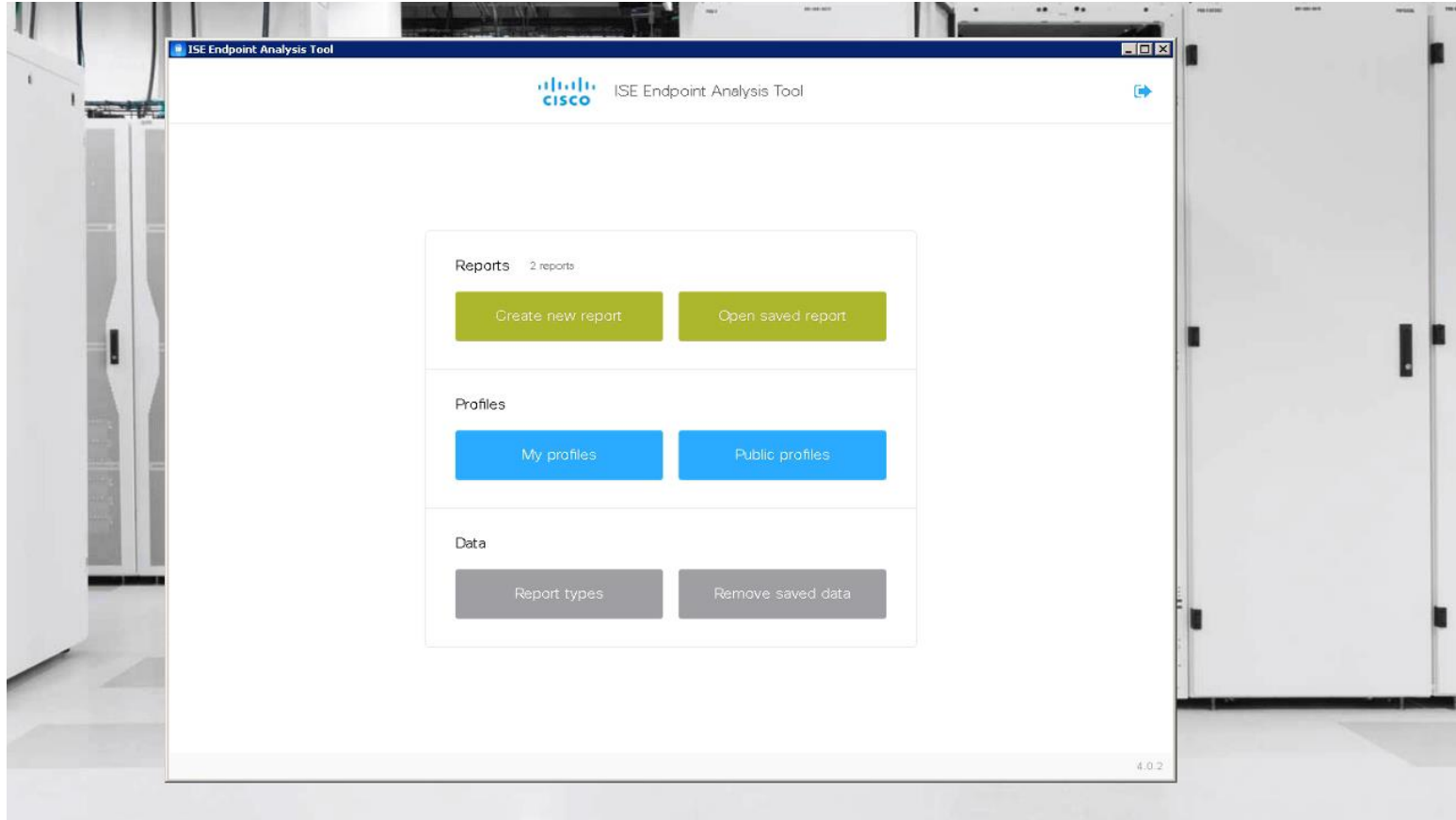
The screenshot shows an Excel spreadsheet with the following data:

	host-name	MatchedPolicy	OUI	sysContact	sysLocation	sysName	hrDeviceDescr	sysDescr	9100-
1									
2		HP-LaserJet-Printer	Hewlett Packard				HP LaserJet 400 MFP M425dn	HP ETHERNET MULTI-ENVIRONMENT,PID:HP LaserJet 400 MFP M425dn	jetdirect
3		HP-LaserJet-Printer	Hewlett Packard				HP LaserJet 400 MFP M425dn	HP ETHERNET MULTI-ENVIRONMENT,PID:HP LaserJet 400 MFP M425dn	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
5	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
6									
7									

ISE Endpoint Analysis Tool

- Free tool available to customers
- Simply register at iseeat.cisco.com using a work email address
- Pulls all endpoints off ISE
- Custom profile creation through the tool

ISE Endpoint Analysis Tool –Endpoint Report



ISE Endpoint Analysis Tool – Custom Profile Creation

ISE Endpoint Analysis Tool

← →

ISE Endpoint Analysis Tool

CLEUR-Report1 1/23/20, 6:13 PM / 5s Export as CSV... Create profile

Show 50 entries Showing 1 to 50 of 110 entries

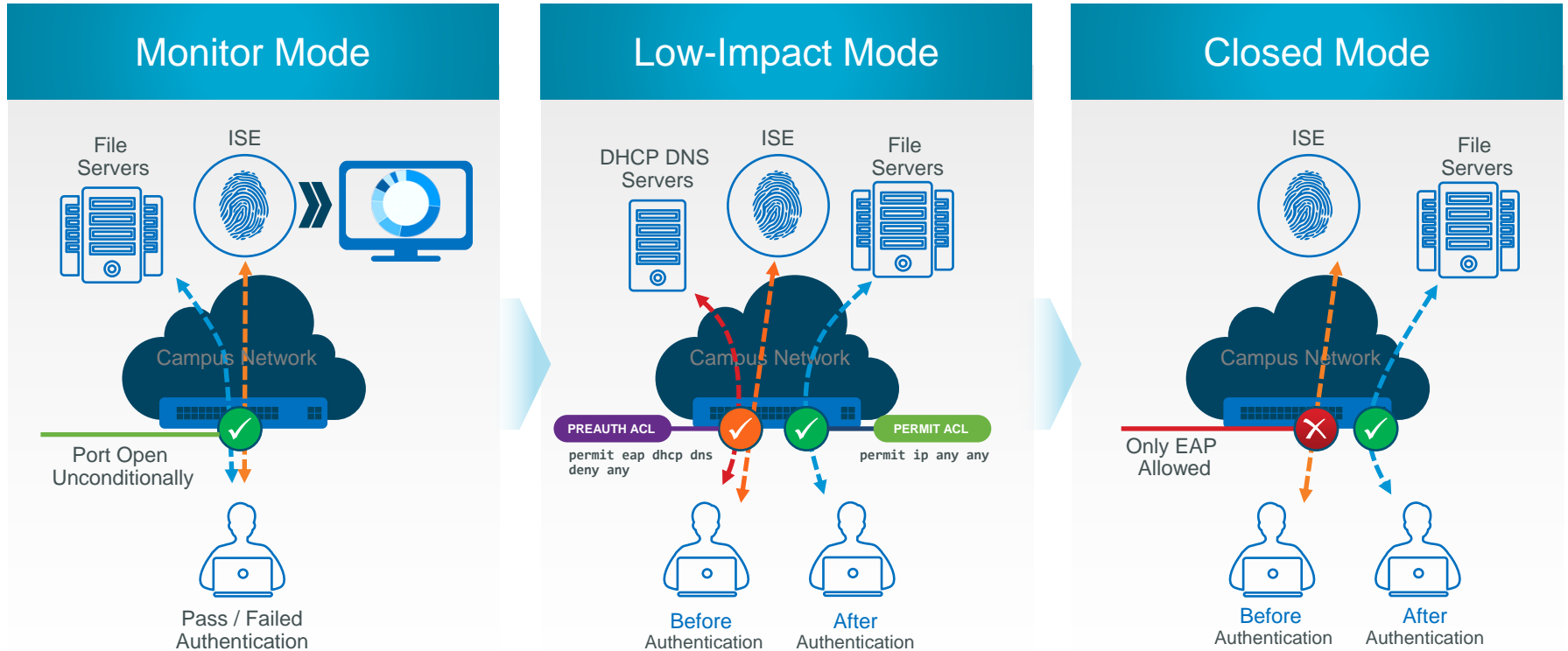
MAC Address	SNMP Device Descript...	SNMP Switc...	NMAP Operating System	OUI Name	McAfee ePO 8061 T...	DHCP Parameter Request List	LLDP System Descript...
00:14:48:00:30:80			Linux 2.4.9 - 2.4.16 (likely embedded)	Inventec Multimedia & Telecom Corporation		1, 3, 6, 12, 15, 28	
5A:69:47:43:EA:77				UNKNOWN		1, 33, 3, 6, 15, 28, 51, 58, 69	
00:0C:29:45:C7:DE				VMware, Inc.		1, 3, 12, 15, 6, 26, 33, 121, 42	
00:0C:29:7E:0C:1E				VMware, Inc.		1, 28, 2, 3, 15, 6, 12, 42	
04:62:75:97:ED:C7			Cisco Aironet 1141N (IOS 12.4) or 3602I (IOS 15...	Cisco Systems, Inc.		1, 60, 6, 13, 44, 3, 67, 12, 33, 150, 45, 125, 135	
00:0C:29:45:C7:D8				VMware, Inc.		1, 2, 3, 5, 6, 11, 12, 13, 15, 16, 17, 18, 45, 54, 60, 67, 128, 129, 130, 131...	
74:DA:38:9B:0C:49				Edimax Technology Co. Ltd.		1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43, 292	
A3:50:9F:9E:AC:90				Intel Corporate		1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43, 292	
00:1A:2F:69:D8:EE				Cisco Systems, Inc.		1, 60, 6, 3, 15, 150, 35	Cisco IP Phone 7961B,V...
E3:AA:77:97:77:5C				Cisco Systems, Inc.		1, 6, 13, 44, 3, 7, 33, 100, 43	
60:20:06:02:7E:86				Cisco Systems, Inc.		1, 6, 13, 44, 3, 7, 33, 100, 43	
00:0C:29:65:3F:0F				VMware, Inc.		1, 3, 6, 12, 15, 66, 67, 150	
00:0C:29:0C:6F:88				VMware, Inc.		1, 28, 2, 3, 15, 6, 12, 40, 41, 42	
00:0C:29:2E:0C:9C				VMware, Inc.			
00:0C:29:34:FF:0C				VMware, Inc.			
00:0C:29:34:FF:0A				VMware, Inc.			
00:0C:29:34:FF:14				VMware, Inc.			
00:0C:29:34:FF:1E				VMware, Inc.			
00:0C:29:36:0B:E7				VMware, Inc.			
00:0C:29:43:2A:06				VMware, Inc.			
00:0C:29:45:C7:E2				VMware, Inc.			
00:0C:29:45:C7:EC				VMware, Inc.			

Previous 1 2 3 Next

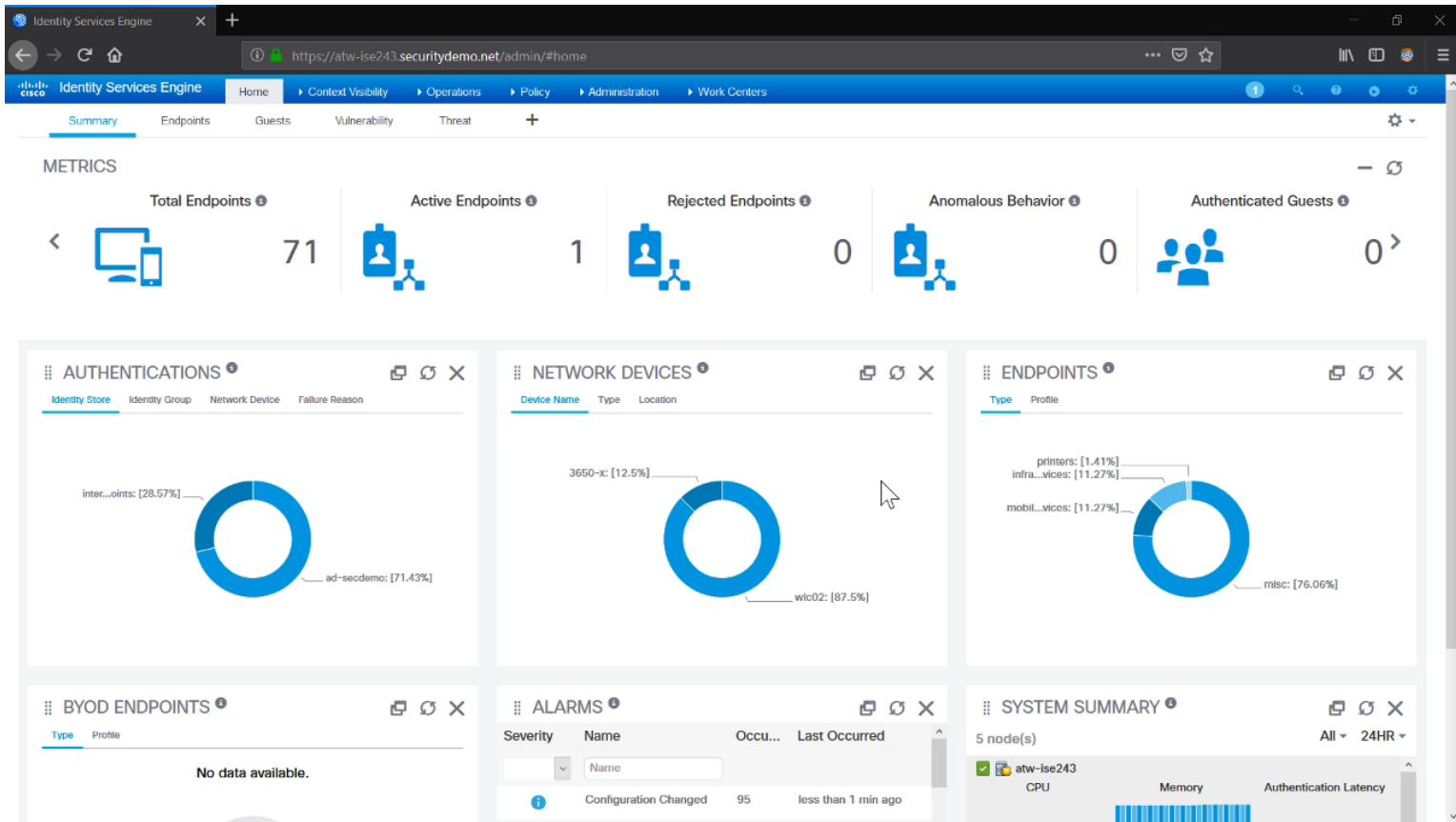
4/3/2

802.1X Deployment Phases

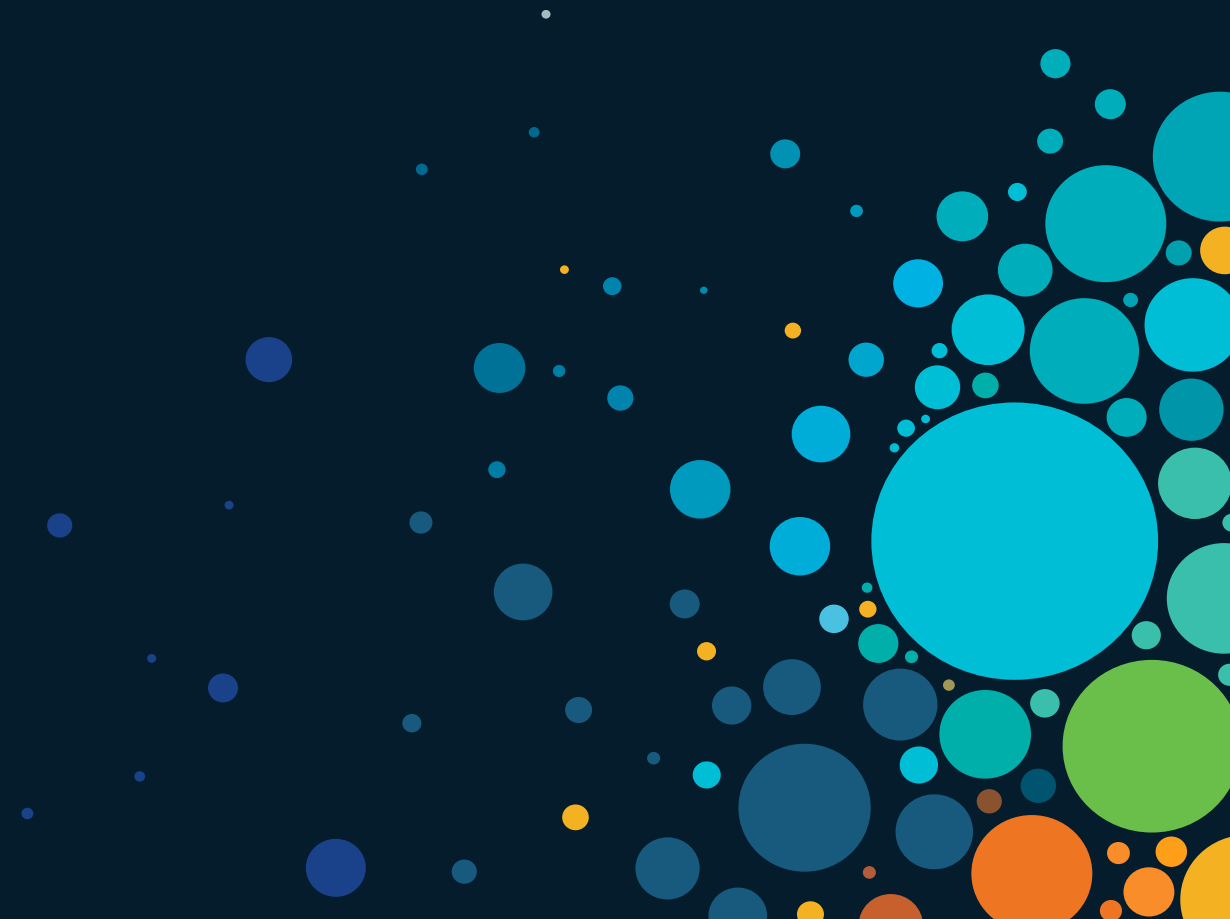
Deploying 802.1x in Phases



Utilizing Policy Sets with Modes



Enforcement

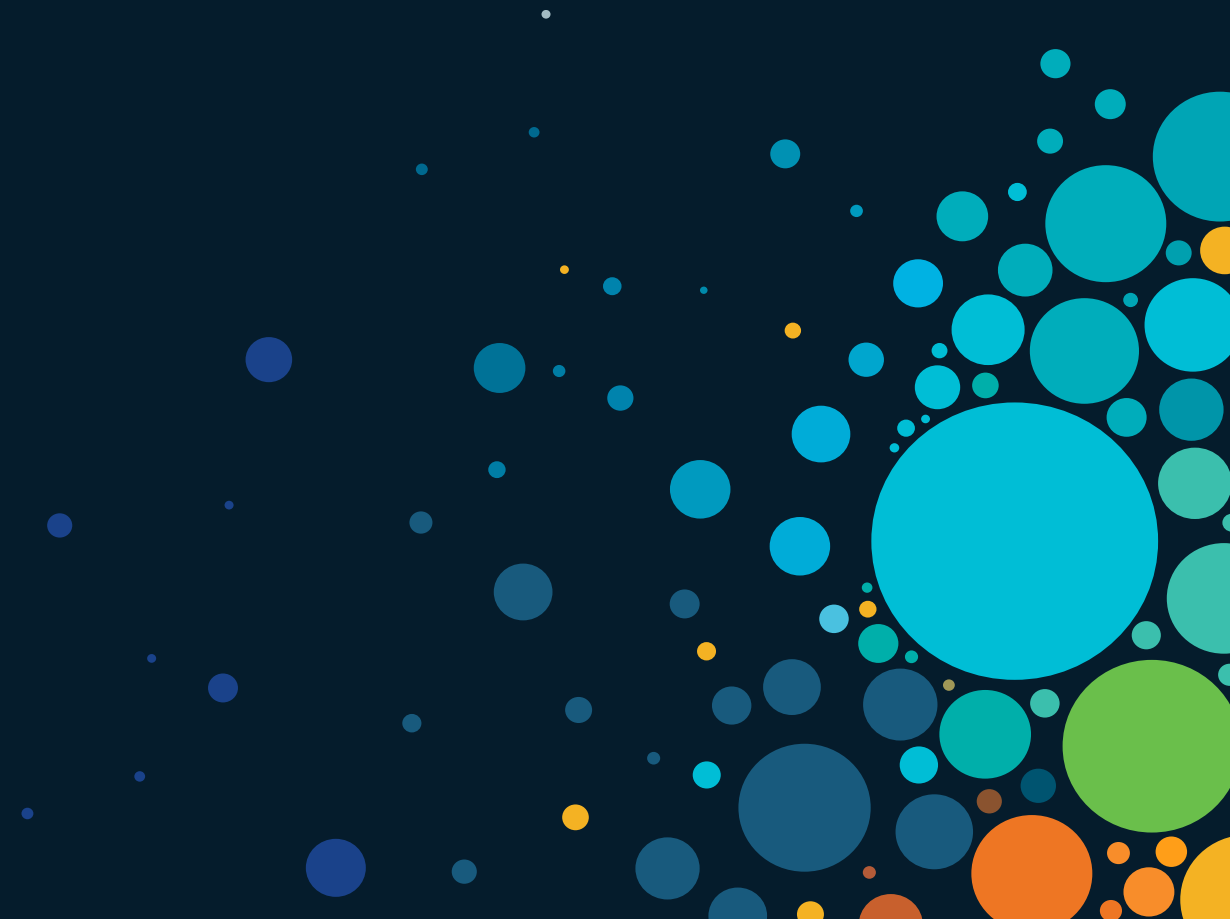


Network access control does not
automatically mean you have
segmentation

Many Options for Enforcement

- Downloadable ACL (dACL)
- ACL
- SGT
- VLAN
 - No east-west segmentation
 - DHCP
- Voice Domain Permission
- Centralized Web Redirection (Guest, BYOD, Client provisioning, etc)
- Auto Smart Port
- Vulnerability scan
- Reauthentication
- MACSec Policy
- Network Edge Access Topology (NEAT)
- Local Web Authentication
- Interface Template
- Wireless and VPN ACLs
- AVC Profile Name
- Custom attributes

Day 2 Operations



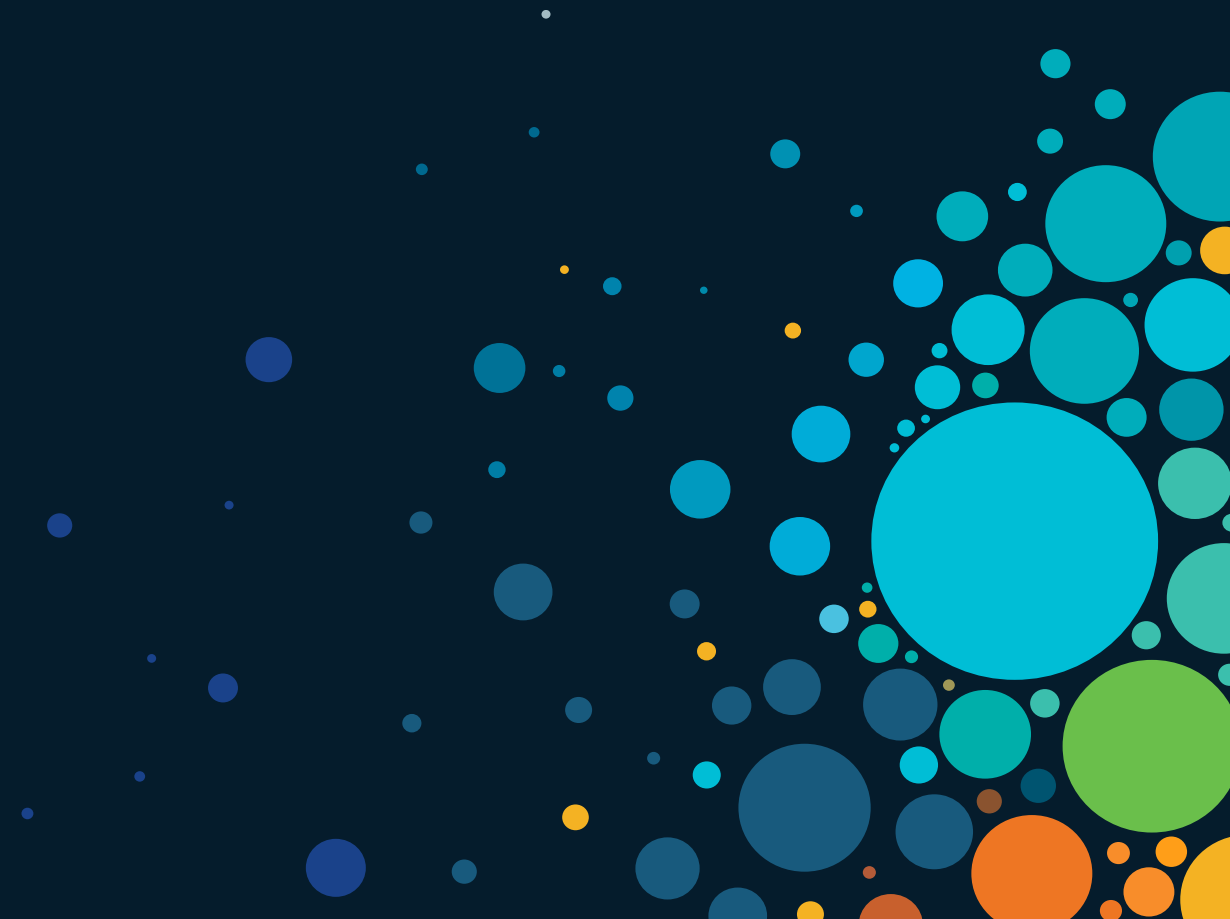
Supporting ISE After Deployment

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

Supporting ISE After Deployment (Cont'd)

- Train Your Support
 - Avoid being called for every issue
 - Playbook for common issues
 - Utilized built-in ISE roles for Helpdesk
- Many document templates available on ISE Communities
- User Communication before and after ISE rollout

Conclusion



Deploying any network access control solution isn't easy....

Planning is essential to any successful development.

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with
Cisco Learning Credits

(CLCs) are prepaid training
vouchers redeemed directly
with Cisco.



Learn



Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train



Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify



Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

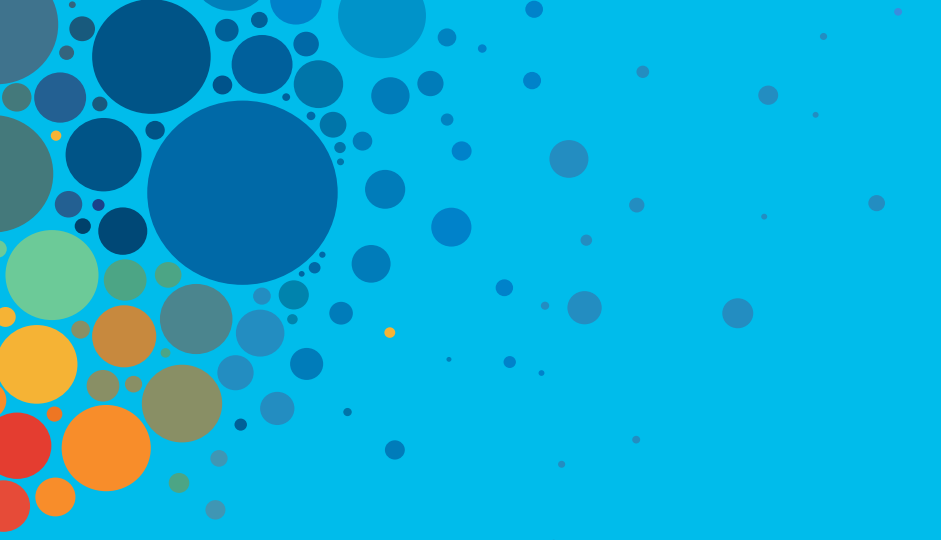
Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

CISCO *Live!*

ALL IN

#CiscoLive