You make **possible**

ISE Deployment, Staging, and Planning

Katherine McNamara – Cybersecurity Systems Engineer
@kmcnam1
BRKSEC-2430

Cisco live!
June 9-13, 2019 · San Diego, CA

Abstract

This session focuses on the preparation of an environment and the design considerations that an engineer new to ISE should think about to ensure a successful ISE deployment. Like any technology, the best configurations and products in the world will not be deployment successfully if the proper planning isn't done first and it's not designed properly. The session will also include common design pitfalls to avoid when planning out how ISE will be deployment using real world examples and how to lower the administrative overhead of an ISE deployment. At the end of the session, attendees can expect to have a better understanding of how to prepare their environment and their staff for an ISE deployment. This session is targeted at Network and Security Engineers, who are tasked in deploying ISE successfully.

Agenda

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

Cisco Webex Teams

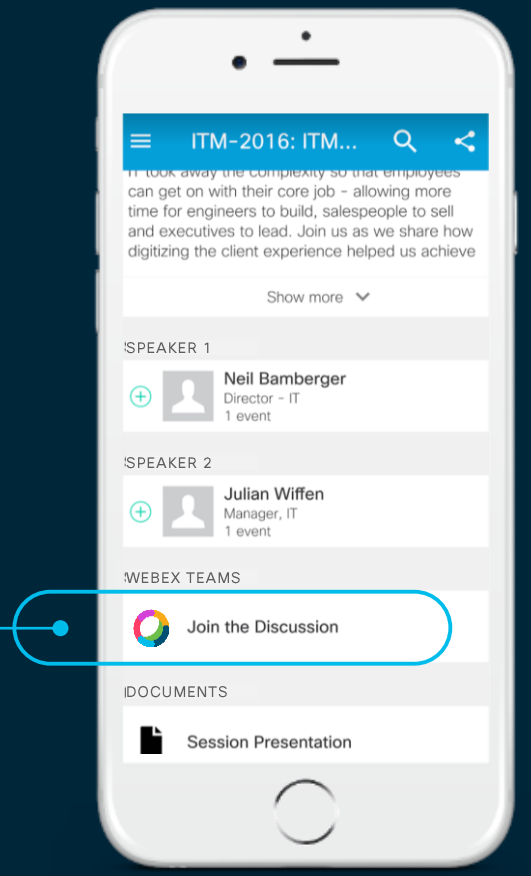
Questions?

Use Cisco Webex Teams 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 Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

Webex Teams will be moderated by the speaker until June 16, 2019.



cs.co/ciscolivebot# BRKSEC-2430

A little about me....

- Started as an early ISE 1.1 customer
- 10+ years of network & security experience
- Lots of paper: BS and MS in IT Security, 2x CCIEs (Data Center + Security), CISSP, and various other industry certifications
- Co-organize for the largest Cisco Meetup study group – Routergods and owner of network-node.com blog
- ...Have a lot of cats...

Agenda

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

Why isn’t there any easy button?

- Often need to work with other teams in the organization:
  - Active Directory
  - PKI
  - Desktop Support
  - Virtualized environment
  - etc
- Discovery
- Planning & Staging

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

Planning is essential to any successful development.

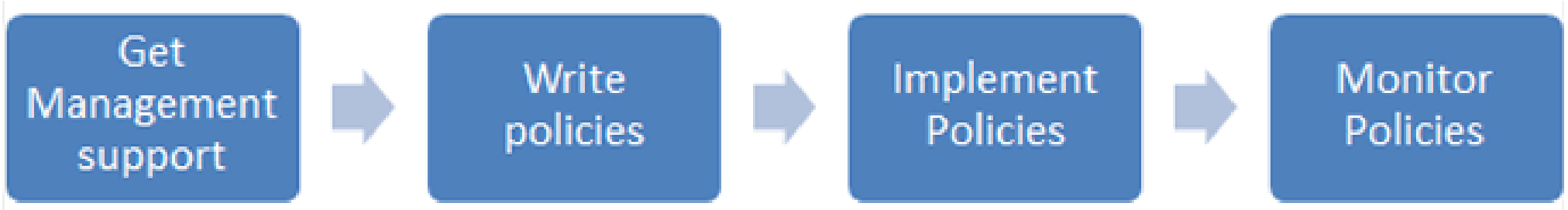
Defining your Security Policy

What is an IT security policy?

"Identifies rules and procedures for all individuals accessing and using an organization's IT assets and resources."

Why is your IT Security Policy important to ISE?

- ISE cannot write the organization's security policy for you
- Know your security policy before you start deploying ISE
- Management buy-in



- Monitor and update polices with your IT Security Policy

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

Where can ISE help achieve these objectives?

- Wired
- Wireless
- VPN
- Device Administration
- Context Sharing (pxGrid)

Agenda

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

Let's talk about the 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

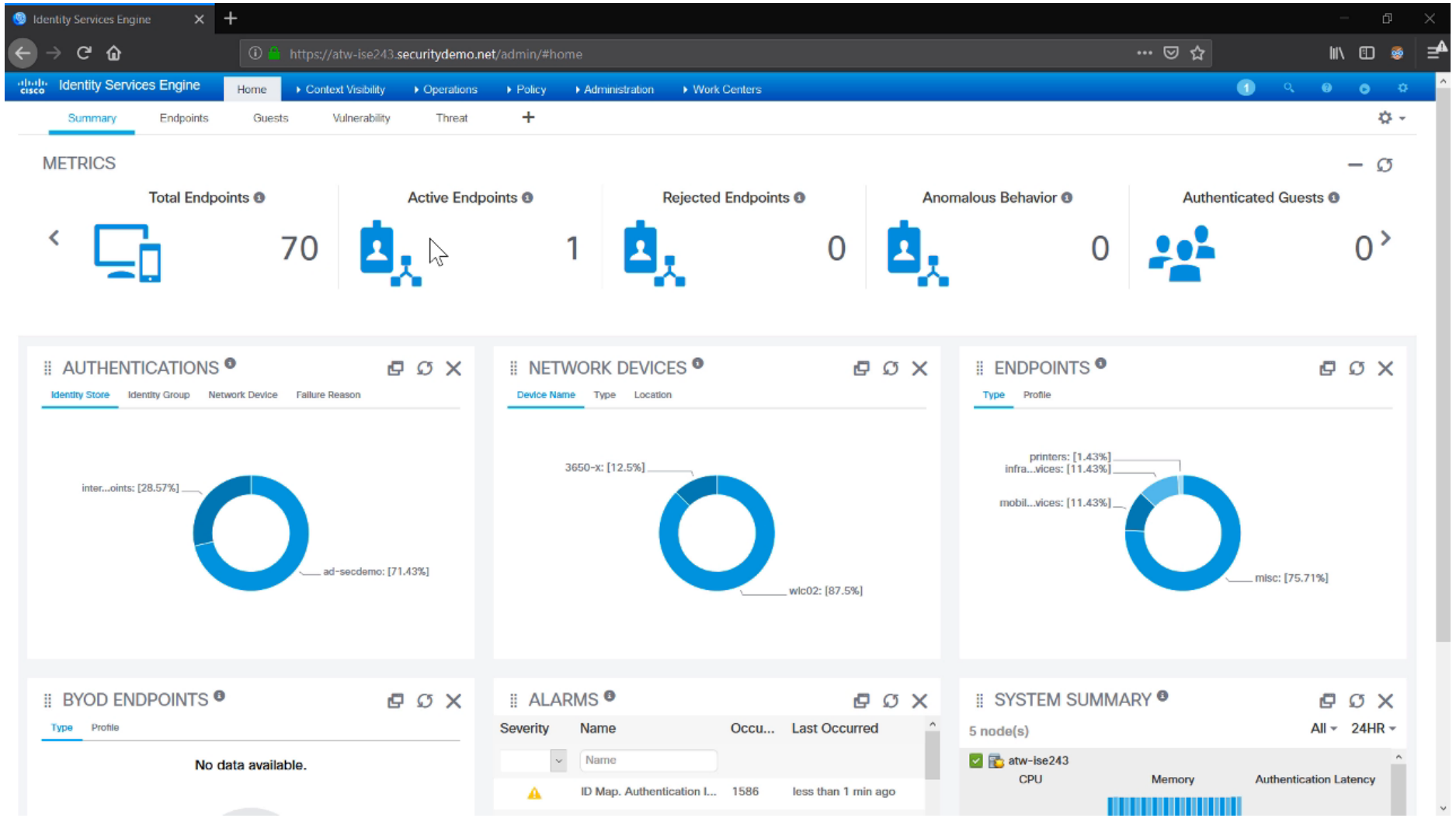
Policy Services Node (PSN)
- Makes policy decisions
- RADIUS/TACACS+ Servers

pXGrid Controller
- Facilitates sharing of context

Different PSN Services

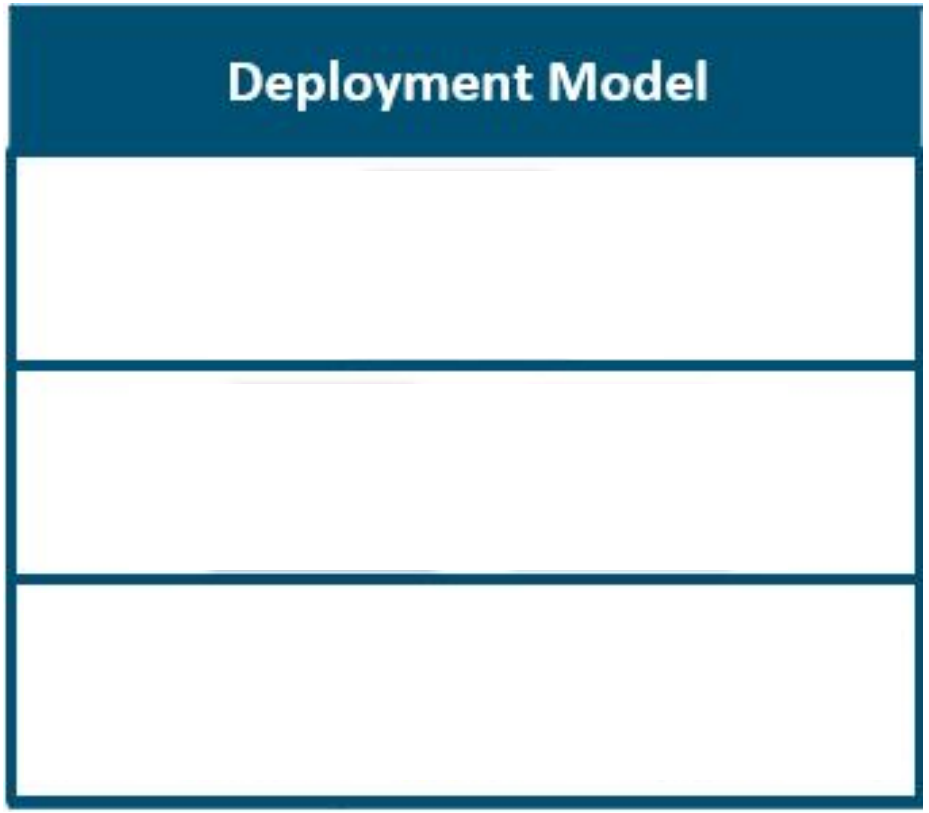
- Session – RADIUS, Guest, Posture, MDM, BYOD/CA
- Profiling
- Threat-Centric NAC (TC-NAC)
- SGT Exchange Protocol (SXP)
- Device Admin (TACACS+)
- Passive Identity

Changing the Persona and Enabling Services



ISE Deployment Models

- Standalone/All Persona
- Hybrid
- Distributed



Important Scalability Numbers – ISE 2.6

Deployment Type	Max # of Concurrently Connected Endpoints in ISE Deployment	Max # of Concurrently Connected Endpoints per PSN
Distributed Deployment	2,000,000 – 3695 as PAN and MnT 500,000 – 3595 as PAN and MnT	10,000 - 100,000 for 36xx series 7,500 – 40,000 for 35xx series
Hybrid Deployment	50,000 – 3695 as PAN and MnT 25,000 – 3655 as PAN and MnT 10,000 – 3615 as PAN and MnT 20,000 – 3595 as PAN and MnT 7,500 – 3515 as PAN and MnT	10,000 - 50,000 for 36xx series 5,000-20,000 for 35xx series
Standalone Deployment	50,000 – 3695 as PAN and MnT 25,000 – 3655 as PAN and MnT 10,000 – 3615 as PAN and MnT 20,000 – 3595 as PAN and MnT 7,500 – 3515 as PAN and MnT	10,000 - 50,000 for 36xx series 5,000-20,000 for 35xx series

ISE Deployment Models

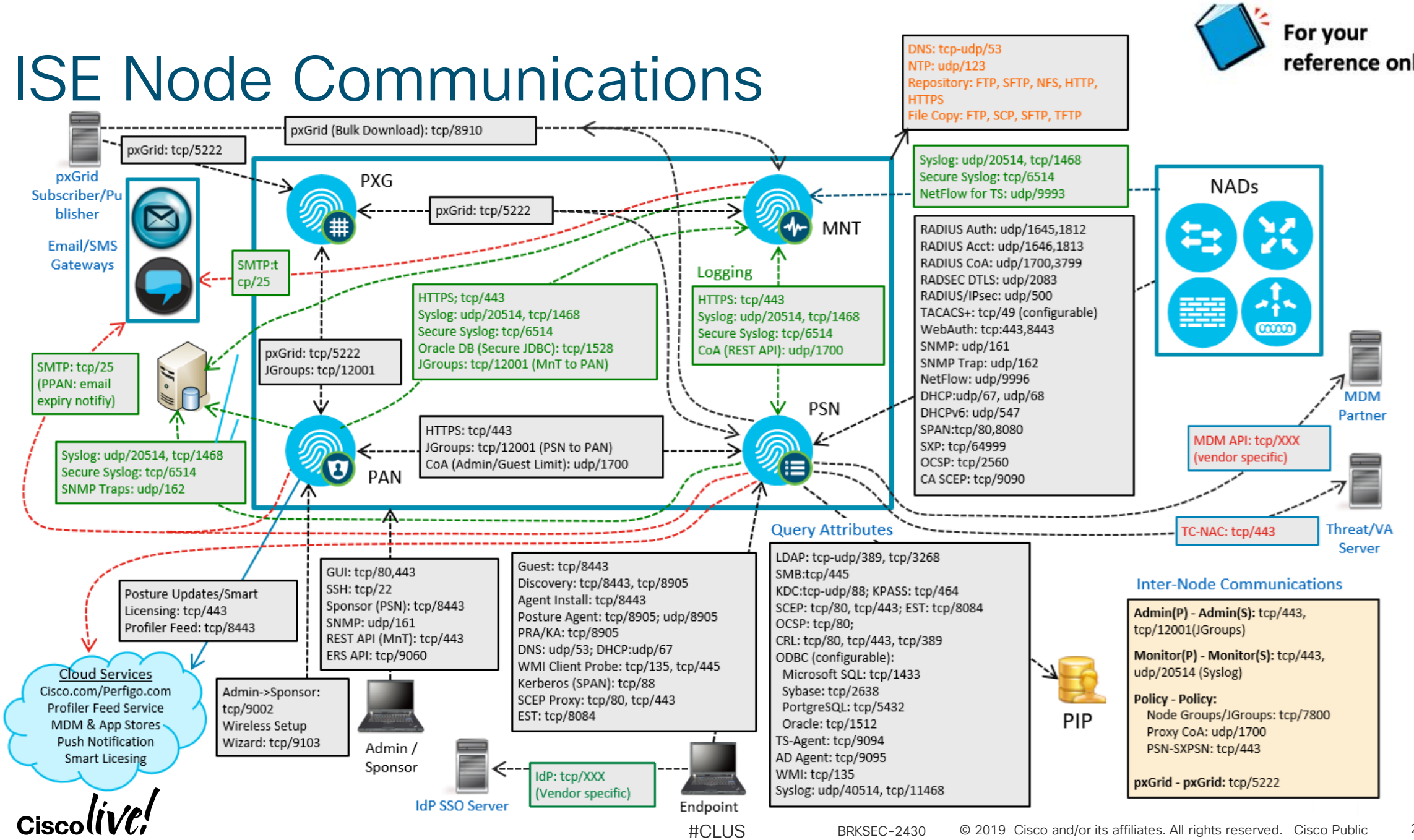
Separate pxGrid nodes?

Deployment Type	Platform	Max Subscribers (Shared PSN/PXG)	Max Subscribers (Dedicated PSN/PXG
Standalone	3515/3595	2	N/A
PAN/MnT/PXG on same node + dedicated PSNs	3515/3595	5	15
Dedicated – All personas on dedicated nodes	3515	-	15
Dedicated – All personas on dedicated nodes	3595	-	25

Other General Considerations

- Concurrently connected endpoints
- Redundancy
- High Availability
- Scaling options
- Latency considerations
  - 300ms between PAN and PSN
  - QA-tested guardrail
- Ports considerations for firewalls and ACLs

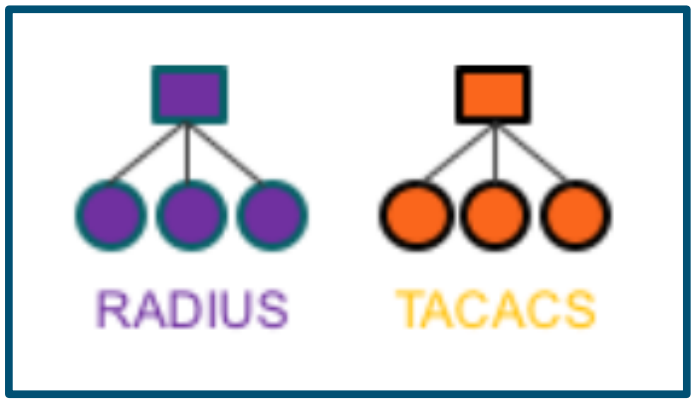
ISE Node Communications

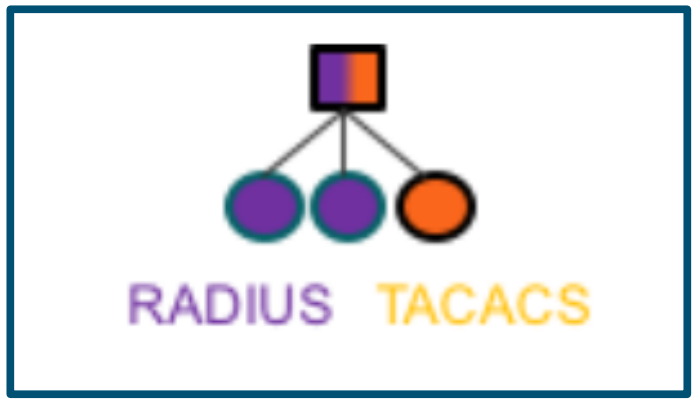


RADIUS & TACACS+ Deployment Options

Three deployment 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





When do we separate TACACS+ and RADIUS?

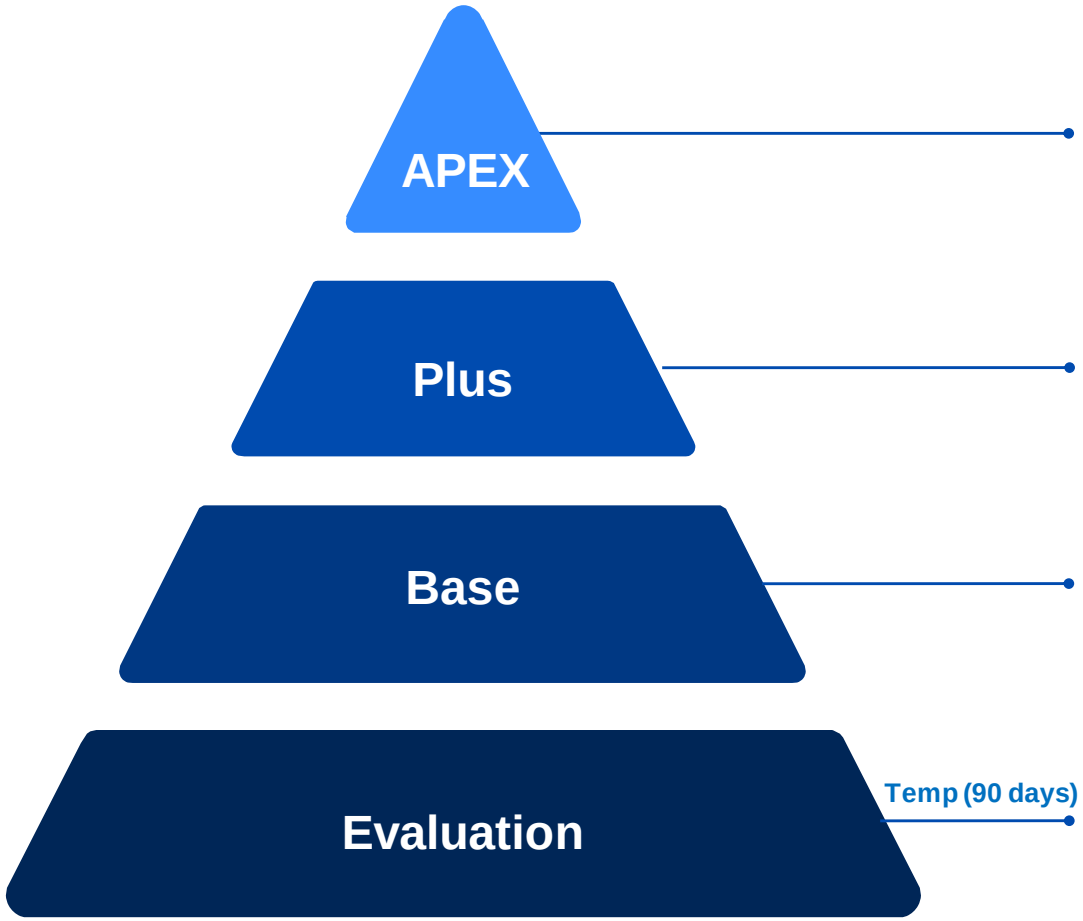
Keep the following in mind:

- How many network devices?
- Number of TACACS+ & RADIUS sessions
- Scripts?
- Network management tools?
- MnT is not taxed is both deployments are large or busy
  - Potential for increased log retention on both deployments
- Per-PSN utilization and load

Hardware Appliance or VM?

- Inter-team communication
- Follow the VM requirements:
  - Sizing
  - OVAs when possible
  - Resource Reservations
- NO Snapshots
- Don’t reduce size of VMs below recommendations

Understanding the ISE License Types



- Third Party Mobile Device Management (MDM)
- Posture Compliance
- Threat Centric NAC (TC-NAC)

- BYOD with built-in Certificate Authority Services
- Profiling and Feed Services
- Endpoint Protection Service (EPS)
- Cisco pxGrid

- Basic network access: AAA, IEEE-802.1X
- Guest management
- Easy Connect (Passive ID)
- TrustSec (SGT, SGACL, ACI Integration)
- ISE Application Programming Interfaces

- Full Cisco ISE functionality for 100 endpoints.

Device Admin

- Cisco ISE requires a Device Administration license to use the TACACS+ service on top of an existing Base or Mobility license.

License Features

For your reference only

Features included by license type

		Base				Device Admin	Plus					ISE Apex + AnyConnect Apex		
		RADIUS / 802.1x	AAA	TrustSec security group tagging	Guest services	TACACS+	Rapid threat containment	ANC/EPS	Device profiling and feed service	BYOD with CA	pxGrid context sharing	MDM / EMM	Threat-Centric NAC	Posture (endpoint compliance and remediation)
Control all access from one place	**Guest** Provide unique guest permissions to visitors	●	●		●									
	Secure access Control user access and ensure device authentication	●	●	●										
	Device Admin Differentiate access for device administrators					●								
	BYOD Seamlessly onboard devices with the right access	●	●	●					●	●				
See and share rich user and device details	**Visibility** See when, where, and why users are on your network	●	●	●					●					
	Integration Share information with other products	●	●	●					●		●			
	Compliance Ensure that endpoints meet network standards	●	●	●								●		●
Stop threats from getting in and spreading	**Segmentation** Limit exposure with pre-defined access segmentation	●	●	●										
	Containment Reduce risk with rapid threat containment	●	●	●			●	●	●					
	Prevention Prevent breaches at the endpoint level	●	●	●									●	

Understanding How Licensing Works

- Endpoint licenses
  - Concurrently connected endpoints
  - Endpoint disconnects – license added back to store
- Device Admin
  - Per PSN with Device Admin service enabled
  - NOT per device count

Agenda

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

Network Device Discovery

- Support for RADIUS and/or TACACS+?
- Cisco device?
  - Hardware Model
  - IOS Version
  - Count

Network Device Discovery (cont'd)

- Non-Cisco device?
  - Vendor Name
  - Hardware Model
  - OS Version
  - Vendor-Specific RADIUS dictionary needed?
  - Support for RADIUS CoA or SNMP CoA?

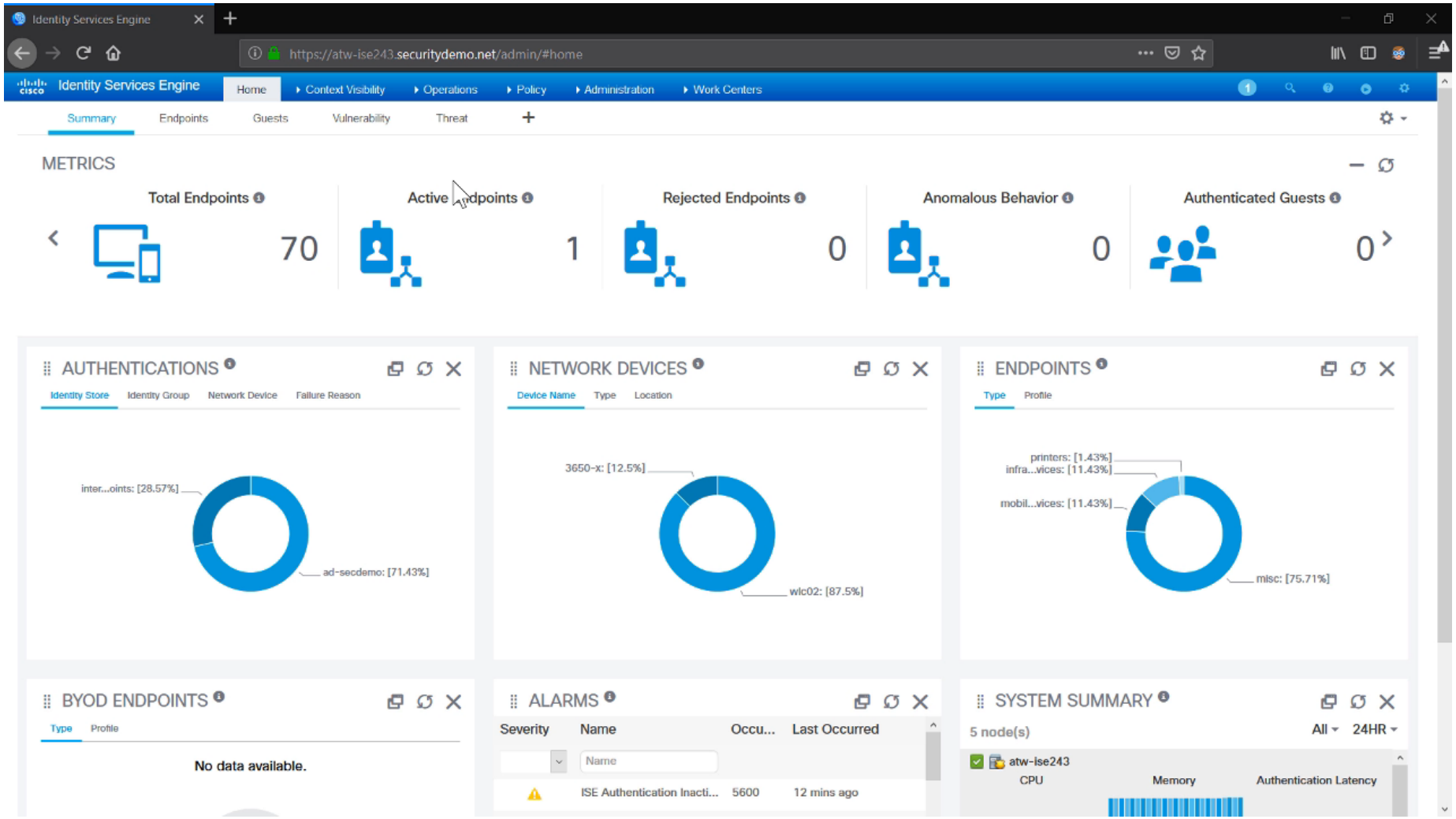
Why is this so important?

Preparation will save you a lot of time and tears

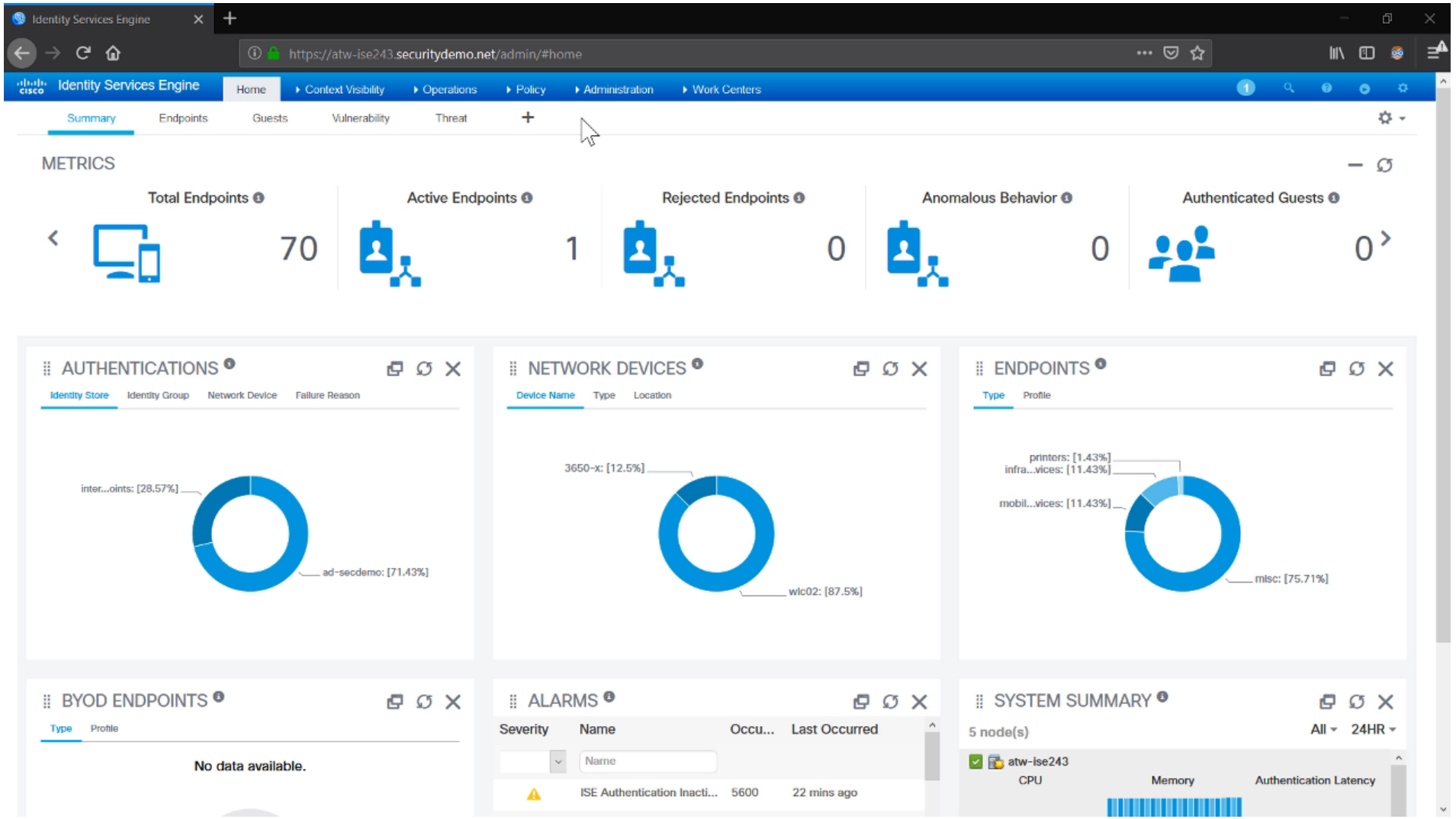
- RADIUS Vendor Dictionaries
- Network Device Profiles Creation
- IOS Versions and Capabilities
- Hardware Limitations
- Protocol Support

Adding RADIUS Vendor Dictionaries

Policy>Policy Elements>Dictionaries>Radius>RADIUS Vendors



Creating a Network Device Profile for 3rd Party Vendors



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] / Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
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
CGS 2520	IOS 15.2(2)E3	√	√	√	√	X	√	√	√

Additional Tips

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

Agenda

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

Identity Source support in ISE

- Active Directory
- LDAP
- ODBC
- RADIUS Token Servers
- RSA SecurID
- SAMLv2 Identity Provider
- Certificate Authentication Profiles for EAP-TLS'
- Social Login

Integration with Identity Sources is Key

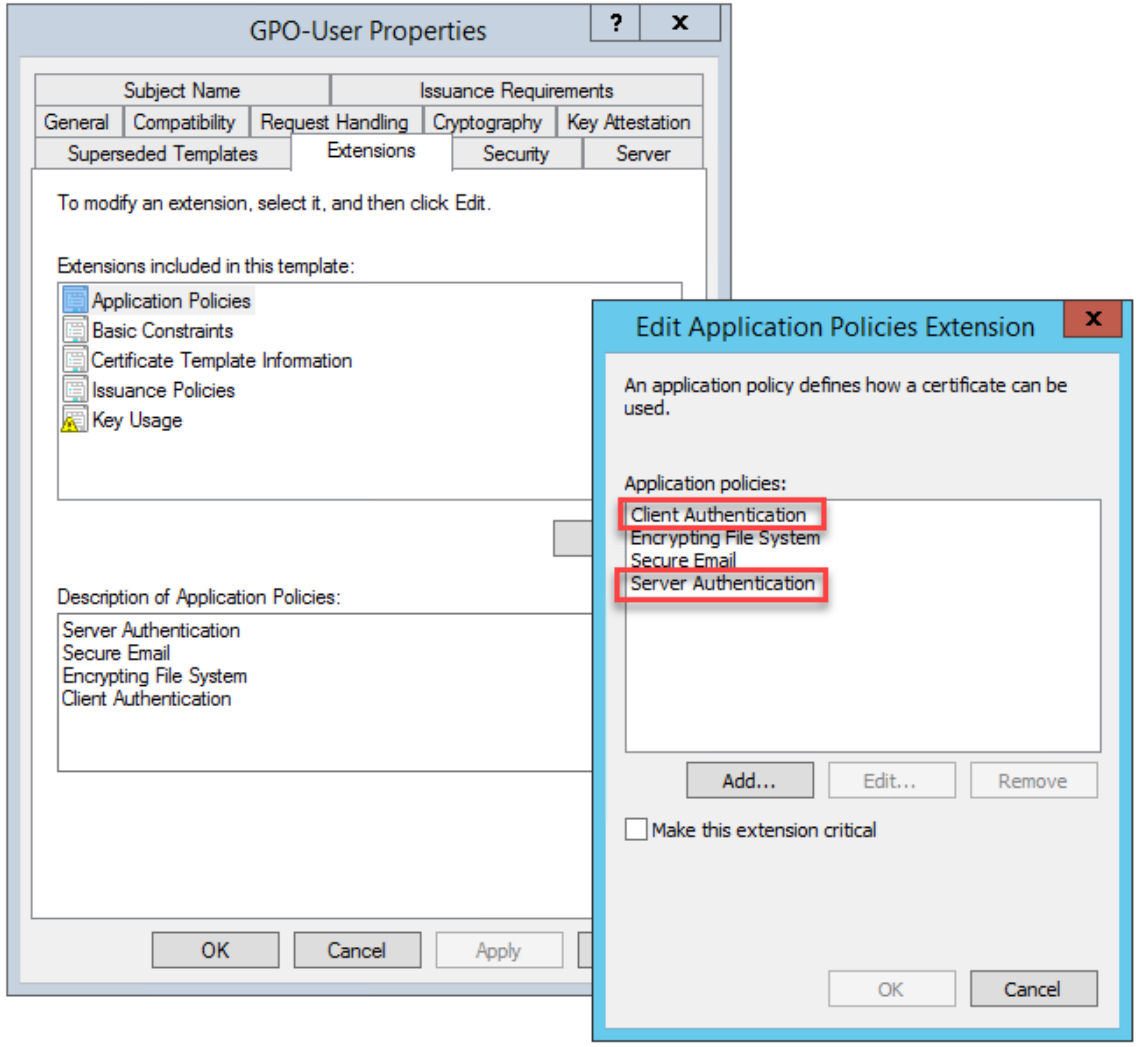
Get the teams that manage the identity source involved early…

- Active Directory?
  - Multiple domains?
  - Multiple forests?
  - Version of AD?
- Common Issues with Domain Join
  - Time Skew
  - AD DNS SRV Records

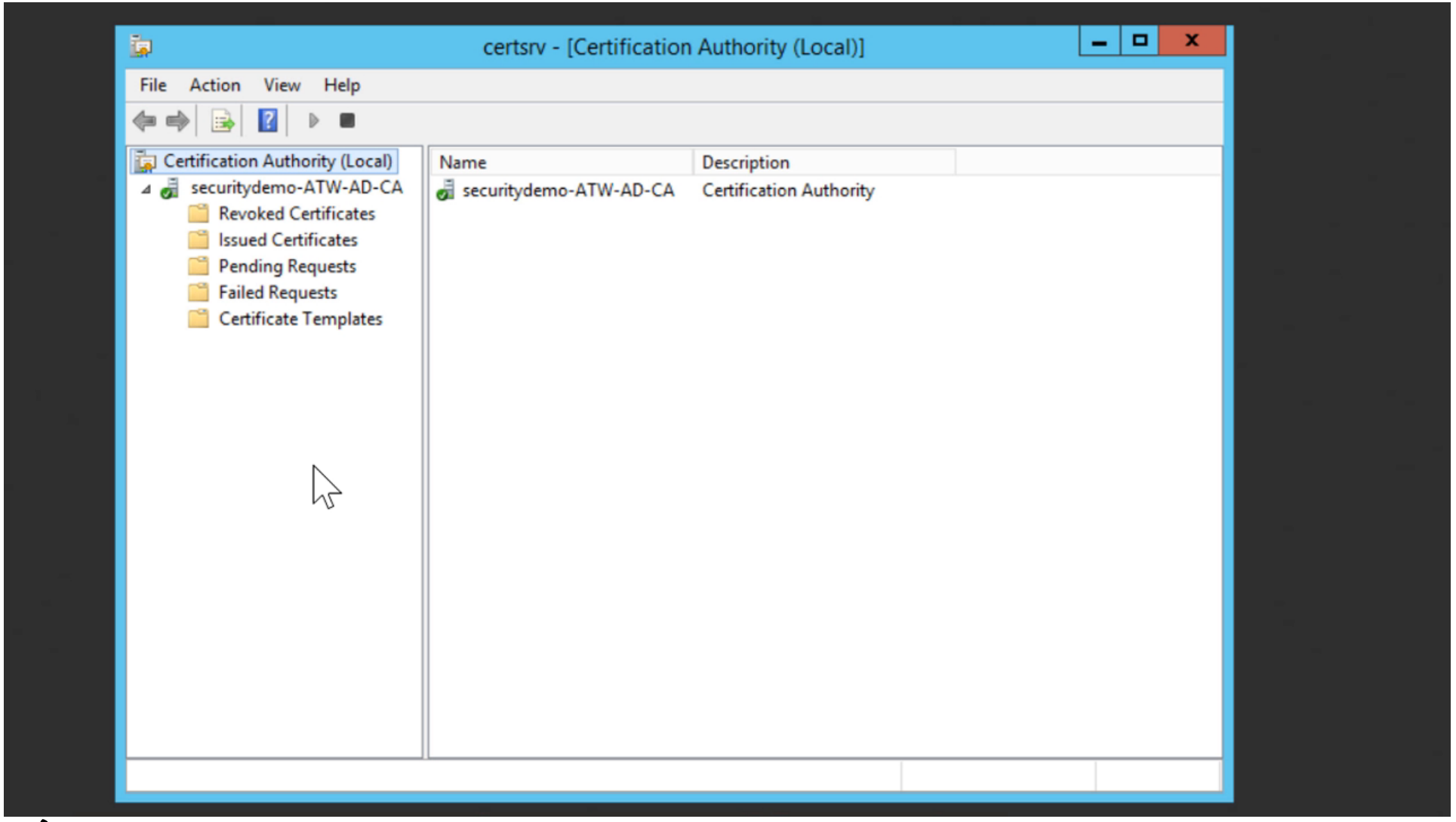
Prepare the Certificates

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

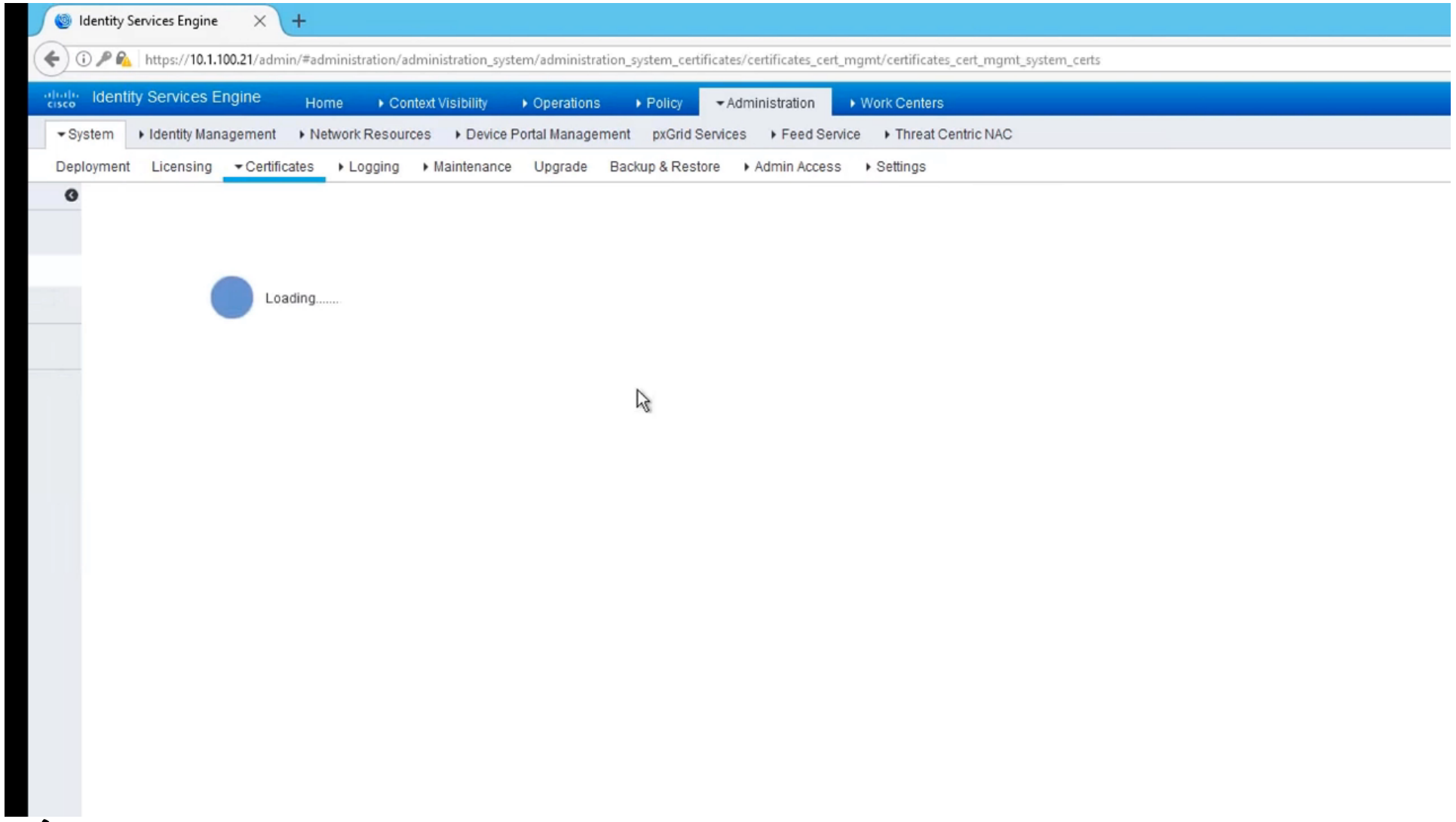
Sample User Certificate Template



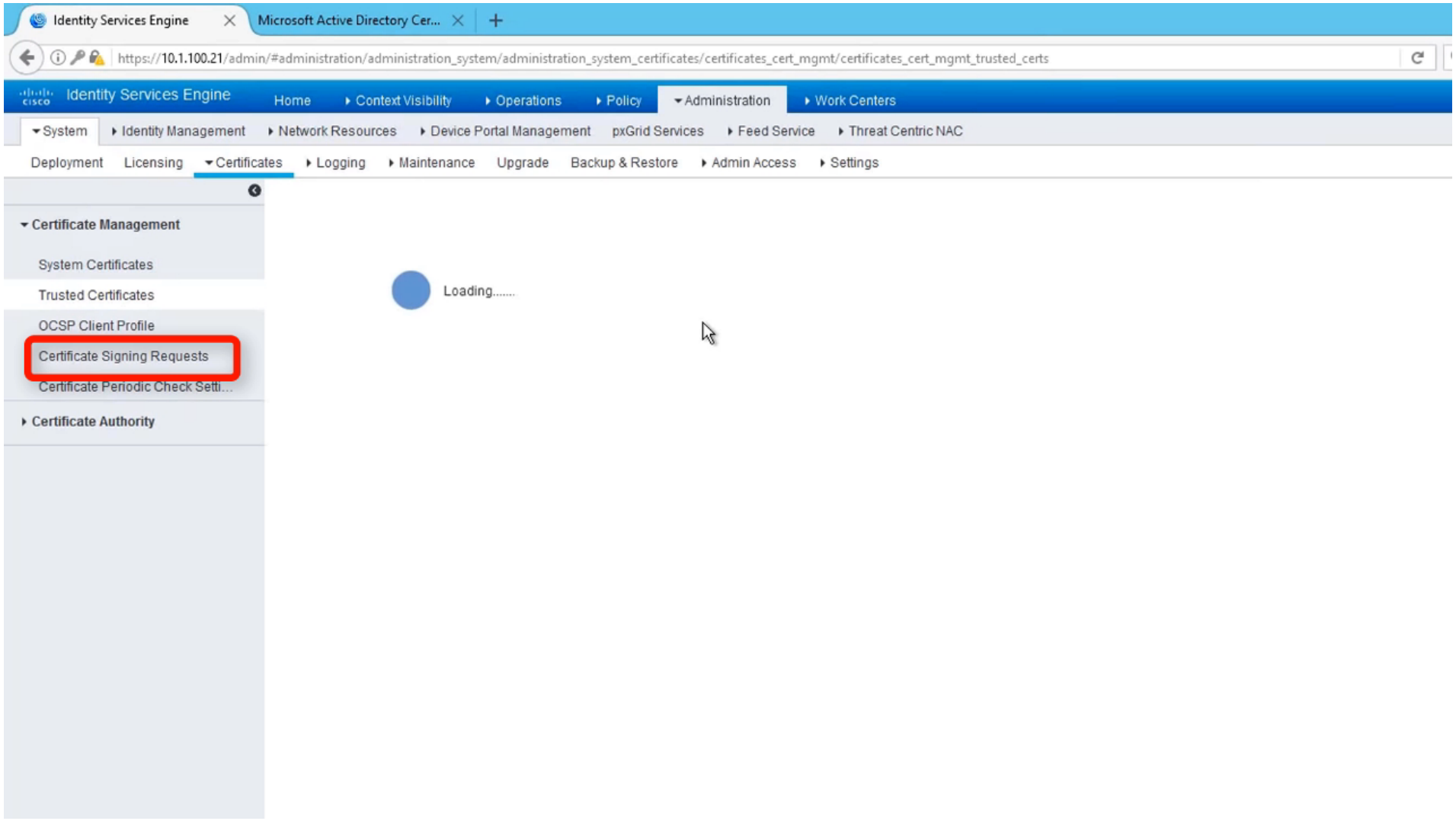
Sample pxGrid Certificate Template



Add a Trusted Root Certificate in ISE



Getting a Certificate Signing Request



Agenda

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

Understand your Endpoints & Supplicants

- Windows 7, 8/8.1, and 10
  - Native Supplicant
  - AnyConnect Network Access Manager (NAM)
- Mac OS X
- Apple iOS
- Android

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

- Group Policy for:
  - Supplicant configuration
  - Pushing certificates
  - Pre-configure SSIDs – better user experience
- Involve the Active Directory Team
- Caveats to be aware of:
  - Potential driver issues – Involve the Desktop Support Team
  - Does not support EAP-chaining

Windows 7, 8/8.1, and 10 – AnyConnect NAM

- Eliminates potential issues from drivers
- Standardization for Windows supplicants
- Options for more EAP-Types
- Supports EAP-Chaining (i.e. User + Computer certificate)
- Anyconnect NAM needs to be deployed – Involved Desktop Support
- Caveats to be aware of:
  - AnyConnect Plus licenses
  - AnyConnect NAM only for Windows endpoints

Mac OS X Supplicant

- Version 10.8+ – 802.1X authentication process started automatically
- Pop-up appears on connect to network
  - Zero-touch deployment if alright with pop-up
- Certificates:
  - Client Provisioning and BYOD configuration to install certificate
  - JAMF or another MDM to install the certificate and supplicant profile

Android and Apple iOS BYOD

- (Optional) Onboard through ISE for PEAP or EAP-TLS
- Apple iOS will install the supplicant profile during client provisioning
- Android devices are different:
  - Doesn't trust apps installed other than the app store by default
  - Download of Cisco Network Setup Assistant App from Google Play required
  - Allow the following URLs in your DNS ACL on the wireless controller:
    - android.clients.google.com
    - google.com

Agenda

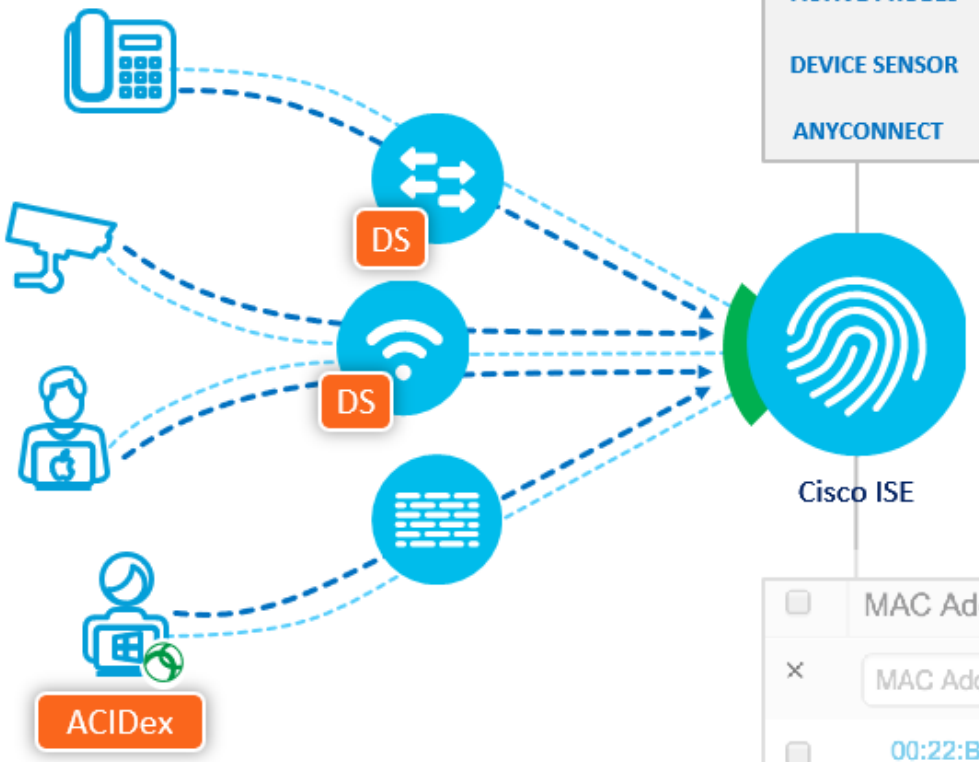
- Where To Start
- ISE Appliances & Deployment Options
- Network Devices
- Identity Sources
- Supplicants
- Profiling
- 802.1x Deployment Phases
- Enforcement
- Day 2 Operations

ISE Profiling

- Because MAC address alone is not enough
- 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

Visibility Data Sources

Endpoints send interesting data, that reveal their device identity



ACTIVE PROBES	Netflow	DHCP	DNS	HTTP	RADIUS	NMAP	SNMP	AD
DEVICE SENSOR	CDP	LLDP	DHCP	HTTP	H323	SIP	MDNS	
ANYCONNECT	ACIDex							

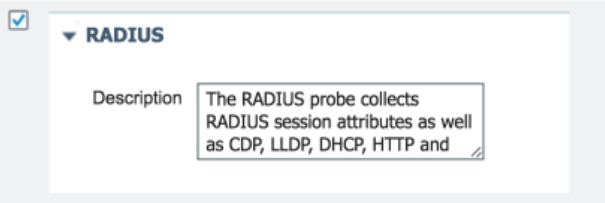
ISE data collection methods for Device profiling

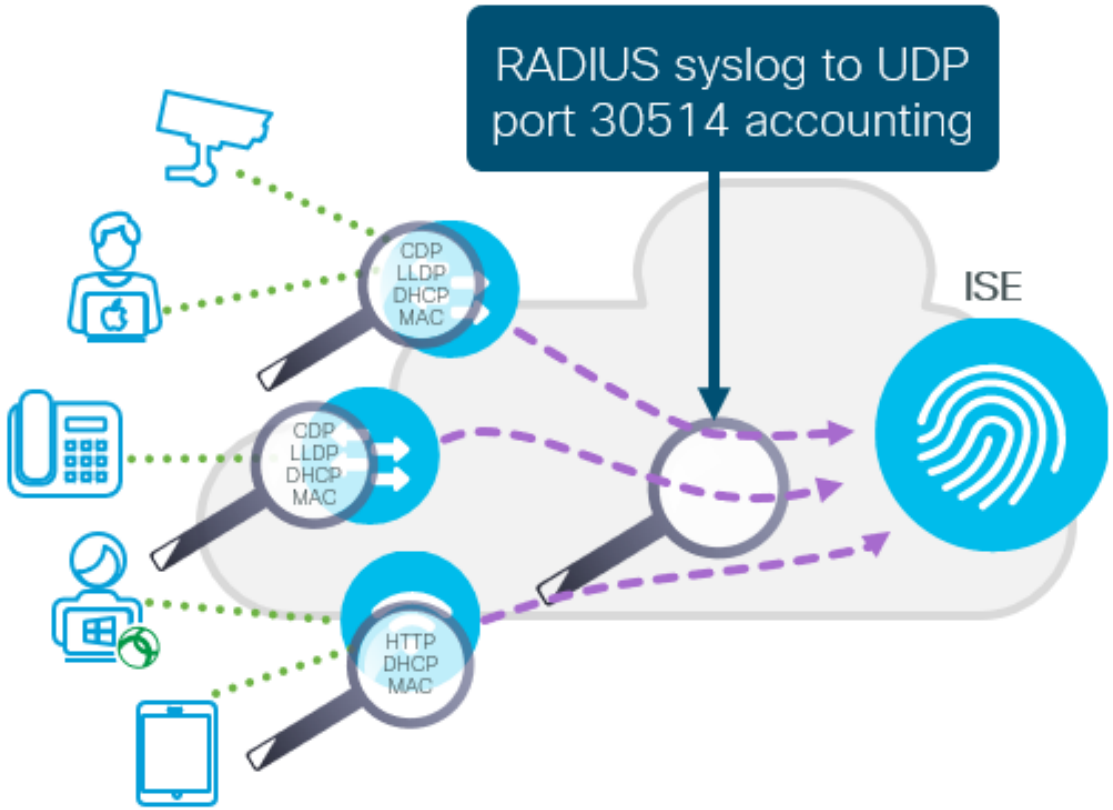
Cisco ISE

Feed Service
(Online/Offline)

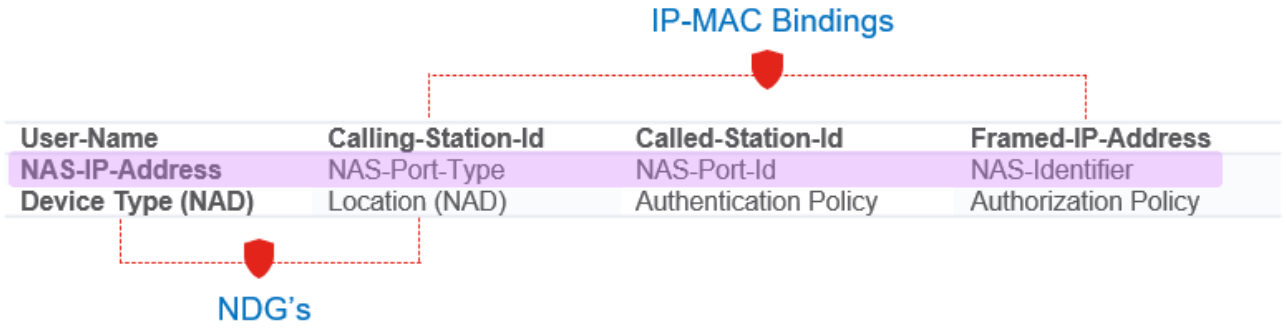
MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

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:



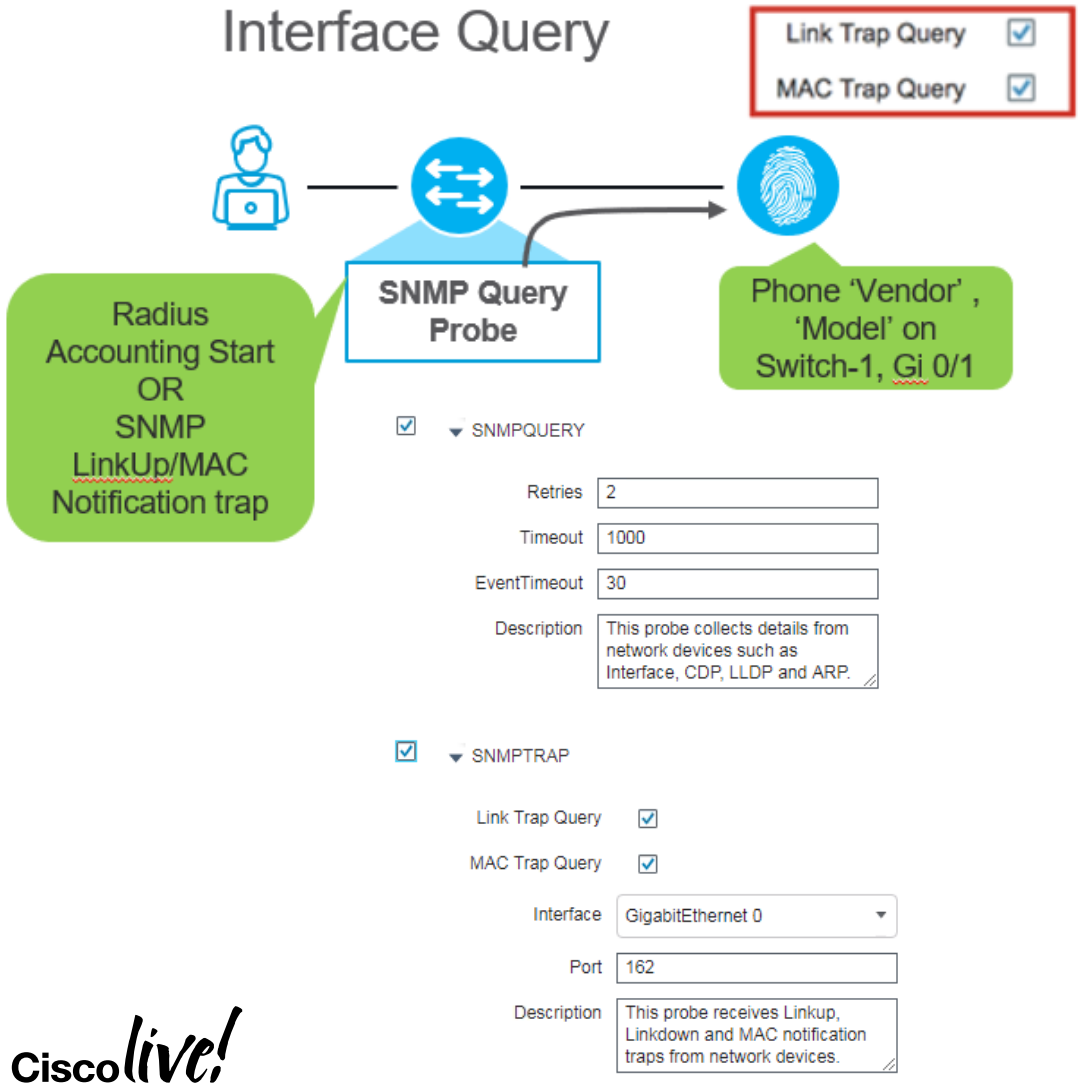
RADIUS Probe Sample Configuration

For your reference only

```
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



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

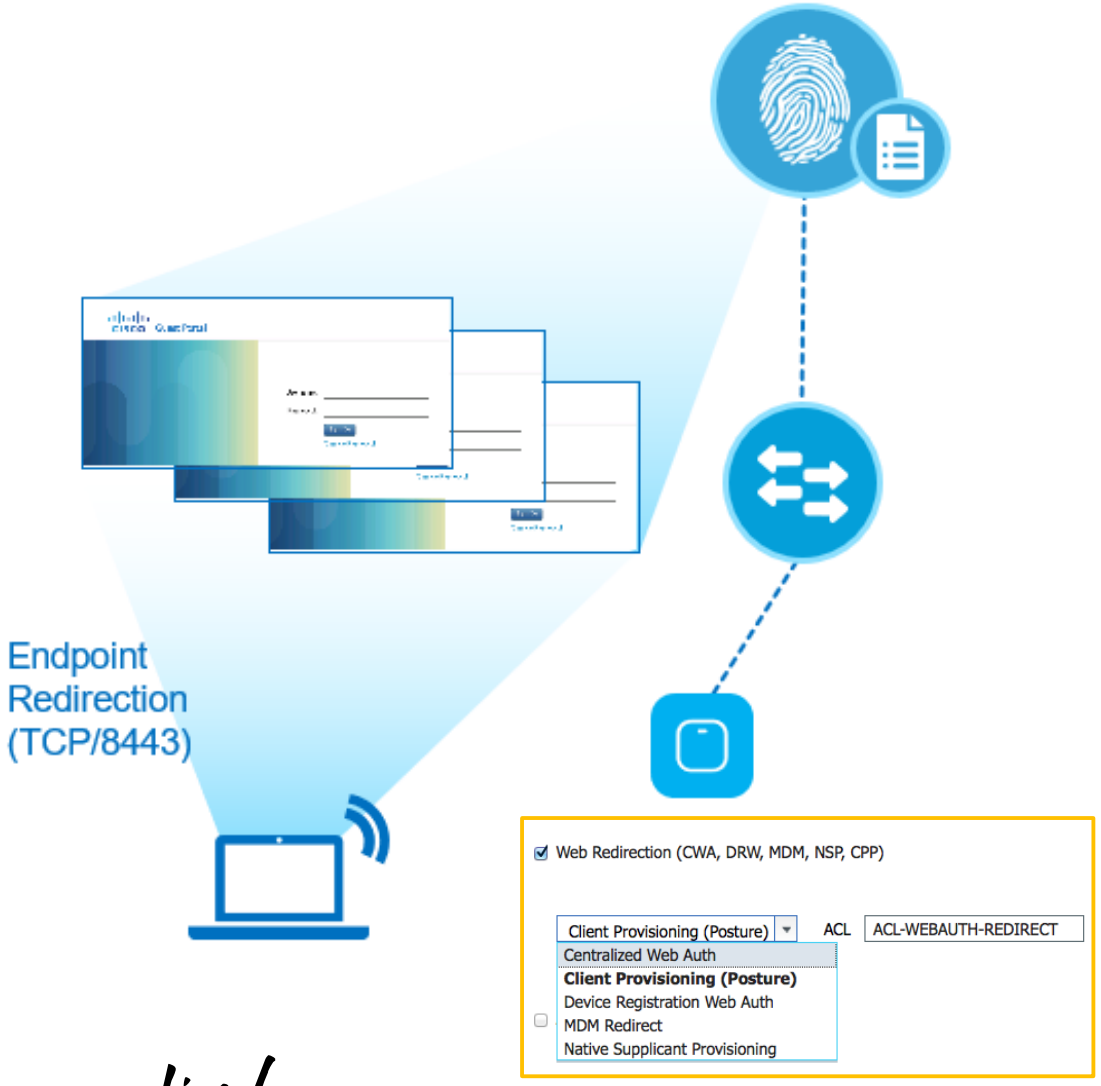
SNMP Probe Sample Configuration

For your reference only

```
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



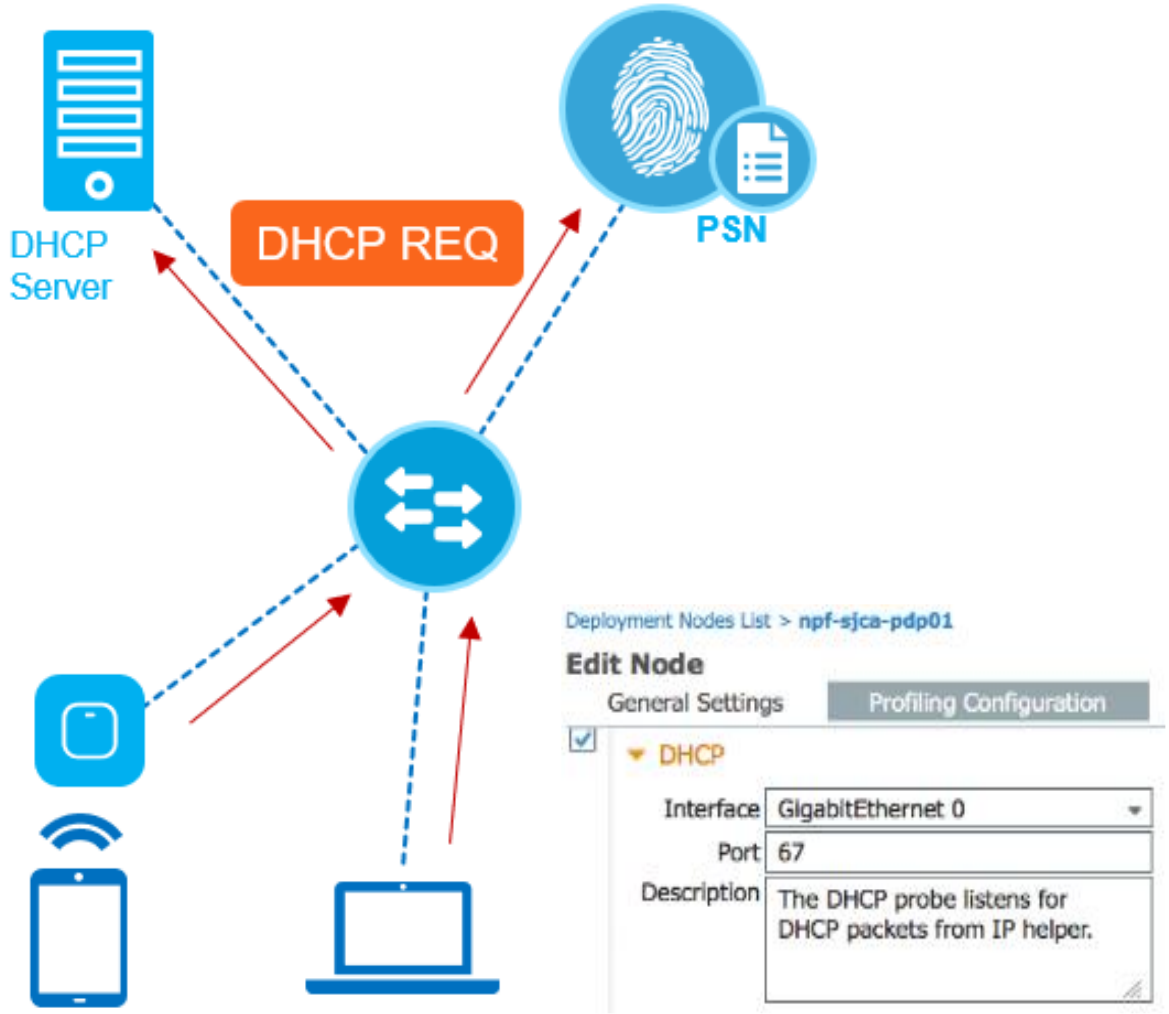
- User-agent is an HTTP request header that is sent from web browsers to web servers. **The user-agent includes application, vendor, and OS information** that can be used in profiling endpoints.
- User-agent attributes can be collected from web browser sessions redirected to ISE for existing serves such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

HTTP Probe Sample Configuration

For your reference only

```
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



- 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

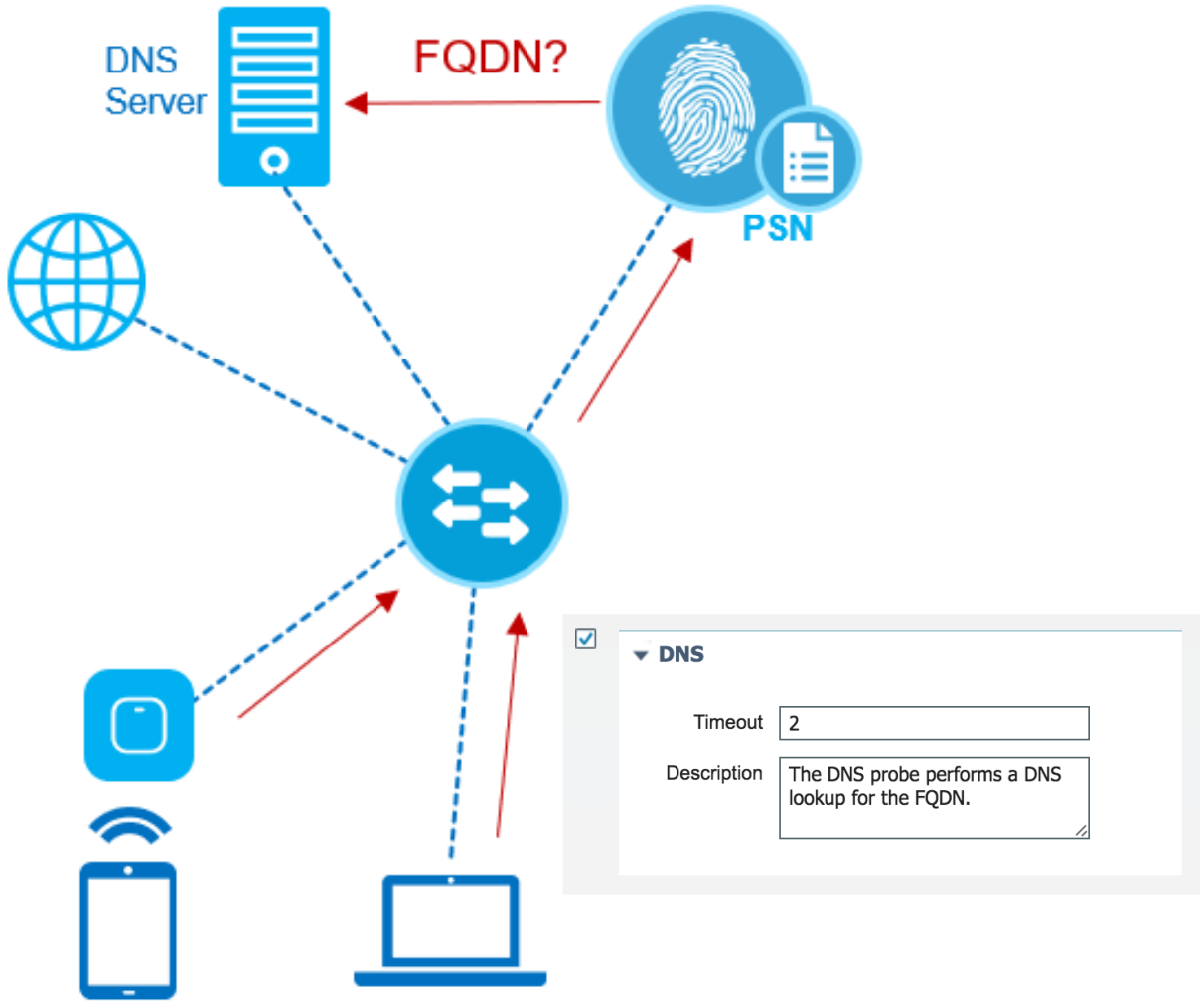
DHCP Probe Sample Configuration

For your reference only

interface vlan 30

ip helper-address <PSN-IP-Address>

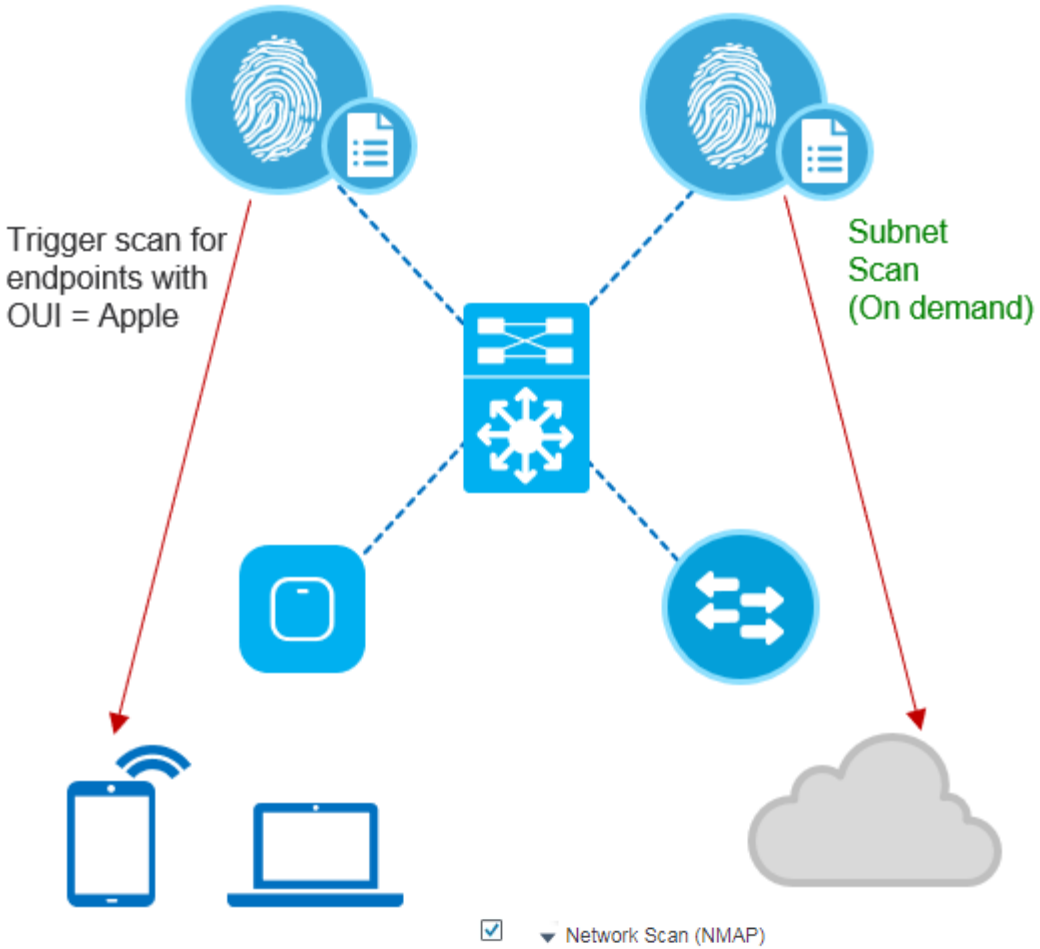
DNS Probe



- 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.

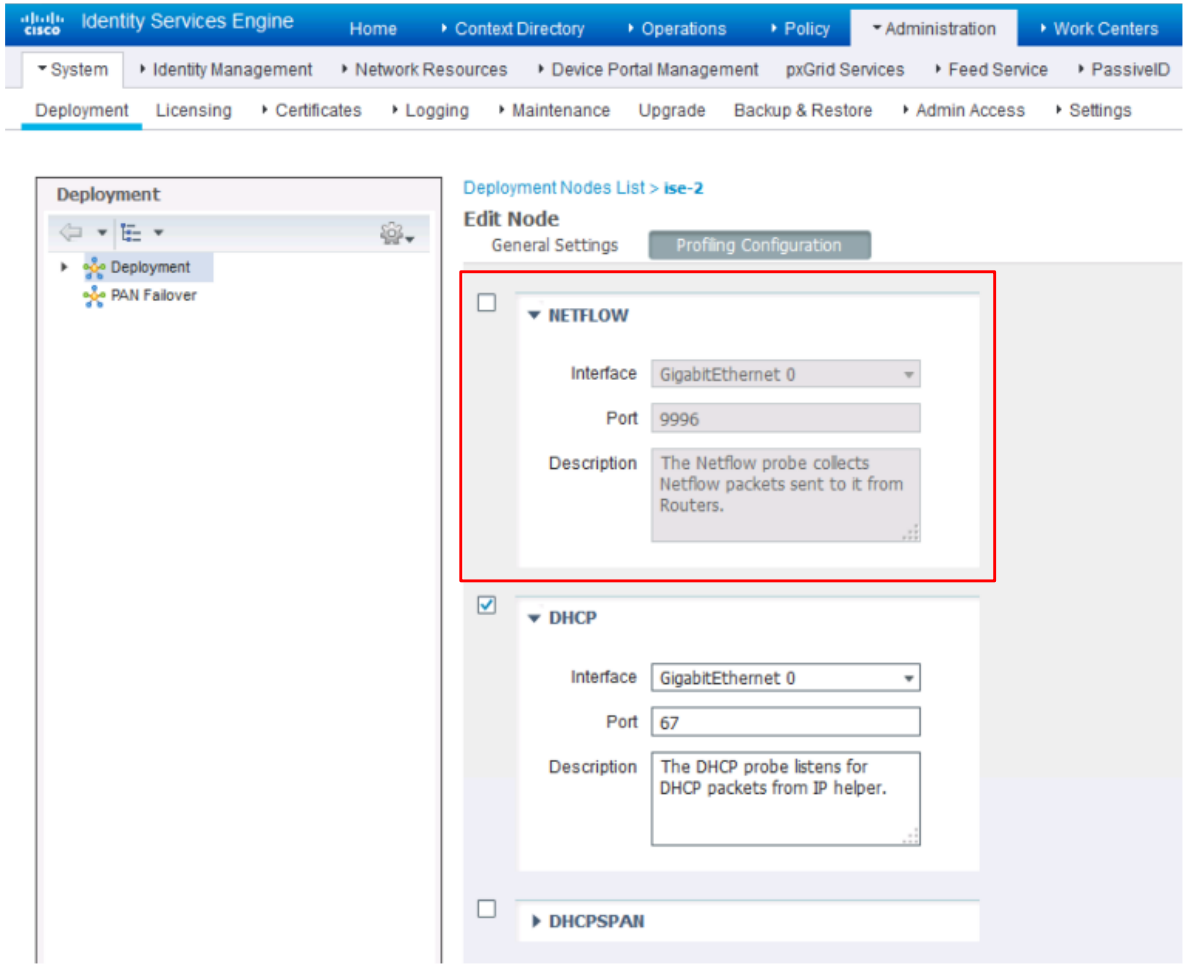
```
DNS Configured in ISE:
!
ip name-server 171.68.226.120
ip name-server 171.68.226.121
!
```

NMAP Probe



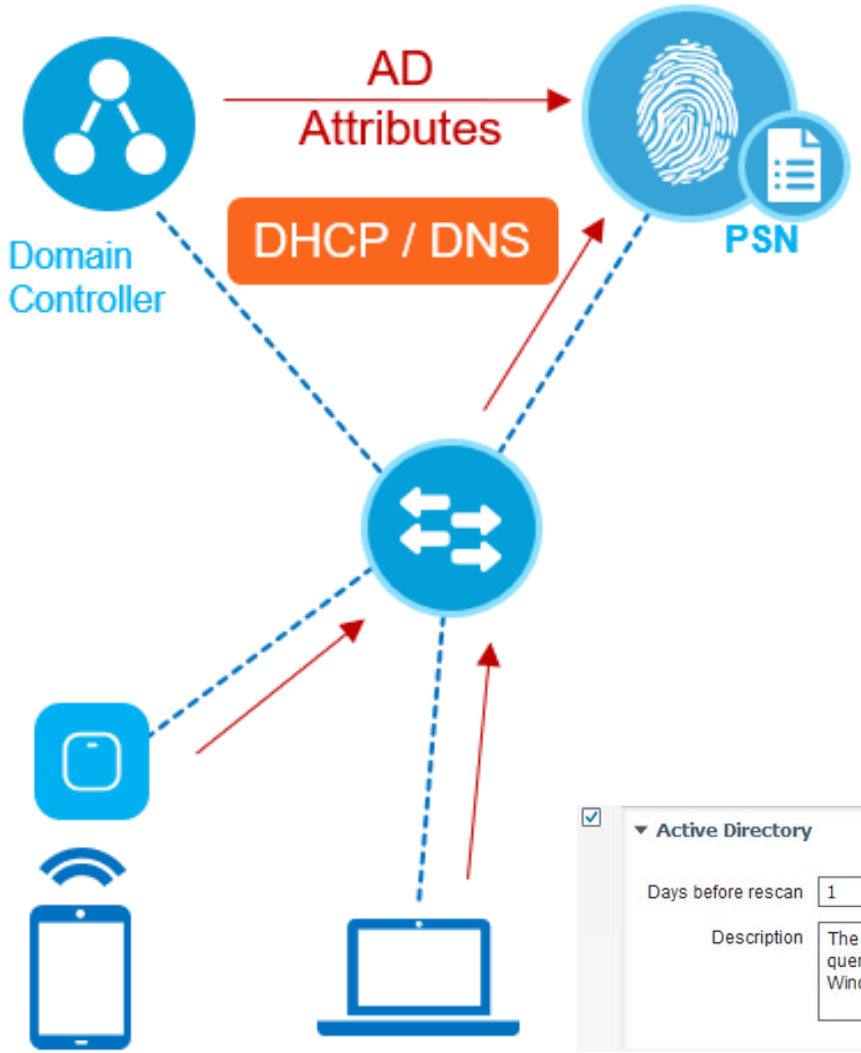
- NMAP utility incorporated into ISE allows profiler to detect new endpoints through a subnet scan and to classify endpoints based on their operating system, OS version, and services as detected by the NMAP.
- The network scan probe is considered an "active" assessment mechanism since it communicates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

NetFlow Probe



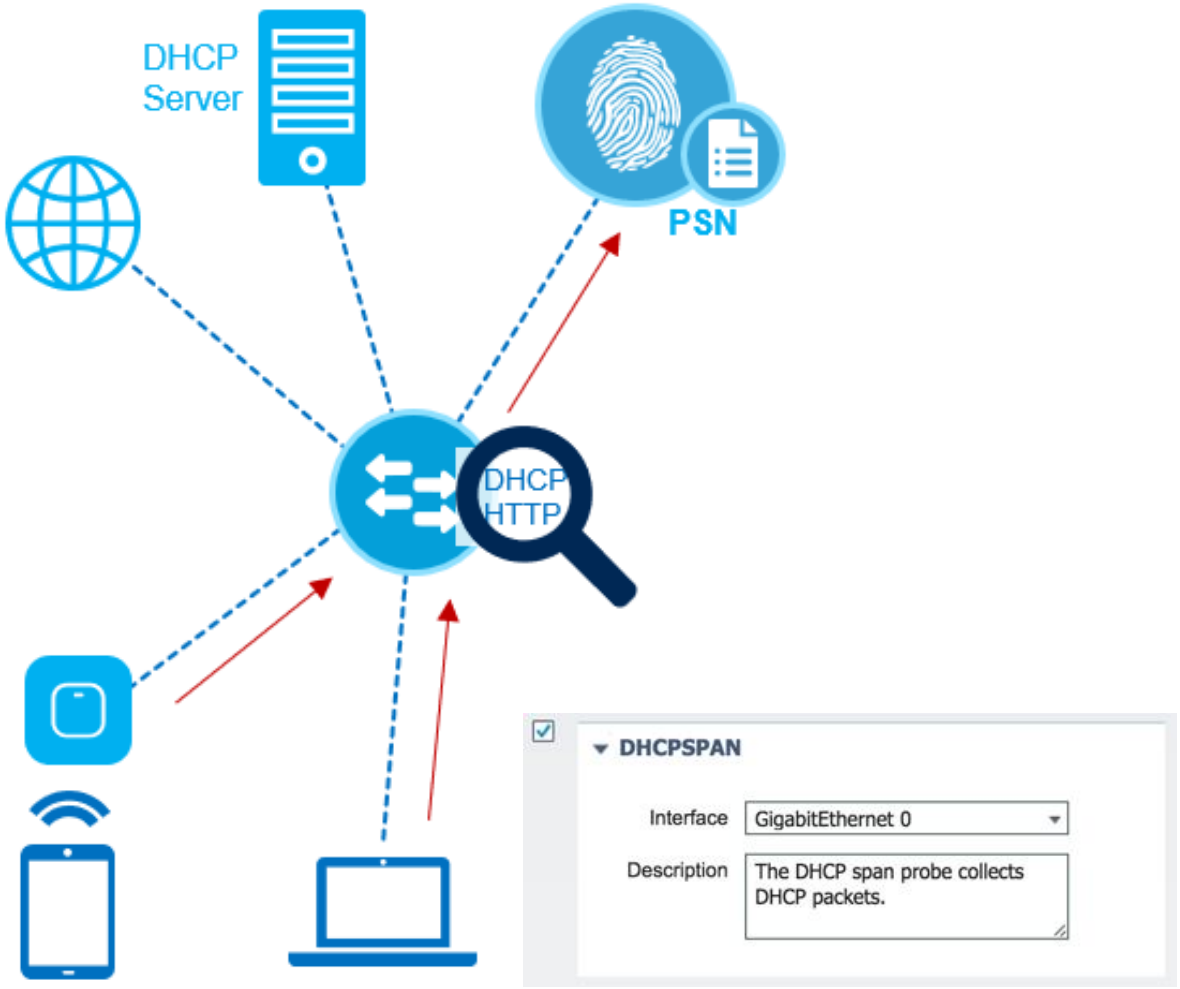
- NetFlow **vendor specific attributes** reveal device identity
- Flow reception on Port # **9996/UDP**
- Cisco ISE profiler implements Cisco IOS NetFlow Version 9, while backward compatible to earlier versions
- Cisco IOS NetFlow Version 5 packets do not contain MAC addresses of endpoints. Prior record 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

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

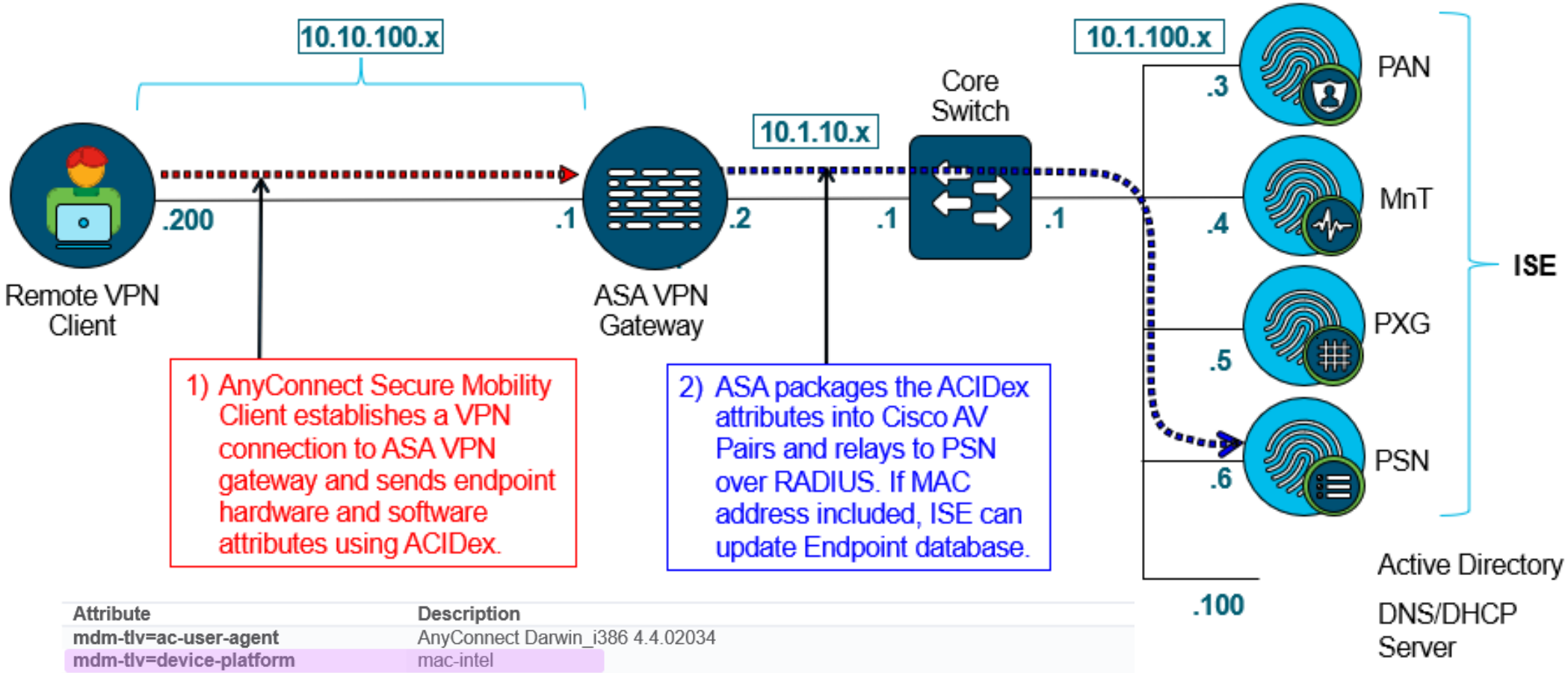
SPAN: DHCP and HTTP Traffic to ISE



- Traffic is mirrored to an Interface on the ISE policy services node
- Both SPAN and remote SPAN are supported
- Provides the same information as the previously mentioned DHCP and HTTP probe but is the least optimal way of sending this information to ISE
- Would not advise to use this if it can be avoided

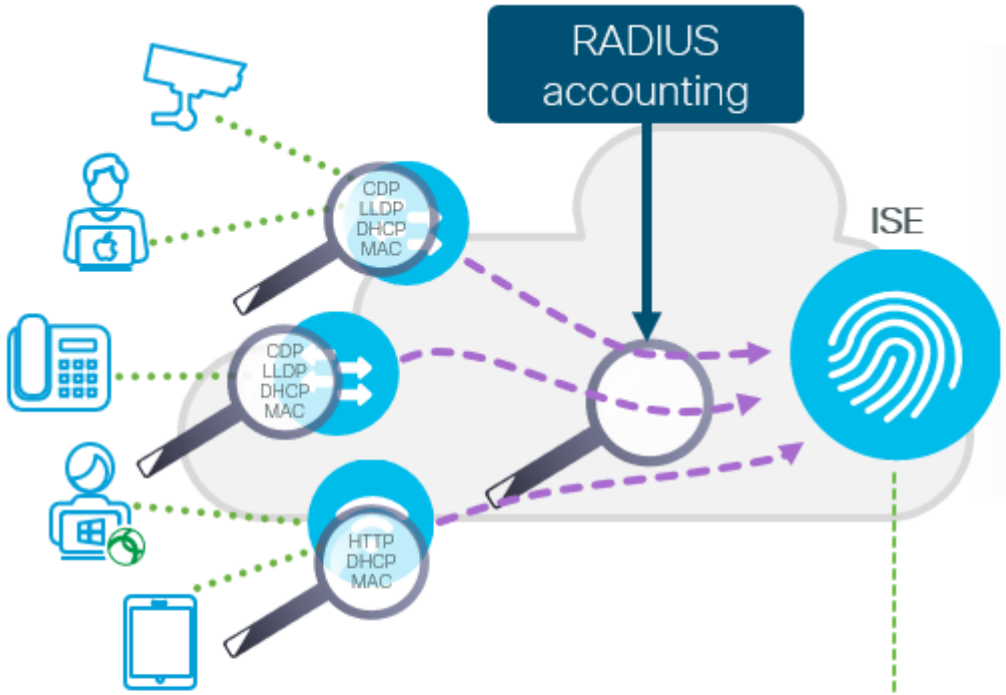
AnyConnect ACIDEX

- Min Ver: AC 3.1MR5 and ASA 9.2.1
- AC 4.1 and ASA 9.3.2 add support for sending the UDID, MEID, or IMEI



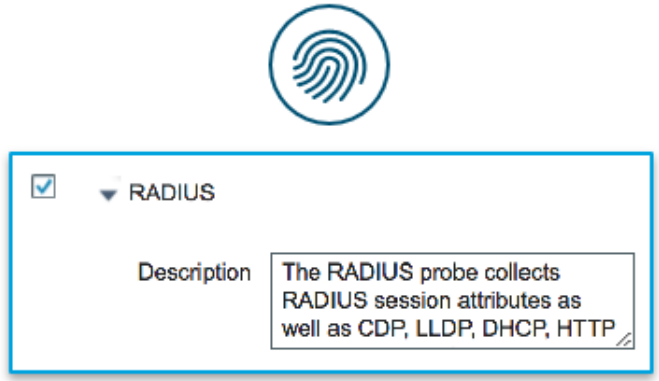
Attribute	Description
mdm-tlv=ac-user-agent	AnyConnect Darwin_i386 4.4.02034
mdm-tlv=device-platform	mac-intel
mdm-tlv=device-platform-version	10.13.6
mdm-tlv=device-type	MacBookPro11,1
mdm-tlv=device-mac	16-d0-98-01-23-45
mdm-tlv=device-public-mac	16-d0-98-01-23-45
mdm-tlv=device-uid	CF1DA510777DC410F2809E5794A829AF74D841BB864E24FFB38C2A1154BBD4E4

Simplify Profiling with Device Sensor



- MAC OUI
- CDP/LLDP
- DHCP
- HTTP (WLC only)
- mDNS,
- H323,
- MSI-Proxy (4k only)

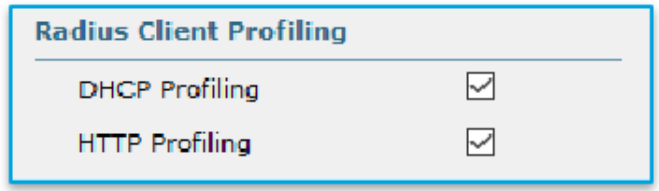
Data From Device Sensor	+	Profile Conditions	=	PROFILED
Example: MAC OUI + Lexmark		If DHCP Class ID Contains E260dn		It's a Lexmark E260n Printer



From 15.0(2)SE

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

From AireOS 7.2



WLANs > (SSID) > Advanced

Device Sensor for Wired

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

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

```
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
```

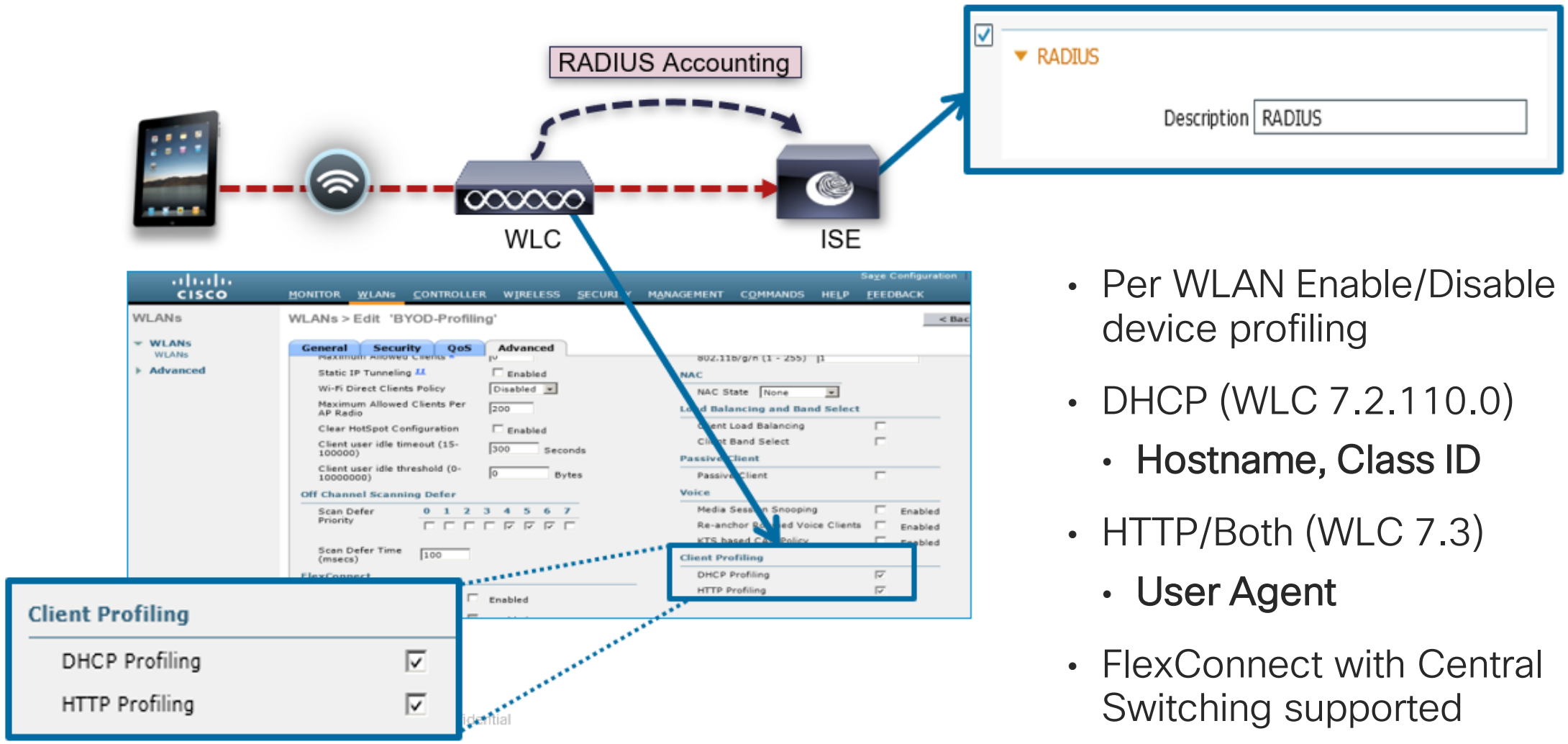
2) Enable sensor data to be sent in RADIUS Accounting including all changes

```
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
```

Wireless Device Sensor

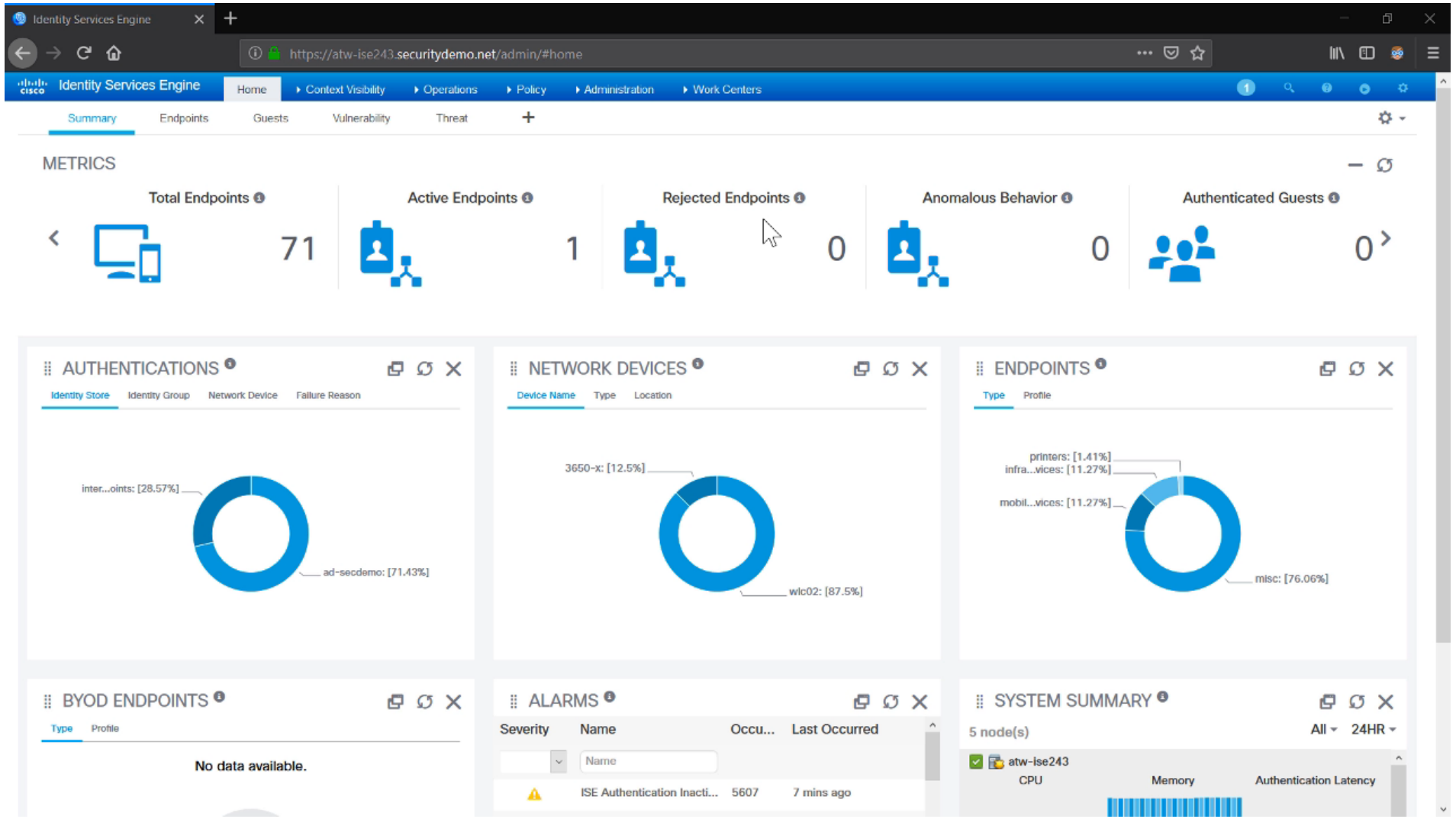


- Per WLAN Enable/Disable device profiling
- DHCP (WLC 7.2.110.0)
  - **Hostname, Class ID**
- HTTP/Both (WLC 7.3)
  - **User Agent**
- FlexConnect with Central Switching supported

Profiler Feed Service

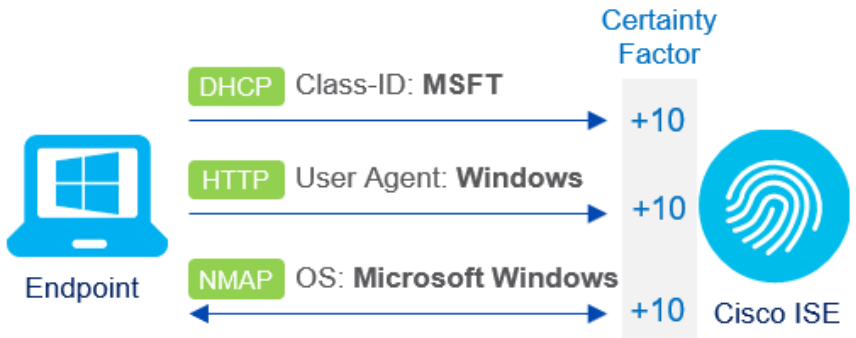
- Provides new and updated
- Ways to update:
  - Manual
  - Scheduled
  - Downloaded for offline installation
- Updates MAC OUIs

Profiler Feed Service



Profiling Policies

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



Profiler Policy List > **Microsoft-Workstation**

Profiler Policy

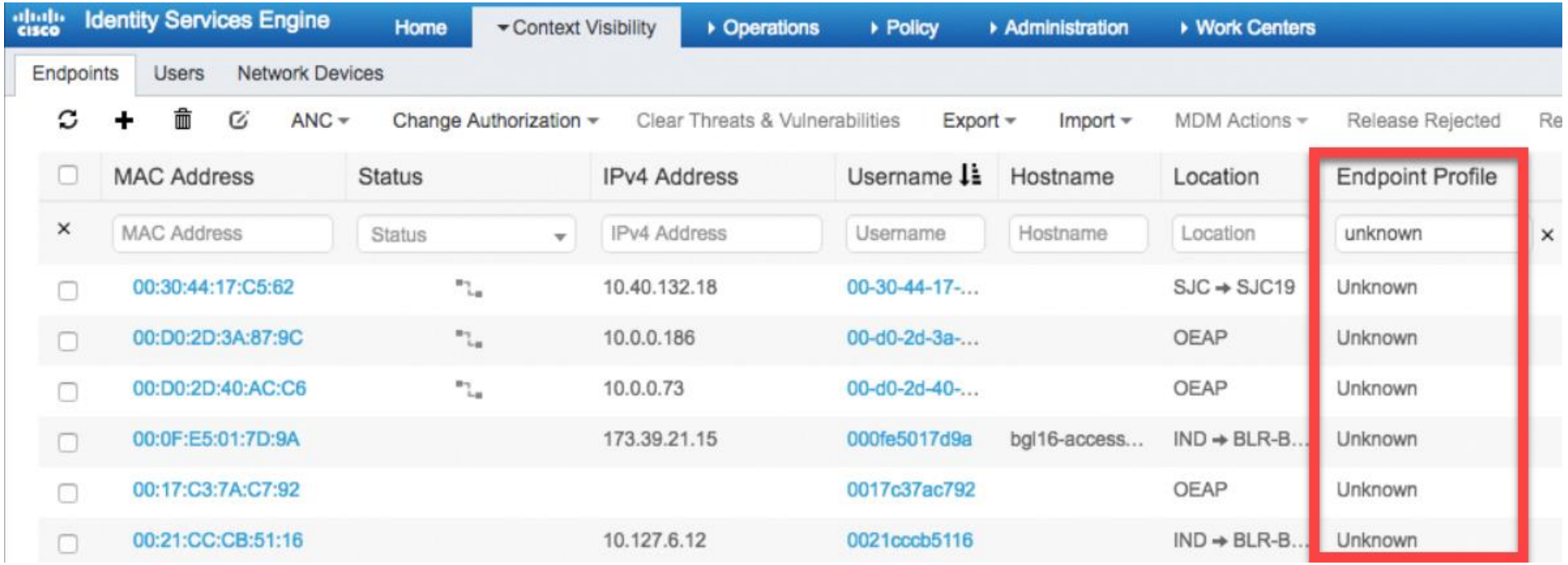
* Name	Microsoft-Workstation
Description	Generic policy for Microsoft workstat
Policy Enabled	☑
* Minimum Certainty Factor	10 (Valid Range 1 to 65535)
* Exception Action	NONE
* Network Scan (NMAP) Action	NONE
Create an Identity Group for the policy	○ Yes, create matching Identity Group
	◉ No, use existing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

Rules

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

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**



Custom Profiles

- Gather more information
  - Create more traffic from the device
  - Run a manual NMAP scan
  - Enable more probes
- Find attributes or combinations of attributes unique to device type
- Focus on:
  - Attributes found every time the endpoint connects
  - Attributes found very early after the endpoint connects

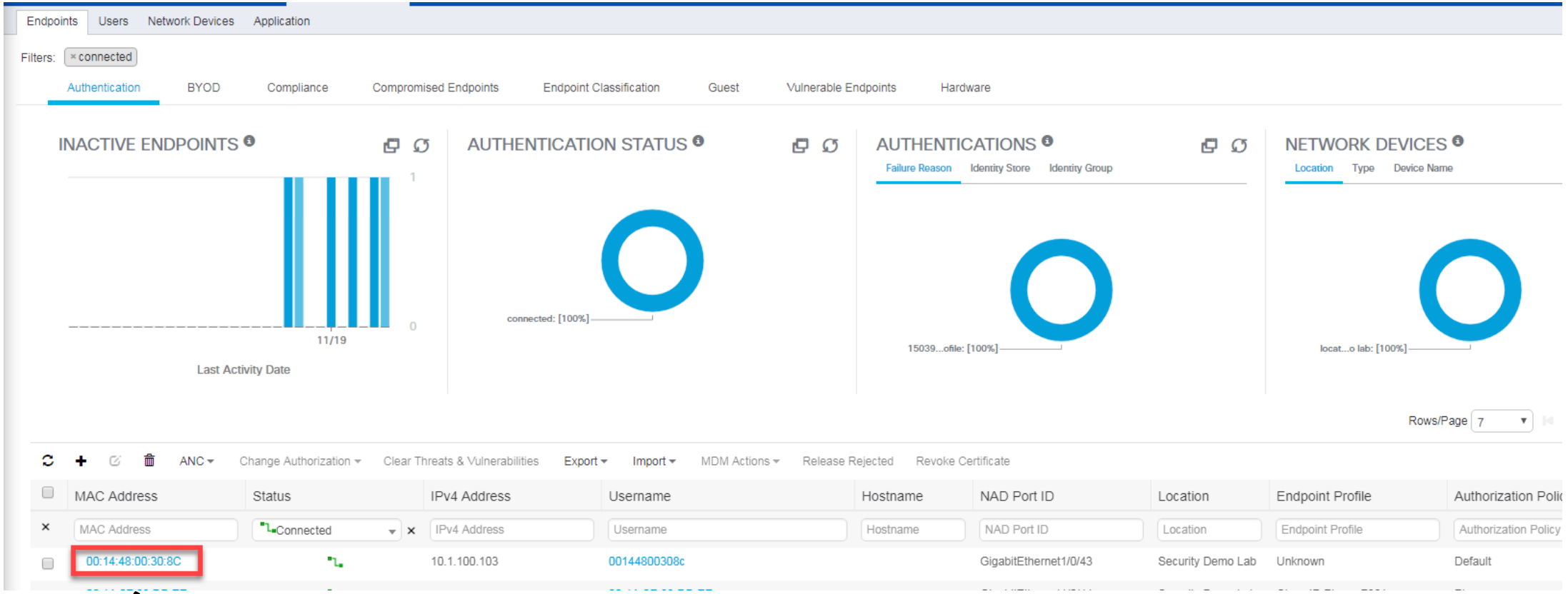
Custom Profiling – Attributes

For your reference only

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

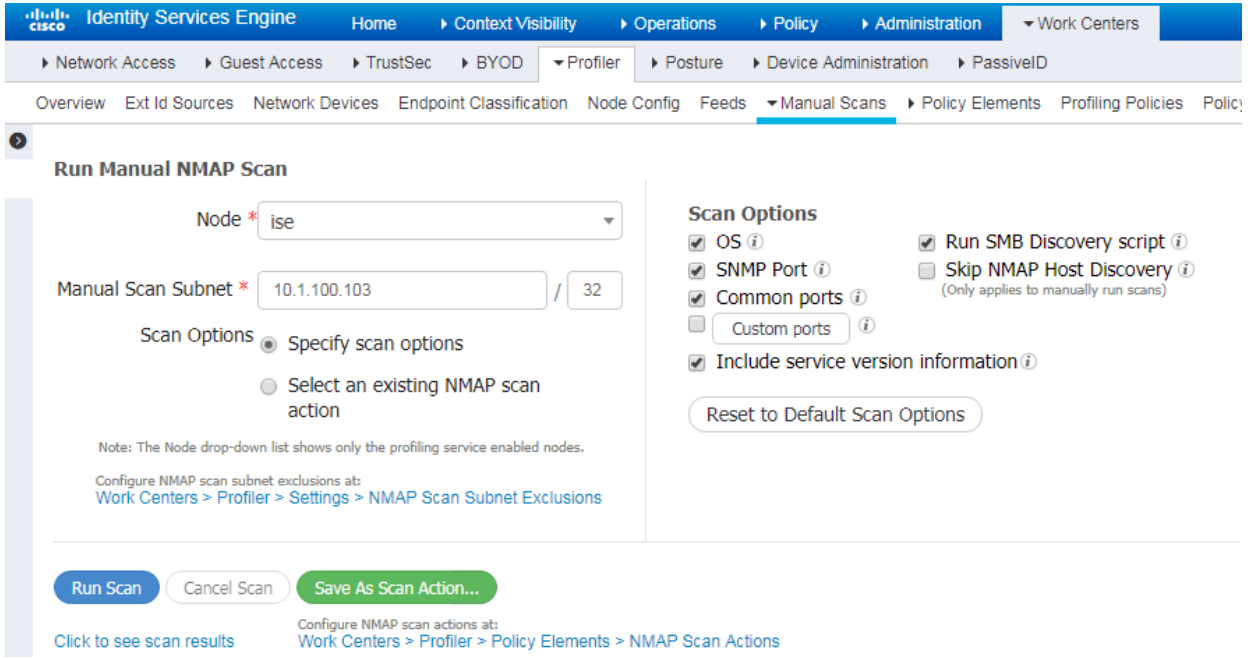
Creating a Custom Profile

- Navigate to **Context Visibility>Endpoints** and click on MAC address of the endpoint.



Creating a Custom Profile (cont'd)

- (Optional) Run a manually NMAP scan against the endpoint by navigating to: **Work Centers>Profiler>Manual Scans**



- Can also save a custom scan for reuse in profiling policy

Creating a Custom Profile (cont'd)

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

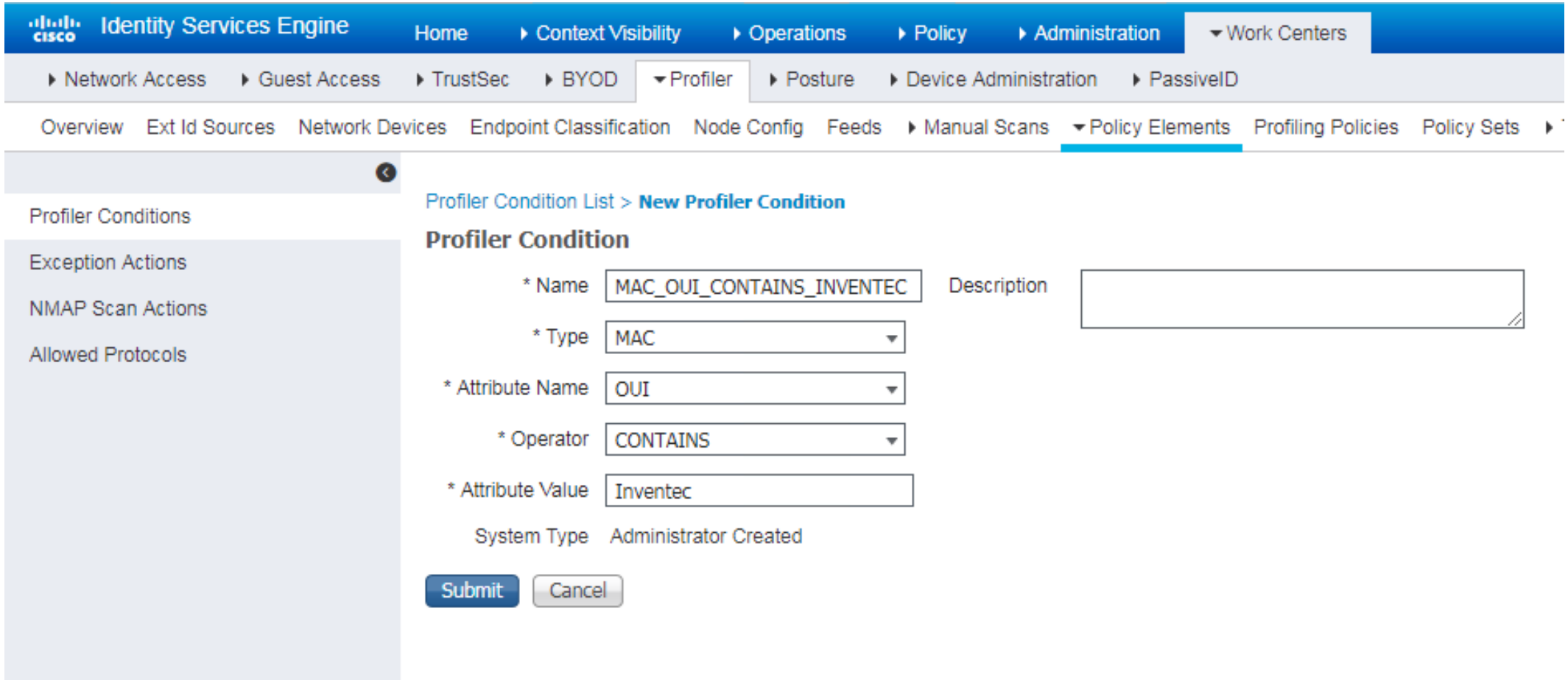
Other Attributes	
5060-tcp	sip
80-tcp	http
AAA-Server	ise
AuthenticationIdentityStore	Internal Endpoints
AuthenticationMethod	Lookup
AuthenticationStatus	AuthenticationPassed
AuthorizationPolicyMatchedRule	Default
BYODRegistration	Unknown
Called-Station-ID	C0-67-AF-EE-09-AB
Calling-Station-ID	00-14-48-00-30-8C
DTLSSupport	Unknown
DestinationIPAddress	10.1.100.21
DestinationPort	1812
Device IP Address	10.1.100.75
Device Type	Device Type#All Device Types#Switches
DeviceRegistrationStatus	NotRegistered
ElapsedDays	0
EndPointMACAddress	00-14-48-00-30-8C
EndPointPolicy	Unknown
EndPointProfilerServer	ise.securitydemo.net
EndPointSource	SNMPQuery Probe
FailureReason	-
Framed-IP-Address	10.1.100.103
IPSEC	IPSEC#Is IPSEC Device#No
IdentityGroup	Unknown
IdentityPolicyMatchedRule	MAB
InactiveDays	0

OUI	Inventec Multimedia & Telecom Corporation
OriginalUserName	00144800308c
PolicyVersion	8
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	WiredMAB
SSID	C0-67-AF-EE-09-AB
SelectedAccessService	PEAP-EAP
SelectedAuthenticationIdentityStores	Internal Endpoints
SelectedAuthorizationProfiles	PermitAccess
Service-Type	Call Check
StaticAssignment	false
StaticGroupAssignment	false
StepData	5= DEVICE.Location, 6= DEVICE.Device Type, 7= DEVICE.Mode, 8= DEVI(Radius.RadiusFlowType, 11=Internal Endpoints, 17= Session.ANCPolicy, 18
Total Certainty Factor	0
TrustSec-Enabled	TrustSec-Enabled#TrustSec-Enabled#Non-TrustSec
UseCase	Host Lookup
User-AD-Last-Fetch-Time	1543131931802
User-Fetch-User-Name	00144800308c
User-Name	00144800308c
UserType	Host
allowEasyWiredSession	false
chaddr	00:14:48:00:30:8c
ciaddr	0.0.0.0

dhcp-class-identifier	udhcp 0.9.7
dhcp-client-identifier	01:00:14:48:00:30:8c
dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 3, 6, 12, 15, 28
dhcp-requested-address	10.1.100.103
dot1xAuthAuthControlledPortControl	2
dot1xAuthAuthControlledPortStatus	2
dot1xAuthSessionUserName	00-14-48-00-30-8C
flags	0x0000
giaddr	10.1.100.75
hlen	6
htype	Ethernet (10Mb)
ifDescr	GigabitEthernet1/0/43
ifIndex	50
ifOperStatus	1
ip	10.1.100.103
op	BOOTREQUEST
operating-system	Linux 2.4.9 - 2.4.18 (likely embedded)
operating-system-result	Linux 2.4.9 - 2.4.18 (likely embedded)
yiaddr	0.0.0.0

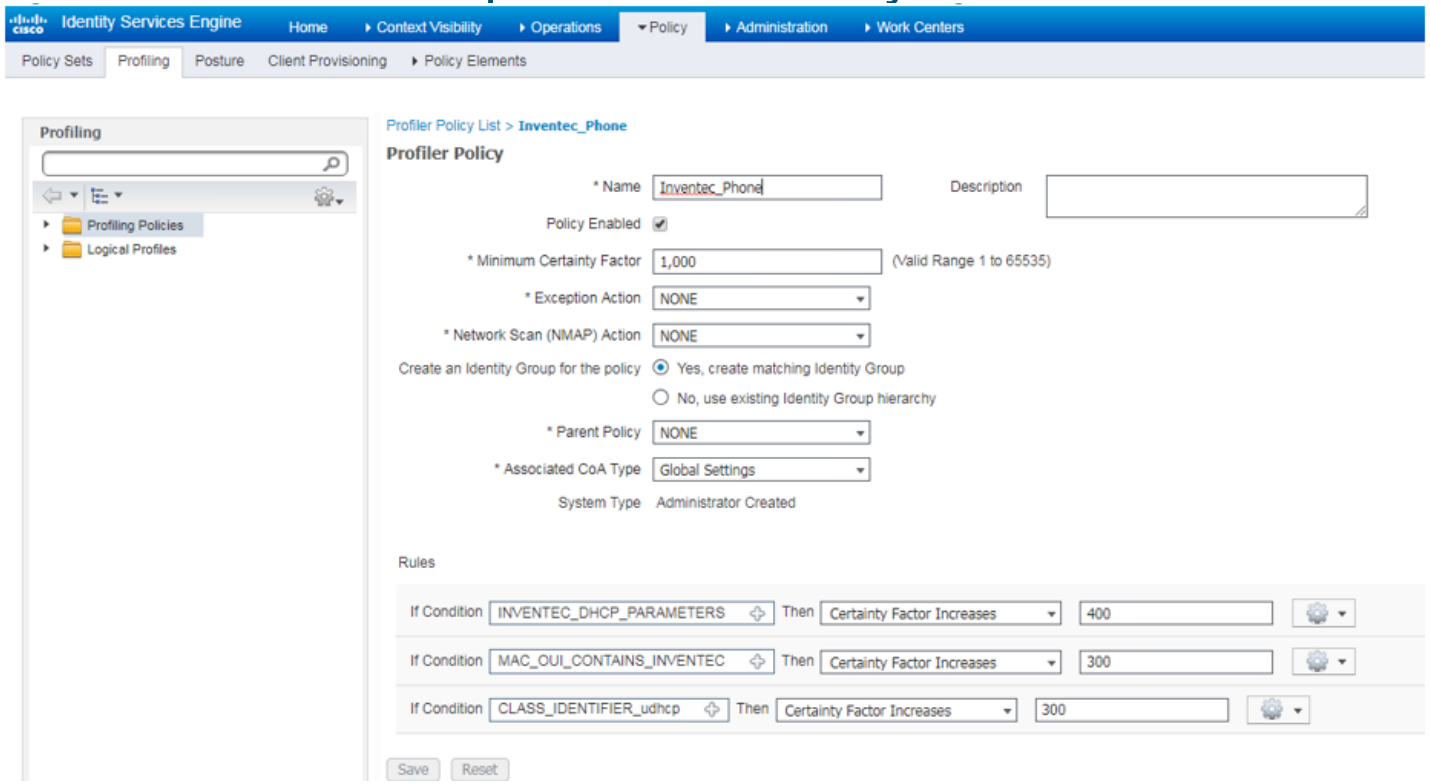
Creating a Custom Profile (cont'd)

Navigate to **Work Centers>Profiler>Policy Elements** and click **Add** to add the attributes from the endpoint to the profiler conditions



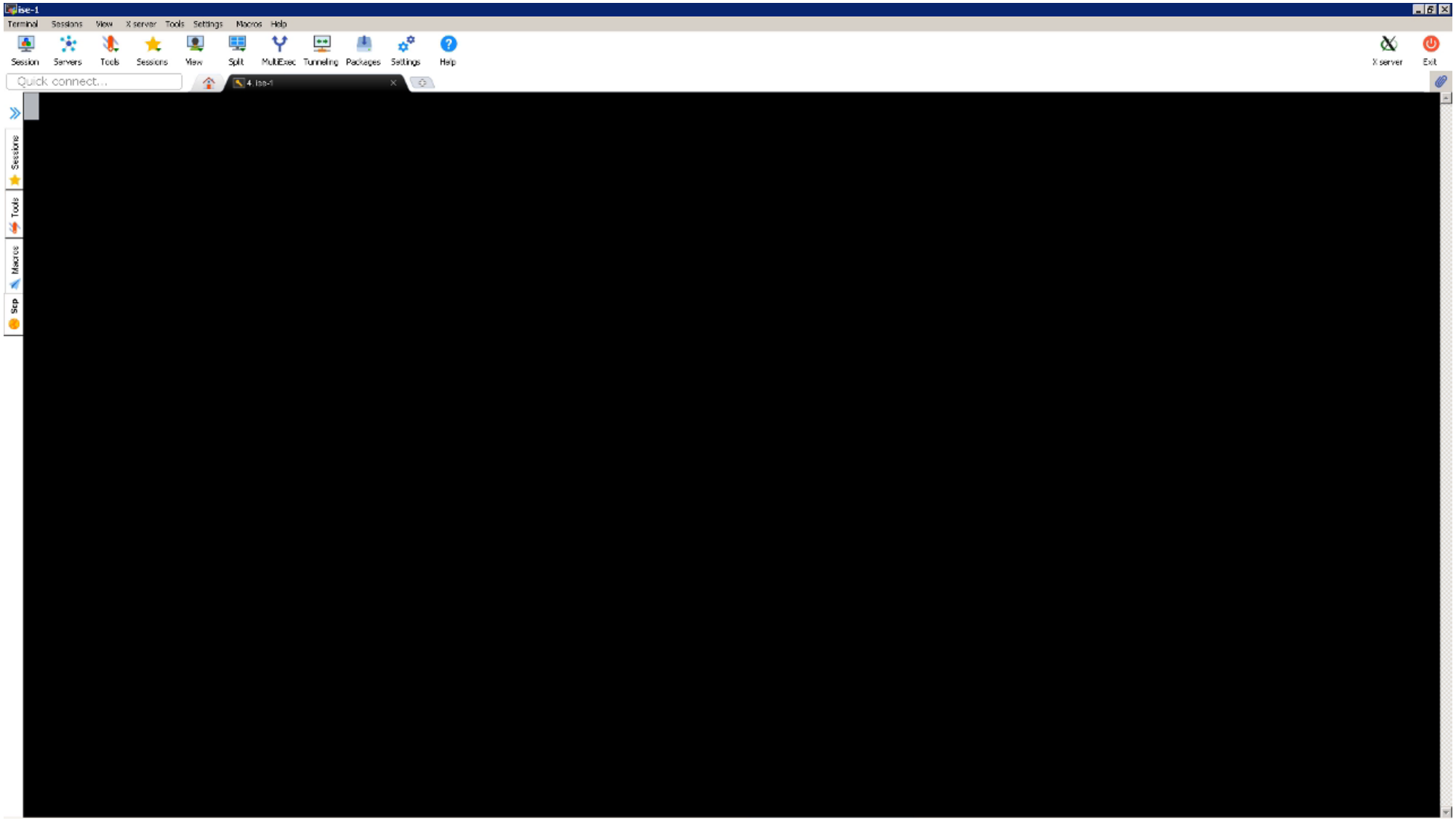
Creating a Custom Profile (cont'd)

Navigate to **Policy>Profiling>Profiling Policy** and click **Add** to create a new profile policy based on the unique attributes you found

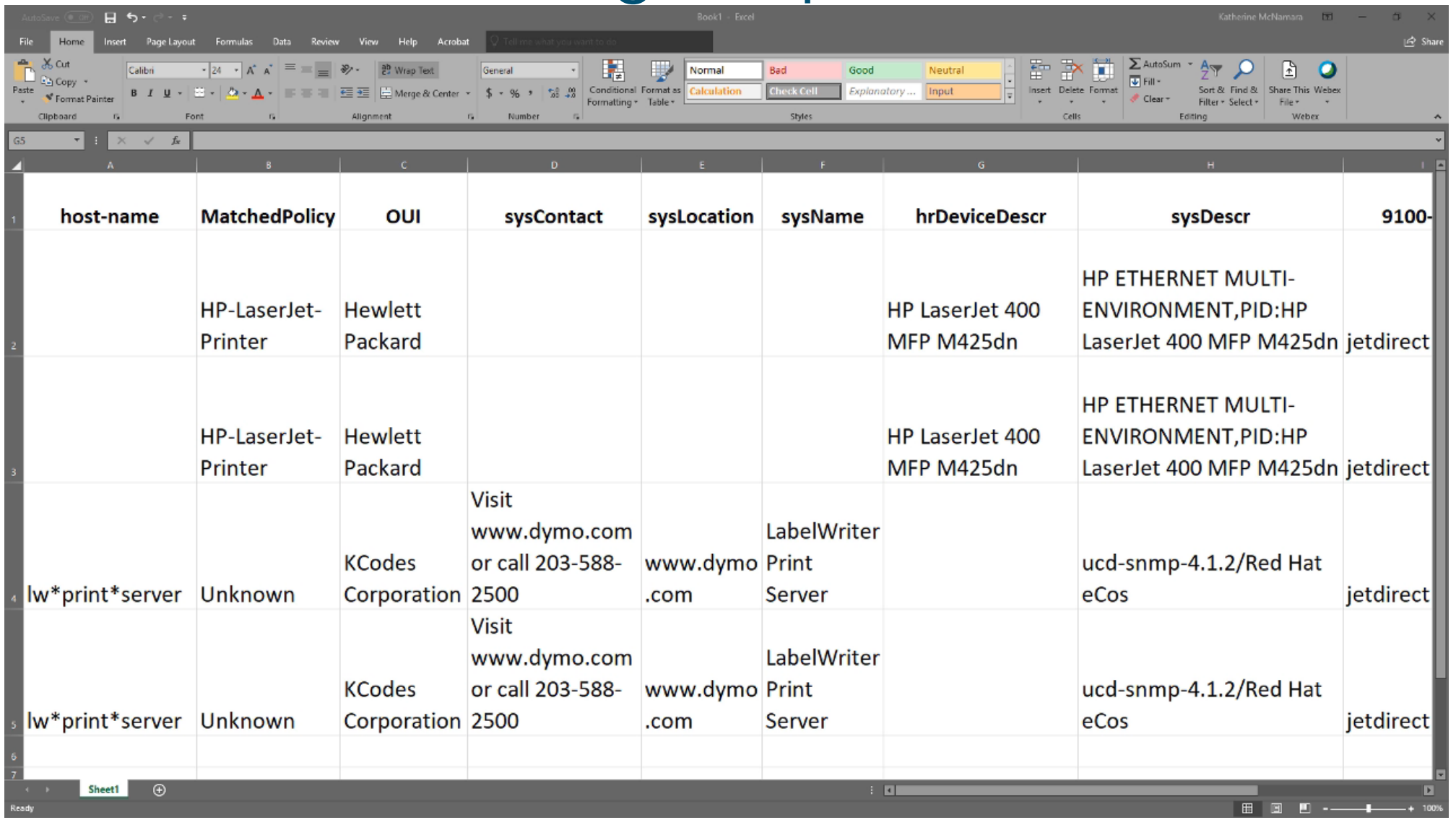


Best practice to start with Minimum Certainty Factor value of at least 1,000 for custom profiler policies

Custom Profiles: Get All Endpoints



Custom Profiles: Using Endpoint Attributes



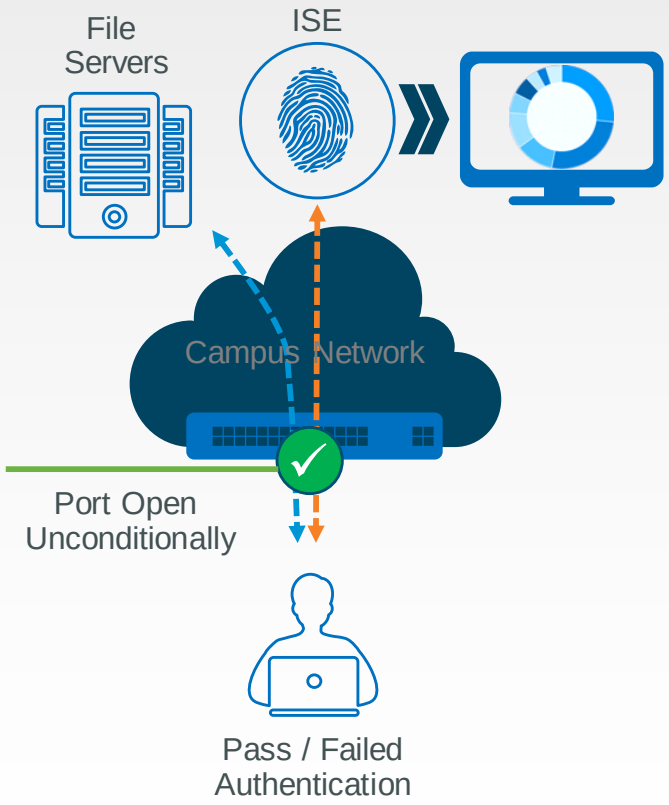
host-name	MatchedPolicy	OUI	sysContact	sysLocation	sysName	hrDeviceDescr	sysDescr	9100-
	HP-LaserJet-Printer	Hewlett Packard				HP LaserJet 400 MFP M425dn	HP ETHERNET MULTI-ENVIRONMENT,PID:HP LaserJet 400 MFP M425dn	jetdirect
	HP-LaserJet-Printer	Hewlett Packard				HP LaserJet 400 MFP M425dn	HP ETHERNET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

Agenda

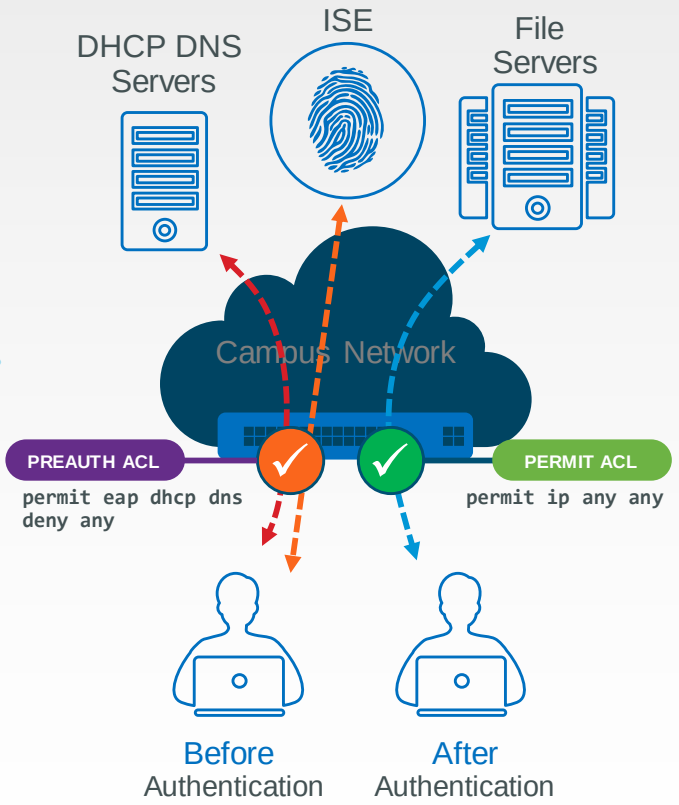
- Where To Start
- ISE Appliances & Deployment Options
- Network Devices
- Identity Sources
- Supplicants
- Profiling
- 802.1x Deployment Phases
- Enforcement
- Day 2 Operations

Deploying 802.1x in Phases

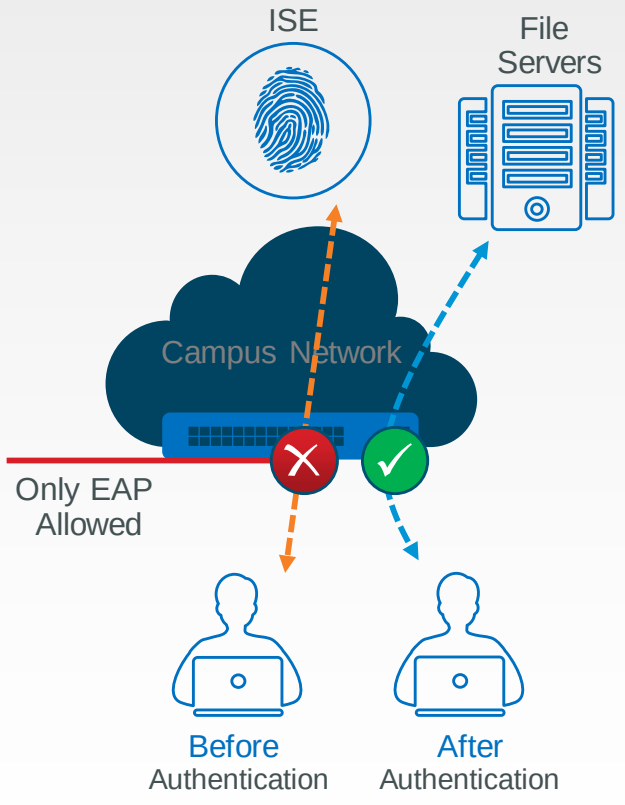
Monitor Mode



Low-Impact Mode



Closed Mode



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
  - No Authorization

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

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

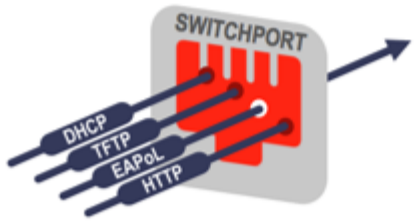
```
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
switchport voice vlan 10
authentication host-mode multi-auth
ip access-group PRE-AUTH in
authentication open
authentication port-control auto
mab
dot1x pae authenticator
authentication violation restrict
```

Low-Impact Mode

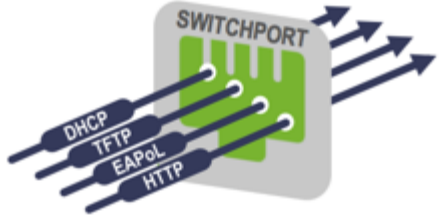
From Monitor Mode

Closed Mode

- Not everyone goes to Closed Mode
- No access at all before authentication
- Rapid access for non-802.1x-capable corporate assets
- Logical isolation of traffic at the access layer
- Return to default “closed” access
- Implement identity-based access assignment



Before Authentication

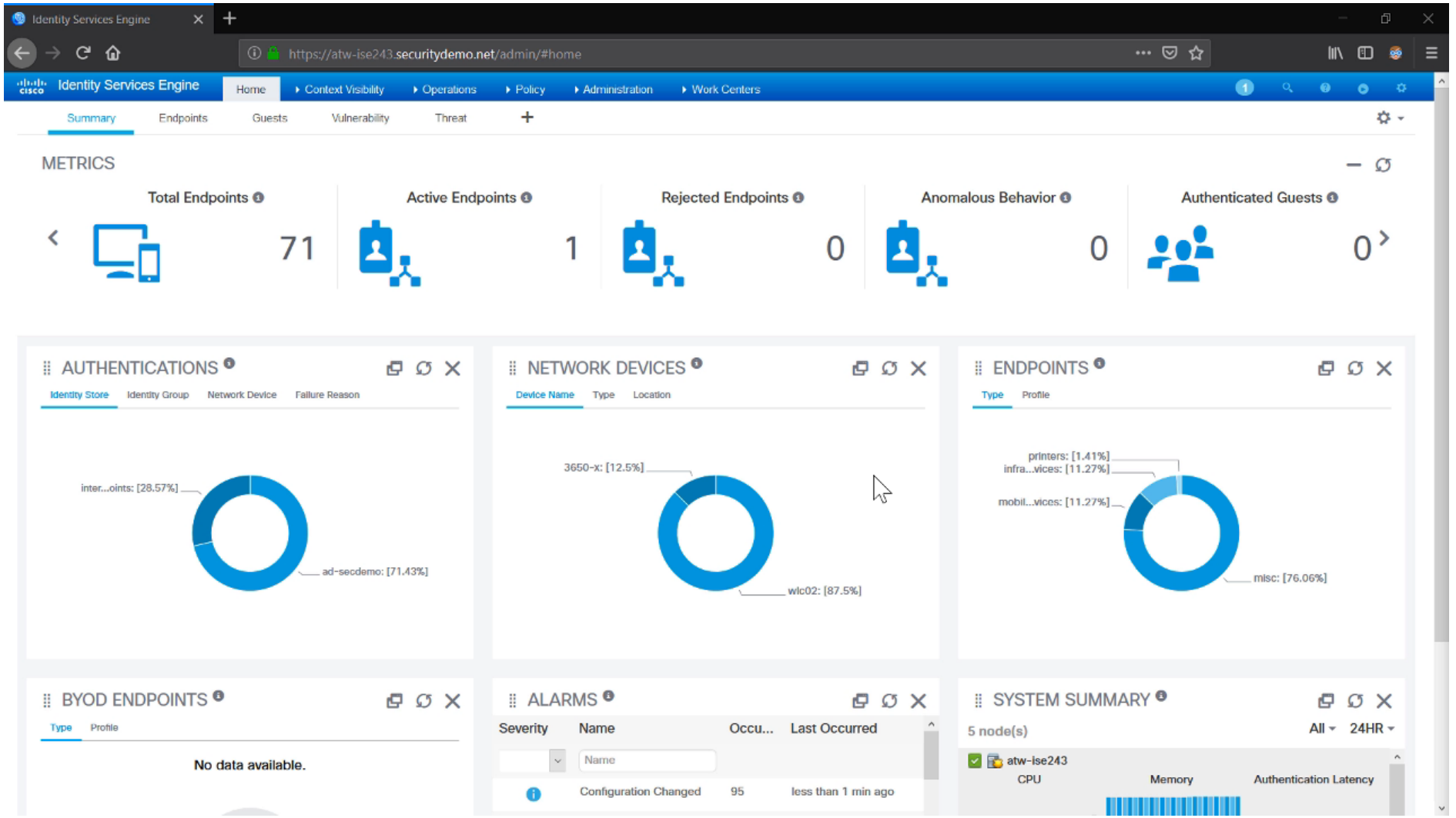


After Authentication

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
```

Utilizing Policy Sets with Modes



Agenda

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

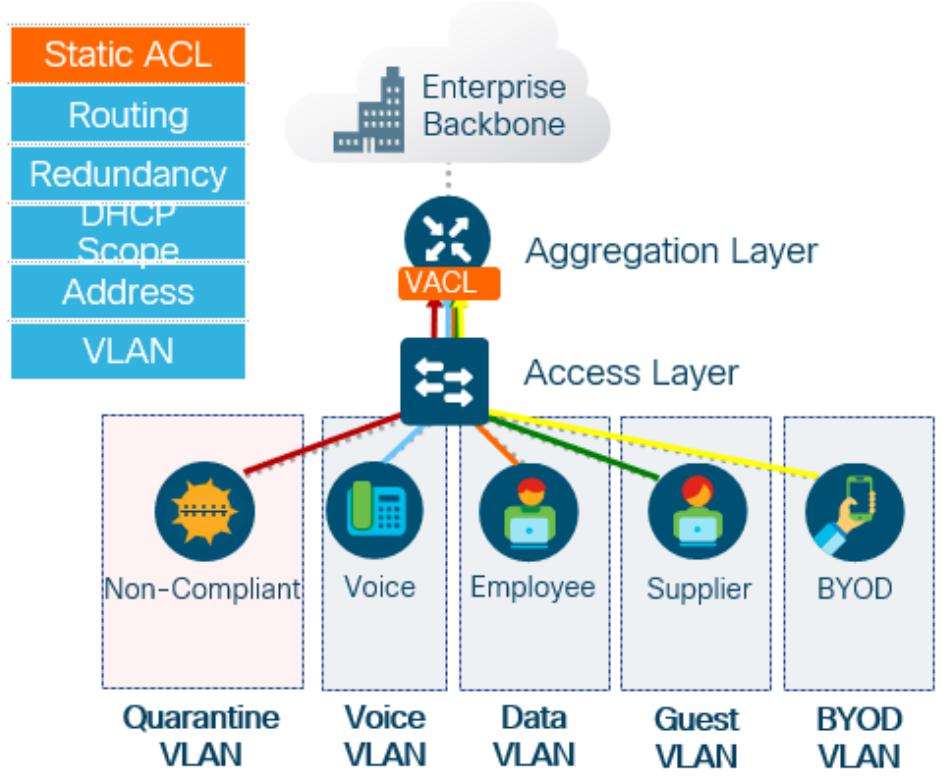
Network access control does not automatically mean you have segmentation

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

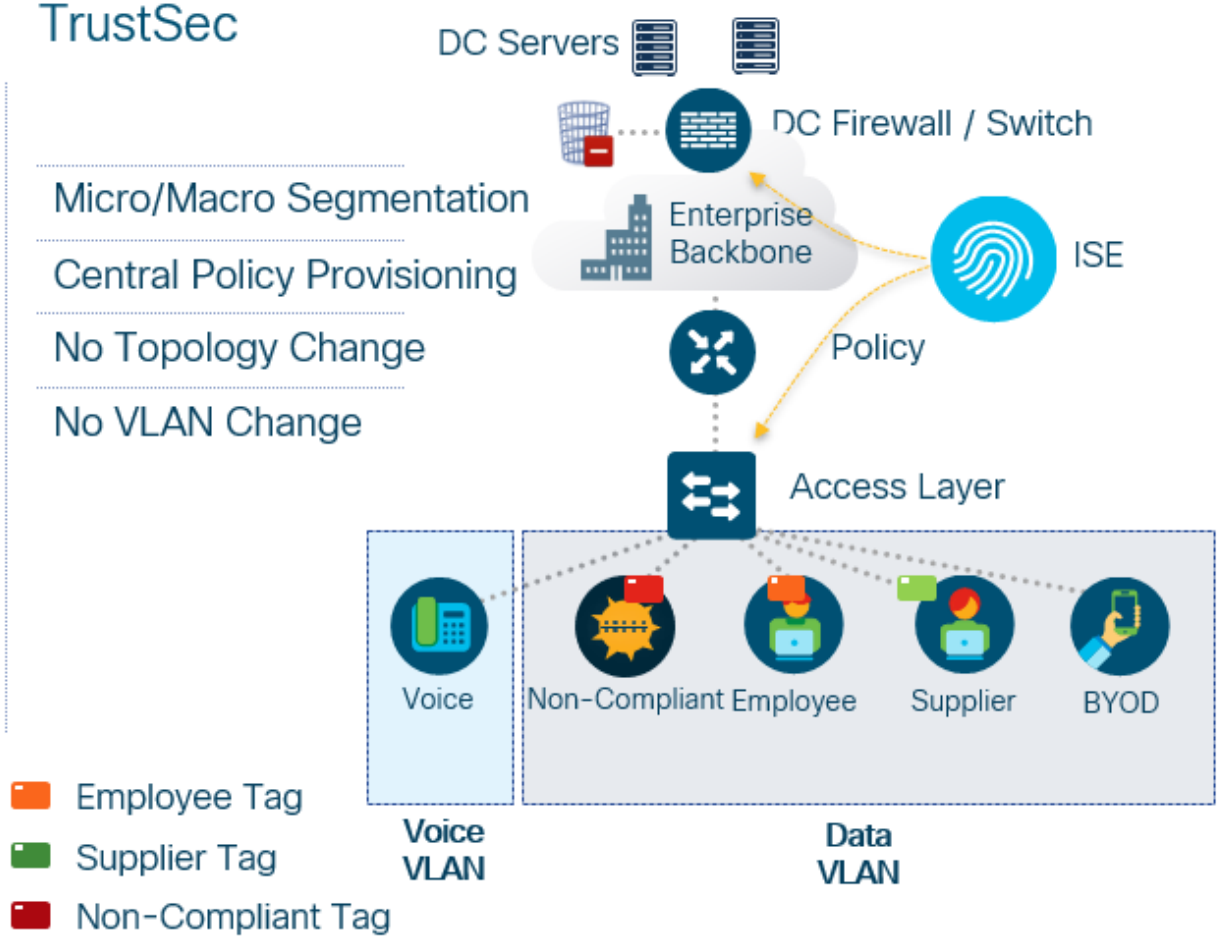
TrustSec for Segmentation

Traditional Segmentation



Security Policy based on Topology
High cost and complex maintenance

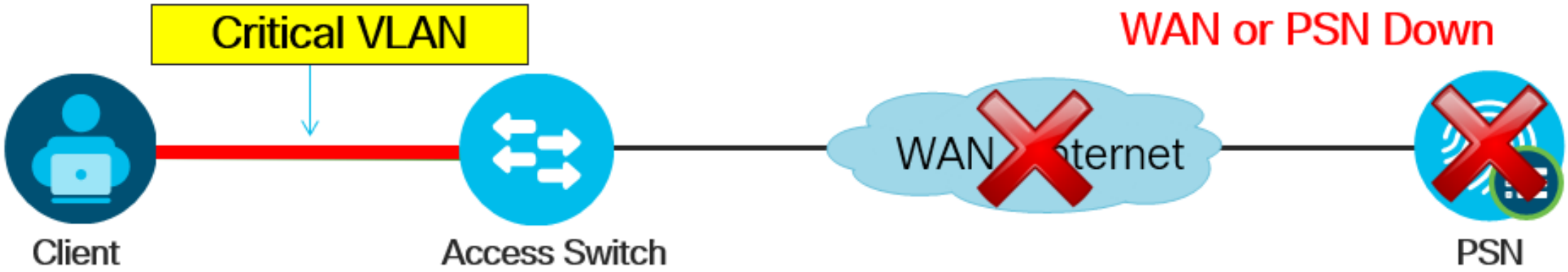
TrustSec



Use existing topology and automate
security policy to reduce OpEx

What about limiting or allowing access if ISE becomes unavailable?

Inaccessible Authentication Bypass



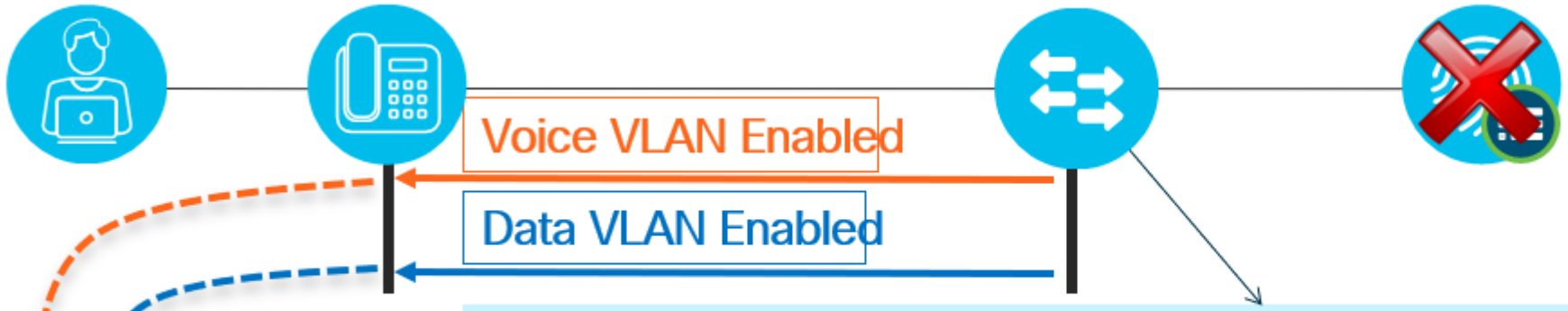
- Switch detects PSN unavailable
- Enables port in critical VLAN
- Existing sessions retain authorization status
- Recovery action can re-initialize port when AAA returns

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

Critical Auth for Data and Voice



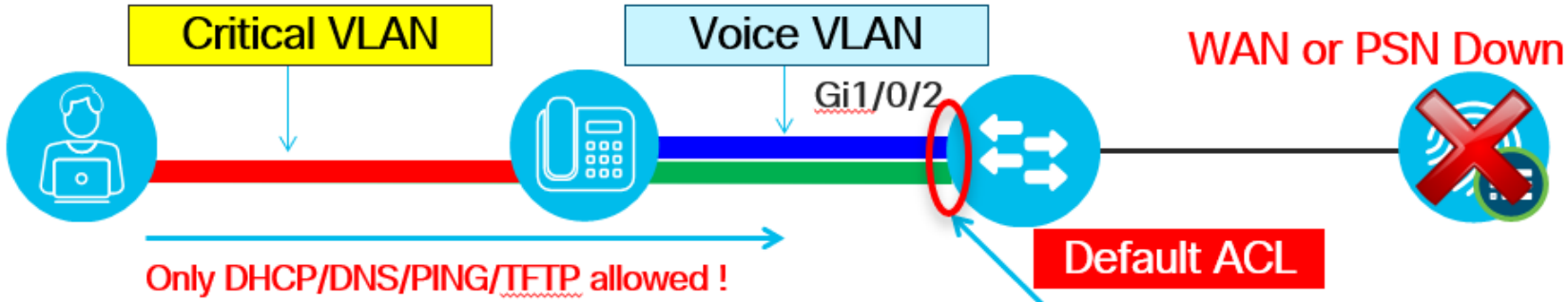

```
interface GigabitEthernet 3/48
 dot1x pae authenticator
 authentication port-control auto
 authentication event server dead action authorize vlan x
 authentication event server dead action authorize voice
```

```
# show authentication sessions interface fa3/48
...
Critical Authorization is in effect for domain(s) DATA and VOICE
```

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
```

Agenda

- Where To Start
- ISE Appliances & Deployment Options
- Network Devices
- Identity Sources
- Supplicants
- Profiling
- 802.1x Deployment Phases
- Enforcement
- 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

You make security **possible**

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

Planning is essential to any successful development.

Helpful Links and Training

- Cisco ISE for BYOD and Secure Unified Access (2nd Edition) – https://tinyurl.com/ise-byod-book
- Cisco Security SISAS – https://tinyurl.com/ise-sisas-book
- Cisco ISE Communities – http://tinyurl.com/ise-communities
- Medical NAC 2.0 Profiles – https://tinyurl.com/ise-medical-nac-2
- ISE Automation and Control Profiles – https://tinyurl.com/ise-automation-library
- ISE Scalability Numbers – https://tinyurl.com/ise-scale

Helpful Links and Training

- ISE NAD Compatability Matrix - https://tinyurl.com/ise-compatibility
- ISE Bandwidth Calculator - http://tinyurl.com/ise-bw-calc
- ISE Switch Configuration Guide - https://tinyurl.com/ise-switch-guide
- ISE WLC Configuration - https://tinyurl.com/ise-wlc-config
- ISE Loadbalancing Guides - https://tinyurl.com/ise-loadbalancing

Helpful Blogs

- Labminutes Videos - http://labminutes.com/video/sec/ISE
- Aaron Woland's Blog Posts
  - https://woland.com
  - https://www.networkworld.com/author/Aaron-Woland/
- Brad Johnson's ISE Support Blog - https://www.ise-support.com/
- My blog - https://www.network-node.com/
- Densemode.com's series on PKI for Network Engineers
  - PKI for Network Engineers Theory: https://tinyurl.com/pki-ne-1
  - Diffie Hellman for people who suck at math: https://tinyurl.com/df-no-math

Complete your online session evaluation

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live water bottle.
- All surveys can be taken in the Cisco Live Mobile App or by logging in to the Session Catalog on ciscolive.cisco.com/us.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.cisco.com.

Continue your education

Demos in the Cisco campus

Walk-in labs

Meet the engineer 1:1 meetings

Related sessions

Action Steps

- What should you do today?
  - Visit the next ISE session or meet the engineer for ISE

- What should you do next week?
  - Build a lab to get your hands on with ISE


Thank you
Ciscolive!
#CLUS

You make **possible**