Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

Advanced ISE and Secure Access Deployment

BRKSEC-3040

Abstract

2011 and 2012 have been very busy years with the adoption of Cisco[1]s Identity Services Engine, with a comprehensive systems-approach to Network Access Control and Policy enforcement. This session will discuss the recommended deployment of Identity Services Engine (ISE) based on best-practices and lessons learned in the Field. At the end of this session, the attendee should have a strong understanding of how to deploy ISE with 802.1X for wired and wireless networks.

We will examine the correct use of profiling probes to meet the needs of the policy, tips and tricks for successful staged roll-outs, Guest Services, Load Balanced Deployment and High-Availability (HA), Distributed Deployment Guidelines, and Bring Your Own Device (BYOD) policy logic.

Note: this session will not cover all possible options for deployment, only best-practices, tips and tricks with the current state of the solution (ISE 1.2). This is an advanced session that assumes prior knowledge of 802.1X and ISE design basics. This session is intended for a technical audience of Network or Security Administrators and Engineers.

Your Speaker

Aaron Woland
CCIE# 20113

Sr. Secure Access TME
Customer Success Team
Secure Access & Mobility Group

loxx@cisco.com

Why this Cisco Live Session?

A Complex Solution

Network Access Devices

ISE Configuration

Switch Config

WLC Config

Profiling Policies

AuthC Policies

AuthZ Policies

Posture Policies

Policies for your Policies

This Presentation Contains a Culmination of Best Practices and Tips from a Wide Range of Cisco Technologists, not just me ☺

Special Thanks to: Jason Frazier, Shelly Cadora, Jason Kunst, Craig Hyps, Darrin Miller and the entire Secure Access & Mobility TME Team




Agenda

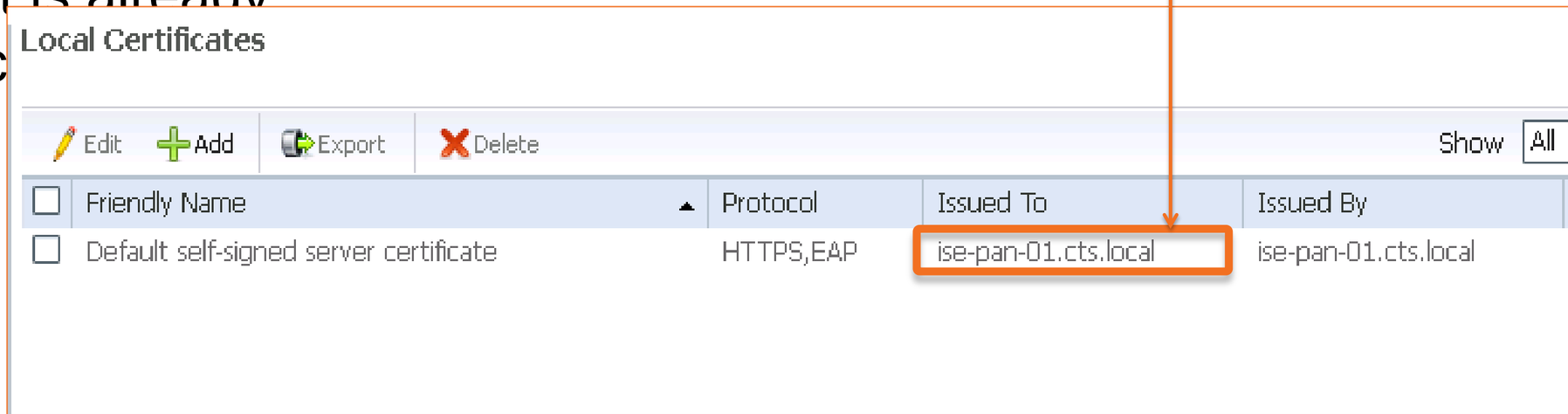
- Best Practice ISE Configurations
- Profiling
- Deployment Considerations and HA
- BYOD
- Policy Tips
- Troubleshooting

ISE Best Practice Tips

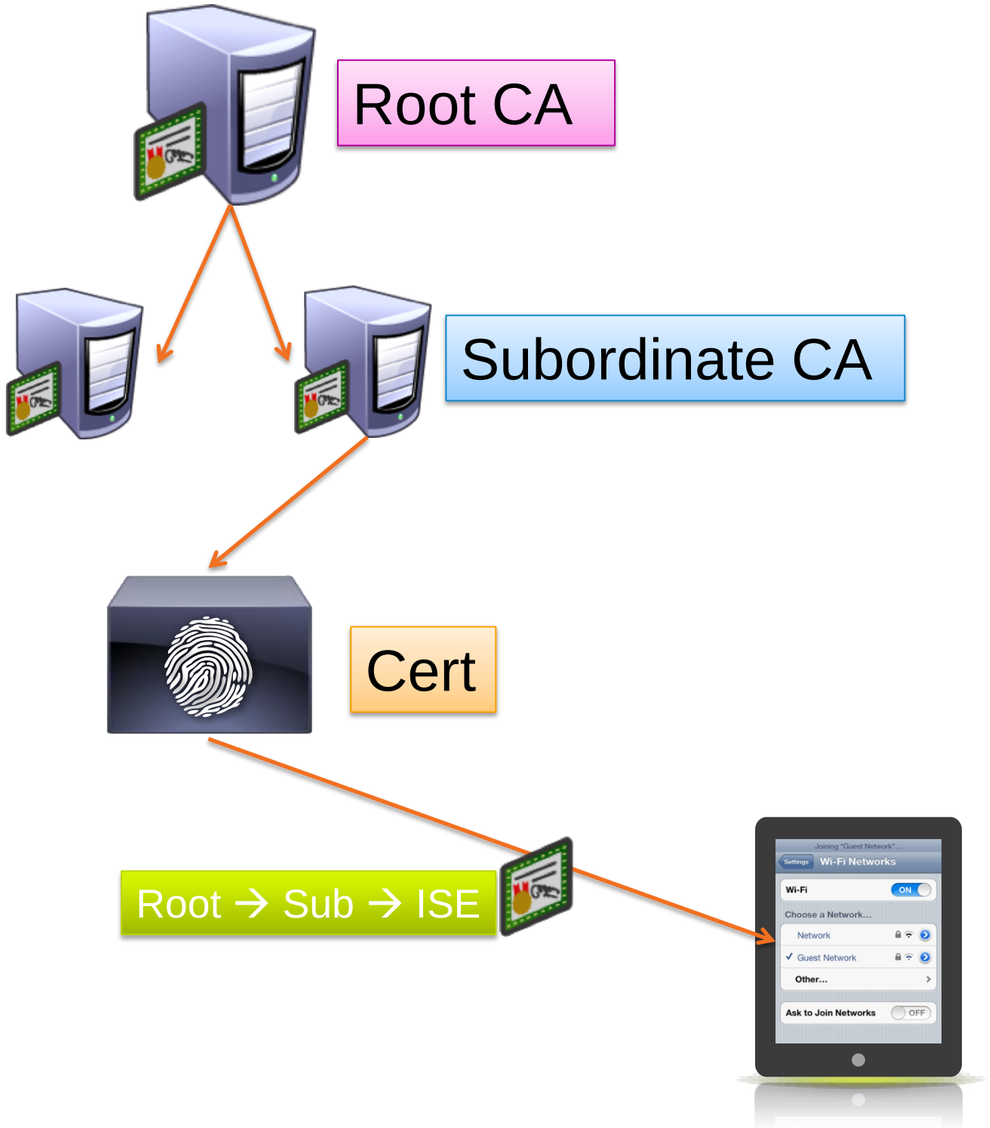
ISE & Certificates

- When running the ISE Install wizard, use lower-case for hostname.
  - Do no use self-signed certificates in production networks
- Certificate is used for all Portal Communication and EAP
  - Using a certificate that is already trusted by all normal c… big benefit.

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: ise-pan-01
Enter IP address[]: 10.1.100.5
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.1.100.1
Enter default DNS domain[]: cts.local
Enter primary nameserver[]: 10.1.100.100
Add secondary nameserver? Y/N [N]: n
Enter NTP server[time.nist.gov]: time.cts.local
Add another NTP server? Y/N [N]: n
Enter system timezone[UTC]:
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface...
_
```



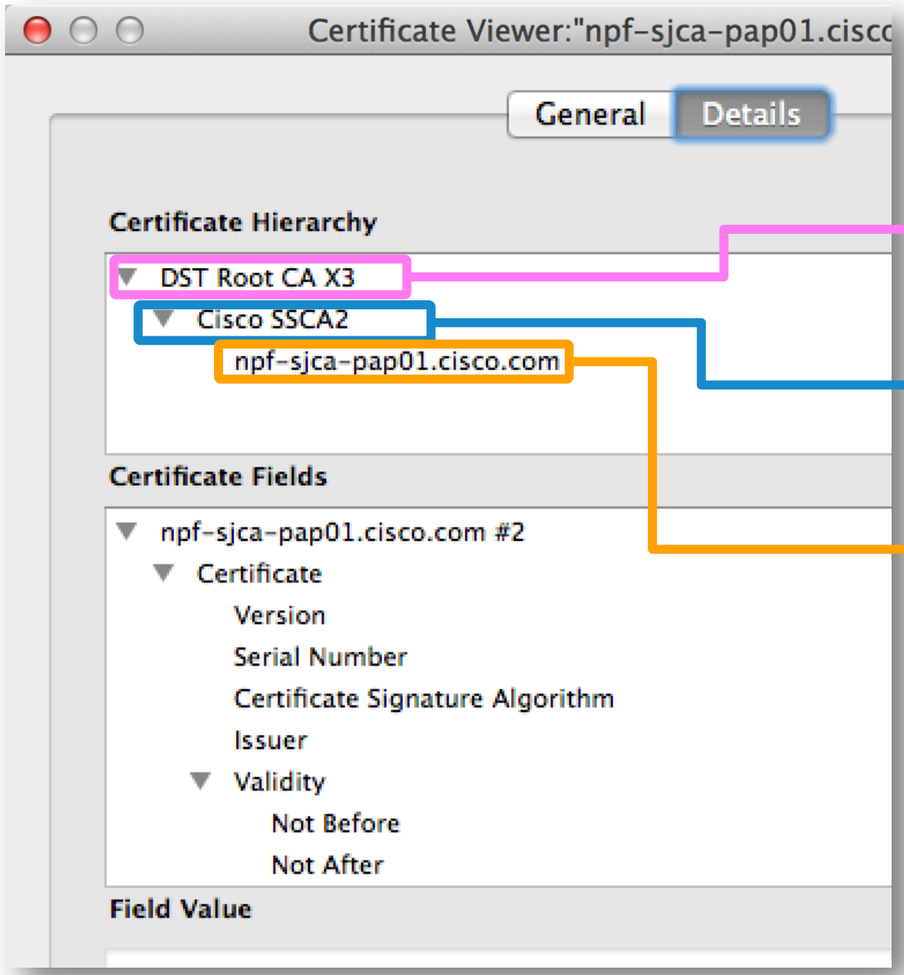
Certificate Chains



- For Scalability, X.509 Certificate Authorities may have hierarchy
- ISE will present full signing chain to client during authentication
  - Client must trust each CA within the chain

Always Add the Root and Subordinate CA

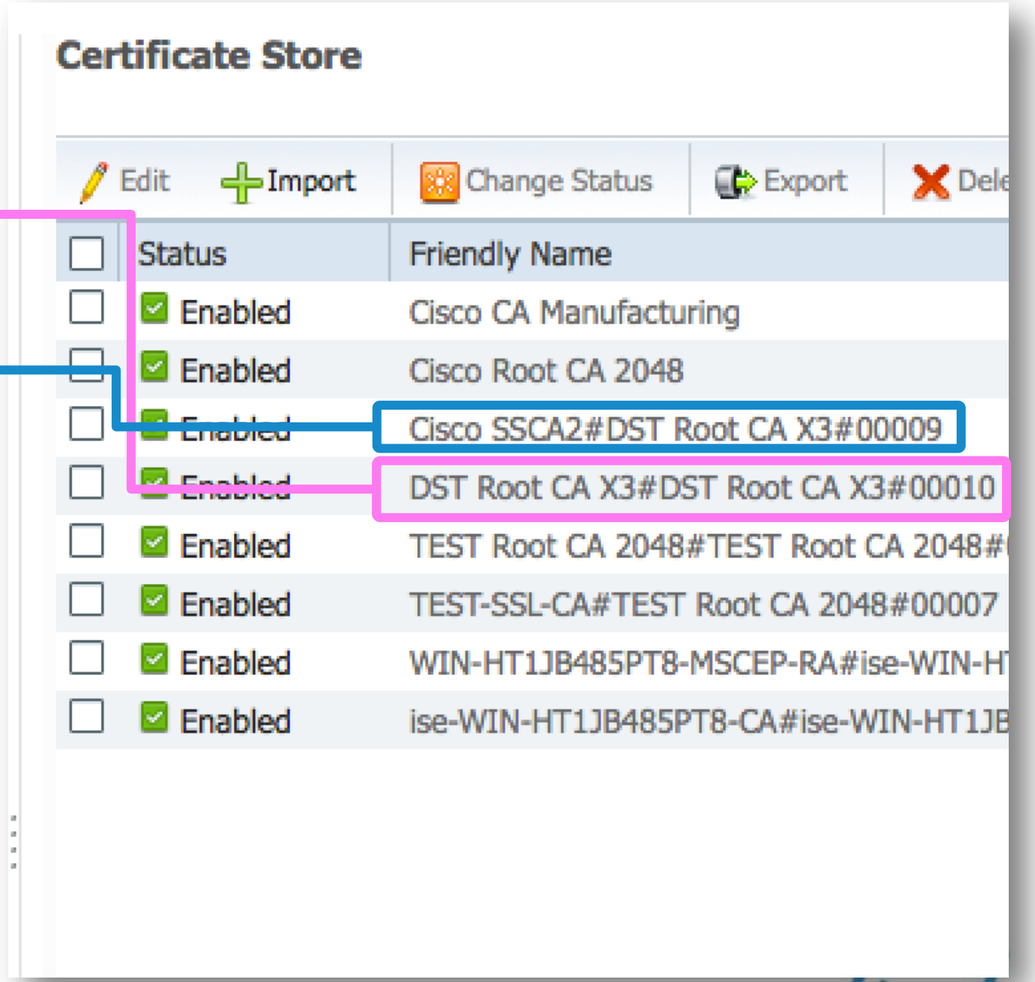
Import Entire Certificate Chain, Individually (no PKCS chains)



Root CA

Subordinate CA

ISE Cert



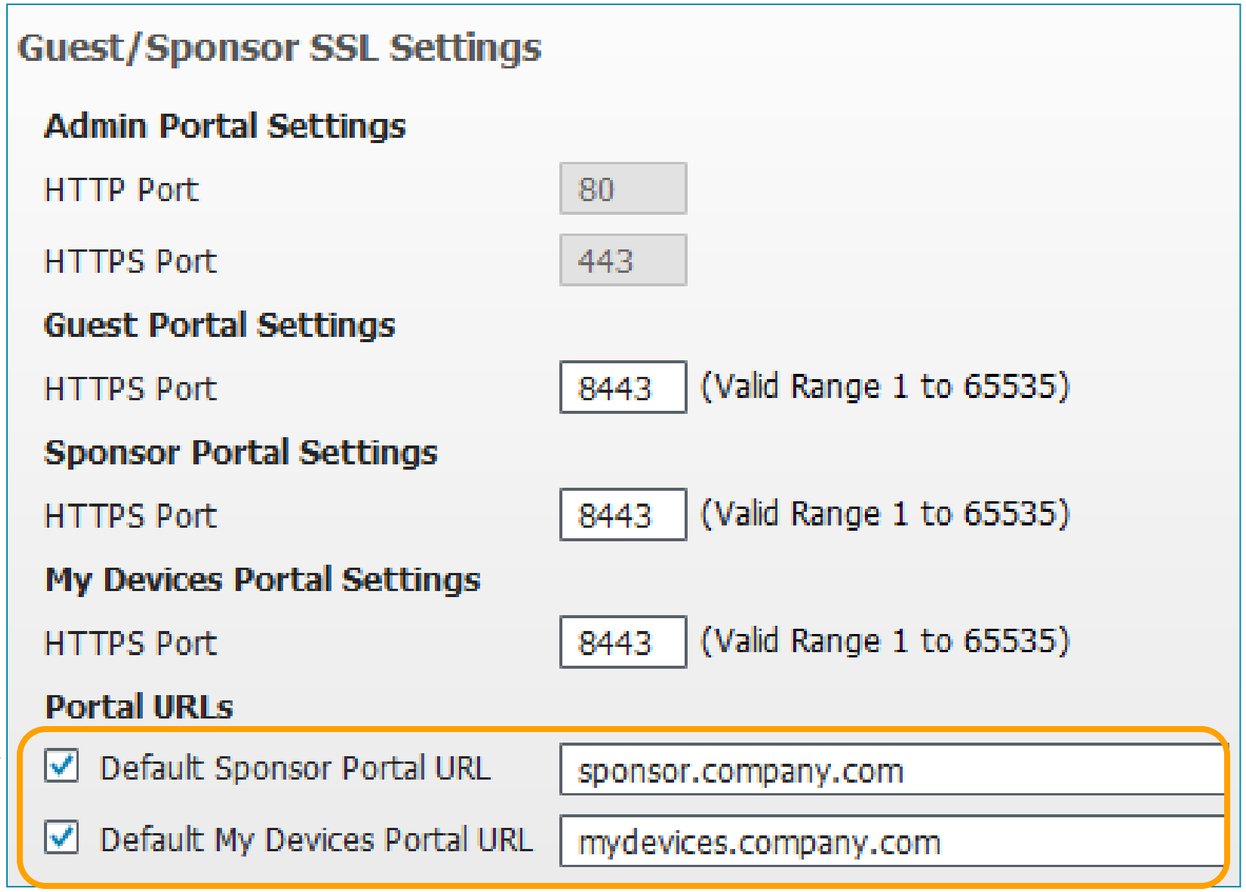
If you must use a PKCS chain, it needs to be in PEM format (not DER)

Certificate “hack” for Friendly URLs

Simple URL for Sponsor / My Devices Portal

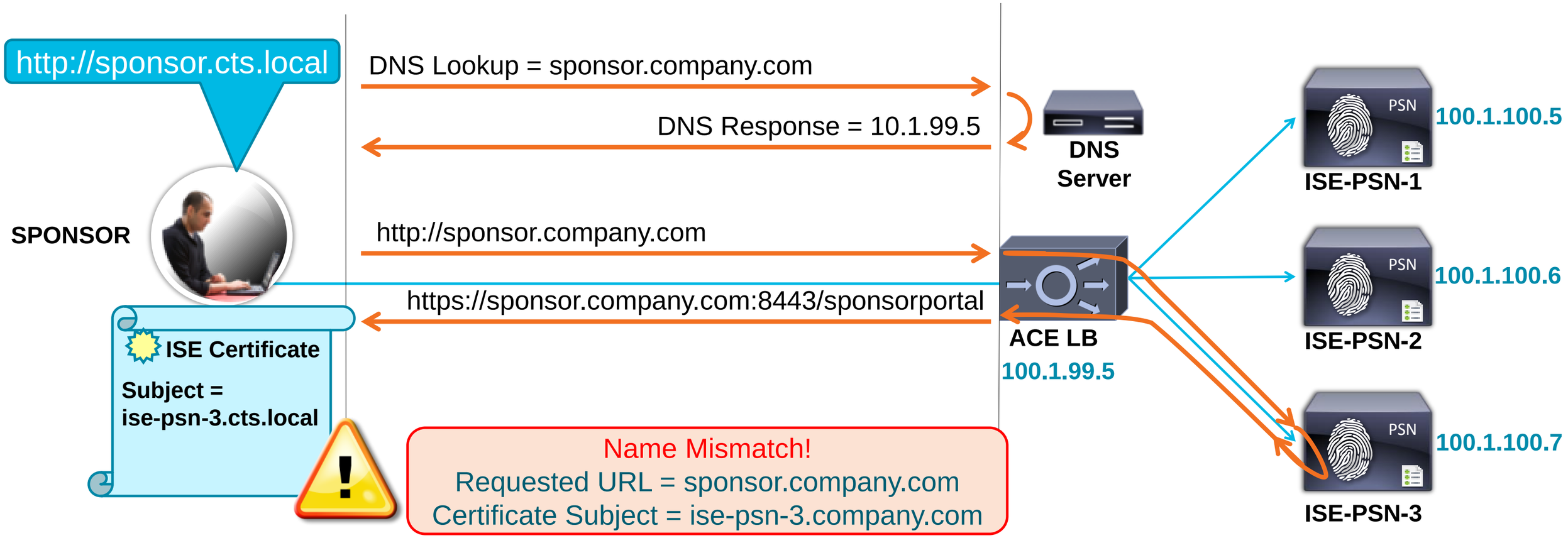
- Sponsor Portal and My Devices Portal can be accessed via a user-friendly URL and selectable port.
- Ex: http://sponsor.company.com

  Automatic redirect to https://fqdn:port
- FQDN for URL must be added to DNS and resolve to the Policy Service node(s) used for Guest Services.
- Recommend populating Subject Alternative Name (SAN) field of PSN local cert with this alternative FQDN to avoid SSL cert warnings due to name mismatch.



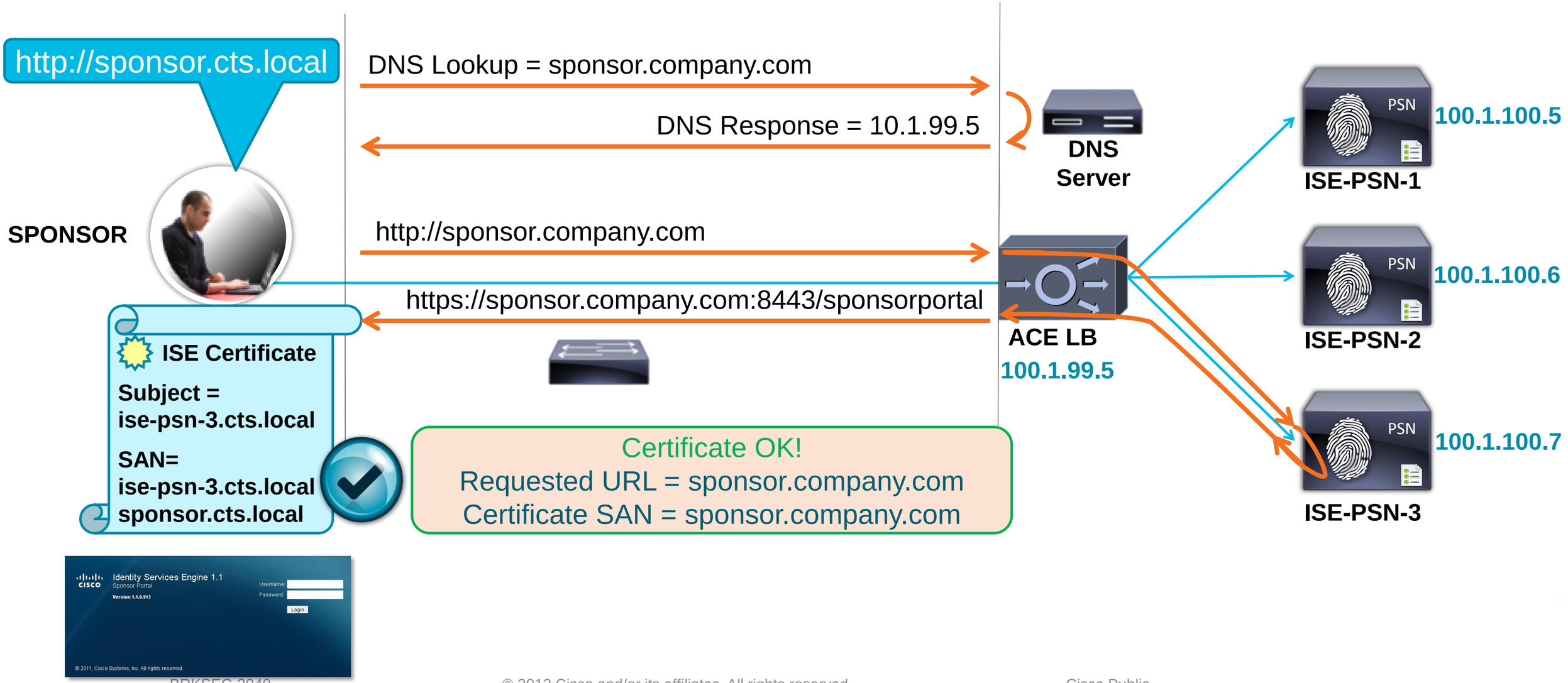
ISE Certificate without SAN

Certificate Warning - Name Mismatch



ISE Certificate with SAN

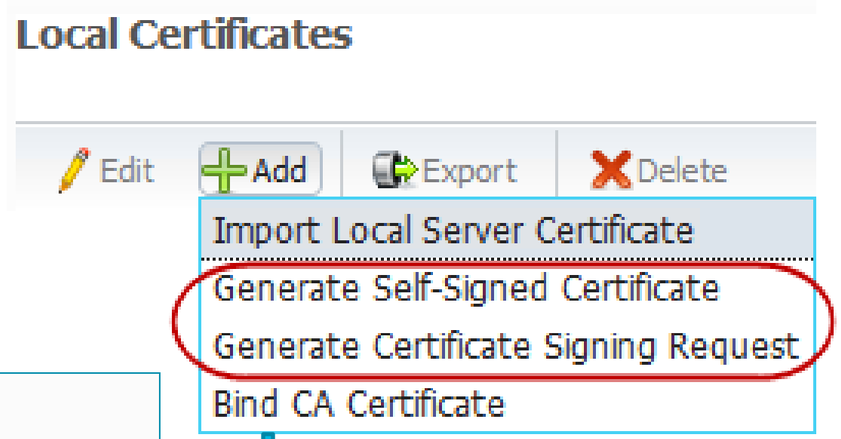
No Certificate Warning

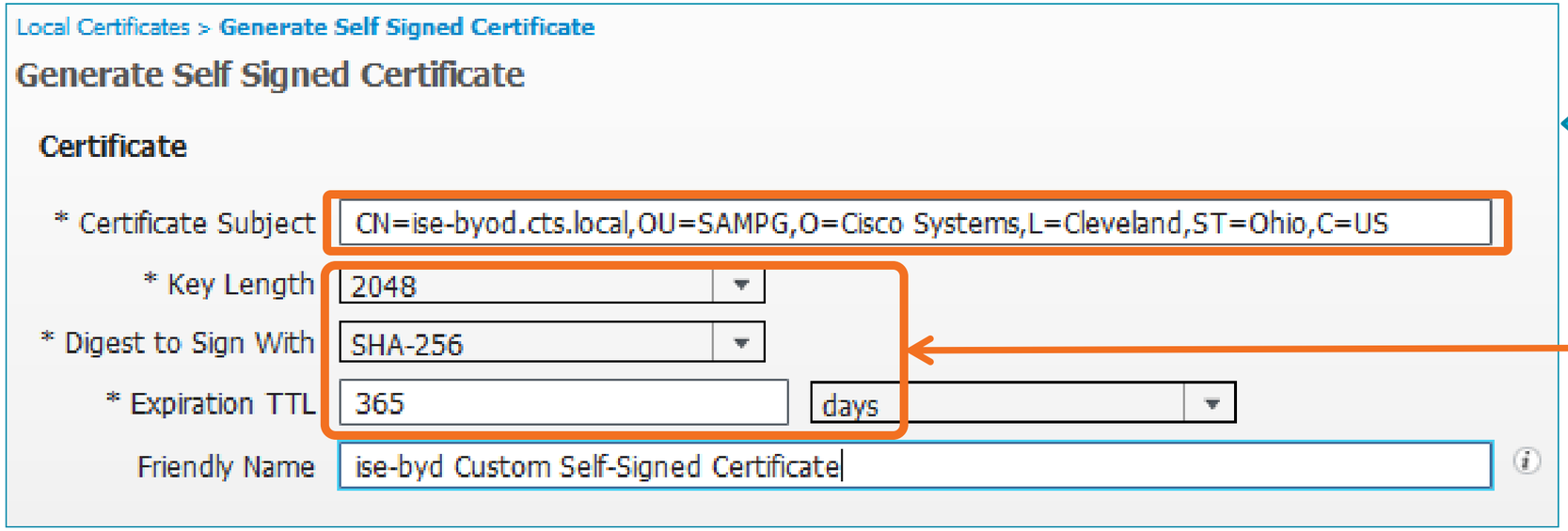


ISE Certificates and Custom Attributes

Basic Subject Name Attributes

- Stand-Alone deployment or Distributed Administration node:
  Administration > System > Certificates > Local Certificates
- Distributed deployment:
  Administration > System > Server Certificate
- Add Cert / CSR with specified attributes:





Customise other attributes as needed

CSCtu03384 [certificate Attribute Value pair order in subject line] fixed in ISE 1.1 to allow entry of multiple attributes in Subject line of ISE CSR request without errors.

ISE Certificates and Custom Attributes

Subject, Subject Alternative Name (SAN), EKU

- Install OpenSSL 0.9.8h
  http://gnuwin32.sourceforge.net/packages/openssl.htm
- Customise the configuration file *openssl.conf*
  - Update alt_names with each alias
  - Be sure to include CN of ISE node (= FQDN)
- Update DNS Records

Dedicated PSN

DNS SERVER
DOMAIN = CTS.LOCAL

ISE-PSN	100.1.100.5
SPONSOR	100.1.100.5
MYDEVICES	100.1.100.5
ISE-PSN-1	100.1.100.5
ISE-PSN-2	100.1.100.6
ISE-PSN-3	100.1.100.7

PSN Cluster

DNS SERVER
DOMAIN = CTS.LOCAL

ISE-PSN	100.1.99.5
SPONSOR	100.1.99.5
MYDEVICES	100.1.99.5
ISE-PSN-1	100.1.100.5
ISE-PSN-2	100.1.100.6
ISE-PSN-3	100.1.100.7

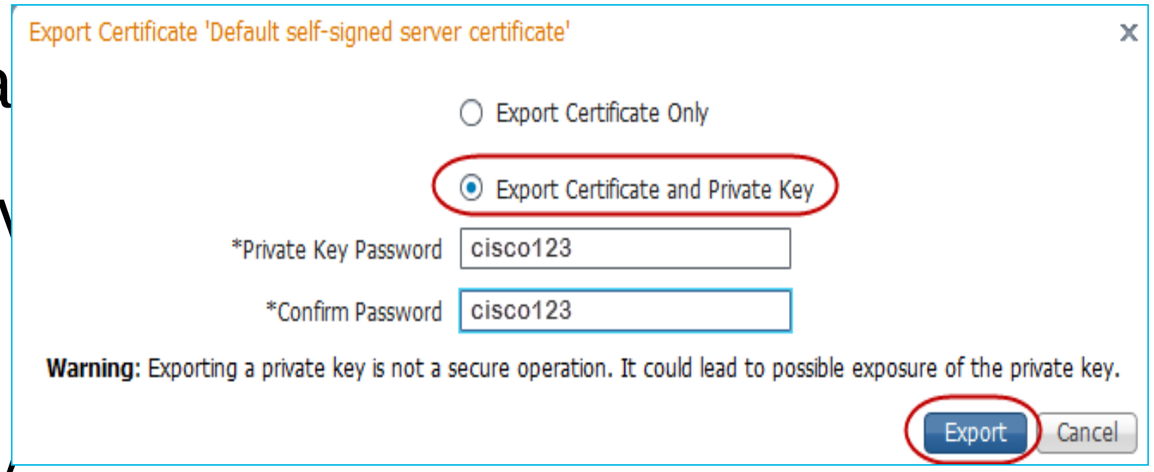
Sample OPENSSL.CONF file

```
##############################################
# This is where we define how to generate CSRs
[ req ]
default_bits  = 2048
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
req_extensions = v3_req
string_mask = nombstr
##############################################
# Per "req" section, define DN info
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default  = US
… <Other DN attributes> …
##############################################
# Extension for requests
[ v3_req ]
basicConstraints = CA:true
extendedKeyUsage  = serverAuth, clientAuth
keyUsage = keyEncipherment, digitalSignature
subjectAltName = @alt_names
[alt_names]
DNS.1   = ise-psn-1.cts.local
DNS.2   = ise-psn.cts.local
DNS.3   = sponsor.cts.local
DNS.4   = mydevices.cts.local
##############################################
```

ISE Certificates and Custom Attributes

- Export Key and Generate CSR using OpenSSL
- Export Self-Signed Cert with Priva
- Extract contents of exported archiv

  Example: Certificate = psn1.pem
  Private Key = psn1.pvk
- Generate CSR using exported key

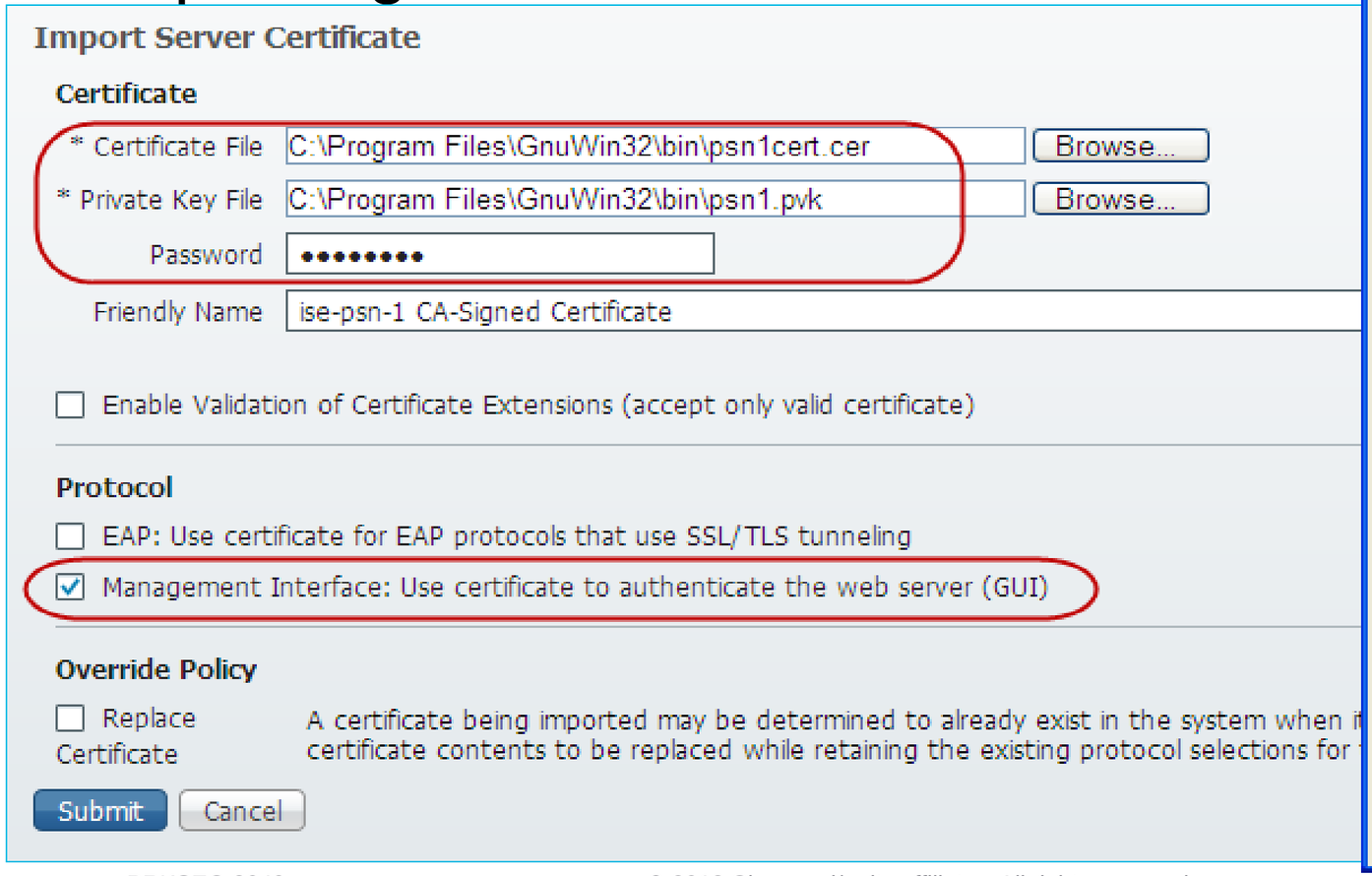


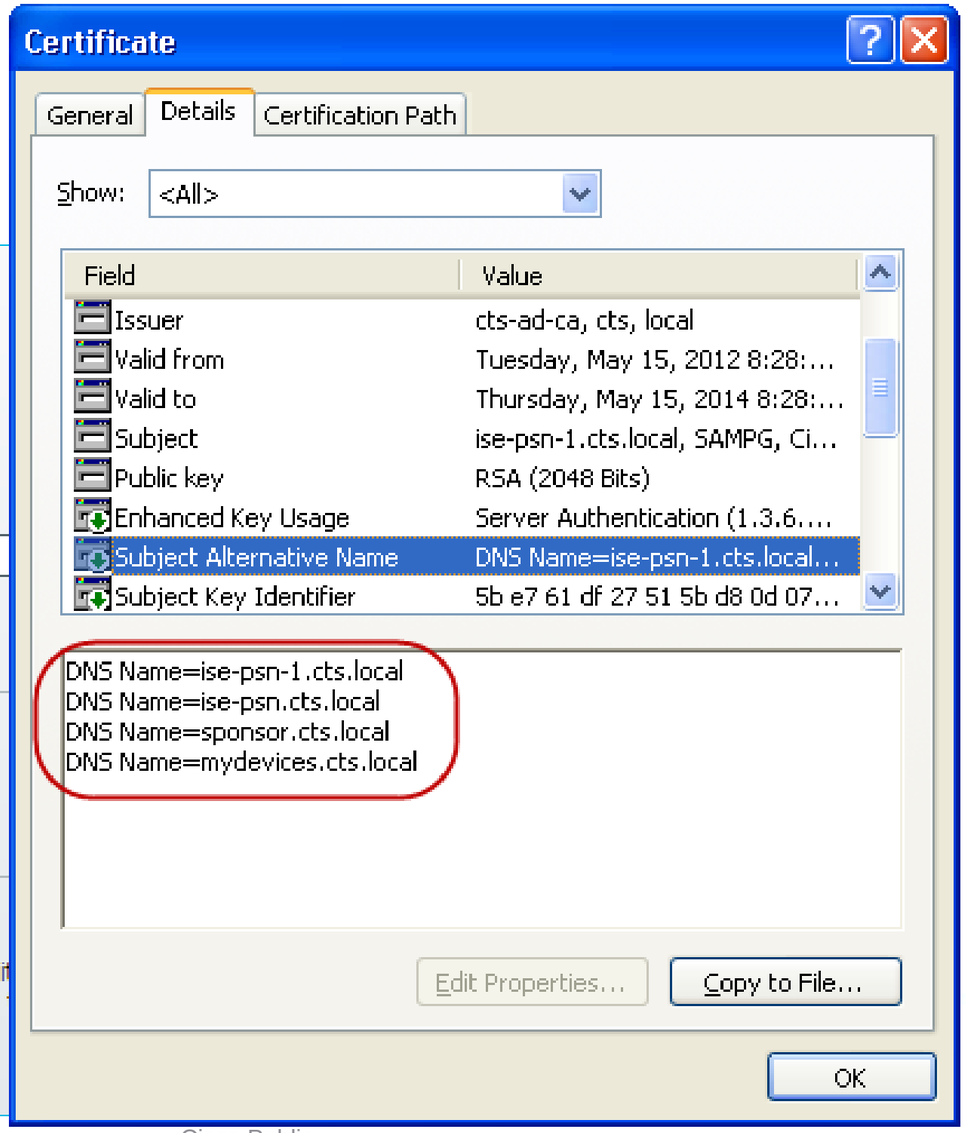

```
C:\Program Files\GnuWin32\bin> openssl req -new -key psn1.pvk -
  new -out psn1csr.pem -config .\openssl.conf

Enter pass phrase for psn1.pvk: cisco123
Country Name (2 letter code) [US]:
State or Province Name (full name) [California]: Ohio
Locality Name (eg, city) [Los Angeles]: Cleveland
Organization Name (eg, company) [Cisco Systems]: Cisco Systems
Organizational Unit Name (eg, section) [ABCDEF Corporation]:
  SAMPG
Common Name (eg, YOUR name) []: ise-psn-1.cts.local
```

ISE Certificates and Custom Attributes

- Sign CSR and Import into ISE
- Submit CSR to CA for signing
- Import signed cert into ISE PSN





Other ISE Best Practice Tips

DNS & NTP

- DNS
  - Reverse DNS required for AD Integration.
  - All ISE Nodes must be resolvable by FQDN
- NTP
  - Cannot stress enough how important time sync is.
  - Use NTP. Ensure it is accurate.
  - Time Zone = UTC a best practice for large deployments.

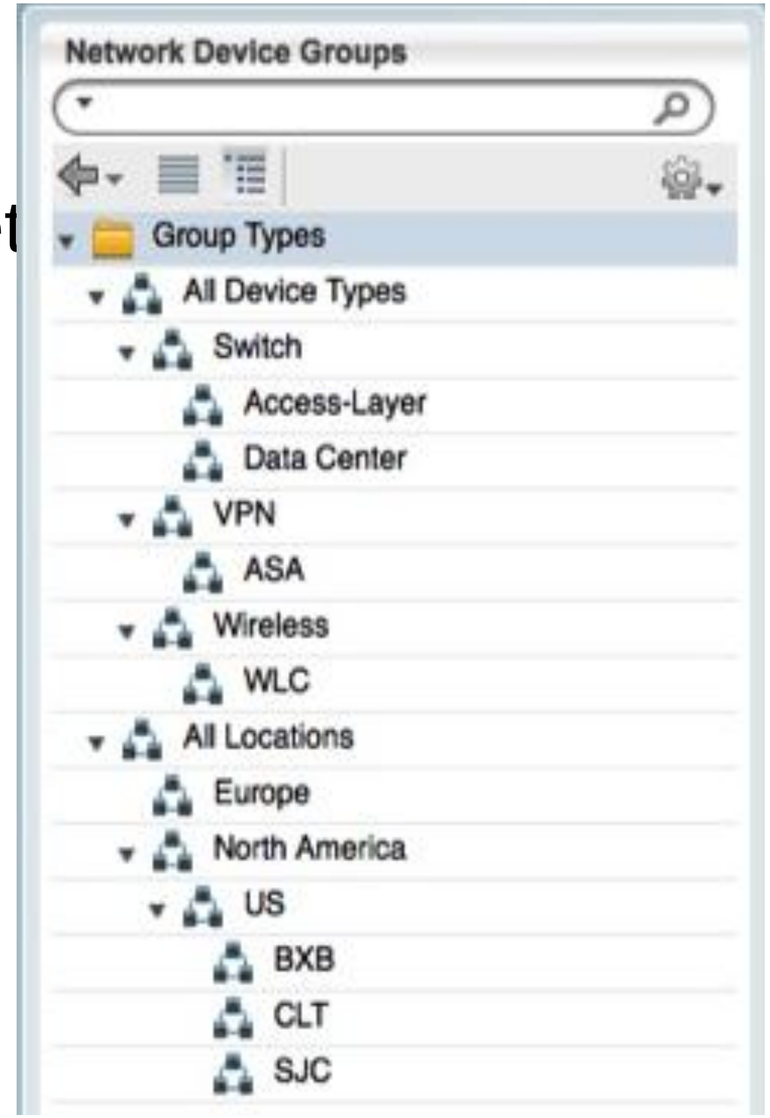
```
ise-pan-01/admin(config)# clock timezone EST5EDT

Changing the system timezone may result in undesired side effects on
any installed application(s).
Are you sure you want to proceed? Y/N [N]: N
ise-pan-01/admin(config)# _
```

Network Device Groups

Creation of Many: Organise & Why Use Them

- A little up-front work, can really help you get policies.
- Organise by:
  - Device Type
    - Wired / Wireless / Firewall / VPN
    - OEAP / CVO
  - Place in Network
    - Access-Layer / Data Centre
  - Geographic Location



Graceful Transition from Monitor Mode to an EndState

Monitor Mode Policies

- BE CAREFUL
- Monitor Mode needs to keep Authorisation Results simple
  - Access-Accept / Reject
  - For Phones, needs: Voice Domain also
- Local Authorisations Still Possible (be careful):

```
interface X
 authentication event fail action next-method
 authentication event server dead action reinitialise vlan 11
 authentication event server dead action authorise voice
 authentication event server alive action reinitialise
 authentication violation restrict
```

Good for Monitor Mode

```
interface X
 authentication event fail action authorise vlan 4096
 authentication event server dead action reinitialise vlan 11
 authentication event server dead action authorise voice
 authentication event server alive action reinitialise
 authentication violation restrict
```

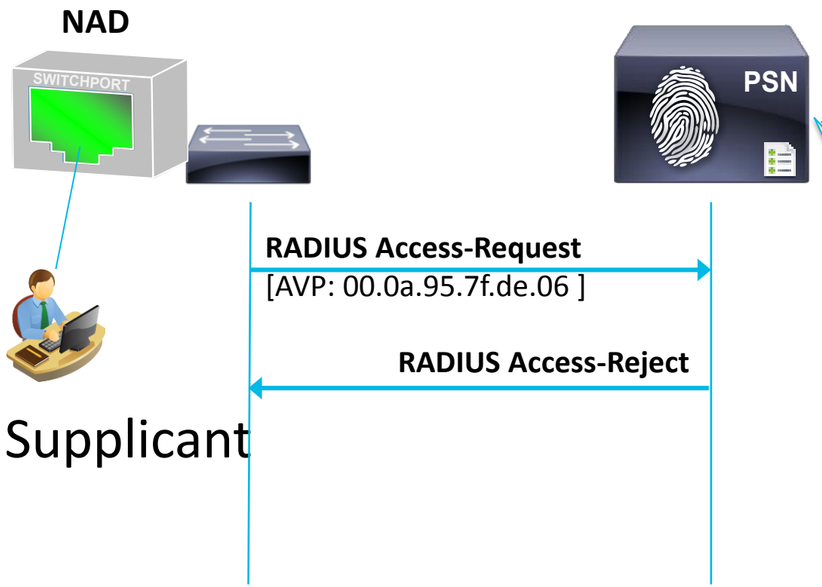
Dangerous for Monitor Mode

Moving from Monitor to Low-Impact Mode

Monitor Mode

```
interface GigabitEthernet1/0/1
 authentication open
 mab
 dot1x pae authenticator
```

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
BYOD	if	BYOD and Employee	then	Employee
Non_AuthZ	if	i-device or Android	then	GUEST
Contractor	if	Contractor	then	Contractor
Employee	if	Employee	then	Employee
Default	If no matches, then		Deny Access	



Matched Rule = Default

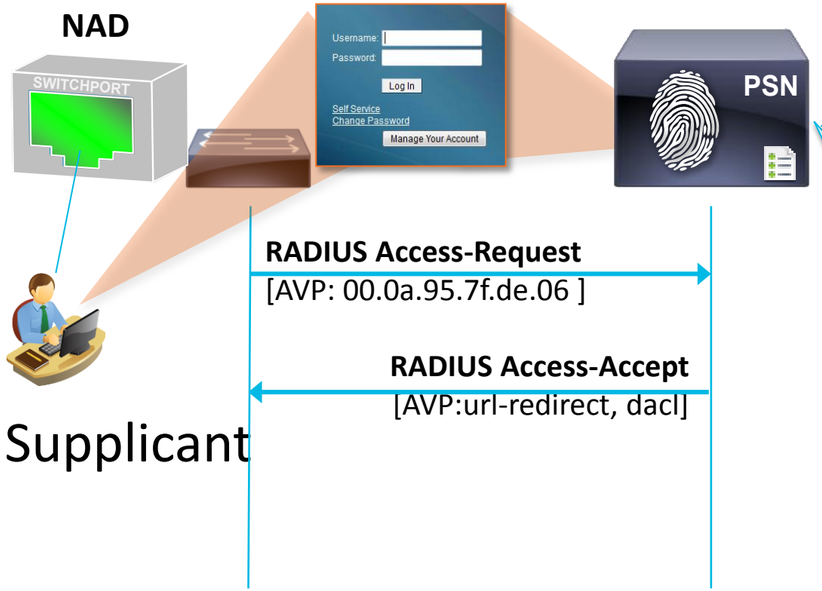
MAC-Addr is Unknown…
Continue to AuthZ table

Moving from Monitor to Low-Impact

Low-Impact

```
interface GigabitEthernet1/0/1
 authentication open
 mab
 dot1x pae authenticator
 ip access-group ACL-DEFAULT in
```

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
BYOD	if	BYOD and Employee	then	Employee
Non_AuthZ	if	i-device or Android	then	GUEST
Contractor	if	Contractor	then	Contractor
Employee	if	Employee	then	Employee
Default	If no matches, then		WEBAUTH	



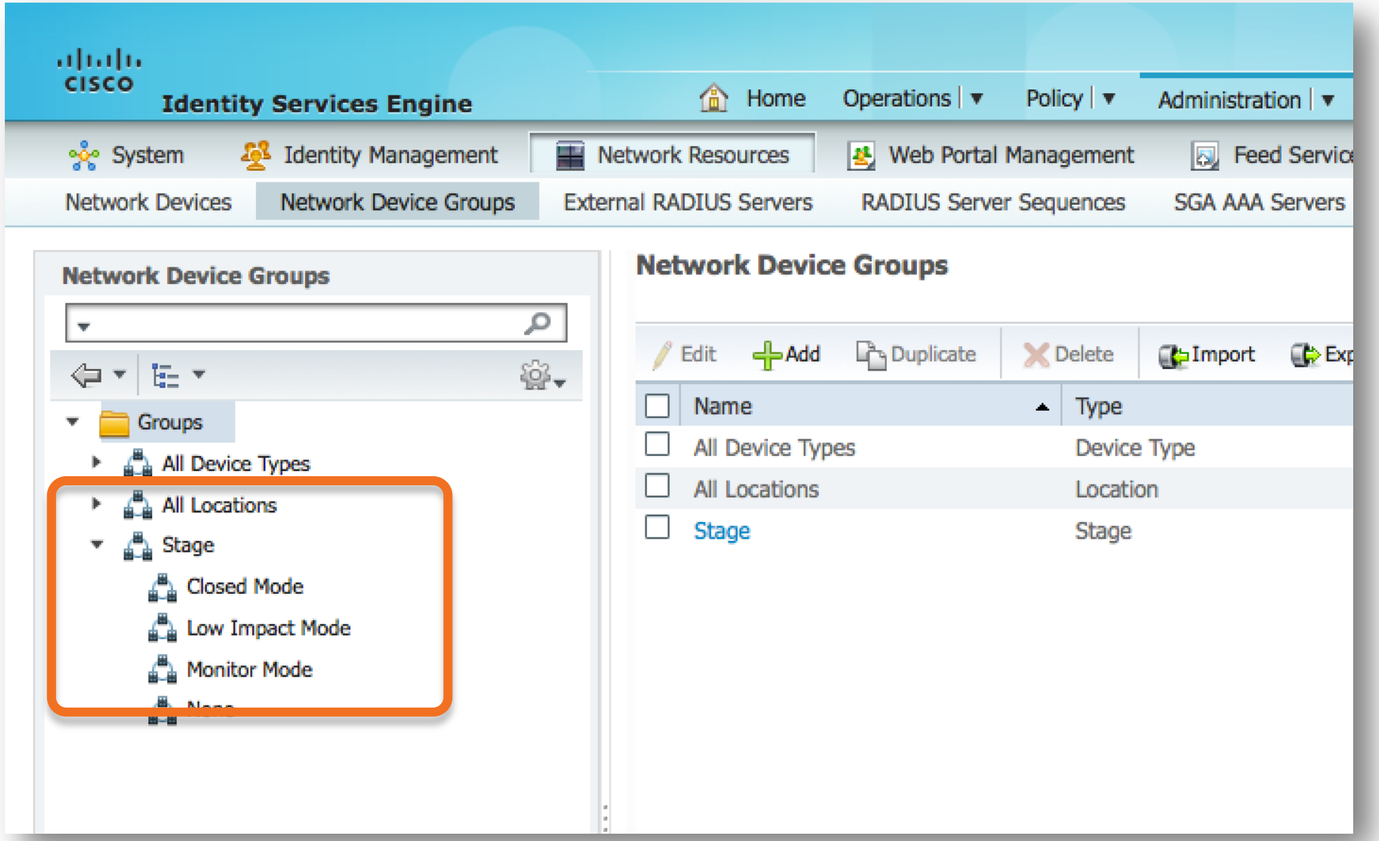
Matched Rule = Default

MAC-Addr is Unknown…
Continue to AuthZ table

Moving from Monitor to Low-Impact

Low-Impact: An Entire Switch at a Time

- Create a Network Device Group for all Switches that will use Low-Impact.

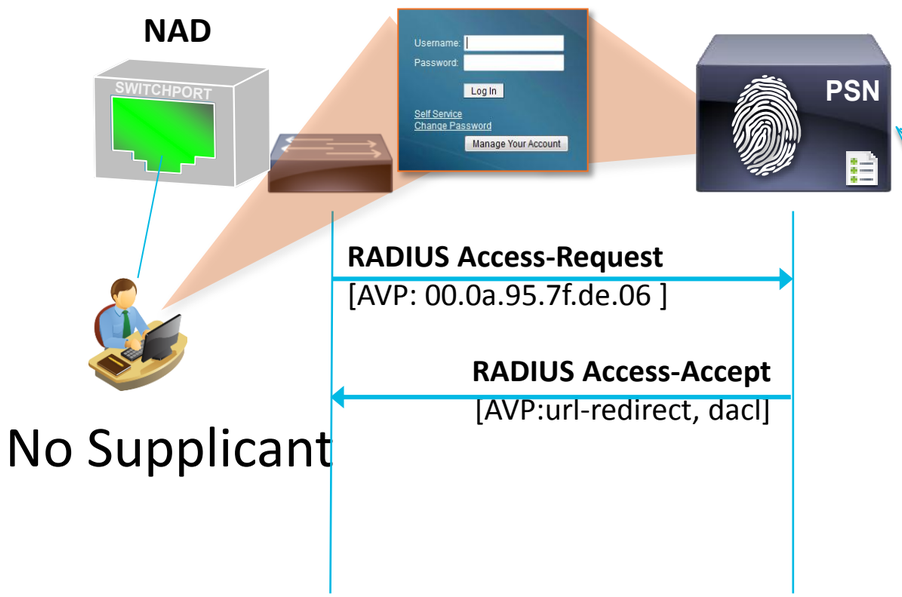


Moving from Monitor to Low-Impact

Low-Impact: An Entire Switch at a Time

```
interface GigabitEthernet1/0/1
 authentication open
 mab
 dot1x pae authenticator
 ip access-group ACL-DEFAULT in
```

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
BYOD	if	BYOD and Employee	then	Employee
Non_AuthZ	if	i-device or Android	then	GUEST
Contractor	if	Contractor	then	Contractor
Employee	if	Employee	then	Employee
Conf_Rooms	if	DEVICE:Stage EQUALS Stage#LowImpact	then	WEBAUTH
Default	If no matches, then	Deny Access		



Matched Rule = Conf_Rooms

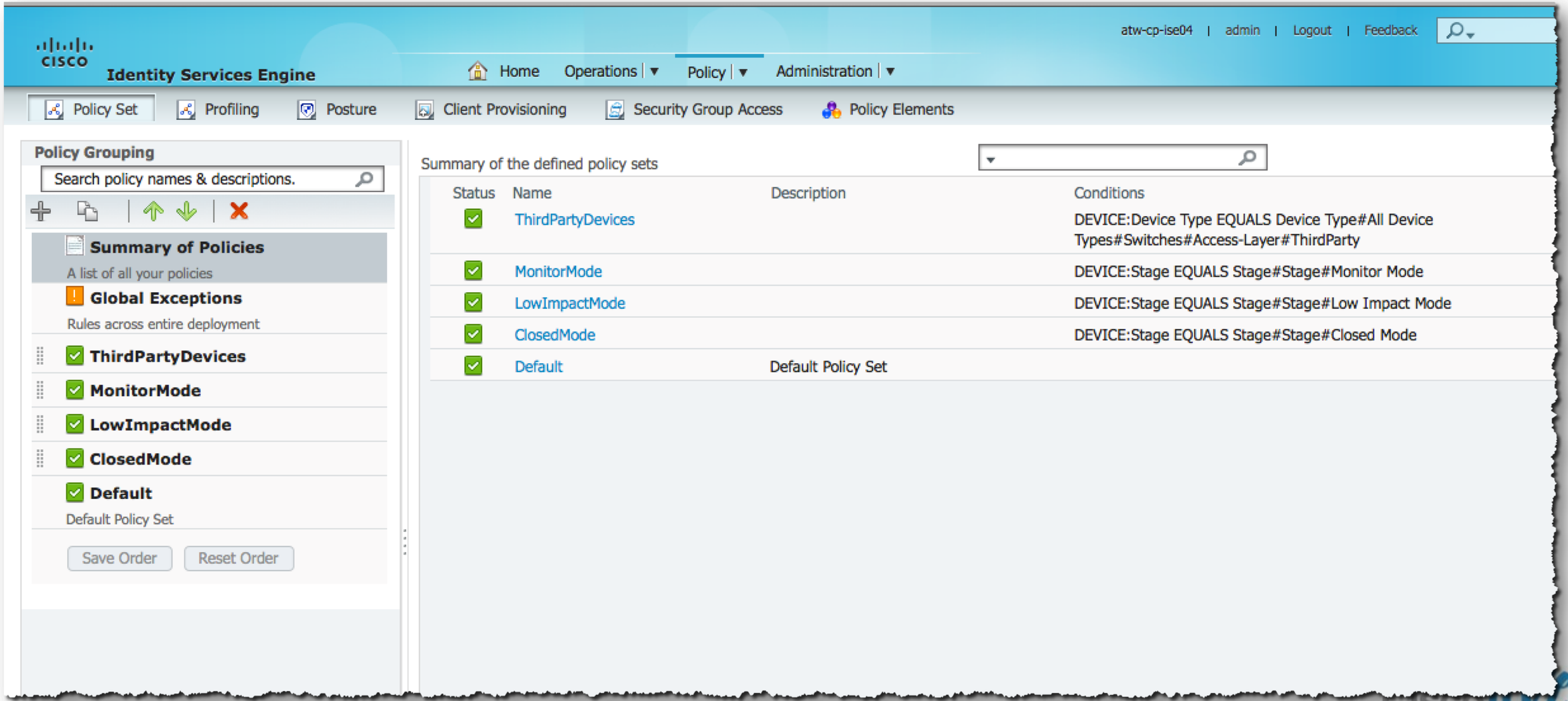
MAC-Addr is Unknown… Continue to AuthZ table

All Other Switches Will still be in Monitor Mode!

ISE 1.2: Policy Sets

Separate Set of Policies for Each Mode of Deployment

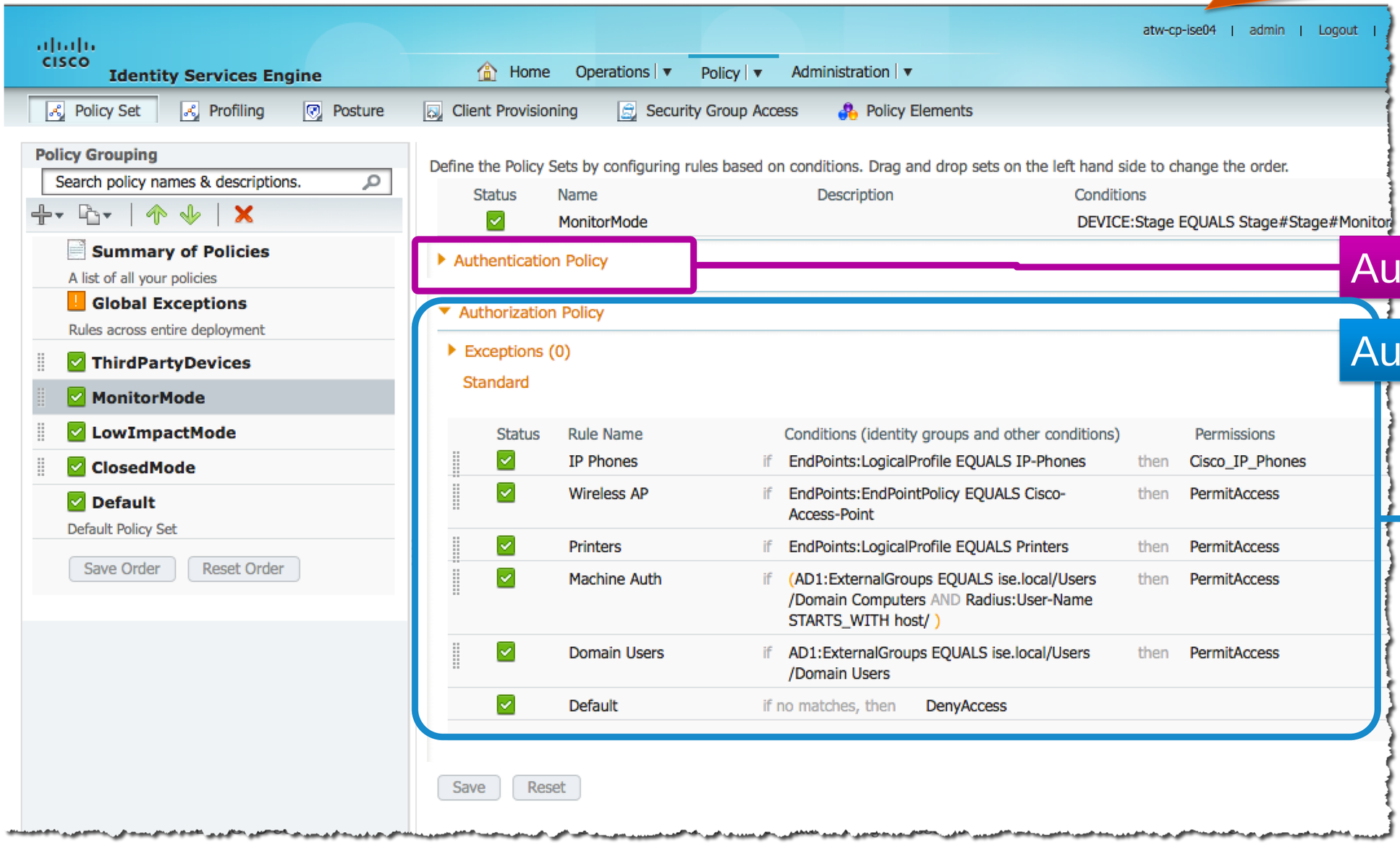
ISE 1.2+



ISE 1.2: Policy Sets

Separate Set of Policies for Each Mode of Deployment

ISE 1.2+

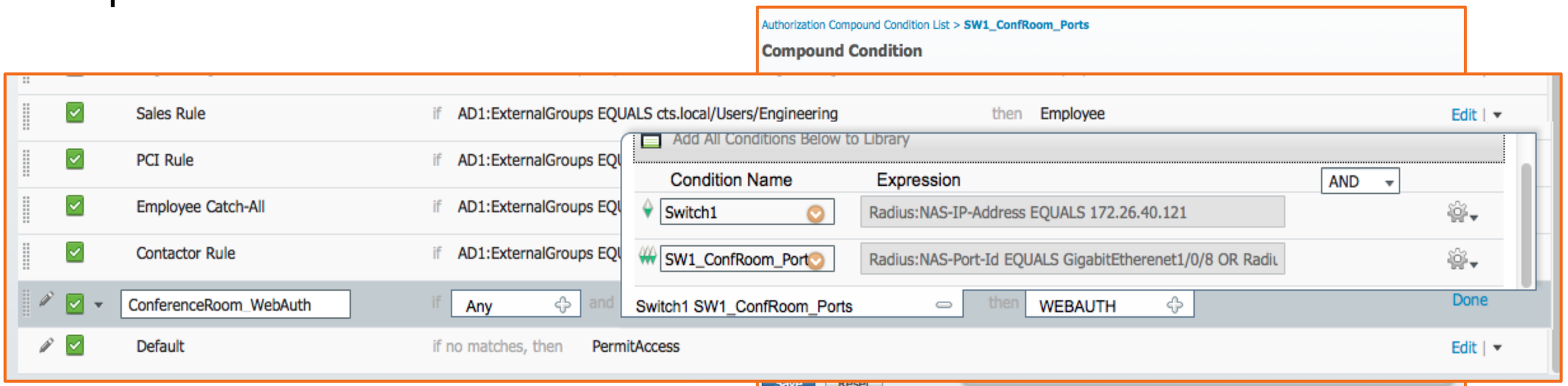


Authentication Policy

Authorisation Policy

Moving from Monitor to Low-Impact

- Specifying NAD + Interfaces in AuthZ Policy
- When you are willing to enable it a switch at a time, it's easy.
  - Most want to enable it a port at a time (Conference rooms only, for example).
- How can we identify which port(s) should be treated differently?
  - We can build a static list of Switches and their Ports
  - Requires 1 AuthZ rule line Per Switch



Moving from Monitor to Low-Impact

mab eap Trick of the Trade

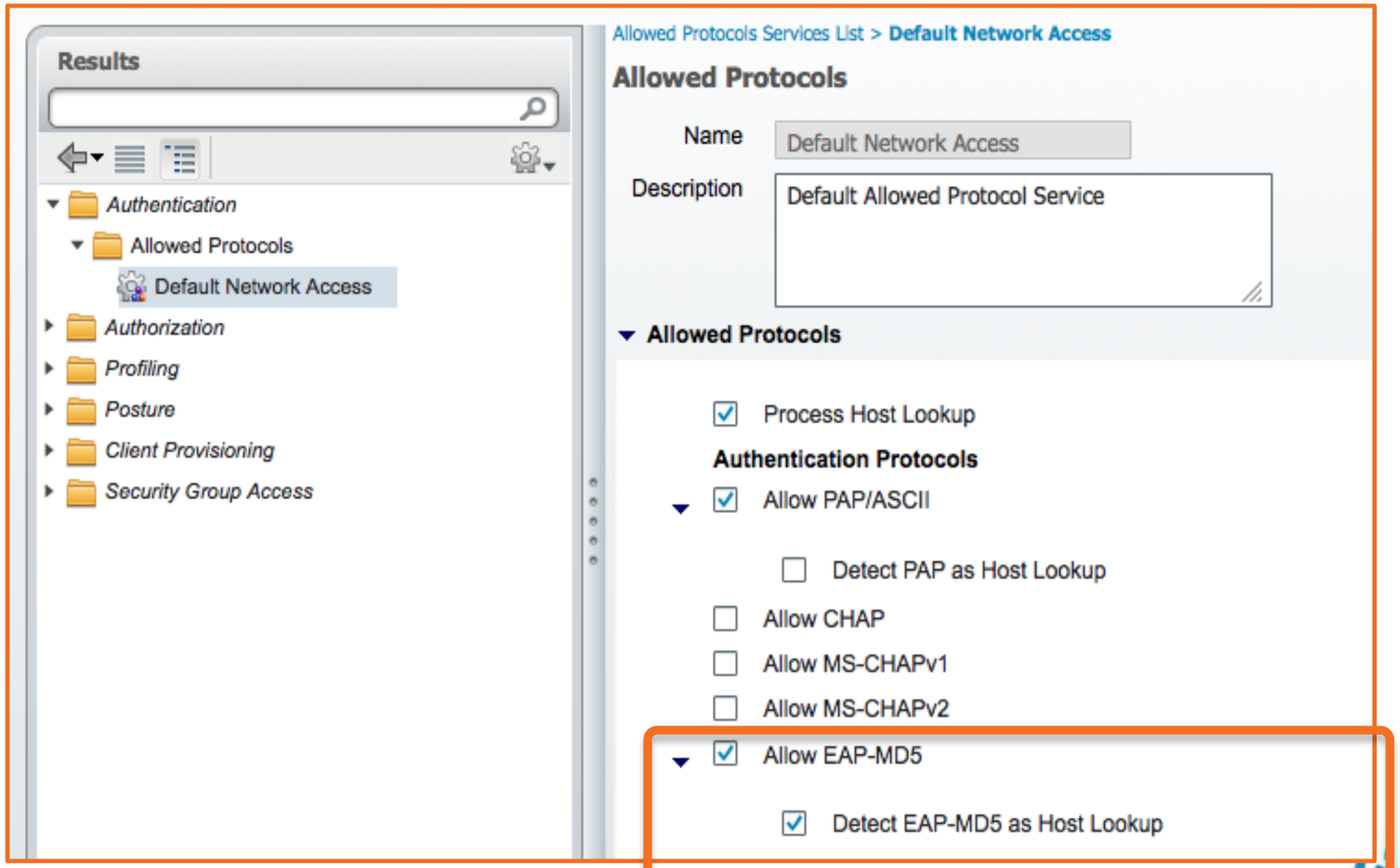
- What is “mab eap”?
  - Option of MAB configuration uses EAP-MD5 to transmit the MAB data.
- Behaviour with ISE will be the same.
  - We can use this as a differentiator ports that should be in Low-Impact.

```
C3750X(config-if)#mab ?
  eap  Use EAP authentication for MAC Auth Bypass
  <cr>
C3750X(config-if)#mab eap
C3750X(config-if)#description Conference Room B
```

Available with ISE 1.1+

Moving from Monitor to Low-Impact

- MAB EAP Trick of the Trade
- Policy → Policy Elements → Authentication → Results →Allowed Protocols
  - Allow EAP-MD5
  - Detect EAP-MD5 as Host Lookup



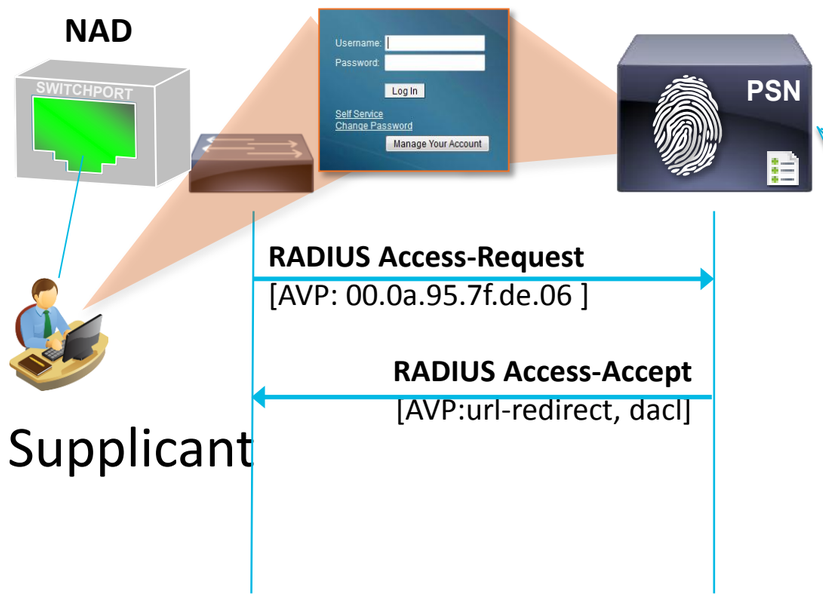
Note: Best-Practice is to never modify default objects

Moving from Monitor to Low-Impact

MAB EAP Trick of the Trade

```
interface GigabitEthernet1/0/1
 authentication open
 mab eap
 dot1x pae authenticator
 ip access-group ACL-DEFAULT in
```

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
BYOD	if	BYOD and Employee	then	Employee
Non_AuthZ	if	i-device or Android	then	GUEST
Contractor	if	Contractor	then	Contractor
Employee	if	Employee	then	Employee
Conf_Rooms	If	Network Access:EapAuthentication EQUALS EAP-MD5	then	WEBAUTH
Default	If no matches, then	Deny Access		



Matched Rule = Conf_Rooms

All Other Switches Will still be in Monitor Mode!

MAC-Addr is Unknown… Continue to AuthZ table

Moving from Monitor to Low-Impact

MAB EAP Trick of the Trade

Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event
		#ACSACL#-IP-PERMIT			SJC-18-sw-1					DACL
		00:50:56:87:00:04	00:50:56:87:00:04	10.1.10.51	SJC-18-sw-1	GigabitEthernet1/0/2	WEBAUTH	Profiled:Workstation	Pending	Authe

Authentication Summary

Logged At:	March 1,2012 1:59:56.355 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	00:50:56:87:00:04
MAC/IP Address:	00:50:56:87:00:04
Network Device:	SJC-18-sw-1 : 192.168.254.1 : GigabitE
Allowed Protocol:	Default Network Access
Identity Store:	Internal Endpoints
Authorization Profiles:	WEBAUTH
SGA Security Group:	
Authentication Protocol :	EAP-MD5

Authentication Details

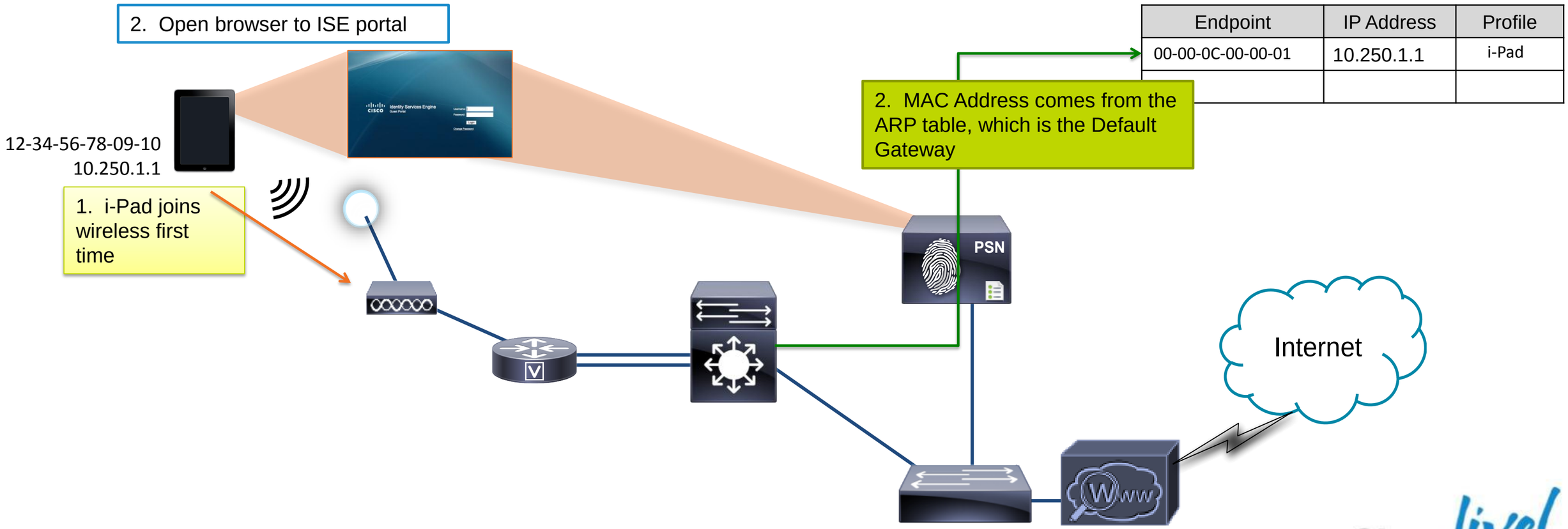
Logged At:	March 1,2012 1:59:56.355 PM
Occurred At:	March 1,2012 1:59:56.355 PM
Server:	ise01
Authentication Method:	dot1x
EAP Authentication Method :	EAP-MD5
EAP Tunnel Method :	
Username:	00:50:56:87:00:04
RADIUS Username :	00:50:56:87:00:04
Calling Station ID:	00:50:56:87:00:04
Framed IP Address:	10.1.10.51
Use Case:	Host Lookup
Network Device:	SJC-18-sw-1

Profiling

Profiling

Importance of DHCP & RADIUS Probes…

- MAC ←→ IP Binding is CRITICAL
- Why: *What happens when the Probe (HTTP or NMAP or even NetFlow) is not L2 Adjacent.*



Profiling

How do we get the MAC←→ IP Bindings?

DHCP Probe

- The dhcp-requested address attribute in the DHCP packet

RADIUS Probe.

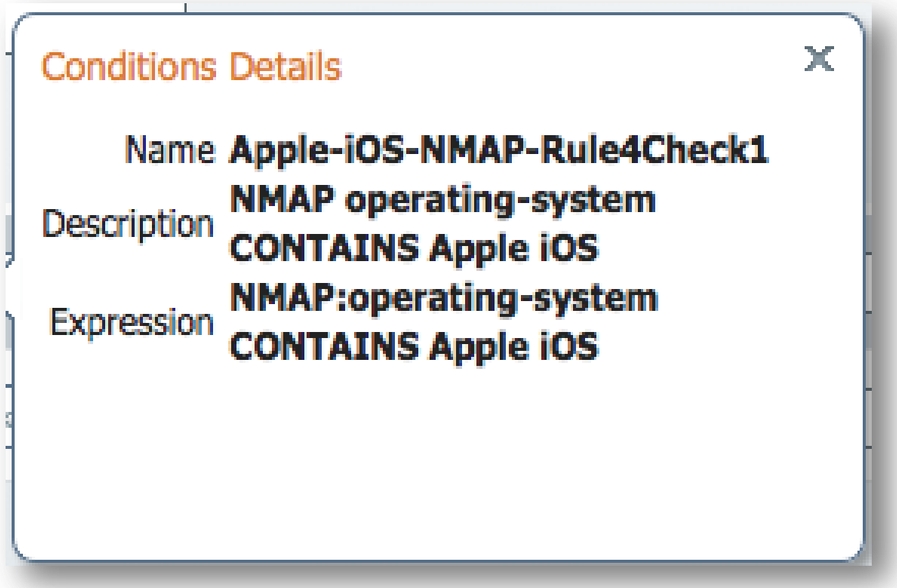
- Framed-IP-address attribute in RADIUS packet

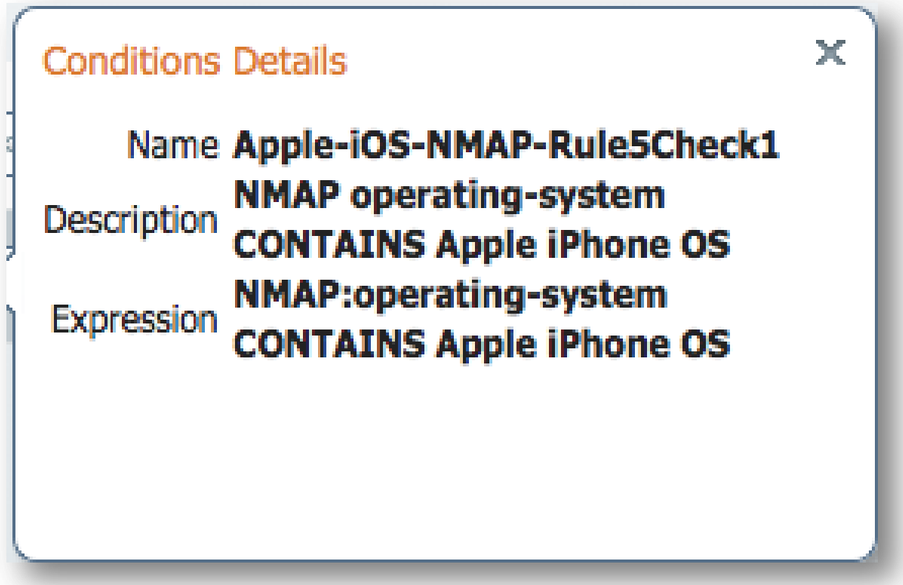
Profiling

i-devices profile w/ NMAP probe

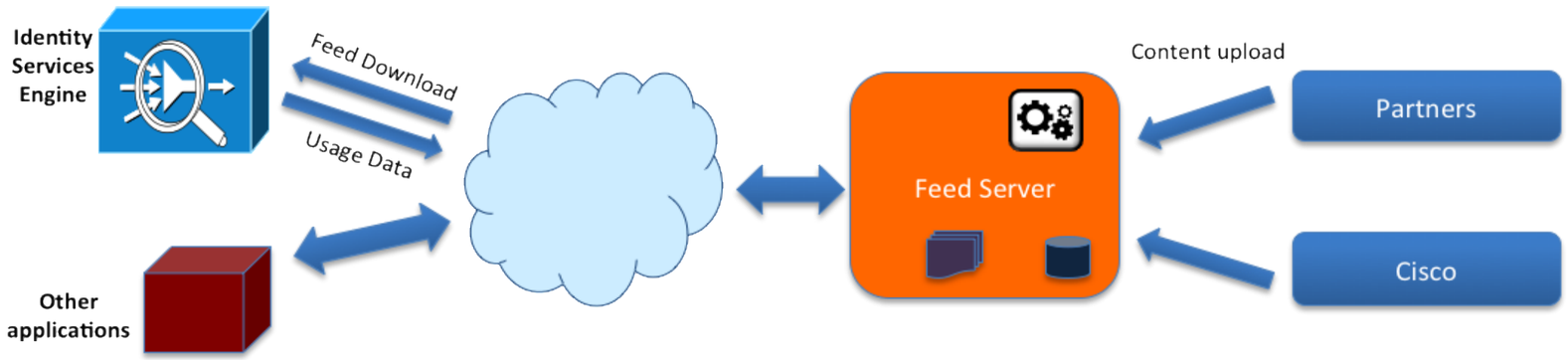
ISE 1.1+

- We gather generic information, such as iOS for OS.

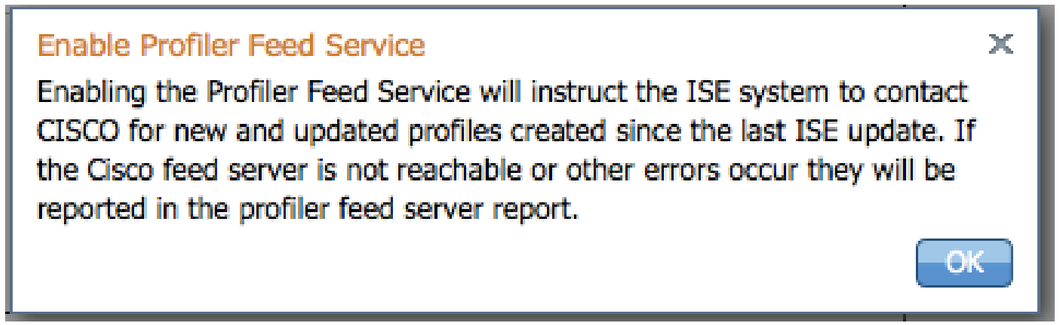


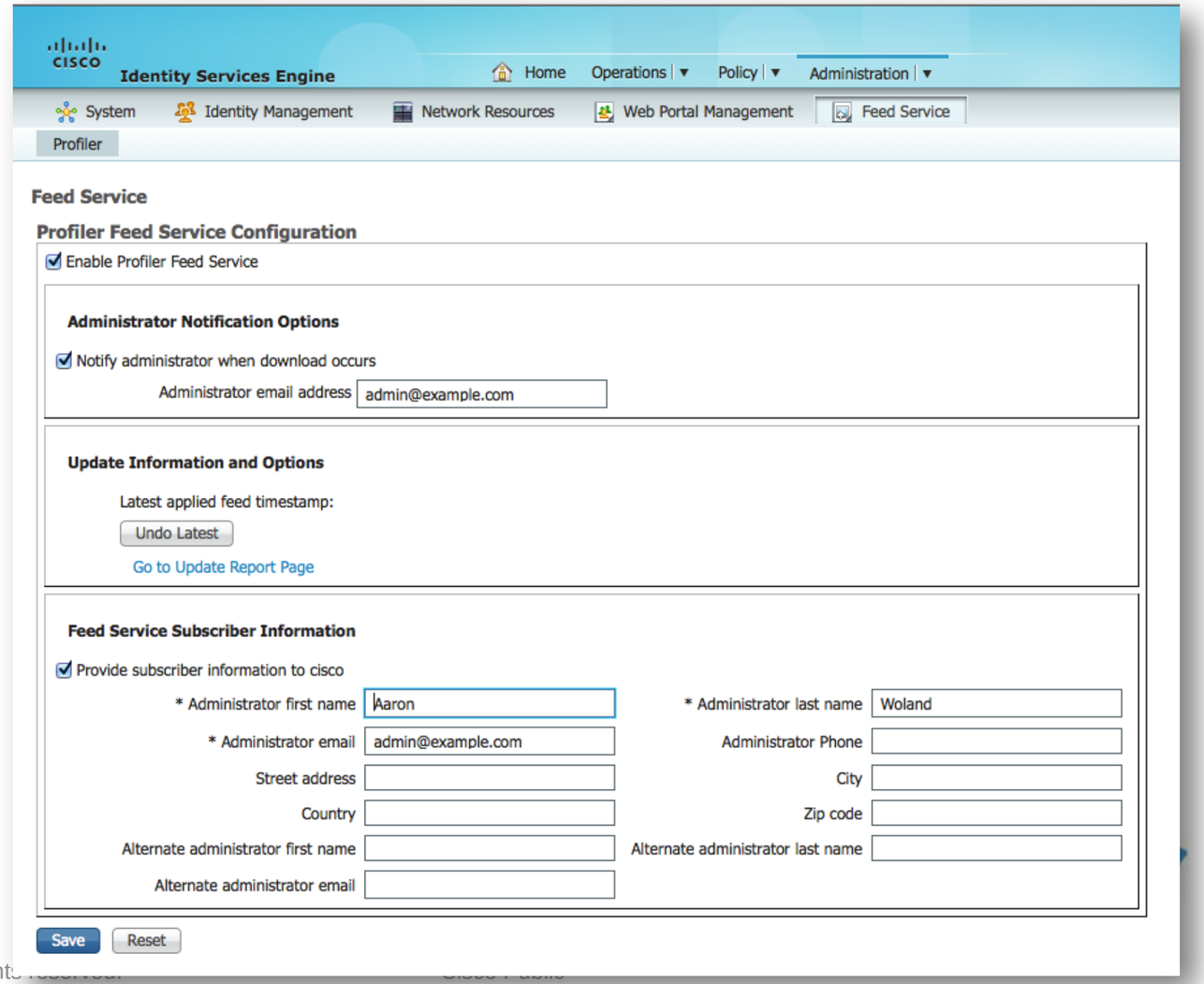


Feed Service



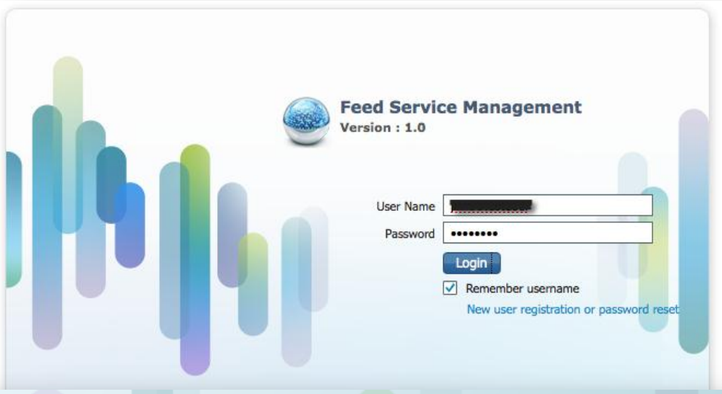
- Feeds OUI's, Profiles, Posture and BootStraps
- Has approval / publish process

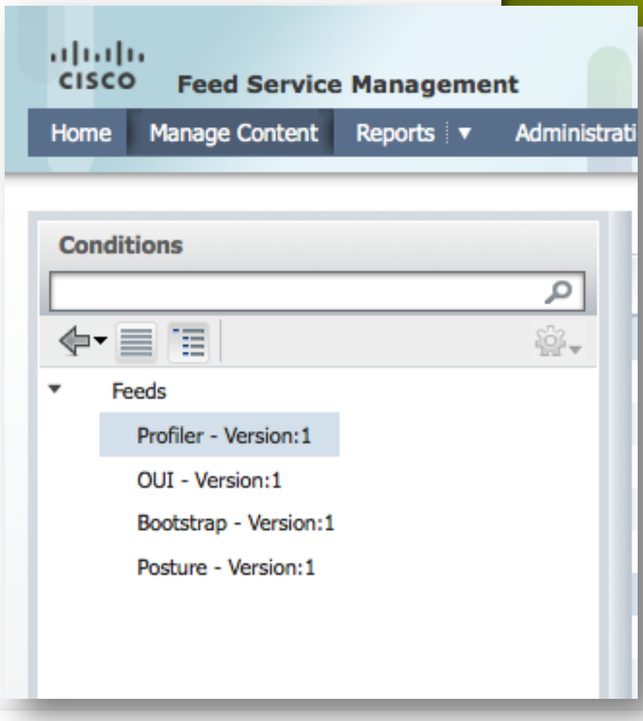


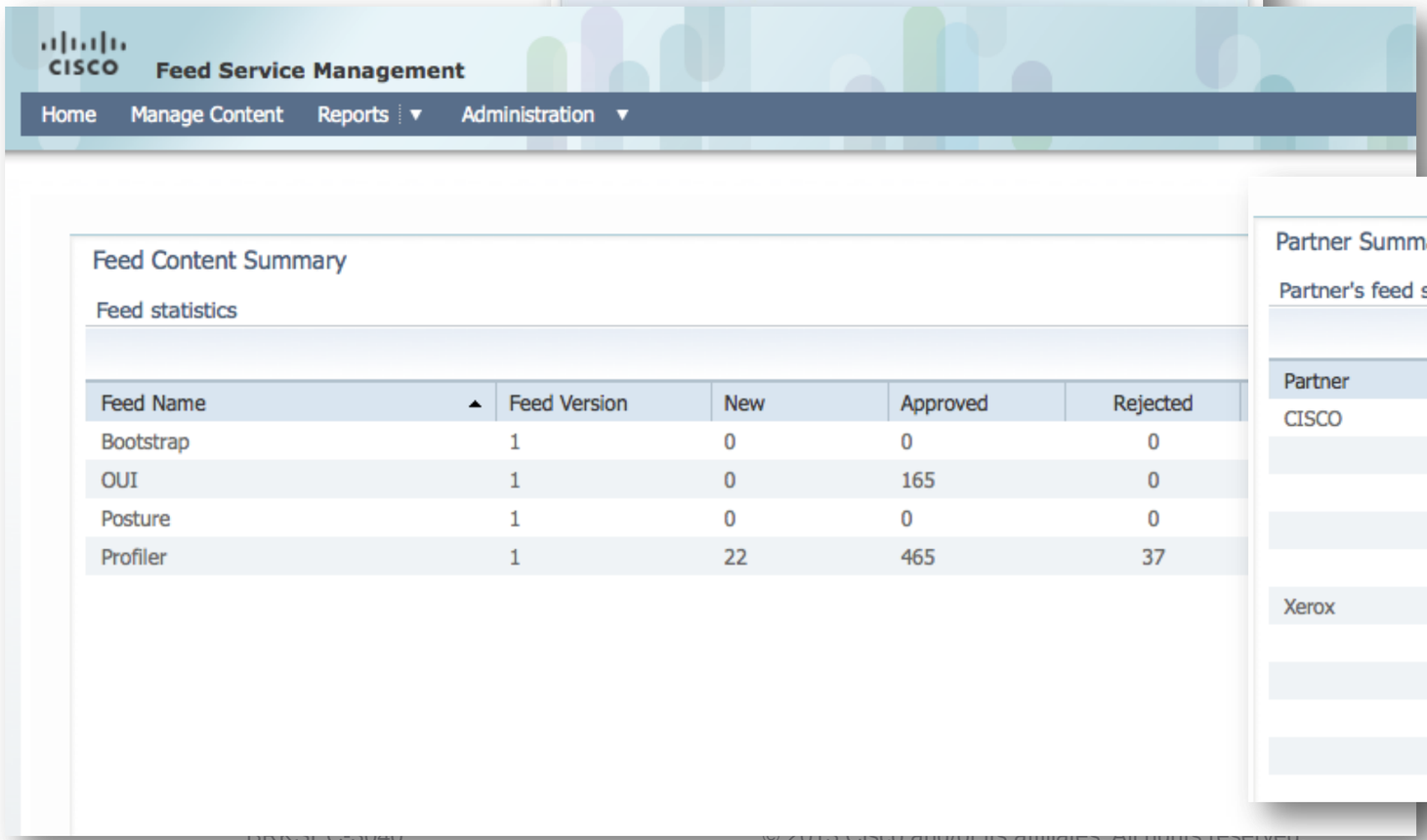


Feed Service Server

A Glimpse







Feed Content Summary

Feed statistics

Feed Name	Feed Version	New	Approved	Rejected
Bootstrap	1	0	0	0
OUI	1	0	165	0
Posture	1	0	0	0
Profiler	1	22	465	37

Partner Summary

Partner's feed statistics

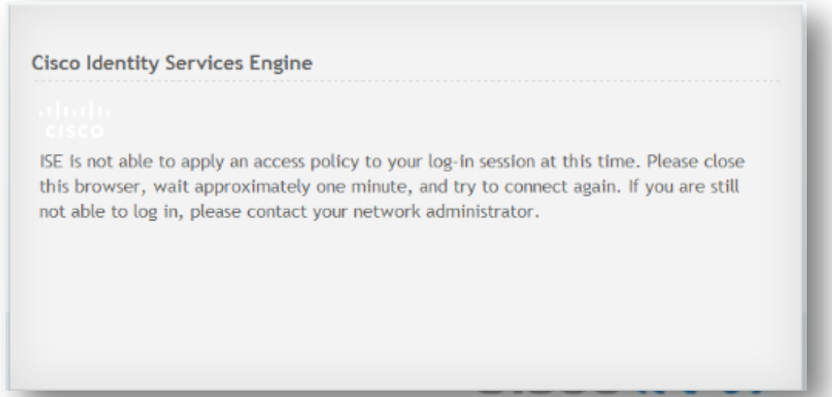
Partner	Feed Name	Feed Version	New	Approved	Rejected
CISCO	***Total***		22	628	27
	Profiler	1	22	463	27
	OUI	1	0	165	0
	Bootstrap	1	0	0	0
	Posture	1	0	0	0
Xerox	***Total***		0	2	10
	Profiler	1	0	2	10
	OUI	1	0	0	0
	Bootstrap	1	0	0	0
	Posture	1	0	0	0

Profiling

Grabbing User-Agent Strings from Portals (CWA or CPP)

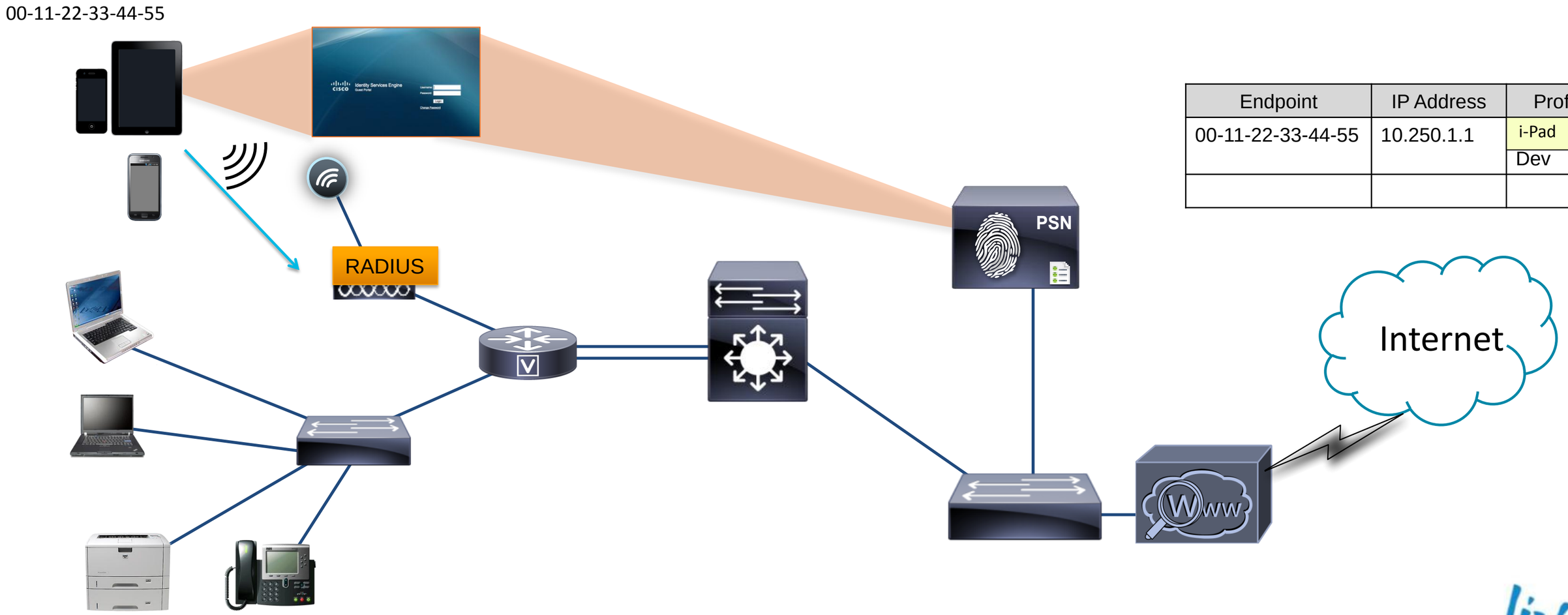
- In ISE 1.0, ISE leverages an invisible http object in the CWA/CPP page to acquire the user agent string during redirect to https for Client Provisioning and Posture content.
  - I.e.: iPad = No Posture Possible; MacOS = MAC Agent; Windows = Windows Agent and/or Temporal Agent
- Although redirected to CPP process, the separate Profiling process was not able to capture the user agent.
  - ISE 1.1+ code has been updated to allow the agent string acquired from the CPP (which evaluates decrypted packet) to be updated to profiling process.
- No HTTP Probe necessary to grab this.
  - This is less Processor intensive, but more “process intensive”

    i.e: it has impact on user-experience.



Getting Traffic to Probes: HTTP

Using the CPP or CWA portal to capture HTTP User-Agent



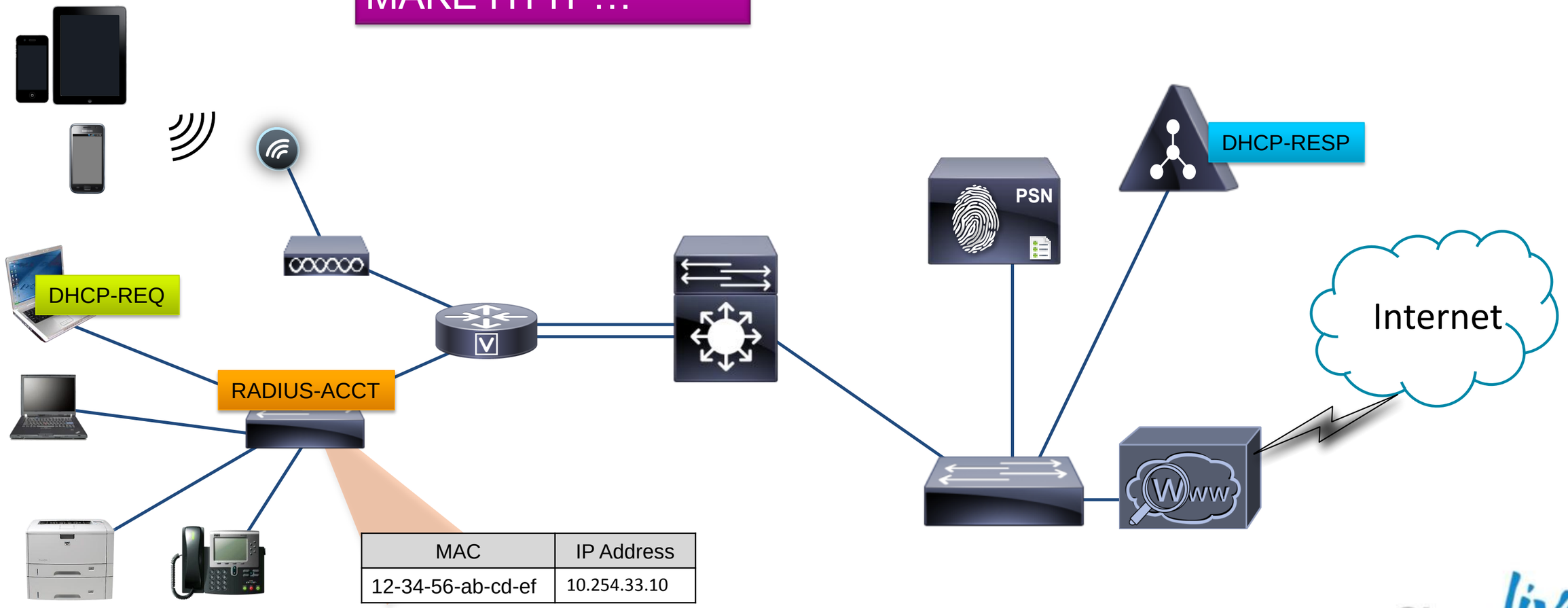
Endpoint	IP Address	Profile
00-11-22-33-44-55	10.250.1.1	i-Pad
		Dev

Getting Traffic to Probes: HTTP

Device Sensor

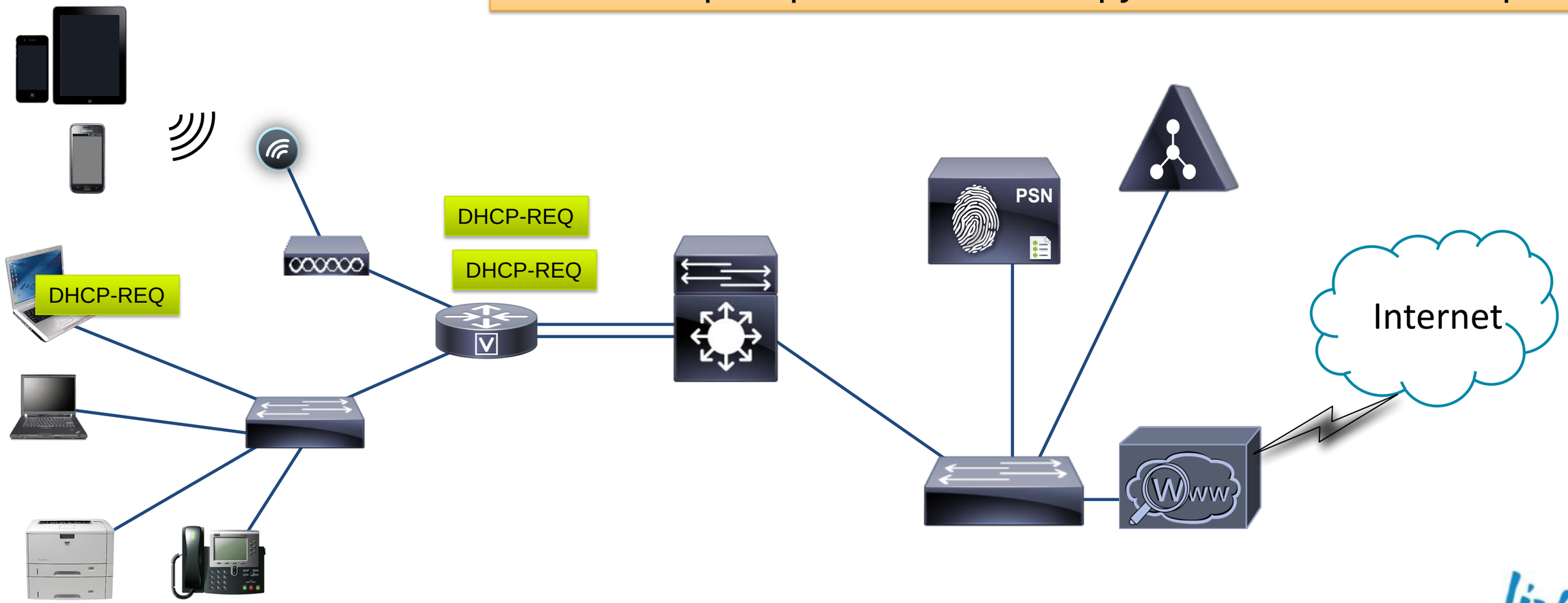
WLC 7.2.110+

AARON CLEAN UP
MAKE HTTP…



Getting Traffic to Probes: DHCP

Can use a ip helper-address to copy ISE on all DHCP requests

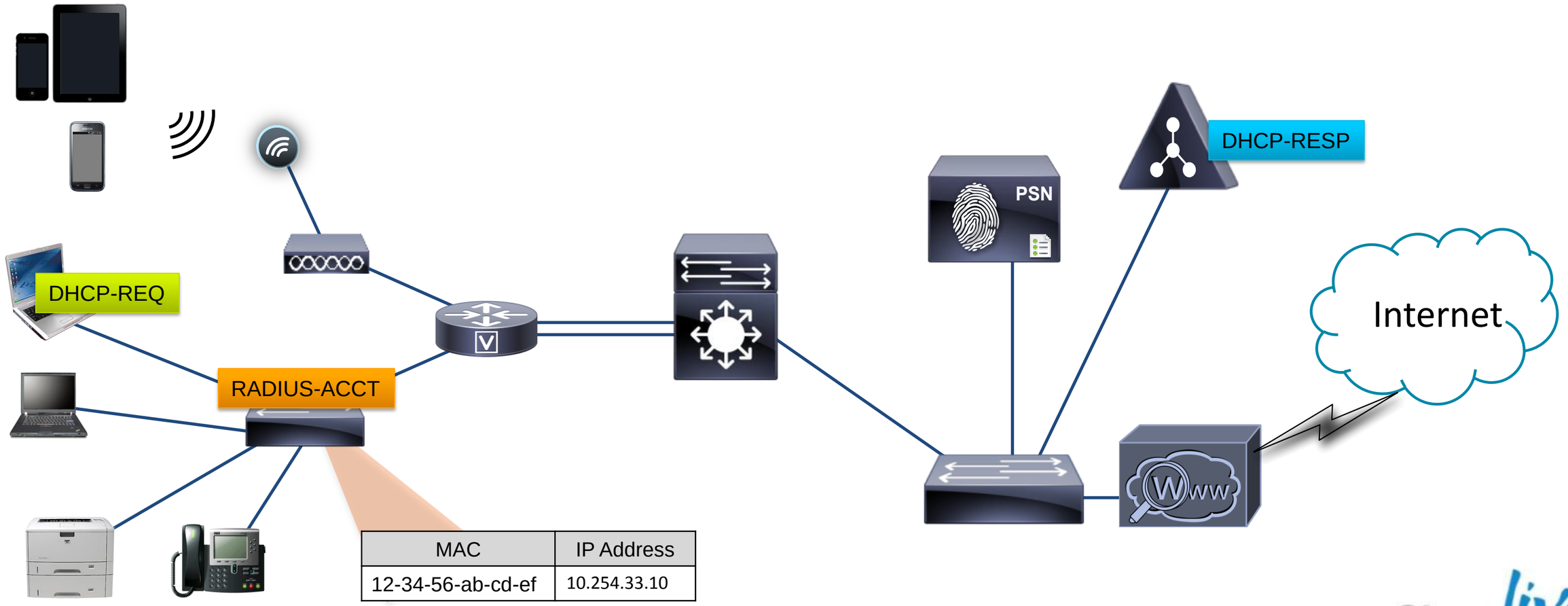


Getting Traffic to Probes: DHCP

Device Sensor

IOS 15.0(1)SE1+

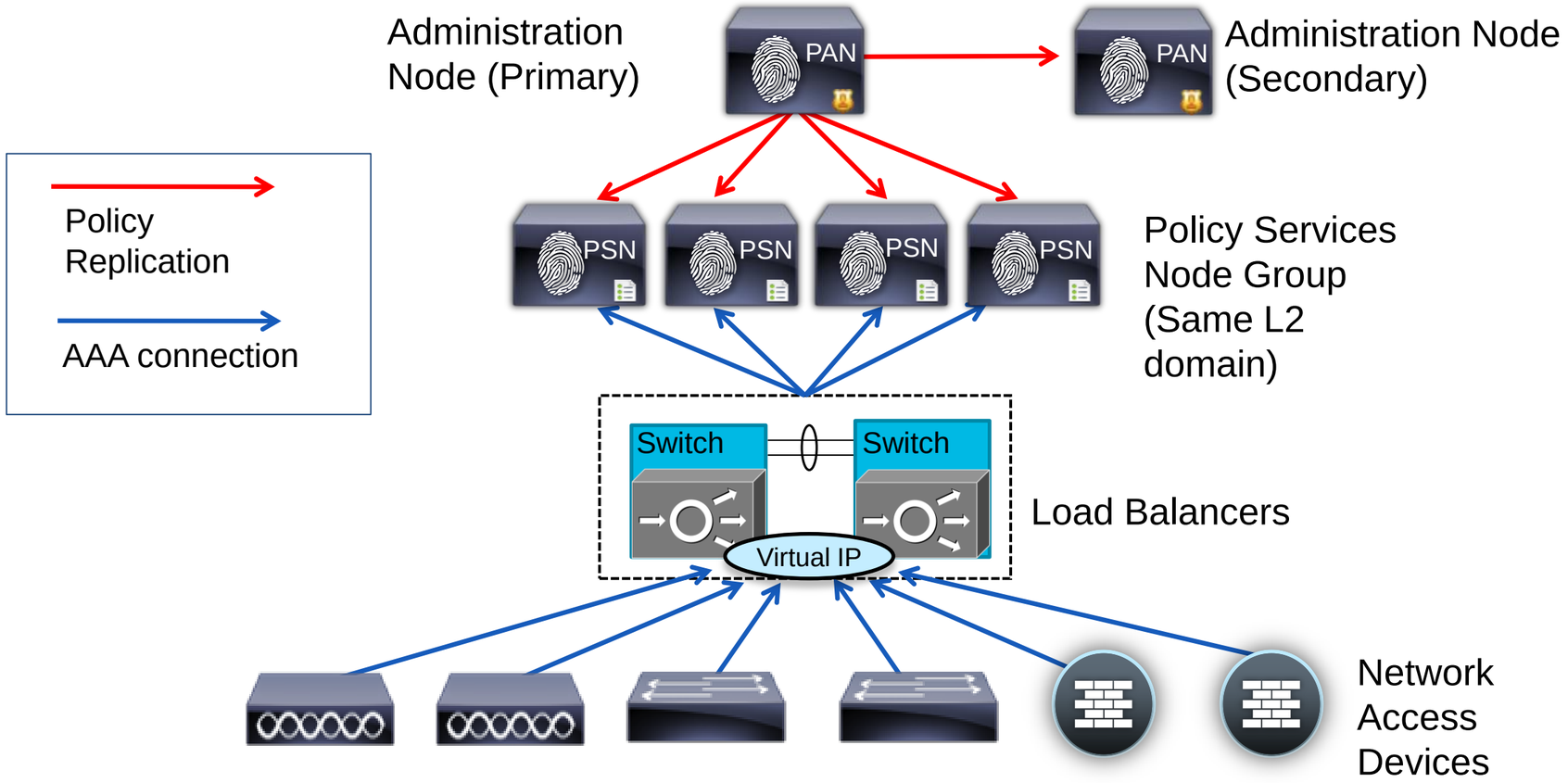
WLC 7.2.110+



Deployment Considerations and High Availability

Policy Service Node Scaling and Redundancy

- NADs can be configured with sequence of redundant RADIUS servers (PSNs).
- Policy Service nodes can also be configured in a cluster, or “node group”, behind a load balancer. NADs send requests to LB virtual IP for Policy Services.
- Policy Service nodes in node group maintain heartbeat to verify member health.

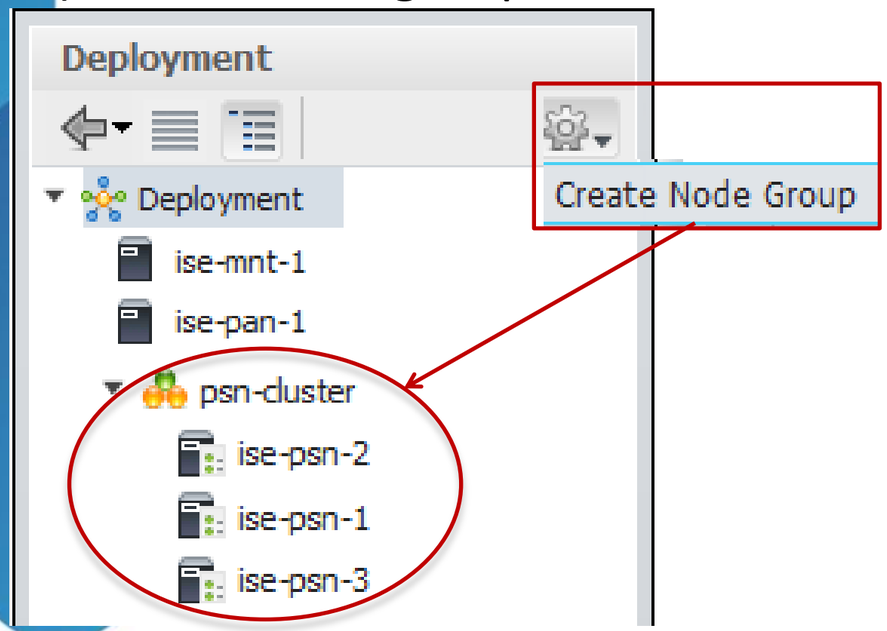


PSN Load Balancing

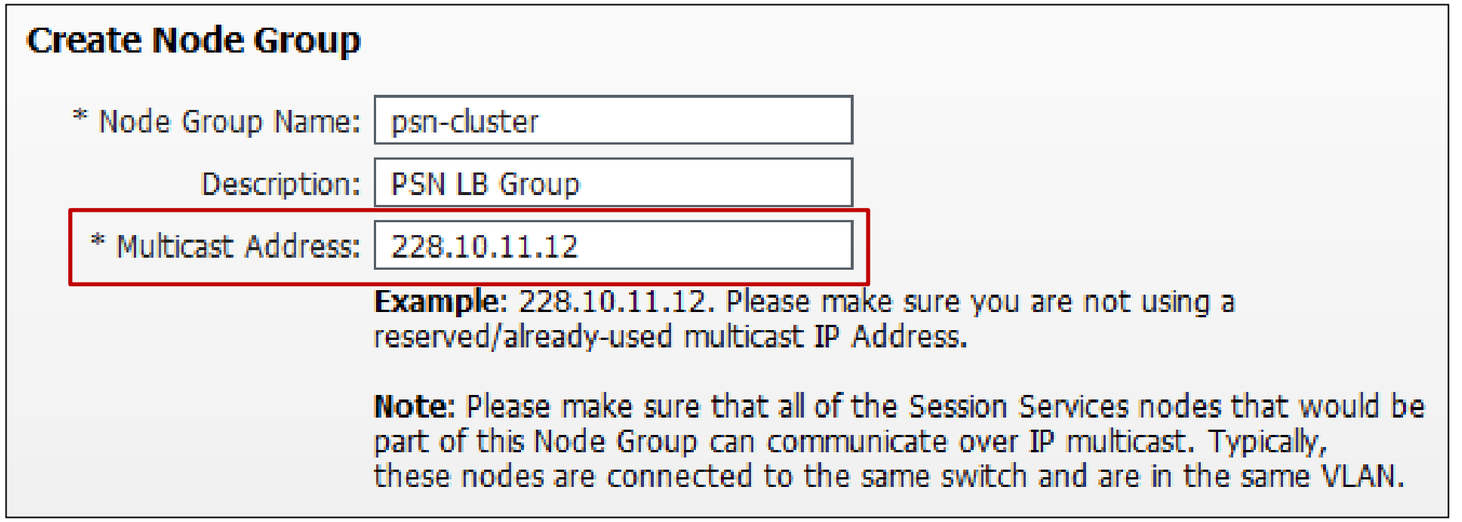
Configure Node Groups

- Administration > System > Deployment

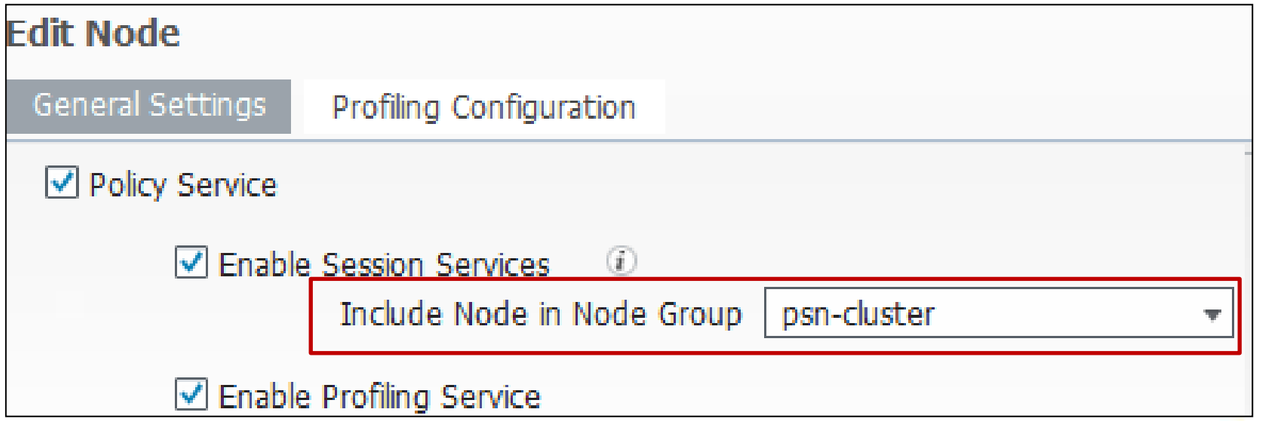
1) Create node group



2) Assign name and available multicast address



3) Add individual PSNs to node group



- Node group members must be L2 adjacent (in same VLAN/subnet)
- Members exchange heartbeats using multicast
- If node fails, group member will send CoA for Posture Pending sessions on failed node.

Load Balancing Preparation

Configure DNS and Certificates

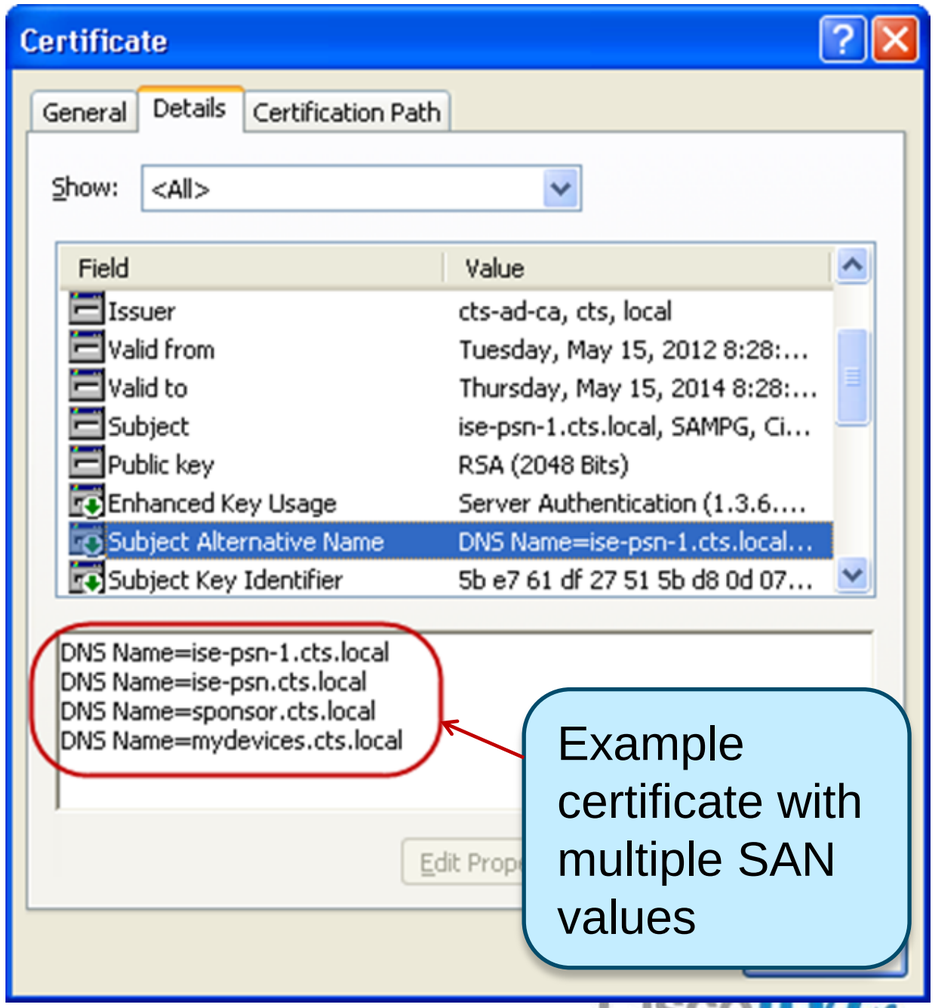
- Configure DNS entry for PSN cluster(s) and assign VIP IP address.

  Example: psn-cluster.company.com

DNS SERVER DOMAIN = COMPANY.COM	
PSN-CLUSTER	10.1.98.10
SPONSOR	10.1.98.10
MYDEVICES	10.1.98.10
ISE-PSN-1	10.1.99.5
ISE-PSN-2	10.1.99.6
ISE-PSN-3	10.1.99.7

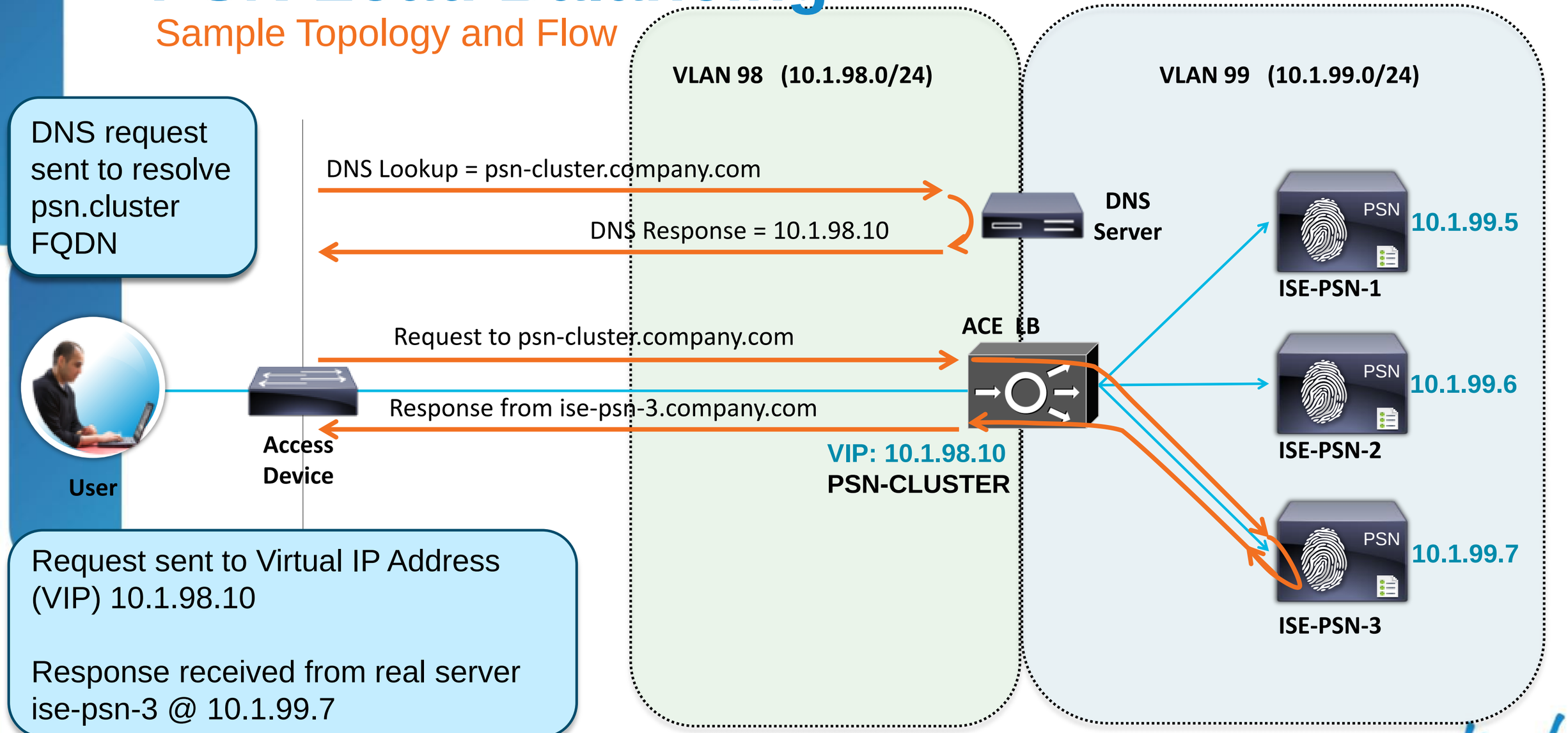
- Configure ISE PSN server certs with Subject Alternative Name configured for other FQDNs to be used by LB VIP.

  Example: ise-psn-1.company.com
  psn-cluster.company.com
  sponsor.company.com
  guest.company.com



PSN Load Balancing

Sample Topology and Flow



HA for Policy Services using Node Groups

Load-Balanced PSN Cluster

- **RADIUS Authentication and Accounting**

  Packets sent to LB virtual IP are load-balanced to real PSN based on configured algorithm.

  – Cisco ACE supports sticky based on source IP, Framed-IP-Address, and Calling-Station-ID to ensure same Policy Service node services RADIUS requests from same endpoint.

CN

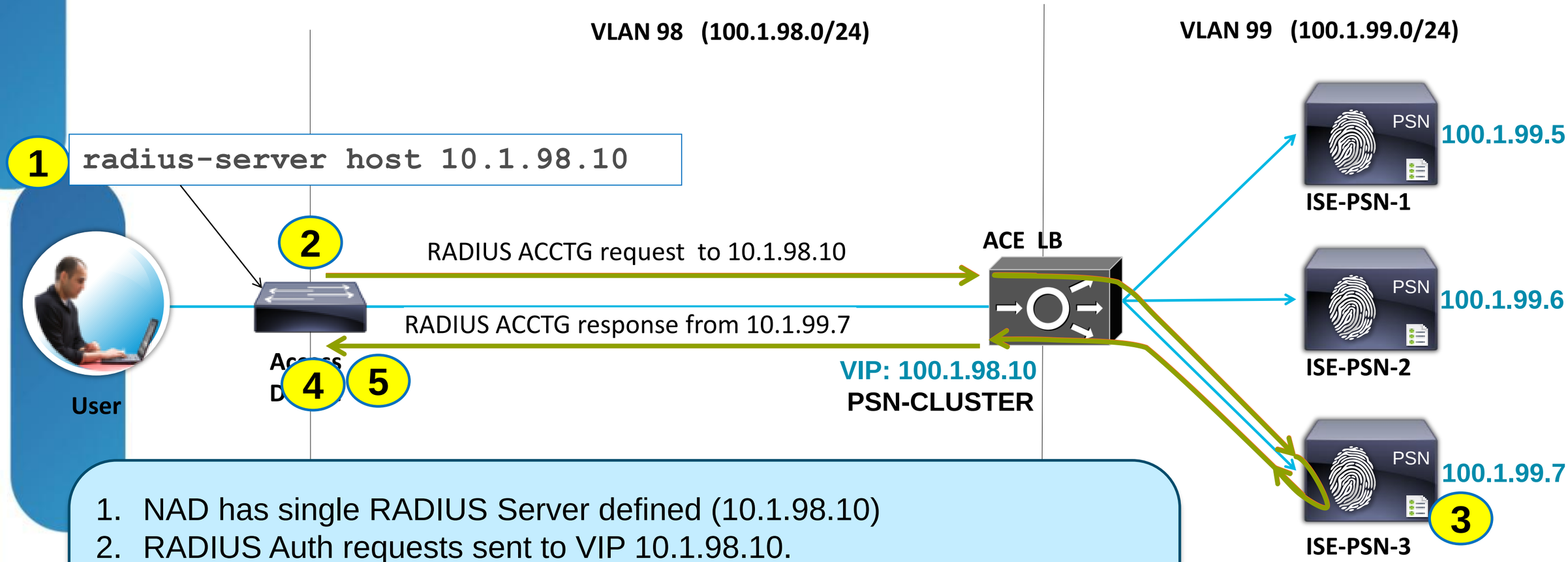
- **Direct HTTP/S Services: Local WebAuth (LWA) / Sponsor Portal / MyDevices Portal**

  Single web portal domain name should resolve to LB virtual IP for http/s load balancing.

  – ACE sticky options can help ensure that successive RADIUS request load balanced to same PSN that served local web authentication

Load Balancing RADIUS

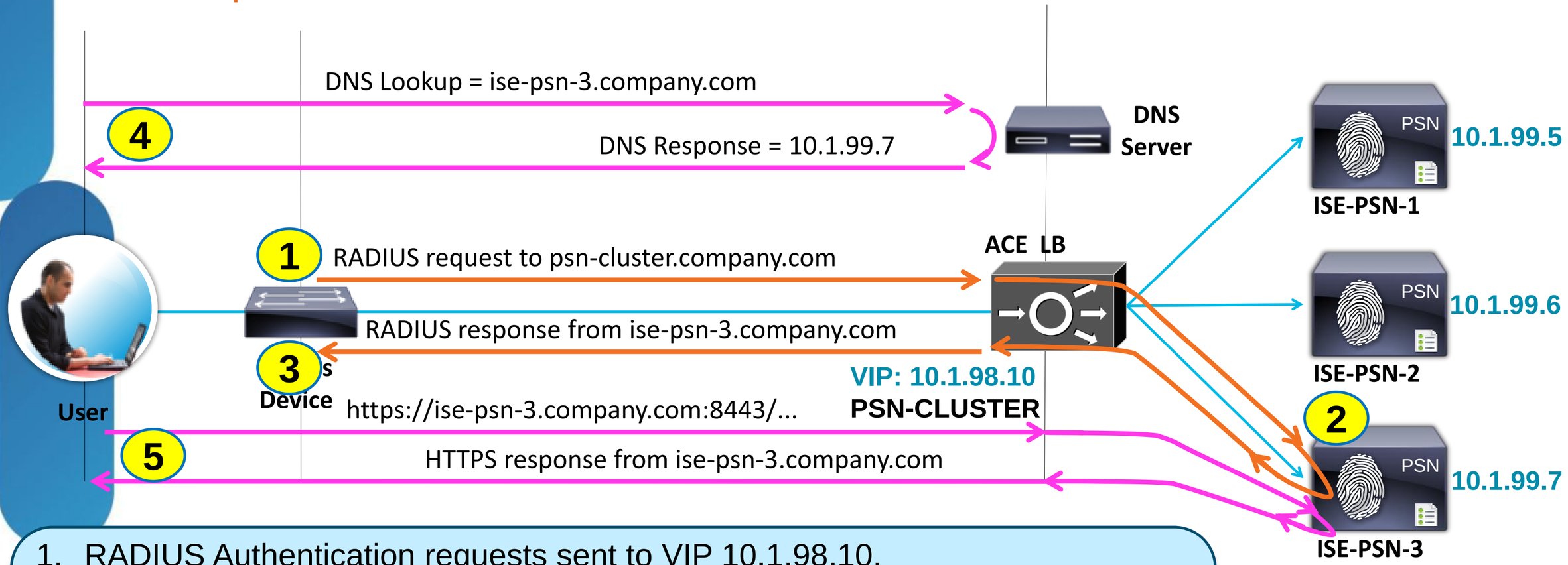
Sample Flow



1. NAD has single RADIUS Server defined (10.1.98.10)
2. RADIUS Auth requests sent to VIP 10.1.98.10.
3. Requests for same endpoint load balanced to same PSN via sticky based on RADIUS Calling-Station-ID and Framed-IP-Address
4. RADIUS Response received from real server ise-psn-3 @ 10.1.99.7
5. RADIUS Accounting sent to/from same PSN based on sticky

Load Balancing with URL-Redirection

Sample Flow



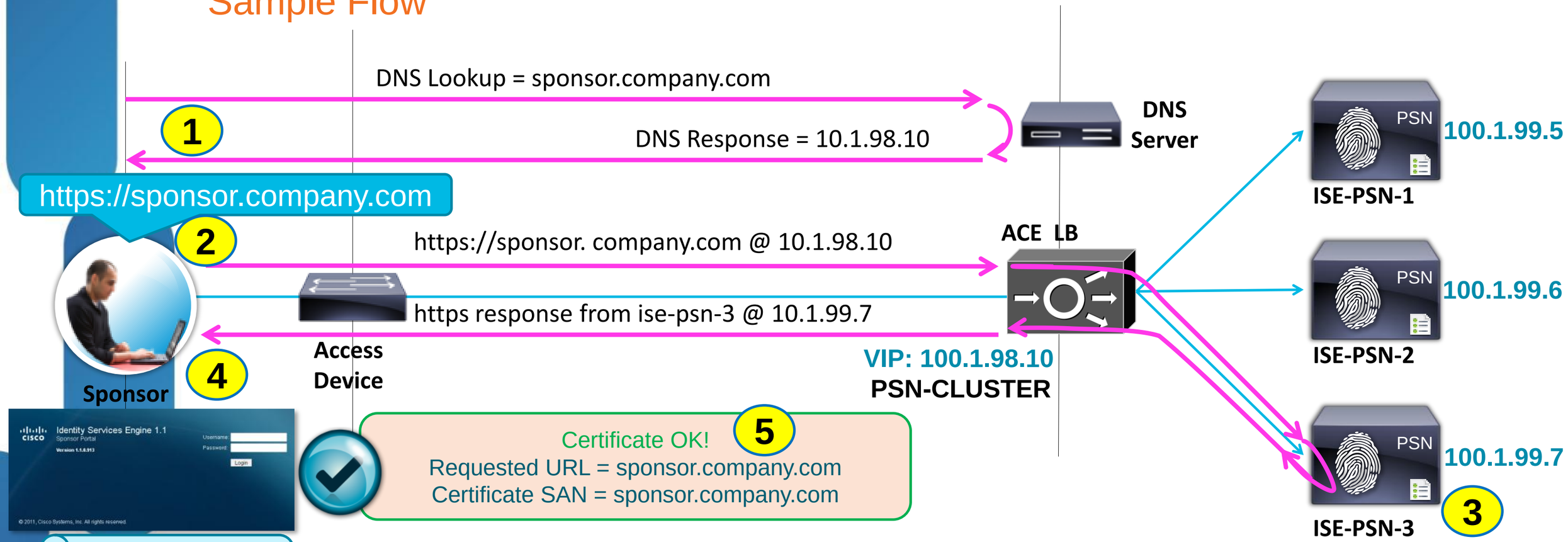
1. RADIUS Authentication requests sent to VIP 10.1.98.10.
2. Requests for same endpoint load balanced to same PSN via RADIUS sticky.
3. RADIUS Authorisation received from ise-psn-3 @ 10.1.99.7 with URL Redirect to https://ise-psn-3.company.com:8443/...
4. Client browser redirected and resolves FQDN in URL to real server address.
5. User sends web request directly to same PSN that serviced RADIUS request.

ISE Certificate

Subject CN =
ise-psn-3.cts.local

Load Balancing Non-Redirected Web Services

Sample Flow



ISE Certificate

Subject = ise-psn-3.cts.local

SAN= ise-psn-3.cts.local sponsor.cts.local

1. Browser resolves sponsor.company.com to VIP @ 10.1.98.10
2. Web request sent to https://sponsor.company.com @ 10.1.98.10
3. ACE load balances request to PSN based on IP or HTTP sticky
4. HTTPS response received from ise-psn-3 @ 10.1.99.7
5. Certificate SAN includes FQDN for both sponsor and ise-psn-3.

Profiling Services Using Load Balancers

Which PSN Services Processes Profile Data?

- **Profiling Probes**
  The following profile data can be load balanced to PSN VIP but may not be processed by same PSN that terminated RADIUS:

  DHCP IP Helper to DHCP probe

  NetFlow export to NetFlow Probe

  SNMP Traps

  Option to leverage Anycast to reduce log targets and facilitate HA

- **SNMP Query Probe (triggered)**
  PSNs configured to send SNMP Queries will send query to NAD that sent RADIUS or SNMP Trap which triggered query. Therefore, SNMP Query data processed by same PSN that terminated RADIUS request for endpoint.

- **SNMP Query Probe (polled)**
  Not impacted by load balancing, although possible that PSN performing polled query is not same PSN that terminates RADIUS for newly discovered endpoints. PSN will sync new endpoint data with Admin. Since poll typically conducted at longer intervals, this should not impact more real-time profiling of endpoints.

Profiling Services Using Load Balancers (Cont.)

Which PSN Services Processes Profile Data?

- **DNS Probe**
  Submitted by same PSN which obtains IP data for endpoint. Typically the same PSN that processes RADIUS, DHCP, or SNMP Query Probe data.
- **NMAP Probe**
  Submitted by same PSN which obtains data which matches profile rule condition.
- **HTTP (via URL redirect)**
  URL redirect will point to PSN that terminates RADIUS auth so HTTP data will be parsed by same PSN.

ACE Health Monitoring Probes

ISE Live Log Activity "Noise"

- No support today for negative filter (!=probe)

- ISE 1.2 will automatically filter out non-confo
  like NAS-Port info) including RADIUS secret
- Additional report filtering forthcoming.

Identity	Server	Network Device	Authorization Profiles
radprobe	ise-psn-3	ace4710	RADIUS_Probes
radprobe	ise-psn-2	ace4710	RADIUS_Probes
radprobe	ise-psn-1	ace4710	RADIUS_Probes
radprobe	ise-psn-3	ace4710	RADIUS_Probes
radprobe	ise-psn-2	ace4710	RADIUS_Probes
radprobe	ise-psn-1	ace4710	RADIUS_Probes
radprobe	ise-psn-3	ace4710	RADIUS_Probes
radprobe	ise-psn-2	ace4710	RADIUS_Probes
radprobe	ise-psn-1	ace4710	RADIUS_Probes
radtest	ise-psn-1	cat3750x	RADIUS_Probes
radprobe	ise-psn-3	ace4710	RADIUS_Probes
radprobe	ise-psn-2	ace4710	RADIUS_Probes
radprobe	ise-psn-1	ace4710	RADIUS_Probes
radprobe	ise-psn-3	ace4710	RADIUS_Probes

ISE and Load Balancers

General Guidelines

- No Source NAT:

  Each PSN must be reachable by the PAN / MNT directly, without having to go through NAT (Routed mode LB, not NAT).

  Each PSN must also be reachable directly from the client network for redirections (CWA, Posture, etc…)

- Perform sticky (aka: persistence) based on Calling-Station-ID and Framed-IP-address

  Session-ID is recommended if load balancer is capable (ACE is not).

- VIP for PSNs gets listed as the RADIUS server on each NAD for all RADIUS AAA.
- Each PSN gets listed individually in the NAD CoA list by real IP address (not VIP).

  If ”Server NAT" the PSN-initiated CoA traffic, then can list single VIP in NAD CoA list.

- Load Balancers get listed as NADs in ISE so their test authentications may be answered.
- ISE uses the Layer 3 address to identify the NAD, not the NAS-IP-Address in the RADIUS packet. This is a primary reason to avoid Source NAT (SNAT) for traffic sent to VIP.

ISE and Load Balancers

Why Source NAT Fails

- Network Access Device (NAD) will be LB, not source NAD

  With SNAT, NAD = LB

  CoA sent to wrong IP address

Network Device	Server	Authorization Pr...	Identity Group
ace4710	ise-psn-2		
ace4710	ise-psn-3	Central_Web_Auth	Profiled:Workstatio...
ace4710	ise-psn-1	Central_Web_Auth	Profiled
ace4710	ise-psn-3	Central_Web_Auth	Profiled:Workstatio...
ace4710	ise-psn-1	Cisco_IP_Phones	Profiled:Cisco-IP-Ph...
ace4710	ise-psn-2	Cisco_IP_Phones	Profiled:Cisco-IP-Ph...
ace4710	ise-psn-2	Employee,SGT_Emp..	RegisteredDevices
ace4710	ise-psn-3	Posture_Remediation	Profiled:Workstatio...
ace4710	ise-psn-3	RADIUS_Probes	

Authentication Details

Logged At:	October 10,2012 10:15:59.418 AM
Occurred At:	October 10,2012 10:15:59.416 AM
Server:	ise-psn-2
Authentication Method:	dot1x
EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	PEAP
Username:	CTS\employee1
RADIUS Username :	CTS\employee1
Calling Station ID:	00:50:56:A0:0B:3A
Framed IP Address:	10.1.10.101
Use Case:	
Network Device:	ace4710
Network Device Groups:	Device Type#All Device Types#Wirec
NAS IP Address:	10.1.50.2
NAS Identifier:	

NAS IP Address is correct, but not currently used for CoA

Live Log Output for Load Balanced Sessions

Real Transactions

1. All RADIUS sent to LB VIP @ 10.1.98.10
2. All phone auth is load balanced from VIP to ise-psn-3 @ 10.1.99.7
3. All PC auth is load balanced to ise-psn-1 @ 10.1.99.5; URL Redirect traffic sent to same PSN.
4. CoA is sent from same PSN that is handling the auth session.
5. dACL download messages are sent from switch itself without a Calling-Station-Id or Framed-IP-Address. Request can be load balanced to any PSN. Not required to pull dACL from same PSN as auth.

Identity	Endpoint ID	IP Address	Server	Authorization Profiles	Identity Group	Posture Status	Event
CTS\employee1	00:50:56:A0:0B:3A	10.1.10.101	ise-psn-1	Employee,SGT_Employee	Profiled:Workstation:Micr...	Compliant	Authentication succeeded
			ise-psn-1			Compliant	Dynamic Authorization su...
#ACSACL#-IP-POSTU			ise-psn-3				DACL Download Succeeded
CTS\employee1	00:50:56:A0:0B:3A	10.1.10.101	ise-psn-1	Posture_Remediation	Profiled:Workstation:Micr...	Pending	Authentication succeeded
host/win7-pc.cts.loca	00:50:56:A0:0B:3A	10.1.10.101	ise-psn-1	AD_Login	Profiled:Workstation:Micr...	NotApplicable	Authentication succeeded
#ACSACL#-IP-AD_LC			ise-psn-1				DACL Download Succeeded
host/win7-pc.cts.loca	00:50:56:A0:0B:3A	10.1.10.101	ise-psn-1	AD_Login	Profiled:Workstation:Micr...	NotApplicable	Authentication succeeded
00:30:94:C4:52:8A	00:30:94:C4:52:8A	10.1.13.100	ise-psn-3	Cisco_IP_Phones	Profiled:Cisco-IP-Phone	NotApplicable	Authentication succeeded

Live Log Output for Load Balanced Sessions

Synthetic Transactions

- Batch of test authentications generated from Catalyst switch:

```
# test aaa group radius radtest cisco123 new-code count 100
```

All RADIUS sent to LB VIP @ 10.1.98.10

Requests evenly distributed across real servers:

- ise-psn-1
- ise-psn-2
- ise-psn-3

Time	Status	Details	Identity	Server	Network Device	Authorization Profiles
Oct 13,12 03:50:28.368 PM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.367 PM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.366 PM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.364 PM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.363 PM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.322 PM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.310 PM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.309 PM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.293 PM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 13,12 03:50:28.292 PM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 13,12 03:50:27.641 PM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes

ISE and Load Balancers

Failure Scenarios

- The VIP is the RADIUS Server, so if the entire VIP is down, then the NAD should fail over to the secondary Data Centre VIP (listed as the secondary RADIUS server on the NAD).
- Probes on the load balancers should ensure that RADIUS is responding as well as HTTPS, at a minimum.

  Validate that RADIUS responds, not just that UDP/1812 & UDP/1813 are open

  Validate that HTTPS responds, not just that TCP/8443 is open
- Upon detection of failed node using probes (or node taken out of service), new requests will be serviced by remaining nodes→ Minimum N+1 redundancy recommended for node groups.
- Use node groups with the L2-adjacent PSNs behind the VIP.

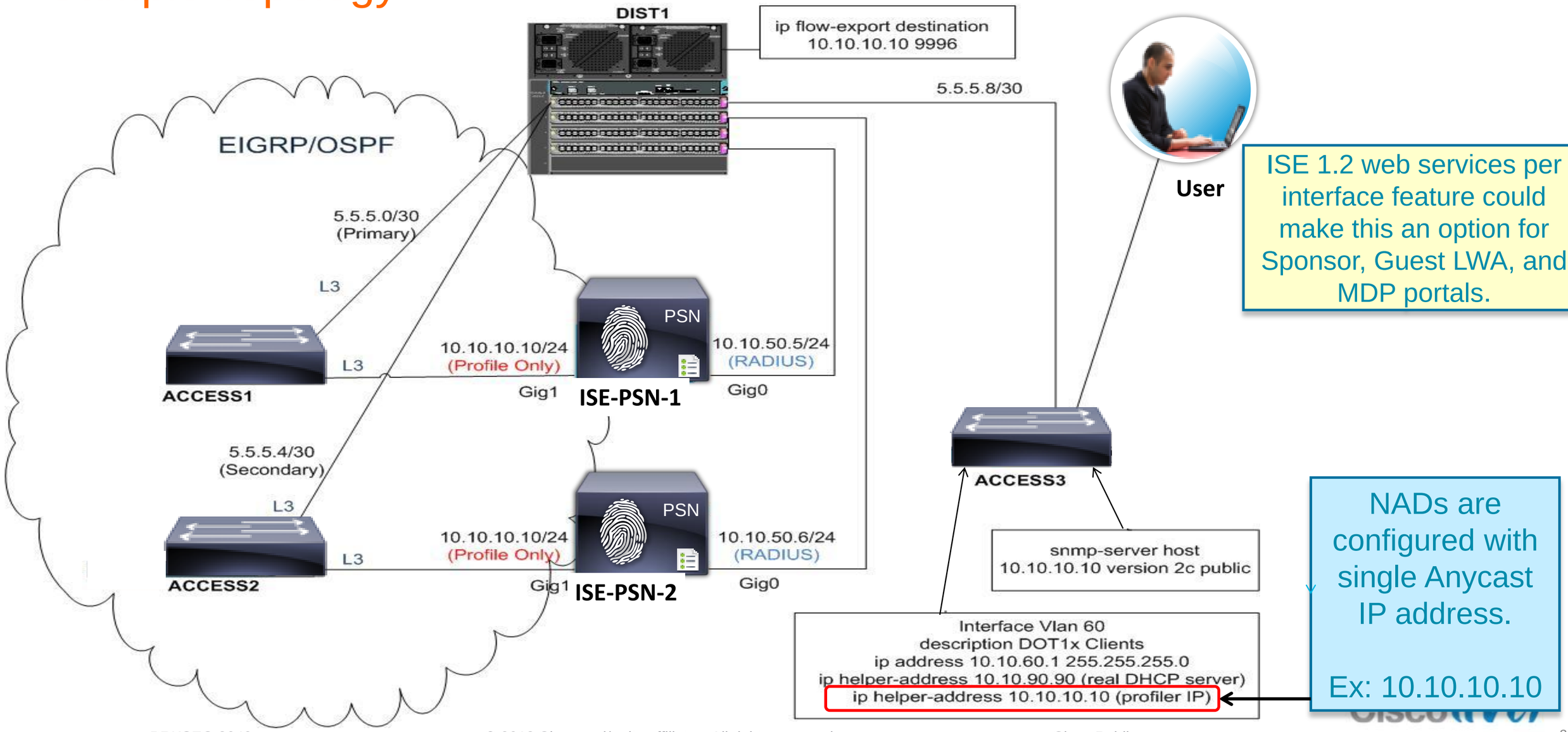
  If node group member fails, then another of the node-group members will issue a CoA-reauth, forcing the sessions to begin again.

  Note: The use of node groups does not require load balancers, but nodes still need to meet L2 adjacency and multicast requirements.

How can my company get HA and scalability without load balancers?

Using Anycast for Profiling Redundancy

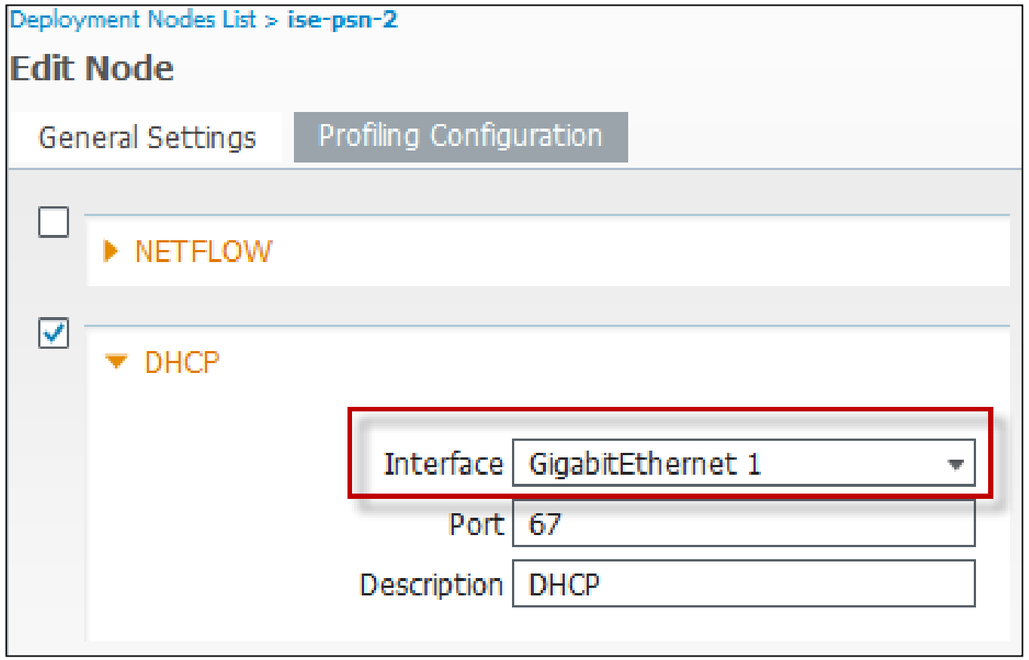
Sample Topology



ISE Configuration for Anycast

On each PSN that will participate in Anycast…

- Configure PSN probes to profile DHCP (IP Helper), SNMP Traps, or NetFlow on dedicated interface
- From CLI, configure dedicated interface with same IP address on each PSN node.



ISE-PSN-1 Example:

```
#ise-psn-1/admin# config t
#ise-psn-1/admin (config)# int GigabitEthernet1
#ise-psn-1/admin (config-GigabitEthernet)# ip address 10.10.10.10 255.255.255.0
```

ISE-PSN-2 Example:

```
#ise-psn-2/admin# config t
#ise-psn-2/admin (config)# int GigabitEthernet1
#ise-psn-2/admin (config-GigabitEthernet)# ip address 10.10.10.10 255.255.255.0
```

Routing Configuration for Anycast

Sample Configuration

- Access Switch 1

```
interface gigabitEthernet 1/0/23
no switchport
ip address 10.10.10.50 255.255.255.0
!
router eigrp 100
no auto-summary
redistribute connected route-map CONNECTED-2-EIGRP
!
route-map CONNECTED-2-EIGRP permit 10
match ip address prefix-list 5
set metric 1000 100 255 1 1500
set metric-type internal
!
route-map CONNECTED-2-EIGRP permit 20
ip prefix-list 5 seq 5 permit 10.10.10.0/24
```

Both switches advertise same network used for profiling but different metrics

- Access Switch 2

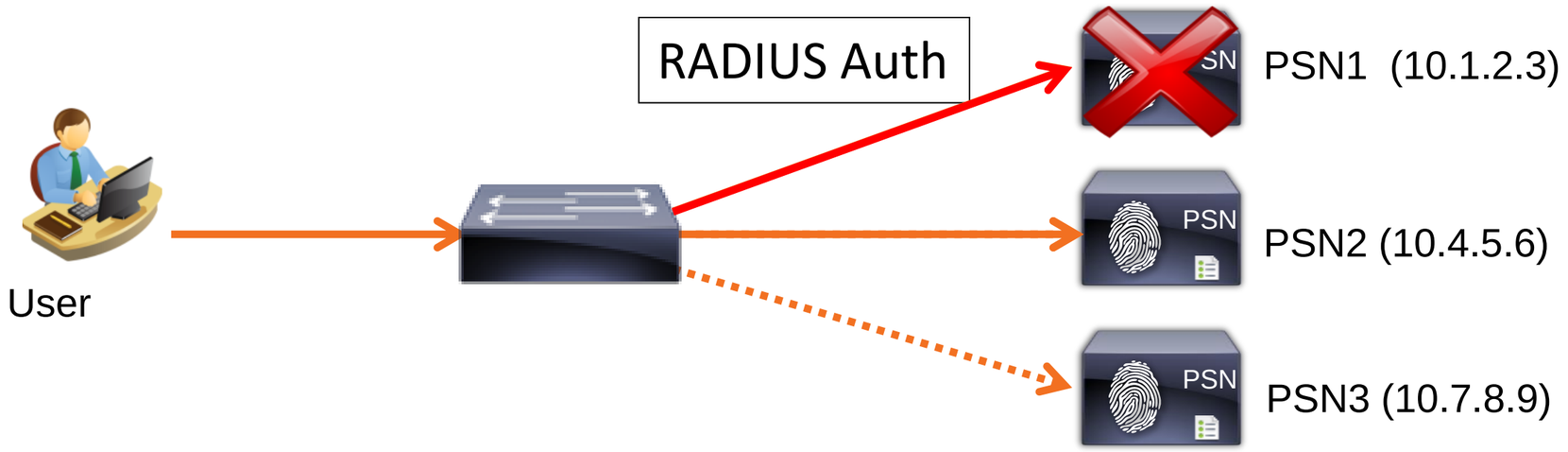
```
interface gigabitEthernet 1/0/23
no switchport
ip address 10.10.10.51 255.255.255.0
!
router eigrp 100
no auto-summary
redistribute connected route-map CONNECTED-2-EIGRP
!
route-map CONNECTED-2-EIGRP permit 10
match ip address prefix-list 5
set metric 500 50 255 1 1500
set metric-type external
!
route-map CONNECTED-2-EIGRP permit 20
ip prefix-list 5 seq 5 permit 10.10.10.0/24
```

less preferred route

NAD-Based RADIUS Server Redundancy (IOS)

Multiple RADIUS Servers Defined in Access Device

- Configure Access Devices with multiple RADIUS Servers.
- Fallback to secondary servers if primary fails

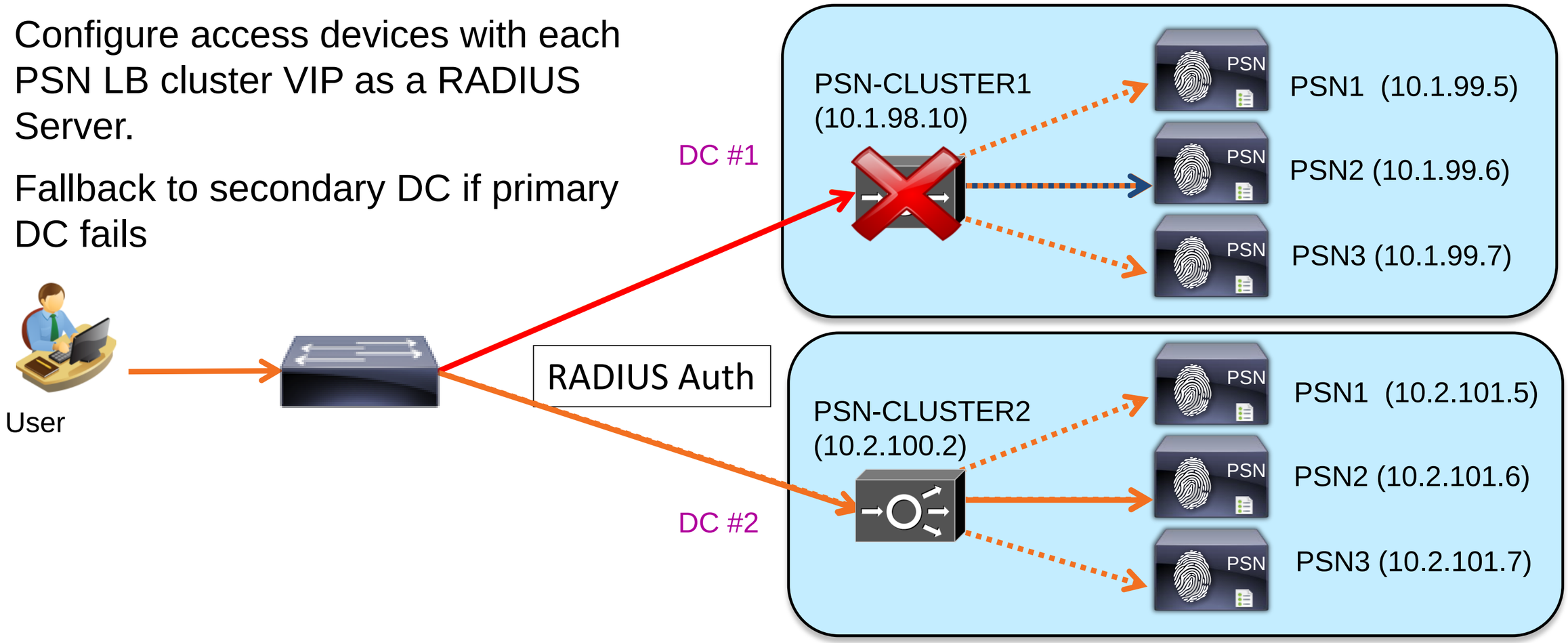



```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813
```

NAD-Based Redundancy

Dual Data Centre w/LB Example

- Configure access devices with each PSN LB cluster VIP as a RADIUS Server.
- Fallback to secondary DC if primary DC fails

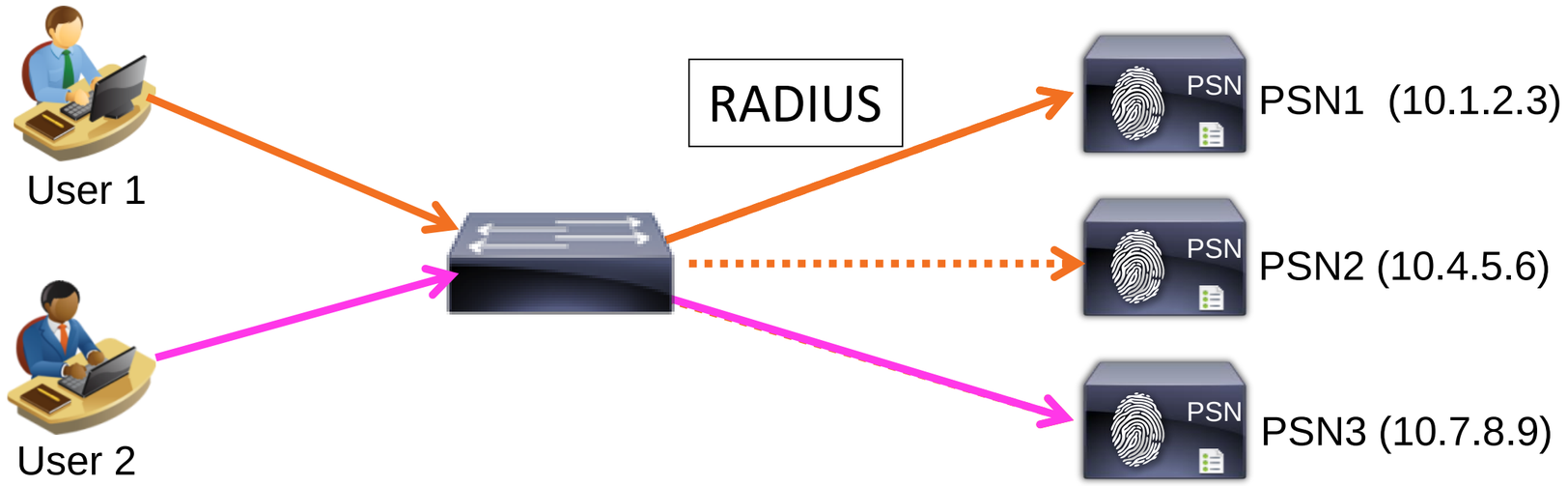



```
radius-server host 10.1.98.10 auth-port 1812 acct-port 1813
radius-server host 10.2.100.2 auth-port 1812 acct-port 1813
```

IOS-Based RADIUS Server Load Balancing

Switch Dynamically Distributes Requests to Multiple RADIUS Servers

- RADIUS LB feature distributes batches of AAA transactions to servers within a group.
- Each batch assigned to server with least number of outstanding transactions.



NAD controls the load distribution of AAA requests to all PSNs in RADIUS group without dedicated LB.

```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813
radius-server load-balance method least-outstanding batch-size 5
```

IOS-Based RADIUS Server Load Balancing

Sample Live Log

- Use **test aaa group** command from IOS CLI
  to test RADIUS auth requests

Reasonable load distribution across all PSNs

Example shows 3 PSNs in RADIUS group

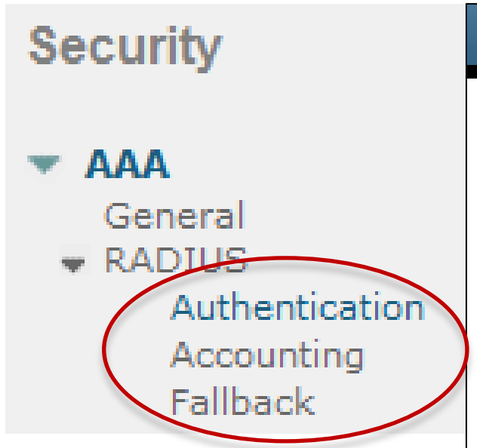
Time	Status	Details	Identity	Server	Network Device	Authorization Profiles
					3750	
Oct 11,12 12:50:08.040 AM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.038 AM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.036 AM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.026 AM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.009 AM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
0:08.009 AM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
0:07.091 AM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
0:07.089 AM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
0:07.089 AM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
0:07.088 AM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
0:07.084 AM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.050 AM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.035 AM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.033 AM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes

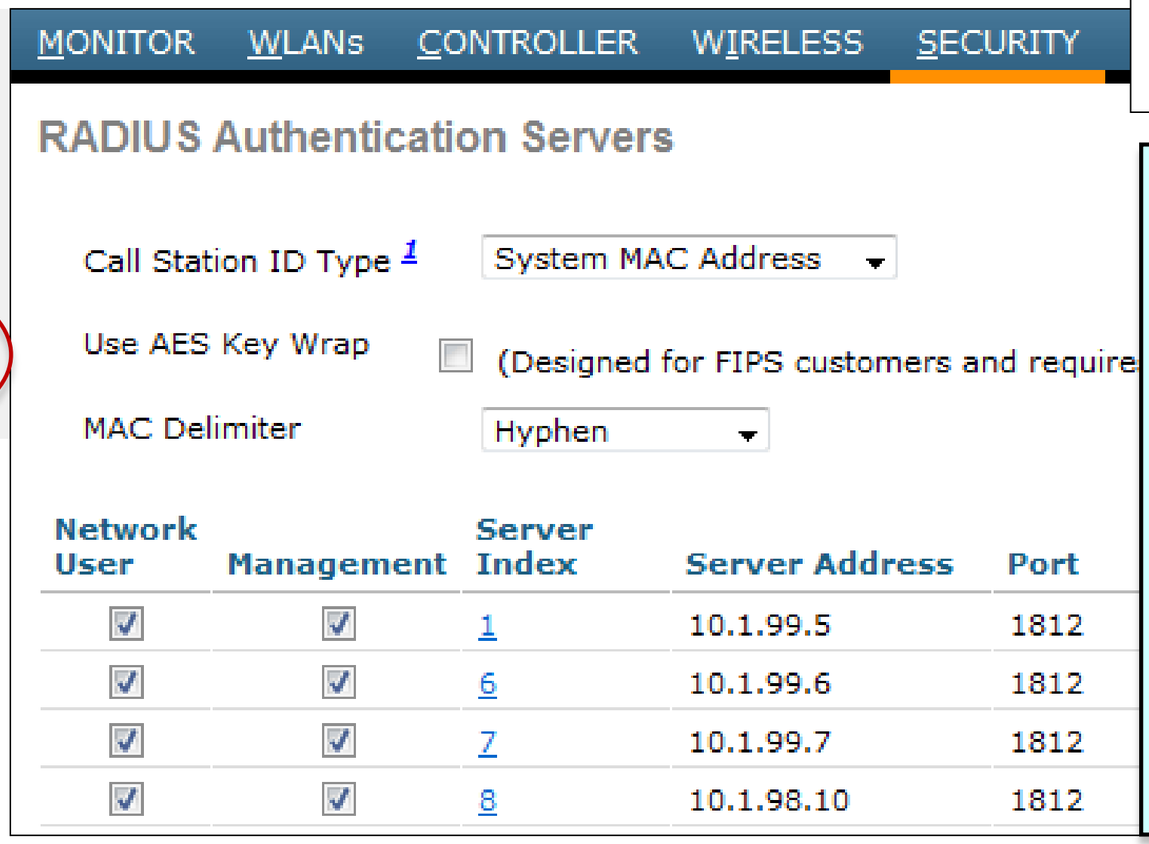
```
cat3750x# test aaa group radius radtest cisco123 new users 4 count 50
AAA/SG/TEST: Sending 50 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
```

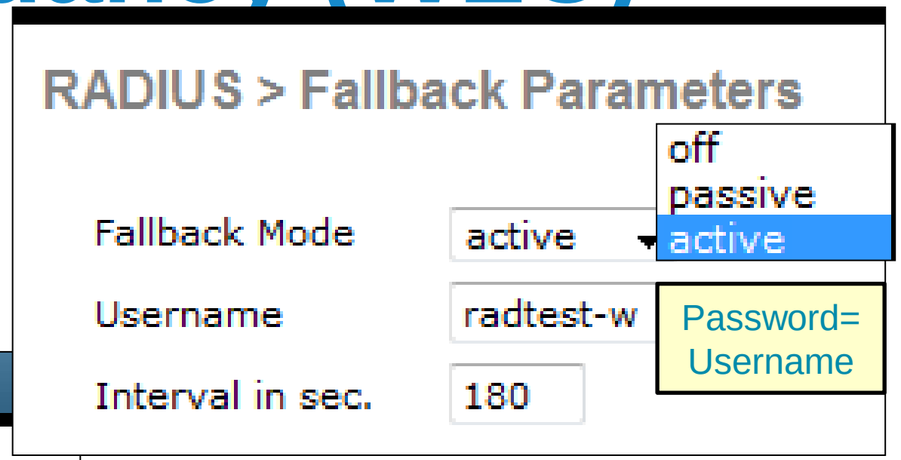
NAD-Based RADIUS Redundancy (WLC)

Wireless LAN Controller

- Multiple RADIUS Auth & Accounting Server Definitions
- RADIUS Fallback options: **none, passive,** or **active**







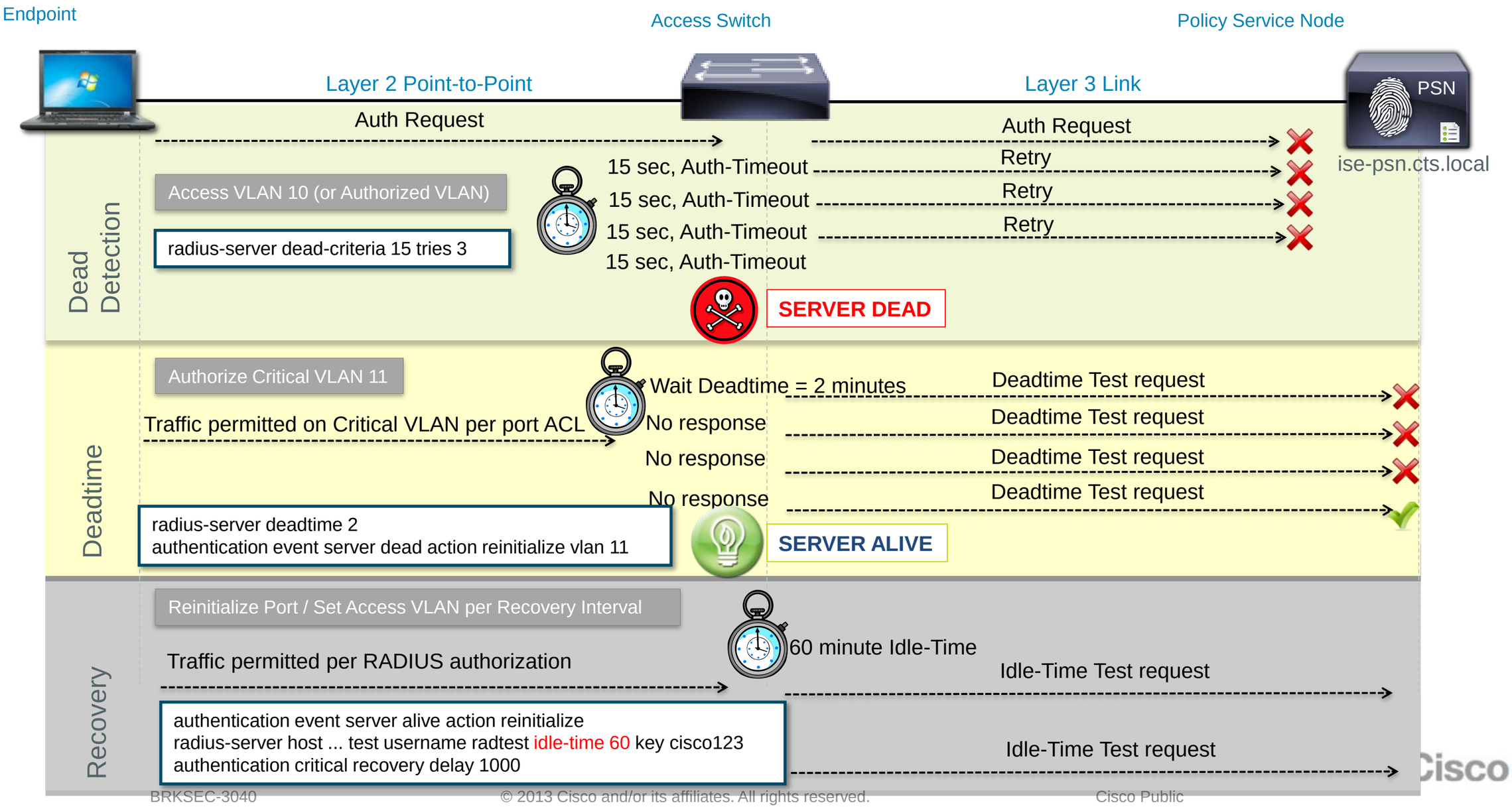
None = Continue exhaustively through list; never preempt to preferred server (entry with lowest index)

Passive = Quarantine failed RADIUS server for interval then return to active list w/o validation; always preempt.

Active = Mark failed server dead then actively probe status per interval w/username until succeed before return to list; always preempt.

http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a008098987e.shtml

NAD Fallback and Recovery Sequence

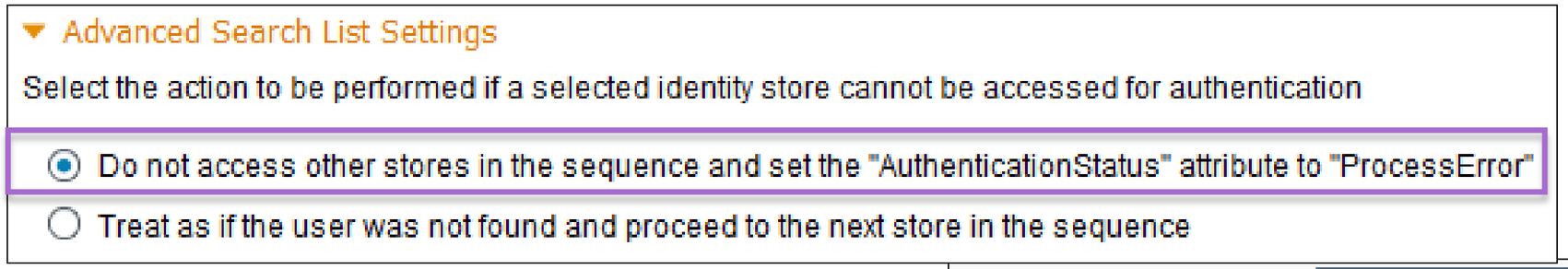


RADIUS Test User Account

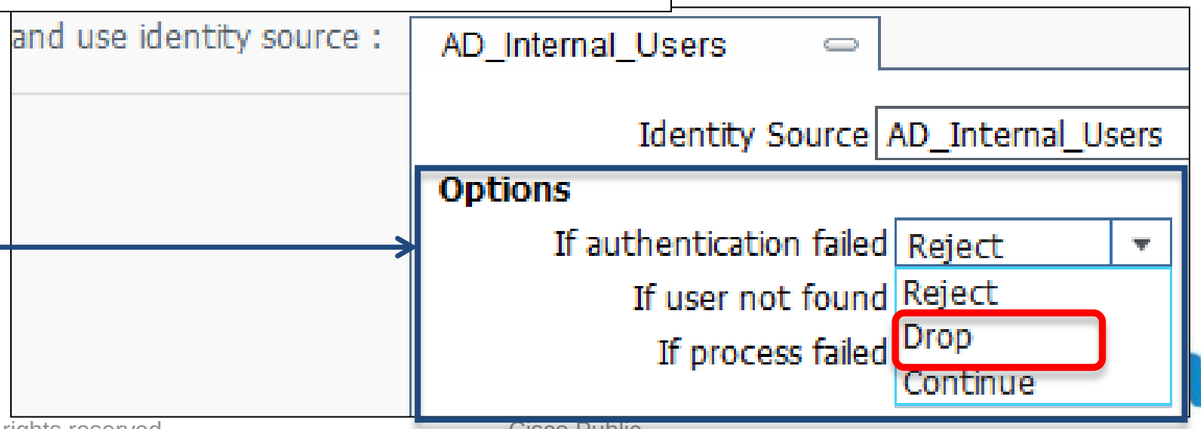
Which User Account Should Be Used?

- Does NAD uniformly treat Auth Fail and Success the same for detecting server health?
  IOS treats them the same; ACE RADIUS probe treats Auth Fail as server down.
- If goal is to validate backend ID store, then Auth Fail may not detect external ID store failure.
  Optionally drop failed authentication requests.

Identity Server Sequence > Advanced Settings:



Authentication Policy > ID Source Custom processing based on authentication results



RADIUS Test User Account

Access-Accept or Access-Reject?

- If valid user account used, how prevent unauthorised access using probe account?
  If Auth Fail treated as probe failure, then need valid account in ISE db or external store.
  - Match auth from probes to specific source/NDG, Service Type, or User Name.
  - Allow AuthN to succeed, but return AuthZ that denies access.

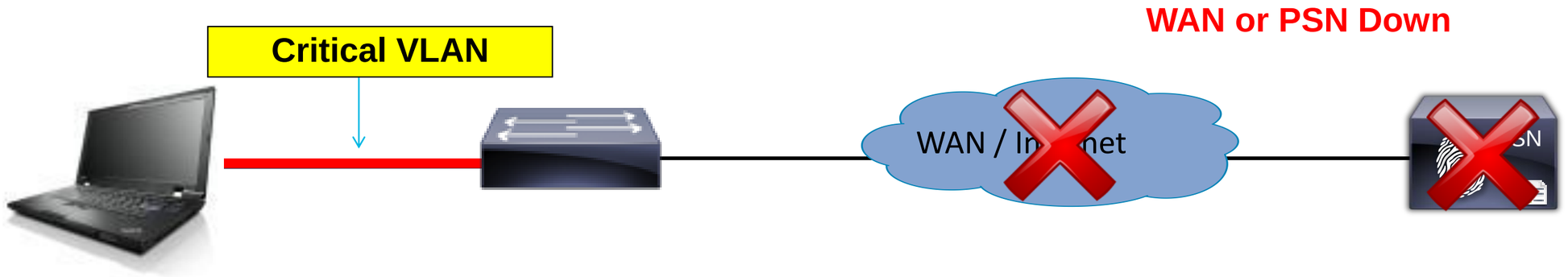
Rule Name	Conditions (identity groups and other conditions)	Permissions
RADIUS Probe	if (Network Access:NetworkDeviceName EQUALS ace4710 OR Radius:User-Name EQUALS radtest)	then RADIUS_Probes

Time	Status	Details	Identity	Network Device	Authorization Profiles	Posture Status	Event	Server
Oct 08,12 07:54:25.958 PM	✓		radprobe	ace4710	RADIUS_Probes	NotApplicable	Authentication succeeded	ise-psn-3
Oct 08,12 07:54:18.957 PM	✓		radprobe	ace4710	RADIUS_Probes	No		ise-psn-2
Oct 08,12 07:53:43.628 PM	✓		radtest	cat3750x	RADIUS_Probes	No		ise-psn-2
Oct 08,12 07:53:27.044 PM	✓		radtest	cat3750x	RADIUS_Probes	NotApplicable	Authentication succeeded	ise-psn-1
Oct 08,12 07:53:26.960 PM	✓		radprobe	ace4710	RADIUS_Probes	NotApplicable	Authentication succeeded	ise-psn-1
Oct 08,12 07:53:25.966 PM	✓		radprobe	ace4710	RADIUS_Probes	NotApplicable	Authentication succeeded	ise-psn-3
Oct 08,12 07:53:18.964 PM	✓		radprobe	ace4710	RADIUS_Probes	NotApplicable	Authentication succeeded	ise-psn-2

Access-Accept
dACL = deny ip any any

Inaccessible Authentication Bypass (IAB)

Also Known As "Critical Auth VLAN"



- Switch detects PSN unavailable by one of two methods
  - Periodic probe
  - Failure to respond to AAA request
- Enables port in critical VLAN
- Existing sessions retain authorisation status
- Recovery action can re-initialise port when AAA returns

Critical VLAN can be anything:

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

SGT will be "unknown"

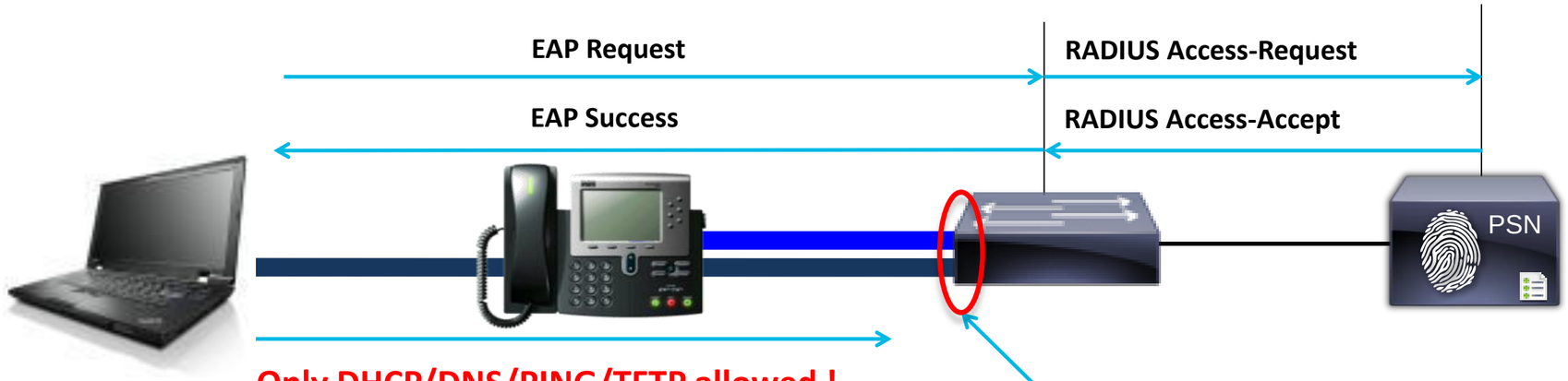
If change VLAN, host may not know to refresh IP!

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

Default Port ACL Issues with No dACL Authorisation

Limited Access If ISE Policy Fails to Return dACL!

- User authentications successful, but authorisation profile does not include dACL to permit access, so endpoint access still restricted by existing port ACL!



Auth Success

Authorisation Profile = Employee

Access Type = Access-Accept

NO dACL!

```
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport voice vlan 13
 ip access-group ACL-DEFAULT in
```

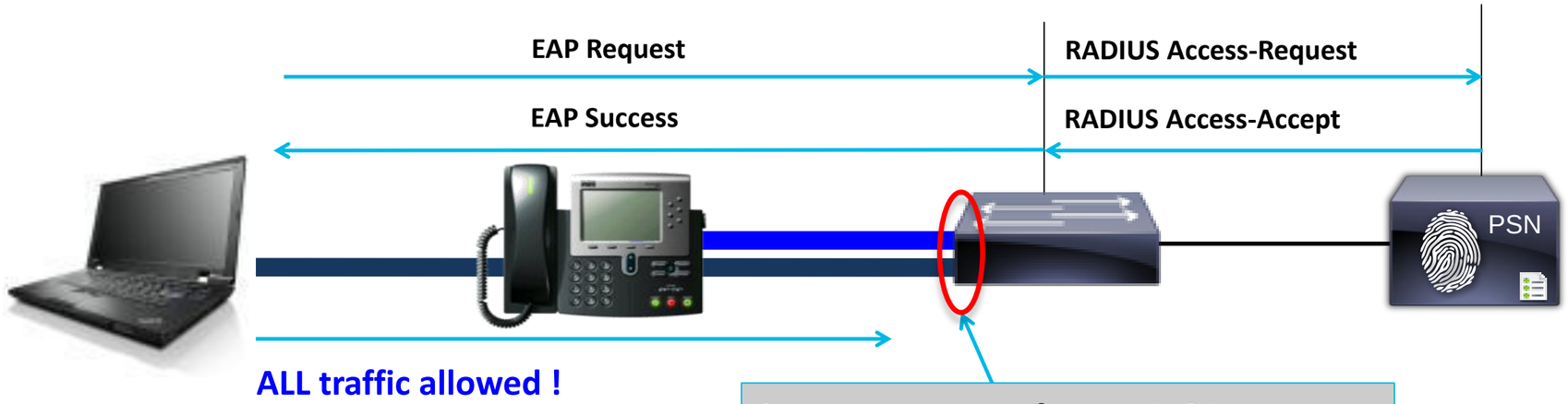
```
ip access-list extended ACL-DEFAULT
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit icmp any any
 permit udp any any eq tftp
```

Protecting Against "No dACL" Authorisation

EPM Access Control

2k/3k: 12.2(55)SE
4k: 12.2(54)G
6k: No support

- If authentication successful and no dACL returned, a **permit ip host any** entry is created for the host. This entry is created only if no ACLs are downloaded from ISE.



Auth Success

Authorisation Profile = Employee

Access Type = Access-Accept

NO dACL!

Insert at top of port ACL:
permit ip any any

epm access control open

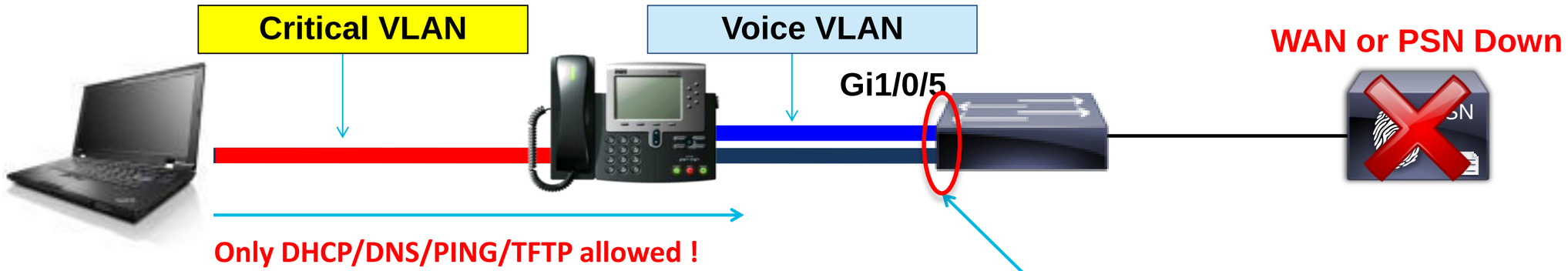
interface GigabitEthernet1/0/2
switchport access **vlan 10**
switchport voice **vlan 13**
ip access-group ACL-DEFAULT in

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

Default Port ACL Issues with Critical VLAN

Limited Access Even After Authorisation to New VLAN!

- Data VLAN reassigned to critical auth VLAN, but new (or reinitialised) 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
```

Critical VLAN w/o Explicit Default Port ACL

Low Impact vs Closed Mode

2k/3k: 12.2(55)SE
4k: 12.2(54)G
6k: No support

- One Solution to dACL + Critical Auth VLAN issue is to simply remove the port ACL!
- Starting in 12.2(55)SE for 2k/3k and 12.2(54)G for 4k, no static port ACL required for dACLs
- Low Impact Mode Use Case:

  Initial access permits all traffic

  Pro: Immediately allows access to critical services for all endpoints including PXE and WoL devices

  Con: Temporary window which allows any unauthenticated endpoint to get full access

- Closed Mode User Case

  No initial access but default authorisation can assign default access policy (typically CWA)

  Pro: No access until port authorised

  Con: Some endpoints may fail due to timing requirements such as PXE or WoL

Using Embedded Event Manager with Critical VLAN

Modify or Remove/Add Static Port ACLs Based on PSN Availability

- EEM available on 3k/4k/6k
- Allows scripted actions to occur based on various conditions and triggers

```
event manager applet default-acl-fallback
 event syslog pattern "%RADIUS-4-RADIUS_DEAD" maxrun 5
 action 1.0 cli command "enable"
 action 1.1 cli command "conf t" pattern "CNTL/Z."
 action 2.0 cli command "ip access-list extended ACL-DEFAULT"
 action 3.0 cli command "1 permit ip any any"
 action 4.0 cli command "end"

event manager applet default-acl-recovery
 event syslog pattern "%RADIUS-4-RADIUS_ALIVE" maxrun 5
 action 1.0 cli command "enable"
 action 1.1 cli command "conf t" pattern "CNTL/Z."
 action 2.0 cli command "ip access-list extended ACL-DEFAULT"
 action 3.0 cli command "no 1 permit ip any any"
 action 4.0 cli command "end"
```

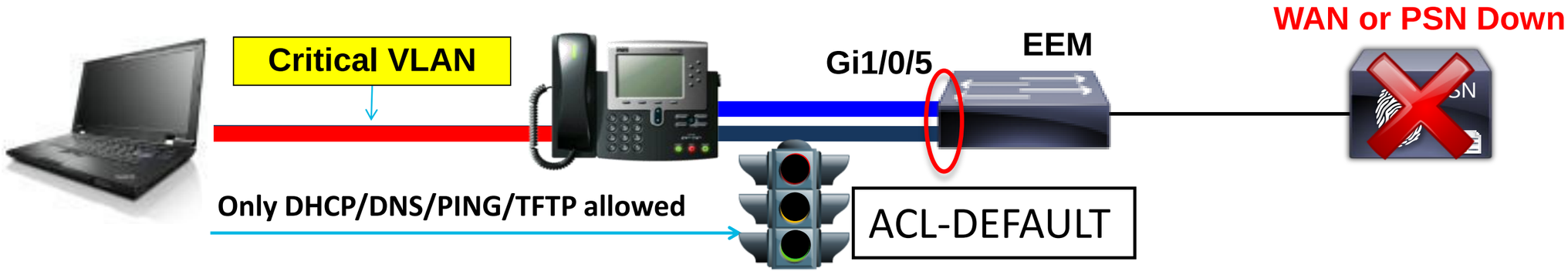
Single RADIUS Server (LB VIP) Example

Multi-server option: %RADIUS-3-ALLDEADSERVER

EEM Example

Remove and Add Port ACL on RADIUS Server Status Syslogs

- Port ACLs block new user connections during Critical Auth



- EEM detects syslog message **`%RADIUS-3-ALLDEADSERVER: Group radius: No active radius servers found`** and *removes* ACL-DEFAULT.

```
event manager applet remove-default-acl
 event syslog pattern "%RADIUS-4-RADIUS_DEAD" maxrun 5
 action 1.0 cli command "enable"
 action 1.1 cli command "conf t" pattern "CNTL/Z."
 action 2.0 cli command "interface range gigabitEthernet 1/0/1 - 24"
 action 3.0 cli command "no ip access-group ACL-DEFAULT in"
 action 4.0 cli command "end"
```

- EEM detects syslog message **`%RADIUS-6-SERVERALIVE: Group radius: Radius server 10.1.98.10:1812,1813 is responding again (previously dead)`** and *adds* ACL-DEFAULT.

```
event manager applet add-default-acl
 event syslog pattern "%RADIUS-4-RADIUS_ALIVE" maxrun 5
 action 1.0 cli command "enable"
 action 1.1 cli command "conf t" pattern "CNTL/Z."
 action 2.0 cli command "interface range gigabitEthernet 1/0/1 - 24"
 action 3.0 cli command "ip access-group ACL-DEFAULT in"
 action 4.0 cli command "end"
```

EEM Example 2

Modify Port ACL Based on Route Tracking

PROGRIZON

EEM Policy Builder:

http://www.progrizon.com/support/pb/pb.php

```
cat6500(config)# track 1 ip route 10.1.98.0 255.255.255.0 reachability

cat6500(config)# event manager applet default-acl-fallback
cat6500(config-applet)# event track 1 state down maxrun 5
cat6500(config-applet)# action 1.0 cli command "enable"
cat6500(config-applet)# action 1.1 cli command "conf t" pattern "CNTL/Z."
cat6500(config-applet)# action 2.0 cli command "ip access-list extended ACL-
DEFAULT"
cat6500(config-applet)# action 3.0 cli command "1 permit ip any any"
cat6500(config-applet)# action 4.0 cli command "end"

cat6500(config)# event manager applet default-acl-recovery
cat6500(config-applet)# event track 1 state up maxrun 5
cat6500(config-applet)# event syslog pattern "%RADIUS-4-RADIUS_ALIVE" maxrun 5
cat6500(config-applet)# action 1.0 cli command "enable"
cat6500(config-applet)# action 1.1 cli command "conf t" pattern "CNTL/Z."
cat6500(config-applet)# action 2.0 cli command "ip access-list extended ACL-
DEFAULT"
cat6500(config-applet)# action 3.0 cli command "no 1 permit ip any any"
cat6500(config-applet)# action 4.0 cli command "end"
```

Bring Your Own……..

Bring Your Own Device (BYOD)
Choose Your Own Device (CYOD)
Bring Your Own App (BYOA)

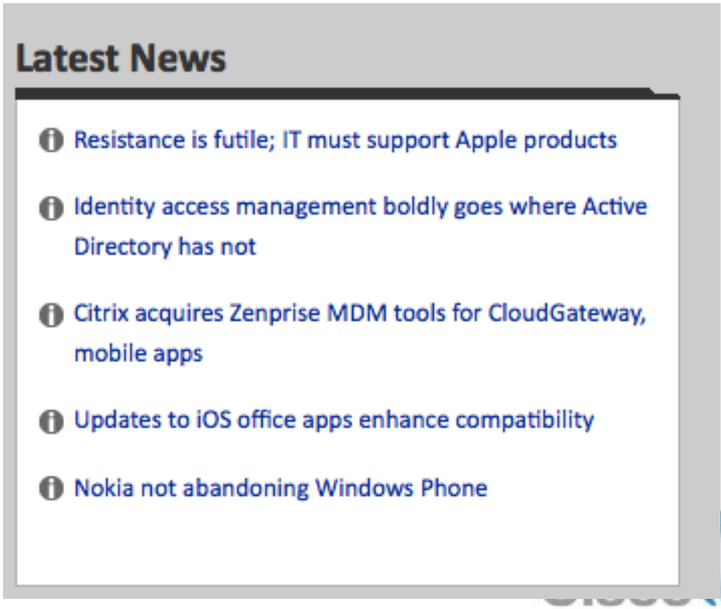
Look back at 2009

Q: Will you Allow Employees to use Personal i-Phones, i-Pads, etc.?

A: Absolutely Not!

- Cisco Responds:

Now, in 2012:



“We're going to demote the PC and the Mac to just be a device. Just like an iPhone, or an iPad, or an iPod Touch. We're going to move the digital hub, the centre of your digital life, into the cloud.”

Steve Jobs, 2011

"Many call this era the post-PC era, but it isn't really about being 'after' the PC, but rather about a new style of personal computing that frees individuals to use computing in fundamentally new ways to improve multiple aspects of their work and personal lives."

Steve Kleynhans,
Gartner Analyst

"We no longer do our computing in a single place and this is creating a lot of problems for businesses."

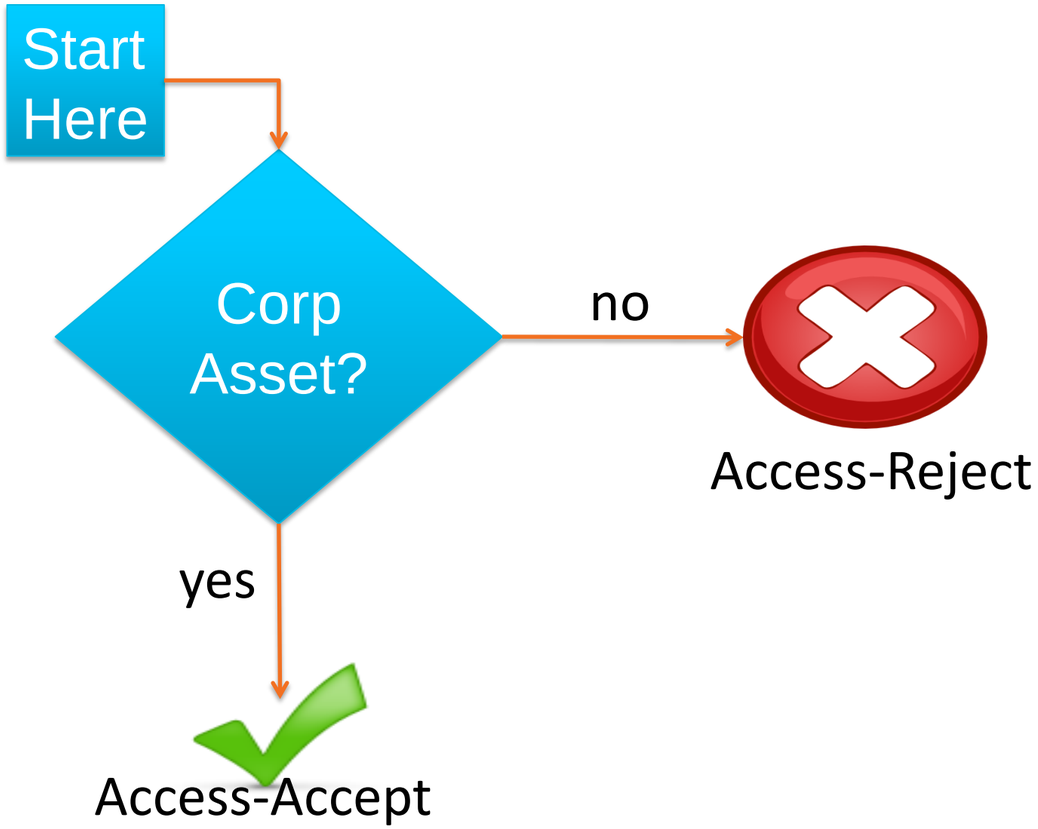
Chris Young VMware, 2010

”I am twice as productive on a MAC than on the Cisco-IT Provisioned ThinkPad that has been weighed down with all the ‘official’ software.”

Aaron Woland, Self Proclaimed Expert on all Things

What Makes a BYOD Policy?

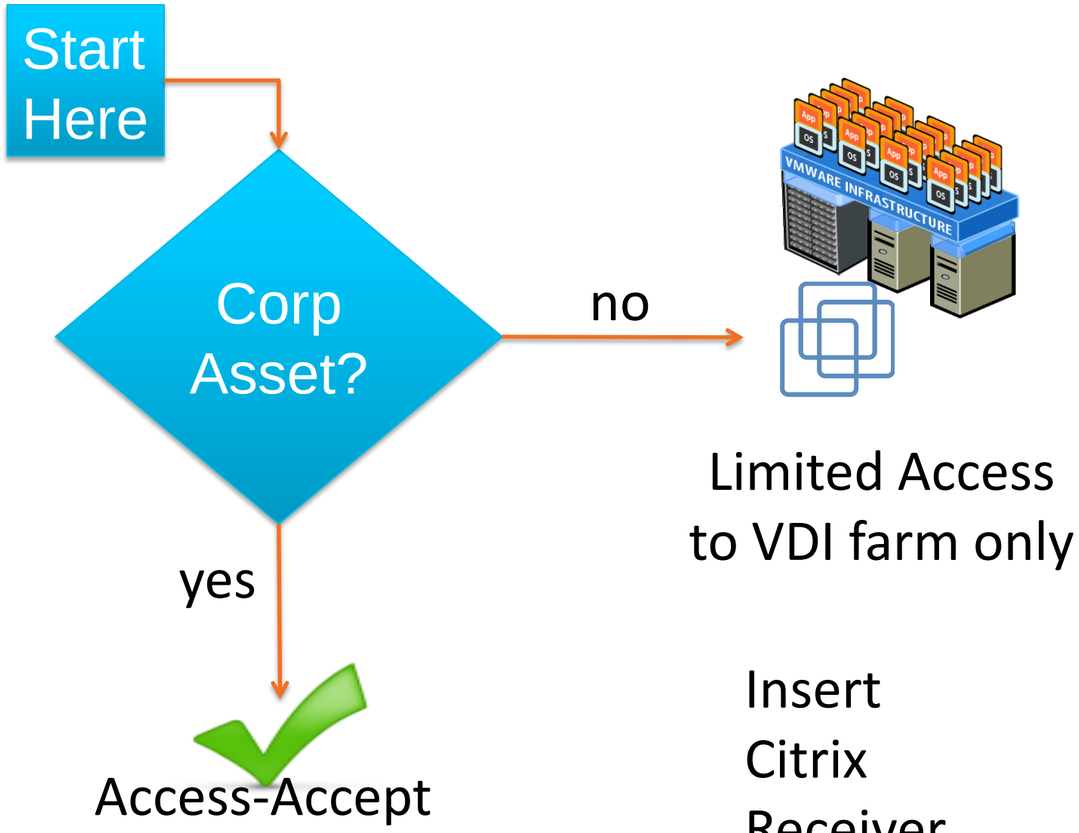
MachineAuth Approach…



- Only corporate devices may access my network, period.
  - Use EAP-TLS with AD-issued non-exportable machine certificates.
  - That is our “BYOD” Policy.
- Not too common anymore.

What Makes a BYOD policy?

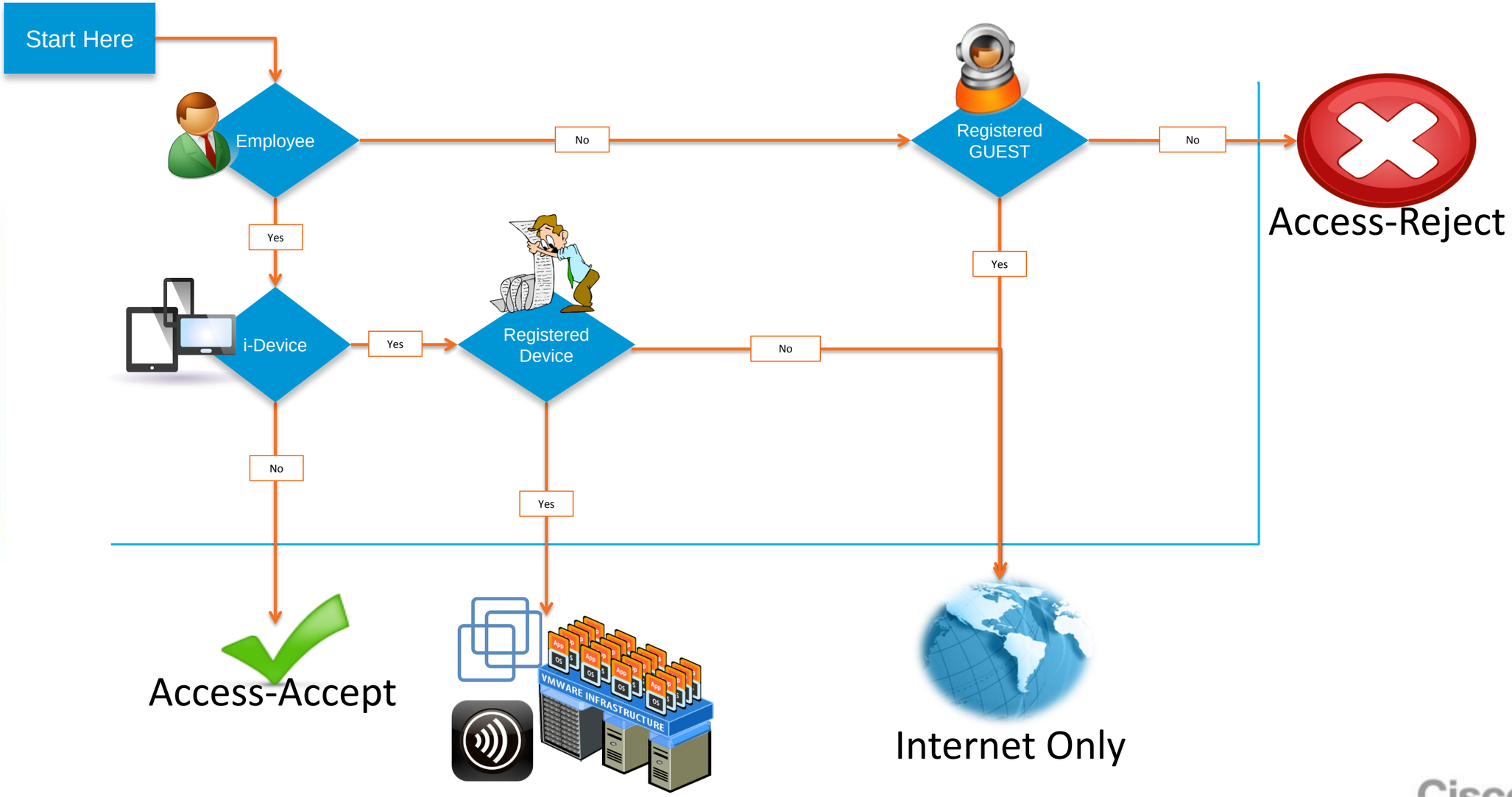
VDx Approach…



- Only corporate devices may access my Corporate Network.
  - Others should get RDP/ICA to a VDI farm.
  - Could use Profiling to determine Corp Asset.
  - Could use Certs or Machine-Auth w/ PEAP-MSChapv2
- Happening a good bit.

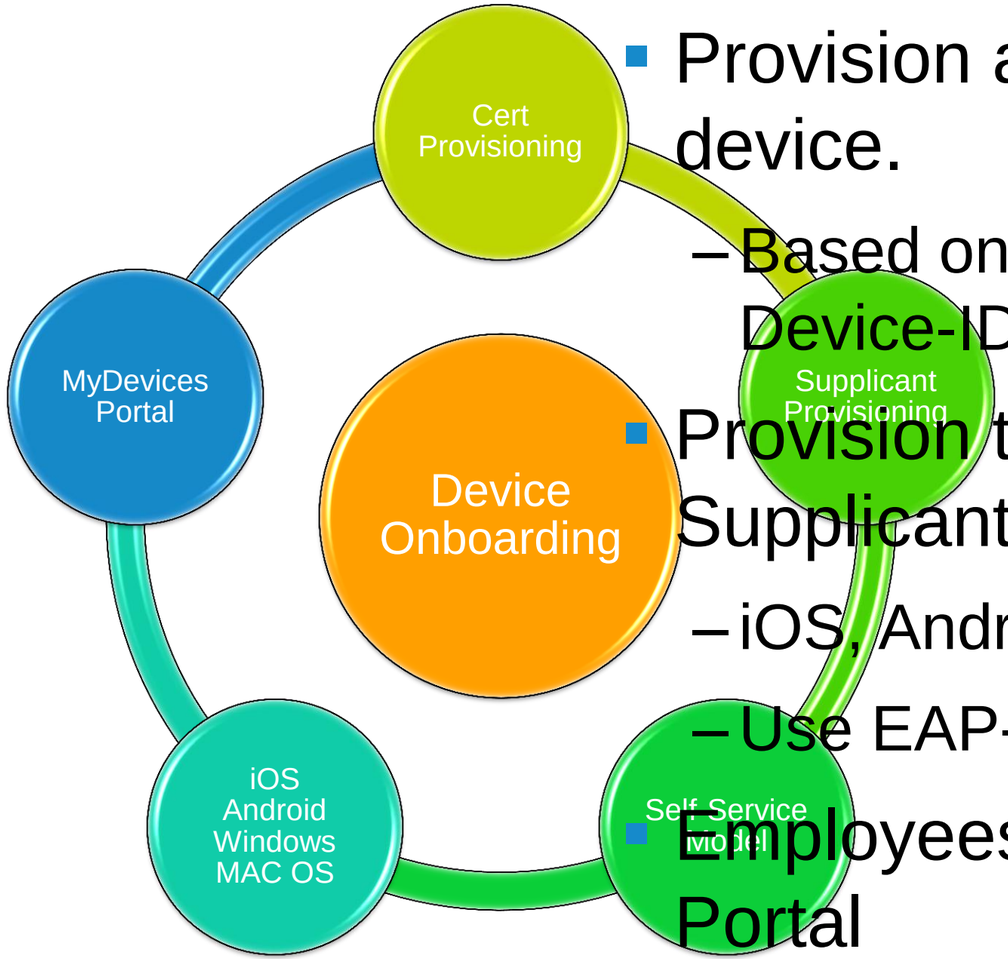
What Makes a BYOD policy?

Even More Complicated



ISE BYOD Release

Identity Services Engine 1.1.1 & Above

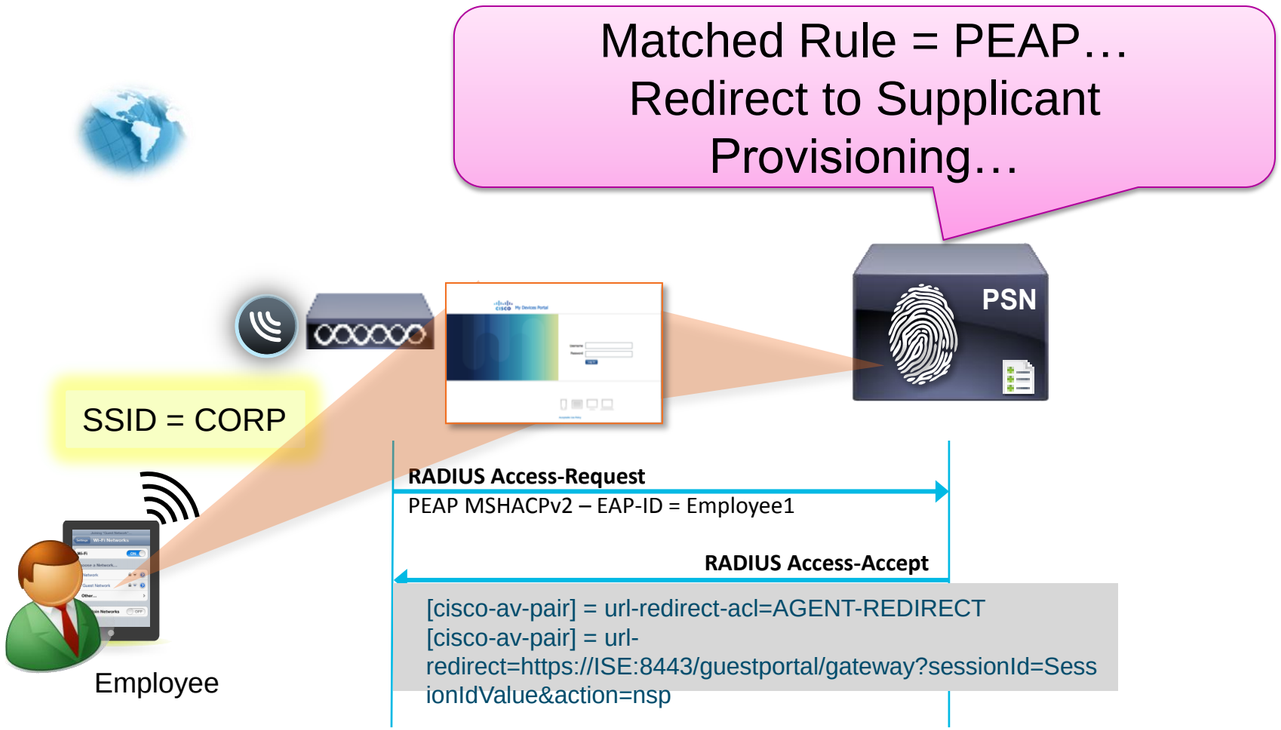


- Provision a Certificate for the device.
  - Based on Employee-ID & Device-ID.
- Provision the Native Supplicant for the Device:
  - iOS, Android, Win & MAC-OSX
  - Use EAP-TLS or PEAP
- Employees get Self-Service Portal
  - Lost Devices are Blacklisted
- Self-Service Model

Authorisation Policy (Single SSID)

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

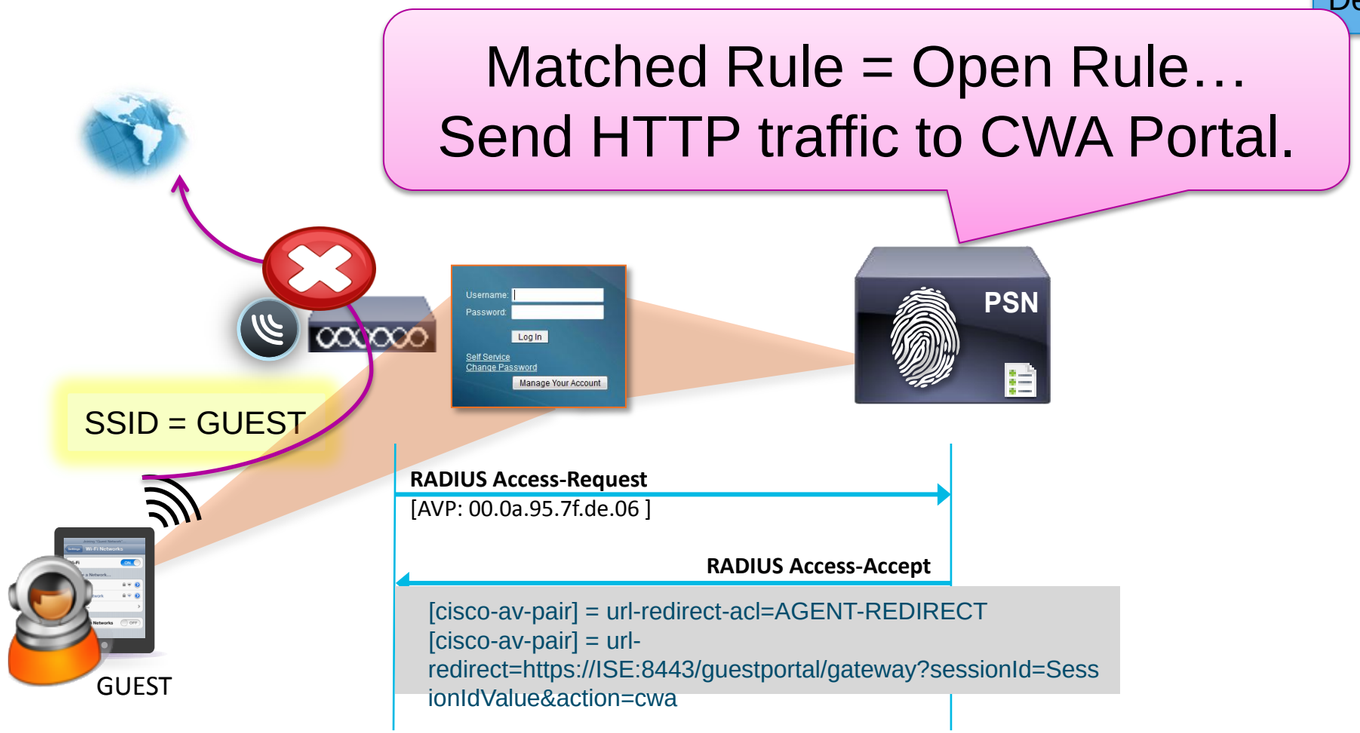
Rule Name		Conditions		Permissions
GUEST	if	GUEST	then	GUEST
Open Rule	if	Wireless_MAB	then	WEBAUTH
PEAP	if	Network Access:EapTunnel EQUALS PEAP	then	Supp-Provision
Employee	if	Employee & EAP-TLS & Certificate SAN = MAC_Addr	then	Employee
Default	If no matches, then		Deny Access	

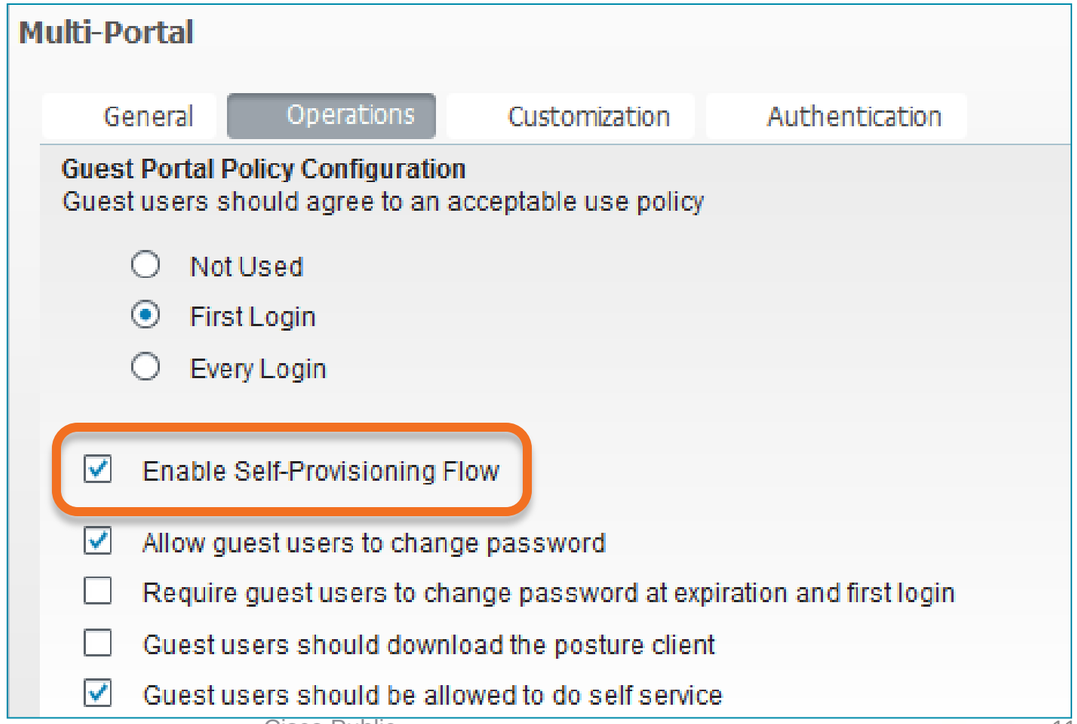


Authorisation Policy (Dual SSID)

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

Rule Name		Conditions		Permissions
GUEST	if	GUEST	then	GUEST
Open Rule	if	Wireless_MAB	then	WEBAUTH
PEAP	if	Network Access:EapTunnel EQUALS PEAP	then	Supp-Provision
Employee	if	Employee & EAP-TLS & Certificate SAN = MAC_Addr	then	Employee
Default	If no matches, then		Deny Access	

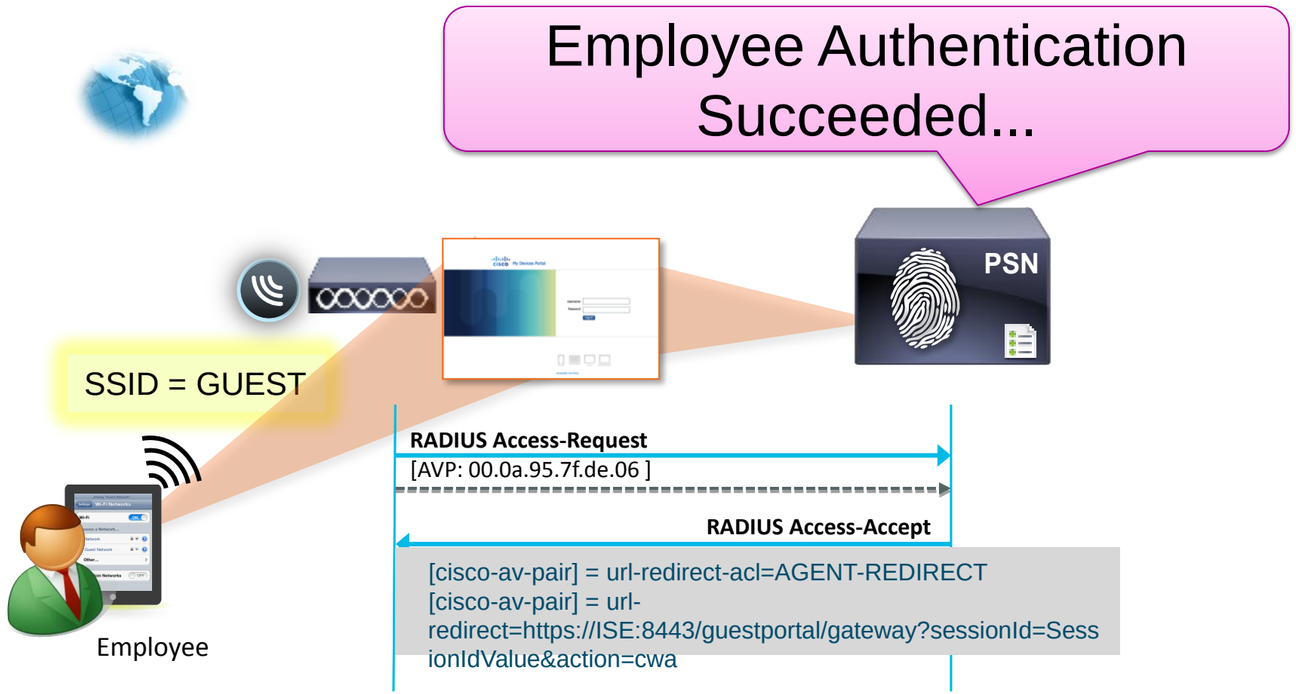


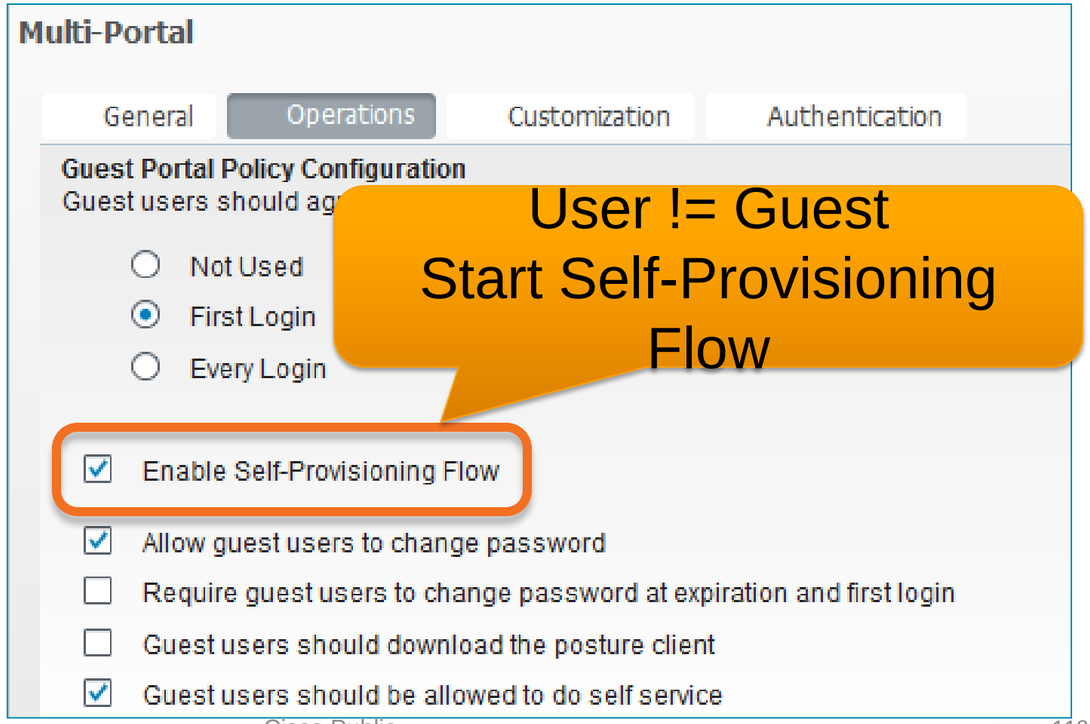


Authorisation Policy (Dual SSID)

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

Rule Name		Conditions		Permissions
GUEST	if	GUEST	then	GUEST
Open Rule	if	Wireless_MAB	then	WEBAUTH
PEAP	if	Network Access:EapTunnel EQUALS PEAP	then	Supp-Provision
Employee	if	Employee & EAP-TLS & Certificate SAN = MAC_Addr	then	Employee
Default	If no matches, then		Deny Access	

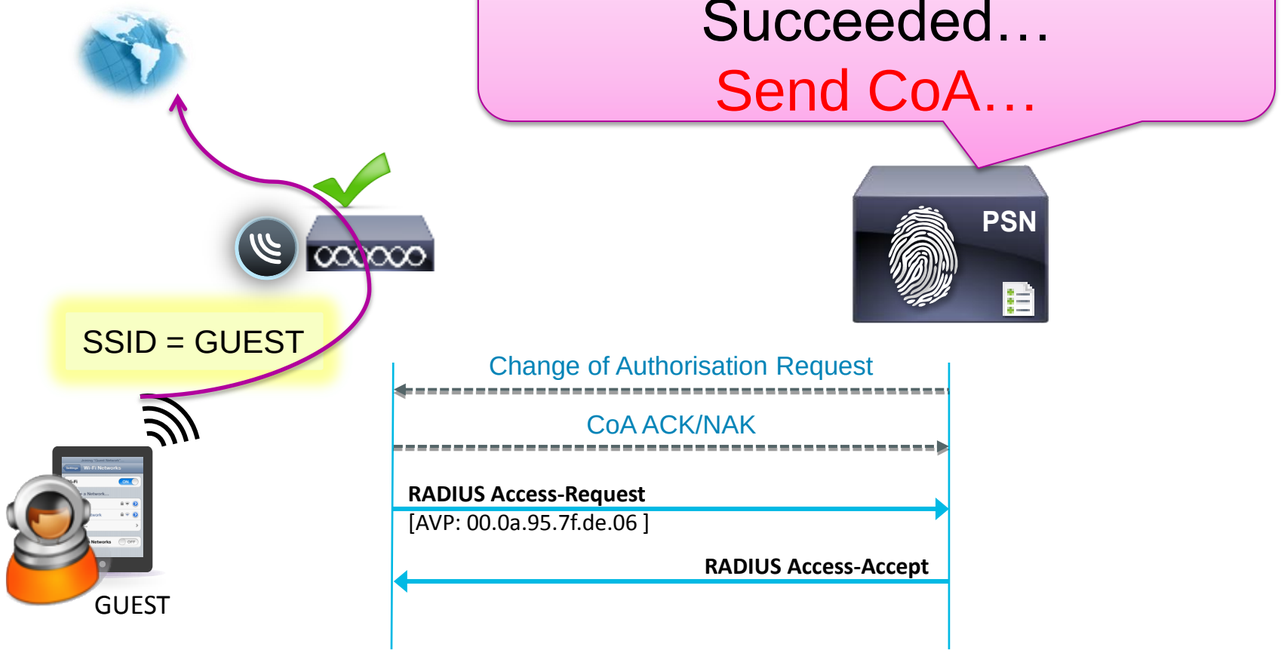


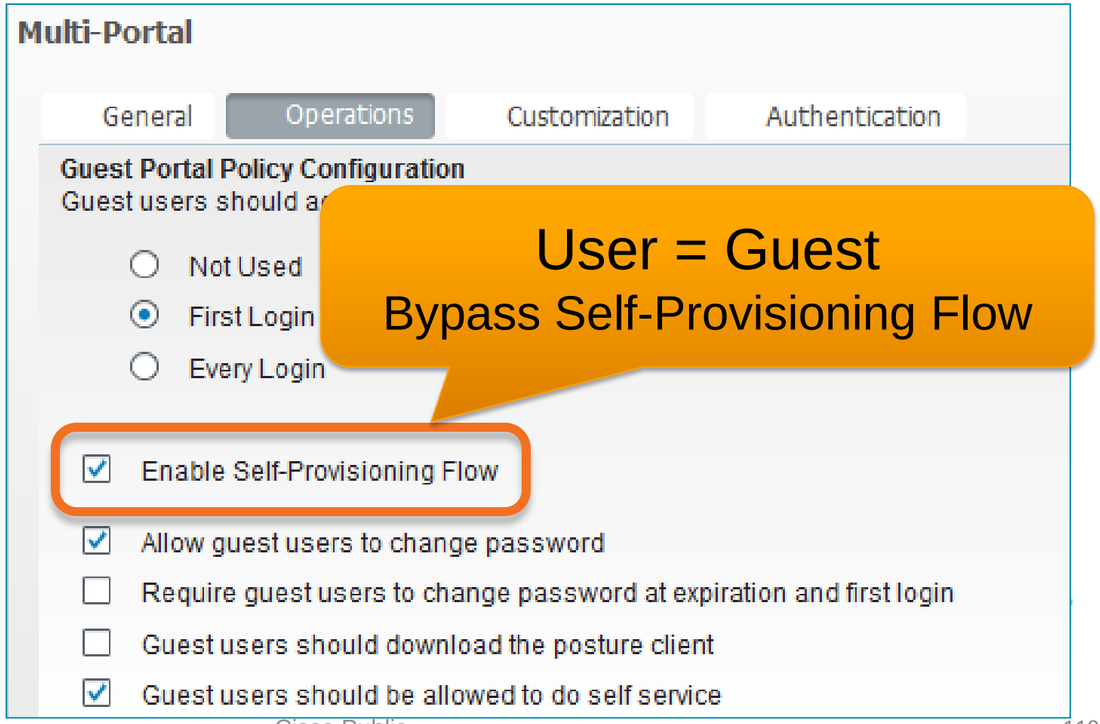


Authorisation Policy (Dual SSID)

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

Rule Name		Conditions		Permissions
GUEST	if	GUEST	then	GUEST
Open Rule	if	Wireless_MAB	then	WEBAUTH
PEAP	if	Network Access:EapTunnel EQUALS PEAP	then	Supp-Provision
Employee	if	Employee & EAP-TLS & Certificate SAN = MAC_Addr	then	Employee
Default	If no matches, then		Deny Access	

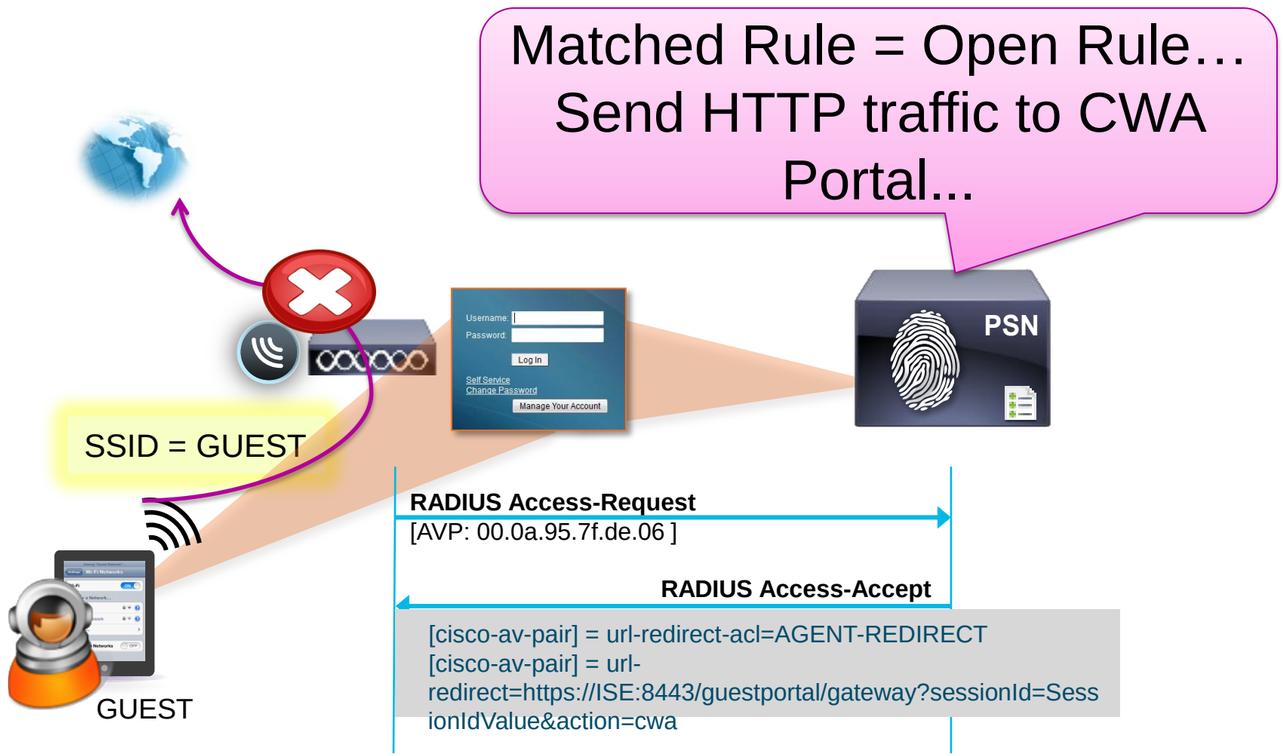


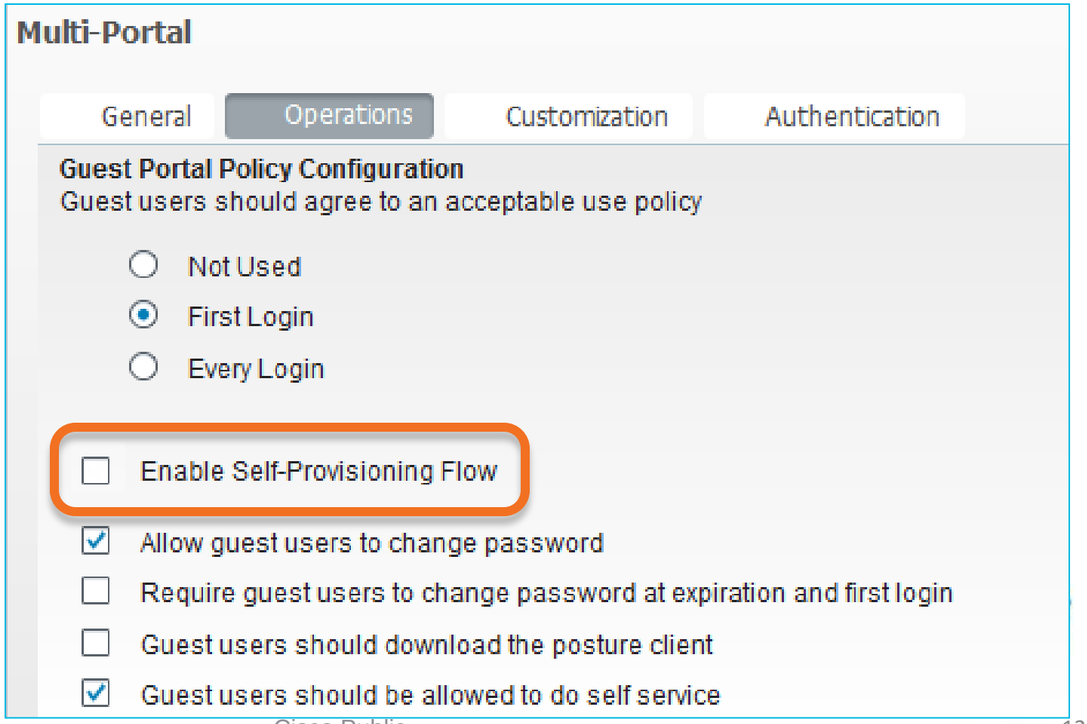


Authorisation Policy

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

Rule Name		Conditions		Permissions
GUEST	if	GUEST	then	GUEST
EmpWebAuth	if	Employee & Guest-Flow	then	Supp-Provision
Open Rule	if	Wireless_MAB	then	WEBAUTH
PEAP	if	Network Access:EapTunnel EQUALS PEAP	then	Supp-Provision
Employee	if	Employee & EAP-TLS & Certificate SAN = MAC_Addr	then	Employee
Default	If no matches, then		Deny Access	

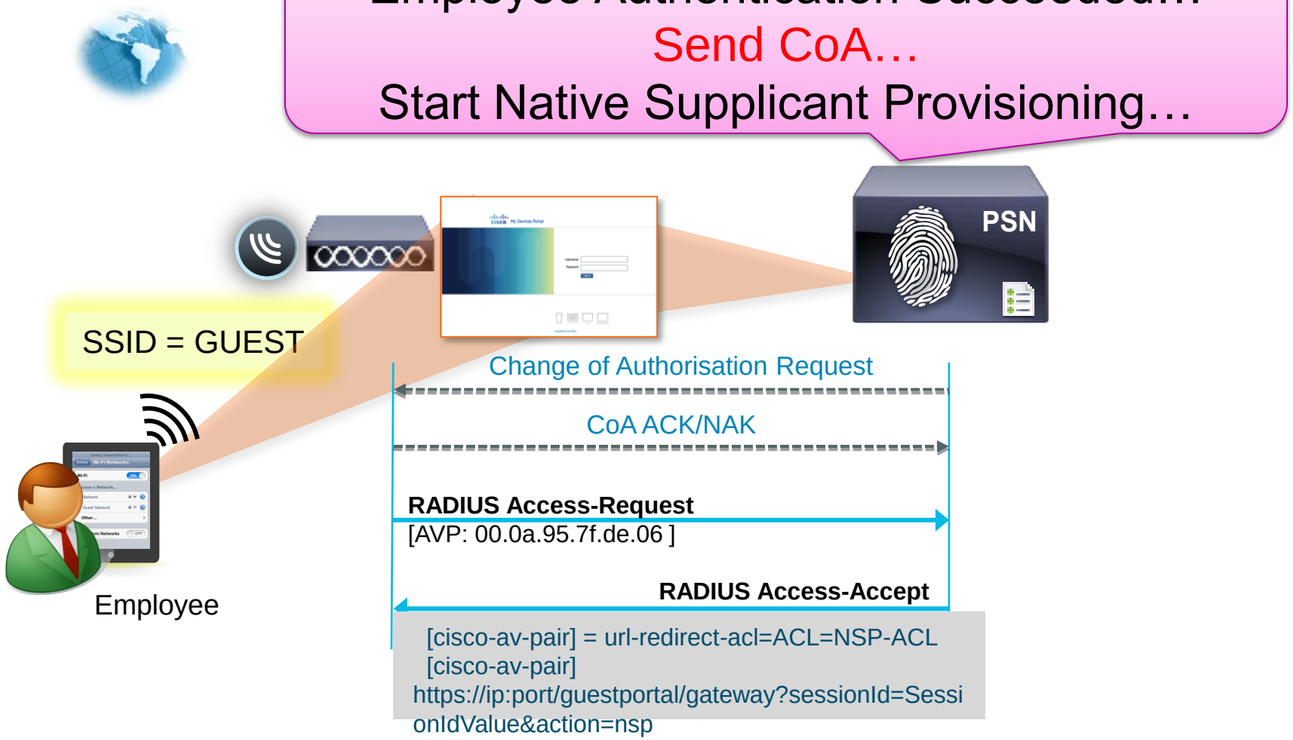


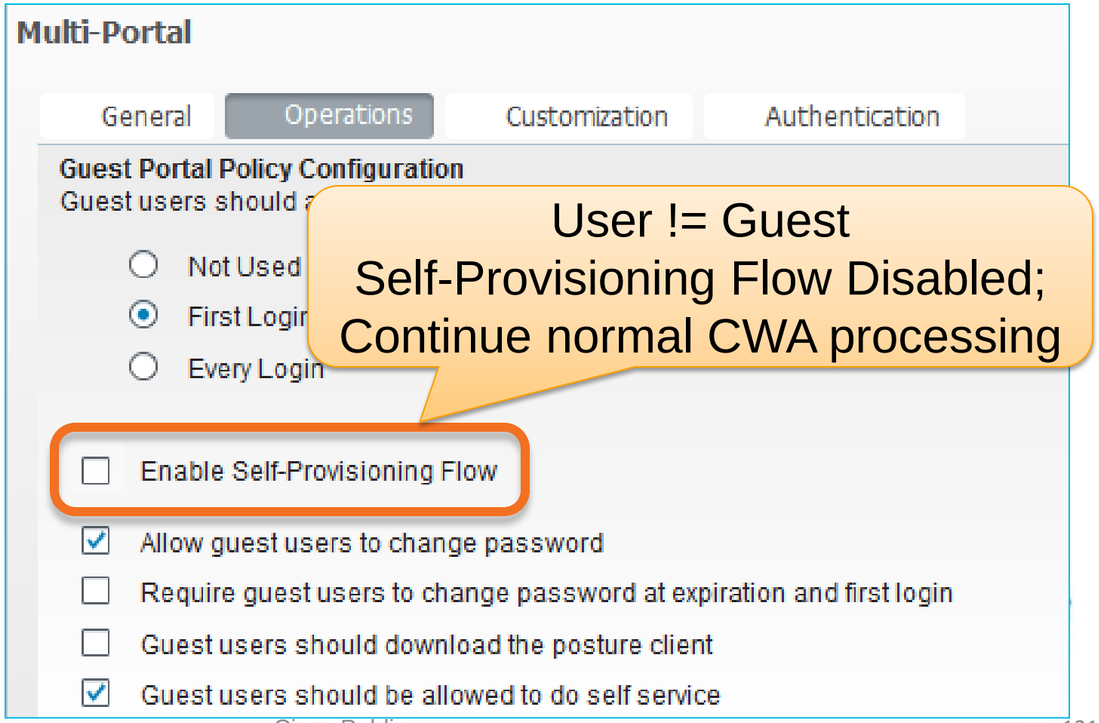


Authorisation Policy

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

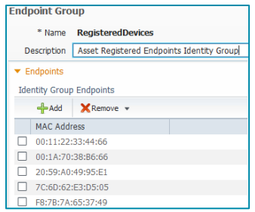
Rule Name		Conditions		Permissions
GUEST	if	GUEST	then	GUEST
EmpWebAuth	if	Employee & Guest-Flow	then	Supp-Provision
Open Rule	if	Wireless_MAB	then	WEBAUTH
PEAP	if	Network Access:EapTunnel EQUALS PEAP	then	Supp-Provision
Employee	if	Employee & EAP-TLS & Certificate SAN = MAC_Addr	then	Employee
Default	If no matches, then		Deny Access	





Native Supplicant Provisioning (iOS use-case)

Employee



RegisteredDevices

Device Registration

HTTPS to the NSP Portal

ISE sends CA certificate to endpoint for trust with OTA

User clicks register.

Device Enrollment

ISE sends Profile Service to iOS Device

CSR is Generated on iOS

Encrypted Profile Service:
https://ISE:8905/auth/OTAMobileConfig?sessionID

CSR sent to ISE

SCEP to MS Cert Authority

Certificate sent to ISE

ISE sends Device Certificate to iOS Device

Device Provisioning

ISE sends Device BYOD_Profile to iOS Device

CSR sent to ISE

SCEP to MS Cert Authority

Certificate sent to ISE

ISE sends User Certificate to iOS Device

SSID = CTS-CORP
EAP-TLS

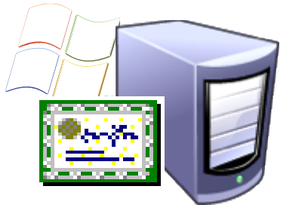
Signing Certificate + User Certificate:
Wi-Fi Profile with EAP-TLS configured

User Certificate Issued

CN = Employee
SAN = 00-0a-95-7f-de-06

NSP (Android use-case)






Employee

RegisteredDevices

SSID = BYOD-Open / CWA

Posture-Required state

CWA Redirect / Redirect ACL = CWA

Device Registration

User opens browser

Redirect to ISE for CWA

CWA login

CWA login successful / Redirect to NSP Portal

User clicks Register

CoA to WLC

Redirect browser to http://play.google.com (Session:DeviceOS=Android)

Access-Request

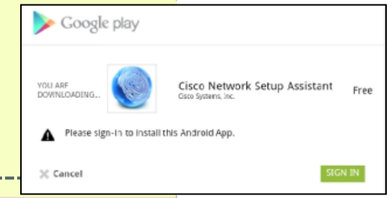
Posture-Required state

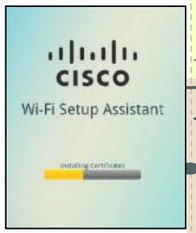
NSP Redirect / Redirect ACL = ALLOW_GOOGLE

Download Supplicant Provisioning Wizard (SPW) app from Google Playsto

Download SPW

Sample WLC
ACL=ALLOW_GOOGLE
permit udp any any dns
permit tcp any <ISE_PSN>
deny ip any <internal_network>
permit tcp any 74.125.0.0 255.255.0.0
permit tcp any 173.194.0.0
255.255.0.0
permit tcp any 206.111.0.0
255.255.0.0
deny ip any any





User installs application and launches

App sends request to http://DFG/auth/discovery

Redirect Discovery to ISE

Device Provisioning

ISE sends Device BYOD_Profile to Android Device

CSR sent to ISE

SCEP to MS Cert Authority

User Cert Issued

Certificate sent to ISE

ISE sends User Certificate to Android Device

SSID = CTS-CORP / EAP-TLS

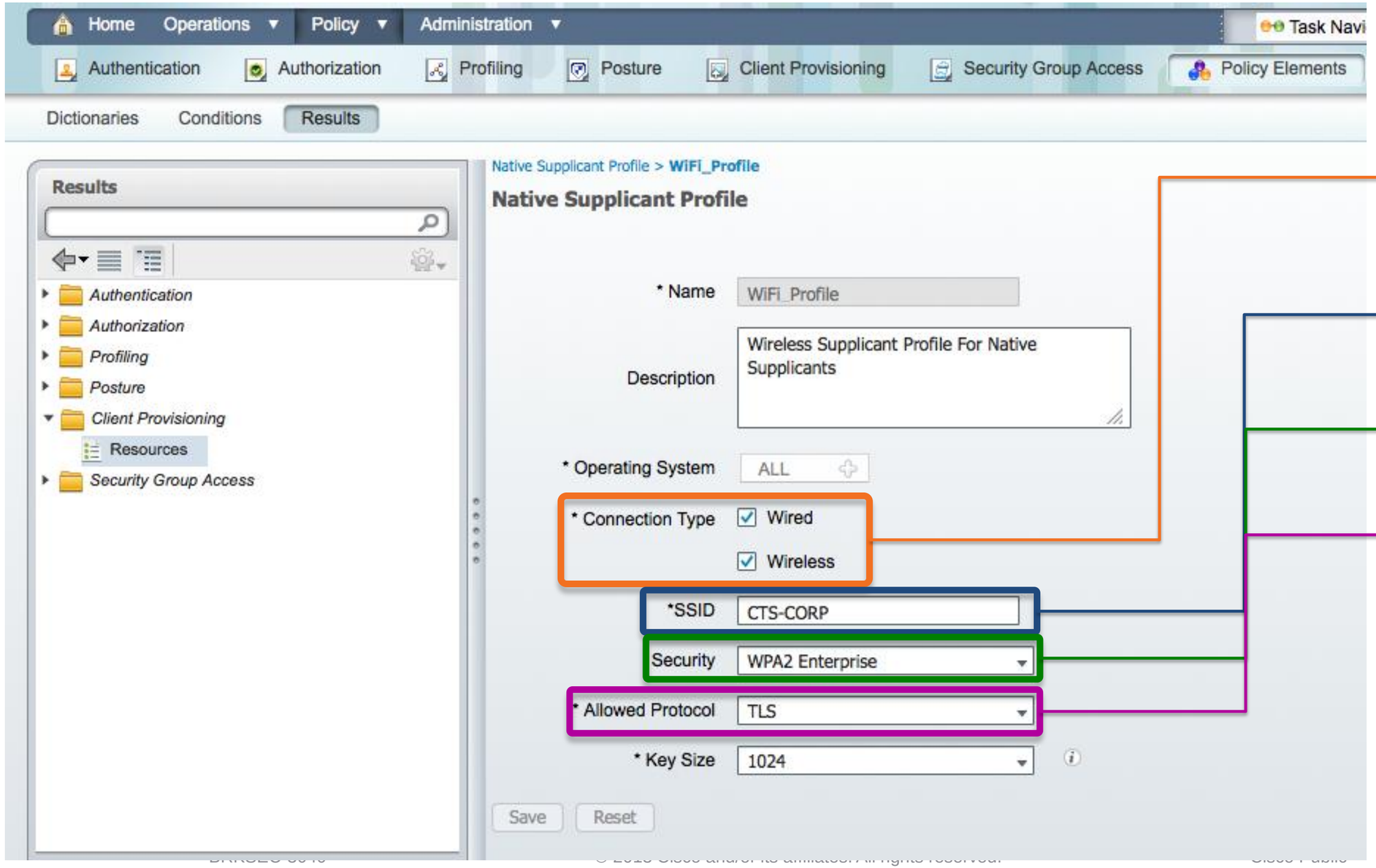
CN = Employee
SAN = 00-0a-95-7f-de-06

Connect using EAP-TLS

RUN state

Access-Accept

Wi-Fi Profile: Client Provisioning Resource



Wired, Wireless or Both

Specify SSID

WPA or WPA2

TLS or PEAP

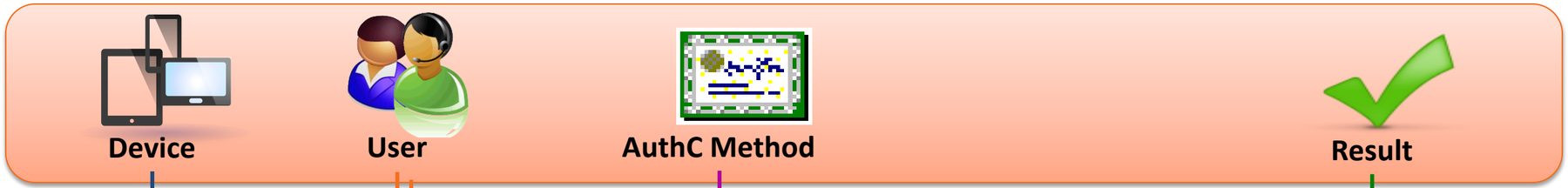
Client Provisioning Policy

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Mac iOS All	and AD1:ExternalGroups EQUALS cts.l...	then WiFi_Profile
Android	If Any	and Android	and AD1:ExternalGroups EQUALS cts.l...	then WiFi_Profile
WinThings	If Any	and Windows...	and AD1:ExternalGroups EQUALS cts.l...	then WinSPWizard 1.0.0.14 And WiFi_Profile
MAC-OSX	If Any	and Mac OSX	and AD1:ExternalGroups EQUALS cts.l...	then MacOsXSPWizard 1.0.0.6 And WiFi_Profile

BYOD Policy in ISE



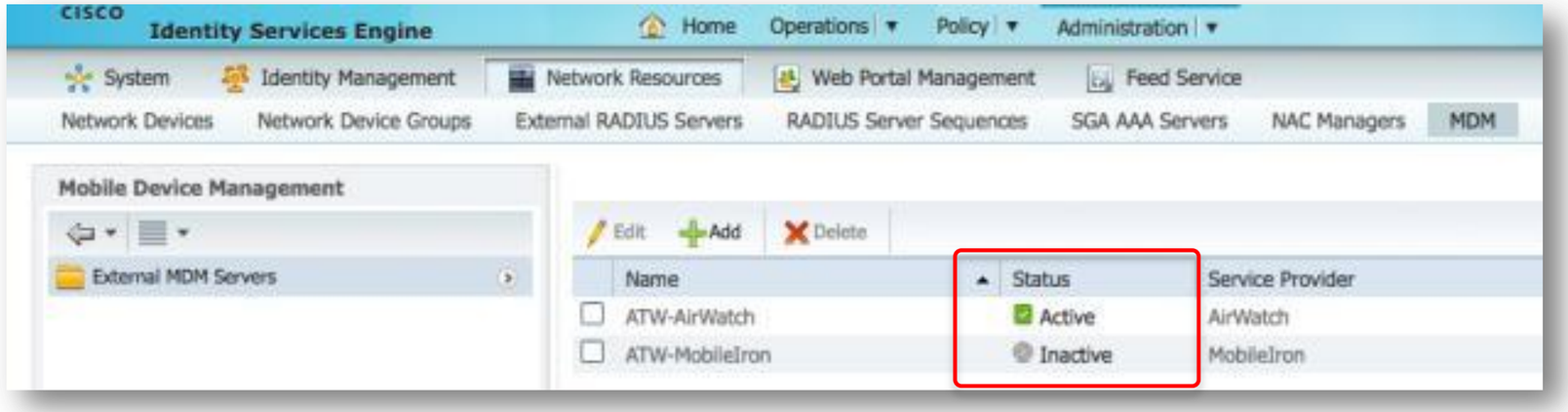
Black List Default	if	**Blacklist**	then	Blacklist_Access
Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
PEAP Rule	if	PEAP	then	SupplicantProvision
Open Rule	if	Wireless_MAB	then	NSP
Employee Rule	if	**RegisteredDevices** AND (Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND AD1:ExternalGroups EQUALS cts.local/Users/Employees)	then	Employee

1.2 MDM Integration

MDM Vendors

Requires a new API in MDM Server

- Only ONE may be active at a time in ISE



- Cisco Published API Specs to 4 Vendors:
  - AirWatch Version 6.2
  - Mobile Iron Version: 5.0
  - ZenPrise Version: 7.1
  - Good Version: 2.3

Initial Vendors

MobileIron®

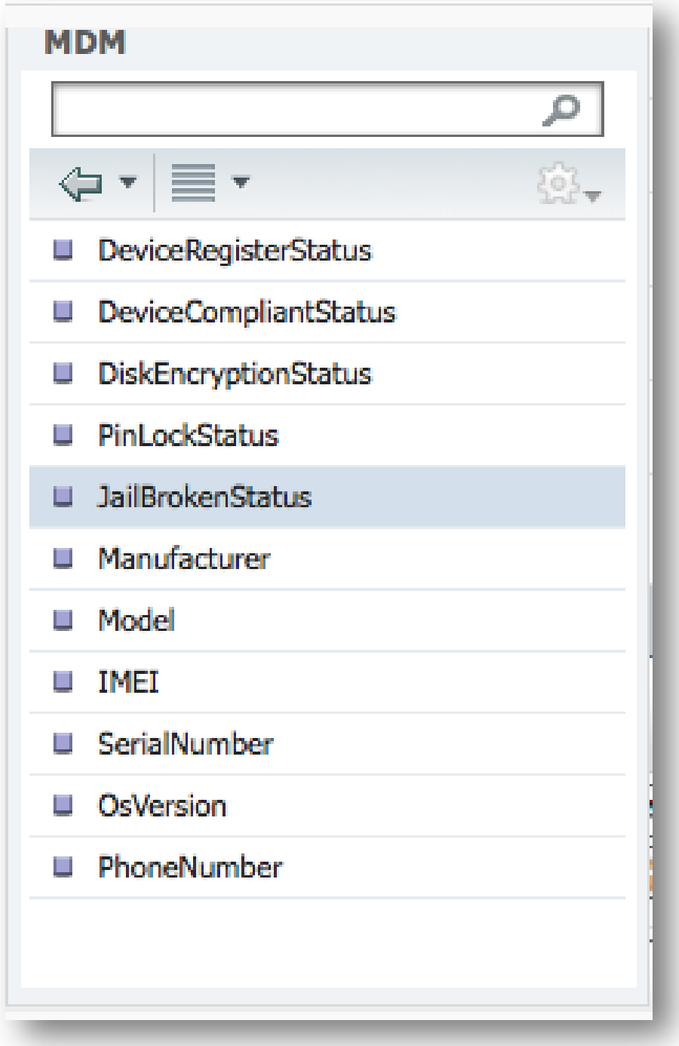
airwatch™

ZENPRISE

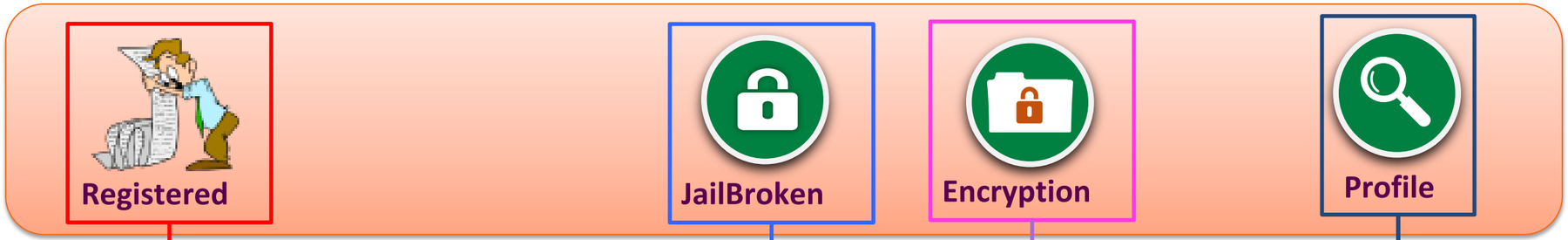
Good

Attributes from MDM

- With the API, we can query on:
  - General Compliant or ! Compliant (Macro level) -or-
    - Disk encryption is one
    - Pin lock
    - Jail broken
- Bulk re-check against the MDM every 4 hours.
  - But we are not using the cached data in the AuthZ
  - If result of Bulk Re-check shows that a device is no longer compliant – we will send a CoA to terminate session.
  - Works same with all 4 vendors.



MDM Integration



PEAP	if (Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP)	then	NSP
SendToMDM	if **RegisteredDevices** AND MDM:DeviceRegisterStatus EQUALS UnRegistered	then	MDM-OnBoard
MobileDevice-Compliant	if (EndPoints:BYODRegistration EQUALS Yes AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:JailBrokenStatus EQUALS Unbroken AND MDM:DiskEncryptionStatus EQUALS On AND EndPoints:LogicalProfile EQUALS i-things)	then	Limited-Employee
Default	if no matches, then	PermitAccess	

Reset

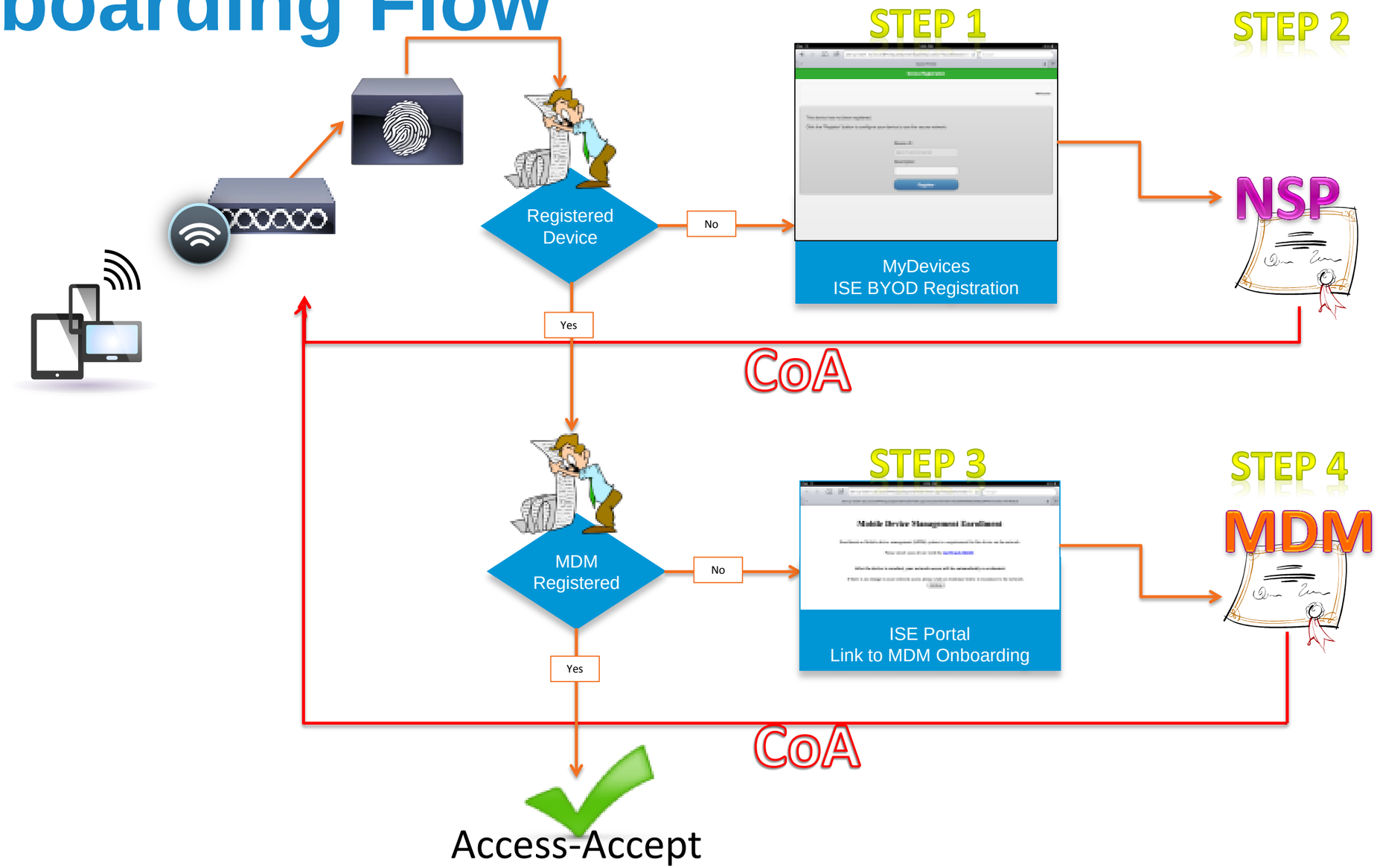
ISE Checks the MDM every session

- Scalability = 30 Calls per second.
  - For Cloud Based Solutions, Bandwidth and Latency will need to be considered.

- Survivability:
  - If the MDM is not available, the rule will not match.
  - Will (by default) stick the user in the “Register with MDM” state.

Looking into alternatives

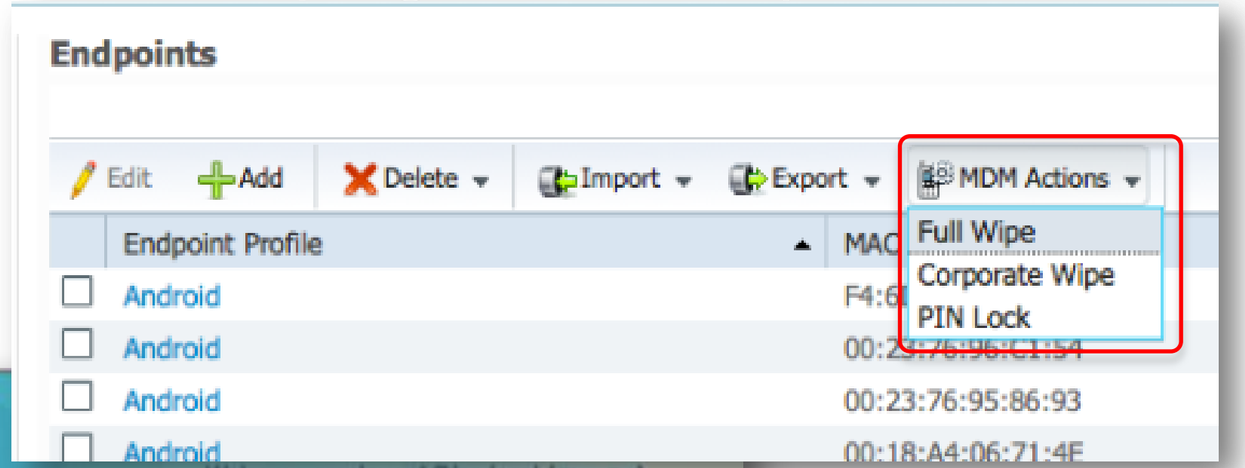
Onboarding Flow

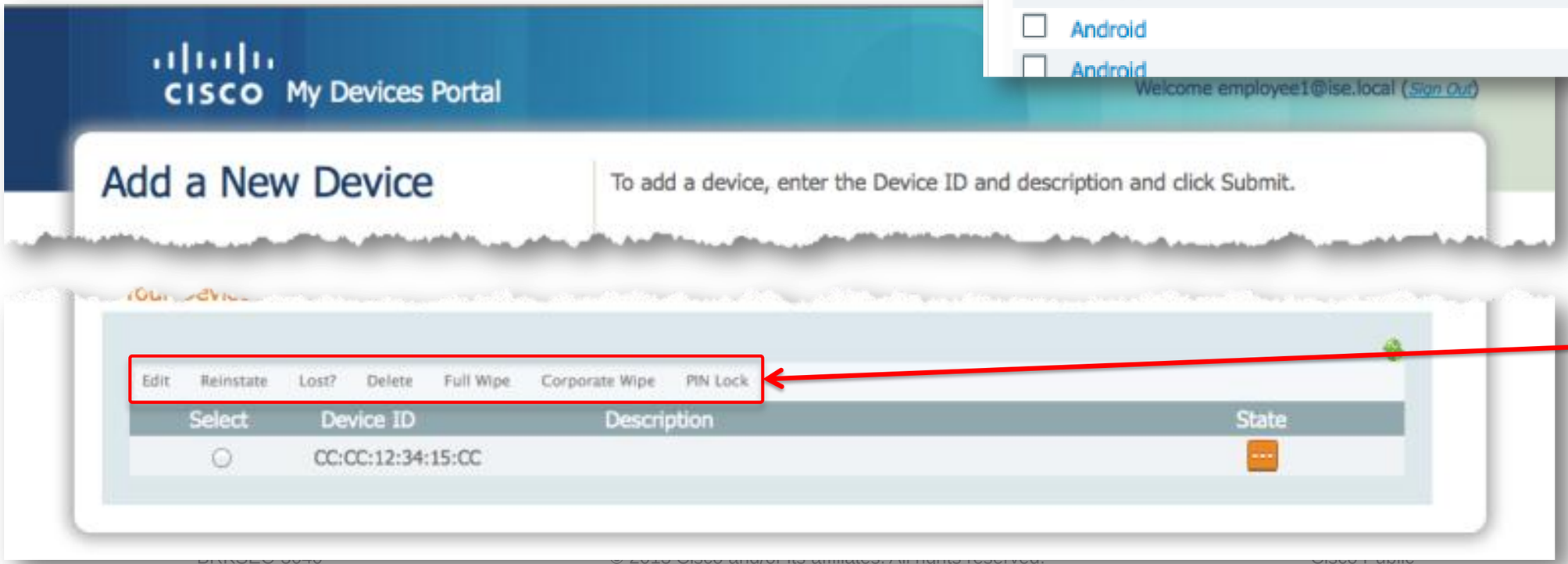


MDM Integration

Ability for administrator and user in ISE to issue remote actions on the device through the MDM server (eg: remote wiping the device)

- MyDevices Portal
- Endpoints Directory in ISE

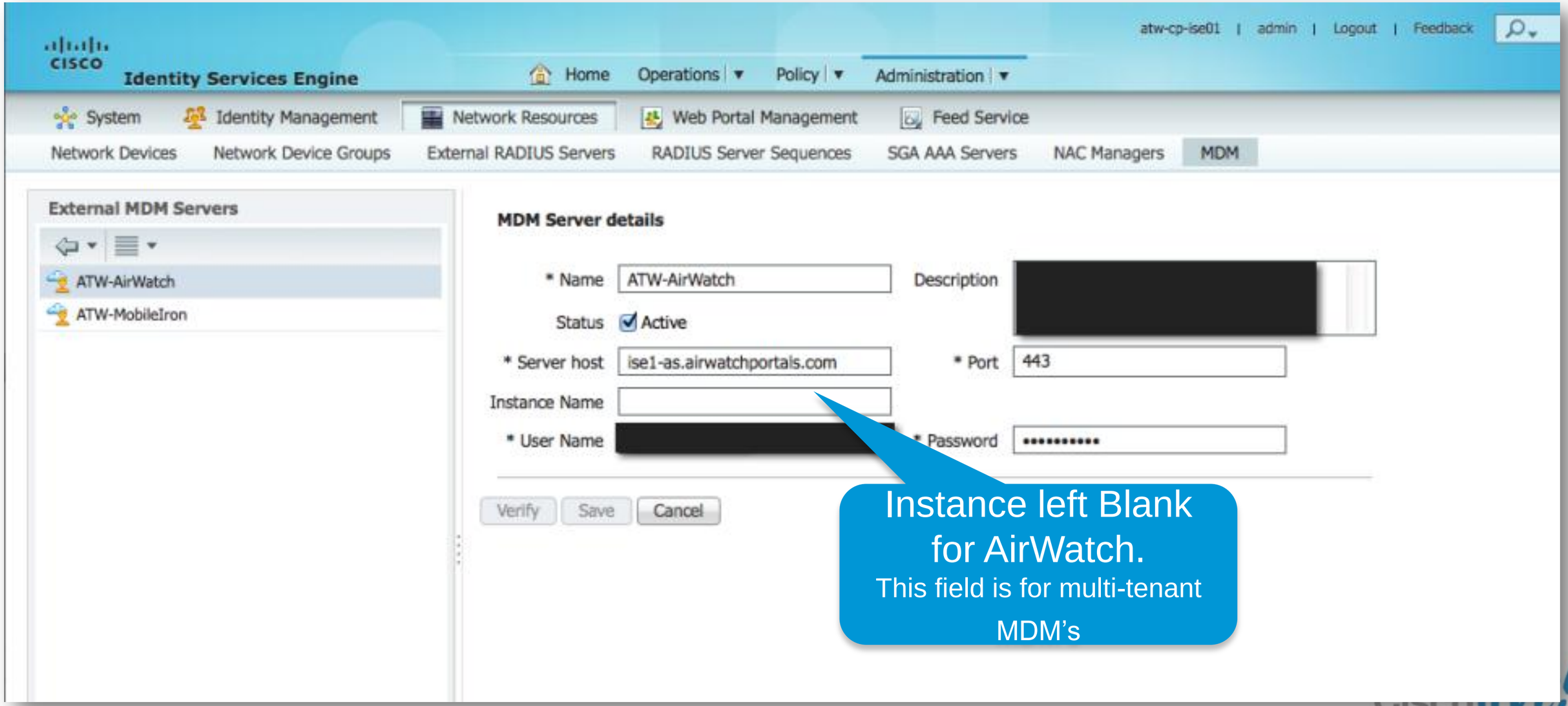




Options

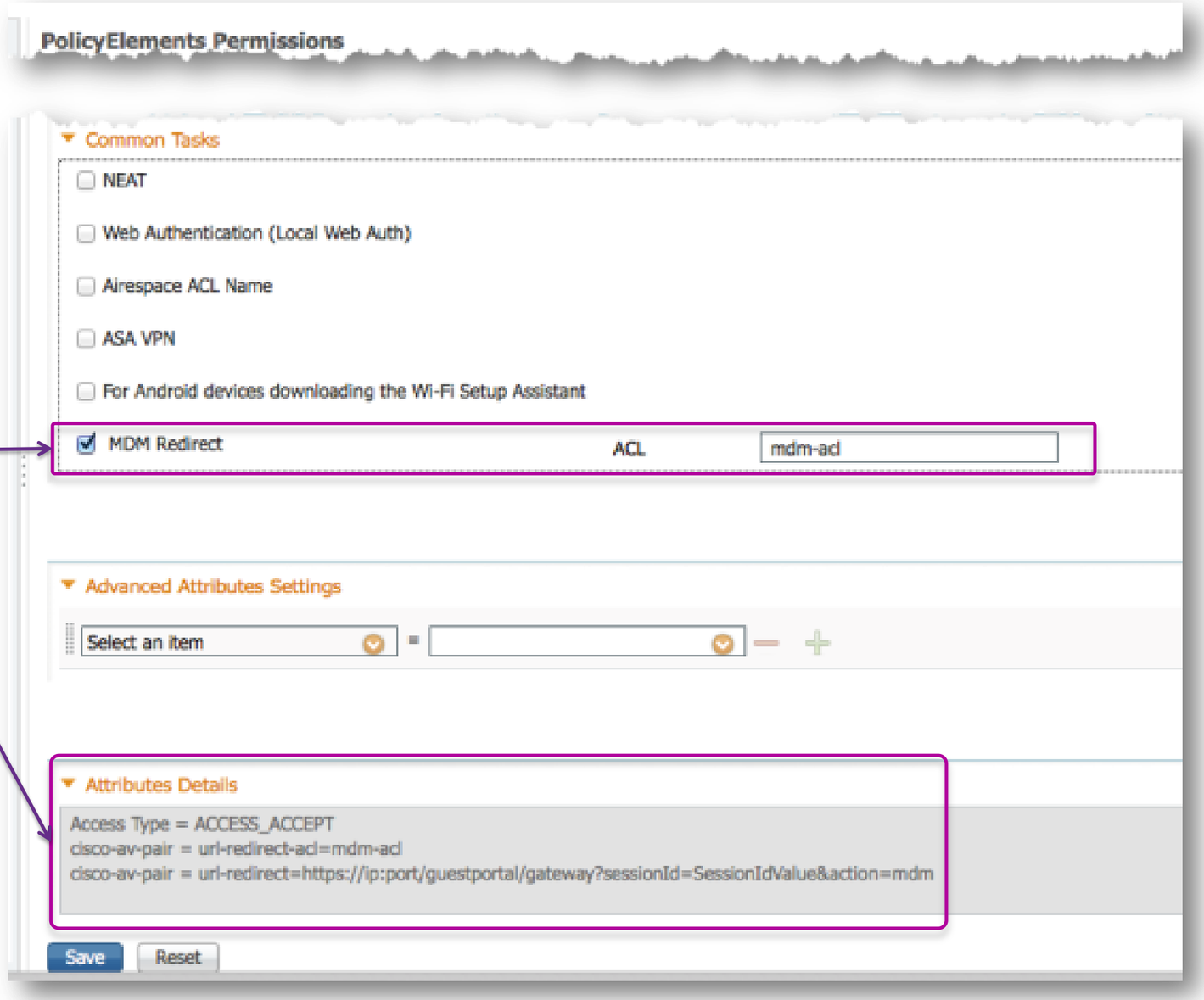
- Edit
- Reinstate
- Lost?
- Delete
- Full Wipe
- Corporate Wipe
- PIN Lock

MDM – Connection Screen



MDM Onboarding

Own Common Task

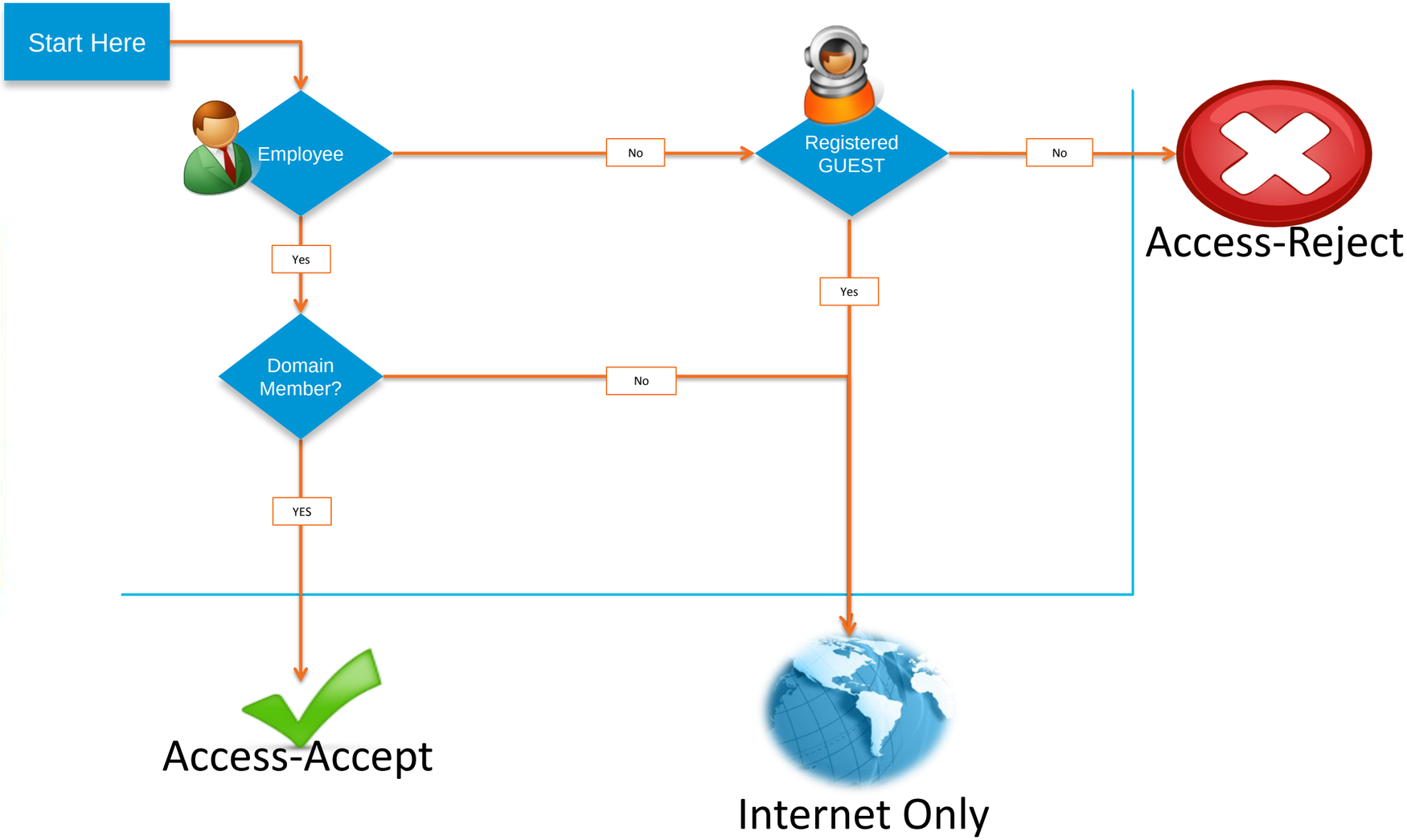


The Opposite End of Spectrum:

How to differentiate corporate provisioned devices?

Corporate Assets

Provide differentiated access for IT-managed systems.



Identifying the Machine AND the USER

Machine Access Restrictions (MAR)

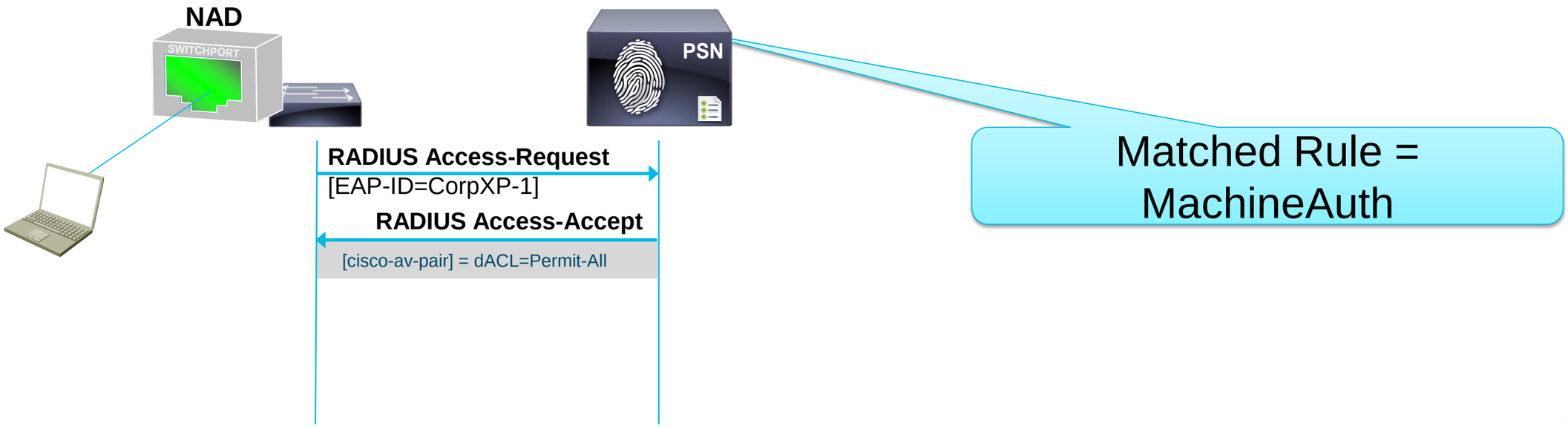
- MAR provides a mechanism for the RADIUS server to search the previous authentications and look for a machine-authentication with the same Calling-Station-ID.
- This means the machine must do authenticate before the user.
  - i.e. Must log out, not use hibernate, etc….
- See the reference slides for more possible limitations.

Machine Access Restrictions (MAR)

MAR Cache

Calling-Station-ID 00:11:22:33:44:55 – Passed

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	if	Domain Computers	then	MachineAuth
Employee	if	Employee & **WasMachineAuthenticated = true**	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	

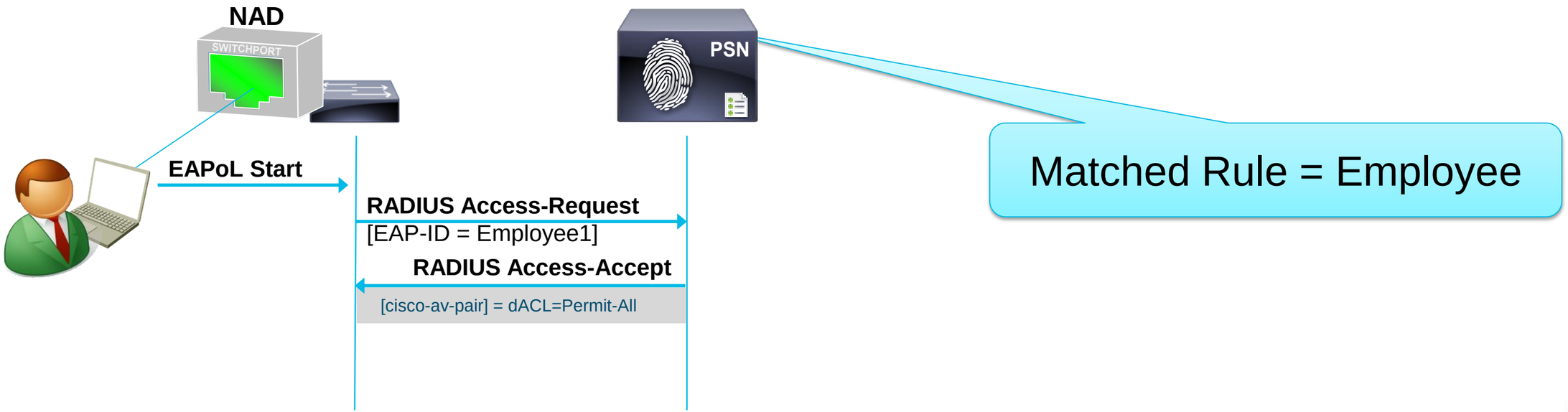


Machine Access Restrictions (MAR)

MAR Cache

Calling-Station-ID 00:11:22:33:44:55 – Passed

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	if	Domain Computers	then	MachineAUth
Employee	if	Employee & **WasMachineAuthenticated = true**	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	



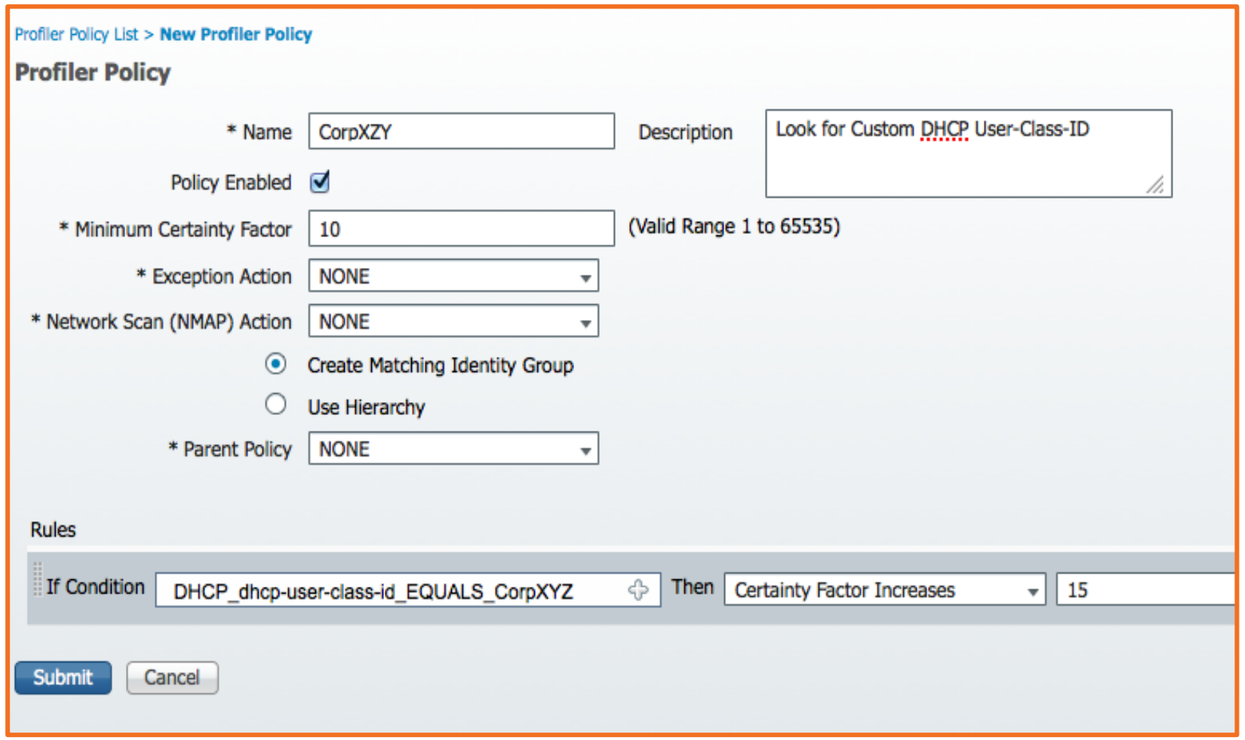
Machine Access Restrictions (MAR)

Potential Issues with MAR

- Potential Issues with MAR:
  - **Wired/WiFi transitions**: Calling-Station-ID (MAC address) is used to link machine and user authentication; MAC address will change when laptop moves from wired to wireless breaking the MAR linkage.
  - **Machine state caching**: The state cache of previous machine authentications is neither persistent across ACS/ISE reboots nor replicated amongst ACS/ISE instances
  - **Hibernation/Standby**: 802.1X fails when the endpoint enters sleep/hibernate mode and then moves to a different location, or comes back into the office the following day, where machine auth cache is not present in new RADIUS server or has timed out.

Identifying the Machine AND the User

Real Customer Example: Custom DHCP Attribute & use Profiler



One customer decided to modify the DHCP User Class-ID on their Domain Members

- Provided a unique way to profile the device as a Corporate Asset.

```
C:\>ipconfig /setclassid "Local Area Connection" CorpXYZ

Windows XP IP Configuration
        DHCP ClassId successfully modified for adapter"Local Area Connection"
```

http://technet.microsoft.com/en-us/library/cc783756(WS.10).aspx

Identifying the Machine AND the User

The next chapter of authentication: EAP-Chaining

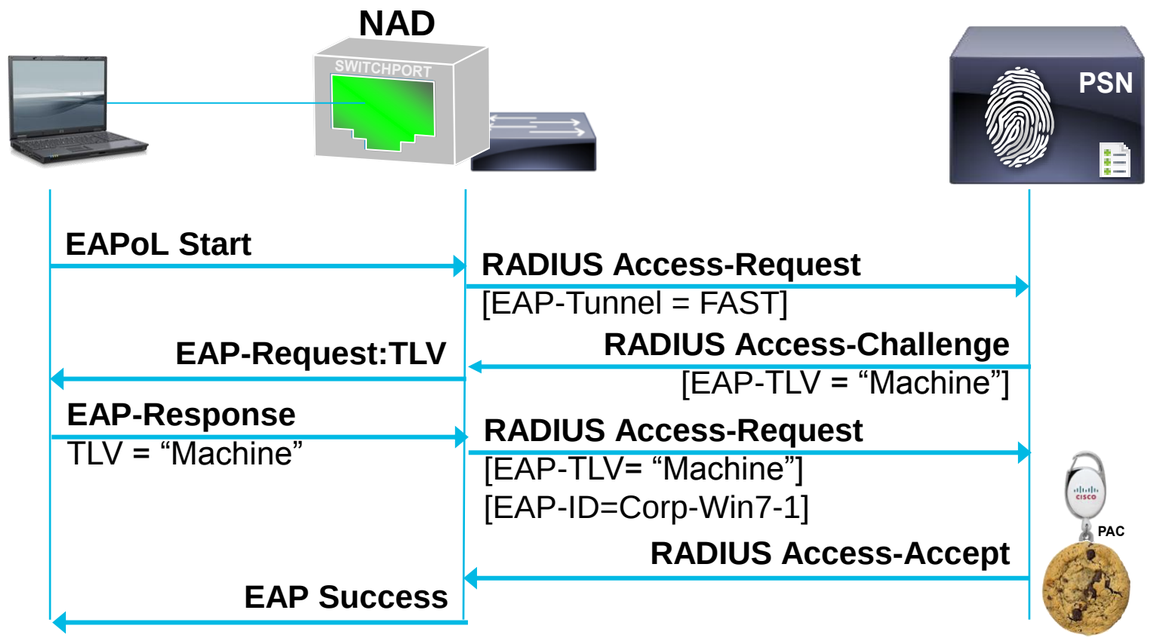
- IETF working group is in process of standardising on Tunneled EAP (TEAP).
  - Next-Generation EAP method that provides all benefits of current EAP Types.
  - Also provides EAP-Chaining.
- Cisco will do it before TEAP is ready
  - EAP-FASTv2
  - AnyConnect 3.1
  - Identity Services Engine 1.1.1 (1.1 Minor Release)

EAP-Chaining

With AnyConnect 3.1.1 and ISE 1.1.1

1. Machine Authenticates
2. ISE Issues Machine AuthZ PAC

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	if	Domain Computers	then	MachineAuth
Employee	if	Employee & **Network Access:EAPChainingResult = User and machine suceeded**	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	

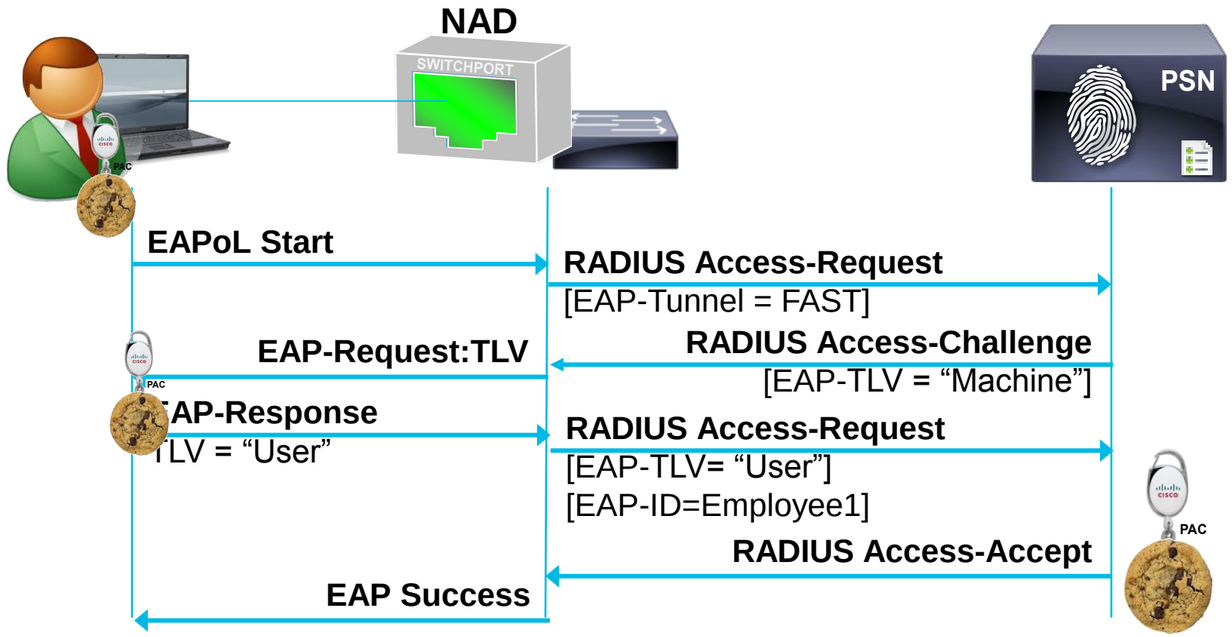


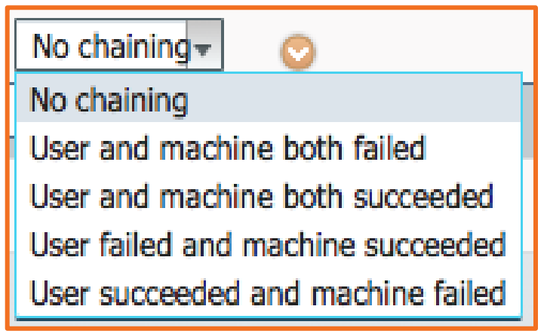
EAP-Chaining

With AnyConnect 3.1.1 and ISE 1.1.1

3. User Authenticates
4. ISE receives Machine PAC
5. ISE issues User AuthZ PAC

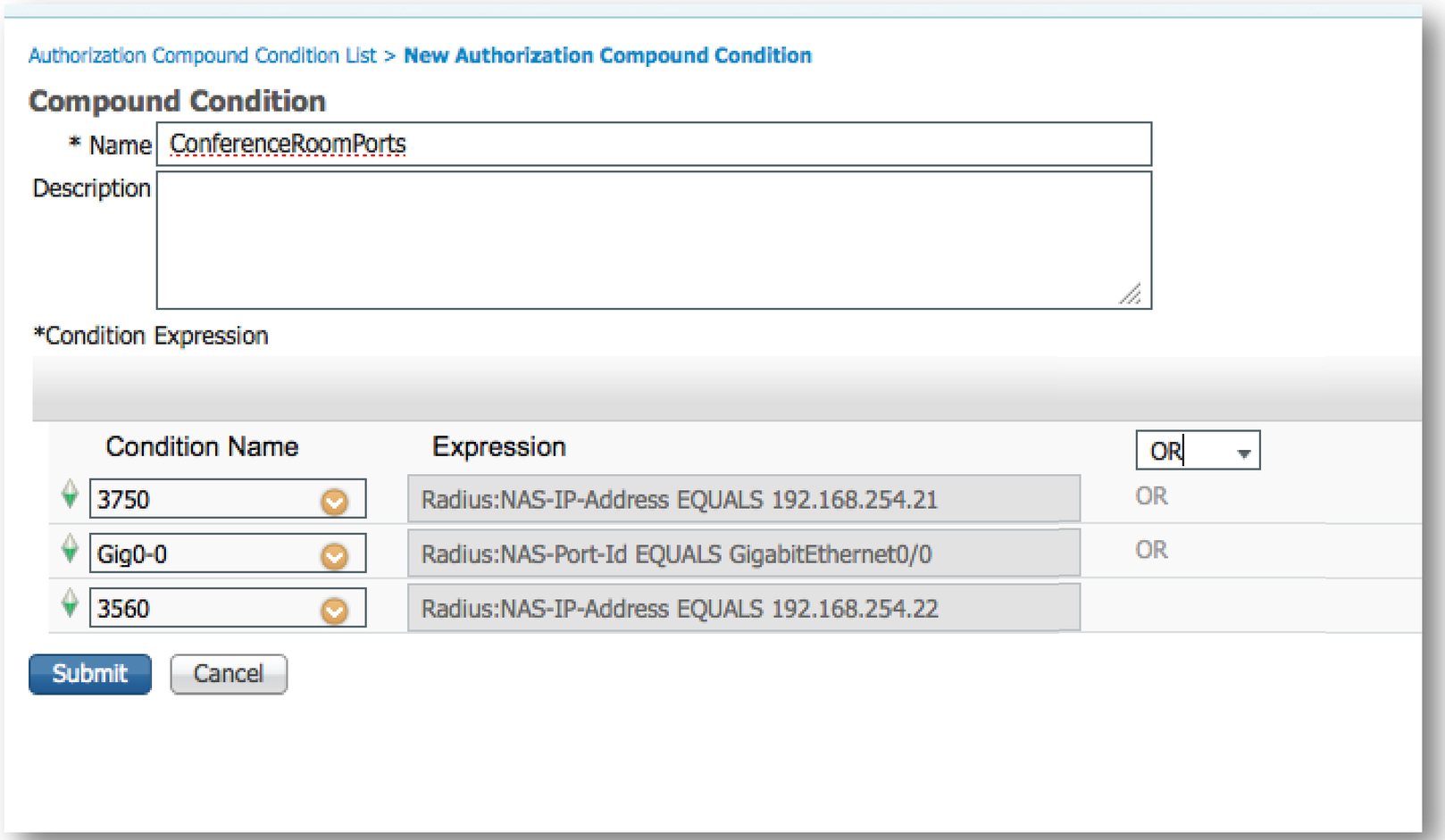
Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	if	Domain Computers	then	MachineAuth
Employee	if	Employee & **Network Access:EAPChainingResult = User and machine suceeded**	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	





Combining AND & OR

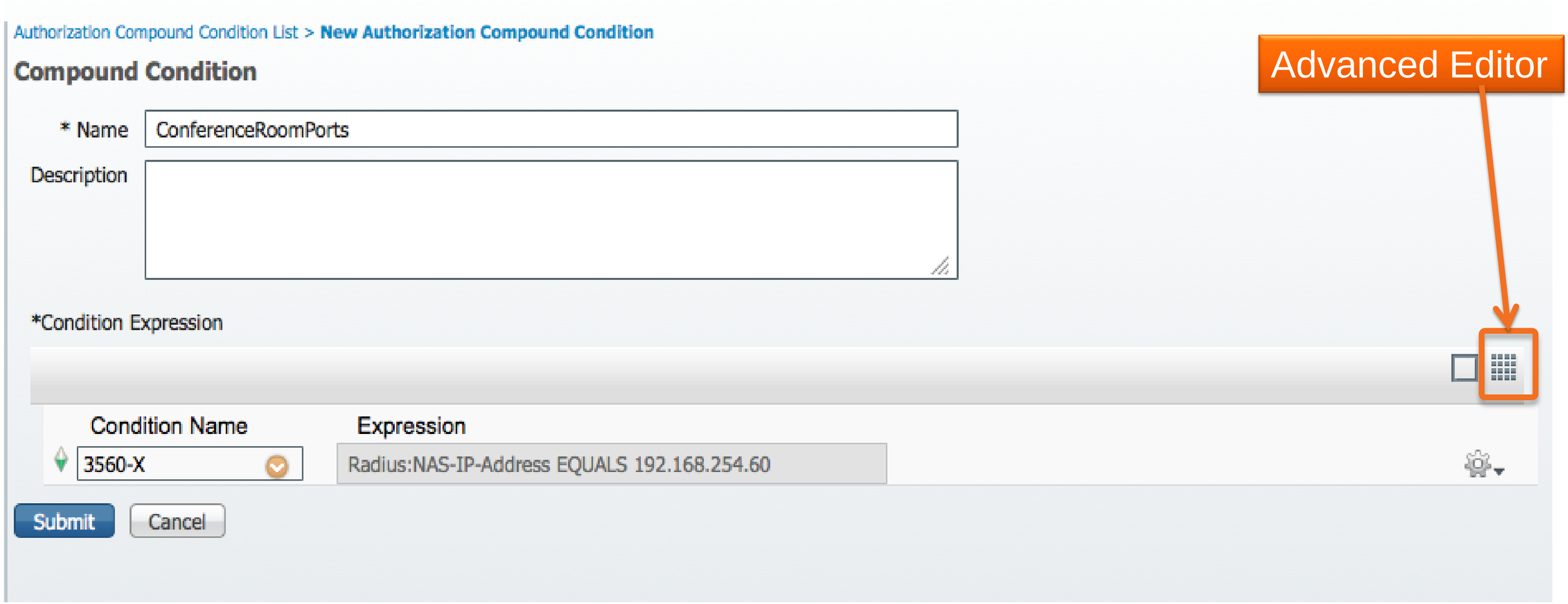
Combining AND with OR in AuthZ Policies



Cannot Mix??

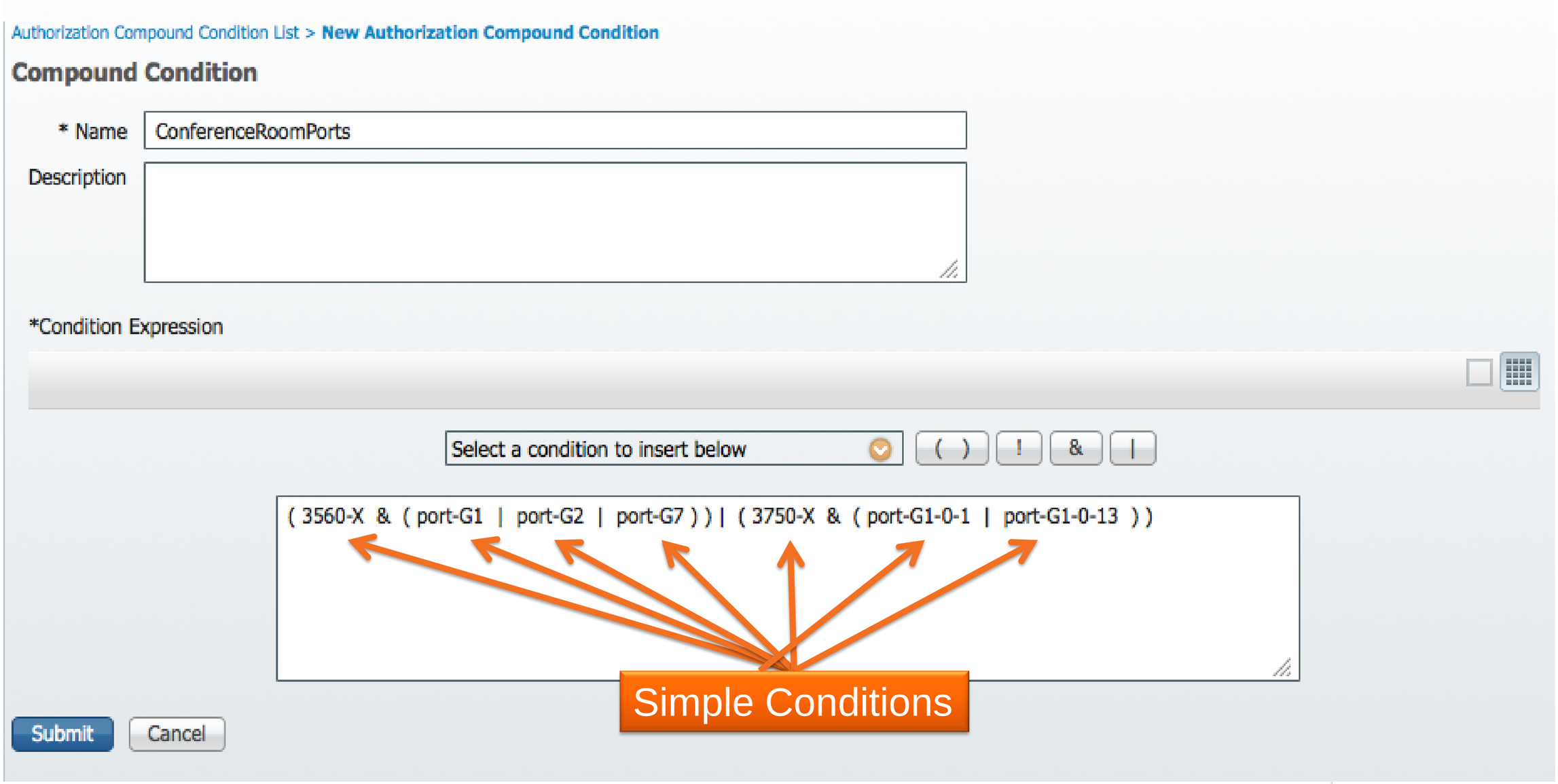
Combining AND with OR in AuthZ Policies

Advanced Editing



Combining AND with OR in AuthZ Policies

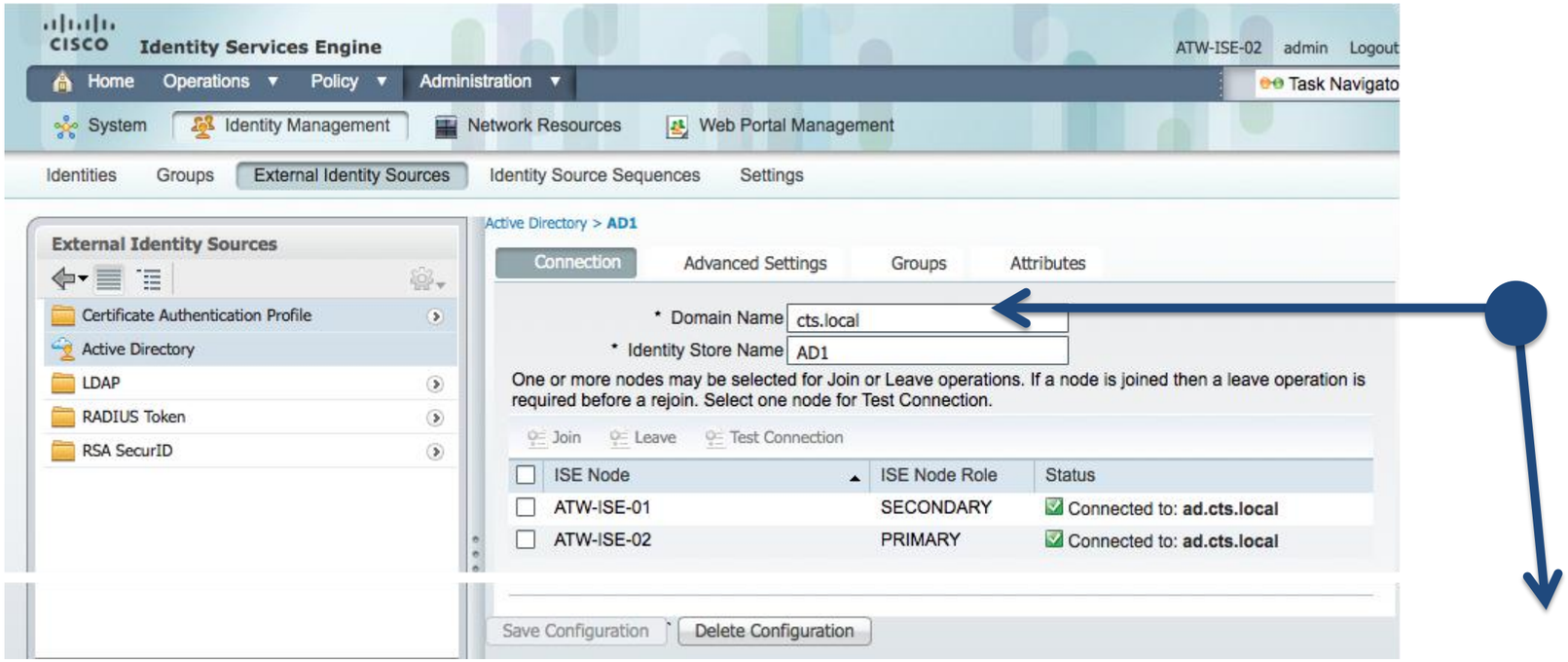
Advanced Editing



Multiple Active – Directory Domains

ISE joins the AD Domain

It may only be a member of a single domain



Active Directory Integration

Multiple Domains

If Trust Relationship(s) Exist

- Then only need to join one domain.

Use When Possible

If no Trust Relationships

- Complicated. Depends on Authentication Requirements & EAP Methods.
- One option: LDAP
- Other option: RADIUS-Proxy

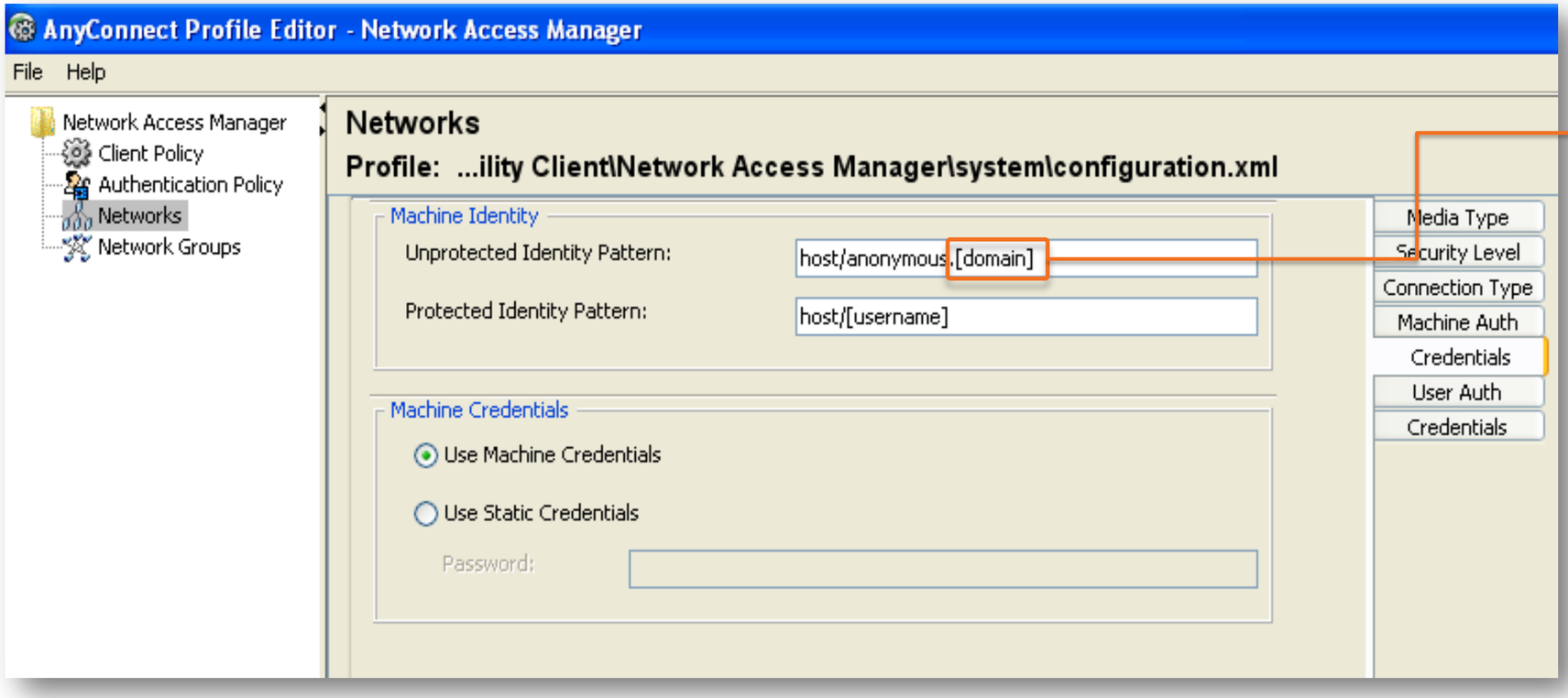
Multiple Active Directory Domains

LDAP

- Key Points:
  - MSCHAPv2 does not work with LDAP, however: EAP-GTC Does.
  - EAP-GTC was removed from the Native Supplicant on Microsoft

Multi-AD Support w/ AnyConnect

Add [domain] to Outer Identity

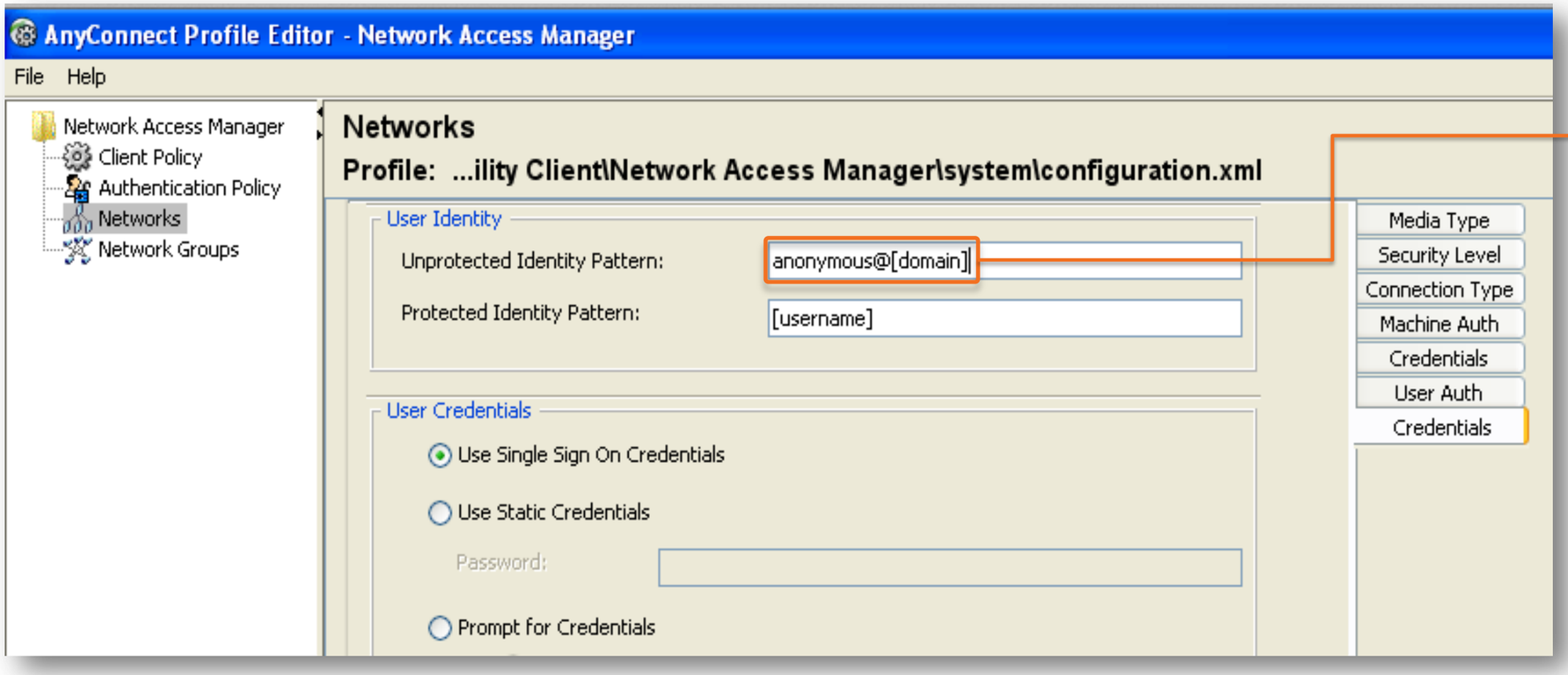


AD Domain Variable

Host/anonymous.CTS.local

Multi-AD Support w/ AnyConnect

Add @[domain] to Outer Identity for Users



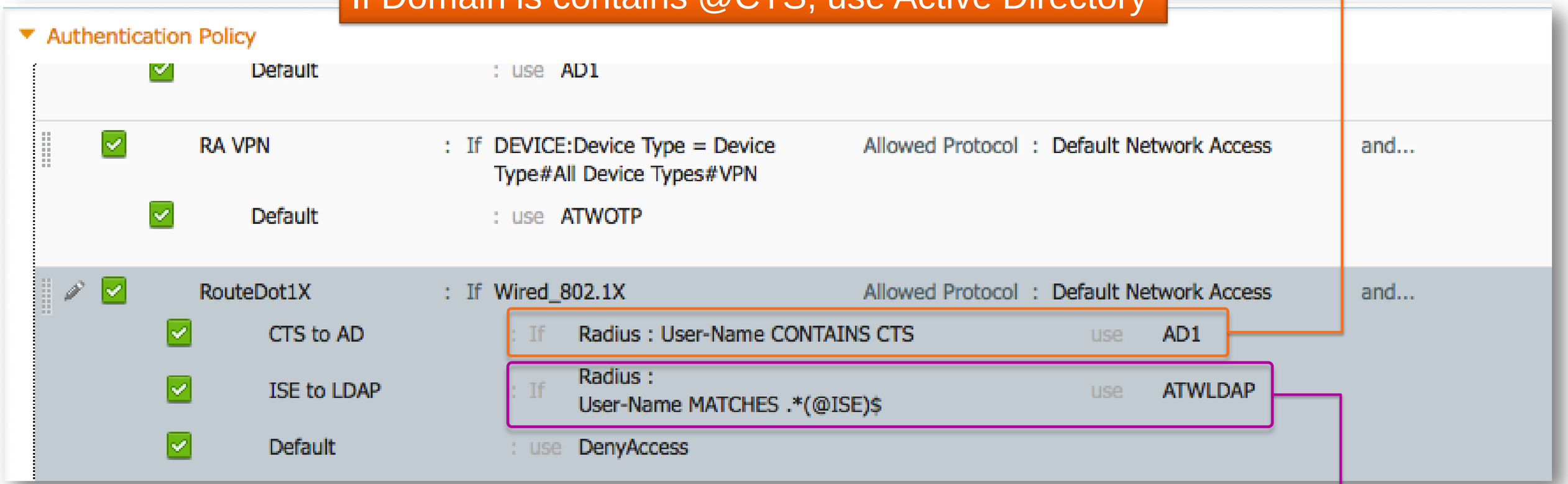
AD Domain Variable

anonymous@CTS.local

Multi-AD Support w/ AnyConnect

Add [domain] to Outer Identity

If Domain is contains @CTS, use Active Directory



If Domain is contains @ISE, use LDAP

What Works with LDAP

	Machine AuthC	Machine AuthZ	User AuthC	User AuthZ
EAP-TLS (port 389)	Yes	Yes, if comparing cert values (O,OU) Yes, if condition uses primary group id=515 (Domain Computers)	Yes	Yes*
EAP-TLS (port 3268)	Yes	Yes, if condition uses primary group id=515 (Domain Computers) Yes, if comparing cert values (O,OU)	Yes	Yes, must have cert published to AD *
PEAP-GTC (port 389)	No	No	Yes	Yes
PEAP-GTC (port 3268)	No	No	No	Yes

* If user belongs to “Domain Users” group only, must use primary group ID= 513 for authz rule

Troubleshooting Tools and Tips

Add in the new stuff we did to keep from installing root-patch & support bundle!!

- Show logging application
- Show logging system

Conditional Debugging

Tip from the Field

- On the WLC, we can debug on a per mac-address basis.

```
(Cisco Controller) >debug client b8:c7:5d:d4:95:32

(Cisco Controller) >
(Cisco Controller) >
(Cisco Controller) >*apfMsConnTask_1: Apr 10 19:02:04.179: b8:c7:5d:d4:95:32 Association received from
   mobile on AP 00:26:cb:4e:b2:d0
*apfMsConnTask_1: Apr 10 19:02:04.179: b8:c7:5d:d4:95:32 10.1.41.101 RUN (20) Changing IPv4 ACL
   'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1697)
*apfMsConnTask_1: Apr 10 19:02:04.179: b8:c7:5d:d4:95:32 10.1.41.101 RUN (20) Changing IPv6 ACL
   'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:1864)
*apfMsConnTask_1: Apr 10 19:02:04.179: b8:c7:5d:d4:95:32 apfApplyWlanPolicy: Retaining the ACL
   recieved in AAA attributes 255 on mobile
*apfMsConnTask_1: Apr 10 19:02:04.179: b8:c7:5d:d4:95:32 Applying site-specific Local Bridging override for
   station b8:c7:5d:d4:95:32 - vapId 1, site 'default-group', interface 'employee'
*apfMsConnTask_1: Apr 10 19:02:04.179: b8:c7:5d:d4:95:32 Applying Local Bridging Interface Policy for
   station b8:c7:5d:d4:95:32 - vlan 41, interface id 11, interface 'employee'
*apfMsConnTask_1: Apr 10 19:02:04.179: b8:c7:5d:d4:95:32 processSsidIE  statusCode is 0 and status is 0
```

Conditional Debugging

Tip from the Field

- No per mac-address debugging on switches, but:
  - We can enable per port rather than per mac.

```
3560-X#debug condition interface g0/1
Condition 1 set
3560-X#debug authentication all
All Auth Manager debugging is on
3560-X#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
3560-X(config)#int g0/1
3560-X(config-if)#shut
3560-X(config-if)#
*Mar 13 17:30:26.848: AUTH-EVENT (Gi0/1) Host access set to ask on unauthorized port since feature
*Mar 13 17:30:26.848: AUTH-EVENT (Gi0/1)  host access set to 1 on GigabitEthernet0/1
*Mar 13 17:30:26.848: AUTH-EVENT (Gi0/1) Setting domain DATA to UNATHED
*Mar 13 17:30:26.848: AUTH-EVENT (Gi0/1) dot1x_is_mab_interested_in_mac: Still waiting for a MAC on
   port GigabitEthernet0/1
*Mar 13 17:30:26.848: AUTH-EVENT (Gi0/1) Host access set to ask on unauthorized port since feature
*Mar 13 17:30:26.848:
```

Critical Items

Critical Items for an Operationally Efficient Environment

- Good, working DNS is a REQUIREMENT
  - Multiple TAC cases where customers don't have working DNS
  - I know: how is that possible, right? ☺
- All ISE nodes must have forward & reverse DNS Entries

Troubleshooting Redirection

- Verify IOS code release and feature set!

```
# show authentication session interface <int>
```

  - Does the IP address display? Verify device tracking table entry.
  - Is the session ID matching?
  - Is the dACL downloaded, if applicable?
  - Is the Redirect ACL applied? If so, verify contents on local switch

Troubleshooting Redirection

```
3560-X(config-if)#do sho authen sess int g0/1
 Interface:  GigabitEthernet0/1
        MAC Address:  0050.5687.0039
         IP Address:  10.1.41.100
          User-Name:  00-50-56-87-00-39
             Status:  Authz Success
             Domain:  DATA
    Security Policy:  Should Secure
    Security Status:  Unsecure

     Oper host mode:  multi-auth
   Oper control dir:  both
    Authorized By:  Authentication Server
       Vlan Group:  N/A
          ACS ACL:  xACSACLx-IP-WebAuthDACL-4f849c3e
  URL Redirect ACL:  ACL-WEBAUTH-REDIRECT
     URL Redirect:  https://ATW-ISE-
02.cts.local:8443/guestportal/gateway?sessionId=0A01283C0000003041DE089E&action=cwa
    Session timeout:  N/A
       Idle timeout:  N/A
  Common Session ID:  0A01283C0000003041DE089E
    Acct Session ID:  0x00000038
            Handle:  0xA3000030
```

```
3560-X(config-if)# do sho ip access-list int g0/1
    permit ip host 10.1.41.100 host 10.1.100.3
    permit ip host 10.1.41.100 host 10.1.100.4
    permit udp host 10.1.41.100 any eq domain (5 matches)
    permit tcp host 10.1.41.100 any eq 8443
    permit tcp host 10.1.41.100 any eq www
```

```
3560-X#sho run | b ip access-list extended ACL-WEBAUTH-REDIRECT
ip access-list extended ACL-WEBAUTH-REDIRECT
 deny   udp any any eq domain
 remark redirect all applicable traffic to the ISE Server
 permit tcp any any eq www
 permit tcp any any eq 443
 remark all other traffic will be implicitly denied from the redirection
```

Troubleshooting Redirection

- **`# show ip access-list interface <int>`**
  - Is the access list properly applied to the client IP address per above? If not…
    - Verify that endpoint has an IP address
    - Verify dACL contents in ISE—ISE may show dACL authorisation applied but switch rejects if ANY syntax error
- Access switch without SVIs for local access VLANs (common L2 case)
  - Is there a route from Management VLAN to client VLAN?
  - Is firewall dropping redirects sourced from Management VLAN?
  - Are dACLs disappearing? If so, does host respond to ARP probes from 0.0.0.0?
    - `Switch(config-if)# ip device tracking probe use-svi`

Wireless URL Redirection Considerations

Apple Captive Network Assistant (CNA)

- Problem: URL redirection on Apple devices may fail due to Apple Captive Network Assistant (CNA)
- Background on CNA:

  Apple iOS feature to facilitate network access when captive portals present that requires login by automatically opening web browser in a controlled window. Feature attempts to detect the presence of captive portal by sending a web request upon WiFi connectivity to http://www.apple.com/library/test/success.html

  – If response received, then Internet access assumed and no further interaction

  – If no response received, Internet access is assumed to be blocked by captive portal and CNA auto-launches browser to requests portal login in a controlled window.

- Solutions:

  1. Disable Auto-Login under WLAN settings (requires user knowledge and interaction)
  2. Configure WLC to bypass CNA:

     ```
     > config network web-auth captive-bypass enable
     ```

     Command available in WLC 7.2:
     http://www.cisco.com/en/US/docs/wireless/controller/7.2/command/reference/cli72commands.html#wp15129591

More Common Problems

Common Problems

Password timeout & lockout of built-in admin account

- Password timeout/lockout of built-in admin?
  - The admin account defaults to lock out after 45 days without a password change.

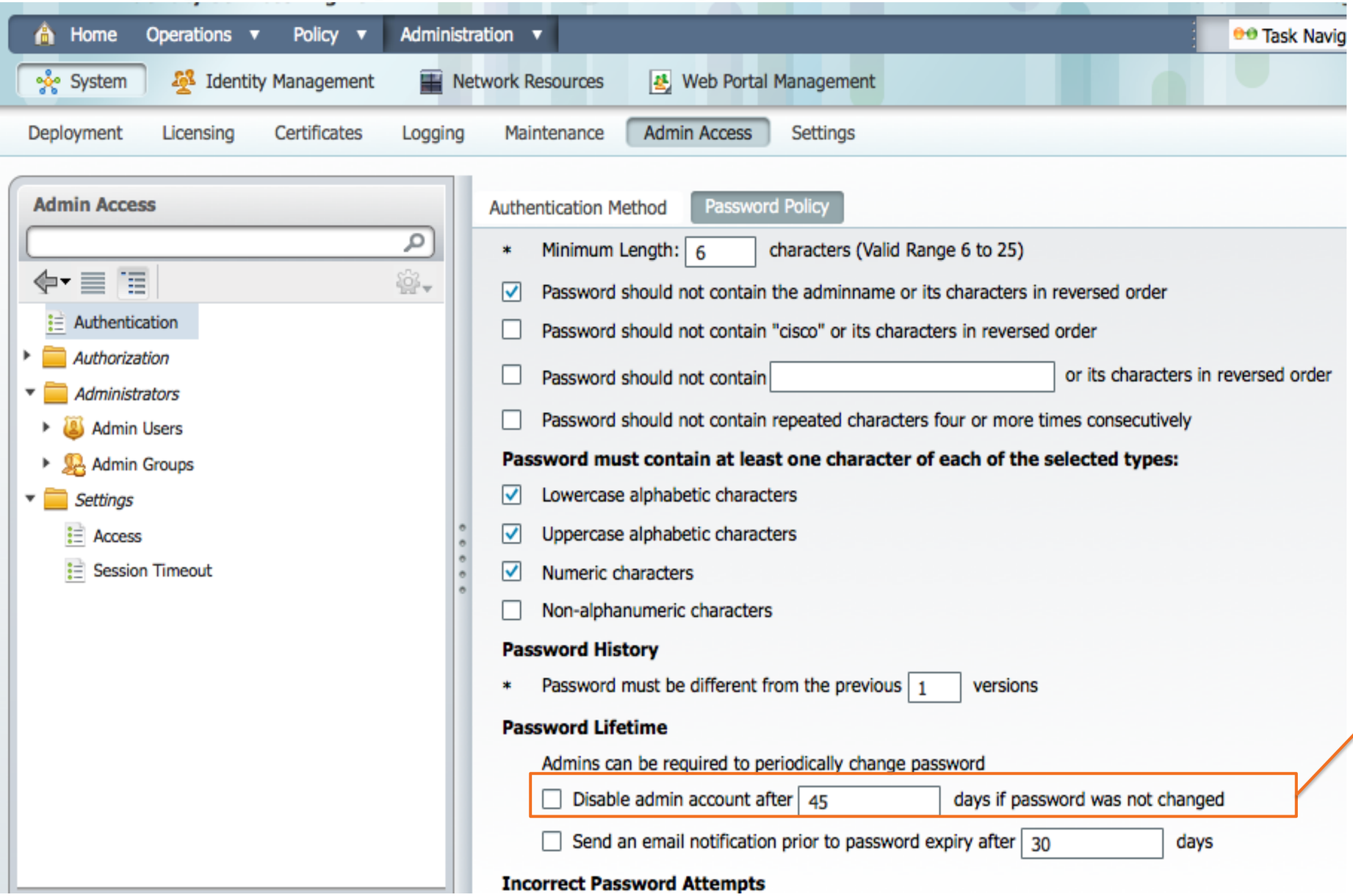
    Many customers have setup ISE and left it to run, not logging into the interface in a “while”.

    They have called me to get password recovery instructions. ☺
  - If your policy allows: disable the built-in account lockout.

```
d$ ssh admin@172.25.73.95
admin@172.25.73.95's password:
Last login: Fri Apr  6 03:58:25 2012 from 10.154.13.123
ATW-ISE-02/admin# application reset
reset-config  reset-passwd
ATW-ISE-02/admin# application reset-passwd ise ?
  <WORD>  Username for which password is to be reset (Max Size - 64)

ATW-ISE-02/admin# application reset-passwd ise admin
```

Common Problems



The default admin account settings.

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww

Cisco live!