TOMORROW starts here.

cisco

Cisco live!

Advanced ISE and Secure Access Deployment

BRKSEC 3045

Hosuk Won
CCIE # 22231
Technical Marketing Engineer

Cisco live!

Abstract

2012 and 2013 have been very busy years with the adoption of Cisco¹s 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.

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

Hosuk Won, CCIE# 22231

Technical Marketing Engineer
Secure Access & Mobility Product Group

howon@cisco.com

This Presentation Contains a Culmination of Best Practices and Tips from Many Technologists

Special Thanks to:
Aaron Woland, Craig Hyps,
Jason Frazier, Shelly Cadora, Jay Cedrone, Darrin Miller
& the entire Secure Access & Mobility Product Team





Agenda

- Certificates, Certificates, Certificates
- NAD Configuration and Logging
- Phased Deployments
- Profiling
- High Availability & Deployment Considerations
- Tips and Tricks
- Non-Cisco Network Integration

Important: Hidden Slide Alert

Look for this “For Your Reference” Symbol in your PDF’s

There is a tremendous amount of hidden content, for you to use later!

For Your Reference




ISE and Certificate Usage

Where are Certificates Used with ISE?

All Web Portals (Admin, WebAuth, MyDevices, Sponsor, CPP, etc.)

Client/Browser

NAD

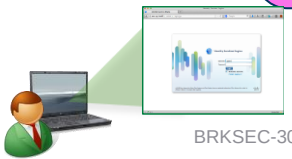
ISE

Step 1: Initiate Request to Establish HTTPS Tunnel with Portal (https://ISE/admin)

Step 2: Certificate sent to Browser

Step 3: User is Prompted to Accept Certificate.
After, it is Stored in Browser, KeyChain, or Trusted Store

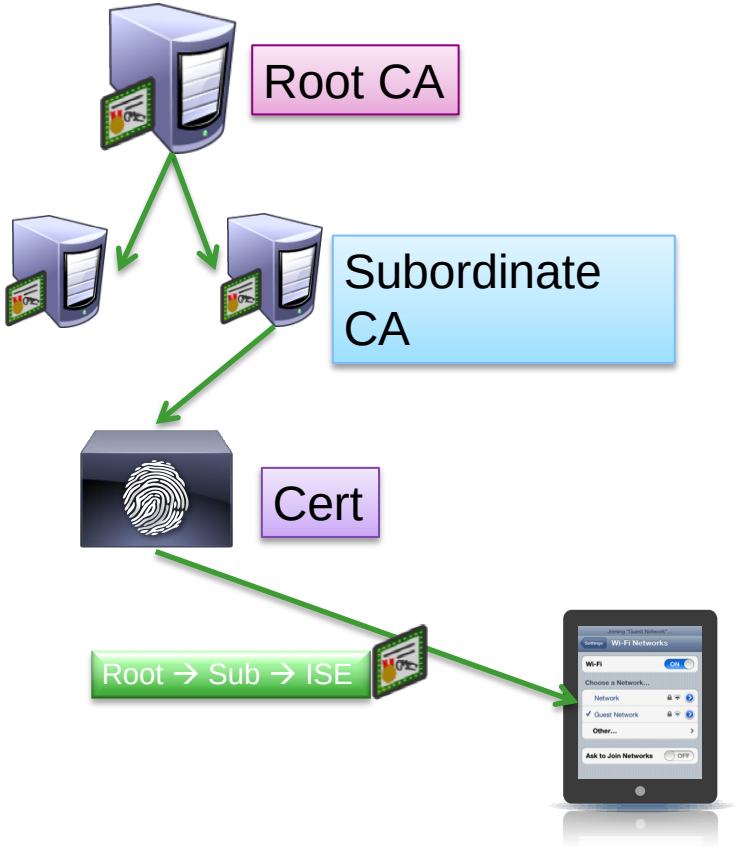
Step 4: TLS Tunnel is Formed, Encrypting the HTTP Communications (HTTPS)



Where are Certificates Used with ISE?

EAP Connections (PEAP, FAST, EAP-TLS)

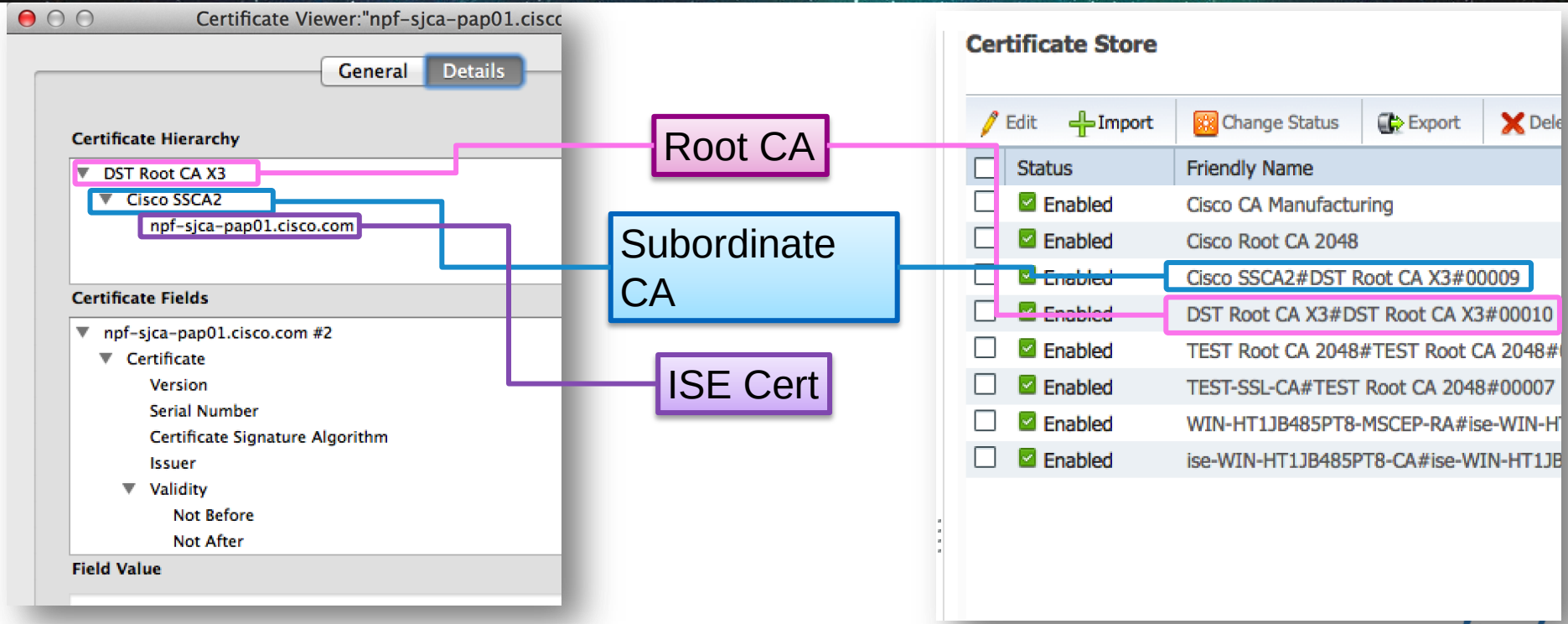
Certificate Chains



- 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)

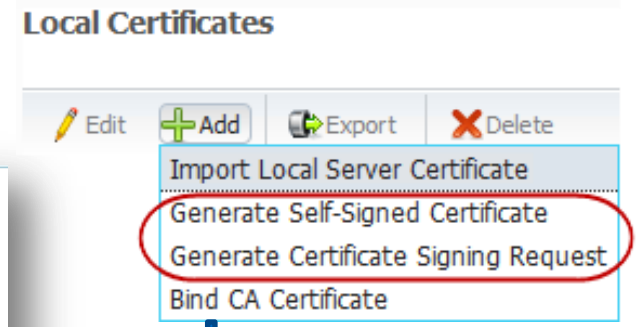


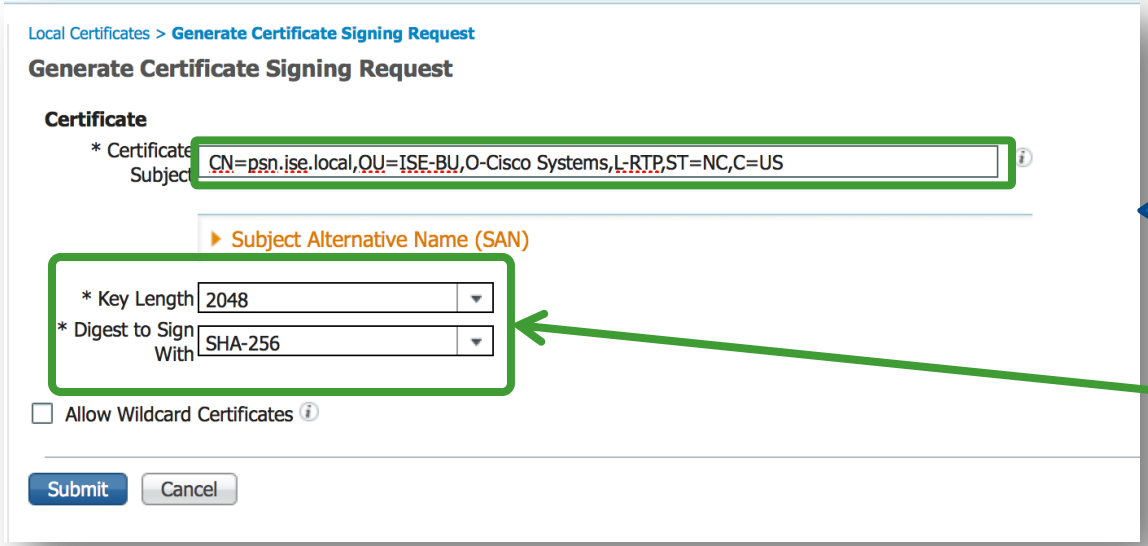
If you must use a PKCS chain, it needs to be in PEM format (not DER)

ISE Certificates and Custom Attributes

Basic Subject Name Attributes

- Add Self Signed Cert / CSR with specified attributes:



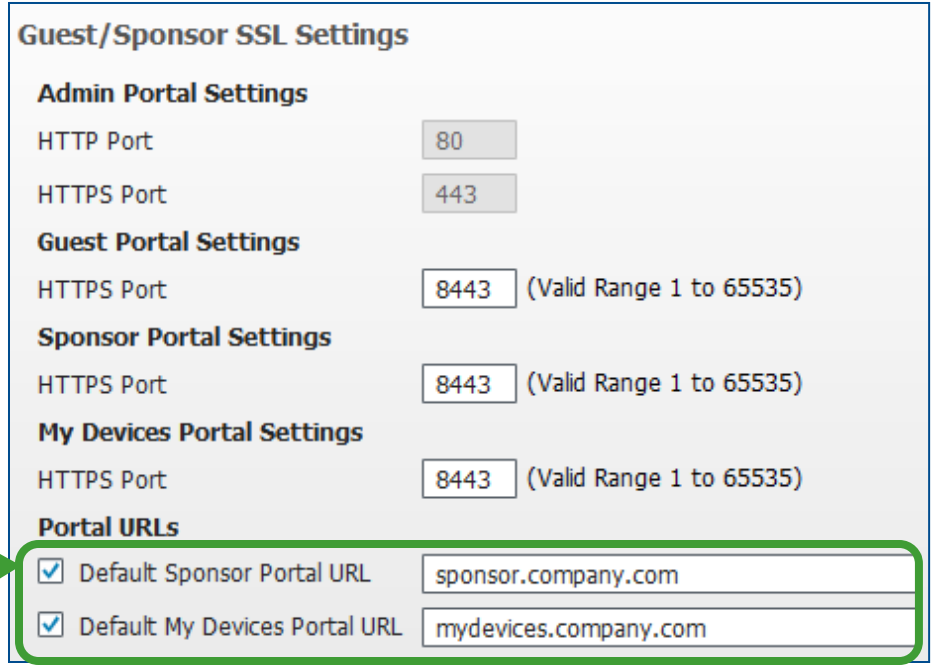


Customise other attributes as needed

Simple URL for Sponsor / My Devices Portal

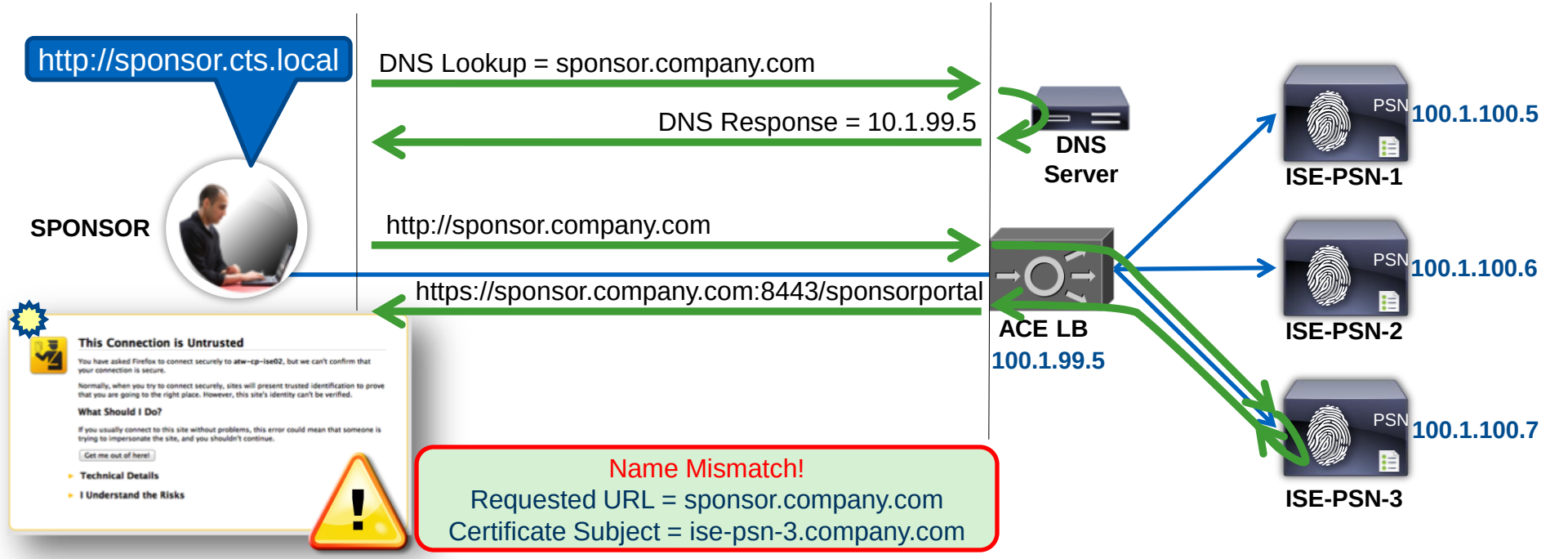
- Sponsor Portal and My Devices Portal can be accessed via a user-friendly URL and selectable port.
- Ex: http://sponsor.company.com

  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.*



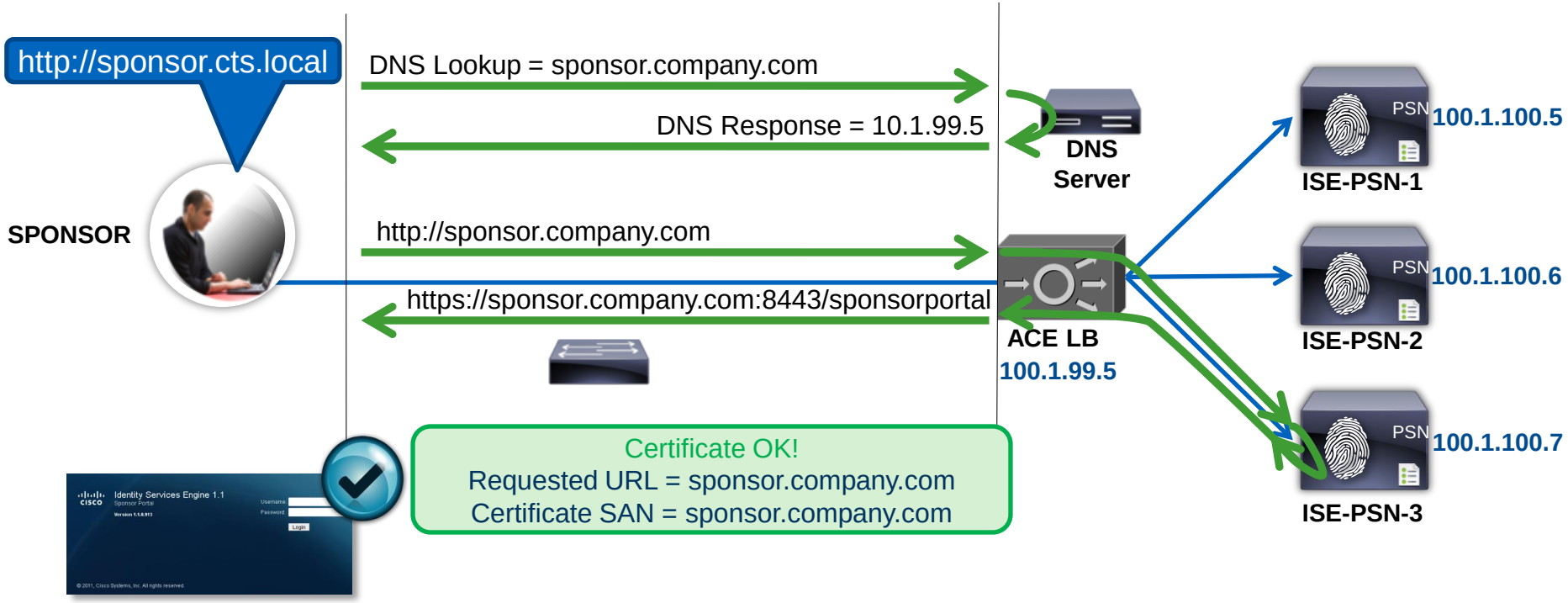
ISE Certificate without SAN

Certificate Warning - Name Mismatch



ISE Certificate with SAN

No Certificate Warning



ISE Certificate with SAN

Built Into ISE 1.2

Local Certificates > Generate Certificate Signing Request

Generate Certificate Signing Request

Certificate

* Certificate Subject: CN=psn.ise.local,OU=ISE-BU,O-Cisco Systems,L-RTP,ST=NC,C=US

Subject Alternative Name (SAN)

DNS Name	psn.ise.local
DNS Name	sponsor.ise.local
DNS Name	mydevices.ise.local
IP Address	10.1.103.5

* Key Length: 2048

* Digest to Sign With: SHA-256

☐ Allow Wildcard Certificates

Submit | Cancel

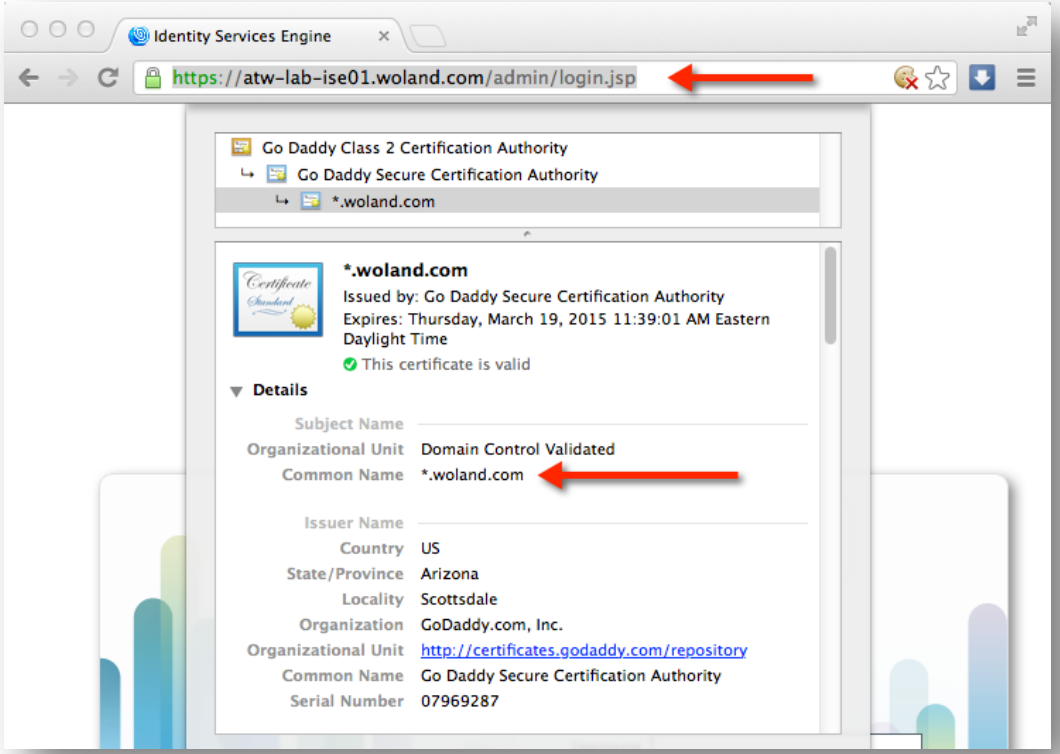
CN must also exist in SAN

Other FQDNs as “DNS Names”

IP Address is also option

ISE Certificate with SAN

Wildcard Certificates



- Wildcard Certificates are used to identify any secure web site that is part of the domain:
  - e.g.: *.woland.com works for:
    - www.woland.com
    - mydevices.woland.com
    - sponsor.woland.com
    - AnyThingIWant.woland.com

ISE Certificate with SAN

Wildcard Certificates – Why use with ISE?

Use of all portals & friendly URL's without Certificate Match Errors.

Most Importantly: Ability to host same certificate on all ISE PSNs

- Why, you ask?.....

Clients Misbehave!

- Example education customer:
  - ONLY 6,000 Endpoints (all BYOD style)
  - 10M Auths / 9M Failures in a 24 hours!
  - 42 Different Failure Scenarios – all related to clients dropping TLS (both PEAP & EAP-TLS).
- Supplicant List:
  - Kyocera, Asustek, Murata, Huawei, Motorola, HTC, Samsung, ZTE, RIM, SonyEric, ChiMeiCo, Apple, Intel, Cybertan, Liteon, Nokia, HonHaiPr, Palm, Pantech, LgElectr, TaiyoYud, Barnes&N
- 5411 No response received during 120 seconds on last EAP message sent to the client
  - This error has been seen at a number of Escalation customers
  - Typically the result of a misconfigured or misbehaving supplicant not completing the EAP process.

Recreating the Issue

What is the spouse factor? when this was completed In the kitchen!! ☺

Recreating the Issue

Cisco Cius	Android 2.2.2 / Kernel 2.6.31.6-mrst
Galaxy Player	Android 2.3.5 / Kernel 2.6.35.7
Galaxy TAB 10.1	Android 4.0.4 / Kernel 3.1.10
Galaxy Tab 2	Android 4.1.1 / Kernel 3.0.31
Acer A110 Tab	Android 4.1.2 / Kernel 3.1.10
Google Nexus7	Android 4.2.2 / Kernel 3.1.10-g05b777c
iPod Touch 1Gen	iOS 3.1.3 (7E18)

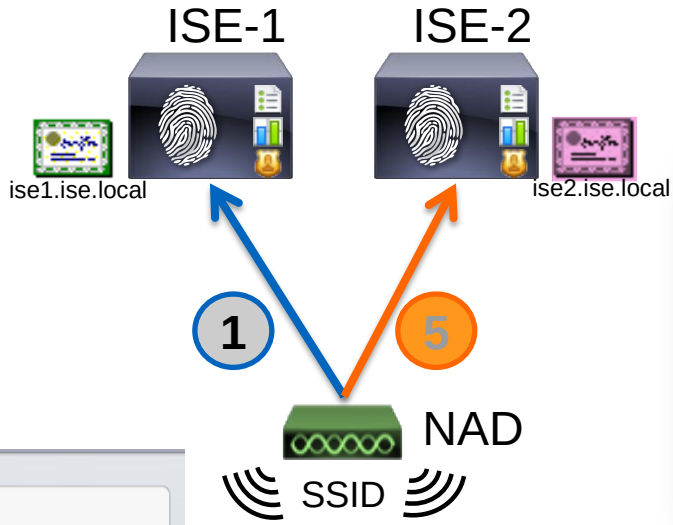
iPad1	iOS 5.1.1 (9B206)
iPad2	iOS 6.0.1 (10A523)
iPad Mini	iOS 6.1.2 (10B146)
iPhone 4	iOS 6.0 (10A403)
iPhone 5	iOS 6.1.3 (10B329)
Nook HD	Nook 2.1.0

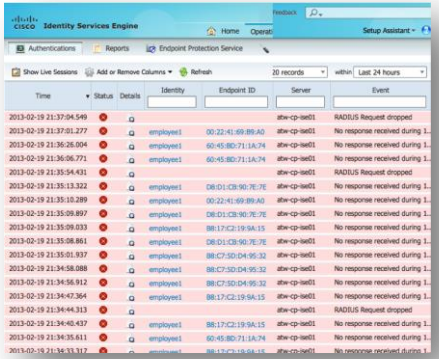
MacBook Pro 17	OSX 10.7.5
MacBook Air	OSX 10.8.2 (12C30006)
Kindle Fire HD	Version 7.3.0_user_3013320
Microsoft Surface	WindowsRT
Win7 Native	Windows7 Ultimate ServicePack1
WinXP Native	WindowsXP SP3
Windows 8 Native	Windows 8 Native Supplicant

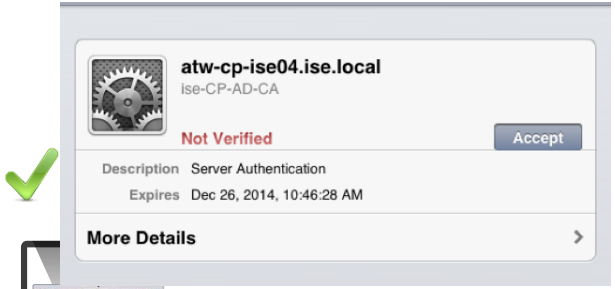
Clients Misbehave: Apple Example

- Multiple PSNs
- Each Cert signed by Trusted Root
- Apple Requires Accept on all certs!
  - Results in 5411 / 30sec retry

Cert Authority





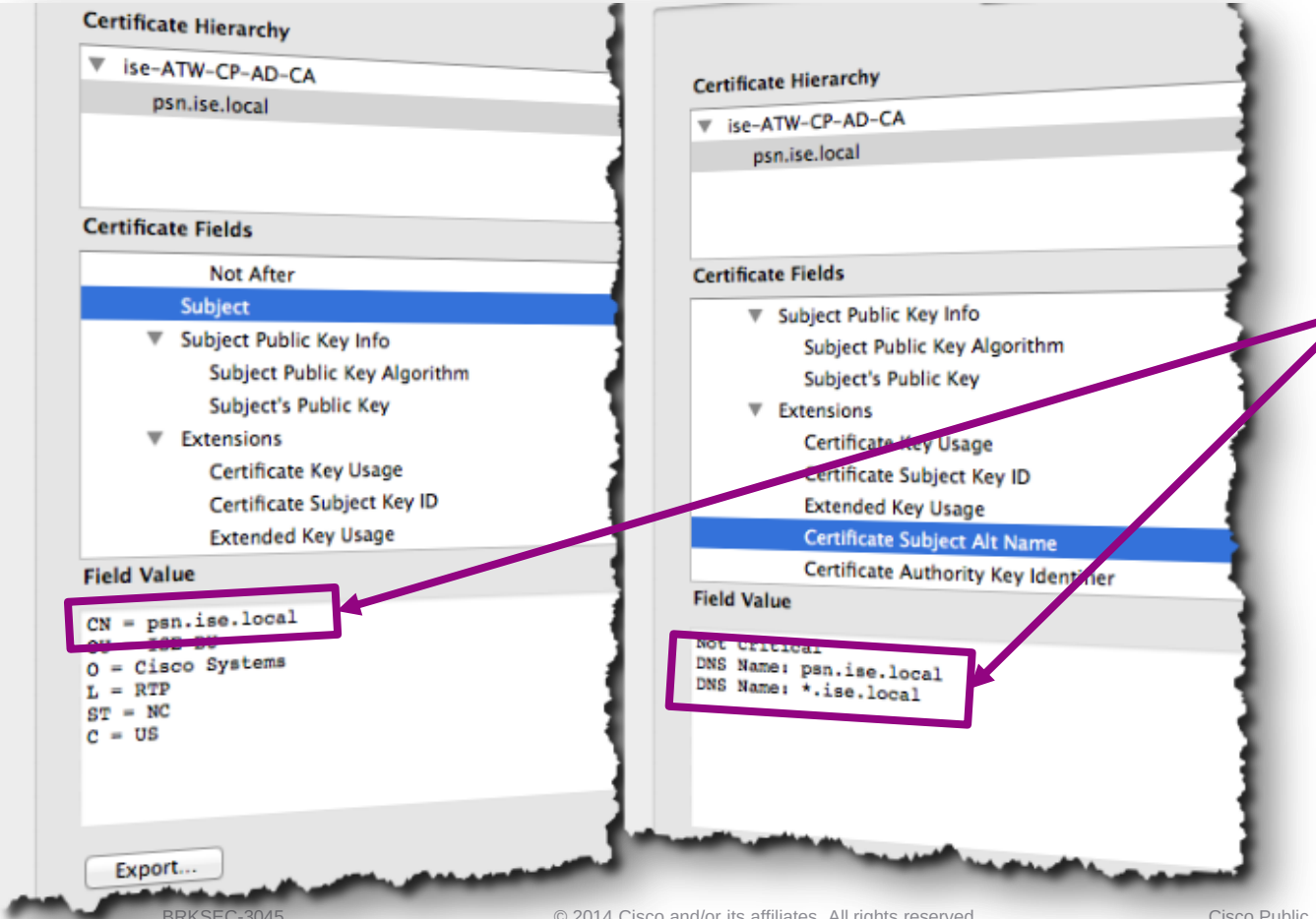


Apple iOS & MacOS

WiFi Profile

1. Authentication goes to ISE-1
2. ISE-1 sends certificate
3. Client trusts ISE-1
4. Client Roams
5. Authentication goes to ISE-2
6. Client Prompts for Accept

Solution: Common Cert, Wildcard in SAN

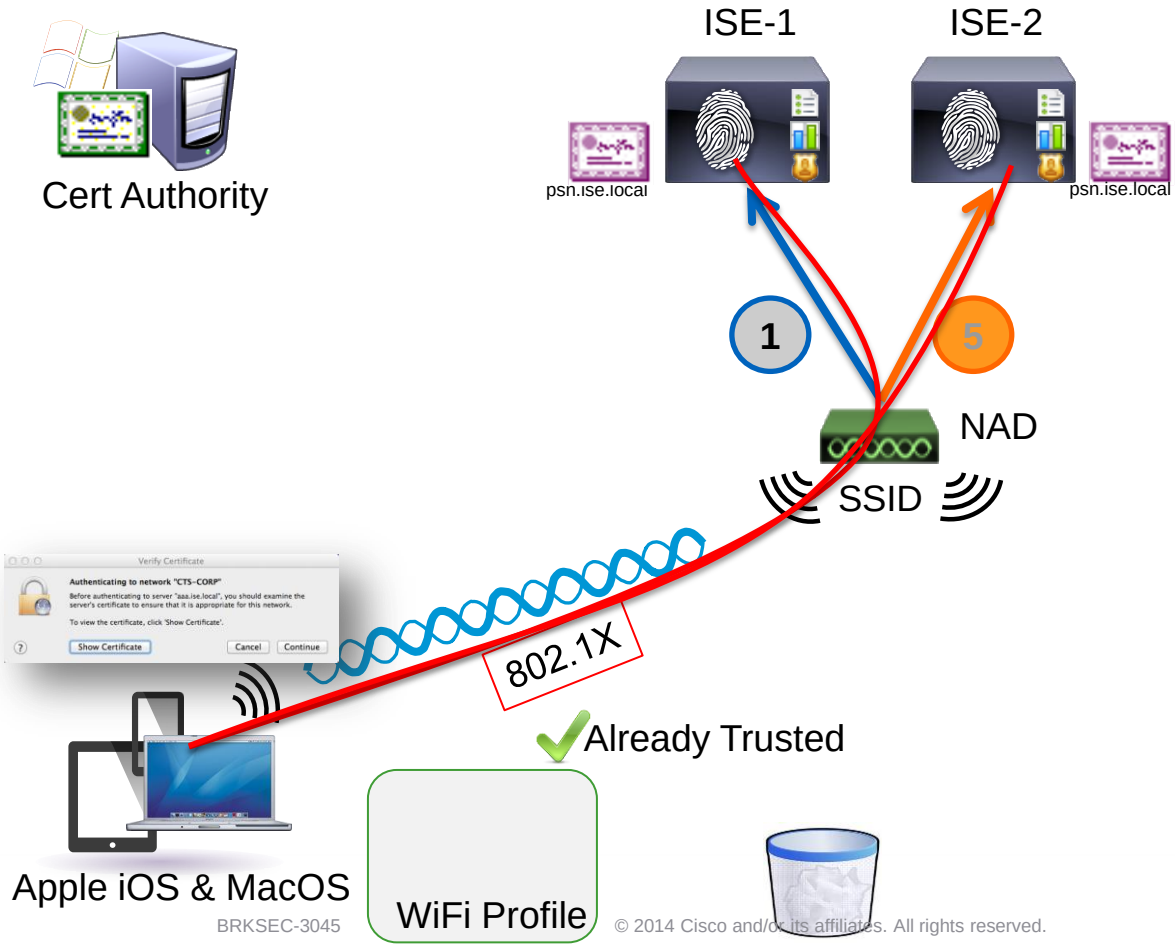


Allows anything ending with The Domain Name.

-

Same EXACT Priv / Pub Key May be installed on all PSNs

Solution: Common Cert, Wildcard in SAN



- CN= psn.ise.local
- SAN contains all PSN FQDNs
  - psn.ise.local
  - *.ise.local
- Tested and works with:
  comodo.com CA
  SSL.com CA
  Microsoft 2008 CA
- Failed with: GoDaddy CA
  -- they don't like * in SAN
  -- they don't like non-* in CN

1. Authentication goes to ISE-1
2. ISE-1 sends certificate
3. Client trusts ISE-1
4. Client Roams
5. Authentication goes to ISE-2
6. Client Already Trusts Cert

Test Results

Device	PEAP	Onboarding	EAP-TLS	Details
Cisco Cius	Y	NA	NA	Android 2.2.2 / Kernel 2.6.31.6-mrst
Galaxy Player	Y	Y	Y	Android 2.3.5 / Kernel 2.6.35.7
Galaxy TAB 10.1	Y	Y	Y	Android 4.0.4 / Kernel 3.1.10
Galaxy Tab 2	Y	Y	Y	Android 4.1.1 / Kernel 3.0.31
Acer A110 Tab	Y	Y	Y	Android 4.1.2 / Kernel 3.1.10
Google Nexus7	Y	Y	Y	Android 4.2.2 / Kernel 3.1.10-g05b777c
iPod Touch 1Gen	Y	NA	NA	iOS 3.1.3 (7E18)
iPad1	Y	Y	Y	iOS 5.1.1 (9B206)
iPad2	Y	Y	Y	iOS 6.0.1 (10A523)
iPad Mini	Y	Y	Y	iOS 6.1.2 (10B146)
iPhone 4	Y	Y	Y	iOS 6.0 (10A403)
iPhone 5	Y	Y	Y	iOS 6.1.3 (10B329)
Nook HD	Y	Y	Y	Nook 2.1.0
MacBook Pro 17	Y	Y	Y	OSX 10.7.5
MacBook Air	Y	Y	Y	OSX 10.8.2 (12C30006)
Kindle Fire HD	Y	NA	NA	Version 7.3.0_user_3013320
Microsoft Surface	Y	NA	NA	WindowsRT
Win7 Native	Y	Y	Y	Windows7 Ultimate ServicePack1
WinXP Native	Y	Y	Y	WindowsXP SP3
Windows 8 Native	Y	Y	Y	Windows 8 Native Supplicant




NAD Configuration and Logging

Challenge: How to reduce the flood of log messages while increasing PSN and MNT capacity and tolerance

Getting More Information With Less Data

Scaling to Meet Current and Next Generation Logging Demands

Rate Limiting at Source

Reauth period
Quiet-period
Held-period / Exclusion Time

Heartbeat Frequency

Reauth phones

Unknown users

Switch

Quiet period

Quiet Period

WLC

Client Exclusion

Roaming supplicant

Misbehaving supplicant

LB

LB Health probes

Filtering at Receiving Chain

Detect and reject misbehaving clients

Log Filter

Reject bad supplicant

PSN

Filter health probes from logging

MNT

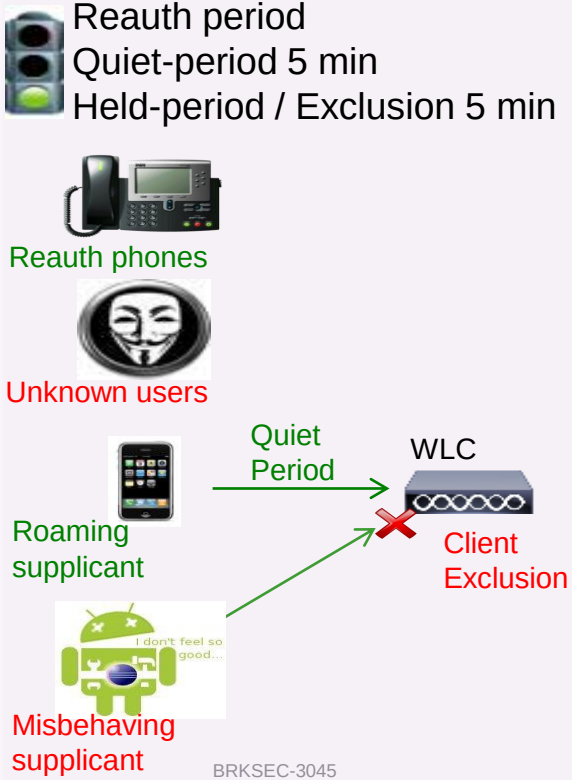
Count and discard repeated events

Count and discard untrusted events

Count and discard repeats and unknown NAD events

Tune NAD Configuration

Rate Limiting at **Wireless** Source



Wireless (WLC)

- **RADIUS Server Timeout:** Increase from default of 2 to 10 sec
- **RADIUS Aggressive-Failover:** Disable aggressive failover
- **RADIUS Interim Accounting:** Set to 15+ min (900+ sec)
- **Idle Timer:** Disable or increase to 1 hour (3600 sec)
- **Session Timeout:** Disable or increase to 2+ hours (7200+ sec)
- **Client Exclusion:** Enable and set exclusion timeout to 300+ sec
- **Roaming:** Enable CCKM / SKC / 802.11r (when feasible)
- **Bugfixes:** Upgrade WLC software to address critical defects

Tune NAD Configuration

Rate Limiting at **Wired** Source

Reauth period
Quiet-period 5 min
Held-period / Exclusion 5 min

Reauth phones

Switch

Quiet Period

Unknown users

Roaming supplicant

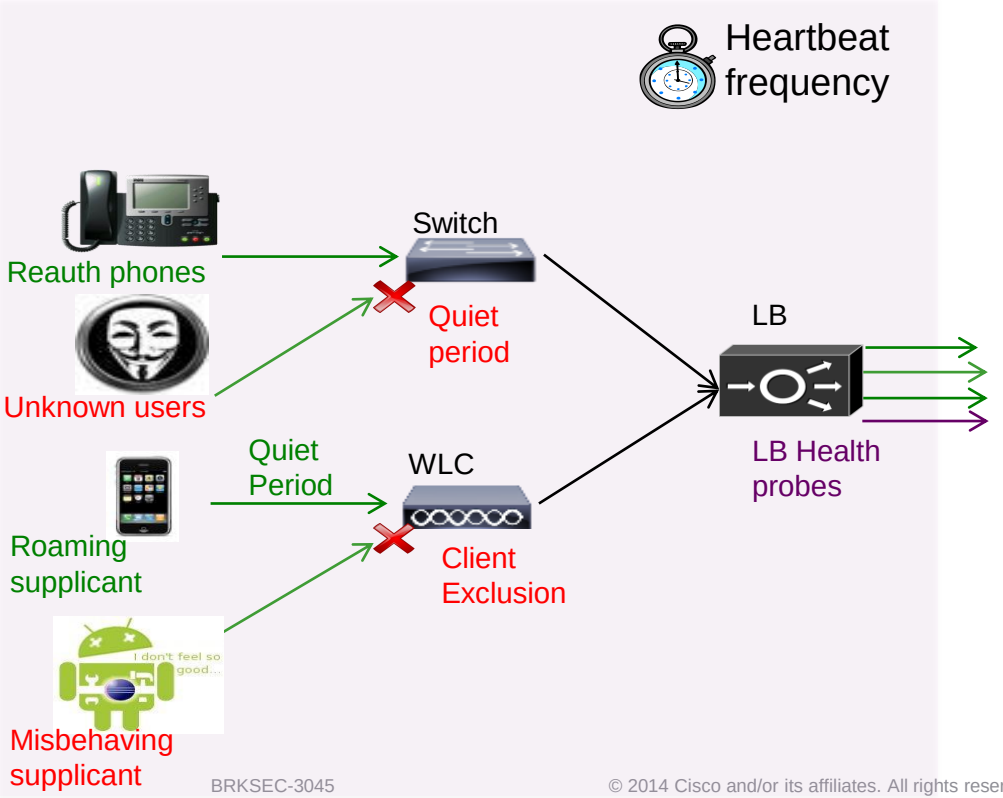
Misbehaving supplicant

Wired (IOS / IOS-XE)

- **RADIUS Interim Accounting:** Recommend 15+ mins (900+ sec)
  - Use *newinfo* parameter if available.
- **802.1X Timeouts**
  - held-period: Increase to 300+ sec
  - quiet-period: Increase to 300+ sec
  - ratelimit-period: Increase to 300+ sec
- **Inactivity Timer:** Disable or increase to 2+ hours (7200+ sec)
- **Session Timeout:** Disable or increase to 2+ hours (7200+ sec)
- **Reauth Timer:** Disable or increase to 2+ hours (7200+ sec)
- **Bugfixes:** Upgrade software to address critical defects.

RADIUS Test Probes

Reduce Frequency of RADIUS Server Health Checks

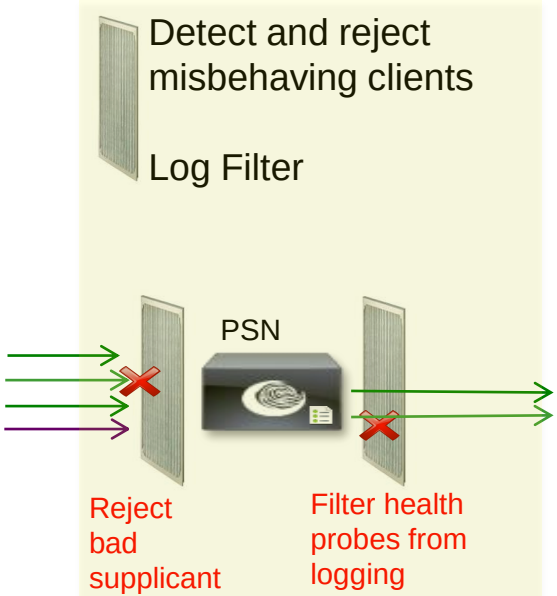


- **Wired NAD**: RADIUS test probe interval set with **idle-time** parameter in radius-server config; Default is 60 minutes
  - No action required
- **Wireless NAD:** If configured, WLC only sends “active” probe when server marked as dead.
  - No action required
- **Load Balancers:** Set health probe intervals and retry values short enough to ensure prompt failover to another server in cluster occurs prior to NAD RADIUS timeout (typically 45-60 sec.) but long enough to avoid excessive test probes.

PSN Noise Suppression and Smarter Logging

Filter Noise and Provide Better Feedback on Authentication Issues

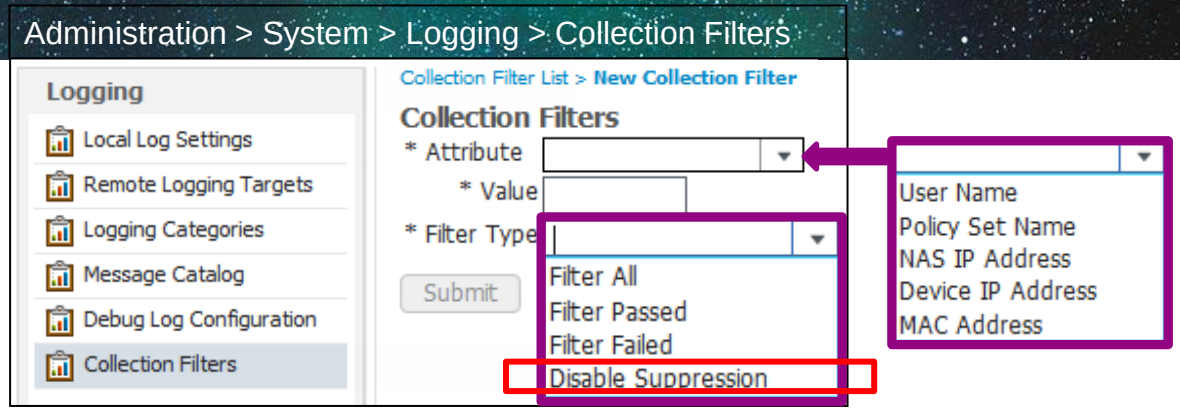
- PSN Collection Filters
- PSN Misconfigured Client Dynamic Detection and Suppression
- PSN Accounting Flood Suppression
- Detect Slow Authentications
- Enhanced Handling for EAP sessions dropped by supplicant or Network Access Server (NAS)
- Failure Reason Message and Classification
- Identify RADIUS Request From Session Started on Another PSN
- Improved Treatment for Empty NAK List

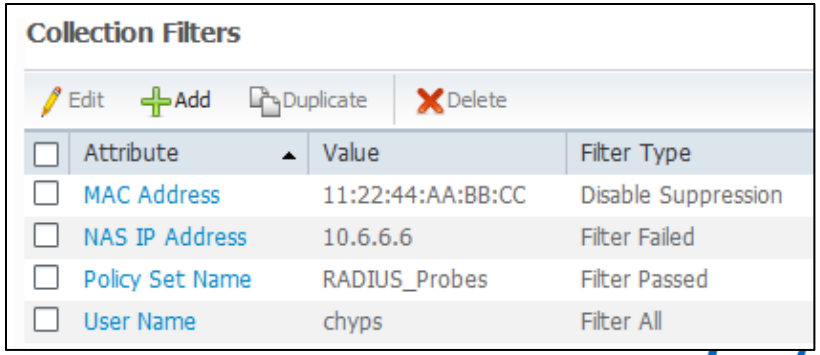


PSN - Collection Filters

Static Client Suppression

- PSN static filter based on single attribute:
  - User Name
  - Policy Set Name
  - NAS-IP-Address
  - Device-IP-Address
  - MAC (Calling-Station-ID)
- Filter Messages Based on Auth Result:
  - All (Passed/Fail)
  - All Failed
  - All Passed
- Select Messages to **Disable Suppression** for failed auth @PSN and successful auth @MnT





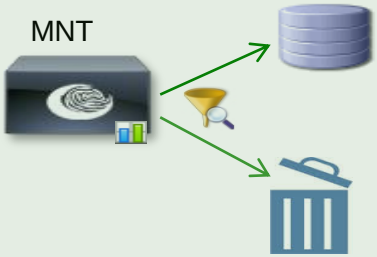
MnT Log Suppression and Smarter Logging

Drop and Count Duplicates / Provide Better Monitoring Tools

- Drop duplicates and increment counter in Live Log for “matching” passed authentications
- Display repeat counter to Live Sessions entries.
- Log RADIUS Drops and EAP timeouts to separate table for reporting purposes and display as counters on Live Log Dashboard along with Misconfigured Supplicants and NADs
- Alarm enhancements
- Revised guidance to limit syslog at the source.
- MnT storage allocation and data retention limits
- More aggressive purging
- Support larger VM disks to increase logging capacity and retention.

Count and discard repeated events

Count and discard untrusted events



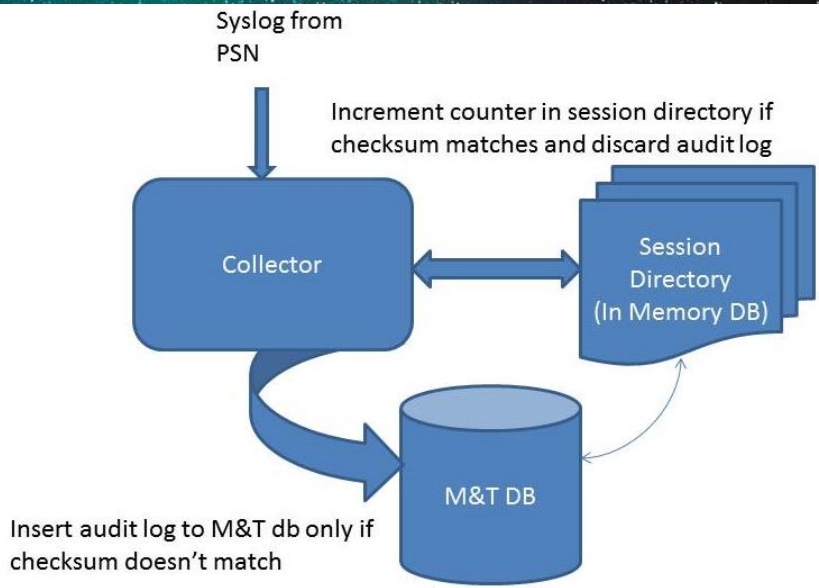
Count and discard repeats and unknown NAD events

MnT Duplicate Passed Auth Suppression

Drop and Count Duplicates

- Unique session entries determined by hash created based on these attributes:
  - **Called Station Id**
  - **User Name**
  - **Posture Status**
  - **CTS Security Group**
  - **Authentication Method**
  - **Authentication Protocol**
  - **NAS IP Address**
  - **NAS Port Id**
  - **Selected Authorisation Profile**

5eaf59f1e6cd6aa6113ca1463c779c3f (MD5 hash)



- "Discard duplicate" logic not applicable to failed auths as these are not cached in session
- RADIUS Accounting (Interim) updates are dropped from storage, but do update session

Live Authentications Log

Dashboard Counters

Drill Down on counters to see details

Identity Services Engine

Home | Operations | ▾ | Policy | ▾ | Administration | ▾

admin | Logout | Feedback

Setup Assistant ▾

Authentications | Reports | Endpoint Protection Service | Troubleshoot

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	392	6	9

Show Live Sessions | Add or Remove Columns ▾ | Refresh

Refresh Every 1 minute | Show Latest 20 records | within Last 24 hours

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server	Event
2013-04-02 15:34:18.963	✓		radtest-w			wlc5508		RADIUS_Probes		NotApplicable	ise-pan2	Authentication succeeded
2013-04-02 15:31:18.884	✓		radtest-w			wlc5508		RADIUS_Probes		NotApplicable	ise-pan2	Authentication succeeded
2013-04-02 14:06:30.332	✓		employee1	7C:6D:62:E3:D5:05		wlc5508		Employee,SGT_Emp..	Any,RegisteredDevi...	NotApplicable	ise-pan2	
2013-04-02 14:06:30.298	✓					wlc5508					ise-pan2	Dynamic Authorization su...
2013-04-02 14:06:29.988	✓		employee1	7C:6D:62:E3:D5:05	10.1.41.101				Any		ise-pan2	Guest Authentication Pas...
2013-04-02 14:06:03.549	✓		7C:6D:62:E3:D5:	7C:6D:62:E3:D5:05		wlc5508		Central_Web_Auth	RegisteredDevices	NotApplicable	ise-pan2	Authentication succeeded
2013-04-02 11:46:34.010	✓		1C:B0:94:A8:46:	1C:B0:94:A8:46:7A		wlc5508		Central_Web_Auth	Android	NotApplicable	ise-pan2	Authentication succeeded
2013-04-02 01:30:25.727	✓		employee1	7C:6D:62:E3:D5:05		wlc5508		Employee,SGT_Emp..	RegisteredDevices	NotApplicable	ise-pan2	Authentication succeeded
2013-04-02 01:28:56.023	✓		staff1	00:11:22:33:44:55		radping2		Central_Web_Auth	RegisteredDevices	NotApplicable	ise-pan2	Authentication succeeded
2013-04-02 01:11:34.484	✓		radtest-w			wlc5508		RADIUS_Probes		NotApplicable	ise-pan2	Authentication succeeded
2013-04-02 00:40:05.009	✓		radtest-w			wlc5508		RADIUS_Probes		NotApplicable	ise-pan2	Authentication succeeded
2013-04-01 23:26:13.801	✓		radtest-w			wlc5508		RADIUS_Probes		NotApplicable	ise-pan2	Authentication succeeded
2013-04-01 23:23:29.001	✓		employee1	7C:6D:62:E3:D5:05		wlc5508		Employee,SGT_Emp..	RegisteredDevices	NotApplicable	ise-pan2	Authentication succeeded

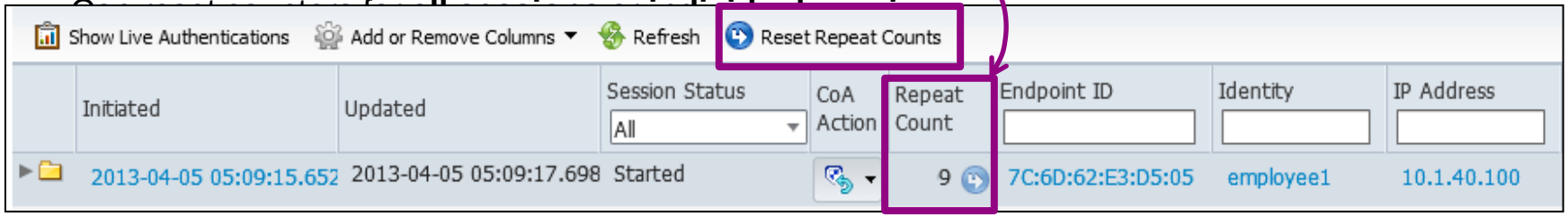
Repeat Counter

Successful Authentication Suppression

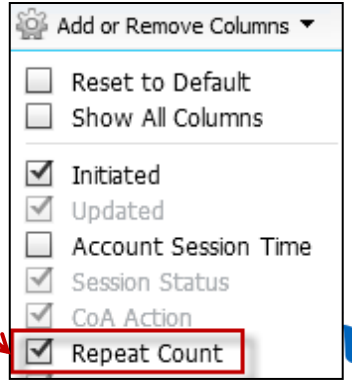
- Global Repeat Counter displayed in Live Authentications Log dashboard:

Repeat Counter
21587

- Session Repeat Counter displayed in Live Sessions Log



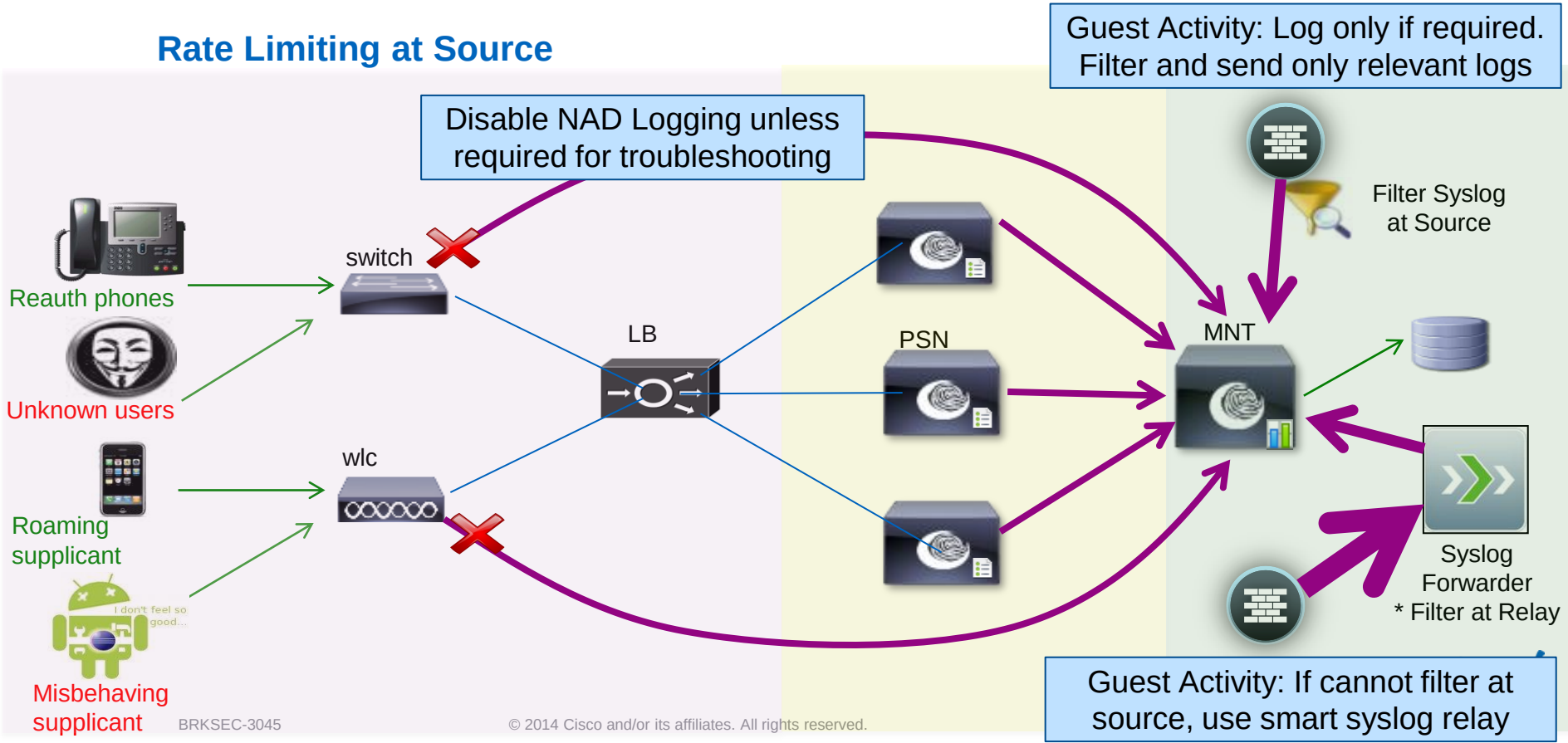
- Be sure to enable display under “Add or Remove Columns”



Minimise Syslog Load on MNT

Disable NAD Logging and Filter Guest Activity Logging

Rate Limiting at Source






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 reinitialize vlan 11
 authentication event server dead action authorize voice
 authentication event server alive action reinitialize
 authentication violation restrict
```

Good for Monitor Mode

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

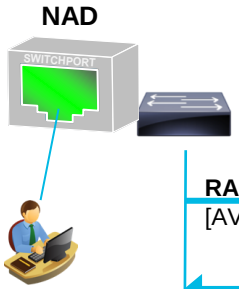
Dangerous for Monitor Mode

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	



No Supplicant

RADIUS Access-Request
[AVP: 00.0a.95.7f.de.06]

RADIUS Access-Reject

Matched Rule = Default

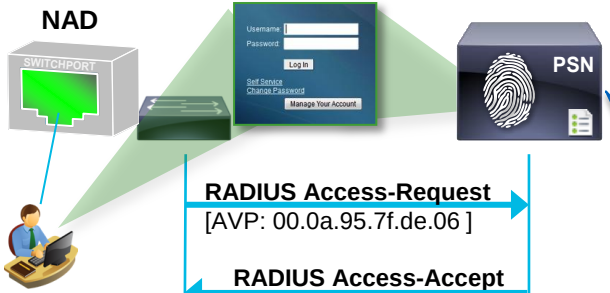
MAC-Addr is Unknown…
Continue to AuthZ table

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		



RADIUS Access-Request
[AVP: 00.0a.95.7f.de.06]

RADIUS Access-Accept
[AVP:url-redirect, dacl]

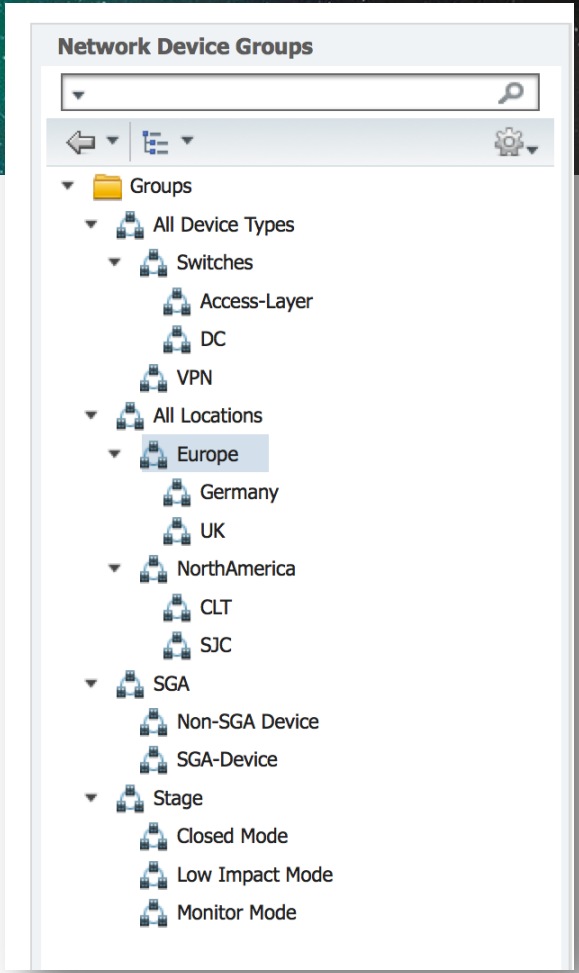
Matched Rule = Default

MAC-Addr is Unknown…
Continue to AuthZ table

Network Device Groups

Creation of many: Organise & Why use them

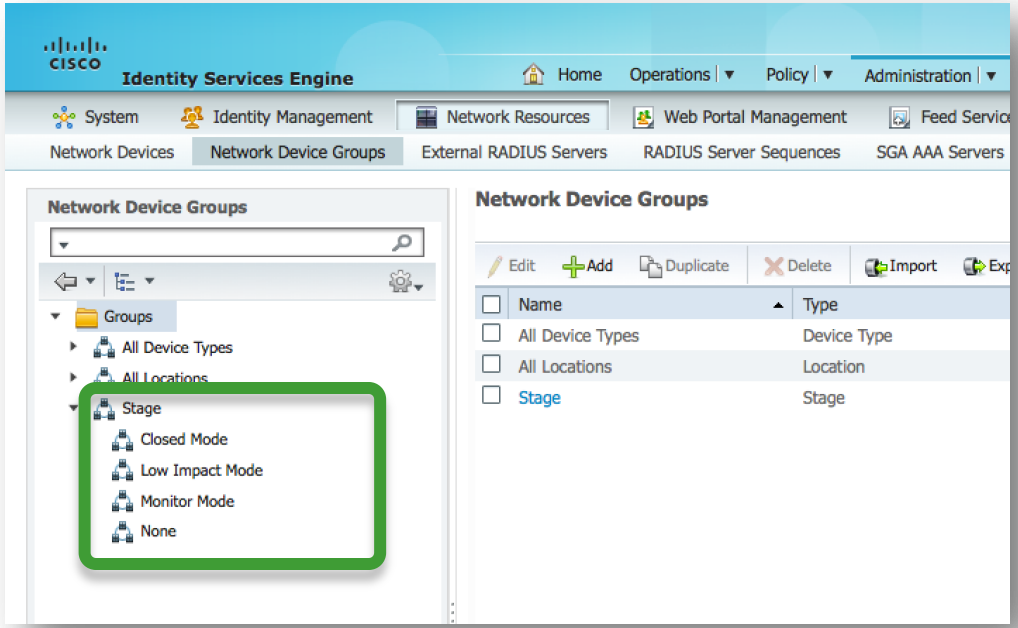
- A little up-front work, can really help you get specific in your policies.
- Organise by:
  - Device Type
    - Wired / Wireless / Firewall / VPN
    - OEAP / CVO
  - Place in Network
    - Access-Layer / Data Centre
  - Geographic Location



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.

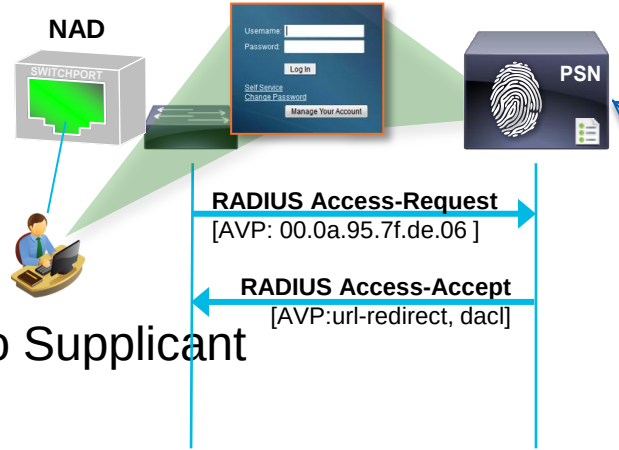


Moving from Monitor to Low-Impact

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		



No Supplicant

Matched Rule = Conf_Rooms

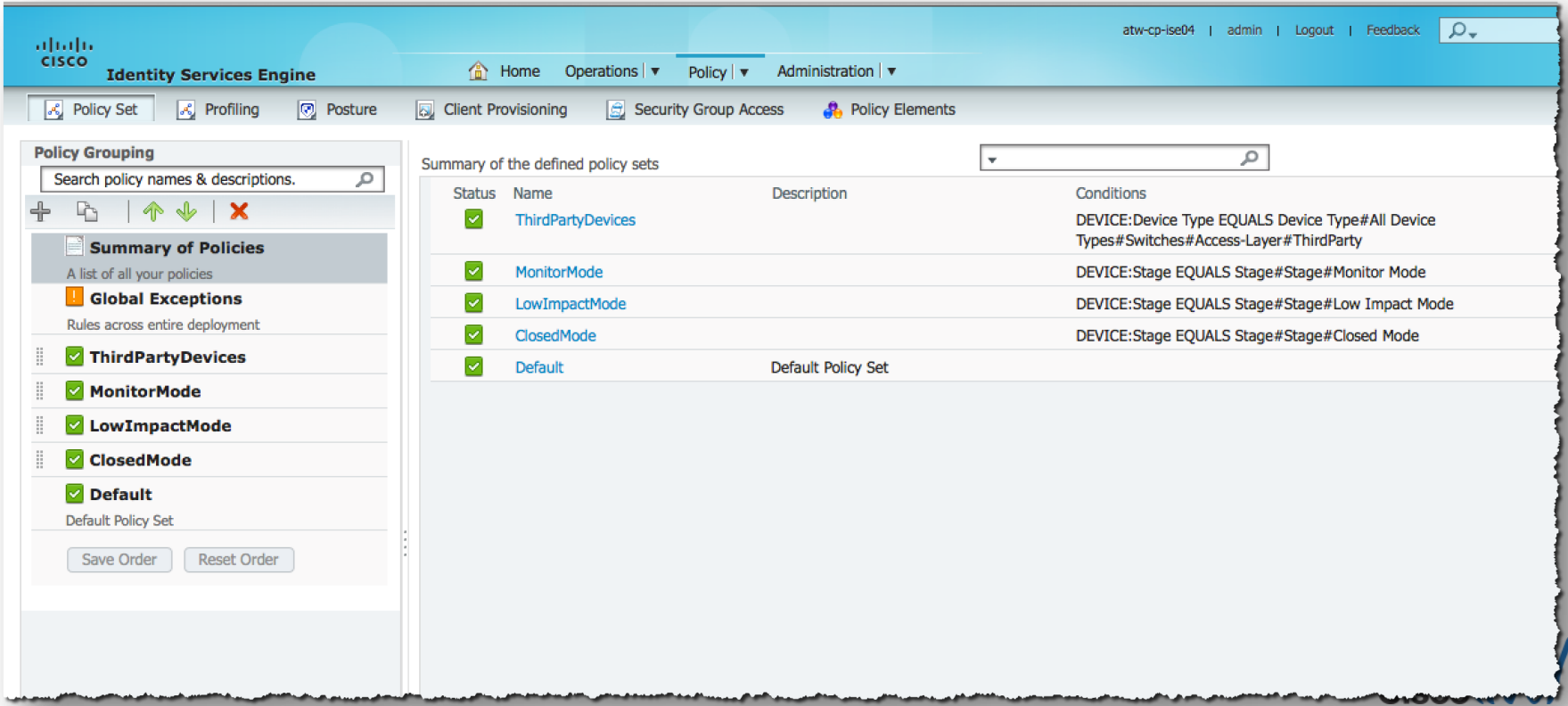
MAC-Addr is Unknown…
Continue to AuthZ table

All Other Switches
Will still be in Monitor
Mode!

ISE 1.2: Policy Sets

Separate Set of Policies for Each Mode of Deployment

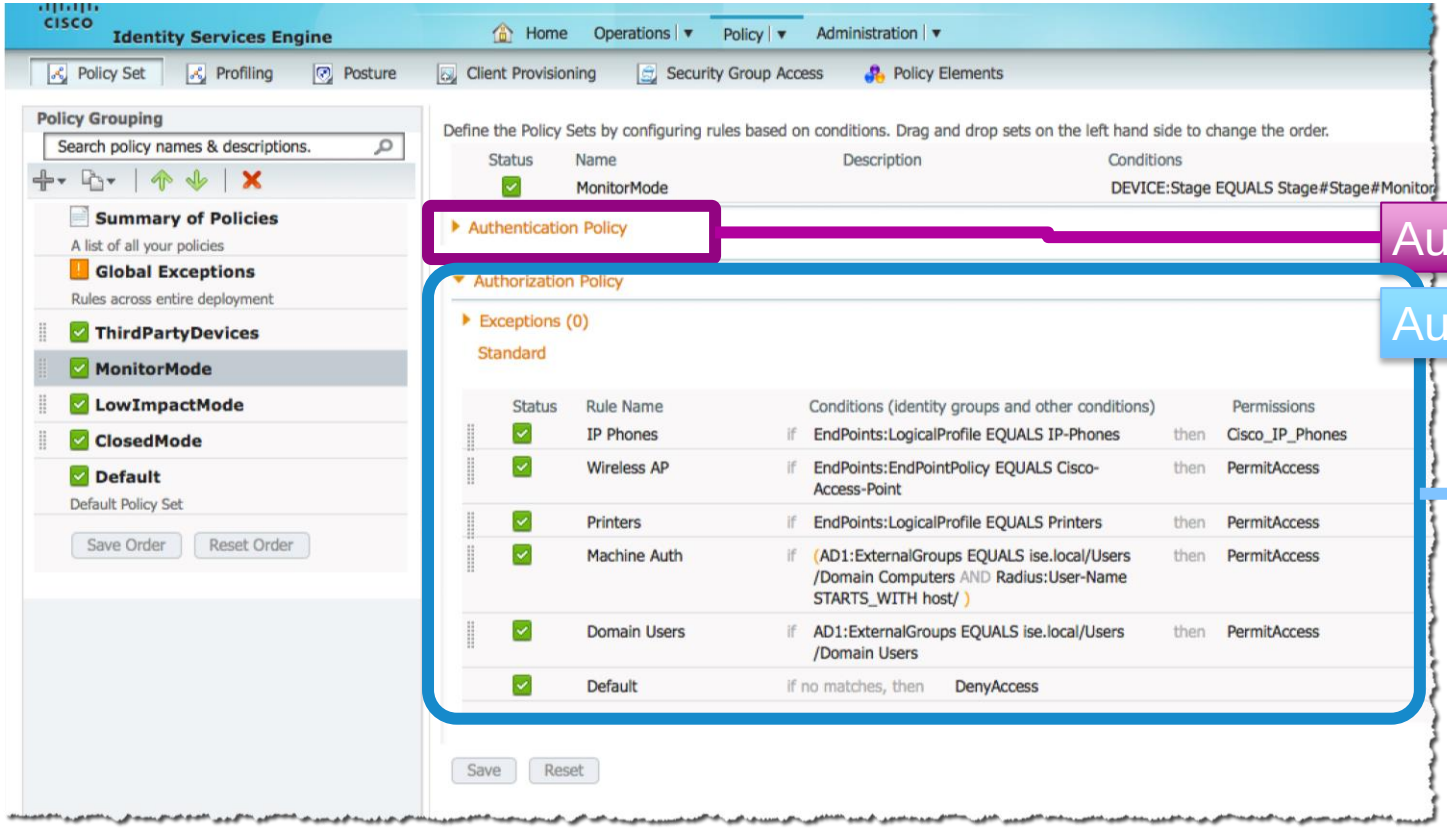
ISE 1.2+



ISE 1.2: Policy Sets

Separate Set of Policies for Each Mode of Deployment

ISE 1.2+



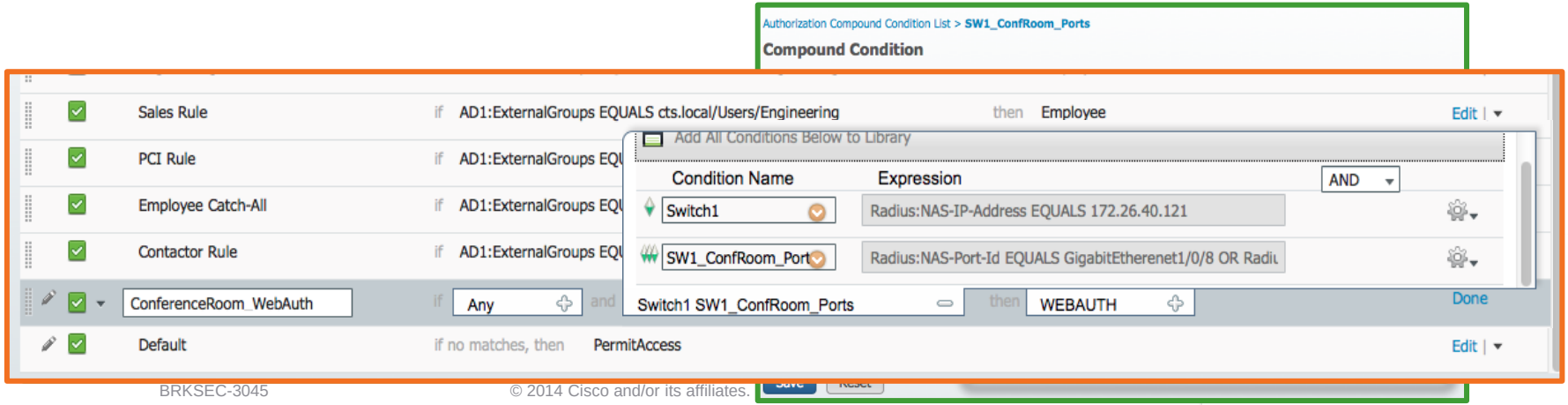
Authentication Policy

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
```

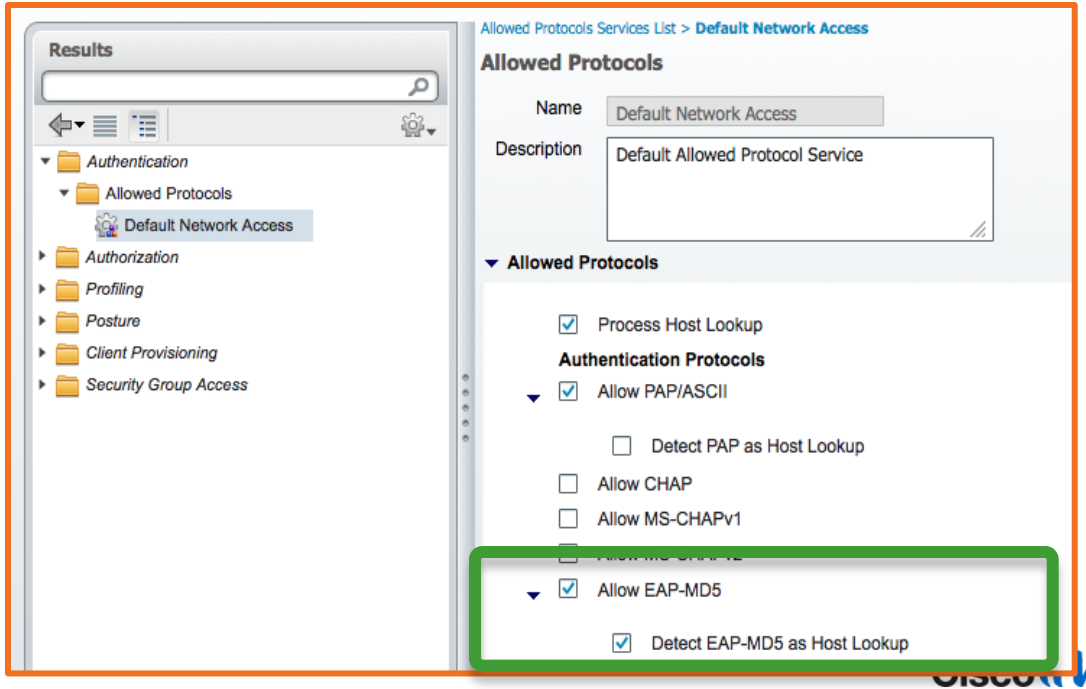
Available with ISE 1.1+

*6500 added support in SXJ4

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



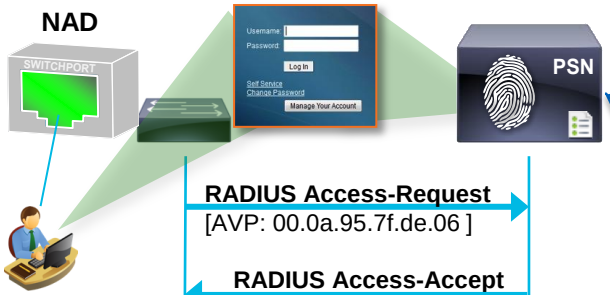
Note: Best-Practice is to never modify default objects

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		



No Supplicant

RADIUS Access-Request
[AVP: 00.0a.95.7f.de.06]

RADIUS Access-Accept
[AVP:url-redirect, dacl]

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 : GigabitEthernet1/0/2
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

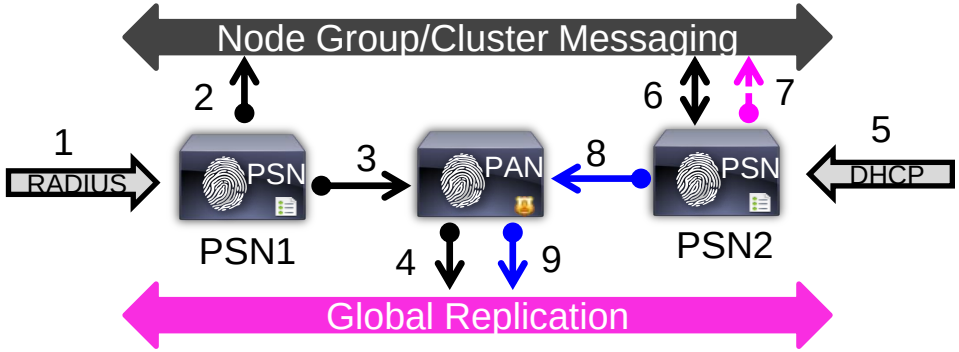



Profiling Best Practices and Key Concepts

Key Profiling Concepts

Profiling is more than just collection of attributes

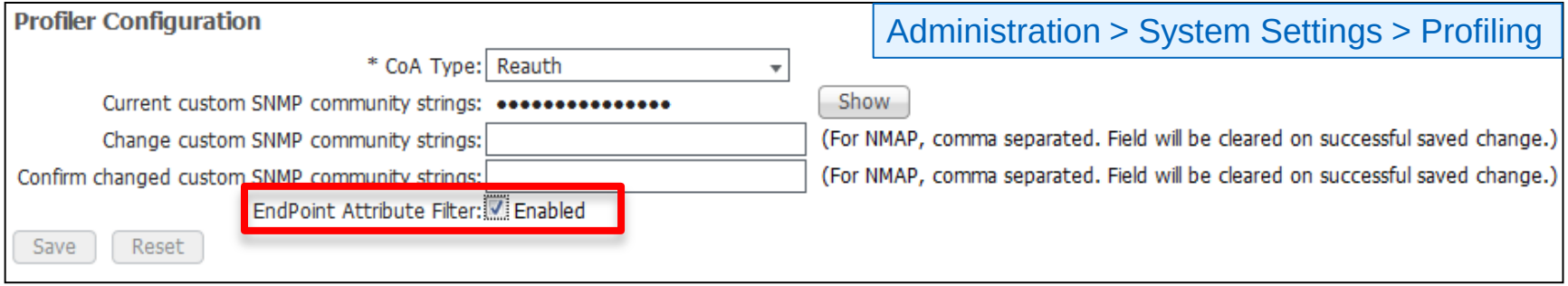
- When those attributes are collected, they have to be replicated to other nodes in the deployment
- You may need more data at start of project than in day-to-day



Profiling Attribute Filter

Whitelist Filter

- Endpoint Attribute Filter – aka “Whitelist filter” (ISE 1.1.2 and above)
  - Disabled by default. If enabled, only these attributes are collected or replicated.



- Whitelist Filter limits profile attribute collection to those required to support used profile policies and critical RADIUS operations.
  - Filter must be disabled to collect and/or replicate other attributes.
  - Attributes used in custom conditions are automatically added whitelist.
  - Regardless of setting, only whitelist attribute changes trigger PSN ownership change.

Distributed Deployments – ISE 1.2

Database Architectural and Replication Model Changes

- Database replication changes from queue-based to message-based transport.
  - No longer uses ping-pong ACK mechanism to replicate data; sends stream of updates until get NAK.
- Conversion to Entity Definition Framework (EDF)
  - Changes from hierarchical Entity-Attribute-Value model to relational database model for significant read-write improvements.
- Moving to 64-bit OS
  - Helps to improve performance by making use of larger memory.
- Local Persistence for Profiler DB.
  - Only update PAN for significant attributes
  - “EndPointServer” owns endpoint. If another PSN receives attributes, then requests sync of attributes from prior owner.
  - PAN receives all updates on significant attribute change as fallback.

MAC ADDRESS
ENDPOINT POLICY
STATIC ASSIGNMENT
STATIC GROUP ASSIGNMENT
ENDPOINT IP
POLICY VERSION
MATCHED VALUE (CF)
NMAP SUBNET SCAN ID
PORTAL USER
DEVICE REGISTRATION STATUS
ENDPOINT PROFILER SERVER

Significant Attributes vs. Whitelist Attributes

Significant Attributes

- Change triggers global replication

MACADDRESS
ENDPOINTIP
MATCHEDVALUE
ENDPOINTPOLICY
ENDPOINTPOLICYVERSION
STATICASSIGNMENT
STATICGROUPASSIGNMENT
NMAPSUBNETSCANID
PORTALUSER
DEVICEREGISTRATIONSTATUS

Whitelist Attributes

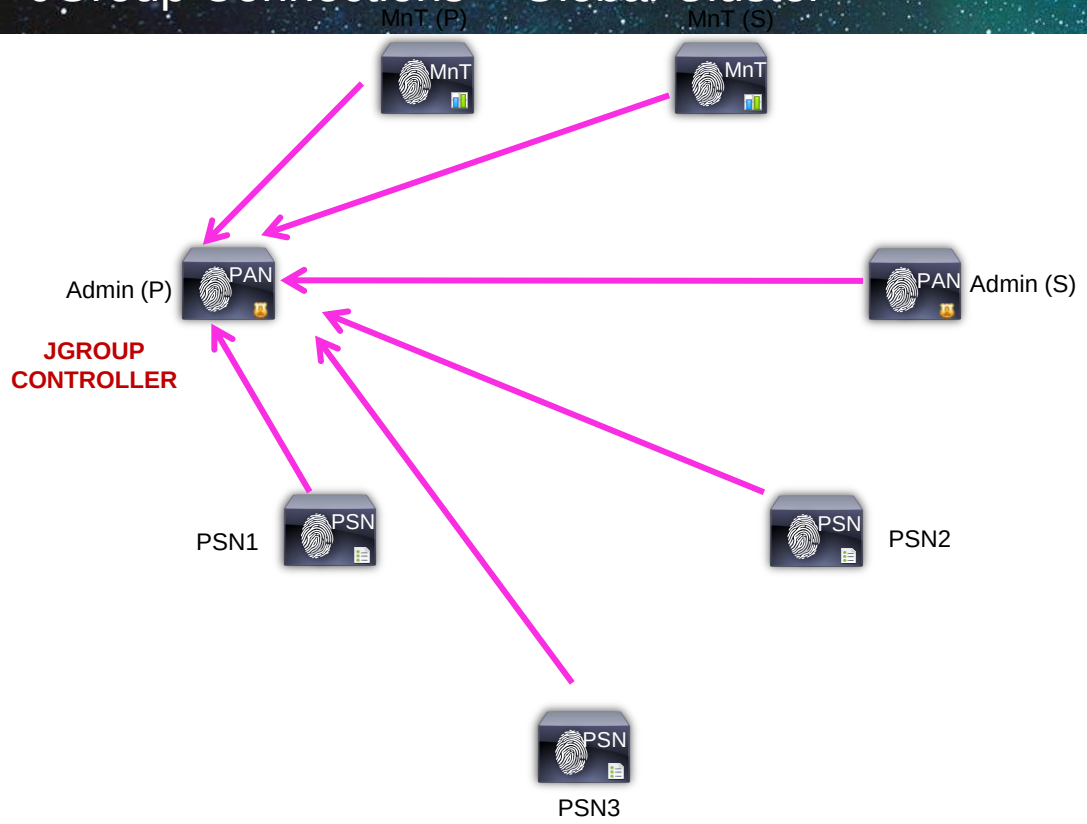
- Local filter: Minimum attributes required for profiling
- Change triggers PSN-PSN replication and ownership change only if value changes

AAA-Server
AuthState
Calling-Station-ID
Certificate Expiration Date
Certificate Issue Date
Certificate Issuer Name
Certificate Serial Number
Description
DestinationIPAddress
Device Identifier
Device Name
DeviceRegistrationStatus
EapAuthentication
EapTunnel
EndPointPolicy
EndPointPolicyID
EndPointProfilerServer
EndPointSource
FQDN
FirstCollection
Framed-IP-Address
IdentityGroup
IdentityGroupID
IdentityStoreGUID
IdentityStoreName
L4_DST_PORT
LastNmapScanTime
MACAddress
MatchedPolicy
MatchedPolicyID
MessageCode
NADAddress
NAS-IP-Address
NAS-Port-Id
NAS-Port-Type
NmapScanCount
NmapSubnetScanID
OS Version
OUI
PolicyVersion
PortalUser
PostureApplicable
Product
RegistrationTimeStamp
Service-Type
StaticAssignment
StaticGroupAssignment
TimeToProfile
Total Certainty Factor
User-Agent
cdpCacheAddress
cdpCacheCapabilities
cdpCacheDeviceId
cdpCachePlatform
cdpCacheVersion
ciaddr
dhcp-class-identifier
dhcp-requested-address
host-name
hrDeviceDescr
ifIndex
ip
lldpCacheCapabilities
lldpCapabilitiesMapSup
ported
lldpSystemDescription
operating-system
sysDescr

ISE 1.2 Inter-Node Communications

JGroup Connections – Global Cluster

- TCP/443 HTTPS (SOAP)
- UDP/45588, UDP/45590, TCP/7802 JGroup MCast
- TCP/12001 JGroups Tunneled
- TCP/2484 Oracle DB (Secure JDBC)



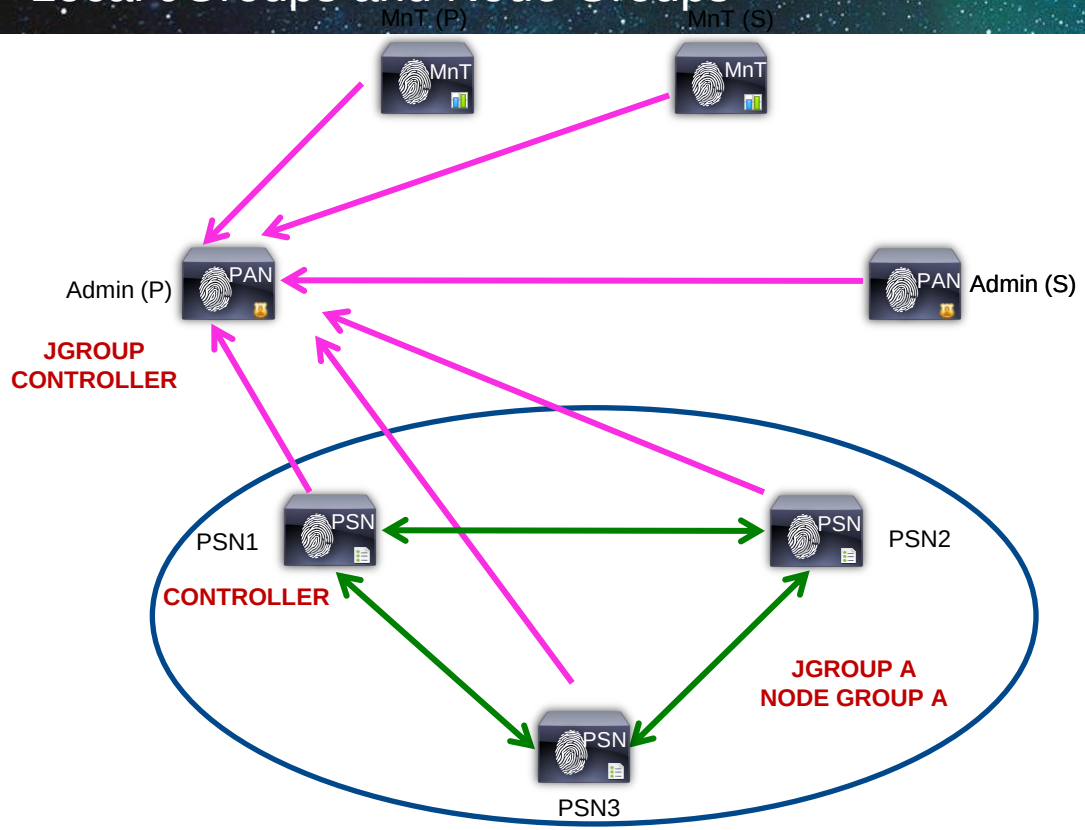
- All Secondary nodes* establish connection to Primary PAN (JGroup Controller) over tunneled connection (TCP/12001) for config/database sync.
- Secondary Admin also listens on TCP/12001 but no connection established unless primary fails/secondary promoted
- All Secondary nodes participate in the Global JGroup cluster.

***Secondary node** = All nodes except Primary Admin node; includes PSNs, MnT and Secondary Admin nodes

ISE 1.2 Inter-Node Communications

Local JGroups and Node Groups

- TCP/443 HTTPS (SOAP)
- UDP/45588, UDP/45590, TCP/7802 JGroup MCast
- TCP/12001 JGroups Tunneled
- TCP/2484 Oracle DB (Secure JDBC)



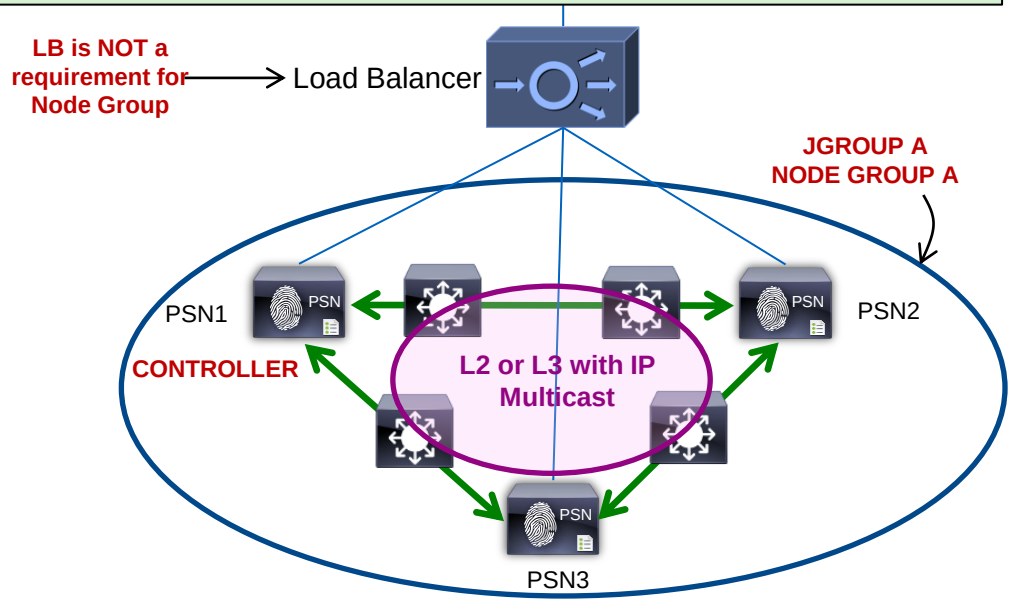
- Node Groups can be used to define local JGroup clusters where members exchange heartbeat and sync profile data over IP multicast.
- Node claims ownership if change in whitelist attribute, triggers inter-PSN sync of attributes; whitelist check always occurs regardless of global attribute filter setting.
- Replication to PAN only occurs if critical attribute changes, then sync all attributes to PAN; if whitelist filter enabled, only whitelist attributes synced to all nodes.

ISE 1.2 Inter-Node Communications

Local JGroups and Node Groups

- TCP/443 HTTPS (SOAP)
- UDP/45588, UDP/45590, TCP/7802 JGroup MCast
- TCP/12001 JGroups Tunneled
- TCP/2484 Oracle DB (Secure JDBC)

- General classification data for given endpoint should stay local to node group = **whitelist attributes**
- Only certain critical data needs to be shared across entire deployment = **significant attributes**

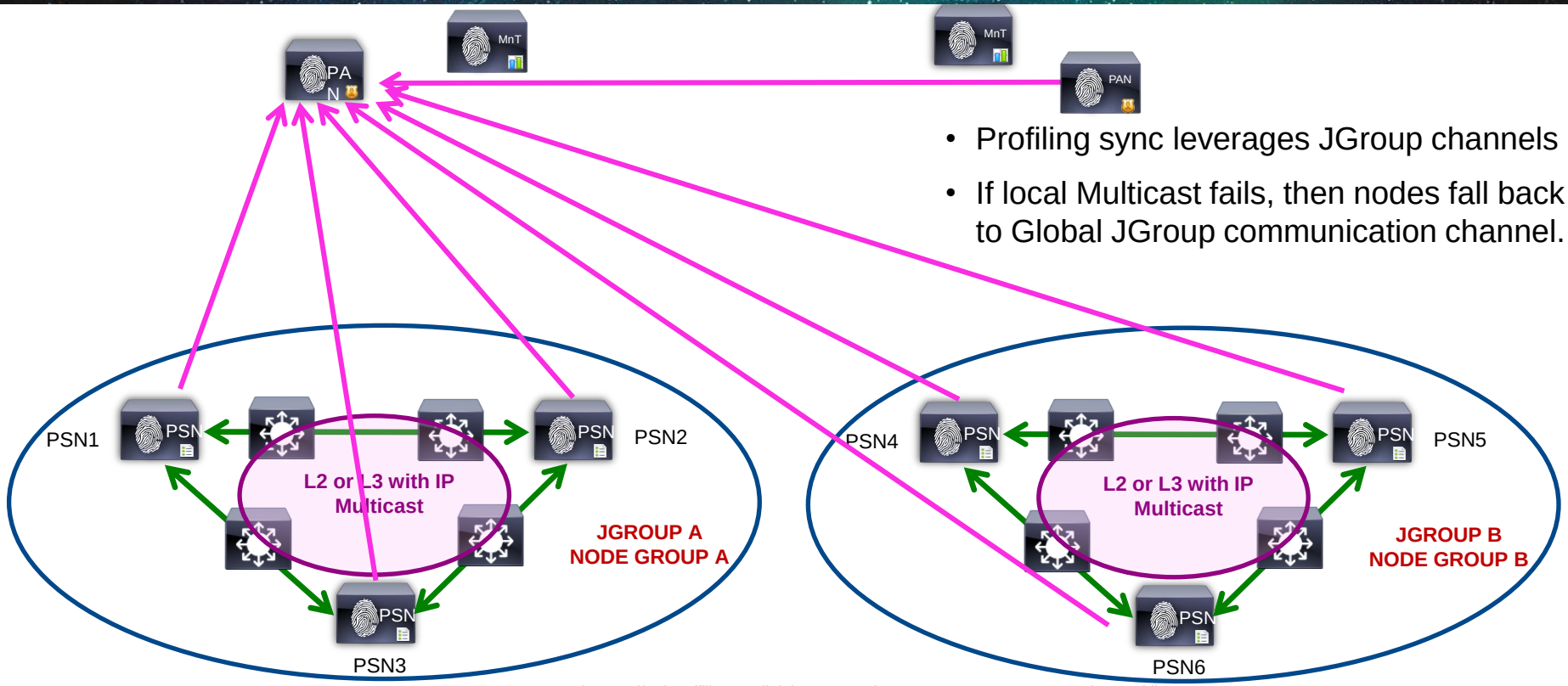


- Node groups continue to provide original function of session recovery for failed PSN.
- Profiling sync leverages JGroup channel
- Each LB cluster should be a node group, but LB is NOT required for node groups.
- Recommend node groups reside in same L2 domain; However, if required, group members can be L3-connected provided IP multicast properly configured (Note: TTL=2).
- Reduces sync updates even if different PSNs receive data – expect few whitelist changes and even fewer critical attribute changes. [IP change is critical attribute]

ISE 1.2 Inter-Node Communications

Local JGroups and Node Groups

- TCP/443 HTTPS (SOAP)
- UDP/45588, UDP/45590, TCP/7802 JGroup MCast
- TCP/12001 JGroups Tunneled
- TCP/2484 Oracle DB (Secure JDBC)



- Profiling sync leverages JGroup channels
- If local Multicast fails, then nodes fall back to Global JGroup communication channel.

ISE Profiling Best Practices

Whenever Possible…

- **Use Device Sensor** on Cisco switches and Wireless LAN Controllers to optimise data collection.

Do NOT send profile data to multiple PSNs !

- **Ensure profile data for a given endpoint is sent to a single PSN (or maximum of 2)**
  - Sending same profile data to multiple PSNs increases inter-PSN traffic and contention for endpoint ownership.
  - For redundancy, consider Load Balancing and Anycast to support a single IP target for profiling using…
  - RADIUS
  - IP Helpers
  - SNMP Traps
  - DHCP/HTTP with ERSPAN (Requires validation)

DO send profile data to single and same PSN or Node Group !

- **Ensure profile data for a given endpoint is sent to the *same* PSN**
  - Sticky is ideal, but not always possible across different probes

DO use Device Sensor !

- **Use node groups and ensure profile data for a given endpoint is sent to *same* node group.**
  - Node Groups avoid inter-PSN contentions and ensure endpoint changes outside of node group.

DO enable the Profiler Attribute Filter !

- **Avoid probes that collect the same endpoint attributes**
  - Example: Device Sensor + SNMP Query/IP Helper
- **Enable Profiler Attribute Filter**

ISE Profiling Best Practices

General Guidelines for Probes

- **HTTP Probe:**
  - Use URL Redirects over SPAN to centralise collection and reduce traffic load related to SPAN/RSPAN.
  - Avoid SPAN. If used, look for key traffic chokepoints such as Internet edge or WLC connection; use intelligent SPAN/tap options or VACL Capture to limit amount of data sent to ISE. Also difficult to provide HA for SPAN.
- **DHCP Probe:**
  - Use IP Helpers when possible—be aware that L3 device serving DHCP will not relay DHCP for same!
  - Avoid DHCP SPAN. If used, make sure probe captures traffic to central DHCP Server. HA challenges.

Do NOT enable all probes by default !

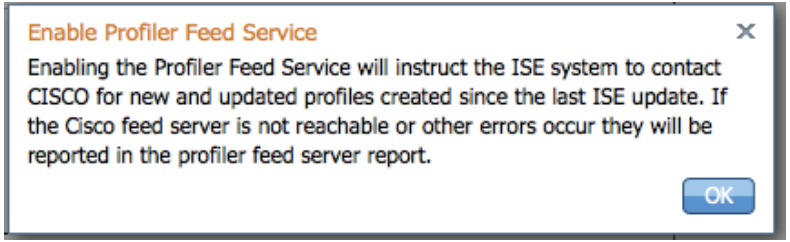
Avoid SPAN, SNMP Traps, and NetFlow probes !

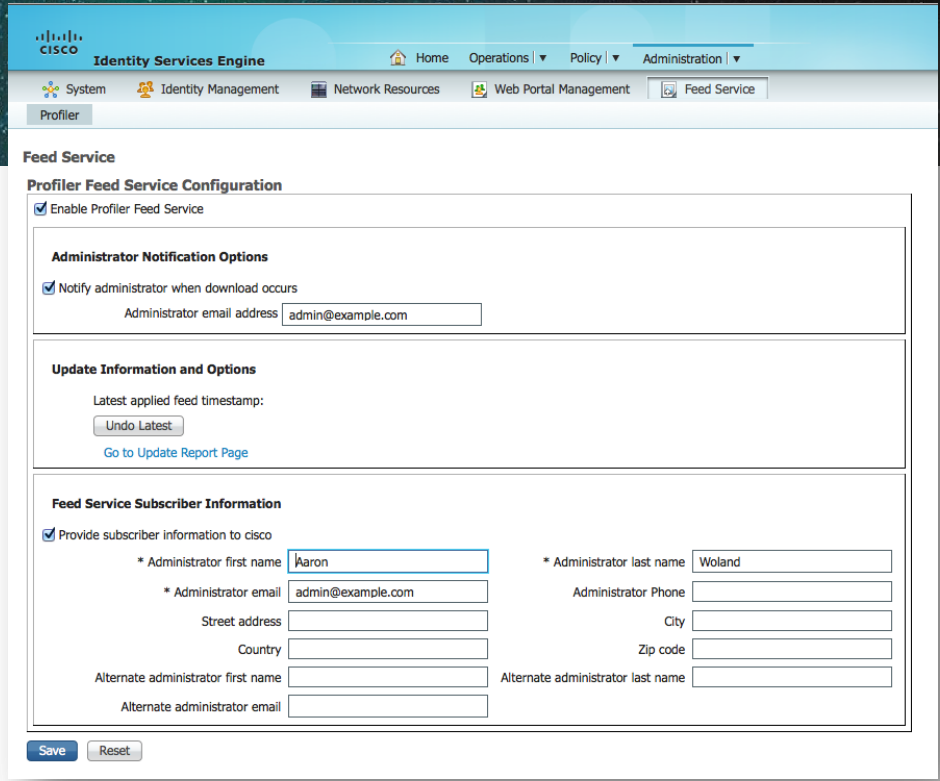
- **SNMP Probe:**
  - Be careful of high SNMP traffic due to triggered RADIUS Accounting updates as a result of high re-auth (low session/re-auth timers) or frequent interim accounting updates.
  - For polled SNMP queries, avoid short polling intervals. Be sure to set optimal PSN for polling in ISE NAD config.
  - SNMP Traps primarily useful for non-RADIUS deployments like NAC Appliance—Avoid SNMP Traps w/RADIUS auth.
- **NetFlow Probe:**

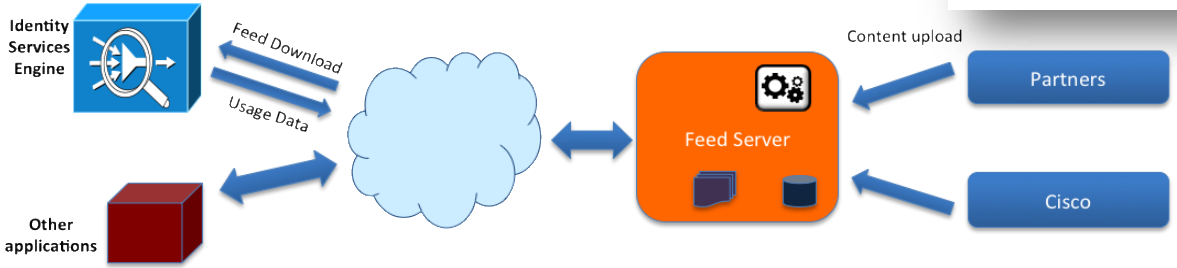
  Use only for specific use cases in centralised deployments—Potential for high load on network devices and ISE.

Feed Service

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

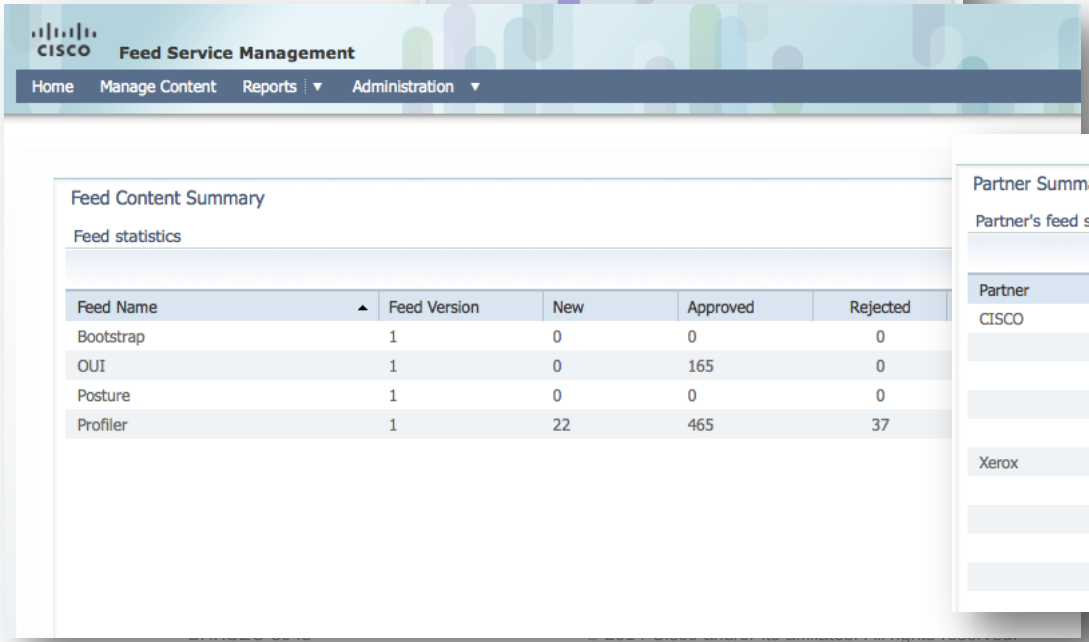






Feed Service Server

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

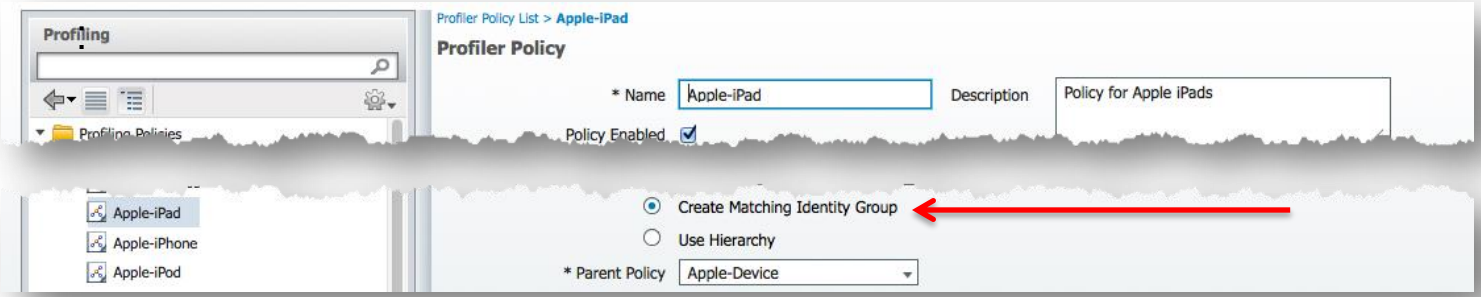
Partner's feed statistics

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

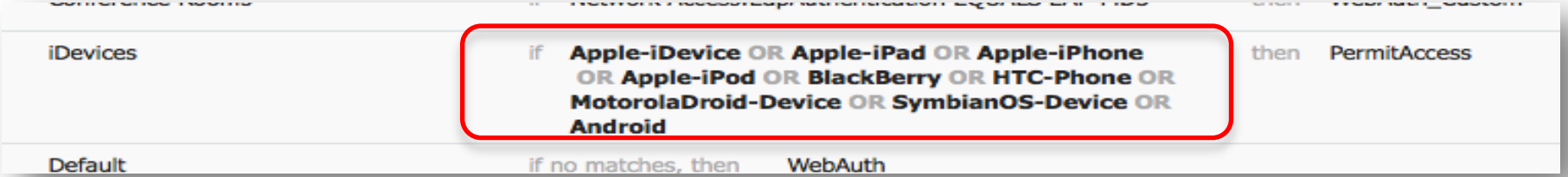
Identity Groups in ISE 1.1.x

Before ISE 1.2:

- Go into each profile & create a Matching Identity Group:



- Then, add each Identity Group to the Authorisation Rule:



Identity Groups in ISE 1.1.x

Side-effect of Identity Groups:

- Cannot use Profile and the BYOD Flow!

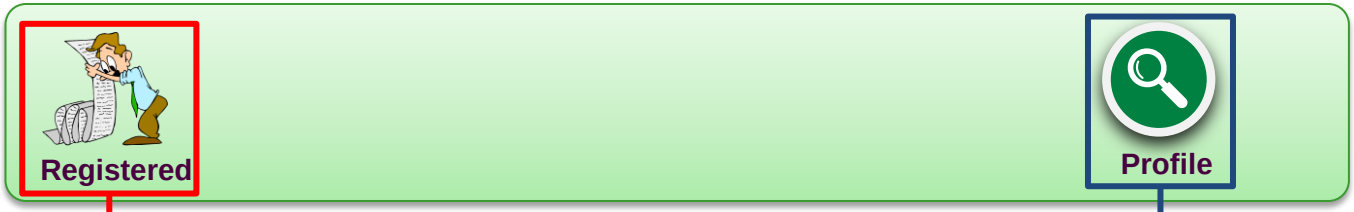
Registered

Profile

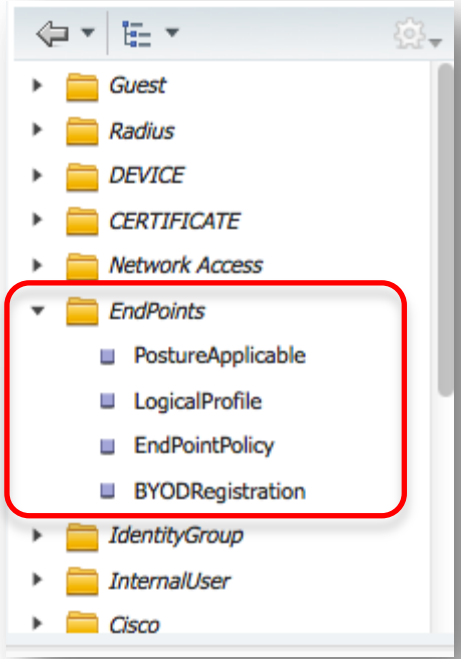
✓	PCI RUle	if	(AD1:ExternalGroups EQUALS cts.local/Users/PCI AND Network Access:EapChainingResult EQUALS User and machine both succeeded AND Session:PostureStatus EQUALS Compliant)	then	PCI AND Employee
✓	Employee Rule	if	**RegisteredDevices** AND (Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND AD1:ExternalGroups EQUALS cts.local/Users/Employees)	then	Employee
✓	Employee Rule_Wired	if	**Microsoft-Workstation** AND Wired_Employee	then	Employee_wired
✓	PEAP Rule	if	PEAP	then	NSP
✓	EAP CHAINING-oneFailed	if	Network Access:EapChainingResult EQUALS User succeeded and machine failed	then	WebAuth

Endpoint Profile as Attribute

No need for Identity Groups anymore!



if	Wireless_MAB	then	WebAuth-WiFi
if	(Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP)	then	NSP
if	(EndPoints:EndPointPolicy EQUALS Apple-iPad AND EndPoints:BYODRegistration EQUALS No)	then	NSP
if	[redacted] AND MDM:DeviceRegisterStatus EQUALS UnRegistered	then	MDM-OnBoard



Logical Profiles

Endpoint Profiling Policies

Logical Profiles List > **i-Devices**

Logical Profile

* Name: i-Devices

Description: All Handheld Stuff

Policy Assignment

Available Policies:

- Apple-Device
- Apple-MacBook
- Applera-Device
- Aruba-Device
- Aruba-AP
- Avaya-Device
- Avaya-IP-Phone
- Brother-Device

> <

Assigned Policies:

- BlackBerry
- Apple-iPhone
- Apple-iDevice
- Android
- HTC-Phone
- Apple-iPad
- Apple-iPod

Logical Profiles == Clean Policies

- Before ISE 1.2:

iDevices	if	**Apple-iDevice** OR **Apple-iPad** OR **Apple-iPhone** OR **Apple-iPod** OR **BlackBerry** OR **HTC-Phone** OR **MotorolaDroid-Device** OR **SymbianOS-Device** OR **Android**	then	PermitAccess
Default	if no matches, then	WebAuth		

- With ISE 1.2:

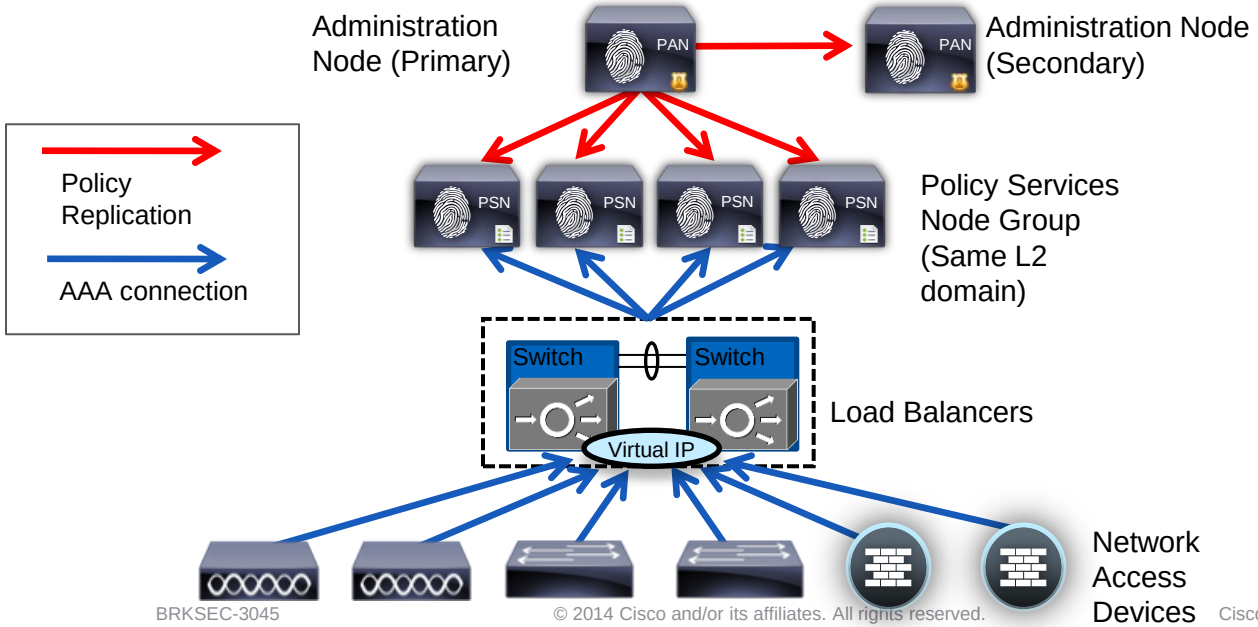
Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
I-Devices	if	EndPoints:LogicalProfile EQUALS i-Devices	then	PermitAccess
Employees	if	AD1:ExternalGroups EQUALS cts.local/Users /Employees	then	PermitAccess AND Employee




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.

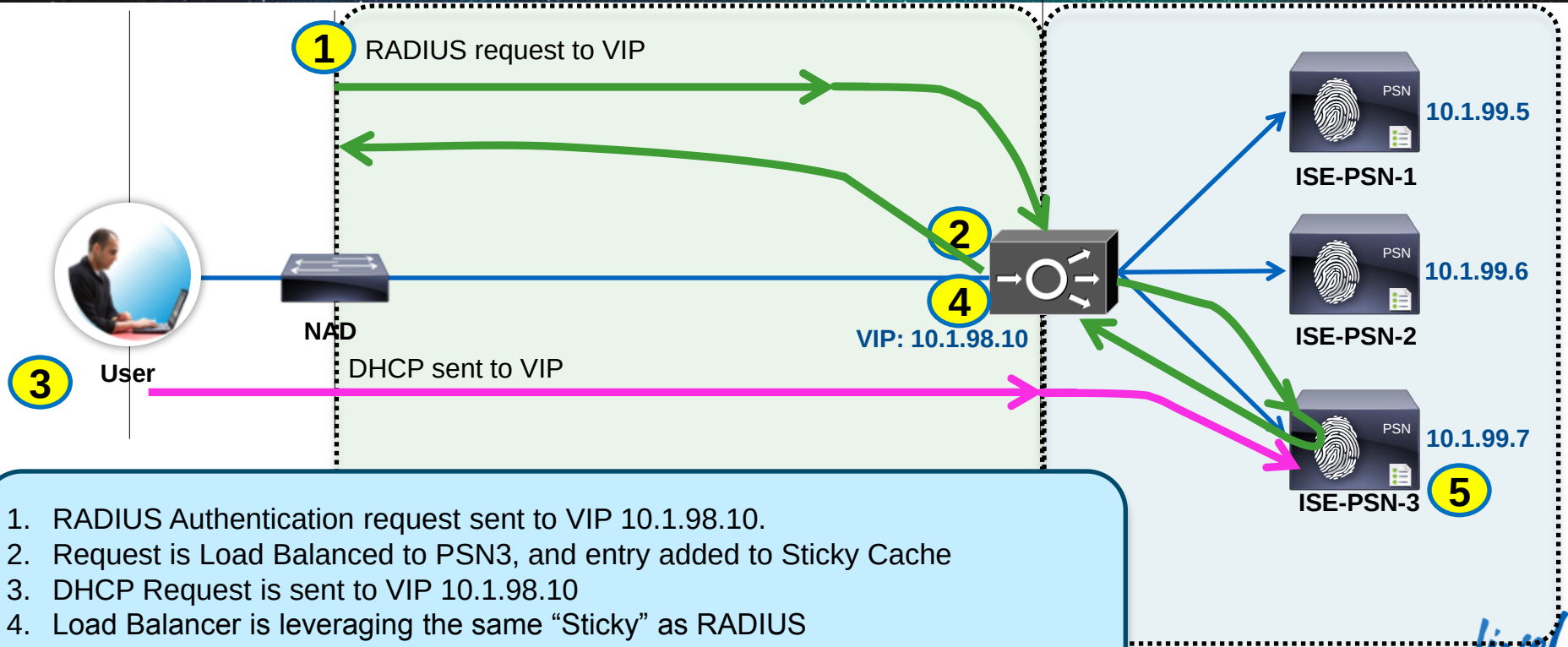


Load Balancing Best Case

Ensuring DHCP & RADIUS reach the SAME PSN

Sticky Cache:

11:22:33:44:55:66 | PSN 3



1. RADIUS Authentication request sent to VIP 10.1.98.10.
2. Request is Load Balanced to PSN3, and entry added to Sticky Cache
3. DHCP Request is sent to VIP 10.1.98.10
4. Load Balancer is leveraging the same “Sticky” as RADIUS
5. DHCP is received by SAME PSN, ensuring VERY Clean Replication

ACE Health Monitoring Probes

ISE Live Log Activity “Noise”

- No support today for negative filter (!=probe) to reduce Live Log noise.

- Log Suppression & Filtering added to ISE 1.2

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

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:	

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	

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

ISE and Load Balancers

Failure Scenarios

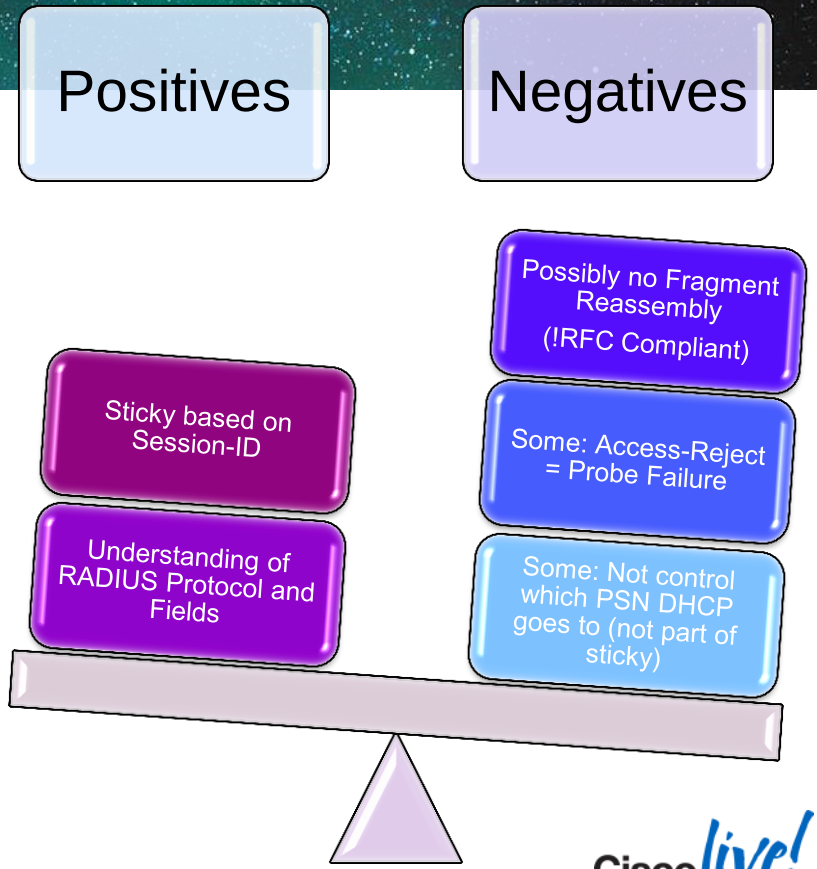
- The VIP is the RADIUS Server, so if the entire VIP is down, then the NAD should fail over to the secondary Data Centre VIP (listed as the secondary RADIUS server on the NAD).
- Probes on the load balancers should ensure that RADIUS is responding as well as HTTPS, at a minimum.
  - Validate that RADIUS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

ISE and Load Balancers

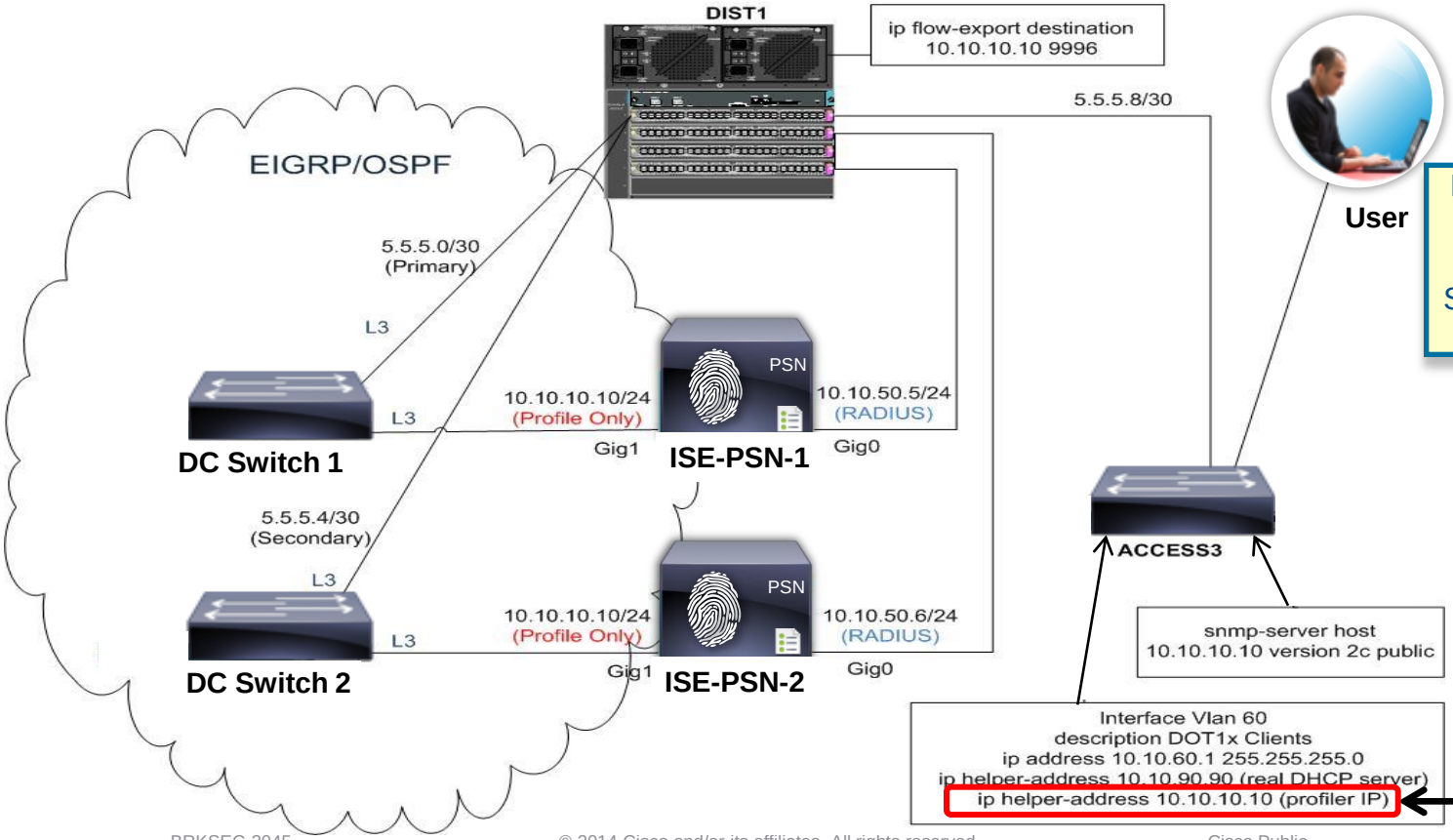
RADIUS LB or UDP?

- Seen Failures Reassembling
  - When large certs in use
- Seen Inability to LB DHCP to more than one server



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

Using AnyCast for Profiling Redundancy



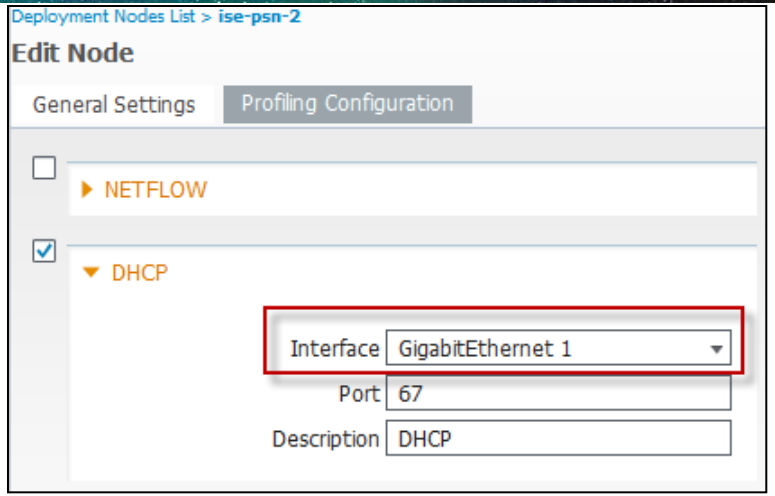
ISE 1.2 web services per interface feature could make this an option for Sponsor, Guest LWA, and MDP portals.

NADs are configured with single Anycast IP address.

Ex: 10.10.10.10

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

- DC 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

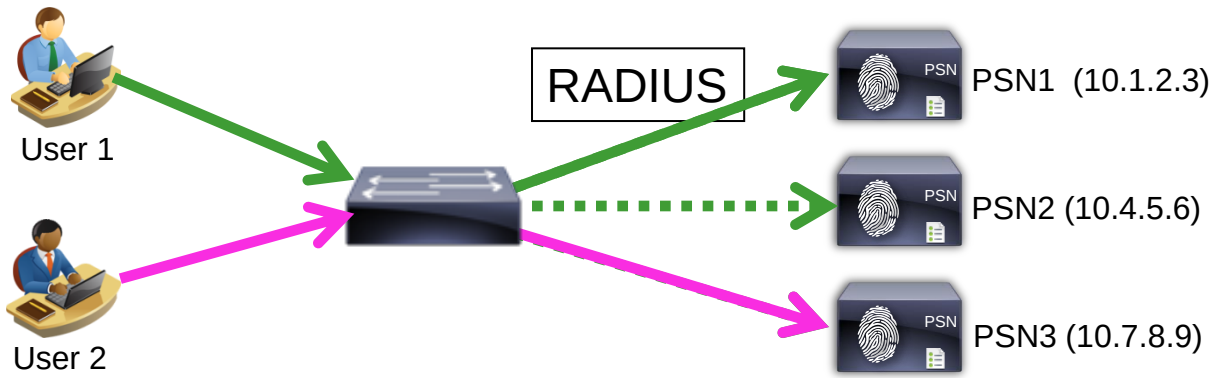
- DC Switch 2

```
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        # less preferred route
set metric-type external
!
route-map CONNECTED-2-EIGRP permit 20
ip prefix-list 5 seq 5 permit 10.10.10.0/24
```

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.



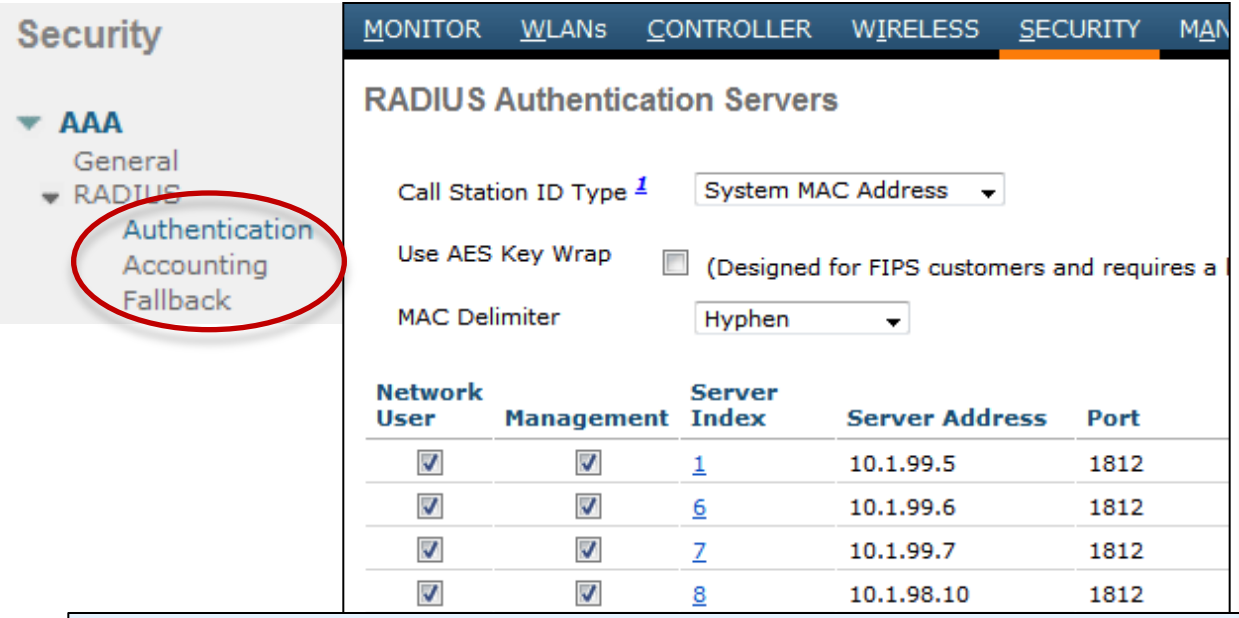
NAD controls the load distribution of AAA requests to all PSNs in RADIUS group without dedicated LB.

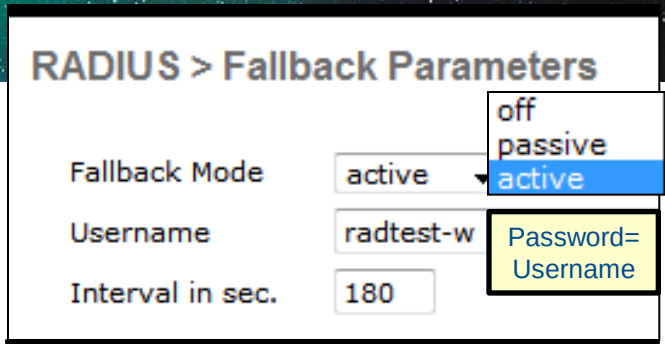
```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813
radius-server load-balance method least-outstanding batch-size 5
```

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.

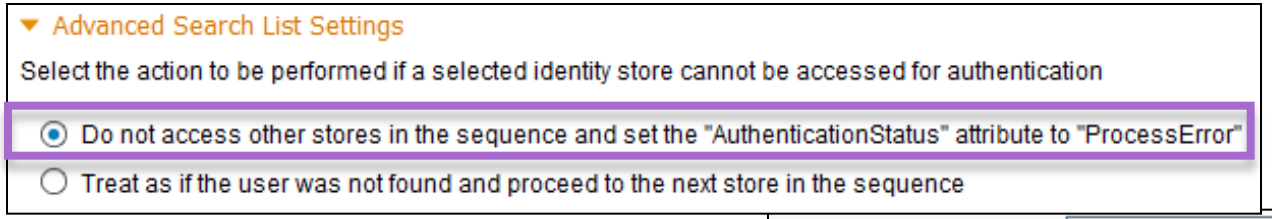
http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a008098987e.shtml

RADIUS Test User Account

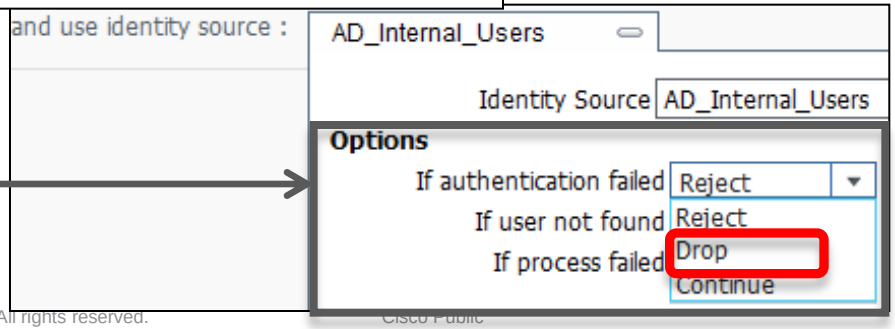
Which User Account Should Be Used?

- 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:

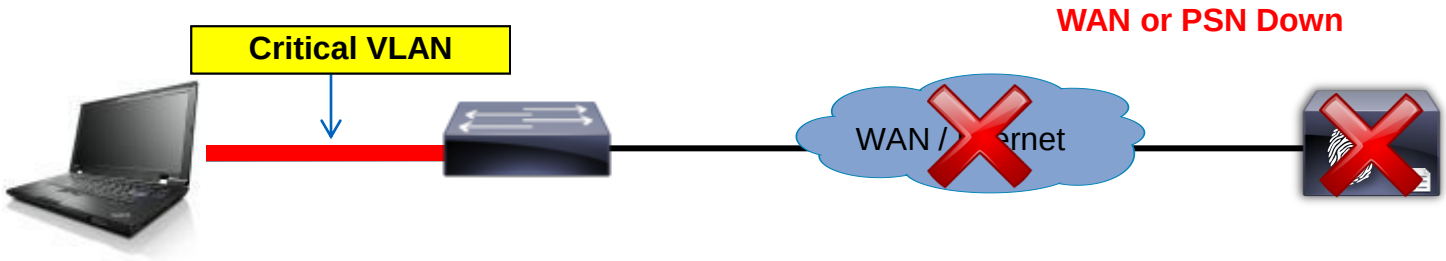


Authentication Policy > ID Source Custom processing based on authentication results



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

Authorization 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
```

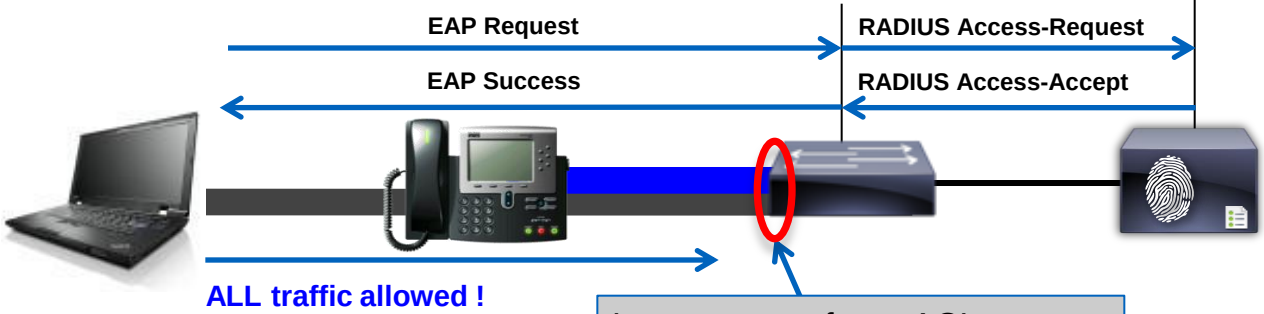
```
ip access-list extended ACL-DEFAULT
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit icmp any any
 permit udp any any eq tftp
```

Protecting Against "No dACL" Authorisation

EPM Access Control

2k/3k: 12.2(55)SE
4k: 12.2(54)SG
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

Authorization Profile = Employee

Access Type = Access-Accept

NO dACL!

Insert at top of port ACL:
permit ip any any

epm access control open

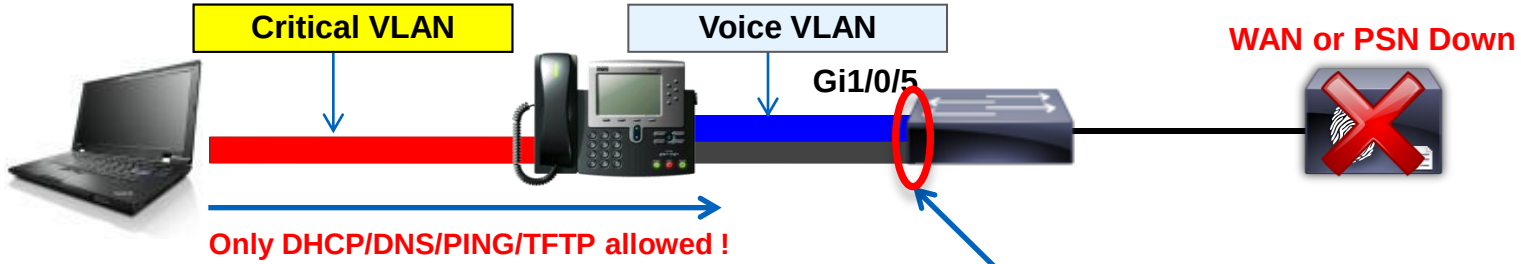
interface GigabitEthernet1/0/2
switchport access **vlan 10**
switchport voice **vlan 13**
ip access-group ACL-DEFAULT in

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)SG
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

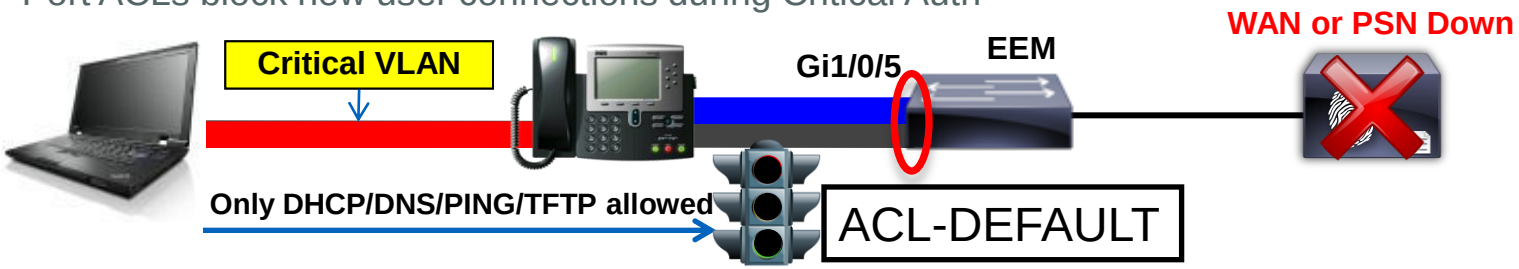
Multi-server option: %RADIUS-3-ALLDEADSERVER

EEM Example

Remove and Add Port ACL on RADIUS Server Status Syslogs

Cat 3K
Cat 4K
Cat 6K

- 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

CISCO PARTNER Technology Developer

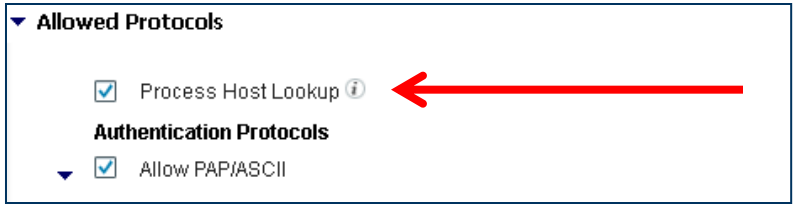
```
cat6500(config)# track 1 ip route 10.1.98.0 255.255.255.0 reachability

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"
```



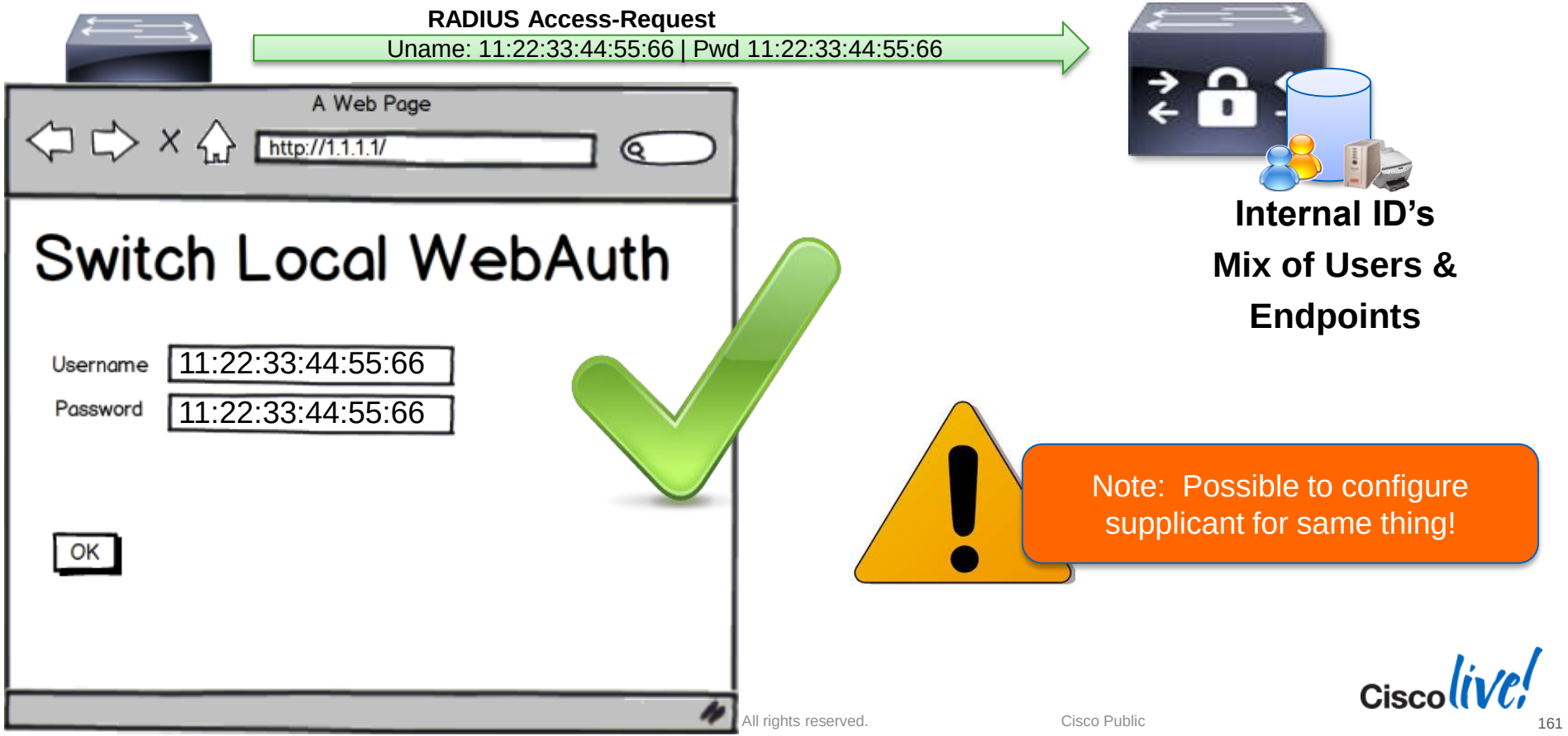

3rd Party NAD Integration

ISE and Endpoint Lookup

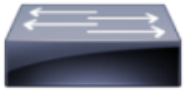
- ISE maintains a separate User and Endpoint "store".
  - User store may be queried at any time.
- By default: endpoint store may only be accessed if the incoming request was identified as a MAB. (Service-Type = Call-Check)
  - ISE also ignores the u-name/pwd fields, but uses the calling-station-id (mac-address of the endpoint)
- Why?
  - **Security!** Before this, malicious users would be able to put a mac-address into the username & password fields of WebAuth (or non-Cisco switches even in the supplicant identity).



Why Restrict MAB to Calling-Station-ID?



Cisco MAB – MAC Authentication Bypass



RADIUS Access-Request


```
▷ User Datagram Protocol, Src Port: sightline (1645), Dst Port: radius (1812)
▽ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0xe4 (228)
    Length: 242
    Authenticator: 972fa8aa903e305faf145f7fac70c713
    [The response to this request is in frame 208]
  ▽ Attribute Value Pairs
    ▽ AVP: l=14  t=User-Name(1): 005056870004
        User-Name: 005056870004
    ▷ AVP: l=18  t=User-Password(2): Encrypted
    ▽ AVP: l=6  t=Service-Type(6): Call-Check(10)
        Service-Type: Call-Check (10)
    ▽ AVP: l=31  t=Vendor-Specific(26) v=Cisco(9)
      ▽ VSA: l=25 t=Cisco-AVPair(1): service-type=Call Check
          Cisco-AVPair: service-type=Call Check
    ▷ AVP: l=6  t=Framed-MTU(12): 1500
    ▷ AVP: l=19  t=Called-Station-Id(30): 1C-DF-0F-31-B0-02
    ▽ AVP: l=19  t=Calling-Station-Id(31): 00-50-56-87-00-04
        Calling-Station-Id: 00-50-56-87-00-04
    ▷ AVP: l=18  t=Message-Authenticator(80): 082aa8d6c0a006adbad6aaf7fdfa7267
    ▷ AVP: l=2  t=EAP-Key-Name(102):
    ▽ AVP: l=49  t=Vendor-Specific(26) v=Cisco(9)
```

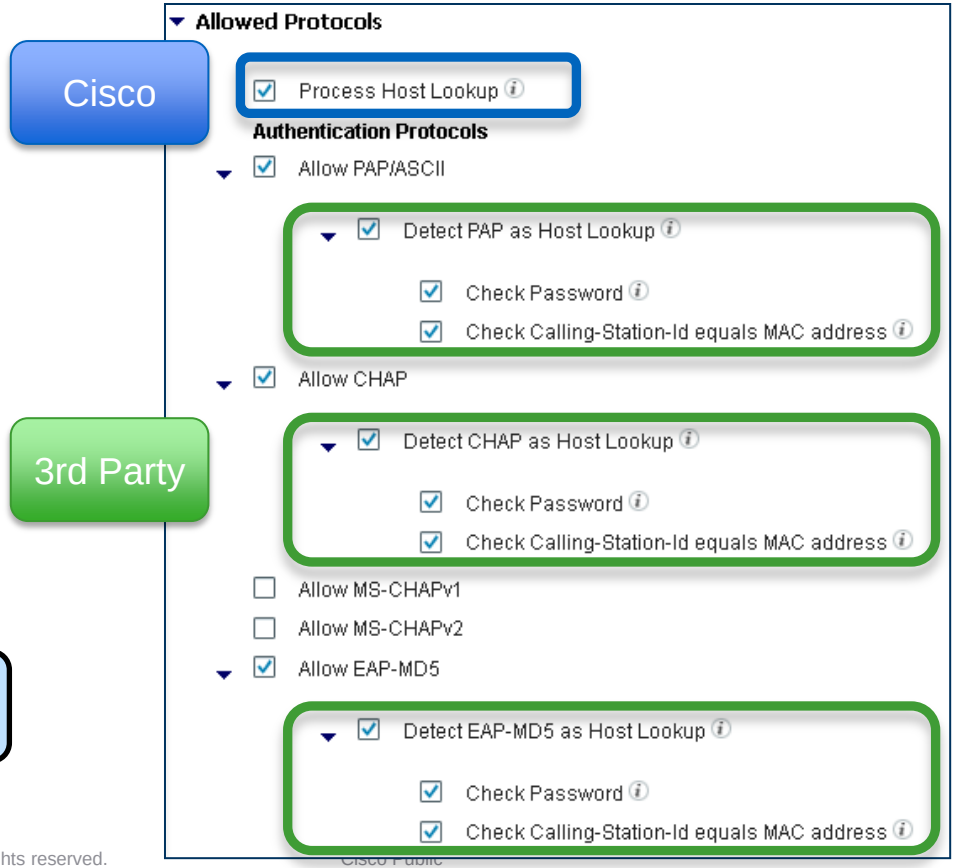
= MAB

= MAC

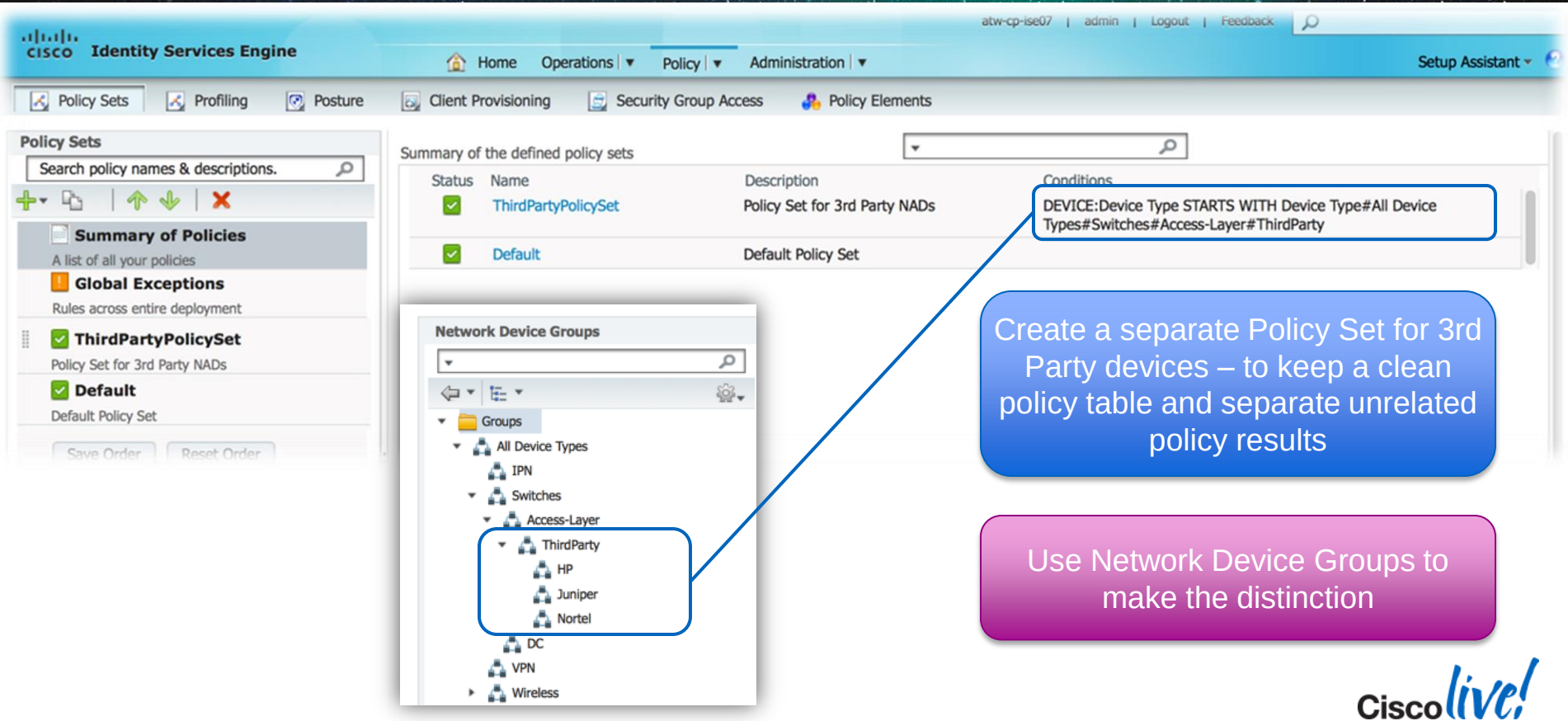
3rd-Party Devices and MAB

- Many 3rd parties use Service-Type = Login for 802.1X, MAB and WebAuth
- Some 3rd Parties do not populate Calling-Station-ID with MAC address.
- With ISE 1.2, MAB can work with different Service-Type, Calling-Station-ID values, and “password” settings.

Recommendation is to keep as many checkboxes enabled as possible for increased security



Setup a Policy Set for 3rd Party NADs



Create a separate Policy Set for 3rd Party devices – to keep a clean policy table and separate unrelated policy results

Use Network Device Groups to make the distinction

Example: Nortel & Alcatel Authentication Policy

Authentication Policy

Nortel AuthC	: If	NDGisNortel	Allow Protocols :	NortelProts	and Edit
PAP-Rule	If	PAP_ASCII	use	Internal Endpoints	
CHAP-Rule	If	CHAP	use	Internal Endpoints	
Default	: use	All_ID_Sources			

Network Device Group = “Nortel”

For “better” security, lock PAP & CHAP into MAB lookups (Internal Endpoints)

All other authentications are sent to an Identity Sequence (Internal Users > Guest > AD)

Allowed Protocols

- [x] Process Host Lookup
- **Authentication Protocols**
- [x] Allow PAP/ASCII
  - [x] Detect PAP as Host Lookup
    - [ ] Check Password
    - [ ] Check Calling-Station-Id equals MAC address
- [x] Allow CHAP
  - [x] Detect CHAP as Host Lookup
    - [ ] Check Password
    - [ ] Check Calling-Station-Id equals MAC address

Example: Rest of 3rd Party Authentication Policy

Most Third Party : If DeviceTypeEQThridParty Allow Protocols : ThirdPartyProtocols and Edit

PAP-Rule : If PAPASCII use Internal Endpoints

CHAP-Rule : If CHAPmd5 use Internal Endpoints

Default : use All_ID_Sources

Default Rule (If no match) : Allow Protocols : Default Network Access and use : DenyAccess Edit

Deny non-matches

Network Device Group = "Third Party"

For "better" security, lock PAP & CHAP into MAB lookups (Internal Endpoints)

All other authentications are sent to an Identity Sequence (Internal Users > Guest > AD)

Allowed Protocols

- Process Host Lookup

Authentication Protocols

- Allow PAP/ASCII
  - Detect PAP as Host Lookup
    - Check Password
    - Check Calling-Station-Id equals MAC address
- Allow CHAP
  - Detect CHAP as Host Lookup
    - Check Password
    - Check Calling-Station-Id equals MAC address

Third Party Vendors VSA Attributes

- You may import other RADIUS Dictionaries into ISE:
  Policy > Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors

Dictionaries for FreeRADIUS will work

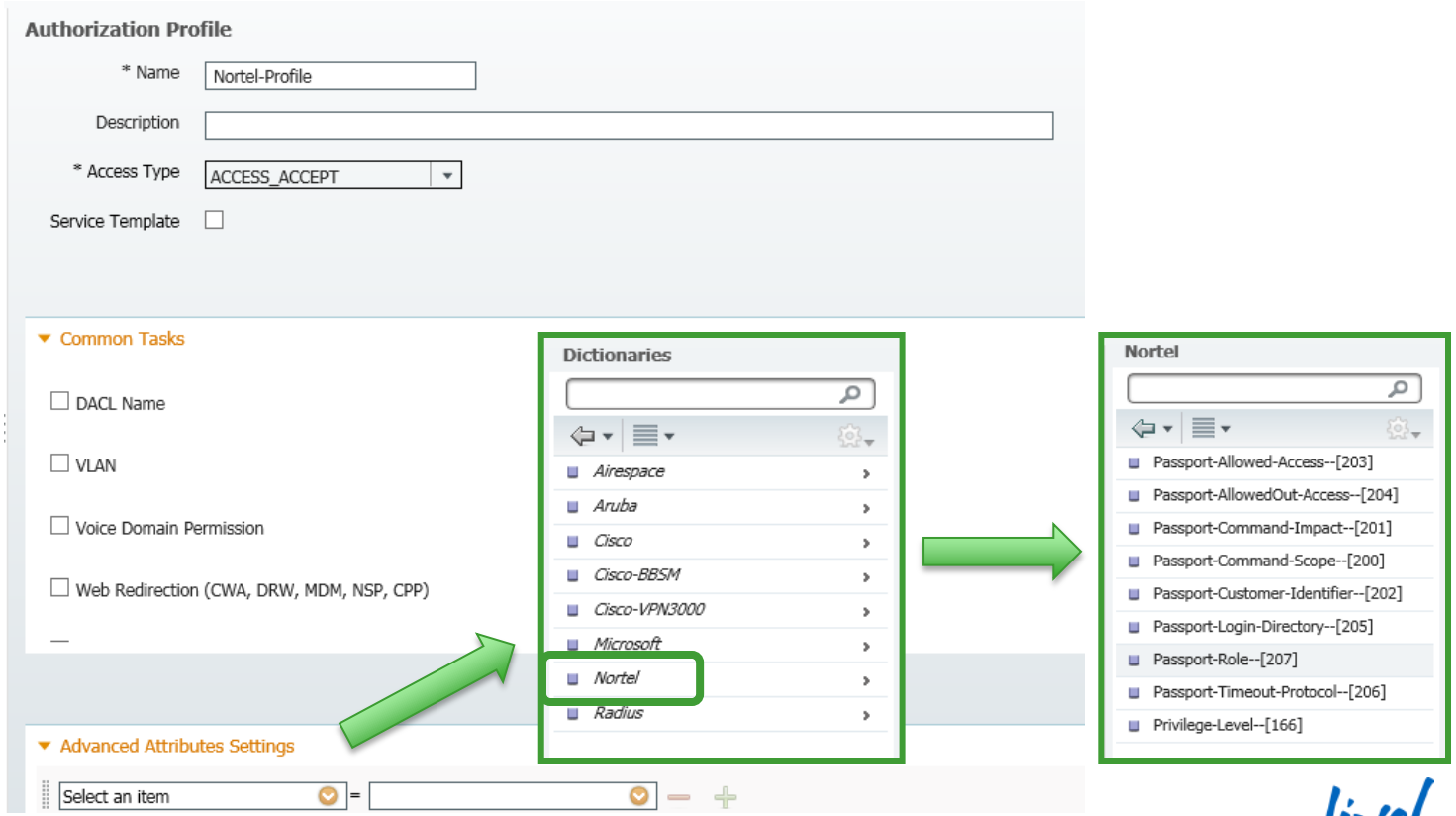
RADIUS Vendors

Edit | Add | Delete | Import | Export

Name	Vendor ID	Description
Airespace	14179	Dictionary for Vendor Airespace
Aruba	14823	Dictionary for Vendor Aruba
Cisco	9	Dictionary for Vendor Cisco
Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000
Microsoft	311	Dictionary for Vendor Microsoft
Nortel	562	Dictionary for Vendor Nortel

Authorisation Profiles for Third Party

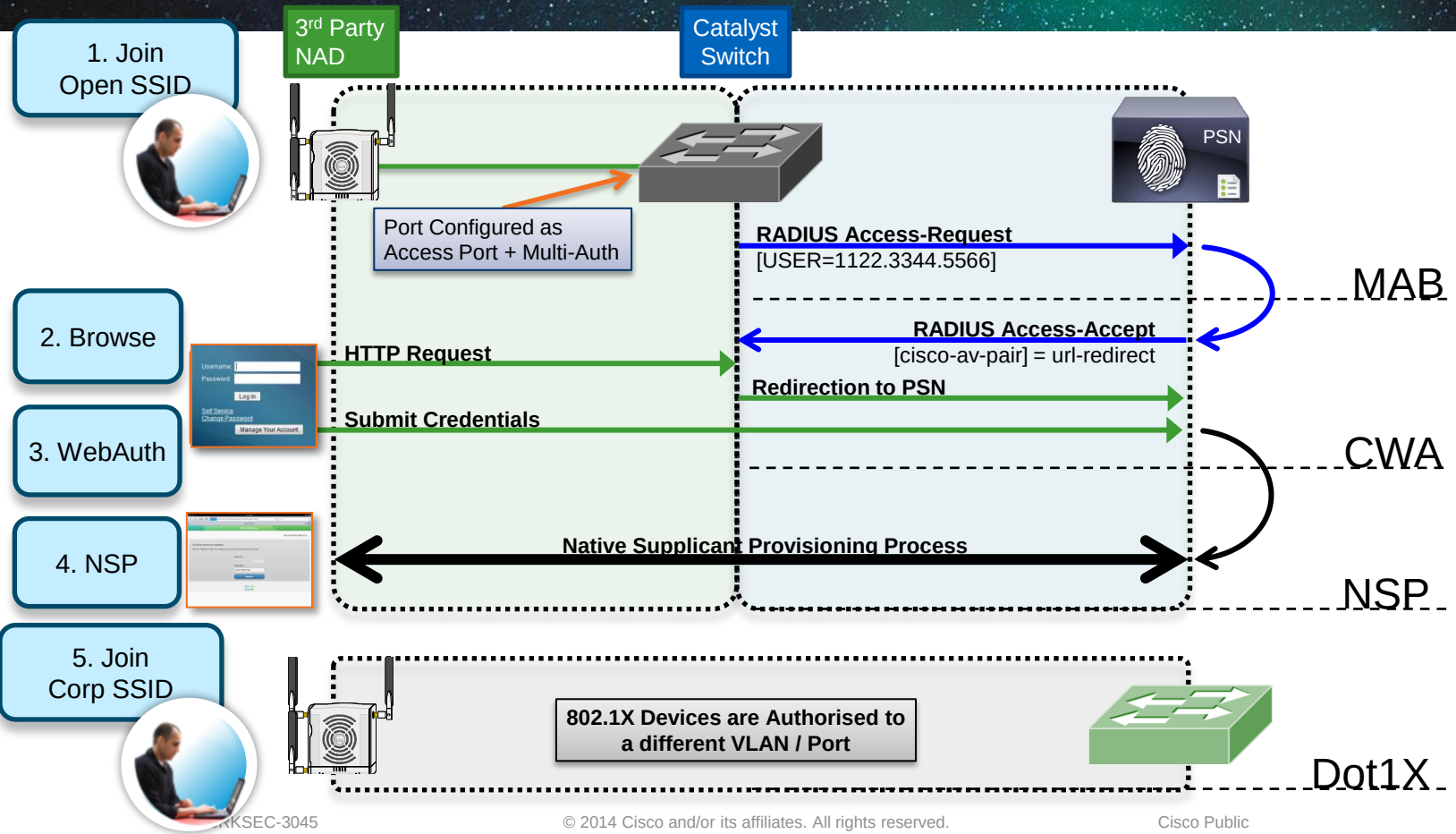
Go to “Advanced Attribute Settings” to use the 3rd Party Dictionaries



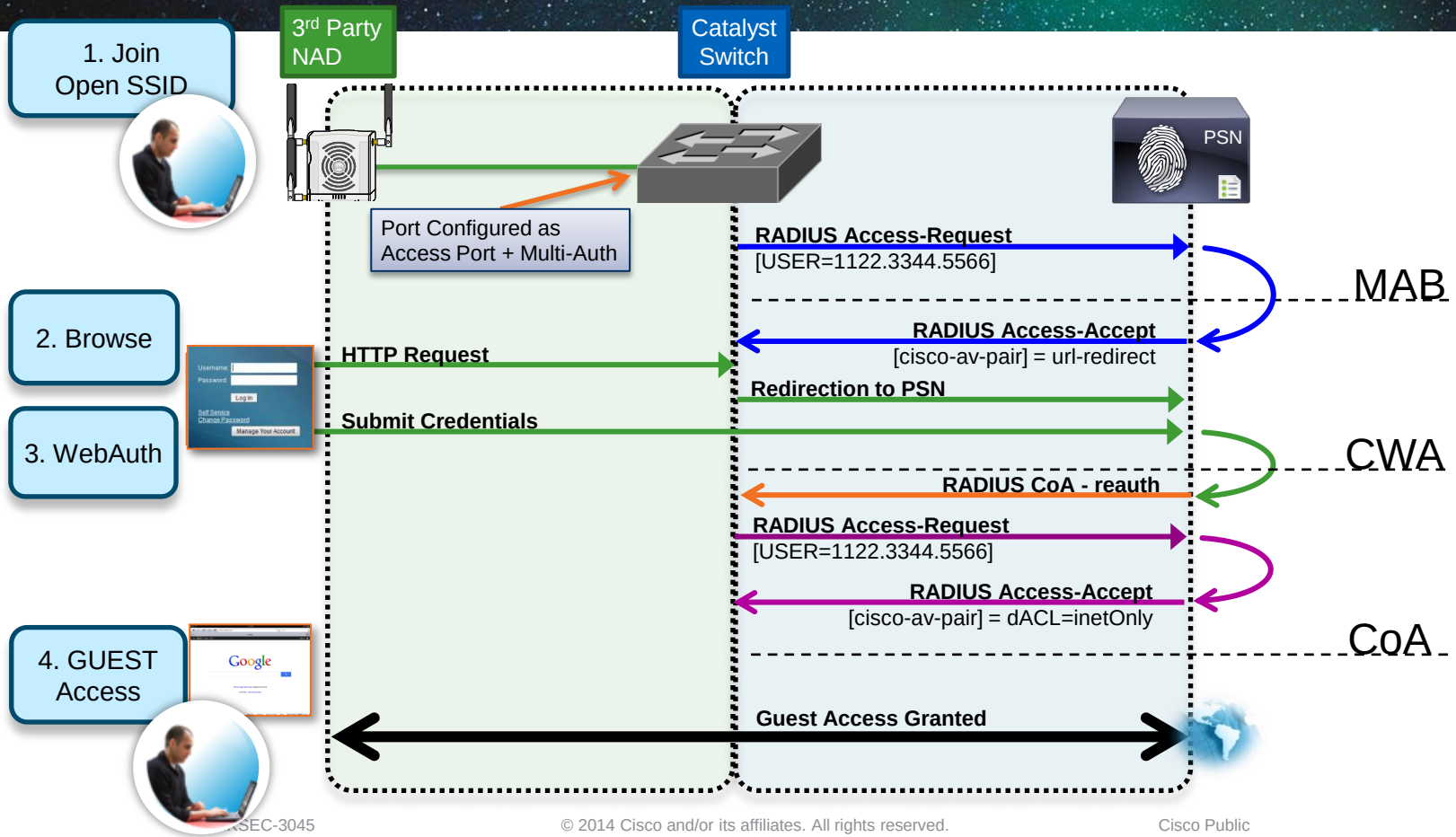



BYOD Onboarding for 3rd Party NADs

Using a Cisco Catalyst Switch as Inline PeP



Using a Cisco Catalyst Switch as Inline PeP



Details On 3rd PARTY On-Boarding Process

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if **Blacklist** AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if **Cisco-IP-Phone**	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
✓	Employee and CorpMachine	if EmployeeFullEAPChain	then Employee Full Access
✓	Employee iDevices	if (EndPoints:LogicalProfile EQUALS iDevices AND Employees)	then Internet Only
✓	Employee Limited	if AD1:ExternalGroups EQUALS ise.local/Users/Employees	then Employee Limited
✓	3rdParty NSP	if (4503 AND Gig2-6 AND Radius:Service-Type EQUALS Call Check)	then WEBAUTH
✓	Default	if no matches, then PermitAccess	

```
interface X
 description For 3rd Party Or
 switchport access vlan 41
 switchport mode access
 switchport voice vlan 99
 ip access-group ACL-ALLO
 authentication event fail acti
 authentication event server
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout quiet-period 300
 dot1x timeout tx-period 10
 spanning-tree portfast
 ip dhcp snooping information option allow-untrusted
end
```

To authenticate virtually unlimited endpoints

Since 99.9999% MAB, try MAB First

Will clear the mac-address after 5 minutes

Enabled Provisioning from CWA Flow

Multi-Portal

General | Operations | Custo

Guest Portal Policy Configuration

Guest users should agree to an acceptable use policy

- ○ Not Used
- ◉ First Login
- ○ Every Login

☑ Enable Self-Provisioning Flow

☑ Enable Mobile Portal

3rd Party Onboarding, WLC Configuration

General Information

Interface Name	Open-PassThru
MAC Address	d0:d0:fd:91:e2:60

Physical Information

Port Number	4
Backup Port	0
Active Port	0
Enable Dynamic AP Management	☐

Interface Address

VLAN Identifier	0
IP Address	10.1.41.254
Netmask	255.255.255.0
Gateway	10.1.41.1

Dedicated Physical Port

Open WLAN

General | **Security** | **QoS** | **Advanced**

Profile Name	OpenPassThru
Type	WLAN
SSID	OpenPassThru
Status	☑ Enabled
Security Policies	None
	(Modifications done under security t
Radio Policy	All
Interface/Interface Group(G)	open-passthru
Multicast Vlan Feature	☐ Enabled
Broadcast SSID	☑ Enabled

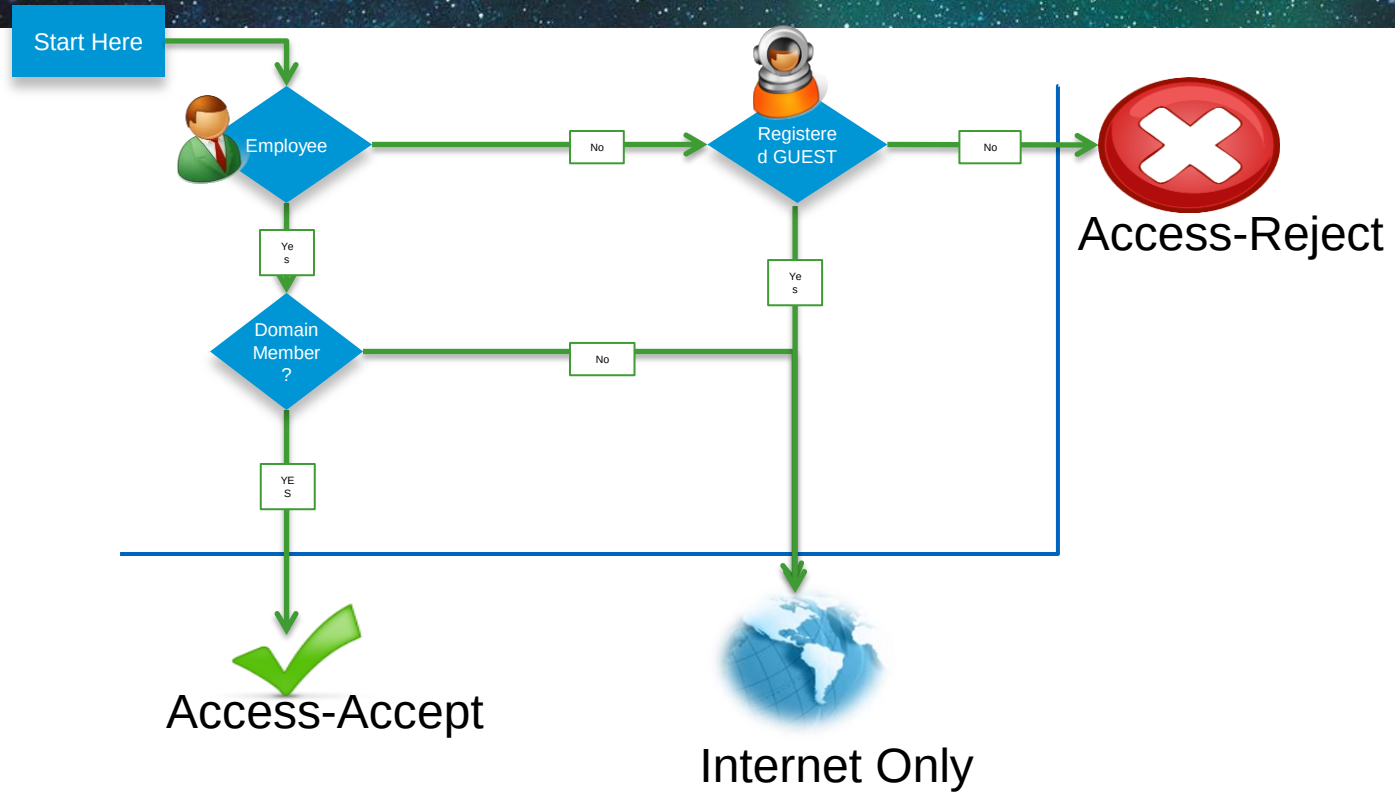



The Opposite of BYOD:

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)

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

The next chapter of authentication: EAP-Chaining

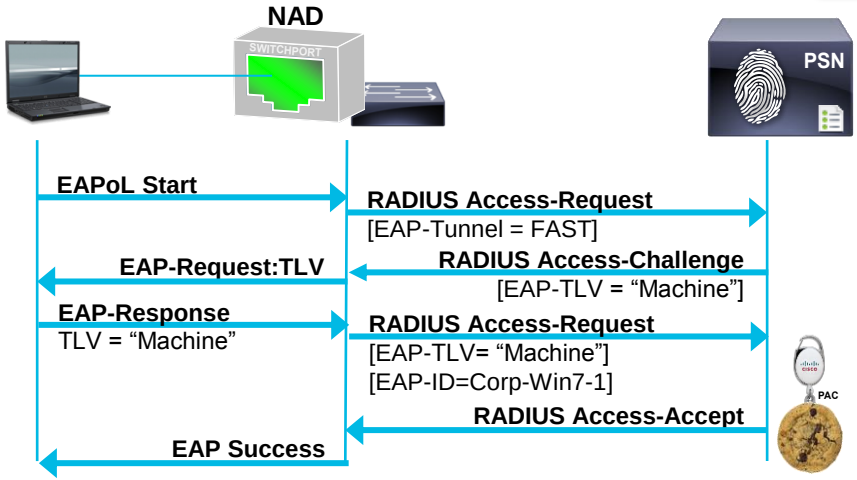
- IETF working group is in process of standardising on Tunneled EAP (TEAP).
  - Next-Generation EAP method that provides all benefits of current EAP Types.
  - Also provides EAP-Chaining.
- Cisco will do it before TEAP is ready
  - EAP-FASTv2
  - AnyConnect 3.1
  - Identity Services Engine 1.1.1 (1.1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

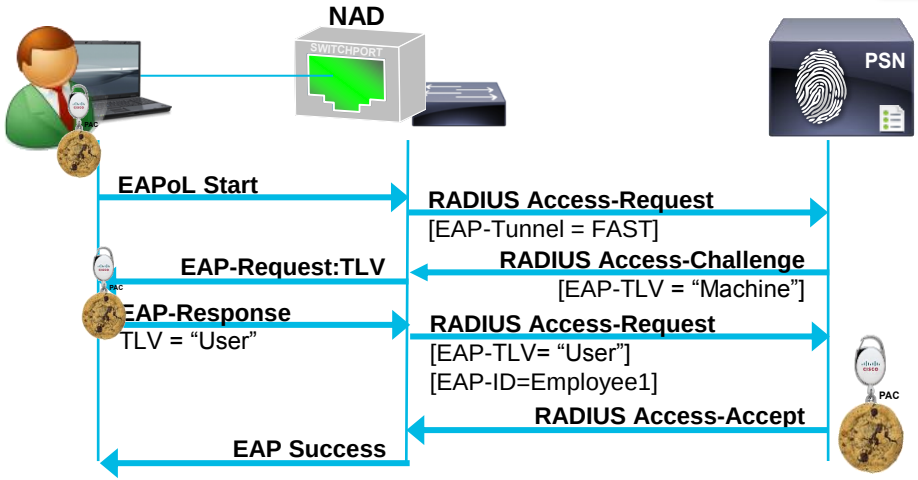


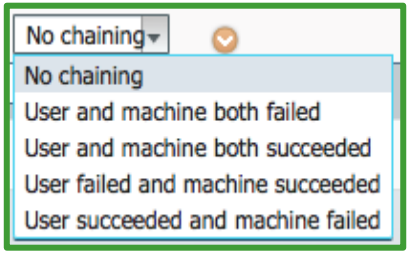
EAP-Chaining

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		





Identifying the Machine AND the User

What to do when EAP-Chaining is not Available?

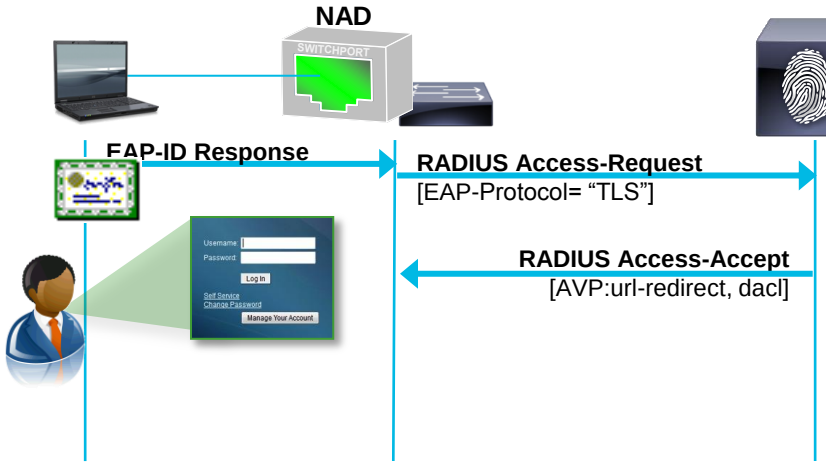
- There are many needs to determine Machine AND the User
  - Windows is the only current OS that can run EAP-Chaining (with AnyConnect)
  - What about iOS or Android based Tablets?

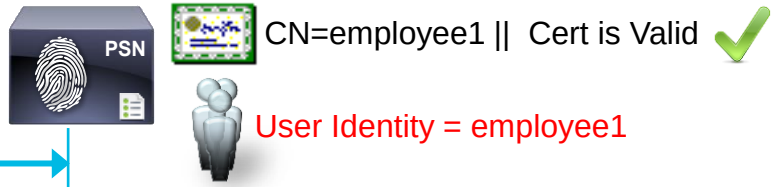
- Chain together 802.1X with Centralised Web Authentication (CWA)
  - Can validate the device using a user-issued certificates
  - Will validate the ‘actual user’ with username/password or smartcard or other method that validates the user

802.1X and CWA Chaining

1. EAP-TLS Authentication
2. ISE Sends Access-Accept w/ URL-Redirect

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
Employee_CWA	if	Employee & **Network Access:UseCase = GuestFlow**	then	Employee & SGT
Employee_1X	if	Employee & **Network Access: EAPAuthentication = EAP-TLS**	then	CWA
Default	If no matches, then		WEBAUTH	

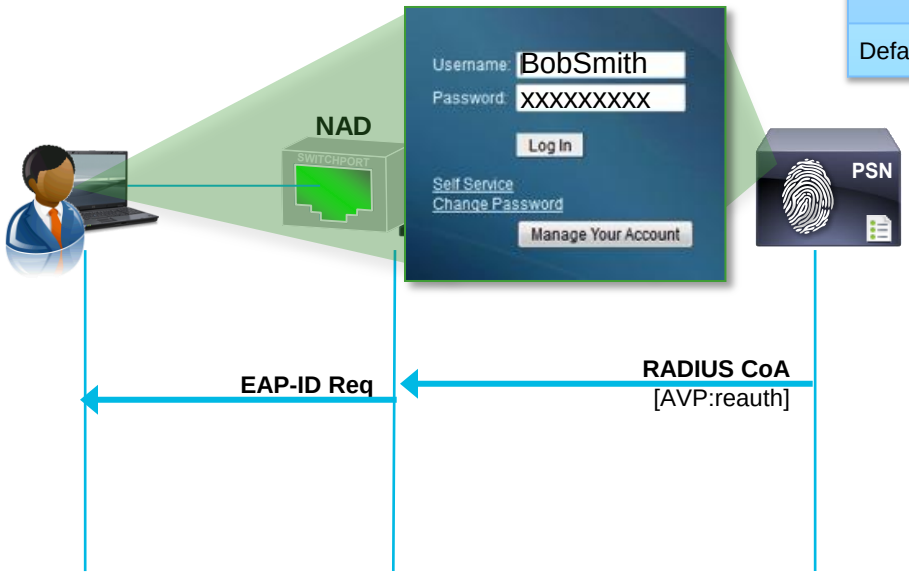




802.1X and CWA Chaining

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
Employee_CWA	if	Employee & **Network Access:UseCase = GuestFlow**	then	Employee & SGT
Employee_1X	if	Employee & **Network Access: EAPAuthentication = EAP-TLS**	then	CWA
Default	If no matches, then		WEBAUTH	

3. User Enters Uname/PWD
4. ISE Sends CoA-reauth

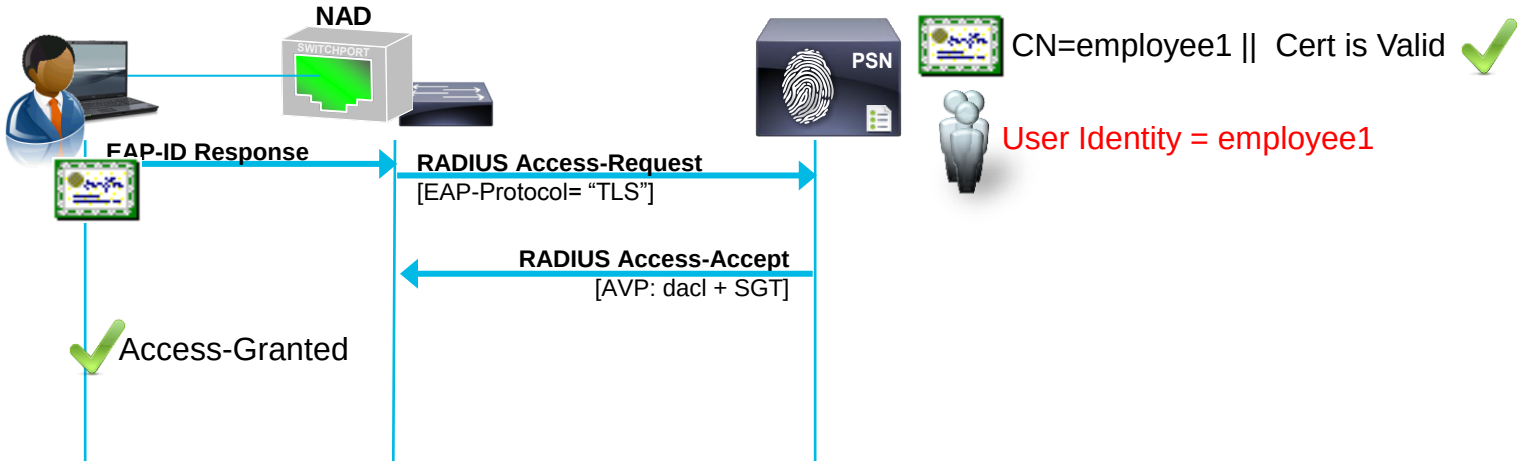


User Identity = employee1

802.1X and CWA Chaining

3. User Enters Uname/PWD
4. ISE Sends CoA-reauth
5. Supplicant Responds with Cert
6. ISE sends Accept, dACL & SGT

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
Employee_CWA	if	Employee & **Network Access:UseCase = GuestFlow**	then	Employee & SGT
Employee_1X	if	Employee & **Network Access: EAPAuthentication = EAP-TLS**	then	CWA
Default	If no matches, then		WEBAUTH	






Combining AND & OR

Combining AND with OR in AuthZ Policies

Authorization Compound Condition List > **New Authorization Compound Condition**

Compound Condition

* Name: ConferenceRoomPorts

Description:

*Condition Expression

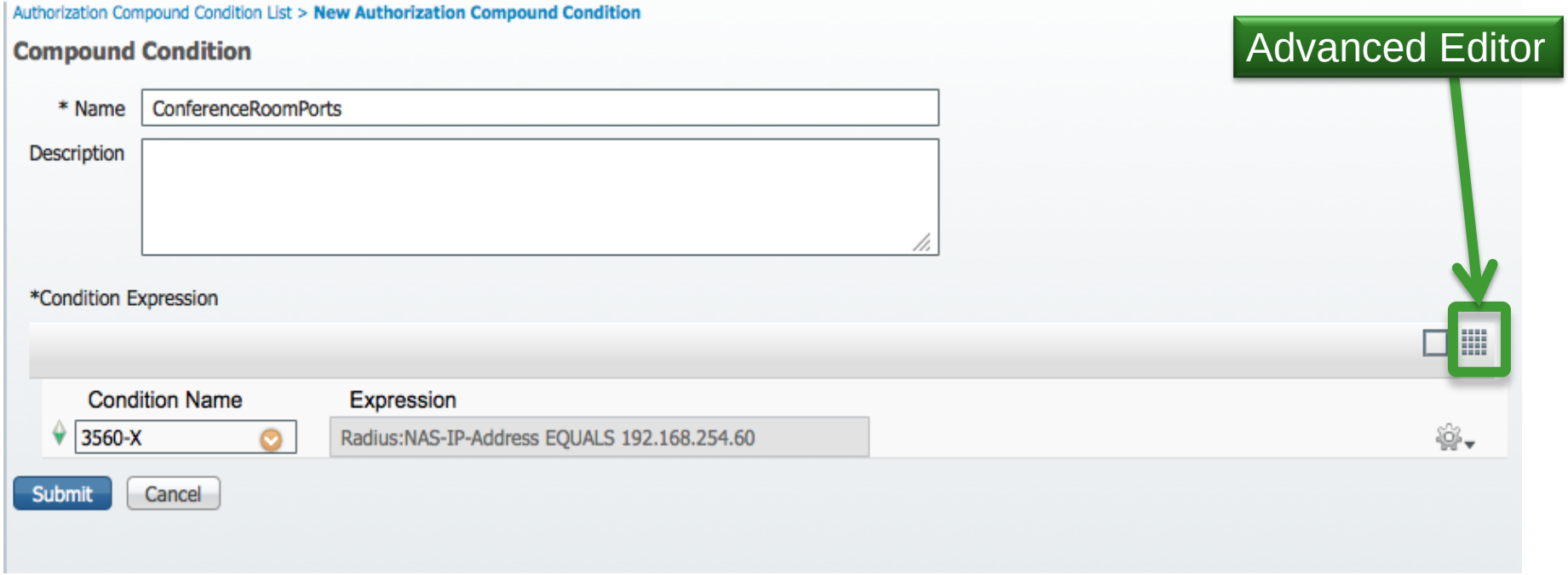
Condition Name	Expression	OR
3750	Radius:NAS-IP-Address EQUALS 192.168.254.21	OR
Gig0-0	Radius:NAS-Port-Id EQUALS GigabitEthernet0/0	OR
3560	Radius:NAS-IP-Address EQUALS 192.168.254.22	

Submit Cancel

Cannot Mix??

Combining AND with OR in AuthZ Policies

Advanced Editing



Combining AND with OR in AuthZ Policies

Advanced Editing

Authorization Compound Condition List > **New Authorization Compound Condition**

Compound Condition

* Name: ConferenceRoomPorts

Description:

*Condition Expression

Select a condition to insert below | ( ) | ! | & | |

```
( 3560-X & ( port-G1 | port-G2 | port-G7 ) ) | ( 3750-X & ( port-G1-0-1 | port-G1-0-13 ) )
```

Simple Conditions

Submit | Cancel

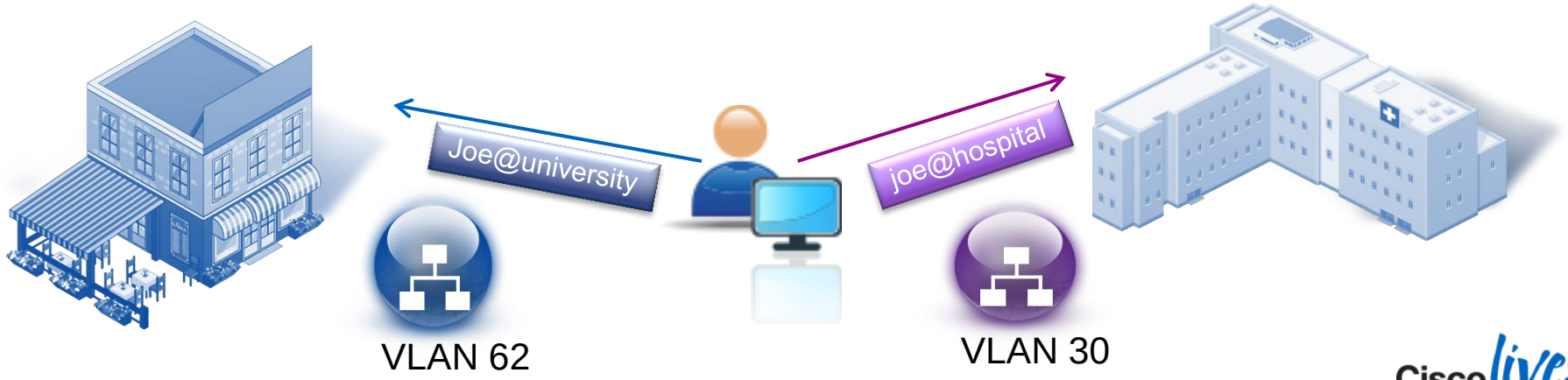



Realm Stripping

Authorisation for AD Domain Stripping

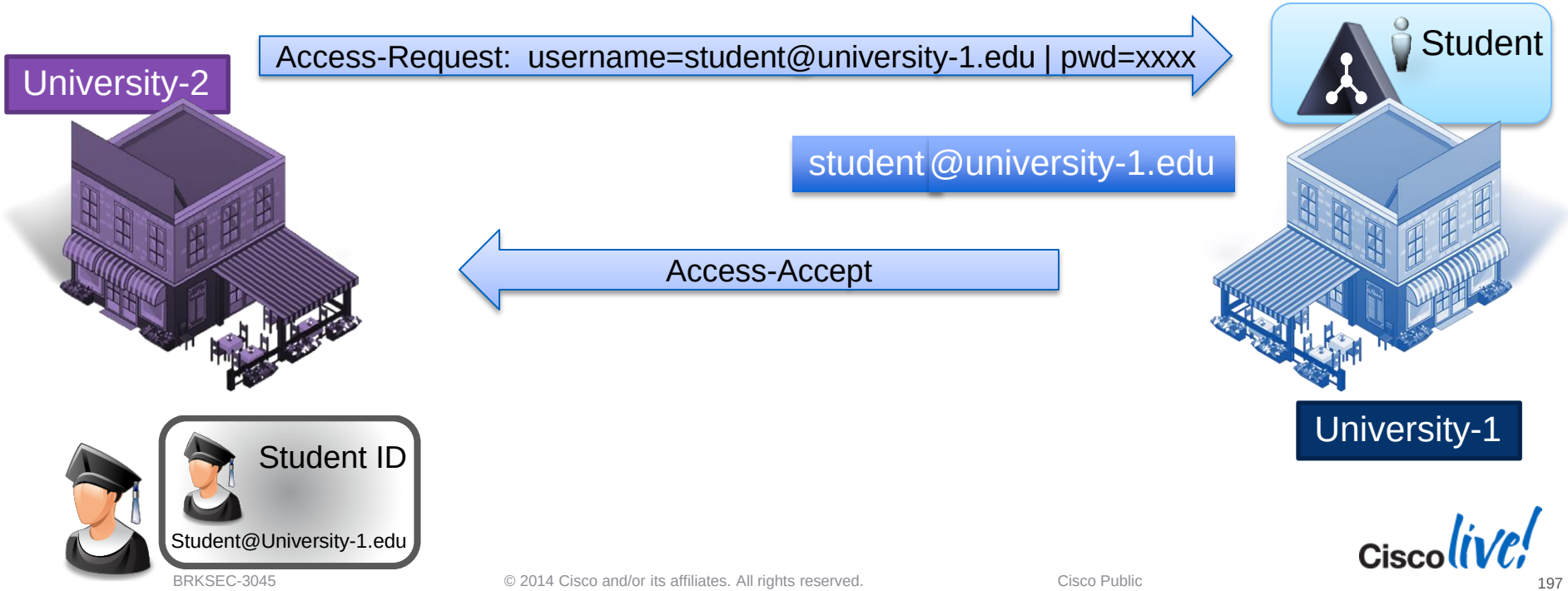
- Authorisation rules can use the realm from the RADIUS username

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	University	if Radius:User-Name CONTAINS @university	then VLAN_University
✓	Hospital	if Radius:User-Name CONTAINS @hospital	then VLAN_Hospital



Realm Stripping (1.2.0 Patch 4)

- Eduroam use case:
  A University-1 student roams to University-2 and connects using the University-2 network



Configuration Example

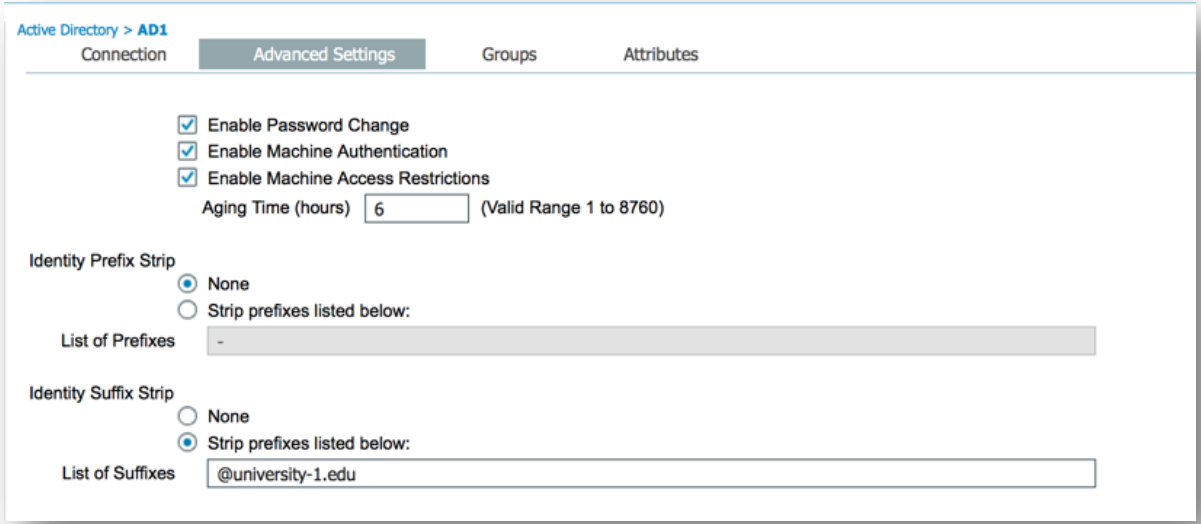
Prefix Stripping

Strip: "dom1\,dom2$,dom3"

dom1\brad becomes **brad**

dom2$brad becomes **brad**

dom3brad becomes **brad**



Suffix Stripping

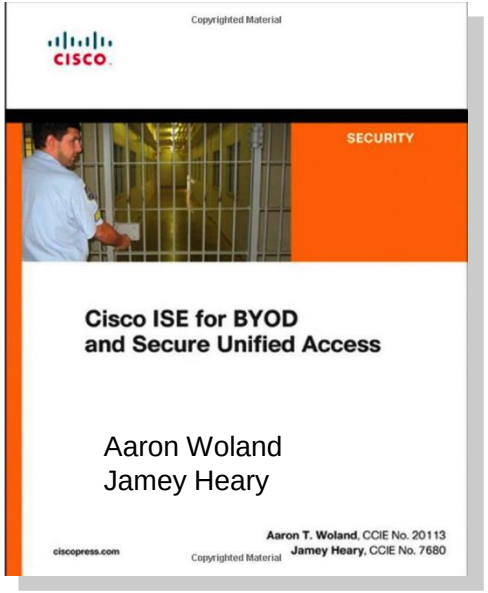
Strip: "@domain.com,@domain2"

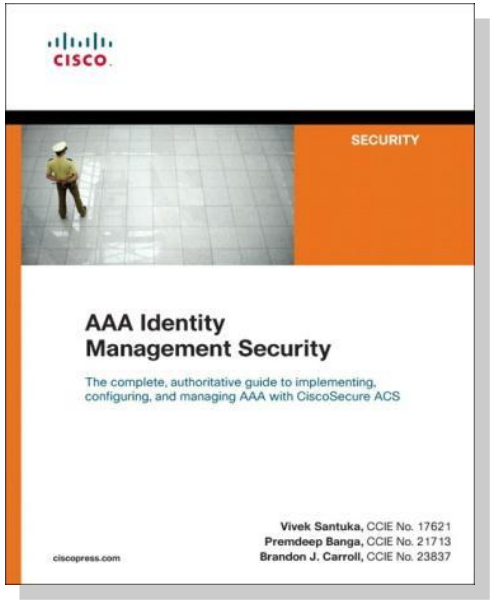
mary@domain.com becomes **mary**

mary@domain2.com becomes **mary**

Recommended Reading

- For reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2014





Links

- Secure Access, TrustSec, and ISE on Cisco.com
  - http://www.cisco.com/go/trustsec
  - http://www.cisco.com/go/ise
  - http://www.cisco.com/go/isepartner

- TrustSec and ISE Deployment Guides:
  - http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

- YouTube: Fundamentals of TrustSec:
  - http://www.youtube.com/ciscocin#p/c/0/MJJ93N-3Iew




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 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 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com

CISCO™