TOMORROW starts here.

CISCO

Cisco live!

Building an Enterprise Access Control Architecture with ISE

BRKSEC-2044

Imran Bashir

Technical Marketing Engineer

Session Abstract

This session covers the building blocks for a policy-based access control architecture for wired, wireless, and VPN networks using Identity Services Engine. Starting with basic user and device authentication and authorisation using technologies like 802.1X, MAB, Web Authentication, and certificates/PKI, the session will show you how to expand policy decisions to include contextual information gathered from profiling, posture assessment, location, and external data stores such as AD and LDAP.

The architecture will be expanded further to address key use cases such as Guest access and management, BYOD (device registration and supplicant provisioning), MDM policy integration, and 802.1AE (MACsec).

Visibility and pervasive policy enforcement through VLANs, ACLs, and Security Group Access (SGA) will also be discussed.

This session is intended for Network, Security and Systems Administrators, Engineers, and Managers that need to implement the next generation Unified Access Network.

Housekeeping

- Reference slides will be in the published version only
- Visit Cisco Live Online: CiscoLive365.com
- Questions are welcome! Try our new online Q&A!
- Please use the microphone
- Please put your phone on stun.
- Visit the World of Solutions and Meet the Engineer
- Feedback welcome. Please complete online evaluation

ENJOY THE RIDE!

Secure Access and TrustSec Introduction

What is Secure Access and TrustSec?

- Think of it as “Next-Generation NAC”
- Secure Access is Cisco’s Architecture for Context-based Identity and Access Control
- TrustSec is a Systems approach to applying Policy across the network and encompasses the building blocks for Identity & Access Control:
  - RADIUS
  - IEEE 802.1X (Dot1x)
  - Profiling Technologies
  - Guest Services
  - Device Management
  - Secure Group Access (SGA)
  - MACsec (802.1AE)
  - Identity Services Engine (ISE)

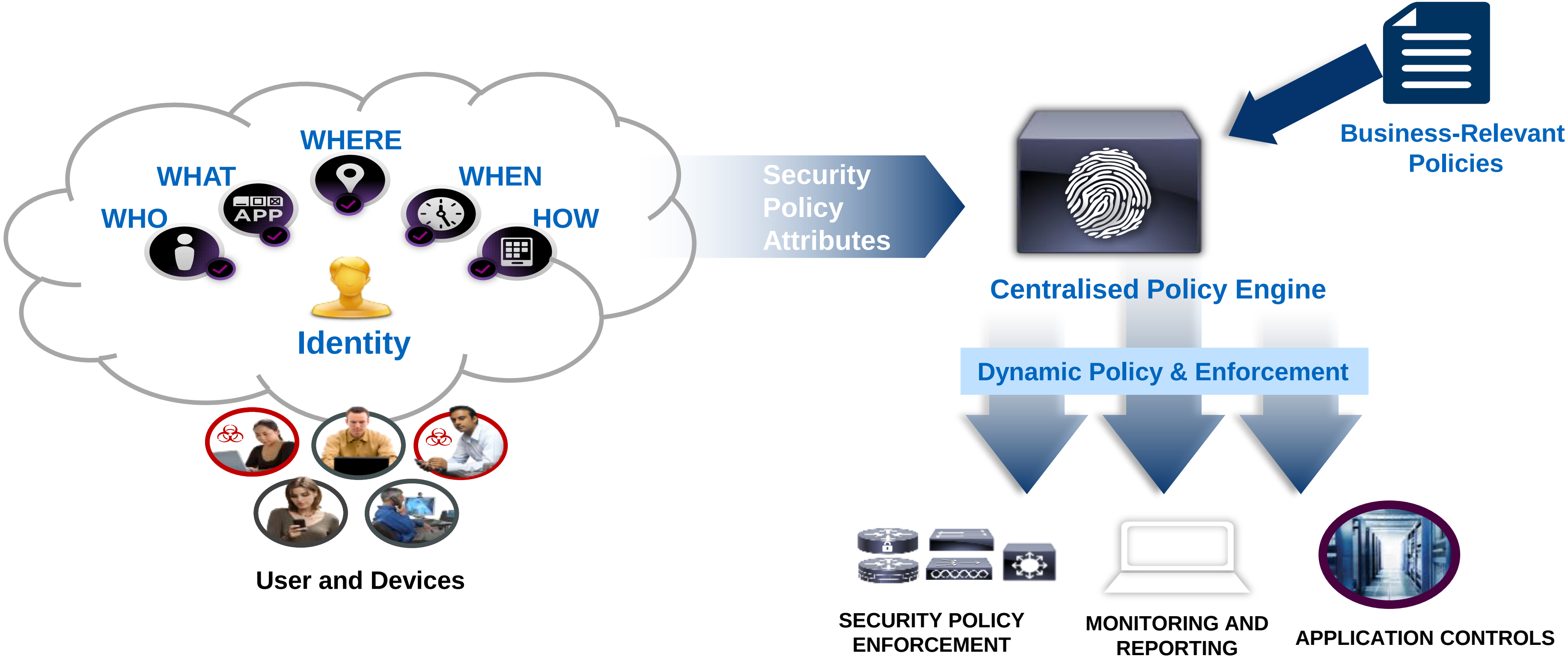
Secure Access and TrustSec = Identity, Right?

- Yes, but it refers to an Identity System (or Solution)
  - Policy servers are only as good as the intel received about the endpoints requiring access and the devices that enforce policy (Switches, WLCs, Firewalls, etc…)
- So what is "Identity"?
  - Understanding the Who / What / Where / When and How of users and devices that access the network = **CONTEXT**

The Importance of Contextual Identity [redacted]

Cisco Secure Access Architecture

Identity and Context-Centric Security


WHERE
WHAT
WHEN
WHO
APP
HOW
Identity
Security Policy Attributes
Centralised Policy Engine
Business-Relevant Policies
Dynamic Policy & Enforcement
User and Devices
SECURITY POLICY ENFORCEMENT
MONITORING AND REPORTING
APPLICATION CONTROLS

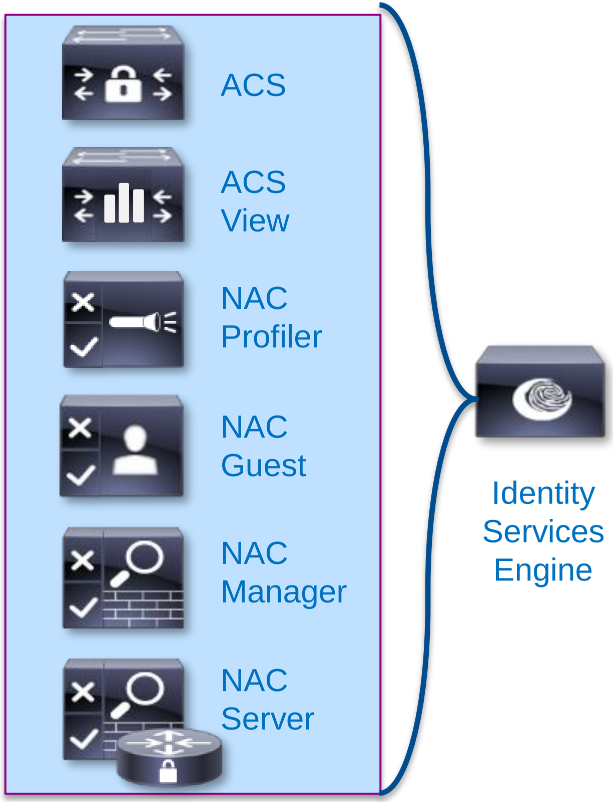
What is the Identity Services Engine?

ISE is a Next-Generation RADIUS Server

RADIUS SERVER CORE

Identity Services Engine

Policy Server Designed for Secure Network Access



Centralised Policy

AAA Services

Posture Assessment

Guest Access Services

Device Profiling

Monitoring

Troubleshooting

Reporting

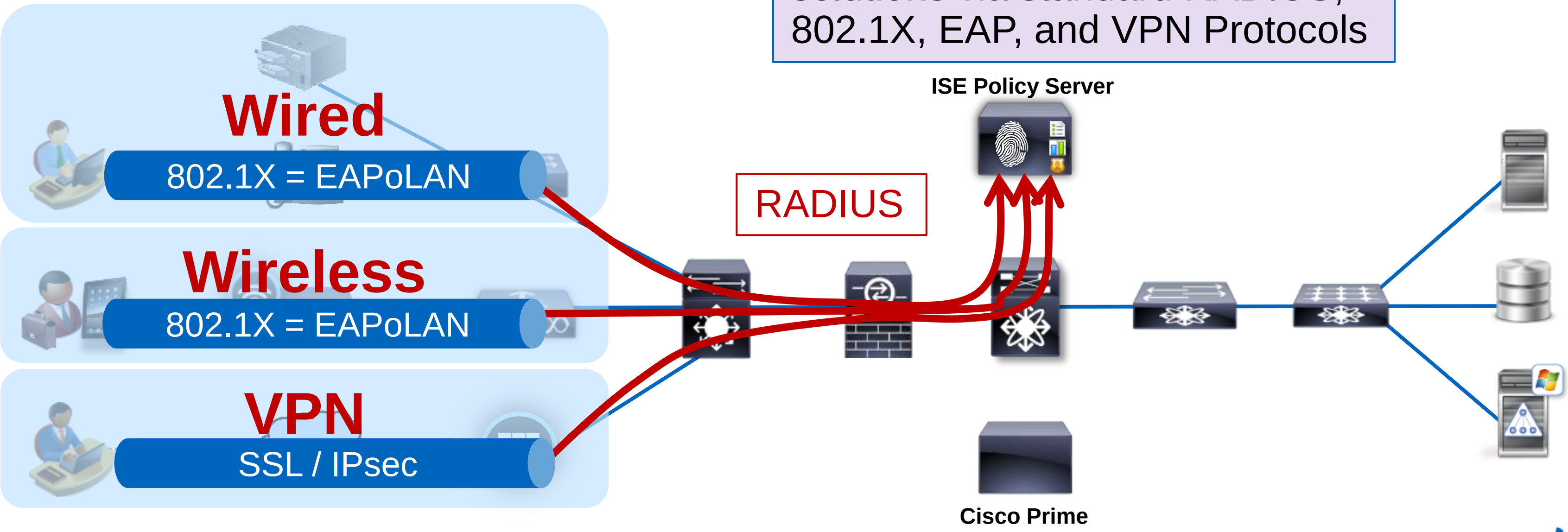
Authentication, Authorisation, and Accounting

“Who” is Connecting, Access Rights Assigned, and Logging It

ISE is a Standards-Based AAA Server

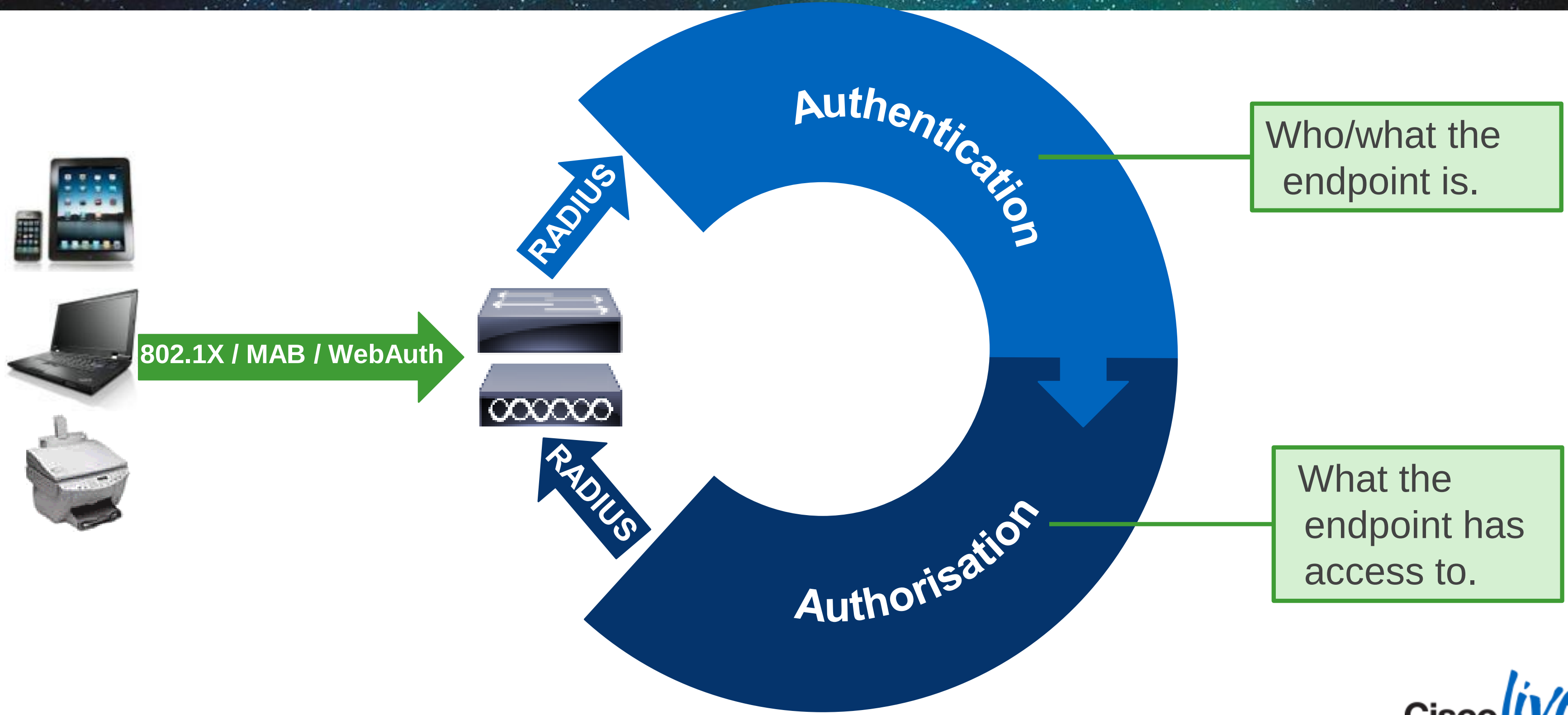
Access Control System Must Support All Connection Methods

Supports Cisco and 3rd-Party solutions via standard RADIUS, 802.1X, EAP, and VPN Protocols



Authentication and Authorisation

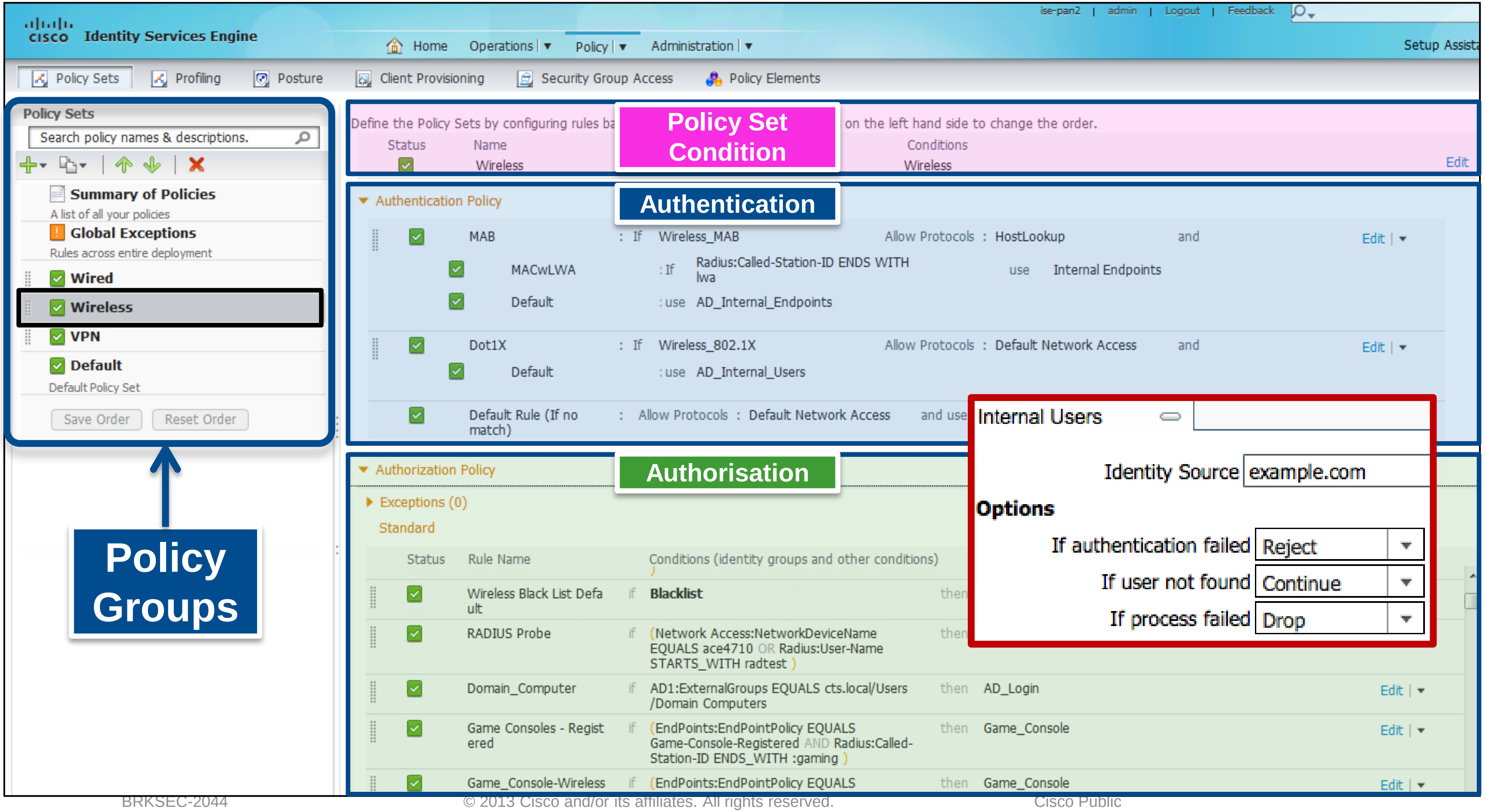
What's the Difference?



Who/what the endpoint is.

What the endpoint has access to.

Separation of Authentication and Authorisation



Policy Sets

Search policy names & descriptions.

Summary of Policies
A list of all your policies

Global Exceptions
Rules across entire deployment

☑ **Wired**

☑ **Wireless**

☑ **VPN**

☑ **Default**
Default Policy Set

Define the Policy Sets by configuring rules ba... on the left hand side to change the order.

Status	Name	Conditions	
☑	Wireless	Wireless	Edit

Policy Set Condition

Authentication Policy

Authentication

☑ MAB : If Wireless_MAB Allow Protocols : HostLookup and Edit |
- ☑ MACwLWA : If Radius:Called-Station-ID ENDS WITH lwa use Internal Endpoints
- ☑ Default : use AD_Internal_Endpoints

☑ Dot1X : If Wireless_802.1X Allow Protocols : Default Network Access and Edit |
- ☑ Default : use AD_Internal_Users

☑ Default Rule (If no match) : Allow Protocols : Default Network Access and use Internal Users

Identity Source: example.com

Options

If authentication failed: Reject

If user not found: Continue

If process failed: Drop

Authorization Policy

Authorisation

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist**	then		
☑	RADIUS Probe	if	(Network Access:NetworkDeviceName EQUALS ace4710 OR Radius:User-Name STARTS_WITH radtest)	then		
☑	Domain_Computer	if	AD1:ExternalGroups EQUALS cts.local/Users /Domain Computers	then	AD_Login	Edit |
☑	Game Consoles - Registered	if	(EndPoints:EndPointPolicy EQUALS Game-Console-Registered AND Radius:Called-Station-ID ENDS_WITH :gaming)	then	Game_Console	Edit |
☑	Game_Console-Wireless	if	(EndPoints:EndPointPolicy EQUALS	then	Game_Console	Edit |

Policy Groups

Authentication Rules

Choosing the Right ID Store

RADIUS Attributes

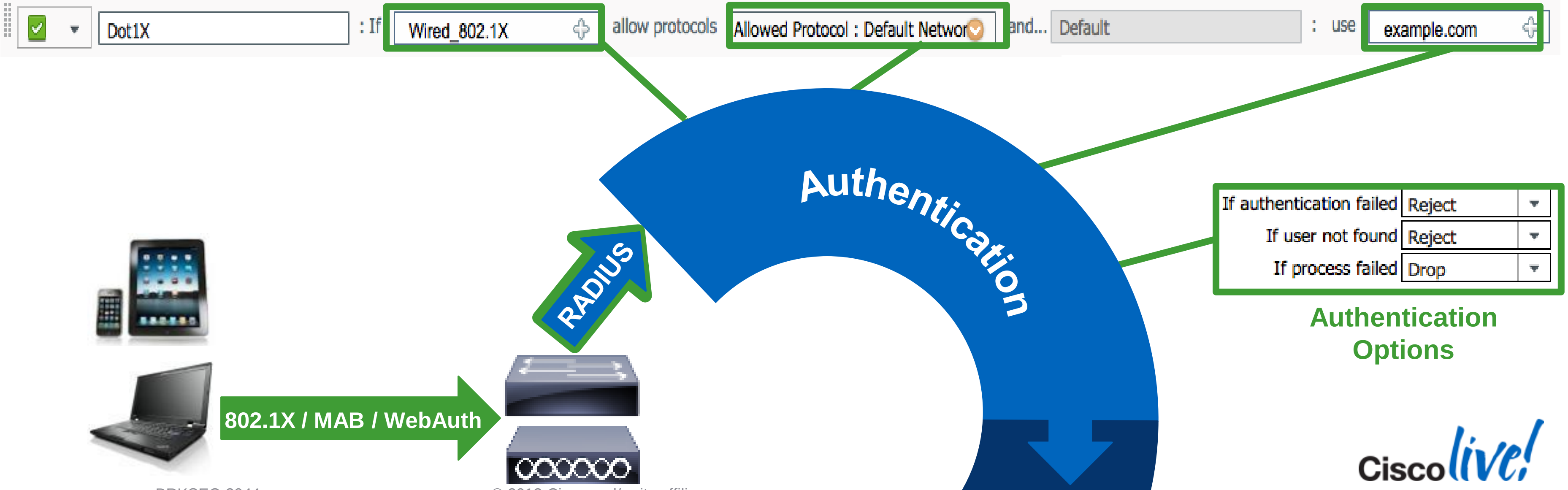
Service type
NAS IP
Username
SSID …

EAP Types

EAP-FAST
EAP-TLS
PEAP
EAP-MD5
Host lookup …

Identity Source

Internal/Certificate
Active Directory
LDAPv3
RADIUS
Identity Sequence



☑ Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Networ and… Default : use example.com

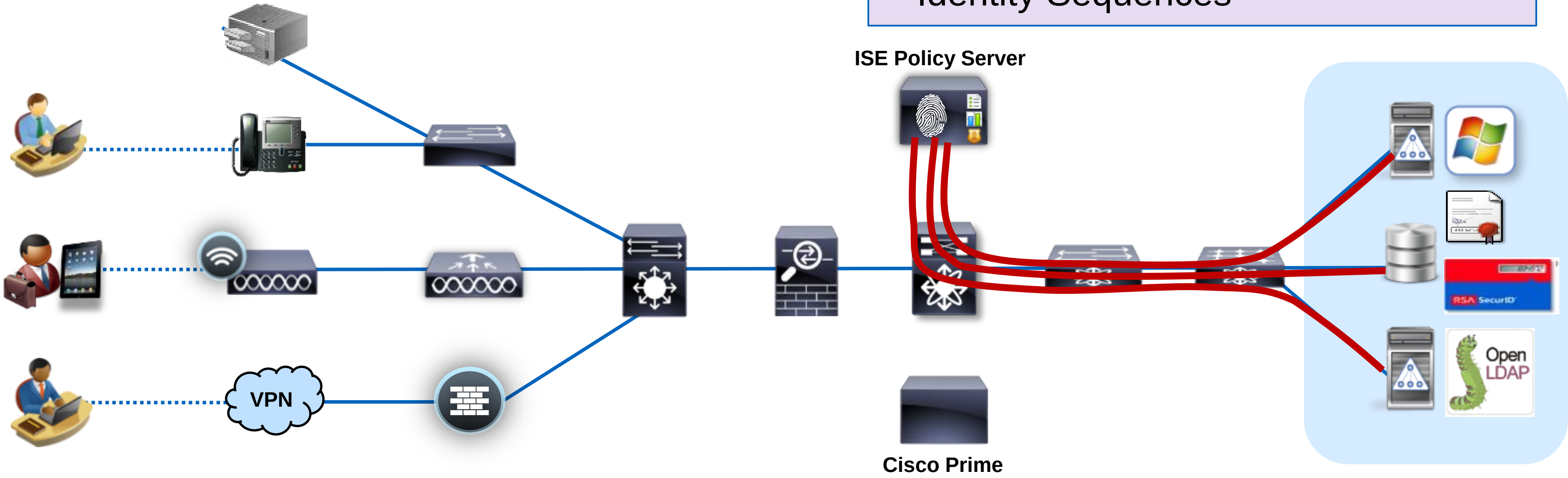
If authentication failed	Reject
If user not found	Reject
If process failed	Drop

Authentication Options

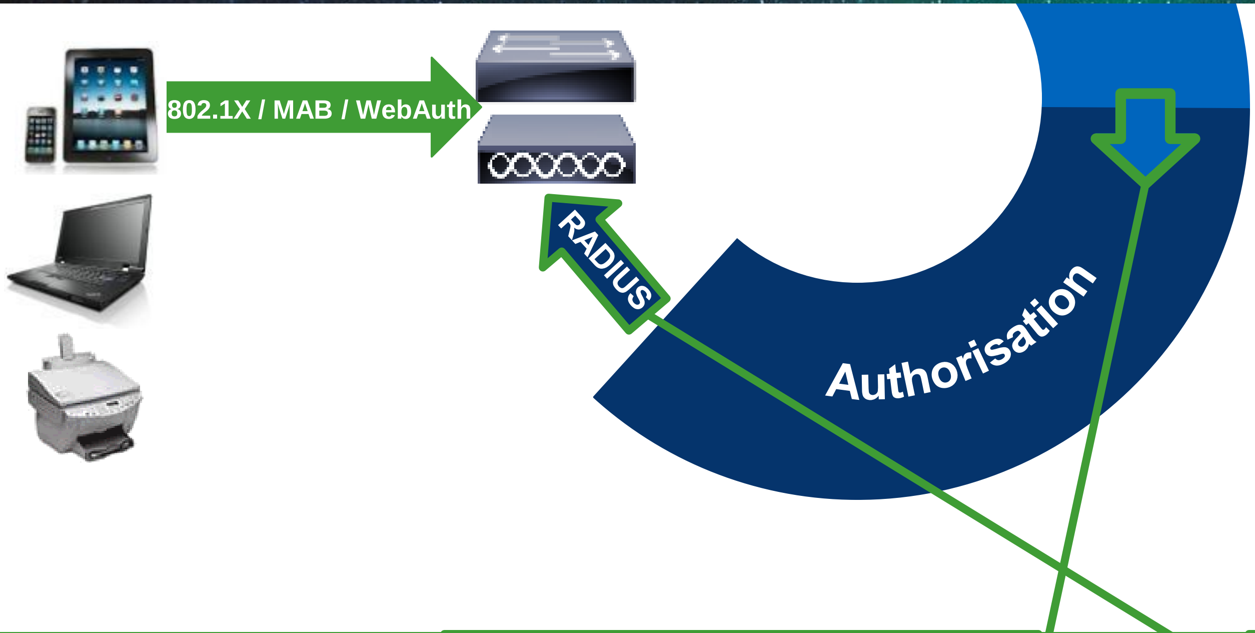
Integrating My Identity Stores

Local / LDAP / AD / RADIUS / Token Servers

- Microsoft AD Servers 2003-2012.
- LDAPv3-Compliant Servers
- External RADIUS Servers
- RSA and RFC-2865-Compliant One-Time Password/Token Servers
- Certificate Servers
- Identity Sequences

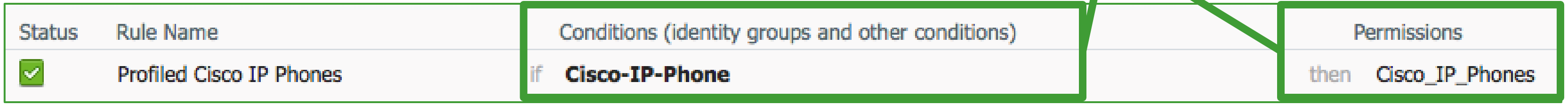


Authorisation Rules



Return standard IETF RADIUS / 3rd-Party Vendor Specific Attributes (VSAs):

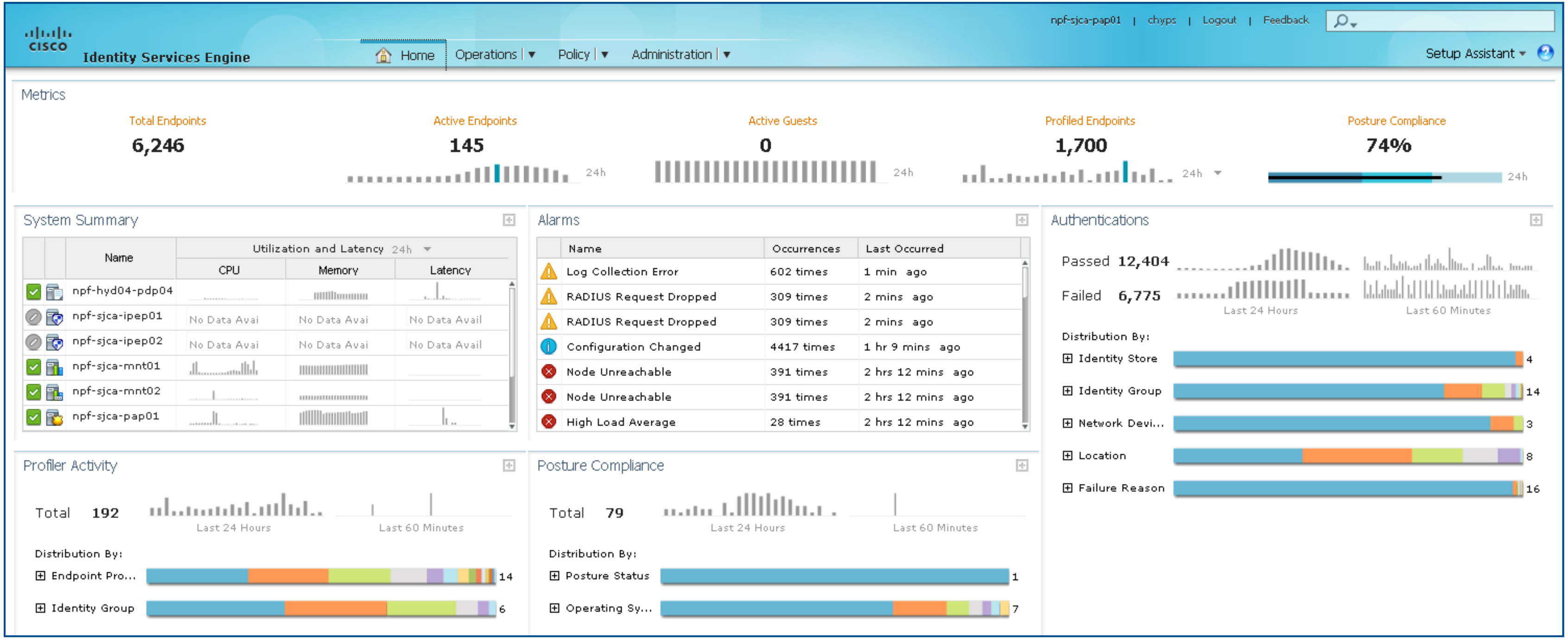
- ACLs (Filter-ID)
- VLANs (Tunnel-Private-Group-ID)
- Session-Timeout
- IP (Framed-IP-Address)
- Vendor-Specific including Cisco, Aruba, Juniper, etc.



Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Profiled Cisco IP Phones	if **Cisco-IP-Phone**	then Cisco_IP_Phones

What About That 3rd “A” in “AAA”?

Accounting



Metrics

Total Endpoints	Active Endpoints	Active Guests	Profiled Endpoints	Posture Compliance
6,246	145	0	1,700	74%
	24h	24h	24h	24h

System Summary

Name	CPU	Memory	Latency
npf-hyd04-pdp04			
npf-sjca-ipep01	No Data Avai	No Data Avai	No Data Avail
npf-sjca-ipep02	No Data Avai	No Data Avai	No Data Avail
npf-sjca-mnt01			
npf-sjca-mnt02			
npf-sjca-pap01			

Utilization and Latency 24h

Alarms

Name	Occurrences	Last Occurred
Log Collection Error	602 times	1 min ago
RADIUS Request Dropped	309 times	2 mins ago
RADIUS Request Dropped	309 times	2 mins ago
Configuration Changed	4417 times	1 hr 9 mins ago
Node Unreachable	391 times	2 hrs 12 mins ago
Node Unreachable	391 times	2 hrs 12 mins ago
High Load Average	28 times	2 hrs 12 mins ago

Authentications

Passed 12,404

Failed 6,775

Last 24 Hours Last 60 Minutes

Distribution By:

⊞ Identity Store	4
⊞ Identity Group	14
⊞ Network Devi...	3
⊞ Location	8
⊞ Failure Reason	16

Profiler Activity

Total 192

Last 24 Hours Last 60 Minutes

Distribution By:

⊞ Endpoint Pro...	14
⊞ Identity Group	6

Posture Compliance

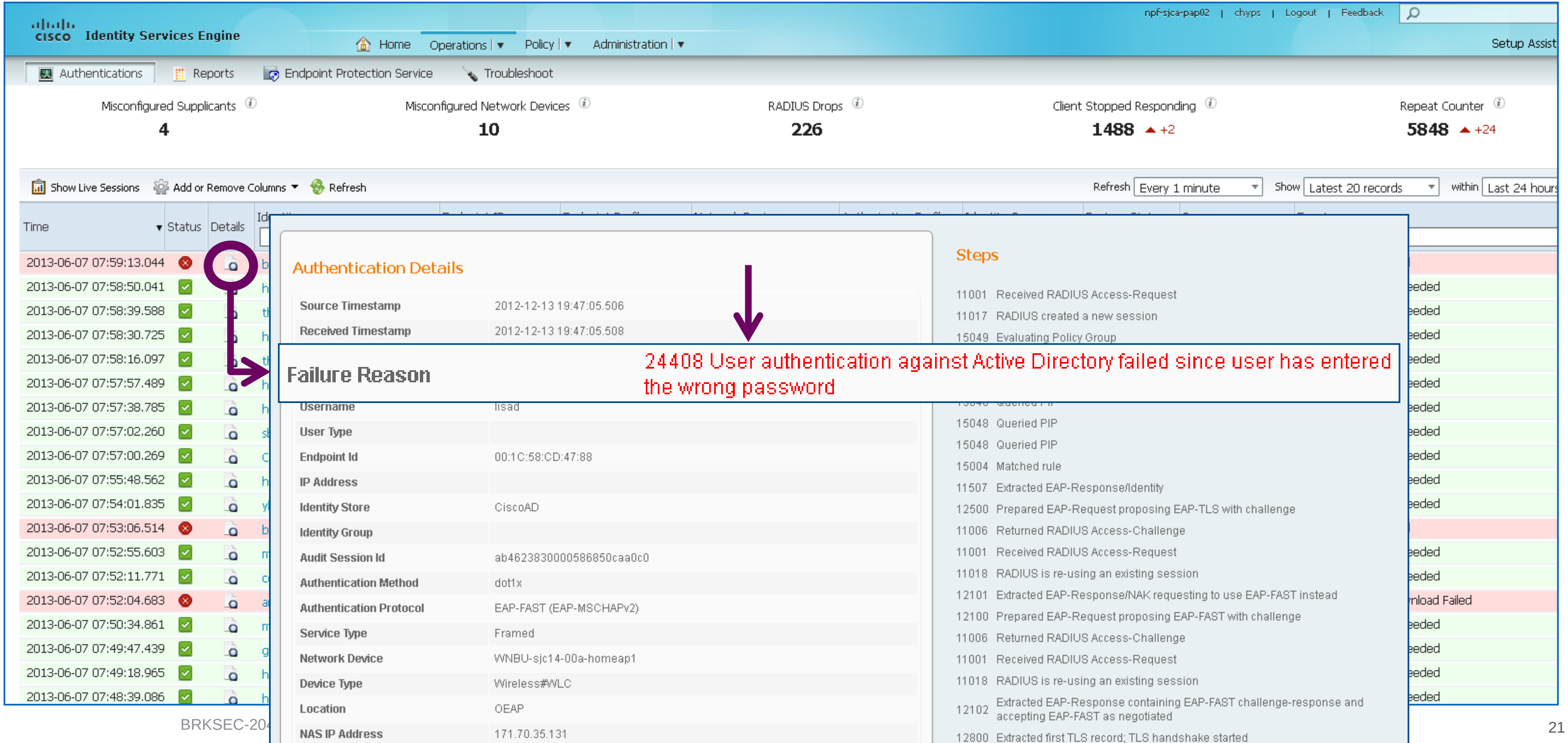
Total 79

Last 24 Hours Last 60 Minutes

Distribution By:

⊞ Posture Status	1
⊞ Operating Sy...	7

Detailed Visibility into Passed/Failed Attempts



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
4	10	226	1488 ▲ +2	5848 ▲ +24

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

Time	Status	Details	Id	
2013-06-07 07:59:13.044	☒		b	
2013-06-07 07:58:50.041	☑		h	eeded
2013-06-07 07:58:39.588	☑		th	eeded
2013-06-07 07:58:30.725	☑		h	eeded
2013-06-07 07:58:16.097	☑		th	eeded
2013-06-07 07:57:57.489	☑		h	eeded
2013-06-07 07:57:38.785	☑		h	eeded
2013-06-07 07:57:02.260	☑		sl	eeded
2013-06-07 07:57:00.269	☑		C	eeded
2013-06-07 07:55:48.562	☑		h	eeded
2013-06-07 07:54:01.835	☑		y	eeded
2013-06-07 07:53:06.514	☒		b	
2013-06-07 07:52:55.603	☑		m	eeded
2013-06-07 07:52:11.771	☑		c	eeded
2013-06-07 07:52:04.683	☒		a	nload Failed
2013-06-07 07:50:34.861	☑		m	eeded
2013-06-07 07:49:47.439	☑		g	eeded
2013-06-07 07:49:18.965	☑		h	eeded
2013-06-07 07:48:39.086	☑		h	eeded

Authentication Details

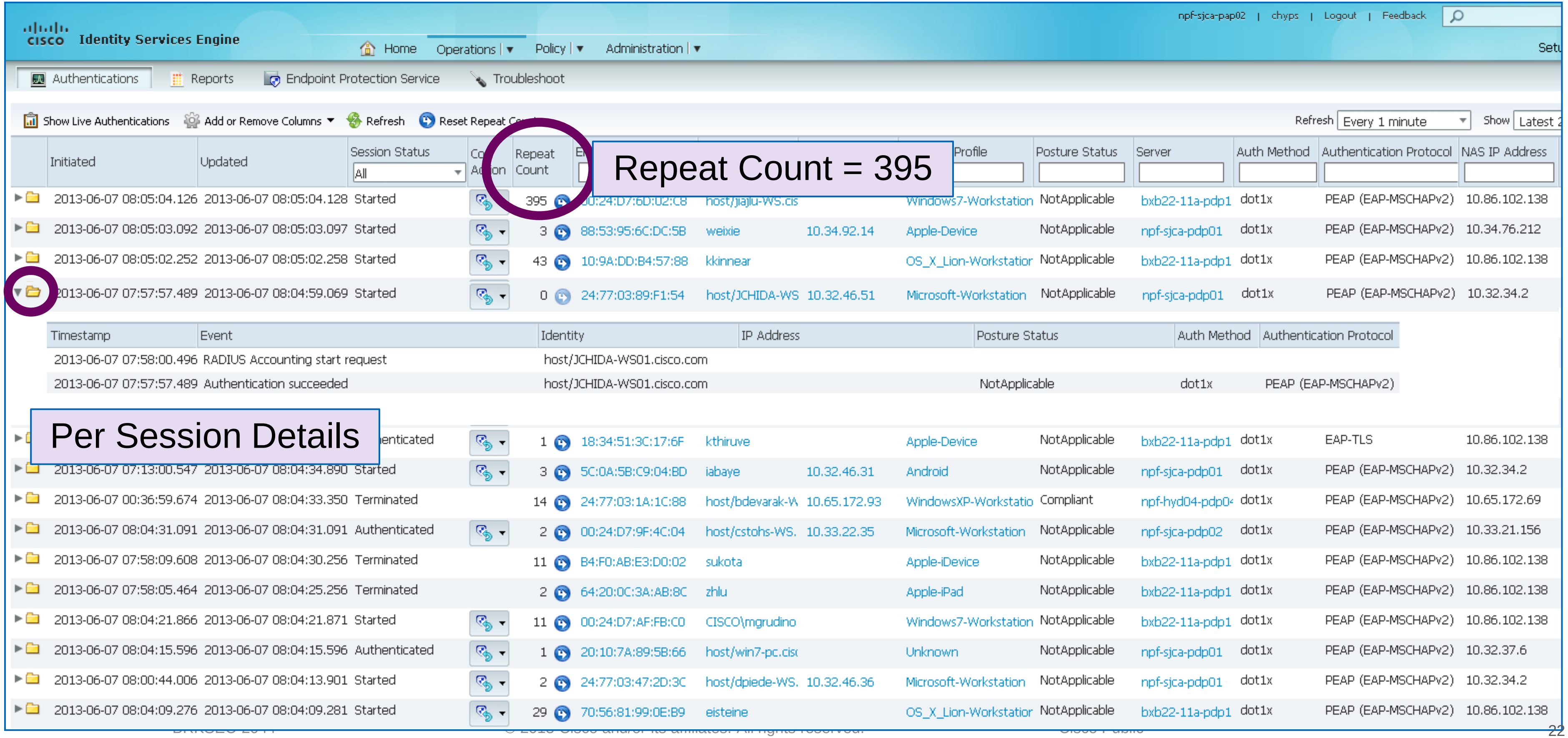
Source Timestamp	2012-12-13 19:47:05.506
Received Timestamp	2012-12-13 19:47:05.508
Username	lisad
User Type	
Endpoint Id	00:1C:58:CD:47:88
IP Address	
Identity Store	CiscoAD
Identity Group	
Audit Session Id	ab4623830000586850caa0c0
Authentication Method	dot1x
Authentication Protocol	EAP-FAST (EAP-MSCHAPv2)
Service Type	Framed
Network Device	WNBU-sjc14-00a-homeap1
Device Type	Wireless#WLC
Location	OEAP
NAS IP Address	171.70.35.131

Failure Reason 24408 User authentication against Active Directory failed since user has entered the wrong password

Steps

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
15049 Evaluating Policy Group
15048 Queried PIP
15048 Queried PIP
15004 Matched rule
11507 Extracted EAP-Response/Identity
12500 Prepared EAP-Request proposing EAP-TLS with challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12101 Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100 Prepared EAP-Request proposing EAP-FAST with challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800 Extracted first TLS record; TLS handshake started

Detailed Visibility into All Active Sessions and Access Policy Applied



Repeat Count = 395

	Initiated	Updated	Session Status	Co Action	Repeat Count	Ei			Profile	Posture Status	Server	Auth Method	Authentication Protocol	NAS IP Address
▶	2013-06-07 08:05:04.126	2013-06-07 08:05:04.128	Started		395		00:24:D7:6D:02:C8	host/jiajlu-WS.cis	Windows7-Workstation	NotApplicable	bxb22-11a-pdp1	dot1x	PEAP (EAP-MSCHAPv2)	10.86.102.138
▶	2013-06-07 08:05:03.092	2013-06-07 08:05:03.097	Started		3		88:53:95:6C:DC:5B	weixie	10.34.92.14 Apple-Device	NotApplicable	npf-sjca-pdp01	dot1x	PEAP (EAP-MSCHAPv2)	10.34.76.212
▶	2013-06-07 08:05:02.252	2013-06-07 08:05:02.258	Started		43		10:9A:DD:B4:57:88	kkinnear	OS_X_Lion-Workstatior	NotApplicable	bxb22-11a-pdp1	dot1x	PEAP (EAP-MSCHAPv2)	10.86.102.138
▼	2013-06-07 07:57:57.489	2013-06-07 08:04:59.069	Started		0		24:77:03:89:F1:54	host/JCHIDA-WS	10.32.46.51 Microsoft-Workstation	NotApplicable	npf-sjca-pdp01	dot1x	PEAP (EAP-MSCHAPv2)	10.32.34.2

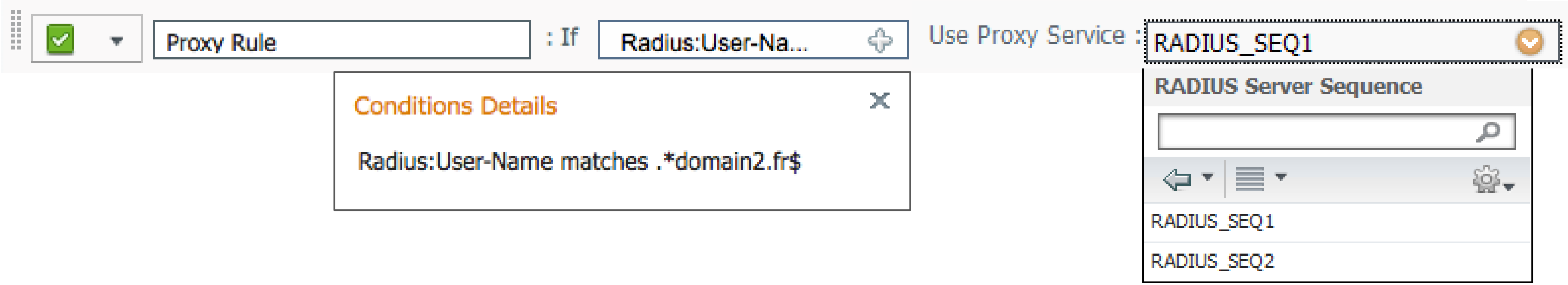
Timestamp	Event	Identity	IP Address	Posture Status	Auth Method	Authentication Protocol
2013-06-07 07:58:00.496	RADIUS Accounting start request	host/JCHIDA-WS01.cisco.com				
2013-06-07 07:57:57.489	Authentication succeeded	host/JCHIDA-WS01.cisco.com		NotApplicable	dot1x	PEAP (EAP-MSCHAPv2)

Per Session Details

	Initiated	Updated	Session Status	Co Action	Repeat Count	Endpoint ID	Identity	IP Address	Profile	Posture Status	Server	Auth Method	Authentication Protocol	NAS IP Address
▶			enticated		1	18:34:51:3C:17:6F	kthiruve		Apple-Device	NotApplicable	bxb22-11a-pdp1	dot1x	EAP-TLS	10.86.102.138
▶	2013-06-07 07:13:00.547	2013-06-07 08:04:34.890	Started		3	5C:0A:5B:C9:04:BD	iabaye	10.32.46.31	Android	NotApplicable	npf-sjca-pdp01	dot1x	PEAP (EAP-MSCHAPv2)	10.32.34.2
▶	2013-06-07 00:36:59.674	2013-06-07 08:04:33.350	Terminated		14	24:77:03:1A:1C:88	host/bdevarak-W	10.65.172.93	WindowsXP-Workstatio	Compliant	npf-hyd04-pdp0	dot1x	PEAP (EAP-MSCHAPv2)	10.65.172.69
▶	2013-06-07 08:04:31.091	2013-06-07 08:04:31.091	Authenticated		2	00:24:D7:9F:4C:04	host/cstohs-WS.	10.33.22.35	Microsoft-Workstation	NotApplicable	npf-sjca-pdp02	dot1x	PEAP (EAP-MSCHAPv2)	10.33.21.156
▶	2013-06-07 07:58:09.608	2013-06-07 08:04:30.256	Terminated		11	B4:F0:AB:E3:D0:02	sukota		Apple-iDevice	NotApplicable	bxb22-11a-pdp1	dot1x	PEAP (EAP-MSCHAPv2)	10.86.102.138
▶	2013-06-07 07:58:05.464	2013-06-07 08:04:25.256	Terminated		2	64:20:0C:3A:AB:8C	zhlu		Apple-iPad	NotApplicable	bxb22-11a-pdp1	dot1x	PEAP (EAP-MSCHAPv2)	10.86.102.138
▶	2013-06-07 08:04:21.866	2013-06-07 08:04:21.871	Started		11	00:24:D7:AF:FB:C0	CISCO\mgrudino		Windows7-Workstation	NotApplicable	bxb22-11a-pdp1	dot1x	PEAP (EAP-MSCHAPv2)	10.86.102.138
▶	2013-06-07 08:04:15.596	2013-06-07 08:04:15.596	Authenticated		1	20:10:7A:89:5B:66	host/win7-pc.cis		Unknown	NotApplicable	npf-sjca-pdp01	dot1x	PEAP (EAP-MSCHAPv2)	10.32.37.6
▶	2013-06-07 08:00:44.006	2013-06-07 08:04:13.901	Started		2	24:77:03:47:2D:3C	host/dpiede-WS.	10.32.46.36	Microsoft-Workstation	NotApplicable	npf-sjca-pdp01	dot1x	PEAP (EAP-MSCHAPv2)	10.32.34.2
▶	2013-06-07 08:04:09.276	2013-06-07 08:04:09.281	Started		29	70:56:81:99:0E:B9	eisteine		OS_X_Lion-Workstatior	NotApplicable	bxb22-11a-pdp1	dot1x	PEAP (EAP-MSCHAPv2)	10.86.102.138

Radius Proxy

ISE Becomes a Broker for RADIUS Servers Outside the Organisation



☑ Proxy Rule : If Radius:User-Na... Use Proxy Service : RADIUS_SEQ1

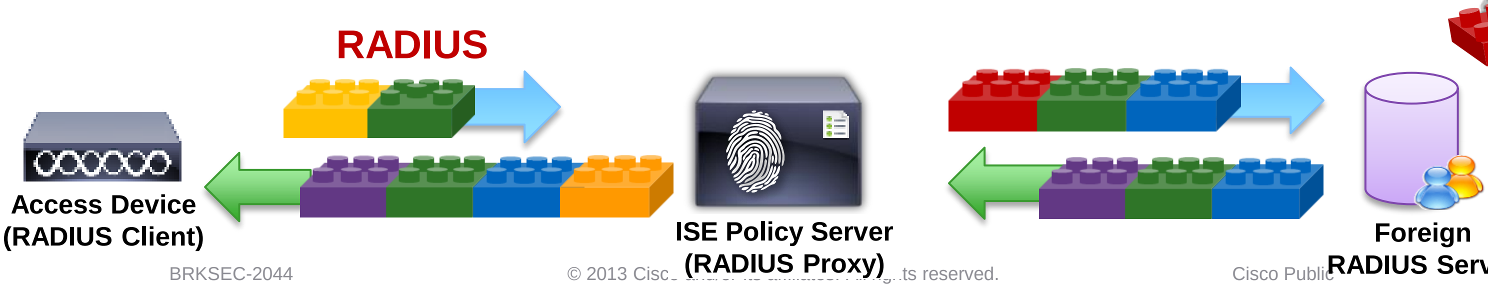
Conditions Details

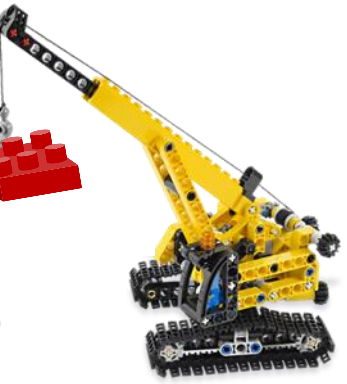
Radius:User-Name matches .*domain2.fr$

RADIUS Server Sequence

- RADIUS_SEQ1
- RADIUS_SEQ2

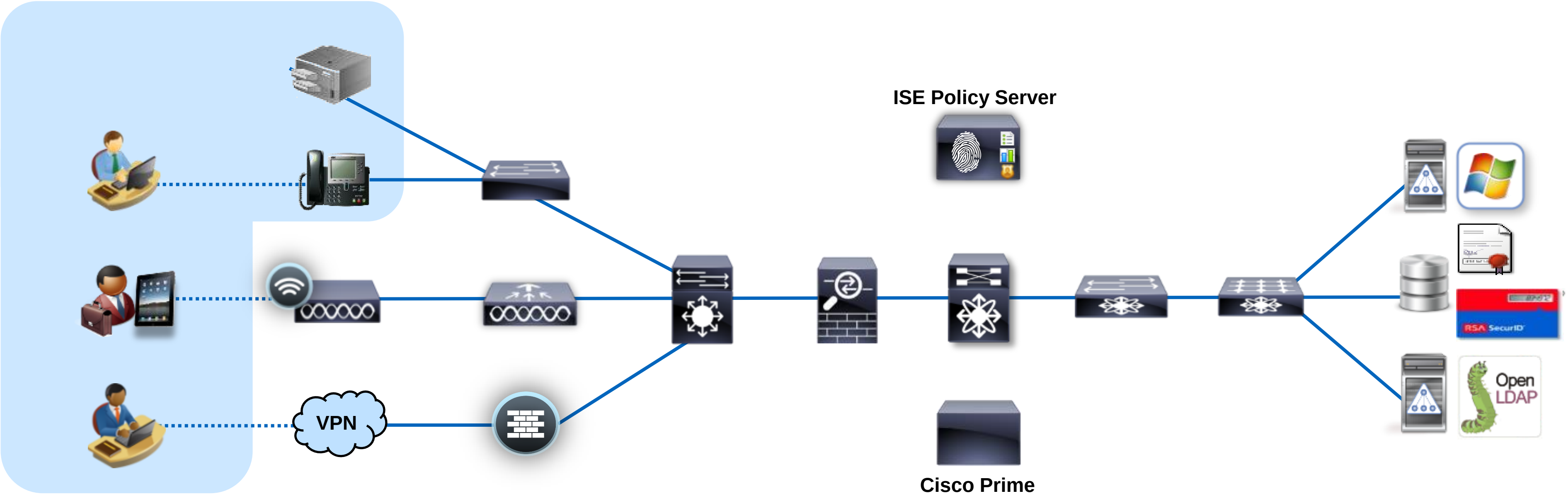
- Add/Remove/Substitute attributes prior to sending to foreign RADIUS server.
- Add/Remove/Substitute attributes prior to sending back to NAD.
- Process request through ISE Authorisation rules before sending final response.





Authenticating and Authorising Any User or Endpoint

Access Control System Must Authenticate / Authorise Everything That Connects to the Network



802.1X and MAB

Let's Begin by Securing User Access with 802.1X

IT Mgr.

I've done my homework in Proof of Concept Lab and it looks good. I'm turning on 802.1X tomorrow…

Enabled 802.1X

I can't connect to my network. It says Authentication failed but I don't know how to fix. My presentation is in 2 hours…

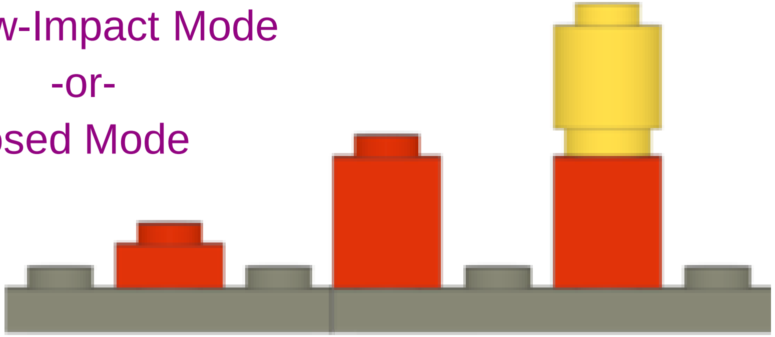
Help Desk calls increase by 40%

Building the Architecture in Phases

- Access-Prevention Technology
  - A Monitor Mode is necessary
  - Must have ways to implement and see who will succeed and who will fail
    - Determine why, and then remediate before taking 802.1X into a stronger enforcement mode.

- Solution = Phased Approach to Deployment:
  - Monitor Mode
  - Low-Impact Mode

    -or-
  - Closed Mode



Monitor Mode

A Process, Not Just a Command

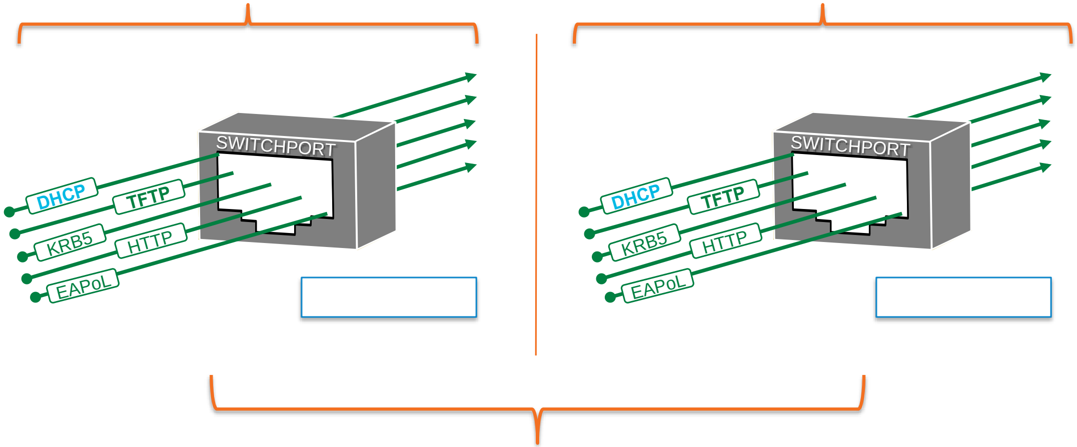
Interface Config

```
interface GigabitEthernet1/0/1
 authentication host-mode multi-auth
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
```

- Enables 802.1X authentication on the switch, but even failed authentication will gain access
- Allows network admins to see who would have failed, and fix it, before causing a Denial of Service ☺

Pre-AuthC

Post-AuthC



Traffic always allowed

AuthC = Authentication
AuthZ = Authorisation

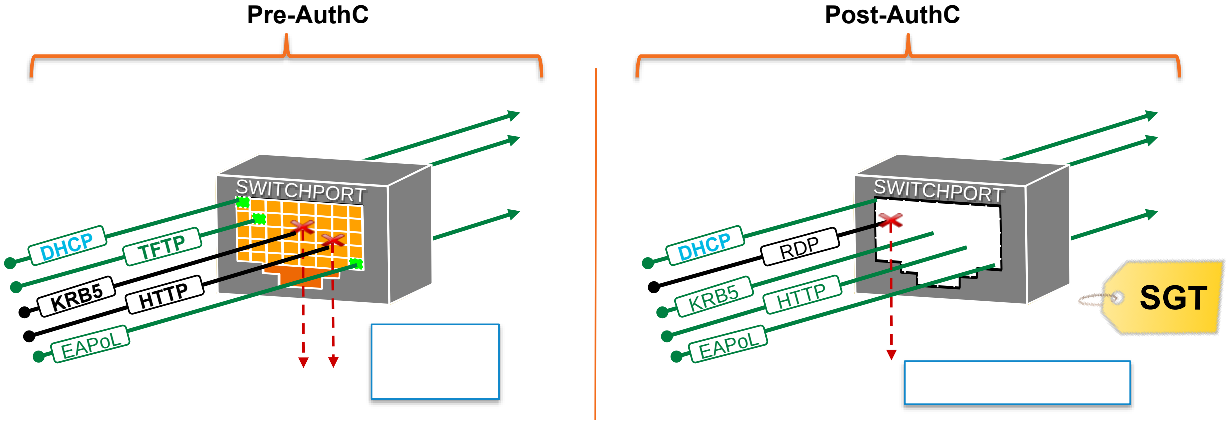
Low-Impact Mode

If Authentication Is Valid, Then **Specific** Access!

Interface Config

```
interface GigabitEthernet1/0/1
 authentication host-mode multi-auth
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
 ip access-group default-ACL in
```

- Limited access prior to authentication
- AuthC success = Role-specific access
  - dVLAN Assignment / dACLs
  - Secure Group Access
- Still allows for pre-AuthC access for Thin Clients, WoL & PXE boot devices, etc…



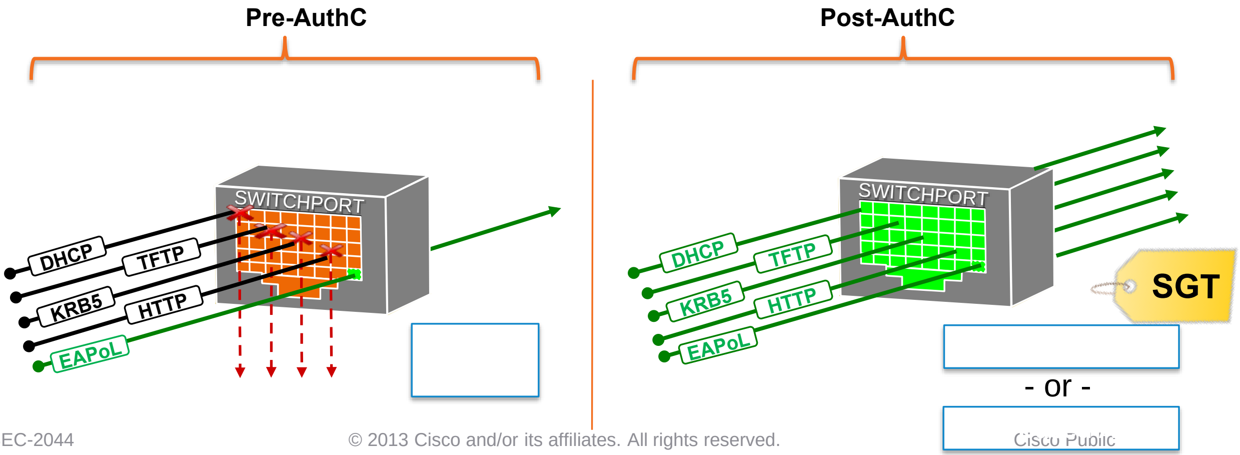
Closed Mode

No Access Prior to Login, Then **Specific** Access!

Interface Config

```
interface GigabitEthernet1/0/1
 authentication host-mode multi-auth
 authentication port-control auto
 mab
 dot1x pae authenticator
```

- Default 802.1X behaviour
- No access at all prior to AuthC
- Still use all AuthZ enforcement types
  - *dACL, dVLAN, SGA*
- Must take considerations for Thin Clients, WoL, PXE devices, etc…



Securing Access From Non-User Devices

- Non-Authenticating Devices
  - These are devices that were forgotten
  - They do not have software to talk EAP on the network

    …or they were not configured for it

    Examples: Printers, IP Phones, Cameras, Badge Readers
  - How to work with these?
- ~~Solution: Do not use 802.1X on ports with Printers~~

  …but what happens when the device moves
  or another endpoint plugs into that port?!
- **Solution: MAC Authentication Bypass (MAB)**

MAC Authentication Bypass (MAB)

What Is It?

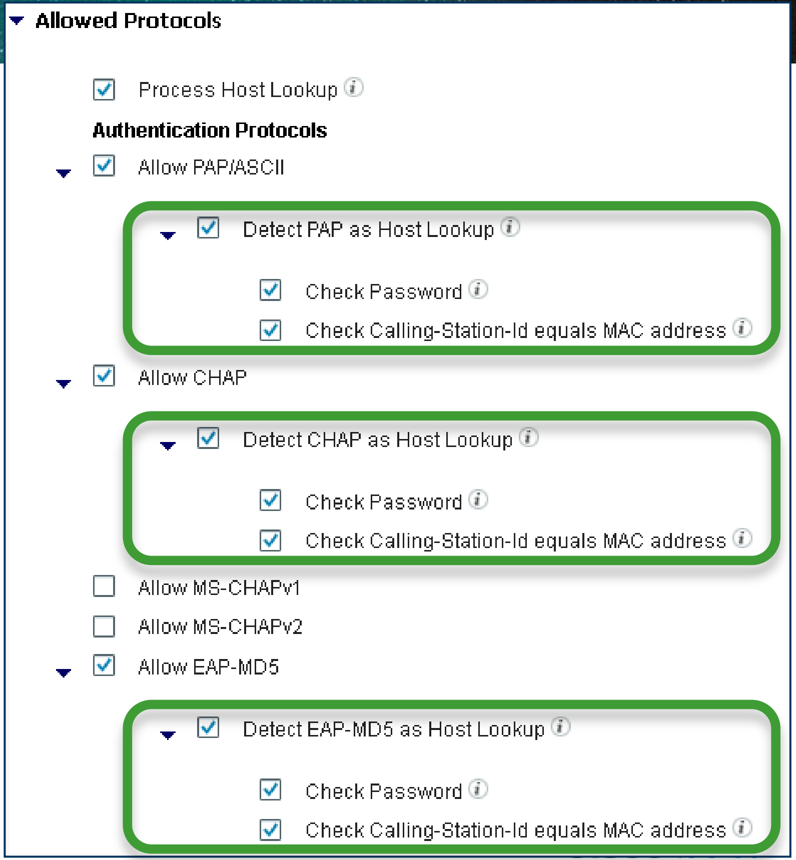
- A list of MAC Addresses that are allowed to “skip” authentication
- Is this a replacement for 802.1X?
  - No Way!
- This is a “Band-aid”
  - In a Utopia, ALL devices authenticate.
- List may be Local or Centralised
  - Can you think of any benefits to a centralised model?

One MAB For All

ISE and 3rd-Party MAB Support

- MAC Authentication is NOT a defined standard.
- Cisco uses the Service-Type = Call-Check to detect MAB and uses Calling-Station-ID for host lookup in identity store.
- Most 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 and Calling-Station-ID values or different “password” settings.

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



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

☐ Allow MS-CHAPv1

☐ Allow MS-CHAPv2

☑ Allow EAP-MD5

☑ Detect EAP-MD5 as Host Lookup

☑ Check Password

☑ Check Calling-Station-Id equals MAC address

Profiling – “What” is Connecting to My Network?

Profiling

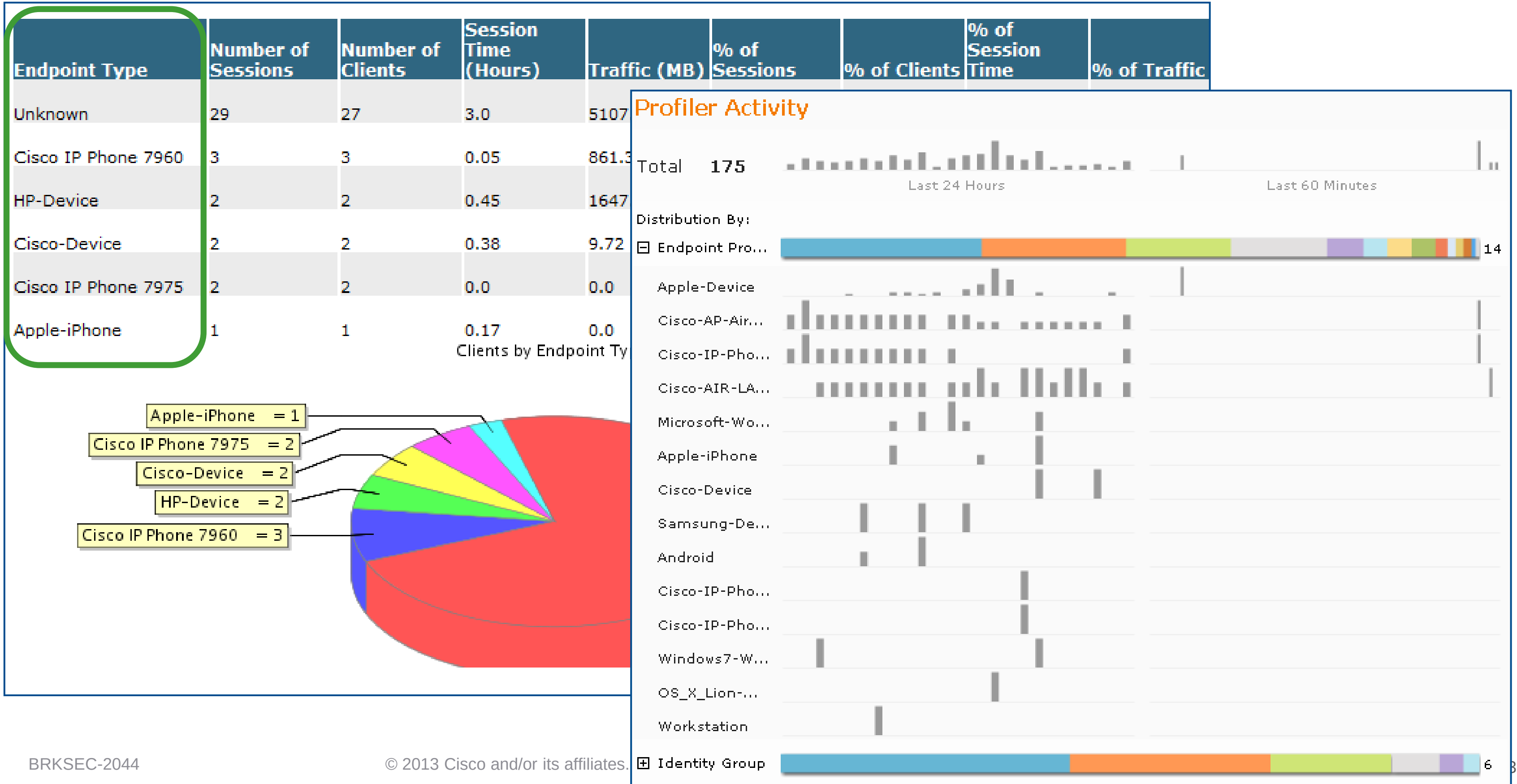
- What ISE Profiling is:
  - Dynamic classification of every device that connects to network using the infrastructure.
  - Provides the context of "What" is connected independent of user identity for use in access policy decisions

PCs	Non-PCs			
	UPS	Phone	Printer	AP

- What Profiling is NOT:
  - An authentication mechanism.
  - An exact science for device classification.

Profiling Technology

Visibility into what is on the network



Endpoint Type	Number of Sessions	Number of Clients	Session Time (Hours)	Traffic (MB)	% of Sessions	% of Clients	% of Session Time	% of Traffic
Unknown	29	27	3.0	5107				
Cisco IP Phone 7960	3	3	0.05	861.3				
HP-Device	2	2	0.45	1647				
Cisco-Device	2	2	0.38	9.72				
Cisco IP Phone 7975	2	2	0.0	0.0				
Apple-iPhone	1	1	0.17	0.0				

Clients by Endpoint Ty

Profiler Activity

Total 175

Distribution By:

⊟ Endpoint Pro... 14

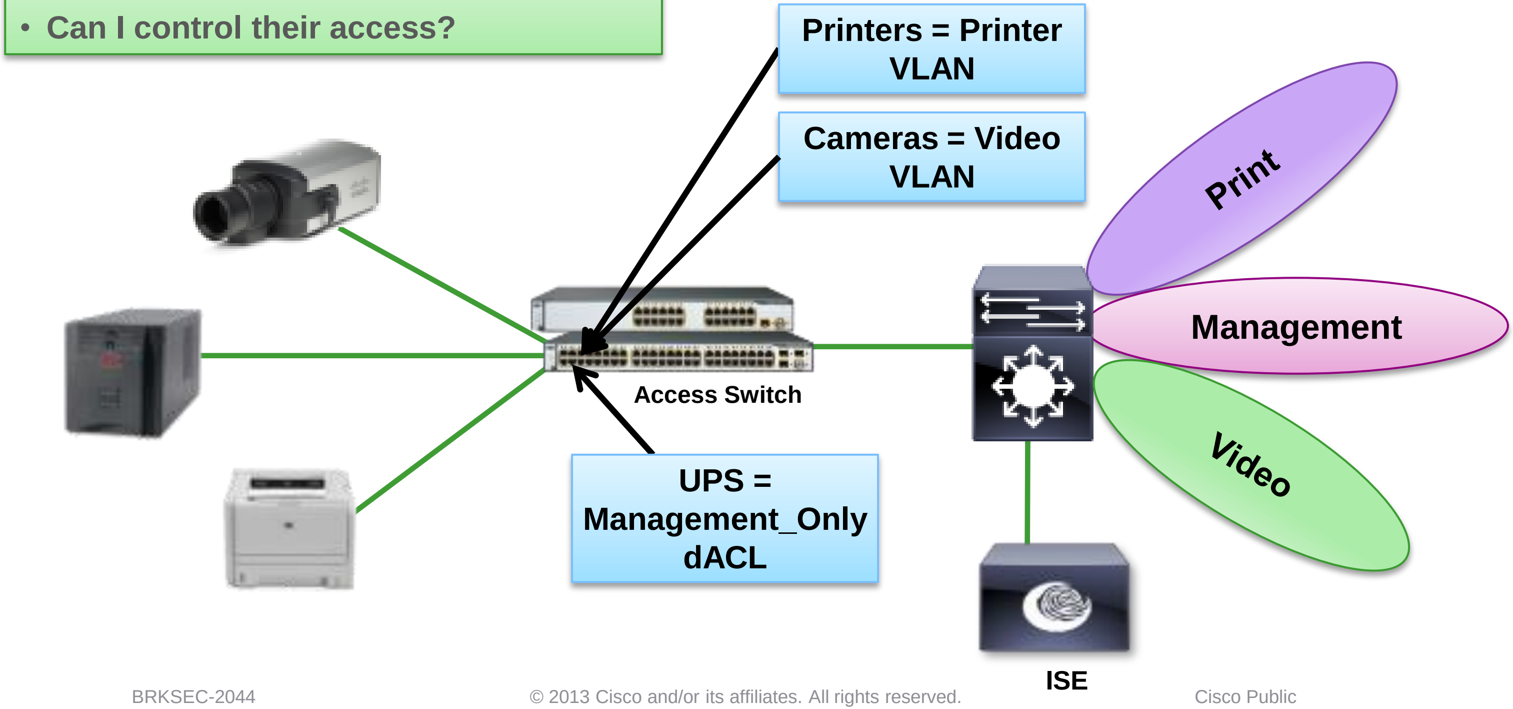
- Apple-Device
- Cisco-AP-Air...
- Cisco-IP-Pho...
- Cisco-AIR-LA...
- Microsoft-Wo...
- Apple-iPhone
- Cisco-Device
- Samsung-De...
- Android
- Cisco-IP-Pho...
- Cisco-IP-Pho...
- Windows7-W...
- OS_X_Lion-...
- Workstation

⊞ Identity Group 6

Profiling Non-User Devices

Dynamic Population of MAB Database Based on Device Type

- How do I discover non-user devices?
- Can I determine what they are?
- Can I control their access?



Profiling User Devices

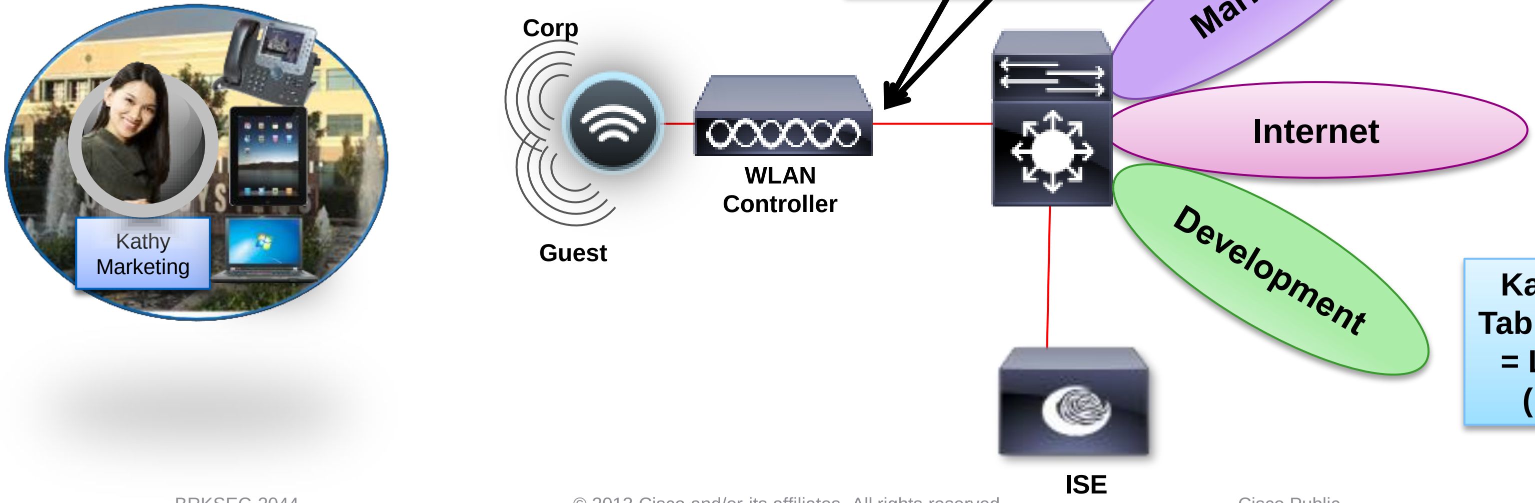
Differentiated Access Based on Device Type

- How can I restrict access to my network?
- Can I manage the risk of using personal PCs, tablets, smart-devices?

Kathy + Corp Laptop = Full Access to Marketing VLAN

Named ACL = Internet_Only

VLAN = Marketing

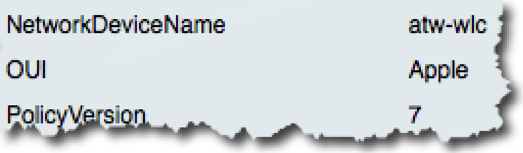


Kathy + Personal Tablet / Smartphone = Limited Access (Internet Only)

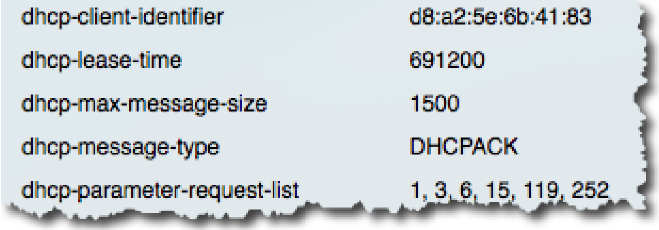
Profiling Technology

How Do We Classify a Device?

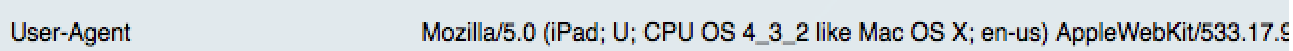
- Profiling uses signatures (similar to IPS)



NetworkDeviceName	atw-wlc
OUI	Apple
PolicyVersion	7

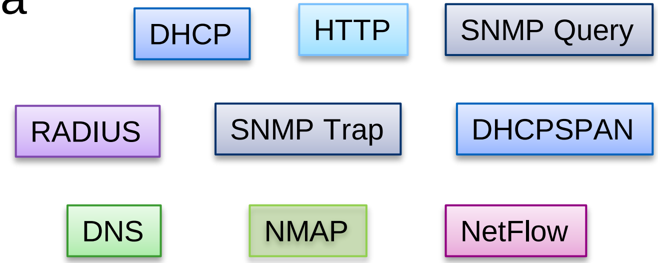


dhcp-client-identifier	d8:a2:5e:6b:41:83
dhcp-lease-time	691200
dhcp-max-message-size	1500
dhcp-message-type	DHCPACK
dhcp-parameter-request-list	1, 3, 6, 15, 119, 252

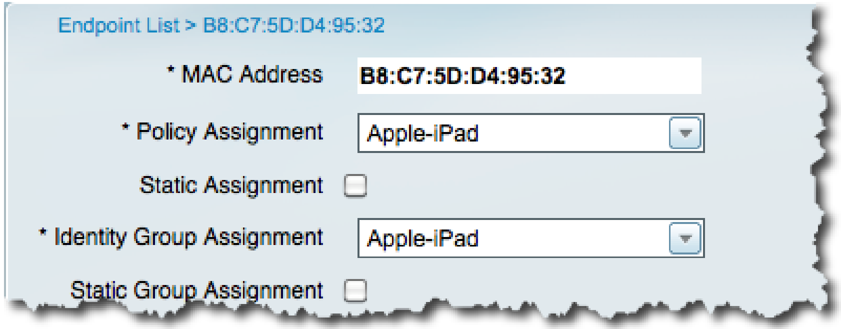


User-Agent	Mozilla/5.0 (iPad; U; CPU OS 4_3_2 like Mac OS X; en-us) AppleWebKit/533.17.9

- Probes are used to collect endpoint data



DHCP
HTTP
SNMP Query
RADIUS
SNMP Trap
DHCPSPAN
DNS
NMAP
NetFlow

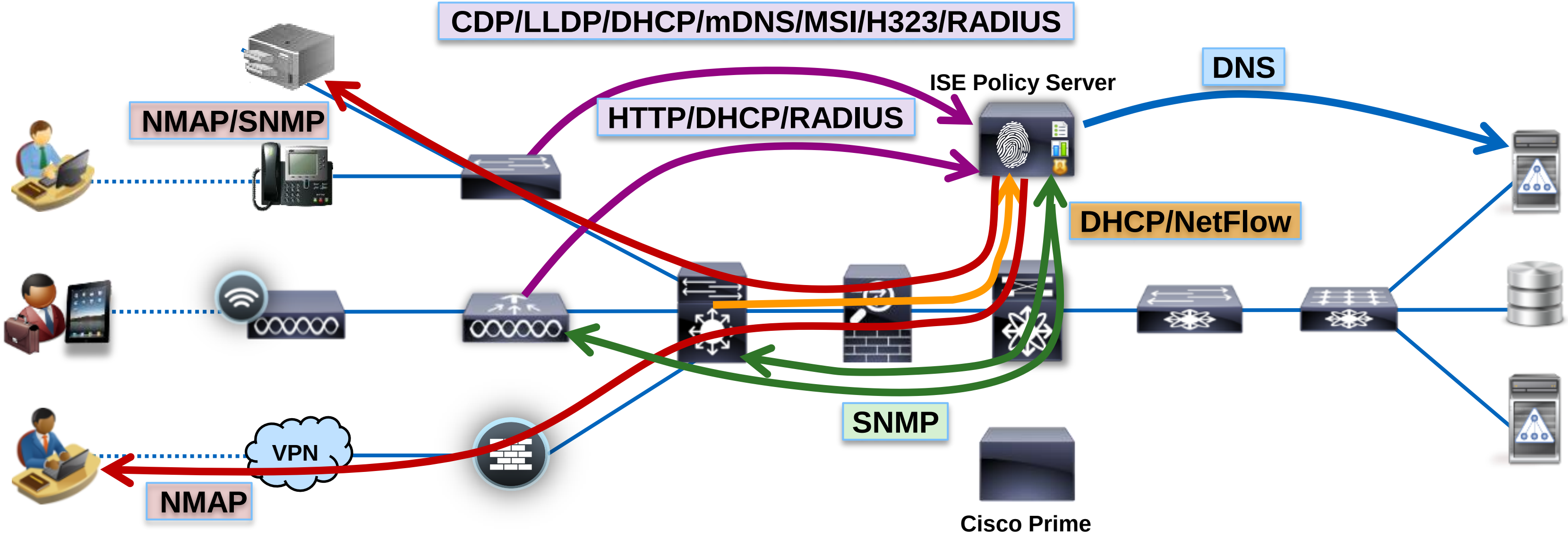


Endpoint List > B8:C7:5D:D4:95:32

* MAC Address	B8:C7:5D:D4:95:32
* Policy Assignment	Apple-iPad
Static Assignment	□
* Identity Group Assignment	Apple-iPad
Static Group Assignment	□

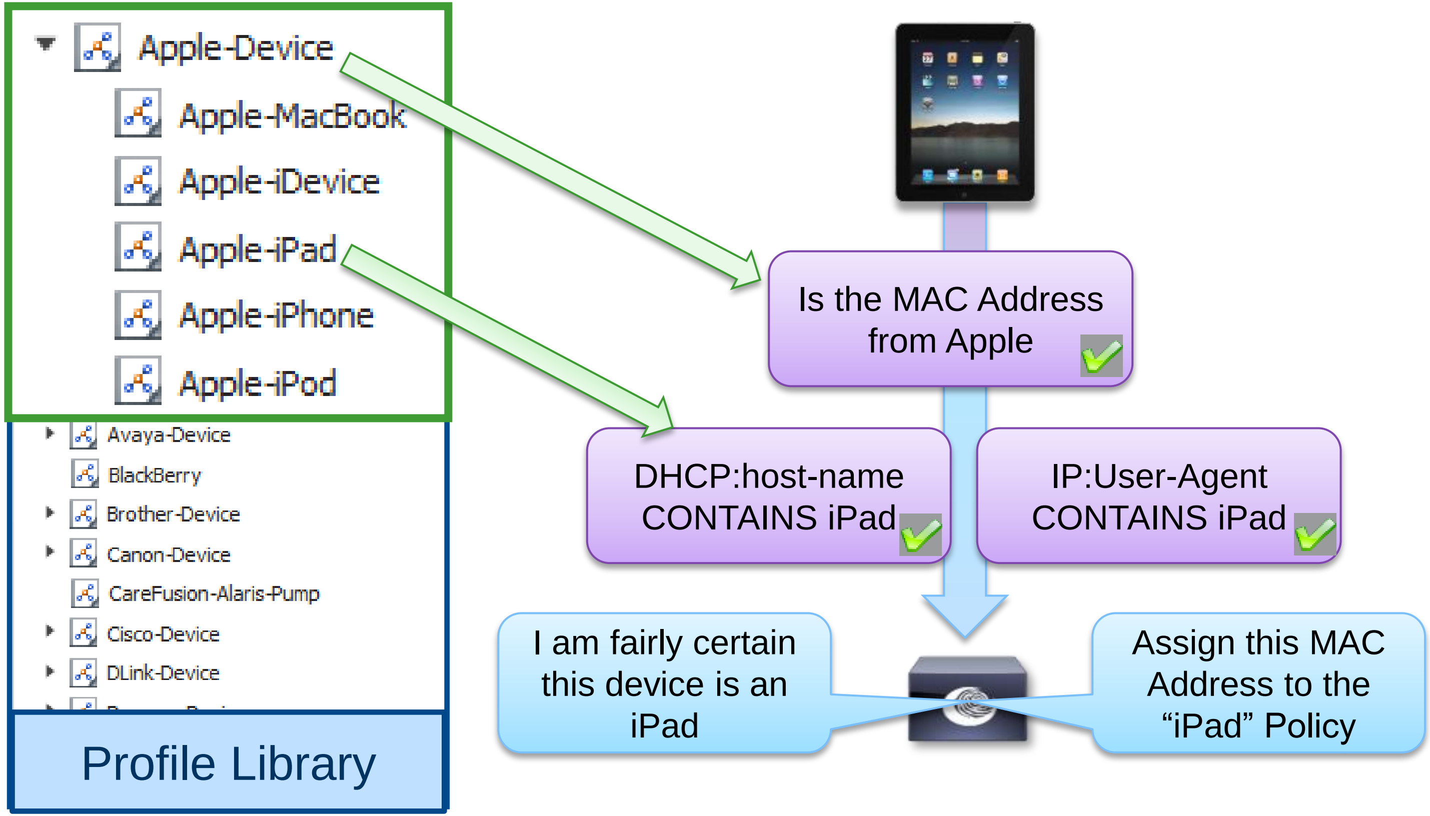
Embedded Endpoint Detection and Classification

Access Control System Must Detect and Classify Everything That Connects to the Network



Profiling Policy Overview

Profile Policies Use a Combination of Conditions to Identify Devices



- Apple-Device
  - Apple-MacBook
  - Apple-iDevice
  - Apple-iPad
  - Apple-iPhone
  - Apple-iPod
- Avaya-Device
- BlackBerry
- Brother-Device
- Canon-Device
- CareFusion-Alaris-Pump
- Cisco-Device
- DLink-Device

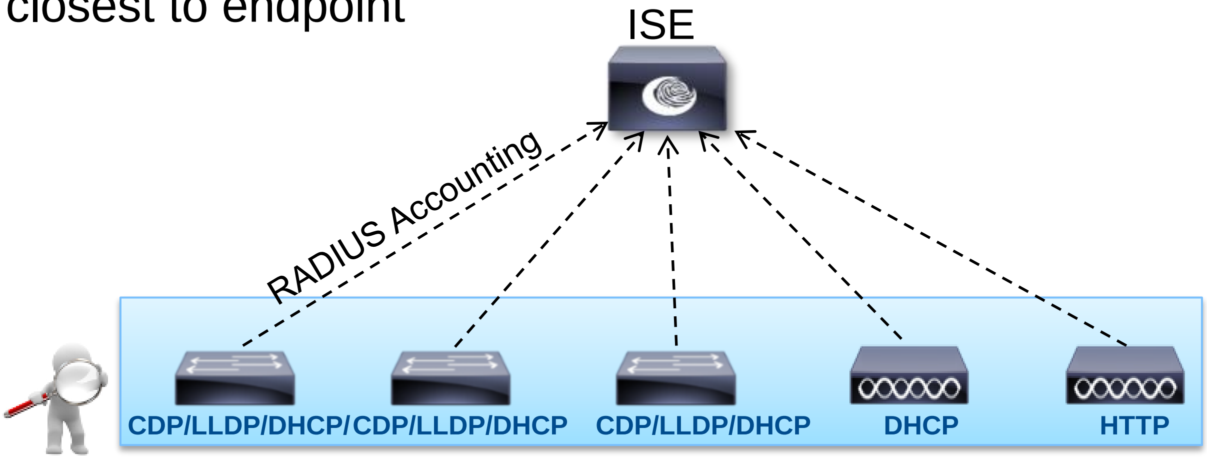
Profile Library
Is the MAC Address from Apple ✓
DHCP:host-name CONTAINS iPad ✓
IP:User-Agent CONTAINS iPad ✓
I am fairly certain this device is an iPad
Assign this MAC Address to the “iPad” Policy

Device Sensor

Distributed Probes with Centralised Collection

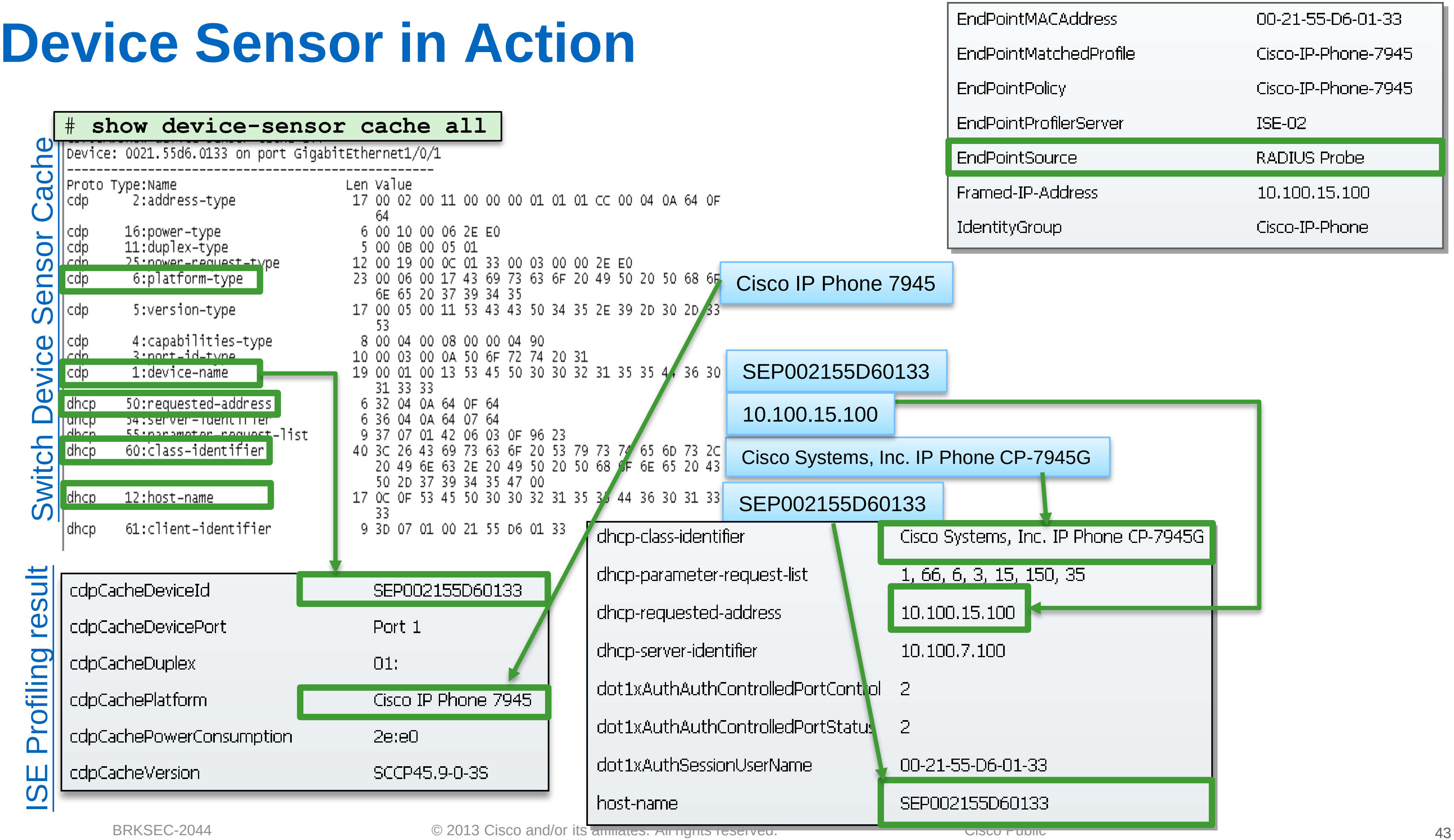
Device Sensor Support
3k/4k/WLC

- The Network IS the Collector!
- Automatic discovery for most common devices (printers, phones, Cisco devices)
- Collects the data at point closest to endpoint
- Topology independent
- Profiling based on:
  - CDP/LLDP
  - DHCP
  - HTTP (WLC only)
  - mDNS, H323, MSI-Proxy (4k only)



Device Sensor Distributed Probes

Device Sensor in Action



Switch Device Sensor Cache

```
# show device-sensor cache all
Device: 0021.55d6.0133 on port GigabitEthernet1/0/1
--------------------------------------------------
Proto Type:Name                          Len Value
cdp      2:address-type                   17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 64 0F
                                             64
cdp     16:power-type                      6 00 10 00 06 2E E0
cdp     11:duplex-type                     5 00 0B 00 05 01
cdp     25:power-request-type             12 00 19 00 0C 01 33 00 03 00 00 2E E0
cdp      6:platform-type                  23 00 06 00 17 43 69 73 63 6F 20 49 50 20 50 68 6F
                                             6E 65 20 37 39 34 35
cdp      5:version-type                   17 00 05 00 11 53 43 43 50 34 35 2E 39 2D 30 2D 33
                                             53
cdp      4:capabilities-type               8 00 04 00 08 00 00 04 90
cdp      3:port-id-type                   10 00 03 00 0A 50 6F 72 74 20 31
cdp      1:device-name                    19 00 01 00 13 53 45 50 30 30 32 31 35 35 44 36 30
                                             31 33 33
dhcp    50:requested-address               6 32 04 0A 64 0F 64
dhcp    54:server-identifier               6 36 04 0A 64 07 64
dhcp    55:parameter-request-list          9 37 07 01 42 06 03 0F 96 23
dhcp    60:class-identifier               40 3C 26 43 69 73 63 6F 20 53 79 73 74 65 6D 73 2C
                                             20 49 6E 63 2E 20 49 50 20 50 68 6F 6E 65 20 43
                                             50 2D 37 39 34 35 47 00
dhcp    12:host-name                      17 0C 0F 53 45 50 30 30 32 31 35 35 44 36 30 31 33
                                             33
dhcp    61:client-identifier               9 3D 07 01 00 21 55 D6 01 33
```

Cisco IP Phone 7945

SEP002155D60133

10.100.15.100

Cisco Systems, Inc. IP Phone CP-7945G

SEP002155D60133

EndPointMACAddress	00-21-55-D6-01-33
EndPointMatchedProfile	Cisco-IP-Phone-7945
EndPointPolicy	Cisco-IP-Phone-7945
EndPointProfilerServer	ISE-02
EndPointSource	RADIUS Probe
Framed-IP-Address	10.100.15.100
IdentityGroup	Cisco-IP-Phone

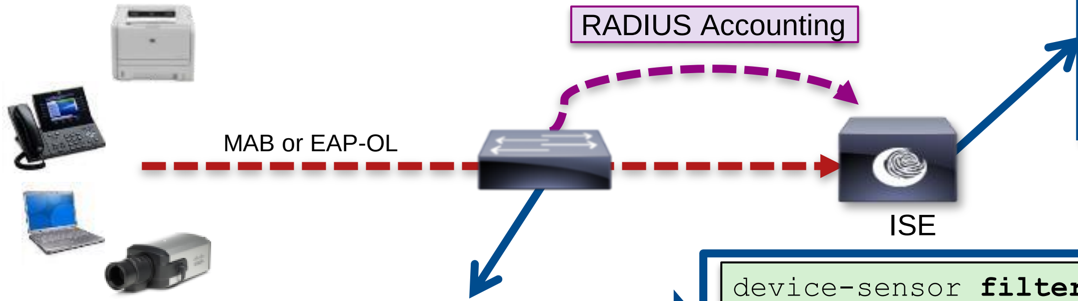
ISE Profiling result

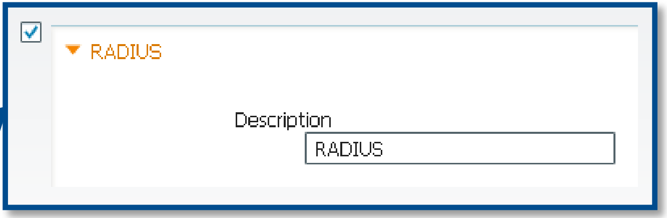
cdpCacheDeviceId	SEP002155D60133
cdpCacheDevicePort	Port 1
cdpCacheDuplex	01:
cdpCachePlatform	Cisco IP Phone 7945
cdpCachePowerConsumption	2e:e0
cdpCacheVersion	SCCP45.9-0-3S

dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7945G
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35
dhcp-requested-address	10.100.15.100
dhcp-server-identifier	10.100.7.100
dot1xAuthAuthControlledPortControl	2
dot1xAuthAuthControlledPortStatus	2
dot1xAuthSessionUserName	00-21-55-D6-01-33
host-name	SEP002155D60133

Wired Device Sensors

Device Detection Based on CDP, LLDP or DHCP




☑ RADIUS

Description: RADIUS

ISE: Enable RADIUS probe

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

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

```
device-sensor filter-list lldp list my_lldp_list
 tlv name system-name
 tlv name system-description
device-sensor filter-spec lldp include list my_lldp_list
```

```
device-sensor filter-list dhcp list my_dhcp_list
 option name host-name
 option name class-identifier
 option name client-identifier
device-sensor filter-spec dhcp include list my_dhcp_list
```

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

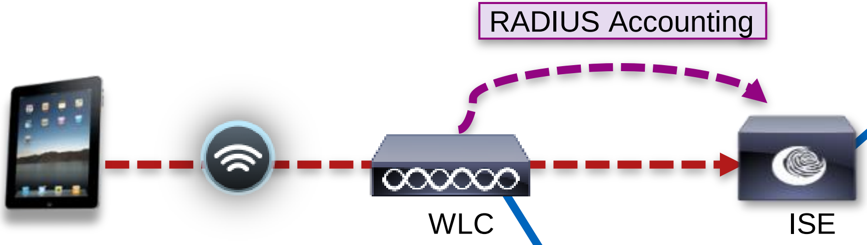
```
device-sensor accounting
device-sensor notify all-changes
```

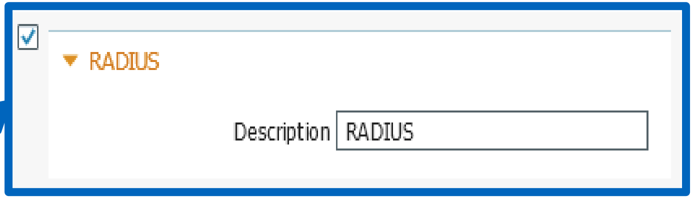
3) Disable local analyser if sending sensor updates to ISE (central analyser)

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

Wireless Device Sensors

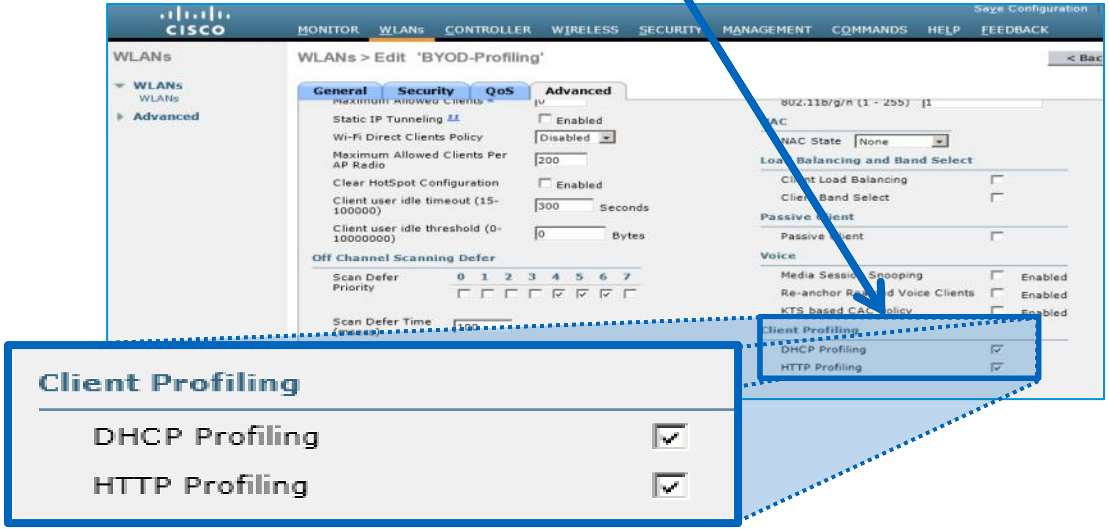
WLC Device Detection Based on DHCP / HTTP





☑ RADIUS

Description: RADIUS



WLANs > Edit 'BYOD-Profiling'

Static IP Tunneling: □ Enabled

Wi-Fi Direct Clients Policy: Disabled

Maximum Allowed Clients Per AP Radio: 200

Clear HotSpot Configuration: □ Enabled

Client user idle timeout (15-100000): 300 Seconds

Client user idle threshold (0-10000000): 0 Bytes

Off Channel Scanning Defer

Scan Defer Priority	0	1	2	3	4	5	6	7
	□	□	□	□	☑	☑	☑	□

Scan Defer Time (msecs): 100

802.11b/g/n (1 - 255): 1

NAC

NAC State: None

Load Balancing and Band Select

Client Load Balancing □

Client Band Select □

Passive Client

Passive Client □

Voice

Media Session Snooping □ Enabled

Re-anchor Roamed Voice Clients □ Enabled

KTS based CAC Policy □ Enabled

Client Profiling

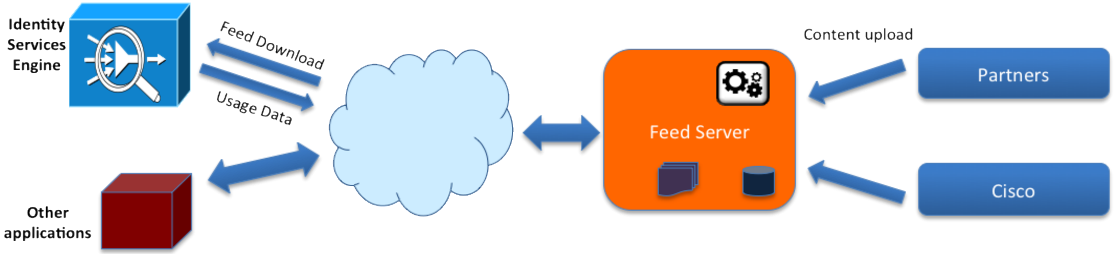
DHCP Profiling ☑

HTTP Profiling ☑

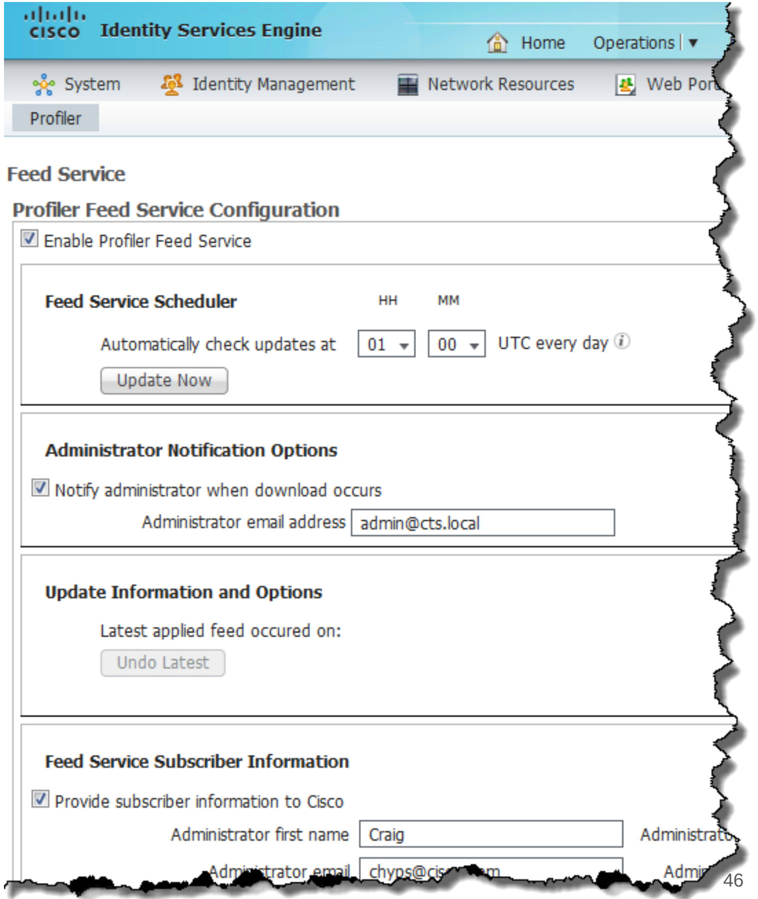
- Per WLAN Enable/Disable device profiling
- DHCP (WLC 7.2.110.0)
  - **Hostname, Class ID**
- HTTP / Both (WLC 7.3)
  - **User Agent**
- FlexConnect with Central Switching supported

How Is Profile Library Kept Current With Latest Devices?

- Dynamic Feed Service



  - Live Update Service for New Profiles and OUI Files
  - Cisco and Cisco Partners contribute to service
  - Opt In Model: New profiles automatically downloaded from Cisco.com and applied to live system.



Feed Service

Profiler Feed Service Configuration

☑ Enable Profiler Feed Service

Feed Service Scheduler

Automatically check updates at HH 01 MM 00 UTC every day

Update Now

Administrator Notification Options

☑ Notify administrator when download occurs

Administrator email address: admin@cts.local

Update Information and Options

Latest applied feed occured on:

Undo Latest

Feed Service Subscriber Information

☑ Provide subscriber information to Cisco

Administrator first name: Craig

Administrato

Administrator email: chyps@cis[illegible]m

Admi

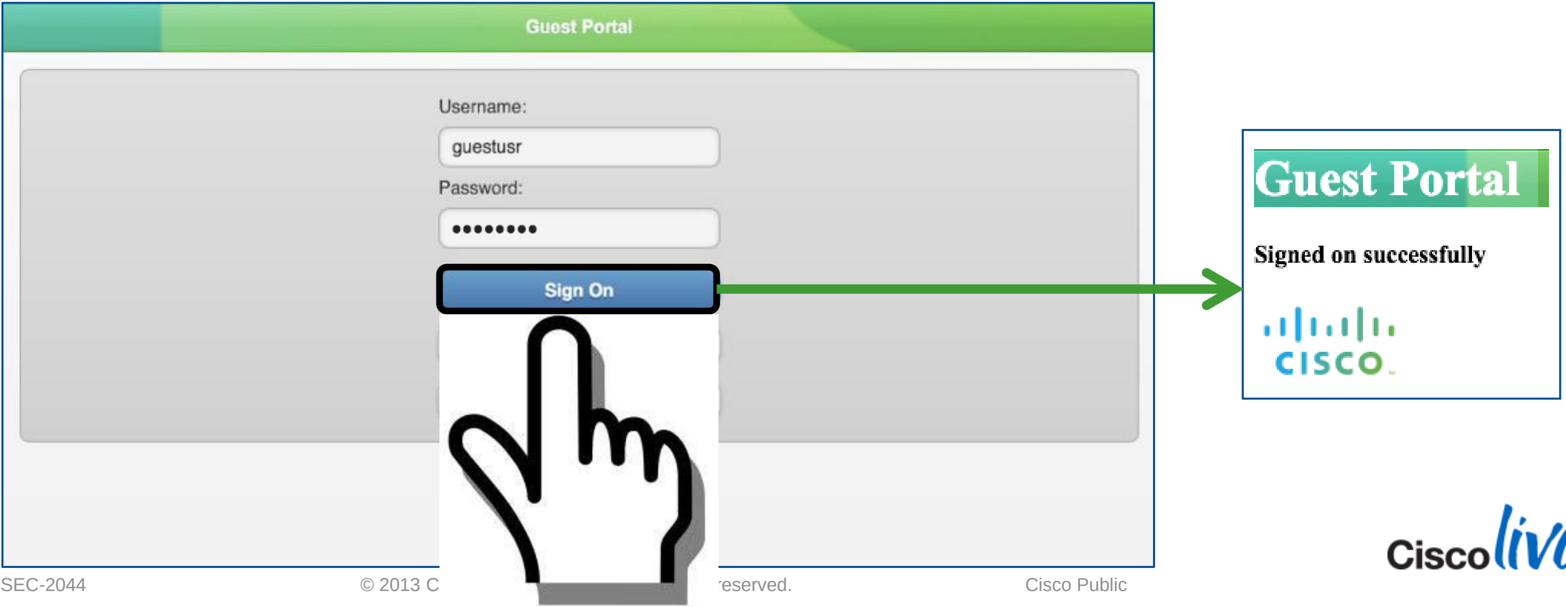
Web Authentication

Handling Guests and Employees Without 802.1X

Employees and some non-user devices	802.1X	✓
All other non-user devices	MAB	✓
Guest Users		✗
Employees with Missing or Misconfigured Supplicants		✗

Enter Web Authentication

- Used to identify users without supplicants
  - Misconfigured, missing altogether, etc.
- Guest Authentication



Guest Portal

Username:

guestusr

Password:

●●●●●●●●●

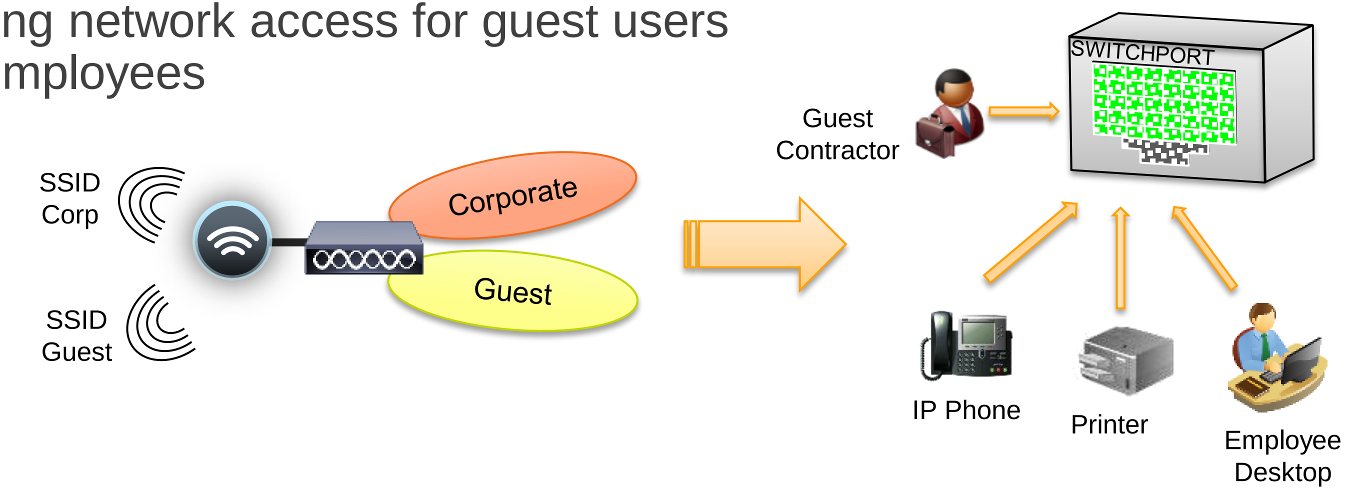
Sign On

Guest Portal

Signed on successfully

Network Access for Guests and Employees

- Unifying network access for guest users and employees



On wireless:

- Using multiple SSIDs
- Open SSID for Guest

On wired:

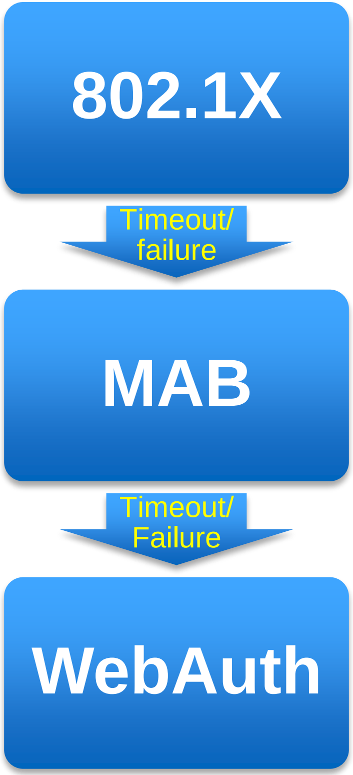
- No notion of SSID
- Unified port: Need to use different auth methods on single port ► Enter Flex Auth

Flex Auth

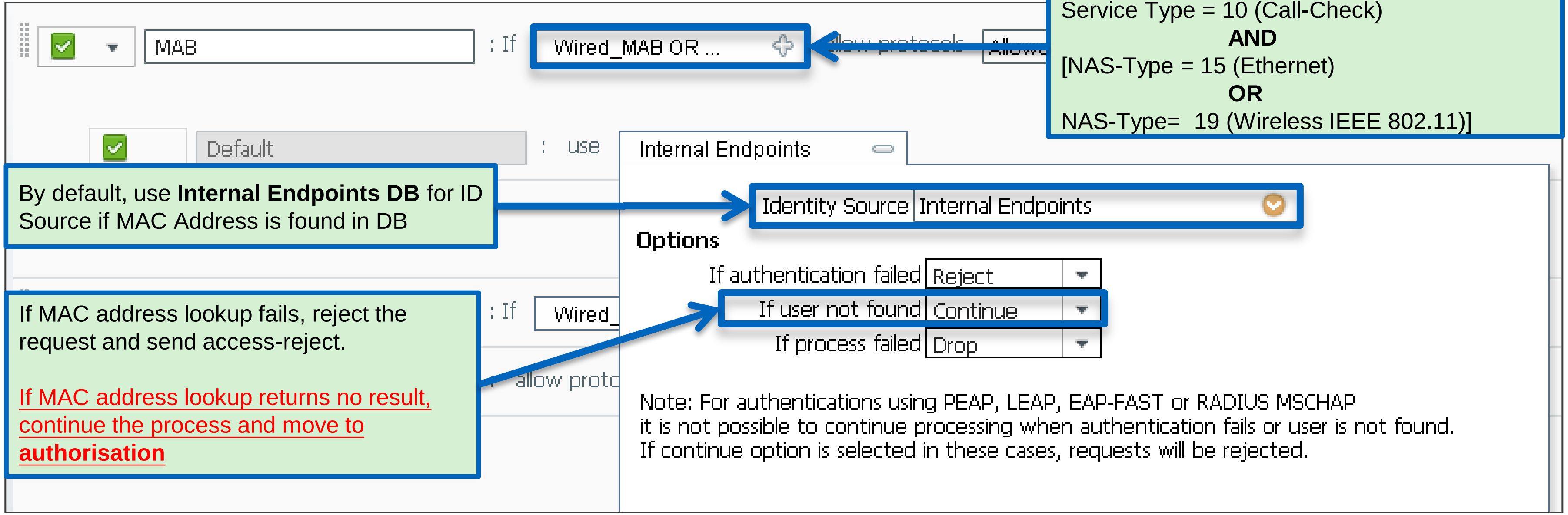
Converging Multiple Authentication Methods on a Single Wired Port

Interface Config

```
interface GigabitEthernet1/0/1
 authentication host-mode multi-auth
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
 !
 authentication event fail action next-method
 authentication order dot1x mab
 authentication priority dot1x mab
```



ISE Authentication Configuration



☑ MAB : If Wired_MAB OR ... allow protocols Allowe
☑ Default : use Internal Endpoints
: If Wired_
allow protc

Identity Source: Internal Endpoints

Options

If authentication failed: Reject

If user not found: Continue

If process failed: Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

Condition is to match RADIUS Attribute Service Type = 10 (Call-Check)
AND
[NAS-Type = 15 (Ethernet)
OR
NAS-Type= 19 (Wireless IEEE 802.11)]

By default, use **Internal Endpoints DB** for ID Source if MAC Address is found in DB

If MAC address lookup fails, reject the request and send access-reject.

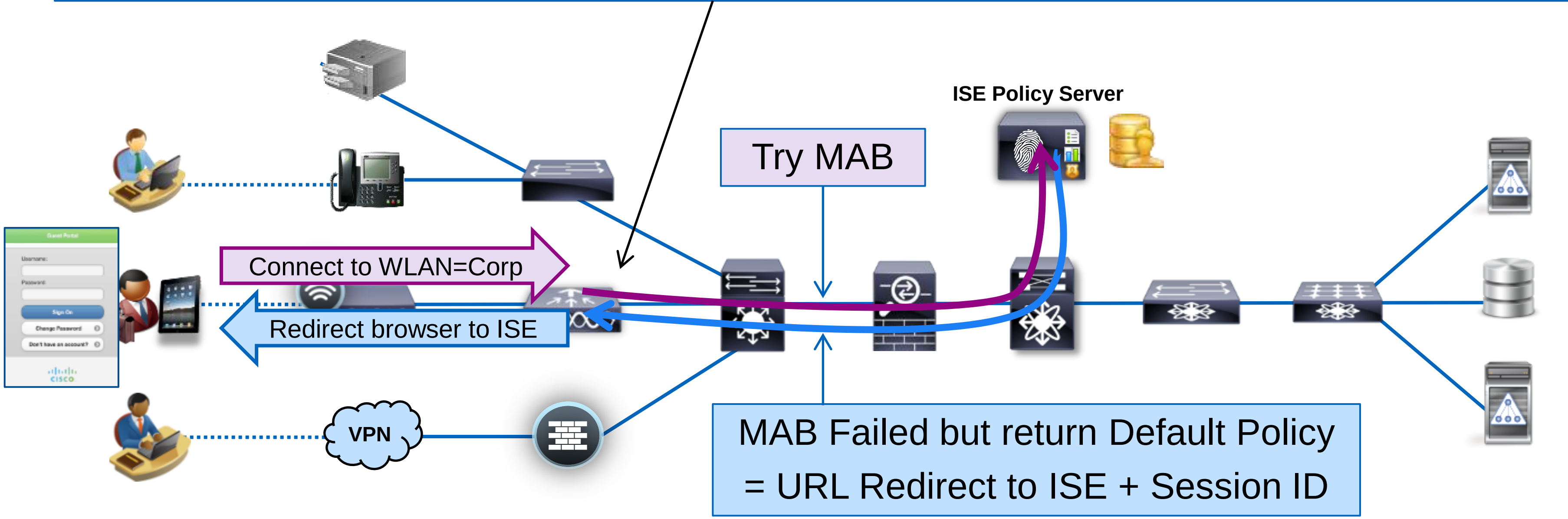
If MAC address lookup returns no result, continue the process and move to **authorisation**

- MAB Requests from Failed Auth user or Timed out user can still be processed to return specific authorisation rule (VLAN, dACL, URL-Redirect, and SGT)
- By default, '**If user not found**' value is set to '**Reject**'

CWA Flow

- Tracking session ID provides support for session lifecycle management including CoA.

https://ise.company.com:8443/guestportal/gateway?sessionId=0A010A...73691A&action=**cwa**



Try MAB

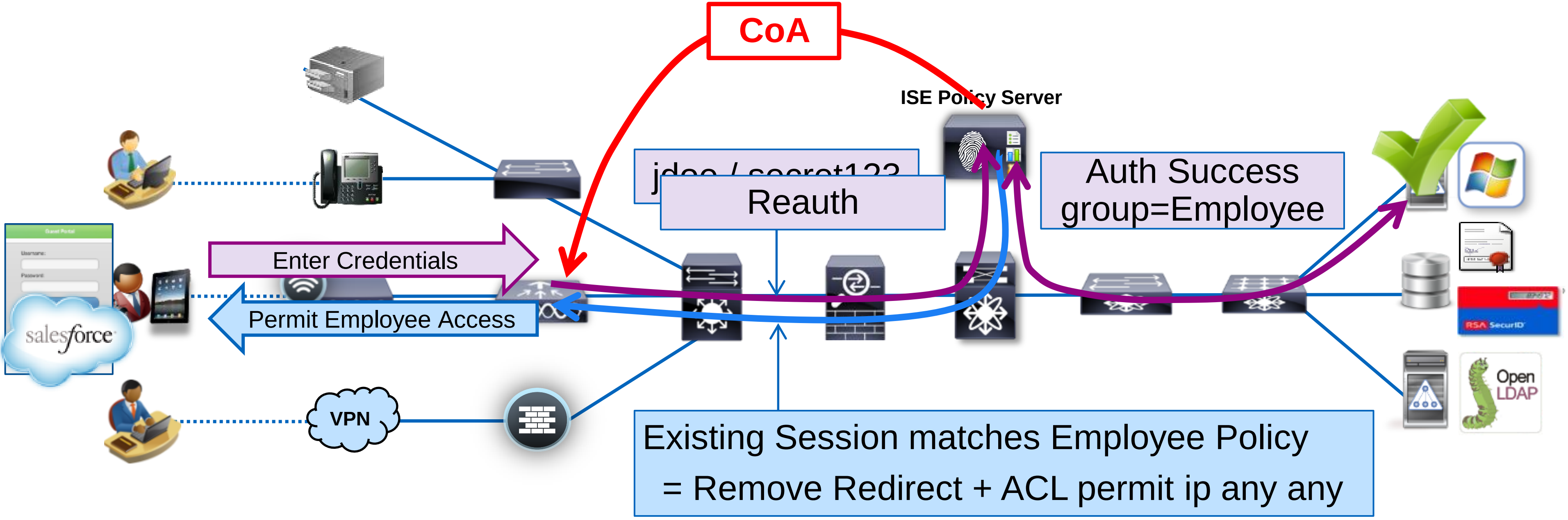
Connect to WLAN=Corp

Redirect browser to ISE

MAB Failed but return Default Policy = URL Redirect to ISE + Session ID

CWA Flow

- CoA allows re-authentication to be processed based on new endpoint identity context.

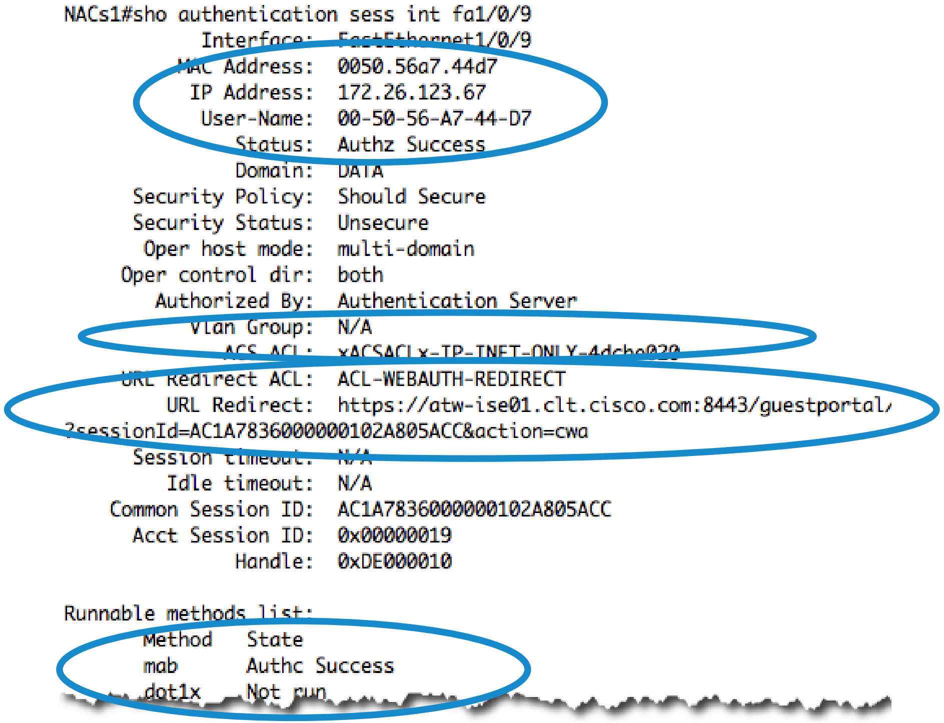


Existing Session matches Employee Policy

= Remove Redirect + ACL permit ip any any

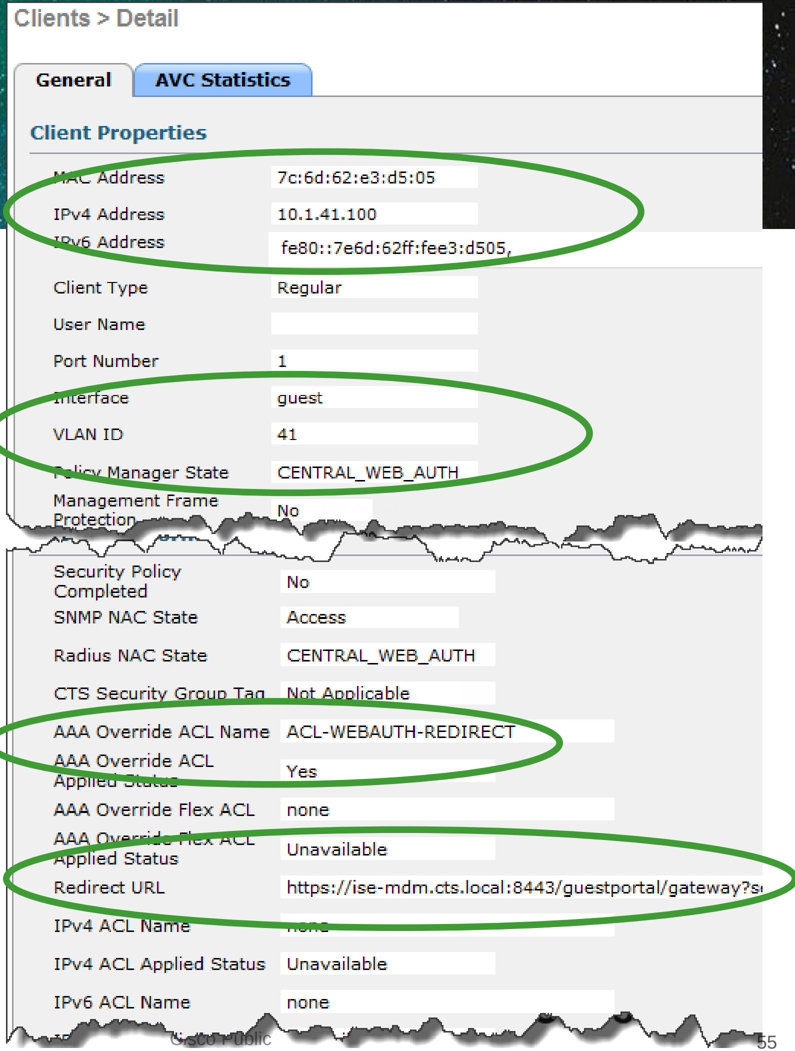
A Systems Approach

Switch/Controller is the Enforcement Point



```
NACs1#sho authentication sess int fa1/0/9
            Interface:  FastEthernet1/0/9
          MAC Address:  0050.56a7.44d7
           IP Address:  172.26.123.67
            User-Name:  00-50-56-A7-44-D7
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-INET-ONLY-4dcbe020
     URL Redirect ACL:  ACL-WEBAUTH-REDIRECT
         URL Redirect:  https://atw-ise01.clt.cisco.com:8443/guestportal/
?sessionId=AC1A7836000000102A805ACC&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  AC1A7836000000102A805ACC
      Acct Session ID:  0x00000019
               Handle:  0xDE000010

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```



Clients > Detail

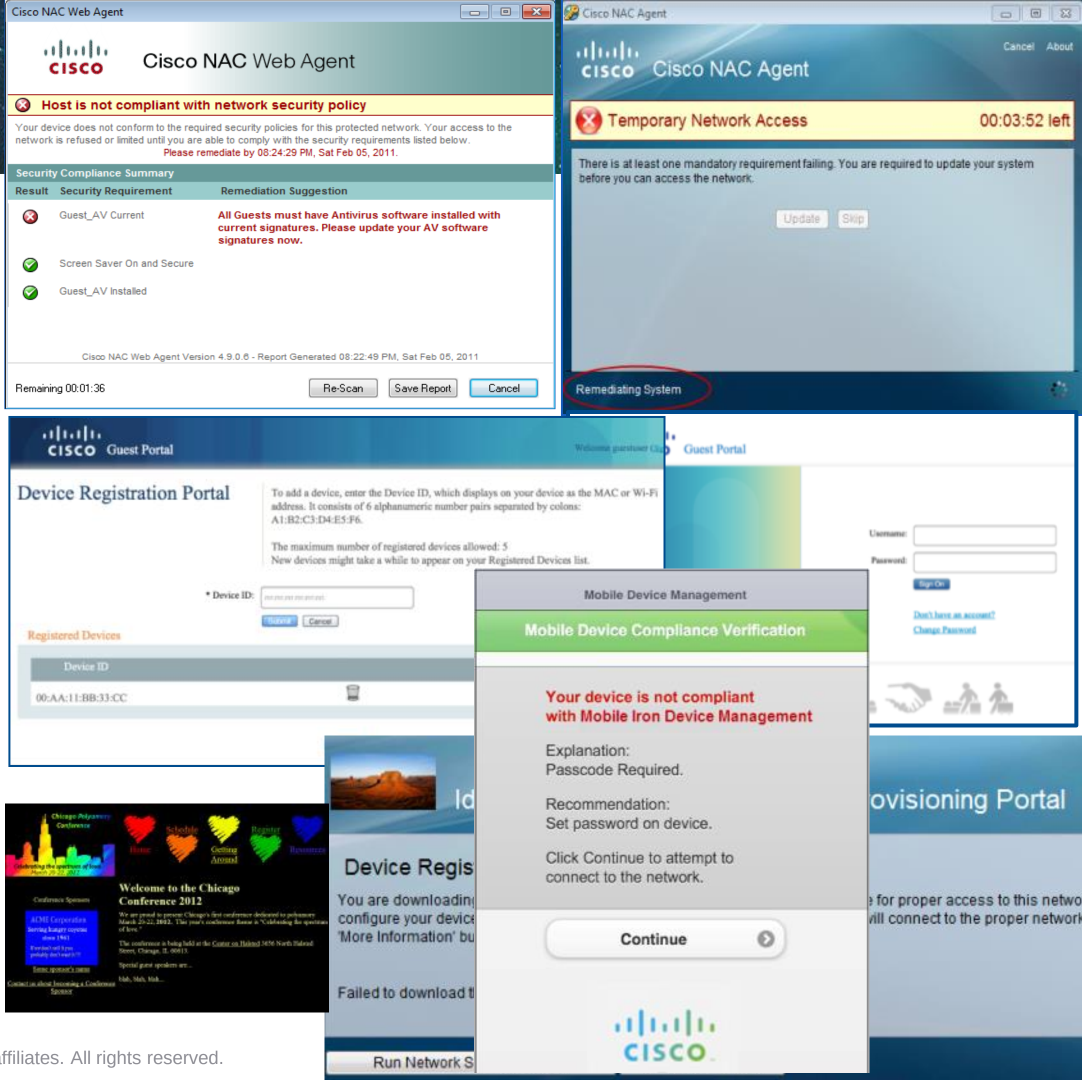
Client Properties

MAC Address	7c:6d:62:e3:d5:05
IPv4 Address	10.1.41.100
IPv6 Address	fe80::7e6d:62ff:fee3:d505,
Client Type	Regular
User Name	
Port Number	1
Interface	guest
VLAN ID	41
Policy Manager State	CENTRAL_WEB_AUTH
Management Frame Protection	No
Security Policy Completed	No
SNMP NAC State	Access
Radius NAC State	CENTRAL_WEB_AUTH
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	ACL-WEBAUTH-REDIRECT
AAA Override ACL Applied Status	Yes
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	https://ise-mdm.cts.local:8443/guestportal/gateway?s
IPv4 ACL Name	none
IPv4 ACL Applied Status	Unavailable
IPv6 ACL Name	none

URL Redirection

ISE uses URL Redirection for:

- Central Web Auth
- Client Software Provisioning
- Posture Discovery / Assessment
- Device Registration WebAuth
- BYOD On-Boarding
  - Certificate Provisioning
  - Supplicant Configuration
- Mobile Device Management
- External Web Pages



Cisco NAC Web Agent

Cisco NAC Web Agent

Host is not compliant with network security policy

Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 08:24:29 PM, Sat Feb 05, 2011.

Security Compliance Summary

Result	Security Requirement	Remediation Suggestion
☒	Guest_AV Current	All Guests must have Antivirus software installed with current signatures. Please update your AV software signatures now.
✓	Screen Saver On and Secure	
✓	Guest_AV Installed	

Cisco NAC Web Agent Version 4.9.0.6 - Report Generated 08:22:49 PM, Sat Feb 05, 2011

Remaining 00:01:36

Re-Scan | Save Report | Cancel

Cisco NAC Agent

Cancel | About

Cisco NAC Agent

Temporary Network Access 00:03:52 left

There is at least one mandatory requirement failing. You are required to update your system before you can access the network.

Update | Skip

Remediating System

Guest Portal

Welcome guestuser

Device Registration Portal

To add a device, enter the Device ID, which displays on your device as the MAC or Wi-Fi address. It consists of 6 alphanumeric number pairs separated by colons: A1:B2:C3:D4:E5:F6.

The maximum number of registered devices allowed: 5
New devices might take a while to appear on your Registered Devices list.

* Device ID:

Submit | Cancel

Registered Devices

Device ID
00:AA:11:BB:33:CC

Guest Portal

Username:

Password:

Sign On

Don't have an account?

Change Password

Mobile Device Management

Mobile Device Compliance Verification

Your device is not compliant with Mobile Iron Device Management

Explanation:
Passcode Required.

Recommendation:
Set password on device.

Click Continue to attempt to connect to the network.

Continue

Device Regis

You are downloadin
configure your devic
'More Information' bu

Failed to download t

Run Network S

ovisioning Portal

for proper access to this netwo
ill connect to the proper networ

Chicago Polyamory Conference

Celebrating the spectrum of love
March 20-22, 2012

Home | Schedule | Getting Around | Register | Resources

Conference Sponsors

ACME Corporation
Serving hungry coyotes since 1961

Some sponsor's name

Contact us about becoming a Conference Sponsor

Welcome to the Chicago Conference 2012

We are proud to present Chicago's first conference dedicated to polyamory March 20-22, 2012. This year's conference theme is "Celebrating the spectrum of love."

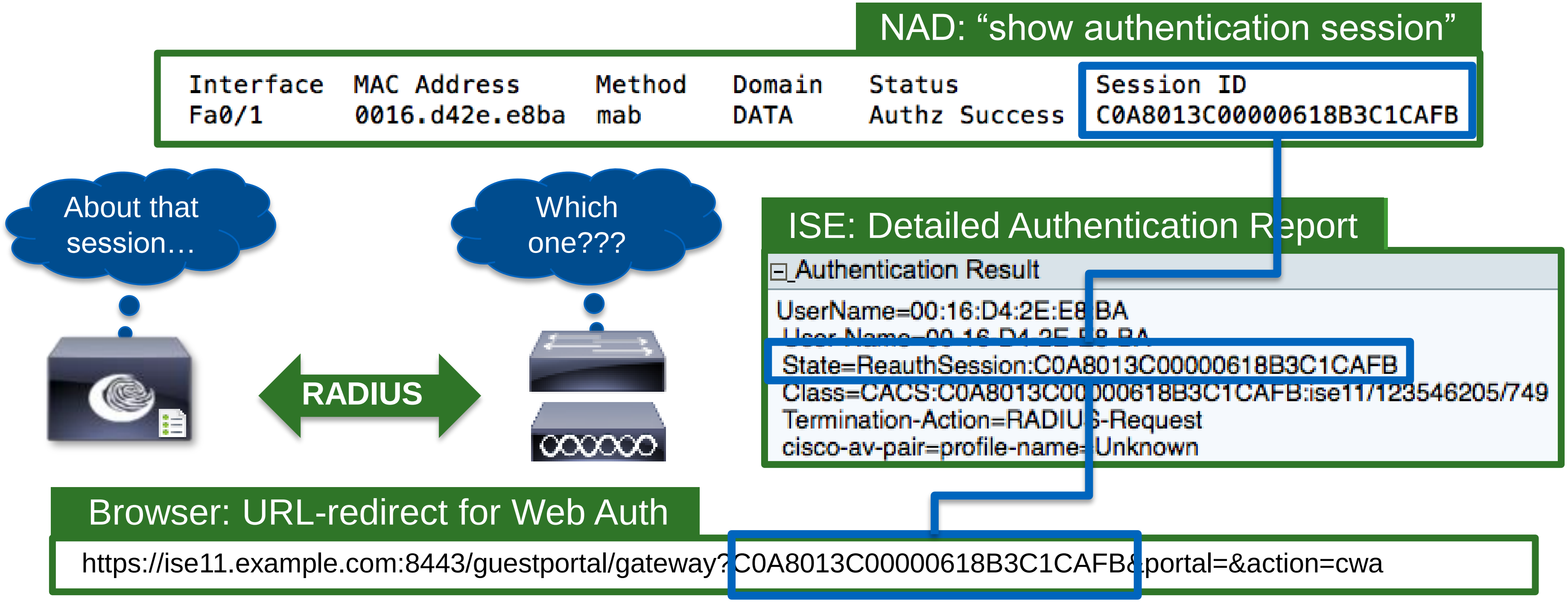
The conference is being held at the Center on Halsted 3656 North Halsted Street, Chicago, IL 60613.

Special guest speakers are...

blah, blah, blah...

Session ID

Glue That Binds Client Session to Access Device and ISE



NAD: “show authentication session”

```
Interface   MAC Address      Method    Domain    Status          Session ID
Fa0/1       0016.d42e.e8ba   mab       DATA      Authz Success   C0A8013C00000618B3C1CAFB
```

ISE: Detailed Authentication Report

⊟ Authentication Result

```
UserName=00:16:D4:2E:E8:BA
User-Name=00-16-D4-2E-E8-BA
State=ReauthSession:C0A8013C00000618B3C1CAFB
Class=CACS:C0A8013C00000618B3C1CAFB:ise11/123546205/749
Termination-Action=RADIUS-Request
cisco-av-pair=profile-name=Unknown
```

Browser: URL-redirect for Web Auth

```
https://ise11.example.com:8443/guestportal/gateway?C0A8013C00000618B3C1CAFB&portal=&action=cwa
```

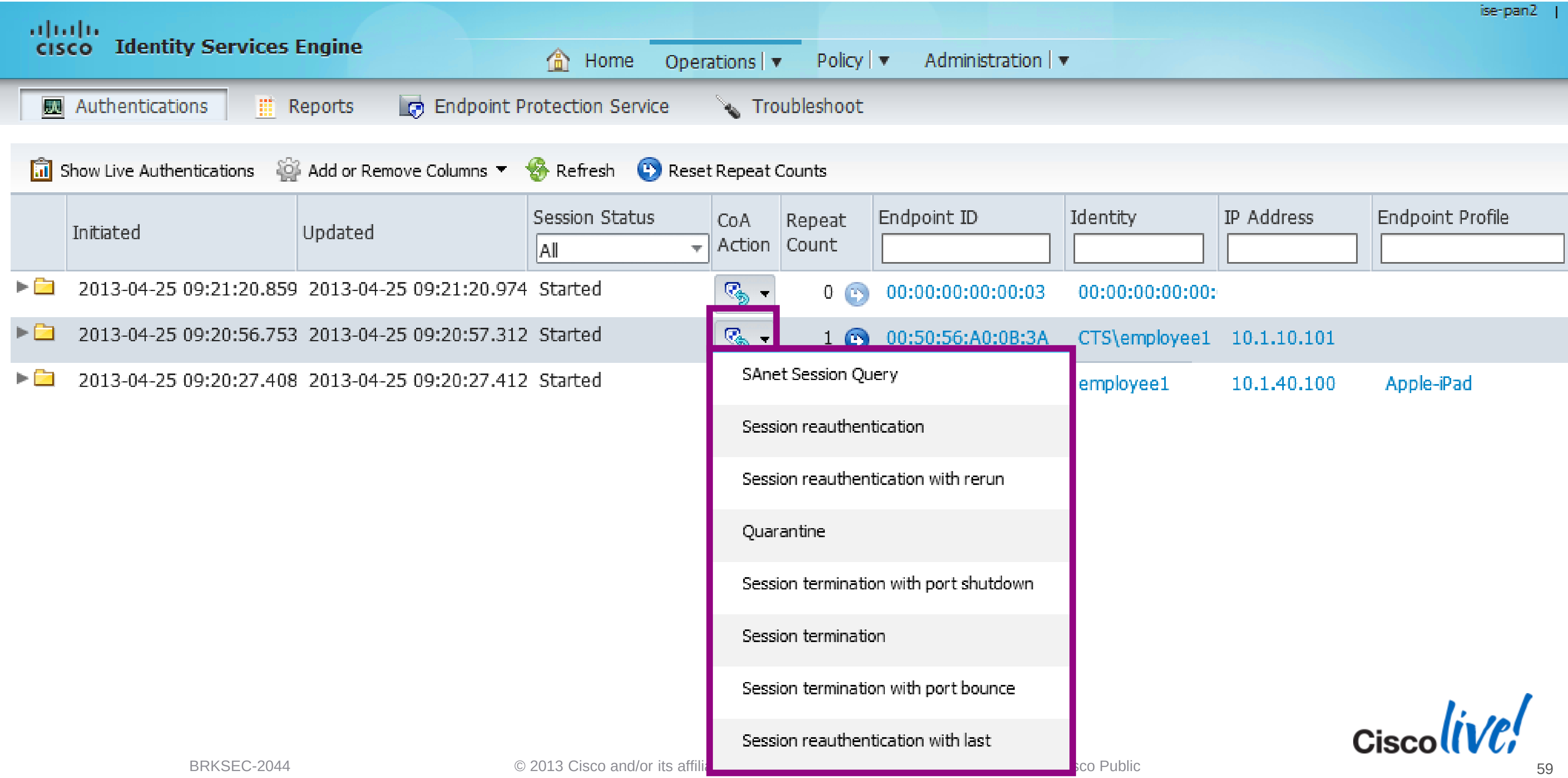
Change of Authorisation (CoA)

Adapt Policy to Changes in Endpoint State (Context)

- **Use Cases:**
  - How do we reauthorise the port when we discover it is an iPad?
  - How do we reauthorise the port once we have your identity through Central Web Auth?
  - How do we change access policy when endpoint becomes compliant with posture policy?
- **Problem:** A RADIUS server cannot start conversation with the authenticator. Authenticator (RADIUS client) must start conversation with the RADIUS server.
  - To get a new policy applied, user must disconnect/reconnect to network.
- **Solution:** CoA (RFC 3576 and 5176 – Dynamic Authorisation Extensions to RADIUS) allows the RADIUS server to start the conversation with the authenticator.

  Allows an enforcement device (switchport, wireless controller, VPN gateway) to change the VLAN/ACL/Redirection for a endpoint without requiring manual intervention by user/admin.

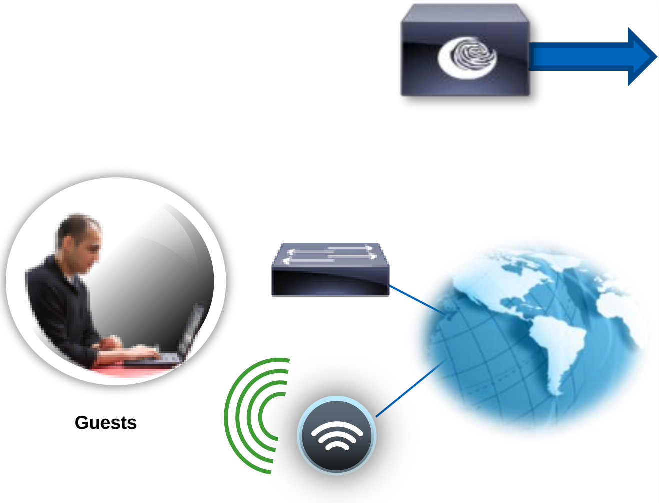
CoA from Live Sessions Log



	Initiated	Updated	Session Status	CoA Action	Repeat Count	Endpoint ID	Identity	IP Address	Endpoint Profile
			All						
▶	2013-04-25 09:21:20.859	2013-04-25 09:21:20.974	Started		0	00:00:00:00:00:03	00:00:00:00:00:		
▶	2013-04-25 09:20:56.753	2013-04-25 09:20:57.312	Started		1	00:50:56:A0:0B:3A	CTS\employee1	10.1.10.101	
▶	2013-04-25 09:20:27.408	2013-04-25 09:20:27.412	Started				employee1	10.1.40.100	Apple-iPad

Integrated Guest Services and Lifecycle Management

Components of a Full Guest Lifecycle Solution



Provisioning: Guest accounts via sponsor portal

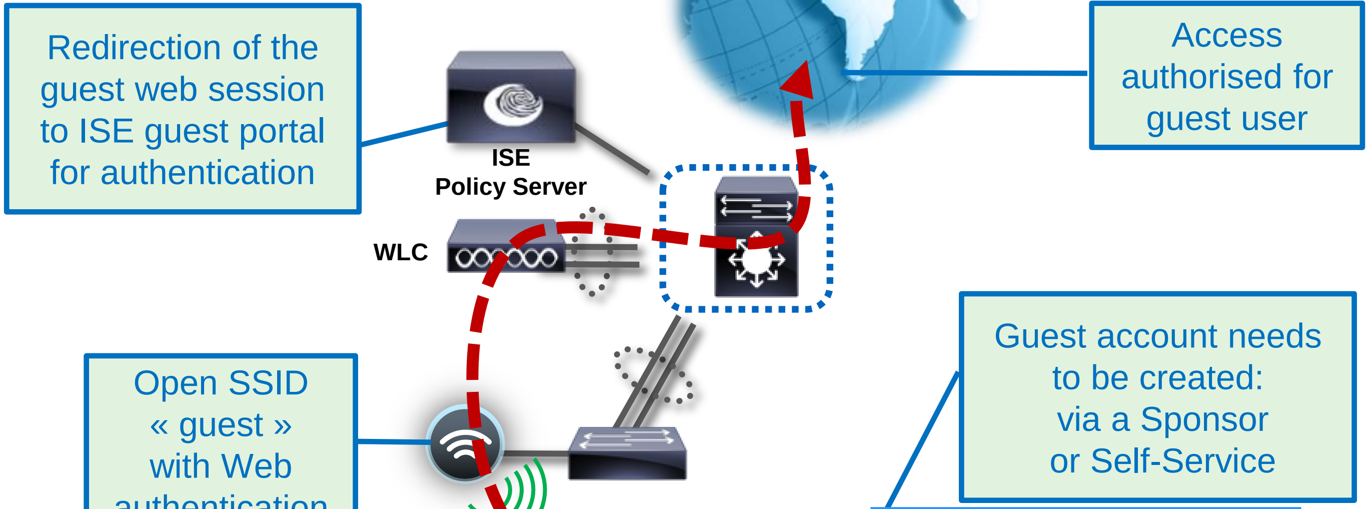
Notify: Guests of account details by print, email, or SMS

Manage: Sponsor privileges, guest accounts and policies, guest portal

Authenticate/Authorise guest via a guest portal on ISE

Report: On all aspects of guest accounts

How Does It Work?

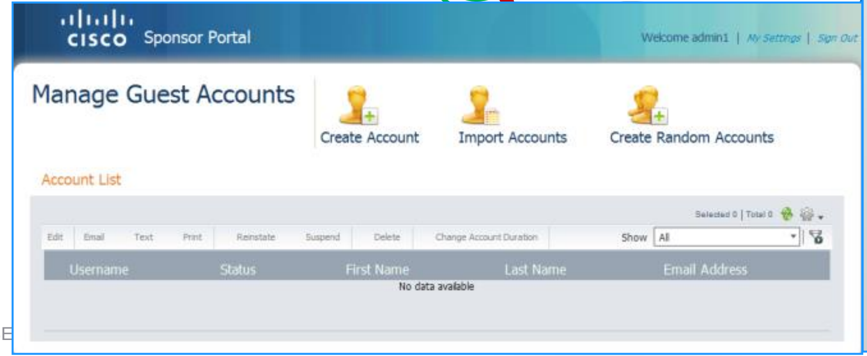


Redirection of the guest web session to ISE guest portal for authentication

Access authorised for guest user

Open SSID « guest » with Web authentication

Guest account needs to be created: via a Sponsor or Self-Service



Sponsor Portal

Welcome admin1 | My Settings | Sign Out

Manage Guest Accounts

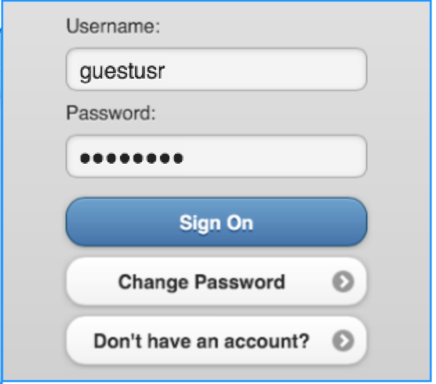
Create Account | Import Accounts | Create Random Accounts

Account List

Selected 0 | Total 0

Edit | Email | Text | Print | Reinstate | Suspend | Delete | Change Account Duration | Show All

Username	Status	First Name	Last Name	Email Address
No data available				



Username: guestusr

Password: ••••••••

Sign On

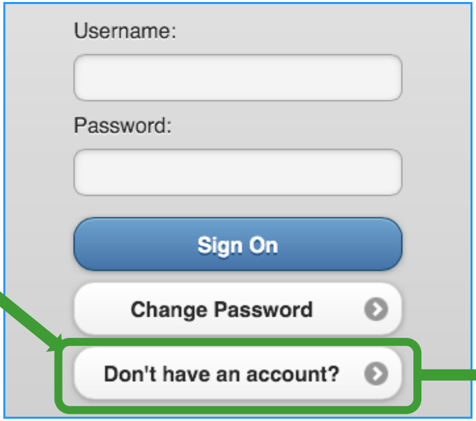
Change Password

Don't have an account?

Guest Users DB – Account Creation Methods

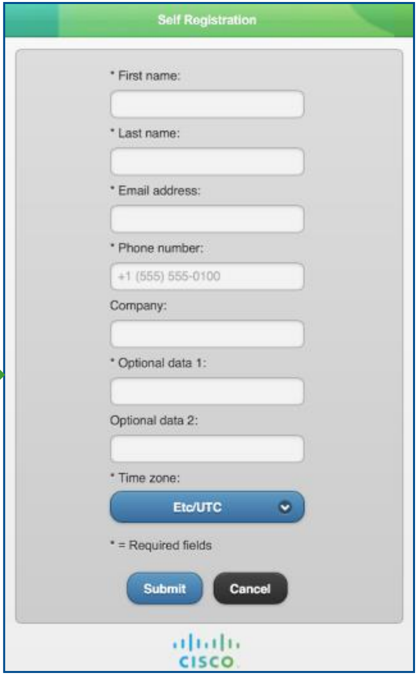
Two Ways to Populate ISE Internal Guest Database

- Self-Service
  Option on ISE 'Guest Portal'



Username:

Password:



Self Registration

* First name:

* Last name:

* Email address:

* Phone number: +1 (555) 555-0100

Company:

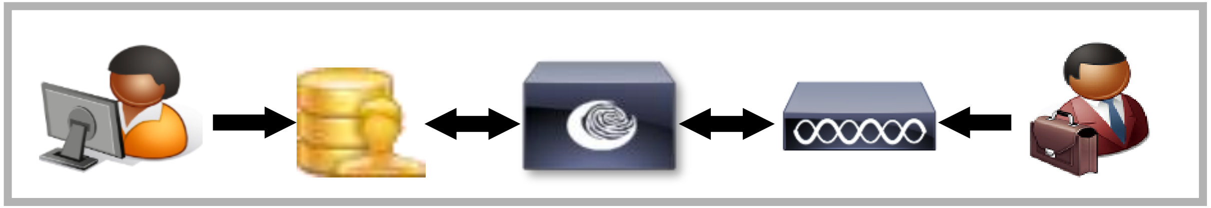
* Optional data 1:

Optional data 2:

* Time zone: Etc/UTC

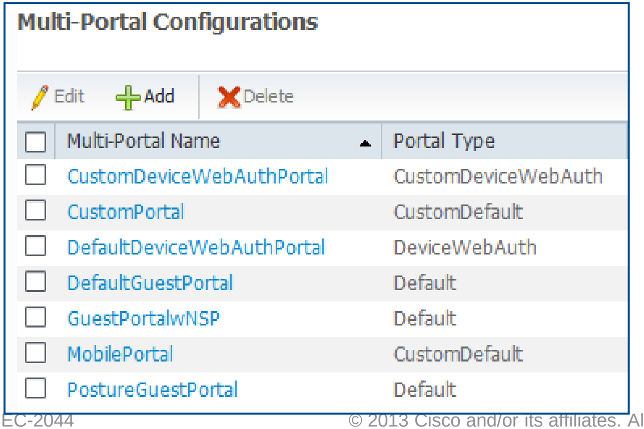
* = Required fields

- Sponsoring
  via ISE 'Sponsor Portal'



ISE – Multiple Guest Portals

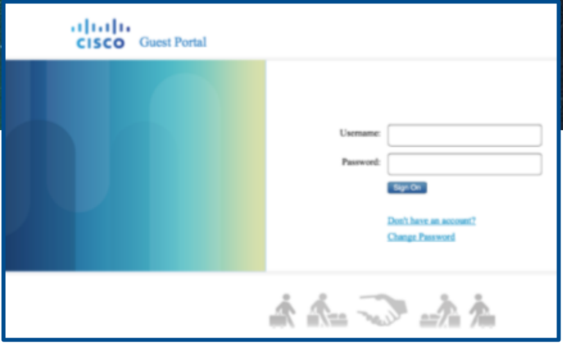
- Several portals may be needed to support different groups/users based on:
  - Location / country
  - Type of device: WLC, switches
  - Local language support
- ISE can hold several portals
- Multiple portals can be used simultaneously for authentication

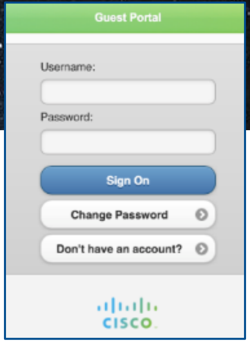


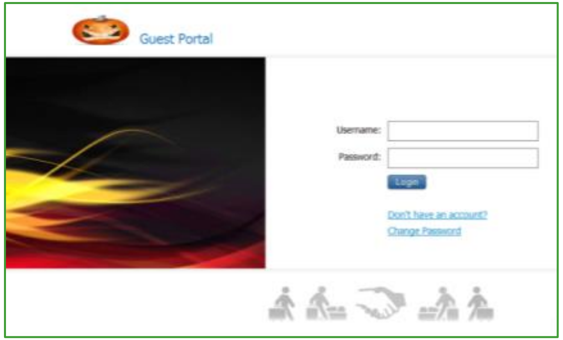
Multi-Portal Configurations

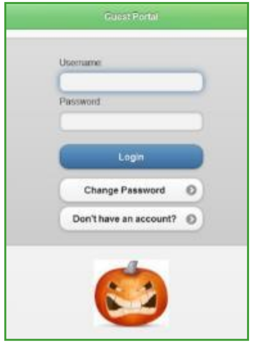
Edit | Add | Delete

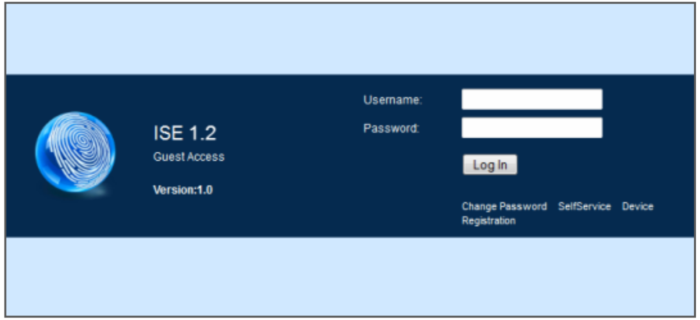
☐	Multi-Portal Name ▲	Portal Type
☐	CustomDeviceWebAuthPortal	CustomDeviceWebAuth
☐	CustomPortal	CustomDefault
☐	DefaultDeviceWebAuthPortal	DeviceWebAuth
☐	DefaultGuestPortal	Default
☐	GuestPortalwNSP	Default
☐	MobilePortal	CustomDefault
☐	PostureGuestPortal	Default



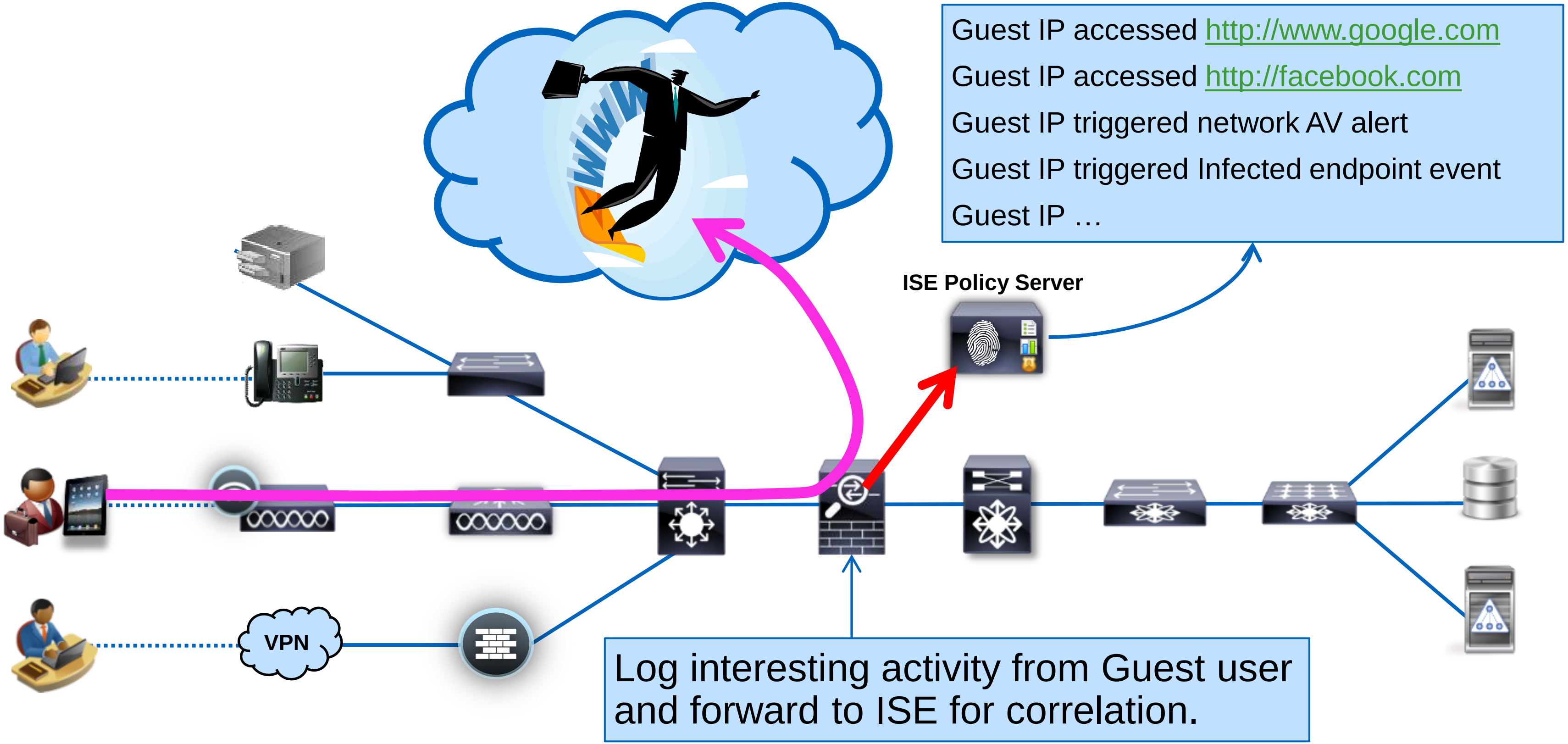








Guest Tracking Leverages Network Logging



Guest IP accessed http://www.google.com

Guest IP accessed http://facebook.com

Guest IP triggered network AV alert

Guest IP triggered Infected endpoint event

Guest IP …

Log interesting activity from Guest user and forward to ISE for correlation.

Posture

Are My Endpoints Compliant?

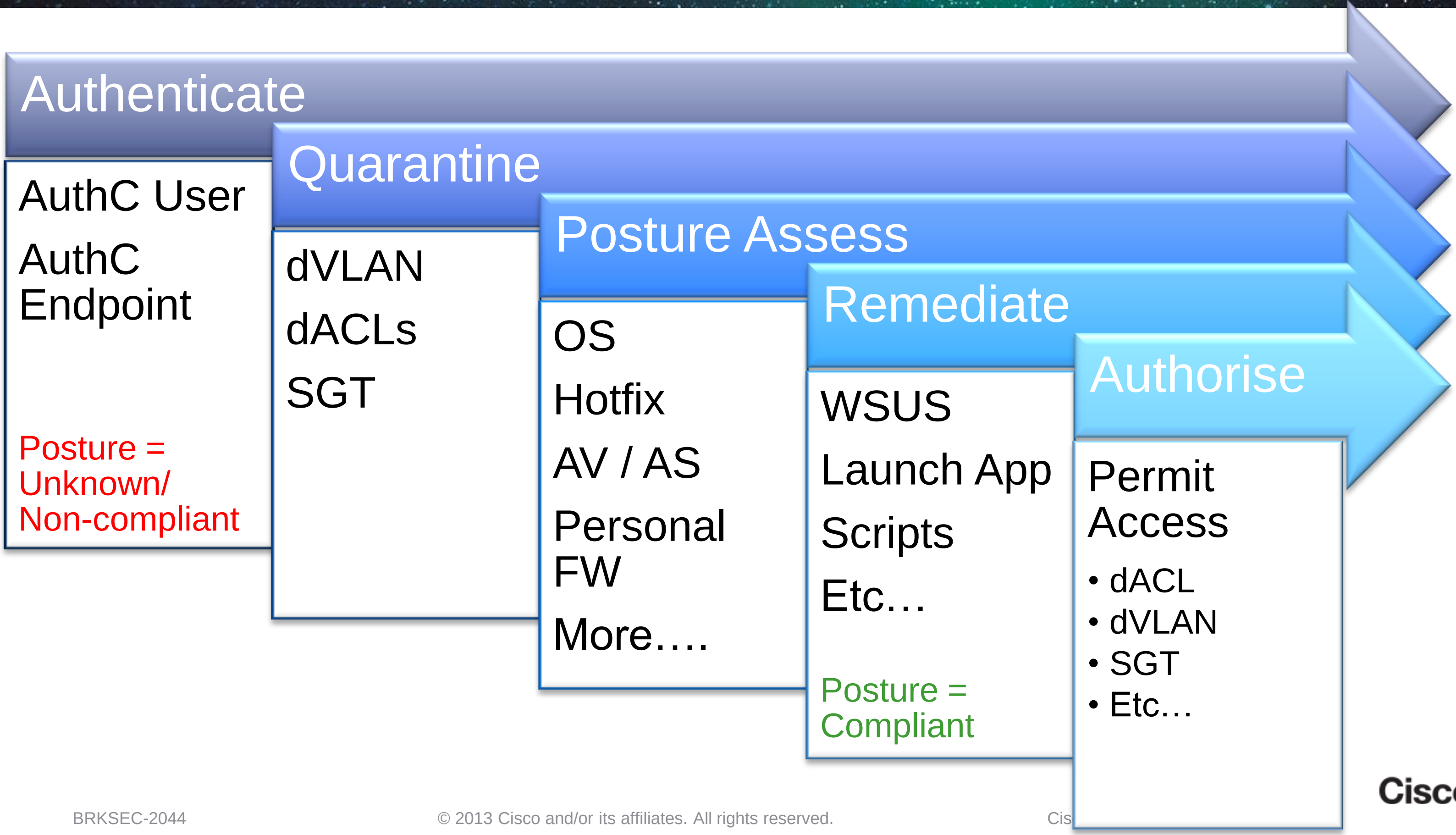
Posture Assessment

Does the Device Meet Security Requirements?

Posture

- Posture = The state-of-compliance with the company's security policy.
  - Is the system running the current Windows Patches?
  - Anti-Virus Installed? Is it Up-to-Date?
  - Anti-Spyware Installed? Is it Up-to-Date?
  - Is the endpoint running corporate application?
  - Is the endpoint running unauthorised application?
- Extends the user / system Identity to include Posture Status.

ISE Posture Assessment



Authenticate

AuthC User

AuthC Endpoint

Posture = Unknown/ Non-compliant

Quarantine

dVLAN

dACLs

SGT

Posture Assess

OS

Hotfix

AV / AS

Personal FW

More….

Remediate

WSUS

Launch App

Scripts

Etc…

Posture = Compliant

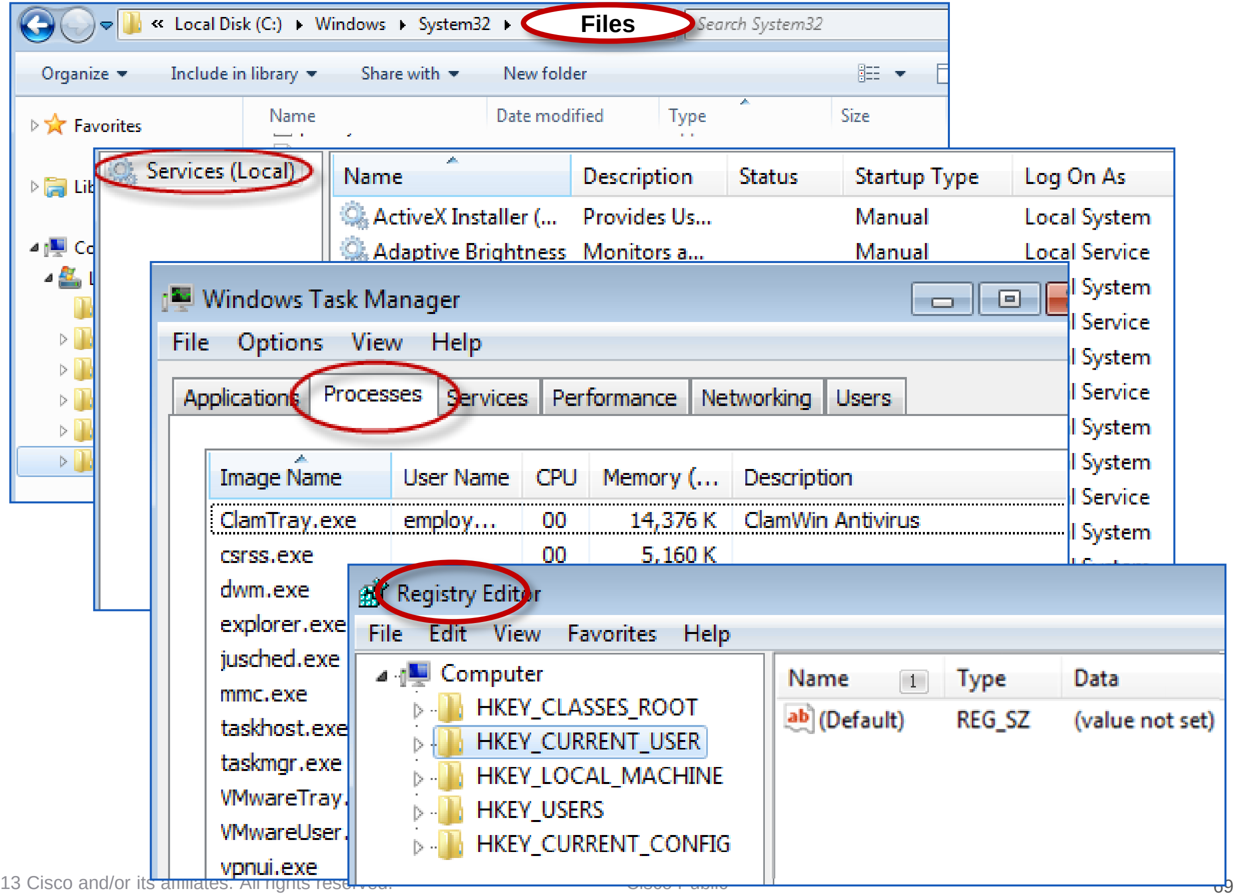
Authorise

Permit Access

- dACL
- dVLAN
- SGT
- Etc…

ISE Posture Assessment Checks

- Microsoft Updates
  - Service Packs
  - Hotfixes
  - OS/Browser versions
- Antivirus
  - Installation/Signatures
- Antispyware
  - Installation/Signatures
- File data
- Services
- Applications/Processes
- Registry keys



Name	Description	Status	Startup Type	Log On As
ActiveX Installer (...	Provides Us...		Manual	Local System
Adaptive Brightness	Monitors a...		Manual	Local Service

Image Name	User Name	CPU	Memory (...	Description
ClamTray.exe	employ...	00	14,376 K	ClamWin Antivirus
csrss.exe		00	5,160 K	
dwm.exe				
explorer.exe				
jusched.exe				
mmc.exe				
taskhost.exe				
taskmgr.exe				
VMwareTray.				
VMwareUser.				
vpnui.exe				

Computer
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Name	Type	Data
ab (Default)	REG_SZ	(value not set)

Posture Assessment

What If a User Fails the Check?

- Remediation
  - The act of correcting any missing or out-of-date items from the Posture Assessment.
- Common automated or guided remediation methods can trigger:
  - Corporate Patching Systems (Examples: BigFix, Altiris, etc.)
  - Windows Software Update Service (WSUS)
  - Windows Update
  - Anti-Virus product Update Services (LiveUpdate.exe, etc.)
  - Software download
  - Redirect to corporate Help Desk Portal
  - Message popup providing more detailed guidance

ISE – Posture Policies

Employee Policy:

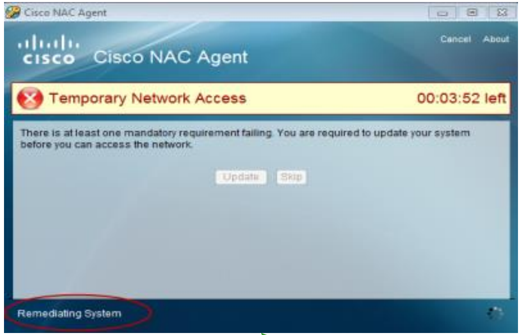
- Microsoft patches updated
- Trend Micro AV installed, running, and current
- Corp asset checks
- Enterprise application running

Contractor Policy:

- Any AV installed, running, and current

Guest Policy: Accept AUP

(No posture - Internet Only)



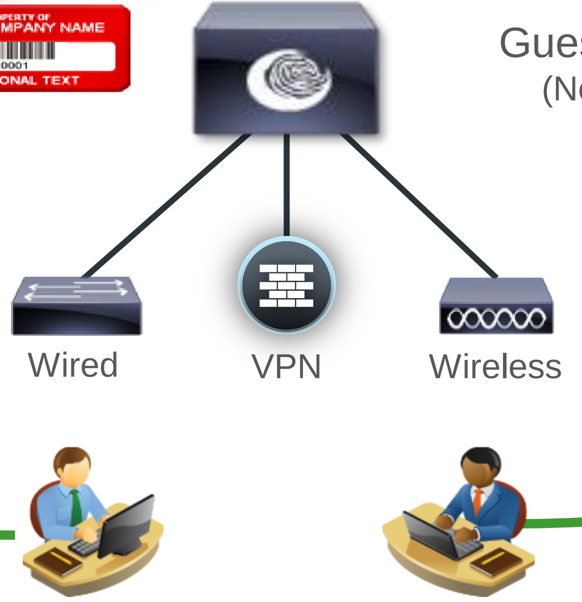
Cisco NAC Agent

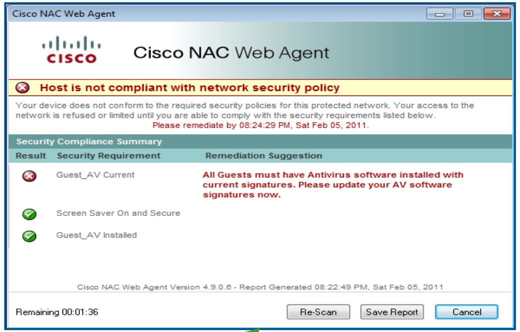
Cisco NAC Agent

Temporary Network Access 00:03:52 left

There is at least one mandatory requirement failing. You are required to update your system before you can access the network.

Remediating System





Cisco NAC Web Agent

Cisco NAC Web Agent

Host is not compliant with network security policy

Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.

Please remediate by 08:24:29 PM, Sat Feb 05, 2011.

Security Compliance Summary

Result	Security Requirement	Remediation Suggestion
☒	Guest_AV Current	All Guests must have Antivirus software installed with current signatures. Please update your AV software signatures now.
✓	Screen Saver On and Secure	
✓	Guest_AV Installed	

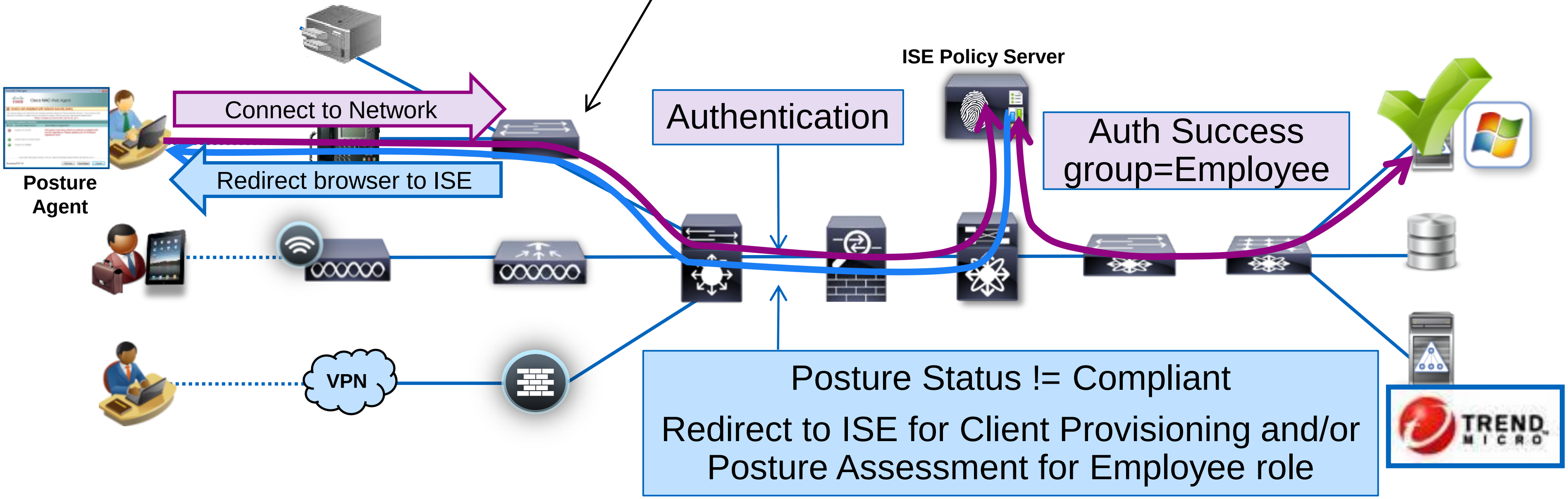
Cisco NAC Web Agent Version 4.9.0.6 - Report Generated 08:22:49 PM, Sat Feb 05, 2011

Remaining 00:01:36

Posture Flow

- If Posture Status = Unknown/Non-Compliant, then Redirect to ISE for Posture Assessment
- If Posture Agent not deployed, then provision Web Agent or Persistent NAC Agent

https://ise.company.com:8443/guestportal/gateway?sessionId=0A010A...73691A&action=**cpp**



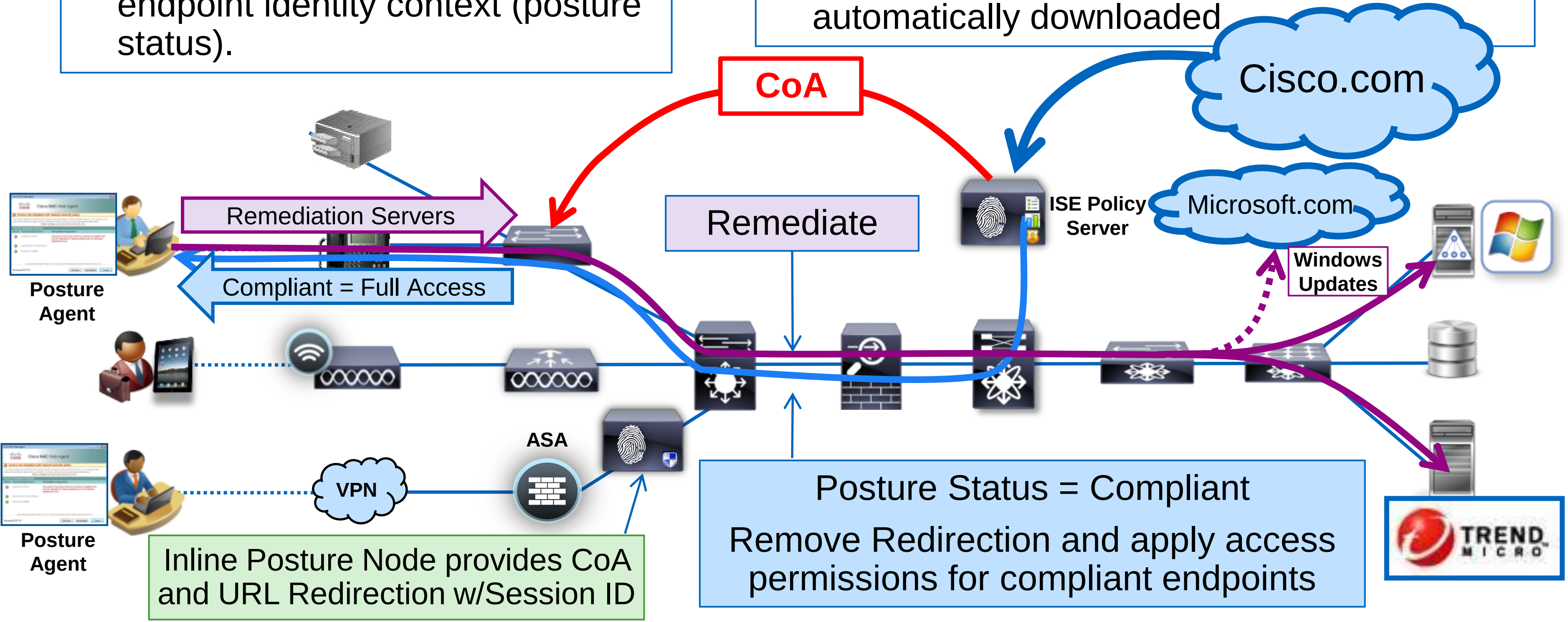
Posture Status != Compliant

Redirect to ISE for Client Provisioning and/or Posture Assessment for Employee role

Posture Remediation and Client Resources

- CoA allows re-authentication to be processed based on new endpoint identity context (posture status).

- Hourly updates for latest posture definitions
- New posture agents and modules automatically downloaded



Inline Posture Node provides CoA and URL Redirection w/Session ID

Posture Status = Compliant

Remove Redirection and apply access permissions for compliant endpoints

BYOD

Extending Network Access to Personal Devices

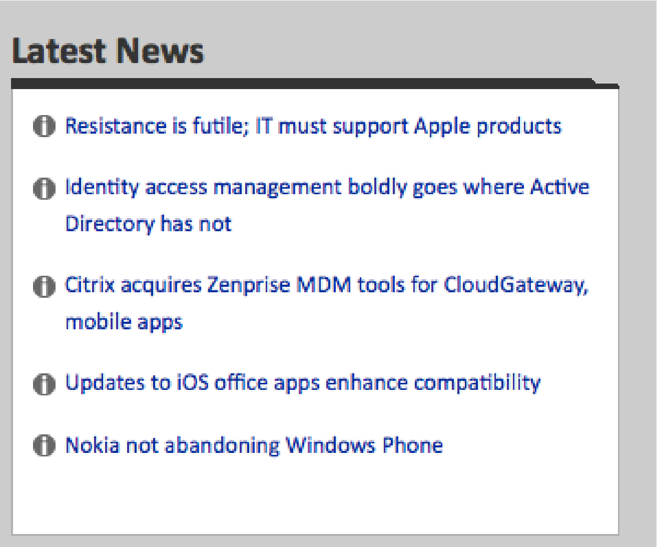
Look Back at 2009

Q: Will you Allow Employees to use personal iPhones, iPads, etc.?

A: Absolutely Not!

Cisco Responds:

Now, in 2013:



Latest News

- Resistance is futile; IT must support Apple products
- Identity access management boldly goes where Active Directory has not
- Citrix acquires Zenprise MDM tools for CloudGateway, mobile apps
- Updates to iOS office apps enhance compatibility
- Nokia not abandoning Windows Phone

“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.”

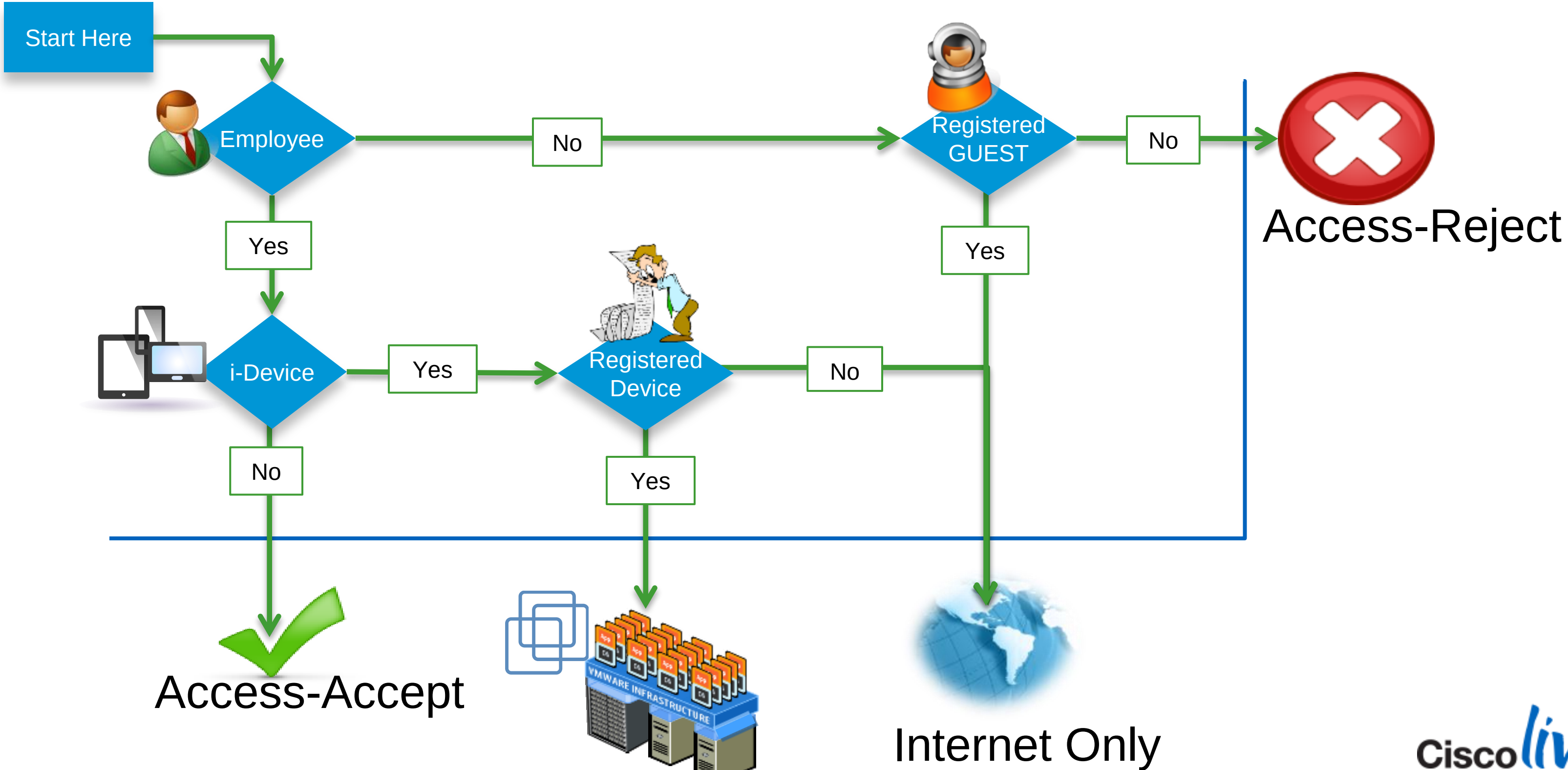
Steve Jobs, 2011

“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

What Makes a BYOD policy?

Sample BYOD Policy Flow



What Makes a BYOD Policy

The Policy Server is Critical to Meeting Your Goals

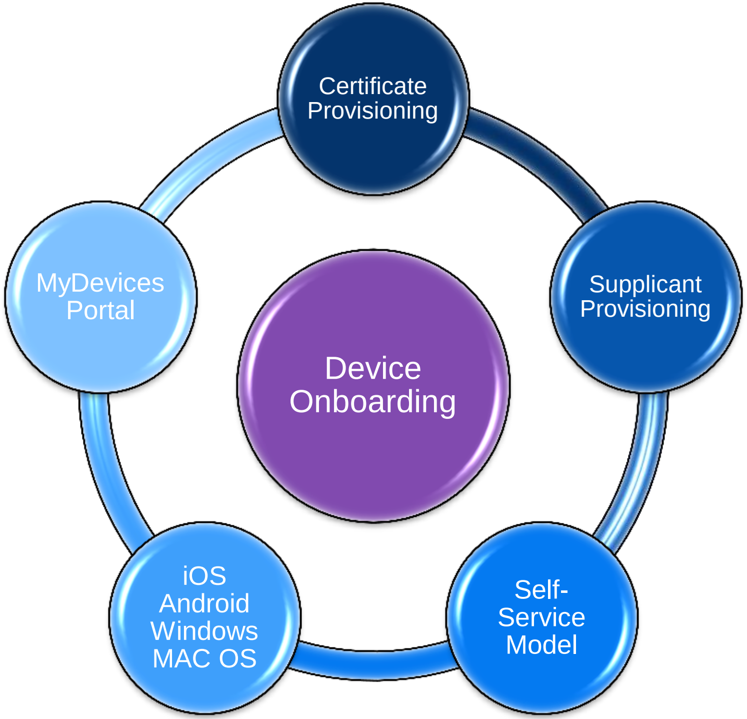
Context-Based Identity and Access Control

- Identity Services Engine = BYOD engine!

Who? Known users (Employees, Sales, HR) Unknown users (Guests)	What? Device identity Device classification (profile) Device health (posture)	How? Wired Wireless VPN
Where? Geographic location Department AP / SSID / Switchport	When? Date Time Start/Stop Access	Other? Custom attributes Device/User states Applications used

Onboarding Personal Devices

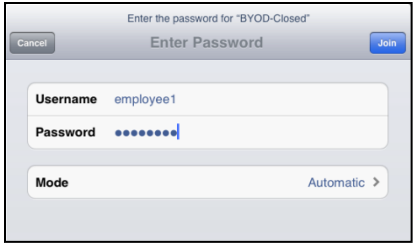
Registration, Certificate and Supplicant Provisioning



- Provisions device Certificates.
  - Based on Employee-ID & Device-ID.
- Provisions Native Supplicants:
  - Windows: XP, Vista, 7 & 8
  - Mac: OS X 10.6, 10.7 & 10.8
  - iOS: 4, 5 & 6
  - Android – 2.2 and above
  - 802.1X + EAP-TLS, PEAP & EAP-FAST
- Employee Self-Service Portal
  - Lost Devices are Blacklisted
  - Self-Service Model reduces IT burden
- Single and Dual SSID onboarding.

Single Versus Dual SSID Provisioning

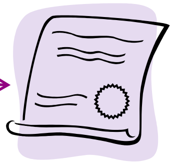
- Single SSID
  - Start with 802.1X on one SSID using PEAP


Enter the password for "BYOD-Closed"

Username employee1
Password ••••••••
Mode Automatic

SSID = BYOD-Closed (802.1X)

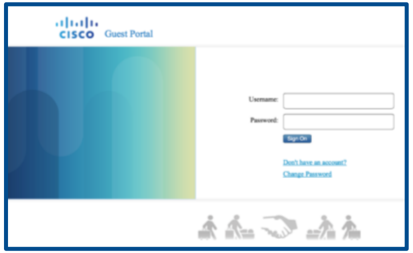
  - End on *same* SSID with 802.1X using EAP-TLS



WLAN Profile
SSID = BYOD-Closed
EAP-TLS
Certificate=MyCert

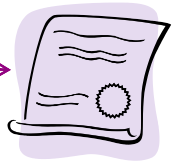
- Dual SSID
  - Start with CWA on one SSID

SSID = BYOD-Open
(MAB / CWA)



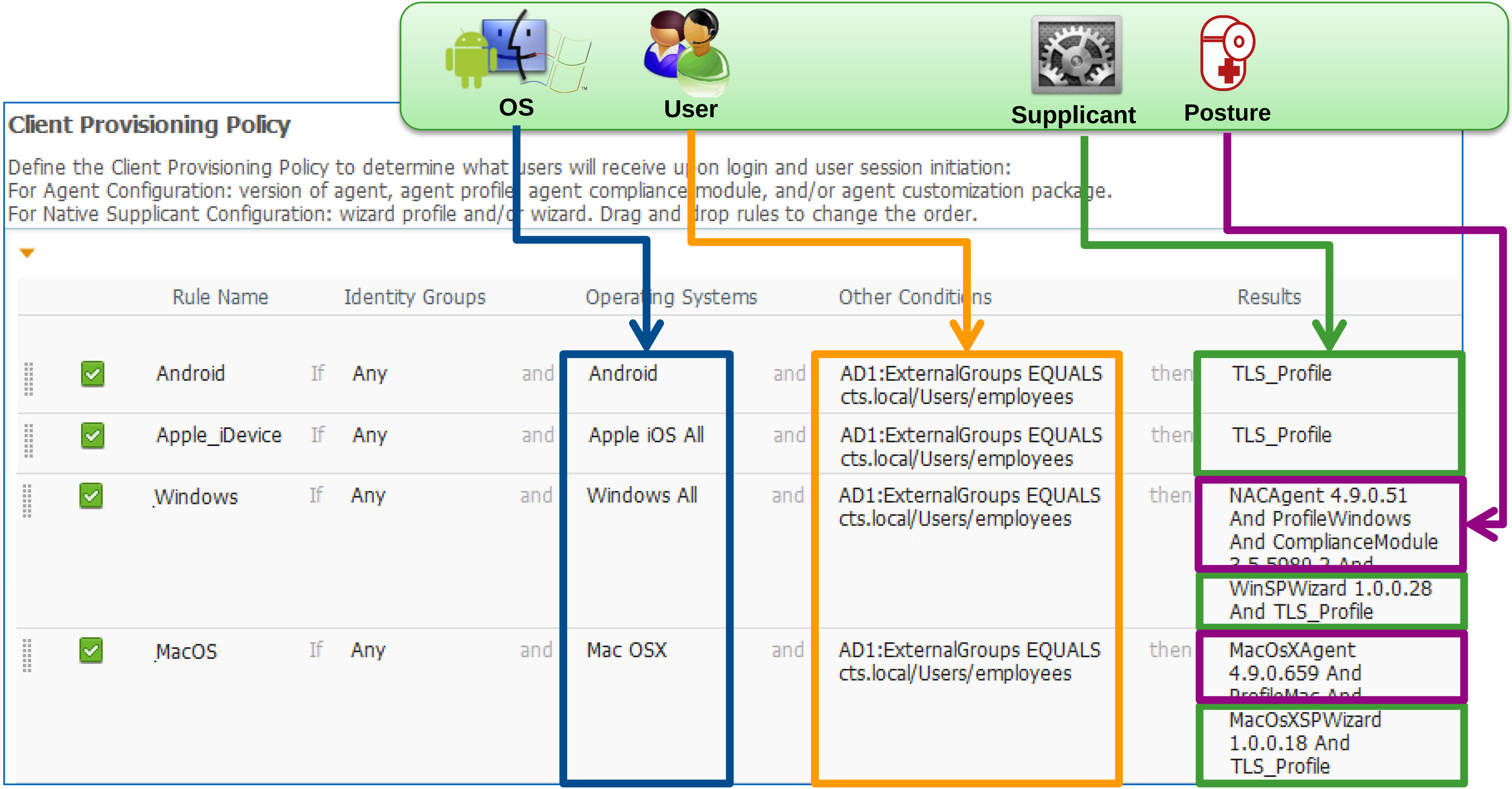
SSID = BYOD-Closed (802.1X)

  - End on *different* SSID with 802.1X using PEAP or EAP-TLS



WLAN Profile
SSID = BYOD-Closed
PEAP or EAP-TLS
(Certificate=MyCert)

Client Provisioning Policy

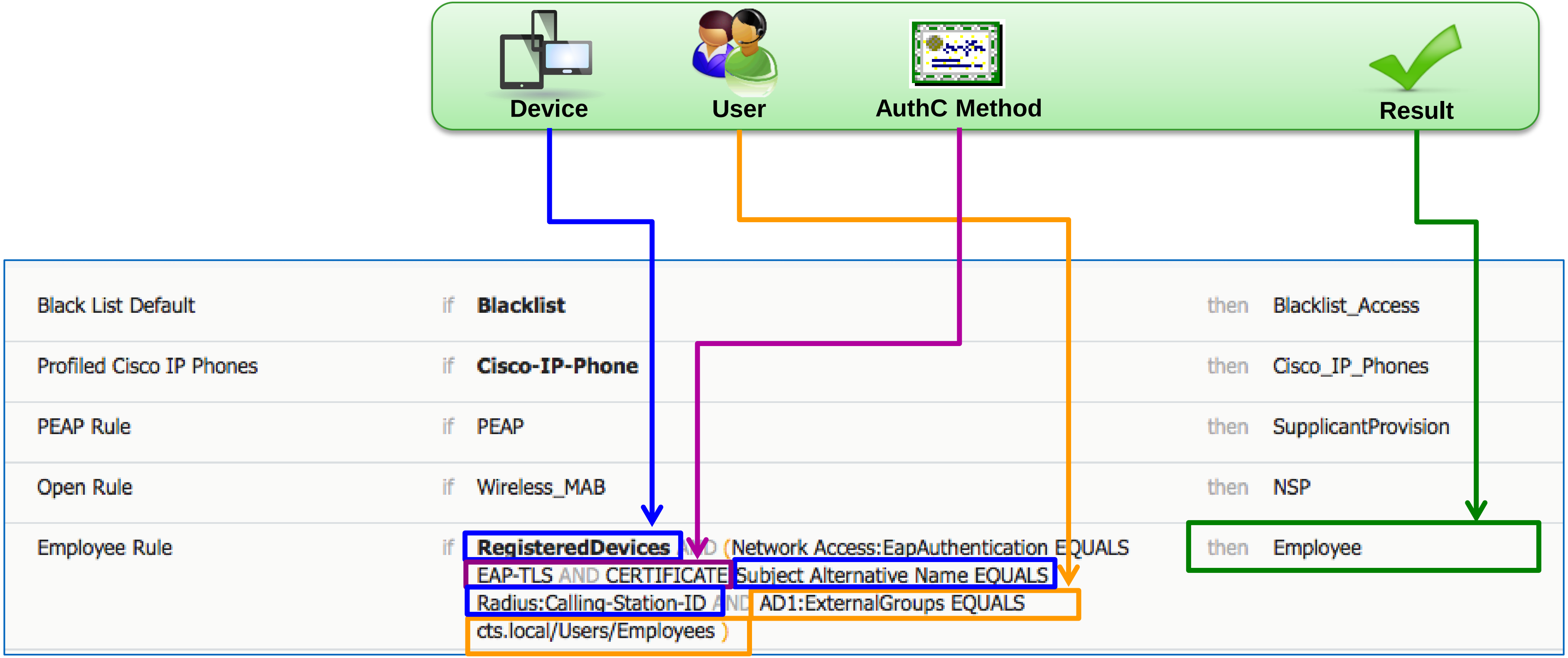


Client Provisioning Policy

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. Drag and drop rules to change the order.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	Android	If	Any	and	Android	and	AD1:ExternalGroups EQUALS cts.local/Users/employees	then	TLS_Profile
☑	Apple_iDevice	If	Any	and	Apple iOS All	and	AD1:ExternalGroups EQUALS cts.local/Users/employees	then	TLS_Profile
☑	Windows	If	Any	and	Windows All	and	AD1:ExternalGroups EQUALS cts.local/Users/employees	then	NACAgent 4.9.0.51 And ProfileWindows And ComplianceModule 3.5.5080.2 And WinSPWizard 1.0.0.28 And TLS_Profile
☑	MacOS	If	Any	and	Mac OSX	and	AD1:ExternalGroups EQUALS cts.local/Users/employees	then	MacOsXAgent 4.9.0.659 And ProfileMac And MacOsXSPWizard 1.0.0.18 And TLS_Profile

BYOD Policy in ISE



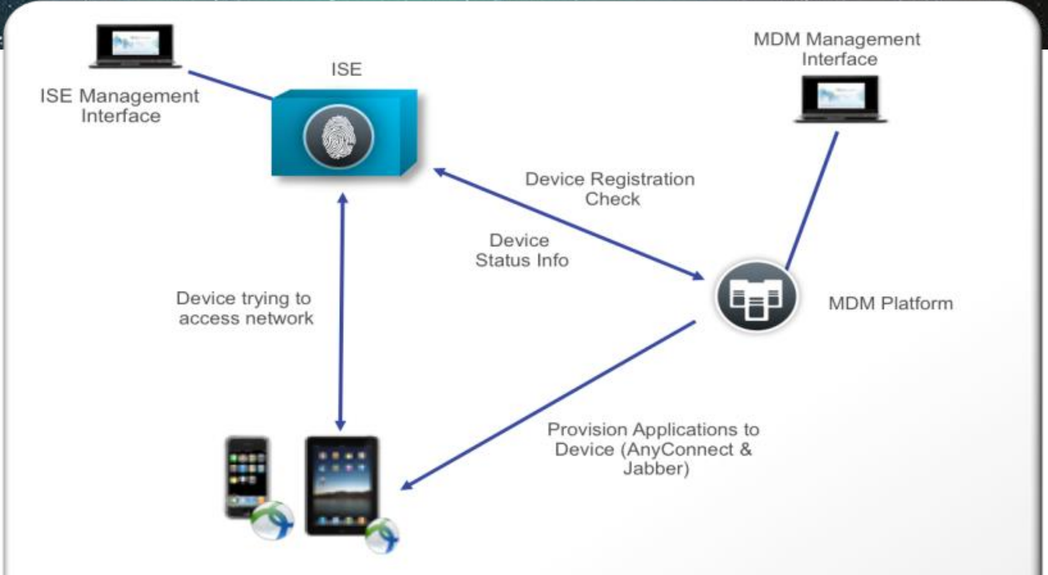
Black List Default	if	**Blacklist**	then	Blacklist_Access
Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
PEAP Rule	if	PEAP	then	SupplicantProvision
Open Rule	if	Wireless_MAB	then	NSP
Employee Rule	if	**RegisteredDevices** AND (Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE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

Mobile Device Management (MDM)

Extending “Posture” Assessment and Remediation to Mobile Devices

ISE Integration with 3rd-Party MDM Vendors

- MDM device registration via ISE
  - Non registered clients redirected to MDM registration page
- Restricted access
  - Non compliant clients will be given restricted access based on policy
- Endpoint MDM agent
  - Compliance
  - Device applications check
- Device action from ISE
  - Device stolen -> wipe data on client


ISE Management Interface
ISE
MDM Management Interface
Device Registration Check
Device Status Info
Device trying to access network
MDM Platform
Provision Applications to Device (AnyConnect & Jabber)

CISCO MCMS

MobileIron
Version: 5.0

airwatch
Version: 6.2

CITRIX ZENPRISE
Version: 7.1

Good
Version: 2.3

SYBASE iAnywhere Afaria

MaaS360 by Fiberlink

MDM Compliance Checking

Compliance and Attribute Retrieval via API

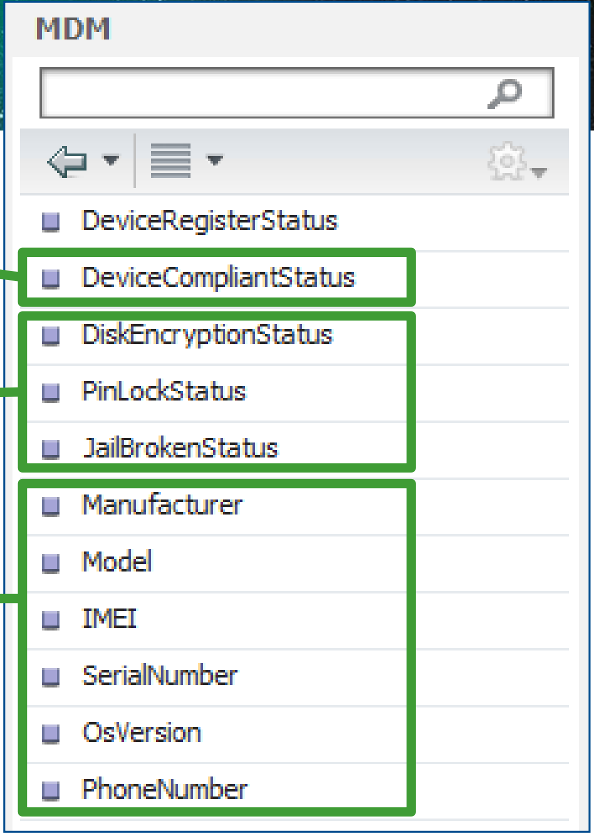
- Compliance based on:
  - General Compliant or ! Compliant status

  Macro level

  OR

  - Disk encryption enabled
  - Pin lock enabled
  - Jail broken status

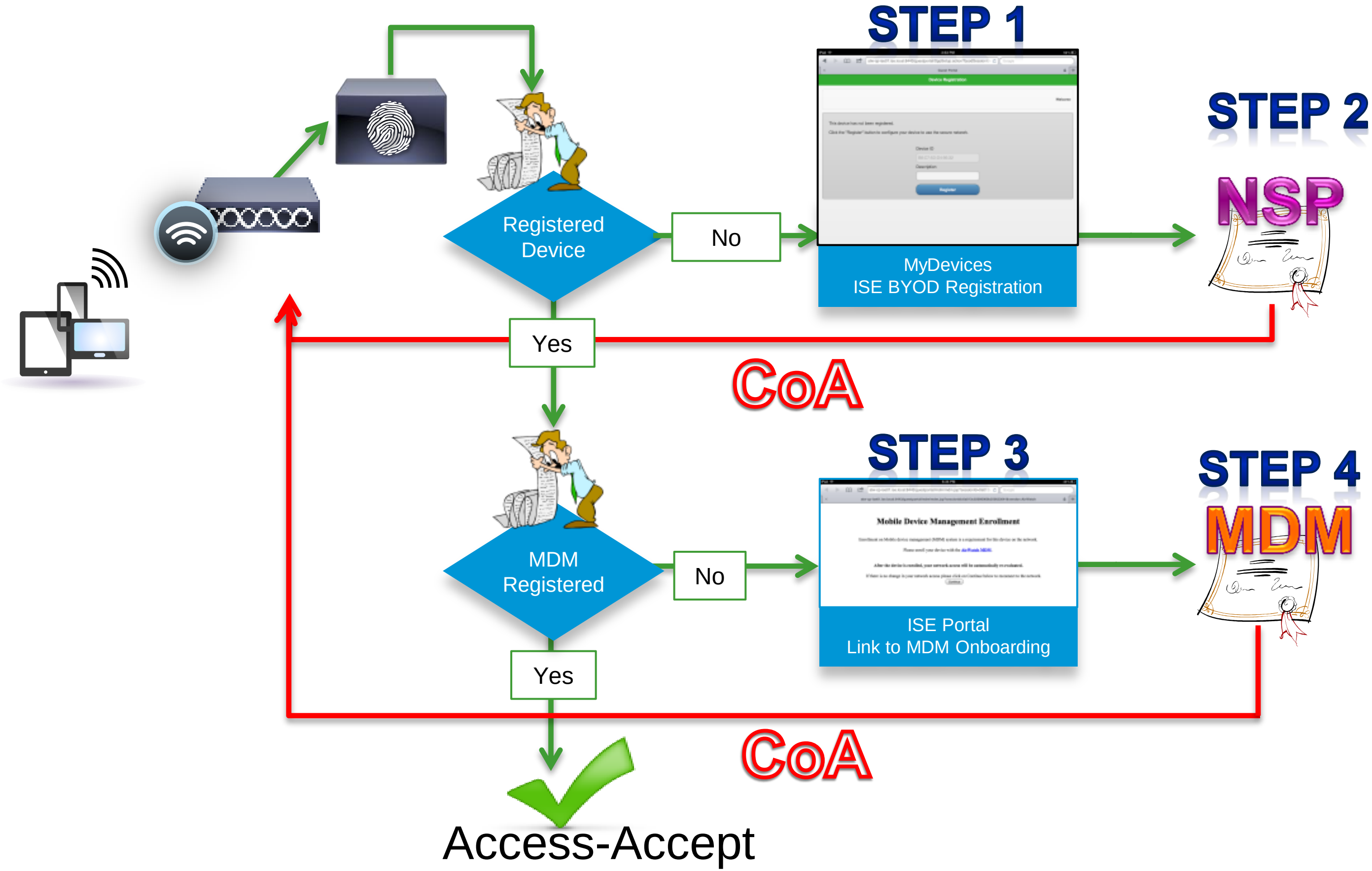
  Micro level
- MDM attributes available for policy conditions
- "Passive Reassessment": Bulk recheck against the MDM server using configurable timer.
  - If result of periodic recheck shows that a connected device is no longer compliant, ISE sends a CoA to terminate session.



MDM

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus
- JailBrokenStatus
- Manufacturer
- Model
- IMEI
- SerialNumber
- OsVersion
- PhoneNumber

MDM Onboarding Flow



This device has not been registered.

Click the "Register" button to configure your device to use the secure network.

Mobile Device Management Enrollment

Enrollment on Mobile device management (MDM) system is a requirement for this device on the network.

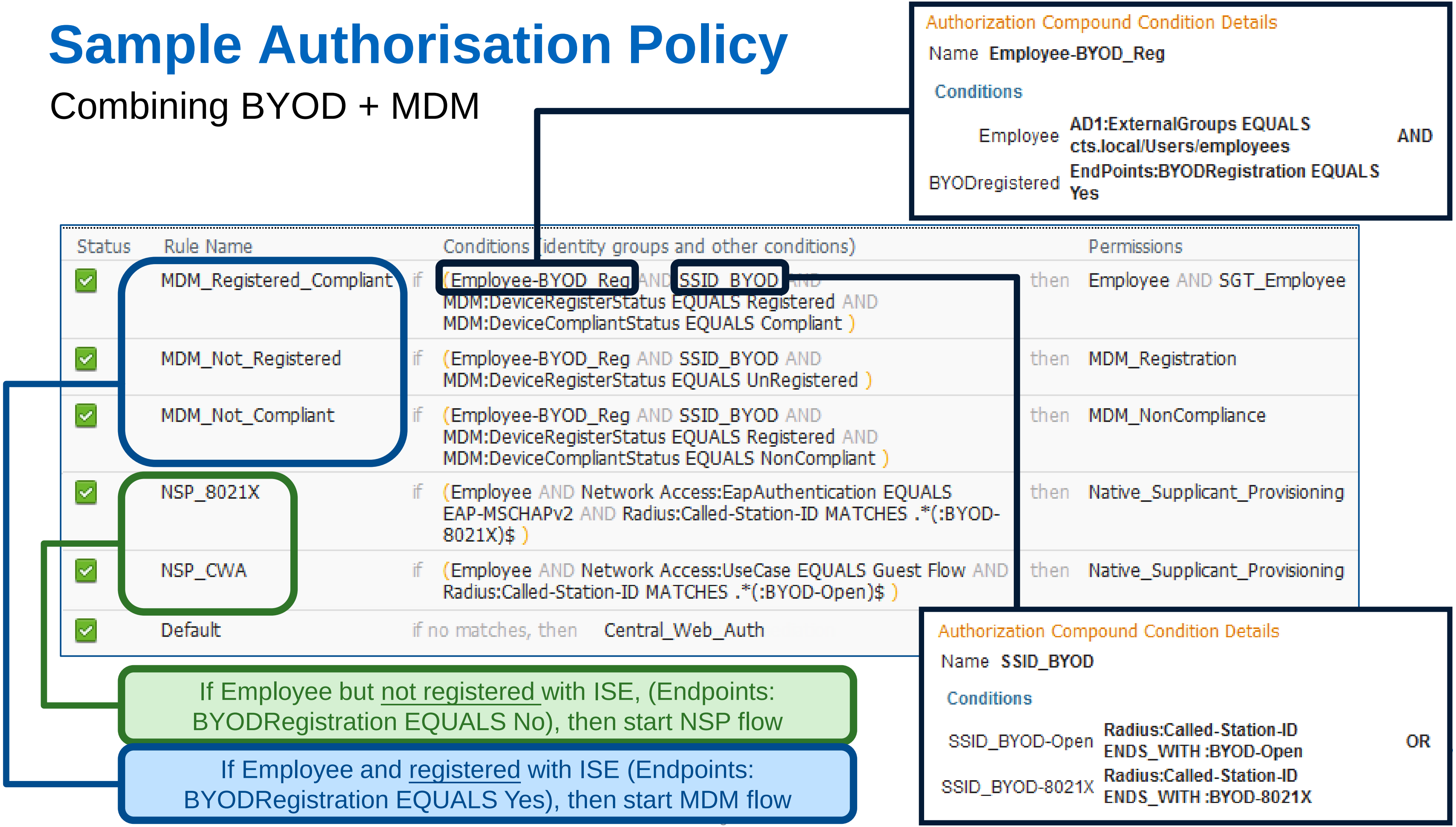
Please enroll your device with the AirWatch MDM.

After the device is enrolled, your network access will be automatically re-evaluated.

If there is no change in your network access please click on Continue below to reconnect to the network.

Sample Authorisation Policy

Combining BYOD + MDM



Authorization Compound Condition Details

Name **Employee-BYOD_Reg**

Conditions

Employee	**AD1:ExternalGroups EQUALS cts.local/Users/employees**	**AND**
BYODregistered	**EndPoints:BYODRegistration EQUALS Yes**	

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	MDM_Registered_Compliant	if	(Employee-BYOD_Reg AND SSID_BYOD AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:DeviceCompliantStatus EQUALS Compliant)	then	Employee AND SGT_Employee
✓	MDM_Not_Registered	if	(Employee-BYOD_Reg AND SSID_BYOD AND MDM:DeviceRegisterStatus EQUALS UnRegistered)	then	MDM_Registration
✓	MDM_Not_Compliant	if	(Employee-BYOD_Reg AND SSID_BYOD AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:DeviceCompliantStatus EQUALS NonCompliant)	then	MDM_NonCompliance
✓	NSP_8021X	if	(Employee AND Network Access:EapAuthentication EQUALS EAP-MSCHAPv2 AND Radius:Called-Station-ID MATCHES .*(:BYOD-8021X)$)	then	Native_Supplicant_Provisioning
✓	NSP_CWA	if	(Employee AND Network Access:UseCase EQUALS Guest Flow AND Radius:Called-Station-ID MATCHES .*(:BYOD-Open)$)	then	Native_Supplicant_Provisioning
✓	Default	if no matches, then	Central_Web_Auth		

Authorization Compound Condition Details

Name **SSID_BYOD**

Conditions

SSID_BYOD-Open	**Radius:Called-Station-ID ENDS_WITH :BYOD-Open**	**OR**
SSID_BYOD-8021X	**Radius:Called-Station-ID ENDS_WITH :BYOD-8021X**	

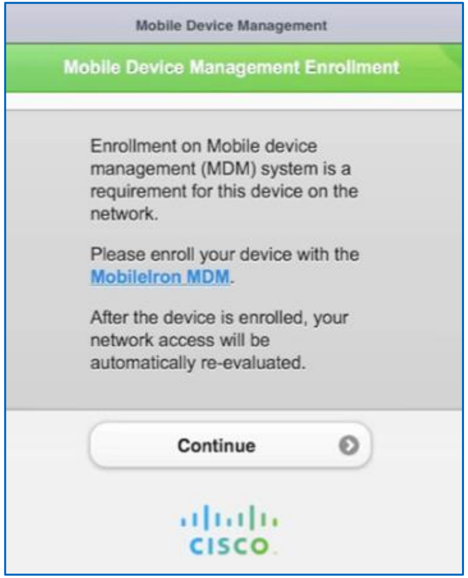
If Employee but not registered with ISE, (Endpoints: BYODRegistration EQUALS No), then start NSP flow

If Employee and registered with ISE (Endpoints: BYODRegistration EQUALS Yes), then start MDM flow

MDM Enrollment and Compliance

User Experience Upon MDM URL Redirect

MDM Enrollment



Mobile Device Management

Mobile Device Management Enrollment

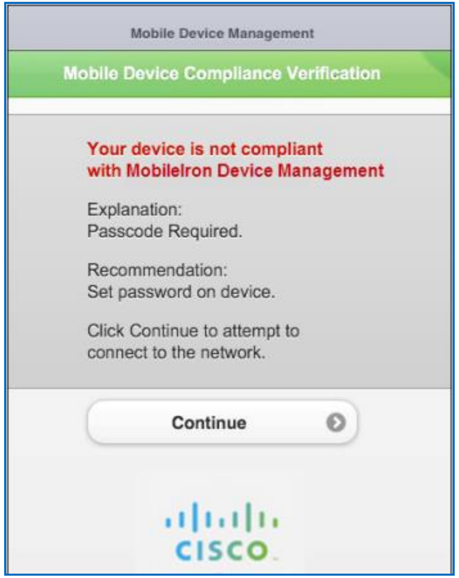
Enrollment on Mobile device management (MDM) system is a requirement for this device on the network.

Please enroll your device with the MobileIron MDM.

After the device is enrolled, your network access will be automatically re-evaluated.

MDM:DeviceRegistrationStatus EQUALS UnRegistered

MDM Compliance



Mobile Device Management

Mobile Device Compliance Verification

Your device is not compliant with MobileIron Device Management

Explanation:
Passcode Required.

Recommendation:
Set password on device.

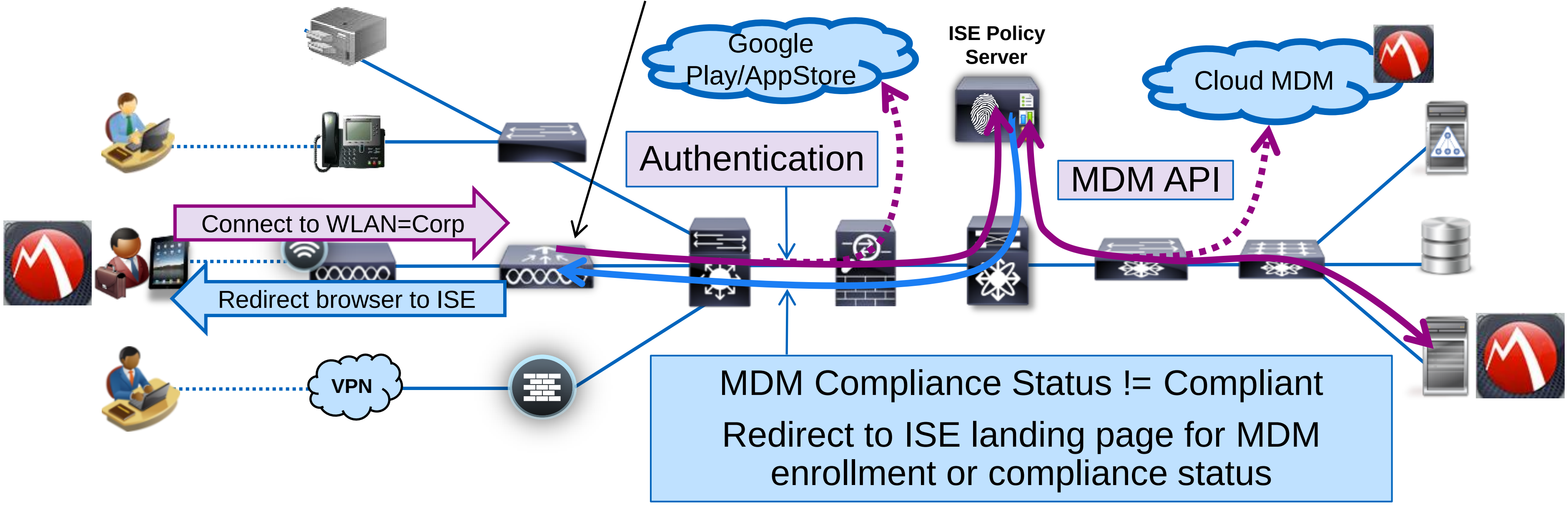
Click Continue to attempt to connect to the network.

MDM:DeviceCompliantStatus EQUALS NonCompliant

MDM Flow

- If MDM Registration Status EQUALS UnRegistered, then Redirect to MDM for Enrollment
- If MDM Compliance Status EQUALS NonCompliant, then Redirect to MDM for Compliance

https://ise.company.com:8443/guestportal/gateway?sessionId=0A010A...73691A&action=**mdm**



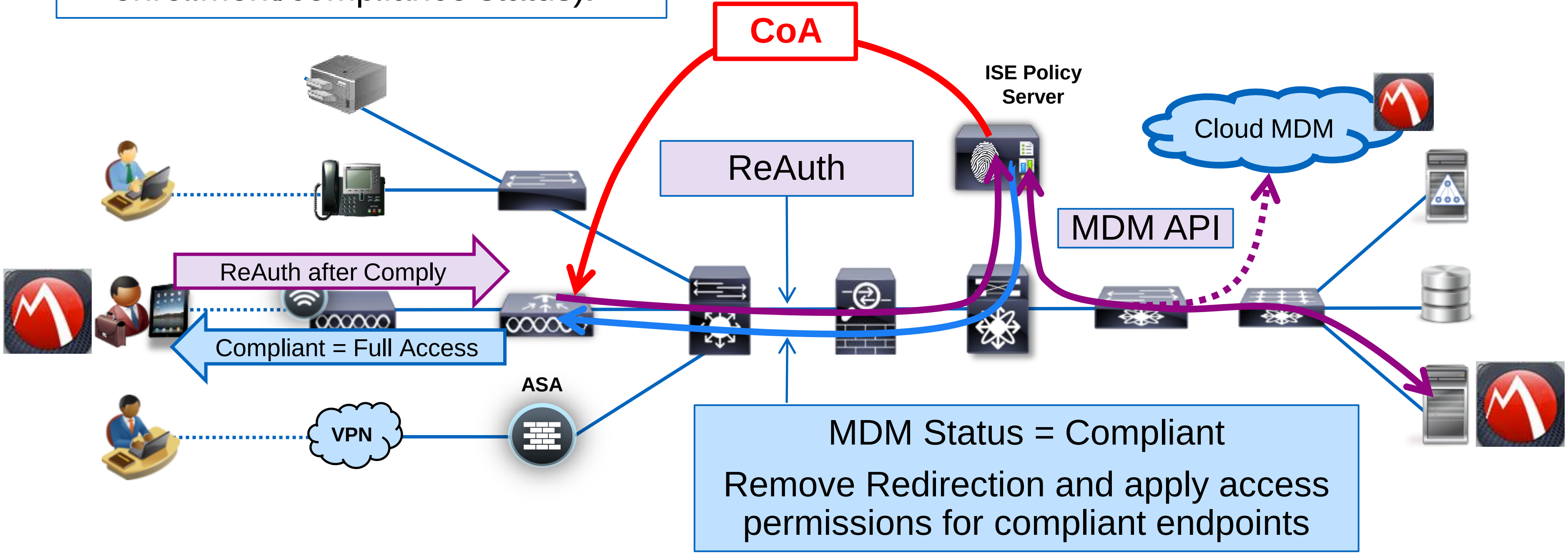
MDM Compliance Status != Compliant

Redirect to ISE landing page for MDM enrollment or compliance status

MDM Remediation

- CoA allows re-authentication to be processed based on new endpoint identity context (MDM enrollment/compliance status).

- MDM Agents downloaded directly from MDM Server or Internet App Stores
- Periodic recheck via API; CoA if not compliant



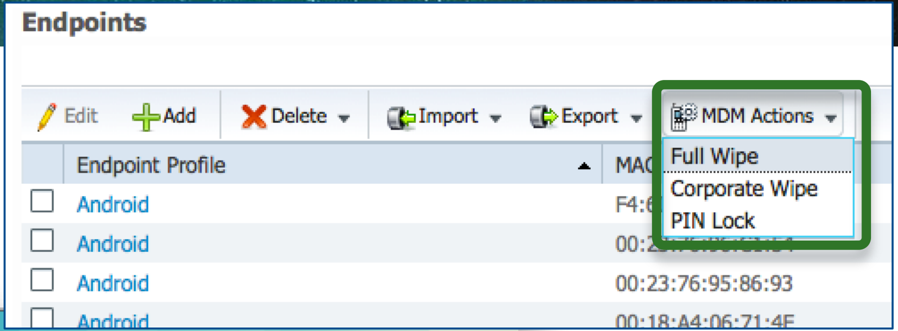
MDM Status = Compliant

Remove Redirection and apply access permissions for compliant endpoints

MDM Integration

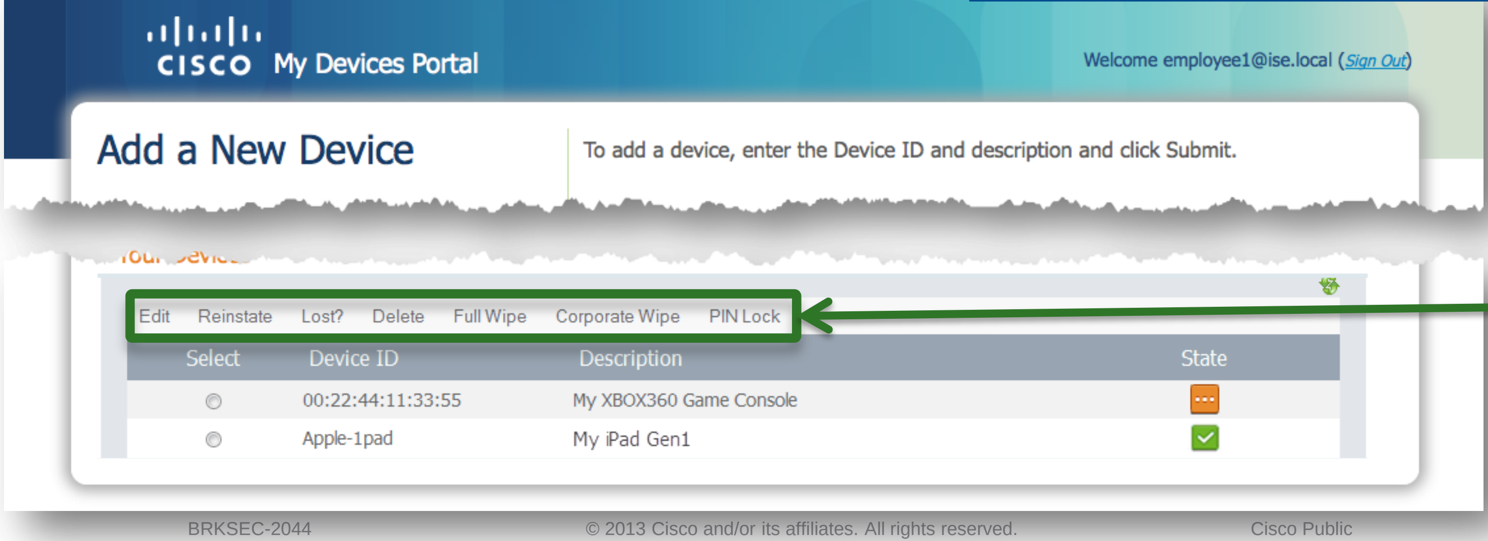
Remediation

- Administrator / user can issue remote actions on the device through MDM server (Example: remote wiping the device)
  - My Devices Portal
  - ISE Endpoints Directory



Endpoints

	Endpoint Profile	MAC
□	Android	F4:6
□	Android	00:2
□	Android	00:23:76:95:86:93
□	Android	00:18:A4:06:71:4F



Welcome employee1@ise.local (Sign Out)

Add a New Device

To add a device, enter the Device ID and description and click Submit.

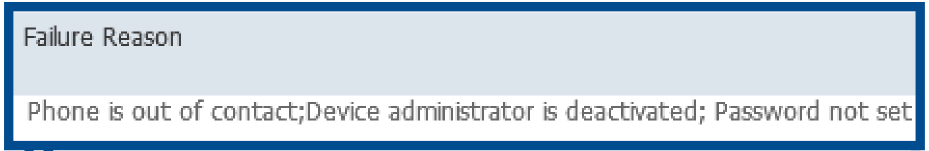
Select	Device ID	Description	State
○	00:22:44:11:33:55	My XBOX360 Game Console	⋯
○	Apple-1pad	My iPad Gen1	✓

Options

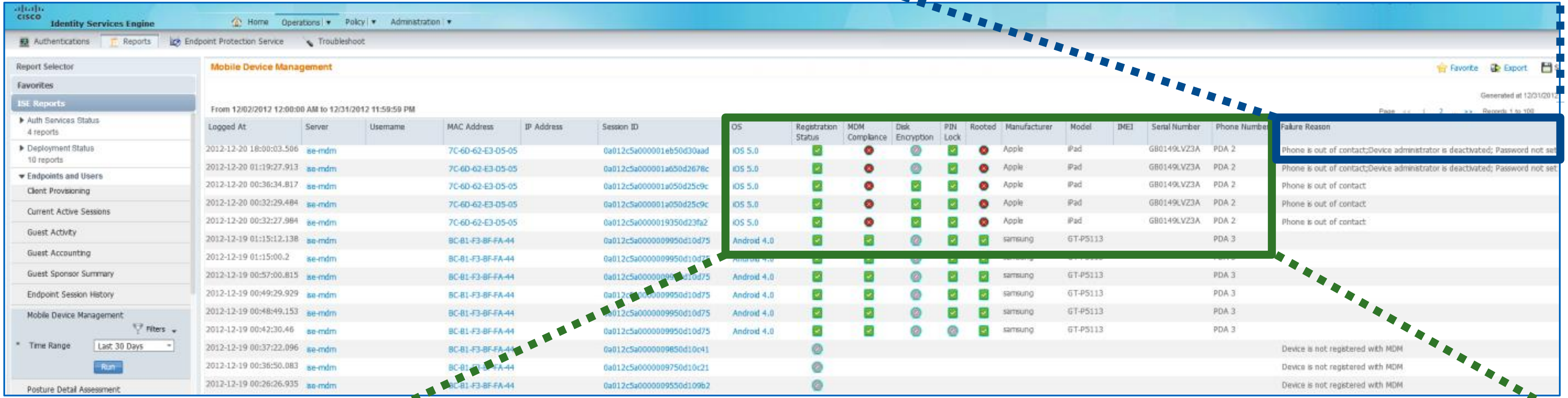
- Edit
- Reinstate
- Lost?
- Delete
- Full Wipe
- Corporate Wipe
- PIN Lock

Reporting

Mobile Device Management Report



Failure Reason
Phone is out of contact;Device administrator is deactivated; Password not set

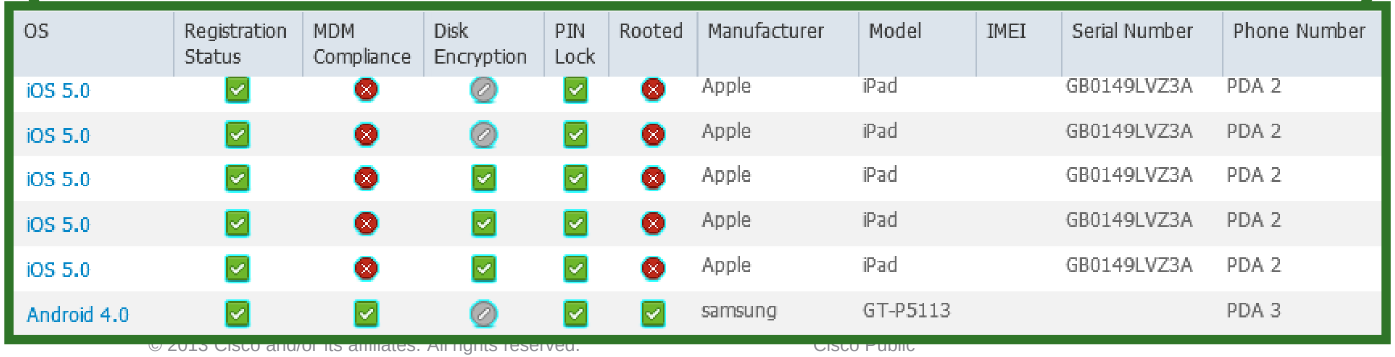


Mobile Device Management

Generated at 12/31/2012

From 12/02/2012 12:00:00 AM to 12/31/2012 11:59:59 PM

Logged At	Server	Username	MAC Address	IP Address	Session ID	OS	Registration Status	MDM Compliance	Disk Encryption	PIN Lock	Rooted	Manufacturer	Model	IMEI	Serial Number	Phone Number	Failure Reason
2012-12-20 18:00:03.506	ise-mdm		7C-6D-62-E3-D5-05		0a012c5a000001eb50d30aad	iOS 5.0	✓	✗	⊘	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact;Device administrator is deactivated; Password not set
2012-12-20 01:19:27.913	ise-mdm		7C-6D-62-E3-D5-05		0a012c5a000001a650d2678c	iOS 5.0	✓	✗	⊘	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact;Device administrator is deactivated; Password not set
2012-12-20 00:36:34.817	ise-mdm		7C-6D-62-E3-D5-05		0a012c5a000001a050d25c9c	iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-20 00:32:29.484	ise-mdm		7C-6D-62-E3-D5-05		0a012c5a000001a050d25c9c	iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-20 00:32:27.984	ise-mdm		7C-6D-62-E3-D5-05		0a012c5a0000019350d23fa2	iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-19 01:15:12.138	ise-mdm		BC-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	⊘	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 01:15:00.2	ise-mdm		BC-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	⊘	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:57:00.815	ise-mdm		BC-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	⊘	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:49:29.929	ise-mdm		BC-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	⊘	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:48:49.153	ise-mdm		BC-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	⊘	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:42:30.46	ise-mdm		BC-B1-F3-8F-FA-44		0a012c5a0000009950d10d75	Android 4.0	✓	✓	⊘	⊘	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:37:22.096	ise-mdm		BC-B1-F3-8F-FA-44		0a012c5a0000009850d10c41		⊘										Device is not registered with MDM
2012-12-19 00:36:50.083	ise-mdm		BC-B1-F3-8F-FA-44		0a012c5a0000009750d10c21		⊘										Device is not registered with MDM
2012-12-19 00:26:26.935	ise-mdm		BC-B1-F3-8F-FA-44		0a012c5a0000009550d109b2		⊘										Device is not registered with MDM

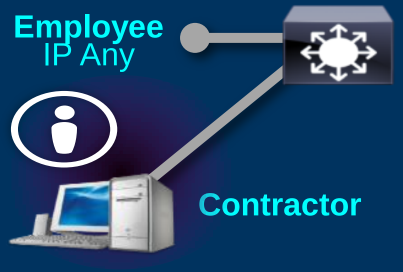


OS	Registration Status	MDM Compliance	Disk Encryption	PIN Lock	Rooted	Manufacturer	Model	IMEI	Serial Number	Phone Number
iOS 5.0	✓	✗	⊘	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	⊘	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
iOS 5.0	✓	✗	✓	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2
Android 4.0	✓	✓	⊘	✓	✓	samsung	GT-P5113			PDA 3

TrustSec and Pervasive Policy Enforcement

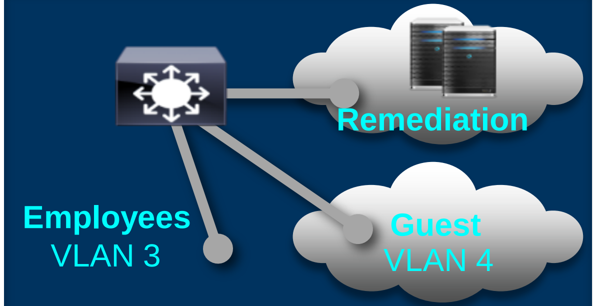
TrustSec Authorisation and Enforcement

dACL or Named ACL



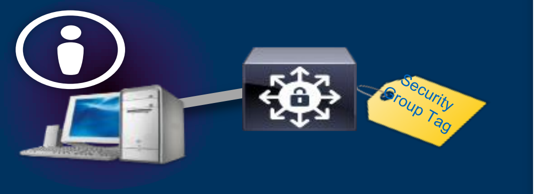
- Less disruptive to endpoint (no IP address change required)
- Improved user experience
- Increased ACL management

VLANS



- Does not require switch port ACL management
- Preferred choice for path isolation
- Requires VLAN proliferation and IP refresh

Security Group Access

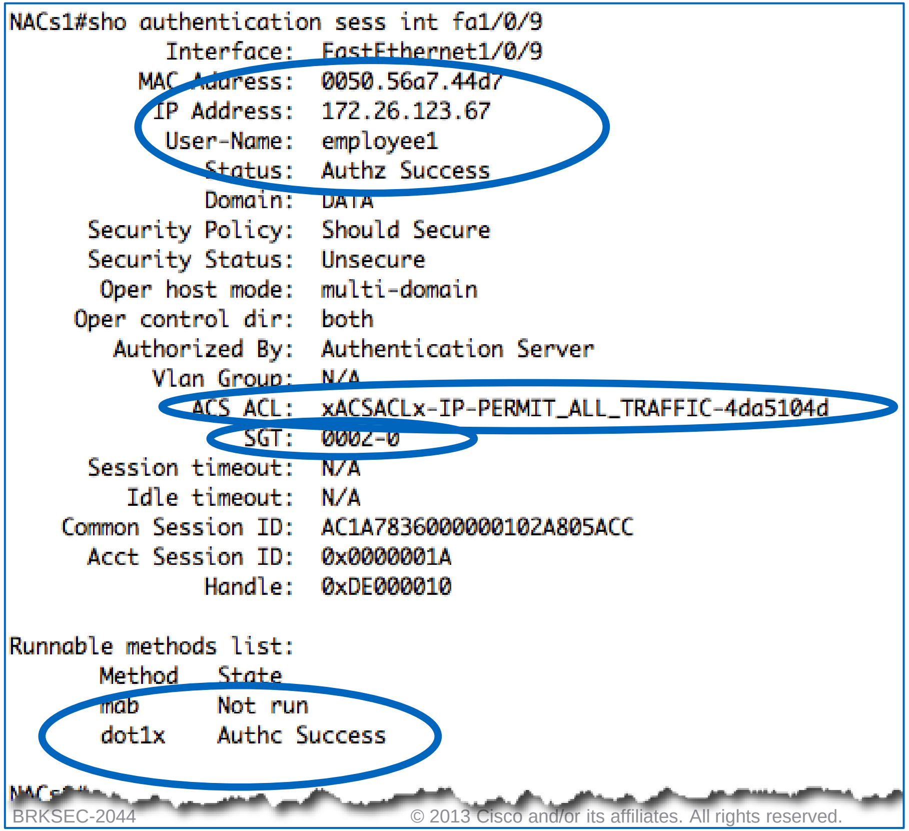


Security Group Access—SXP, SGT, SGACL, SGFW

- Simplifies ACL management
- Uniformly enforces policy independent of topology
- Fine-grained access control

A Systems Approach

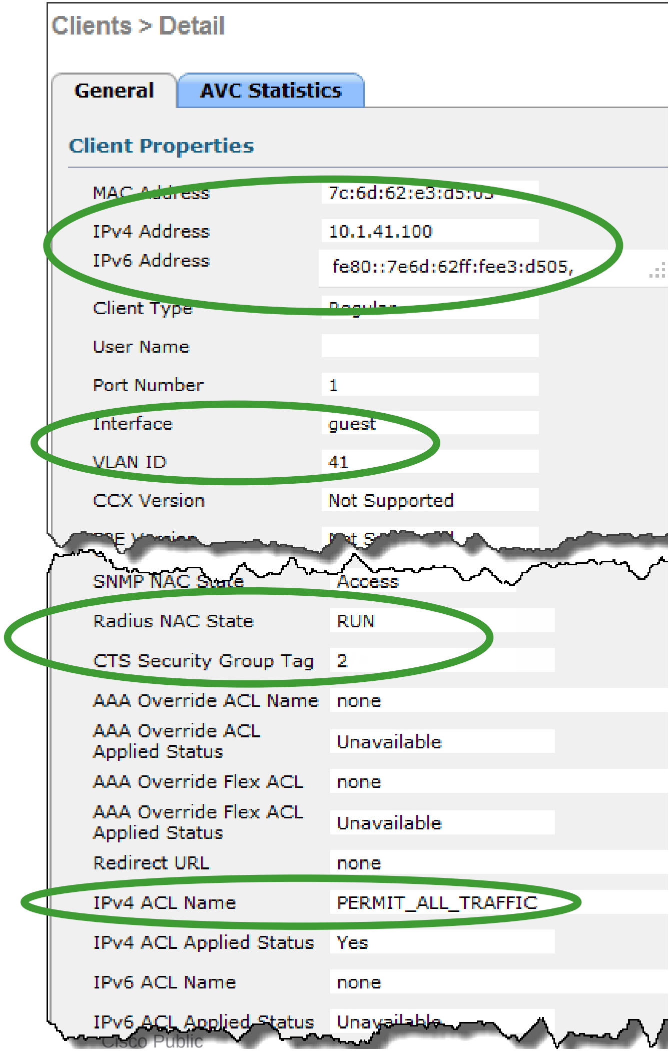
Switch/Controller is the Enforcement Point



```
NACs1#sho authentication sess int fa1/0/9
            Interface:  FastEthernet1/0/9
          MAC Address:  0050.56a7.44d7
           IP Address:  172.26.123.67
            User-Name:  employee1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4da5104d
                  SGT:  0002-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  AC1A7836000000102A805ACC
      Acct Session ID:  0x0000001A
               Handle:  0xDE000010

Runnable methods list:
       Method   State
       mab      Not run
       dot1x    Authc Success

NACs1#
```



Clients > Detail

Client Properties

MAC Address	7c:6d:62:e3:d5:05
IPv4 Address	10.1.41.100
IPv6 Address	fe80::7e6d:62ff:fee3:d505,
Client Type	Regular
User Name	
Port Number	1
Interface	guest
VLAN ID	41
CCX Version	Not Supported
E2E Version	Not Supported
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	2
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	PERMIT_ALL_TRAFFIC
IPv4 ACL Applied Status	Yes
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable

What is Secure Group Access?

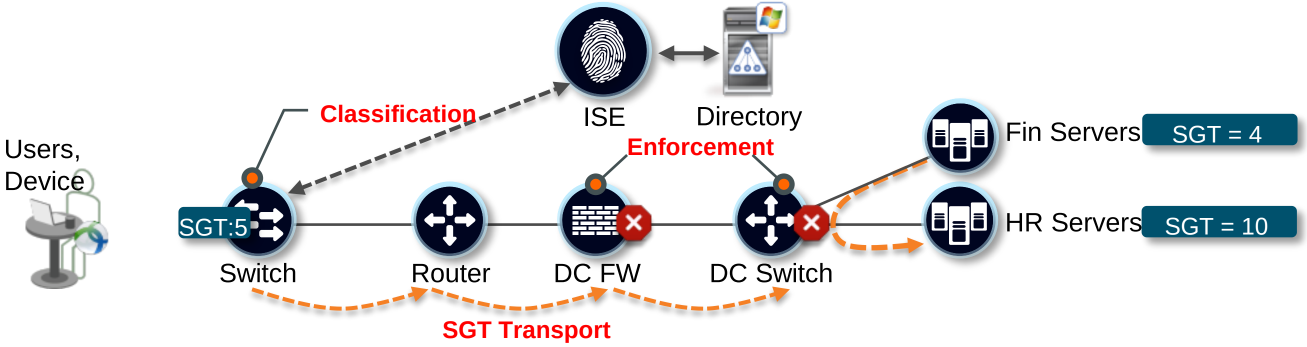
SGA is a Part of TrustSec

- Next-Generation Access Control Enforcement
  - Removes concern TCAM Space for detailed Ingress ACLs
  - Removes concern of ACE explosion on DC Firewalls
- Assign a TAG at login → Enforce that tag in the network or Data Centre.

BRKSEC-2690 – Deploying Security Group Tags

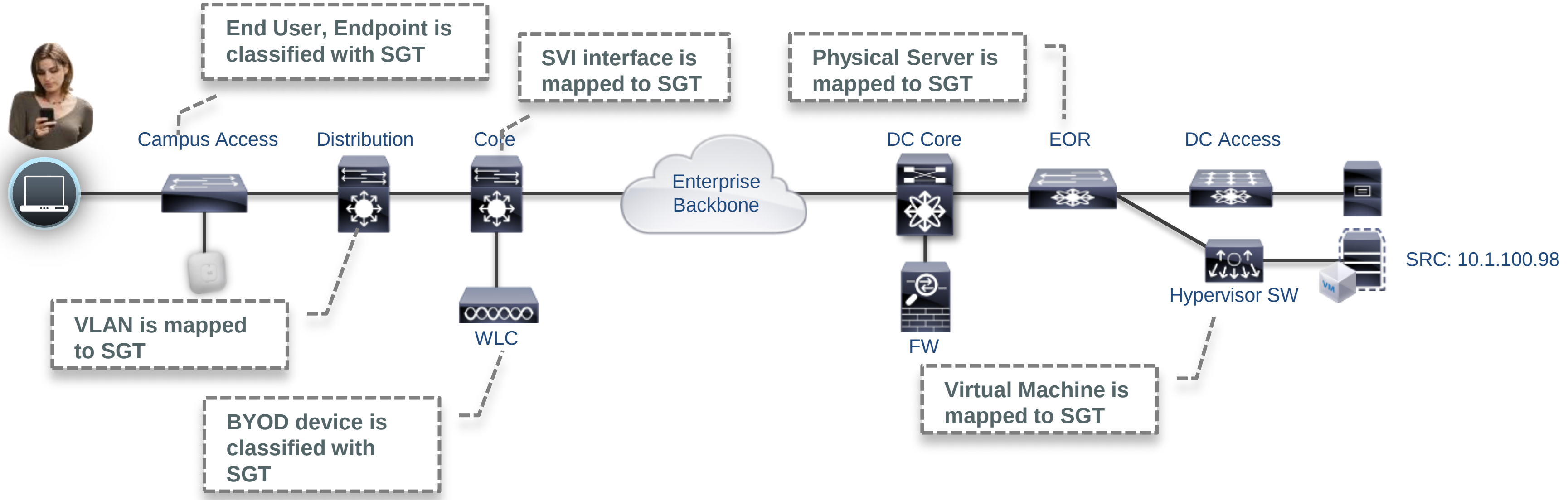
BRKSEC-3690 – Advanced Security Group Tags: The Detailed Walk Through

SGA Overview



- **Classification** of systems/users based on **context** (ex: user role, device, location, access method)
- TrustSec allows context info from ISE to be shared between switches, routers, WLCs and firewalls to make real-time decisions
- Allows forwarding, filtering or inspection decisions to be based upon intelligent tags
- Tags can be applied to individual users, servers, networks or network connections
- Provides virtual network segmentation, flexible access control and FW rule automation

SGT Assignments



End User, Endpoint is classified with SGT

SVI interface is mapped to SGT

Physical Server is mapped to SGT

VLAN is mapped to SGT

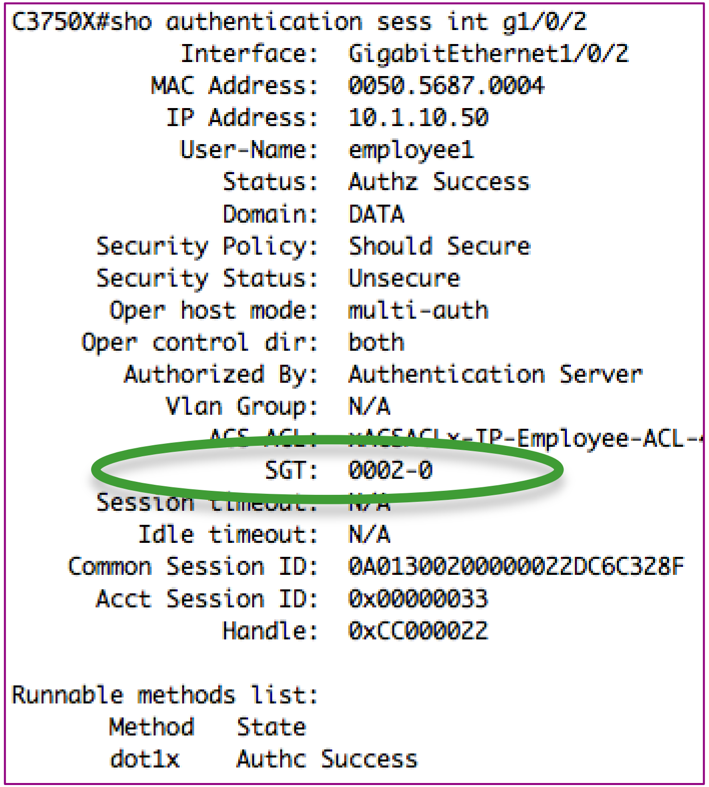
BYOD device is classified with SGT

Virtual Machine is mapped to SGT

SGT Assigned Via ISE Authorisation Example

SGT Assignment Process:

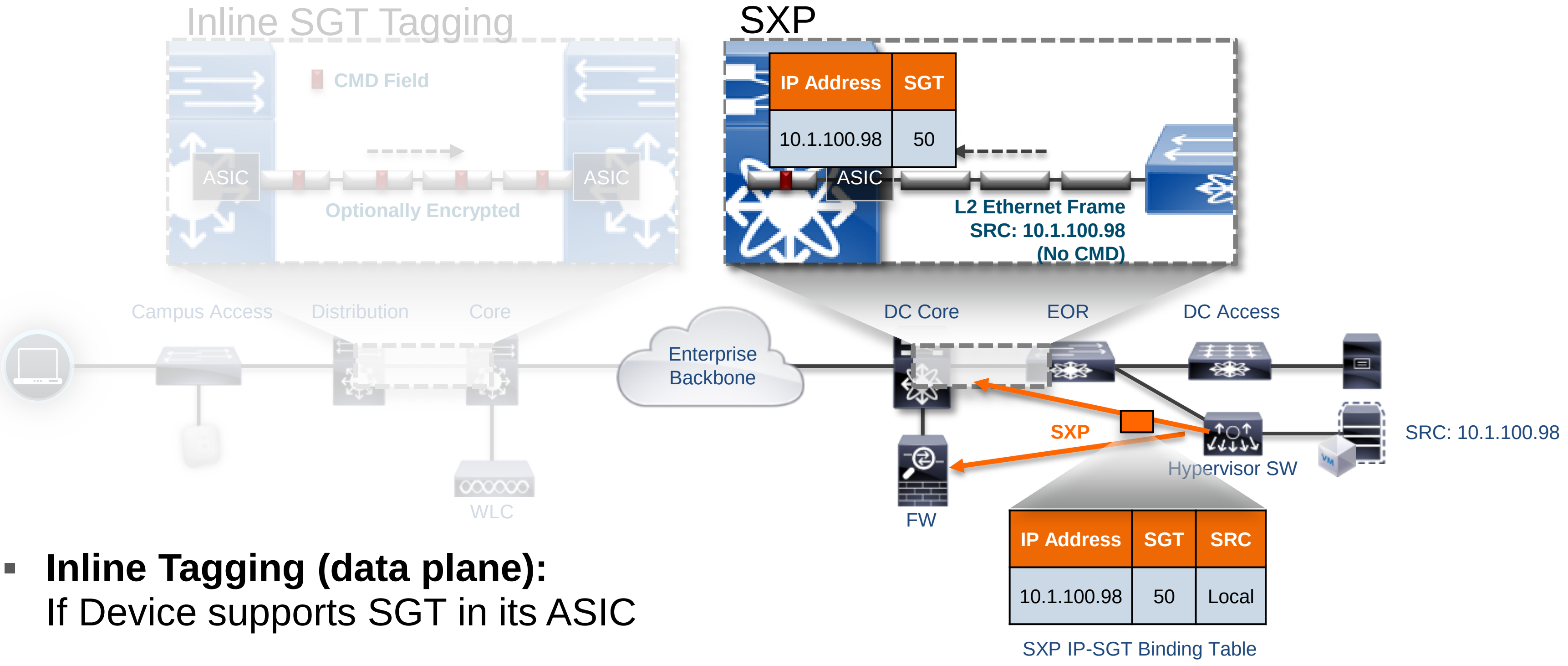
1. A user (or device) logs into network via 802.1X
2. ISE is configured to send a TAG in the Authorisation Result – based on the “ROLE” of the user/device
3. The Switch/Controller applies this TAG to the users traffic.



```
C3750X#sho authentication sess int g1/0/2
            Interface:  GigabitEthernet1/0/2
          MAC Address:  0050.5687.0004
           IP Address:  10.1.10.50
            User-Name:  employee1
               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-Employee-ACL-4
                  SGT:  0002-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A01300200000022DC6C328F
      Acct Session ID:  0x00000033
               Handle:  0xCC000022

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

How is the SGT Classification Shared?



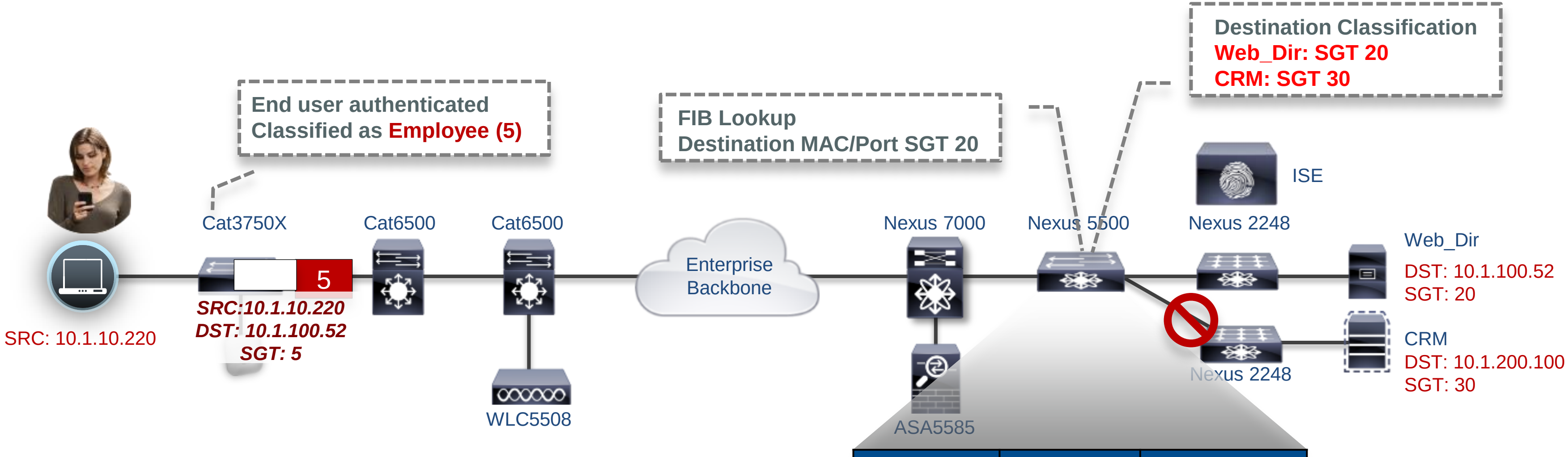
IP Address	SGT
10.1.100.98	50

IP Address	SGT	SRC
10.1.100.98	50	Local

SXP IP-SGT Binding Table

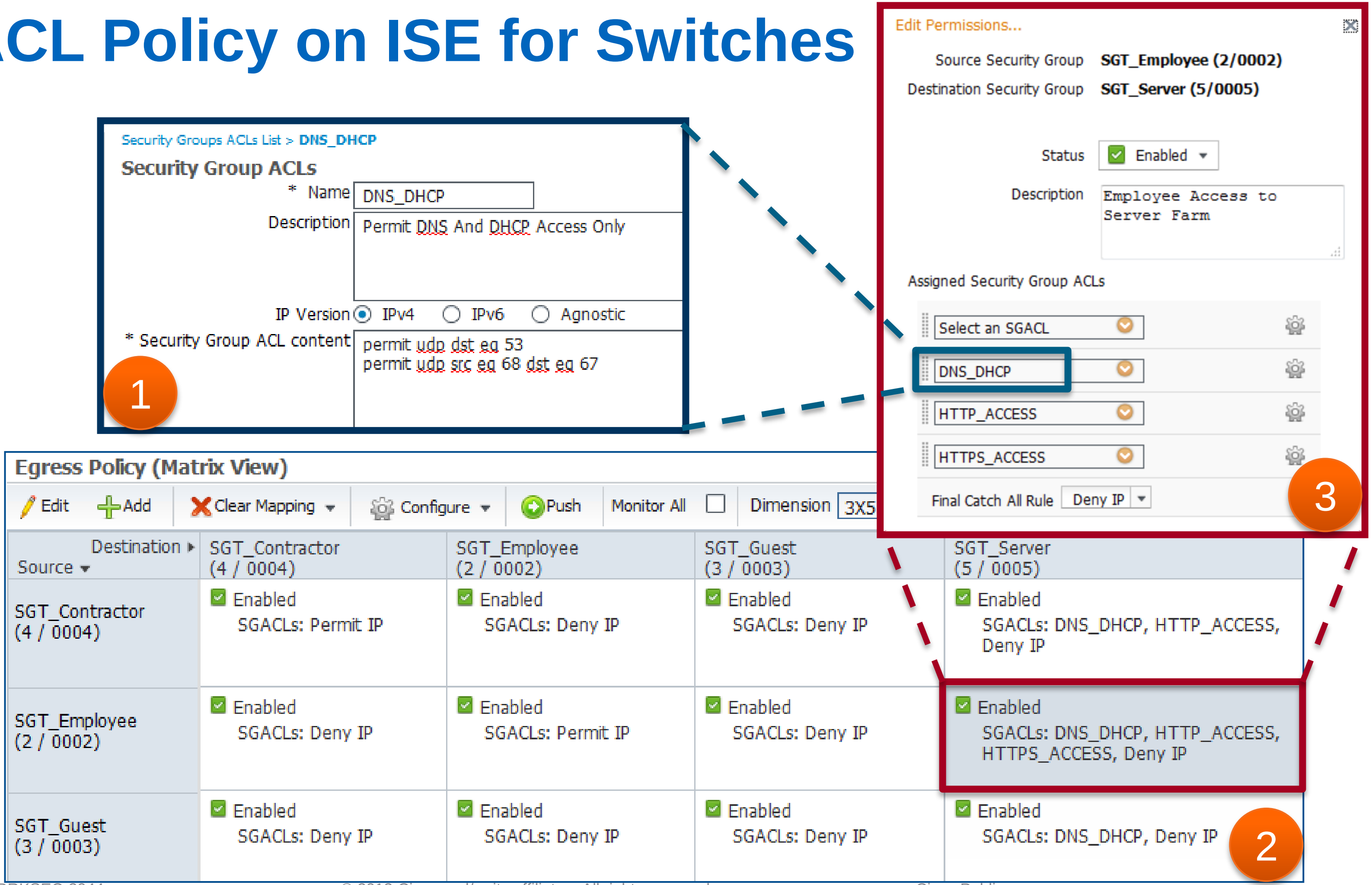
- **Inline Tagging (data plane):**
  If Device supports SGT in its ASIC
- **SXP (control plane):** Shared between devices that do not have SGT-capable hardware

How is Policy Enforced with SGACL



SRC\DST	Web_Dir (20)	CRM (30)
Employee (5)	SGACL-A	SGACL-B
BYOD (7)	Deny	Deny

SGACL Policy on ISE for Switches



Security Groups ACLs List > **DNS_DHCP**

Security Group ACLs

* Name	DNS_DHCP
Description	Permit DNS And DHCP Access Only
IP Version	● IPv4 ○ IPv6 ○ Agnostic
* Security Group ACL content	permit udp dst eq 53 permit udp src eq 68 dst eq 67

1

Egress Policy (Matrix View)

Destination ▸ Source ▾	SGT_Contractor (4 / 0004)	SGT_Employee (2 / 0002)	SGT_Guest (3 / 0003)	SGT_Server (5 / 0005)
SGT_Contractor (4 / 0004)	☑ Enabled SGACLs: Permit IP	☑ Enabled SGACLs: Deny IP	☑ Enabled SGACLs: Deny IP	☑ Enabled SGACLs: DNS_DHCP, HTTP_ACCESS, Deny IP
SGT_Employee (2 / 0002)	☑ Enabled SGACLs: Deny IP	☑ Enabled SGACLs: Permit IP	☑ Enabled SGACLs: Deny IP	☑ Enabled SGACLs: DNS_DHCP, HTTP_ACCESS, HTTPS_ACCESS, Deny IP
SGT_Guest (3 / 0003)	☑ Enabled SGACLs: Deny IP	☑ Enabled SGACLs: Deny IP	☑ Enabled SGACLs: Deny IP	☑ Enabled SGACLs: DNS_DHCP, Deny IP

2

Edit Permissions...

Source Security Group	**SGT_Employee (2/0002)**
Destination Security Group	**SGT_Server (5/0005)**
Status	☑ Enabled ▾
Description	Employee Access to Server Farm

Assigned Security Group ACLs

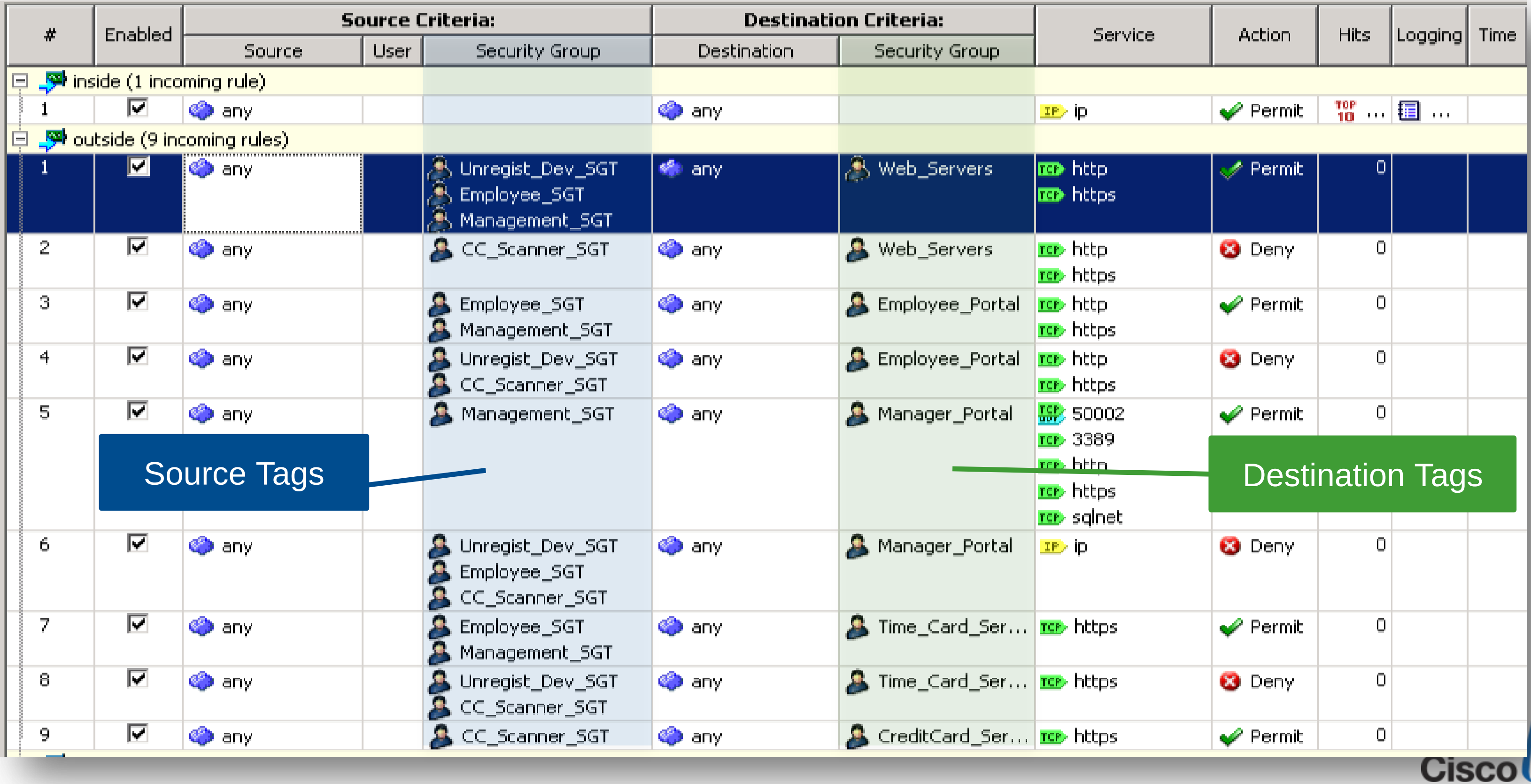
- Select an SGACL
- DNS_DHCP
- HTTP_ACCESS
- HTTPS_ACCESS

Final Catch All Rule: Deny IP ▾

3

Security Group Based Access Control for Firewalls

Security Group Firewall (SGFW)



#	Enabled	Source Criteria:			Destination Criteria:		Service	Action	Hits	Logging	Time
		Source	User	Security Group	Destination	Security Group					
⊟ inside (1 incoming rule)											
1	☑	any			any		ip	✓ Permit	TOP 10 …	…	
⊟ outside (9 incoming rules)											
1	☑	any		Unregist_Dev_SGT Employee_SGT Management_SGT	any	Web_Servers	http https	✓ Permit	0		
2	☑	any		CC_Scanner_SGT	any	Web_Servers	http https	☒ Deny	0		
3	☑	any		Employee_SGT Management_SGT	any	Employee_Portal	http https	✓ Permit	0		
4	☑	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Employee_Portal	http https	☒ Deny	0		
5	☑	any		Management_SGT	any	Manager_Portal	50002 3389 http https sqlnet	✓ Permit	0		
6	☑	any		Unregist_Dev_SGT Employee_SGT CC_Scanner_SGT	any	Manager_Portal	ip	☒ Deny	0		
7	☑	any		Employee_SGT Management_SGT	any	Time_Card_Ser…	https	✓ Permit	0		
8	☑	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Time_Card_Ser…	https	☒ Deny	0		
9	☑	any		CC_Scanner_SGT	any	CreditCard_Ser…	https	✓ Permit	0		

Source Tags

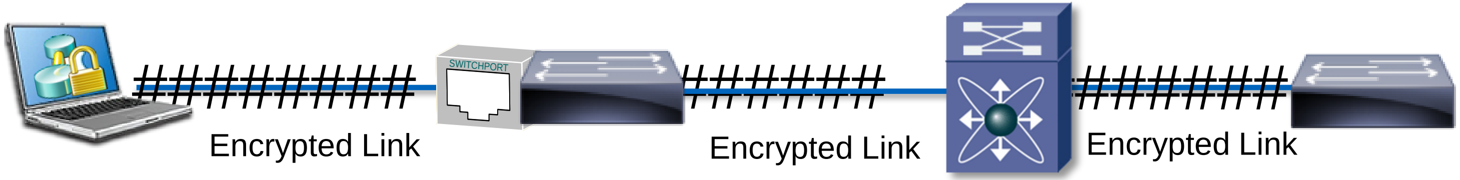
Destination Tags

MACsec and NDAC

Media Access Control Security and Network Device Admission Control

- MACsec: Layer-2 Encryption (802.1AE)
  - Industry Standard Extension to 802.1X
  - Encrypts the links between host and switch and links between switches.
  - Traffic in the backplane is unencrypted for inspection, etc.
  - Client requires a supplicant that supports MACsec and the encryption key-exchange

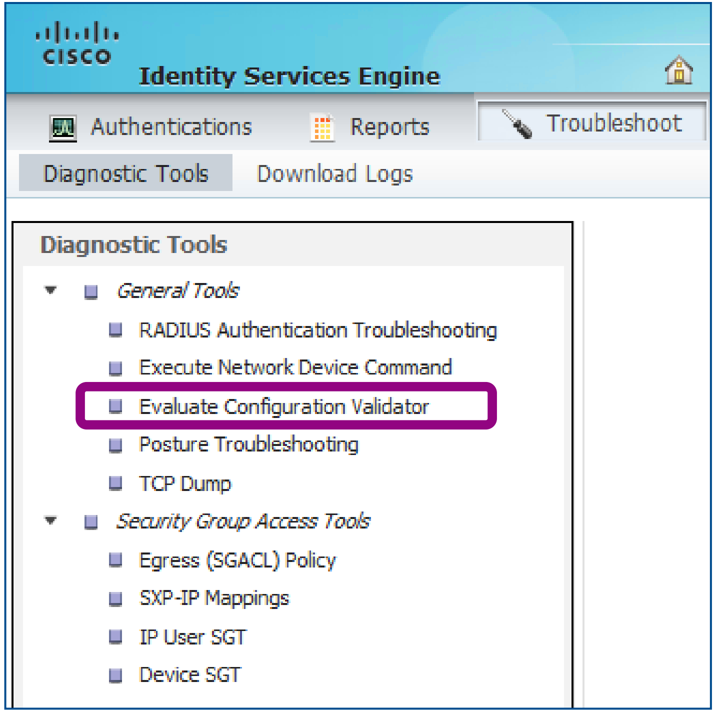
- NDAC: Authenticate and Authorise switches entering the network
  - Only honors SGTs from Trusted Peers
  - Can retrieve policies from the ACS/ISE Server and "proxy" the trust to other devices.

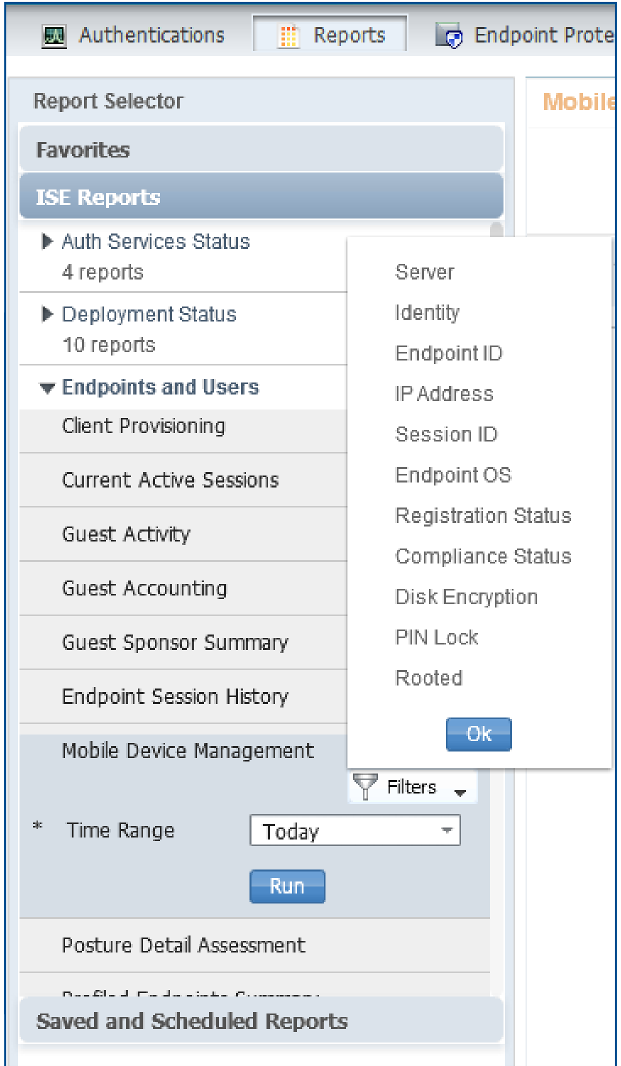


For more on MACsec: BRKSEC-2690 – Deploying Security Group Tags

Management Ecosystem

Troubleshooting and Reporting

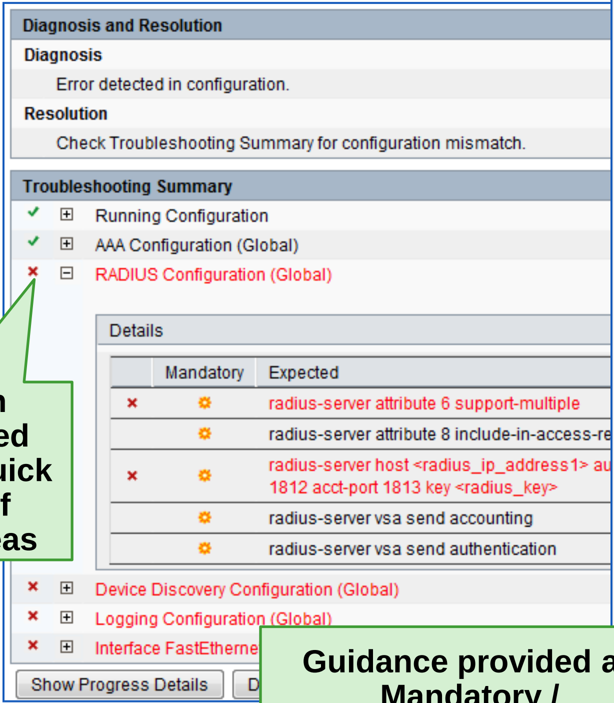




Integrated Troubleshooting

Network Device Configuration Audit

Are my switchports properly configured to support 802.1X, MAB, and Web Authentication per Cisco best practices?



Diagnosis and Resolution

Diagnosis

Error detected in configuration.

Resolution

Check Troubleshooting Summary for configuration mismatch.

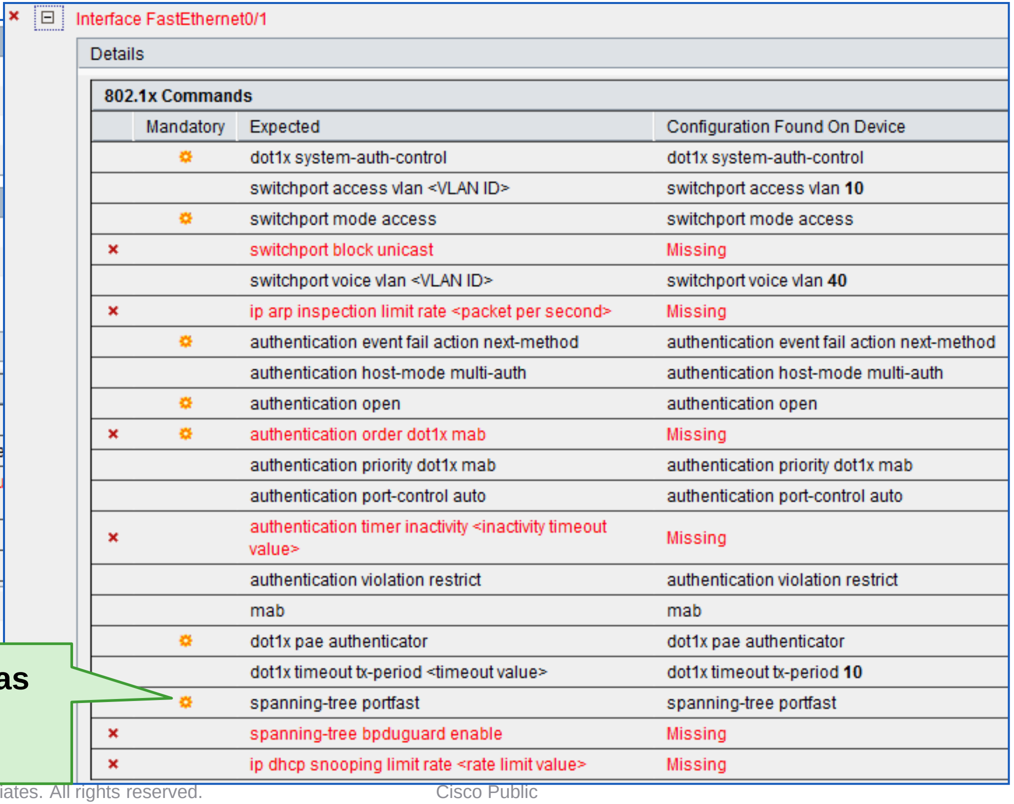
Troubleshooting Summary

- ✓ ⊞ Running Configuration
- ✓ ⊞ AAA Configuration (Global)
- ✗ ⊟ RADIUS Configuration (Global)

Details

	Mandatory	Expected
✗	✸	radius-server attribute 6 support-multiple
	✸	radius-server attribute 8 include-in-access-re
✗	✸	radius-server host <radius_ip_address1> au 1812 acct-port 1813 key <radius_key>
	✸	radius-server vsa send accounting
	✸	radius-server vsa send authentication

- ✗ ⊞ Device Discovery Configuration (Global)
- ✗ ⊞ Logging Configuration (Global)
- ✗ ⊞ Interface FastEthernet



✗ ⊟ Interface FastEthernet0/1

Details

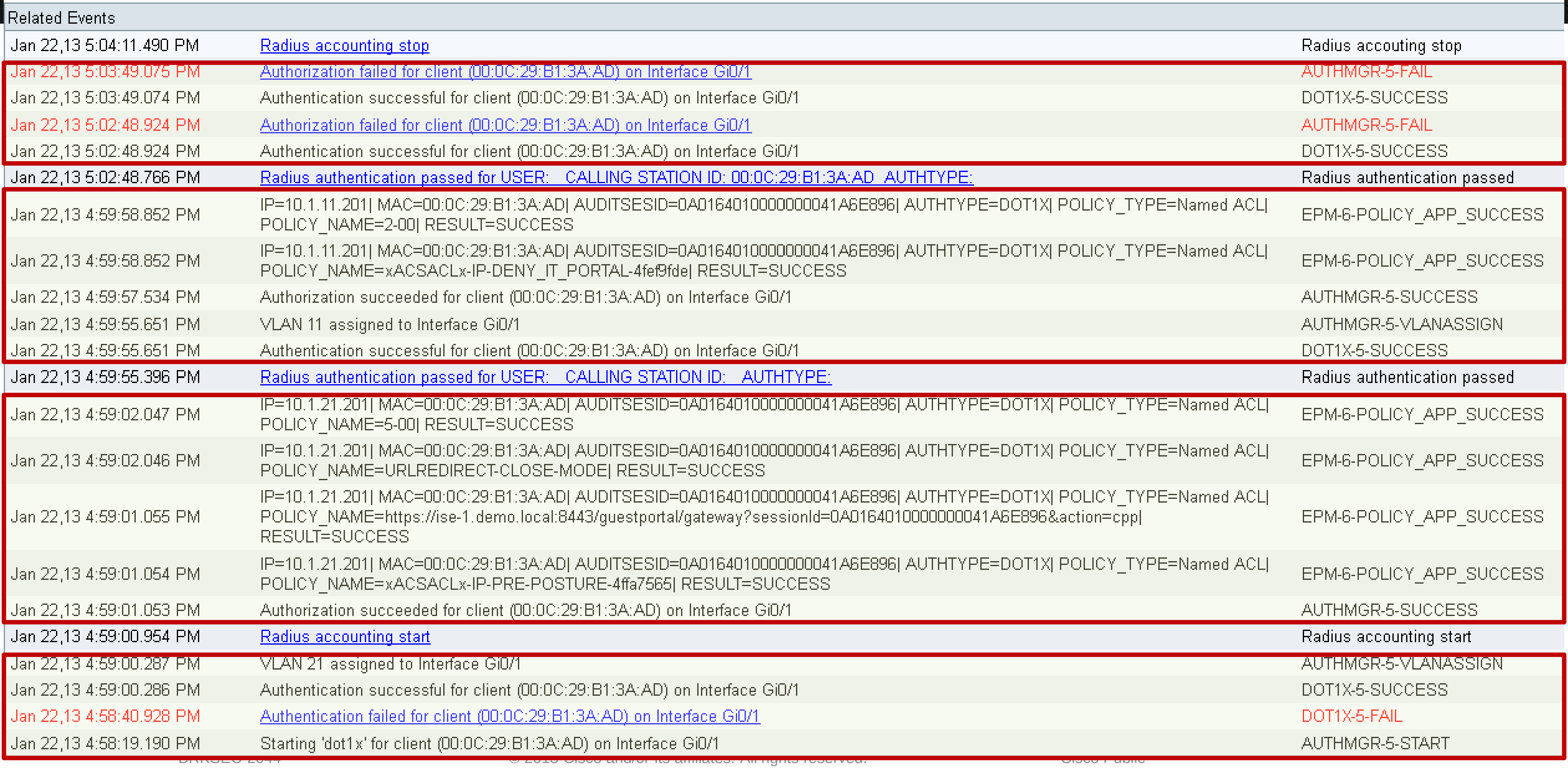
802.1x Commands

	Mandatory	Expected	Configuration Found On Device
	✸	dot1x system-auth-control	dot1x system-auth-control
		switchport access vlan <VLAN ID>	switchport access vlan **10**
	✸	switchport mode access	switchport mode access
✗		switchport block unicast	Missing
		switchport voice vlan <VLAN ID>	switchport voice vlan **40**
✗		ip arp inspection limit rate <packet per second>	Missing
	✸	authentication event fail action next-method	authentication event fail action next-method
		authentication host-mode multi-auth	authentication host-mode multi-auth
	✸	authentication open	authentication open
✗	✸	authentication order dot1x mab	Missing
		authentication priority dot1x mab	authentication priority dot1x mab
		authentication port-control auto	authentication port-control auto
✗		authentication timer inactivity <inactivity timeout value>	Missing
		authentication violation restrict	authentication violation restrict
		mab	mab
	✸	dot1x pae authenticator	dot1x pae authenticator
		dot1x timeout tx-period <timeout value>	dot1x timeout tx-period **10**
	✸	spanning-tree portfast	spanning-tree portfast
✗		spanning-tree bpduguard enable	Missing
✗		ip dhcp snooping limit rate <rate limit value>	Missing

Icons with colour-coded entries for quick analysis of problem areas

Guidance provided as Mandatory / Recommended

Network Device Logs Contribute to ISE Troubleshooting



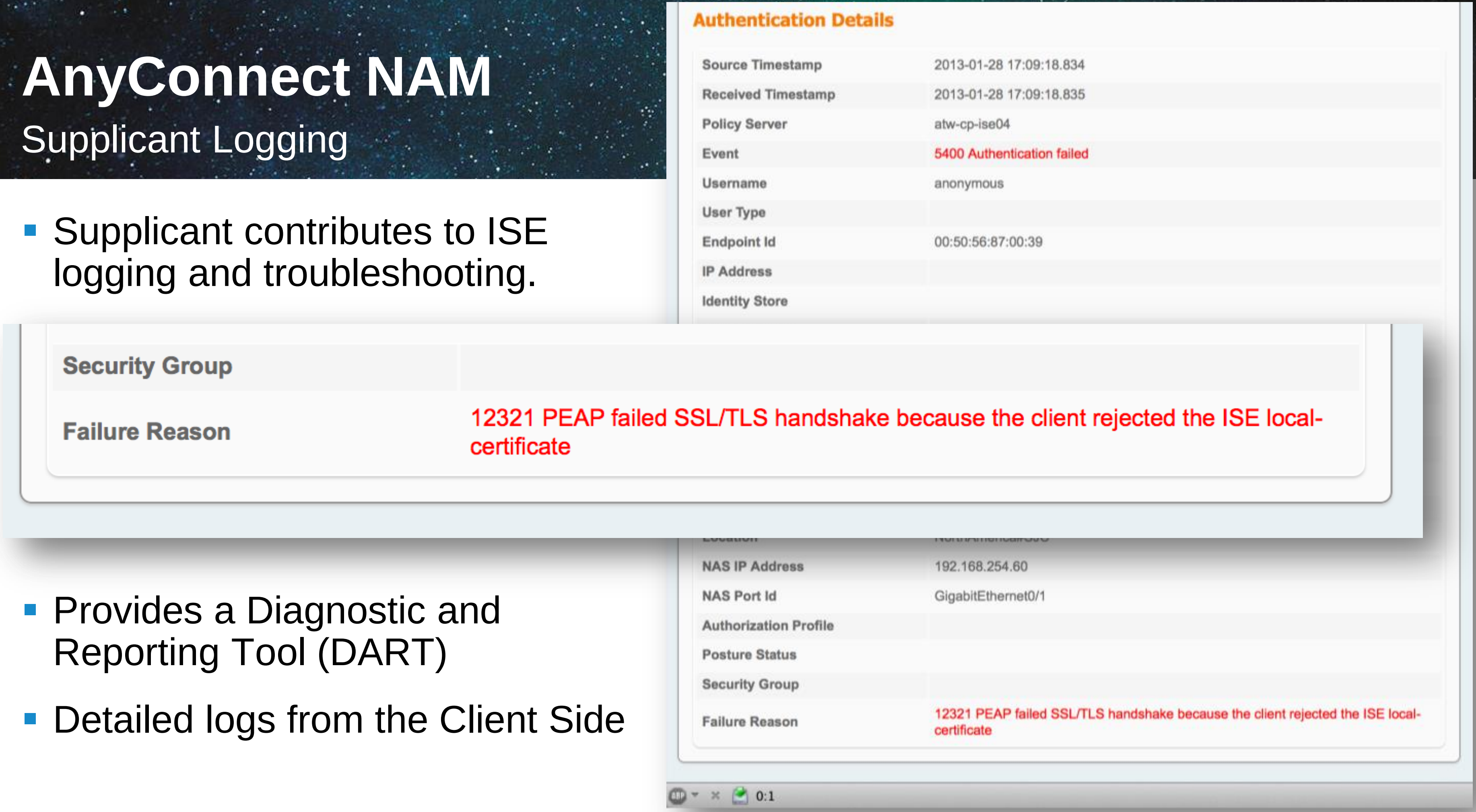
Related Events

Jan 22,13 5:04:11.490 PM	Radius accounting stop	Radius accouting stop
Jan 22,13 5:03:49.075 PM	Authorization failed for client (00:0C:29:B1:3A:AD) on Interface Gi0/1	AUTHMGR-5-FAIL
Jan 22,13 5:03:49.074 PM	Authentication successful for client (00:0C:29:B1:3A:AD) on Interface Gi0/1	DOT1X-5-SUCCESS
Jan 22,13 5:02:48.924 PM	Authorization failed for client (00:0C:29:B1:3A:AD) on Interface Gi0/1	AUTHMGR-5-FAIL
Jan 22,13 5:02:48.924 PM	Authentication successful for client (00:0C:29:B1:3A:AD) on Interface Gi0/1	DOT1X-5-SUCCESS
Jan 22,13 5:02:48.766 PM	Radius authentication passed for USER: CALLING STATION ID: 00:0C:29:B1:3A:AD AUTHTYPE:	Radius authentication passed
Jan 22,13 4:59:58.852 PM	IP=10.1.11.201| MAC=00:0C:29:B1:3A:AD| AUDITSESID=0A0164010000000041A6E896| AUTHTYPE=DOT1X| POLICY_TYPE=Named ACL| POLICY_NAME=2-00| RESULT=SUCCESS	EPM-6-POLICY_APP_SUCCESS
Jan 22,13 4:59:58.852 PM	IP=10.1.11.201| MAC=00:0C:29:B1:3A:AD| AUDITSESID=0A0164010000000041A6E896| AUTHTYPE=DOT1X| POLICY_TYPE=Named ACL| POLICY_NAME=xACSACLx-IP-DENY_IT_PORTAL-4fef9fde| RESULT=SUCCESS	EPM-6-POLICY_APP_SUCCESS
Jan 22,13 4:59:57.534 PM	Authorization succeeded for client (00:0C:29:B1:3A:AD) on Interface Gi0/1	AUTHMGR-5-SUCCESS
Jan 22,13 4:59:55.651 PM	VLAN 11 assigned to Interface Gi0/1	AUTHMGR-5-VLANASSIGN
Jan 22,13 4:59:55.651 PM	Authentication successful for client (00:0C:29:B1:3A:AD) on Interface Gi0/1	DOT1X-5-SUCCESS
Jan 22,13 4:59:55.396 PM	Radius authentication passed for USER: CALLING STATION ID: AUTHTYPE:	Radius authentication passed
Jan 22,13 4:59:02.047 PM	IP=10.1.21.201| MAC=00:0C:29:B1:3A:AD| AUDITSESID=0A0164010000000041A6E896| AUTHTYPE=DOT1X| POLICY_TYPE=Named ACL| POLICY_NAME=5-00| RESULT=SUCCESS	EPM-6-POLICY_APP_SUCCESS
Jan 22,13 4:59:02.046 PM	IP=10.1.21.201| MAC=00:0C:29:B1:3A:AD| AUDITSESID=0A0164010000000041A6E896| AUTHTYPE=DOT1X| POLICY_TYPE=Named ACL| POLICY_NAME=URLREDIRECT-CLOSE-MODE| RESULT=SUCCESS	EPM-6-POLICY_APP_SUCCESS
Jan 22,13 4:59:01.055 PM	IP=10.1.21.201| MAC=00:0C:29:B1:3A:AD| AUDITSESID=0A0164010000000041A6E896| AUTHTYPE=DOT1X| POLICY_TYPE=Named ACL| POLICY_NAME=https://ise-1.demo.local:8443/guestportal/gateway?sessionId=0A0164010000000041A6E896&action=cpp| RESULT=SUCCESS	EPM-6-POLICY_APP_SUCCESS
Jan 22,13 4:59:01.054 PM	IP=10.1.21.201| MAC=00:0C:29:B1:3A:AD| AUDITSESID=0A0164010000000041A6E896| AUTHTYPE=DOT1X| POLICY_TYPE=Named ACL| POLICY_NAME=xACSACLx-IP-PRE-POSTURE-4ffa7565| RESULT=SUCCESS	EPM-6-POLICY_APP_SUCCESS
Jan 22,13 4:59:01.053 PM	Authorization succeeded for client (00:0C:29:B1:3A:AD) on Interface Gi0/1	AUTHMGR-5-SUCCESS
Jan 22,13 4:59:00.954 PM	Radius accounting start	Radius accounting start
Jan 22,13 4:59:00.287 PM	VLAN 21 assigned to Interface Gi0/1	AUTHMGR-5-VLANASSIGN
Jan 22,13 4:59:00.286 PM	Authentication successful for client (00:0C:29:B1:3A:AD) on Interface Gi0/1	DOT1X-5-SUCCESS
Jan 22,13 4:58:40.928 PM	Authentication failed for client (00:0C:29:B1:3A:AD) on Interface Gi0/1	DOT1X-5-FAIL
Jan 22,13 4:58:19.190 PM	Starting 'dot1x' for client (00:0C:29:B1:3A:AD) on Interface Gi0/1	AUTHMGR-5-START

AnyConnect NAM

Supplicant Logging

- Supplicant contributes to ISE logging and troubleshooting.
- Provides a Diagnostic and Reporting Tool (DART)
- Detailed logs from the Client Side

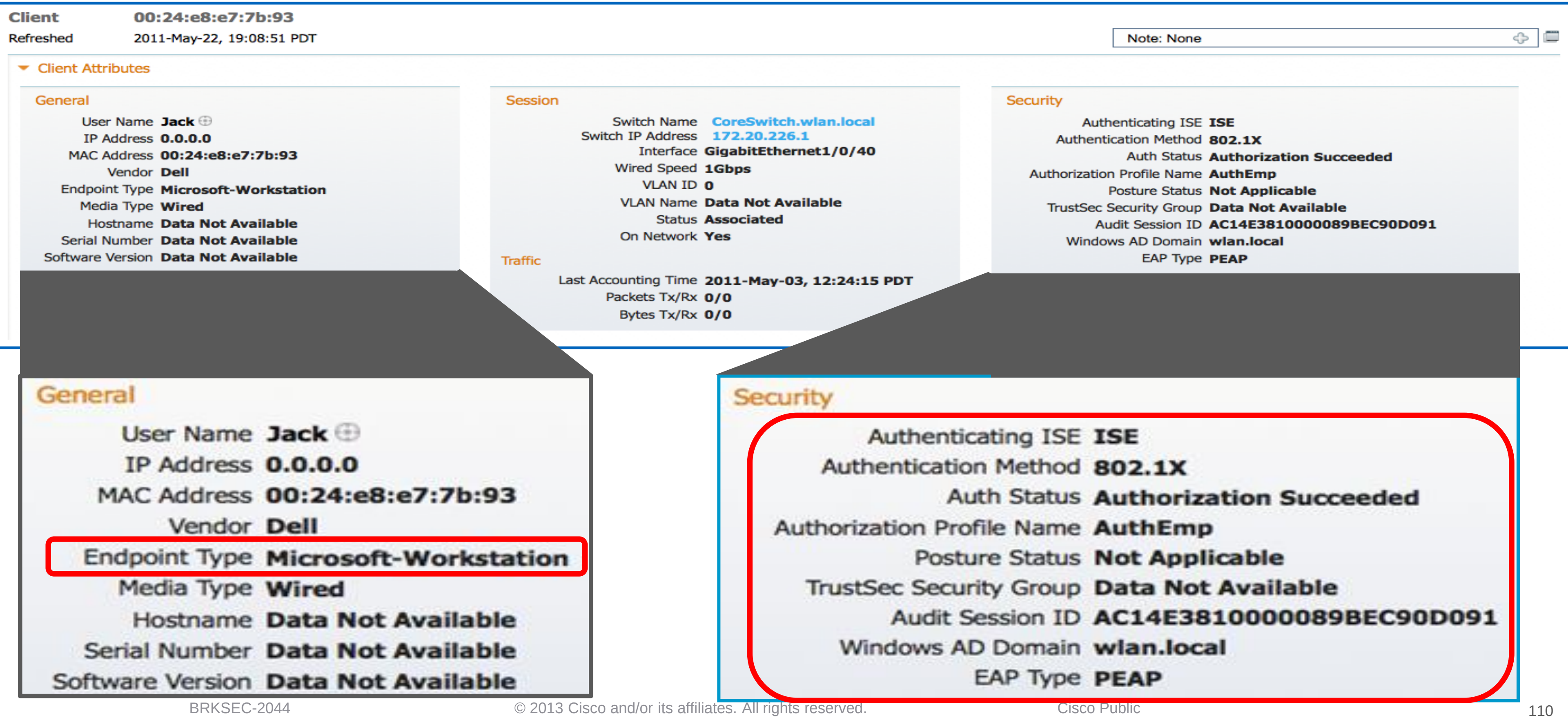


Authentication Details

Source Timestamp	2013-01-28 17:09:18.834
Received Timestamp	2013-01-28 17:09:18.835
Policy Server	atw-cp-ise04
Event	5400 Authentication failed
Username	anonymous
User Type	
Endpoint Id	00:50:56:87:00:39
IP Address	
Identity Store	
NAS IP Address	192.168.254.60
NAS Port Id	GigabitEthernet0/1
Authorization Profile	
Posture Status	
Security Group	
Failure Reason	12321 PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

Security Group	
Failure Reason	12321 PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

NCS + ISE: Client Profile and Posture



Client 00:24:e8:e7:7b:93

Refreshed 2011-May-22, 19:08:51 PDT

Note: None

Client Attributes

General

User Name	Jack
IP Address	0.0.0.0
MAC Address	00:24:e8:e7:7b:93
Vendor	Dell
Endpoint Type	Microsoft-Workstation
Media Type	Wired
Hostname	Data Not Available
Serial Number	Data Not Available
Software Version	Data Not Available

Session

Switch Name	CoreSwitch.wlan.local
Switch IP Address	172.20.226.1
Interface	GigabitEthernet1/0/40
Wired Speed	1Gbps
VLAN ID	0
VLAN Name	Data Not Available
Status	Associated
On Network	Yes

Traffic

Last Accounting Time	2011-May-03, 12:24:15 PDT
Packets Tx/Rx	0/0
Bytes Tx/Rx	0/0

Security

Authenticating ISE	ISE
Authentication Method	802.1X
Auth Status	Authorization Succeeded
Authorization Profile Name	AuthEmp
Posture Status	Not Applicable
TrustSec Security Group	Data Not Available
Audit Session ID	AC14E3810000089BEC90D091
Windows AD Domain	wlan.local
EAP Type	PEAP

General

User Name	Jack
IP Address	0.0.0.0
MAC Address	00:24:e8:e7:7b:93
Vendor	Dell
Endpoint Type	Microsoft-Workstation
Media Type	Wired
Hostname	Data Not Available
Serial Number	Data Not Available
Software Version	Data Not Available

Security

Authenticating ISE	ISE
Authentication Method	802.1X
Auth Status	Authorization Succeeded
Authorization Profile Name	AuthEmp
Posture Status	Not Applicable
TrustSec Security Group	Data Not Available
Audit Session ID	AC14E3810000089BEC90D091
Windows AD Domain	wlan.local
EAP Type	PEAP

ISE SIEM/Threat Defence Ecosystem

- Provide ISE context—identity, device-type, authorisation group, posture, authentications—to SIEM and Threat Defence partners
- Partners use context to identify users, devices and network privilege level associated with security events
- Enable SIEM/TD to scrutinise specific environments like BYOD or high-risk user groups
- Analyse ISE data for anomalous activity
- Optionally take network action on users/devices via ISE

Partners

hp ArcSight

IBM QRadar

Lancope

LogRhythm

splunk>

Symantec

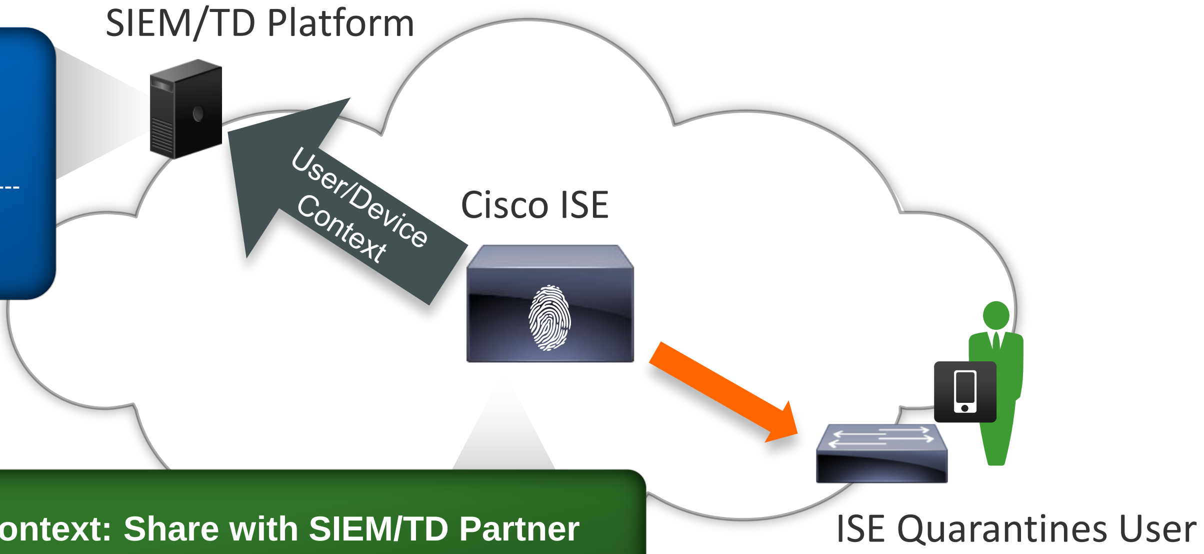
TIBCO

Ecosystem Partners

Cisco ISE SIEM & Threat Defence

Policy: Detect sensitive data access from mobile devices; quarantine such users

Data: "Sensitive Data"
Type: "Mobile Device"



Context: Share with SIEM/TD Partner

USER : DEVICE TYPE : CONN STATUS

APIs and pxGrid

Sharing Context Throughout the Network

ISE APIs

What Are They?   Why Do I Care?

- ISE 1.0/1.1 provides the **REpresentational State Transfer (REST) API** framework that allows information to be sent / received via XML using HTTP/S.

  REST API allows programmatic retrieval of ISE session and troubleshooting information from MnT DB as well as issue CoA for sessions directly from custom applications.

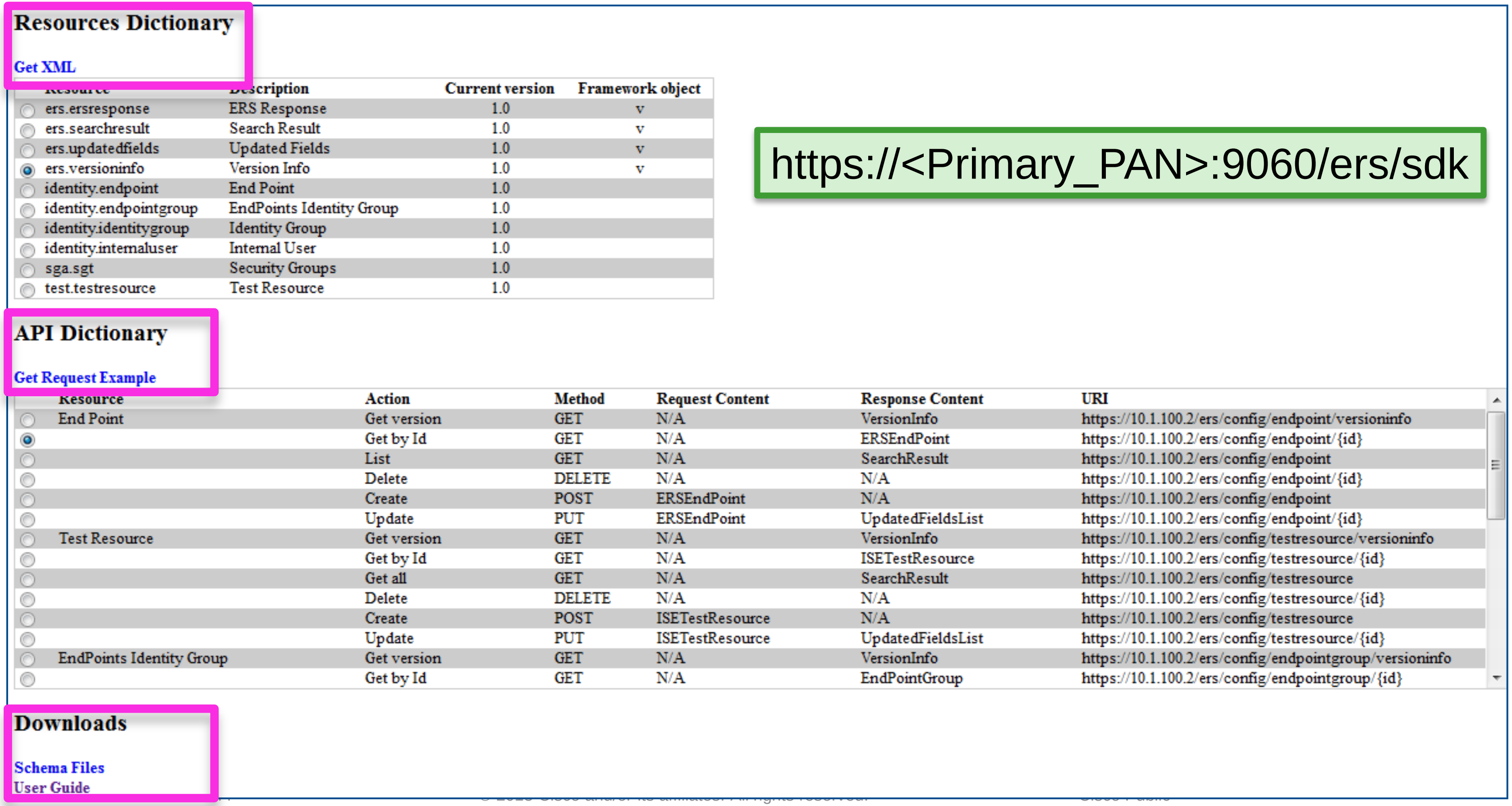
- ISE 1.2 introduces support for **External RESTful Services (ERS) API** and is based on the HTTP protocol and REST methodology.

  ERS allows programmatic CRUD (Create, Read, Update, Delete) operations on ISE resources including Internal Users, Internal Endpoints and Identity Groups (User and Endpoint).

ERS SDK

Software Development Kit to aid deployment.

https://<Primary_PAN>:9060/ers/sdk



Resources Dictionary

Get XML

	Resource	Description	Current version	Framework object
○	ers.ersresponse	ERS Response	1.0	v
○	ers.searchresult	Search Result	1.0	v
○	ers.updatedfields	Updated Fields	1.0	v
●	ers.versioninfo	Version Info	1.0	v
○	identity.endpoint	End Point	1.0	
○	identity.endpointgroup	EndPoints Identity Group	1.0	
○	identity.identitygroup	Identity Group	1.0	
○	identity.internaluser	Internal User	1.0	
○	sga.sgt	Security Groups	1.0	
○	test.testresource	Test Resource	1.0	

API Dictionary

Get Request Example

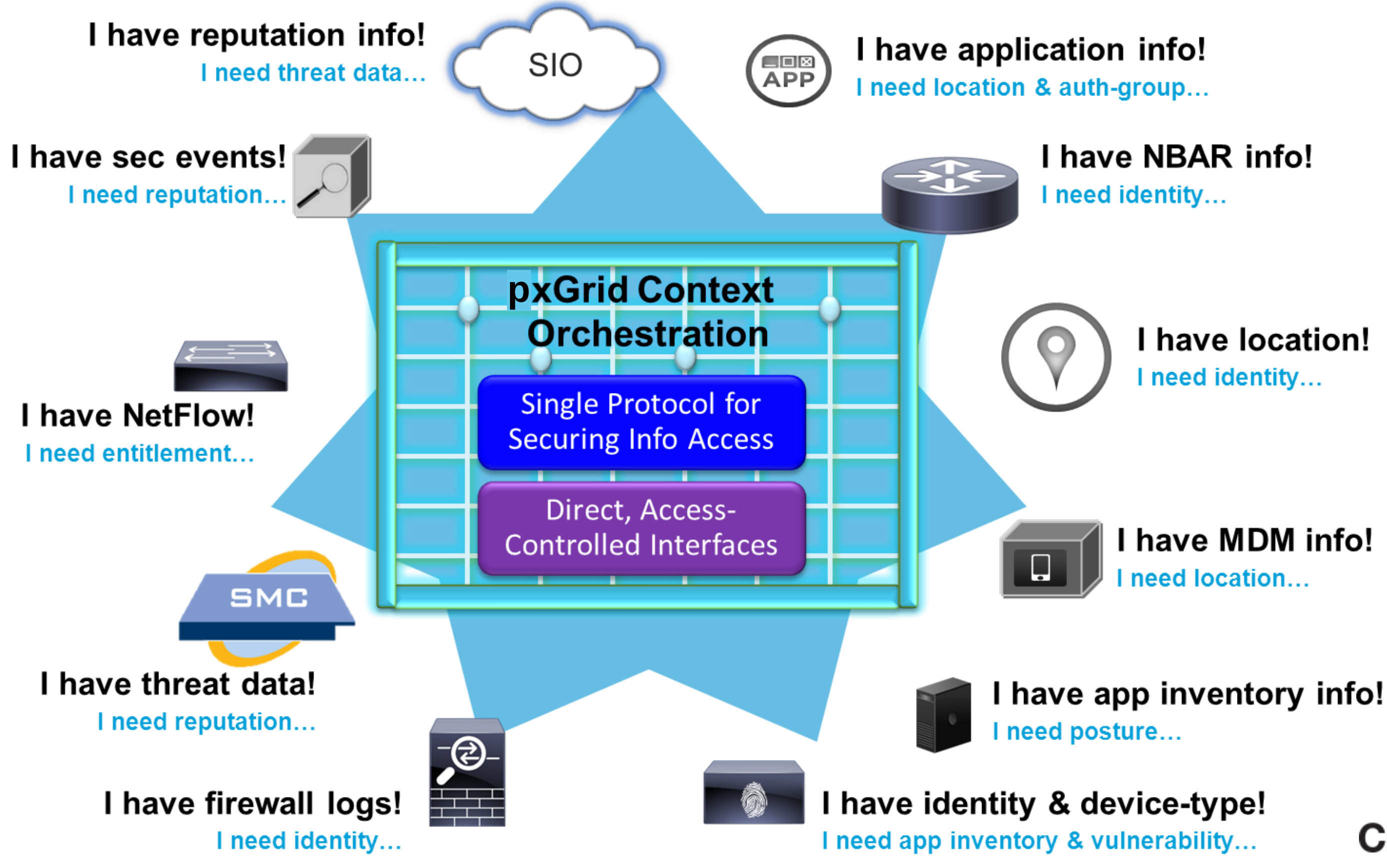
	Resource	Action	Method	Request Content	Response Content	URI
○	End Point	Get version	GET	N/A	VersionInfo	https://10.1.100.2/ers/config/endpoint/versioninfo
●		Get by Id	GET	N/A	ERSEndPoint	https://10.1.100.2/ers/config/endpoint/{id}
○		List	GET	N/A	SearchResult	https://10.1.100.2/ers/config/endpoint
○		Delete	DELETE	N/A	N/A	https://10.1.100.2/ers/config/endpoint/{id}
○		Create	POST	ERSEndPoint	N/A	https://10.1.100.2/ers/config/endpoint
○		Update	PUT	ERSEndPoint	UpdatedFieldsList	https://10.1.100.2/ers/config/endpoint/{id}
○	Test Resource	Get version	GET	N/A	VersionInfo	https://10.1.100.2/ers/config/testresource/versioninfo
○		Get by Id	GET	N/A	ISETestResource	https://10.1.100.2/ers/config/testresource/{id}
○		Get all	GET	N/A	SearchResult	https://10.1.100.2/ers/config/testresource
○		Delete	DELETE	N/A	N/A	https://10.1.100.2/ers/config/testresource/{id}
○		Create	POST	ISETestResource	N/A	https://10.1.100.2/ers/config/testresource
○		Update	PUT	ISETestResource	UpdatedFieldsList	https://10.1.100.2/ers/config/testresource/{id}
○	EndPoints Identity Group	Get version	GET	N/A	VersionInfo	https://10.1.100.2/ers/config/endpointgroup/versioninfo
○		Get by Id	GET	N/A	EndPointGroup	https://10.1.100.2/ers/config/endpointgroup/{id}

Downloads

Schema Files
User Guide

Platform eXchange Grid (pxGrid)

Network Context Orchestration



I have reputation info!
I need threat data…

SIO

I have application info!
I need location & auth-group…

I have sec events!
I need reputation…

I have NBAR info!
I need identity…

pxGrid Context Orchestration

Single Protocol for Securing Info Access

Direct, Access-Controlled Interfaces

I have location!
I need identity…

I have NetFlow!
I need entitlement…

I have MDM info!
I need location…

SMC

I have threat data!
I need reputation…

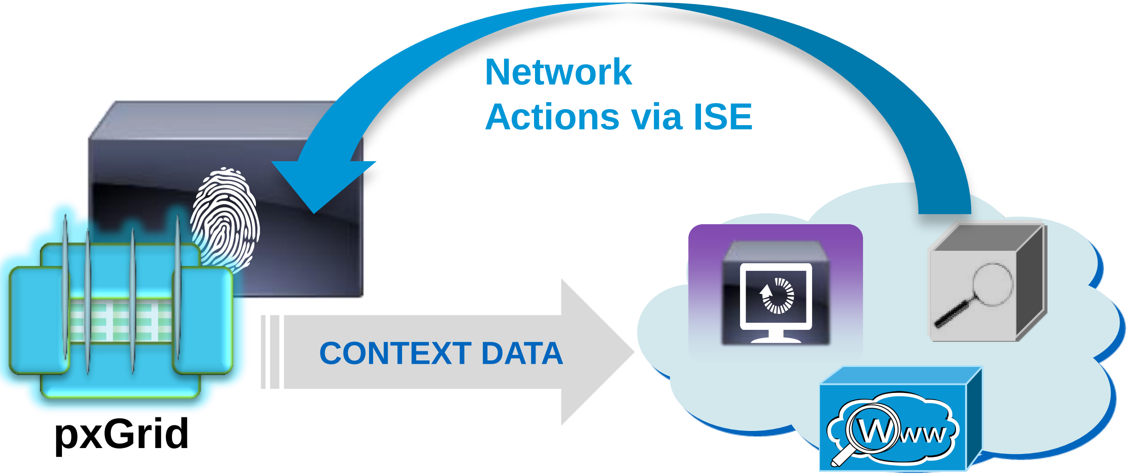
I have app inventory info!
I need posture…

I have firewall logs!
I need identity…

I have identity & device-type!
I need app inventory & vulnerability…

pxGrid

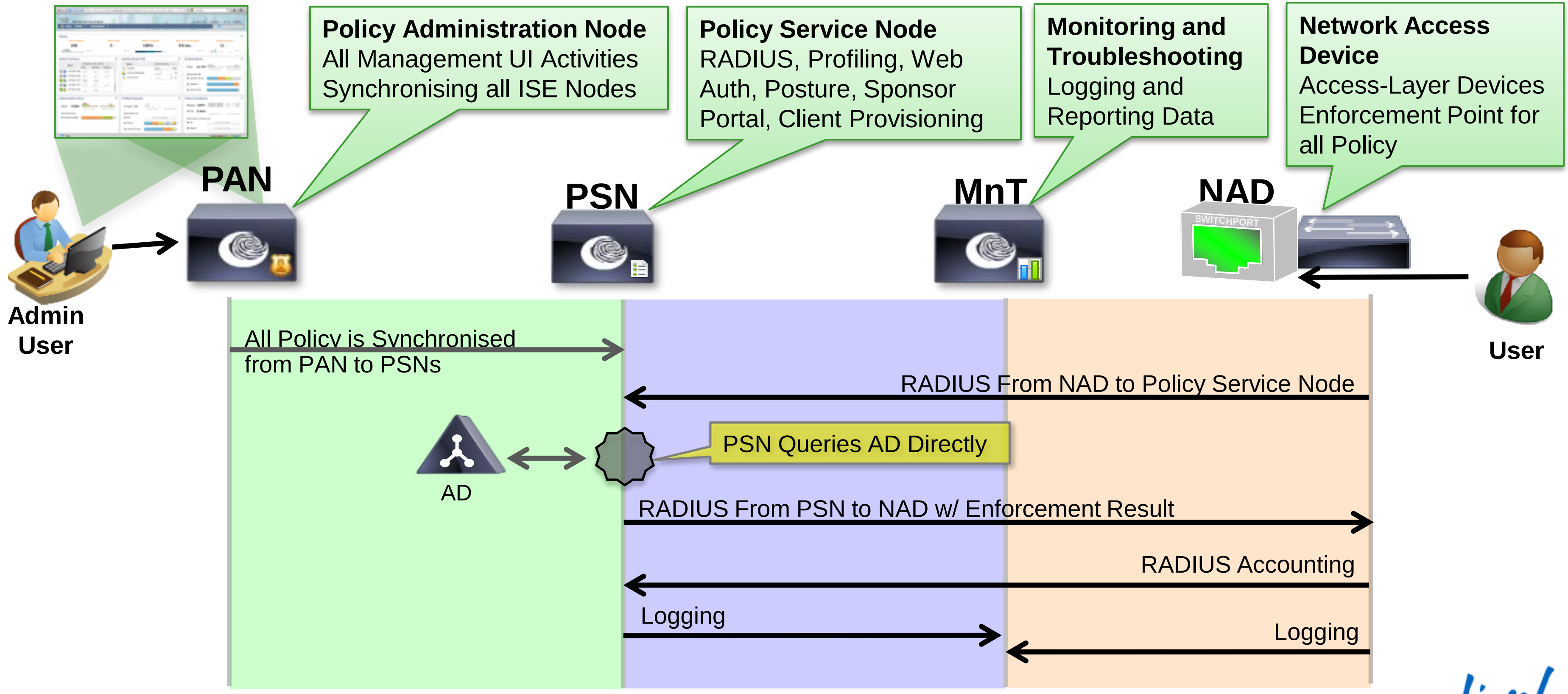
Access-Controlled Interface to ISE Context & Network Control



- Focus is export of ISE session context and enabling remediation actions from external systems
- Granular context acquisition via queries to publisher/subscriber interface

ISE Deployment Architecture

ISE Node Personas = Functional Roles



Policy Administration Node
All Management UI Activities
Synchronising all ISE Nodes

Policy Service Node
RADIUS, Profiling, Web Auth, Posture, Sponsor Portal, Client Provisioning

Monitoring and Troubleshooting
Logging and Reporting Data

Network Access Device
Access-Layer Devices
Enforcement Point for all Policy

Admin User

PAN

PSN

MnT

NAD

User

All Policy is Synchronised from PAN to PSNs

RADIUS From NAD to Policy Service Node

AD

PSN Queries AD Directly

RADIUS From PSN to NAD w/ Enforcement Result

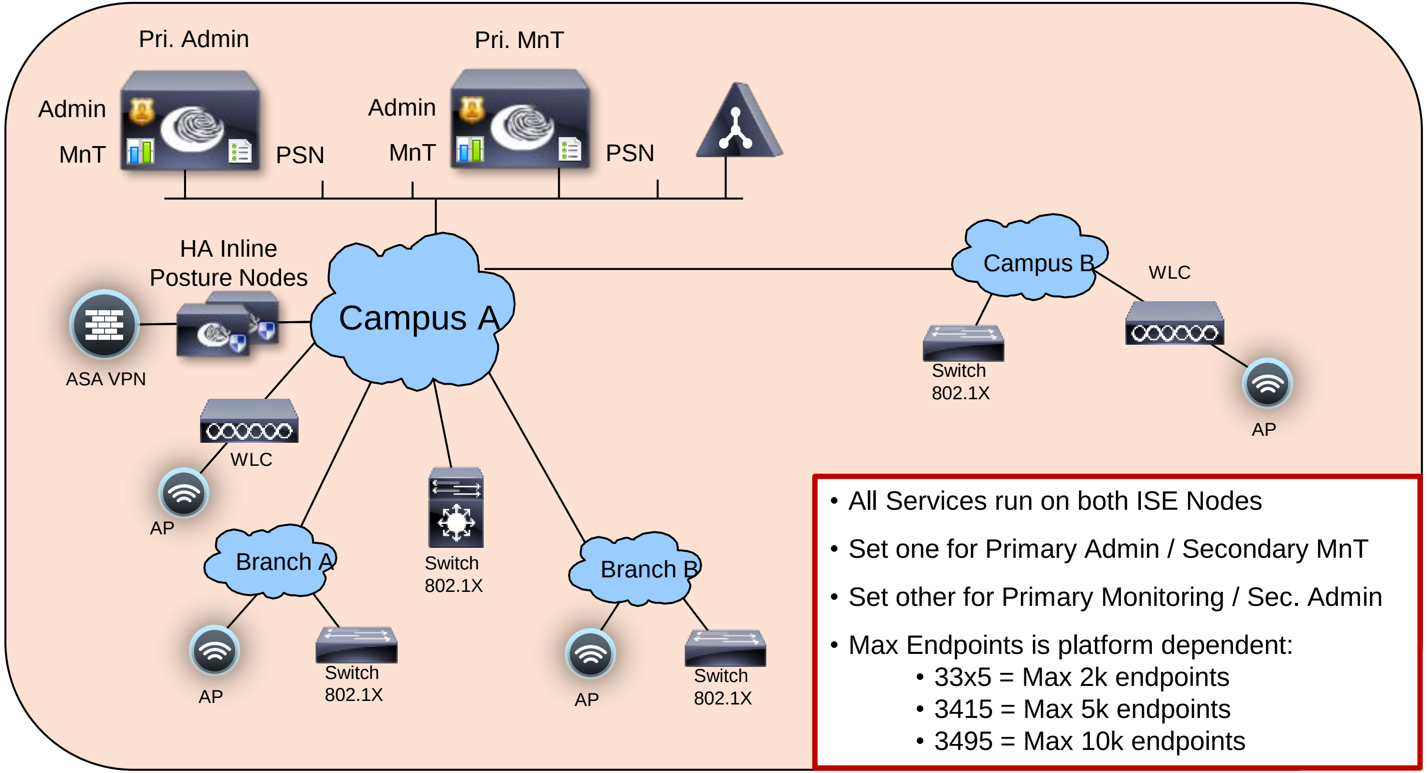
RADIUS Accounting

Logging

Logging

Basic 2-Node ISE Deployment (Redundant)

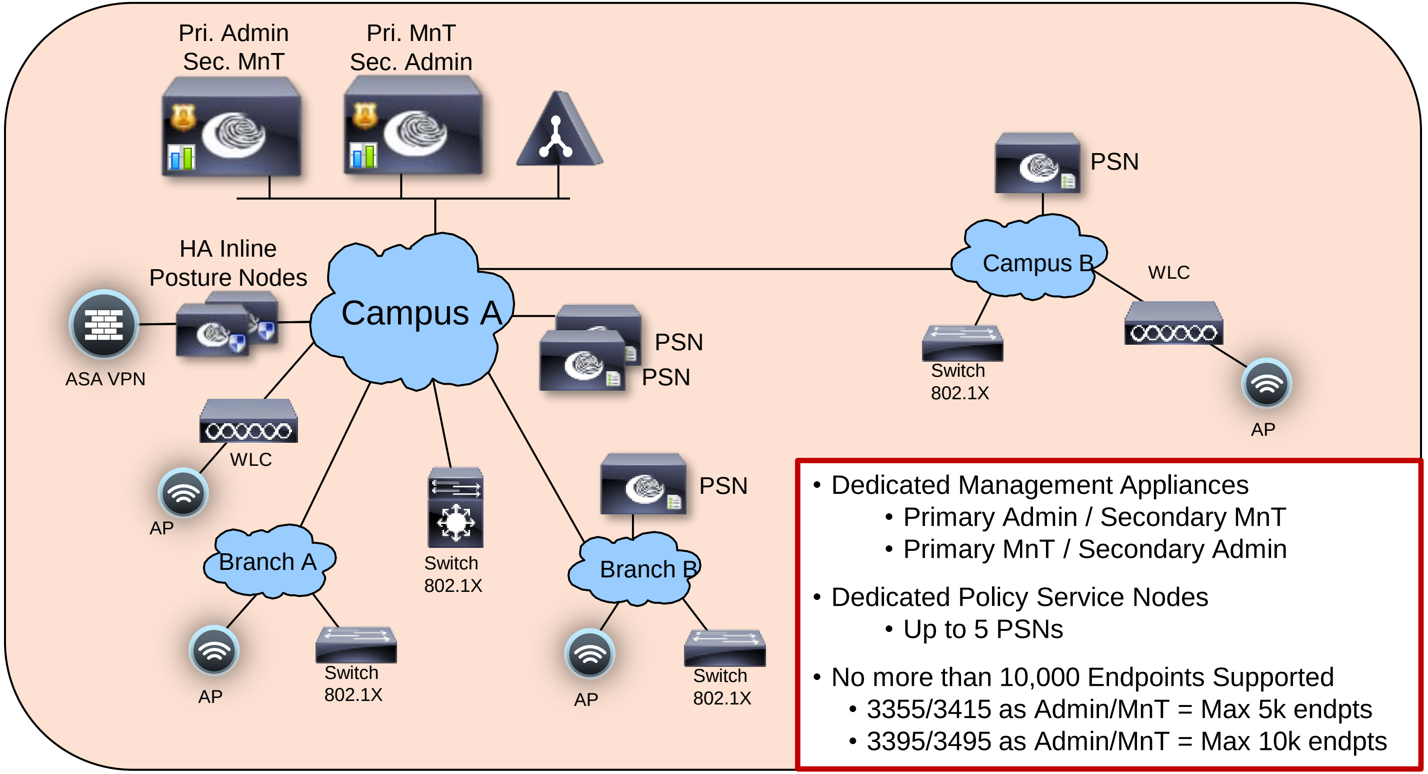
Maximum Endpoints = 10,000 (Platform dependent)



- All Services run on both ISE Nodes
- Set one for Primary Admin / Secondary MnT
- Set other for Primary Monitoring / Sec. Admin
- Max Endpoints is platform dependent:
    - 33x5 = Max 2k endpoints
    - 3415 = Max 5k endpoints
    - 3495 = Max 10k endpoints

Basic Distributed Deployment

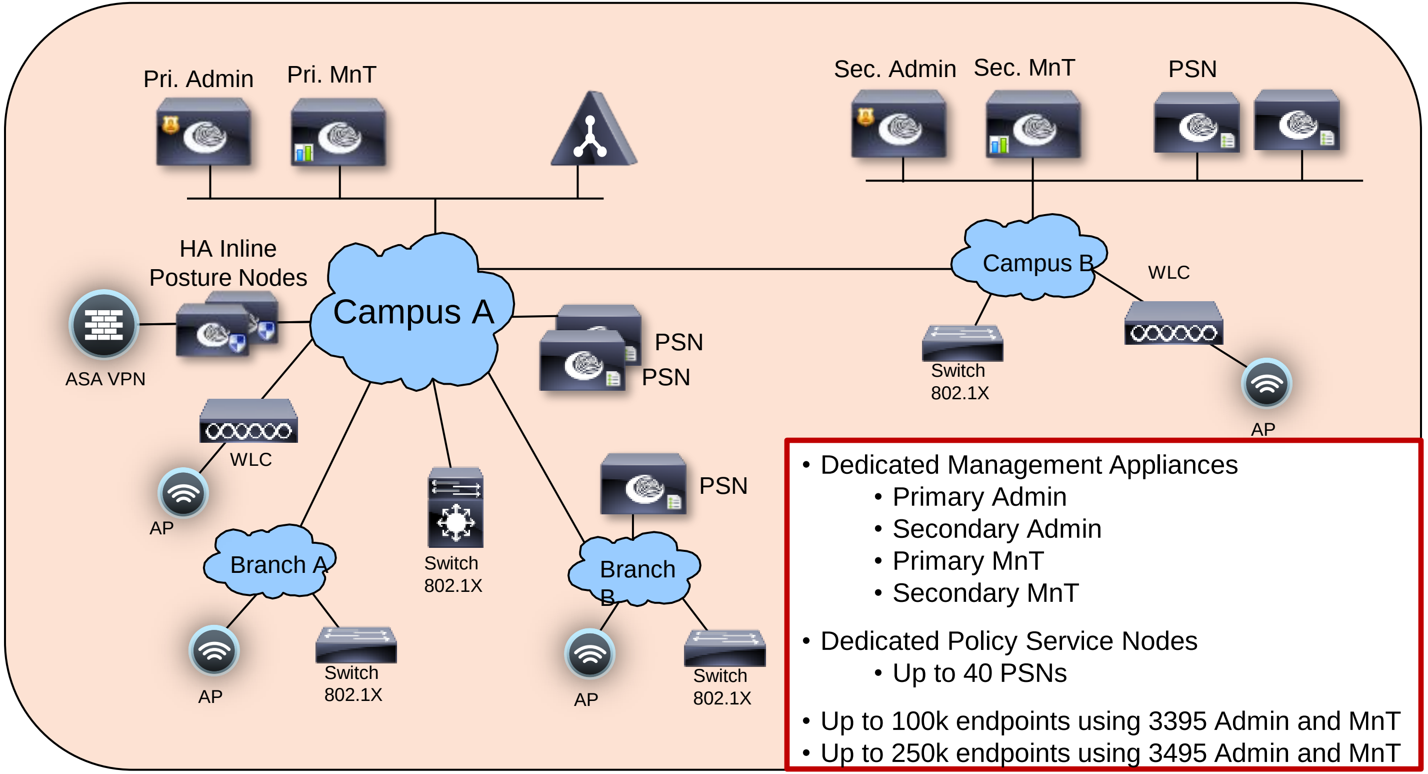
Maximum Endpoints = 10,000 / Maximum 5 PSNs



- Dedicated Management Appliances
  - Primary Admin / Secondary MnT
  - Primary MnT / Secondary Admin
- Dedicated Policy Service Nodes
  - Up to 5 PSNs
- No more than 10,000 Endpoints Supported
  - 3355/3415 as Admin/MnT = Max 5k endpts
  - 3395/3495 as Admin/MnT = Max 10k endpts

Fully Distributed Deployment

Maximum Endpoints = 250,000 / Maximum 40 PSNs

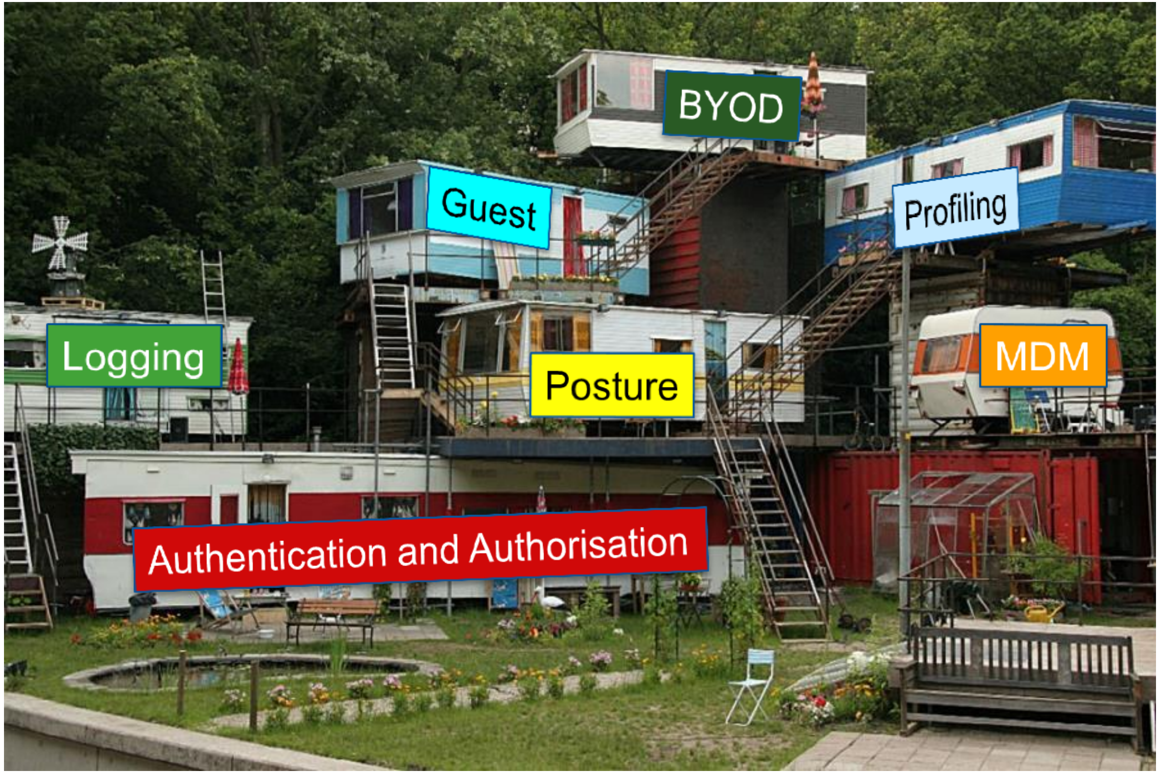


- Dedicated Management Appliances
  - Primary Admin
  - Secondary Admin
  - Primary MnT
  - Secondary MnT
- Dedicated Policy Service Nodes
  - Up to 40 PSNs
- Up to 100k endpoints using 3395 Admin and MnT
- Up to 250k endpoints using 3495 Admin and MnT

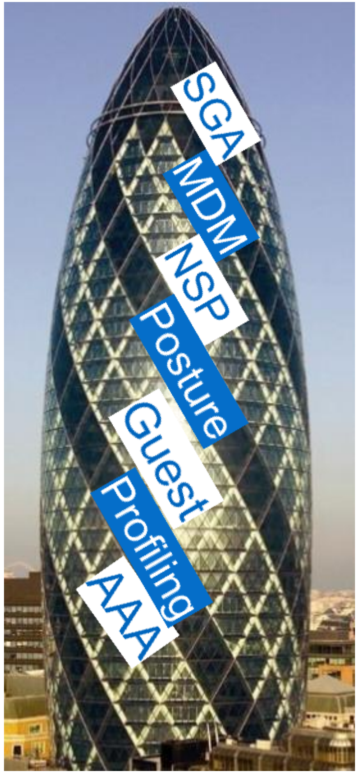
A Systems Approach to Building an Identity Access Control Architecture

Building an Identity-Based Network Architecture

Ad-Hoc Couplings Versus Systems Approach



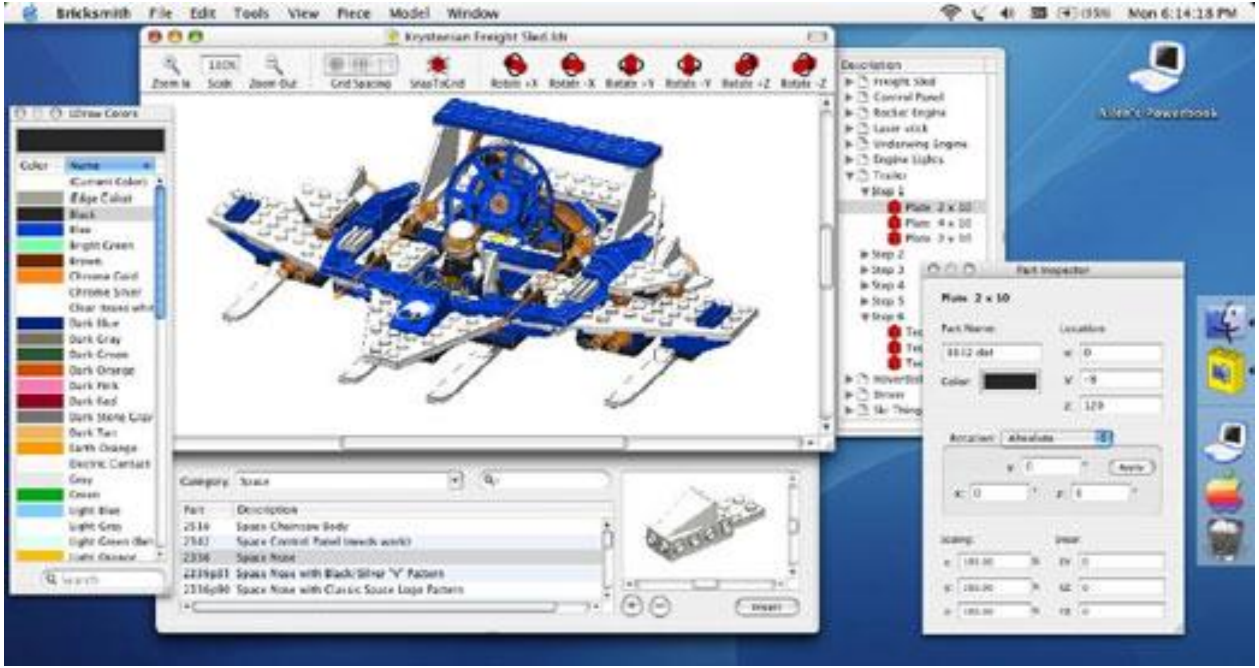
VS



Building an Identity-Based Network Architecture

Architecture and Building Plan

- Start with a High Level Design (HLD) of the big picture, current limitations and future requirements
- Test and tune with testing to develop the “Blueprint” or Low-Level Design (LLD) with detailed configurations and deployment steps.



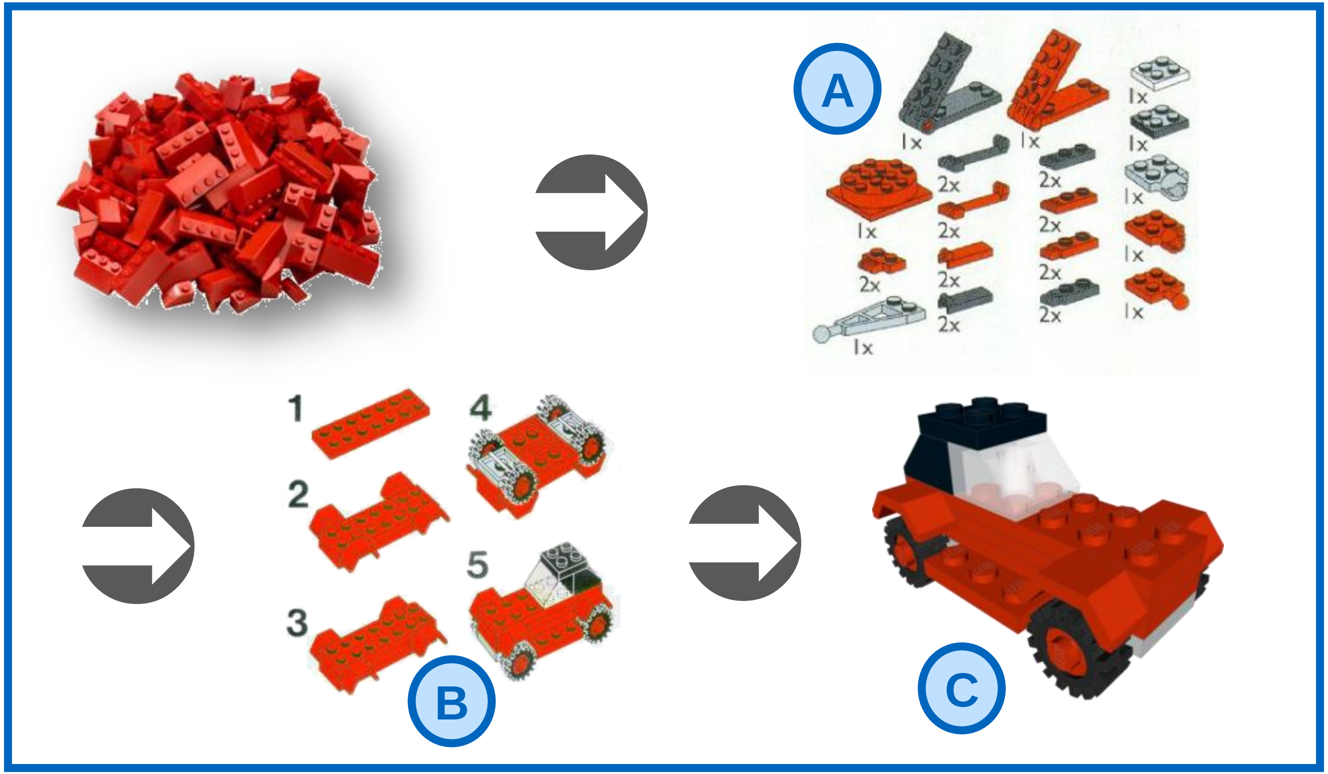
Building an Identity-Based Network Architecture

Architecture and Building Plan

A Make sure you have the right pieces before production.

C Keep end goal in mind BUT…

B Deploy in phases to minimise disruption and increase adoption rate.



Choosing the Correct Building Blocks
The “TrustSec” Portfolio

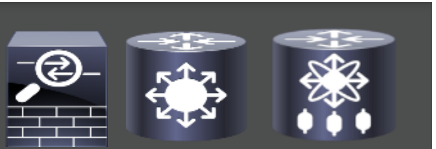
www.cisco.com/go/trustsec

Policy
Administration
Policy Decision

Identity Services Engine (ISE)
Identity Access Policy System

Policy
Enforcement
TrustSec Powered

Cisco 2960/3560/3700/4500/6500, Nexus 7000
switches, Wireless and Routing Infrastructure



Cisco ASA, ISR, ASR 1000

Policy
Information
TrustSec Powered

About

Clean Access Agent
by Cisco Systems

Version 3.4.0
Copyright 2004 Cisco Systems, Inc.

NAC Agent

Web Agent

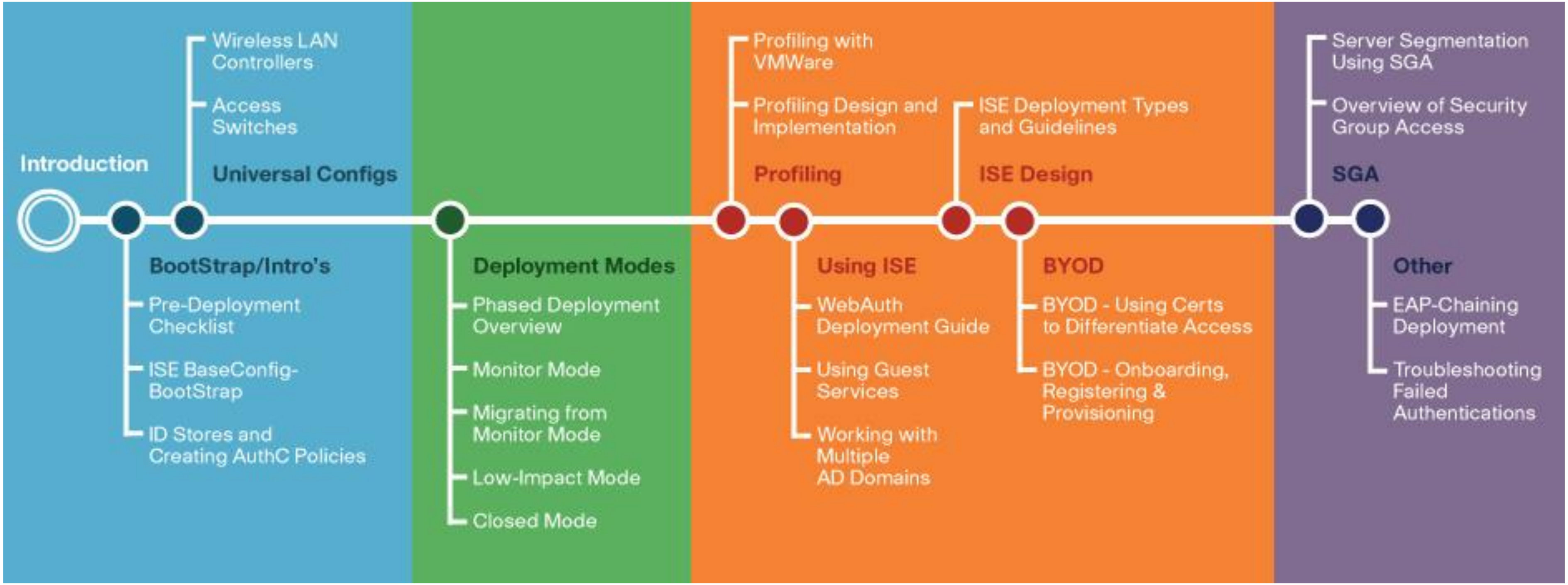
No-Cost Persistent and Temporal Clients
for Posture, and Remediation

802.1X Supplicant
AnyConnect or
OS-Embedded Supplicant

Identity-Based Access Is a Feature of the Network
Spanning Wired, Wireless, and VPN

TrustSec Design and How-To Guides

Secure Access Blueprints


Introduction
Universal Configs
Wireless LAN Controllers
Access Switches
BootStrap/Intro's
Pre-Deployment Checklist
ISE BaseConfig-BootStrap
ID Stores and Creating AuthC Policies
Deployment Modes
Phased Deployment Overview
Monitor Mode
Migrating from Monitor Mode
Low-Impact Mode
Closed Mode
Profiling
Profiling with VMWare
Profiling Design and Implementation
Using ISE
WebAuth Deployment Guide
Using Guest Services
Working with Multiple AD Domains
ISE Design
ISE Deployment Types and Guidelines
BYOD
BYOD - Using Certs to Differentiate Access
BYOD - Onboarding, Registering & Provisioning
SGA
Server Segmentation Using SGA
Overview of Security Group Access
Other
EAP-Chaining Deployment
Troubleshooting Failed Authentications

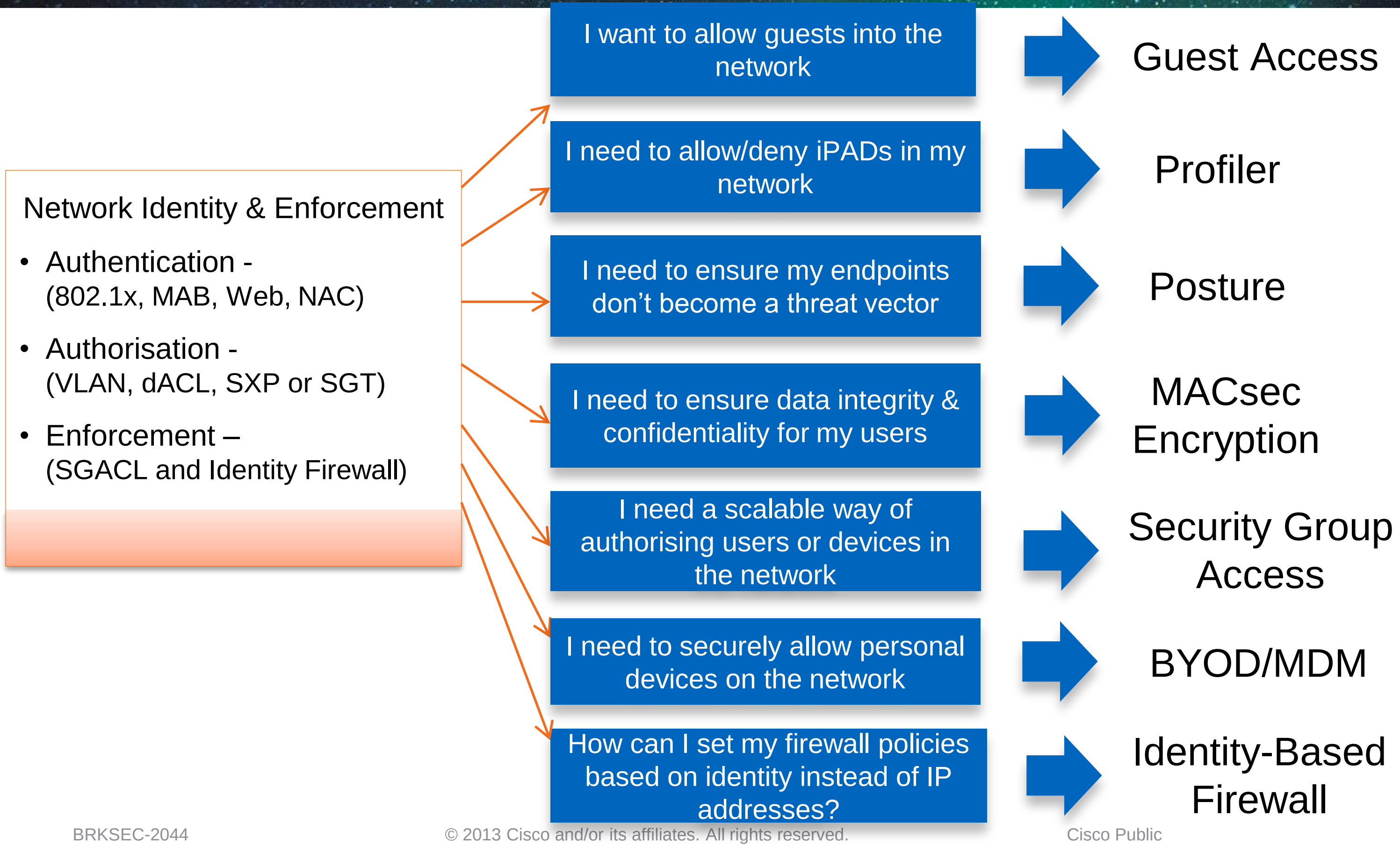
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Building an Identity-Based Network Architecture

Pulling It All Together

Summary

Cisco Secure Access and TrustSec Technology Review:



Network Identity & Enforcement

- Authentication - (802.1x, MAB, Web, NAC)
- Authorisation - (VLAN, dACL, SXP or SGT)
- Enforcement – (SGACL and Identity Firewall)

I want to allow guests into the network → Guest Access

I need to allow/deny iPADs in my network → Profiler

I need to ensure my endpoints don’t become a threat vector → Posture

I need to ensure data integrity & confidentiality for my users → MACsec Encryption

I need a scalable way of authorising users or devices in the network → Security Group Access

I need to securely allow personal devices on the network → BYOD/MDM

How can I set my firewall policies based on identity instead of IP addresses? → Identity-Based Firewall

Summary

- Cisco Secure Access + TrustSec is an architecture for enterprise-wide identity access control built on standards and powered with Cisco intelligence.
- ISE is an Identity Policy Server for gathering context about every connected endpoint and enables centralised policy configuration, context sharing, and visibility with distributed policy enforcement.
- Secure Access with ISE integrates user and device identity, profiling, posture, onboarding, and MDM with additional endpoint attributes to provide a contextual identity for all connected devices.
- Secure Group Access pushes contextual identity into the network to deliver next generation policy enforcement across switches, routers, and firewalls.
- Cisco offers blueprints to aid in the design and deployment of identity access solutions based on Secure Access architecture.
- Cisco Secure Access can be deployed in phases to ease deployment and increase success.

Related Sessions

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 TM