
TOMORROW
starts here.
CISCO
Cisco live!

Building an Enterprise Access Control Architecture using ISE and TrustSec

BRKSEC-2044

Imran Bashir
Technical Marketing Engineer

#clmel

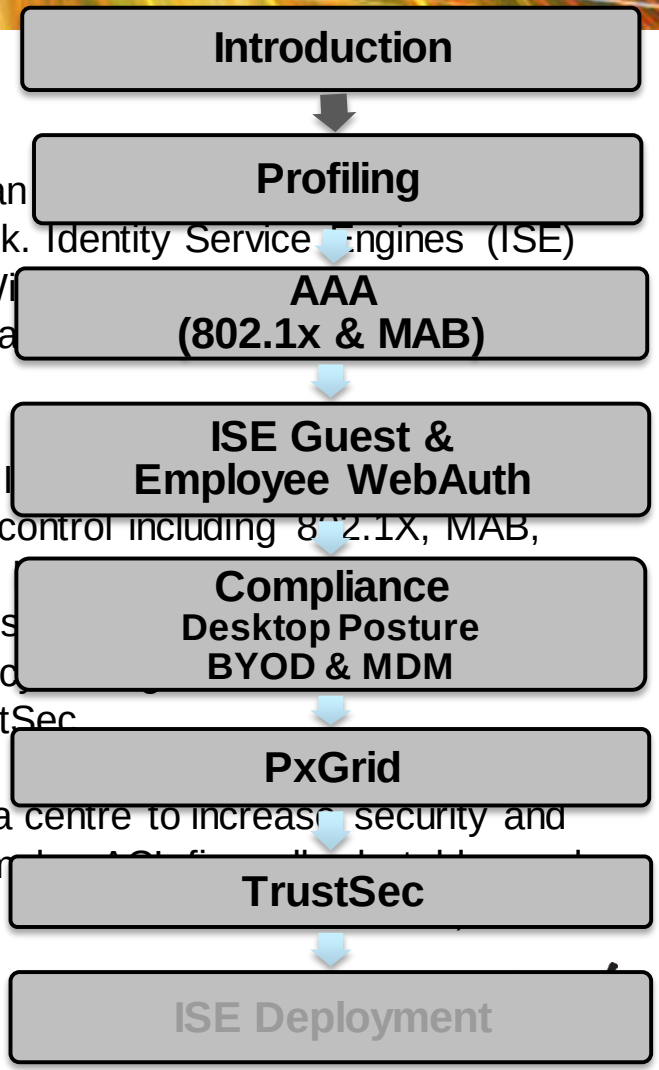
Cisco live!

Session Abstract

Tomorrow's requirement to network the Internet of Things requires an
that contextually regulates who and what is allowed onto the network. Identity Service Engines (ISE)
plays a central role in providing network access control for Wired, Wi
addition, ISE is the policy control point for TrustSec, which controls a
resources.

This session will focus on: 1. Emerging business requirements and
profiling, posture, BYOD and MDM. 2. Secure policy based access control including 802.1X, MAB,
Web Authentication, and certificates/PKI. The session will show you
to include contextual information gathered from profiling, posture ass
data stores such as AD and LDAP. 3. Enforcing network access polic
such as VLANs and ACLS and emerging technologies such as TrustSec

Cisco TrustSec technology is used to segment the campus and data centre to increase security and
drive down the operational expenses associated with managing com
ACLs lists. This session is an introduction to the following advanced
BRKSEC-3698; BRKSEC-3690; TECSEC-3691.



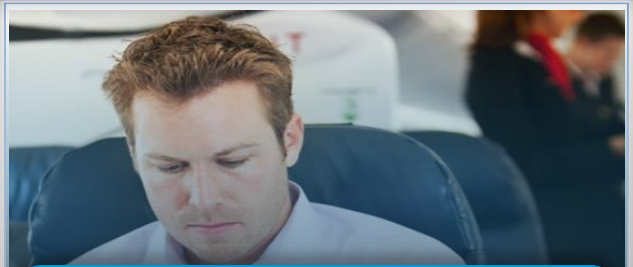
IT Trends of Securing Access

Internet of Things Encompasses **Everything**

2004

Antivirus software installed

Operating system patches up-to-date



Today

BYOD for productivity and personalisation

Average worker with 3 devices

~ 7 Billion connected devices

Tomorrow

Over 15 Billion devices by 2015

71% mobile video traffic in 2016

2/3 of worker in cloud by 2016

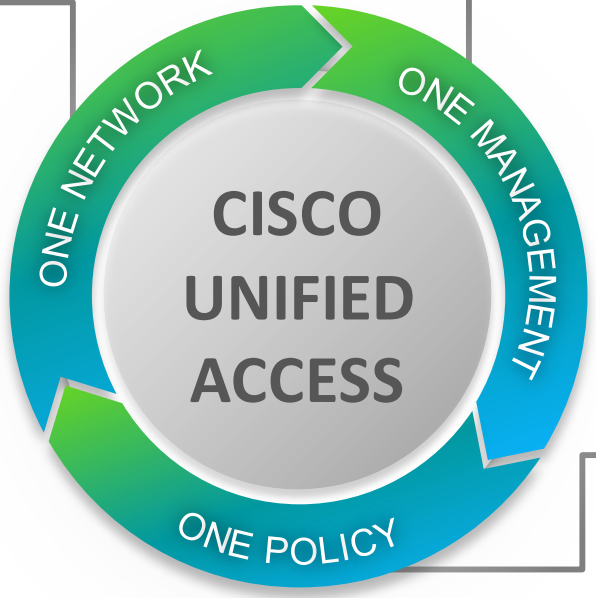
50% workloads are virtualised

Mobile Malware doubled

ISE Provides ONE Policy for Unified Access

ONE NETWORK

Integrated Wired and Wireless in ONE Physical Infrastructure, with ONE Operating System & Open APIs



ONE MANAGEMENT

Single Plane of Glass Management with **Cisco Prime**

ONE POLICY

Simplified, Unified Policy Management with Cisco ISE

Cisco Identity Services Engine (ISE)

Delivering the Visibility and Control for Secure Network Access

Cisco ISE is the Market Leader

Why Cisco ISE?

Cisco ISE Provides Comprehensive, Unified Policy Management and Enforcement to Ensure Secure Wired, Wireless, and VPN Access

- **Visibility Driven** – Accurately Identify and Assess Network Users & Devices
- **Access Control** – Grant/Limit access to align with appropriate business policy
- **Threat Focused** – Minimise the spread of network threats & the impact of data breaches

The Different Ways Customers Use ISE

Guest Access Management

Easily provide guests limited-time, limited-resource Internet access

BYOD and Enterprise Mobility

Seamlessly & securely onboard devices with the right levels of access

Secure Access across the Entire Network

Simplify & unify enterprise network access policy across wired, wireless, & VPN

With Cisco TrustSec®

Identity-aware Network Segmentation and Access Policy Enforcement

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

Visibility "What" is Co
Network?

Introduction

Profiling

AAA
(802.1x & MAB)

ISE Guest &
Employee WebAuth

Compliance
Desktop Posture
BYOD & MDM

PxGrid

TrustSec

ISE Deployment

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

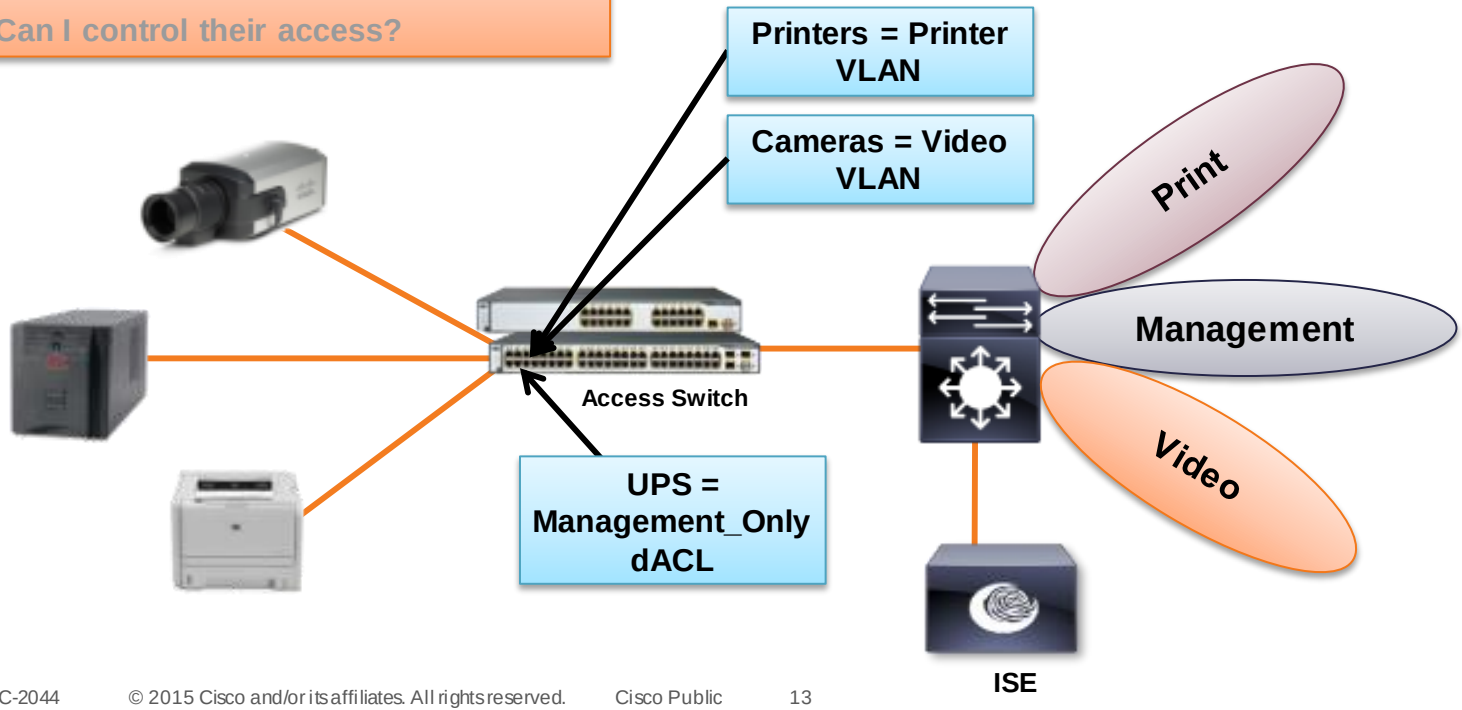
PCs	Non-PCs			
	UPS	Phone	Printer	AP

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

Profiling Non-User Devices

Dynamic Population of MAB Database Based on Device Type

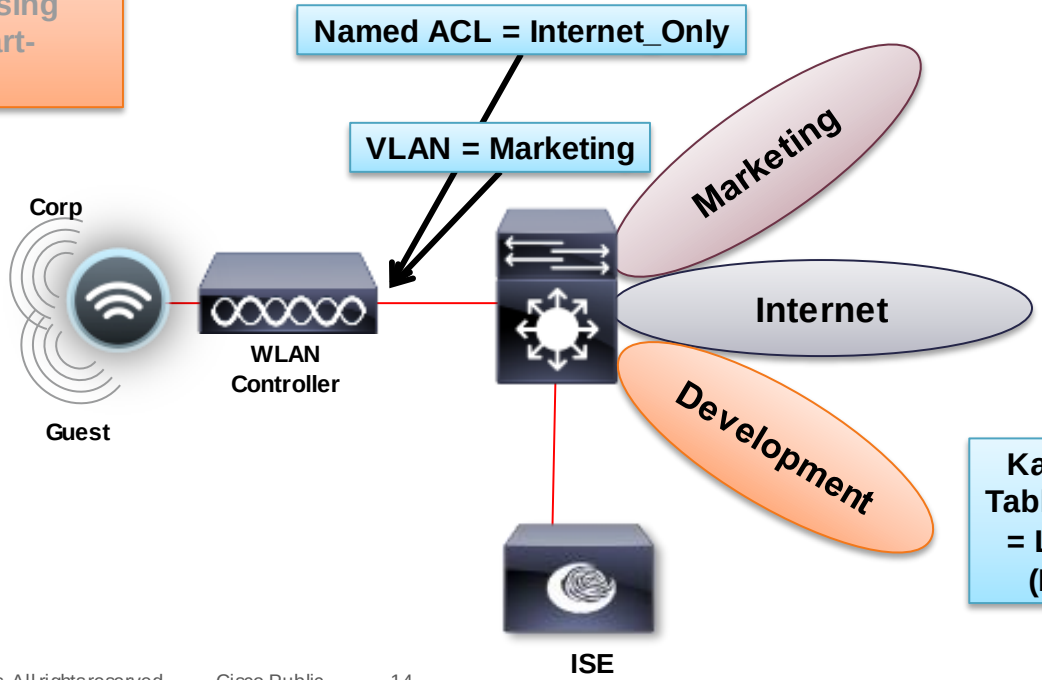
- How do I discover non-user devices?
- Can I determine what they are?
- Can I control their access?



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?



Profiling Technology

How Do We Classify a Device?

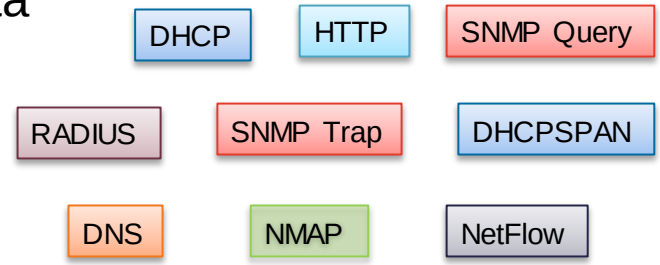
- Profiling uses signatures (similar to IPS)

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

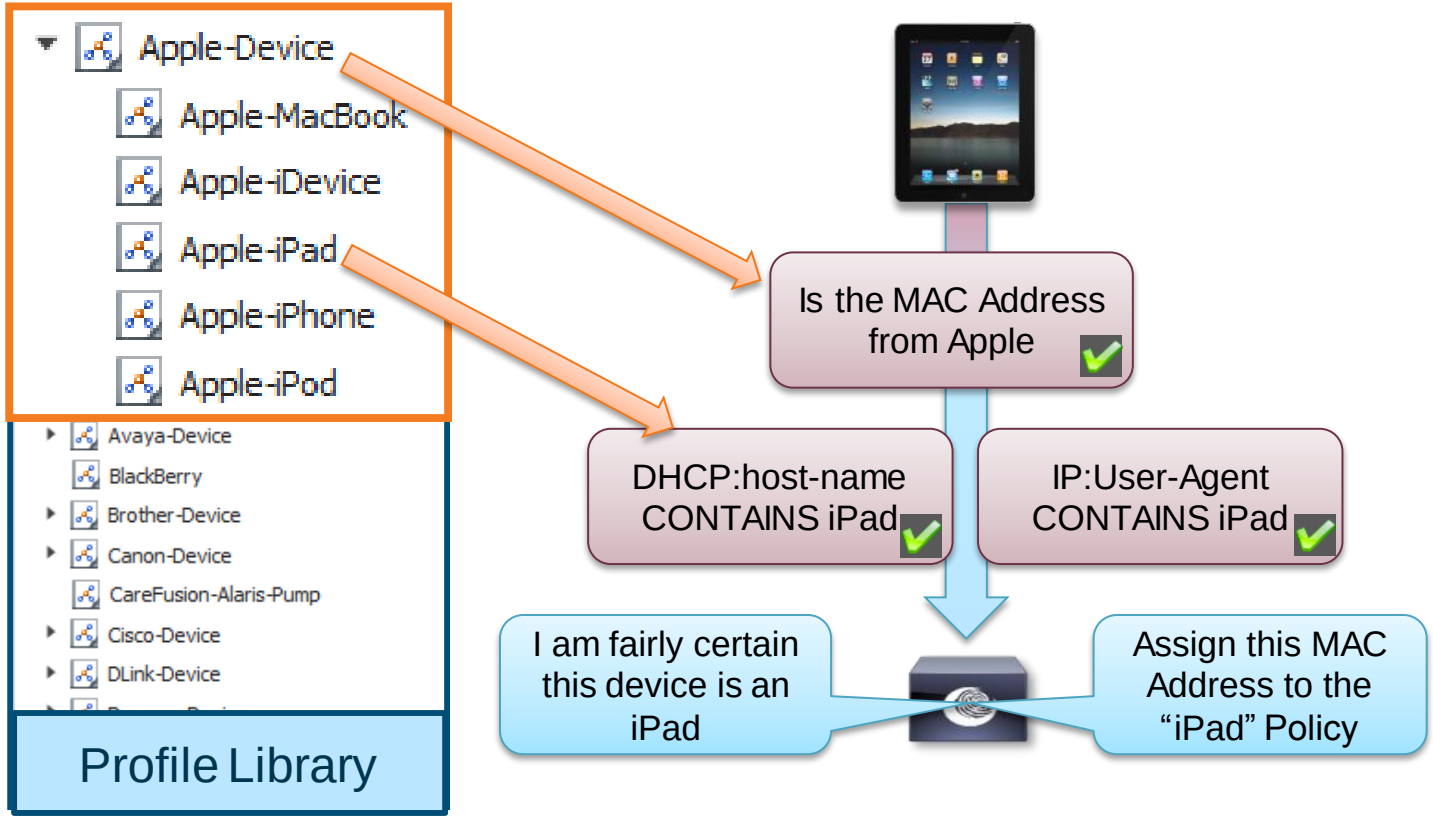
User-Agent	Mozilla/5.0 (iPad; U; CPU OS 4_3_2 like Mac OS X; en-us) AppleWebKit/533.17.9

- Probes are used to collect endpoint data



Profiling Policy Overview

Profile Policies Use a Combination of Conditions to Identify Devices

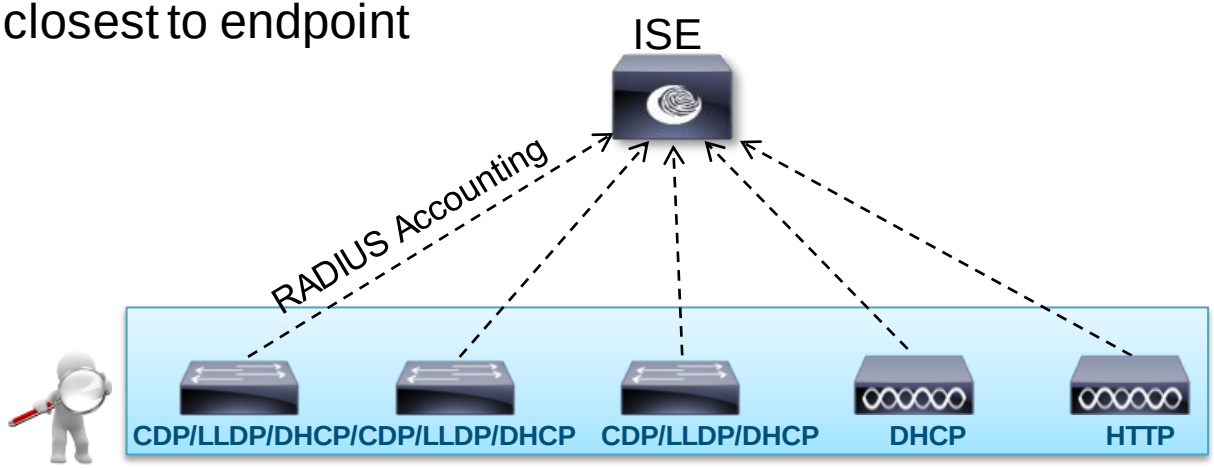


Device Sensor

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

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

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 4[illegible] 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 3[illegible] 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

ISE Profiling result

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

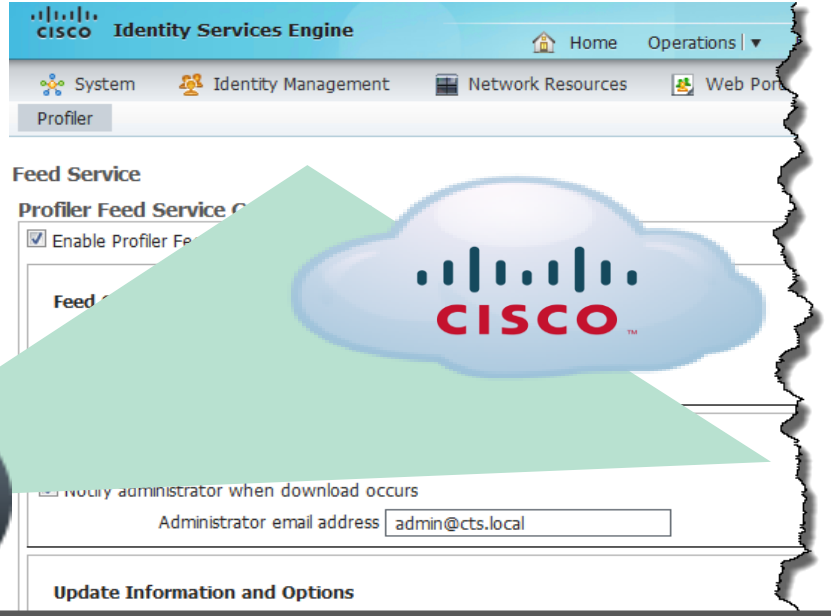
dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7945G
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35
dhcp-requested-address	10.100.15.100
dhcp-server-identifier	10.100.7.100
dot1xAuthAuthControlledPortControl	2
dot1xAuthAuthControlledPortStatus	2
dot1xAuthSessionUserName	00-21-55-D6-01-33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

Device Profile Feed Service

Another Cisco Innovation and Industry First!

1,000s of NEW devices launch every day

The **Internet of Things** makes "keeping up" a complete nightmare…until now.



Device feed service shares new, vetted device profiles from the Cisco community

More supported devices with real-time updates = ***faster onboarding for users***

Verification

Control

Authentication, Authorisation, ar

"Who" is Connecting, Access Rights Assigr

Introduction

Profiling

AAA
(802.1x & MAB)

ISE Guest &
Employee WebAuth

Compliance
Desktop Posture
BYOD & MDM

PxGrid

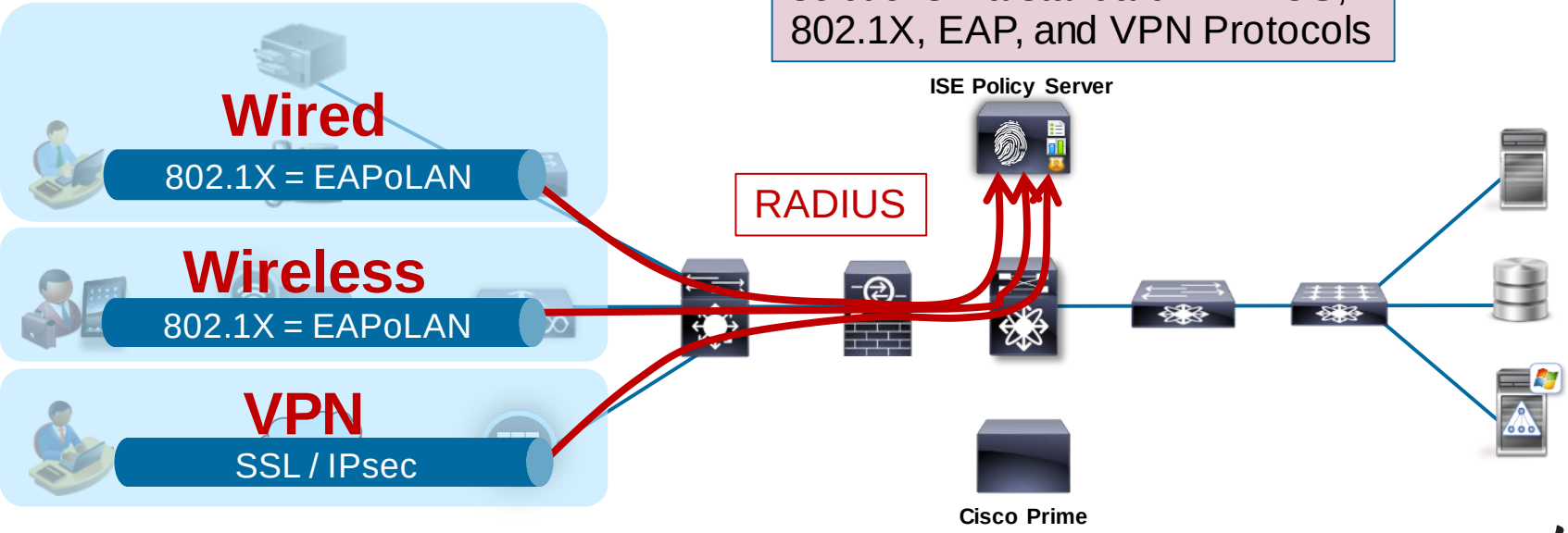
TrustSec

ISE Deployment

ISE is a Standards-Based AAA Server

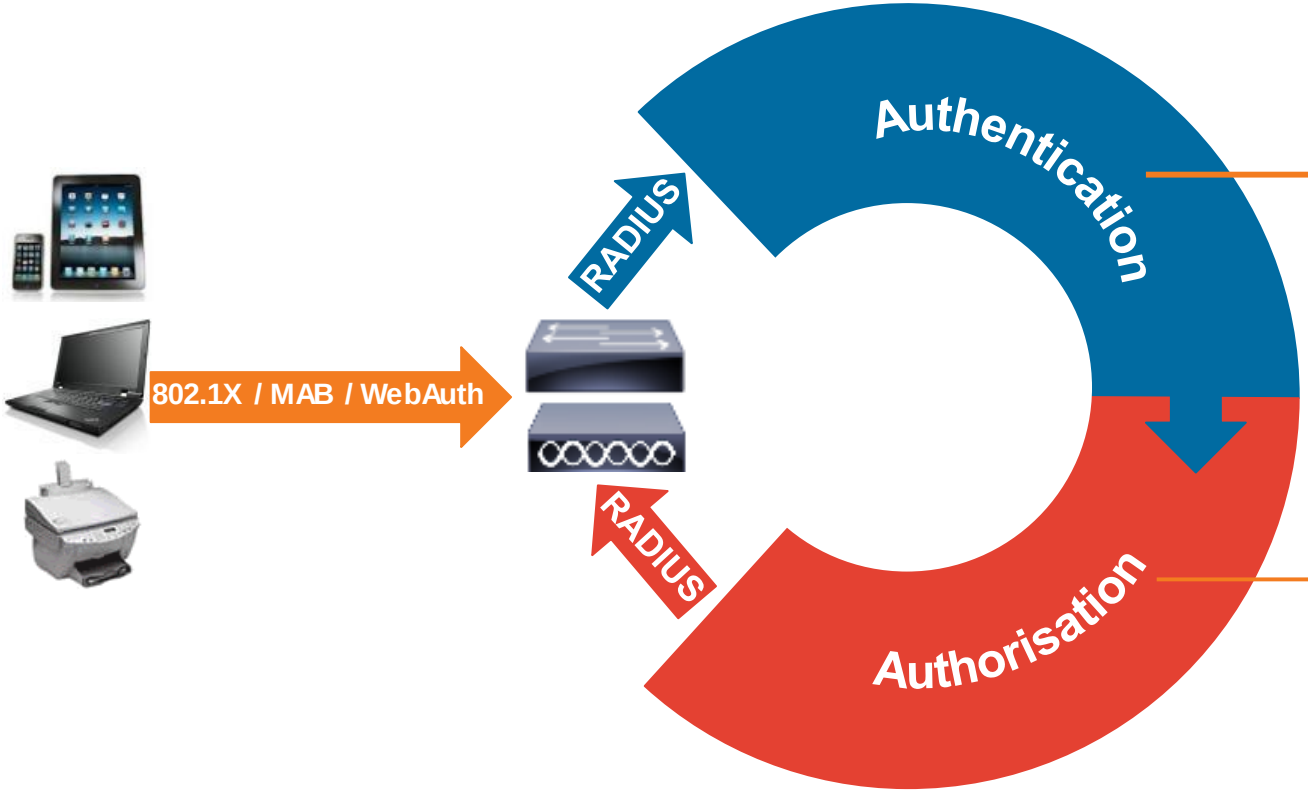
Access Control System Must Support All Connection Methods

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



Authentication and Authorisation

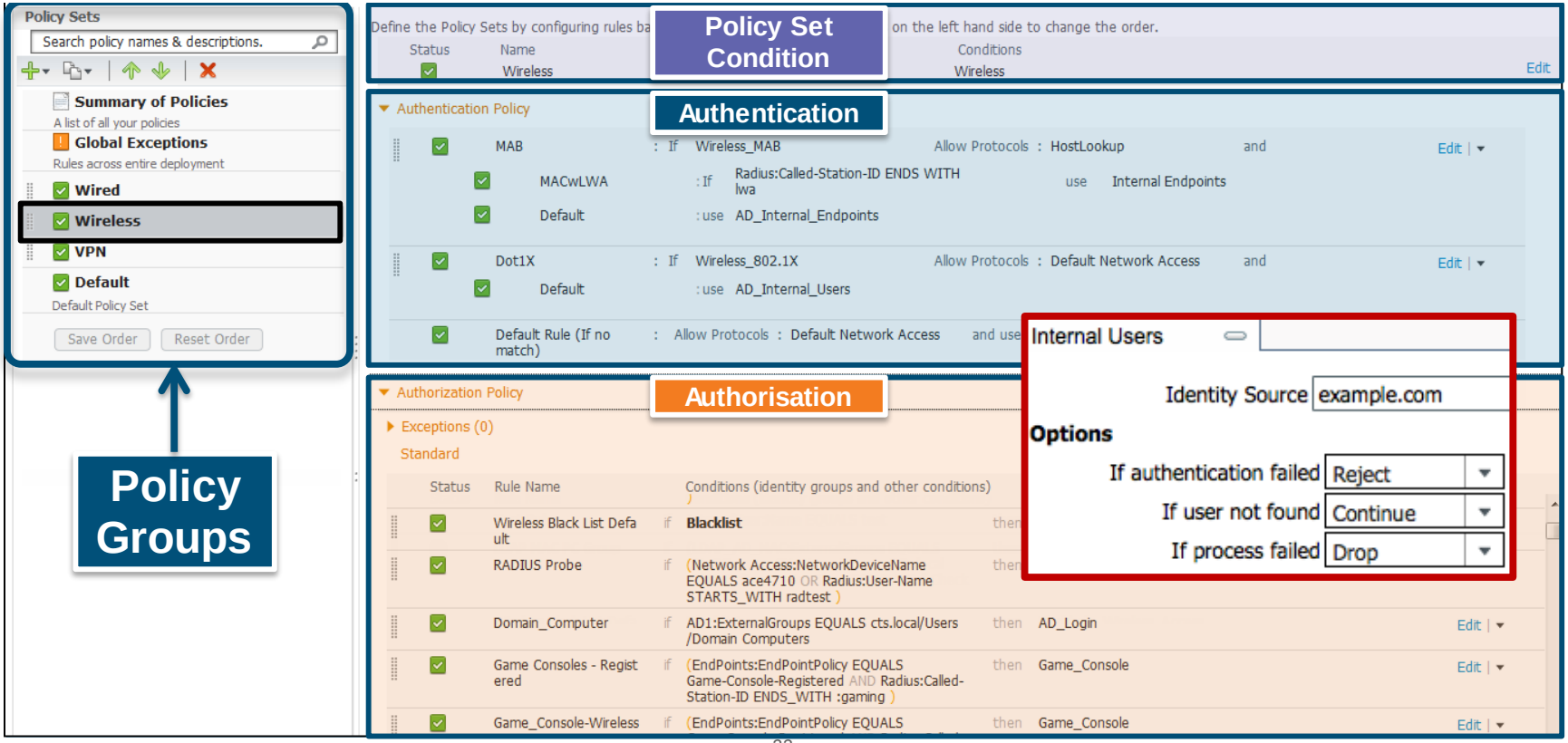
What's the Difference?



Who/what the endpoint is.

What the endpoint has access to.

Separation of Authentication and Authorisation



Tree View

Policy Set

AuthC Protocols

Identity Store

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description	Conditions	
✓	Wireless		Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11	Edit

Authentication Policy

✓	Dot1X	: If	Wireless_802.1X	Allow Protocols : Default Network Access	and	Edit |
✓	PEAP	: If	Network Access:EapTunnel EQUALS PEAP	use	All_AD_Instances	
✓	TLS	: If	Network Access:EapAuthentication EQUALS EAP-TLS	use	ATW_CAP	
✓	Default	: use	DenyAccess			
✓	MAB	: If	Wireless_MAB	Allow Protocols : Default Network Access	and	Edit |
✓	Default	: use	Internal Endpoints			
✓	Default Rule (If no match)	:	Allow Protocols : Default Network Access	and use : DenyAccess		Edit |

Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Network Device	D
All									
ℹ		0	employee1	8C:7C:92:2F:B8:CD	Apple-iPad				
✓			employee1	8C:7C:92:2F:B8:CD	Apple-iPad	Wireless >> Dot1X >> TLS	Wireless >> TLS-Accept	WLC-02	

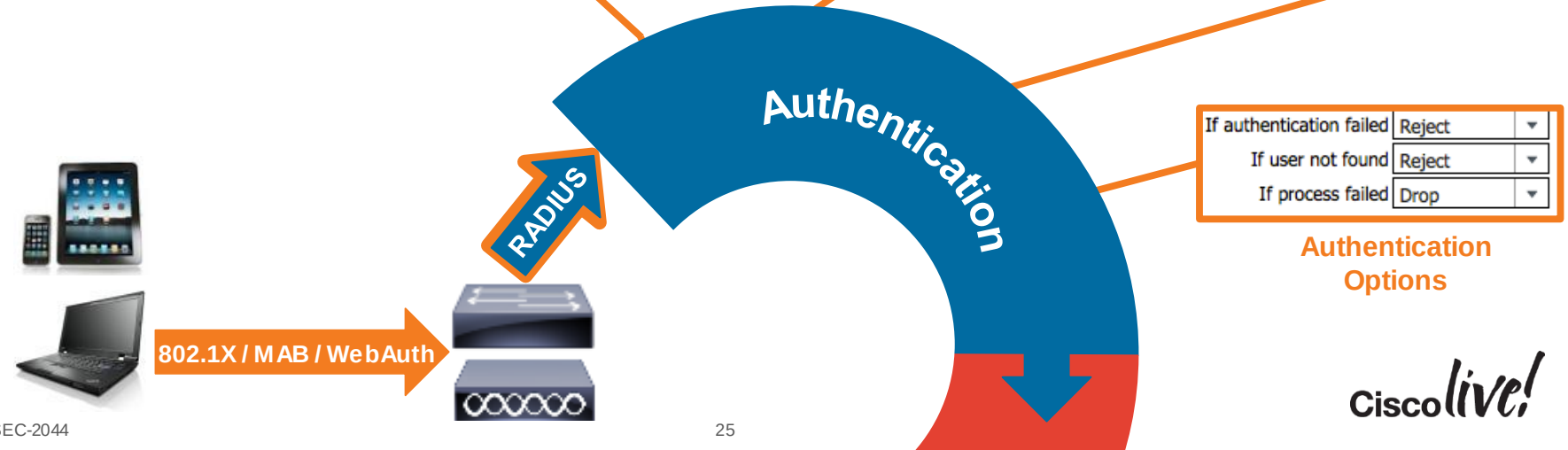
Authentication Rules

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

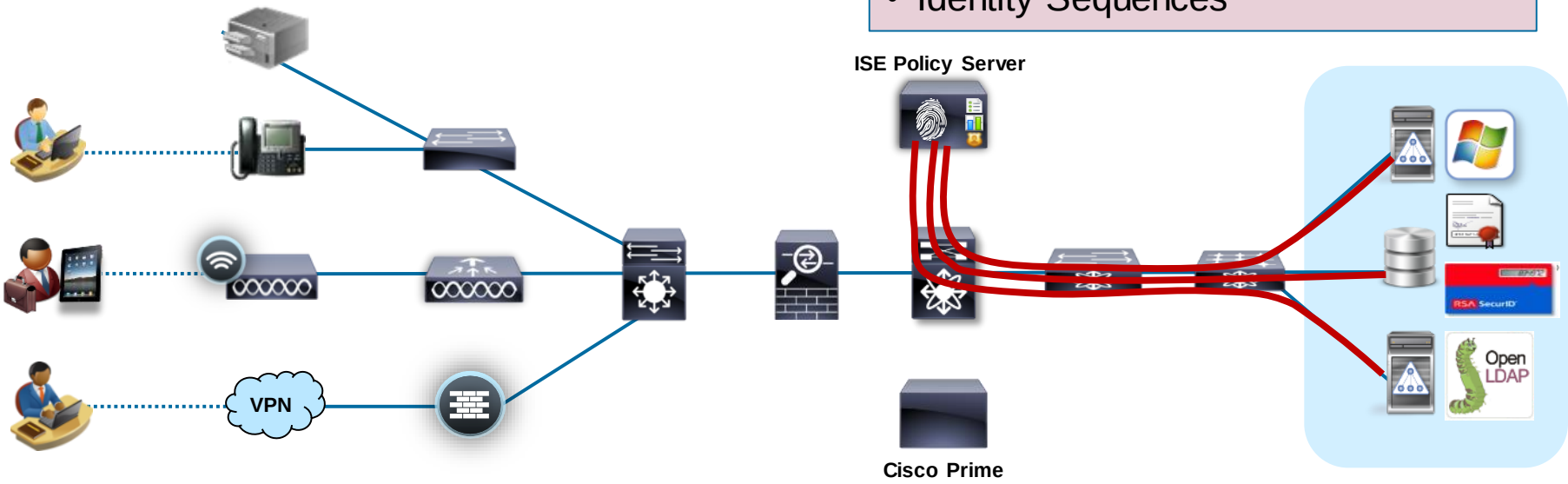


Authentication Options

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



Multi–Forest Active Directory Support

ISE 1.3 is designed for growing businesses. With support for multiple Active Directory domains, ISE 1.3 enables authentication and attribute collection across the largest enterprises.

- ✓ Support for 50 concurrent Active Directory join points
- ✓ No need for 2-way trust relationship between domains
- ✓ Advanced algorithms for dealing with identical usernames.

AD Authentication Flow

Active Directory Scopes > Default_Scop

Connection | Authenti

Use Domain Nar

S

Au

Poli

A

Allow Authe

Enable Selected

Active D

Defa

AN

SC

scop

scop

AN

Name			
AUSTRALIA.			
CANBERRA.AUSTRALIA.OCEANIA.ACS....	OCEANIA.ACS.COM	domain	NO
OCEANIA.ACS.COM	OCEANIA.ACS.COM	domain	NO
amer.acs.com	amer.acs.com	domain	YES
brazil.south.amer.acs.com	amer.acs.com	domain	YES

Identity Rewrite

Identity Rewrite allows usernames to be modified before they are applied to the Active Directory service. The rewrite results. ISE processes the policy in order, and the first condition which matches the request username

Identity Rewrite

Identity Rewrite allows usernames to be modified before they are applied to the Active Directory service. The rewrite results. ISE processes the policy in order, and the first condition which matches the request username in square brackets) may be used to transfer elements of the original username to the result. The Test facility p

- ○ Do not apply Rewrite Rules to modify username
- ◉ Apply the Rewrite Rules Below to modify username

Test rewrite Rules: Launch Test

* If Identity Matches	host/[HOSTNAME].[DOMAIN]	rewrite as	host/[HOSTNAME].[DOMAIN]
* If Identity Matches	host/[HOSTNAME]	rewrite as	host/[HOSTNAME]
* If Identity Matches	[DOMAIN]\[IDENTITY]	rewrite as	[DOMAIN]\[IDENTITY]
* If Identity Matches	[IDENTITY]@[DOMAIN]	rewrite as	[IDENTITY]@[DOMAIN]

Test Authentication

External Identity Sources

- Certificate Authentication Profile
- Active Directory
  - Default_Scope
  - scope1
  - scope2

Active Directory Scopes

Edit | Add | Delete | Node View | Advanced Tools

Name
Default_Scope
scope1

Advanced Tools:
- Test User for Scope
- Diagnostics Tool
- Advanced Tuning
- Enter Single Scope View

Can run from scope level

Active Directory Scopes > Default_Scope,scope2 > **AMER.ACS.COM**

Connection | Authentication Domains | Groups | Attributes | Advanced Settings

Scope **Default_Scope,scope2**

* Domain Name AMER.ACS.COM

Use Domain Name as Identity Store Name (First 32 characters)

Specify Identity Store Name

* Identity Store Name AMER.ACS.COM

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. S
Connection.

Join | Leave | Test User | Diagnositcs Tool | Refresh

Can run from AD Join Point

Test Authentication

Test User Authentication

* Username: acsadmin

* Password: ••••••••

Authentication Type: Kerberos

- **Kerberos**
- Lookup
- MS-RPC

Authorization Data:

Test

Authentication Result | Groups | Attributes

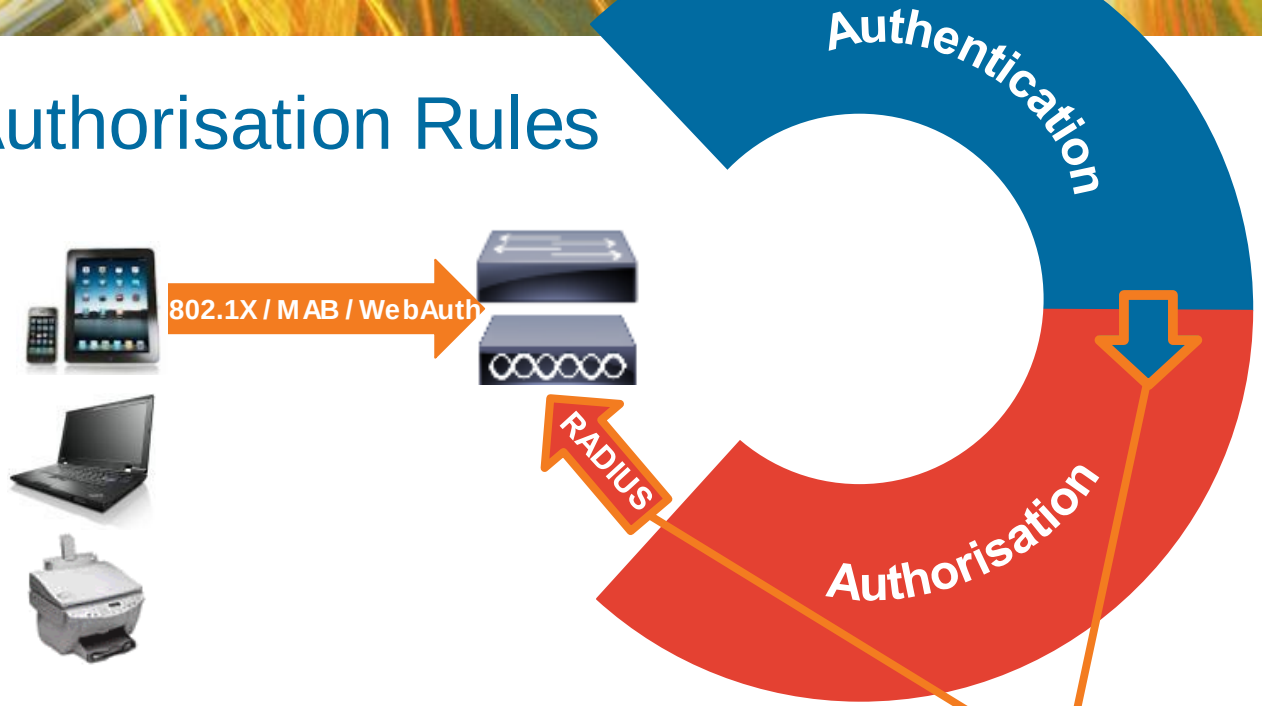
```
Test Username            : acsadmin
ISE NODE                 : dcmgash-ise3-cloud.cisco.com
Scope                    : Default_Scope
Instance                 : amer.acs.com

Authentication Result    : FAILED

Error                    : No such user
```

Different authentication types

ISE node can be selected to run the test auth

Can provide group & attribute details if options are selected

Authorisation Rules



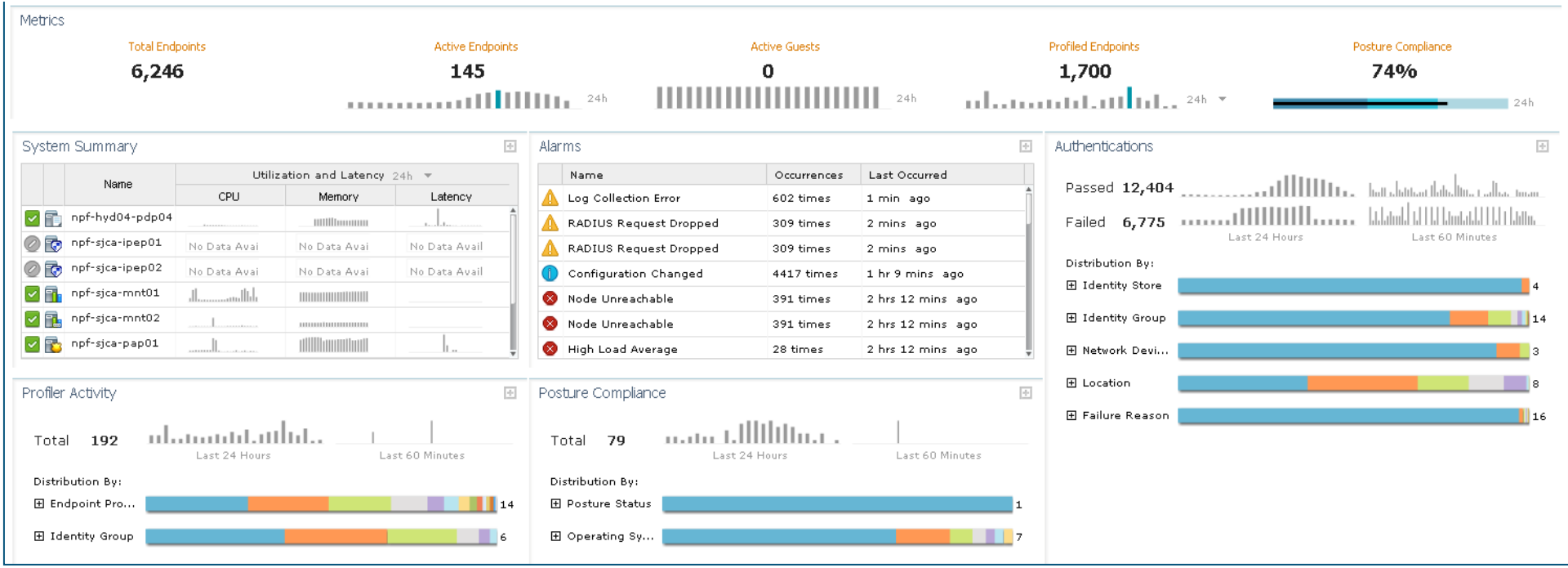
Return standard IETF RADIUS / 3rd-Party Vendor Specific Attributes (VSAs):

- 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



Detailed Visibility into Passed/Failed Attempts

Authentications | Reports | Endpoint Protection Service | Troubleshoot

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

Show Live Sessions | Add or Remove Columns | Refresh

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

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Server	Failure Reason
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	✓		sb							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	✓		yb							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
Policy Server	npf-sjca-pdp01
Event	5400 Authentication failed
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

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP
15048	Queried PIP
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

Authentications | Reports | Endpoint Protection Service | Troubleshoot

Show Live Authentications | Add or Remove Columns | Refresh | Reset Repeat Count

Refresh: Every 1 minute | Show: Latest 2

Repeat Count = 395

Initiated	Updated	Session Status	Repeat Count	Identity	IP Address	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/jiajiu-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

		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

Verification

Control

802.1X and MAB

Introduction

Profiling

AAA
(802.1x & MAB)

ISE Guest &
Employee WebAuth

Compliance
Desktop Posture
BYOD & MDM

PxGrid

TrustSec

ISE Deployment

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

Closed Mode

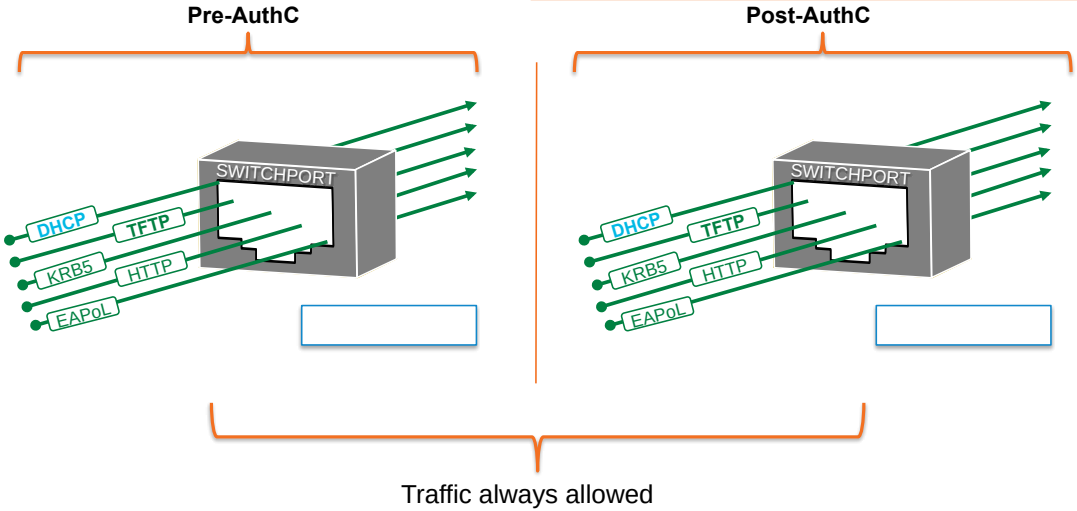
Monitor Mode

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 ☺



AuthC = Authentication
AuthZ = Authorisation

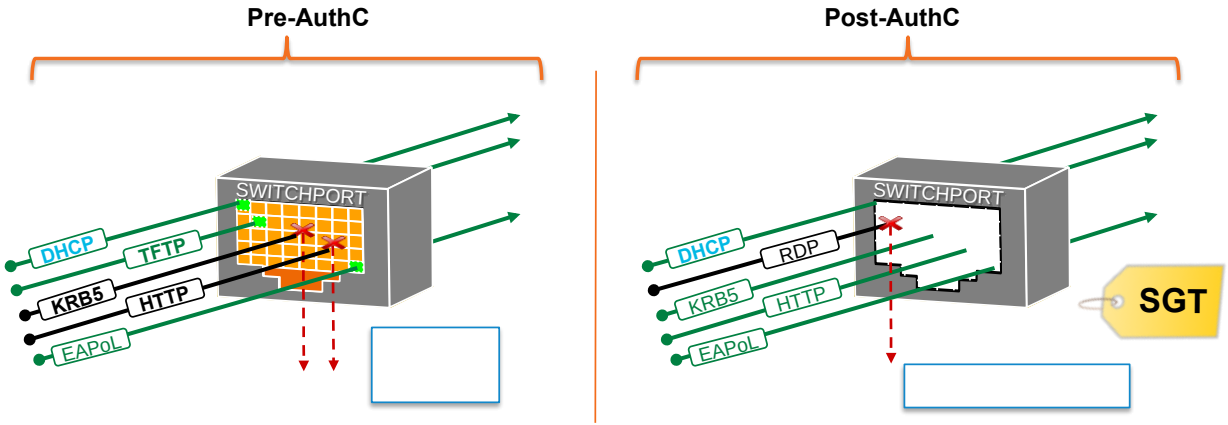
Low-Impact Mode

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…



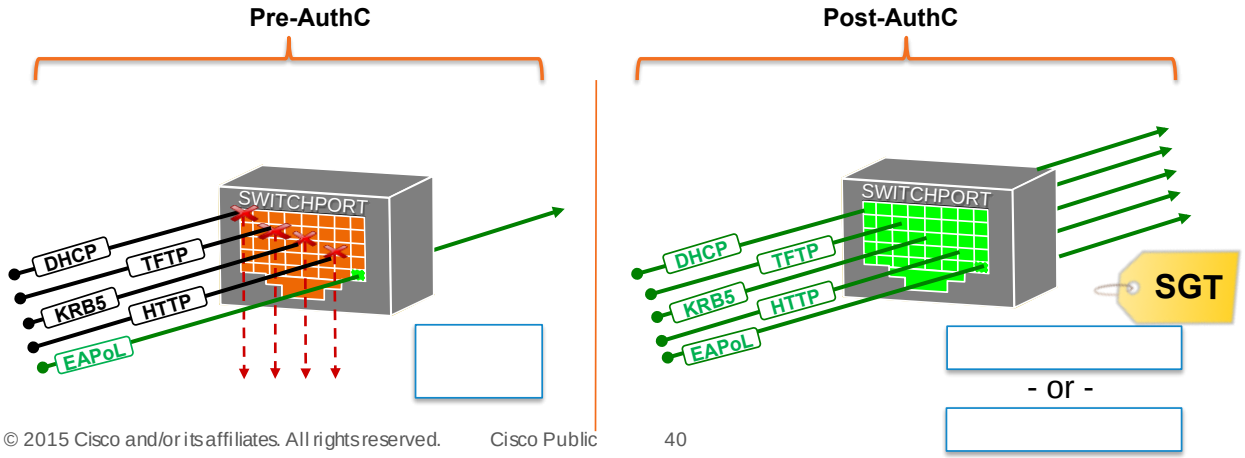
Closed Mode

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?

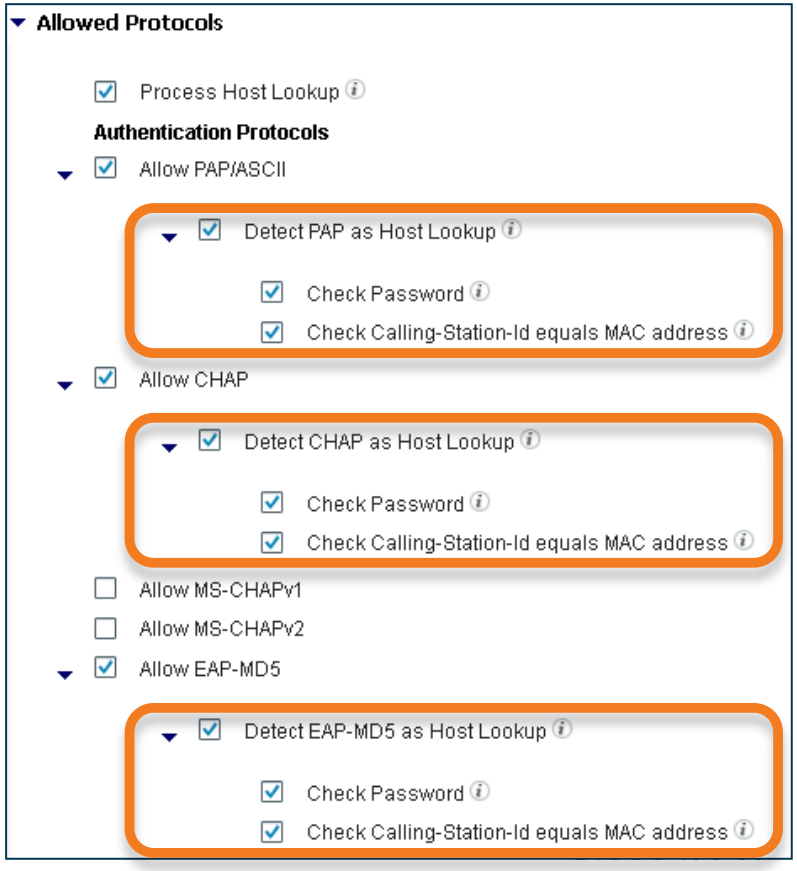
- A list of MAC Addresses that are allowed to “skip” authentication
- Is this a replacement for 802.1X?
  - No Way!
- This is a “Band-aid”
  - In a Utopia, ALL devices authenticate.
- List may be Local or Centralised
  - Can you think of any benefits to a centralised model?

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



Web Authentication

Introduction

Profiling

AAA
(802.1x & MAB)

ISE Guest &
Employee WebAuth

Compliance
Desktop Posture
BYOD & MDM

PxGrid

TrustSec

ISE Deployment

Handling Guests and Employees Without 802.1X

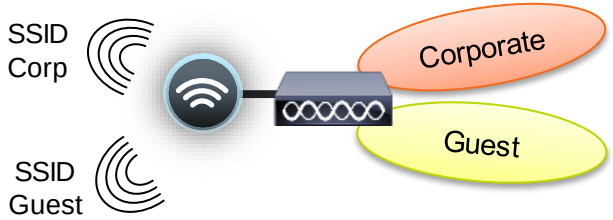
Employees and some non-user devices	802.1X	✓
All other non-user devices	MAB	✓
Guest Users		✗
Employees with Missing or Misconfigured Supplicants		✗

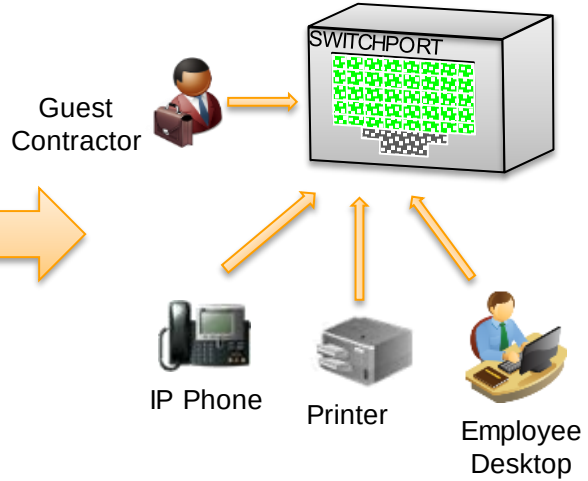
Username: Employee
Password: ****
Sign On

Username: Guest
Password: ****
Sign On

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:

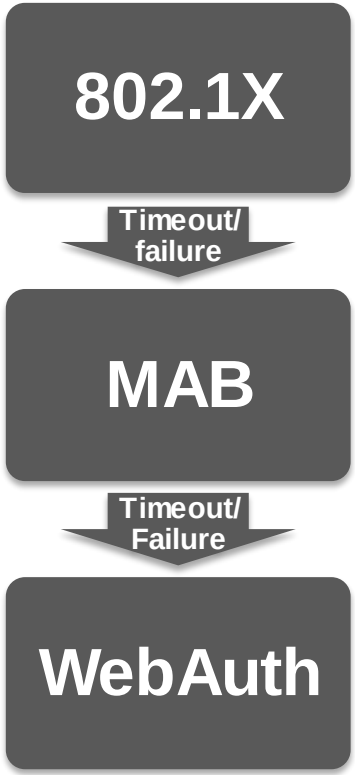
- No notion of SSID
- Unified port: Need to use different auth methods on single port ▸ Enter Flex Auth

Flex Auth

Converging Multiple Authentication Methods on a Single Wired Port

Interface Config

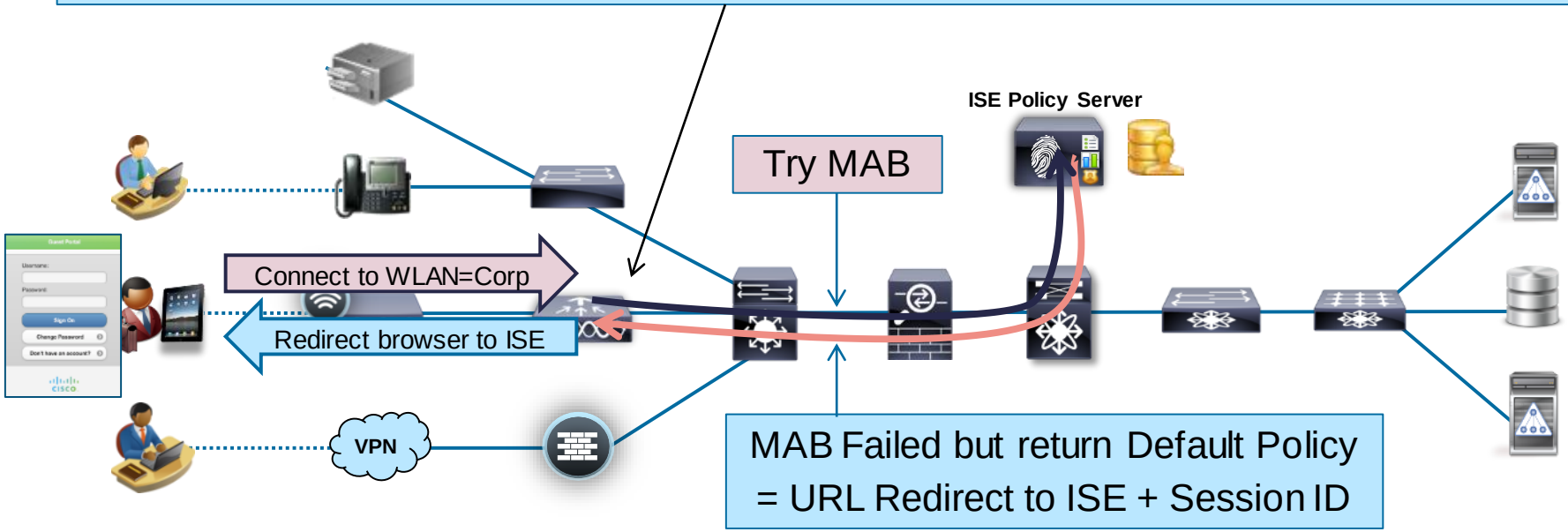
```
interface GigabitEthernet1/0/1
 authentication host-mode multi-auth
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
 !
 authentication event fail action next-method
 authentication order dot1x mab
 authentication priority dot1x mab
```



CWA Flow

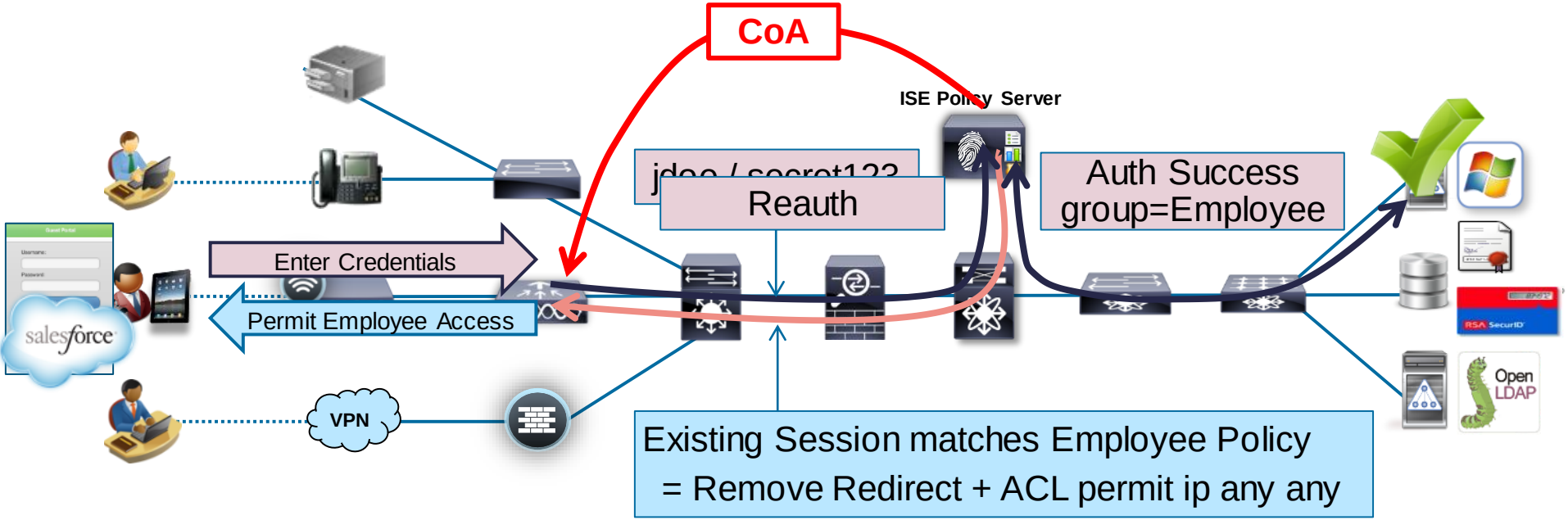
- Tracking session ID provides support for session lifecycle management including CoA.

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



CWA Flow

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



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

General | AVC Statistics

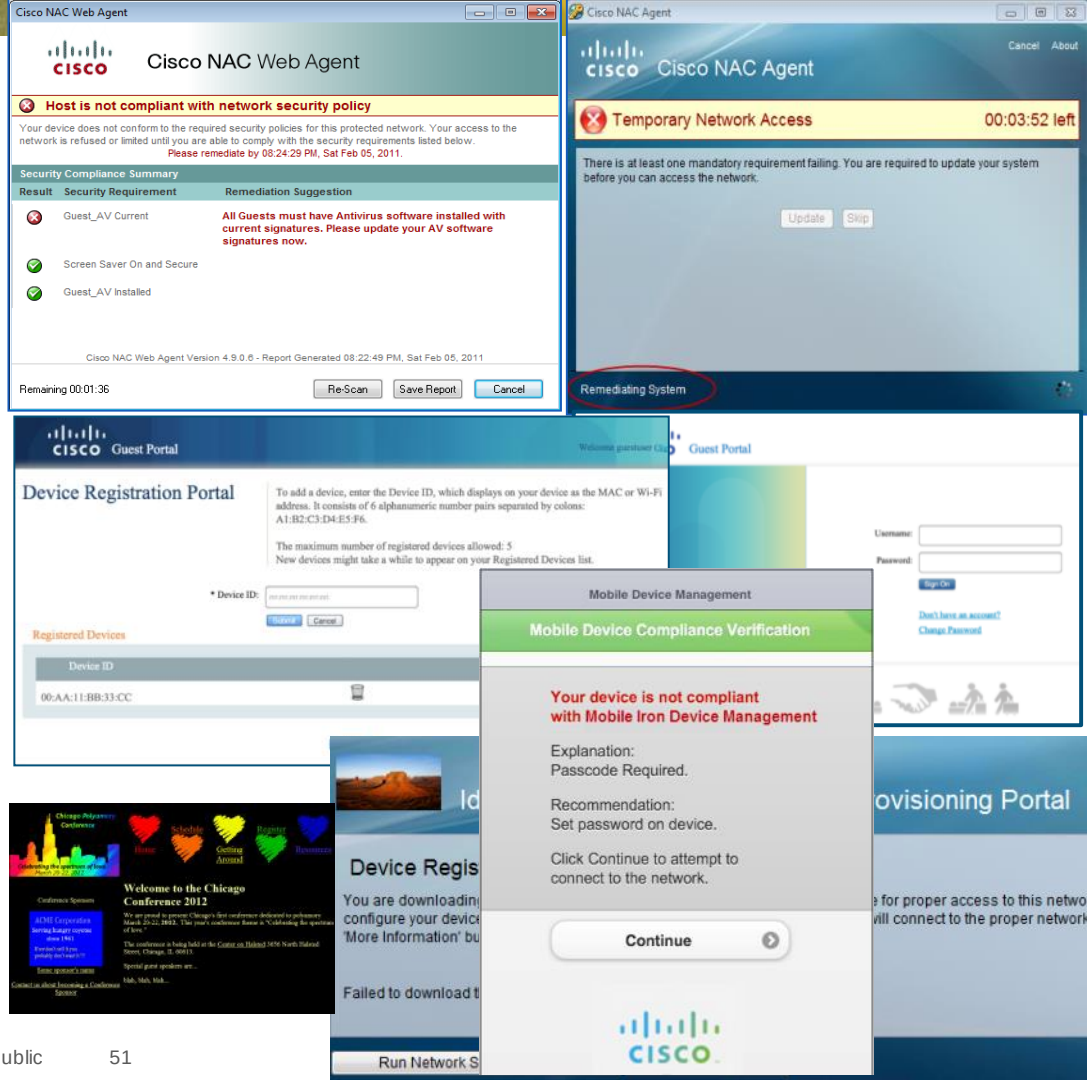
Client Properties

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



Session ID

Glue That Binds Client Session to Access Device and ISE

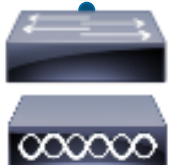
NAD: "show authentication session"

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

About that session…

Which one???

RADIUS



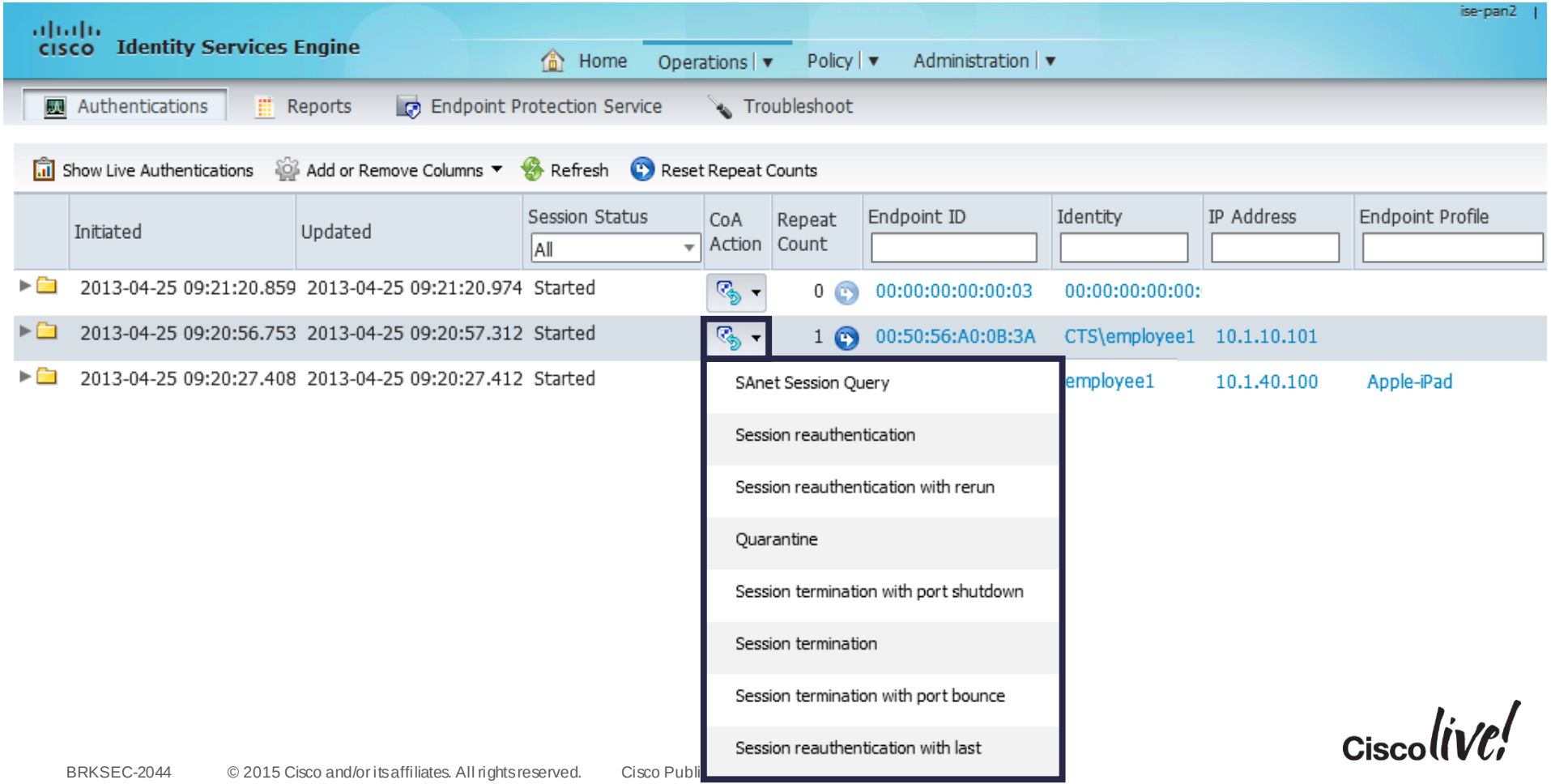
ISE: Detailed Authentication Report

```
⊟ Authentication Result
UserName=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
```

CoA from Live Sessions Log



Identity Services Engine Enhancements

Introduction

Profiling

AAA
(802.1x & MAB)

ISE Guest &
Employee WebAuth

Compliance
Desktop Posture
BYOD & MDM

PxGrid

TrustSec

ISE Deployment

ISE for Guest Access Management

Automate and Control the Entire Guest Lifecycle

Hotspot, Self Service, & Sponsor

Complete control over Guest Policy, with custom portals, for un-credentialed Internet access and employee-sponsored credentialed access.

Guests Tracking and Management

Track Guest access and activity across your network for security and compliance demands

Free up IT Support time

Self -provisioning & automated onboarding reduce the IT resource burden

Cisco ISE Guest

All New Guest Admin Experience

- Setup a Guest experience in 5 minutes!
- Flow Visualiser: see what guests will experience
- Customisation Preview: See your customisation real time

All User Facing Pages Customisable

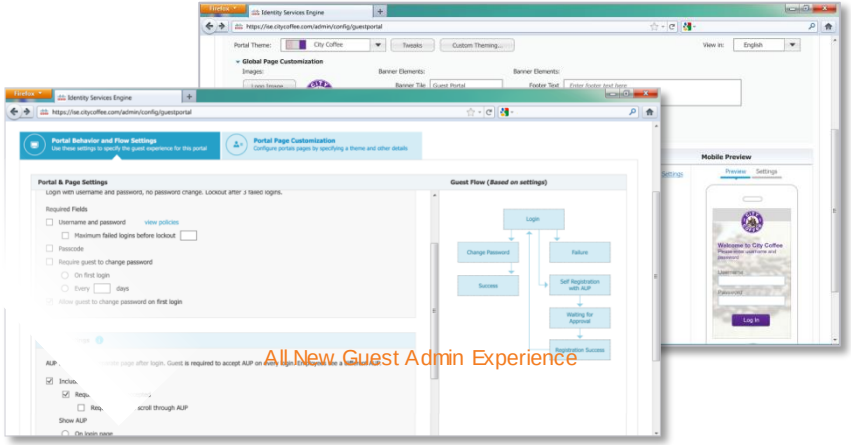
- Includes: Guest, Sponsor, My Devices Portals and receipts via print, email & SMS
- Robust WYSIWYG customisation with Themes
- Standards based CSS & HTML for Advanced Admins

Out-of-the-box Guest Flows

- Hotspot
- Self Service with SMS Notifications & Approvals
- Brand-able Sponsor Portal (*Mobile and Desktop*)

Guest REST API

- Create and manage guest accounts
- Search, filter and bulk operation support



All New Guest Admin Experience

Guests

Branded Sponsor Portal

Receipts
Print, Email and SMS

Branded Guest Receipts & Notifications

Guest Receipts with Your Brand

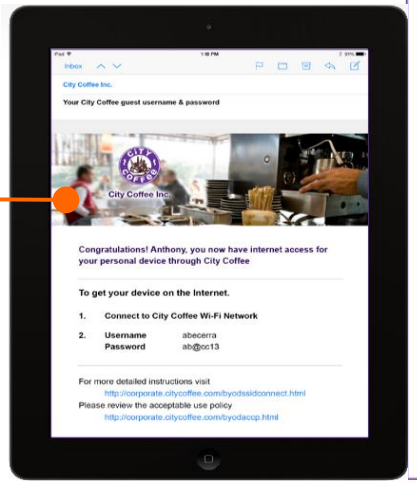
Whether you're delivering guest credentials on the printed page, over email or SMS, ISE makes it easy to deliver your complete branded experience.

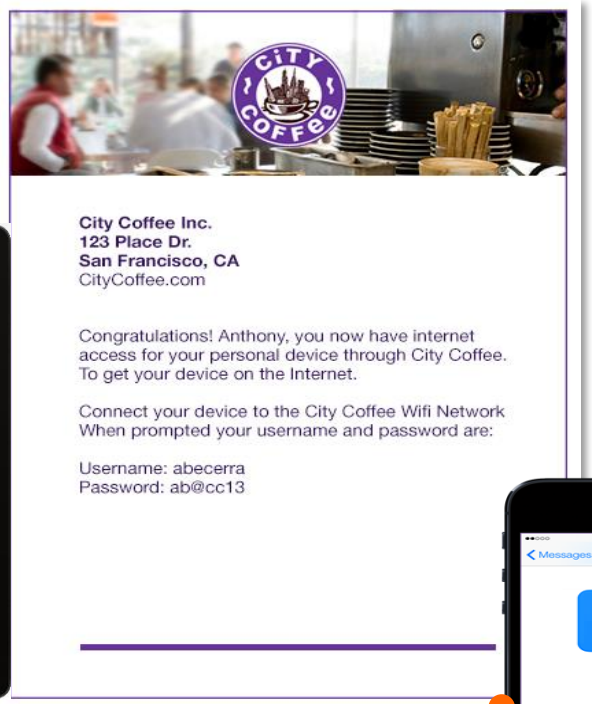
Email Notifications

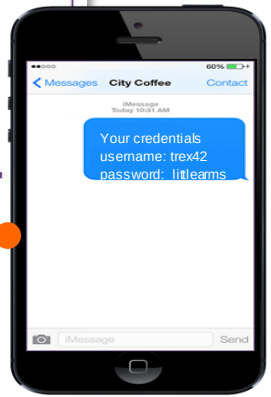
Do you have Guests visiting? Send them login credentials before they even arrive!

SMS Notifications

Send credentials directly to a guests mobile phone.



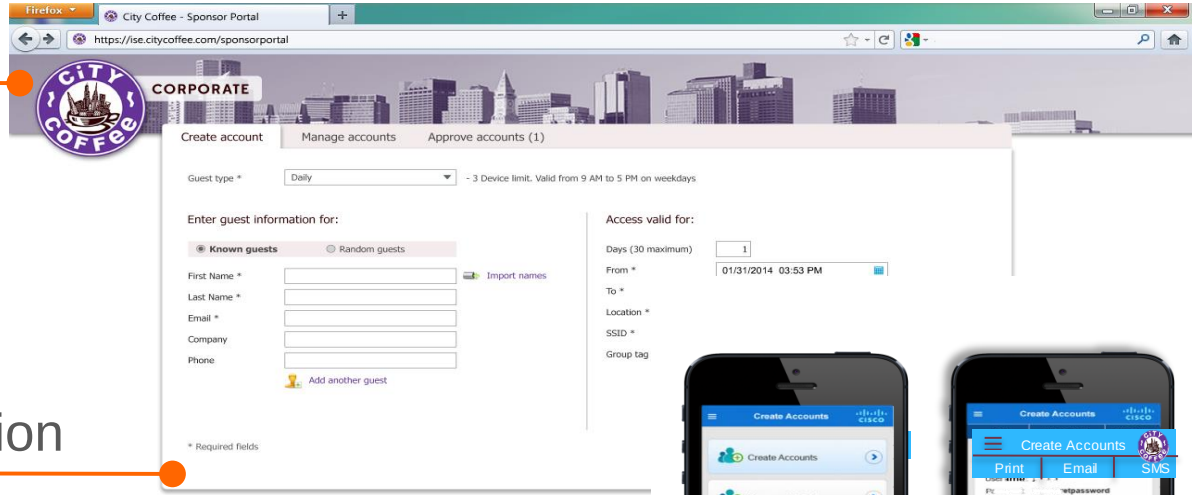




Sponsor Portal

Branding with Themes!

Themes give you complete control over the look and feel of your sponsor Portal. Use our out-of-the-box themes or create your own using *ThemeRoller for jQuery Mobile* or standard CSS.

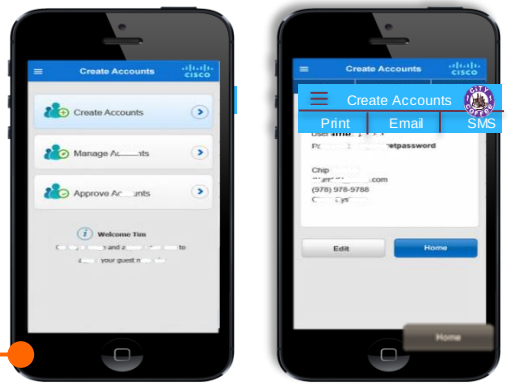


Streamlined Guest Creation

Set up your sponsor portal to show only the fields you need for your business.

Mobile Sponsors

You are free to move about the cabin! Create and manage guest accounts from your mobile phone or tablet.

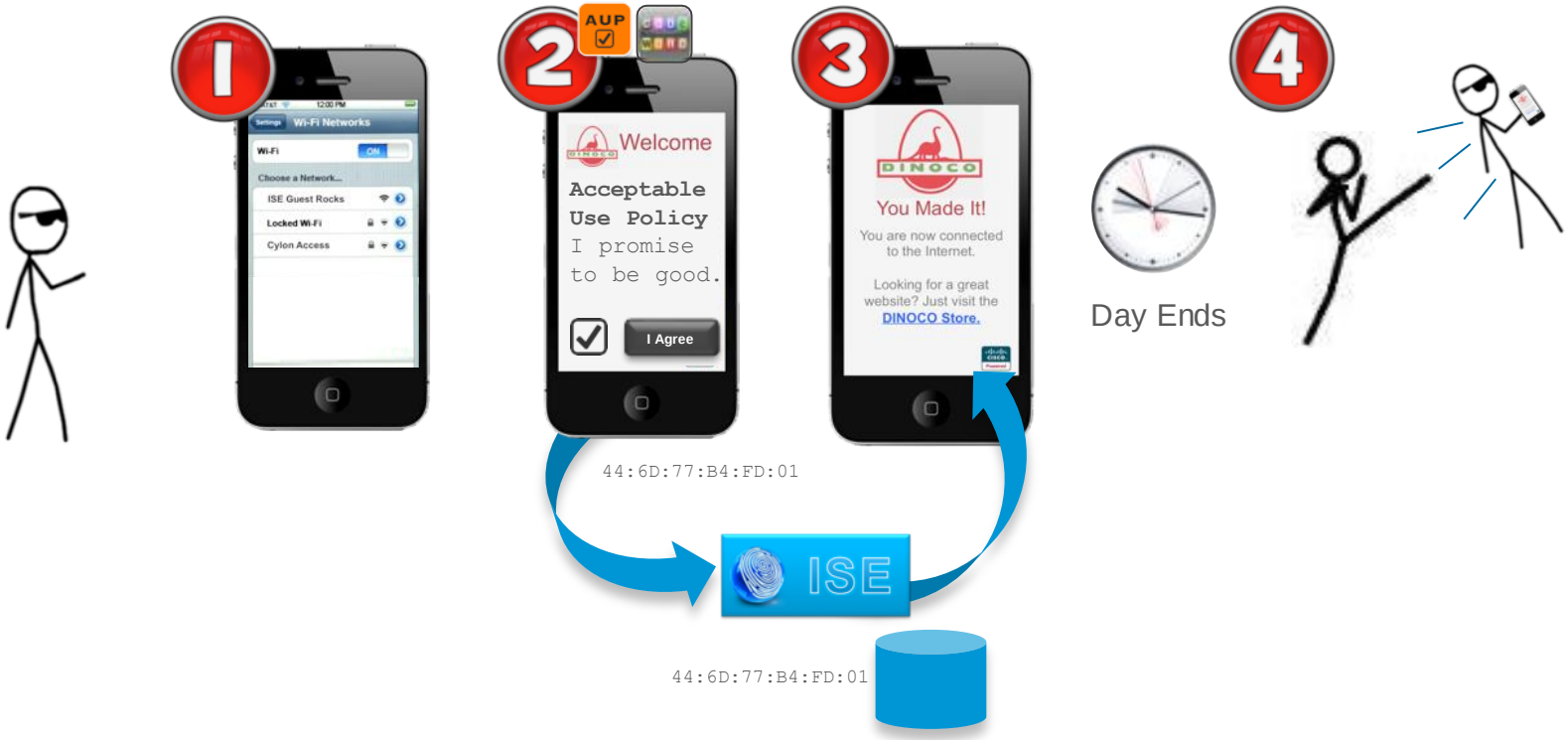


Basic Supported Guest Flows

1. Hotspot
2. Self Service
3. Self Service Sponsor Approved
4. Sponsored

Hotspot

Guest Flow #1

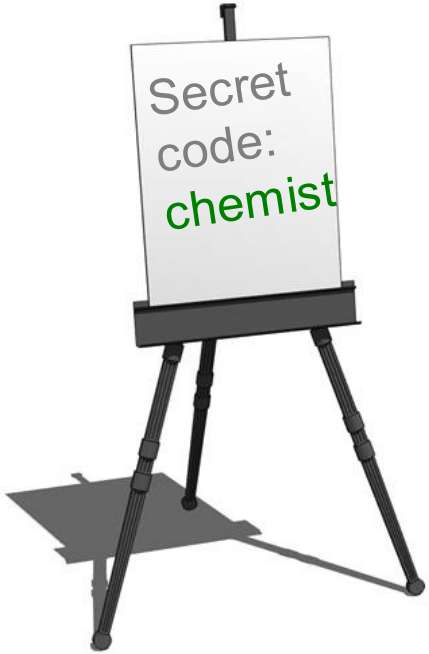


Goal: Get them on the Internet with AUP acceptance no matter who they are and remember who they are next time so you don't get in their way.

Secret Code Controls Access to Guest Wi-Fi

Registration code: require the user to enter a code before completing a self service registration.

Access code: require the user to enter a code before accessing a hotspot or logging in using guest credentials.



Self Service with Email Verification

Guest Flow #2

Fill In A Simple Form

Check Your Email

Connect to WFI

Self Service with SMS

Guest Flow #2

Goal: Get them on the Internet as long as you have a 3rd party identifier that proves who the user is.

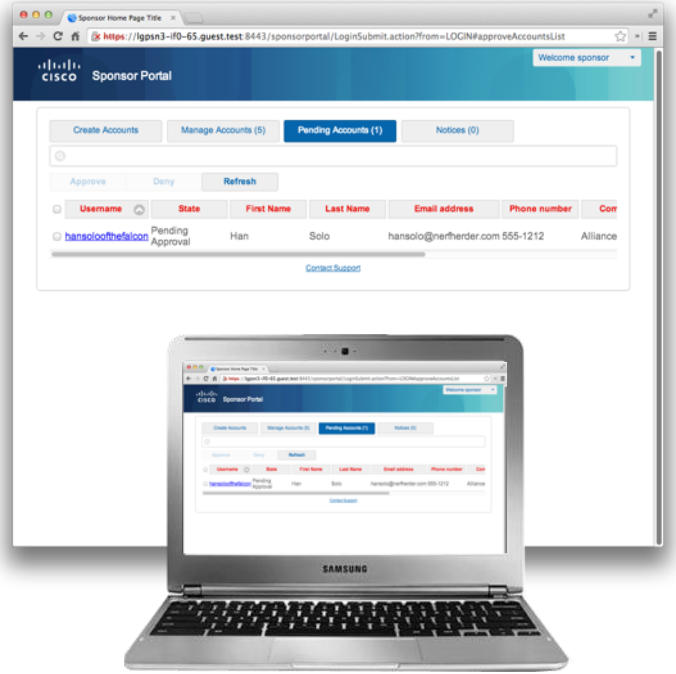
Self Registration with Sponsored Approval

Guest Flow #3

ISE sends email requesting approval

Logs into Sponsor Portal and Approves or rejects

Approving Self Registration Requests



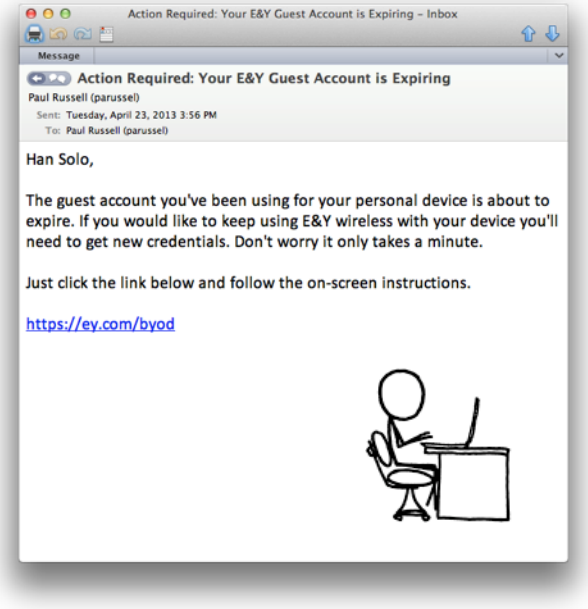
DESKTOP

Mobile

Sponsored Flow

Guest Flow #4

Pre-Expiration Notification



DESKTOP

Mobile

Posture

Are My Endpoints Compliant?

Introduction

Profiling

AAA
(802.1x & MAB)

ISE Guest &
Employee WebAuth

Compliance
Desktop Posture
BYOD & MDM

PxGrid

TrustSec

ISE Deployment

Posture Assessment

Does the Device Meet Security Requirements?

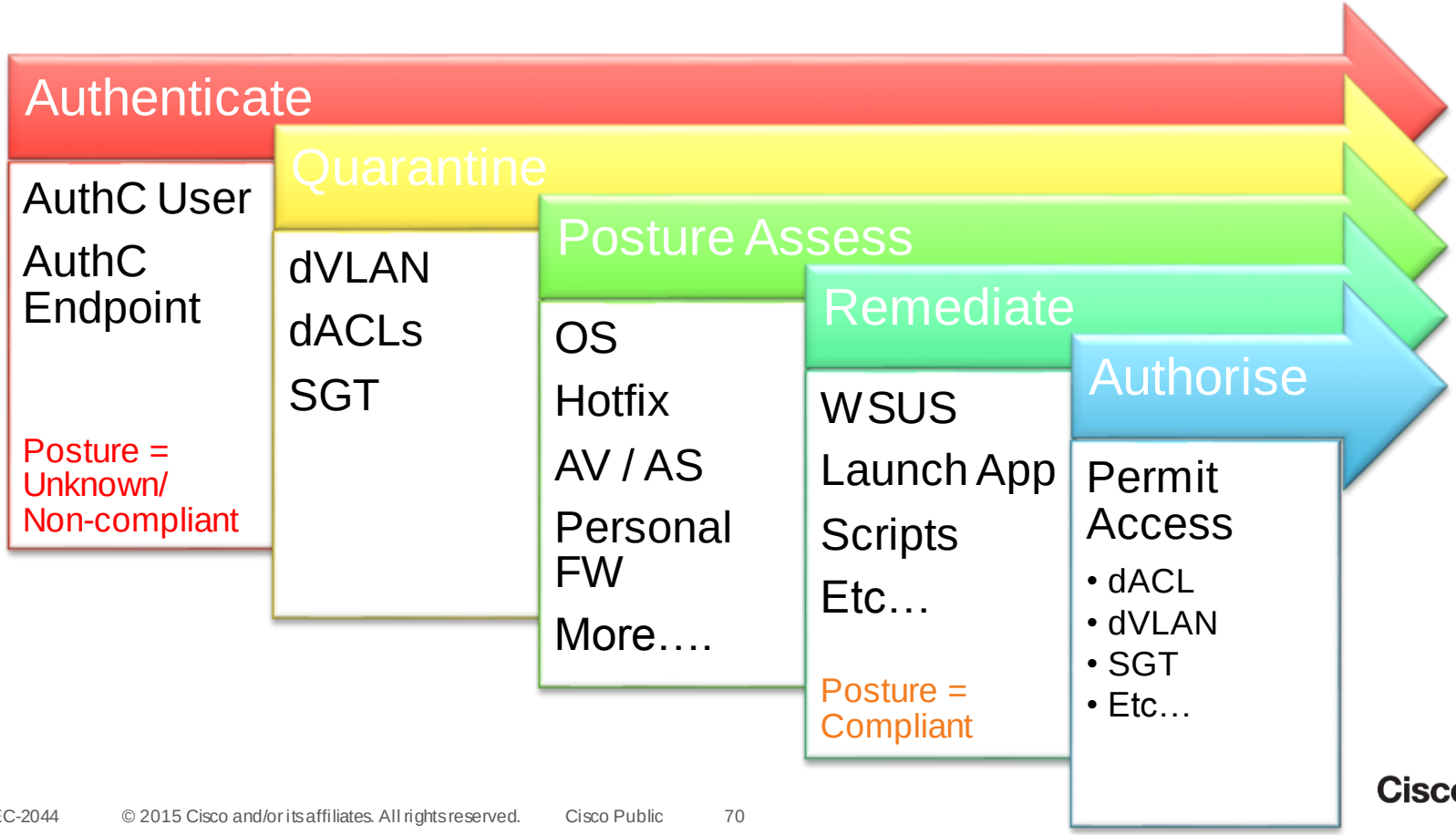
Posture

- Posture = The state-of-compliance with the company's security policy.

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

- Extends the user / system Identity to include Posture Status.

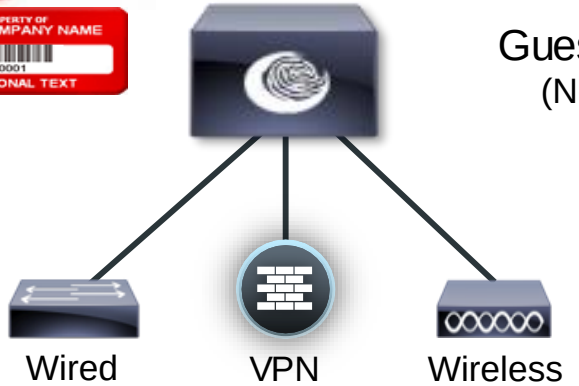
ISE Posture Assessment



ISE – Posture Policies

Employee Policy:

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



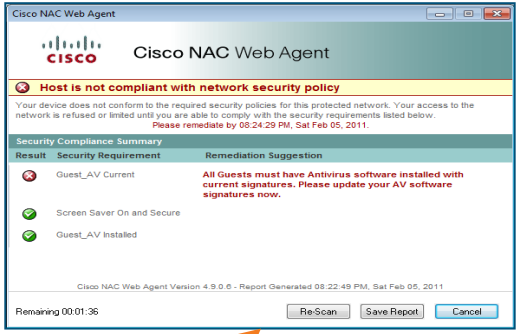
Employees

Contractors/Guests

Contractor Policy:

- Any AV installed, running, and current

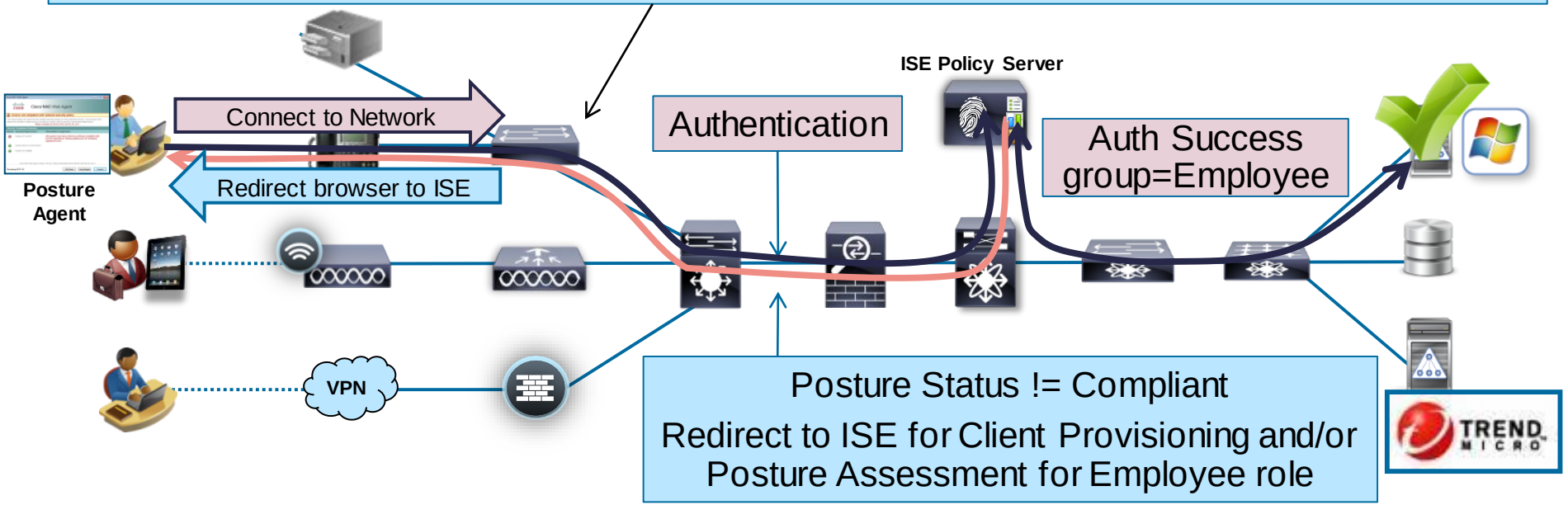
Guest Policy: Accept AUP
(No posture - Internet Only)



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

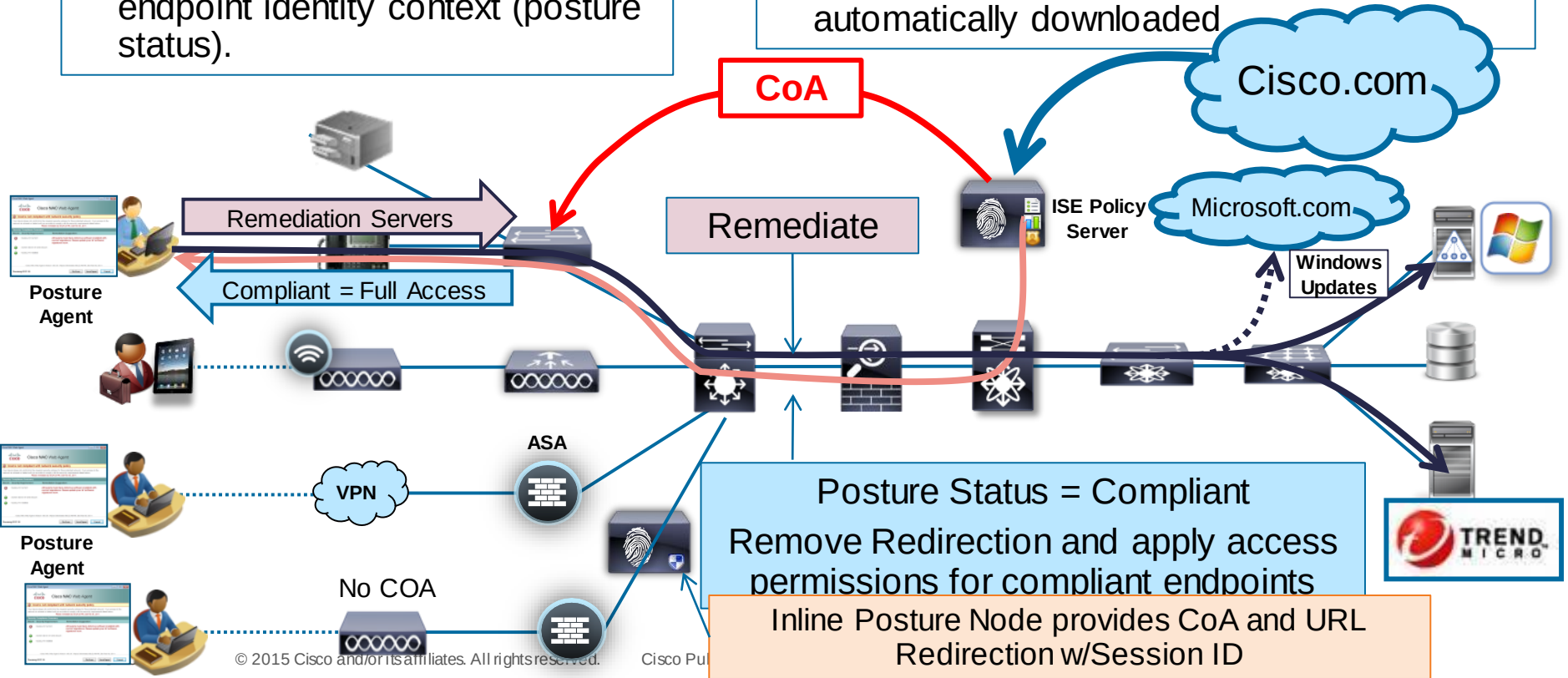
https://ise.company.com:8443/guestportal/gateway?sessionId=0A010A...73691A&action=**cpp**



Posture Remediation and Client Resources

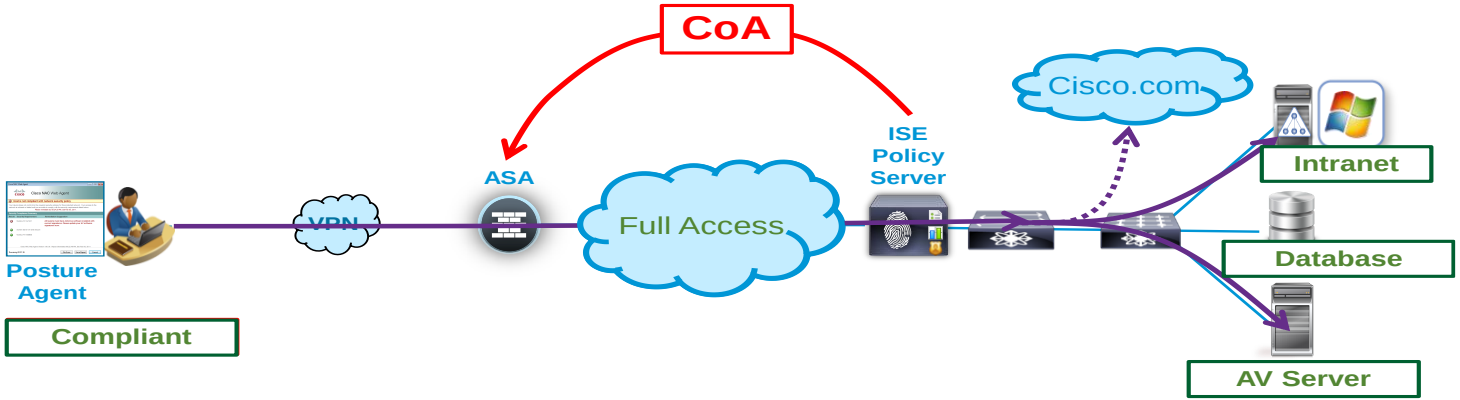
- CoA allows re-authentication to be processed based on new endpoint identity context (posture status).

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

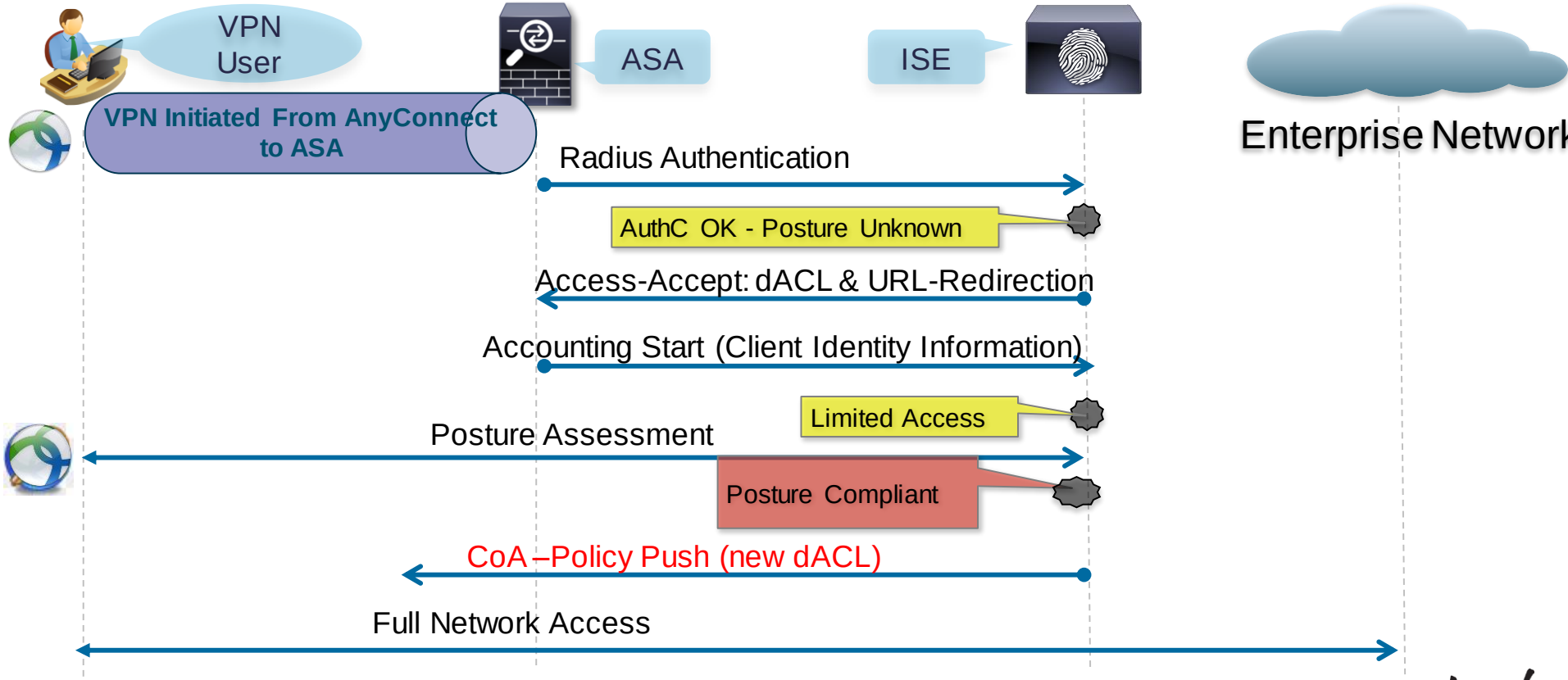


ASA/ISE Integration Feature Overview

- Support VPN posture specifically between the ASA & ISE deployments
- **Remove** the requirements for IPN (Inline Posture Node) in ASA/VPN/ISE deployments.
  - IPN is a device that would sit behind the ASA and enforce ISE policy



ASA Posture Assessment Flow



BYOD

Extending Network Access to Personal Devices

Introduction

Profiling

AAA
(802.1x & MAB)

ISE Guest &
Employee WebAuth

Compliance
Desktop Posture
BYOD & MDM

PxGrid

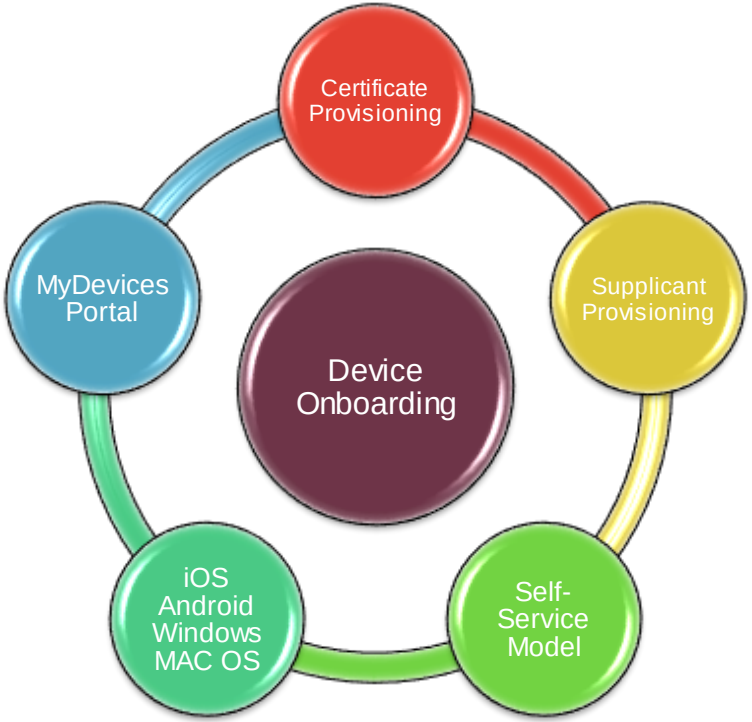
TrustSec

ISE Deployment

BYOD

Onboarding Personal Devices

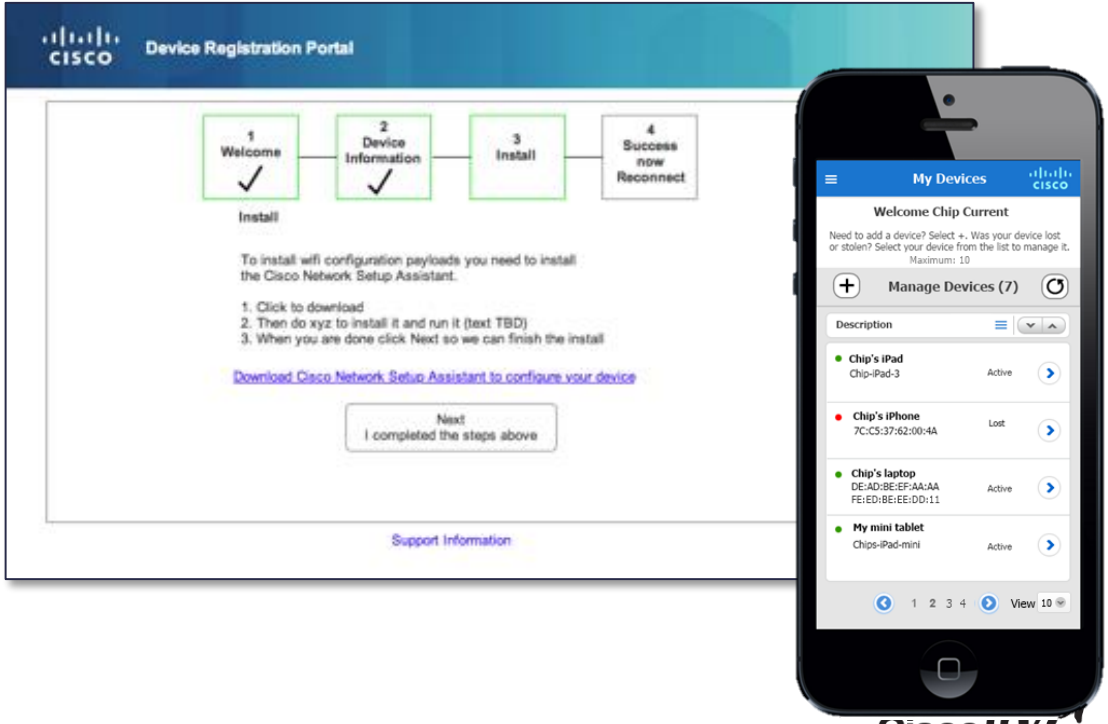
Registration, Certificate and Supplicant Provisioning



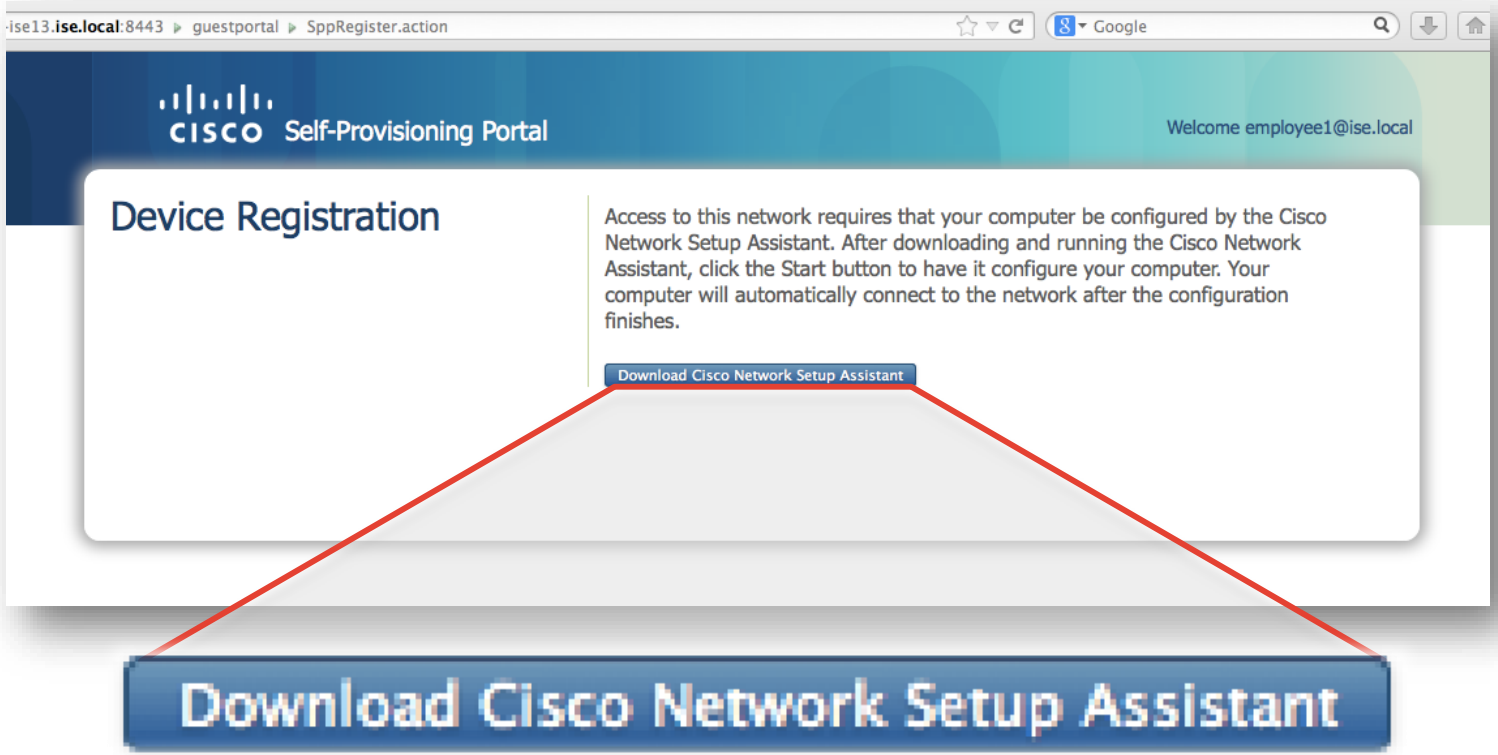
- Provisions device Certificates.
  - Based on Employee-ID & Device-ID.
- Provisions Native Supplicants:
  - Windows: XP, Vista, 7 & 8
  - Mac: OS X 10.6, 10.7, 10.8, 10.9 & 10.10
  - iOS: 4, 5, 6, 7 & 8
  - Android – 2.2 and above
  - 802.1X + EAP-TLS, PEAP & EAP-FAST
- Employee Self-Service Portal
  - Lost Devices are Blacklisted
  - Self-Service Model reduces IT burden
- Single and Dual SSID onboarding.

Walk Through BYOD Onboarding

- Out of the box flow walks users through onboarding.
- Fully customisable user experience with Themes.
- My Devices gives end users control to add an manage their devices.
- Mobile and desktop ready out of the box.

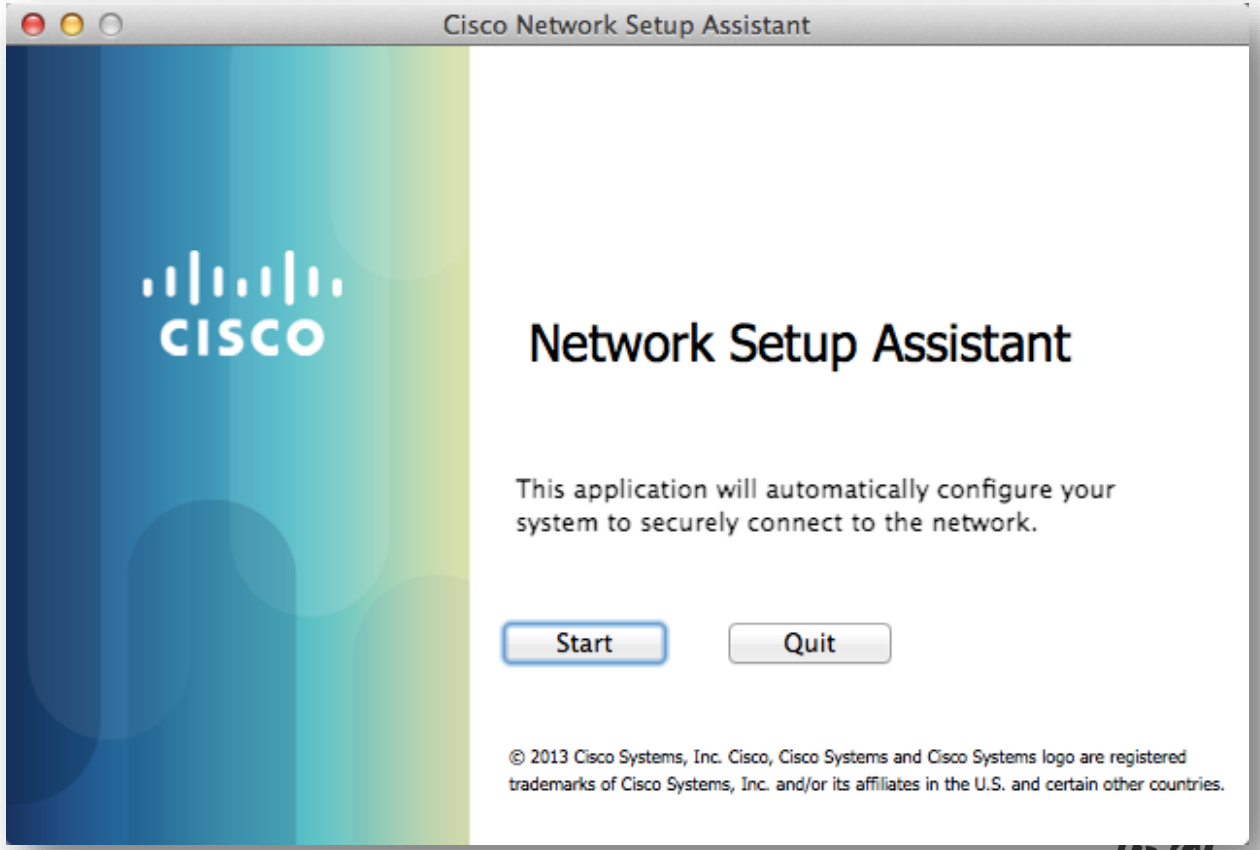


Java-Less Provisioning



Java-Less Provisioning

- Downloads as DMG
- Double-Click to Run App



Certificate Renewals

1.2.1

	Works	Comments
Before Expiry		
iOS	✓	
Android	✓	
Windows	✓	
MAC-OSX	✓	
After Expiry		
iOS	✓	
Android	✓	
Windows	✗	Supplicant will not use an expired cert
MAC-OSX	✓	Not tested yet

Allowing Expired Certificates

1.2.1

- Allow EAP-TLS
  - Allow Expired Certificates
- Allow LEAP
- Allow PEAP

  PEAP Inner Methods
  - Allow EAP-MS-CHAPv2
    - Allow Password Change Retries 1 (Valid Range 0 to 3)
  - Allow EAP-GTC
    - Allow Password Change Retries 1 (Valid Range 0 to 3)
  - Allow EAP-TLS
    - Allow Expired Certificates
  - Allow PEAPv0 only for legacy clients
- Allow EAP-FAST

  EAP-FAST Inner Methods
  - Allow EAP-MS-CHAPv2
    - Allow Password Change Retries 3 (Valid Range 0 to 3)
  - Allow EAP-GTC
    - Allow Password Change Retries 3 (Valid Range 0 to 3)
  - Allow EAP-TLS
    - Allow Expired Certificates
  - Use PACs / Don't Use PACs

Option to allow expired certs for:

- Pure EAP-TLS
- EAP-TLS as an Inner Method

Redirect Expired Certs

1.2.1

Authorization Policy

Exceptions (0)

Standard

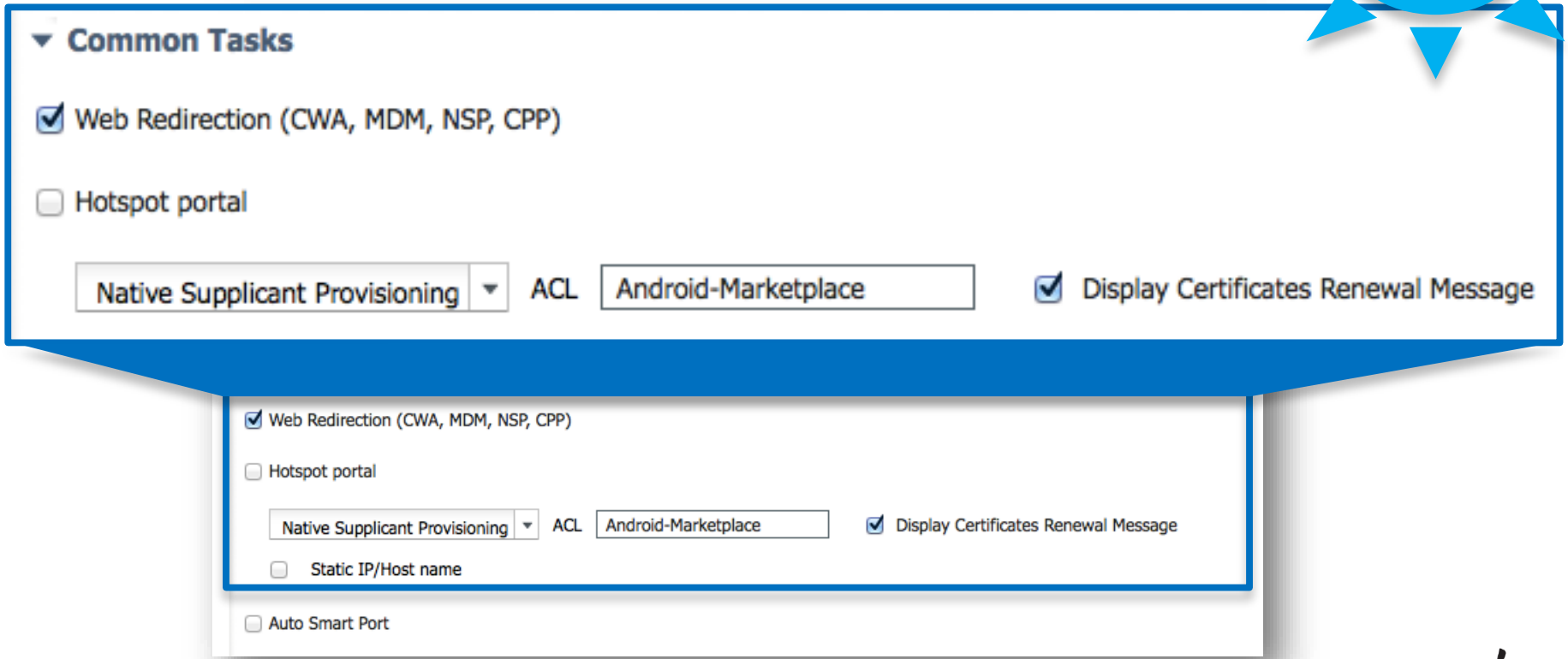
Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
✓	ExpiredCerts-WinThings	if (CERTIFICATE:Days to Expiry LESS 14 AND EndPoints:EndPointPolicy EQUALS Microsoft-Device)	then	NSP_Expired
✓	ExpiredCerts-Others	if CERTIFICATE:Days to Expiry LESS 1	then	NSP_Expired
✓	NSP	if Network Access:EapTunnel EQUALS PEAP	then	BYOD AND NSP
✓	Employee Full Access	if CWA:CWA_ExternalGroups EQUALS ise.local:ise.local/Users/Employees	then	PermitAccess AND Employee
✓	TLS-Accept	if Network Access:EapAuthentication EQUALS EAP-TLS	then	BYOD AND CWAchain
✓	Default	if no matches, then DenyAccess		

Windows

Everything Else

Certificate Renewal: Optional Message

1.2.1

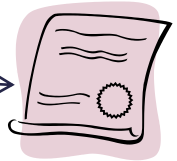


Single Versus Dual SSID Provisioning

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

SSID = BYOD-Closed (802.1X)

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



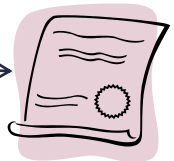
WLAN Profile
SSID = BYOD-Closed
EAP-TLS
Certificate=MyCert

- 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)

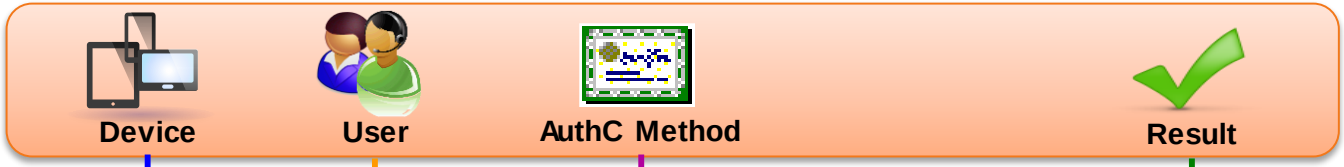
Client Provisioning Policy

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

ISE BYOD Certificate Configuration

SCEP Enrollment Profile and CA Certificate Import

Administration > System > Certificates > SCEP CA Profiles

SCEP Certificate Authority Certificates > SCEP

Edit Profile

SCEP Certificate Authority

* Name	SCEP
Description	URL for Simple Certificate Enrollment to CA Server
* URL	**http://ad.cts.local/certsrv/mscep**
Certificate Request Agent Certificate	**AD-MSCEP-RA**

Test Connectivity

The SCEP server certificate and CA and registration authority (RA) certificates of the certificate chain for the SCEP server are automatically retrieved into the Cisco® ISE trust store.

Administration > System > Certificates > Certificate Store

Certificate Store

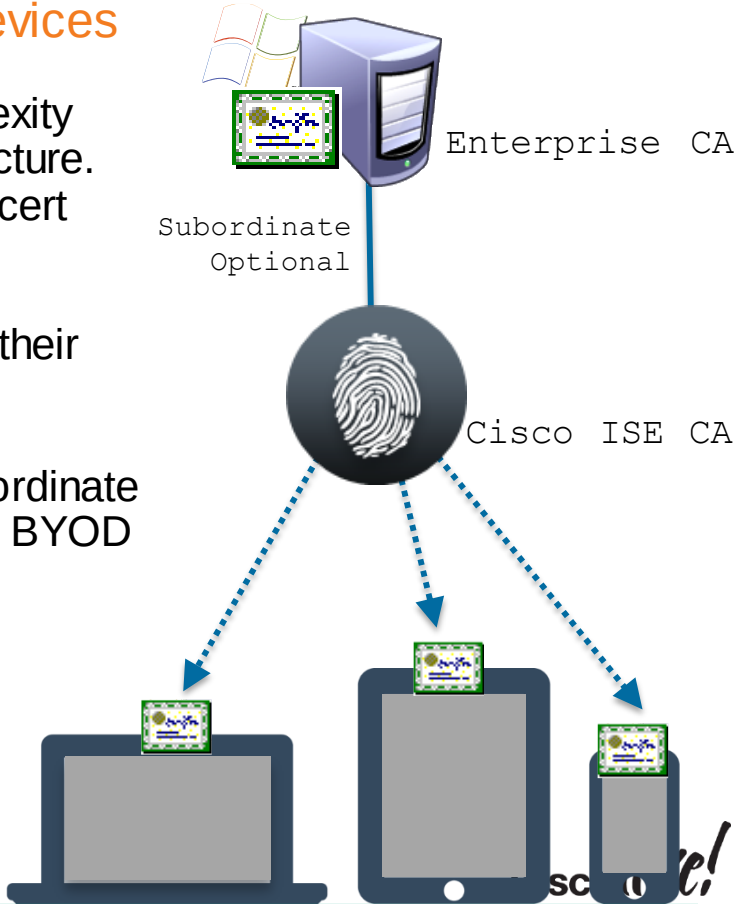
Edit | Import | Export | Delete | Show All

Friendly Name	Issued To	Issued By	Valid From	Expiration Date	Status
AD CA Server cert	cts-ad-ca	cts-ad-ca	Wed, 14 Mar 2012	Tue, 14 Mar 2017	✓
SCEP Cert	AD-MSCEP-RA	cts-ad-ca	Wed, 14 Mar 2012	Fri, 14 Mar 2014	✓
ise-byod.cts.local#ise-byod.cts.local#00001	ise-byod.cts.local	ise-byod.cts.local	Sun, 1 Apr 2012	Mon, 1 Apr 2013	✓

ISE 1.3: Internal Certificate Authority

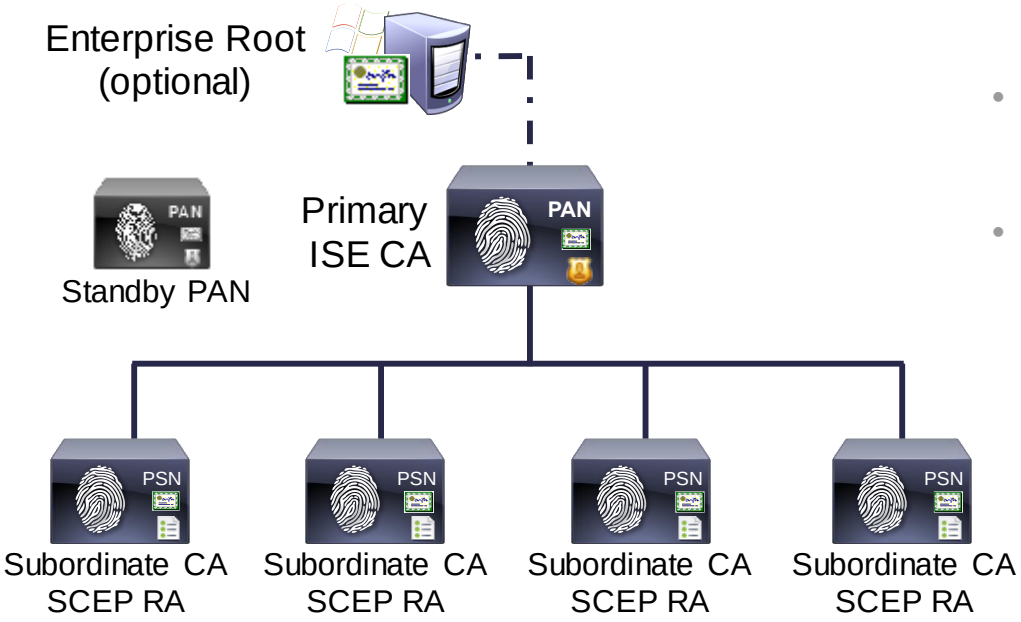
Simplifying certificate management for BYOD devices

- Managing certificates for BYOD adds significant complexity and expense when using Microsoft Public Key Infrastructure. The ISE Certificate Authority is designed to work in concert with your existing PKI to simplify BYOD deployments.
- Single Management Console – Manage endpoints and their certs. Delete an endpoint ISE deletes the cert.
- Simplified deployment – Supports stand alone and subordinate deployments. Removes corporate PKI team from every BYOD interaction.



***Designed for BYOD and MDM use-cases only, not a general purpose CA**

PKI Hierarchy and Roles



- Primary PAN is Root CA for ISE deployment
- All PSNs are Subordinate CAs to PAN

  PSNs are SCEP Registration Authorities (RAs)
- ISE PAN may be Subordinate to an existing Root CA or may be Standalone Root.
- Promotion of Standby PAN:

  Will not have any effect on operation of the subordinate CAs.

  For Standby to become Root CA must manually install the Private/Public keys from Primary PAN.

Native Supplicant Profile

Identity Services Engine

Home | Operations

Policy Sets | Profiling | Posture | Client Provisioning | TrustSec

Dictionaries | Conditions | Results

Results

- Authentication
- Authorization
- Profiling
- Posture
- Client Provisioning
  - Resources
- TrustSec

Native Supplicant Profile > New Supplicant Profile

Native Supplicant Profile

* Name: NSP-InternalCA

Description: Native Supplicant Provisioning Profile That Uses Internal CA

* Operating System: ALL

* Connection Type: ☑ Wired ☑ Wireless

*SSID: CTS-CORP

Security: WPA2 Enterprise

* Allowed Protocol: TLS

* Certificate Template: CTS-BYOD

Submit | Cancel

* Operating System: ALL

* Connection Type: ☑ Wired ☑ Wireless

*SSID: CTS-CORP

Security: WPA2 Enterprise

* Allowed Protocol: TLS

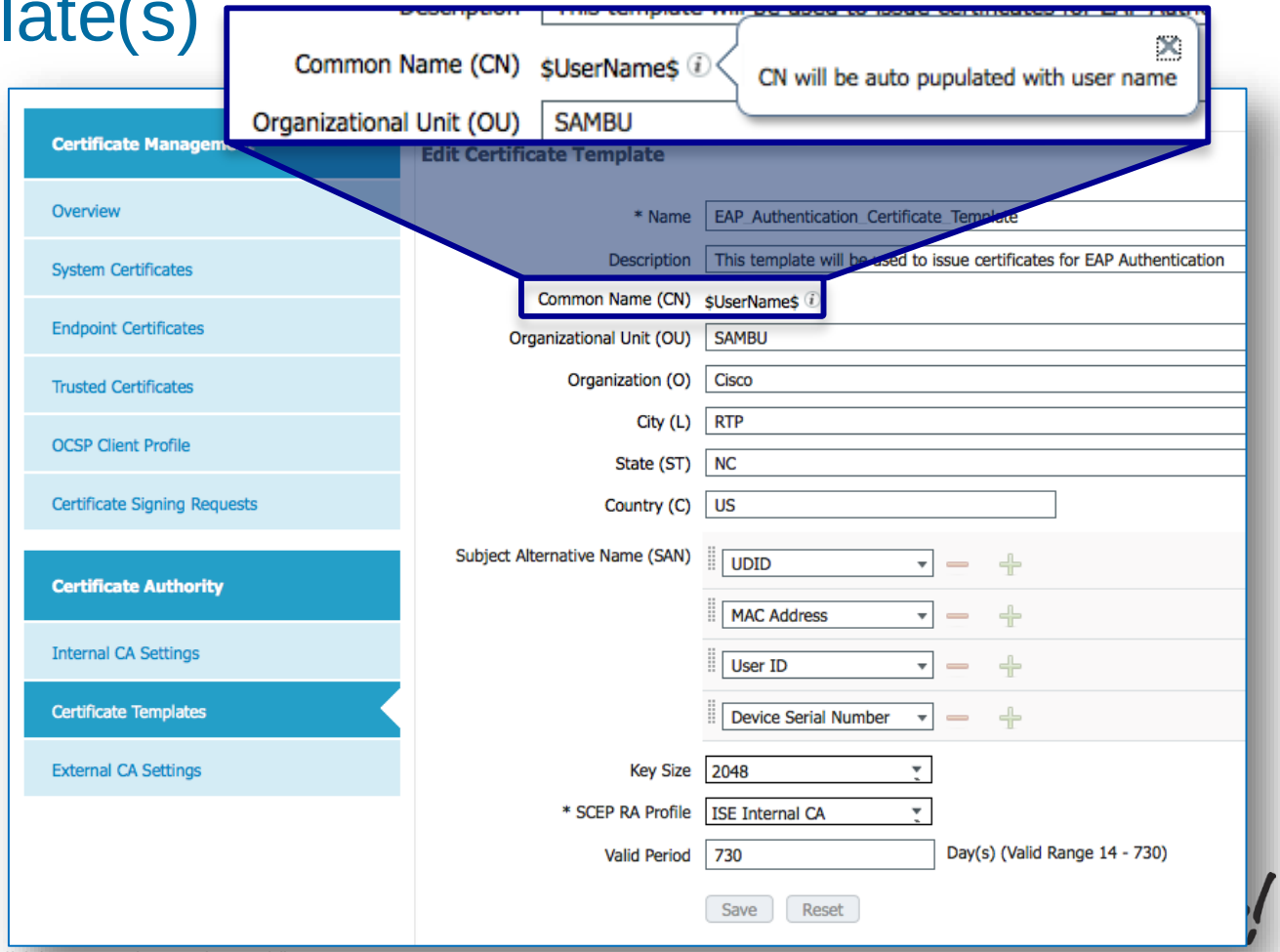
* Certificate Template: CTS-BYOD

Cisco live!

Certificate Template(s)

- Define Internal or External CA
- Set the Key Sizes
- SAN Field Options
  - UUID
  - DNS Name
  - MAC Address
  - Serial #

  (No Free-Form Input)
- Set length of validity



Revoke Certificates from ISE

ISE is OCSP Responder for cert validation – no CRL Lists !

- Automatically Revoked when an Endpoint is marked as “Lost”
- Certificates may be Manually Revoked

employee1	8C:7C:92:2F:B8:CD	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	C=US, ST=State, L=Str...	Revoked

System | Identity Management | Identity Mapping | Network Resources | Web Portal Management | Feed Service | pxGrid Services

Deployment | Licensing | Certificates | Logging | Maintenance | Backup & Restore | Admin Access | Settings

Certificate Management

- Overview
- System Certificates
- Endpoint Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests

Certificate Authority

Endpoint Certificates

View | Revoke | 1 - 7 of 7 | Show 25 per page | Page 1 of 1 | Show Quick Filter

Friendly Name	Device Unique Id	Valid From	Valid To	Issued By	Issued To	Status	Cert. Template
employee1	8C:7C:92:2F:B8:CD	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	C=US, ST=State, L=Str...	Revoked	EAP_Authentication...
employee1	A8:06:00:C5:9C:1D	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	CN=employee1	Active	EAP_Authentication...
employee1	8C:7C:92:2F:B8:CD	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	C=US, ST=NC, L=RTP, ...	Revoked	EAP_Authentication...
employee1	4C:AA:16:A2:93:0B	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	CN=employee1	Active	EAP_Authentication...
employee1	10:BF:48:D0:05:67	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	CN=employee1	Active	EAP_Authentication...
employee2	4C:AA:16:A2:93:0B	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	CN=employee2	Active	EAP_Authentication...
employee1	8C:7C:92:2F:B8:CD	2014-04-27	2015-04-28	CN=Cisco ISE Endpoint ...	C=US, ST=NC, L=RTP, ...	Active	EAP_Authentication...

Mobile Device Manageme

Extending "Posture" Assessment and Rem

Introduction

Profiling

AAA
(802.1x & MAB)

ISE Guest &
Employee WebAuth

Compliance
Desktop Posture
BYOD & MDM

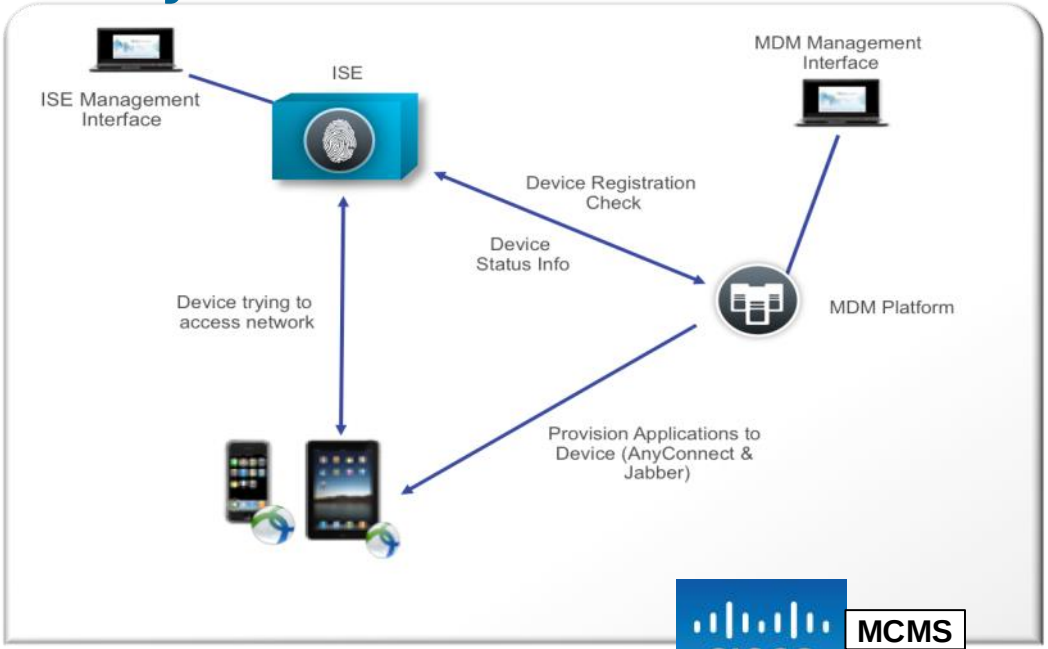
PxGrid

TrustSec

ISE Deployment

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



MCMS

MobileIron Version: 5.0

airwatch Version: 6.2

CITRIX ZENPRISE Version: 7.1

Good Version: 2.3

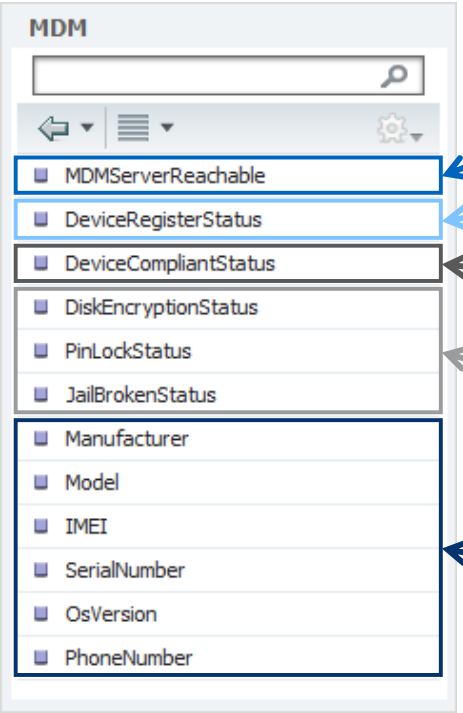
SYBASE iAnywhere Afaria

MaaS360 by Fiberlink

Configure ISE Authorisation Policy

Configure ISE Authorisation Policy

Path: Policy > Authorisation (MDM Attributes)



MDM Server reachability

Endpoint registration status

Endpoint macro-level compliance status

Endpoint micro-level compliance status
(Disk Encryption-, Pinlock-, and Jail broken status)

MDM attributes available for policy conditions
(Manufacturer, Model, IMEI, Serial Number,
OS Version, Phone Number)

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	

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

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

Authorization Compound Condition Details

Name **SSID_BYOD**

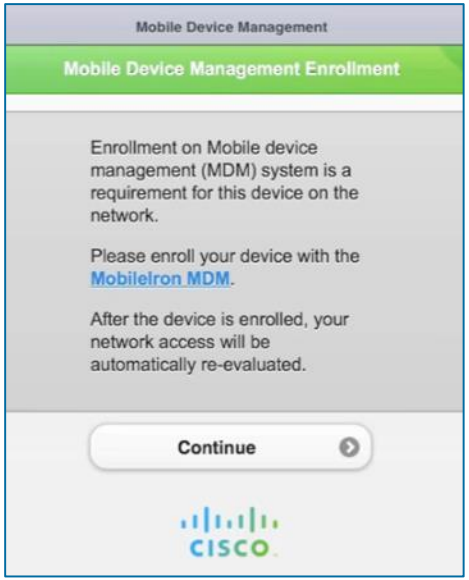
Conditions

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

MDM Enrollment and Compliance

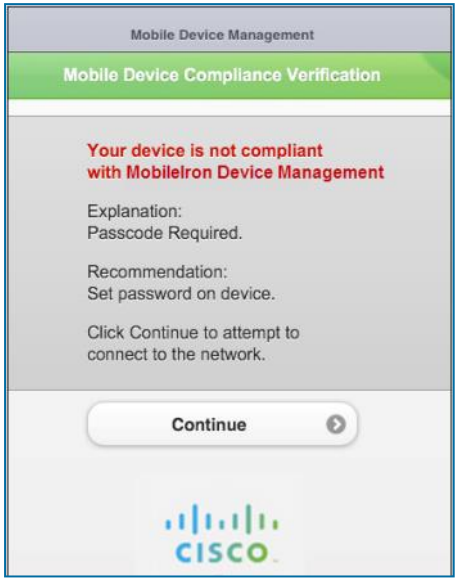
User Experience Upon MDM URL Redirect

MDM Enrollment



MDM:DeviceRegistrationStatus EQUALS UnRegistered

MDM Compliance

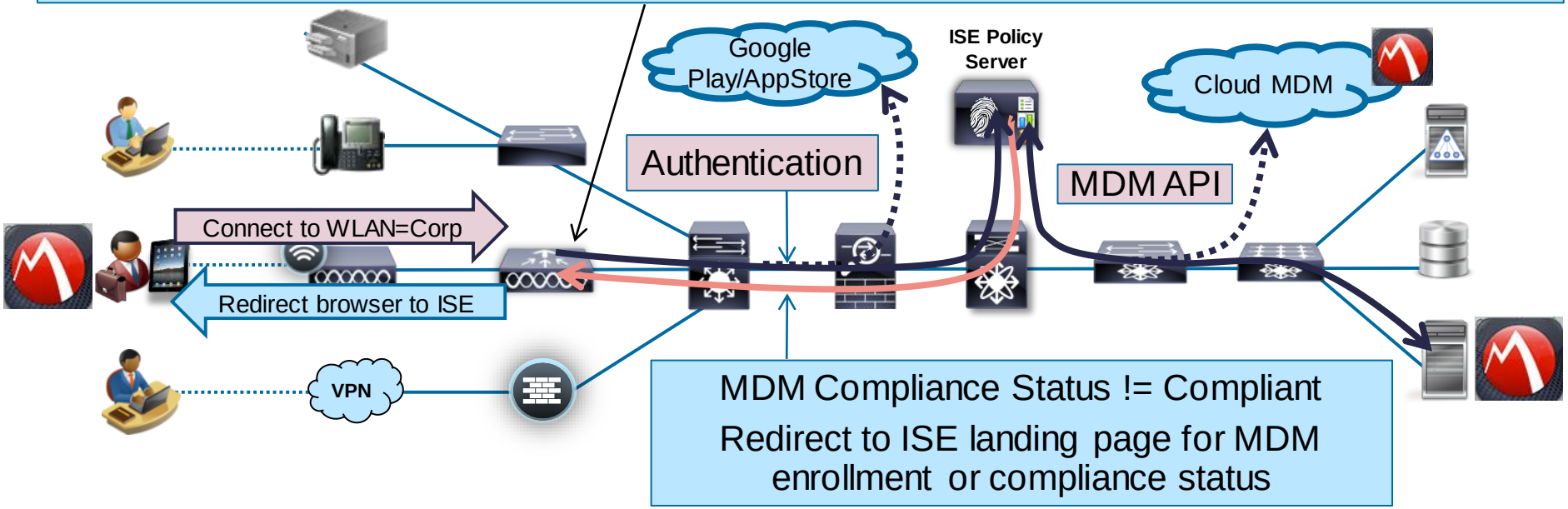


MDM:DeviceCompliantStatus EQUALS NonCompliant

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

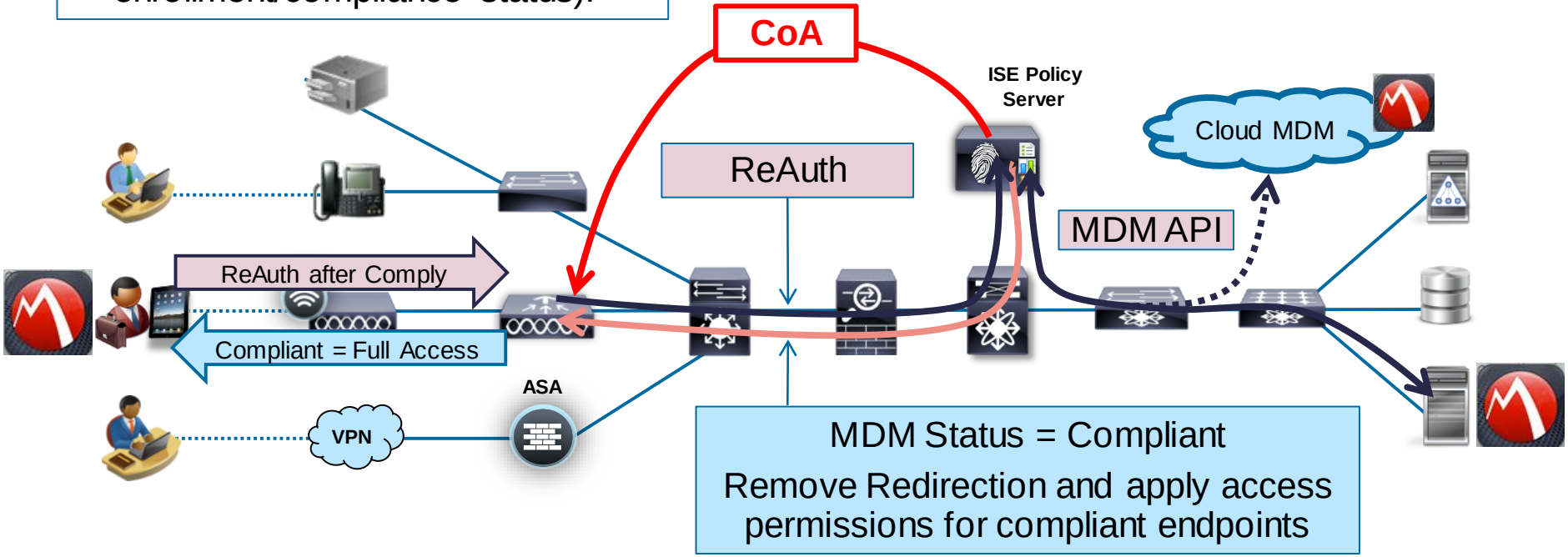
https://ise.company.com:8443/guestportal/gateway?sessionId=0A010A...73691A&action=**mdm**



MDM Remediation

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

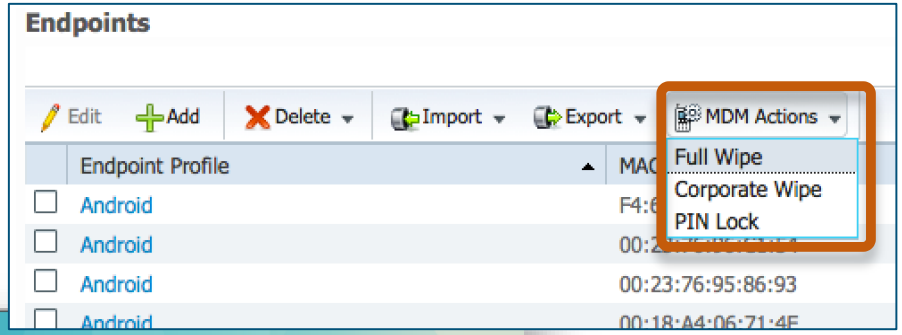
- MDM Agents downloaded directly from MDM Server or Internet App Stores
- Periodic recheck via API; CoA if not compliant

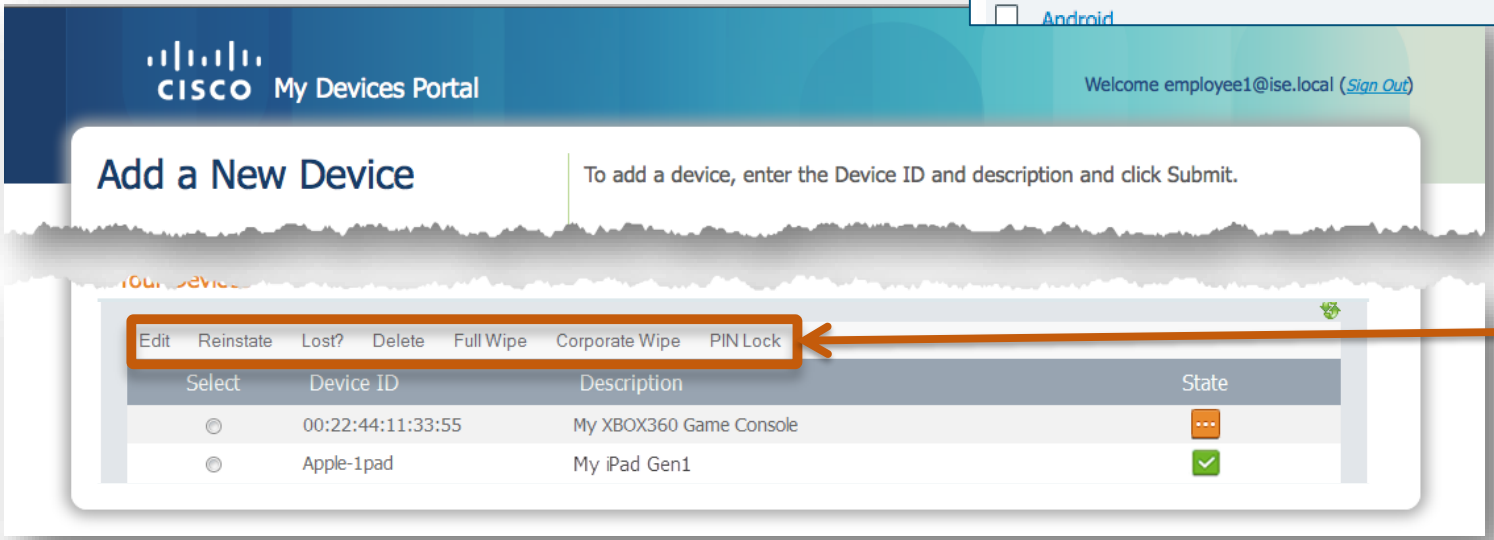


MDM Integration

Remediation

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





Options

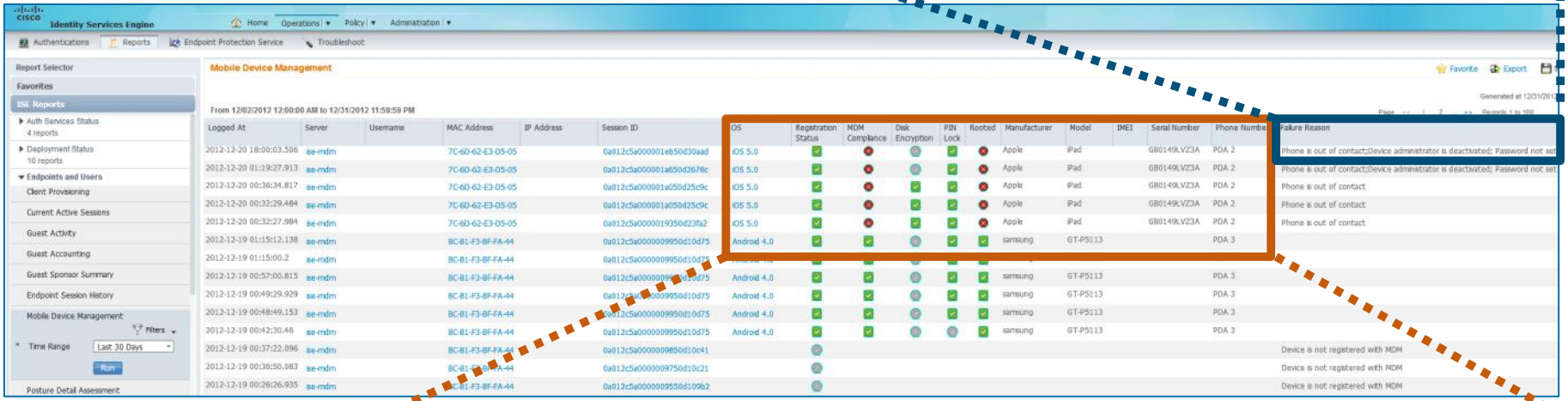
- Edit
- Reinstate
- Lost?
- Delete
- Full Wipe
- Corporate Wipe
- PIN Lock

Reporting

Mobile Device Management Report

Failure Reason

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



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

APIs and pxGrid
Sharing Context Throughout the Network

Introduction

Profiling

AAA
(802.1x & MAB)

ISE Guest &
Employee WebAuth

Compliance
Desktop Posture
BYOD & MDM

PxGrid

TrustSec

ISE Deployment

Single-Purpose APIs are Great for One Purpose

…Integrating One System to One Other System

I have reputation info!

I need threat data…

I have application info!

I need location & auth group…

TRADITIONAL APIs – One Integration at a Time

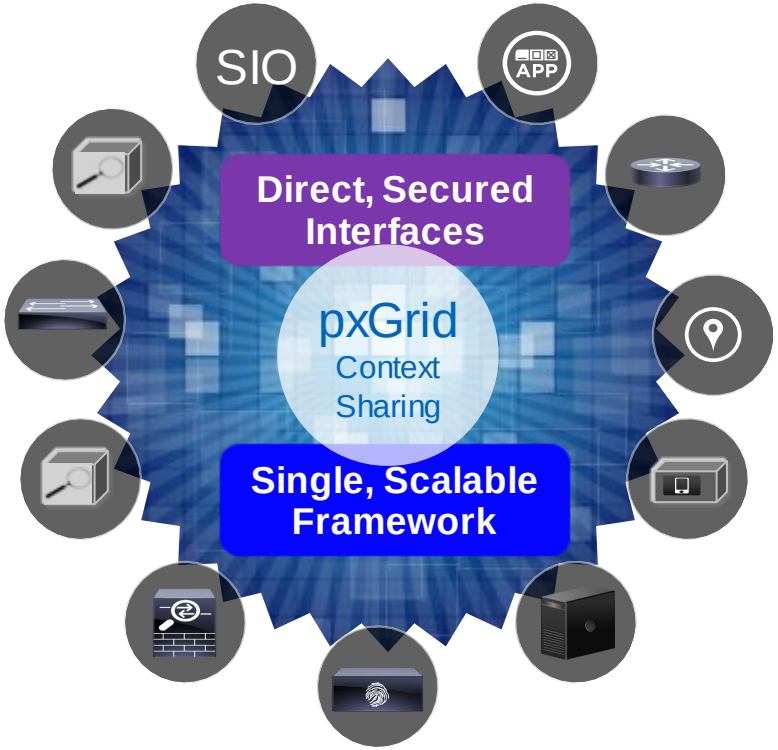
- Single-purpose function = need for many APIs/dev (and lots of testing)
- Not configurable = too much/little info for interface systems (scale issues)
- Pre-defined data exchange = wait until next release if you need a change
- Polling architecture = can't scale beyond 1 or 2 system integrations
- Security can be "loose"

I have identity & device-type!

I need app inventory & vulnerability…

Cisco Platform Exchange Grid – pxGrid

Enabling the Potential of Network-Wide Context Sharing



INFRASTRUCTURE FOR A ROBUST ECOSYSTEM

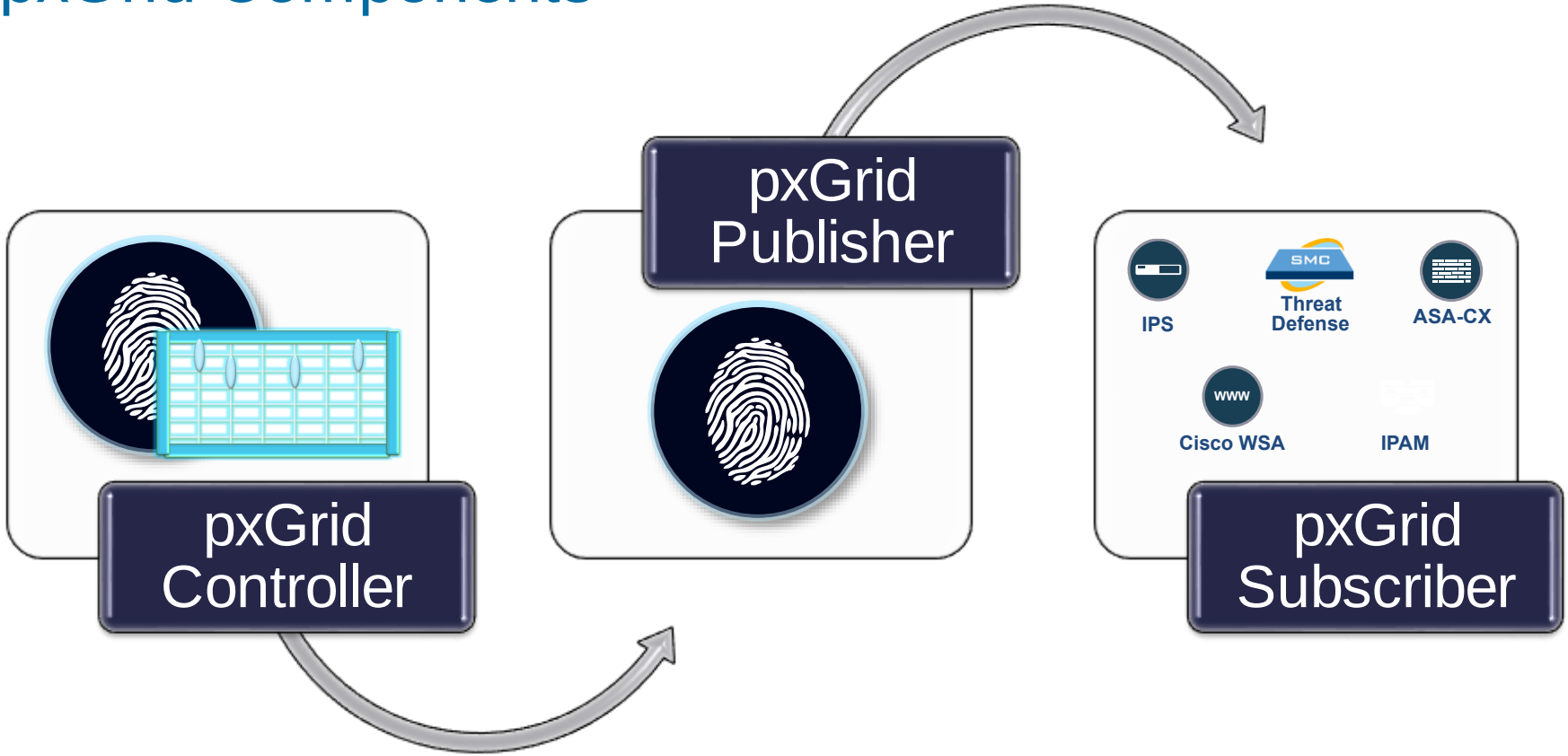
- Single framework – develop once, instead of multiple APIs
- Customise and secure what context gets shared and with which platforms
- Bi-directional – share and consume context
- Enables any pxGrid partner to share with any other pxGrid partner
- Integrating with Cisco ONE SDN for broad network control functions

The Next Wave of Cisco pxGrid Partnerships

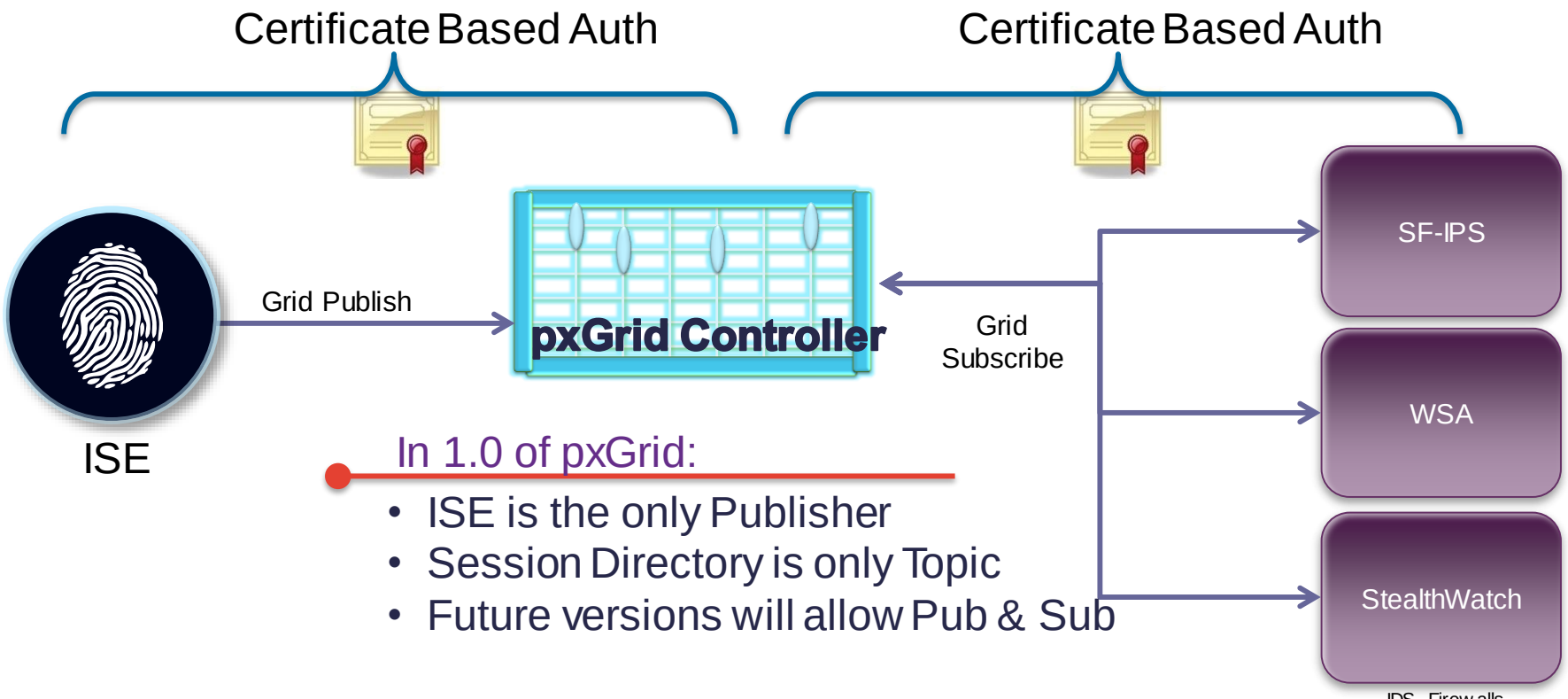
Sharing Context with an Even Broader Ecosystem

- Faster Remediation of Threats with SIEM
- Extension of Access Policy & Compliance with MDM
- Context-driven OT Policy and Segmentation for IoT
- Endpoint Vulnerability Remediation
- Simplified Network Troubleshooting and Forensics
- SSO Secure Access to Sensitive Data on Mobile Devices

pxGrid Components



pxGrid Architecture



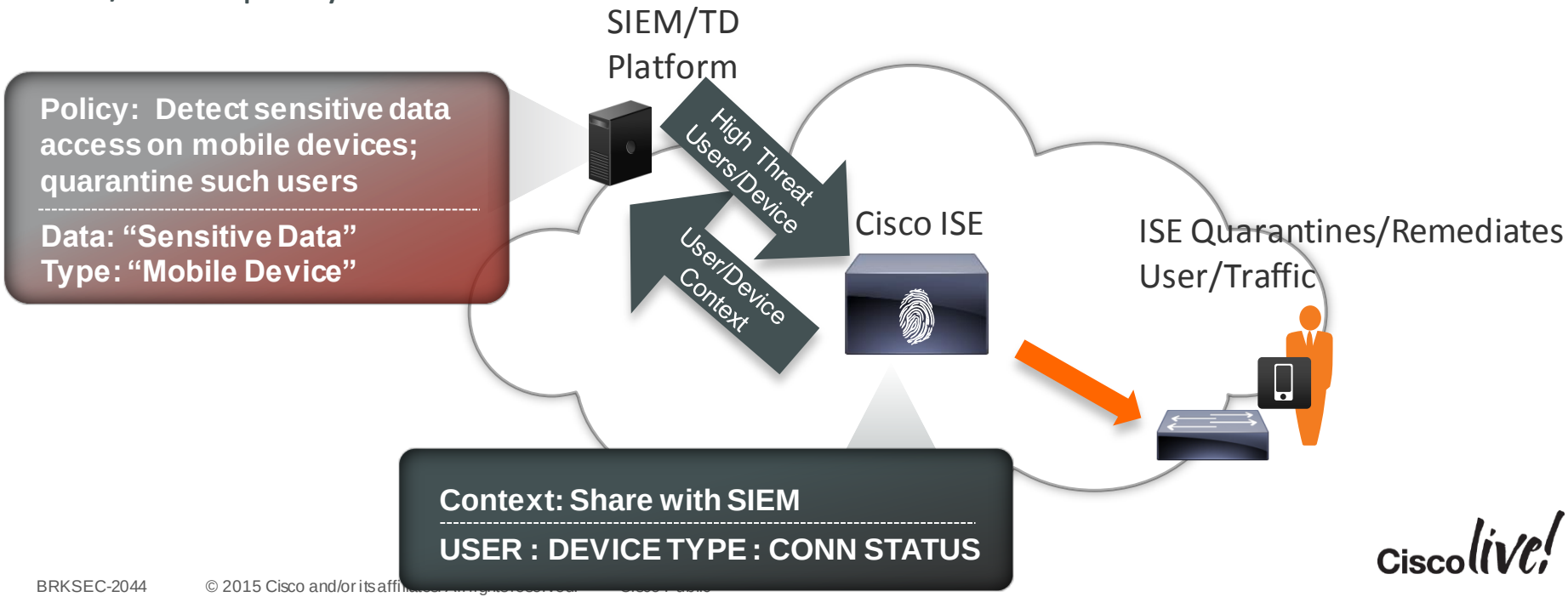
In 1.0 of pxGrid:

- ISE is the only Publisher
- Session Directory is only Topic
- Future versions will allow Pub & Sub

SIEM/Threat Defence Integration

Use Case: Identity and device aware threat management

Increase confidence around event severity levels in SIEMs and TD consoles; make events actionable in the network. SIEM/TD share "worst offenders" with ISE for user/device policy decisions.



IP Address & DNS Management

User, Group and Device Based Monitoring & Reporting

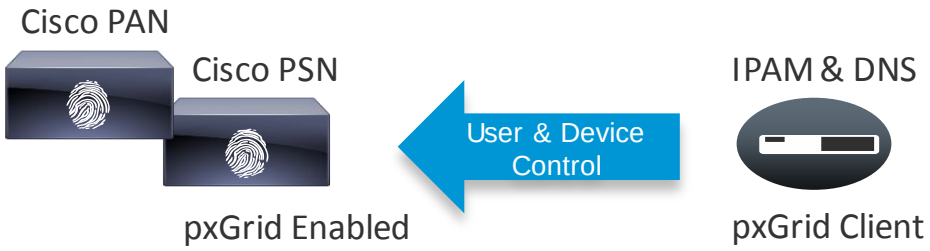
Use Case: Simplify IPAM and DNS reporting

Supplement IP and MAC address-based DHCP and DNS monitoring and reporting with "who, what and where". This reduces manual reporting or in-house development by IT orgs.

Report:

Who is accessing XYZ domain?

What devices and OS's are on the network?



Context: Subscribe to Session Topic

USER : DEVICE TYPE : GROUP

TrustSec Introduction

Introduction

Profiling

AAA
(802.1x & MAB)

ISE Guest &
Employee WebAuth

Compliance
Desktop Posture
BYOD & MDM

PxGrid

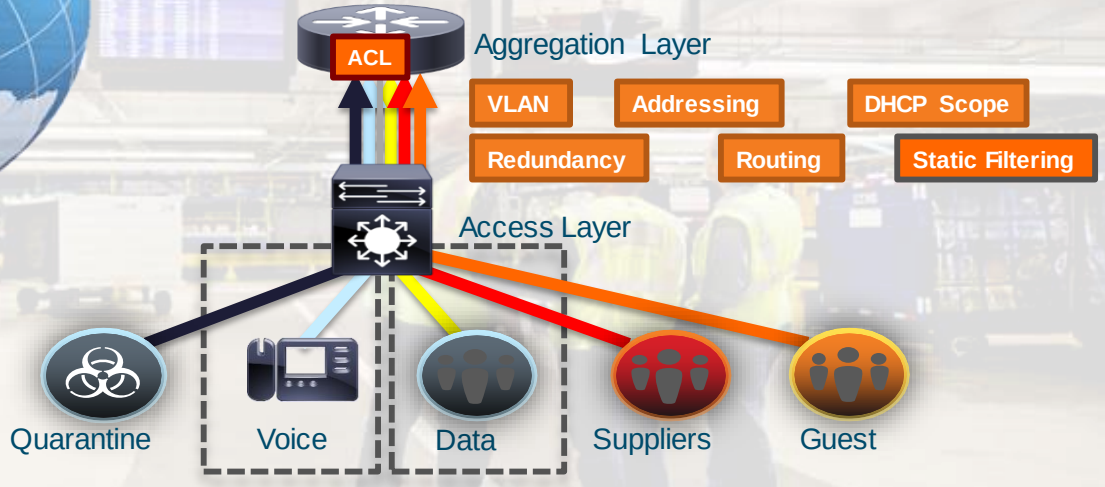
TrustSec

ISE Deployment

TrustSec Introduction

Policy and Segmentation

Design needs to be replicated to multiple locations, buildings, floors

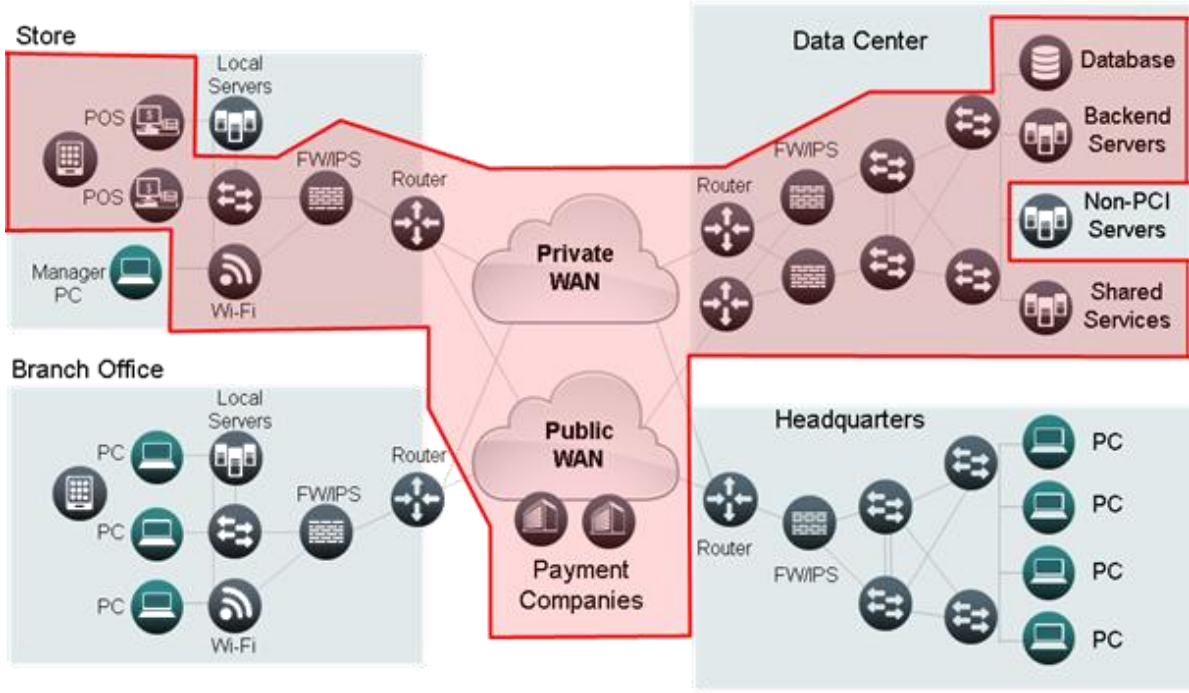


Simple Segmentation with 2 VLANs

More Segmentation with 5 VLANs

Software-Defined Segmentation with Cisco TrustSec/ SGT

- Simplicity: consistent policy enforcement on all networks
- Agility: reduce attack surface, keep pace with business
- Ready: secure, comply today



How TrustSec/ SGT is Used Today

User to DC Access Control

Network & Role Segmentation

BYOD Security

Application Protection

Secure Contractor Access

PCI & PHI Compliance

Campus & DC Segmentation

Server Segmentation

Firewall Rule Reduction

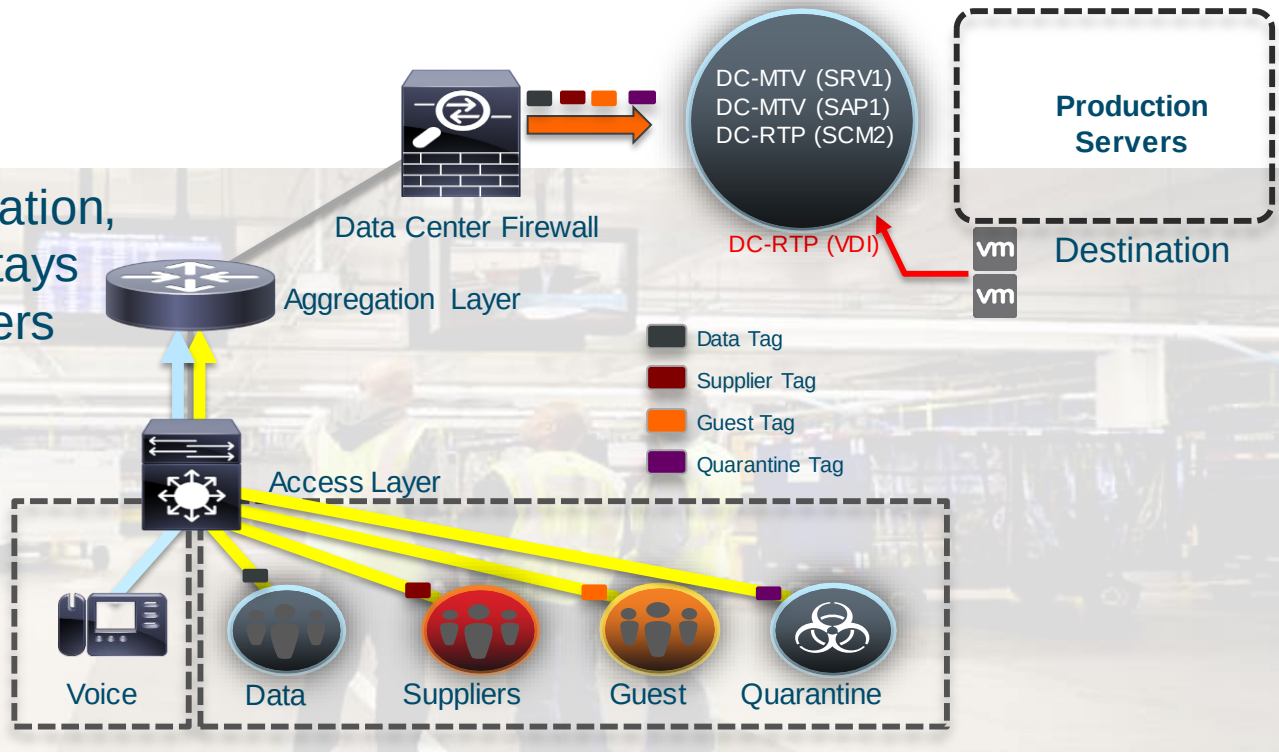
Fast Server Provisioning

Threat Defence

Machine-Machine Control

Segmentation with Security Group

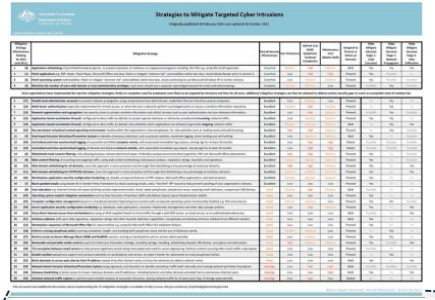
Regardless of topology or location, policy (Security Group Tag) stays with users, devices, and servers



Retaining initial VLAN/Subnet Design

Improving Security..

Strategies to mitigate TCI



Australian Government

Department of Defence

Intelligence and Security

Mitigation Strategy Effectiveness Ranking for 2014 (and 2012)	Mitigation Strategy	User esistance	Upfront Cost (Staff, Equipment, Technical Complexity)
10 (7)	**Network segmentation and segregation** into security zones to protect se	Low	High

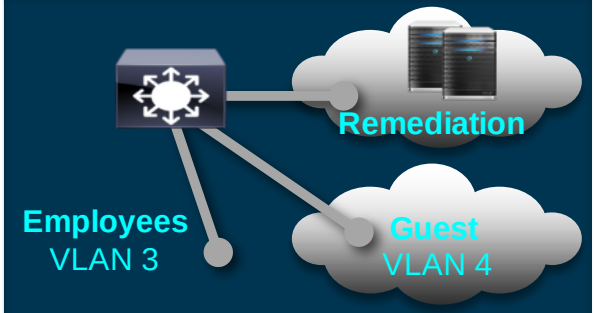
Technical Complexity)

High

http://www.asd.gov.au/infosec/top-mitigations/top3

TrustSec Authorisation and Enforcement

VLANS



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

dACL or Named ACL

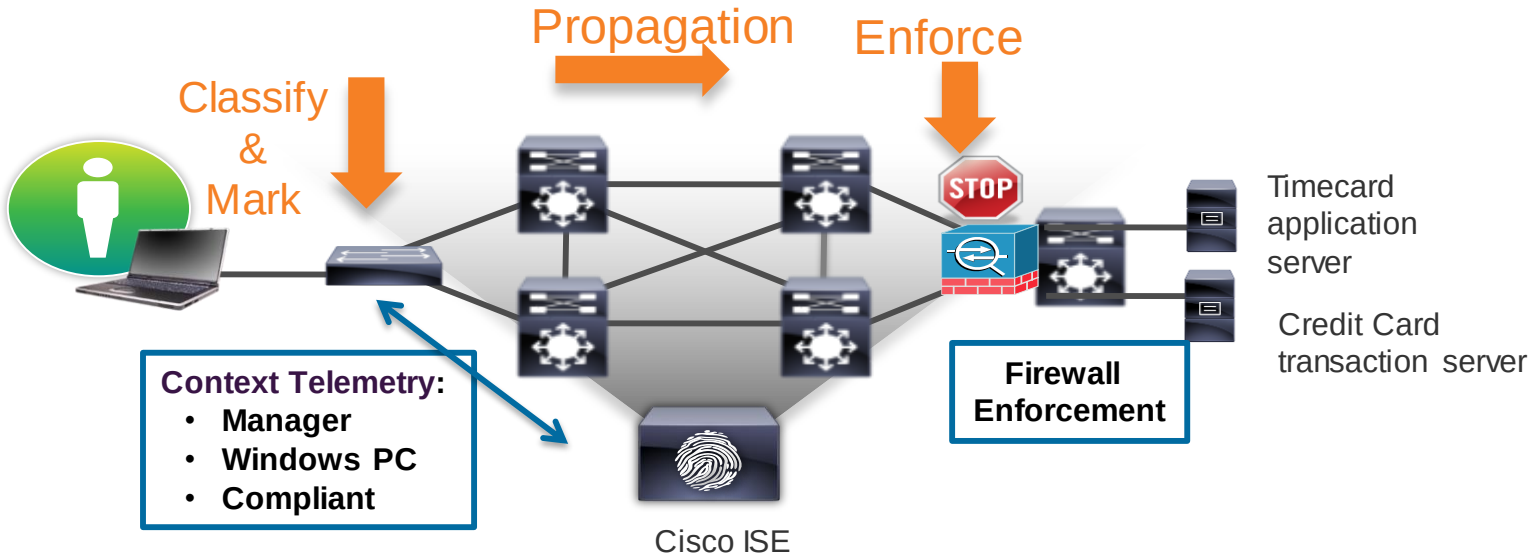
- Less disruptive to endpoint (no IP address change required)
- Improved user experience
- Increased ACL management

Security Group Access

Security Group Access—SXP, SGT, SGACL, SGFW

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

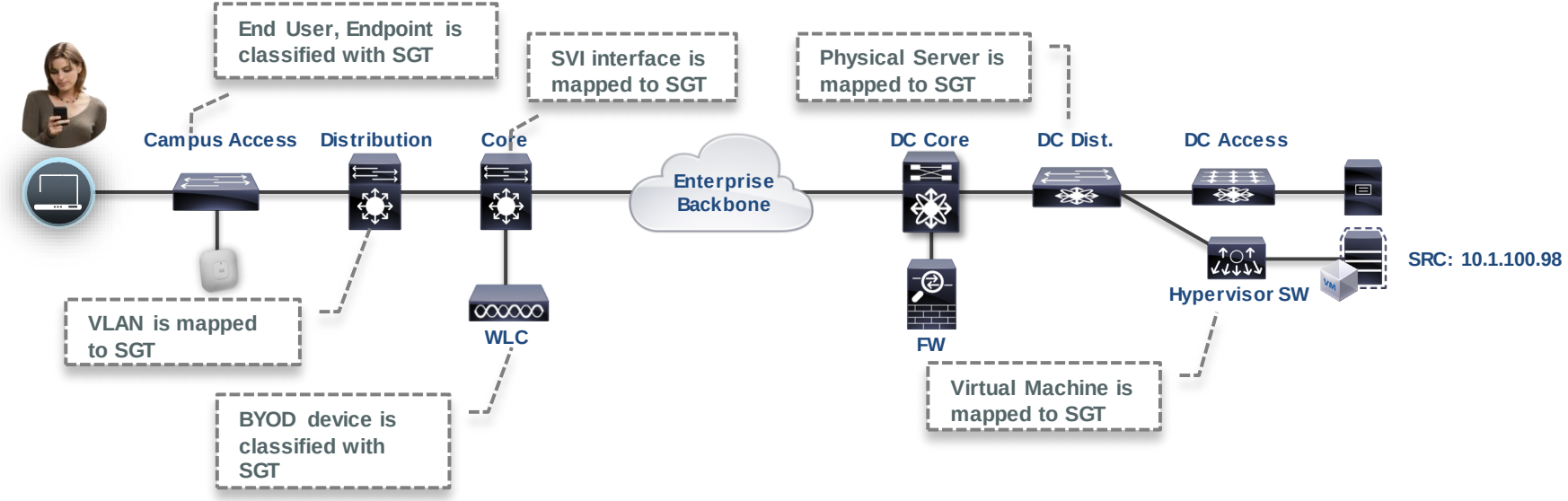
Enforcing Policy Downstream



Classify Mark, Propagate, Enforce

- IP Precedence and DiffServ code points
- 802.1Q User Priority
- MPLS VPN
- **TrustSec**

How a SGT is Assigned



Classification Summary

Dynamic Classification

802.1X/ RAS VPN Authentication

Web Authentication

MAC Auth Bypass

Common Classification for Mobile Devices

Static Classification

- IP Address
- VLANs
- Subnets
- L2 Interface
- L3 Interface
- Virtual Port Profile
- Layer 2 Port Lookup
  Pre-fix learning

SGT

Common Classification for Servers, Topology-based policy, etc.

Static Classification

IOS CLI Example

IP to SGT mapping

```
cts role-based sgt-map A.B.C.D sgt SGT_Value
```

L2IF to SGT mapping

```
(config-if-cts-manual)#policy static sgt SGT_Value
```

VLAN to SGT mapping

```
cts role-based sgt-map vlan-list VLAN sgt SGT_Value
```

L3IF to SGT mapping

```
cts role-based sgt-map interface name sgt SGT_Value
```

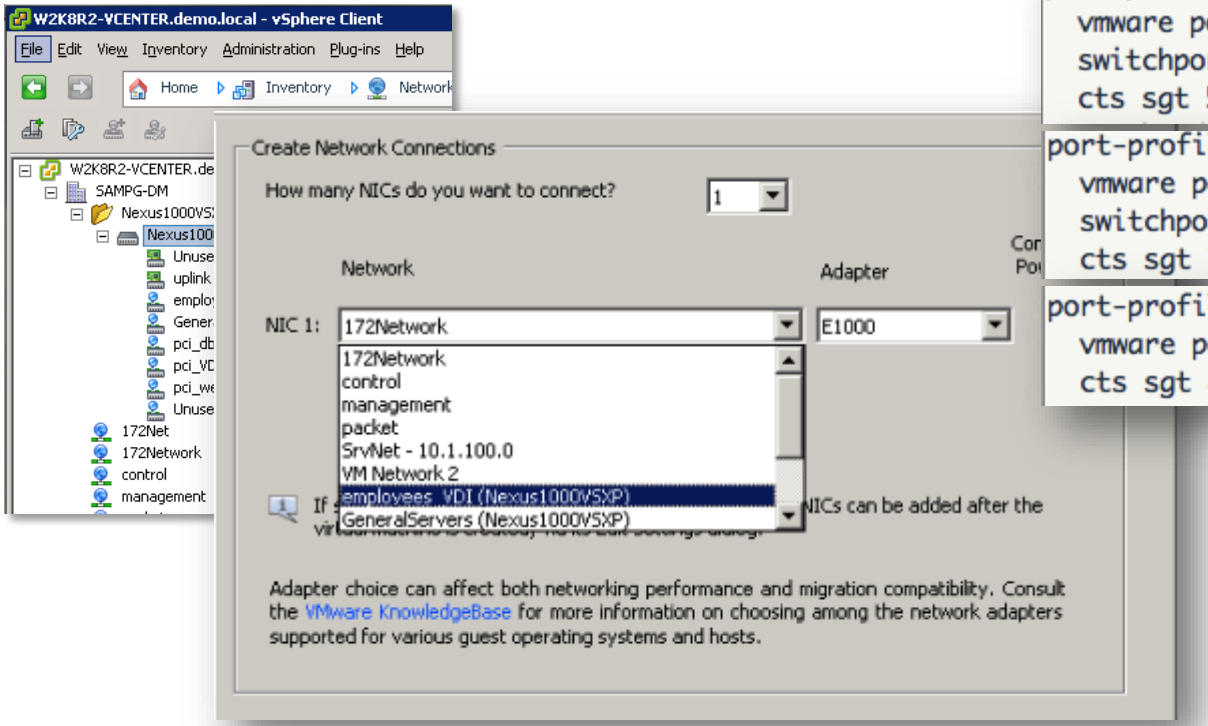
Subnet to SGT mapping

```
cts role-based sgt-map A.B.C.D/nn sgt SGT_Value
```

L3 ID to Port Mapping

```
(config-if-cts-manual)#policy dynamic identity name
```

SGT to Port Profile



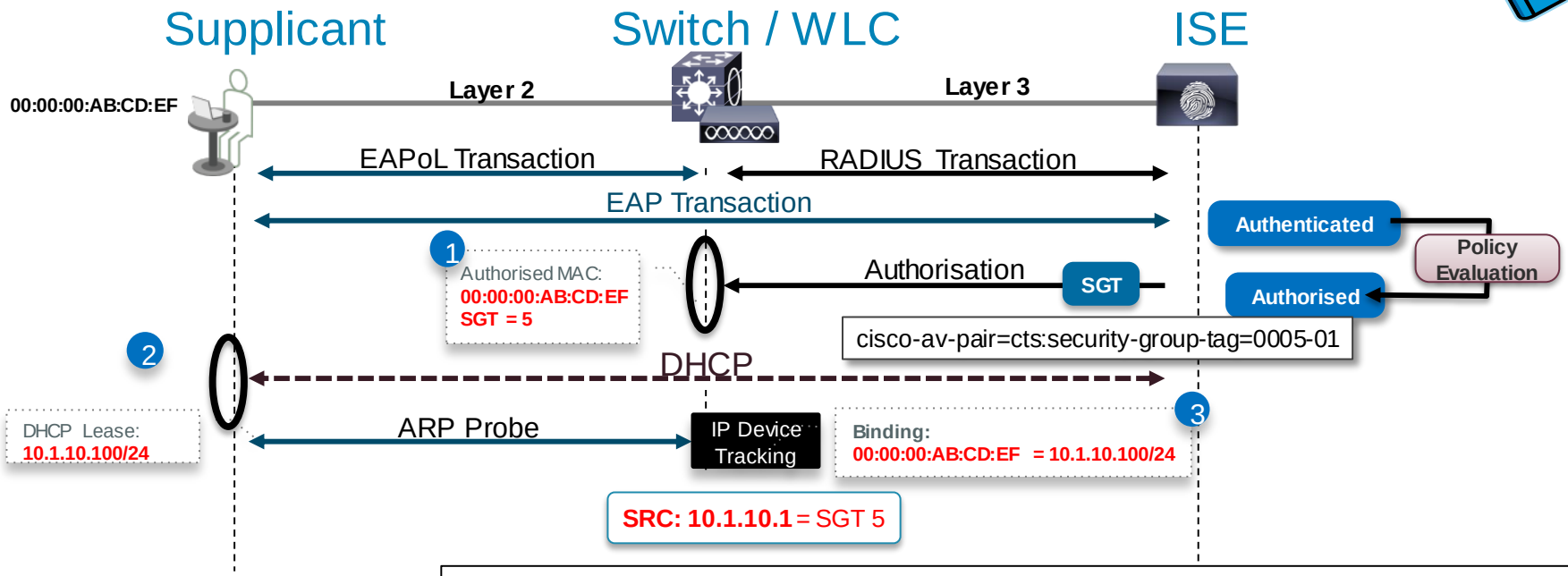

```
port-profile type vethernet GeneralServers
  vmware port-group
  switchport access vlan 100
  cts sgt 5
```

```
port-profile type vethernet pci_web
  vmware port-group
  switchport access vlan 100
  cts sgt 7
```

```
port-profile type vethernet pci_db
  vmware port-group
  cts sgt 8
```

Nexus 1000v version 2.1

Dynamic Classification Process in Detail



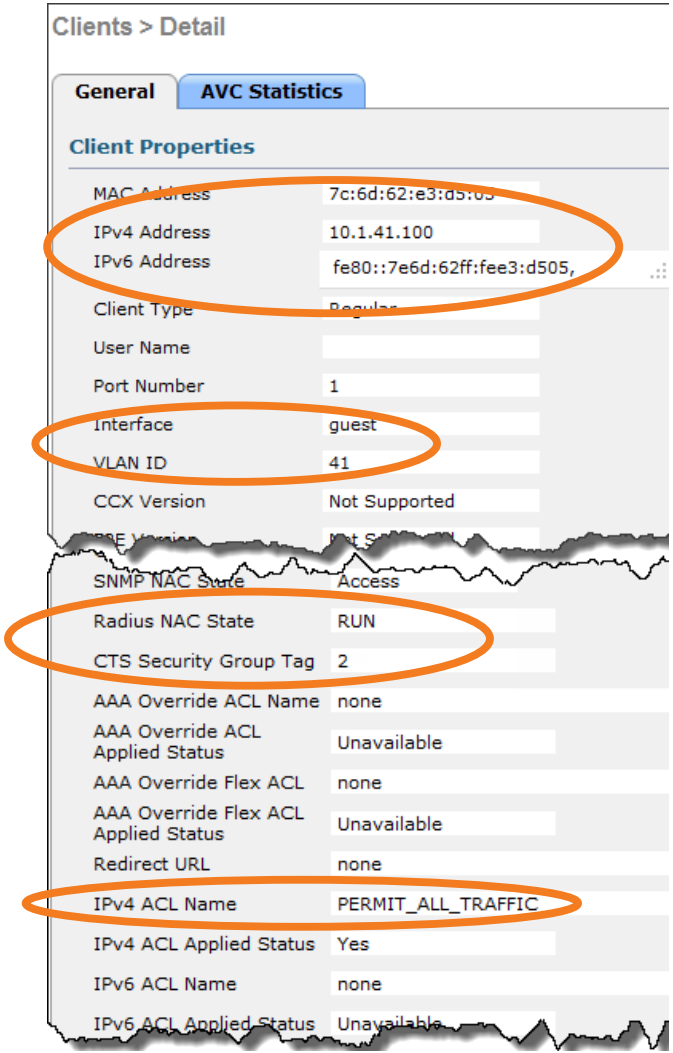
Make sure that IP Device Tracking is TURNED ON

```
3560X#show cts role-based sgt-map all details
Active IP-SGT Bindings Information

IP Address              Security Group          Source
============================================
10.1.10.1               3:SGA_Device            INTERNAL
10.1.10.100             5:Employee              LOCAL
```


A Systems Approach

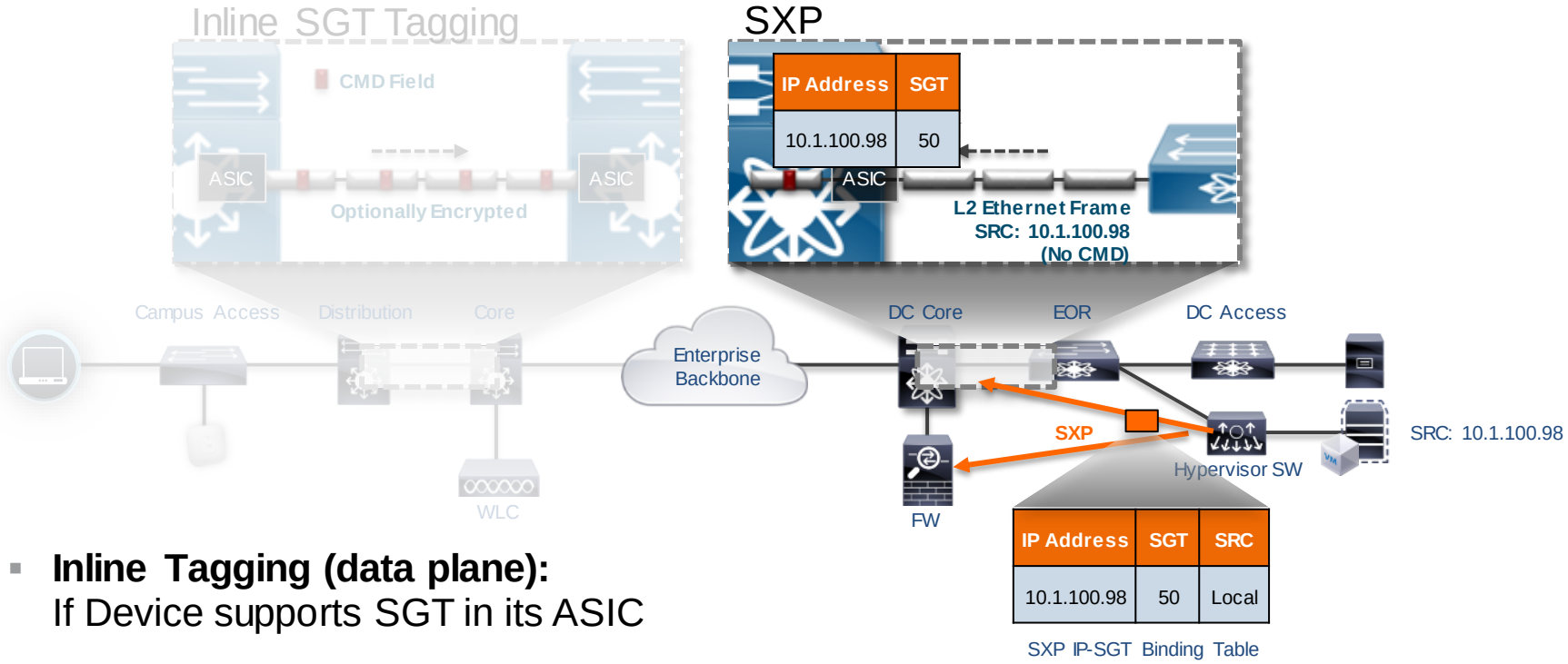
- Switch/Controller is the Enforcement Point

```
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
```



How is the SGT Classification Shared?

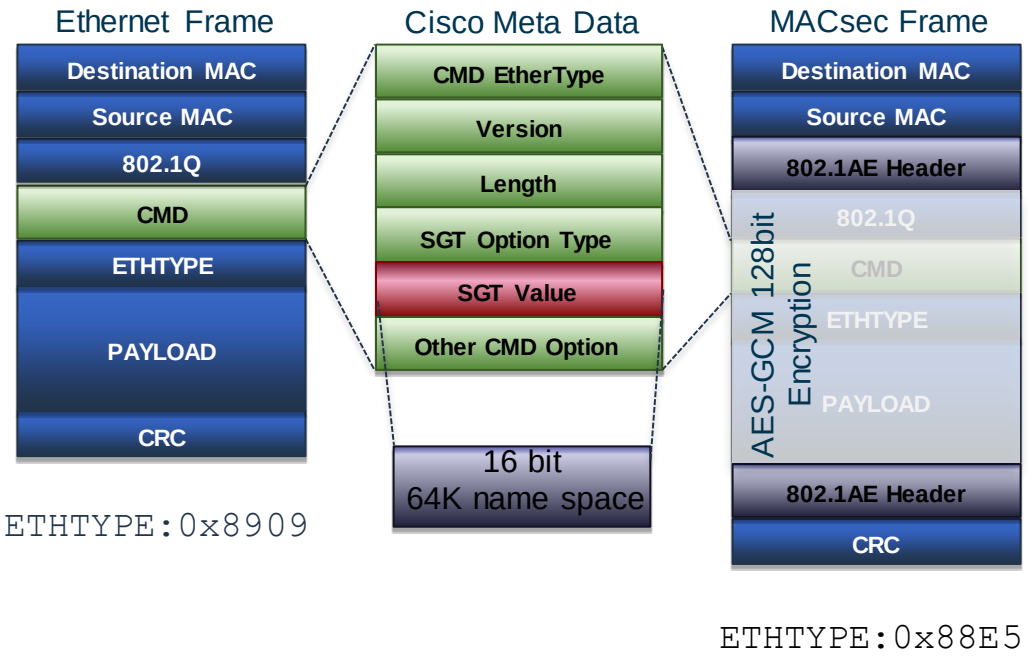
Propagation



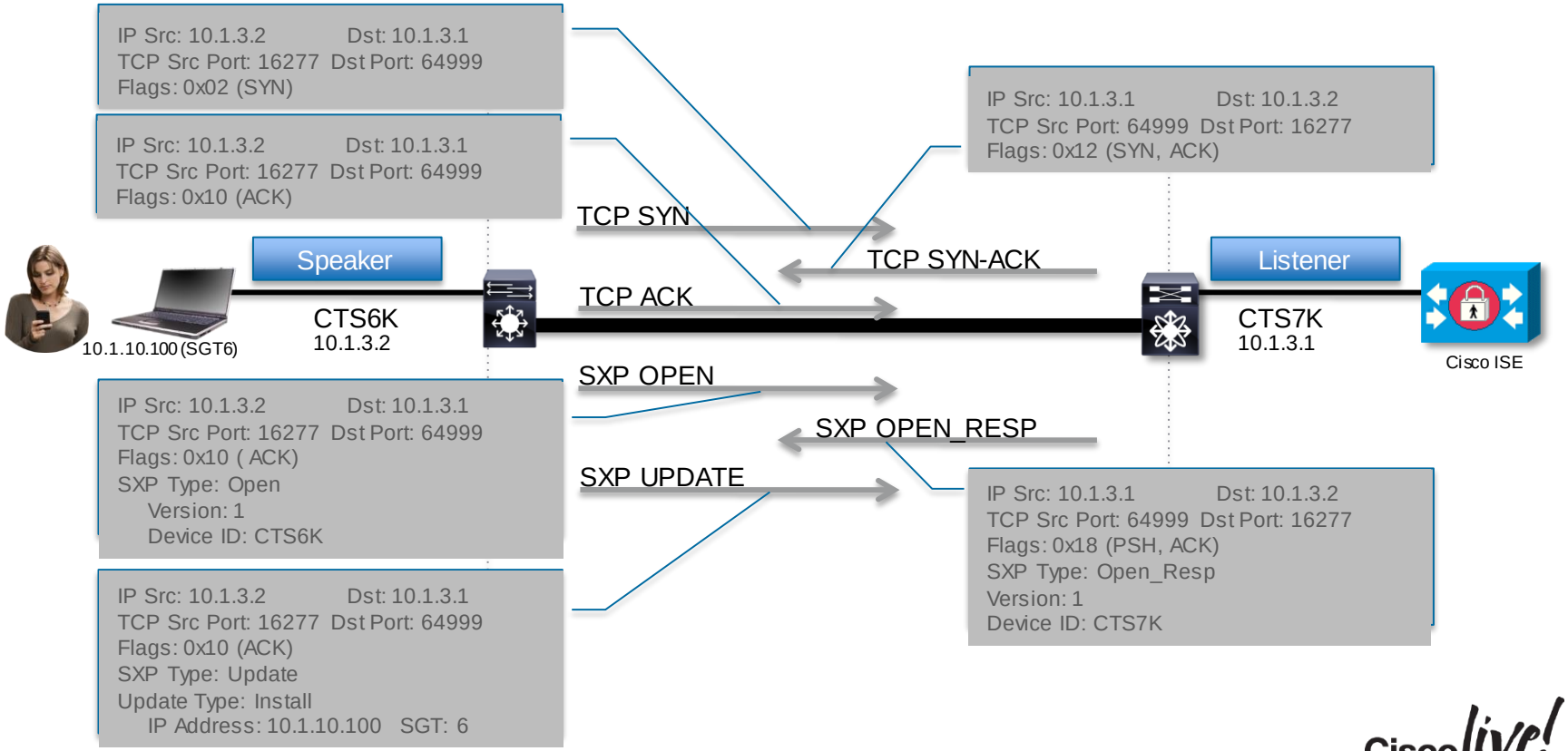
- **Inline Tagging (data plane):** If Device supports SGT in its ASIC
- **SXP (control plane):** Shared between devices that do not have SGT-capable hardware

Inline Tagging

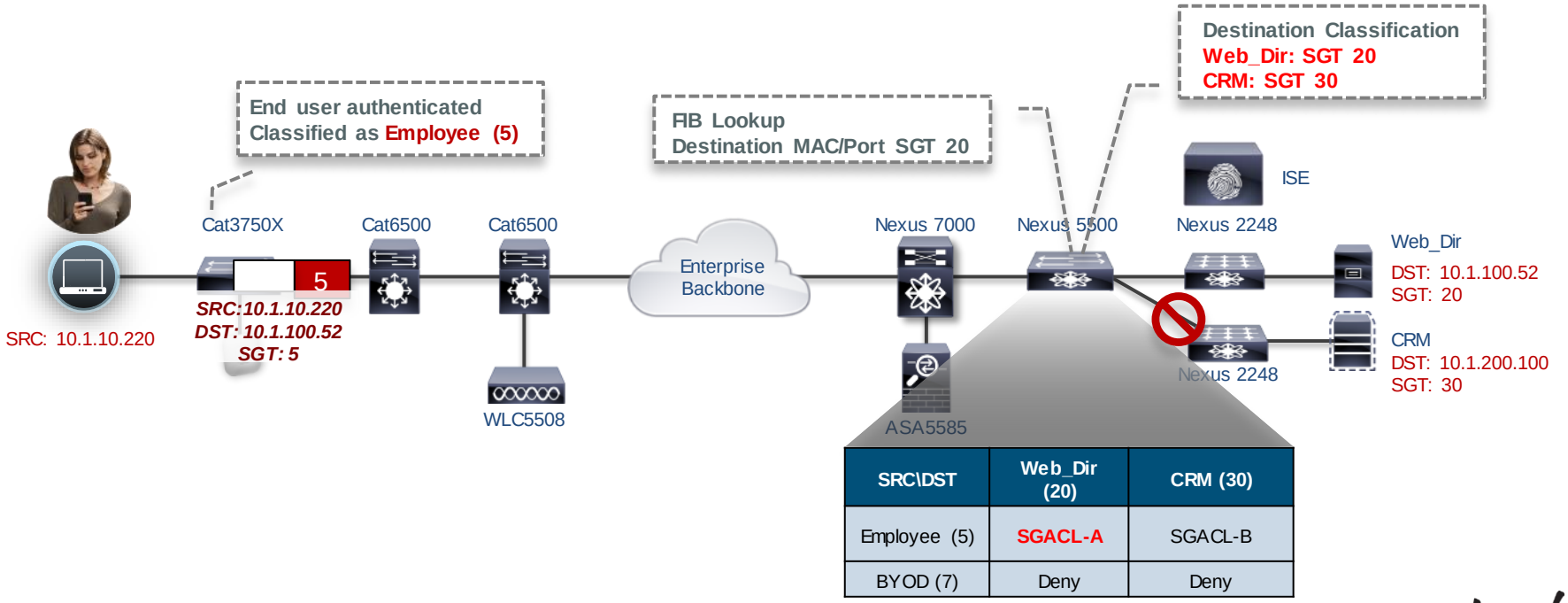
- SGT embedded within Cisco Meta Data (CMD) in Layer 2 frame
- Capable switches understands and process SGT at line-rate
- Optional MACsec protection
- No impact to QoS, IP MTU/Fragmentation
- L2 Frame Impact: ~40 bytes
- Recommend L2 MTU~1600 bytes



SXP Flow



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

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

Egress Policy (Matrix View)

Edit | Add | Clear Mapping | Configure | Push | Monitor All | Dimension 3X5

Source \ Destination	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

Security Group Based Access Control for Firewalls

Security Group Firewall (SGFW)

#	Enabled	Source Criteria: Source	Source Criteria: User	Source Criteria: Security Group	Destination Criteria: Destination	Destination Criteria: Security Group	Service	Action	Hits	Logging	Time
inside (1 incoming rule)											
1	☑	any			any		ip	Permit	...	...	
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

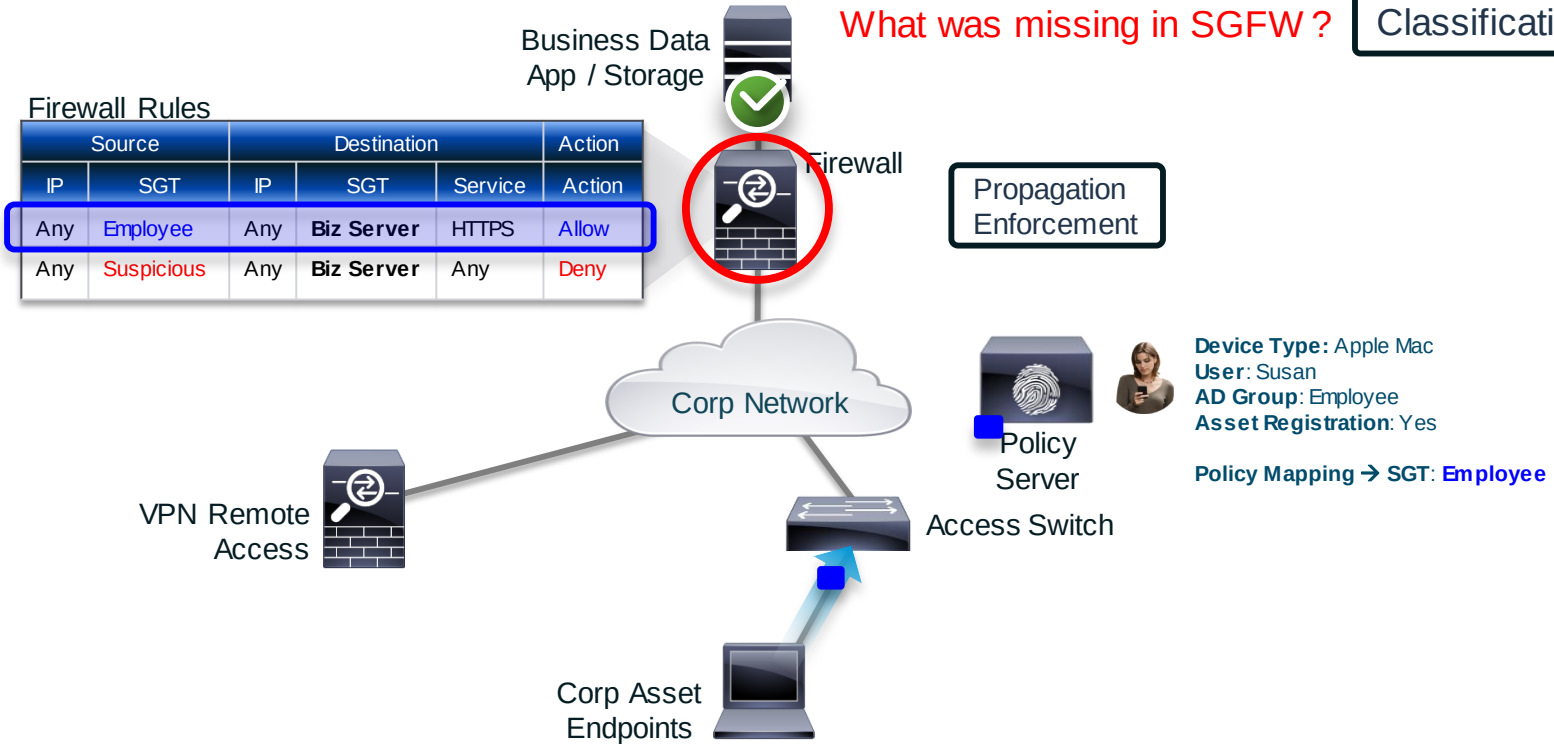
Destination Tags

Review: SGFW Flow

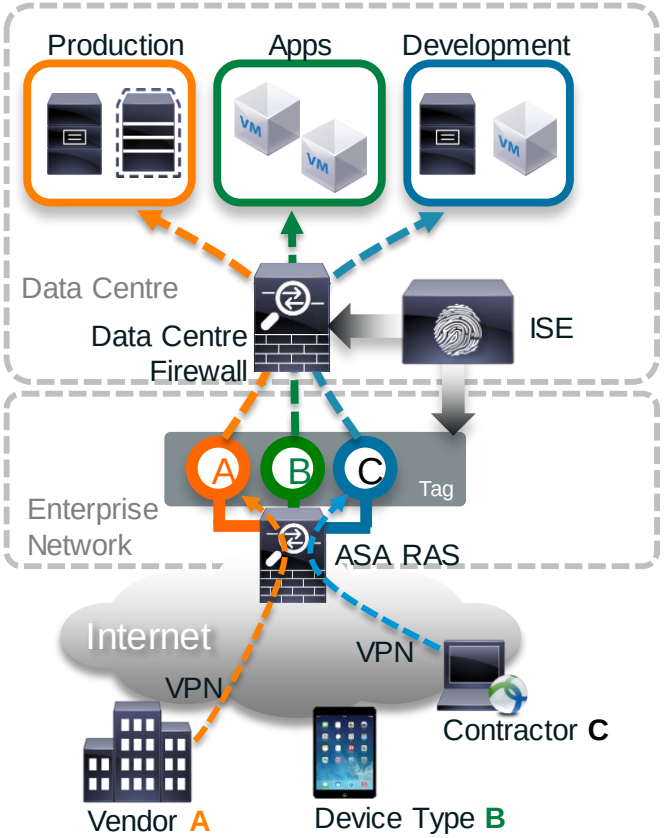
What was missing in SGFW ? Classification

Firewall Rules

Source		Destination			Action
IP	SGT	IP	SGT	Service	Action
Any	Employee	Any	**Biz Server**	HTTPS	Allow
Any	Suspicious	Any	**Biz Server**	Any	Deny



Visibility and Control for Remote Access



Simplified Remote Access

Filtering based on SGT (Tag), not based on pooled IP addresses allows simplified cross connect of access policy for multiple RAS VPN points

Firewall Policy maintenance (add, edit, delete) is streamlined for service change

Use Case: DC Access Access Control

Reduced OPEX

Admin reduction 24 -> 6 People

Reduced "ACE" Entries

Reduction 60 - 90%.

Topology Independent

Rules with no IP addresses

Contextual Access

User+Device

User+Device+Access_type

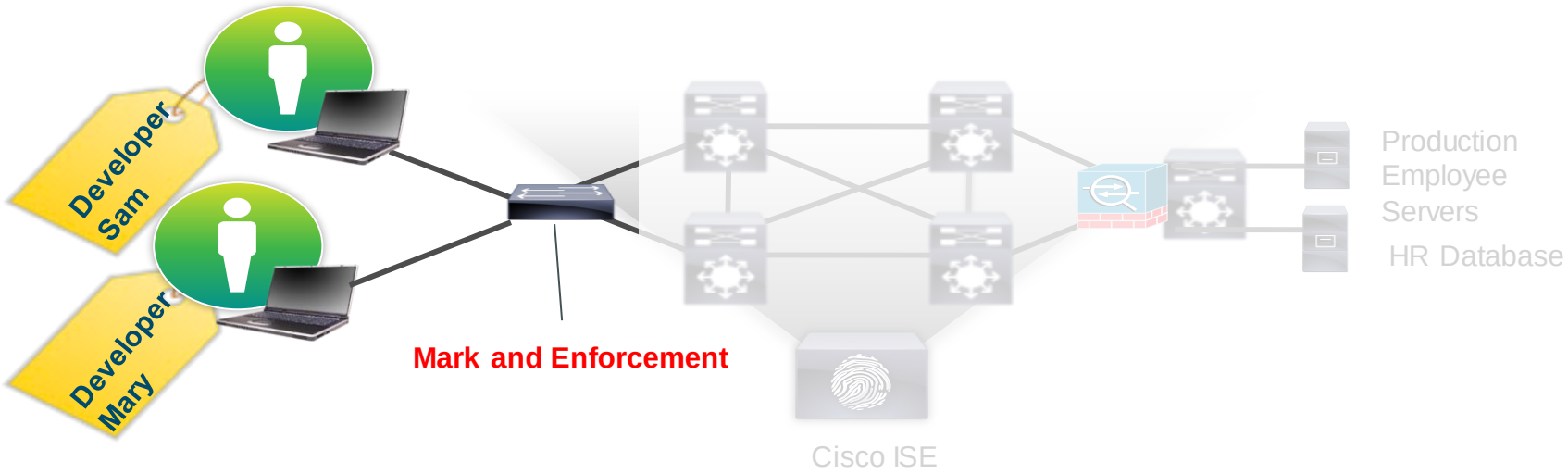
Traditional Firewall Rules

Policy Object - S	Source	Policy Object- D	Dest.	Svc	Act.
Finance	10.1.1.0/24	Fin Web Server	172.1.1.1	Web	Permit
	10.1.2.0/24				
	10.1.3.0/24				
Engr	10.1.1.0/24	Devlp Server	172.1.1.2	Web	Permit
	10.1.2.0/24				
	10.1.3.0/24				

SGA Firewall Rules

SGT - User	SGT - Service	Svc	Act.
Finance-Corp-PC	Fin Web Server	Web	Permit
Finance-IPAD	Fin Web Server	Web	Deny
Engr-All-Devices	Devlp Server	Web	Permit

Use Case: Peer-to-Peer Malware Control



Assets

Source	Sales	Developer	Guests	Inter Acc
Sales	Malware Blocking	DENY	DENY	PER
Developer	DENY	Malware Blocking	DENY	PER
Guest	DENY	DENY	DENY	PER

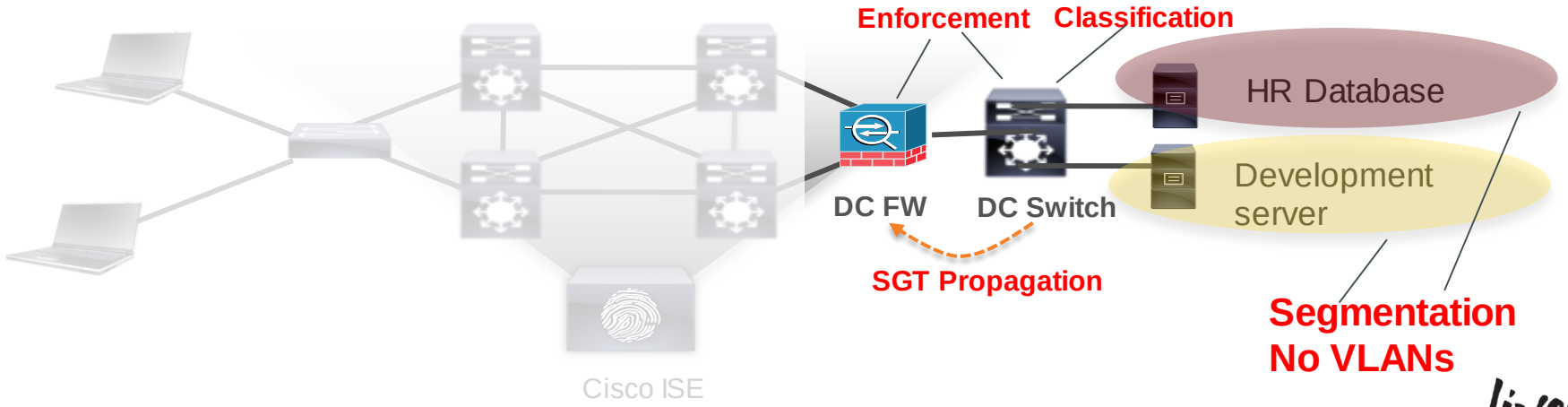
Malware Blocking ACL

```
Deny tcp dst eq 445 log; block SMB file sharing
Deny tcp dst range 137 139 log; block NetBios Session Service
Permit all
```

Use Case: Data Centre Segmentation

Protected Assets

Source	Production Servers	Development Servers	HR Database	Storage
Production Servers	PERMIT	DENY	DENY	PERMIT
Development Servers	DENY	PERMIT	DENY	PERMIT
HR Database	DENY	DENY	PERMIT	PERMIT
Storage	PERMIT	PERMIT	PERMIT	PERMIT

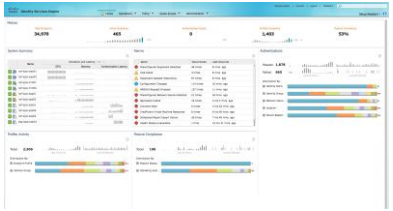


ISE + Fire + TrustSec

Before

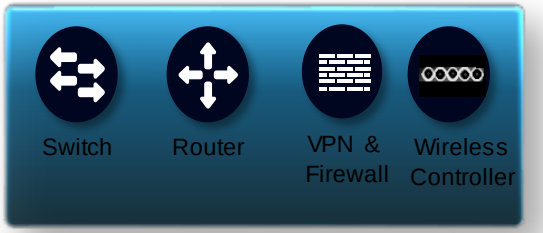
- Threat Detection
- Prevention and Mitigation

During



- Collecting additional telemetry
- Added visibility
- Evaluate Policy

After



Segmentation Policy Enforcement

- Containment (Quarantine or Block all together)
- Apply QoS
- Apply policy routing
- Deep inspection

Threat data Sharing →

Enforce →

TrustSec Platform Support

Classification

- Catalyst 2960S/C/Plus/X/XR
- Catalyst 3560-E/-C/-X
- Catalyst 3750-E/-X
- Catalyst 3850 NEW
- WLC 5760
- Catalyst 4500E (Sup6E/7E)
- Catalyst 6500E (Sup720/2T)
- Wireless LAN Controller 2500/5500/WiSM2
- Nexus 7000
- Nexus 5500
- Nexus 1000v
- ISR G2 , CGR2000
- ASA5500 (VPN RAS) Beta

Propagation

- SXP — Catalyst 2960-S/-C/-Plus/-X/-XR
- SXP — Catalyst 3560-E/-C/, 3750-E
- SXP SGT — Catalyst 3560-X, 3750-X
- SXP SGT — Catalyst 3850 NEW
- SXP — Catalyst 4500E (Sup6E)
- SXP SGT — Catalyst 4500E (7E), 4500X
- SXP — Catalyst 6500E (Sup720)
- SXP SGT — Catalyst 6500E(2T) & 6800 NEW
- SXP — WLC 2500, 5500, WiSM2
- SXP SGT — WLC 5760 NEW
- SXP — Nexus 1000v
- SXP SGT — Nexus 5500/22xx FEX
- SXP SGT — Nexus 7000/22xx FEX
- SXP SGT GETVPN IPsec — ISRG2* CGR2000
- SXP SGT GETVPN IPsec — ASR1000
- SXP — ASA5500 Firewall, ASASM

Enforcement

- SGACL — Catalyst 3560-X
- Catalyst 3750-X
- SGACL — Catalyst 3850 NEW
- WLC 5760 NEW
- SGACL — Catalyst 4500E (7E) NEW
- Catalyst 6500E (2T)
- SGACL — Catalyst 6800 NEW
- Nexus 7000
- Nexus 5500
- SGACL
- SGFW — ISR G2, CGR2000
- SGFW — ASR 1000 Router
- CSR1000v Router
- SGFW — ASA 5500 & ASA-SM
- ASAv Beta

- Inline SGT on all ISRG2 except 800 series:

SXP: IETF Internet Draft

SXP submitted to IETF and is being implemented by other vendors. Bayshore Networks announce support in January 2014.

```
Network Working Group                                          M. Smith
Internet-Draft                                               R. Kandula
Intended status: Informational                            Cisco Systems
Expires: July 21, 2014                                  January 17, 2014


                 Source-Group Tag eXchange Protocol (SXP)
                        draft-smith-kandula-sxp-00

Abstract

   This document discusses source-group tag exchange protocol (SXP), a
   control protocol to propagate IP address to Source Group Tag (SGT)
   binding information across network devices.
```


A Systems Approach to Building an Identity Access Control Architecture

Cisco live!

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

NAC Agent

Web Agent

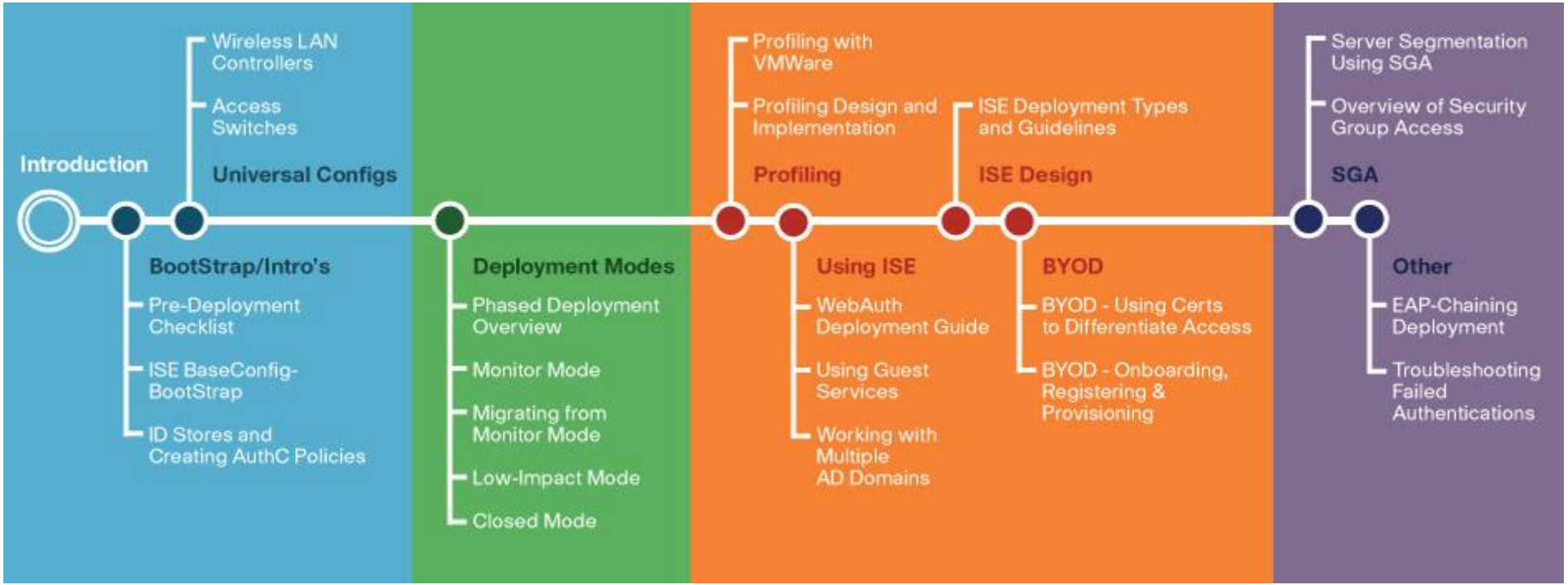
No-Cost Persistent and Temporal Clients for Posture, and Remediation

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



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

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.

Call to Action

- **Visit** the Cisco Campus at the World of Solutions to experience the following demos/solutions in action:
- **Meet** the Engineer, **Discuss** your project's challenges
- **Visit** CiscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!

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

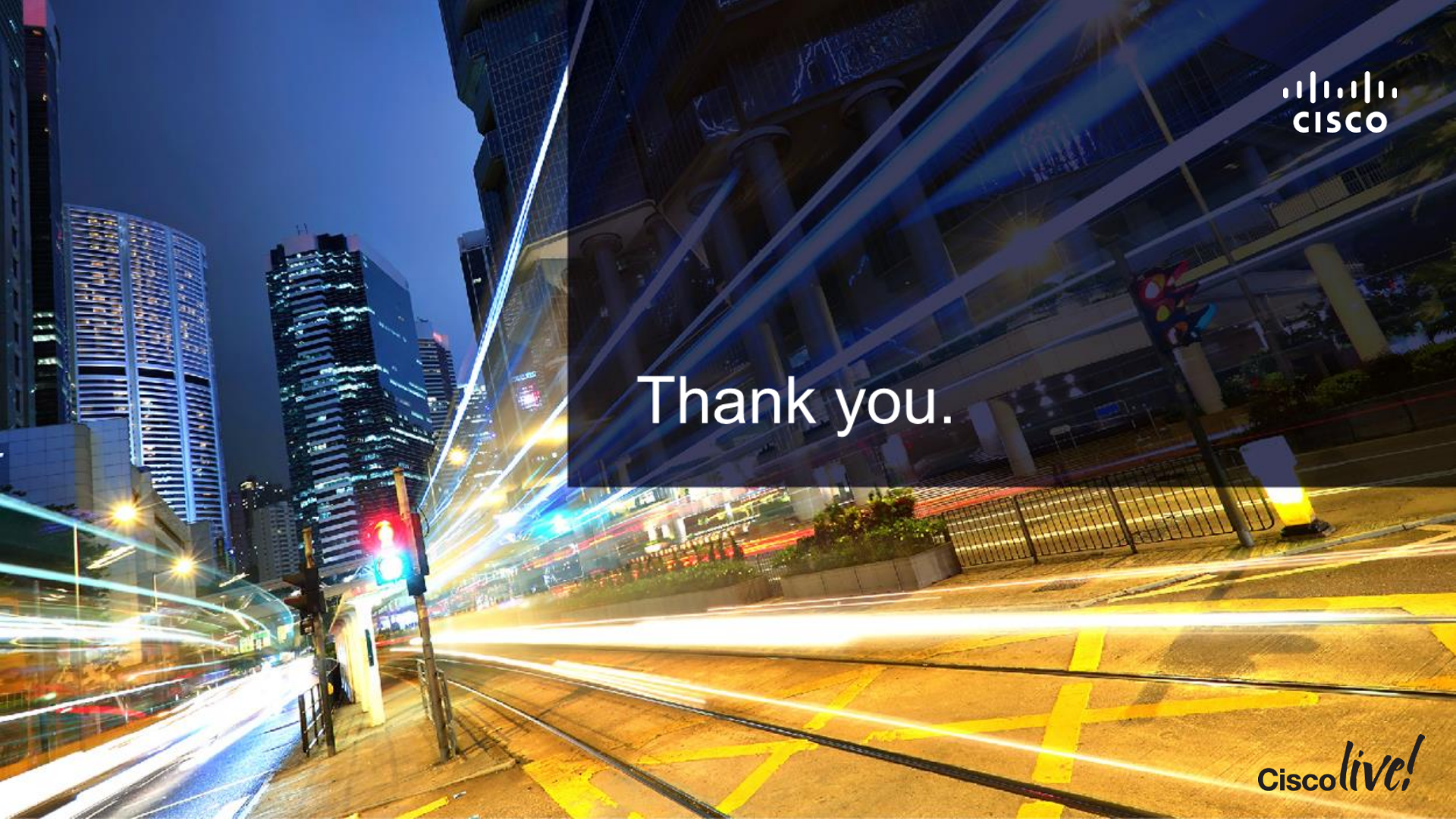
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

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 http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 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


Thank you.
cisco
Cisco live!

CISCO