



*TOMORROW
starts here.*

Cisco *live!*



Written to Realised Security Policy

BRKSEC-1011

Yuval Shchory

Manager, Product Management, SBG

#clmel

Cisco *live!*

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 (ISE).

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 and **ISE 1.3 new features** will be introduced.

The Cisco live! logo, featuring the word "Cisco" in a standard sans-serif font and "live!" in a stylized, handwritten-style font.

Housekeeping

 Reference slides will be in the published version only

 Visit Cisco Live Online: CiscoLive.com

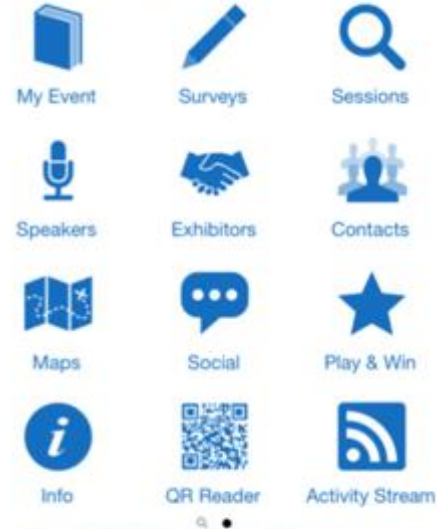
 Questions are welcome! Try our new online Q&A!

 Please use the microphone if exists

 Please put your phone on stun

 Visit the World of Solutions and Meet the Engineer

 Feedback welcome. Please complete online evaluation



CiscoLive!

Agenda

- Introduction & Welcome
- Secure Access Architecture
- Gaining Visibility
- Authenticating and Authorising
- Visitation Rules
- Keeping the Network Clean
- Connecting not-so-Geeky Geeks
- Securing by Roles in the Network
- Sharing Context
- Summary



Agenda

- Introduction & Welcome
- **Secure Access Architecture**
- Gaining Visibility
- Authenticating and Authorising
- Visitation Rules
- Keeping the Network Clean
- Connecting not-so-Geeky Geeks
- Securing by Roles in the Network
- Sharing Context
- Summary



Security Challenges vs Tools

Do You Use the Right Tool?

- Visibility
 - What is connected to my network
 - How do I identify, classify tomorrow's devices
- Cost Control
 - ACL and VLANs are expensive to maintain and are highly topology dependent
- Easy setup :
 - guests, BYOD, Remote Access
- Security
 - Before : Preventing through segmentation
 - During : Identifying anomalous behaviour
 - After : Quarantine to remediate

The screenshot shows the Cisco Systems Network Configuration interface. The main window is titled "Network Configuration" and contains a sub-section for "Add AAA Client". The form includes the following fields and options:

- AAA Client Hostname: WLC
- AAA Client IP Address: 172.16.1.30
- Key: disco123
- Authenticate Using: RADIUS (Cisco Airespace)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure):
- Log Update/Watchdog Packets from this AAA Client:
- Log RADIUS Tunneling Packets from this AAA Client:
- Replace RADIUS Port info with Username from this AAA Client:

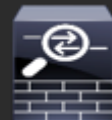
At the bottom of the form, there are three buttons: "Submit", "Submit + Apply", and "Cancel". Below the buttons is a "Back to Help" link.

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

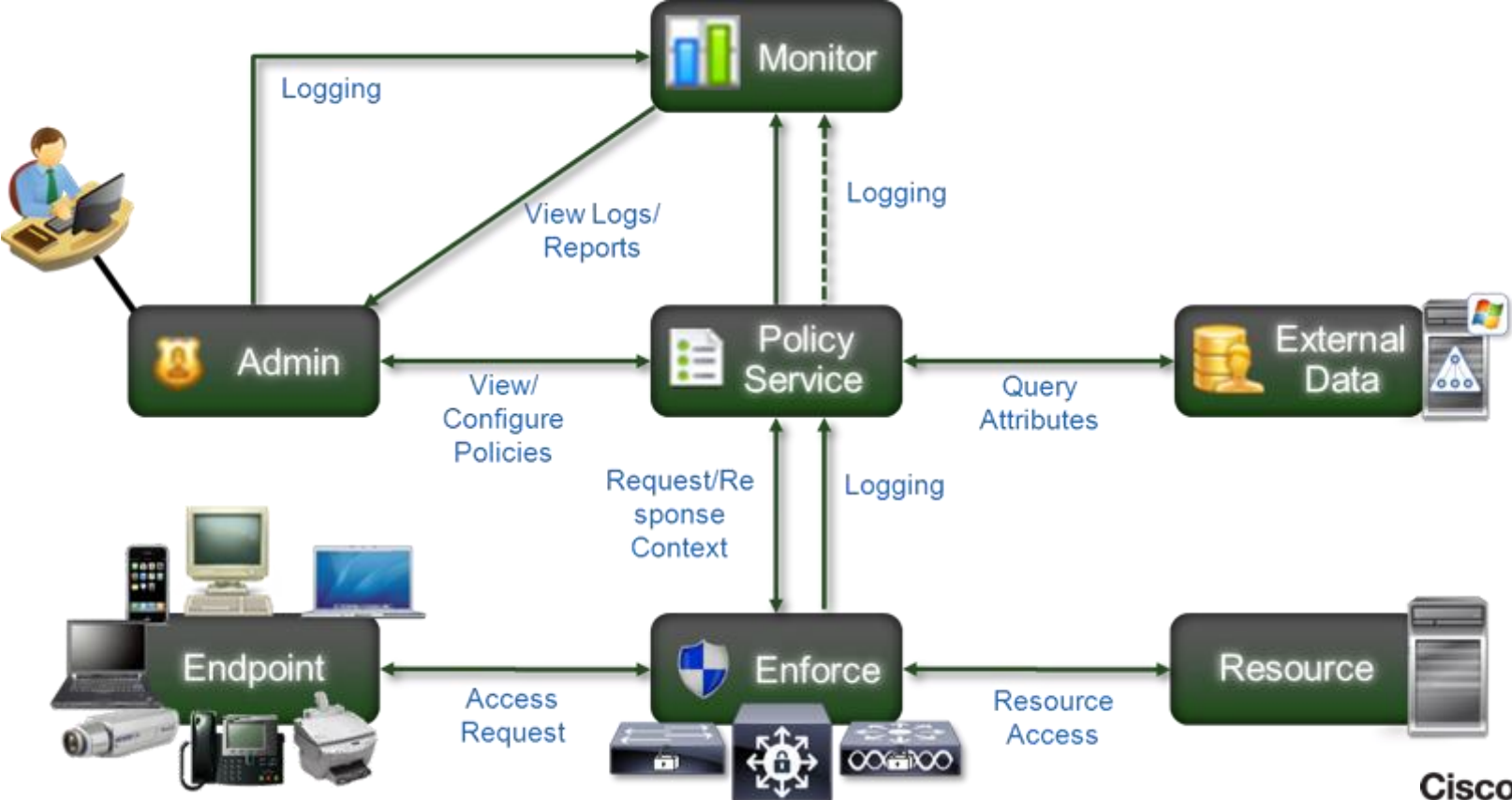


802.1X Supplicant
AnyConnect or
OS-Embedded Supplicant

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



ISE Policy Architecture



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](#), including:
 - Profiling Technologies
 - RADIUS
 - IEEE 802.1X (Dot1x)
 - Guest Services
 - Device Management
 - TrustSec
 - MACsec (802.1AE)
 - Identity Services Engine (ISE)



Cisco Identity Services Engine (ISE)

All-in-One Enterprise Policy Control



Identity
Context



Who



What



Where



When



How

Security Policy Attributes



Cisco® ISE



Business-Relevant
Policies

Wired

Wireless

VPN



Virtual machine client, IP device, guest, employee, and remote user



The Importance of Contextual Identity

Agenda

- Introduction & Welcome
- Secure Access Architecture
- **Gaining Visibility**
- Authenticating and Authorising
- Visitation Rules
- Keeping the Network Clean
- Connecting not-so-Geeky Geeks
- Securing by Roles in the Network
- Sharing Context
- Summary





Visibility
Network?

“What” is Connecting to My

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



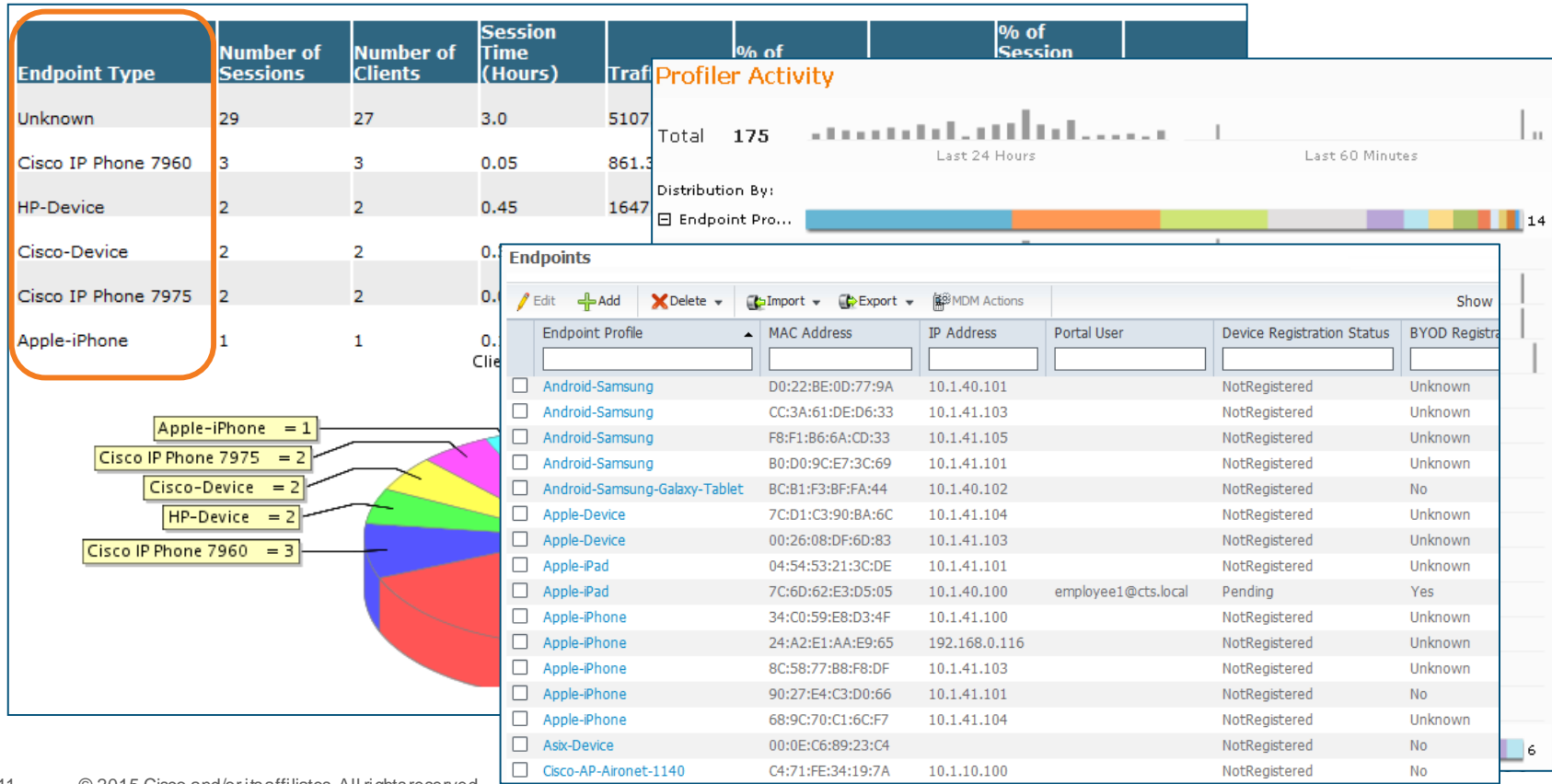
PCs	Non-PCs			
	UPS	Phone	Printer	AP

- What Profiling is NOT:

- An authentication mechanism.
- An exact science for device classification.

Profiling Technology

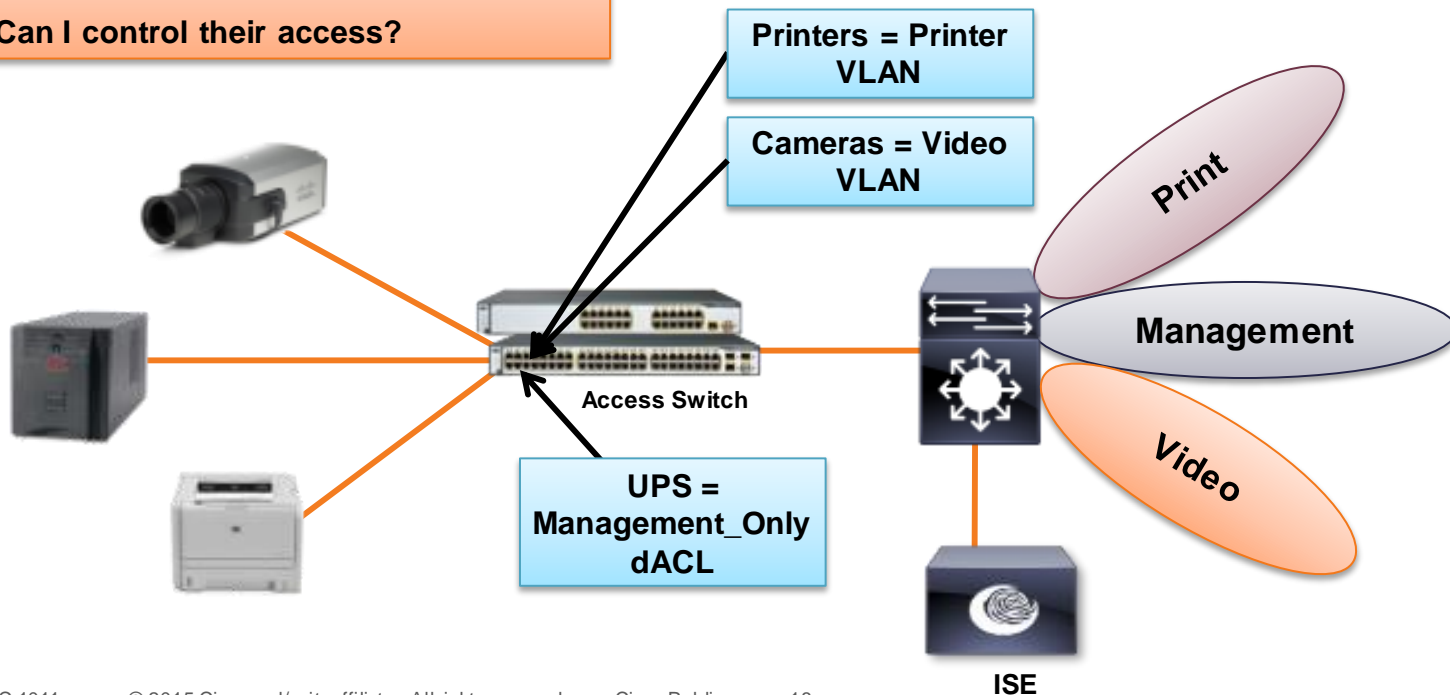
Visibility Into What Is On the Network



Profiling Non-User Devices

Dynamic Population of MAB Database Based on Device Type

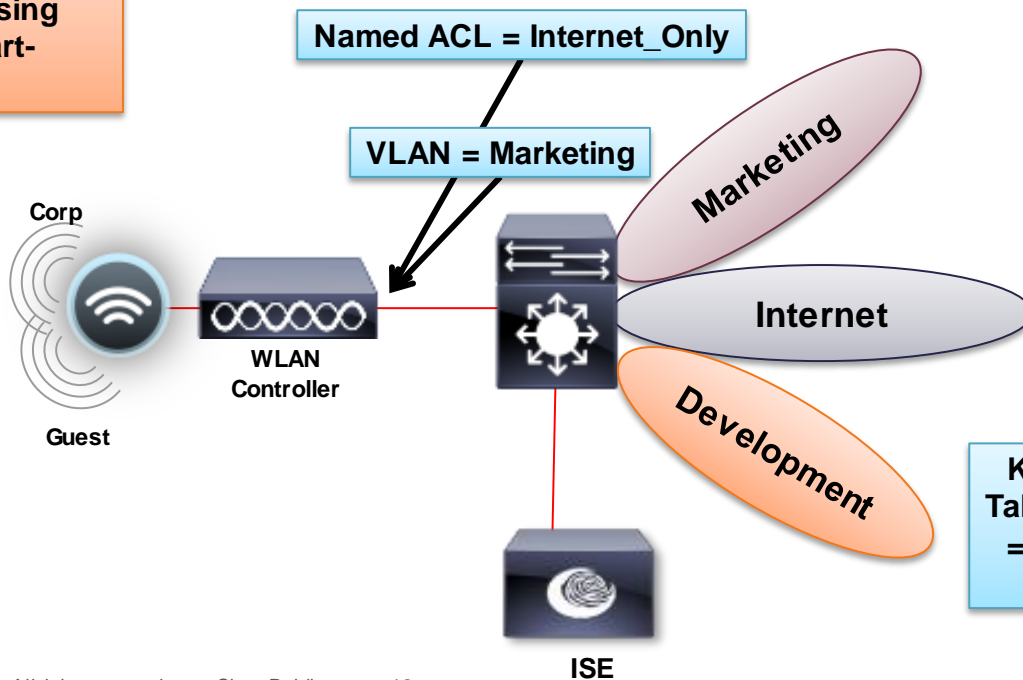
- How do I discover non-user devices?
- Can I determine what they are?
- Can I control their access?



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

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

Profiling Technology

How Do We Classify a Device?



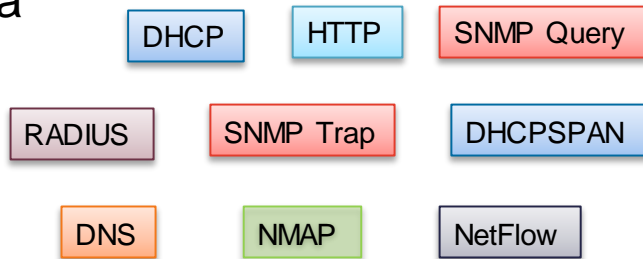
- Profiling uses signatures (similar to IPS)

```
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

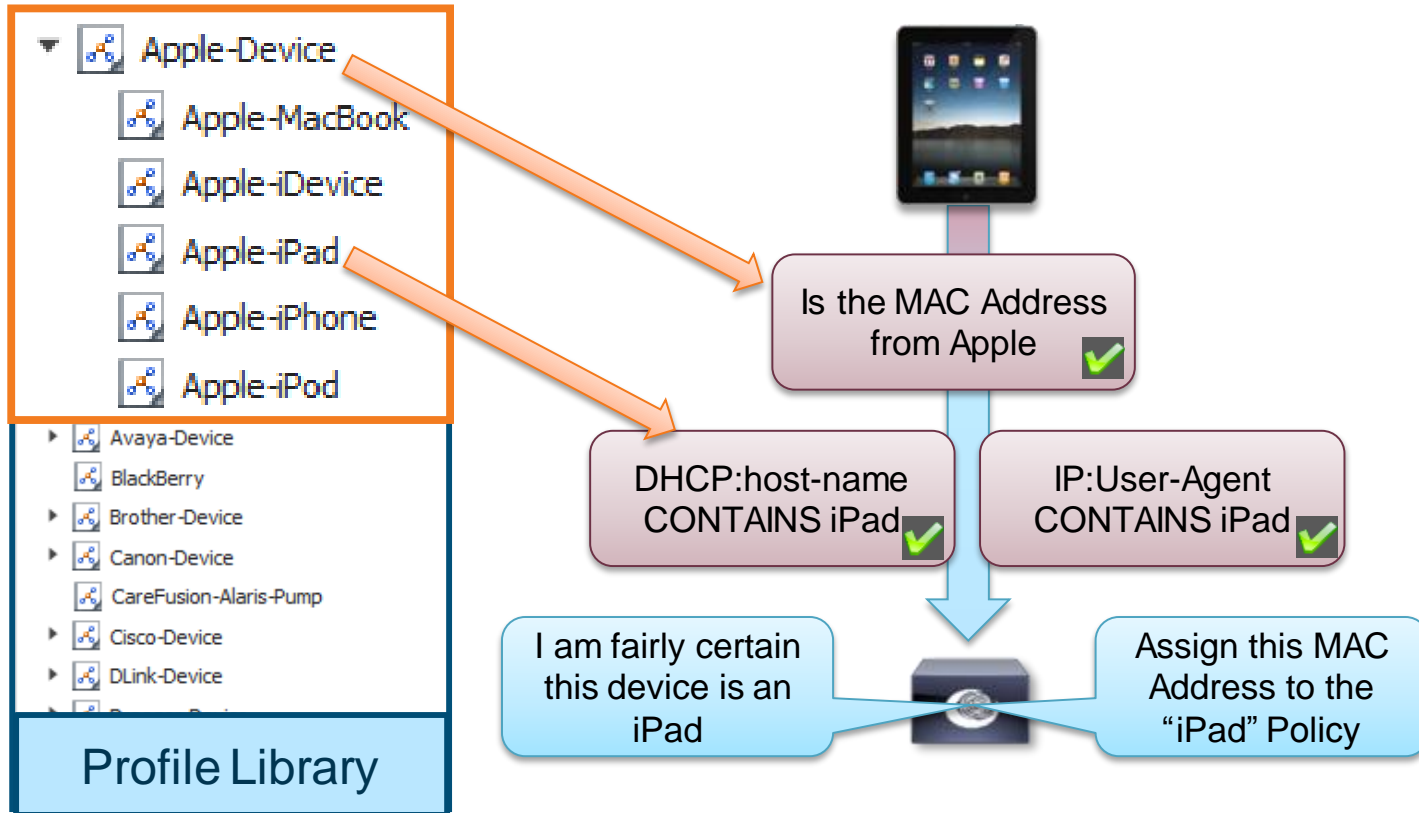


Endpoint List > B8:C7:5D:D4:95:32

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

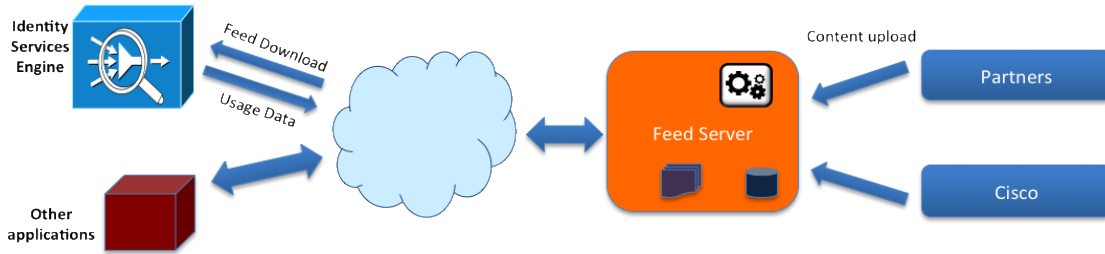
Profiling Policy Overview

Profile Policies Use a Combination of Conditions to Identify Devices



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.

Identity Services Engine | Home | Operations | System | Identity Management | Network Resources | Web Portal

Profiler

Feed Service

Profiler Feed Service Configuration

- Enable Profiler Feed Service

Feed Service Scheduler

Automatically check updates at: HH:MM UTC every day

01:00 UTC every day

Administrator Notification Options

- Notify administrator when download occurs

Administrator email address: admin@cts.local

Update Information and Options

Latest applied feed occurred on:

Feed Service Subscriber Information

- Provide subscriber information to Cisco

Administrator first name: Craig | Administrator email: chyps@cis.com

Agenda

- Introduction & Welcome
- Secure Access Architecture
- Gaining Visibility
- **Authenticating and Authorising**
- Visitation Rules
- Keeping the Network Clean
- Connecting not-so-Geeky Geeks
- Securing by Roles in the Network
- Sharing Context
- Summary





Verification



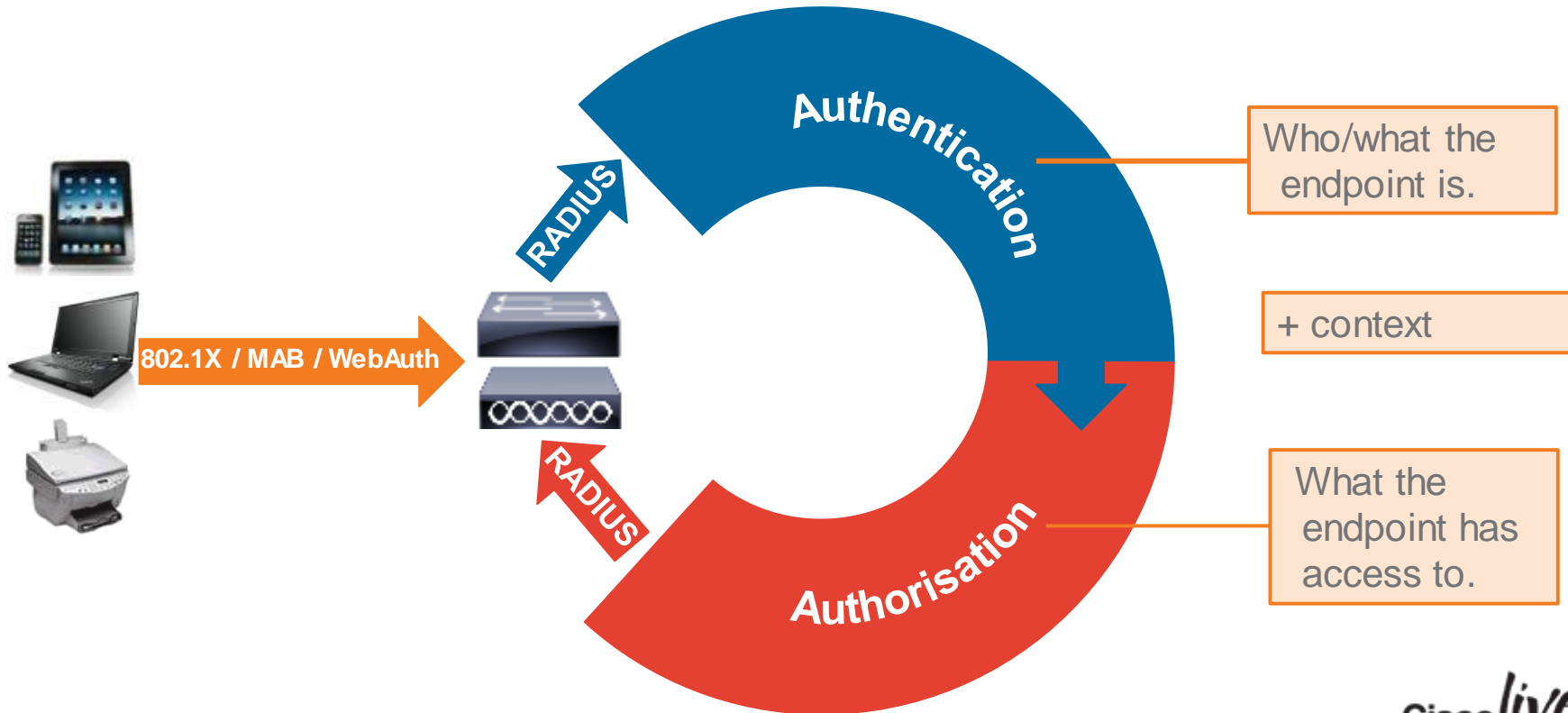
Control

Authentication, Authorisation, and Accounting

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

Authentication and Authorisation

What's the Difference?



Separation of Authentication and Authorisation

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The main content area is divided into several sections:

- Policy Sets:** A sidebar on the left shows a list of policy sets: Global Exceptions, Wired, **Wireless** (highlighted with a black box), VPN, and Default. A blue box labeled 'Policy Groups' with an arrow points to this sidebar.
- Policy Set Condition:** A purple box highlights the 'Wireless' policy set in the main area.
- Authentication Policy:** A blue box labeled 'Authentication' highlights the 'Authentication Policy' section, which contains rules for MAB, MACwLWA, Default, Dot1X, and a Default Rule.
- Authorization Policy:** An orange box labeled 'Authorisation' highlights the 'Authorization Policy' section, which includes a table of rules.
- Internal Users:** A red box highlights the 'Internal Users' configuration, showing the 'Identity Source' as 'example.com' and 'Options' for failed authentication: 'If authentication failed' (Reject), 'If user not found' (Continue), and 'If process failed' (Drop). An orange box labeled 'Default from ISE 1.3' points to the 'Continue' option.

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

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

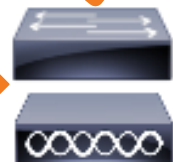
Dot1X : If **Wired_802.1X** allow protocols **Allowed Protocol : Default Network** and... Default : use **example.com**

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

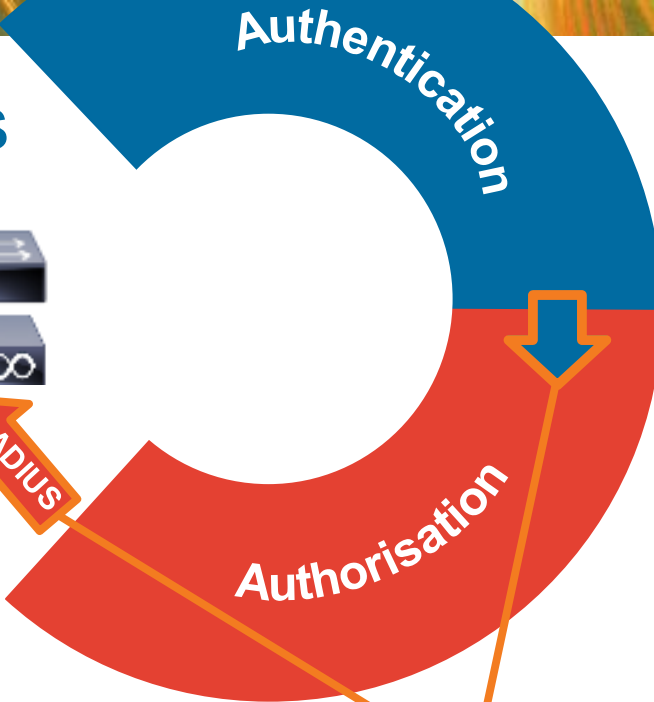
Authentication Options



802.1X / MAB / WebAuth



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.

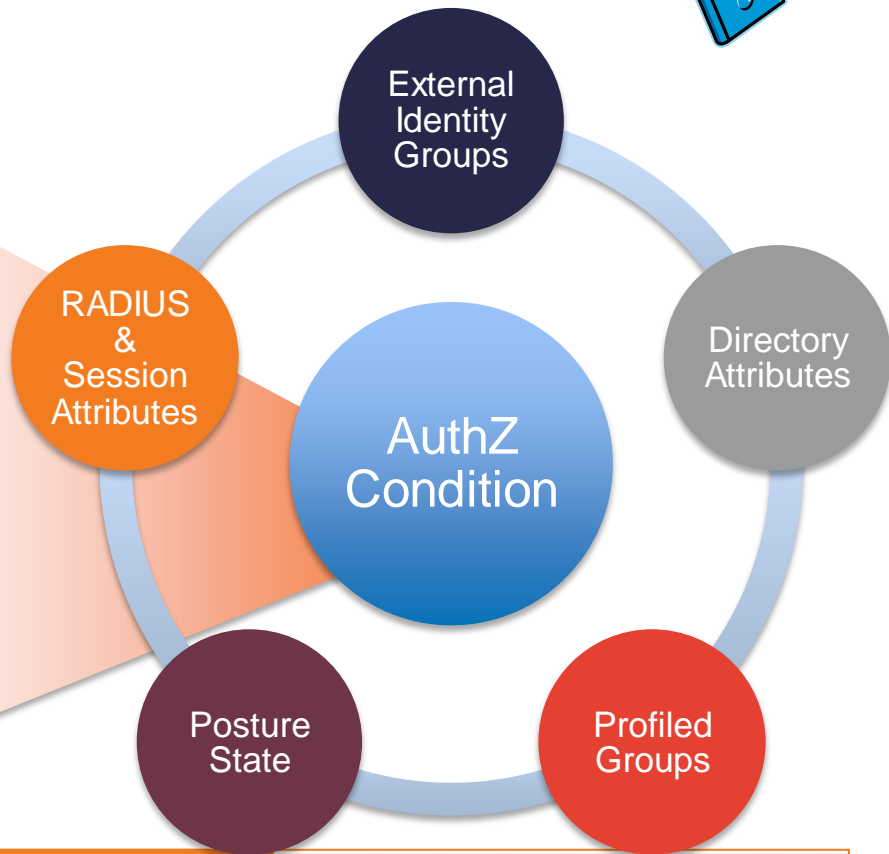
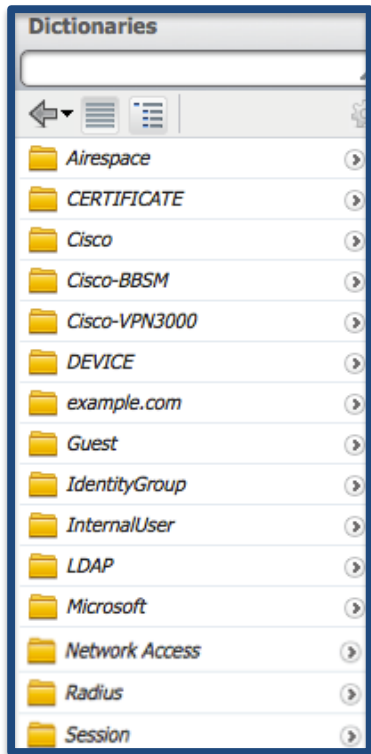
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones

context





Authorisation Conditions



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

Detailed Visibility into Passed/Failed Attempts

The screenshot displays the Cisco Identity Services Engine (ISE) interface. At the top, navigation tabs include Home, Operations, Policy, and Administration. A secondary navigation bar contains Authentication, Reports, Endpoint Protection Service, and Troubleshoot. Below this, a summary row shows key metrics: Misconfigured Suppliers (4), Misconfigured Network Devices (10), RADIUS Drops (226), Client Stopped Responding (1488), and Repeat Counter (5848).

The main content area features a table of authentication sessions. A red circle highlights a failed attempt at 2013-06-07 07:59:13.044. An arrow points from this row to a detailed view window. This window is divided into three sections: Authentication Details, Failure Reason, and Steps.

Authentication Details:

Source Timestamp	2012-12-13 19:47:05.506
Received Timestamp	2012-12-13 19:47:05.508

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

At the bottom left, the text 'BRKSEC-1011 © 2013' is visible.

Agenda



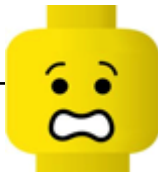

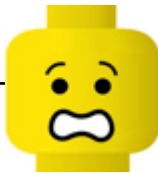

- Introduction & Welcome
- Secure Access Architecture
- Gaining Visibility
- Authenticating and Authorising
- **Visitation Rules**
- Keeping the Network Clean
- Connecting not-so-Geeky Geeks
- Securing by Roles in the Network
- Sharing Context
- Summary



A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, a modern pedestrian bridge spans across the street, illuminated with blue lights. Tall buildings with lit windows and colorful architectural lighting (including red and blue) form the city skyline. The overall atmosphere is one of a bustling, modern urban environment.

Identity Services Engine Guest Services

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:


Password:

Username:


Password:

Guest Access: Life Cycle Management



Provision 


Create Guest Accounts in the Sponsor Portal

Manage 

Create Sponsor Policy


Manage sponsor groups

Customise Portals

Notify 

Notify Guest using different method

- Print
- Email
- SMS

Report 

Report on all aspects of Guest Accounts

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

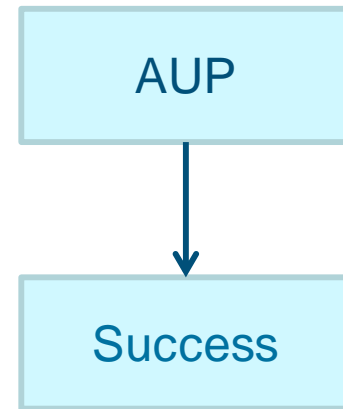
The screenshot displays the Cisco Identity Services Engine (ISE) configuration page for Guest Access. The main heading is 'Configure Guest and Sponsor Access'. On the left, there are five menu items: Overview, Guest Portals, Guest Types, Sponsor Groups, and Sponsor Portals. The 'Guest Portals' menu item is selected and highlighted in blue. On the right, the 'Guest Portals' configuration area is shown, with a sub-heading 'Guest Portals' and a description: 'Choose one of the three pre-defined portal types, which you can edit or delete'. Below this, there are three portal types listed, each with a 'Create' button and a green checkmark indicating it is used in specific authorization rules:

- Hotspot Guest Portal (default)**: Guests do not require username and password credentials to access the network. Used in 2 rules in the Authorization policy.
- Self-Registered Guest Portal (default)**: Guests are allowed to create their own accounts and access the network. Used in 1 rule in the Authorization policy.
- Sponsored Guest Portal (default)**: Sponsors create guest accounts, and guests access the network. Used in 1 rule in the Authorization policy.

Hotspot



Day Ends



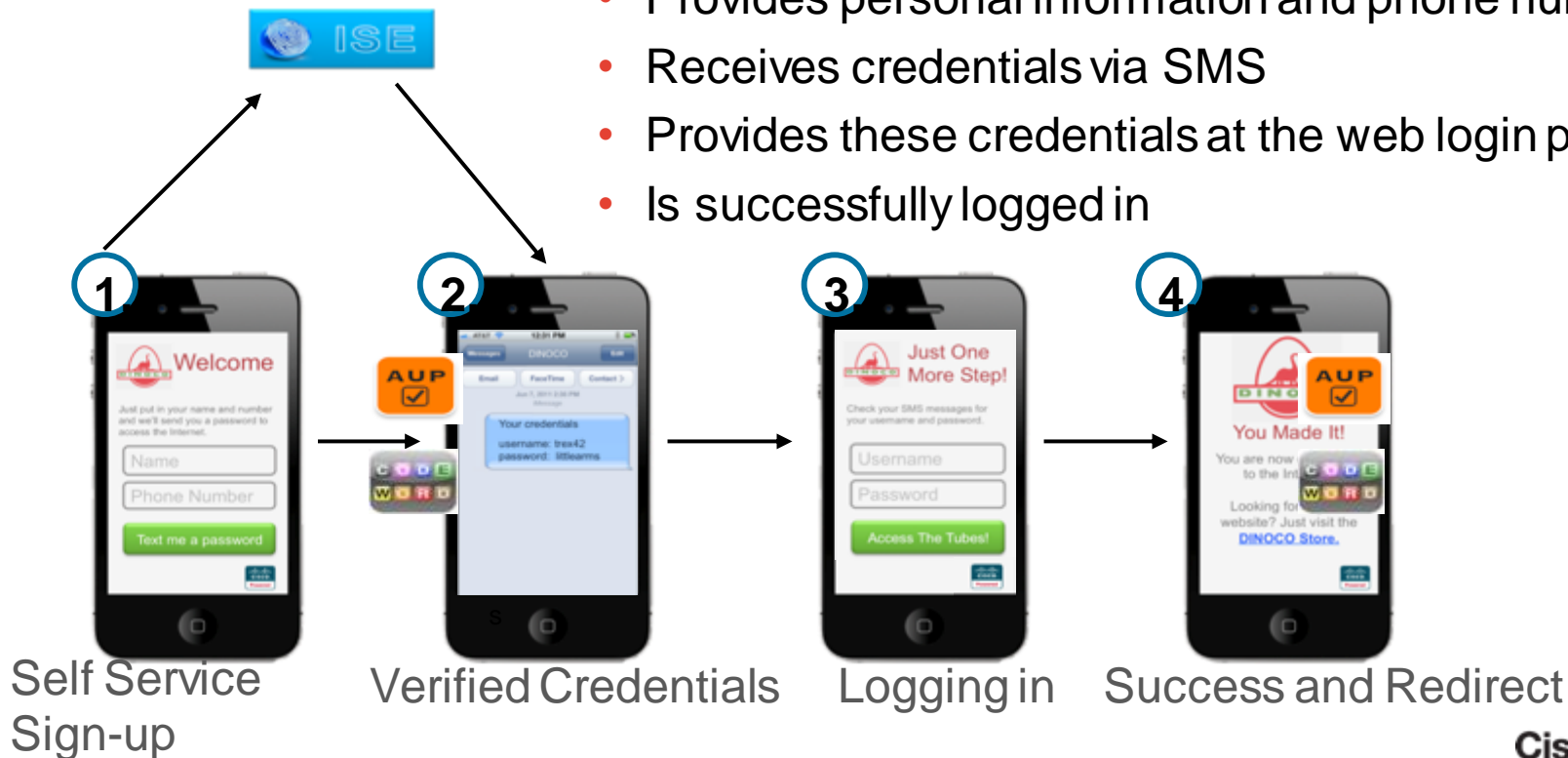
Goal: Get them on the Internet with AUP acceptance no matter who they are and remember them so you don't get in their way each time they connect.



Self-Registered Guest Access with SMS

The user

- Provides personal information and phone number
- Receives credentials via SMS
- Provides these credentials at the web login page
- Is successfully logged in



Streamlined Sponsor Portals

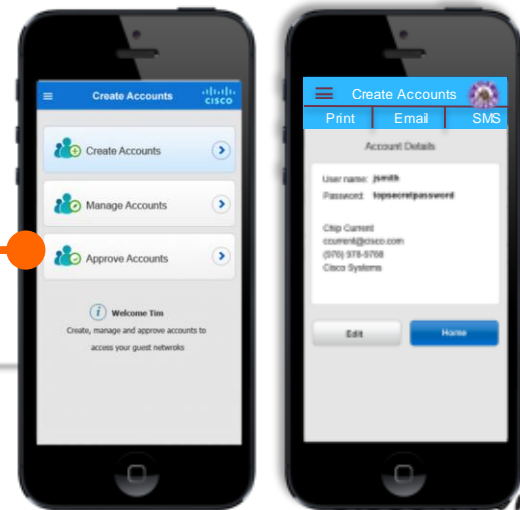
Branding with Themes!

Streamlined Guest Creation

Quickly create single or multiple accounts

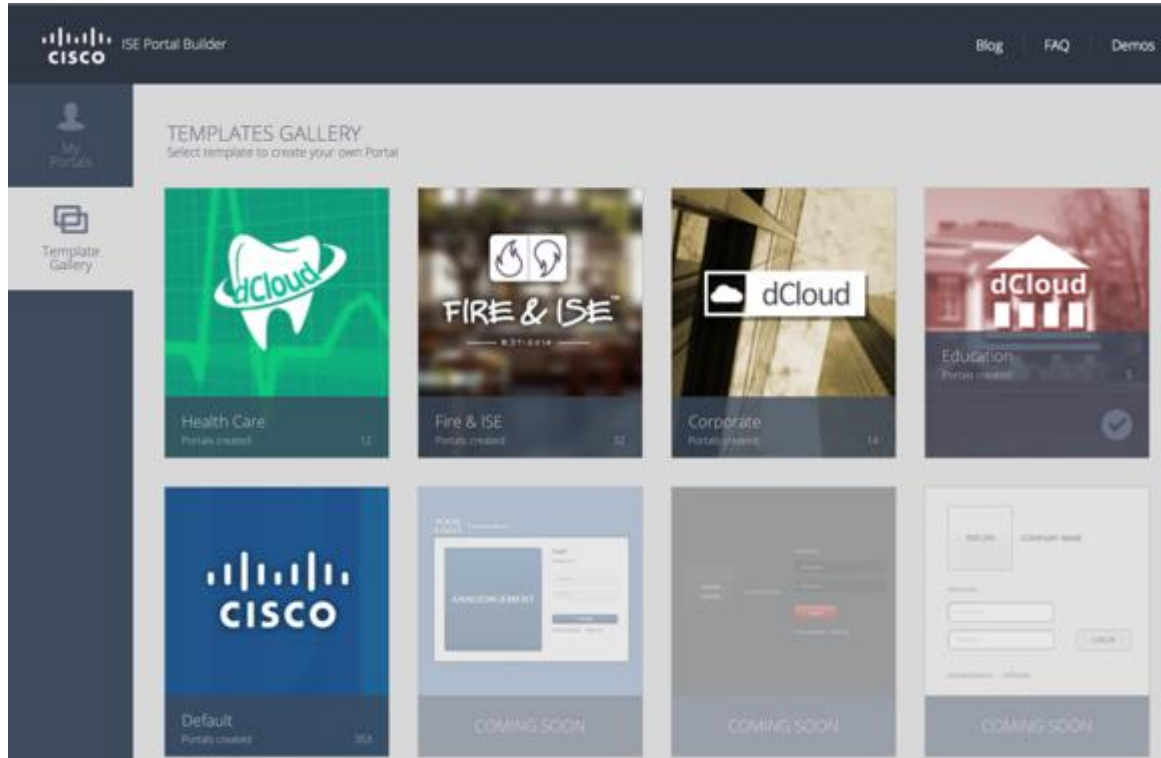
Mobile Sponsors

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



How Could I Create My Own Portal in Minutes?

<https://isepb.cisco.com>

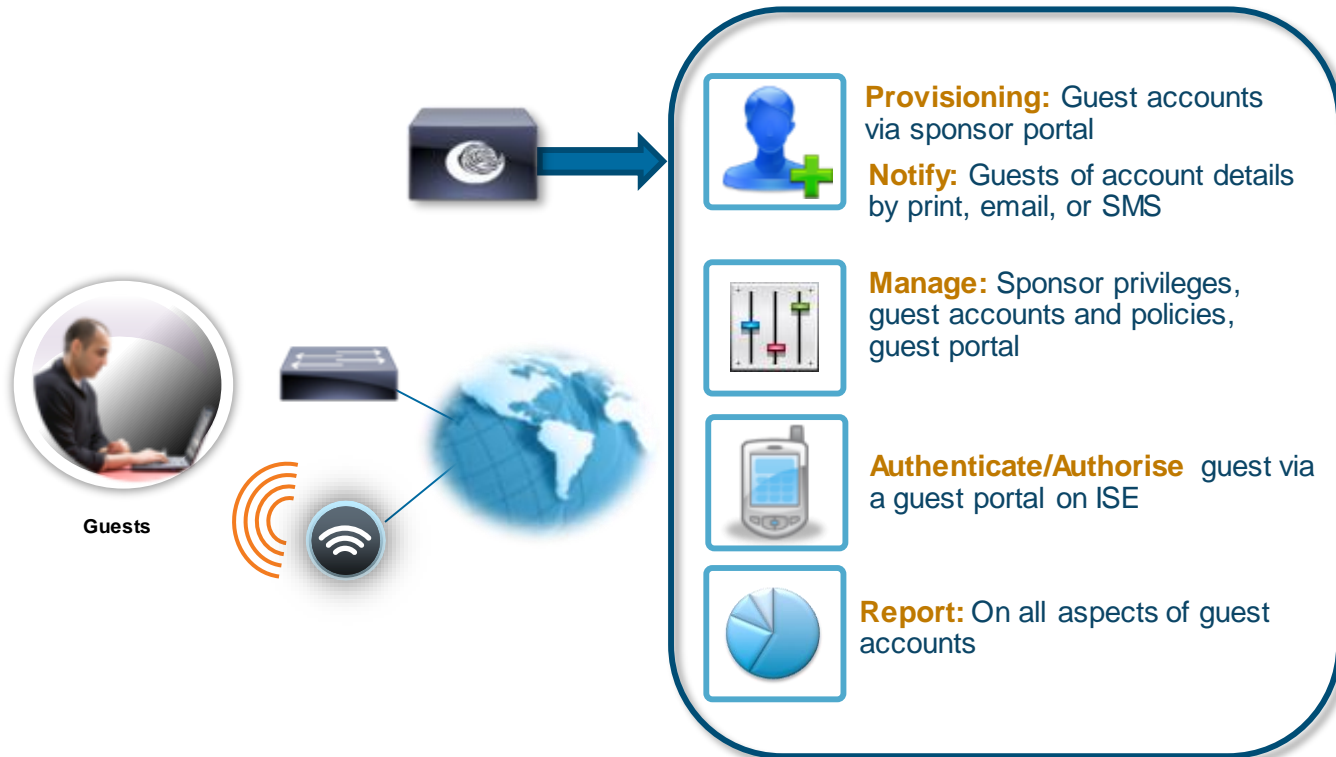


- 17 languages
- All portal support (hotspot, self registered, BYOD, ...)



CiscoLive!

Components of a Full Guest Lifecycle Solution



Agenda

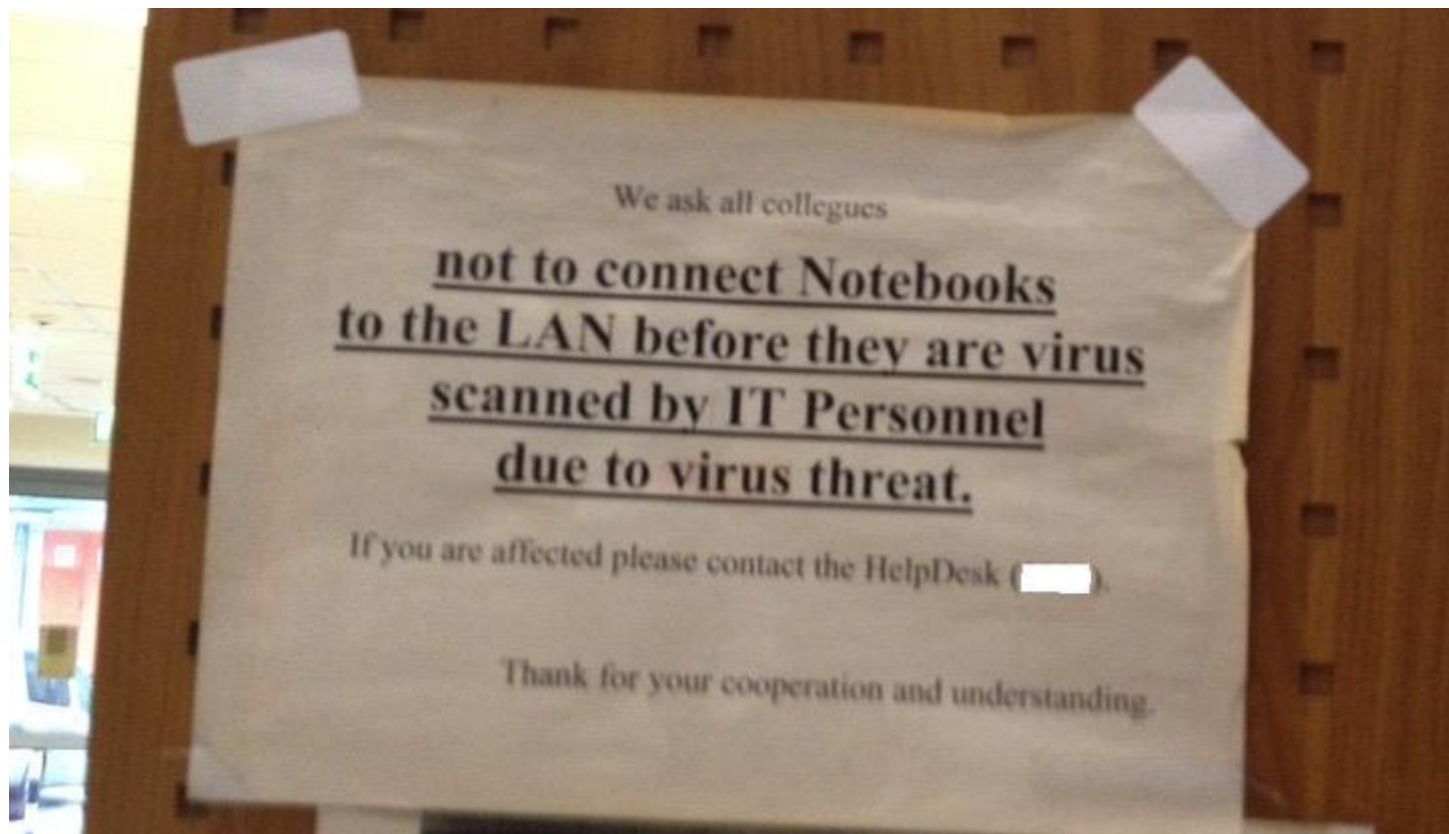
- Introduction & Welcome
- Secure Access Architecture
- Gaining Visibility
- Authenticating and Authorising
- Visitation Rules
- **Keeping the Network Clean**
- Connecting not-so-Geeky Geeks
- Securing by Roles in the Network
- Sharing Context
- Summary





Posture
Are My Endpoints Compliant?

Are My Endpoints Compliant?

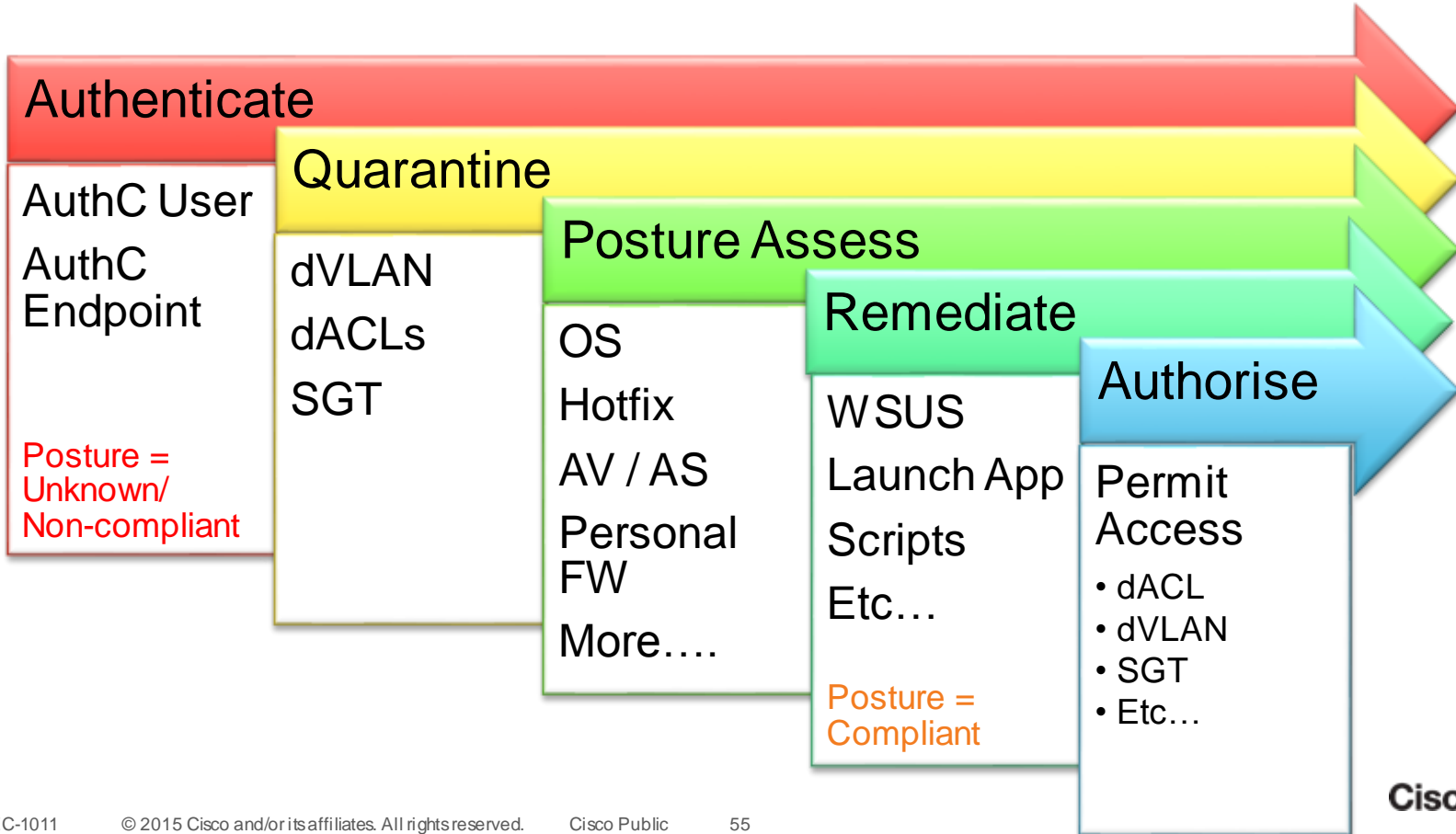


Posture Assessment



- Does the PC Desktop 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



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

The screenshot displays a Windows File Explorer window showing the path Local Disk (C:) > Windows > System32. The 'Files' folder is circled in red. Below it, the 'Services (Local)' folder is also circled in red. Overlaid on this is the Windows Task Manager window, with the 'Processes' tab selected and circled in red. The Task Manager window shows a list of processes with columns for Image Name, User Name, CPU, Memory, and Description. Below the Task Manager is the Registry Editor window, with the 'Registry Editor' title bar circled in red. The Registry Editor shows the tree view expanded to Computer > HKEY_CURRENT_USER, and the right pane shows the (Default) value of type REG_SZ.

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.				
vpui.exe				

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

Posture Lease

Once postured compliant, user may disconnect/reconnect multiple times before re-posture

ise | admin | Logout | Feedback

CISCO Identity Services Engine

Home Operations Policy Guest Access Administration

System Identity Management Network Resources Device Portal Management pxGrid Services Feed

pxGrid Identity Mapping

Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings

Settings

- Client Provisioning
- Endpoint Protection Service
- FIPS Mode
- Alarm Settings
- Posture
 - General Settings

Posture General Settings

Remediation Timer Minutes

Network Transition Delay Seconds

Default Posture Status

Automatically Close Login Success Screen After Seconds

Posture Lease

Perform posture assessment every time a user connects to the network

Posture Lease

- Perform posture assessment every time a user connects to the network
- Perform posture assessment every Days

Valid range 1 to 365 days.

Note : This configuration applies only to AnyConnect Agent and not to NAC Agent and Web Agent.

Agenda

- Introduction & Welcome
- Secure Access Architecture
- Gaining Visibility
- Authenticating and Authorising
- Visitation Rules
- Keeping the Network Clean
- **Connecting not-so-Geeky Geeks**
- Securing by Roles in the Network
- Sharing Context
- Summary



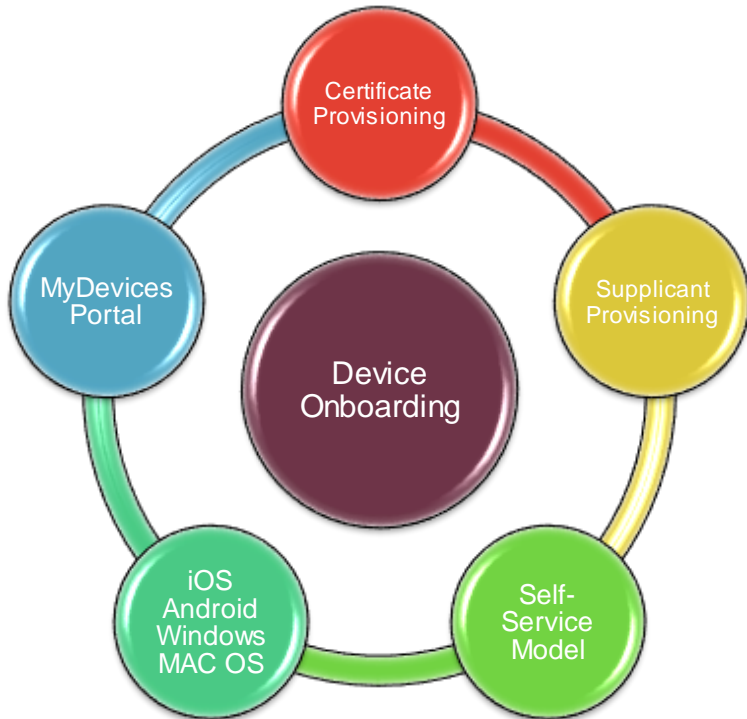
A nighttime photograph of a city street with light trails from cars. In the background, there are modern buildings, some with blue and purple lighting. A pedestrian bridge spans across the street. The foreground is dominated by long, curved light trails in yellow, orange, and red, suggesting a long exposure of traffic.

BYOD

Extending Network Access to Personal Devices

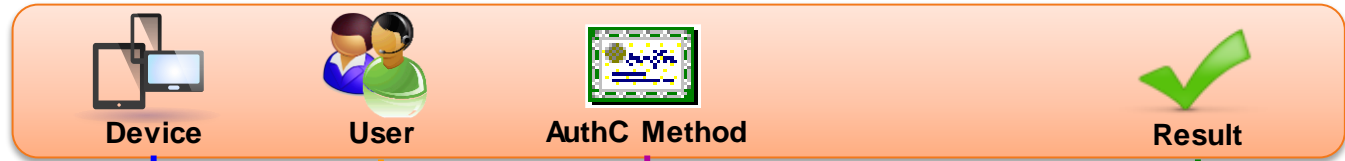
Onboarding Personal Devices

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 & 7
 - 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.

BYOD Policy in ISE



Registered?
Cert SAN value = MAC?

AD Employee?

Employee Access

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

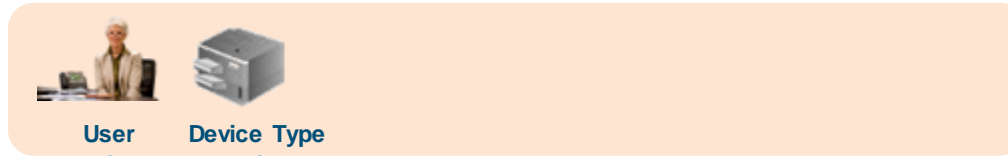
Auth Method = Cert?

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)

ISE Authorisation Policy Definition



- Simple



Authorization Policy At A Glance
First Matched Rule Applies

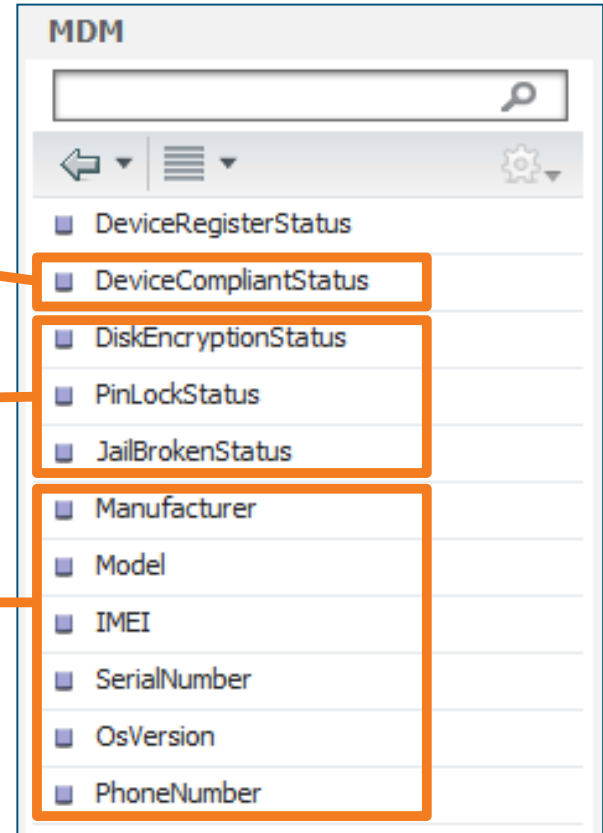
Standard				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
✓ Enabled	Profiled Cisco IP Phones	Cisco-IP-Phone		Cisco_IP_Phones
✓ Enabled	Employee	Any	AD1:ExternalGroups EQUALS demo.local/Users/employees	PermitAccess
✓ Enabled	Guest	Guest		Guest
✓ Enabled	Default	Any		Web_Auth

Enforcement Policy

- Permissions = Authorisations
- Defines the access control policy and other attributes to be applied to the auth session.

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
 - If result of periodic recheck shows that a connected device is no longer compliant, ISE sends a CoA to terminate session.



MDM Integration Example with Meraki EMM

External MDM Server List > meraki

MDM Server details

* Name: meraki

* Hostname or IP Address: n100.meraki.com

* Port: 443

Instance Name:

* User Name: 1234567890ABC

* Password: *

Description:



* Polling Interval: 5 (minutes) ⓘ

Enable

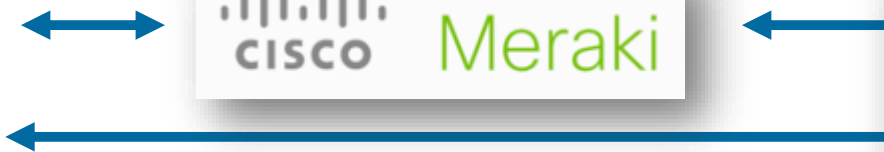
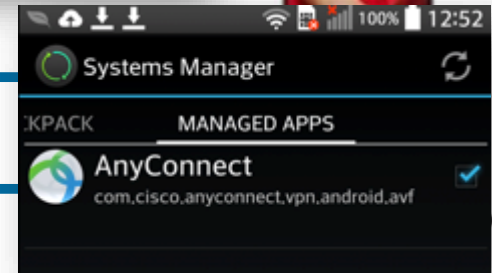
Test Connection

App management

Edit Scope ▾ Delete ▾ Push ▾ Search... ▾ 2 apps

<input type="checkbox"/>	#	OS	Name ▾	Scope
<input type="checkbox"/>	1	iOS	 Meraki Systems Manager	All devices
<input type="checkbox"/>	2	Android	 AnyConnect ICS+	All devices

- OS X
 - Disk encryption
- Windows
 - Antivirus running
 - Antispyware installed
- Mobile devices
 - Passcode lock
 - Device is not compromised ⓘ



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 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

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

Reporting

Mobile Device Management Report

Failure Reason

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

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
2013-12-20 18:02:53.506	iseندن		7C:40:42:43:05:05		fa112c5a00001e50043aa4	iOS 5.0	✓	✗	⊗	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact; Device administrator is deactivated; Password not set
2013-12-20 01:19:27.813	iseندن		7C:40:42:43:05:05		fa112c5a00001a8004367676	iOS 5.0	✓	✗	⊗	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact; Device administrator is deactivated; Password not set
2013-12-20 00:58:34.617	iseندن		7C:40:42:43:05:05		fa112c5a00001a10042525c6	iOS 5.0	✓	✗	⊗	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-20 00:22:39.484	iseندن		7C:40:42:43:05:05		fa112c5a00001a10042525c6	iOS 5.0	✓	✗	⊗	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2012-12-20 00:32:27.384	iseندن		7C:40:42:43:05:05		fa112c5a0000193504223f62	iOS 5.0	✓	✗	⊗	✓	✗	Apple	iPad		GB0149LVZ3A	PDA 2	Phone is out of contact
2013-12-20 01:15:12.138	iseندن		8C:41:43:6F:FA:44		fa112c5a00001990040c0a75	Android 4.3	✓	✓	⊗	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 01:15:05.2	iseندن		8C:41:43:6F:FA:44		fa112c5a00001990040c0a75	Android 4.3	✓	✓	⊗	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:57:20.815	iseندن		8C:41:43:6F:FA:44		fa112c5a00001990040c0a75	Android 4.3	✓	✓	⊗	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:49:29.929	iseندن		8C:41:43:6F:FA:44		fa112c5a00001990040c0a75	Android 4.3	✓	✓	⊗	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:04:48.153	iseندن		8C:41:43:6F:FA:44		fa112c5a00001990040c0a75	Android 4.3	✓	✓	⊗	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:42:30.446	iseندن		8C:41:43:6F:FA:44		fa112c5a00001990040c0a75	Android 4.3	✓	✓	⊗	✓	✓	samsung	GT-P5113			PDA 3	
2013-12-20 00:37:22.896	iseندن		8C:41:43:6F:FA:44		fa112c5a00001990040c0a75	Android 4.3	✓	✓	⊗	✓	✓	samsung	GT-P5113			PDA 3	
2012-12-19 00:36:50.482	iseندن		8C:41:43:6F:FA:44		fa112c5a0000199750c09c21	Android 4.3	✓	✓	⊗	✓	✓	samsung	GT-P5113			PDA 3	Device is not registered with MDM
2012-12-19 00:26:28.303	iseندن		8C:41:43:6F:FA:44		fa112c5a0000199750c09c21	Android 4.3	✓	✓	⊗	✓	✓	samsung	GT-P5113			PDA 3	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

From 01/09/2015 12:00:00.000 AM to 01/09/2015 12:22:01.014 PM

Page << 1 >> Records 1 to 2

Logged At	Server	Identity	Endpoint ID	IP Address	Session ID	Endpoint OS	Registration Status	MDM Compliance	Disk Encryption	PIN Lock	Rooted	Manufacturer
2015-01-09 12:12:59.636	ise		8C-3A-E3-72-		1f4ba8c00000001333a5af54	REL	✓	✓	⊗	⊗	✗	LGE
2015-01-09 11:54:39.246	ise		8C-3A-E3-72-		1f4ba8c00000001333a5af54	REL	✓	✓	⊗	⊗	✗	LGE

Agenda

- Introduction & Welcome
- Secure Access Architecture
- Gaining Visibility
- Authenticating and Authorising
- Visitation Rules
- Keeping the Network Clean
- Connecting not-so-Geeky Geeks
- **Securing by Roles in the Network**
- Sharing Context
- Summary



A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, a modern pedestrian bridge with blue lighting spans across the street. Tall buildings with illuminated windows and storefronts line the street, and traffic lights are visible in the distance.

TrustSec Introduction

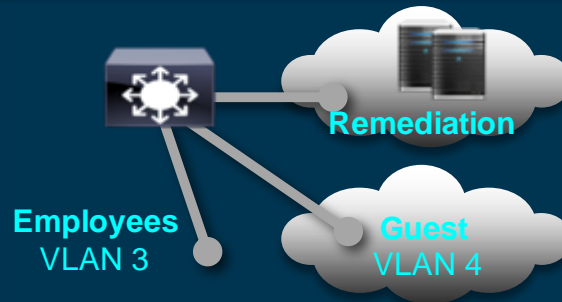
TrustSec Authorisation and Enforcement

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



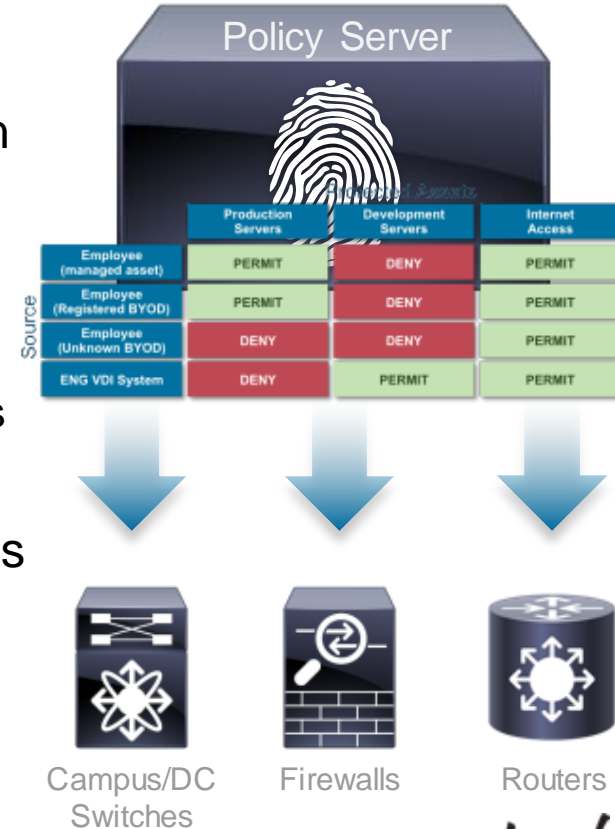
Security Group Access—SXP, SGT, SGACL, SGFW

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

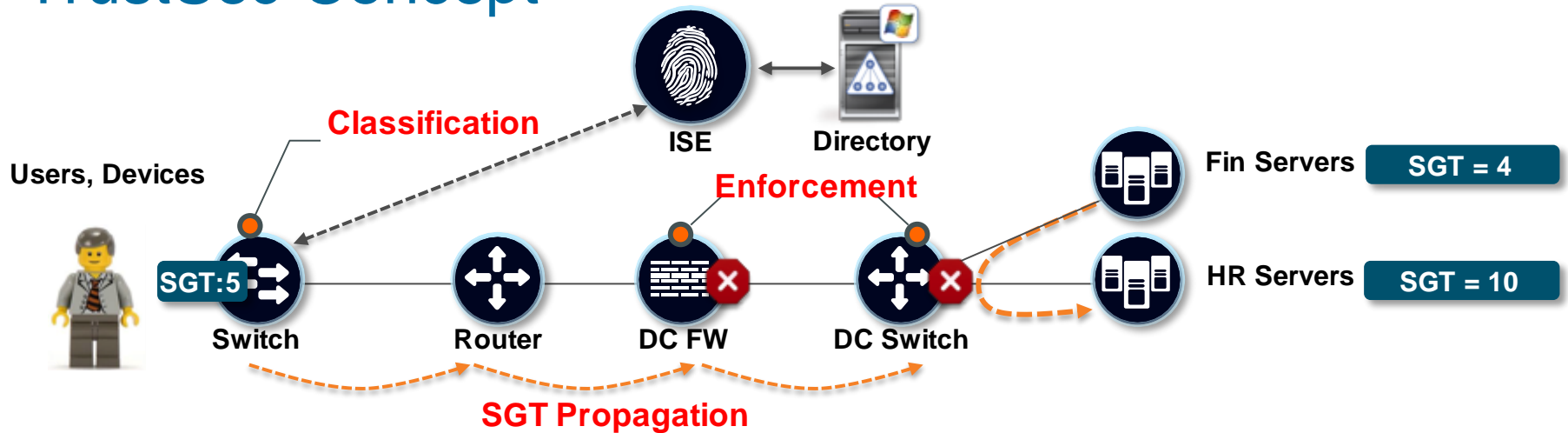
What is TrustSec?

- Software-defined segmentation technology supported in over **20 Cisco product families**
- PCI DSS validated
- Next-Generation Access Control Enforcement
 - Removes concern of TCAM space for detailed Ingress ACLs
 - Removes concern of ACE explosion on DC Firewalls
- Assign a TAG at login → Enforce that tag in the Campus / Branch / Data centre / Firewall
- Allows you to:
 - Segment network using logical security groups
 - Control access to assets based on security groups
 - Scale security enforcement

Centrally controlled by ISE

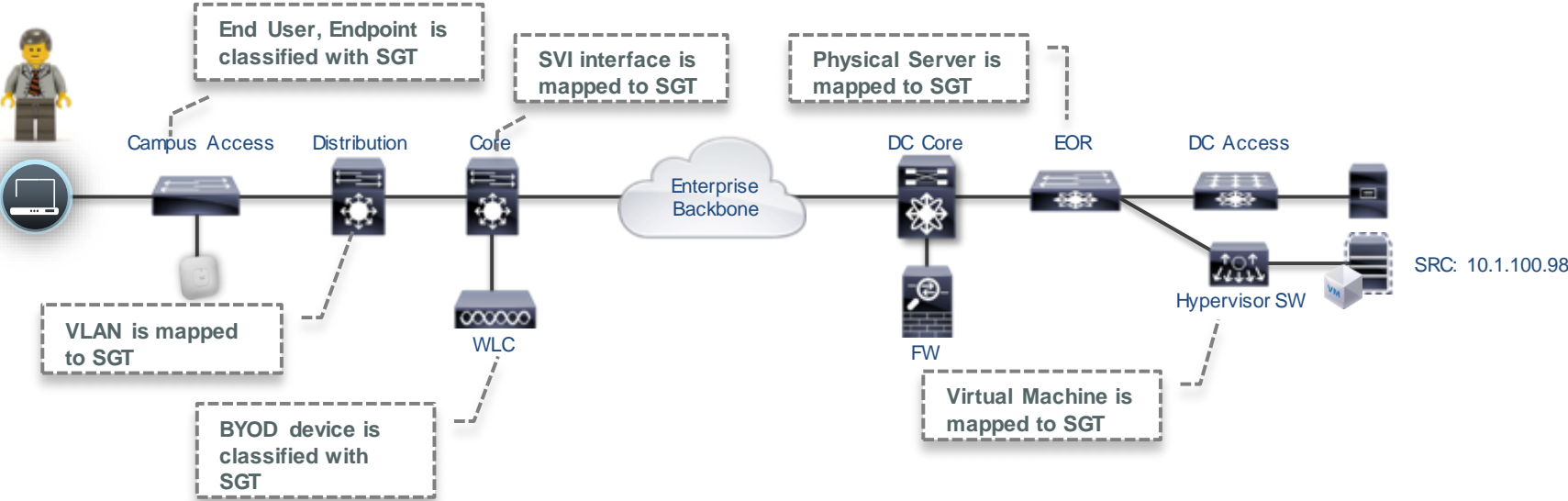


TrustSec Concept

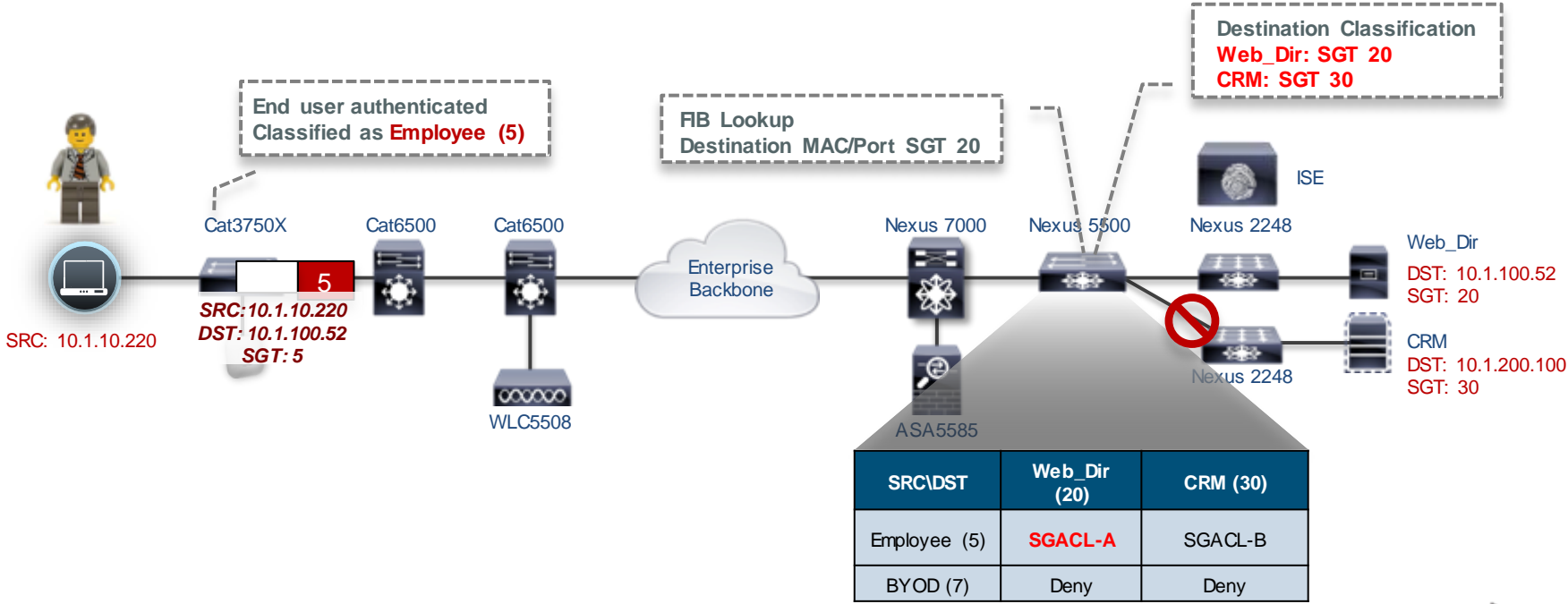


- Classification of systems/users based on **context** (user role, device, location, access method)
- A Security Group Tag (SGT) is assigned based on context
- SGT used by firewalls, routers and switches to make intelligent blocking decisions

SGT Assignments



How is Policy Enforced with SGACL



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	<input checked="" type="checkbox"/>	any			any		ip	Permit	TOP 10	
outside (9 incoming rules)											
1	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT Employee_SGT Management_SGT	any	Web_Servers	http https	Permit	0		
2	<input checked="" type="checkbox"/>	any		CC_Scanner_SGT	any	Web_Servers	http https	Deny	0		
3	<input checked="" type="checkbox"/>	any		Employee_SGT Management_SGT	any	Employee_Portal	http https	Permit	0		
4	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Employee_Portal	http https	Deny	0		
5	<input checked="" type="checkbox"/>	any		Management_SGT	any	Manager_Portal	50002 3389 http https sqlnet	Permit	0		
6	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT Employee_SGT CC_Scanner_SGT	any	Manager_Portal	ip	Deny	0		
7	<input checked="" type="checkbox"/>	any		Employee_SGT Management_SGT	any	Time_Card_Ser...	https	Permit	0		
8	<input checked="" type="checkbox"/>	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Time_Card_Ser...	https	Deny	0		
9	<input checked="" type="checkbox"/>	any		CC_Scanner_SGT	any	CreditCard_Ser...	https	Permit	0		

Source Tags

Destination Tags

Agenda

- Introduction & Welcome
- Secure Access Architecture
- Gaining Visibility
- Authenticating and Authorising
- Visitation Rules
- Keeping the Network Clean
- Connecting not-so-Geeky Geeks
- Securing by Roles in the Network
- **Sharing Context**
- Summary



A nighttime photograph of a city street. In the foreground, there are long, curved light trails from cars, primarily in shades of yellow and orange. In the middle ground, a pedestrian bridge with blue lighting spans across the street. In the background, there are several tall buildings with lit windows and some flags on poles. The overall scene is illuminated by city lights.

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.

Resources Dictionary

Get XML

Resource	Description	Current version	Framework object
<input type="radio"/> ers.ersresponse	ERS Response	1.0	v
<input type="radio"/> ers.searchresult	Search Result	1.0	v
<input type="radio"/> ers.updatefields	Updated Fields	1.0	v
<input checked="" type="radio"/> ers.versioninfo	Version Info	1.0	v
<input type="radio"/> identity.endpoint	End Point	1.0	
<input type="radio"/> identity.endpointgroup	EndPoints Identity Group	1.0	
<input type="radio"/> identity.identitygroup	Identity Group	1.0	
<input type="radio"/> identity.intermaluser	Internal User	1.0	
<input type="radio"/> sga.sgt	Security Groups	1.0	
<input type="radio"/> test.testresource	Test Resource	1.0	

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

API Dictionary

Get Request Example

Resource	Action	Method	Request Content	Response Content	URI
<input type="radio"/> End Point	Get version	GET	N/A	VersionInfo	https://10.1.100.2/ers/config/endpoint/versioninfo
	<input checked="" type="radio"/> Get by Id	GET	N/A	ERSEndPoint	https://10.1.100.2/ers/config/endpoint/{id}
	<input type="radio"/> List	GET	N/A	SearchResult	https://10.1.100.2/ers/config/endpoint
	<input type="radio"/> Delete	DELETE	N/A	N/A	https://10.1.100.2/ers/config/endpoint/{id}
	<input type="radio"/> Create	POST	ERSEndPoint	N/A	https://10.1.100.2/ers/config/endpoint
	<input type="radio"/> Update	PUT	ERSEndPoint	UpdateFieldsList	https://10.1.100.2/ers/config/endpoint/{id}
<input type="radio"/> Test Resource	Get version	GET	N/A	VersionInfo	https://10.1.100.2/ers/config/testresource/versioninfo
	<input type="radio"/> Get by Id	GET	N/A	ISETestResource	https://10.1.100.2/ers/config/testresource/{id}
	<input type="radio"/> Get all	GET	N/A	SearchResult	https://10.1.100.2/ers/config/testresource
	<input type="radio"/> Delete	DELETE	N/A	N/A	https://10.1.100.2/ers/config/testresource/{id}
	<input type="radio"/> Create	POST	ISETestResource	N/A	https://10.1.100.2/ers/config/testresource
	<input type="radio"/> Update	PUT	ISETestResource	UpdateFieldsList	https://10.1.100.2/ers/config/testresource/{id}
<input type="radio"/> EndPoints Identity Group	Get version	GET	N/A	VersionInfo	https://10.1.100.2/ers/config/endpointgroup/versioninfo
	<input type="radio"/> Get by Id	GET	N/A	EndPointGroup	https://10.1.100.2/ers/config/endpointgroup/{id}

Downloads

Schema Files

User Guide

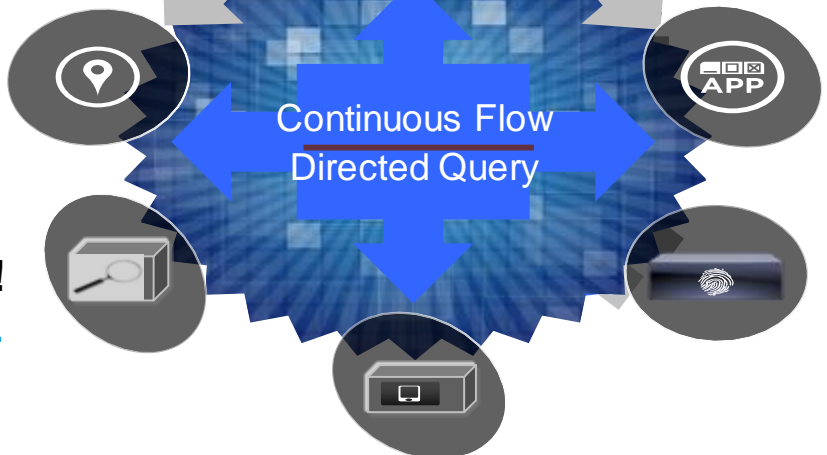
How pxGrid Works

Authorise → Publish → Discover → Subscribe → Query



ISE as pxGrid Controller

CISCO ISE



I have location!
I need app & identity...

I have application info!
I need location & device-type

I have sec events!
I need identity & device...

I have identity & device!
I need geo-location & MDM...

I have MDM info!
I need location...

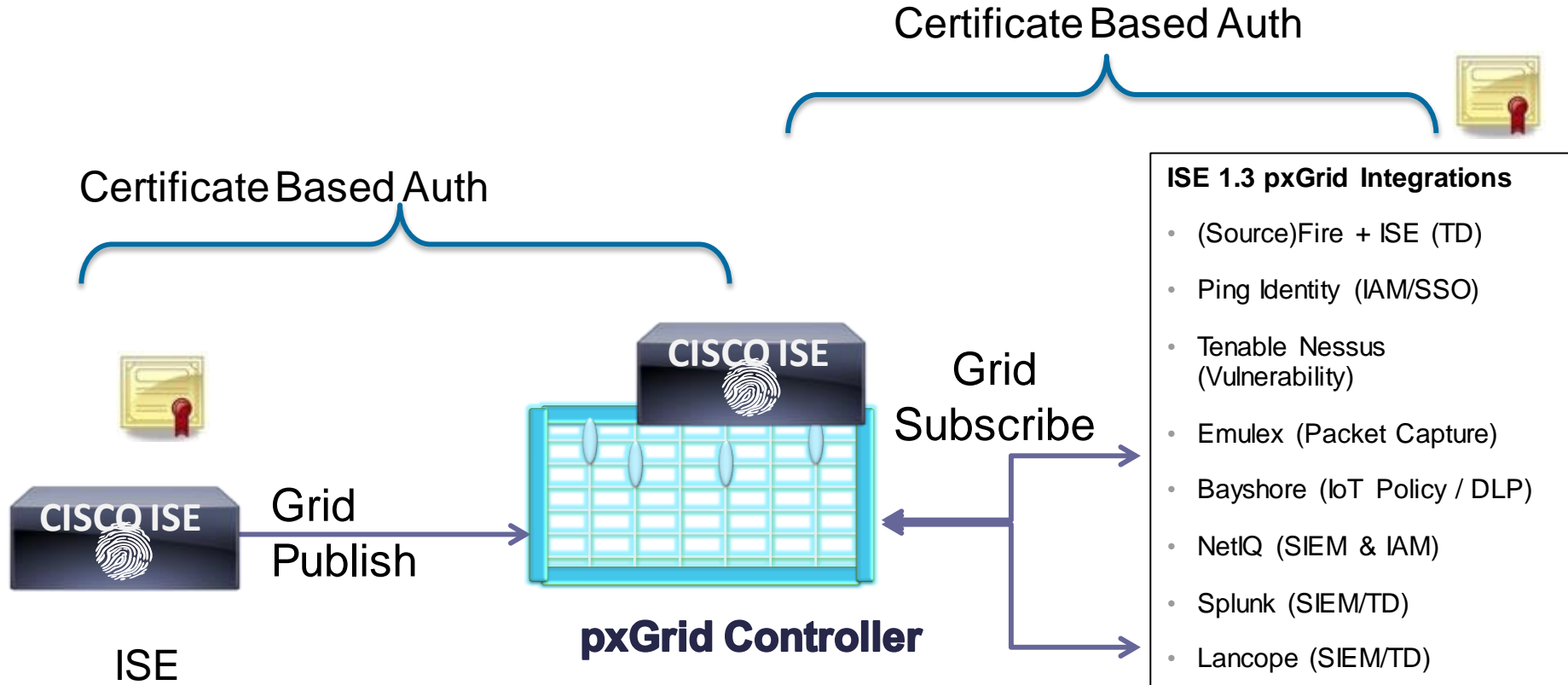
pxGrid

- 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

pxGrid Architecture



Agenda

- Introduction & Welcome
- Secure Access Architecture
- Gaining Visibility
- Authenticating and Authorising
- Visitation Rules
- Keeping the Network Clean
- Connecting not-so-Geeky Geeks
- Securing by Roles in the Network
- Sharing Context
- **Summary**





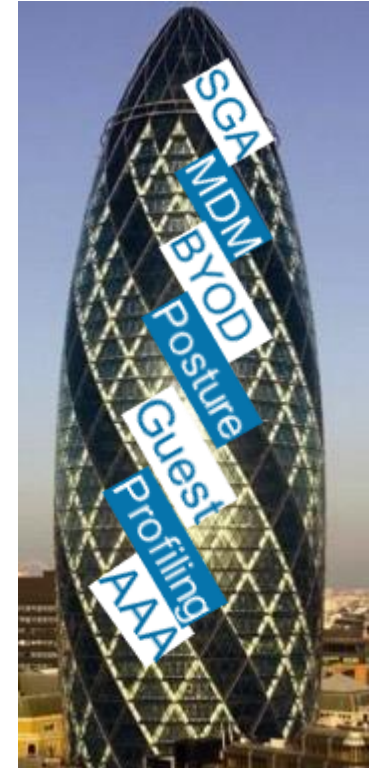
Summary

Building an Identity-Based Network Architecture

- Ad-Hoc Couplings Versus Systems Approach



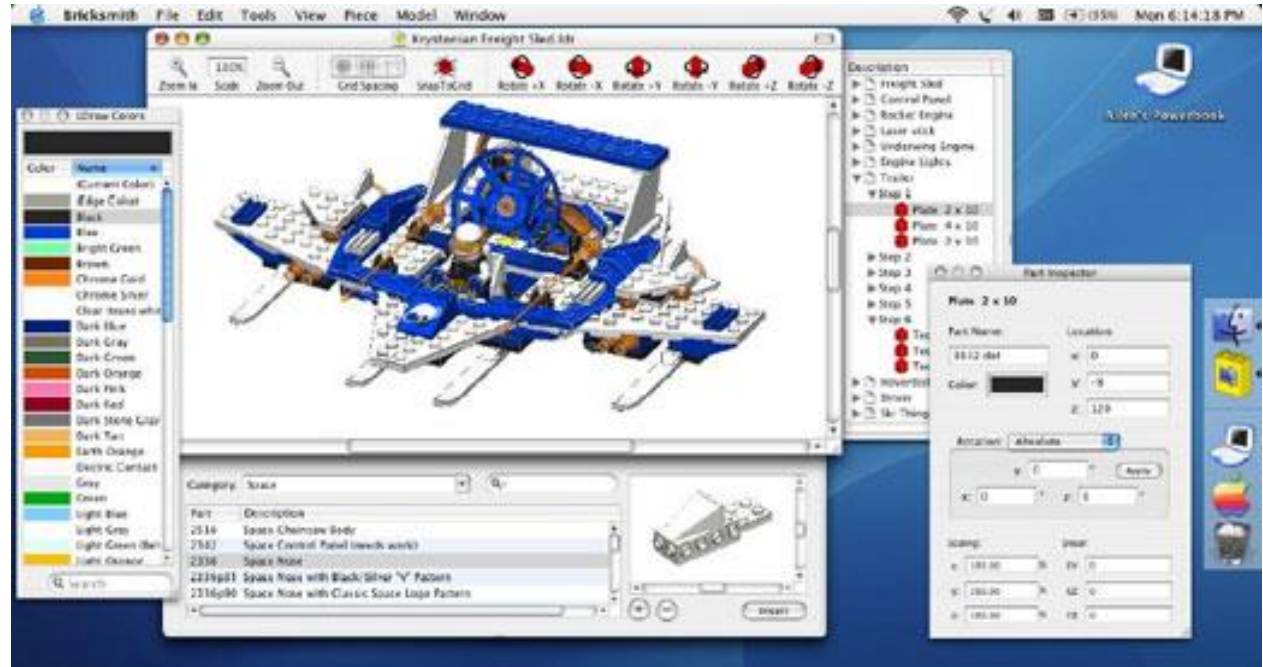
VS



Building an Identity-Based Network Architecture

- Architecture and Building Plan

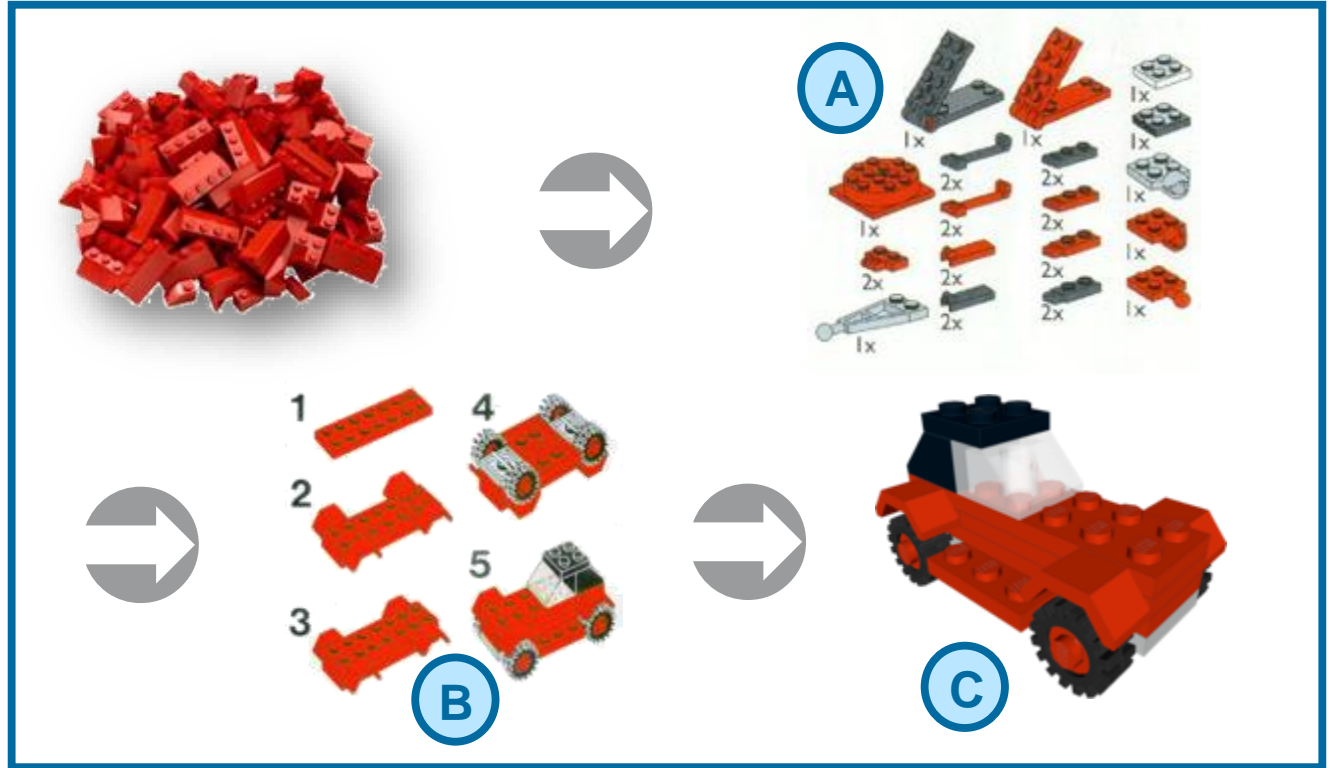
- Start with a High Level Design (HLD) of the big picture, current limitations and future requirements
- Test and tune with testing to develop the “Blueprint” or Low-Level Design (LLD) with detailed configurations and deployment steps.



Building an Identity-Based Network Architecture

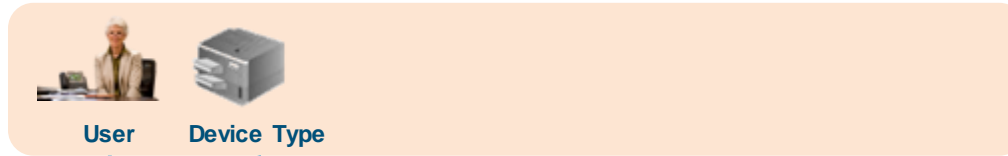
- Architecture and Building Plan

- (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.



Written to Realise Security Policy

Simple Version



Authorization Policy At A Glance
First Matched Rule Applies

Standard				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
✓ Enabled	Profiled Cisco IP Phones	Cisco-IP-Phone		Cisco_IP_Phones
✓ Enabled	Employee	Any	AD1:ExternalGroups EQUALS demo.local/Users/employees	PermitAccess
✓ Enabled	Guest	Guest		Guest
✓ Enabled	Default	Any		Web_Auth

Enforcement Policy

- Permissions = Authorisations
- Defines the access control policy and other attributes to be applied to the auth session.

Written to Realise Security Policy

Advanced Version



Authorization Policy At A Glance

First Matched Rule Applies

Standard

Status	Rule Name	Identity Groups	Other Conditions	Permissions
✓ Enabled	Profiled Cisco IP Phones	Cisco_IP_Phone		Cisco_IP_Phones
✓ Enabled	Game_Console	Game_Console-Registered		Game_Console
✓ Enabled	Domain_Computer	Any	demo.local:ExternalGroups EQUALS demo.local:Users/Domain Computers AND San_Jose MATCHES *(demo.local)\$	AD_Login
✓ Enabled	Employee-Wired	Any	Employee_Wired AND Posture_Compliant	Employee
✓ Enabled	Employee-Wireless	Workstation	Employee_Wireless AND Posture_Compliant MATCHES [0-5]	Employee_Wireless
✓ Enabled	Employee-iPAD	Apple-iPad	Employee_Wireless AND Posture_Compliant AND North_America	Employee_iPAD
✓ Enabled	Contractor-iPAD	Android OR Apple-iPad OR Apple-iphone OR Apple-iPod OR BlackBerry	Contractor_Wireless AND Posture_Compliant AND North_America	Contractor_iPAD
✓ Enabled	Guest-Wired	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wired AND Posture_Compliant	Guest
✓ Enabled	Guest-Wireless	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wireless AND Posture_Compliant	Guest_Wireless
⊘ Disabled	Default-Posture	Any		CWA_Posture_Remediation
✓ Enabled	Default	Any		Central_Web_Auth

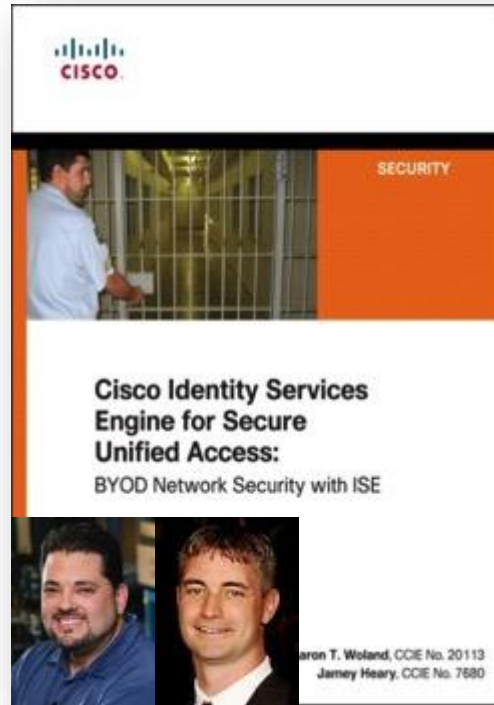
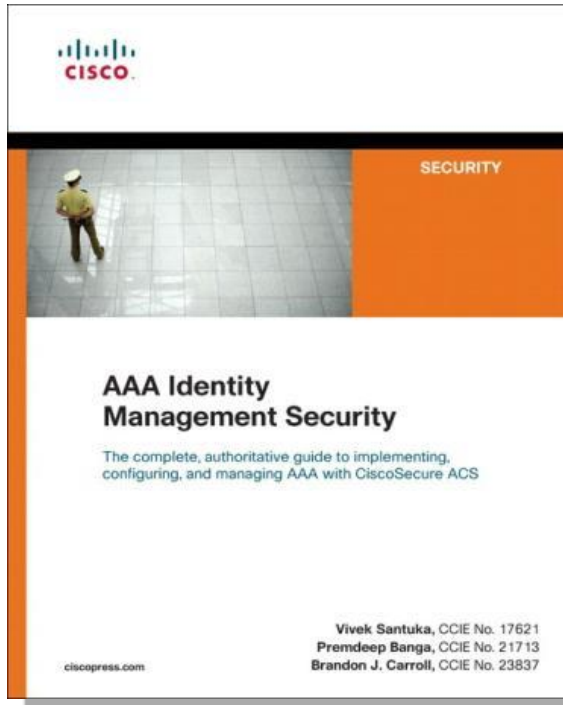
Legend: User, Device Type, Location, Posture, Time, Access Method, Custom

Call to Action

- Visit the World of Solutions for
 - Cisco Campus –
 - ISE 1.3 Guest and Enterprise Mobility Secure Access Meraki MDM
 - Cisco TrustSec
 - ISE 1.3 pxGrid with Technology Partners
 - Walk in Labs, Technical Solution Clinics
- Meet the Engineer
 - Gyorgy Acs, Craig Hys, Aaron Woland, Kevin Regan, Darrin Miller, ANY Cisco SE
- Lunch time Table Topics
- DevNet zone related labs and sessions
- Recommended Reading: for reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2015

Recommended Reading

- For reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2015



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, ISE : <https://www.youtube.com/user/CiscoISE>
- Fundamentals of TrustSec:
 - <http://www.youtube.com/ciscocin#p/c/0/MJJ93N-3lew>



Q & A

Cisco *live!*

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

CiscoLive!



Thank you.

Cisco *live!*



CISCO