Cisco TrustSec Solution & Identity Services Engine Overview

Kemal Akozer

Product Manager

Secure Access and Mobility Group

Cisco Systems

March, 2012

Agenda

- Today's Challenges with Secure and Controlled Network Access
- Benefits of TrustSec Solution with Identity Services Engine (ISE)
- Cisco ISE Features, Packaging, Licenses, Personnas and Ordering
- Cisco TrustSec Solution Components and Roadmap
- Cisco TrustSec Wireless Solution (BYOD)
- Cisco BYOD Solution: Building Blocks and Roadmap

Evolution of Network Access

Mobile Workers Personal Devices
Hotspot
VPN
VPN
Internet
VPN
Employee (Sales) Managed Desktop?
Printer (Payroll)
Security Systems
Employee (Finance) Managed Desktop?
Employee (Sales) Managed Desktop?
Branch Network
Campus Network
Printer (Sales)
Internal Resources
LWAPP
LWAPP
Guest
Guest
Wireless Employee
IP Camera
Game Console
Contractor
Wireless Employee

The New Borderless Network

Enabling a Borderless Experience

Securely | Reliably | Seamlessly

RIGHT USER

RIGHT PLACE

RIGHT DEVICE

RIGHT TIME

Device Diversity is Here to Stay

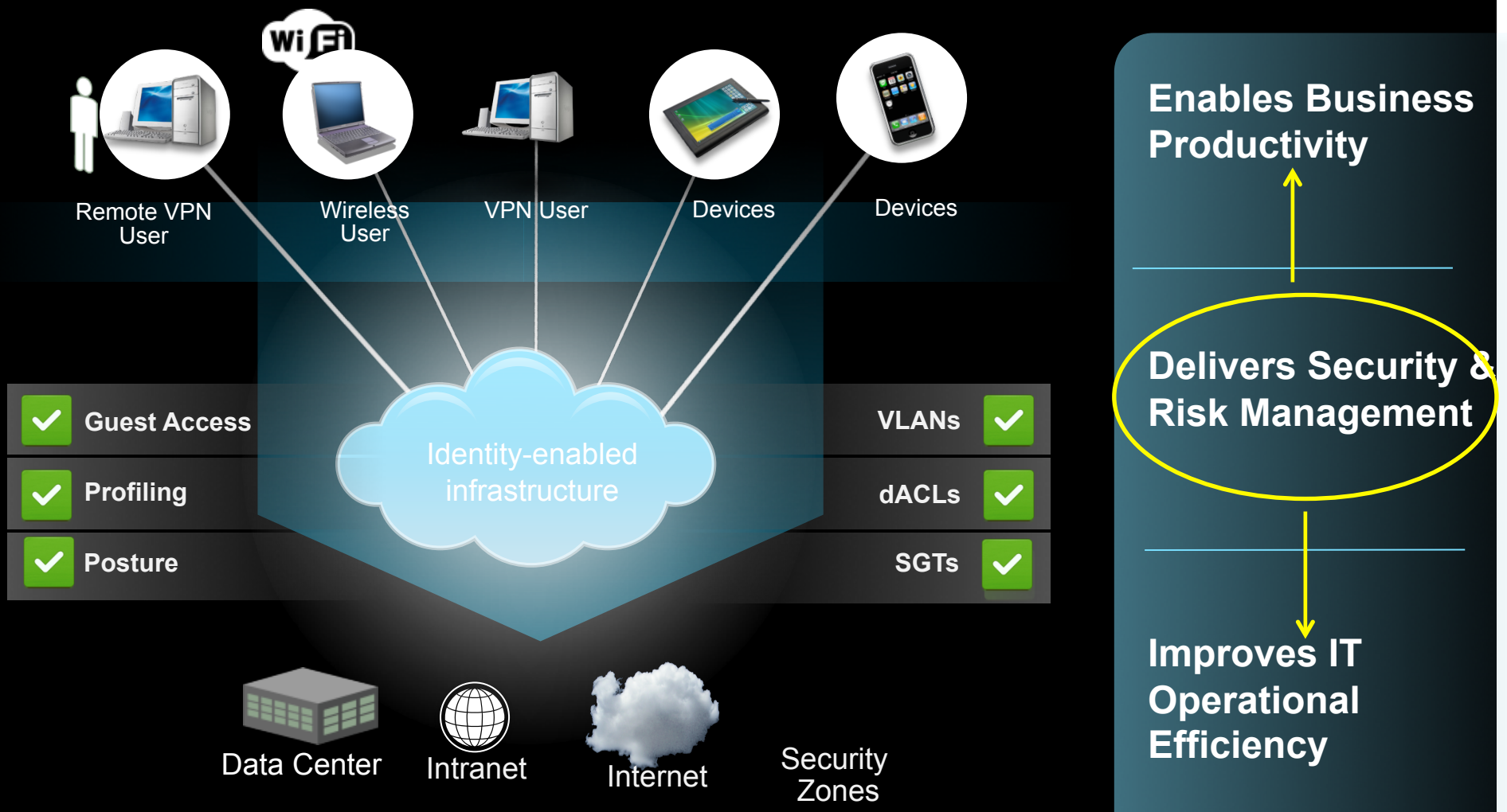
User Wants

- Consistent experience on multiple devices
- Seamless transitions between devices
- Separation of work and personal data
- Keep up with technology and social trends

IT Wants

- Proactive adoption of consumer/mobile devices
- Embrace BYOD without sacrificing security, management, business standards
- Lower organizational costs
- Improved agility

Introducing Cisco TrustSec



How Does ISE Address My Challenges?

Cisco ISE

I want to allow only authorized users access to my network	Authentication and Authorization
I want to allow guests into the network	Guest Lifecycle Management
I need to allow/deny iPad in my network (BYOD)	Profiling Services
I need to ensure my endpoints don't become a threat vector	Posture Services
I need a scalable way of authorizing users or devices in the network	Security Group Access Management
How can I set my firewall policies based on identity instead of IP addresses?	Identity-based Firewall*

Network Identity & Enforcement (TrustSec)

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

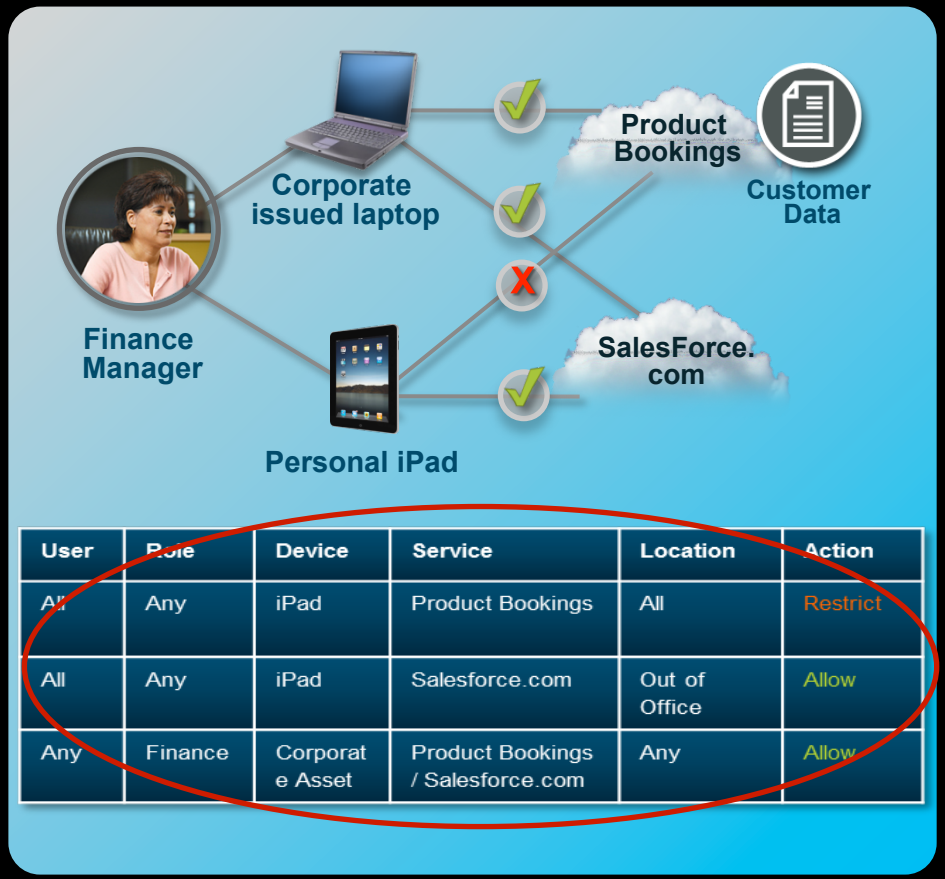
Industry's First One Box Solution!

Why Is the TrustSec Architecture Different from our Competitors

- ✓ Policy Management for wired, wireless and VPN users
- ✓ Integrated lifecycle services (posture, profiling, guest)
- ✓ Differentiated identity and authorization features
  - Monitor mode (no enforcement)
  - Flexible authentication via ID store sequences
  - Multiple authentication (Device and User)
- ✓ Flexible and scalable enforcement (authorization) options
- ✓ Layer-2 Encryption to protect communications and SGTs

Policy Based Access

Identity Services Engine Delivers “Business Policy”

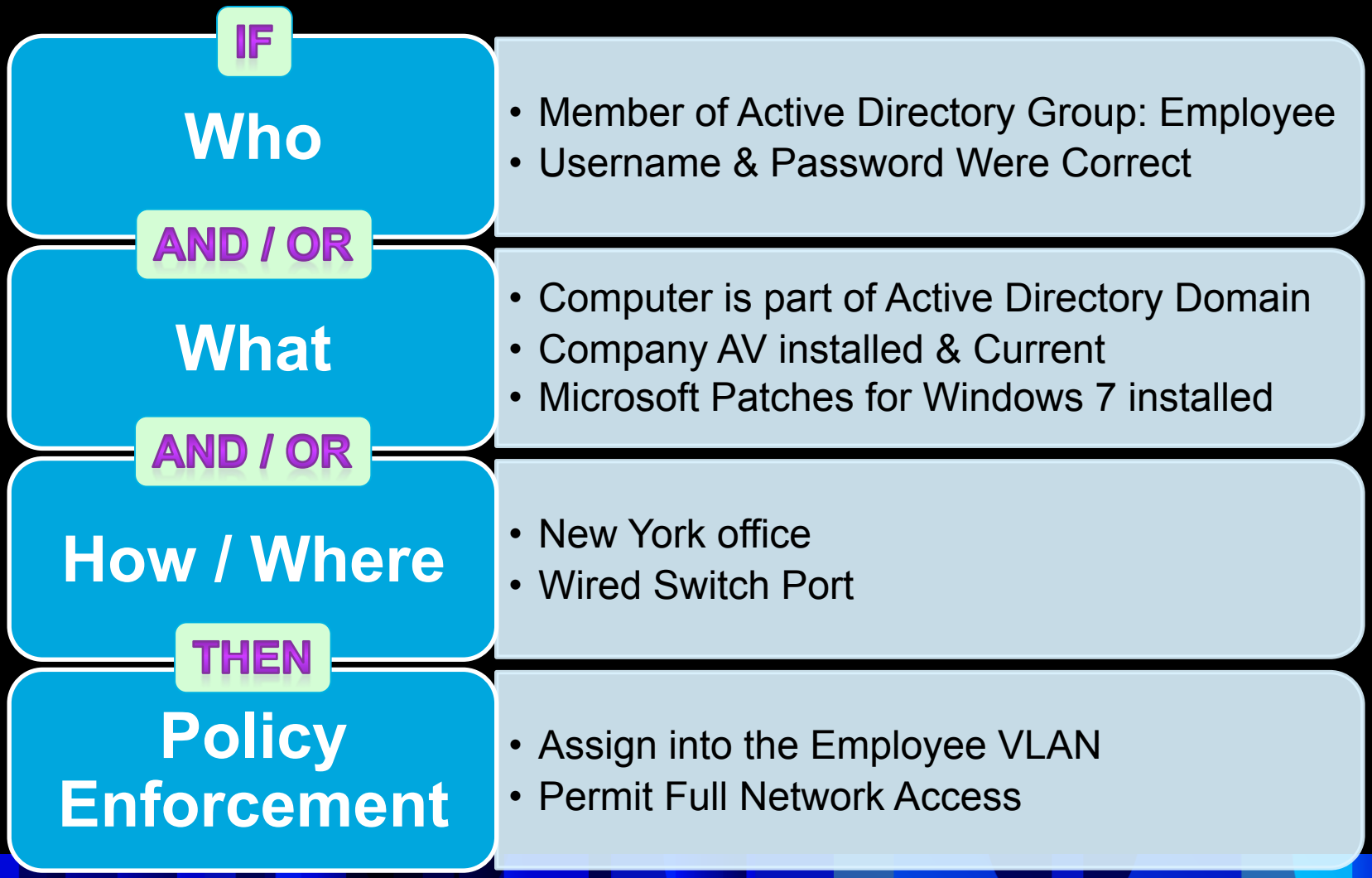


User	Role	Device	Service	Location	Action
All	Any	iPad	Product Bookings	All	Restrict
All	Any	iPad	Salesforce.com	Out of Office	Allow
Any	Finance	Corporate Asset	Product Bookings / Salesforce.com	Any	Allow

- Define network policy as an extension of business goals
- Policy extends to all access types (wired, wireless, VPN)
- Lifecycle Services Integration – guest, profiling, posture
- Optional encryption-based Policies for Security-conscious users

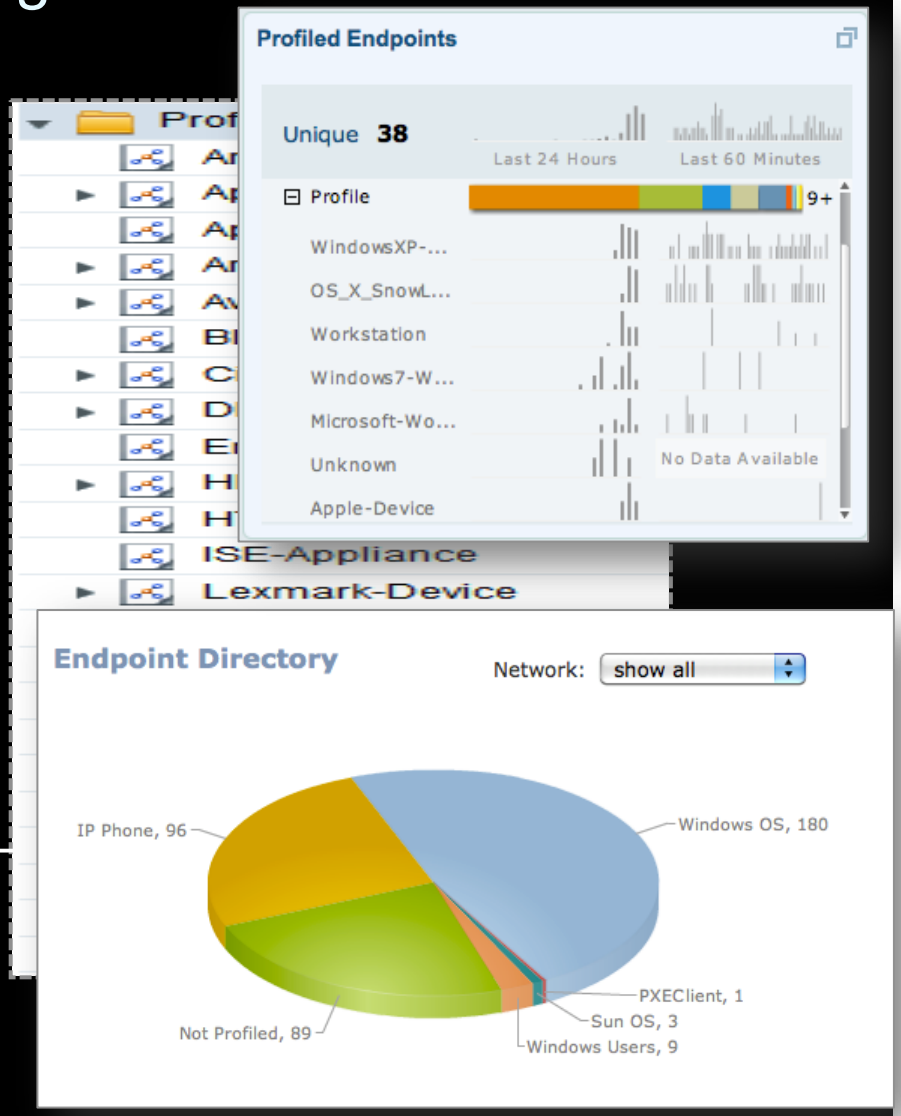
Why Cisco ISE?

Policy Example: Employee using Allowed System



Identity and Context-Awareness
ISE Profiling for Non-Authenticating Devices

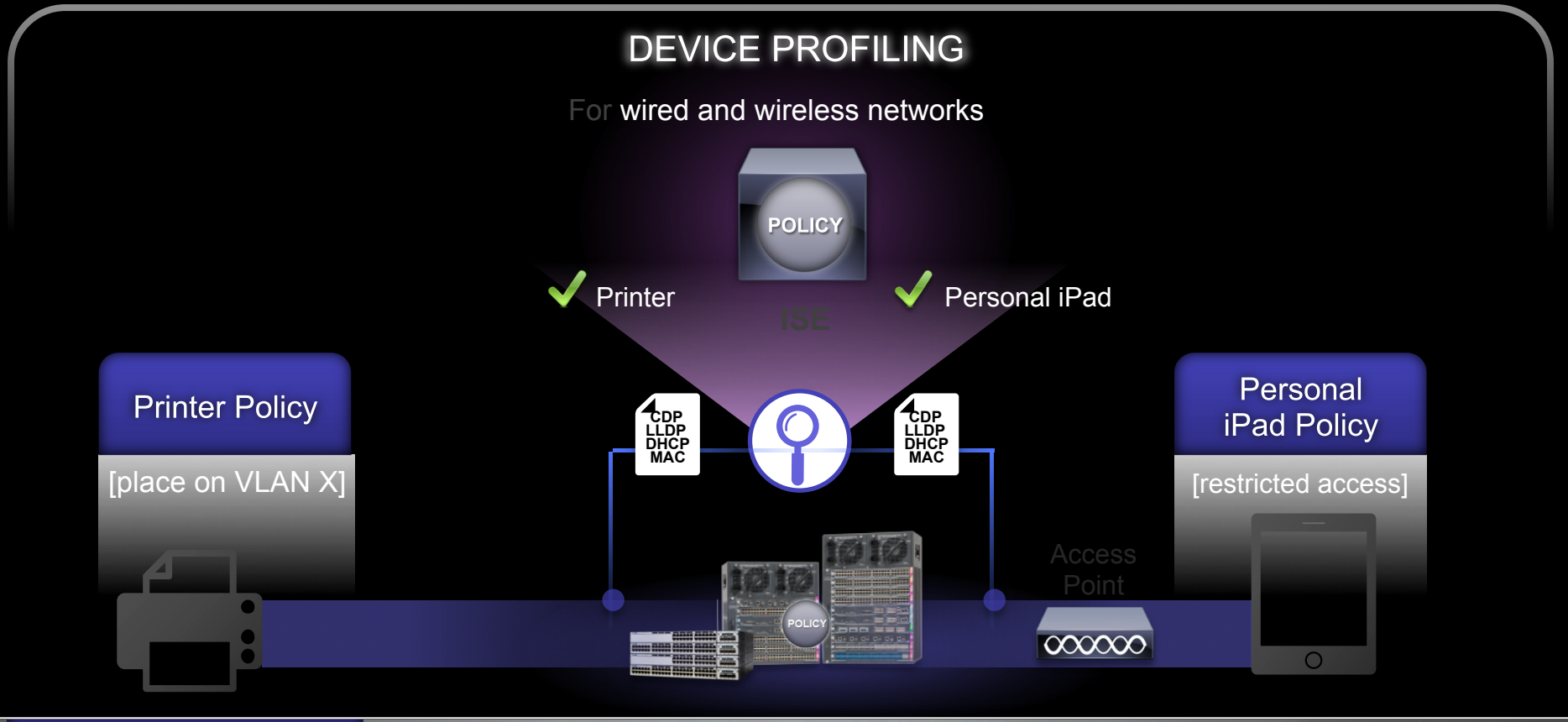
"What is on my Network"



- Reduces MAB effort **by identifying more than 90 device categories**
- **Create policy for users and endpoints –**
  - "Limited access by employee on IPAD"
- **Confidence-match based on multiple attributes**

Device Identification

Automated Device Classification Using Cisco Infrastructure



Benefits

Efficient Device Classification Leveraging Infrastructure

DEPLOYMENT SCENARIO WITH CISCO DEVICE SENSORS

COLLECTION
Switch Collects Device Related Data and Sends Report to ISE

CLASSIFICATION
ISE Classifies Device, Collects Flow Information and Provides Device Usage Report

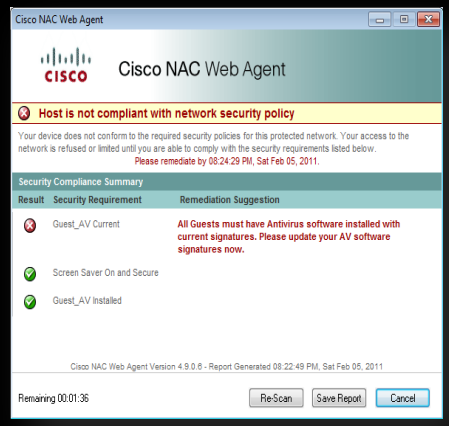
AUTHORIZATION
ISE Executes Policy Based on User and Device

ISE Lifecycle Services

ISE Posture Ensures Endpoint Health before Network Access

Wired, wireless, VPN user

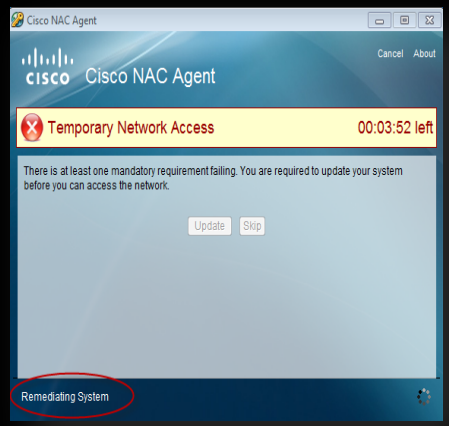
Non-Compliant



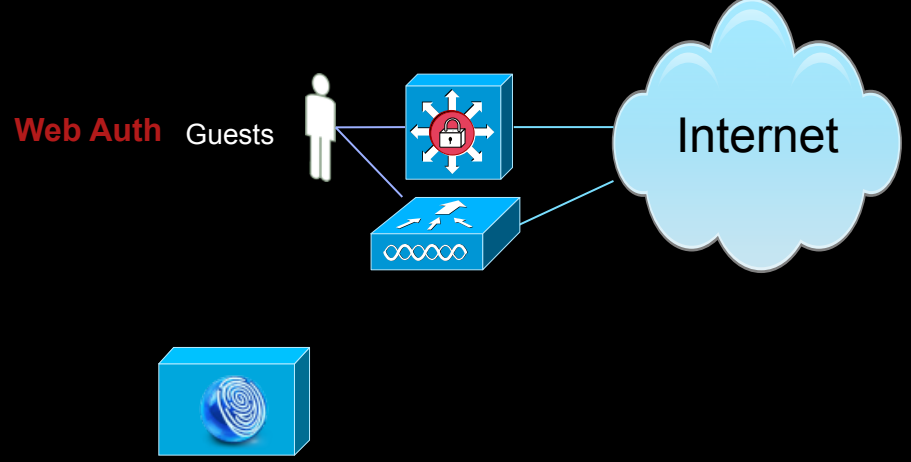
Employee Policy:

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

Temporary Limited Network Access until remediation is complete



ISE Lifecycle Services
ISE Guest Service for managing guests



Guest Policy:
- **Wireless or wired access**
- Internet-only access

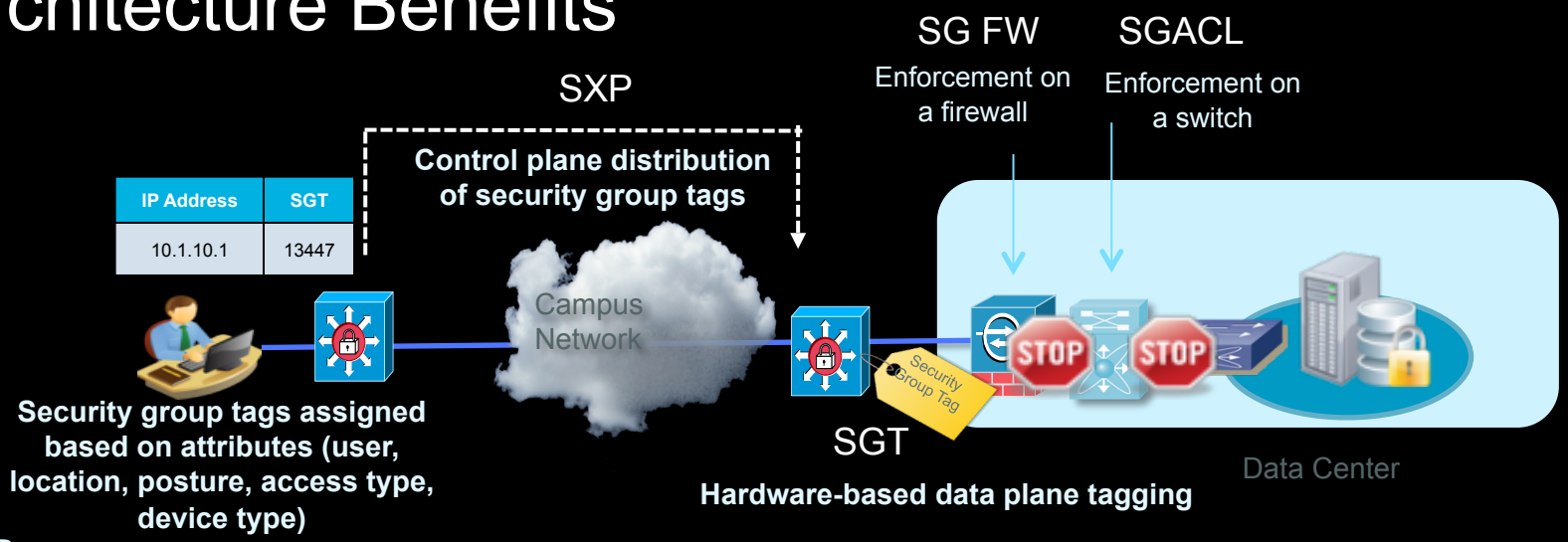
Provision: Guest accounts via sponsor portal

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

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

Report: On all aspects of guest accounts

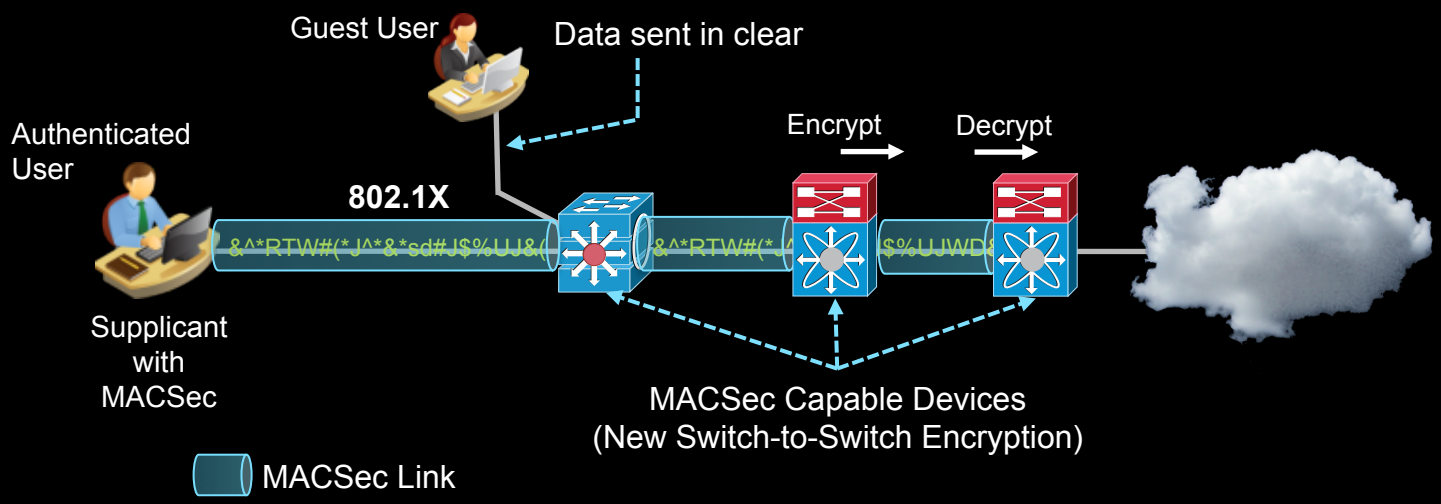
Security Group Access
Architecture Benefits



- **Pros:**
  - Security Group Access makes 802.1X authorization/enforcement more scalable than VLAN or DACL.
  - SGT assigned based on “context”, i.e. a user is assigned into specific organization roles based on location, posture, access type, device type
  - Single-sign on (i.e. tag assigned at first network egress point) and flexible enforcement
  - Provides value for the network infrastructure
- **Cons:**
  - Limited Platform support now, but new platforms being added at each release
  - **Campus:** Cat 3K/4K/6K SXP **Branch:** ISR SXP, ASR 1K SGT
  - **Enforcement:** Cat 6K (Campus aggregation) or N7K SGT/SGACL (Data Center)

TrustSec Encryption

Encryption for policy-based encrypted access and SGT integrity



Downlink Encryption

- Anyconnect 3.0 (software or hardware)
- MACSec-ready hardware:
  - Intel 82576, Intel 82599, Intel ICH10 on Dell, Lenova, Fujitsu, HP desktops
- Terminating on Cat 3K (available now)
- Terminating on Cat 4K (Mar/Apr)

Uplink Encryption (Sw to Sw)

- Switch-to-Switch Encryption
- Cat 3K – 1G use existing ports or new service module for 10G
- Cat 6K SUP 2T Module
- Nexus 7K
- Cat4K – SUp7E uplinks and 47xx series line cards – March/April

Uplink Encryption (DC to DC)

- Nexus 7K DC to DC encryption

ISE Monitoring Authentications

"Live" Authentication log displays all auth events in a single table

Manual/Auto refresh for last X records in last # hours

"Live" Authentications!

Filter by full/partial input

Passed / Failed row colors

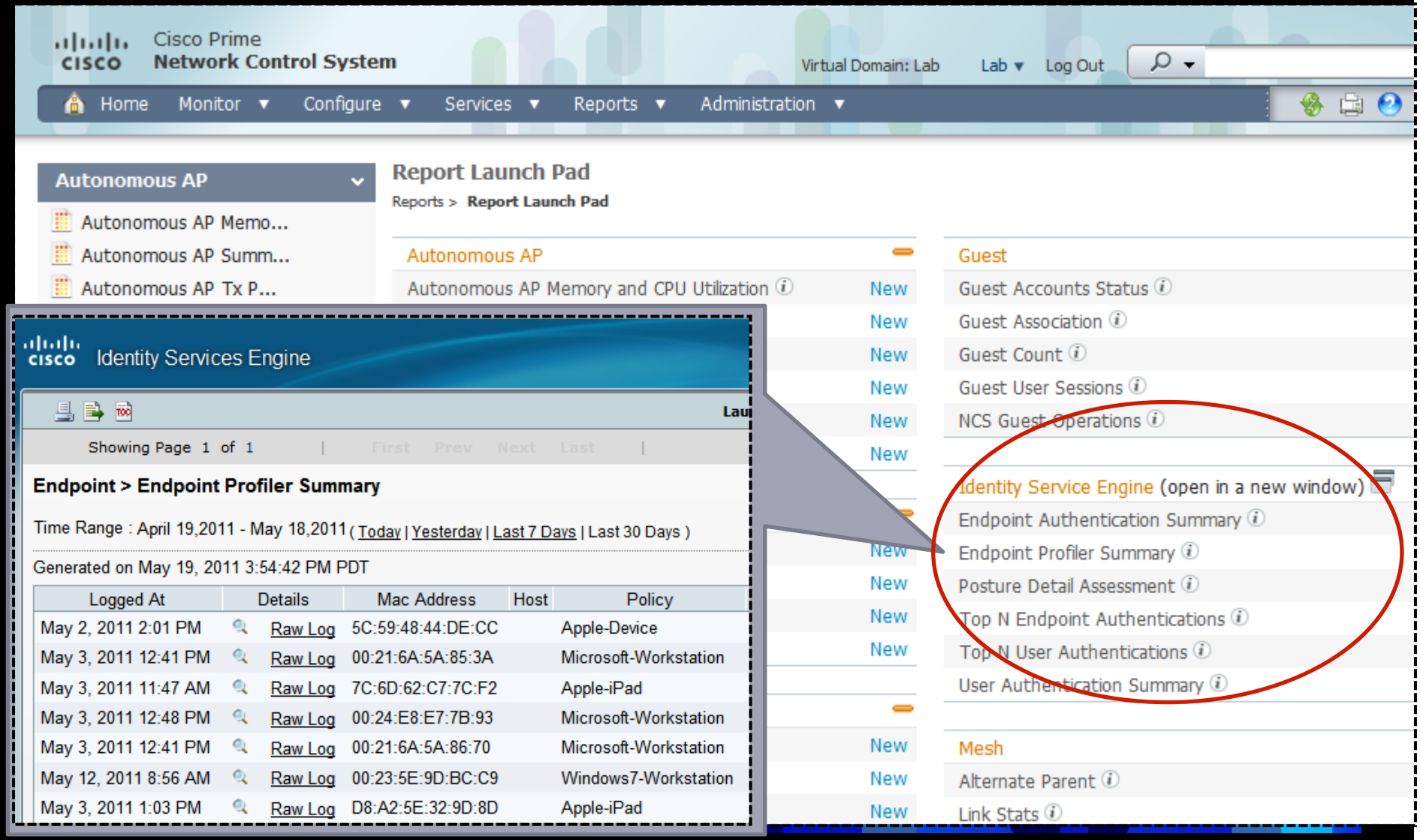
Drill-down

Refresh Every 30 seconds | Show Latest 100 records

Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure
Jan 25,12 04:07:38.628 PM	✗		tiryan	D8:B3:77:53:E4:5C		wlc2106					EAP session ti...	5411
Jan 25,12 04:06:02.249 PM	✓		tiryan	D8:B3:77:53:E4:5C		wlc2106		Internet_Only	Internal_group,Profil..	NotApplicable	Authentication ...	
	✓		tiryan	88:9F:FA:6E:19:CB		wlc2106		Internet_Only	Internal_group,Profil..	NotApplicable	Authentication ...	
	✓		tiryan	88:9F:FA:6E:19:CB		wlc2106		Internet_Only	Internal_group,Profil..	NotApplicable	Authentication ...	
	✓		tiryan	88:9F:FA:6E:19:CB		wlc2106		Internet_Only	Internal_group,Profil..	NotApplicable	Authentication ...	
Jan 25,12 02:31:21.620 PM	✗		tiryan	CC:08:E0:0E:B3:32		wlc2106					EAP session ti...	5411
Jan 25,12 02:31:15.581 PM	✗		tiryan	CC:08:E0:0E:B3:32		wlc2106					EAP session ti...	5411
Jan 25,12 02:31:07.575 PM	✗		tiryan	CC:08:E0:0E:B3:32		wlc2106					EAP session ti...	5411
Jan 25,12 02:27:21.784 PM	✗		tiryan			wlc2106					EAP session ti...	5411
Jan 25,12 02:26:32.382 PM	✓		tiryan	38:E7:D8:F2:C8:C9		wlc2106		Internet_Only	Internal_group,Profil..	NotApplicable	Authentication ...	
Jan 25,12 02:25:55.293 PM	✓		tiryan	D8:B3:77:53:E4:5C		wlc2106		Internet_Only	Internal_group,Profil..	NotApplicable	Authentication ...	
Jan 25,12 02:11:13.617 PM	✓		tiryan	D8:B3:77:53:E4:5C		wlc2106		Internet_Only	Internal_group,Profil..	NotApplicable	Authentication ...	
Jan 25,12 02:10:47.292 PM	✗		tiryan	D8:B3:77:53:E4:5C		wlc2106					EAP session ti...	5411
Jan 25,12 02:09:57.439 PM	✗		tiryan	D8:B3:77:53:E4:5C		wlc2106					EAP session ti...	5411

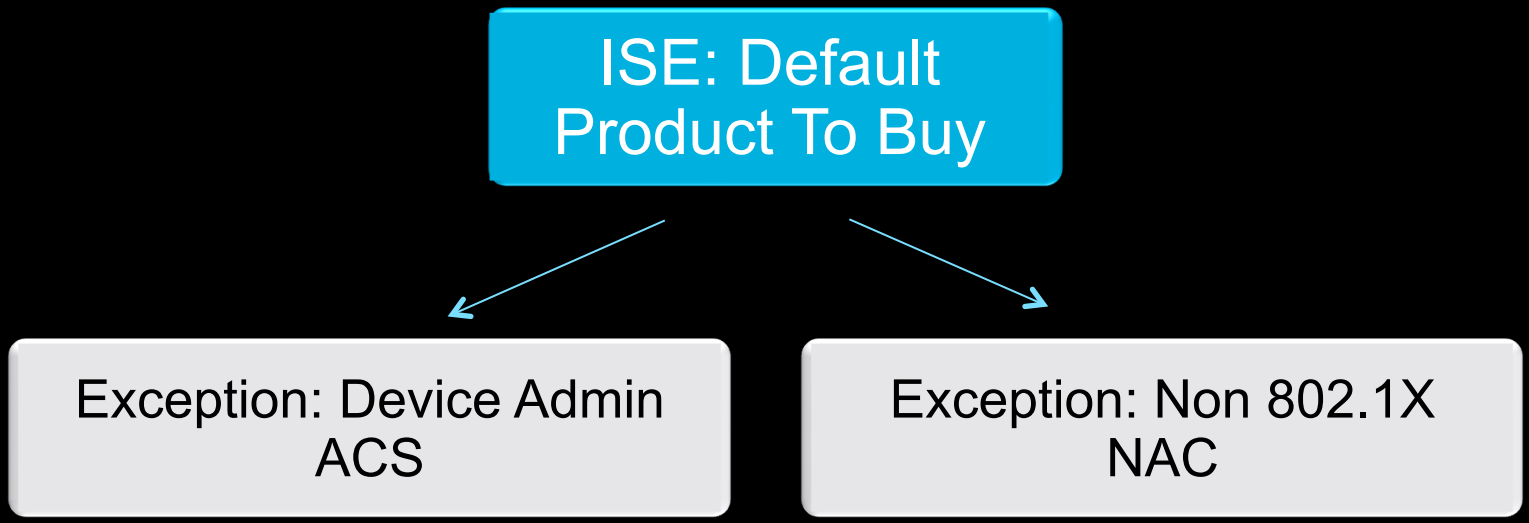
Last update: Jan 25, 12 04:13:32.190 PM EST

NCS Provides Cross-Linking to ISE
Reports on Profiling



Do I need ISE vs. ACS or NAC?

ISE is the default choice unless it cannot meet your needs



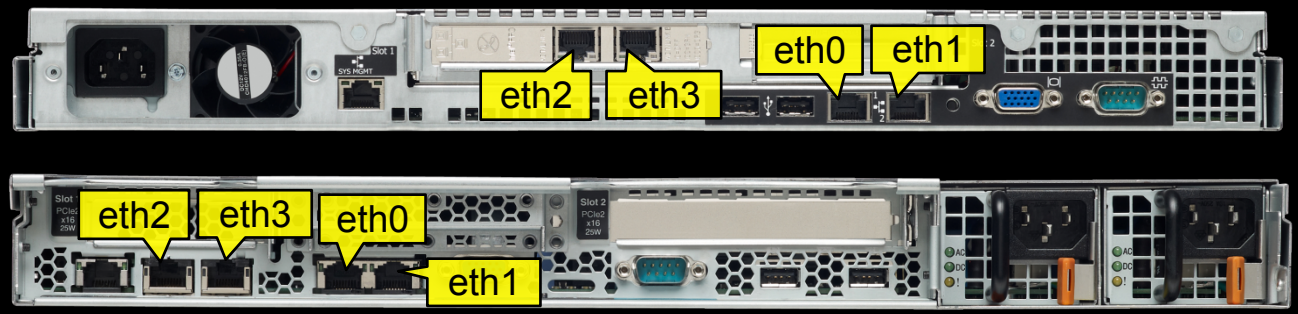
ISE Version	ISE 1.x	ISE 2.0
Device Admin	Buy ACS	Buy ISE
non-802.1x	Buy NAC	Buy ISE

- **ISE SW id Upgradable from Cisco ACS and NAC**

ISE Platforms

Hardware	Small	Medium	Large	VM
Model	**1121/3315** Based on the IBM System x3250 M2	**3355** Based on the IBM System x3550 M2	**3395** Based on the IBM System x3550 M2	VMware Server v2.0 (Demos) VMware ESX v4.0 / v4.1 VMware ESXi v4.0 / v4.1
CPU	1x Quad-core Xeon 2.66GHz	1x Quad-core Nehalem 2GHz	2x Quad-core Nehalem 2GHz	>= 1 processor
RAM	4GB	4GB	4GB	4GB (max)
Disk	2 x 250-GB SATA (500GB available)	2 x 300-GB 2.5" SATA (600GB available)	4 x 300-GB 2.5" SAS I (600GB available)	Admin: >= 60GB Policy Service: >= 60GB Monitoring: >= 200GB
RAID	No	Yes: RAID 0	Yes: RAID 1	-
Network	4 x Gigabit Ethernet	4 x Gigabit Ethernet	4 x Gigabit Ethernet	4 x Gigabit Ethernet
Power	Single 650W	650W Redundant	650W Redundant	-
Node Roles	All Roles	All Roles	All Roles	No Inline Posture Node

No additional NICs supported



ISE Packaging and Licensing

Identity Services Engine

Wireless Upgrade License (ATP)
Extend Policy for Wired and VPN Endpoints

Wireless License
Policy for Wireless Endpoints
5 Yr Term Licensing

Base License (ATP)
Policy for Wired, Wireless and VPN Endpoints
Perpetual Licensing

- Authentication / Authorization
- Guest Provisioning
- Link Encryption Policies

Advanced License (ATP)
Policy for Wired, Wireless and VPN Endpoints
3/5 Yr Term Licensing

- Device Profiling
- Host Posture
- Security Group Access

Platforms
Small 3315/1121 | Medium 3355 | Large 3395 | Virtual Appliance

Place New Features in Existing Switch Packaging:

Campus (Cat 3K/4K):
- LAN Base – 802.1X, SXP, IOS sensor, MACSec
- IP Base – SGT, SGACL

Aggregation (Cat 6K):
- IP Base – 802.1X, SXP, SGT, SGACL

Router (ASR 1K/ISR):
- Base packaging –SXP
- Advanced/Security – SG FW

Data Center (Nexus):
- Advanced LAN License → Base Package

Built into Headend

Anyconnect

Optional client

ISE Personas

Policy Administration Node

Interface to configure policies

Monitoring & Troubleshooting Node

Interface for logging and report data

Policy Service Node (formerly Policy Decision Point)

Engine that makes policy decisions

ISE Nodes and Personas

Single ISE Node (appliance or VM)

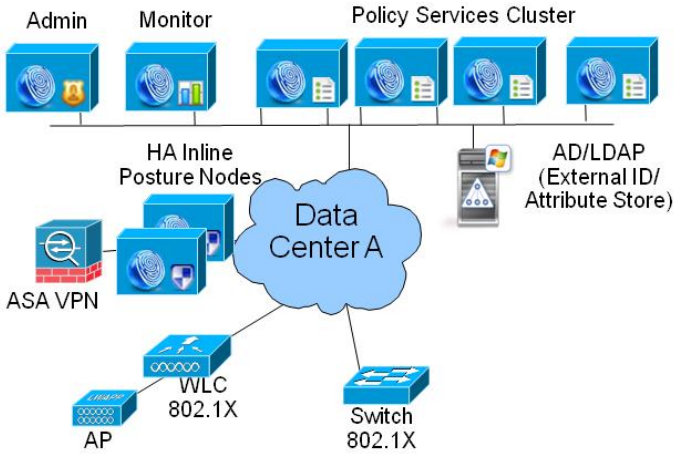
Persona – One or more of the following:
- **Administration**
- **Monitoring**
- **Policy Service**

OR

Single Inline Posture Node (appliance only)

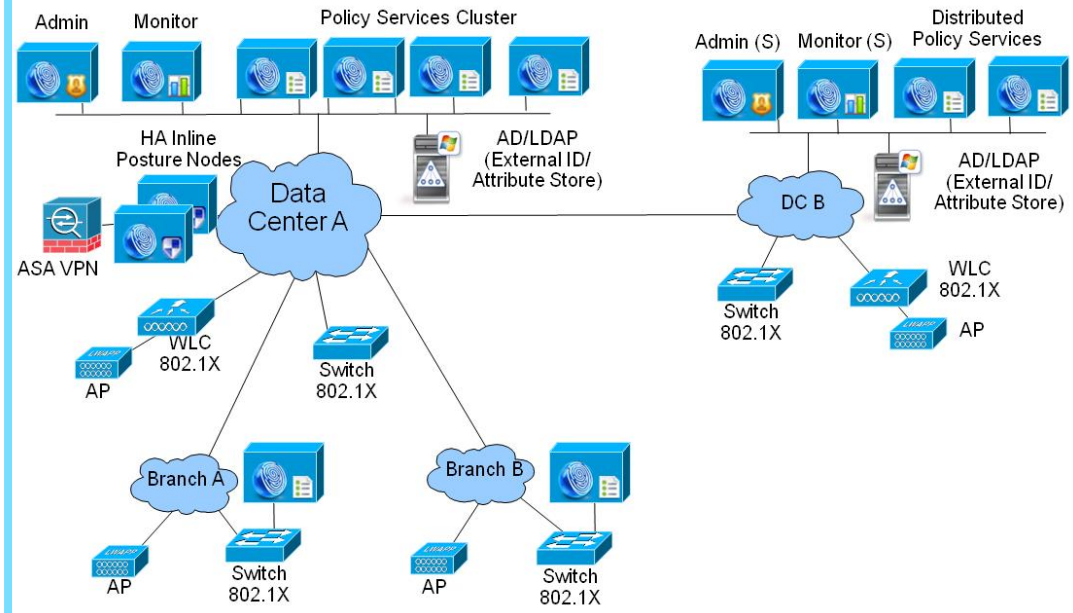
Deployment Types

Centralized Deployment



✓ All ISE Persona's deployed in a single site

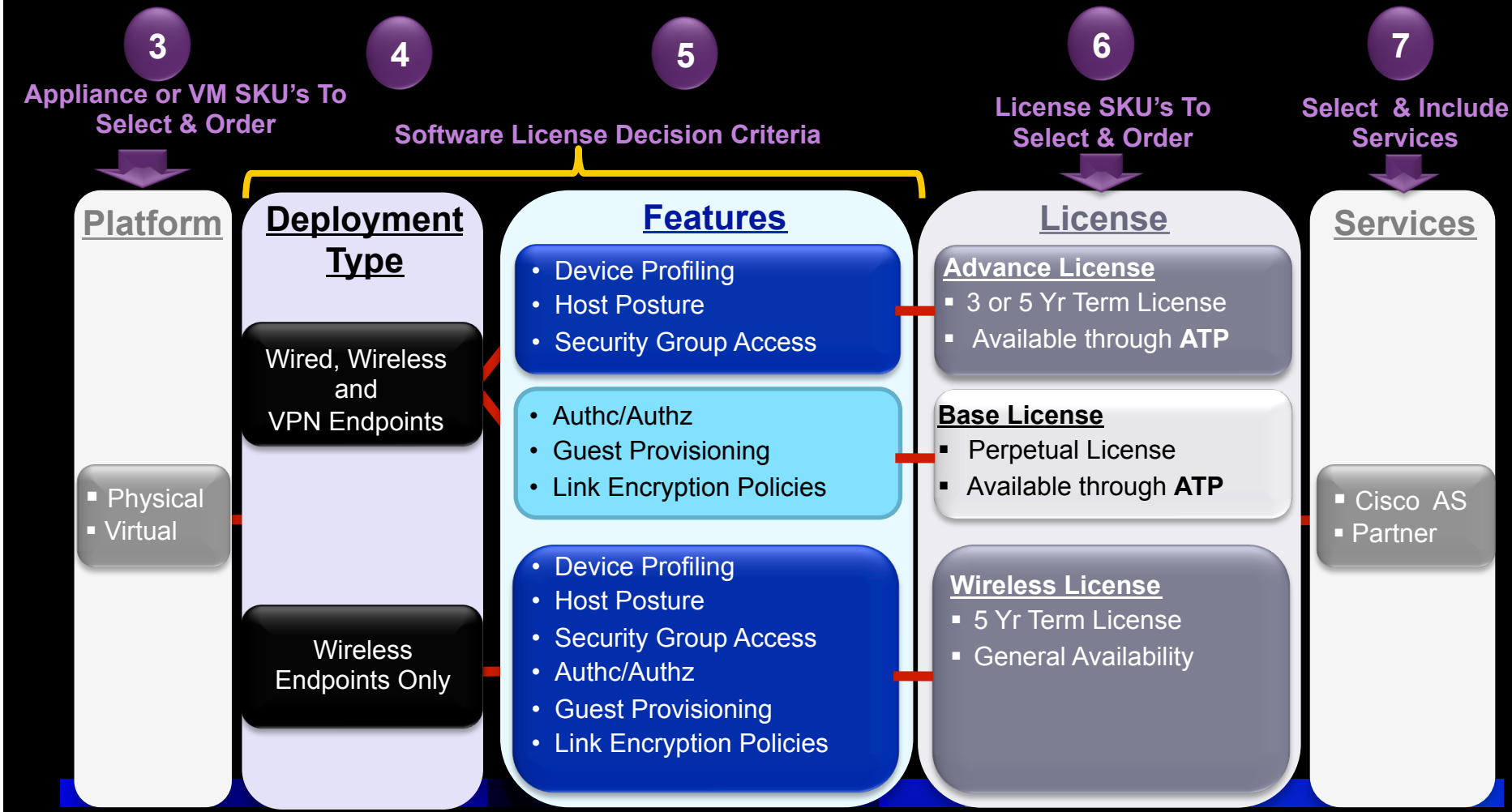
Distributed Deployment



✓ ISE Persona's deployed across multiple sites

ISE Ordering Steps

1. Determine max number of endpoints concurrently on the network
2. Determine number of ISE instances needed for the design



TrustSec 2.0 (Already Released)
Components, Hardware and Releases

Component	Hardware	Features	Release
ISE	Any: 1121/3315 3355/3395 VMWare	Integrated AAA, policy server, and services (guest profiler, posture)	ISE 1.0
Catalyst 2K/3K	2960, 2960S, 3560, 3560E, 3560X 3750, 3750E, 3750X	Baseline Identity features, dot1X authentication, CoA, SXP	12.2(55)SE3
	3560X, 3750X	MACsec SW2SW, SXP	15.0(1)SE1
Catalyst 4K	Sup6E	Baseline Identity features, dot1X authentication, CoA, SXP	* Not tested
Catalyst 6K	Sup32 / Sup720	Baseline Identity features, dot1X authentication, CoA, SXP	12.2(33)SXI7
		SXP IPv6, VRF Aware TrustSec	12.2(33)SXJ1
	Sup2T	• Baseline Identity features, dot1X authentication, SXP • MACsec switch-to-switch encryption • SGT and SGACL enforcement with Cat 6K Sup 2T	12.2(50)SY
NX7K		• MACsec switch-to-switch encryption • SGT and SGACL enforcement	5.2.1 (Delhi)
AnyConnect		Integration of 802.1X supplicant (no MACsec)	* Anyconnect 3.0
Wireless LAN Controller		Profiling and CoA	Unified Wireless 7.0.116
ASR1K	RP1/RP2 ASR1001	SGA integration - SXP/SGT for tagging at WAN aggregation layer or extranet	3.4

, AnyConnect 3.0 with MACsec w/ISE validation is part of TrustSec 2.1

TrustSec Roadmap

EC | CC | PLAN

Q2 CY 2012

TrustSec 2.1

Infrastructure:
Identity enhancements
- *Critical voice VLAN*
- Identity on ISR G2 native ports
- IOS Sensor (device profiler)

MACsec – Cat 4K uplink/downlink

Management/Policy
ISE 1.1
NCS 1.0
LMS 4.2

Security Group Access
Wireless SXP
Nexus 5K/2K - SXP, SGT, SGACL
ISR – SXP, SGT
ASR1K – SXP/SGT
VDI and Anyconnect + RDP

Firewall Enforcement:
SGFW: ISR, ASR1K Firewall

Q4 CY 2012

TrustSec 2.2

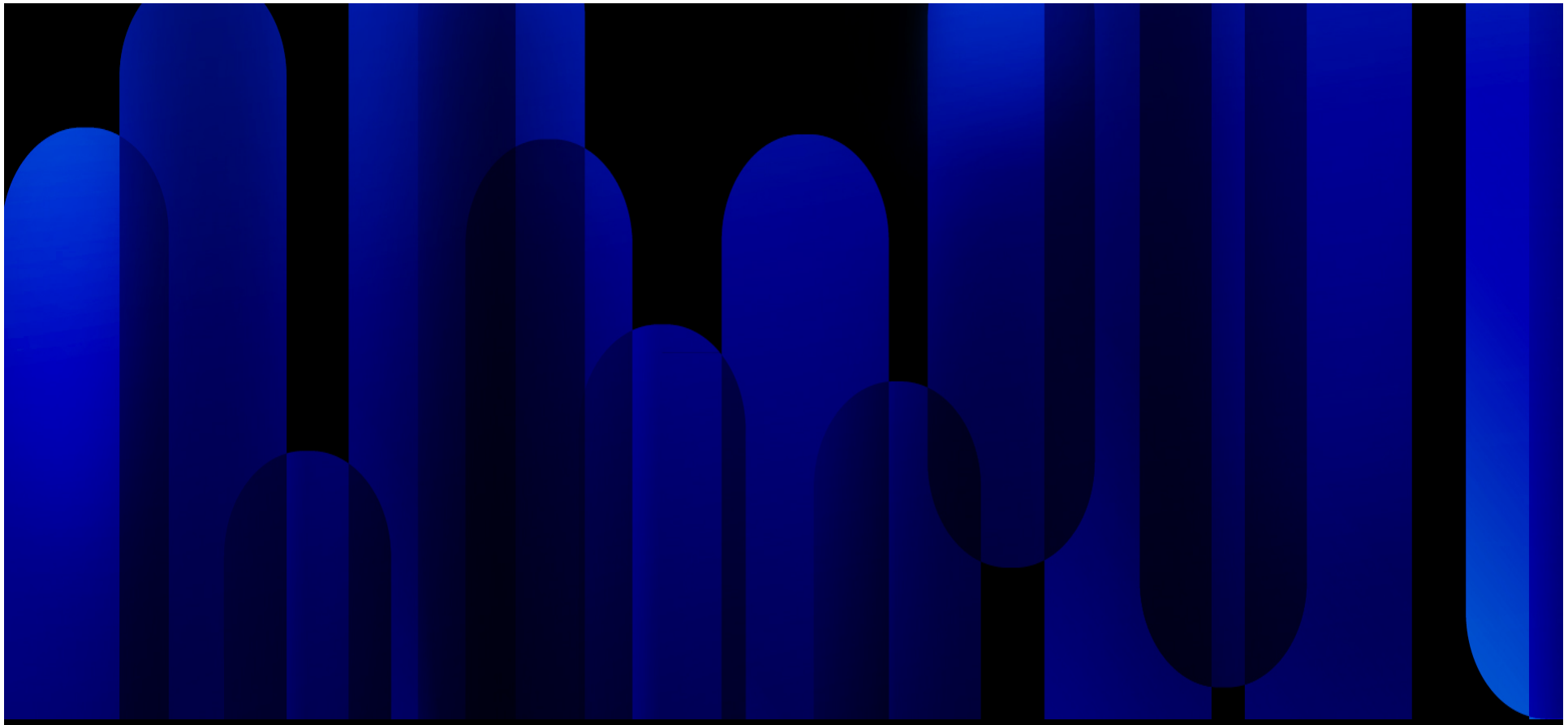
Infrastructure:
Expanded platforms:
- Cat 4K Predator Platform– 4540X & 4524X (40 port and 24 port)
- Sup 7E-L w/ YAP SW
- WLC enhancements – IOS sensor, device profiling with locally switched Flexconnect

Management/Policy
ISE 1.2
Lumos Zone-based FW support in NCS WAN 1.1
Lumos/NCS – M&T in NCS 1.2

Security Group Access
- Cat3K- SGT, SGACL
- Cat 2K - SXP
- ISR/ASR1K – SGT over IPSec VPN links
- N7K VLAN to SGT mapping
- SGA Proxy Feature

Firewall Enforcement
SGFW: ASA Firewall

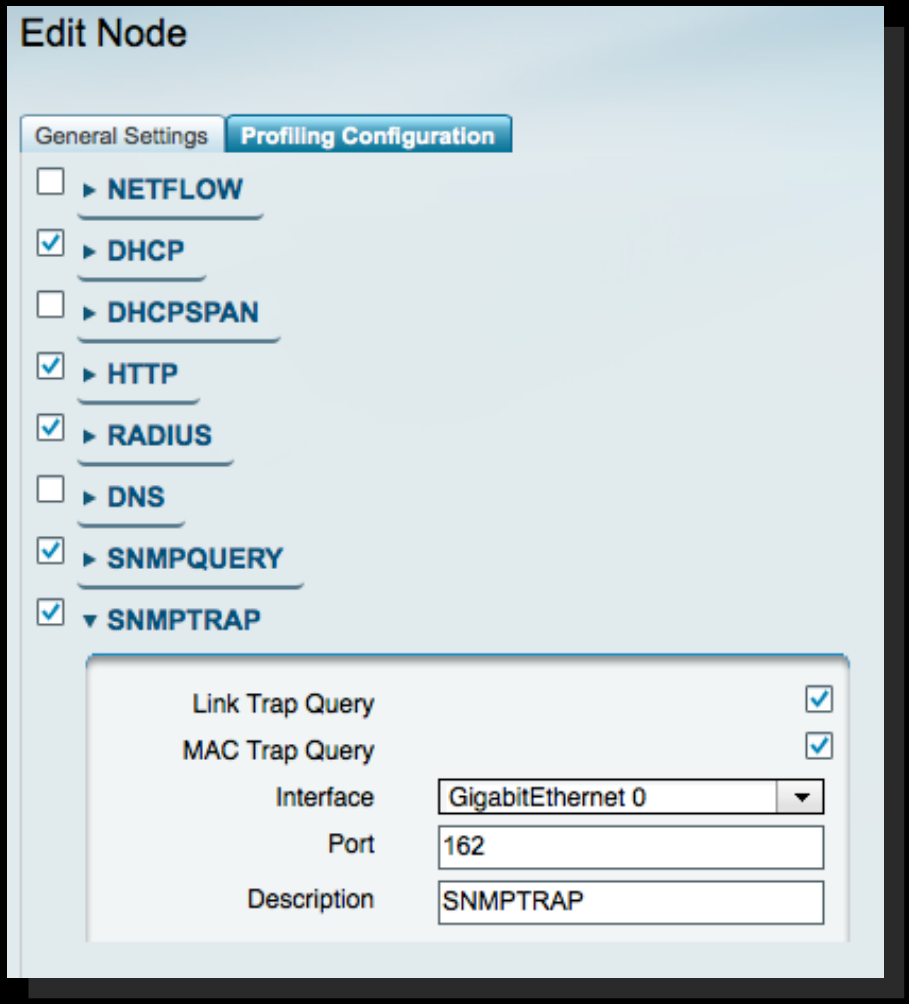
Client
- Anyconnect - EAP Chaining



TrustSec Wireless Deployments (BYOD)

ISE Profiler Configuration is now VERY EASY

1) Enable probe types to use
2) Use predefined profiler rule sets or built your own
3) Enable Profile as an Identity Group, and use it in authentication / authorization



http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

ISE Device Profiling Example - iPad

Is the MAC Address from Apple?

Does the Hostname Contain “iPad”?

Is the Web Browser Safari on an iPad?

Once the device is profiled, it is stored within the ISE for future associations:

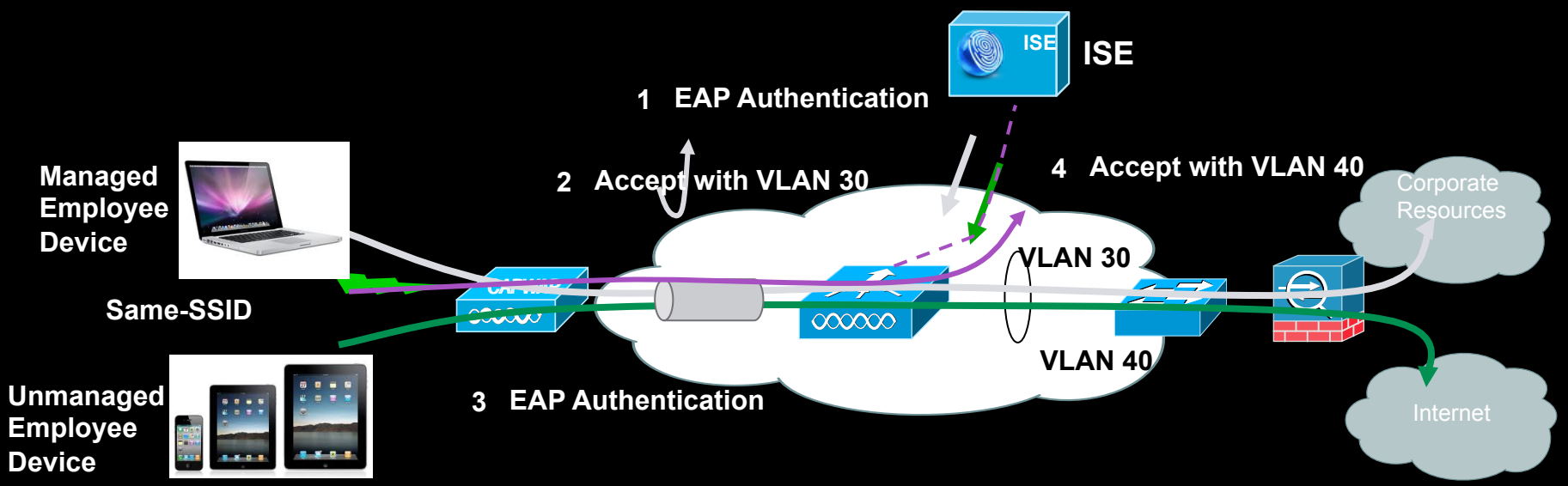
Endpoints

Edit | Create | Delete | Import | Export

Endpoint Profile	MAC Address
Apple-iPad	D8:A2:5E:32:9D:8D
Microsoft-Workstation	00:21:6A:5A:85:3A
Microsoft-Workstation	00:24:E8:E7:7B:93
Microsoft-Workstation	00:21:6A:5A:86:70
Windows7-Workstation	00:23:5E:9D:BC:C9

Apple iPad

Use Case:
Managed vs. Unmanaged Employee Device



- Users, using the same SSID & same User/PW, can be associated to different VLAN interfaces after EAP authentication
- Employee using managed device with their AD user id can be assigned to VLAN 30 to have full access to the network - Certificate or Registered MAC address
- Employee using unmanaged or personal iPad/iPhone with their AD user id can be assigned to VLAN 40 to have internet access only

ISE Access Policy Based on Device Type

What?

Who=Employee

Authorization Policy At A Glance

First Matched Rule Applies

Standard

Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Employee-PC	Workstation	demo.local:ExternalGroups EQUALS demo.local/Users /employees	Employee_PC
Enabled	Employee-iPAD	Apple-iPad	demo.local:ExternalGroups EQUALS demo.local/Users /employees	Employee_iPAD

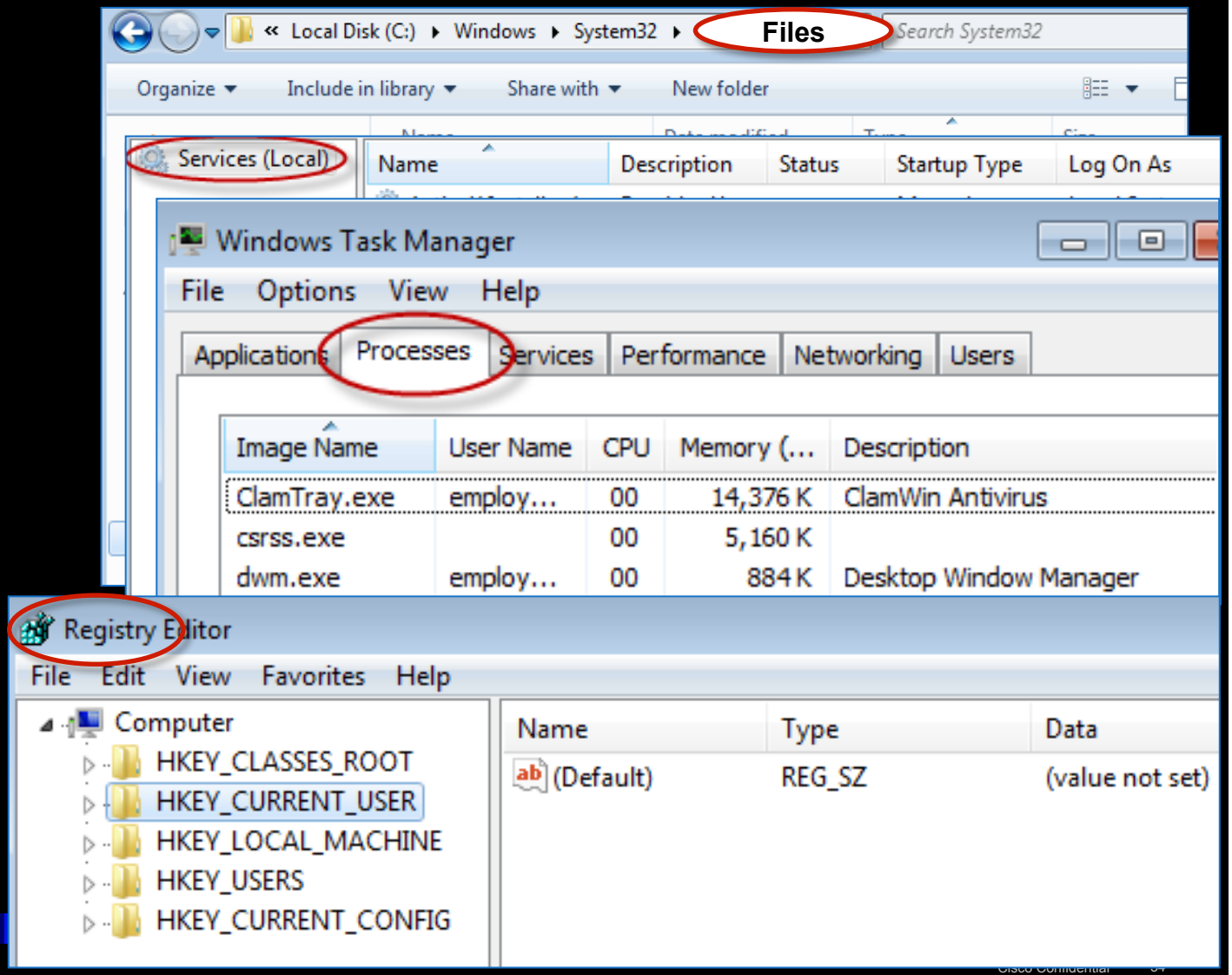
Permissions = Authorizations
- Employee_PC Set VLAN = 30 (Full Access)
- Employee_iPAD Set VLAN = 40 (Internet Only)

Posture Assessment

Leveraging the NAC Agent additional information is learned through Posture

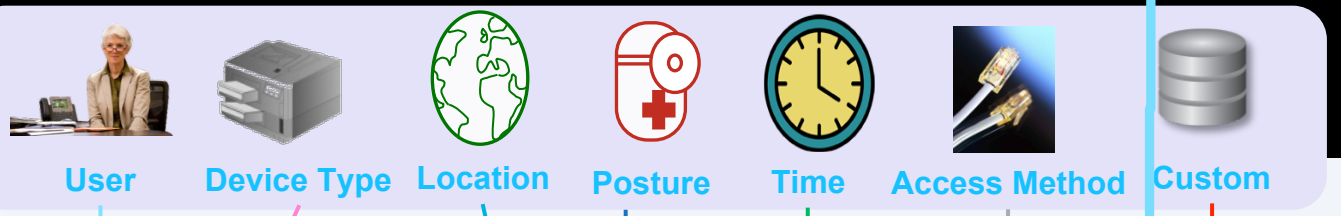
- Posture = the state-of-compliance with the company's security policy.
  - Is the system running the current Windows Patches?
  - Anti-Virus Installed? Is it Up-to-Date?
  - Anti-Spyware Installed? Is it Up-to-Date?
- Now we can extend the user / system Identity to include their Posture Status.
- What can be checked?
  - AV/AS, Registry, Files, Application / Process, Windows updates, WSUS and more.
- If not compliant – Auto remediation, alert, download file
- NAC Agent (persistent) and Web Agent (Temporal) support

ISE – Posture Assessment Checks



Putting It All Together in Authorization Policies

Authorization Policy = Access Permissions



Authorization Policy At A Glance

First Matched Rule Applies

Standard

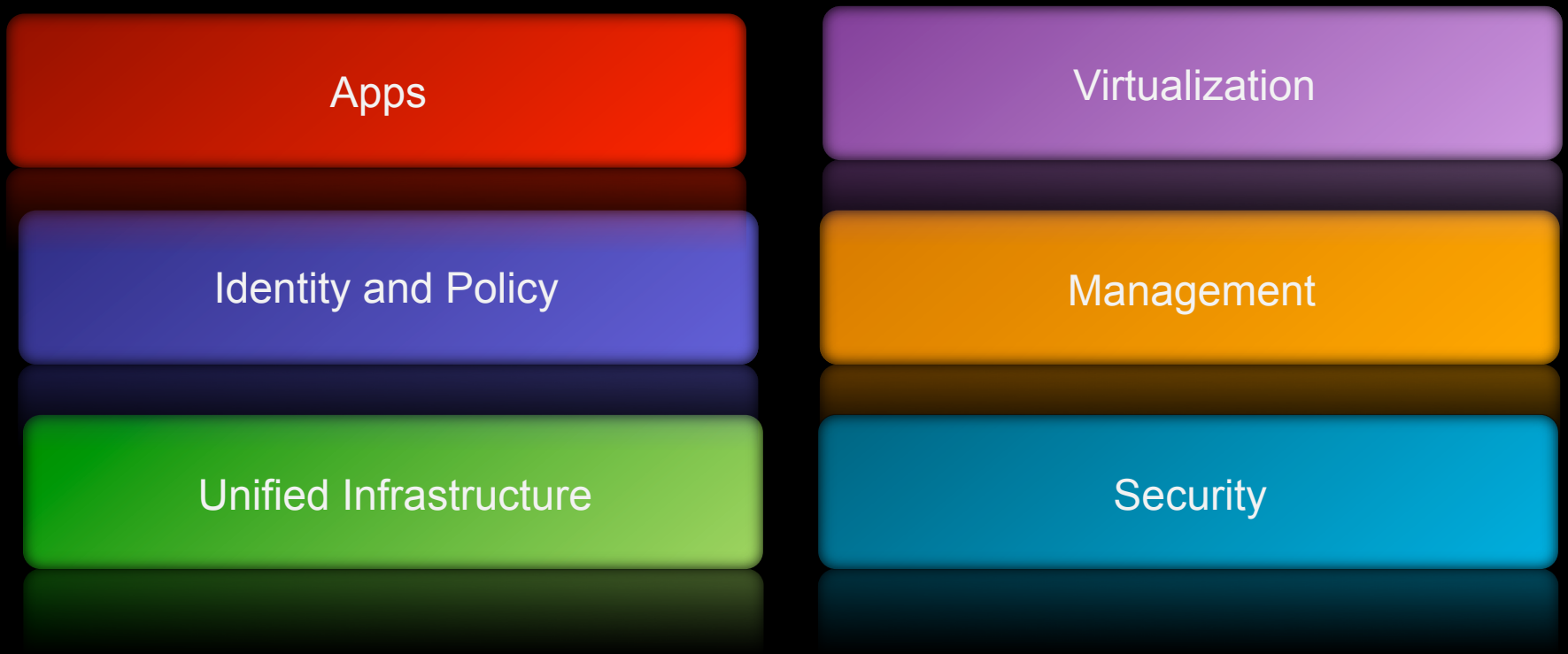
Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Profiled Cisco IP Phones	Cisco-IP-Phone		Cisco_IP_Phones
Enabled	Game_Console	Game_Console-Registered		Game_Console
Enabled	Domain_Computer	Any	demo.local:ExternalGroups EQUALS demo.local/Users/Domain Computers AND San_Jose AND CERTIFICATE:Subject Alternative Nam MATCHES .*(demo.local)$ AND Radius:User-Name MATCHES ^(host/).*	AD_Login
Enabled	Employee-Wired	Any	Employee_Wired AND Posture_Compliant	Employee
Enabled	Employee-Wireless	Workstation	Employee_Wireless AND Posture_Compliant AND LDAP1:badPwdCour 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	Contrator_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

The Building Blocks of Cisco BYOD Solution

The BYOD Spectrum

Limit	Basic	Enhanced	Next Generation
Environment requires tight controls	**Focus on basic services, easy access, almost anybody**	**Enable differentiated services, on-boarding with security but no ownership**	**Corp native apps, new services, full control**
Corp Only Device Mfg Environment NYSE Trading Floor Classified Gov Networks Traditional Enterprise	**Broader Device Types But Internet Only** Edu Environments Public Institutions Simple Guest	**Multiple Device Types + Access Methods** Healthcare Early BYOD Enterprise Adopters Contractor Enablement	**Multiple Device Types, Corp Issued** Innovative Enterprises Retail on Demand Mobile Sales Services (Video, Collaboration, etc.)

Cisco BYOD Building Blocks



BYOD Use Cases & Solutions

Use Case	Limit	Basic	Enhanced	Advanced
Business Policy	Block Access	Role Based Access; (Guest Access)	Secure granular On-site and Off-Site Mobility	Full Workspace Experience
IT Requirements	• **Visibility to who/ what is on network** • **Restrict access to only corporate issued devices.**	• **Restrict personal devices to public internet.** • **Restricted access to internal sites**	• **Allow granular on-site and off-site access to network/ applications**	• **Enable a full mobile and collaboration experience**
User Scenario (Example)	Hospital extends wired access to medical staff only	Hospital provides guest access to patients	Doctor uses personal device in hospital and in an offsite coffee-shop	Hospital administrator is granted full network access and uses native applications
Solution Technology	Cisco Switches Cisco WLC Cisco Prime NCS Cisco Identity Services Engine	Cisco Switches Cisco WLC Cisco Prime NCS Cisco Identity Services Engine	Cisco Switches Cisco WLC Cisco Prime NCS Cisco Identity Services Engine Cisco Firewalls Cisco ESA/WSA. AnyConnect., ScanSafe Application Virtualization Cisco VXI , UCS, Nexus Enterprise Apps Collaboration Apps	Cisco Switches Cisco WLC Cisco Prime NCS Cisco Identity Services Engine Cisco Firewalls Cisco ESA/WSA. AnyConnect., ScanSafe Application Virtualization Cisco VXI , UCS, Nexus Enterprise Apps Collaboration Apps

Core network
Management
Identity and Policy
Security and Remote Access
Virtualization
Applications

BYOD: Use Case #1

Policy is to enable wireless and remote access for corporate and personal devices. Personal devices are restricted to email and basic web services.

Technologies

- 802.1X, Profiling, Guest Access, BYOD on-boarding

Solution Components

- Cisco WLCs
- ASA & AnyConnect
- ISE
- NCS Prime

BYOD: Use Case #2 – Next Generation (Retail)

Policy is to give sales assistants tablets for real time inventory, credit card transactions, customer helpline, etc. via native + collaboration apps with tight controls for PCI compliance. In store customers get free Internet access

Technologies

- 802.1X, Profiling, Guest, ISE + MDM Services, Collaboration + Native Apps

Solution Components

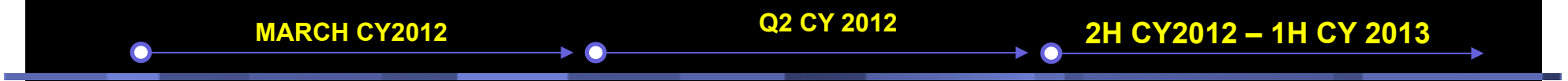
- Cisco Branch Routers
- ISE + NCS Prime
- DC (Nexus + UCS)
- Collaboration Apps

3rd Party

- MDM
- Native Apps

BYOD Roadmap

Cisco BYOD Roadmap



PHASE 1: CONTROL

- Network access control with comprehensive device profiling
- Guest Access
- View, control and troubleshoot all devices and application performance on entire network
- Centralized wired/wireless policy and role based grouping
- Malware protection with cloud connected hybrid web security
- Hi-Density .11n WiFi
- Seamless roaming Cellular to WiFi

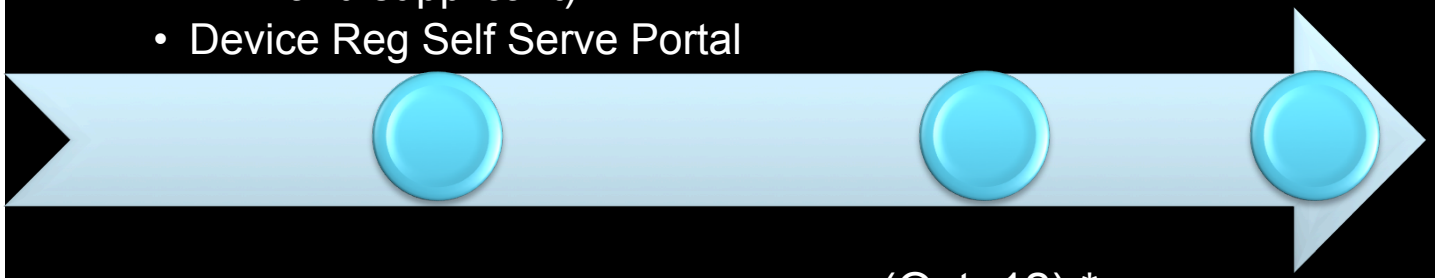
PHASE 2: SIMPLIFY

- Zero touch device registration and provisioning of employee/ guest devices
- Fast roaming in WiFi network

PHASE 3: INTEGRATE

- Integrate policy management with mobile device management
- Consistent policies for wired/wireless/VPN
- Cisco Prime infrastructure with wired/wireless integration and full 360 view of users, devices & apps
- Cisco Prime Assurance per user, per flow – policy based
- UC integrated enterprise 3G/4G experience

ISE Roadmap Highlights



ISE 1.1MR (June 12)

- BYOD Provisioning for iOS, Andriod, Windows and OS X and supplicant)
- Device Reg Self Serve Portal

BYOD Endpoint Provisioning

Scalbility imprrovements
Profile Service ++
Mobile Policy
Enhanced Reporting

ISE 1.2 (Oct. 12) *

- New UCS-based Appliances (34x5)
- Scale to 250k Endpoint System Scale
- Service Provisioning Bootstrap
- Enhanced Contextual Data
- More Flexible Reporting Logic
- Expanded NCS Integration
- Profiler Feed Service
- Common Criteria
- 3rd Party MDM
- WLC Based Device Sensor Integration

- IPV6
- TACACS+
- Unified AnyConnect Agent
- Mobile + Posture
- VDX/VDI Context
- Expanded Profiling Ecosystem
- Multi-Version Support
- Community Portal
- ID FW Integration

Beyond 1.2 **

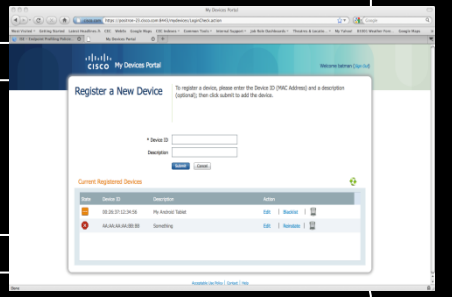
*** Going through formal commit process**

**** Still under evaluation**

ISE 1.1 MR Functionality

Supplicant profile provisioning on supported platforms (iOS, Android, Windows, OS X)

Self/Sponsor registration portals for users and devices



Certificate provisioning as registry authority (RA) adding username and device ID to cert (integrates with existing corp CA/PKI)

Secure access (open to closed network, single SSID, certificate based differentiation of service)

User initiated control their devices (designate “Lost” -> black-listing, re-instate device, etc)

MDM Strategy

Partner With Top MDM Providers For a Complete Solution

Initial Vendors

Others to follow …

ISE + MDM Functionality

On Premises MDM Device Registration - non registered clients redirected to MDM registration page

Restricted Access - non compliant clients will be given restricted access based on MDM posture state

Augment Endpoint Data - Update data from endpoint which cannot be gathered by profiling

Ability to initiate device action from ISE - eg: device stolen -> need to wipe data on client (Stretch for 1.2).

Key Takeaways

Key Takeaways:

- TrustSec brings a LOT of features that differentiate
- TrustSec can help solve top of mind issues like BYOD
- TrustSec uses ISE as the Policy Engine – Enforcement is at the Edge Device (Switch / WLC / Router)
- TrustSec is deployed successfully in many Cisco customer networks
- Cisco invests in BYOD solution with MDM partners