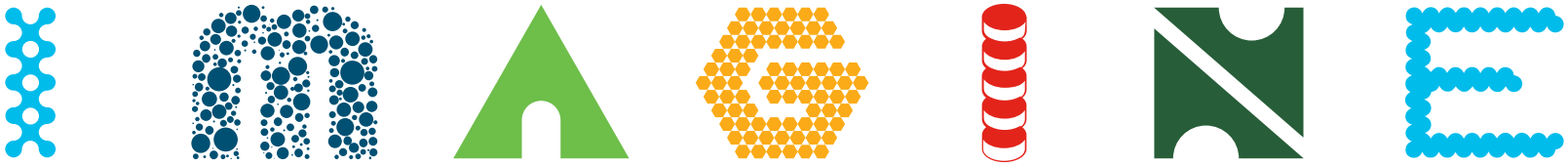


INTUITIVE

Cisco live!

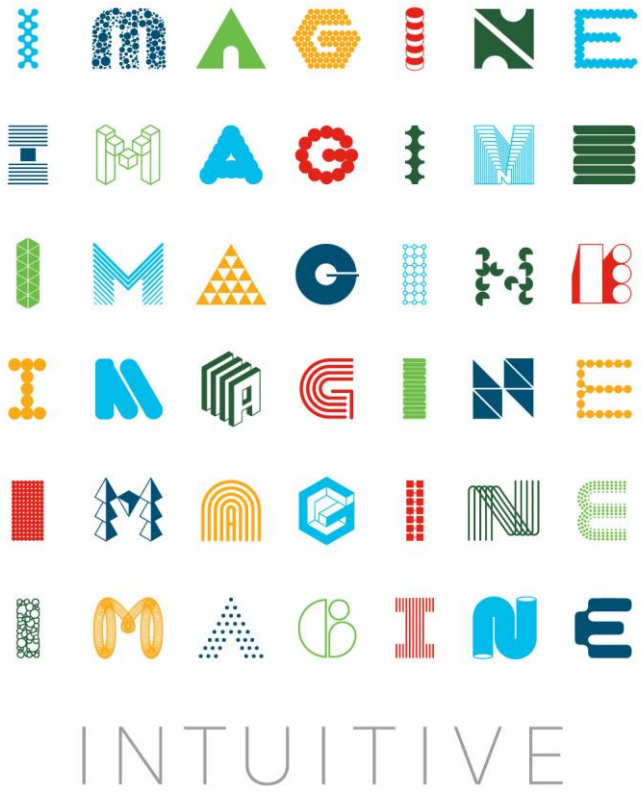
June 10-14, 2018 • Orlando, FL

#CLUS

Advanced ISE Services, Tips & Tricks

Craig Hyps, Principal Engineer

BRKSEC-3697



Session Abstract

Cisco Identity Services Engine (ISE) delivers context-based access control for every endpoint that connects to your network and serves as the advanced policy engine behind Cisco's Digital Network Architecture (DNA). In addition to providing visibility into all things and users that connect to the network, ISE offers a comprehensive solution for Authentication, automated Device Classification and IoT onboarding, Guest Access, Bring Your Own Device (BYOD), Endpoint Compliance, Software-Defined Segmentation, Context Sharing, Threat-Centric NAC, and controlled access to network devices.

This session will focus on the advanced services of ISE including successful deployment strategies, overall best practices, lessons learned from the trenches, as well as serviceability tips and tricks to help you gain optimal value and productivity from ISE. The session will also explore strategies for implementing successful access policies based on a Trusted Device + Trusted User.

ISE Sessions @Live Orlando 2018

You Are Here

Sunday

TECSEC-2672
Identity Services Engine 2.4 Best Practices
Jesse Dubois, Eugene Korneychuk, Kevin Redmon, Vivek Santuka
Monday 9:00-6:00

Monday

BRKSEC-2059
Deploying ISE in a Dynamic Environment
Clark Gambrel
Monday 1:30-3:30

Wednesday

BRKSEC-3697
Advanced ISE Services, Tips & Tricks
Craig Hyps, Wednesday 8:00-10:00

BRKCOC-2018
Inside Cisco IT: How Cisco Deployed ISE and Group Based Policies throughout the Enterprise
Raj Kumar, David Iacobacci
Wednesday 8:30-10:00

BRKSEC-2464
Lets get practical with your network security by using Cisco ISE
Imran Bashir, Wednesday 10:30-12:00

BRKSEC-2695
Building an Enterprise Access Control Architecture using ISE and Group Based Policies
Imran Bashir, Wednesday 1:30-3:30

Thursday

BRKSEC-3699
Designing ISE for Scale & High Availability
Craig Hyps
Thursday 8:00-10:00

BRKSEC-2038
Security for the Manufacturing Floor - The New Frontier
Shaun Muller
Thursday 10:30-12:00

BRKSEC-2039
Cisco Medical Device Segmentation
Tim Lovelace, Mark Bernard
Thursday 1:00-2:30

ISE Integrations and Lab Sessions

Labs

LABSEC-2330
Rapid Threat Detection on ISE 2.3 With Cisco Fire power integration via Pxgrid
Kushagra Kaushik, Prachi Chauhan

LABSEC-1200
ISE 2.3 : Dot1x : Troubleshooting tips and tricks
Kushagra Kaushik, Prachi Chauhan

Tuesday

BRKSEC-3557
Advanced Security Integration, Tips & Tricks
Aaron Woland
Tuesday 4:00-6:00

Wednesday

SOLSEC-2002
Extending Cisco Identity Services Engine Policies to the Cloud and Beyond
Doug Johnson
Wednesday 11:10-11:25

BRKSEC-3889
Advanced Security Architecture Integrations using APIs and pxGrid
Jamie Sanbower
Wednesday 1:30-3:30

Thursday

BRKSEC-3014
Security Monitoring with Stealthwatch: The Detailed Walkthrough
Matthew Robertson
Thursday 8:00-10:00

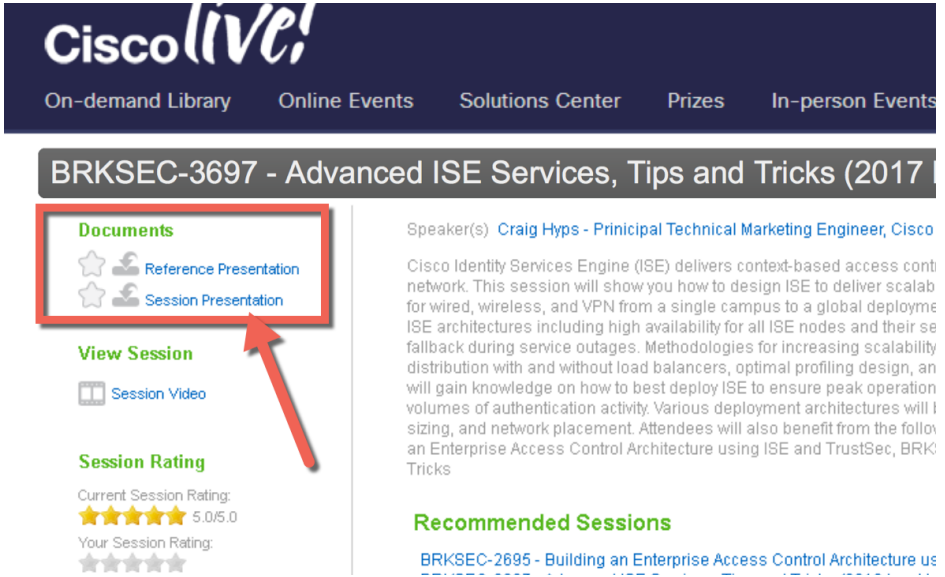
DEVNET-1010
Using Cisco pxGrid for Security Platform Integration
Nancy Cam-Winget, Syam Appala
Thursday 10:30-11:15

Important: Hidden Slide Alert

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

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

For Your Reference



**~400 Slides in PDF

Cisco Webex Teams

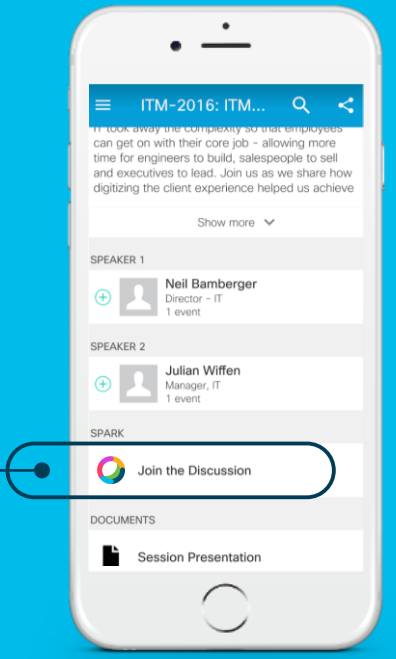
Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How

1. Find this session in the Cisco Events App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

Webex Teams will be moderated by the speaker until June 18, 2018.



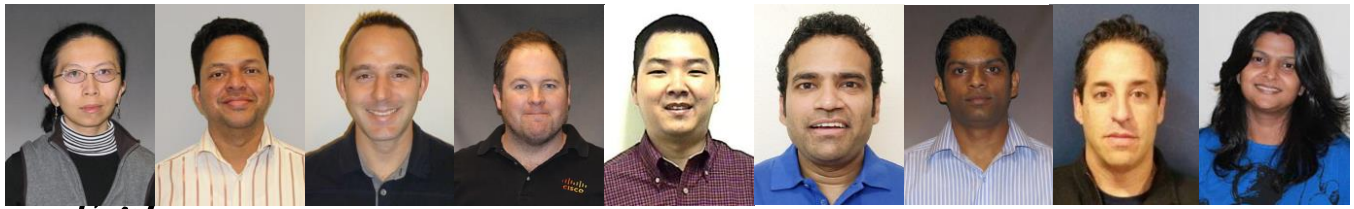
cs.co/ciscolivebot#BRKSEC-3697

Where can I get help after Cisco Live?

ISE Public Community http://cs.co/ise-community

Questions answered by ISE TMEs and other Subject Matter Experts – the same persons that support your local Cisco and Partner SEs!

ISE Compatibility Guides http://cs.co/ise-compatibility
ISE Design Guides http://cs.co/ise-guides



Courtesy of Thomas Howard

Session Agenda

- Installation and Upgrade
- Auth Policy Tuning and Tricks
- AD Integration
- Guest and Web Services
- Profiling and Anomalous Behavior Detection
- Posture Best Practices 
- TACACS+ Design
- Passive Identity and Easy Connect
- Trusted Device + Trusted User
- Context Visibility

 Time Permitting

Installation and Upgrade

ISE 2.4 Sizing by Deployment/Platform/Persona

Max Concurrent Session Counts by Deployment Model and Platform

- By Deployment

Deployment Model	Platform	Max Active Sessions per Deployment	Max # Dedicated PSNs / PXGs	Min # Nodes (no HA) / Max # Nodes (w/ HA)
	3515	7,500	0	1 / 2
	3595	20,000	0	1 / 2
	3515 as PAN+MNT	7,500	5 / 2*	2 / 7
	3595 as PAN+MNT	20,000	5 / 2*	2 / 7
	3595 as PAN and MNT	500,000	50 / 2	3 / 58
	3595 as PAN and Large MNT	500,000	50 / 4	3 / 58

Max Active Sessions != Max Endpoints; ISE 2.1+ supports 1.5M Endpoints

- By PSN

Scaling per PSN	Platform	Max Active Sessions per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3515	7,500
	SNS-3595	40,000

* Each dedicated pxGrid node reduces PSN count by 1 (Hybrid deployment only)

ISE 2.4 Appliance Support

- Hardware Appliances
  - SNS-3515
  - SNS-3595

- Virtual Appliances
  - Small (based on SNS-3515)
  - Medium (based on SNS-3595)
  - Large (based on Memory-Enhanced SNS-3595)

No SNS-34x5 Support in ISE 2.4

ISE 2.3 is last supported release for SNS-3400 Series

SNS-34x5 End of Life/End of Sale Notice: https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/eos-eol-notice-c51-737032.html

Sizing Production VMs to Physical Appliances

Summary

Appliance used for sizing comparison	CPU		Memory (GB)	Physical Disk (GB) **
	# Cores	Clock Rate*		
SNS-3415	4	2.4	16	600
SNS-3495	8	2.4	32	600
SNS-3515	6	2.3	16	600
SNS-3595	8	2.6	64	1,200

* Minimum VM processor clock rate = 2.0GHz per core (same as OVA).

** Actual disk requirement is dependent on persona(s) deployed and other factors. See slide on Disk Sizing.

Warning: # Cores not always = # Logical processors / vCPUs due to Hyper Threading

ISE OVA Templates

Summary

OVA Template	CPU			Virtual Memory (GB)	Virtual NICs (GB)	Virtual Disk Size	Target Node Type
	# CPUs	Clock Rate (GHz)	Total CPU (MHz)				
Eval	2	2.3	4,600	8	4	200GB	EVAL
SNS3415	4	2.0	8,000	16	4	200GB	PSN/PXG
						600GB	PAN/MnT
SNS3495	8	2.0	16,000	32	4	200GB	PSN/PXG
						600GB	PAN/MnT
SNS3515	~~8~~ 12	2.0	12,000	16	6	200GB	PSN/PXG
						600GB	PAN/MnT
SNS3595	~~8~~ 16	2.0	16,000	64	6	200GB	PSN/PXG
						1.2TB	PAN/MnT

CSCvh71644 - VMware OVA templates for SNS-35xx are not detected correctly...

For 35x5 ISE VMs, HyperThreading is Mandatory

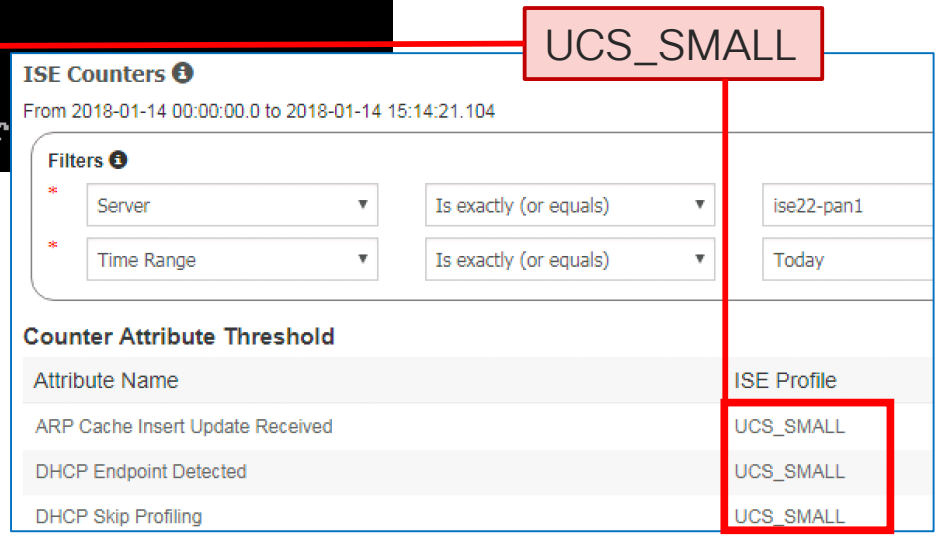
ISE Platform Properties

Verify ISE Detects Proper VM Resource Allocation

- From CLI...
  - `ise-node/admin#` **`show tech | begin PlatformProperties`**

```
PlatformProperties whoami: root

PlatformProperties show inventory: Process Output:

Profile : UCS_SMALL
Current Memory Size : 16267516
Time taken for NSFAdminServiceFactor
```

- From Admin UI (ISE 2.2 +)
  - Operations > Reports > Diagnostics > ISE Counters > [node] (Under ISE Profile column)



ISE VM Provisioning Guidance

- Use reservations (built into OVAs)
- Do not oversubscribe!

Customers with VMware expertise may choose to disable resource reservations and over-subscribe, but do so at own risk.

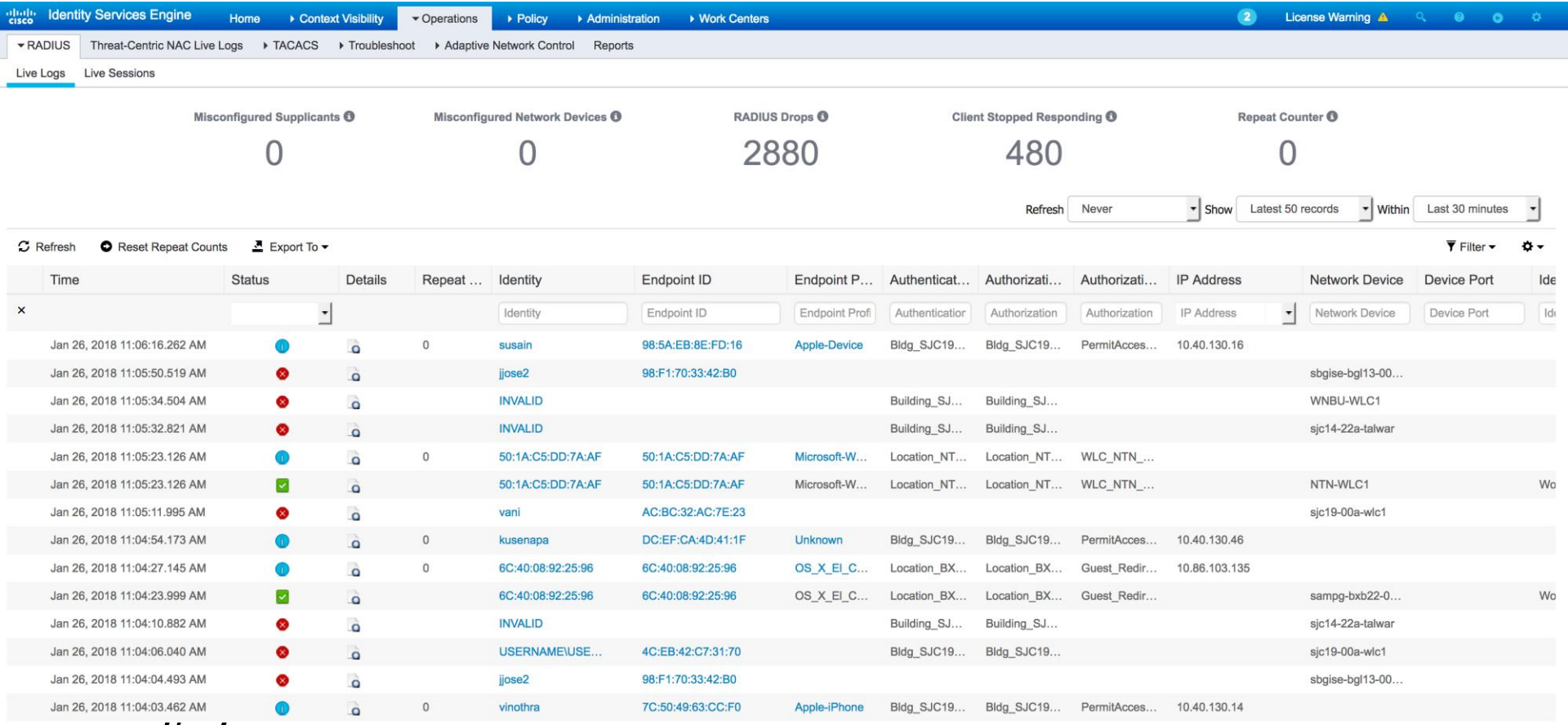
Introducing “Super” MnT

For Any Deployment where High-Perf MnT Operations Required

- Virtual Appliance Only option in ISE 2.4
  - Requires Large VM License
- 3595 specs + 256 GB
  - 8 cores @ 2GHz min (16000+ MHz)
    = 16 logical processors
  - 256GB RAM
  - Up to 2TB* disk w/ fast I/O
- Fast I/O Recommendations:
  - Disk Drives (10k/15k RPM or SSD)
  - Fast RAID w/Caching (ex: RAID 10)
  - More disks (ex: 8 vs 4)

* CSCvb75235 - DOC ISE VM installation can't be done if disk is greater than or equals to 2048 GB or 2 TB

ISE 2.4 MnT -- Fast Access to Logs and Reports



Flash Removal (ISE 2.4)

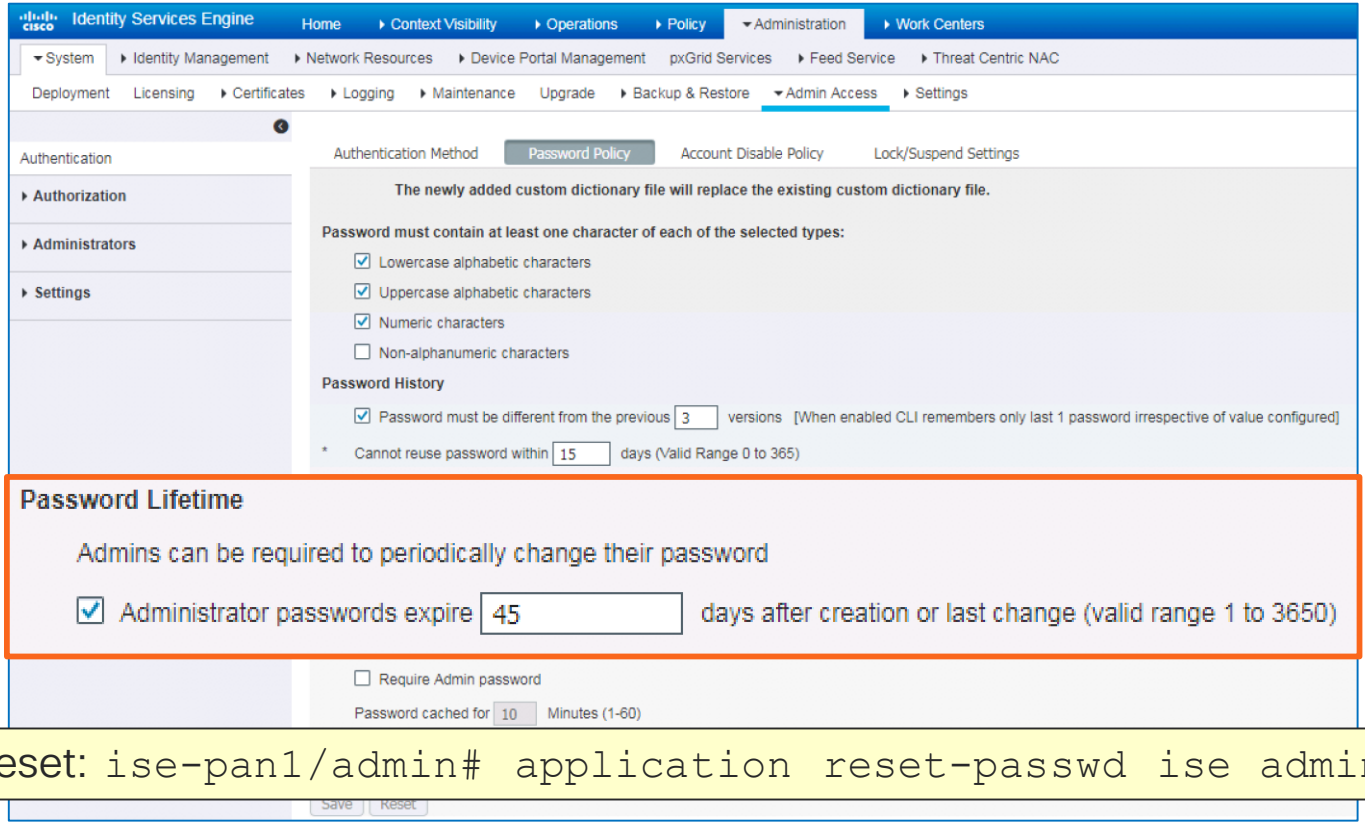
And no Yahoo! User Interface Library (YUI)

- “No Flash”
- C’mon, you mean just a little bit of flash, right?
- No. I’m Saying No Flash! There is no Flash in this product!

Post-Install Setup – First Things First

Update Admin Access Settings

- Set password policy and lockout settings.
- Consider secondary super admin account as backup.

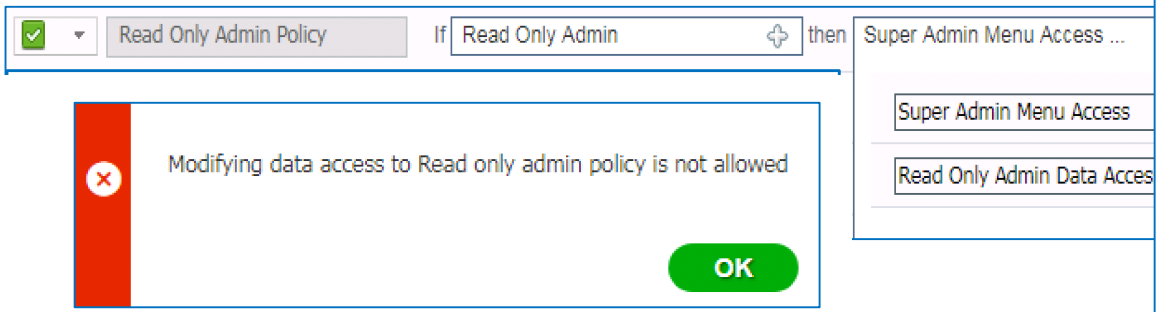


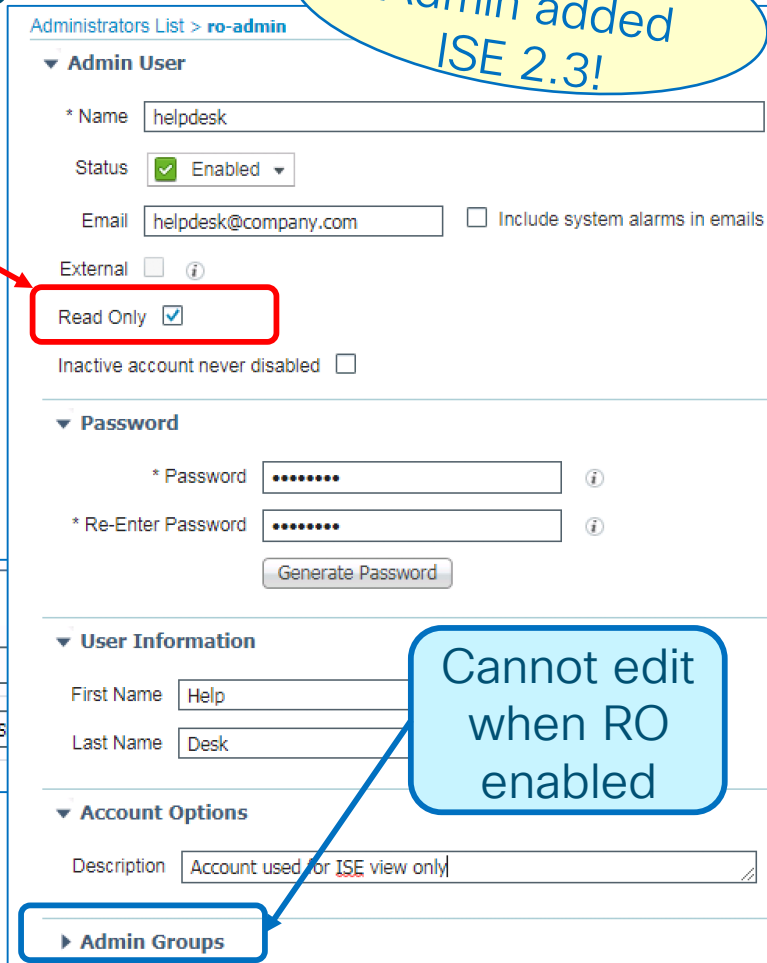
Admin UI Password Reset: `ise-pan1/admin# application reset-passwd ise admin`

Post-Install Setup – First Things First

Configure Read-Only (RO) Admins

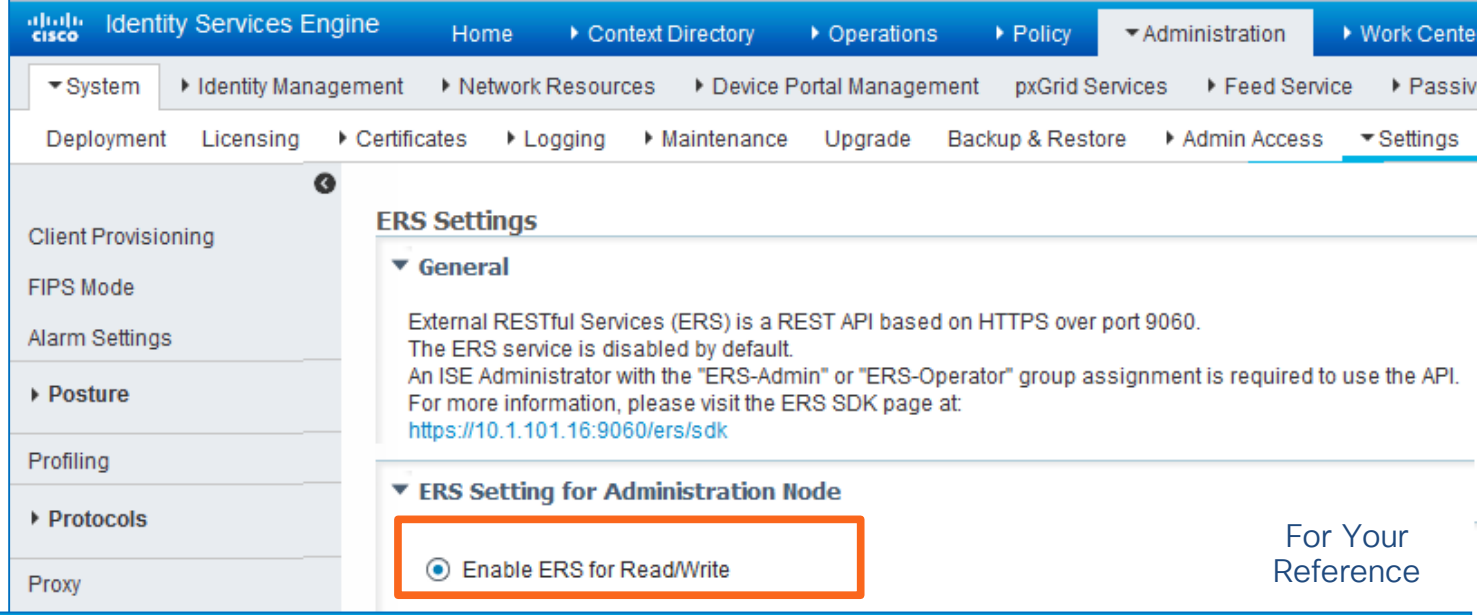
- Simply enable “Read Only” flag for admin user account
- RO Admin granted full Menu Access but Read Only to Data. Menu access can be changed, but not data access.



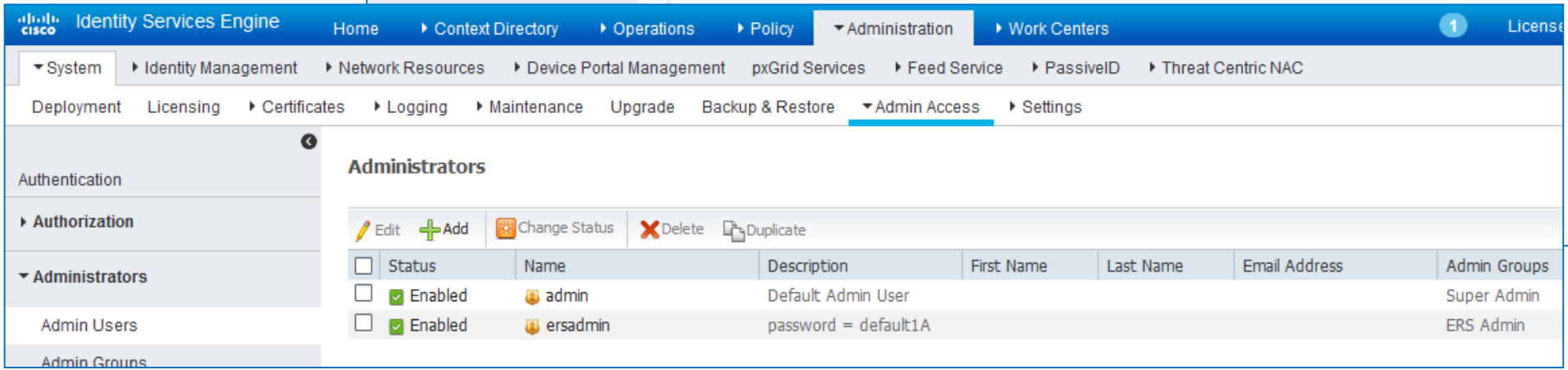


Configure ERS API

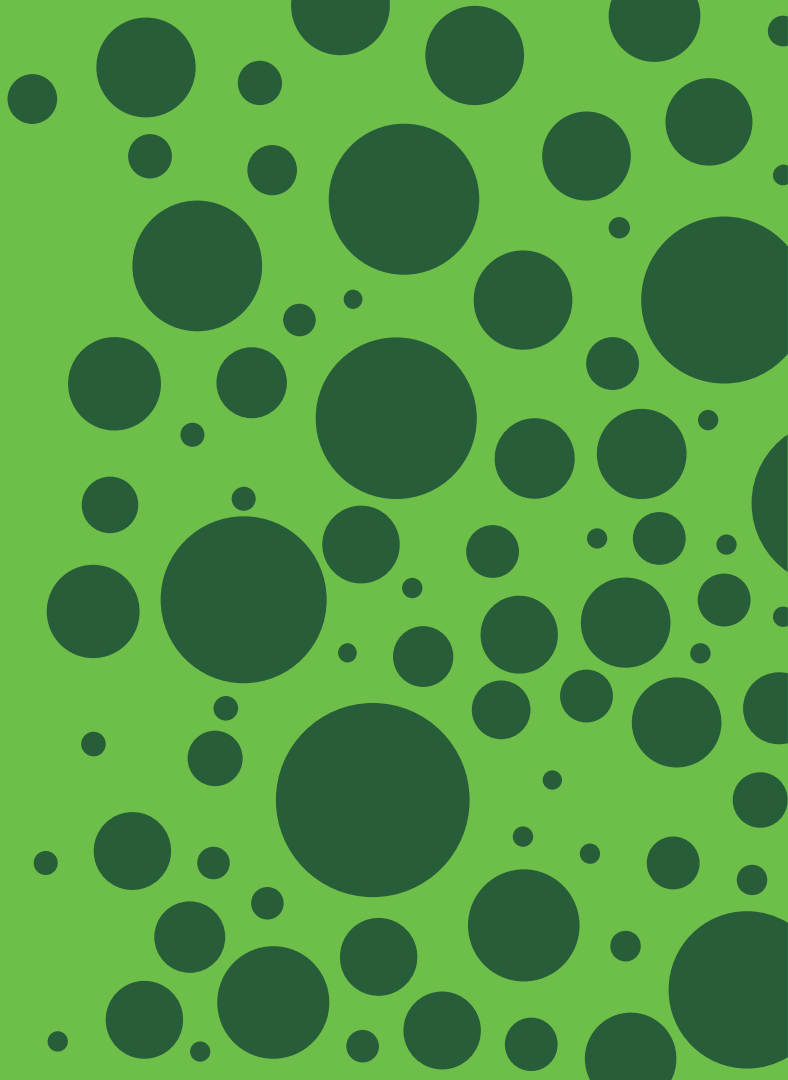
1. Enable ERS
2. Create ERS Admin user
3. Add to ERS Admin Group



For Your Reference



ISE Upgrades



Upgrade Readiness Tool (URT)

Available on Cisco.com under ISE Software

Introduced in ISE 2.3

Upgrade Readiness Tool (URT) to validate config DB upgrade from 2.0, 2.0.1, 2.1, 2.2, 2.3 to 2.4. This is a signed bundle for image integrity. ise-urtbundle-2.4.0.357-1.0.0.SPA.x86_64.tar.gz	29-MAR-2018

- CLI tool used outside of upgrade bundle
- Detect potential upgrade issues BEFORE upgrade.
- No downtime needed to run tool.
- Runs data upgrade on cloned database on Secondary PAN or Standalone node.
- Reports failures/success for each stage as well as time estimate for upgrade.

```
####################################
# Running Upgrade Readiness Tool (URT) #
####################################
This tool will perform following tasks:
1. Pre-requisite checks
2. Clone config database
3. Copy upgrade files
4. Data upgrade on cloned database
5. Time estimate for upgrade

Pre-requisite checks
====================
Disk Space sanity check - Successful
NTP sanity - Successful
Appliance/VM compatibility - Successful
Trust Cert Validation - Successful
System Cert Validation - Successful
Invalid MDMServerNames in Authorization
Policies check -Successful
6 out of 6 pre-requisite checks passed
_______
Clone config database...
```

Upgrade Enhancements

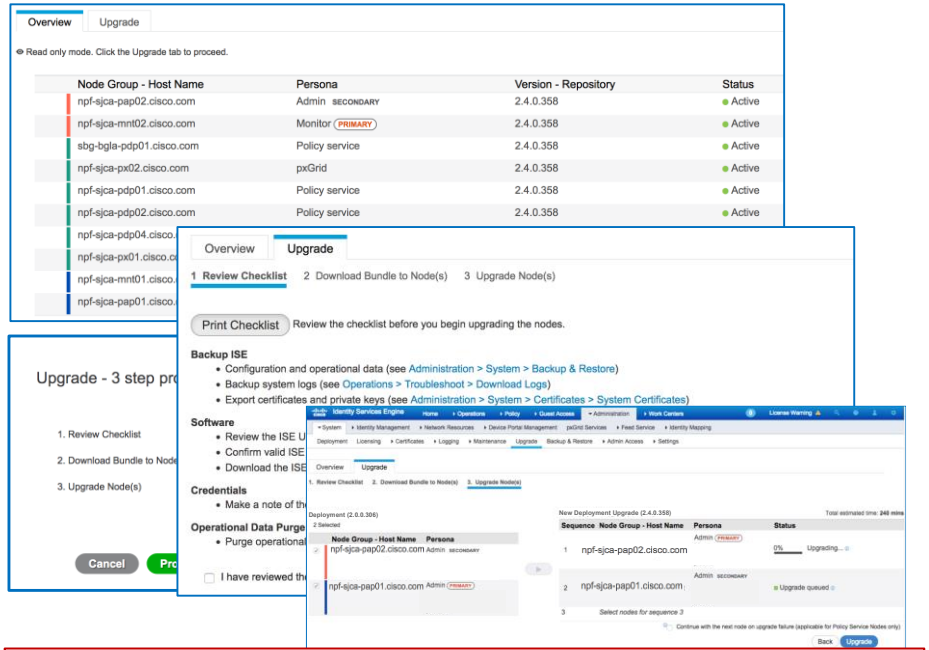
Example URT Outputs

```
- Data upgrade step 93/96, NSFUpgradeService(2.3.0.206)... Done in 0 seconds.
- Data upgrade step 94/96, ProfilerUpgradeService(2.3.0.206)... Done in 1 seconds.
- Data upgrade step 95/96, GuestAccessUpgradeService(2.3.0.206)... Done in 6 seconds.
- Successful
Running data upgrade for node specific data on cloned database
- Successful

Time estimate for upgrade
=========================
Estimated time for each node(in mins):
upsdev-vm11(STANDALONE):193



Application successfully installed
upsdev-vm11/admin#
```

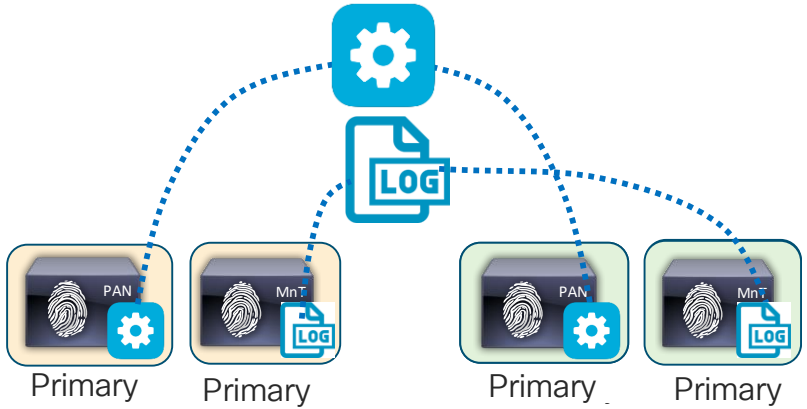
```
- Data upgrade step 90/97, NetworkAccessUpgrade(2.3.0.178)... Done in 0 seconds.
- Data upgrade step 91/97, NetworkAccessUpgrade(2.3.0.182)... Done in 0 seconds.
- Data upgrade step 92/97, CertMgmtUpgradeService(2.3.0.194)... Done in 3 seconds.
- Data upgrade step 93/97, UPSUpgradeHandler(2.3.0.201)... Failed.
- Failed
Final cleanup before exiting...

Collecting log files ...
- Encrypting logs bundle...
Please enter encryption password:
Please enter encryption password again to verify:
Encrypted URT logs(urt_logs.tar.gpg) are available in localdisk. Please reach out to Cisco to debug
% Post-install step failed. Please check the logs for more details.
upsdev-vm11/admin# exit
```

ISE Upgrade: Standard or Backup/Restore Method

Standard Upgrade



Backup/Restore



Backup/Restore method requires more manual effort, but provides ”cleanest” upgrade.

CSCvi38845 Upgrade fails after Feed update due to less heapspace -- Requires new Upgrade Bundles to be posted to Software Center

CSCvh57345 Restore of 1.4/2.0/2.0.1 backup fails which taken after Feed update -- Fixed in 2.2 Patch 8 and 2.4

ISE Upgrade Best Practices Guide

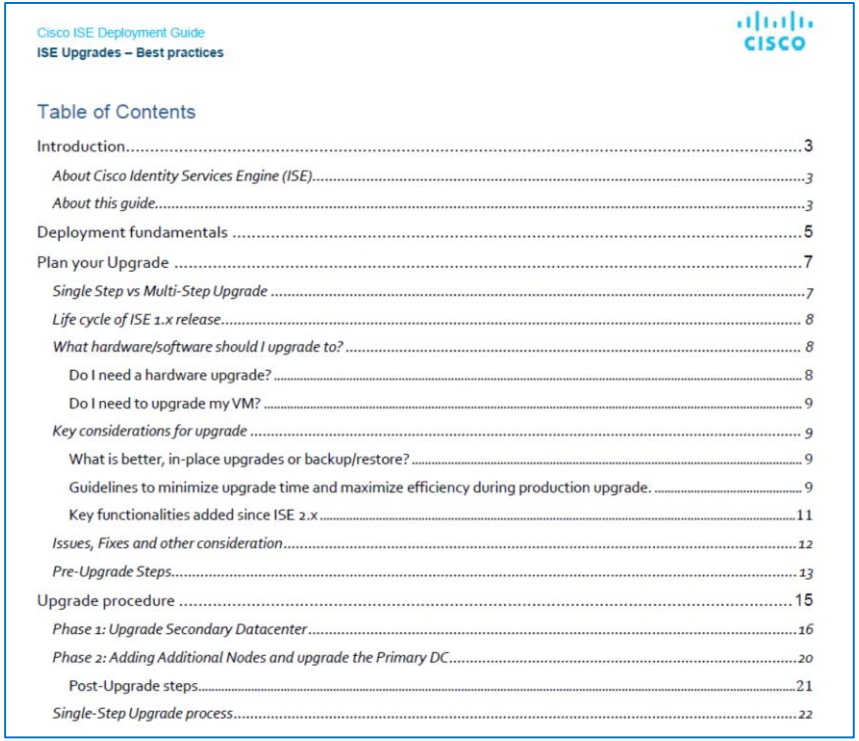
https://communities.cisco.com/docs/DOC-77486

Cisco ISE Deployment Guide
ISE Upgrades – Best practices

ISE upgrades – Best Practices

This deployment guide is intended to provide key details, information related to best practices, tips and tricks for smooth upgrade of Cisco Identity Services Engine software.

Krishnan Thiruvengadam
April 19, 2018

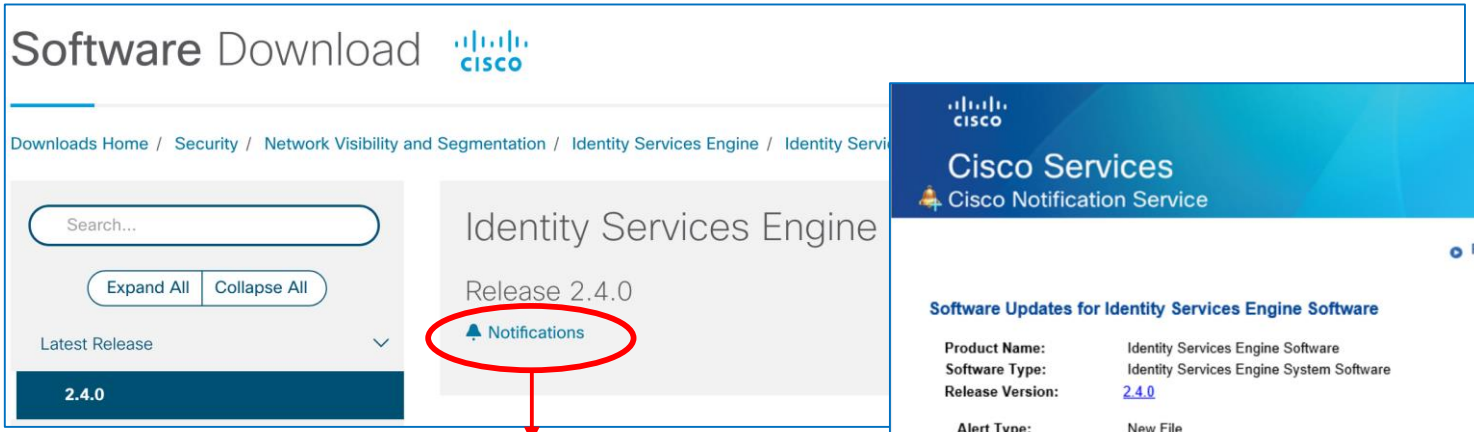


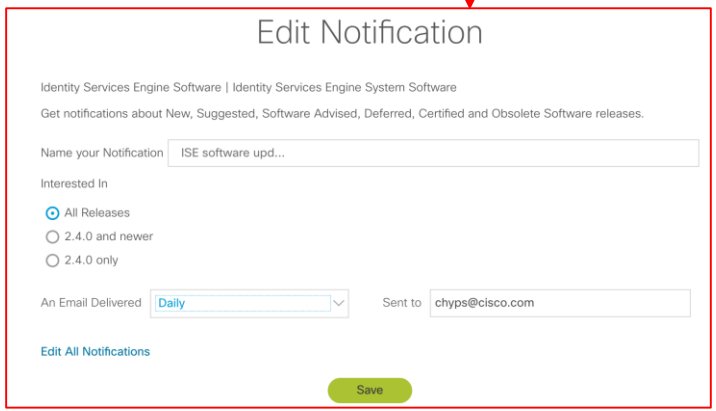
Cisco ISE Deployment Guide
ISE Upgrades – Best practices

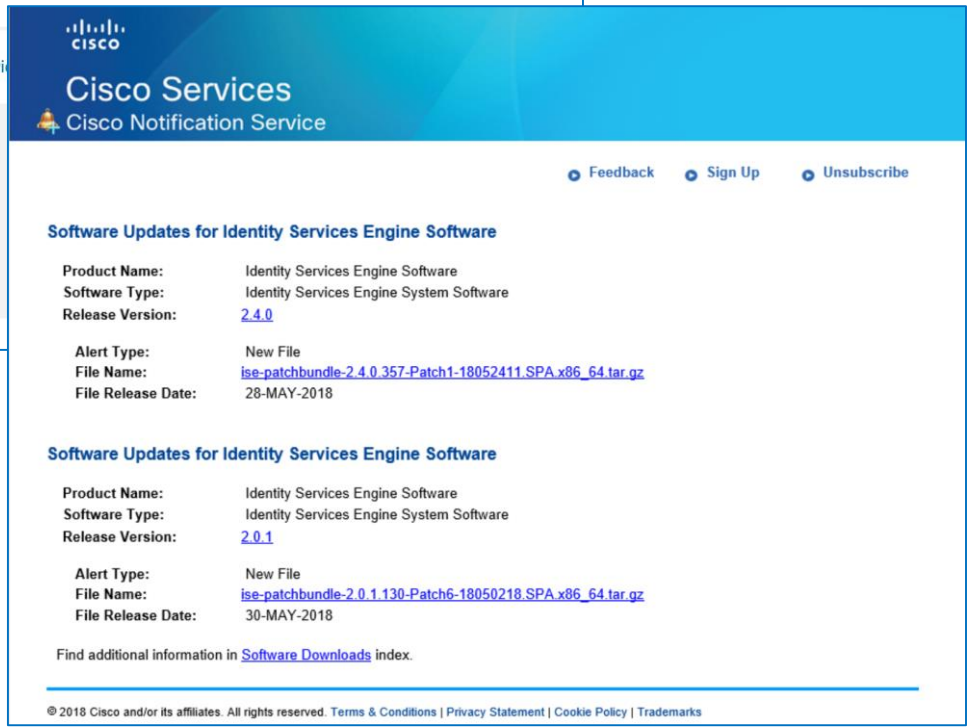
Table of Contents

Cisco Software Notifications

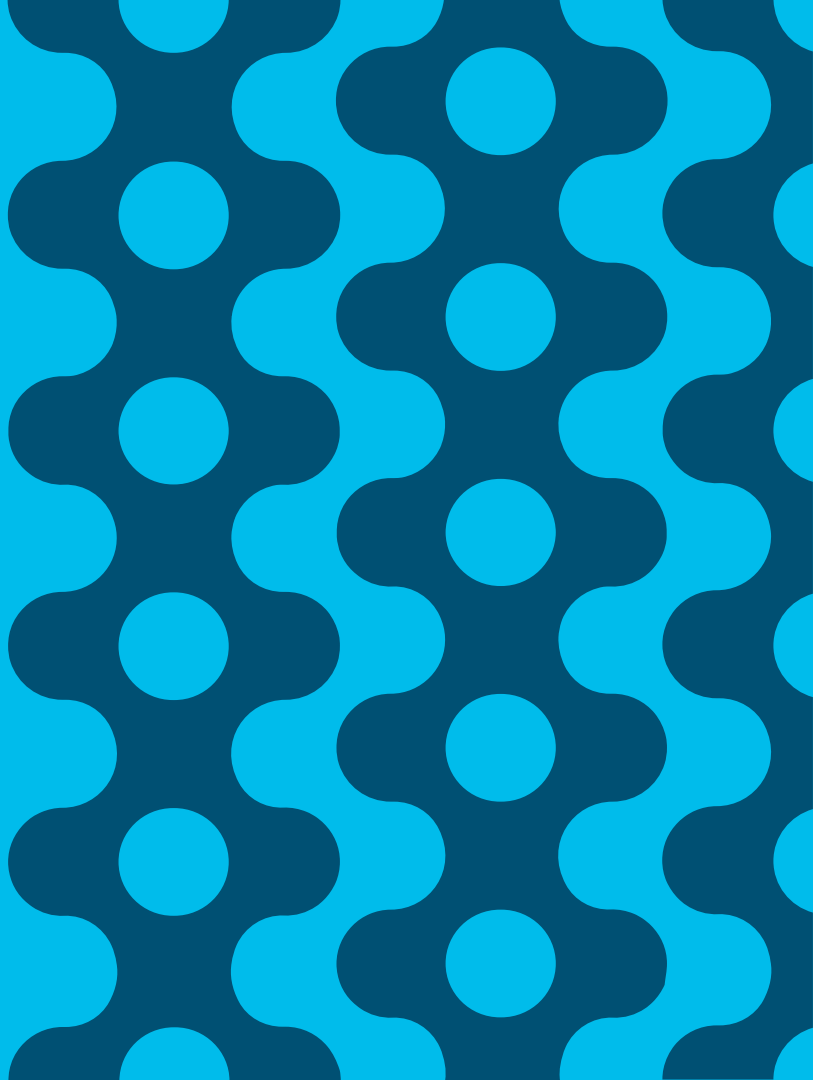
Be Alerted for New ISE Versions, Patches, PSIRTs, Field Notices, EoL, Bugs





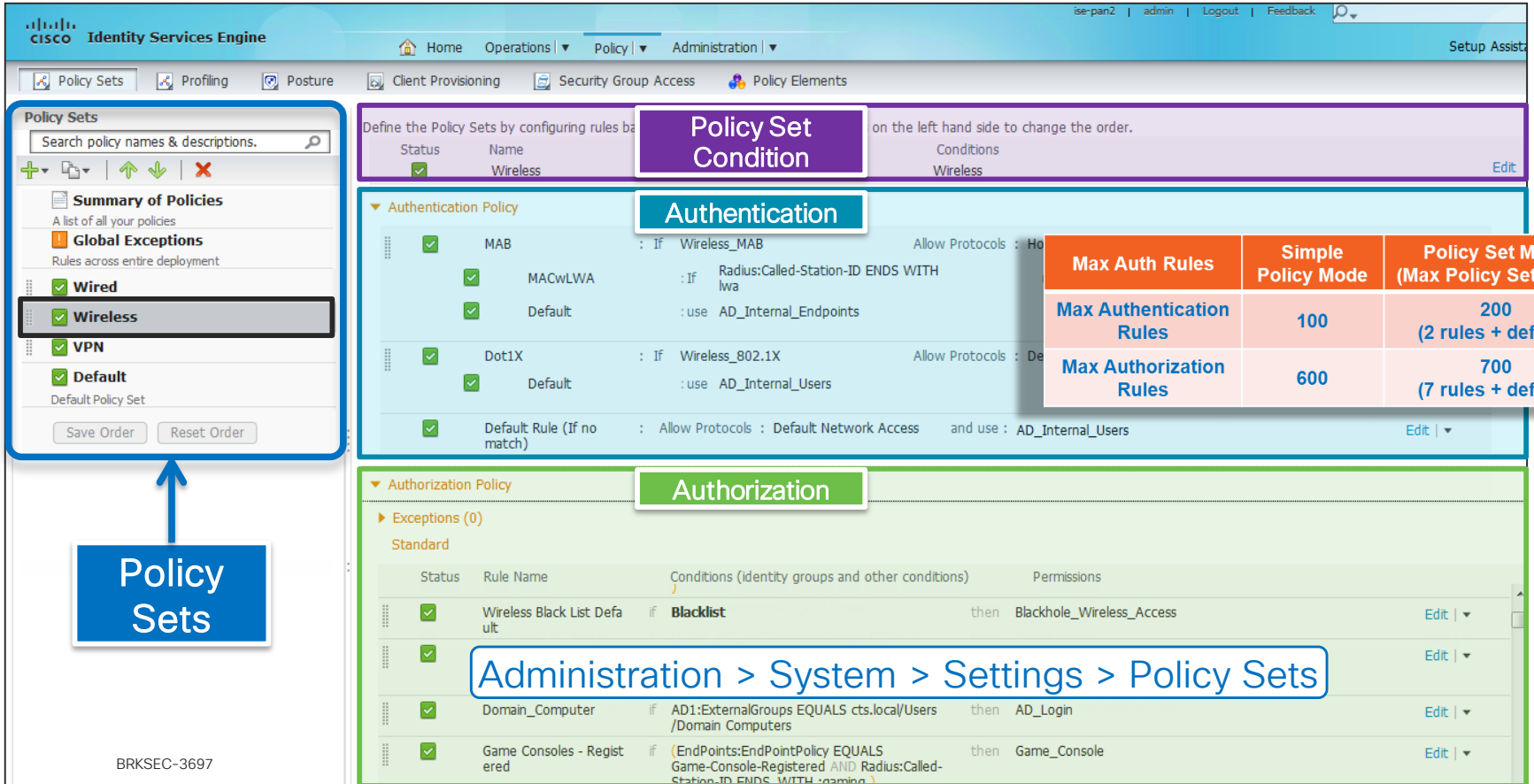


Auth Policy Tuning and Optimization



Auth Policy Optimization (ISE 2.2 and Earlier)

Leverage Policy Sets to Organize and Scale Policy Processing

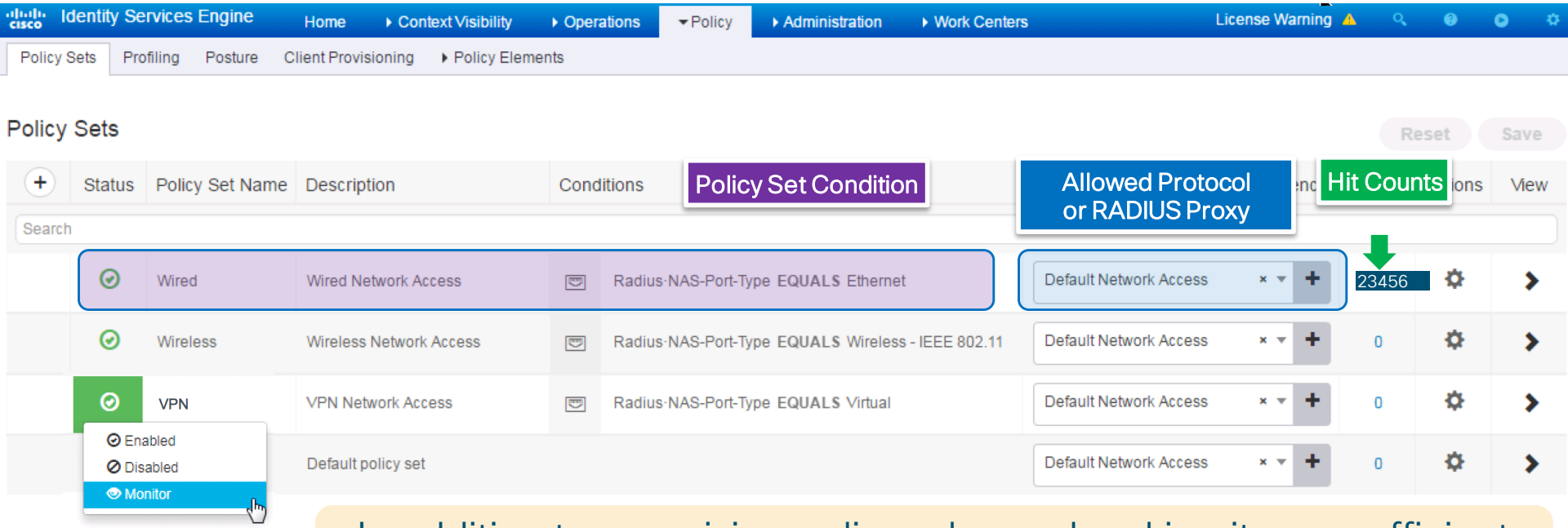


Max Auth Rules	Simple Policy Mode	Policy Set Mode (Max Policy Sets=100)
Max Authentication Rules	100	200 (2 rules + default)
Max Authorization Rules	600	700 (7 rules + default)

Policy Sets

Standard Equipment under new ISE 2.3 Policy User Interface

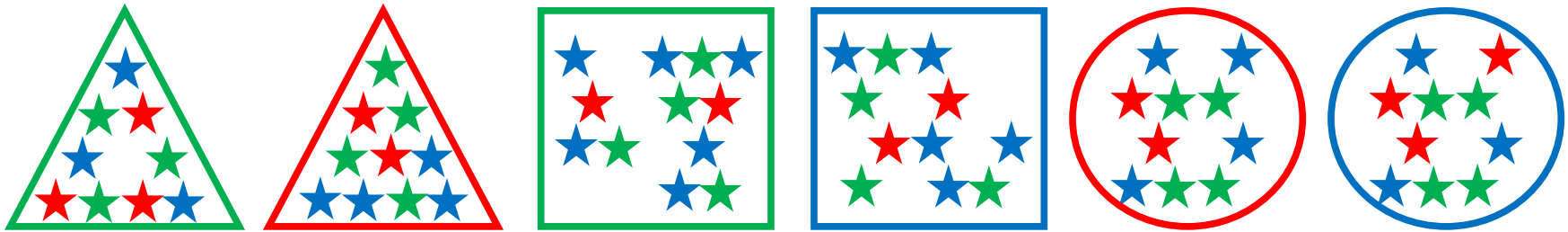
- No Authentication Outer Rule – Now part of Policy Set



In addition to organizing policy rules and making it more efficient and easy to manage, policy sets are great for staging test rules

Search Speed Test

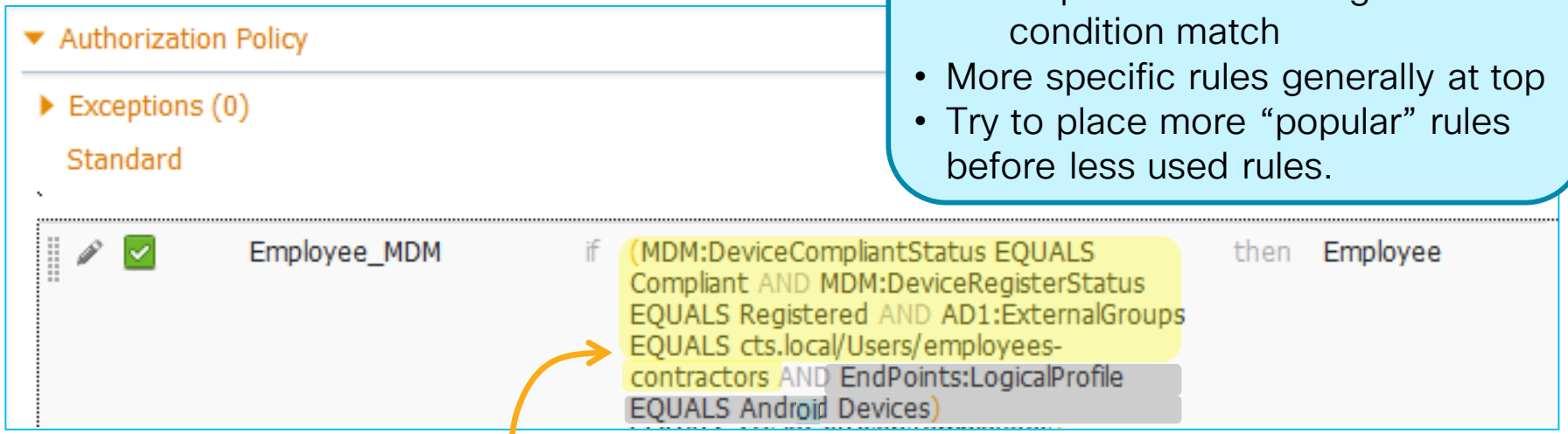
- Find the object where…
  - Total stars = 10
  - Total green stars = 4
  - Total red stars = 2
  - Outer shape = Red Triangle



Auth Policy Optimization

Avoid Unnecessary External Store Lookups

- Policy Logic:
  - First Match, Top Down
  - Skip Rule on first negative condition match
- More specific rules generally at top
- Try to place more “popular” rules before less used rules.

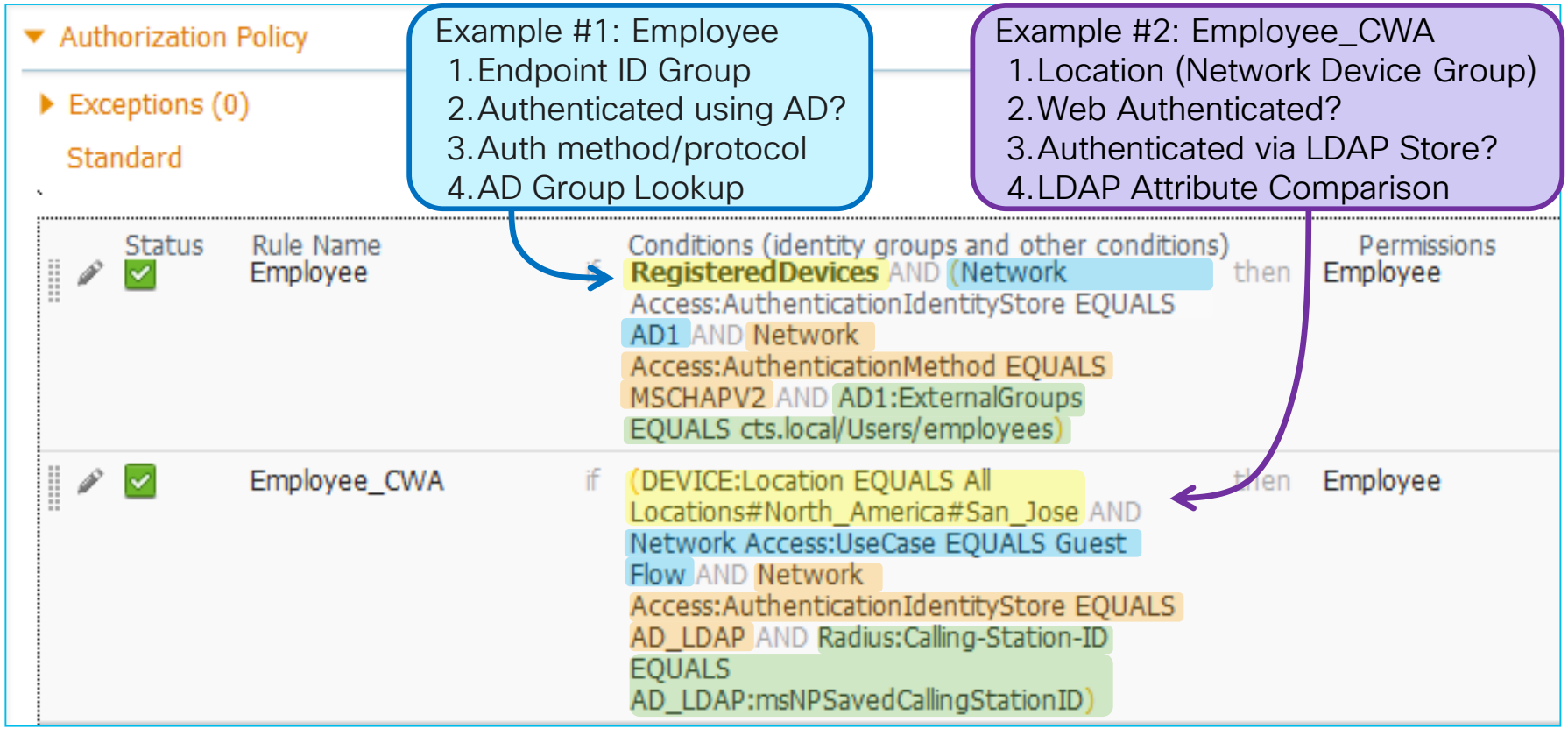


Example of a Poor Rule: Employee_MDM

- All lookups to External Policy and ID Stores performed first, then local profile match!

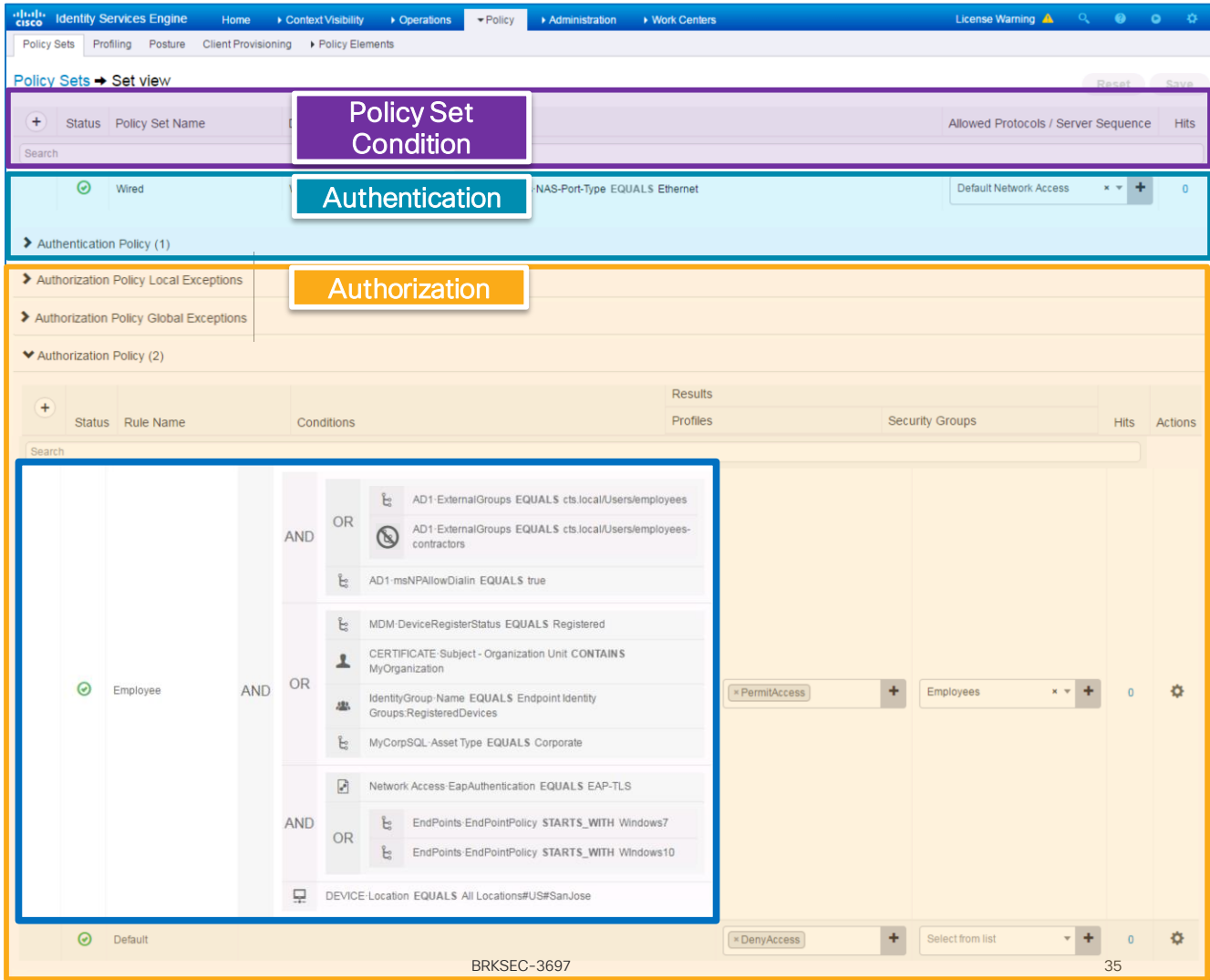
Auth Policy Optimization

Rule Sequence and Condition Order is Important!



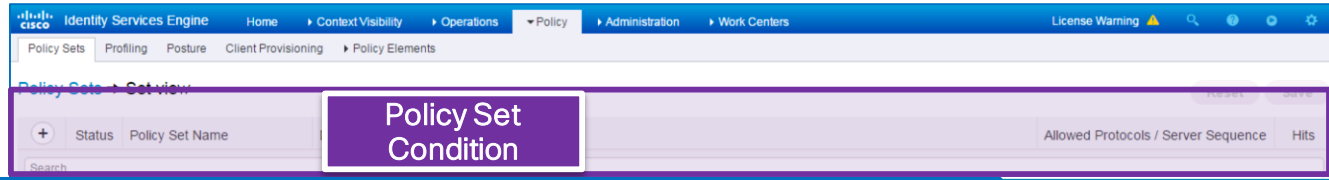
Auth Policy

ISE 2.3 Example

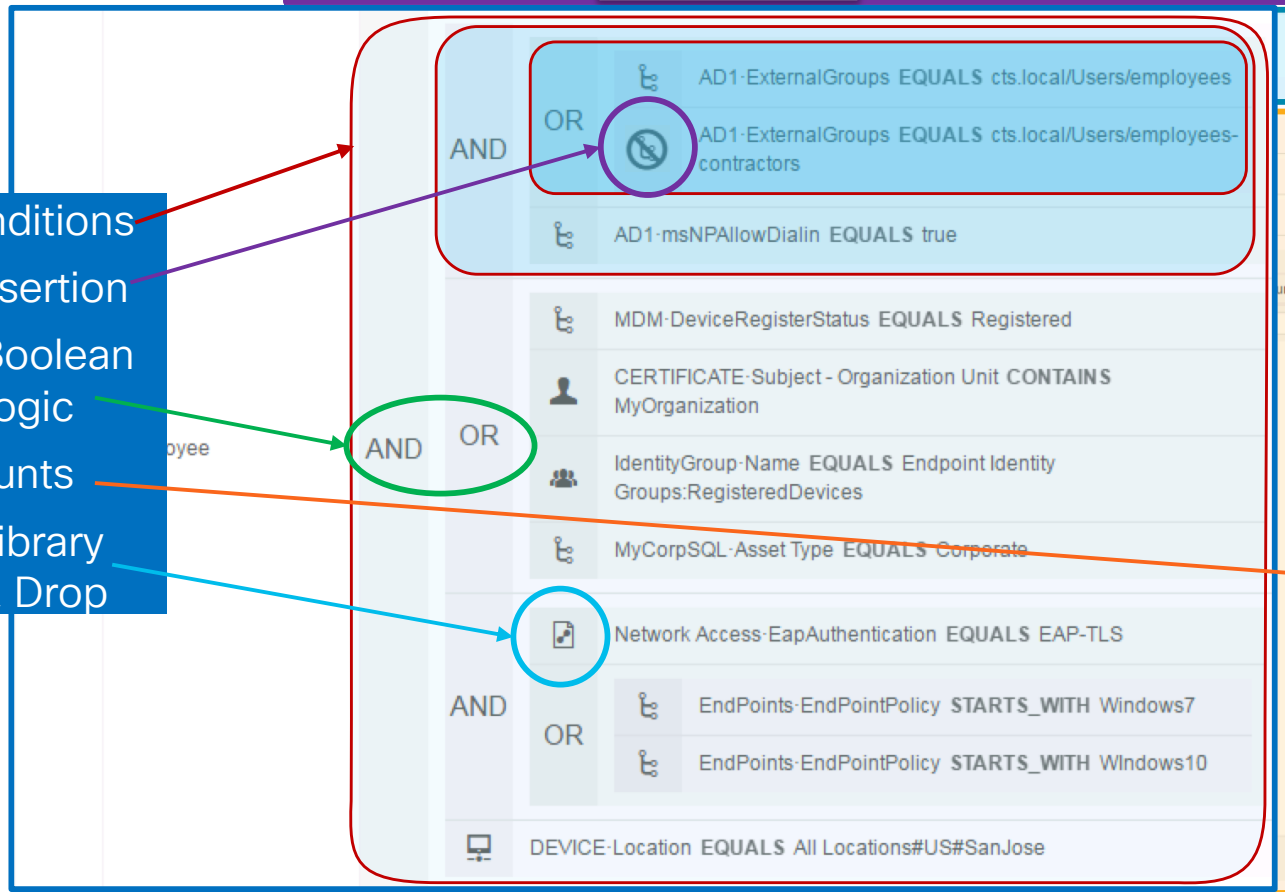


Auth Policy

ISE 2.3 Example



- Nested Conditions
- "IS NOT" insertion
- Simplified Boolean (AND/OR) logic
- Rule Hit Counts
- Condition Library with Drag & Drop



Advanced Compound Conditions (before ISE 2.3)

Tic-Tac-Toe

Policy > Policy Elements > Conditions

Authorization Simple Conditions

For Policy Export go to Administration > System > Backup & Restore > Policy

Edit | Add | Duplicate | Delete

Name	Expression
Anomalous_Behavior	EndPoints:AnomalousBehaviour EQUALS t
Anomalous_Exception	EndPoints:EndPointPolicy EQUALS Anomal
Asia	DEVICE:Location EQUALS All Locations#S
CertRe	
Europe	
India	
Mobile_	
Printer_	
SSID1	ssid
SSID2	Radius:Called-Station-ID ENDS_WITH ssid
US_East	DEVICE:Location EQUALS All Locations#N
US_West	DEVICE:Location EQUALS All Locations#San Jose
Wireless_Access	Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11
Workstation_Devices	EndPoints:LogicalProfile EQUALS Workstations

First create Simple Conditions. Required to make Advanced Compound Conditions.

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

Authorization Compound Conditions

* Na

Descript

If you switch to the advance view, you can not switch back. Do you want to proceed?

Yes | No

*Condition Expression

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

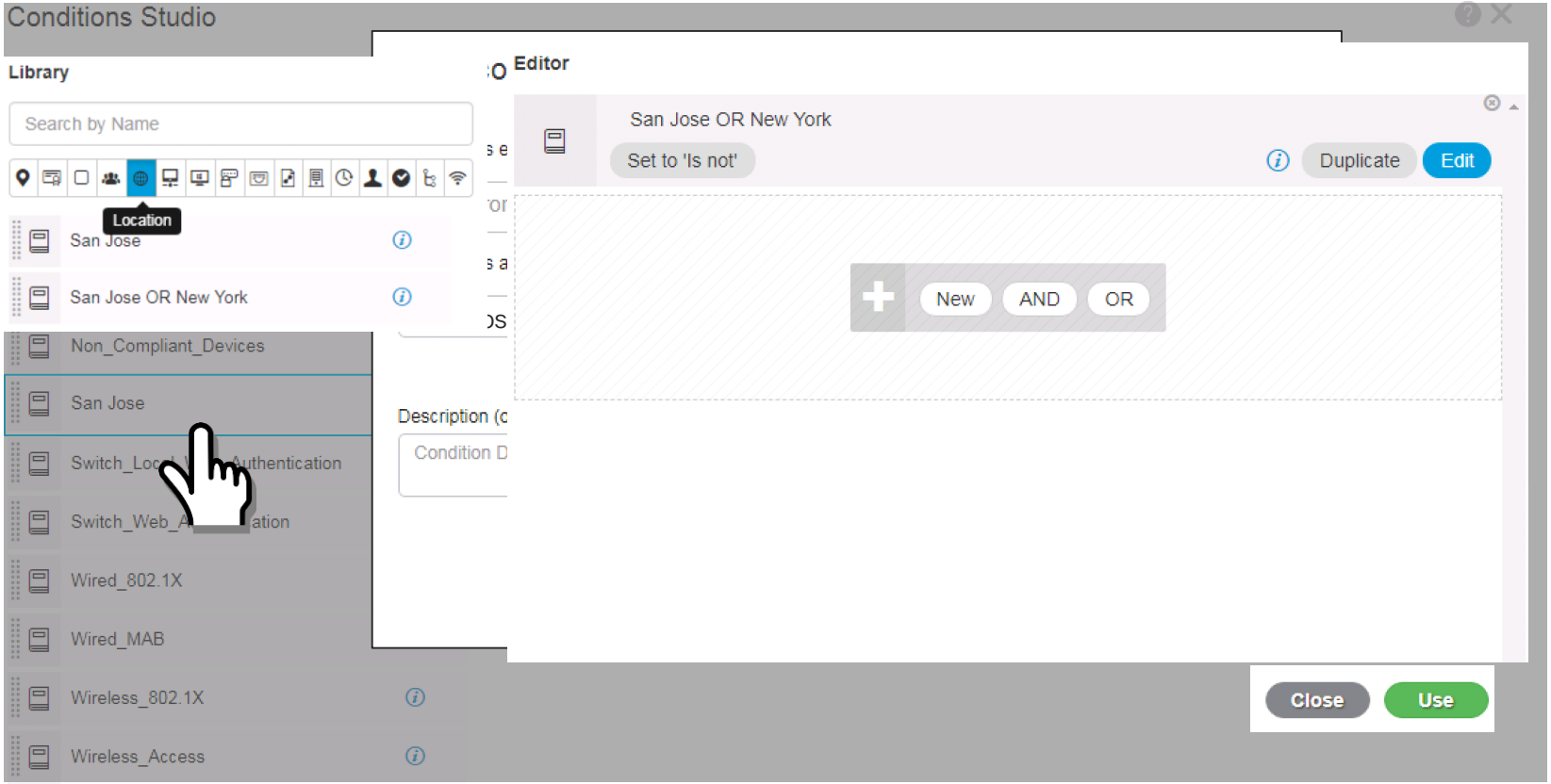
((Mobile_Devices | Workstation_Devices & SSID1) & US_West) |
((Mobile_Devices & SSID2) | (Workstation_Devices & ! SSID2) & US_East)

Simple Conditions

- SSID1
- SSID2
- Mobile_Devices
- Printer_Devices
- Workstation_Devices
- Anomalous_Behavior

First Things First – Build Common Conditions

Save with User-Friendly, Intuitive Names



ISE 2.4 Auth Policy Scale

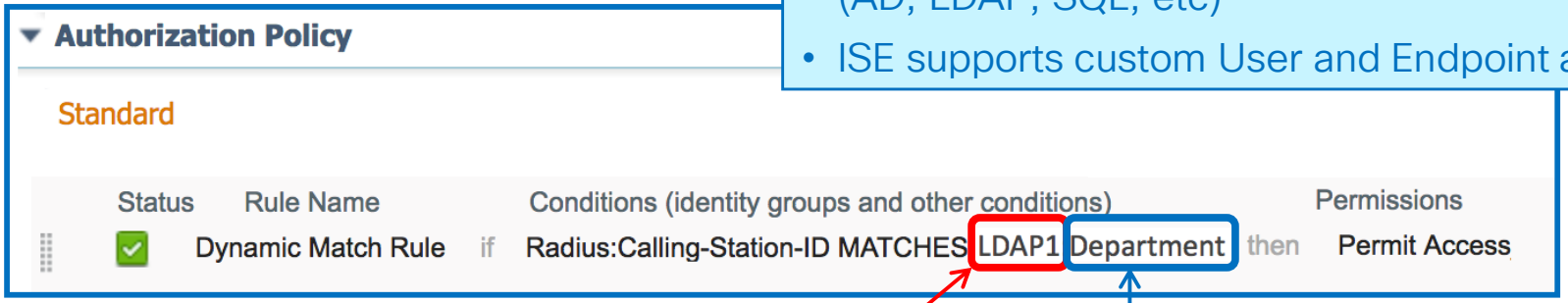
- Max Policy Sets = 200
  (up from 100 in 2.2; up from 40 in 2.1)
- Max Authentication Rules = 1000
  (up from 200 in 2.2; up from 100 in 2.1)
- Max Authorization Rules = 3000
  (up from 700 in 2.2; up from 600 in 2.1)
- Max Authorization Profiles = 3200
  (up from 1000 in 2.2; up from 600 in 2.1)

Dynamic Variable Substitution

Rule Reduction

- Match conditions to unique values stored per-User/Endpoint in internal or external ID stores (AD, LDAP, SQL, etc)
- ISE supports custom User and Endpoint attributes

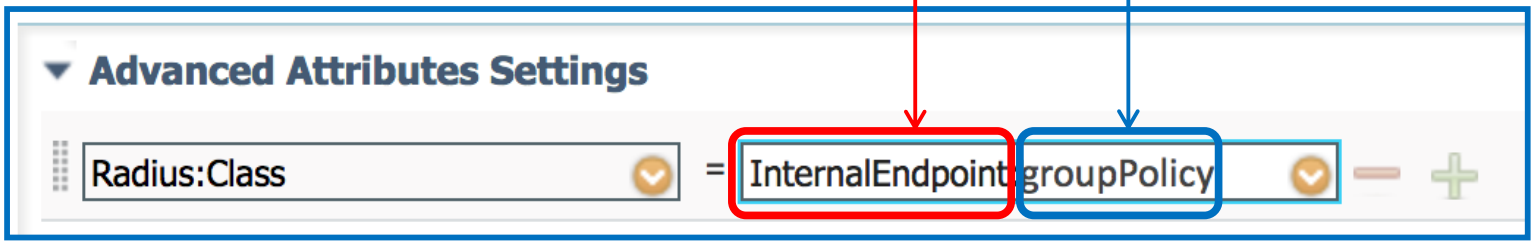
- Authorization Policy Conditions



ID Store

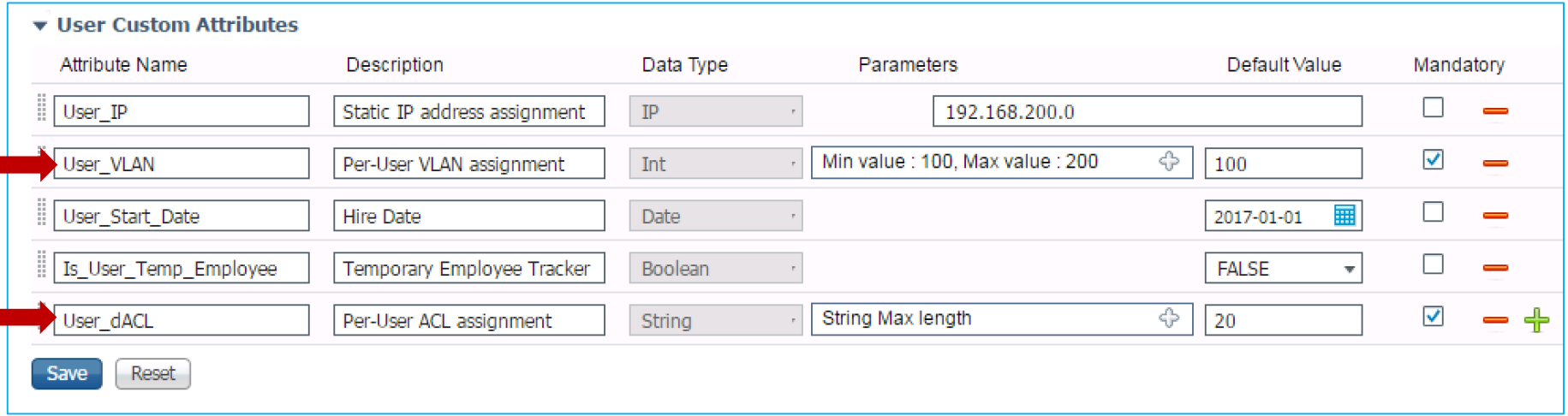
Attribute

- Authorization Profile Conditions



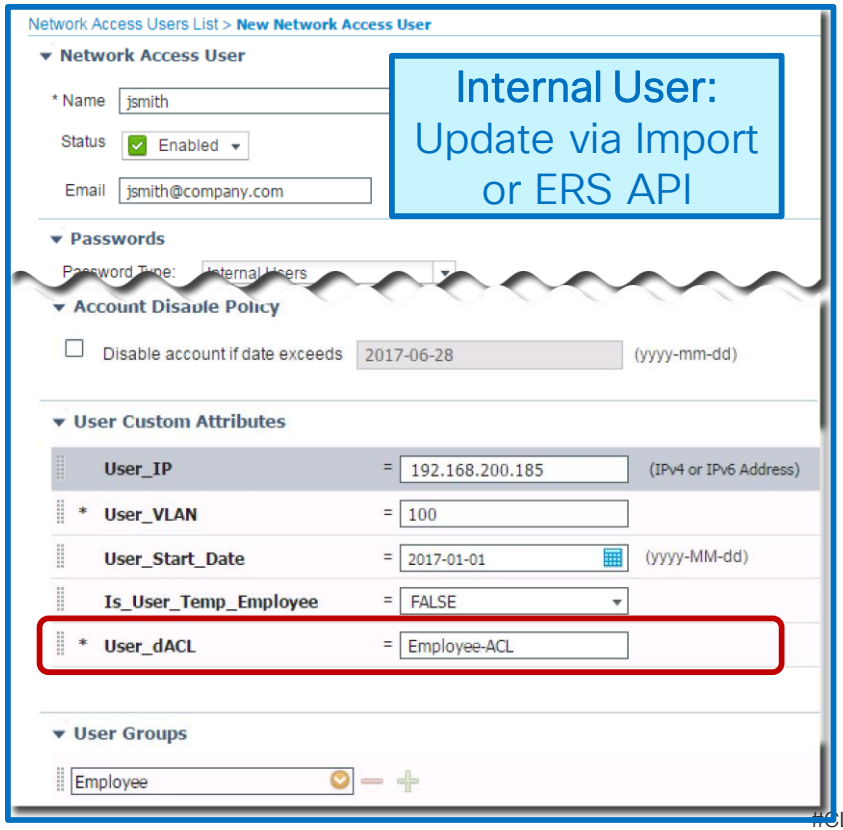
Dynamic Variable Substitution – Example

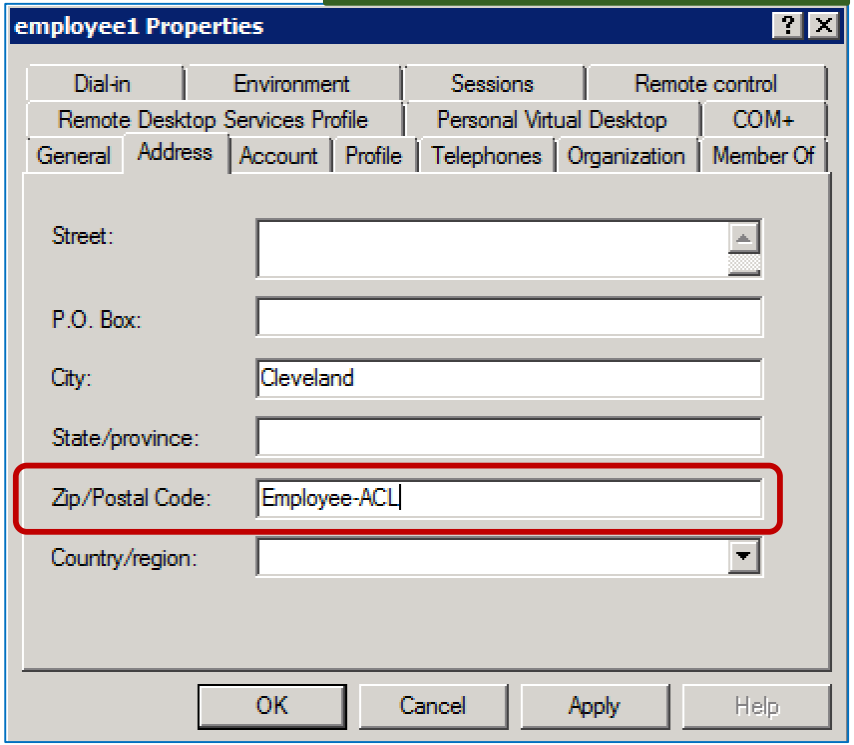
Define Custom User Attributes



Dynamic Variable Substitution – Example

Populate Internal or External User Account

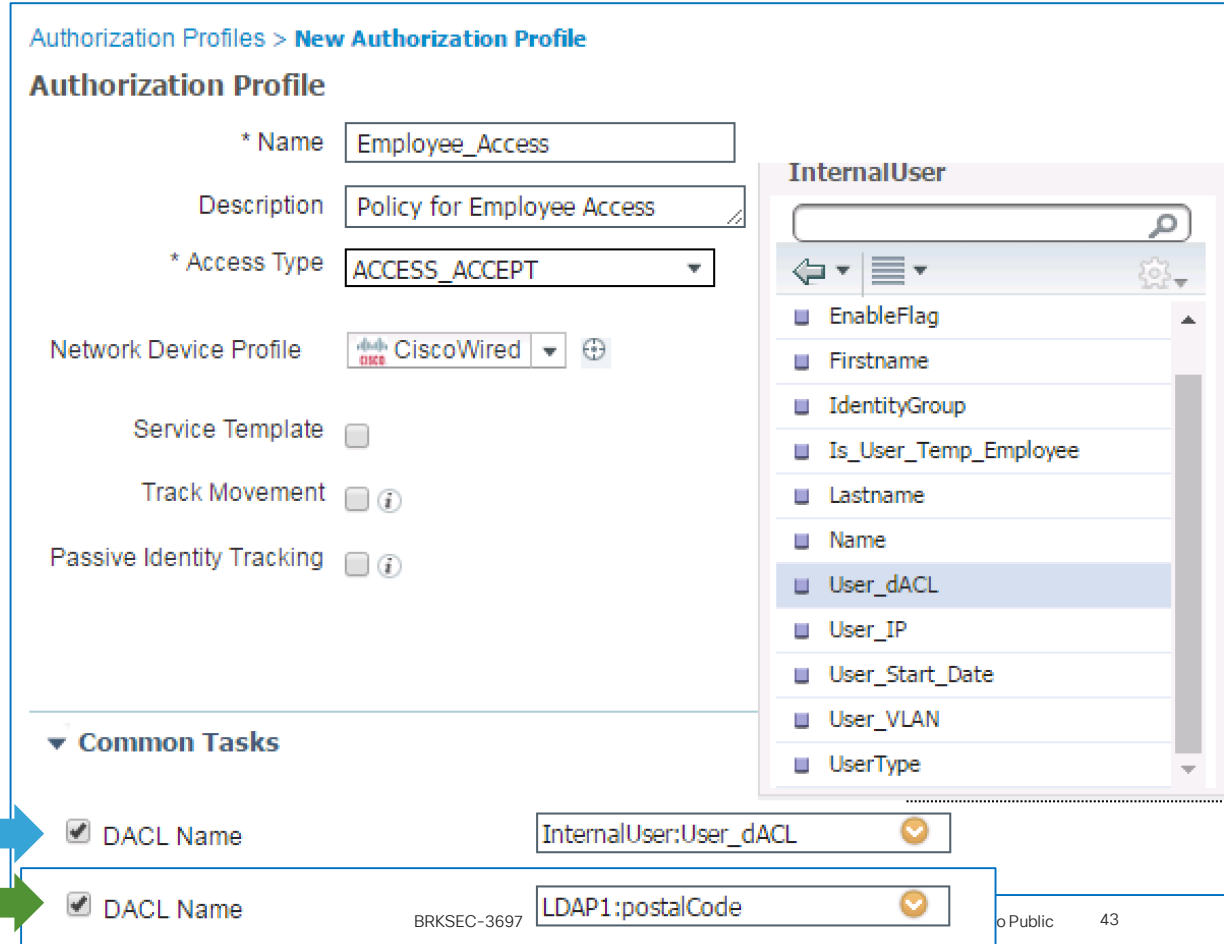




Dynamic DACL Values in Authorization Profile

Per-User Policy in 1 rule

1. Populate attribute in internal or external ID store.
2. Reference attribute in Authorization Profile under dACL



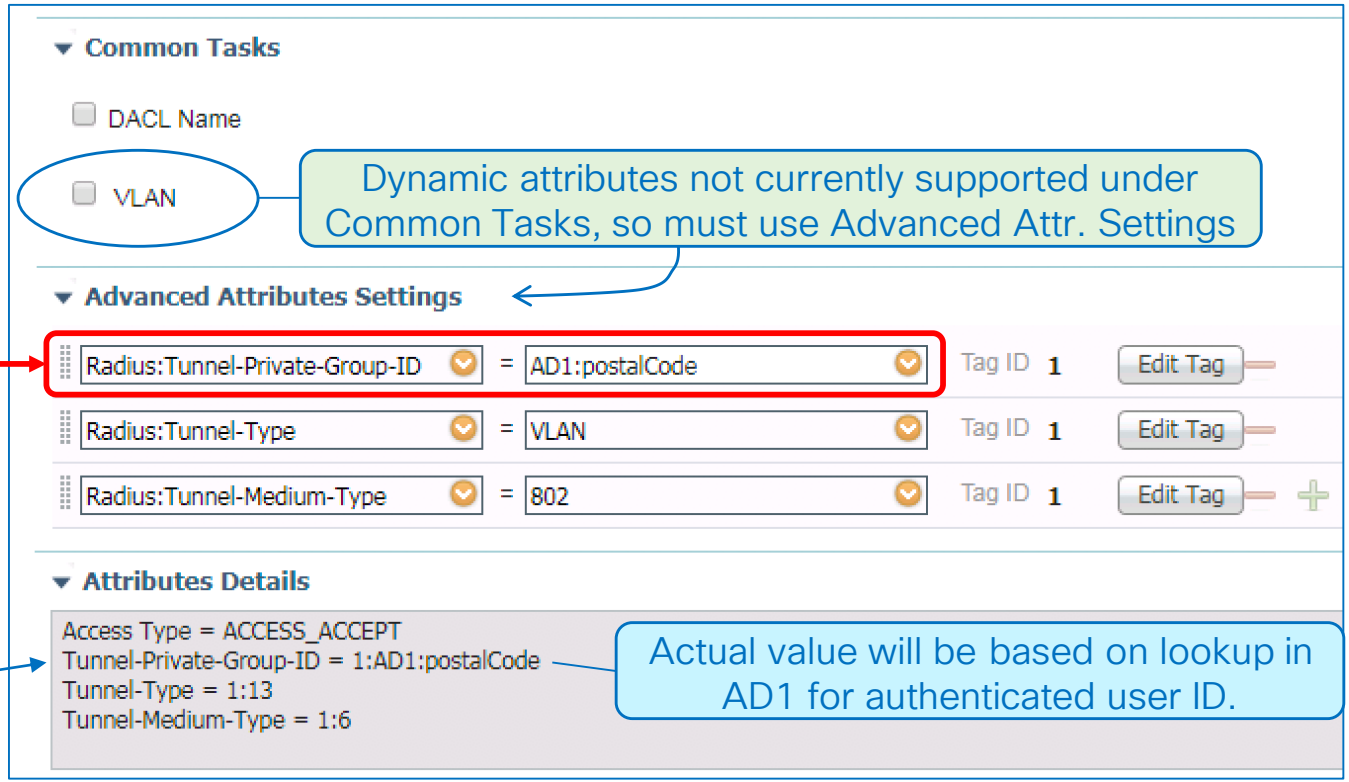
Internal User example

External User example

Dynamic VLAN Values in Authorization Profile

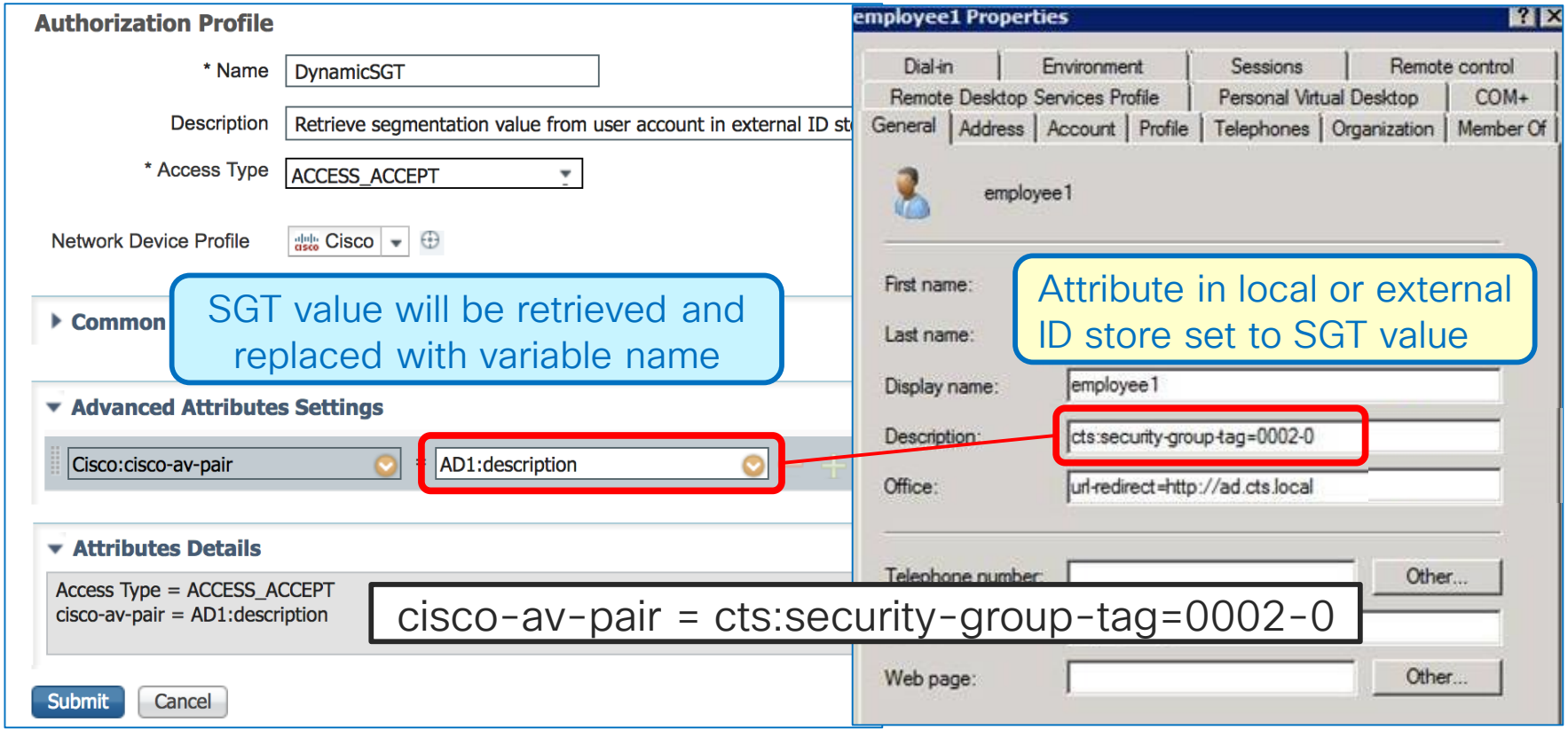
Per-User/Endpoint Policy in Single Authorization Rule

- Set VLAN number of name in unique attribute in local or external ID store.
- Ex: AD1:postalcode
- VLAN value will be retrieved and replaced with variable name:

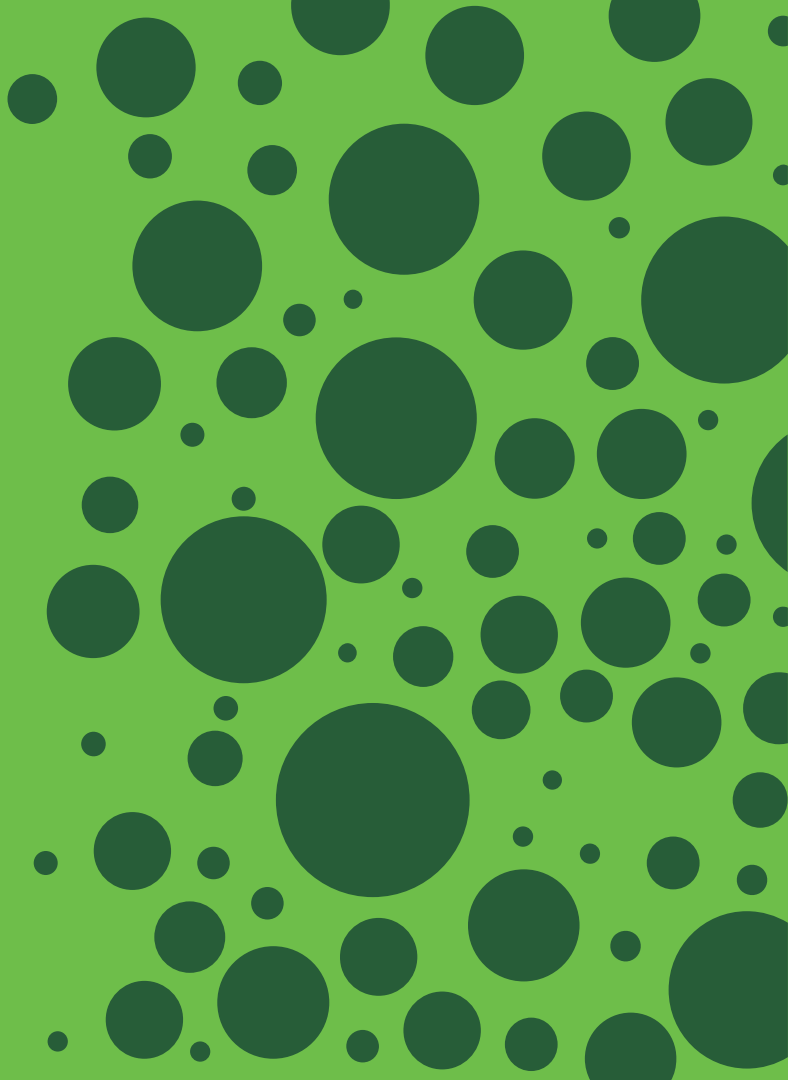


Dynamic Authorization for Security Group Tags

Segmentation Policy Based on Per-User/Device Attributes



Policy Trace – What If Analysis for Auth Policy



Session Trace (aka Policy Trace Tool)

What-If ISE Policy Tester

Three-Step Process:

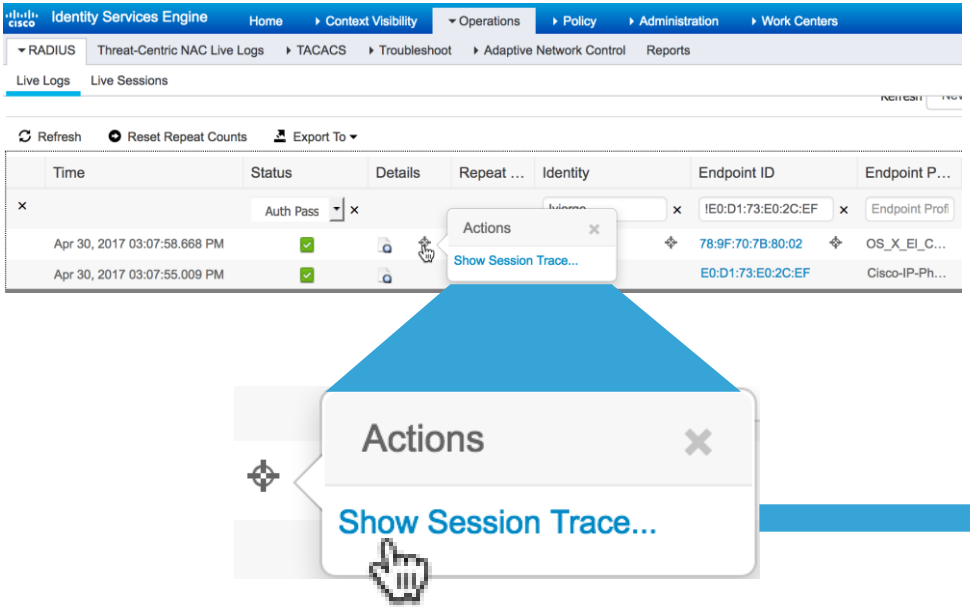
1. Build test policy 
2. Run test 
3. View and compare results 

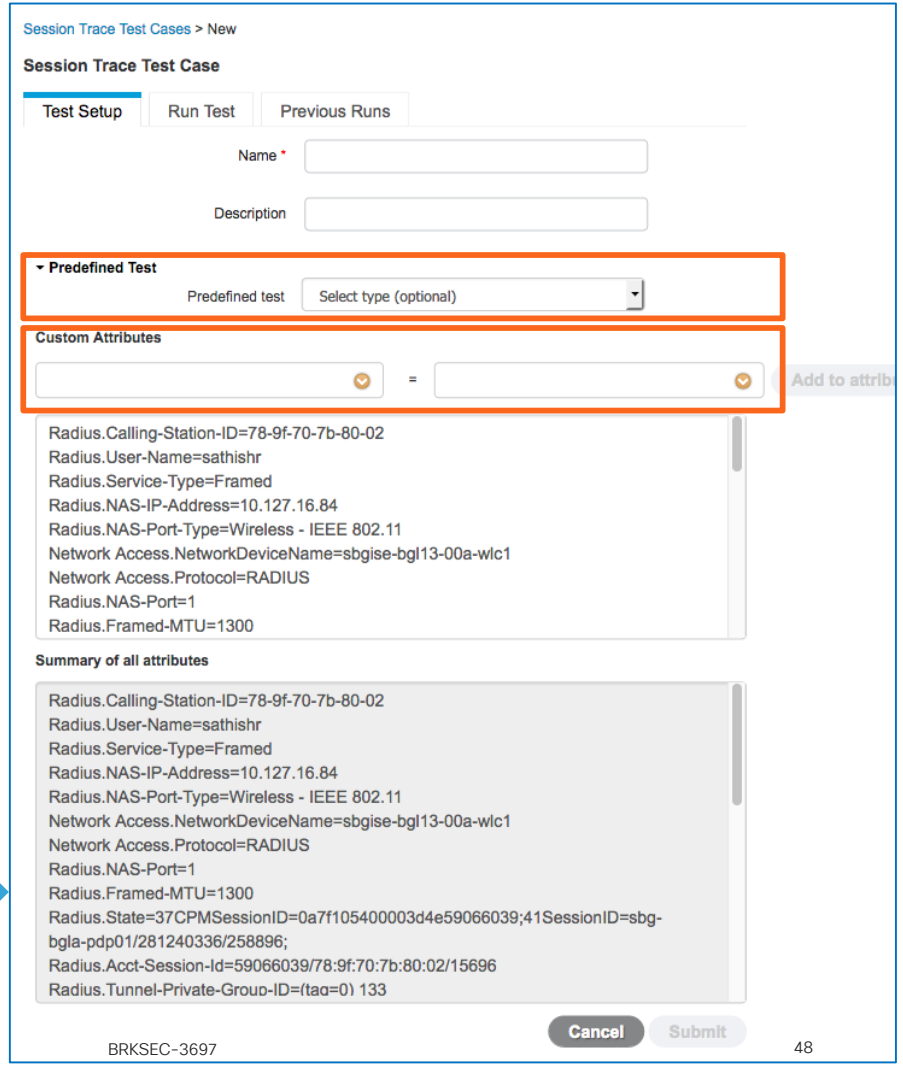
Test policy is run through same rules engine as real traffic, but completely simulated.

No actual endpoints or network devices required!

Build Test Policy

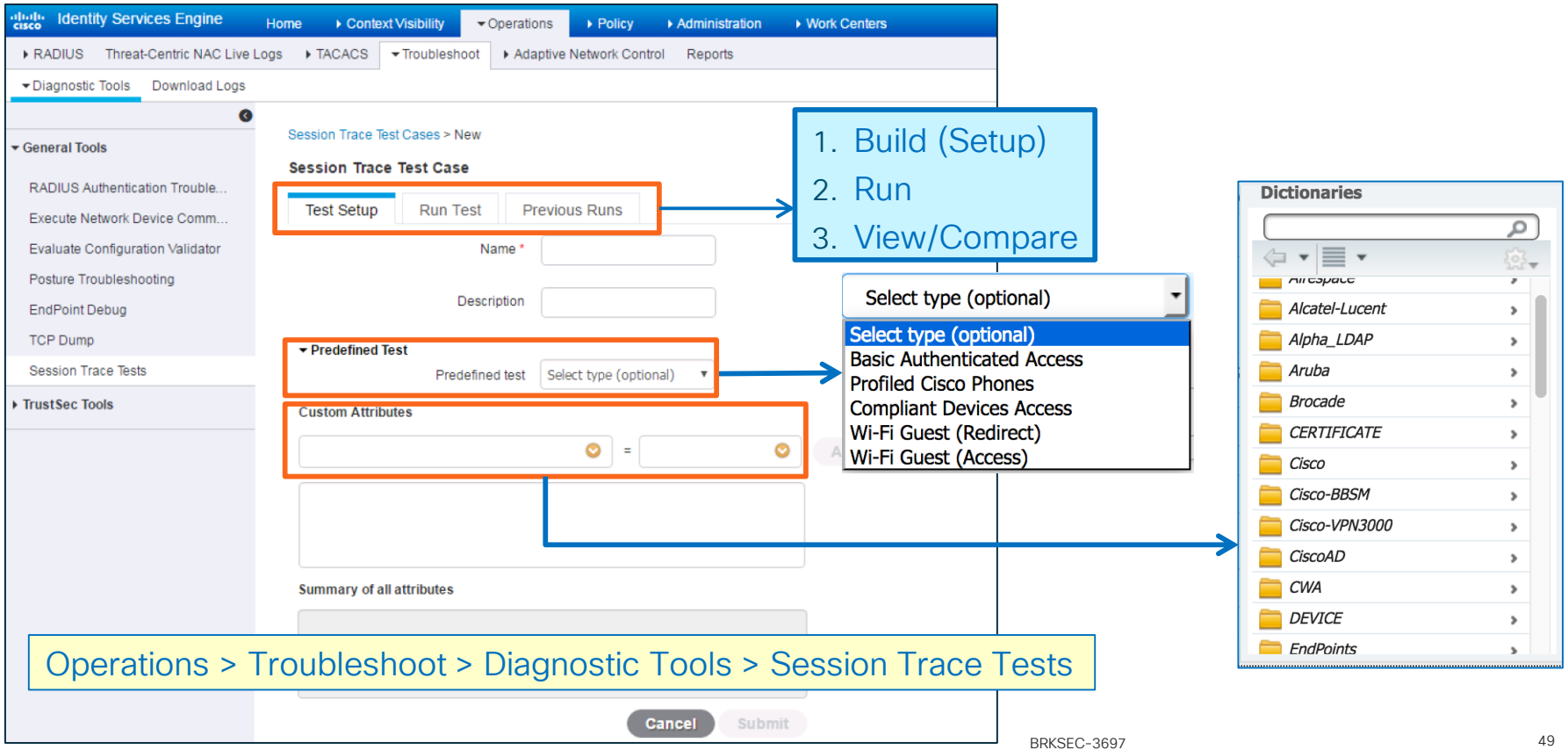
Option 1: Start with Existing Session





Build Test Policy

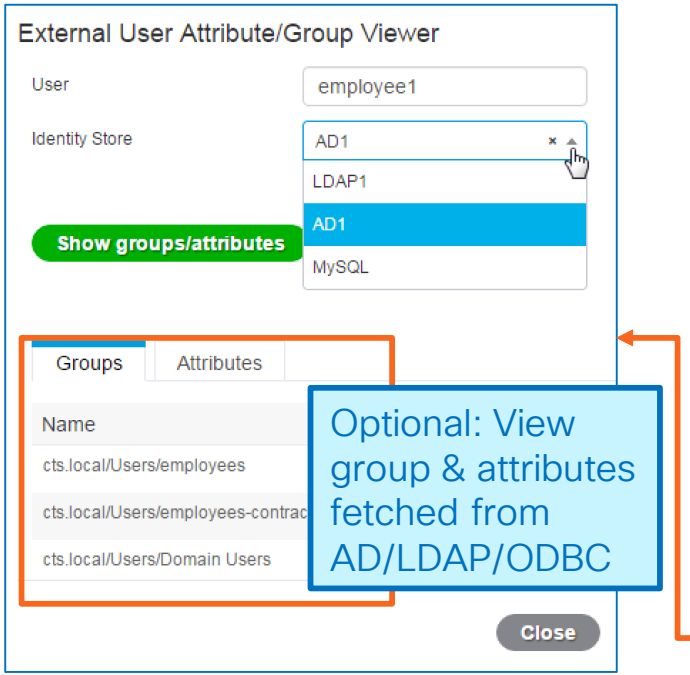
Option 2: Start from Scratch (Fully Custom Policy)



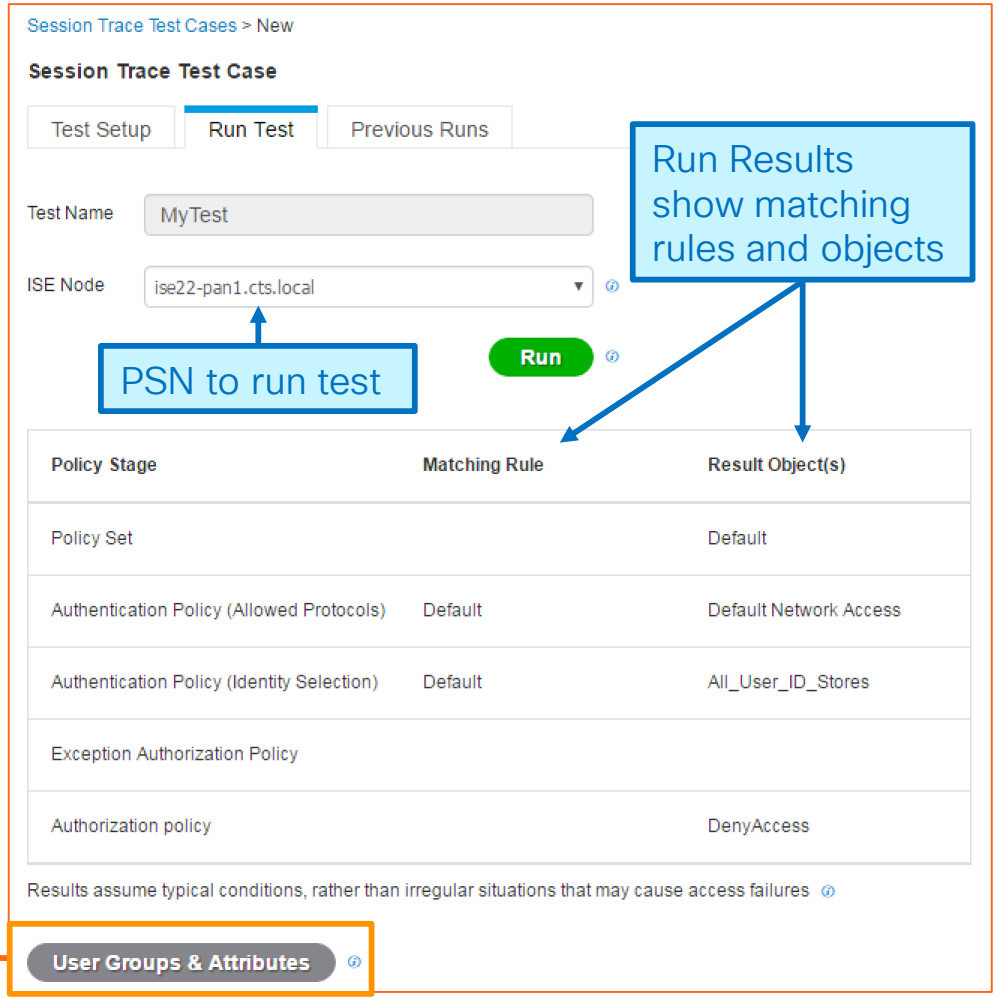
Session Trace

Run Test

- User Groups & Attributes



Optional: View group & attributes fetched from AD/LDAP/ODBC



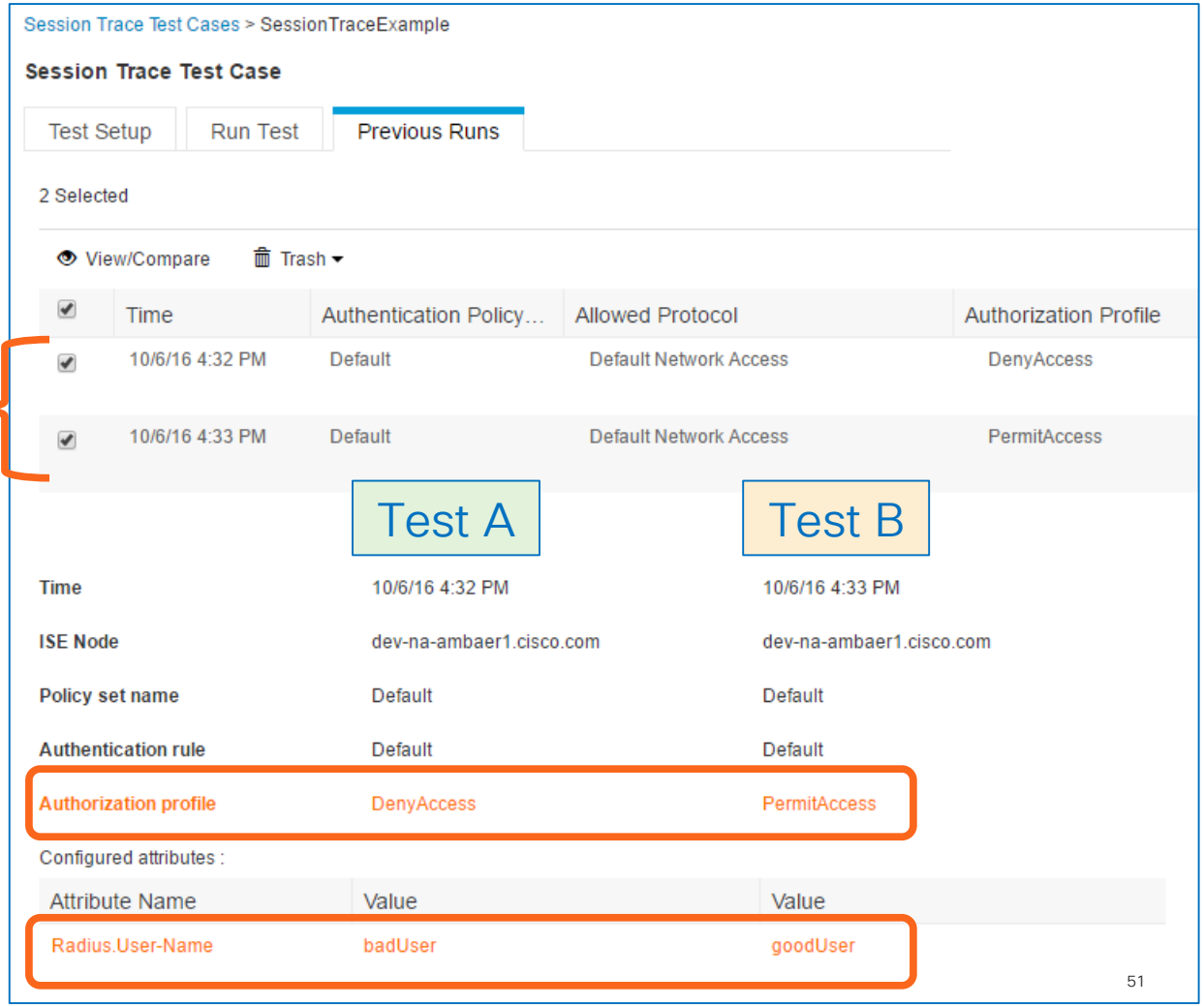
Run Results show matching rules and objects

PSN to run test

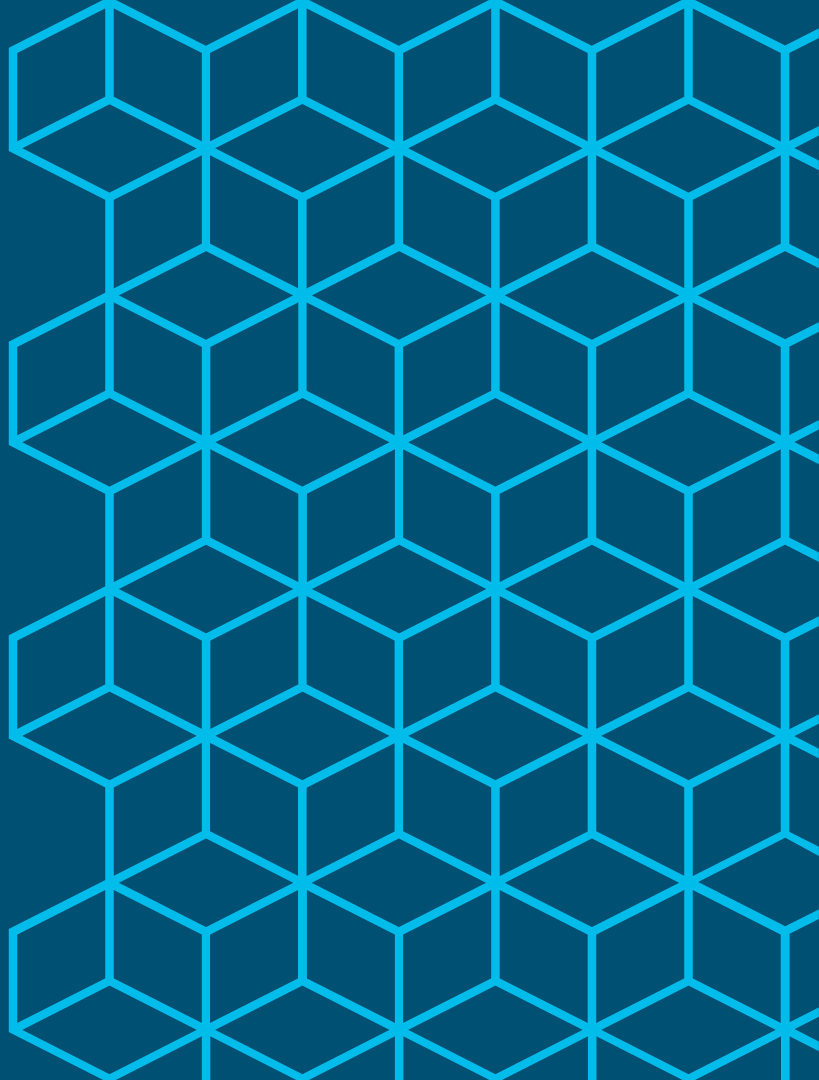
Session Trace

View and Compare Previous Test Runs

Select the previous runs to view and/or compare



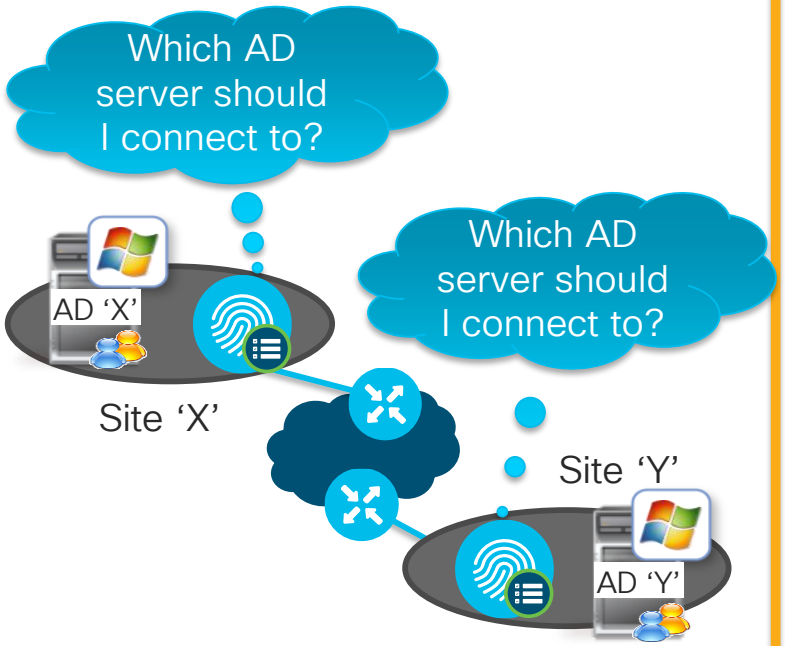
Tuning AD Integration



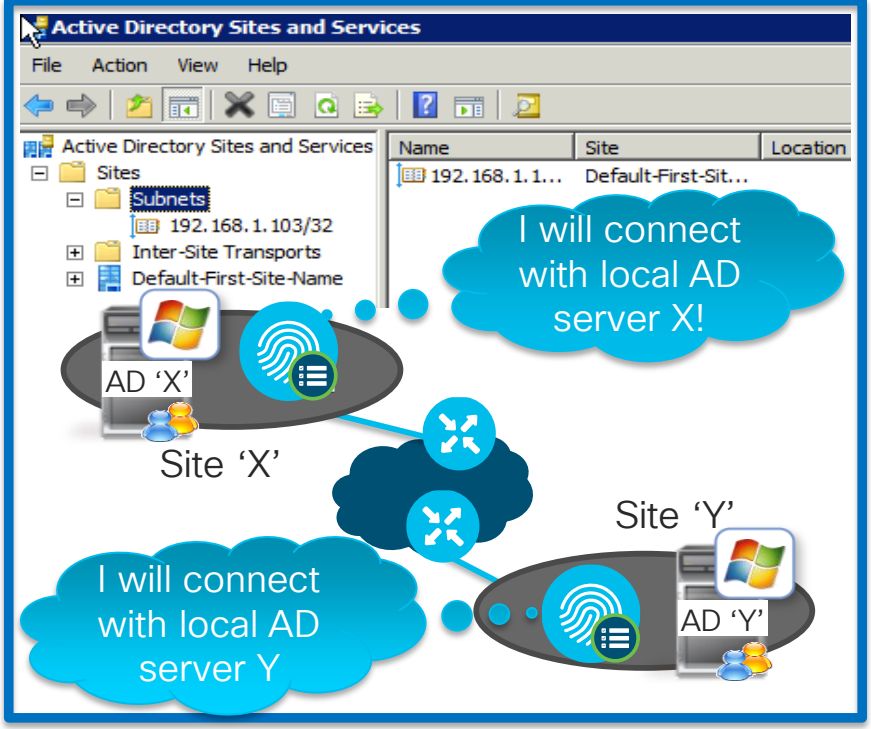
Scaling AD Integration w/Sites & Services

How do I ensure Local PSN is connecting to Local AD controller?

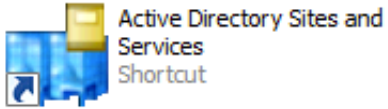
Without Site & Services



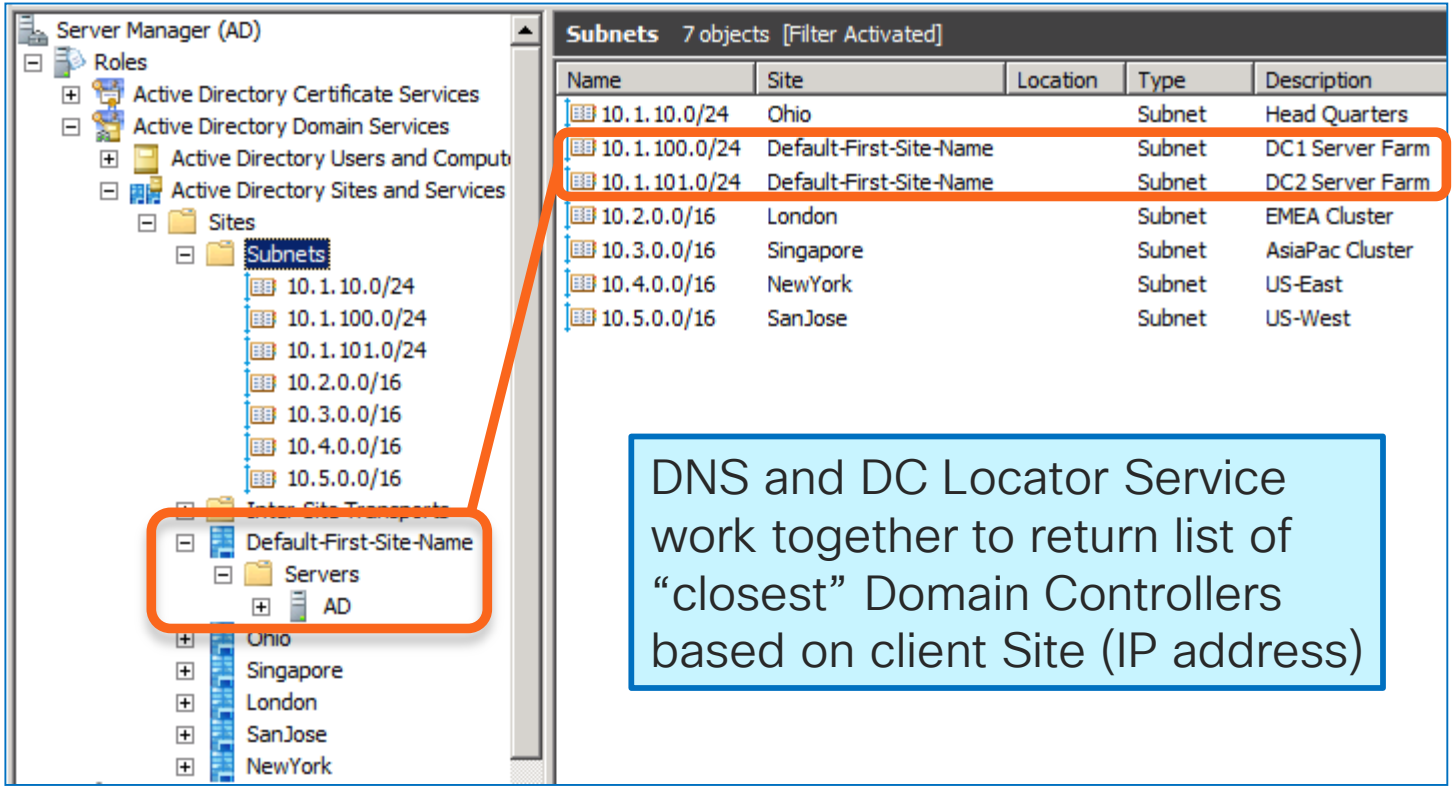
Properly Configured



AD Sites and Services



Links AD Domain Controllers to ISE Servers Based on IP Address

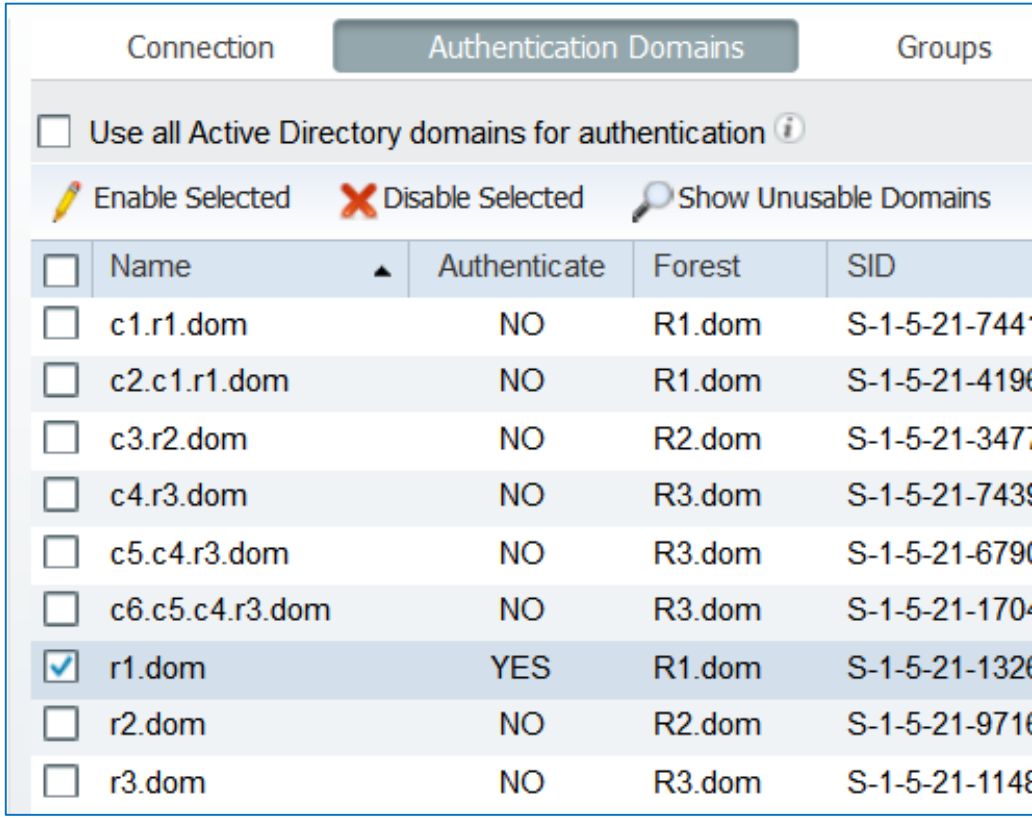


Authentication Domains (Whitelisting)

- "Whitelist" only the domains of interest—those used for authentication!
- In this example, the join point can see many trusted domains but we only care about r1.dom

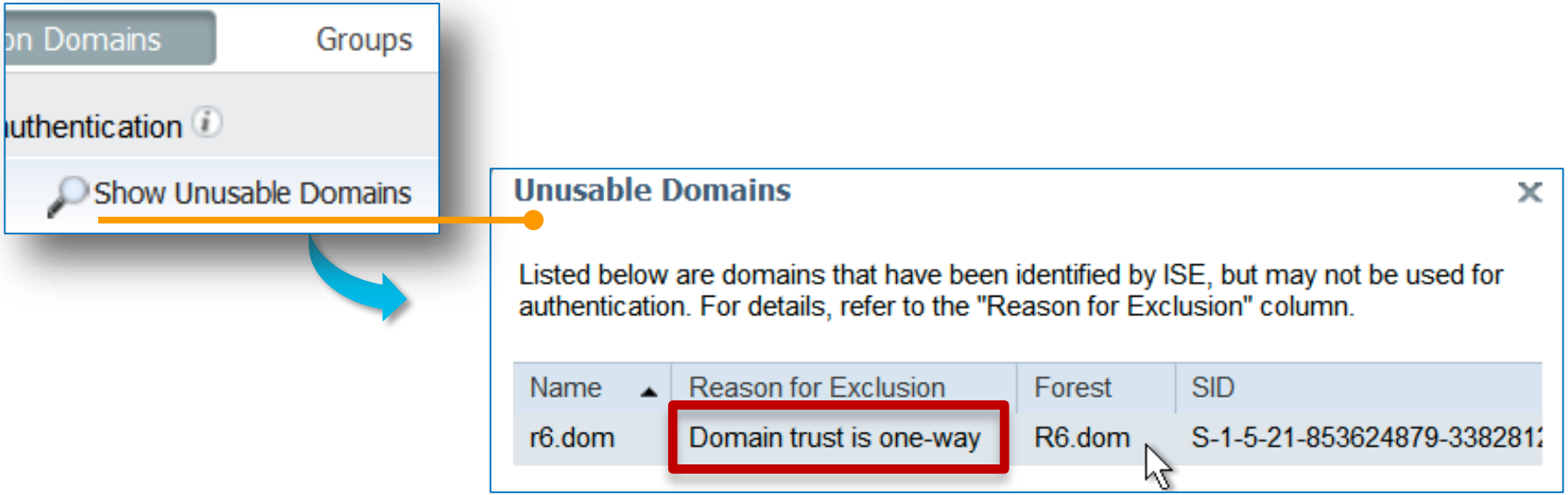
Enable r1.dom

And disable the rest



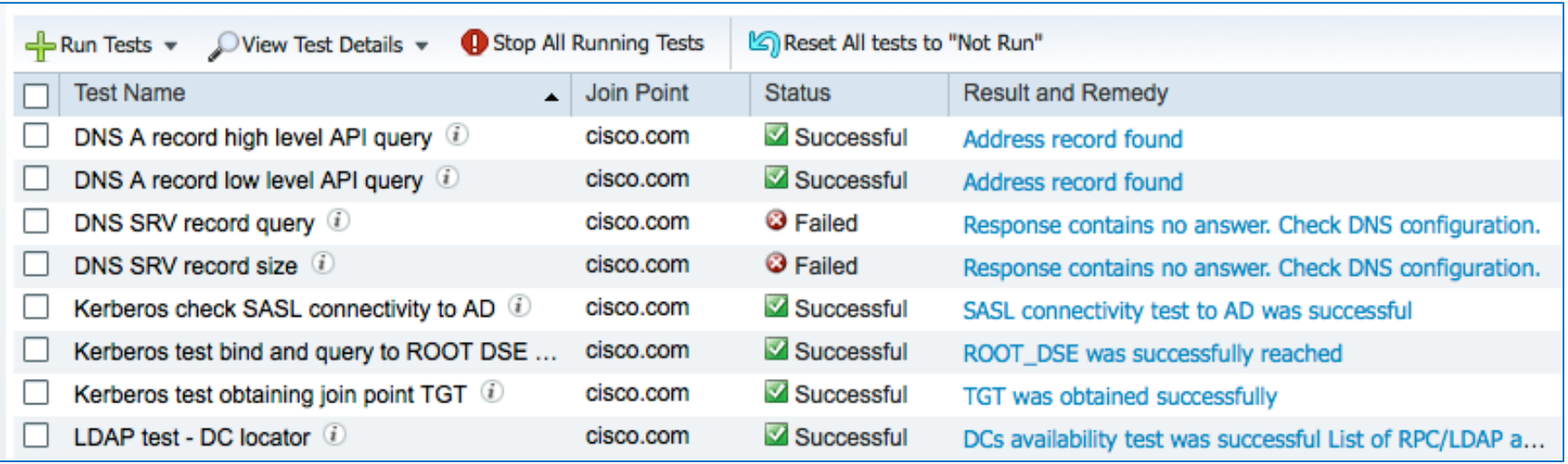
Authentication Domains – Unusable Domains

- Domains that are unusable, e.g. 1-way trusts, are hidden automatically
- There's an option to reveal these and see the reason



Run the AD Diagnostic Tool

Check AD Joins at Install & Periodically to Verify Potential AD Connectivity Issues



Test Name	Join Point	Status	Result and Remedy
DNS A record high level API query	cisco.com	Successful	Address record found
DNS A record low level API query	cisco.com	Successful	Address record found
DNS SRV record query	cisco.com	Failed	Response contains no answer. Check DNS configuration.
DNS SRV record size	cisco.com	Failed	Response contains no answer. Check DNS configuration.
Kerberos check SASL connectivity to AD	cisco.com	Successful	SASL connectivity test to AD was successful
Kerberos test bind and query to ROOT DSE ...	cisco.com	Successful	ROOT_DSE was successfully reached
Kerberos test obtaining join point TGT	cisco.com	Successful	TGT was obtained successfully
LDAP test - DC locator	cisco.com	Successful	DCs availability test was successful List of RPC/LDAP a...

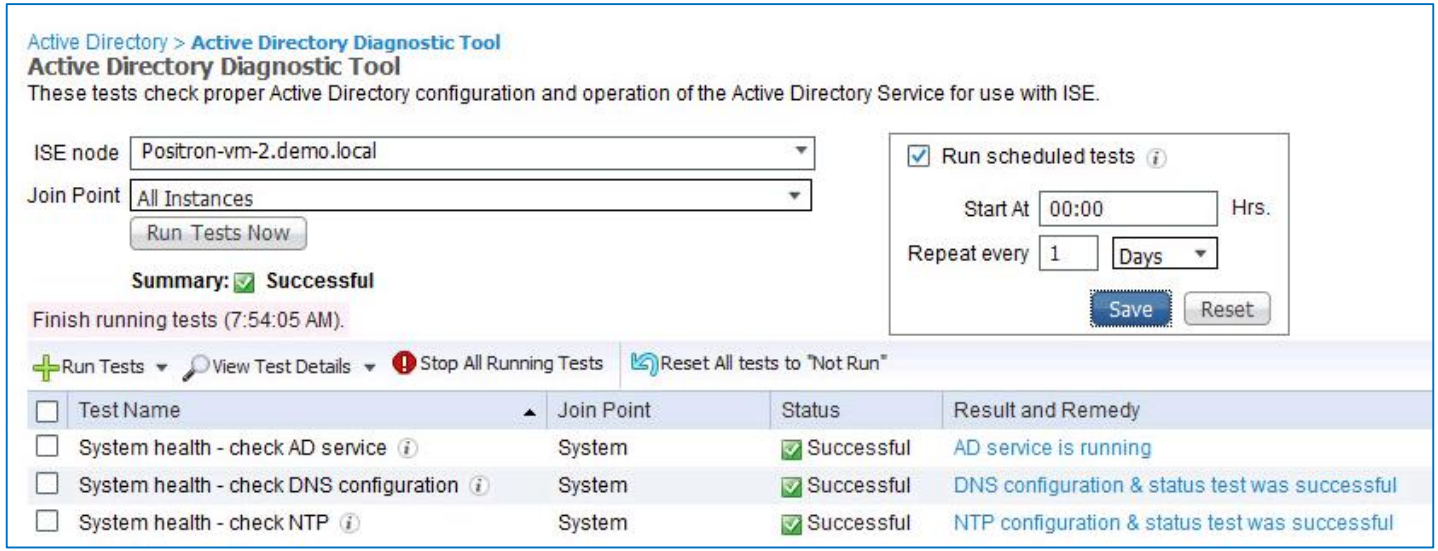
- The DNS SRV errors can actually mean something else
  - The response was too big...and retried with TCP, etc.
  - A sniffer can confirm
  - AD Sites or DNS configuration changes are required to get that optimized

AD Background Diagnostics

Schedule Periodic Testing to Verify AD Connectivity and Health

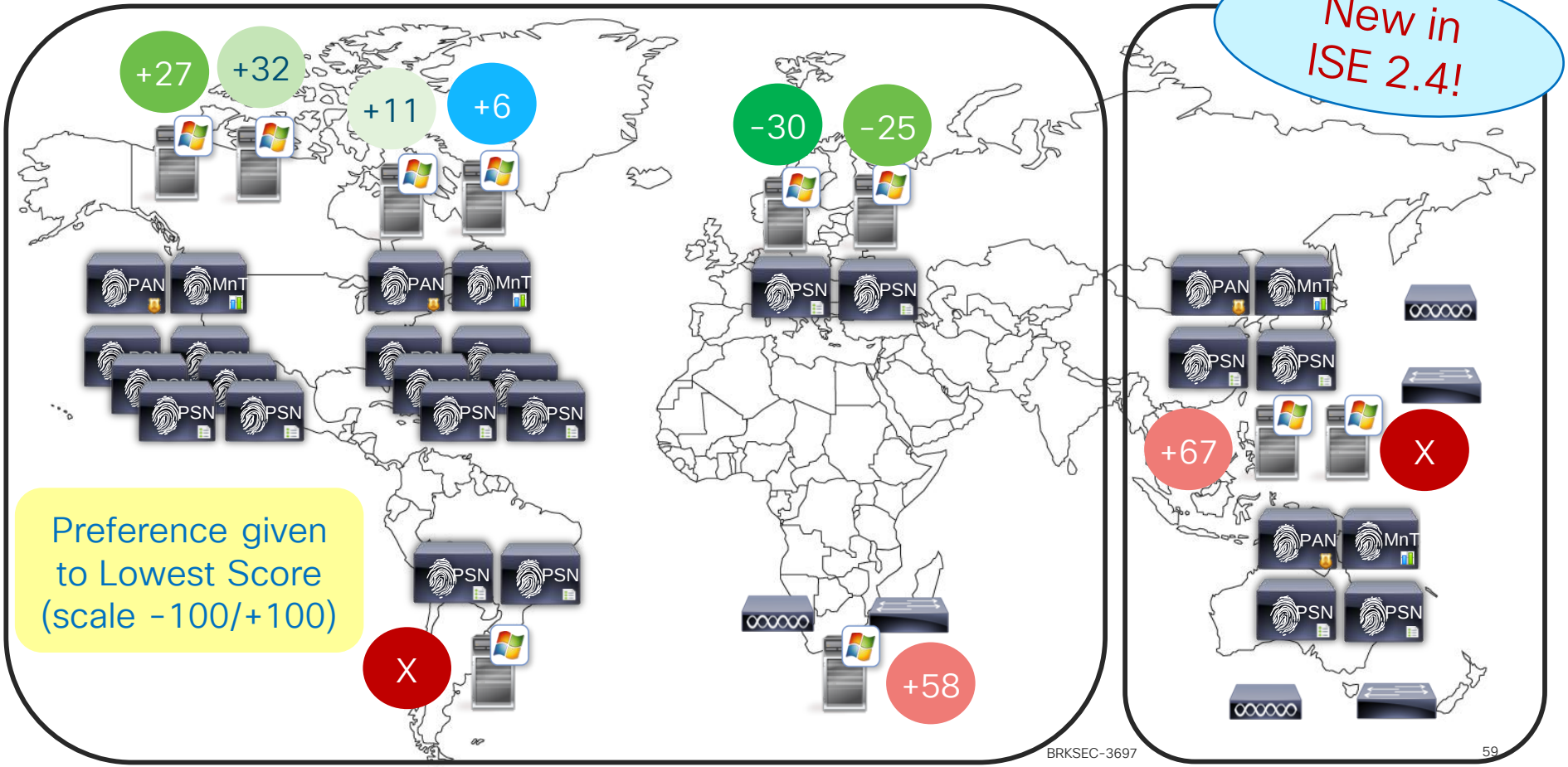
New in ISE 2.4!

- AD diagnostic tests run in the background without interrupting user auth
  - Scheduled to daily at 00:00, by default
  - Alarm is fired if test fails



Enhanced AD Domain Controller Management and Failover

Preferred DC Based on Scoring System



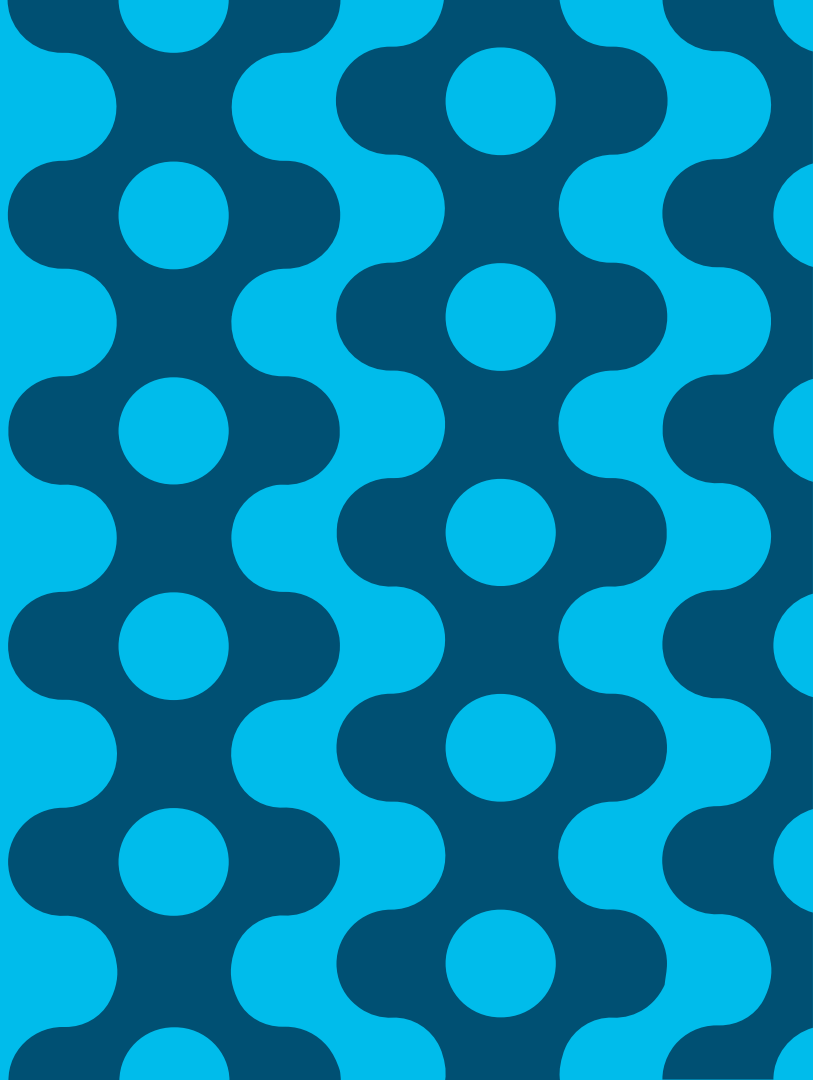
AD Integration Best Practices

BRKSEC-2132 What's new in ISE Active Directory Connector (CiscoLive.com/online) -Chris Murray

- DNS servers in ISE nodes must have all relevant AD records (A, PTR, SRV)
- Ensure NTP configured for all ISE nodes and AD servers
- Configure AD Sites and Services
  (with ISE machine accounts configured for relevant Sites)
- Configure Authentication Domains (Whitelist domains used) (ISE 1.3)
- Use UPN/fully qualified usernames when possible to expedite use lookups
- Use AD indexed attributes* when possible to expedite attribute lookups
- Run *Scheduled* Diagnostics from ISE Admin interface to check for issues.

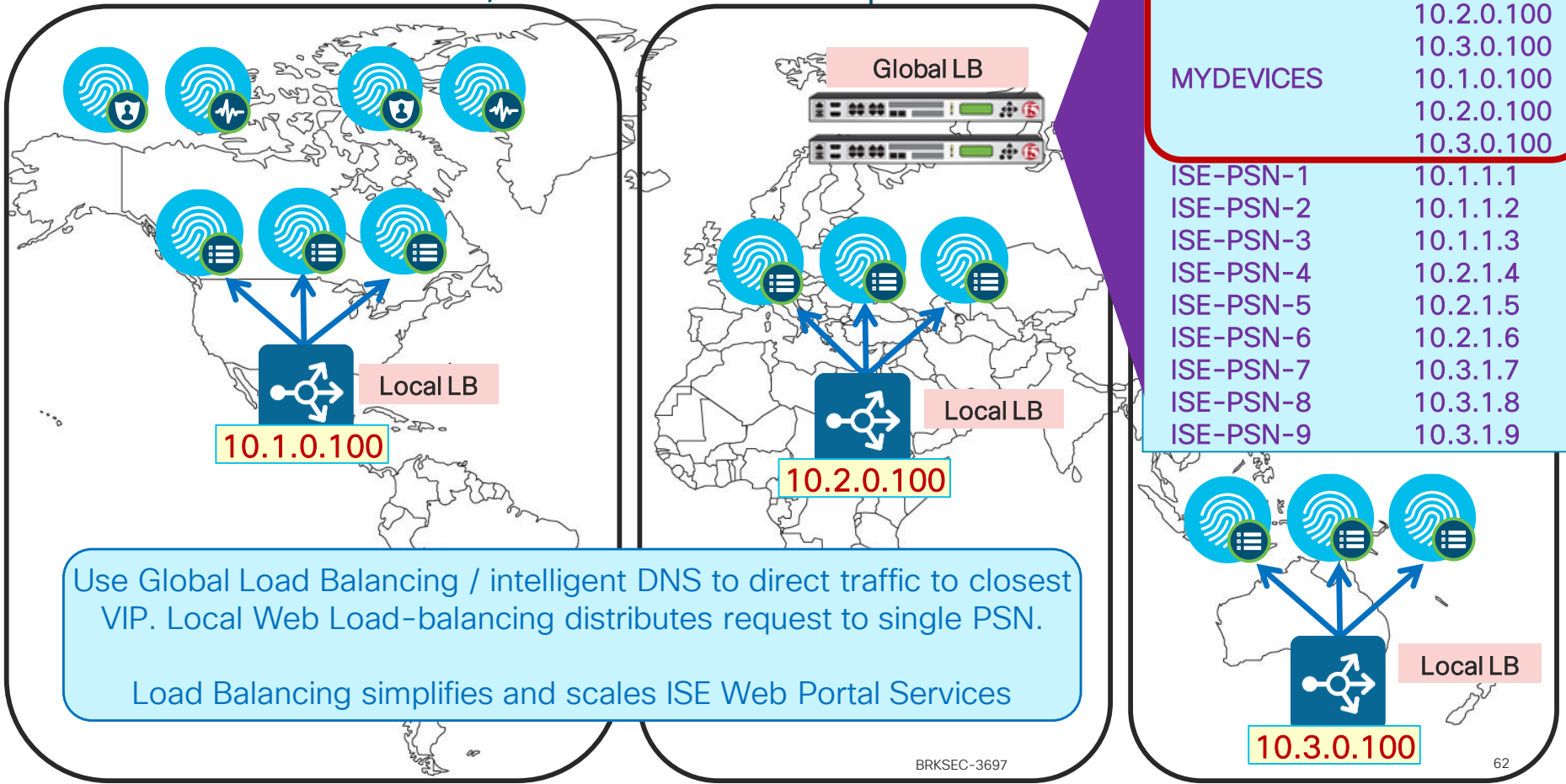
* Microsoft AD Indexed Attributes:
  http://msdn.microsoft.com/en-us/library/ms675095%28v=vs.85%29.aspx
  http://technet.microsoft.com/en-gb/library/aa995762%28v=exchg.65%29.aspx

Guest and Web Authentication Services



Single URL for Sponsors/MyDevices

Global Load Balancers / “Smart DNS” Example



DNS SERVER: DOMAIN = COMPANY.COM

SPONSOR	10.1.0.100
	10.2.0.100
	10.3.0.100
MYDEVICES	10.1.0.100
	10.2.0.100
	10.3.0.100
ISE-PSN-1	10.1.1.1
ISE-PSN-2	10.1.1.2
ISE-PSN-3	10.1.1.3
ISE-PSN-4	10.2.1.4
ISE-PSN-5	10.2.1.5
ISE-PSN-6	10.2.1.6
ISE-PSN-7	10.3.1.7
ISE-PSN-8	10.3.1.8
ISE-PSN-9	10.3.1.9

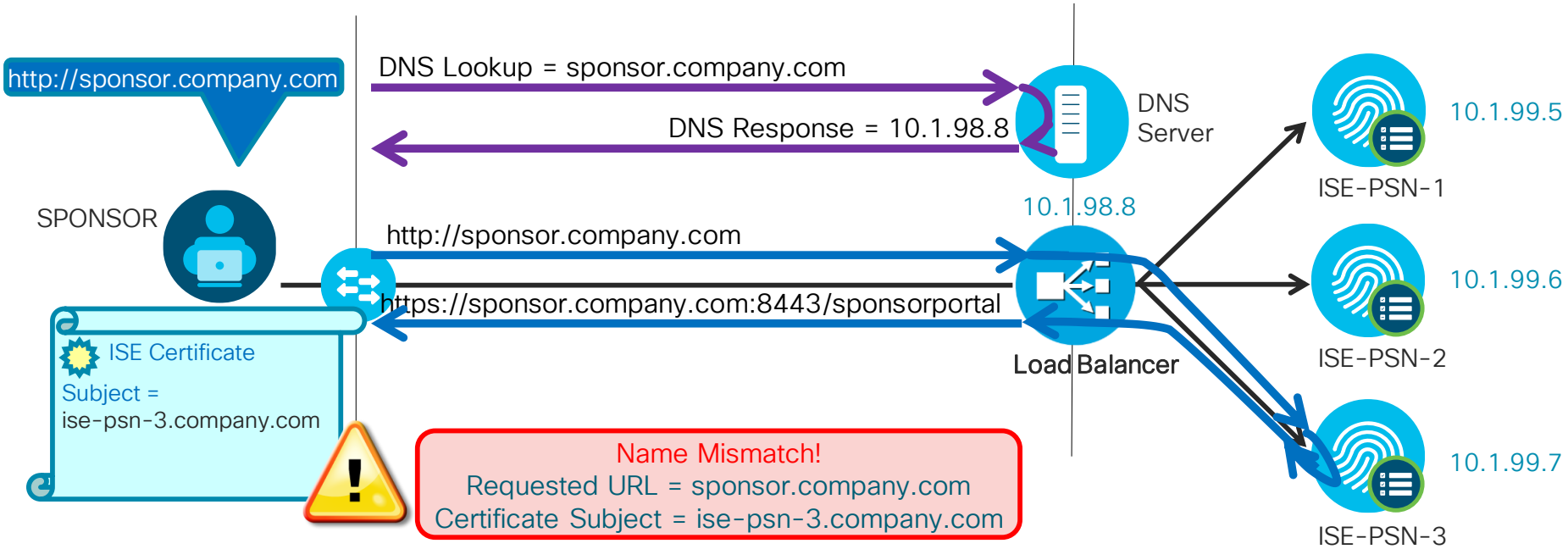
Use Global Load Balancing / intelligent DNS to direct traffic to closest VIP. Local Web Load-balancing distributes request to single PSN.

Load Balancing simplifies and scales ISE Web Portal Services

ISE Certificate without SAN

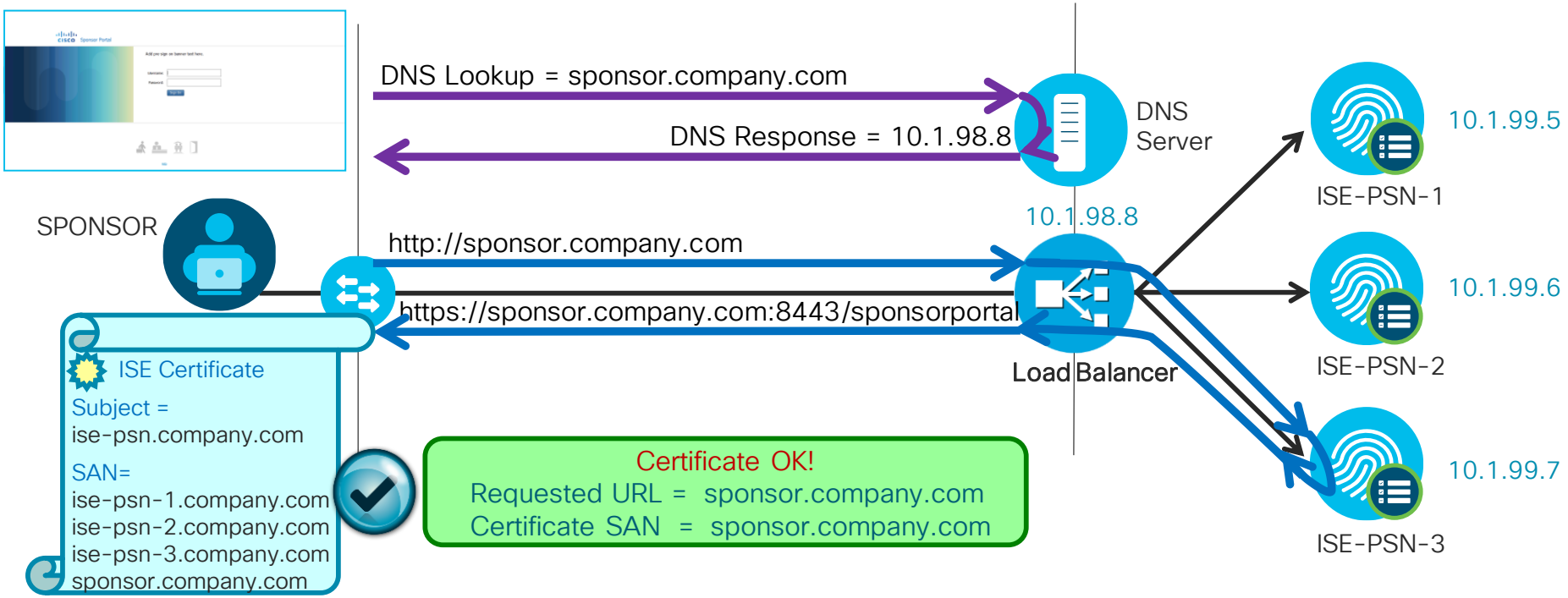
Certificate Warning - Name Mismatch

ISE Web Services: Sponsor, Guest, My Devices, CWA, Hotspot, Posture, Client Provisioning, MDM, BYOD, Cert



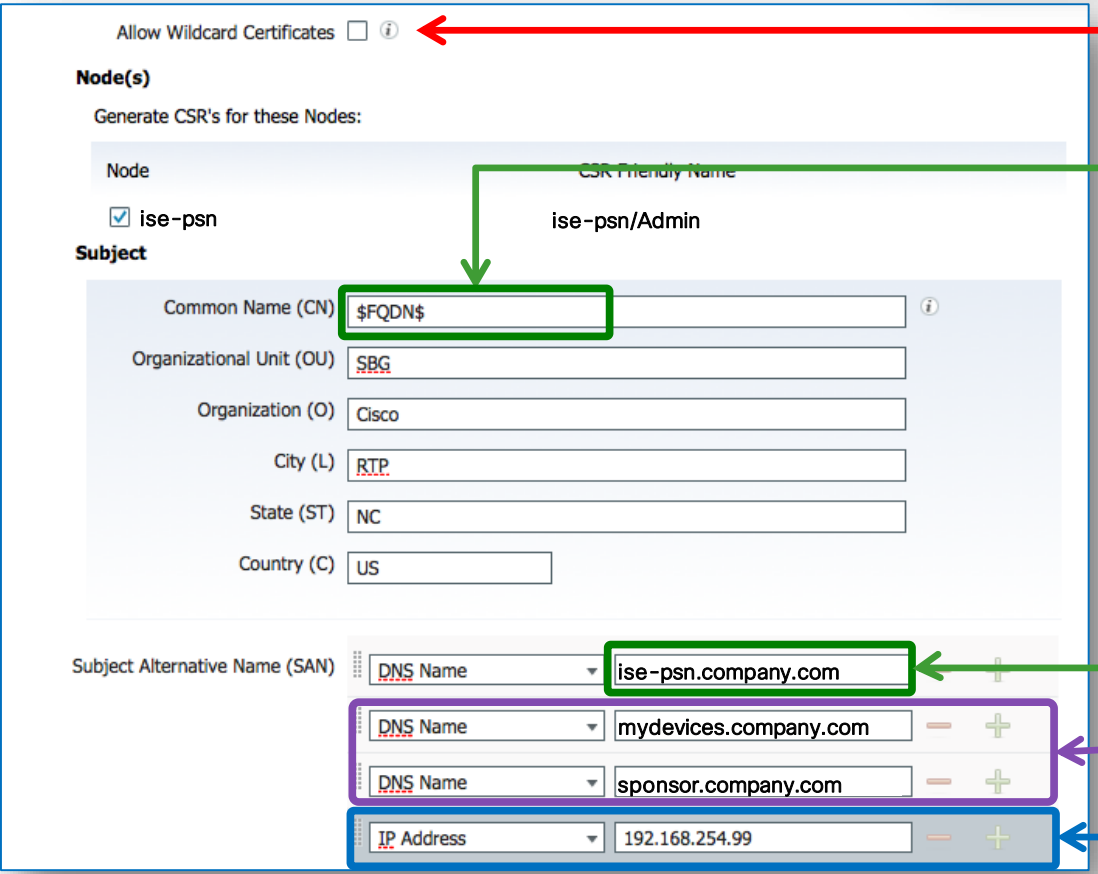
ISE Certificate with SAN

No Certificate Warning



“Universal Certs”

UCC or Wildcard SAN Certificates



Check box to use wildcards

CN must also exist in SAN

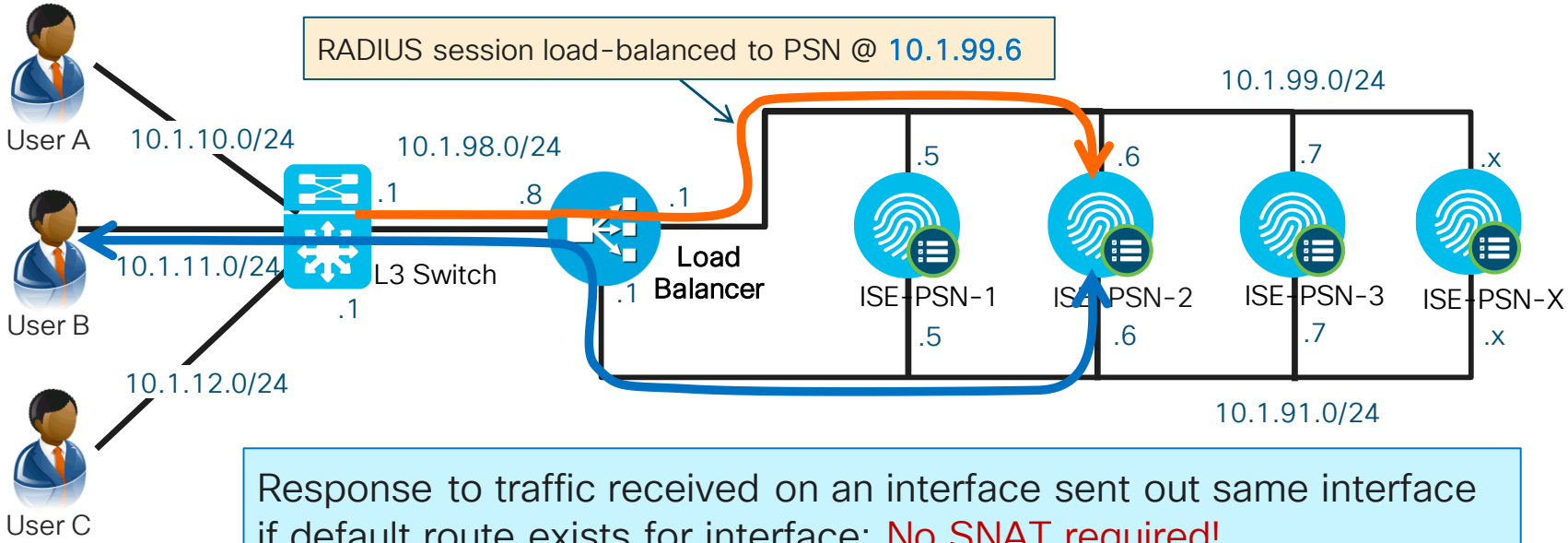
Universal Cert options:
- UCC / Multi-SAN
- Wildcard SAN

Other FQDNs or wildcard as “DNS Names”

IP Address is also option

Dedicated Web Interfaces

Direct Access and URL-Redirected Traffic with Dedicated PSN Web Interfaces



Response to traffic received on an interface sent out same interface if default route exists for interface: No SNAT required!

Default route 0.0.0.0/0 10.1.99.1 eth0
Default route 0.0.0.0/0 10.1.91.1 eth1

Dedicated Web Interfaces

Symmetric Traffic Flows

- Configure default routes for each interface to support symmetric return traffic

```
ise24-psn-x/admin# config t
Enter configuration commands, one per line.  End with CNTL/Z.
ise13-psn-x/admin(config)#  ip route 0.0.0.0 0.0.0.0 gateway 10.1.91.1
```

- Validate new default route

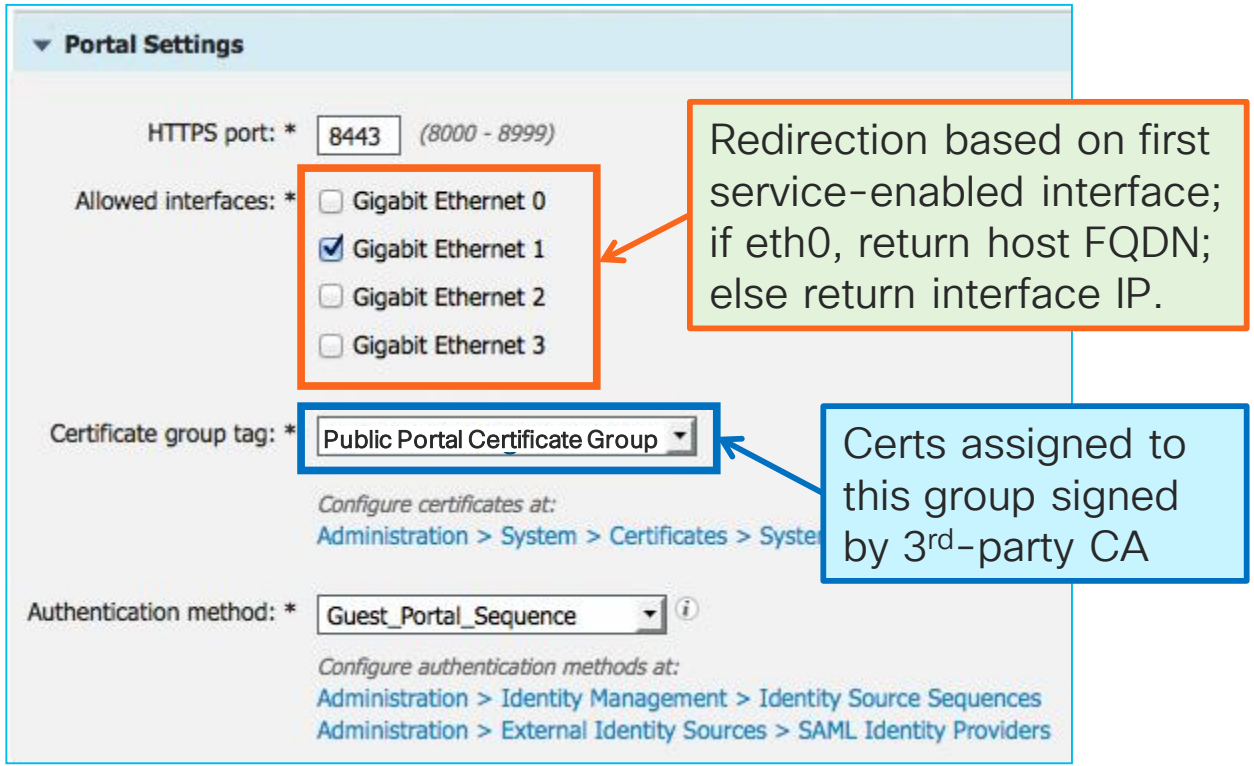
```
ise24-psn-x/admin# sh ip route

Destination          Gateway              Iface
-----------          -------              -----
10.1.91.0/24         0.0.0.0              eth1
10.1.99.0/24         0.0.0.0              eth0
default              10.1.91.1            eth1
default              10.1.99.1            eth0
```

What is default route for outbound connections when multiple default routes configured?

ISE 1.3/1.4: Round-robin
ISE 2.0: ip default-gateway

Use Publicly-Signed Certs for Guest Portals!

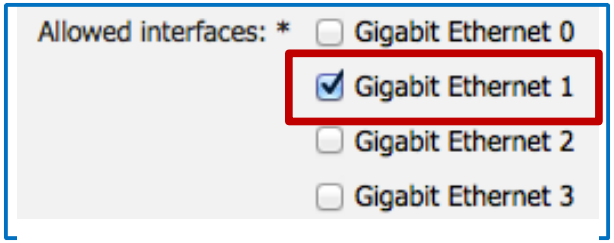
- Starting in ISE 1.3, HTTPS cert for Admin can be different from web portals
- Guest portals can use a different, public certificate
- Admin and internal employee portals (or EAP) can still use certs signed by private CA.



Secondary Interface – CWA Example

DNS & Port Settings–Single Non-Management Interface Enabled for Guest Portal

- CWA Guest Portal access for ISE-PSN-1 configured for eth1



- IP Address for eth1 on ISE-PSN-1 is 10.1.91.5

ISE Node	IP Address	Interface
ISE-PSN-1	10.1.99.5	# eth0
ISE-PSN-1	10.1.91.5	# eth1
ISE-PSN-1	10.1.92.5	# eth2
ISE-PSN-1	10.1.93.5	# eth3
ISE-PSN-1	10.1.94.5	# eth4
ISE-PSN-1	10.1.95.5	# eth5

- Authorization for URL Redirect

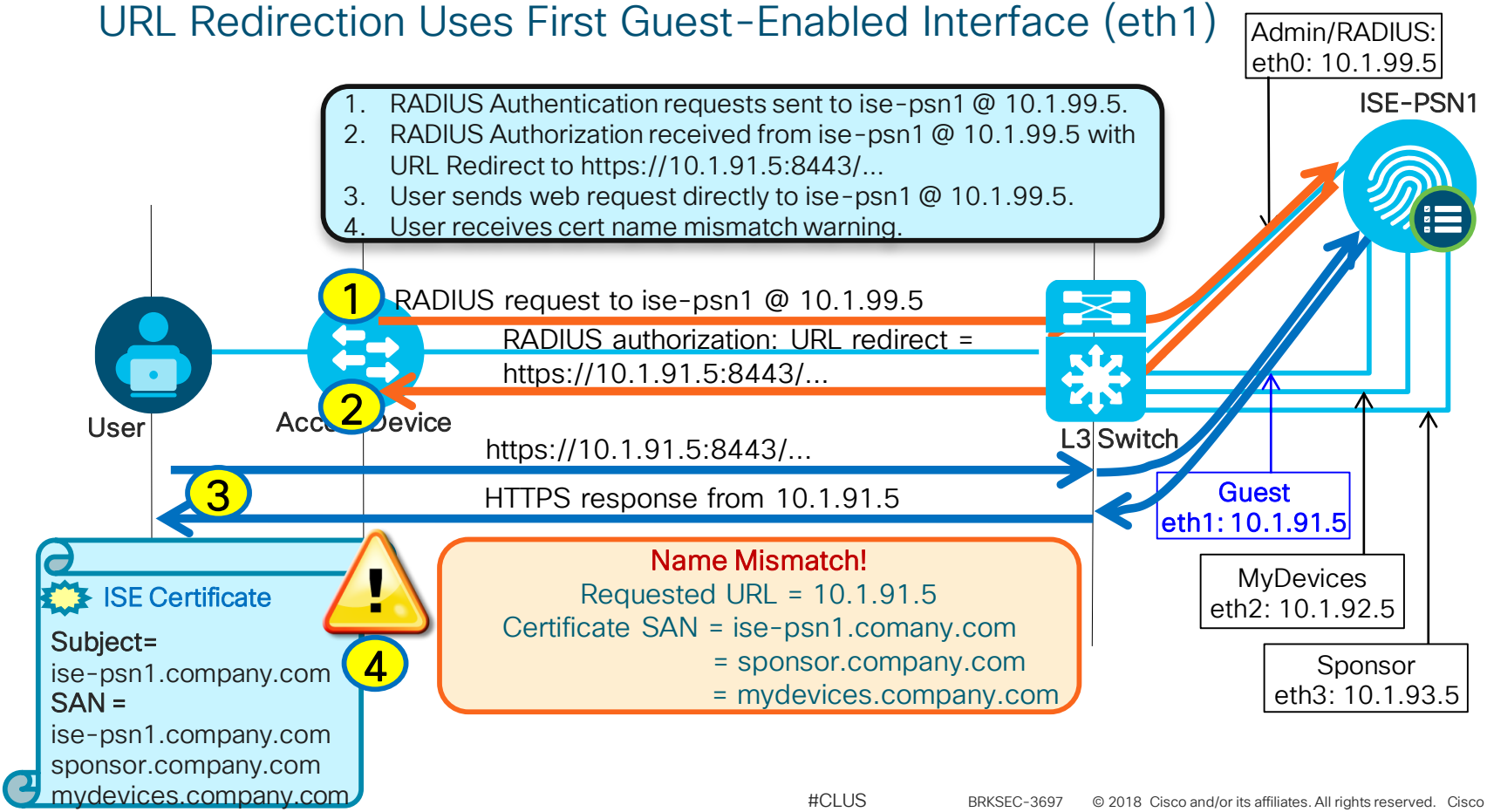
```
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=Se
```

- By default, PSN substitutes host FQDN for 'ip' on eth0, but interface IP for other interfaces. So what is the resulting redirect for eth1?

```
cisco-av-pair = url-redirect=https://10.1.91.5:8443/portal/gateway?sess
```

CWA Example with FQDNs in SAN

URL Redirection Uses First Guest-Enabled Interface (eth1)



Interface Alias Example

DNS and Port Settings – Single Interface Enabled for Guest

- Interface eth1 enabled for Guest Portal
- (config)# ip host 10.1.91.5 ise-psn1-guest.company.com
- URL redirect = https://**ise-psn1-guest.company.com**:8443/...
- Guest DNS resolves FQDN to correct IP address

FQDN with Publicly-Signed Cert

DNS SERVER
DOMAIN = COMPANY.COM

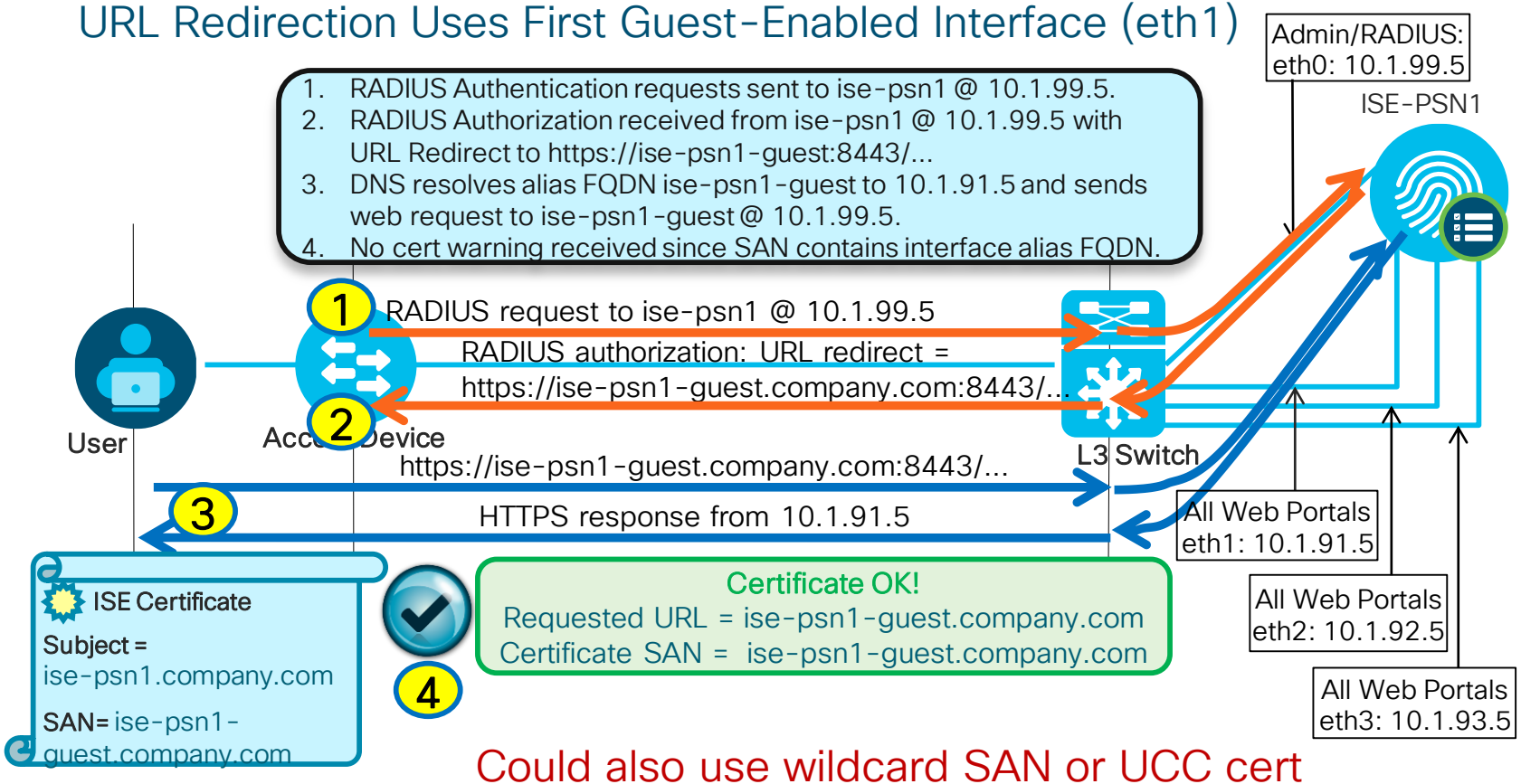
ISE-PSN1-GUEST	IN	A	10.1.91.5	# eth1
ISE-PSN2-GUEST	IN	A	10.1.91.6	# eth1
ISE-PSN3-GUEST	IN	A	10.1.91.7	# eth1

DNS SERVER
DOMAIN = COMPANY.LOCAL

ISE-PSN1	IN	A	10.1.99.5	# eth0
ISE-PSN1-MDP	IN	A	10.1.92.5	# eth2
ISE-PSN1-SPONSOR	IN	A	10.1.93.5	# eth3
ISE-PSN2	IN	A	10.1.99.6	# eth0
ISE-PSN2-MDP	IN	A	10.1.92.6	# eth2
ISE-PSN2-SPONSOR	IN	A	10.1.93.6	# eth3
ISE-PSN3	IN	A	10.1.99.7	# eth0
ISE-PSN3-MDP	IN	A	10.1.92.7	# eth2
ISE-PSN3-SPONSOR	IN	A	10.1.93.7	# eth3

CWA Example using Interface Alias

URL Redirection Uses First Guest-Enabled Interface (eth1)

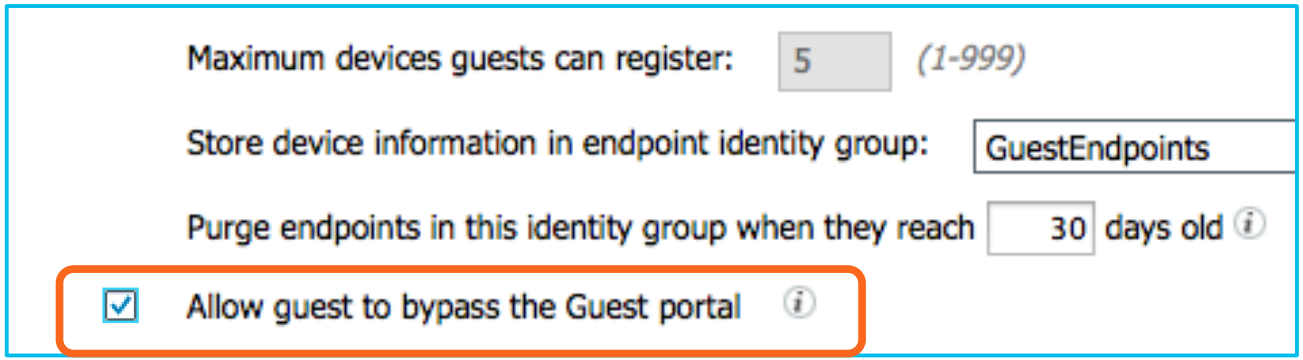


Could also use wildcard SAN or UCC cert

Using Guest Accounts with VPN and 802.1X

"Activated Guest" allows guests accounts to be used without ISE web auth portal

- Guests auth with 802.1X using EAP methods like PEAP-MSCHAPv2 / EAP-GTC
- 802.1X auth performance generally much higher than web auth



Warning: Watch for expired guest accounts, else high # auth failures !

Note: AUP and Password Change cannot be enforced since guest bypasses portal flow.

Scaling Web Auth

"Remember Me" Guest Flows

- User logs in to Hotspot/CWA portal and MAC address auto-registered into GuestEndpoint group
- AuthZ Policy for GuestEndpoints ID Group grants access until device purged

Endpoint identity group: * GuestEndpoints

Purge endpoints in this identity group when they reach 30 days

Configure endpoint purge at
Administration > Identity Management > Settings > Endpoint purge

New in ISE 2.3; configurable in ISE 2.4

Work Centers > Guest Access > Settings > Logging

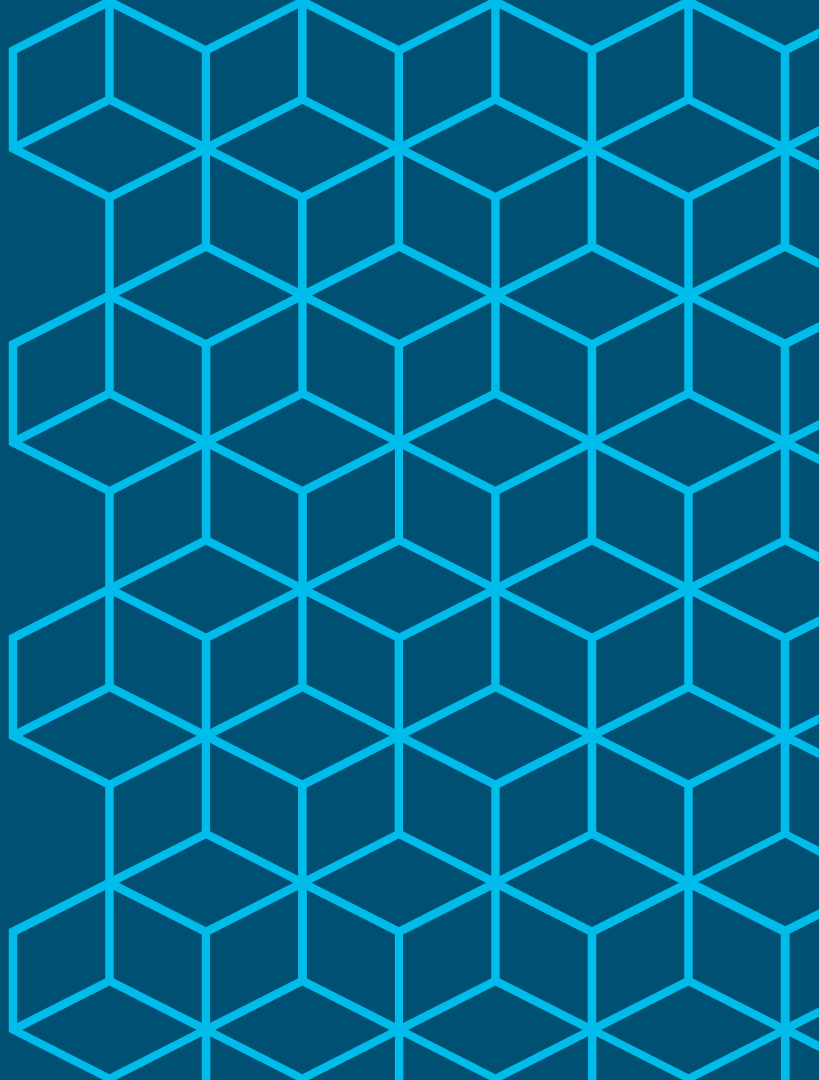
When guest portal is bypassed, authorization is based on endpoint group

☑ Show endpoint's associated portal user ID (vs. MAC address) as the username

Reset Save

Guest users are tracked by the MAC address of their device. When guest users are displayed in reports, the username is the MAC address. If you select this option, reports will display the portal user ID as the username, instead of the MAC address.

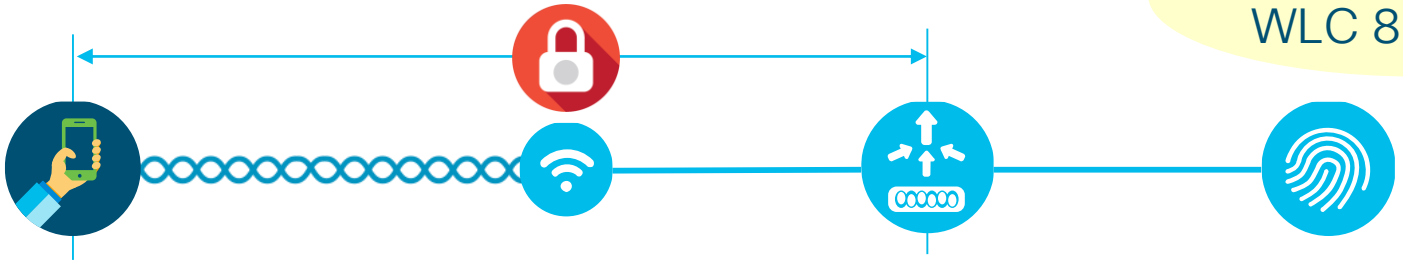
Pre-Shared Key (PSK) and Identity PSK (IPSK)

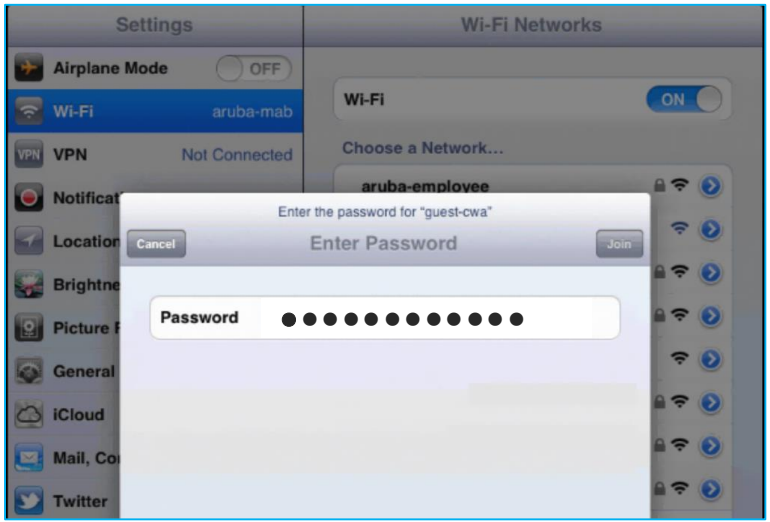


RADIUS NAC on WPA/WPA2-PSK WLAN

Web Authentication over a Protected Network

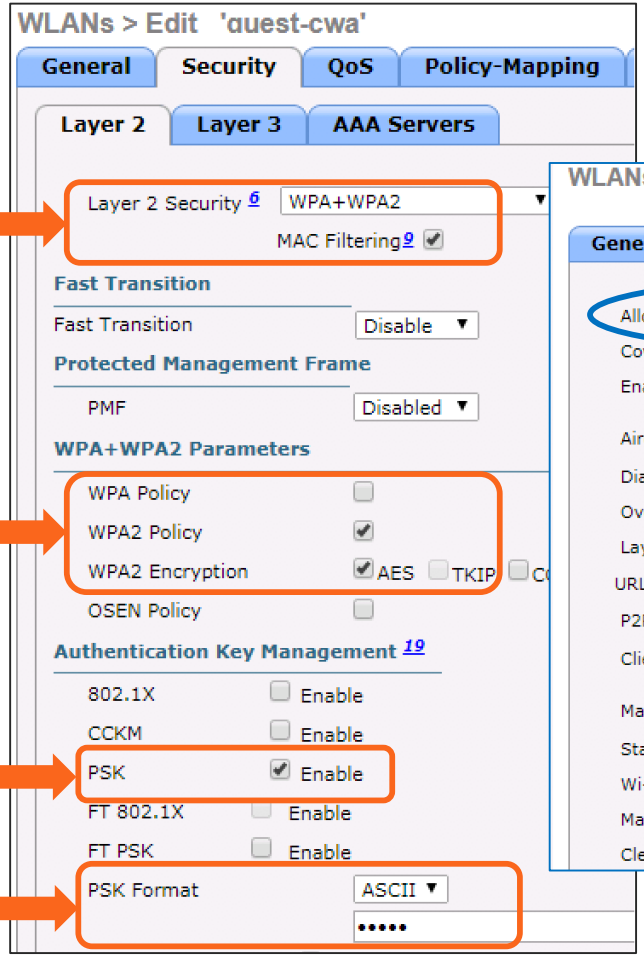
Introduced in WLC 8.3.102.0

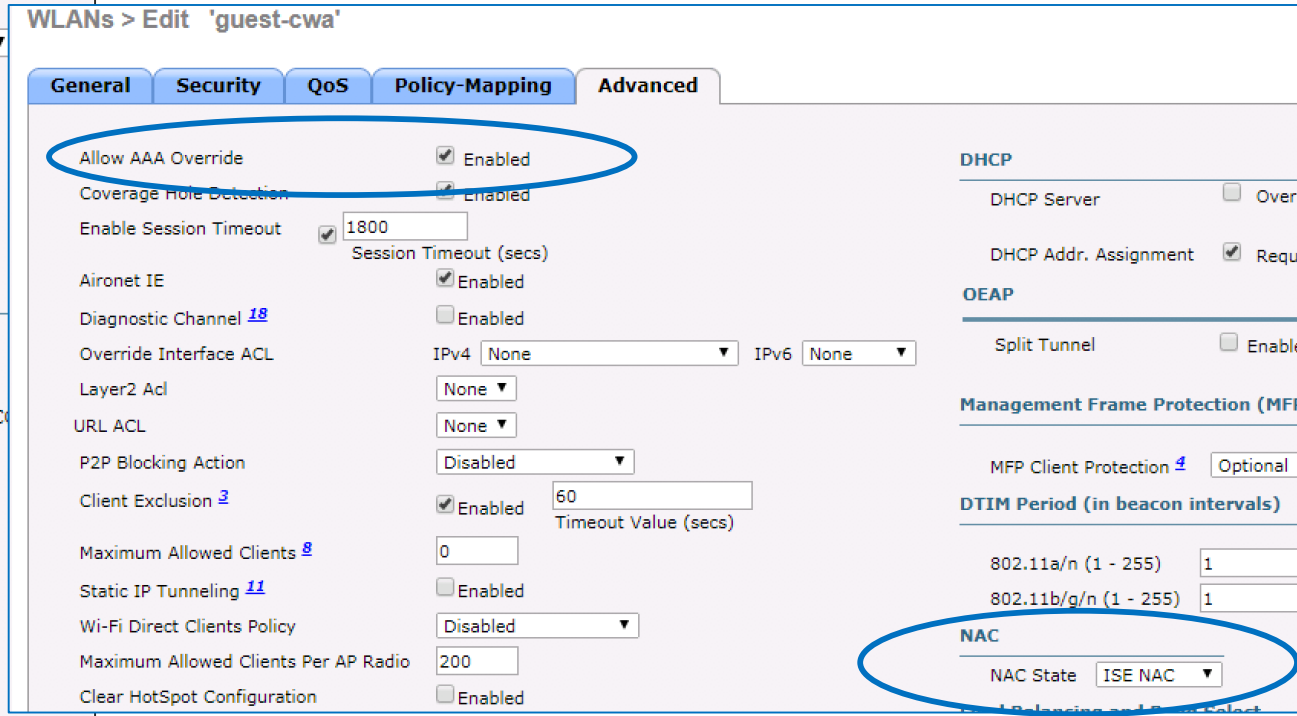




RADIUS NAC on WPA/WPA2-PSK WLAN

Introduced in WLC 8.3.102.0

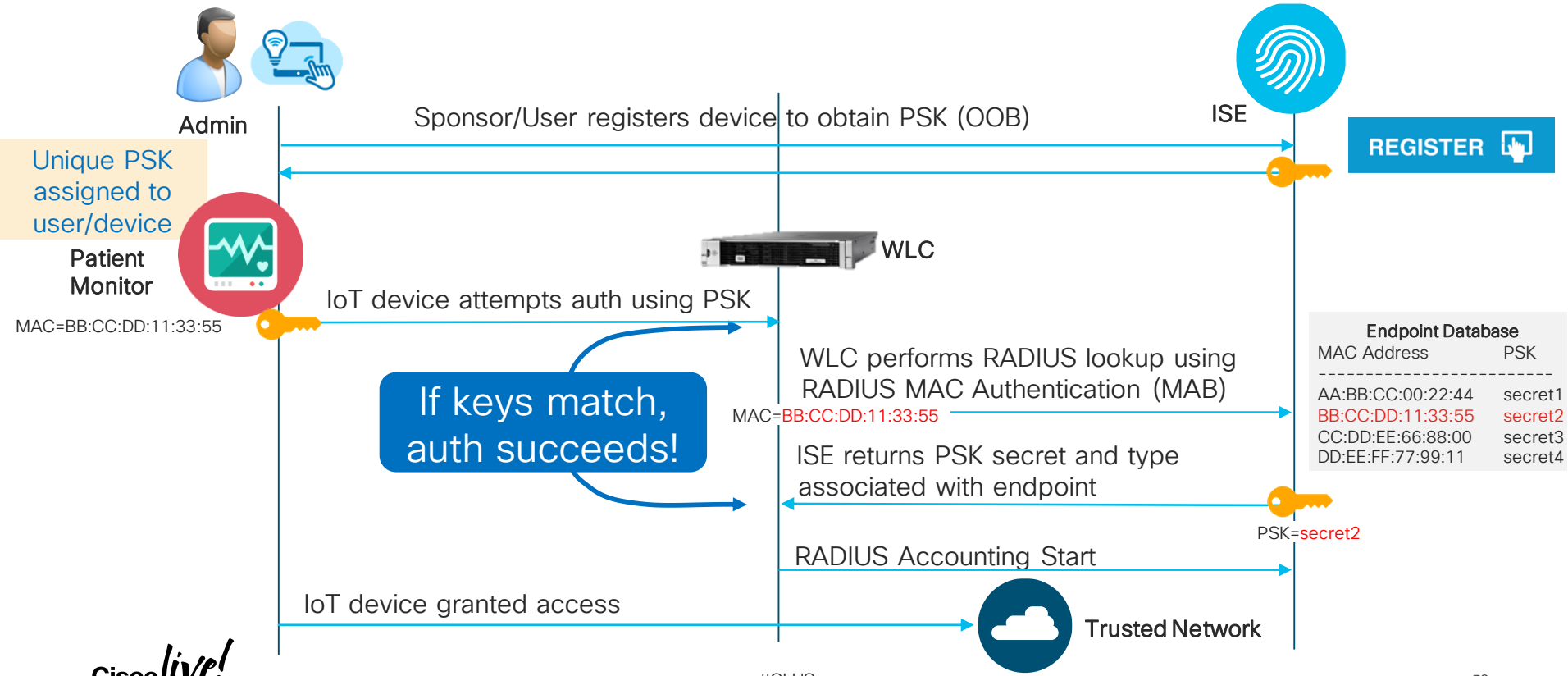




Identity PSK

PSK "Lookups" to ISE via RADIUS

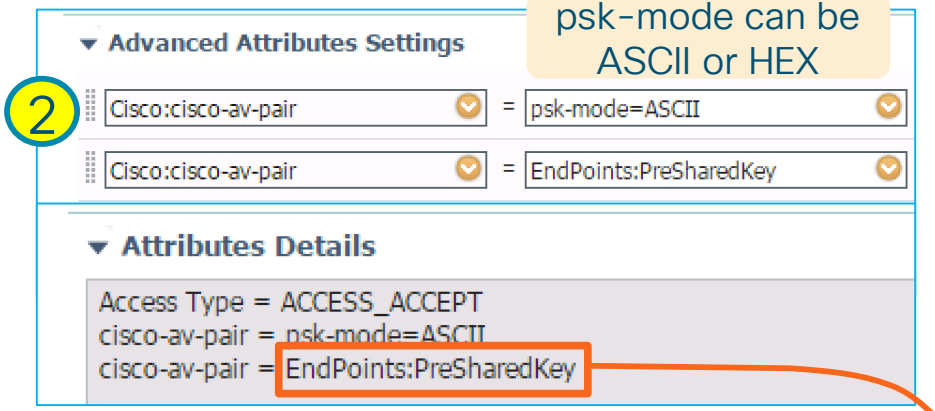
Introduced in WLC 8.5.103.0



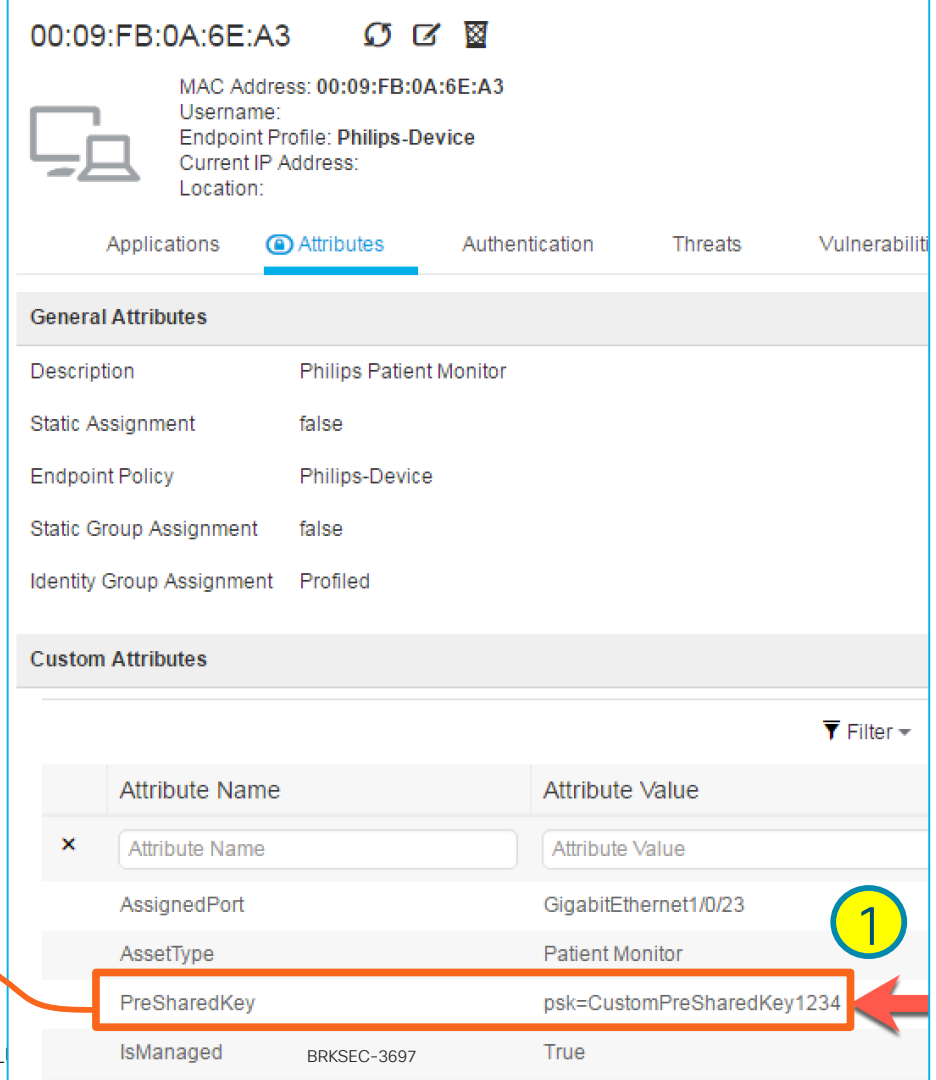
ISE Stores PSKs in Endpoint Database

Step 1. Assign PSK to endpoint or group of endpoints using Admin UI, Registration Portal, or ERS API

Step 2. Return endpoint PSK to WLC using RADIUS



cisco-av-pair=**psk=CustomPreSharedKey1234**



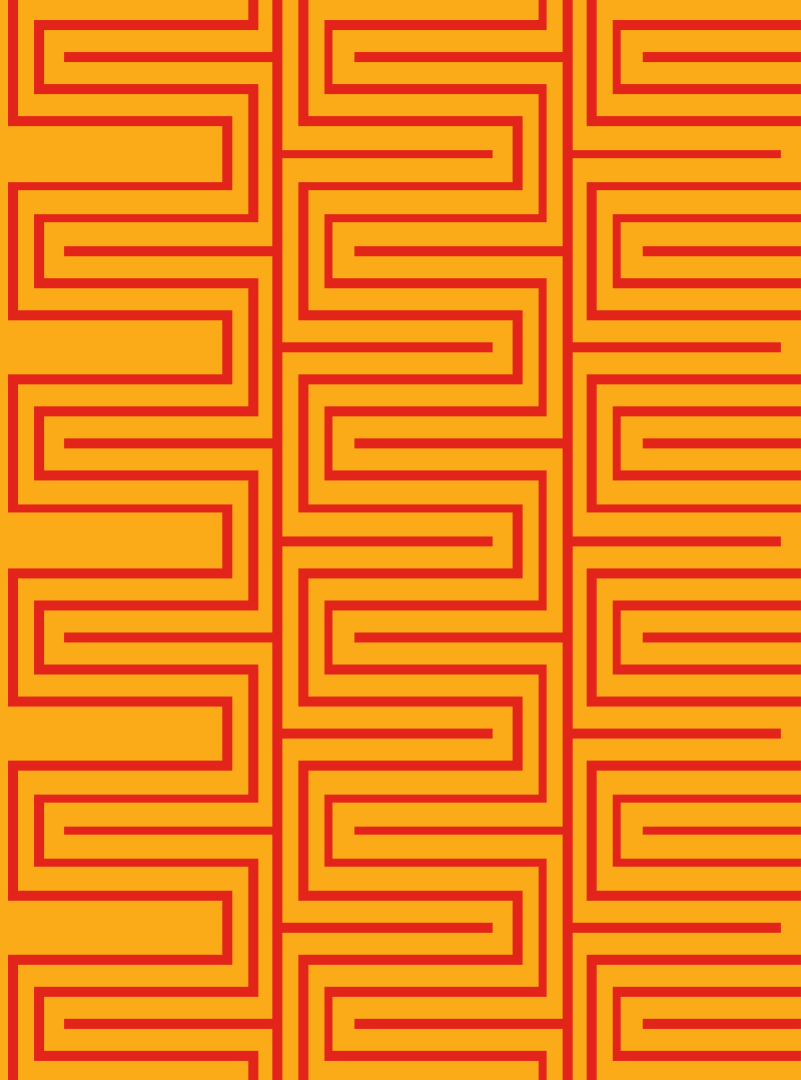
ERS API to add PSK to endpoint

MAC Address 00:09:FB:0A:6E:A3

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<ns4:endpoint description="Philips Patient Monitor" id="d60d3d90-35ee-11e7-8631-46cff03358ad" name="00:09:FB:0A:6E:A3" xmlns:ers="ers.ise.cisco.com"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:ns4="identity.ers.ise.cisco.com">
   <link rel="self" href="https://ise22-pan1.cts.local:9060/ers/config/endpoint/d60d3d90-35ee-11e7-8631-46cff03358ad" type="application/xml"/>
   <customAttributes>
      <customAttributes>
         <entry>
            <key>AssignedPort</key>
            <value>GigabitEthernet1/0/23</value>
         </entry>
         <entry>
            <key>AssetType</key>
            <value>Patient Monitor</value>
         </entry>
         <entry>
            <key>PreSharedKey</key>
            <value>psk=CustomPreSharedKey1234</value>
         </entry>
         <entry>
            <key>IsManaged</key>
            <value>True</value>
         </entry>
      </customAttributes>
   </customAttributes>
   <groupId>aa10ae00-8bff-11e6-996c-525400b48521</groupId>
   <identityStore></identityStore>
   <identityStoreId></identityStoreId>
   <mac>00:09:FB:0A:6E:A3</mac>
   <portalUser>JohnSmith</portalUser>
   <profileId>30e1c590-8c00-11e6-996c-525400b48521</profileId>
   <staticGroupAssignment>false</staticGroupAssignment>
   <staticProfileAssignment>false</staticProfileAssignment>
</ns4:endpoint>
```

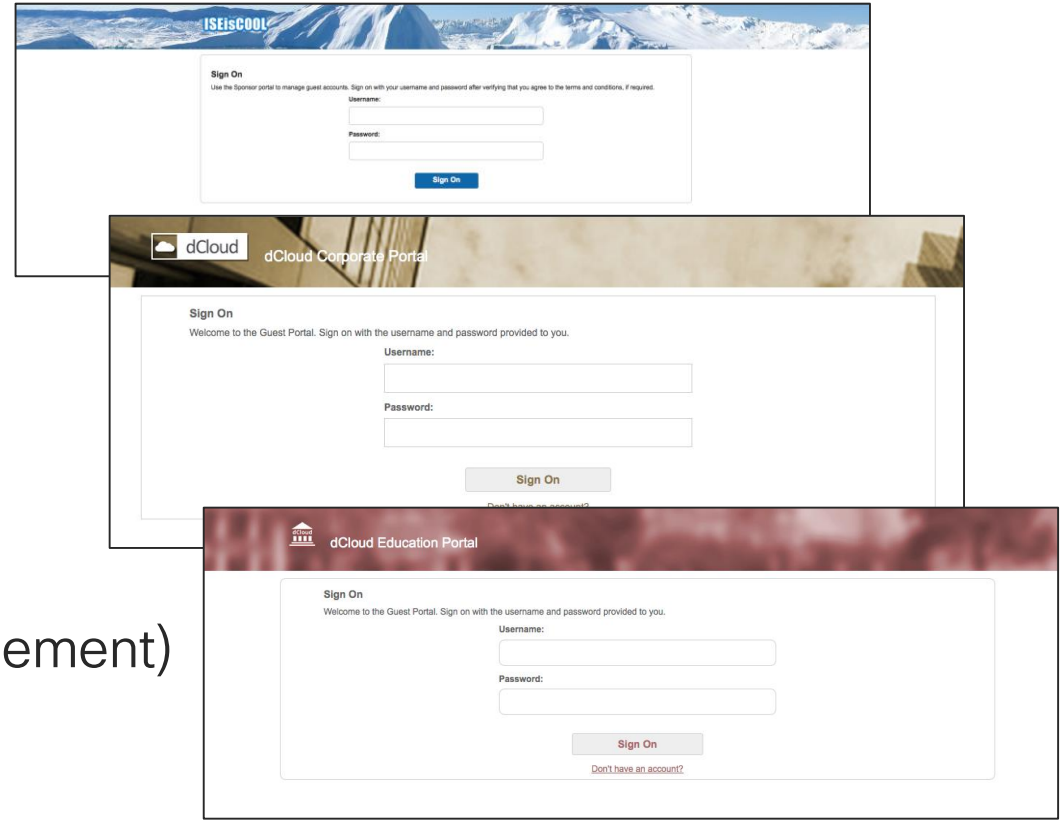
```
<customAttributes>
   <entry>
      <key>AssignedPort</key>
      <value>GigabitEthernet1/0/23</value>
   </entry>
   <entry>
      <key>AssetType</key>
      <value>Patient Monitor</value>
   </entry>
   <entry>
      <key>PreSharedKey</key>
      <value>psk=CustomPreSharedKey1234</value>
   </entry>
   <entry>
      <key>IsManaged</key>
      <value>True</value>
   </entry>
</customAttributes>
```

Portal Customization



Which Portals are Customizable

- Guest
- Sponsor
- BYOD (Device Registration)
- My Devices
- Certificate Provisioning
- Client Provisioning (Desktop Posture)
- MDM (Mobile Device Management)
- Blacklist



Admin Users that ISE Customization Supports

Embedded Interfaces for Different Skillsets

Average User

No understanding of HTML, CSS or JavaScript or design. Wants a button to push to make everything work.

The Tweaker

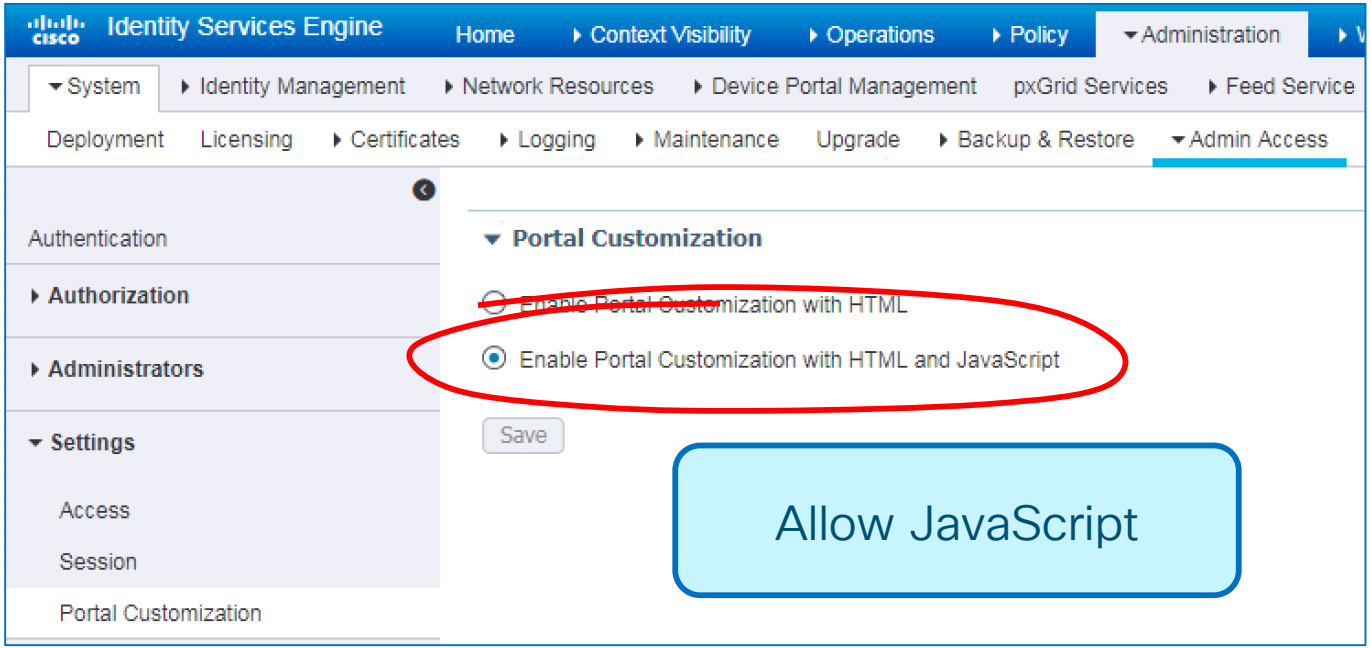
Some CSS & JavaScript ability but doesn't want to rewrite all guest pages from scratch. An intuitive editing UI is preferred.

The Coder

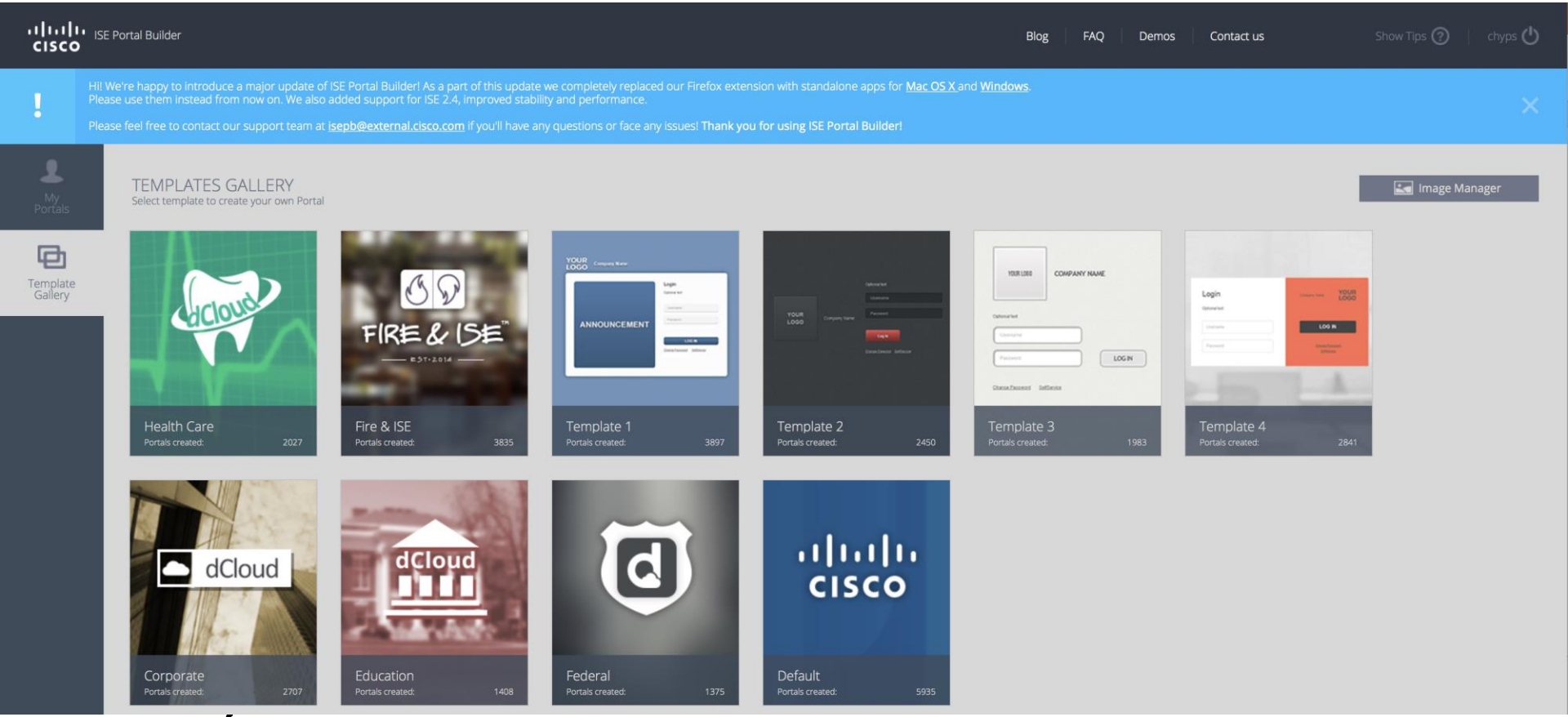
Experienced with HTML, CSS & JavaScript. Is brought in to do complex web design.

Advanced Portal Customization

Administration > System > Admin Access > Settings > Portal Customization



ISE Portal Builder (isepb.cisco.com)



Portal Customization

Community Tips and Tricks

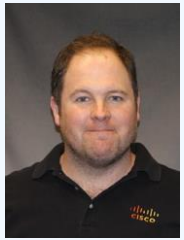
https://communities.cisco.com/docs/DOC-64018

cisco Communities Welcome,

ISE Guest & Web Authentication

created by Thomas Howard on Nov 24, 2015 9:17 AM, last modified by jakunst on May 24, 2018 1:08 PM

- Release Enhancements
  - ISE 2.3
  - ISE 2.1/2.2
- Product Training
- Demos
- Blogs
- Configuration
  - Misc
  - Remember Me
  - NAC Guest Server
  - Meraki How To and Video
  - Web Portal access via SAML SSO
  - Integrations
  - Miscellaneous
  - SMS
- Special Flows
- Customizations
  - General customizations
  - Guest
    - Credential login page



Jason Kunst

Customizations

Support for 1.3+

- I have a script that shows me how to hide an element on a page but I want to also hide something else, how do i find it?
  - This video shows you in an example on the sponsor portal page

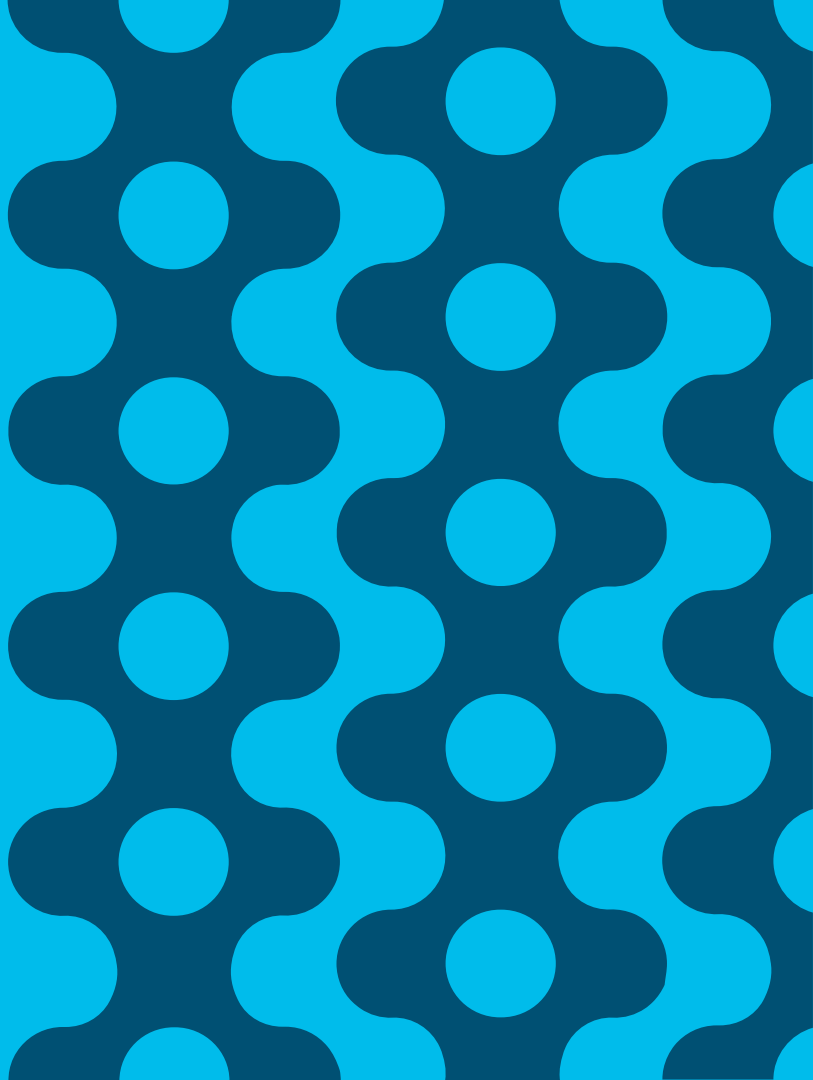
General customizations

- How to center ISE content in a frame.
- ISE Web Portals providing a different logo per language
- Insert a background image (built-into ISE 2.2)
- Guest Page insert image with hyperlink

Guest

- How To: ISE Web Portal Customization Options
- ISE Portal Builder - create customized portals (guest, byod, mdm, posture) using drag & drop editor
- Single Credential Login to Guest Portal (same password used for all accounts and hiding field)
  - Used for guest scenario where they only want a 6 number passcode (not a username + password)
- Hotspot as a Message Portal with Support link
  - redirect user to a meaningful message portal when being redirected due to quarantine or blacklist (only 1 blacklist portal allowed)
- Login page auto-redirect to create an account page
  - This script is used for providing guests direct access to self-registration page.
    - For a kiosk that might be in a lobby
    - guest flow is usually going to create an account first (and not needing the login page)
    - Meraki LWA where they want to link customer directly to self-reg portal from the splash page
- ISE Guest registration (create account) and login on same page
- Hotspot Portal with information collection
  - Makes a self-reg portal into a hotspot flow that allows you to collect information (such as email address)
  - Re: Ise guest self registration page checkbox requirement for newsletter
- ISE Guest Portal Customization hide username password field
- Captcha type protection for self-reg and login pages
  - i am not a computer, human interaction
- Linking one guest portal to another guest portal

Profiling Tips and Tricks



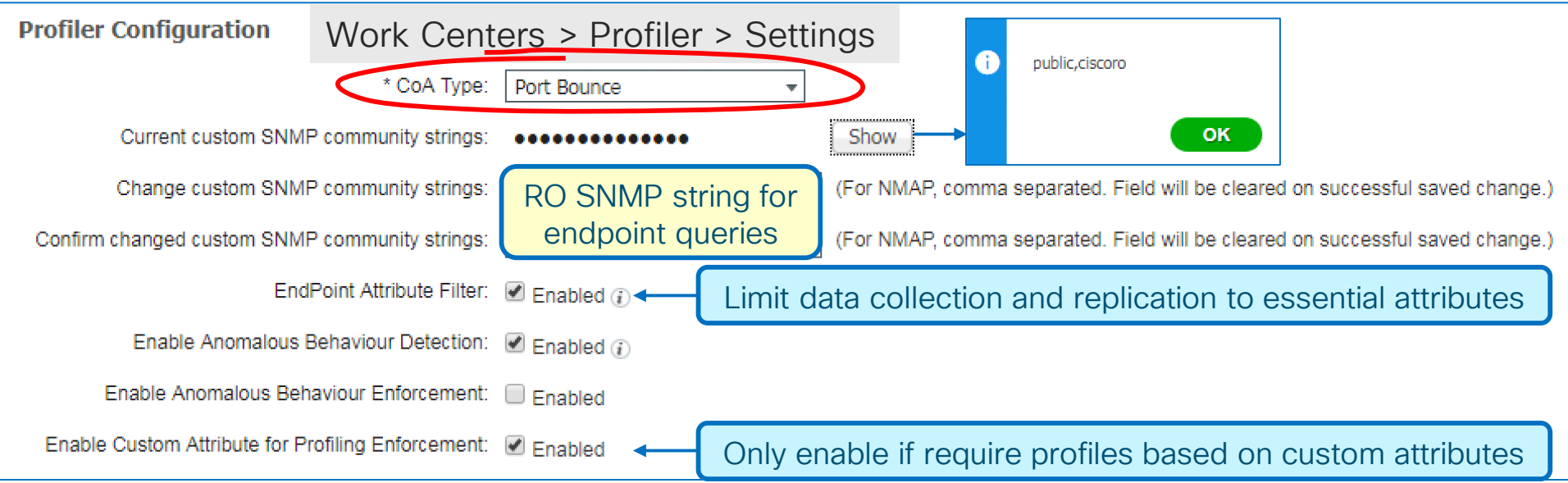
Agenda

- First Things First
- Feed Services and Community Profiles
- Logical Profiles
- Custom Profile Creation

Profiler Setup – First Things First

Configure Global Profiler Settings

- Set default CoA type for profile changes >> None/Reauth/Port Bounce

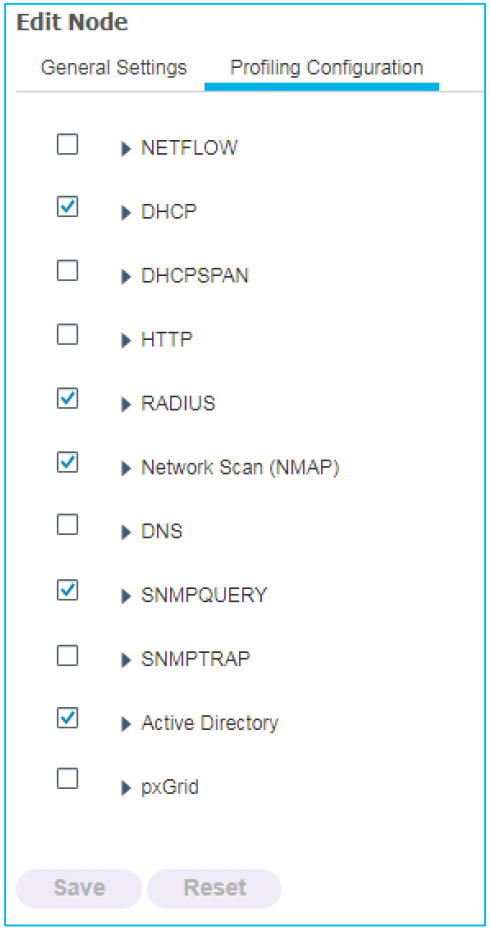


Verify Required Profiler Probes Enabled

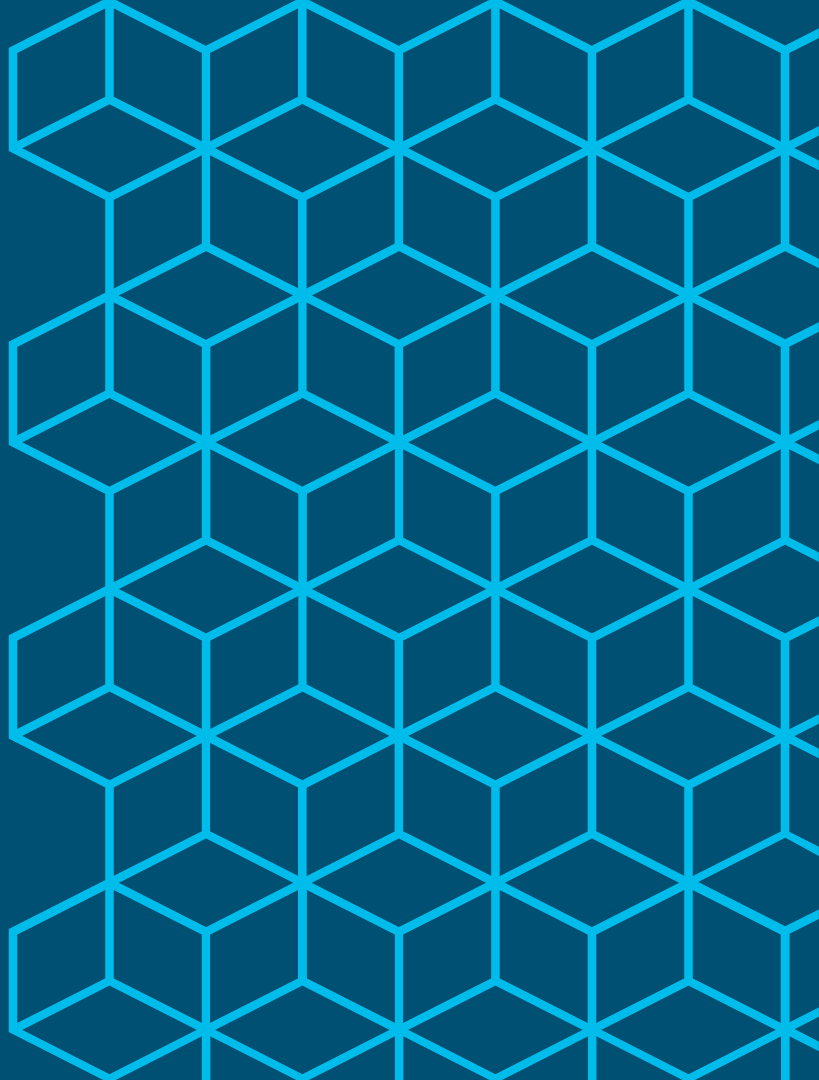
Work Centers > Profiler > Node Config

- Only enable what is needed.
- By default, RADIUS probe always running (even without Plus License) to collect endpoint data needed for Context Visibility and to allow Purge functions to operate with Guest accounts.
- HTTP Probe is automatically running for redirected web flows, but can be enabled to additionally collect browser user agent data from SPAN or direct portal access.
- DNS should generally be enabled if there is a reasonable naming schema assigned to hosts in DNS.

- Remember that network must also be configured to support profiling queries, or to send data to ISE PSNs.
- Distribution switches that serve as L3 gateways should be added as NADs for SNMP polling of ARP tables.



“ISE Feed Service is like a box of chocolates. You never know what you’re gonna get.”

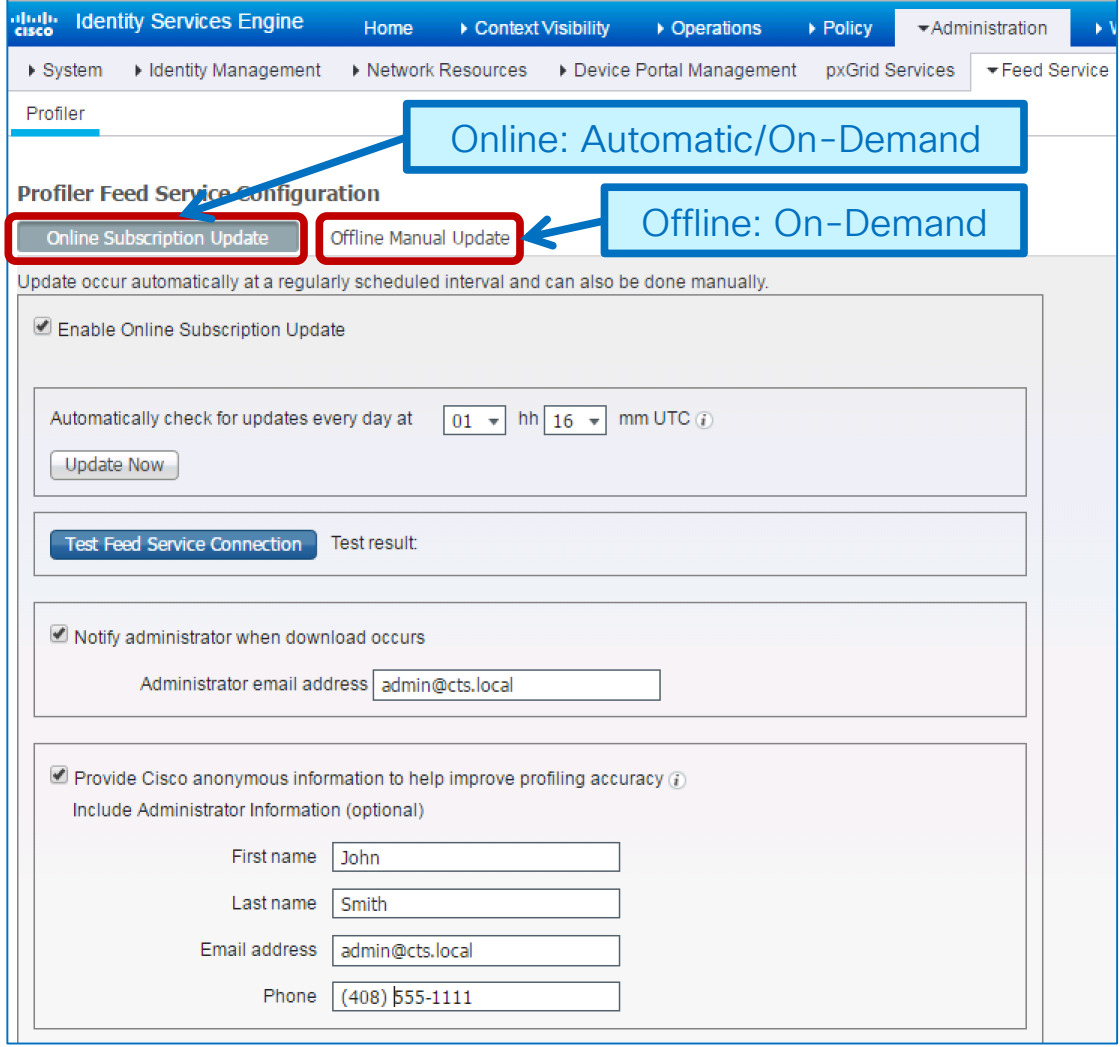


Profiler Feed Service Updates

Both Online and Offline Service

- Scheduled and On-Demand Profiler Feed Service updates from Cisco.com when have direct Internet connection from ISE Primary Admin node.

- Offline Feed Updates available when Internet access restricted.
  - Highly-Secured deployments
  - Proof of Concepts
  - Lab Testing
  - Demos

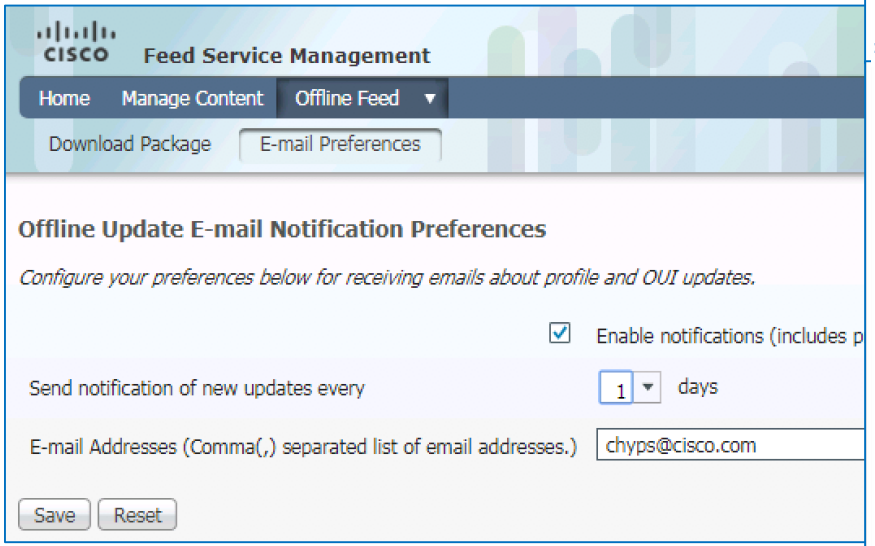


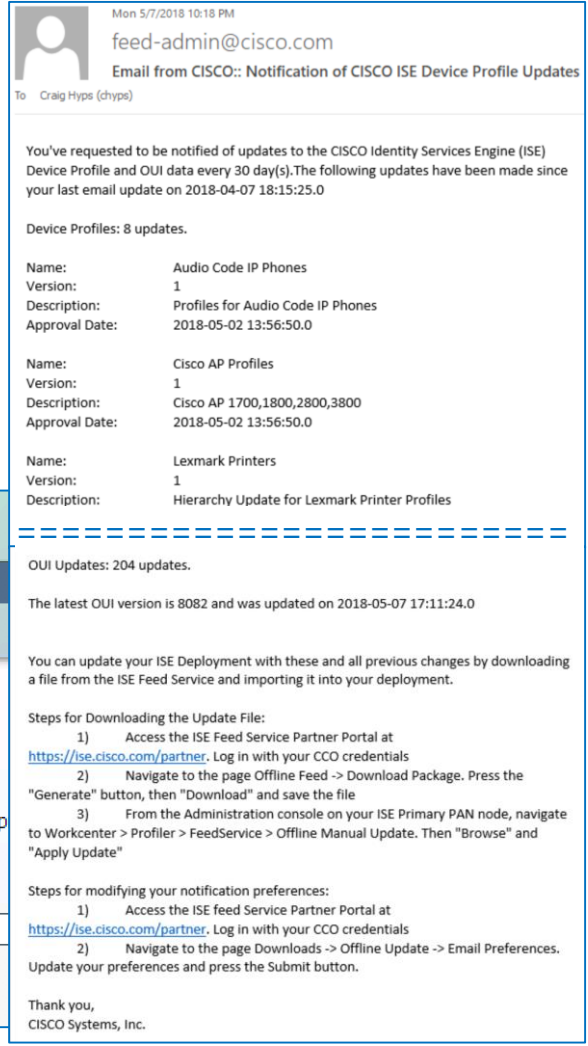
Profiler Feed Best Practices

https://ise.cisco.com/partner/

1. **Disable Online Subscription Updates**
2. **Test updates** in lab or other pre-staging environment (via live or offline updates) *before* apply updates to production.

3. **Setup email notifications** to be alerted for new OUI and Profile updates



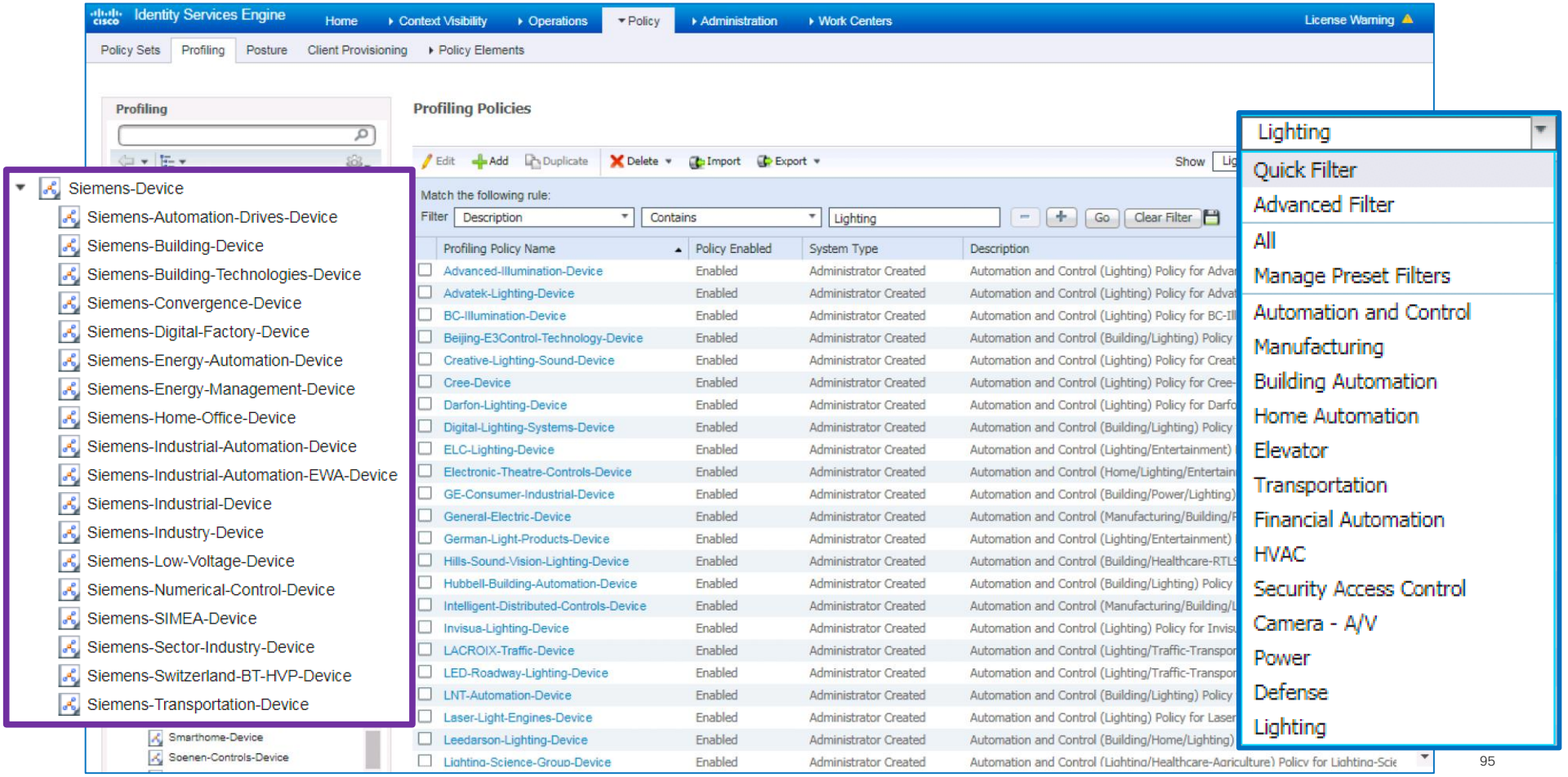


New and Updated IoT Profile Libraries

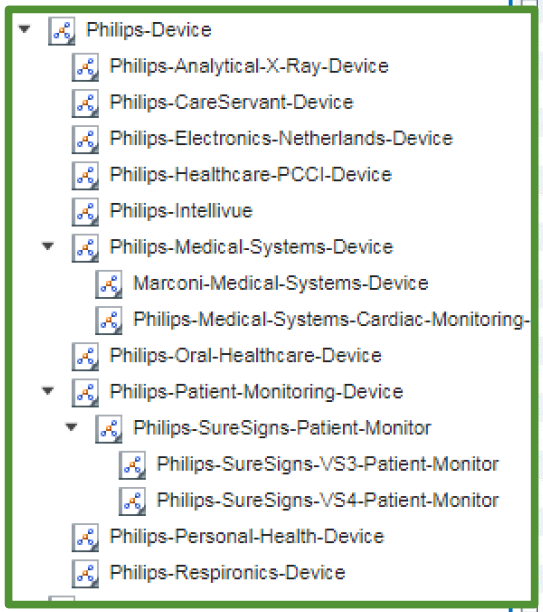
Auto-detect and classify Automation and Control endpoints

- Automation and Control
  - Industrial / Manufacturing
  - Building Automation
  - Power / Lighting
  - Transportation / Logistics
  - Financial (ATM, Vending, PoS, eCommerce)
  - IP Camera / Audio-Video / Surveillance and Access Control
  - Other (Defense, HVAC, Elevators, etc)
- Windows Embedded
- Medical NAC Profile Library – Updated

700+ Automation and Control Profiles



300+ Medical Device Profiles



Profiling Policies

Selected 0 | Total 315

Edit | Add | Duplicate | Delete | Import | Export | Show: Quick Filter

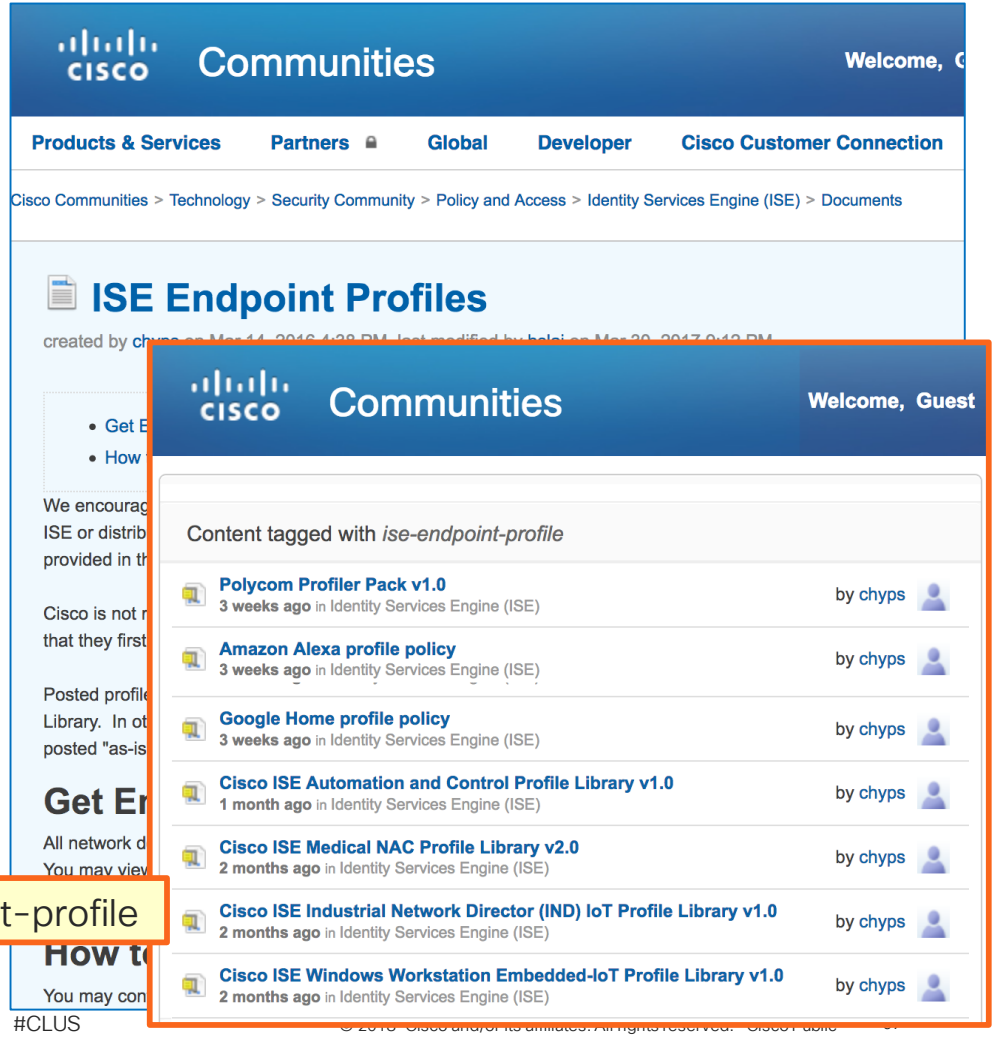
Profiling Policy Name	Policy Enabled	System Type	Description
			Healthcare
Draeger-Medical-Device	Enabled	Administrator Created	Healthcare policy for Draeger-Medical devices
Draeger-Medical-Systems-Device	Enabled	Administrator Created	Healthcare policy for Draeger-Medical-Systems devices
Dragerwerk-Device	Enabled	Administrator Created	Healthcare policy for Dragerwerk devices
Durr-Dental-Device	Enabled	Administrator Created	Healthcare policy for Durr-Dental devices
Edwards-Lifesciences-Device	Enabled	Administrator Created	Healthcare policy for Edwards-Lifesciences devices
Ellex-Medical-Device	Enabled	Administrator Created	Healthcare policy for Ellex-Medical devices
Eppendorf-Device	Enabled	Administrator Created	Healthcare policy for Eppendorf devices
Essilor-Device	Enabled	Administrator Created	Healthcare policy for Essilor devices
Etymonic-Design-Device	Enabled	Administrator Created	Healthcare policy for Etymonic-Design devices
Fisher-Paykel-Device	Enabled	Administrator Created	Healthcare policy for Fisher-Paykel devices
Fluke-Biomedical-Device	Enabled	Administrator Created	Healthcare policy for Fluke-Biomedical devices
Fresenius-Medical-Care-Device	Enabled	Administrator Created	Healthcare policy for Fresenius-Medical-Care devices
Fukuda-Denshi-Device	Enabled	Administrator Created	Healthcare policy for Fukuda-Denshi devices
GE-Healthcare-Device	Enabled	Administrator Created	Healthcare policy for GE-Healthcare devices
GE-Medical-System-Device	Enabled	Administrator Created	Healthcare policy for GE-Medical-System devices
GN-ReSound-Device	Enabled	Administrator Created	Healthcare policy for GN-ReSound devices
Gambro-Lundia-Device	Enabled	Administrator Created	Healthcare policy for Gambro-Lundia devices
Gem-Med-Device	Enabled	Administrator Created	Healthcare policy for Gem-Med devices
Getinge-Device	Enabled	Administrator Created	Healthcare policy for Getinge devices
Getinge-IT-Solutions-Device	Enabled	Administrator Created	Healthcare policy for Getinge-IT-Solutions devices
Getinge-Sterilization-Device	Enabled	Administrator Created	Healthcare policy for Getinge-Sterilization devices
HL7-Client	Enabled	Administrator Created	Healthcare policy for HL7-Client devices
HL7-Server	Enabled	Administrator Created	Healthcare policy for HL7-Server devices
HORIBA-Medical-Device	Enabled	Administrator Created	Healthcare policy for HORIBA-Medical devices

Community Profiles

communities.cisco.com/docs/DOC-66340

- Alternative method to submit and access new profiles
- Why not use Feed Service Portal?
  - Less formal method
  - Staging area to vet new profiles
  - Allows sharing of vertical-specific profiles that may not be of interest to general customer.
  - **Currently a 2000 Profile Limit**

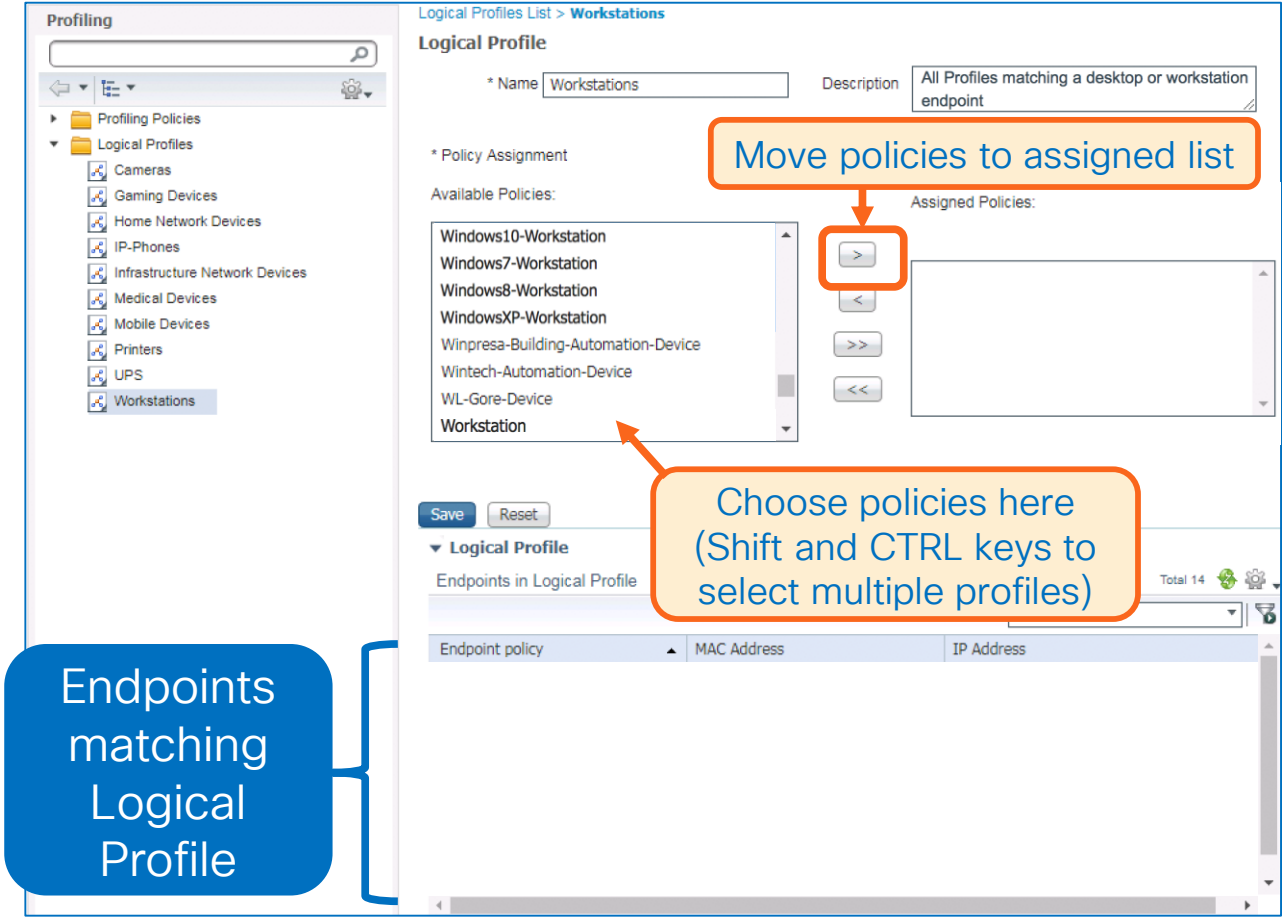
https://communities.cisco.com/tags/ise-endpoint-profile



Logical Profiles

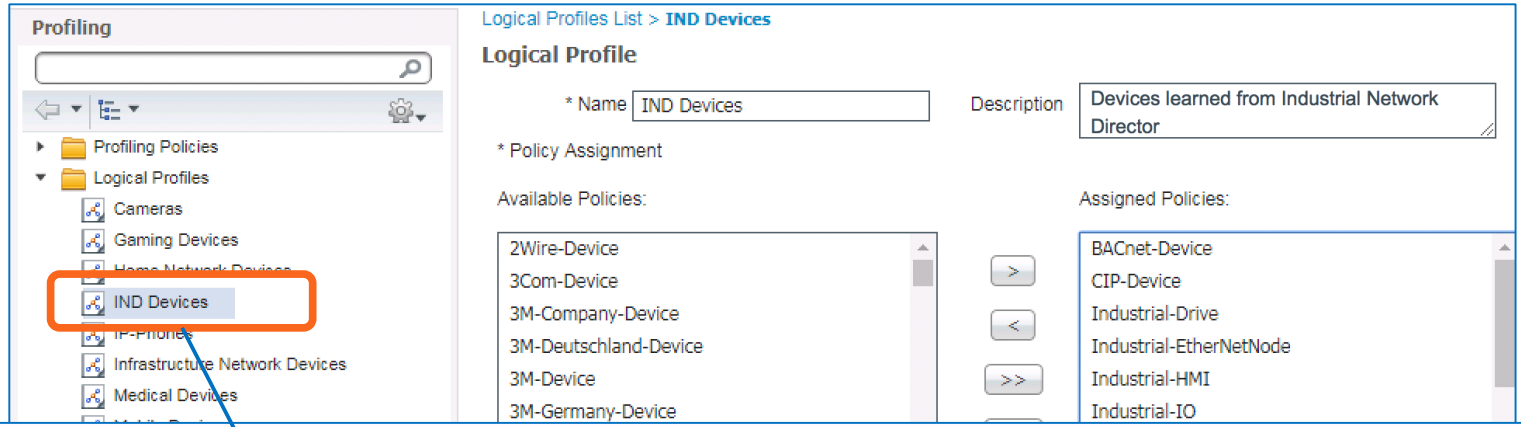
Work Centers > Profiler > Profiling Policies > Logical Profiles

- Logical Profiles help organize views and simplify policy rules.
- An endpoint profile can be a member of multiple Logical Profiles
- Use Logical Profiles instead of Identity Groups when possible



Logical Profiles

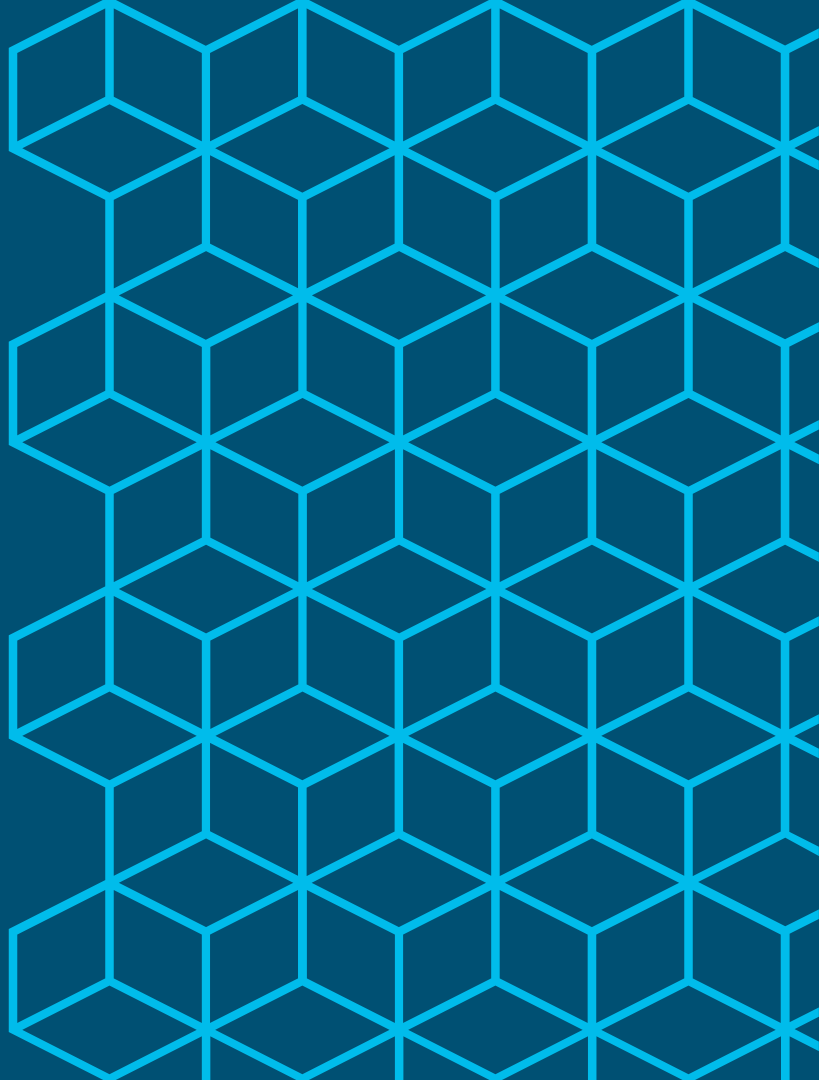
Authorization Policy Rules



Authorization Policy (14)

Status	Rule Name	Conditions		Results Profiles	Results Security Groups	Hits	Actions
Search							
✓	Wireless Black List Default	AND	Wireless_Access IdentityGroup·Name EQUALS Endpoint Identity Groups:Blacklist	× Blackhole_Wireless_Access	Quarantine	51	
✓	Manufacturing	AND	EndPoints·LogicalProfile EQUALS IND Devices EndPoints·assetGroup EQUALS Pod5	× PermitAccess	Manufacturing	822	
✓	Profiled Cisco IP Phones		IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	× Cisco_IP_Phones	Phones	21397	
✓	Profiled Non Cisco IP Phones		Non_Cisco_Profiled_Phones	× Non_Cisco_IP_Phones	Phones	4281	

Custom Profile Creation



Get all Endpoints

Generate and Offload Report

Available in:
- ISE 2.0.1 Patch 3
- ISE 2.1 Patch 4
- ISE 2.2 FCS and later

```
# application configure ise
```

```
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Enable/Disable Wifi Setup
[18]Reset Config Wifi Setup
[19]Exit

16
Starting to generate All Endpoints report
Processing.....
Copying files to /localdisk
Completed generating All Endpoints report. You can find details in following files located under /localdisk
FullReport_25-Apr-2017.csv
```

- Report saved to local disk.
- To view, copy to external repository. Example:

```
# copy  disk:/FullReport_25-May-2018.csv  ftp://10.1.100.200
```

Get All Endpoints – Example Report (excerpt)

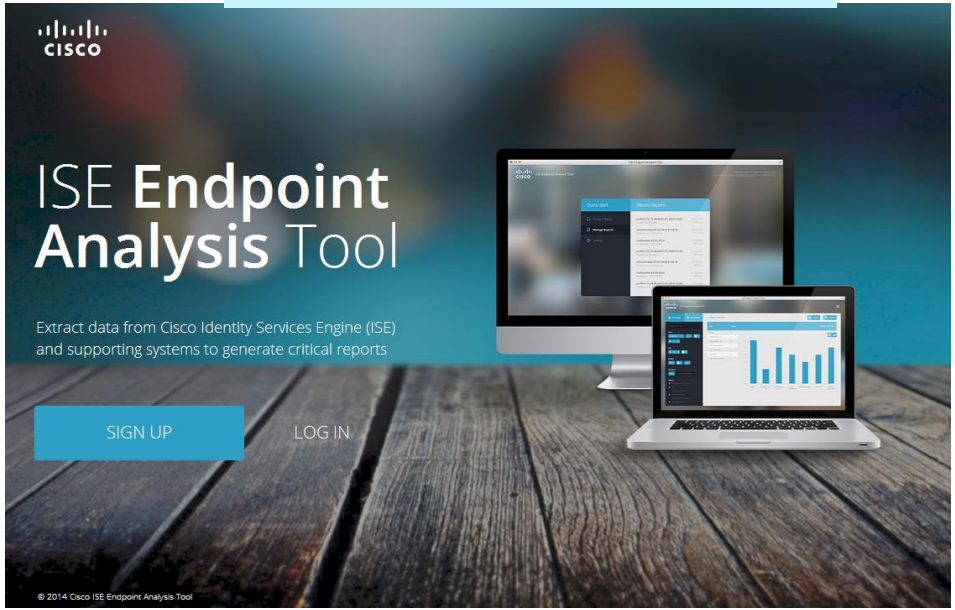
MACAddress	ip	FQDN	host-name	IdentityGroup	MatchedPolicy	OUI	dhcp-class-identifier	dhcp-user-class-id	dhcp-parameter-request-list	User-Agent
70:70:0D:72:47:BA			chyps-iPhone7	Profiled	Apple-iPhone	Apple, Inc.			1, 121, 3, 6, 15, 119, 252	
3C:E5:A6:C3:8A:90	10.1.10.100		WA2612-AGN	Unknown	Unknown	Hangzhou H3C Technologies Co., Limited	H3C. H3C WA2612-AGN		1, 121, 3, 6, 15, 33, 43	
00:50:56:91:7D:B3	10.1.10.104		win7-pc2	Workstation	Microsoft-Workstation	VMware, Inc.	MSFT 5.0	57:69:6e:64:6f:77:73:37	1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43	
00:50:56:A0:0B:3A	10.1.10.103		win7-pc	Workstation	Microsoft-Workstation	VMware, Inc.	MSFT 5.0	43:6f:72:70:2d:57:69:6e:37	1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43	
00:09:FB:0C:2D:F9	10.1.10.105		philips-mx450	Profiled	Philips-Device	Philips Patient Monitoring			1, 28, 2, 121, 15, 6, 12, 40, 41, 42, 26, 119, 3, 121, 249, 33, 252, 42	
00:1A:1E:CF:B8:82	10.1.10.102		00:1a:1e:cf:b8:82	Profiled	Aruba-AP	Aruba Networks	ArubaAP		1, 3, 4, 6, 12, 15, 28, 42, 43, 60	
7C:6D:62:E3:D5:05	172.16.10.216		Apple-1pad	Apple-iDevice	Apple-iDevice	Apple, Inc.			1, 3, 6, 15, 119, 252	
6C:20:56:13:E9:FC	10.1.10.101		ap1602	Profiled	Cisco-AP-Aironet-1600	Cisco Systems, Inc	Cisco AP c1600		1, 6, 15, 44, 3, 7, 33, 150, 43	
00:50:56:91:42:61	10.1.101.9			Profiled	ISE-Appliance	VMware, Inc.				
3C:61:04:FA:6F:01	10.10.50.2			Juniper-Device	Juniper-Device	Juniper Networks				
00:C0:B7:68:31:E1	172.16.1.28			Profiled	American-Power-Conversion-Device	AMERICAN POWER CONVERSION CORP				

Profiler Attributes!

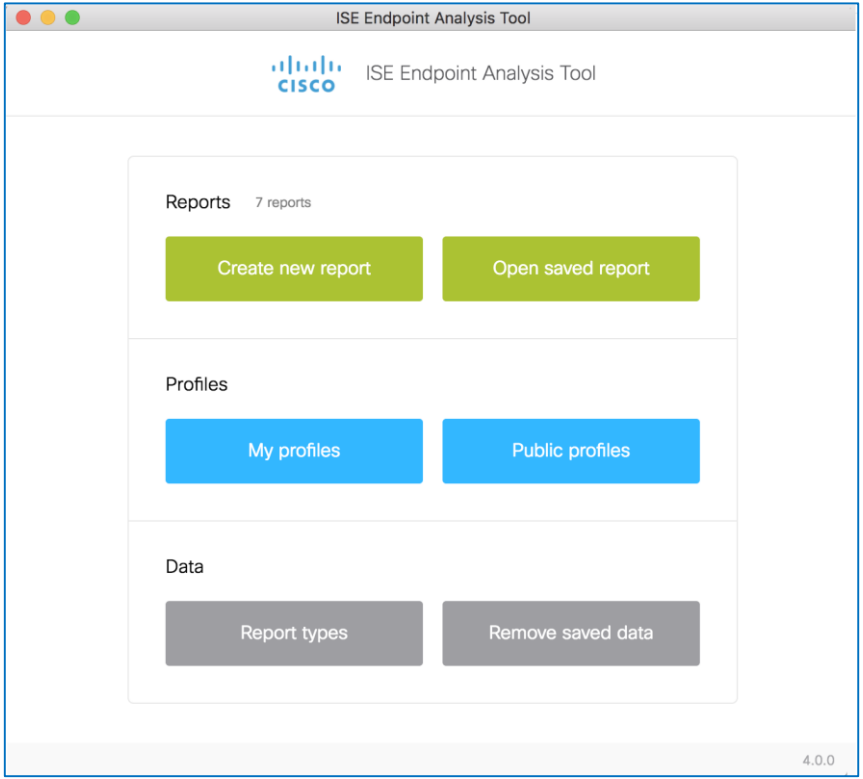
EAT

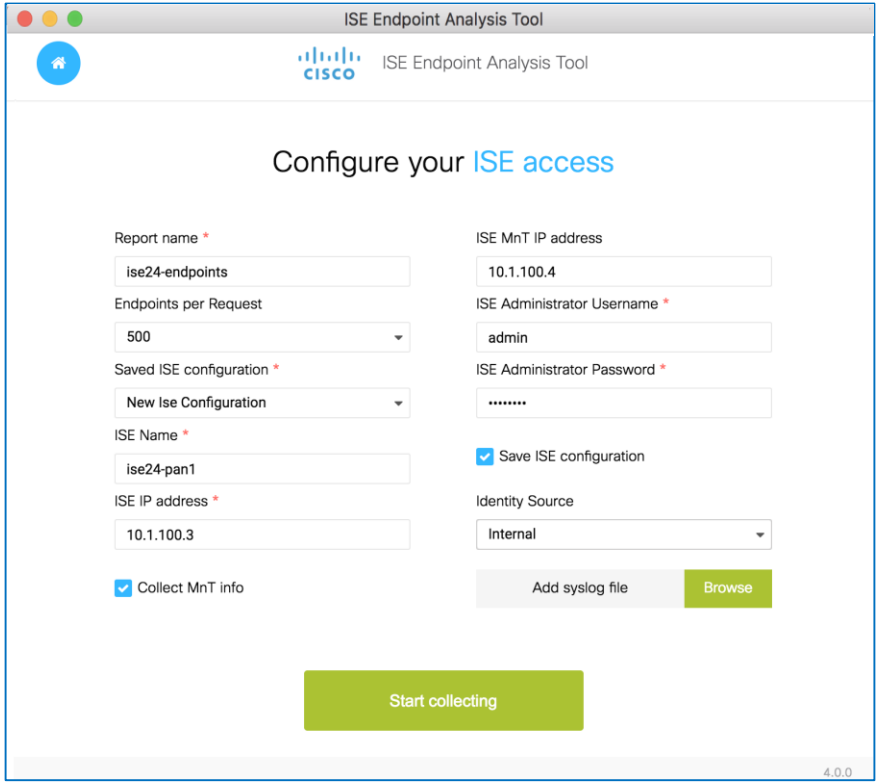
- Registration required
  - Open to partners and customers
- Simple/Intuitive
  - Best effort support
- Collects endpoint attributes from Primary PAN db
  - Optional collection and correlation to ISE Auth Logs
- Select/all export to CSV
- Automatic data collection to Cisco cloud for profiling analysis

http://iseeat.cisco.com

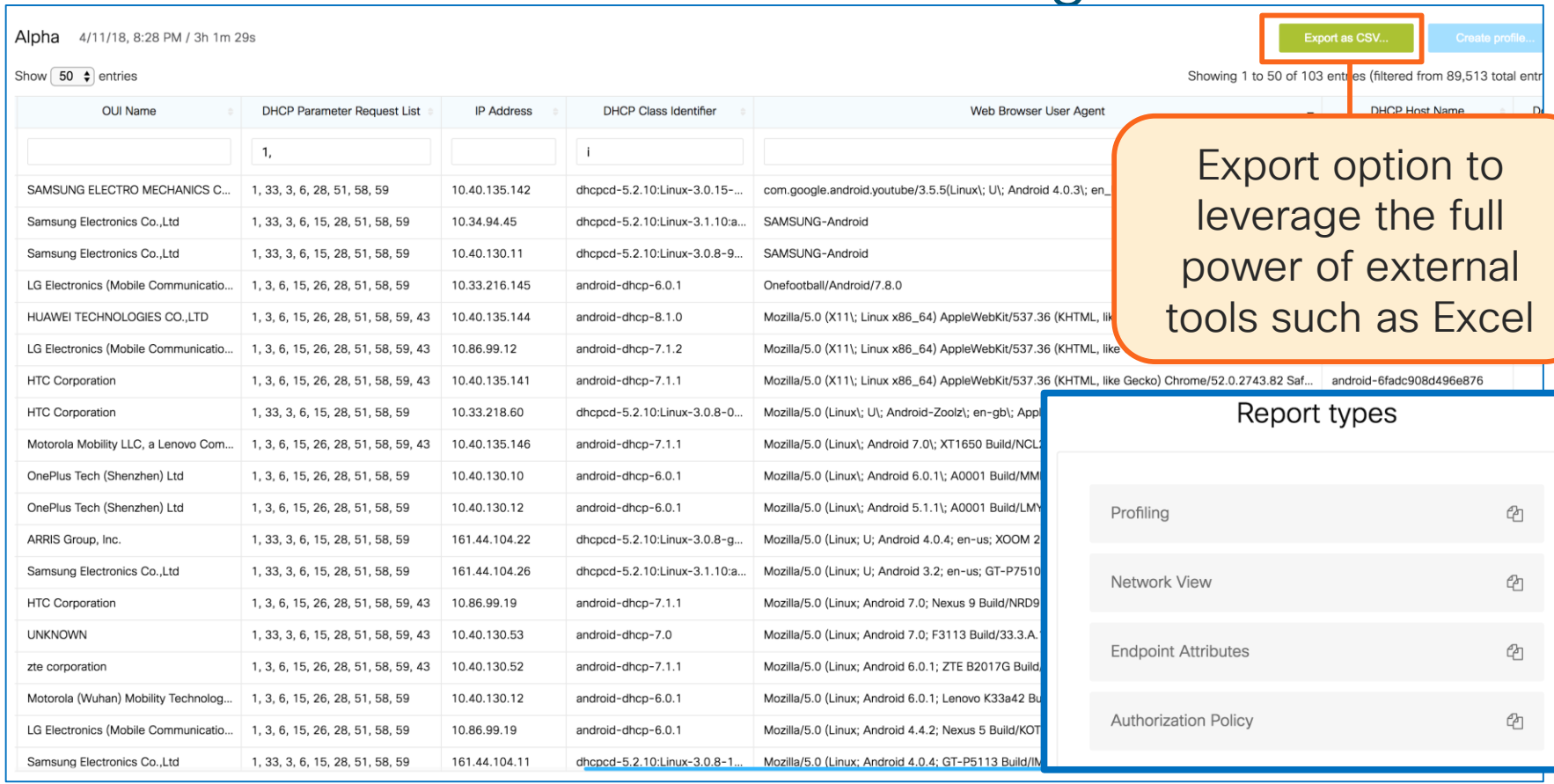


Generating EAT Reports





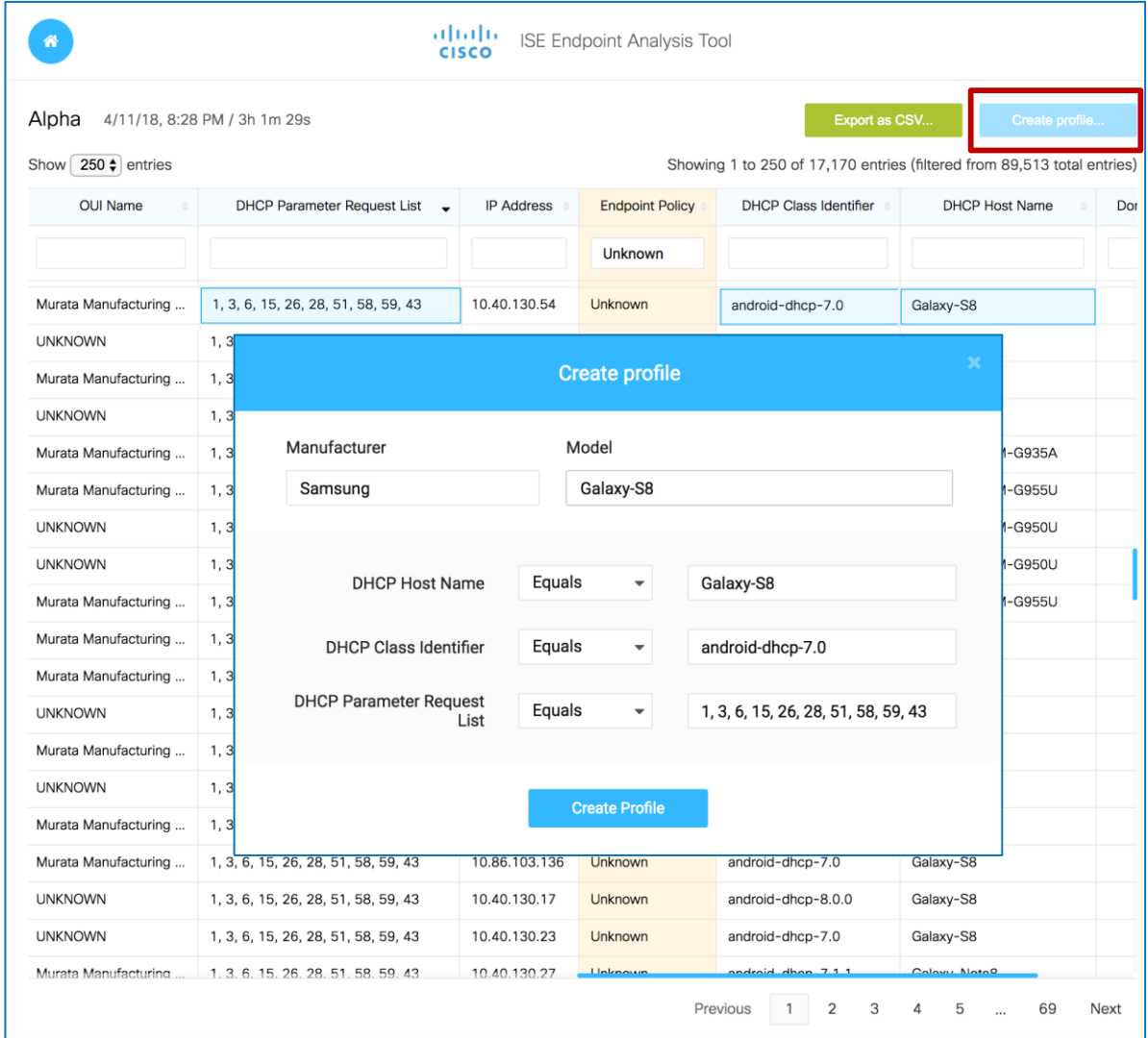
EAT – Embedded Filter and Sorting



EAT

Profile Creation

- Select attributes to be used in new profile and click “Create Profile”
- Option to edit condition criteria before complete.
- Import XML into ISE.
- Advanced profile tuning can be performed inside ISE (change hierarchy, policy name, Scan/CoA actions, etc.)



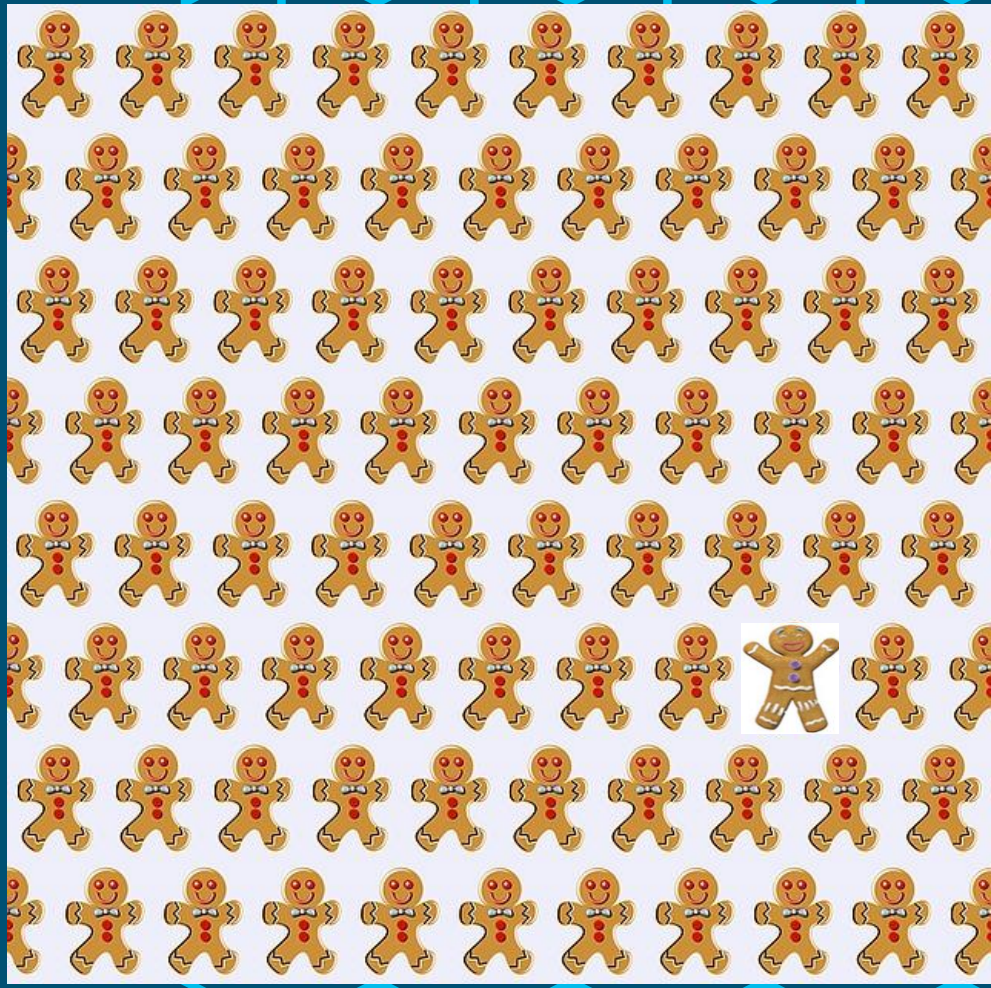
Sample EAT Report (CSV Export)

MACAddress	OUI	MatchedPolicy	dhcp-class-identifier	dhcp-parameter-request-list	operating-system-result	User-Agent
8C:79:67:95:12:9A	zte corporation	Android	dhcpcd-5.5.6		Android	Dalvik/2.1.0 (Linux\; U\; Android 5.1\; Z958 Build/LMY47O)
8C:79:67:B4:B4:68	zte corporation	Android	android-dhcp-7.1.1	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	Android	Mozilla/5.0 (Linux; Android 6.0.1; ZTE B2017G Build/MMB29M; wv) AppleW
A8:A6:68:D9:BA:A8	zte corporation	Android	dhcpcd-5.5.6	1, 33, 3, 6, 15, 28, 51, 58, 59		
D0:5B:A8:30:7A:65	zte corporation	Android	dhcpcd-5.5.6		Android	Dalvik/2.1.0 (Linux\; U\; Android 5.1\; Z958 Build/LMY47O)
D8:55:A3:97:AD:26	zte corporation	Android	dhcpcd-5.5.6		Android	Dalvik/2.1.0 (Linux\; U\; Android 5.1.1\; LS-5504 Build/LMY47V)
D8:55:A3:CA:E6:1B	zte corporation	Android	dhcpcd-5.5.6	1, 33, 3, 6, 15, 26, 28, 51, 58, 59	Android 4.4 KitKat	Dalvik/1.6.0 (Linux\; U\; Android 4.4.2\; Z667T Build/KVT49L)
F8:DF:A8:79:FF:C4	zte corporation	Android	android-dhcp-6.0.1	1, 3, 6, 15, 26, 28, 51, 58, 59		
00:BB:3A:53:F7:DA	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpcd-5.5.6	1, 33, 3, 6, 15, 28, 51, 58, 59	FreeBSD general purpose 8.X	Dalvik/1.6.0 (Linux\; U\; Android 4.4.4\; SD4930UR Build/KTU84P)
00:BB:3A:B8:3A:C9	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpcd-5.2.10		Android 4.0.x Ice Cream Sandwich	Dalvik/1.6.0 (Linux\; U\; Android 4.0.3\; KFTT Build/IML74K)
00:BB:3A:F4:22:EB	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpcd-5.2.10	1, 33, 3, 6, 15, 28, 51, 58, 59	Android 4.0.x Ice Cream Sandwich	Dalvik/1.6.0 (Linux\; U\; Android 4.0.3\; KFTT Build/IML74K)
00:BB:3A:F9:14:5C	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpcd-5.5.6		Android 4.2 Jelly Bean	Dalvik/1.6.0 (Linux\; U\; Android 4.2.2\; SD4930UR Build/JDQ39)
74:75:48:94:D6:26	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpcd-5.5.6	1, 33, 3, 6, 15, 28, 51, 58, 59	Android 4.4 KitKat	Mozilla/5.0 (Linux; A ebKit/53
A0:02:DC:26:82:0C	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpcd-5.5.6		Linksys WET54G wireless bridge	Dalvik/1.6.0 (Linu
A0:02:DC:28:A1:D8	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linu
A0:02:DC:48:71:A1	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpcd-5.5.6	1, 33, 3, 6, 15, 28, 51, 58, 59	Android 4.2 Jelly Bean	Dalvik/1.6.0 (Linu
A0:02:DC:97:F2:0D	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linu
A0:02:DC:9D:60:42	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linu
10:AE:60:13:63:C7	Private	Android-Amazon-Kindle	dhcpcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linu
10:AE:60:69:84:0E	Private	Android-Amazon-Kindle	dhcpcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linu
10:AE:60:DA:B7:0D	Private	Android-Amazon-Kindle	dhcpcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linu
F0:4F:7C:C7:9E:C5	Private	Android-Amazon-Kindle	dhcpcd-5.2.10	1, 33, 3, 6, 15, 28, 51, 58, 59	Android 4.0.x Ice Cream Sandwich	Dalvik/1.6.0 (Linu
F0:A2:25:0C:23:39	Private	Android-Amazon-Kindle	dhcpcd 4.0.15	1, 121, 33, 3, 6, 15, 28, 51, 58, 59, 119	Android 2.3.x Gingerbread	Mozilla/5.0 (Linux BREA
F0:A2:25:4F:E0:D6	Private	Android-Amazon-Kindle			Android 2.3.x Gingerbread	Mozilla/5.0 (Linux; U ERBREA
F0:A2:25:7A:29:26	Private	Android-Amazon-Kindle			Android 2.3.x Gingerbread	Dalvik/1.4.0 (Linux\; U\; Android 2.3.4\; Kindle Fire Build/GINGERBREAD)
F0:A2:25:BF:71:01	Private	Android-Amazon-Kindle			Android 2.3.x Gingerbread	Mozilla/5.0 (Linux; U; Android 2.3.7; md-us; Kindle Fire Build/GRK39F; Cya
F0:A2:25:C9:4F:62	Private	Android-Amazon-Kindle	dhcpcd 4.0.15		Android 2.3.x Gingerbread	Mozilla/5.0 (Linux; U; Android 2.3.4; en-us; Kindle Fire Build/GINGERBREA
F0:A2:25:EC:A7:E8	Private	Android-Amazon-Kindle	dhcpcd 4.0.15		Android 2.3.x Gingerbread	Mozilla/5.0 (Linux; U; Android 2.3.4; en-us; Kindle Fire Build/GINGERBREA
F0:A2:25:EF:82:24	Private	Android-Amazon-Kindle	dhcpcd 4.0.15		Android 2.3.x Gingerbread	Mozilla/5.0 (Linux; U; Android 2.3.4; en-us; Kindle Fire Build/GINGERBREA
08:60:6E:A3:2E:15	ASUSTek COMPUTER INC.	Android-Asus			Android	Android
08:60:6E:AC:24:63	ASUSTek COMPUTER INC.	Android-Asus	dhcpcd-5.5.6			
08:60:6E:AE:ED:A7	ASUSTek COMPUTER INC.	Android-Asus	dhcpcd-5.5.6			
10:BF:48:BF:76:39	ASUSTek COMPUTER INC.	Android-Asus	dhcpcd-5.5.6	1, 33, 3, 6, 15, 26, 28, 51, 58, 59	Android	Android
10:BF:48:BF:8A:C1	ASUSTek COMPUTER INC.	Android-Asus	dhcpcd-5.5.6		Android	android-async-http/1.3.1 (http://loopj.com/android-async-http)
10:BF:48:C1:8B:41	ASUSTek COMPUTER INC.	Android-Asus	dhcpcd-5.5.6	1, 33, 3, 6, 15, 28, 51, 58, 59	Android	Android

Leverage the full power of external tools such as Excel

Anomaly Behavior Detection

There's something suspicious about #58. He's acting a bit too ginger for my liking. We better send a team in to check it out!



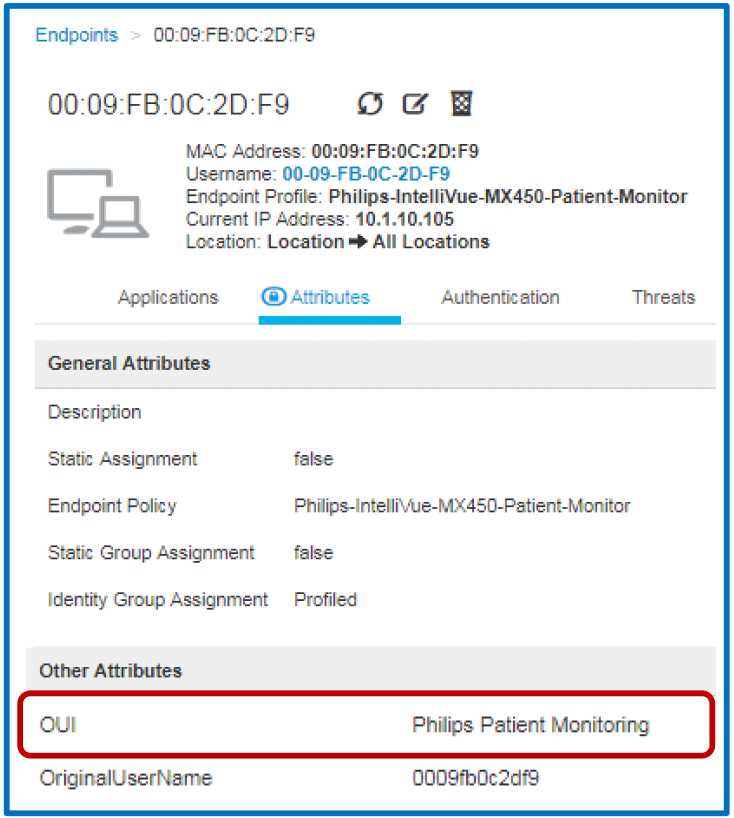
Unveiling the #1 ISE feature to prevent MAC Spoofing!

Authentication

And the #1 method to reduce the impact of a spoofed device...

Principle of Least Privilege

Almost Everything Can Be Spoofed!



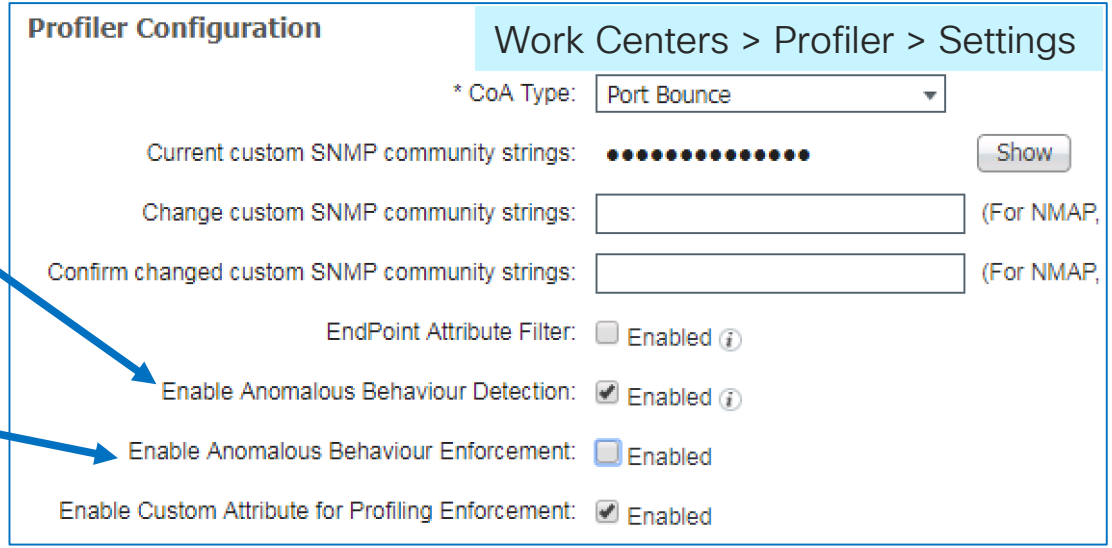
dhcp-class-identifier	PHILIPS IntelliVue MX450 Patient Monitor
dhcp-message-type	DHCPDISCOVER
dhcp-parameter-request-list	1, 28, 2, 121, 15, 6, 12, 40, 41, 42, 26, 119, 3, 249, 33, 252,
dhcp-requested-address	10.1.10.105
host-name	philips-mx450
htype	Ethernet (10Mb)
ifDescr	GigabitEthernet1/0/2
ip	10.1.10.105
lldpCacheCapabilities	S
lldpCapabilitiesMapSupported	S
lldpChassisId	10.1.10.105
lldpPortDescription	Interface 3 as ens33
lldpPortId	00:09:fb:0c:2d:f9
lldpSystemDescription	Linux philips-mx450.cts.local 3.10.0-327.el7.x86_64 #1 SMP
lldpSystemName	philips-mx450.cts.local
lldpUndefined127	00:12:0f:01:03:80:37:00:1e
User-Agent	This is a Philips IntelliVue MX450 Patient Monitor. Do not argue with the facts!

ISE Anomalous Behavior Detection (ABD)

- ISE 2.2 introduced Phase 1 of ISE Anomalous Behavior Detection
- Goal of Phase 1:
  - Monitor endpoint attributes collected from ISE Profiler and detect most common cases of conflicting behavior, as may result from a basic MAC Spoofing attempt.

Enable Anomaly Behavior Detection (Visibility Only)

Trigger Enforcement for endpoints flagged anomalous

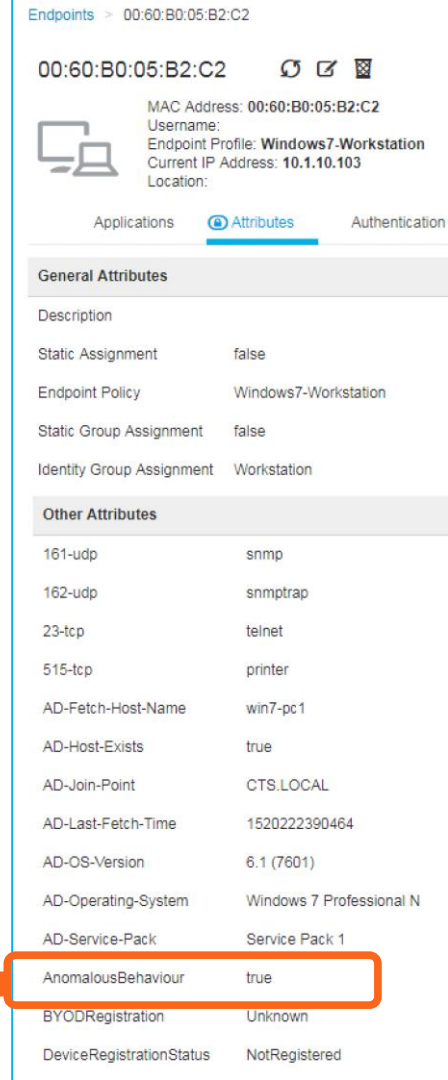


Which Behavior is Deemed Anomalous?

- ISE ABD Phase 1 rules check for the following basic indicators of anomalous behavior:
  1. Any change in DHCP-Class-Id (Option 60)
  2. Any change in RADIUS NAS-Port-Type between Wired and Wireless
  3. Change in profile from ‘printer’ or ‘phone’ to ‘workstation’.
- If endpoint MAC matches any of the above rules, it is flagged Anomalous
- If Enforcement enabled, CoA triggered on endpoint session.

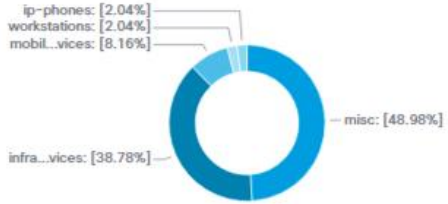
Enable Anomalous Behaviour Enforcement: ☑ Enabled

AnomalousBehaviour true



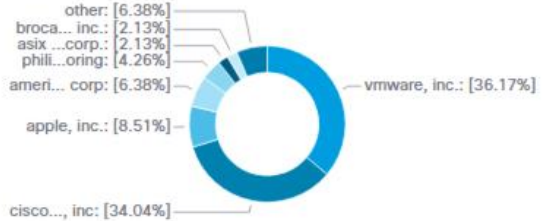
ENDPOINTS

Type | Profile



ENDPOINT CATEGORIES

OUI | OS Types | Identity Group



NETWORK DEVICES

Location | Type | Device Name

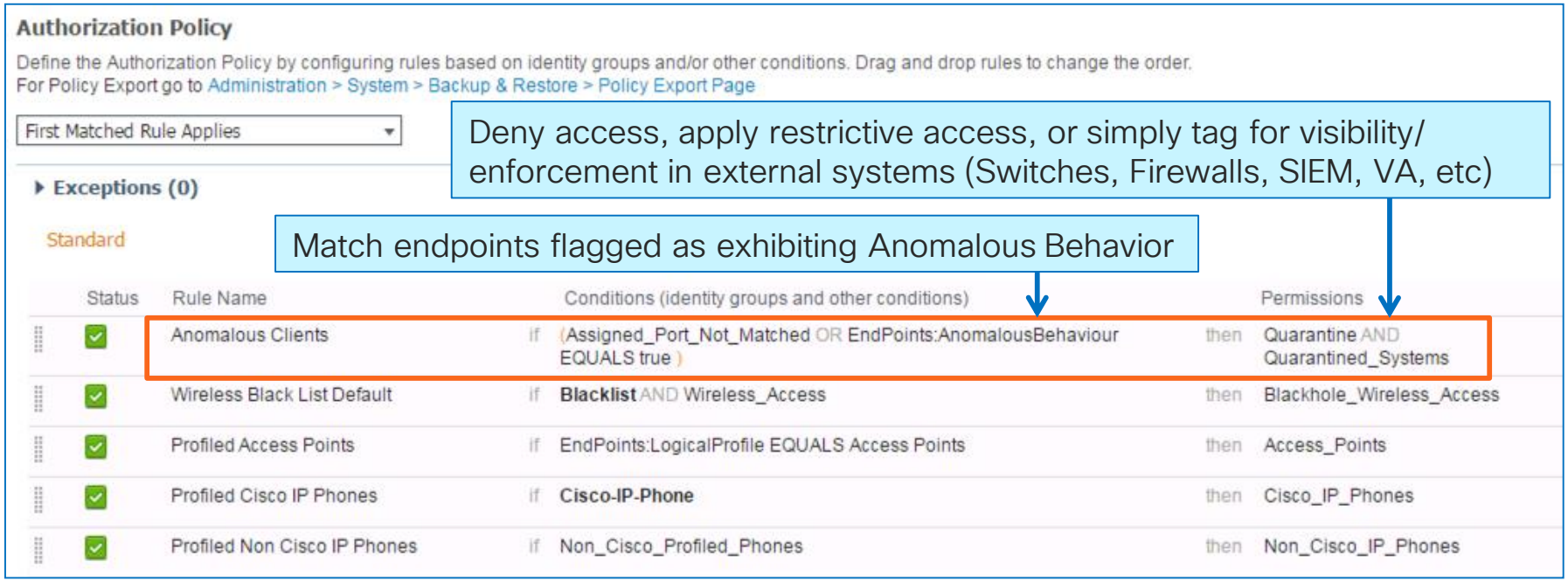
Rows/Page 10 | 1 / 5 | Go | 49 Tot

ANC | Change Authorization | Clear Threats & Vulnerabilities | Export | Import | MDM Actions | Release Rejected | Revoke Certificate | Filter

MAC Address	OUI	Anomalous Behavior	IPv4 Address	Hostname	Endpoint Profile	Logical Profile	OS Types
00:00:0C:FF:ED:B1	Cisco Systems, Inc		172.16.1.66		Cisco-Device		
00:0B:45:B2:47:C0	Cisco Systems, Inc				Cisco-Switch		
00:09:5C:11:22:44	Philips Medical System...	true	10.1.10.102	win7-pc	Philips-Medical-Systems-Cardiac-Monito...	Medical Devices	Windows 7 Profession...
00:09:FB:0C:2D:F8	Philips Patient Monitori...		10.1.101.240	S8MX450	Philips-Patient-Monitoring-Device	Medical Devices	
00:09:FB:0C:2D:F9	Philips Patient Monitori...		10.1.10.105	philips-mx450	Philips-Patient-Monitoring-Device		

Authorization Policy Example

Optional: Dynamically Re-Authorize Anomalous Endpoints with New Access Policy



ABD Considerations/Caveats

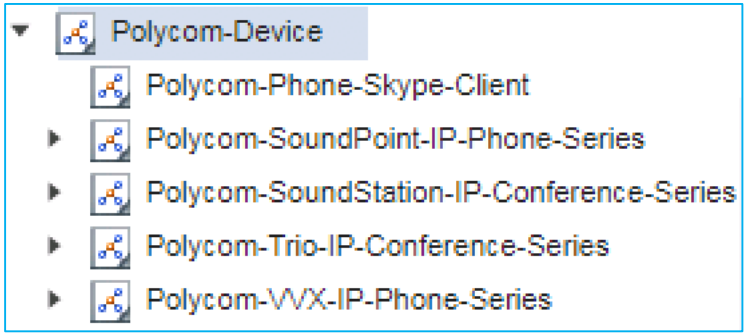
- Once flagged, currently the only option to clear flag is to Delete the endpoint!
- Profiling / ABD is NOT an exact science. Expect false positives. Examples:
  - **PXE-Boot clients:** DHCP-Class-Id starts as “PXEClient:Arch:...” upon initial boot, and then switches to new value when boots off new image.
  - **Skype/Lync clients:** DHCP-Class-Id communicated as expected (for example, a phone device as “Polycom” or Windows workstation as “MSFT 5.0”, then later DHCP Inform searches for Communication Server address and sends “MS-UC-Client” in DHCP-Class-Id.
- Class-Id changes work well for Windows Workstations but are hit-and-miss for Mac OS and Linux.

Example Workarounds for ABD False Positives

- Example 1

Rule Name	Conditions	Permissions	SGT
ABD Exception	EndpointsAnomalousBehaviour=true **AND** Endpoints:EndpointProfile = Polycom-Device	Phone-Access	Inspect
ABD Quarantine	EndpointsAnomalousBehaviour=true	Quarantine	Quarantine
IP-Phones	Endpoints:LogicalProfile = IP-Phones	Phone-Access	Voice

- Example 2
  - Apply new Polycom Profile Pack so that all legitimate Polycom devices match more specific policy; limit access to generic Polycom-Device.
- Example 3
  - Block DHCP Informs from reaching ISE PSNs!



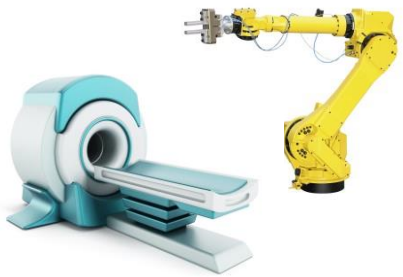
Mac OS Workstation Example

Original Endpoint Attributes		Post-Spoof Attributes	
OUI	Cisco Systems, Inc	OUI	Cisco Systems, Inc
		EndPointPolicy	Cisco-IP-Phone-7975
		Total Certainty Factor	255
		User-Name	CP-7975G-SEP00235E17FDB3
		cdpCacheCapabilities	H;P;M
		cdpCacheDeviceId	SEP00235E17FDB3
		cdpCachePlatform	Cisco IP Phone 7975
		cdpCacheVersion	SCCP75.9-3-1ES27S
		dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7975G
		dhcp-client-identifier	01:00:23:5e:17:fd:b3
dhcp-message-type	DHCPREQUEST	dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35	dhcp-parameter-request-list	1, 3, 6, 15, 119, 95, 252, 44, 46
dhcp-requested-address	10.13.1.204	dhcp-requested-address	10.10.1.103
host-name	SEP00235E17FDB3	host-name	chyps-macbookpro
Net New, but insufficient to change profile		User-Agent	Mac OS X/10.8.5 (12F45)

- ISE Profiler *adds/merges* attributes. It does not clear attributes with null values nor delete previously learned attributes.
- Mac OS client did not populate DHCP-Class-Id, so no change to attribute and ABD not triggered.
- No profile change occurred due to pre-existing attributes, so again, ABD not triggered.

Using Exception Actions to Detect and Quarantine Anomalous Endpoints

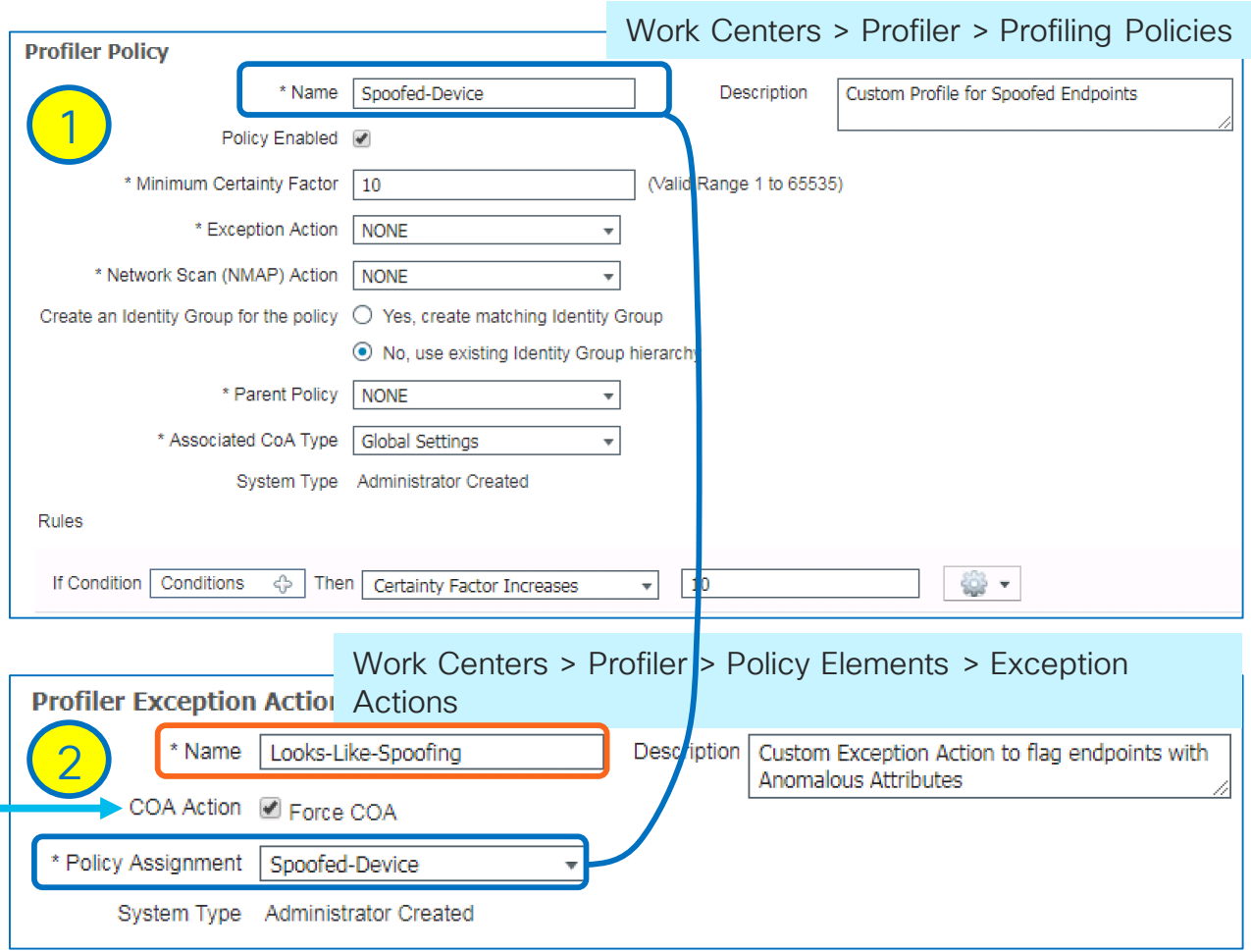
- What is a Profiling Exception Action?
  - An Exception Action allows an endpoint to be statically mapped to a new profile policy with optional CoA.
- Requirements to trigger Exception Action (EA)
  - Endpoint must match the profile policy where EA configured.
  - Endpoint must match the condition which triggers EA.
- Two useful cases for Exception Actions:
  1) Lock critical device to a policy once profile matched.
  2) Trigger policy action when conflicting attributes detected for given endpoint (Ex: presence of unexpected attributes)



Configuring Exception Actions

- Step 1 – Create a new Profile Policy – no rules required.
- Step 2 – Create a new Exception Action that assigns the new policy from Step 1.

  Check “Force CoA” to trigger immediate policy enforcement.



Mac OS Workstation Example

Original Endpoint Attributes

OUI	Cisco Systems, Inc
EndPointPolicy	Cisco-IP-Phone-7975
Total Certainty Factor	255
User-Name	CP-7975G-SEP00235E17FDB3
cdpCacheCapabilities	H;P;M
cdpCacheDeviceId	SEP00235E17FDB3
cdpCachePlatform	Cisco IP Phone 7975
cdpCacheVersion	SCCP75.9-3-1ES27S
dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7975G
dhcp-client-identifier	01:00:23:5e:17:fd:b3
dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35
dhcp-requested-address	10.13.1.204
host-name	SEP00235E17FDB3

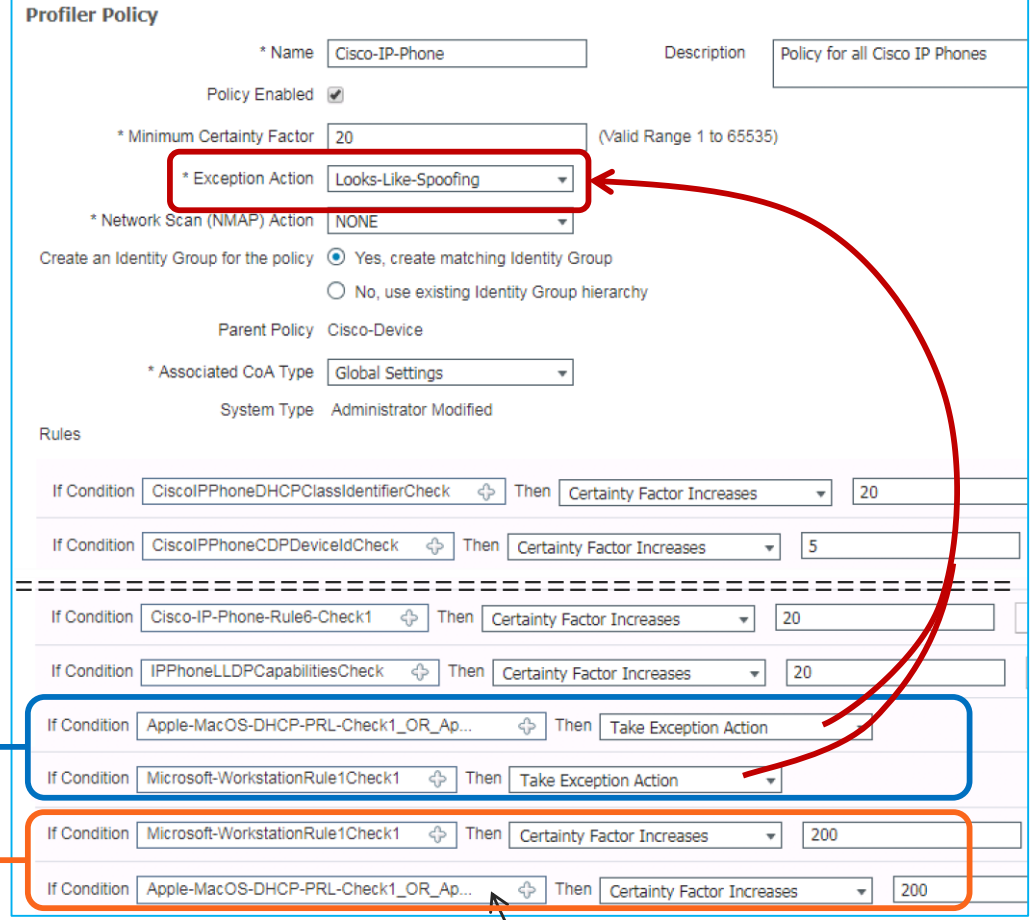
Post-Spoof Attributes

OUI	Cisco Systems, Inc
EndPointPolicy	Cisco-IP-Phone-7975
Total Certainty Factor	255
User-Name	CP-7975G-SEP00235E17FDB3
cdpCacheCapabilities	H;P;M
cdpCacheDeviceId	SEP00235E17FDB3
cdpCachePlatform	Cisco IP Phone 7975
cdpCacheVersion	SCCP75.9-3-1ES27S
dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7975G
dhcp-client-identifier	01:00:23:5e:17:fd:b3
dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 3, 6, 15, 119, 95, 252, 44, 46
dhcp-requested-address	10.10.1.103
host-name	chyps-macbookpro
User-Agent	Mac OS X/10.8.5 (12F45)

Exception Actions

Phone Profile Example

- Step 3 – To base or child policy, add conditions deemed anomalous.
- In this example, DHCP attributes unique to Windows and Mac OS workstations are added to an IP phone profile (a common and accessible IoT endpoint in the workplace.)
- Conditions are configured to:
  1. Trigger the named exception action “Looks-Like-Spoofing”
  2. Increase Certainty Factor (likelihood profile will continue to match)



3

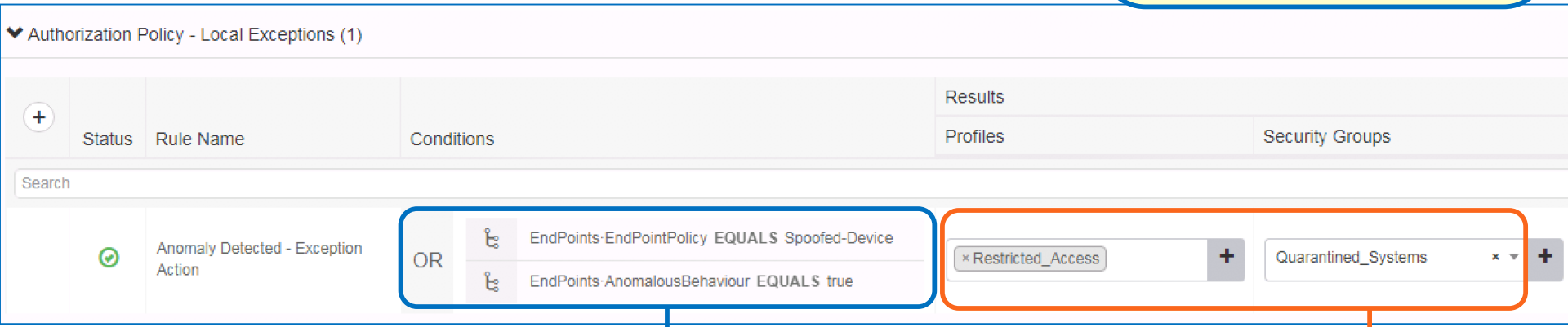
Apple-MacOS-DHCP-PRL-Check1	Administrator Created	dhcp-parameter-request-list EQUALS 1, 3, 6, 15, 119, 95, 252, 44, 46
Apple-MacOS-DHCP-PRL-Check2	Administrator Created	dhcp-parameter-request-list EQUALS 1, 121, 3, 6, 15, 119, 252, 95, 44, 46
Apple-MacOS-DHCP-PRL-Check3	Administrator Created	dhcp-parameter-request-list EQUALS 1, 3, 6, 15, 119, 95, 252, 44, 46, 47

Match Apple MacOS DHCP PRL Check 1 or 2 or 3

Exception Action Enforcement

- Step 4 – When CoA triggered on Exception Action, match on new rule for suspect endpoint

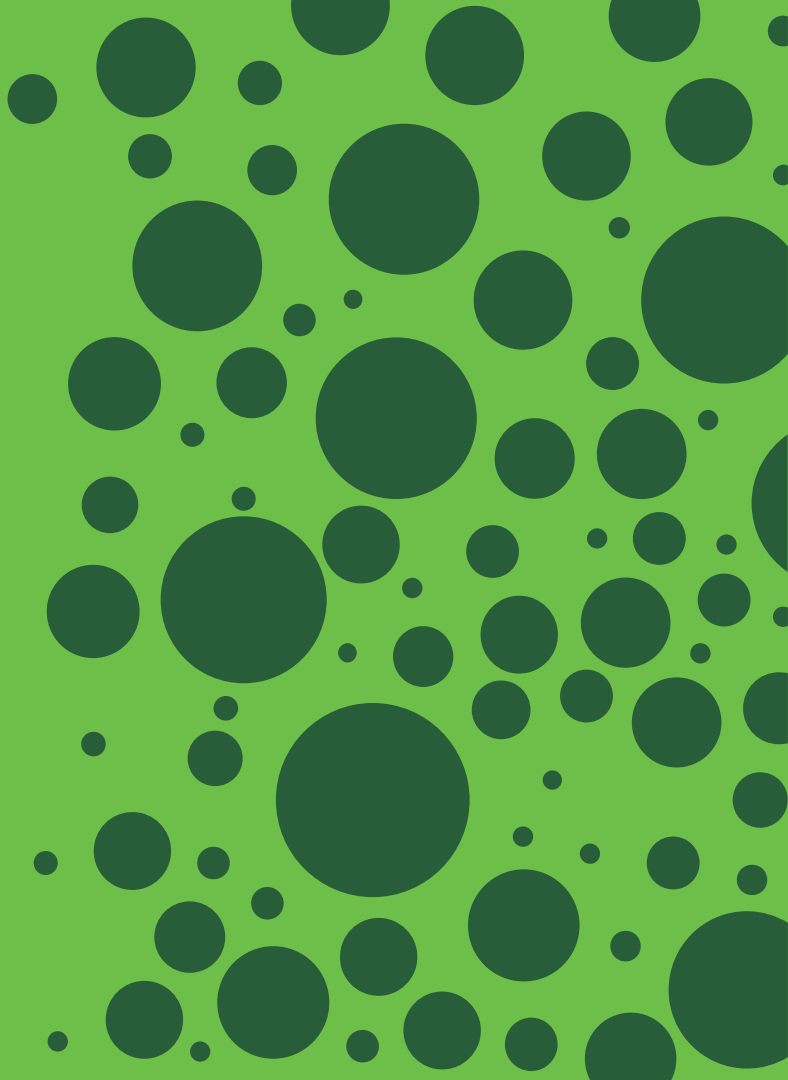
Once issue addressed, unlike ABD flags, Exception Action assignments can be easily removed by deleting static assignment in Admin UI or via ERS API



In above example, Anomalous Behavior Detection is combined with Exception Actions for broader coverage.

Restricted access is optional; policy may simply flag endpoints for closer inspection via Security Group Tags

ISE Posture Best Practices



Agenda

- Client Types and Selection
- First-Time Setup Checklist
- Phased Approach to Posture
- Posture Discovery

ISE Posture Agent Options

	Temporal Stealth Agent	Temporal Agent	AnyConnect Stealth Agent	AnyConnect Agent
Use Case	Discovery stage; pre-production or proof-of-concept	Temporary User: Visitor, Short-Term Contractor	Long-Term User: Employee, Long-Term Contractor	Long-Term User: Employee, Long-Term Contractor
User Interaction	None	Each connection	Minimal/None	Fully Interactive
Install Rights Required	Uses saved Admin credentials in ISE	No admin rights required	Admin rights for initial install only	Admin rights for initial install only
Provisioning	Standalone ISE deployment only; no user interaction	During each new client connection	During initial connection, direct portal, or software distribution app	During initial connection, direct portal, or software distribution app
Remediation	None–Visibility Only	Manual Only	Automatic Only	Manual or Automatic

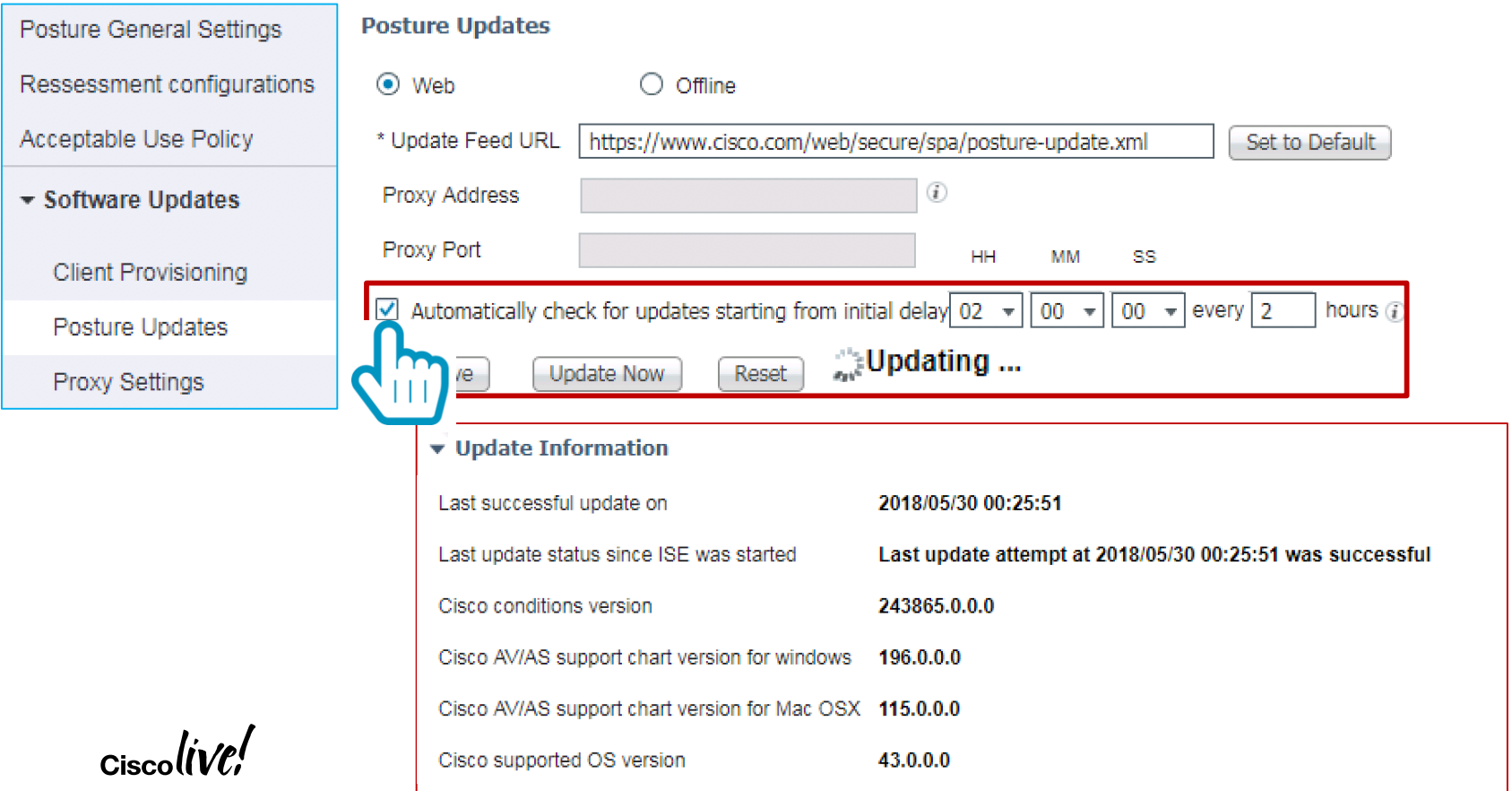
First-Time Posture Checklist

What to do First!

1. Global Setup
   - Update Posture Settings
   - Download Software/Posture Updates
2. Add/Configure Client Provisioning Resources
3. Use Default Client Provisioning Policies or Add New Policies
4. Enable Default Posture Policies or Build New Posture Policies
5. Enable Default Authorization Policy Rules for Posture or Configure New Policies

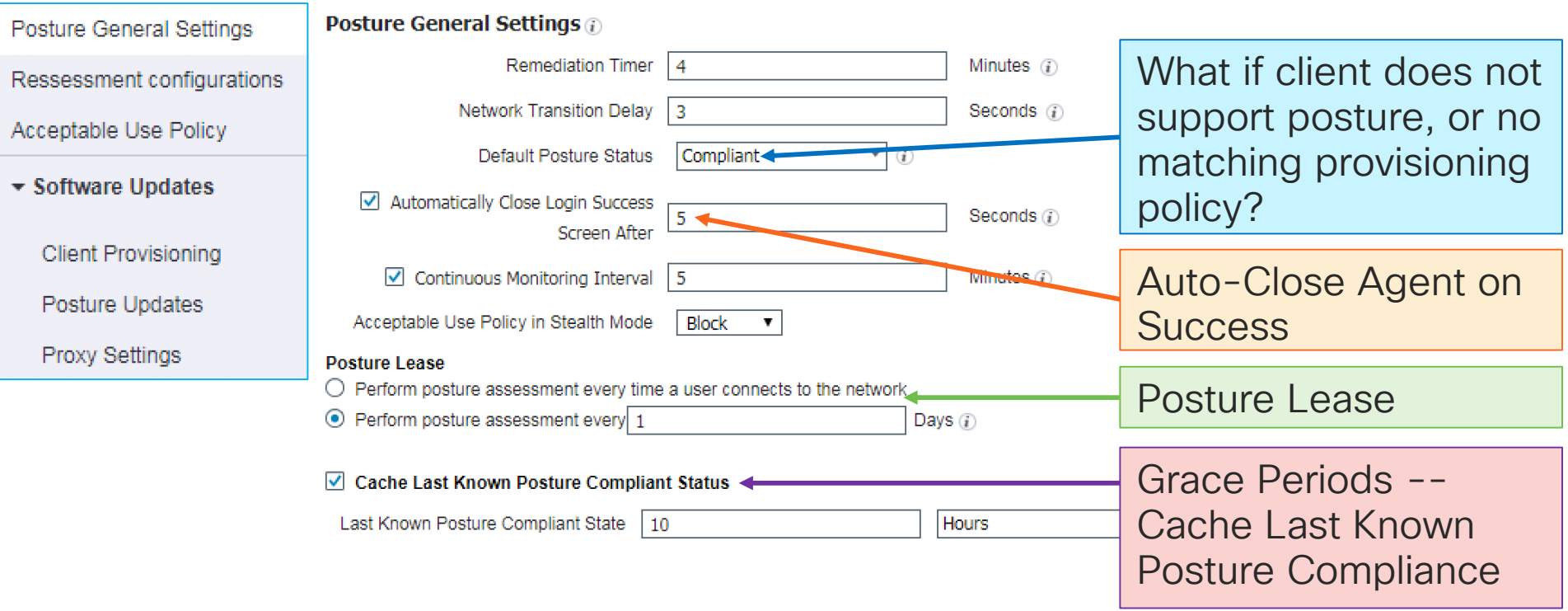
Global Settings – Posture Updates

Work Centers > Posture > Settings > Software Updates > **Posture Updates**



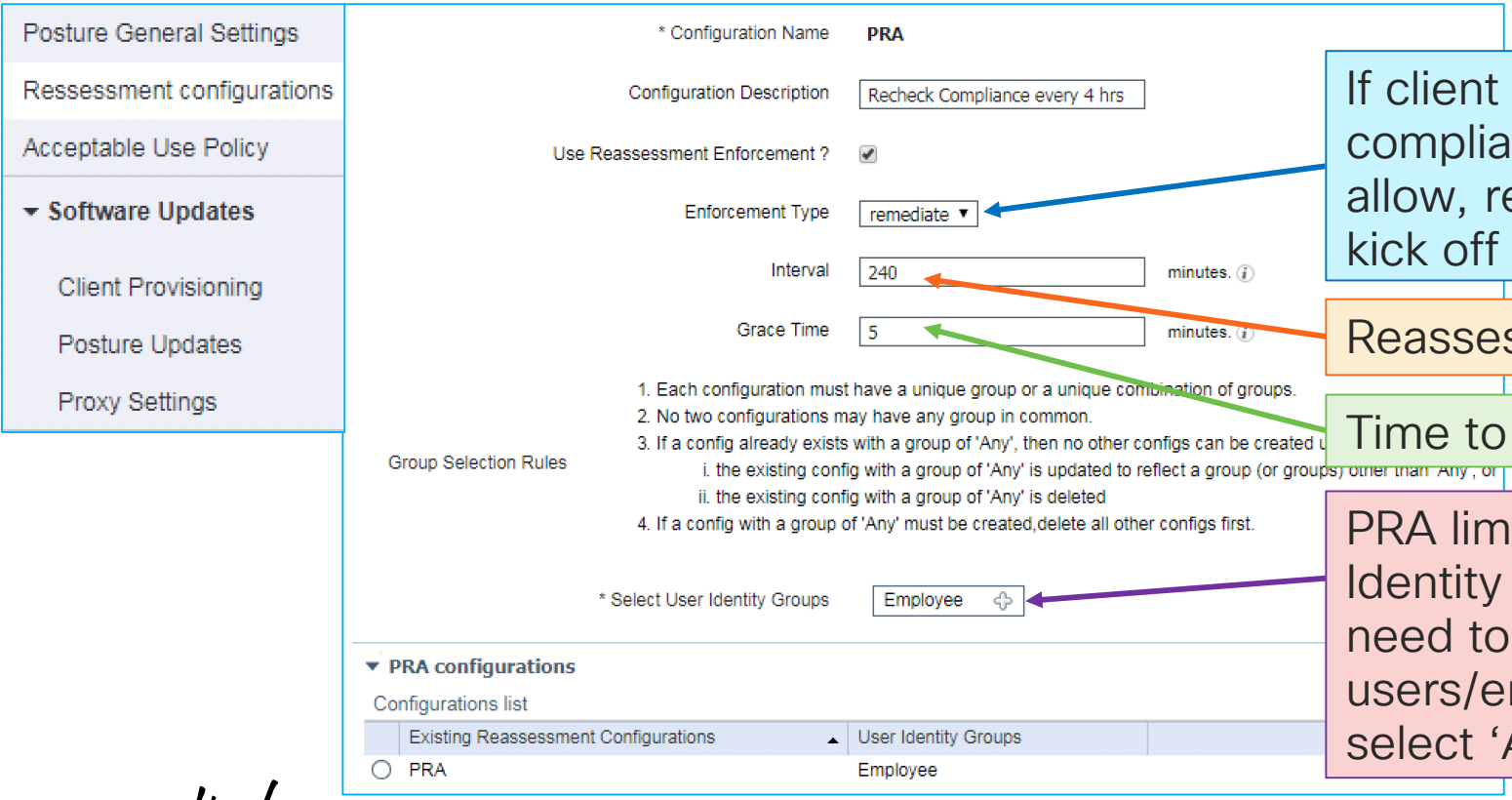
Posture General Settings

Work Centers > Posture > Settings > **Posture General Settings**



Passive Re-Assessment (PRA)

Work Centers > Posture > Settings > **Reassessment configurations**



If client no longer compliant on rescan, allow, remediate, or kick off network?

Reassessment interval

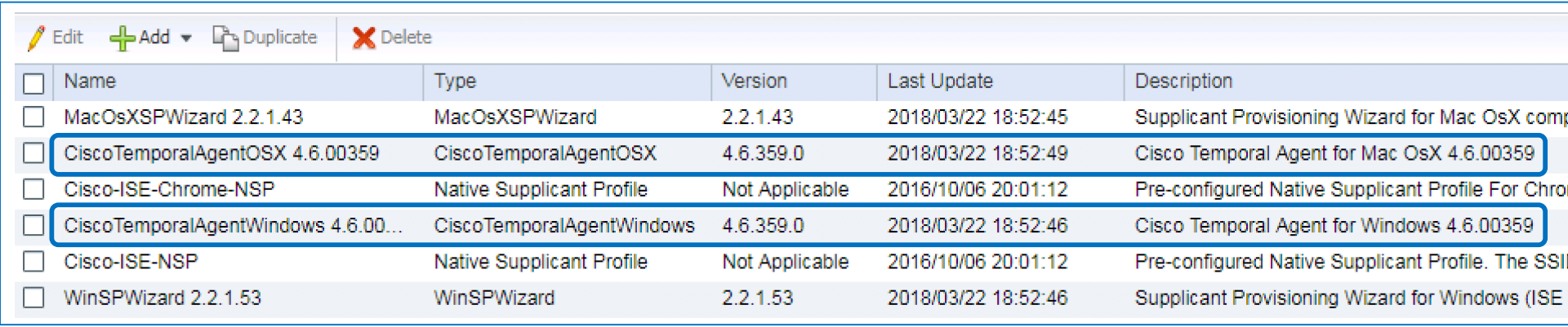
Time to remediate

PRA limited to ISE Identity Groups. If need to apply to all users/endpoints, then select ‘Any’

Populate Required Client Provisioning Resources

Work Centers > Posture > Client Provisioning > Resources

- Some software like full AnyConnect Agent must be downloaded from Cisco Software Center and uploaded into ISE.
- Other software can be auto-populated, downloaded/created offline and uploaded, or created directly within ISE.
- AnyConnect Temporal Agents are pre-loaded in ISE 2.3+



Name	Type	Version	Last Update	Description
MacOsXSPWizard 2.2.1.43	MacOsXSPWizard	2.2.1.43	2018/03/22 18:52:45	Supplicant Provisioning Wizard for Mac OsX comp
CiscoTemporalAgentOSX 4.6.00359	CiscoTemporalAgentOSX	4.6.359.0	2018/03/22 18:52:49	Cisco Temporal Agent for Mac OsX 4.6.00359
Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/10/06 20:01:12	Pre-configured Native Supplicant Profile For Chro
CiscoTemporalAgentWindows 4.6.00...	CiscoTemporalAgentWindows	4.6.359.0	2018/03/22 18:52:46	Cisco Temporal Agent for Windows 4.6.00359
Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/10/06 20:01:12	Pre-configured Native Supplicant Profile. The SSI
WinSPWizard 2.2.1.53	WinSPWizard	2.2.1.53	2018/03/22 18:52:46	Supplicant Provisioning Wizard for Windows (ISE

AnyConnect Cocktail Mix

Mandatory Ingredients

1. Add together:
   - 1 part AnyConnect Secure Mobility Client v4.x
   - 1 part AC/ISE Compliance Module v4.x
   - 1 part AnyConnect Profile
2. Shake into single AnyConnect Configuration Package
3. Serve with your favorite Client Provisioning Policy Rule

Optional Ingredients per Taste

- Profiles for VPN, NAM, Web Security, AMP, NVM, Umbrella, Customer Experience
- Localization and Customization Bundles

Software Center: https://software.cisco.com/download/home/283000185

Don't forget to add ISE !!!

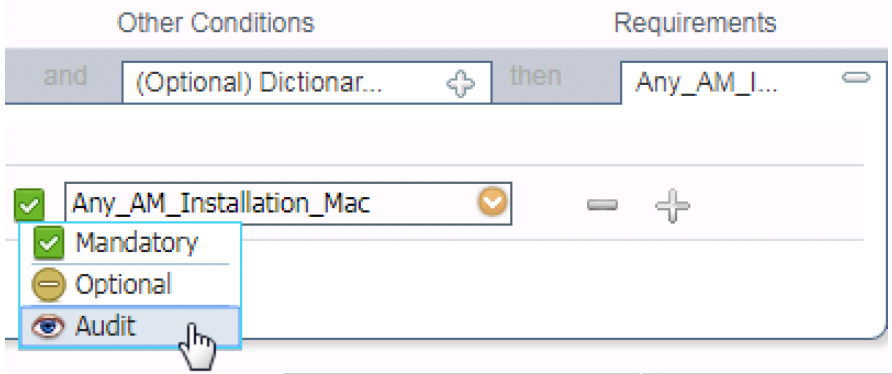
Phased Approach to Posture/Compliance

Don't Swallow the Entire Watermelon at Once

- Enable "Visibility Only" Policies with Temporal or Persistent Agents – No remediation
- Enable Posture Policies as Optional or in Audit Mode.
- Start small in terms of # items checked assessed.
- Start off with specific target devices, users, or locations.
- Enable Posture Lease to extend compliance status after initial check.
- When move to enforcement, implement Grace Periods.
- Gradually increase coverage and enforcement as needed.

Deploy and Verify Posture Policies

Enable Posture in Production with Minimal Impact

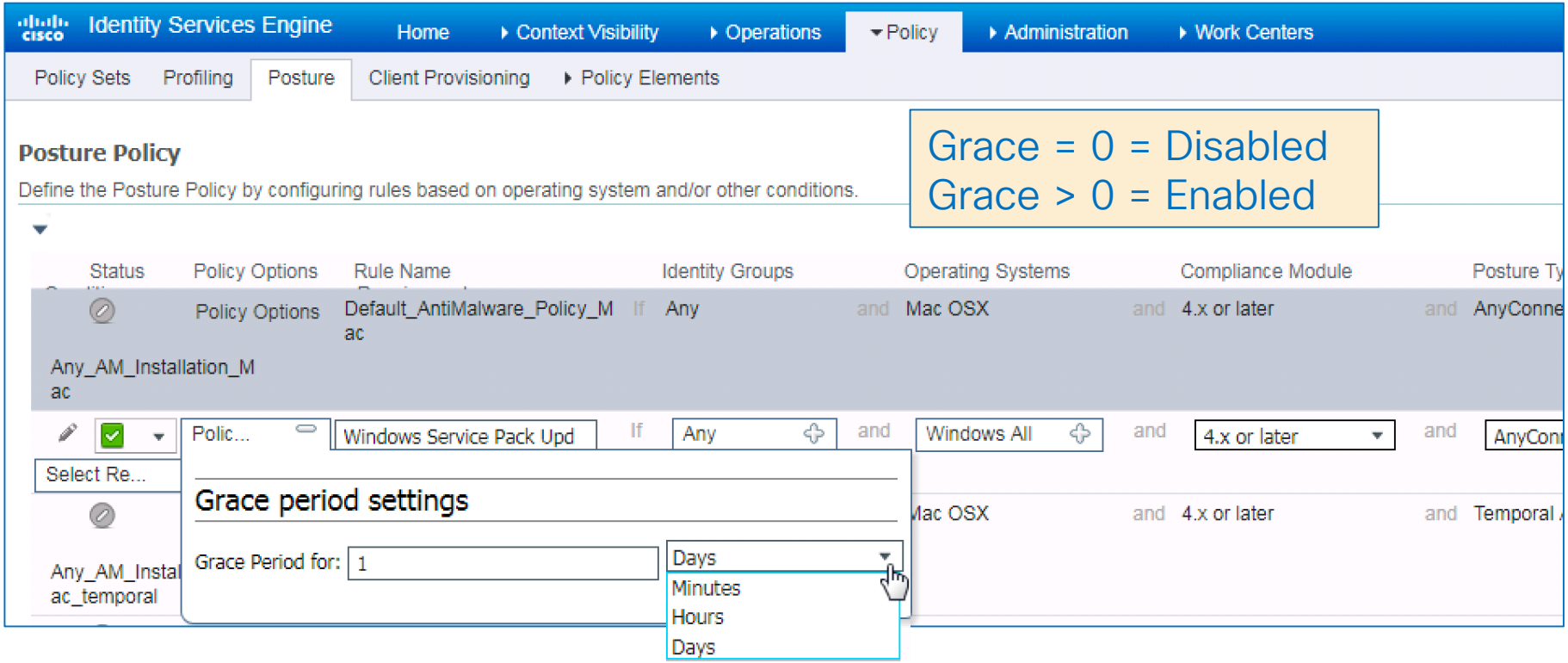


- To limit impact, Posture requirement can be set to Optional or Audit

Requirement Type	Description
Mandatory	User is notified of failure results and given a remediation timer to make corrective action to comply with the posture policy
Optional	User is notified of failure results and given the option to continue in order to bypass the posture assessment policy
Audit	User is not notified of any failure results based on posture assessment policy

Posture Enhancements

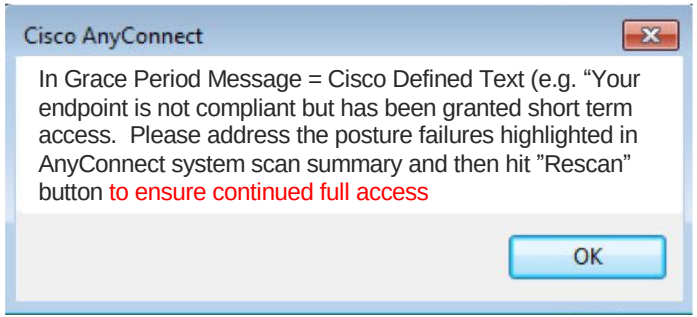
Grace Periods

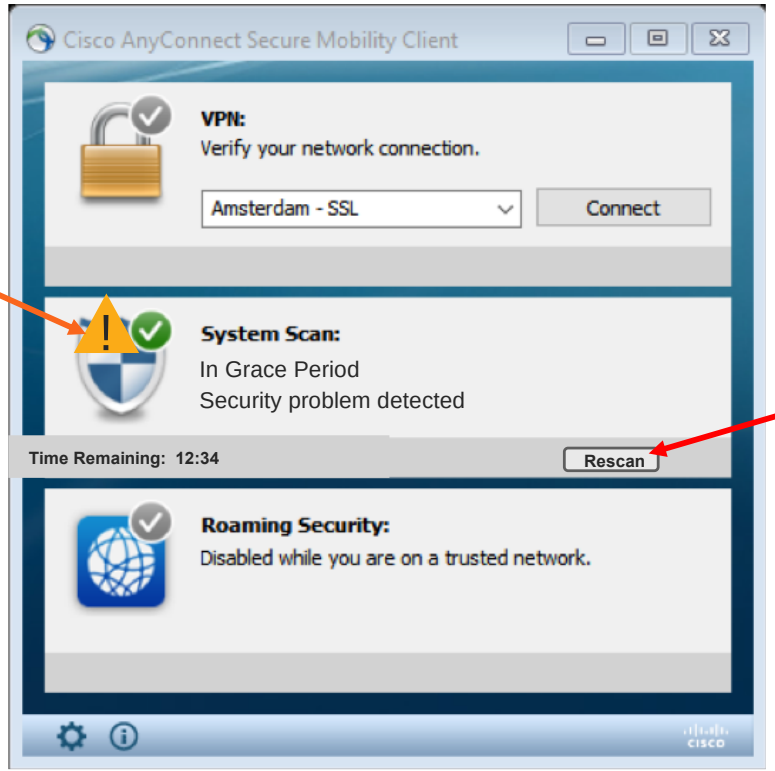


Grace Period and Remediation

Rescan allows ad-hoc posture assessment

Warning Icons with Appropriate Message

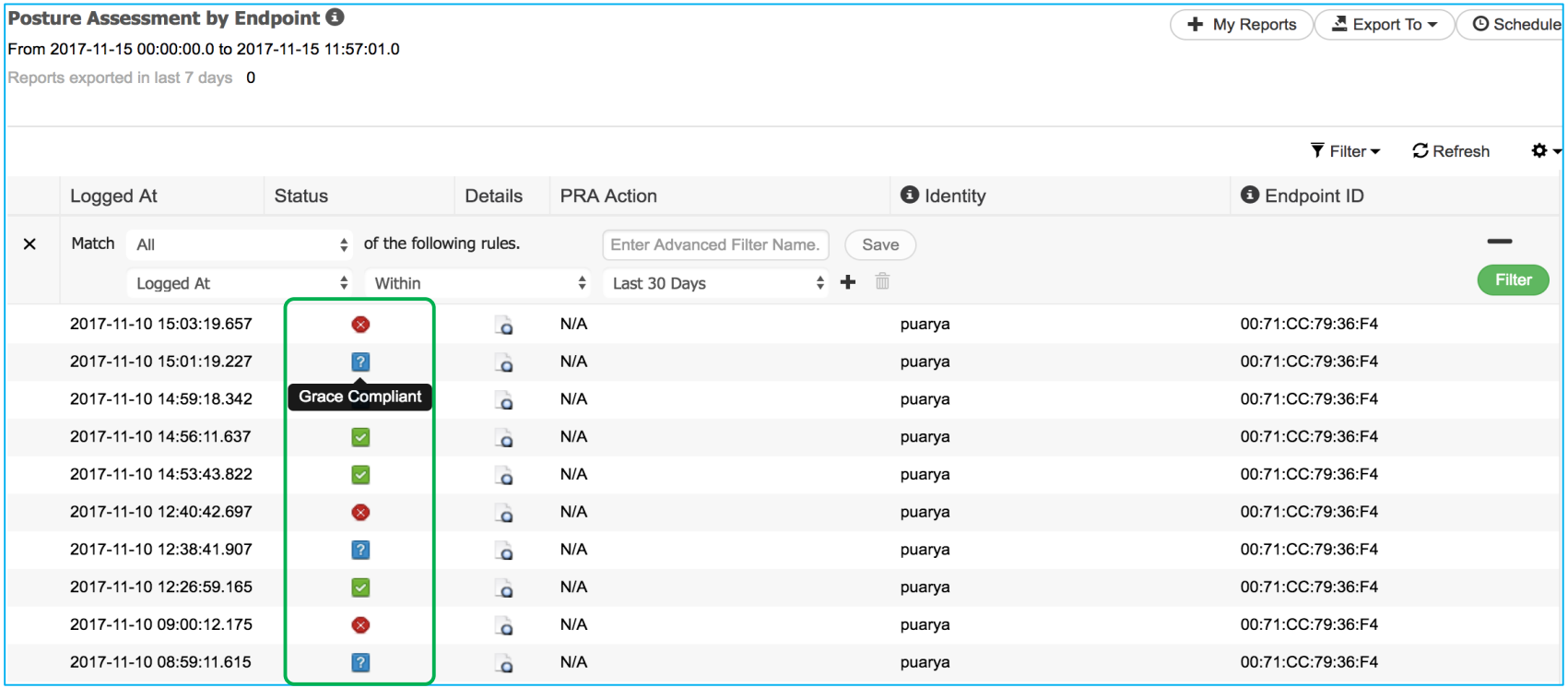




- Persistent Rescan button.
- Admin option to enable/disable
- Off by default for backwards compatibility

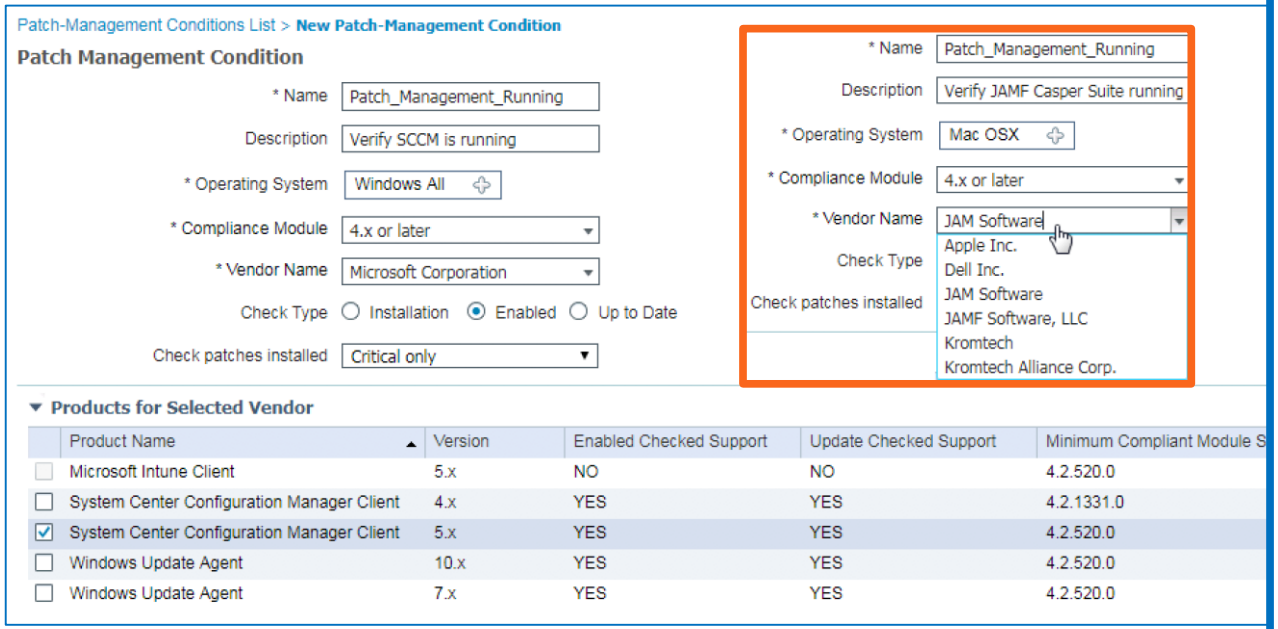
Design posture policies

Reports for Grace Period -- ‘Grace Compliant’



Alternative Approaches to Full ISE Compliance Assessment and Remediation

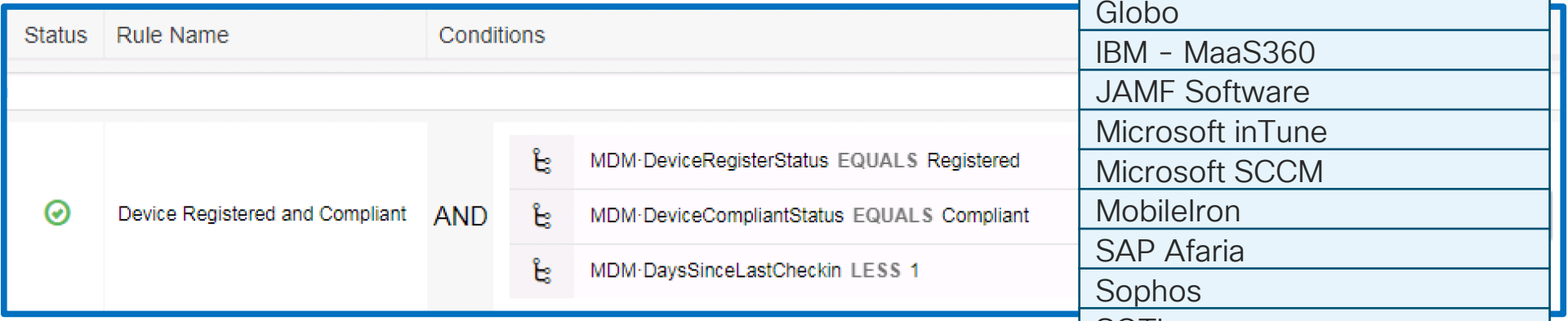
- Simply Check if Patch Management Installed/Running



BMC Software, Inc.
CSIS Security Group
Dell Inc.
F-Secure Corporation
G Data Software AG
GFI Software Ltd.
IBM Corp.
Innovative Solutions
Kaspersky Lab
LANDESK Software, Inc.
Lumension Security, Inc.
McAfee, Inc.
Megaify Software Co., Ltd.
Microsoft Corporation
Norman AS
Secunia
Shavlik Technologies, LLC
Smart PC Solutions, Inc
Symantec Corporation
ThreatTrack Security, Inc.
VMware, Inc.

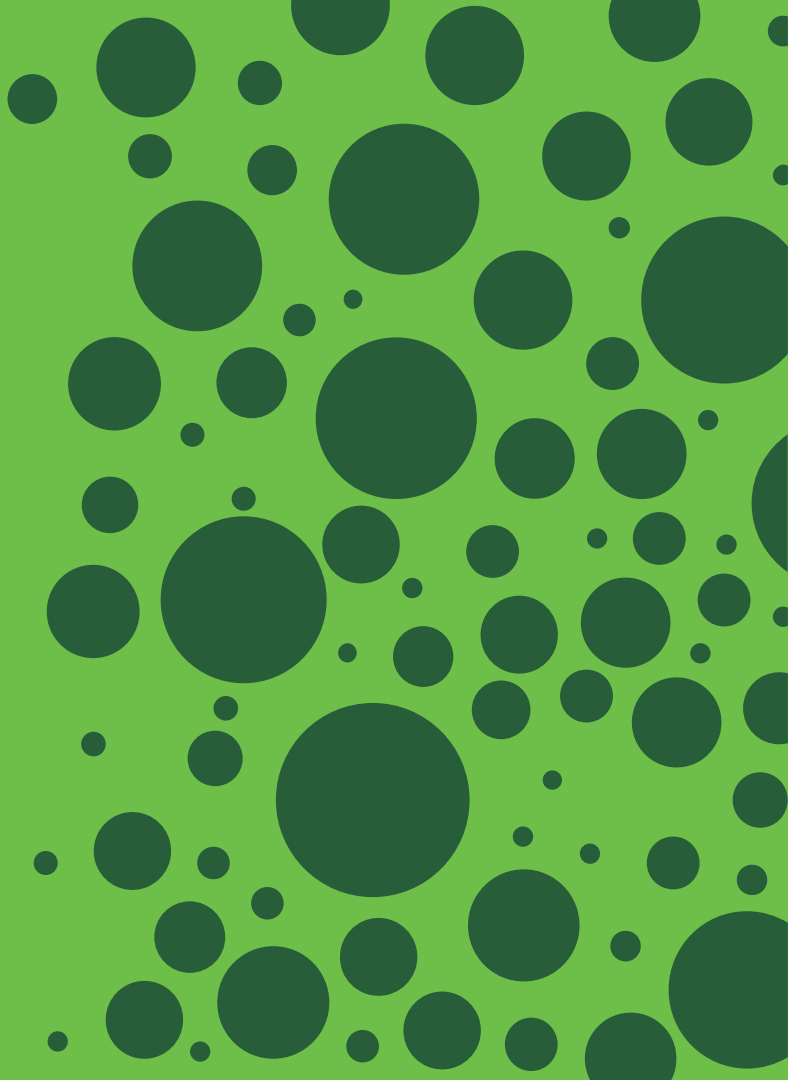
Alternative Approaches to Full ISE Compliance Assessment and Remediation

- Is Device Registered/Compliant per External Device Manager/MDM?
- When did device last check in?



MDM/DM Integrations
Absolute
AirWatch
Blackberry – BES
Blackberry – Good Secure EMM
Citrix Xenmobile
Globo
IBM – MaaS360
JAMF Software
Microsoft inTune
Microsoft SCCM
MobileIron
SAP Afaria
Sophos
SOTI
Symantec
Tangoe
Meraki EMM

Posture Discovery



AC Posture Discovery

Review

Parallel Probing (Behavior **Prior to** ISE 2.2/AnyConnect 4.4)

Is the endpoint on the ISE network?	✓

Note: Discovery Host should NOT be a PSN, but IP reachable target which intercepts NAD

Redirection is the ONLY supported method for initial discovery!

- **Default Gateway of primary interface.**
  Such as 10.86.116.1, /auth/discovery, redirection expected.
- **Discovery Host**
  If it was set in the agent profile ISEPostureCFG.xml
  /auth/discovery, redirection expected
- **enroll.cisco.com**
  hard coded
  /auth/discovery, redirection expected
- **Previously connected head-ends**
  From ConnectionData.xml
  No redirection expected

AnyConnect PSN Node Discovery

Phased Discovery

Parallel Probing

AC 4.4

ISE 2.2

Sequential Probing

Phase 1

Default Gateway of primary interface.
Such as 10.86.116.1, (/auth/discovery, redirection expected)

Discovery Host
If it was set in the agent profile ISEPostureCFG.xml
(/auth/discovery, redirection expected)

enroll.cisco.com
hard coded
(/auth/discovery, redirection expected)

Previously connected PSNs
From ConnectionData.xml
No redirection expected

Phase 2

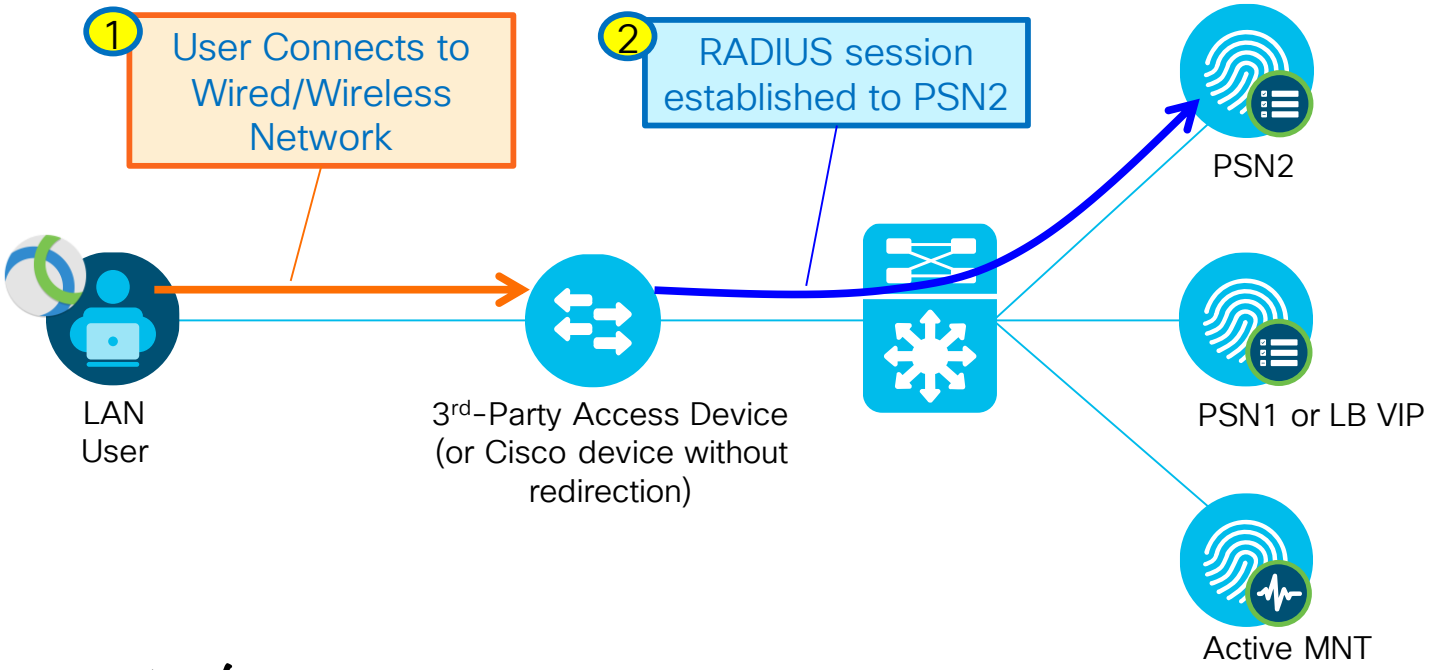
Packets to a "Call Home" list (inc. VIP of LB)
(ISEPostureCFG.xml (no redirection–MnT lookup if needed)

Previously connected PSNs
ConnectionData.xml (no redirection–MnT lookup if needed)

enroll.cisco.com
hard coded (no redirection–MnT lookup if needed)

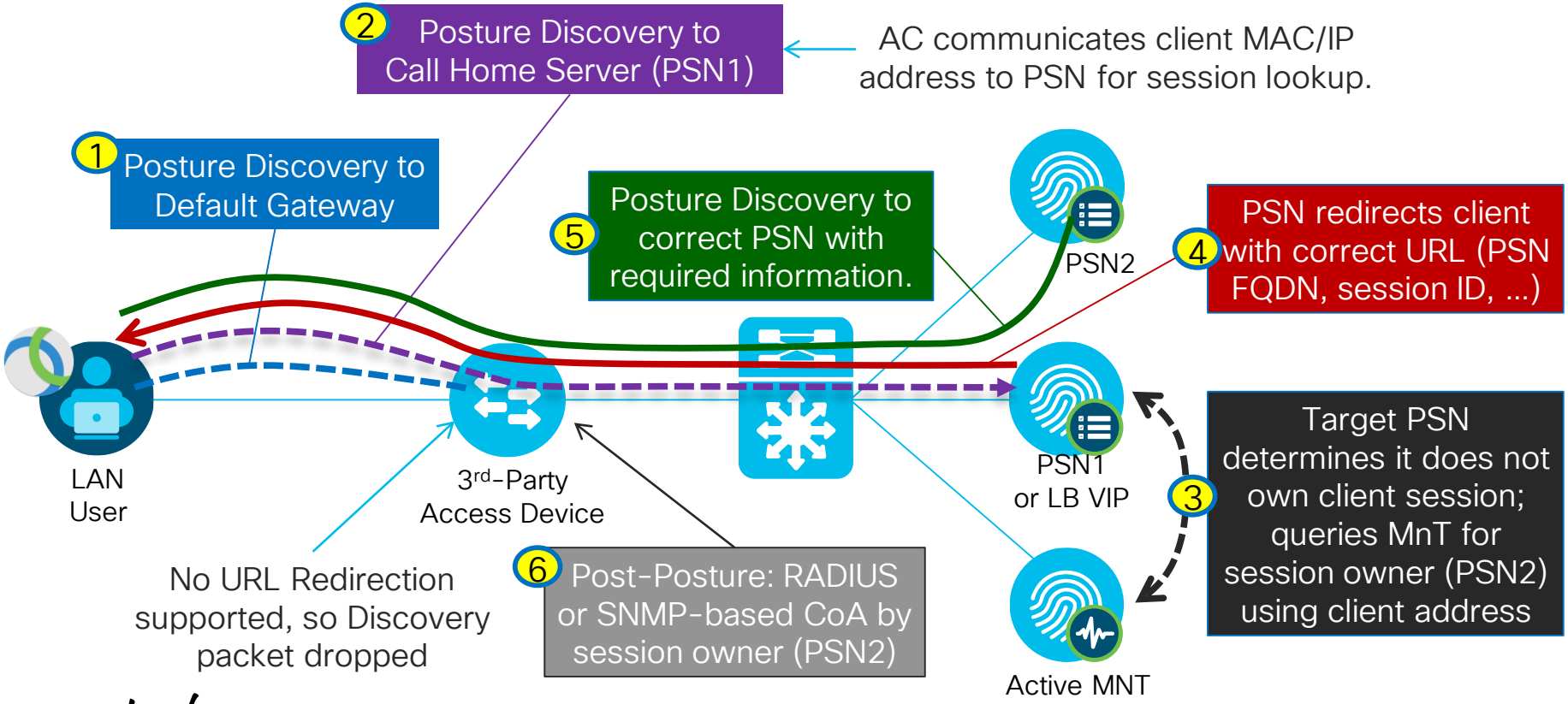
ISE 2.2/AC 4.4 Posture Discovery

RADIUS Session



ISE 2.2/AC 4.4 Posture Discovery

Posture Discovery



AnyConnect Posture Profile

Discovery Host and Call Home Lists

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Discovery host	redirect.company.com		The server that the agent should connect to
* Server name rules	*.company.com	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com
Call Home List	psn1.company.com, psn2.company.com, vip1.company.com:8888, vip2.company.com:8888,	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

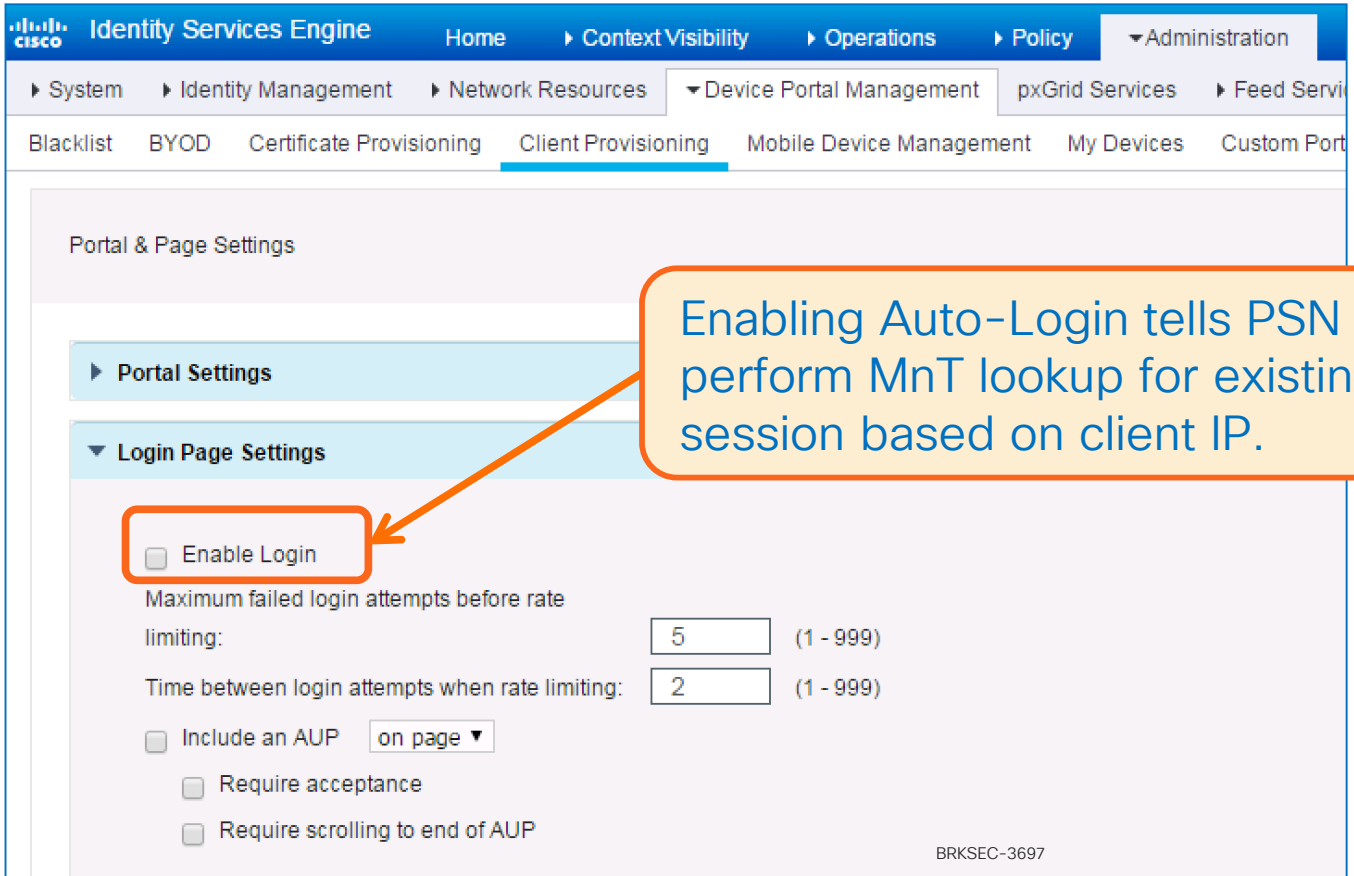
Single Entry for Initial Discovery

List of PSNs (or VIPs!) to use as a fallback to initial Discovery

Note: It is recommended that a separate profile be created for Windows and OSX deployments

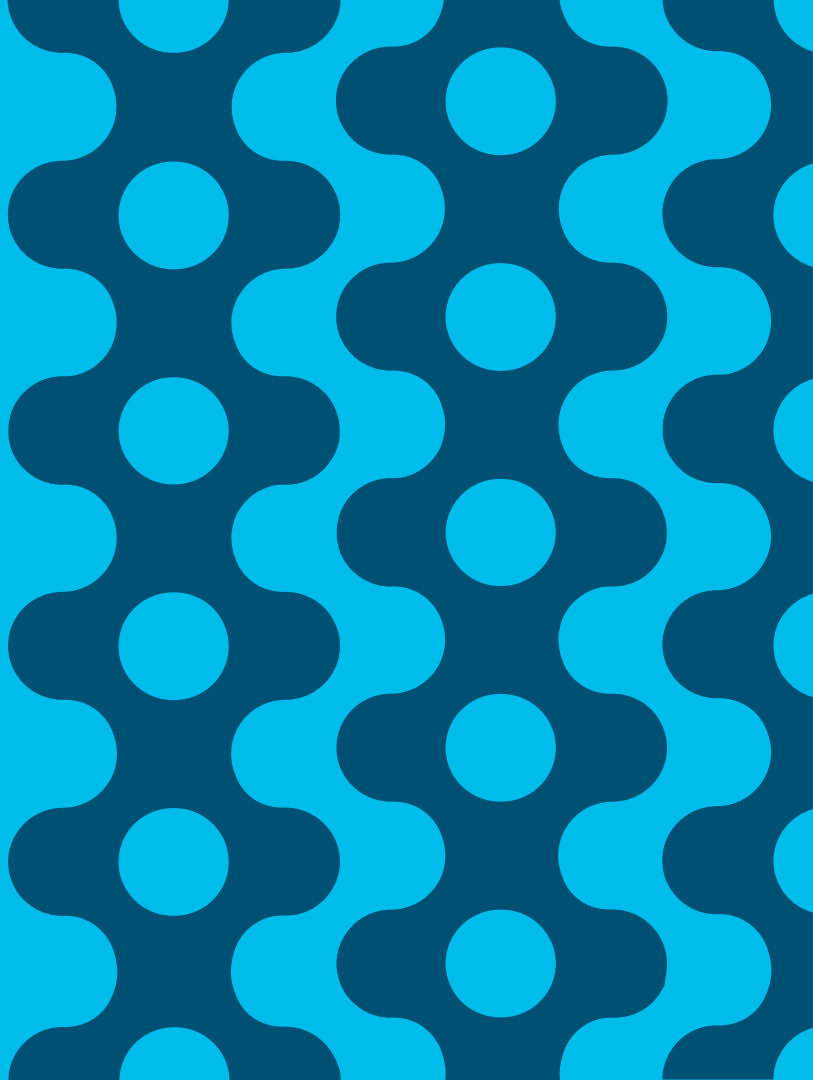
AnyConnect Provisioning Portal

SSO Experience for On-Prem Users!



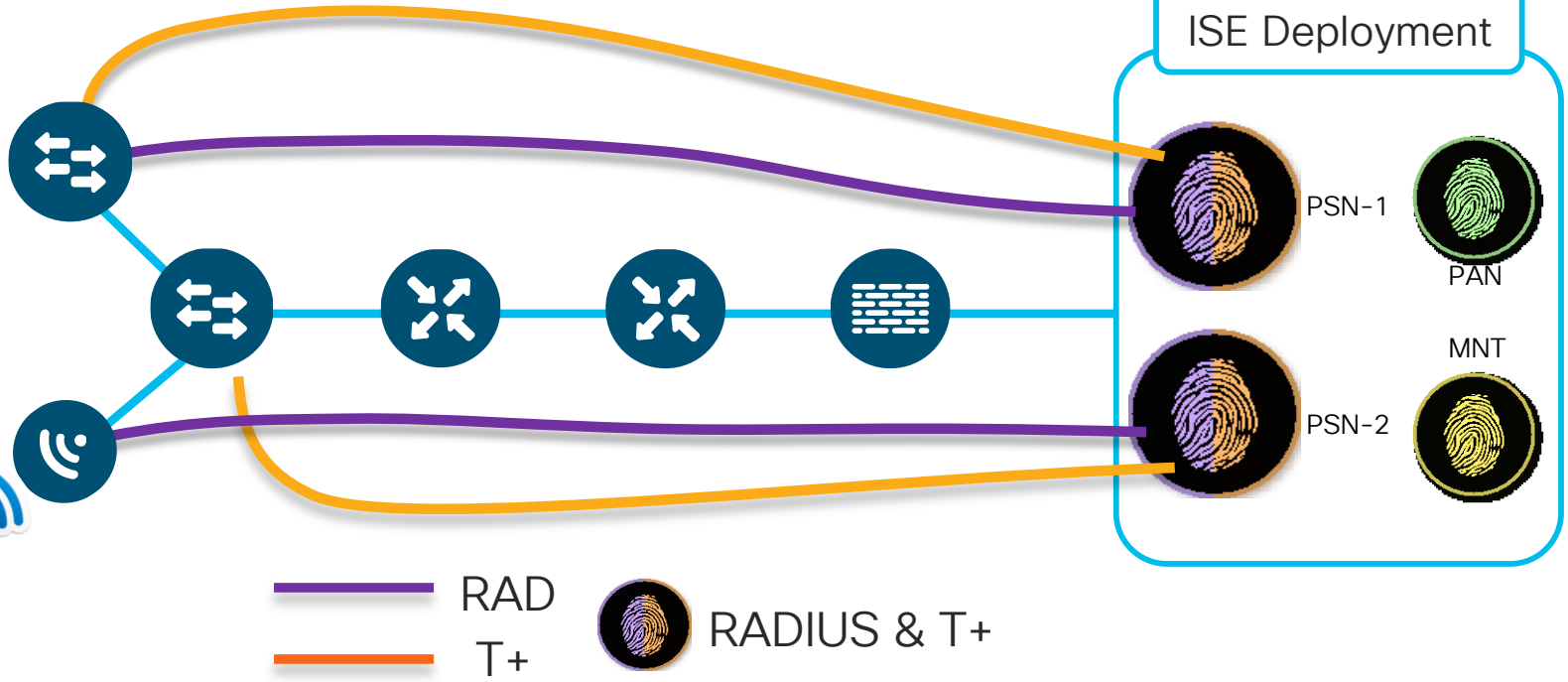
Enabling Auto-Login tells PSN to perform MnT lookup for existing session based on client IP.

TACACS+ Deployment Best Practices

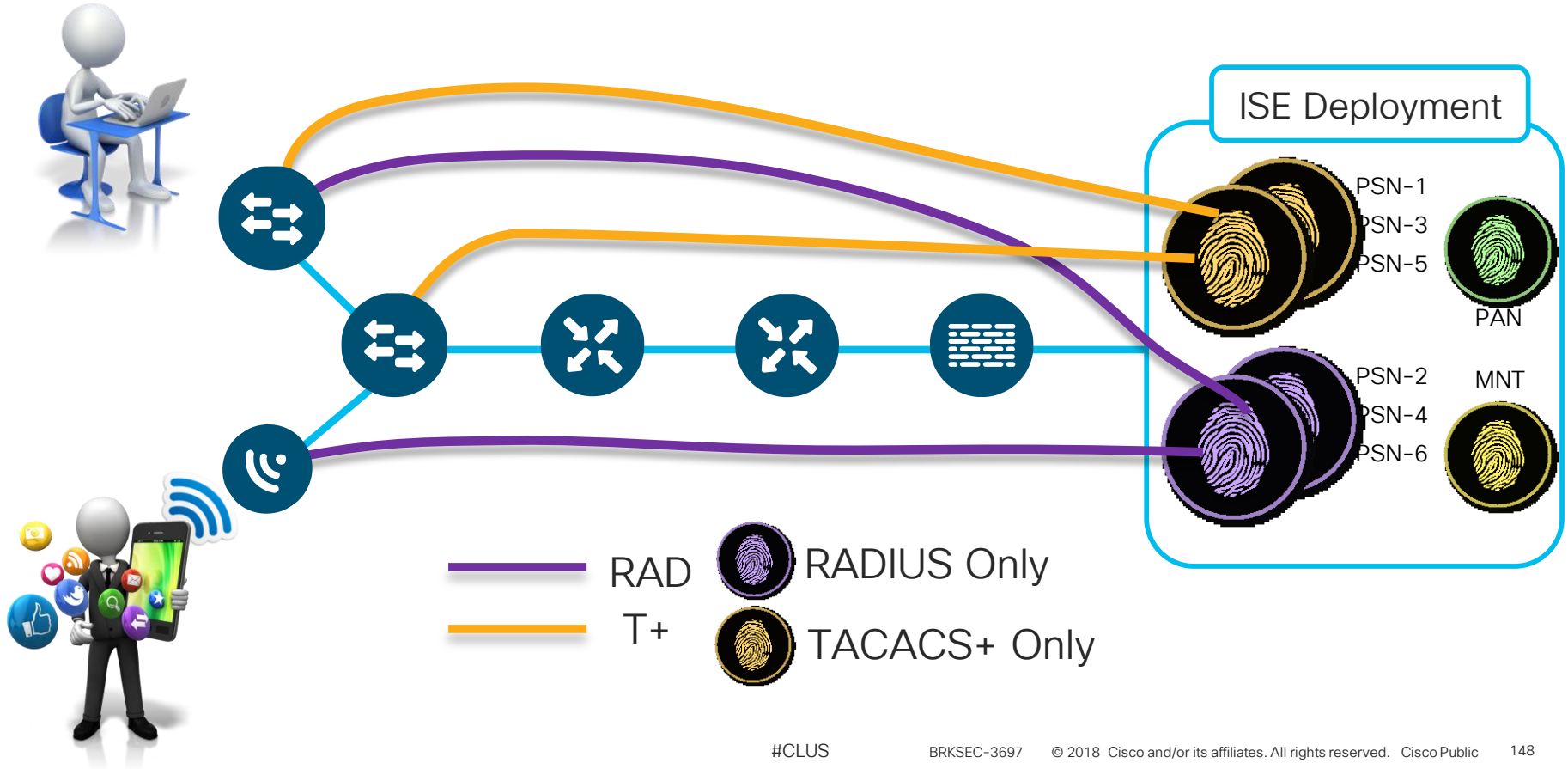


Cisco live!

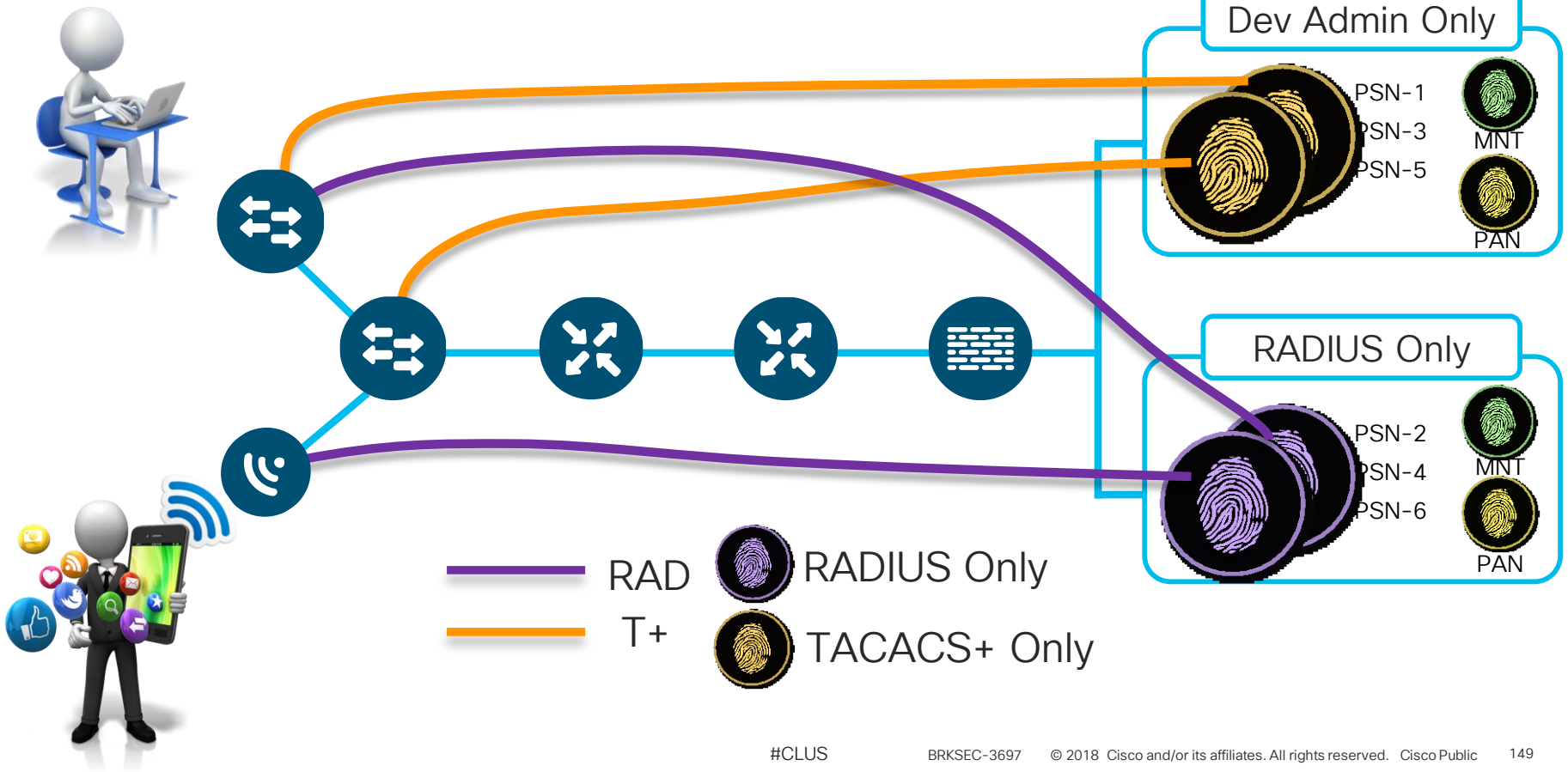
Design #1 – RADIUS & TACACS+ Share PSNs



Design #2 – RADIUS & T+ Use Dedicated PSNs

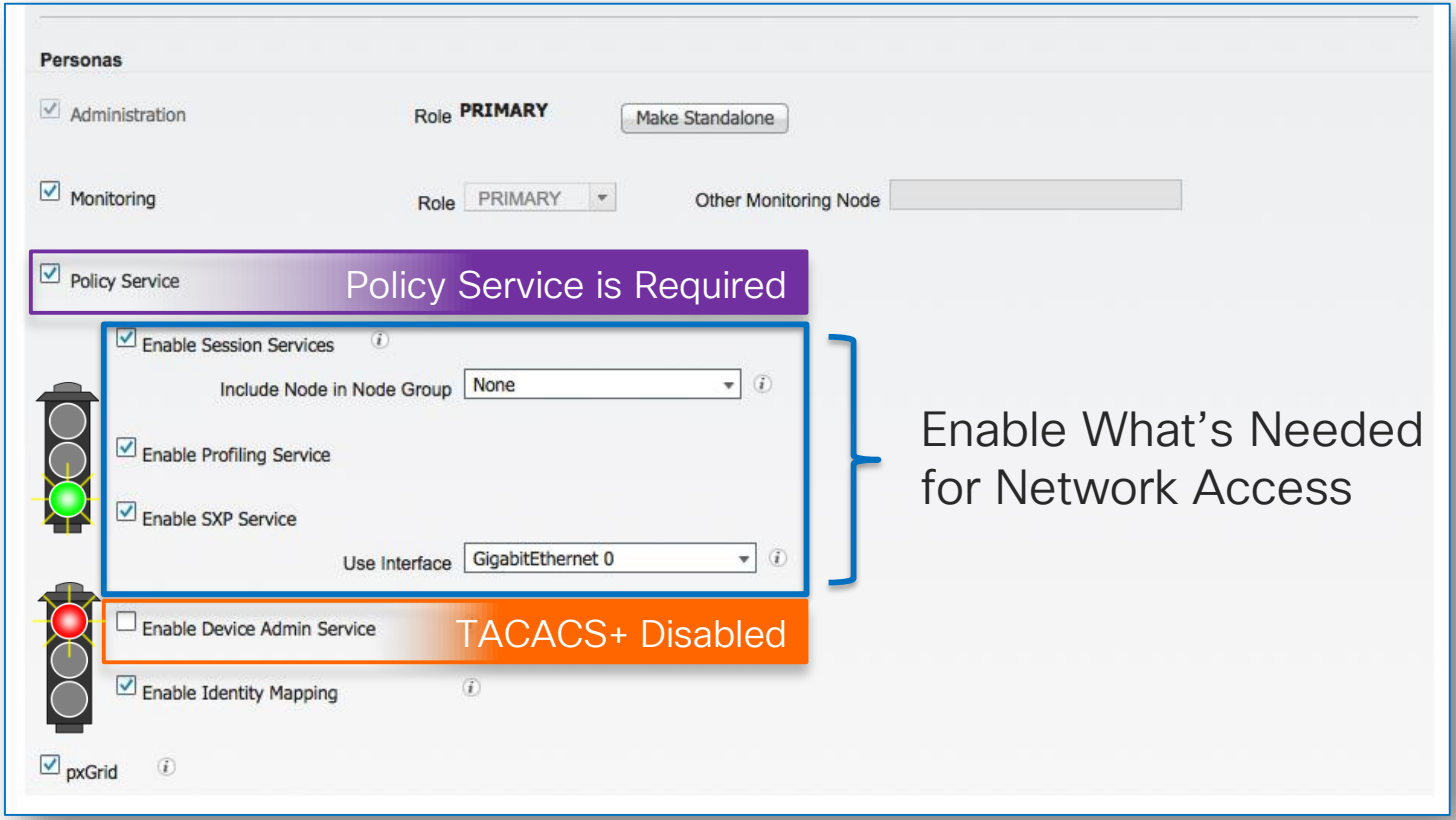


Design #3 – Separate Deployments for RAD & T+



RADIUS Only PSNs

Administration > System > Deployment > [ISE node]



TACACS+ Only PSNs

Administration > System > Deployment > [ISE node]

Options for Deploying Device Admin

https://communities.cisco.com/docs/DOC-63930

Priorities according to Policy and Business Goals		Separate Deployment   RADIUS TACACS	Separate PSNs  RADIUS TACACS	Mixed PSNs  RADIUS/ TACACS
Separation of Configuration/ Duty	Yes: Specialization for TACACS+			
	No: Shared resources/Reduced $$			
Independent Scaling of Services	Yes: Scale as needed/No impact on Device Admin from RADIUS services			
	No: Avoid underutilized PSNs			
Suitable for high-volume Device Admin	Yes: Services dedicated to TACACS+			
	No: Focus on “human” device admins			
Separation of Logging Store	Yes: Optimize log retention VM			
	No: Centralized monitoring			

ACS to ISE Migration

https://communities.cisco.com/docs/DOC-63880

Communities

Products & Services | Partners | Global | Developer

Cisco Communities > Technology > Security Community > Policy and Access > Identity Servic

ACS to ISE Migration

- Video Tutorials
- Demos
- How To Document
- Migration Paths
  - ACS 4.x to ACS 5.x
  - ACS 5.x to ACS 5.5 / 5.6 / 5.7 / 5.8
- ACS vs ISE Comparison (Why do you need to migrate to ISE?)
- ACS vs ISE Deployment Sizing
- ACS End of Life
- Migration Tool Guide

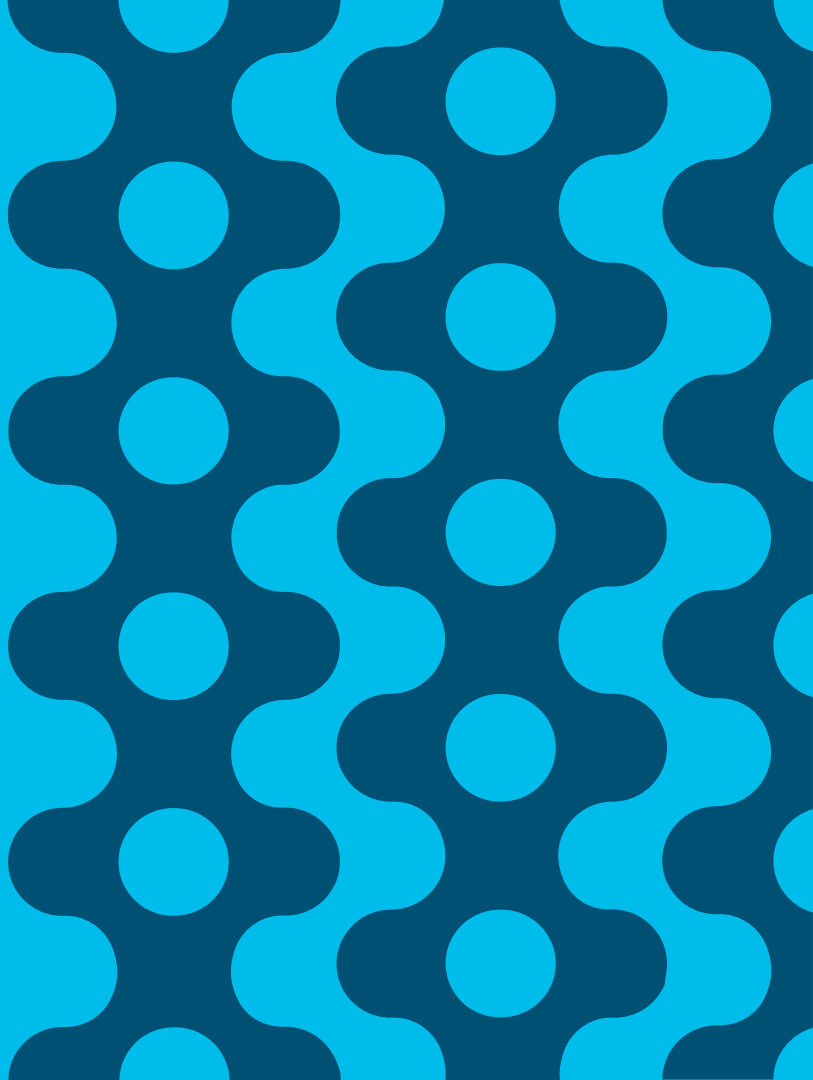
Cisco ACS to ISE Migration Guide

Secure Access How to Guides Series

Author: Krishnan Thiruvengadam

Date: June 2nd, 2016

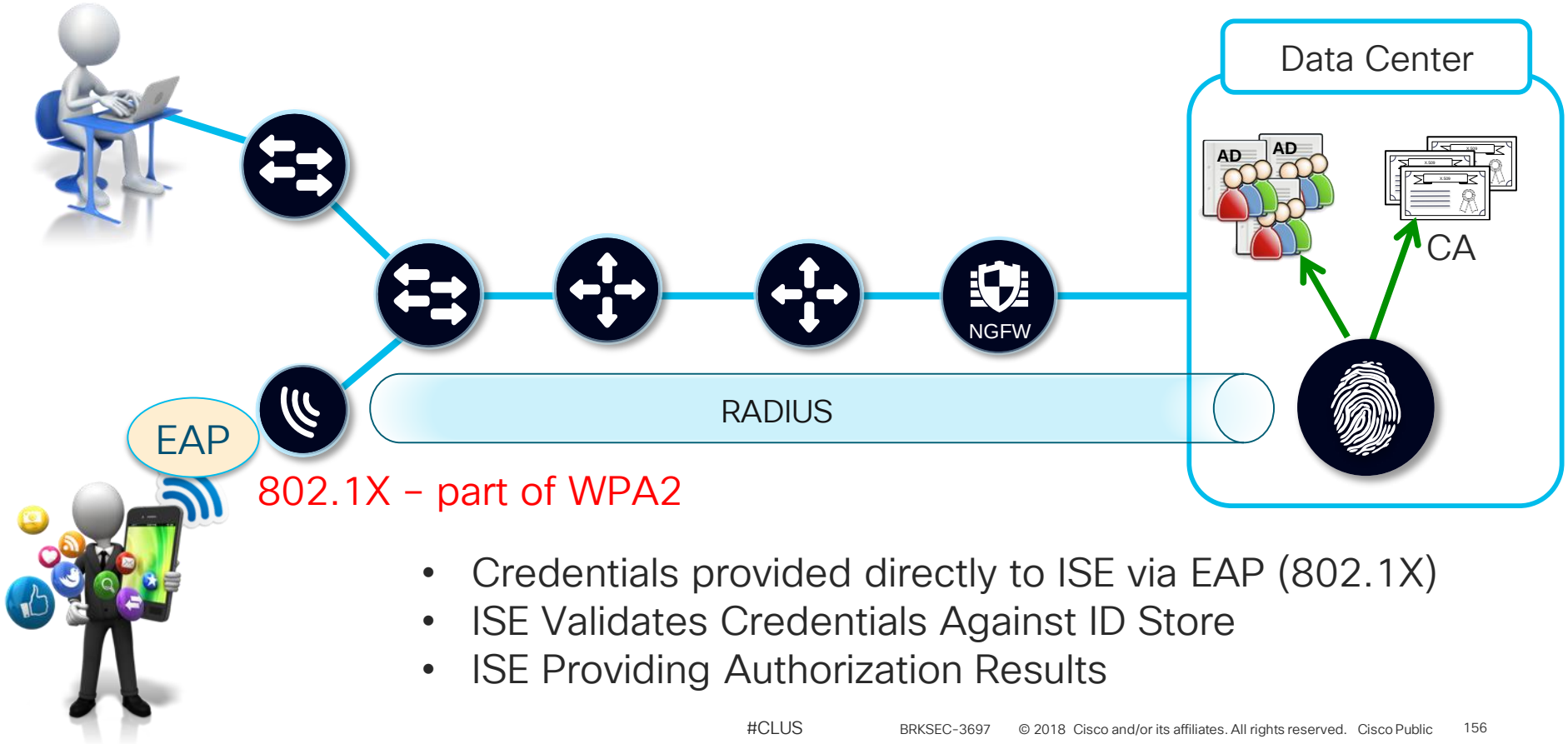
What is Passive Identity



Passive vs Active Identity / Authentication

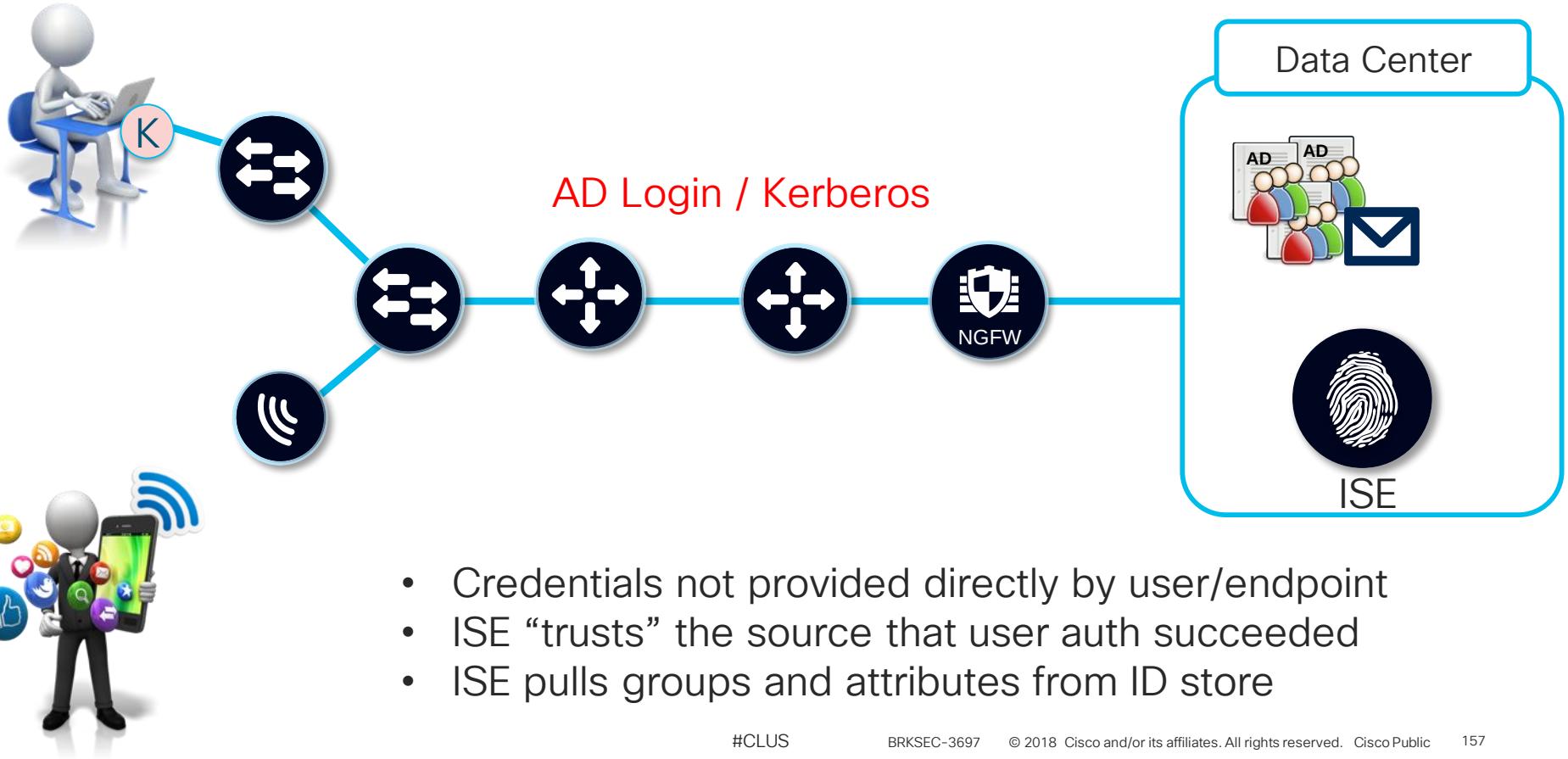
- Most of security vendors (including Cisco) use **Passive Authentication** to provide user identity for security policies.
  - It's "*asking*" Microsoft AD to please tell our product the username & IP address of users who authenticate to AD. *i.e.: It's all hearsay*
  - Example: Context Directory Agent (CDA) using Windows Management Infrastructure (WMI) to tell it when a user authenticates and current IP.
- **Active authentication** is learning it from the endpoint/user directly.
  - Ex: chyps@cisco.com has authenticated to the wireless network "Blizzard"
  - Cisco ISE is the authentication server & learns directly from Craig
    - It's more reliable and works for all devices/users, not just AD managed systems.

Active Authentication



- Credentials provided directly to ISE via EAP (802.1X)
- ISE Validates Credentials Against ID Store
- ISE Providing Authorization Results

Passive Authentication

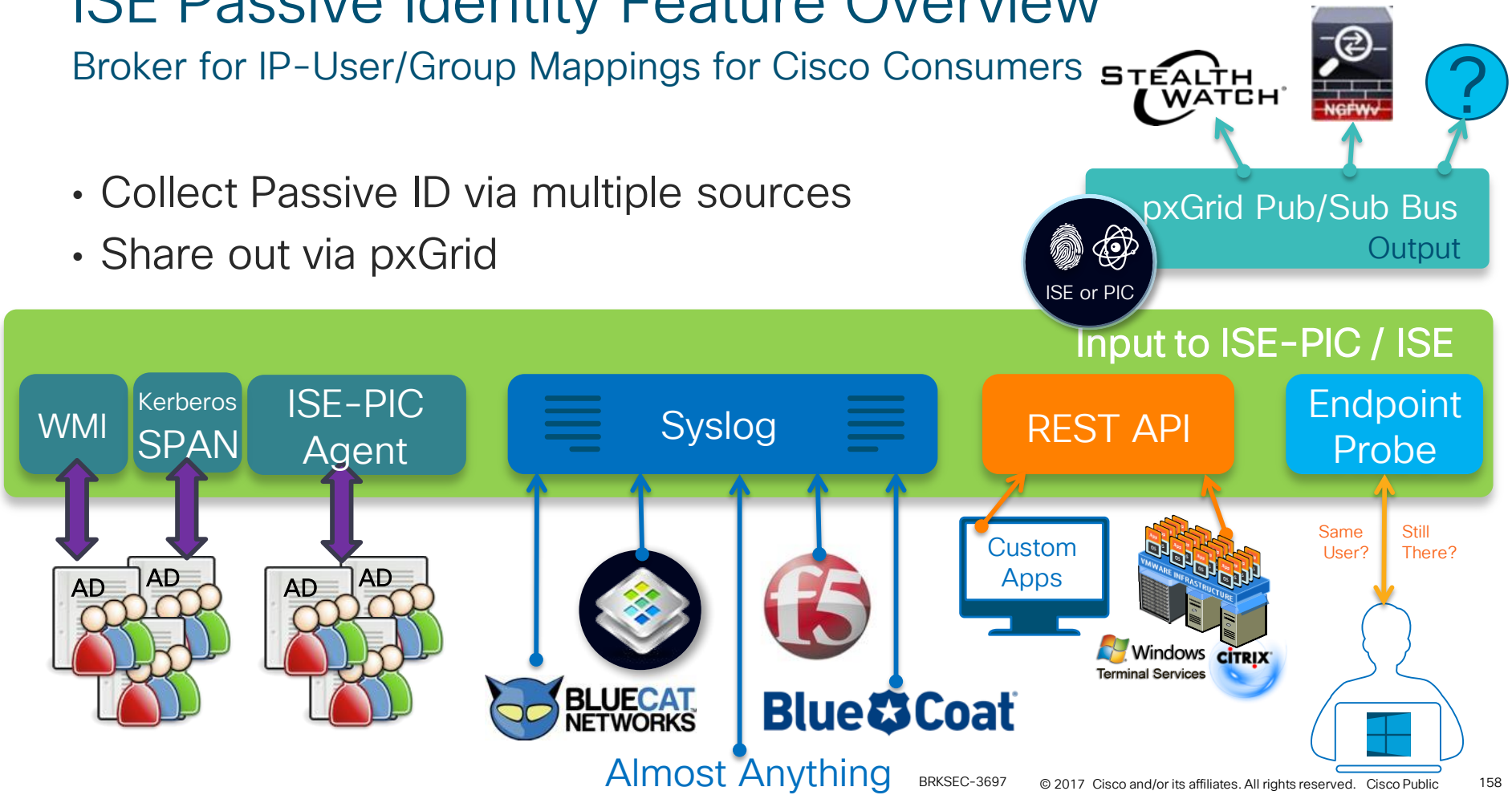


- Credentials not provided directly by user/endpoint
- ISE “trusts” the source that user auth succeeded
- ISE pulls groups and attributes from ID store

ISE Passive Identity Feature Overview

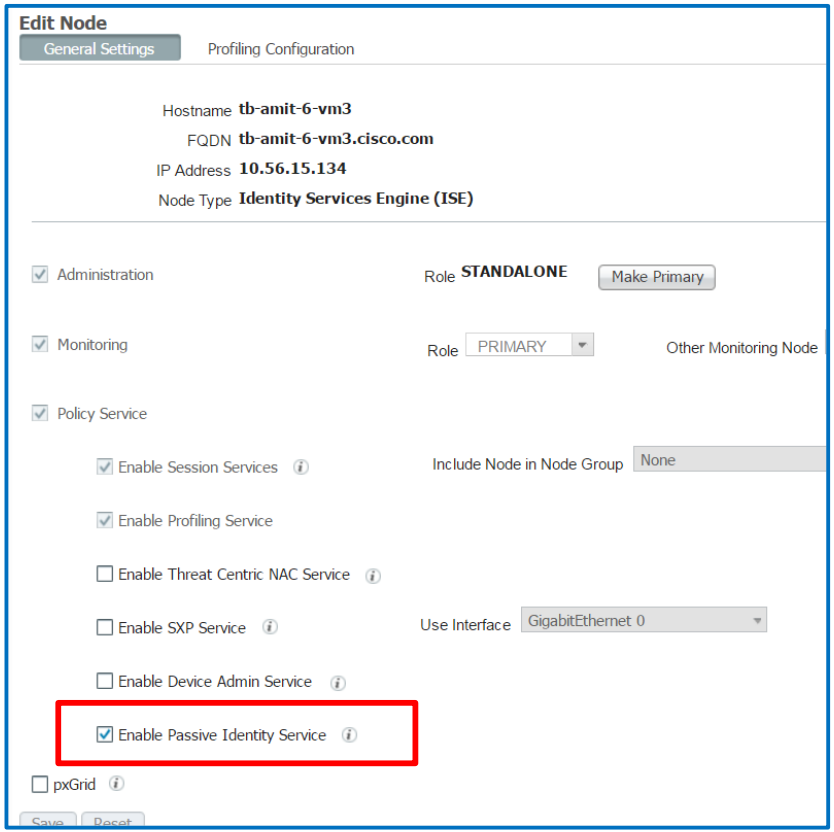
Broker for IP-User/Group Mappings for Cisco Consumers

- Collect Passive ID via multiple sources
- Share out via pxGrid

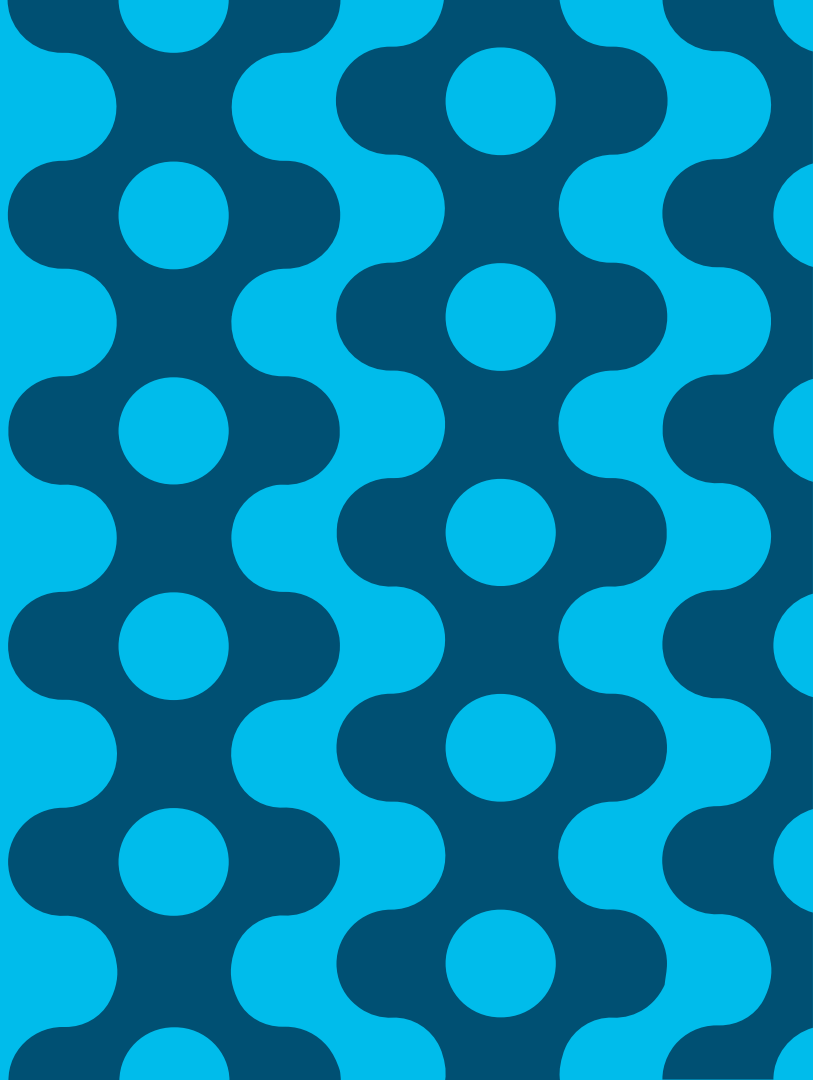


Enabling ISE Passive Identity Service

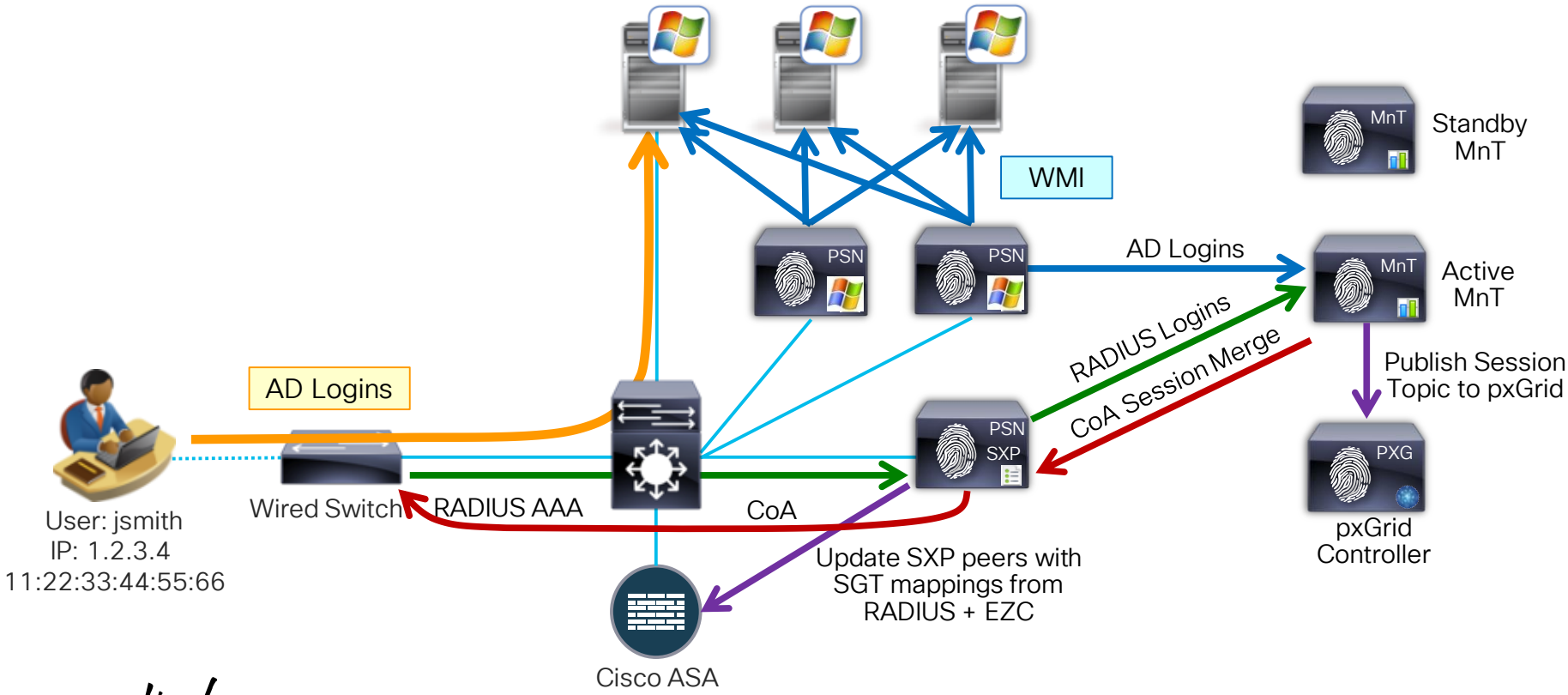
- Enable Passive ID on ISE PSNs
- Enables all passive identity provider features
- Typically need only 2 nodes (for redundancy) to support WMI.
- Additional PSNs can be enabled for Passive ID to support:
  - PIC Agent
  - Syslog
  - Endpoint probes
  - SPAN
  - API / TS Agent



Easy Connect: Identifying Trusted Users without 802.1X User Authentication



Passive Identity / Easy Connect Architecture

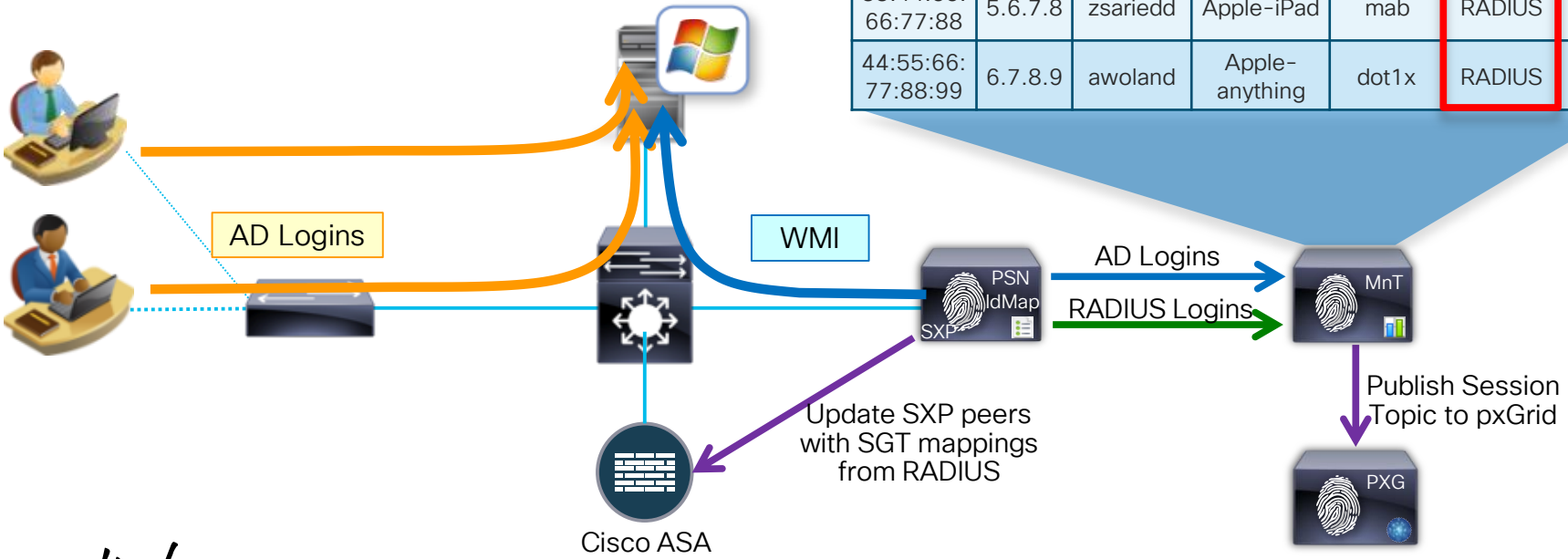


Easy Connect

Consuming Both AD and RADIUS Logins

Windows Event log	
IP Address	Username
1.2.3.4	chyps
2.3.4.5	imbashir

ISE Session Directory						
MAC	IP	Uname	Profile	Method	Source	SGT
	1.2.3.4	chyps			Identity Mapping	
	2.3.4.5	imbashir			Identity Mapping	
22:33:44:55:66:77	3.4.5.6	hslai	Samsung Galaxy	dot1x	RADIUS	10
33:44:55:66:77:88	5.6.7.8	zsariedd	Apple-iPad	mab	RADIUS	20
44:55:66:77:88:99	6.7.8.9	awoland	Apple-anything	dot1x	RADIUS	10



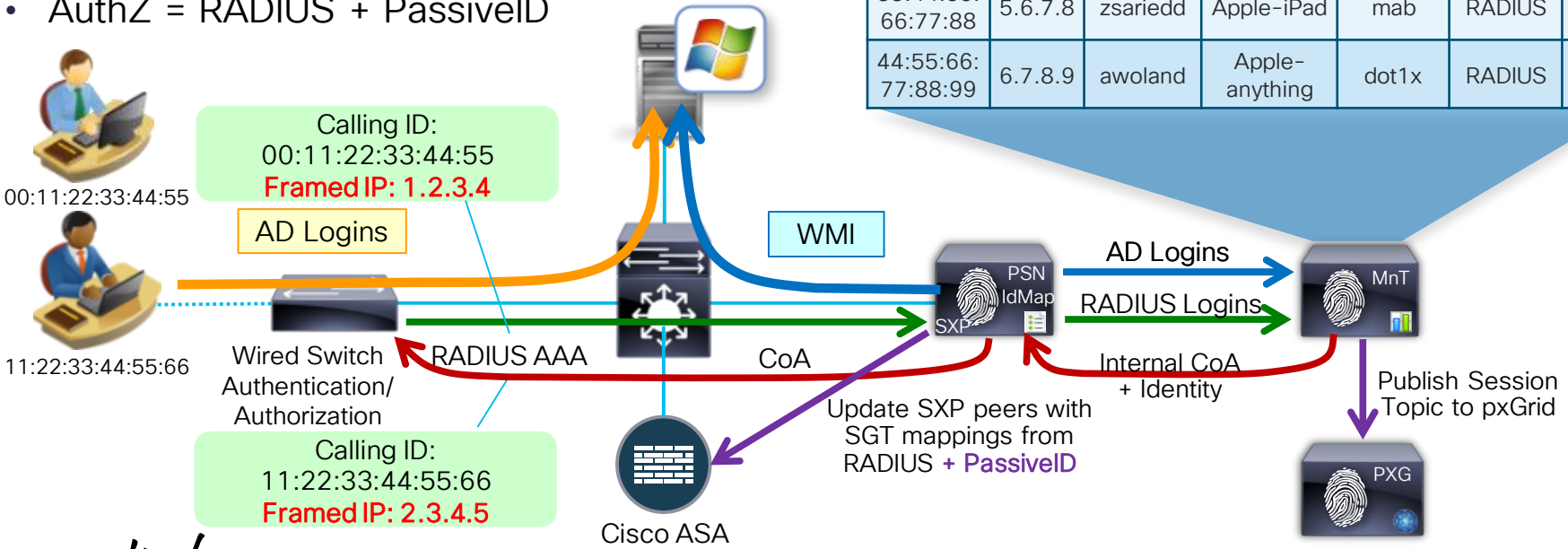
Easy Connect Enforcement

Merging RADIUS and AD Login Identity

- Merge *active* RADIUS Identity with *passive* AD Identity
- AuthZ = RADIUS + PassiveID

Windows Event log	
IP Address	Username
1.2.3.4	chyps
2.3.4.5	imbashir

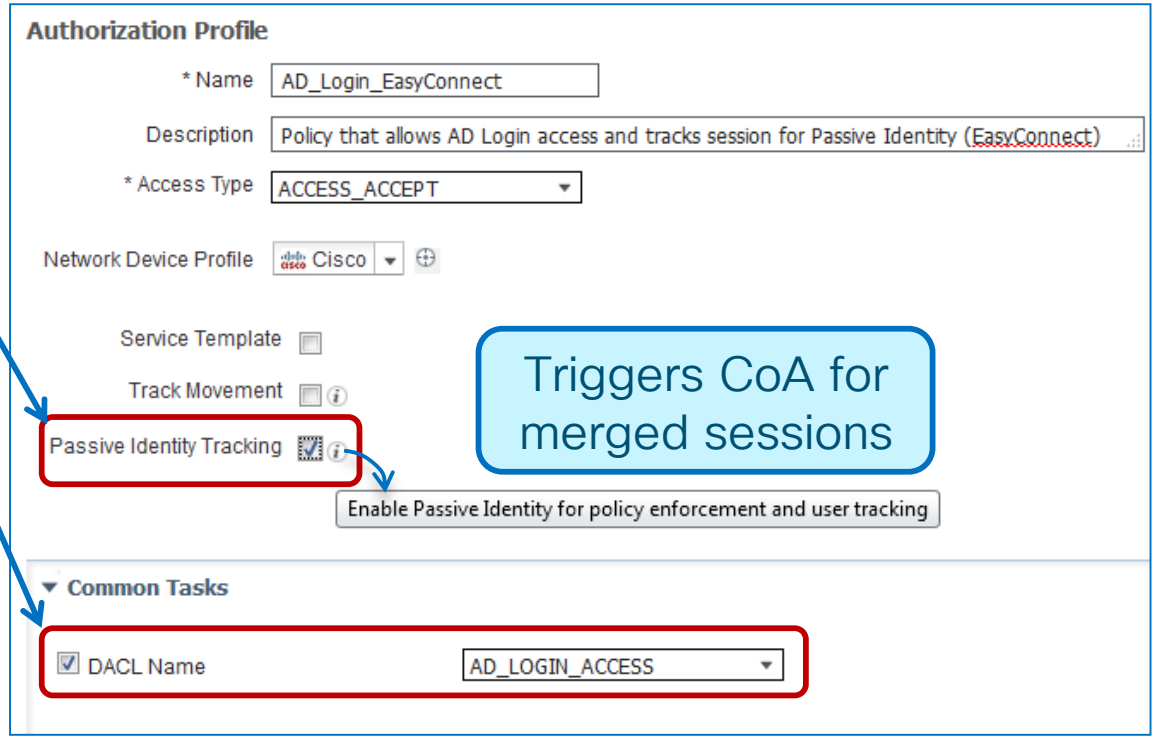
ISE Session Directory						
MAC	IP	Uname	Profile	Method	Source	SGT
00:11:22:33:44:55	1.2.3.4	chyps	Windows7-WS	Dot1x +PsvID	IdMap RADIUS	10
11:22:33:44:55:66	2.3.4.5	imbashir	Windows 10	MAB +PsvID	IdMap RADIUS	30
22:33:44:55:66:77	3.4.5.6	hslai	Samsung Galaxy	dot1x	RADIUS	10
33:44:55:66:77:88	5.6.7.8	zsariedd	Apple-iPad	mab	RADIUS	20
44:55:66:77:88:99	6.7.8.9	awoland	Apple-anything	dot1x	RADIUS	10



Easy Connect Configuration (beyond Passive ID)

Authorization Profile

- To enable Easy Connect, Authorization Profile must:
  - Flag session as candidate for Passive Identity tracking.
  - Permit access for AD login.
- MnT node:
  - Merges RADIUS session with AD passive ID session based on matching IP address.
  - Generates CoA reauth to PSN to apply new authorization policy based on AD identity (Passive ID).



Easy Connect Configuration

Authorization Policy

- Add conditions based on Passive Identity

"Easy Connect Chaining"

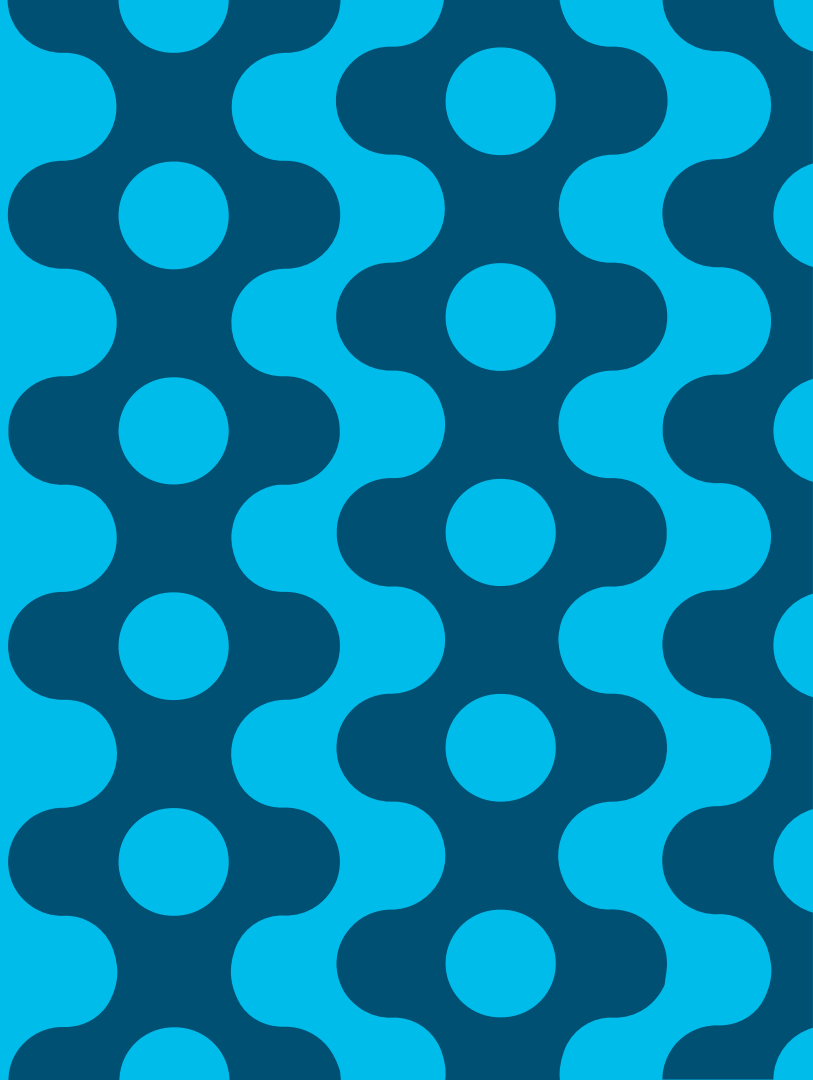
Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Employee (1X plus EasyConnect)	if (Wired_802.1X AND AD1:ExternalGroups EQUALS cts.local/Users /Domain Computers AND PassiveID:PassiveID_Groups EQUALS AD1:cts.local/Users/employees)	then Employee
✓	Employee (1X Only)	if (Wired_802.1X AND AD1:ExternalGroups EQUALS cts.local/Users /employees)	then Employee
✓	Employee (MAB plus EasyConnect)	if (Wired_MAB AND PassiveID:PassiveID_Groups EQUALS AD1:cts.local/Users/employees)	then Employee
✓	Employee (WebAuth)	if (Wired_MAB AND AD1:ExternalGroups EQUALS cts.local/Users /employees)	then Employee
✓	AD_Computer (1X Only)	if (Wired_802.1X AND AD1:ExternalGroups EQUALS cts.local/Users /Domain Computers)	then AD_Login_EasyConnect
✓	Limited Access (AD or CWA)	if Wired_MAB	then AD_Login_EasyConnect

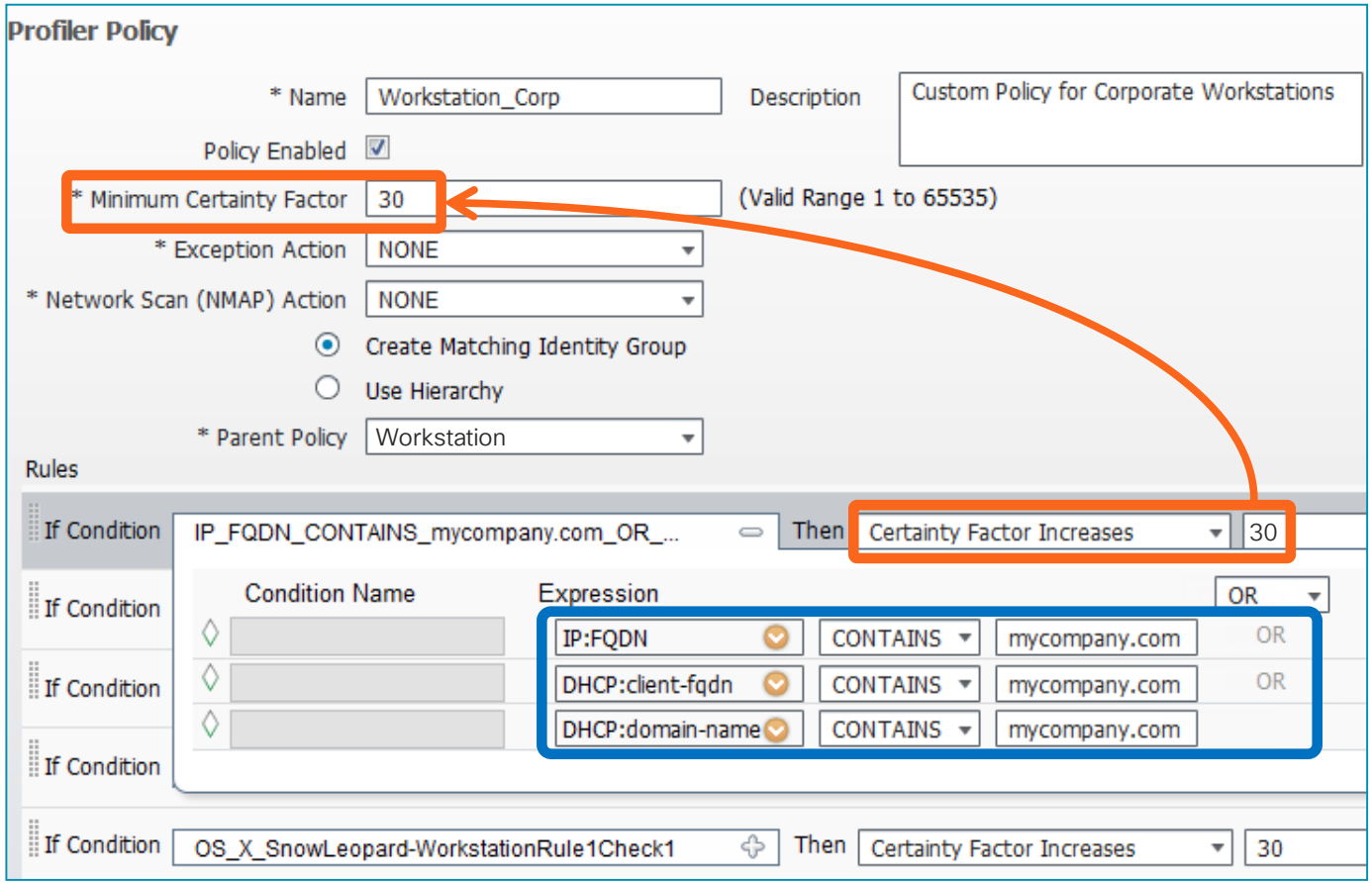
Identifying Trusted Devices without 802.1X Machine Authentication



Cisco live!

Identifying Trusted Devices using Profiler

- Custom Profile Workstation_Corp
- Add child policy to current Workstation profile.
- Add rule to match any (logical OR) of these conditions to *mycompany.com*:
  - DNS FQDN
  - DHCP client-fqdn
  - DHCP domain-name



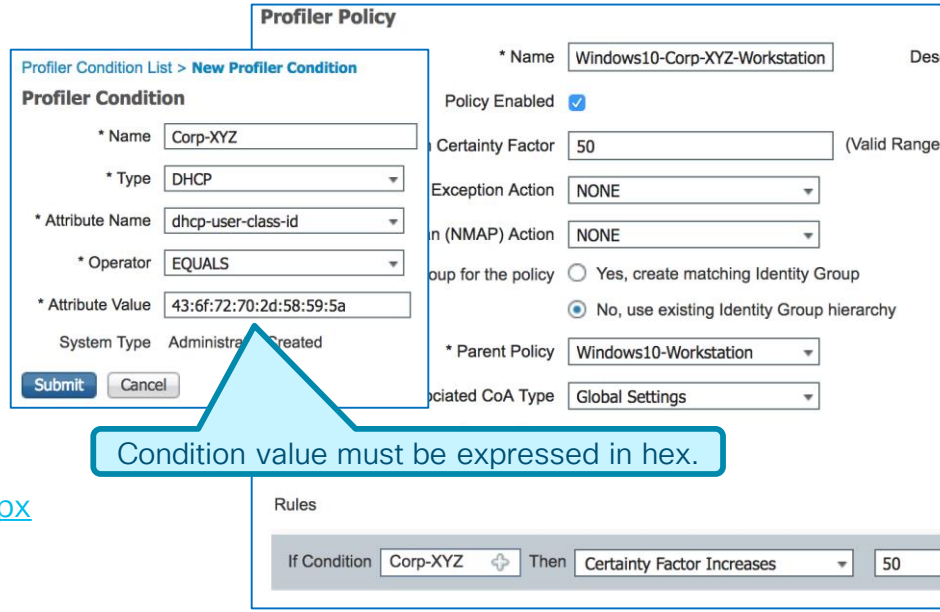
Identifying Trusted Devices using Profiler

Real Customer Example: Profiling Based on a Custom DHCP Attribute

- Custom DHCP-User-Class-Identifier for Domain Computers
  - Provides a unique way to profile the device as a Corporate Asset.
- Manual Configuration Example:

```
C:\>ipconfig /setclassid "Local Area Connection" Corp-XYZ

Windows 7 IP Configuration
    DHCP ClassId successfully modified for adapter "Local Area Connection"
```

http://technet.microsoft.com/enus/library/cc783756(WS.10).aspx

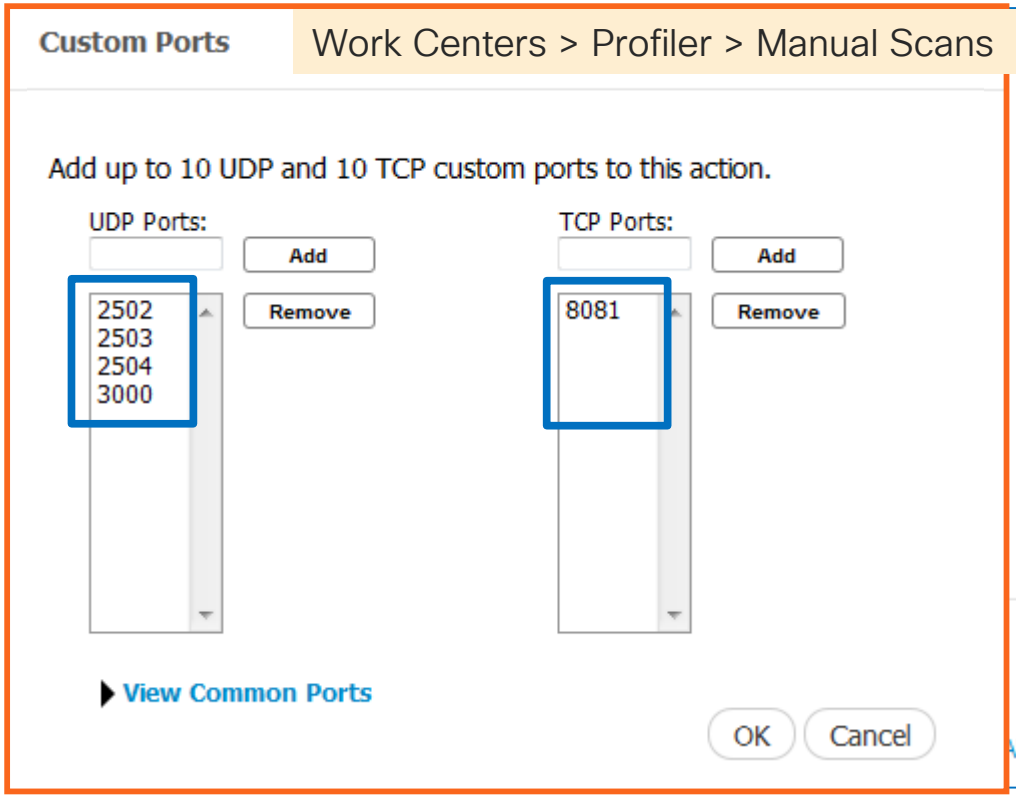


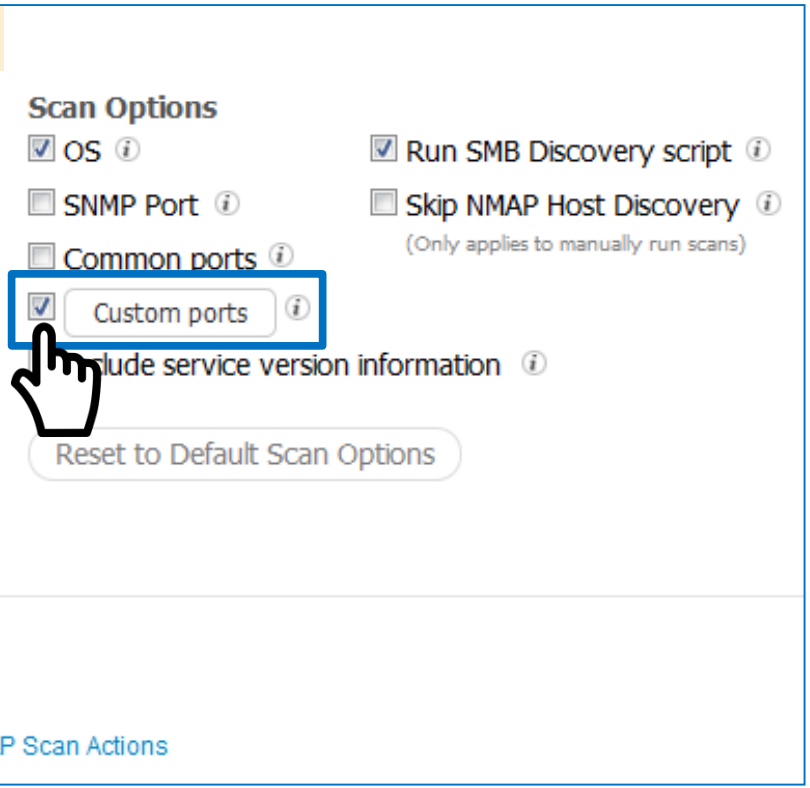
- GPO Script Configuration Example:

1 - Create a GPO which has the necessary IPCONFIG command in a startup script
2 - Create a Domain Local group called something like 'Laptop Computer Accounts' and add all the laptop computer accounts
3 - Modify the GPO by removing the 'Authenticated Users' from the permissions list
4 - Add the 'Laptop Computer Accounts' group to the permissions list and assign 'Read' and 'Apply Group Policy' permissions.
5 - Link the GPO to the domain root (or the highest level OU which will encompass all computer accounts)

Identifying Trusted Devices using NMAP

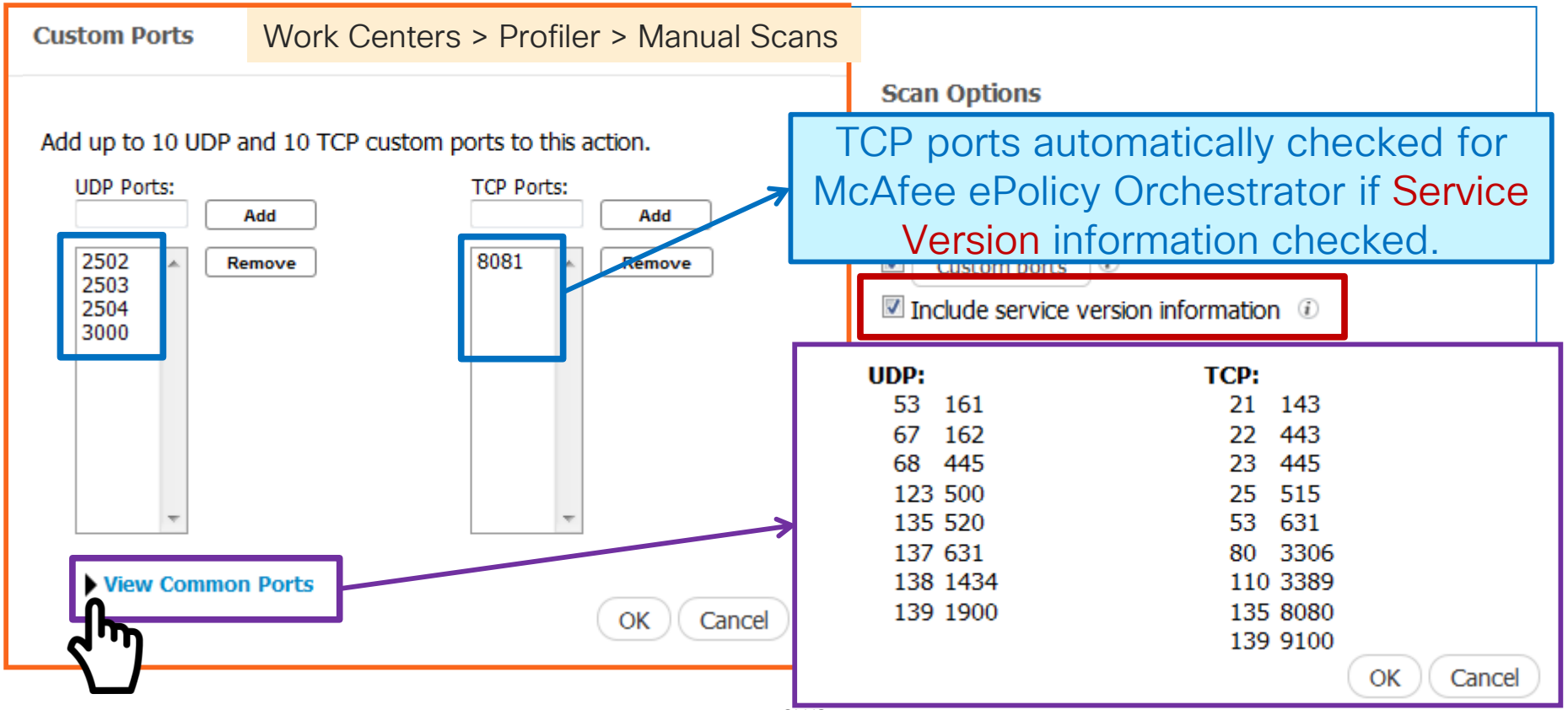
Custom Port Scans





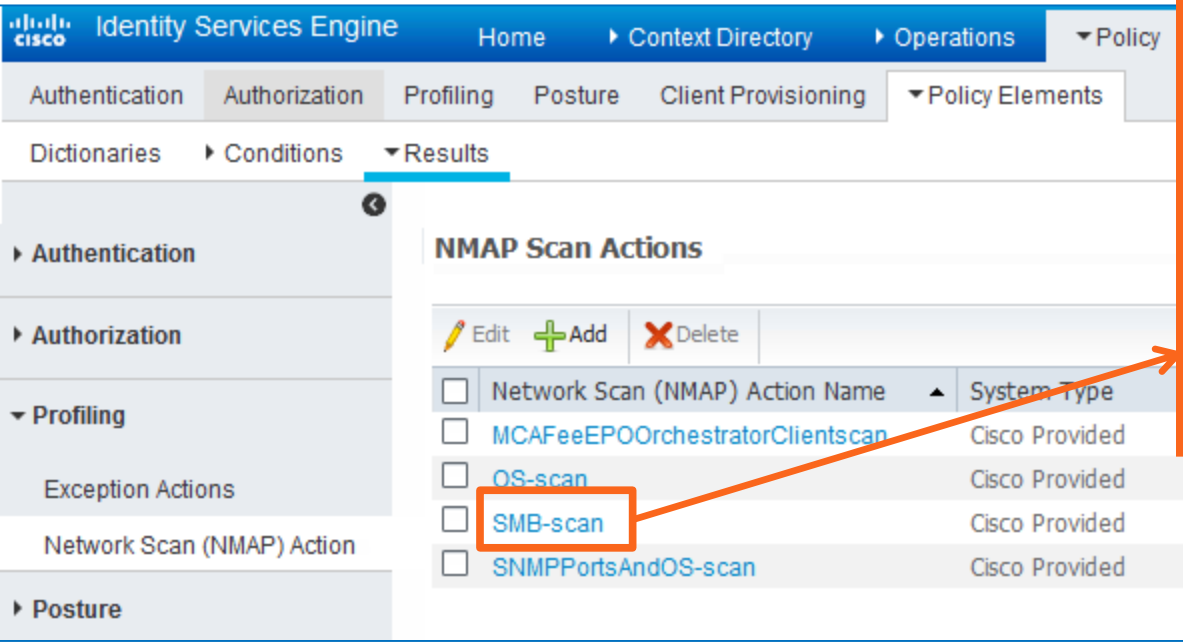
Identifying Trusted Devices using NMAP

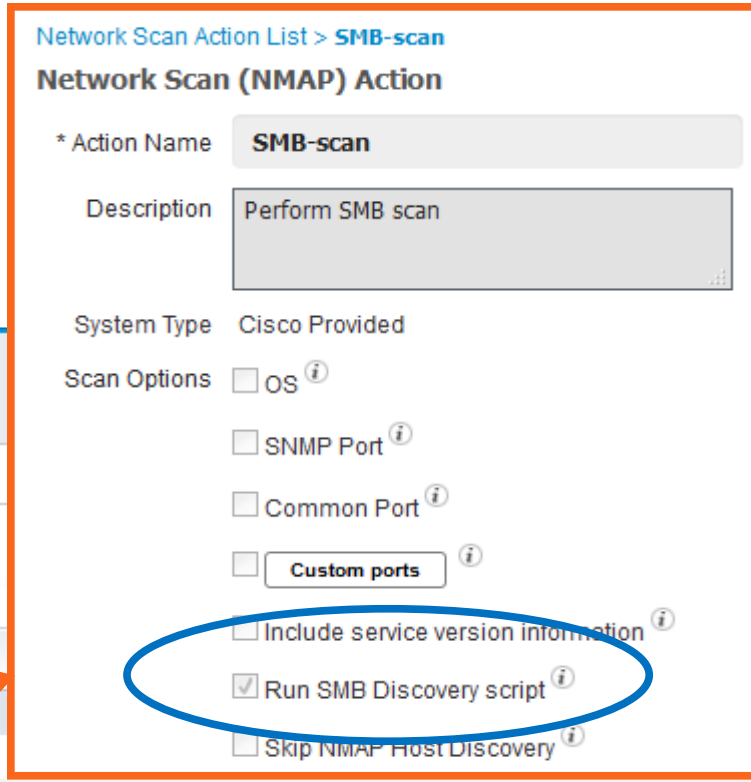
Service Information



NMAP Scan Actions

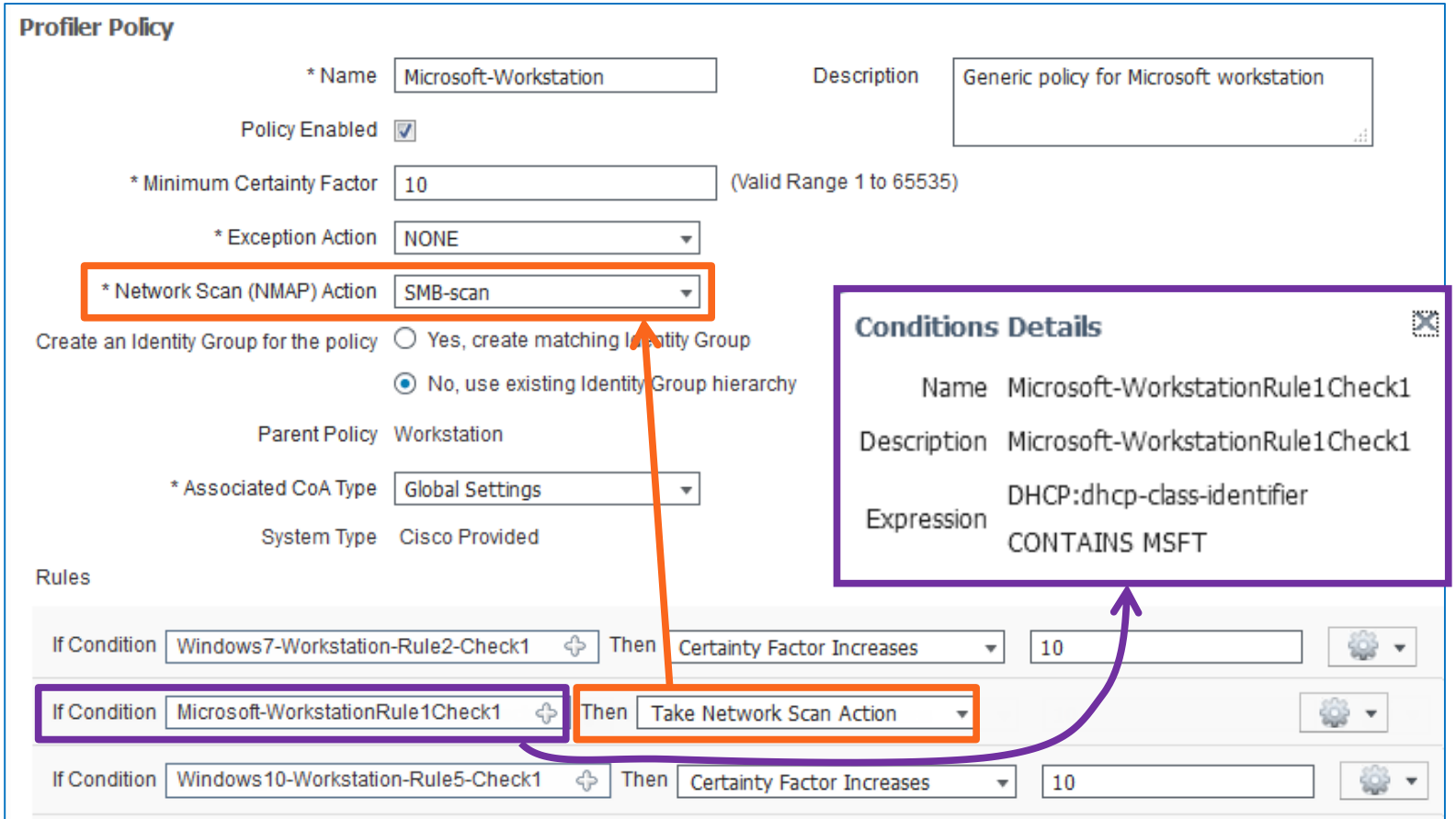
Used in Profiler Policies (triggered scans) or Manual Scans





Triggered NMAP Scan using Template

Work Centers > Profiler > Profiling Policies



Enhanced NMAP Probe

SMB Discovery

SMB.cpe	cpe:/o:microsoft:windows_7::-:professional
SMB.fqdn	win7-pc.cts.local
SMB.lanmanager	Windows 7 Professional N 6.1
SMB.operating-system	Windows 7 Professional N 7600
SMB.server	WIN7-PC\x00
SMB.workgroup	CTS\x00

Detailed Windows Info including:

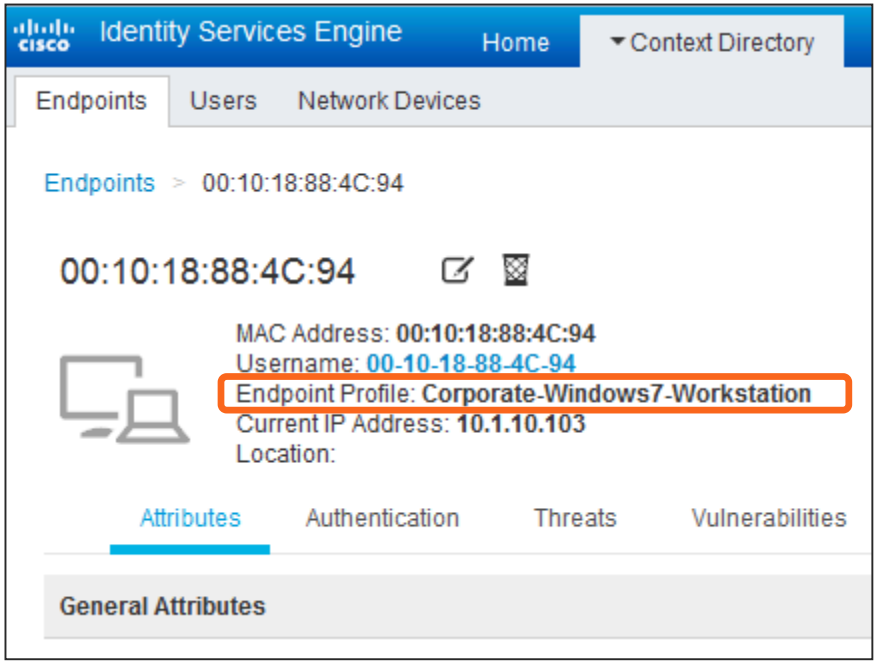
- Common Platform Enumeration (CPE)
- FQDN
- Operating System version
- Domain
- Workgroup

NMAP Reference: https://nmap.org/nsedoc/scripts/smb-os-discovery.html

If unable to get SMB info, verify SMB can access computer:
Windows 7 Scan to Folder SMB Setup www.kb.lesolson.com/InstantKB20/Attachment130.aspx

Enhanced NMAP Probe

Custom Ports, Service Info, ePO Check



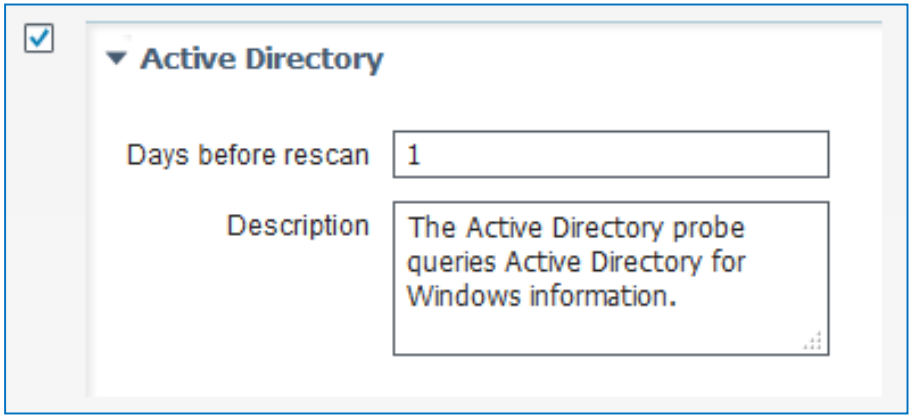
Custom Port Check on TCP/8081 and McAfee ePolicy Orchestrator Agent Check

123-udp	ntp
135-tcp	msrpc-Microsoft Windows RPC
135-udp	msrpc
137-udp	netbios-ns-Microsoft Windows netbios-ssn-workgroup: CTS
138-udp	netbios-dgm
139-tcp	netbios-ssn-Microsoft Windows 98 netbios-ssn
139-udp	netbios-ssn
1434-udp	ms-sql-m
161-udp	snmp
1900-udp	upnp
445-tcp	microsoft-ds-Microsoft Windows 10 microsoft-ds
445-udp	microsoft-ds
500-udp	isakmp
520-udp	route
53-udp	domain
631-udp	ipp
67-udp	dhcps
68-udp	dhcpc
8081-tcp	http-Network Associates ePolicy Orchestrator

AD Probe

Work Centers > Profiler > Node Config > Deployment > (node) > Profiler Config

- Increases OS fidelity through detailed info extracted via AD.
- Distinguishes corporate from non-corporate endpoints. ➔ IS device a Corp Asset?
- Leverages AD Runtime Connector
- Attempts fetch of AD attributes once computer hostname learned from:
  - DHCP Probe
  - DNS Probe
  - Machine Auth
- AD queries gated by:
  - Rescan interval (default 1 day)
  - Profiler activity for endpoint



Note: If AD probe enabled after endpoint learned and hostname acquired, then no AD query.

AD Probe

Conditions and Attributes

Match on the following:
- AD Computer?
- Join Point Domain
- OS, Version, and Service Pack

Profiler Condition List > **New Profiler Condition**

Profiler Condition

Conditions

* Name	AD-Check	Description	Custom AD Probe Condition
* Type	ACTIVEDIRECTORY		
* Attribute Name	AD-Host-Exists		
* Operator	AD-Host-Exists AD-Join-Point AD-Operating-System AD-OS-Version AD-Service-Pack		
* Attribute Value			
System Type			

Submit Cancel

Sample Attributes

AD-Fetch-Host-Name	win7-pc.cts.local
AD-Host-Exists	true
AD-Join-Point	CTS.LOCAL
AD-Last-Fetch-Time	1460430231349
AD-OS-Version	6.1 (7600)
AD-Operating-System	Windows 7 Professional N

MAB → DHCP → AD Probe

Simple as 1 – 2 – 3 !

Identifying Corporate Assets using Posture

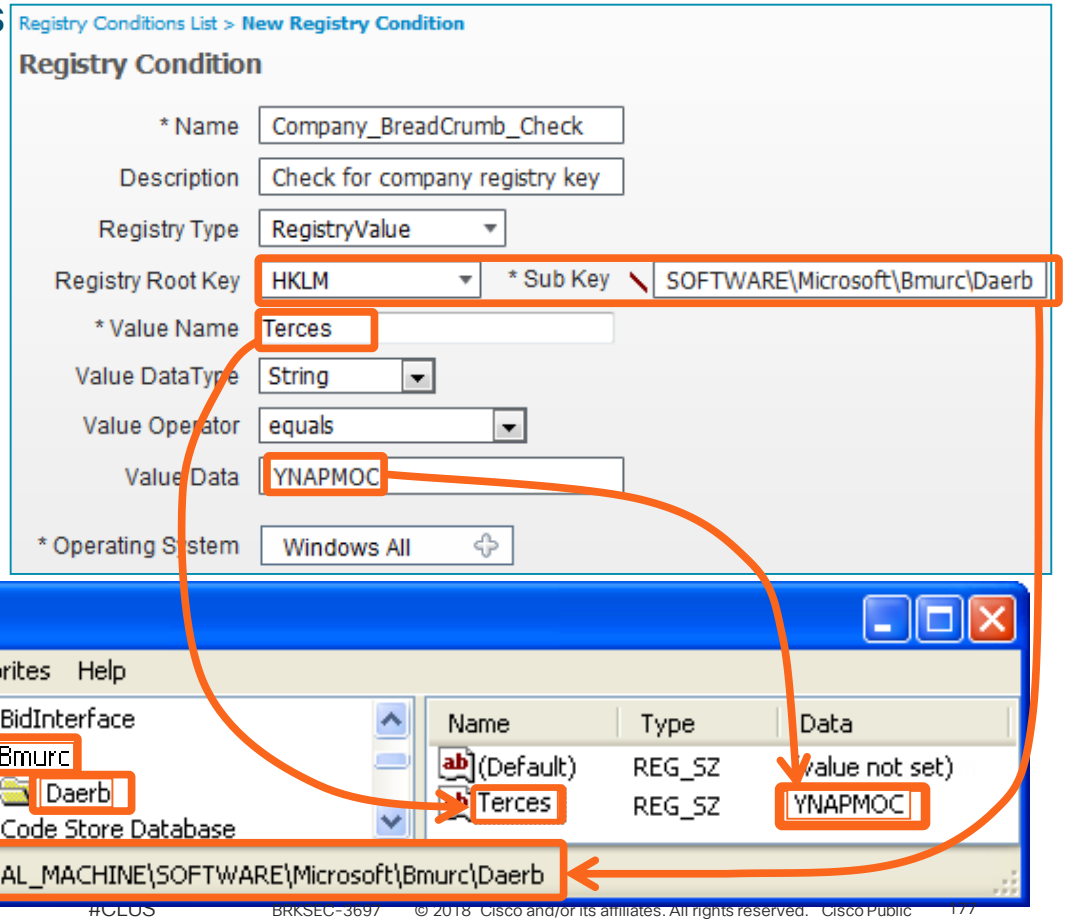
Check for Unique Corp Attributes

- ISE Posture checks registry for pre-populated or unique entries.
  - Ex: Check for key Terces with value YNAPMOC under HKLM\SOFTWARE\Microsoft\Bmurc\Daerb\

COMPANY secreT breaD crumB

- Optional Checks:
  - Files unique to corporate image
  - Applications/ Services specific to organization's SOE.

SOE=Standard Operating Environment



Endpoint Custom Attributes

Administration > Identity Management > Settings

- User Custom Attributes
- User Authentication Settings
- Endpoint Purge
- Endpoint Custom Attributes

Endpoint Custom Attributes

Endpoint Attributes (for reference)

Mandatory	Attribute Name	Data Type
	PortalUser	

Endpoint Custom Attributes

Attribute name	
AssetType	
AssetTagNumber	
SerialNumber	
ProfitCenter	
CorpDevice	String

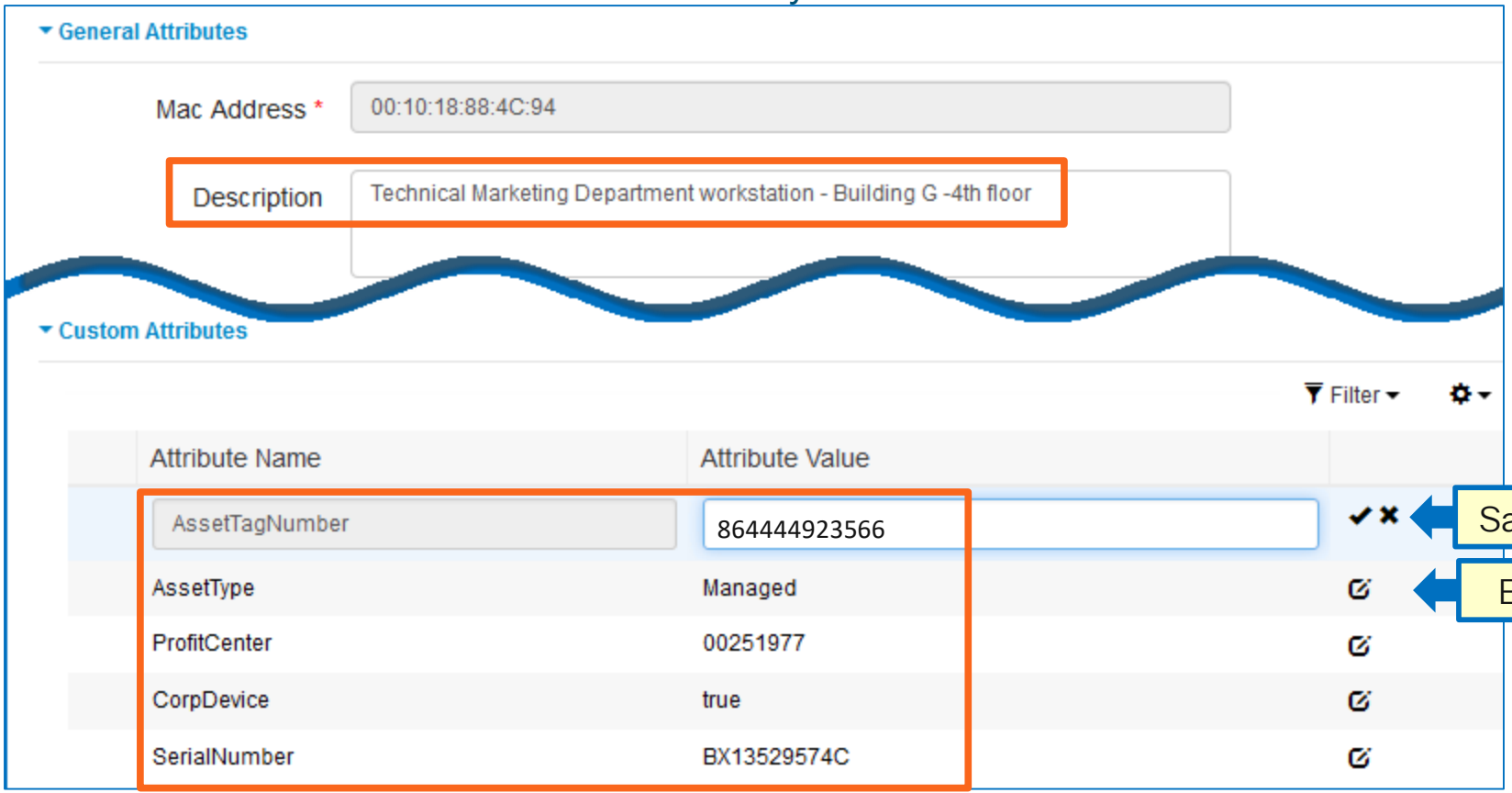
String
Int
Boolean
Float
Long
IP
Date

Once defined, Custom Attributes can be set using:

- Admin UI
- File/LDAP Import
- ERS API
- pxGrid

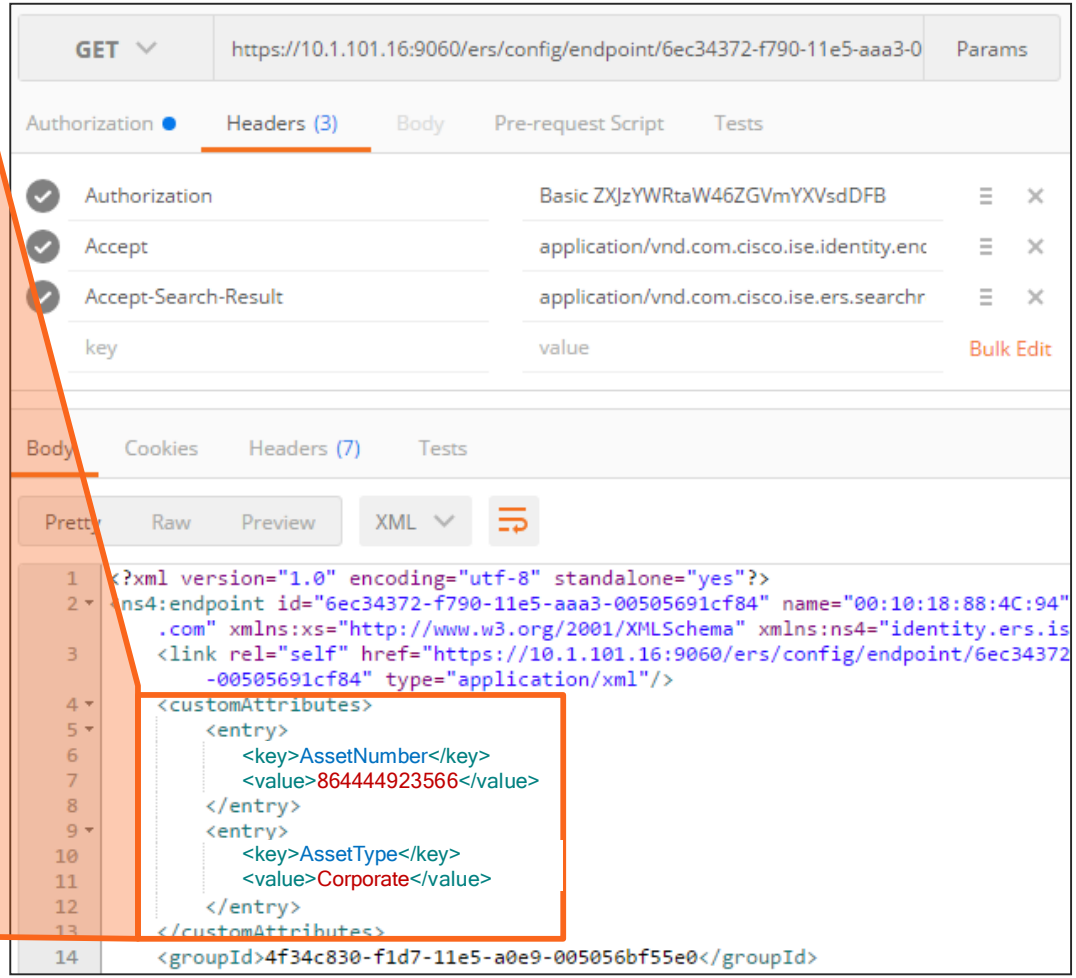
Endpoint Custom Attributes

Edit Attributes From Context Visibility



Endpoint ERS API

```
<customAttributes>
    <entry>
        <key>ProfitCenter</key>
        <value>00251977</value>
    </entry>
    <entry>
        <key>CorpDevice</key>
        <value>true</value>
    </entry>
    <entry>
        <key>AssetNumber</key>
        <value>864444923566</value>
    </entry>
    <entry>
        <key>AssetType</key>
        <value>Corporate</value>
    </entry>
</customAttributes>
```

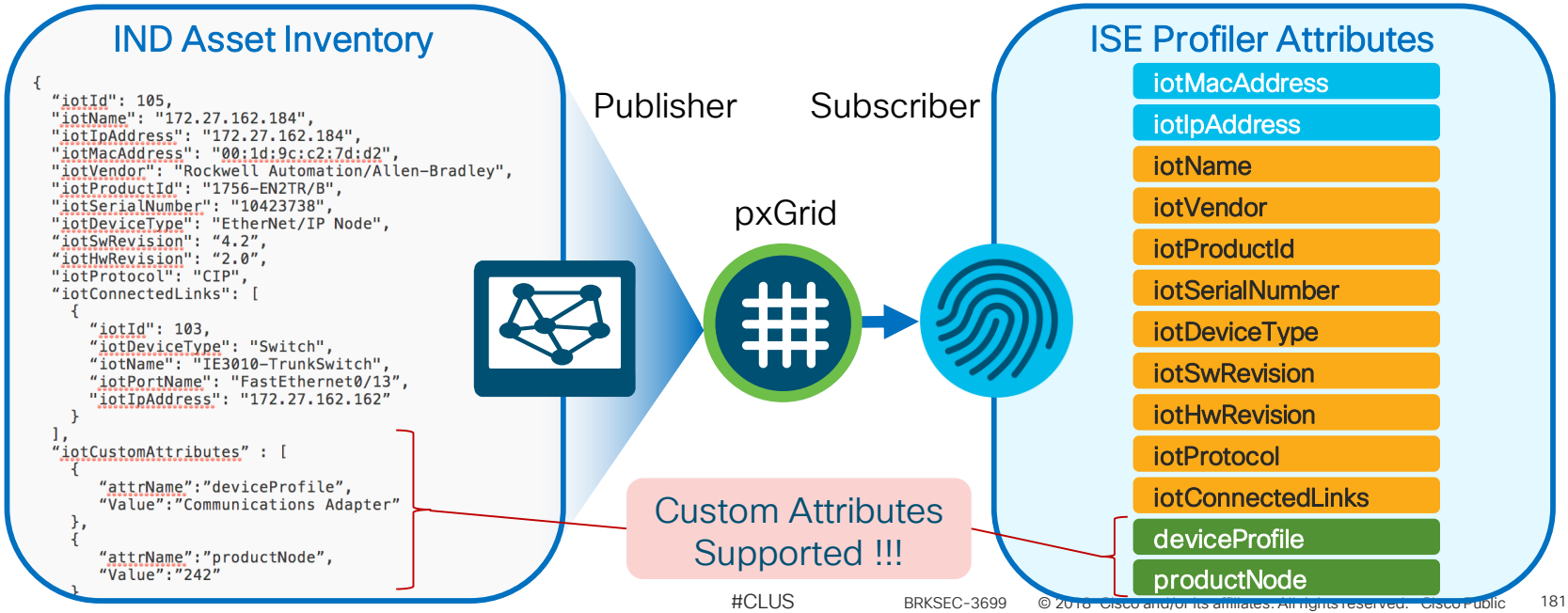


pxGrid Probe (Context In)

Industrial Network Director (IND) Example

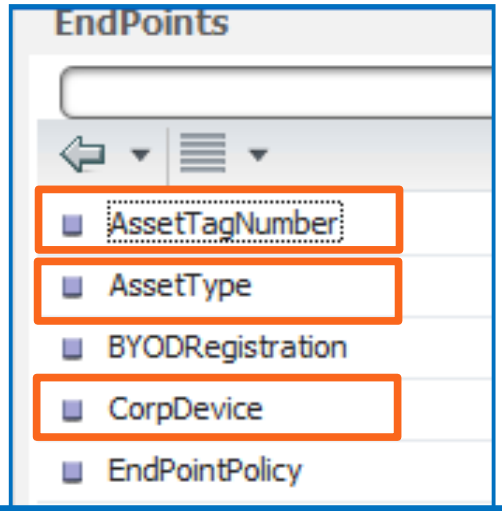
New in ISE 2.4

- IND communicates with Industrial Switches and Security Devices and collects detailed information about the connected manufacturing devices.
- IND v1.3 adds pxGrid Publisher interface to communicate IoT attributes to ISE.

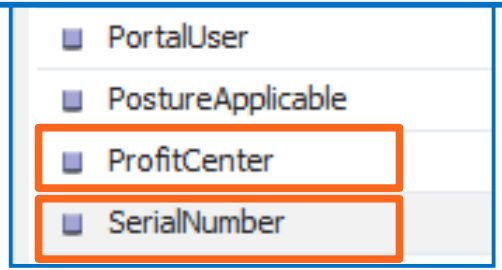


Custom Endpoint Attributes

- Exposed to Authorization Policy Rule Conditions



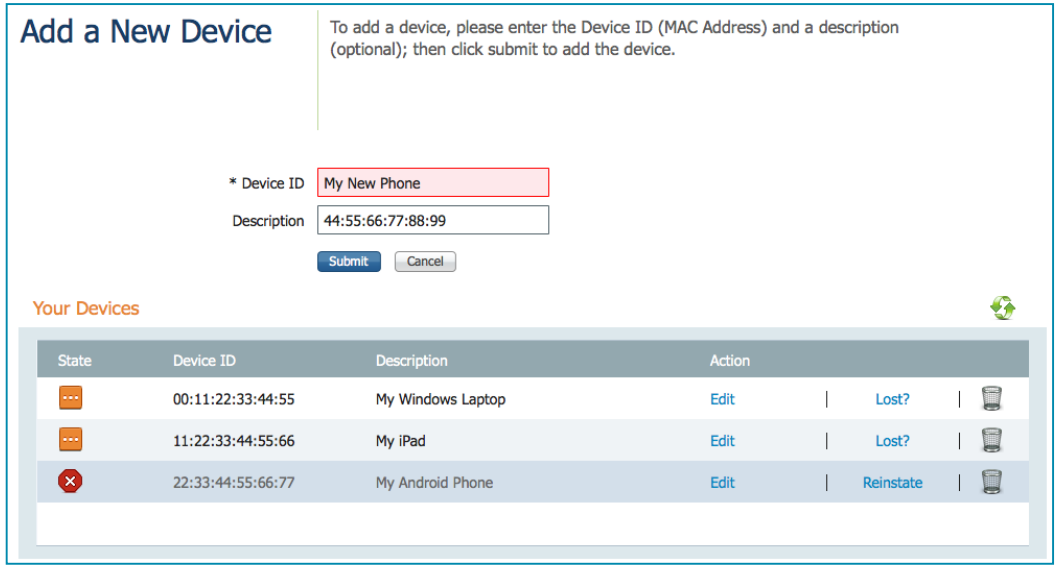
Rule Name		Conditions (identity groups and other conditions)		Permissions
Corporate PC Policy	if	(EndPoints:CorpDevice EQUALS True AND EndPoints:EndPointPolicy EQUALS Microsoft-Workstation)	then	PermitAccess



Identifying Corporate Assets

Device Registration

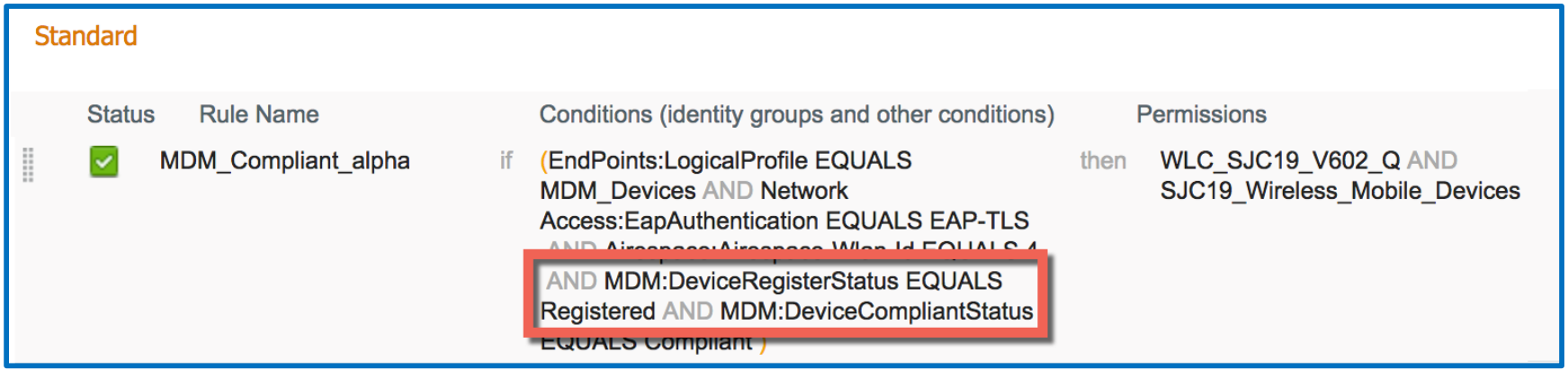
- Is a user-registered device a *corporate* asset?
- Registered devices added from self-serve portals used to track *personal* devices.
- Cannot validate self-registered devices as 'corporate' unless use some other method.



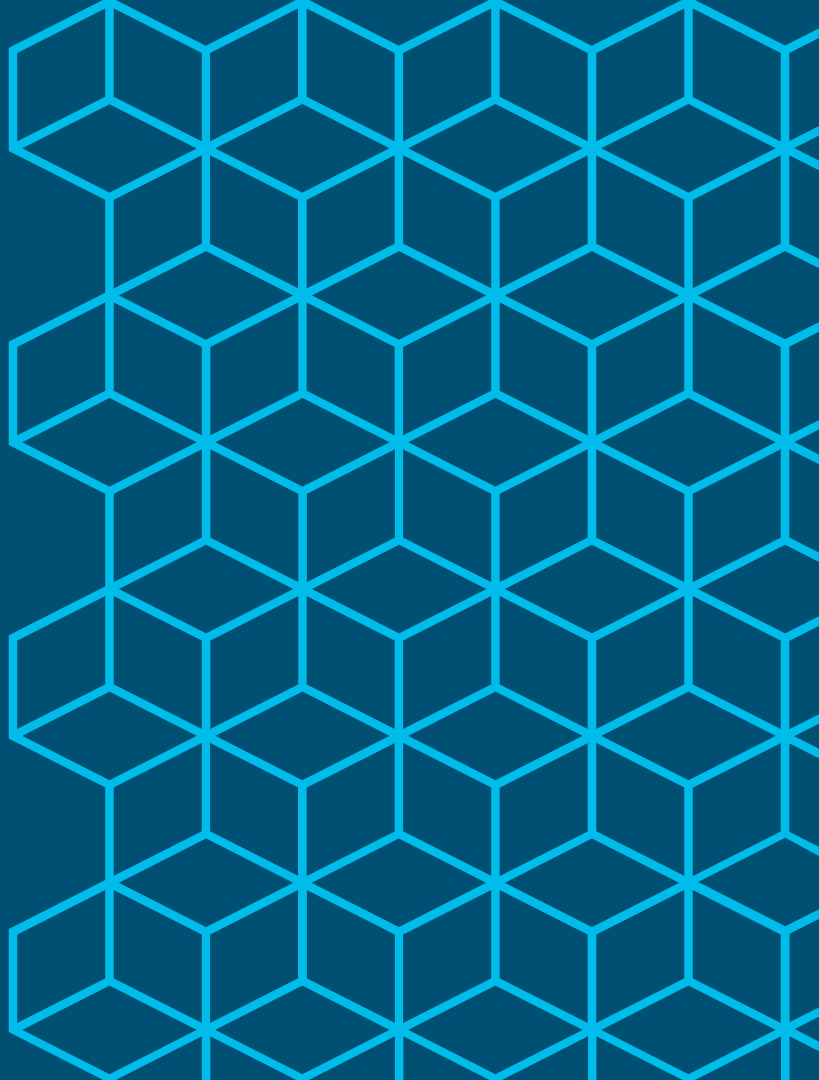
External Device Registration

Is Device Registered in a Trusted System?

- ISE can check enrollment and compliance with most MDM/EMM vendors as well as SCCM and Intune.



Methods for Linking Trusted Devices with Trusted Users



Identifying the Machine AND the USER

Machine Access Restrictions (MAR)

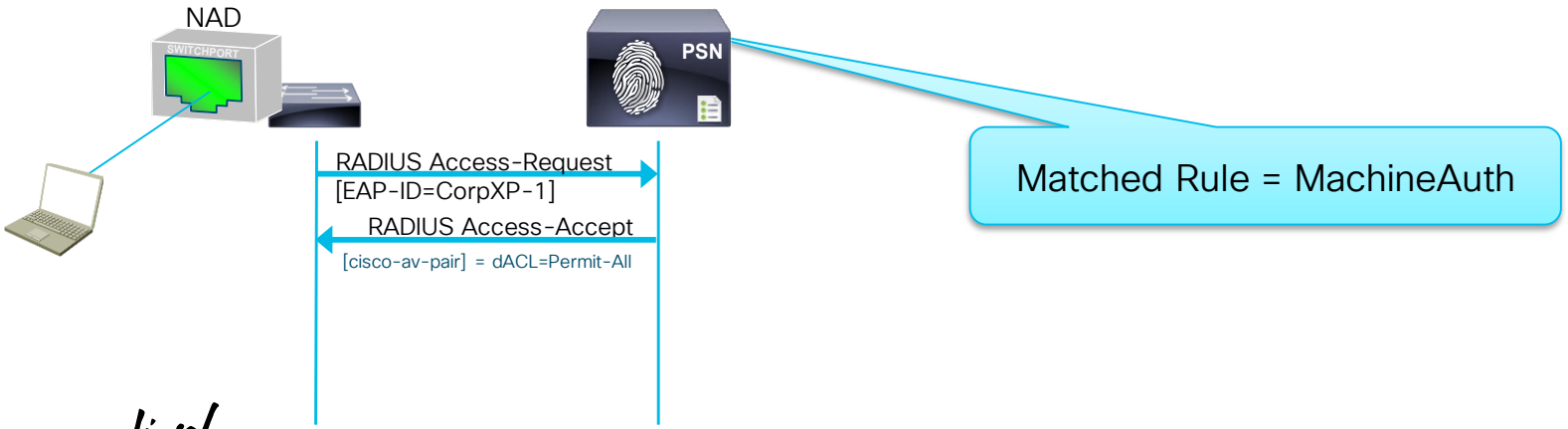
- MAR provides a mechanism for the RADIUS server to search the previous authentications and look for a machine-authentication with the same Calling-Station-ID.
- This means the machine must authenticate before the user.
  - i.e. Must log out, not use hibernate, etc….
- See the reference slides for more possible limitations.

Machine Access Restrictions (MAR)

MAR Cache

Calling-Station-ID 00:11:22:33:44:55 – Passed

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	**if**	**Domain Computers**	**then**	**MachineAuth**
Employee	if	Employee & WasMachineAuthenticated = true	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	

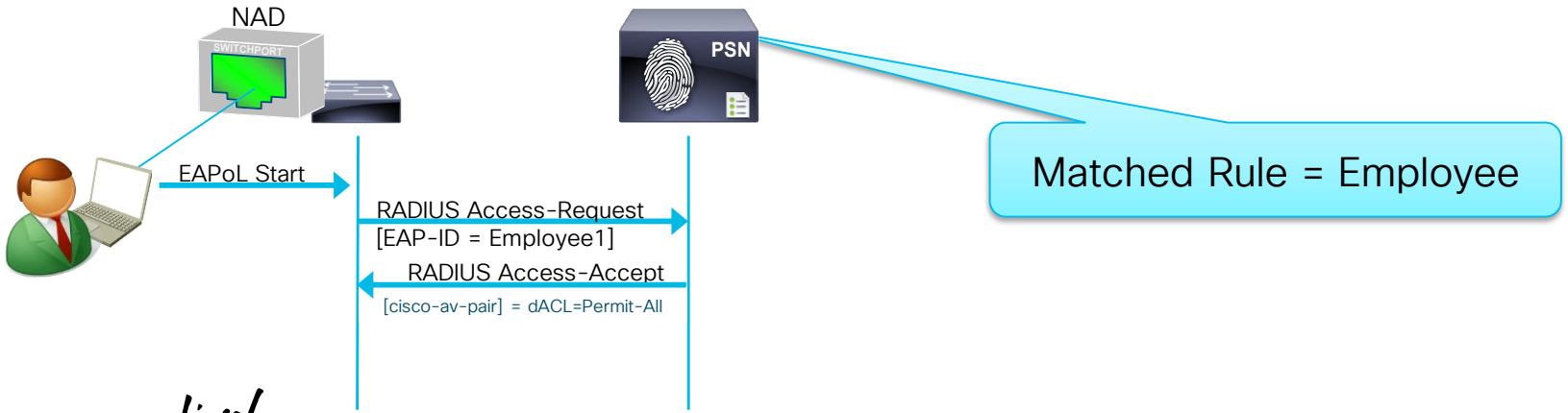


Machine Access Restrictions (MAR)

MAR Cache

Calling-Station-ID 00:11:22:33:44:55 – Passed

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	if	Domain Computers	then	MachineAUth
Employee	**if**	**Employee & WasMachineAuthenticated = true**	**then**	**Employee**
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	



Problems Faced Today w/ Secure Network Access

- What Certificates do I Trust For EAP?
- How can I easily get a Certificate onto my Systems
- Easily Renew My Certificates
- Identify Computer and User

TEAP vs. Other EAP Types

	EAP- TEAP (RFC-7170)	EAP-FASTv2 (Proprietary)	EAP-PEAP	EAP-TTLS (RFC-5281)
Certificate Provisioning in-band	✓	✗	✗	✗
Distribute EAP Server Trust-List	✓	✗	✗	✗
User + Machine EAP Chaining	✓	✓	✗	✗
Posture Transport in-band (PT-TLS or PT-EAP)	✓	✗	✗	✗
Certificate Renewals in-Band	✓	✗	✗	✗
Fast Reconnect w/ Server	✓	✗	✗	✓
Fast Reconnect w/ PAC File	✓	✓	✗	✗

Identifying the Machine AND the User

The next chapter of authentication: EAP-Chaining

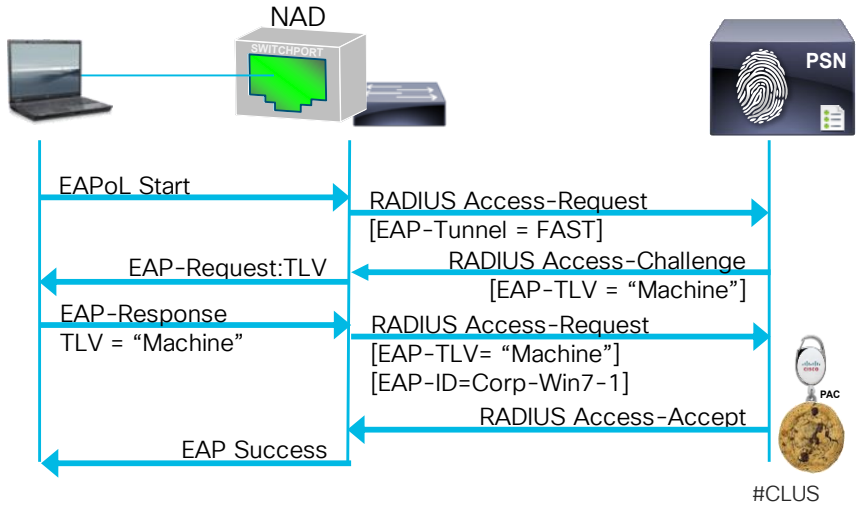
- RFC-7170: Tunneled EAP (TEAP).
  - Next-Generation EAP method that provides all benefits of current EAP Types.
  - Also provides EAP-Chaining.
  - http://www.rfc-editor.org/rfc/rfc7170.txt
- Cisco did it YEARS before TEAP was/is adopted
  - EAP-FASTv2
  - AnyConnect 3.1+
  - Identity Services Engine 1.1.1+
  - **Adopted & in Production at Organizations World-Wide!
    - Only True Chain of Machine + User

EAP-Chaining

With AnyConnect 3.1.1 and ISE 1.1.1

1. Machine Authenticates
2. ISE Issues Machine AuthZ PAC

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	**if**	**Domain Computers**	**then**	**MachineAuth**
Employee	if	Employee & Network Access:EAPChainingResult = User and machine suceeded	then	Employee
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	



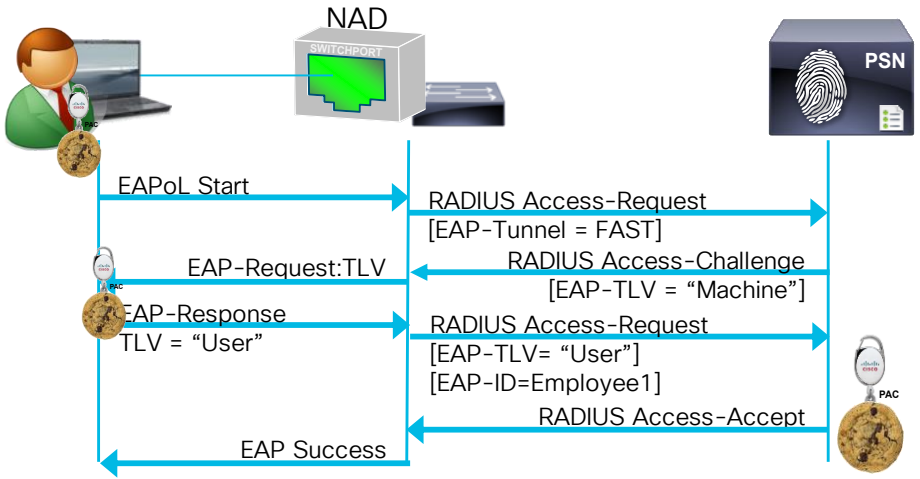
PAC = Protected Access Credentials

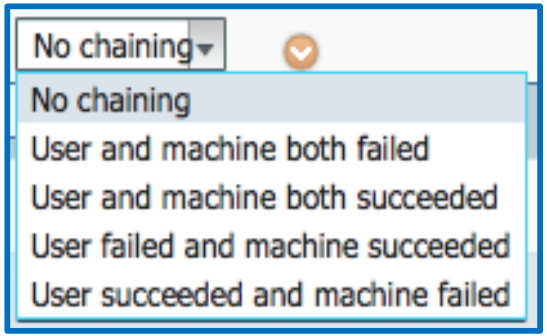
EAP-Chaining

With AnyConnect 3.1.1 and ISE 1.1.1

3. User Authenticates
4. ISE receives Machine PAC
5. ISE issues User AuthZ PAC

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
MachineAuth	if	Domain Computers	then	MachineAuth
Employee	**if**	**Employee & Network Access:EAPChainingResult = User and machine suceeded**	**then**	**Employee**
GUEST	if	GUEST	then	GUEST
Default	If no matches, then		WEBAUTH	





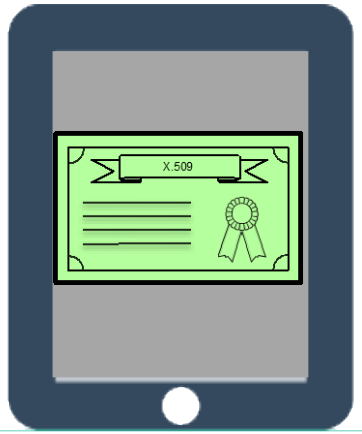
Identifying the Machine AND the User

What to do when EAP-Chaining is not Available?

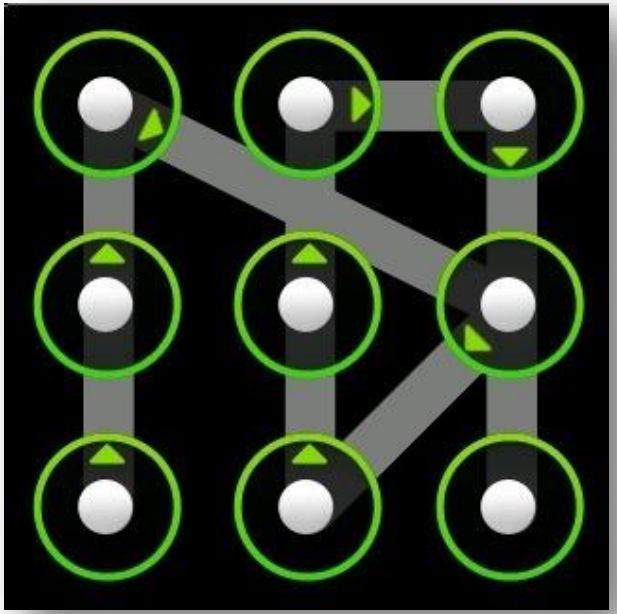
- There are many requirements to determine Machine AND the User
  - Windows is the only current OS that can run EAP-Chaining (with AnyConnect)
  - What about iOS or Android based Tablets?
- Chain together 802.1X with Easy Connect (EZC)
  - Validate the device using machine auth or user-issued certificate
  - Validate the user with AD or other credentials learned from external provider
- Chain together 802.1X with Centralized Web Authentication (CWA)
  - Validate the device using machine auth or user-issued certificate
  - Validate the user with username/password or SAML auth

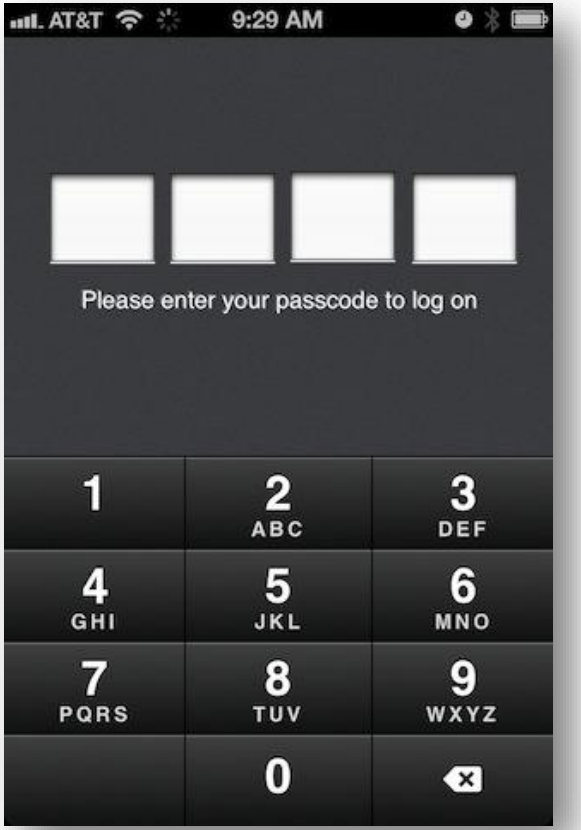
Mobile Device w/ Certificate

What Identifies the Actual User?



Mobile Device
w/ Certificate

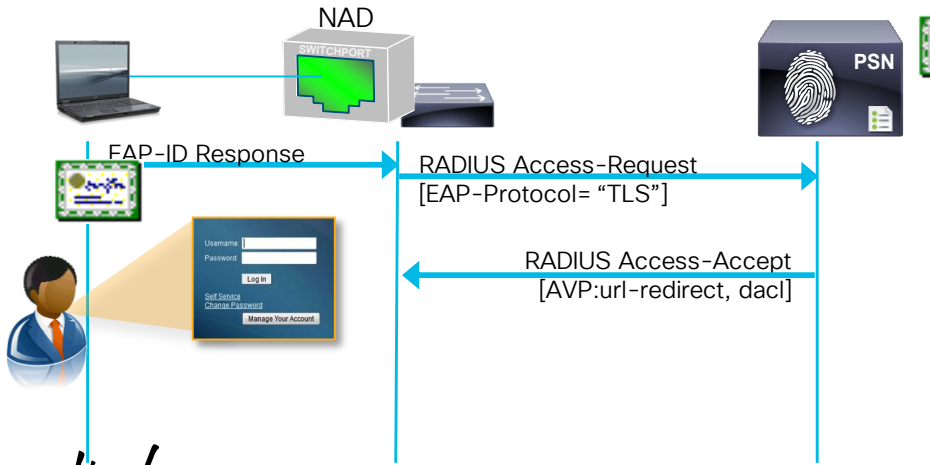




802.1X and CWA Chaining

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

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



CN=employee1 || Cert is Valid

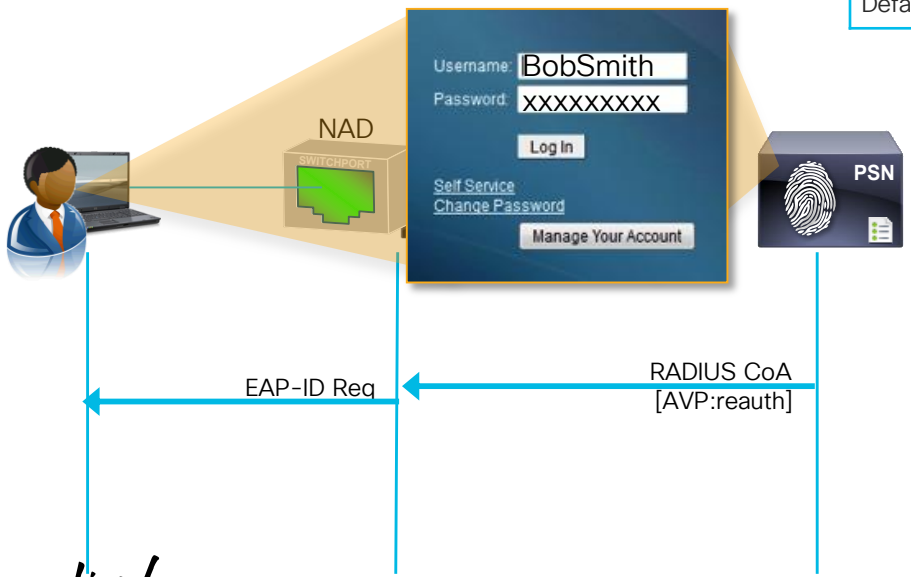
Session Data

User Identity = employee1
User Group = employees

802.1X and CWA Chaining

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
Employee_CWA	if	AD:ExternalGroup=Employees AND CWA:CWA_ExternalGroup= Employees	then	Employee & SGT
Employee_1X	if	Employee & Network Access: EAPAuthentication = EAP-TLS	then	CWAchain
Default	If no matches, then		WEBAUTH	

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



Session Data

User Identity = employee1
User Group = employees

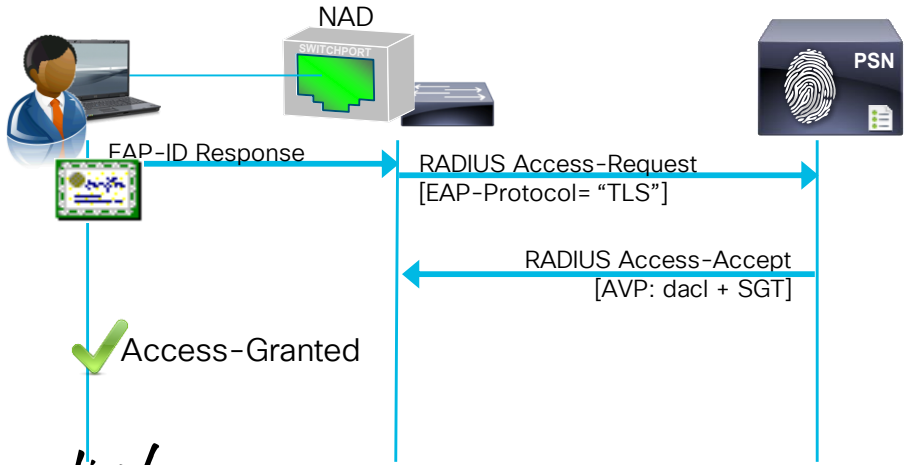
+

CWA Identity = BobSmith
CWA Group = employees

802.1X and CWA Chaining

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

Rule Name		Conditions		Permissions
IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phone
Employee_CWA	if	AD:ExternalGroup=Employees AND CWA:CWA_ExternalGroup= Employees	then	Employee & SGT
Employee_1X	if	Employee & Network Access: EAPAuthentication = EAP-TLS	then	CWAchain
Default	If no matches, then		WEBAUTH	



CN=employee1 || Cert is Valid

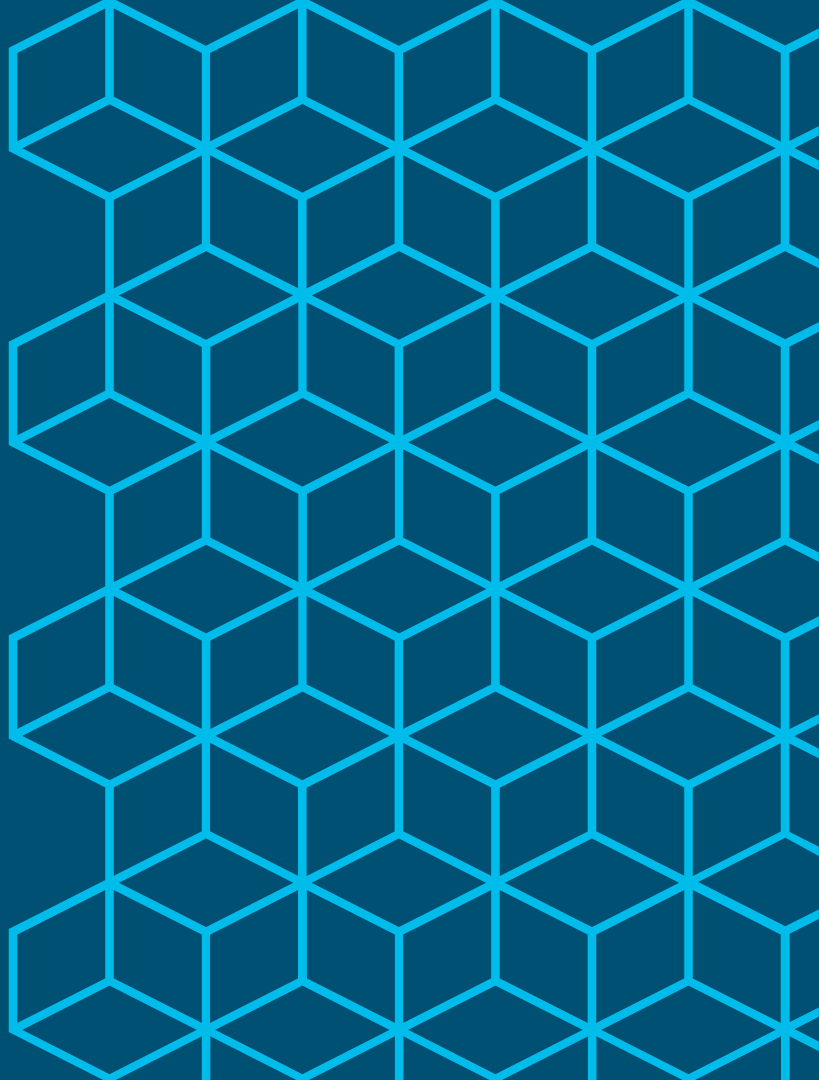
Session Data

User Identity = employee1
User Group = employees

+

CWA Identity = BobSmith
CWA Group = employees

Trusted Device and Trusted User Putting it All Together



Identifying Trusted Devices

ISE Profiling

- Device Classification and Trusted (Whitelist)  Identification

Profiling Source	Condition
DNS	Matching Hostname/Domain Name
NMAP	SMB Discovery for matching AD domain name
NMAP	McAfee ePO Agent Detection
AD Probe	Computer exists in AD domain
DHCP	Custom User Class ID pushed via GPO
pxGrid	Endpoint Assets published by external source

Identifying Trusted Devices

Other options to identify trusted computers

Source	Description
AD/LDAP/ODBC/RADIUS	Lookup device in existing trusted ID store
MDM / EMM	Lookup device in existing trusted DM store
Posture	Endpoint inspection for managed device attribs
Device Registration	Admins / Trusted users vouch for device
BYOD	Onboard personal assets as trusted device
Import / API	Seed inventory of managed / trusted devices
Custom Attributes	Import/API marking of trusted endpoints

Matching Trusted Users to Trusted Devices

Combinations Flows

Source	Description
MAR	Cache previous successful Machine Auth event and link to user auth with same MAC
CWA Chaining	Link Web Authentication to current 802.1X auth
EZC Chaining	Link Passive ID to current MAB/802.1X auth
EAP Chaining	Link Machine 802.1X and User 802.1X auth
TEAP	Link Machine 802.1X and User 802.1X auth

Implicit Device Trust

- 802.1X User Authentication using non-Exportable certificates
- 802.1X User Authentication with embedded device data in certificate
  - Example, match authenticating MAC address to issued certificate value
- Multi-Factor authentication (MFA) based on individual user input.
- Devices authenticated using Easy Connect are implicitly members of AD domain
  - In order trigger AD login event, device must be member of domain
  - AD login is not simply authentication using AD credentials

Trusted Device and Trusted User Policies

 = Implicitly Trusted Device  = Trusted Device  = Trusted User

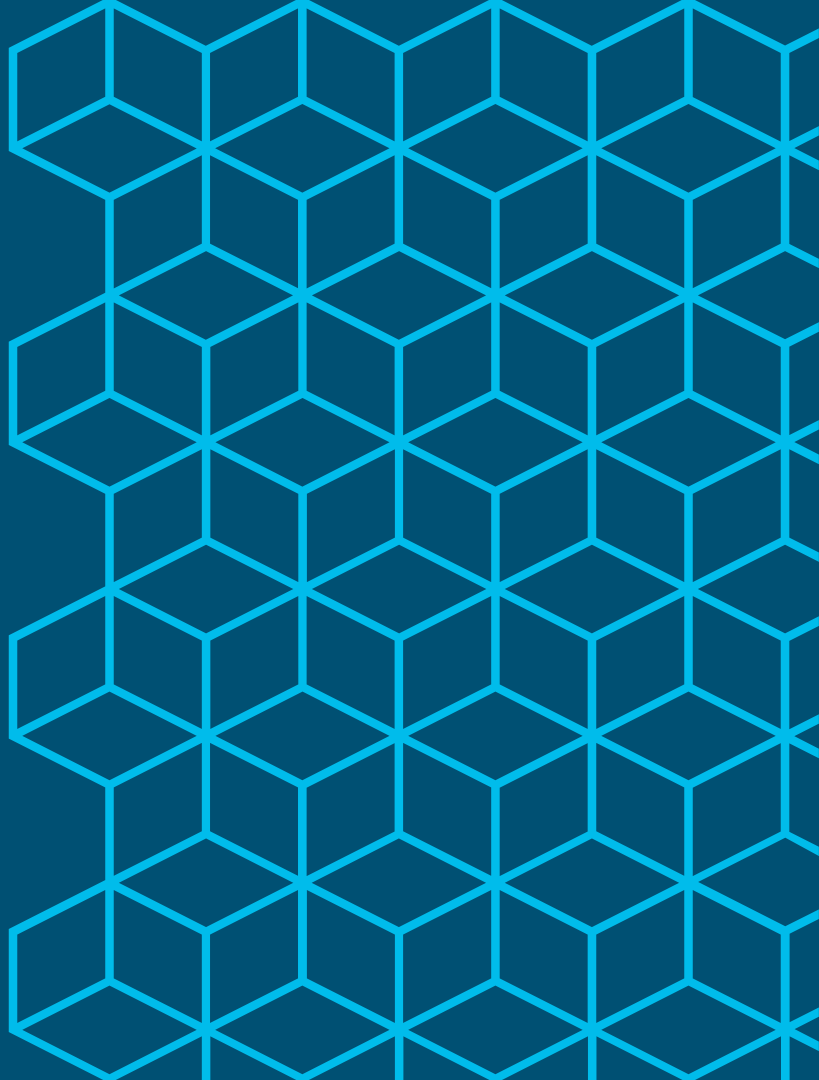
Auth Method	Sample Auth Policy	SGT		
802.1X Machine + User (EAP Chain)	AD_PC_Employee_1X	AD_PC-Employee		
802.1X Machine + EZC (EZC Chain)	AD_PC_Employee_EZC	AD_PC-Employee		
802.1X Machine + CWA (CWA Chain)	AD_PC_Employee_WebAuth	AD_PC-Employee		
802.1X User Auth + EZC (EZC Chain)	Employee_1X_EZConnect	AD_PC-Employee		
802.1X User Auth	Employee_1X	Employee		
802.1X Machine Auth Only	AD_PC_1X	AD_Computer		
MAB + EZConnect (no 1X)	Employee_EZConnect	AD_PC-Employee		
MAB + CWA (no 1X)	Employee_WebAuth	Employee		
MAB + Trusted Device Profile	AD_PC_MAB	AD_Computer		

Trusted Device and Trusted User Policies

* Include Trusted Device Profile  = Trusted Device  = Trusted User

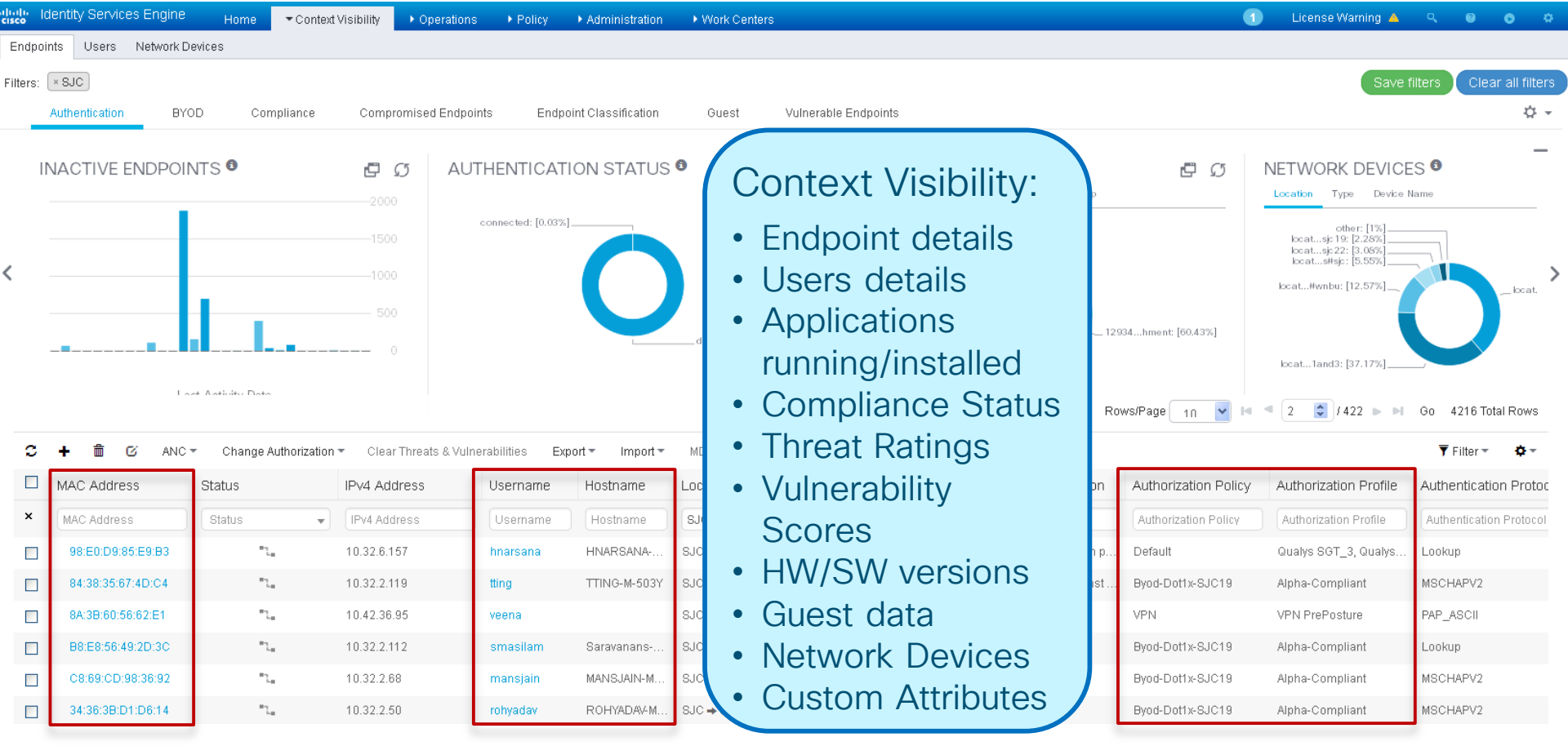
Auth Method	Sample Auth Policy	SGT		
802.1X Machine + User (EAP Chain)	AD_PC_Employee_1X	AD_PC-Employee	✓	✓
802.1X Machine + EZC (EZC Chain)	AD_PC_Employee_EZC	AD_PC-Employee	✓	✓
802.1X Machine + CWA (CWA Chain)	AD_PC_Employee_WebAuth	AD_PC-Employee	✓	✓
802.1X User Auth + EZC (EZC Chain)	Employee_1X_EZConnect	AD_PC-Employee	✓	✓
802.1X User Auth	Employee_1X	Employee	✓	✓
802.1X Machine Auth Only	AD_PC_1X	AD_Computer	✓	
MAB + EZConnect (no 1X)	Employee_EZConnect	AD_PC-Employee	✓	✓
MAB + CWA (no 1X)	Employee_WebAuth	Employee	✓	✓
MAB + Trusted Device Profile	AD_PC_MAB	AD_Computer	✓	

Context Visibility



Context Visibility

Authenticated Devices – Filter by Trusted Device/Trusted User Policy

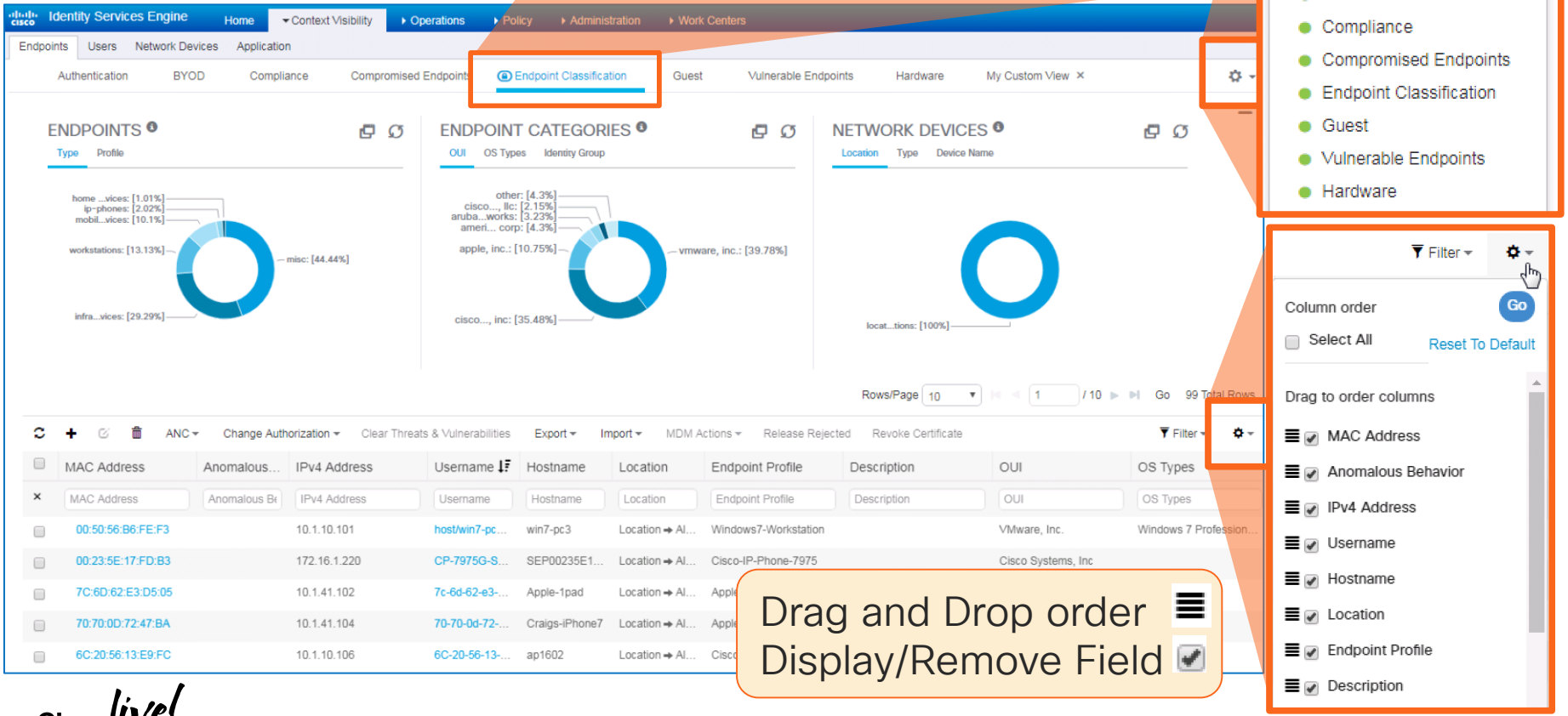


Context Visibility:

- Endpoint details
- Users details
- Applications running/installed
- Compliance Status
- Threat Ratings
- Vulnerability Scores
- HW/SW versions
- Guest data
- Network Devices
- Custom Attributes

Context Visibility

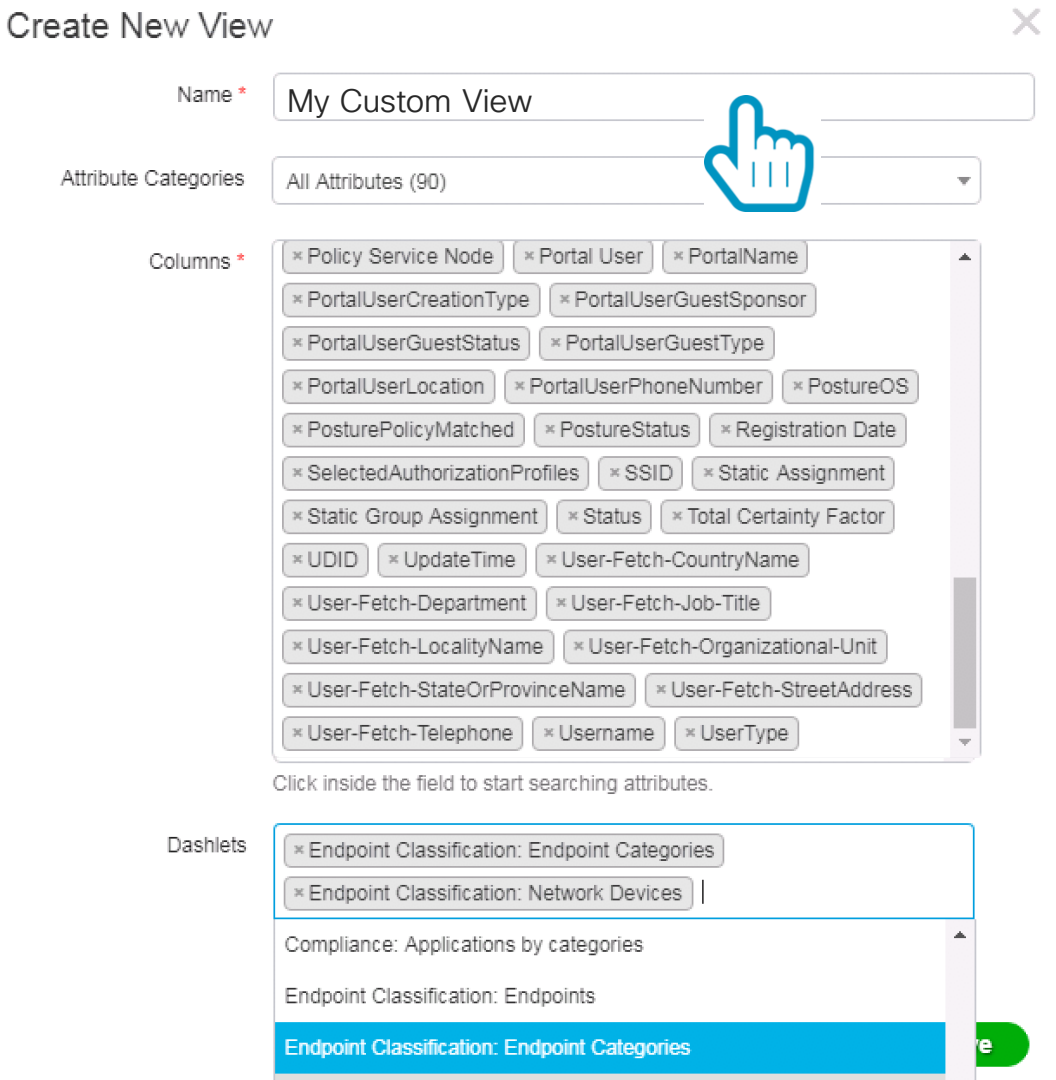
Admin Personalization



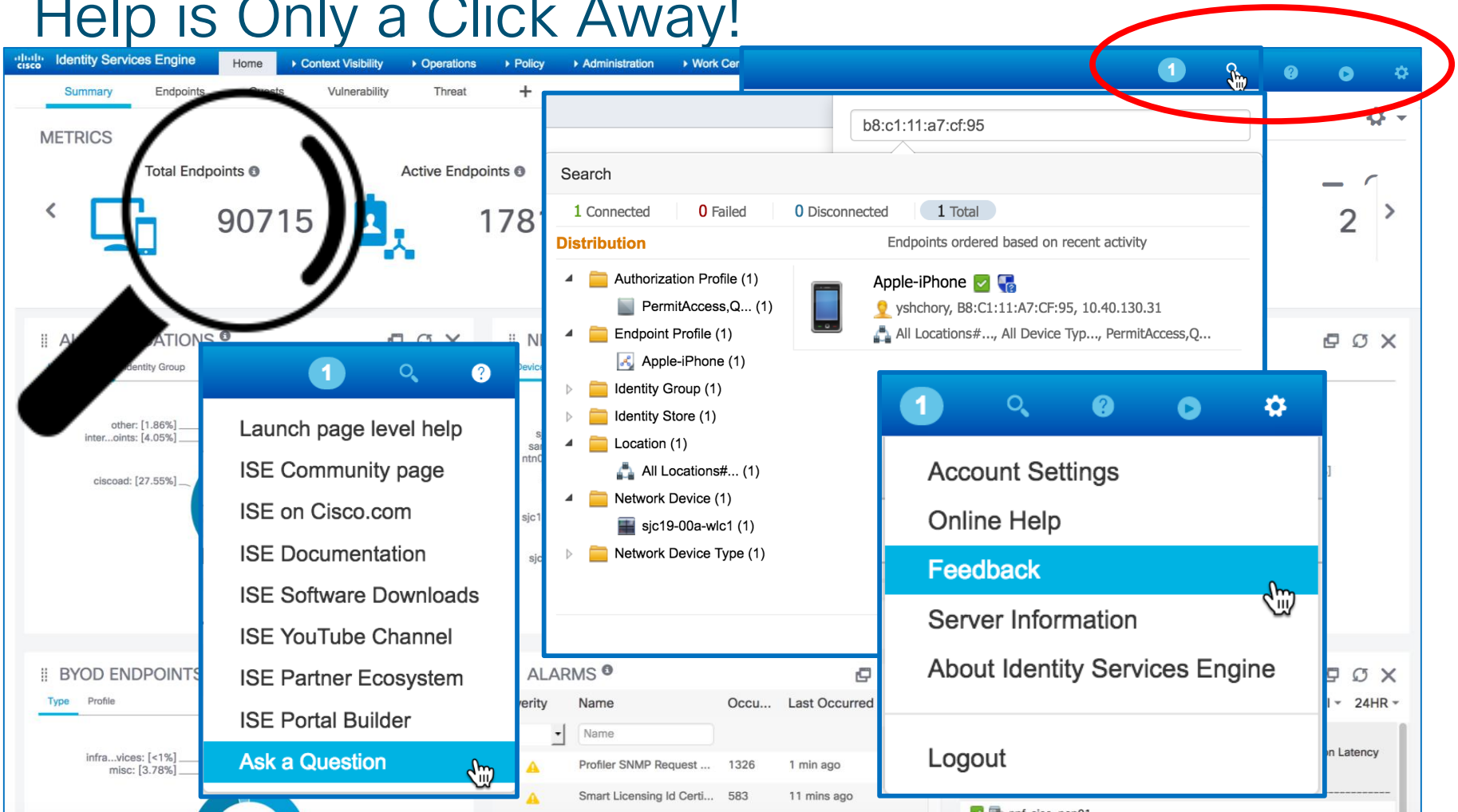
Context Visibility

Custom Views

- Admin-Specific Views
- Choose the Attributes
- Choose the associated dashlets.
- Use the table editor to manage column width, order, and columns to display.



Help is Only a Click Away!

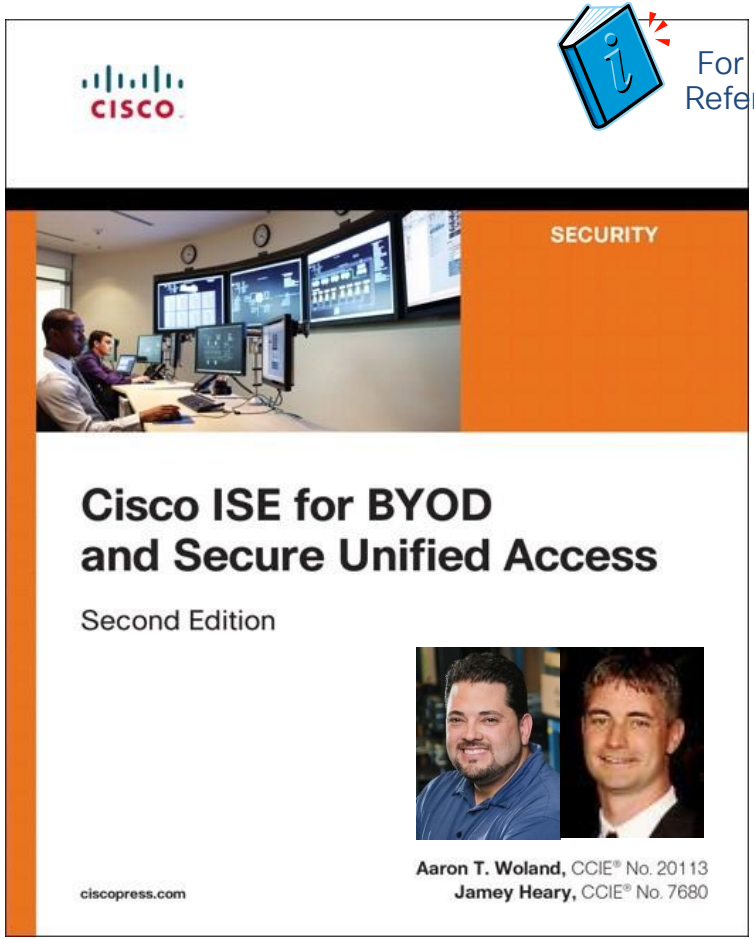


Summary

- In addition to comprehensive authentication and authorization services, ISE detects all users and things connected to the network and collects rich context used for policy decisions.
- The data collected by ISE directly, or learned from external sources of truth, serves as the basis for managing access of trusted devices and trusted users to services.
- Context can be used by ISE but also shared with other systems to provide higher degrees of visibility, efficiency, and effectiveness in connected systems.

Recommended Reading

- http://www.ciscopress.com/store/cisco-ise-for-byod-and-secure-unified-access-9781587144738
- http://amzn.com/1587144735



For Your Reference

For Your Reference

Additional Resources

ISE Public Community	http://cs.co/ise-community
ISE Compatibility Guides	http://cs.co/ise-compatibility
ISE Design Guides	http://cs.co/ise-guides

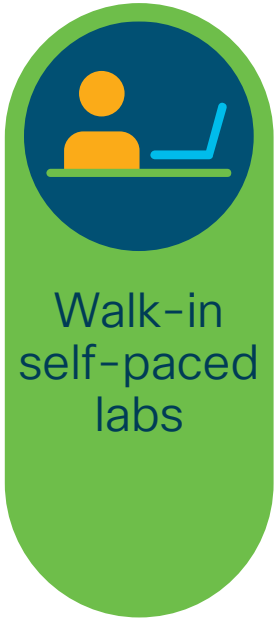
Complete your online session evaluation

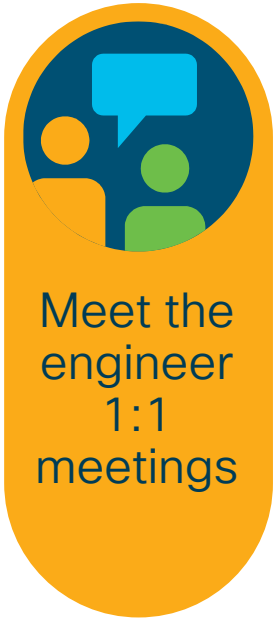
Give us your feedback to be entered into a Daily Survey Drawing.

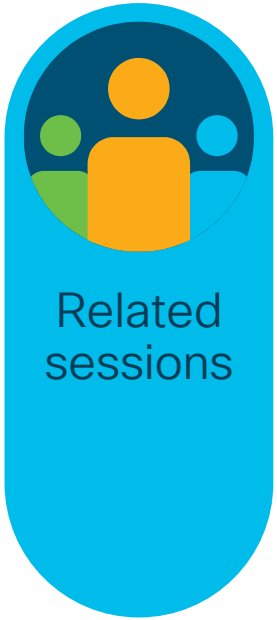
Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.

Continue your education







Thank you

INTUITIVE