

INTUITIVE

**Cisco** *live!*  
June 10-14, 2018 • Orlando, FL



# Advanced ISE Services, Tips & Tricks

Craig Hys, Principal Engineer  
BRKSEC-3697



Cisco *live!*

#CLUS



INTUITIVE

# 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

You Are Here

# @Live Orlando 2018

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



# Cisco Webex Teams

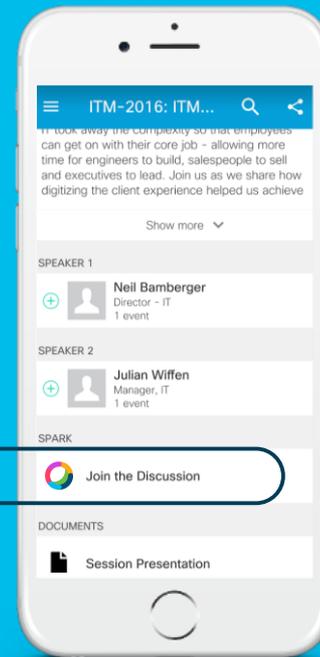
## Questions?

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](https://cs.co/ciscolivebot#BRKSEC-3697)

# Where can I get help after Cisco Live?



ISE Public Community

<http://cs.co/ise-community>

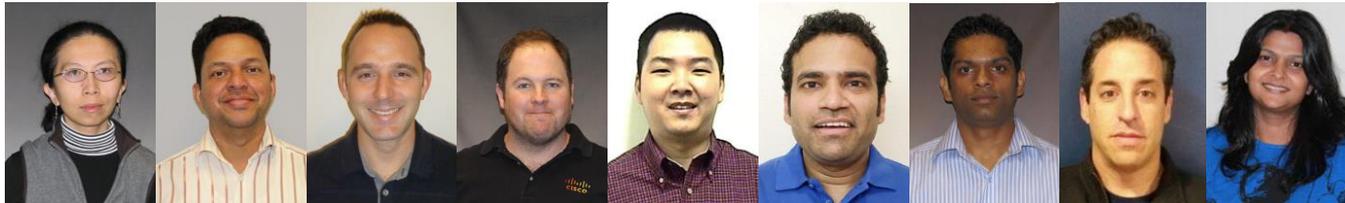
Questions answered by ISE TMEs and other Subject Matter Experts – the same persons that support your local Cisco and Partner SEs!

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	<del>8</del> 12	2.0	12,000	16	6	200GB	PSN/PXG
						600GB	PAN/MnT
SNS3595	<del>8</del> 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 Counters ⓘ  
From 2018-01-14 00:00:00.0 to 2018-01-14 15:14:21.104

Filters ⓘ

- \* Server [dropdown] Is exactly (or equals) [dropdown] ise22-pan1
- \* Time Range [dropdown] Is exactly (or equals) [dropdown] Today

Counter Attribute Threshold

Attribute Name	ISE Profile
ARP Cache Insert Update Received	UCS_SMALL
DHCP Endpoint Detected	UCS_SMALL
DHCP Skip Profiling	UCS_SMALL

# 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)

MnT



\* 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

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 2880 Client Stopped Responding 480 Repeat Counter 0

Refresh Never Show Latest 50 records Within Last 30 minutes

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Ide
Jan 26, 2018 11:06:16.262 AM			0	susain	98:5A:EB:8E:FD:16	Apple-Device	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.16			
Jan 26, 2018 11:05:50.519 AM				jjose2	98:F1:70:33:42:B0						sbgise-bgl13-00...		
Jan 26, 2018 11:05:34.504 AM				INVALID			Building_SJ...	Building_SJ...			WNBU-WLC1		
Jan 26, 2018 11:05:32.821 AM				INVALID			Building_SJ...	Building_SJ...			sjc14-22a-talwar		
Jan 26, 2018 11:05:23.126 AM			0	50:1A:C5:DD:7A:AF	50:1A:C5:DD:7A:AF	Microsoft-W...	Location_NT...	Location_NT...	WLC_NTN...				
Jan 26, 2018 11:05:23.126 AM				50:1A:C5:DD:7A:AF	50:1A:C5:DD:7A:AF	Microsoft-W...	Location_NT...	Location_NT...	WLC_NTN...		NTN-WLC1		Wo
Jan 26, 2018 11:05:11.995 AM				vani	AC:BC:32:AC:7E:23						sjc19-00a-wlc1		
Jan 26, 2018 11:04:54.173 AM			0	kusenapa	DC:EF:CA:4D:41:F	Unknown	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.46			
Jan 26, 2018 11:04:27.145 AM			0	6C:40:08:92:25:96	6C:40:08:92:25:96	OS_X_EI_C...	Location_BX...	Location_BX...	Guest_Redir...	10.86.103.135			
Jan 26, 2018 11:04:23.999 AM				6C:40:08:92:25:96	6C:40:08:92:25:96	OS_X_EI_C...	Location_BX...	Location_BX...	Guest_Redir...		sampg-bxb22-0...		Wo
Jan 26, 2018 11:04:10.882 AM				INVALID			Building_SJ...	Building_SJ...			sjc14-22a-talwar		
Jan 26, 2018 11:04:06.040 AM				USERNAMEUSE...	4C:EB:42:C7:31:70		Bldg_SJC19...	Bldg_SJC19...			sjc19-00a-wlc1		
Jan 26, 2018 11:04:04.493 AM				jjose2	98:F1:70:33:42:B0						sbgise-bgl13-00...		
Jan 26, 2018 11:04:03.462 AM			0	vinothra	7C:50:49:63:CC:F0	Apple-iPhone	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.14			

# 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.

Identity Services Engine Administration > Work Centers > Admin Access > Settings > Password Policy

The newly added custom dictionary file will replace the existing custom dictionary file.

Password must contain at least one character of each of the selected types:

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numeric characters
- Non-alphanumeric characters

Password History

- Password must be different from the previous  versions [When enabled CLI remembers only last 1 password irrespective of value configured]
- \* Cannot reuse password within  days (Valid Range 0 to 365)

**Password Lifetime**

Admins can be required to periodically change their password

- Administrator passwords expire  days after creation or last change (valid range 1 to 3650)
- Require Admin password
- Password cached for  Minutes (1-60)

Save Reset

```
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.

True RO Admin added ISE 2.3!

Administrators List > ro-admin

▼ Admin User

\* Name

Status  Enabled ▼

Email   Include system alarms in emails

External  ⓘ

Read Only

Inactive account never disabled

▼ Password

\* Password  ⓘ

\* Re-Enter Password  ⓘ

▼ User Information

First Name

Last Name

▼ Account Options

Description

▶ Admin Groups

Read Only Admin Policy If  then

- Super Admin Menu Access
- Read Only Admin Data Access

 Modifying data access to Read only admin policy is not allowed

Cannot edit when RO enabled

# Configure ERS API

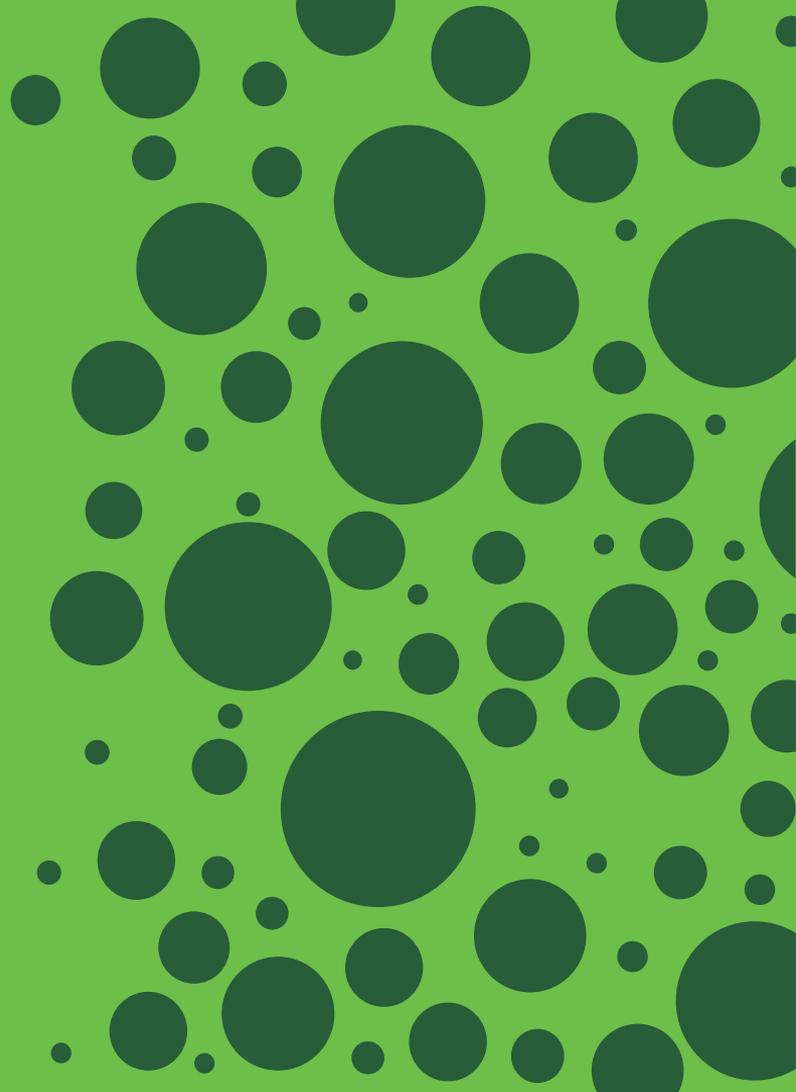
1. Enable ERS
2. Create ERS Admin user
3. Add to ERS Admin Group

The screenshot shows the Cisco Identity Services Engine Administration interface. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and PassivID. The main content area is titled "ERS Settings" and contains a "General" section with the following text: "External RESTful Services (ERS) is a REST API based on HTTPS over port 9060. The ERS service is disabled by default. An ISE Administrator with the 'ERS-Admin' or 'ERS-Operator' group assignment is required to use the API. For more information, please visit the ERS SDK page at: <https://10.1.101.16:9060/ers/sdk>". Below this, the "ERS Setting for Administration Node" section has a radio button selected for "Enable ERS for Read/Write", which is highlighted with an orange box. The text "For Your Reference" is visible on the right side of the screenshot.

The screenshot shows the Cisco Identity Services Engine Administration interface, specifically the "Administrators" page. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, PassivID, and Threat Centric NAC. The main content area is titled "Administrators" and contains a table with the following data:

Status	Name	Description	First Name	Last Name	Email Address	Admin Groups
<input checked="" type="checkbox"/>	admin	Default Admin User				Super Admin
<input checked="" type="checkbox"/>	ersadmin	password = default1A				ERS Admin

# 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. 29-MAR-2018

[ise-urtbundle-2.4.0.357-1.0.0.SPA.x86\\_64.tar.gz](#)

- 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

Overview Upgrade

Read only mode. Click the Upgrade tab to proceed.

Node Group - Host Name	Persona	Version - Repository	Status
npf-sjca-pap02.cisco.com	Admin secondary	2.4.0.358	Active
npf-sjca-mnt02.cisco.com	Monitor (PRIMARY)	2.4.0.358	Active
sbg-bglia-pdp01.cisco.com	Policy service	2.4.0.358	Active
npf-sjca-px02.cisco.com	pxGrid	2.4.0.358	Active
npf-sjca-pdp01.cisco.com	Policy service	2.4.0.358	Active
npf-sjca-pdp02.cisco.com	Policy service	2.4.0.358	Active
npf-sjca-pdp04.cisco.com	Policy service	2.4.0.358	Active
npf-sjca-px01.cisco.com	pxGrid	2.4.0.358	Active
npf-sjca-mnt01.cisco.com	Monitor (PRIMARY)	2.4.0.358	Active
npf-sjca-pap01.cisco.com	Admin secondary	2.4.0.358	Active

1 Review Checklist 2 Download Bundle to Node(s) 3 Upgrade Node(s)

Print Checklist Review the checklist before you begin upgrading the nodes.

Backup ISE

- Configuration and operational data (see Administration > System > Backup & Restore)
- Backup system logs (see Operations > Troubleshoot > Download Logs)
- Export certificates and private keys (see Administration > System > Certificates > System Certificates)

Software

- Review the ISE Upgrade Checklist
- Confirm valid ISE Upgrade Bundles
- Download the ISE Upgrade Bundles

Credentials

- Make a note of the current credentials

Operational Data Purge

- Purge operational data

Cancel Proceed

Overview Upgrade

Deployment Learning Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Deployment (2.0.0.358)

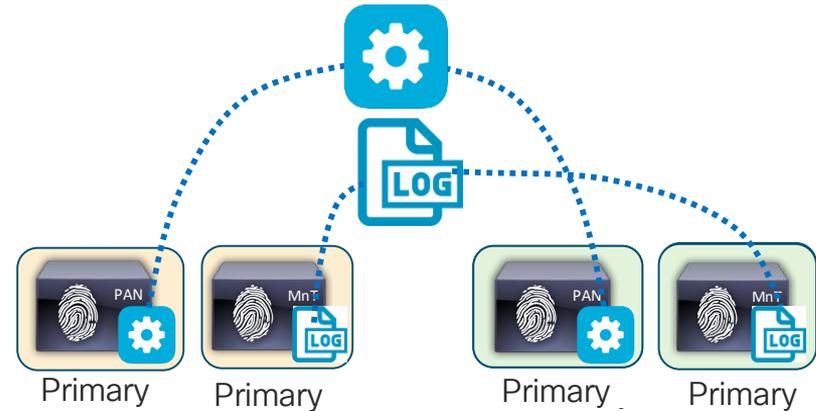
New Deployment Upgrade (2.4.0.358)

Sequence	Node Group - Host Name	Persona	Status	Total estimated time: 240 mins
1	npf-sjca-pap02.cisco.com	Admin secondary	0%	Upgrading...
2	npf-sjca-pap01.cisco.com	Admin secondary	100%	Upgrade queued
3	Select nodes for sequence 3			

Continue with the next node on upgrade failure (applicable for Policy Service Nodes only)

Back Upgrade

## Backup/Restore



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

CSCvi38845 Upgrade fails after Feed update due to less heap space -- 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



Cisco ISE Deployment Guides

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

Introduction.....	3
<i>About Cisco Identity Services Engine (ISE).....</i>	3
<i>About this guide.....</i>	3
Deployment fundamentals .....	5
Plan your Upgrade .....	7
<i>Single Step vs Multi-Step Upgrade .....</i>	7
<i>Life cycle of ISE 1.x release.....</i>	8
<i>What hardware/software should I upgrade to? .....</i>	8
Do I need a hardware upgrade? .....	8
Do I need to upgrade my VM? .....	9
<i>Key considerations for upgrade .....</i>	9
What is better, in-place upgrades or backup/restore? .....	9
Guidelines to minimize upgrade time and maximize efficiency during production upgrade. ....	9
Key functionalities added since ISE 2.x.....	11
<i>Issues, Fixes and other consideration.....</i>	12
<i>Pre-Upgrade Steps.....</i>	13
Upgrade procedure .....	15
<i>Phase 1: Upgrade Secondary Datacenter .....</i>	16
<i>Phase 2: Adding Additional Nodes and upgrade the Primary DC.....</i>	20
Post-Upgrade steps.....	21
<i>Single-Step Upgrade process.....</i>	22

# Cisco Software Notifications

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

**Software Download**

Downloads Home / Security / Network Visibility and Segmentation / Identity Services Engine / Identity Services Engine

Search...

Expand All Collapse All

Latest Release

**2.4.0**

Identity Services Engine

Release 2.4.0

**Notifications**

**Edit Notification**

Identity Services Engine Software | Identity Services Engine System Software

Get notifications about New, Suggested, Software Advised, Deferred, Certified and Obsolete Software releases.

Name your Notification

Interested In

All Releases

2.4.0 and newer

2.4.0 only

An Email Delivered  Sent to

[Edit All Notifications](#)

**Cisco Services**

Cisco Notification Service

[Feedback](#) [Sign Up](#) [Unsubscribe](#)

**Software Updates for Identity Services Engine Software**

**Product Name:** Identity Services Engine Software  
**Software Type:** Identity Services Engine System Software  
**Release Version:** [2.4.0](#)  
**Alert Type:** New File  
**File Name:** [ise-patchbundle-2.4.0\\_357-Patch1-18052411.SPA\\_x86\\_64.tar.gz](#)  
**File Release Date:** 28-MAY-2018

**Software Updates for Identity Services Engine Software**

**Product Name:** Identity Services Engine Software  
**Software Type:** Identity Services Engine System Software  
**Release Version:** [2.0.1](#)  
**Alert Type:** New File  
**File Name:** [ise-patchbundle-2.0.1\\_130-Patch6-18050218.SPA\\_x86\\_64.tar.gz](#)  
**File Release Date:** 30-MAY-2018

Find additional information in [Software Downloads](#) index.

© 2018 Cisco and/or its affiliates. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks](#)

# Auth Policy Tuning and Optimization

# Auth Policy Optimization (ISE 2.2 and Earlier)

## Leverage Policy Sets to Organize and Scale Policy Processing

**Policy Sets**

Search policy names & descriptions.

Summary of Policies  
A list of all your policies

Global Exceptions  
Rules across entire deployment

- Wired
- Wireless**
- VPN
- Default  
Default Policy Set

Save Order Reset Order

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

Status	Name	Conditions
✓	Wireless	Wireless

**Policy Set Condition**

**Authentication**

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)

**Authorization**

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if <b>Blacklist</b>	then Blackhole_Wireless_Access
✓	Domain_Computer	if AD1:ExternalGroups EQUALS cts.local/Users /Domain Computers	then AD_Login
✓	Game Consoles - Registered	if (EndPoint:EndPointPolicy EQUALS Game-Console-Registered AND Radius:Called-Station-ID-ENDS-WITH-naming)	then Game_Console

**Policy Sets**

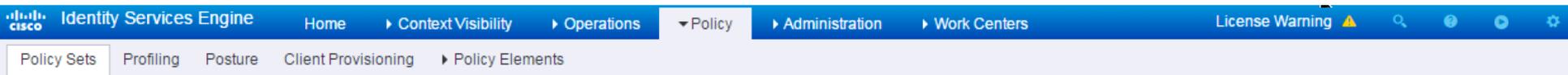
Administration > System > Settings > Policy Sets

BRKSEC-3697

# Policy Sets

Standard Equipment under new ISE 2.3 Policy User Interface

- No Authentication Outer Rule – Now part of Policy Set



## Policy Sets

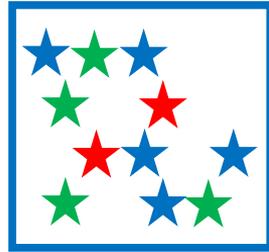
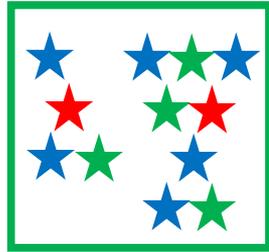
	Status	Policy Set Name	Description	Conditions	Policy Set Condition	Allowed Protocol or RADIUS Proxy	Hit Counts	Actions	View
	<input checked="" type="checkbox"/>	Wired	Wired Network Access		Radius-NAS-Port-Type EQUALS Ethernet	Default Network Access	23456		
	<input checked="" type="checkbox"/>	Wireless	Wireless Network Access		Radius-NAS-Port-Type EQUALS Wireless - IEEE 802.11	Default Network Access	0		
	<input checked="" type="checkbox"/>	VPN	VPN Network Access		Radius-NAS-Port-Type EQUALS Virtual	Default Network Access	0		
	<input type="checkbox"/>		Default policy set			Default Network Access	0		

- Enabled
- Disabled
- Monitor

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

### Authorization Policy

#### Exceptions (0)

#### Standard

```
Employee_MDM if (MDM:DeviceCompliantStatus EQUALS Compliant AND MDM:DeviceRegisterStatus EQUALS Registered AND AD1:ExternalGroups EQUALS cts.local/Users/employees-contractors AND EndPoints:LogicalProfile EQUALS Android Devices) then Employee
```

- 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!

## Authorization Policy

Exceptions (0)

Standard

Example #1: Employee

1. Endpoint ID Group
2. Authenticated using AD?
3. Auth method/protocol
4. AD Group Lookup

Example #2: Employee\_CWA

1. Location (Network Device Group)
2. Web Authenticated?
3. Authenticated via LDAP Store?
4. LDAP Attribute Comparison

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Employee	<code>RegisteredDevices AND (Network Access:AuthenticationIdentityStore EQUALS AD1 AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND AD1:ExternalGroups EQUALS cts.local/Users/employees)</code>	Employee
<input checked="" type="checkbox"/>	Employee_CWA	<code>if (DEVICE:Location EQUALS All Locations#North_America#San_Jose AND Network Access:UseCase EQUALS Guest Flow AND Network Access:AuthenticationIdentityStore EQUALS AD_LDAP AND Radius:Calling-Station-ID EQUALS AD_LDAP:msNPSavedCallingStationID)</code>	Employee

# Auth Policy

## ISE 2.3 Example

The screenshot displays the Cisco ISE 2.3 Policy Set configuration interface. The top navigation bar includes tabs for Policy Sets, Profiling, Posture, Client Provisioning, Policy Elements, Policy, Administration, and Work Centers. The main content area is divided into sections for Authentication and Authorization.

**Authentication Policy (1):** Shows a policy set named "Wired" with a status of "On". The condition is "NAS-Port-Type EQUALS Ethernet".

**Authorization Policy (2):** Shows a policy set named "Employee" with a status of "On". The conditions are:

- AND
  - OR
    - AD1-ExternalGroups EQUALS cts.local/Users/employees
    - AD1-ExternalGroups EQUALS cts.local/Users/employees-contractors
  - AD1-msNPAAllowDialin EQUALS true
- AND
  - OR
    - MDM-DeviceRegisterStatus EQUALS Registered
    - CERTIFICATE-Subject - Organization Unit CONTAINS MyOrganization
    - IdentityGroup Name EQUALS Endpoint Identity Groups.RegisteredDevices
    - MyCorpSQL-Asset Type EQUALS Corporate
  - AND
    - OR
      - Network Access:EapAuthentication EQUALS EAP-TLS
      - EndPoints EndPointPolicy STARTS\_WITH Windows7
      - EndPoints EndPointPolicy STARTS\_WITH Windows10
    - DEVICE-Location EQUALS All Locations#US#SanJose

The right side of the interface shows the "Results" section with "Profiles" (PermitAccess), "Security Groups" (Employees), and "Hits" (0).

# Auth Policy

## ISE 2.3 Example

Policy Set Condition

AND

OR

AD1-ExternalGroups EQUALS cts.local/Users/employees

AD1-ExternalGroups EQUALS cts.local/Users/employees-contractors

AD1-msNPAllowDialin EQUALS true

MDM-DeviceRegisterStatus EQUALS Registered

CERTIFICATE-Subject - Organization Unit CONTAINS MyOrganization

IdentityGroup-Name EQUALS Endpoint Identity Groups:RegisteredDevices

MyCorpSQL-Asset Type EQUALS Corporate

Network Access-EapAuthentication EQUALS EAP-TLS

AND

OR

EndPoints-EndPointPolicy STARTS\_WITH Windows7

EndPoints-EndPointPolicy STARTS\_WITH Windows10

DEVICE-Location EQUALS All Locations#US#SanJose

Employees 4228

- 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	#L
India	#B
Mobile	e D
Printer	rs
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



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

#### Simple Conditions

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

SSID1

SSID2

Mobile\_Devices

Printer\_Devices

Workstation\_Devices

Anomalous\_Behavior

# First Things First – Build Common Conditions

Save with User-Friendly, Intuitive Names

The screenshot displays the 'Conditions Studio' interface, which is divided into two main sections: a 'Library' on the left and an 'Editor' on the right.

**Library:** This section contains a search bar labeled 'Search by Name' and a toolbar with various icons. Below the toolbar is a list of conditions. The 'San Jose' condition is highlighted, and a tooltip labeled 'Location' is visible above it. A hand cursor is pointing at the 'San Jose' entry in the list. Other conditions in the list include 'San Jose OR New York', 'Non\_Compliant\_Devices', 'Switch\_Log... Authentication', 'Switch\_Web\_A... ation', 'Wired\_802.1X', 'Wired\_MAB', 'Wireless\_802.1X', and 'Wireless\_Access'.

**Editor:** This section shows the configuration for the selected 'San Jose OR New York' condition. It features a title bar with the condition name, a 'Set to 'Is not'' button, and 'Duplicate' and 'Edit' buttons. Below the title bar is a large dashed box containing a '+ New AND OR' button, indicating the logical structure of the condition. At the bottom right of the editor, there are 'Close' and 'Use' buttons.

# 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

- Authorization Policy Conditions

- 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**

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Dynamic Match Rule	if Radius:Calling-Station-ID MATCHES LDAP1 Department then	Permit Access

- Authorization Profile Conditions

▼ **Advanced Attributes Settings**

Radius:Class = InternalEndpoint groupPolicy

# Dynamic Variable Substitution - Example

## Define Custom User Attributes

▼ **User Custom Attributes**

Attribute Name	Description	Data Type	Parameters	Default Value	Mandatory
User_IP	Static IP address assignment	IP	192.168.200.0		<input type="checkbox"/>
User_VLAN	Per-User VLAN assignment	Int	Min value : 100, Max value : 200	100	<input checked="" type="checkbox"/>
User_Start_Date	Hire Date	Date		2017-01-01	<input type="checkbox"/>
Is_User_Temp_Employee	Temporary Employee Tracker	Boolean		FALSE	<input type="checkbox"/>
User_dACL	Per-User ACL assignment	String	String Max length	20	<input checked="" type="checkbox"/>

# Dynamic Variable Substitution - Example

## Populate Internal or External User Account

External User:  
AD / LDAP / SQL / OTP

Network Access Users List > New Network Access User

**Network Access User**

\* Name:

Status:  Enabled

Email:

**Internal User:  
Update via Import  
or ERS API**

**Passwords**

Password Type:

**Account Disable Policy**

Disable account if date exceeds  (yyyy-mm-dd)

**User Custom Attributes**

User_IP	=	<input type="text" value="192.168.200.185"/>	(IPv4 or IPv6 Address)
* User_VLAN	=	<input type="text" value="100"/>	
User_Start_Date	=	<input type="text" value="2017-01-01"/>	(yyyy-MM-dd)
Is_User_Temp_Employee	=	<input type="text" value="FALSE"/>	
* User_dACL	=	<input type="text" value="Employee-ACL"/>	

**User Groups**

**employee1 Properties**

Dial-in	Environment	Sessions	Remote control			
Remote Desktop	Services Profile	Personal Virtual Desktop	COM+			
General	Address	Account	Profile	Telephones	Organization	Member Of

Street:

P.O. Box:

City:

State/province:

**Zip/Postal Code:**

Country/region:

OK Cancel Apply Help

# 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

Authorization Profiles > **New Authorization Profile**

### Authorization Profile

\* Name: Employee\_Access  
Description: Policy for Employee Access  
\* Access Type: ACCESS\_ACCEPT

Network Device Profile: CiscoWired

Service Template:   
Track Movement:   
Passive Identity Tracking:

▼ **Common Tasks**

DACL Name: InternalUser:User\_dACL  
 DACL Name: LDAP1:postalCode

**InternalUser**

- EnableFlag
- Firstname
- IdentityGroup
- Is\_User\_Temp\_Employee
- Lastname
- Name
- User\_dACL**
- User\_IP
- User\_Start\_Date
- User\_VLAN
- UserType

BRKSEC-3697

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:

**Common Tasks**

- DACL Name
- VLAN

Dynamic attributes not currently supported under Common Tasks, so must use Advanced Attr. Settings

**Advanced Attributes Settings**

Attribute	Value	Tag ID	Action
Radius:Tunnel-Private-Group-ID	AD1:postalCode	1	Edit Tag
Radius:Tunnel-Type	VLAN	1	Edit Tag
Radius:Tunnel-Medium-Type	802	1	Edit Tag

**Attributes Details**

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:AD1:postalCode
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

Actual value will be based on lookup in AD1 for authenticated user ID.

# Dynamic Authorization for Security Group Tags

## Segmentation Policy Based on Per-User/Device Attributes

The image shows two overlapping windows from a Cisco configuration interface. The left window is titled "Authorization Profile" and the right window is titled "employee1 Properties".

**Authorization Profile Configuration:**

- Name: DynamicSGT
- Description: Retrieve segmentation value from user account in external ID store
- Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Advanced Attributes Settings: Cisco:cisco-av-pair (selected), AD1:description (selected)
- Attributes Details: Access Type = ACCESS\_ACCEPT, cisco-av-pair = AD1:description

**employee1 Properties Configuration:**

- First name: (empty)
- Last name: (empty)
- Display name: employee1
- Description: cts:security-group-tag=0002-0
- Office: url-redirect=http://ad.cts.local

**Annotations:**

- A blue callout box points to the "Advanced Attributes Settings" section, stating: "SGT value will be retrieved and replaced with variable name".
- A yellow callout box points to the "Description" field in the "employee1 Properties" window, stating: "Attribute in local or external ID store set to SGT value".
- A red box highlights the "AD1:description" dropdown in the "Advanced Attributes Settings" section.
- A black box at the bottom contains the mapping: `cisco-av-pair = cts:security-group-tag=0002-0`.

# 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

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

RADIUS Threat-Centric NAC Live Logs > TACACS > Troubleshoot > Adaptive Network Control Reports

Live Logs Live Sessions

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...
Apr 30, 2017 03:07:58.668 PM	✓	Auth Pass			78:9F:70:7B:80:02	OS_X_EI_C...
Apr 30, 2017 03:07:55.009 PM	✓				E0:D1:73:E0:2C:EF	Cisco-IP-Ph...

Actions

- Show Session Trace...

Actions

Show Session Trace...

Session Trace Test Cases > New

### Session Trace Test Case

Test Setup Run Test Previous Runs

Name \*

Description

Predefined Test

Predefined test Select type (optional)

Custom Attributes

RADIUS.Calling-Station-ID=78-9f-70-7b-80-02  
Radius.UserName=sathishr  
Radius.Service-Type=Framed  
Radius.NAS-IP-Address=10.127.16.84  
Radius.NAS-Port-Type=Wireless - IEEE 802.11  
Network Access.NetworkDeviceName=sbgise-bgl13-00a-wlc1  
Network Access.Protocol=RADIUS  
Radius.NAS-Port=1  
Radius.Framed-MTU=1300

Summary of all attributes

RADIUS.Calling-Station-ID=78-9f-70-7b-80-02  
Radius.UserName=sathishr  
Radius.Service-Type=Framed  
Radius.NAS-IP-Address=10.127.16.84  
Radius.NAS-Port-Type=Wireless - IEEE 802.11  
Network Access.NetworkDeviceName=sbgise-bgl13-00a-wlc1  
Network Access.Protocol=RADIUS  
Radius.NAS-Port=1  
Radius.Framed-MTU=1300  
Radius.State=37CPMSessionID=0a7f105400003d4e59066039;41SessionID=sbg-bgla-pdp01/281240336/258896;  
Radius.Acct-Session-Id=59066039/78:9f:70:7b:80:02/15696  
Radius.Tunnel-Private-Group-ID=(taq=0) 133

Cancel Submit

# Build Test Policy

## Option 2: Start from Scratch (Fully Custom Policy)

**1. Build (Setup)**  
**2. Run**  
**3. View/Compare**

Select type (optional)

- Basic Authenticated Access
- Profiled Cisco Phones
- Compliant Devices Access
- Wi-Fi Guest (Redirect)
- Wi-Fi Guest (Access)

**Dictionaries**

- airspaces
- Alcatel-Lucent
- Alpha\_LDAP
- Aruba
- Brocade
- CERTIFICATE
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- CiscoAD
- CWA
- DEVICE
- EndPoints

Operations > Troubleshoot > Diagnostic Tools > Session Trace Tests

Cancel Submit

# Session Trace

## Run Test

- User Groups & Attributes

External User Attribute/Group Viewer

User:

Identity Store:

- AD1
- LDAP1
- AD1**
- MySQL

**Show groups/attributes**

Groups | Attributes

Name
cts.local/Users/employees
cts.local/Users/employees-contrac
cts.local/Users/Domain Users

**Close**

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

Session Trace Test Cases > New

### Session Trace Test Case

Test Setup | **Run Test** | Previous Runs

Test Name:

ISE Node:

**Run**

**Run Results show matching rules and objects**

**PSN to run test**

Policy Stage	Matching Rule	Result Object(s)
Policy Set		Default
Authentication Policy (Allowed Protocols)	Default	Default Network Access
Authentication Policy (Identity Selection)	Default	All_User_ID_Stores
Exception Authorization Policy		
Authorization policy		DenyAccess

Results assume typical conditions, rather than irregular situations that may cause access failures ⓘ

**User Groups & Attributes** ⓘ

# Session Trace

View and Compare  
Previous Test Runs

Select the previous runs to view and/or compare

Session Trace Test Cases > SessionTraceExample

### Session Trace Test Case

Test Setup Run Test **Previous Runs**

2 Selected

View/Compare Trash

<input checked="" type="checkbox"/>	Time	Authentication Policy...	Allowed Protocol	Authorization Profile
<input checked="" type="checkbox"/>	10/6/16 4:32 PM	Default	Default Network Access	DenyAccess
<input checked="" type="checkbox"/>	10/6/16 4:33 PM	Default	Default Network Access	PermitAccess

Test A

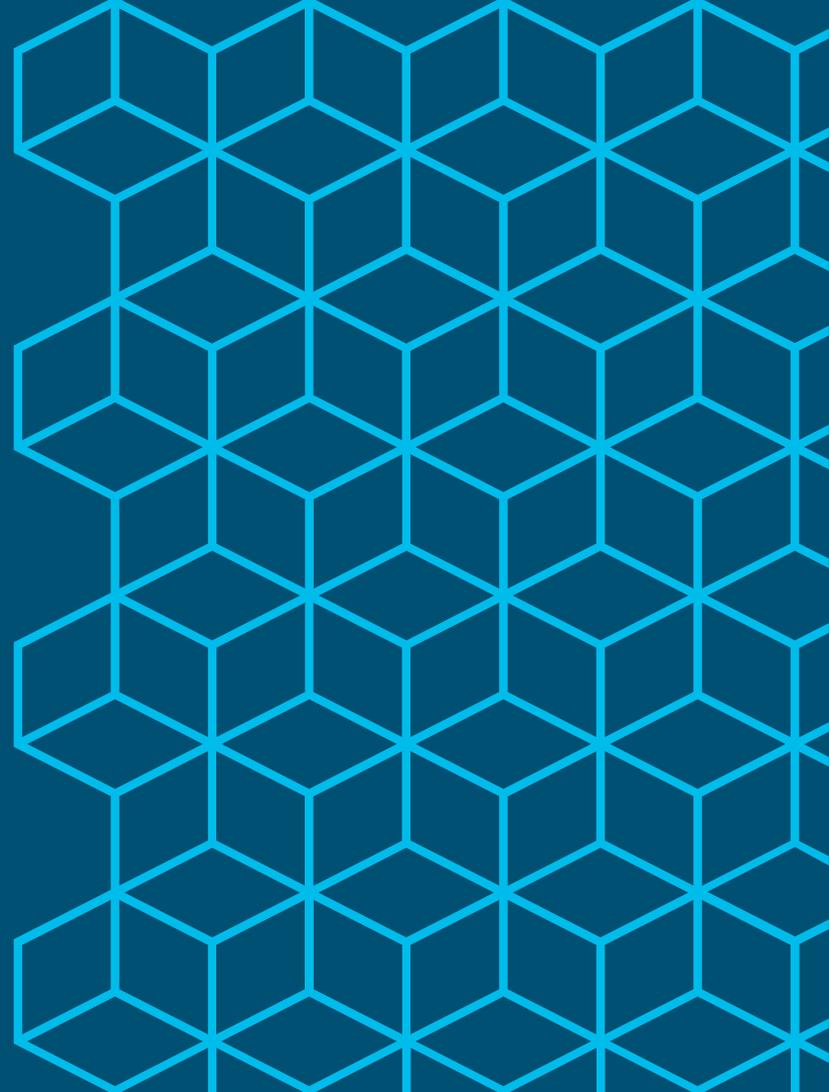
Test B

Time	10/6/16 4:32 PM	10/6/16 4:33 PM
ISE Node	dev-na-ambaer1.cisco.com	dev-na-ambaer1.cisco.com
Policy set name	Default	Default
Authentication rule	Default	Default
Authorization profile	DenyAccess	PermitAccess

Configured attributes :

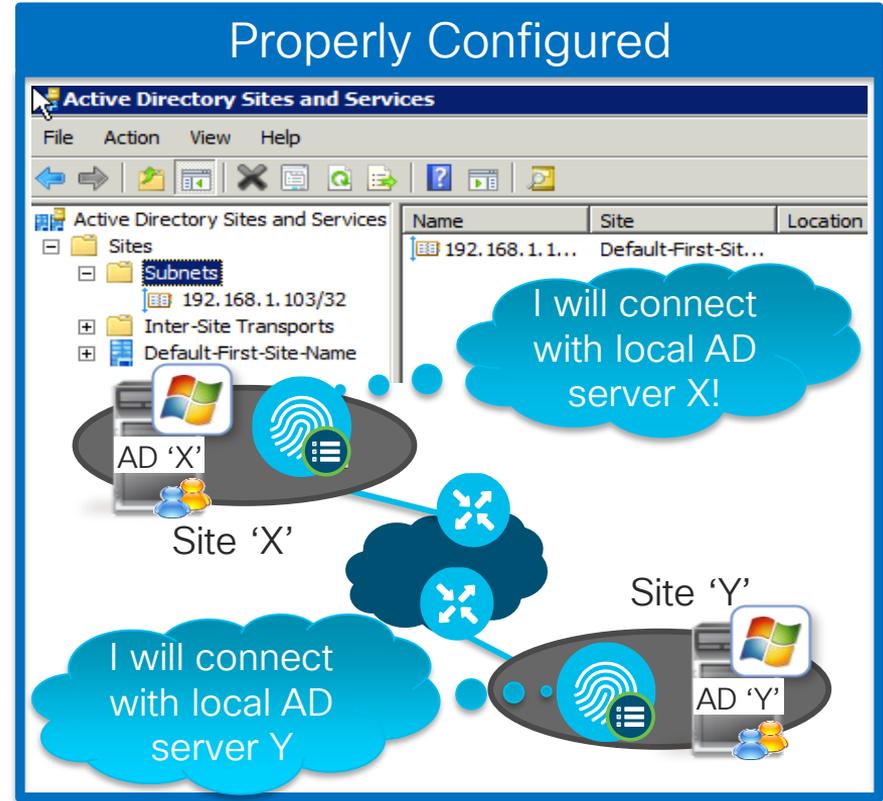
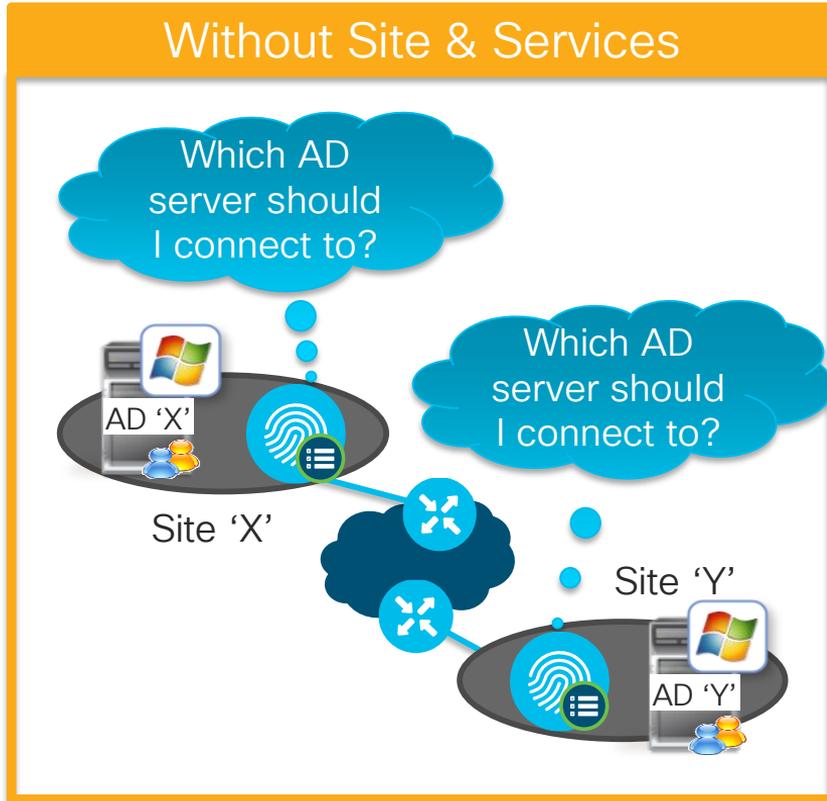
Attribute Name	Value	Value
Radius.User-Name	badUser	goodUser

# Tuning AD Integration

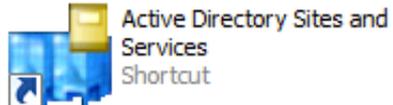


# Scaling AD Integration w/Sites & Services

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



# AD Sites and Services



Links AD Domain Controllers to ISE Servers Based on IP Address

The screenshot shows the Active Directory Sites and Services console. On the left, the tree view shows 'Sites' > 'Subnets' with a list of subnets. An orange box highlights the 'Default-First-Site-Name' site under 'Sites'. On the right, the 'Subnets' table lists 7 objects. An orange box highlights the two subnets under 'Default-First-Site-Name': 10.1.100.0/24 (DC1 Server Farm) and 10.1.101.0/24 (DC2 Server Farm). A blue callout box points to these subnets.

Name	Site	Location	Type	Description
10.1.10.0/24	Ohio		Subnet	Head Quarters
10.1.100.0/24	Default-First-Site-Name		Subnet	DC1 Server Farm
10.1.101.0/24	Default-First-Site-Name		Subnet	DC2 Server Farm
10.2.0.0/16	London		Subnet	EMEA Cluster
10.3.0.0/16	Singapore		Subnet	AsiaPac Cluster
10.4.0.0/16	NewYork		Subnet	US-East
10.5.0.0/16	SanJose		Subnet	US-West

DNS and DC Locator Service work together to return list of “closest” Domain Controllers based on client Site (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

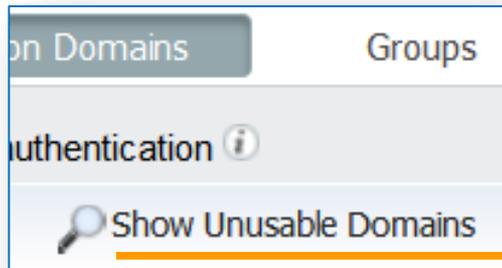
Enable r1.dom

And disable the rest

<input type="checkbox"/>	Name	Authenticate	Forest	SID
<input type="checkbox"/>	c1.r1.dom	NO	R1.dom	S-1-5-21-744
<input type="checkbox"/>	c2.c1.r1.dom	NO	R1.dom	S-1-5-21-4196
<input type="checkbox"/>	c3.r2.dom	NO	R2.dom	S-1-5-21-3477
<input type="checkbox"/>	c4.r3.dom	NO	R3.dom	S-1-5-21-7439
<input type="checkbox"/>	c5.c4.r3.dom	NO	R3.dom	S-1-5-21-6790
<input type="checkbox"/>	c6.c5.c4.r3.dom	NO	R3.dom	S-1-5-21-1704
<input checked="" type="checkbox"/>	r1.dom	YES	R1.dom	S-1-5-21-1320
<input type="checkbox"/>	r2.dom	NO	R2.dom	S-1-5-21-9716
<input type="checkbox"/>	r3.dom	NO	R3.dom	S-1-5-21-1148

# 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



**Unusable Domains** ✕

Listed below are domains that have been identified by ISE, but may not be used for authentication. For details, refer to the "Reason for Exclusion" column.

Name ▲	Reason for Exclusion	Forest	SID
r6.dom	Domain trust is one-way	R6.dom	S-1-5-21-853624879-3382812

# Run the AD Diagnostic Tool

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

<input type="checkbox"/>	Test Name	Join Point	Status	Result and Remedy
<input type="checkbox"/>	DNS A record high level API query <i>i</i>	cisco.com	✓ Successful	Address record found
<input type="checkbox"/>	DNS A record low level API query <i>i</i>	cisco.com	✓ Successful	Address record found
<input type="checkbox"/>	DNS SRV record query <i>i</i>	cisco.com	✗ Failed	Response contains no answer. Check DNS configuration.
<input type="checkbox"/>	DNS SRV record size <i>i</i>	cisco.com	✗ Failed	Response contains no answer. Check DNS configuration.
<input type="checkbox"/>	Kerberos check SASL connectivity to AD <i>i</i>	cisco.com	✓ Successful	SASL connectivity test to AD was successful
<input type="checkbox"/>	Kerberos test bind and query to ROOT DSE ...	cisco.com	✓ Successful	ROOT_DSE was successfully reached
<input type="checkbox"/>	Kerberos test obtaining join point TGT <i>i</i>	cisco.com	✓ Successful	TGT was obtained successfully
<input type="checkbox"/>	LDAP test - DC locator <i>i</i>	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

Active Directory > Active Directory Diagnostic Tool

### Active Directory Diagnostic Tool

These tests check proper Active Directory configuration and operation of the Active Directory Service for use with ISE.

ISE node:

Join Point:

Run scheduled tests ⓘ

Start At:  Hrs.

Repeat every:

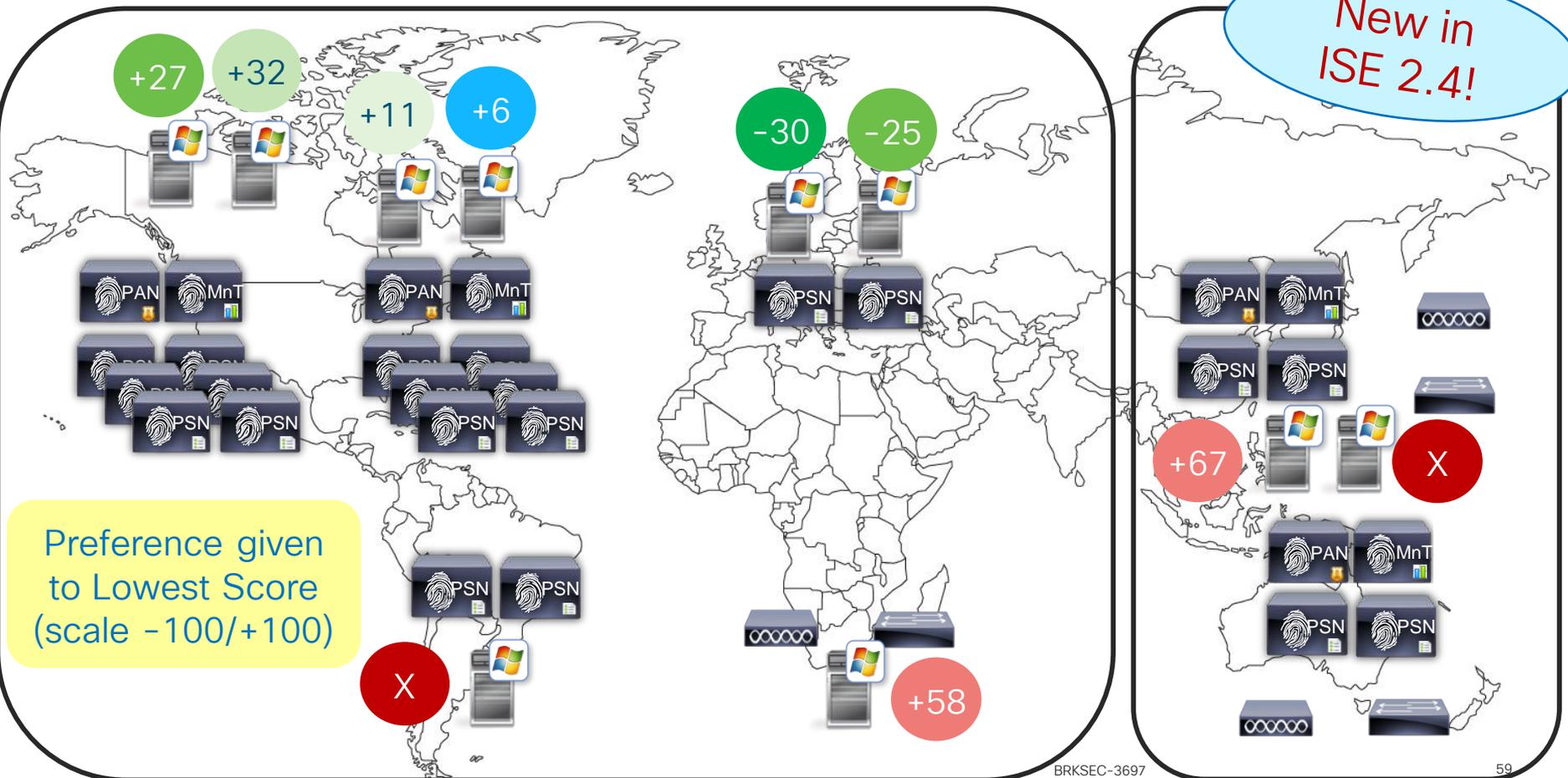
**Summary:**  Successful

Finish running tests (7:54:05 AM).

<input type="checkbox"/>	Test Name	Join Point	Status	Result and Remedy
<input type="checkbox"/>	System health - check AD service ⓘ	System	<input checked="" type="checkbox"/> Successful	AD service is running
<input type="checkbox"/>	System health - check DNS configuration ⓘ	System	<input checked="" type="checkbox"/> Successful	DNS configuration & status test was successful
<input type="checkbox"/>	System health - check NTP ⓘ	System	<input checked="" type="checkbox"/> Successful	NTP configuration & status test was successful

# 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 user 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:

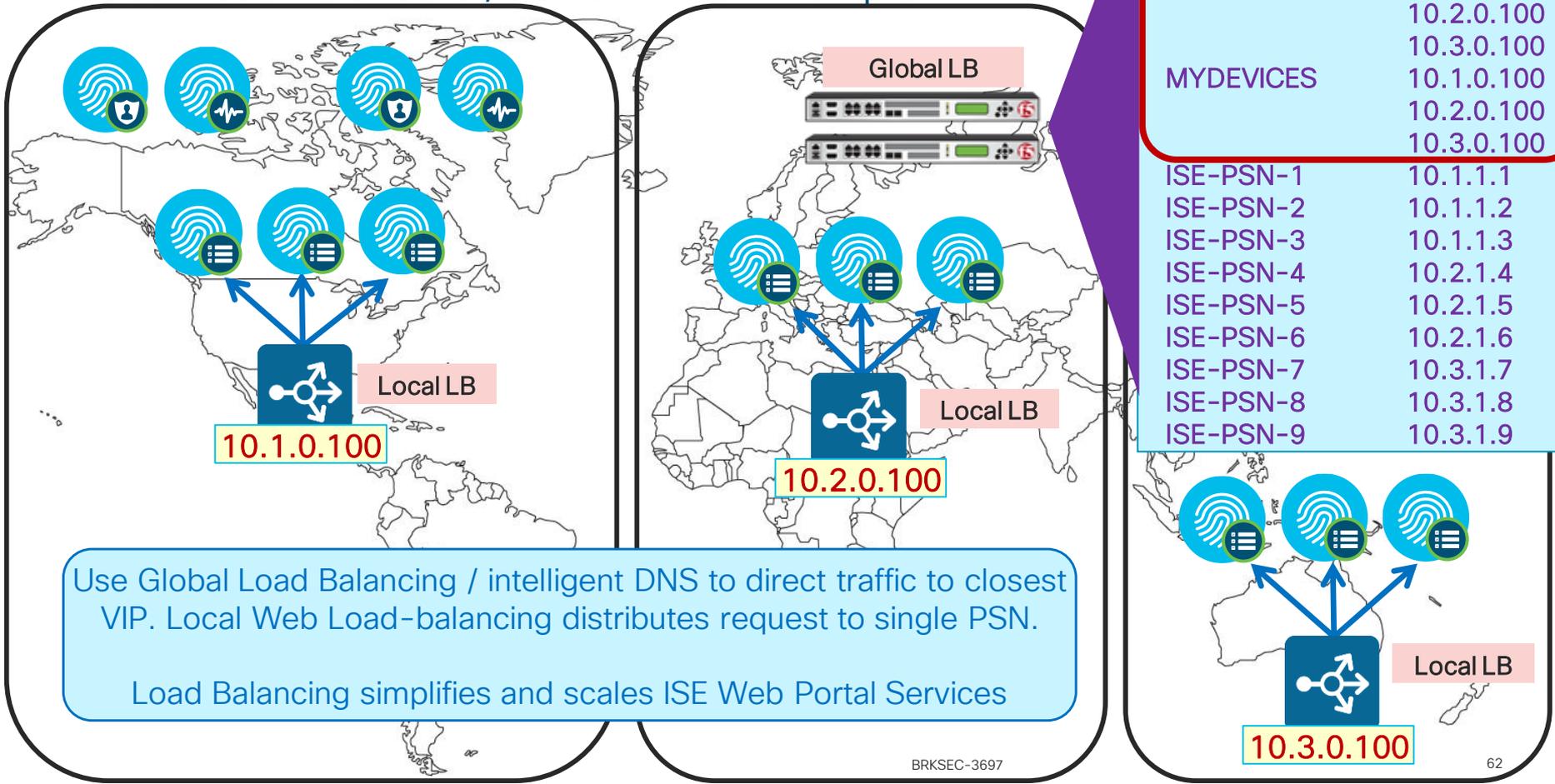
<http://msdn.microsoft.com/en-us/library/ms675095%28v=vs.85%29.aspx>

<http://technet.microsoft.com/en-gb/library/aa995762%28v=exchg.65%29.aspx>

# Guest and Web Authentication Services

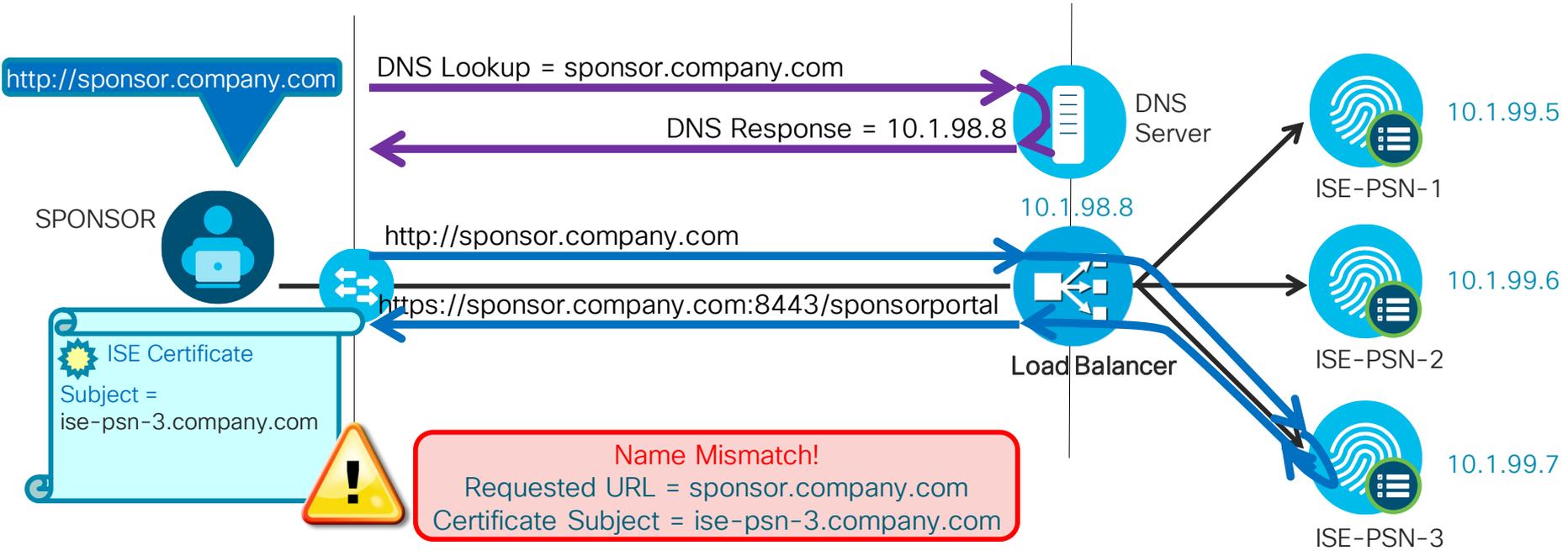
# Single URL for Sponsors/MyDevices

## Global Load Balancers / "Smart DNS" Example



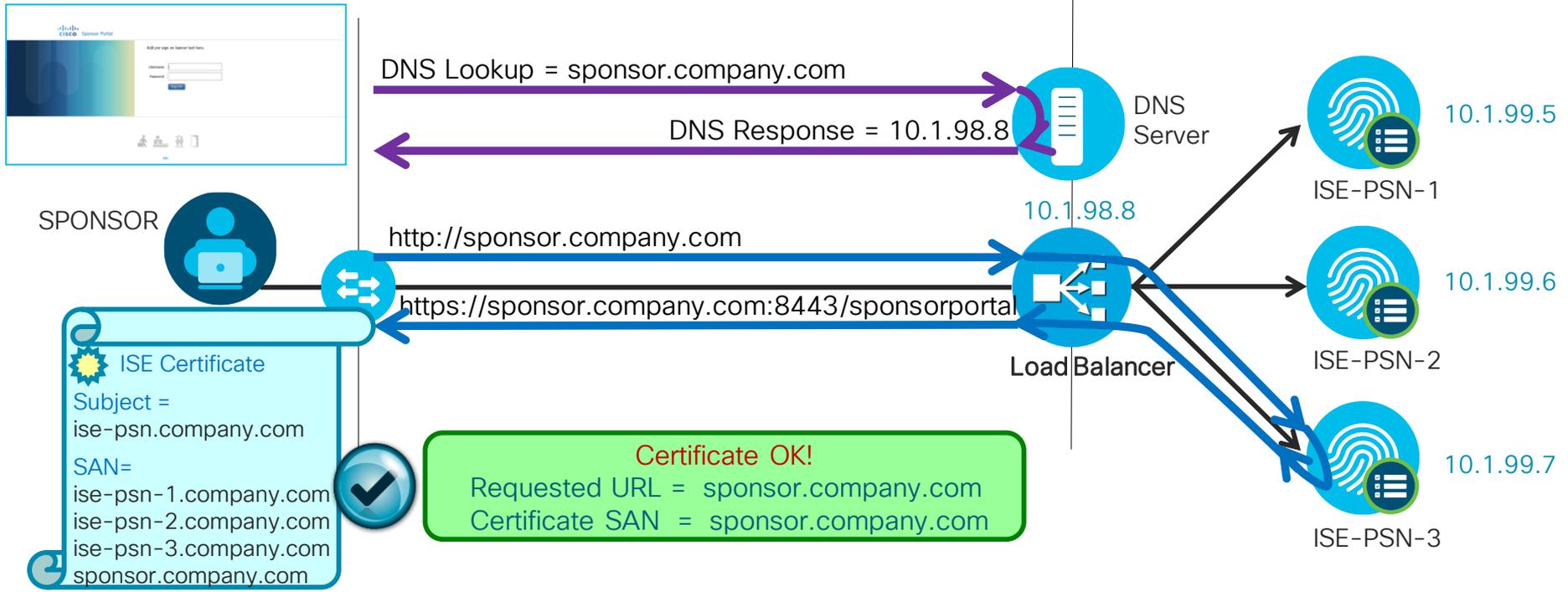
# ISE Certificate without SAN

## Certificate Warning - Name Mismatch



# ISE Certificate with SAN

## No Certificate Warning



# “Universal Certs”

## UCC or Wildcard SAN Certificates

Subject Alternative Name (SAN)   - +

- +

Check box to use wildcards

Allow Wildcard Certificates  ⓘ

### Node(s)

Generate CSR's for these Nodes:

Node  ise-psn  
CSR Friendly Name ise-psn/Admin

### Subject

Common Name (CN)  ⓘ

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN)   - +

- +

- +

- +

CN must also exist in SAN

Universal Cert options:

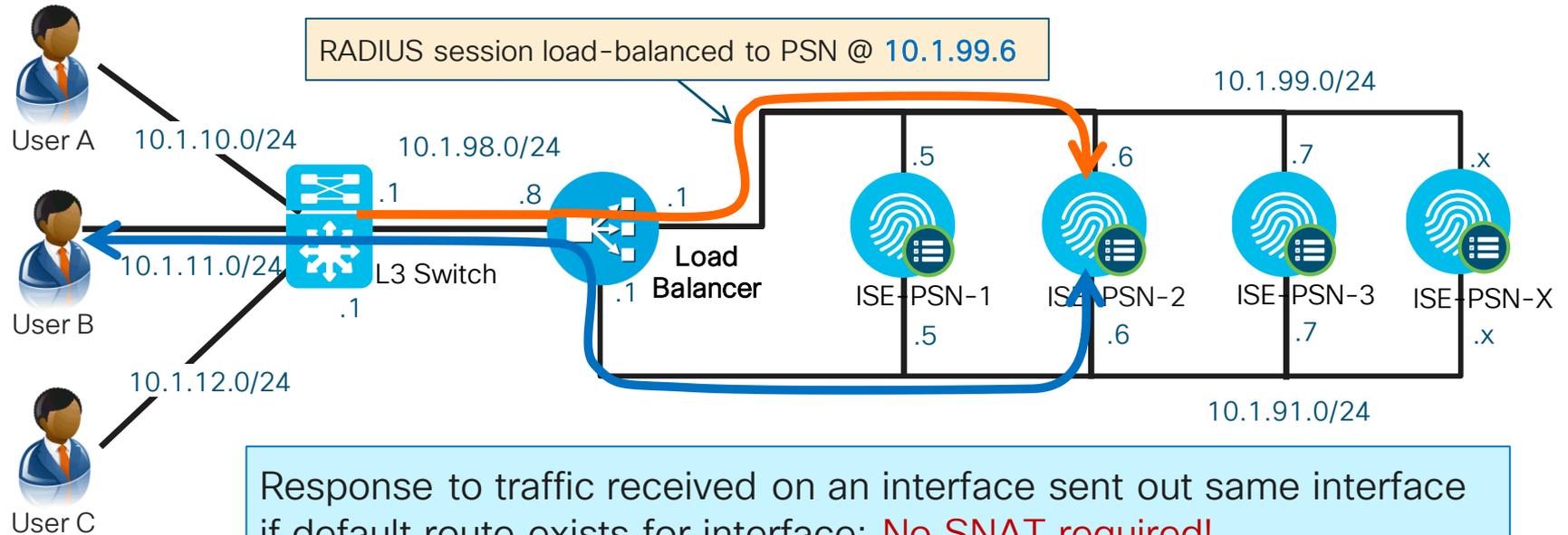
- UCC / Multi-SAN
- Wildcard SAN

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



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
<b>default</b>	<b>10.1.91.1</b>	<b>eth1</b>
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.

The screenshot shows the 'Portal Settings' configuration page in Cisco ISE. The 'HTTPS port' is set to 8443. Under 'Allowed interfaces', 'Gigabit Ethernet 1' is selected. The 'Certificate group tag' is set to 'Public Portal Certificate Group'. The 'Authentication method' is 'Guest\_Portal\_Sequence'. Three callout boxes provide additional context: an orange box points to the 'Allowed interfaces' list with the text 'Redirection based on first service-enabled interface; if eth0, return host FQDN; else return interface IP.'; a blue box points to the 'Certificate group tag' dropdown with the text 'Certs assigned to this group signed by 3rd-party CA'; and a light green box points to the 'Allowed interfaces' list with the text 'Redirection based on first service-enabled interface; if eth0, return host FQDN; else return interface IP.'

**Portal Settings**

HTTPS port: \*  (8000 - 8999)

Allowed interfaces: \*

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3

Certificate group tag: \*

Configure certificates at:  
[Administration > System > Certificates > System](#)

Authentication method: \*  ⓘ

Configure authentication methods at:  
[Administration > Identity Management > Identity Source Sequences](#)  
[Administration > External Identity Sources > SAML Identity Providers](#)

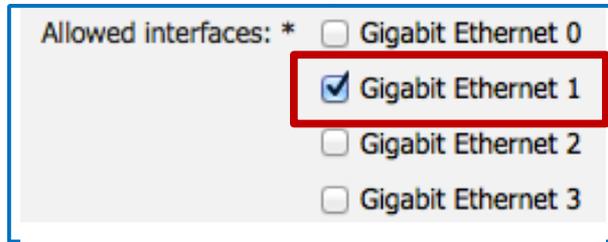
Redirection based on first service-enabled interface; if eth0, return host FQDN; else return interface IP.

Certs assigned to this group signed by 3rd-party 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



Allowed interfaces: \*

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3

- 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

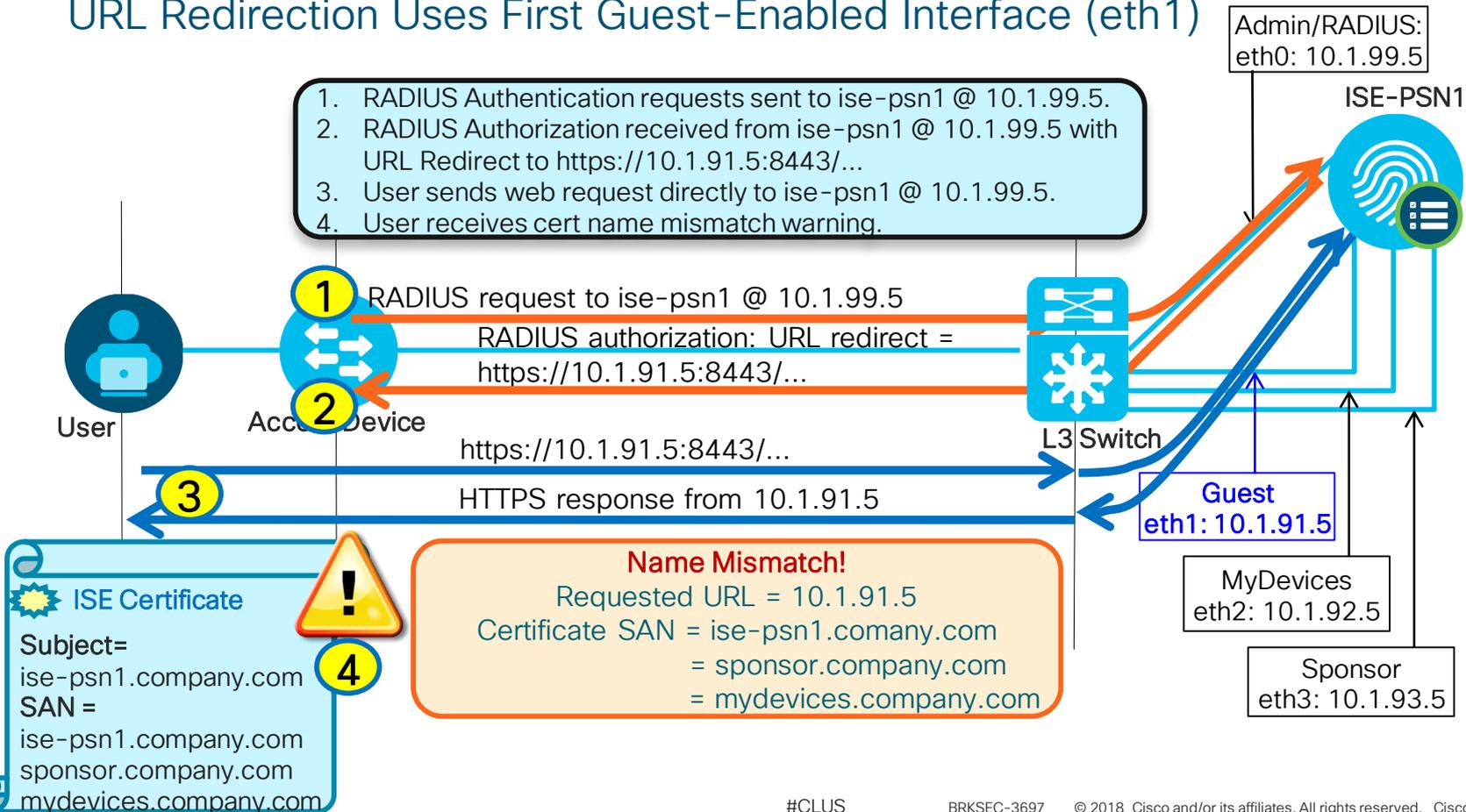
```
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=Se
```

- 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

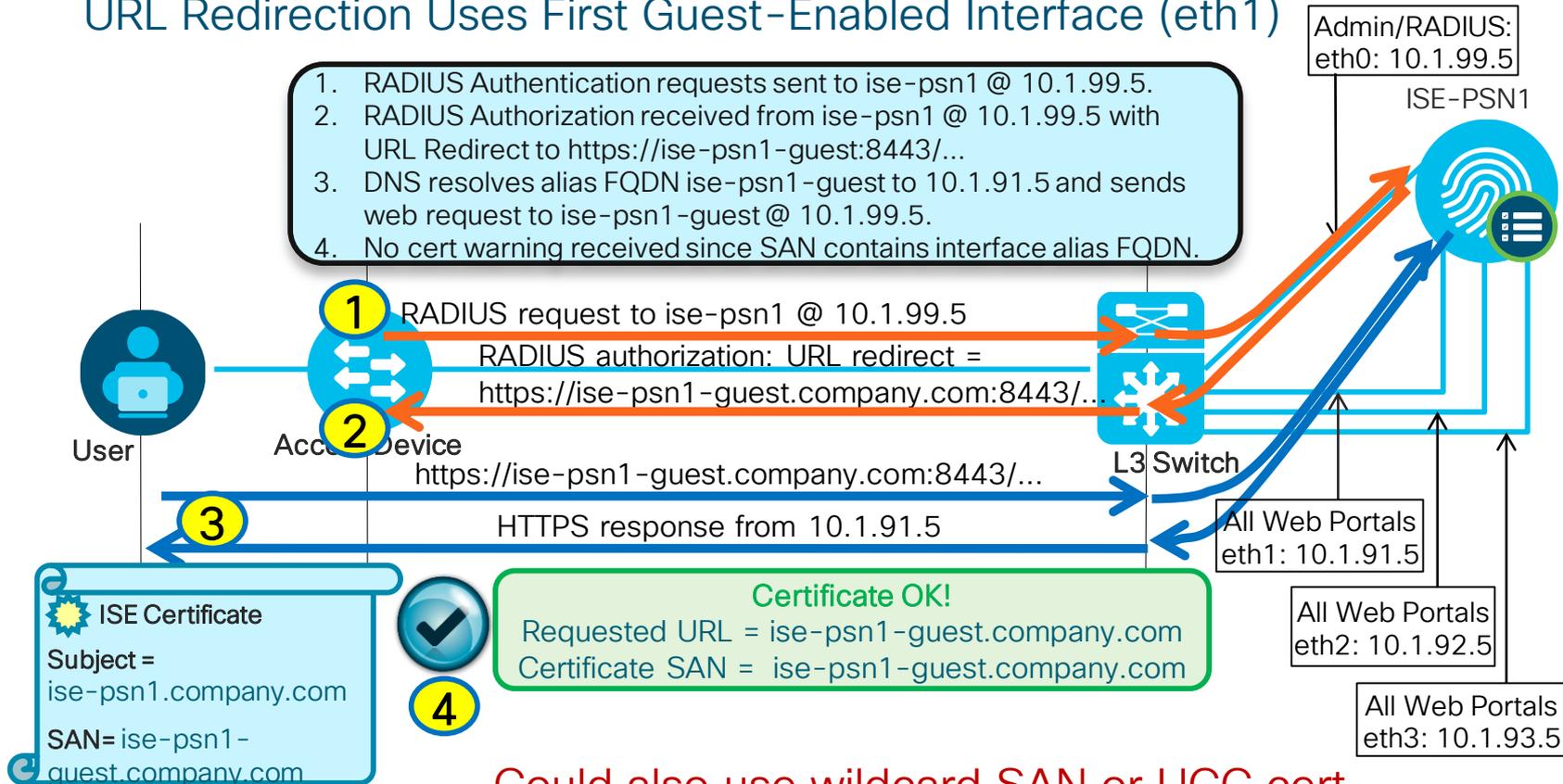
DNS SERVER				
DOMAIN = COMPANY.COM				
ISE-PSN1-GUEST	IN	A	10.1.91.5	# eth1
ISE-PSN2-GUEST	IN	A	10.1.91.6	# eth1
ISE-PSN3-GUEST	IN	A	10.1.91.7	# eth1

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)

1. RADIUS Authentication requests sent to ise-psn1 @ 10.1.99.5.
2. RADIUS Authorization received from ise-psn1 @ 10.1.99.5 with URL Redirect to https://ise-psn1-guest:8443/...
3. DNS resolves alias FQDN ise-psn1-guest to 10.1.91.5 and sends web request to ise-psn1-guest@ 10.1.99.5.
4. No cert warning received since SAN contains interface alias FQDN.

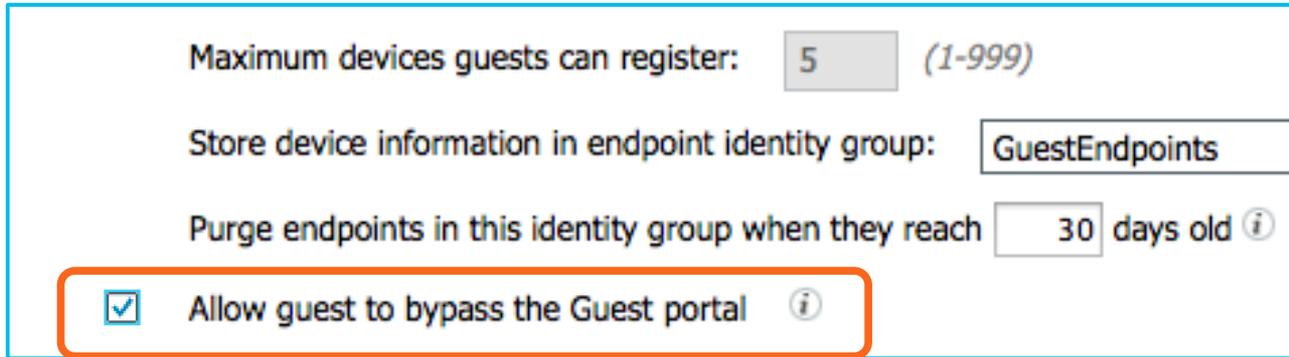


Could also use wildcard SAN or UCC cert

# Using Guest Accounts with VPN and 802.1X

“Activated Guest” allows guest 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



A screenshot of the ISE configuration interface for guest accounts. The interface includes several fields and a checkbox. The 'Maximum devices guests can register' field is set to 5, with a range of (1-999). The 'Store device information in endpoint identity group' field is set to GuestEndpoints. The 'Purge endpoints in this identity group when they reach' field is set to 30 days old. The 'Allow guest to bypass the Guest portal' checkbox is checked and highlighted with an orange border.

Maximum devices guests can register: 5 (1-999)

Store device information in endpoint identity group: GuestEndpoints

Purge endpoints in this identity group when they reach 30 days old ⓘ

Allow guest to bypass the Guest portal ⓘ

**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: \*

Purge endpoints in this identity group when they reach  days

*Configure endpoint purge at*  
[Administration > Identity Management > Settings > Endpoint purge](#)

### 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

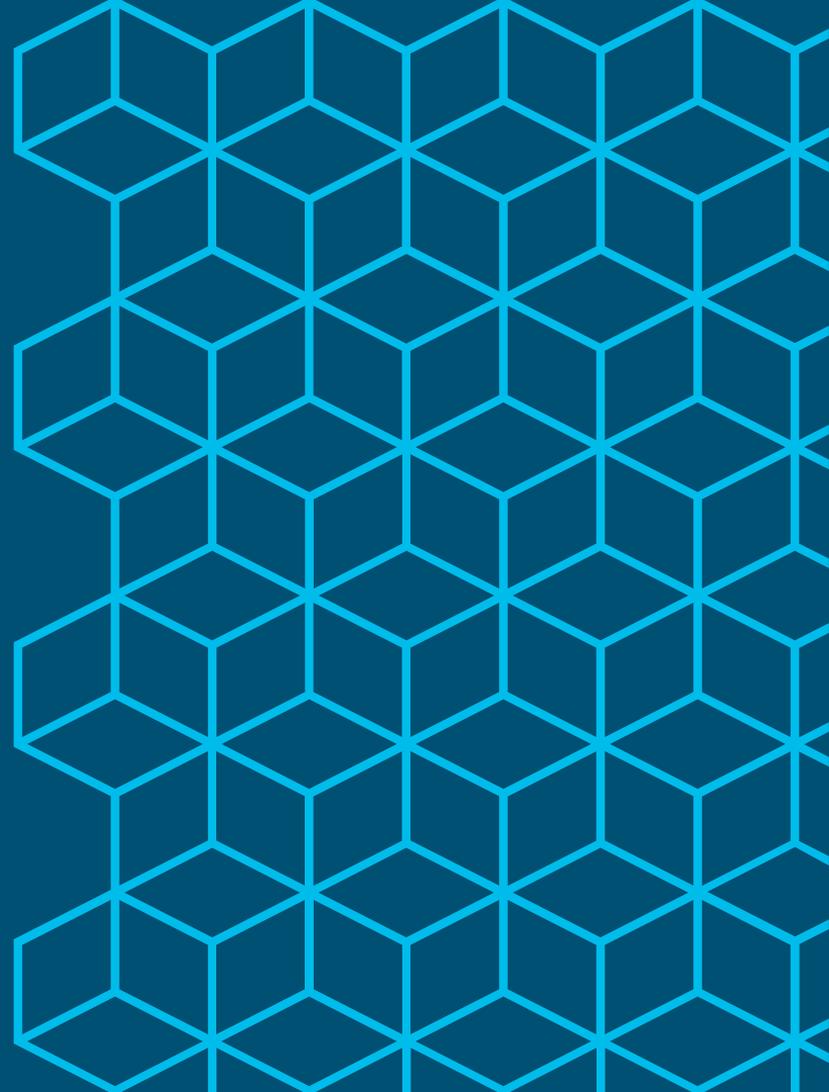
Reset

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.

New in ISE 2.3; configurable in ISE 2.4

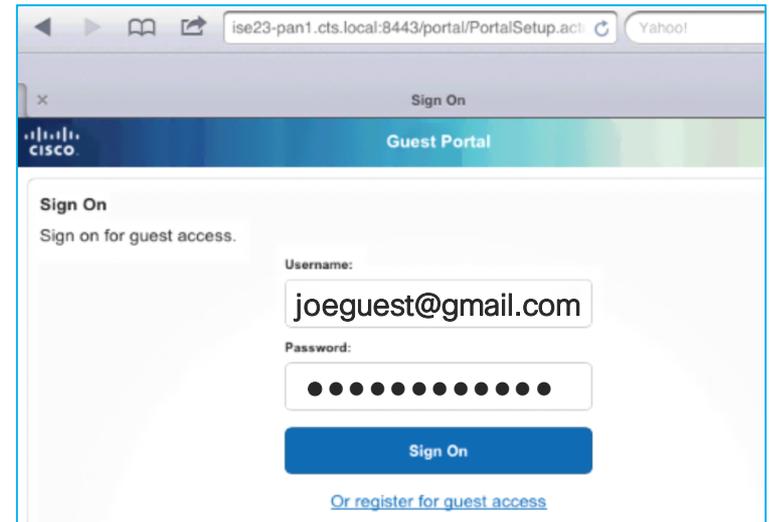
# Pre-Shared Key (PSK) and Identity PSK (IPSK)



# 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

WLANs > Edit 'guest-cwa'

General Security QoS Policy-Mapping

Layer 2 Layer 3 AAA Servers

Layer 2 Security [6](#) WPA+WPA2  
MAC Filtering [9](#)

Fast Transition  
Fast Transition Disable

Protected Management Frame  
PMF Disabled

WPA+WPA2 Parameters

WPA Policy   
WPA2 Policy   
WPA2 Encryption  AES  TKIP  CCMP   
OSEN Policy

Authentication Key Management [19](#)

802.1X  Enable  
CCKM  Enable  
PSK  Enable  
FT 802.1X  Enable  
FT PSK  Enable  
PSK Format ASCII   
•••••

WLANs > Edit 'guest-cwa'

General Security QoS Policy-Mapping Advanced

Allow AAA Override  Enabled  
Coverage Hole Detection  Enabled  
Enable Session Timeout  1800  
Session Timeout (secs)  
Aironet IE  Enabled  
Diagnostic Channel [18](#)  Enabled  
Override Interface ACL IPv4 None  IPv6 None   
Layer2 Acl None   
URL ACL None   
P2P Blocking Action Disabled   
Client Exclusion [3](#)  Enabled 60  
Timeout Value (secs)  
Maximum Allowed Clients [8](#) 0  
Static IP Tunneling [11](#)  Enabled  
Wi-Fi Direct Clients Policy Disabled   
Maximum Allowed Clients Per AP Radio 200  
Clear HotSpot Configuration  Enabled

DHCP  
DHCP Server  Over  
DHCP Addr. Assignment  Requ

OEAP  
Split Tunnel  Enabl

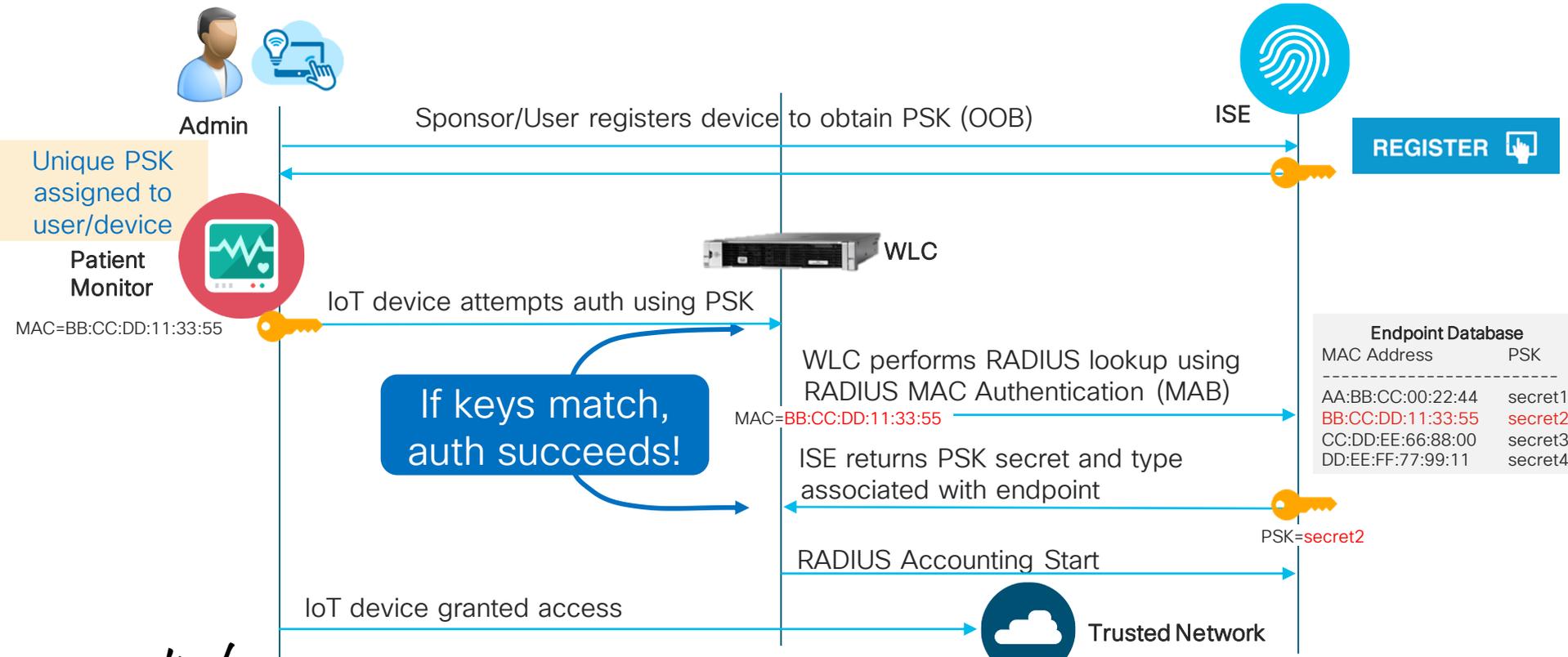
Management Frame Protection (MFP)  
MFP Client Protection [4](#)  Optional  
DTIM Period (in beacon intervals)  
802.11a/n (1 - 255) 1  
802.11b/g/n (1 - 255) 1

NAC  
NAC State ISE NAC

# 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

## Advanced Attributes Settings

psk-mode can be ASCII or HEX

2 Cisco:cisco-av-pair = psk-mode=ASCII

Cisco:cisco-av-pair = EndPoints:PreSharedKey

## Attributes Details

Access Type = ACCESS\_ACCEPT

cisco-av-pair = psk-mode=ASCII

cisco-av-pair = EndPoints:PreSharedKey

cisco-av-pair=psk=CustomPreSharedKey1234

#CL

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



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

Username:

Endpoint Profile: Philips-Device

Current IP Address:

Location:

Applications

Attributes

Authentication

Threats

Vulnerability

## General Attributes

Description Philips Patient Monitor

Static Assignment false

Endpoint Policy Philips-Device

Static Group Assignment false

Identity Group Assignment Profiled

## Custom Attributes

Filter

Attribute Name	Attribute Value
AssignedPort	GigabitEthernet1/0/23
AssetType	Patient Monitor
PreSharedKey	psk=CustomPreSharedKey1234
IsManaged	BRKSEC-3697 True

1

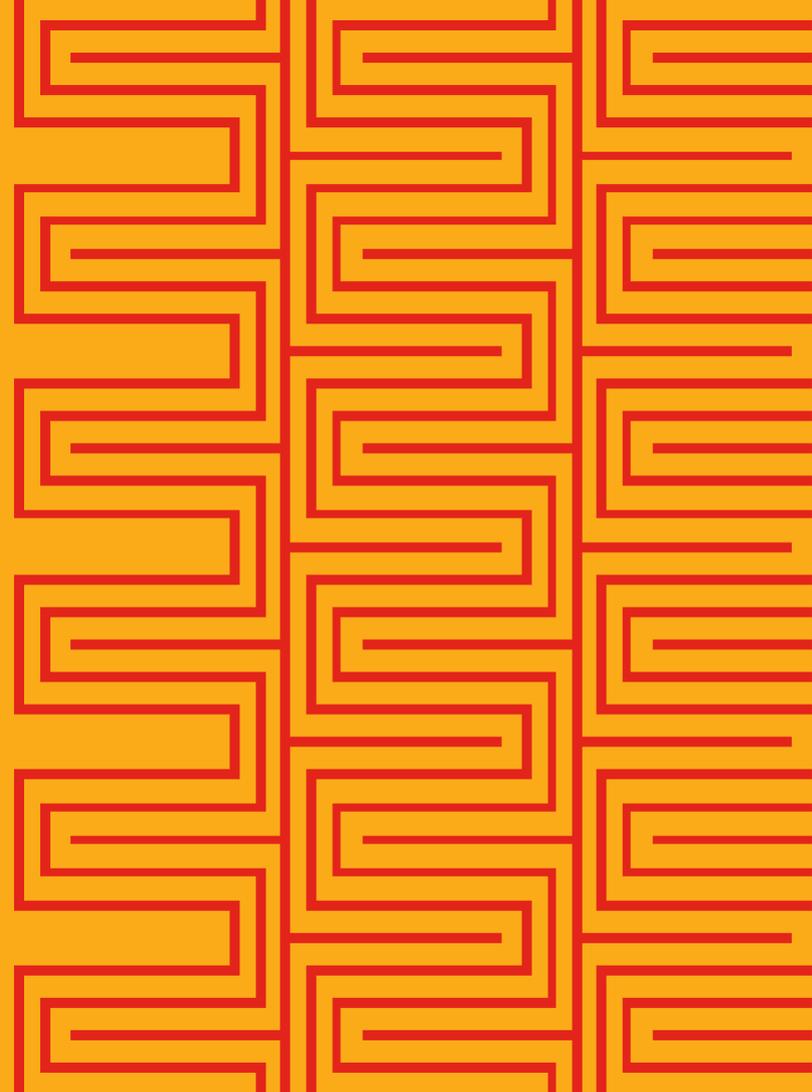
# ERS API to add PSK to endpoint

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>
```

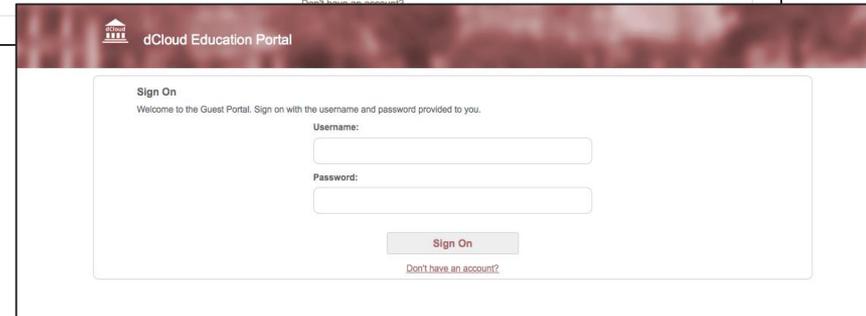
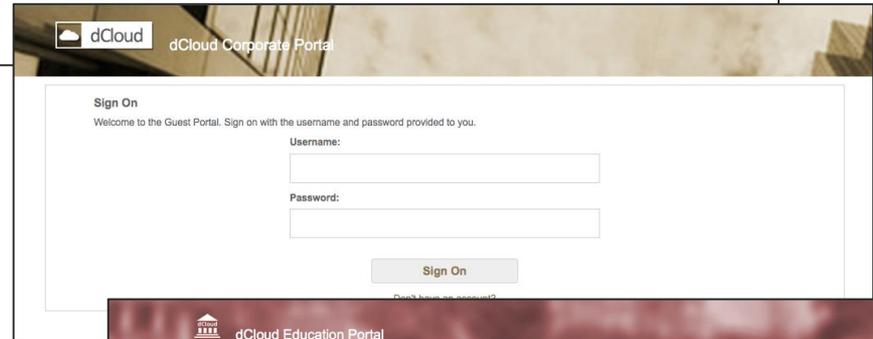
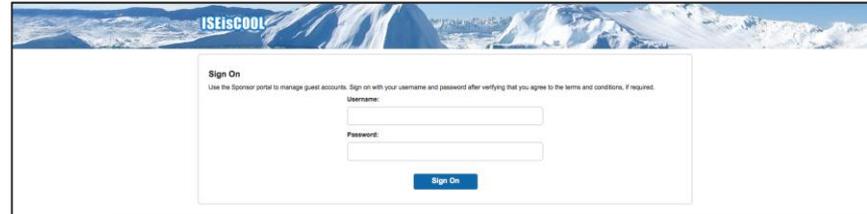
```
<customAttributes>
  <entry>
    <key>AssignedPort</key>
    <value>GigabitEthernet1/0/23</value>
  </entry>
  <entry>
    <key>AssetType</key>
    <value>Patient Monitor</value>
  </entry>
  <entry>
    <key>PreSharedKey</key>
    <value>psk=CustomPreSharedKey1234</value>
  </entry>
  <entry>
 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

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation path is Administration > System > Admin Access > Settings > Portal Customization. The left sidebar shows a navigation menu with categories: Authentication, Authorization, Administrators, Settings, and Portal Customization. The main content area is titled 'Portal Customization' and contains two radio button options: 'Enable Portal Customization with HTML' (unselected) and 'Enable Portal Customization with HTML and JavaScript' (selected). A red circle highlights the selected option. Below the options is a 'Save' button. A blue callout box with a white border and rounded corners contains the text 'Allow JavaScript'.

# ISE Portal Builder (isepb.cisco.com)

Hi! We're happy to introduce a major update of ISE Portal Builder! As a part of this update we completely replaced our Firefox extension with standalone apps for [Mac OS X](#) and [Windows](#). Please use them instead from now on. We also added support for ISE 2.4, improved stability and performance.

Please feel free to contact our support team at [isepb@external.cisco.com](mailto:isepb@external.cisco.com) if you'll have any questions or face any issues! Thank you for using ISE Portal Builder!



My Portals



Template Gallery

## TEMPLATES GALLERY

Select template to create your own Portal

Image Manager

Health Care  
Portals created: 2027

FIRE & ISE  
Portals created: 3835

Template 1  
Portals created: 3897

Template 2  
Portals created: 2450

Template 3  
Portals created: 1983

Template 4  
Portals created: 2841

Corporate  
Portals created: 2707

Education  
Portals created: 1408

Federal  
Portals created: 1375

Default  
Portals created: 5935

# Portal Customization

## Community Tips and Tricks

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



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

### Profiler Configuration

Work Centers > Profiler > Settings

\* CoA Type: Port Bounce

Current custom SNMP community strings: ●●●●●●●●●●

Show



Change custom SNMP community strings:

RO SNMP string for endpoint queries

(For NMAP, comma separated. Field will be cleared on successful saved change.)

Confirm changed custom SNMP community strings:

(For NMAP, comma separated. Field will be cleared on successful saved change.)

EndPoint Attribute Filter:  Enabled ⓘ

Limit data collection and replication to essential attributes

Enable Anomalous Behaviour Detection:  Enabled ⓘ

Enable Anomalous Behaviour Enforcement:  Enabled

Enable Custom Attribute for Profiling Enforcement:  Enabled

Only enable if require profiles based on custom attributes

# 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.

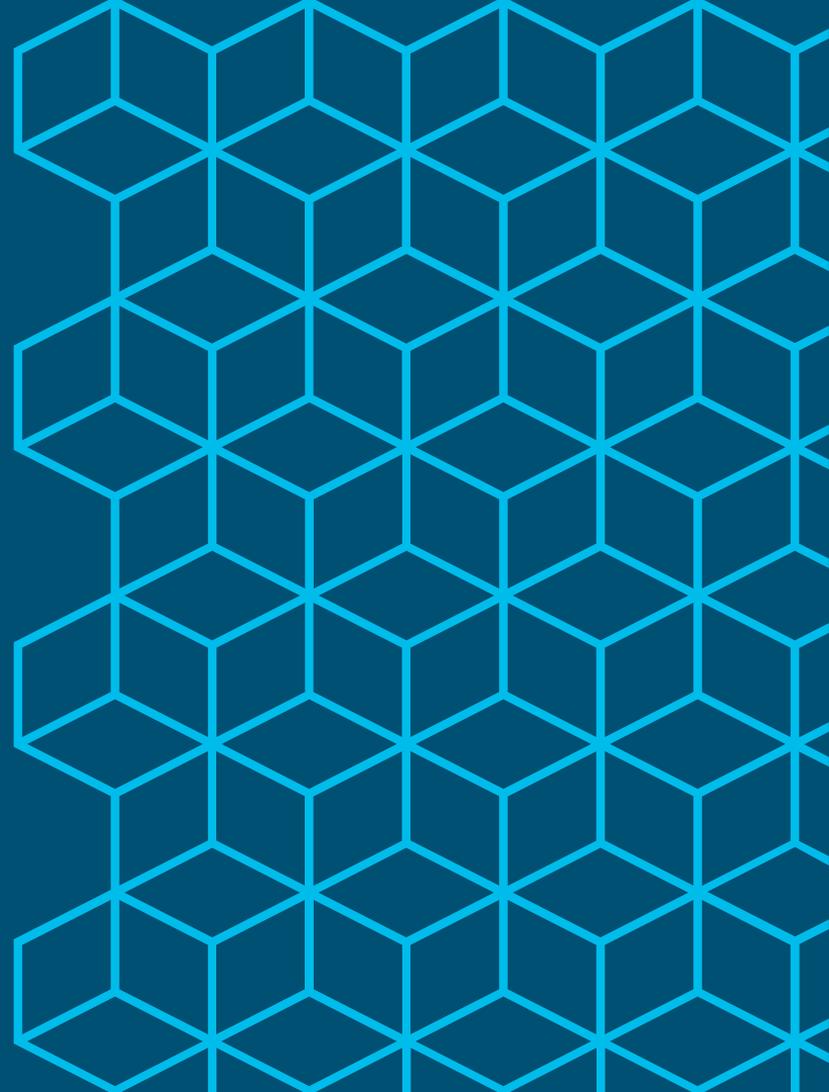
**Edit Node**

General Settings **Profiling Configuration**

- ▶ NETFLOW
- ▶ DHCP
- ▶ DHCPSPAN
- ▶ HTTP
- ▶ RADIUS
- ▶ Network Scan (NMAP)
- ▶ DNS
- ▶ SNMPQUERY
- ▶ SNMPTRAP
- ▶ Active Directory
- ▶ pxGrid

Save Reset

“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



A screenshot of the Cisco Identity Services Engine (ISE) Profiler Feed Service Configuration page. The page is titled "Profiler Feed Service Configuration" and shows two main update options: "Online Subscription Update" and "Offline Manual Update". Both options are highlighted with red boxes. A blue box labeled "Online: Automatic/On-Demand" points to the "Online Subscription Update" option, and another blue box labeled "Offline: On-Demand" points to the "Offline Manual Update" option. The "Online Subscription Update" section is expanded, showing a checkbox for "Enable Online Subscription Update" which is checked. Below this, there is a field for "Automatically check for updates every day at" with a dropdown menu set to "01" and "16" for "mm UTC". There is an "Update Now" button. Below that is a "Test Feed Service Connection" button and a "Test result:" field. The "Notify administrator when download occurs" section is also expanded, showing a checkbox checked and a text field for "Administrator email address" containing "admin@cts.local". The "Provide Cisco anonymous information to help improve profiling accuracy" section is also expanded, showing a checkbox checked and a section for "Include Administrator Information (optional)" with fields for "First name" (John), "Last name" (Smith), "Email address" (admin@cts.local), and "Phone" ((408) 555-1111). The page header shows the navigation menu with "Home", "Context Visibility", "Operations", "Policy", "Administration", "System", "Identity Management", "Network Resources", "Device Portal Management", "pxGrid Services", and "Feed Service".

# 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



**Feed Service Management**

Home Manage Content Offline Feed

Download Package E-mail Preferences

### Offline Update E-mail Notification Preferences

*Configure your preferences below for receiving emails about profile and OUI updates.*

Enable notifications (includes p

Send notification of new updates every  days

E-mail Addresses (Comma(,) separated list of email addresses.)

Save Reset

Mon 5/7/2018 10:18 PM  
feed-admin@cisco.com  
Email from CISCO: Notification of CISCO ISE Device Profile Updates

To Craig Hyps (chyps)

You've requested to be notified of updates to the CISCO Identity Services Engine (ISE) Device Profile and OUI data every 30 day(s).The following updates have been made since your last email update on 2018-04-07 18:15:25.0

Device Profiles: 8 updates.

Name:	Audio Code IP Phones
Version:	1
Description:	Profiles for Audio Code IP Phones
Approval Date:	2018-05-02 13:56:50.0

Name:	Cisco AP Profiles
Version:	1
Description:	Cisco AP 1700,1800,2800,3800
Approval Date:	2018-05-02 13:56:50.0

Name:	Lexmark Printers
Version:	1
Description:	Hierarchy Update for Lexmark Printer Profiles

=====  
OUI Updates: 204 updates.

The latest OUI version is 8082 and was updated on 2018-05-07 17:11:24.0

You can update your ISE Deployment with these and all previous changes by downloading a file from the ISE Feed Service and importing it into your deployment.

Steps for Downloading the Update File:

- 1) Access the ISE Feed Service Partner Portal at <https://ise.cisco.com/partner>. Log in with your CCO credentials
- 2) Navigate to the page Offline Feed -> Download Package. Press the "Generate" button, then "Download" and save the file
- 3) From the Administration console on your ISE Primary PAN node, navigate to Workcenter > Profiler > FeedService > Offline Manual Update. Then "Browse" and "Apply Update"

Steps for modifying your notification preferences:

- 1) Access the ISE feed Service Partner Portal at <https://ise.cisco.com/partner>. Log in with your CCO credentials
- 2) Navigate to the page Downloads -> Offline Update -> Email Preferences. Update your preferences and press the Submit button.

Thank you,  
CISCO Systems, Inc.

# 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

The screenshot displays the Cisco Identity Services Engine (ISE) Profiling Policies page. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The page title is "Profiling Policies".

On the left, a sidebar shows a tree view of device categories under "Siemens-Device":

- Siemens-Device
  - Siemens-Automation-Drives-Device
  - Siemens-Building-Device
  - Siemens-Building-Technologies-Device
  - Siemens-Convergence-Device
  - Siemens-Digital-Factory-Device
  - Siemens-Energy-Automation-Device
  - Siemens-Energy-Management-Device
  - Siemens-Home-Office-Device
  - Siemens-Industrial-Automation-Device
  - Siemens-Industrial-Automation-EWA-Device
  - Siemens-Industrial-Device
  - Siemens-Industry-Device
  - Siemens-Low-Voltage-Device
  - Siemens-Numerical-Control-Device
  - Siemens-SIMEA-Device
  - Siemens-Sector-Industry-Device
  - Siemens-Switzerland-BT-HVP-Device
  - Siemens-Transportation-Device

The main content area shows a search filter: "Match the following rule: Filter [Description] Contains [Lighting]. Below this is a table of policies:

Profiling Policy Name	Policy Enabled	System Type	Description
<input type="checkbox"/> Advanced-Illumination-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Adv...
<input type="checkbox"/> Advatek-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Adv...
<input type="checkbox"/> BC-Illumination-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for BC-Il...
<input type="checkbox"/> Beijing-E3Control-Technology-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy...
<input type="checkbox"/> Creative-Lighting-Sound-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Creat...
<input type="checkbox"/> Cree-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Cree...
<input type="checkbox"/> Darfon-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Darfo...
<input type="checkbox"/> Digital-Lighting-Systems-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy...
<input type="checkbox"/> ELC-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting/Entertainment)
<input type="checkbox"/> Electronic-Theatre-Controls-Device	Enabled	Administrator Created	Automation and Control (Home/Lighting/Entertain...
<input type="checkbox"/> GE-Consumer-Industrial-Device	Enabled	Administrator Created	Automation and Control (Building/Power/Lighting)
<input type="checkbox"/> General-Electric-Device	Enabled	Administrator Created	Automation and Control (Manufacturing/Building/F...
<input type="checkbox"/> German-Light-Products-Device	Enabled	Administrator Created	Automation and Control (Lighting/Entertainment)
<input type="checkbox"/> Hills-Sound-Vision-Lighting-Device	Enabled	Administrator Created	Automation and Control (Building/Healthcare-RTLS...
<input type="checkbox"/> Hubbell-Building-Automation-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy...
<input type="checkbox"/> Intelligent-Distributed-Controls-Device	Enabled	Administrator Created	Automation and Control (Manufacturing/Building/L...
<input type="checkbox"/> Invisua-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Invis...
<input type="checkbox"/> LACROIX-Traffic-Device	Enabled	Administrator Created	Automation and Control (Lighting/Traffic-Transpor...
<input type="checkbox"/> LED-Roadway-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting/Traffic-Transpor...
<input type="checkbox"/> LNT-Automation-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy...
<input type="checkbox"/> Laser-Light-Engines-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Laser...
<input type="checkbox"/> Leedarsen-Lighting-Device	Enabled	Administrator Created	Automation and Control (Building/Home/Lighting)
<input type="checkbox"/> Lihtino-Science-Group-Device	Enabled	Administrator Created	Automation and Control (Lihtino/Healthcare-Aaricul...

On the right, a dropdown menu is open, showing filter options:

- Lighting
- Quick Filter
- Advanced Filter
- All
- Manage Preset Filters
- Automation and Control
- Manufacturing
- Building Automation
- Home Automation
- Elevator
- Transportation
- Financial Automation
- HVAC
- Security Access Control
- Camera - A/V
- Power
- Defense
- Lighting

# 300+ Medical Device Profiles

- Philips-Device
  - Philips-Analytical-X-Ray-Device
  - Philips-CareServant-Device
  - Philips-Electronics-Netherlands-Device
  - Philips-Healthcare-PCCI-Device
  - Philips-Intellivue
  - Philips-Medical-Systems-Device
    - Marconi-Medical-Systems-Device
    - Philips-Medical-Systems-Cardiac-Monitoring-Device
  - Philips-Oral-Healthcare-Device
  - Philips-Patient-Monitoring-Device
    - Philips-SureSigns-Patient-Monitor
      - Philips-SureSigns-VS3-Patient-Monitor
      - Philips-SureSigns-VS4-Patient-Monitor
  - Philips-Personal-Health-Device
  - Philips-Respironics-Device

Profiling Policies

Selected 0 | Total 315

Edit Add Duplicate Delete Import Export

Show Quick Filter

Profiling Policy Name	Policy Enabled	System Type	Description
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>

CiscoLive!

The screenshot shows the Cisco Communities website interface. At the top, there's a navigation bar with the Cisco logo and the word 'Communities'. Below that, there are tabs for 'Products & Services', 'Partners', 'Global', 'Developer', and 'Cisco Customer Connection'. The main content area is titled 'ISE Endpoint Profiles' and lists several profile libraries created by 'chyps'. The page is highlighted with an orange border.

Profile Name	Created	Author
Polycom Profiler Pack v1.0	3 weeks ago in Identity Services Engine (ISE)	by chyps
Amazon Alexa profile policy	3 weeks ago in Identity Services Engine (ISE)	by chyps
Google Home profile policy	3 weeks ago in Identity Services Engine (ISE)	by chyps
Cisco ISE Automation and Control Profile Library v1.0	1 month ago in Identity Services Engine (ISE)	by chyps
Cisco ISE Medical NAC Profile Library v2.0	2 months ago in Identity Services Engine (ISE)	by chyps
Cisco ISE Industrial Network Director (IND) IoT Profile Library v1.0	2 months ago in Identity Services Engine (ISE)	by chyps
Cisco ISE Windows Workstation Embedded-IoT Profile Library v1.0	2 months ago in Identity Services Engine (ISE)	by chyps

# 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

Profiling

Logical Profiles List > Workstations

**Logical Profile**

\* Name: Workstations Description: All Profiles matching a desktop or workstation endpoint

\* Policy Assignment

Available Policies:

- Windows10-Workstation
- Windows7-Workstation
- Windows8-Workstation
- WindowsXP-Workstation
- Winpresa-Building-Automation-Device
- Wintech-Automation-Device
- WL-Gore-Device
- Workstation

Assigned Policies:

Move policies to assigned list

Choose policies here (Shift and CTRL keys to select multiple profiles)

Endpoints in Logical Profile

Endpoint policy	MAC Address	IP Address
-----------------	-------------	------------

Total 14

Endpoints matching Logical Profile

# Logical Profiles

## Authorization Policy Rules

Profiling

Logical Profiles List > **IND Devices**

**Logical Profile**

\* Name:  Description:

\* Policy Assignment

Available Policies:

- 2Wire-Device
- 3Com-Device
- 3M-Company-Device
- 3M-Deutschland-Device
- 3M-Device
- 3M-Germany-Device

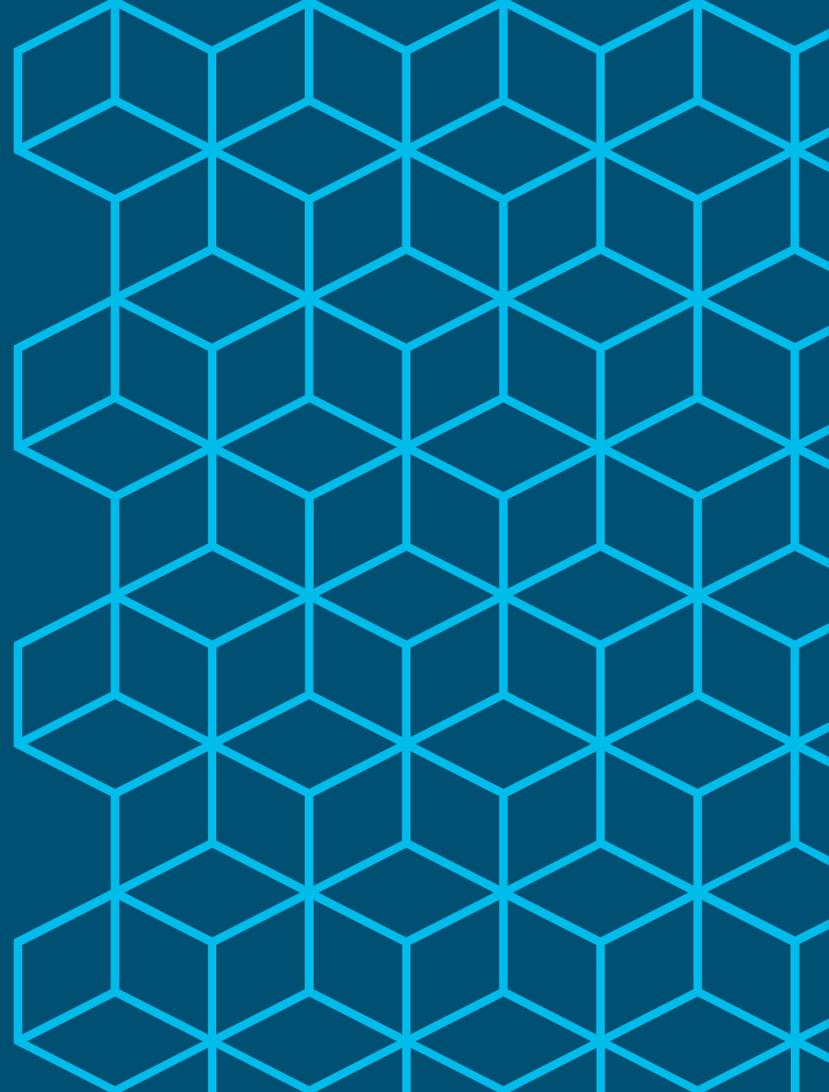
Assigned Policies:

- BACnet-Device
- CIP-Device
- Industrial-Drive
- Industrial-EtherNetNode
- Industrial-HMI
- Industrial-IO

Authorization Policy (14)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
✔	Wireless Black List Default	AND <ul style="list-style-type: none"><li>Wireless_Access</li><li>IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist</li></ul>	* Blackhole_Wireless_Access +	Quarantine x +	51	⚙
✔	Manufacturing	AND <ul style="list-style-type: none"><li>Endpoints:LogicalProfile EQUALS IND Devices</li><li>Endpoints:assetGroup EQUALS Pod5</li></ul>	* PermitAccess +	Manufacturing x +	822	⚙
✔	Profiled Cisco IP Phones	IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	* Cisco_IP_Phones +	Phones x +	21397	⚙
✔	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	* Non_Cisco_IP_Phones +	Phones x +	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)

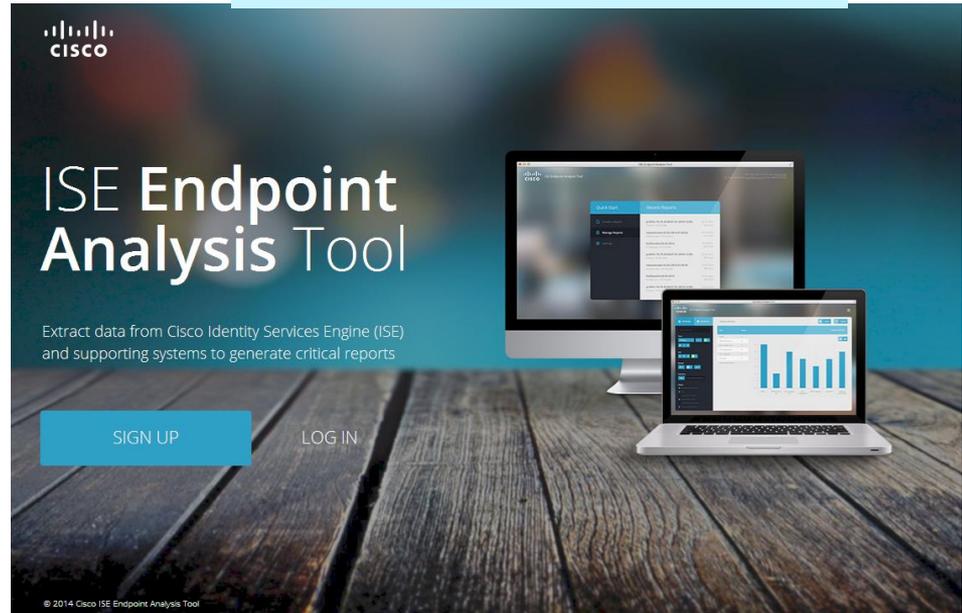
MACAddress	ip	FQDN	host-name	IdentityGroup	MatchedPolicy	OUI	dhcp-class-identifier	dhcp-user-class-id	dhcp-parameter-request-list	User-Agent
70:70:0D:72:47:BA			chyps-iPhone7	Profiled	Apple-iPhone	Apple, Inc.			1, 121, 3, 6, 15, 119, 252	
3C:E5:A6:C3:8A:90	10.1.10.100		WA2612-AGN	Unknown	Unknown	Hangzhou 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

The screenshot shows the main dashboard of the ISE Endpoint Analysis Tool. At the top, there is a header with the Cisco logo and the text "ISE Endpoint Analysis Tool". Below the header, there are three main sections: "Reports", "Profiles", and "Data".

- Reports:** Labeled "7 reports", it contains two green buttons: "Create new report" and "Open saved report".
- Profiles:** Contains two blue buttons: "My profiles" and "Public profiles".
- Data:** Contains two grey buttons: "Report types" and "Remove saved data".

The version number "4.0.0" is visible in the bottom right corner of the window.

The screenshot shows the configuration page titled "Configure your ISE access". The page contains several form fields and checkboxes for setting up the tool's connection to the ISE.

- Report name \***: Text input field with value "ise24-endpoints".
- Endpoints per Request**: Dropdown menu with value "500".
- Saved ISE configuration \***: Dropdown menu with value "New Ise Configuration".
- ISE Name \***: Text input field with value "ise24-pan1".
- ISE IP address \***: Text input field with value "10.1.100.3".
- ISE MnT IP address**: Text input field with value "10.1.100.4".
- ISE Administrator Username \***: Text input field with value "admin".
- ISE Administrator Password \***: Password input field with value "\*\*\*\*\*".
- Save ISE configuration**: Checked checkbox.
- Identity Source**: Dropdown menu with value "Internal".
- Collect MnT info**: Checked checkbox.
- Add syslog file**: Text input field.
- Browse**: Green button next to the syslog file field.

A large green "Start collecting" button is located at the bottom of the form. The version number "4.0.0" is visible in the bottom right corner of the window.

# EAT - Embedded Filter and Sorting

Alpha 4/11/18, 8:28 PM / 3h 1m 29s

Show 50 entries

Showing 1 to 50 of 103 entries (filtered from 89,513 total entries)

Export as CSV...

Create profile...

OUI Name	DHCP Parameter Request List	IP Address	DHCP Class Identifier	Web Browser User Agent	DHCP Host Name
	1,		i		
SAMSUNG ELECTRO MECHANICS C...	1, 33, 3, 6, 28, 51, 58, 59	10.40.135.142	dhcpd-5.2.10:Linux-3.0.15-...	com.google.android.youtube/3.5.5(Linux); U; Android 4.0.3; en...	
Samsung Electronics Co.,Ltd	1, 33, 3, 6, 15, 28, 51, 58, 59	10.34.94.45	dhcpd-5.2.10:Linux-3.1.10.a...	SAMSUNG-Android	
Samsung Electronics Co.,Ltd	1, 33, 3, 6, 15, 28, 51, 58, 59	10.40.130.11	dhcpd-5.2.10:Linux-3.0.8-9...	SAMSUNG-Android	
LG Electronics (Mobile Communicatio...	1, 3, 6, 15, 26, 28, 51, 58, 59	10.33.216.145	android-dhcp-6.0.1	Onefootball/Android/7.8.0	
HUAWEI TECHNOLOGIES CO.,LTD	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.135.144	android-dhcp-8.1.0	Mozilla/5.0 (X11); Linux x86_64 AppleWebKit/537.36 (KHTML, like...	
LG Electronics (Mobile Communicatio...	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.86.99.12	android-dhcp-7.1.2	Mozilla/5.0 (X11); Linux x86_64 AppleWebKit/537.36 (KHTML, like...	
HTC Corporation	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.135.141	android-dhcp-7.1.1	Mozilla/5.0 (X11); Linux x86_64 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.82 Saf...	android-6fadc908d496e876
HTC Corporation	1, 33, 3, 6, 15, 28, 51, 58, 59	10.33.218.60	dhcpd-5.2.10:Linux-3.0.8-0...	Mozilla/5.0 (Linux); U; Android-Zoolz; en-gb; App...	
Motorola Mobility LLC, a Lenovo Com...	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.135.146	android-dhcp-7.1.1	Mozilla/5.0 (Linux); Android 7.0; XT1650 Build/NCL2...	
OnePlus Tech (Shenzhen) Ltd	1, 3, 6, 15, 26, 28, 51, 58, 59	10.40.130.10	android-dhcp-6.0.1	Mozilla/5.0 (Linux); Android 6.0.1; A0001 Build/MM...	
OnePlus Tech (Shenzhen) Ltd	1, 3, 6, 15, 26, 28, 51, 58, 59	10.40.130.12	android-dhcp-6.0.1	Mozilla/5.0 (Linux); Android 5.1.1; A0001 Build/LMY...	
ARRIS Group, Inc.	1, 33, 3, 6, 15, 28, 51, 58, 59	161.44.104.22	dhcpd-5.2.10:Linux-3.0.8-g...	Mozilla/5.0 (Linux; U; Android 4.0.4; en-us; XOOM 2...	
Samsung Electronics Co.,Ltd	1, 33, 3, 6, 15, 28, 51, 58, 59	161.44.104.26	dhcpd-5.2.10:Linux-3.1.10.a...	Mozilla/5.0 (Linux; U; Android 3.2; en-us; GT-P7510...	
HTC Corporation	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.86.99.19	android-dhcp-7.1.1	Mozilla/5.0 (Linux; Android 7.0; Nexus 9 Build/NRD9...	
UNKNOWN	1, 33, 3, 6, 15, 28, 51, 58, 59, 43	10.40.130.53	android-dhcp-7.0	Mozilla/5.0 (Linux; Android 7.0; F3113 Build/33.3.A...	
zte corporation	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.130.52	android-dhcp-7.1.1	Mozilla/5.0 (Linux; Android 6.0.1; ZTE B2017G Build...	
Motorola (Wuhan) Mobility Technolog...	1, 3, 6, 15, 26, 28, 51, 58, 59	10.40.130.12	android-dhcp-6.0.1	Mozilla/5.0 (Linux; Android 6.0.1; Lenovo K33a42 Bu...	
LG Electronics (Mobile Communicatio...	1, 3, 6, 15, 26, 28, 51, 58, 59	10.86.99.19	android-dhcp-6.0.1	Mozilla/5.0 (Linux; Android 4.4.2; Nexus 5 Build/KOT...	
Samsung Electronics Co.,Ltd	1, 33, 3, 6, 15, 28, 51, 58, 59	161.44.104.11	dhcpd-5.2.10:Linux-3.0.8-1...	Mozilla/5.0 (Linux; Android 4.0.4; GT-P5113 Build/MM...	

Export option to leverage the full power of external tools such as Excel

### Report types

- Profiling
- Network View
- Endpoint Attributes
- Authorization Policy

# 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.)

The screenshot displays the Cisco ISE Endpoint Analysis Tool interface. At the top right, the Cisco logo and the text "ISE Endpoint Analysis Tool" are visible. Below the header, there is a status bar showing "Alpha 4/11/18, 8:28 PM / 3h 1m 29s". To the right of this bar are two buttons: "Export as CSV..." and "Create profile...", the latter of which is highlighted with a red box. Below the status bar, there is a "Show" dropdown set to "250" and a message "Showing 1 to 250 of 17,170 entries (filtered from 89,513 total entries)".

The main content area is a table with columns: OUI Name, DHCP Parameter Request List, IP Address, Endpoint Policy, DHCP Class Identifier, DHCP Host Name, and Dor. The table contains several rows of data, including entries for "Murata Manufacturing ..." and "UNKNOWN".

A "Create profile" dialog box is overlaid on the table. The dialog has a blue header with the title "Create profile" and a close button. It contains two input fields for "Manufacturer" (set to "Samsung") and "Model" (set to "Galaxy-S8"). Below these are three rows of configuration options, each with a label, a dropdown menu set to "Equals", and a text input field:

- DHCP Host Name: Equals, Galaxy-S8
- DHCP Class Identifier: Equals, android-dhcp-7.0
- DHCP Parameter Request List: Equals, 1, 3, 6, 15, 26, 28, 51, 58, 59, 43

A blue "Create Profile" button is located at the bottom of the dialog.

At the bottom of the interface, there is a pagination bar with "Previous", "1", "2", "3", "4", "5", "...", "69", and "Next".

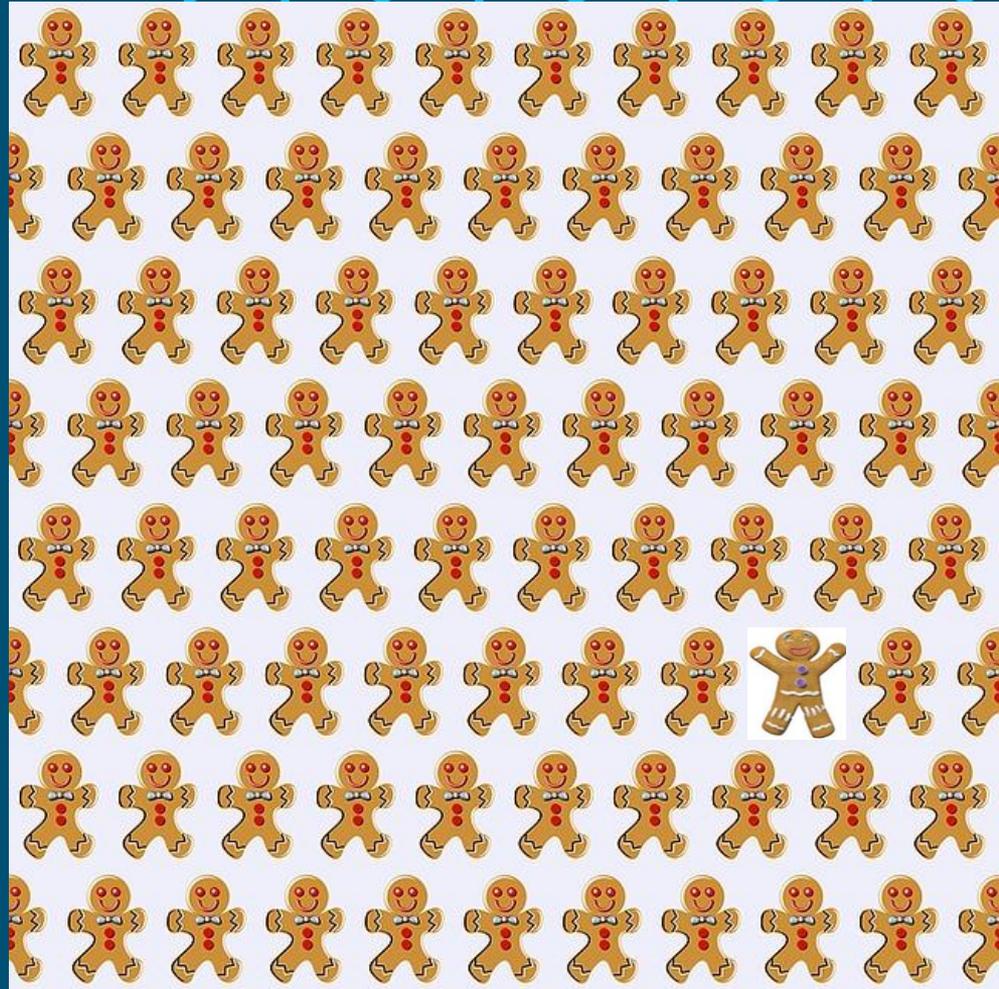
# Sample EAT Report (CSV Export)

MACAddress	OUI	MatchedPolicy	dhcp-class-identifier	dhcp-parameter-request-list	operating-system-result	User-Agent
8C:79:67:95:12:9A	zte corporation	Android	dhcpdcd-5.5.6		Android	Dalvik/2.1.0 (Linux; U; Android 5.1; Z958 Build/LMY470)
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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2404.144 Mobile Safari/537.36
A8:A6:68:D9:BA:A8	zte corporation	Android	dhcpdcd-5.5.6	1, 33, 3, 6, 15, 28, 51, 58, 59		
D0:5B:A8:30:7A:65	zte corporation	Android	dhcpdcd-5.5.6		Android	Dalvik/2.1.0 (Linux; U; Android 5.1; Z958 Build/LMY470)
D8:55:A3:97:AD:26	zte corporation	Android	dhcpdcd-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	dhcpdcd-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:CA	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	dhcpdcd-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	dhcpdcd-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	dhcpdcd-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	dhcpdcd-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	dhcpdcd-5.5.6	1, 33, 3, 6, 15, 28, 51, 58, 59	Android 4.4 KitKat	Mozilla/5.0 (Linux; Android 4.4.2; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2404.144 Mobile Safari/537.36)
A0:02:DC:26:82:0C	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpdcd-5.5.6		Linksys WET54G wireless bridge	Dalvik/1.6.0 (Linux; U; Android 4.4.2; Build/JDQ39)
A0:02:DC:28:A1:D8	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpdcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linux; U; Android 4.4.2; Build/JDQ39)
A0:02:DC:48:71:A1	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpdcd-5.5.6	1, 33, 3, 6, 15, 28, 51, 58, 59	Android 4.2 Jelly Bean	Dalvik/1.6.0 (Linux; U; Android 4.2.2; Build/JDQ39)
A0:02:DC:97:F2:0D	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpdcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linux; U; Android 4.4.2; Build/JDQ39)
A0:02:DC:9D:60:42	Amazon Technologies Inc.	Android-Amazon-Kindle	dhcpdcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linux; U; Android 4.4.2; Build/JDQ39)
10:AE:60:13:63:C7	Private	Android-Amazon-Kindle	dhcpdcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linux; U; Android 4.4.2; Build/JDQ39)
10:AE:60:69:84:0E	Private	Android-Amazon-Kindle	dhcpdcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linux; U; Android 4.4.2; Build/JDQ39)
10:AE:60:DA:B7:0D	Private	Android-Amazon-Kindle	dhcpdcd-5.5.6		Android 4.4 KitKat	Dalvik/1.6.0 (Linux; U; Android 4.4.2; Build/JDQ39)
F0:4F:7C:C7:9E:C5	Private	Android-Amazon-Kindle	dhcpdcd-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)
F0:A2:25:0C:23:39	Private	Android-Amazon-Kindle	dhcpdcd 4.0.15	1, 121, 33, 3, 6, 15, 28, 51, 58, 59, 119	Android 2.3.x Gingerbread	Mozilla/5.0 (Linux; Android 2.3.4; en-us; Kindle Fire Build/GINGERBREAD) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2404.144 Mobile Safari/537.36
F0:A2:25:4F:E0:D6	Private	Android-Amazon-Kindle			Android 2.3.x Gingerbread	Mozilla/5.0 (Linux; Android 2.3.4; en-us; Kindle Fire Build/GINGERBREAD) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2404.144 Mobile Safari/537.36
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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2404.144 Mobile Safari/537.36
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; CyanogenMod-10) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2404.144 Mobile Safari/537.36
F0:A2:25:C9:4F:62	Private	Android-Amazon-Kindle	dhcpdcd 4.0.15		Android 2.3.x Gingerbread	Mozilla/5.0 (Linux; U; Android 2.3.4; en-us; Kindle Fire Build/GINGERBREAD) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2404.144 Mobile Safari/537.36
F0:A2:25:EC:A7:E8	Private	Android-Amazon-Kindle	dhcpdcd 4.0.15		Android 2.3.x Gingerbread	Mozilla/5.0 (Linux; U; Android 2.3.4; en-us; Kindle Fire Build/GINGERBREAD) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2404.144 Mobile Safari/537.36
F0:A2:25:EF:82:24	Private	Android-Amazon-Kindle	dhcpdcd 4.0.15		Android 2.3.x Gingerbread	Mozilla/5.0 (Linux; U; Android 2.3.4; en-us; Kindle Fire Build/GINGERBREAD) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/44.0.2404.144 Mobile Safari/537.36
08:60:6E:A3:2E:15	ASUSTek COMPUTER INC.	Android-Asus			Android	Android
08:60:6E:AC:24:63	ASUSTek COMPUTER INC.	Android-Asus	dhcpdcd-5.5.6			
08:60:6E:AE:ED:A7	ASUSTek COMPUTER INC.	Android-Asus	dhcpdcd-5.5.6			
10:BF:48:BF:76:39	ASUSTek COMPUTER INC.	Android-Asus	dhcpdcd-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	dhcpdcd-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	dhcpdcd-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!

Endpoints > 00:09:FB:0C:2D:F9

00:09:FB:0C:2D:F9



MAC Address: 00:09:FB:0C:2D:F9  
Username: 00-09-FB-0C-2D-F9  
Endpoint Profile: Philips-IntelliVue-MX450-Patient-Monitor  
Current IP Address: 10.1.10.105  
Location: Location → All Locations

Applications **Attributes** Authentication Threats

## General Attributes

### Description

Static Assignment	false
Endpoint Policy	Philips-IntelliVue-MX450-Patient-Monitor
Static Group Assignment	false
Identity Group Assignment	Profiled

## Other Attributes

OUI	Philips Patient Monitoring
OriginalUserName	0009fb0c2df9

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
IldpCacheCapabilities	S
IldpCapabilitiesMapSupported	S
IldpChassisId	10.1.10.105
IldpPortDescription	Interface 3 as ens33
IldpPortId	00:09:fb:0c:2d:f9
IldpSystemDescription	Linux philips-mx450.cts.local 3.10.0-327.el7.x86_64 #1 SMP
IldpSystemName	philips-mx450.cts.local
IldpUndefined127	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

The screenshot shows the 'Profiler Configuration' page in the ISE GUI. The breadcrumb path is 'Work Centers > Profiler > Settings'. The 'CoA Type' is set to 'Port Bounce'. There are fields for 'Current custom SNMP community strings' (masked with dots), 'Change custom SNMP community strings', and 'Confirm changed custom SNMP community strings'. The 'EndPoint Attribute Filter' is disabled. 'Enable Anomalous Behaviour Detection' is checked and enabled. 'Enable Anomalous Behaviour Enforcement' is unchecked and disabled. 'Enable Custom Attribute for Profiling Enforcement' is checked and enabled. Two blue arrows point from the callout boxes on the left to the 'Enable Anomalous Behaviour Detection' and 'Enable Anomalous Behaviour Enforcement' checkboxes.

**Profiler Configuration** Work Centers > Profiler > Settings

\* CoA Type:

Current custom SNMP community strings: ●●●●●●●●●●

Change custom SNMP community strings:  (For NMAP,

Confirm changed custom SNMP community strings:  (For NMAP,

EndPoint Attribute Filter:  Enabled ⓘ

Enable Anomalous Behaviour Detection:  Enabled ⓘ

Enable Anomalous Behaviour Enforcement:  Enabled

Enable Custom Attribute for Profiling Enforcement:  Enabled

# 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, Enable Anomalous Behaviour Enforcement:  Enabled  
CoA triggered on endpoint session.

AnomalousBehaviour true

Endpoints 00:60:B0:05:B2:C2

00:60:B0:05:B2:C2   

MAC Address: 00:60:B0:05:B2:C2  
Username:  
Endpoint Profile: Windows7-Workstation  
Current IP Address: 10.1.10.103  
Location:

Applications **Attributes** Authentication

### General Attributes

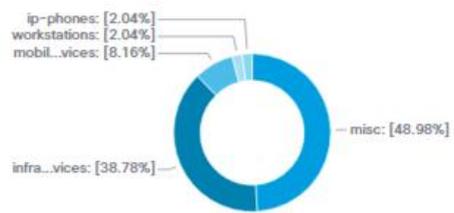
Description	
Static Assignment	false
Endpoint Policy	Windows7-Workstation
Static Group Assignment	false
Identity Group Assignment	Workstation

### Other Attributes

161-udp	snmp
162-udp	snmptrap
23-tcp	telnet
515-tcp	printer
AD-Fetch-Host-Name	win7-pc1
AD-Host-Exists	true
AD-Join-Point	CTS.LOCAL
AD-Last-Fetch-Time	1520222390464
AD-OS-Version	6.1 (7601)
AD-Operating-System	Windows 7 Professional N
AD-Service-Pack	Service Pack 1
AnomalousBehaviour	true
BYODRegistration	Unknown
DeviceRegistrationStatus	NotRegistered

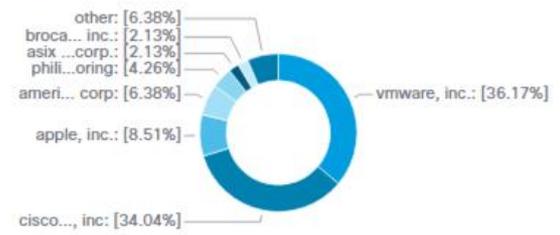
### ENDPOINTS

Type Profile



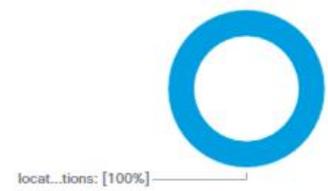
### ENDPOINT CATEGORIES

OUI OS Types Identity Group



### NETWORK DEVICES

Location Type Device Name



Rows/Page 10 1 / 5 Go 49 To

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

**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

▶ Exceptions (0)

Standard

Match endpoints flagged as exhibiting Anomalous Behavior

Deny access, apply restrictive access, or simply tag for visibility/enforcement in external systems (Switches, Firewalls, SIEM, VA, etc)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Anomalous Clients	if (Assigned_Port_Not_Matched OR EndPoints:AnomalousBehaviour EQUALS true )	then Quarantine AND Quarantined_Systems
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Access Points	if EndPoints:LogicalProfile EQUALS Access Points	then Access_Points
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones

# 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

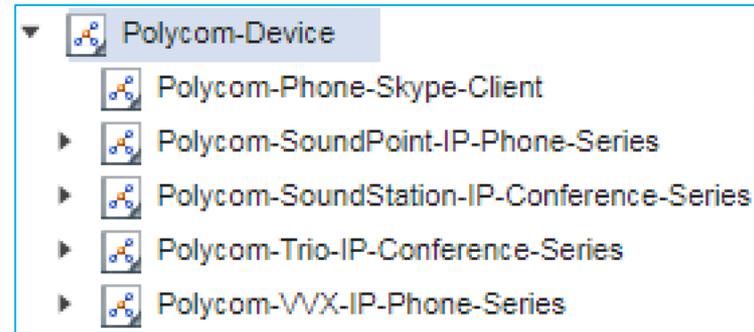
Rule Name	Conditions	Permissions	SGT
ABD Exception	EndpointsAnomalousBehaviour=true AND Endpoints:EndpointProfile = Polycom-Device	Phone-Access	Inspect
ABD Quarantine	EndpointsAnomalousBehaviour=true	Quarantine	Quarantine
IP-Phones	Endpoints:LogicalProfile = IP-Phones	Phone-Access	Voice

## • 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

OUI Cisco Systems, Inc

- 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.

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

Net New, but insufficient to change profile

## 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)

# 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.

Work Centers > Profiler > Profiling Policies

### Profiler Policy

1

\* Name  Description

Policy Enabled

\* Minimum Certainty Factor  (Valid Range 1 to 65535)

\* Exception Action

\* Network Scan (NMAP) Action

Create an Identity Group for the policy  Yes, create matching Identity Group  
 No, use existing Identity Group hierarchy

\* Parent Policy

\* Associated CoA Type

System Type Administrator Created

Rules

If Condition  Then

Work Centers > Profiler > Policy Elements > Exception Actions

### Profiler Exception Action

2

\* Name  Description

COA Action  Force CoA

\* Policy Assignment

System Type Administrator Created

# 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:
  - Trigger the named exception action “Looks-Like-Spoofing”
  - Increase Certainty Factor (likelihood profile will continue to match)

**Profiler Policy**

\* Name: Cisco-IP-Phone Description: Policy for all Cisco IP Phones

Policy Enabled

\* Minimum Certainty Factor: 20 (Valid Range 1 to 65535)

\* Exception Action: Looks-Like-Spoofing

\* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy:  Yes, create matching Identity Group  
 No, use existing Identity Group hierarchy

Parent Policy: Cisco-Device

\* Associated CoA Type: Global Settings

System Type: Administrator Modified

Rules

If Condition: CiscoIPPhoneDHCPClassIdentifierCheck	Then: Certainty Factor Increases	20
If Condition: CiscoIPPhoneCDPDeviceIdCheck	Then: Certainty Factor Increases	5
If Condition: Cisco-IP-Phone-Rule6-Check1	Then: Certainty Factor Increases	20
If Condition: IPPhoneLLDPCapabilitiesCheck	Then: Certainty Factor Increases	20
If Condition: Apple-MacOS-DHCP-PRL-Check1_OR_Ap...	Then: Take Exception Action	
If Condition: Microsoft-WorkstationRule1Check1	Then: Take Exception Action	
If Condition: Microsoft-WorkstationRule1Check1	Then: Certainty Factor Increases	200
If Condition: Apple-MacOS-DHCP-PRL-Check1_OR_Ap...	Then: Certainty Factor Increases	200

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

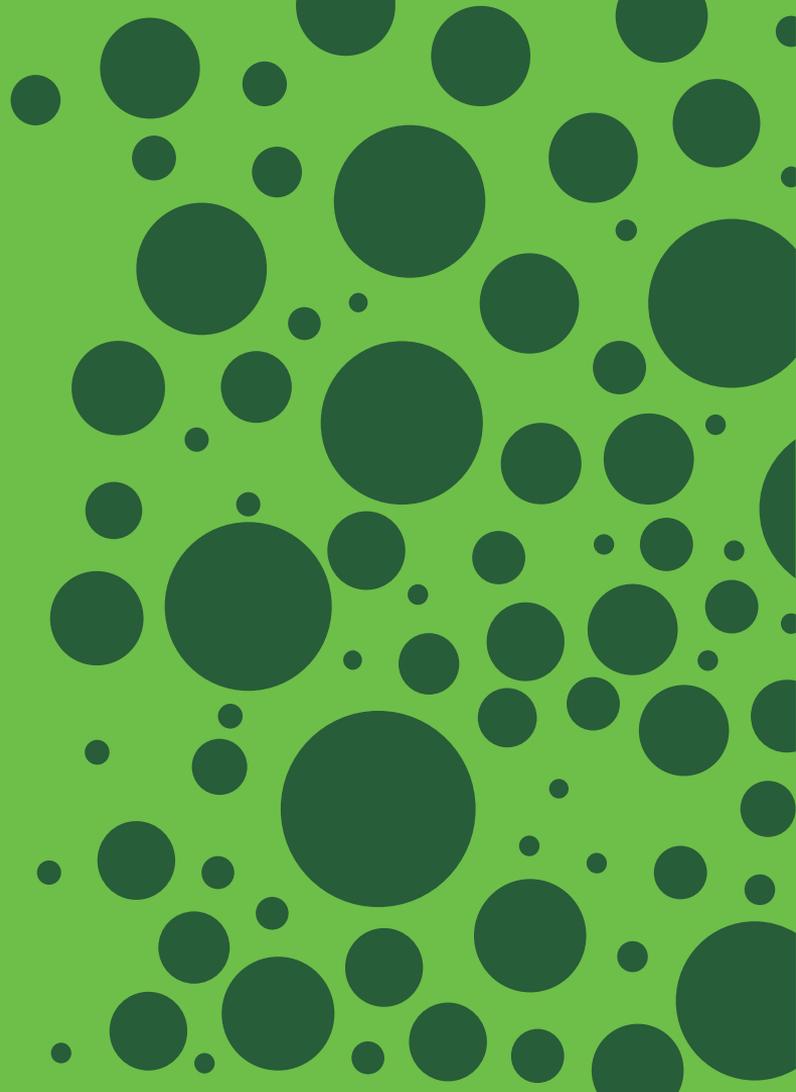
Authorization Policy - Local Exceptions (1)

	Status	Rule Name	Conditions	Results	Profiles	Security Groups
<input type="checkbox"/>		Anomaly Detected - Exception Action	OR EndPoints-EndPointPolicy EQUALS Spoofed-Device EndPoints-AnomalousBehaviour EQUALS true		*Restricted_Access	Quarantined_Systems

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
Reassessment configurations
Acceptable Use Policy
▼ Software Updates
Client Provisioning
Posture Updates
Proxy Settings

## Posture Updates

Web  Offline

\* Update Feed URL

Proxy Address  ⓘ

Proxy Port  HH MM SS

Automatically check for updates starting from initial delay    every  hours ⓘ



 **Updating ...**

### ▼ Update Information

Last successful update on	2018/05/30 00:25:51
Last update status since ISE was started	Last update attempt at 2018/05/30 00:25:51 was successful
Cisco conditions version	243865.0.0.0
Cisco AV/AS support chart version for windows	196.0.0.0
Cisco AV/AS support chart version for Mac OSX	115.0.0.0
Cisco supported OS version	43.0.0.0

# Posture General Settings

Work Centers > Posture > Settings > Posture General Settings

- Posture General Settings
- Resessment configurations
- Acceptable Use Policy
- ▼ Software Updates
  - Client Provisioning
  - Posture Updates
  - Proxy Settings

## Posture General Settings ⓘ

Remediation Timer  Minutes ⓘ

Network Transition Delay  Seconds ⓘ

Default Posture Status  ⓘ

Automatically Close Login Success Screen After  Seconds ⓘ

Continuous Monitoring Interval  Minutes ⓘ

Acceptable Use Policy in Stealth Mode

## Posture Lease

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

Cache Last Known Posture Compliant Status

Last Known Posture Compliant State  Hours

What if client does not support posture, or no matching provisioning policy?

Auto-Close Agent on Success

Posture Lease

Grace Periods -- Cache Last Known Posture Compliance

# Passive Re-Assessment (PRA)

Work Centers > Posture > Settings > Reassessment configurations

Posture General Settings
Reassessment configurations
Acceptable Use Policy
▼ Software Updates
Client Provisioning
Posture Updates
Proxy Settings

\* Configuration Name **PRA**

Configuration Description

Use Reassessment Enforcement?

Enforcement Type

Interval  minutes. ⓘ

Grace Time  minutes. ⓘ

Group Selection Rules

1. Each configuration must have a unique group or a unique combination of groups.
2. No two configurations may have any group in common.
3. If a config already exists with a group of 'Any', then no other configs can be created unless:
  - i. the existing config with a group of 'Any' is updated to reflect a group (or groups) other than 'Any', or
  - ii. the existing config with a group of 'Any' is deleted
4. If a config with a group of 'Any' must be created, delete all other configs first.

\* Select User Identity Groups  ⓘ

▼ PRA configurations

Configurations list

Existing Reassessment Configurations	User Identity Groups
<input type="radio"/> PRA	Employee

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+

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



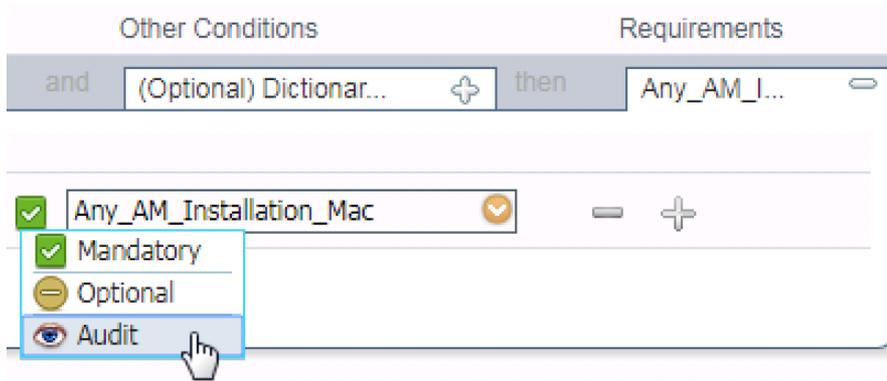
# Phased Approach to Posture/Compliance

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 <b>make corrective action</b> to comply with the posture policy
Optional	User is notified of failure results and given the option to continue in order to <b>bypass the posture</b> assessment policy
Audit	<b>User is not notified</b> of any failure results based on posture assessment policy

# Posture Enhancements

## Grace Periods

**Posture Policy**  
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Grace = 0 = Disabled  
Grace > 0 = Enabled

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type
<input checked="" type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect
<input checked="" type="checkbox"/>	Policy Options	Windows Service Pack Upd	If Any	and Windows All	and 4.x or later	and AnyConnect
<input checked="" type="checkbox"/>	Policy Options	Any_AM_Installation_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal

**Grace period settings**

Grace Period for: 1

- Days
- Minutes
- Hours
- Days

# Grace Period and Remediation

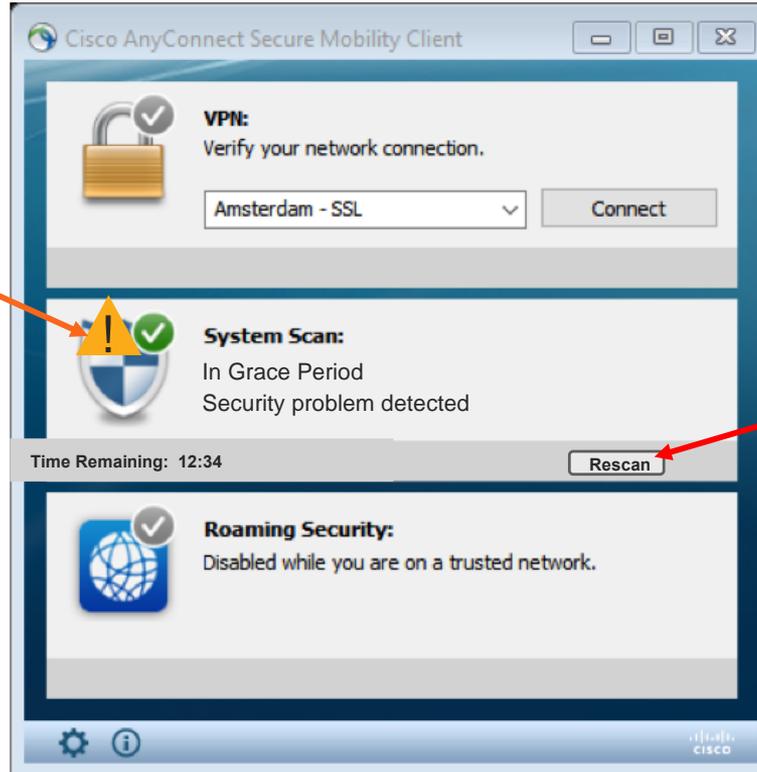
Rescan allows ad-hoc posture assessment

Warning Icons  
with Appropriate  
Message

Cisco AnyConnect

In Grace Period Message = Cisco Defined Text (e.g. "Your endpoint is not compliant but has been granted short term access. Please address the posture failures highlighted in AnyConnect system scan summary and then hit "Rescan" button to ensure continued full access

OK



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

# Design posture policies

## Reports for Grace Period -- 'Grace Compliant'

**Posture Assessment by Endpoint** ⓘ

From 2017-11-15 00:00:00.0 to 2017-11-15 11:57:01.0

Reports exported in last 7 days 0

+ My Reports Export To Schedule

Filter Refresh

Logged At	Status	Details	PRA Action	Identity	Endpoint ID
X Match All of the following rules. Enter Advanced Filter Name. Save					
Logged At	Within	Last 30 Days + - Filter			
2017-11-10 15:03:19.657	✗		N/A	puarya	00:71:CC:79:36:F4
2017-11-10 15:01:19.227	?		N/A	puarya	00:71:CC:79:36:F4
2017-11-10 14:59:18.342	Grace Compliant		N/A	puarya	00:71:CC:79:36:F4
2017-11-10 14:56:11.637	✓		N/A	puarya	00:71:CC:79:36:F4
2017-11-10 14:53:43.822	✓		N/A	puarya	00:71:CC:79:36:F4
2017-11-10 12:40:42.697	✗		N/A	puarya	00:71:CC:79:36:F4
2017-11-10 12:38:41.907	?		N/A	puarya	00:71:CC:79:36:F4
2017-11-10 12:26:59.165	✓		N/A	puarya	00:71:CC:79:36:F4
2017-11-10 09:00:12.175	✗		N/A	puarya	00:71:CC:79:36:F4
2017-11-10 08:59:11.615	?		N/A	puarya	00:71:CC:79:36:F4

# Alternative Approaches to Full ISE Compliance Assessment and Remediation

- Simply Check if Patch Management Installed/Running

Patch-Management Conditions List > **New Patch-Management Condition**

**Patch Management Condition**

\* Name: Patch\_Management\_Running  
 Description: Verify SCCM is running  
 \* Operating System: Windows All  
 \* Compliance Module: 4.x or later  
 \* Vendor Name: Microsoft Corporation  
 Check Type:  Installation  Enabled  Up to Date  
 Check patches installed: Critical only

**Products for Selected Vendor**

	Product Name	Version	Enabled	Checked Support	Update Checked Support	Minimum Compliant Module S
<input type="checkbox"/>	Microsoft Intune Client	5.x	NO		NO	4.2.520.0
<input type="checkbox"/>	System Center Configuration Manager Client	4.x	YES		YES	4.2.1331.0
<input checked="" type="checkbox"/>	System Center Configuration Manager Client	5.x	YES		YES	4.2.520.0
<input type="checkbox"/>	Windows Update Agent	10.x	YES		YES	4.2.520.0
<input type="checkbox"/>	Windows Update Agent	7.x	YES		YES	4.2.520.0

\* Name: Patch\_Management\_Running  
 Description: Verify JAMF Casper Suite running  
 \* Operating System: Mac OSX  
 \* Compliance Module: 4.x or later  
 \* Vendor Name: JAM Software  
 Check Type:  Apple Inc.  Dell Inc.  JAM Software  JAMF Software, LLC  Kromtech  Kromtech Alliance Corp.

- 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.

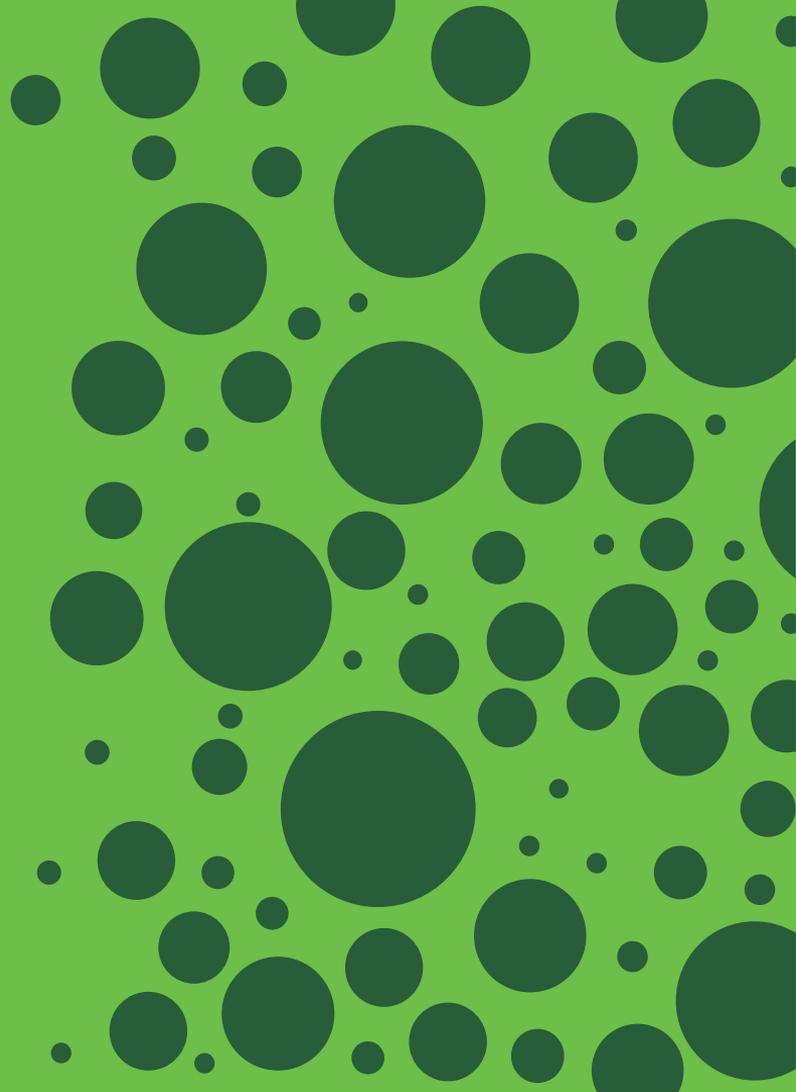
# Alternative Approaches to Full ISE Compliance Assessment and Remediation

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

Status	Rule Name	Conditions
	Device Registered and Compliant	AND <ul style="list-style-type: none"><li>MDM-DeviceRegisterStatus EQUALS Registered</li><li>MDM-DeviceCompliantStatus EQUALS Compliant</li><li>MDM-DaysSinceLastCheckin LESS 1</li></ul>

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

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.

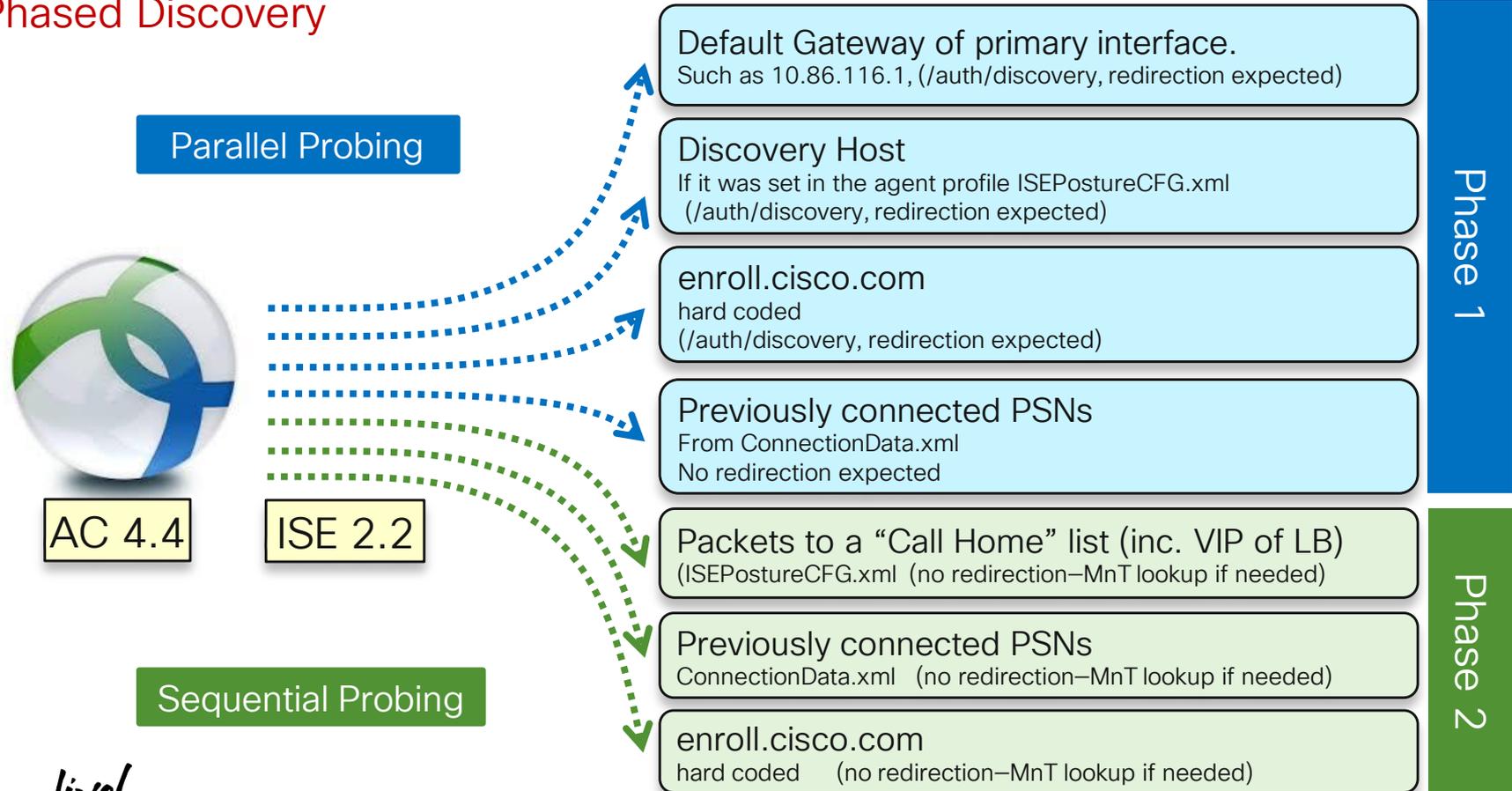
Discovery Host  
If it was set in the agent profile ISEPostureCFG.xml  
/auth/discovery, redirection expected

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

Previously connected head-ends  
From ConnectionData.xml  
No redirection expected

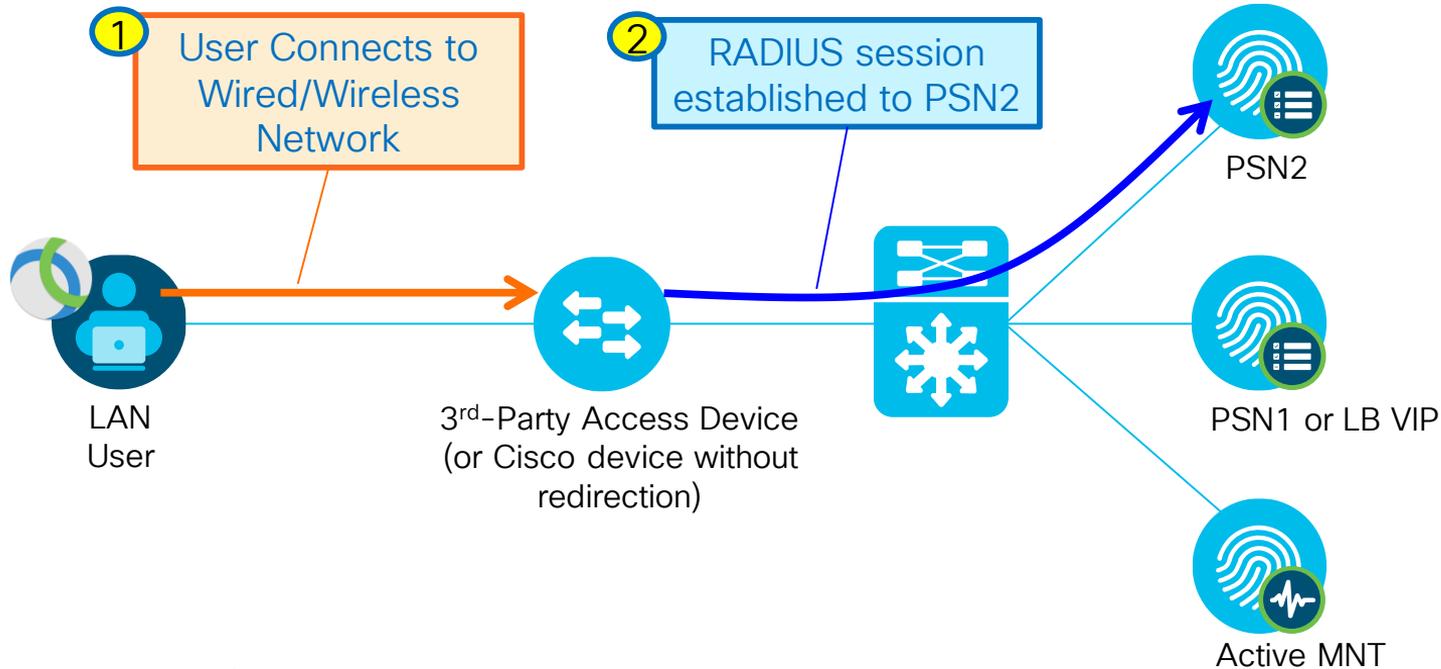
# AnyConnect PSN Node Discovery

## Phased Discovery



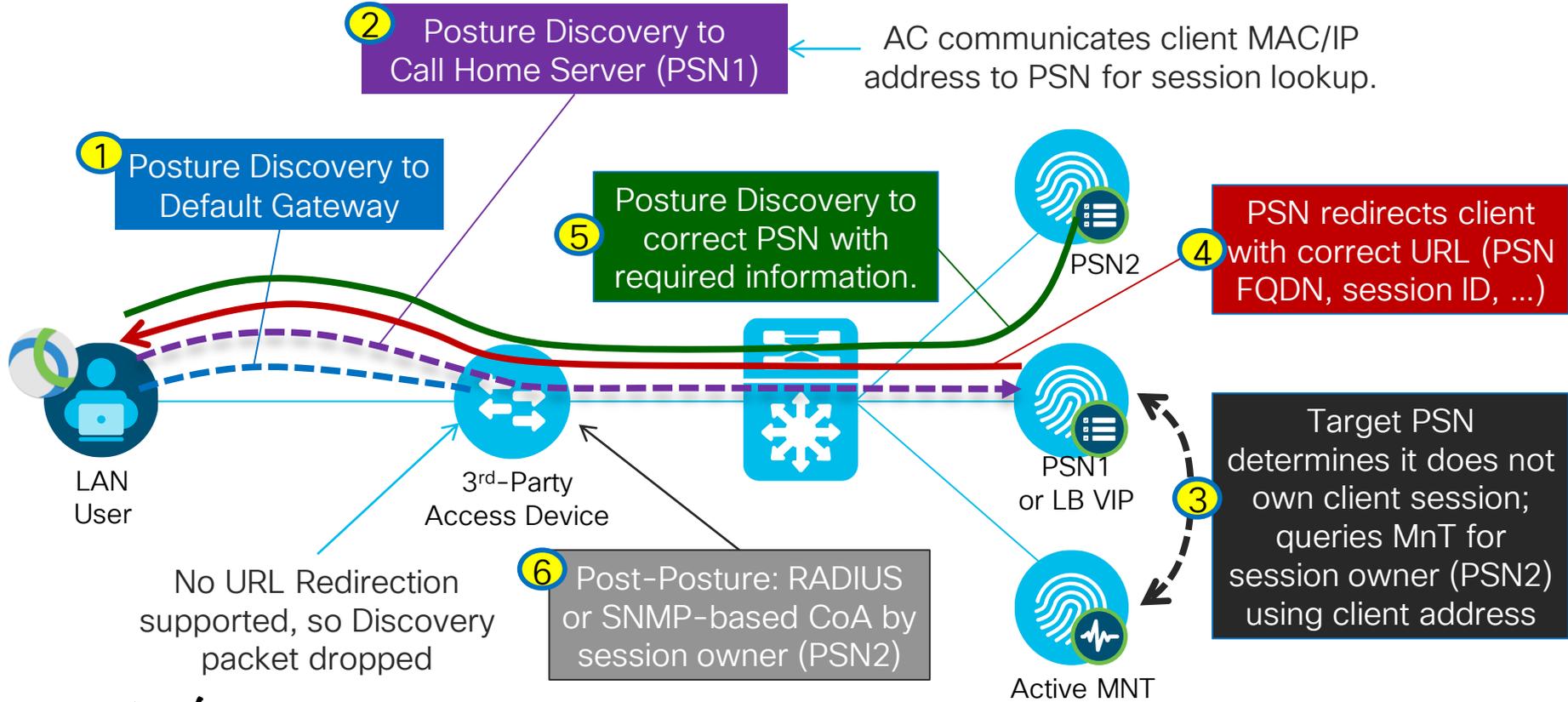
# ISE 2.2/AC 4.4 Posture Discovery

## RADIUS Session



# ISE 2.2/AC 4.4 Posture Discovery

## Posture Discovery



# AnyConnect Posture Profile

## Discovery Host and Call Home Lists

### Posture Protocol

Single Entry for Initial Discovery

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if there is a Passive Reassessment communication failure
Discovery host	<input type="text" value="redirect.company.com"/>		The server that the agent should connect to
* Server name rules	<input type="text" value="*.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	<input type="text" value="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)	List of PSNs (or VIPs!) to use as a fallback to initial Discovery 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	<input type="text" value="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

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!

Identity Services Engine

Home ▶ Context Visibility ▶ Operations ▶ Policy ▶ Administration

▶ System ▶ Identity Management ▶ Network Resources ▶ Device Portal Management ▶ pxGrid Services ▶ Feed Services

Blacklist BYOD Certificate Provisioning **Client Provisioning** Mobile Device Management My Devices Custom Portals

Portal & Page Settings

▶ Portal Settings

▼ Login Page Settings

Enable Login

Maximum failed login attempts before rate limiting:  (1 - 999)

Time between login attempts when rate limiting:  (1 - 999)

Include an AUP  ▼

Require acceptance

Require scrolling to end of AUP

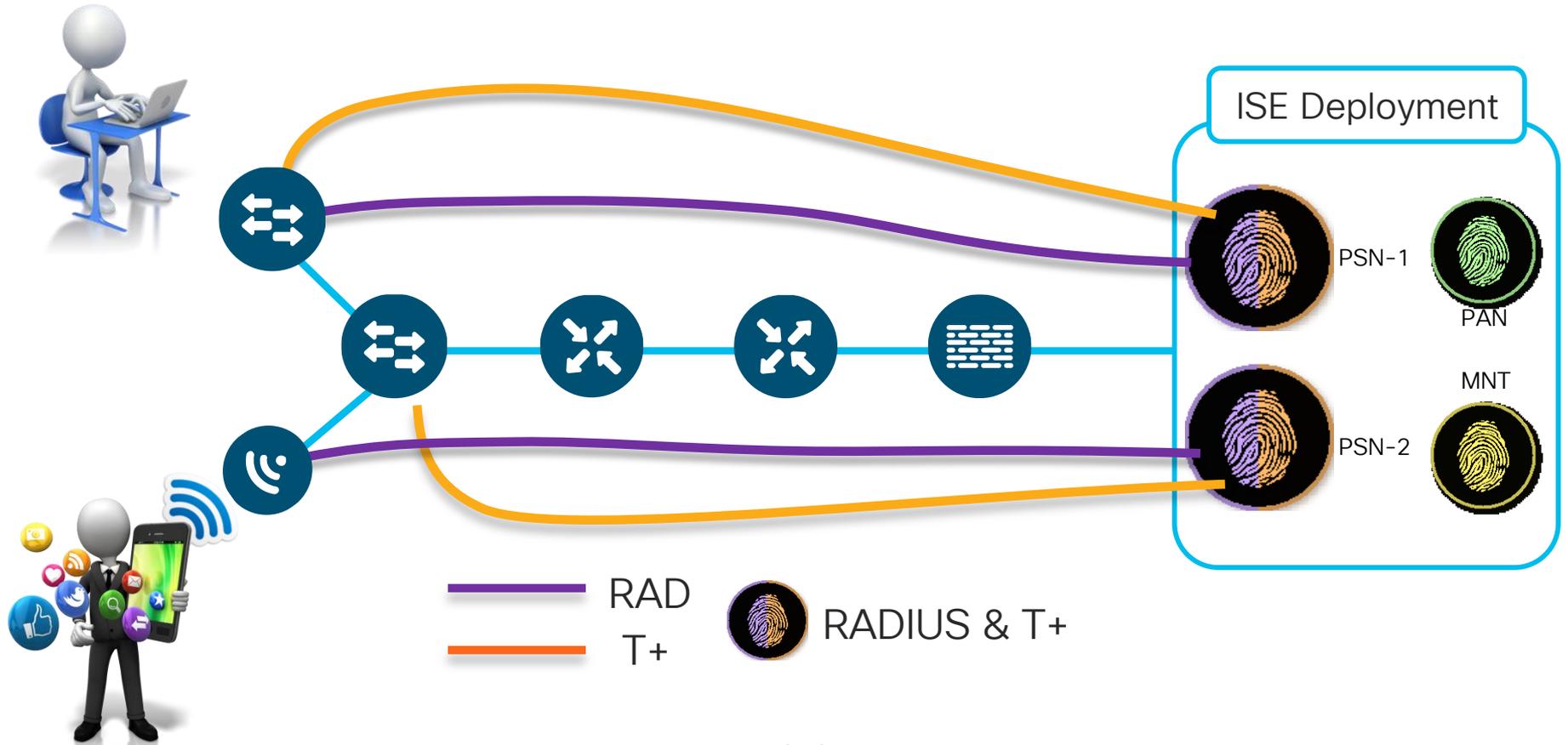
Enabling Auto-Login tells PSN to perform MnT lookup for existing session based on client IP.

BRKSEC-3697

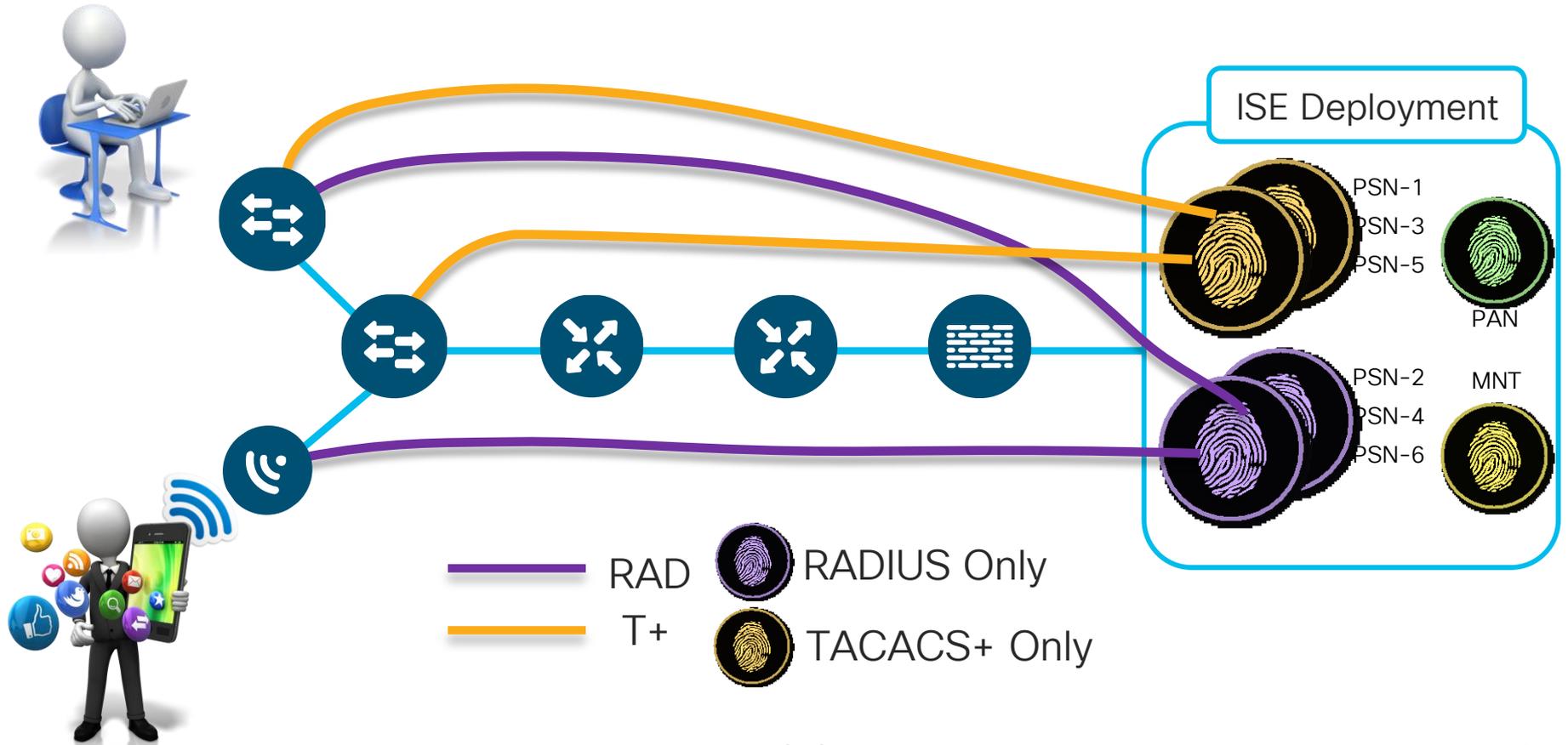
Cisco Public 145

# TACACS+ Deployment Best Practices

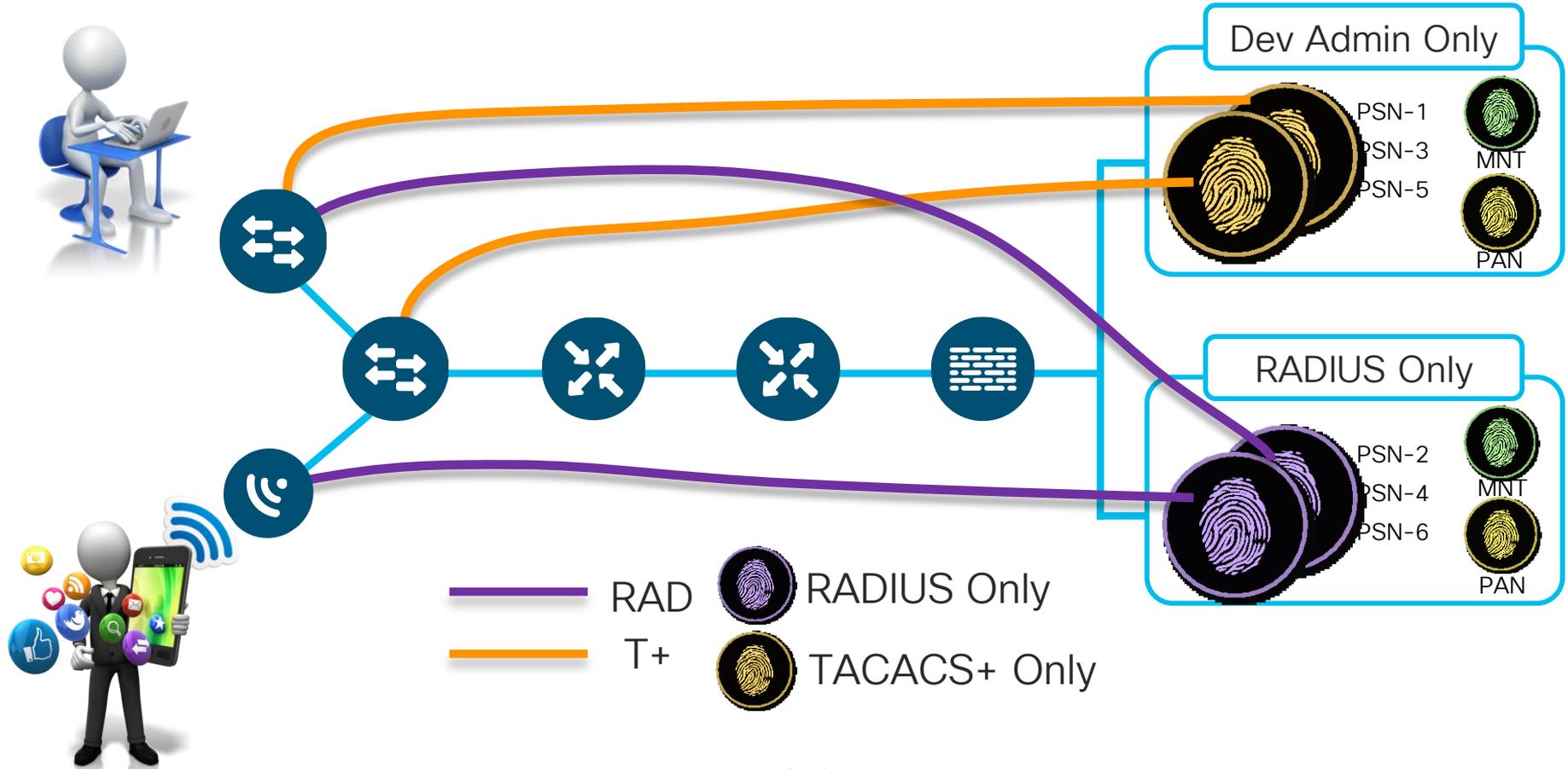
# Design #1 - RADIUS & TACACS+ Share PSNs



# Design #2 - RADIUS & T+ Use Dedicated PSNs



# Design #3 - Separate Deployments for RAD & T+



# RADIUS Only PSNs

Administration > System > Deployment > [ISE node]

**Personas**

- Administration Role **PRIMARY** Make Standalone
- Monitoring Role PRIMARY Other Monitoring Node
- Policy Service **Policy Service is Required**
  - Enable Session Services Include Node in Node Group None i
  - Enable Profiling Service
  - Enable SXP Service Use Interface GigabitEthernet 0 i
  - Enable Device Admin Service **TACACS+ Disabled**
  - Enable Identity Mapping i
- pxGrid i

Enable What's Needed for Network Access

# TACACS+ Only PSNs

Administration > System > Deployment > [ISE node]

**Personas**

- Administration Role **PRIMARY** Make Standalone
- Monitoring Role PRIMARY Other Monitoring Node
- Policy Service **Policy Service is Required**
  - Enable Session Services Include Node in Node Group: None  
 Enable Profiling Service  
 Enable SXP Service Use Interface: GigabitEthernet 0
  - Enable Device Admin Service **Device Admin = T+**
  - Enable Identity Mapping
  - pxGrid

Disable Network Access Services

# Options for Deploying Device Admin

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

<b>Priorities</b> 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+	Green	Red	Red
	No: Shared resources/Reduced \$\$	Red	Yellow	Green
Independent Scaling of Services	Yes: Scale as needed/No impact on Device Admin from RADIUS services	Green	Yellow	Red
	No: Avoid underutilized PSNs	Red	Yellow	Green
Suitable for high-volume Device Admin	Yes: Services dedicated to TACACS+	Green	Green	Red
	No: Focus on “human” device admins	Red	Yellow	Green
Separation of Logging Store	Yes: Optimize log retention VM	Green	Red	Red
	No: Centralized monitoring	Red	Green	Green

# ACS to ISE Migration

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



**CISCO** Communities

Products & Services Partners Global Developer

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

## 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**



### Cisco ACS to ISE Migration Guide

*Secure Access How to Guides Series*

Author: Krishnan Thiruvengadam  
Date: June 2nd, 2016



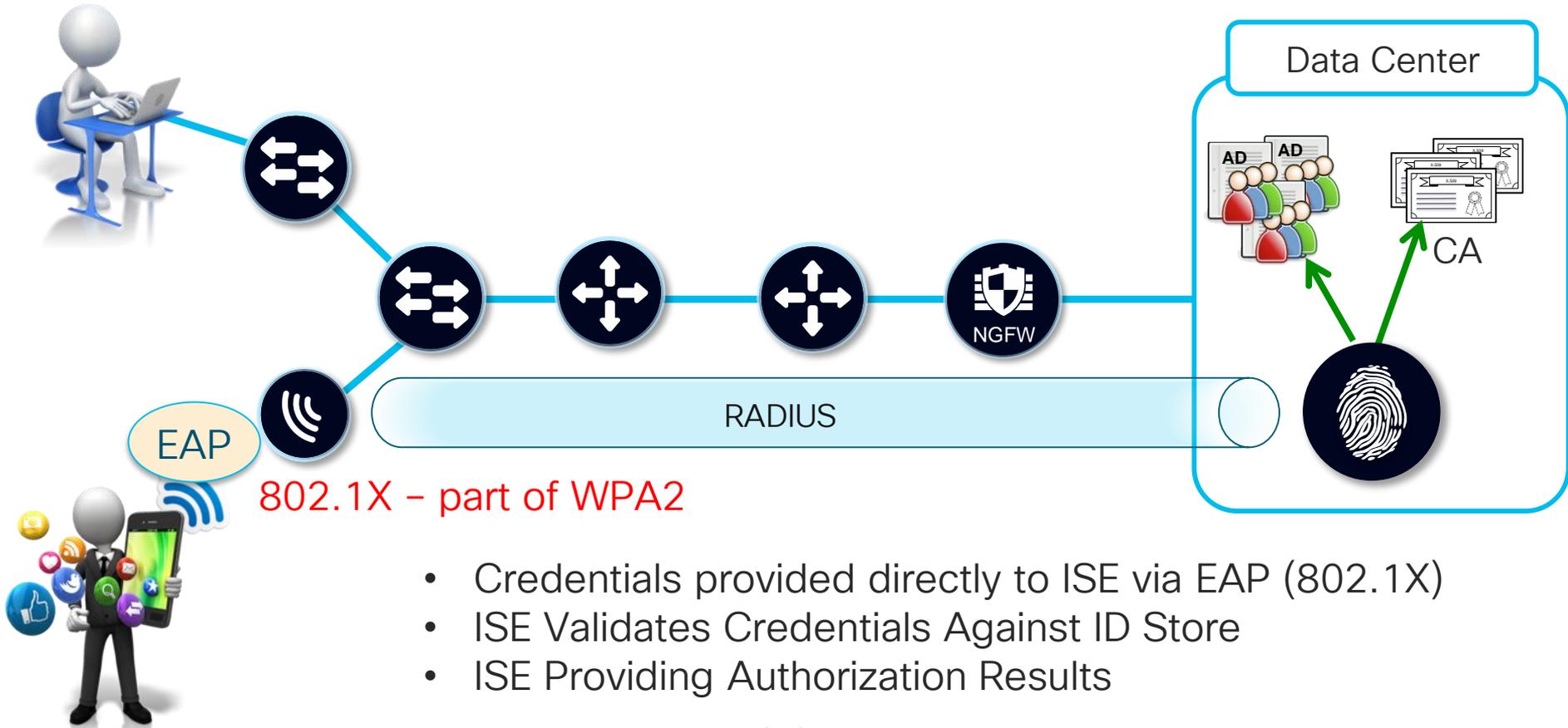
BRKSEC-3697 reserved. Cisco Public 153

# What is Passive Identity

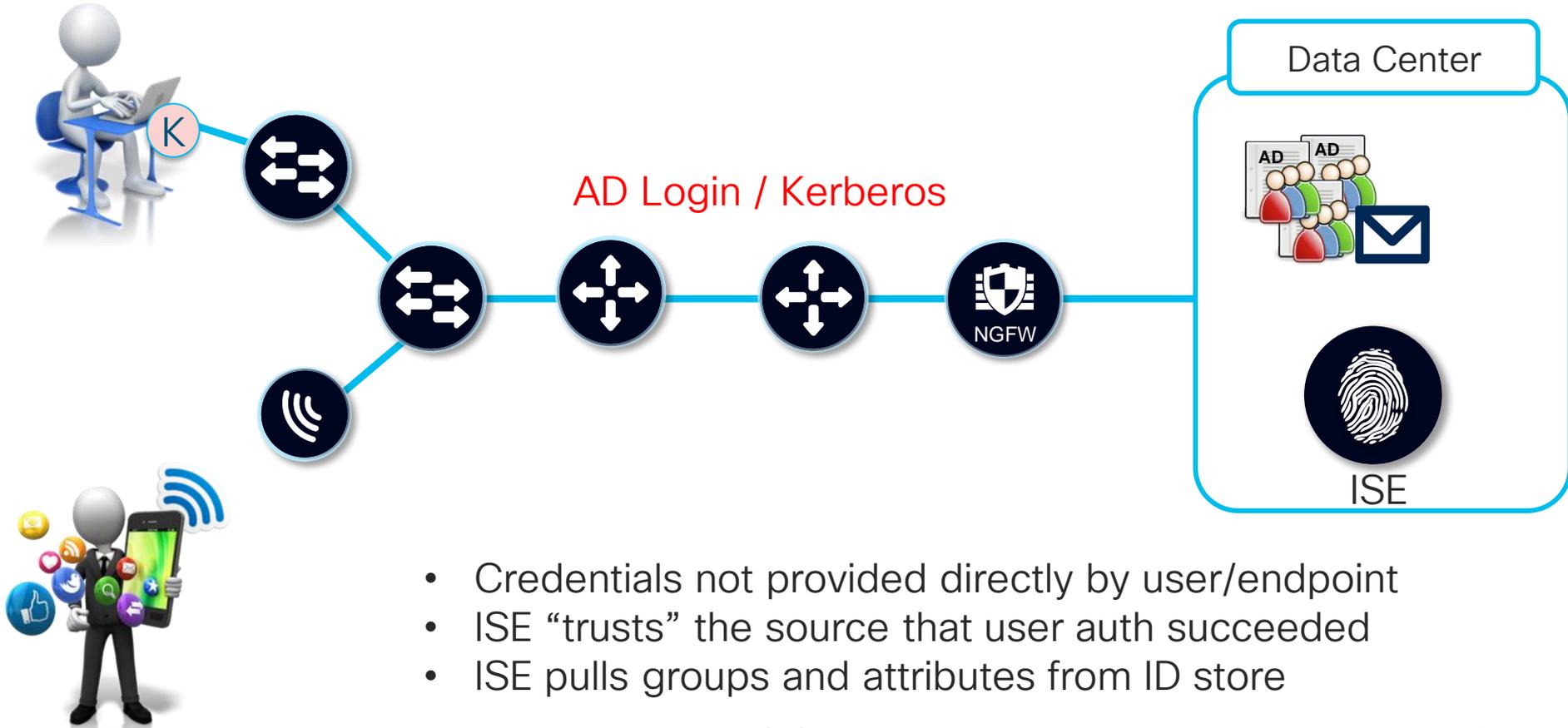
# Passive vs Active Identity / Authentication

- 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](mailto: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



# Passive Authentication

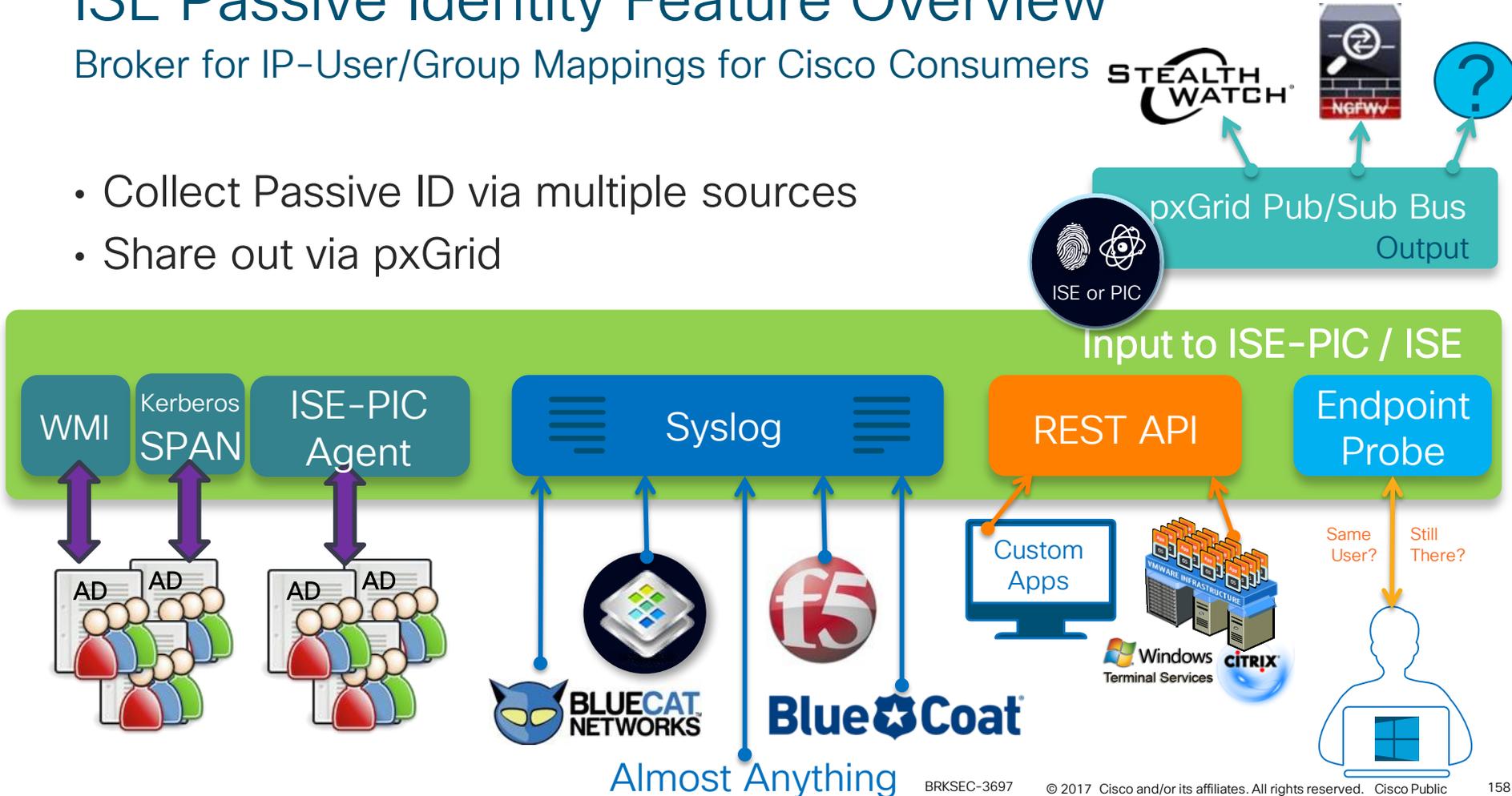


- Credentials not provided directly by user/endpoint
- ISE “trusts” the source that user auth succeeded
- ISE pulls groups and attributes from ID store

# 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

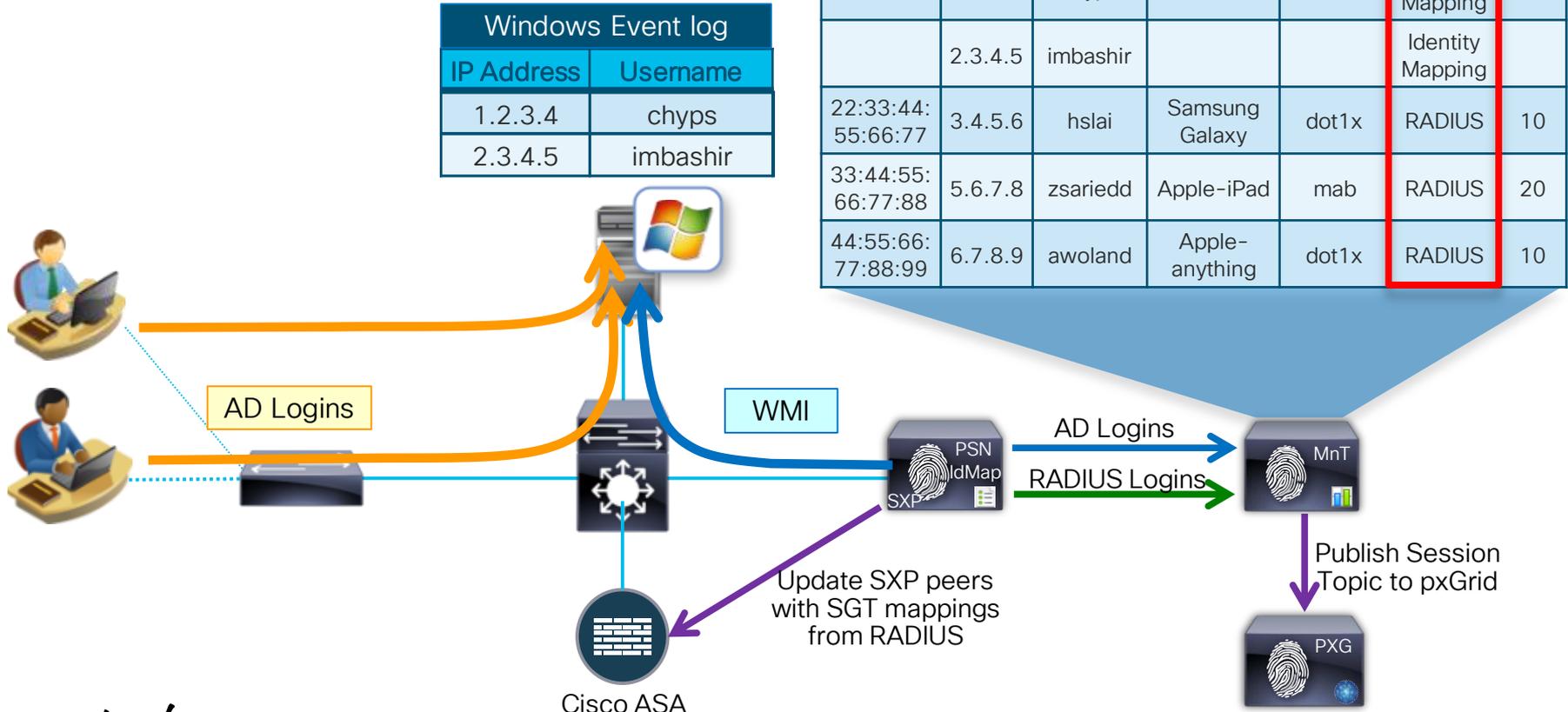
The screenshot shows the 'Edit Node' configuration page for a node named 'tb-amit-6-vm3'. The page is divided into 'General Settings' and 'Profiling Configuration' tabs. Under 'General Settings', the Hostname is 'tb-amit-6-vm3', FQDN is 'tb-amit-6-vm3.cisco.com', and IP Address is '10.56.15.134'. The Node Type is 'Identity Services Engine (ISE)'. Under 'Profiling Configuration', several services are listed with checkboxes and roles. The 'Enable Passive Identity Service' checkbox is checked and highlighted with a red box. Other services include Administration (checked, role STANDALONE), Monitoring (checked, role PRIMARY), Policy Service (checked), Enable Session Services (checked), Enable Profiling Service (checked), Enable Threat Centric NAC Service (unchecked), Enable SXP Service (unchecked), Enable Device Admin Service (unchecked), and pxGrid (unchecked). The 'Use Interface' is set to 'GigabitEthernet 0'.

# Easy Connect: Identifying Trusted Users without 802.1X User Authentication



# Easy Connect

## Consuming Both AD and RADIUS Logins



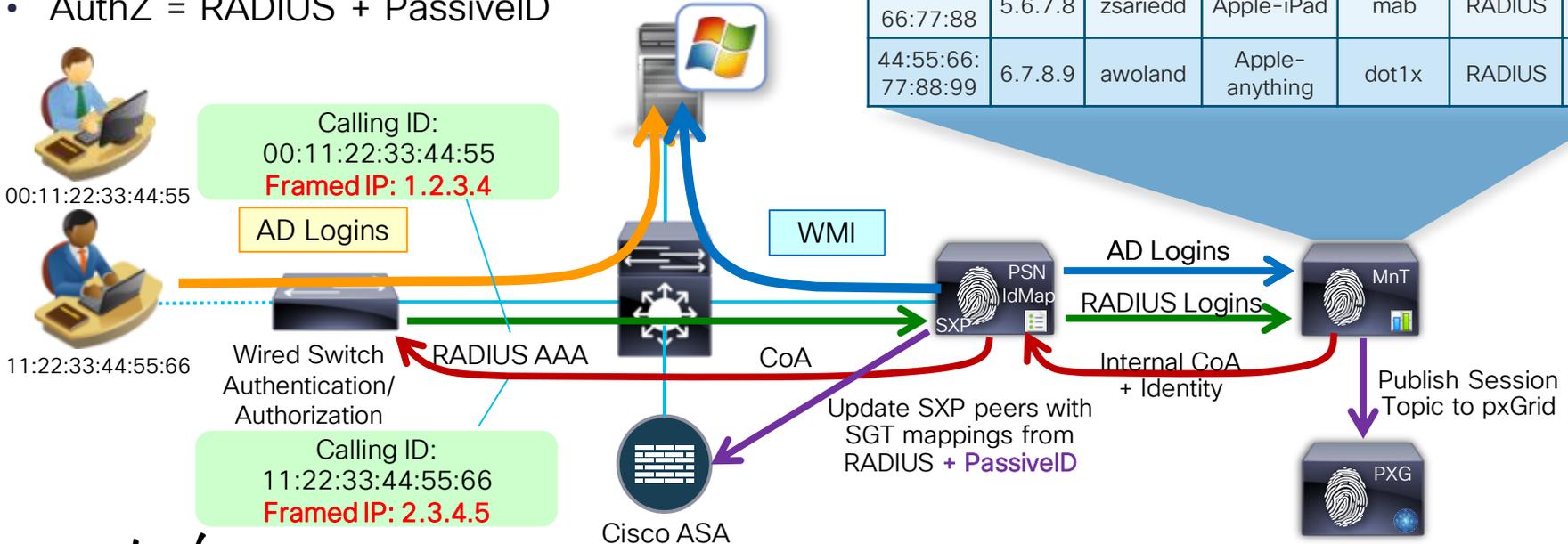
# Easy Connect Enforcement

## 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	Identity-RADIUS	10
11:22:33:44:55:66	2.3.4.5	imbashir	Windows 10	MAB+PsvID	Identity-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).

**Authorization Profile**

\* Name:

Description:

\* Access Type:

Network Device Profile:

Service Template:

Track Movement:

Passive Identity Tracking

**Common Tasks**

DACL Name:

# 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

# 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

**Profiler Policy**

\* Name: Workstation\_Corp Description: Custom Policy for Corporate Workstations

Policy Enabled:

\* Minimum Certainty Factor: 30 (Valid Range 1 to 65535)

\* Exception Action: NONE

\* Network Scan (NMAP) Action: NONE

Create Matching Identity Group  
 Use Hierarchy

\* Parent Policy: Workstation

**Rules**

If Condition: IP\_FQDN\_CONTAINS\_mycompany.com\_OR\_... Then: Certainty Factor Increases 30

Condition Name	Expression	OR
IP:FQDN	CONTAINS mycompany.com	OR
DHCP:client-fqdn	CONTAINS mycompany.com	OR
DHCP:domain-name	CONTAINS mycompany.com	

If Condition: OS\_X\_SnowLeopard-WorkstationRule1Check1 Then: Certainty Factor Increases 30

# 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](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)

**Profiler Policy**

\* Name: Windows10-Corp-XYZ-Workstation

Policy Enabled:

Certainty Factor: 50 (Valid Range)

Exception Action: NONE

in (NMAP) Action: NONE

Group for the policy:  Yes, create matching Identity Group  
 No, use existing Identity Group hierarchy

\* Parent Policy: Windows10-Workstation

Associated CoA Type: Global Settings

**Profiler Condition List > New Profiler Condition**

**Profiler Condition**

\* Name: Corp-XYZ

\* Type: DHCP

\* Attribute Name: dhcp-user-class-id

\* Operator: EQUALS

\* Attribute Value: 43:6f:72:70:2d:58:59:5a

System Type: Administrative Created

Submit Cancel

**Condition value must be expressed in hex.**

**Rules**

If Condition: Corp-XYZ Then: Certainty Factor Increases 50

# Identifying Trusted Devices using NMAP

## Custom Port Scans

Custom Ports

Work Centers > Profiler > Manual Scans

Add up to 10 UDP and 10 TCP custom ports to this action.

UDP Ports:

Add

2502  
2503  
2504  
3000

Remove

TCP Ports:

Add

8081

Remove

▶ View Common Ports

OK

Cancel

### Scan Options

OS ⓘ

Run SMB Discovery script ⓘ

SNMP Port ⓘ

Skip NMAP Host Discovery ⓘ

(Only applies to manually run scans)

Common ports ⓘ

Custom ports ⓘ



Include service version information ⓘ

Reset to Default Scan Options

AP Scan Actions

# Identifying Trusted Devices using NMAP

## Service Information

Custom Ports

Work Centers > Profiler > Manual Scans

Add up to 10 UDP and 10 TCP custom ports to this action.

UDP Ports:

Add

2502  
2503  
2504  
3000

Remove

TCP Ports:

Add

8081

Remove

Scan Options

TCP ports automatically checked for McAfee ePolicy Orchestrator if **Service Version** information checked.

Custom ports

Include service version information ⓘ

▶ View Common Ports

OK

Cancel

UDP:

53 161  
67 162  
68 445  
123 500  
135 520  
137 631  
138 1434  
139 1900

TCP:

21 143  
22 443  
23 445  
25 515  
53 631  
80 3306  
110 3389  
135 8080  
139 9100

OK

Cancel

# NMAP Scan Actions

Used in Profiler Policies (triggered scans)  
or Manual Scans

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Directory', and 'Operations'. Below it, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', and 'Client Provisioning'. The 'Results' tab is selected. On the left sidebar, there are sections for 'Authentication', 'Authorization', 'Profiling', and 'Posture'. The main content area is titled 'NMAP Scan Actions' and contains a table of actions. The 'SMB-scan' action is highlighted with a red box. An orange arrow points from this box to the detailed configuration view on the right.

Network Scan (NMAP) Action Name	System Type
<input type="checkbox"/> MCAFeeEPOOrchestratorClientscan	Cisco Provided
<input type="checkbox"/> OS-scan	Cisco Provided
<input type="checkbox"/> <b>SMB-scan</b>	Cisco Provided
<input type="checkbox"/> SNMPPortsAndOS-scan	Cisco Provided

The detailed configuration view for the 'SMB-scan' action is shown. It includes the following fields:

- \* Action Name:** SMB-scan
- Description:** Perform SMB scan
- System Type:** Cisco Provided
- Scan Options:**
  - OS
  - SNMP Port
  - Common Port
  - Custom ports
  - Include service version information
  - Run SMB Discovery script
  - Skip NMAP Host Discovery

The 'Run SMB Discovery script' option is circled in blue.

# Triggered NMAP Scan using Template

Work Centers > Profiler > Profiling Policies

**Profiler Policy**

\* Name  Description

Policy Enabled

\* Minimum Certainty Factor  (Valid Range 1 to 65535)

\* Exception Action

\* Network Scan (NMAP) Action

Create an Identity Group for the policy  Yes, create matching Identity Group  
 No, use existing Identity Group hierarchy

Parent Policy Workstation

\* Associated CoA Type

System Type Cisco Provided

**Rules**

If Condition	<input type="text" value="Windows7-Workstation-Rule2-Check1"/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="10"/>
If Condition	<input type="text" value="Microsoft-WorkstationRule1Check1"/>	Then	<input type="text" value="Take Network Scan Action"/>	
If Condition	<input type="text" value="Windows10-Workstation-Rule5-Check1"/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="10"/>

**Conditions Details**

Name Microsoft-WorkstationRule1Check1

Description Microsoft-WorkstationRule1Check1

Expression DHCP:dhcp-class-identifier  
CONTAINS MSFT

# 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](http://www.kb.lesolson.com/InstantKB20/Attachment130.aspx)

# Enhanced NMAP Probe

## Custom Ports, Service Info, ePO Check

**Identity Services Engine** Home Context Directory

Endpoints Users Network Devices

Endpoints > 00:10:18:88:4C:94

00:10:18:88:4C:94

MAC Address: 00:10:18:88:4C:94  
Username: 00-10-18-88-4C-94  
**Endpoint Profile: Corporate-Windows7-Workstation**  
Current IP Address: 10.1.10.103  
Location:

Attributes Authentication Threats Vulnerabilities

General Attributes

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

123-udp	ntp
135-tcp	microsoft-rpc-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	dhcpc
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



**Active Directory**

Days before rescan

Description

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

### Conditions

Profiler Condition List > **New Profiler Condition**

#### Profiler Condition

\* Name

Description

\* Type

\* Attribute Name

\* Operator

\* Attribute Value

System Type



### 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\

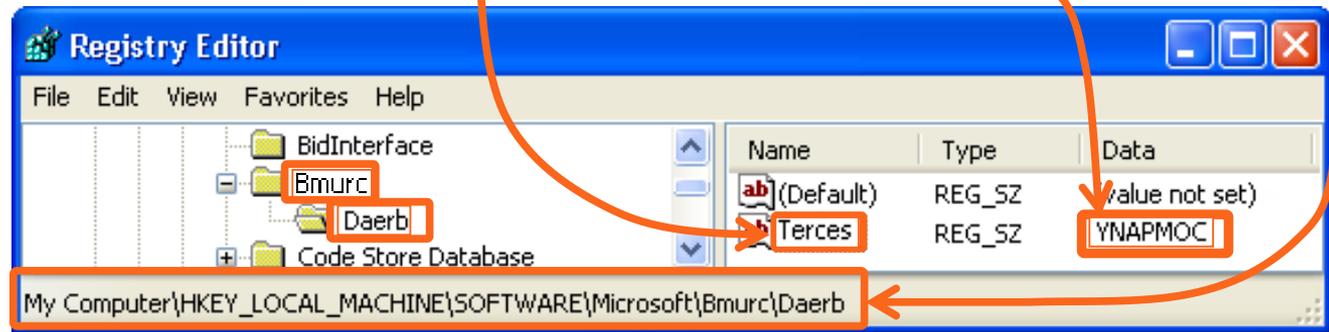
COMPANY secret bread crumb

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

Registry Conditions List > New Registry Condition

### Registry Condition

\* Name: Company\_BreadCrumb\_Check  
Description: Check for company registry key  
Registry Type: RegistryValue  
Registry Root Key: HKLM \* Sub Key: SOFTWARE\Microsoft\Bmurc\Daerb  
\* Value Name: Terces  
Value DataType: String  
Value Operator: equals  
Value Data: YNAPMOC  
\* Operating System: Windows All



SOE=Standard Operating Environment

# Endpoint Custom Attributes

Administration > Identity Management > Settings

Once defined, Custom Attributes can be set using:

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

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

Int

Boolean

Float

Long

IP

Date

String

# Endpoint Custom Attributes

## Edit Attributes From Context Visibility

▼ General Attributes

Mac Address \* 00:10:18:88:4C:94

Description Technical Marketing Department workstation - Building G -4th floor

▼ Custom Attributes

Filter ⌵ ⚙

Attribute Name	Attribute Value	
AssetTagNumber	864444923566	✓ ✕
AssetType	Managed	✎
ProfitCenter	00251977	✎
CorpDevice	true	✎
SerialNumber	BX13529574C	✎

Save/Delete

Edit

# 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>
```

The screenshot displays a REST client interface for the endpoint `https://10.1.101.16:9060/ers/config/endpoint/6ec34372-f790-11e5-aaa3-0`. The 'Headers' tab is selected, showing the following headers:

Header	Value
Authorization	Basic ZXJzYWRtaW46ZGVmYXVsdDFB
Accept	application/vnd.com.cisco.ise.identity.enc
Accept-Search-Result	application/vnd.com.cisco.ise.ers.searchr

The 'Body' tab is also visible, showing the XML payload for the customAttributes section:

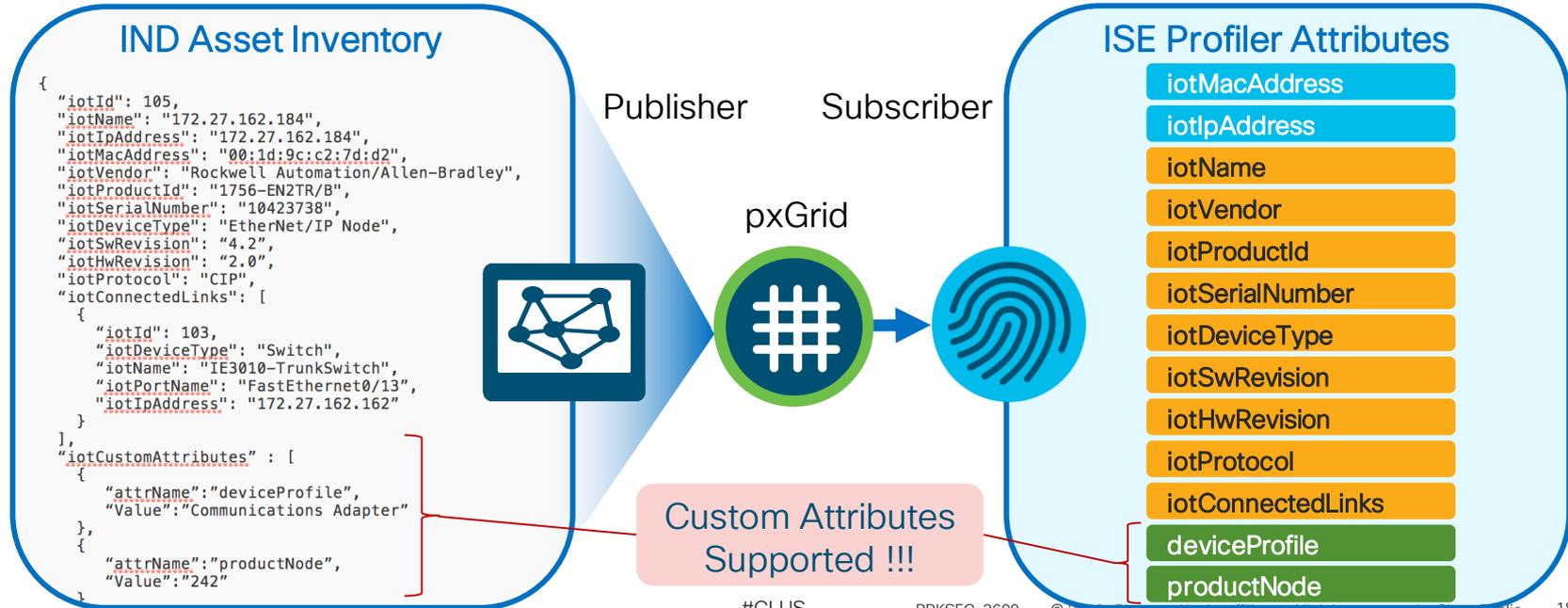
```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<ns4:endpoint id="6ec34372-f790-11e5-aaa3-00505691cf84" name="00:10:18:88:4C:94"
.com" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:ns4="identity.ers.is
<link rel="self" href="https://10.1.101.16:9060/ers/config/endpoint/6ec34372
-00505691cf84" type="application/xml"/>
<customAttributes>
  <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

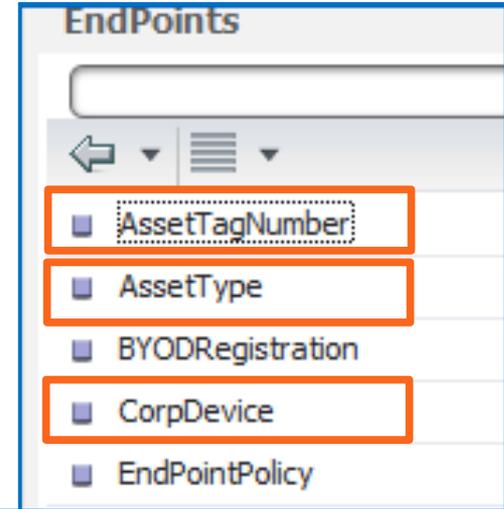
New in  
ISE 2.4

- 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.

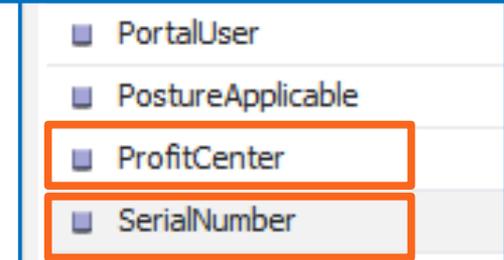


# Custom Endpoint Attributes

- Exposed to Authorization Policy Rule Conditions



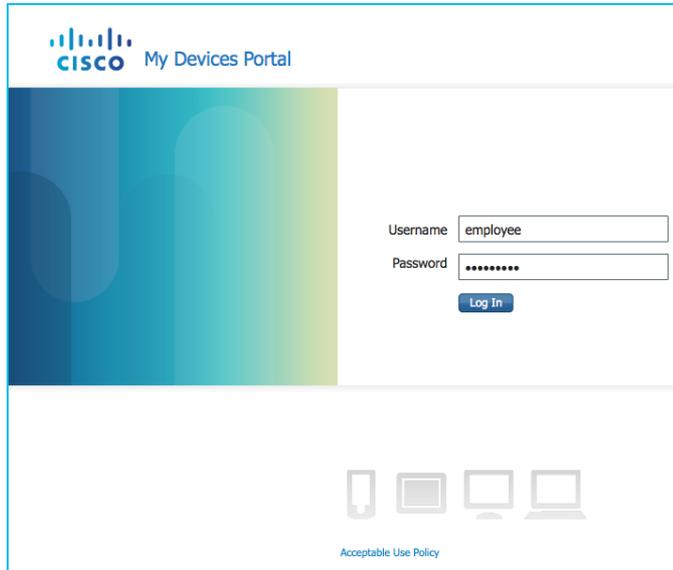
Rule Name	Conditions (identity groups and other conditions)	Permissions
Corporate PC Policy	if (EndPoints:CorpDevice EQUALS True AND EndPoints:EndPointPolicy EQUALS Microsoft-Workstation)	then PermitAccess



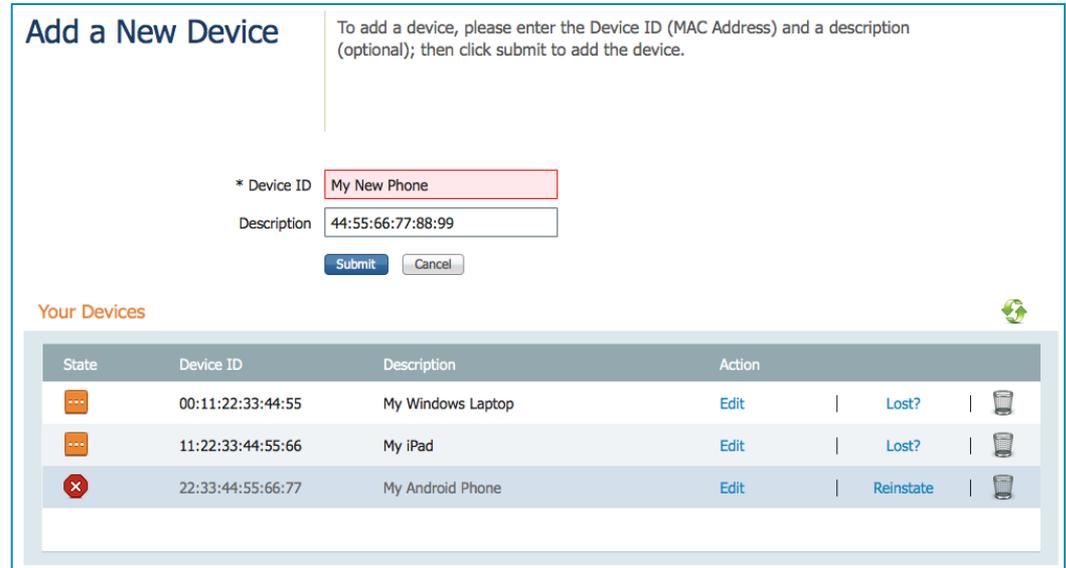
# Identifying Corporate Assets

## 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.



The image shows the Cisco My Devices Portal login interface. It features the Cisco logo and the text "My Devices Portal" at the top left. Below this, there is a login form with fields for "Username" (containing "employee") and "Password" (masked with dots). A "Log In" button is positioned below the password field. At the bottom of the page, there are icons for a smartphone, tablet, laptop, and desktop monitor, along with a link to the "Acceptable Use Policy".



The image shows the "Add a New Device" form and a table of registered devices. The form includes a title "Add a New Device" and instructions: "To add a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device." The form has two input fields: "\* Device ID" (containing "My New Phone") and "Description" (containing "44:55:66:77:88:99"). There are "Submit" and "Cancel" buttons below the fields. Below the form is a section titled "Your Devices" with a refresh icon. It contains a table with the following data:

State	Device ID	Description	Action		
...	00:11:22:33:44:55	My Windows Laptop	Edit	Lost?	
...	11:22:33:44:55:66	My iPad	Edit	Lost?	
✖	22:33:44:55:66:77	My Android Phone	Edit	Reinstate	

# External Device Registration

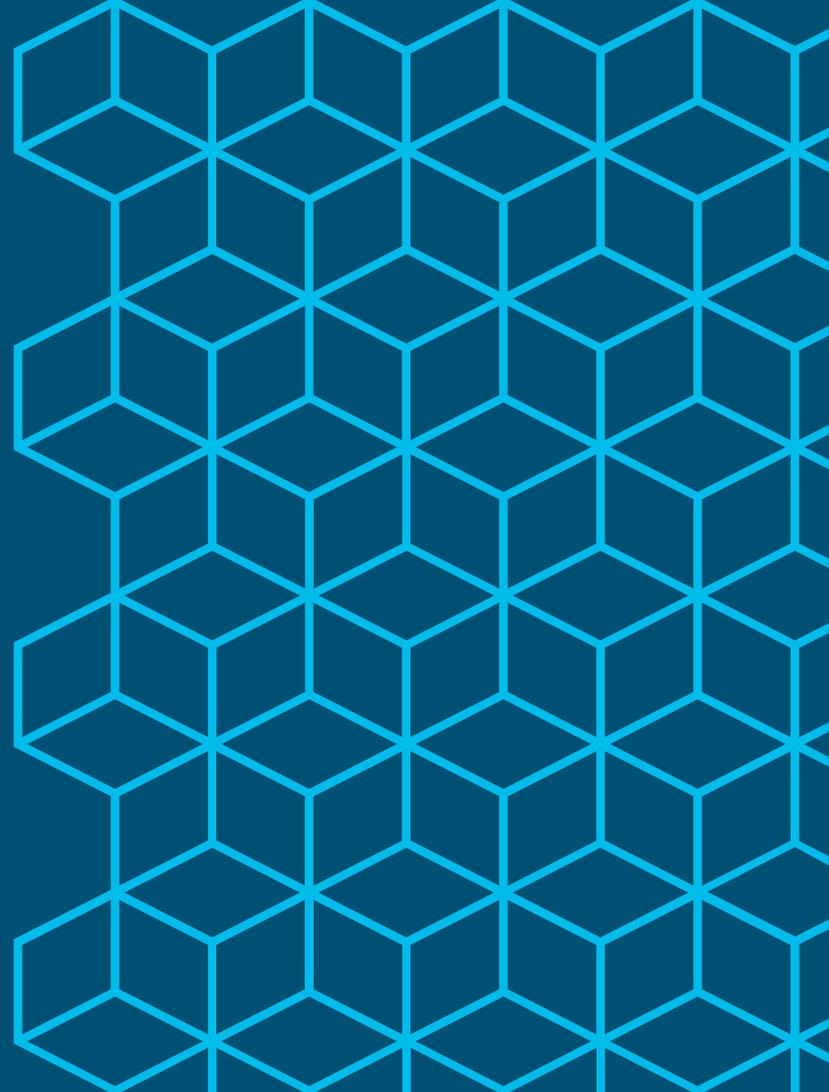
## Is Device Registered in a Trusted System?

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

### Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	MDM_Compliant_alpha	if (EndPoints:LogicalProfile EQUALS MDM_Devices AND Network Access:EapAuthentication EQUALS EAP-TLS AND Airspace:Airspace_Wlan_Id EQUALS 1 AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:DeviceCompliantStatus EQUALS Compliant )	then WLC_SJC19_V602_Q AND SJC19_Wireless_Mobile_Devices

# Methods for Linking Trusted Devices with Trusted Users



# Identifying the Machine AND the USER

## Machine Access Restrictions (MAR)

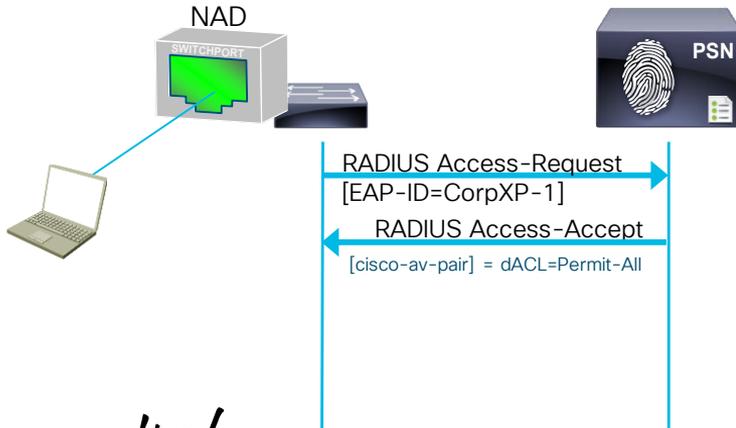
- MAR provides a mechanism for the RADIUS server to search the previous authentications and look for a machine-authentication with the same Calling-Station-ID.
- This means the machine must authenticate before the user.
  - i.e. Must log out, not use hibernate, etc....
- See the reference slides for 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
<b>MachineAuth</b>	<b>if Domain Computers</b>	<b>then</b>	<b>MachineAuth</b>
Employee	if Employee & WasMachineAuthenticated = true	then	Employee
GUEST	if GUEST	then	GUEST
Default	If no matches, then	WEBAUTH	



Matched Rule = MachineAuth

# Machine Access Restrictions (MAR)

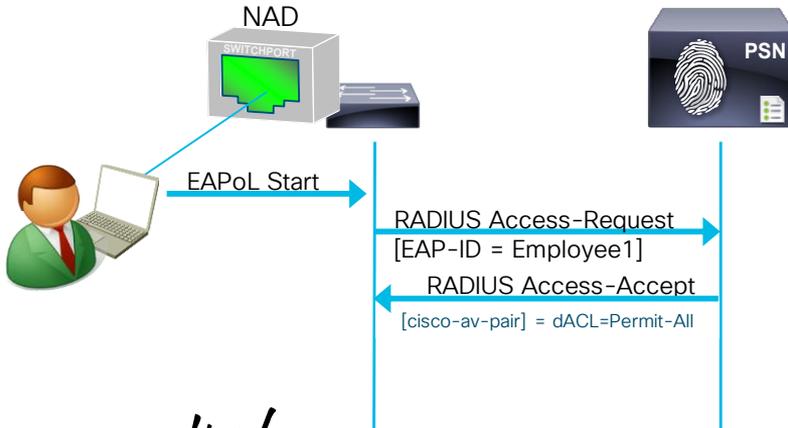
MAR Cache

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
<b>Employee</b>	<b>if Employee &amp; WasMachineAuthenticated = true</b>	<b>then</b>	<b>Employee</b>
GUEST	if GUEST	then	GUEST
Default	If no matches, then	WEBAUTH	



Matched Rule = Employee



# 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

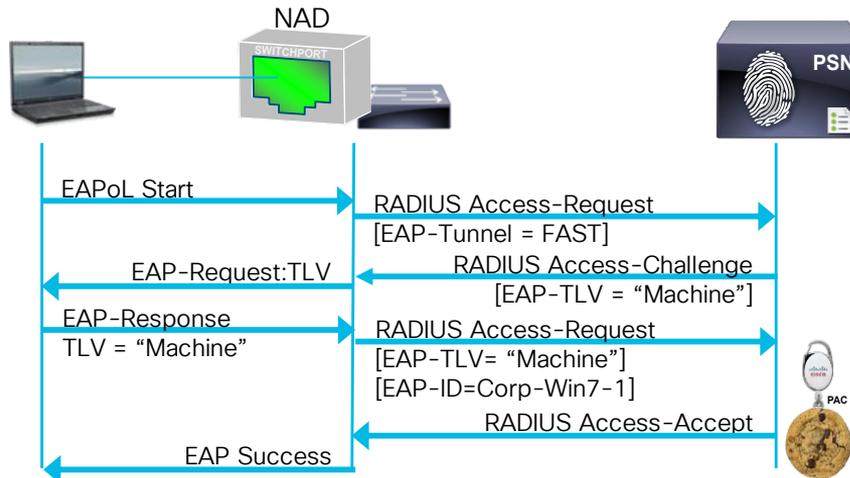
# EAP-Chaining

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
<b>MachineAuth</b>	if <b>Domain Computers</b>	then	<b>MachineAuth</b>
Employee	if Employee & Network Access:EAPChainingResult = User and machine succeeded	then	Employee
GUEST	if GUEST	then	GUEST
Default	If no matches, then	WEBAUTH	



PAC = Protected Access Credentials

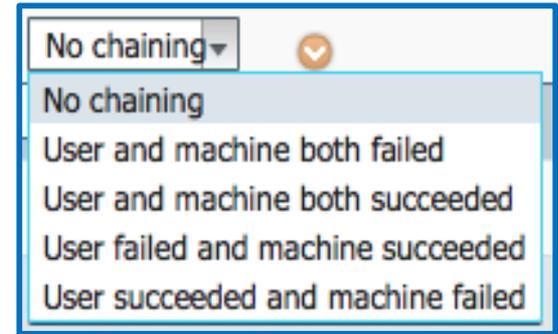
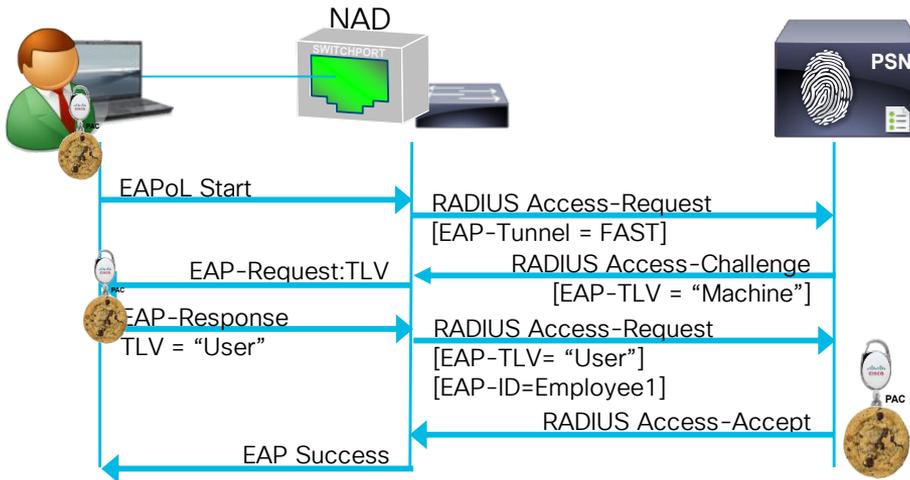
# EAP-Chaining

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 succeeded	then	Employee
GUEST	if GUEST	then	GUEST
Default	If no matches, then	WEBAUTH	



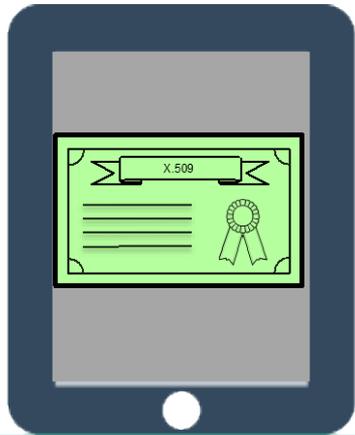
# Identifying the Machine AND the User

## What to do when EAP-Chaining is not Available?

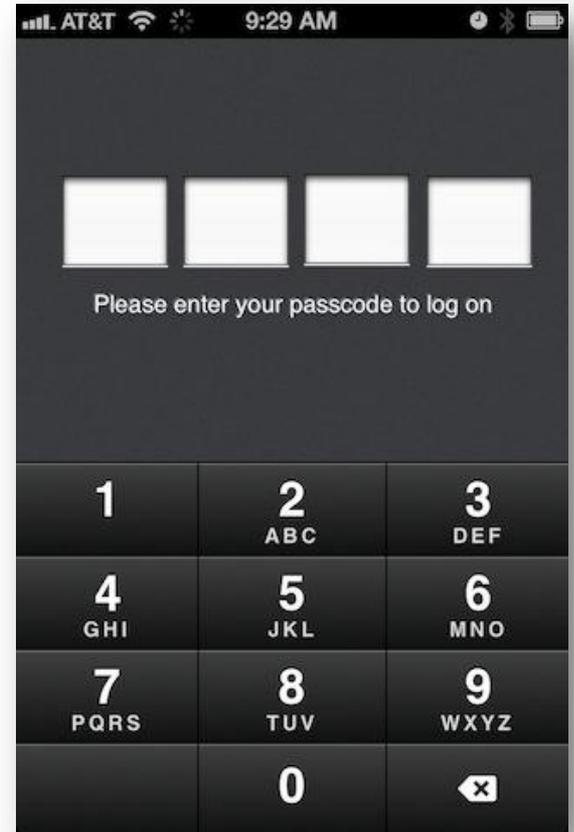
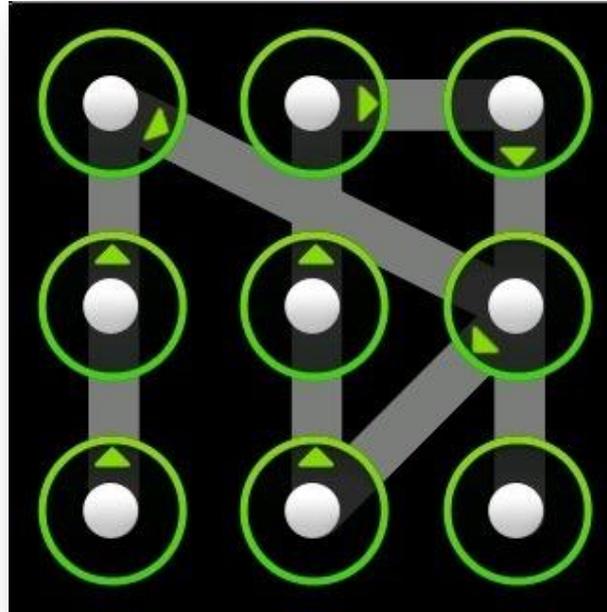
- There are many requirements to determine Machine AND the User
  - Windows is the only current OS that can run EAP-Chaining (with AnyConnect)
  - What about iOS or Android based Tablets?
- Chain together 802.1X with Easy Connect (EZC)
  - Validate the device using machine auth or user-issued certificate
  - 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?



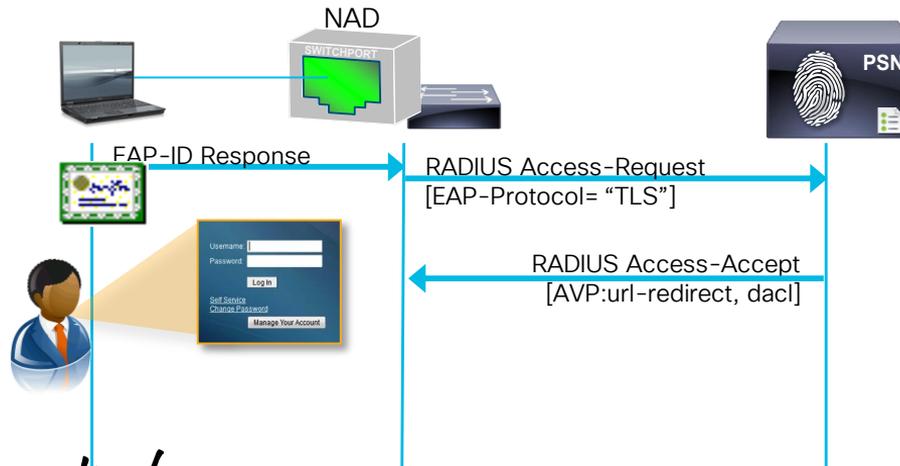
Mobile Device  
w/ Certificate



# 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 <b>Employee &amp; Network Access:</b> EAPAuthentication = EAP-TLS	then CWChain
Default	If no matches, then	WEBAUTH



CN=employee1 || Cert is Valid ✓

## Session Data

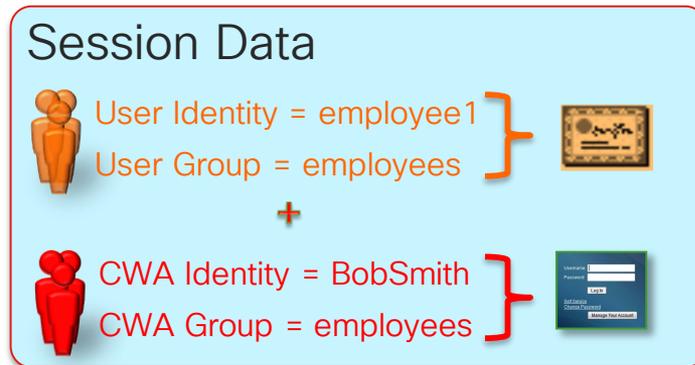
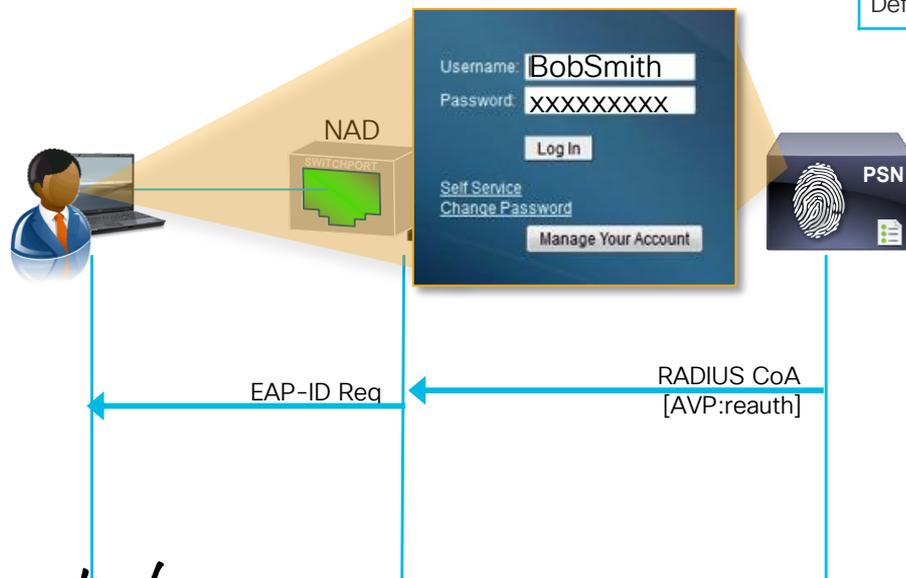
 User Identity = employee1  
 User Group = employees



# 802.1X and CWA Chaining

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

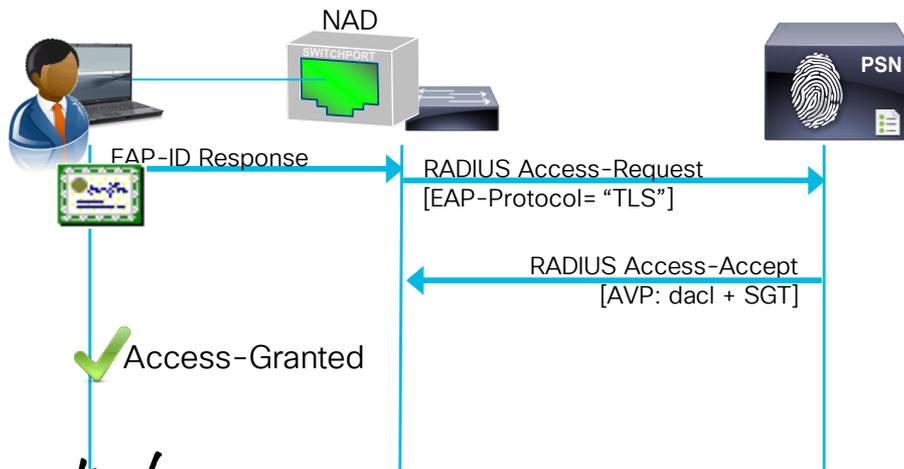
Rule Name	Conditions	Permissions
IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phone
Employee_CWA	if AD:ExternalGroup=Employees AND CWA:CWA_ExternalGroup=Employees	then Employee & SGT
Employee_1X	if Employee & Network Access: EAPAuthentication = EAP-TLS	then CWACHain
Default	If no matches, then	WEBAUTH



# 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 CWChain
Default	If no matches, then	WEBAUTH



CN=employee1 || Cert is Valid ✓

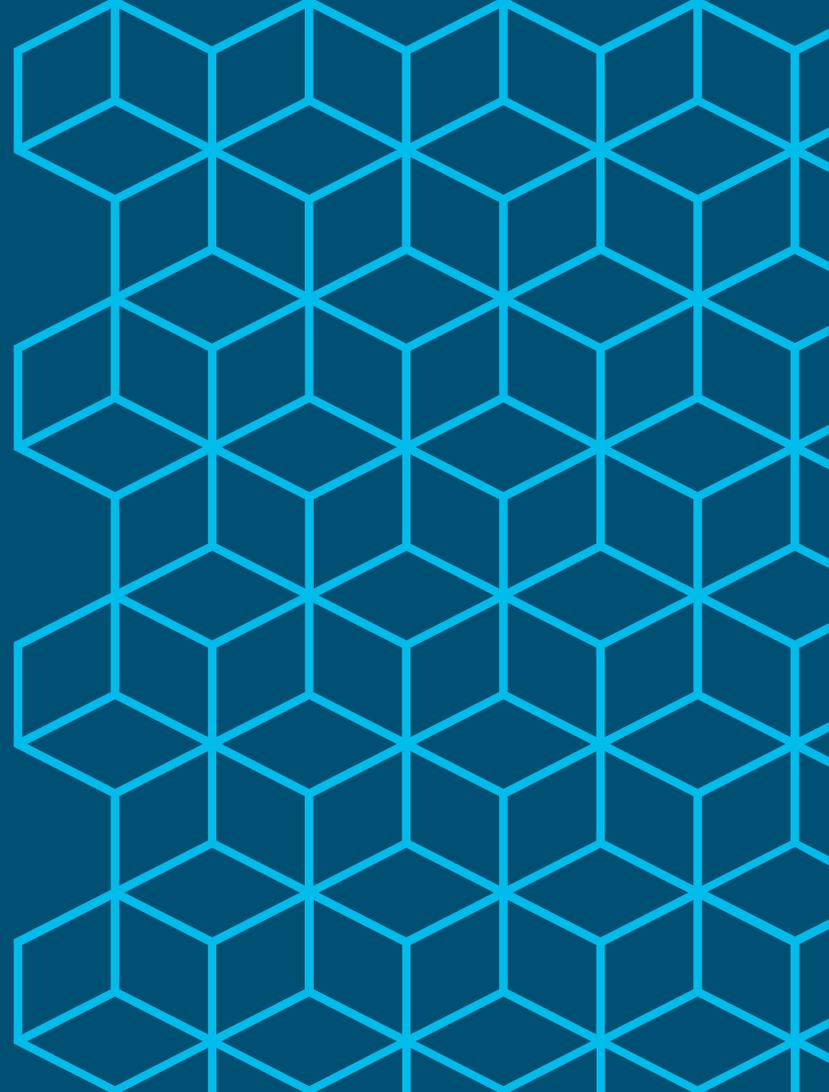
## Session Data

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

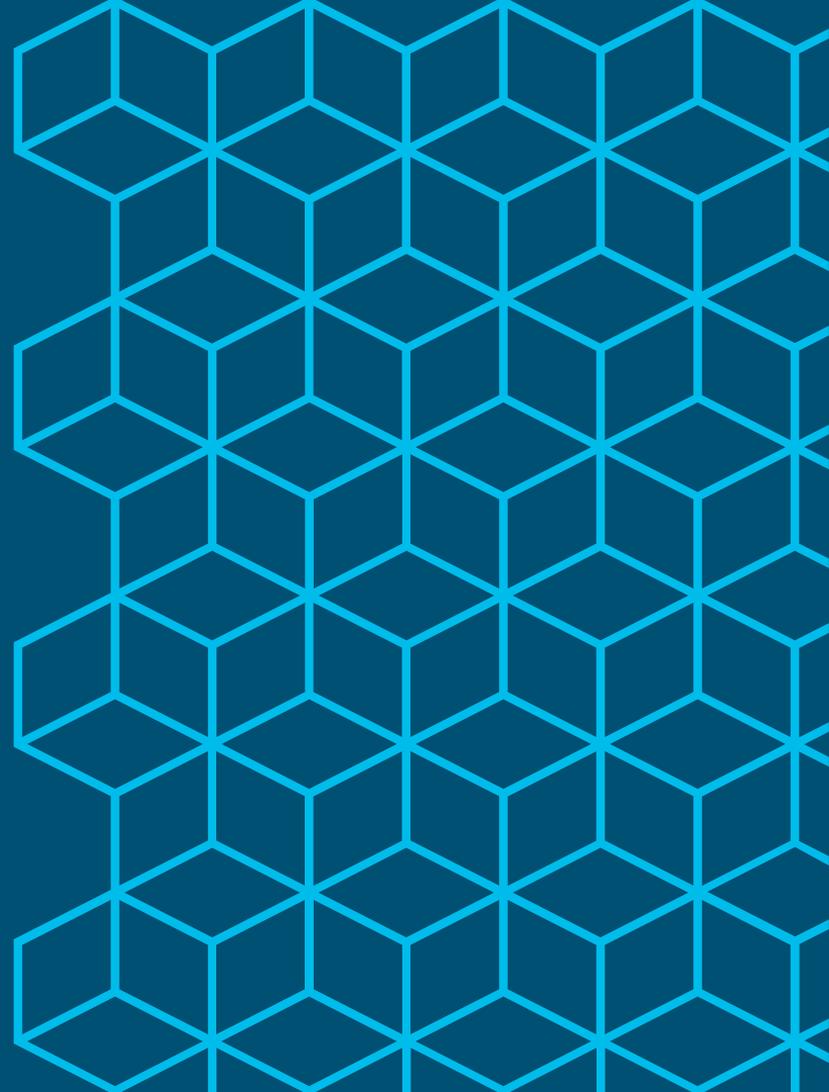
Auth Method	Sample Auth Policy	SGT		
802.1X Machine + User (EAP Chain)	AD_PC_Employee_1X	AD_PC-Employee		
802.1X Machine + EZC (EZC Chain)	AD_PC_Employee_EZC	AD_PC-Employee		
802.1X Machine + CWA (CWA Chain)	AD_PC_Employee_WebAuth	AD_PC-Employee		
802.1X User Auth + EZC (EZC Chain)	Employee_1X_EZConnect	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

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

- INACTIVE ENDPOINTS:** A bar chart showing the number of inactive endpoints over time.
- AUTHENTICATION STATUS:** A donut chart showing the distribution of authentication statuses, with 'connected' at 0.03%.
- NETWORK DEVICES:** A donut chart showing the distribution of network devices by location, with 'locat...land3' at 37.17%.

A central blue callout box highlights the following data points:

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

Below the charts, there are three tables with red boxes highlighting specific columns:

MAC Address	Status	IPv4 Address	Username	Hostname
98:E0:D9:85:E9:B3		10.32.6.157	hnarsana	HNARSANA...
84:38:35:67:4D:C4		10.32.2.119	tting	TTING-M-503Y
8A:3B:60:56:62:E1		10.42.36.95	veena	
B8:E8:56:49:2D:3C		10.32.2.112	smasilam	Saravans...
C8:69:CD:98:36:92		10.32.2.68	mansjain	MANSJAIN-M...
34:36:3B:D1:D6:14		10.32.2.50	rohyadav	ROHYADAV-M...

Authorization Policy	Authorization Profile	Authentication Protocol
Authorization Policy	Authorization Profile	Authentication Protocol
Default	Qualys SGT_3, Qualys...	Lookup
Byod-Dot1x-SJC19	Alpha-Compliant	MSCHAPV2
VPN	VPN PrePosture	PAP_ASCII
Byod-Dot1x-SJC19	Alpha-Compliant	Lookup
Byod-Dot1x-SJC19	Alpha-Compliant	MSCHAPV2
Byod-Dot1x-SJC19	Alpha-Compliant	MSCHAPV2

# Context Visibility

## Admin Personalization

The screenshot displays the Cisco ISE Context Visibility interface. At the top, the navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area is divided into three sections: 'ENDPOINTS', 'ENDPOINT CATEGORIES', and 'NETWORK DEVICES'. Each section contains a donut chart showing the distribution of data. Below these charts is a table of endpoints with columns for MAC Address, Anomalous Behavior, IPv4 Address, Username, Hostname, Location, Endpoint Profile, Description, OUI, and OS Types. The table shows several rows of endpoint data.

Annotations highlight key features:

- Endpoint Classification:** A callout box points to the 'Endpoint Classification' link in the top navigation bar, with the text 'Click to set as default selection'.
- Endpoint Classification Settings:** A callout box points to the 'Endpoint Classification' link in the main navigation bar, with a gear icon for settings.
- Endpoint Classification List:** A callout box points to a list of endpoint categories on the right side of the interface, including Authentication, BYOD, Compliance, Compromised Endpoints, Endpoint Classification, Guest, Vulnerable Endpoints, and Hardware.
- Column Order Settings:** A callout box points to the 'Column order' settings panel on the right, which allows users to drag and drop columns to reorder them and toggle the display of fields.
- Drag and Drop Order:** A callout box points to the 'Drag to order columns' section of the settings panel, with the text 'Drag and Drop order Display/Remove Field'.

# 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.

### Create New View

Name \*

Attribute Categories

Columns \*

- \* Policy Service Node
- \* Portal User
- \* PortalName
- \* PortalUserCreationType
- \* PortalUserGuestSponsor
- \* PortalUserGuestStatus
- \* PortalUserGuestType
- \* PortalUserLocation
- \* PortalUserPhoneNumber
- \* PostureOS
- \* PosturePolicyMatched
- \* PostureStatus
- \* Registration Date
- \* SelectedAuthorizationProfiles
- \* SSID
- \* Static Assignment
- \* Static Group Assignment
- \* Status
- \* Total Certainty Factor
- \* UDID
- \* UpdateTime
- \* User-Fetch-CountryName
- \* User-Fetch-Department
- \* User-Fetch-Job-Title
- \* User-Fetch-LocalityName
- \* User-Fetch-Organizational-Unit
- \* User-Fetch-StateOrProvinceName
- \* User-Fetch-StreetAddress
- \* User-Fetch-Telephone
- \* Username
- \* UserType

Click inside the field to start searching attributes.

Dashlets

- \* Endpoint Classification: Endpoint Categories
- \* Endpoint Classification: Network Devices |
- Compliance: Applications by categories
- Endpoint Classification: Endpoints
- Endpoint Classification: Endpoint Categories

# Help is Only a Click Away!

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Center'. A red circle highlights the top right corner of the interface, containing a search icon, a question mark icon, a play icon, and a settings icon. A magnifying glass is positioned over the 'Total Endpoints' metric, which shows a value of 90715. A search bar at the top right contains the IP address 'b8:c1:11:a7:cf:95'. Below the search bar, a distribution list shows various categories such as 'Authorization Profile (1)', 'Endpoint Profile (1)', 'Identity Group (1)', 'Identity Store (1)', 'Location (1)', 'Network Device (1)', and 'Network Device Type (1)'. Two help menus are overlaid on the interface. The left menu, titled 'Launch page level help', lists various resources including 'ISE Community page', 'ISE on Cisco.com', 'ISE Documentation', 'ISE Software Downloads', 'ISE YouTube Channel', 'ISE Partner Ecosystem', and 'ISE Portal Builder', with an 'Ask a Question' button at the bottom. The right menu, titled 'Account Settings', lists 'Online Help', 'Feedback' (highlighted with a mouse cursor), 'Server Information', 'About Identity Services Engine', and 'Logout'. The background interface shows a 'METRICS' section with 'Total Endpoints' at 90715 and 'Active Endpoints' at 178. A 'Distribution' section shows endpoints ordered by recent activity, with one 'Apple-iPhone' device listed. An 'ALARMS' section is visible at the bottom, showing a table with columns for 'Severity', 'Name', 'Occu...', and 'Last Occurred'.

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Center

Summary Endpoints Alerts Alerts Vulnerability Threat

METRICS

Total Endpoints 90715 Active Endpoints 178

Search b8:c1:11:a7:cf:95

1 Connected 0 Failed 0 Disconnected 1 Total

Distribution Endpoints ordered based on recent activity

- Authorization Profile (1)
  - PermitAccess,Q...
- Endpoint Profile (1)
  - Apple-iPhone (1)
- Identity Group (1)
- Identity Store (1)
- Location (1)
  - All Locations#...
- Network Device (1)
  - sjc19-00a-wlc1 (1)
- Network Device Type (1)

Apple-iPhone

yshchory, B8:C1:11:A7:CF:95, 10.40.130.31

All Locations#..., All Device Typ..., PermitAccess,Q...

ALARMS

Severity	Name	Occu...	Last Occurred
Warning	Profiler SNMP Request ...	1326	1 min ago
Warning	Smart Licensing Id Certi...	583	11 mins ago

Launch page level help

ISE Community page

ISE on Cisco.com

ISE Documentation

ISE Software Downloads

ISE YouTube Channel

ISE Partner Ecosystem

ISE Portal Builder

Ask a Question

Account Settings

Online Help

Feedback

Server Information

About Identity Services Engine

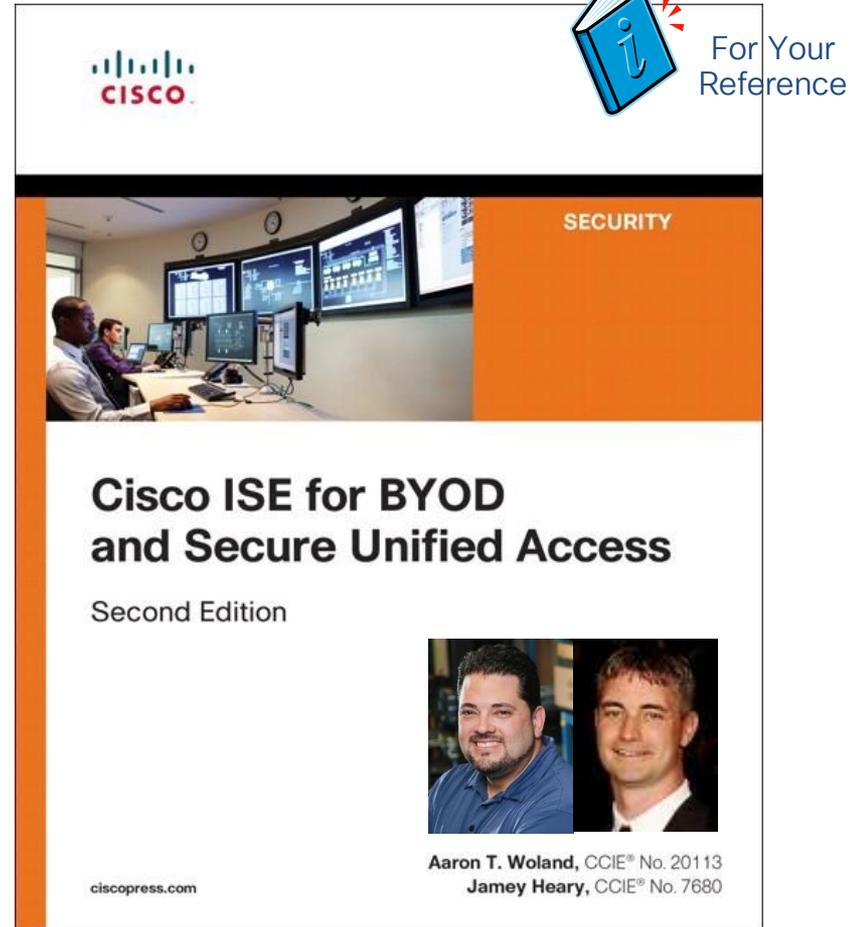
Logout

# 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>





# 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

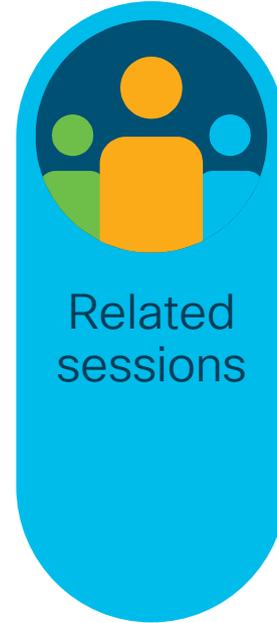
Give us your feedback to be entered into a Daily Survey Drawing.

Complete your session surveys through the Cisco Live mobile app or on [www.CiscoLive.com/us](http://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](http://www.CiscoLive.com/Online).

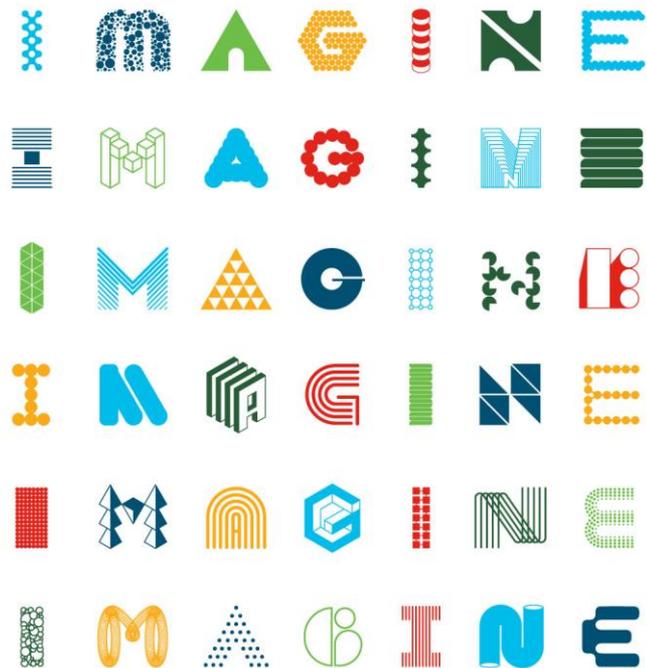


# Continue your education





Thank you



INTUITIVE



INTUITIVE