



Cisco *live!*

6-9 March 2018 • Melbourne, Australia

Designing ISE for Scale & High Availability

Jason Kunst, Technical Marketing Engineer @nacbot

BRKSEC-3699

Cisco Spark

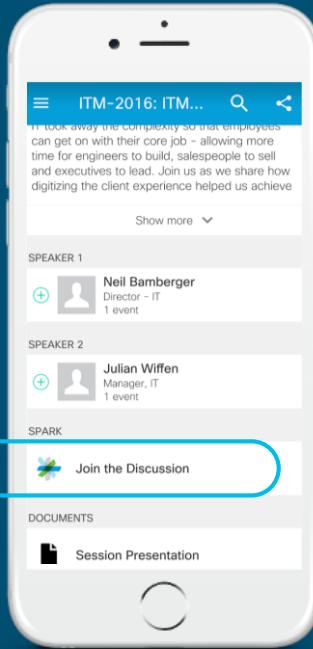


Questions?

Use Cisco Spark to communicate
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion” ——————
3. Install Spark or go directly to the space
4. Enter messages/questions in the space



Session Abstract

Cisco Identity Services Engine (ISE) delivers context-based access control for every endpoint that connects to your network. This session will show you how to design ISE to deliver scalable and highly available access control services for wired, wireless, and VPN from a single campus to a global deployment.

Focus is on design guidance for distributed ISE architectures including high availability for all ISE nodes and their services as well as strategies for survivability and fallback during service outages. Methodologies for increasing scalability and redundancy will be covered such as load distribution with and without load balancers, optimal profiling design, and the use of Anycast.

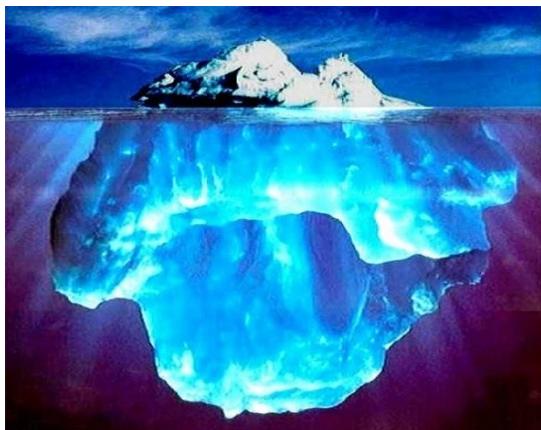
Attendees of this session will gain knowledge on how to best deploy ISE to ensure peak operational performance, stability, and to support large volumes of authentication activity. Various deployment architectures will be discussed including ISE platform selection, sizing, and network placement.

Important: Hidden Slide Alert



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

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



Cisco live!



For Your
Reference

~500 +/- Slides in
Session Reference PDF



Available on ciscolive.com

BRKSEC-3699 - Designi

Documents

- Session Presentation
- Session Reference

View Session

- Session Video

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>

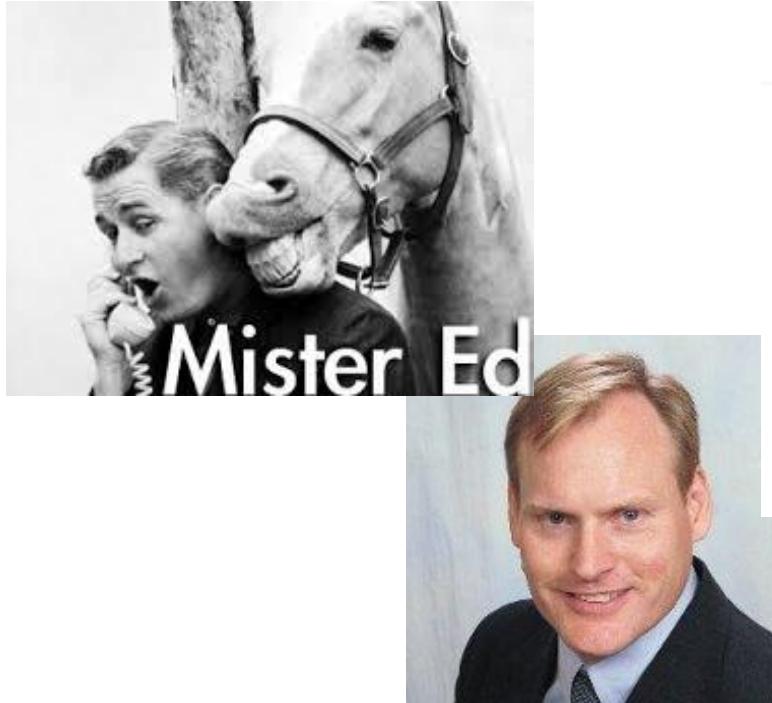
U
P
D
E
S
I
G
N
A
U
T
H
E
R
E
C
T
I
O
N
8
0
2
.1
X
You take the blue pill – the story ends, you walk out of this room and believe whatever you want to believe.

Remember, all I'm offering is the truth – nothing more.

- *The Matrix*, 1999

S
A
Y
O
D
T
R
A
T
I
O
N
I
S
L
I
S
A
N
X
You take the red pill – you stay in this room, and I show you how deep the rabbit hole goes.

From the horses mouth



Cisco live!

On-Demand Library Online Events In-Person Events About Cisco Live Login

Show Favorites Only [Clear All](#)

1 to 10 of 10 results found

Advanced - Designing ISE for Scale & High Availability - BRKSEC-3699	
Event: 2016 Berlin	
Craig Hyps, Principal Technical Marketing Engineer	
Designing ISE for Scale & High Availability - BRKSEC-3699	
Event: 2017 Las Vegas	
Craig Hyps, Principal Technical Marketing Engineer	
Advanced - Designing ISE for Scale & High Availability - BRKSEC-3699	
Event: 2015 Milan	
Craig Hyps, Principal Technical Marketing Engineer	

<https://www.ciscolive.com/global/on-demand-library/?search=hyps#/>

J A S O N K U N S T



Cisco *live!*



Cisco *live!*







Agenda

- Sizing Deployments and Nodes
- Bandwidth and Latency
- Scaling ISE Services
- RADIUS, AD/LDAP, Passive ID, Guest, Web Services, TACACS+
- Profiling and Database Replication
- MnT (Optimise Logging and Noise Suppression)
- High Availability
 - Appliance Redundancy
 - Admin, MnT, and pxGrid Nodes
 - Certificate Services Redundancy
 - PSN Redundancy with and without Load Balancing
 - NAD Fallback and Recovery
- Monitoring Load and System Health

Deployment Models and Sizing

Node Types



- Policy Service Node (PSN)
 - Makes policy decisions
 - RADIUS/TACACS+ server & provides endpoint/user services
- Policy Administration Node (PAN)
 - Interface to configure policies and manage ISE deployment
 - Replication hub for all database config changes
- Monitoring & Troubleshooting Node (MnT)
 - Interface to reporting and logging
 - Destination for syslog from other ISE nodes and optionally NADs
- pxGrid Controller
 - Facilitates sharing of information between network elements

Can run in a single host



Standalone Deployment

All Personas on a Single Node: PAN, PSN, MnT, pxGrid

- Maximum sessions – Platform dependent
 - 5,000 for 3415
 - **7,500 for 3515**
 - 10,000 for 3495
 - **20,000 for 3595**



Policy Administration Node

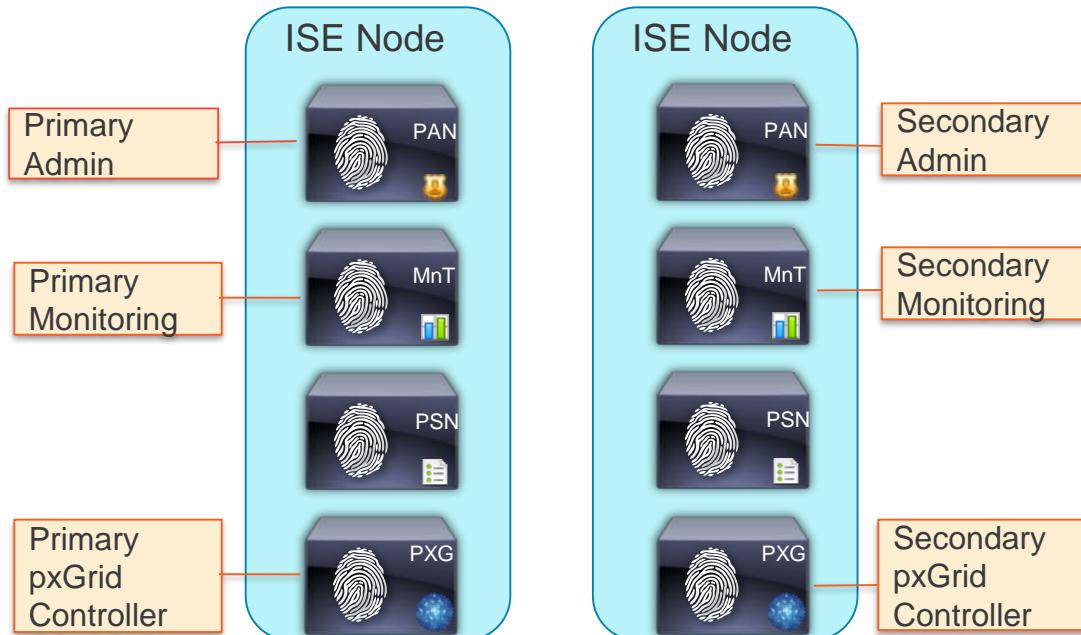
Monitoring and Troubleshooting Node

Policy Service Node

pxGrid Node

Basic 2-Node ISE Deployment (Redundant)

- Maximum sessions— 20,000 (platform dependent—same as standalone)
- Redundant sizing – 20,000 (platform dependent—same as standalone)



Distributed Persona Deployment

Admin + MnT on Same Appliance; Policy Service on Dedicated Appliance

- 2 x Admin+Monitor+pxGRID
- Max 5 PSNs
 - **Optional: Dedicate 2 of the 5 for pxGrid**
- Max sessions – Platform dependent
 - 5,000 for 3415 as PAN+MnT
 - **7,500 for 3515** as PAN+MnT
 - 10,000 for 3495 as PAN+MnT
 - **20,000 for 3595** as PAN+MnT



Distributed Persona Deployment

Dedicated Appliance for Each Persona: Admin, Monitoring, pxGrid, Policy Service

- 2 x Admin and 2 x Monitoring (and up to 4 x pxGrid)
- Max PSNs (Platform dependent)
 - 40 using 3495 as PAN and MnT
 - **50 using 3595** as PAN and MnT
- Max sessions (Platform dependent)
 - 250k using 3495 as PAN and MnT
 - **500k using 3595** as PAN and MnT



Sizing Guidance for ISE Nodes

34xx/35xx Scaling by Deployment/Platform/Persona

ISE 2.1+ Max Concurrent Session Counts by Deployment Model and Platform

Size	Deployment Model	Platform	Max Active Sessions per Deployment	Max # Dedicated PSNs / PXGs	Min # Nodes (no HA) / Max # Nodes (w/ HA)
		3415	5,000	0	1 / 2
		3495	10,000	0	1 / 2
		3515	7,500	0	1 / 2
		3595	20,000	0	1 / 2
		3415 as PAN+MNT	5,000	5 / 2*	2 / 7
		3495 as PAN+MNT	10,000	5 / 2*	2 / 7
		3515 as PAN+MNT	7,500	5 / 2*	2 / 7
		3595 as PAN+MNT	20,000	5 / 2*	2 / 7
 optional		3495 as PAN and MNT	250,000	40 / 2	3 / 44
		3595 as PAN and MNT	500,000	50 / 4	3 / 58
		3595 as PAN and Super MnT	500,000	50 / 4	3 / 58

Scaling per PSN	Platform	Max Sessions per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3415	5,000
	SNS-3495	20,000
	SNS-3515	7,500
	SNS-3595	40,000

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

Policy Service Node Sizing

Physical and Virtual Appliance Guidance

- Max Sessions Per Appliance for Dedicated PSN

Form Factor	Platform Size	Appliance	Maximum Sessions
Physical	Small	SNS-3415	5,000
	Large	SNS-3495	20,000
	Small (New)	SNS-3515	* 7,500
	Large (New)	SNS-3595	* 40,000
Virtual	S/L	VM	*5,000-40,000

* Under ISE 2.0.1, scaling for Small & Large 35x5 appliance same as Small & Large 34x5 appliance.

SNS appliances have unique UDI from manufacturing. If use general UCS appliance, then must deploy as VM

General VM appliance sizing guidance:

- Select physical appliance that meets required persona and scaling requirements
- Configure VM to match or exceed the ISE physical appliance specifications

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 2.2 OVA Template

Summary

- “Eval” OVA for PoC/Lab testing up to 100 Endpoints (no resv)
- All 3xx5 templates reserve CPU and Memory
- If require more custom disk option, then deploy .iso
- Disks up to 2TB supported for greater MnT storage

OVA Template	CPU			Virtual Memory (GB)	Virtual NICs (GB)	Virtual Disk Size	Target Node Type
	# Cores	Clock Rate (GHz)	Total CPU (MHz)				
ISE-2.3.0.x-virtual-eval.ova	2	2.3	4,600	8	4	200GB	EVAL
ISE-2.3.0.x-virtual-SNS3415-[Disk].ova	4	2.0	8,000	16	4	200GB	PSN/PXG
ISE-2.3.0.x-virtual-SNS3495-[Disk].ova	8	2.0	12,000	32	4	600GB	PAN/MnT
ISE-2.3.0.x-virtual-SNS3515-[Disk].ova	6	2.0	16,000	16	6	200GB	PSN/PXG
ISE-2.3.0.x-virtual-SNS3595-[Disk].ova	8	2.0	16,000	64	6	600GB	PAN/MnT
						200GB	PSN/PXG
						1.2TB	PAN/MnT

Example: ISE-2.3.0.298-virtual-200GB-SNS3515.ova

Resource Reservations

ISE Platform Properties

Minimum VM Resource Allocation

Minimum CPU Cores	Minimum RAM	Minimum Disk	Platform Profile
2	4	100 GB	EVAL
4	4	200GB	IBM_SMALL_MEDIUM
4	4	200GB	IBM_LARGE
4	16	200GB	UCS_SMALL
8	32	200GB	UCS_LARGE
12	16	200GB	SNS_3515
16	64	200GB	SNS_3595
16	256	200GB	“Super MnT”

- Least Common Denominator used to set platform.
- Example:
4 cores
32GB RAM
= UCS_SMALL

More to come!

Why Do I Care?

Because memory,
max sessions, and
other table spaces
are based on
Persona and
Platform Profile

ISE 2.2 OVA Templates

Summary

OVA Template	CPU			Virtual Memory (GB)	Virtual NICs (GB)	Virtual Disk Size	Target Node Type
	# Cores	Clock Rate (GHz)	Total CPU (MHz)				
ISE-2.3.0.x-virtual-eval.ova	2	2.3	4,600	8	4	200GB	EVAL
ISE-2.3.0.x-virtual-SNS3415-[Disk].ova	4	2.0	8,000	16	4	200GB	PSN/PXG
						600GB	PAN/MnT
ISE-2.3.0.x-virtual-SNS3495-[Disk].ova	8	2.0	12,000	32	4	200GB	PSN/PXG
						600GB	PAN/MnT
ISE-2.3.0.x-virtual-SNS3515-[Disk].ova	6	2.0	16,000	16	6	200GB	PSN/PXG
						600GB	PAN/MnT
ISE-2.3.0.x-virtual-SNS3595-[Disk].ova	8	2.0	16,000	64	6	200GB	PSN/PXG
						1.2TB	PAN/MnT

ISE Platform Properties

Minimum VM Resource Allocation

Minimum CPU Cores	Minimum RAM	Minimum Disk	Platform Profile
2	4	100 GB	EVAL
4	4	200GB	IBM_SMALL_MEDIUM
4	4	200GB	IBM_LARGE
4	16	200GB	UCS_SMALL
8	32	200GB	UCS_LARGE
12	16	200GB	SNS_3515
16	64	200GB	SNS_3595
16	256	200GB	“Super MnT”

- Least Common Denominator used to set platform.
- Example:
4 cores
32GB RAM
= UCS_SMALL

Assumes
HyperThreading
Enabled

ISE 2.2 OVA Templates

Summary

OVA Template	CPU			Virtual Memory (GB)	Virtual NICs (GB)	Virtual Disk Size	Target Node Type
	# Cores	Clock Rate (GHz)	Total CPU (MHz)				
ISE-2.3.0.x-virtual-eval.ova	2	2.3	4,600				
ISE-2.3.0.x-virtual-SNS3415-[Disk].ova	4	2.0	8,000				
ISE-2.3.0.x-virtual-SNS3495-[Disk].ova	8	2.0	12,000				
ISE-2.3.0.x-virtual-SNS3515-[Disk].ova	8	2.0	16,000				
ISE-2.3.0.x-virtual-SNS3595-[Disk].ova	8	2.0	16,000				

For 35x5 ISE VMs,
HyperThreading is
Mandatory, unless
you double (\$\$) the
physical cores
allocated to VM !!

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

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 NSFAdminServiceFact
```

```
UCS_SMALL
```

- 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 ⓘ

Attribute	Value	Operator	Value
Server	ise22-pan1	Is exactly (or equals)	
Time Range	Today	Is exactly (or equals)	

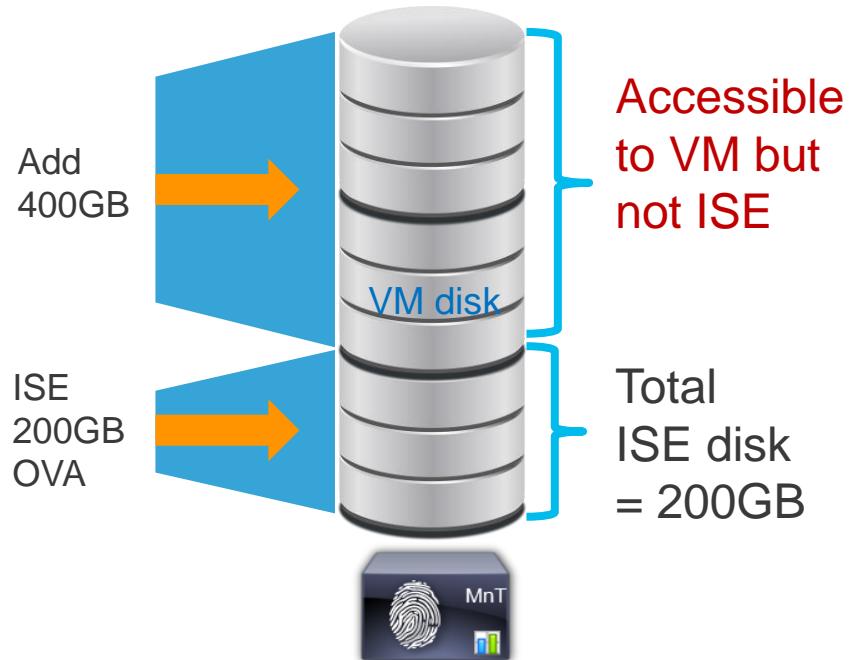
Counter Attribute Threshold

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

VM Disk Allocation

CSCvc57684 Incorrect MnT allocations if setup with VM disk resized to larger without ISO re-image

- ISE OVAs prior to ISE 2.2 sized to 200GB. Often sufficient for PSNs or pxGrid nodes but not MnT.
- Misconception: Just get bigger tank and ISE will grow into it!
- No auto-resize of ISE partitions when disk space added after initial software install
- Requires re-image using .iso
- Alternatively: Start with larger OVA (ISE 2.2)



ISE 2.4 MnT -- Fast Access to Logs and Reports

Screenshot of the Cisco Identity Services Engine (ISE) 2.4 Management Navigation (MnT) interface, showing live logs and repeat counts.

Top Navigation:

- Home, Context Visibility, Operations, Policy, Administration, Work Centers
- License Warning (2 notifications)
- Search and settings icons

Sub-Menu:

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

Live Logs Tab:

- Misconfigured Suplicants: 0
- Misconfigured Network Devices: 0
- RADIUS Drops: 2880
- Client Stopped Responding: 480
- Repeat Counter: 0

Filter Options:

- Refresh: Never
- Show: Latest 50 records
- Within: Last 30 minutes

Data Table:

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Id...
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
Jan 26, 2018 11:05:11.995 AM	✗	○		vani	AC:BC:32:AC:7E:23								Wo...
Jan 26, 2018 11:04:54.173 AM	●	○	0	kusenapa	DC:EF:CA:4D:41:1F	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_El_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_El_C...	Location_BX...	Location_BX...	Guest_Redir...				sampg-bxb22-0...
Jan 26, 2018 11:04:10.882 AM	✗	○		INVALID			Building_SJ...	Building_SJ...					Wo...
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			

Introducing “Super” MnT

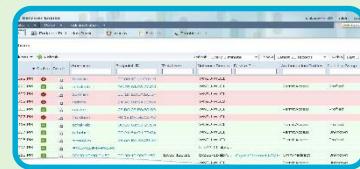
For Any Deployment where High-Perf MnT Operations Required

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



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

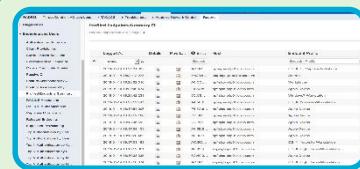
ISE 2.4 MnT Vertical Scaling Scaling Enhancements



Faster Live Log Access

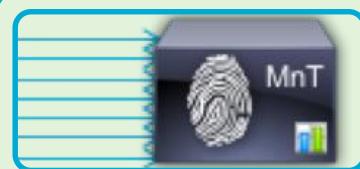
- Run session directory tables from pinned memory
- Tables optimised for faster queries

Benefits MnT
on ALL ISE
platforms



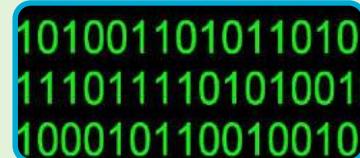
Faster Report & Export Performance

- Report related tables pinned into memory for faster retrieval.
- Optimise tables based on platform capabilities.



Collector Throughput improvement

- Added Multithreaded processing capability to collector.
- Increased collector socket buffer size to avoid packet drops.



Major Data Reduction

- Remove detailed BLOB data > 7 days old (beyond 2.3 reductions)
- Database optimisations resulting in up to 80% efficiencies

Flash Removal

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!



MnT Node Log Storage Requirements for RADIUS

Days Retention Based on # Endpoints and Disk Size (ISE 2.2+)

Total Disk Space Allocated to MnT Node

	200 GB	400 GB	600 GB	1024 GB	2048 GB
Total Endpoints	504	1007	1510	2577	5154
5,000	504	1007	1510	2577	5154
10,000	252	504	755	1289	2577
25,000	101	202	302	516	1031
50,000	51	101	151	258	516
100,000	26	51	76	129	258
150,000	17	34	51	86	172
200,000	13	26	38	65	129
250,000	11	21	31	52	104
500,000	6	11	16	26	52

ISE 2.2 = 50% days increase over 2.0/2.1

ISE 2.3 = 25-33% increase over 2.2

ISE 2.4 = 40-60% increase over 2.2

Assumptions:

- 10+ auths/day per endpoint
- Log suppression enabled

Based on 60% allocation of MnT disk to RADIUS logging
(Prior to ISE 2.2, only 30% allocations)

RADIUS and TACACS+

MnT Log Allocation

ISE 2.2+

- Administration > System > Maintenance > Operational Data Purging

Database Utilization

The diagram illustrates the total log allocation across three categories: RADIUS, T+, and 80% Purge. A cursor points to the RADIUS section, which is highlighted in blue. Below the diagram, a database icon is shown with the text 'ise22-pan1.cts.local' and '384 GB'.

Total Log Allocation

RADIUS T+ 80% Purge

ise22-pan1.cts.local
384 GB

Data Retention Period

	Days
RADIUS	30
TACACS	30

Default Retention reduced from 90 -> 30 days

M&T_PRIMARY
Radius : 67 GB
Days : 24

Enable Export Repository
datastore2

[Create Repository](#)

Encryption Key
.....

Save Reset

- 60% total disk allocated to both RADIUS and TACACS+ for logging (Previously fixed at 30% and 20%)
- Purge @ 80% (First In-First Out)
- Optional archive of CSV to repository

Purge data Now

Purge all data

Purge data older than 90 Days

RADIUS

TACACS

Purge

ISE VM Provisioning & Disk IO Guidance

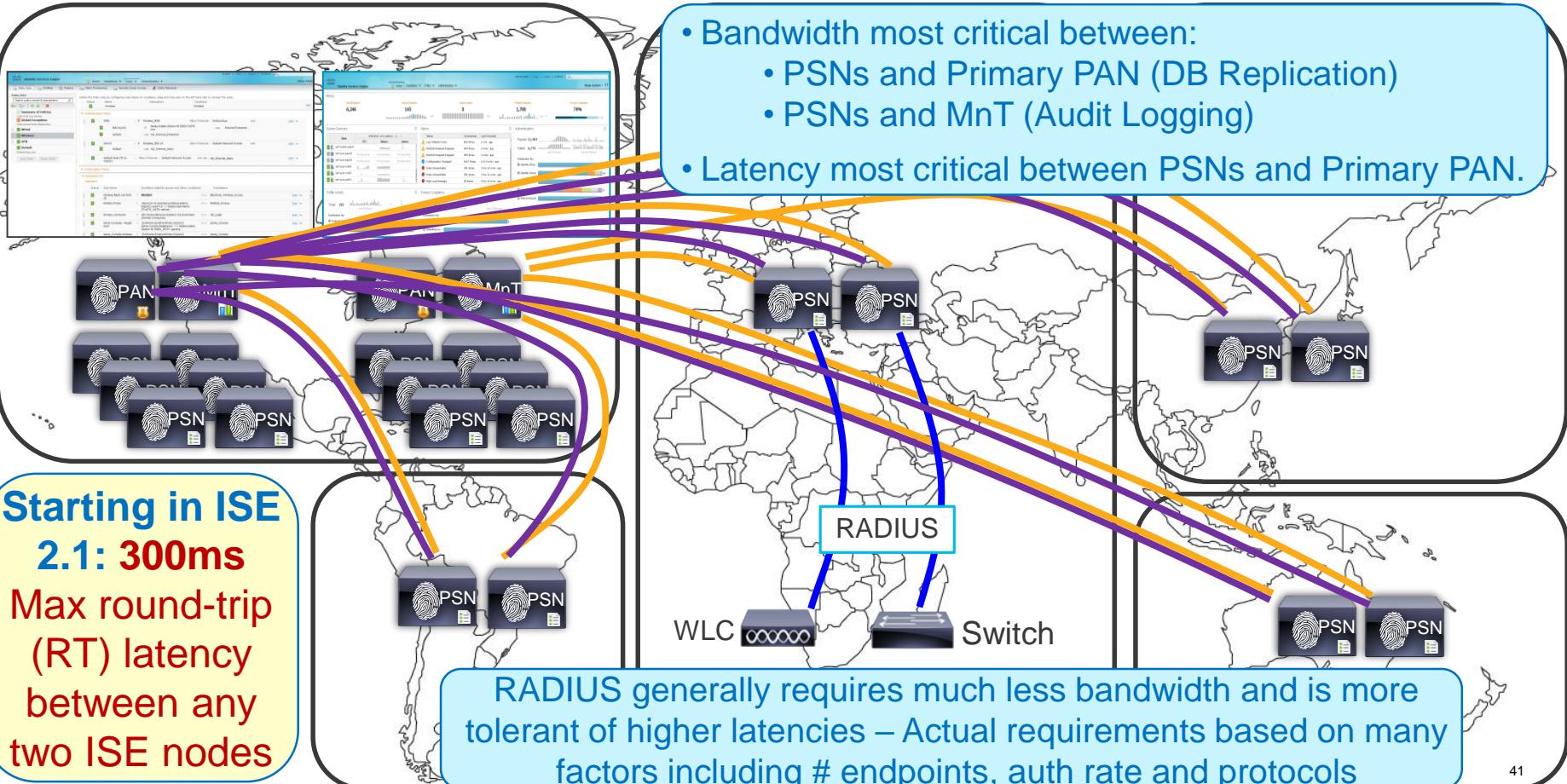
- VMotion supported but storage VMotion not tested.
- Thin Provisioning supported (recommend Thick Provisioning for MnT)
- Hyper-Threading is **mandatory** for 3595-based VMs (Sizing assumes HT enabled, but HT does not double # physical cores! Reservations based on physical cores)
- IO Performance Requirements:
 - Read 300+ MB/sec
 - Write 50+ MB/sec
- Recommended disk/controller:
 - 10k RPM+ disk drives
 - Supercharge with SSD !
 - Caching RAID Controller
 - RAID mirroring
 - Slower writes using RAID 5*

- No specific storage media and file system restrictions. For example, VMFS is not required and NFS allowed *provided* storage is supported by VMware and meets ISE IO performance requirements.
- Customers with VMware expertise may choose to disable resource reservations and over-subscribe, but do so at own risk.

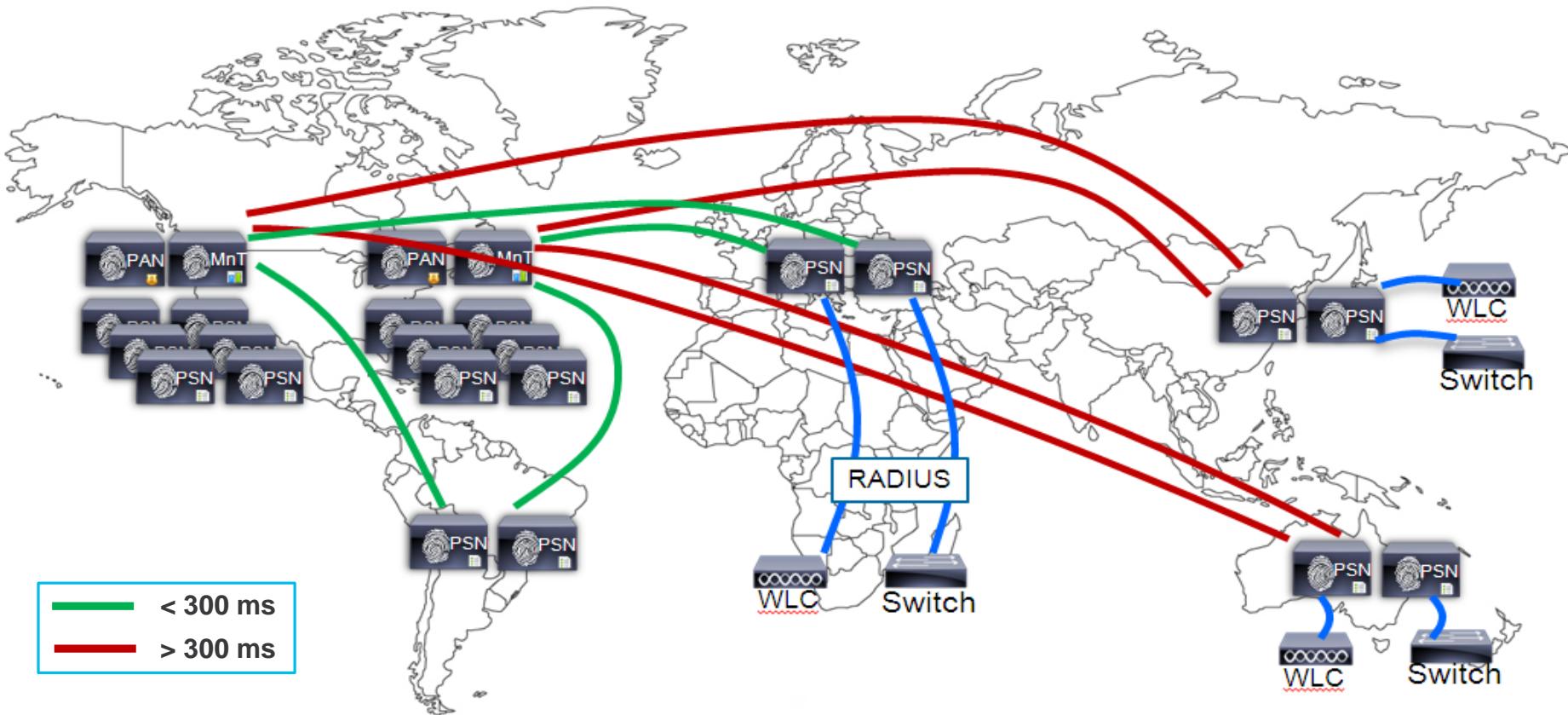
*RAID performance levels: <http://www.datarecovery.net/articles/raid-level-comparison.html>
<http://docs.oracle.com/cd/E19658-01/820-4708-13/appendixa.html>

Bandwidth and Latency

Bandwidth and Latency

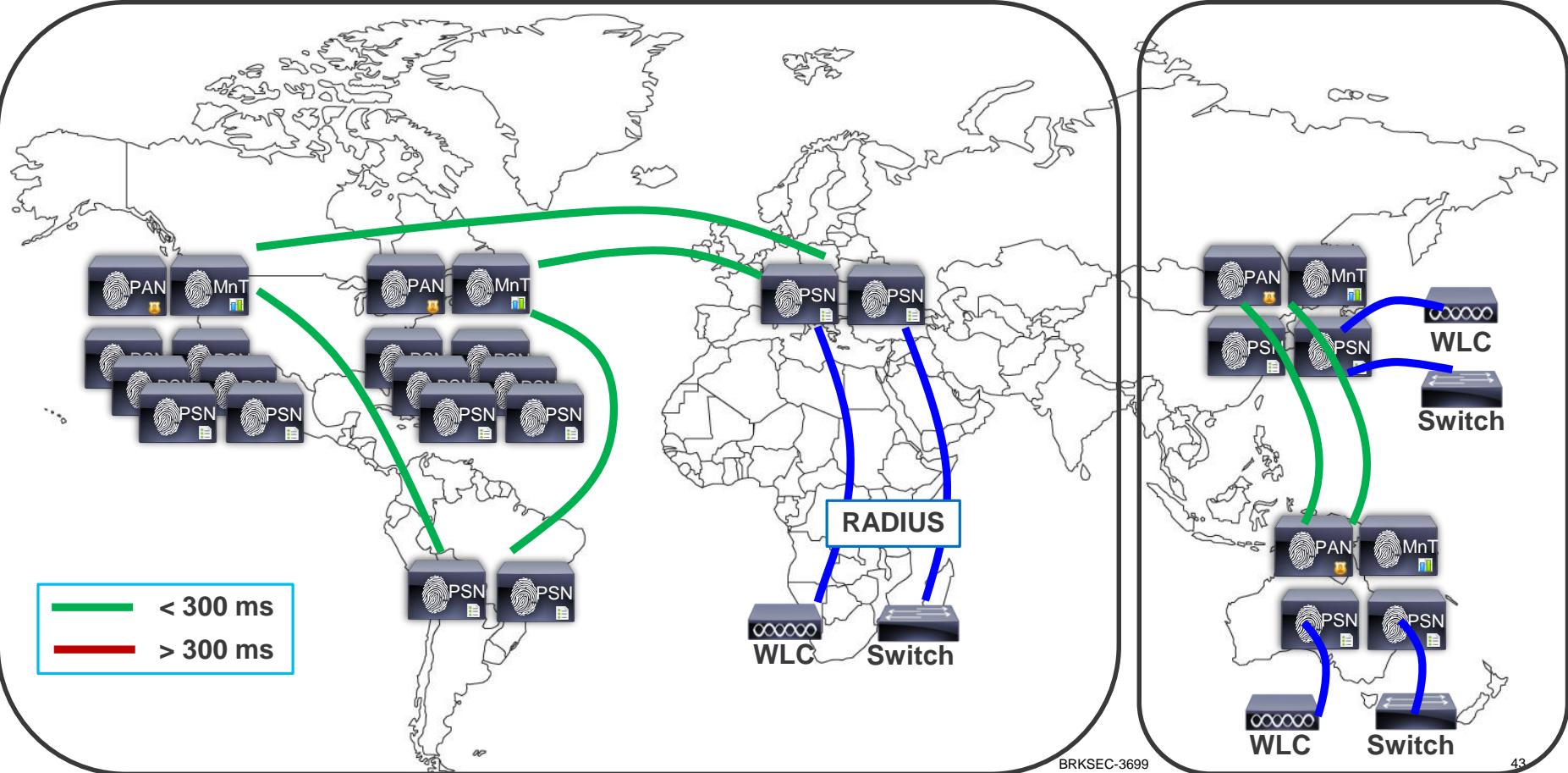


What if Distributed PSNs > 300ms RTT Latency?



Option #1: Deploy Separate ISE Instances

Per-Instance Latency < 300ms



Scaling ISE Services

Scaling ISE Services Agenda

- AAA and Auth Policy Tuning
- Active Directory and LDAP Integration
- Passive Identity and Easy Connect
- Guest and Web Authentication and Location Services
- Compliance Services—Posture and MDM
- TACACS+ Design and Scaling
- Profiling and Database Replication
- MnT (Optimise Logging and Noise Suppression)

ISE Personas and Services

Enable Only What Is Needed !!

- ISE Personas:

- PAN
- MNT
- PSN
- pxGrid

- PSN Services

- Session
- Profiling
- TC-NAC
- ISE SXP
- Device Admin (TACACS+)
- Passive Identity (Easy Connect)

Session Services includes base user services such as RADIUS, Guest, Posture, MDM, BYOD/CA

Personas

Role: SECONDARY

Role: SECONDARY Other Monitoring Node: []

Include Node in Network: []

Use Interface: GigabitEthernet1/0/1

pxGrid

Administration

Monitoring

Policy Service

Enable Session Services

Enable Profiling Service

Enable Threat Centric NAC Service

Enable SXP Service

Enable Device Admin Service

Enable Passive Identity Service

Avoid unnecessary overload of PSN services

Some services should be dedicated to one or more PSNs

Auth Policy Optimisation (ISE 2.2 and Earlier)

Leverage Policy Sets to Organise and Scale Policy Processing

CISCO Identity Services Engine

ise-pan2 | admin | Logout | Feedback | O

Setup Assistant

Policy Sets

Search policy names & descriptions.

+ - X

Summary of Policies
A list of all your policies

Global Exceptions
Rules across entire deployment

Wired

Wireless (highlighted)

VPN

Default
Default Policy Set

Save Order Reset Order

Policy Set Condition

Status Name
Wireless

on the left hand side to change the order.

Conditions Wireless

Edit

Authentication Policy

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)

MAB : If Wireless_MAB
Allow Protocols : Ho
MACwLWA : If Radius:Called-Station-ID ENDS WITH lwa
Default : use AD_Internal_Endpoints

Dot1X : If Wireless_802.1X
Allow Protocols : De
Default : use AD_Internal_Users

Default Rule (If no match) : Allow Protocols : Default Network Access and use : AD_Internal_Users

Edit |

Authorization Policy

Authorisation

Exceptions (0)

Standard

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

Administration > System > Settings > Policy Sets

Policy Sets

Standard Equipment under new ISE 2.3 Policy User Interface

- No Authentication Outer Rule – Now part of Policy Set



Screenshot of the Cisco Identity Services Engine (ISE) 2.3 Policy User Interface showing the Policy Sets page.

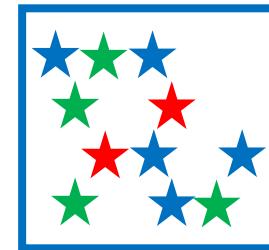
The interface includes a top navigation bar with tabs: Home, Context Visibility, Operations, Policy, Administration, Work Centers, License Warning, and various icons.

The main content area shows a table of Policy Sets:

Policy Set Name	Description	Conditions	Policy Set Condition	Allowed Protocol or RADIUS Proxy	Hit Counts
Wired	Wired Network Access	Radius-NAS-Port-Type EQUALS Ethernet	Default Network Access	23456	
Wireless	Wireless Network Access	Radius-NAS-Port-Type EQUALS Wireless - IEEE 802.11	Default Network Access	0	
VPN	VPN Network Access	Radius-NAS-Port-Type EQUALS Virtual	Default Network Access	0	
Default	Default policy set		Default Network Access	0	

Search Speed Test

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



Auth Policy Optimisation

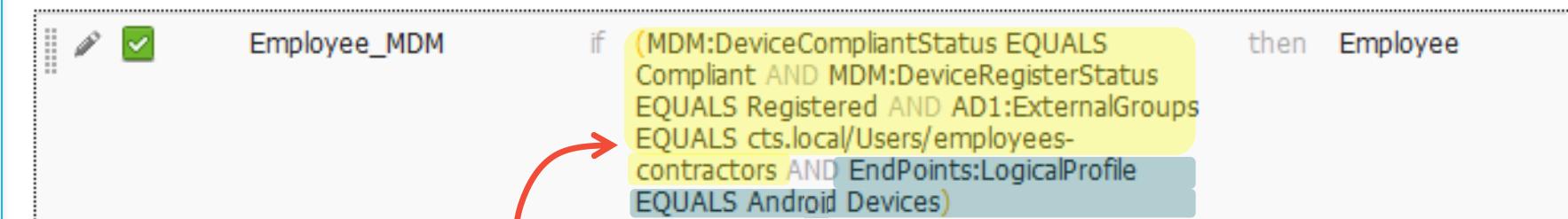
Avoid Unnecessary External Store Lookups

▼ Authorization Policy

► Exceptions (0)

Standard

- 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 Optimisation

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
	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
	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

Screenshot of the Cisco Identity Services Engine (ISE) 2.3 interface showing the configuration of an authentication policy.

The main navigation bar includes Home, Context Visibility, Operations, Policy, Administration, Work Centers, and License Warning.

The current view is under Policy Sets > Set view.

Policy Set Condition: A purple box highlights the "Policy Set Condition" section.

Authentication: A blue box highlights the "Authentication" tab.

Authorisation: An orange box highlights the "Authorisation" tab.

Conditions: The conditions section shows a complex logical expression:

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

Results: Shows a single rule: PermitAccess for Employees.

BRKSEC-3699

Auth Policy

ISE 2.3 Example

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets Set view

Status Policy Set Name Search

Policy Set Condition

Allowed Protocols / Server Sequence Hits

Default Network Access

Security Groups Hits Actions

Employees 0

Select from list 0

55

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

EndPoints-EndPointPolicy STARTS_WITH Windows7

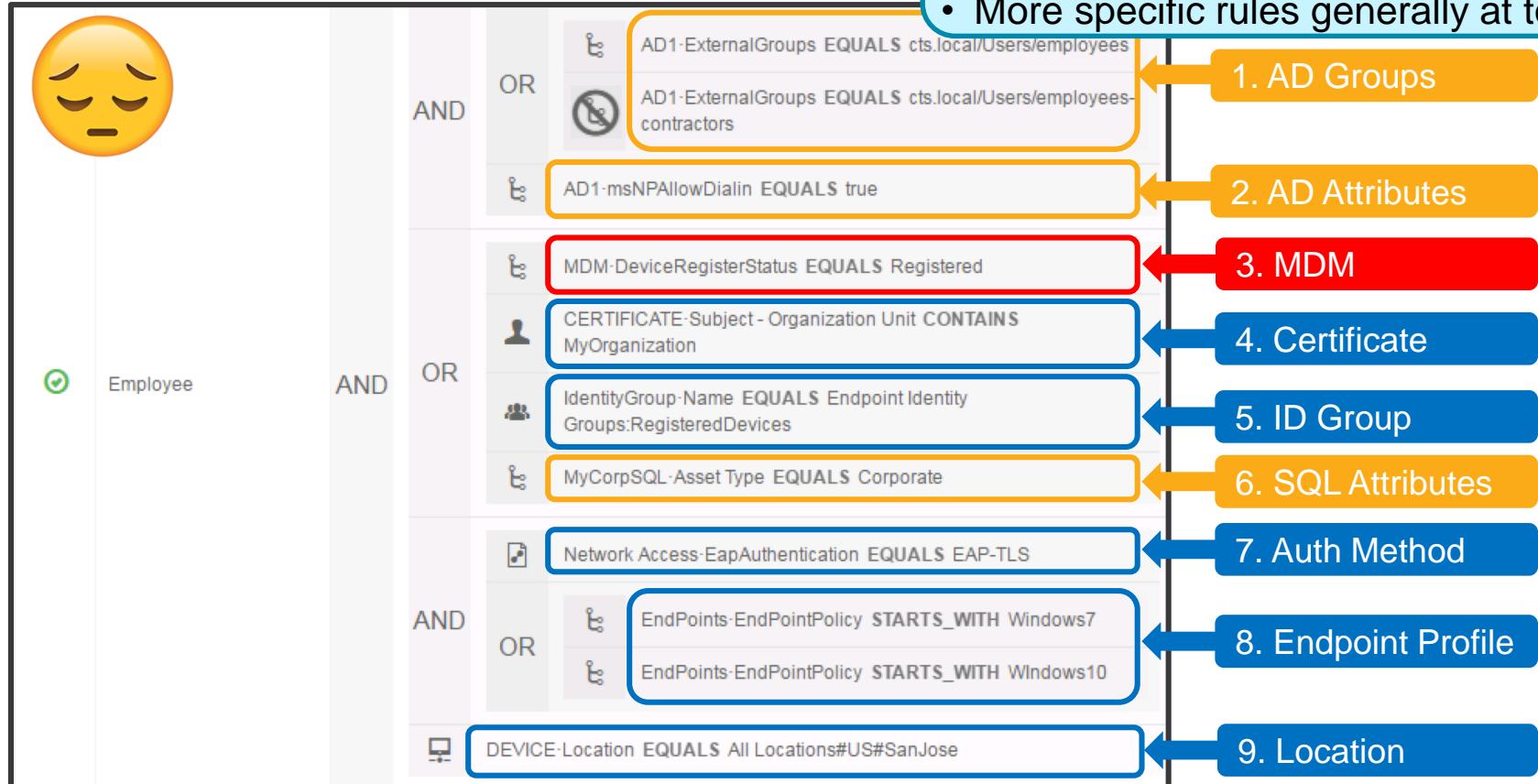
EndPoints-EndPointPolicy STARTS_WITH Windows10

DEVICE-Location EQUALS All Locations#US#SanJose

Auth Policy Optimisation

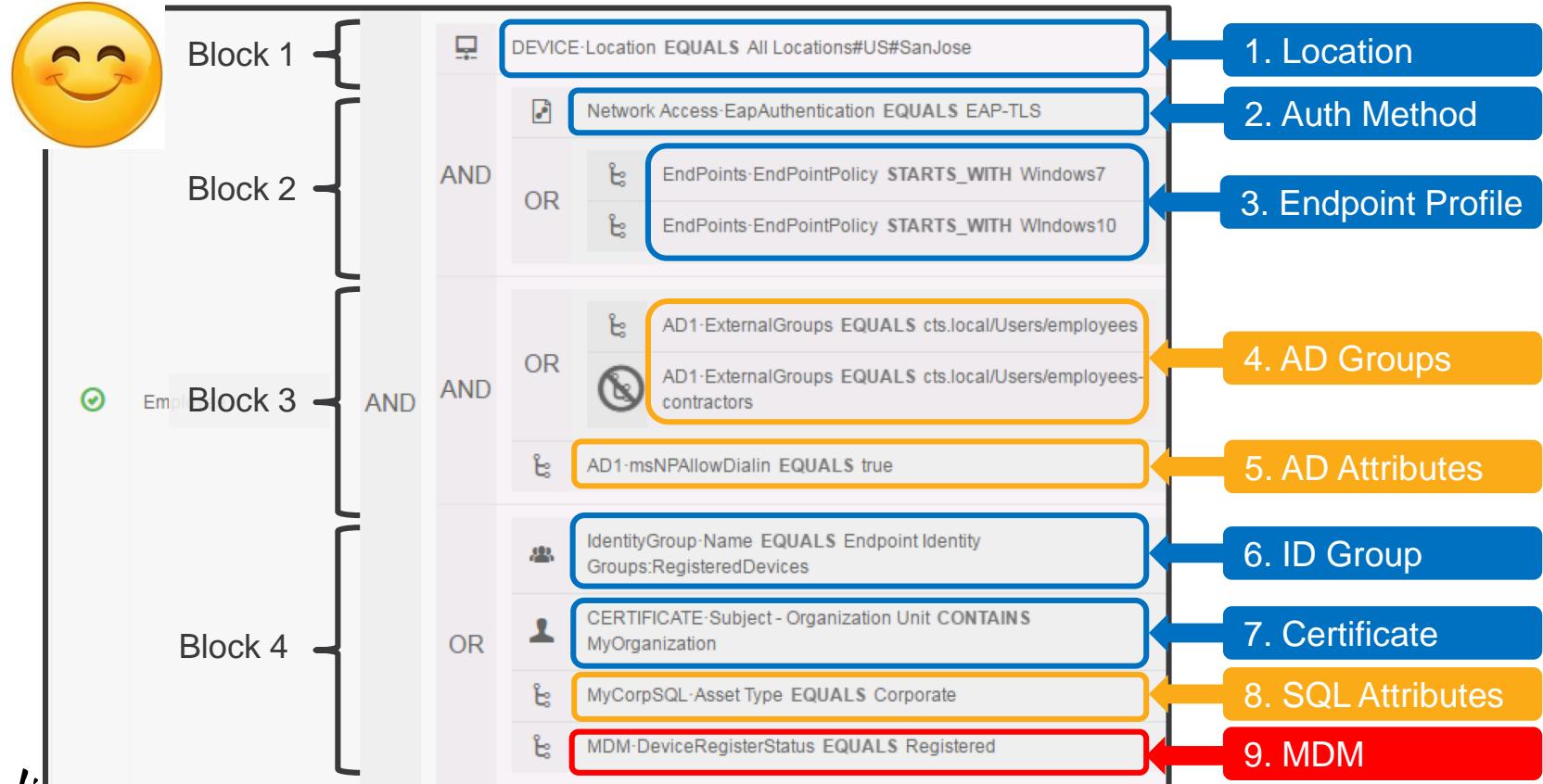
ISE 2.3 Bad Example

- Policy Logic:
 - First Match, Top Down
 - Skip Rule on first negative match
- More specific rules generally at top



Auth Policy Optimisation

ISE 2.3 Better Example!



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 Authorisation Rules = **3000**
(up from 700 in 2.2; up from 600 in 2.1)
- Max Authorisation Profiles = **3200**
(up from 1000 in 2.2; up from 600 in 2.1)



Dynamic Variable Substitution - Example

Populate Internal / External User

Network Access Users List > New Network Access User

Network Access User

* Name: jsmith

Status: Enabled

Email: jsmith@company.com

Internal User:
Update via Import or ERS API

Passwords

Password Type: Internal Users

Account Disable Policy

Disable account if date exceeds: 2017-06-28 (yyyy-mm-dd)

User Custom Attributes

User_IP	= 192.168.200.185	(IPv4 or IPv6 Address)
* User_VLAN	= 100	
User_Start_Date	= 2017-01-01	(yyyy-MM-dd)
Is_User_Temp_Employee	= FALSE	
* User_dACL	= Employee-ACL	

User Groups

Employee

External User:
AD / LDAP / SQL / OTP

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: Cleveland

State/province:

Zip/Postal Code: Employee-ACL Employee-ACL

Country/region:

OK | Cancel | Apply | Help

Dynamic DACLs in Authorisation Profile

Per-User Policy in 1 rule

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

Cisco

Internal User example

External User example

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: i

Passive Identity Tracking: i

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

Enable EAP Session Resume / Fast Reconnect

Major performance boost, but not complete auth so avoid excessive timeout value

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation bar includes Home, Operations, Policy, Guest Access, Administration, Work Centers, System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Identity M, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings.

The left sidebar lists Client Provisioning, FIPS Mode, Alarm Settings, Posture, Profiling, and Protocols (EAP-FAST, EAP-TLS, PEAP, EAP-TTLS, RADIUS). The EAP-TLS section is highlighted with a red box.

The main content area displays the "EAP TLS Settings" page. It includes fields for "Enable EAP TLS Session Resume" (checked), "EAP TLS Session Timeout" (set to 7,200 seconds), and "Cache TLS (TLS Handshake Only/Skip Cert)".

The "PEAP Settings" section shows "Enable PEAP Session Resume" (checked), "PEAP Session Timeout" (set to 7,200 seconds), and "Enable Fast Reconnect" (checked). A blue box highlights the "Cache TLS session" and "Skip inner method" options.

A note in a red box states: "Note: Both Server and Client must be configured for Fast Reconnect".

At the bottom right, a configuration box for "Select Authentication Method: Win 7 Supplicant" includes "Enable Fast Reconnect" (checked), "Enforce Network Access Protection" (unchecked), and "Disconnect if server does not present cryptobinding TLV" (unchecked).

Buttons at the bottom include Save, Reset, and Configure... .

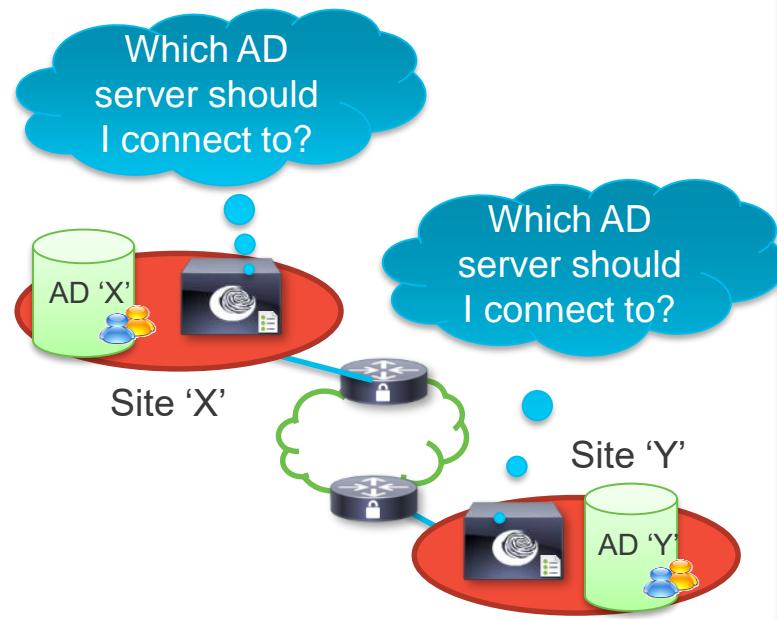
Scaling AD and LDAP Integration

Scaling AD Integration w/ Sites & Services

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

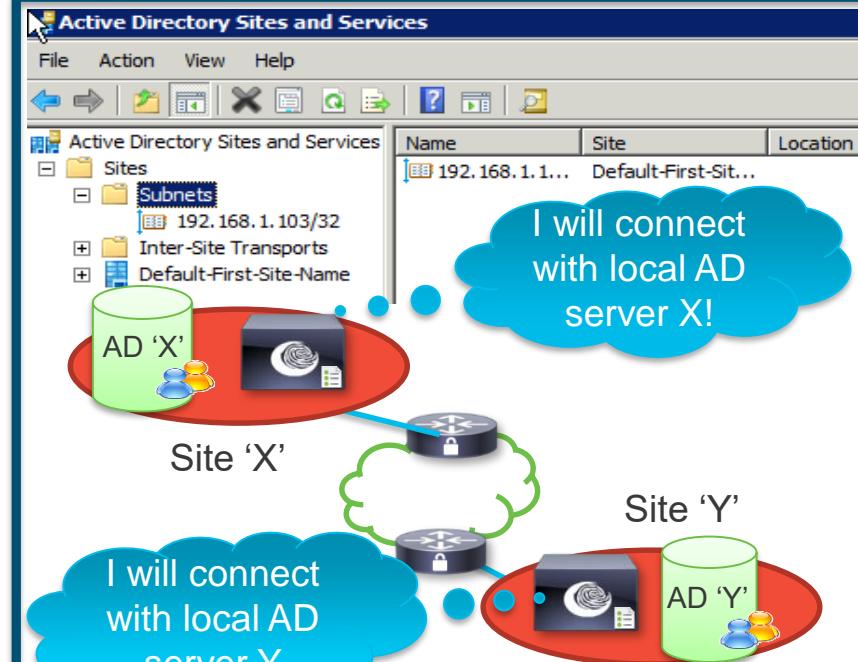


Without Site & Services



Cisco Live!

Properly Configured





AD Sites and Services

Links AD Domain Controllers to ISE Servers Based on IP Address

The screenshot shows the Windows Server Manager interface under the 'Server Manager (AD)' section. In the left navigation pane, under 'Roles', 'Active Directory Domain Services' is expanded, showing 'Active Directory Users and Computers' and 'Active Directory Sites and Services'. 'Active Directory Sites and Services' is further expanded to show 'Sites' and 'Subnets'. The 'Subnets' node is selected, displaying a list of 7 objects. The list includes:

Name	Site	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

A red box highlights the 'Default-First-Site-Name' entry. Another red box highlights the 'Servers' node under 'Default-First-Site-Name', which contains 'AD'. A callout box with a blue border and arrow points from the 'Servers' node to the following text:

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-1-5-21-419
<input type="checkbox"/>	c3.r2.dom	NO	R2.dom	S-1-5-21-347
<input type="checkbox"/>	c4.r3.dom	NO	R3.dom	S-1-5-21-743
<input type="checkbox"/>	c5.c4.r3.dom	NO	R3.dom	S-1-5-21-679
<input type="checkbox"/>	c6.c5.c4.r3.dom	NO	R3.dom	S-1-5-21-170
<input checked="" type="checkbox"/>	r1.dom	YES	R1.dom	S-1-5-21-132
<input type="checkbox"/>	r2.dom	NO	R2.dom	S-1-5-21-971
<input type="checkbox"/>	r3.dom	NO	R3.dom	S-1-5-21-1148

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: Positron-vm-2.demo.local

Join Point: All Instances

Run Tests Now

Summary: Successful

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

Run scheduled tests i

Start At: 00:00 Hrs.

Repeat every: 1 Days

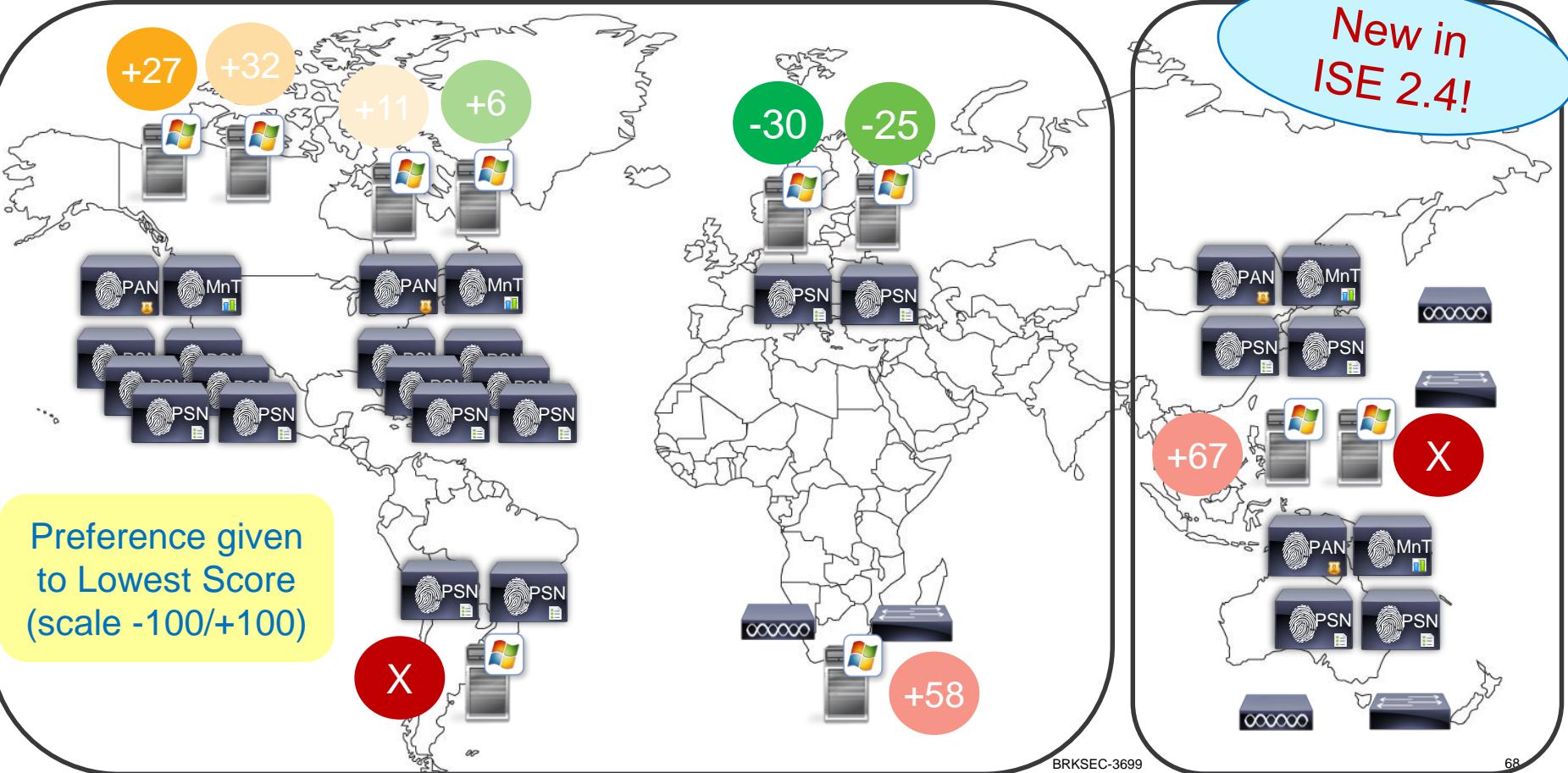
Save Reset

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

+ Run Tests View Test Details Stop All Running Tests Reset All tests to "Not Run"

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>



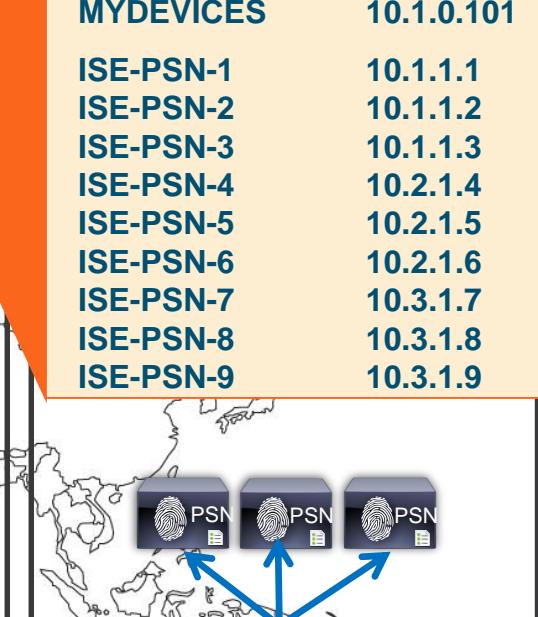
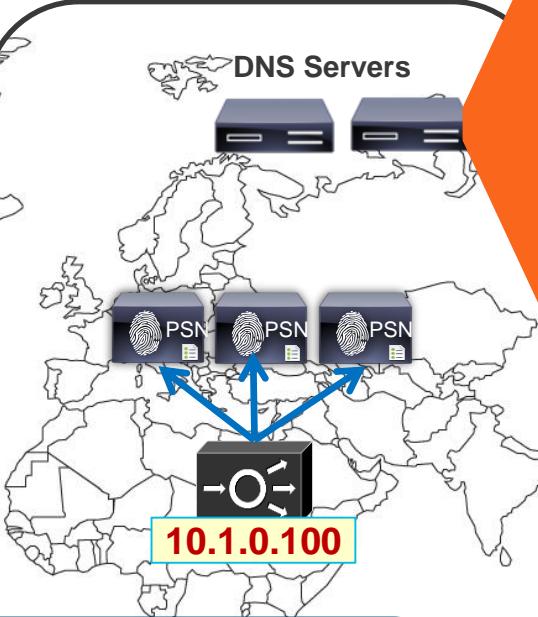
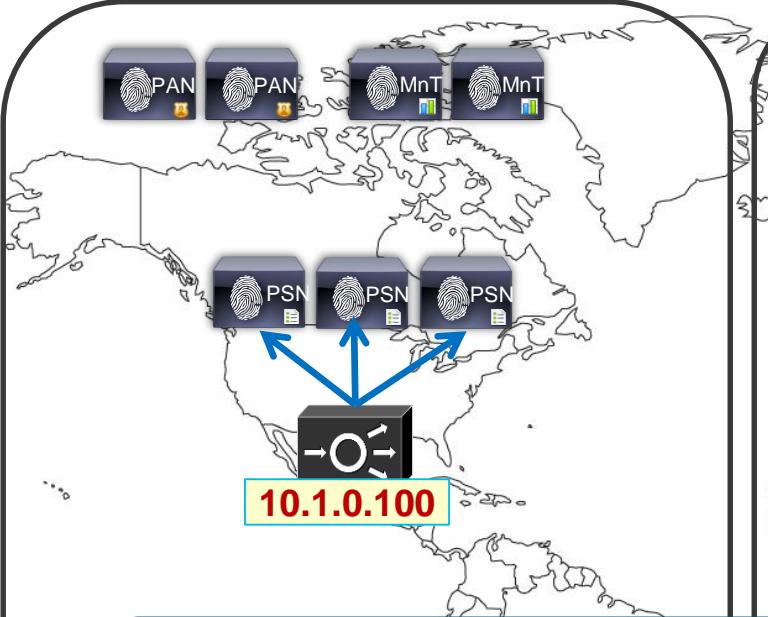
BRKSEC-3697 Advanced ISE Services, Tips and Tricks
(<https://www.ciscolive.com/global/on-demand-library/?#/>)
2016 Las Vegas - by Aaron Woland
2017 BRKSEC-3697 video content by Craig Hyps

Scaling Passive Identity and Easy Connect

Scaling Guest and Web Authentication Services

Scaling Global Sponsor / MyDevices

Anycast Example



Use **Global Load Balancer or Anycast** (example shown) to direct traffic to closest VIP. Web Load-balancing distributes request to single PSN.

Load Balancing also helps to scale Web Portal Services

DNS SERVER: DOMAIN = COMPANY.COM

SPONSOR	10.1.0.100
MYDEVICES	10.1.0.101
ISE-PSN-1	10.1.1.1
ISE-PSN-2	10.1.1.2
ISE-PSN-3	10.1.1.3
ISE-PSN-4	10.2.1.4
ISE-PSN-5	10.2.1.5
ISE-PSN-6	10.2.1.6
ISE-PSN-7	10.3.1.7
ISE-PSN-8	10.3.1.8
ISE-PSN-9	10.3.1.9

Scaling Guest Authentications Using 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

Maximum devices guests can register: (1-999)

Store device information in endpoint identity group:

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



Allow guest to bypass the Guest portal i

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 

New in
ISE 2.4

Reset

Save

Cisco live!

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.

Endpoint Purging Examples

System Identity Management Identity Mapping Network Resources Device Portal Management Feed Service pxGrid Services

Identities Groups External Identity Sources Identity Source Sequences Settings

Settings

User Custom Attributes
User Password Policy
Endpoint Purge

Matching Conditions
Purge by:

- # Days After Creation
- # Days Inactive
- Specified Date

Endpoint Purge

Define the EndPoint Purge Policy by configuration rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Status	Rule Name	Conditions (identity groups and/or other conditions)
<input checked="" type="checkbox"/>	GuestEndPointsPurgeRule	if GuestEndpoints AND ElapsedDays Greater than 30
<input checked="" type="checkbox"/>	RegisteredEndPointsPurgeRule	if RegisteredDevices AND ElapsedDays Greater than 30
<input checked="" type="checkbox"/>	DailyPurgeEndpointPurgeRule	if DailyPurgeGroup AND ENDPOINTPURGE ElapsedDays EQUALS 1
<input checked="" type="checkbox"/>	WeeklyPurgeEndpointPurgeRule	if WeeklyPurgeGroup AND ENDPOINTPURGE ElapsedDays EQUALS 7
<input checked="" type="checkbox"/>	InactiveEndpointPurgeRule	if Profiled AND ENDPOINTPURGE InactiveDays GREATER THAN 90
<input checked="" type="checkbox"/>	SpecialEventPurgeRule	if SpecialEventDevices AND ENDPOINTPURGE PurgeDate EQUALS 2014-09-15

Schedule

Purge endpoints from the identity table at a specific time

Schedule : Every at

Purge immediately

On Demand Purge

BRKSEC-3699

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public

72

Scaling Posture & MDM

Posture Lease

Once Compliant, user may leave/reconnect multiple times before re-posture

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes Home, Operations, Policy, Guest Access, and Administration. Below the navigation is a menu bar with System, Identity Management, Identity Mapping, Network Resources, Web Portal Management, Feed Service, Deployment, Licensing, Certificates, Logging, Maintenance, Backup & Restore, Admin Access, and Settings. The Settings tab is selected. On the left, a sidebar under the 'Settings' heading lists Client Provisioning, Endpoint Protection Service, FIPS Mode, Alarm Settings, Posture (with sub-options: General Settings, Reassessments, Updates, Acceptable Use Policy, Profiling), and Protocols. The main content area displays 'Posture General Settings' with fields for Remediation Timer (4 Minutes), Network Transition Delay (3 Seconds), Default Posture Status (Compliant), and Automatically Close Login Success Screen After (0 Seconds). The 'Posture Lease' section contains two radio button options: 'Perform posture assessment every time a user connects to the network' (selected) and 'Perform posture assessment every [1] Days'. A note below states: 'Note : The above configuration applies only to AnyConnect Agent and not to NAC Agent and Web Agent.' A callout bubble points from the 'Posture Lease' section in the screenshot to the same section on the ISE interface.

Posture Lease

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

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

MDM Scalability and Survivability

What Happens When the MDM Server is Unreachable?

- Scalability ≈ 30 Calls per second per PSN.
 - Cloud-Based deployment typically built for scale and redundancy
 - For cloud-based solutions, Internet bandwidth and latency must be considered.
 - Premise-Based deployment may leverage load balancing
 - ISE 1.4+ supports multiple MDM servers – could be same or different vendors.

- Authorisation permissions can be set based on MDM connectivity status:

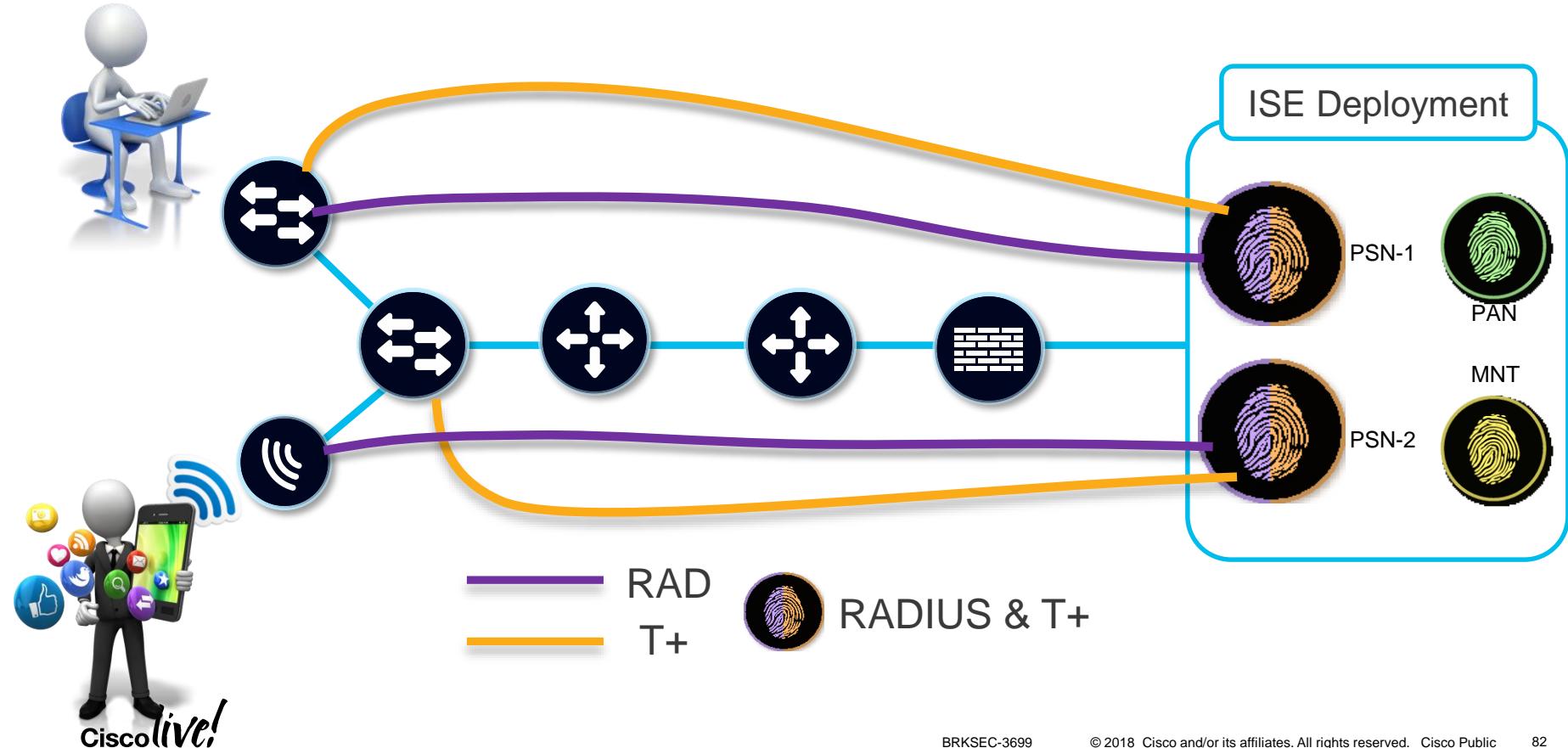
- **MDM:MDMServerReachable Equals UnReachable**
MDM:MDMServerReachable Equals Reachable

<input checked="" type="checkbox"/>	MobileDevice_Unreachable	if	(EndPoints:BYODRegistration EQUALS Yes AND MDM:MDMServerReachable EQUALS UnReachable)	then	MDM_Fail_Open
-------------------------------------	--------------------------	----	---	------	---------------

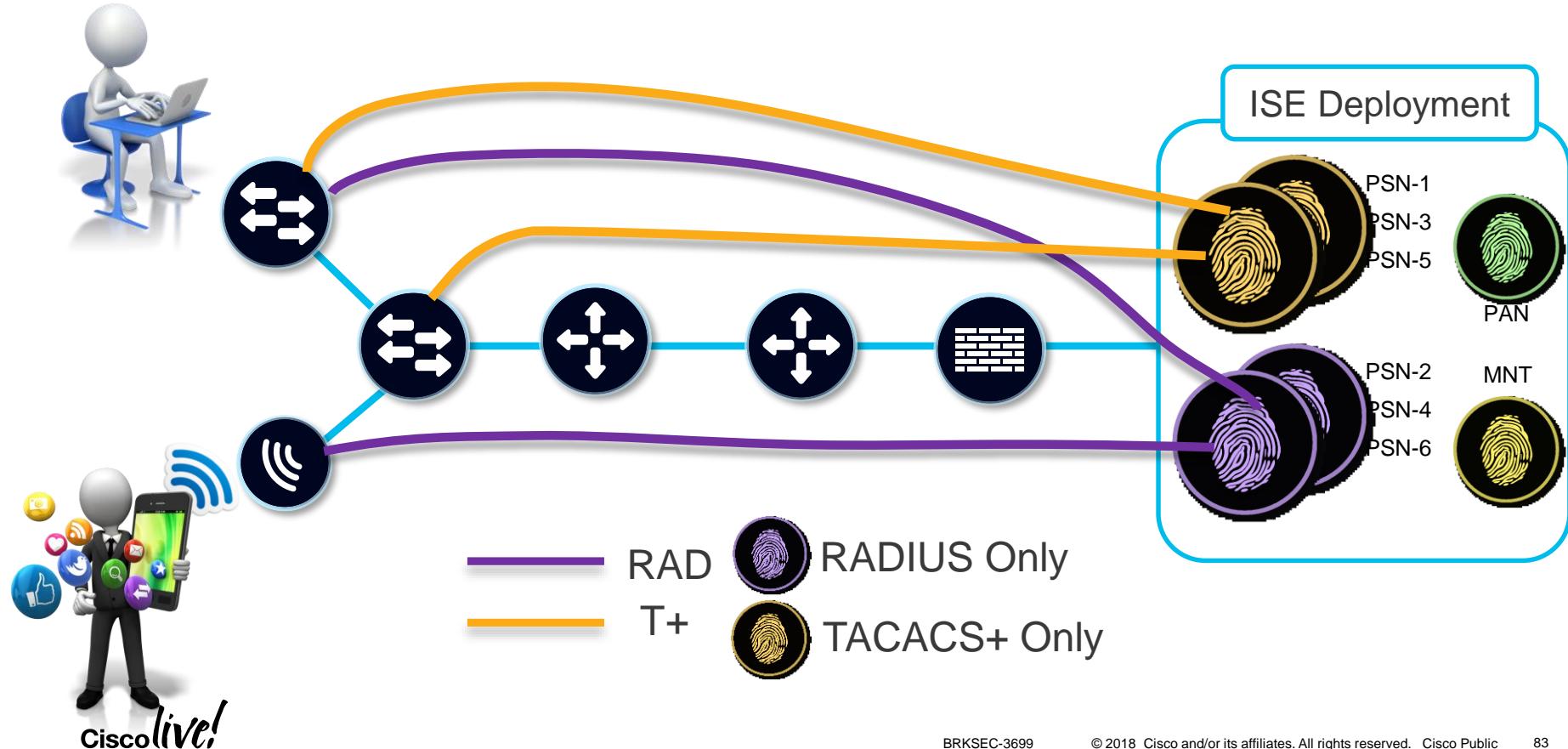
- All attributes retrieved & reachability determined by single API call on each new session.

TACACS+ Design and Scaling

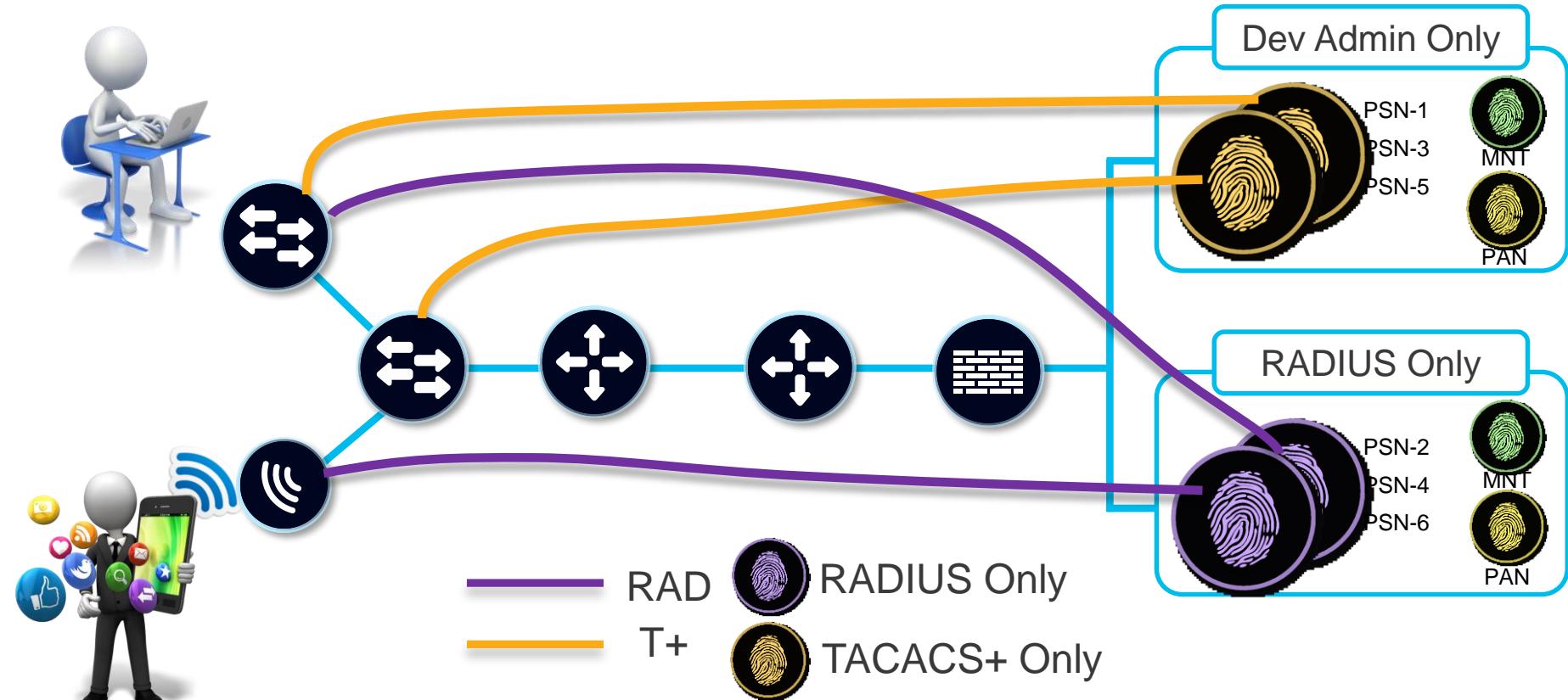
Design #1 – RADIUS & TACACS+ Share PSNs



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 i
Include Node in Node Group None i

 Enable Profiling Service i
 Enable SXP Service i

 Enable Device Admin Service TACACS+ Disabled i
 Enable Identity Mapping i

pxGrid i

Enable What's Needed for Network Access

TACACS+ Disabled

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 i
Include Node in Node Group None i

Enable Profiling Service

Enable SXP Service

Use Interface GigabitEthernet 0 i

Enable Device Admin Service Device Admin = T+ i

Enable Identity Mapping i

pxGrid i

Disable Network Access Services

Cisco live!

Options for Deploying Device Admin

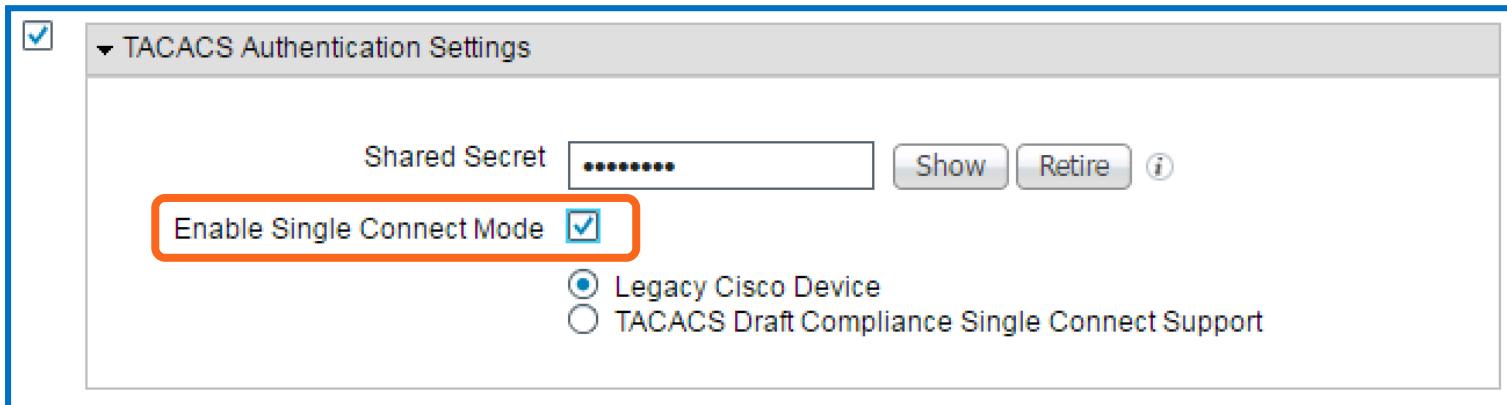
<https://communities.cisco.com/docs/DOC-63930>

Priorities		Separate Deployment	Separate PSNs	Mixed PSNs
<ul style="list-style-type: none">- According to Policy and Business Goals		 RADIUS TACACS	 RADIUS TACACS	 RADIUS/TACACS
Separation of Configuration/Duty	Yes: Specialisation for TACACS+			
	No: Shared resources/Reduced \$\$			
Independent Scaling of Services	Yes: Scale as needed/No impact on Device Admin from RADIUS services			
	No: Avoid underutilised PSNs			
Suitable for high-volume Device Admin	Yes: Services dedicated to TACACS+			
	No: Focus on “human” device admins			
Separation of Logging Store	Yes: Optimise log retention VM			
	No: Centralised monitoring			

Single Connect Mode

Scaling TACACS+ for High-Volume NADs

- Multiplexes T+ requests over single TCP connection
 - All T+ requests between NAD and ISE occur over single connection rather than separate connections for each request.
- Recommended for TACACS+ “Top Talkers”
- Note: TCP sockets locked to NADs, so limit use to NADs with highest activity.



Administration > Network Resources > Network Devices > (NAD)

Scaling Profiling and Database Replication

Endpoint Attribute Filter and Whitelist Attributes

Reduces Data Collection and Replication to Subset of Profile-Specific Attributes

- Endpoint Attribute Filter – aka “Whitelist filter”
 - Disabled by default. If enabled, only these attributes are collected or replicated.

Profiler Configuration

Administration > System Settings > Profiling

* CoA Type: Reauth	Save	Reset
Current custom SNMP community strings: <input type="text" value="*****"/>	Show	(For NMAP, comma separated. Field will be cleared on successful saved change.)
Change custom SNMP community strings: <input type="text" value=""/>	(For NMAP, comma separated. Field will be cleared on successful saved change.)	
Confirm changed custom SNMP community strings: <input type="text" value=""/>		
EndPoint Attribute Filter: <input checked="" type="checkbox"/> Enabled		

- Whitelist Filter limits profile attribute collection to those required to support default (Cisco-provided) profiles and critical RADIUS operations.
 - Filter must be disabled to collect and/or replicate other attributes.
 - Attributes used in custom conditions are automatically added to whitelist.

Whitelist Attributes vs Significant Attributes

Sampling of All Endpoint Attributes

PolicyVersion	UseCase
OUI	UserType
EndPointMACAddress	GroupsOrAttributesProcessF
MatchedPolicy	ExternalGroups
EndPointMatchedProfile	Called-Station-ID
EndPointPolicy	Calling-Station-ID
Total Certainty Factor	DestinationIPAddress
EndPointProfilerServer	DestinationPort
EndPointSource	Device IP Address
StaticAssignment	MACAddress
StaticGroupAssignment	MessageCode
UpdateTime	NADAddress
Description	NAS-IP-Address
IdentityGroup	NAS-Port
ElapsedDays	NAS-Port-Id
InactiveDays	NAS-Port-Type
NetworkDeviceGroups	NetworkDeviceName
Location	RequestLatency
Device Type	Service-Type
IdentityAccessRestricted	Timestamp
IdentityStoreName	User-Name
ADDomain	Egress-VLANID
AuthState	Egress-VLAN-Name
ISEPolicySetName	Airespace-Wlan-Id
IdentityPolicyMatchedRule	Device Port
AllowedProtocolMatchedRule	EapTunnel
SelectedAccessService	Framed-IP-Address
SelectedAuthenticationIdentityStores	NAS-Identifier
AuthenticationIdentityStore	RadiusPacketType
AuthenticationMethod	Vlan
AuthorizationPolicyMatchedRule	VlanName
SelectedAuthorizationProfiles	cafSessionAuthUserName
CPMSessionID	cafSessionAuthVlan
AAA-Server	cafSessionAuthorizedBy
OriginalUserName	cafSessionDomain
DetailedInfo	cafSessionStatus
EapAuthentication	dot1dBasePort
NasRetransmissionTimeout	dot1xAuthAuthControlledPort
TotalFailedAttempts	dot1xAuthAuthControlledPort
TotalFailedTime	dot1xAuthSessionUserName

Whitelist Attributes		
161-udp	FirstCollection	MDN
AAA-Server	FQDN	MDMSerialNumber
AC_User_Agent	Framed-IP-Address	MDMServerReachable
AUPAccepted	host-name	MDMUpdateTime
BYODRegistration	hrDeviceDescr	NADAddress
CacheUpdateTime	IdentityGroup	NAS-IP-Address
Calling-Station-ID	IdentityGroupID	NAS-Port-Id
cdpCacheAddress	IdentityStoreGUID	NAS-Port-Type
cdpCacheCapabilities	IdentityStoreName	NmapScanCount
cdpCacheDeviceId	ifIndex	NmapSubnetScanID
cdpCachePlatform	ip	operating-system
cdpCacheVersion	L4_DST_PORT	OS Version
Certificate Expiration Date	LastNmapScanTime	OUI
Certificate Issue Date	lldpCacheCapabilities	PhoneID
Certificate Issuer Name	lldpCapabilitiesMapSupported	PhoneIDType
Certificate Serial Number	lldpSystemDescription	PolicyVersion
ciaddr	MACAddress	PortalUser
CreateTime	MatchedPolicy	PostureApplicablePrevious
Description	MatchedPolicyID	DeviceRegistrationStatus
DestinationIPAddress	MDMCompliant	ProductRegistrationTimeStamp
Device Identifier	MDMCompliantFailureReason	StaticAssignment
Device Name	MDMDiskEncrypted	StaticGroupAssignment
DeviceRegistrationStatus	MDMEnrolled	sysDescr
dhcp-class-identifier	MDMIMEI	TimeToProfile
dhcp-requested-address	MDMJailBroken	Total Certainty Factor
EndPointPolicy	MDMMManufacturer	UpdateTime
EndPointPolicyID	MDMModel	User-Agent
EndPointProfilerServer	MDMOSVersion	
EndPointSource	MDMPhoneNumber	

client-lqdn

IPV4_IDENT

mdns_VSM_srv_identifier

Triggers Node Group Update and Ownership Change

mdns_VSM_txt_identifier
sipDeviceName
sipDeviceVendor
sipDeviceVersion
device-platform
device-platform-version
device-type
AD-Host-Exists
AD-Join-Point
logging-System

Triggers Global Replication

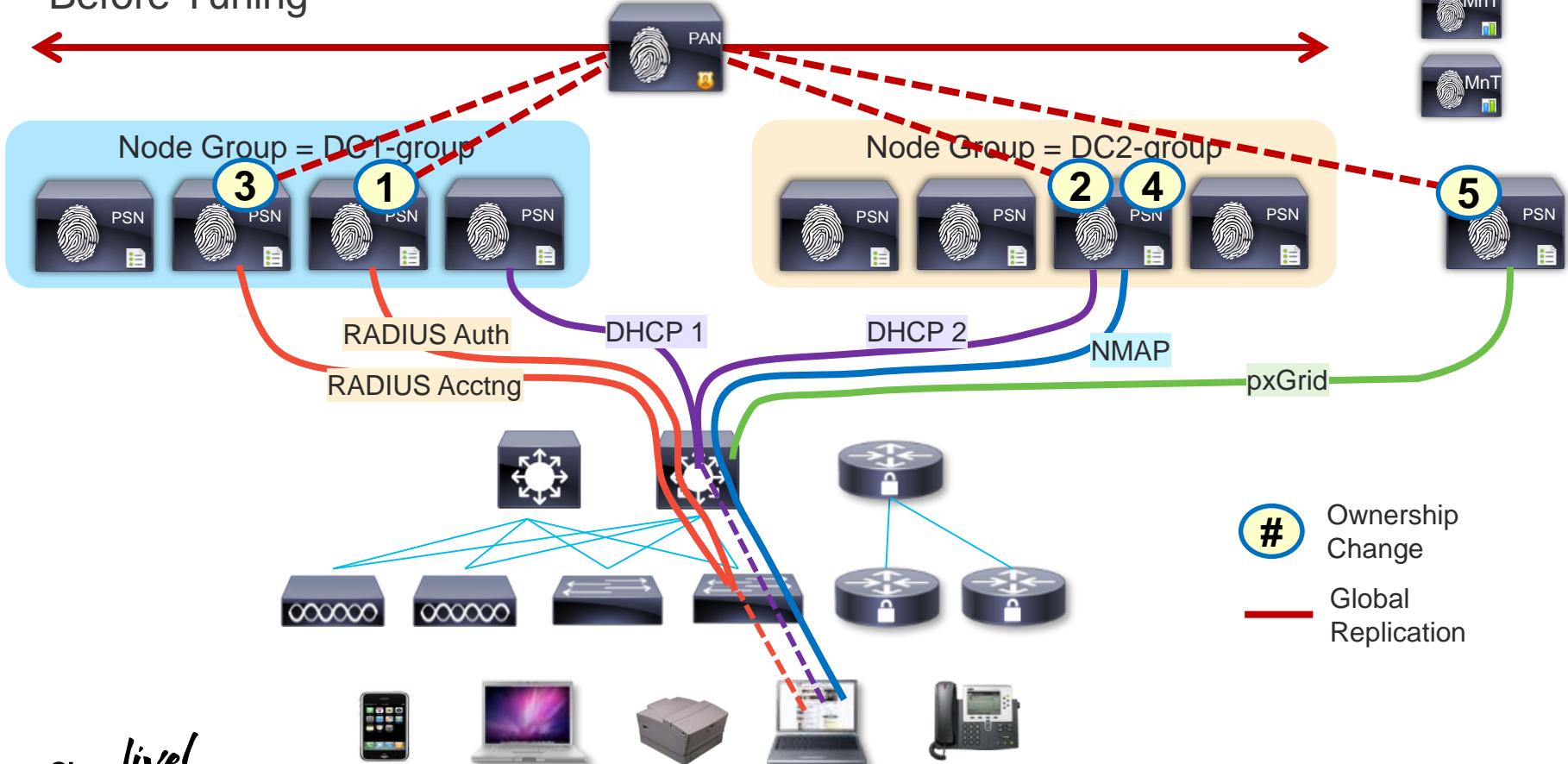
Significant Attributes

MACADDRESS
MATCHEDVALUE
ENDPOINTPOLICY
ENDPOINTPOLICYVERSION
STATICASSIGNMENT
STATICGROUPASSIGNMENT
NMAPSUBNETSCANID
PORTALUSER
DEVICEREGISTRATIONSTATUS

138-udp
139-udp

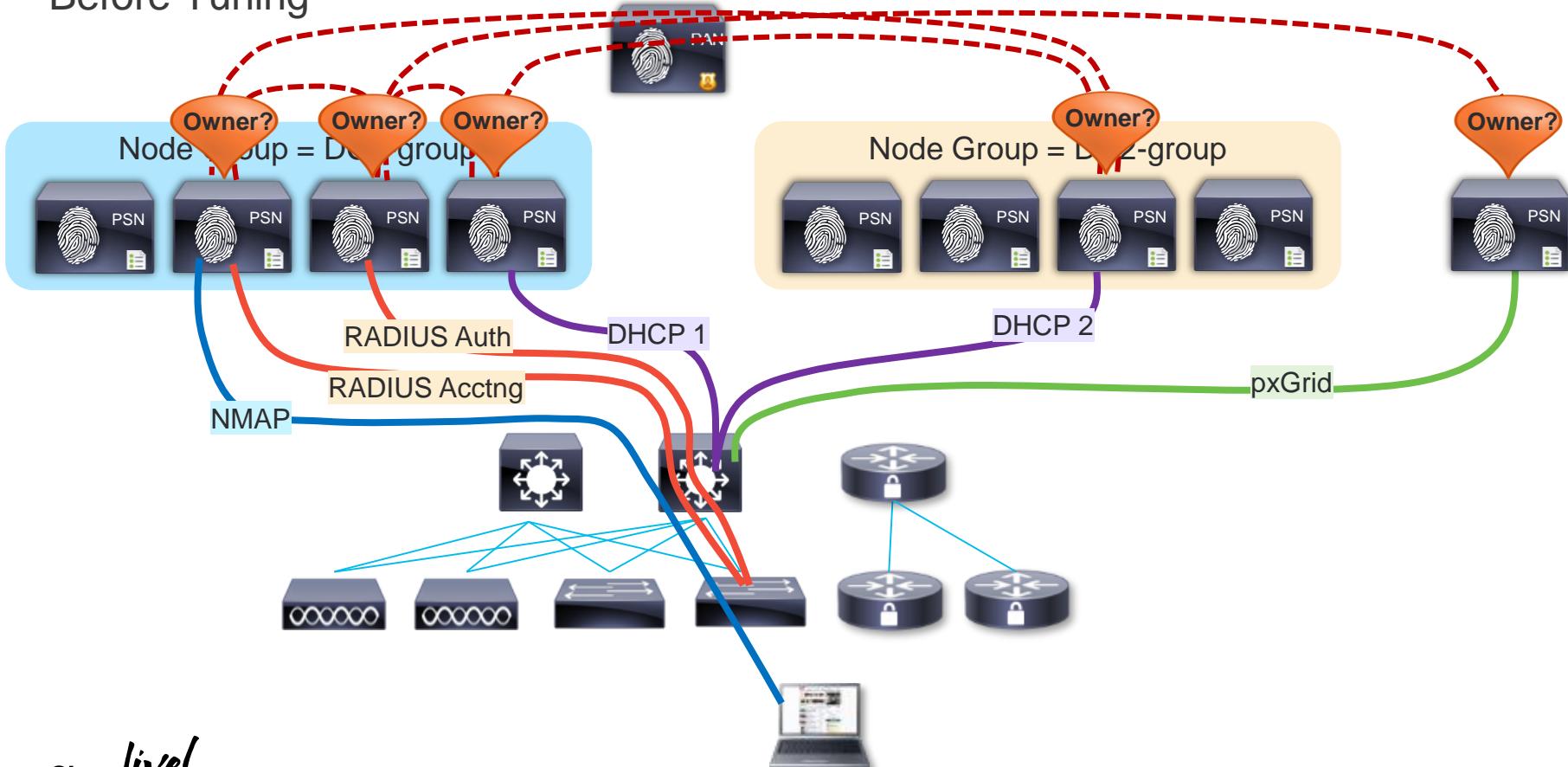
Profiling and Data Replication

Before Tuning



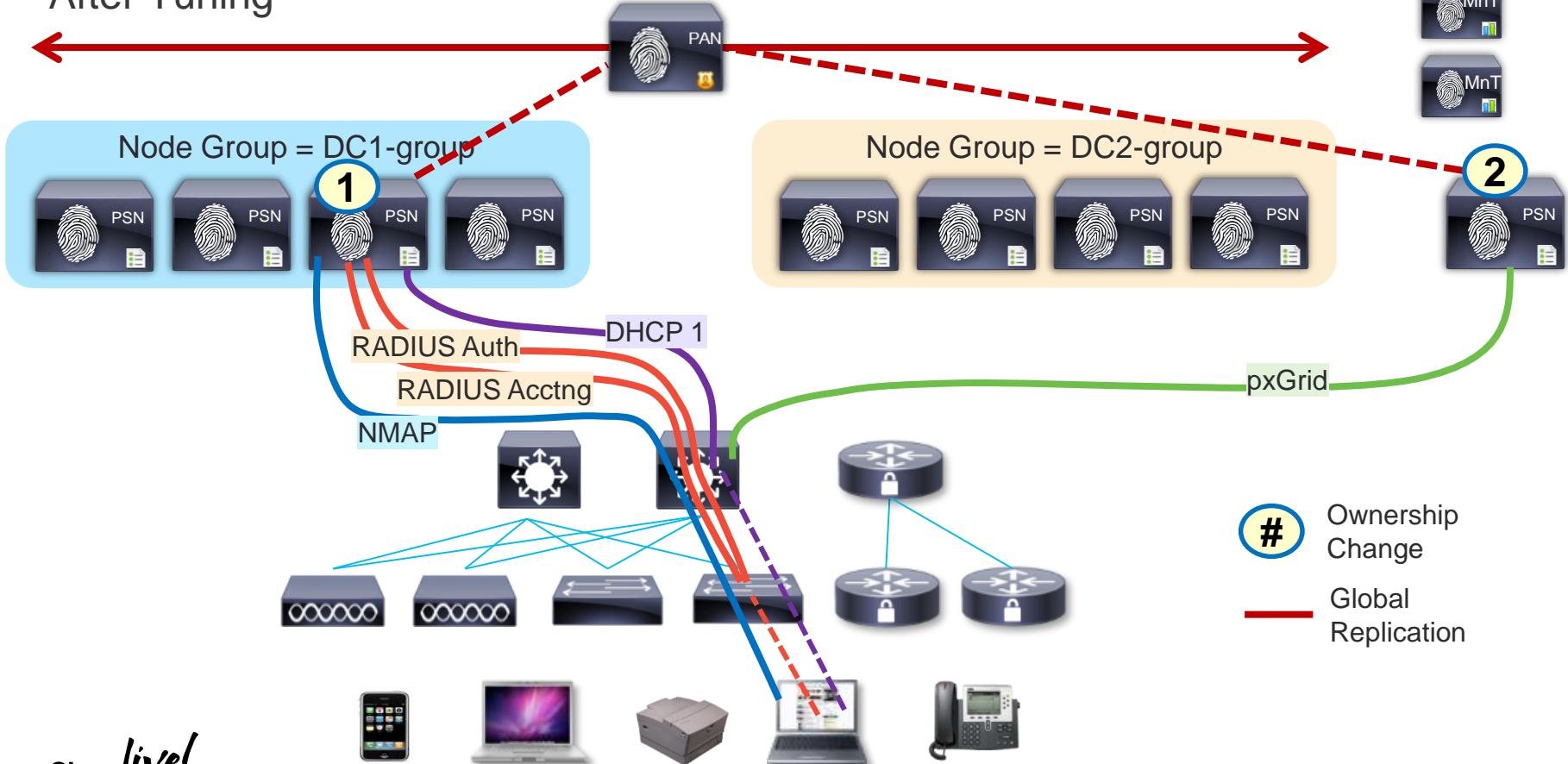
Impact of Ownership Changes

Before Tuning



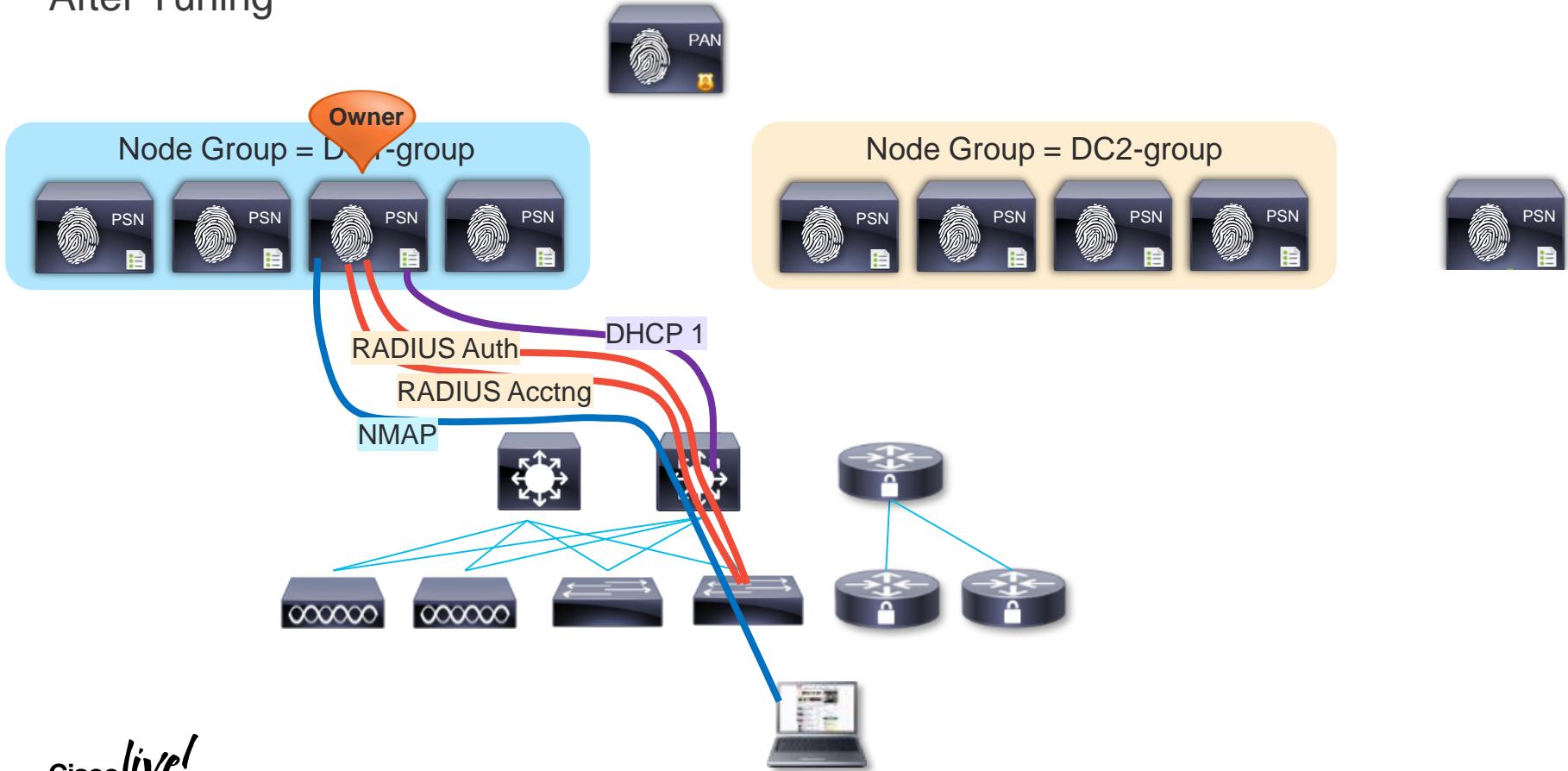
Profiling and Data Replication

After Tuning



Impact of Ownership Changes

After Tuning



ISE Profiling Best Practices

Whenever Possible...

- Use Device Sensor on Cisco switches & Wireless Controllers to optimise data collection.
- Ensure profile data for a given endpoint is sent to a single PSN (or maximum of 2)
 - Sending profile data to multiple PSNs creates uncertainty around endpoint ownership.
 - For redundancy, consider Load Balancing and Anycast to support a single IP target for RADIUS or profiling using...
 - DHCP IP Helpers
 - SNMP Traps
 - DHCP/HTTP with ERSPAN (Requires validation)
- **DO send profile data to single and same PSN or Node Group !**
 - Can do as above, but not always possible across different probes
- Use node groups and ensure profile data for a given endpoint is sent to *same* node group.
DO use Device Sensor !
 - Node Groups reduce inter-PSN communications and need to replicate endpoint changes outside of node group.
- **DO enable the Profiler Attribute Filter !**
 - Example: Device Sensor + SNMP Query/IP Helper
- Enable Profiler Attribute Filter

ISE Profiling Best Practices

General Guidelines for Probes

- **HTTP Probe:**

- Use URL Redirects instead of SPAN to centralise collection and reduce traffic load related to SPAN/RSPAN.
- **Avoid SPAN.** If used, look for key traffic chokepoints such as Internet edge or WLC connection; use intelligent SPAN/tap options or VACL Capture to limit amount of data sent to ISE. Also difficult to provide HA for SPAN.

- **DHCP Probe:**

- Use IP Helpers when possible—be aware that L3 device serving DHCP will not relay DHCP for same!
- **Do NOT enable all probes by default !** (Add DHCP SPAN) — make sure traffic sent to ISE is from DHCP Server. HA challenges.

- **SNMP Probe:**

- **Avoid SPAN, SNMP Traps, and NetFlow probes !** For polled SNMP queries, avoid short polling intervals. Be sure to set optimal PSN for polling in ISE NAD config.
- **SNMP Traps** primarily useful for non-RADIUS deployments like NAC Appliance—**Avoid SNMP Traps w/RADIUS auth.**

- **NetFlow Probe** dedicated!

Use only for specific use cases in centralised deployments—Potential for high load on network devices and ISE.

- **pxGrid Probe:**

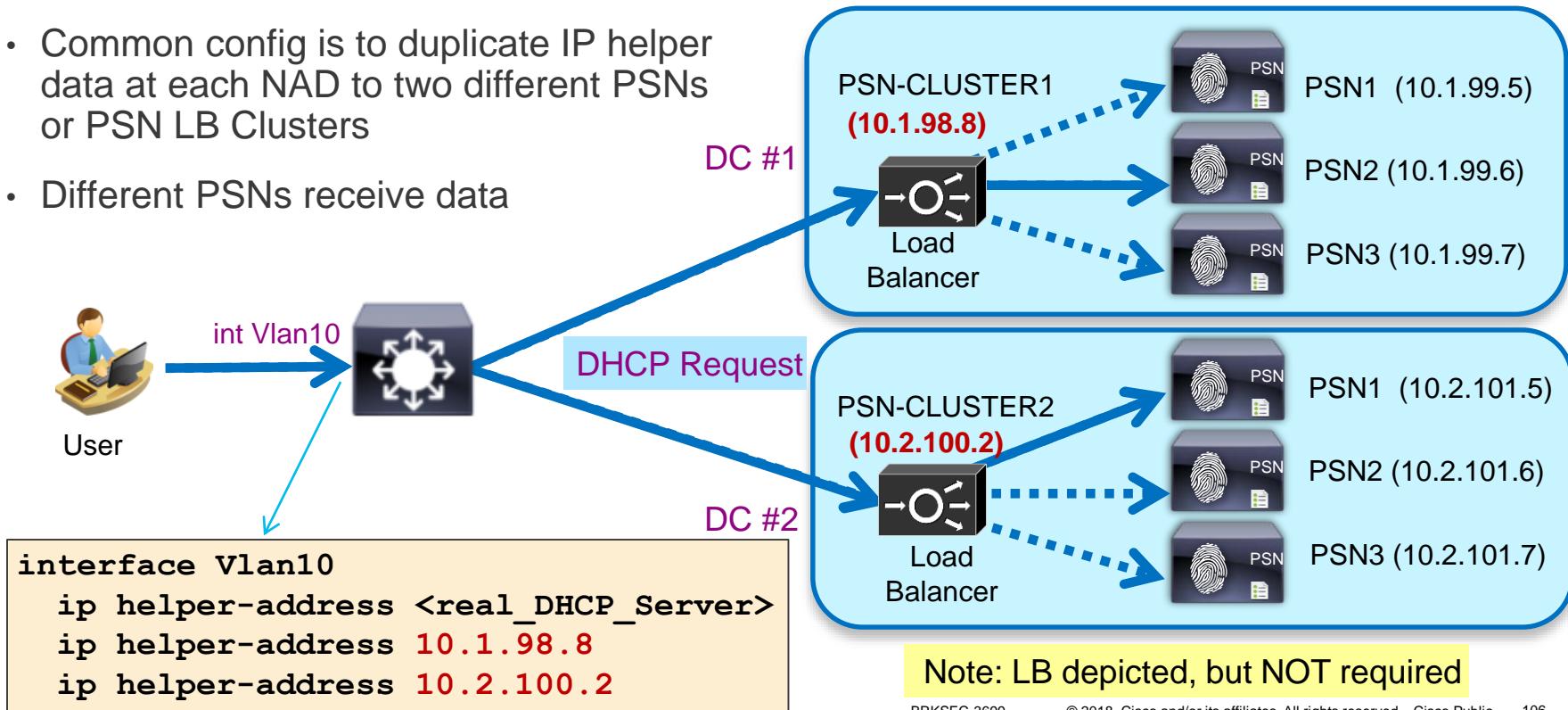
Limit # PSNs enabled for pxGrid as each becomes a Subscriber to same data. 2 needed for redundancy. Dedicate PSNs for pxGrid Probe if high-volume data from Publishers.

Profiling Redundancy – Duplicating Profile Data

Different DHCP Addresses

- Provides Redundancy but Leads to Contention for Ownership = Replication

- Common config is to duplicate IP helper data at each NAD to two different PSNs or PSN LB Clusters
- Different PSNs receive data

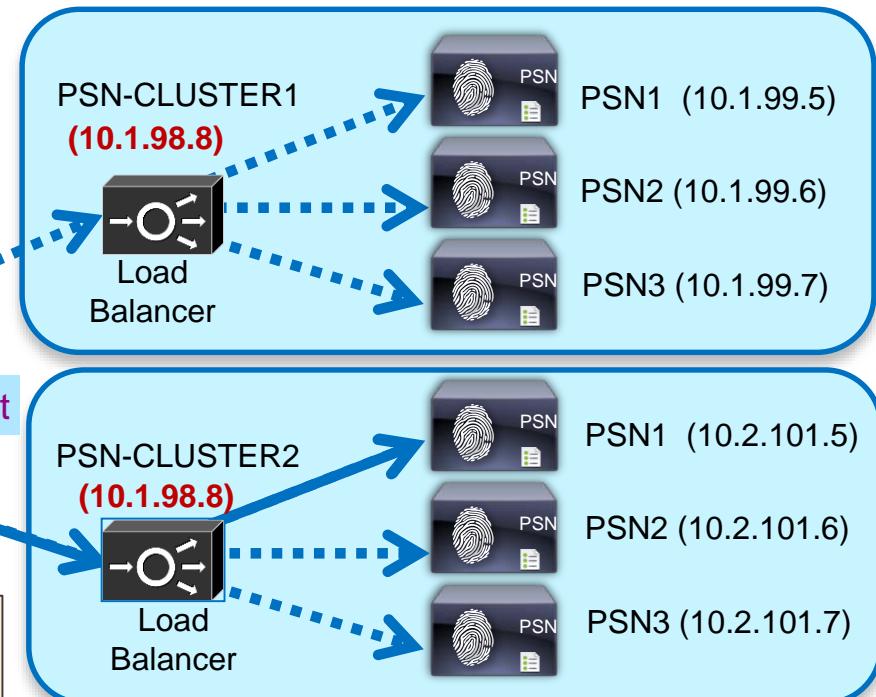
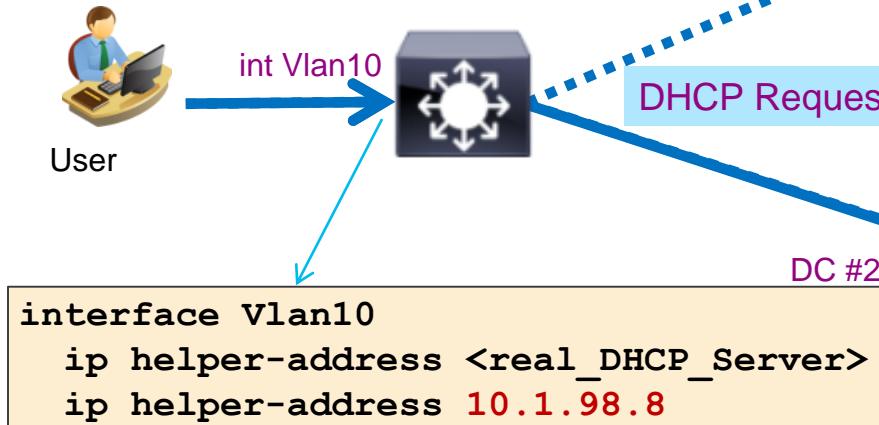


Scaling Profiling and Replication

Single DHCP VIP Address using Anycast

- Limit Profile Data to a Single PSN and Node Group

- Different PSNs or Load Balancer VIPs host same target IP for DHCP profile data
- Routing metrics determine which PSN or LB VIP receives DHCP from NAD



Cisco Industrial Network Director (IND)

www.cisco.com/go/ind



IND is specifically designed to help operations teams manage automation by providing full visibility and control of the Industrial Ethernet infrastructure in the context of the automation process.

IND Inventory

INDUSTRIAL NETWORK DIRECTOR

Operate > Inventory

Device Filters 

12 Device(s)											
	Name	Device Type	Protocol	IP Address	MAC Address	Vendor	Product ID	Serial Number	Connected To	Group	Description
<input type="checkbox"/>	10.195.119.33	HMI	CIP	10.195.119.33	00:1d:9c:cc:84:53	Rockwell Automation/Allen-Bradley	PanelView Plus_6 100	12551566	 1	Root > Painting > Cell-1	Root > Painting > Cell-1
<input type="checkbox"/>	10.195.119.34	EtherNet/IP Node	CIP	10.195.119.34	e4:90:69:a9:1e:a2	Rockwell Automation/Allen-Bradley	1734-AENTR/B Ethernet Adapter	1617714109	 1	Root > Painting > Cell-1	Root > Painting > Cell-1
<input type="checkbox"/>	10.195.119.35	EtherNet/IP Node	CIP	10.195.119.35	e4:90:69:a9:19:04	Rockwell Automation/Allen-Bradley	1734-AENTR/B Ethernet Adapter	1617714655	 1	Root > Painting > Cell-1	Root > Painting > Cell-1
<input type="checkbox"/>	10.195.119.36	EtherNet/IP Node	CIP	10.195.119.36	e4:90:69:a3:7e:c4	Rockwell Automation/Allen-Bradley	1734-AENTR/B Ethernet Adapter	1616202231	 1	Root > Painting > Cell-1	Root > Painting > Cell-1
<input type="checkbox"/>	10.195.119.37	EtherNet/IP Node	CIP	10.195.119.37	e4:90:69:a3:50:ae	Rockwell Automation/Allen-Bradley	1734-AENTR/B Ethernet Adapter	1616116586	 1	Root > Painting > Cell-1	Root > Painting > Cell-1

▼ CATEGORY

- Supported Devices
- Other Devices

▼ DEVICE TYPE

- Controller (4)
- EtherNet/IP Node (5)
- HMI (1)
- IO (2)
- Unknown

▼ PROTOCOL

- CIP (7)
- MODBUS (2)
- PROFINET (3)
- UNKNOWN

▼ VENDOR

- Rockwell Automation/Allen-Bradley (7)
- Schneider Electric (2)
- Siemens - Automation - EWA (1)
- Unknown (2)

INDUSTRIAL NETWORK DIRECTOR

Operate > Inventory

 10  

< Back  192.168.200.40 Open Device Manager

DEVICE OVERVIEW

Name: 192.168.200.40

IP Address: 192.168.200.40

MAC Address: 00:1d:9c:ca:85:8b

Device Type: EtherNet/IP Node

Vendor: Rockwell Automation/Allen-Bradley

Product ID: 0xC8

Serial Number: 12174476

Industrial Protocol: CIP

Connected to: IE3000-119-21 - FastEthernet1/0

ADDITIONAL DETAILS

Vendor ID: 0x1

Product Type: 0xC

Device Profile: Communications Adapter

Product Code: 0xC8

Major Revision: 0xA

Minor Revision: 0x7

Status: 0x30

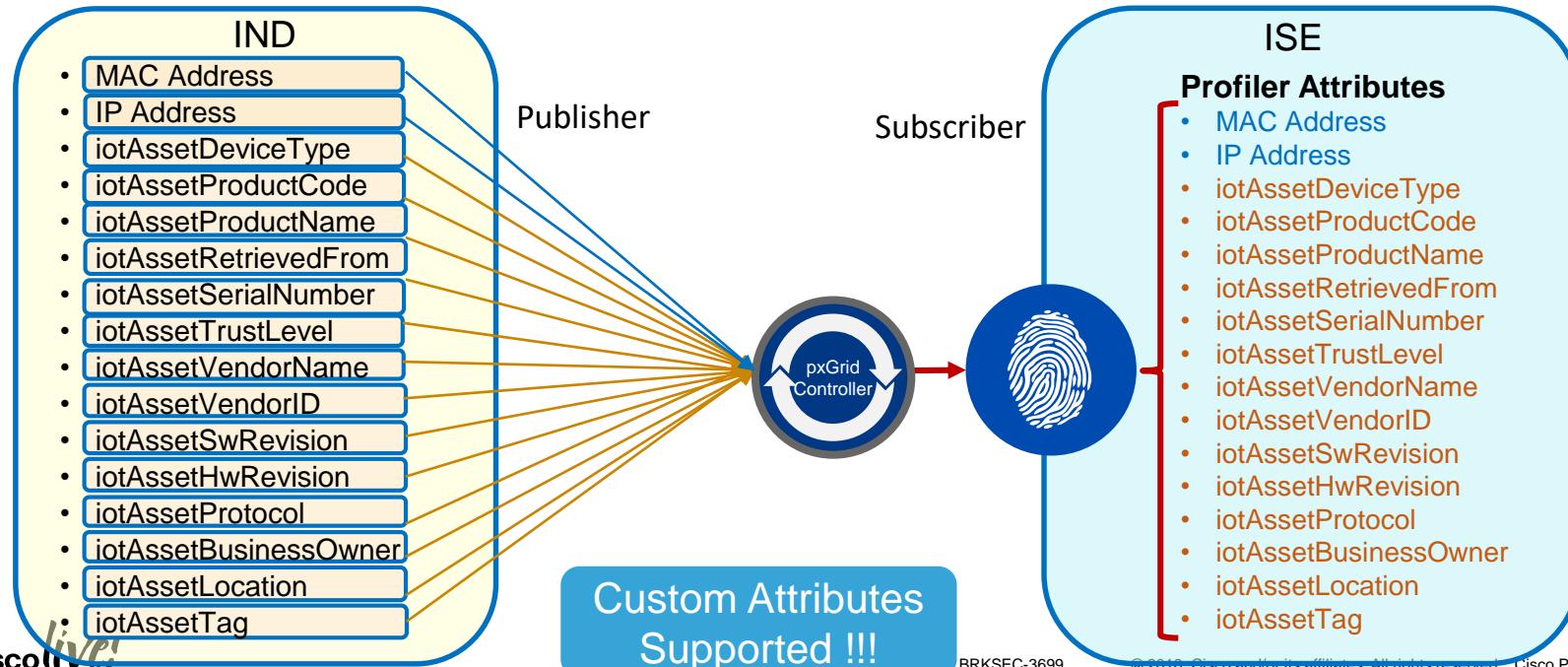
Product Name: 1756-EN2TR/C 217021900

pxGrid Profiler Probe (Context In)

New in
ISE 2.4

First Integration is with Industrial Network Director (IND)

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



pxGrid-In Probe Attributes

- Endpoint Attribute Details
- Core set of pxGrid Profile attributes
- Vendors can also send custom attributes

Cisco Identity Services Engine		Home	Context Visibility	Operations
Endpoints	Users	Network Devices	Application	
MACAddress	00:1D:9C:CA:85:8B			
MatchedPolicy	Rockwell-Automation-Device			
StaticAssignment	false			
StaticGroupAssignment	false			
Total Certainty Factor	5			
assetConnectedLinks.assetDeviceType	Switch			
assetConnectedLinks.assetId	40109			
assetConnectedLinks.assetIpAddress	10.195.119.22			
assetConnectedLinks.assetName	IE4000-119-22			
assetConnectedLinks.assetPortName	GigabitEthernet1/2			
assetDeviceType	Controller			
assetId	60100			
assetIpAddress	10.195.119.38			
assetMacAddress	00:1d:9c:ca:85:8b			
assetName	10.195.119.38			
assetProductId	1756-EN2TR/C 217021900			
assetProtocol	CIP			
assetSerialNumber	12174476			
assetVendor	Rockwell Automation/Allen-Bradley			
ip	10.195.119.38 TECSEC-3673			

pxGrid Probe
Attributes from
IND

Profiling Based on Custom Attributes

Performance Hit so Disabled By Default

New in
ISE 2.4

- Global Setting MUST be **enabled**
- If disabled:
 - Custom Attributes are NOT updated over pxGrid
 - Profiler ignores any conditions based on Custom Attributes, even if Custom Attribute is populated.

The screenshot shows the Cisco ISE web interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat C, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The Settings link is underlined, indicating it is the active section. On the left, a sidebar lists Client Provisioning, FIPS Mode, Security Settings, Alarm Settings, Posture (which is expanded), Profiling, Protocols (also expanded), Proxy, SMTP Server, and SMS Gateway. The main content area is titled 'Profiler Configuration'. It contains fields for 'CoA Type' (set to 'Port Bounce'), 'Current custom SNMP community strings' (showing '*****' and a 'Show' button), 'Change custom SNMP community strings' (with a placeholder '(For NMAP)'), 'Confirm changed custom SNMP community strings' (with a placeholder '(For NMAP)'), 'EndPoint Attribute Filter' (checkbox 'Enabled' is unchecked), 'Enable Anomalous Behaviour Detection' (checkbox 'Enabled' is checked), 'Enable Anomalous Behaviour Enforcement' (checkbox 'Enabled' is unchecked), and 'Enable Custom Attribute for Profiling' (checkbox 'Enabled' is checked). A large blue callout box at the bottom right highlights the 'Enable Custom Attribute for Profiling' checkbox with the text 'Enable Custom Attribute for Profiling: Enabled'.

Profiler Conditions Based on Custom Attributes

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below the navigation is a menu bar with Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements (selected). A sub-menu under Policy Elements shows Dictionaries, Conditions (selected), and Results.

The main content area displays the "Profiler Condition List > New Profiler Condition" page. The form fields are as follows:

- * Name: Custom_Attribute_Check5
- * Type: CUSTOMATTRIBUTE
- * Attribute Name: AssetDB_Device_Type
- * Operator: STARTSWITH
- * Attribute Value: CIP_PLC-5

Below the form, it says System Type: Administrator Created. At the bottom are Submit and Cancel buttons.

A large blue callout box highlights the "Type" dropdown menu, which lists various profiler condition types. The "CUSTOMATTRIBUTE" option is highlighted with a red rectangle.

New in
ISE 2.4

ISE 2.4 - New Profile Policies by the Numbers

Delivered Via Feed Service

- New Profiles:
 - Xerox – 45
 - HP – 139
 - Brother – 174
 - Cisco AP – 4
 - Fingerbank – 36
 - Audio Code – 7
 - Lexmark - 187
 - Customer – 38
 - Updated Profiles:
 - Xerox – 140
 - HP – 37
 - Brother – 4
 - Lexmark – 4
-

Total = **185**

Total = **630**

New and Updated IoT Profile Libraries (Coming March 2018)

Delivered via ISE Community: <https://communities.cisco.com/docs/DOC-66340>

- 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 (Defence, HVAC, Elevators, etc)
- Windows Embedded
- Medical NAC Profile Library – Updated



600+ Automation and Control Profiles (~900 with MedNAC)

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, and License Warning. The main content area is titled "Profiling Policies". On the left, a tree view shows various Siemens device categories. The central part of the screen displays a table of profiling policies with columns for Profiling Policy Name, Policy Enabled, System Type, and Description. A search bar at the top of the table allows filtering by "Lighting". To the right, a sidebar titled "Lighting" provides a "Quick Filter" and a list of automation categories: 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, and Lighting.

Profiling Policies

Profiling Policy Name	Policy Enabled	System Type	Description
Advanced-Illumination-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Advanced Illumination Device
Advatek-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Advatek Lighting Device
BC-Illumination-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for BC-Illumination Device
Beijing-E3Control-Technology-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy for Beijing-E3Control Technology Device
Creative-Lighting-Sound-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Creative Lighting Sound Device
Cree-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Cree Device
Darfon-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Darfon Lighting Device
Digital-Lighting-Systems-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy for Digital Lighting Systems Device
ELC-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting/Entertainment) Policy for ELC Lighting Device
Electronic-Theatre-Controls-Device	Enabled	Administrator Created	Automation and Control (Home/Lighting/Entertainment) Policy for Electronic Theatre Controls Device
GE-Consumer-Industrial-Device	Enabled	Administrator Created	Automation and Control (Building/Power/Lighting) Policy for GE Consumer Industrial Device
General-Electric-Device	Enabled	Administrator Created	Automation and Control (Manufacturing/Building/Lighting) Policy for General Electric Device
German-Light-Products-Device	Enabled	Administrator Created	Automation and Control (Lighting/Entertainment) Policy for German Light Products Device
Hills-Sound-Vision-Lighting-Device	Enabled	Administrator Created	Automation and Control (Building/Healthcare-RTLS) Policy for Hills Sound Vision Lighting Device
Hubbell-Building-Automation-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy for Hubbell Building Automation Device
Intelligent-Distributed-Controls-Device	Enabled	Administrator Created	Automation and Control (Manufacturing/Building/Lighting) Policy for Intelligent Distributed Controls Device
Invisia-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Invisia Lighting Device
LACROIX-Traffic-Device	Enabled	Administrator Created	Automation and Control (Lighting/Traffic-Transportation) Policy for LACROIX Traffic Device
LED-Roadway-Lighting-Device	Enabled	Administrator Created	Automation and Control (Lighting/Traffic-Transportation) Policy for LED Roadway Lighting Device
LNT-Automation-Device	Enabled	Administrator Created	Automation and Control (Building/Lighting) Policy for LNT Automation Device
Laser-Light-Engines-Device	Enabled	Administrator Created	Automation and Control (Lighting) Policy for Laser Light Engines Device
Leedarson-Lighting-Device	Enabled	Administrator Created	Automation and Control (Building/Home/Lighting) Policy for Leedarson Lighting Device
Lihtina-Science-Group-Device	Enabled	Administrator Created	Automation and Control (Lighting/Healthcare-Agriculture) Policy for Lihtina-Science Group Device

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

119

Why Do I Care About # Profiles?



- ISE 2.1+ supports a MAX of **2000** profiles
 - Let's Do the Math...
 - ~600 Base Profiles
 - ~600 New Feed Profiles (2.4)
 - ~275 Medical NAC Profiles
 - ~625 Automation & Control Profiles
-
- ~2100 Profiles**
- No restrictions on profile import, so must check # profiles in library before import large batch of new profiles

Scaling MnT (Optimise Logging and Noise Suppression)

The Fall Out From the Mobile Explosion and IoT

- Explosion in number and type of endpoints on the network.
- High auth rates from mobile devices—many personal (unmanaged).
 - Short-lived connections: Continuous sleep/hibernation to conserve battery power, roaming, ...
- Misbehaving supplicants: Unmanaged endpoints from numerous mobile vendors may be misconfigured, missing root CA certificates, or running less-than-optimal OS versions
- Misconfigured NADs. Common issue is setting timeouts too low & not throttling misbehaving clients.
- Misconfigured Load Balancers—Suboptimal persistence and excessive RADIUS health probes.
- Increased logging from Authentication, Profiling, NADs, Guest Activity, ...
- System not originally built to scale to new loads.
- End user behaviour when above issues occur.
- Bugs in client, NAD, or ISE.



A Few Bad Apples Can Spoil the Whole Bunch



Clients Misbehave!

- Example education customer:
 - ONLY 6,000 Endpoints (all BYOD style)
 - 10M Auths / 9M Failures in a 24 hours!
 - 42 Different Failure Scenarios – all related to clients dropping TLS (both PEAP & EAP-TLS).
- Suplicant List:
 - Kyocera, Asustek, Murata, Huawei, Motorola, HTC, Samsung, ZTE, RIM, SonyEric, ChiMeiCo, Apple, Intel, Cybertan, Liteon, Nokia, HonHaiPr, Palm, Pantech, LgElectr, TaiyoYud, Barnes&N
- **5411 No response received during 120 seconds on last EAP message sent to the client**
 - This error has been seen at a number of Escalation customers
 - Typically the result of a misconfigured or misbehaving supplicant not completing the EAP process.



Challenge: How to reduce the flood of log messages while increasing PSN and MNT capacity and tolerance



Getting More Information With Less Data

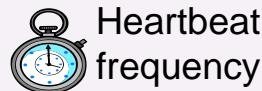
Scaling to Meet Current and Next Generation Logging Demands

Rate Limiting at Source

Reauth period

Quiet-period 5 min

Held-period / Exclusion 5 min



Reauth phones



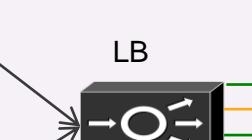
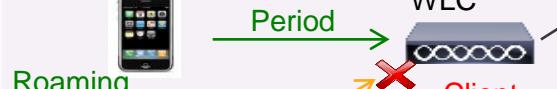
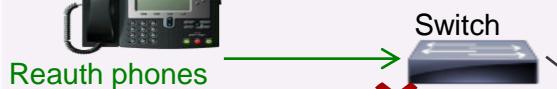
Unknown users



Roaming supplicant



Misbehaving supplicant



LB Health probes



Detect and reject misbehaving clients

Log Filter



PSN



Reject bad supplicant



Filter health probes from logging



Count and discard repeated events



MNT



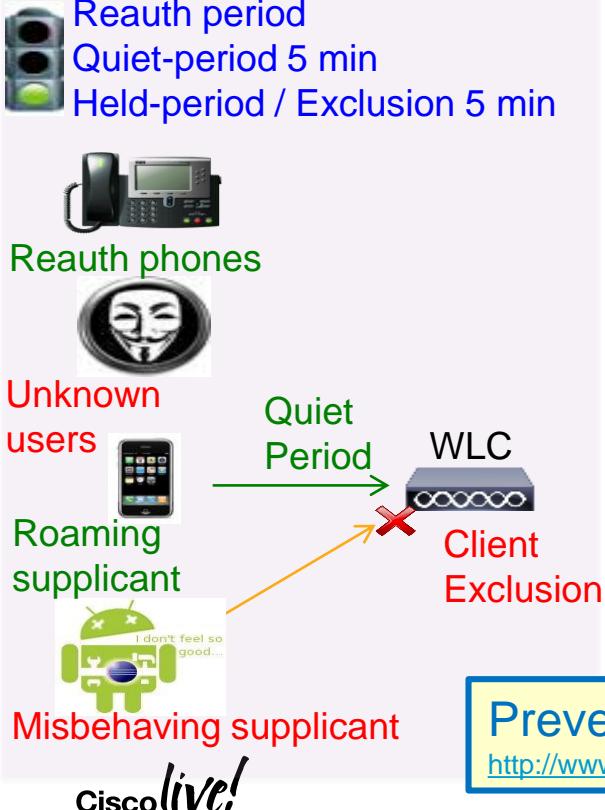
Count and discard repeats and unknown NAD events

Filtering at Receiving Chain

Tune NAD Configuration

Rate Limiting at Wireless Source

BRKSEC-2059 Deploying ISE in a Dynamic Environment - Clark Gambrel



Wireless (WLC)

- RADIUS Server Timeout:** Increase from default of 2 to 5 sec
- RADIUS Aggressive-Failover:** Disable aggressive failover
- RADIUS Interim Accounting:** v7.6: Disable; v8.0+: Enable with interval of 0. (Update auto-sent on DHCP lease or Device Sensor)
- Idle Timer:** Increase to 1 hour (3600 sec) for secure SSIDs
- Session Timeout:** Increase to 2+ hours (7200+ sec)
- Client Exclusion:** Enable and set exclusion timeout to 180+ sec
- Roaming:** Enable CCKM / SKC / 802.11r (when feasible)
- Bugfixes:** Upgrade WLC software to address critical defects

Prevent Large-Scale Wireless RADIUS Network Melt Downs

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/118703-technote-wlc-00.html>

Added in
WLC 8.4

One-Click Setup for ISE Best Practice Config

The image displays two screenshots of the Cisco Wireless Local Controller (WLC) 8.4 interface. The left screenshot shows the 'RADIUS Authentication Servers > New' configuration page. The right screenshot shows the 'WLANS > Edit 'v-employee'' configuration page. Both screenshots highlight the 'Apply Cisco ISE Default settings' checkbox, which is checked in both cases. A large orange box encloses the text 'Apply Cisco ISE Default Settings' and the word 'Enabled'.

RADIUS Authentication Servers > New

- Server Index (Priority): 2
- Server IP Address(Ipv4/Ipv6): 10.1.101.17
- Shared Secret Format: ASCII
- Shared Secret: XXXXXXXX
- Confirm Shared Secret: XXXXXXXX
- Apply Cisco ISE Default settings**:
- Key Wrap: (Designed for FIPS customers and requires a FIPS-compliant cipher suite)
- Port Number: 1812
- Server Status: Enabled
- Support for CoA: Disabled
- Server Timeout: 2 seconds
- Network User:
- Management:
- Management Retransmit Time:
- Tunnel Proxy: Enable
- IPSec: Enable

WLANS > Edit 'v-employee'

- General Security QoS Policy-Mapping Advanced**
- Layer 2 Layer 3 AAA Servers**
- Select AAA servers below to override use of default servers on the RADIUS Servers
- RADIUS Server Overwrite interface: Enabled
- Apply Cisco ISE Default Settings**:
- Authentication Servers Accounting Servers**
- Server 1: Enabled, IP:10.1.98.8, Port:1812, Accounting IP:10.1.98.8, Port:1813
- Server 2: None
- Server 6: None
- RADIUS Server Accounting**

Which WLC Software Should I Deploy?

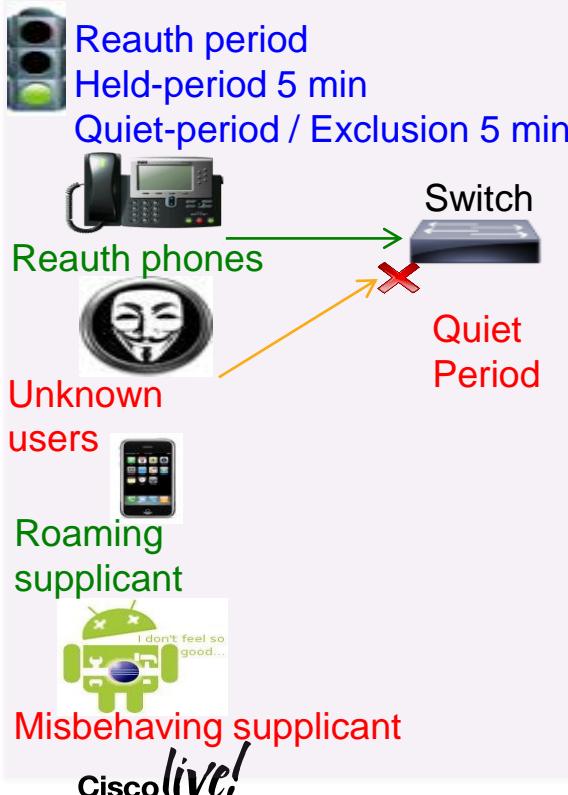
- **8.0.152.0** – Currently the most mature and reliable release.
- **8.2.166.0** – Mature - Recommended when need new feature/hardware support.
- **8.3.133.0** – Less Mature – Recommend if require new features in 8.3.x
- **8.5.110.0** – Cutting edge – Recommend if require new features in 8.5.x
- **8.6.101.0** – Bleeding edge – Only if absolutely require new features in 8.6.x
- Example critical defects resolved in maintenance and new releases:

CDETS	Title
CSCul83594	Session-id is not synchronised across mobility, if the network is open (fixed in 8.6)
CSCuu82607	Evaluation of all for OpenSSL June 2015
CSCuu68490	duplicate radius-acct update message sent while roaming
CSCus61445	DNS ACL on wlc is not working - AP not Send DTLS to WLC
CSCuq48218	Cisco WLC cannot process multiple sub-attributes in single RADIUS VSA
CSCuo09947	RADIUS AVP #44 (Acct-Session-ID) to be sent in RADIUS authentication messages

<https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/200046-TAC-Recommended-AireOS.html>

Tune NAD Configuration

Rate Limiting at **Wired** Source

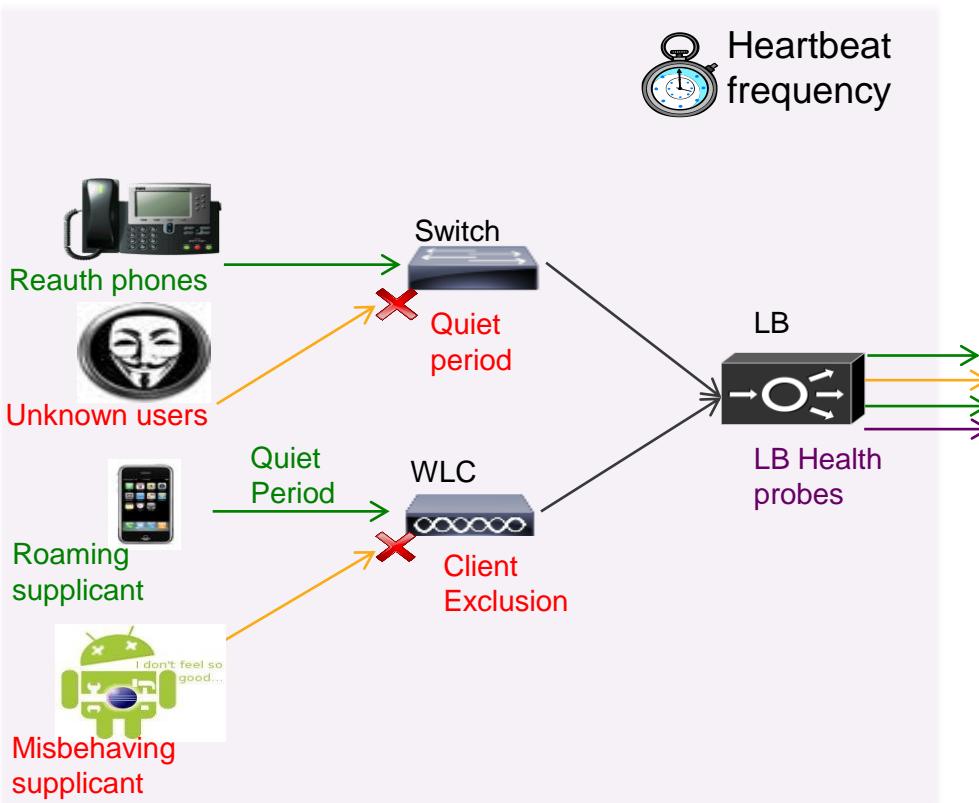


Wired (IOS / IOS-XE)

- **RADIUS Interim Accounting**: Use *newinfo* parameter with long interval (for example, 24-48 hrs), if available. Otherwise, set 15 mins. **If LB present, set shorter than RADIUS persistence time.**
- **802.1X Timeouts**
 - held-period: Increase to 300+ sec
 - quiet-period: Increase to 300+ sec
 - ratelimit-period: Increase to 300+ sec
- **Inactivity Timer**: Disable or increase to 1+ hours (3600+ sec)
- **Session Timeout**: Disable or increase to 2+ hours (7200+ sec)
- **Reauth Timer**: Disable or increase to 2+ hours (7200+ sec)
- **Bugfixes**: Upgrade software to address critical defects.

RADIUS Test Probes

Reduce Frequency of RADIUS Server Health Checks

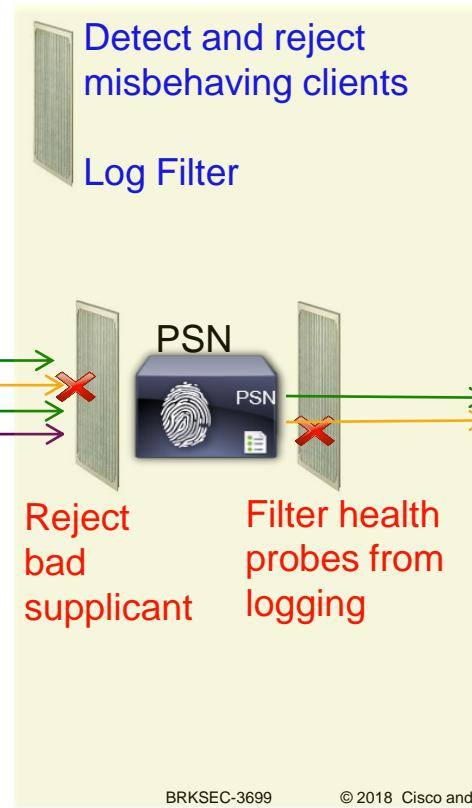


- **Wired NAD:** RADIUS test probe interval set with **idle-time** parameter in radius-server config; Default is 60 minutes
 - No action required
- **Wireless NAD:** If configured, WLC only sends “active” probe when server marked as dead.
 - No action required
- **Load Balancers:** Set health probe intervals and retry values short enough to ensure prompt failover to another server in cluster occurs prior to NAD RADIUS timeout (typically 20-60 sec.) but long enough to avoid excessive test probes.

PSN Noise Suppression and Smarter Logging

Filter Noise and Provide Better Feedback on Authentication Issues

- PSN Collection Filters
- PSN Misconfigured Client Dynamic Detection and Suppression
- PSN Accounting Flood Suppression
- Detect Slow Authentications
- Enhanced Handling for EAP sessions dropped by supplicant or Network Access Server (NAS)
- Failure Reason Message and Classification
- Identify RADIUS Request From Session Started on Another PSN
- Improved Treatment for Empty NAK List



PSN Filtering and Noise Suppression

ISE 2.2+

Dynamic Client Suppression

Flag misconfigured supplicants for same auth failure within specified interval and stop logging to MnT

Send alarm with failure statistics

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports UDP Ports DTLS

SUPPRESS REPEATED FAILED CLIENTS

Suppress repeated failed clients i

Detect two failures within minutes(1 - 30)

Report failures once every minutes (15 - 60)

Reject repeated failed RADIUS requests i

Failures prior to automatic rejection seconds (2 - 100)

Continue rejecting seconds (2 - 100)

Ignore repeated accounting updates within seconds (1 - 86,400)

SUPPRESS SUCCESSFUL CONNECTIONS

Suppress repeated successful connections i

AUTHENTICATION DATA

Highlight steps lost seconds (500 - 10,000)

Valid Time ranges displayed by default

Each endpoint tracked by:

- Calling-Station-ID (MAC Address)
- NAS-IP-Address (NAD address)
- Failure reason

PSN Filtering and Noise Suppression

Dynamic Client Suppression

Flag misconfigured supplicants for same auth failure within specified interval and stop logging to MnT

Send alarm with failure statistics

Send immediate Access-Reject (do not even process request) IF:
1) Flagged for suppression
2) Fail auth total X times for same failure reason (inc 2 prev)

Fully process next request after rejection period expires.

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports UDP Ports DTLS

Suppress Repeated Failed Clients

Suppress repeated failed clients i

Detect two failures within minutes(1 - 30)

Report failures once every minutes (15 - 60)

Reject repeated failed RADIUS requests i

Failures prior to automatic rejection minutes(1 - 30) Hard-coded @ 5 in ISE 2.0

Continue rejecting requests for minutes (5 - 180)

Ignore repeated accounting updates within seconds (1 - 86,400)

Suppress Successful Reports

Suppress repeated successful authentications i

Authentication Details

Highlight steps longer than milliseconds (500 - 10,000)

PSN Noise Suppression

Drop Excessive RADIUS Accounting Updates from “Misconfigured NADs”

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports UDP Ports DTLS

SUPPRESS REPEATED FAILED CLIENTS

Suppress repeated failed clients i

Detect two failures within i minutes(1 - 30)

Report failures once every i minutes (15 - 60)

Reject repeated failed RADIUS requests i

Failures prior to automatic rejection i (2-100)

Continue rejecting requests for i minutes (5 - 180)

Ignore repeated accounting updates within i seconds (1 - 86,400)

SUPPRESS SUCCESSFUL REPORTS

Suppress repeated successful authentications i

AUTHENTICATION DETAILS

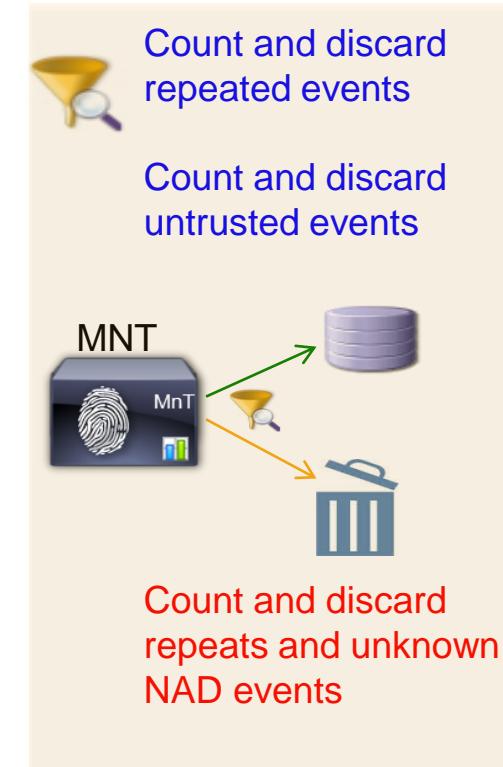
Highlight steps longer than i milliseconds (500 - 10,000)

Allow 2 RADIUS Accounting
Updates for same session in
specified interval, then drop.

MnT Log Suppression and Smarter Logging

Drop and Count Duplicates / Provide Better Monitoring Tools

- Drop duplicates and increment counter in Live Log for “matching” passed authentications
- Display repeat counter to Live Sessions entries.
- Update session, but do not log RADIUS Accounting Interim Updates
- Log RADIUS Drops and EAP timeouts to separate table for reporting purposes and display as counters on Live Log Dashboard along with Misconfigured Supplicants and NADs
- Alarm enhancements
- Revised guidance to limit syslog at the source.
- MnT storage allocation and data retention limits
- More aggressive purging
- Allocate larger VM disks to increase logging capacity and retention.



MnT Noise Suppression

SUPPRESS STORAGE OF REPEATED SUCCESSFUL AUTH EVENTS

SUPPRESS SUCCESSFUL REPORTS
= DO NOT SAVE REPEATED SUCCESSFUL AUTH EVENTS FOR THE SAME SESSION TO MNT DB

THESE EVENTS WILL NOT DISPLAY IN LIVE AUTHENTICATIONS LOG BUT DO INCREMENT REPEAT COUNTER.

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports UDP Ports DTLS

SUPPRESS REPEATED FAILED CLIENTS

Suppress repeated failed clients i

Detect two failures within i minutes(1 - 30)

Report failures once every i minutes (15 - 60)

Reject repeated failed RADIUS requests i

Failures prior to automatic rejection i (2-100)

Continue rejecting requests for i minutes (5 - 180)

Ignore repeated accounting updates within i seconds (1 - 86,400)

SUPPRESS SUCCESSFUL REPORTS

Suppress repeated successful authentications i

Authentication Details

Highlight steps longer than i milliseconds (500 - 10,000)

MnT Noise Suppression

SUPPRESS Storage of Repeated Successful Auth Events

Step latency is visible in Live Logs details

Administration > System > Settings > Protocols > RADIUS

RADIUS Settings

Suppression & Reports UDP Ports DTLS

Suppress Repeated Failed Clients

Suppress repeated failed clients ⓘ
Detect two failures within ⓘ minutes(1 - 30)
Report failures once every ⓘ minutes (15 – 60)

Reject repeated failed RADIUS requests ⓘ
Failures prior to automatic rejection ⓘ (2-100)
Continue rejecting requests for ⓘ minutes (5 – 180)
Ignore repeated accounting updates within ⓘ seconds (1 - 86,400)

Suppress Successful Reports

Suppress repeated successful authentications ⓘ

Authentication Details

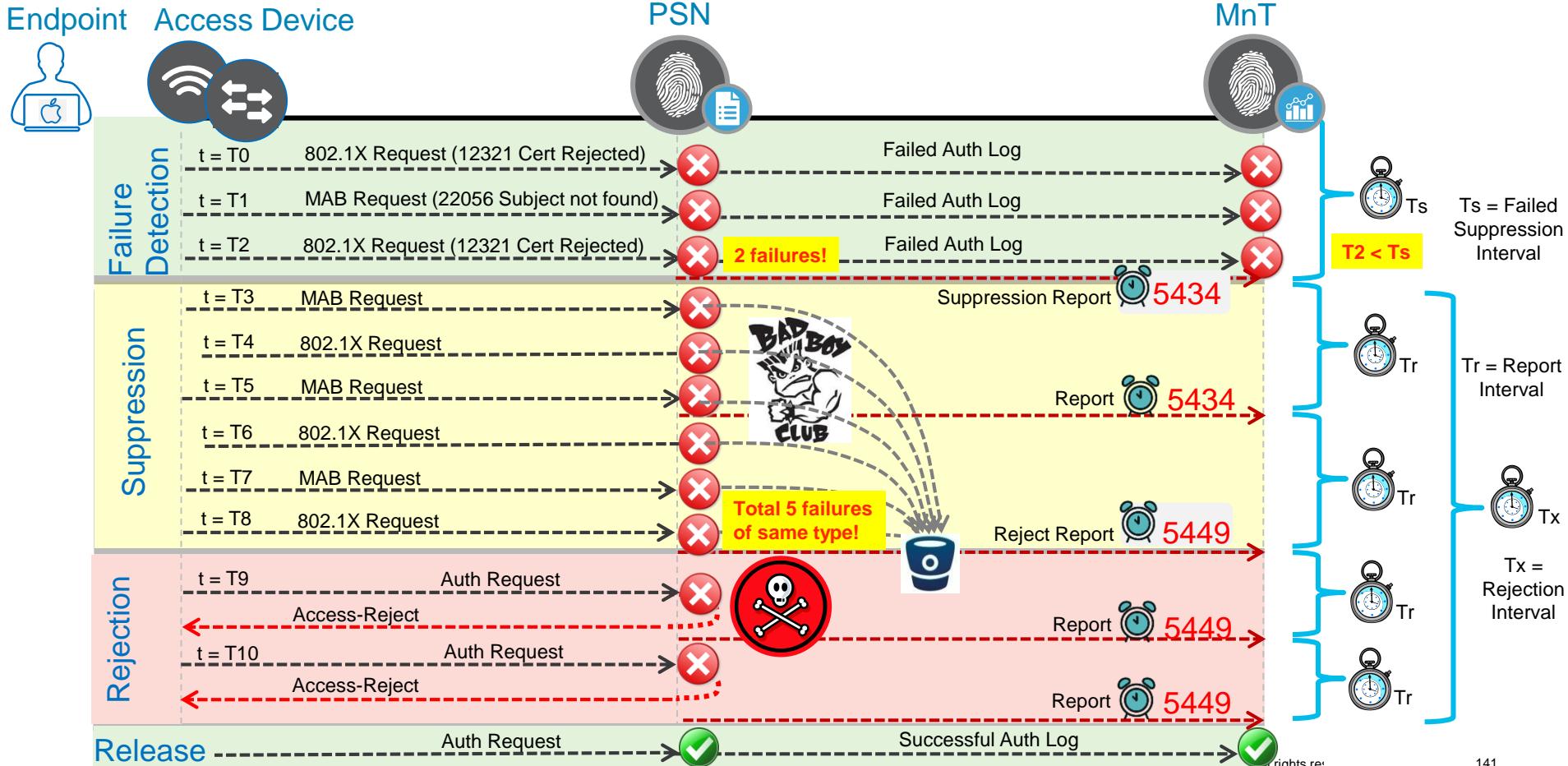
Highlight steps longer than ⓘ milliseconds (500 - 10,000)

Suppress Successful Reports
= Do not save **repeated successful auth events for the same session** to MnT DB

These events will not display in Live Authentications Log but do increment Repeat Counter.

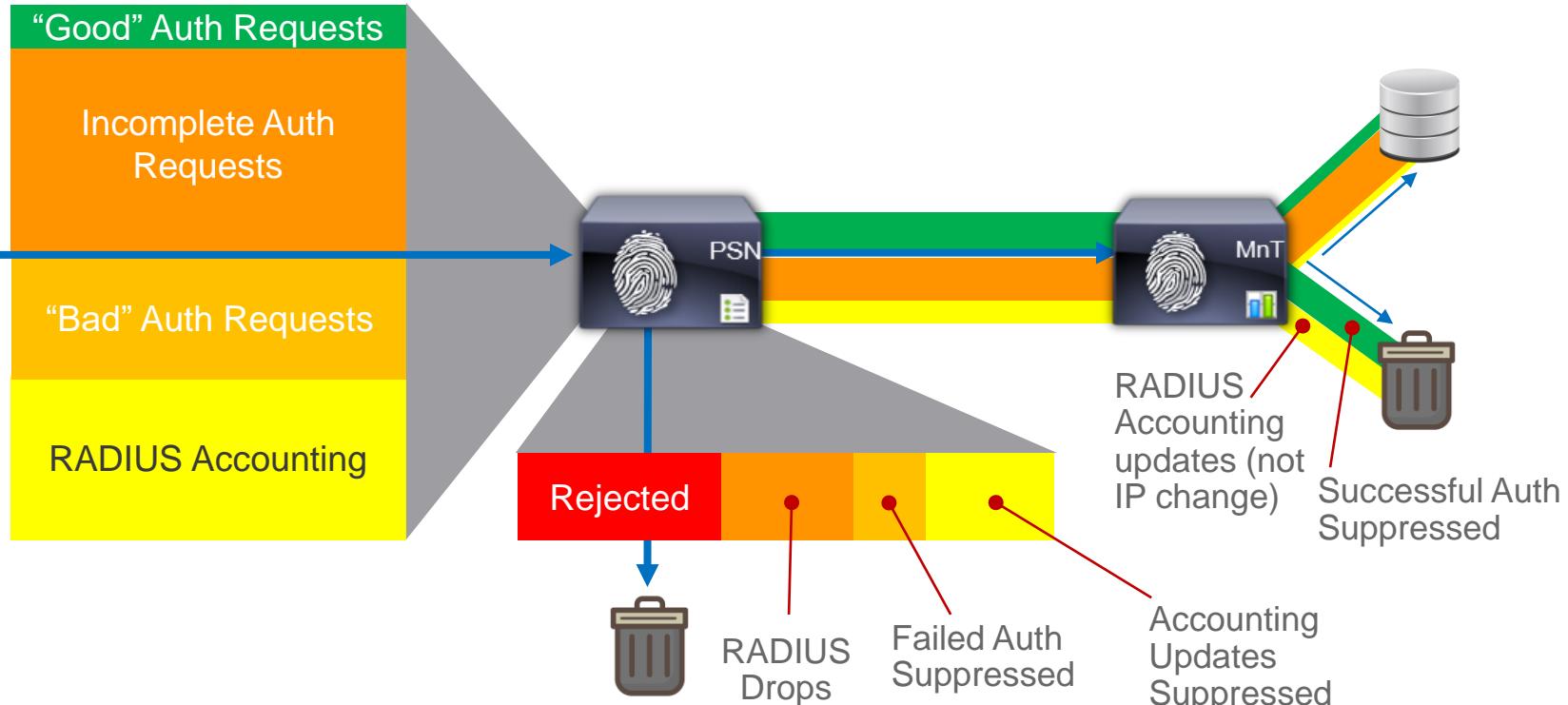
Detect NAD retransmission timeouts and Log auth steps > threshold.

Client Suppression and Reject Timers

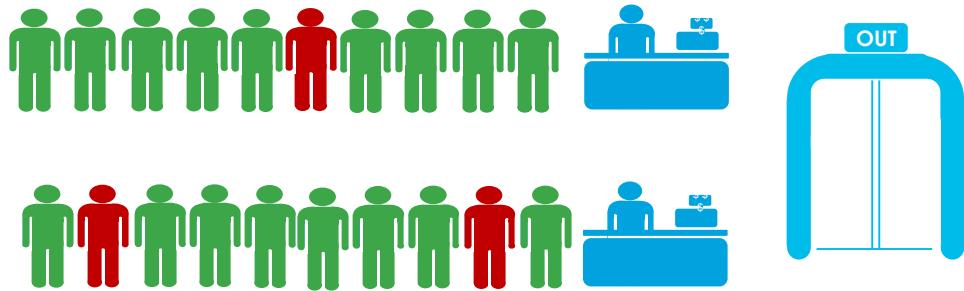
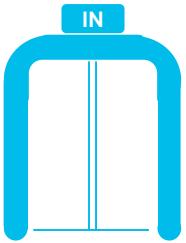


ISE Log Suppression

“Good”-put Versus “Bad”-put



Typical Load Example

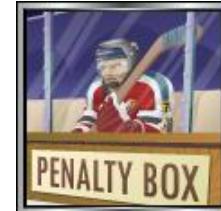


Extreme Noise Load Example



WLC – Client Exclusion

Blacklist Misconfigured or Malicious Clients



- **Excessive Authentication Failures**—Clients are excluded on the fourth authentication attempt, after three consecutive failures.
- Client excluded for Time Value specified in WLAN settings. Recommend increase to 1-5 min (60-300 sec). **3 min** is a good start.

MONITOR WLANS CONTROLLER WIRELESS SECURITY

WLANS > Edit 'BYOD-8021X'

General Security QoS Advanced

Client Exclusion ³ Enabled 60
Timeout Value (secs)

MONITOR WLANS CONTROLLER WIRELESS SECURITY

Client Exclusion Policies

Excessive 802.11 Association Failures
 Excessive 802.11 Authentication Failures
 Excessive 802.1X Authentication Failures
 IP Theft or IP Reuse
 Excessive Web Authentication Failures

Note: Diagrams show default values

Cisco live!

Live Authentications and Sessions

Screenshot of the Cisco Identity Services Engine (ISE) interface showing live authentications and sessions.

The interface includes navigation tabs: Home, Operations, Policy, Administration, and a search bar at the top right.

Key statistics displayed:

- Reconfigured Suplicants: 21
- Reconfigured Network Devices: 10
- RADIUS Dropped: 521
- Client Stopped Responding: 6716
- Repeat Counts: 19052

The main table displays live sessions with the following columns:

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-09-27 14:46:33.005	1	0	0	vipinj	CC:3A:61:12:ED:D5	Android-Samsung	
2013-09-27 14:46:30.890	1	0	11	aarondek	64:A3:CB:52:74:B1	Apple-iDevice	
2013-09-27 14:46:29.658	1	0	99	wekang	B8:78:2E:60:7F:14	Apple-iDevice	
2013-09-27 14:46:29.252	1	0	1	mutama	CC:78:5F:43:97:71	Apple-iDevice	
2013-09-27 14:46:25.595	1	0	0	jeffreedy	F0:CB:A1:75:31:4D	Apple-iPhone	
2013-09-27 14:46:25.595	1	0	0	jeffreedy	F0:CB:A1:75:31:4D	Apple-iPhone	WNBU_NGWC...
2013-09-27 14:46:22.636	1	0	0	jeffreedy	F0:CB:A1:75:31:4D	Apple-iPhone	WNBU-WLC1
2013-09-27 14:46:21.486	1	0	0	anonymous	00:1E:65:D6:93:E2		WNBU-WLC1
2013-09-27 14:46:18.884	1	0	7	dsladden	0C:77:1A:9A:F6:73	Apple-iPhone	

A red box highlights the most recent successful authentication entry (2013-09-27 14:46:21.486). A blue box highlights the same entry, with a callout note: "Blue entry = Most current Live Sessions entry with repeated successful auth counter".

Below the table, a section titled "Recent Events" shows log entries:

Event	Source IP	Destination IP	Protocol	Action	Session State	Auth Status	
1. user	70.11.24.89.14.44	WORKSTATION	NetApp	PermitAccess	Apple-iPhone	NetApp	NetApp
2. user	70.11.24.89.14.44	WNBU-WLC2	NetApp	PermitAccess	Apple-iPhone	NetApp	NetApp

Authentication Suppression

Enable/Disable

- **Global Suppression Settings:** Administration > System > Settings > Protocols > RADIUS

Failed Auth Suppression	Successful Auth Suppression
SUPPRESS ANOMALOUS CLIENTS <input checked="" type="checkbox"/> ⓘ	SUPPRESS REPEATED SUCCESSFUL AUTHENTICATIONS <input checked="" type="checkbox"/> ⓘ

Caution: Do not disable suppression in deployments with very high auth rates.

It is highly recommended to keep Auth Suppression enabled to reduce MnT logging

- **Selective Suppression using Collection Filters:** Administration > System > Logging > Collection Filters

Configure specific traffic to bypass Successful Auth Suppression

Useful for troubleshooting authentication for a specific endpoint or group of endpoints, especially in high auth environments where global suppression is always required.

Collection Filter List > [Calling-Station-ID](#)

Collection Filters

* Attribute	MAC Address
* Value	11:22:44:AA:BB:CC
* Filter Type	Disable Suppression
Save Filter All Filter Passed Filter Failed Disable Suppression	

Per-Endpoint Time-Constrained Suppression

Screenshot of the Cisco Identity Services Engine (ISE) Endpoint Protection Service interface.

The main dashboard shows the following statistics:

- Unconfigured Suplicants: 21
- Unconfigured Network Devices: 10
- RADIUS Dropped: 521
- Client Stopped Responding: 6716
- Total Repeat Counts: 19052

A table lists recent events:

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-09-27 14:46:33.005	Info	vipinj	0	CC:3A:61:12:ED:D5	Android-Samsung		
2013-09-27 14:46:30.890	Info	aarondek	11	64:A3:CB:52:74:B1	Apple-iDevice		

A context menu is open on the second row (aarondek):

- Endpoint Debug...
- Modify Collection Filters...
- Bypass Suppression Filtering for 1 hour** (highlighted with an orange box)
- Settings...
- Global Settings...
- About Adobe Flash Player 11.7.700.224...

A blue callout bubble with the text "Right Click" points to the "Bypass Suppression Filtering for 1 hour" option.

Below the table, a list of endpoint details is shown:

Identity	Profile	Access Status	Session State
CC:78:2E:60:7F:14	Apple-iDevice	NotApplicable	Authenticating
CC:78:5F:43:97:71	Apple-iPhone	NotApplicable	Authenticating
F0:CB:A1:75:31:4D	Apple-iPhone	NotApplicable	Authenticating
F0:CB:A1:75:31:4D	Apple-iPhone	NotApplicable	Authenticating
F0:CB:A1:75:31:4D	Apple-iPhone	NotApplicable	Authenticating
00:1E:65:D6:93:E2		NotApplicable	Authenticating
0C:77:1A:9A:F6:73	Apple-iPhone	NotApplicable	Authenticating

Visibility Into Reject Endpoints!

ISE 2.2+

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

Summary Endpoints Guests Vulnerability Threat + METRICS

Total Endpoints 59700 Active Endpoints 1325 Rejected Endpoints 193 Anomalous Behavior 7 Authenticated 0

A large red oval highlights the "Rejected Endpoints" section.

AUTHENTICATIONS

Identity Store Identity Group Network Device Failure Reason

ciscoad: [87.52%], inter...oints: [7.95%], otp_server: [4.38%], other: [<1%]

NETWORK DEVICES

Device Name Type Location

Device Name	Type	Location
sampg...-wlc1	[24.52%]	
sjc19...u-wlc	[19.68%]	
ntn01-11a-sw3	[17.97%]	
eng-b...a-sw1	[10.02%]	
sbg-b...-wlc1	[6.76%]	
sjc14...alwar	[6.59%]	
eng-b...a-sw1	[4.37%]	
rcdn5...ana1	[3.37%]	
other	[6.73%]	

ENDPOINTS

Type Profile

mobil...vices: [42.47%], misc: [27.11%], workstations: [24.72%], infra...vices: [2.75%], other: [2.95%]

The screenshot displays the ISE 2.2+ dashboard. At the top, a navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below this is a summary section with tabs for Summary, Endpoints, Guests, Vulnerability, and Threat, plus a '+' button. The 'Summary' tab is selected. The 'METRICS' section shows counts for Total Endpoints (59700), Active Endpoints (1325), Rejected Endpoints (193, highlighted by a large red oval), Anomalous Behavior (7), and Authenticated users (0). Below the metrics are three main sections: 'AUTHENTICATIONS' (Identity Store, Identity Group, Network Device, Failure Reason), 'NETWORK DEVICES' (Device Name, Type, Location), and 'ENDPOINTS' (Type, Profile). The 'AUTHENTICATIONS' section features a donut chart with segments for ciscoad, inter...oints, otp_server, and other. The 'NETWORK DEVICES' section lists network devices with their respective types and locations. The 'ENDPOINTS' section shows a donut chart with segments for mobil...vices, misc, workstations, infra...vices, and other.

Releasing Rejected Endpoints

ISE 2.2+

Screenshot of the Cisco Identity Services Engine (ISE) 2.2+ interface, specifically the Authentication tab under Endpoints.

The main view shows the **INACTIVE ENDPOINTS** section with a count of 3500. A modal window is open for endpoint **24:A0:74:F2:DE:DC**, which is currently **Rejected**. The status is shown as **Connected** with a green icon, but the button indicates it is **Rejected**.

The **AUTHENTICATION STATUS** section shows a pie chart of authentication failure reasons:

- other: [5.29%]
- 22056...re(s): [3.86%]
- 5440 ...d new: [4.73%]
- 12937...ssage: [7%]
- 12930...ssage: [17.02%]
- 24408...sword: [22.9%]

The **AUTHENTICATIONS** section displays a table of authentication failure details:

Failure Reason	Identity Store	Identity Group
12937 Suplicant stopped responding	LR-B...	Unknown
24408 User authentication against A...	JC19 → Apple-Device	Apple-iDevice
12934 Suplicant stopped respondi...	-	-

At the bottom, there are buttons for **Release Rejected** and **Revoke Certificate**.

Releasing Rejected Endpoints

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below this, the Endpoints tab is selected, with sub-options for Authentication, BYOD, Compliance, Compromised Endpoints, Endpoint Classification, Guest, and Vulnerable Endpoints.

The main content area displays two sections: "INACTIVE ENDPOINTS" and "AUTHENTICATION STATUS". The "INACTIVE ENDPOINTS" section shows a list of MAC addresses. One entry, "E4:98:D6:1C:7C:6C", is highlighted with a blue selection box and has a red minus sign icon next to it, indicating a rejected state. A hand cursor is positioned over this minus sign icon.

The "AUTHENTICATION STATUS" section includes a table of failure reasons:

Failure Reason	Identity Store	Identity Group
other: [5.29%]		
22056...re(s): [3.86%]		
5440 ...d new: [4.73%]		
12937...ssage: [7%]		

A large blue callout box highlights the "Rejected" status of the selected MAC address and contains the text "Release Rejected". Another yellow callout box at the bottom right states "Query/Release Rejected also available via ERS API!".

At the bottom of the screen, there is footer information including IP addresses (60:F1:89:4C:FD:12, 10.33.248.143), names (znajmudd, ZSARIEDD...), and service names (SJC, OEAP).

No Log Suppression



With Log Suppression



Distributed Logging



High Availability

High Availability Agenda

- ISE Appliance Redundancy
- ISE Node Redundancy
 - Administration Nodes
 - Monitoring Nodes
 - pxGrid Nodes
- HA for Certificate Services
- Policy Service Node Redundancy
 - Load Balancing
 - Non-LB Options
- NAD Fallback and Recovery

ISE Appliance Redundancy

Appliance Redundancy

In-Box High Availability

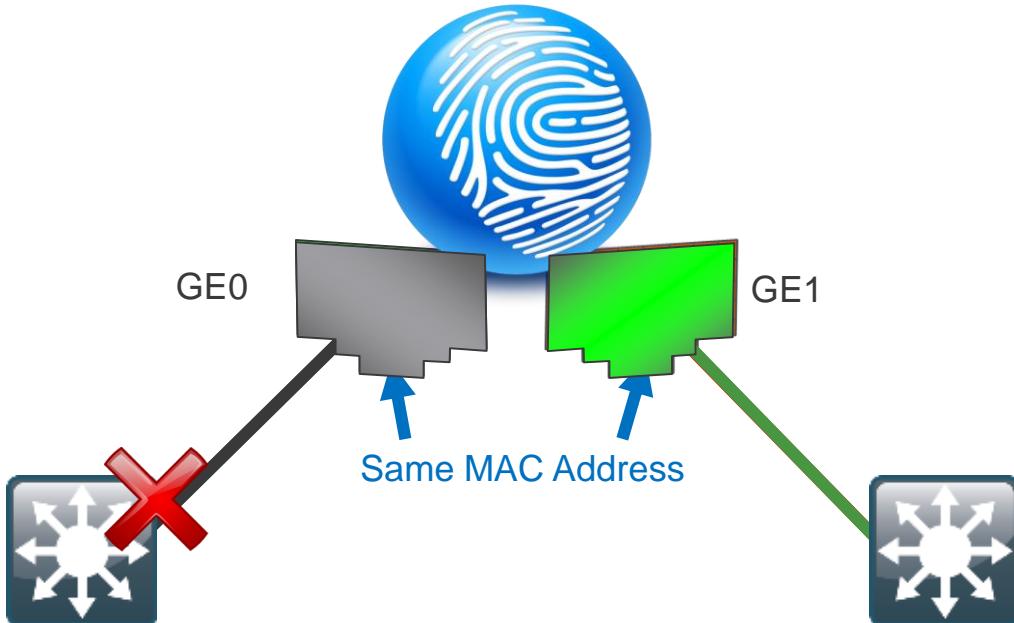
SNS-3500 Series

Platform	SNS-3415 (34x5 Small)	SNS-3495 (34x5 Large)	SNS-3515 (35x5 Small)	SNS-3595 (35x5 Large)
Drive Redundancy	No (1) 600GB disk	Yes (2) 600-GB	No (1) 600GB disk	Yes (4) 600GB disk
Controller Redundancy	No	Yes (RAID 1)	No (1GB FBWC Controller Cache)	Yes (RAID 10) (1GB FBWC Cache)
Ethernet Redundancy	Yes* 4 GE NICs = Up to 2 bonded NICs	Yes* 4 GE NICs = Up to 2 bonded NICs	Yes* 6 GE NICs = Up to 3 bonded NICs	Yes* 6 GE NICs = Up to 3 bonded NICs
Redundant Power	No (2 nd PSU optional) UCSC-PSU-650W	Yes	No (2 nd PSU optional) UCSC-PSU1-770W	Yes

* ISE 2.1 introduced NIC Teaming support for High Availability only (not active/active)

Bonded Interfaces for Redundancy

When GE0 is Down, GE1 Takes Over



- Both interfaces assume the same L2 address.
- When GE0 fails, GE1 assumes the IP address and keeps the communications alive.
- Based on Link State of the Primary Interface
- Every 100 milliseconds the link state of the Primary is inspected.

NIC Teaming

NIC Teaming / Interface Bonding

- Configured using CLI only!
- GE0 + GE1 Bonding Example:
admin (config-GigabitEthernet0) # **backup interface GigabitEthernet 1**
- Requires service restart. After restart, ISE recognises bonded interfaces for Deployment and Profiling; Guest requires manual config of eligible interfaces.

Edit Node

General Settings Profiling Configuration

DHCP

Interface	bond0
Port	bond0
Description	GigabitEthernet 2
	GigabitEthernet 3
	All



Allowed Make selections in one or both columns based on your PSN configurations.

interfaces: If bonding is not configured i on a PSN, use:

Gigabit Ethernet 0
 Gigabit Ethernet 1
 Gigabit Ethernet 2
 Gigabit Ethernet 3
 Gigabit Ethernet 4
 Gigabit Ethernet 5

If bonding is configured i on a PSN, use:

Bond 0 Uses Gigabit Ethernet 0 as primary, 1 as backup.
 Bond 1 Uses Gigabit Ethernet 2 as primary, 3 as backup.
 Bond 2 Uses Gigabit Ethernet 4 as primary, 5 as backup.

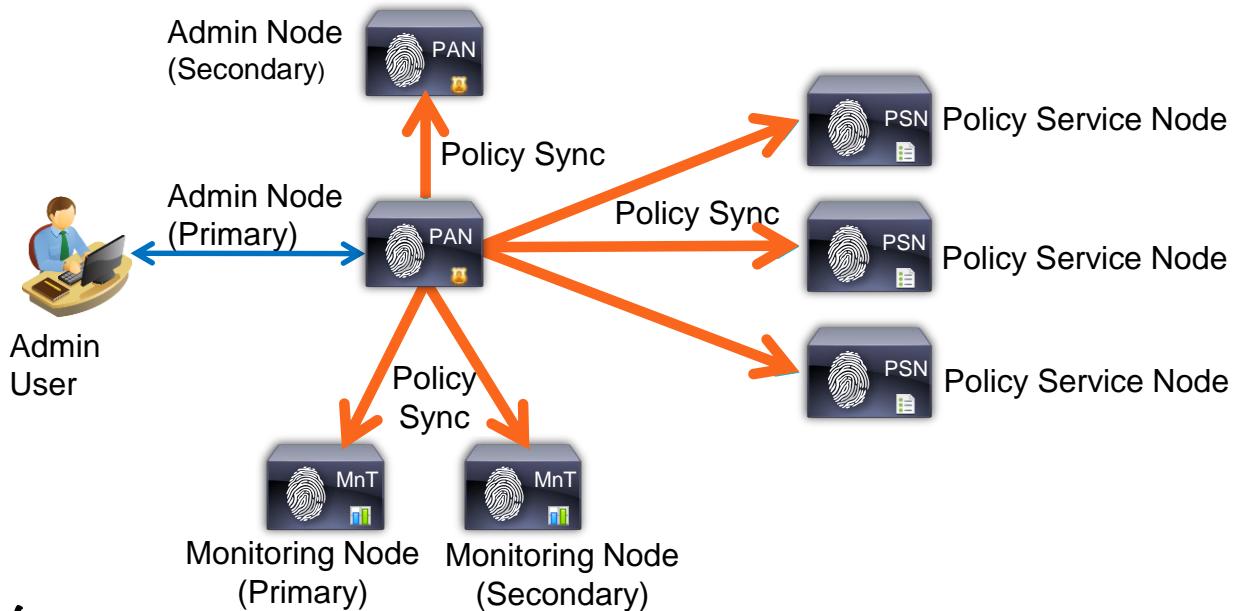
ISE Node/Persona Redundancy

Admin Node HA and Synchronisation

PAN Steady State Operation

- Maximum two PAN nodes per deployment
- Active / Standby

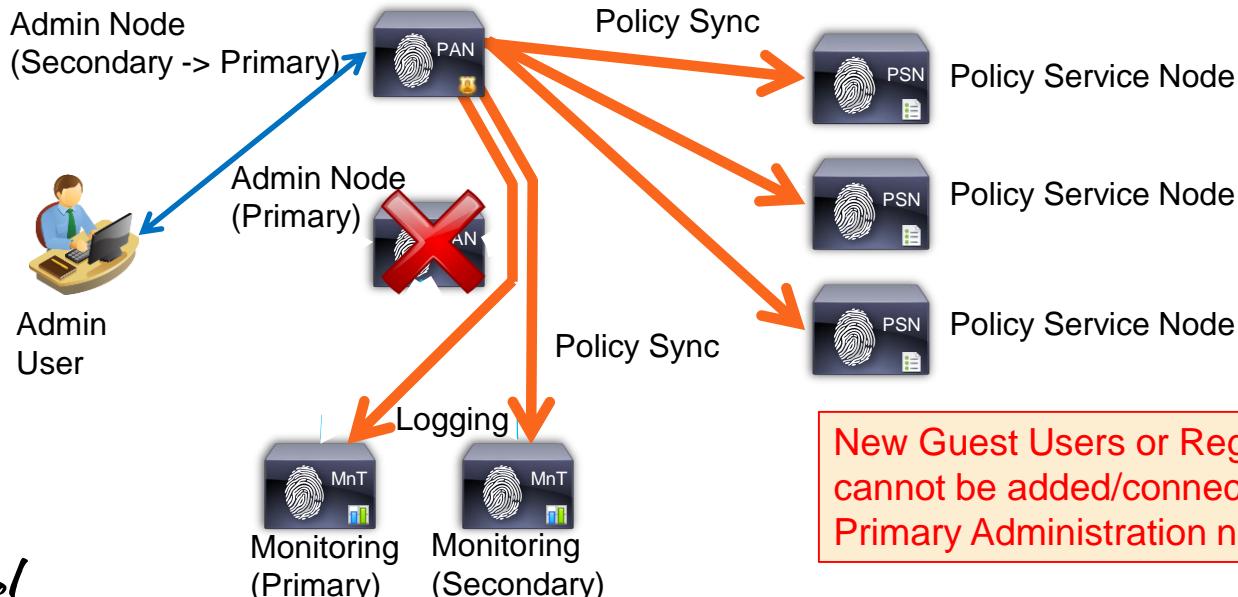
- Changes made to Primary Administration DB are automatically synced to all nodes.



Admin Node HA and Synchronisation

Primary PAN Outage and Recovery

- Prior to ISE 1.4, upon Primary PAN failure, admin user must connect to Secondary PAN and **manually promote** Secondary to Primary; new Primary syncs all new changes.
- PSNs buffer endpoint updates if Primary PAN unavailable; buffered updates sent once PAN available.

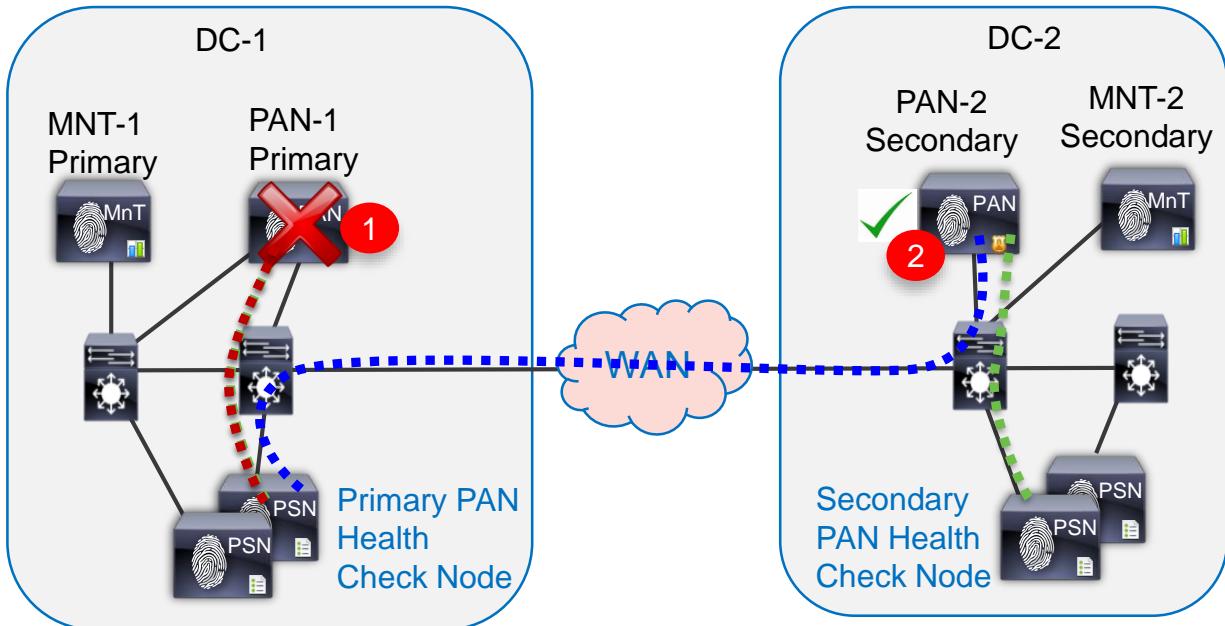


Automatic PAN Switchover

Introduced ISE 1.4

Don't forget, after switchover
admin must connect to PAN-2
for ISE management!

- Primary PAN (PAN-1) down or network link down.
- If Health Check Node unable to reach PAN-1 but can reach PAN-2 → trigger failover
- Secondary PAN (PAN-2) is promoted by Health Check Node
- PAN-2 becomes Primary and takes over PSN replication.



Note: Switchover is NOT immediate. Total time based on polling intervals and promotion time.
Expect ~15 - 30 minutes.

PAN Failover

Health Check Node Configuration

- Configuration using GUI only under [Administration > System > Deployment > PAN Failover](#)

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Operations, Policy, Guest Access, and Administration. Below the navigation is a toolbar with System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Deployment (selected), Licensing, Certificates, Logging, Maintenance, Backup & Restore, Admin Access, and Settings.

The main content area is titled "PAN Failover Configuration" with the sub-instruction "Automatic Failover if Primary Administration node goes down." A red box highlights the configuration fields:

- * Enable PAN Auto Failover:
- * Primary Health Check Node: npf-sjca-mnt01.cisco.com (with a tooltip for Primary Administration Node)
- * Secondary Health Check Node: npf-sjca-mnt02.cisco.com (with a tooltip for Secondary Administration Node)
- * Polling Interval: 120 (with a tooltip for Seconds (Range 30 - 300))
- * Number Of Failure Polls Before Failover: 5 (with a tooltip for Count (Range 2 - 60))

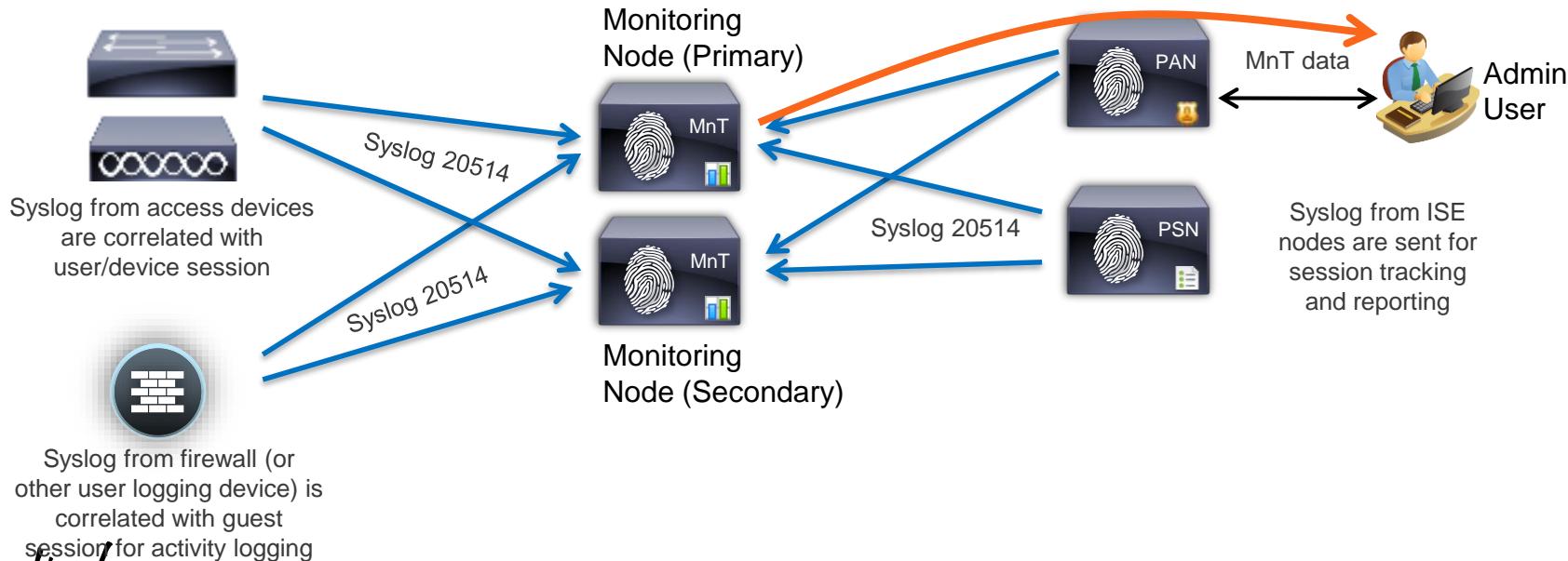
A blue callout box points to the Primary Health Check Node field with the text "Health Check Node CANNOT be a PAN !!". Another blue callout box at the bottom right points to the Number Of Failure Polls Before Failover field with the text "Requires Minimum of 3 nodes – 3rd node is independent observer".

HA for Monitoring and Troubleshooting

Steady State Operation

- Maximum two MnT nodes per deployment
- Active / Active

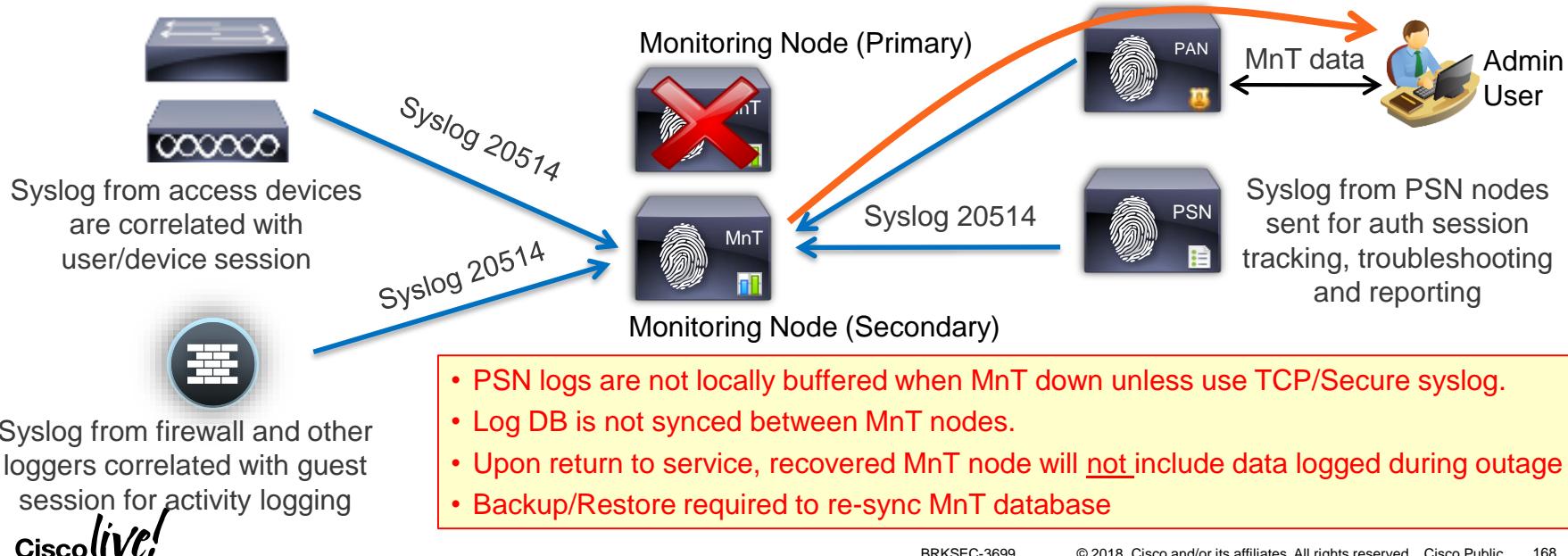
- MnT nodes concurrently receive logging from PAN, PSN, NAD, and ASA
- PAN retrieves log/report data from Primary MnT node when available



HA for Monitoring and Troubleshooting

Primary MnT Outage and Recovery

- Upon MnT node failure, PAN, PSN, NAD, and ASA continue to send logs to remaining MnT node
- PAN auto-detects Active MnT failure and retrieves log/report data from Secondary MnT node.
- Full failover to Secondary MnT may take from 5-15 min depending on type of failure.



HA for pxGrid v1

Steady State

PAN Publisher Topics:

- Controller Admin
- TrustSec/SGA
- Endpoint Profile

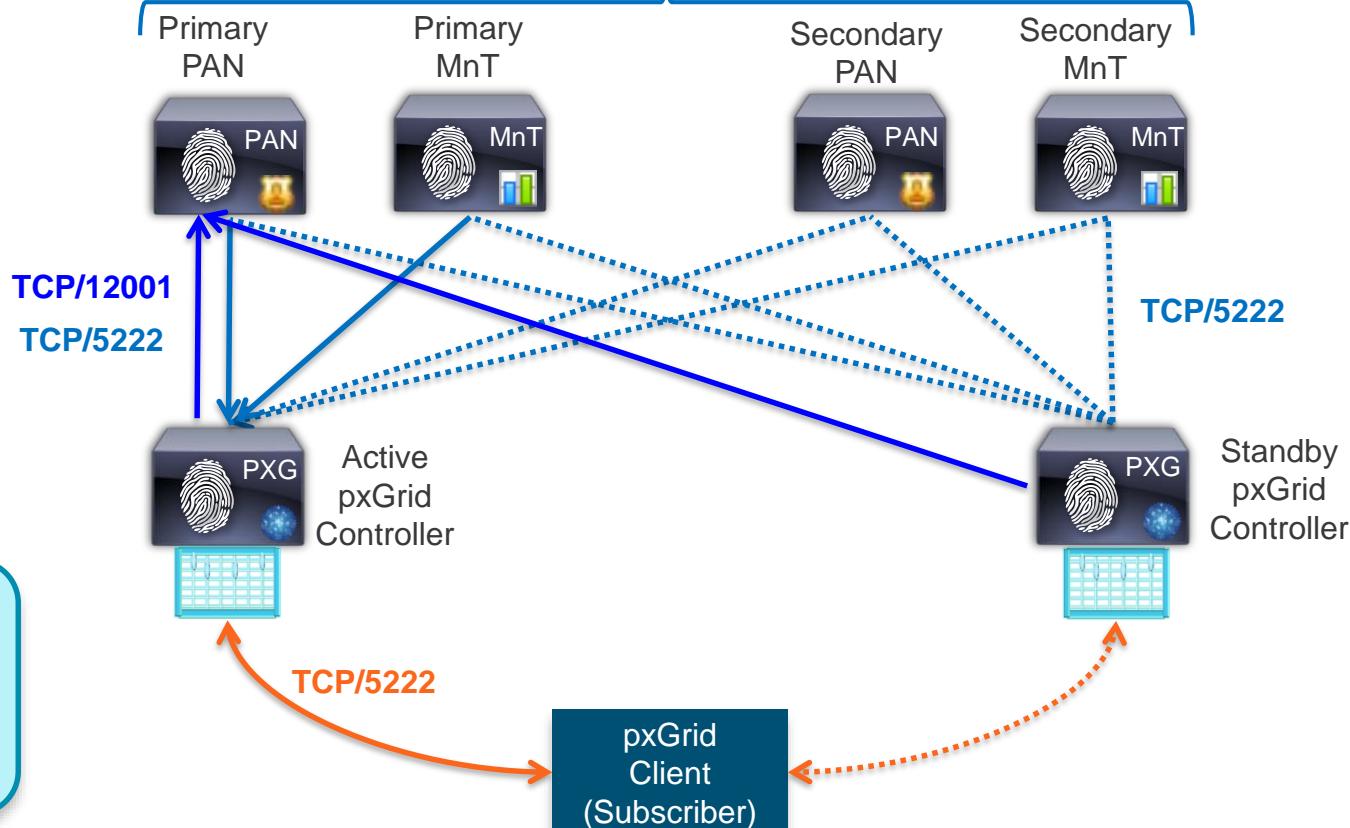
MnT Publisher Topics:

- Session Directory
- Identity Group
- ANC (EPS)

- pxGrid clients can be configured with up to 2 servers.
- Clients connect to single active controller

pxGrid
Clients
(Publishers)

- Max two pxGrid v1 nodes per deployment
(Active/Standby)



HA for pxGrid v1

Failover and Recovery

pxGrid
Clients
(Publishers)

- Max two pxGrid v1 nodes per deployment
(Active/Standby)

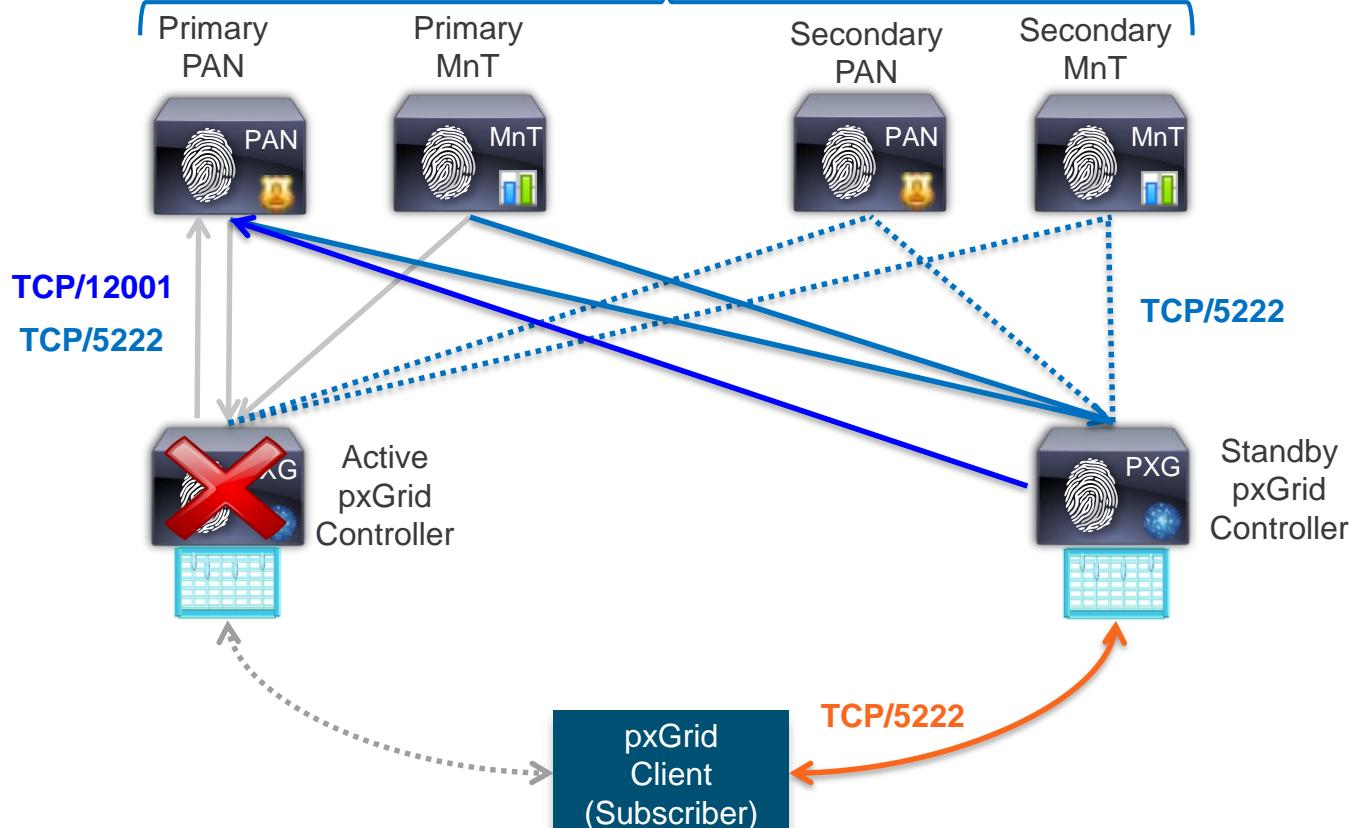
PAN Publisher Topics:

- Controller Admin
- TrustSec/SGA
- Endpoint Profile

MnT Publisher Topics:

- Session Directory
- Identity Group
- ANC (EPS)

If active pxGrid Controller fails, clients automatically attempt connection to standby controller.



HA for pxGrid v2 (ISE 2.3+)

Steady State

pxGrid
Clients
(Publishers)

- 2.3: Max two pxGrid v2 nodes/deployment (**Active/Active**)
- 2.4: Max 4 nodes (**All Active**)

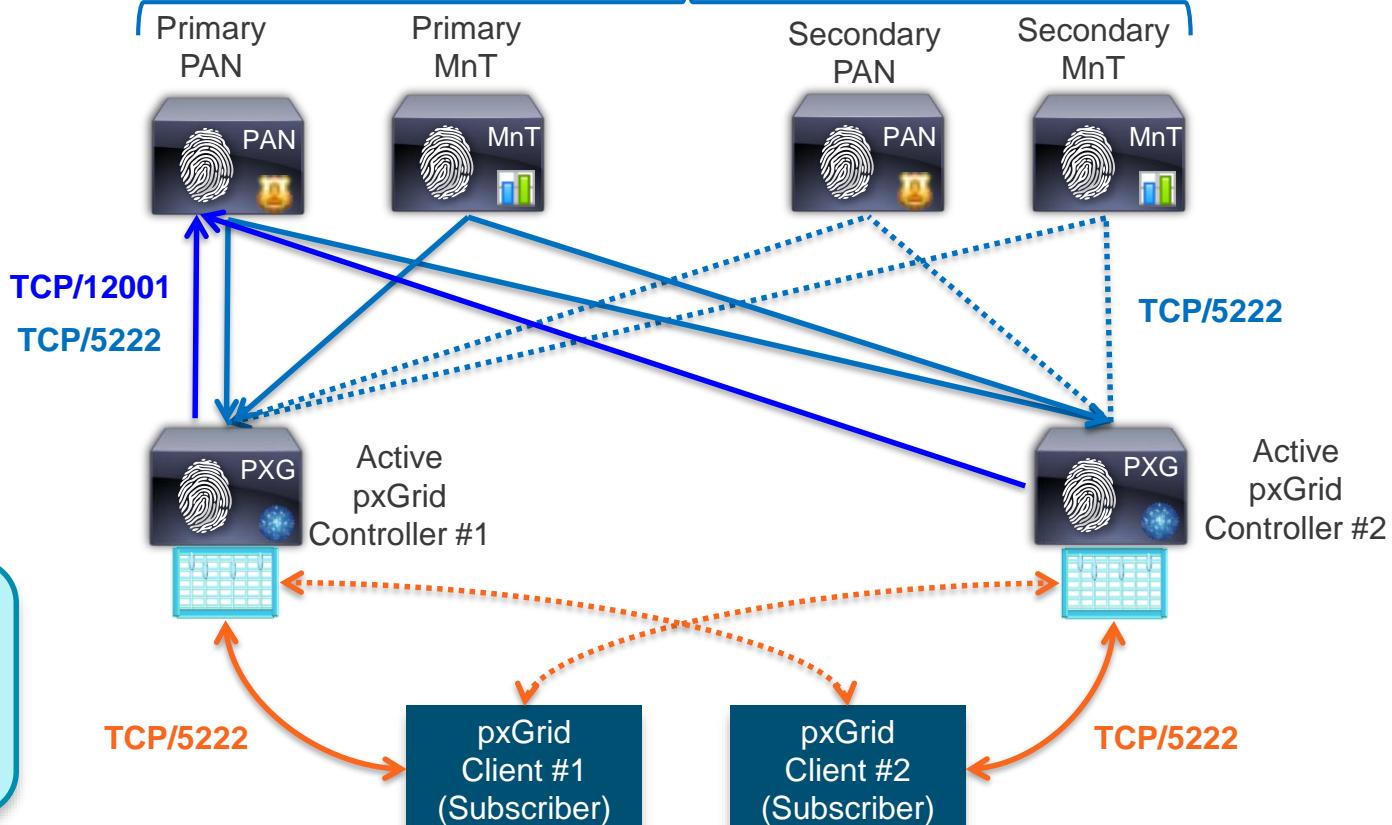
PAN Publisher Topics:

- Controller Admin
- TrustSec/SGA
- Endpoint Profile

MnT Publisher Topics:

- Session Directory
- Identity Group
- ANC (EPS)

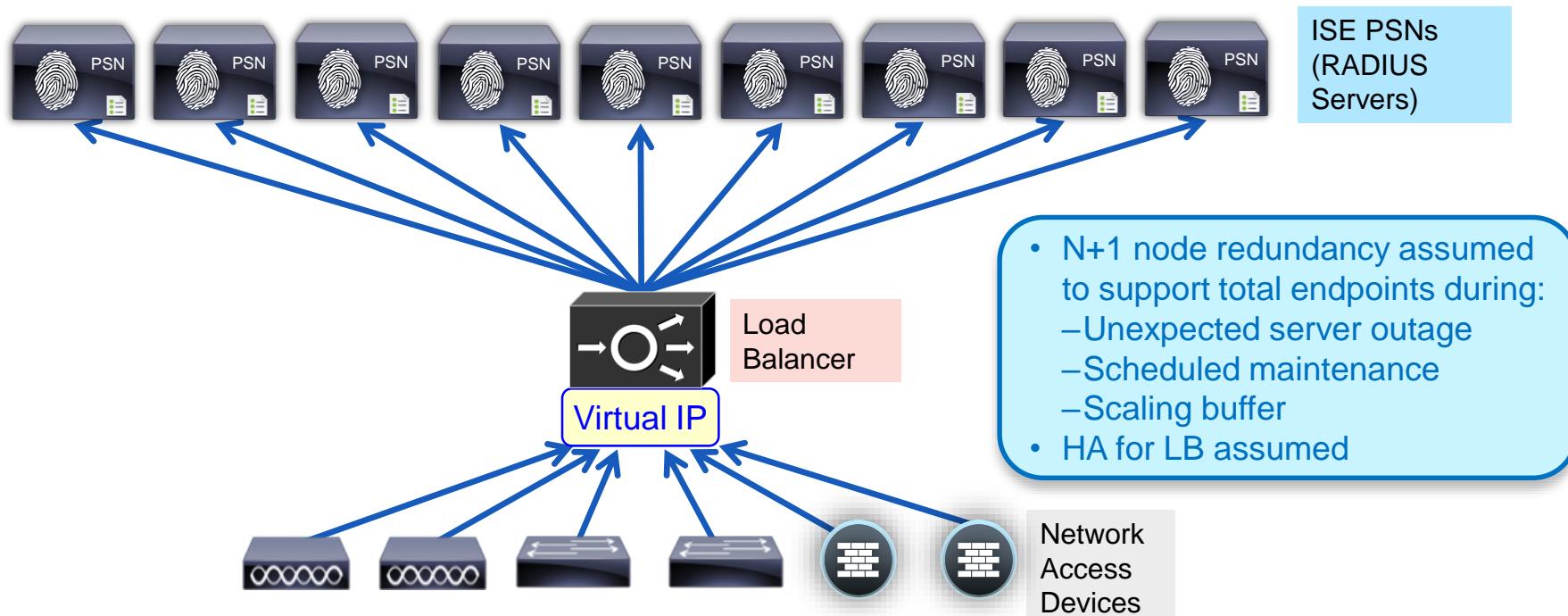
- pxGrid clients can be configured with up to 2 controllers.
- Clients connect to any 2 controllers



PSN Load Balancing

Load Balancing RADIUS, Web, and Profiling Services

- Policy Service nodes can be configured in a cluster behind a load balancer (LB).
- Access Devices send RADIUS AAA requests to LB virtual IP.

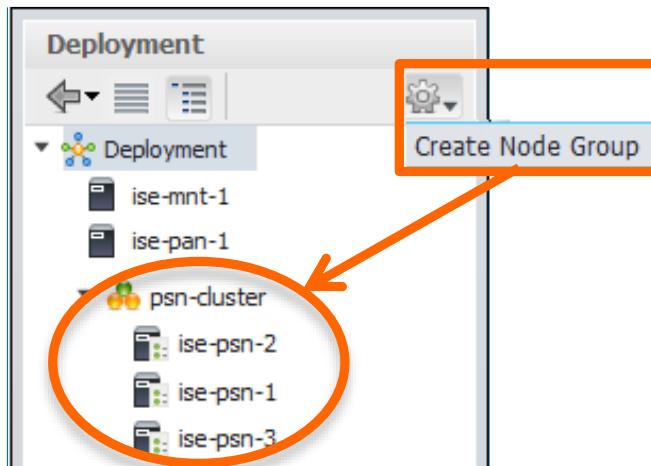


Configure Node Groups for LB Cluster

All PSNs in LB Cluster in Same Node Group

- Administration > System > Deployment

1) Create node group



- Node group members can be L2 or L3
- Multicast no longer a requirement since ISE 1.3

2) Assign name (and multicast address if ISE 1.2)

Create Node Group

* Node Group Name: psn_cluster

Description: Data Center - F5 LB Cluster

Submit Reset

3) Add individual PSNs to node group

Edit Node

General Settings Profiling Configuration

Policy Service

Enable Session Services

Include Node in Node Group psn-cluster

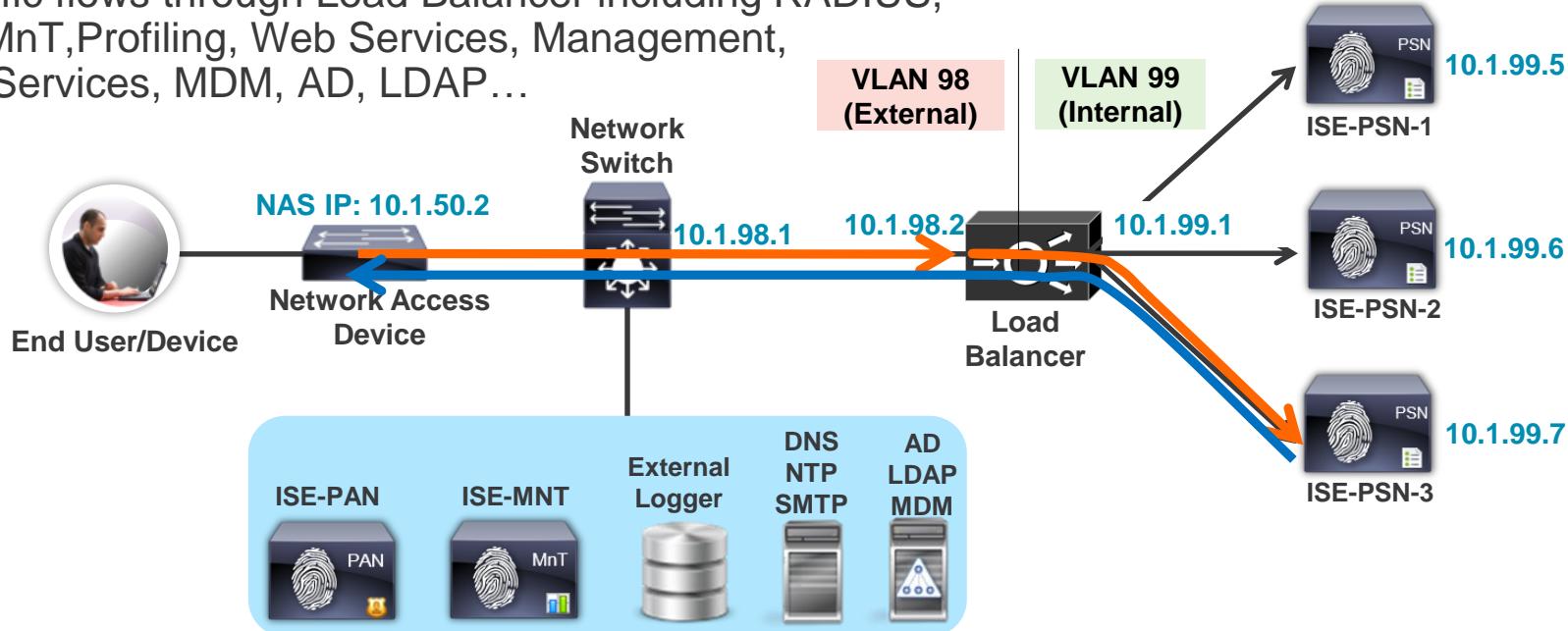
Enable Profiling Service

Traffic Flow—Fully Inline: Physical Separation

Physical Network Separation Using Separate LB Interfaces

- Load Balancer is directly inline between PSNs and rest of network.
- All traffic flows through Load Balancer including RADIUS, PAN/MnT, Profiling, Web Services, Management, Feed Services, MDM, AD, LDAP...

Fully Inline Traffic Flow
recommended—
physical or logical



Load Balancing Policy Services

- **RADIUS AAA Services**

Packets sent to LB virtual IP are load-balanced to real PSN based on configured algorithm. Sticky algorithm determines method to ensure same Policy Service node services same endpoint.

- **Web Services:**

- **URL-Redirected:** Posture (CPP) / Central WebAuth (CWA) / Native Supplicant Provisioning (NSP) / Hotspot / Device Registration WebAuth (DRW), Partner MDM.

No LB Required! PSN that terminates RADIUS returns URL Redirect with its own certificate CN name substituted for 'ip' variable in URL.

- **Direct HTTP/S: Local WebAuth (LWA) / Sponsor / MyDevices Portal, OCSP**

Single web portal domain name should resolve to LB virtual IP for http/s load balancing.

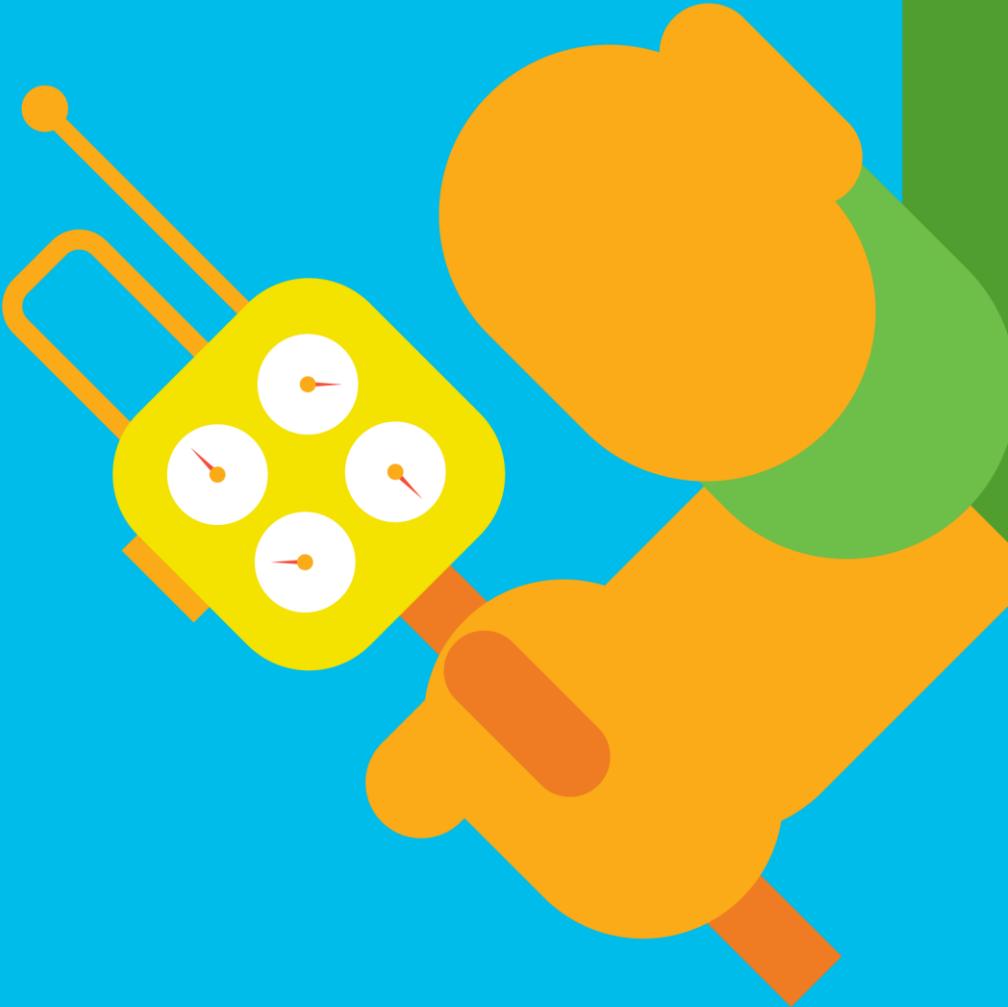
- **Profiling Services: DHCP Helper / SNMP Traps / Netflow / RADIUS**

LB VIP is the target for one-way Profile Data (no response required). VIP can be same or different than one used by RADIUS LB; Real server interface can be same or different than one used by RADIUS

- **TACACS+ AAA Services: (Session and Command Auth and Accounting)**

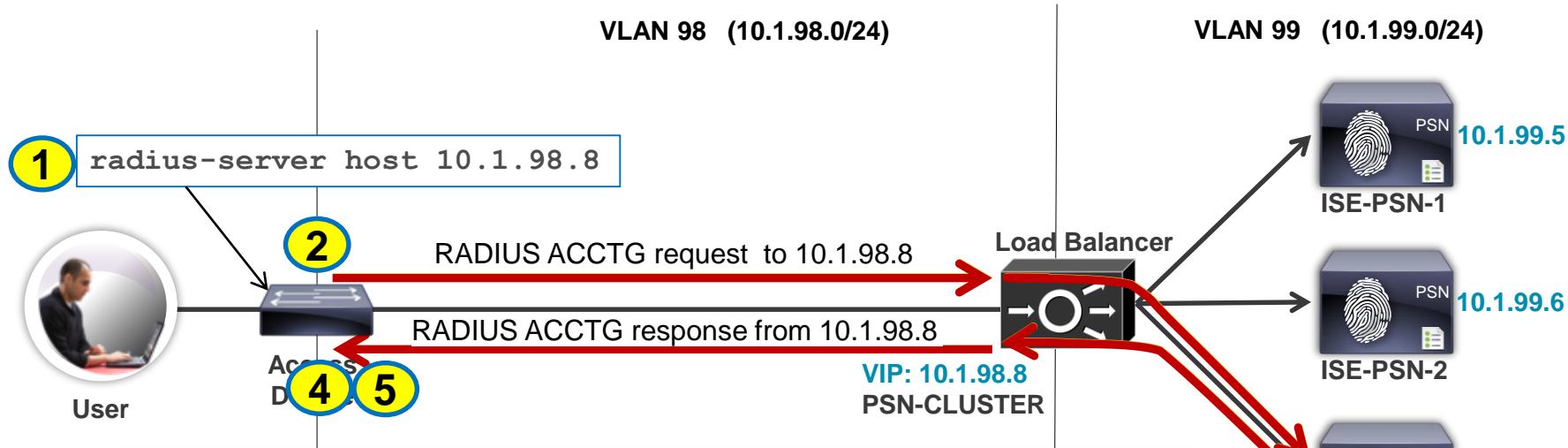
LB VIP is target for TACACS+ requests. T+ not session based like RADIUS, so not required that requests go to same PSN

Load Balancing RADIUS



Load Balancing RADIUS

Sample Flow



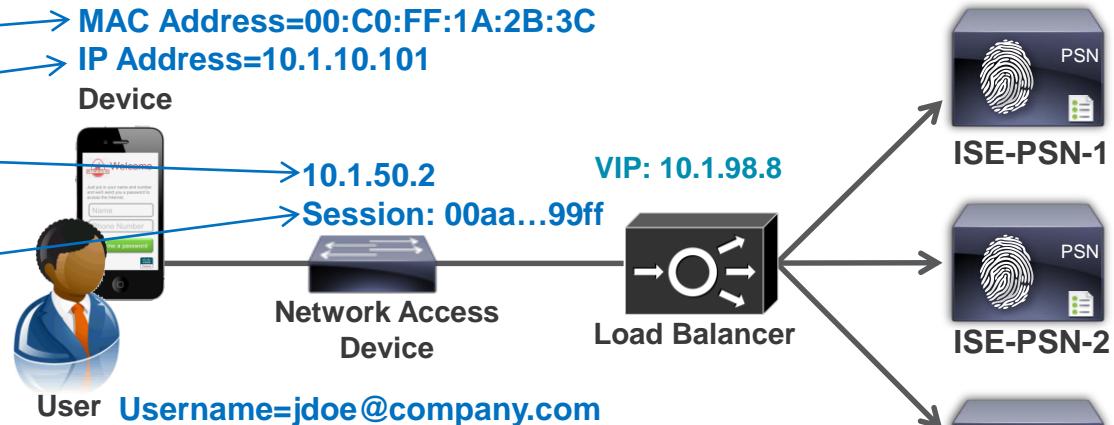
1. NAD has single RADIUS Server defined (10.1.98.8)
2. RADIUS Auth requests sent to VIP @ 10.1.98.8
3. Requests for same endpoint load balanced to same PSN via sticky based on RADIUS Calling-Station-ID and Framed-IP-Address
4. RADIUS response received from VIP @ 10.1.98.8
(originated by real server ise-psn-3 @ 10.1.99.7 and source translated by LB)
5. RADIUS Accounting sent to/from same PSN based on sticky

Load Balancer Persistence (Stickiness) Guidelines

Persistence Attributes

- Common RADIUS Sticky Attributes

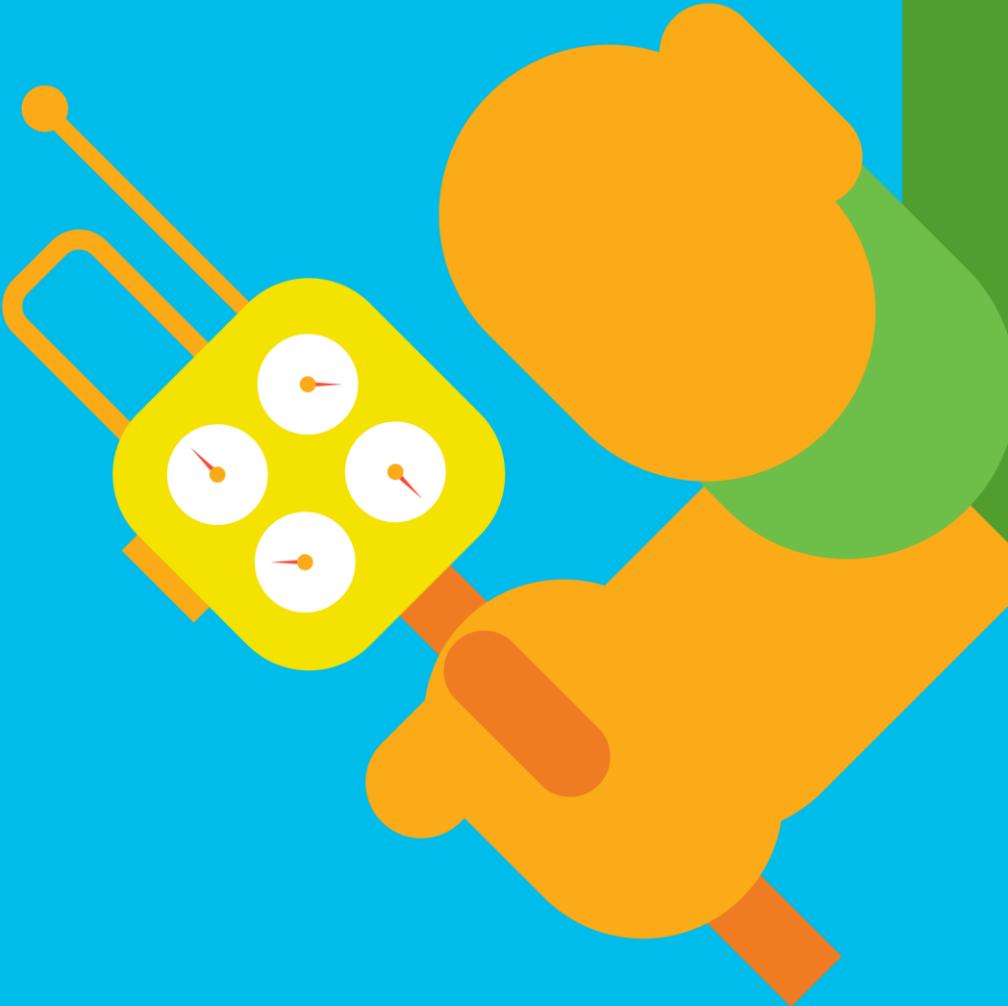
- Client Address
 - Calling-Station-ID
 - Framed-IP-Address
- NAD Address
 - NAS-IP-Address
 - Source IP Address
- Session ID
 - RADIUS Session ID
 - Cisco Audit Session ID



- Best Practice Recommendations (depends on LB support and design)

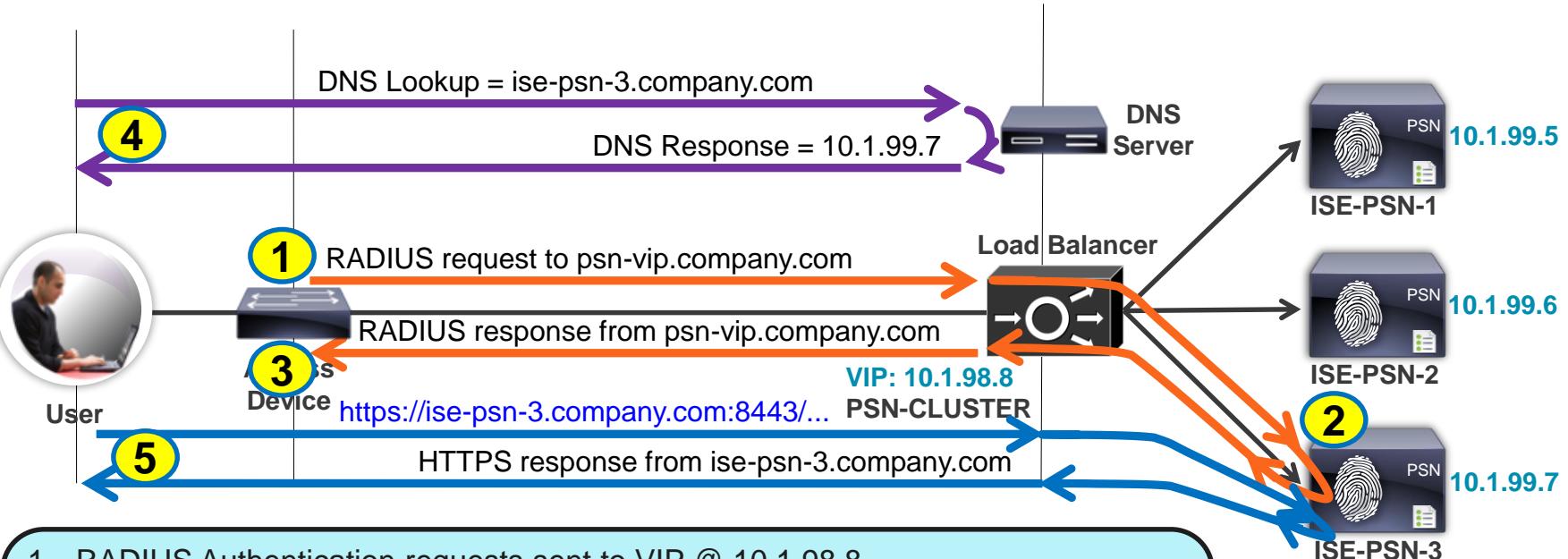
1. Calling-Station-ID for persistence across NADs and sessions
2. Source IP or NAS-IP-Address for persistence for all endpoints connected to same NAD
3. Audit Session ID for persistence across re-authentications

Load Balancing ISE Web Services



Load Balancing with URL-Redirection

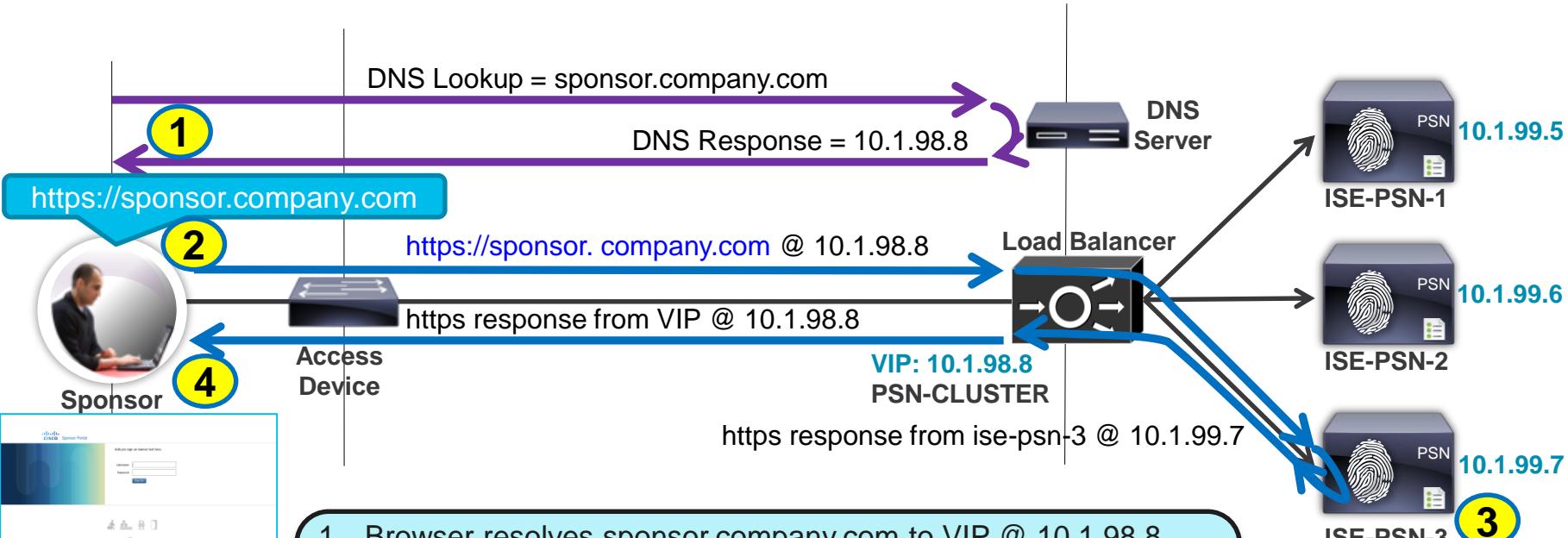
URL Redirect Web Services: Hotspot/DRW, CWA, BYOD, Posture, MDM



1. RADIUS Authentication requests sent to VIP @ 10.1.98.8
2. Requests for same endpoint load balanced to same PSN via RADIUS sticky.
3. RADIUS Authorisation received from VIP @ 10.1.98.8 (originated by ise-psn-3 @ 10.1.99.7 with URL Redirect to [https://ise-psn-3.company.com:8443/...](https://ise-psn-3.company.com:8443/)).
4. Client browser redirected and resolves FQDN in URL to real server address.
5. User sends web request directly to same PSN that serviced RADIUS request.

Load Balancing Non-Redirected Web Services

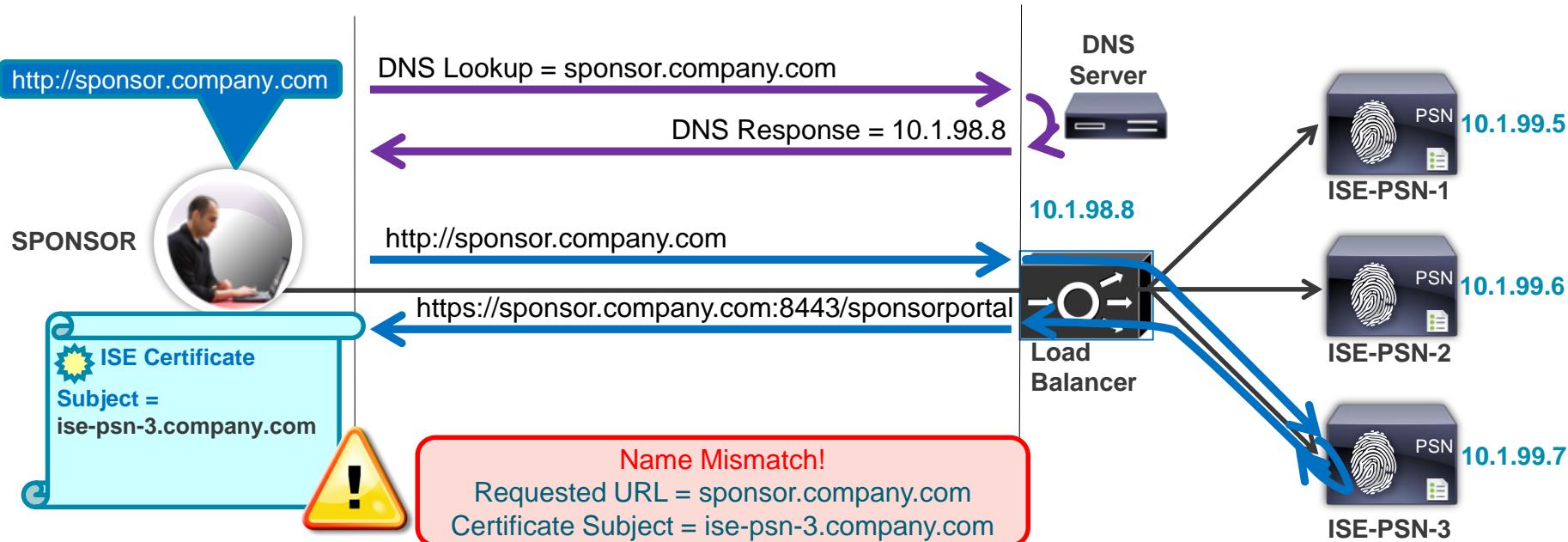
Direct Web Services: Sponsor, My Devices, LWA, OCSP



1. Browser resolves `sponsor.company.com` to VIP @ `10.1.98.8`
2. Web request sent to `https://sponsor.company.com` @ `10.1.98.8`
3. ACE load balances request to PSN based on IP or HTTP sticky
4. HTTPS response received from `ise-psn-3` @ `10.1.99.7` → translated to VIP @ `10.1.98.8` when passes through LB.

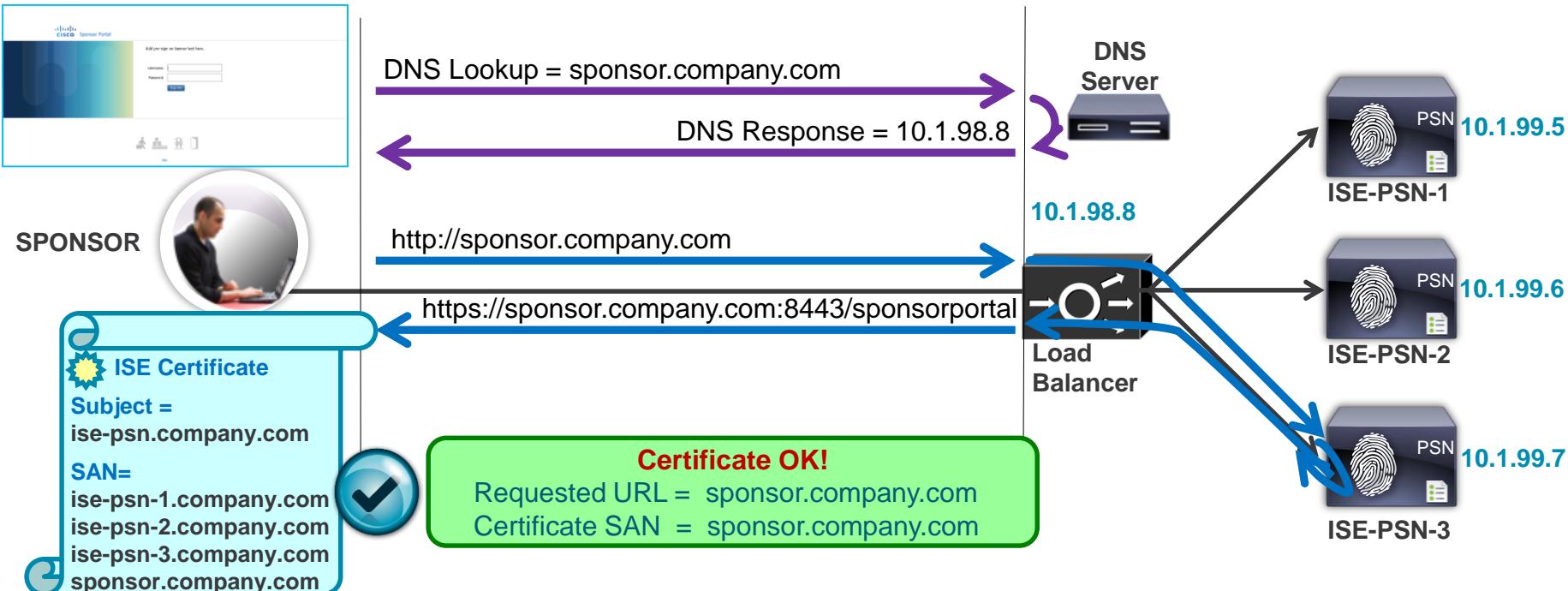
ISE Certificate without SAN

Certificate Warning - Name Mismatch



ISE Certificate with SAN

No Certificate Warning



“Universal Certs”

UCC or Wildcard SAN Certificates

Subject Alternative Name (SAN)

DNS Name	psn.ise.company.com
DNS Name	*.ise.company.com

Allow Wildcard Certificates ⓘ

Check box to use wildcards

Node(s)

Generate CSR's for these Nodes:

Node

ise-psn

Subject

Common Name (CN)

\$FQDN\$

CSR Friendly Name

ise-psn/Admin

CN must also exist in SAN

Organizational Unit (OU)

SBG

Organization (O)

Cisco

City (L)

RTP

State (ST)

NC

Country (C)

US

Universal Cert options:

- UCC / Multi-SAN
- Wildcard SAN

Subject Alternative Name (SAN)

DNS Name

ise-psn.company.com

DNS Name

mydevices.company.com

DNS Name

sponsor.company.com

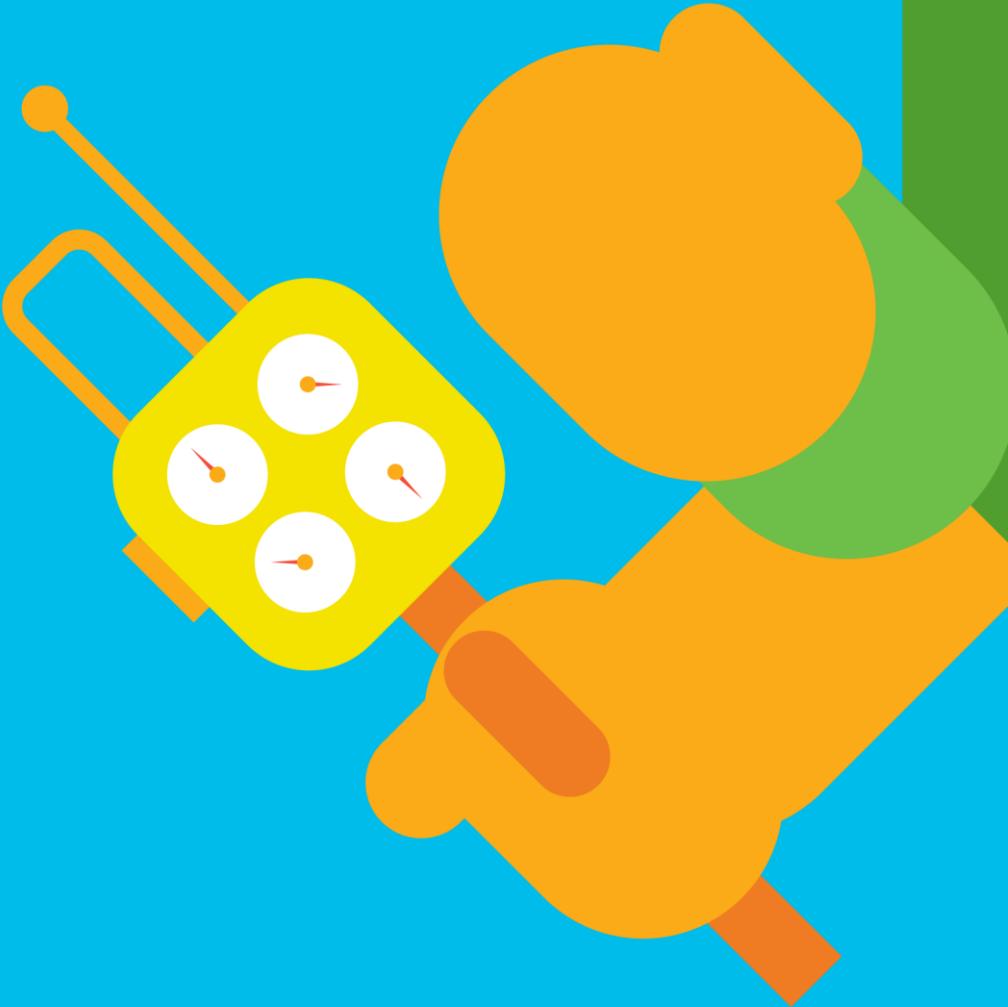
IP Address

192.168.254.99

Other FQDNs or wildcard
as “DNS Names”

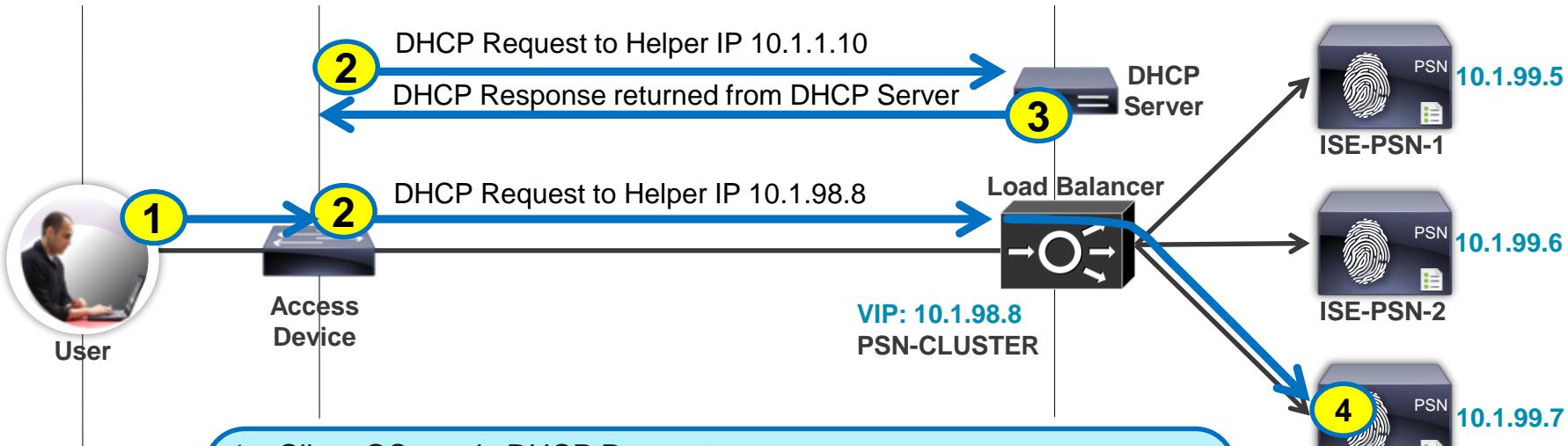
IP Address is also option

Load Balancing ISE Profiling Services



Load Balancing Profiling Services

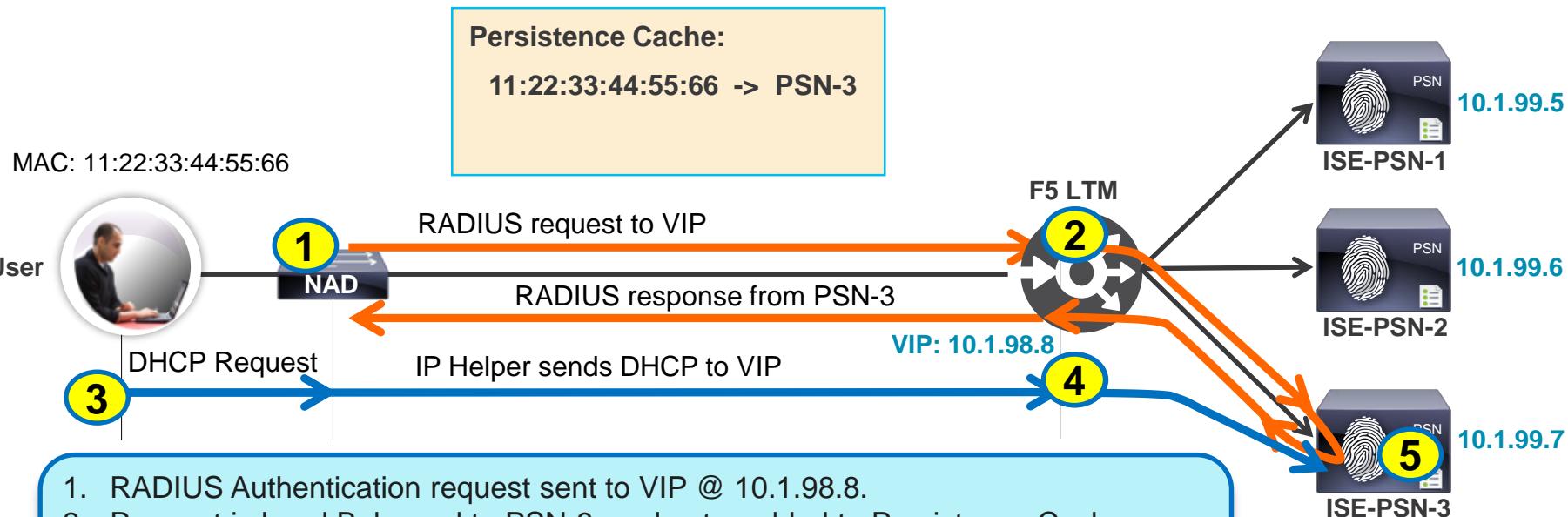
Sample Flow



1. Client OS sends DHCP Request
2. Next hop router with IP Helper configured forwards DHCP request to real DHCP server and to secondary entry = LB VIP
3. Real DHCP server responds and provide client a valid IP address
4. DHCP request to VIP is load balanced to PSN @ 10.1.99.7 based on source IP stick (L3 gateway) or DHCP field parsed from request.

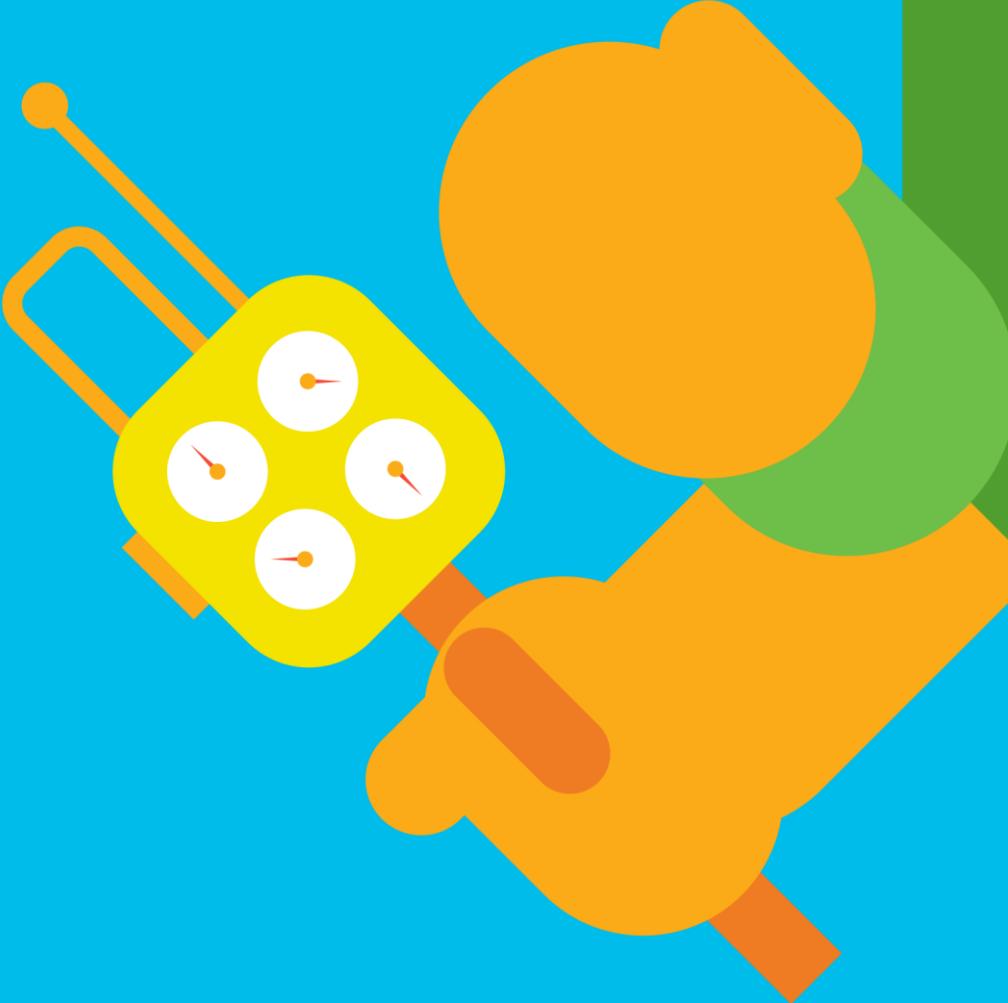
Load Balancing Sticky Guidelines

Ensure DHCP and RADIUS for a Given Endpoint Use Same PSN



1. RADIUS Authentication request sent to VIP @ 10.1.98.8.
2. Request is Load Balanced to PSN-3, and entry added to Persistence Cache
3. DHCP Request is sent to VIP @ 10.1.98.8
4. Load Balancer uses the same “Sticky” as RADIUS based on client MAC address
5. DHCP is received by same PSN, thus optimising endpoint replication

Load Balancing TACACS+



Vendor-Specific LB Configurations

- F5 LTM
- Citrix NetScaler
- Cisco ACE
- Cisco ITD (Note)

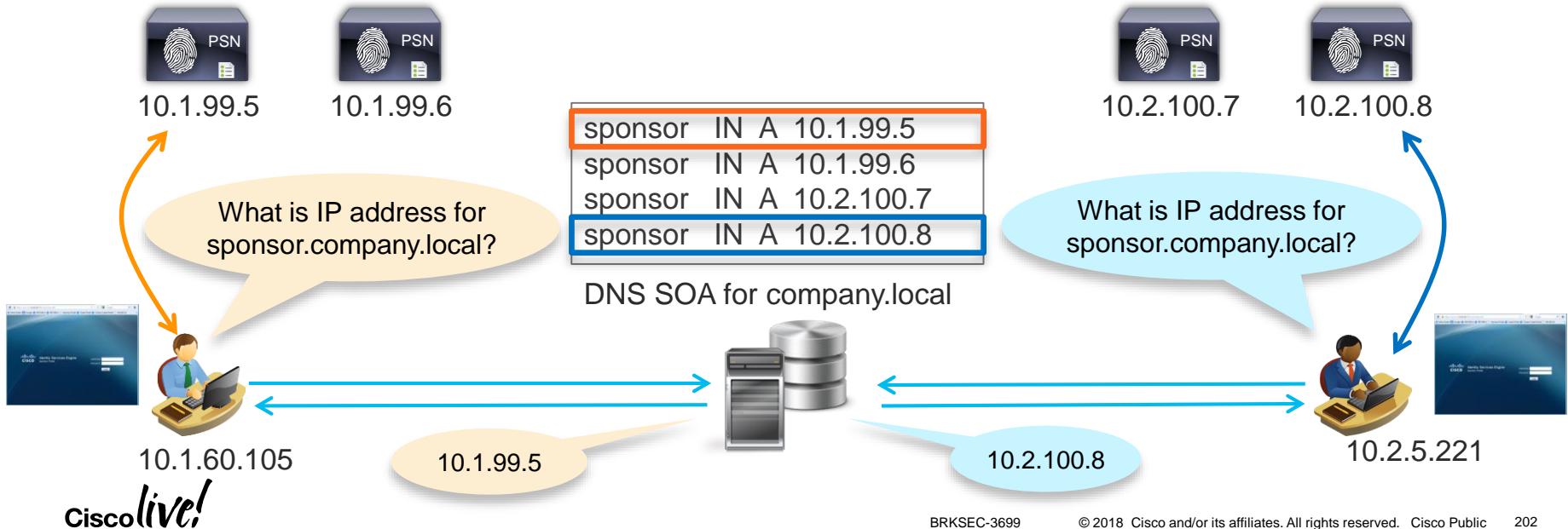
<https://communities.cisco.com/docs/DOC-64434>

PSN HA Without Load Balancers

Load Balancing Web Requests Using DNS

Client-Based Load Balancing/Distribution Based on DNS Response

- Examples:
Cisco Global Site Selector (GSS) / F5 BIG-IP GTM / Microsoft's DNS Round-Robin feature
- Useful for web services that use static URLs including LWA, Sponsor, My Devices, OCSP.



ISE Configuration for Anycast

Anycast address should only be applied to ISE secondary interfaces, or LB VIP, but never to ISE GE0 management interface.

On each PSN that will participate in Anycast...

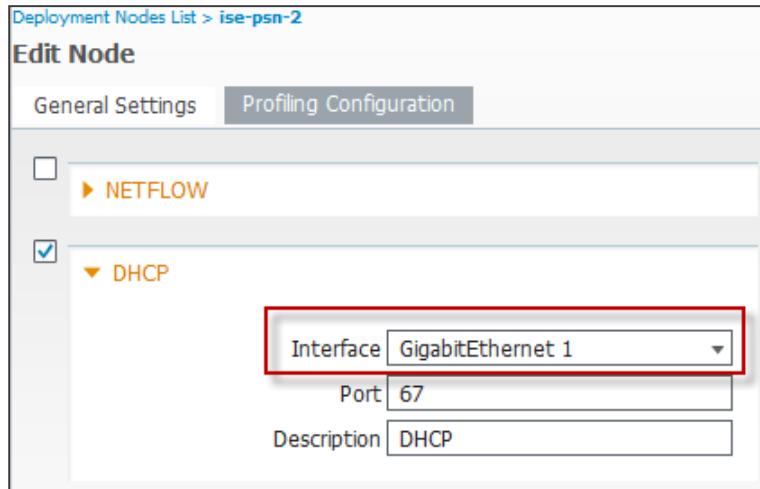
1. Configure PSN probes to profile DHCP (IP Helper), SNMP Traps, or NetFlow **on dedicated interface**
2. From CLI, configure dedicated interface with same IP address on each PSN node.

ISE-PSN-1 Example:

```
#ise-psn-1/admin# config t  
#ise-psn-1/admin (config)# int GigabitEthernet1  
#ise-psn-1/admin (config-GigabitEthernet)# ip address 10.10.10.10 255.255.255.0
```

ISE-PSN-2 Example:

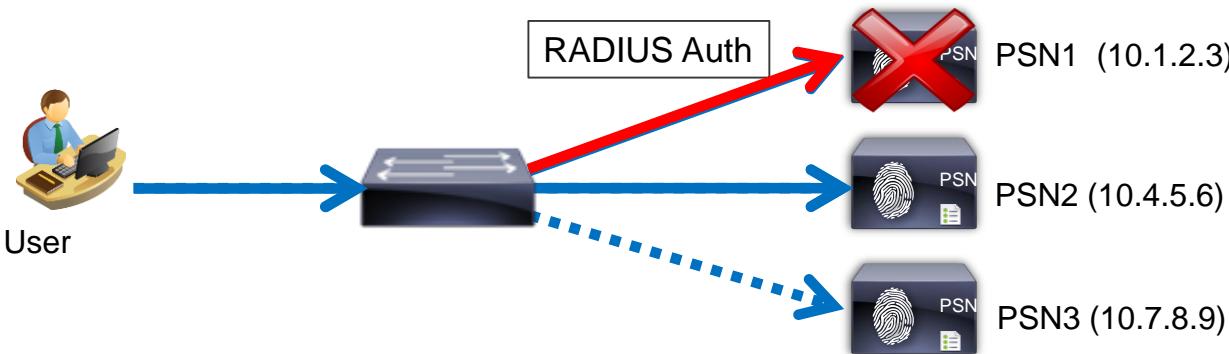
```
#ise-psn-1/admin# config t  
#ise-psn-1/admin (config)# int GigabitEthernet1  
#ise-psn-1/admin (config-GigabitEthernet)# ip address 10.10.10.10 255.255.255.0
```



NAD-Based RADIUS Server Redundancy (IOS)

Multiple RADIUS Servers Defined in Access Device

- Configure Access Devices with multiple RADIUS Servers.
- Fallback to secondary servers if primary fails

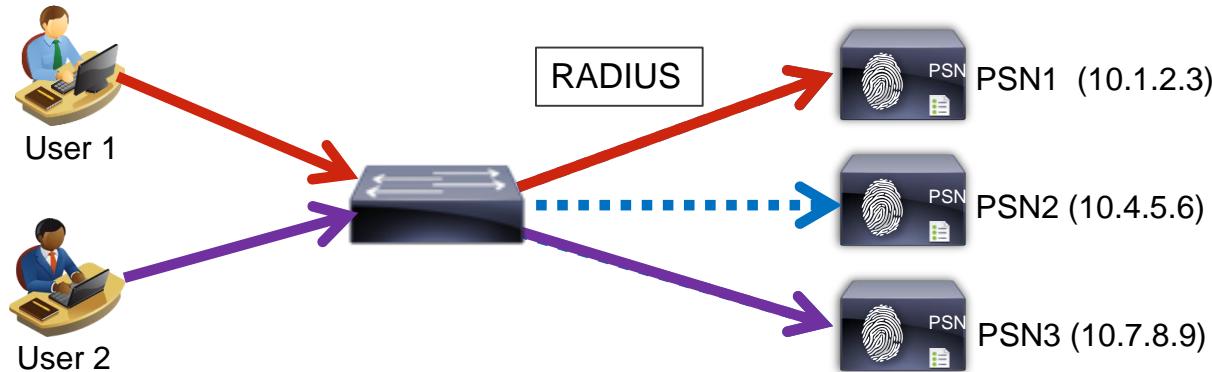


```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813  
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813  
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813
```

IOS-Based RADIUS Server Load Balancing

Switch Dynamically Distributes Requests to Multiple RADIUS Servers

- RADIUS LB feature distributes batches of AAA transactions to servers within a group.
- Each batch assigned to server with least number of outstanding transactions.



NAD controls the load distribution of AAA requests to all PSNs in RADIUS group without dedicated LB.

```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813  
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813  
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813  
radius-server load-balance method least-outstanding batch-size 5
```

IOS-Based RADIUS Server Load Balancing

Sample Live Log

- Use **test aaa group** command from IOS CLI to test RADIUS auth requests

Reasonable load distribution across all PSNs
Example shows 3 PSNs in RADIUS group

Time	Status	Details	Identity	Server	Network Device	Authorization Profiles
Oct 11,12 12:50:08.040 AM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.038 AM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.036 AM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.026 AM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
Oct 11,12 12:50:08.009 AM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
0:08.009 AM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
0:07.091 AM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
0:07.089 AM	✓		radtest	ise-psn-3	cat3750x	RADIUS_Probes
0:07.089 AM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
0:07.088 AM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
0:07.084 AM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.050 AM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.035 AM	✓		radtest	ise-psn-2	cat3750x	RADIUS_Probes
Oct 11,12 12:50:07.033 AM	✓		radtest	ise-psn-1	cat3750x	RADIUS_Probes

```
cat3750x# test aaa group radius radtest cisco123 new users 4 count 50
```

```
AAA/SG/TEST: Sending 50 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
```

NAD-Based RADIUS Redundancy (WLC)

Wireless LAN Controller

- Multiple RADIUS Auth & Accounting Server Definitions
- RADIUS Fallback options: **none**, **passive**, or **active**

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. On the left, under the 'Security' tab, the 'AAA' section is expanded, showing 'General', 'RADIUS', and three sub-options: 'Authentication' (circled in red), 'Accounting', and 'Fallback'. The 'Fallback' option is also circled in red. The main pane displays the 'RADIUS Authentication Servers' configuration. It includes fields for 'Call Station ID Type' (set to 'System MAC Address'), 'Use AES Key Wrap' (unchecked), 'MAC Delimiter' (set to 'Hyphen'), and a table of servers. The table has columns: Network User, Management, Server Index, Server Address, and Port. Four servers are listed with their indices, addresses, and ports:

Network User	Management	Server Index	Server Address	Port
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.1.99.5	1812
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6	10.1.99.6	1812
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7	10.1.99.7	1812
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8	10.1.98.10	1812

To the right, a detailed view of the 'Fallback Parameters' is shown. It includes fields for 'Fallback Mode' (set to 'active', highlighted in blue), 'Username' (set to 'radtest-w'), and 'Interval in sec.' (set to '180'). A note next to the 'Username' field says 'Password=Username'. A large callout box provides definitions for the fallback modes:

- Off** = Continue exhaustively through list; never preempt to preferred server (entry with lowest index)
- Passive** = Quarantine failed RADIUS server for interval then return to active list w/o validation; always preempt.
- Active** = Mark failed server dead then actively probe status per interval w/username until succeed before return to list; always preempt.

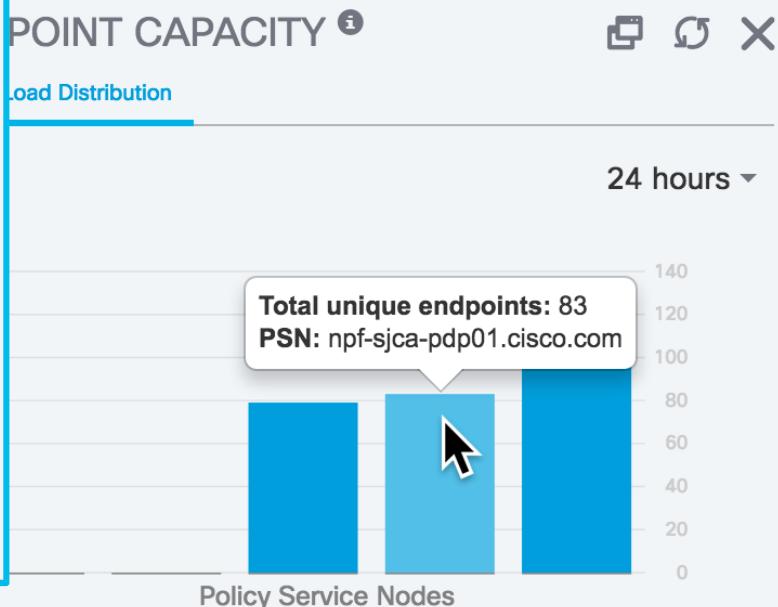
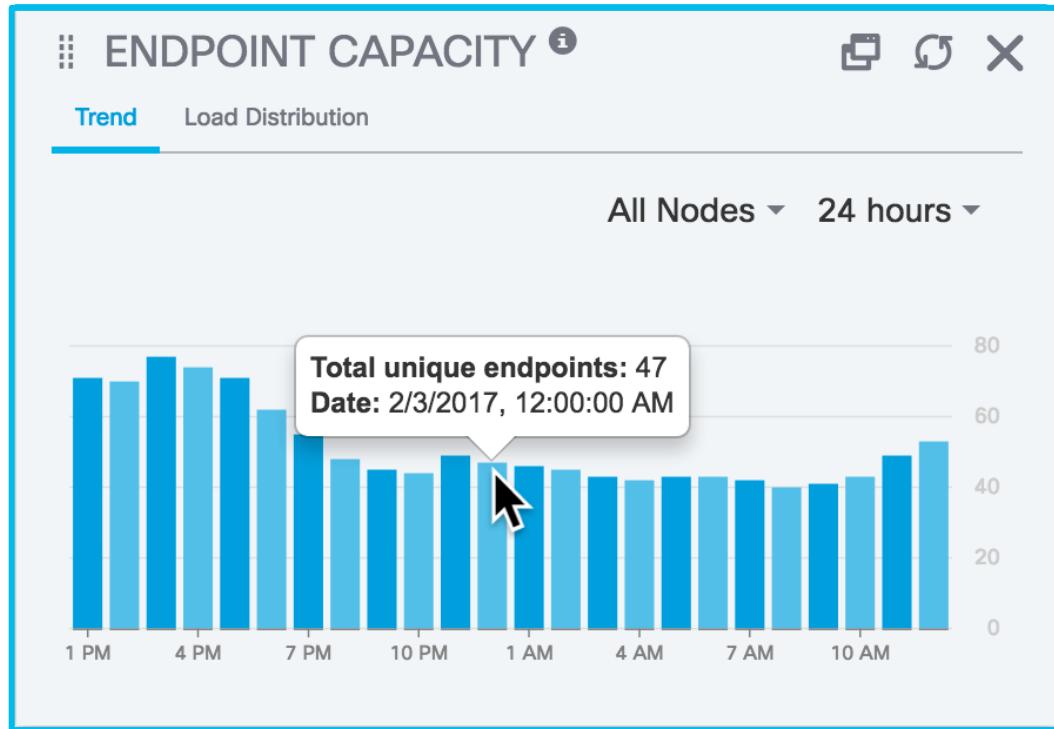


NAD Fallback and Recovery

Monitoring Load and System Health

Endpoint Capacity Report

ISE 2.2+



Key Performance Metrics (KPM)

ISE 2.2+

- KPM Reports added in ISE 2.2: [Operations > Reports > Diagnostics > KPM](#)
- Also available from CLI (# application configure ise) since ISE 1.4
- Provide RADIUS Load, Latency, and Suppression Stats

Key Performance Metrics i

From 2017-01-06 00:00:00.0 to 2017-02-05 22:32:38.128

Logged Time	Server	Radius Requests/Hr	Logged To M...	Noise/Hr	Suppression/Hr	Avg Load	Max Load	Avg Latency...	Avg TPS
2017-02-05 18:01:22.0	npf-sjca-pdp01	343	598	-255	-74.34	4.77	10.83	0.67	0.1
2017-02-05 18:01:22.0	sbg-bgl-a-pdp01	262	174	88	33.59	2.27	3.75	2.57	0.07
2017-02-05 18:01:22.0	npf-sjca-pdp02	169	271	-102	-60.36	2.16	3.75	0.63	0.05
2017-02-05 17:01:40.0	sbg-bgl-a-pdp01	227	147	80	35.24	2.39	3.75	0.35	0.06
2017-02-05 17:01:40.0	npf-sjca-pdp02	187	275	-88	-47.06	3.33	8.75	0.64	0.05
2017-02-05 17:01:40.0	npf-sjca-pdp01	343	596	-253	-73.76	3.03	4.17	0.69	0.1
2017-02-05 16:01:23.0	npf-sjca-pdp02	188	297	-109	-57.98	2.39	3.75	0.64	0.05
2017-02-05 16:01:23.0	npf-sjca-pdp01	356	625	-269	-75.56	4.39	9.17	0.74	0.1
2017-02-05 16:01:23.0	sbg-bgl-a-pdp01	253	131	122	48.22	1.67	2.5	0.72	0.07

Serviceability Counter Framework (CF)

The Easy Way: MnT auto-collects key metrics from each node!



- Enable/disable from 'app configure ise'
- Enabled by default
- Threshold are hard set by platform size
- Alarm sent when exceed threshold
- Running count displayed per collection interval

ISE Counters (From 2017-04-30 00:00:00.0 to 2017-04-30 15:15:47.612)

Counter Attribute Threshold	Value	Platform	Count
Endpoint Oracle Persist Received	IBM_LARGE	9000	
Endpoint Ownership Change	IBM_LARGE	5000	
Endpoint Profiling Events	IBM_LARGE	80000	
Endpoint Reprofiling Events	IBM_LARGE	8000	
Endpoint Cache Insert Update Received	IBM_LARGE	95000	
Hostname Event Fetch from AD	IBM_LARGE	100000	
HTTP Endpoint Detected	IBM_LARGE	800	
NMAP Scan Event Query	IBM_LARGE	8000	
Network Device Session ...	IBM_LARGE	20000	
OCSP Monitoring	IBM_LARGE	800	
RADIUS Errors	IBM_LARGE	8000	
Threat-Centric NAC Live Logs	IBM_LARGE	20000	

Closing Comments

Key Takeaway Points

- CHECK ISE Virtual Appliances for proper resources and platform detection!
- Avoid excessive auth activity through proper NAD / supplicant tuning and Log Suppression
- Minimise data replication by implementing node groups and profiling best practices
- Leverage load balancers for scale, high availability, and simplifying network config changes
- Be sure to have a local fallback plan on your network access devices

Cisco Community Page on Sizing and Scalability

<https://communities.cisco.com/docs/DOC-68347>

The screenshot shows a blue header bar with the Cisco logo and the word 'Communities'. Below it, a breadcrumb navigation path is visible: Cisco Communities > Technology > Security > Policy and Access > Identity Services Engine (ISE) > Documents. The main content area has a white background and features a large blue title 'ISE Performance & Scale' with a document icon. To the right of the title is a vertical dashed line. A blue curved arrow points from the bottom left towards the vertical line. The page lists several topics under 'ISE Performance & Scale':

- ISE 2.4 Deployment Scale and Limits
- ISE 2.2+ Deployment Scale and Limits
- ISE Hardware Platforms
- ISE PSN Performance
 - ISE TACACS+ Performance
 - ISE 2.3 RADIUS Performance
 - ISE 2.2 RADIUS Performance
 - ISE 2.0 Scenario-Based Performance
 - ISE 2.2 Passive Identity (Passive ID) and Easy Connect Scaling
 - Passive ID / EZC Scaling Per Deployment
 - Passive ID / Easy Connect Scaling per PSN dedicated to Passive ID Service
 - Passive ID - Provider and Consumer Scaling
 - ISE 2.2 Platform Exchange Grid (pxGrid) Scaling
 - pxGrid Scaling per Deployment
 - pxGrid Scaling per Dedicated pxGrid Node

- ISE 2.2 SXP Scaling
 - ISE SXP Scaling per Deployment
 - ISE SXP Scaling per SXPSN
- ISE 2.2 Threat-Centric NAC (TC-NAC) Scaling
 - TC-NAC Scaling per Deployment
 - TC-NAC Scaling per PSN
- ISE Storage Requirements
 - VM Disk Size Minimum Requirement
 - MnT Persona Log Storage Requirements
 - RADIUS Log Retention (Days):
 - TACACS+ log retention(Days)
 - Scripted device admin model:
 - Human admin - Device admin model
- ISE Latency & Bandwidth
 - ISE 2.0 Latency
 - ISE 2.1 Latency
 - WAN Bandwidth Calculator
- Sources

ISE Performance & Scale Resources

<https://communities.cisco.com/docs/DOC-65625>

- Cisco Live: BRKSEC-3699
Reference version
- ISE Load Balancing Design Guide
- Performance and Scale guidance in HLD template
- Calculators for Bandwidth and Logging



ISE Deployment Sizing and Scalability

created by Craig Hyps on Feb 14, 2016 1:18 AM, last modified by Craig Hyps on Mar 10, 2016 12:36 PM

ISE Install Guide on Deployment Sizing

Cisco Live Breakout Session BRKSEC-3699 on ISE Large Scale Design including Sizing, High Availability, Load Balancing, and Best Practices:

Includes Working Configs for ACE and F5

[BRKSEC-3699 Designing ISE for Scale & High Availability](#) presented by Craig Hyps : [Presentation \(PDF\)](#) | [Reference \(PDF\)](#)

ISE Load Balancing

ISE Latency and Bandwidth Calculators

ISE MnT Log sizing calculator for TACACS+ and RADIUS

ISE Performance Metrics are contained in the [High-Level Design Document](#)

Q & A

Complete Your Online Session Evaluation

- Give us your feedback and receive a **Cisco Live 2018 Cap** by completing the overall event evaluation and 5 session evaluations.
- All evaluations can be completed via the Cisco Live Mobile App.

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



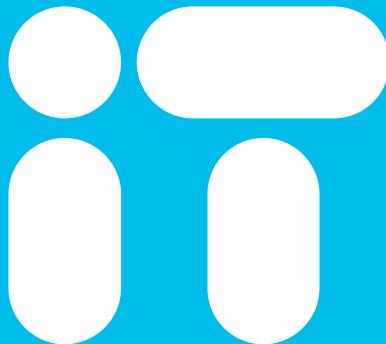


Cisco *live!*

Thank you



You're



Cisco *live!*