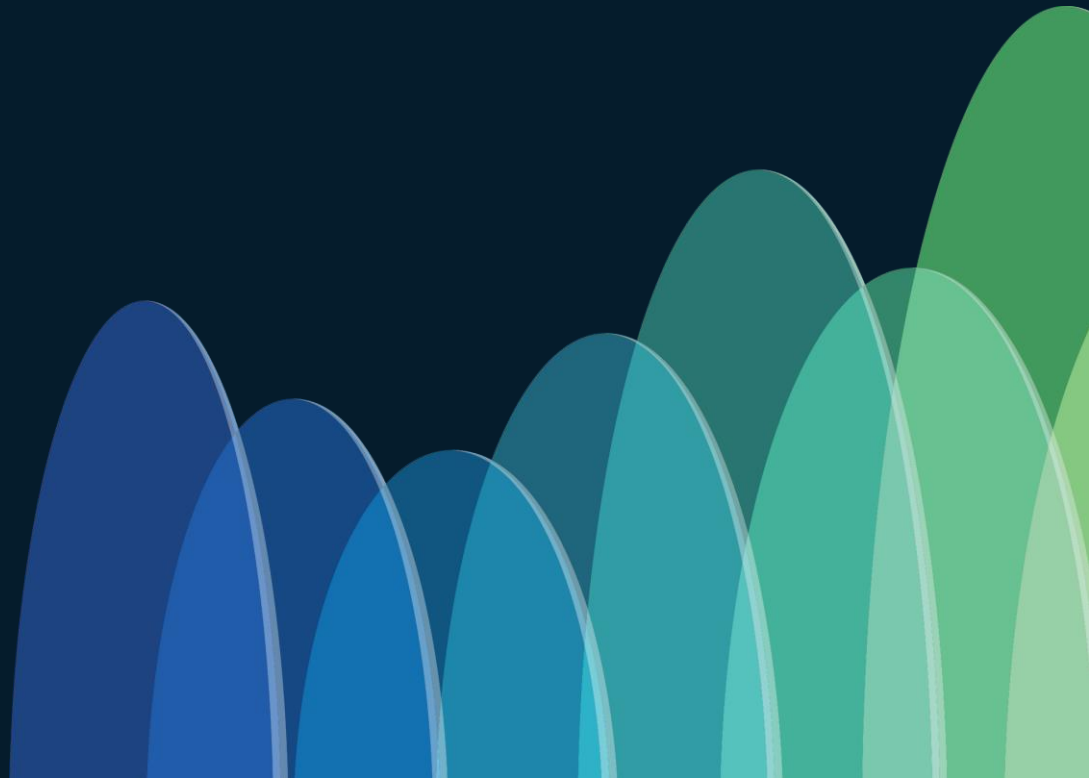
Cisco ISE Performance, Scalability and Best Practices

Jesse Dubois - TAC Security Technical Leader

BRKSEC-3234

Introduction



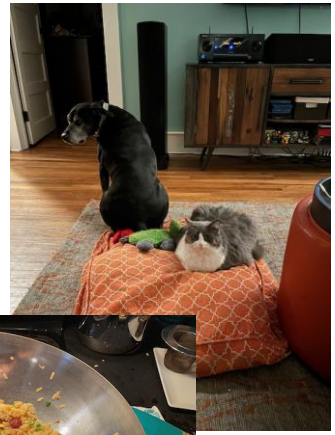
About Jesse Dubois

job.jessedubois: 18 years in TAC

details.jessedubois:

- Location: Durham, North Carolina
- Interests: Brewing, Golf, Cooking
- Pets: Dunkel, Apollo, Comet, Calypso
- Latest Travel: Brussels, Belgium









Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

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

Webex spaces will be moderated by the speaker until February 28, 2025.

Session Abstract

In today's world of constant attacks, malware and Ransomware, its important to design, deploy and manage your network with an identity aware secure access platform. Cisco ISE plays a key role for many security solutions and is also one of the main pillars in the overall Cisco's Software defined Access Architecture.

This session will show you how to deliver scalable and highly available access control services using ISE for wired, wireless, and VPN from a single campus to a global deployment. Methodologies for increasing scalability and redundancy will be covered such as load distribution with and without load balancers, optimal profiling design, lessons learned from the trenches, as well as serviceability tips and tricks to help you gain optimal value and productivity from ISE.

Attendees of this session will gain knowledge on how to best design 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. Cisco ISE also enables cross-platform network system collaboration across your IT infrastructure by using pxGrid to monitor security, detect threats, and set network policy. Manage assets, configuration, identity, and access. The session will go through such deployment considerations and common architectures.

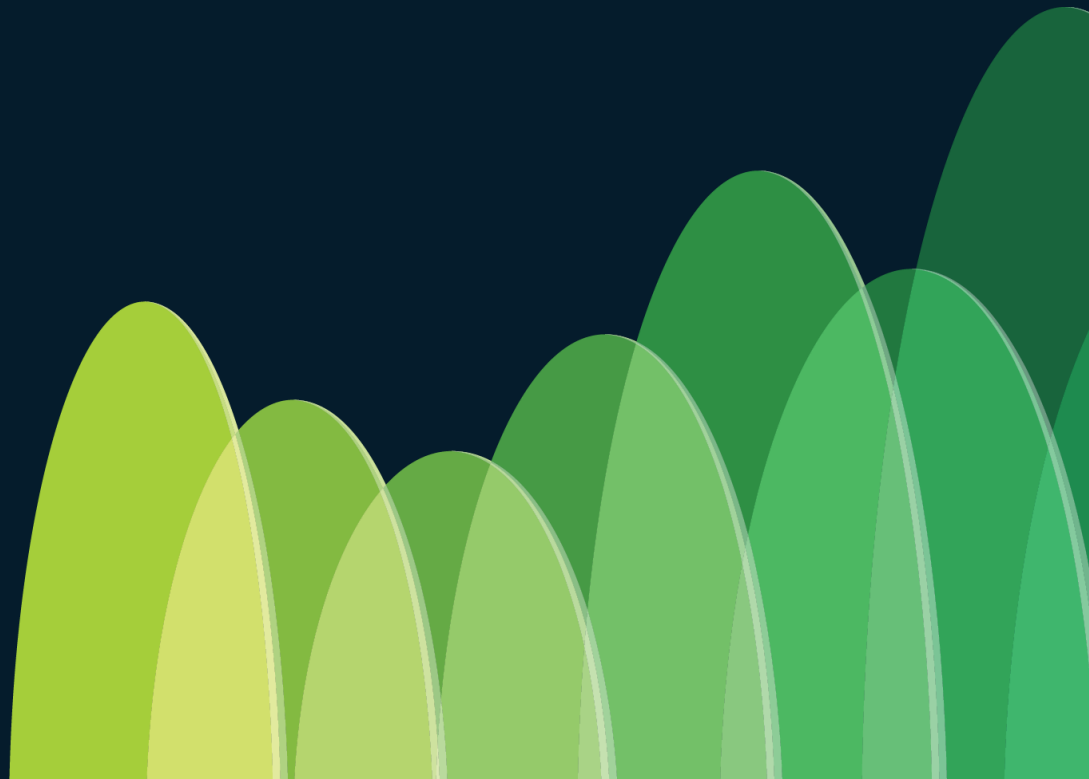
Session Objectives

- How to choose the deployment design that works for you!
- How to get the most out of your deployment.
- My Tips – What we see in TAC/Escalation (Best Practices)
  - Avoid commonly seen pitfalls.
- Not a session on configuration.
  - Will include links where appropriate to guides.

Agenda

- Deployment/Sizing
- Scaling ISE Services
  - Certificates
  - Network Devices
  - BlastRADIUS
  - Load Balancing
  - Profiling
  - External Databases
- MnT / Log Analytics

Deployment / Sizing



ISE Architecture

Standalone ISE

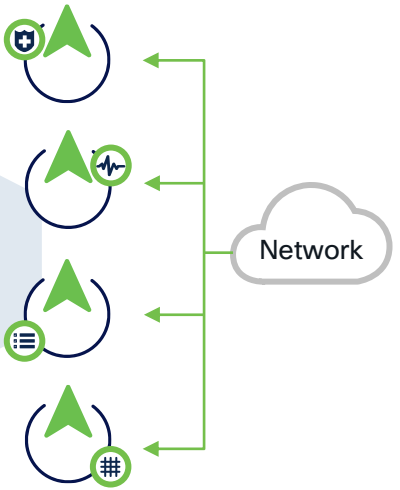
Policy Administration Node (PAN)
- Single plane of glass for ISE admin
- Replication hub for all config changes

Monitoring & Troubleshooting Node (MnT)
- Reporting and logging node
- Syslog collector from ISE Nodes

Policy Services Node (PSN)
- Makes policy decisions
- RADIUS / TACACS+ Servers

pxGrid Controller
- Facilitates sharing of context

Distributed ISE



Single Node (Virtual/Appliance)		Multiple Nodes (Virtual/Appliance)
Up to 50,000 concurrent endpoints	3700	Up to 2,000,000 concurrent endpoints

Deployment Options

Small

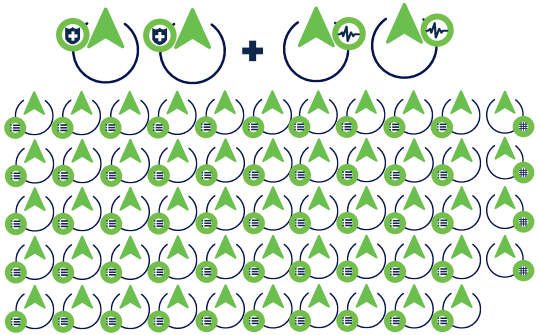
- All Personas on 2 nodes
- Optional 3rd node for:
  - Dedicated PSN
  - pxGrid node
  - Health Check node
  - 3rd node does not increase scale, it is for redundancy and load sharing purposes only!

Medium

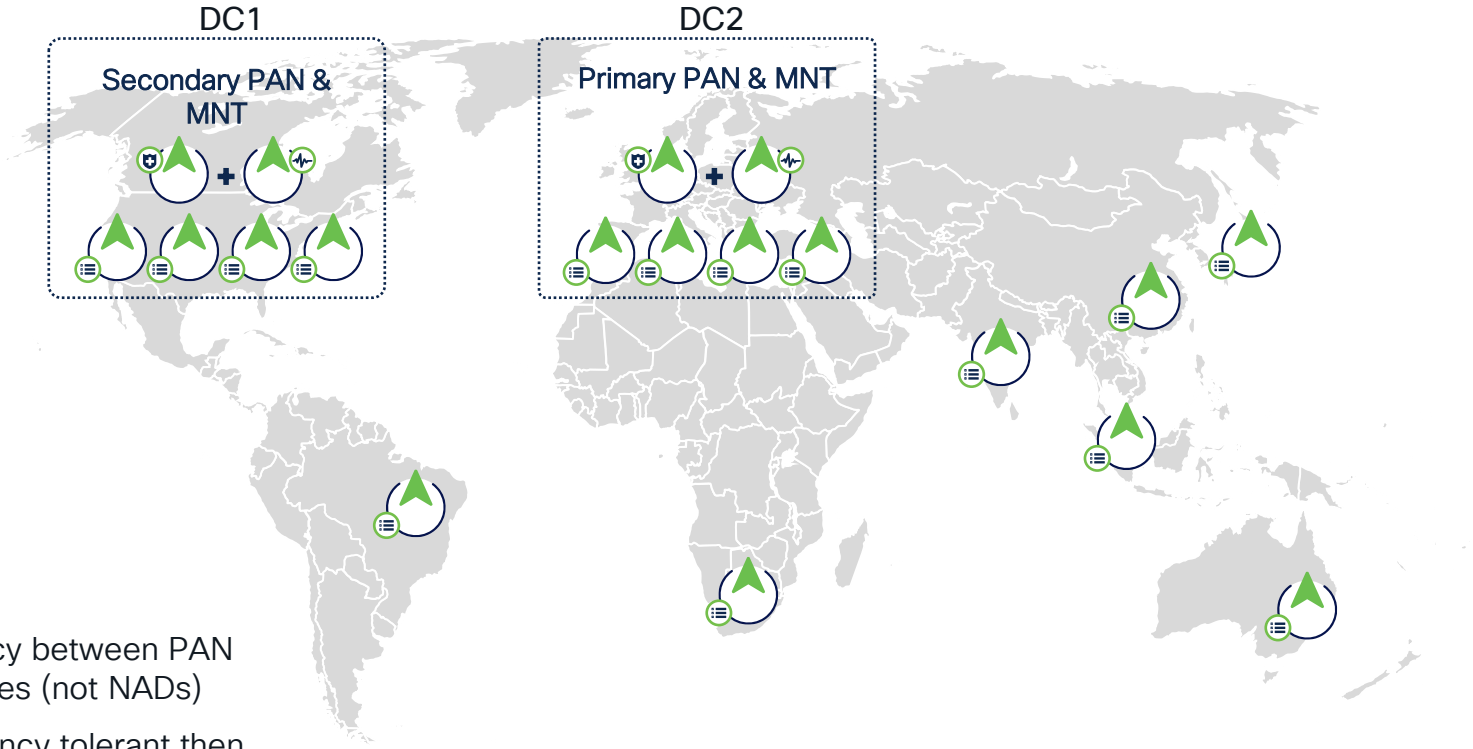
- Maximum 8 nodes
- PAN + MnT on same node
- PSNs on dedicated nodes
- pxGrid can be enabled on up to 2 nodes
  - Dedicated with 4 PSNs
  - Added to PAN + MnT
  - Added to 2 PSNs

Large

- Maximum of 58 nodes
- All personas on dedicated nodes.
- Up to 50 PSNs
- Up to 4 pxGrid nodes

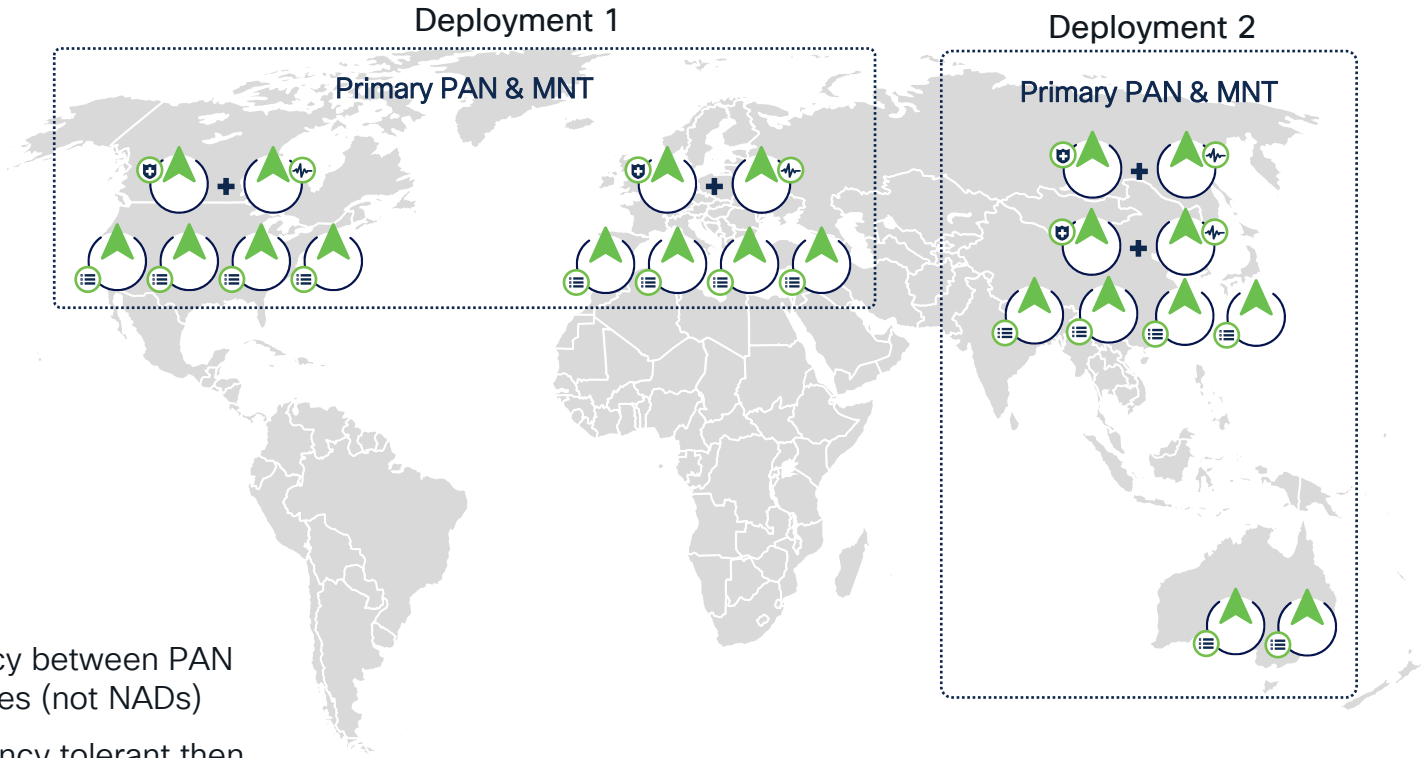


Large Deployment: Centralized or Distributed



- Max 300ms latency between PAN and other ISE nodes (not NADs)
- RADIUS more latency tolerant then internode communication.

Large Deployment: Separate Cubes



- Max 300ms latency between PAN and other ISE nodes (not NADs)
- RADIUS more latency tolerant then internode communication.

Latency Guidance

- Latency guidance is not a “fall off the cliff” number, but a guard rail based on what QA has tested.
  - 300ms can be ok
  - 150ms may be to much
- Profiler config is primary determinant in replication requirements.
- Higher auth/profiling rates may require lower latency.

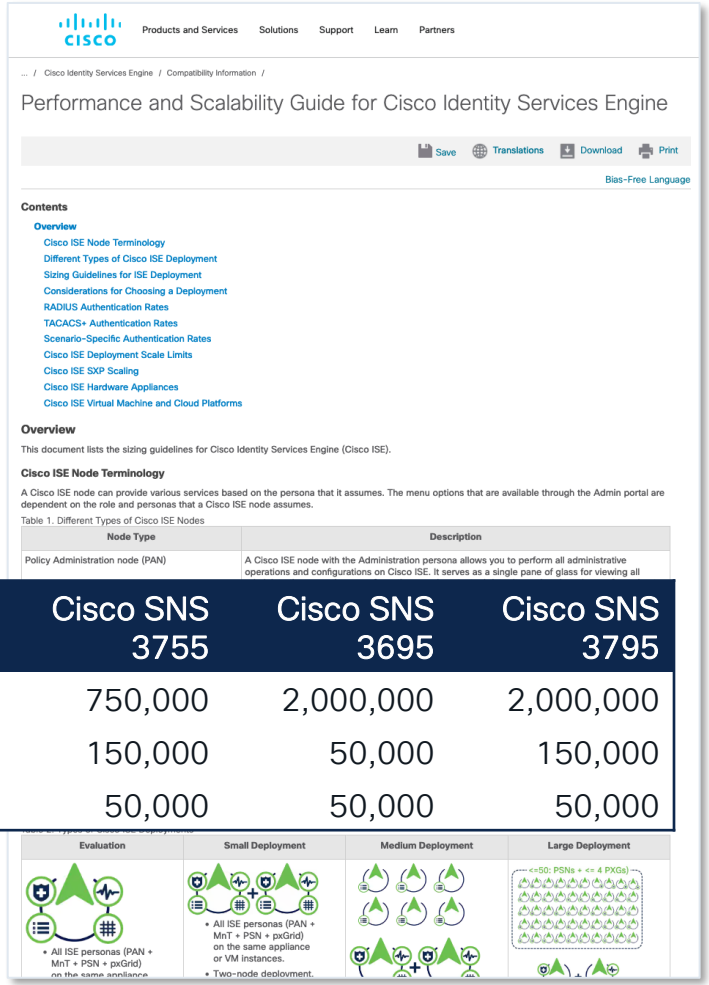
ISE Max Sessions

Maximum Concurrent Active Sessions

- ISE Licensing counts *active endpoint sessions*
- RADIUS Accounting defines session Start & Stop events
- Sessions **Start** upon RADIUS Authorization
- Sessions **Stop** upon :
  1) Disconnect 2) Session Expiration 3) Idle Timeout

Table 3. Maximum Concurrent Active Sessions for Deployments

Deployment	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Large	500,000	Unsupported	Unsupported	500,000	750,000	2,000,000	2,000,000
Medium	20,000	12,500	75,000	25,000	150,000	50,000	150,000
Small	20,000	12,500	25,000	25,000	50,000	50,000	50,000



Steady State versus Peak Demand

- Must take into account transactions per second (TPS)!
- You will have a mix of static and mobile endpoints
- Some endpoints are always on with long (8+ hours) session expirations
- Usage patterns will cause regional and periodic ebbs, flows, and spikes
  - Increased regional activity “follows the sun”
  - Wireless roaming spikes on the hour to change classrooms and meetings
- Mobile endpoints hibernate & roam causing a 3–10X+ larger load
- Misconfigured devices can have 100–1000X larger than average auth load

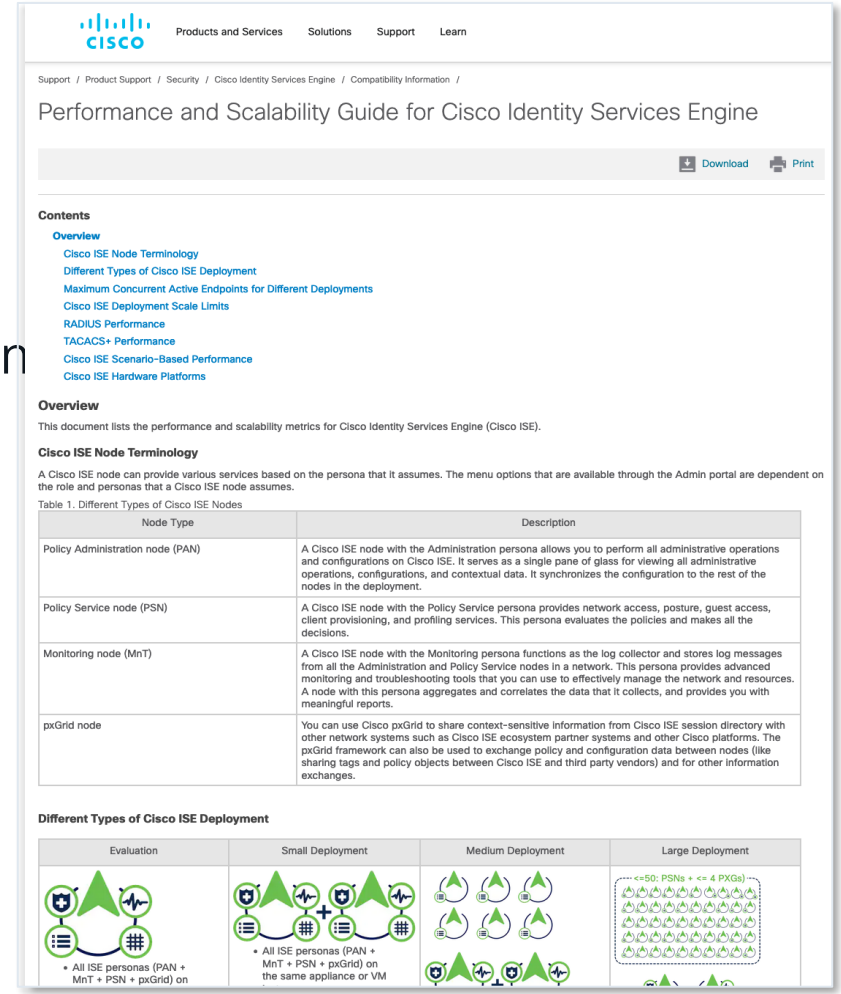
Table 4. Maximum Concurrent Active Sessions for Different ISE Appliances Acting as PSNs

PSN Type	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Dedicated PSN (only PSN persona)	40,000	25,000	50,000	50,000	100,000	100,000	100,000
Shared PSN (multiple personas)	20,000	12,500	25,000	25,000	50,000	50,000	50,000

ISE Performance & Scale

- Deployment Types
- Maximum Concurrent Active Session
- Deployment Scale Limits
- Protocol Performance
- Scenario Performance
- Configuration Objects

cs.co/ise-scale



cisco Products and Services Solutions Support Learn

Support / Product Support / Security / Cisco Identity Services Engine / Compatibility Information /

Performance and Scalability Guide for Cisco Identity Services Engine

Download Print

Contents

Overview

This document lists the performance and scalability metrics for Cisco Identity Services Engine (Cisco ISE).

Cisco ISE Node Terminology

A Cisco ISE node can provide various services based on the persona that it assumes. The menu options that are available through the Admin portal are dependent on the role and personas that a Cisco ISE node assumes.

Table 1. Different Types of Cisco ISE Nodes

Node Type	Description
Policy Administration node (PAN)	A Cisco ISE node with the Administration persona allows you to perform all administrative operations and configurations on Cisco ISE. It serves as a single pane of glass for viewing all administrative operations, configurations, and contextual data. It synchronizes the configuration to the rest of the nodes in the deployment.
Policy Service node (PSN)	A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions.
Monitoring node (MnT)	A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from all the Administration and Policy Service nodes in a network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage the network and resources. A node with this persona aggregates and correlates the data that it collects, and provides you with meaningful reports.
pxGrid node	You can use Cisco pxGrid to share context-sensitive information from Cisco ISE session directory with other network systems such as Cisco ISE ecosystem partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes (like sharing tags and policy objects between Cisco ISE and third party vendors) and for other information exchanges.

Different Types of Cisco ISE Deployment

Evaluation	Small Deployment	Medium Deployment	Large Deployment
• All ISE personas (PAN + MnT + PSN + pxGrid) on	• All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM		<=50: PSNs + <= 4 PXGs)

cisco Live!

Node Resource Profiles

Platform	Extra Small	Small	Medium	Large
Hardware	N/A	SNS-3715-K9	SNS-3755-K9	SNS-3795-K9
VMWare/Hyper-V/KVM	8 CPUs 32GB RAM 300GB Disk	24 CPUs 32GB RAM 300GB – 1.2TB Disk	40 CPUs 96GB RAM 300 GB – 1.2TB Disk	40 CPUs 256GB RAM 1.2TB – 2.4TB Disk
AWS	m5.2xlarge	c5.9xlarge* m5.8xlarge	m5.16xlarge	m5.16xlarge
Azure	Standard_D8s_v4	Standard_F32s_v2* Standard_D32s_v4	Standard_D64s_v4	Standard_D64s_v4
OCI	Optimized3.Flex (8 OCPU and 32 GB)	Optimized3.Flex (16 OCPU and 64 GB)* Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (32 OCPU and 256 GB)

*This instance is compute-optimized and provides better performance compared to the general purpose instances.

Node is “profiled” each time it boots up, if profiles change resources are reallocated.

Why Do Node Resource Profiles Matter?

- Internal Resources Allocated:
  - Java Heap Sizes
  - Oracle Memory Sizes
  - Thread Pool Sizes
  - Max Sessions
  - Etc…
- Virtual appliances mapped to physical profiles

Example:

What we check:

#Active profile properties [profile = sns3615, persona = pap_mnt]

Profile differences:

<sns3615>.tomcat.runtimeThreadPool.maxThreads=200
<sns3755>.tomcat.runtimeThreadPool.maxThreads=300

Persona differences:

<sns3615>.oracle.pga=1200
<sns3615>.<mnt>.oracle.pga=2400

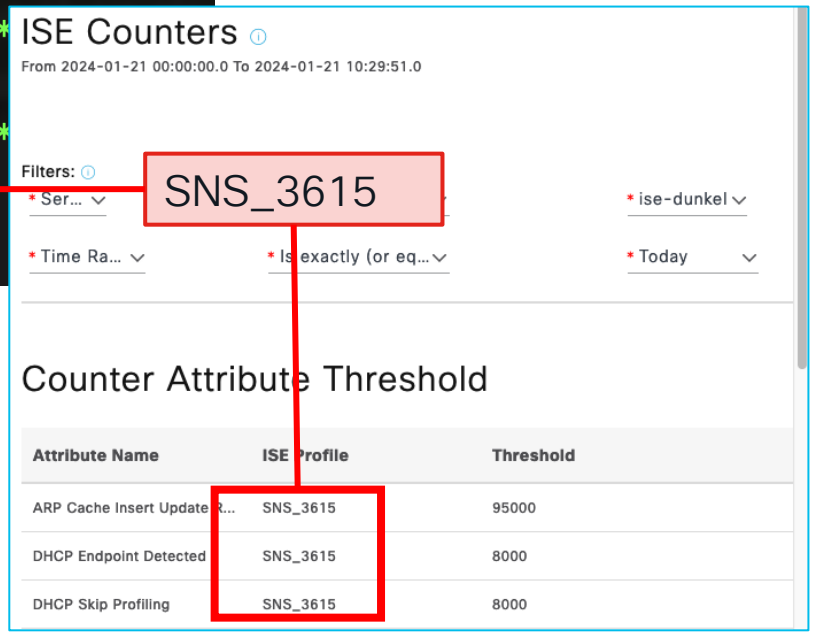
ISE Platform Properties

Verify ISE Detects Proper VM Resource Allocation

- From CLI...
  - ise-node/admin# **show tech | begin “Displaying ISE Profile“**

```
**********************************
Displaying ISE Profile ...
**********************************
Profile : sns3615
TPM: Module Absent
```

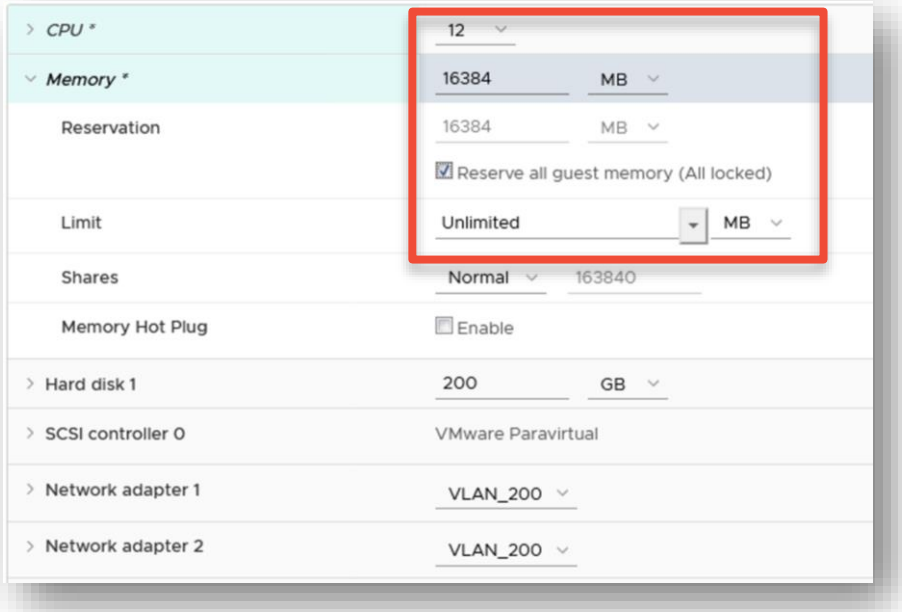
- From Admin UI
  - Operations > Reports > Diagnostics > ISE Counters > [node] (Under ISE Profile column)



Virtual Machine Resources

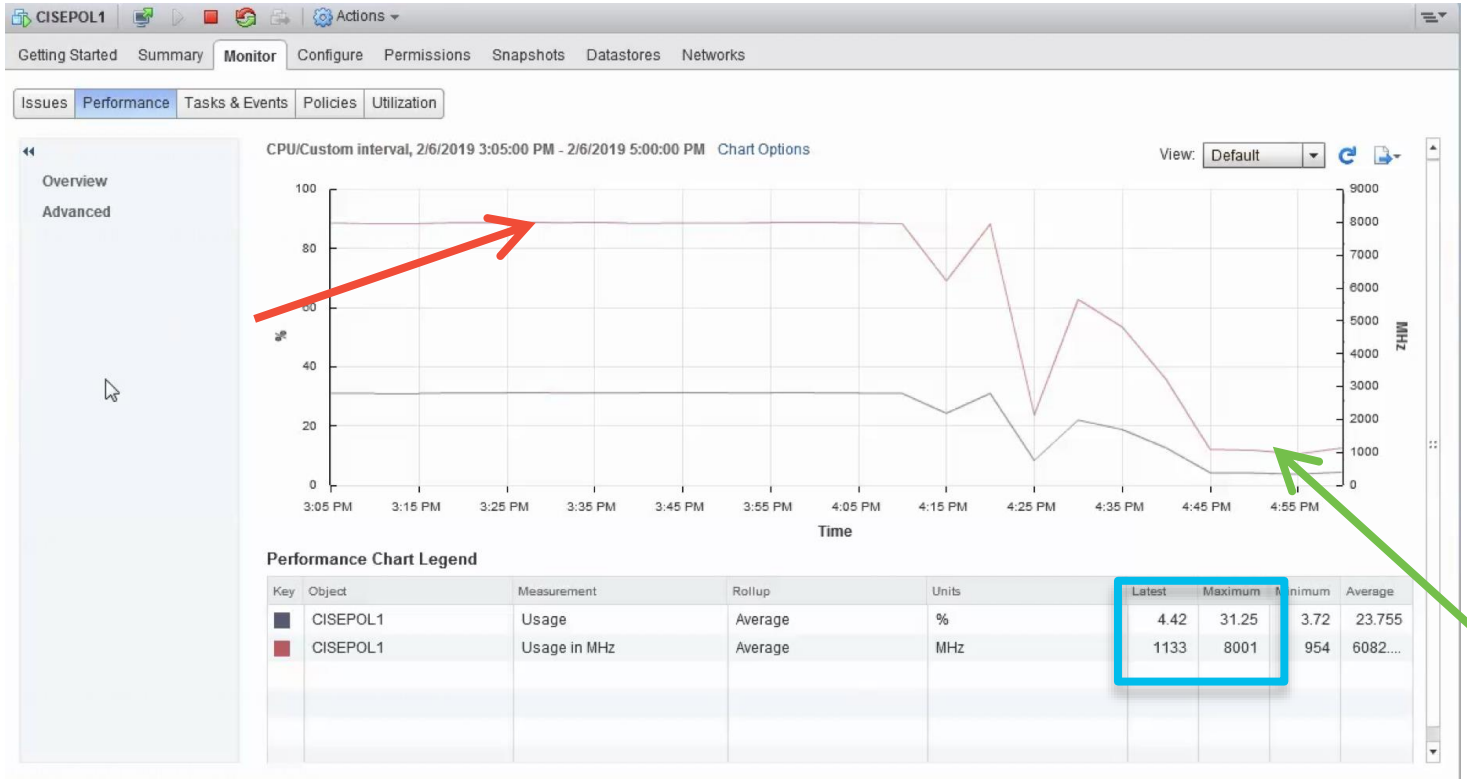
Reservations/Features

- Applies to all virtual platforms – VMWare, KVM, Hyper-V, AHV
- Reserve 100% of CPU and Memory
- Use thick provisioning of disk.
- Do no set resource limits.



Virtual Machine Resources

Reservations – Before and After



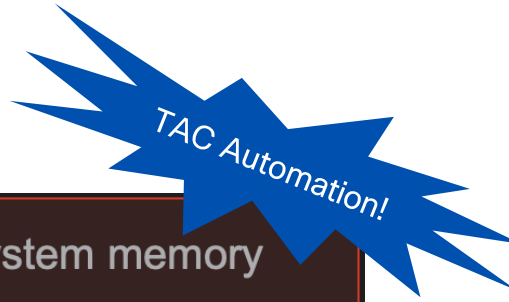
Updated 3615/3715 (32GB) Node Guidance

- Small Deployments:
  - Recommend RADIUS or TACACS+ only workloads.
  - Log Analytics off by default, saves 2gb of memory.
  - Not recommended for AI/ML Profiling, ACI Integration, workload connectors.
- Medium Deployments:
  - Above applies if PAN/MNT nodes are 32GB memory nodes.
- Recommendation:
  - Use at least medium nodes (96GB memory) if advanced features are desired.
  - Apply latest patches for memory rebalancing changes.

Virtual Machine Resources

Limits

- Do not set resource limits!
  - Resource requirements change between versions.

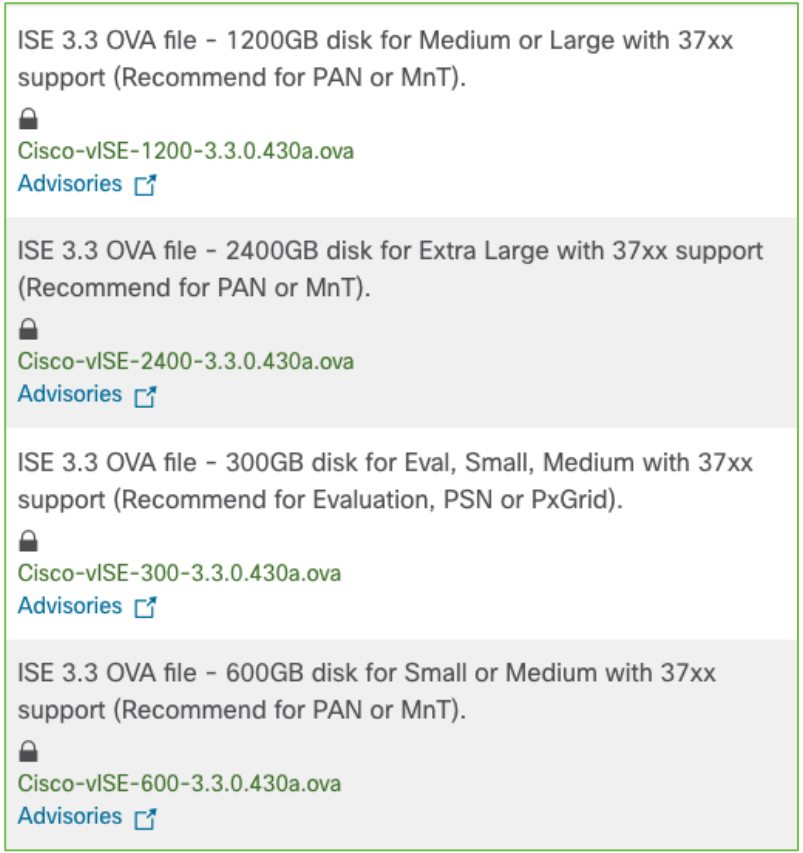


! Virtual Machine Memory limit is lower than the allocated system memory

The VM Memory Limit is currently set to 16777216 kB and VM system memory is currently 32719416 kB.
When the VM Memory Limit is less than system memory, this can lead to the Application Server or OS crashing and not being able to recover on it's own.
Please verify that the VM memory limit is greater than or equal to the allocated system memory in the VM settings. If limit is unset that is also acceptable.

Better Yet! Use the OVAs.

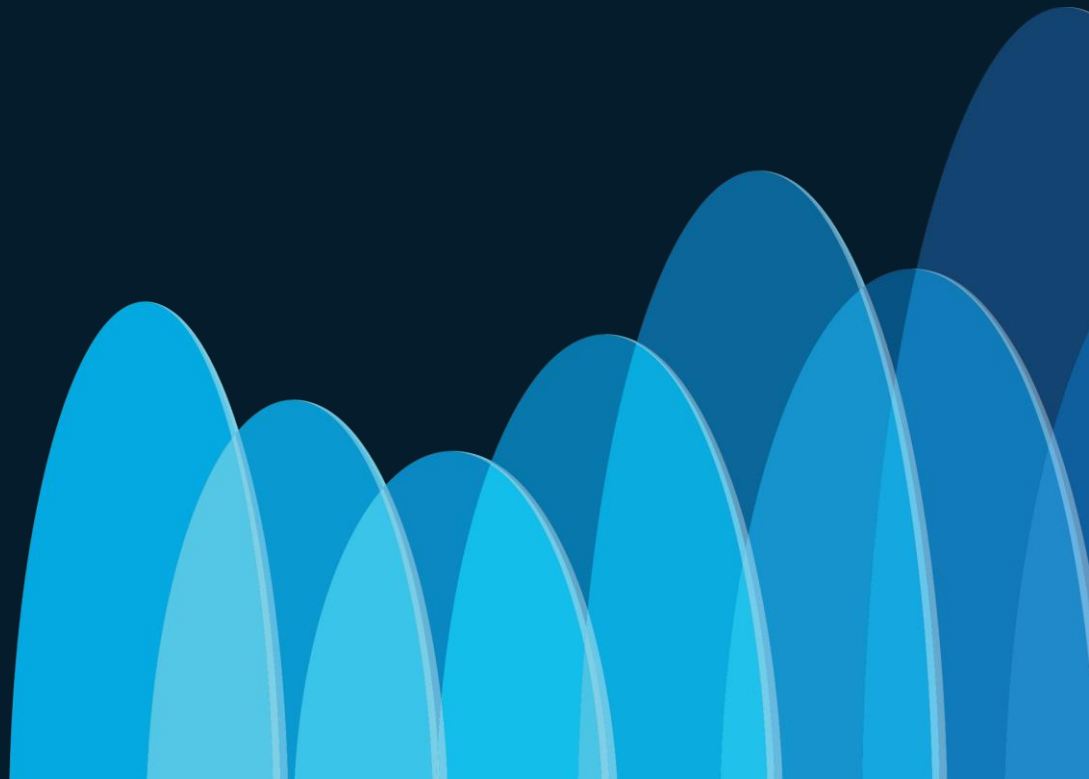
- Simplified for ISE 3.3
- Choose OVA based on Disk Size required.
- Will be prompted to choose node size needed.
- Reservations set automatically.



Other Cautions

- No snapshots!
  - Unable to quiesce database.
  - Use ISE Backup/Restore functionality for disaster recovery.
- Hot vMotion is supported.
  - Tested by System Scale and Test team.
  - TAC Experience:
    - Every environment is different, still some risk in losing the node.
    - Some risk in storage not re-attaching at they hypervisor level.
  - Safer to shut down the node and use cold vMotion.

Scaling ISE Services



cisco Live!

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. Often timeouts too low & misbehaving clients go unchecked/not throttled.
- 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 behavior when above issues occur.
- Bugs in client, NAD, or ISE.

Turn Down the Firehose

Multilayer Approach

Rate Limiting at Source

Reauth period
Quiet-period 5 min
Held-period / Exclusion 5 min

Heartbeat frequency

Reauth phones

Switch

Quiet period

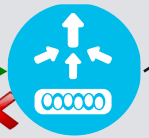
Unknown users

Load Balancer

LB Health probes

WLC

Quiet Period



Client Exclusion

Roaming supplicant

Misbehaving supplicant

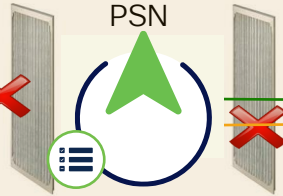
Filtering at Receiving Chain

Detect and reject misbehaving clients

Log Filter

Count and discard repeated events

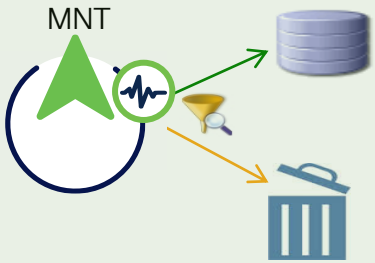
Count and discard untrusted events



Reject bad supplicant

PSN

Filter health probes from logging

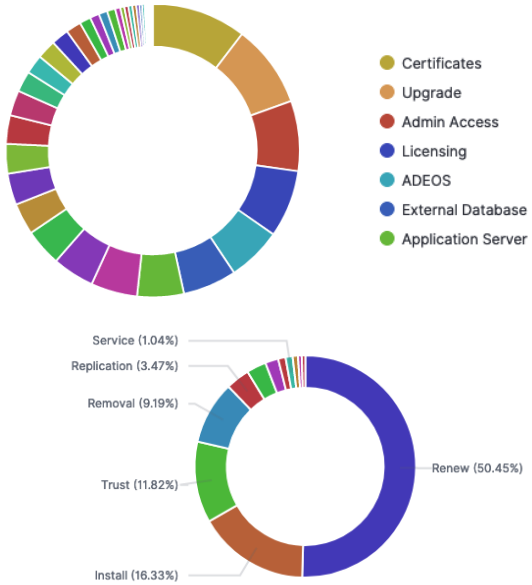


MNT

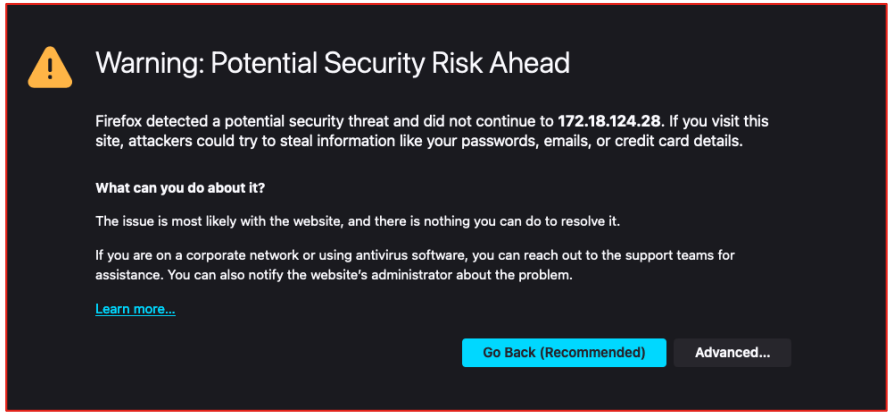
Count and discard repeats and unknown NAD events

Let’s Talk About Certificates

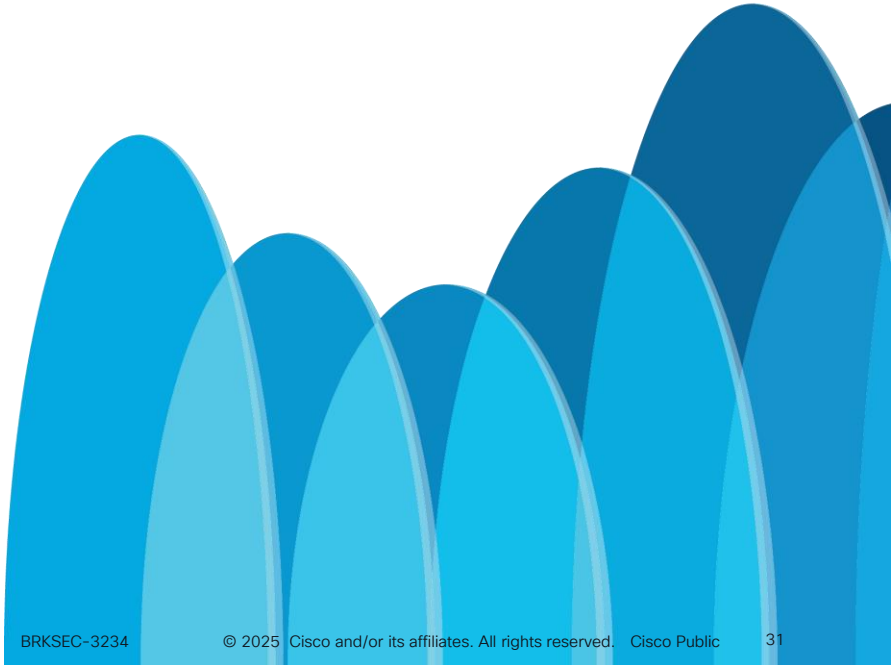
- Top TAC Case Generator!



- While we’re here….
  - Purchase Public Certificates!
  - Don’t train users to accept man-in-the–middle attacks.

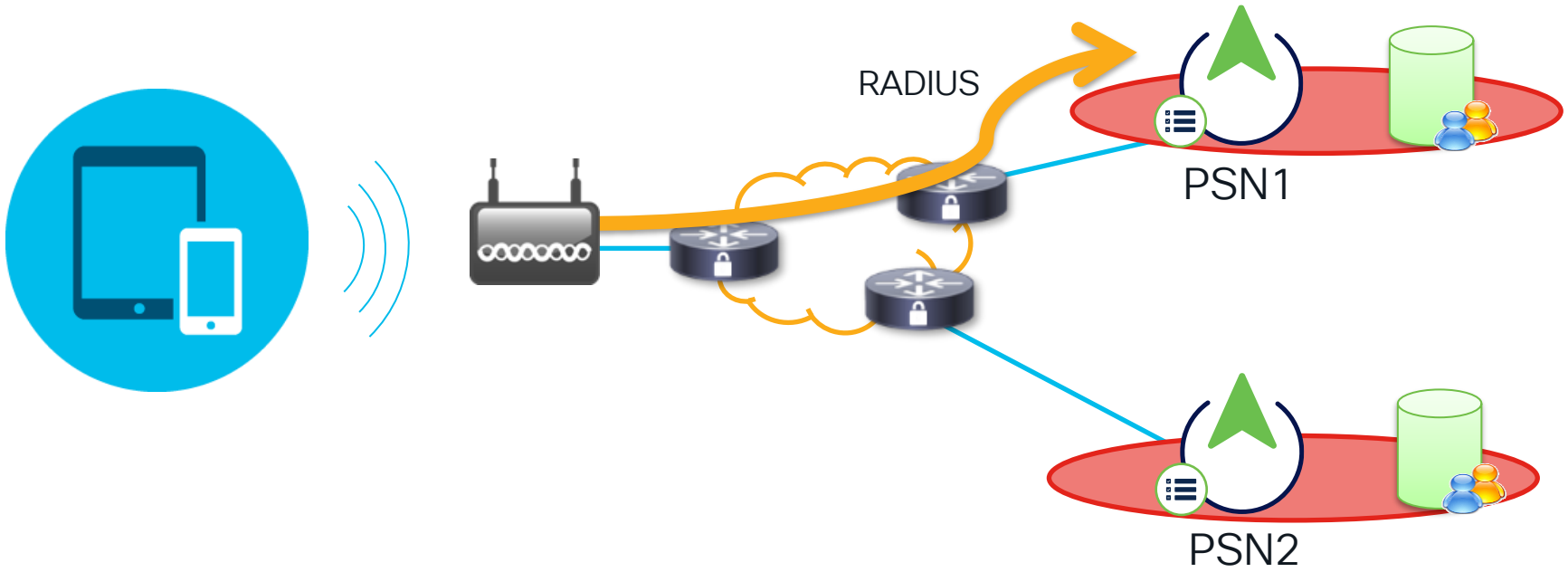


The ~~Skateboarder~~



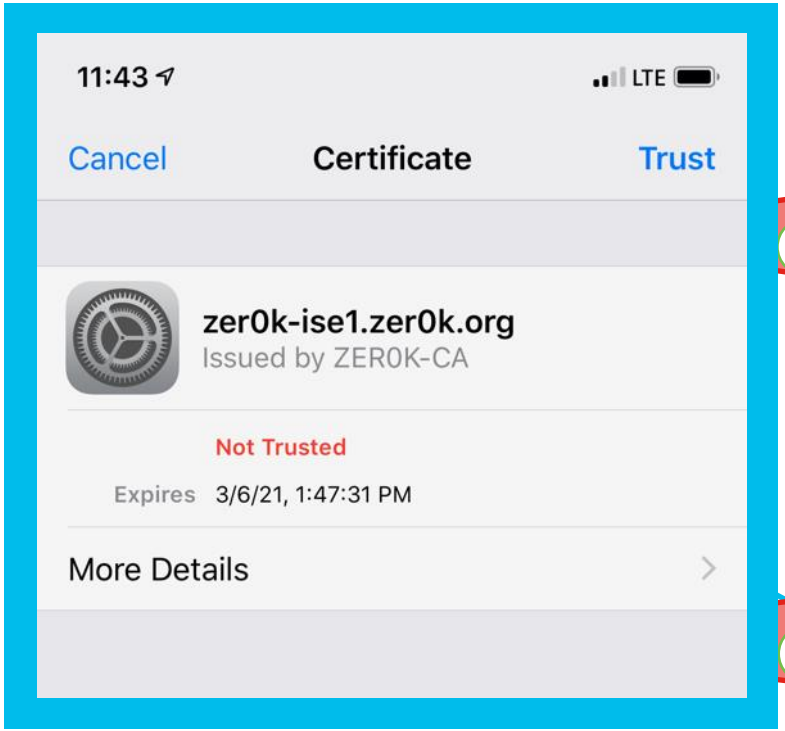
iPhones and Certificates

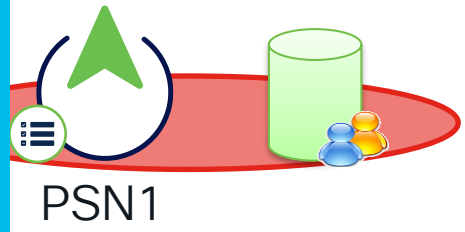
Problem

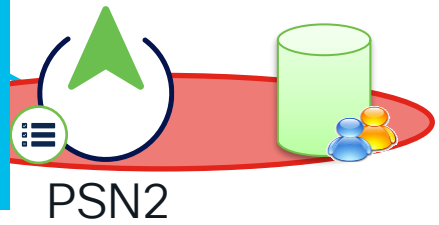


iPhones and Certificates

Problem

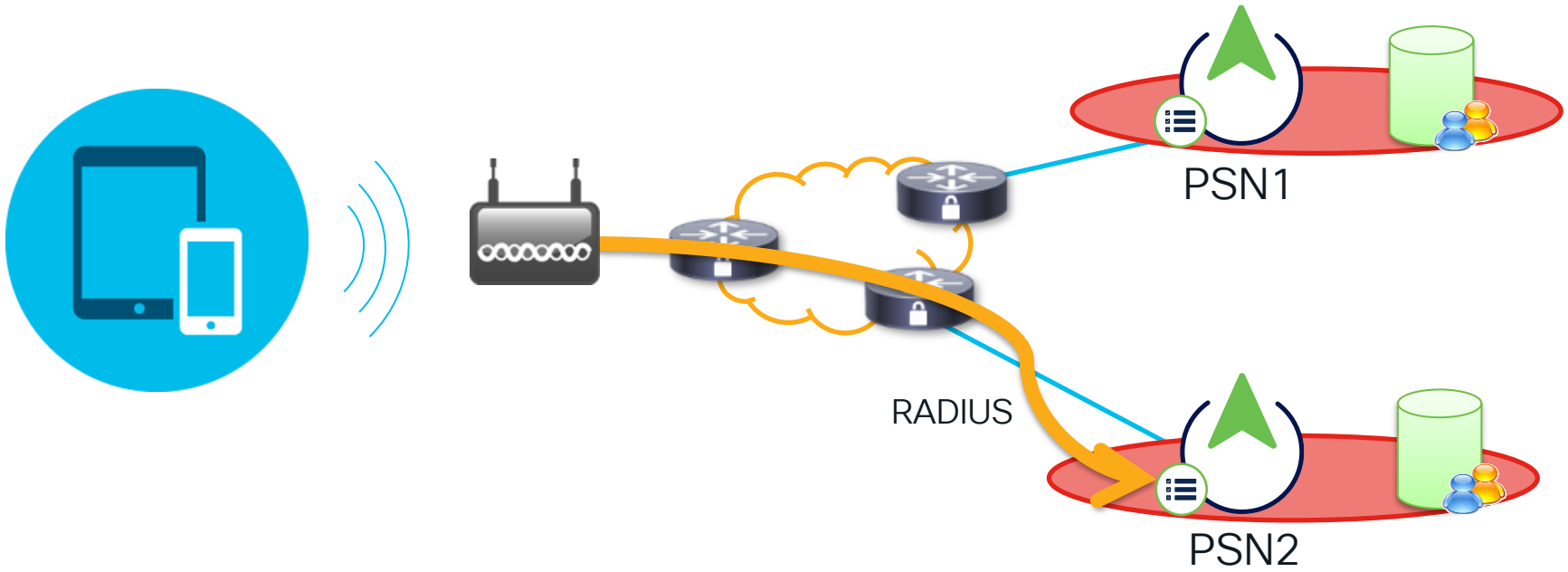






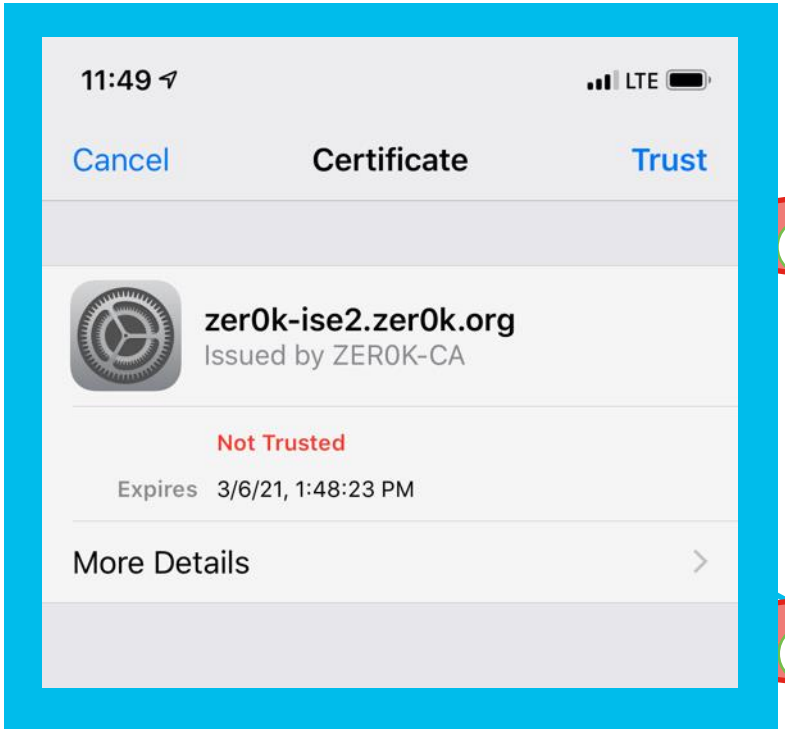
iPhones and Certificates

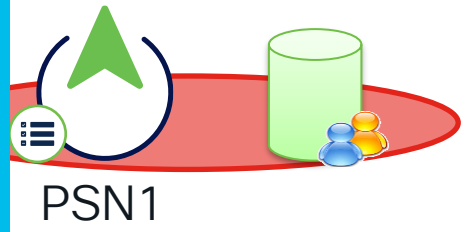
Problem

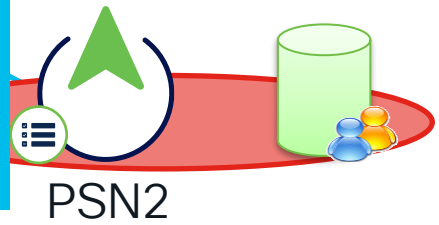


iPhones and Certificates

Problem







iPhones and Certificates

Problem

- If users aren't looking at the phone:

Jun 05, 2019 10:57:56.269 AM	⊗		jfrost	EC:2C:E2:16:05:4A	5440 Endpoint abandoned EAP session and started new
Jun 05, 2019 10:57:05.726 AM	⊗		jfrost	EC:2C:E2:16:05:4A	5440 Endpoint abandoned EAP session and started new

- Multiply this by hundreds of phones and multiple PSNs…
- Additionally, it is a poor end user experience.

Wildcard Certificates

WildSAN or MultiSAN

Details

Issued To	
Common Name (CN)	zer0k-ise.zer0k.org
Organization Unit (OU)	TAC
Organization (O)	Cisco
City (L)	RTP
State (ST)	NC
Country (C)	US
Serial Number	42:00:00:00:0D:46:82:65:3D:42:C8:3C:CE:00:00:00:00:00:0D
Subject Alternative Names	DNS:zer0k-ise.zer0k.org,DNS:*.zer0k.org

Details

Issued To	
Common Name (CN)	zer0k-ise.zer0k.org
Organization Unit (OU)	TAC
Organization (O)	Cisco
City (L)	Durham
State (ST)	NC
Country (C)	US
Serial Number	42:00:00:00:0E:A2:5A:BC:97:2A:E9:9A:9F:00:00:00:00:00:0E
Subject Alternative Names	DNS:zer0k-zer0k.org,DNS:ise-dunkel.zer0k.org,DNS:ise-maibock.zer0k.org,DNS:zer0k-ise1.zer0k.org,DNS:zer0k-ise2.zer0k.org

WildSAN Security

- Certificate is valid for the entire domain:
  - Ex. zer0k.org
- If key is lost, cert could validate any site in the domain.

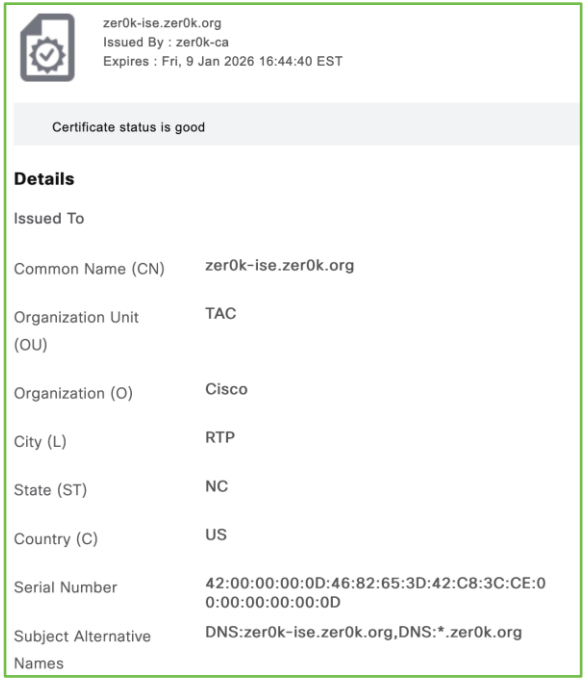
- Solution – subdomain!
- Deploy ISE in a subdomain:
  - Ex. ise.zer0k.org
  - Limits validity of the certificate.
- Deploy MultiSAN
  - More expensive.
  - More difficult to expand deployment in future.

Detour: Common Pitfall

Wildcard Certificate Renewal

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
zer0k-wildsan	Admin, EAP Authentication		zer0k-ise.zer0k.org	zer0k-ca	Wed, 10 Jan 2024	Fri, 9 Jan 2026	Active

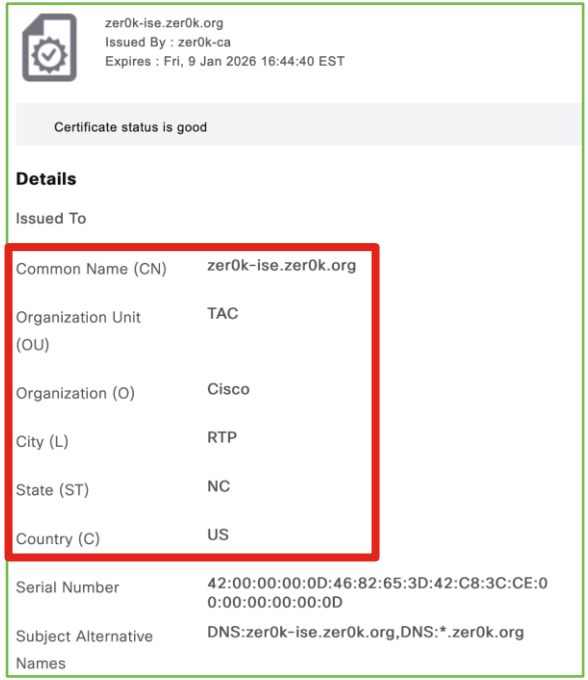
- Problem…. Renew certificate but keep same CN
- ISE does not allow 2 certificates with same subject.
- Uploading cert with same subject replaces existing cert.
- Can’t stage the certificate.
- Inconsistent replication of wildcard certs.



Wildcard Certificate Renewal

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
zer0k-wildsan	Admin, EAP Authentication		zer0k-ise.zer0k.org	zer0k-ca	Wed, 10 Jan 2024	Fri, 9 Jan 2026	Active

- Solution!
- The subject isn't just the CN, it is all of this!
- Change any 1 field and the subject is unique.

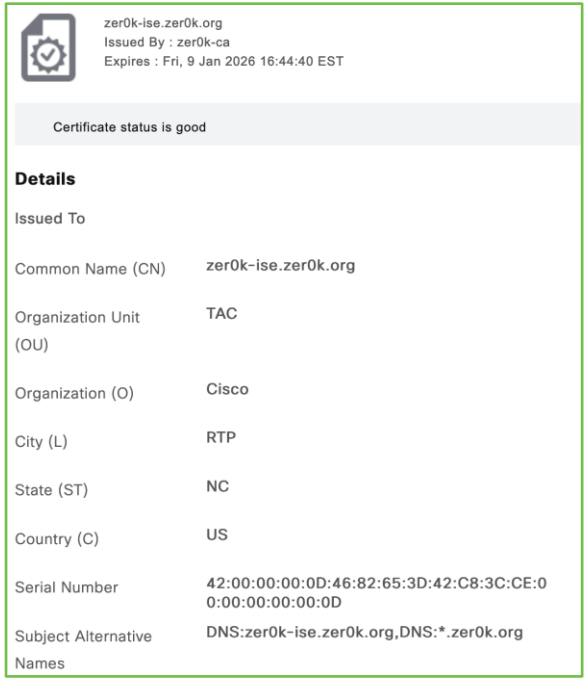


Wildcard Certificate Renewal

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
zer0k-wildsan	Admin, EAP Authentication		zer0k-ise.zer0k.org	zer0k-ca	Wed, 10 Jan 2024	Fri, 9 Jan 2026	Active

-= Prerequisite =-

- Ensure all nodes are in sync and not replicating slowly
- If CA certs have changed:
  - Upload them to ISE
  - Set them for “Trust for authentication within ISE” (admin) and/or “Trust for client authentication and Syslog” (EAP)

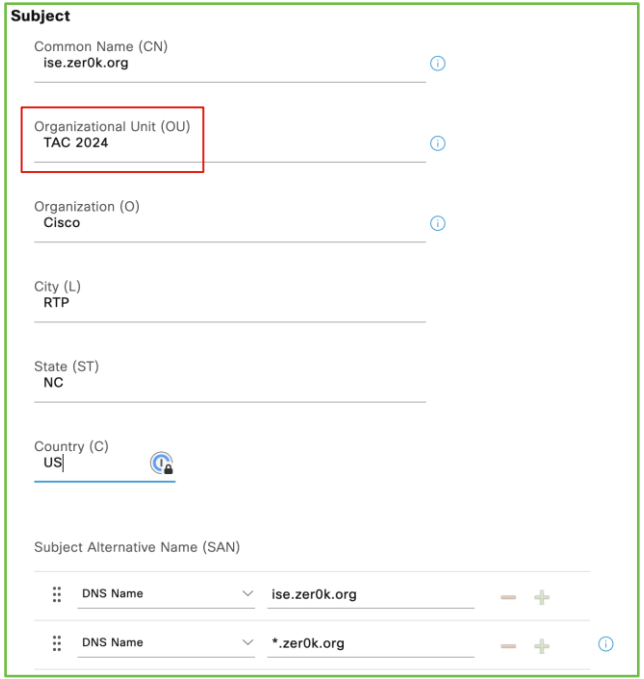


Wildcard Certificate Renewal

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
zer0k-wildsan	Admin, EAP Authentication		zer0k-ise.zer0k.org	zer0k-ca	Wed, 10 Jan 2024	Fri, 9 Jan 2026	Active

-= Step1 =-

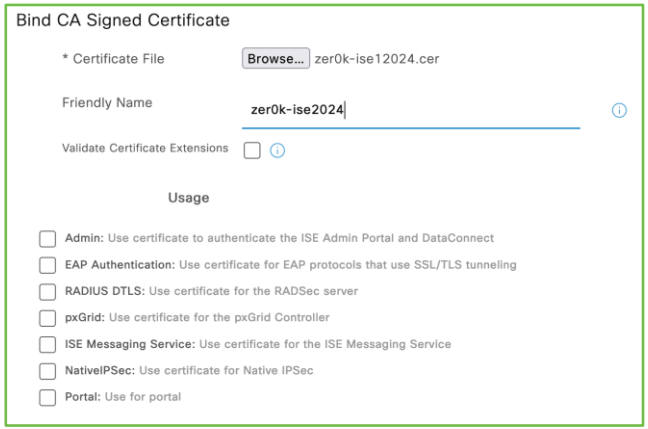
- Create a new CSR modifying the OU, O, L, ST, or C field.
  - OU tends to be the best candidate.
- Have CSR signed by CA.



Wildcard Certificate Renewal

-= Step 2 =-

- Bind cert to CSR without choosing any roles.
- Log directly into each node and view the certificates page.
- Verify that the certificate has been successfully replicated to all nodes.
- If not:
  - ISE 3.2+, syncup nodes with missing certs.
  - ISE 3.1 or earlier, delete cert, fix nodes, try again -or- deregister nodes, install wildcard cert, reregister nodes.

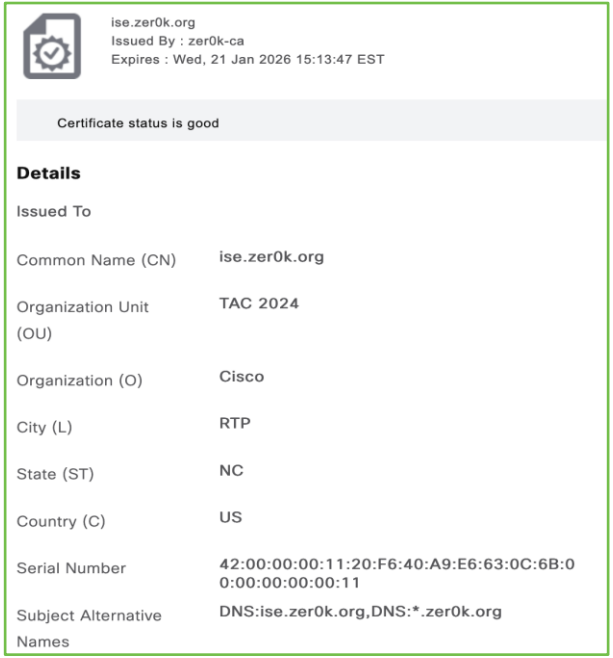


Wildcard Certificate Renewal

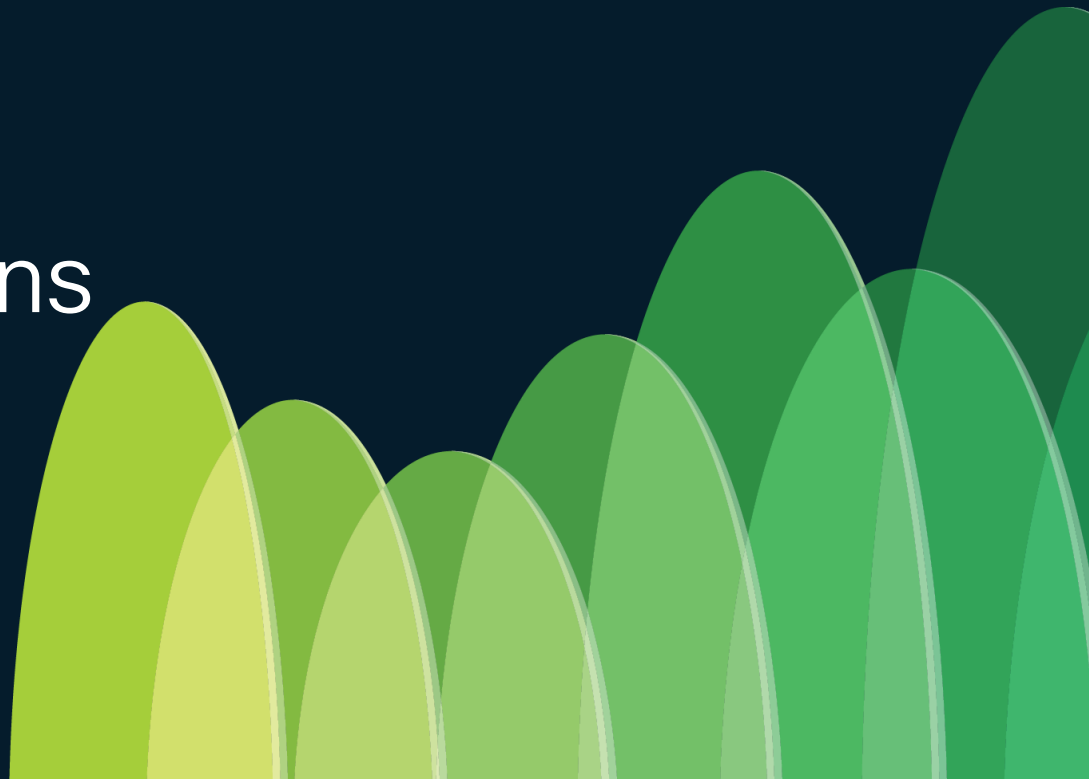
☐	zer0k-ise2024	Admin, EAP Authentication	ise.zer0k.org	zer0k-ca	Mon, 22 Jan 2024	Wed, 21 Jan 2026 ✅ Active

-= Step 3 =-

- Select desired roles for certificate.
  - If admin is selected all nodes will reboot.
  - ISE 3.3+ has scheduled restart feature.
- Test!
- Delete the old certificate.



Network Device Recommendations



cisco Live!

Accounting Best Practices (Wired)

- Ensure that start and stop accounting is configured
- Keep interim accounting to a minimum
  - Inactive sessions are purged after 5 days

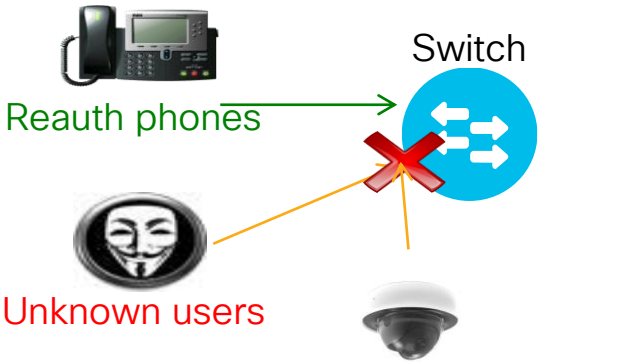
Cisco Switches

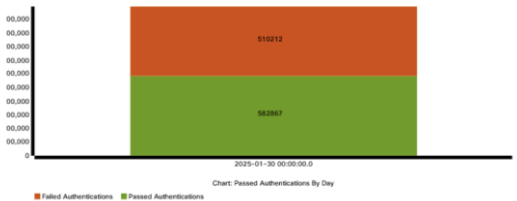
sw# aaa accounting update newinfo periodic 2880

https://cs.co/ise-wired

Tune Wired NAD Configuration

Rate Limiting at Wired Source

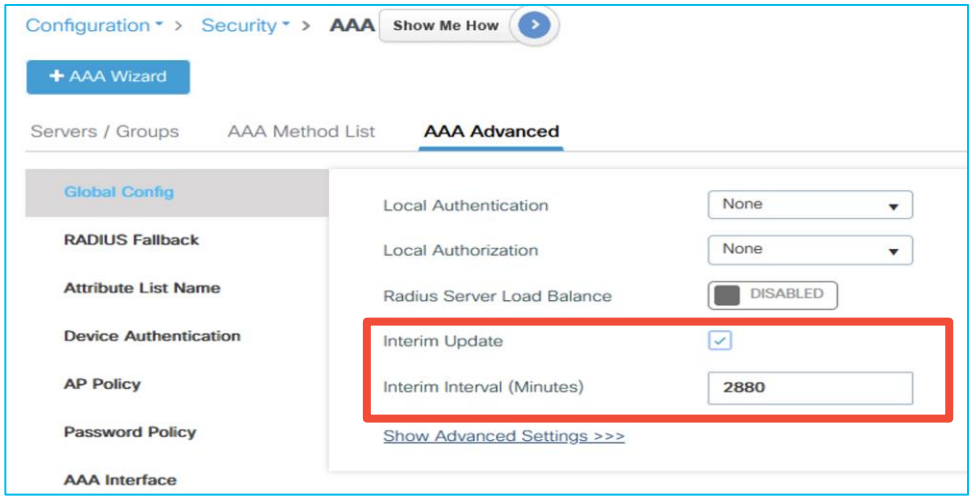




- **802.1X Timeouts**
  - held-period: Increase to 300+ sec
  - quiet-period: Increase to 300+ sec
  - ratelimit-period: Increase to 300+ sec
  - tx-period: 10 seconds
- **Inactivity Timer:** Disable or increase to 1+ hours (3600+ sec)
- **Session Timeout:** Disable or increase to 2+ hours (7200+ sec)
- **Reauth Timer:** Disable or increase to 2+ hours (7200+ sec)
- **Bugfixes:** Upgrade software to address critical defects.

9800 WLC

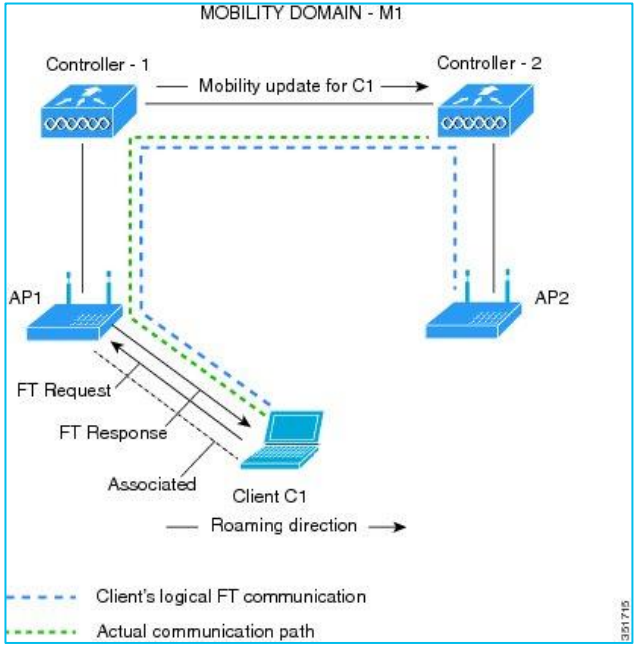
- Configure Interim-Accounting to send updates on new-info or roam only.



https://community.cisco.com/t5/security-knowledge-base/ise-and-catalyst-9800-series-integration-guide/ta-p/3753060

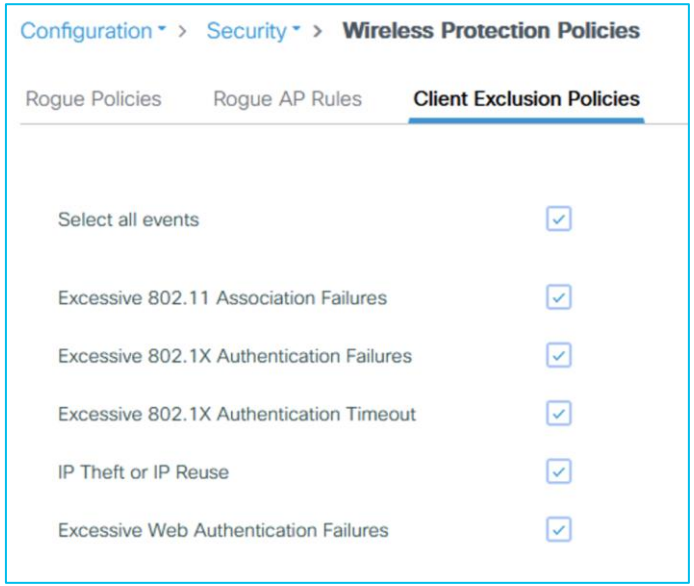
Use Fast BSS Transition (802.11r)

- Allow clients to roam without full 802.1x authentication.
- Supported by:
  - Apple Devices
  - Android Devices (platform and version dependent)
  - Some Windows devices (driver dependent)
- Clients that don't support 802.11r work on the same WLAN.
- TAC recommends over-the-air mode.

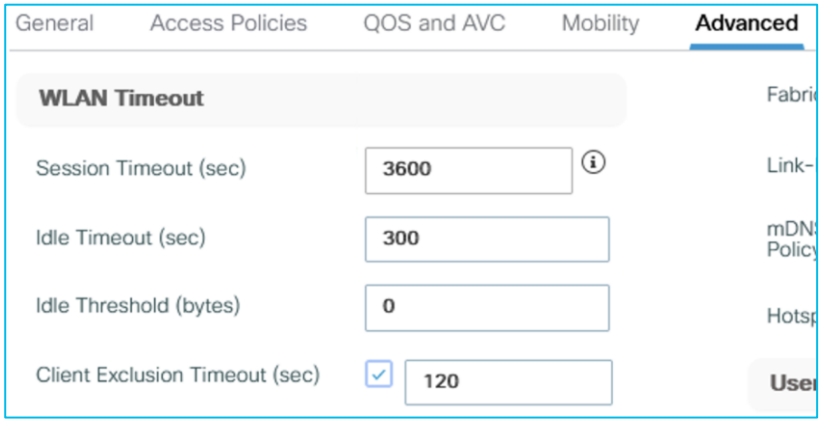


https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/802-11r-bss-fast-transition.html

9800 WLC Client Exclusions



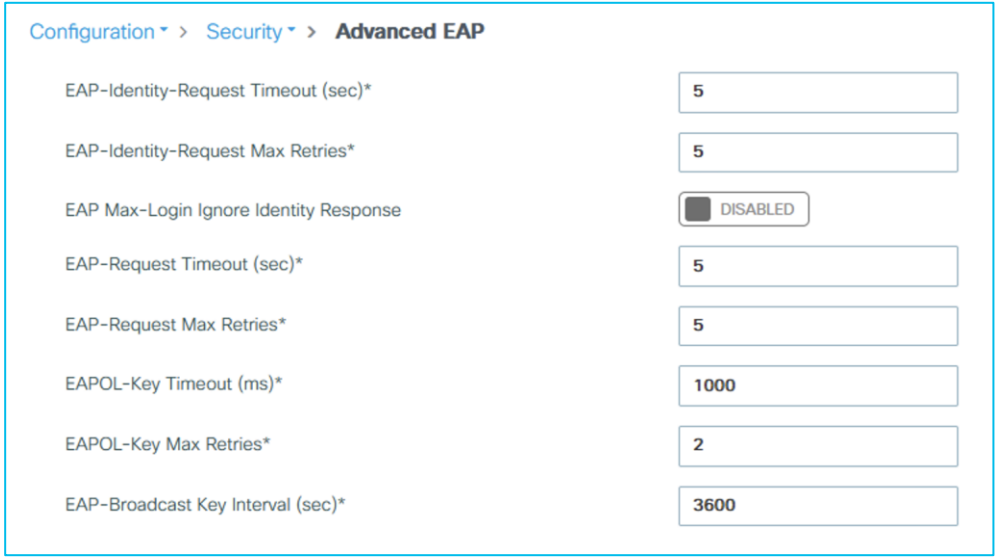
Configuration > Tags & Profiles > Policy



9800 WLC Client Exclusions

Tweaking EAP Timers

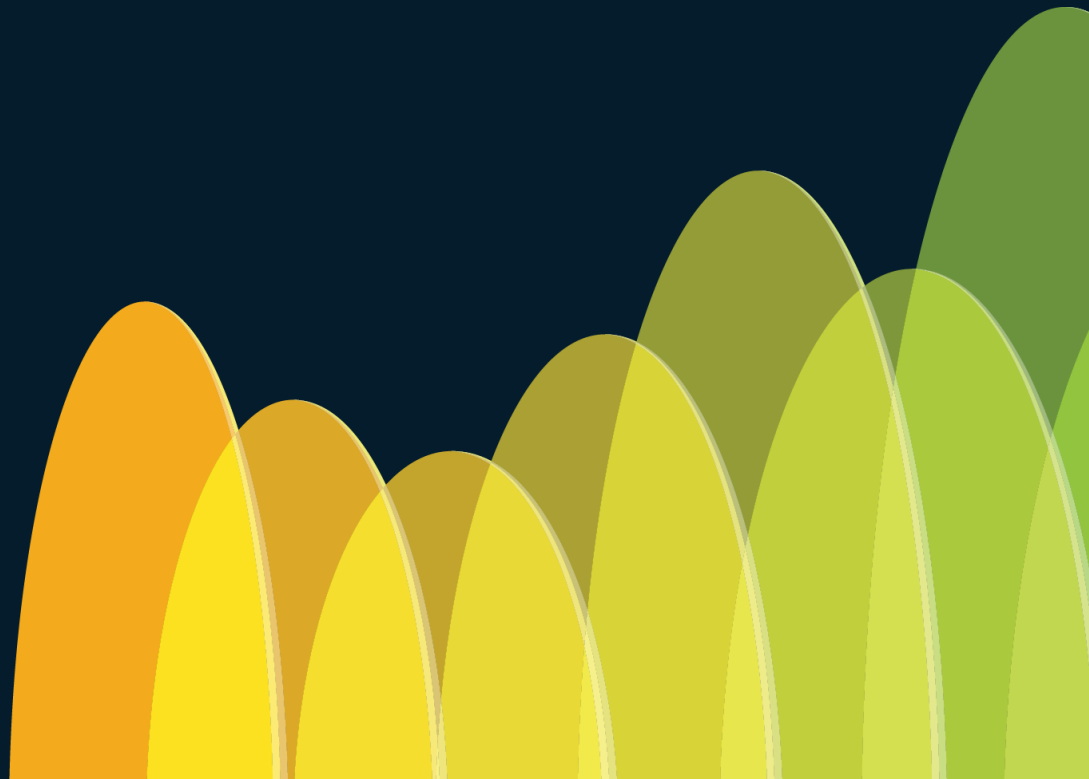
- Clients excluded on
  - 6th 802.1x failure
  - 5th 802.1x timeout
- Advanced EAP timers should be tweaked to allow exclusion before client restarts.



Number of RADIUS Servers

- Keep it to 3 or less
- 3 retries at 5 seconds means 15 seconds per server.
- Devices won't wait long enough to make more worth while.
- More adds more chance for cascading failures.
- Need more? Add a load balancer!
- Use a dead timer of 10 minutes or more.
  - If all servers are exhausted the top server will be tried before the deadtime expires.

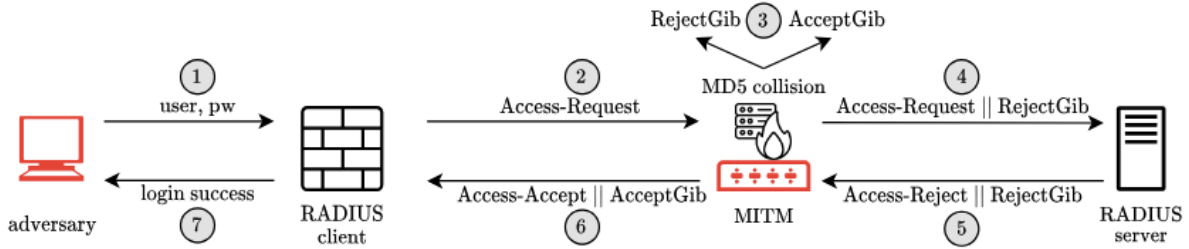
BlastRADIUS



cisco Live!

BlastRADIUS – What is it?

- CVE-2024-3596
- Uses online MD5 prefix collisions to modify a RADIUS response
  - Example - changing an Access-Reject to and Access-Accept
  - Must man-in-the-middle the RADIUS flow
- Can impact any Non-EAP RADIUS flow
  - EAP RFC Mandates the use of Message-Authenticator
- Utilizes the Proxy-State attribute to generate the collision gibberish

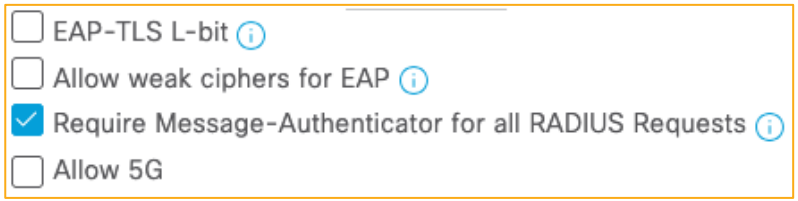


Mitigation – End to End Encryption

- Radius over TLS (TCP) or RADIUS over DTLS (UDP)
  - ISE Supports DTLS today
  - Prevents Man-in-the-middle using strong, modern encryption
  - Provides full packet privacy
- Requires deployment and continued management of certificates on ISE and NADs
- Up to 15% performance hit for ISE authentication rate.
- IPSec can be used but is limited to 50 tunnels per PSN.

Mitigation – Message-Authenticator

- Message-Authenticator
  - NAD must send it in all requests
  - Server must require it in all requests
  - Server must send it in all responses
  - NAD must require it in all responses

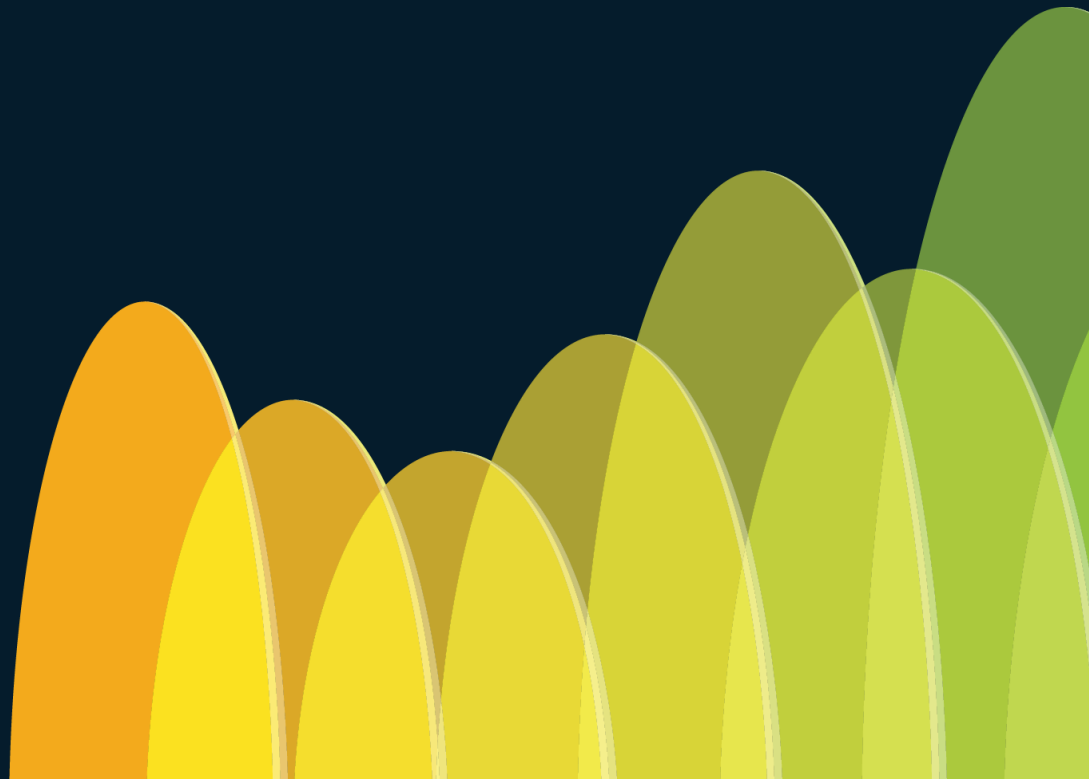


- ISE as a RADIUS Server can be configured per-above.
- ISE as a RADIUS Client: CSCwk67747
- 9800 sends and requires it with both 802.1x and MAC authentication
- IOS-XE sends and requires it with both 802.1x and MAC authentication

BlastRADIUS Resources

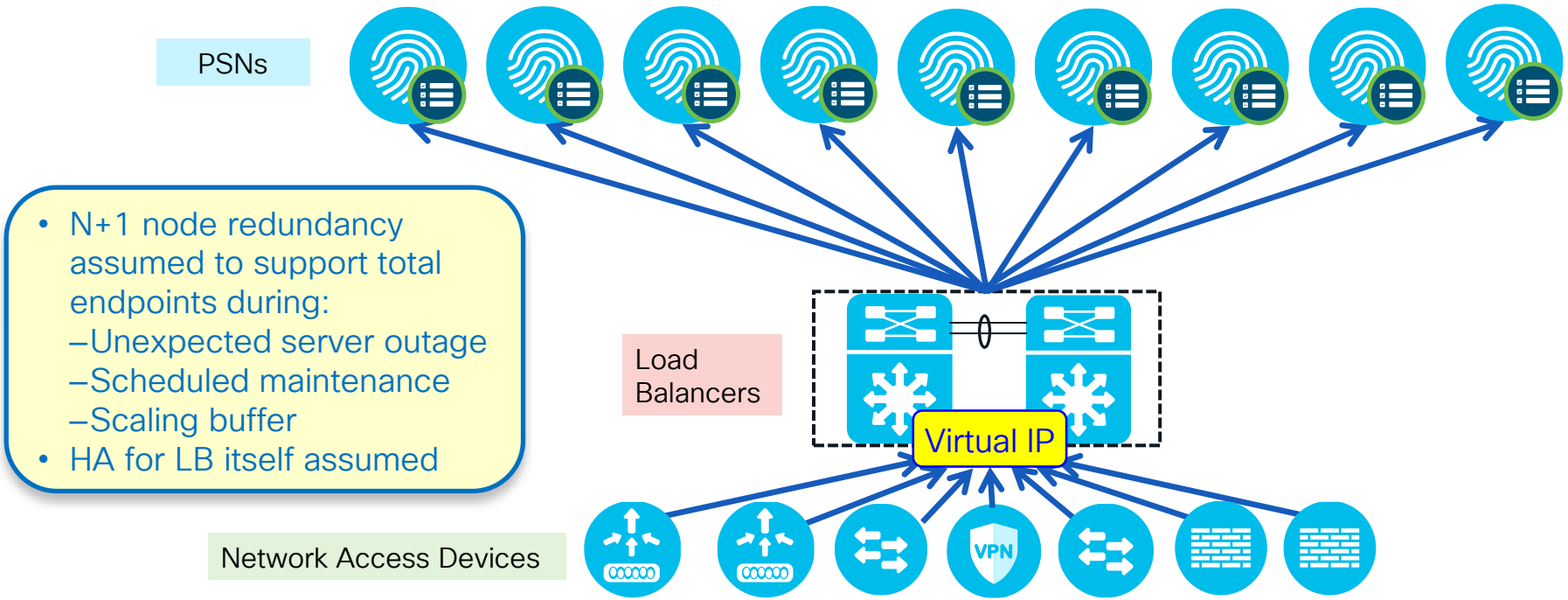
- Cisco Security Advisory
  - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3
- Mitigation Guide
  - https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/222287-blast-radius-cve-2024-3596-protocol-sp.html
- DTLS Configuration Example
  - https://community.cisco.com/t5/networking-knowledge-base/configuring-radius-over-dtls-with-cat9k-and-ise-3-0/ta-p/4438427

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 and TACACS+ AAA requests to LB virtual IP.



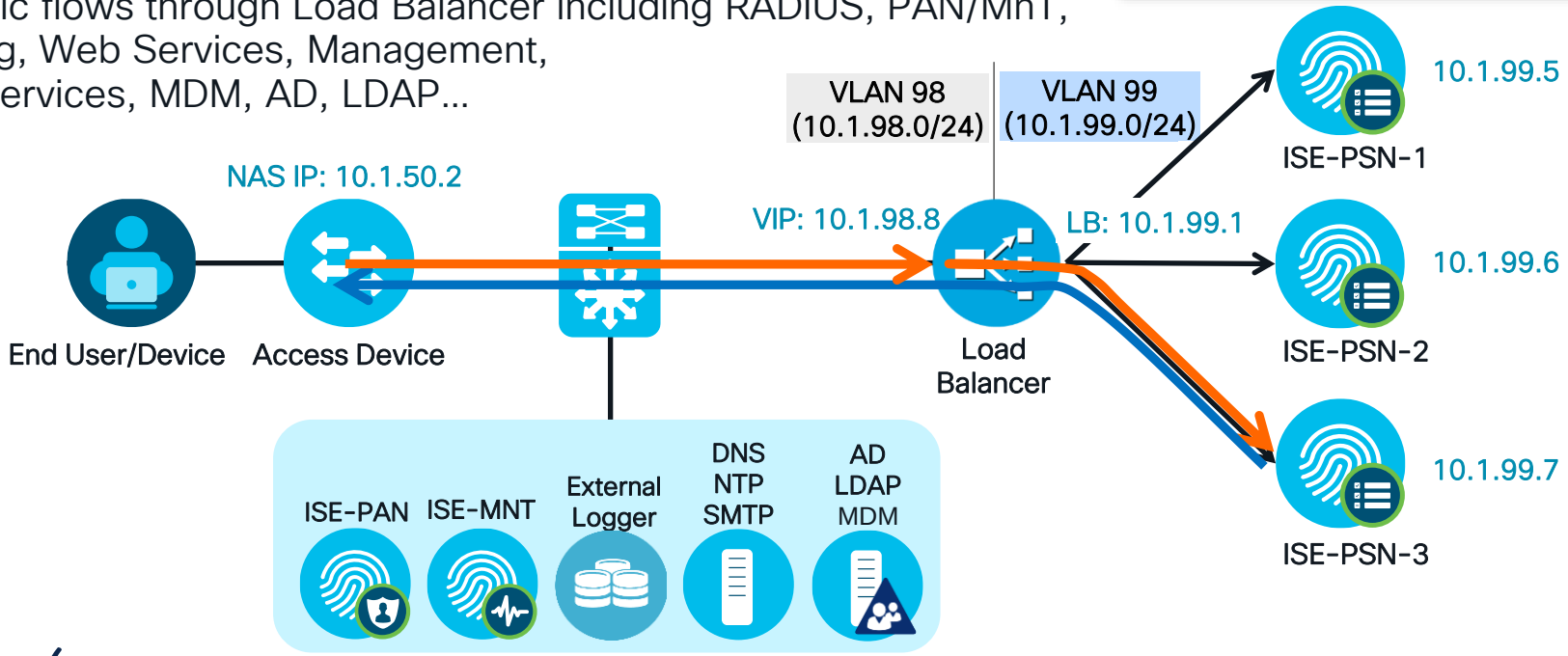
- N+1 node redundancy assumed to support total endpoints during:
  - –Unexpected server outage
  - –Scheduled maintenance
  - –Scaling buffer
- HA for LB itself assumed

Traffic Flow—Fully Inline: Physical Separation

Physical Network Separation Using Separate LB Interfaces

Fully Inline Traffic Flow recommended—physical or logical

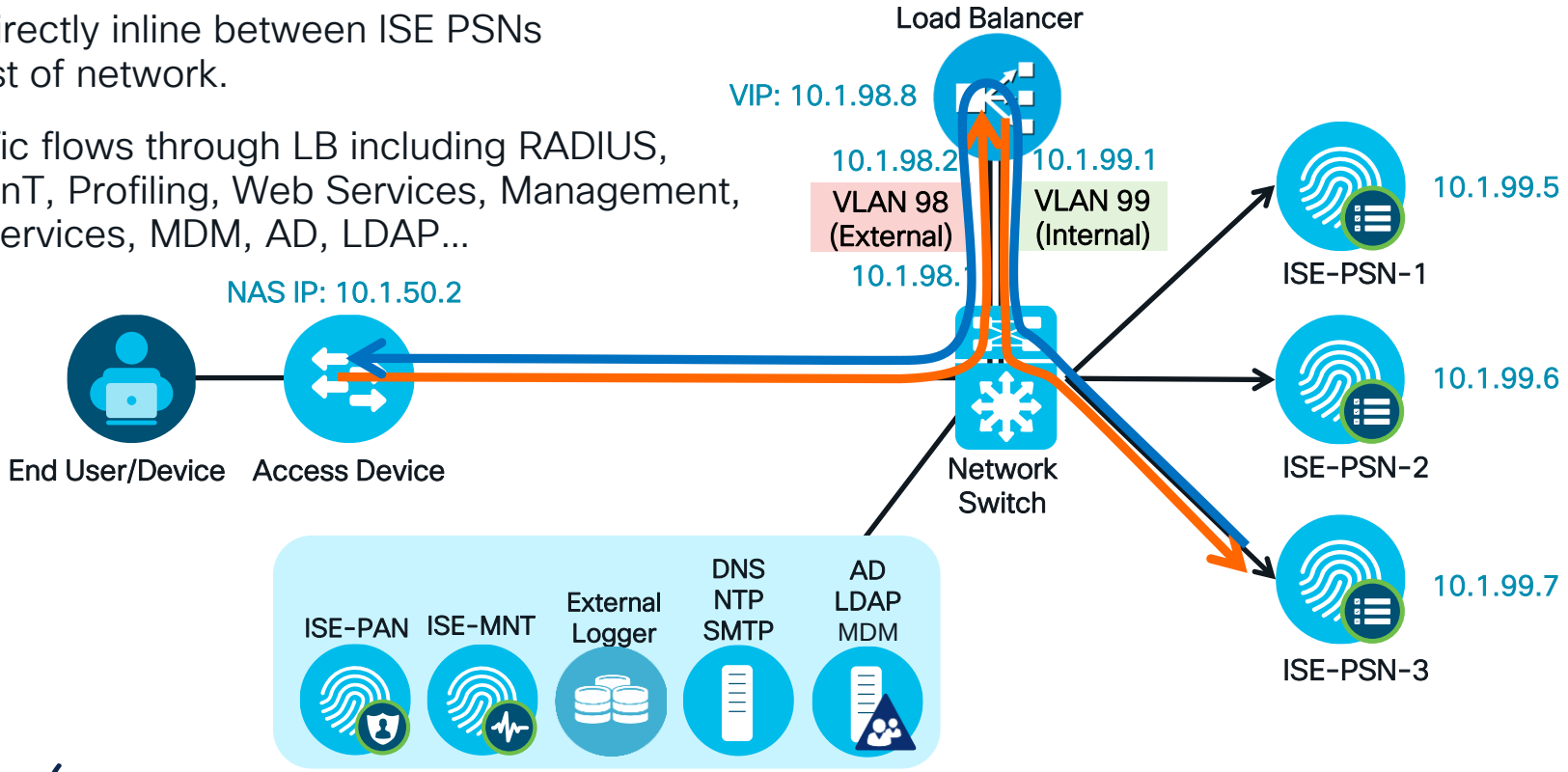
- Load Balancer is directly inline between PSNs and rest of network.
- All traffic flows through Load Balancer including RADIUS, PAN/MnT, Profiling, Web Services, Management, Feed Services, MDM, AD, LDAP…



Traffic Flow—Fully Inline: VLAN Separation

Logical Network Separation Using Single LB Interface and VLAN Trunking

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



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

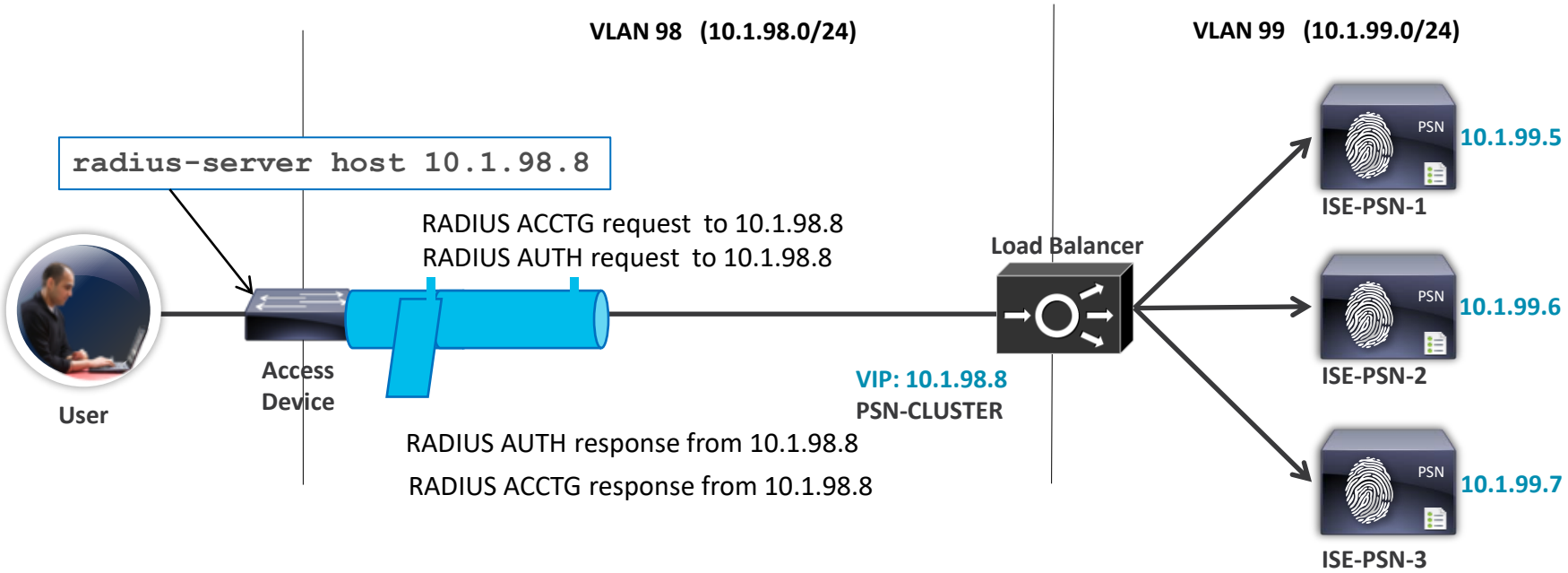
  LB VIP is the target for one-way Profile Data (no response required). VIP can be same or different than one used by RADIUS LB; Real server interface can be same or different than one used by RADIUS

- **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

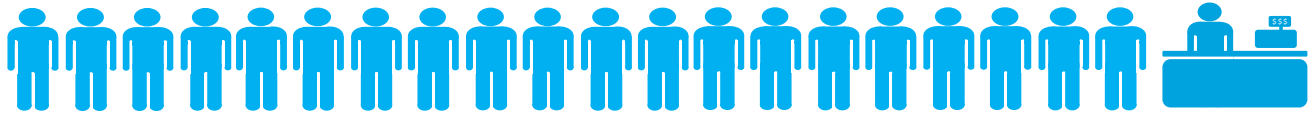
Avoid spraying packets!!!

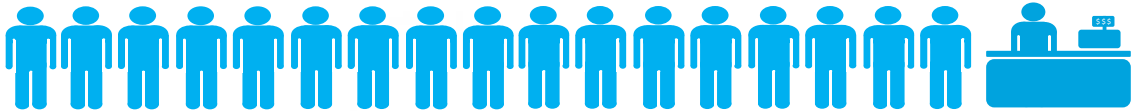


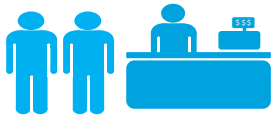
12953 Received EAP packet from the middle of conversation that contains a session on this PSN that does not exist
11051 RADIUS packet contains invalid state attribute

Load Balancing RADIUS

IP vs Calling Station ID Stickiness

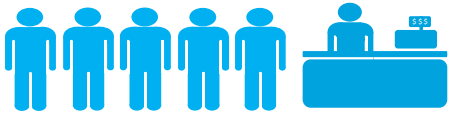






Use Calling-Station-ID for Stickiness

Fallback to NAS-IP-Address



Load Balancer RADIUS Test Probes

Citrix Example

- Probe frequency and retry settings:
  - Time interval between probes:
    interval *seconds* # Default: 5
  - Number of retries
    retries *number* # Default: 3
- Sample Citrix probe configuration:

```
add lb monitor PSN-Probe RADIUS -respCode 2
-userName citrix_probe -password citrix123
-radKey cisco123 -LRTM ENABLED -interval 10
-retries 3 -destPort 1812
```

- Recommended setting: Failover must occur before RADIUS timeout (typically 15-35 sec) while avoiding excessive probing

F5 Example

- Probe frequency and retry settings:
  - Time interval between probes:
    Interval *seconds* # Default: 10
  - Timeout before failure = 3*(interval)+1:
    Timeout *seconds* # Default: 31
- Sample F5 RADIUS probe configuration:

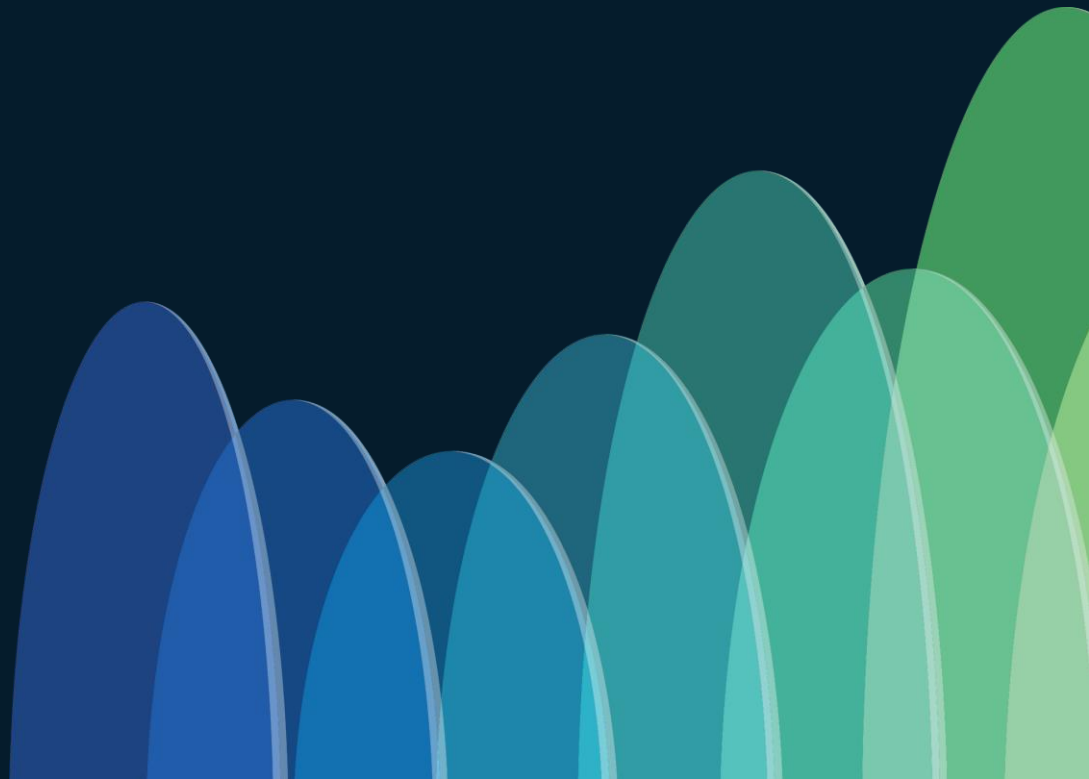
```
Name PSN-Probe
Type  RADIUS
Interval 10
Timeout 31
Manual Resume No
Check Util Up Yes
User Name f5-probe
Password f5-ltm123
Secret cisco123
Alias Address * All Addresses
Alias Service Port 1812
Debug No
```

Load Balancer for ISE Best Practice Check List

- Persistence (Stickyness) is a must!
- Persistence based on Calling-Station-ID is best
- Avoid using Source-IP address for sticky value
- Sticky Timers need to be at least 1 hour
- DO NOT Round Robin Traffic
- Use the vendor specific guides from the community:

https://cs.co/ise-berg#load-balancing

Profiling



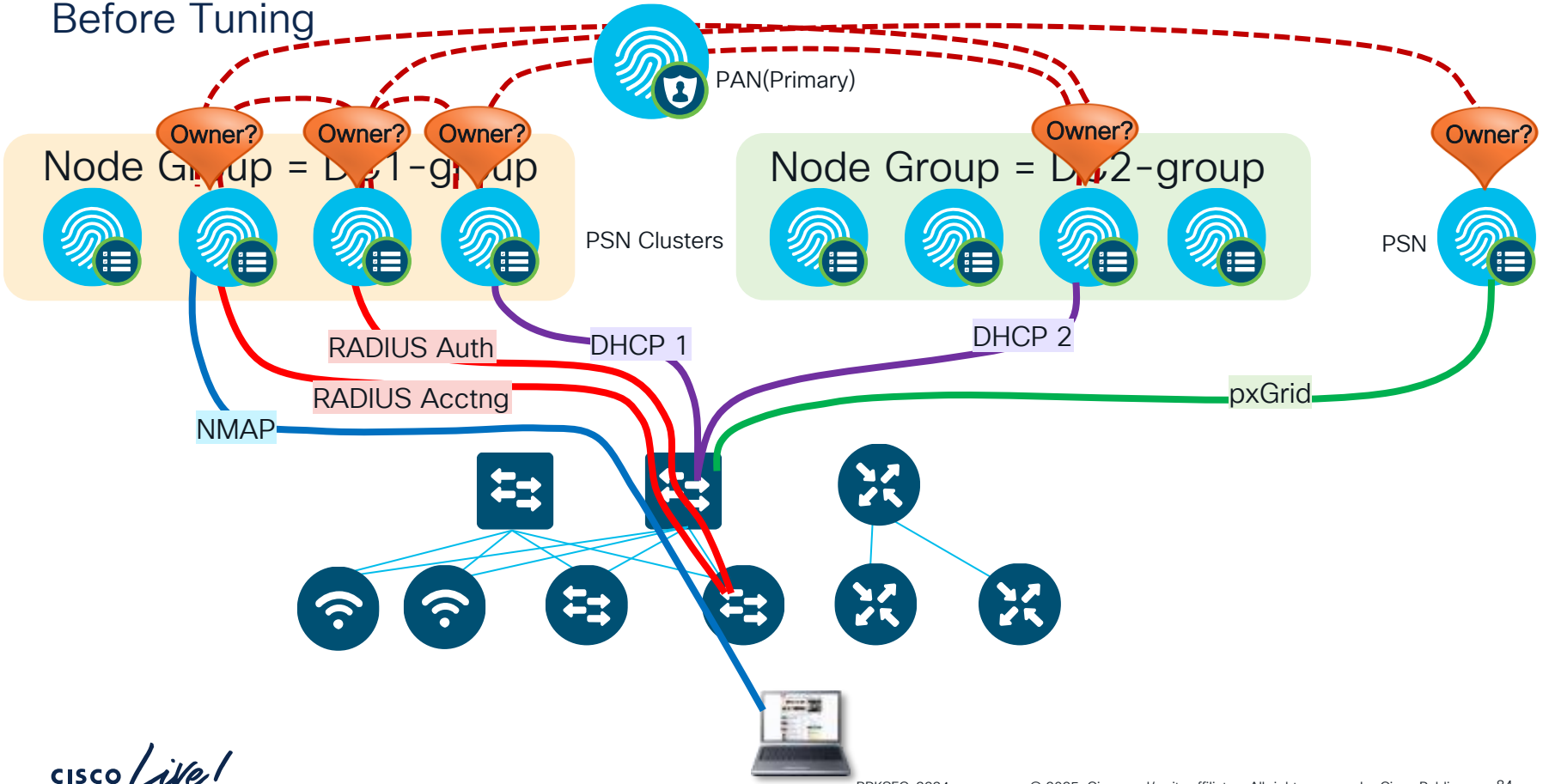
Profiling Probe Selection Best Practices

Probe	Key Profiling Attributes
RADIUS	MAC Address (OUI), IP Address, NDG values
RADIUS w/Device Sensor	CDP/LLDP, DHCP, User-Agent, mDNS, H323/SIP
RADIUS w/ACIDex	MAC Address (OUI), UDID, Operating System, Platform/Device Type
SNMP	MAC Address (OUI), CDP/LLDP, ARP tables
DHCP	DHCP
DNS	FQDN
HTTP	User-Agent
NetFlow	Protocol, Source/Dest IP, Source/DestPorts
NMAP	OS, Common and custom ports, Service Version Info, SMB & SNMP data
AD	Operating System and Version, AD Domain
pxGrid	IoT Asset, Custom Attributes
Endpoint Custom Attributes	*Customer defined*

ISE Profiling Design Guide cs.co/ise-profiling

Impact of Ownership Changes

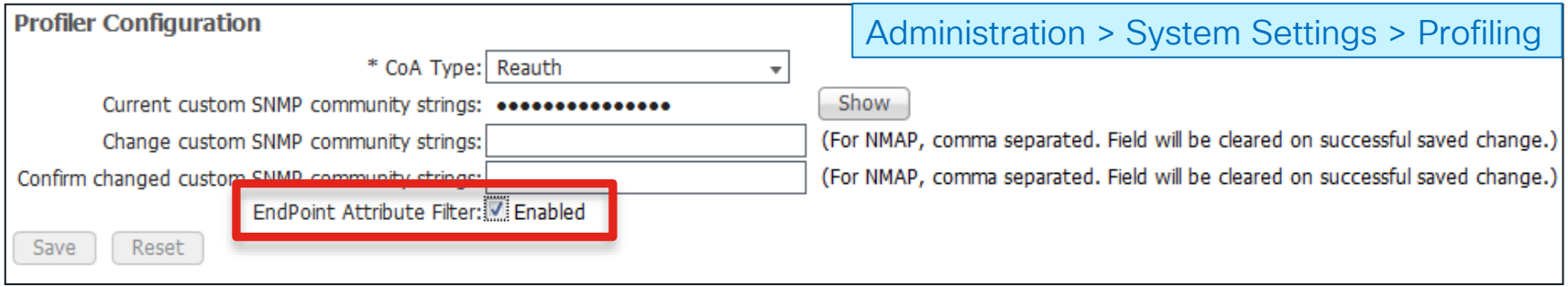
Before Tuning



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.

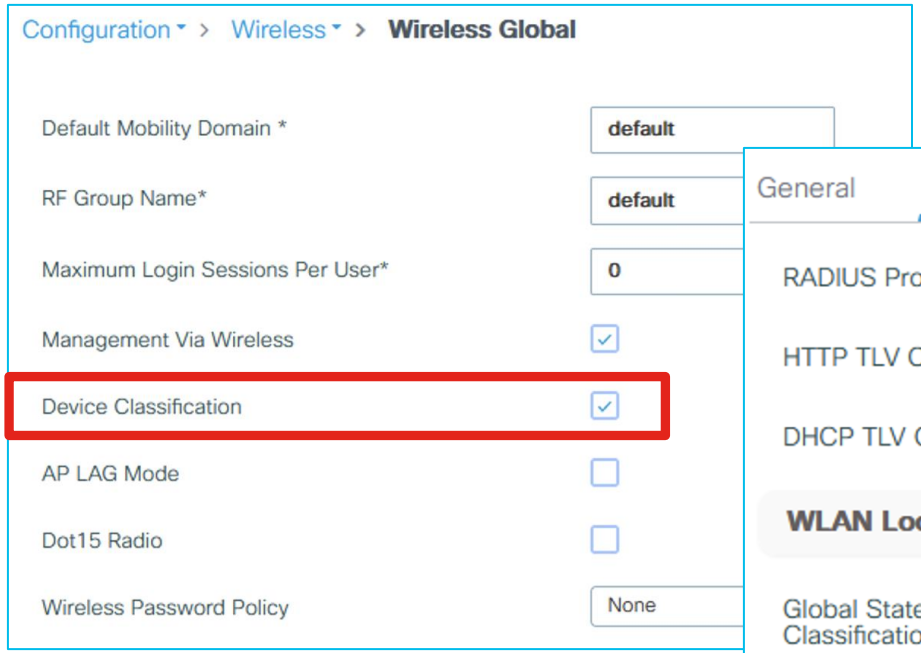


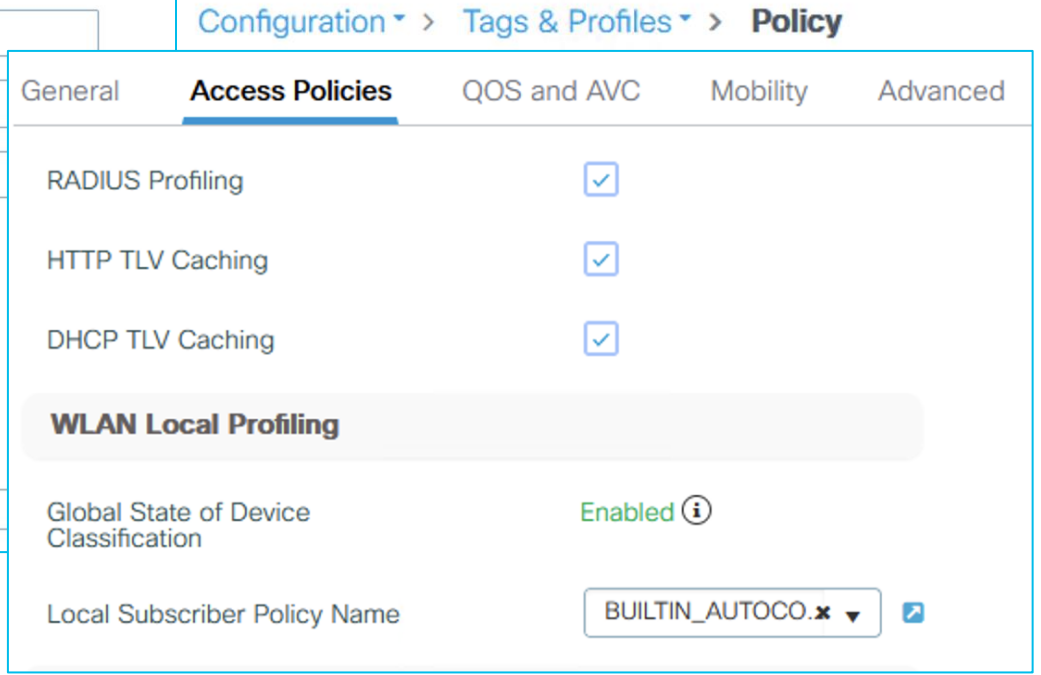
- Whitelist Filter limits profile attribute collection to those required to support default (Cisco-provided) profiles and critical RADIUS operations.
  - Filter must be disabled to collect and/or replicate other attributes.
  - Attributes used in custom conditions are automatically added to whitelist.

Device Sensor

- Sends profiling via RADIUS Accounting
- Replaces Probes:
  - HTTP Probe
  - SNMP Probe
    - CDP/LLDP
  - DHCP Probe
- No additional load balancing considerations
- Supported on Cisco Catalyst Switches and WLCs

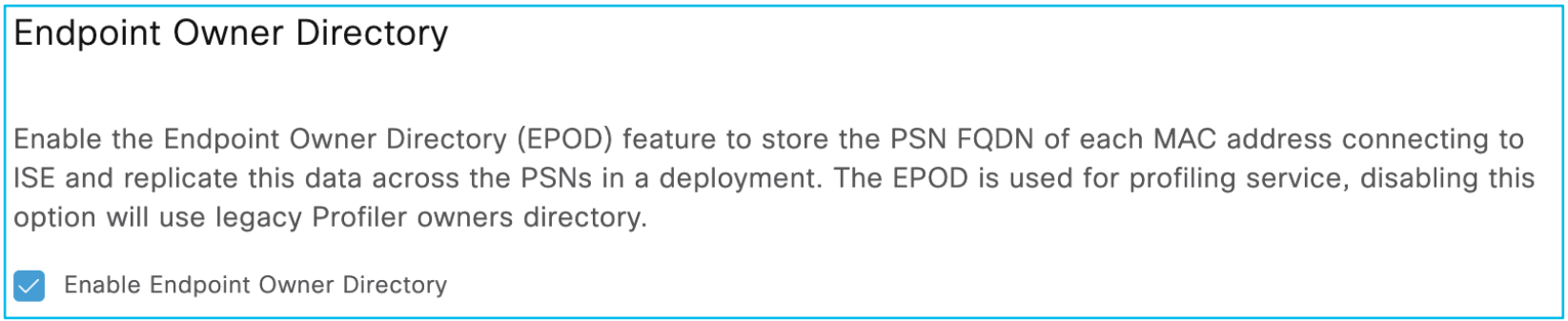
Device Sensor (9800)





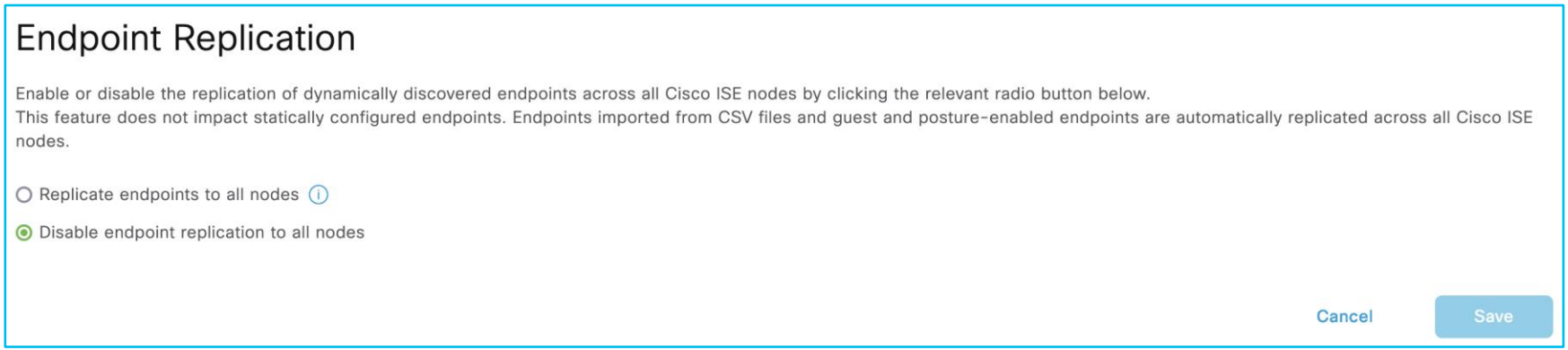
Profiling Endpoint Owner Directory

- Changes how endpoint ownership works
- Rather then new PSN taking ownership and transferring attributes to itself, queries current owner instead.
  - Reduces owner thrashing
  - Reduces data sent between nodes
- Administration -> System -> Settings -> Light Data Distribution



Endpoint replication

- Endpoint replication has two channels, Jgroups and Redis (mesh)
- Remove redundant replication which was eating up resources
- Only impacts dynamically learned (profiled) endpoints
- Enabled by default after upgrade to ISE 3.3.
- Administration -> System -> Settings -> Endpoint Replication



ISE Profiling Best Practices

General Guidelines for Probes

- **HTTP Probe:**
  - Use URL Redirects instead of SPAN to centralize 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!
  - Avoid DHCP SPAN. If used, make sure probe captures traffic to central DHCP Server. HA challenges.
- **SNMP Probe:**
  - 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:**
  - Use only for specific use cases in centralized 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.

ISE Profiling Best Practices

- Whenever Possible…

- Use Device Sensor on Cisco switches & Wireless Controllers to optimize data collection.
- Ensure profile data for a given endpoint is sent to a single PSN (or maximum of 2)
  - Sending same profile data to multiple PSNs increases inter-PSN traffic and contention for endpoint ownership.
- Ensure profile data for a given endpoint is sent to the *same* PSN
  - Same issue 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.
  - Node Groups reduce inter-PSN communications and need to replicate endpoint changes outside of node group.
- Avoid probes that collect the same endpoint attributes
  - Example: Device Sensor + DHCP Probe
- Enable Endpoint Attribute Filter

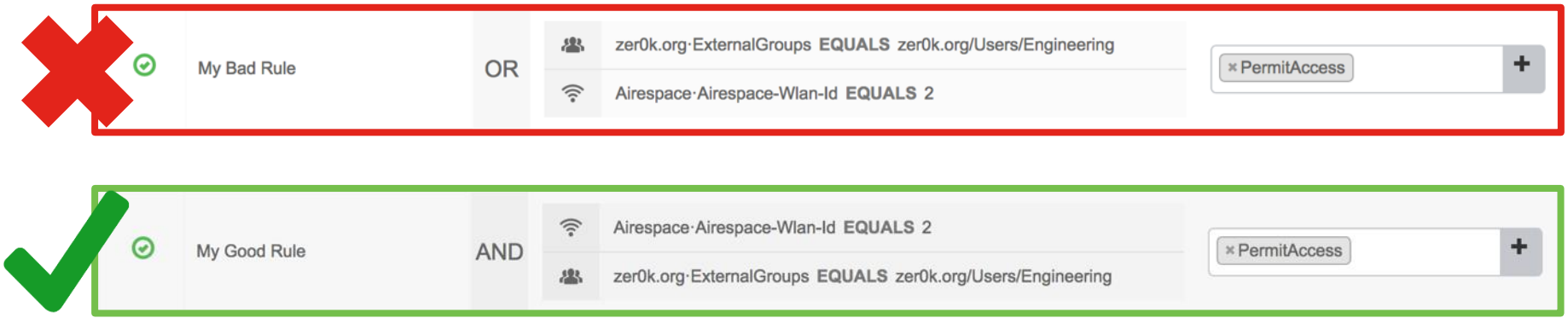
External Databases

Policy Sets

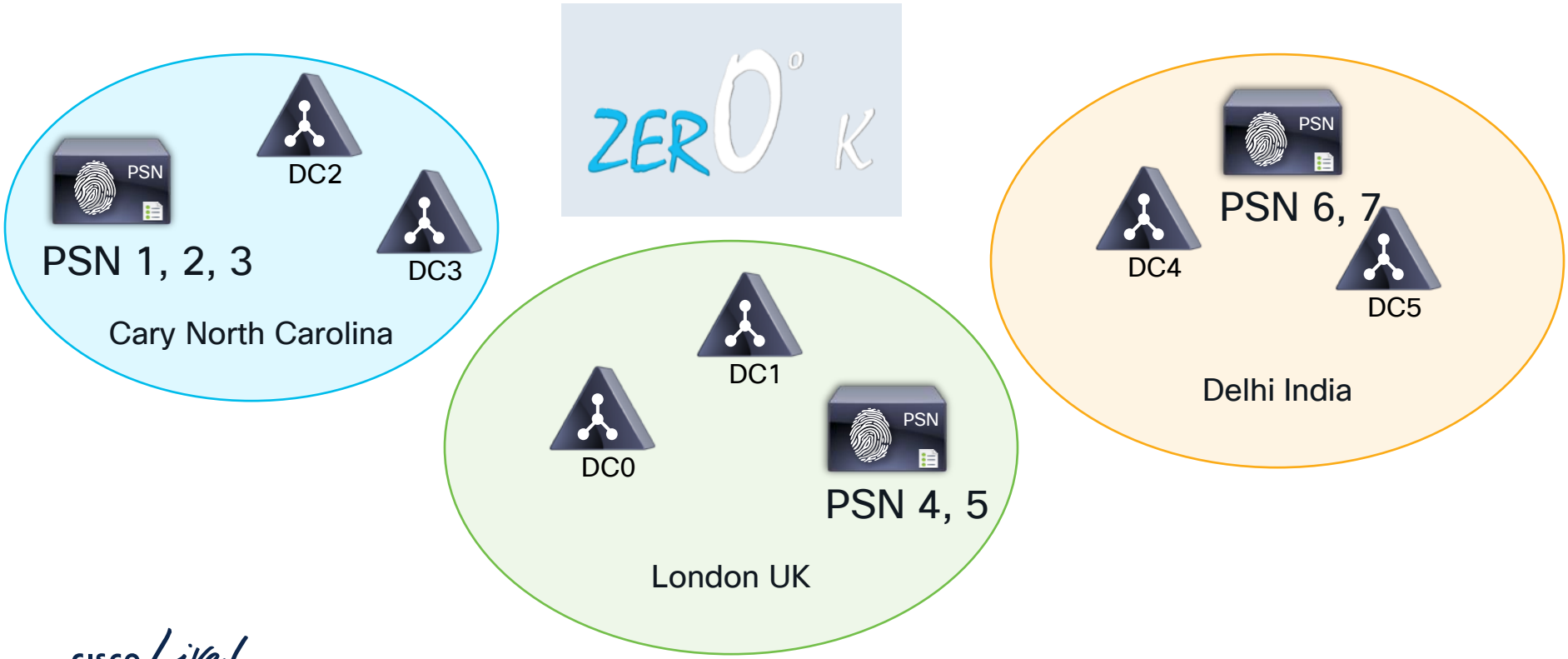
- USE THEM!
- Group Like Rules:
  - Guest vs. Corporate SSID, MAB vs 802.1x devices, etc…
- Improves rule readability.
- Reduces configuration mistakes.
- Improves rule processing.
- Can be created based on any attribute available in initial RADIUS packet.

Authorization Best Practices

- Order conditions so internal attributes are matched before external attributes
- Do not authorize MAC addresses against Active Directory
  - Why would this be a bad idea?
  - Use **Network Access:AuthenticationIdentityStore** to reduce external ID store lookups
- Order rules from most used to least used



MS AD Sites and Services



DNS Caching

- Active Directory is DNS Heavy!
- Enabled by default starting with ISE 3.3

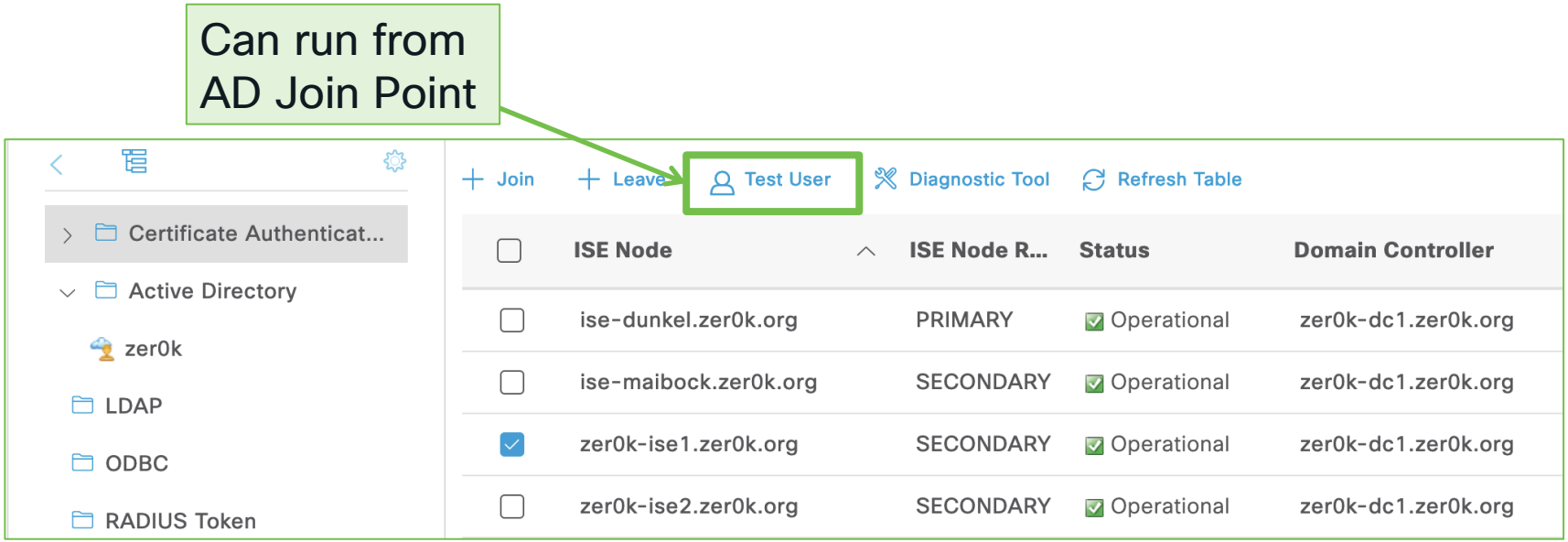
From each node CLI:
service cache enable hosts ttl 180

No.	Time	Source	Destination	Protocol	Length	Info
1824	37.482898	172.18.124.26	172.18.124.23	DNS	121	Standard query 0xc9c9 SRV _ldap._tcp.Default-First-Site-Name._sites.gc._msdcs.zer0k.org
1825	37.484022	172.18.124.23	172.18.124.26	DNS	313	Standard query response 0xc9c9 SRV _ldap._tcp.Default-First-Site-Name._sites.gc._msdcs.z
1840	37.687312	172.18.124.26	172.18.124.23	DNS	79	Standard query 0xfa2f A zer0k-dc1.zer0k.org
1841	37.687312	172.18.124.26	172.18.124.23	DNS	79	Standard query 0xfe2b AAAA zer0k-dc1.zer0k.org
1842	37.687640	172.18.124.23	172.18.124.26	DNS	135	Standard query response 0xfe2b AAAA zer0k-dc1.zer0k.org AAAA fd2f:624f:f359:c124:1eea:47
1843	37.687643	172.18.124.23	172.18.124.26	DNS	111	Standard query response 0xfa2f A zer0k-dc1.zer0k.org A 172.18.124.23 A 172.30.112.1
2097	41.767565	172.18.124.26	172.18.124.23	DNS	80	Standard query 0xdd8a A ise-dunkel.zer0k.org
2098	41.767565	172.18.124.26	172.18.124.23	DNS	80	Standard query 0x5a88 AAAA ise-dunkel.zer0k.org
2099	41.767909	172.18.124.23	172.18.124.26	DNS	137	Standard query response 0x5a88 AAAA ise-dunkel.zer0k.org SOA zer0k-dc1.zer0k.org
2100	41.767909	172.18.124.23	172.18.124.26	DNS	96	Standard query response 0xdd8a A ise-dunkel.zer0k.org A 172.18.124.20
2144	42.784260	172.18.124.26	172.18.124.23	DNS	80	Standard query 0x9905 A zer0k-ise2.zer0k.org
2145	42.784260	172.18.124.26	172.18.124.23	DNS	80	Standard query 0xc20e AAAA zer0k-ise2.zer0k.org
2146	42.784586	172.18.124.23	172.18.124.26	DNS	96	Standard query response 0x9905 A zer0k-ise2.zer0k.org A 172.18.124.28
2147	42.784586	172.18.124.23	172.18.124.26	DNS	137	Standard query response 0xc20e AAAA zer0k-ise2.zer0k.org SOA zer0k-dc1.zer0k.org
2810	55.026035	172.18.124.26	172.18.124.23	DNS	81	Standard query 0x33c0 A ise-maibock.zer0k.org
2811	55.026035	172.18.124.26	172.18.124.23	DNS	81	Standard query 0xc53e AAAA ise-maibock.zer0k.org
2812	55.026389	172.18.124.23	172.18.124.26	DNS	97	Standard query response 0x33c0 A ise-maibock.zer0k.org A 172.18.124.21
2813	55.026394	172.18.124.23	172.18.124.26	DNS	138	Standard query response 0xc53e AAAA ise-maibock.zer0k.org SOA zer0k-dc1.zer0k.org
3969	78.222560	172.18.124.26	172.18.124.23	DNS	80	Standard query 0xaf3f A ise-dunkel.zer0k.org
3970	78.222560	172.18.124.26	172.18.124.23	DNS	80	Standard query 0xde3c AAAA ise-dunkel.zer0k.org
3971	78.222960	172.18.124.23	172.18.124.26	DNS	137	Standard query response 0xde3c AAAA ise-dunkel.zer0k.org SOA zer0k-dc1.zer0k.org
3972	78.223423	172.18.124.23	172.18.124.26	DNS	96	Standard query response 0xaf3f A ise-dunkel.zer0k.org A 172.18.124.20

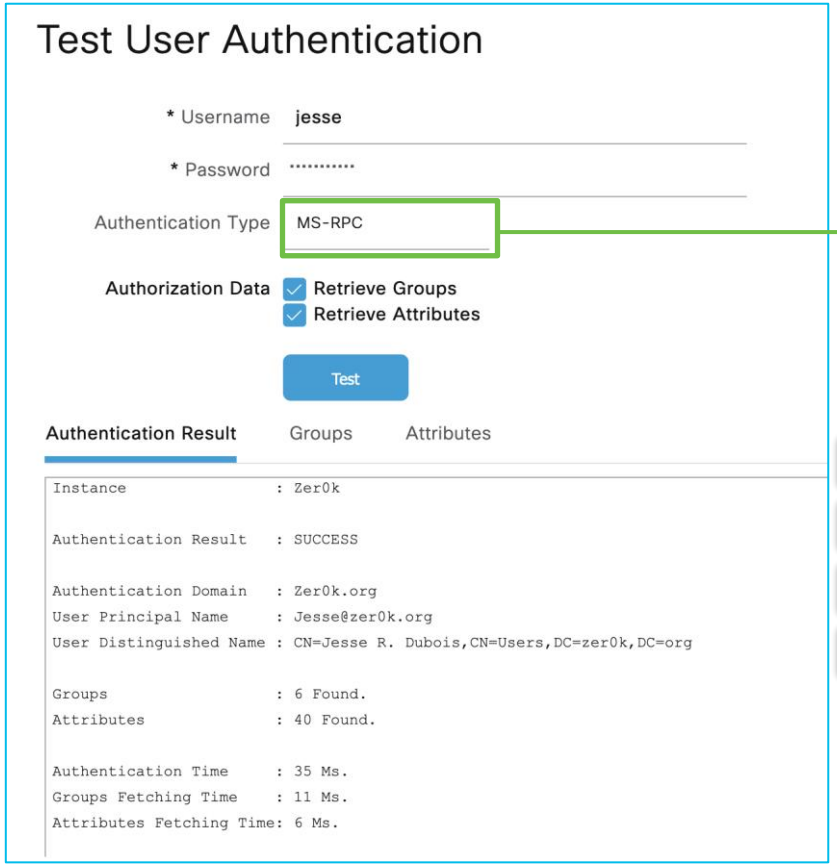
AD Join Point and Authentication Domains

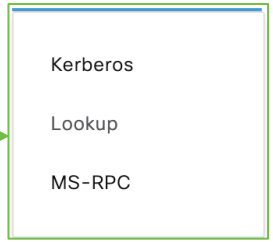
- Trusted (intra-/inter-forest) domains automatically discovered from the Join Point.
- These are the domains with 2-way bidirectional trust with the Join Point.
- You can then select/deselect which one to use (all selected by default).
- Deselect domains not used by ISE.

AD Test Authentication



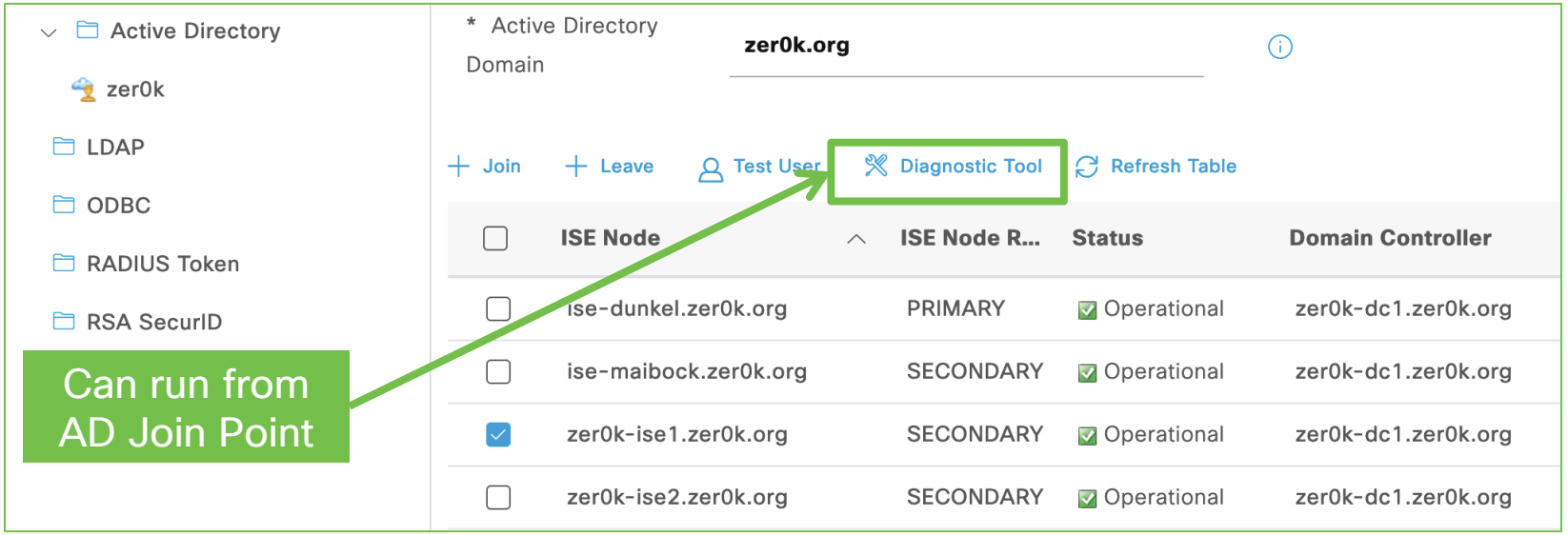
AD Test Authentication



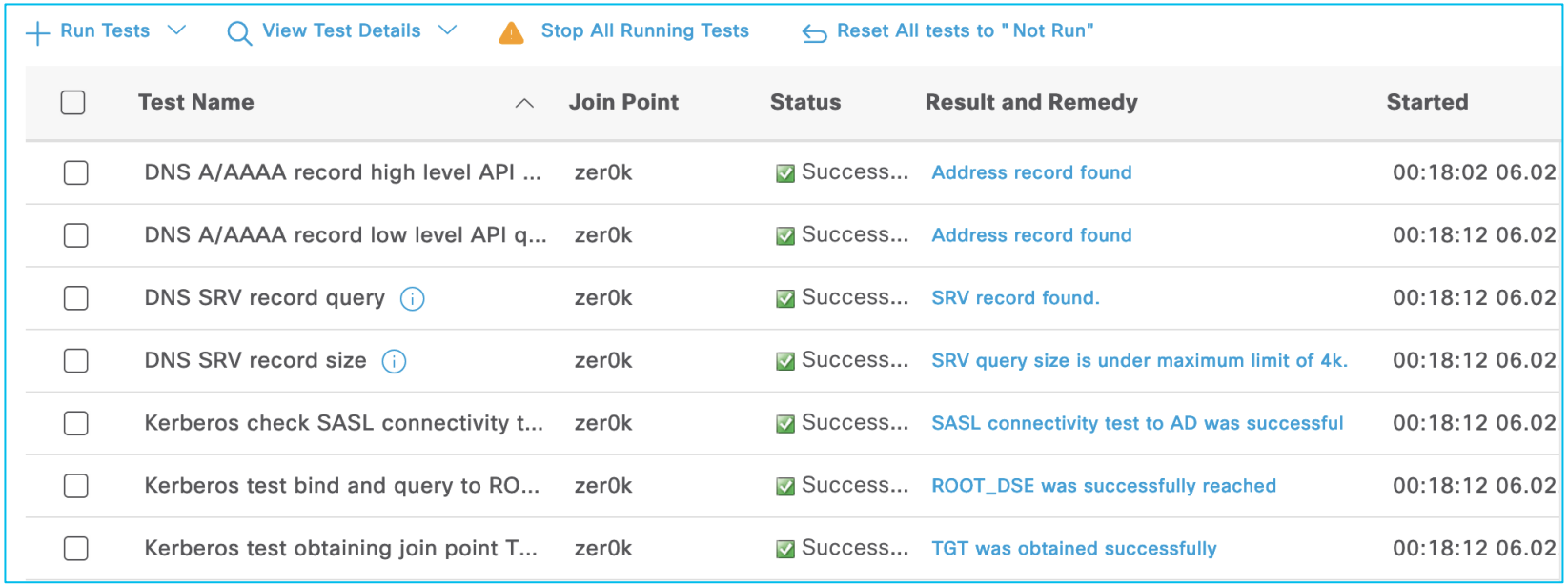


- Different authentication types
- ISE node can be selected to run the test auth
- Can provide group & attribute details if options are selected
- Millisecond Response Times

Domain Diagnostics



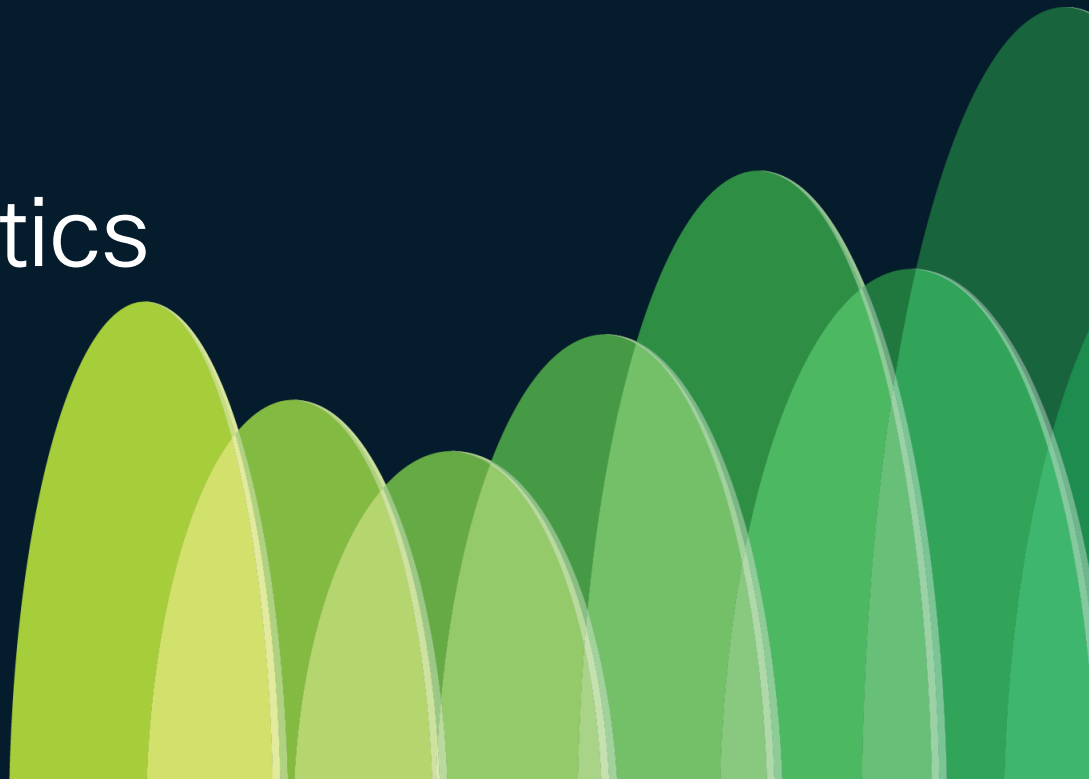
Domain Diagnostics



Active Directory Best Practices

- Use Sites and Services to contact local domain controllers
- Use Allowed Domains to restrict negative lookups
- Dedicate Domain Controllers in high volume environments
- Enable DNS Caching on each node
- Test and Monitor for Request Latency
- Use Domain Diagnostics to ensure Active Directory health

MnT / Log Analytics



External Syslog

- Use IP address where possible
- Limit number of Syslog targets
- Limit log categories
- Logging is done directly from the PSNs

zer0k_splunk	splunk.zer0k.org	514	UDP SysLog
zer0k_splunk_IP	172.18.124.23	514	UDP SysLog

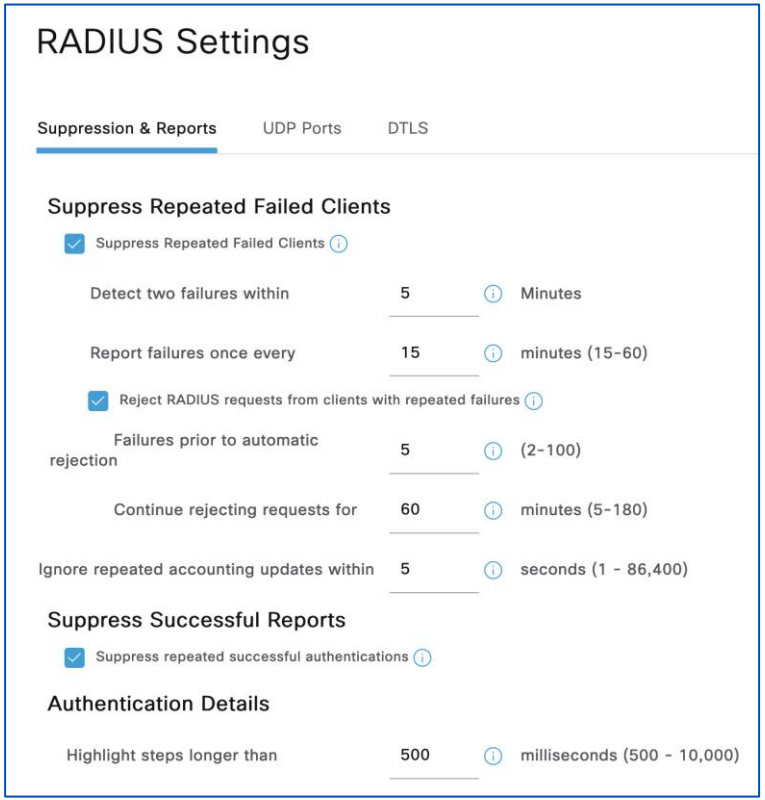
DNS Caching

- Enabled by default starting with ISE 3.3
  - External SYSLOG with FQDN sends DNS request for every SYSLOG packet without it!

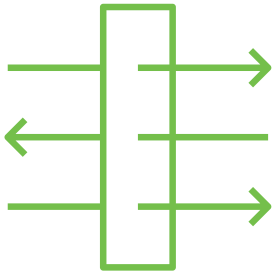
service cache enable hosts ttl 180

Logging Suppression

Administration -> Settings -> Protocols -> RADIUS

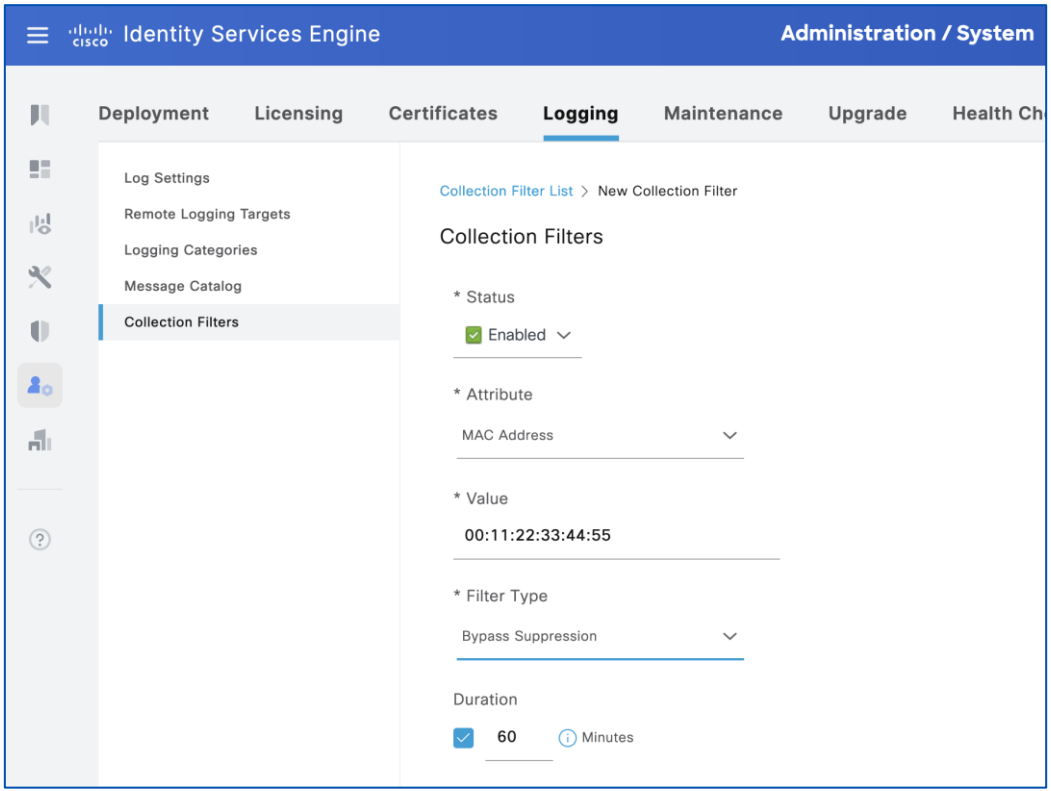


- Do not disable suppression on production deployments.
- If troubleshooting, disable on a per client basis.
- Protects the deployment!



Manual Collection Filters

Administration -> Logging -> Collection Filters



Keepalive Probes

Failed Accepted

- IOS XE treats a failed authentication as alive
  - Some load balancers such as F5 and Netscalaer as well
- Can expect probe to always fail authentication
- Filter only failed so any passed can be audited
- Other devices may see failed as alive, must test

Status	Attribute	Value	Filter Type	Time left (in minutes)
Enabled	User Name	ios-probe	Filter Failed	Unlimited

Keepalive Probes

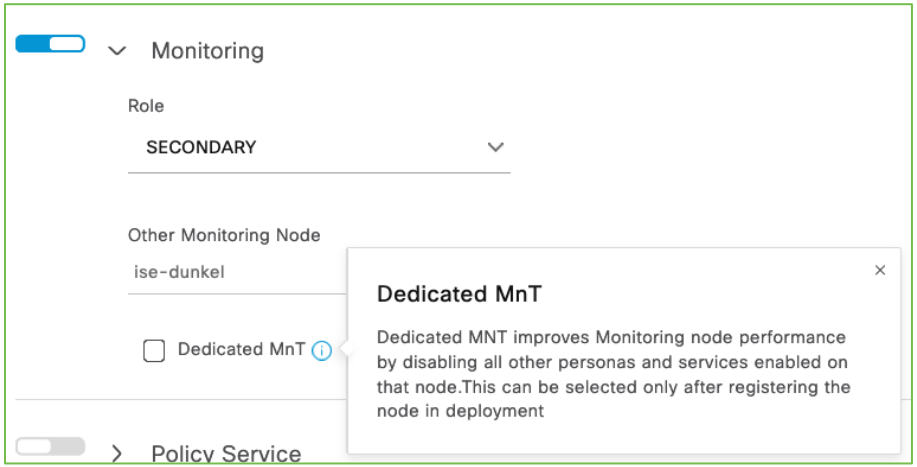
Passed Required

- If probe authentication must Pass
  - Use Local User
  - Prevents External Database slowness from impacting performance
- Filter Passed and Failed by Username

Status	Attribute	Value	Filter Type	Time left (in minutes)
Enabled	User Name	loadbalance-probe	Filter All	Unlimited

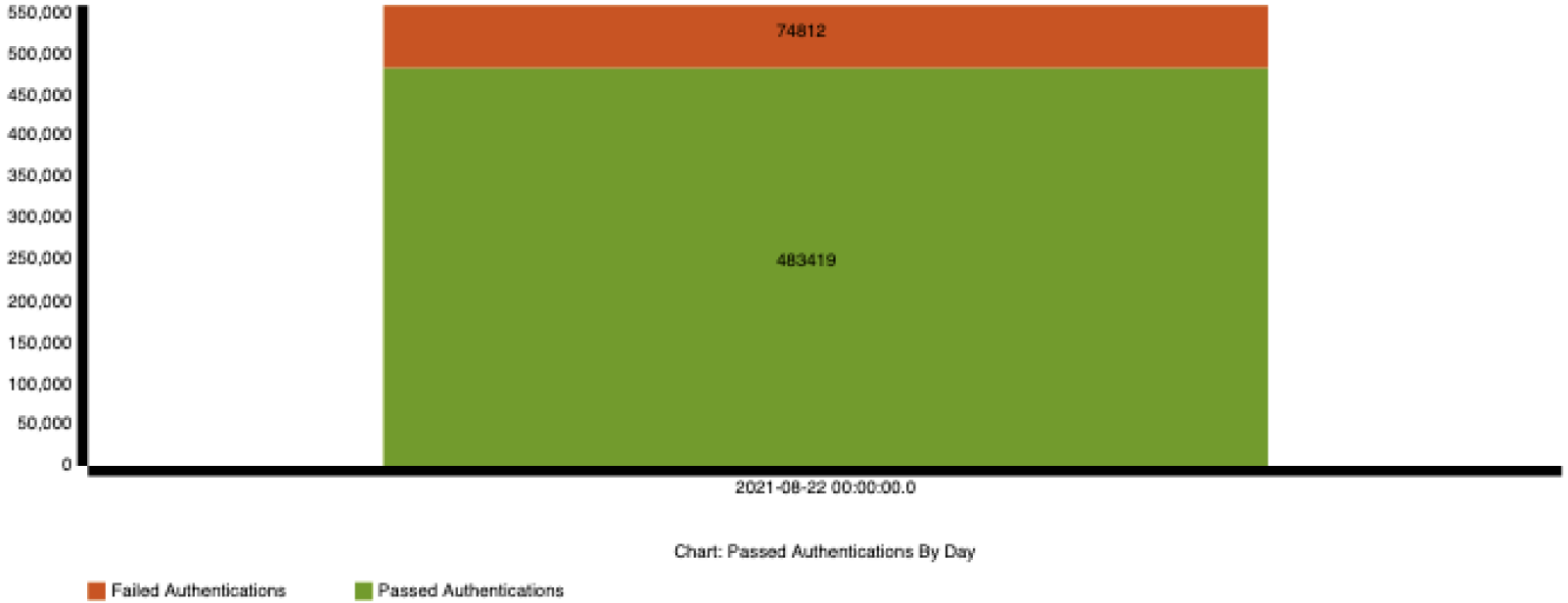
Dedicated MnT

- Only supported in Large Deployment
- Disables all roles besides MnT
- Disables replication to node freeing up:
  - Disk I/O
  - CPU
  - Memory



Authentication Summary Report

Passed/Failed Ratio



Authentication Summary Report

Authentications By Identity Store

Identity Store	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak response Time (ms)
Internal Endpoints	261263	0	261263	0	15.06	27355
zer0k.org	193777	794	194571	0.41	54	17916
Internal Users	25136	1	25137	0	27.5	2778
Guest Users	77	6	83	7.23	14.87	60

Authentication Summary Report

Authentications By ISE Server

Server	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak response Time (ms)
zer0k-ise1	114142	143	114285	0.13	17.03	50044
zer0k-ise2	69354	12697	82051	15.47	20.51	10009
zer0k-ise3	6531	51	6582	0.77	20.01	1551
zer0k-ise4	4331	0	4331	0	75.33	1128

Millisecond Timestamps in Live Logs

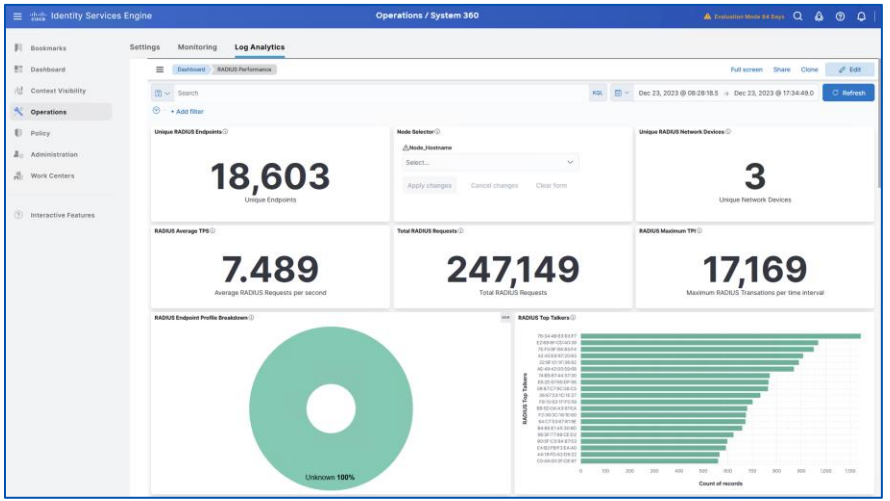
- Internal vs. External Latency
- Just because it isn't red doesn't mean it isn't impactful

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11117	Generated a new session ID	1
15049	Evaluating Policy Group	84
15008	Evaluating Service Selection Policy	0
15041	Evaluating Identity Policy	181
15048	Queried PIP - Network Access.AuthenticationMethod	14
15013	Selected Identity Source - Internal Users	60
24210	Looking up User in Internal Users IDStore - test1	509
24212	Found User in Internal Users IDStore	3
22037	Authentication Passed	0
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	0
15036	Evaluating Authorization Policy	1
24209	Looking up Endpoint in Internal Endpoints IDStore - test1	0
24217	The host is not found in the internal endpoints identity store	4
15048	Queried PIP - Radius.NAS-Port-Type	680
15048	Queried PIP - Network Access.UserName	10
15048	Queried PIP - IdentityGroup.Name	2
15048	Queried PIP - EndPoints.LogicalProfile	5
15048	Queried PIP - Network Access.AuthenticationStatus	0
15016	Selected Authorization Profile - PermitAccess	2
22081	Max sessions policy passed	0
22080	New accounting session created in Session cache	0
11002	Returned RADIUS Access-Accept	1

Log Analytics

- Operations -> System 360 -> Log Analytics
- Available from ISE 3.1
- Enabled by default in ISE 3.3

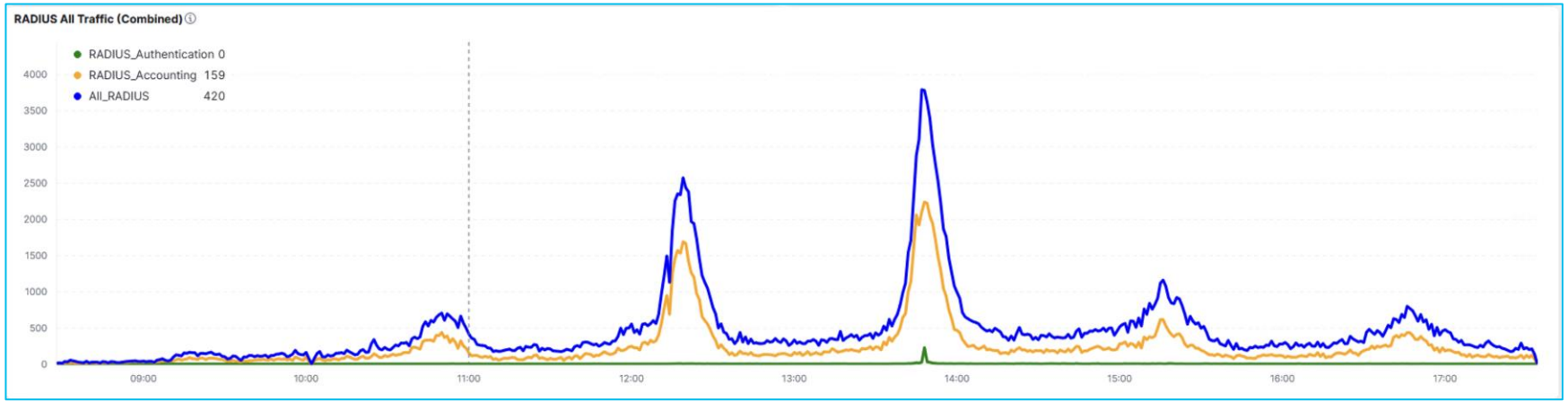


Understanding your ISE deployment with C.L.A.R.K. (Cisco Log Analysis & Remediation Kiosk)
BRKSEC-2897
CLUS 2023

https://www.ciscolive.com/on-demand/on-demand-library.html#/session/1686177803851001VeK2

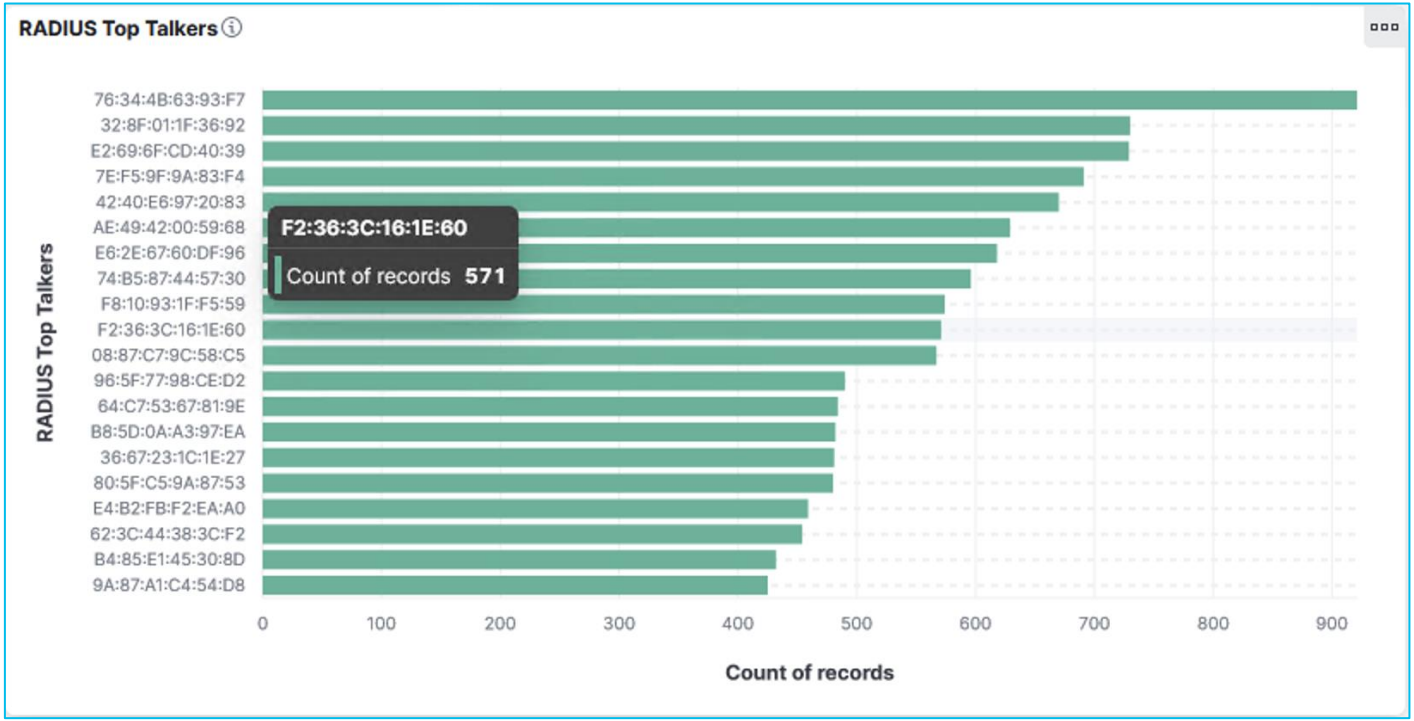
Log Analytics

TPS / Auth to Accounting Ratio



Log Analytics

Top Talkers

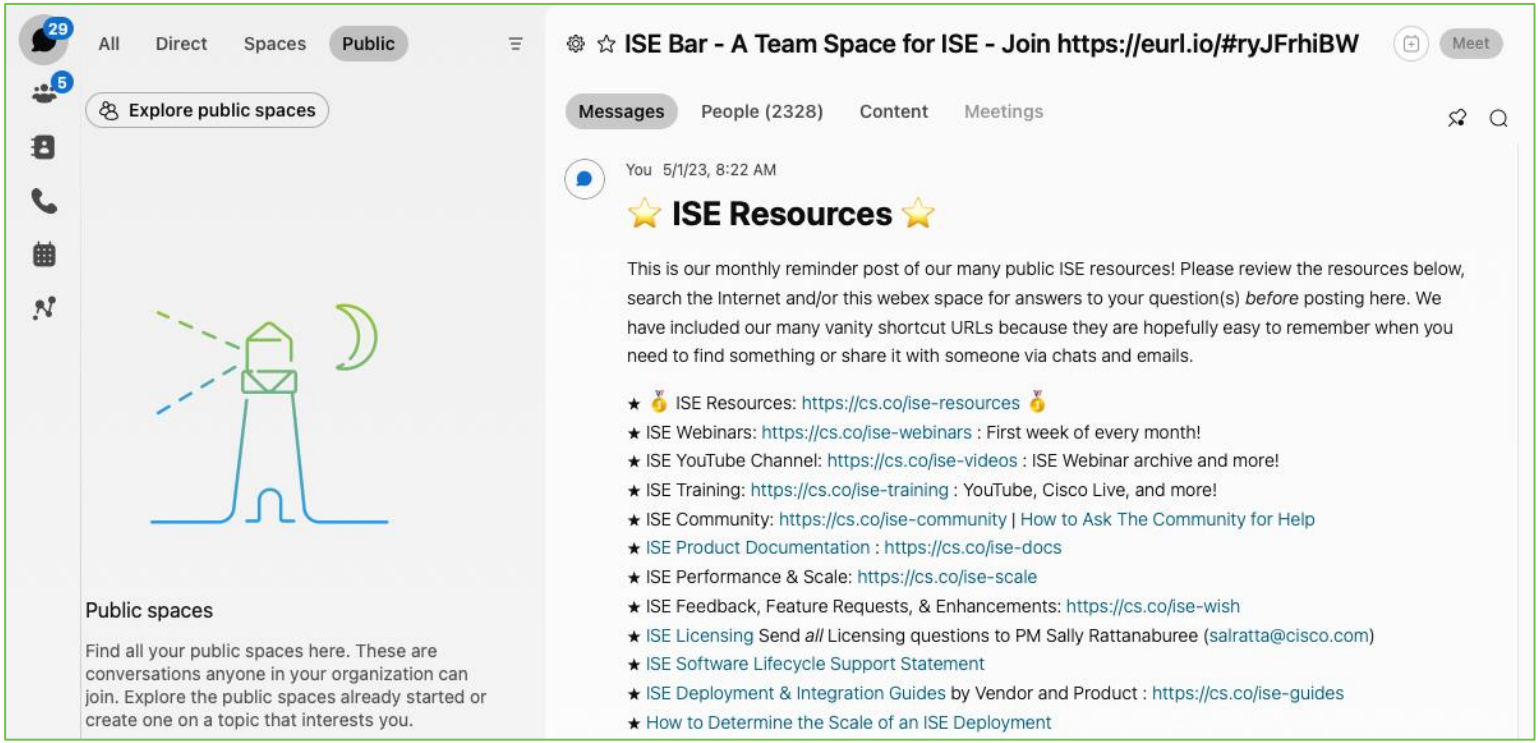


Key Takeaways

- Adhere to Deployment and Node sizing guidelines to ensure proper resources are allocated.
- Leverage load balancers for scale, high availability, and simplifying network config changes.
- Use best practice network device configurations.
- Ensure external databases are responding efficiently.
- Don’t overwhelm ISE with unnecessary information.
- Monitor for changes that increase requests to ISE.

ISE Bar: A Webex Team Space for ISE

eurl.io/#ryJFrhiBW



Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

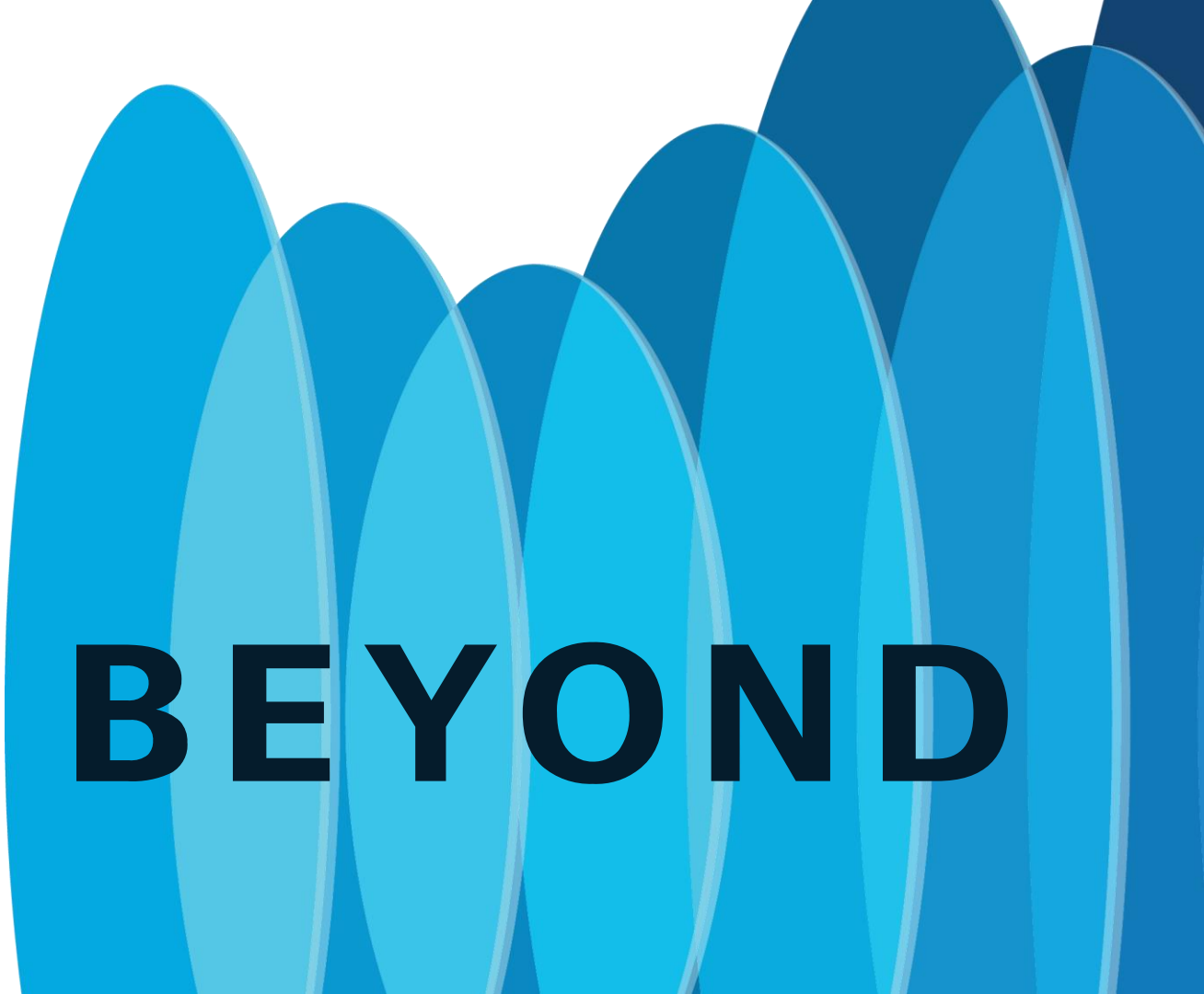
Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: jedubois@cisco.com


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND