cisco Live!

# Let’s go

The bridge to possible

# Cisco ISE Performance, Scalability and Best Practices

BRKSEC-2234

Jesse Dubois, TAC Security Technical Leader

# Introduction

# About Jesse Dubois

- name: Jesse Dubois
- job.jessedubois: 18 years in TAC

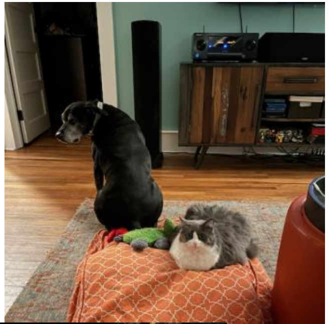
details.jessedubois:

Location: Durham, North Carolina

Interests: Brewing, Golf, Cooking

Pets: Dunkel, Apollo, Comet, Calypso

Latest Travel: Brussels, Belgium



# 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.

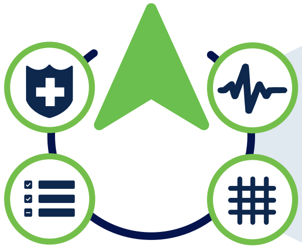
# Agenda

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

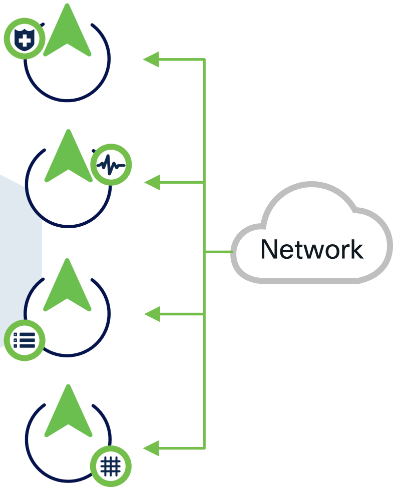
# Deployment / Sizing

# ISE Architecture

Standalone ISE



Distributed 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

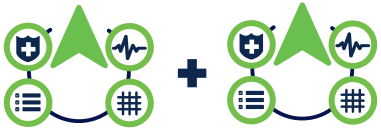
**pxGrid Controller**
- Facilitates sharing of context

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

# Deployment Options

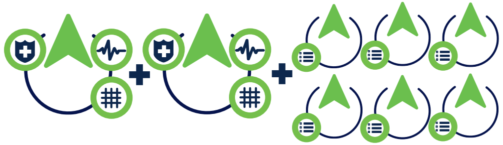
## Small

- 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!



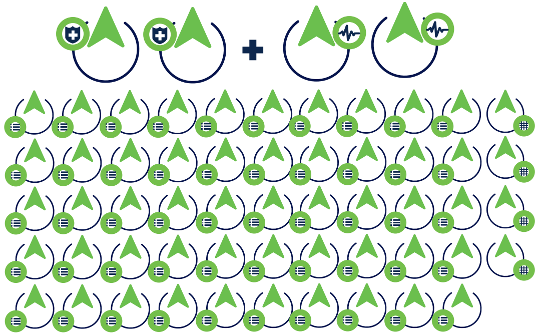
## Medium

- 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

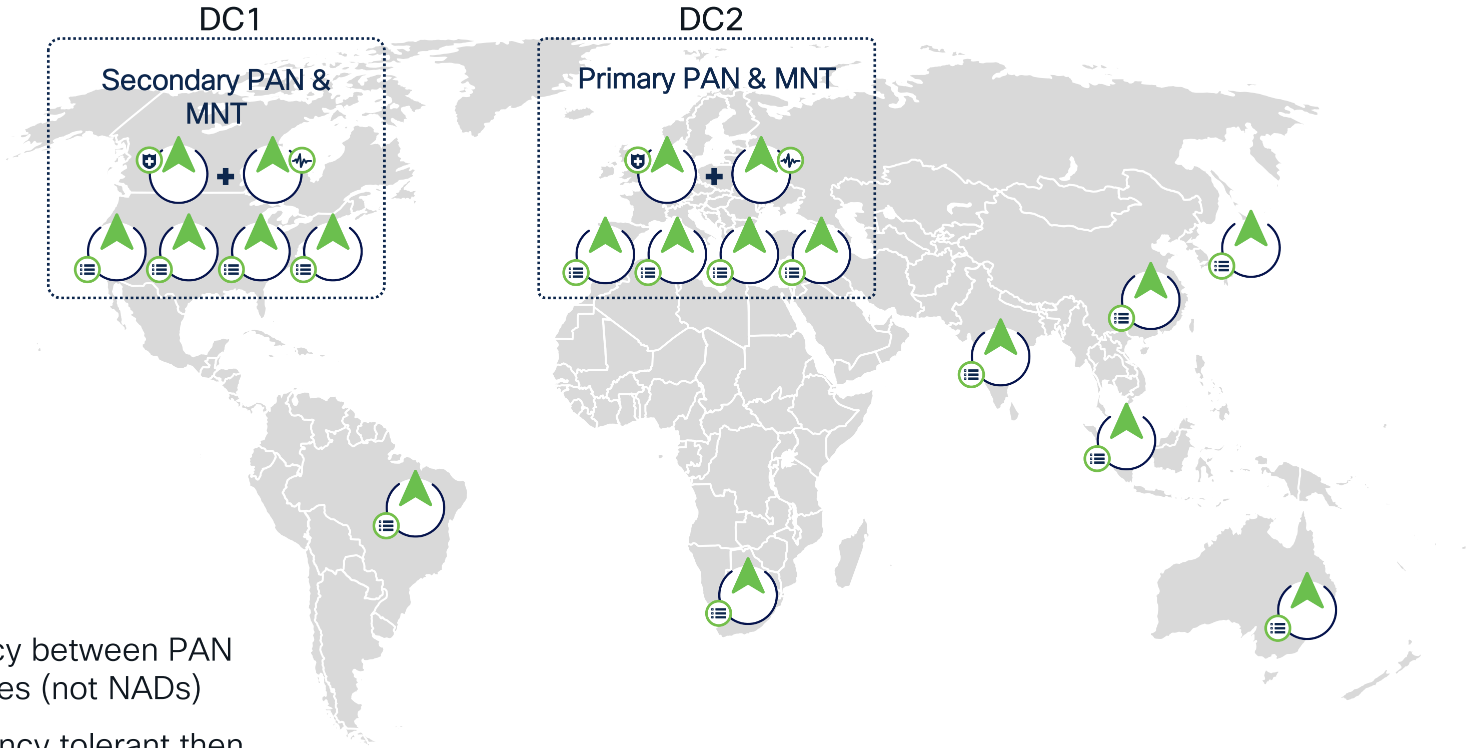


## Large

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

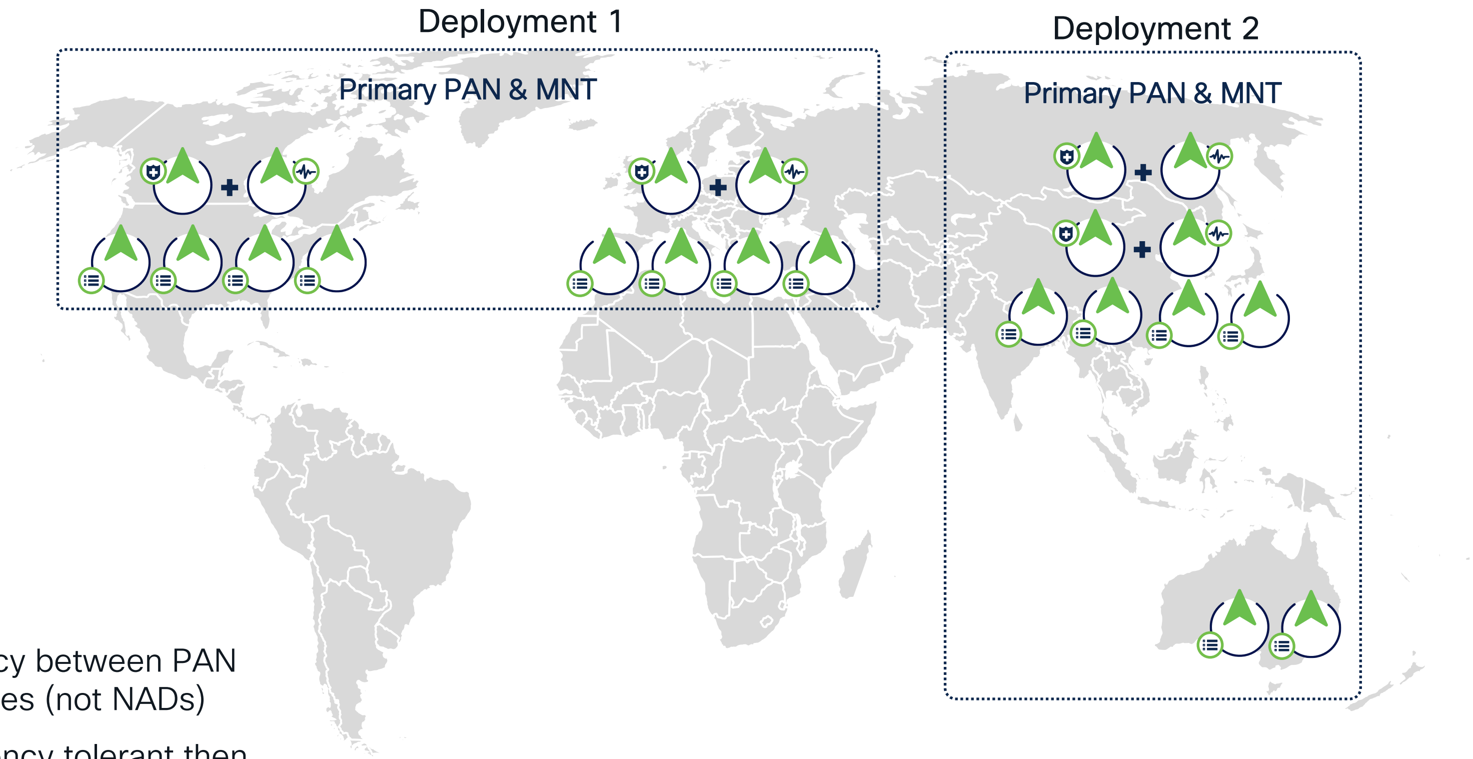


# Large Deployment: Centralized or Distributed



- 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.

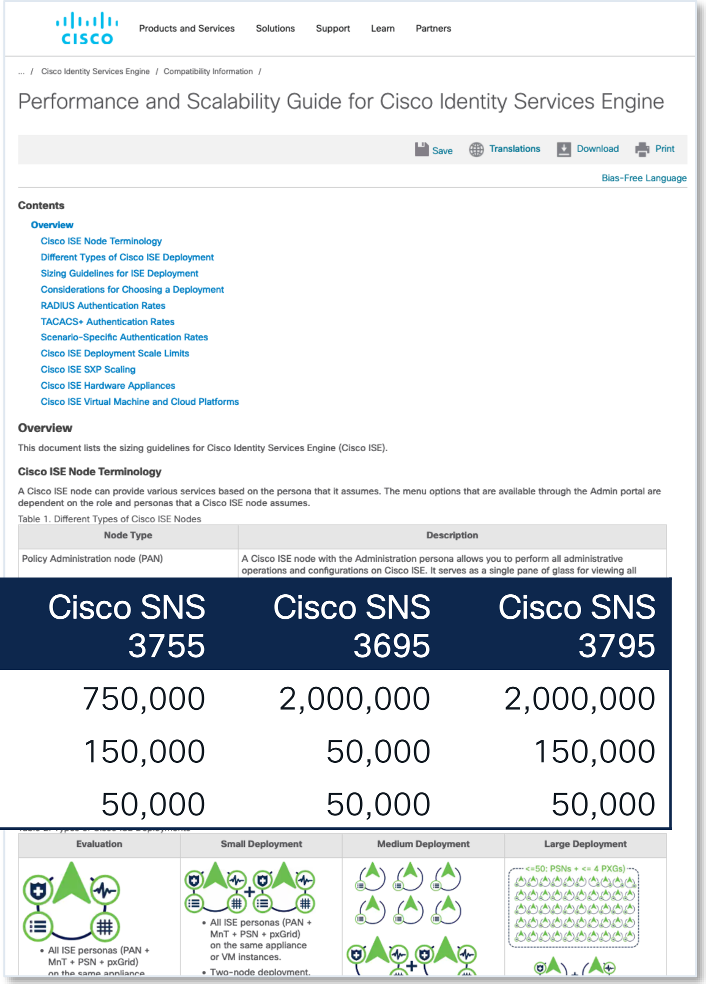
# ISE Max Sessions

## 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 |



... / Cisco Identity Services Engine / Compatibility Information /

Performance and Scalability Guide for Cisco Identity Services Engine

Contents

Overview

This document lists the sizing guidelines 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 |

| Evaluation | Small Deployment | Medium Deployment | Large Deployment |
|---|---|---|---|
| • All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance | • All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM instances.<br>• Two-node deployment. | | <=50: PSNs + <= 4 PXGs) |

# 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

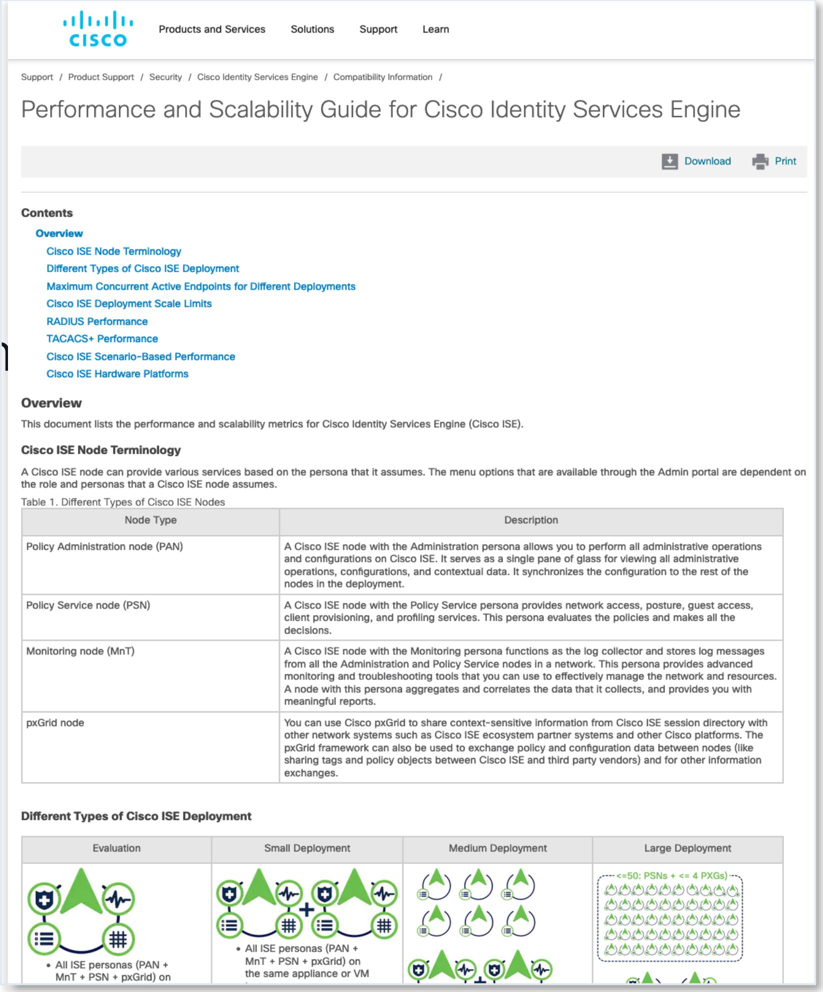
Table 4. Maximum Concurrent Active Sessions for Different ISE Appliances Acting as PSNs

| 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 Sessions
- Deployment Scale Limits
- Protocol Performance
- Scenario Performance
- Configuration Objects

cs.co/ise-scale



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

## Performance and Scalability Guide for Cisco Identity Services Engine

**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) |

# 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<br>32GB RAM<br>300GB Disk | 24 CPUs<br>32GB RAM<br>300GB – 1.2TB Disk | 40 CPUs<br>96GB RAM<br>300 GB – 1.2TB Disk | 40 CPUs<br>256GB RAM<br>1.2TB – 2.4TB Disk |
| AWS | m5.2xlarge | c5.9xlarge*<br>m5.8xlarge | m5.16xlarge | m5.16xlarge |
| Azure | Standard_D8s_v4 | Standard_F32s_v2*<br>Standard_D32s_v4 | Standard_D64s_v4 | Standard_D64s_v4 |
| OCI | Optimized3.Flex (8 OCPU and 32 GB) | Optimized3.Flex (16 OCPU and 64 GB)*<br>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*

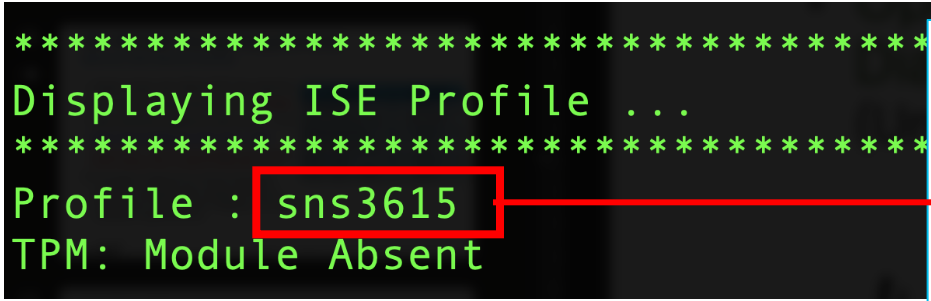
Persona differences:

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

# ISE Platform Properties

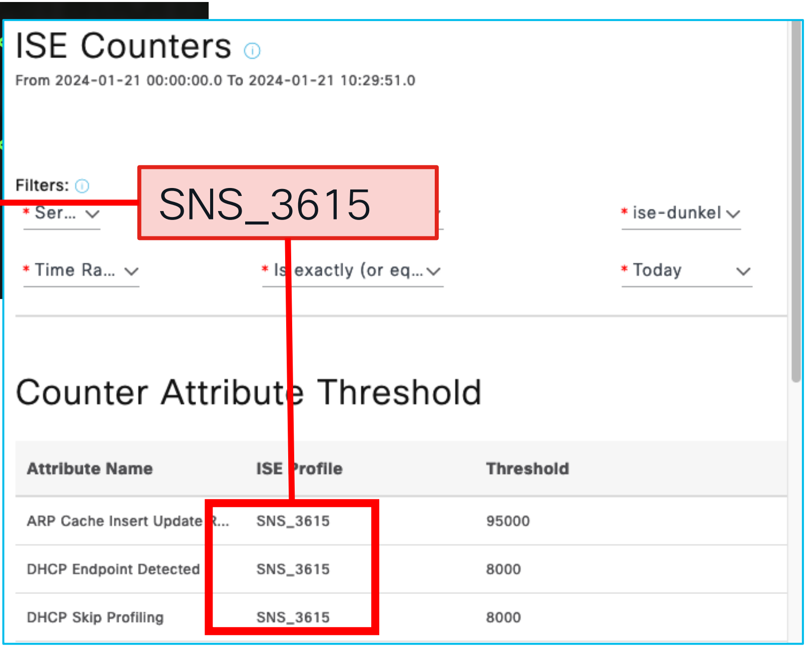
## Verify ISE Detects Proper VM Resource Allocation

- 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)



ISE Counters

From 2024-01-21 00:00:00.0 To 2024-01-21 10:29:51.0

Filters:

SNS_3615

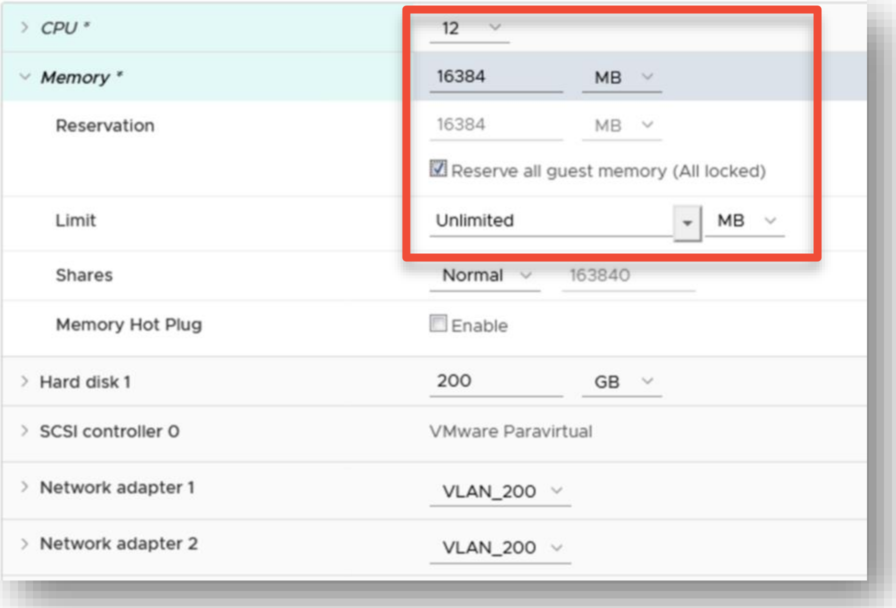
Counter Attribute Threshold

| Attribute Name | ISE Profile | Threshold |
|---|---|---|
| ARP Cache Insert Update R... | SNS_3615 | 95000 |
| DHCP Endpoint Detected | SNS_3615 | 8000 |
| DHCP Skip Profiling | SNS_3615 | 8000 |

# Virtual Machine Resources

## Reservations/Features

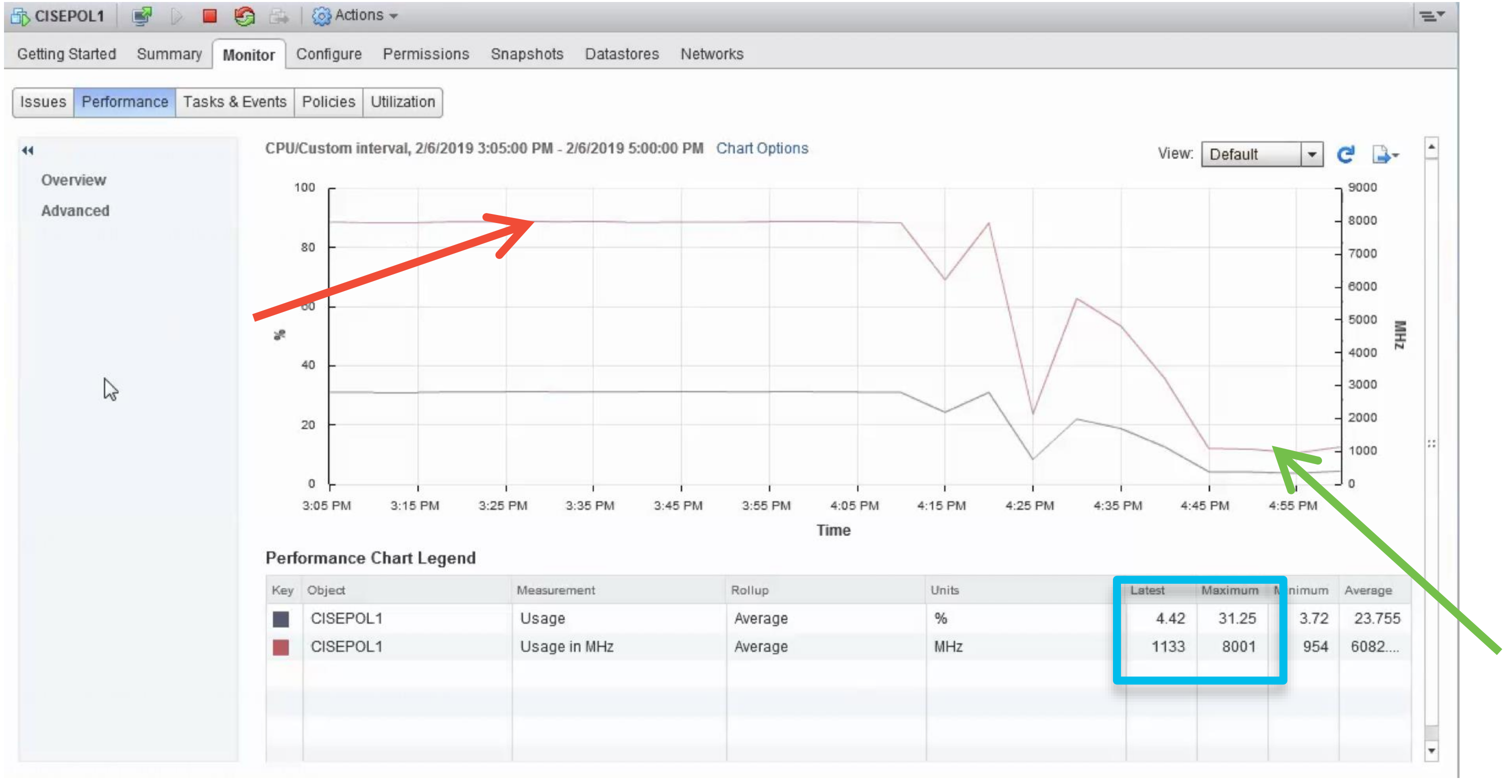
- Applies to all virtual platforms – VMWare, KVM, Hyper-V, AHV
- Reserve 100% of CPU and Memory
- Use thick provisioning of disk.
- Do no set resource limits.



| | |
|---|---|
| CPU * | 12 |
| Memory * | 16384 MB |
| Reservation | 16384 MB<br>☑ Reserve all guest memory (All locked) |
| Limit | Unlimited MB |
| Shares | Normal 163840 |
| Memory Hot Plug | □ Enable |
| Hard disk 1 | 200 GB |
| SCSI controller 0 | VMware Paravirtual |
| Network adapter 1 | VLAN_200 |
| Network adapter 2 | VLAN_200 |

# Virtual Machine Resources

## Reservations – Before and After

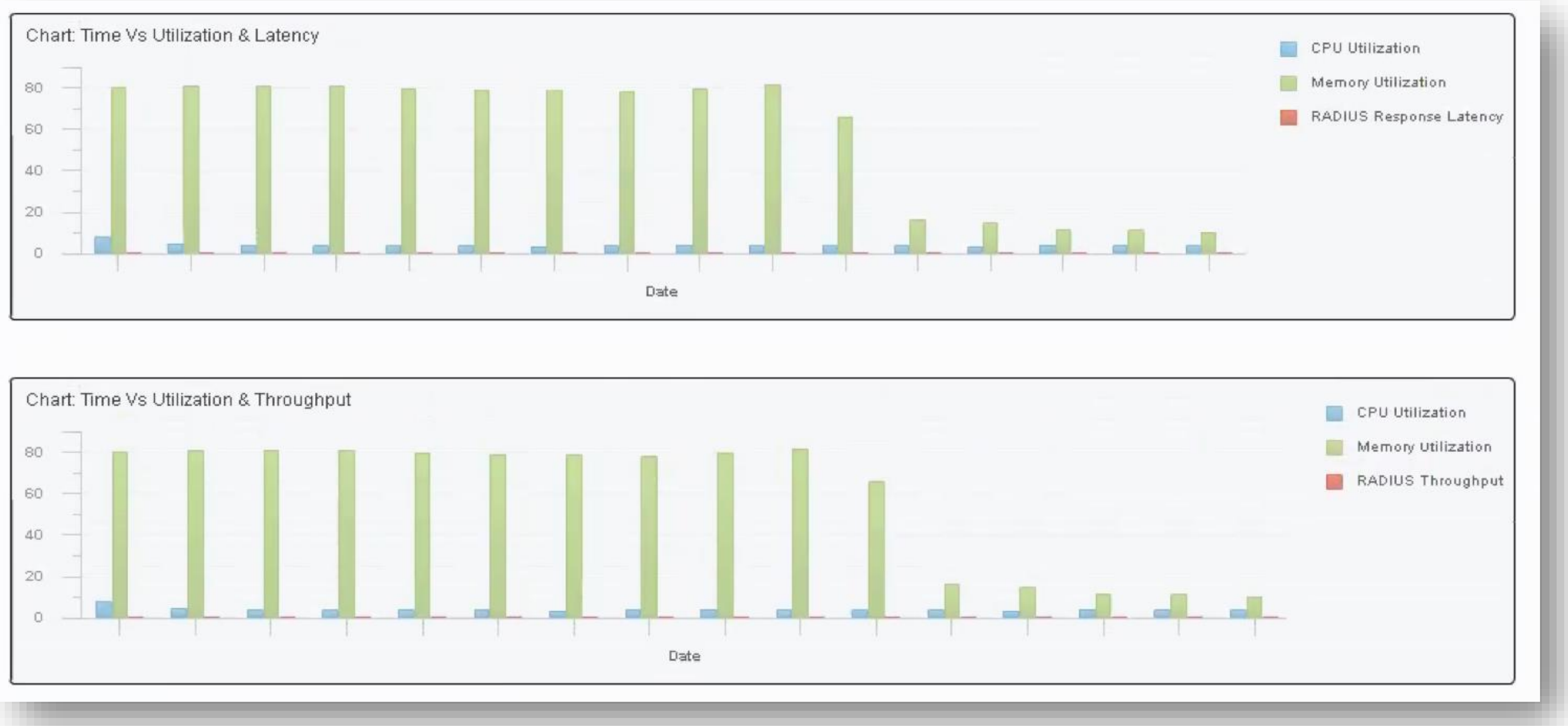


Performance Chart Legend

| Key | Object | Measurement | Rollup | Units | Latest | Maximum | Minimum | Average |
|---|---|---|---|---|---|---|---|---|
| ■ | CISEPOL1 | Usage | Average | % | 4.42 | 31.25 | 3.72 | 23.755 |
| 🟥 | CISEPOL1 | Usage in MHz | Average | MHz | 1133 | 8001 | 954 | 6082.... |

# Advice: VM Resources

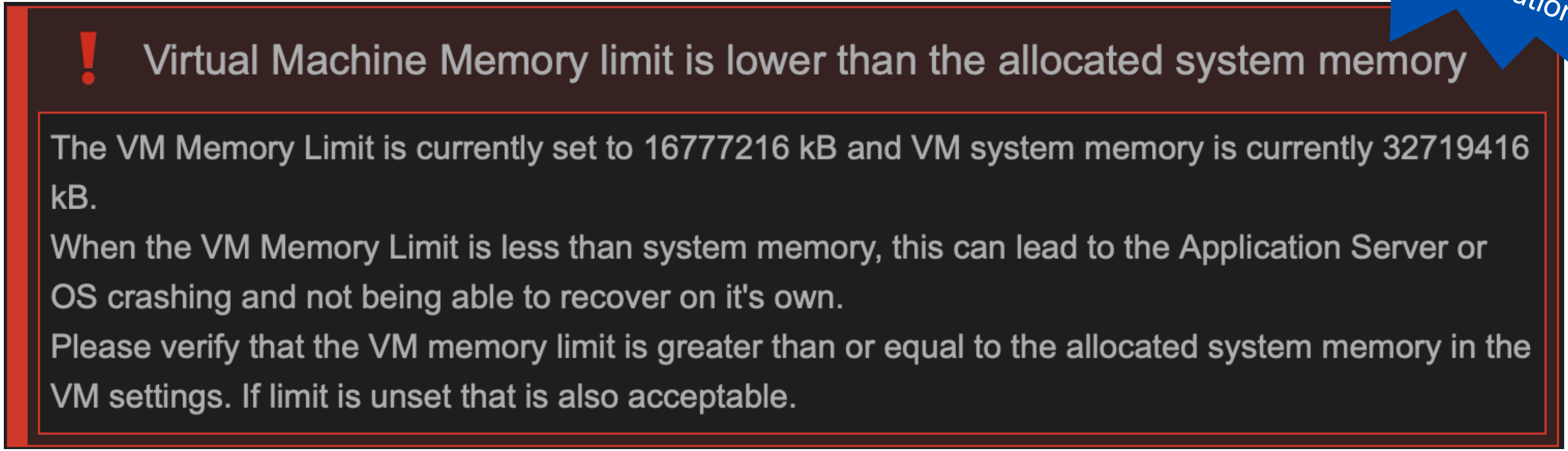
## Reservations – Latency Before & After



# Virtual Machine Resources

## Limits

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



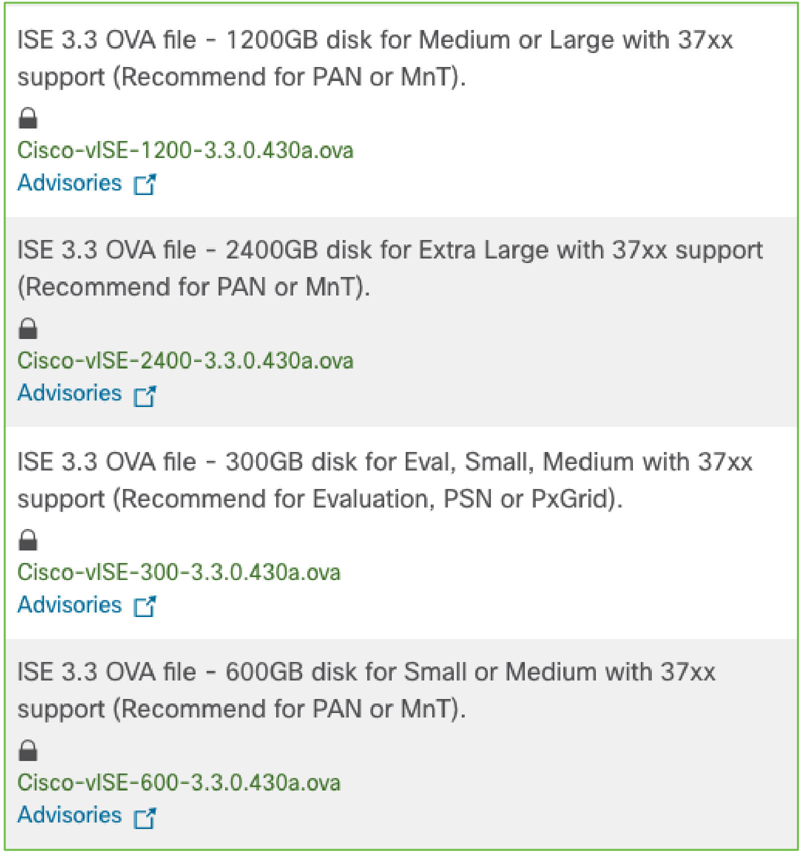
! Virtual Machine Memory limit is lower than the allocated system memory

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.

TAC Automation!

# 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.



ISE 3.3 OVA file - 1200GB disk for Medium or Large with 37xx support (Recommend for PAN or MnT).

Cisco-vISE-1200-3.3.0.430a.ova

Advisories

ISE 3.3 OVA file - 2400GB disk for Extra Large with 37xx support (Recommend for PAN or MnT).

Cisco-vISE-2400-3.3.0.430a.ova

Advisories

ISE 3.3 OVA file - 300GB disk for Eval, Small, Medium with 37xx support (Recommend for Evaluation, PSN or PxGrid).

Cisco-vISE-300-3.3.0.430a.ova

Advisories

ISE 3.3 OVA file - 600GB disk for Small or Medium with 37xx support (Recommend for PAN or MnT).

Cisco-vISE-600-3.3.0.430a.ova

Advisories

# 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

# The Fall Out From the Mobile Explosion and IoT

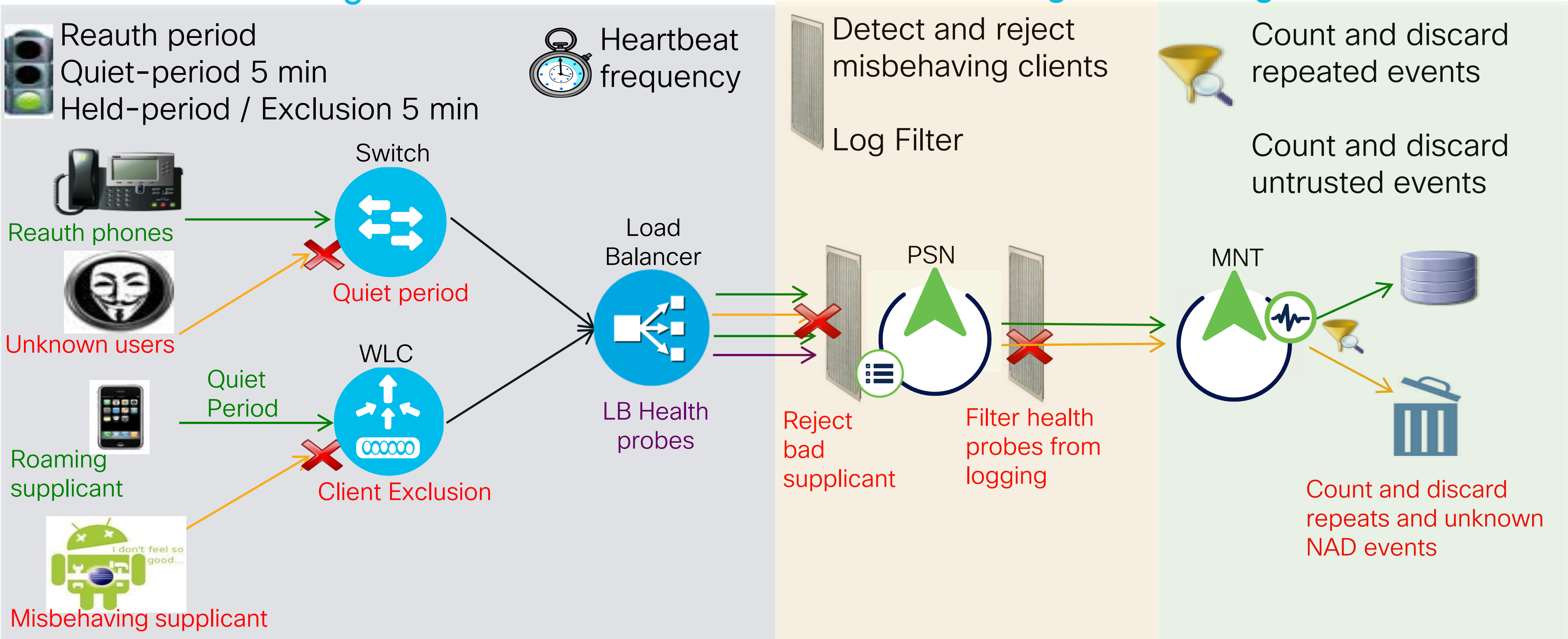
- Explosion in number and type of endpoints on the network.
- High auth rates from mobile devices—many personal (unmanaged).
  - Short-lived connections: Continuous sleep/hibernation to conserve battery power, roaming, ...
- Misbehaving supplicants: Unmanaged endpoints from numerous mobile vendors may 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

### Filtering at Receiving Chain



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

Heartbeat frequency

Detect and reject misbehaving clients

Log Filter

Count and discard repeated events

Count and discard untrusted events

Switch

Reauth phones

Quiet period

Unknown users

WLC

Quiet Period

Roaming supplicant

Client Exclusion

Misbehaving supplicant

Load Balancer

LB Health probes

PSN

Reject bad supplicant

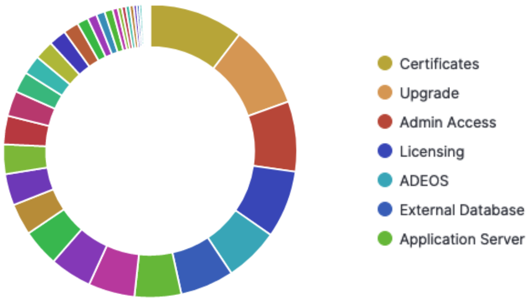
Filter health probes from logging

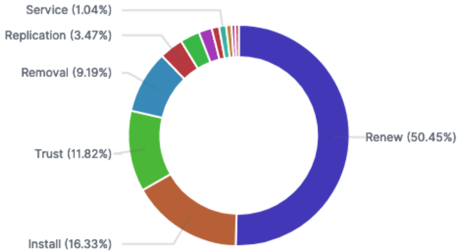
MNT

Count and discard repeats and unknown NAD events

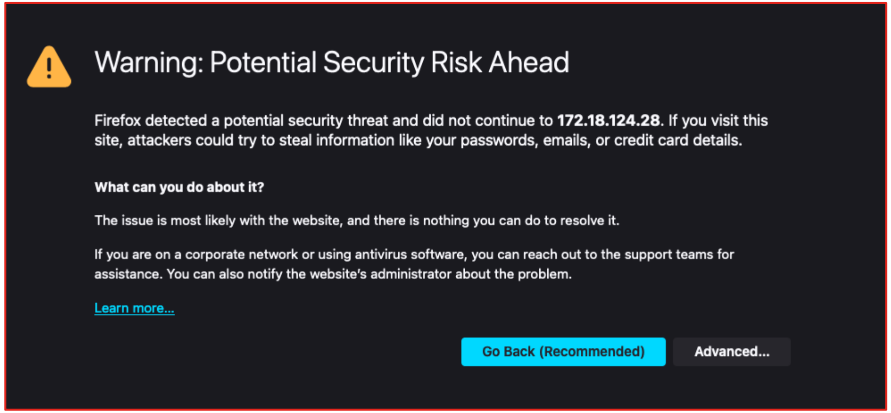
# Let’s Talk About Certificates

- Top TAC Case Generator!





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



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **172.18.124.28**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

**What can you do about it?**

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website’s administrator about the problem.

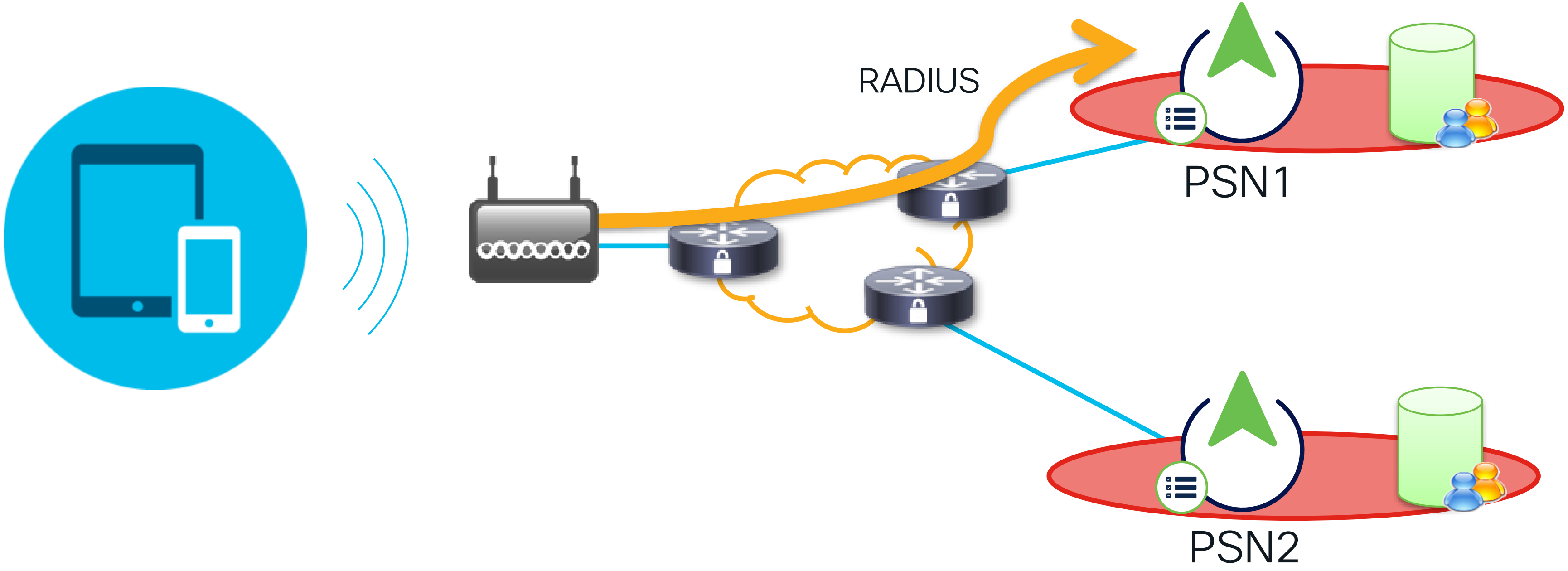
Hoverboarder

^

*The ~~Skateboarder~~*

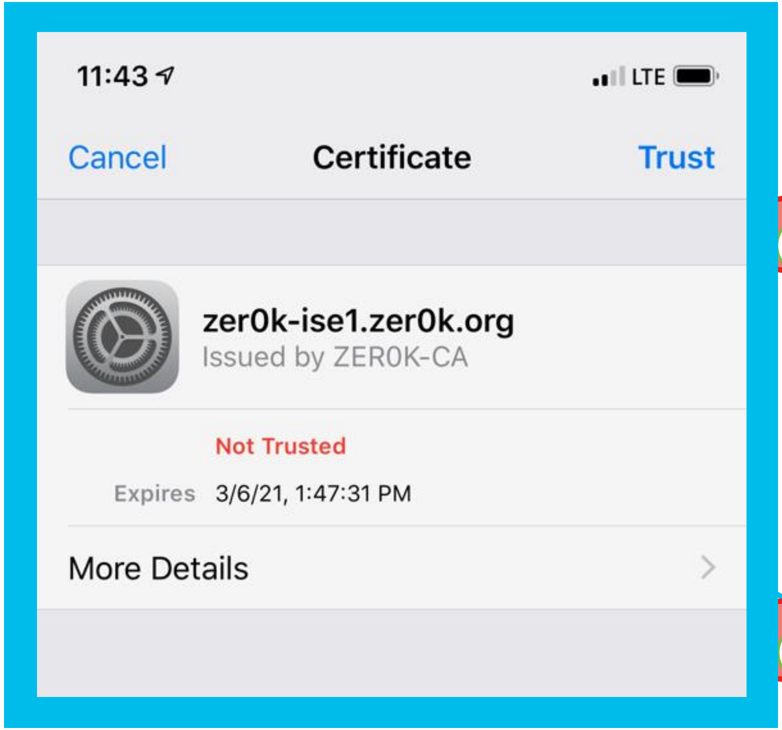
# iPhones and Certificates

## Problem



# iPhones and Certificates

## Problem

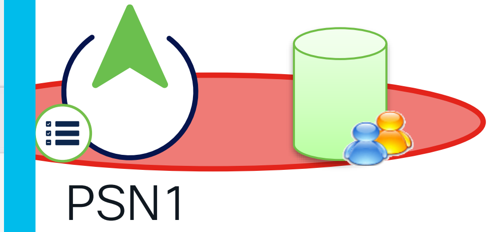


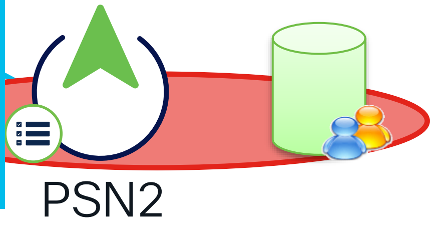
zer0k-ise1.zer0k.org
Issued by ZER0K-CA

Not Trusted

Expires 3/6/21, 1:47:31 PM

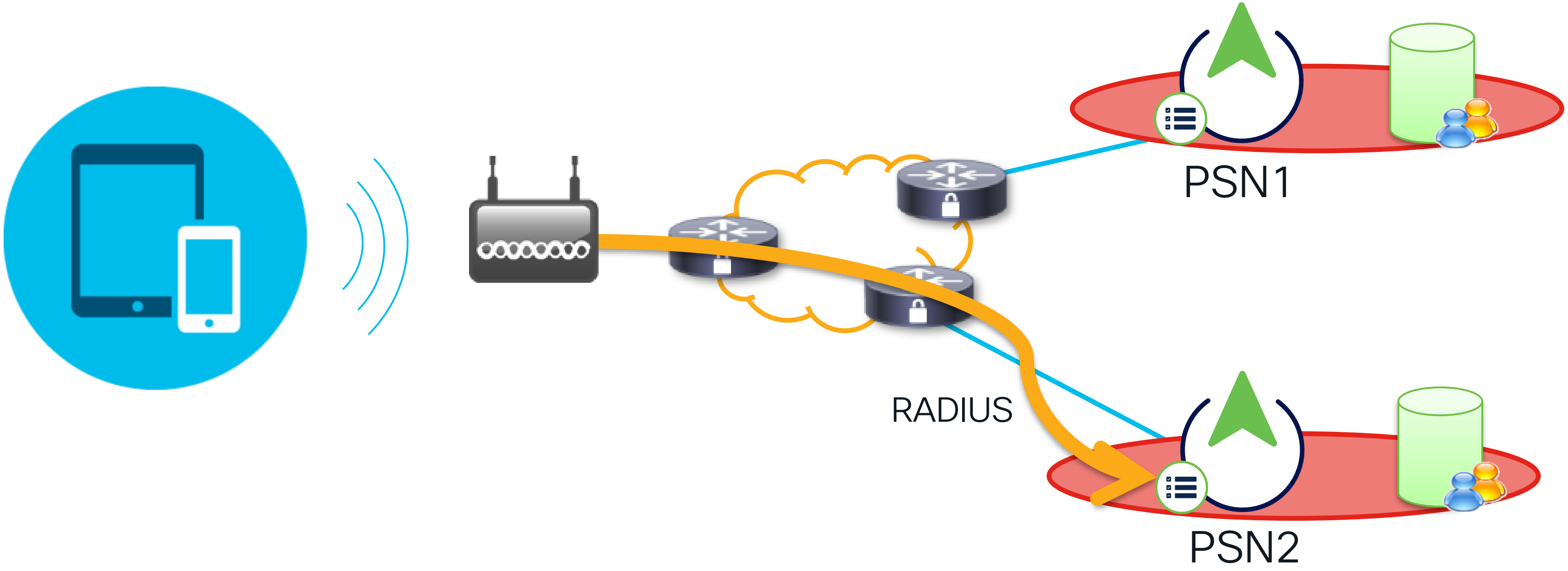
More Details





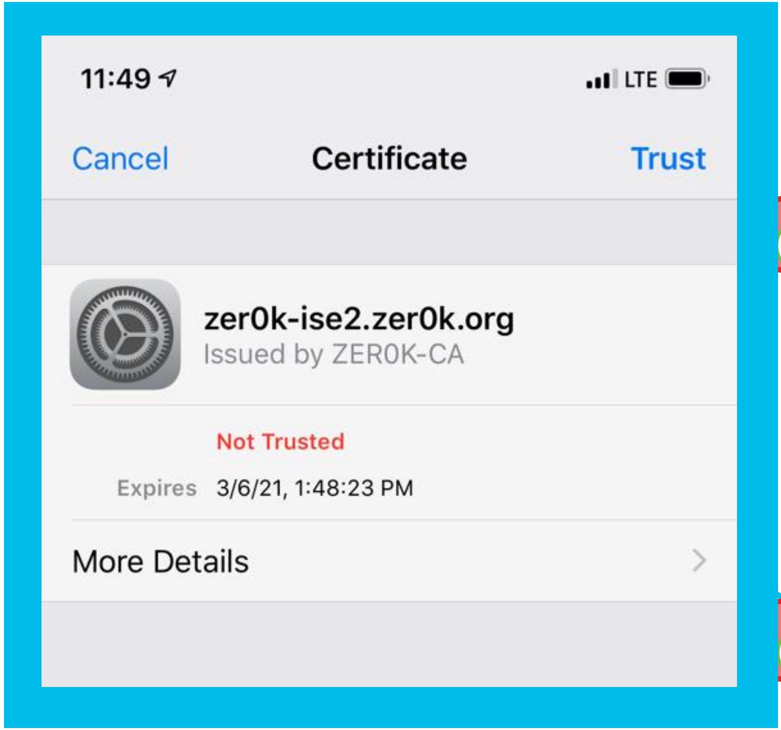
# iPhones and Certificates

## Problem



# iPhones and Certificates

## Problem



11:49 LTE

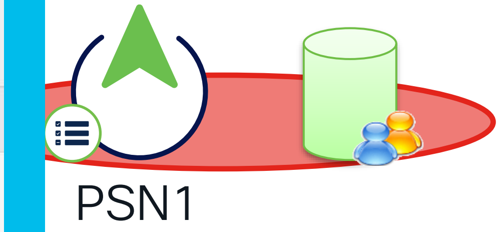
Cancel Certificate Trust

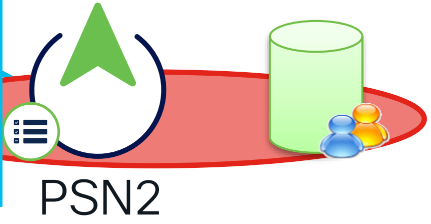
**zer0k-ise2.zer0k.org**
Issued by ZER0K-CA

Not Trusted

Expires 3/6/21, 1:48:23 PM

More Details

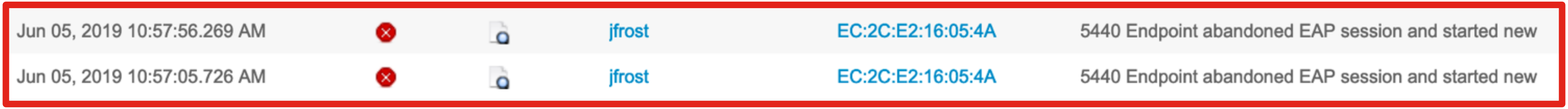




# iPhones and Certificates

## Problem

- If users aren’t looking at the phone:

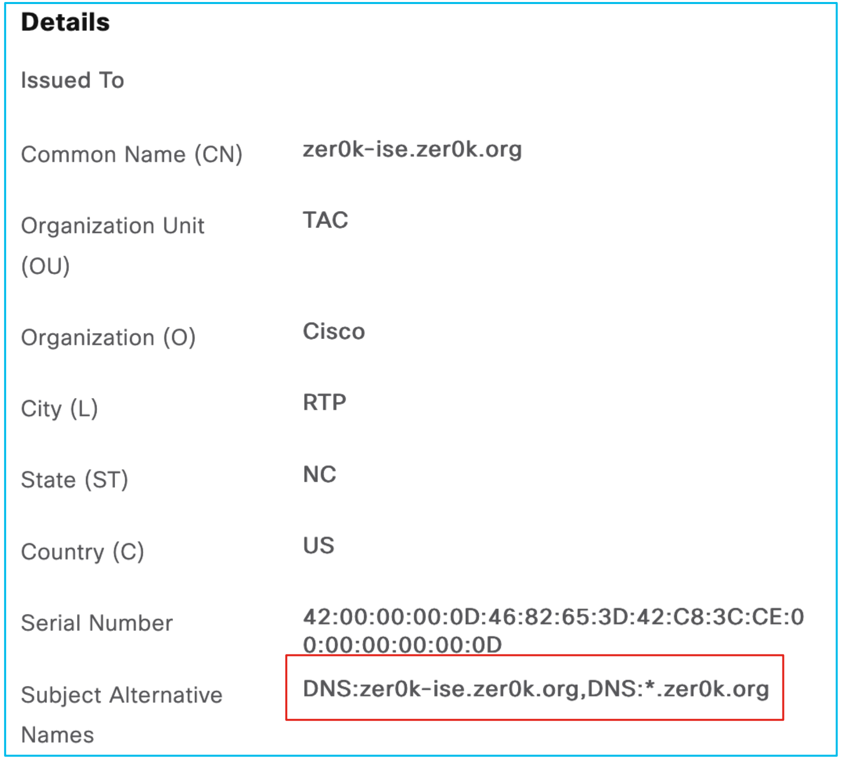


| | | | | | |
|---|---|---|---|---|---|
| Jun 05, 2019 10:57:56.269 AM | ✖ | 🔍 | jfrost | EC:2C:E2:16:05:4A | 5440 Endpoint abandoned EAP session and started new |
| Jun 05, 2019 10:57:05.726 AM | ✖ | 🔍 | jfrost | EC:2C:E2:16:05:4A | 5440 Endpoint abandoned EAP session and started new |

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

# Wildcard Certificates

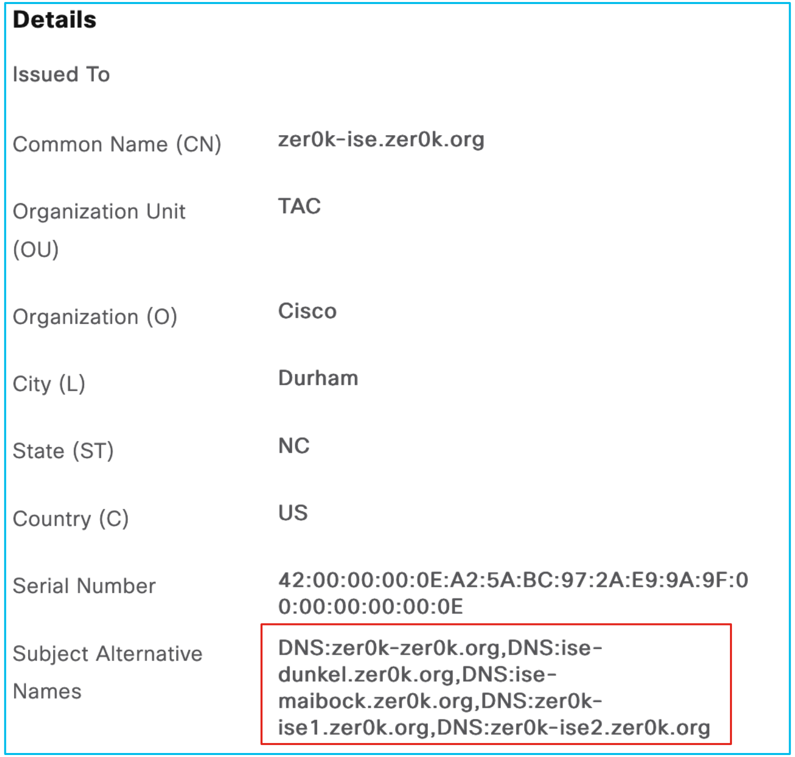
## WildSAN or MultiSAN



**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 |

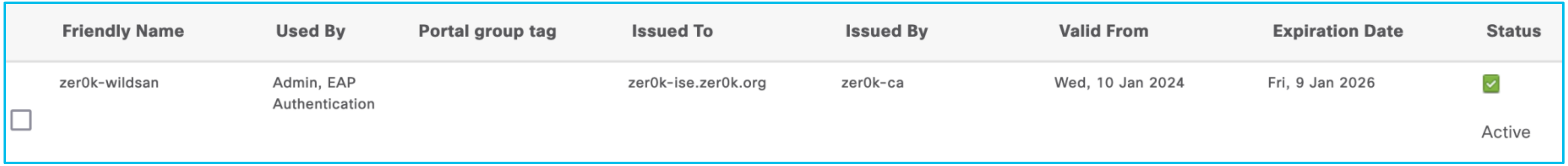
# WildSAN Security

- 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.

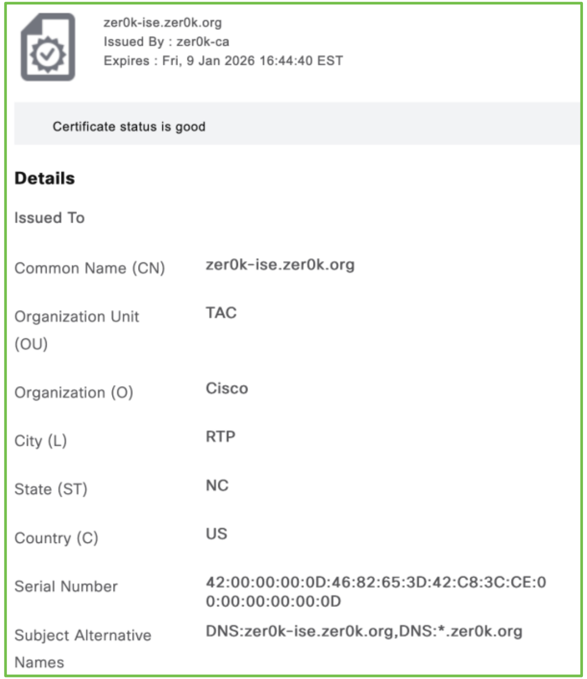
# Detour:
# Common Pitfall

# 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.



zer0k-ise.zer0k.org
Issued By : zer0k-ca
Expires : Fri, 9 Jan 2026 16:44:40 EST

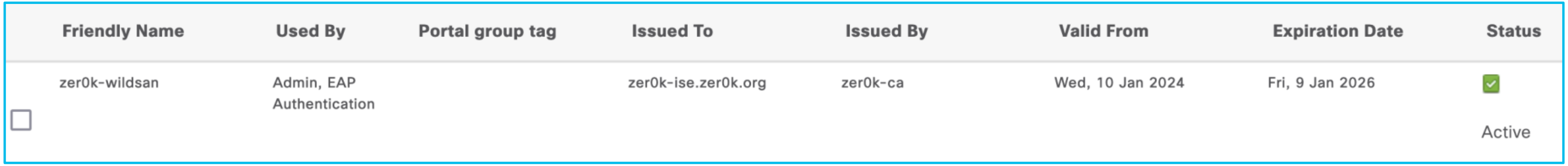
Certificate status is good

**Details**

Issued To

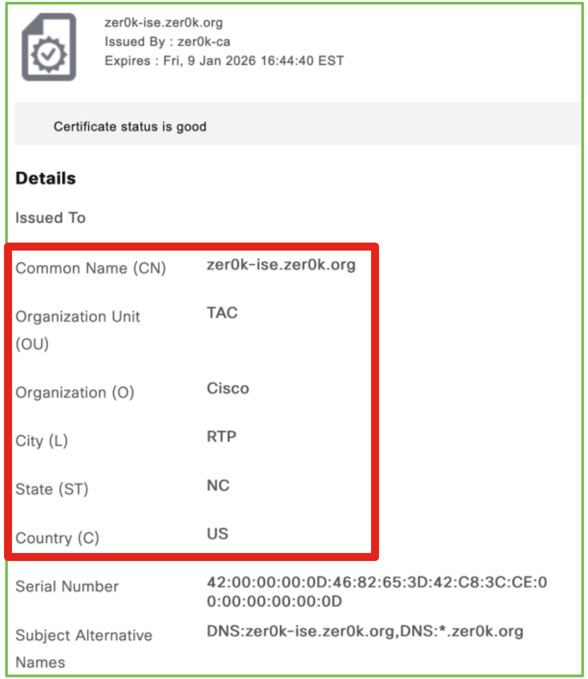
| | |
|---|---|
| Common Name (CN) | zer0k-ise.zer0k.org |
| Organization Unit (OU) | TAC |
| Organization (O) | Cisco |
| City (L) | RTP |
| State (ST) | NC |
| Country (C) | US |
| Serial Number | 42:00:00:00:0D:46:82:65:3D:42:C8:3C:CE:00:00:00:00:00:0D |
| Subject Alternative Names | DNS:zer0k-ise.zer0k.org,DNS:*.zer0k.org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

# 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.



zer0k-ise.zer0k.org
Issued By : zer0k-ca
Expires : Fri, 9 Jan 2026 16:44:40 EST

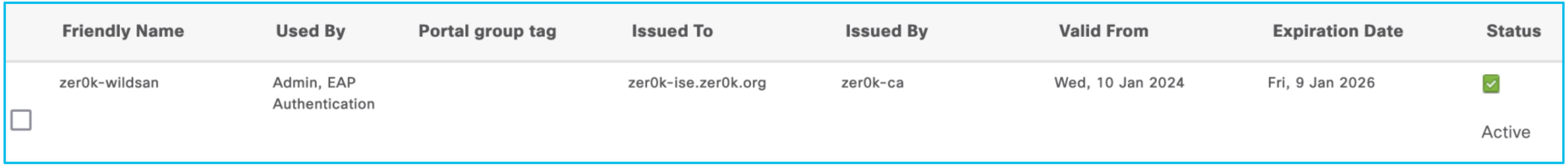
Certificate status is good

**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 |

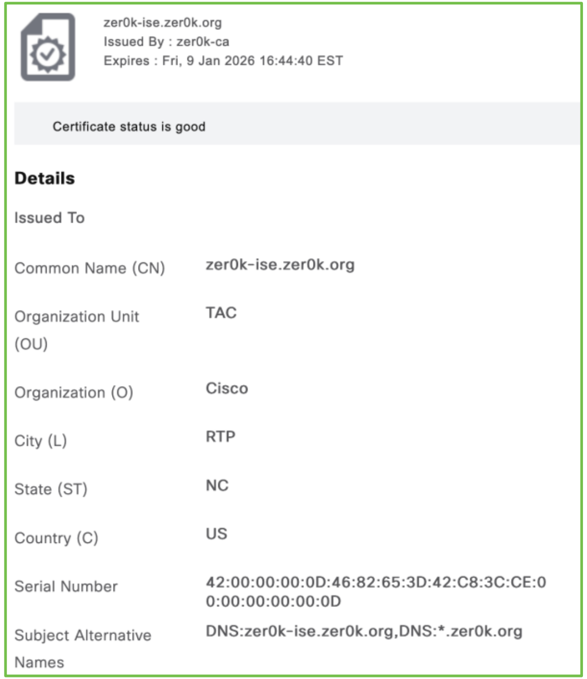
# Wildcard Certificate Renewal



| | 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)



zer0k-ise.zer0k.org
Issued By : zer0k-ca
Expires : Fri, 9 Jan 2026 16:44:40 EST

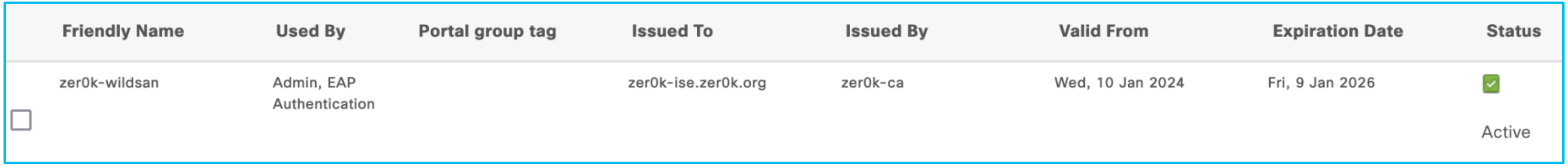
Certificate status is good

**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 |

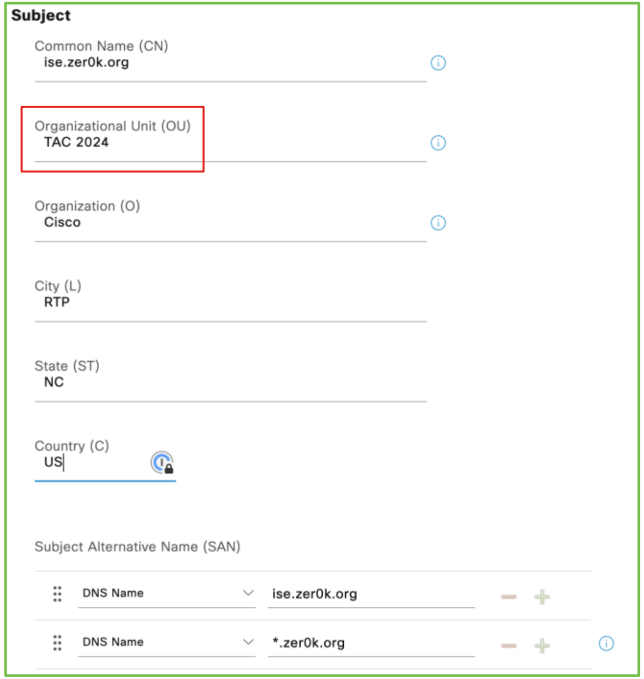
# Wildcard Certificate Renewal



| | 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.



**Subject**

Common Name (CN): ise.zer0k.org

Organizational Unit (OU): TAC 2024

Organization (O): Cisco

City (L): RTP

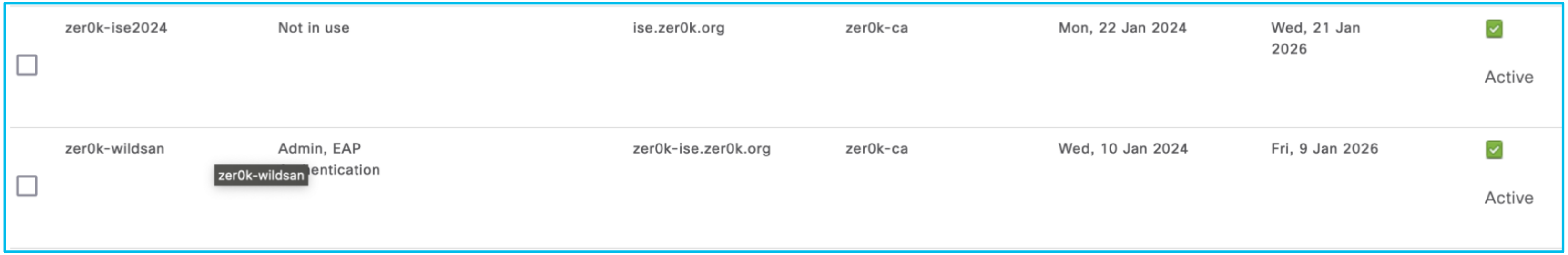
State (ST): NC

Country (C): US

Subject Alternative Name (SAN)

| | |
|---|---|
| DNS Name | ise.zer0k.org |
| DNS Name | *.zer0k.org |

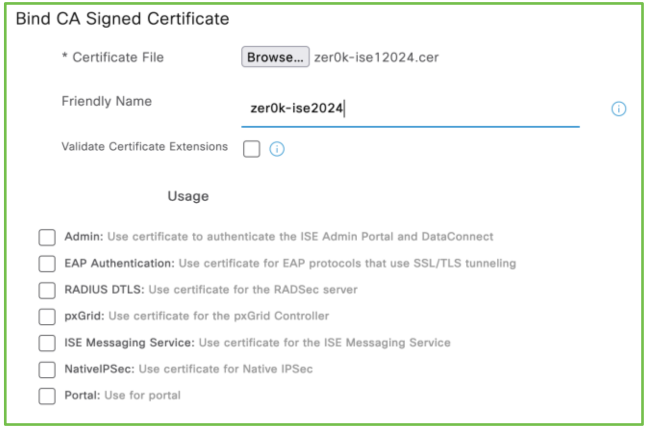
# Wildcard Certificate Renewal



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| □ | zer0k-ise2024 | Not in use | ise.zer0k.org | zer0k-ca | Mon, 22 Jan 2024 | Wed, 21 Jan 2026 | ✓ Active |
| □ | zer0k-wildsan | Admin, EAP<br>zer0k-wildsan entication | zer0k-ise.zer0k.org | zer0k-ca | Wed, 10 Jan 2024 | Fri, 9 Jan 2026 | ✓ Active |

## -= 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.



Bind CA Signed Certificate

* Certificate File Browse... zer0k-ise12024.cer

Friendly Name zer0k-ise2024

Validate Certificate Extensions □

Usage

□ **Admin:** Use certificate to authenticate the ISE Admin Portal and DataConnect

□ **EAP Authentication:** Use certificate for EAP protocols that use SSL/TLS tunneling

□ **RADIUS DTLS:** Use certificate for the RADSec server

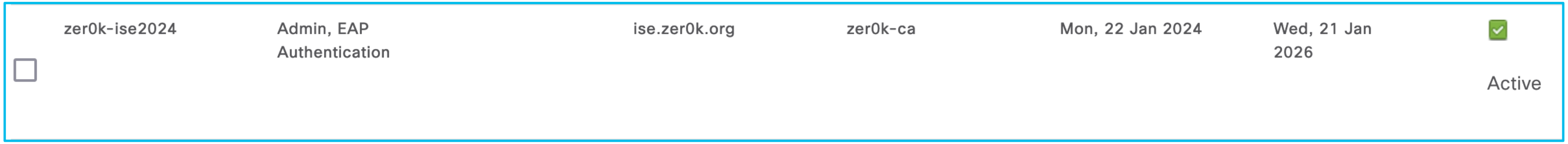
□ **pxGrid:** Use certificate for the pxGrid Controller

□ **ISE Messaging Service:** Use certificate for the ISE Messaging Service

□ **NativeIPSec:** Use certificate for Native IPSec

□ **Portal:** Use for portal

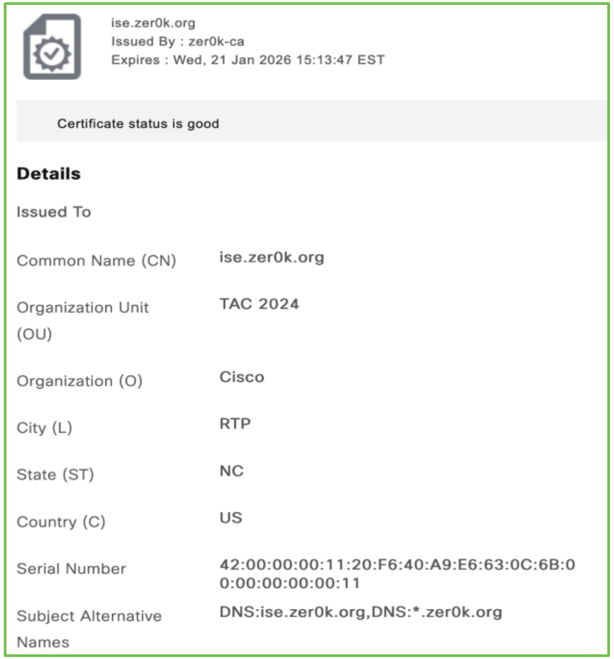
# Wildcard Certificate Renewal



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| □ | 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.



ise.zer0k.org
Issued By : zer0k-ca
Expires : Wed, 21 Jan 2026 15:13:47 EST

Certificate status is good

**Details**

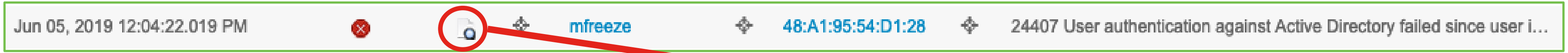
Issued To

| | |
|---|---|
| Common Name (CN) | ise.zer0k.org |
| Organization Unit (OU) | TAC 2024 |
| Organization (O) | Cisco |
| City (L) | RTP |
| State (ST) | NC |
| Country (C) | US |
| Serial Number | 42:00:00:00:11:20:F6:40:A9:E6:63:0C:6B:00:00:00:00:00:11 |
| Subject Alternative Names | DNS:ise.zer0k.org,DNS:*.zer0k.org |

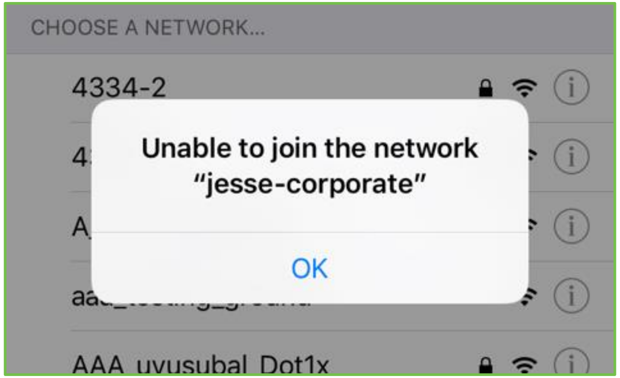
# PEAP Password Retries

## Problem

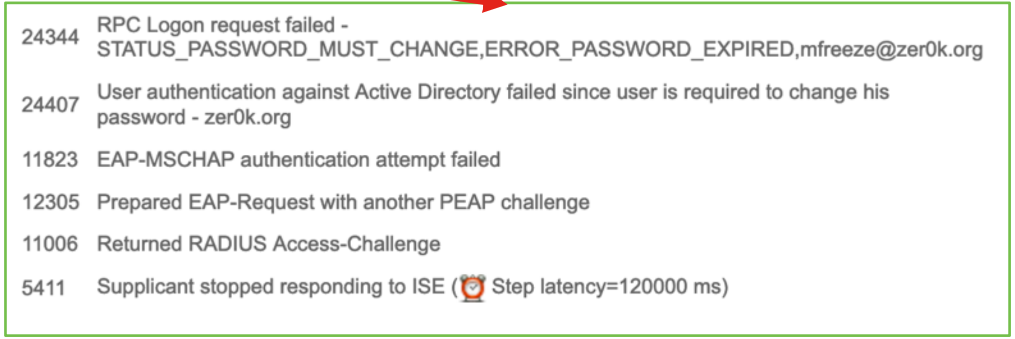
- Very few supplicants support PEAP Password Retries
- Supplicants will restart authentication when not supported.



```
Jun 05, 2019 12:04:22.019 PM    mfreeze    48:A1:95:54:D1:28    24407 User authentication against Active Directory failed since user i...
```



Unable to join the network “jesse-corporate”

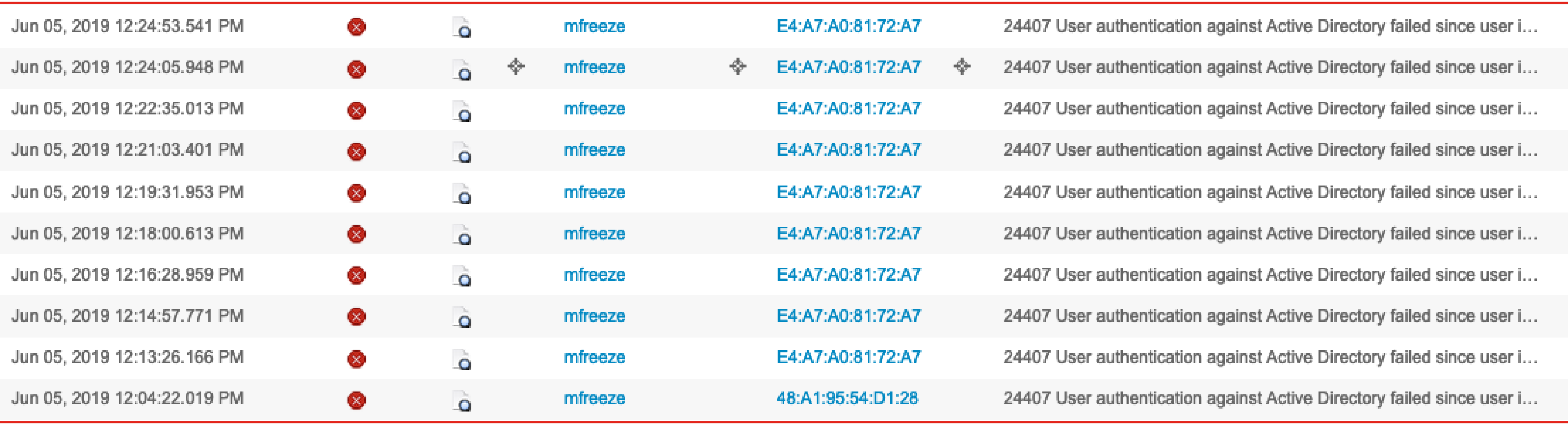


```
24344   RPC Logon request failed -
        STATUS_PASSWORD_MUST_CHANGE,ERROR_PASSWORD_EXPIRED,mfreeze@zer0k.org
24407   User authentication against Active Directory failed since user is required to change his
        password - zer0k.org
11823   EAP-MSCHAP authentication attempt failed
12305   Prepared EAP-Request with another PEAP challenge
11006   Returned RADIUS Access-Challenge
5411    Supplicant stopped responding to ISE (⏰ Step latency=120000 ms)
```

# PEAP Password Retries

## Problem

- Wireless Client Exclusions never kick in...

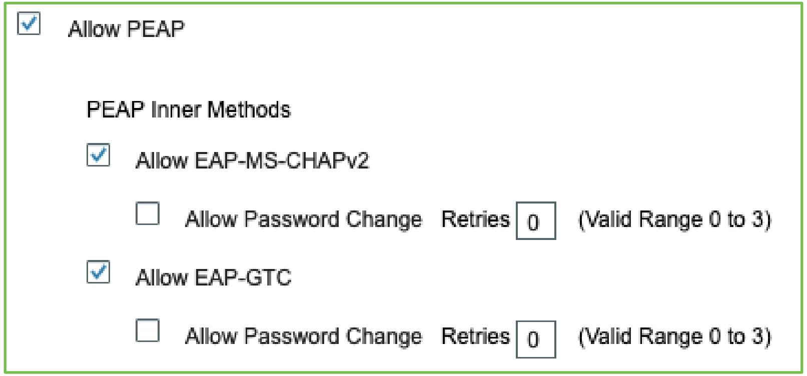


| | | | | | |
|---|---|---|---|---|---|
| Jun 05, 2019 12:24:53.541 PM | ⊗ | 🔍 | mfreeze | E4:A7:A0:81:72:A7 | 24407 User authentication against Active Directory failed since user i... |
| Jun 05, 2019 12:24:05.948 PM | ⊗ | 🔍 | mfreeze | E4:A7:A0:81:72:A7 | 24407 User authentication against Active Directory failed since user i... |
| Jun 05, 2019 12:22:35.013 PM | ⊗ | 🔍 | mfreeze | E4:A7:A0:81:72:A7 | 24407 User authentication against Active Directory failed since user i... |
| Jun 05, 2019 12:21:03.401 PM | ⊗ | 🔍 | mfreeze | E4:A7:A0:81:72:A7 | 24407 User authentication against Active Directory failed since user i... |
| Jun 05, 2019 12:19:31.953 PM | ⊗ | 🔍 | mfreeze | E4:A7:A0:81:72:A7 | 24407 User authentication against Active Directory failed since user i... |
| Jun 05, 2019 12:18:00.613 PM | ⊗ | 🔍 | mfreeze | E4:A7:A0:81:72:A7 | 24407 User authentication against Active Directory failed since user i... |
| Jun 05, 2019 12:16:28.959 PM | ⊗ | 🔍 | mfreeze | E4:A7:A0:81:72:A7 | 24407 User authentication against Active Directory failed since user i... |
| Jun 05, 2019 12:14:57.771 PM | ⊗ | 🔍 | mfreeze | E4:A7:A0:81:72:A7 | 24407 User authentication against Active Directory failed since user i... |
| Jun 05, 2019 12:13:26.166 PM | ⊗ | 🔍 | mfreeze | E4:A7:A0:81:72:A7 | 24407 User authentication against Active Directory failed since user i... |
| Jun 05, 2019 12:04:22.019 PM | ⊗ | 🔍 | mfreeze | 48:A1:95:54:D1:28 | 24407 User authentication against Active Directory failed since user i... |

# PEAP Password Retries

## Solution

- Disable PEAP Password Retries
- Policy -> Policy Elements -> Results -> Authentication -> Allowed Protocols



☑ Allow PEAP

PEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

□ Allow Password Change Retries 0 (Valid Range 0 to 3)

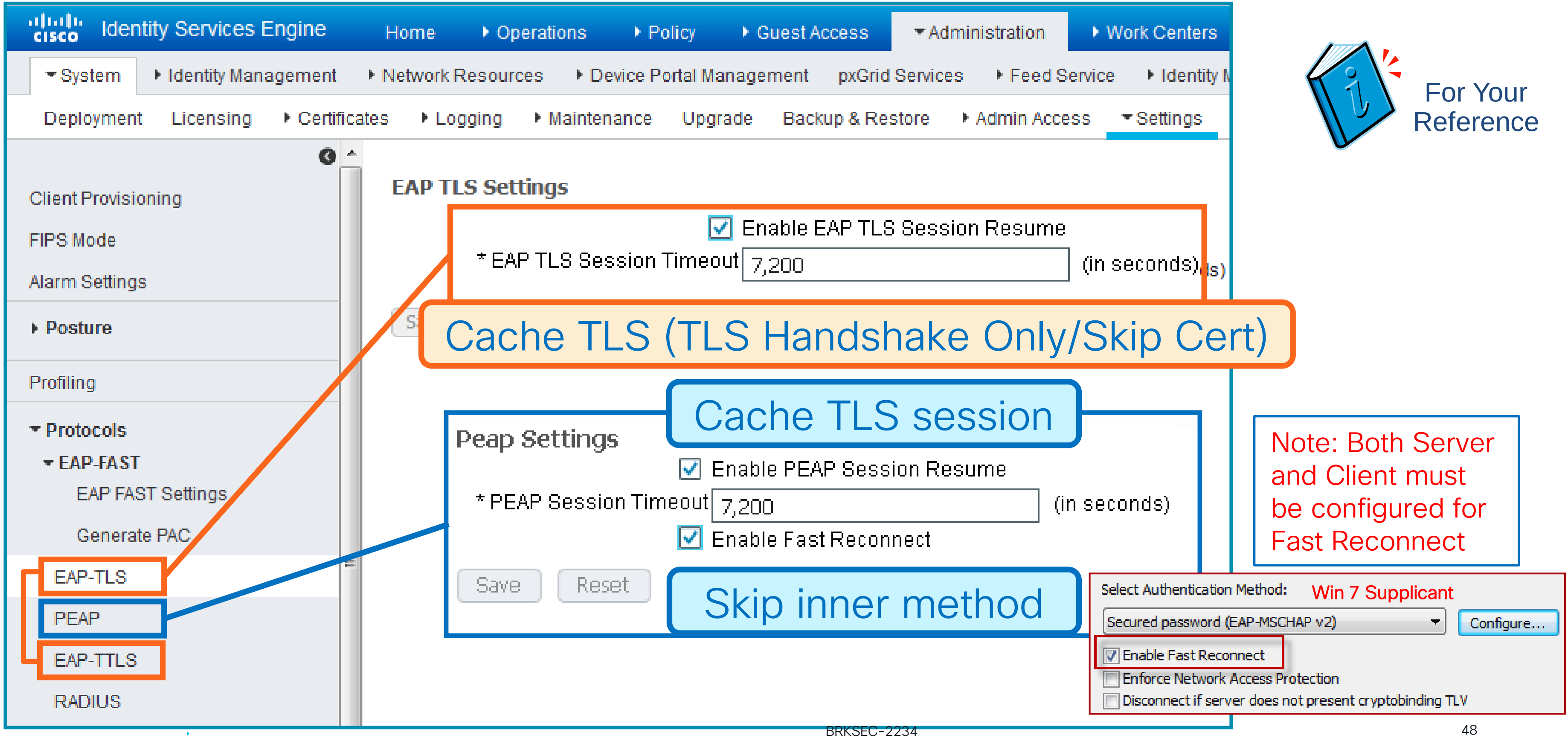
☑ Allow EAP-GTC

□ Allow Password Change Retries 0 (Valid Range 0 to 3)

- Create separate authentication rules if retries are needed for Windows Supplicants

# Enable EAP Session Resume / Fast Reconnect

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



**EAP TLS Settings**

☑ Enable EAP TLS Session Resume

* EAP TLS Session Timeout 7,200 (in seconds)s)

Cache TLS (TLS Handshake Only/Skip Cert)

**Peap Settings**

Cache TLS session

☑ Enable PEAP Session Resume

* PEAP Session Timeout 7,200 (in seconds)

☑ Enable Fast Reconnect

Skip inner method

Note: Both Server and Client must be configured for Fast Reconnect

Select Authentication Method: Win 7 Supplicant

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

□ Enforce Network Access Protection

□ Disconnect if server does not present cryptobinding TLV

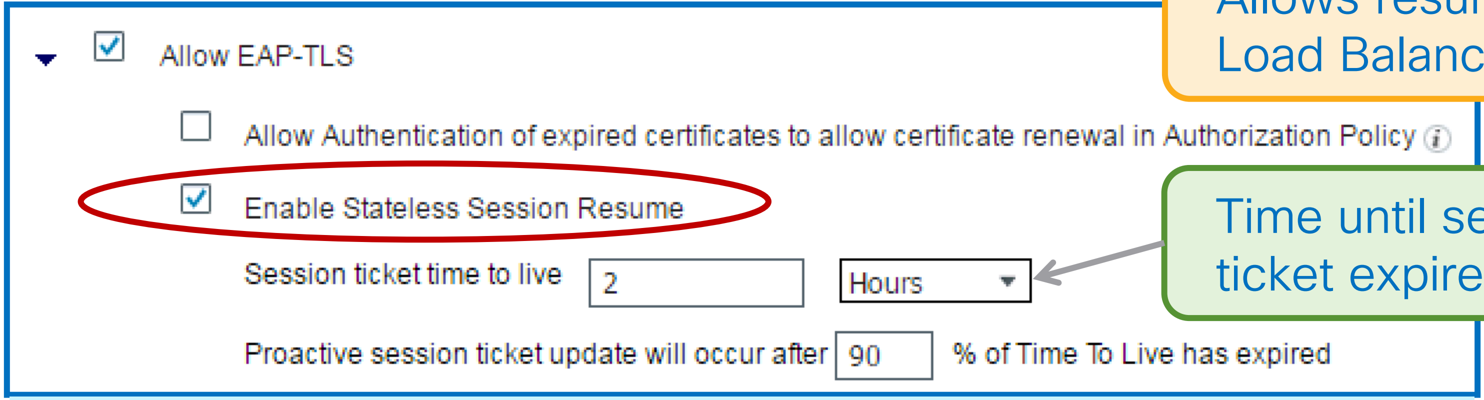
# ISE Stateless Session Resume

## Allows Session Resume Across All PSNs

- Session ticket extension per RFC 5077

  [Transport Layer Security (TLS) Session Resumption without Server-Side State]

- ISE issues TLS client a session ticket that can be presented to any PSN to shortcut reauth process (Default = Disabled)



☑ Allow EAP-TLS

□ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

☑ Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after 90 % of Time To Live has expired

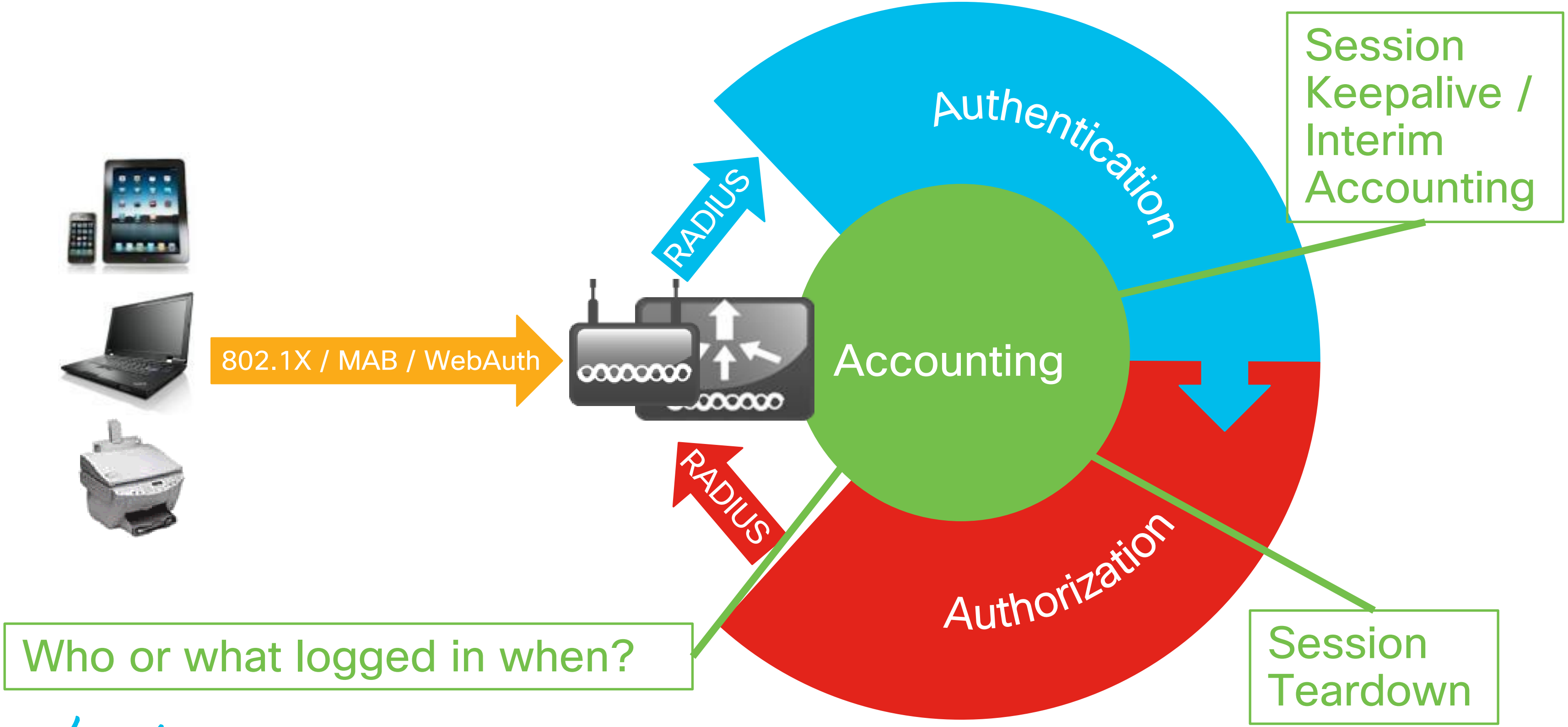
Allows resume with Load Balancers

Time until session ticket expires

Policy > Policy Elements > Results > Authentication > Allowed Protocols

# Network Device Recommendations

# Accounting



802.1X / MAB / WebAuth
RADIUS
RADIUS
Authentication
Accounting
Authorization
Session Keepalive / Interim Accounting
Session Teardown
Who or what logged in when?

# 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

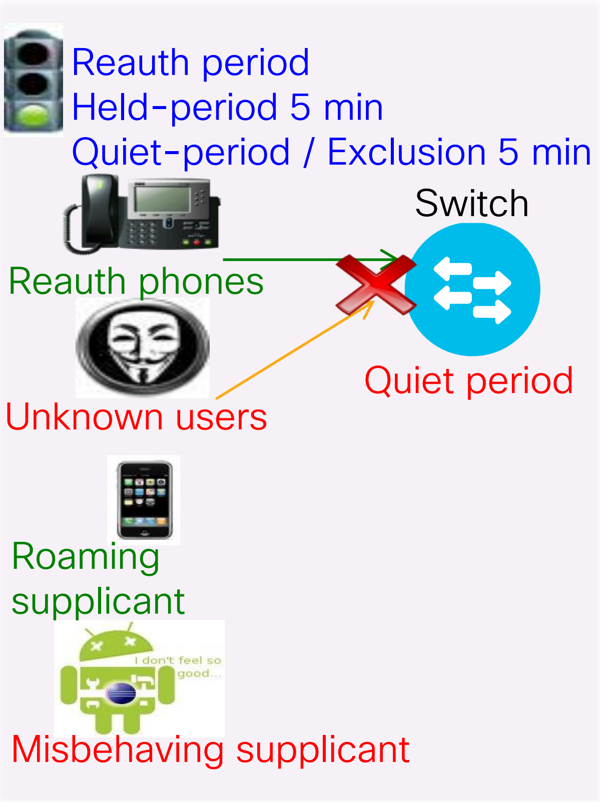
Cisco Switches

*sw# aaa accounting update newinfo periodic 1440*

https://community.cisco.com/t5/security-documents/ise-secure-wired-access-prescriptive-deployment-guide/ta-p/3641515

# 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.

# AireOS WLC Recommended Configuration

- Do not configure interim accounting to ISE servers
  - Interim accounting set by default when needed by ISE
  - Increases load with no added benefit
  - Pre 8.0 leave the interim accounting setting disabled
  - Post 8.0 check the interim accounting box with a timer of 0 seconds
- Use public certificates on ISE and WLC Virtual IP to reduce client messaging.
- When using an Anchor/Foreign Setup do not configure AAA on the Anchor Controller.

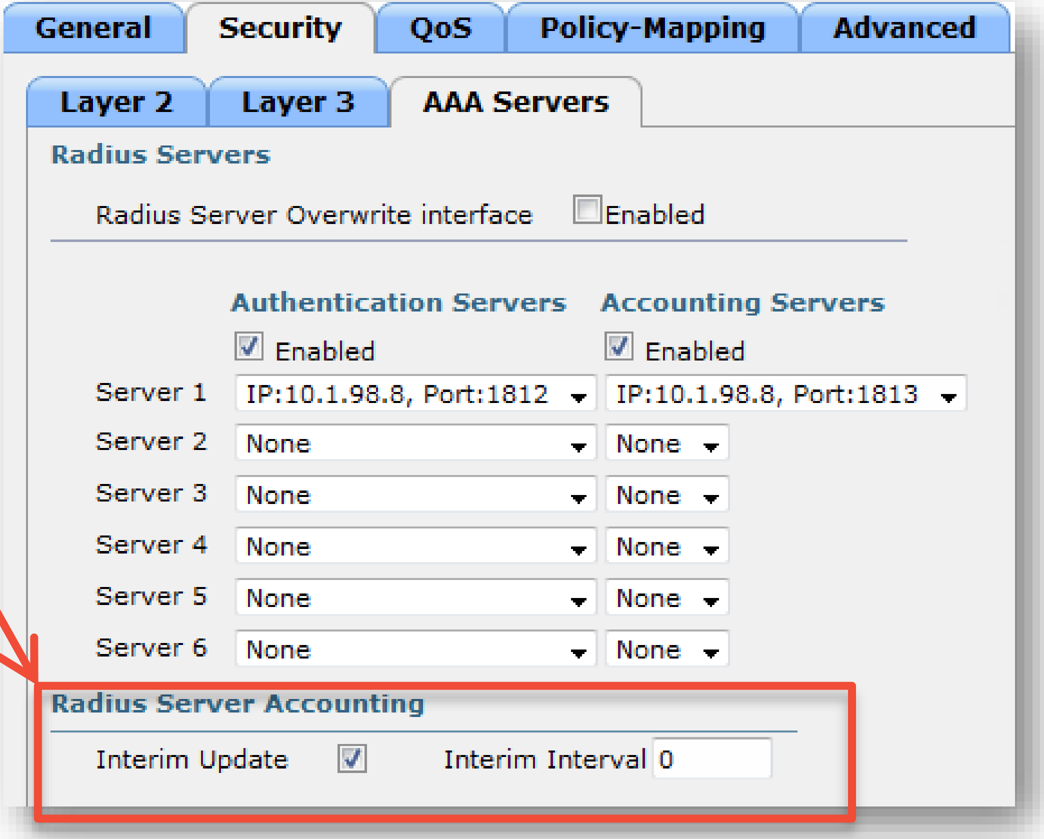
Prevent Large Scale RADIUS Meltdowns

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

# Advice: Timers - WLANs

## Interim Update

- WLC 7.6:
  - Recommended setting: Disabled
- WLC 8.0+:
  - Recommended setting: Enabled with Interval set to 0
  - Behavior: Only send update on IP address change
  - Device Sensor updates not impacted
- Settings mapped correctly on upgrades



Radius Servers

Radius Server Overwrite interface □ Enabled

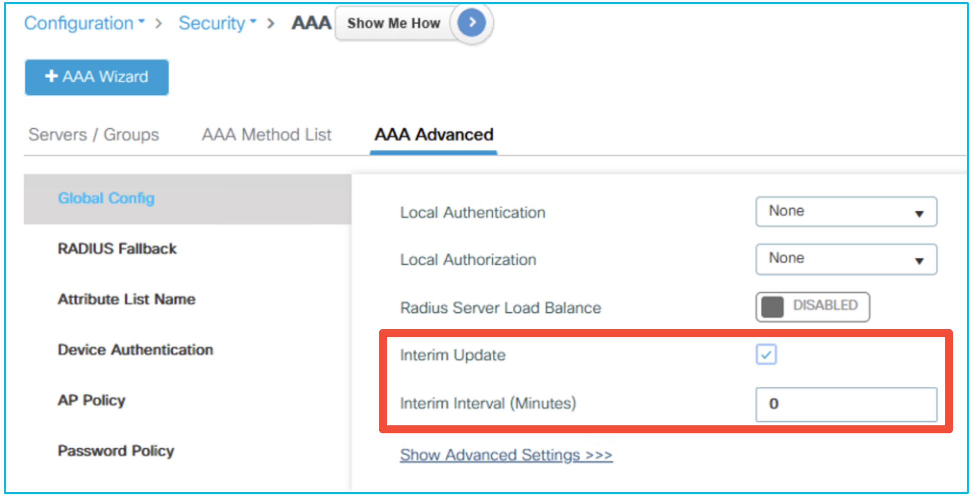
| | Authentication Servers | Accounting Servers |
|---|---|---|
| | ☑ Enabled | ☑ Enabled |
| Server 1 | IP:10.1.98.8, Port:1812 | IP:10.1.98.8, Port:1813 |
| Server 2 | None | None |
| Server 3 | None | None |
| Server 4 | None | None |
| Server 5 | None | None |
| Server 6 | None | None |

Radius Server Accounting

Interim Update ☑ Interim Interval 0

# 9800 WLC

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



Configuration > Security > AAA Show Me How

Servers / Groups AAA Method List AAA Advanced
Global Config
RADIUS Fallback
Attribute List Name
Device Authentication
AP Policy
Password Policy

Local Authentication: None

Local Authorization: None

Radius Server Load Balance: DISABLED

Interim Update: ☑

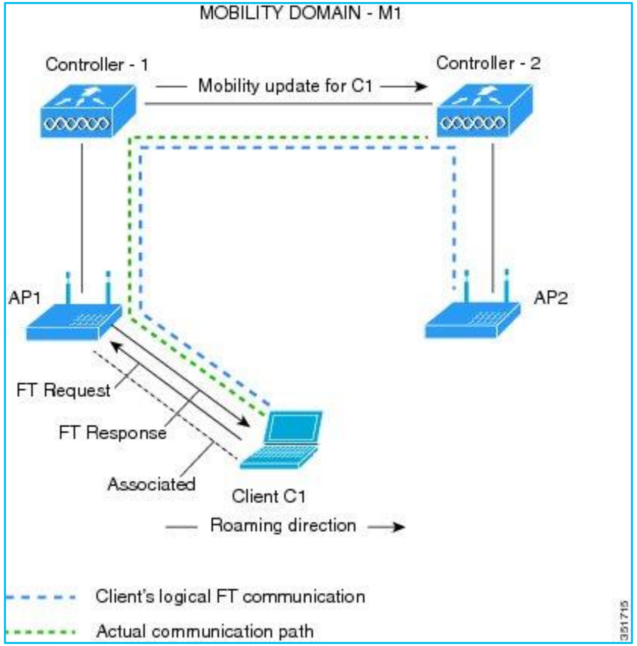
Interim Interval (Minutes): 0

Show Advanced Settings >>>

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

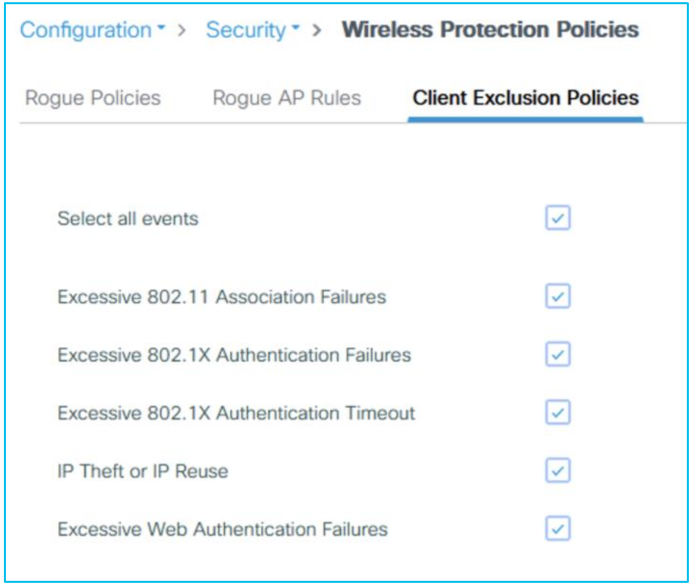
# Use Fast BSS Transition (802.11r)

- 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 done 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 > Security > **Wireless Protection Policies**

Rogue Policies | Rogue AP Rules | **Client Exclusion Policies**

Select all events ☑

Excessive 802.11 Association Failures ☑

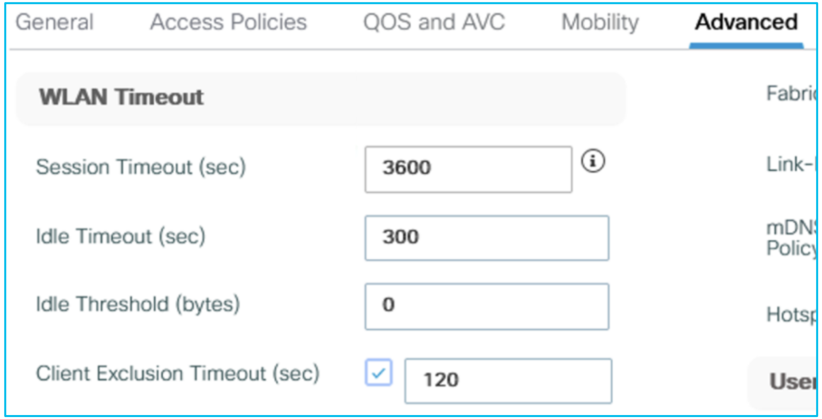
Excessive 802.1X Authentication Failures ☑

Excessive 802.1X Authentication Timeout ☑

IP Theft or IP Reuse ☑

Excessive Web Authentication Failures ☑

Configuration > Tags & Profiles > Policy



General | Access Policies | QOS and AVC | Mobility | **Advanced**

**WLAN Timeout**

Session Timeout (sec): 3600

Idle Timeout (sec): 300

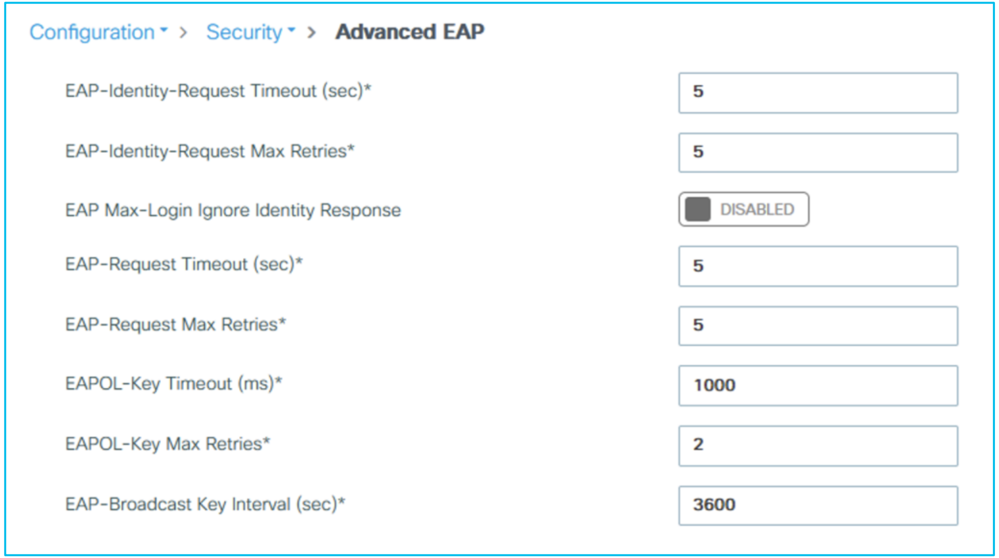
Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 120

# 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.



| | |
|---|---|
| EAP-Identity-Request Timeout (sec)* | 5 |
| EAP-Identity-Request Max Retries* | 5 |
| EAP Max-Login Ignore Identity Response | DISABLED |
| EAP-Request Timeout (sec)* | 5 |
| EAP-Request Max Retries* | 5 |
| EAPOL-Key Timeout (ms)* | 1000 |
| EAPOL-Key Max Retries* | 2 |
| EAP-Broadcast Key Interval (sec)* | 3600 |

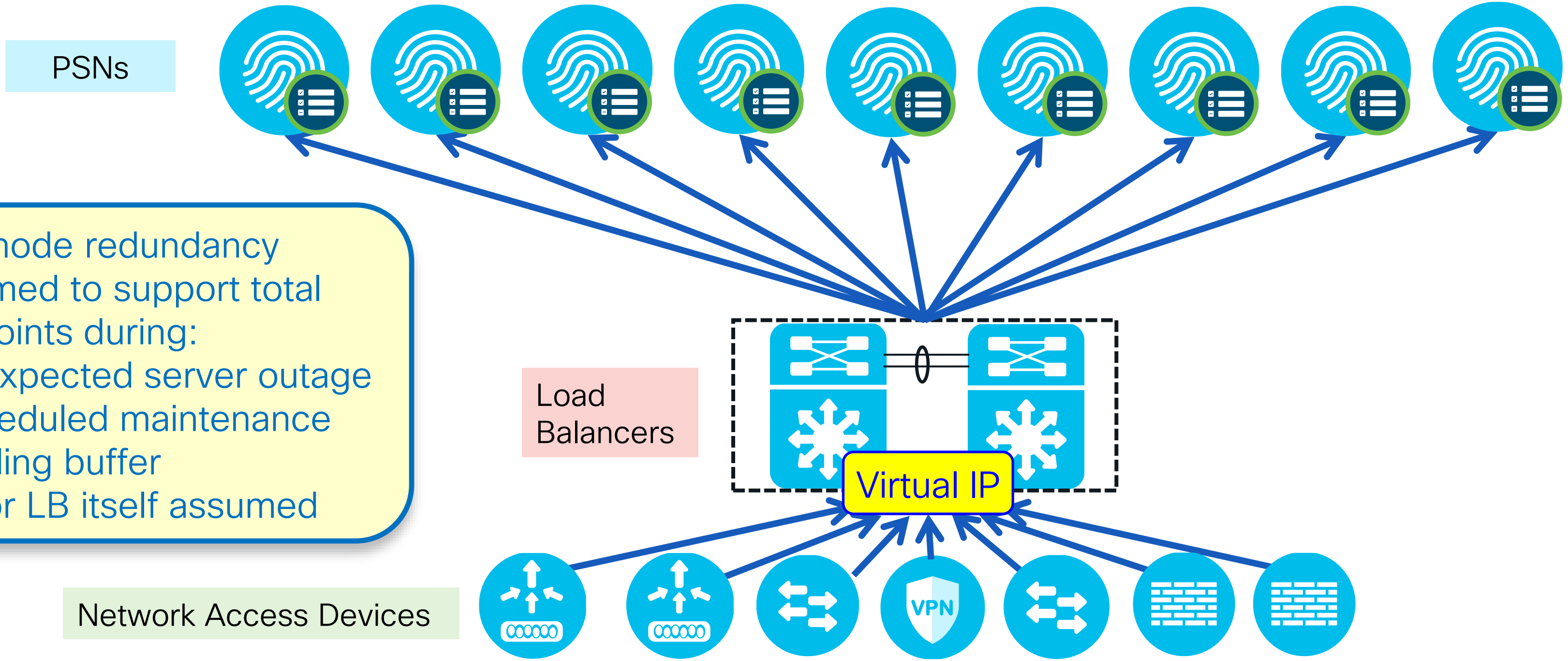
# Number of RADIUS Servers

- 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.

# Load Balancing

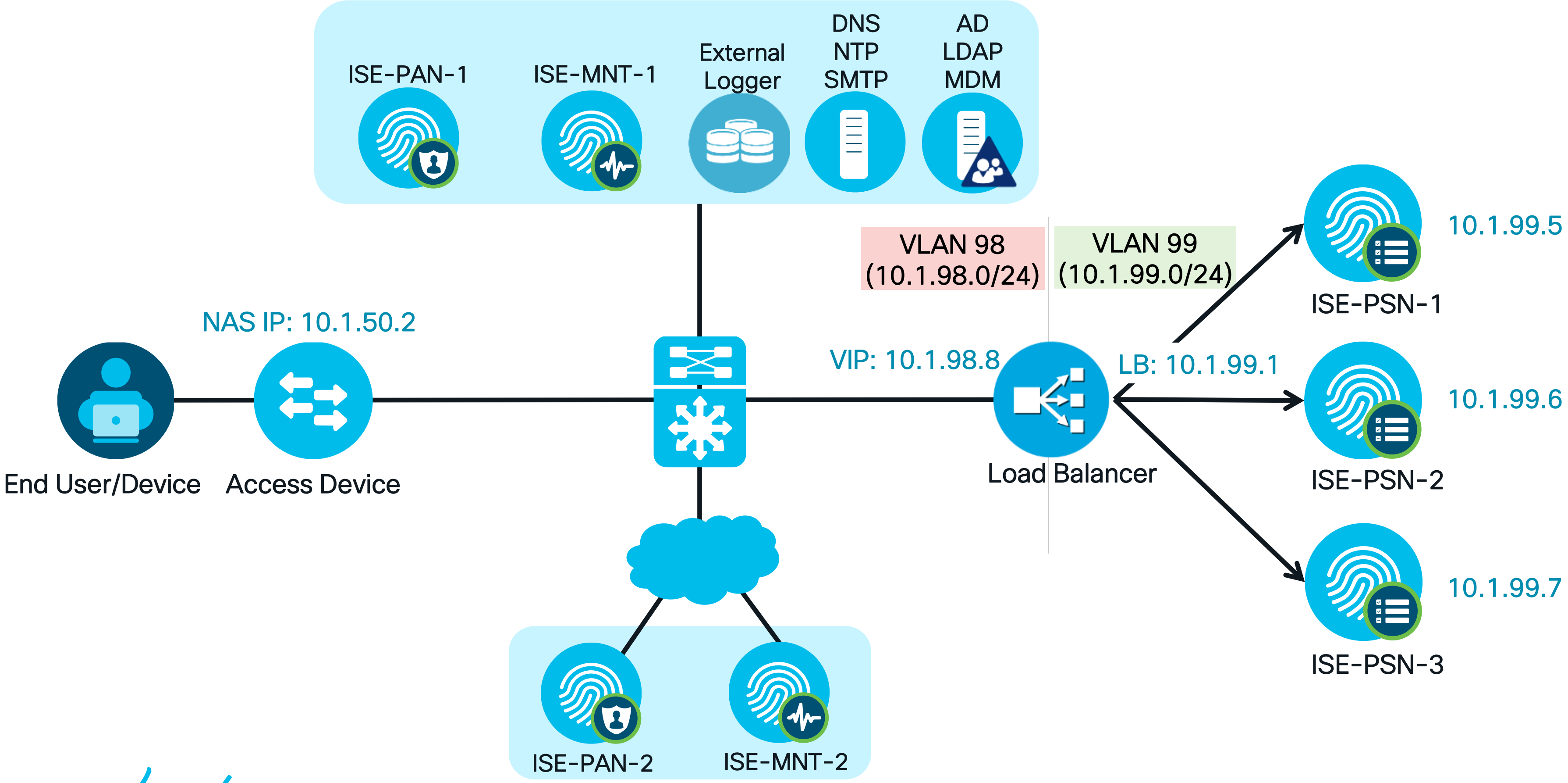
# Load Balancing RADIUS, Web, and Profiling Services

- 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

# High-Level Load Balancing Diagram

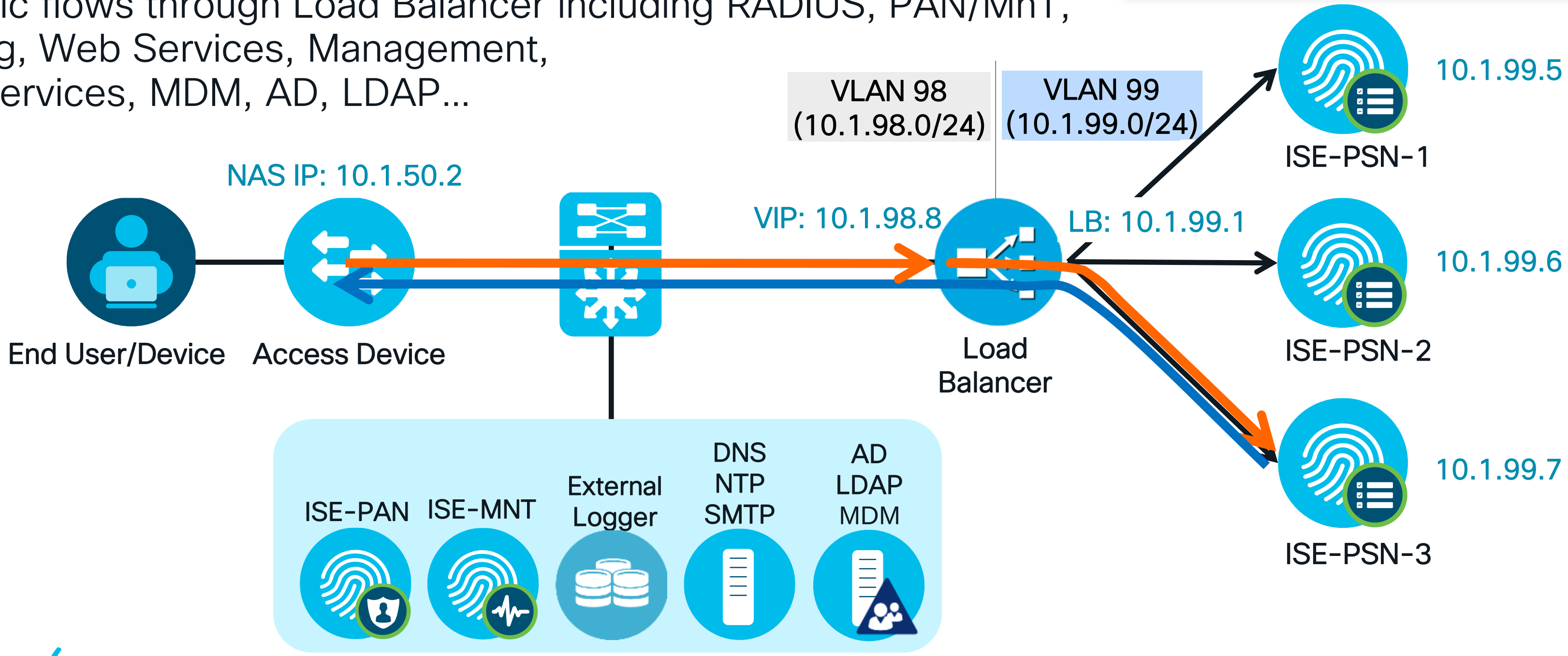


# Traffic Flow—Fully Inline: Physical Separation

## Physical Network Separation Using Separate LB Interfaces

Fully Inline Traffic Flow recommended—physical or logical

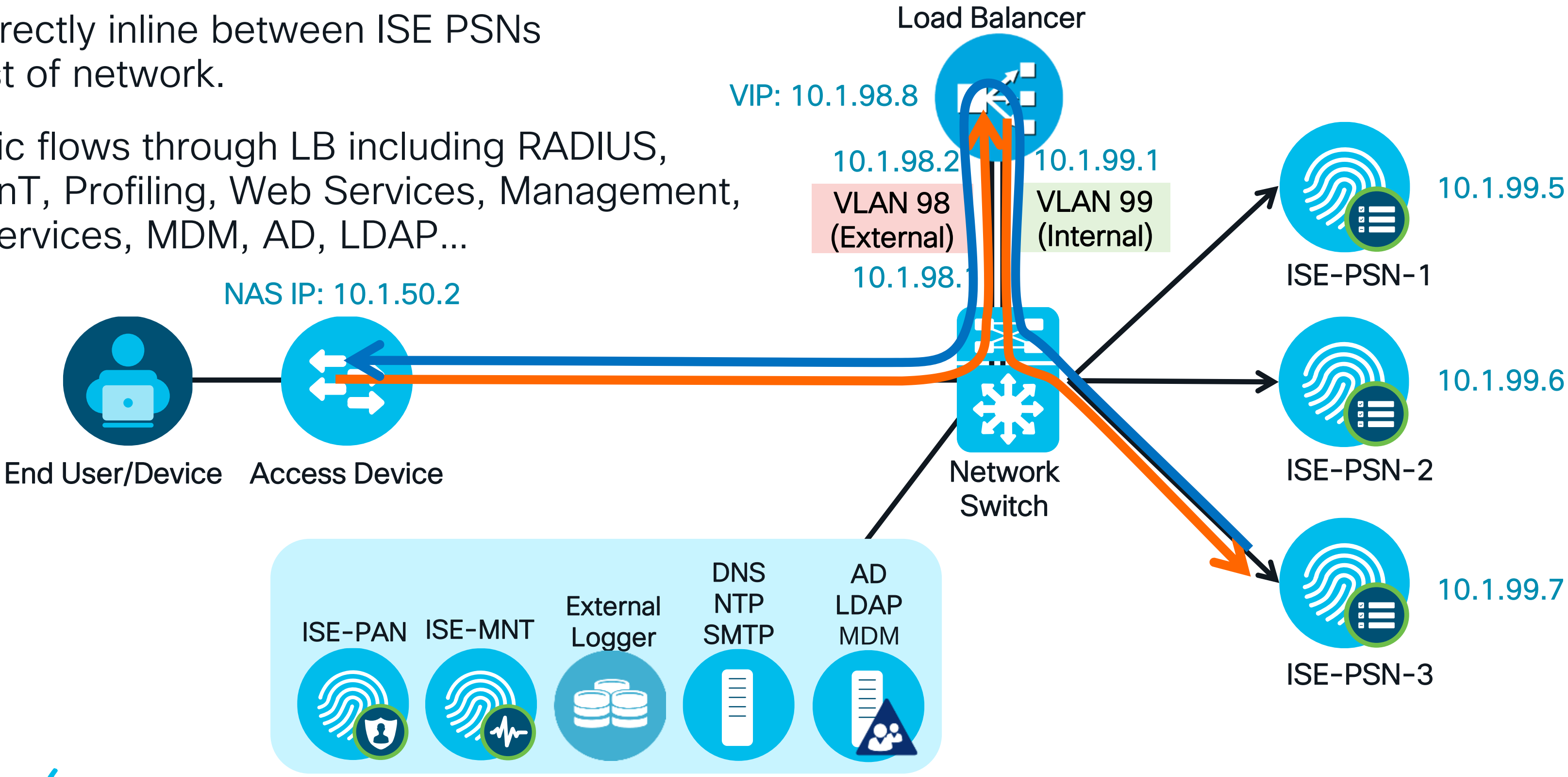
- Load Balancer is directly inline between PSNs and rest of network.
- All traffic flows through Load Balancer including RADIUS, PAN/MnT, Profiling, Web Services, Management, Feed Services, MDM, AD, LDAP…



# 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...

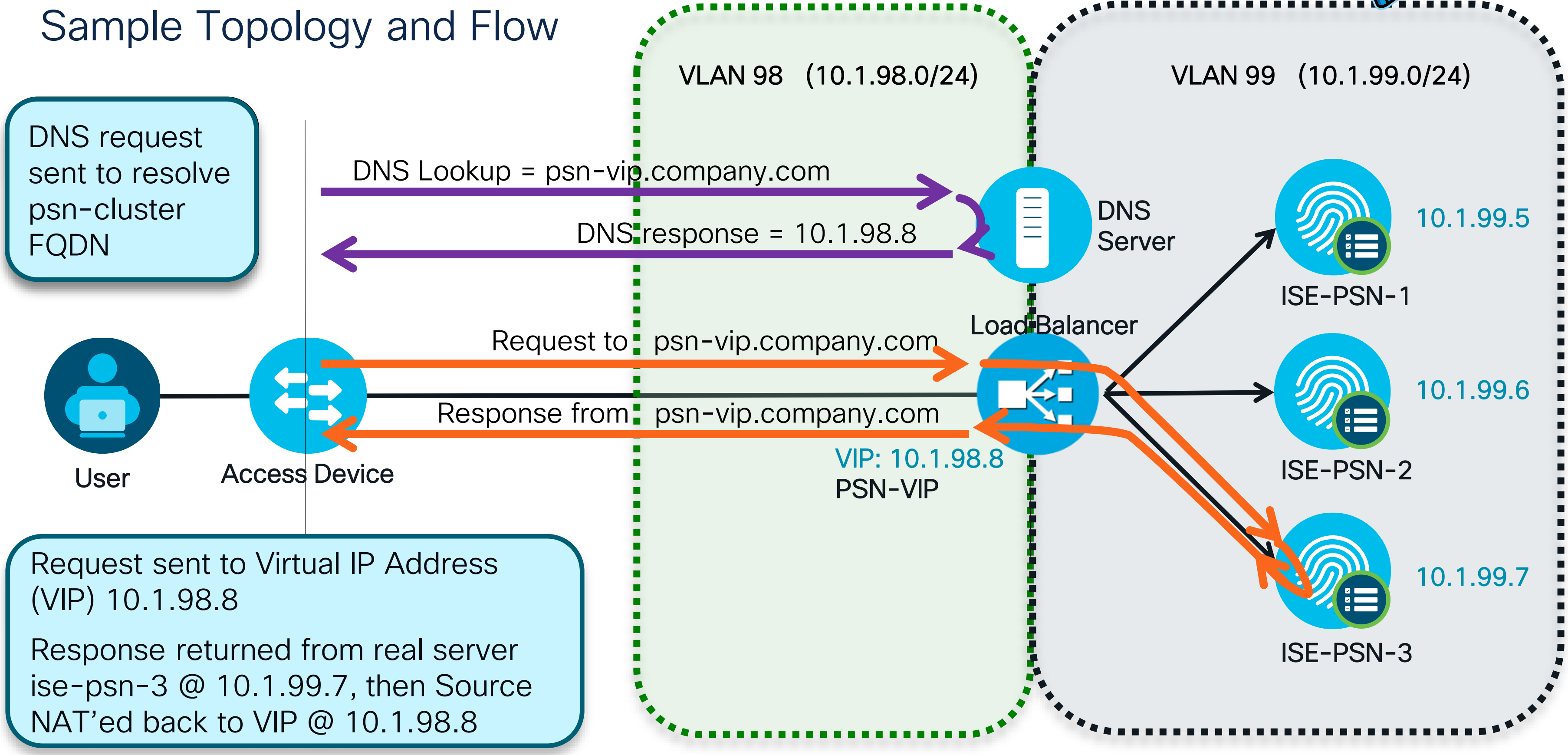


# PSN Load Balancing

## Sample Topology and Flow

For Your Reference

DNS request sent to resolve psn-cluster FQDN



Request sent to Virtual IP Address (VIP) 10.1.98.8

Response returned from real server ise-psn-3 @ 10.1.99.7, then Source NAT'ed back to VIP @ 10.1.98.8

# 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

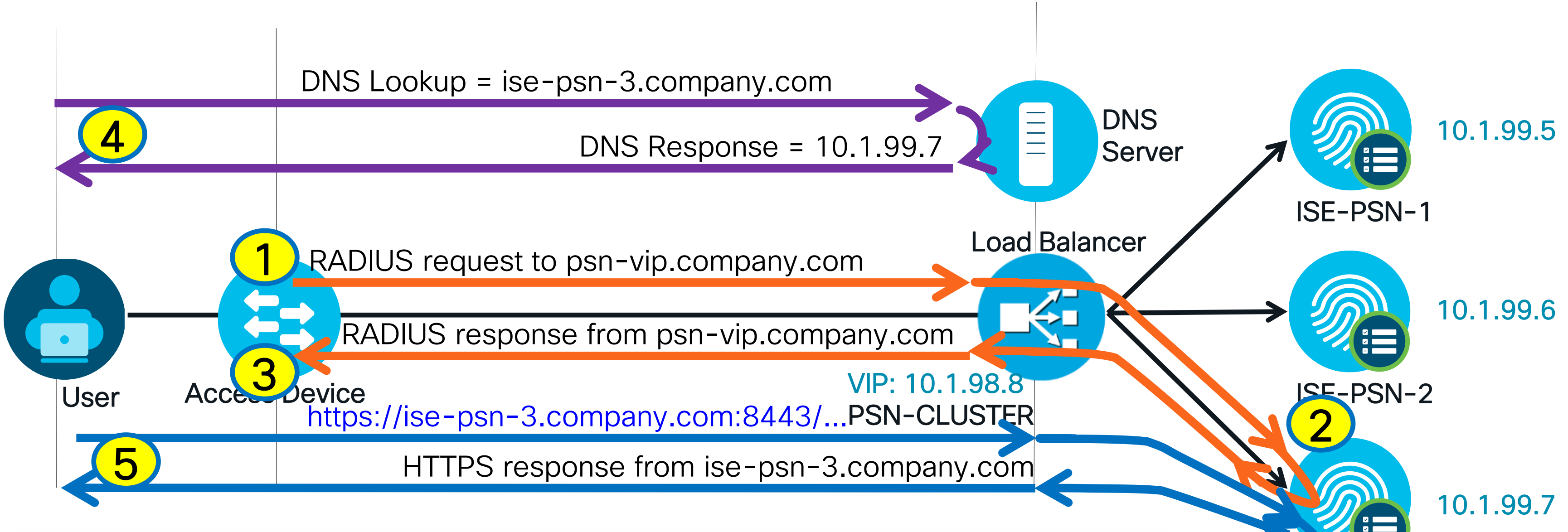
  LB VIP is the target for one-way Profile Data (no response required). VIP can be same or different than one used by RADIUS LB; Real server interface can be same or different than one used by RADIUS

- **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 with URL-Redirection

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


DNS Lookup = ise-psn-3.company.com
4
DNS Response = 10.1.99.7
DNS Server
10.1.99.5
ISE-PSN-1
Load Balancer
1
RADIUS request to psn-vip.company.com
RADIUS response from psn-vip.company.com
10.1.99.6
User
3
Access Device
VIP: 10.1.98.8
PSN-CLUSTER
ISE-PSN-2
2
https://ise-psn-3.company.com:8443/...
5
HTTPS response from ise-psn-3.company.com
10.1.99.7
ISE-PSN-3

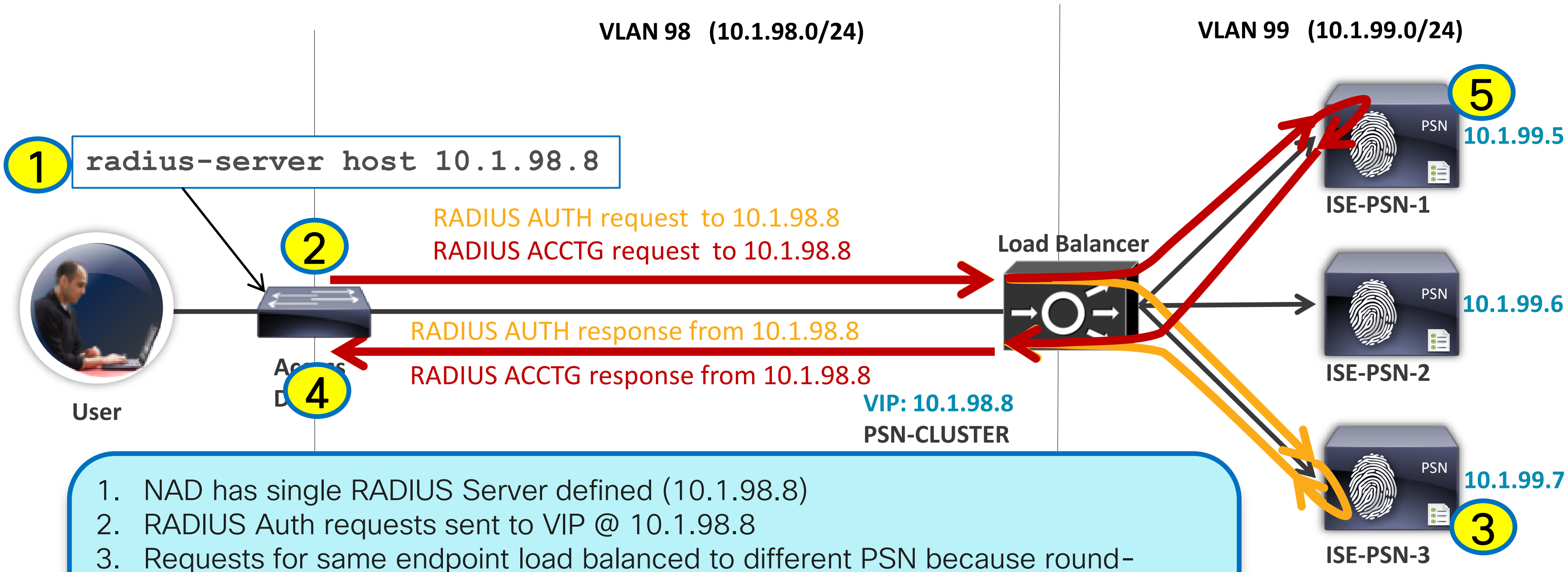
1. RADIUS Authentication requests sent to VIP @ 10.1.98.8
2. Requests for same endpoint load balanced to same PSN via RADIUS sticky.
3. RADIUS Authorization received from VIP @ 10.1.98.8 (originated by ise-psn-3 @ 10.1.99.7 with URL Redirect to https://ise-psn-3.company.com:8443/...
4. Client browser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

ISE Certificate

Subject CN =
ise-psn-3.company.com

# Load Balancing RADIUS

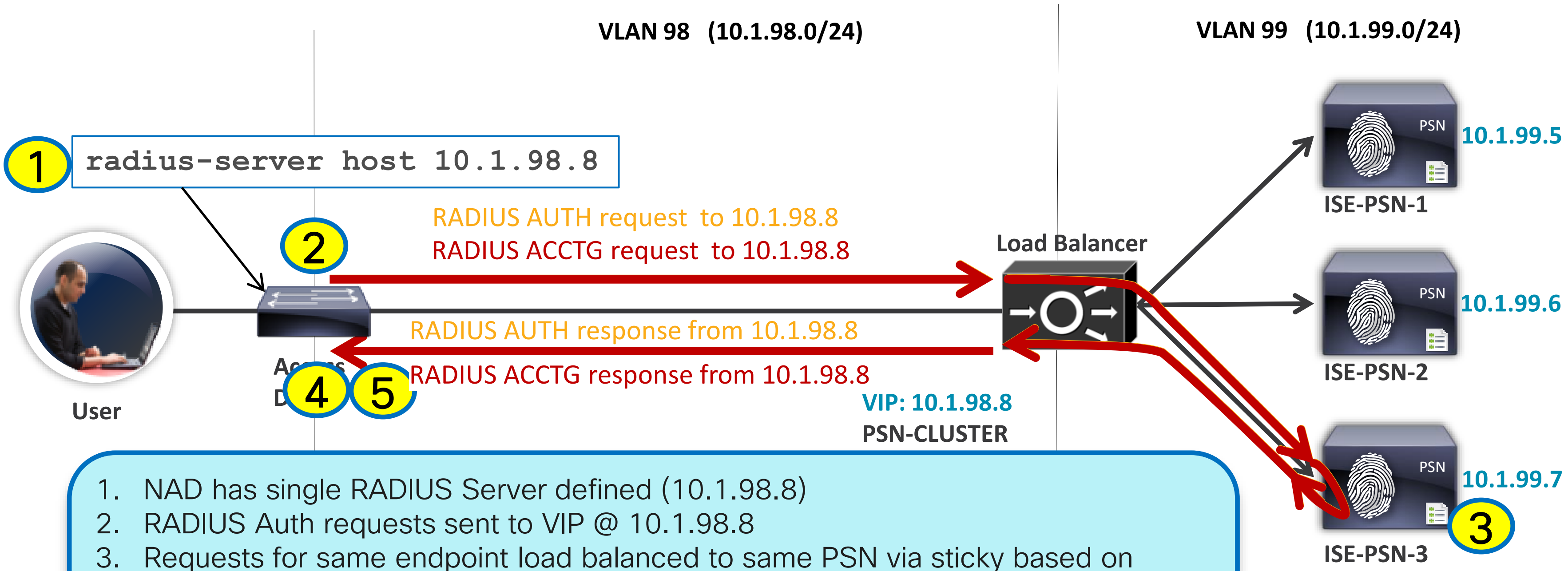
## Not Sticky


VLAN 98 (10.1.98.0/24)
VLAN 99 (10.1.99.0/24)
1
radius-server host 10.1.98.8
2
RADIUS AUTH request to 10.1.98.8
RADIUS ACCTG request to 10.1.98.8
RADIUS AUTH response from 10.1.98.8
RADIUS ACCTG response from 10.1.98.8
4
Access
D
User
Load Balancer
VIP: 10.1.98.8
PSN-CLUSTER
5
PSN
10.1.99.5
ISE-PSN-1
PSN
10.1.99.6
ISE-PSN-2
PSN
10.1.99.7
3
ISE-PSN-3

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 different PSN because round-robin(RR) load balancing is used without persistance (sticky).
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 different PSN based on RR and no sticky

# Load Balancing RADIUS

## Sticky

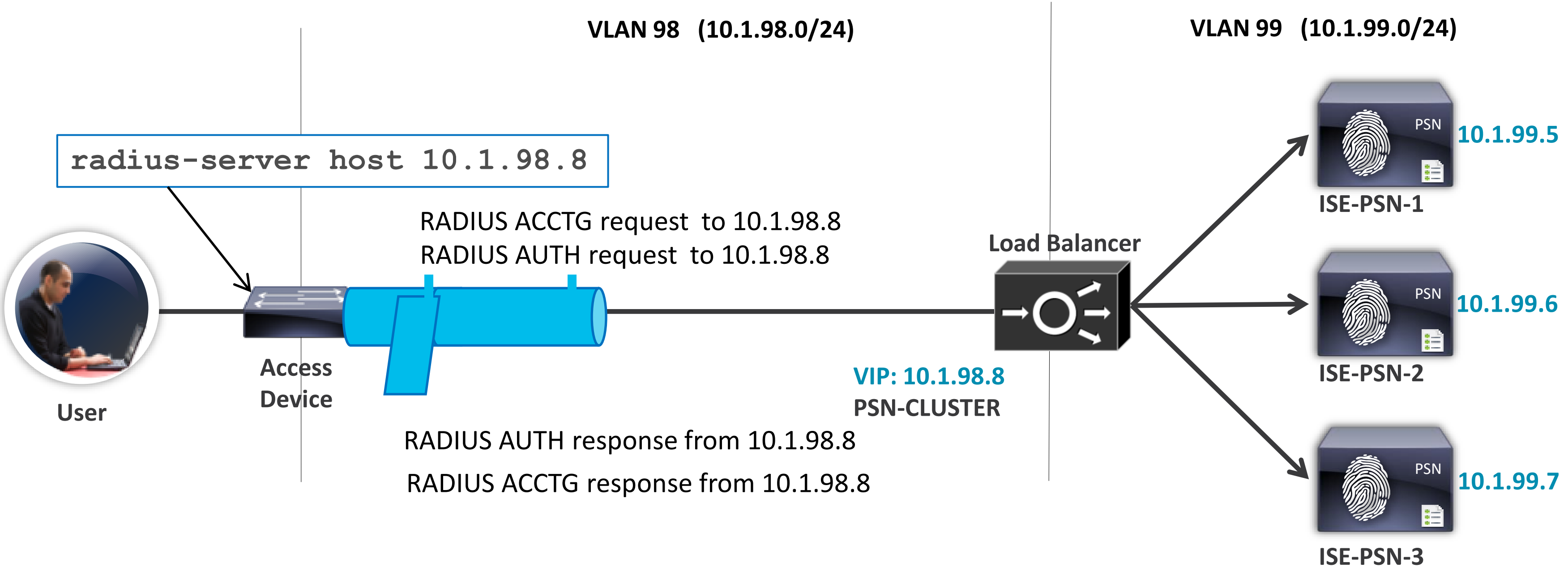


```
radius-server host 10.1.98.8
```

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 Balancing RADIUS

## Avoid spraying packets!!!



```
radius-server host 10.1.98.8
```

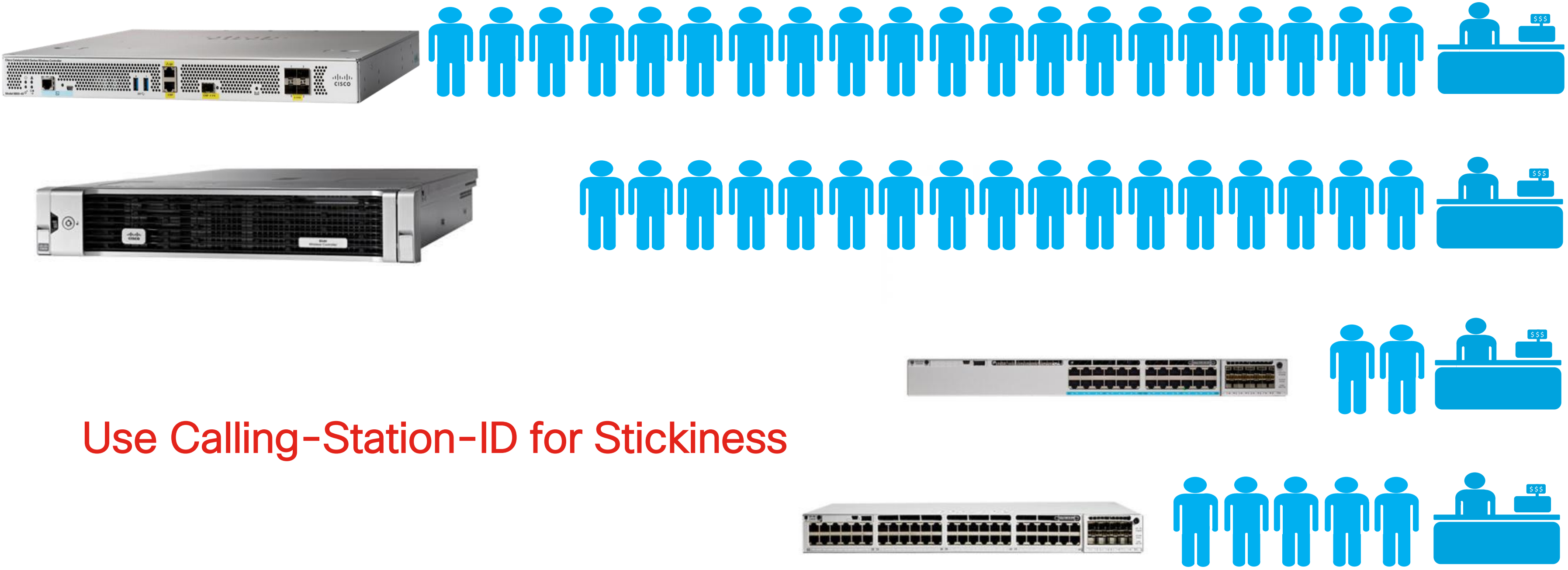
RADIUS ACCTG request to 10.1.98.8
RADIUS AUTH request to 10.1.98.8

RADIUS AUTH response from 10.1.98.8

RADIUS ACCTG response from 10.1.98.8

# Load Balancing RADIUS

## IP vs Calling Station ID Stickiness



Use Calling-Station-ID for Stickiness

# 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://community.cisco.com/t5/security-knowledge-base/ise-security-ecosystem-integration-guides/ta-p/4782363#load-balancing

# Profiling

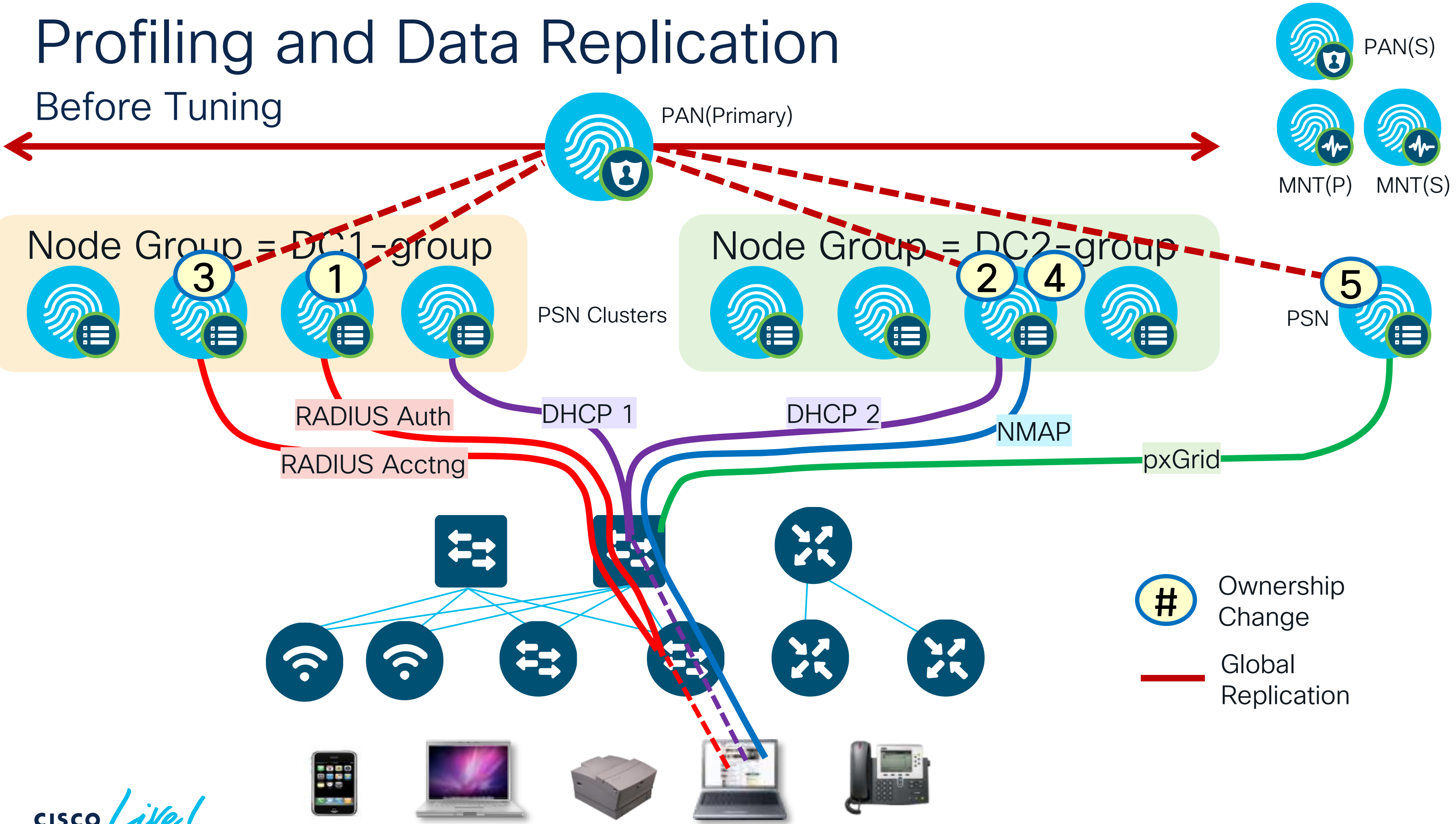
# Profiling Probe Selection Best Practices

| 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

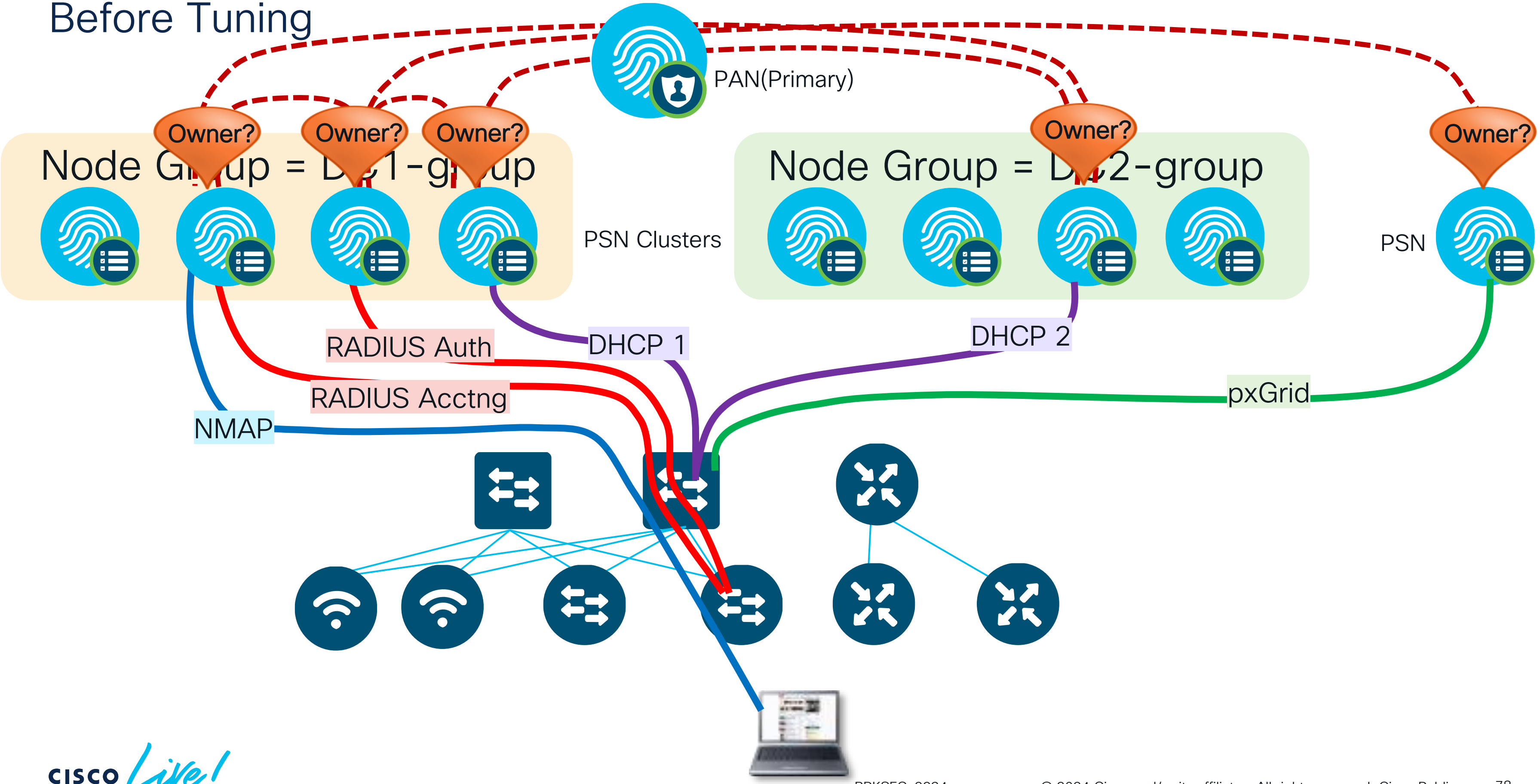
# Profiling and Data Replication

## Before Tuning



# Impact of Ownership Changes

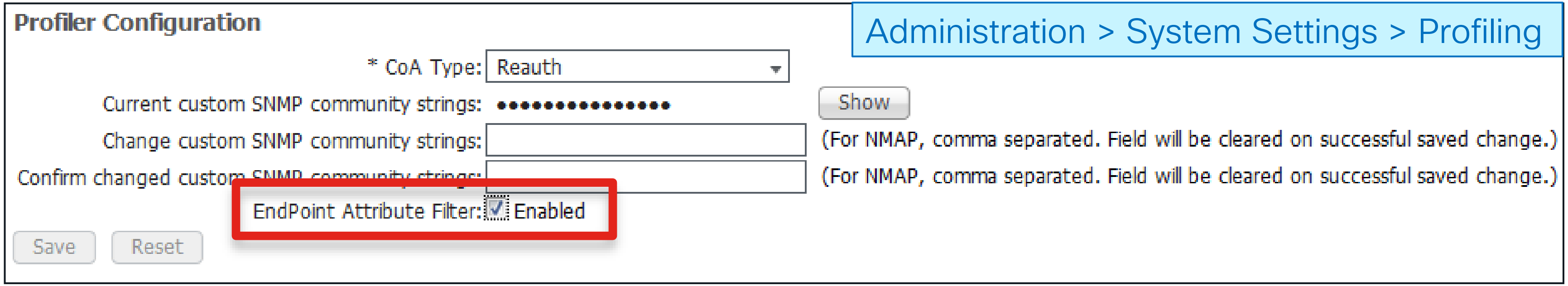
## Before Tuning



# 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.



Administration > System Settings > Profiling

**Profiler Configuration**

* CoA Type: Reauth

Current custom SNMP community strings: ••••••••••••••• Show

Change custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

Confirm changed custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

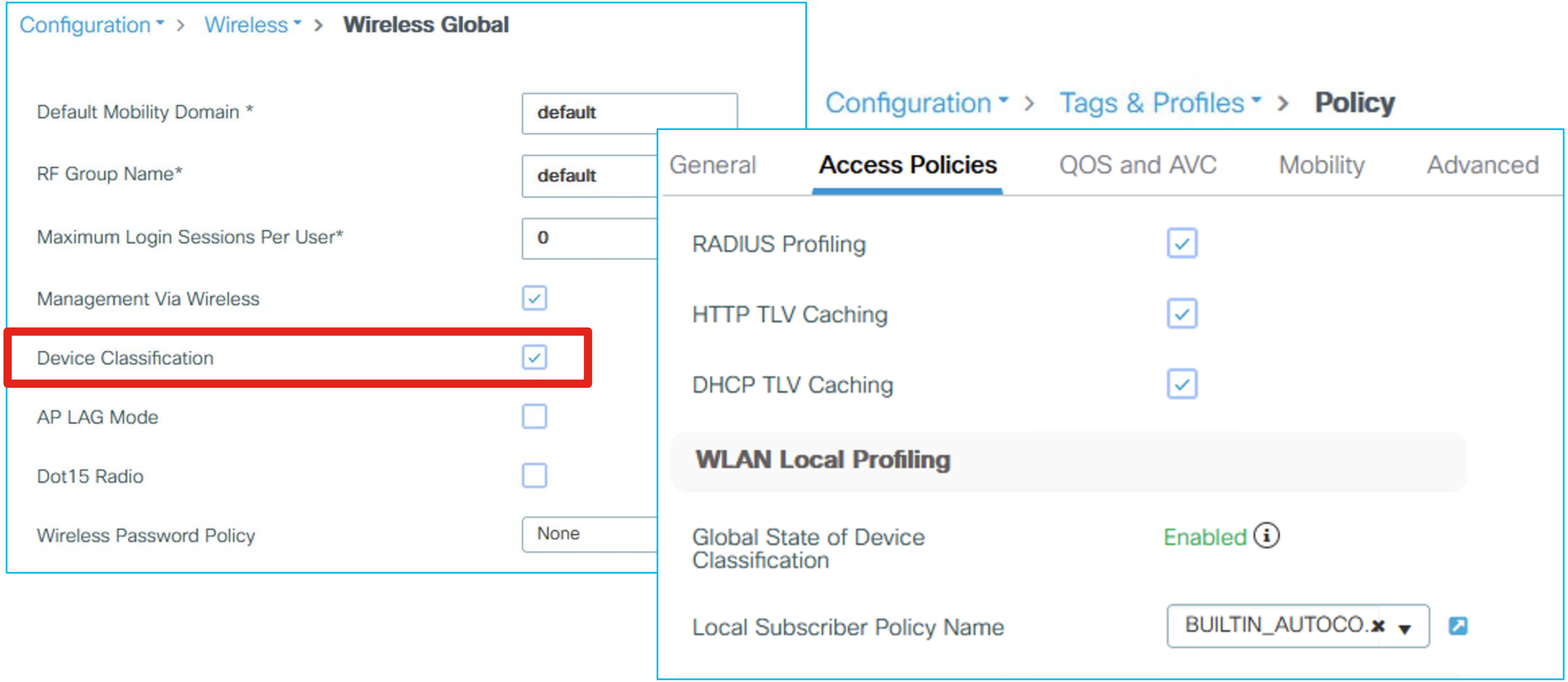
EndPoint Attribute Filter: ☑ Enabled

- 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)



Configuration > Wireless > Wireless Global

Default Mobility Domain * default

RF Group Name* default

Maximum Login Sessions Per User* 0

Management Via Wireless ☑

Device Classification ☑

AP LAG Mode □

Dot15 Radio □

Wireless Password Policy None

Configuration > Tags & Profiles > Policy

RADIUS Profiling ☑

HTTP TLV Caching ☑

DHCP TLV Caching ☑

**WLAN Local Profiling**

Global State of Device Classification Enabled

Local Subscriber Policy Name BUILTIN_AUTOCO.

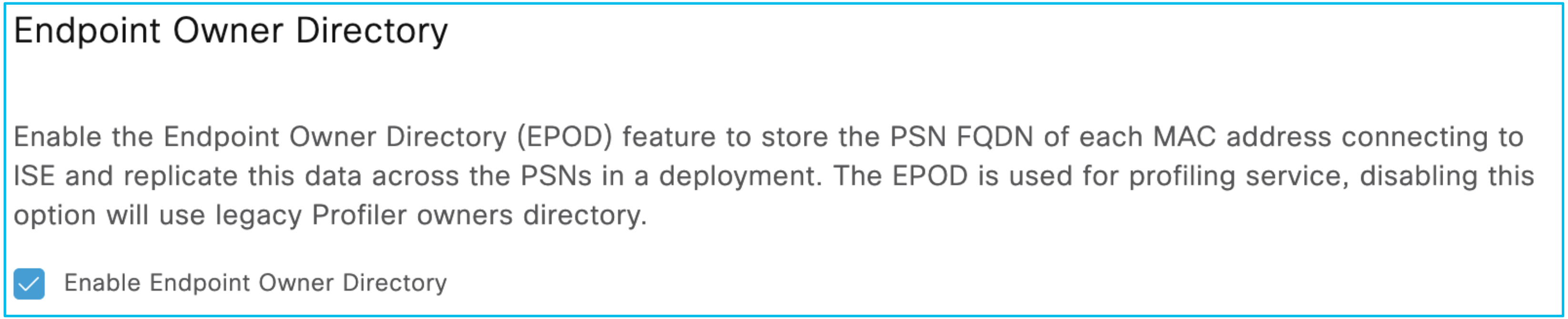
# Profiling Filtering

## Default Radius Probe

- Introduced in versions:
  - 2.7 patch 8, 3.0 patch 7, 3.1 patch 5, 3.2 patch 1, 3.3 FCS
- Default RADIUS Probe sends data to profiler -> Profiler profiles
  - Default RADIUS Probe gets SYSLOGs from runtime
  - Filter defines messages to be ignored by profiler
  - Reduces profiling events that were adding no value
- No action required by admin!
  - Other then be running one of the above versions or later.

# 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



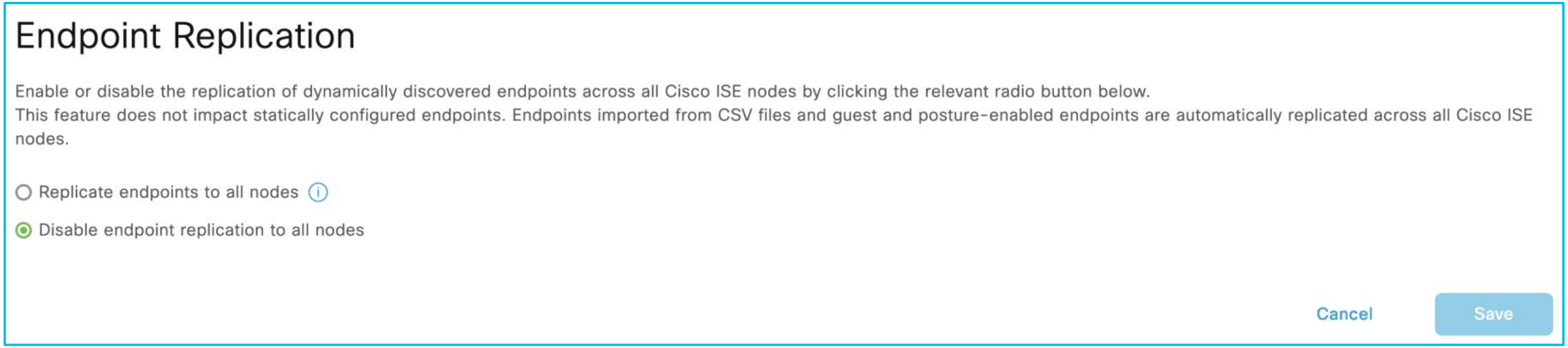
Endpoint Owner Directory

Enable the Endpoint Owner Directory (EPOD) feature to store the PSN FQDN of each MAC address connecting to ISE and replicate this data across the PSNs in a deployment. The EPOD is used for profiling service, disabling this option will use legacy Profiler owners directory.

☑ Enable Endpoint Owner Directory

# 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



## Endpoint Replication

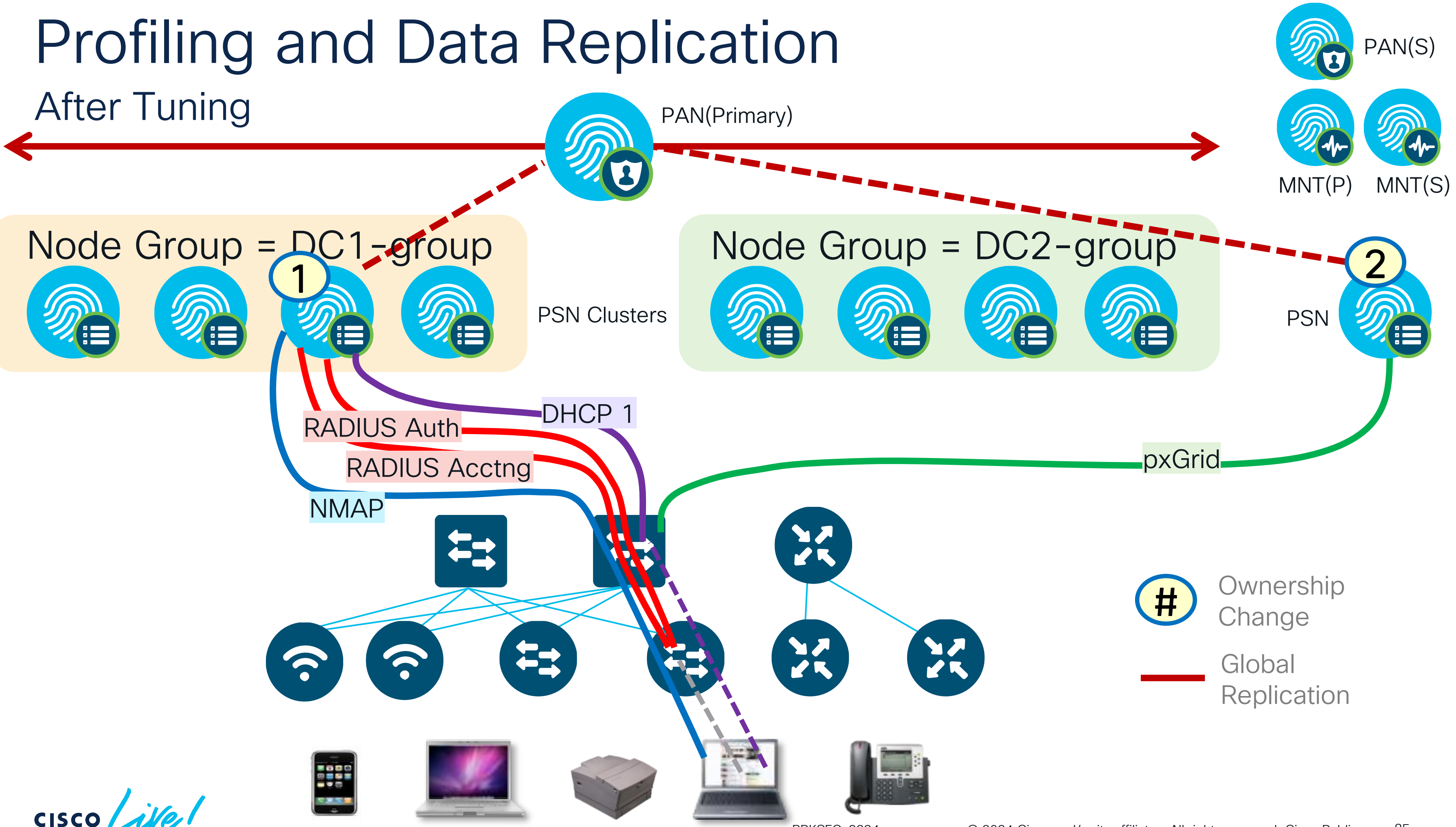
Enable or disable the replication of dynamically discovered endpoints across all Cisco ISE nodes by clicking the relevant radio button below.
This feature does not impact statically configured endpoints. Endpoints imported from CSV files and guest and posture-enabled endpoints are automatically replicated across all Cisco ISE nodes.

○ Replicate endpoints to all nodes ⓘ

● Disable endpoint replication to all nodes

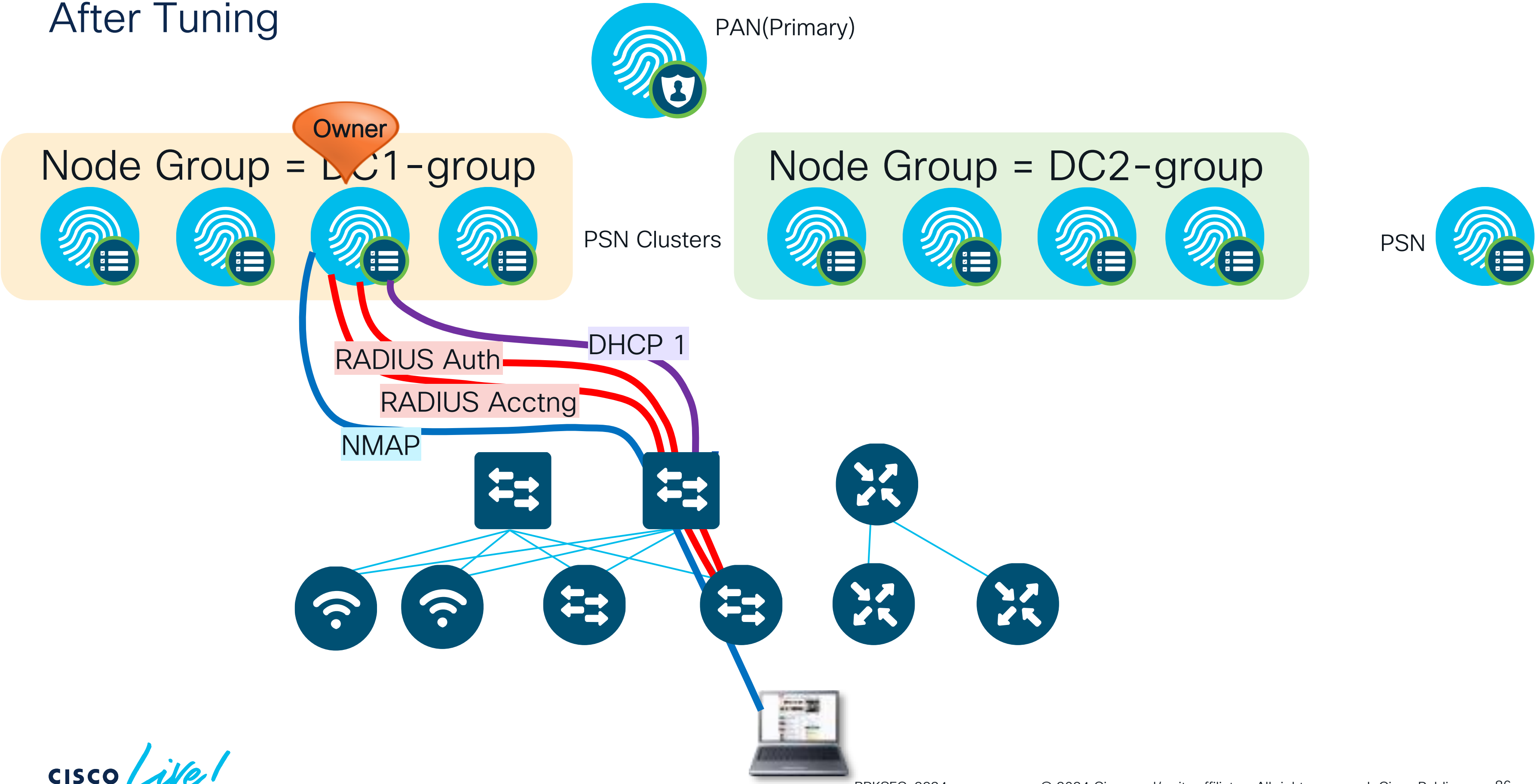
# Profiling and Data Replication

## After Tuning



# Impact of Ownership Changes

## After Tuning



# 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.

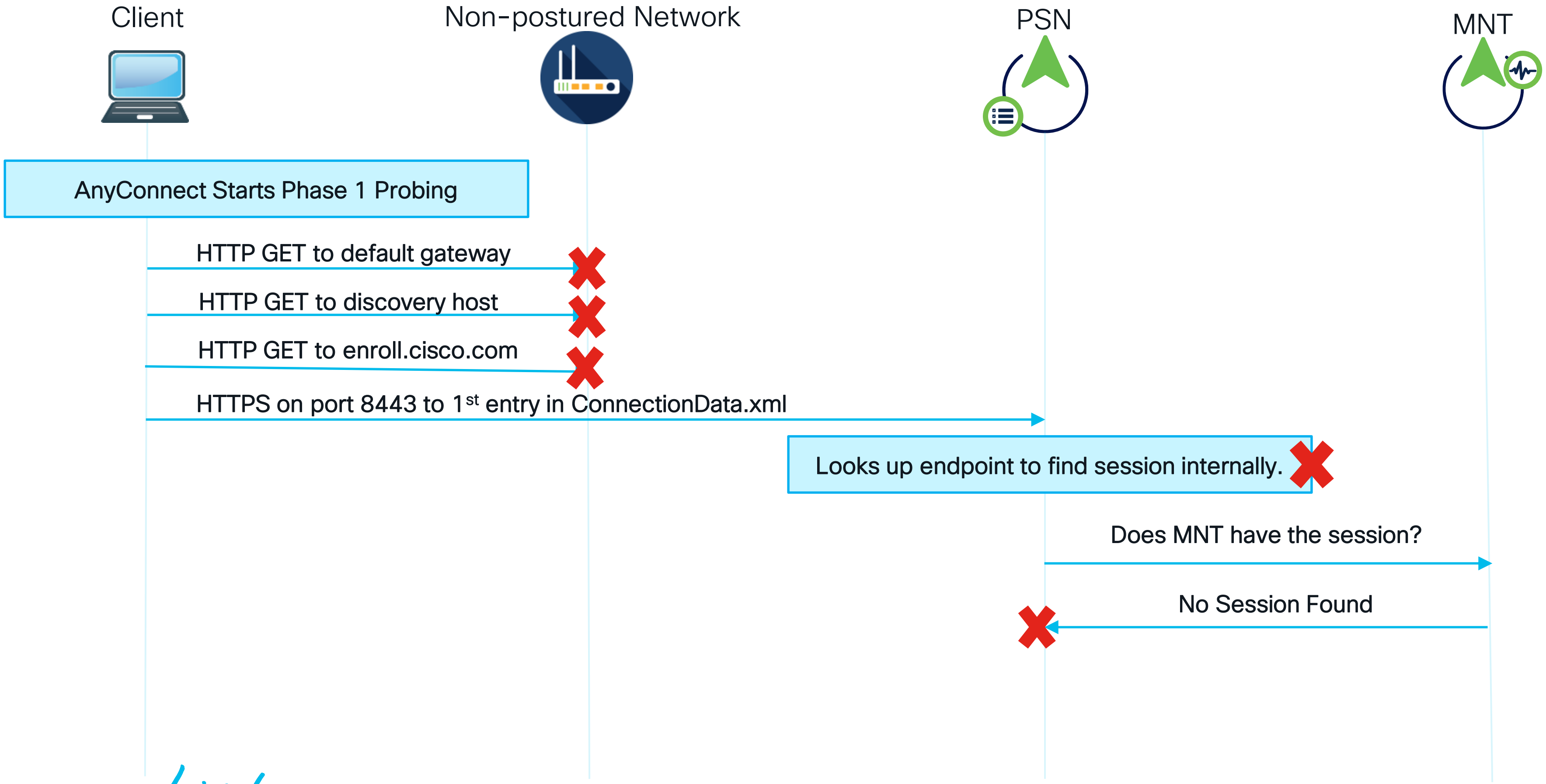
# ISE Profiling Best Practices

- 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**

# Posture

# Posture Probe from Unknown Client



Client

Non-postured Network

PSN

MNT

AnyConnect Starts Phase 1 Probing

HTTP GET to default gateway

HTTP GET to discovery host

HTTP GET to enroll.cisco.com

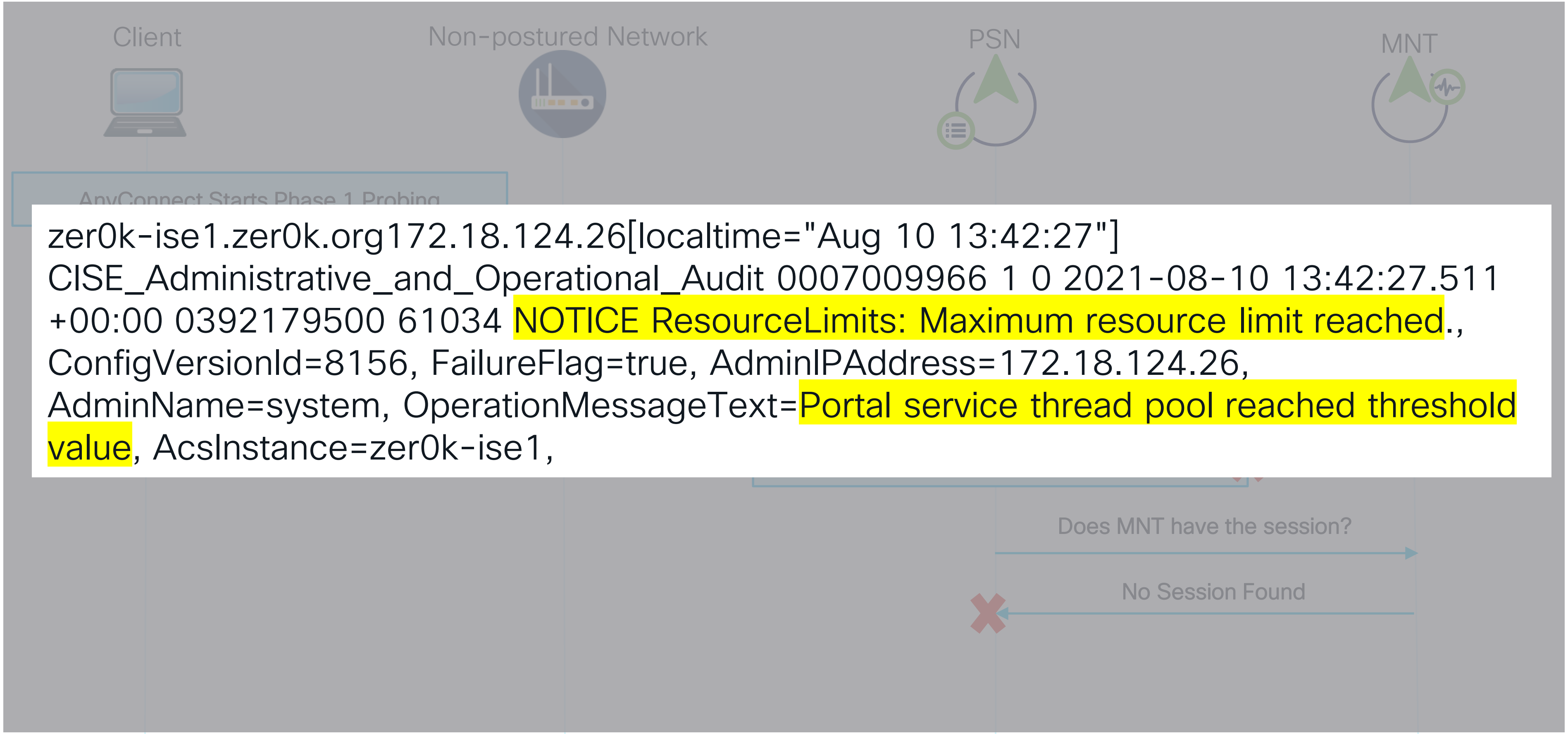
HTTPS on port 8443 to 1st entry in ConnectionData.xml

Looks up endpoint to find session internally.

Does MNT have the session?

No Session Found

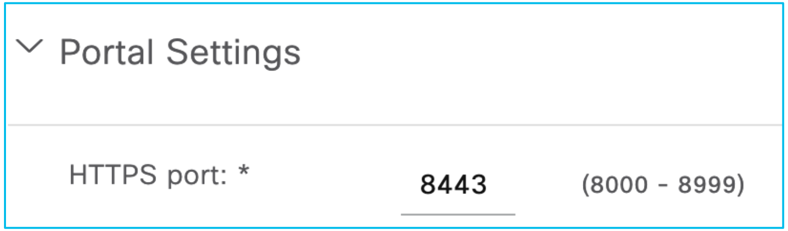
# Posture Probe from Unknown Client



```
zer0k-ise1.zer0k.org172.18.124.26[localtime="Aug 10 13:42:27"]
CISE_Administrative_and_Operational_Audit 0007009966 1 0 2021-08-10 13:42:27.511
+00:00 0392179500 61034 NOTICE ResourceLimits: Maximum resource limit reached.,
ConfigVersionId=8156, FailureFlag=true, AdminIPAddress=172.18.124.26,
AdminName=system, OperationMessageText=Portal service thread pool reached threshold
value, AcsInstance=zer0k-ise1,
```

# Block Posture Probes

- Block TCP port 8443 to PSNs from Non-postured networks.
  - ACLs, Firewalls, SGTs, etc...
- If Sponsor or Guest portals are in use from those networks the portal ports can be changed.

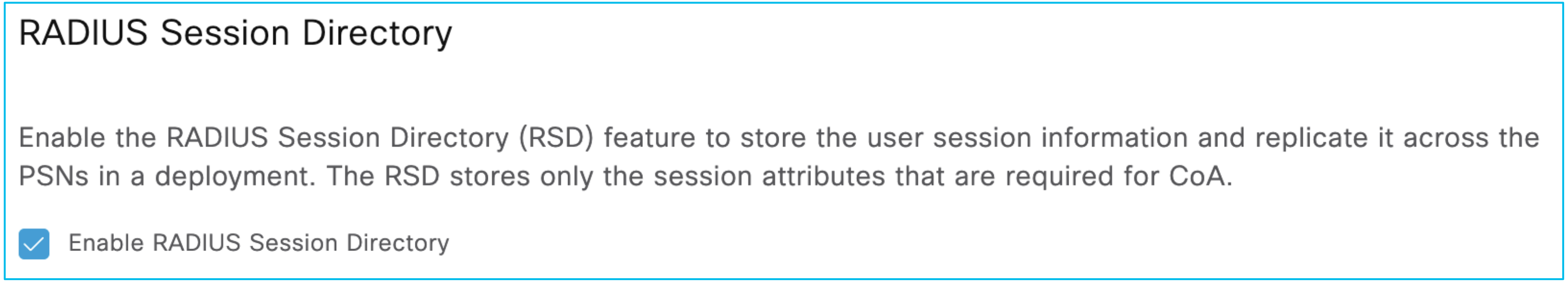


Portal Settings

HTTPS port: * 8443 (8000 - 8999)

# RADIUS Session Directory

- Solves client contacting MnT for Sessions started on another PSN
- Protects MnT from unnecessary lookups
- Administration -> System -> Settings -> Light Data Distribution



RADIUS Session Directory

Enable the RADIUS Session Directory (RSD) feature to store the user session information and replicate it across the PSNs in a deployment. The RSD stores only the session attributes that are required for CoA.

☑ Enable RADIUS Session Directory

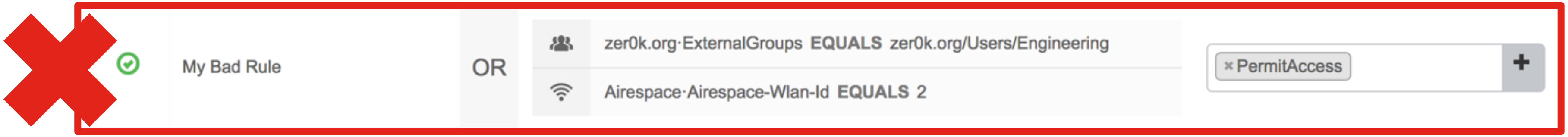
# External Databases

# 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



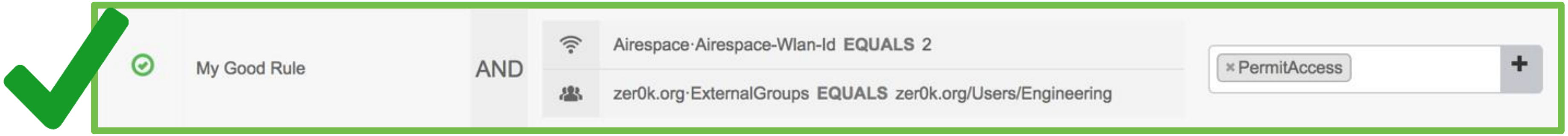
My Bad Rule

OR

zer0k.org·ExternalGroups **EQUALS** zer0k.org/Users/Engineering

Airespace·Airespace-Wlan-Id **EQUALS** 2

× PermitAccess



My Good Rule

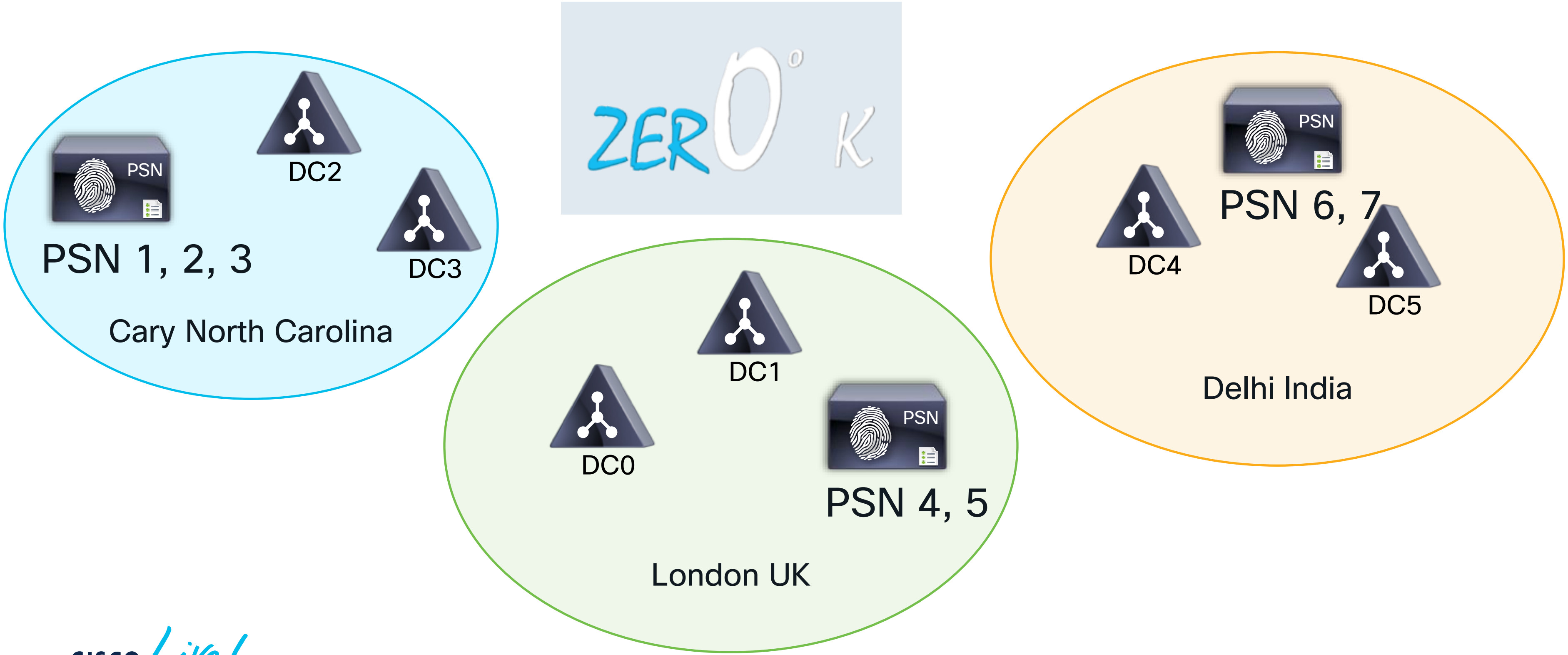
AND

Airespace·Airespace-Wlan-Id **EQUALS** 2

zer0k.org·ExternalGroups **EQUALS** zer0k.org/Users/Engineering

× PermitAccess

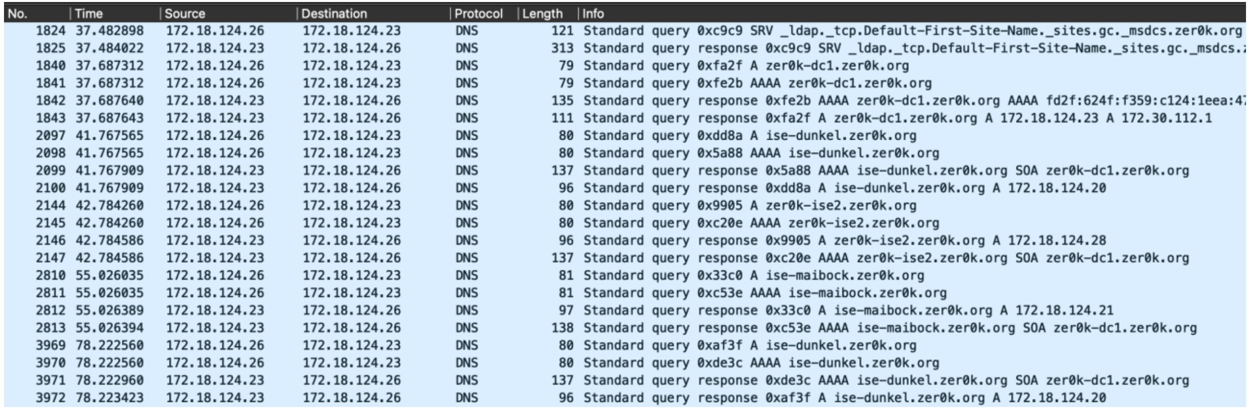
# MS AD Sites and Services



# DNS Caching

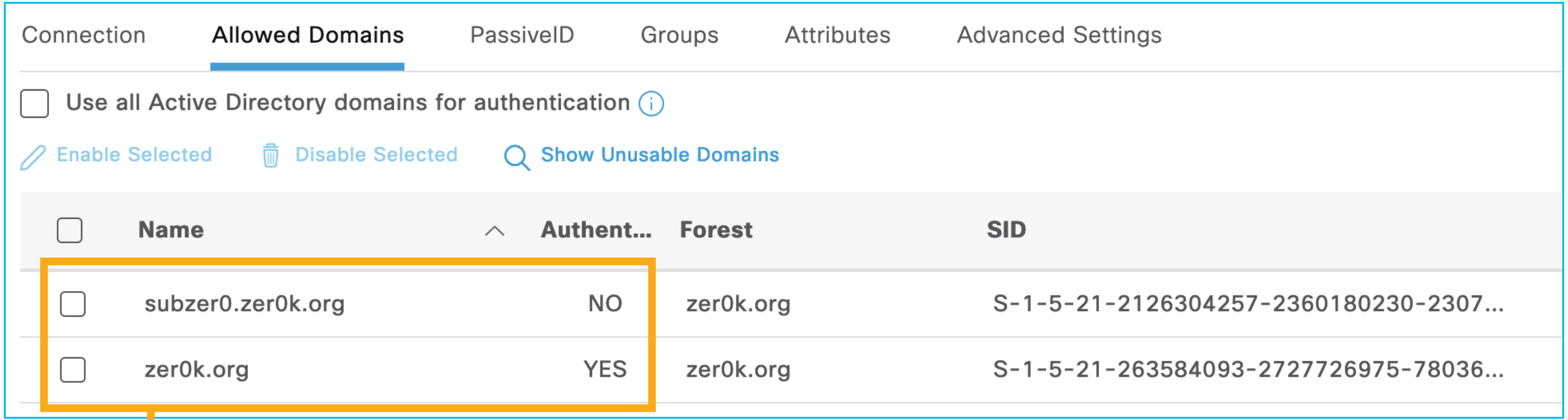
- Active Directory is DNS Heavy!
- Enabled by default starting with ISE 3.3

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.
  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



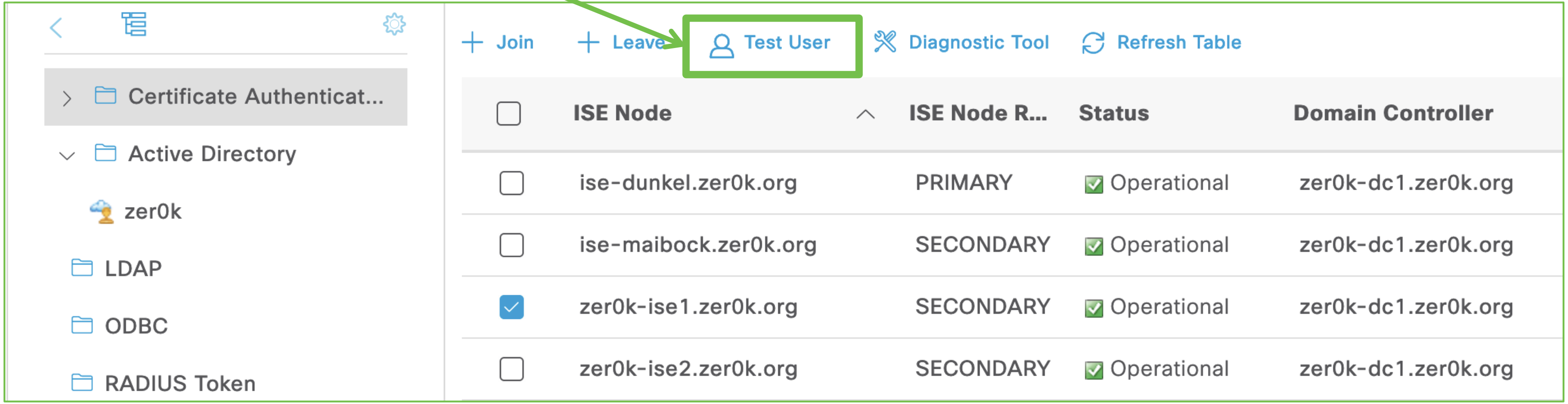
□ Use all Active Directory domains for authentication ⓘ

| □ | Name | Authent... | Forest | SID |
|---|---|---|---|---|
| □ | subzer0.zer0k.org | NO | zer0k.org | S-1-5-21-2126304257-2360180230-2307... |
| □ | zer0k.org | YES | zer0k.org | S-1-5-21-263584093-2727726975-78036... |

- 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.

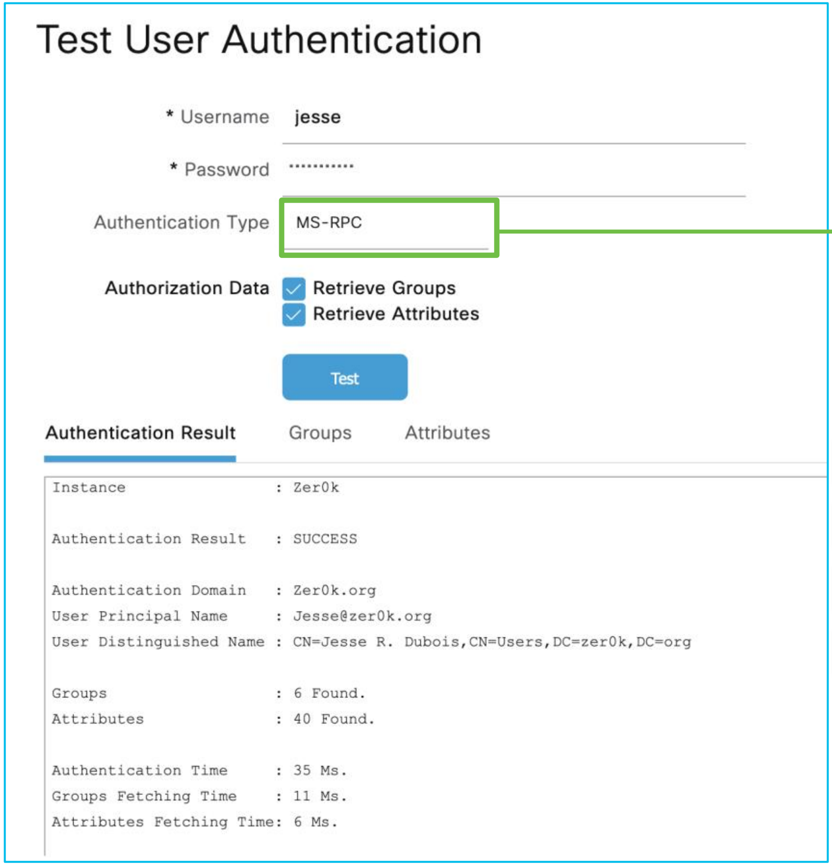
# AD Test Authentication

Can run from AD Join Point



| | ISE Node | ISE Node R... | Status | Domain Controller |
|---|---|---|---|---|
| □ | ise-dunkel.zer0k.org | PRIMARY | ☑ Operational | zer0k-dc1.zer0k.org |
| □ | ise-maibock.zer0k.org | SECONDARY | ☑ Operational | zer0k-dc1.zer0k.org |
| ☑ | zer0k-ise1.zer0k.org | SECONDARY | ☑ Operational | zer0k-dc1.zer0k.org |
| □ | zer0k-ise2.zer0k.org | SECONDARY | ☑ Operational | zer0k-dc1.zer0k.org |

# AD Test Authentication



## Test User Authentication

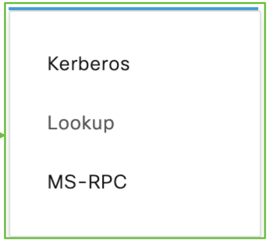
* Username: jesse

* Password: ············

Authentication Type: MS-RPC

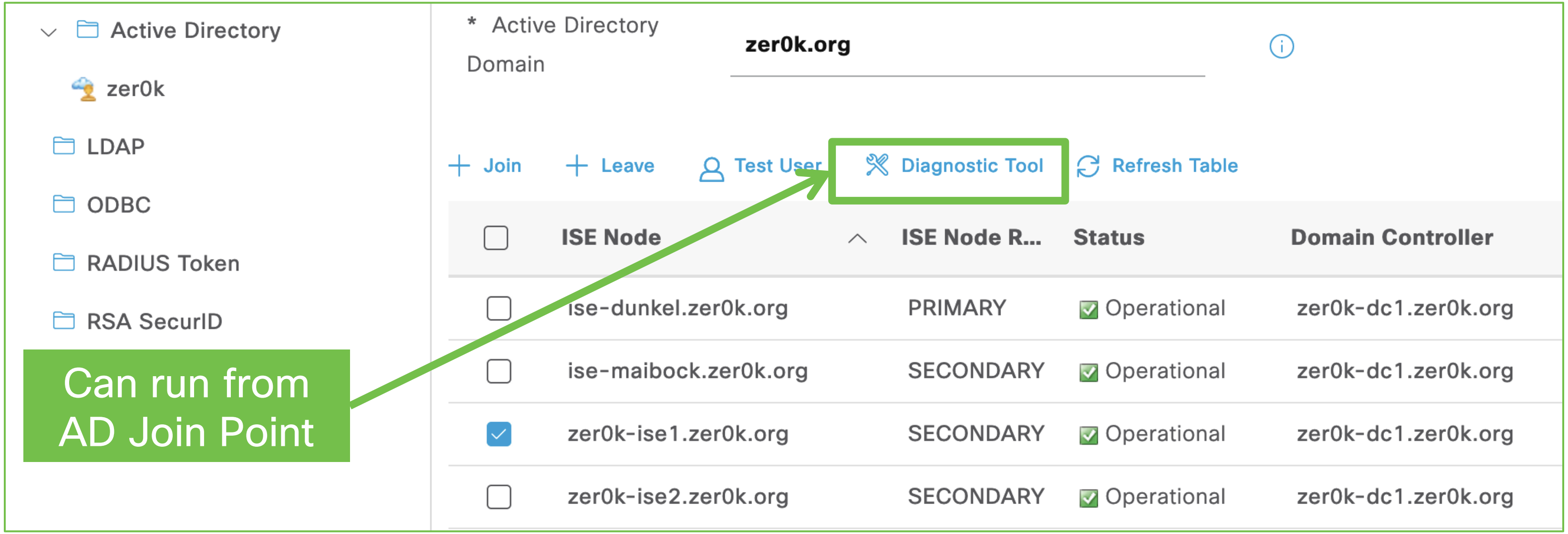
Authorization Data: ☑ Retrieve Groups ☑ Retrieve Attributes

```
Instance                 : Zer0k

Authentication Result    : SUCCESS

Authentication Domain    : Zer0k.org
User Principal Name      : Jesse@zer0k.org
User Distinguished Name : CN=Jesse R. Dubois,CN=Users,DC=zer0k,DC=org

Groups                   : 6 Found.
Attributes               : 40 Found.

Authentication Time      : 35 Ms.
Groups Fetching Time     : 11 Ms.
Attributes Fetching Time: 6 Ms.
```



- 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

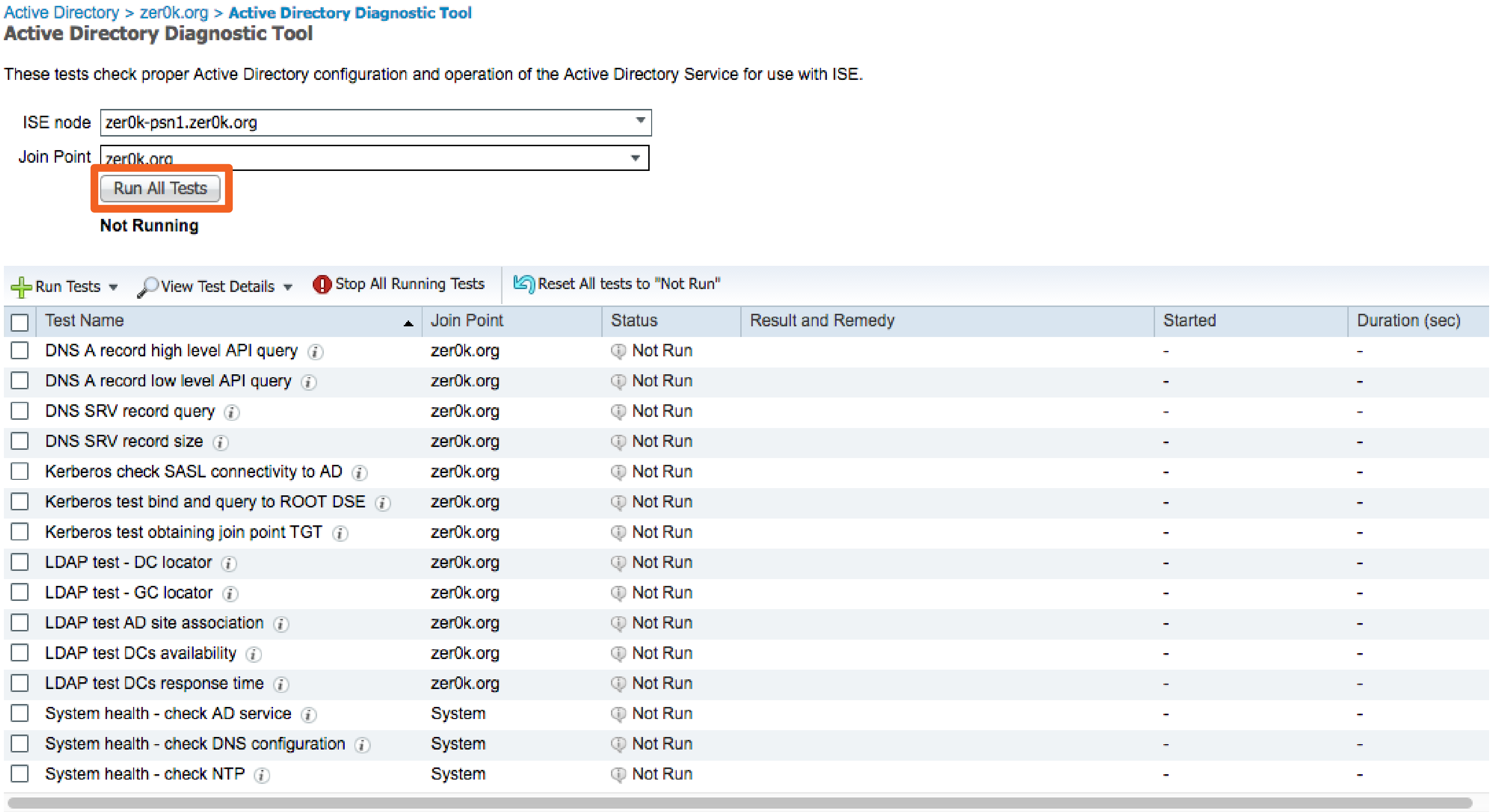


* Active Directory Domain: zer0k.org

| ☐ | ISE Node | ISE Node R... | Status | Domain Controller |
|---|---|---|---|---|
| ☐ | ise-dunkel.zer0k.org | PRIMARY | ✓ Operational | zer0k-dc1.zer0k.org |
| ☐ | ise-maibock.zer0k.org | SECONDARY | ✓ Operational | zer0k-dc1.zer0k.org |
| ☑ | zer0k-ise1.zer0k.org | SECONDARY | ✓ Operational | zer0k-dc1.zer0k.org |
| ☐ | zer0k-ise2.zer0k.org | SECONDARY | ✓ Operational | zer0k-dc1.zer0k.org |

Can run from AD Join Point

# Domain Diagnostics



Active Directory > zer0k.org > **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.

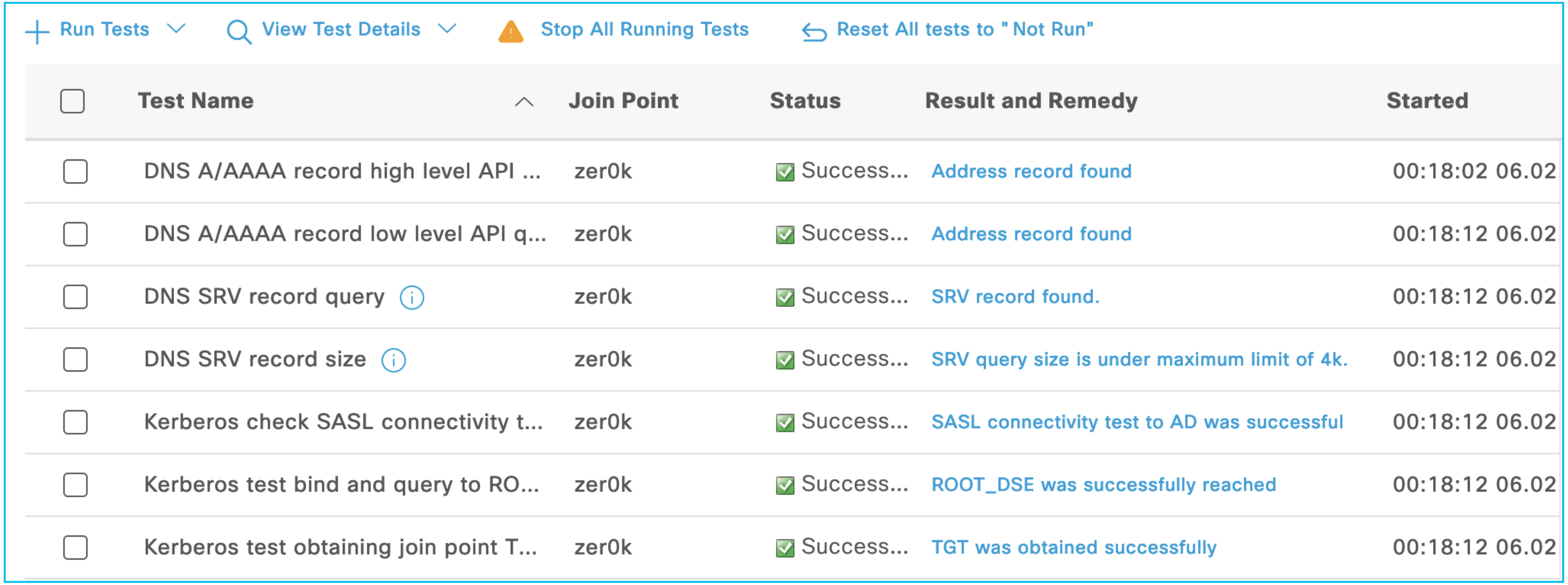
ISE node: zer0k-psn1.zer0k.org

Join Point: zer0k.org

**Not Running**

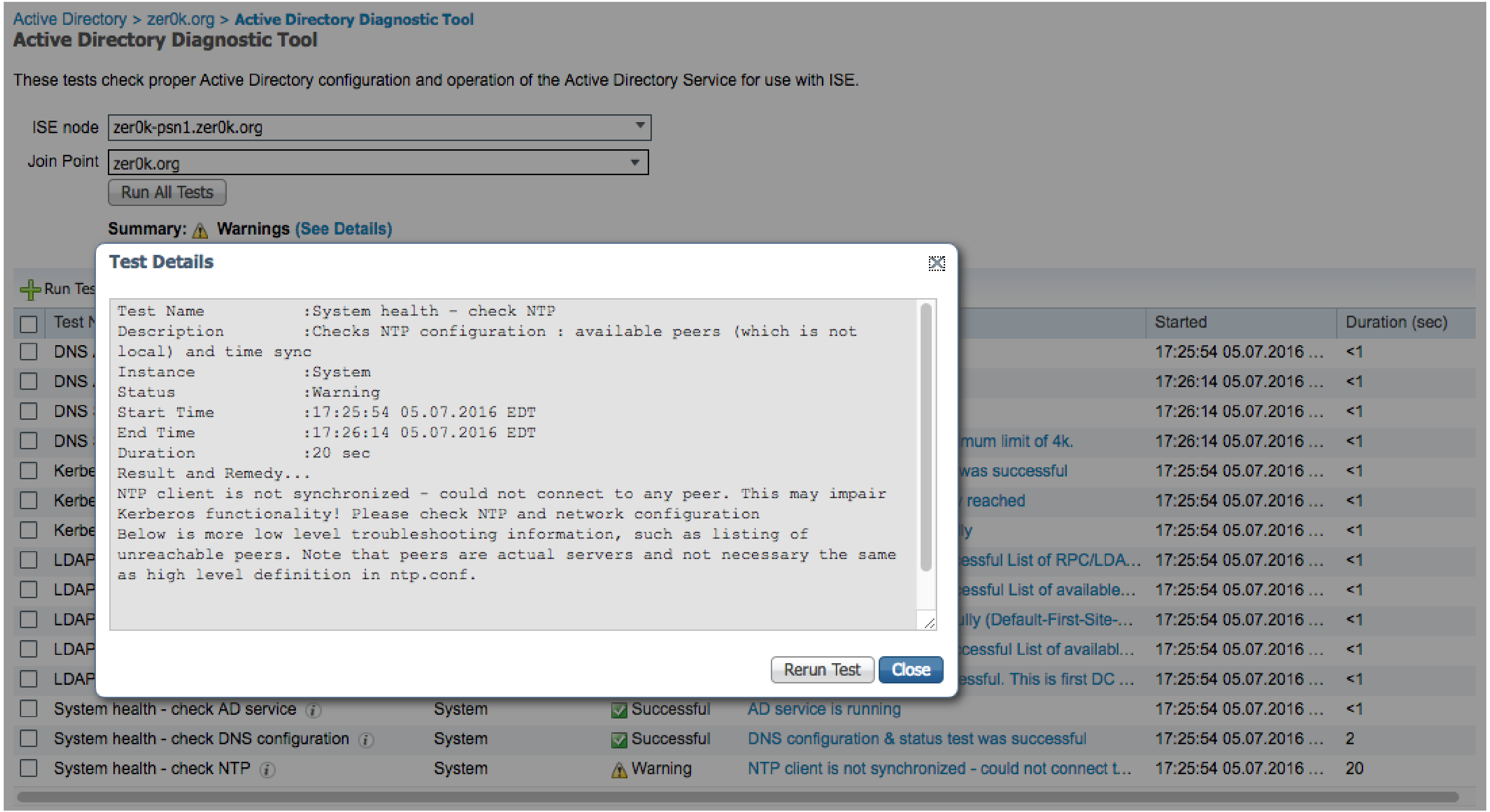
| □ | Test Name | Join Point | Status | Result and Remedy | Started | Duration (sec) |
|---|---|---|---|---|---|---|
| □ | DNS A record high level API query | zer0k.org | Not Run | | - | - |
| □ | DNS A record low level API query | zer0k.org | Not Run | | - | - |
| □ | DNS SRV record query | zer0k.org | Not Run | | - | - |
| □ | DNS SRV record size | zer0k.org | Not Run | | - | - |
| □ | Kerberos check SASL connectivity to AD | zer0k.org | Not Run | | - | - |
| □ | Kerberos test bind and query to ROOT DSE | zer0k.org | Not Run | | - | - |
| □ | Kerberos test obtaining join point TGT | zer0k.org | Not Run | | - | - |
| □ | LDAP test - DC locator | zer0k.org | Not Run | | - | - |
| □ | LDAP test - GC locator | zer0k.org | Not Run | | - | - |
| □ | LDAP test AD site association | zer0k.org | Not Run | | - | - |
| □ | LDAP test DCs availability | zer0k.org | Not Run | | - | - |
| □ | LDAP test DCs response time | zer0k.org | Not Run | | - | - |
| □ | System health - check AD service | System | Not Run | | - | - |
| □ | System health - check DNS configuration | System | Not Run | | - | - |
| □ | System health - check NTP | System | Not Run | | - | - |

# Domain Diagnostics



| □ | Test Name | Join Point | Status | Result and Remedy | Started |
|---|---|---|---|---|---|
| □ | DNS A/AAAA record high level API ... | zer0k | ☑ Success... | Address record found | 00:18:02 06.02 |
| □ | DNS A/AAAA record low level API q... | zer0k | ☑ Success... | Address record found | 00:18:12 06.02 |
| □ | DNS SRV record query ⓘ | zer0k | ☑ Success... | SRV record found. | 00:18:12 06.02 |
| □ | DNS SRV record size ⓘ | zer0k | ☑ Success... | SRV query size is under maximum limit of 4k. | 00:18:12 06.02 |
| □ | Kerberos check SASL connectivity t... | zer0k | ☑ Success... | SASL connectivity test to AD was successful | 00:18:12 06.02 |
| □ | Kerberos test bind and query to RO... | zer0k | ☑ Success... | ROOT_DSE was successfully reached | 00:18:12 06.02 |
| □ | Kerberos test obtaining join point T... | zer0k | ☑ Success... | TGT was obtained successfully | 00:18:12 06.02 |

# Domain Diagnostics



Active Directory > zer0k.org > 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: zer0k-psn1.zer0k.org

Join Point: zer0k.org

**Summary:** ⚠ **Warnings (See Details)**

**Test Details**

```
Test Name           :System health - check NTP
Description         :Checks NTP configuration : available peers (which is not
local) and time sync
Instance            :System
Status              :Warning
Start Time          :17:25:54 05.07.2016 EDT
End Time            :17:26:14 05.07.2016 EDT
Duration            :20 sec
Result and Remedy...
NTP client is not synchronized - could not connect to any peer. This may impair
Kerberos functionality! Please check NTP and network configuration
Below is more low level troubleshooting information, such as listing of
unreachable peers. Note that peers are actual servers and not necessary the same
as high level definition in ntp.conf.
```

| □ | Test N | | | | Started | Duration (sec) |
|---|---|---|---|---|---|---|
| □ | DNS . | | | | 17:25:54 05.07.2016 ... | <1 |
| □ | DNS . | | | | 17:26:14 05.07.2016 ... | <1 |
| □ | DNS : | | | | 17:26:14 05.07.2016 ... | <1 |
| □ | DNS : | | | mum limit of 4k. | 17:26:14 05.07.2016 ... | <1 |
| □ | Kerbe | | | was successful | 17:25:54 05.07.2016 ... | <1 |
| □ | Kerbe | | | reached | 17:25:54 05.07.2016 ... | <1 |
| □ | Kerbe | | | lly | 17:25:54 05.07.2016 ... | <1 |
| □ | LDAP | | | essful List of RPC/LDA... | 17:25:54 05.07.2016 ... | <1 |
| □ | LDAP | | | essful List of available... | 17:25:54 05.07.2016 ... | <1 |
| □ | LDAP | | | lly (Default-First-Site-... | 17:25:54 05.07.2016 ... | <1 |
| □ | LDAP | | | cessful List of availabl... | 17:25:54 05.07.2016 ... | <1 |
| □ | LDAP | | | essful. This is first DC ... | 17:25:54 05.07.2016 ... | <1 |
| □ | System health - check AD service ⓘ | System | ✓ Successful | AD service is running | 17:25:54 05.07.2016 ... | <1 |
| □ | System health - check DNS configuration ⓘ | System | ✓ Successful | DNS configuration & status test was successful | 17:25:54 05.07.2016 ... | 2 |
| □ | System health - check NTP ⓘ | System | ⚠ Warning | NTP client is not synchronized - could not connect t... | 17:25:54 05.07.2016 ... | 20 |

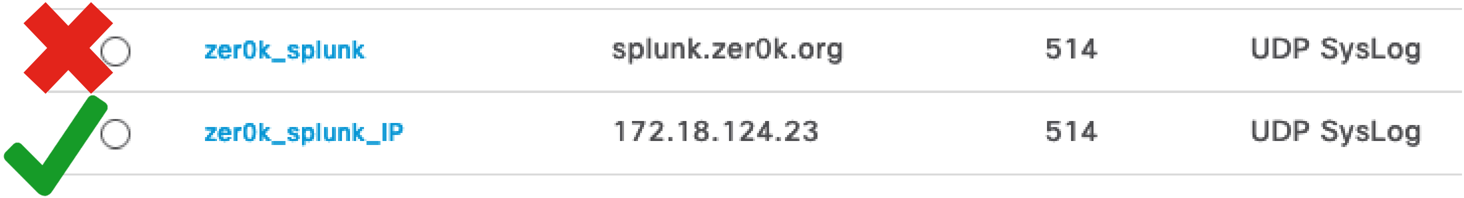
# Active Directory Best Practices

- 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

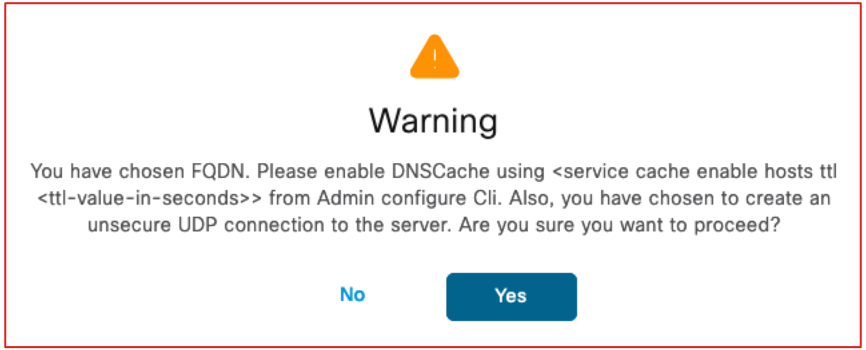


| | | | | |
|---|---|---|---|---|
| ✗ ○ | zer0k_splunk | splunk.zer0k.org | 514 | UDP SysLog |
| ✓ ○ | zer0k_splunk_IP | 172.18.124.23 | 514 | UDP SysLog |

# 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*

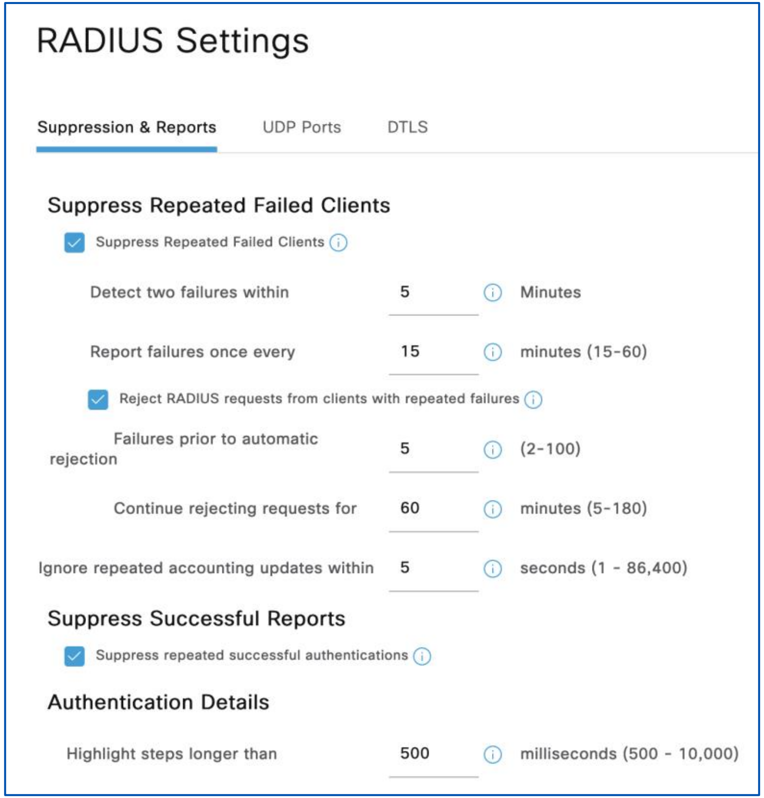


Warning

You have chosen FQDN. Please enable DNSCache using <service cache enable hosts ttl <ttl-value-in-seconds>> from Admin configure Cli. Also, you have chosen to create an unsecure UDP connection to the server. Are you sure you want to proceed?

# Logging Suppression

## Administration -> Settings -> Protocols -> RADIUS



### RADIUS Settings

#### Suppress Repeated Failed Clients

☑ Suppress Repeated Failed Clients ⓘ

| | | | |
|---|---|---|---|
| Detect two failures within | 5 | ⓘ | Minutes |
| Report failures once every | 15 | ⓘ | minutes (15-60) |

☑ Reject RADIUS requests from clients with repeated failures ⓘ

| | | | |
|---|---|---|---|
| Failures prior to automatic rejection | 5 | ⓘ | (2-100) |
| Continue rejecting requests for | 60 | ⓘ | minutes (5-180) |
| Ignore repeated accounting updates within | 5 | ⓘ | seconds (1 - 86,400) |

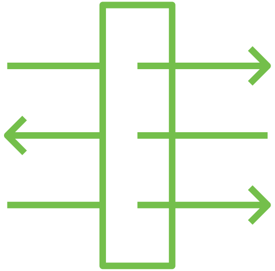
#### Suppress Successful Reports

☑ Suppress repeated successful authentications ⓘ

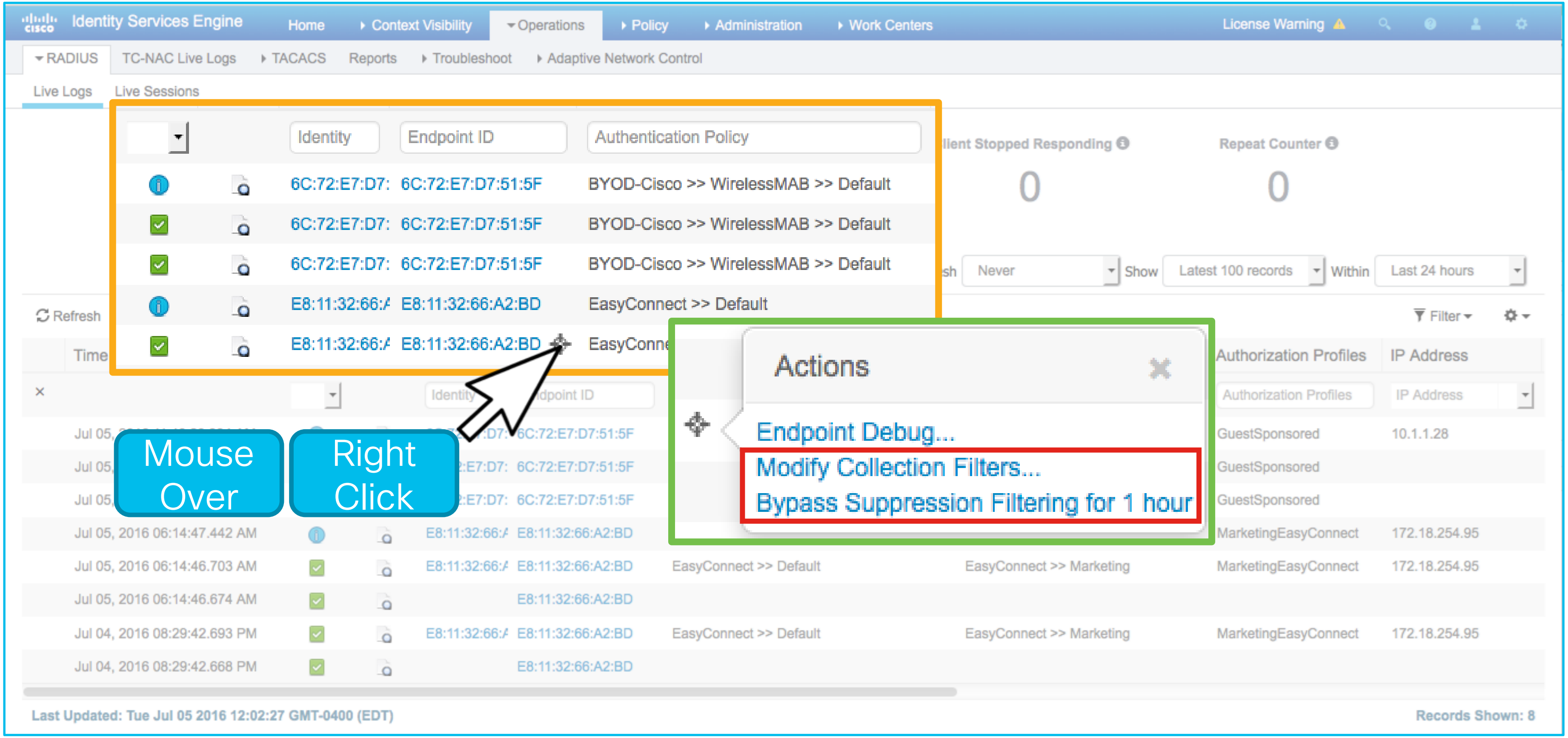
#### Authentication Details

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

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



# Per-Endpoint Suppression Bypass



| | | Identity | Endpoint ID | Authentication Policy |
|---|---|---|---|---|
| ⓘ | | 6C:72:E7:D7: | 6C:72:E7:D7:51:5F | BYOD-Cisco >> WirelessMAB >> Default |
| ✓ | | 6C:72:E7:D7: | 6C:72:E7:D7:51:5F | BYOD-Cisco >> WirelessMAB >> Default |
| ✓ | | 6C:72:E7:D7: | 6C:72:E7:D7:51:5F | BYOD-Cisco >> WirelessMAB >> Default |
| ⓘ | | E8:11:32:66:/ | E8:11:32:66:A2:BD | EasyConnect >> Default |
| ✓ | | E8:11:32:66:/ | E8:11:32:66:A2:BD | EasyConne |

Client Stopped Responding: 0

Repeat Counter: 0

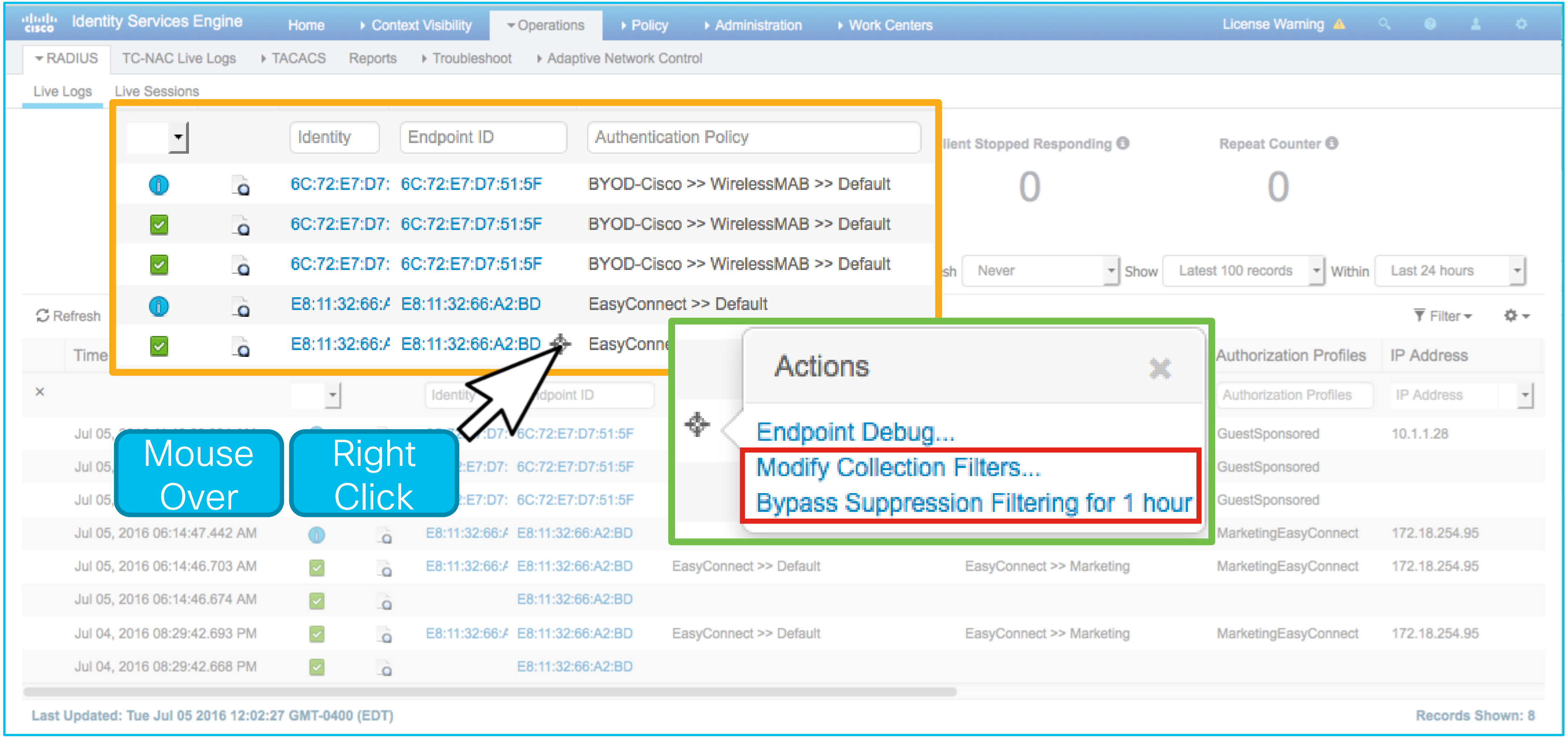
Actions
- Endpoint Debug...
- Modify Collection Filters...
- Bypass Suppression Filtering for 1 hour

| Time | | | Identity | Endpoint ID | | | Authorization Profiles | IP Address |
|---|---|---|---|---|---|---|---|---|
| Jul 05, | | | | 6C:72:E7:D7:51:5F | | | GuestSponsored | 10.1.1.28 |
| Jul 05, | | | :E7:D7: | 6C:72:E7:D7:51:5F | | | GuestSponsored | |
| Jul 05, | | | :E7:D7: | 6C:72:E7:D7:51:5F | | | GuestSponsored | |
| Jul 05, 2016 06:14:47.442 AM | ⓘ | | E8:11:32:66:/ | E8:11:32:66:A2:BD | | | MarketingEasyConnect | 172.18.254.95 |
| Jul 05, 2016 06:14:46.703 AM | ✓ | | E8:11:32:66:/ | E8:11:32:66:A2:BD | EasyConnect >> Default | EasyConnect >> Marketing | MarketingEasyConnect | 172.18.254.95 |
| Jul 05, 2016 06:14:46.674 AM | ✓ | | | E8:11:32:66:A2:BD | | | | |
| Jul 04, 2016 08:29:42.693 PM | ✓ | | E8:11:32:66:/ | E8:11:32:66:A2:BD | EasyConnect >> Default | EasyConnect >> Marketing | MarketingEasyConnect | 172.18.254.95 |
| Jul 04, 2016 08:29:42.668 PM | ✓ | | | E8:11:32:66:A2:BD | | | | |

Last Updated: Tue Jul 05 2016 12:02:27 GMT-0400 (EDT)

Records Shown: 8

# Per-Endpoint Suppression Bypass



| | | Identity | Endpoint ID | Authentication Policy |
|---|---|---|---|---|
| ⓘ | | 6C:72:E7:D7: | 6C:72:E7:D7:51:5F | BYOD-Cisco >> WirelessMAB >> Default |
| ✓ | | 6C:72:E7:D7: | 6C:72:E7:D7:51:5F | BYOD-Cisco >> WirelessMAB >> Default |
| ✓ | | 6C:72:E7:D7: | 6C:72:E7:D7:51:5F | BYOD-Cisco >> WirelessMAB >> Default |
| ⓘ | | E8:11:32:66:/ | E8:11:32:66:A2:BD | EasyConnect >> Default |
| ✓ | | E8:11:32:66:/ | E8:11:32:66:A2:BD | EasyConne |

lient Stopped Responding: 0

Repeat Counter: 0

sh: Never | Show: Latest 100 records | Within: Last 24 hours

**Actions**

- Endpoint Debug...
- Modify Collection Filters...
- Bypass Suppression Filtering for 1 hour

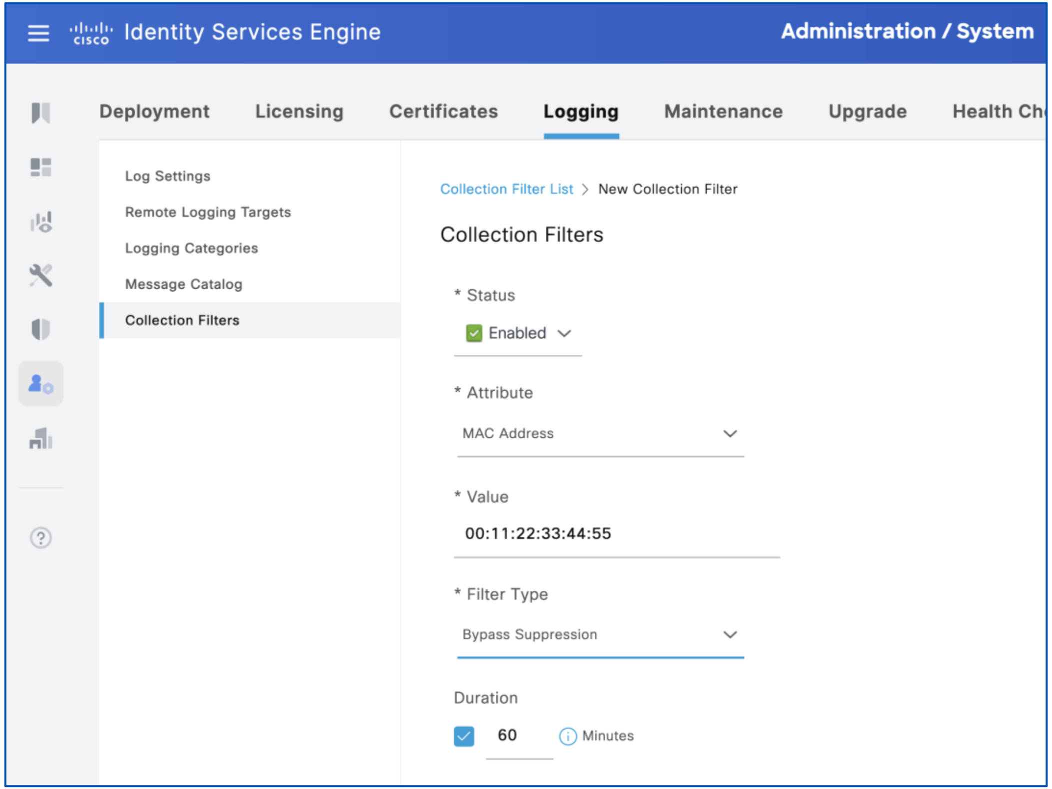
| Time | | | Identity | Endpoint ID | Authentication Policy | Authorization Policy | Authorization Profiles | IP Address |
|---|---|---|---|---|---|---|---|---|
| Jul 05, | | | :D7: | 6C:72:E7:D7:51:5F | | | GuestSponsored | 10.1.1.28 |
| Jul 05, | | | :E7:D7: | 6C:72:E7:D7:51:5F | | | GuestSponsored | |
| Jul 05, | | | :E7:D7: | 6C:72:E7:D7:51:5F | | | GuestSponsored | |
| Jul 05, 2016 06:14:47.442 AM | ⓘ | | E8:11:32:66:/ | E8:11:32:66:A2:BD | | | MarketingEasyConnect | 172.18.254.95 |
| Jul 05, 2016 06:14:46.703 AM | ✓ | | E8:11:32:66:/ | E8:11:32:66:A2:BD | EasyConnect >> Default | EasyConnect >> Marketing | MarketingEasyConnect | 172.18.254.95 |
| Jul 05, 2016 06:14:46.674 AM | ✓ | | | E8:11:32:66:A2:BD | | | | |
| Jul 04, 2016 08:29:42.693 PM | ✓ | | E8:11:32:66:/ | E8:11:32:66:A2:BD | EasyConnect >> Default | EasyConnect >> Marketing | MarketingEasyConnect | 172.18.254.95 |
| Jul 04, 2016 08:29:42.668 PM | ✓ | | | E8:11:32:66:A2:BD | | | | |

Last Updated: Tue Jul 05 2016 12:02:27 GMT-0400 (EDT)

Records Shown: 8

# Manual Collection Filters

## Administration -> Logging -> Collection Filters



Collection Filters

* Status: ☑ Enabled

* Attribute: MAC Address

* Value: 00:11:22:33:44:55

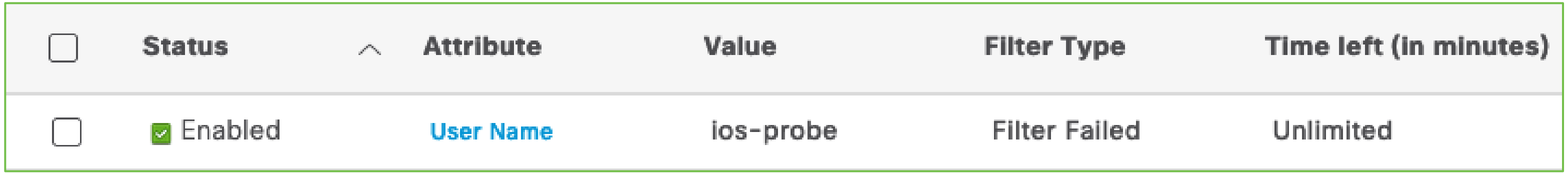
* Filter Type: Bypass Suppression

Duration: ☑ 60 Minutes

# 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

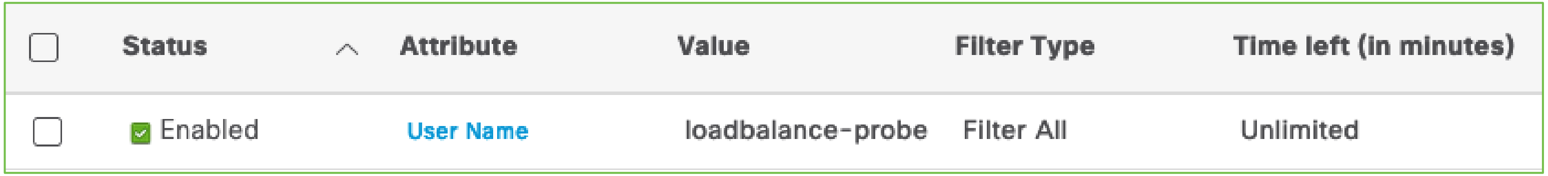


| □ | Status | Attribute | Value | Filter Type | Time left (in minutes) |
|---|---|---|---|---|---|
| □ | ☑ Enabled | User Name | ios-probe | Filter Failed | Unlimited |

# Keepalive Probes

## Passed Required

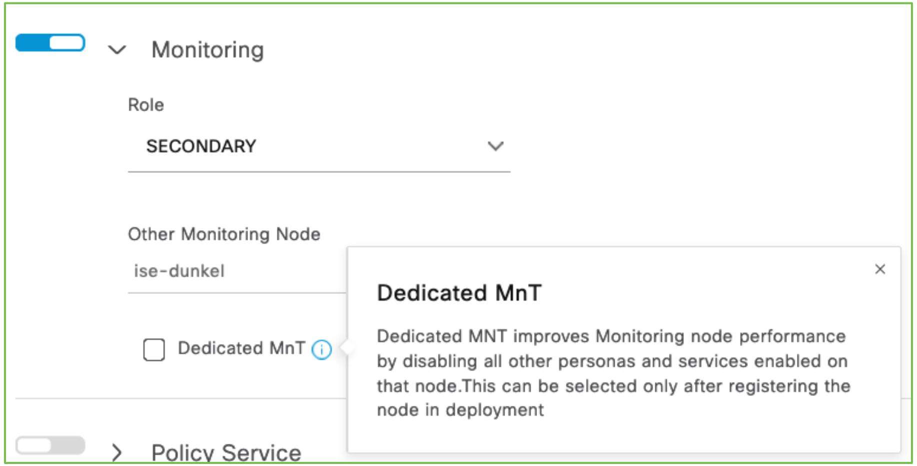
- If probe authentication must Pass
  - Use Local User
  - Prevents External Database slowness from impacting performance
- Filter Passed and Failed by Username



| ☐ | 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



Role

SECONDARY

Other Monitoring Node

ise-dunkel

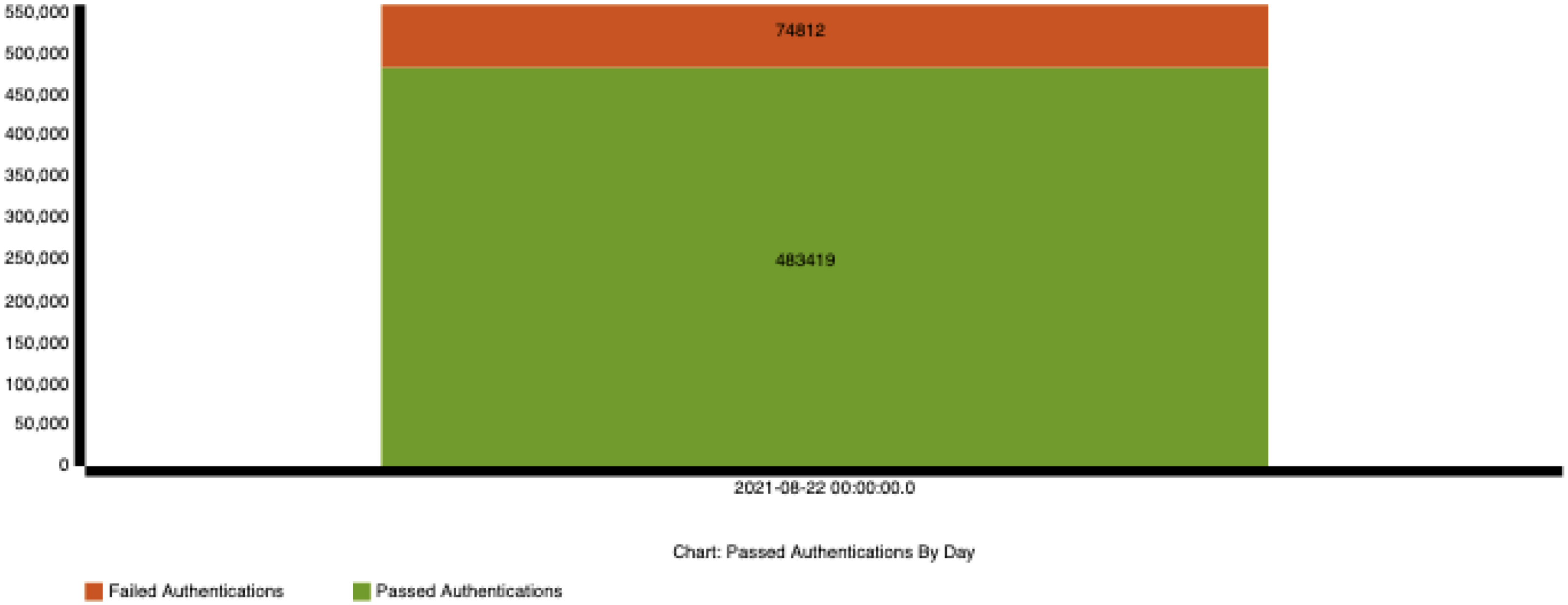
□ Dedicated MnT

**Dedicated MnT**

Dedicated MNT improves Monitoring node performance by disabling all other personas and services enabled on that node.This can be selected only after registering the node in deployment

# 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

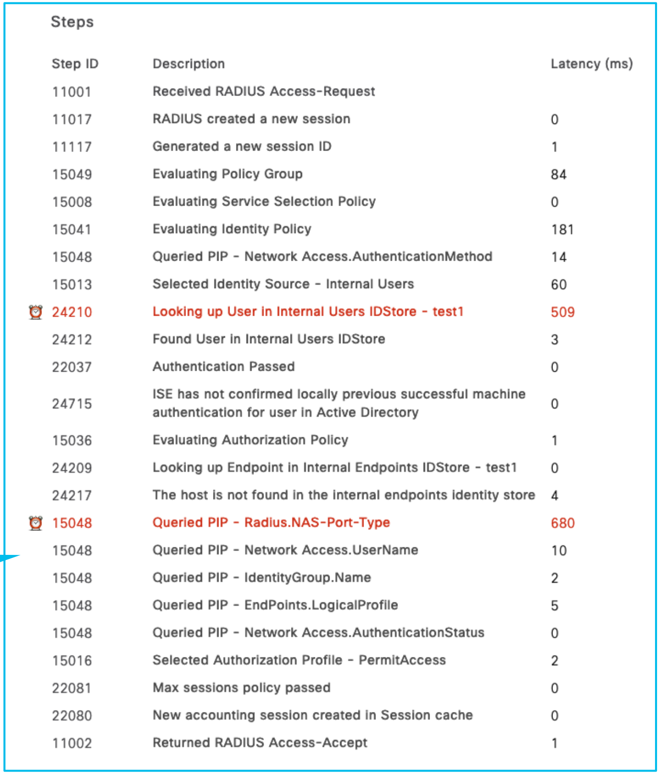
## Authentications By ISE Server

| 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

New in 3.3!

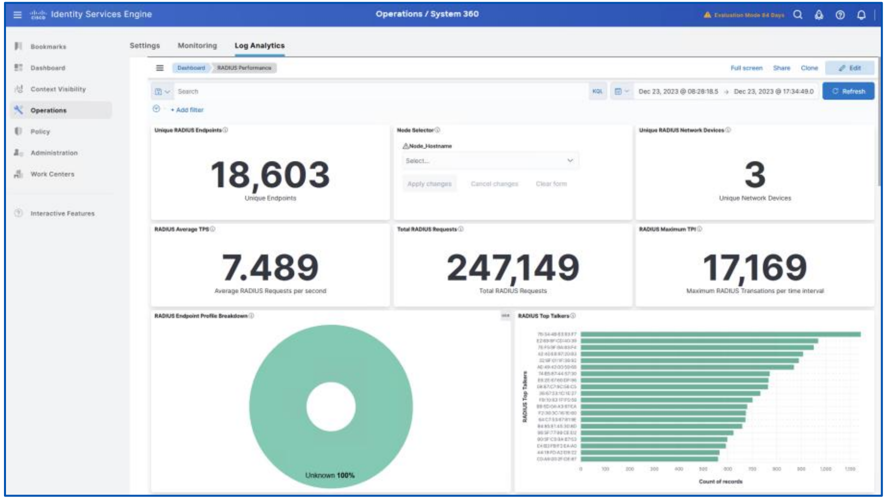


Steps

| 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

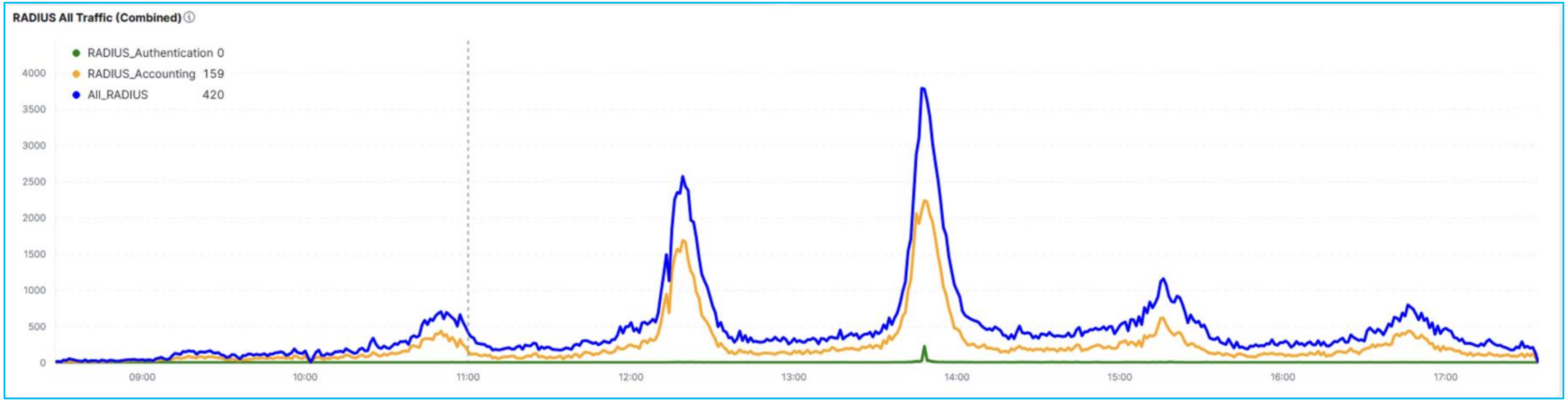


Understanding your ISE deployment with C.L.A.R.K. (Cisco Log Analysis & Remediation Kiosk)
BRKSEC-2897
CLUS 2023

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

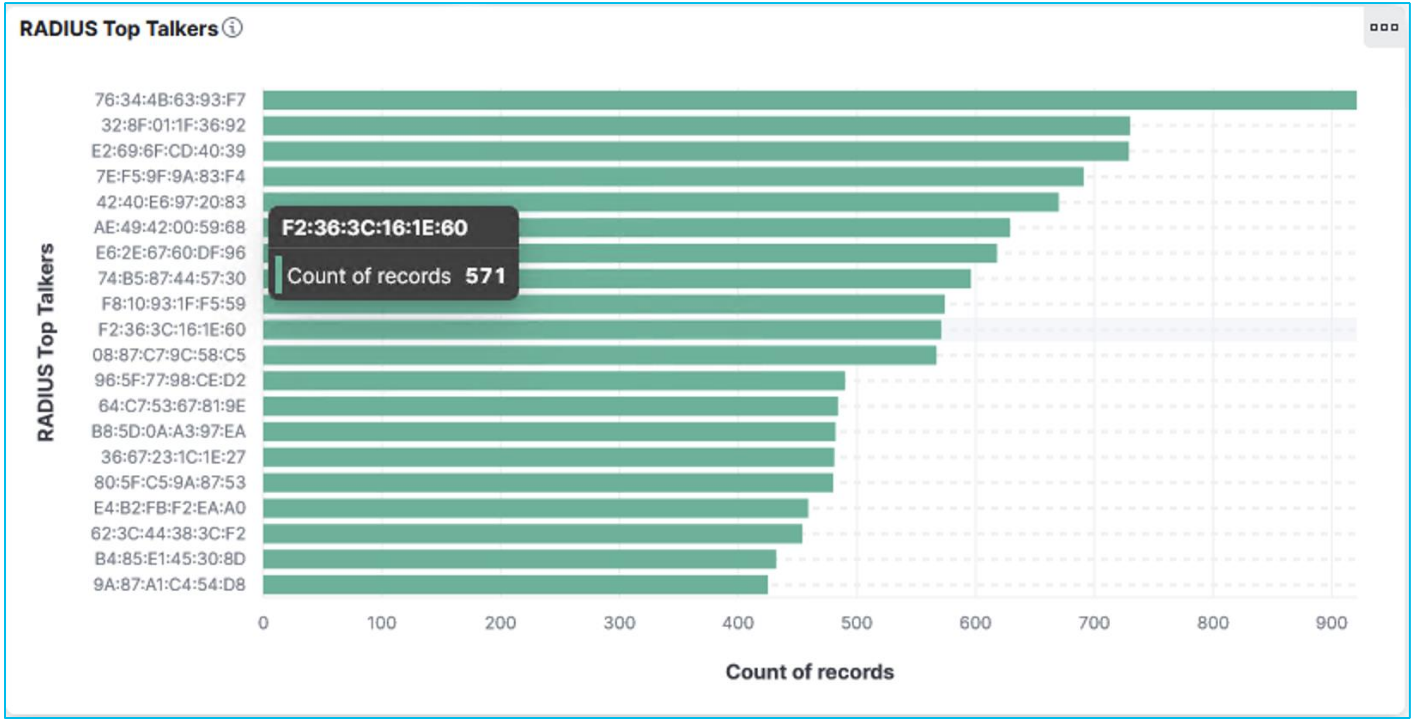
# Log Analytics

## TPS / Auth to Accounting Ratio



# Log Analytics

## Top Talkers

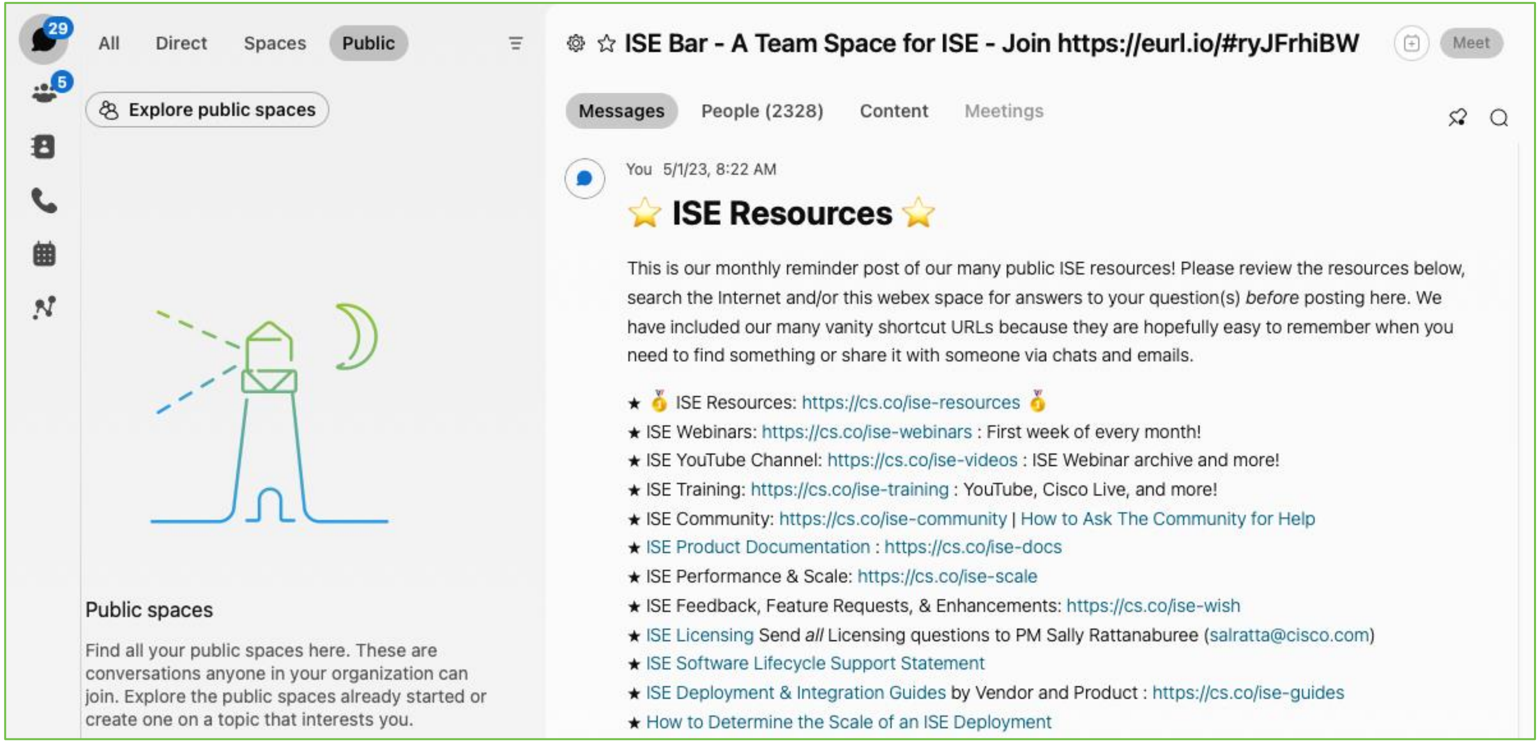


# Key Takeaways

- 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



ISE Bar - A Team Space for ISE - Join https://eurl.io/#ryJFrhiBW

Public spaces

Find all your public spaces here. These are conversations anyone in your organization can join. Explore the public spaces already started or create one on a topic that interests you.

You 5/1/23, 8:22 AM

## ⭐ ISE Resources ⭐

This is our monthly reminder post of our many public ISE resources! Please review the resources below, search the Internet and/or this webex space for answers to your question(s) *before* posting here. We have included our many vanity shortcut URLs because they are hopefully easy to remember when you need to find something or share it with someone via chats and emails.

★ 🥇 ISE Resources: https://cs.co/ise-resources 🥇
★ ISE Webinars: https://cs.co/ise-webinars : First week of every month!
★ ISE YouTube Channel: https://cs.co/ise-videos : ISE Webinar archive and more!
★ ISE Training: https://cs.co/ise-training : YouTube, Cisco Live, and more!
★ ISE Community: https://cs.co/ise-community | How to Ask The Community for Help
★ ISE Product Documentation : https://cs.co/ise-docs
★ ISE Performance & Scale: https://cs.co/ise-scale
★ ISE Feedback, Feature Requests, & Enhancements: https://cs.co/ise-wish
★ ISE Licensing Send *all* Licensing questions to PM Sally Rattanaburee (salratta@cisco.com)
★ ISE Software Lifecycle Support Statement
★ ISE Deployment & Integration Guides by Vendor and Product : https://cs.co/ise-guides
★ How to Determine the Scale of an ISE Deployment

The bridge to possible

# Thank you

cisco *Live!*

Let’s go