ISE Profiling Architecture and Best Practices



Alex Bubnov
TAC Security Technical Leader

BRKSEC-3519

Session Objective

- Make you familiar with the Profiler architecture on ISE, consider endpoint attribute replication scenarios in distributed deployments, dependency on other services and performance impact
- Share tips from TAC/Escalation to avoid commonly seen pitfalls.
- Highlight configuration best practices and limits
- Show ISE built-in diagnostics and analytics capabilities

Not in the scope:

- Profiler Probe configuration details
- MFC and AI Endpoint Analytics

© 2026 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Profiling basics

02 Profiler architecture

03 Profiler Performance

04 Additional features

05 Problem diagnostic

06 Conclusion

07 Hidden slides

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Webex App

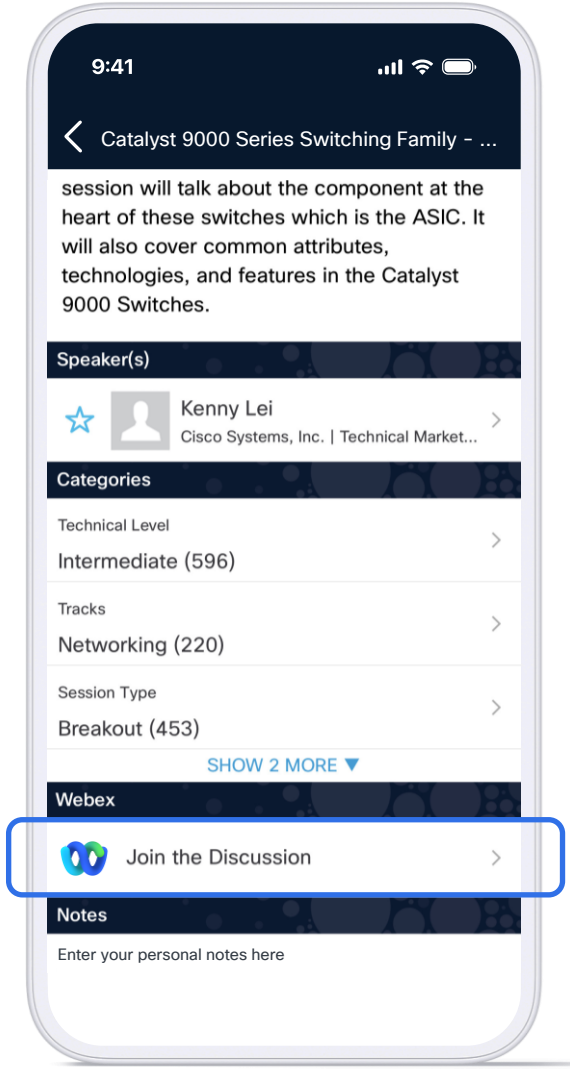
Questions?

Use Webex App to chat with the speaker after the session

How

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

Webex spaces will be moderated by the speaker until February 27, 2026.



© 2026 Cisco and/or its affiliates. All rights reserved.

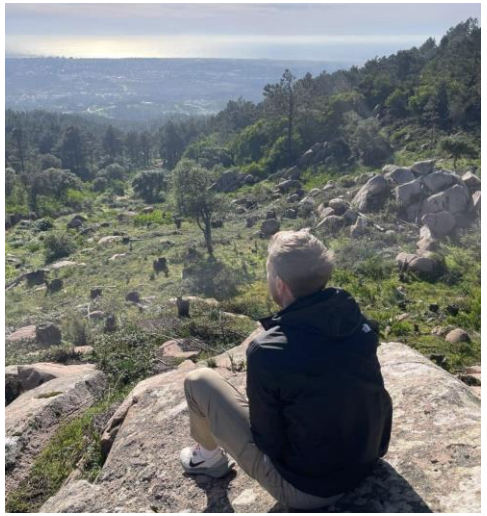
About Alex Bubnov

- Security TAC Technical Leadership Team
- 15+ years of network and security experience
- On personal note:
  - Family
  - 3x3
  - Ski
- Lives in Lisbon, Portugal
- Holds AAA pack =) :









© 2026 Cisco and/or its affiliates. All rights reserved.

Profiling Basics

Granular visibility into endpoints

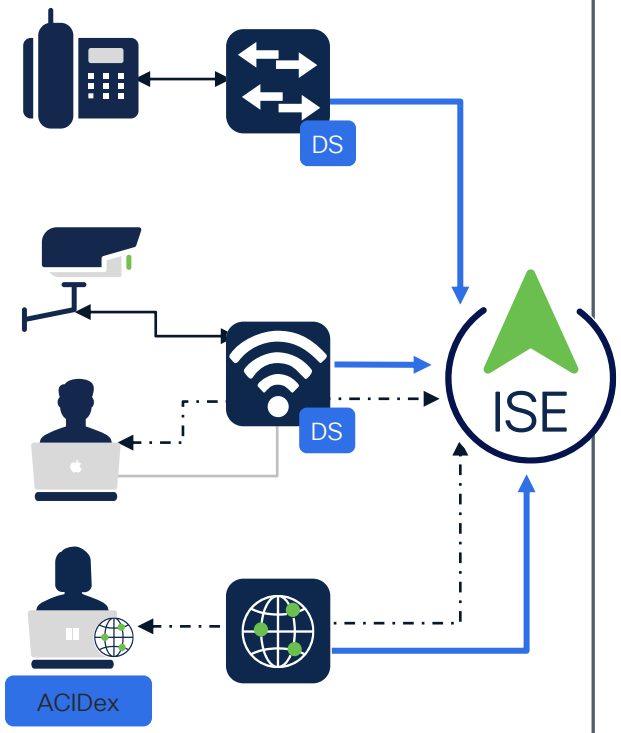


IP Address: 192.168.0.1	**Who**	Bob (Contractor)
Unknown	**What**	Apple iPad/iOS/18.6.2
10:30 AM GMT	**When**	10:30 AM GMT
Floor-1, Lisbon, Building 12	**Where**	Floor-1, Lisbon, Building 12
Wireless	**How**	Wireless
Unknown	**Apps**	Firefox, Cisco Secure Client
Unknown	**HW**	Mac M1
Access to any device/user	**Result**	Authorized network access



© 2026 Cisco and/or its affiliates. All rights reserved.

Context sources



AnyConnect Identity Extensions (ACIDex)
Device Sensor (DS)

ISE Data Collection Methods for Device Profiling:

Probes: Netflow | DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | AD | PxGrid

Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

SecureClient: ACIDex

EA: Cisco AI Endpoint Analytics

MDM: Endpoint information from MDM

API: ERS | Open-Api | Rest

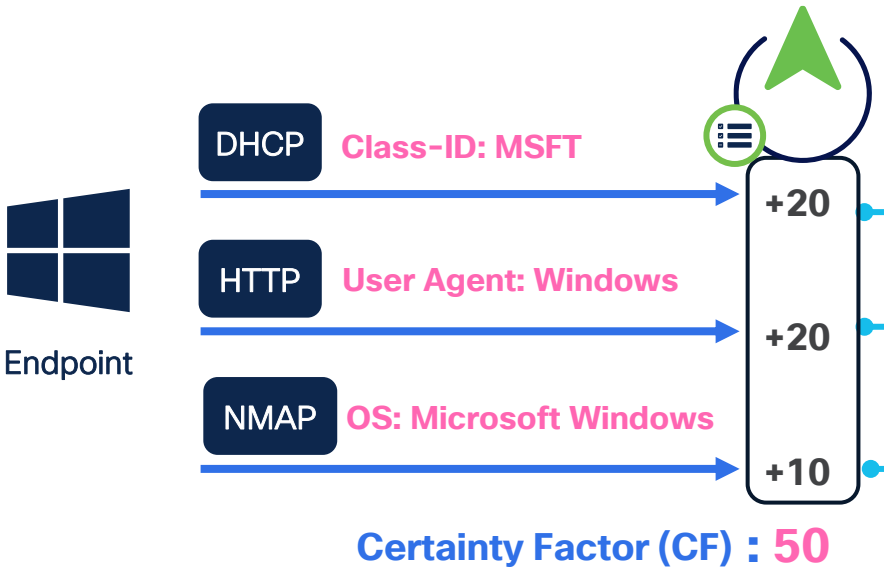
Feed: Certainty Factor service + Cloud MFC

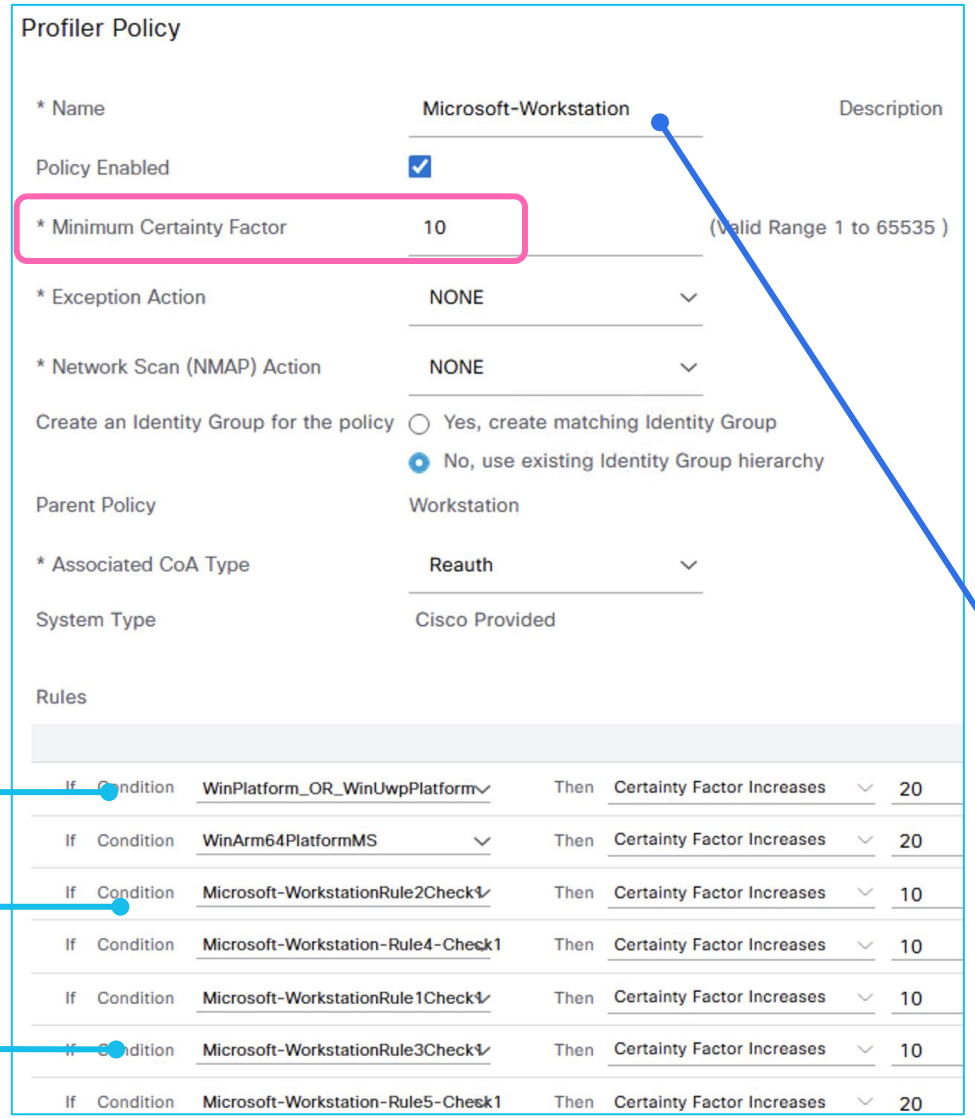
© 2026 Cisco and/or its affiliates. All rights reserved.

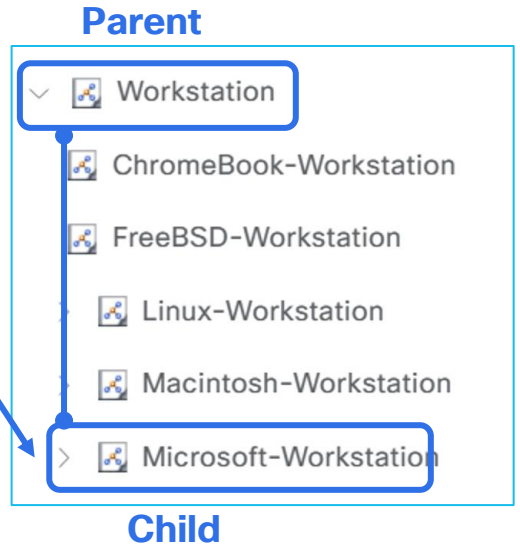
Policy based endpoint profiling

High level workflow:

- Attributes collection from endpoint
- Match the attributes to profiler conditions
- Profiler conditions are then used as rules in the Profiler Policy
- The policy with the highest **Certainty Factor** wins and is gets assigned to the endpoint

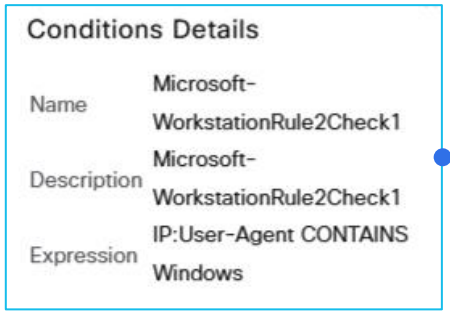


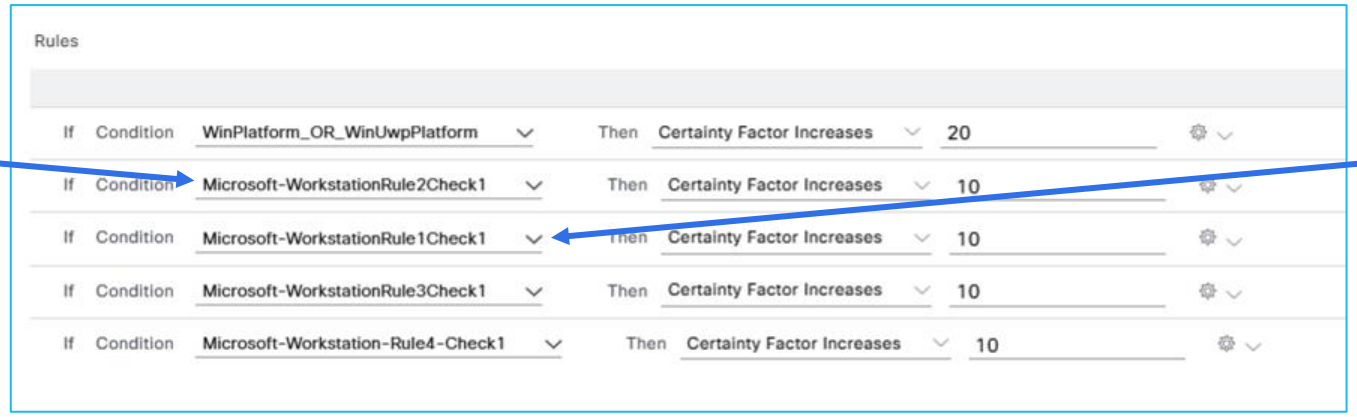


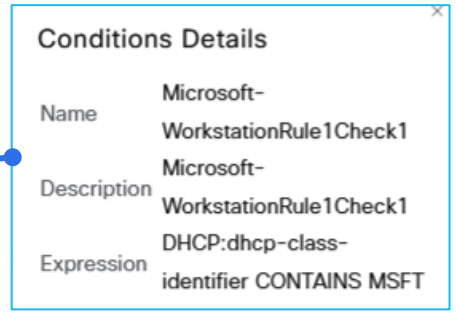


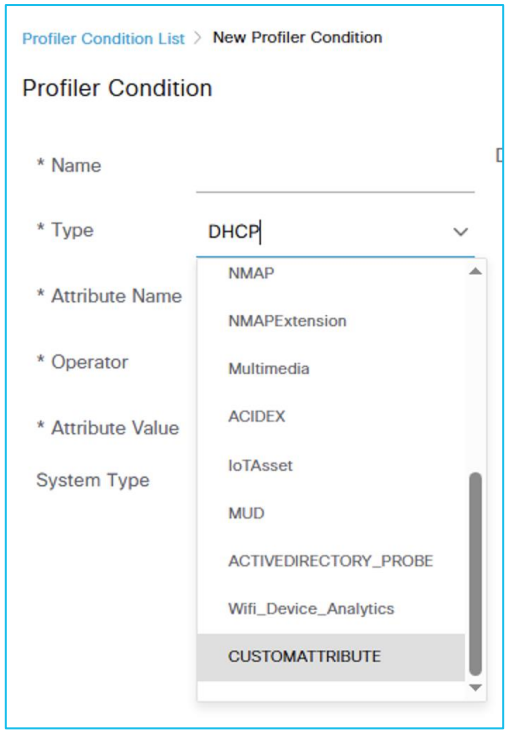
© 2026 Cisco and/or its affiliates. All rights reserved.

Policy based endpoint profiling







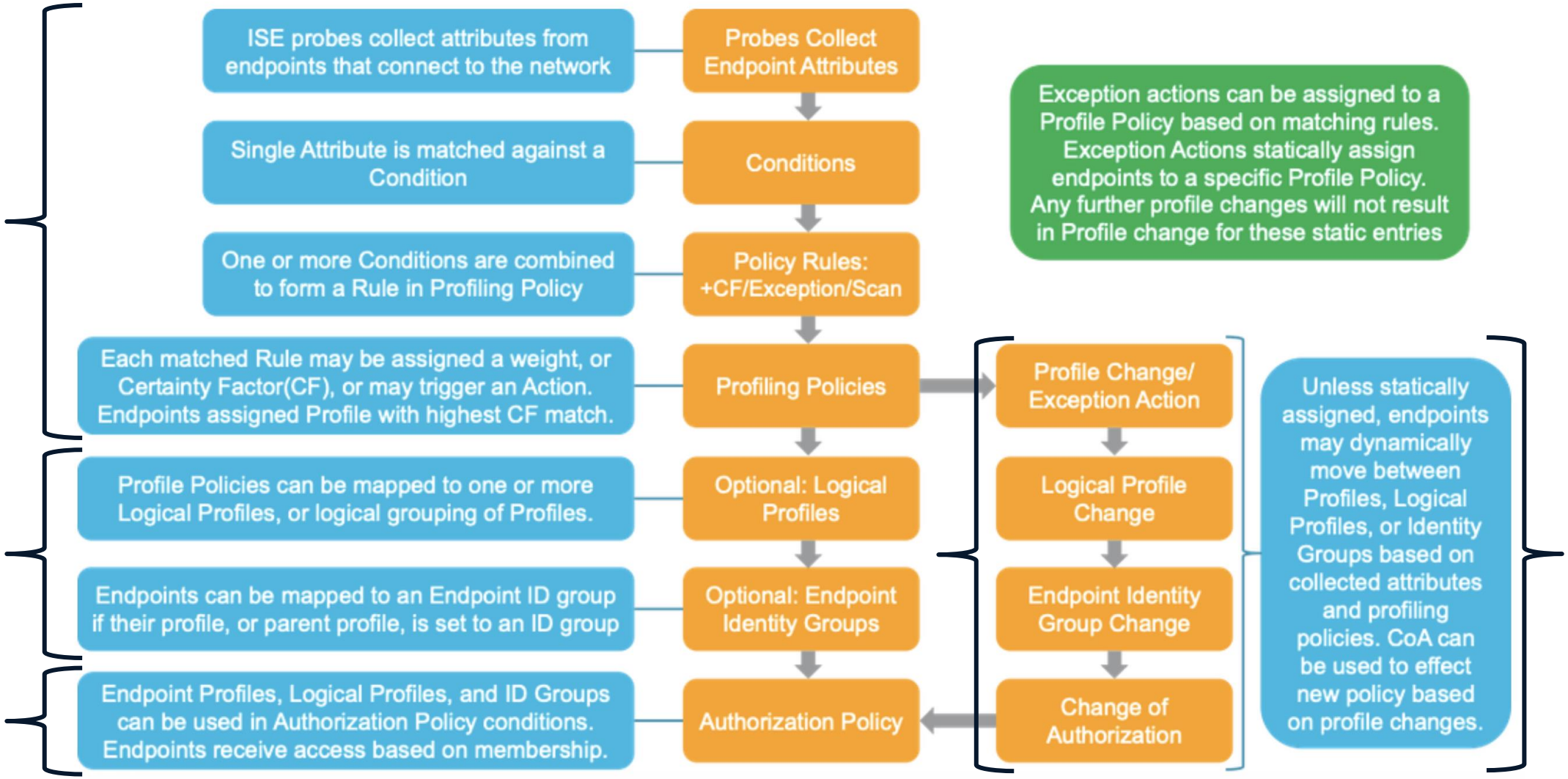


Conditions:

- **Cisco Provided (system-defined):** predefined profiling conditions (not removable)
- **Administrator Created:**
  - Profiler conditions that you create as an administrator of Cisco ISE
  - System-defined profiling conditions that are duplicated are identified as Administrator Created.

© 2026 Cisco and/or its affiliates. All rights reserved.

Policy based endpoint profiling





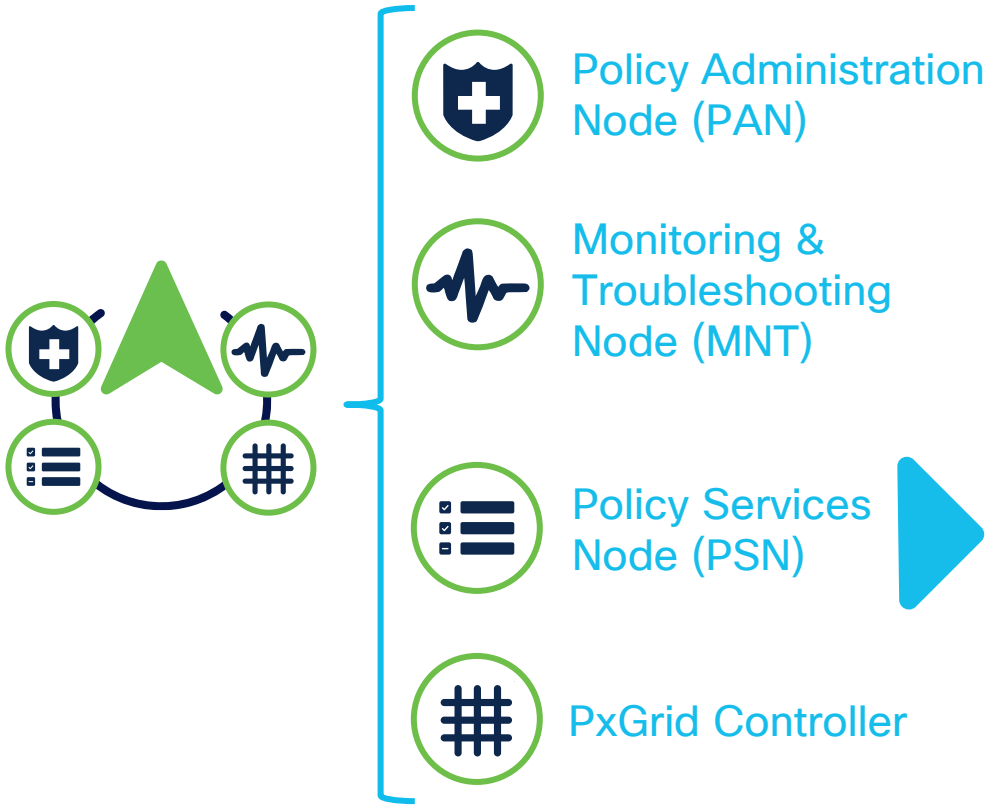
[ISE Profiling Design Guide]

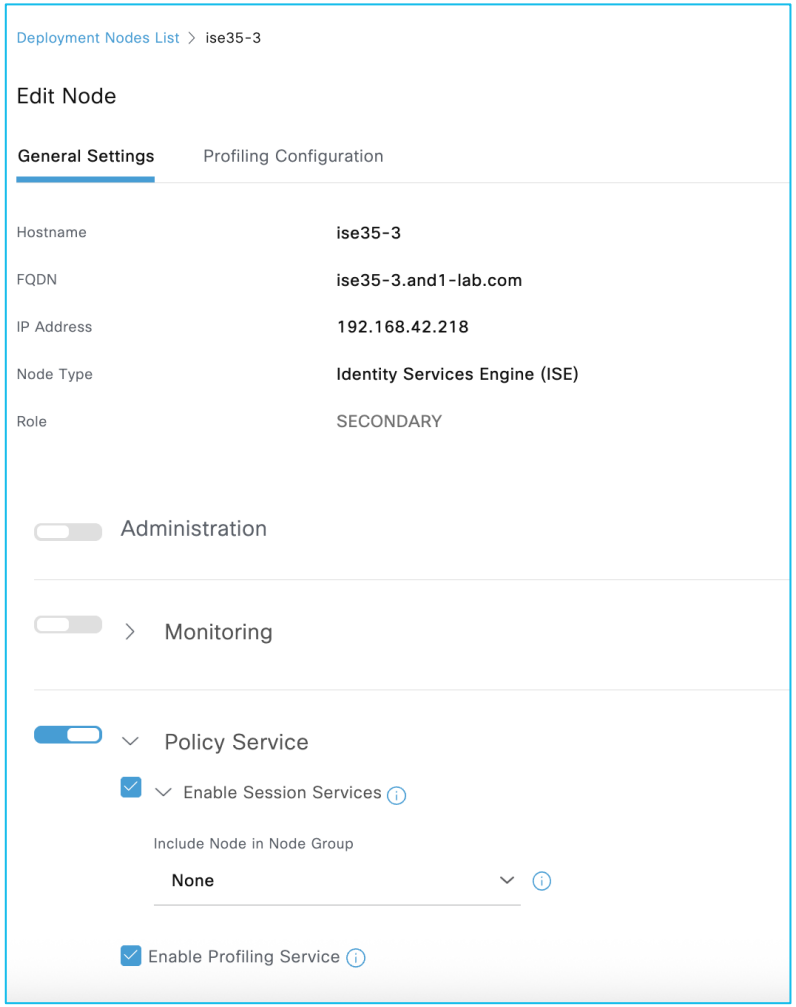
© 2026 Cisco and/or its affiliates. All rights reserved.

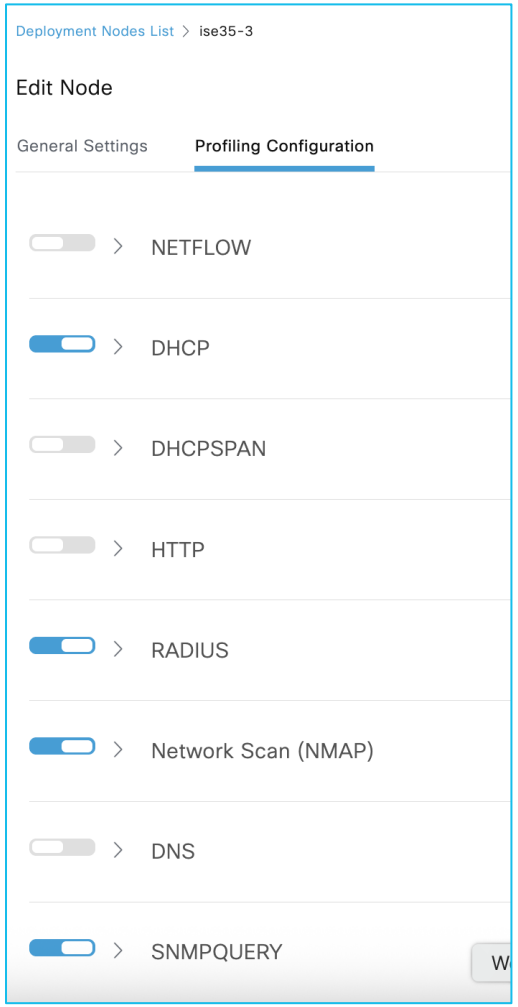
cisco

Enable Profiling service and probes

Administration>System>Deployment>PSN>Profiling Configuration







© 2026 Cisco and/or its affiliates. All rights reserved.

Implicit Profiling

Always on probes:

RADIUS

- The RADIUS probe is running by default, even for systems not configured for Profiling Service
- Ensures ISE can track endpoint authentication and authorization details to use in **Context Visibility** as well as to track the create/update timestamps for purposes of **endpoint purging operations**

HTTP

- When a PSN terminates URL-redirected flows (Posture, CWA, MDM, BYOD), it has visibility into the decrypted HTTPS data
- PSN will parse the **browser user agent** string from the web traffic and correlate the data to the endpoint even when HTTP probe is disabled on the PSN



Note: Even if disabled, Profiling service is also used by ISE for Endpoint Identity Group management

© 2026 Cisco and/or its affiliates. All rights reserved.

Profiler Architecture

Endpoint attributes

- **Endpoint Attributes –** Set of context collected and associated with specific endpoint, identified by MAC(ID) in ISE databases:

Configuration database (DB)



- Used as the centralized database on ISE for both:
  - Configuration data
  - Operational data (includes endpoint attributes)
- Consistent across all ISE nodes in the deployment
- Replicated from PAN

Endpoint Cache

- Fast in-memory key-value database
- Separate on each PSN
- Achieves high performance while PSN get endpoint attributes from local cache
- Stores different types of data consumed by key services on ISE

Context Visibility database



- Fast separate DB to store information about endpoints.
- Located on PAN and SAN
- Used by Context Visibility service on ISE

© 2026 Cisco and/or its affiliates. All rights reserved.

Significant attributes

Certain critical data needs to be shared across entire deployment. ISE stores these type of attributes in **Configuration Database (DB)** and trigger **DB persistency** – Replication to PAN with Global Replication (**if enabled**)

Significant attributes:
- EndpointPolicy
- StaticAssignement
- StaticGroupAssignment
- IdentityGroupId
- MatchedPolicyId
- PortalUser
- AUPaccepted
- BYODRegistration
- DeviceRegistrationStatus
- IP

+

WiFi Device Analytics:
- Model_num
- Firmware_version
- Os_version
- Manufacturer_name
- Model_name
- Hw_model
- Vendor_type

MFC:
- Hardware Manufacturer
- Hardware Model
- Operating System
- Device Type
- Endpoint Policy

MDM:
- Mdm_compliant
- Hardware_model
- Operating_system
- Device_type
- Endpoint_policy
- Etc.

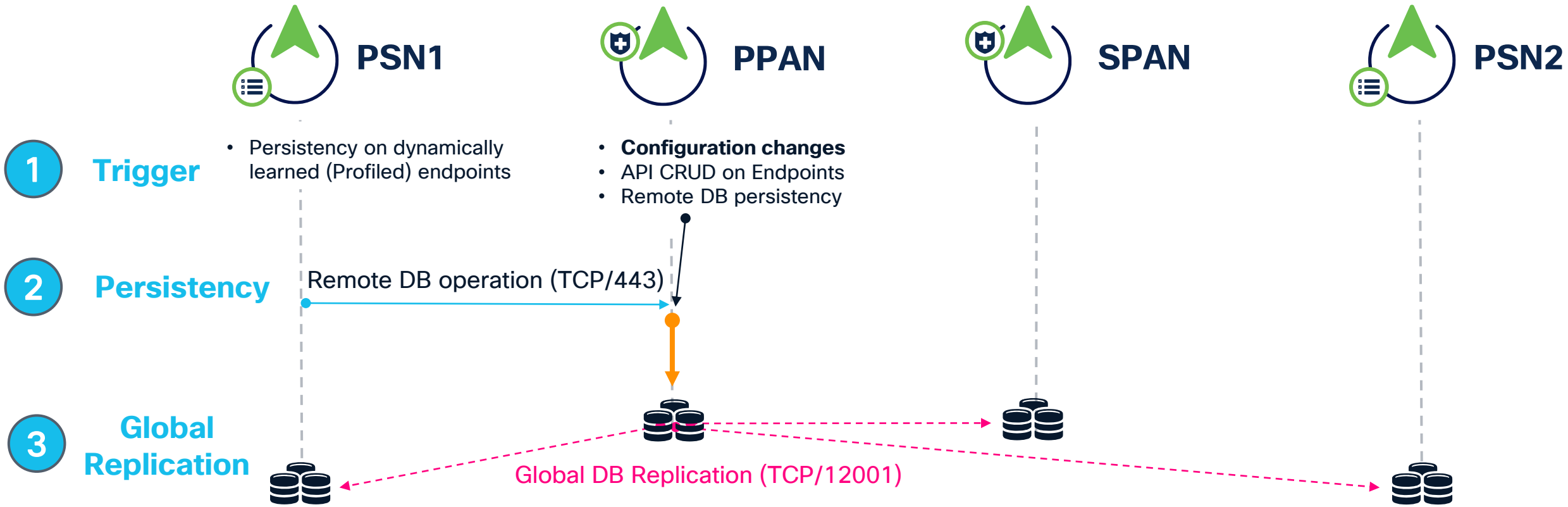
* Not significant attributes as such, but trigger DB persistency operations



Note: As the number of endpoints increase, **frequent significant attribute change could make Profiler primary contributor of DB replication**

© 2026 Cisco and/or its affiliates. All rights reserved.

Data Base Replication

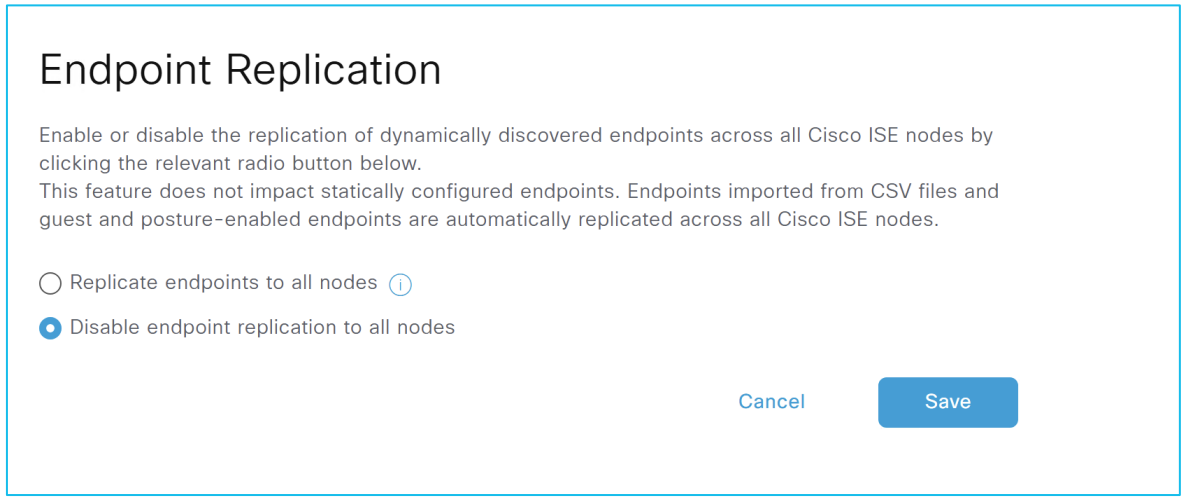


- **Global Replication** – configuration and operational data synchronizations
- DB is managed by PAN and replicated to Secondary nodes

© 2026 Cisco and/or its affiliates. All rights reserved.

Endpoint Replication

Administration > System > Settings > Endpoint Replication



- **Disabled by default from ISE 3.3**
- **Hidden from menu in ISE 3.5** (controlled via **OpenAPI**: ***/api/swagger-ui/index.html?urls.primaryName=Endpoint Replication#/***)

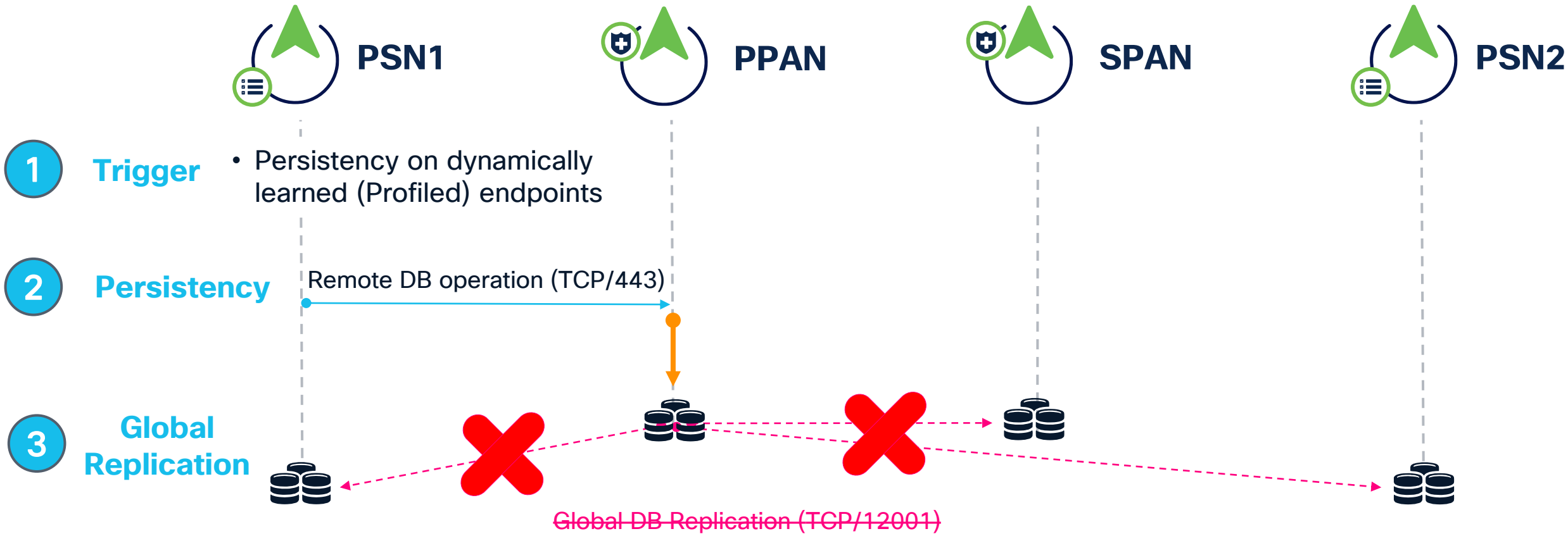
- **When disabled**, it removes redundant replication on Create/Update flow for dynamically learned (profiled) endpoints
- Reduce excessive resource consumptions on DB operations
- PPAN continue replication on configuration updates

Note:

- Don't enable unless explicitly recommended!
- Enabling EP Replication **MUST** be followed by a **Manual Sync of all PSNs** in the deployment

© 2026 Cisco and/or its affiliates. All rights reserved.

Endpoint Replication Off

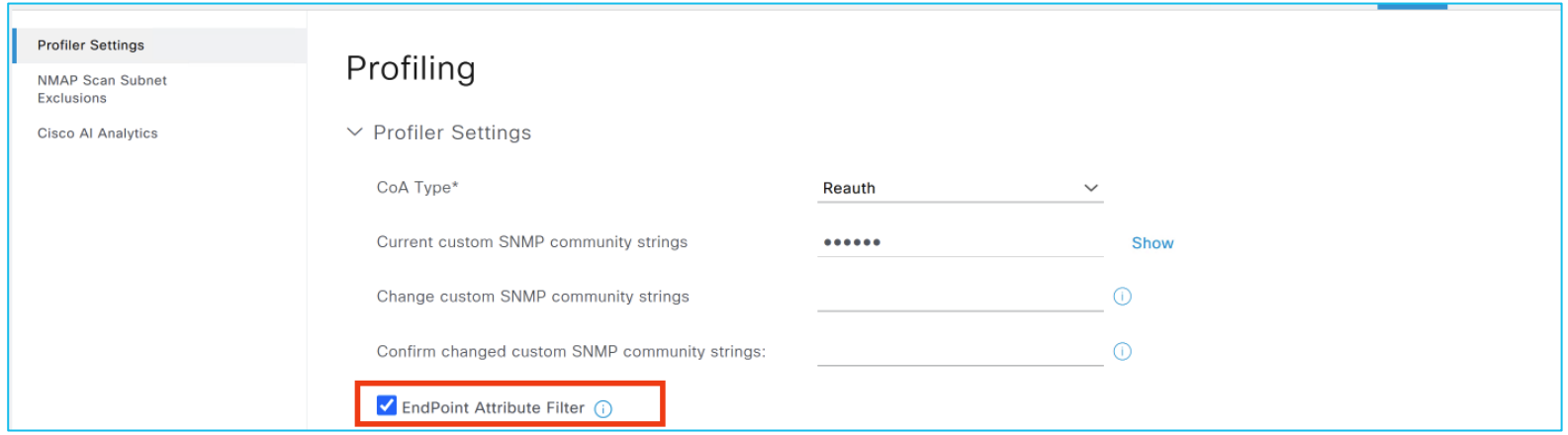


© 2026 Cisco and/or its affiliates. All rights reserved.

Endpoint Attribute Filter and Whitelist Attributes

Work Center > Profiler > Settings

- **Endpoint Attribute Filter** – aka "**Whitelist**". Reduces endpoint data collection and replication to subset of Profile-specific attributes:
  - Limits profile attribute collection/replication to those required to support default (Cisco-Provided) Profiling Polices, critical RADIUS operations, BYOD, WebAuth
- The whitelist is automatically updated to reflect changes from the Feed and updates to administrator-created conditions
- Any attribute that is not present in the **Whitelist** is dropped immediately at the time of collection, and the attribute is not used for Profiling process



Note: Recommended to **enable the Endpoint Attribute Filter** in production deployments.

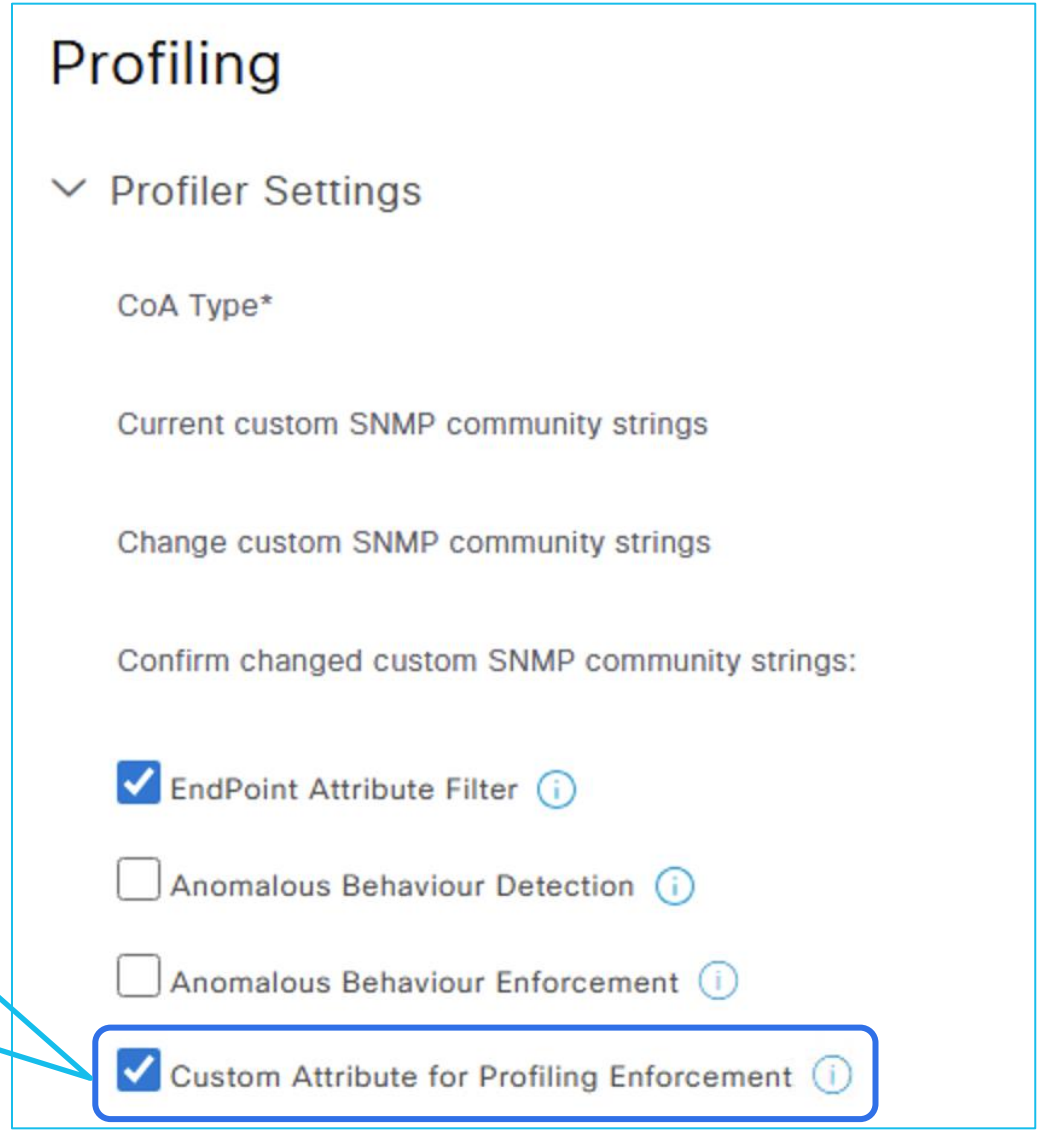
© 2026 Cisco and/or its affiliates. All rights reserved.

Custom Attributes

Values for Endpoint Custom Attributes can be assigned or updated using the following methods :

- Admin UI (Singular entry or file import)
- REST API
- PxGrid probe

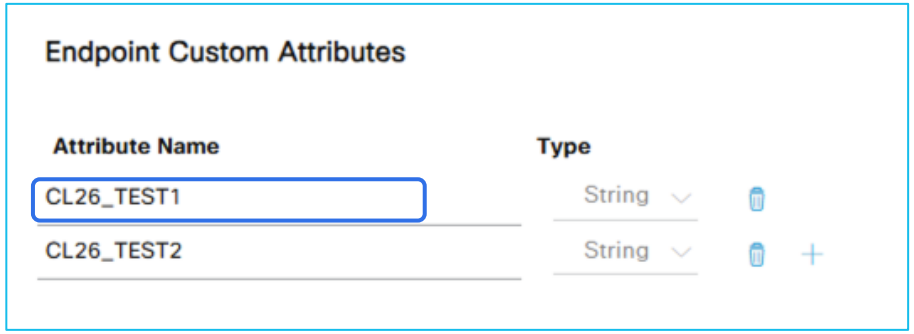
- **When enabled**, ISE consume the custom attributes, and trigger reprofiling whenever the custom attributes are updated. **Affect performance with big attribute update rate**
- **When disabled**, Profiler ignores any conditions based on Custom Attributes, even if Custom Attribute is populated
- **Do not enable this unless specifically required**



© 2026 Cisco and/or its affiliates. All rights reserved.

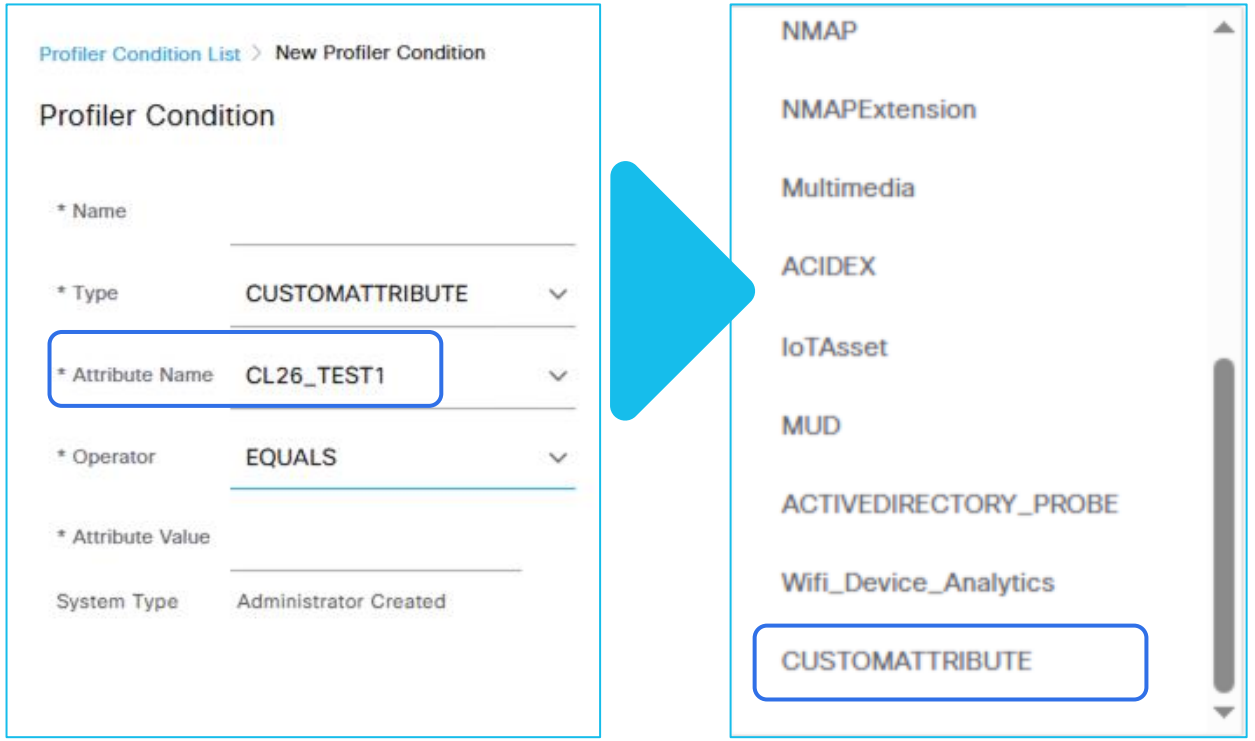
Custom Attributes (GUI workflow)

1. **Administration > Identity Management > Settings > Endpoint Custom Attributes** to define Endpoint Custom Attributes



2. **Work Centers> Profiler > Policy Elements >Profiler Condition >** New – to create new condition

3. Add the condition to Profiling policy Rule. The attribute will be Whitelisted



4. Populate the attribute to endpoints with any available method.

© 2026 Cisco and/or its affiliates. All rights reserved.

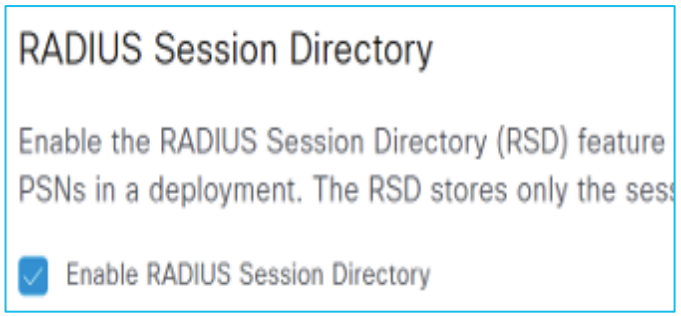
Light Data Distribution

Administration>System>Settings>Light Data Distribution

LDD:Session

Radius Session Directory (RSD) stores a 'light' session information in cache and replicates it across the deployment

Only limited set of attributes is shared. Primary use – CoA Framework, Posture



LDD:EndPointOwner

Each endpoint on ISE has an owner – ISE node, that is responsible for maintaining the full set of endpoint attributes

Endpoint Owner Directory (EPOD) stores endpoint to owner ISE node bindings. The information is replicated between other ISE nodes



Ownership takeover:

EPOD enabled (default and recommended behavior)

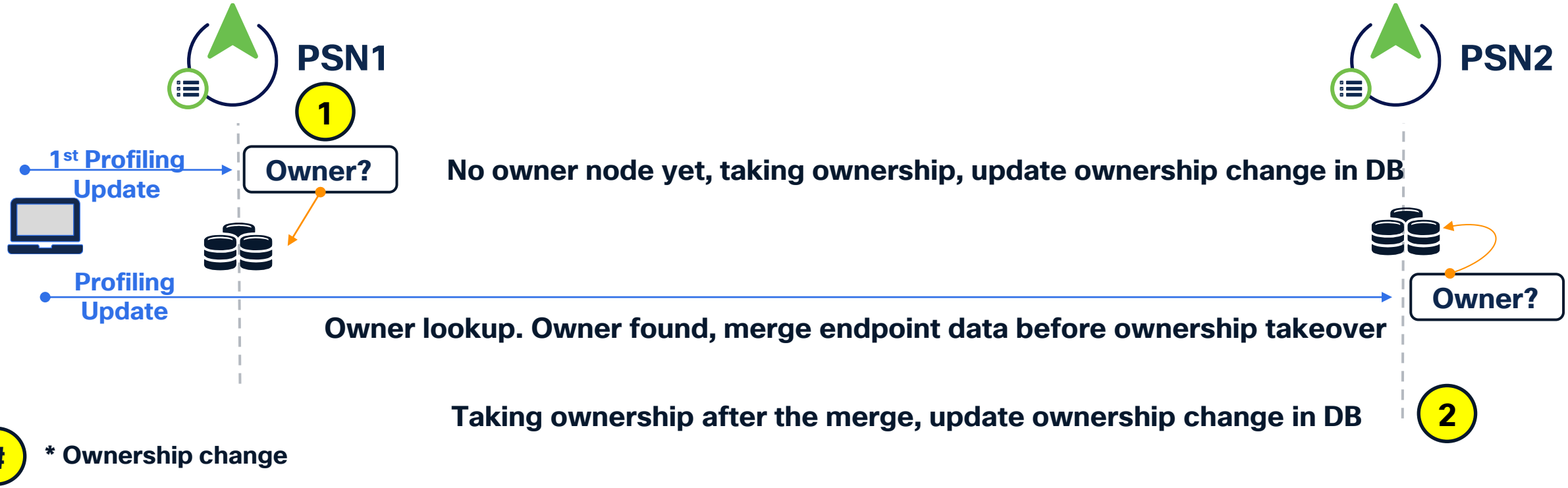
- Owner is not changed unless there is update with **higher priority** to other PSN. Priority order:
  - RADIUS Authentication (**top priority**)
  - RADIUS Accounting
  - DHCP, SNMP, HTTP, etc.

EPOD disabled

- Multiple PSNs that received probe response would compete for endpoint **ownership takeover**.
- PSN takes ownership and pulls attributes from current owner
- Update ownership (Jgroup replication)

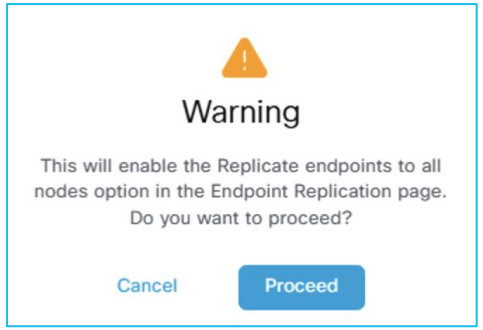
© 2026 Cisco and/or its affiliates. All rights reserved.

EPOD disabled (Legacy)



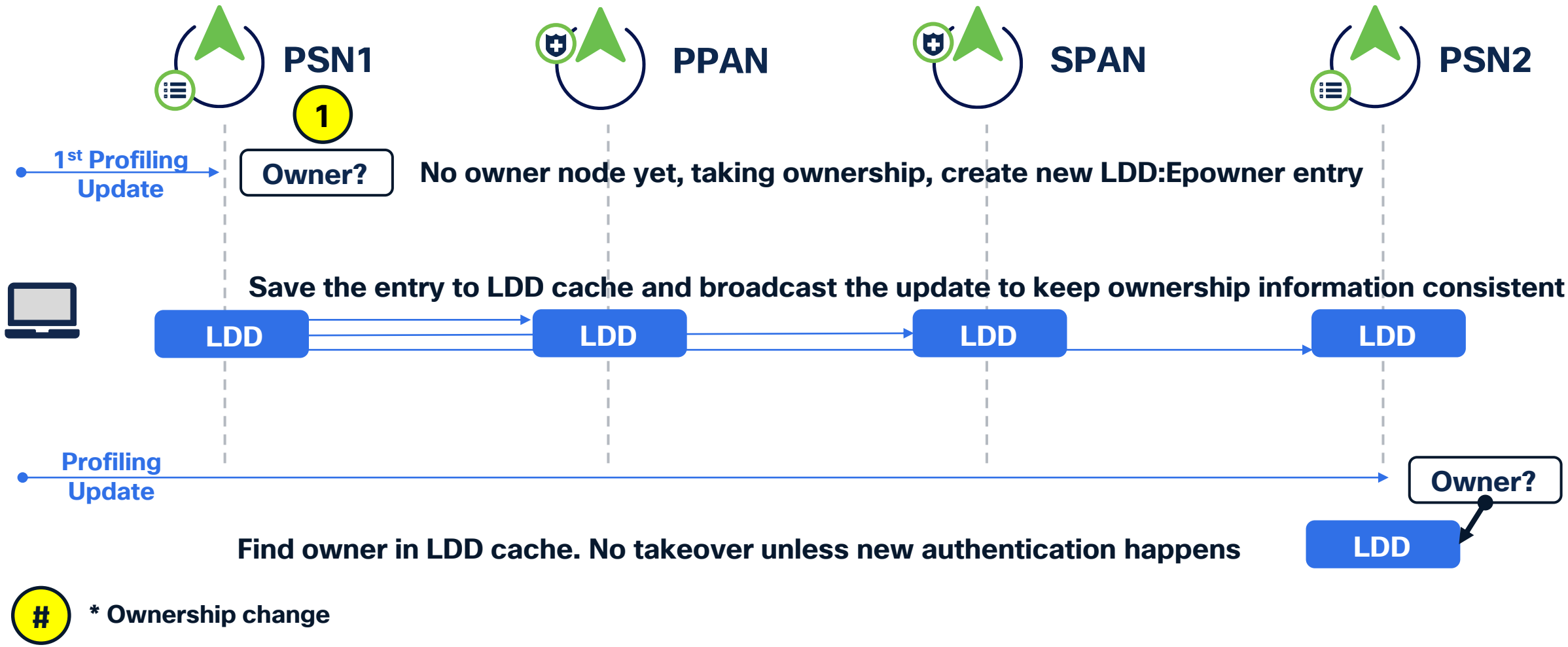
Why we don't recommend:

- **Additional DB lookups, Ownership flaps, excessive replications**
- **Turns on EP Replication automatically**. **Manual PSN sync is needed to avoid DB inconsistency (!)**



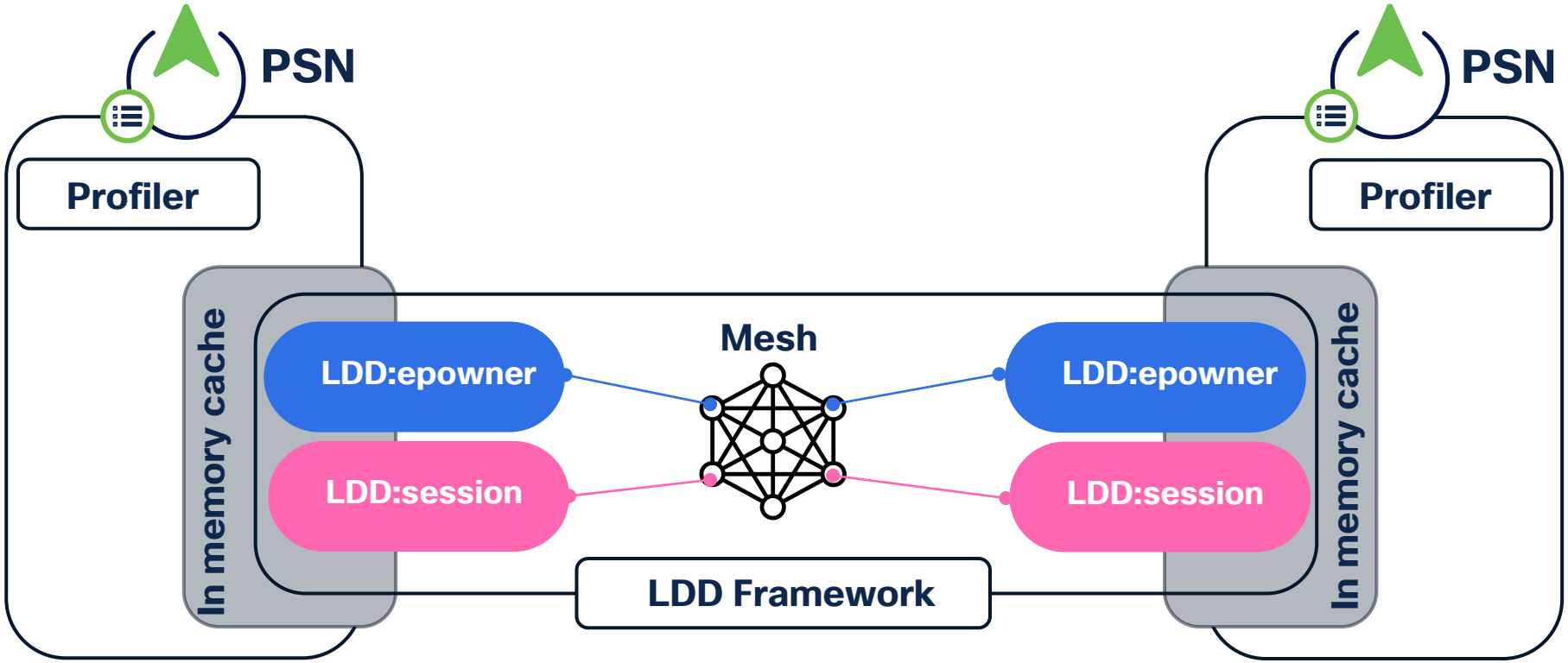
© 2026 Cisco and/or its affiliates. All rights reserved.

EPOD enabled (Recommended)



© 2026 Cisco and/or its affiliates. All rights reserved.

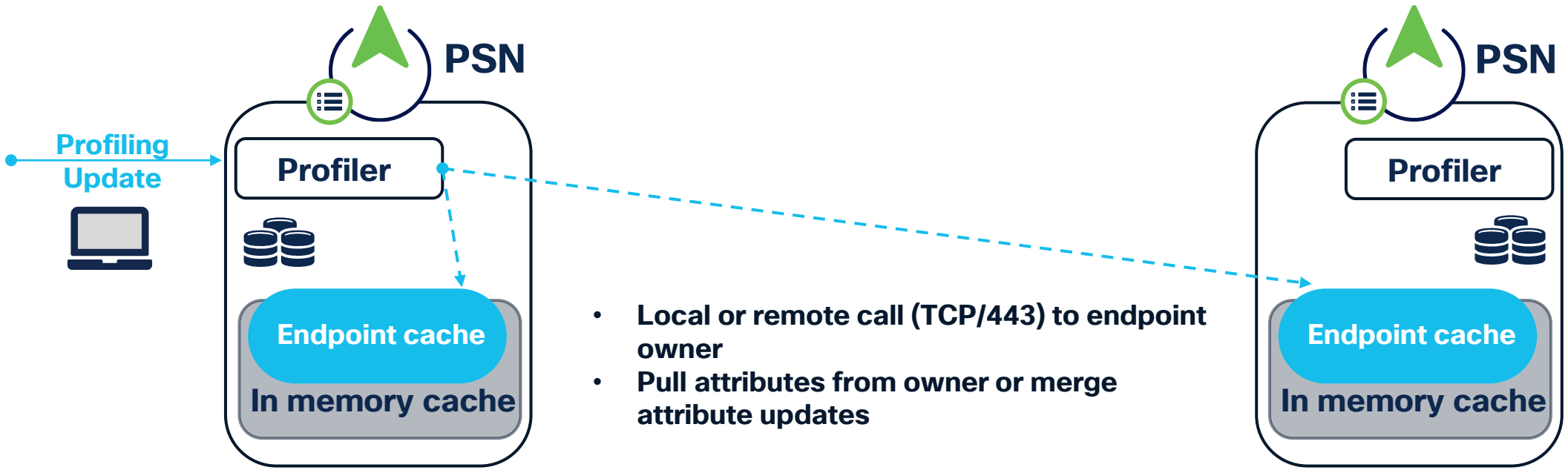
Light Data Distribution (LDD)



- **LDD Framework** – handle information in fast in-memory DB and replicate it other the deployment by message broker
- **SSL TCP/8671 and TCP/6379** using **ISE Messaging Service certificate chain** for **Mesh communication**
- RSD and EPOD listening for LDD updates broadcasted to each PSN

© 2026 Cisco and/or its affiliates. All rights reserved.

Endpoint Cache



- Separate on each PSN
- Owner PSN stores full endpoint information in the Endpoint Cache
- Not replicated, nodes make remote read and merge with the owner
- Used by PSNs to make policy decisions

© 2026 Cisco and/or its affiliates. All rights reserved.

Profiler CoA

- Change of Authorization **helps to enforce new policies** when endpoint has been classified/re-classified

First time CoA

- For endpoints profiled for first time, **first CoA event is delayed for 10 seconds**.
- It gives Profiler time to fetch additional attributes and finalize classification.
- Sent CoA unconditionally after 10 second delay

CoASourceComponent	Profiler
CoAReason	Endpoint profiled for first time

Conditional CoA

- For all other use cases Conditional CoA method is used:
  - CoA is triggered only if IdentityGroup/EndpointPolicy/LogicalProfile attribute (for the profiled endpoint) exist in any AuthZ Policy rule. If not, CoA is suppressed

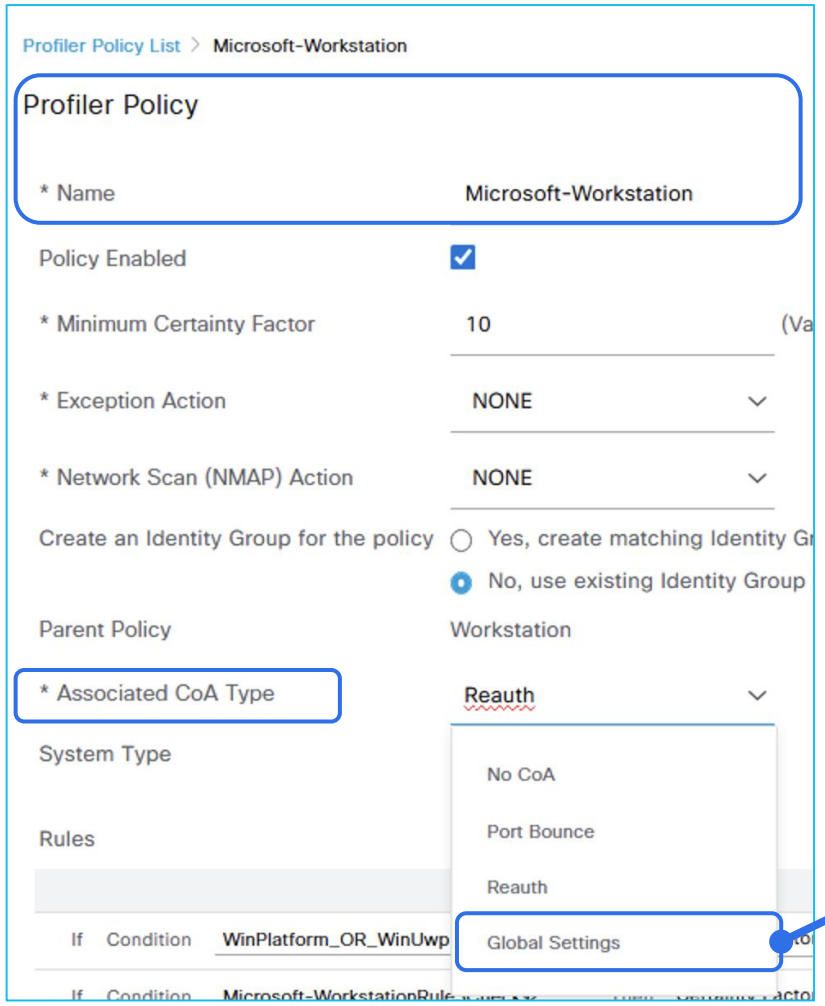
CoASourceComponent	Profiler
CoAReason	Change in endpoint identity group/policy/logical profile which are used in authorization policies

- CoA framework is concurrently shared between ISE services like Profiler, MDM, Posture
- Profiler interact with **RADIUS** component on ISE for triggering CoA to update authorization states for profiled endpoints

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Profiler CoA

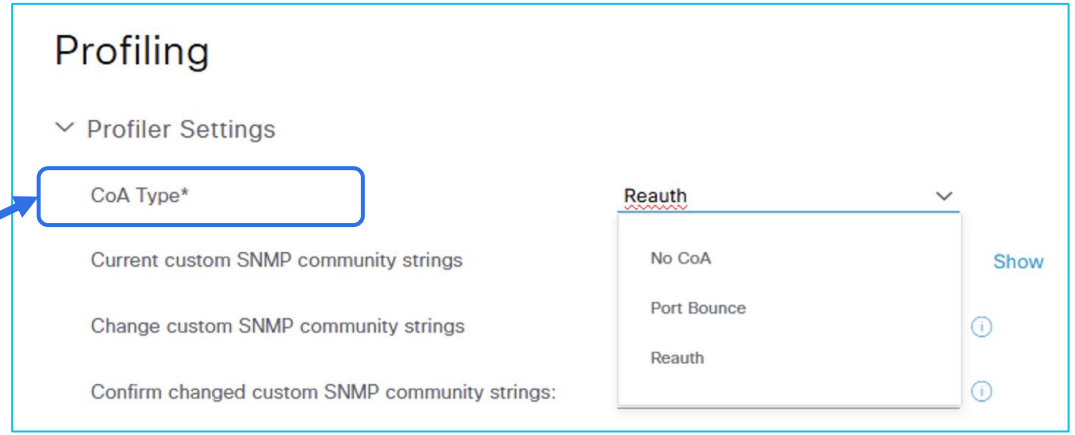


CoA type:

- **Reauth**
- **Port Bounce**
- **No CoA**

Inherit Global CoA settings unless profile specific action is set.

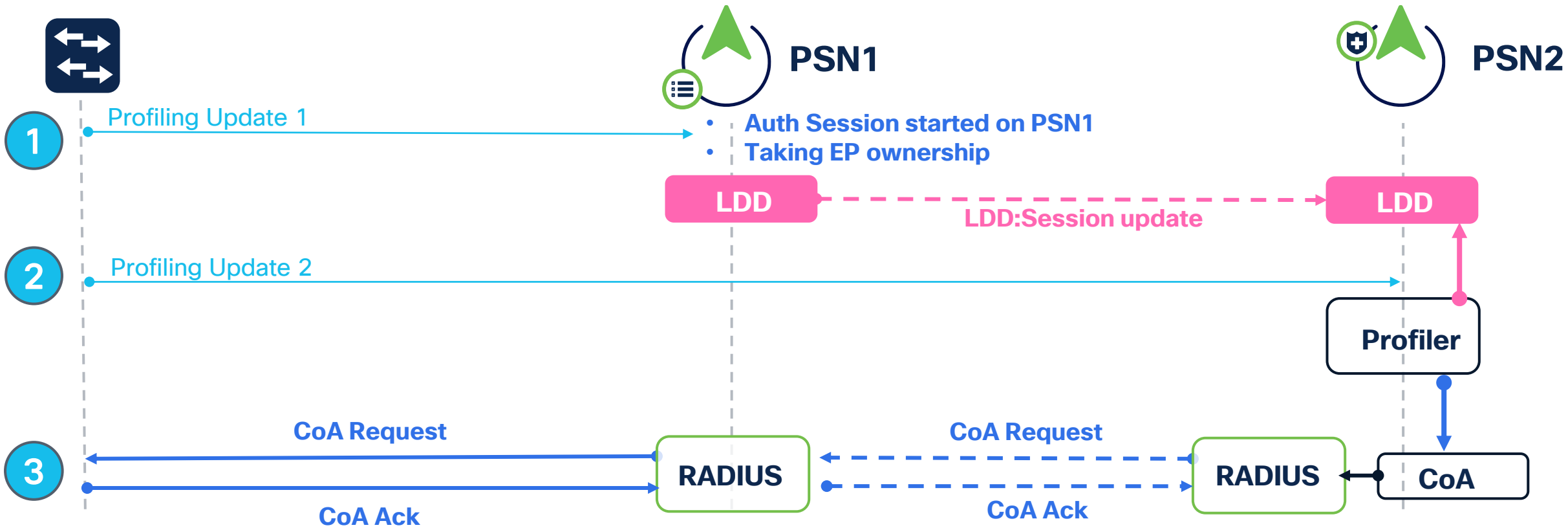
Exception: Global **No CoA** overrides all configuration settings in endpoint profiling policies as there is no CoA issued in Cisco ISE irrespective of CoA configured per endpoint profiling policy.



© 2026 Cisco and/or its affiliates. All rights reserved.

CoA Proxy

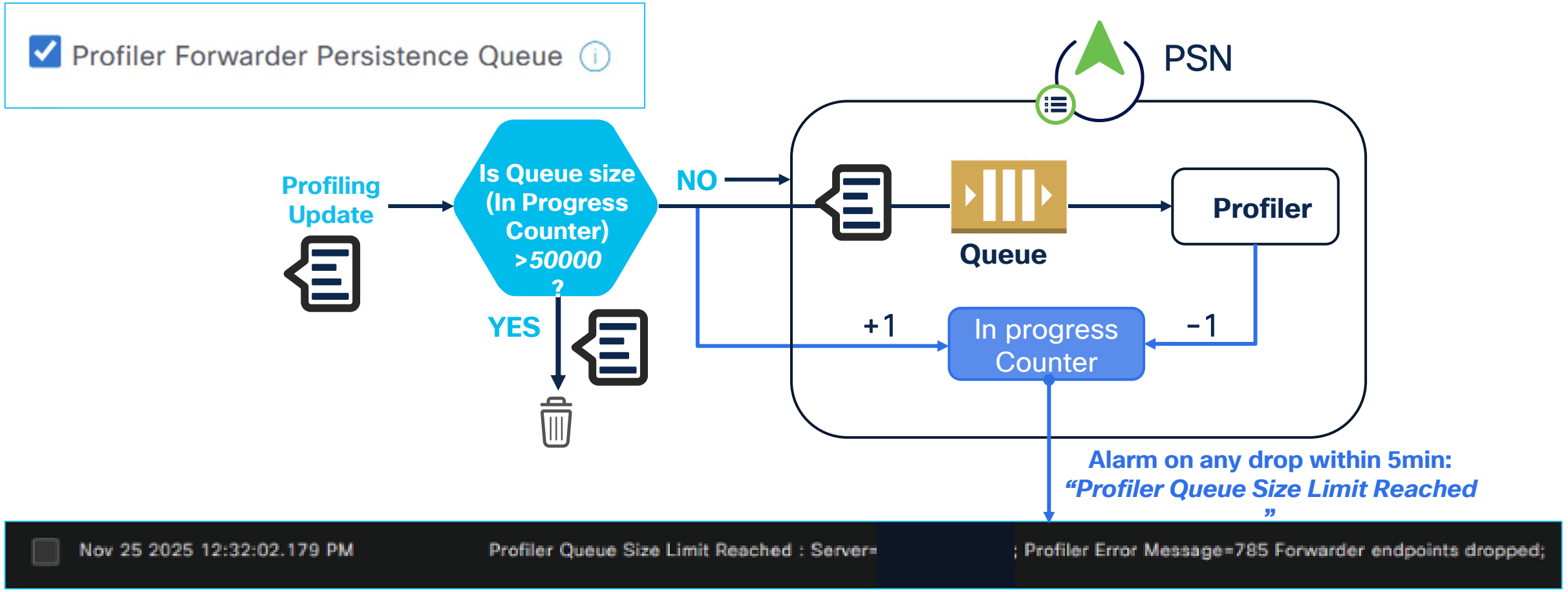
- Redirect CoA message to PSN handling the session even if Profiling event happens on other node
- LDD use case, ISE node has checks if **Session cache** contains enough information to satisfy CoA API, otherwise check with MNT



© 2026 Cisco and/or its affiliates. All rights reserved.

Profiler Forwarder Persistence Queue

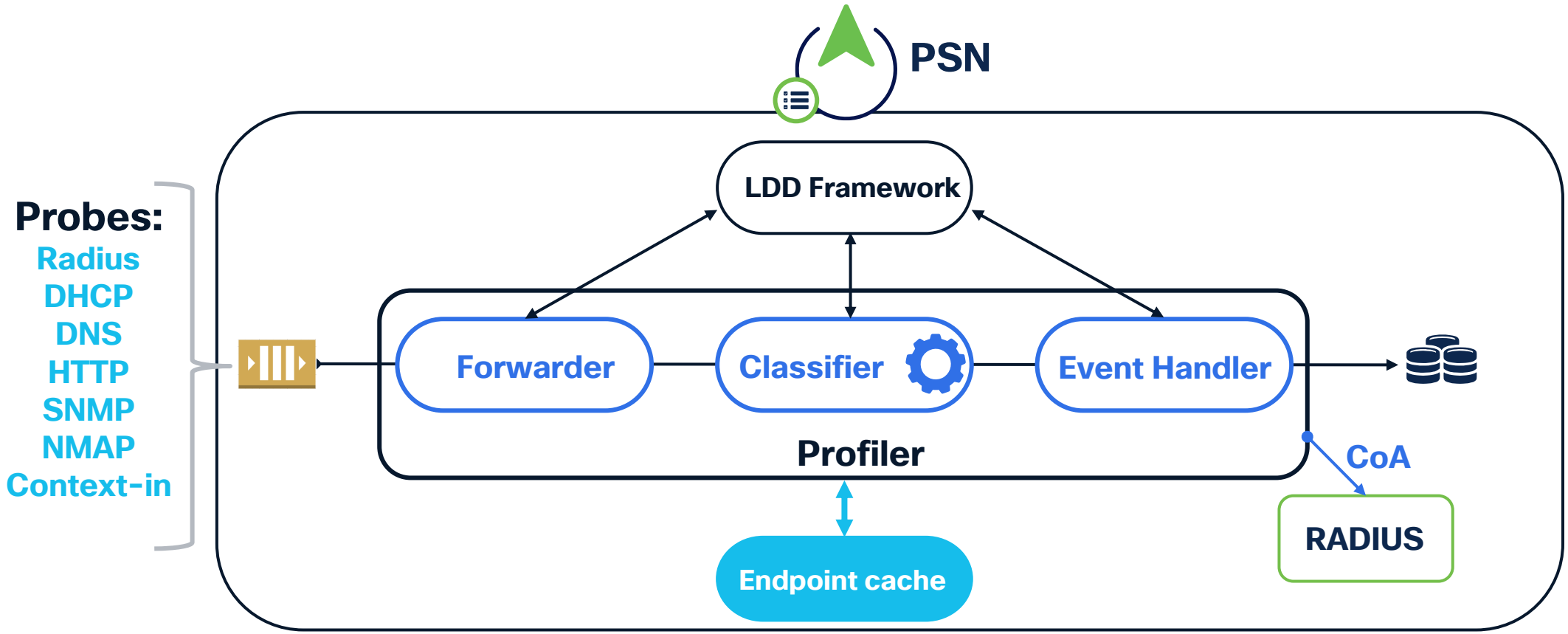
Work Centers > Profiler > Settings



Read as: PSN has dropped 785 endpoint updates **during** that 5-minute interval

© 2026 Cisco and/or its affiliates. All rights reserved.

Profiler Components



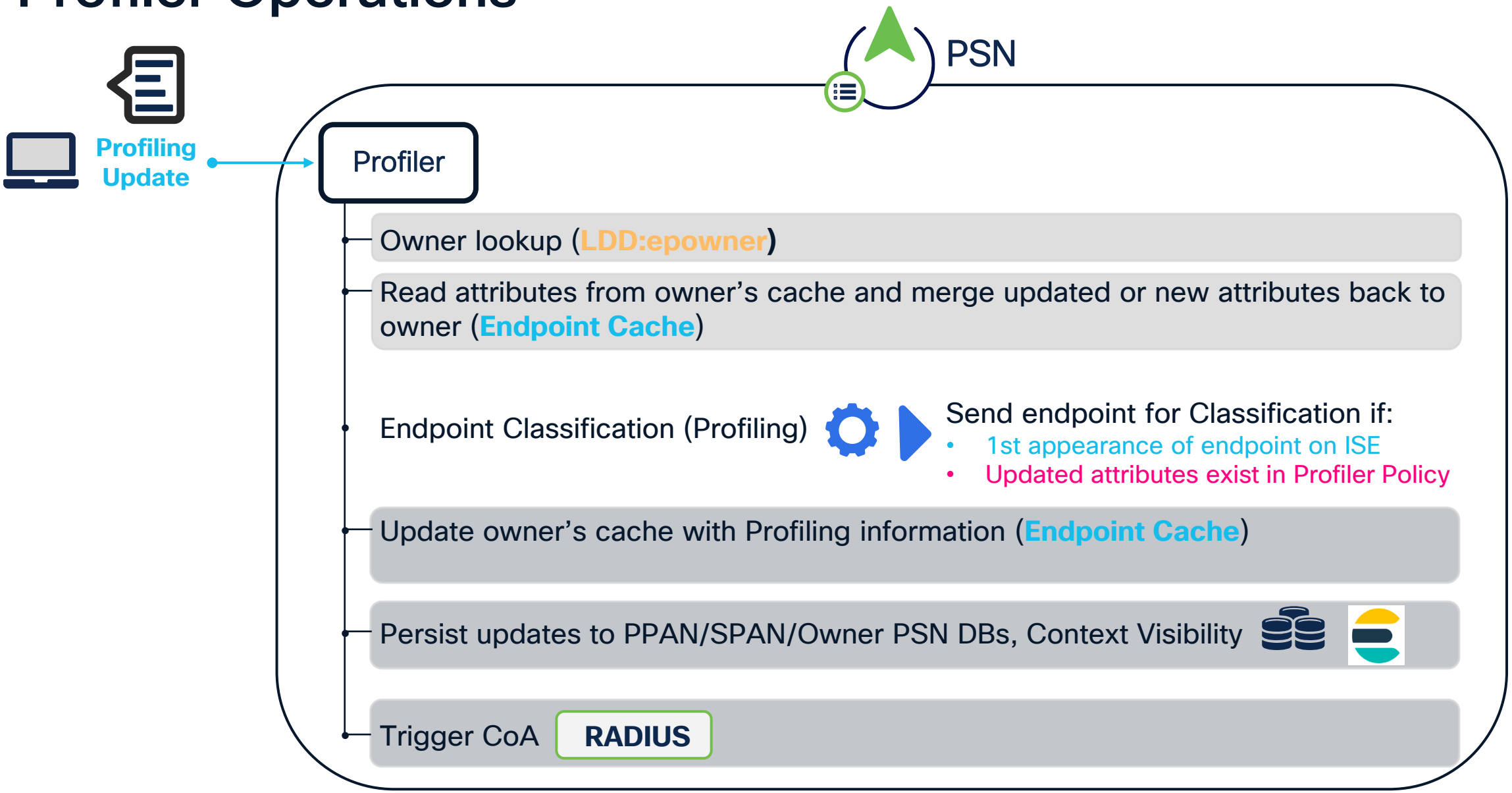
Forwarder - Main ingress queue of endpoint attributes collected by the Profiler

Classifier - match endpoint attributes with Profiler Policy

Event Handler - DB query operations

© 2026 Cisco and/or its affiliates. All rights reserved.

Profiler Operations



© 2026 Cisco and/or its affiliates. All rights reserved.

Profiler Performance

Profiler limits

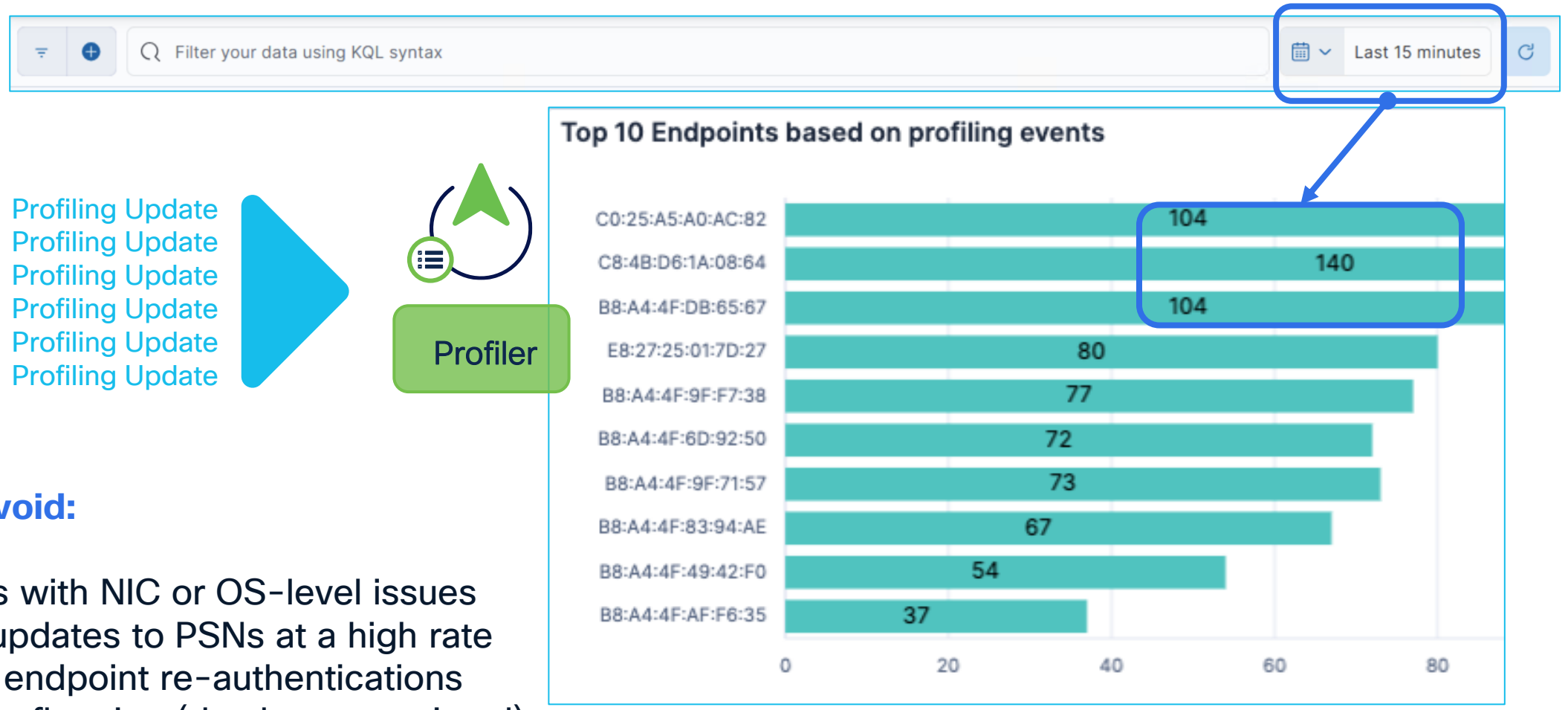
Counter	Value	Comments
max Endpoints in Endpoint Cache	**100 000**	Least Recently Used Algo(LRU)
Forwarder Queue Size	**50 000**	
Total Endpoints in DB	Cisco SNS 3695, 3795, or 3895 as dedicated/shared PAN: **4,000,000** Cisco SNS 3655 as dedicated/shared PAN: **1,000,000** Cisco SNS 3755 or 3855 as dedicated/shared PAN: **1,500,000** Cisco SNS 3715 or 3815 as shared PAN: **50,000** Cisco SNS 3615 as shared PAN: **25,000**	
Concurrent Active Endpoints	**2 000 000**	Cisco SNS 3695, 3795, or 3895 as dedicated PAN or MnT
Profiler updates per second	**250 (**200 for Small)	



[Performance and Scalability Guide for Cisco Identity Services Engine]

© 2026 Cisco and/or its affiliates. All rights reserved.

Performance challenges: sudden flood of endpoint events



Things to avoid:

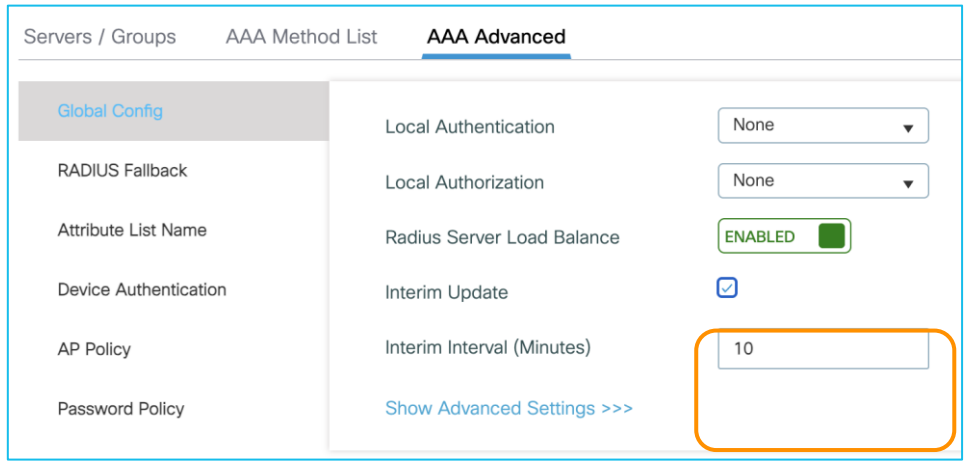
- Endpoints with NIC or OS-level issues sending updates to PSNs at a high rate
- Frequent endpoint re-authentications
- IP address flapping (database-persisted)
- Excessive MDM or AI Endpoint Analytics updates (database-persisted)

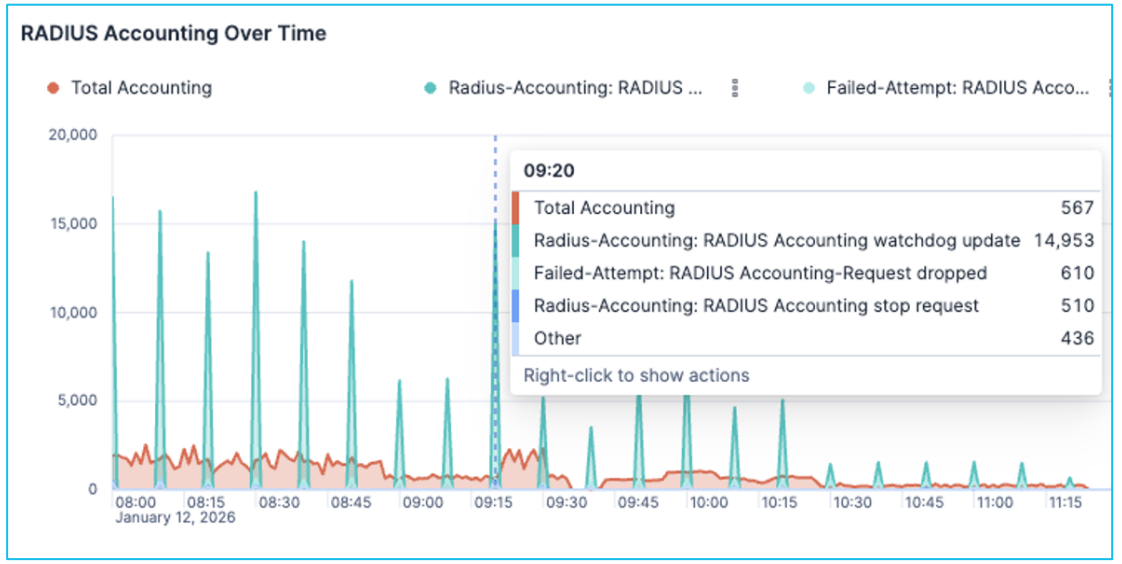
© 2026 Cisco and/or its affiliates. All rights reserved.

Performance challenges: NAD misconfiguration

NADs sends frequent or redundant accounting updates:

(config)#aaa accounting update newinfo periodic 10

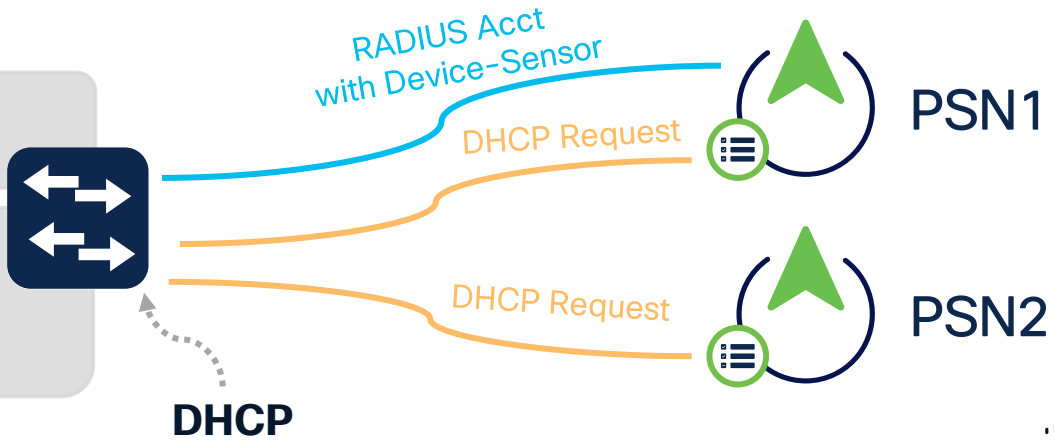




Duplicate attribute information:

device-sensor notify all-changes
access-session accounting attr filter-spec include list Def_Acct_List

interface Vlan100
ip helper-address <real DHCP>
ip helper-address <PSN1>
ip helper-address <PSN2>

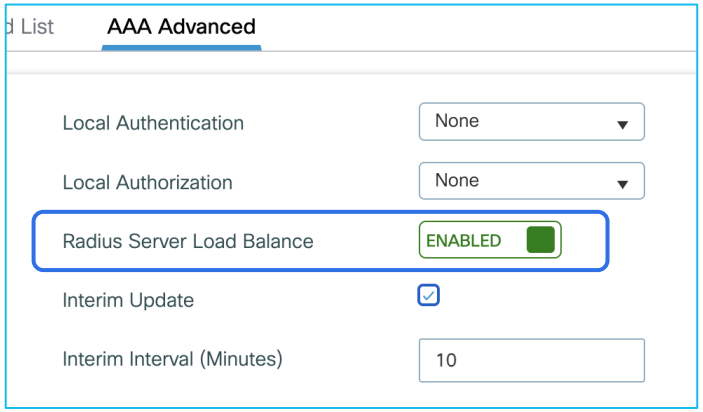


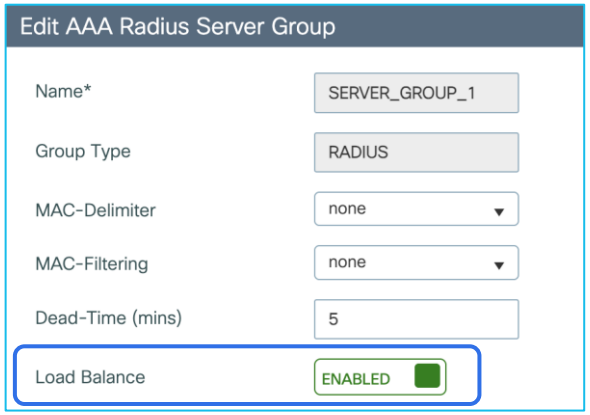
© 2026 Cisco and/or its affiliates. All rights reserved.

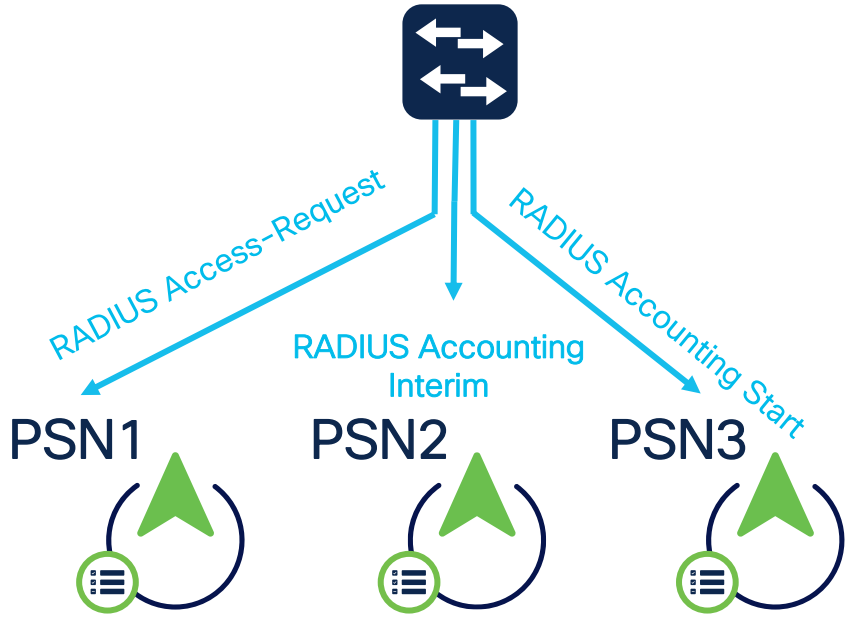
Performance challenges: NAD misconfiguration

IOS-XE built in RADIUS traffic load-balance:

aaa group server radius dnac-client-radius-group
server name dnac-radius_192.168.42.213
server name dnac-radius_192.168.42.214
radius-server load-balance method least-out batch-size 5



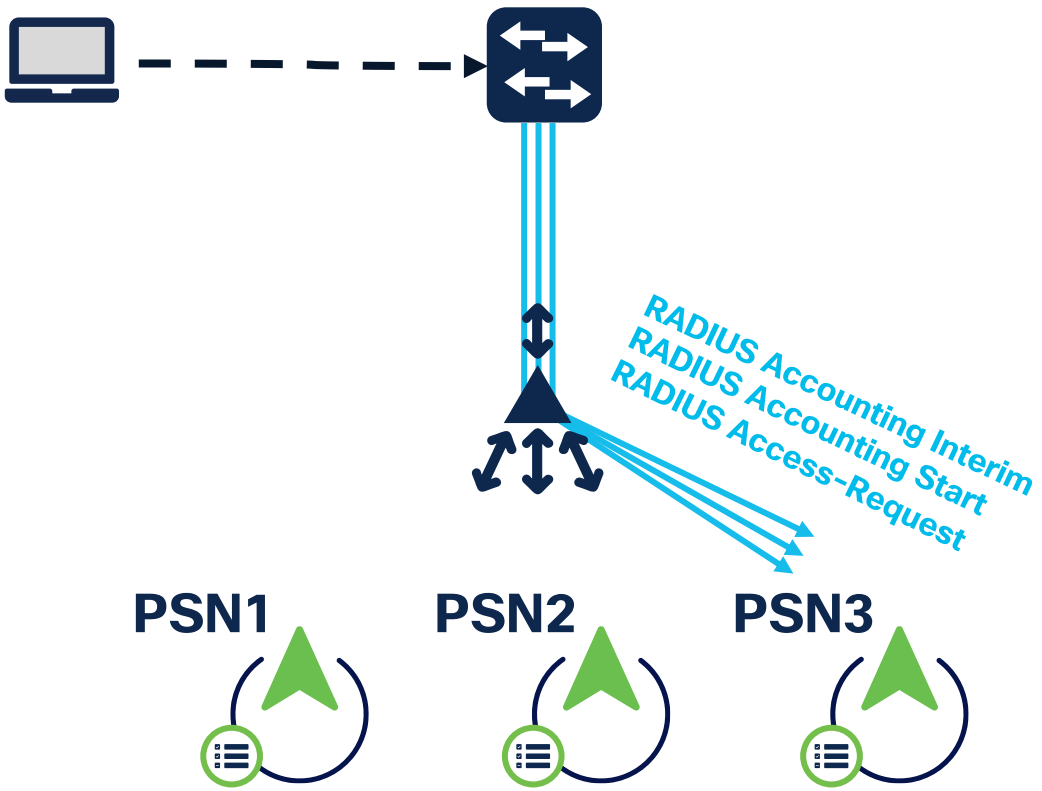




- Batches of RADIUS messages (not transactions) are distributed across AAA servers within the group Each batch assigned to the server with the fewest outstanding transactions
- **No Persistence**. No stickiness maintained for endpoint updates to PSNs
- Leading to multiple non-owner PSN updates. **NOT RECOMMENDED!**

© 2026 Cisco and/or its affiliates. All rights reserved.

Performance challenges: external LB



Note: Persistence helps prevent endpoint owner flapping for endpoints that reauthenticate frequently

Best Practice Check list:

- **Persistence (Stickiness)**
- **Make sure Persistence works across multiple LB services, example from F5:**

F5 Big-IP: Session Persistence Profiles

- Calling-Station-ID based persistence is the best option
- Avoid using Source-IP address for sticky value
- Sticky Timers need to be at least 1 hour
- DO NOT Round Robin Traffic
- Usually special script applied on LB which helps to keep persistence in place between different applications/ports
- Use the vendor specific guides from the community:

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

© 2026 Cisco and/or its affiliates. All rights reserved.

Performance challenges: Infrastructure

Problem	Impact	How to protect
High network latency between ISE nodes	**(>300ms)** Silently affect multiple operations and services on ISE. Force to slow down overall performance.	Monitor network latency for ISE-to-ISE and ISE-to-NAD locations
Blocked ports between ISE nodes: TCP/8671, TCP/6379, TCP/12001, TCP/443	Breaks communication links between ISE nodes (Jgroups, LDD, ISE Messaging)	Make sure all required port available between ISE nodes according to ISE Ports Reference
Forward/Reverse DNS resolution failed between ISE nodes	Requires for mutual trust between ISE nodes, breaks entire communications	Preserve Forward/Reverse entries availability across all regions and zone where ISE nodes deployed
Queue Link Errors	Breaks communication links between ISE nodes: ISE Messaging, LDD	Make sure 'ISE Messaging Service' certificate chain issued by ISE root CA is consistent and not expired on each ISE node Check the link for more details

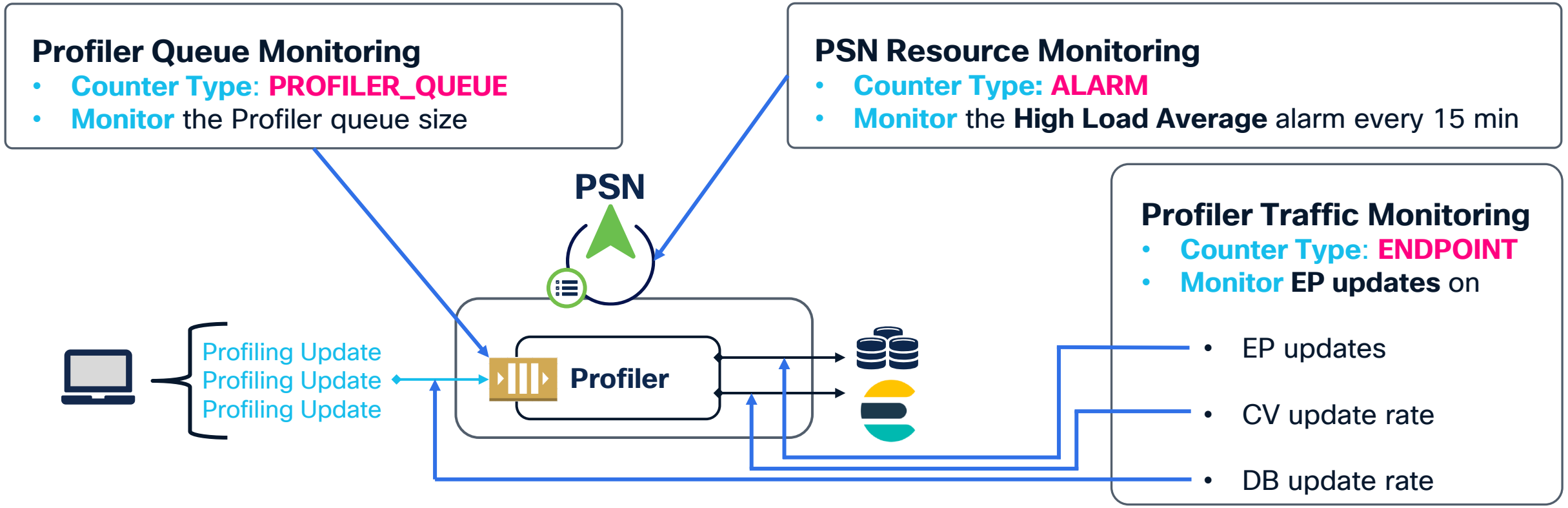
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

ISE Profiler Resiliency (3.5+)

The feature is intended to mitigate:

- Sudden spikes in inflow of EP updates or RADIUS traffic and avoid global impact to overall Profiler service and common performance of ISE node
- High resource usage on ISE PSN node



© 2026 Cisco and/or its affiliates. All rights reserved.

ISE Profiler Resiliency (3.5+)

Profiler Traffic Monitoring

Actions:

- Mark EP as chatty based on **thresholds:**
  EP updates: 30 updates/min
  CV updates: 15 updates/min
  DB Updates: 5 updates/min
- **Stop** processing the probe data for chatty endpoint till **Cool off period –** 5 min

Profiler Queue Monitoring

Actions:

- **80% full**
  - Suppress interim
  - Suppress reclassification
- **90% and 100% full**
  - Process only new EPs

Cool off period – 5 min

- Generate Audit log whenever Profiler service is degraded

PSN Resource Monitoring

Actions:

Degrade Profiler service by:
- Suppressing interim
- Suppressing reclassification

Cool off period – 5 min (depends on the alarm timers as well)

- Generate Audit log whenever Profiler service is degraded

Threshold: Maximum cut off, number of EP updates, queue counters in %, etc.

Duration: The time period (in seconds) during which the counter is monitored

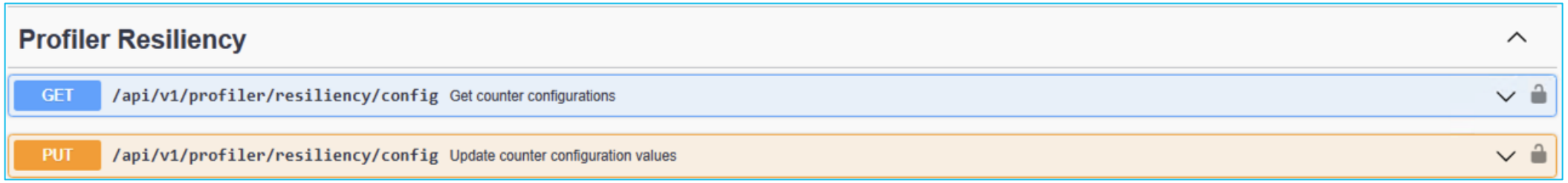
Cool off period: time to suppress EP updates

© 2026 Cisco and/or its affiliates. All rights reserved.

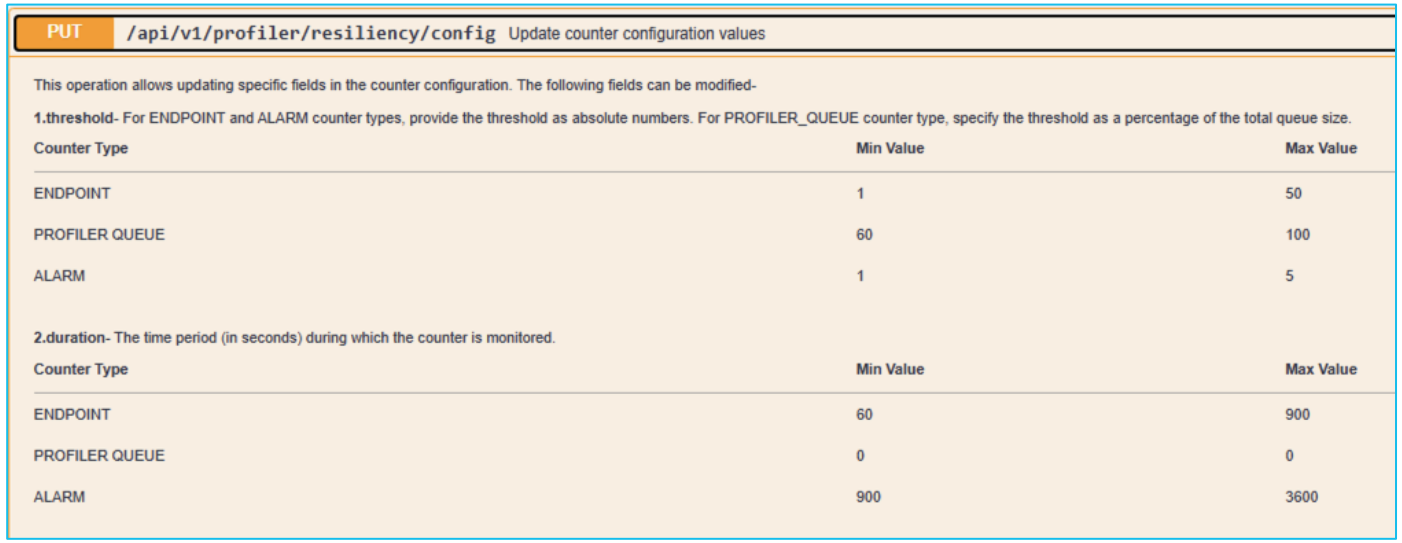
ISE Profiler Resiliency (3.5+)

Managed with Open APIs:

- **/api/v1/profiler/resiliency/config (GET)** – to get th default config
- **/api/v1/profiler/resiliency/config (PUT)** – to update the default config



- Limits we can set:

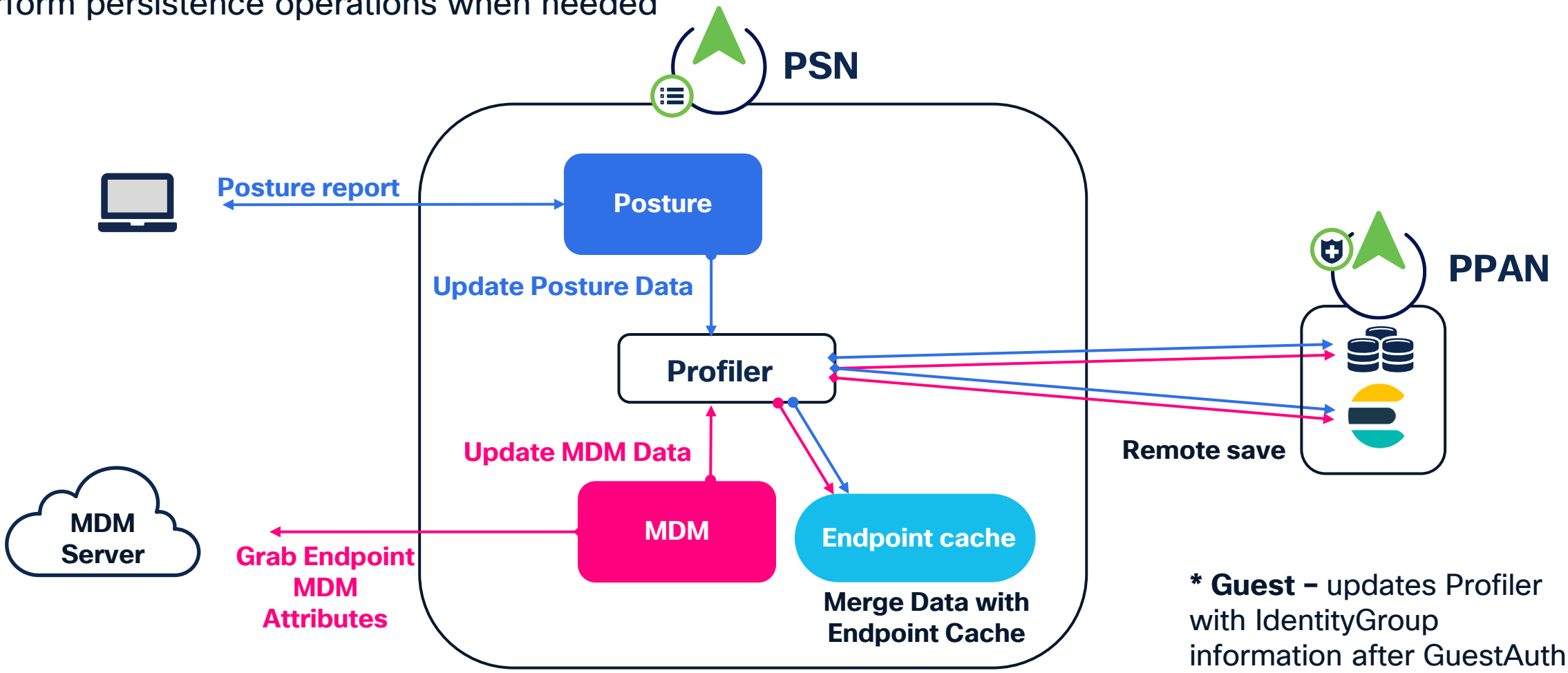


© 2026 Cisco and/or its affiliates. All rights reserved.

Additional Services

Profiler as a service

The Profiler provides services to merge and retrieve information from the endpoint cache and to perform persistence operations when needed



*** Guest –** updates Profiler with IdentityGroup information after GuestAuth

© 2026 Cisco and/or its affiliates. All rights reserved.

Context Visibility (CV)



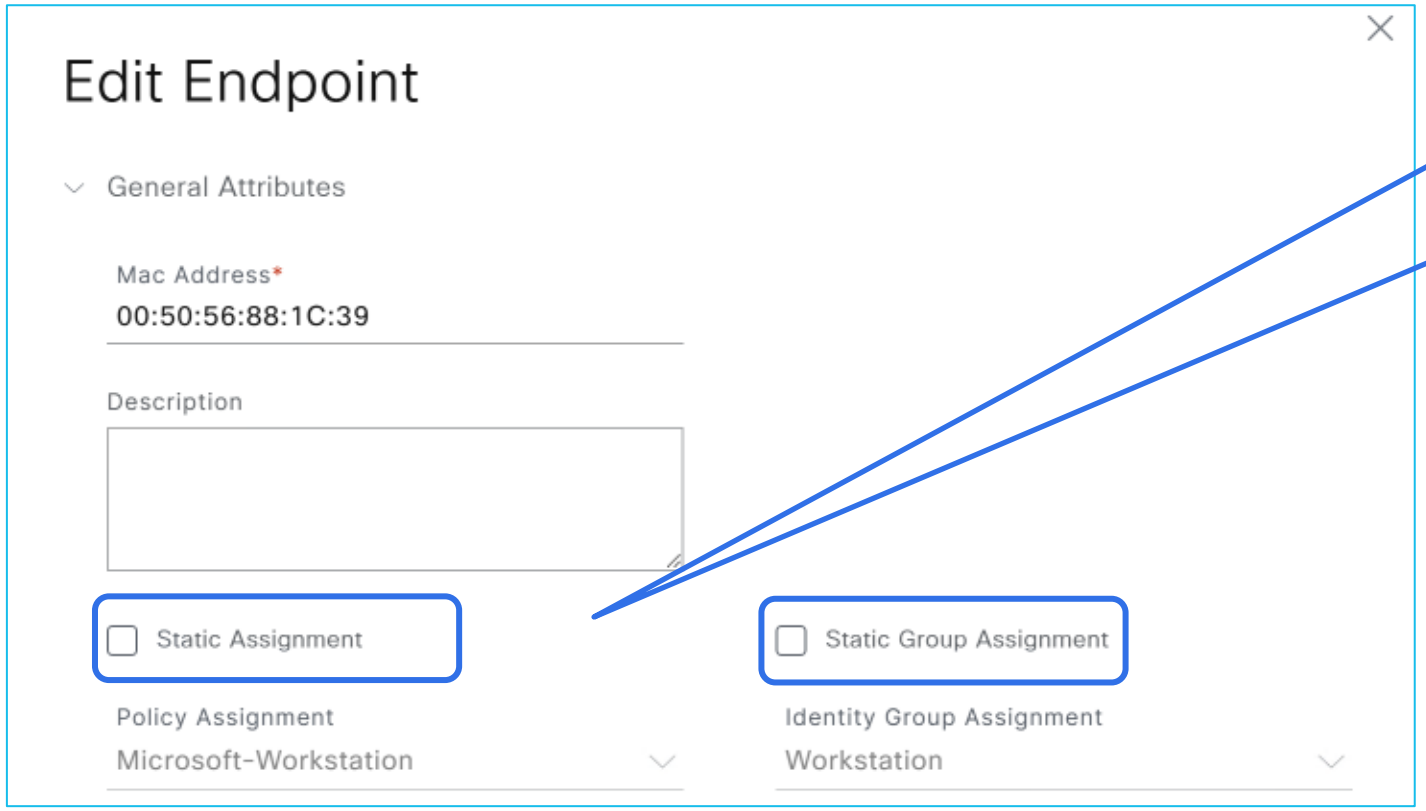
- Centralized store of endpoint attributes **consumed by ISE GUI**.
- Runs on **PPAN** and SPAN. Provides ability to aggregate, store and search high volumes of data. Stored in **Context Visibility Database.**
- Profiling updates **persisted** to Context Visibility Database. **Context Visibility has different set of significant attributes to persist**
- **Before ISE 3.4**, this existed as an Elasticsearch cluster, with the PPAN as the master and the SPAN as the replica. **Starting with ISE 3.4**, Elasticsearch instances are independent on the PPAN and SPAN. **Be sure to track updates to the Context Visibility reset procedure**:

Reset Identity Services Engine (ISE) Context Visibility

© 2026 Cisco and/or its affiliates. All rights reserved.

Static Group Assignment (SGA)

- Significant attribute, resides in DB. Triggers Global Replication on change.
- **ISE rely on DB to get information about static group**, not Endpoint cache.
- Assign Endpoint Identity Group or Endpoint Policy attributes



Statuc assignment rules

- **If unchecked**, assignment status set to dynamic for the endpoint that allows dynamic profiling
- **If checked**, Identity Group attribute assigned statically, and not changed by Prfoling classification results

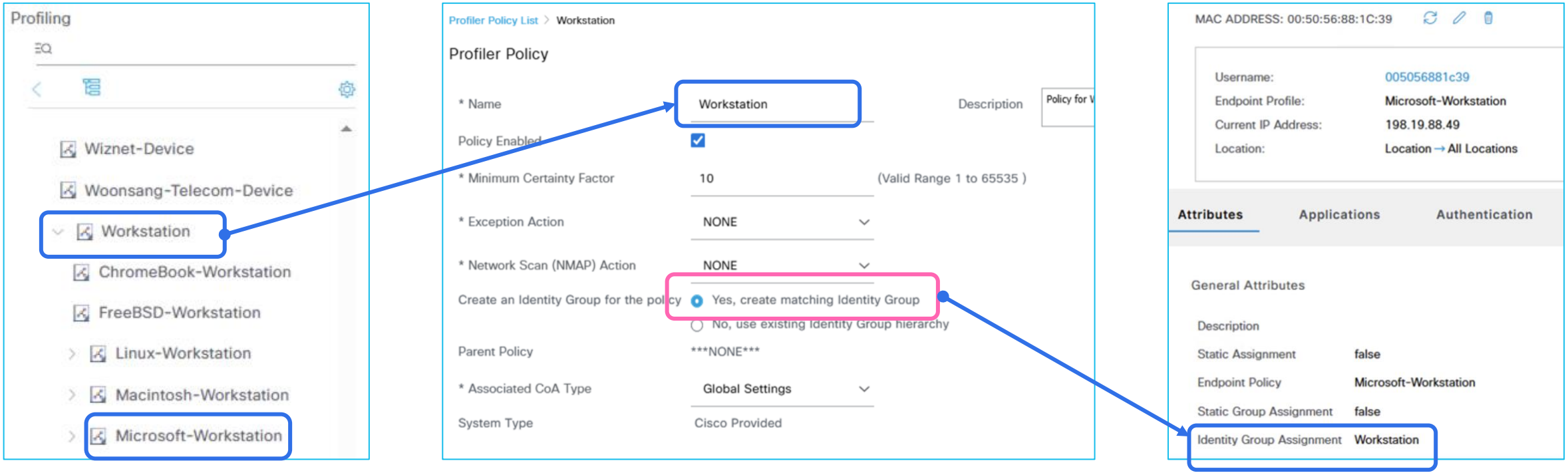
SGA options:

- Manual assignment:
  - GUI
  - API
- Dynamic assignment according to Profiling Policies

© 2026 Cisco and/or its affiliates. All rights reserved.

Static Group Assignment (SGA)

Dynamic change as a result of Classification:



© 2026 Cisco and/or its affiliates. All rights reserved.

Static Group Assignment (SGA)

When group has changed (by any method), CoA is triggered if:

- Active session for the endpoint exist on ISE
- The IdentityGroup is configured in AuthZ Policies

CoA event appears in **Live Logs**, fliter out the event by endpoint MAC and find the source and reason of the CoA

Cisco ISE

Other Attributes

ConfigVersionId	14
Event-Timestamp	1769546685
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	832c950d-4a10-41e3-9918-d03a3c9ee587
TotalAuthenLatency	20159897
ClientLatency	20159828
CoASourceComponent	Profiler
CoAReason	Change in endpoint identity group/policy/logical profile which are used in authorization policies
Network Device Profile	Cisco
Location	Location#All Locations

© 2026 Cisco and/or its affiliates. All rights reserved.

Endpoint Purge

Administration->Identity Management->Settings->Endpoint Purge

Purging Rule Structure:

Identity Groups:
- Endpoint IdentityGroup
- Profiling Policy
- Logical Profile

+

Time Condition:
- InactiveDays
- ElapsedDays
- PurgeDate

*At least one is required

+

Additional conditions from Dictionaries

*Optional

Purge routine is triggered from schedule (03:00 AM daily by default). On demand Purge option is also available:

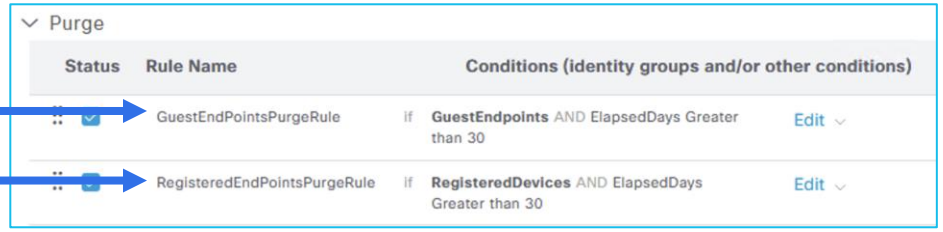


© 2026 Cisco and/or its affiliates. All rights reserved.

Endpoint Purge

Out of the box, ISE provides only two rules:

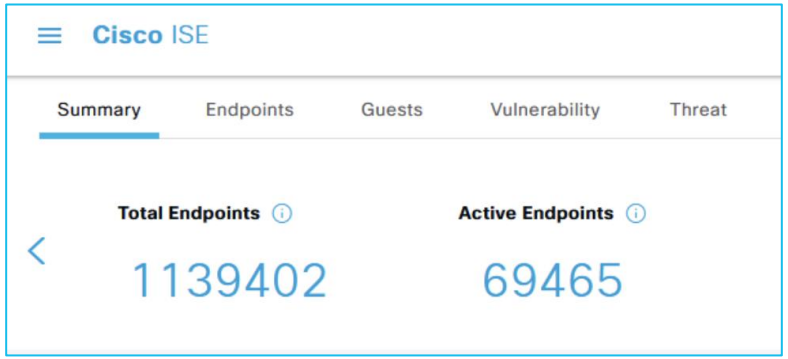
- Guest endpoints inactive for more than 30 days
- Registered endpoints inactive for more than 30 days



It's very generic, but only Administrator can set it right according to company demands.

If leave as is:

- ISE deployment accumulating millions of stale endpoint records over months/years.
- Leads to performance degradation, increased administrative overhead, and increased load on PAN and PSNs.
- Cleanup often requires TAC intervention, database scripts, and operational downtime



Recommended minimum to configure preserve rules to avoid high-volume endpoint categories that commonly accumulate in modern networks, such as:

- Unknown endpoints (not from Guest flow)
- Mobile endpoints with MAC randomisation
- Failed-authentication endpoints

© 2026 Cisco and/or its affiliates. All rights reserved.

Endpoint Purge

- ISE processes endpoints in batches during a single purging run. The batch size is 10,000 for version 3.3 and earlier, and 50,000 for version 3.4 and later. Endpoints are evaluated against the existing purging policy.
- This can take a significant amount of time when purging policy rules are “pure” and many stale endpoints already exist in the database



The endpoint purge routine runs on all nodes in the deployment

- Find endpoints owned locally by PSN1
- Read these endpoints from Endpoint cache and evaluate on Purge Policy
- If endpoint ownership entry is there but endpoint is not found in Endpoint Cache – check in DB (PAN)

- PAN takes responsibility of running purge routine on:
  - PSNs with Profiling service disabled.
  - Endpoint is not found locally in owner’s cache
- PAN pick endpoints for Purging Policy evaluation in following order:
  - Endpoint cache
  - Context Visibility
  - Database

© 2026 Cisco and/or its affiliates. All rights reserved.

Problem Diagnostic

Problem definition and sympthoms

Problems with Profiler service itself:

- **Reduced Visibility** – Administrators may see incomplete or outdated endpoint profiling information in the ISE dashboard
- **Delayed Profiling** – New endpoint profiling data cannot be processed immediately, causing delays in endpoint classification
- **Possible Policy Mismatches** – Since profiling feeds into authorization policies, incorrect or outdated endpoint profiles might result in devices being assigned the wrong network access policies



System specific issues:

- Too many replication events in the deployment
- ISE node resources under high usage
- High replication activity
- ISE node(s) marked as out-of-sync in deployment
- ISE App. Crash with events of "java.lang.OutOfMemoryError: Metaspace”
- High Authentication Latency

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

What questions do I need to ask?

Gathering the maximum amount of context about the problem is the most effective and fastest way to solve it

- **WHO** is affected?
  - One user/Group of users/All users
- **WHERE** the problem seen?
  - One location/Multiple locations/All
  - On every ISE node or specific node(s)
- **WHICH** services affected besides Profiling?
- **WHEN** is this happening?
  - All the time?
  - Specific time (morning/noon/peak-traffic time)?
- **SINCE WHEN** the issue observed

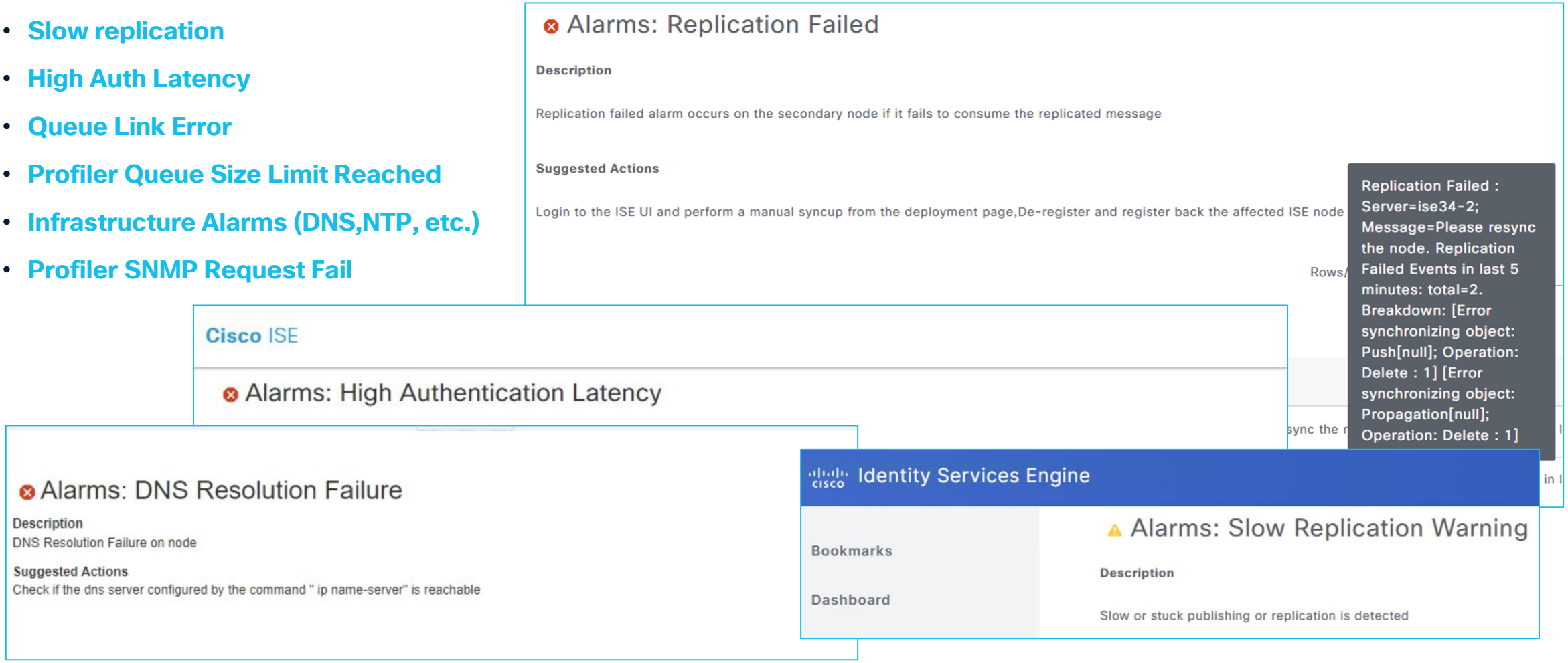
- **HAS** anything changed?
  - Infrastructure changes
  - ISE/NAD/Network Configuration changes
  - Deployment changes: add/remove nodes, any Persona/PSN services changes for existing nodes
  - Upgrades, patch installations happened recently
- **CAN** the problem be reproduced?

© 2026 Cisco and/or its affiliates. All rights reserved.

Where should I look for: Alarms

ISE Dashboard> Alarms

- **Replication Failed**
- **Slow replication**
- **High Auth Latency**
- **Queue Link Error**
- **Profiler Queue Size Limit Reached**
- **Infrastructure Alarms (DNS,NTP, etc.)**
- **Profiler SNMP Request Fail**

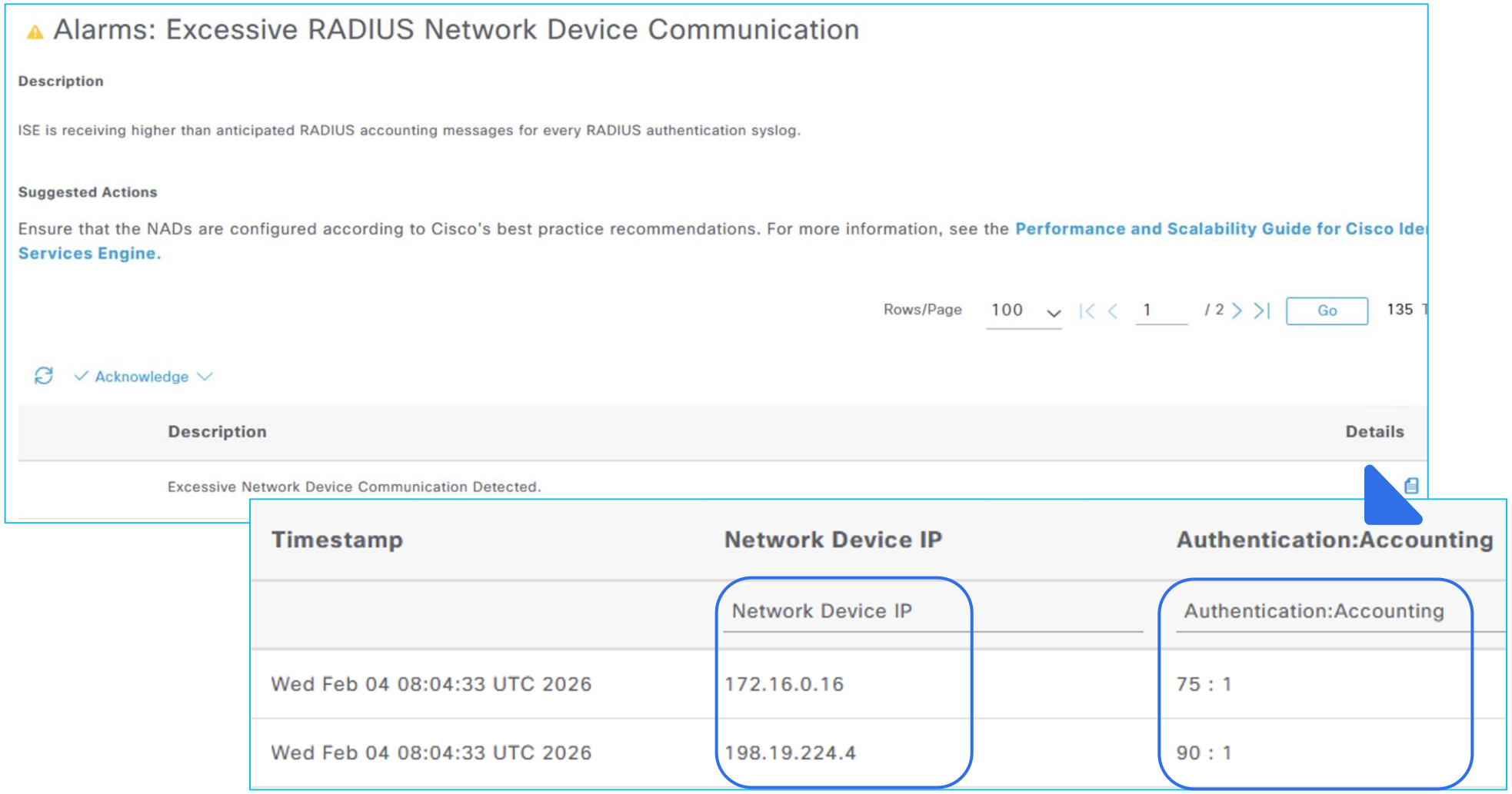


© 2026 Cisco and/or its affiliates. All rights reserved.

Where should I look for: Alarms

ISE Dashboard> Alarms

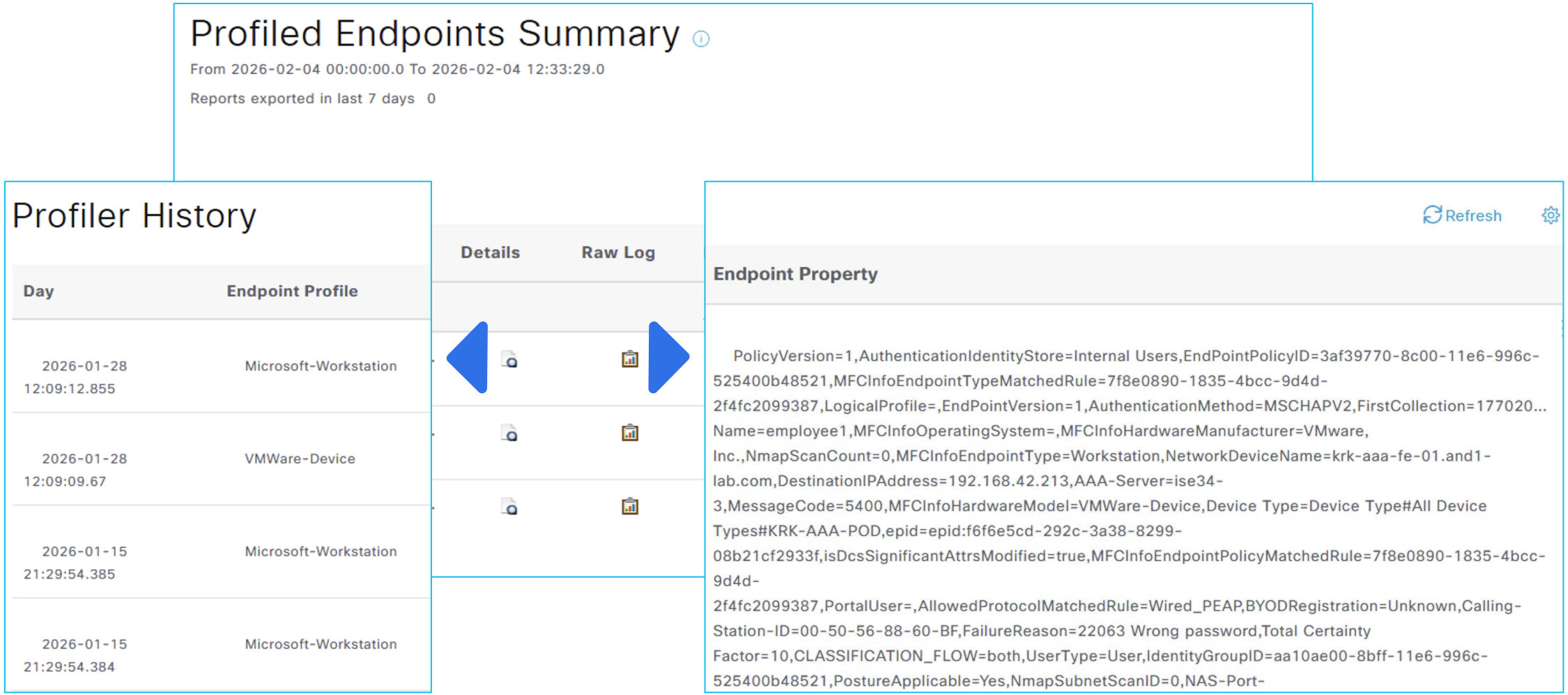
- **Excessive RADIUS Network Device Communication**



© 2026 Cisco and/or its affiliates. All rights reserved.

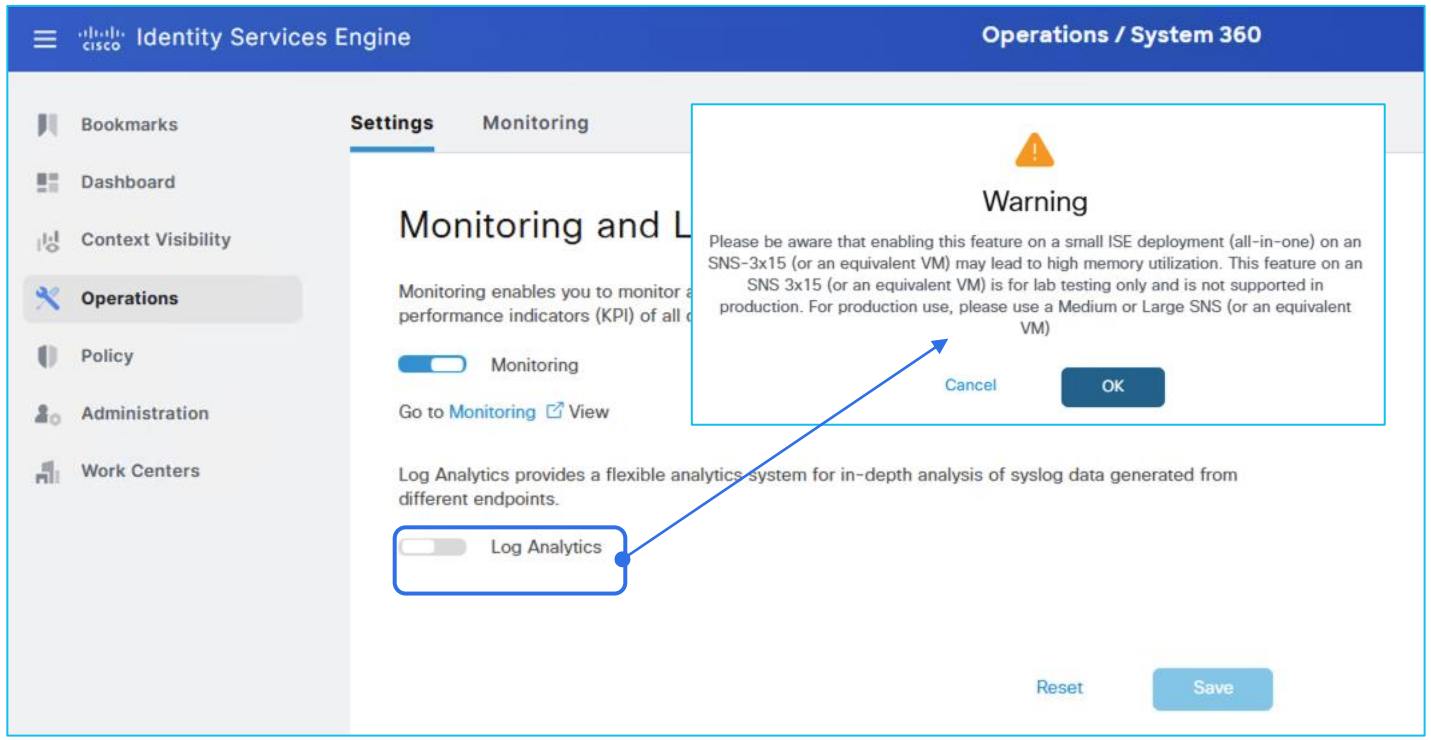
Where should I look for: Reports

Work Centers > Profiler > Reports > Reports > Profiler Endpoint Summary



© 2026 Cisco and/or its affiliates. All rights reserved.

System 360



Check previous Cisco Live sessions covering System 360 service in more details:

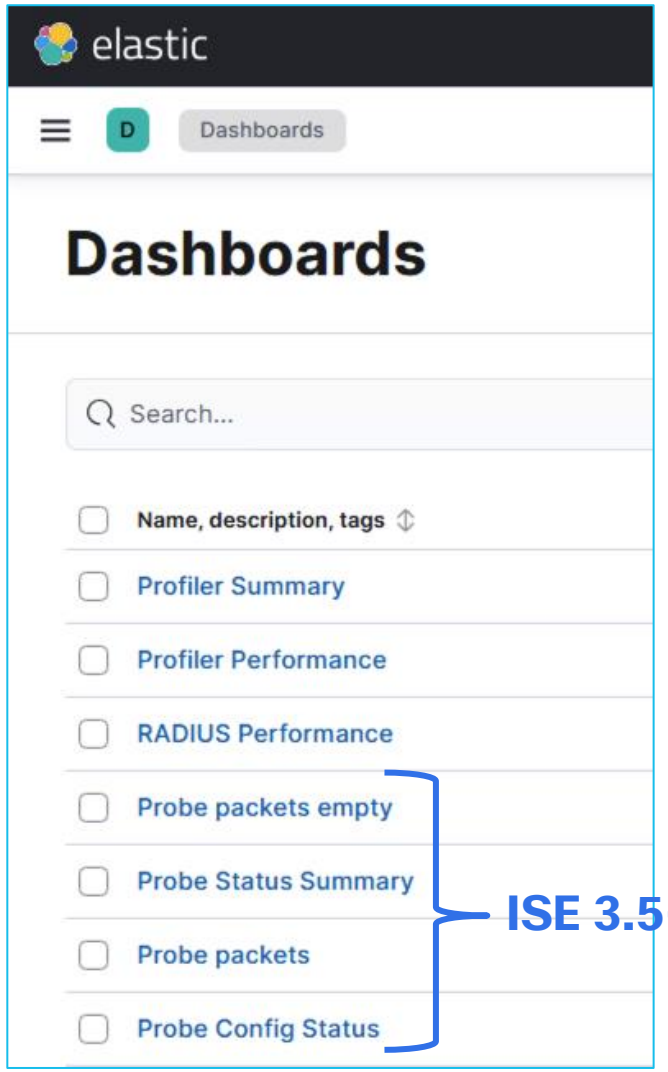
- TACSEC-2018. Identity Service Engine Log Analytics
- BRKSEC-2897. Understanding Your ISE Deployment with C.L.A.R.K

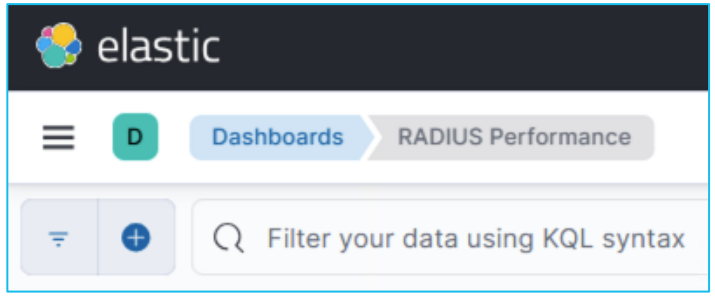
Note: Before enabling the Log Analytics service on Small and Medium deployments, mind to check the statement from ISE Performance and Scale guide:

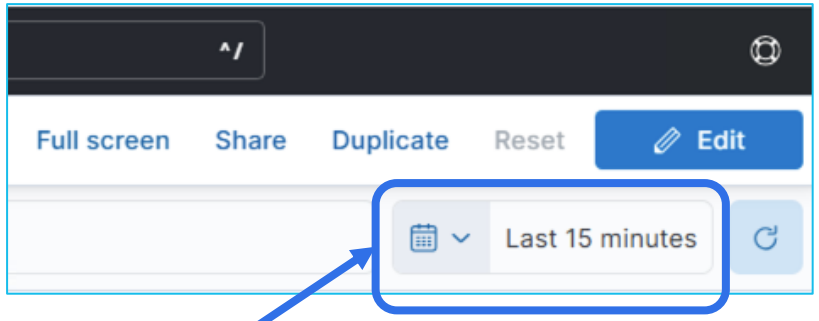
"Small and Medium deployments with a 32 GB memory instance (Cisco SNS 3615 or Cisco SNS 3715) acting as PAN/MnT are highly recommended for RADIUS or TACACS+ workloads. If your deployment includes both RADIUS and TACACS+ scaled workloads or needs advanced features that are introduced from Cisco ISE 3.2 onwards (like PxGrid Direct, PxGrid Cloud, Log Analytics, AI Profiling), it is recommended to use nodes with a minimum of 24 CPUs and 96 GB memory or more (such as Cisco SNS 3655) as PAN/MnT. These features require higher resources to function optimally."

© 2026 Cisco and/or its affiliates. All rights reserved.

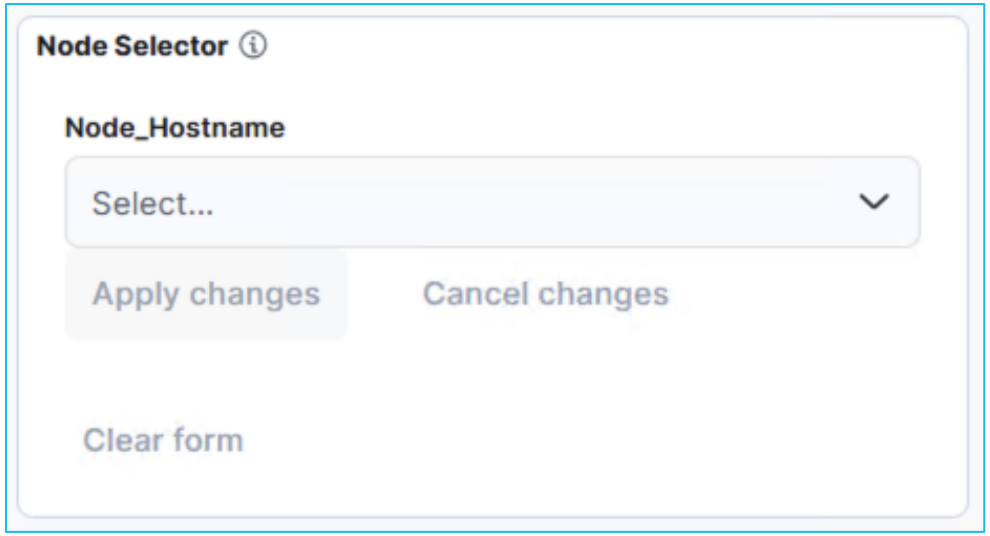
System 360





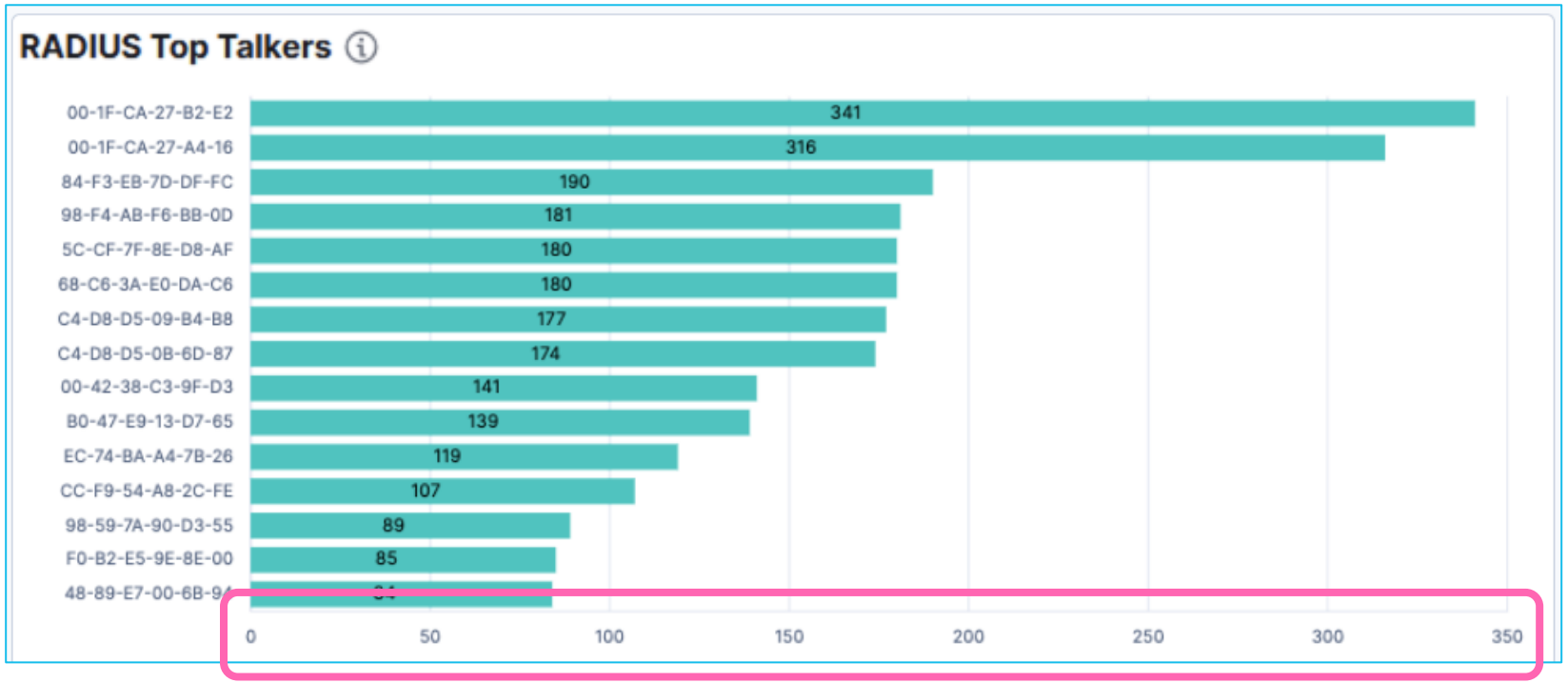


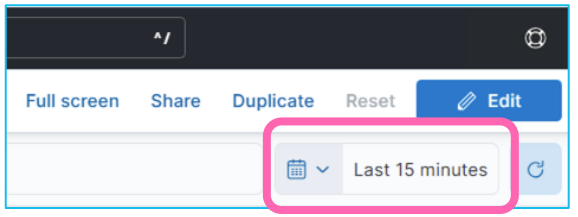
- **Select Dashboard and set timeframe**
- **Check summary analytics across all nodes in your deployment or select specific PSN:**



© 2026 Cisco and/or its affiliates. All rights reserved.

System 360 (RADIUS Performance)

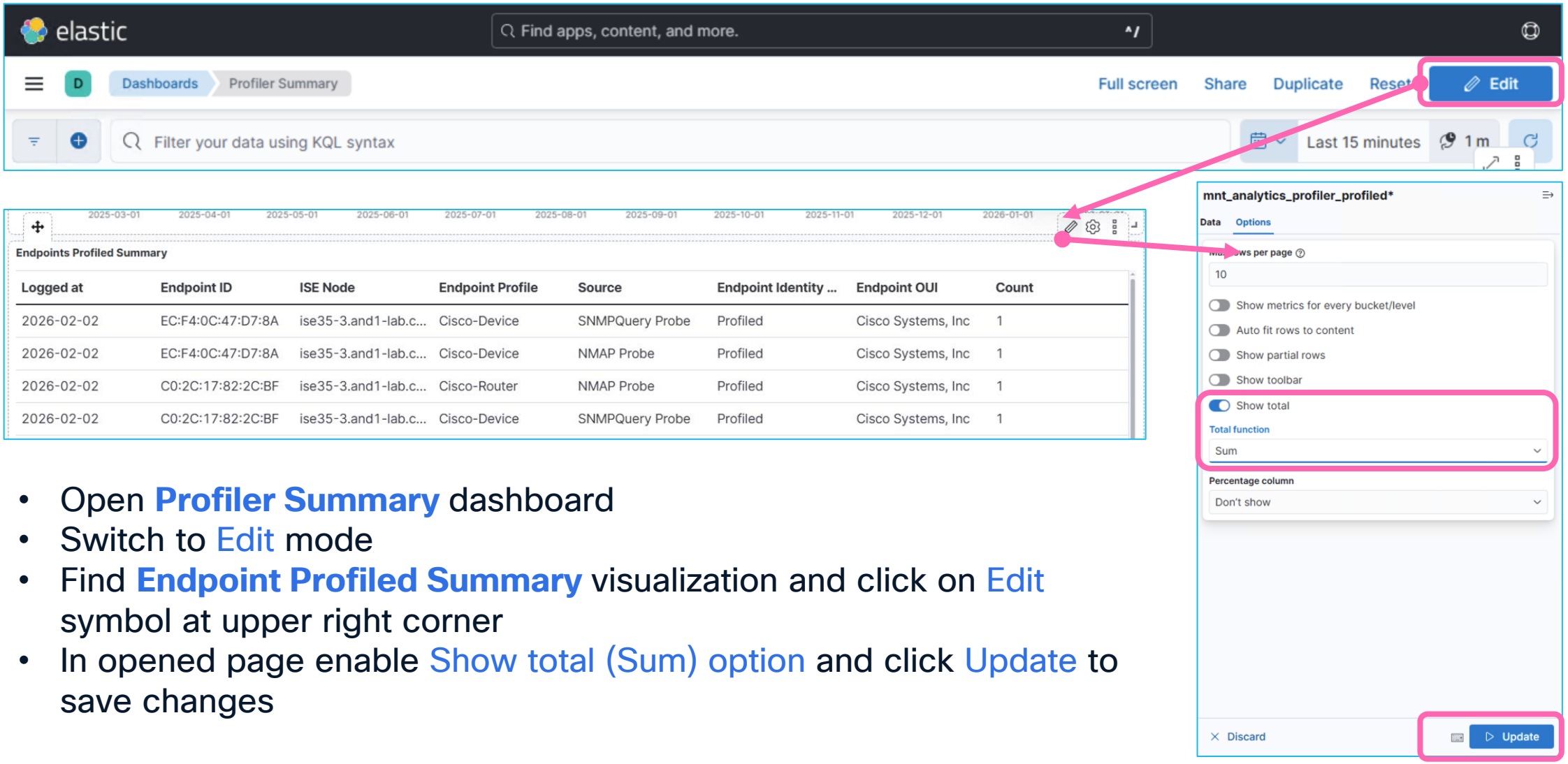




Each top talker endpoint triggered 100+ RADIUS events in last 15 minutes

© 2026 Cisco and/or its affiliates. All rights reserved.

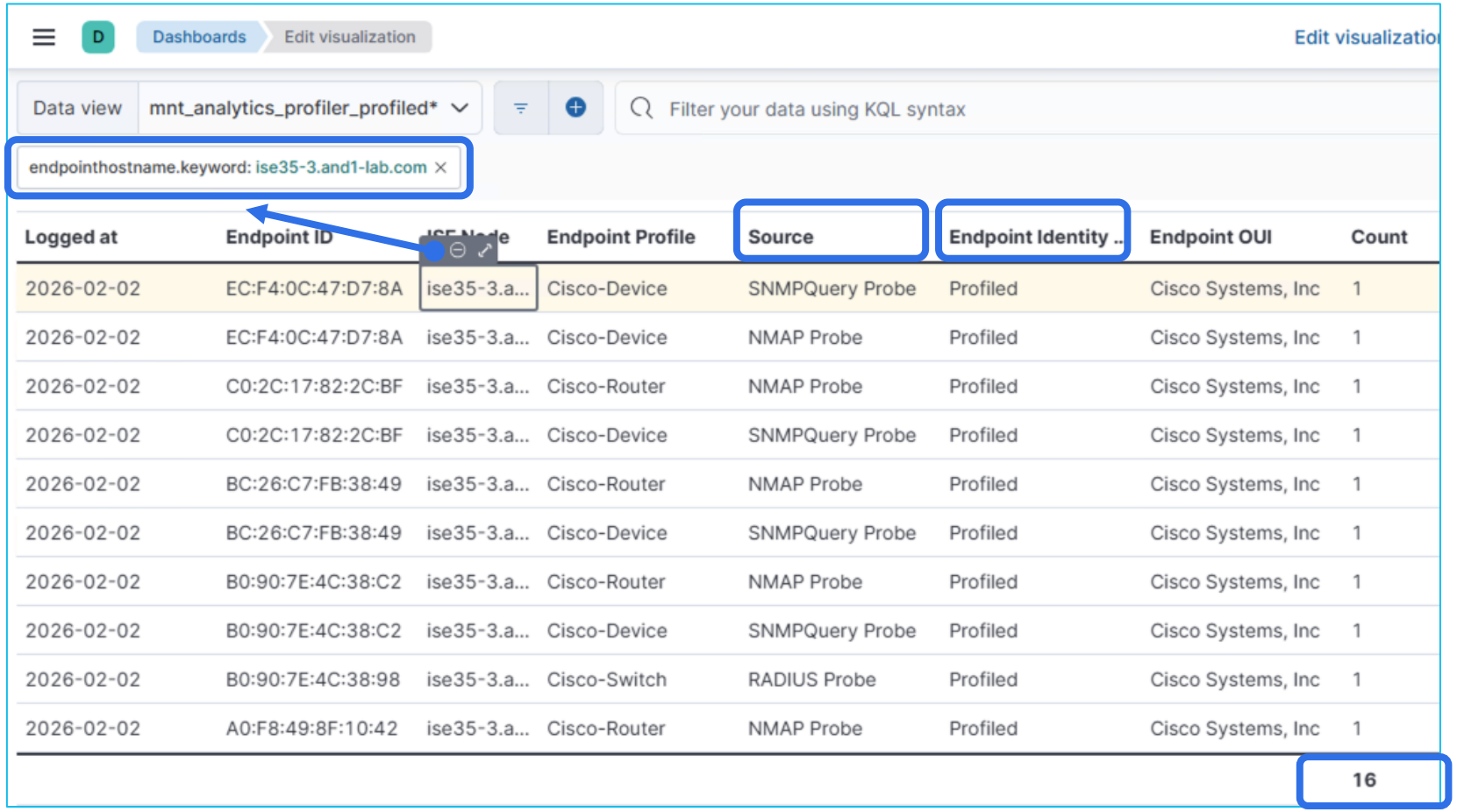
System 360 (Profiler Summary)



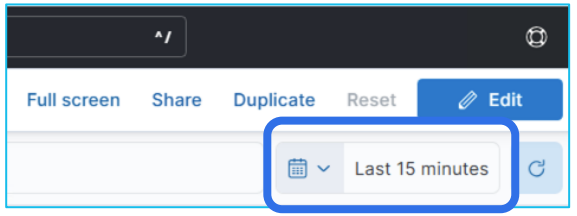
- Open **Profiler Summary** dashboard
- Switch to Edit mode
- Find **Endpoint Profiled Summary** visualization and click on Edit symbol at upper right corner
- In opened page enable Show total (Sum) option and click Update to save changes

© 2026 Cisco and/or its affiliates. All rights reserved.

System 360 (Profiler Summary)



Logged at	Endpoint ID	ISE Node	Endpoint Profile	Source	Endpoint Identity ..	Endpoint OUI	Count
2026-02-02	EC:F4:0C:47:D7:8A	ise35-3.a...	Cisco-Device	SNMPQuery Probe	Profiled	Cisco Systems, Inc	1
2026-02-02	EC:F4:0C:47:D7:8A	ise35-3.a...	Cisco-Device	NMAP Probe	Profiled	Cisco Systems, Inc	1
2026-02-02	C0:2C:17:82:2C:BF	ise35-3.a...	Cisco-Router	NMAP Probe	Profiled	Cisco Systems, Inc	1
2026-02-02	C0:2C:17:82:2C:BF	ise35-3.a...	Cisco-Device	SNMPQuery Probe	Profiled	Cisco Systems, Inc	1
2026-02-02	BC:26:C7:FB:38:49	ise35-3.a...	Cisco-Router	NMAP Probe	Profiled	Cisco Systems, Inc	1
2026-02-02	BC:26:C7:FB:38:49	ise35-3.a...	Cisco-Device	SNMPQuery Probe	Profiled	Cisco Systems, Inc	1
2026-02-02	B0:90:7E:4C:38:C2	ise35-3.a...	Cisco-Router	NMAP Probe	Profiled	Cisco Systems, Inc	1
2026-02-02	B0:90:7E:4C:38:C2	ise35-3.a...	Cisco-Device	SNMPQuery Probe	Profiled	Cisco Systems, Inc	1
2026-02-02	B0:90:7E:4C:38:98	ise35-3.a...	Cisco-Switch	RADIUS Probe	Profiled	Cisco Systems, Inc	1
2026-02-02	A0:F8:49:8F:10:42	ise35-3.a...	Cisco-Router	NMAP Probe	Profiled	Cisco Systems, Inc	1
							16

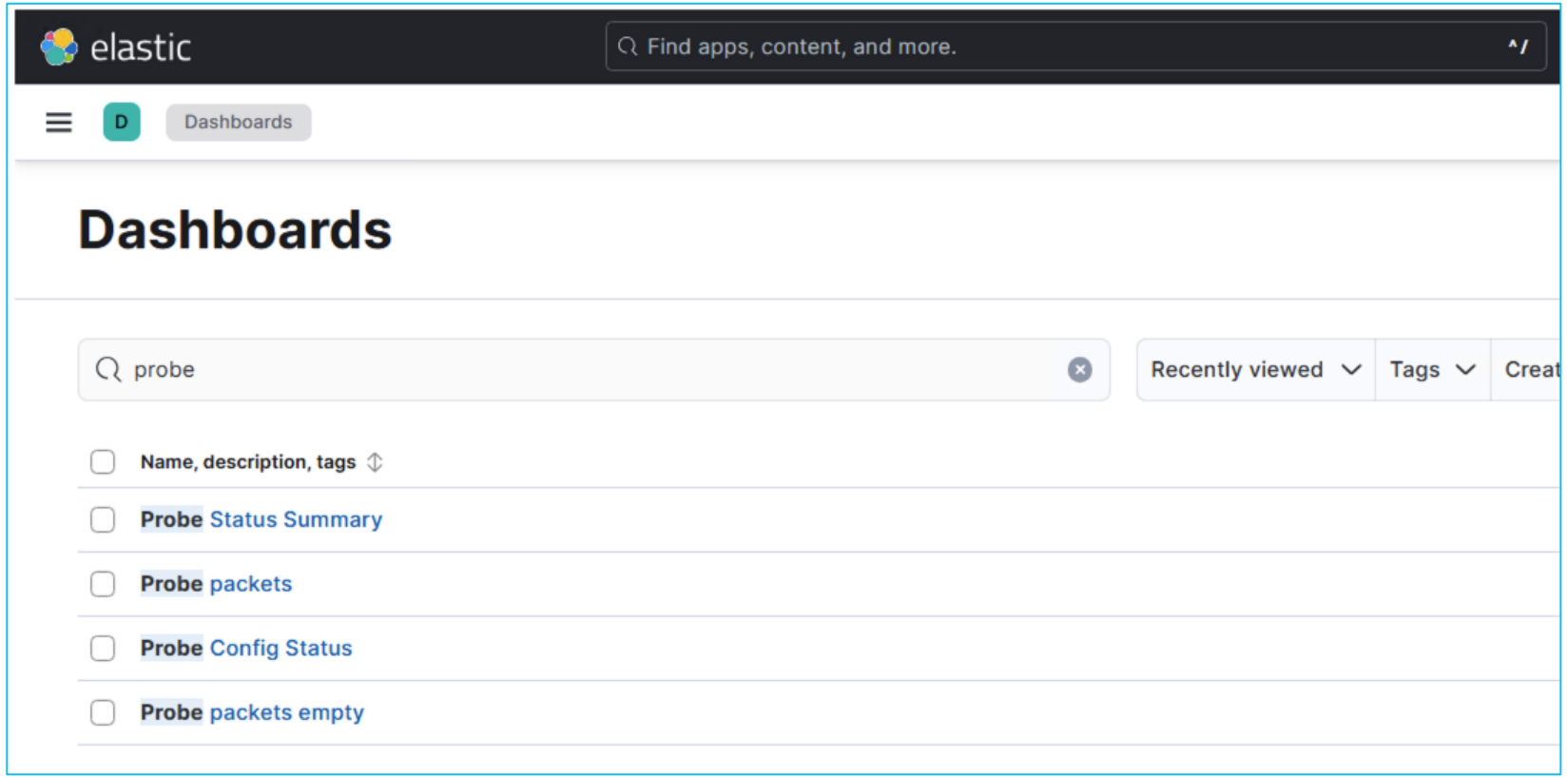


Filter on required fields to get more detailed insides within defined time frame

© 2026 Cisco and/or its affiliates. All rights reserved.

System 360 (Probe Status Summary 3.5+)

New **Probe** Dashboards:

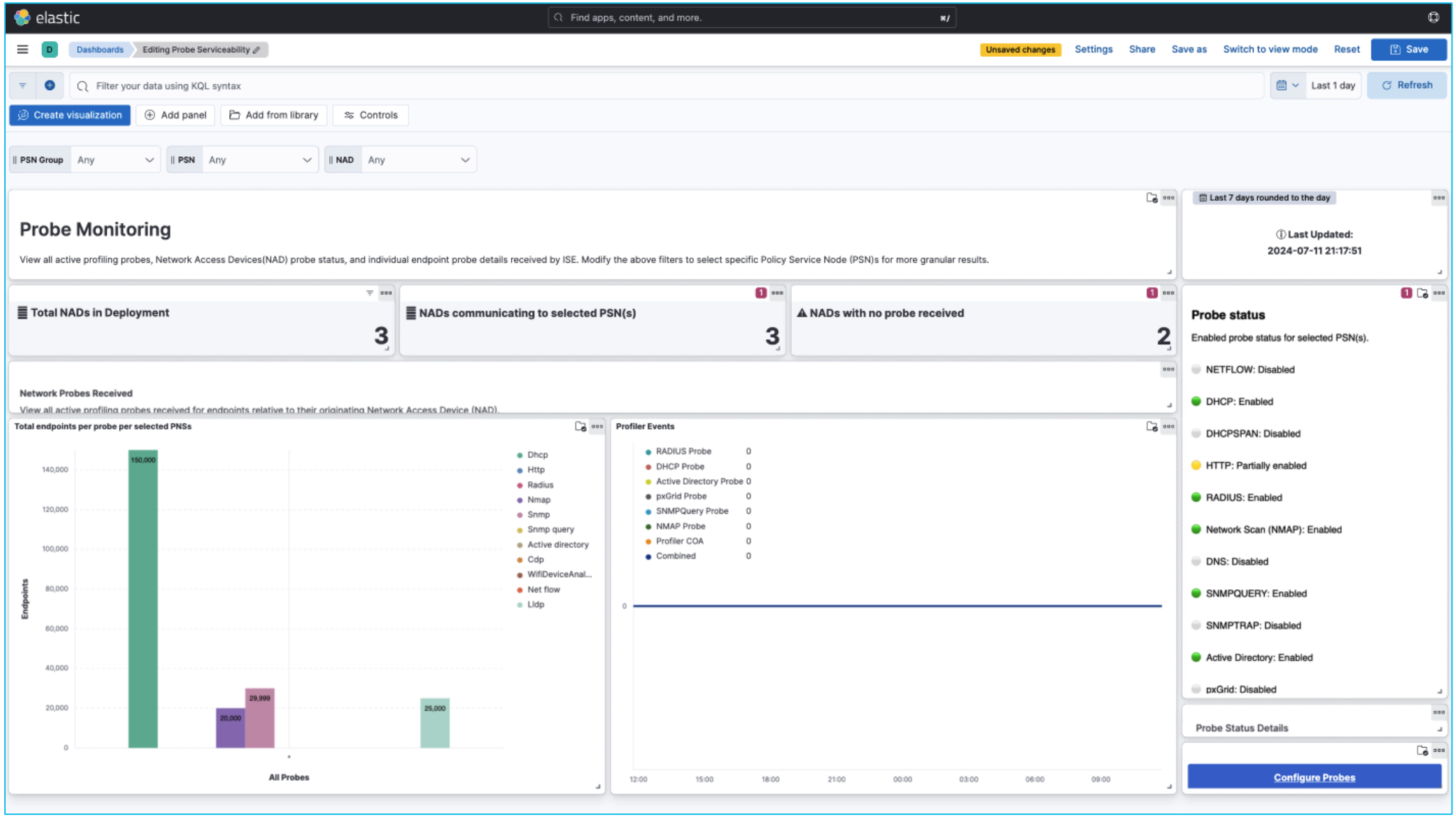


Enables more detailed insight into probe data in the ISE UI:

- Retrieves endpoint details from the endpoint cache on PSNs
- Aggregates statistics and populates dashboards, including:
  - Total count of endpoints with probes
  - Endpoint probes per NAD
  - And more

© 2026 Cisco and/or its affiliates. All rights reserved.

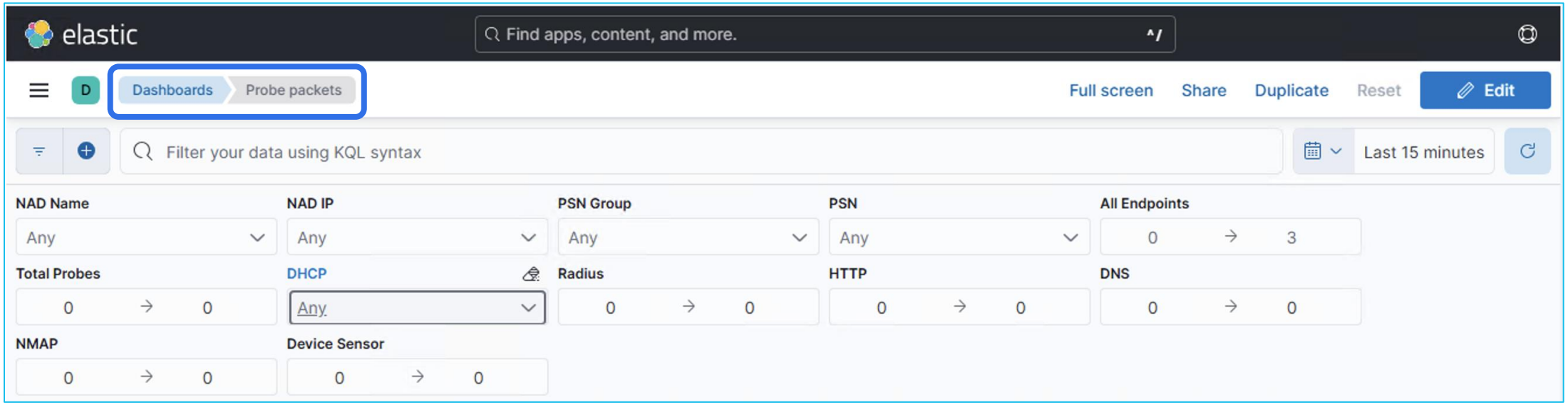
System 360 (Probe Status Summary 3.5+)

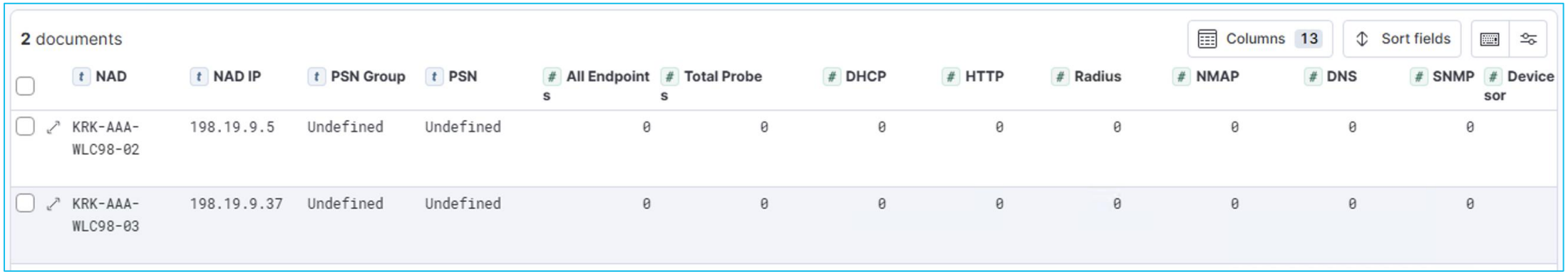


© 2026 Cisco and/or its affiliates. All rights reserved.

System 360 (Probe Status Summary 3.5+)

NAD view:



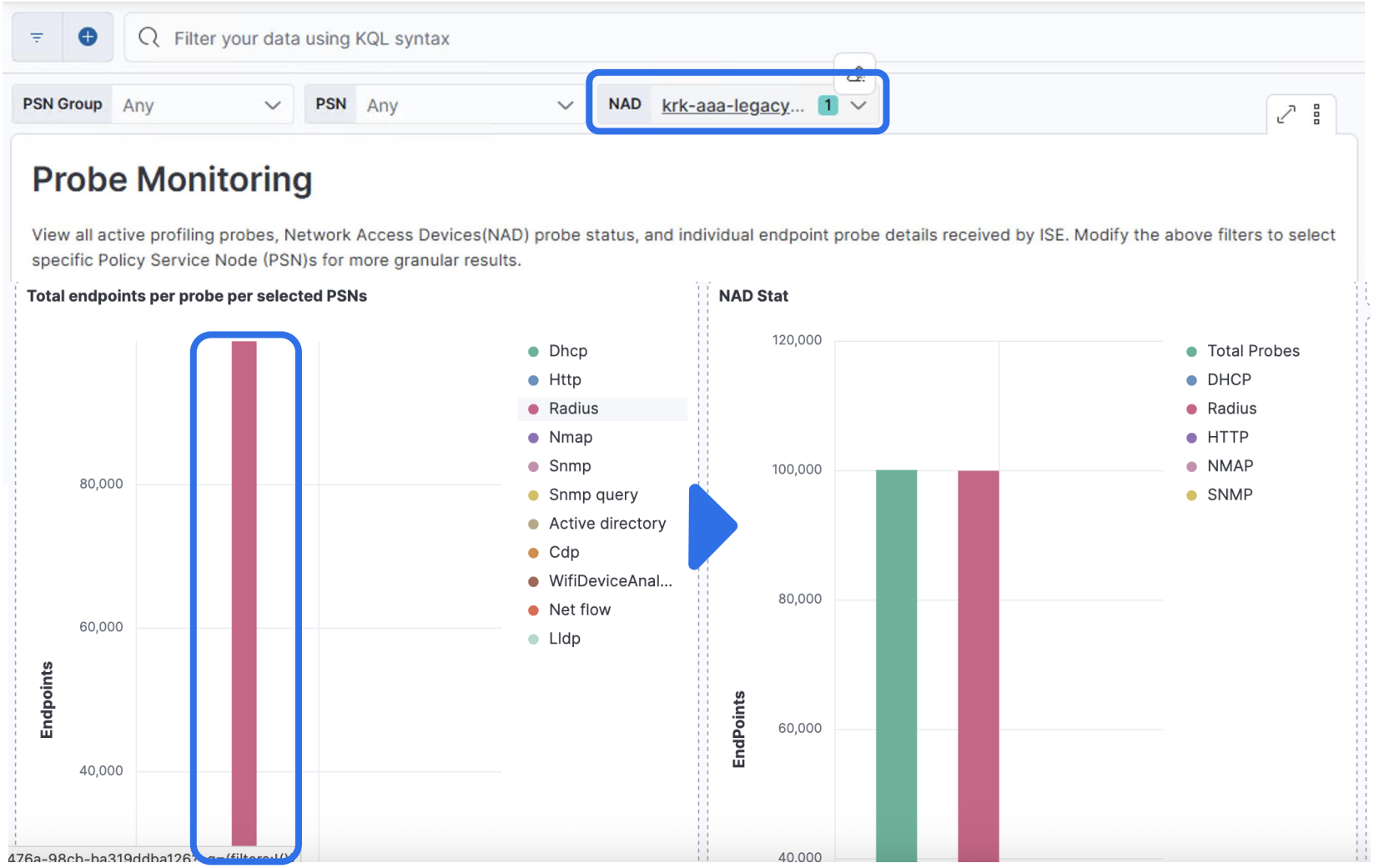


NAD	NAD IP	PSN Group	PSN	All Endpoints	Total Probes	DHCP	HTTP	Radius	NMAP	DNS	SNMP	Device sor
KRK-AAA-WLC98-02	198.19.9.5	Undefined	Undefined	0	0	0	0	0	0	0	0	
KRK-AAA-WLC98-03	198.19.9.37	Undefined	Undefined	0	0	0	0	0	0	0	0	

© 2026 Cisco and/or its affiliates. All rights reserved.

System 360 (Probe Status Summary 3.5+)

Total endpoints per probe on selected PSN view:

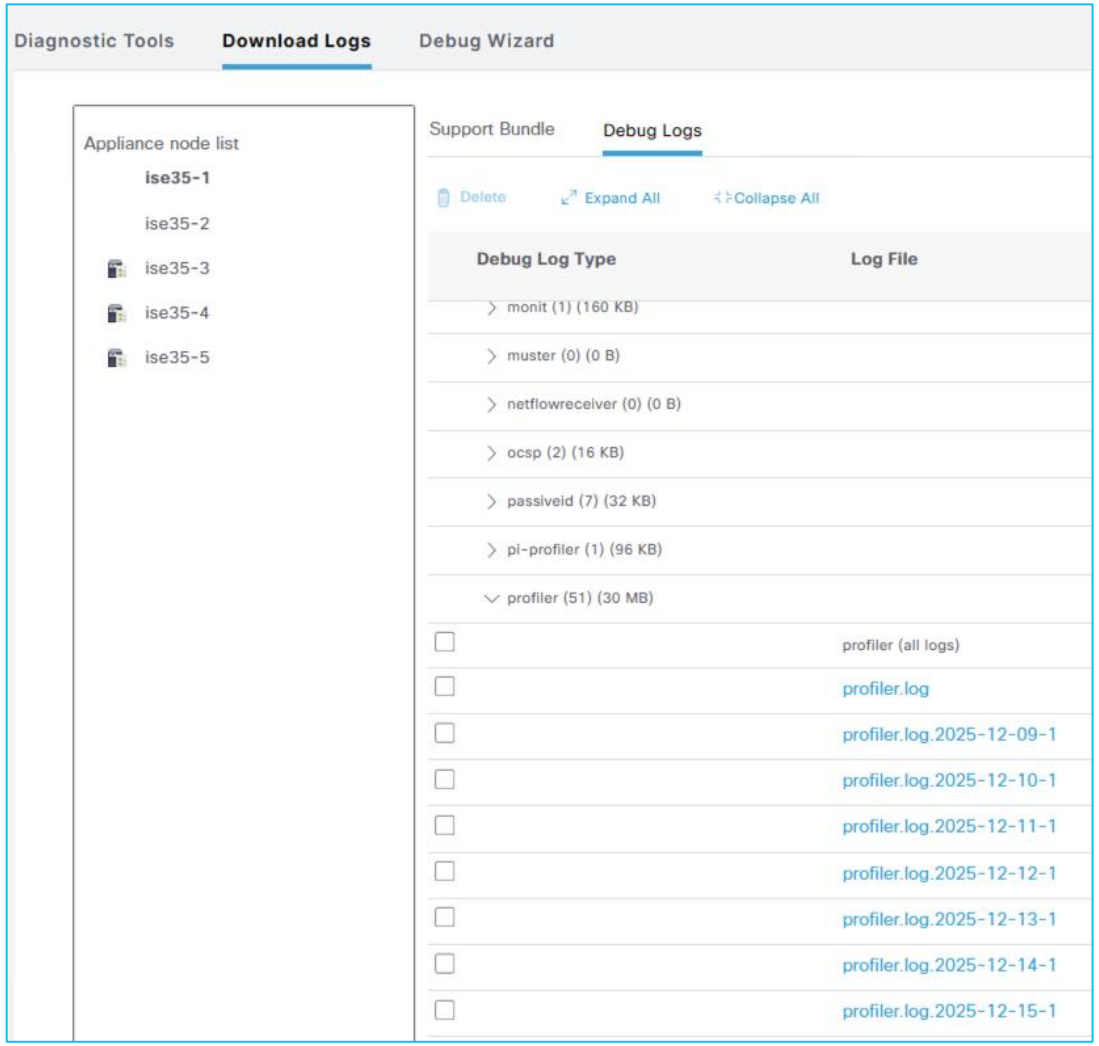


© 2026 Cisco and/or its affiliates. All rights reserved.

Where should I look for: Log files

- Two main categories:
  - **Application logs** – related to ISE applications like guest, profiler, runtime, replication, etc Available through GUI, CLI, included into the Support Bundle
  - **System Logs** – related to underlying OS and generic services (ADE, dmesg, messages, etc). Available through CLI (not all from ADE) and included into the Support Bundle
- Download log files GUI:

  Operations>Troubleshoot>Download Logs, select the node and click on Debug Logs



© 2026 Cisco and/or its affiliates. All rights reserved.

Where should I look for: Log files

CLI (ADE.OS) check:

```
ise34-1/admin#show logging application | b profiler.log
      68826 Jan 28 2026 11:50:10  ise-pi-profiler.log
     139272 Jan 13 2026 23:58:30  ise-pi-profiler.log.2026-01-13-1
     145997 Jan 14 2026 23:59:25  ise-pi-profiler.log.2026-01-14-1
     152584 Jan 15 2026 23:55:58  ise-pi-profiler.log.2026-01-15-1
     139272 Jan 16 2026 23:56:29  ise-pi-profiler.log.2026-01-16-1
     139272 Jan 17 2026 23:57:03  ise-pi-profiler.log.2026-01-17-1
     139272 Jan 18 2026 23:57:37  ise-pi-profiler.log.2026-01-18-1
     139272 Jan 19 2026 23:58:11  ise-pi-profiler.log.2026-01-19-1
     139272 Jan 20 2026 23:58:44  ise-pi-profiler.log.2026-01-20-1
     139272 Jan 21 2026 23:59:17  ise-pi-profiler.log.2026-01-21-1
```

- Filter the output, for example: *ise32-1/admin#show logging application localStore/iseLocalStore.log | include “Profiler:”*

```
ise34-3/admin#show logging application localStore/iseLocalStore.log | include Profiler:
2026-01-28 12:09:09.670 +00:00 0001319480 80002 INFO  Profiler: Profiler EndPoint profiling event occurred, ConfigVersionId=33, EndpointCertainityMetric=10, EndpointMacAddress=00:50:
56:88:1C:39, EndpointMatchedPolicy=VMWare-Device, EndpointNADAddress=198.19.254.26, EndpointOUI=VMware\, Inc., EndpointPolicy=VMWare-Device, EndpointProperty=PolicyVersion=1\,EndPoin
tPolicyID=3af39770-8c00-11e6-996c-525400b48521\,MFCInfoEndpointTypeMatchedRule=7f8e0890-1835-4bcc-9d4d-2f4fc2099387\,LogicalProfile=\,EndPointVersion=1\,AuthenticationMethod=Lookup\,
FirstCollection=1769602149635\,CacheUpdateTime=1769602149664\,StaticAssignment=false\,User-Name=005056881c39\,MFCInfoOperatingSystem=\,MFCInfoHardwareManufacturer=VMware\, Inc.\,Nmap
ScanCount=0\,MFCInfoEndpointType=Workstation\,NetworkDeviceName=krk-aaa-legacy-sw-06\,DestinationIPAddress=192.168.42.213\,AAA-Server=ise34-3\,MessageCode=5200\,MFCInfoHardwareModel=
VMWare-Device\,Device Type=Device Type#All Device Types#KRK-AAA-POD\,epid=epid:a505e14e-2da7-373a-85c2-179464ea8c86\,isDcsSignificantAttrsModified=true\,MFCInfoEndpointPolicyMatchedR
ule=7f8e0890-1835-4bcc-9d4d-2f4fc2099387\,PortalUser=\,AllowedProtocolMatchedRule=Default\,BYODRegistration=Unknown\,Calling-Station-ID=00-50-56-88-1C-39\,FailureReason=-\,Total Cert
ainty Factor=10\,CLASSIFICATION_FLOW=both\,IdentityGroupID=aa10ae00-8bff-11e6-996c-525400b48521\,PostureApplicable=Yes\,NmapSubnetScanID=0\,NAS-Port-Type=Ethernet\,TimeToProfile=25\,
DeviceRegistrationStatus=NotRegistered\,MFCInfoEndpointPolicy=VMWare-Device\,MFCInfoHardwareManufacturerMatchedRule=7f8e0890-1835-4bcc-9d4d-2f4fc2099387\,MatchedPolicyID=3af39770-8c0
0-11e6-996c-525400b48521\,MFCInfoOperatingSystemMatchedRule=\,SSID=80-90-7E-4C-38-86\,UserName=00-50-56-88-1C-39\,FeedService=false\,CreateTime=1769602149668\,MFCInfoHardwareModelMat
chedRule=7f8e0890-1835-4bcc-9d4d-2f4fc2099387\,UseCase=Host Lookup\,SelectedAuthorizationProfiles=PermitAccess\,StaticGroupAssignment=false\,NAS-Port-Id=GigabitEthernet1/0/6\,DTLSSup
port=Unknown\,LastActivity=1769602149635\,Response=\{User-Name=00-50-56-88-1C-39\; Class=CACS:1A0113C600000C100478AAB1:ise34-3/557841593/51430\; cisco-av-pair=cts:security-group-tag=
001b-03\; LicenseTypes=1\; \}\,LastNmapScanTime=0\,UpdateTime=0\,AuthorizationPolicyMatchedRule=CTS_POD8\,Location=Location#All Locations, EndpointSourceEvent=RADIUS Probe, EndpointI
dentityGroup=Profiled, ProfilerServer=ise34-3.and1-lab.com,
```

- tail is available at the end (same as “tail -f” in Linux)

© 2026 Cisco and/or its affiliates. All rights reserved.

Debug Guidelines

- **Do NOT enable DEBUG (unless explicitly requested by TAC) if:**
  - Resource consumption on the ISE node is extremely high.
  - The issue is intermittent and cannot be reproduced during troubleshooting.
  - There is uncertainty regarding which components require debugging, and no relevant clues have been identified.
- **Enable DEBUG only if all the above conditions are FALSE, and:**
  - Clearly specify the components to be debugged; avoid enabling DEBUG broadly or without a targeted purpose.
  - Run DEBUG for the minimum necessary duration and immediately revert severity levels to their default settings after successfully reproducing the issue

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Files to grab/verify

Filename	Comments
iselocalstore.log	Out of the box contain plenty of information about profiling, radius, posture, mdm, system events and counters, etc. Contain failed and successful events. Most important set of files for retrospective problem investigation
profiler.log	Main log file for Profiler component on ISE. When enabled in DEBUG, provides low level diagnostic information but fill size quote pretty much fast, hence overwrite diagnostic information. Make sense if PSN is processing big amount of data.
ise-psc.log	Worth to check if MDM, Posture services engaged into the flow
prrt-server.log	Logs from RADIUS service on ISE
replication.log	If replication related alamrs appears on ISE Dashboard, worth to check details in this file, even with INFO level (default) it provides Global Replication details and track failure events
ea.log	If Endpoint AI Analytics is engaged
lsd.log	LDD service logs

© 2026 Cisco and/or its affiliates. All rights reserved.

Conclusion

Key takeaways

- Endpoint Attribute Types:
  - *Significant*: Database consistent; triggers persistency
  - *Whitelisted*: Attributes permitted in profiling policies
  - *Custom*: Manually created or received via PxGrid probe; added to whitelist if configured in profiling policies
  - *Other*: Filtered out; does not trigger classification
- Each endpoint is assigned an owner—an ISE node responsible for maintaining the complete set of endpoint attributes
- The LDD framework consists of a session cache, owner cache, and message broker. Stores abbreviated information about session and the owning ISE node for each endpoint
- Endpoint cache – Separate on each PSN. Stores full endpoint information in the Endpoint Cache. Used by PSNs to make policy decisions
- Keep EP replication disabled unless explicitly advised (automatically enabled when LDD is disabled)
- If EP replication has not been previously enabled and must be activated, manually synchronize ISE nodes with the PAN
- RADIUS and HTTP probes continuously supplies the Profiler with all incoming updates even if Profiling service is disabled on the node

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Recommendations

- Always use the latest recommended ISE versions and patches to ensure up-to-date fixes
- Avoid Load-balance persistency issues—endpoint stickiness is essential.
- Prevent sudden floods of profiling updates. More endpoints, attribute updates increase profiler operations, which can bottleneck ISE scalability and performance
- Avoid aggressive profiling policies: do not overcomplicate with excessive rules, conditions, or custom attributes not used for asset classification. Prevent duplicate profiler probe information
- Address infrastructure concerns: avoid network latency between ISE nodes greater than 300ms, ensure proper DNS resolution, and verify required port availability if firewalls are present between ISE nodes
- Monitor the total number of endpoints on ISE. Set custom purging rules based on requirements and preserve common high-volume endpoint categories

© 2026 Cisco and/or its affiliates. All rights reserved.

Complete your session surveys



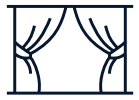
Complete your surveys in the Cisco Events App.



Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

© 2026 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

Contact me at: abubnov@cisco.com

© 2026 Cisco and/or its affiliates. All rights reserved.

Thank you

cisco Live !


CISCO