Deploy ISE Posture

Contents

Introduction

This document describes some baseline configurations that address several use cases with redirection-based posture.

Restrictions

The configurations in this document work for Cisco NADs, but not necessarily for third party NADs.

Posture Client Behavior

The posture client can trigger probes at these times:

- Initial login
- Layer 3 (L3) change/Network Interface Card (NIC) change (new IP address, NIC state change)

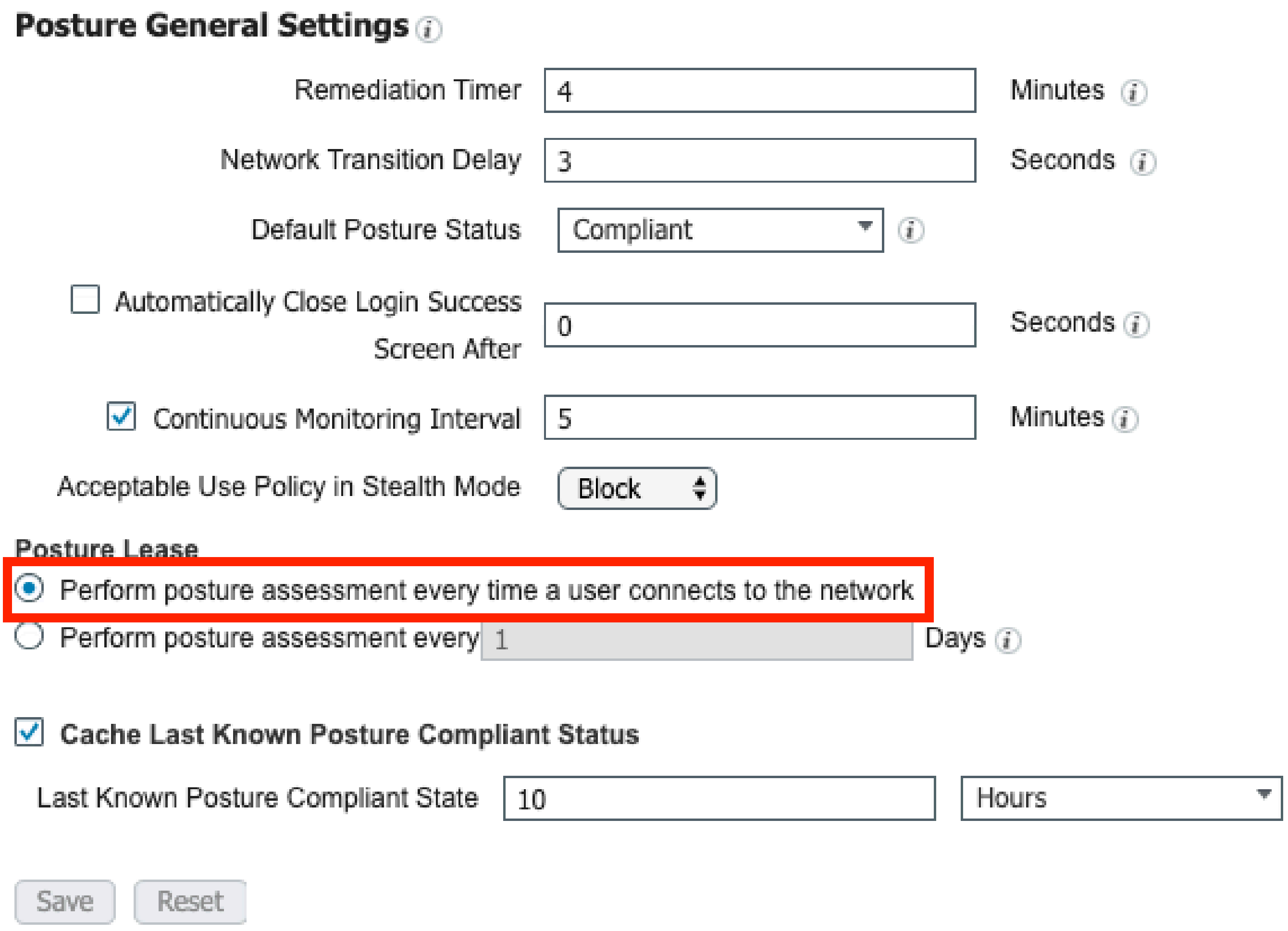
Use Cases

Use Case 1 - Client reauthentication forces the NAD to generate a new session ID.

In this use case, the client is still compliant, but because of reauthentication, the NAD is in the redirect state (redirect URL and access list).

By default, Identity Services Engine (ISE) is configured to perform a posture assessment every time that it connects to the network, more specifically for each new session.

This setting is configured under Work Centers > Posture > Settings > Posture General Settings.



Posture General Settings

Remediation Timer: 4 Minutes

Network Transition Delay: 3 Seconds

Default Posture Status: Compliant

□ Automatically Close Login Success Screen After: 0 Seconds

☑ Continuous Monitoring Interval: 5 Minutes

Acceptable Use Policy in Stealth Mode: Block

Posture Lease

● Perform posture assessment every time a user connects to the network

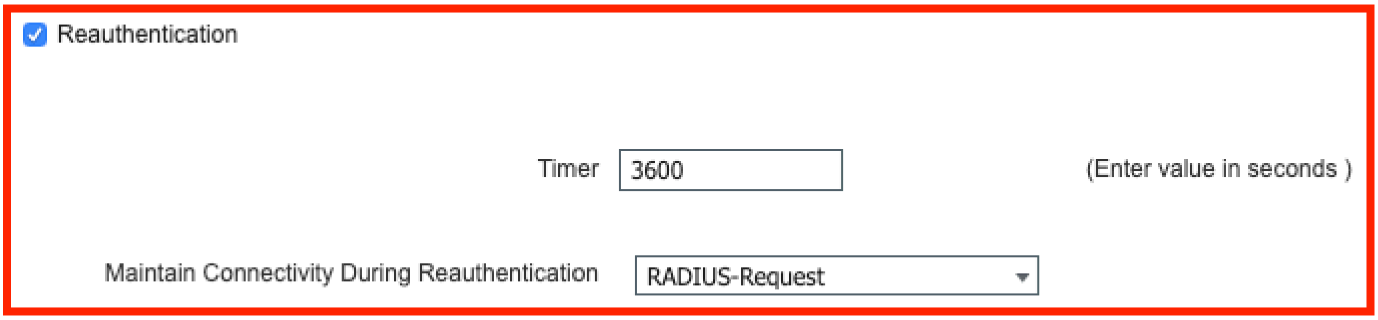
○ Perform posture assessment every 1 Days

☑ **Cache Last Known Posture Compliant Status**

Last Known Posture Compliant State: 10 Hours

In order to keep the NAD from generating a new session ID on reauthentication, configure these reauthentication values in the authorization profile. The reauthentication timer displayed is not a standard recommendation and consider reauthentication timers per deployment based on connection type (wireless/wired), design (what are the persistence rules on the loadbalancer), and so on.

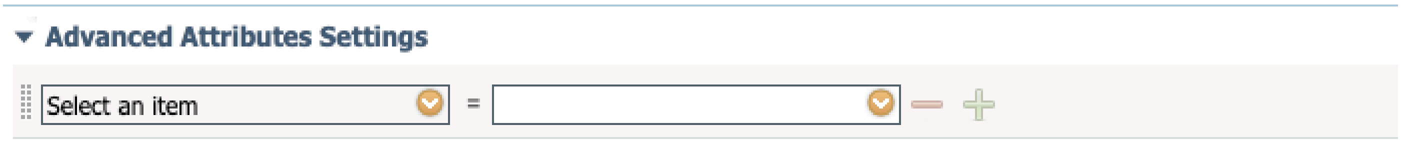
Policy > Policy Elements > Results > Authorization > Authorization Profiles



☑ Reauthentication

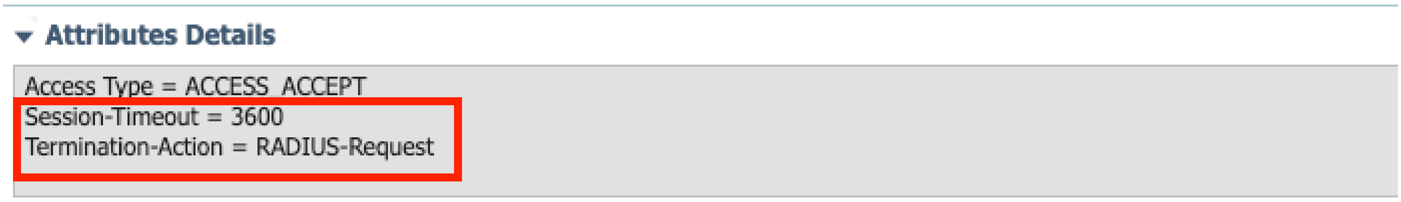
Timer 3600 (Enter value in seconds)

Maintain Connectivity During Reauthentication RADIUS-Request



Advanced Attributes Settings

Select an item =



Attributes Details

Access Type = ACCESS_ACCEPT
Session-Timeout = 3600
Termination-Action = RADIUS-Request

On switches, you need to configure each interface, or template, to get its reauthentication timer from ISE.

```
authentication timer reauthenticate server
```

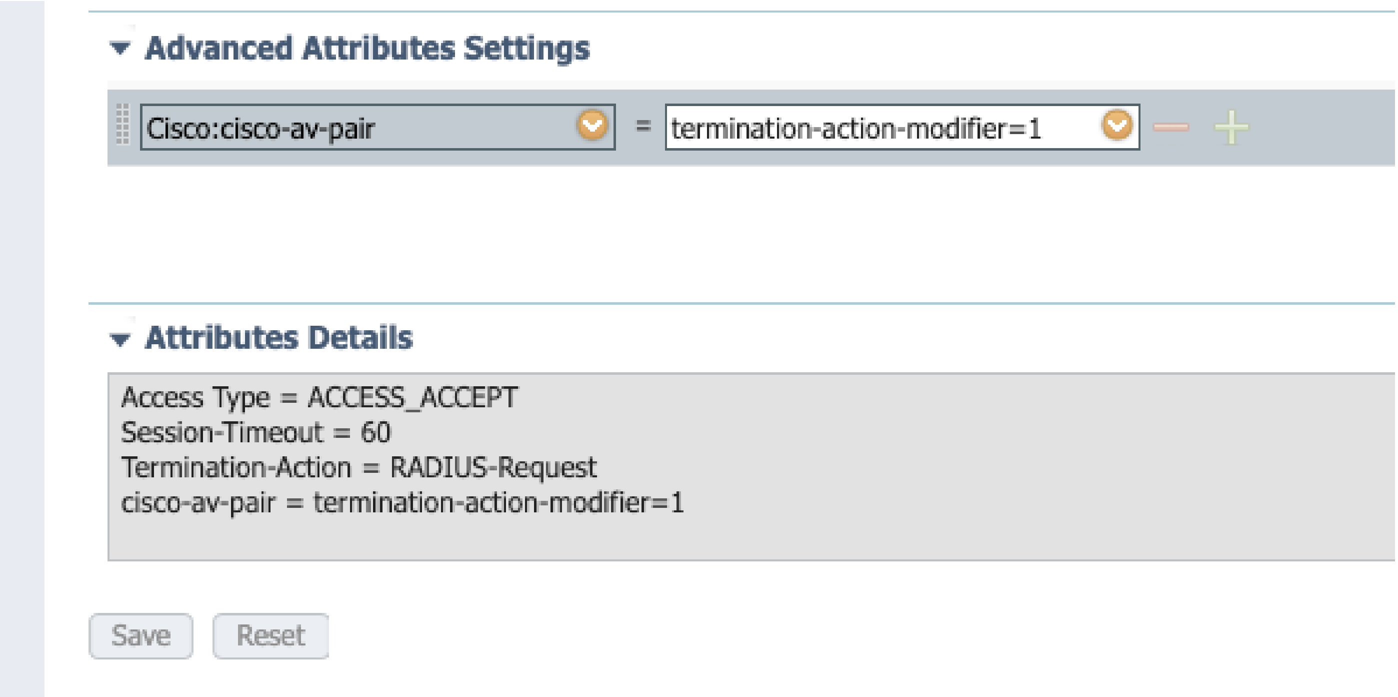
Note: If there is a load balancer, you need to make sure that persistance is configured in a way that reauthentications can be returned to the original Policy Service (PSN).

Use Case 2 - The switch is configured with order MAB DOT1X and priority DOT1X MAB (Wired).

In this case reauthentications can be terminated, because an accounting stop for the 802.1x session can be sent when MAC Authentication Bypass (MAB) is attempted during reauthentication.

- The accounting stop that is sent for the MAB process when it fails authentication is correct, as the username for the client changes from the 802.1X username to the MAB username.
- Dot1x as the method-id in the accounting stop is also correct as the authorizing method was dot1x.
- When Dot1x method succeeds, it sends an accounting start with method-id as dot1x. Here as well, this behavior is as expected.

In order to resolve this issue, configure the cisco-av-pair:termination-action-modifier=1 on the authZ profile used when an endpoint is compliant. This attribute-value (AV) pair specifies that the NAD reuses the method chosen in the original authentication regardless of the configured order.



Cisco:cisco-av-pair = termination-action-modifier=1

```
Access Type = ACCESS_ACCEPT
Session-Timeout = 60
Termination-Action = RADIUS-Request
cisco-av-pair = termination-action-modifier=1
```

Use Case 3 - Wireless clients roam and authentications for different APs are going to different controllers.

For this situation, the wireless network needs to be designed so that the access points (APs) within reach to other APs for roaming use the same active controller. One example is Wireless LAN Controller (WLC) stateful switchover (SSO) failover. For more information about High Availability (HA) SSO for WLC, see High Availability (SSO) Deployment Guide.

Use Case 4 - Deployments with load balancers (Pre 2.6 Patch 6, 2.7 Patch P2, and 3.0).

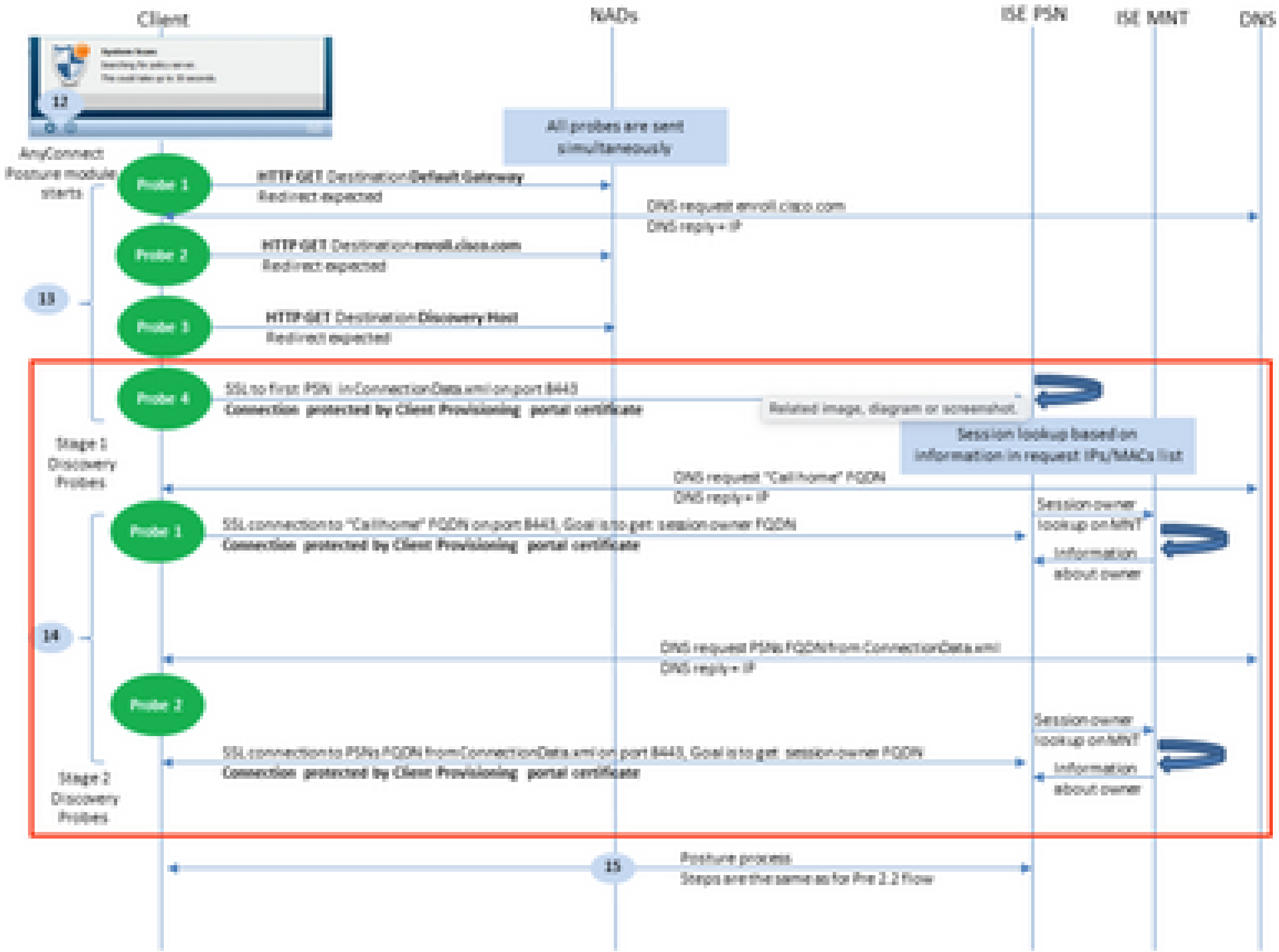
In deployments with load balancers involved, it is important to make sure that after you make the changes in the previous use cases, the sessions continue to go to the same PSN. Prior to the version/patches listed for this step, posture status is not replicated between the nodes via Light Data Dirstribution (formerly Light Session Directory). Because of this, it is possible for different PSNs to return different posture status results.

If persistance is not configured correctly, sessions that reauthenticate could go to a different PSN than the one that was originally used. If this happens, the new PSN could mark the sessions compliance status as unknown and pass the authZ result with the redirect access control list (ACL)/URL and limit the endpoints access. Again, this change on the NAD would not be recognized by the posture module and probes would not be triggered.

For more information on how to configure load balancers, see Cisco & F5 Deployment Guide: ISE Load Balancing Using BIG-IP. It provides a high level overview and F5 specific configuration of a best practice design for ISE deployments in a load balanced environment.

Use Case 5 - Stage 2 discovery probes are responsed to by a different server than the client is authenticated with (Pre 2.6 Patch 6, 2.7 Patch 2, and 3.0).

Take a look at the probes within the red box in this diagram..


Client
NADs
ISE PSN
ISE MNT
DNS
12
AnyConnect Posture module starts
All probes are sent simultaneously
Probe 1
HTTP GET Destination Default Gateway
Redirect expected
DNS request enroll.cisco.com
DNS reply= IP
Probe 2
HTTP GET Destination enroll.cisco.com
Redirect expected
13
Probe 3
HTTP GET Destination Discovery Host
Redirect expected
Probe 4
SSL to first PSN in ConnectionData.xml on port 8443
Connection protected by Client Provisioning portal certificate
Related image, diagram or screenshot.
Session lookup based on information in request IPs/MACs list
Stage 1 Discovery Probes
DNS request "Callhome" FQDN
DNS reply= IP
Probe 1
SSL connection to "Callhome" FQDN on port 8443, Goal is to get session owner FQDN
Connection protected by Client Provisioning portal certificate
Session owner lookup on MNT
Information about owner
14
DNS request PSNs FQDN from ConnectionData.xml
DNS reply= IP
Probe 2
SSL connection to PSNs FQDN from ConnectionData.xml on port 8443, Goal is to get session owner FQDN
Connection protected by Client Provisioning portal certificate
Session owner lookup on MNT
Information about owner
Stage 2 Discovery Probes
15
Posture process
Steps are the same as for Pre 2.2 flow

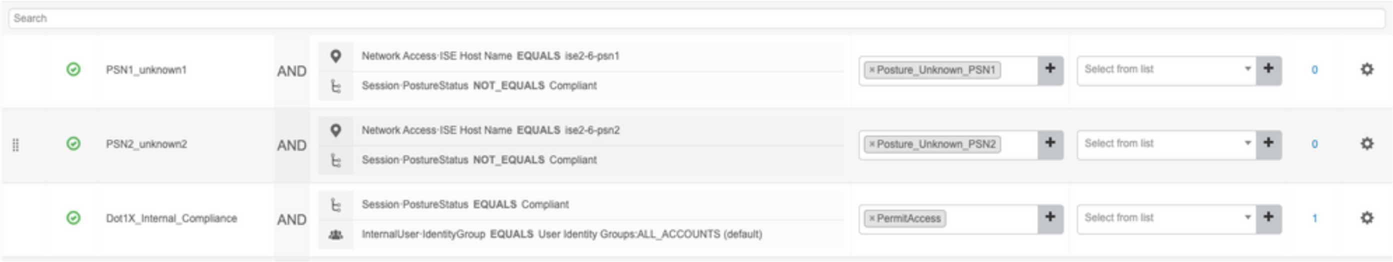
PSNs stores session data for five days, so sometimes session data for a "compliant" session still lives on the origninal PSN even if the client no longer authenticates with that node. If the probes enclosed in the red box are responded to by a PSN other than the one that currently authenticates the session AND that PSN has previously owned and marked this endpoint compliant, it is possible for there to be a mismatch between the posture status of the posture module on the endpoint and current authenticating PSN.

Here are a few common scenarios where this mismatch can occur:

- An accounting stop is not received for an endpoint when it disconnects from the network.
- The NAD failed over from one PSN to another.
- A load balancer forwards authentications to different PSNs for the same endpoint.

In order to protect from this behavior, ISE can be configured to only allow discovery probes from a particular endpoint to reach the PSN that it currently authenticates to. In order to acheive this, configure a different authorization policy for each PSN in your deployment. In these policies, reference a different authZ profile that contains a Downloadable Access Control List (DACL) which allows probes ONLY to the PSN specified in the authZ condition. See this example::

Each PSN has a rule for unknown posture status:

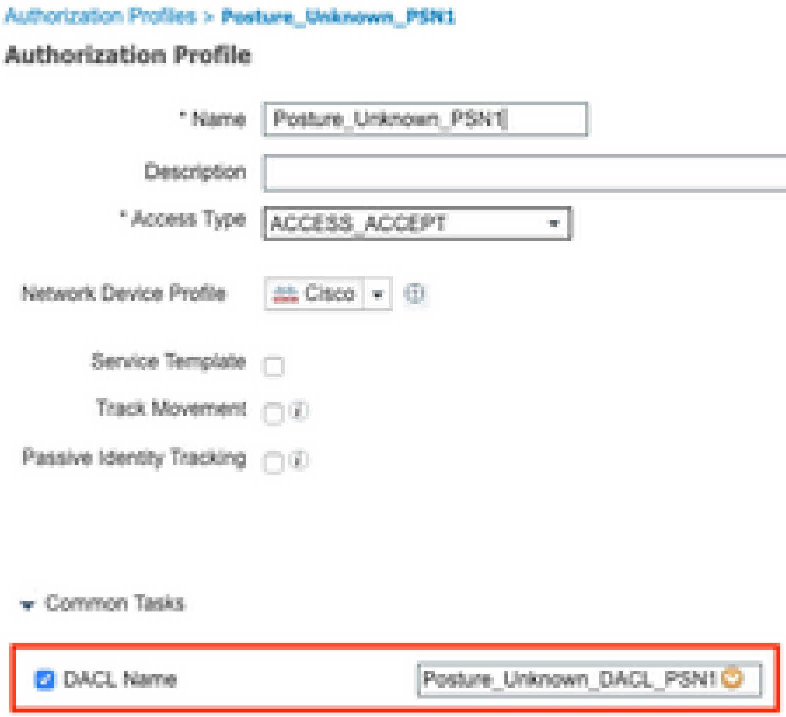


Search

	Rule Name		Conditions	Profiles	Security Groups	Hits
✓	PSN1_unknown1	AND	Network Access·ISE Host Name EQUALS ise2-6-psn1 Session·PostureStatus NOT_EQUALS Compliant	× Posture_Unknown_PSN1	Select from list	0
✓	PSN2_unknown2	AND	Network Access·ISE Host Name EQUALS ise2-6-psn2 Session·PostureStatus NOT_EQUALS Compliant	× Posture_Unknown_PSN2	Select from list	0
✓	Dot1X_Internal_Compliance	AND	Session·PostureStatus EQUALS Compliant InternalUser·IdentityGroup EQUALS User Identity Groups:ALL_ACCOUNTS (default)	× PermitAccess	Select from list	1

Each individual profile references a different DACL.

Note: For wireless, use Airespace ACLs.



Authorization Profiles > Posture_Unknown_PSN1

Authorization Profile

* Name: Posture_Unknown_PSN1

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: □

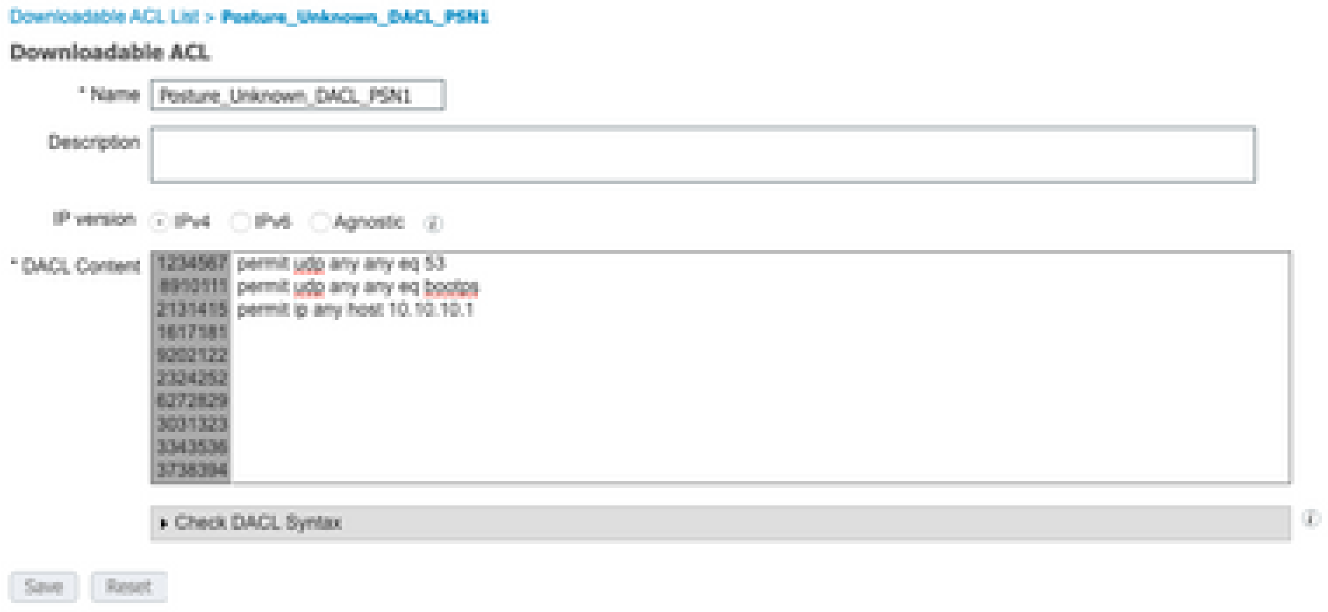
Track Movement: □

Passive Identity Tracking: □

Common Tasks

☑ DACL Name: Posture_Unknown_DACL_PSN1

Each DACL only allows probe access to the PSN that handles the authentication.



Downloadable ACL List > Posture_Unknown_DACL_PSN1

Downloadable ACL

* Name: Posture_Unknown_DACL_PSN1

Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
permit udp any any eq 53
permit udp any any eq bootps
permit ip any host 10.10.10.1
```

In the previous example, 10.10.10.1 is the IP address of PSN 1. The DACL referenced can be altered for any additional services/IPs as needed, but limits access to only the PSN that handles authentication.

Behavior Change Post 2.6 Patch 6, 2.7 Patch 2, and 3.0

Posture status has been added into the RADIUS Session Directory via the Light Data Distribution framework. Each time a posture status update is received on any PSN, replicated to ALL PSNs in the deployment. Once this change is in effect, the implications of authentications and or probes that reach different PSNs on different authentications are removed and any PSN can reply to all endpoints regardless of where they are currently authenticated.

In the five use cases in this document, consider these behaviors:

Use Case 1 - Client reauthentication forces the NAD to generate a new session ID. The client is still compliant, but because of reauthentication, the NAD is in the redirect state (redirect URL and access list).

- This behavior does not change and this configuration can still be implemented on ISE and the NADs.

Use Case 2 - The switch is configured with order MAB DOT1X and priority DOT1X MAB (Wired).

- This behavior does not change and this configuration can still be implemented on ISE and the NADs.

Use Case 3 - Wireless clients roam and authentications for different APs are going to different controllers.

- This behavior does not change and this configuration can still be implemented on ISE and the NADs.

Use Case 4 - Deployments with load balancers.

- The best practices defined in the load balancing guide can still be followed, but in the event that authentications are forwarded to different PSNs by the load balancer, the correct posture status can be returned to the client.

Use Case 5 - Stage 2 discovery probes are responsed to by a different server than the client is authenticated with

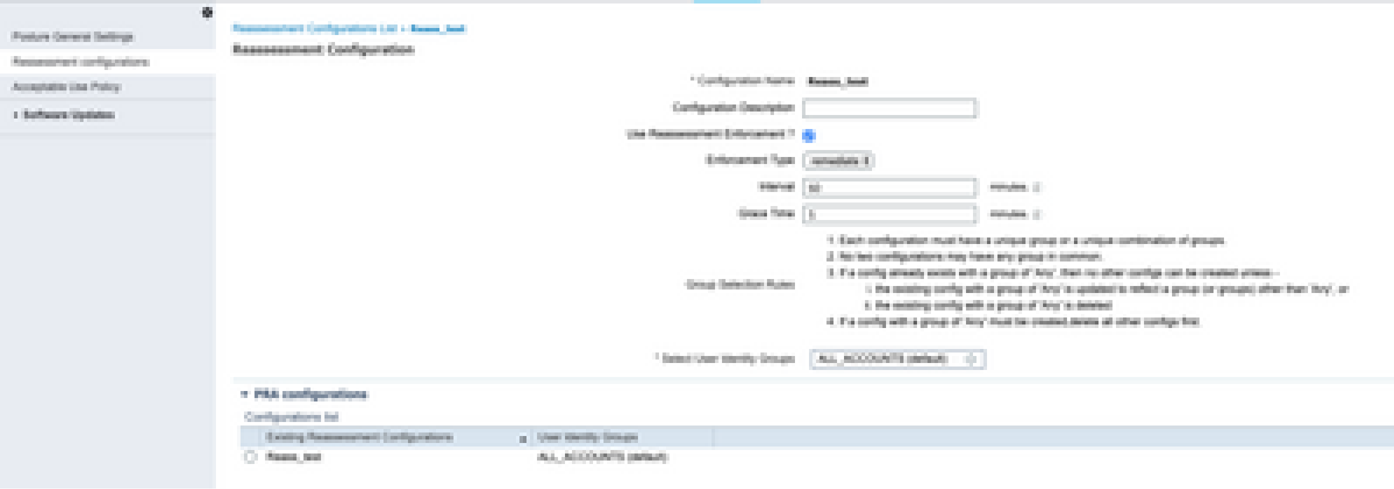
- This cannot be an issue with the new behvaior and the per-PSN authorization profile is unnecessary.

Considerations When Maintaining the Same SessionID

When you use the methods listed in this document, a user that remains connected to the network could potentially remain compliant for long periods of time. Even though they reauthenticate, the sessionID does not change and therefore ISE continues to pass the AuthZ result for their rule matching the compliant status.

In this event, Periodic Reassessment needs to be configured so that Posture is required to make sure the endpoint remains compliant with corporate policies at at defined intervals.

This can be configured under Work Centers > Posture > Settings > Ressessment configurations.



Posture General Settings
Reassessment configurations
Acceptable Use Policy
▸ Software Updates

Reassessment Configurations List > Reass_test
Reassessment Configuration

* Configuration Name: Reass_test
Configuration Description:
Use Reassessment Enforcement ? ●
Enforcement Type: remediate
Interval: [illegible] minutes
Grace Time: [illegible] minutes
Group Selection Rules:
1. Each configuration must have a unique group or a unique combination of groups.
2. No two configurations may have any group in common.
3. If a config already exists with a group of 'Any', then no other configs can be created unless -
   i. the existing config with a group of 'Any' is updated to reflect a group (or groups) other than 'Any', or
   ii. the existing config with a group of 'Any' is deleted
4. If a config with a group of 'Any' must be created,delete all other configs first.

* Select User Identity Groups: ALL_ACCOUNTS (default)

▾ **PRA configurations**
Configurations list

	Existing Reassessment Configurations	User Identity Groups
○	Reass_test	ALL_ACCOUNTS (default)