

# Meilleures pratiques et considérations relatives au déploiement ISE

## Contenu

[Introduction](#)

[Restrictions](#)

[Comportement du client de posture](#)

[Scénarios :](#)

[Cas d'utilisation 1 - La réauthentification du client force la NAD à générer un nouvel ID de session.](#)

[Cas d'utilisation 2 : le commutateur est configuré avec la commande MAB DOT1X et la priorité DOT1X MAB \(câblée\).](#)

[Cas d'utilisation 3 : les clients sans fil se déplacent et les authentications pour différents points d'accès se rendent à différents contrôleurs.](#)

[Cas d'utilisation 4 - Déploiements avec équilibreurs de charge \(Pre 2.6 Patch 6, 2.7 Patch P2 et 3.0\).](#)

[Cas d'utilisation 5 - Les sondes de détection de l'étape 2 sont traitées par un serveur différent de celui avec lequel le client est authentifié \(Pre 2.6 Patch 6, 2.7 Patch 2 et 3.0\).](#)

[Correctif de changement de comportement 2.6, correctif 2.7 et correctif 3.0](#)

[Considérations relatives à la maintenance du même ID de session](#)

## Introduction

Ce document décrit certaines configurations de base qui traitent de plusieurs cas d'utilisation avec une posture basée sur la redirection. Dans ces configurations, le client reste conforme, mais le périphérique d'accès au réseau (NAD) limite l'accès car il est en état de redirection.

## Restrictions

Les configurations de ce document fonctionnent pour les NAD Cisco, mais pas nécessairement pour les NAD tiers.

## Comportement du client de posture

Le client de posture déclenchera des sondes à ces moments :

- Connexion initiale
- Modification de la couche 3 (couche 3)/modification de la carte réseau (NIC) (nouvelle adresse IP, changement d'état de la carte réseau)

## Scénarios :

**Cas d'utilisation 1 - La réauthentification du client force la NAD à générer un nouvel ID de session.**

Dans ce cas d'utilisation, le client est toujours conforme, mais en raison de la réauthentification, la NAD est dans l'état de redirection (URL de redirection et liste d'accès).

Par défaut, Identity Services Engine (ISE) est configuré pour effectuer une évaluation de la position chaque fois qu'il se connecte au réseau, en particulier pour chaque nouvelle session.

Ce paramètre est configuré sous Centres de travail > Posture > Settings > Posture General Settings.

### Posture General Settings i

Remediation Timer	<input type="text" value="4"/>	Minutes <span>i</span>
Network Transition Delay	<input type="text" value="3"/>	Seconds <span>i</span>
Default Posture Status	<input type="text" value="Compliant"/> <span>i</span>	
<input type="checkbox"/> Automatically Close Login Success Screen After	<input type="text" value="0"/>	Seconds <span>i</span>
<input checked="" type="checkbox"/> Continuous Monitoring Interval	<input type="text" value="5"/>	Minutes <span>i</span>
Acceptable Use Policy in Stealth Mode	<input type="text" value="Block"/>	

### Posture Lease

Perform posture assessment every time a user connects to the network

Perform posture assessment every  Days i

### Cache Last Known Posture Compliant Status

Last Known Posture Compliant State

Afin d'empêcher la NAD de générer un nouvel ID de session lors de la réauthentification, configurez ces valeurs de réauthentification dans le profil d'autorisation. Le compteur de réauthentification affiché n'est pas une recommandation standard, les compteurs de réauthentification doivent être pris en compte par déploiement en fonction du type de connexion (sans fil/filaire), de la conception (quelles sont les règles de persistance sur le répartiteur de charge), etc.

Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation

Reauthentication

Timer  (Enter value in seconds)

Maintain Connectivity During Reauthentication

#### ▼ Advanced Attributes Settings

=  - +

#### ▼ Attributes Details

Access Type = ACCESS ACCEPT  
 Session-Timeout = 3600  
 Termination-Action = RADIUS-Request

Sur les commutateurs, vous devez configurer chaque interface, ou modèle, pour obtenir son compteur de réauthentification auprès d'ISE.

```
authentication timer reauthenticate server
```

**Note:** S'il existe un équilibrage de charge, vous devez vous assurer que la persistance est configurée de manière à ce que les réauthentifications soient retournées au service de stratégie d'origine (PSN).

## Cas d'utilisation 2 : le commutateur est configuré avec la commande MAB DOT1X et la priorité DOT1X MAB (câblée).

Dans ce cas, les réauthentifications seront terminées, car un arrêt de comptabilité pour la session 802.1x sera envoyé lorsque le contournement d'authentification MAC (MAB) est tenté pendant la réauthentification.

- L'arrêt de la comptabilité envoyé pour le processus MAB en cas d'échec de l'authentification est correct, car le nom d'utilisateur du client passe du nom d'utilisateur 802.1X au nom d'utilisateur MAB.
- Dot1x comme ID de méthode dans l'arrêt comptable est également correct car la méthode d'autorisation était dot1x.
- Lorsque la méthode Dot1x réussit, elle envoie un début de comptabilisation avec l'id de méthode dot1x. Ici aussi, ce comportement est comme prévu.

Afin de résoudre ce problème, configurez `cisco-av-pair:termination-action-modificateur = 1` sur le profil authZ utilisé lorsqu'un point de terminaison est conforme. Cette paire attribut-valeur (AV) spécifie que la NAD doit réutiliser la méthode choisie dans l'authentification d'origine, quel que soit

l'ordre configuré.

The screenshot displays a configuration interface with two main sections:

- Advanced Attributes Settings:** A configuration row showing the attribute `Cisco:cisco-av-pair` set to `termination-action-modifier=1`. The interface includes a list icon on the left, a dropdown arrow on the attribute name, an equals sign, a dropdown arrow on the value, and minus/plus icons on the right.
- Attributes Details:** A summary box containing the following values:
  - Access Type = ACCESS\_ACCEPT
  - Session-Timeout = 60
  - Termination-Action = RADIUS-Request
  - cisco-av-pair = termination-action-modifier=1

At the bottom of the interface, there are two buttons: **Save** and **Reset**.

### Cas d'utilisation 3 : les clients sans fil se déplacent et les authentifications pour différents points d'accès se rendent à différents contrôleurs.

Dans ce cas, le réseau sans fil doit être conçu de sorte que les points d'accès (AP) à portée d'autres points d'accès pour l'itinérance utilisent le même contrôleur actif. Un exemple est le basculement SSO (Stateful switchover) du contrôleur de réseau local sans fil (WLC). Pour plus d'informations sur la haute disponibilité (HA) SSO pour WLC, consultez le [Guide de déploiement de la haute disponibilité \(SSO\)](#).

### Cas d'utilisation 4 - Déploiements avec équilibreurs de charge (Pre 2.6 Patch 6, 2.7 Patch P2 et 3.0).

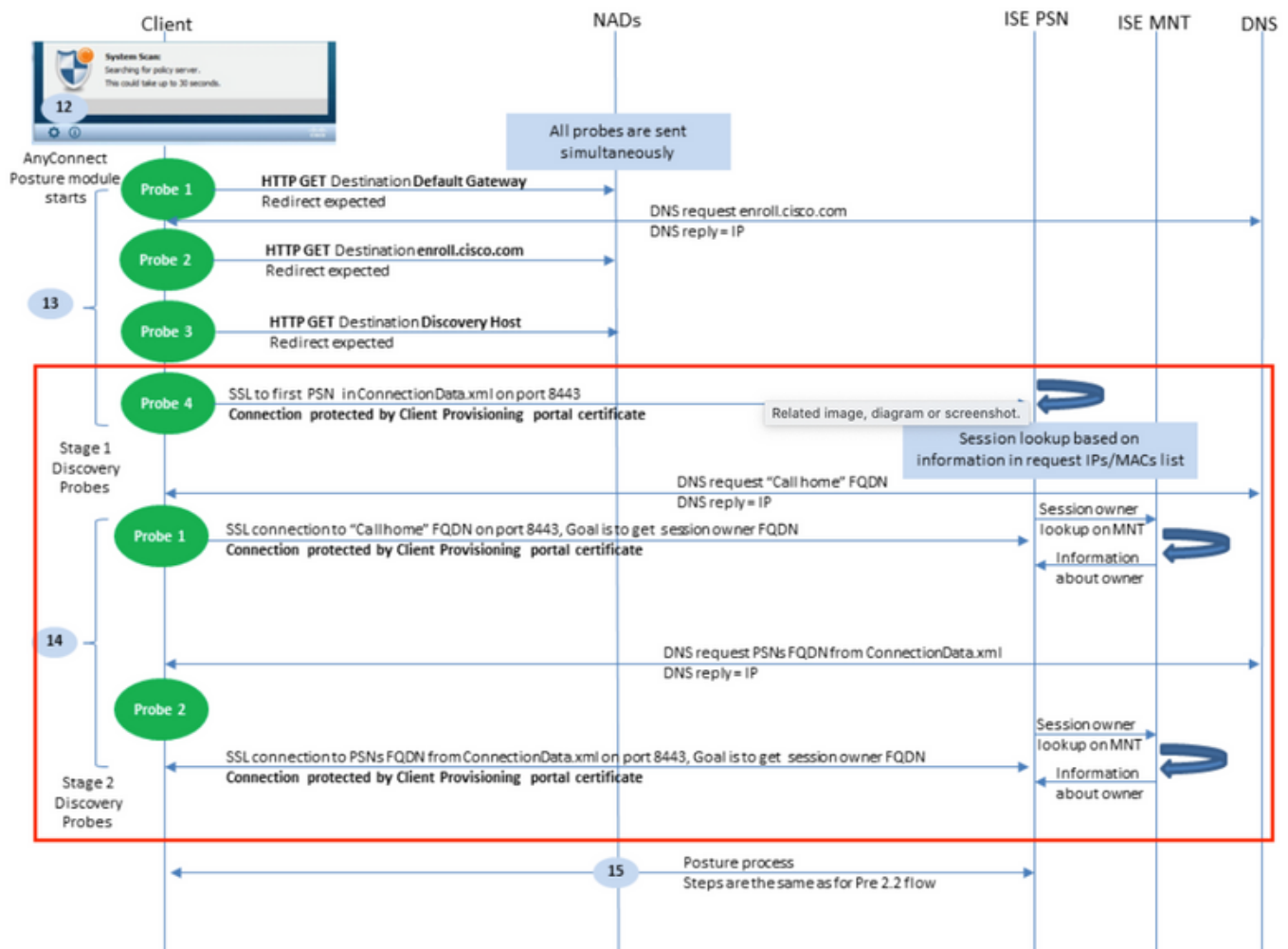
Dans les déploiements avec équilibreurs de charge impliqués, il est important de s'assurer qu'après avoir effectué les modifications dans les cas d'utilisation précédents, les sessions continuent à aller sur le même PSN. Avant la version/les correctifs répertoriés pour cette étape, l'état de la position n'est pas répliqué entre les noeuds via la distribution de données claires (anciennement Light Session Directory). Pour cette raison, il est possible que différents PSN retournent des résultats d'état différents.

Si la persistance n'est pas configurée correctement, les sessions qui se réauthentifient peuvent se rendre sur un PSN différent de celui utilisé à l'origine. Si cela se produit, le nouveau PSN pourrait marquer l'état de conformité des sessions comme inconnu et transmettre le résultat authZ avec la liste de contrôle d'accès (ACL)/URL et limiter l'accès aux points d'extrémité. Encore une fois, ce changement sur la NAD ne serait pas reconnu par le module de posture et les sondes ne seront pas déclenchées.

Pour plus d'informations sur la configuration des équilibreurs de charge, reportez-vous au [Guide de déploiement de Cisco & F5 : Équilibrage de charge ISE avec BIG-IP](#). Il fournit une vue d'ensemble de haut niveau et une configuration spécifique de F5 d'une conception des meilleures pratiques pour les déploiements ISE dans un environnement à charge équilibrée.

## Cas d'utilisation 5 - Les sondes de détection de l'étape 2 sont traitées par un serveur différent de celui avec lequel le client est authentifié (Pre 2.6 Patch 6, 2.7 Patch 2 et 3.0).

Regardez les sondes de la zone rouge dans ce diagramme.



Les PSN stockent les données de session pendant cinq jours, de sorte que parfois les données de session d'une session « conforme » demeurent sur le PSN d'origine même si le client ne s'authentifie plus auprès de ce nœud. Si les sondes contenues dans la zone rouge sont traitées par un PSN autre que celui qui authentifie actuellement la session ET que PSN a précédemment possédé et marqué ce terminal conforme, il est possible qu'il y ait une incompatibilité entre l'état de posture du module de posture sur le terminal et le PSN d'authentification en cours.

Voici quelques scénarios courants dans lesquels cette incompatibilité peut se produire :

- Un arrêt de compte n'est pas reçu pour un point d'extrémité lorsqu'il se déconnecte du réseau.
- La NAD a échoué d'un PSN à un autre.
- Un équilibreur de charge transfère les authentifications vers différents PSN pour le même terminal.

Afin de se protéger de ce comportement, ISE peut être configuré pour autoriser uniquement les sondes de détection d'un point d'extrémité particulier à atteindre le PSN auquel il s'authentifie actuellement. Pour ce faire, configurez une politique d'autorisation différente pour chaque PSN de votre déploiement. Dans ces stratégies, référez un profil authZ différent qui contient une liste de contrôle d'accès téléchargeable (DACL) qui autorise UNIQUEMENT les sondes sur le PSN

spécifié dans la condition authZ. Voir cet exemple :

Chaque PSN aura une règle pour l'état de posture inconnu :

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

Chaque profil individuel fait référence à une liste de contrôle d'accès DACL différente.

**Note:** Pour les connexions sans fil, utilisez des listes de contrôle d'accès Airespace.

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

Chaque DACL autorise uniquement l'accès de sonde au PSN qui gère l'authentification.

### Downloadable ACL

\* Name

Description

IP version  IPv4  IPv6  Agnostic [?](#)

\* DACL Content

1234567	permit udp any any eq 53
8910111	permit udp any any eq bootps
2131415	permit ip any host 10.10.10.1
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	

[?](#)

Dans l'exemple précédent, 10.10.10.1 est l'adresse IP de PSN 1. La DACL référencée peut être modifiée pour tous les services/adresses IP supplémentaires si nécessaire, mais doit limiter l'accès au seul PSN qui gère l'authentification.

## Correctif de changement de comportement 2.6, correctif 2.7 et correctif 3.0

L'état de la position a été ajouté au répertoire de session RADIUS via le cadre de distribution de données claires. Chaque fois qu'une mise à jour d'état de position est reçue sur un PSN, elle est répliquée sur TOUS les PSN du déploiement. Une fois cette modification en vigueur, les implications des authentifications et/ou des sondes qui atteignent différents PSN sur différentes authentifications sont supprimées et tout PSN devrait pouvoir répondre à tous les points de terminaison, quel que soit l'endroit où ils sont actuellement authentifiés.

Dans les cinq cas d'utilisation de ce document, tenez compte des comportements suivants :

Cas d'utilisation 1 - La réauthentification du client force la NAD à générer un nouvel ID de session. Le client est toujours conforme, mais en raison de la réauthentification, la NAD est dans l'état de redirection (URL de redirection et liste d'accès).

- Ce comportement ne changera pas et cette configuration doit encore être implémentée sur ISE et les NAD.

Cas d'utilisation 2 : le commutateur est configuré avec la commande MAB DOT1X et la priorité DOT1X MAB (câblée).

- Ce comportement ne changera pas et cette configuration doit encore être implémentée sur ISE et les NAD.

Cas d'utilisation 3 : les clients sans fil se déplacent et les authentifications pour différents points d'accès se rendent à différents contrôleurs.

- Ce comportement ne changera pas et cette configuration doit encore être implémentée sur ISE et les NAD.

## Cas d'utilisation 4 - Déploiements avec équilibrage de charge.

- Les meilleures pratiques définies dans le guide d'équilibrage de charge doivent toujours être suivies, mais si les authentifications sont transmises à différents PSN par l'équilibreur de charge, l'état correct doit être retourné au client.

Cas d'utilisation 5 - Les sondes de découverte de l'étape 2 sont traitées par un serveur différent de celui avec lequel le client est authentifié.

- Ceci ne doit pas être un problème avec le nouveau comportement et le profil d'autorisation par PSN ne doit pas être nécessaire.

## Considérations relatives à la maintenance du même ID de session

Lorsque vous utilisez les méthodes répertoriées dans ce document, un utilisateur qui reste connecté au réseau peut potentiellement rester conforme pendant de longues périodes. Même s'ils se réauthentifient, l'ID de session ne change pas et, par conséquent, ISE continuera à transmettre le résultat AuthZ pour leur règle correspondant à l'état conforme.

Dans ce cas, une réévaluation périodique doit être configurée de sorte que la posture soit requise pour s'assurer que le terminal reste conforme aux politiques de l'entreprise à des intervalles définis.

Vous pouvez le configurer sous Centres de travail > Posture > Settings > Resessment configurations.

The screenshot shows the 'Reassessment Configuration' page in the Cisco ISE management console. The left sidebar contains navigation options: 'Posture General Settings', 'Reassessment configurations', 'Acceptable Use Policy', and 'Software Updates'. The main content area is titled 'Reassessment Configuration' and includes the following fields and options:

- \* Configuration Name: **Reass\_test**
- Configuration Description: [Empty text box]
- Use Reassessment Enforcement?:
- Enforcement Type: **remediate** (dropdown menu)
- Interval: **60** minutes (input field)
- Grace Time: **5** minutes (input field)
- Group Selection Rules: [Empty text box]
- \* Select User Identity Groups: **ALL\_ACCOUNTS (default)** (dropdown menu)

Below the configuration fields, there are four numbered 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.

At the bottom, there is a section for 'PRA configurations' with a 'Configurations list' table:

Existing Reassessment Configurations	User Identity Groups
<input type="radio"/> Reass_test	ALL_ACCOUNTS (default)