Déployer la position ISE

Table des matières

Introduction

Ce document décrit certaines configurations de base qui traitent plusieurs cas d'utilisation avec une posture basée sur la redirection.

Restrictions

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

Comportement du client Posture

Le client de posture peut déclencher des sondes à ces moments :

- Connexion initiale
- Modification de couche 3 (L3)/carte réseau (NIC) (nouvelle adresse IP, changement d'état de la carte réseau)

Scénarios :

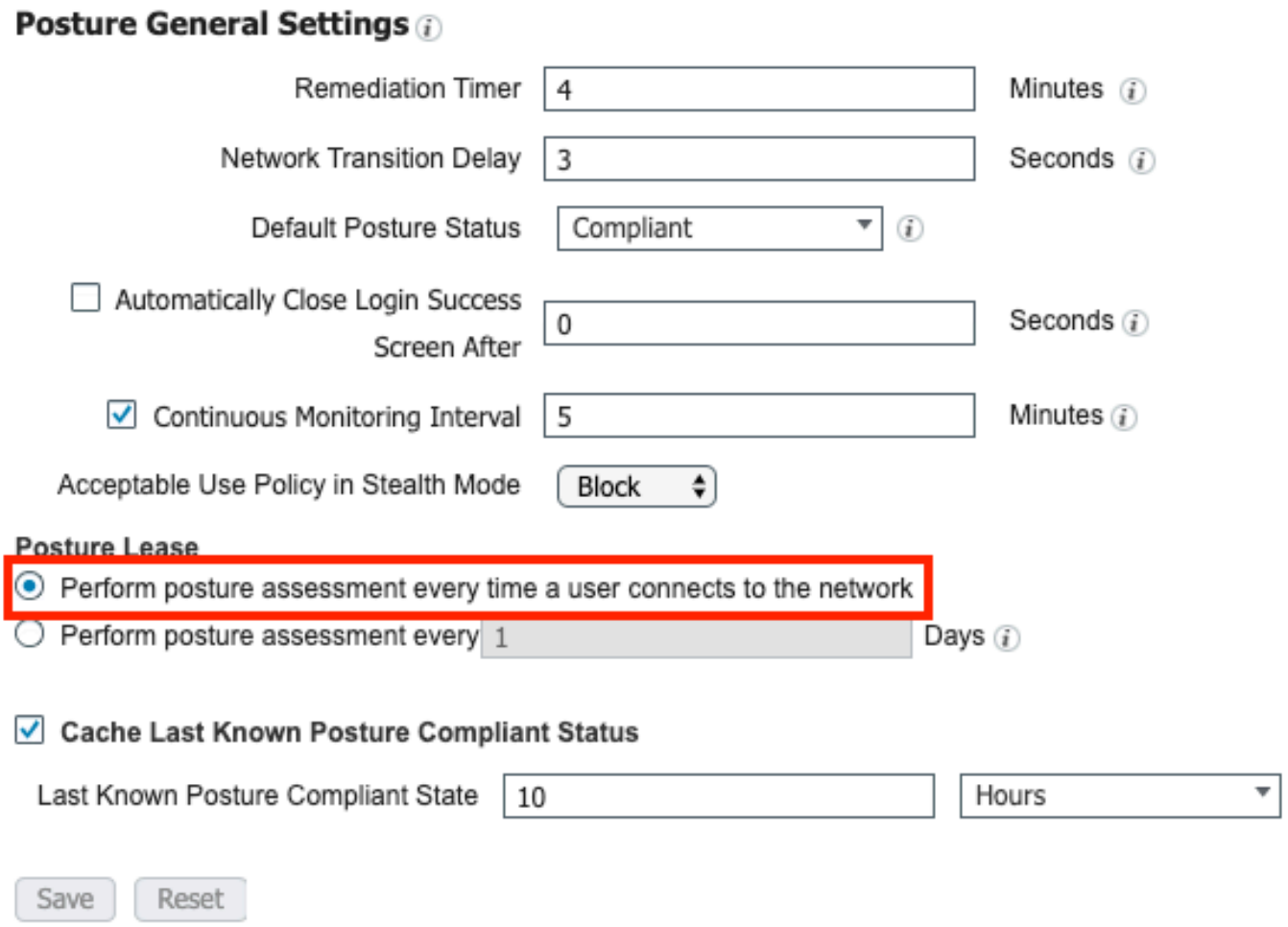
Cas d'utilisation 1 : la réauthentification du client force le NAD à générer un nouvel ID de session

Dans ce cas, le client est toujours conforme, mais en raison de la réauthentification, le NAD est à

l'état de redirection (URL de redirection et liste d'accès).

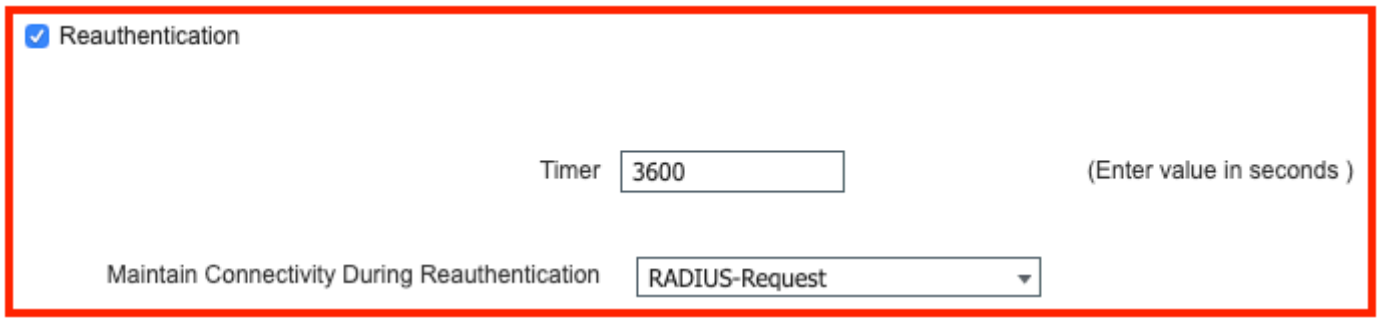
Par défaut, Identity Services Engine (ISE) est configuré pour effectuer une évaluation de position chaque fois qu'il se connecte au réseau, plus spécifiquement pour chaque nouvelle session.

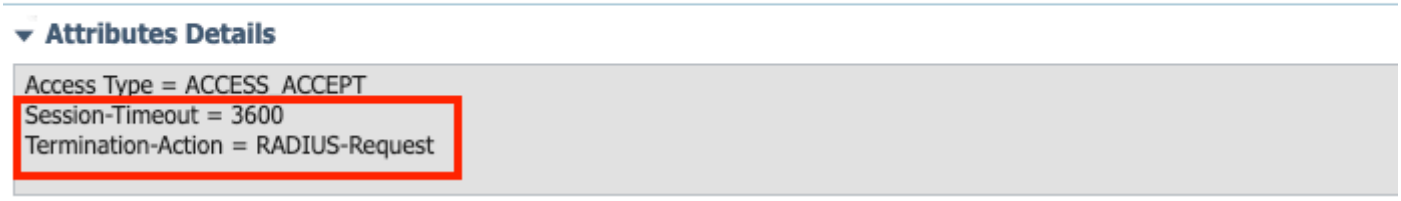
Ce paramètre est configuré sous Work Centers > Posture > Settings > Posture General Settings.



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

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





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

```
authentication timer reauthenticate server
```

Remarque : S'il existe un équilibreur de charge, vous devez vous assurer que la persistance est configurée de manière à ce que les réauthentifications puissent être renvoyées au Service de stratégie (PSN) d'origine.

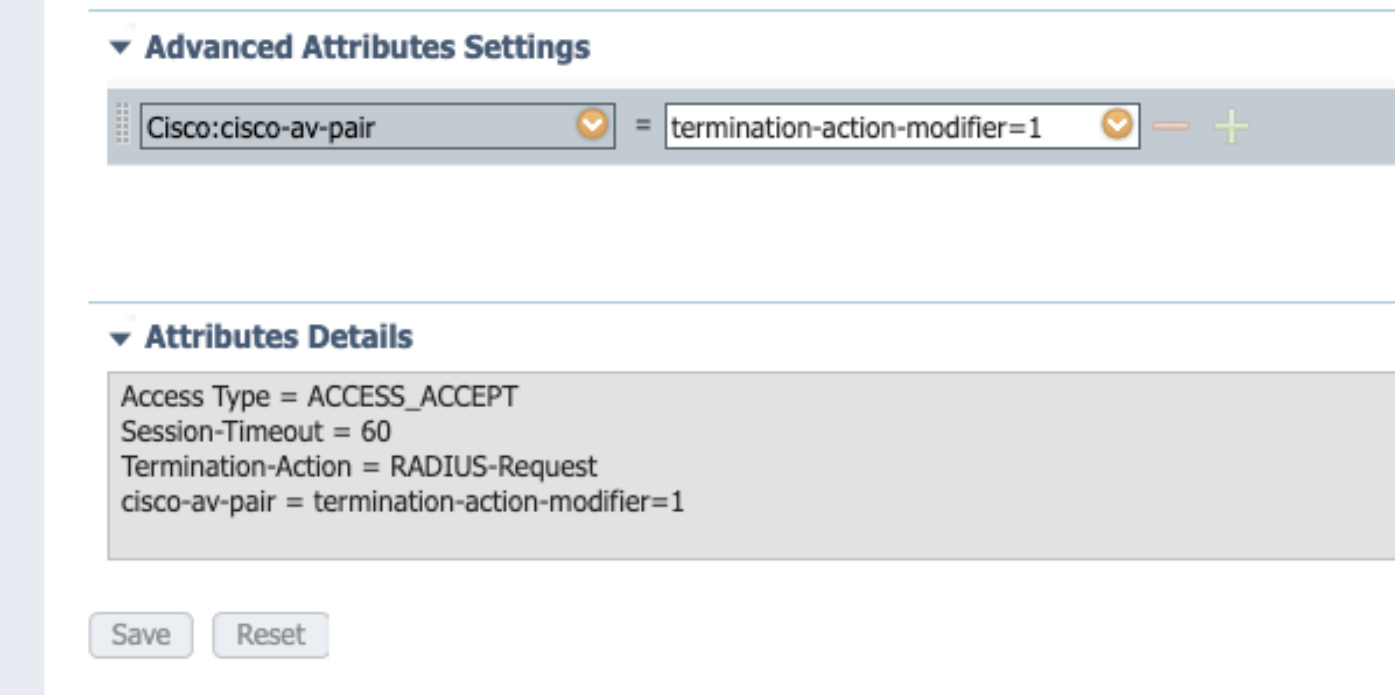
Cas d'utilisation 2 : le commutateur est configuré avec MAB de commande DOT1X et MAB DOT1X prioritaire (câblé)

Dans ce cas, les réauthentifications peuvent être interrompues car un arrêt de la gestion des comptes pour la session 802.1x peut être envoyé lorsque le contournement d'authentification MAC (MAB) est tenté pendant la réauthentification.

- L'arrêt de la gestion des comptes 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 en tant qu'id de méthode dans l'arrêt de comptabilisation 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 conforme aux attentes.

Afin de résoudre ce problème, configurez le cisco-av-pair : termination-action-modificateur=1 sur le profil authZ utilisé quand un terminal est conforme. Cette paire attribut-valeur (AV) indique que le NAD réutilise la méthode choisie dans l'authentification d'origine, quel que soit l'ordre configuré.



Exemple d'utilisation 3 : les clients sans fil se déplacent et les authentifications de différents points d'accès sont envoyées à différents contrôleurs

Pour cette situation, le réseau sans fil doit être conçu de sorte que les points d'accès (AP) à portée d'autres AP pour l'itinérance utilisent le même contrôleur actif. Le basculement SSO (stateful switchover) du contrôleur LAN sans fil (WLC) en est un exemple. Pour plus d'informations sur High Availability (HA) SSO for WLC, consultez le Guide de déploiement de High Availability (SSO) .

Cas d'utilisation 4 : déploiements avec équilibreurs de charge (versions antérieures à 2.6 Patch 6, 2.7 Patch P2 et 3.0)

Dans les déploiements impliquant des équilibreurs de charge, il est important de s'assurer qu'après avoir apporté les modifications dans les cas d'utilisation précédents, les sessions continuent d'accéder au même PSN. Avant la version ou les correctifs répertoriés pour cette étape, l'état de posture n'est pas répliqué entre les noeuds via Light Data Distribution (anciennement Light Session Directory). De ce fait, il est possible que différents PSN retournent différents résultats d'état de posture.

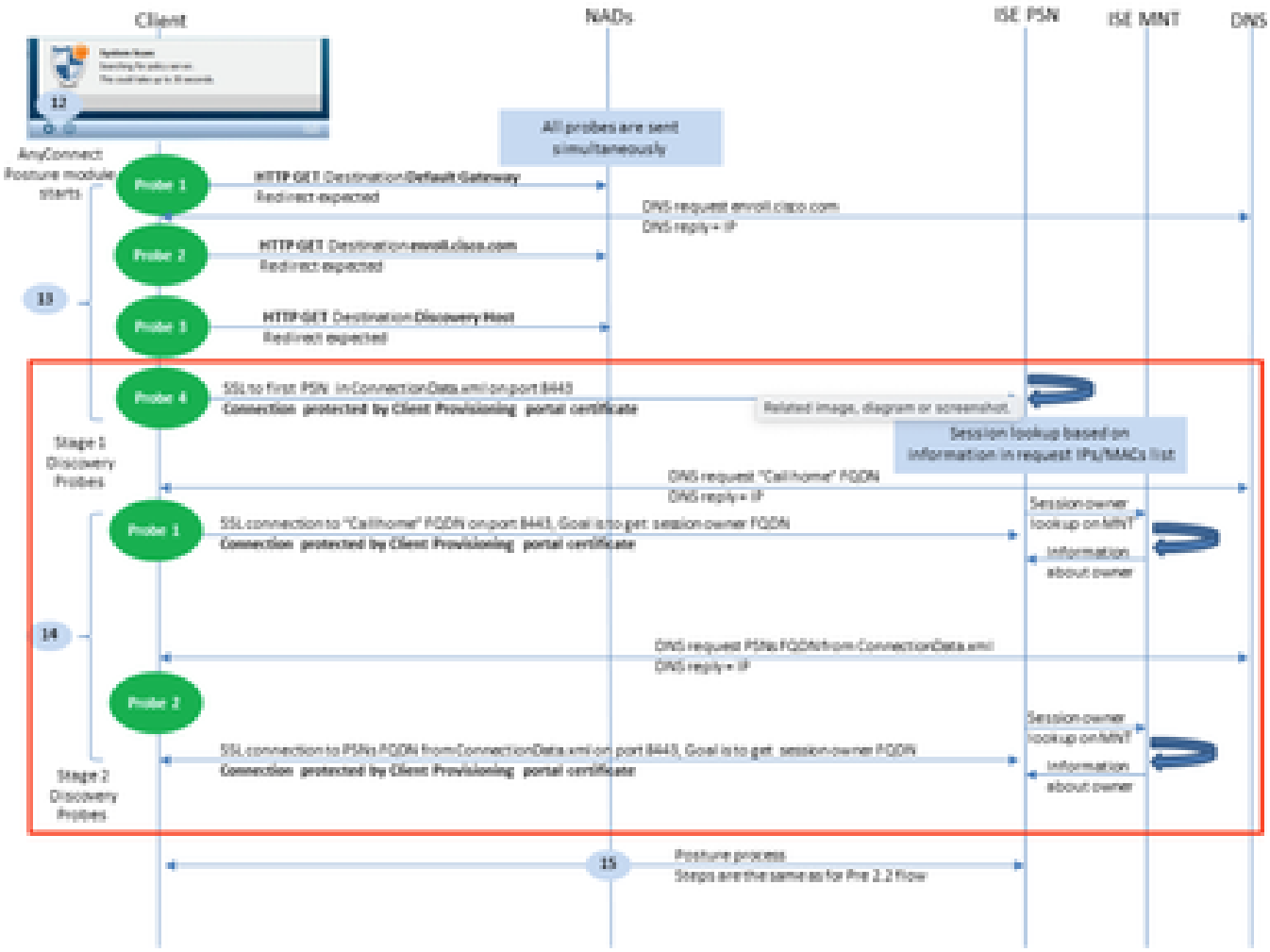
Si la persistance n'est pas configurée correctement, les sessions qui se réauthentifient peuvent accéder à un PSN différent de celui qui a été utilisé à l'origine. Dans ce cas, le nouveau PSN peut marquer l'état de conformité des sessions comme inconnu et transmettre le résultat authZ avec

l'URL/liste de contrôle d'accès de redirection et limiter l'accès aux points d'extrémité. Encore une fois, ce changement sur le NAD ne serait pas reconnu par le module de posture et les sondes ne seraient pas déclenchées.

Pour plus d'informations sur la façon de configurer les équilibreurs de charge, consultez le Guide de déploiement de Cisco et F5 : Équilibrage de charge ISE avec BIG-IP. Il fournit une présentation générale et une configuration spécifique F5 d'une conception basée sur les meilleures pratiques pour les déploiements ISE dans un environnement à charge équilibrée.

Cas d'utilisation 5 - Les sondes de détection de l'étape 2 reçoivent une réponse d'un serveur différent de celui avec lequel le client est authentifié (pré-2.6 Patch 6, 2.7 Patch 2 et 3.0)

Regardez les sondes dans la zone rouge de ce schéma.



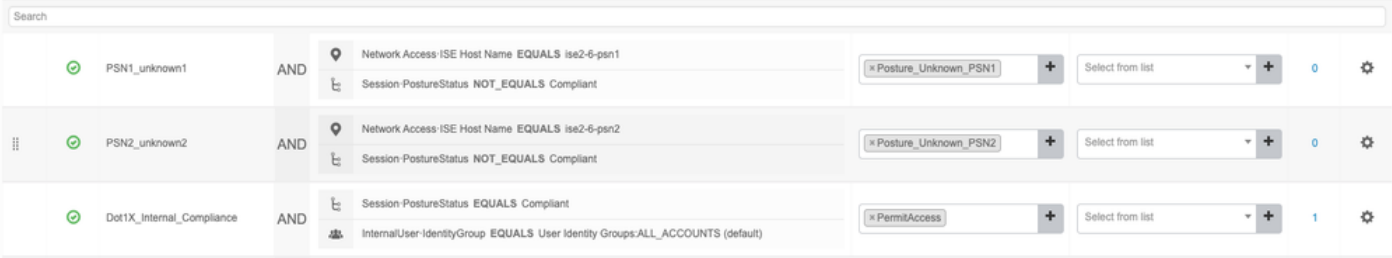
Les PSN stockent les données de session pendant cinq jours, de sorte que parfois les données de session d'une session conforme demeurent sur le PSN d'origine même si le client ne s'authentifie plus auprès de ce noeud. Si les sondes contenues dans la zone rouge reçoivent une réponse d'un PSN autre que 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 incohérence entre l'état de posture du module de posture sur le terminal et le PSN d'authentification actuel.

Voici quelques scénarios courants dans lesquels ce décalage peut se produire :

- Aucun arrêt de la gestion des comptes n'est reçu pour un point d'extrémité lorsqu'il se déconnecte du réseau.
- Le NAD a basculé d'un PSN à un autre.
- Un équilibreur de charge transfère les authentifications à différents PSN pour le même terminal.

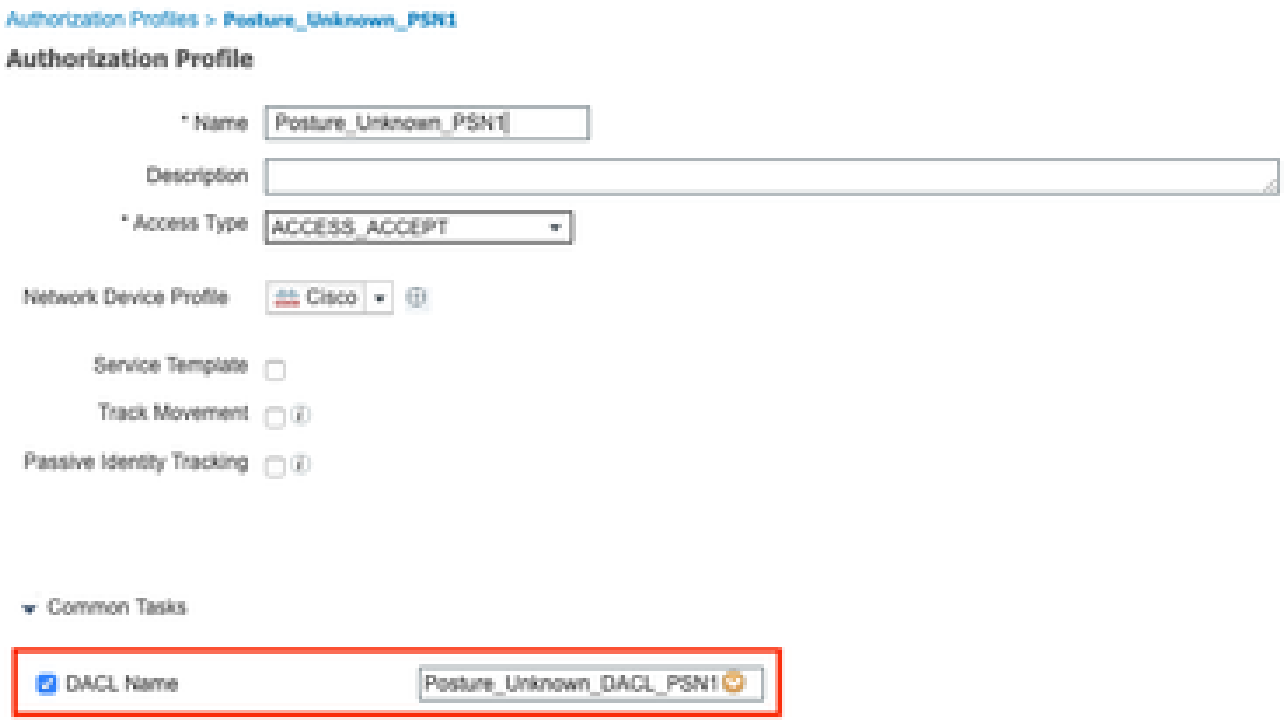
Afin de se protéger de ce comportement, ISE peut être configuré pour autoriser uniquement les sondes de détection d'un point de terminaison particulier à atteindre le PSN auquel il s'authentifie actuellement. Pour ce faire, configurez une stratégie d'autorisation différente pour chaque PSN de votre déploiement. Dans ces politiques, référencez un profil authZ différent qui contient une liste de contrôle d'accès téléchargeable (DACL) qui autorise les sondes UNIQUEMENT vers le PSN spécifié dans la condition authZ. Voir cet exemple :

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

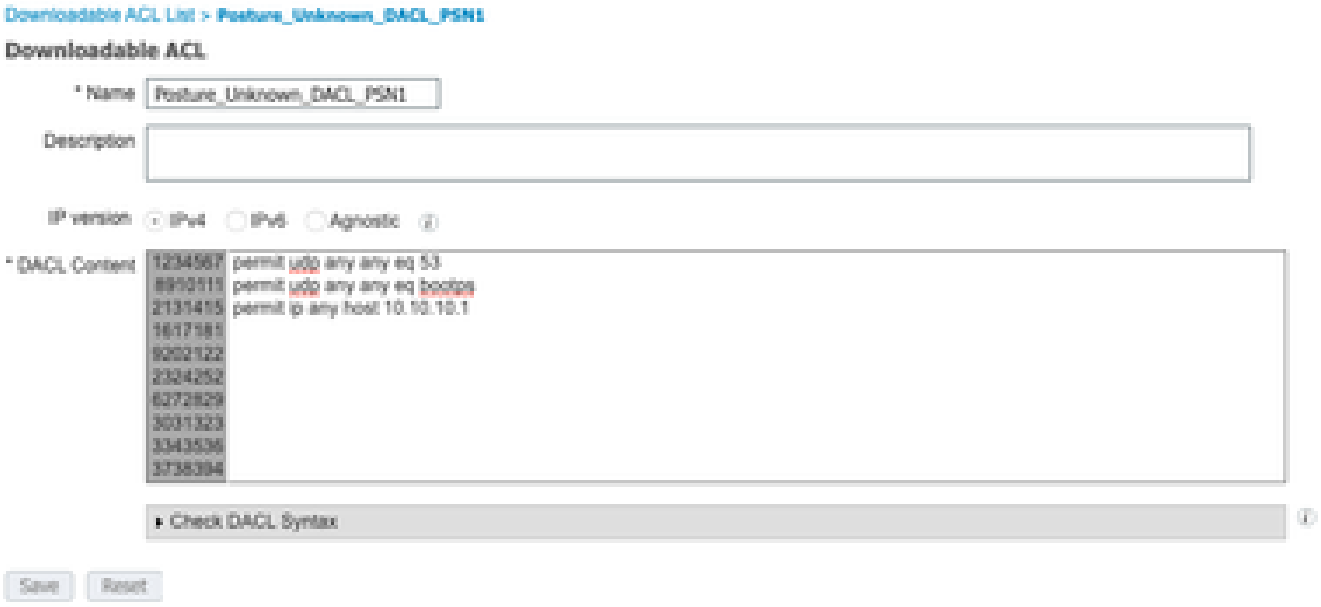


Chaque profil individuel fait référence à une DACL différente.

Remarque : Pour les réseaux sans fil, utilisez les ACL Airespace.



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



Dans l'exemple précédent, 10.10.10.1 est l'adresse IP de PSN 1. La DACL référencée peut être modifiée pour n'importe quel service/IP supplémentaire selon les besoins, mais limite l'accès au PSN qui gère l'authentification.

Changement de comportement post 2.6 Patch 6, 2.7 Patch 2 et 3.0

L'état de la position a été ajouté au répertoire de session RADIUS via le cadre de distribution des données lumineuses. 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 effective, les implications des authentifications et/ou des sondes qui atteignent différents PSN sur différentes authentifications sont supprimées, et tout PSN peut répondre à tous les terminaux, quel que soit l'endroit où ils sont actuellement authentifiés.

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

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

- Ce comportement ne change pas et cette configuration peut toujours être implémentée sur ISE et les NAD.

Cas d'utilisation 2 : le commutateur est configuré avec MAB DOT1X d'ordre et DOT1X MAB de priorité (filaire).

- Ce comportement ne change pas et cette configuration peut toujours être implémentée sur ISE et les NAD.

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

- Ce comportement ne change pas et cette configuration peut toujours être implémentée sur ISE et les NAD.

Cas d'utilisation 4 : déploiements avec équilibreurs de charge.

- Les meilleures pratiques définies dans le guide d'équilibrage de charge peuvent toujours être suivies, mais dans le cas où les authentifications sont transmises à différents PSN par l'équilibreur de charge, l'état de posture correct peut être renvoyé au client.

Cas d'utilisation 5 - Les sondes de détection de l'étape 2 reçoivent une réponse d'un serveur différent de celui avec lequel le client est authentifié

- Cela ne peut pas être un problème avec le nouveau comportement et le profil d'autorisation par PSN est inutile.

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 continue à transmettre le résultat AuthZ pour leur règle correspondant à l'état de conformité.

Dans ce cas, une réévaluation périodique doit être configurée afin que Posture soit nécessaire pour garantir que le terminal reste conforme aux stratégies de l'entreprise à intervalles définis.

Vous pouvez le configurer sous Work Centers > Posture > Settings > Reassessment configurations.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.