Mise en oeuvre de la posture ISE sans redirection

Table des matières

Introduction

Ce document décrit l'utilisation et la configuration du flux de posture sans redirection et des conseils de dépannage.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Flux de posture sur ISE
- Configuration des composants de posture sur ISE
- Redirection vers les portails ISE

Pour une meilleure compréhension des concepts décrits plus loin, il est recommandé de passer par :

Comparaison des versions antérieures d'ISE avec le flux de posture ISE dans ISE 2.2
Gestion et positionnement des sessions ISE

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE version 3.1
- Cisco Secure Client 5.0.01242

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre lâ€™incidence possible des commandes.

Informations générales

Le flux de posture ISE se compose des étapes suivantes :

0. Authentification/Autorisation. Généralement effectuée juste avant le début de l'écoulement de posture, mais elle peut être contournée pour certains cas d'utilisation tels que la réévaluation de posture (PRA). Comme l'authentification elle-même ne déclenche pas la découverte de posture, cela n'est pas considéré comme essentiel pour chaque flux de posture.

1. Découverte. Processus effectué par le module Secure Client ISE Posture pour trouver le propriétaire PSN de la **session active en cours**.
2. Provisionnement client. Processus effectué par ISE pour fournir au client les versions correspondantes du module de posture ISE et du module de conformité Cisco Secure Client (anciennement AnyConnect). Dans cette étape, la copie locale du profil de posture contenu dans et signé par le PSN particulier est également envoyée au client.
3. Analyse du système. Les stratégies de position configurées sur ISE sont évaluées par le module de conformité.
4. Correction (Facultatif). Effectué dans le cas où les politiques de posture ne sont pas conformes.
5. CoA. Une nouvelle autorisation est nécessaire pour accorder un accès réseau final (conforme ou non conforme).

Ce document se concentre sur le processus de découverte du flux de posture ISE.

Cisco recommande d'utiliser la redirection pour le processus de détection. Cependant, dans certains cas, la redirection n'est pas possible à mettre en oeuvre, par exemple lorsque des périphériques réseau tiers ne sont pas pris en charge. Ce document vise à fournir une orientation générale et les meilleures pratiques pour mettre en oeuvre et dépanner une posture sans redirection dans de tels environnements.

La description complète du flux sans redirection est décrite dans Comparer les versions antérieures d'ISE au flux de posture d'ISE dans ISE 2.2.

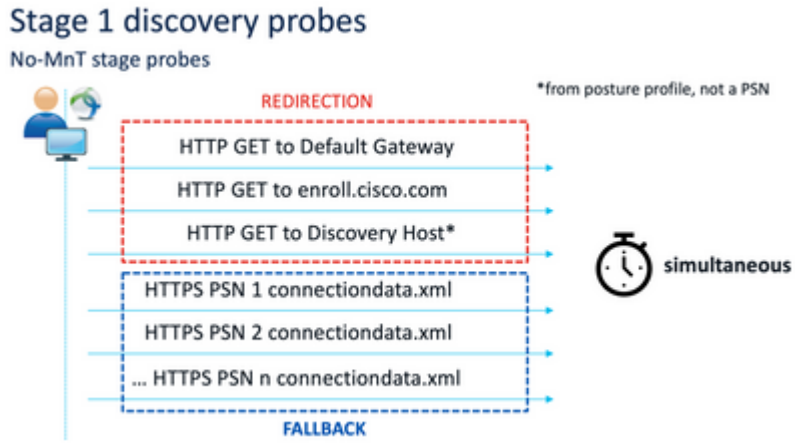
Il existe deux types de sondes de détection de position qui n'utilisent pas la redirection :

1. Connectiondata.xml
2. Liste Call Home

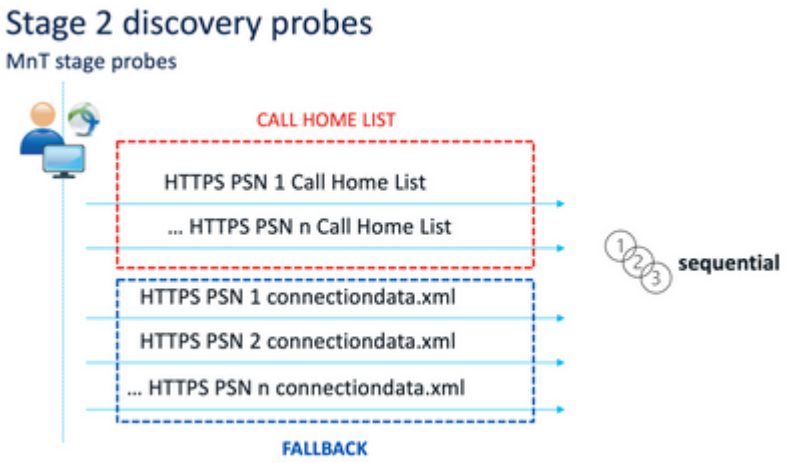
Connectiondata.xml

Le fichier Connectiondata.xml est un fichier créé et mis à jour automatiquement par Cisco Secure Client. Il se compose d'une liste de PSN auxquels le client s'est précédemment connecté avec succès pour la posture, par conséquent, il ne s'agit que d'un fichier local et son contenu n'est pas persistant sur tous les terminaux.

Le but principal de connectiondata.xml est de fonctionner comme mécanisme de sauvegarde pour les sondes de détection des étapes 1 et 2. Si les sondes de redirection ou Call Home List ne parviennent pas à trouver un PSN avec une session active, Cisco Secure Client envoie une requête directe à chacun des serveurs répertoriés dans le fichier connectiondata.xml.



Étape 1 - Sondes de détection



Étape 2 - Sondes de détection

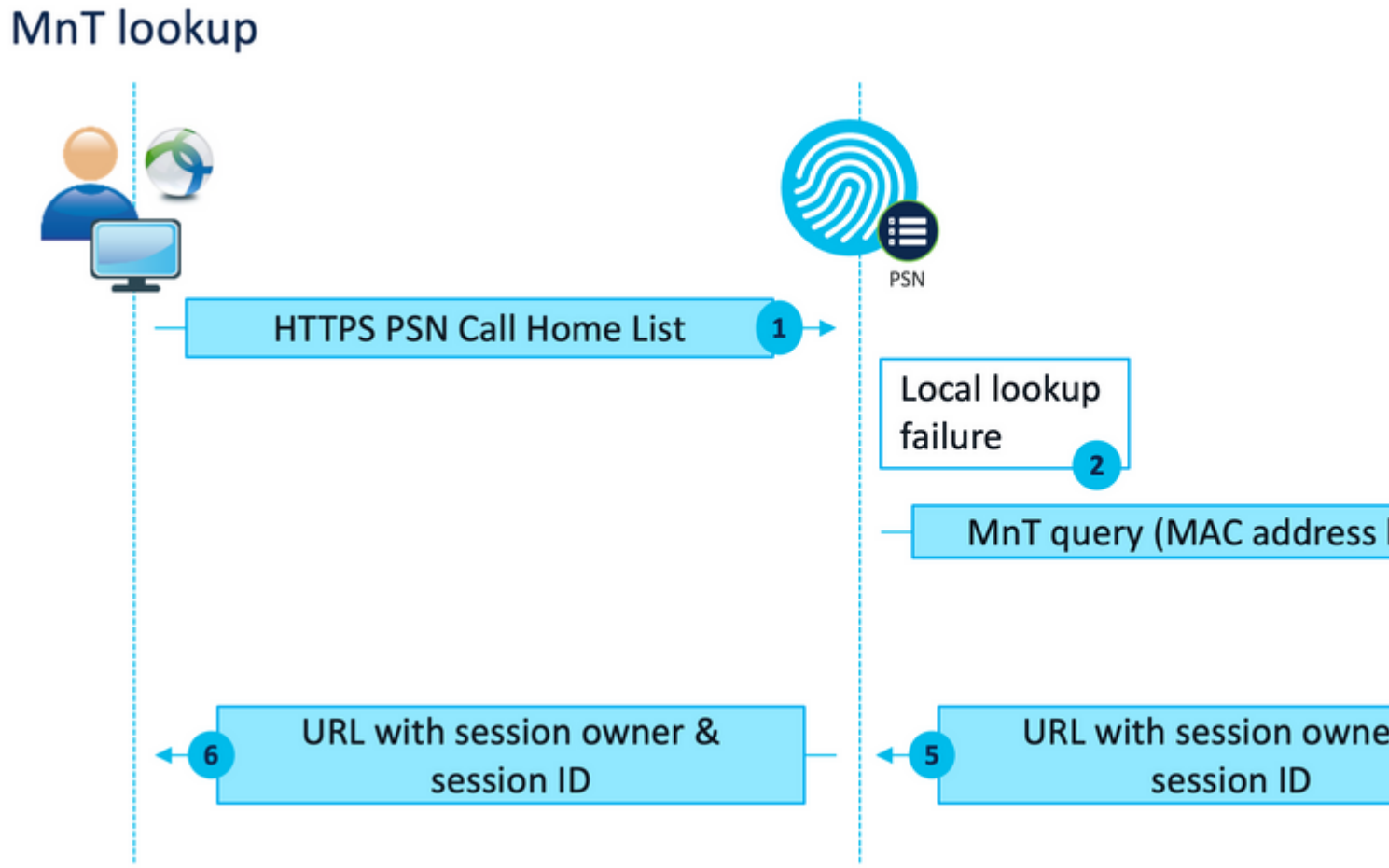
Un problème courant causé par l'utilisation de sondes connectionData.xml est une surcharge du déploiement ISE due à un grand nombre de requêtes HTTPS envoyées par les points d'extrémité. Il est important de considérer que, bien que le fichier connectiondata.xml soit efficace en tant que mécanisme de sauvegarde pour éviter les pannes complètes des mécanismes de redirection et de posture non réorientable, il ne constitue pas une solution durable pour un environnement de posture. Par conséquent, il est nécessaire de diagnostiquer et de résoudre les problèmes de conception et de configuration qui provoquent la défaillance des sondes de détection principales et qui entraînent des problèmes de détection.

Liste Call Home

La liste Call Home est une section du profil de posture dans laquelle une liste de PSN est spécifiée pour être utilisée pour la posture. Contrairement au fichier connectiondata.xml, il est créé et géré par un administrateur ISE et peut nécessiter une phase de conception pour une configuration optimale. La liste des PSN dans la liste Call Home doit correspondre à la liste des serveurs d'authentification et de gestion des

comptes qui est configurée dans le périphérique réseau ou l'équilibreur de charge pour RADIUS.

Les sondes Call Home List permettent l'utilisation d'une recherche MnT lors d'une recherche de session active en cas d'échec d'une recherche locale dans un PSN. La même fonctionnalité s'étend aux sondes connectiondata.xml uniquement lorsqu'elles sont utilisées lors de la détection de l'étape 2. Pour cette raison, toutes les sondes de l'étape 2 sont également appelées sondes de nouvelle génération.



flux de recherche MnT

Conception

Comme un processus de découverte sans redirection implique souvent un flux plus complexe et un plus grand nombre de traitements sur PSN et MnT par rapport à un flux de redirection, il existe deux défis communs qui peuvent survenir au cours de la mise en oeuvre :

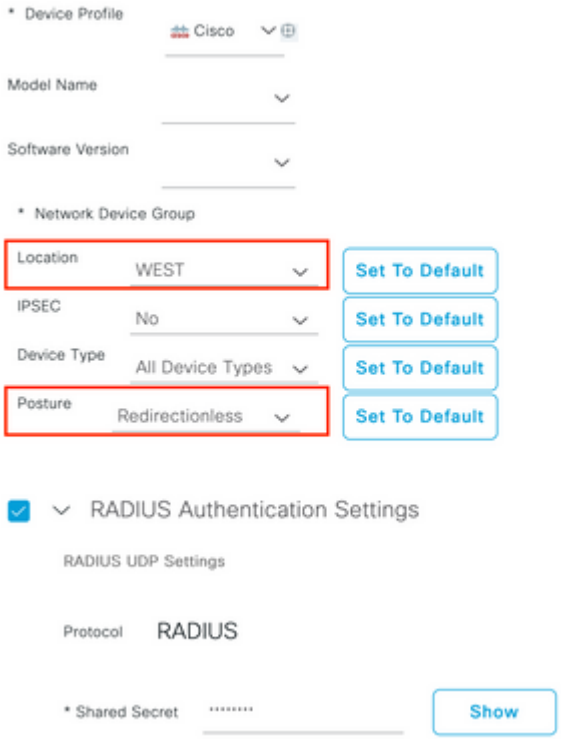
1. Découverte efficace
2. Performances du déploiement ISE

Afin de faire face à ces défis, il est recommandé de concevoir la liste Call Home pour limiter le nombre de PSN qu'un terminal donné peut utiliser pour la posture. Pour les déploiements de moyenne et grande envergure, il est nécessaire de distribuer le déploiement afin de créer plusieurs listes Call Home avec un nombre réduit de PSN, en conséquence la liste des PSN qui sont utilisés pour l'authentification RADIUS pour un périphérique réseau donné devrait être limitée de la même manière pour correspondre à la liste Call Home correspondante.

Les aspects suivants peuvent être pris en compte lors du développement de la stratégie de distribution PSN afin de déterminer le nombre maximal de PSN dans chaque liste Call Home :

- Nombre de PSN dans le déploiement
- Spécifications matérielles des noeuds PSN et MnT
- Nombre maximal de sessions de posture simultanées dans le déploiement
- Nombre de périphériques réseau
- Environnements hybrides (redirection simultanée et implémentation de posture sans redirection)
- Nombre de cartes utilisées par les points d'extrémité
- Emplacement des périphériques réseau et des PSN
- Types de connexion réseau utilisés pour la position (filaire, sans fil, VPN)

2. Sur ISE, accédez à **Administration** > **Network Resources** > **Network Devices** et cliquez sur **Add**. Configurez les groupes de périphériques réseau conformément à la conception et activez les **paramètres d'authentification RADIUS** pour configurer le **secret partagé**.



Configuration des périphériques réseau

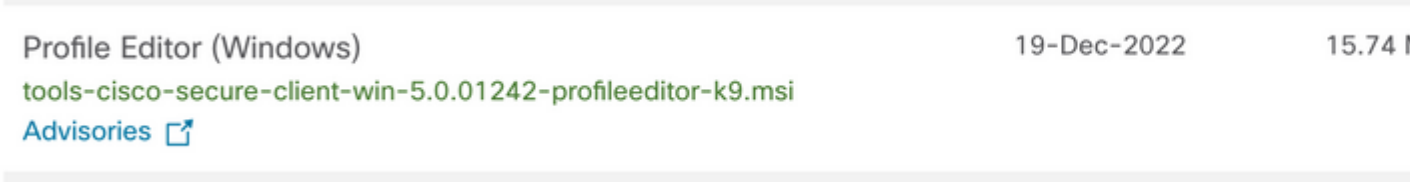
Provisionnement client

Il existe deux façons de fournir au client le logiciel et le profil appropriés pour effectuer la posture dans un environnement sans redirection :

1. Mise en service manuelle (pré-déploiement)
2. Portail d'approvisionnement client (déploiement Web)

Provisionnement manuel (pré-déploiement)

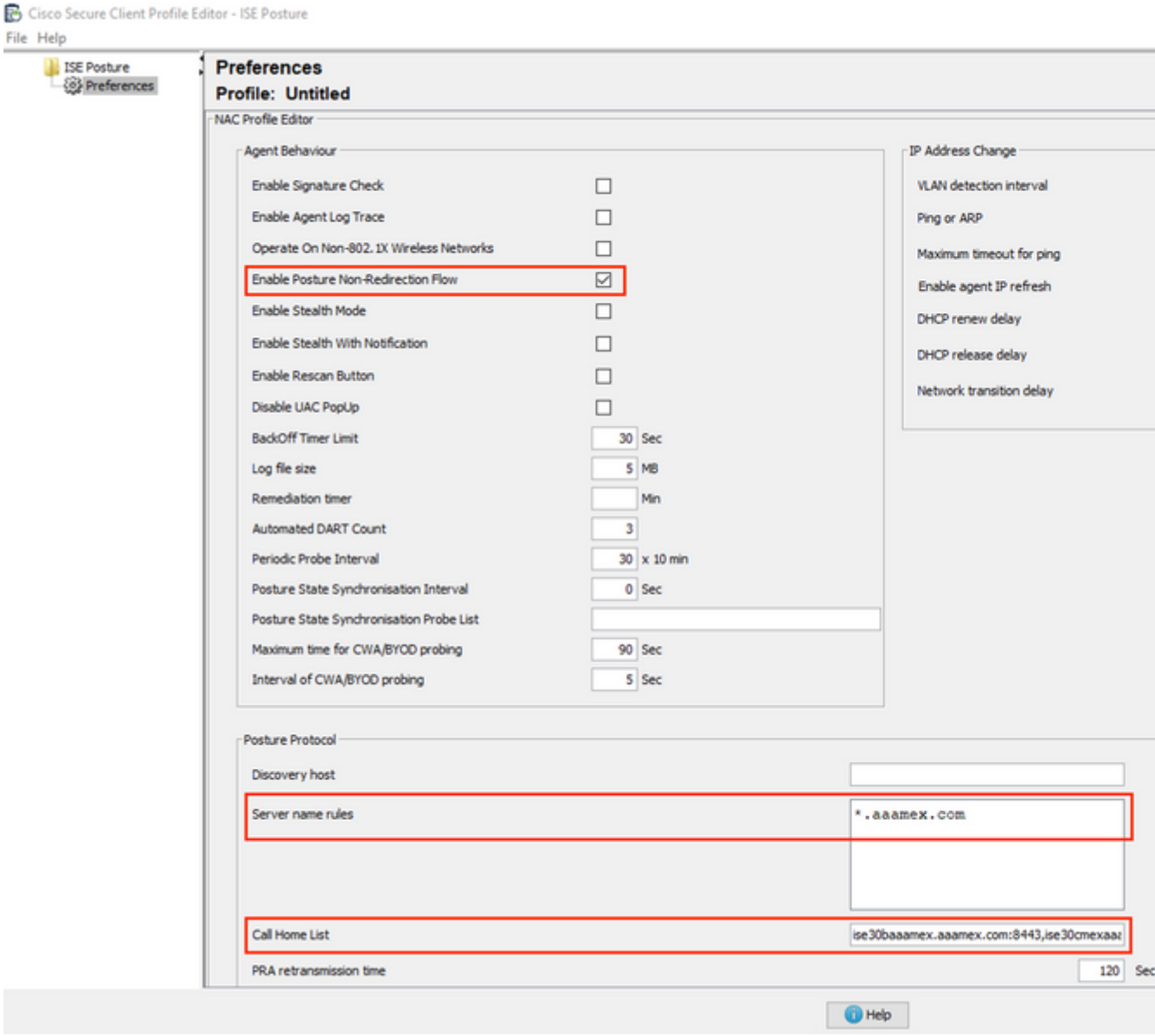
1. Téléchargez et installez Cisco Secure Client Profile Editor à partir de Cisco Software Download.



Package Éditeur de profil

2. Ouvrez l'éditeur de profil de posture ISE :
   - Assurez-vous que l'option **Enable Posture Non-Redirection Flow** est activée.
   - Configurez les **règles de nom de serveur** séparées par des virgules**.** Utilisez un seul astérisque * pour autoriser la connexion à tout PSN, des valeurs génériques pour autoriser la connexion à tout PSN dans un domaine spécifique ou les FQDN PSN pour limiter la connexion à des PSN spécifiques.

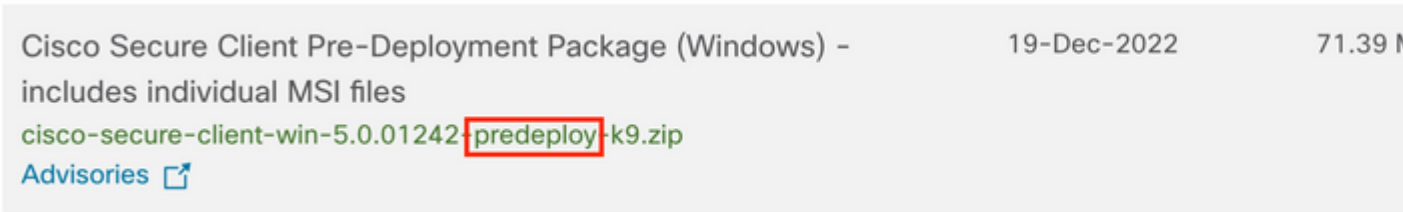
- Configurez **Call Home List** pour spécifier la liste de PSN séparés par des virgules. Veillez à ajouter le port du portail d'approvisionnement du client au format FQDN:port ou IP:port.



Configuration du profil de posture avec l'Éditeur de profil

> **Remarque** : reportez-vous à l'étape 4 de la section Politique d'approvisionnement du client pour obtenir des instructions sur la façon de vérifier le port du portail d'approvisionnement du client si nécessaire.

3. Répétez l'étape 2 pour chaque liste Call Home utilisée.
4. Téléchargez le package de prédéploiement du client sécurisé Cisco à partir de [Téléchargement de logiciels Cisco.](#)

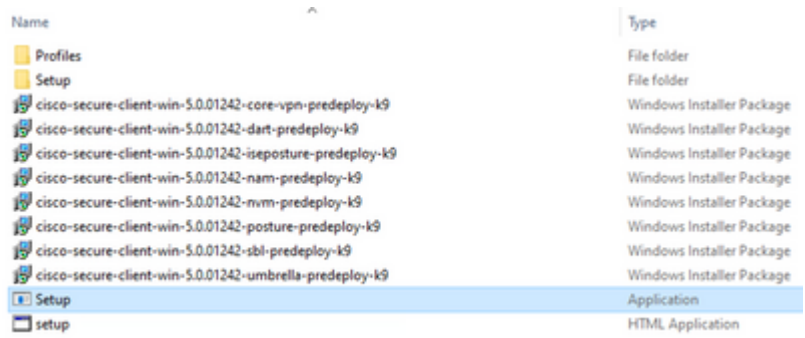


5. Enregistrez le profil sous le nom ISEPostureCFG.xml.
6. Distribuez les fichiers de profil et d'installation dans un fichier d'archive ou copiez les fichiers sur les clients.

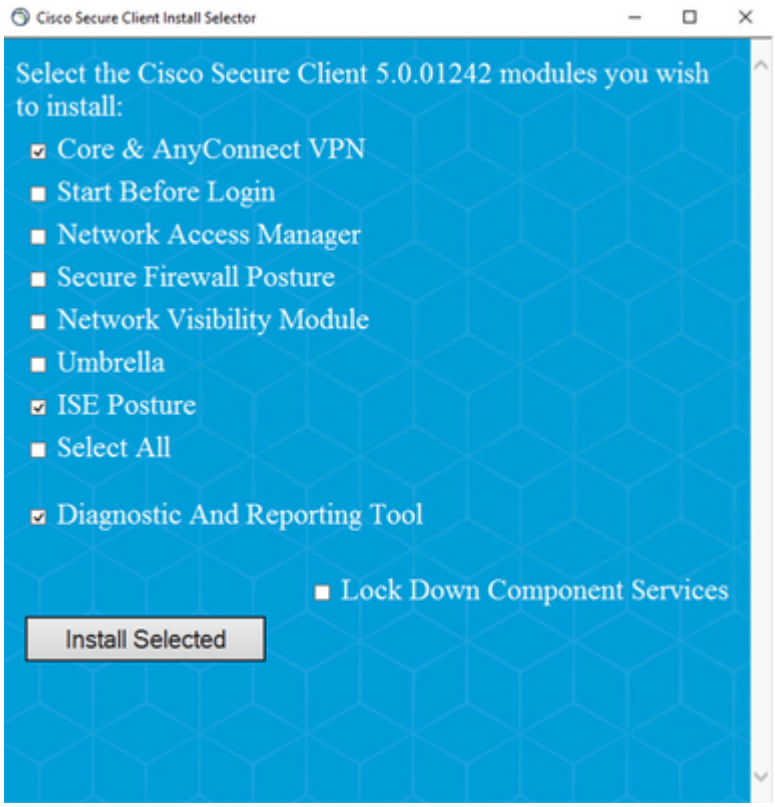
> **Avertissement** : assurez-vous que les mêmes fichiers Cisco Secure Client figurent également sur les têtes de réseau auxquelles vous prévoyez de vous connecter : pare-feu sécurisé ASA, ISE, etc. Même lorsque le provisionnement manuel est utilisé, ISE doit être configuré pour le provisionnement client avec la version logicielle correspondante. Reportez-vous à la section Configuration de la stratégie de provisionnement du client pour obtenir des instructions détaillées.

---

7. Sur le client, ouvrez le fichier zip dans et exécutez le programme d'installation pour installer les modules Core et ISE Posture. Vous pouvez également utiliser les fichiers msi individuels pour installer chaque module. Dans ce cas, vous devez vous assurer que le module core-vpn est installé en premier.



Cisco Secure Client pré-déploie le contenu du package



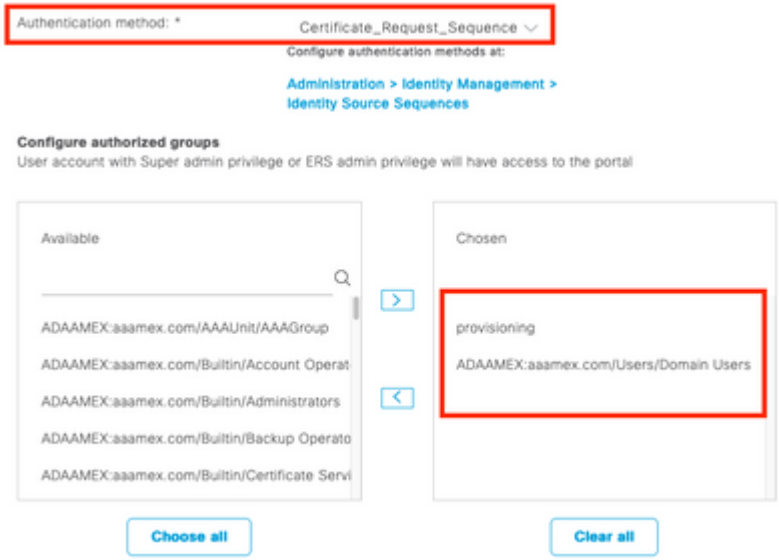
Conseil : installez l'outil Diagnostic and Reporting Tool à utiliser à des fins de dépannage.

8. Une fois l'installation terminée, copiez le fichier xml de profil de posture aux emplacements suivants :
   - Windows : %ProgramData%\Cisco\Cisco Secure Client\ISE Posture
   - MacOS : /opt/cisco/secureclient/iseposture/

Portail d'approvisionnement client (déploiement Web)

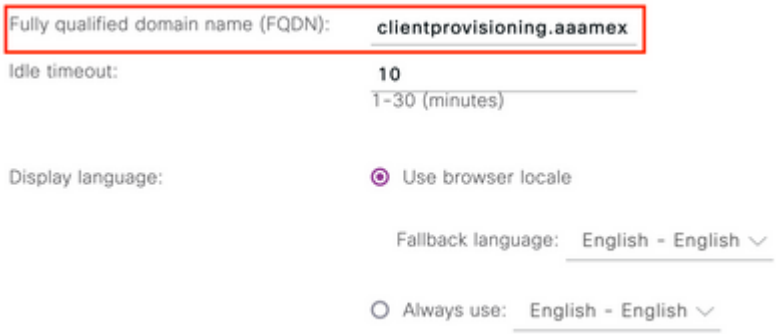
ISE Client Provisioning Portal peut être utilisé pour installer le module Cisco Secure Client ISE Posture et le profil de posture d'ISE. Il peut également être utilisé pour pousser le profil de posture seul si le module de posture ISE est déjà installé sur le client.

1. Accédez à **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning** Portal pour ouvrir la configuration du portail. Développez la section **Paramètres du portail** et localisez le champ **Méthode d'authentification**, sélectionnez la **séquence source d'identité** à utiliser pour l'authentification dans le portail.
2. Configurez les groupes d'identités internes et externes qui sont autorisés à utiliser le portail d'approvisionnement du client.



Méthode d'authentification et groupes autorisés dans les paramètres du portail

3. Dans le champ **Nom de domaine complet (FQDN)**, configurez l'URL utilisée par les clients pour accéder au portail. Pour configurer plusieurs noms de domaine complets, entrez les valeurs séparées par des virgules.



4. Configurez le ou les serveurs DNS pour résoudre l'URL du portail vers les PSN de la liste Call Home correspondante.

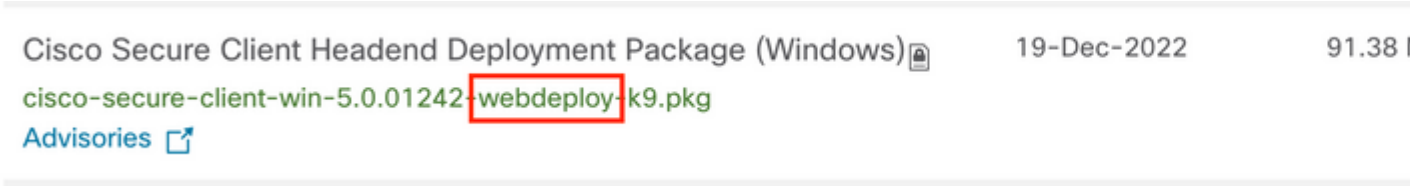
5. Fournir le nom de domaine complet aux utilisateurs finaux pour qu'ils puissent accéder au portail afin d'installer le logiciel ISE Posture.

Remarque : pour utiliser le nom de domaine complet du portail, les clients doivent disposer de la chaîne de certificats Admin PSN et de la chaîne de certificats Portal installées dans le magasin de confiance, et le certificat Admin doit contenir le nom de domaine complet du portail dans le champ SAN.

Stratégie de provisionnement du client

La mise en service du client doit être configurée sur ISE, quel que soit le type de mise en service (pré-déploiement ou déploiement Web) utilisé pour installer Cisco Secure Client sur les terminaux.

1. Téléchargez le package Cisco Secure Client webdeploy à partir de Cisco Software Download.

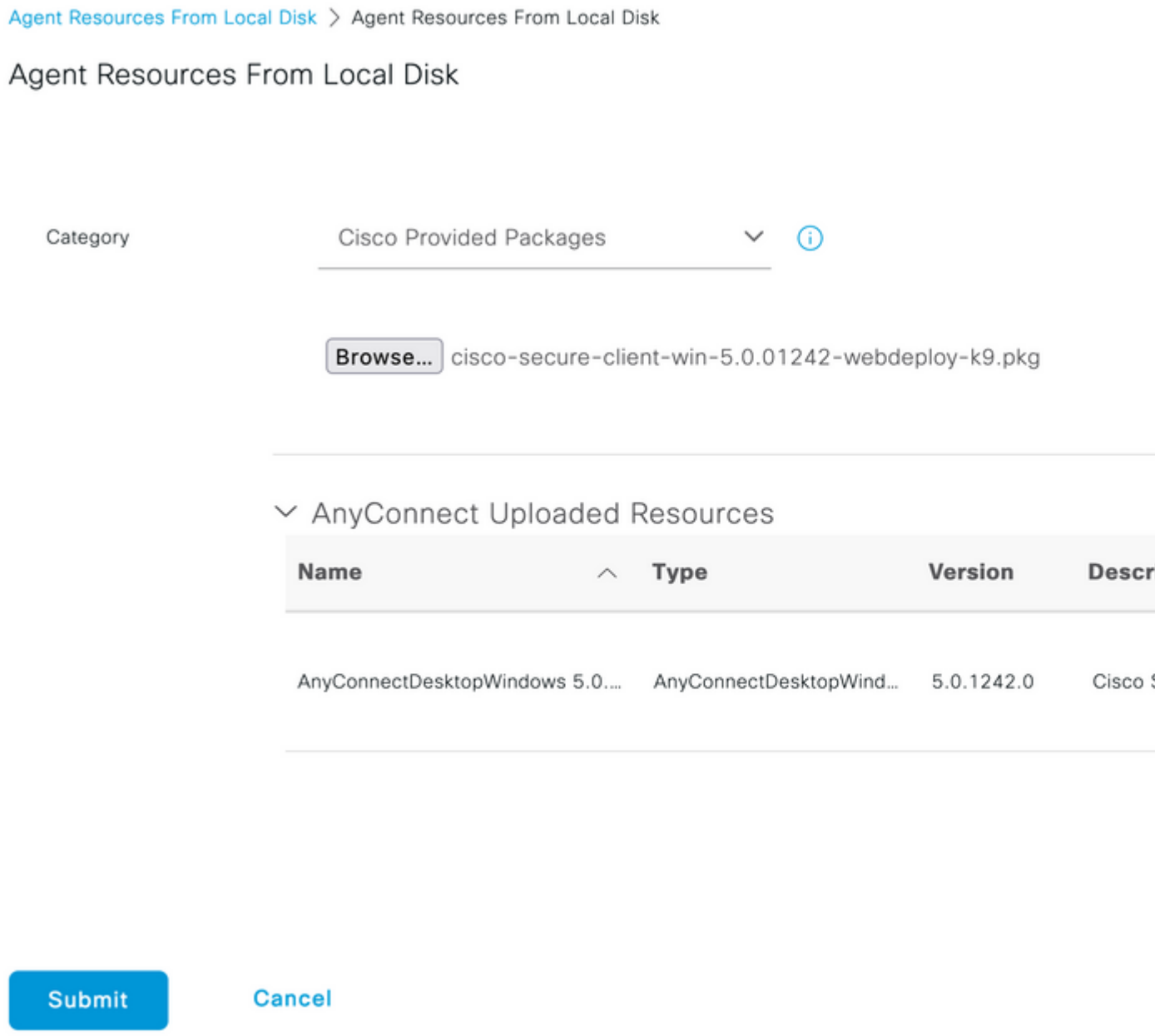


Package de déploiement Web Cisco Secure Client

2. Téléchargez le dernier package de déploiement Web du module de conformité à partir de Téléchargement de logiciels Cisco.

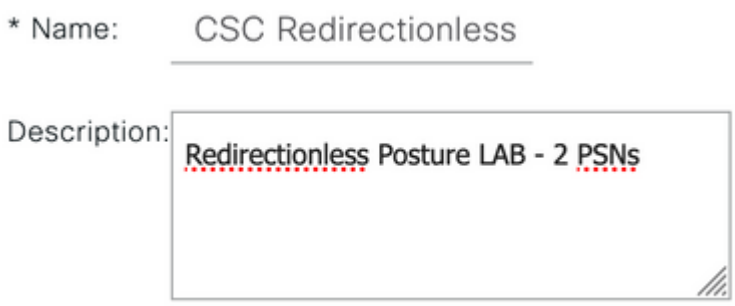
Module de conformité ISE, package webdeploy

3. Sur ISE, accédez à Work Centers > Posture > Client Provisioning > **Resources** et cliquez sur **Add** > **Agent resources from local disk**. Sélectionnez **Cisco Provided Packages** dans le menu déroulant Category et téléchargez le package de déploiement Web Cisco Secure Client précédemment téléchargé. Répétez la même procédure pour télécharger le module de conformité.



Télécharger les packages fournis par Cisco vers ISE

4. Dans l'onglet **Resources**, cliquez sur **Add** > **AnyConnect Posture Profile**. Sur le profil :
   - Configurez un **nom** pouvant être utilisé pour identifier le profil dans ISE.
   - Configurez les **règles de nom de serveur** séparées par des virgules**.** Utilisez un seul astérisque * pour autoriser la connexion à tout PSN, des valeurs génériques pour autoriser la connexion à tout PSN dans un domaine spécifique ou les FQDN PSN pour limiter la connexion à des PSN spécifiques.
   - Configurez **Call Home List** pour spécifier la liste de PSN séparés par des virgules. Assurez-vous d'ajouter le port du portail d'approvisionnement du client au format FQDN:port ou IP:port.



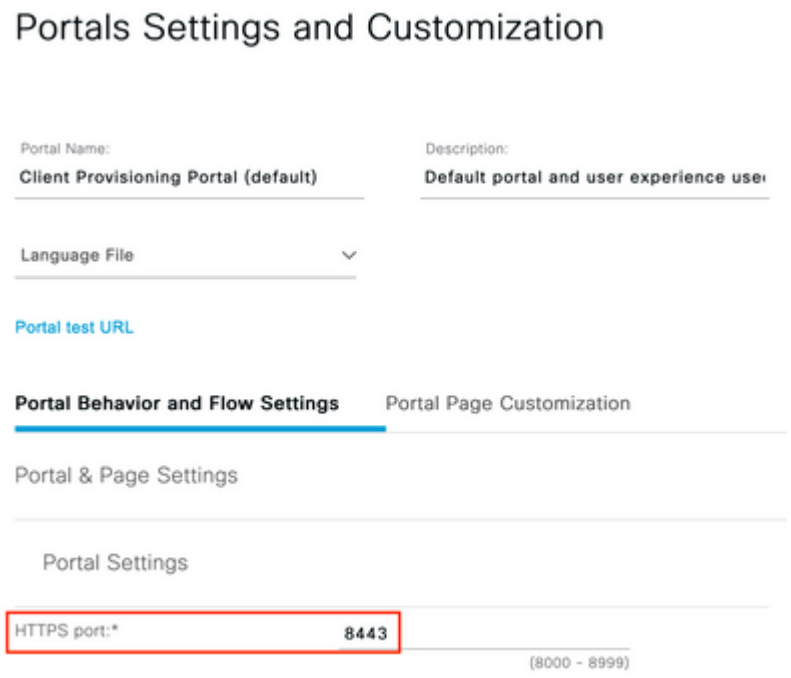
Configuration du profil de position ISE I

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
* Server name rules	*.aamex.com	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List	xx.aamex.com:8443,	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Configuration du profil de posture ISE II

Pour trouver le port qui doit être utilisé dans la liste Call Home, accédez à **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning Portal**, sélectionnez le portail en cours d'utilisation et développez Portal Settings.



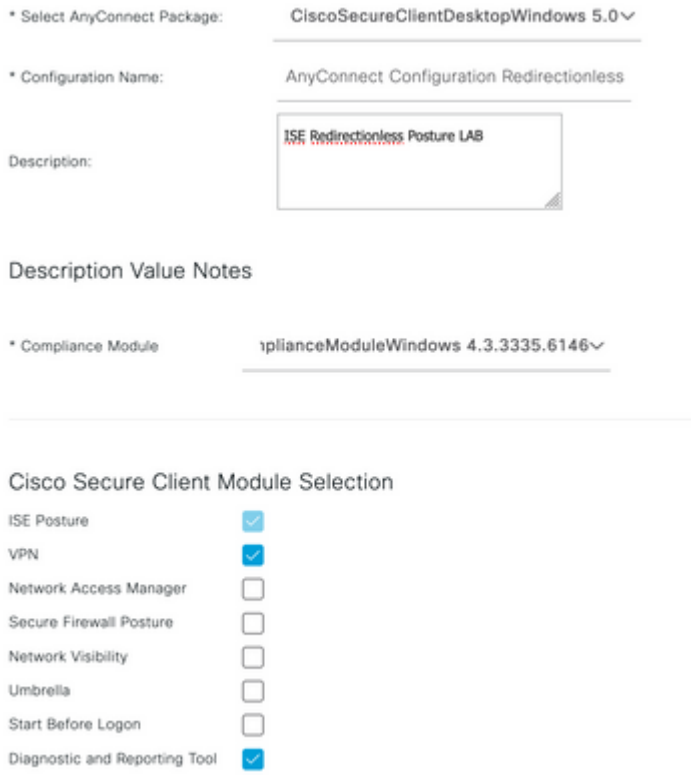
Port du portail de provisionnement client

5. Dans lâ€™onglet **Resources**, cliquez sur **Add** > **AnyConnect Configuration**. Sélectionnez le package Cisco Secure Client et le module de conformité à utiliser.

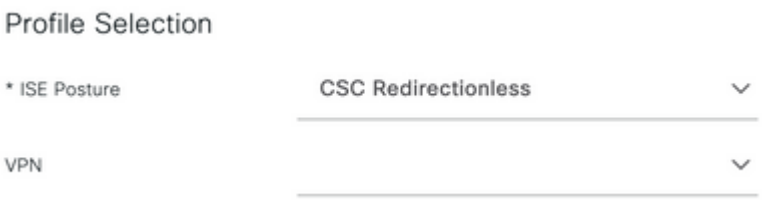
> **Avertissement** : si le client sécurisé Cisco a été pré-déployé sur les clients, assurez-vous que la version sur ISE correspond à la version sur les terminaux. Si ASA ou FTD est utilisé pour le déploiement Web, la version de ce périphérique doit également correspondre.

---

6. Faites défiler jusqu'à la section **Sélection de la posture** et sélectionnez le profil qui a été créé à l'étape 1. Cliquez sur **Submit** au bas de la page pour enregistrer la configuration.



Configuration AnyConnect



Sélection du profil

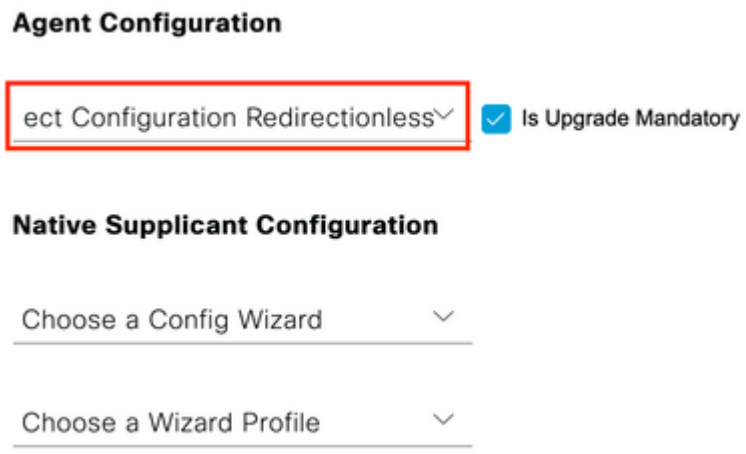
7. Accédez à **Work Centers** > **Posture** > **Client Provisioning** > **Client Provisioning policy**. Localisez la stratégie utilisée pour le système d'exploitation requis et cliquez sur **Edit**. Cliquez sur le signe **+** dans la colonne **Results** et sélectionnez la configuration AnyConnect de l'étape 5 sous la section **Agent Configuration**.

> **Remarque** : dans le cas de plusieurs listes Call Home, utilisez le champ **Other Conditions** pour envoyer le bon profil aux clients correspondants. Dans l'exemple, Device Location Group

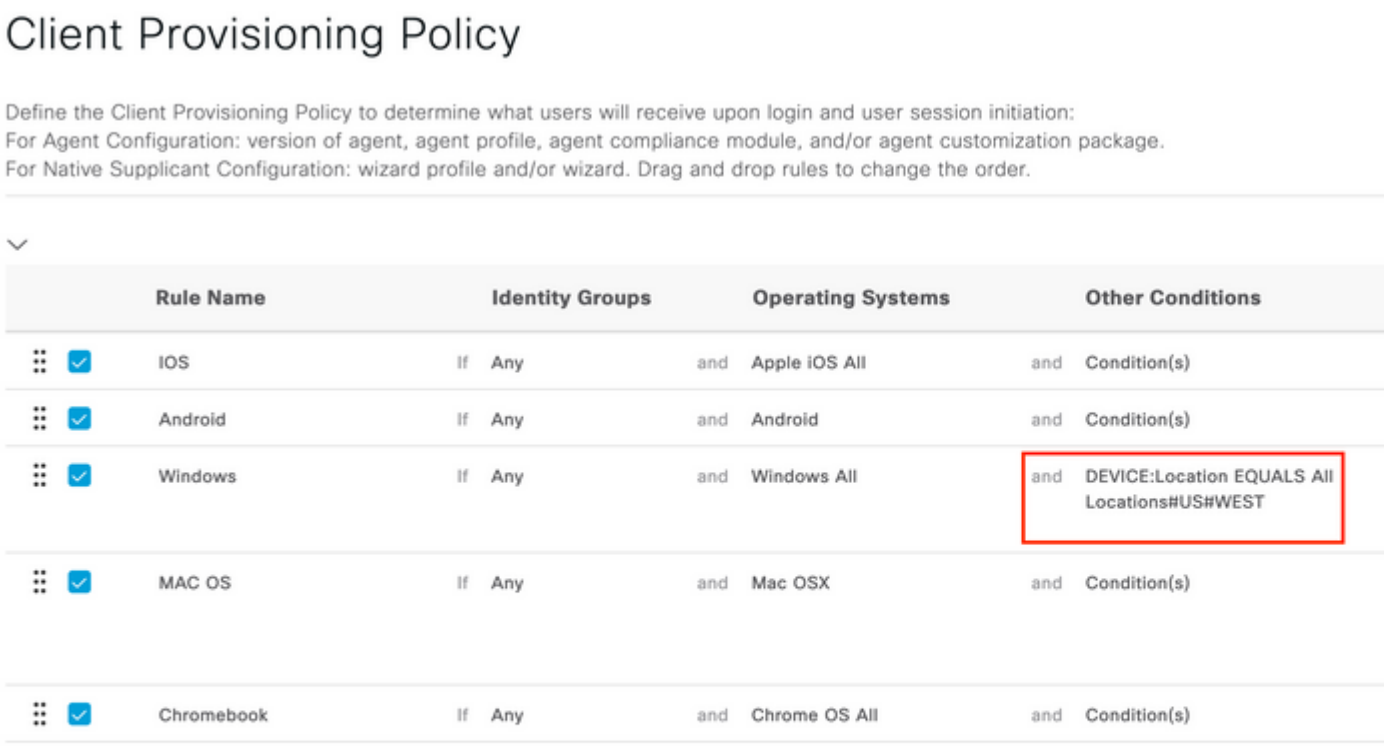
---

est utilisé pour identifier le profil de posture qui est poussé dans la stratégie.

Conseil : si plusieurs stratégies d'approvisionnement client sont configurées pour le même système d'exploitation, il est recommandé de les rendre mutuellement exclusives, c'est-à-dire qu'un client donné ne doit pouvoir accéder qu'à une seule stratégie à la fois. Les attributs RADIUS peuvent être utilisés sous la colonne **Other Conditions** pour différencier une politique d'une autre.



Configuration de l'agent de stratégie de provisionnement client



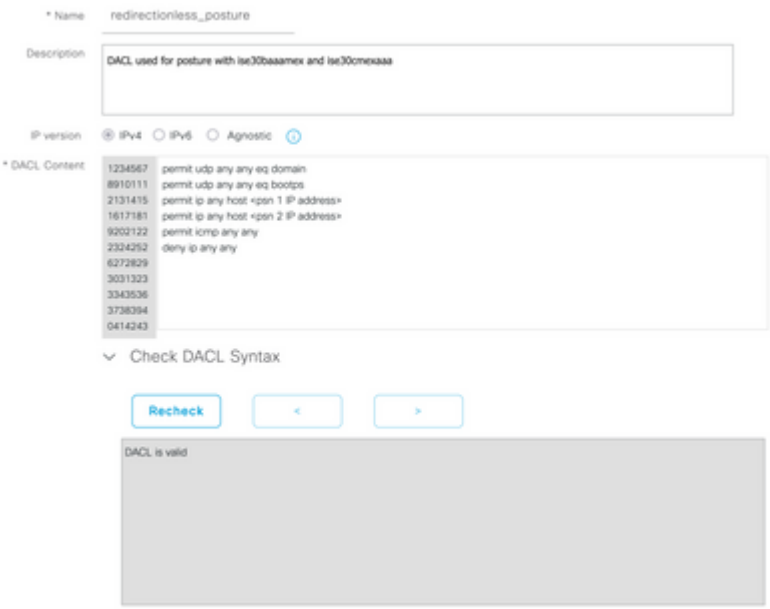
Politique de provisionnement client

8. Répétez les étapes 4 à 7 pour chaque liste Call Home et le profil de position correspondant en cours d'utilisation. Pour les environnements hybrides, les mêmes profils peuvent être utilisés pour rediriger les clients.

Autorisation

Profil d'autorisation

1. Accédez à Policy > Policy Elements > Results > **Authorization** > **Downloadable ACLs** et cliquez sur **Add**.
2. Créez une liste DACL pour autoriser le trafic vers DNS, DHCP (le cas échéant), les PSN ISE et bloquer tout autre trafic. Assurez-vous d'autoriser tout autre trafic nécessaire à l'accès avant l'accès conforme final.



Configuration DACL

permit udp any any eq domain
permit udp any any eq bootps
permit ip any host

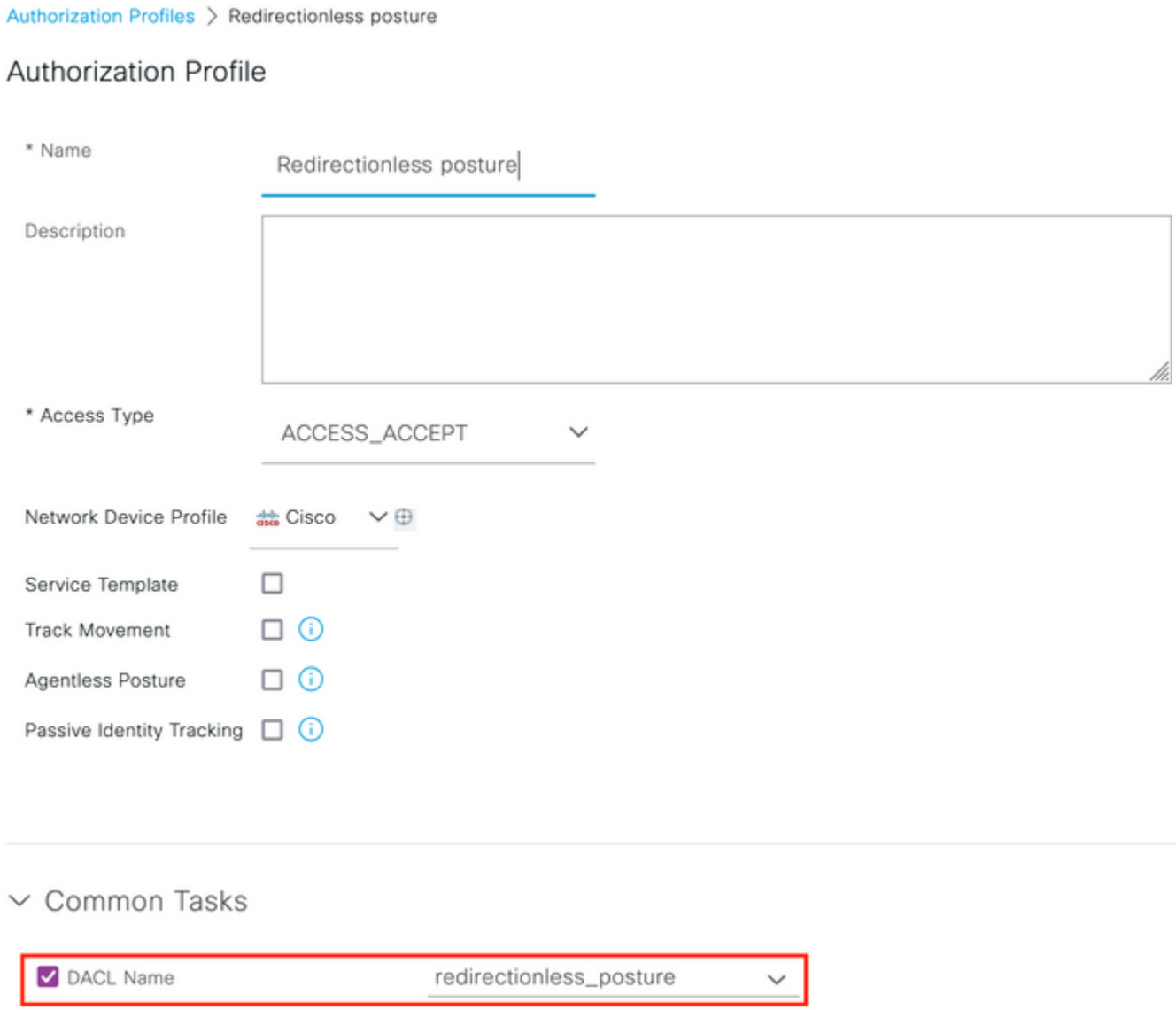
permit ip any host

deny ip any any

Attention : certains périphériques tiers peuvent ne pas prendre en charge les listes de contrôle d'accès numériques. Dans ce cas, il est nécessaire d'utiliser un ID de filtre ou d'autres attributs spécifiques au fournisseur. Reportez-vous à la documentation du fournisseur pour plus d'informations. Si aucune liste de contrôle dâ€™accès nâ€™est utilisée, assurez-vous de configurer la liste correspondante dans le périphérique réseau.

---

3. Accédez à Politique > Éléments de politique > Résultats > **Autorisation** > **Profils d'autorisation** et cliquez sur **Ajouter**. Attribuez un nom au profil d'autorisation et sélectionnez le **nom DACL** dans **Tâches courantes.** Dans le menu déroulant, sélectionnez la DACL créée à l'étape 2.



Profil d'autorisation

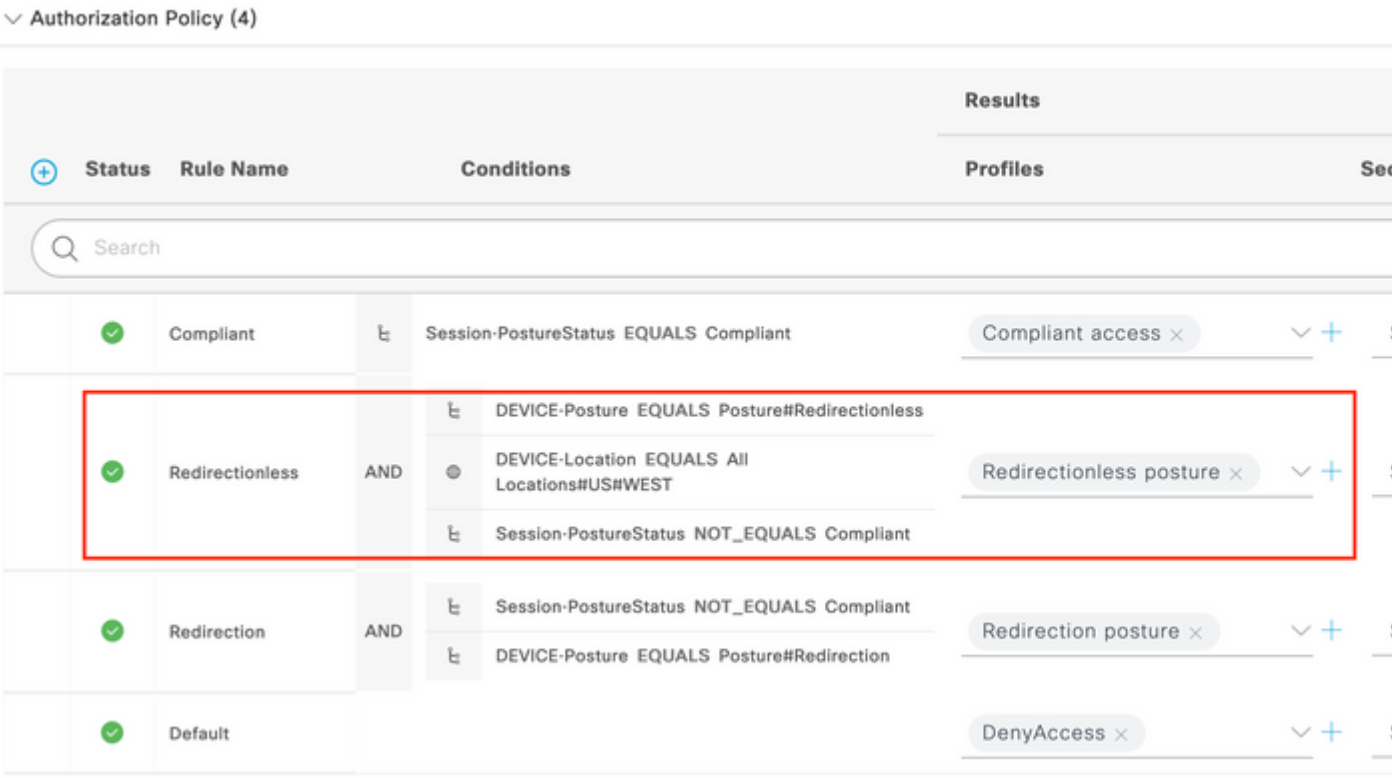
> **Remarque** : si aucune liste de contrôle d'accès n'est utilisée, utilisez **Filter-ID** from **Common Tasks** ou les **Advanced Attribute Settings** pour transmettre le nom de la liste de contrôle d'accès correspondante.

---

4. Répétez les étapes 1 à 3 pour chaque liste Call Home utilisée. Pour les environnements hybrides, un seul profil d'autorisation est nécessaire pour la redirection. La configuration du profil d'autorisation pour la redirection sort du cadre de ce document.

Politique d'autorisation

1. Accédez à **Policy** > **Policy Sets** et ouvrez le jeu de stratégies utilisé ou créez-en un nouveau.
2. Faites défiler jusqu'à la section **Authorization Policy**. Créez une stratégie d'autorisation à l'aide de **Session PostureStatus NOT_EQUALS Compliant** et sélectionnez le profil d'autorisation créé dans la section précédente.



Stratégies d'autorisation

3. Répétez l'étape 2 pour chaque profil d'autorisation avec la liste Call Home correspondante utilisée. Pour les environnements hybrides, une seule politique d'autorisation de redirection est nécessaire.

Dépannage

Conformité au client sécurisé Cisco et état Non applicable (en attente) sur ISE

Sessions obsolètes/fantômes

La présence de sessions obsolètes ou fantômes dans le déploiement peut générer des pannes intermittentes et apparemment aléatoires avec la découverte de posture sans redirection, ce qui a pour conséquence que les utilisateurs sont bloqués dans une posture d'accès inconnu/non applicable sur ISE alors que l'interface utilisateur du client sécurisé Cisco montre un accès conforme.

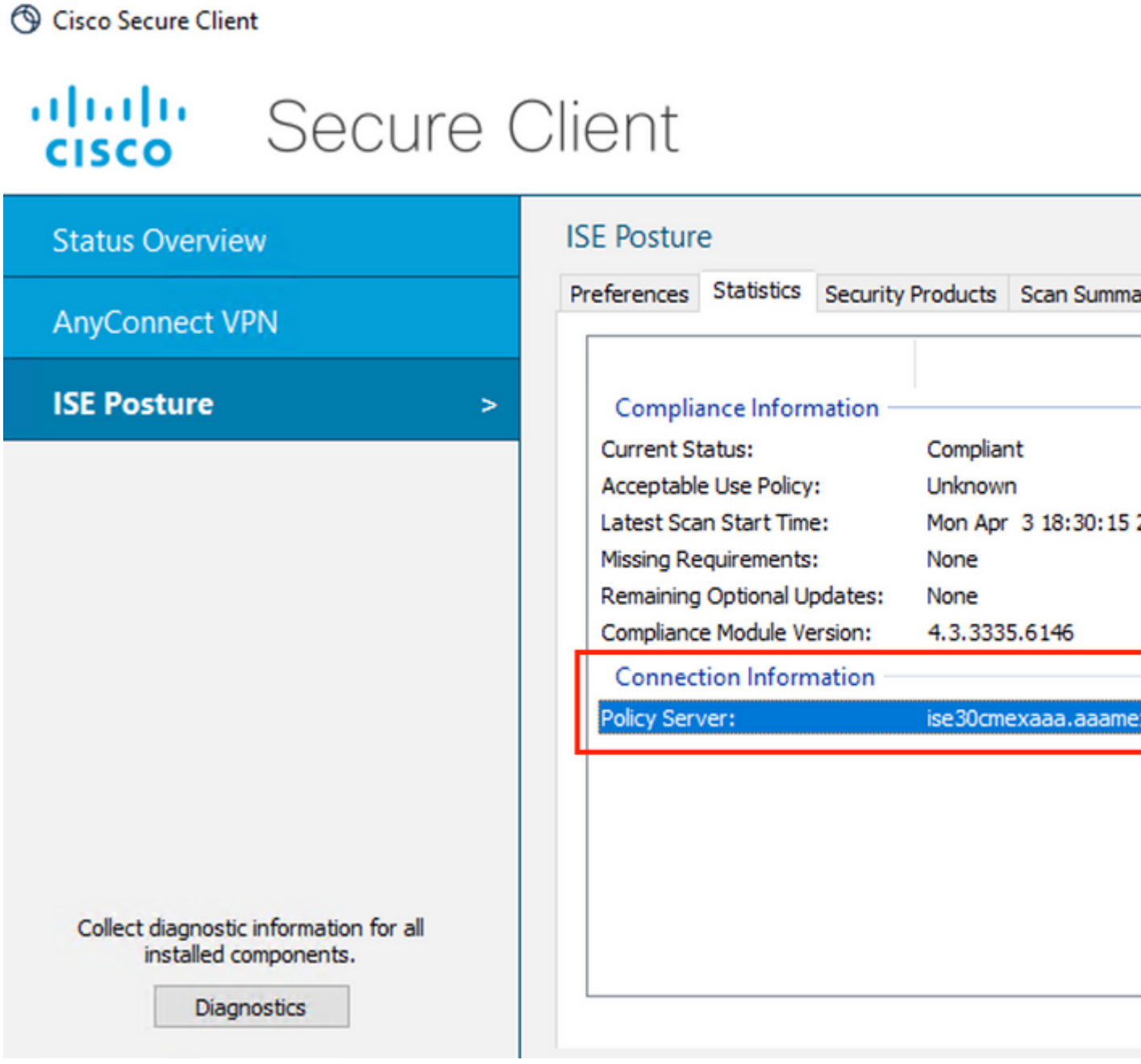
Les sessions obsolètes sont d'anciennes sessions qui ne sont plus actives. Ils sont créés par une demande d'authentification et un démarrage de la gestion des comptes, mais aucun arrêt de la gestion des comptes n'est reçu sur le PSN pour effacer la session.

Les sessions fantômes sont des sessions qui n'ont jamais été actives dans un PSN particulier. Ils sont créés par une mise à jour intermédiaire de la comptabilité, mais aucun arrêt de la comptabilité n'est reçu sur le PSN pour effacer la session.

Identifier

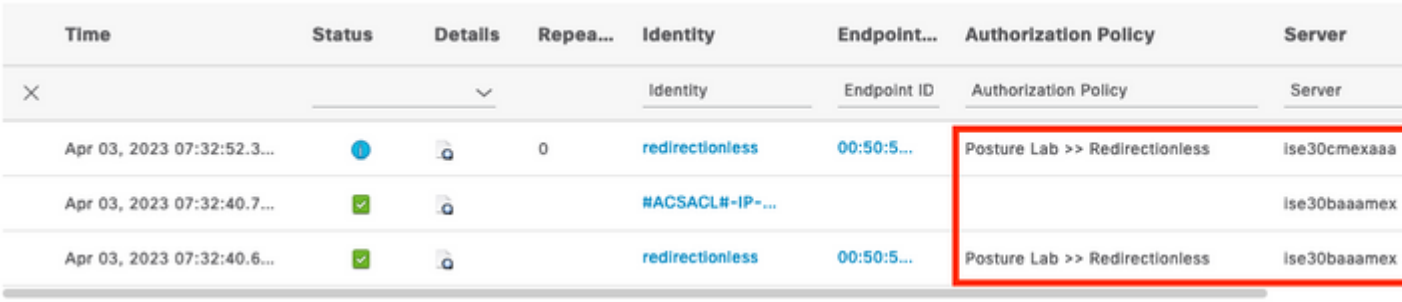
Pour identifier un problème de session obsolète/fantôme, vérifiez le PSN utilisé dans l'analyse du système sur le client et comparez-le au PSN effectuant l'authentification :

1. Dans l'interface utilisateur de Cisco Secure Client, cliquez sur l'**icône** relative à l'**engrenage** dans le coin inférieur gauche. Dans le menu de gauche, ouvrez la section **Position ISE** et accédez à l'onglet **Statistiques**. Notez le serveur de stratégie dans les informations de connexion.



Policy Server pour la position ISE dans Cisco Secure Client

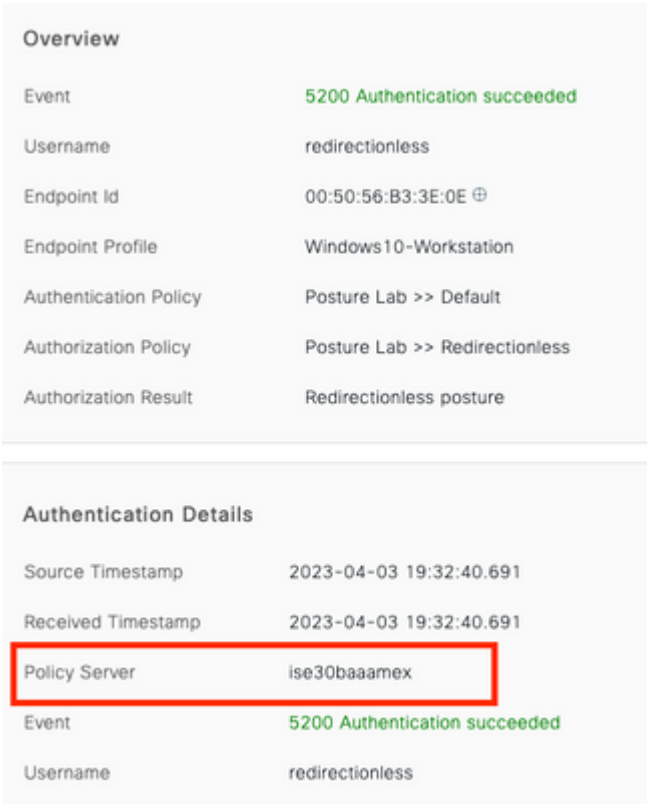
2. Dans les journaux en direct ISE RADIUS, prenez note des points suivants :
   - Changement d'état de posture
   - Modification du serveur
   - Aucun changement dans la politique d'autorisation et le profil d'autorisation
   - Pas de journal en direct CoA



Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server
				Identity	Endpoint ID	Authorization Policy	Server
Apr 03, 2023 07:32:52.3...			0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30cmexaaa
Apr 03, 2023 07:32:40.7...				#ACSACL#-IP-...			ise30baaamex
Apr 03, 2023 07:32:40.6...				redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30baaamex

Journaux actifs pour les sessions obsolètes/fantômes

3. Ouvrez la session en direct ou les détails du journal en direct de la dernière authentification. Notez que le serveur Policy Server, s'il diffère du serveur observé à l'étape 1, indique un problème avec les sessions obsolètes/fantômes.



Overview

Event	5200 Authentication succeeded
Username	redirectionless
Endpoint Id	00:50:56:B3:3E:0E
Endpoint Profile	Windows10-Workstation
Authentication Policy	Posture Lab >> Default
Authorization Policy	Posture Lab >> Redirectionless
Authorization Result	Redirectionless posture

Authentication Details

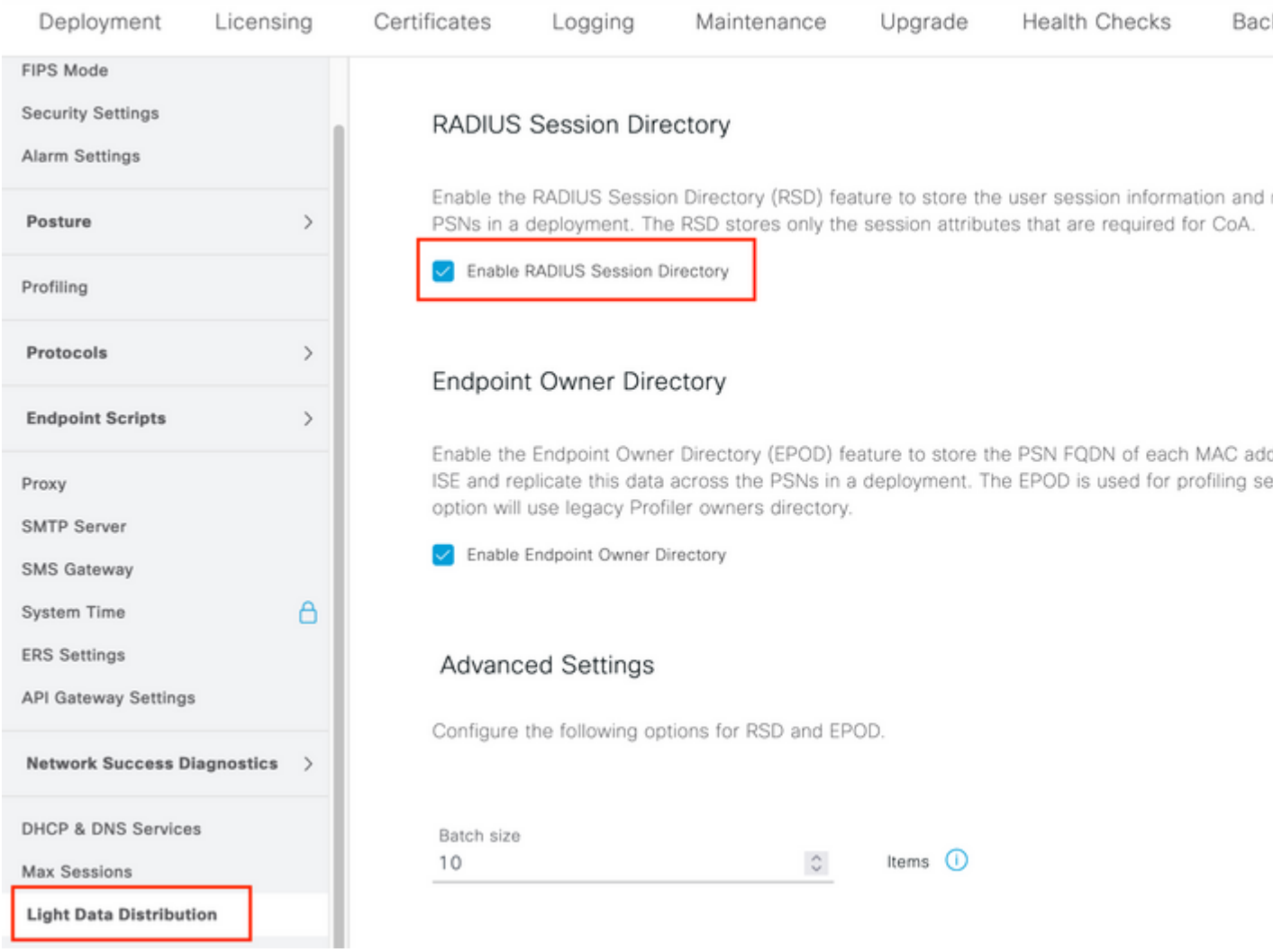
Source Timestamp	2023-04-03 19:32:40.691
Received Timestamp	2023-04-03 19:32:40.691
Policy Server	ise30baaamex
Event	5200 Authentication succeeded
Username	redirectionless

Serveur de stratégie dans les détails du journal en direct

Solution

Les versions ISE supérieures aux correctifs 6 et 3 de la version 2.6 d'ISE mettent en oeuvre le répertoire de session RADIUS comme solution pour un scénario de session obsolète/fantôme dans un flux de posture sans redirection.

1. Accédez à Administration > **System** > **Settings** > **Light Data Distribution** et vérifiez que la case à cocher Enable RADIUS Session Directory est activée.



Activer le répertoire de session RADIUS

2. À partir de l'interface de ligne de commande ISE, vérifiez que **ISE Messaging Service** est exécuté sur **tous les PSN** en exécutant la commande **show applications status ise.**

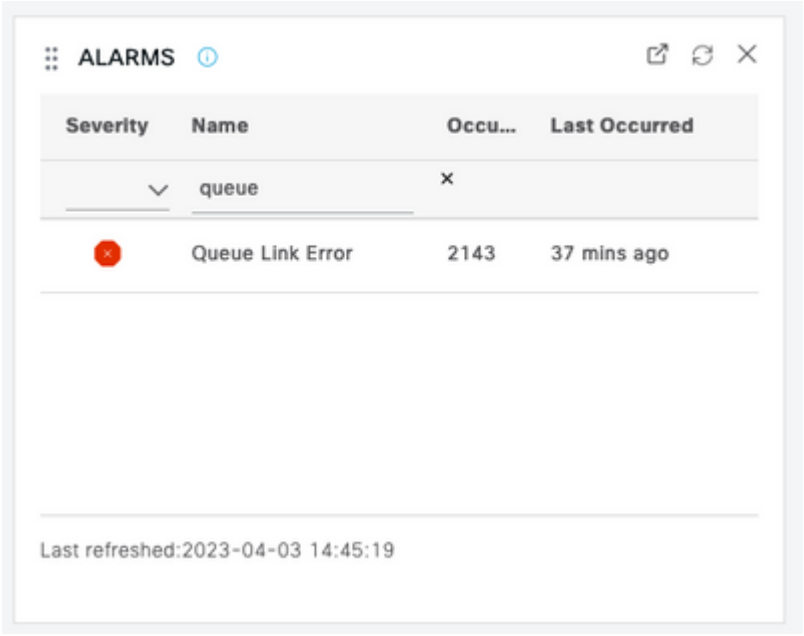
```
ise30cmexaaa/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          12434
Database Server                        running          112 PROCESSES
Application Server                     running          33093
Profiler Database                      running          19622
ISE Indexing Engine                    running          42923
AD Connector                           running          60317
M&T Session Database                   running          19361
M&T Log Processor                      running          33283
Certificate Authority Service          disabled
EST Service                            disabled
SXP Engine Service                     disabled
Docker Daemon                          running          14791
TC-NAC MongoDB Container               running          18594
TC-NAC Core Engine Container           running          18981
VA Database                            running          53465
VA Service                             running          53906
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  running          55480
PassiveID Syslog Service               running          56312
PassiveID API Service                  running          57153
PassiveID Agent Service                running          58079
PassiveID Endpoint Service             running          59138
PassiveID SPAN Service                 running          60059
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          16526
ISE API Gateway Database Service       running          18463
ISE API Gateway Service                running          23052
```

Service de messagerie ISE en cours

> **Remarque** : ce service fait référence à la méthode de communication utilisée pour RSD entre PSN et doit être exécuté quel que soit l'état du paramètre de service de messagerie ISE pour Syslog qui peut être défini à partir de l'interface utilisateur ISE.

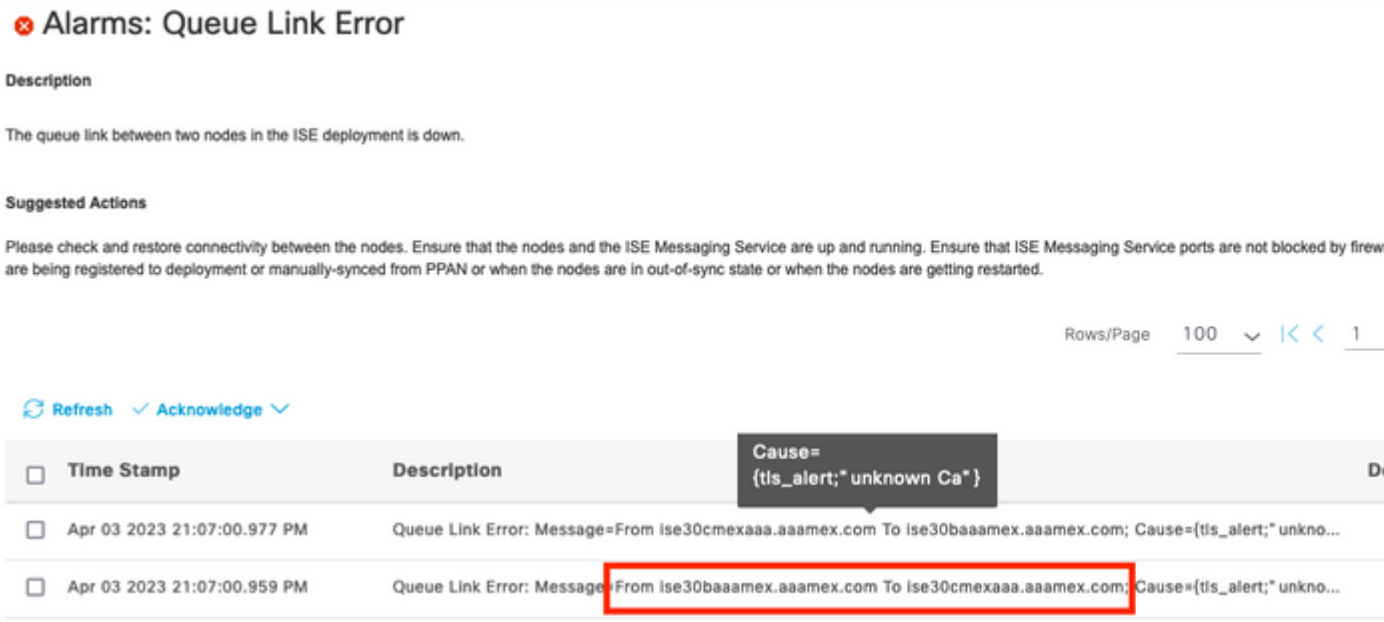
---

3. Accédez à **Tableau de bord** ISE et localisez le dashlet **Alarmes**. Vérifiez s'il existe des alarmes d'**erreur de liaison de file d'attente**. Cliquez sur le nom de l'alarme pour en savoir plus.



Alarmes d'erreur Queue Link

4. Vérifiez si les alarmes sont générées entre les PSN utilisés pour la posture.



Détails d'alarme Queue Link Error

5. Passez le curseur sur la description de l'alarme pour afficher tous les détails et prendre note du champ Cause. Les deux causes les plus courantes d'erreur de liaison de file d'attente sont :
   - Time out : indique que les requêtes envoyées par un noeud à un autre noeud sur le port 8671 ne reçoivent pas de réponse dans le seuil. Pour corriger le problème, vérifiez que le port TCP 8671 est autorisé entre les noeuds.
   - Autorité de certification inconnue : indique que la chaîne de certificats qui signe le certificat de messagerie ISE n'est pas valide ou est incomplète. Pour corriger cette erreur :
     a. Accédez à **Administration** > **System** > **Certificates** > Certificate sign requests.
     b. Cliquez sur **Générer des demandes de signature de certificat (CSR)**.
     c. Dans le menu déroulant, sélectionnez **ISE Root CA** et cliquez sur **Replace ISE Root CA Certificate chain**.
     Si l'autorité de certification racine ISE n'est pas disponible, accédez à **Certificate Authority** > **Internal CA settings** et cliquez sur **Enable Certificate Authority**, puis revenez au CSR et régénérez l'autorité de certification racine.
     d. Générez un nouveau CSR et sélectionnez **ISE Messaging Service** dans le menu déroulant.
     e. Sélectionnez tous les noeuds du déploiement et régénérez le certificat.

> **Remarque** : il est prévu d'observer les alarmes d'erreur de liaison de file d'attente avec la cause Unknown CA ou Econ refusé tandis que les certificats sont régénérés, surveiller les alarmes après la génération de certificat pour confirmer que le problème est résolu.

Performances

Identifier

Les problèmes de performances tels qu'une utilisation CPU élevée et une charge moyenne élevée liés à une posture sans redirection peuvent avoir un impact sur PSN ainsi que sur les noeuds MnT et sont souvent accompagnés ou précédés par les événements suivants :

- Aléatoire ou intermittente *Aucun serveur de stratégie détecté* erreurs dans Cisco Secure Client
- *La limite de ressources maximale a atteint* les rapports pour le *pool de threads de service Portal a atteint les* événements de *valeur de seuil*. Accédez à Opérations > **Rapports** > **Rapports** > **Audit** >

Audit des opérations pour afficher les rapports.
- *La requête de posture à la recherche MNT contient des* alarmes *élevées*. Ces alarmes sont uniquement générées sur ISE 3.1 et les versions ultérieures.

Solution

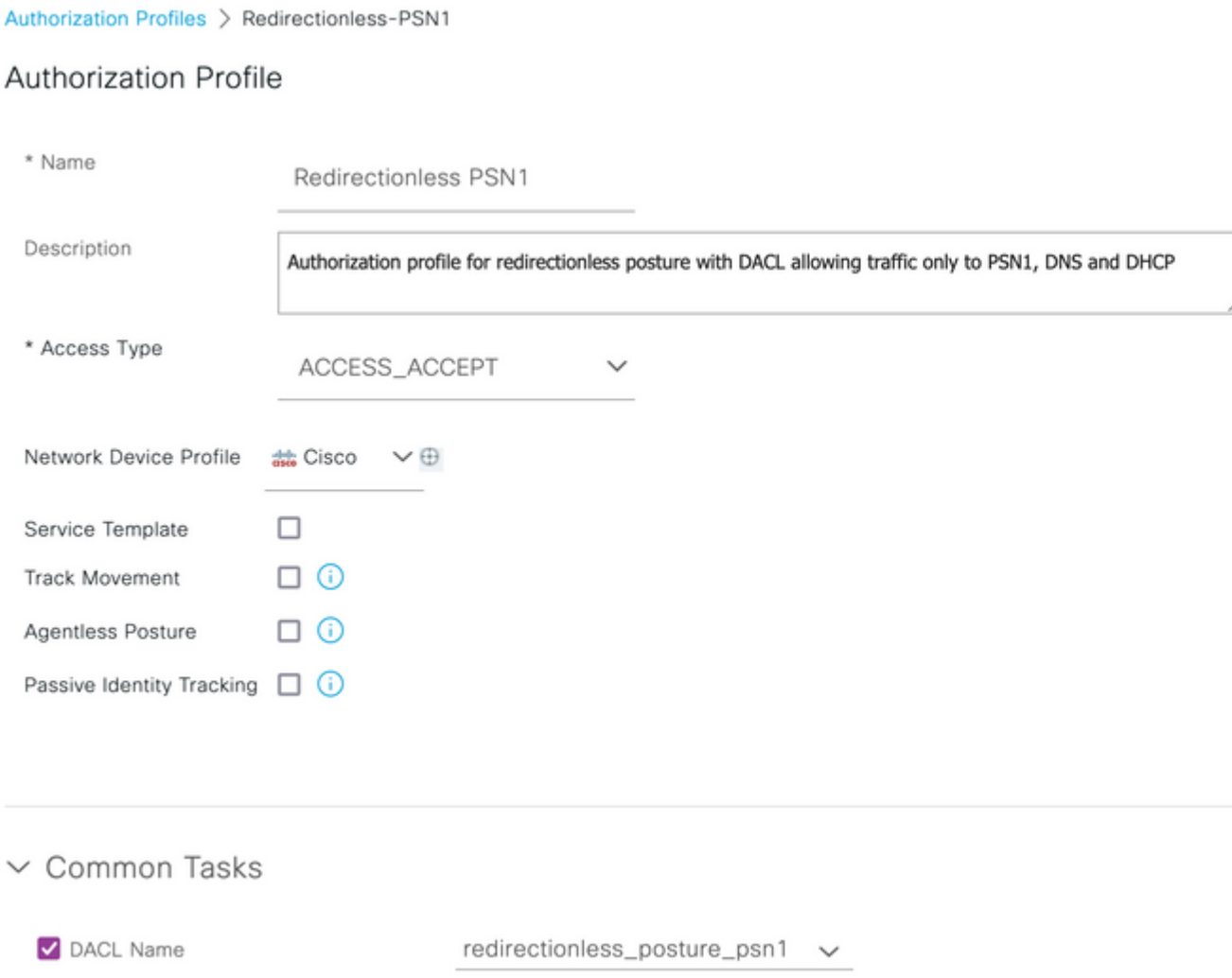
Si la performance du déploiement est affectée par une position sans redirection, cela indique souvent une implémentation inefficace. Il est recommandé de réviser les aspects suivants :

- Nombre de PSN utilisés par liste Call Home. Envisagez de réduire le nombre de PSN pouvant être utilisés pour chaque terminal ou périphérique réseau, conformément à la conception.
- Port du portail d'approvisionnement client dans la liste Call Home. Assurez-vous que le numéro de port du portail est inclus après l'adresse IP ou le nom de domaine complet de chaque noeud.

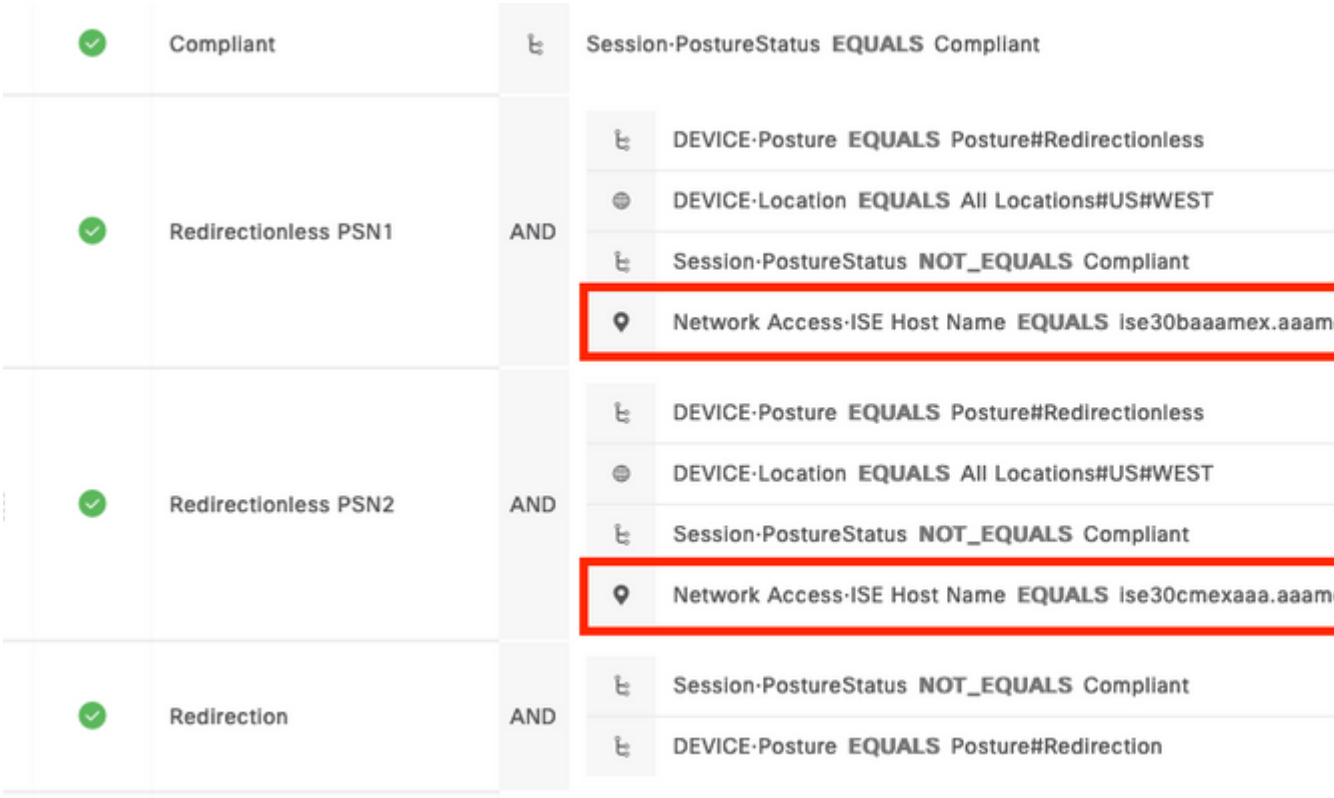
Pour atténuer l'impact :

1. Effacez le fichier connectiondata.xml des points de terminaison en supprimant le fichier du dossier Cisco Secure Client et redémarrez le service ISE Posture ou Cisco Secure Client. Si les services ne sont pas redémarrés, l'ancien fichier est régénéré et les modifications ne prennent pas effet. Cette action doit également être effectuée après la révision et la modification des listes Call Home.
2. Utilisez des DACL ou d'autres ACL pour bloquer le trafic vers les PSN ISE pour les connexions réseau lorsque cela n'est pas pertinent :

    - Pour les connexions où la position n'est pas appliquée dans les stratégies d'autorisation mais qui s'appliquent aux terminaux avec le module Cisco Secure Client ISE Posture installé, bloquez le trafic des clients vers tous les PSN ISE pour les ports TCP 8905 et le port Client Provisioning Portal. Cette action est également recommandée pour la posture avec mise en oeuvre de la redirection.
    - Pour les connexions où la position est appliquée dans les stratégies d'autorisation, autorisez le trafic des clients vers le PSN d'authentification et bloquez le trafic vers d'autres PSN dans le déploiement. Cette action peut être mise en oeuvre temporairement pendant la révision de la conception.



Profil d'autorisation avec DACL pour PSN unique



Politiques d'autorisation par PSN

Gestion de comptes

La comptabilité RADIUS est essentielle pour la gestion des sessions sur ISE. Étant donné que la position dépend de l'exécution d'une session active, une configuration incorrecte ou un manque de comptabilité peut également avoir un impact sur la découverte de position et les performances ISE. Il est important de vérifier que la gestion des comptes est correctement configurée sur le périphérique réseau pour envoyer des demandes d'authentification, le démarrage de la gestion des comptes, l'arrêt de la gestion des comptes et les mises à jour de la gestion des comptes à un seul PSN pour chaque session.

Pour vérifier les paquets de comptabilité reçus sur ISE, accédez à **Operations** > **Reports** > **Reports** > **Endpoints and Users** > RADIUS Accounting.

Informations connexes

- Assistance technique et téléchargements Cisco

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.