Configurez ISE 2.1 NAC Menace-central (TC-NAC) avec des services d'AMP et de posture

Contenu

Introduction

Ce document décrit comment configurer le NAC Menace-central avec la protection anticipée de malware (AMP) sur le Cisco Identity Services Engine (ISE) 2.1. Des niveaux d'importance de menace et les résultats d'estimation de vulnérabilité peuvent être utilisés pour contrôler dynamiquement le niveau d'accès d'un point final ou d'un utilisateur. Les services de posture sont également soient couverts comme partie de ce document.

> **Note**: Le but du document est de décrire l'intégration ISE 2.1 avec l'AMP, posent des services sont affichés car ils sont exigés quand nous provision l'AMP d'ISE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Engine de gestion d'identité de Cisco
- Protection anticipée de malware

Composants utilisés

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

- Version 2.1 d'engine de gestion d'identité de Cisco
- Contrôleur LAN Sans fil (WLC) 8.0.121.0
- AnyConnect VPN Client 4.2.02075
- Service Pack 1 de Windows 7

Configurer

Diagramme du réseau

Écoulement détaillé

1. Le client se connecte au réseau, l'**AMP_Profile** est assigné et l'utilisateur est réorienté au portail de ravitaillement d'Anyconnect. Si Anyconnect n'est pas détecté sur l'ordinateur, tous les modules configurés (VPN, AMP, posture) sont installés. La configuration est poussée chaque module avec ce profil

2. Une fois qu'Anyconnect est installé, l'estimation de posture fonctionne

3. Le module d'Enabler d'AMP installe le connecteur de FireAMP

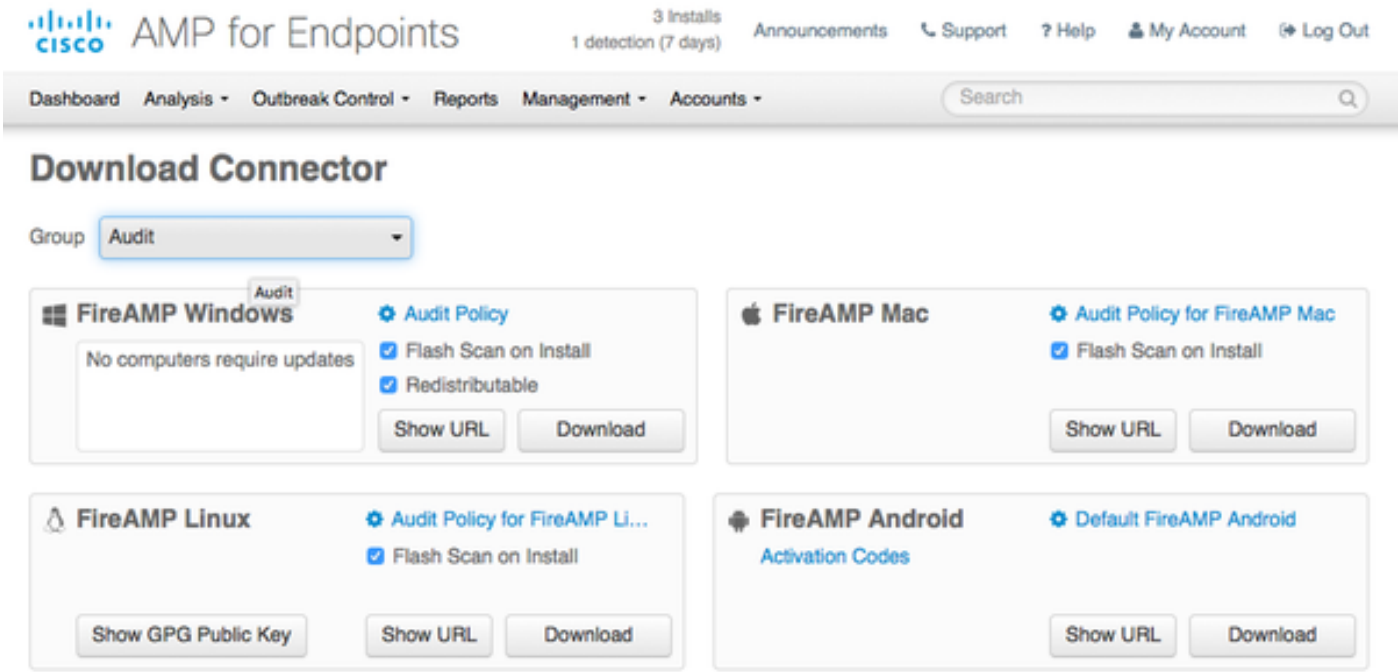
4. Quand les essais de client pour télécharger le logiciel malveillant, connecteur d'AMP jette un message d'avertissement et le signale au nuage d'AMP

5. Le nuage d'AMP envoie ces informations à ISE

Configurez le nuage d'AMP

Étape 1. Connecteur de téléchargement de nuage d'AMP

Afin de télécharger le connecteur, naviguez vers le connecteur de Gestion > de téléchargement. Puis type de sélection et **téléchargement** FireAMP (Windows, Android, MAC, Linux). Dans ce cas l'**audit** a été sélectionné et le fichier d'installation de FireAMP pour Windows.

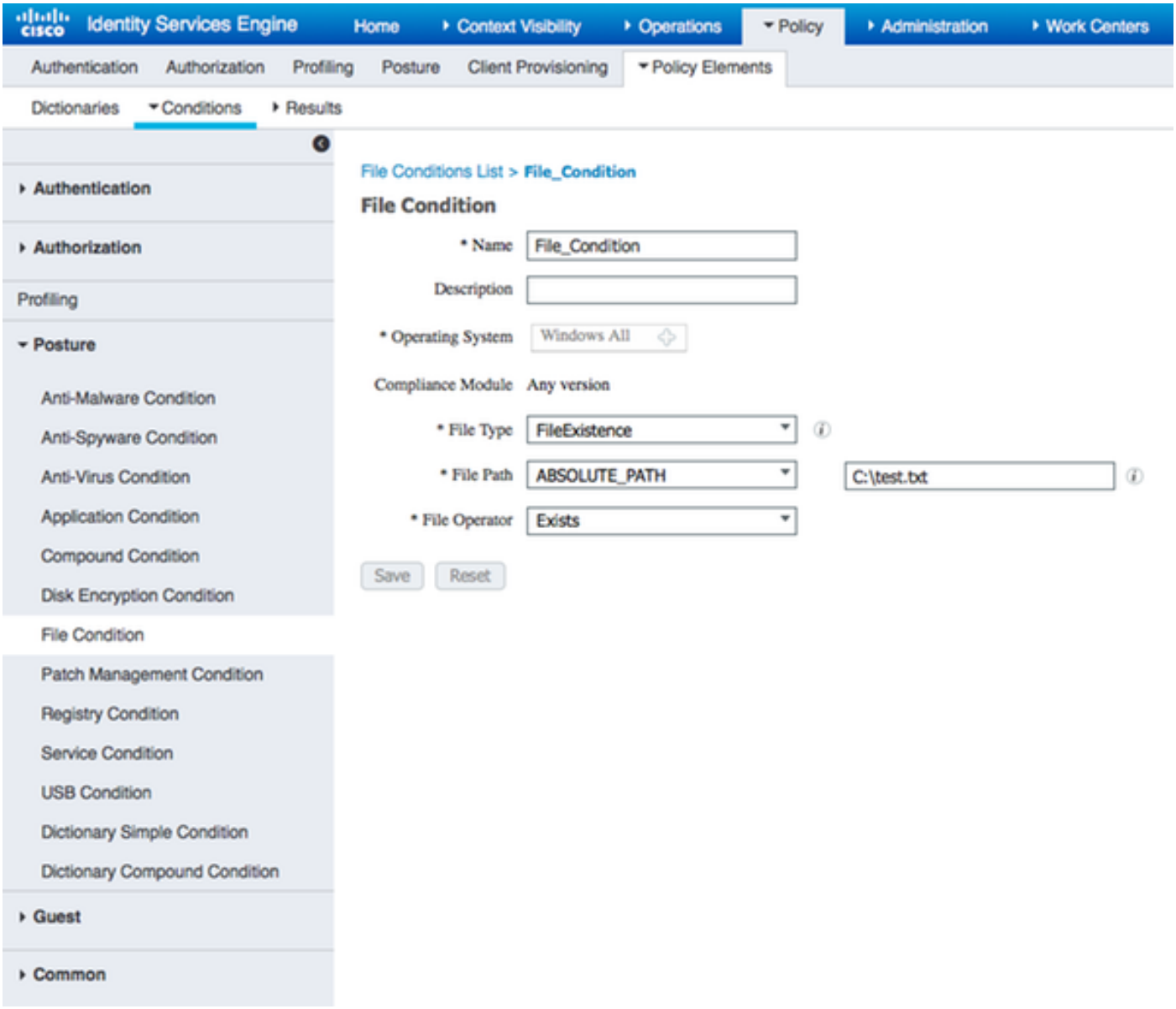


> **Note**: Télécharger ce fichier génère un fichier .exe appelé l'**Audit_FireAMPSetup.exe dans l'**exemple. Ce fichier a été envoyé au web server pour être disponible une fois que l'utilisateur demande la configuration de l'AMP.

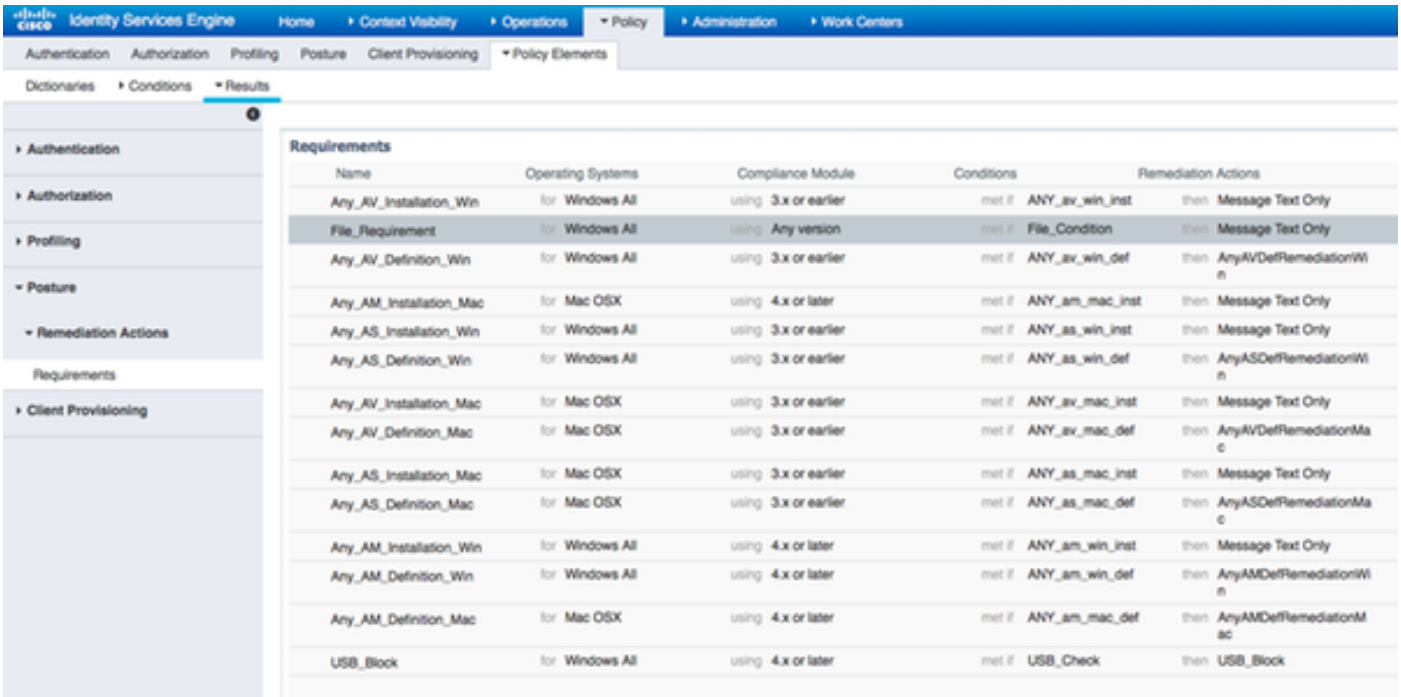
Configurez ISE

Étape 1. Configurez les stratégies et les états de posture

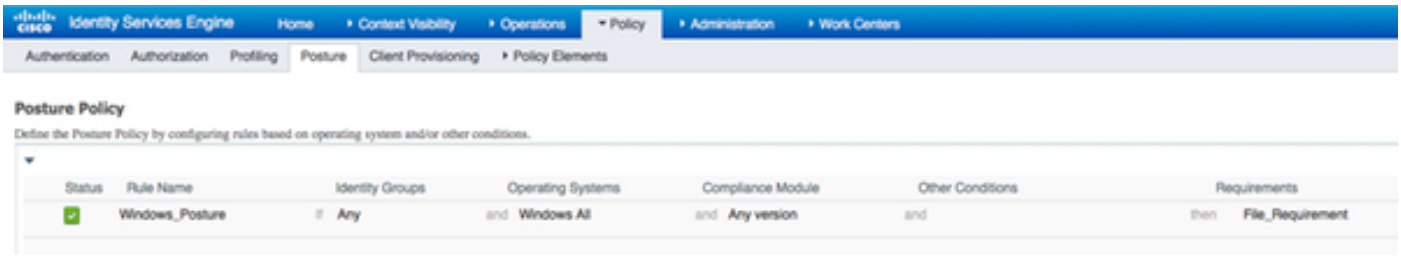
Naviguez vers la stratégie > les éléments > les états > la posture > le fichier Condition.You de stratégie peut voir qu'un état simple pour l'existence de fichier a été créé. Le fichier doit exister si le point final est d'être conforme avec la stratégie vérifiée par le module de posture :



Cette condition est utilisée pour une condition requise :

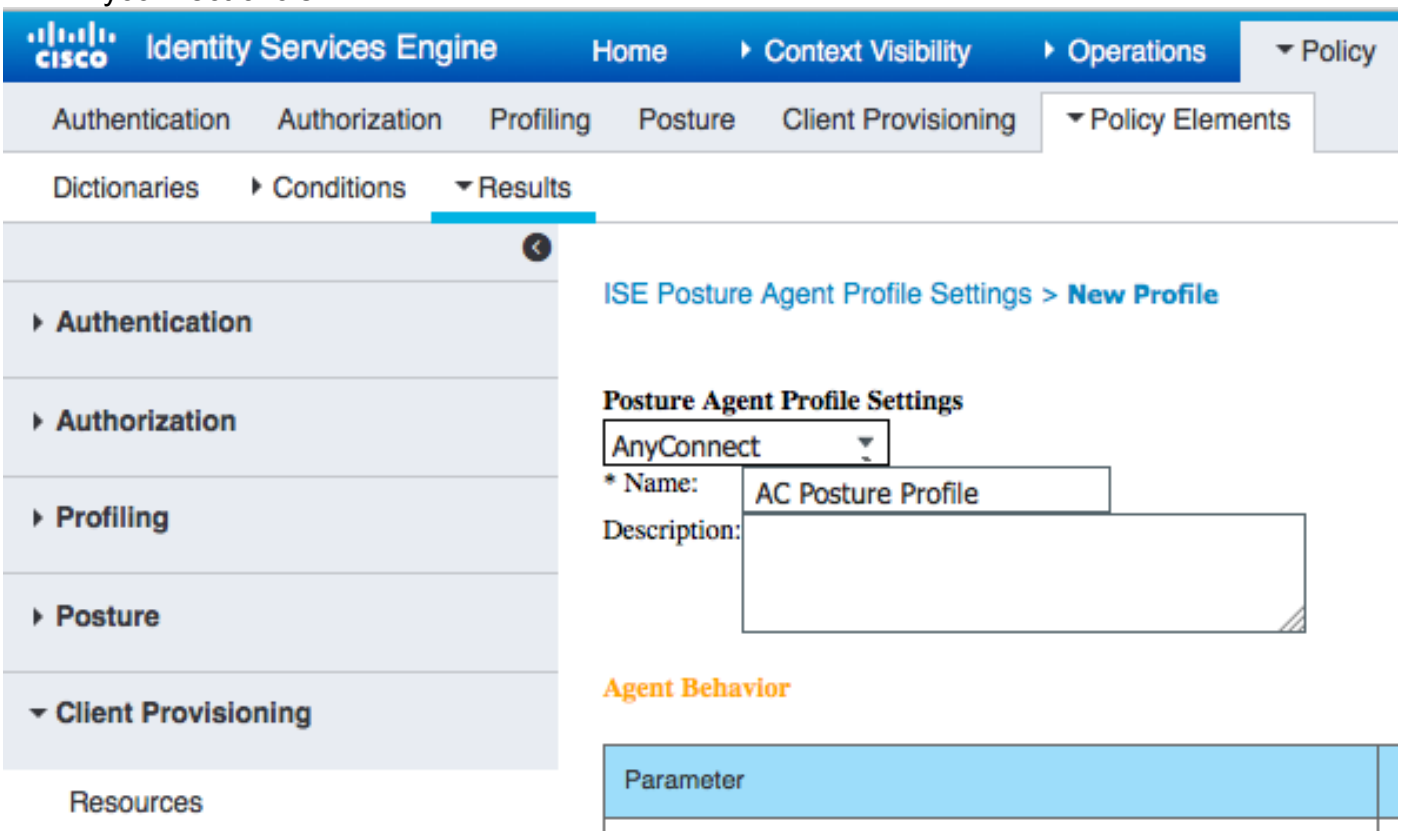


La condition requise est utilisée dans la stratégie de posture pour des systèmes de Microsoft Windows :

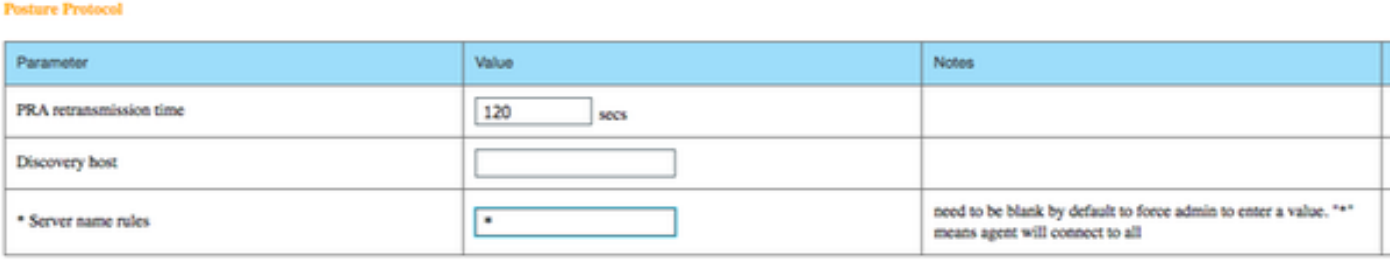


Étape 2. Configurez le profil de posture

- Naviguez vers la stratégie > les éléments de stratégie > les résultats > le ravitaillement > les ressources de client et ajoutez le profil de posture d'agent de Contrôle d'admission au réseau (NAC) ou d'agent d'AnyConnect
- Anyconnect choisi

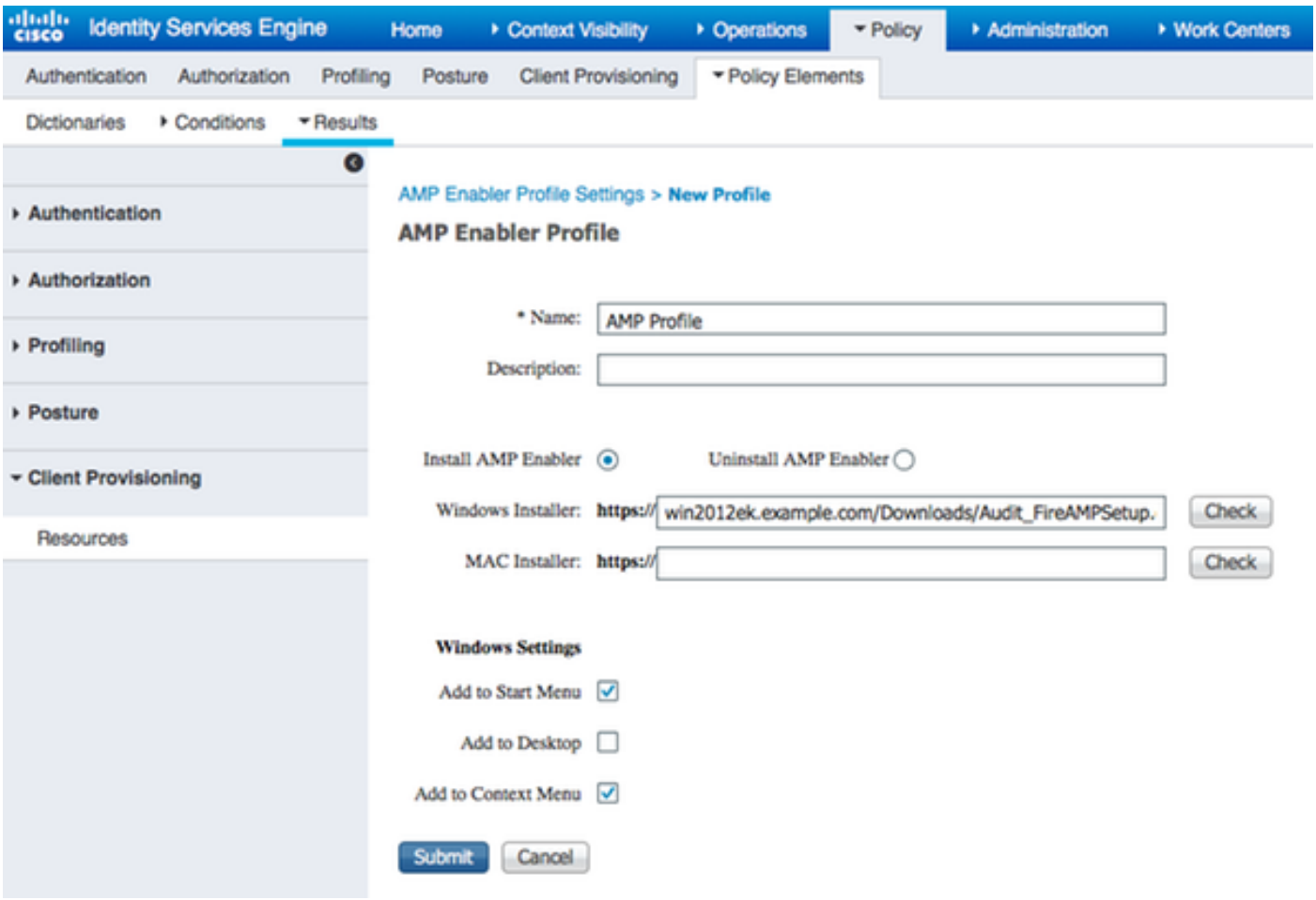


- De la section Protocole de posture ajoutez * afin de permettre à l'agent pour se connecter à tous les serveurs



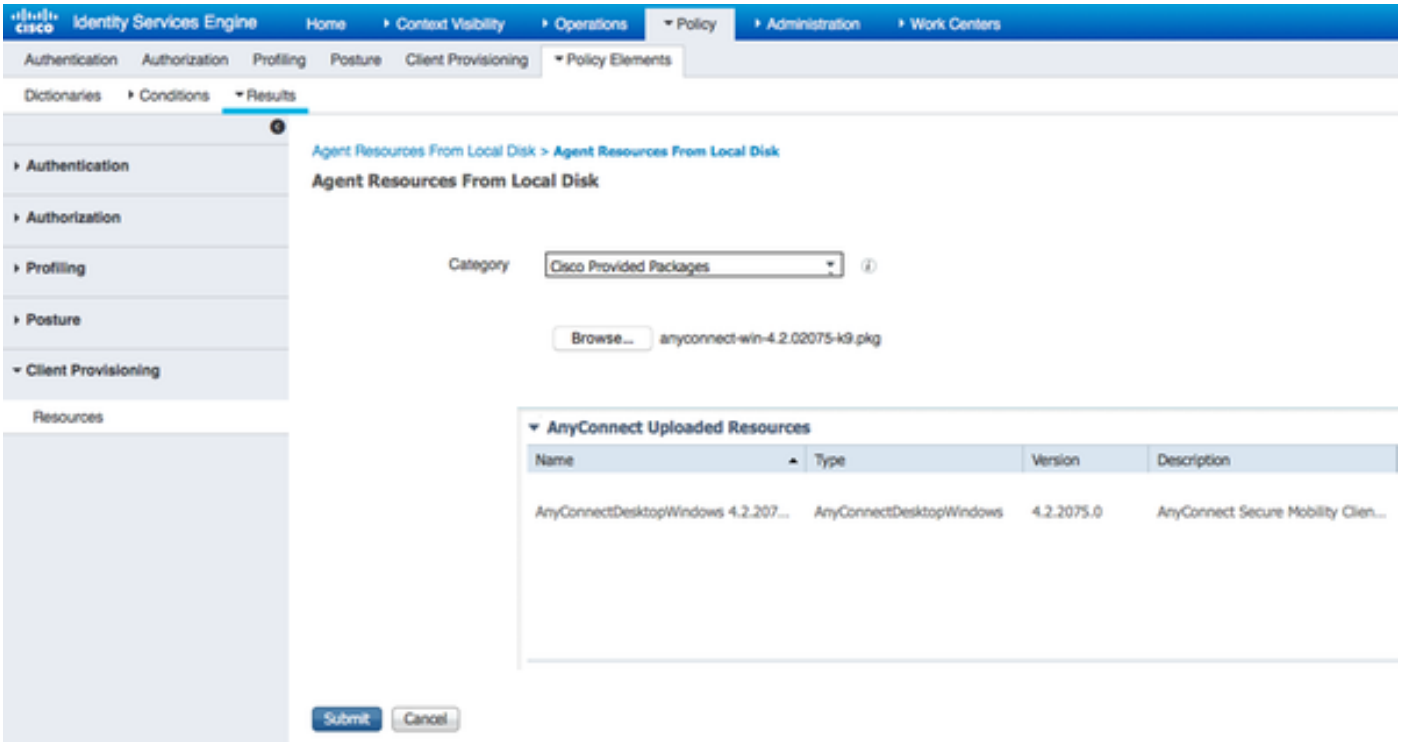
Étape 3. Configurez le profil d'AMP

Le profil d'AMP contient les informations où l'installer windows se trouve. L'installer windows a été téléchargé plus tôt du nuage d'AMP. Il devrait être accessible de la machine cliente. Le certificat du serveur HTTPS, où l'installateur se trouve devrait sont de confiance par la machine cliente aussi bien.

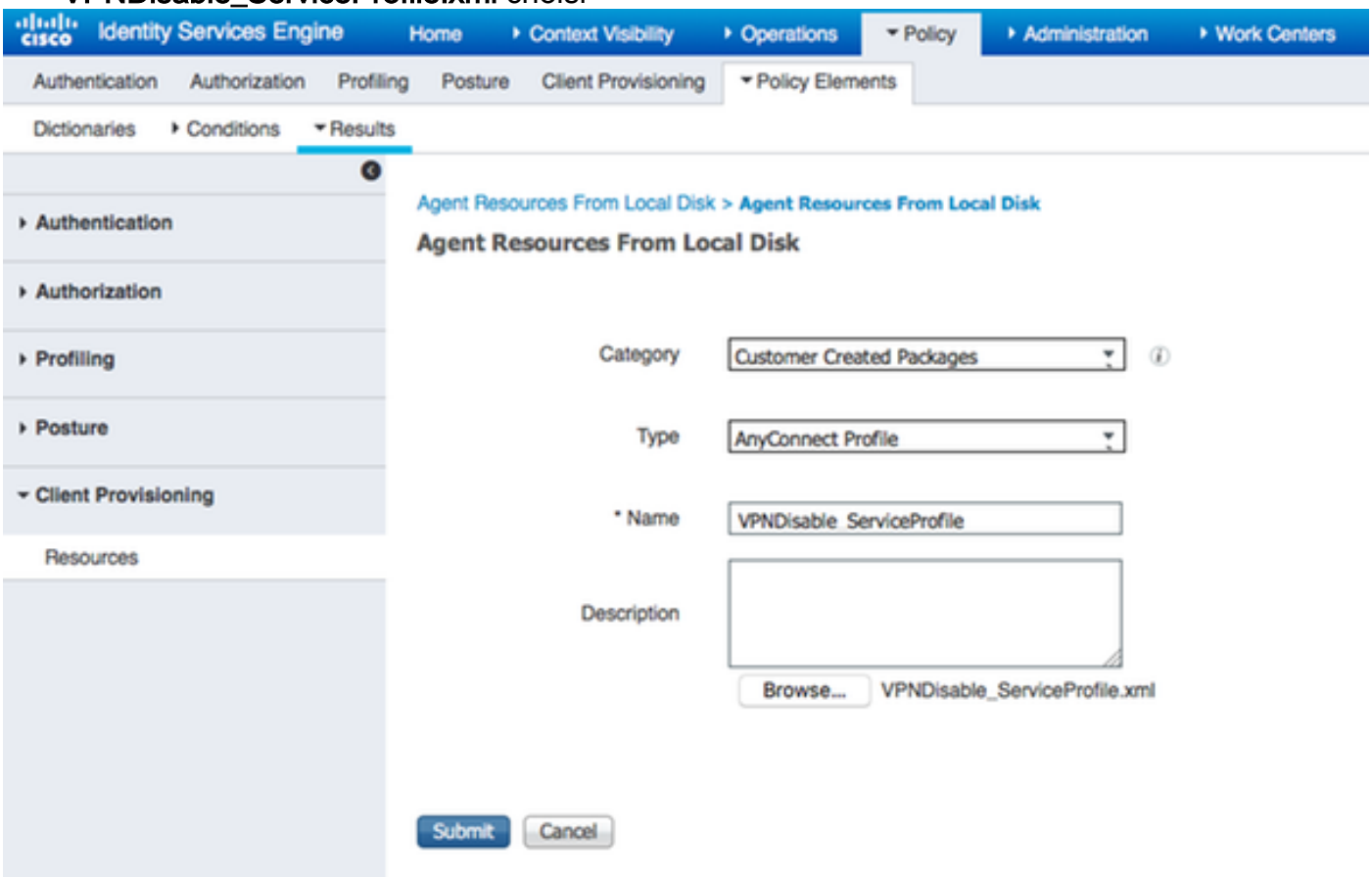


Étape 2. Applications de téléchargement et profil XML à ISE

- Téléchargez l'application manuellement du site de Cisco de fonctionnaire : **anyconnect-win-4.2.02075-k9.pkg**
- Sur ISE, naviguez vers la stratégie > les éléments de stratégie > les résultats > le ravitaillement > les ressources de client, et ajoutez les **ressources en agent à partir du disque local**
- Choisissez **Cisco a fourni des modules** et **anyconnect-win-4.2.02075-k9.pkg** choisi



- Naviguez vers la stratégie > les éléments de stratégie > les résultats > le ravitaillement > les ressources de client et ajoutez les **ressources en agent à partir du disque local**
- Choisissez les **modules** et le **profil d'AnyConnect créés par client de** type. **VPNDisable_ServiceProfile.xml** choisi



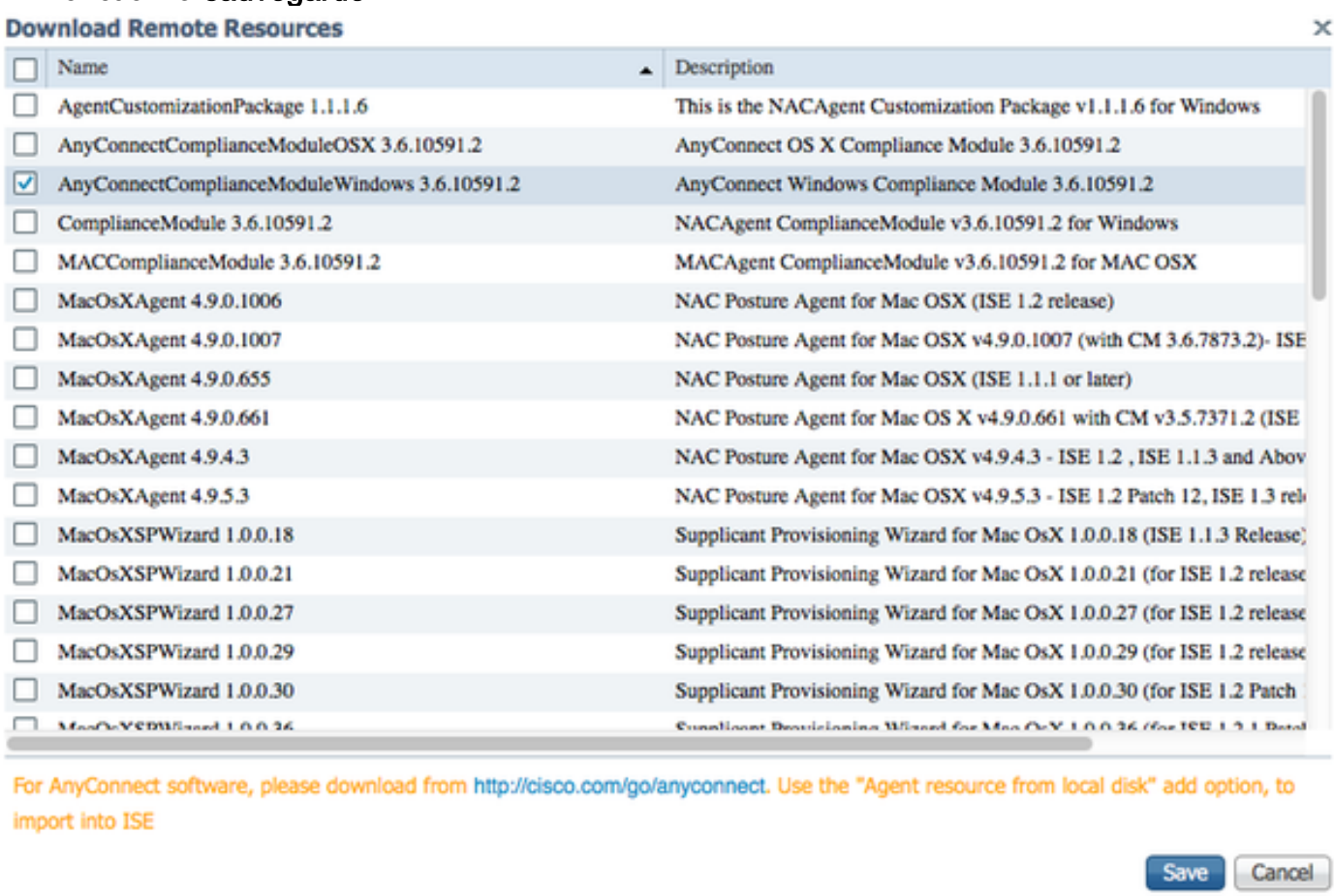
Note: **VPNDisable_ServiceProfile.xml** est utilisé pour masquer le titre VPN, puisque cet exemple n'utilise pas le module VPN. C'est le contenu de VPNDisable_ServiceProfile.xml **:**

xmlns <AnyConnectProfile de " http://schemas.xmlsoap.org/encoding/ » de xmlns= : xsi du

```
xsi= " http://www.w3.org/2001/XMLSchema-instance" : schemaLocation= "
http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd " >
 <ClientInitialization>
 <ServiceDisable>true</ServiceDisable>
 </ClientInitialization>
</AnyConnectProfile>
```

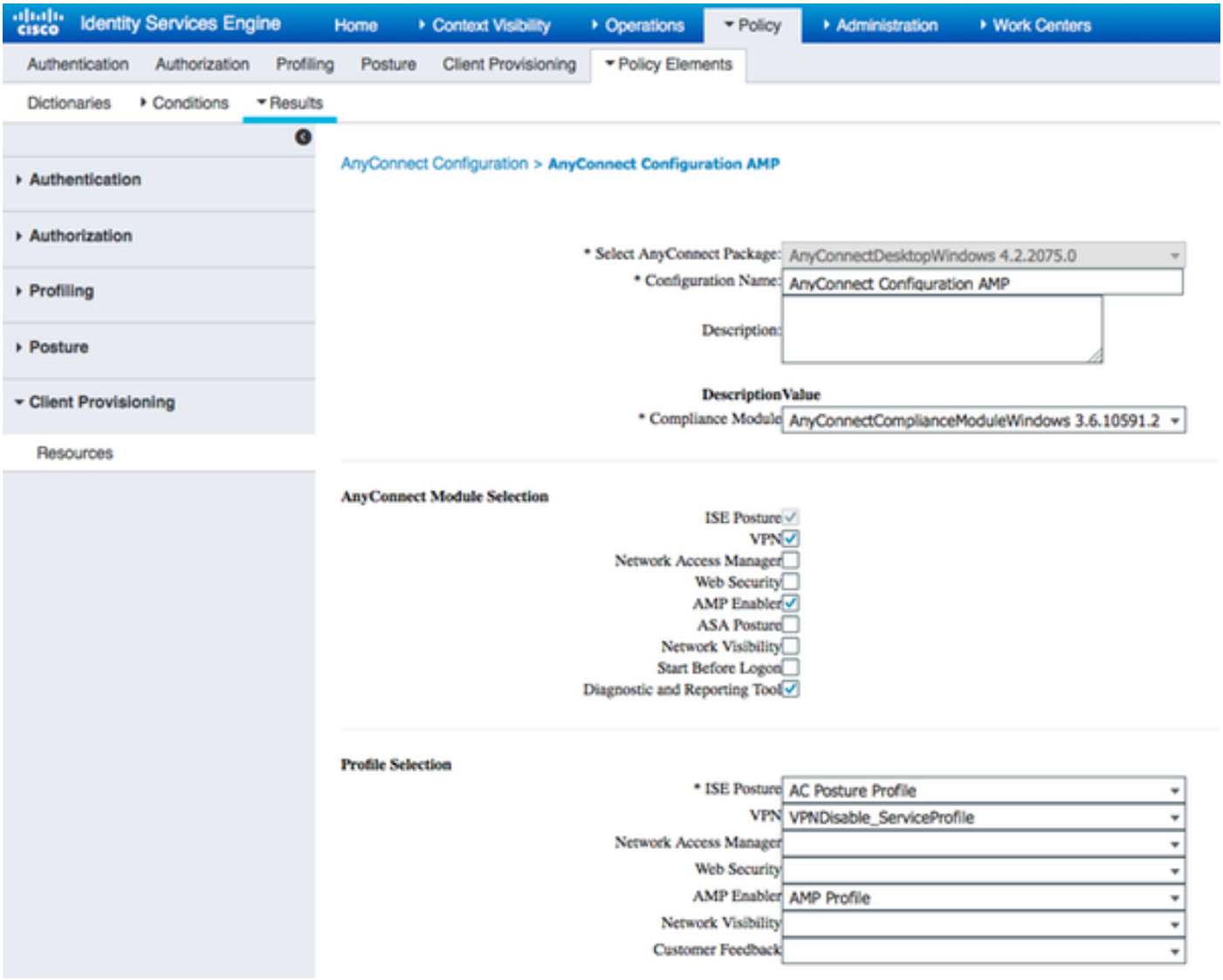
Étape 3. Module de conformité d'AnyConnect de téléchargement

- Naviguez vers la stratégie > les éléments de stratégie > les résultats > le ravitaillement > les ressources de client et ajoutez les **ressources en agent du site de Cisco**
- **Le module** choisi **3.6.10591.2 de conformité d'AnyConnect Windows** et cliquent sur en fonction la **sauvegarde**



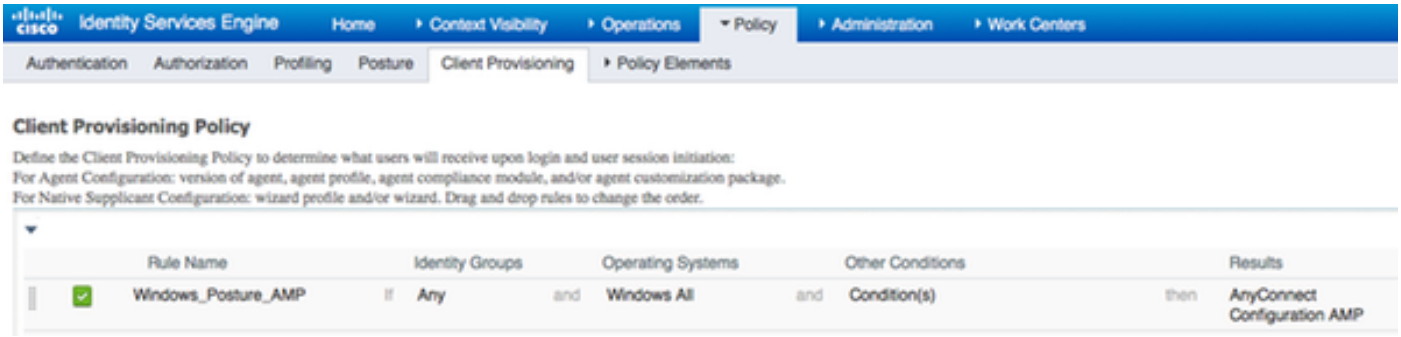
Étape 4. Ajoutez la configuration d'AnyConnect

- Naviguez vers la stratégie > les éléments de stratégie > les résultats > le ravitaillement > les ressources de client, et ajoutez la **configuration d'AnyConnect**
- Configurez le nom et sélectionnez le module de conformité et tous modules requis d'AnyConnect (VPN, AMP, et posture)
- Dans la **sélection de profil**, choisissez le profil configuré plus tôt pour chaque module



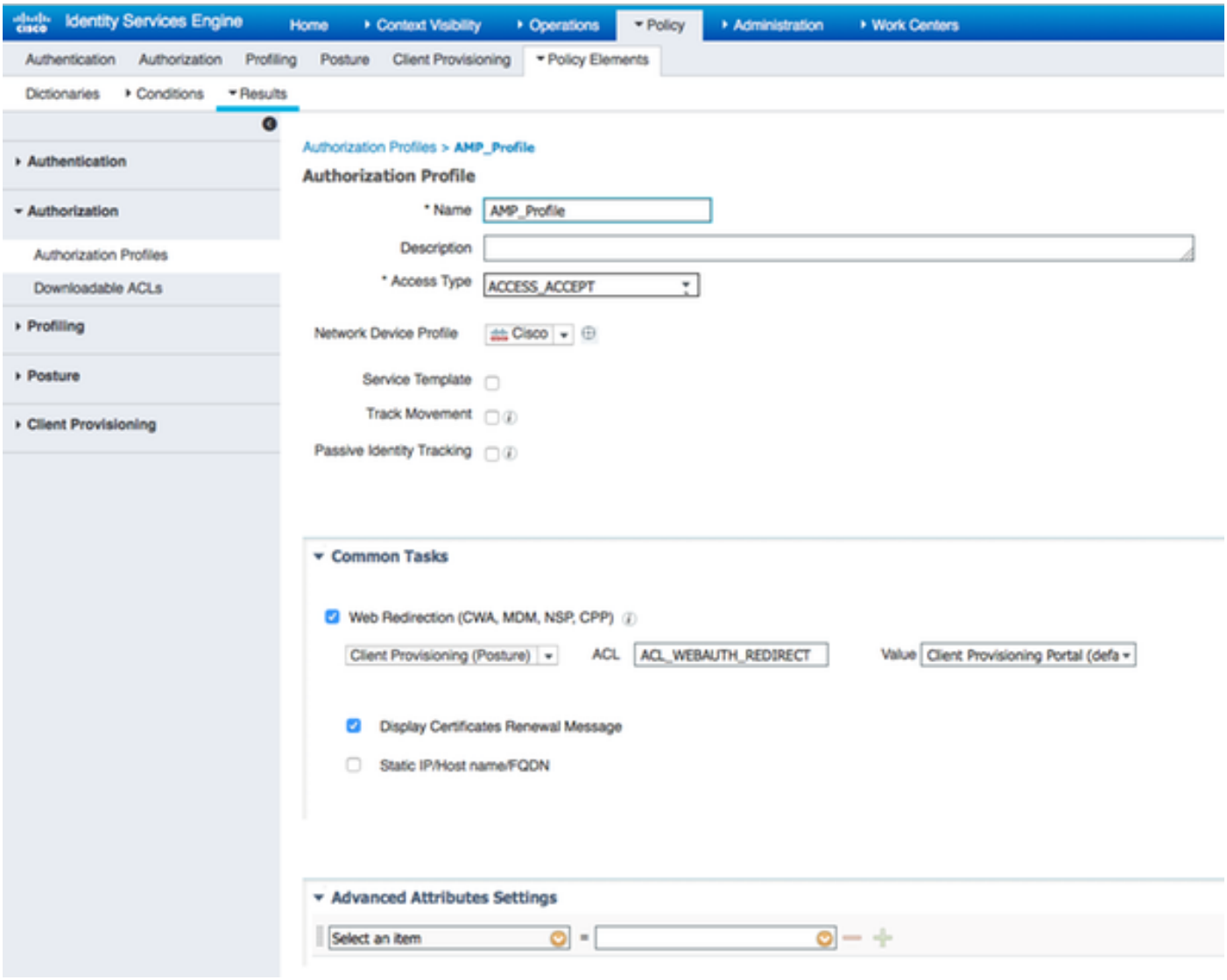
Étape 5. Configurez les règles de ravitaillement de client

La configuration d'AnyConnect créée plus tôt est mise en référence dans les règles de **ravitaillement de client**

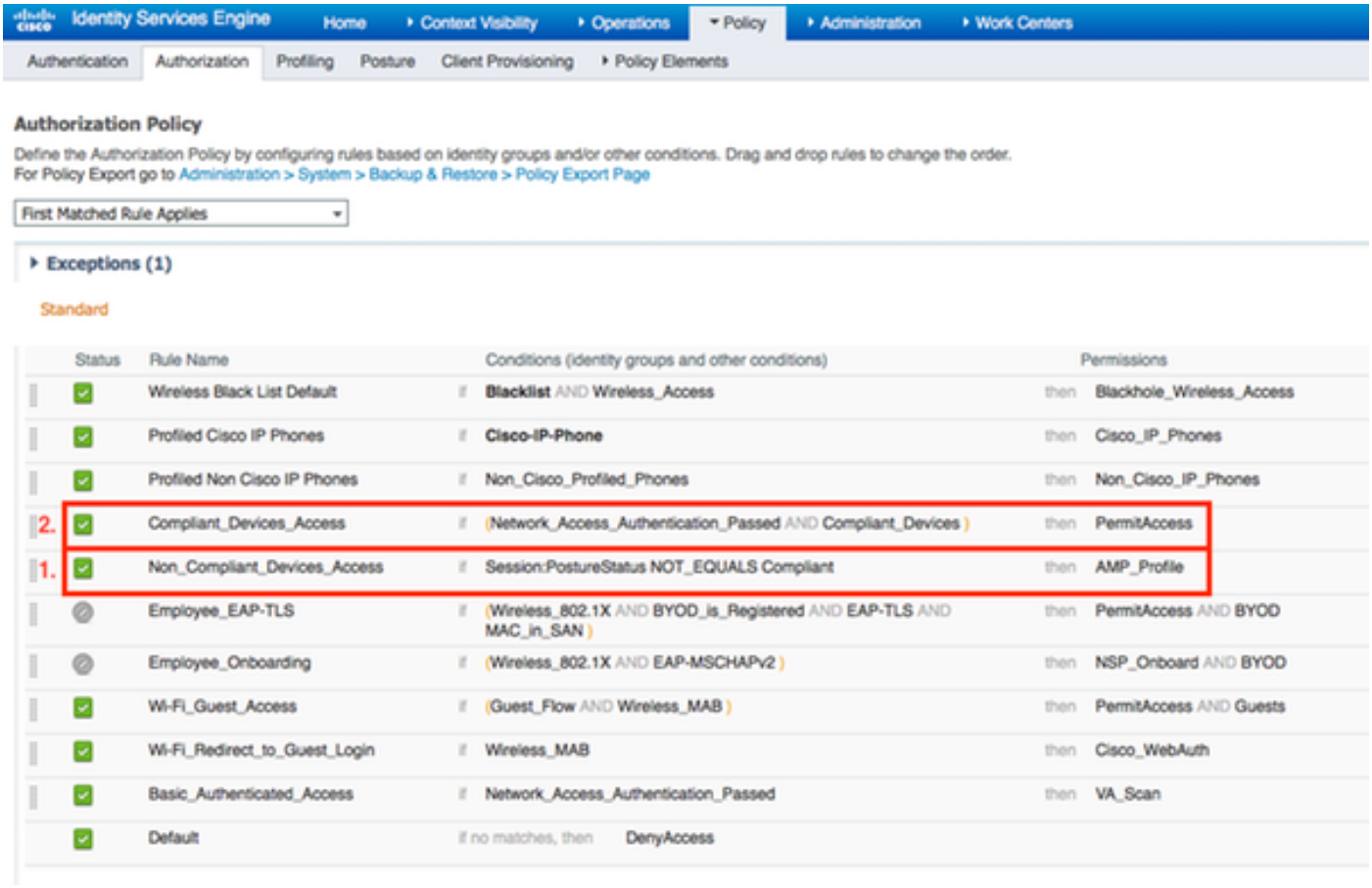


Étape 6. Configurez les stratégies d'autorisation

D'abord la redirection au portail de ravitaillement de client a lieu. Des stratégies standard d'autorisation pour la posture sont utilisées.

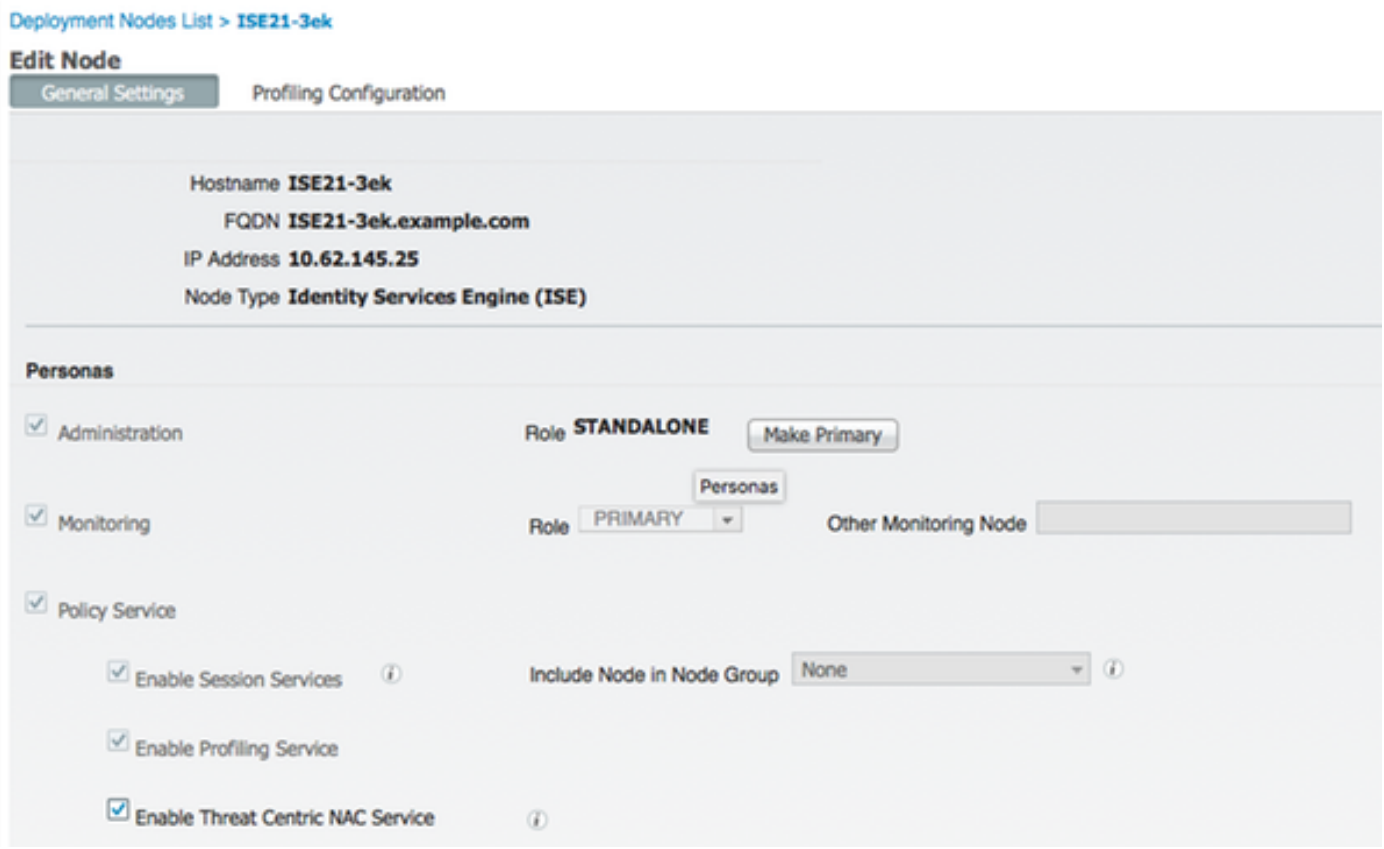


Après, une fois que conforme, l'accès complet est assigné



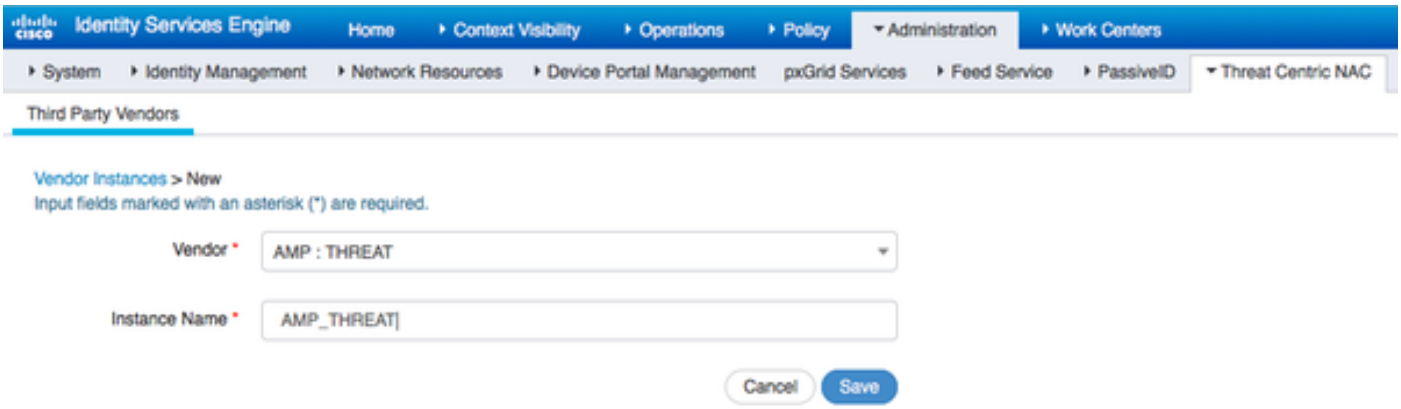
Étape 7. Services de l'enable TC-NAC

Les services de l'enable TC-NAC sous la gestion > le déploiement > éditent le noeud. Case à cocher **centrale de service de la menace NAC d'enable de** contrôle.

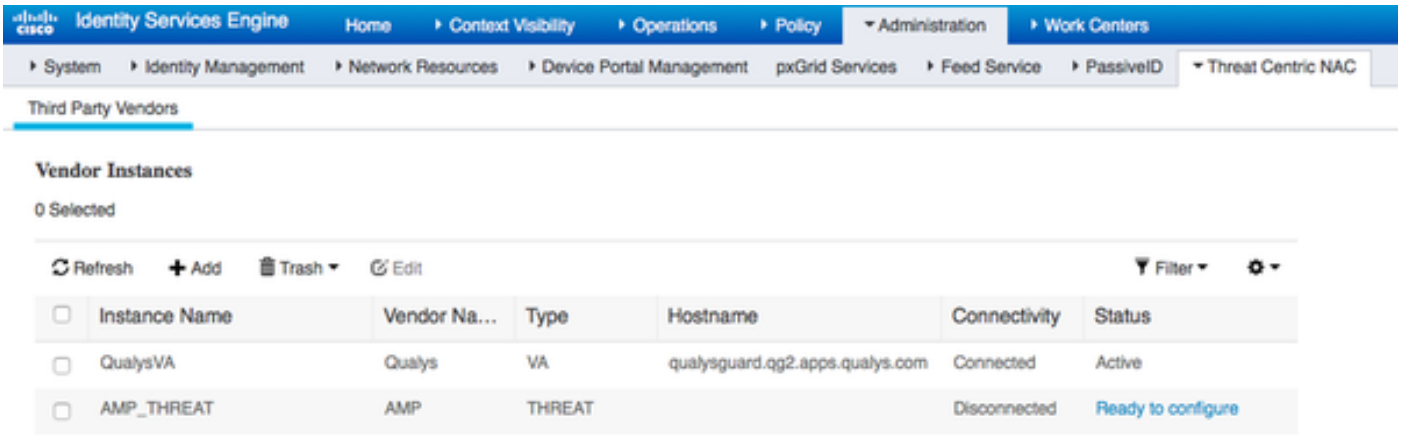


Étape 8. Configurez l'adaptateur d'AMP

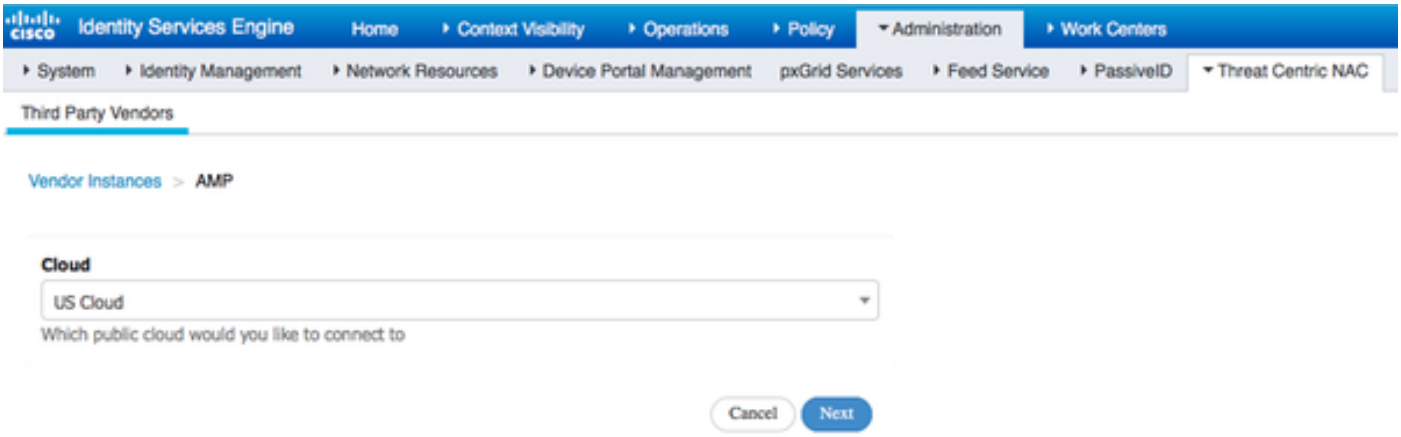
Naviguez vers la gestion > la menace centrales NAC > constructeurs tiers > ajoutent. Cliquez sur en fonction la **sauvegarde**



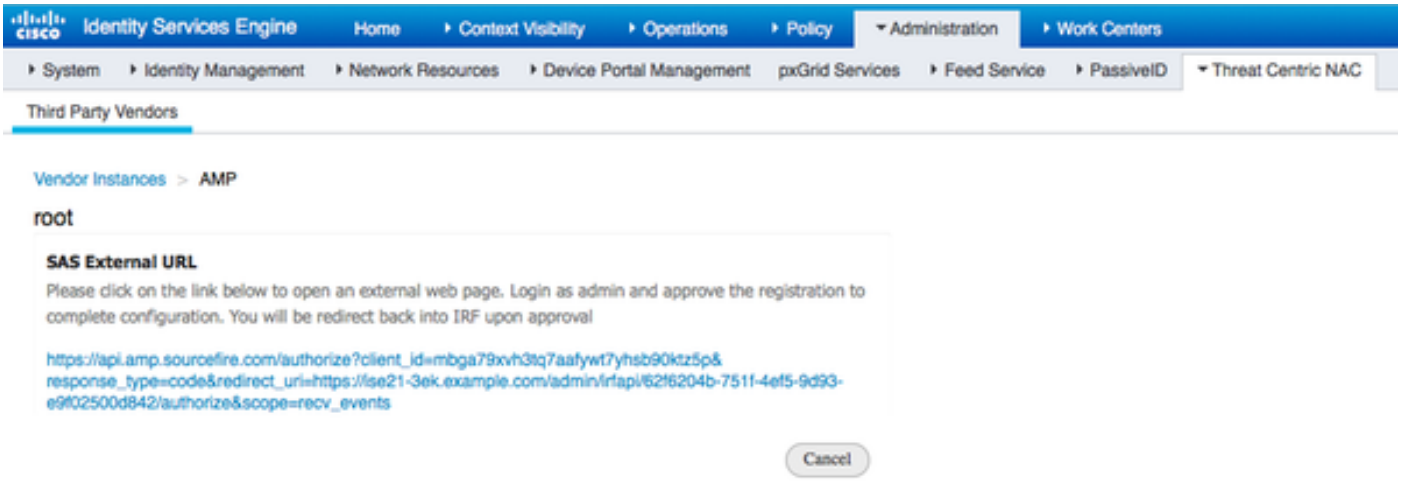
Il devrait transition **préparer pour configurer l'**état. Cliquez sur en fonction **prêt à configurer**



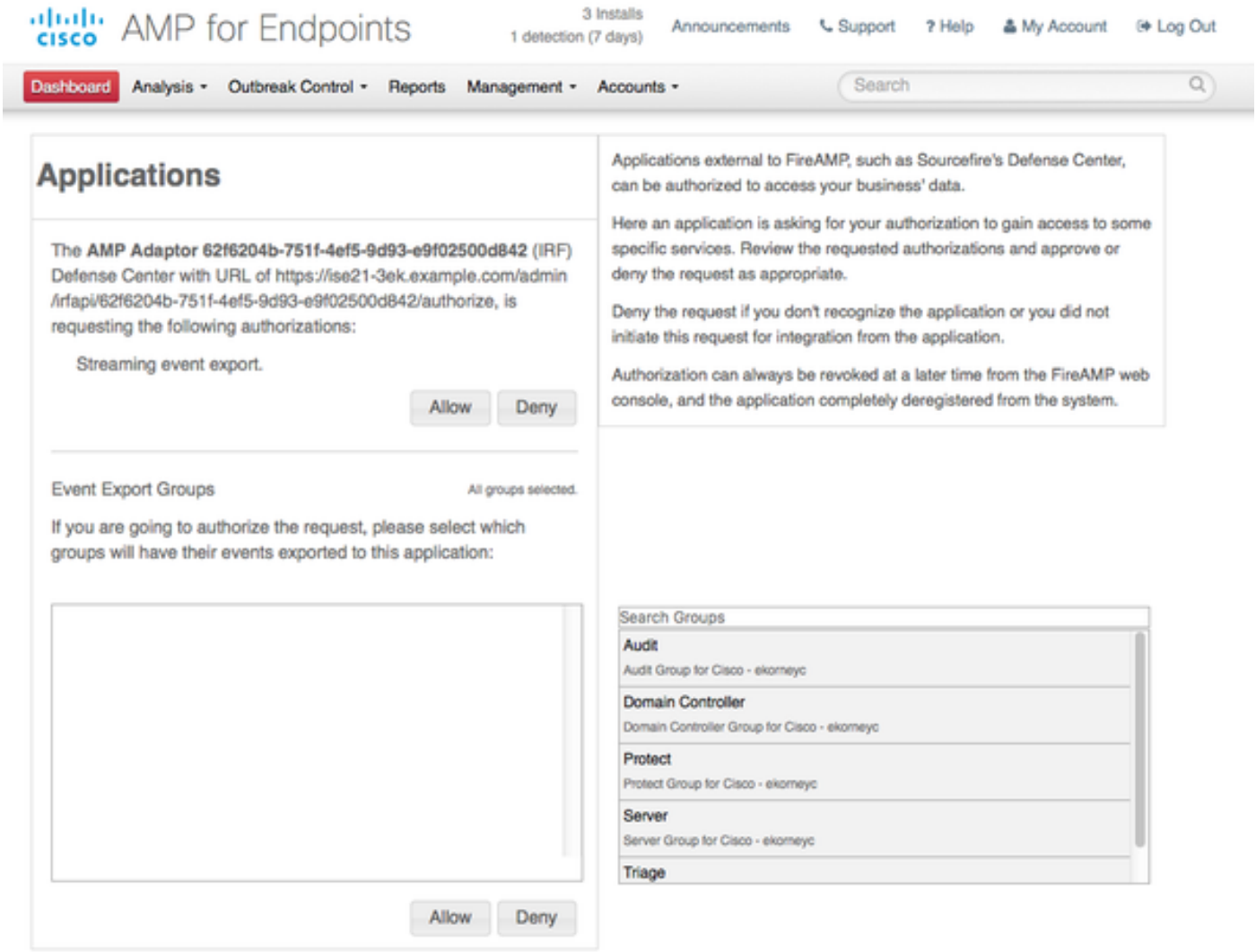
Sélectionnez le **nuage** et cliquez sur en fonction **ensuite**



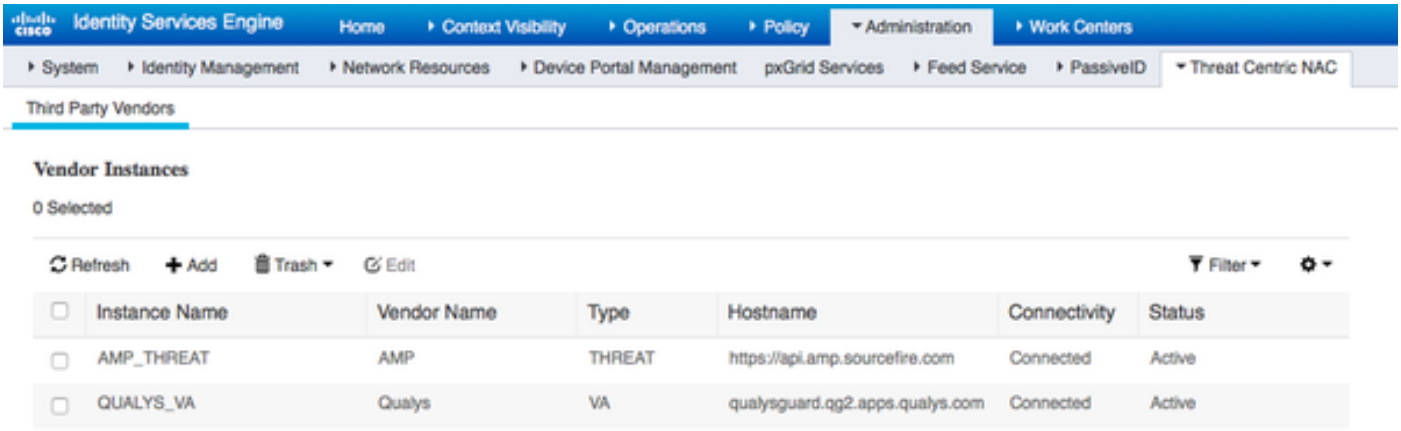
Cliquez sur le lien et la procédure de connexion de FireAMP comme admin dans FireAMP.



Le clic **autorisent** dans le panneau d'**applications** à autoriser la demande coulante d'exportation d'événement. Ensuite cette action, vous êtes réorienté de nouveau à Cisco ISE



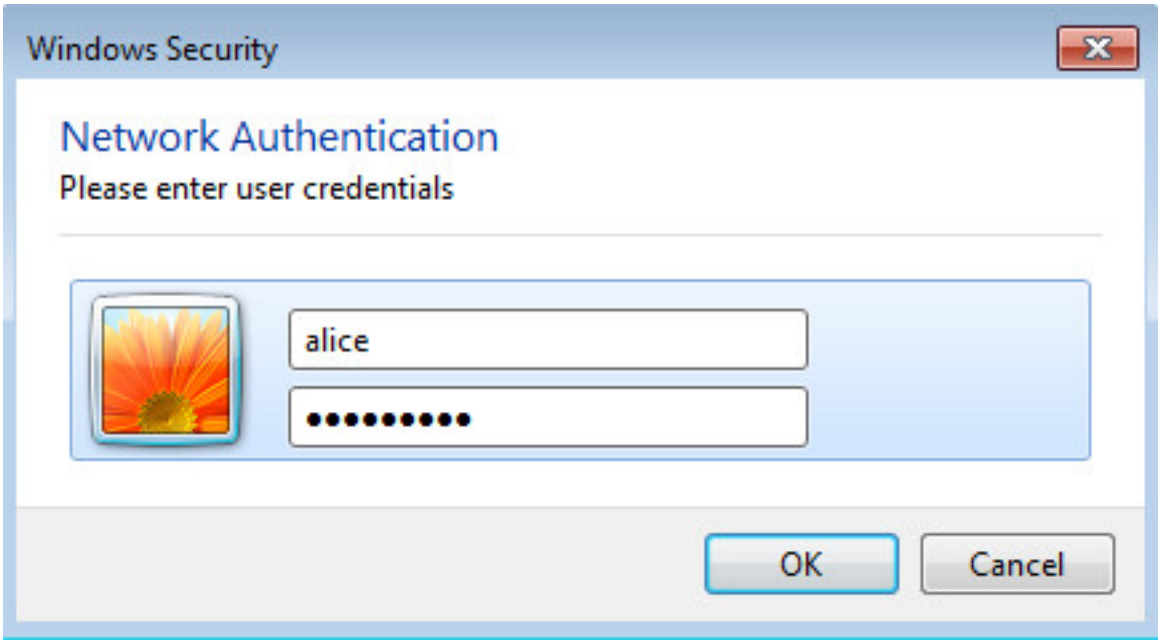
Sélectionnez les événements (par exemple, téléchargement méfiant, connexion au domaine méfiant, malware exécuté, compromission de Javas) ces vous voudrait surveiller. Le résumé de la configuration d'exemple d'adaptateur est affiché dans la page récapitulative de configuration. Transitions d'exemple d'adaptateur vers connecté/état active.



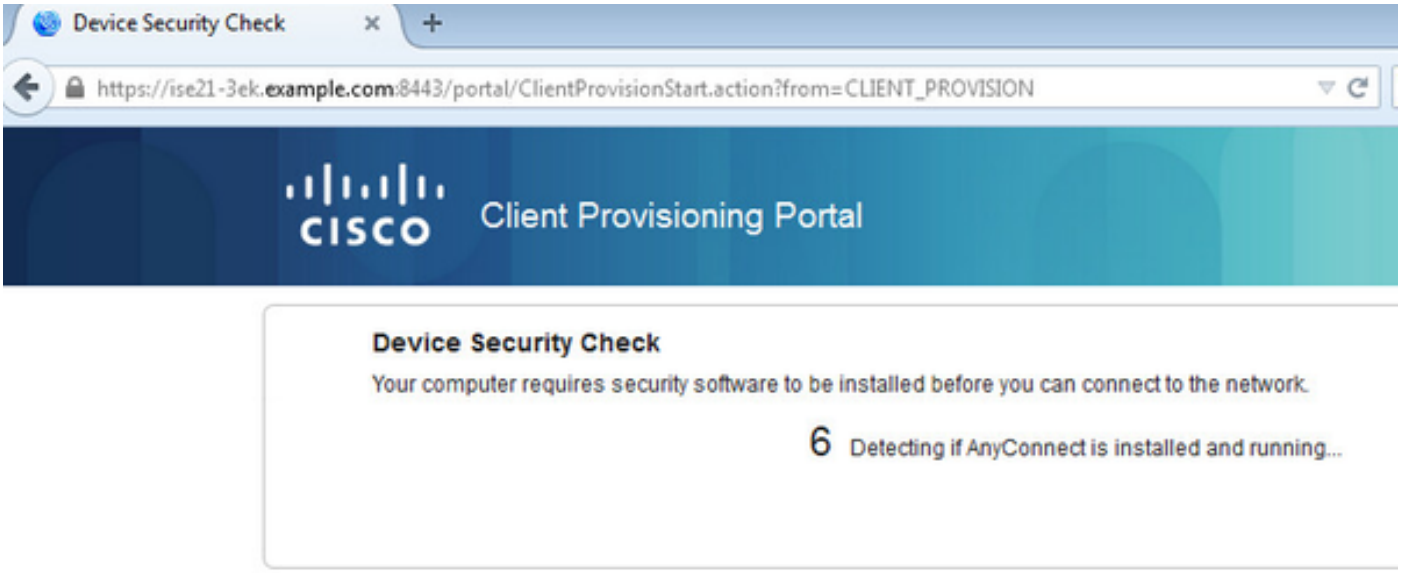
Vérifiez

Point final

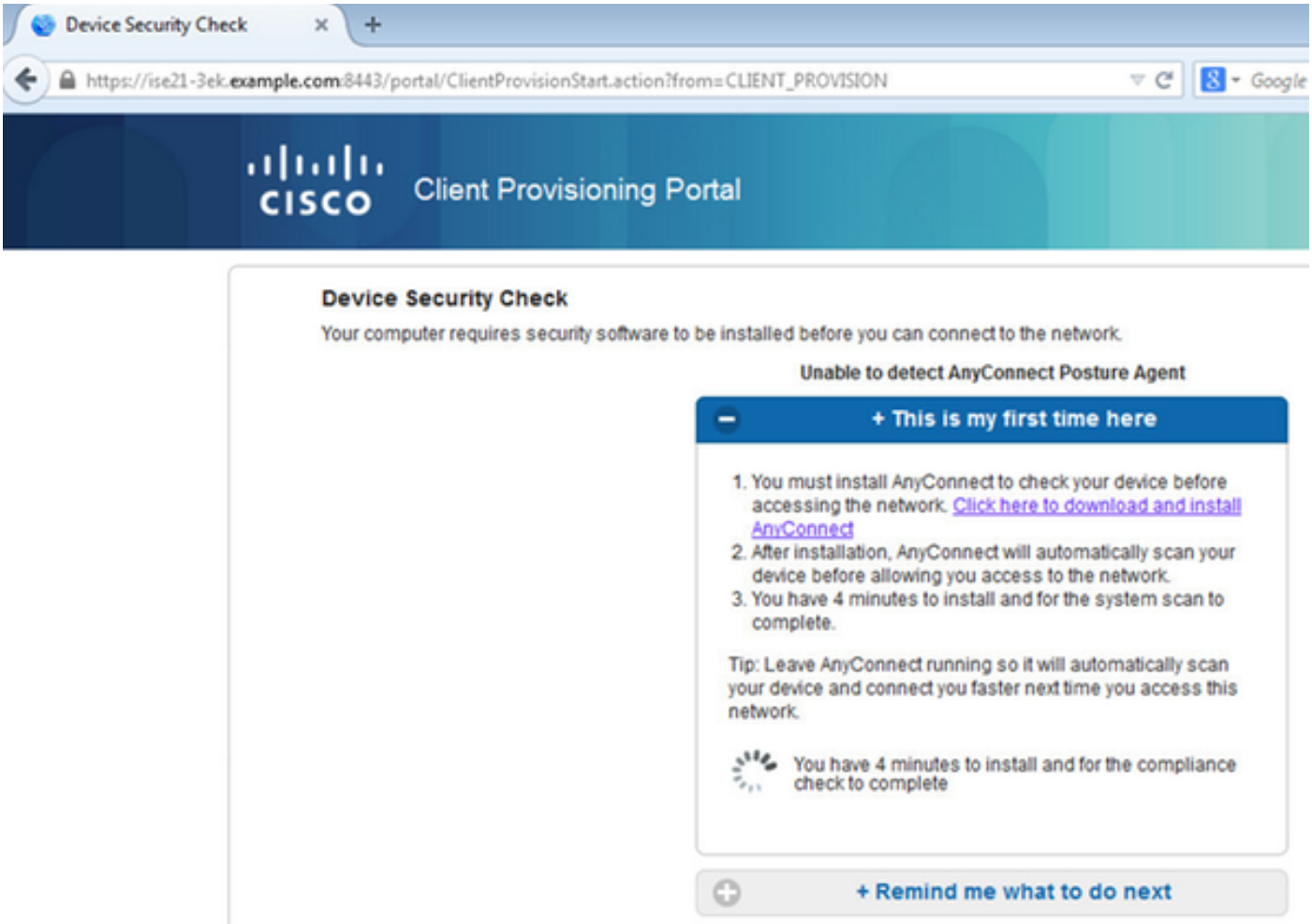
Connectez au réseau Sans fil par l'intermédiaire de PEAP (MSCHAPv2).



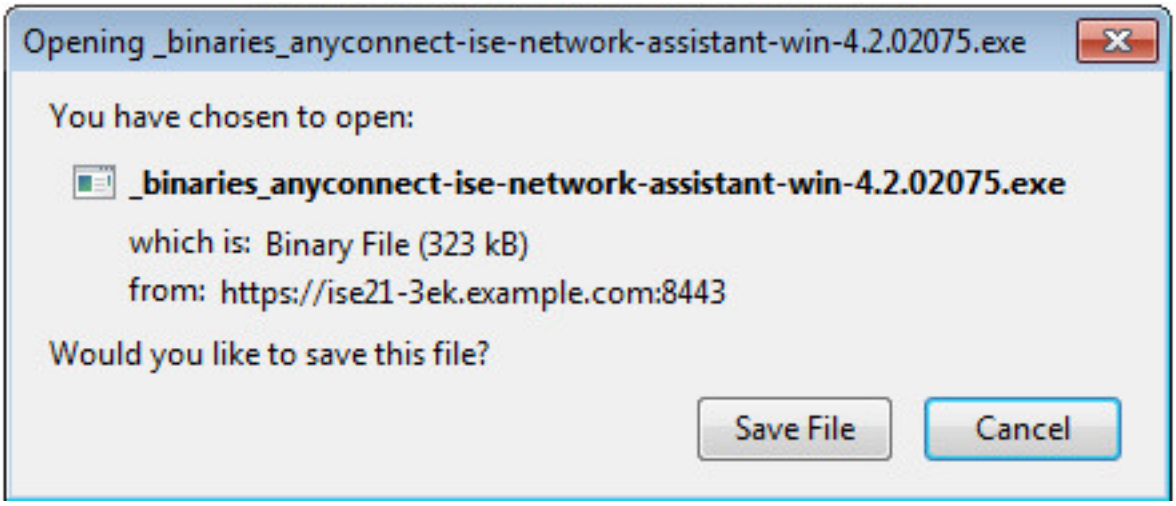
Une fois que connecté la redirection au portail de ravitaillement de client a lieu.



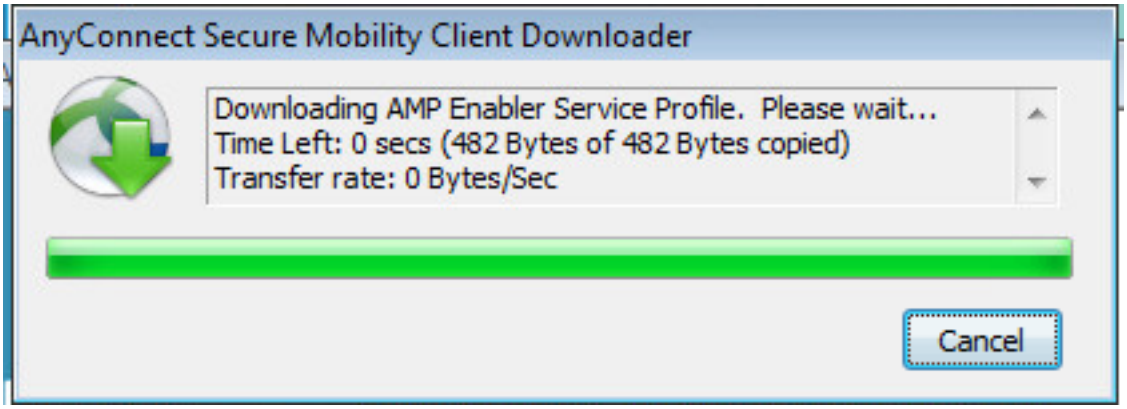
Puisqu'il n'y a rien installé sur la machine cliente, ISE incite pour l'installation de client d'AnyConnect.

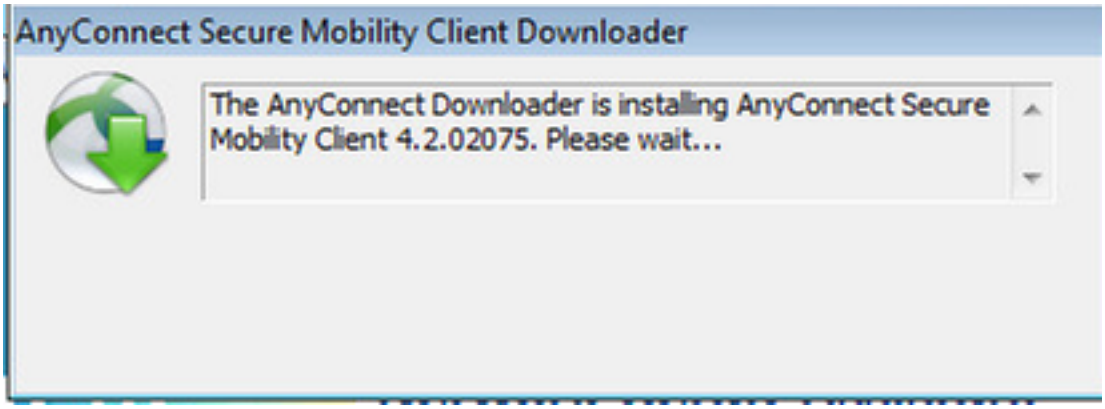


L'application auxiliaire de configuration réseau (NSA) devrait être téléchargée et passage de machine cliente.

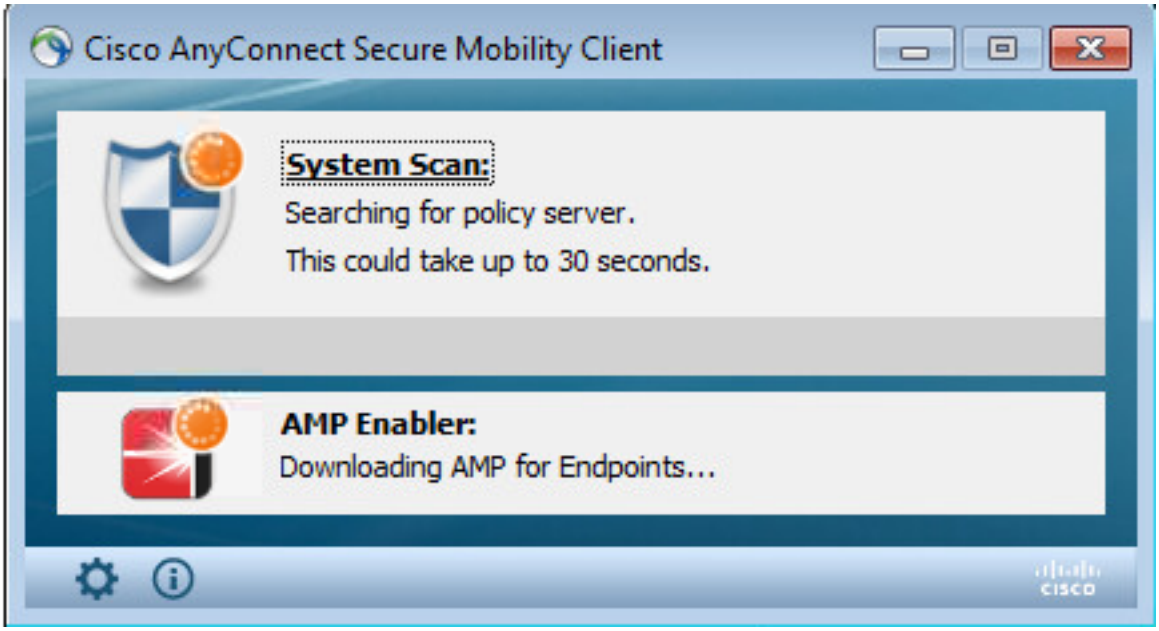


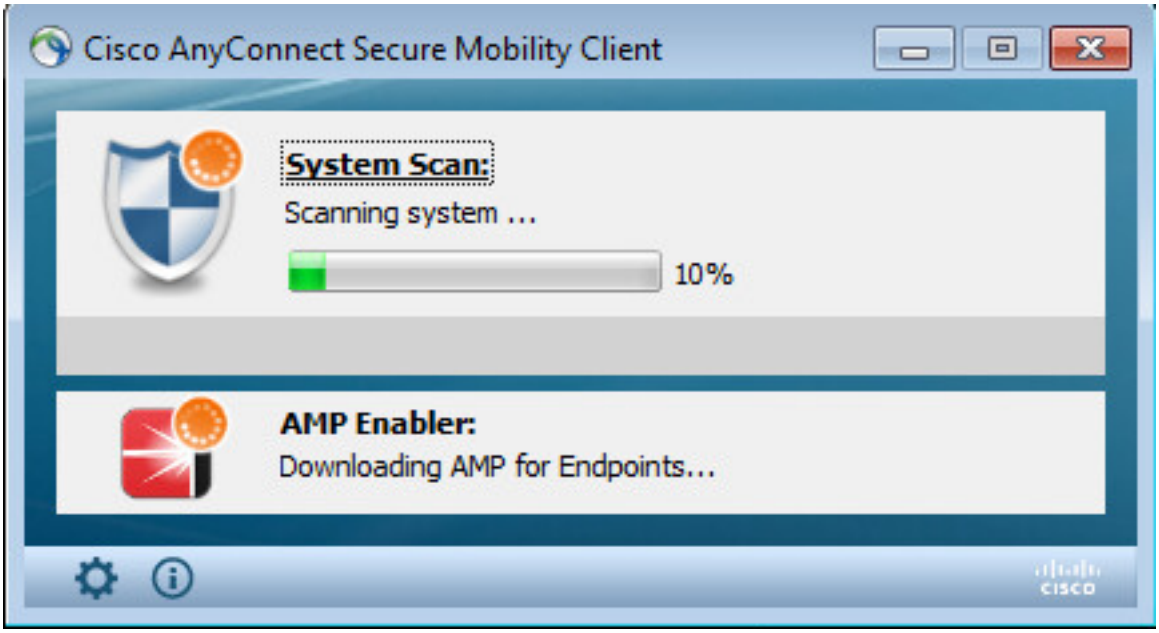
Le NSA prend soin d'installer des éléments requis et des profils.



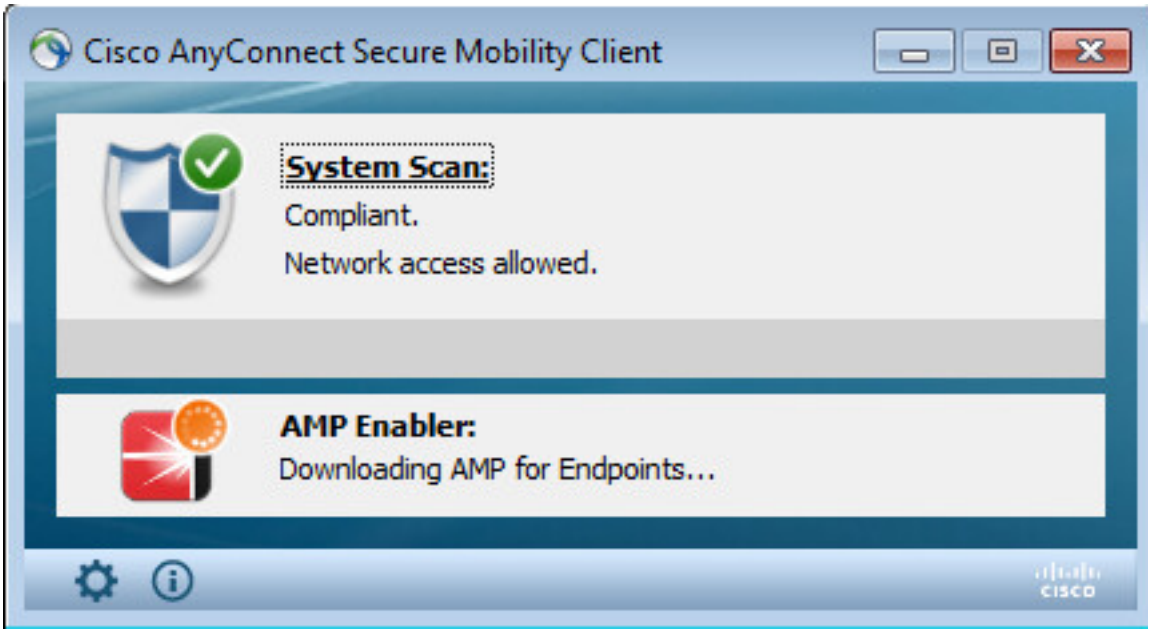


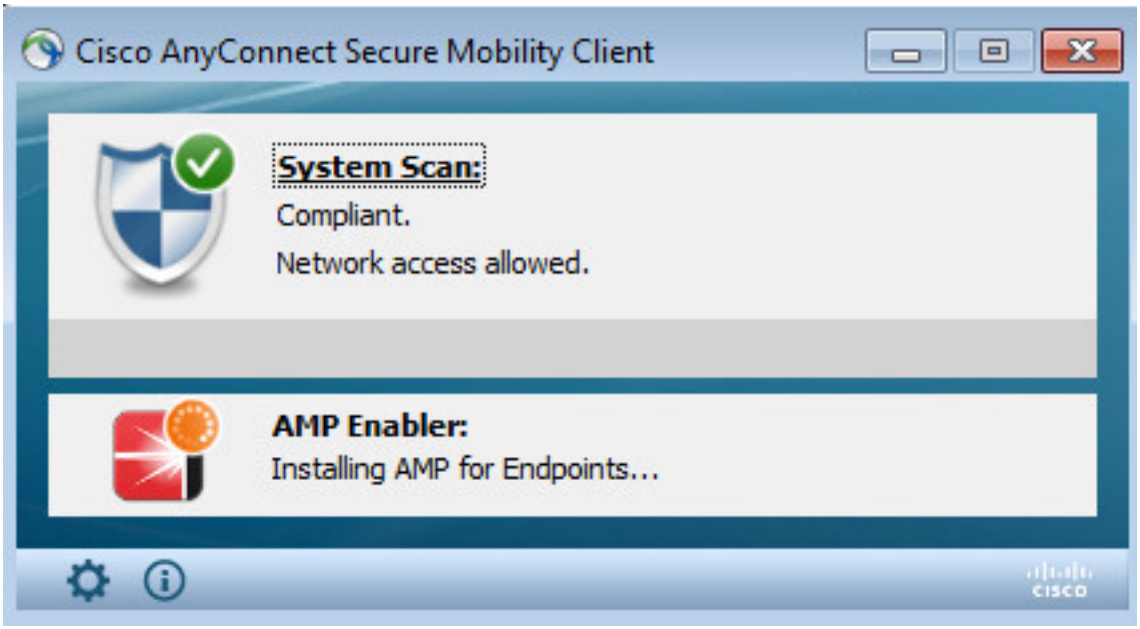
Une fois que l'installation est de finition, le module de posture d'AnyConnect exécute le contrôle de conformité.

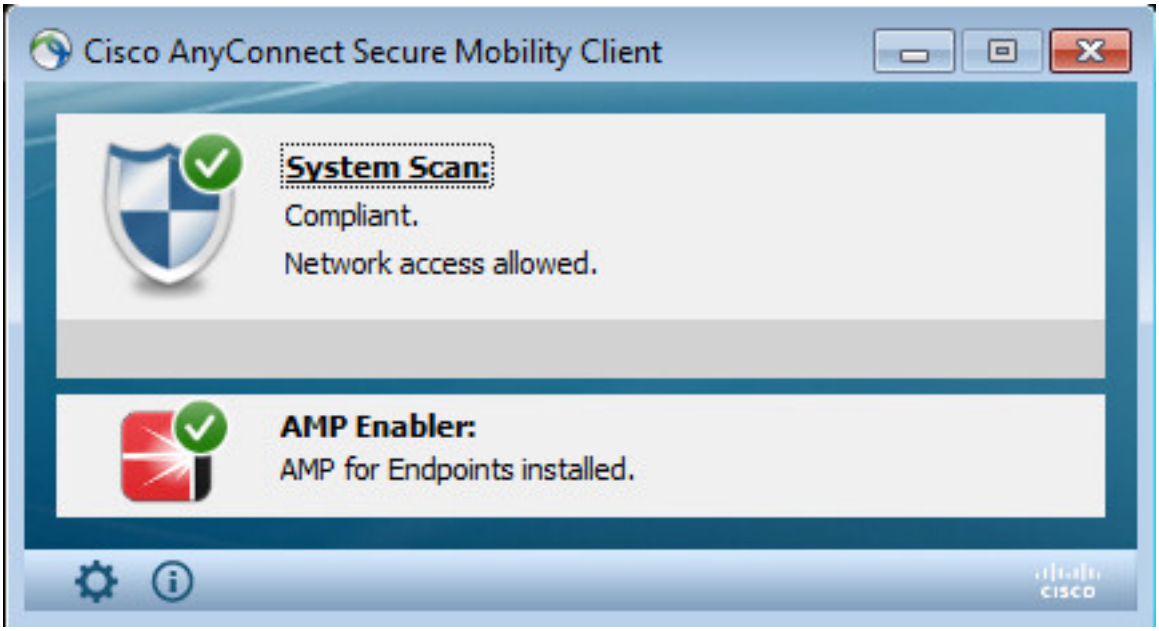




Car l'accès complet est donné, si le point final est conforme, l'AMP est téléchargé et installé du web server spécifié plus tôt dans le profil d'AMP.

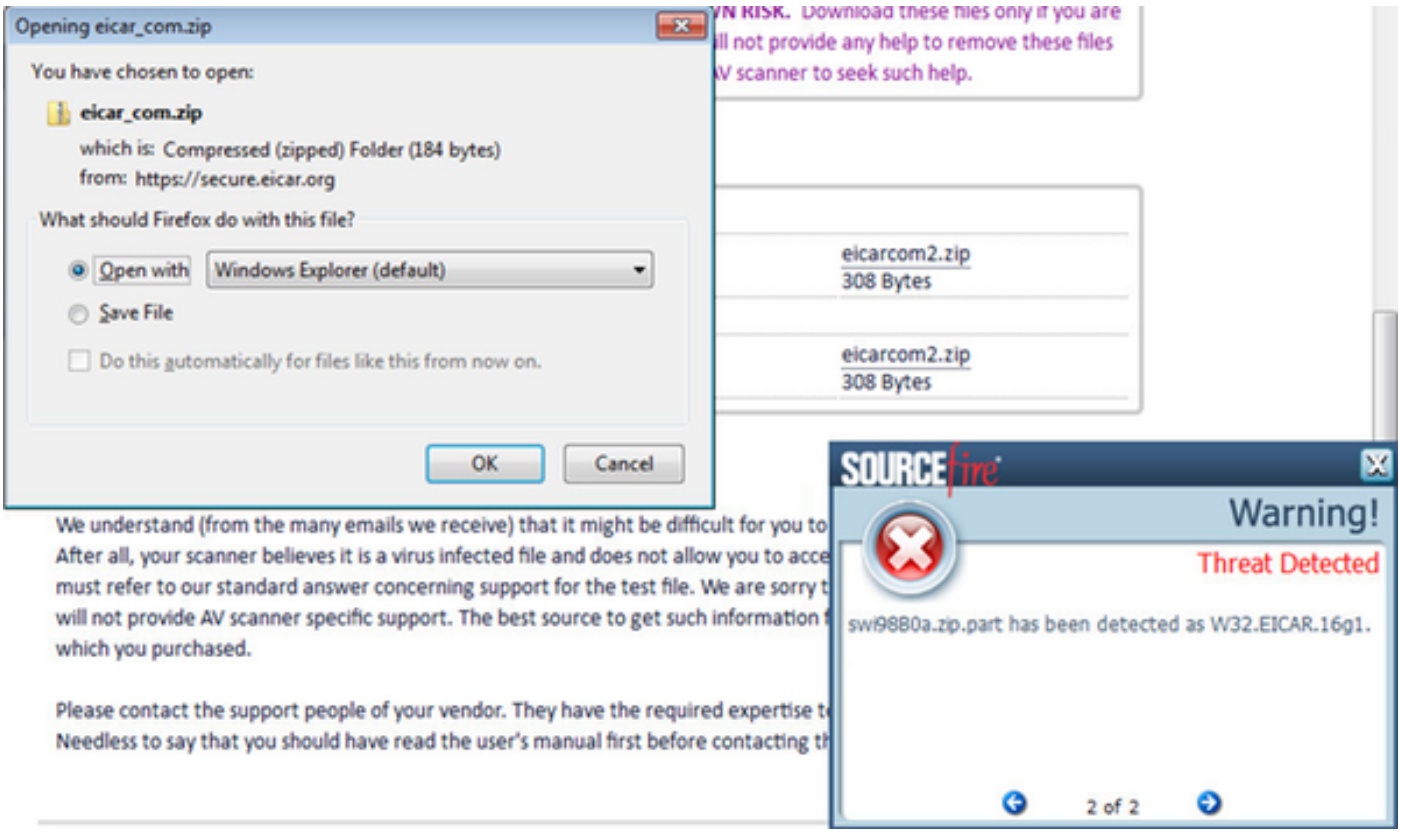






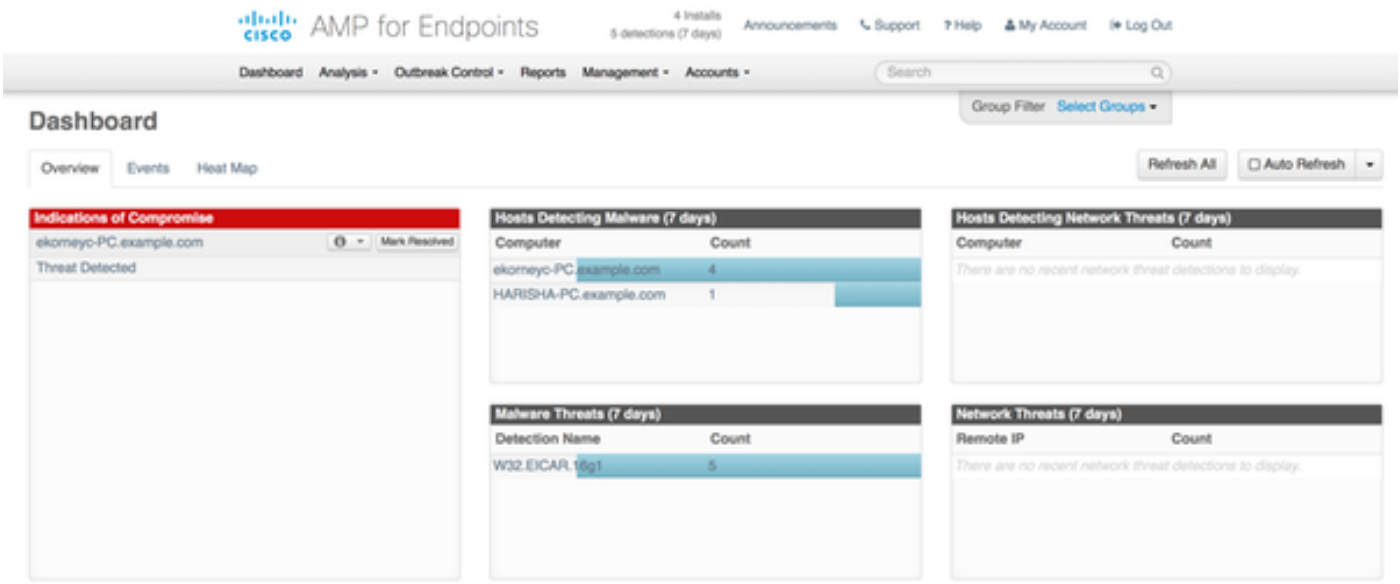
Le connecteur d'AMP apparaît.

Pour tester l'AMP dans l'action la chaîne d'Eicar contenue dans un fichier zip est téléchargée. La menace est détectée, et signalée pour le nuage d'AMP.

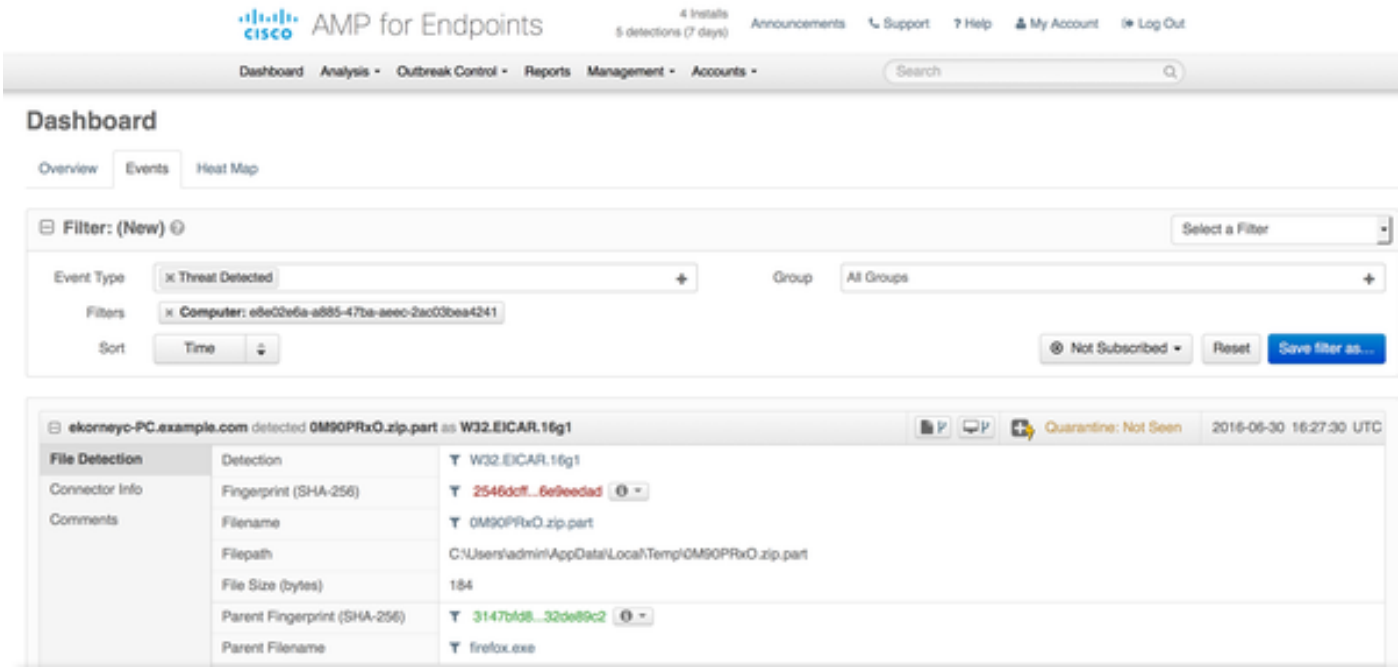


Nuage d'AMP

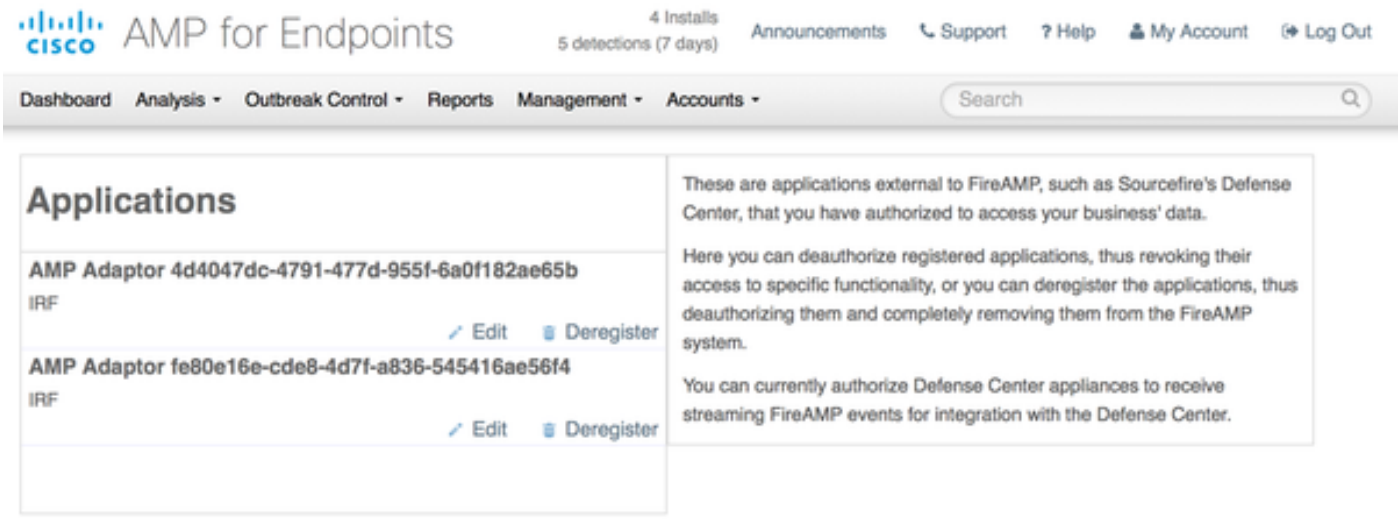
Pour vérifier les détails du tableau de bord de menace du nuage d'AMP peut être utilisé.



Afin d'obtenir plus de détails au sujet de la menace, filepath et fingerpints, vous pouvez cliquer sur en fonction l'hôte, où le malware a été détecté.

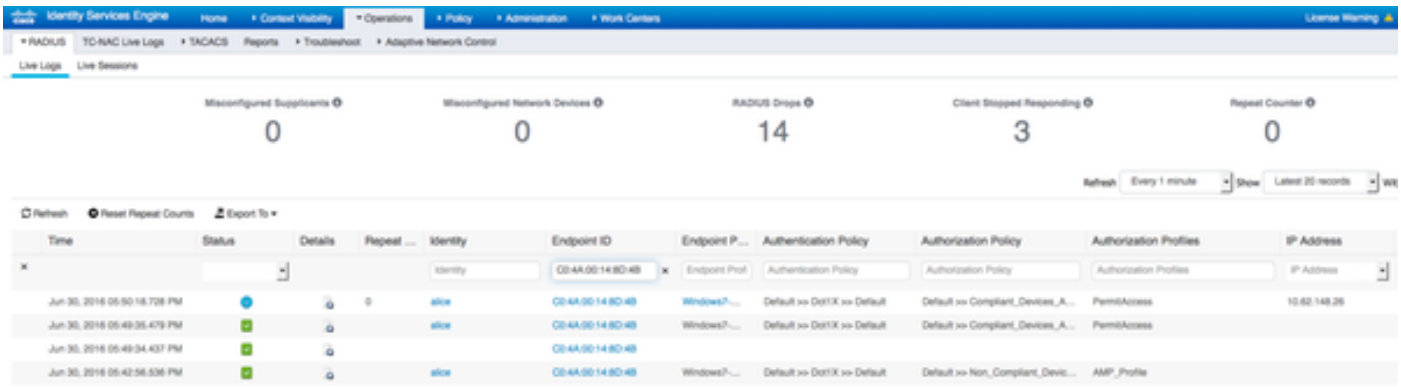


Pour visualiser ou radier de l'immatriculation l'exemple d'ISE que vous pouvez naviguer vers des comptes > des applications

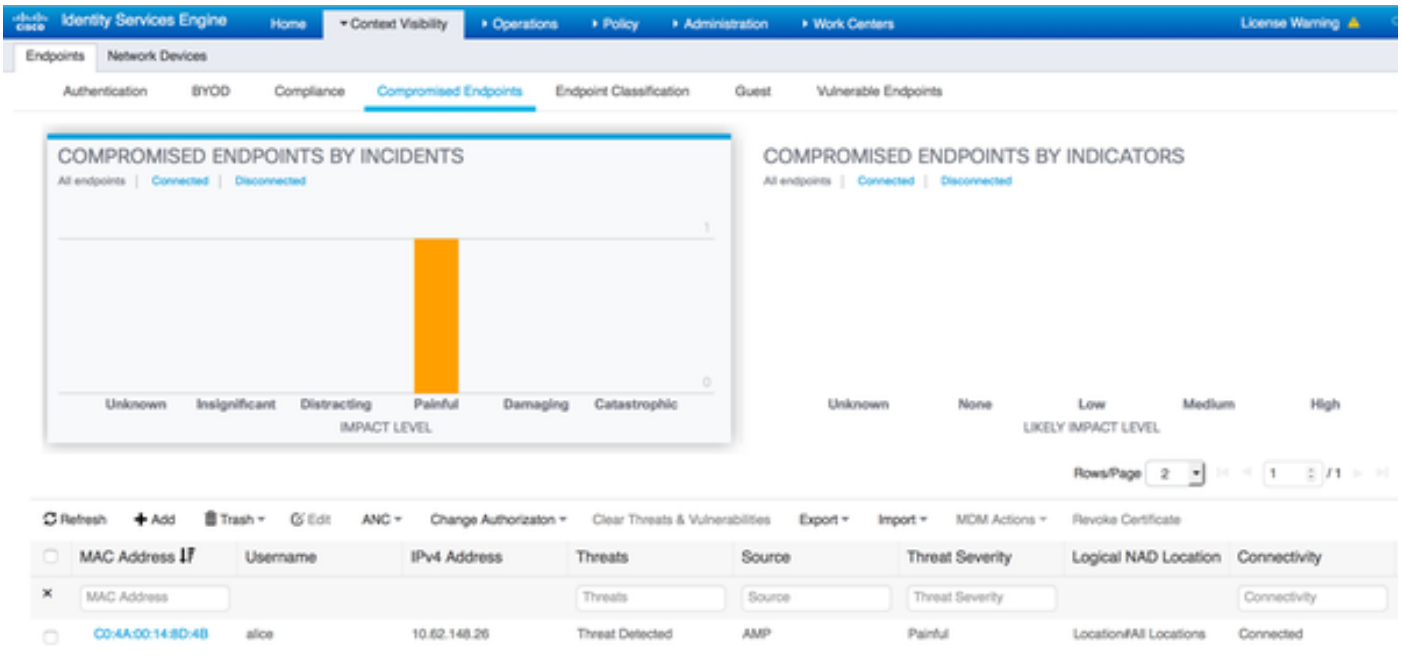


ISE

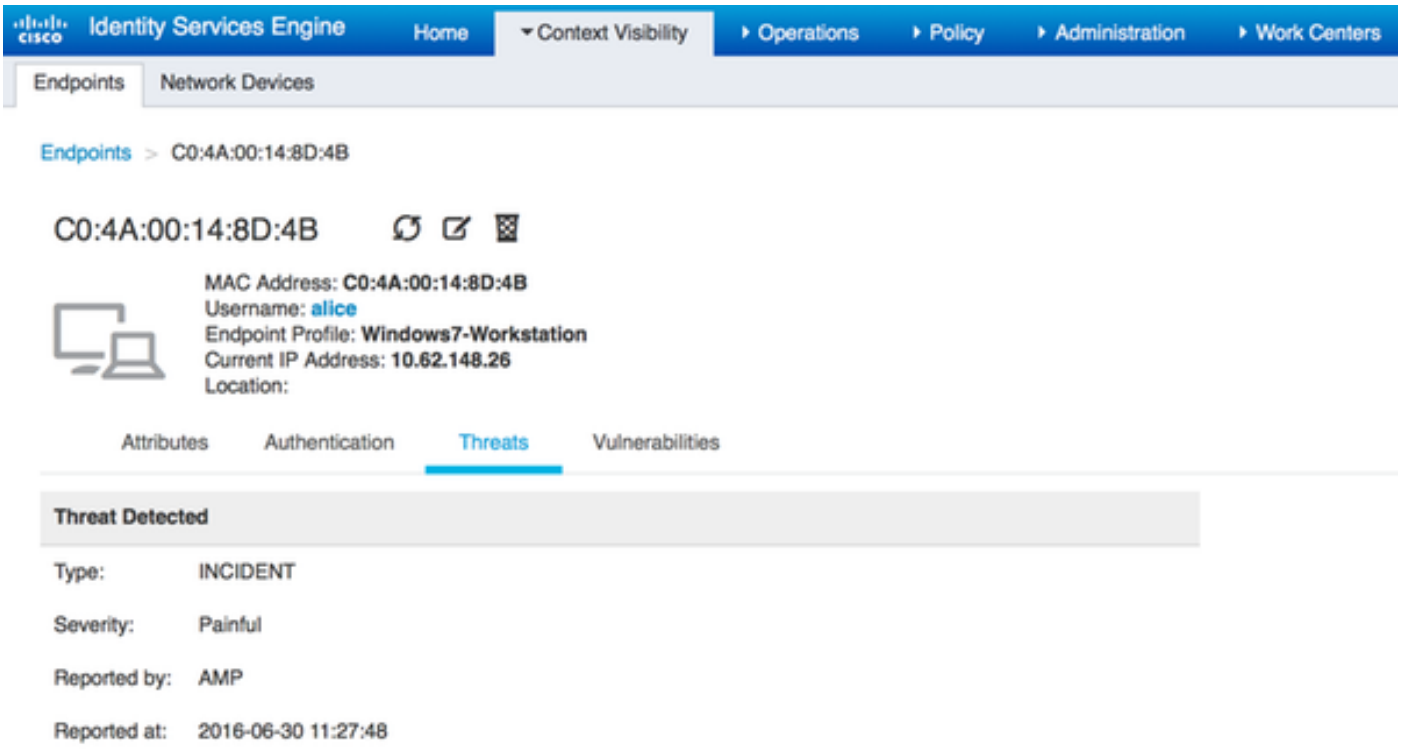
Sur ISE que lui-même l'écoulement régulier de posture est vu, redirection a lieu d'abord pour vérifier la conformité de réseau. Dès que le point final sera conforme, CoA Reauth est envoyé et le nouveau profil avec PermitAccess est assigné.



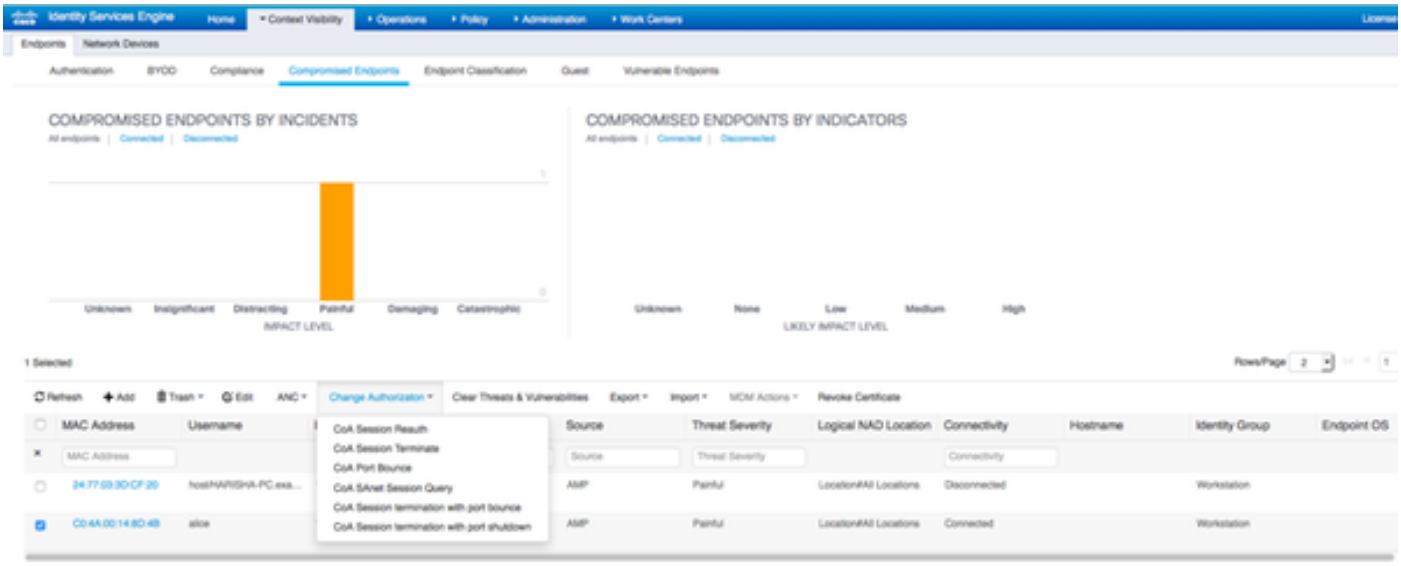
Pour visualiser les menaces détectées que vous pouvez naviguer vers la visibilité > les points finaux de contexte > des points finaux compromis



Si vous sélectionnez le point final et naviguez vers l'onglet de menace, plus de détails sont affichés.



Quand un événement de menace est détecté pour un point final, vous pouvez sélectionner l'adresse MAC du point final à la page compromise de points finaux et appliquer une stratégie ANC (si configuré, par exemple quarantaine). Alternativement vous pouvez émettre la modification de l'autorisation de terminer la session.



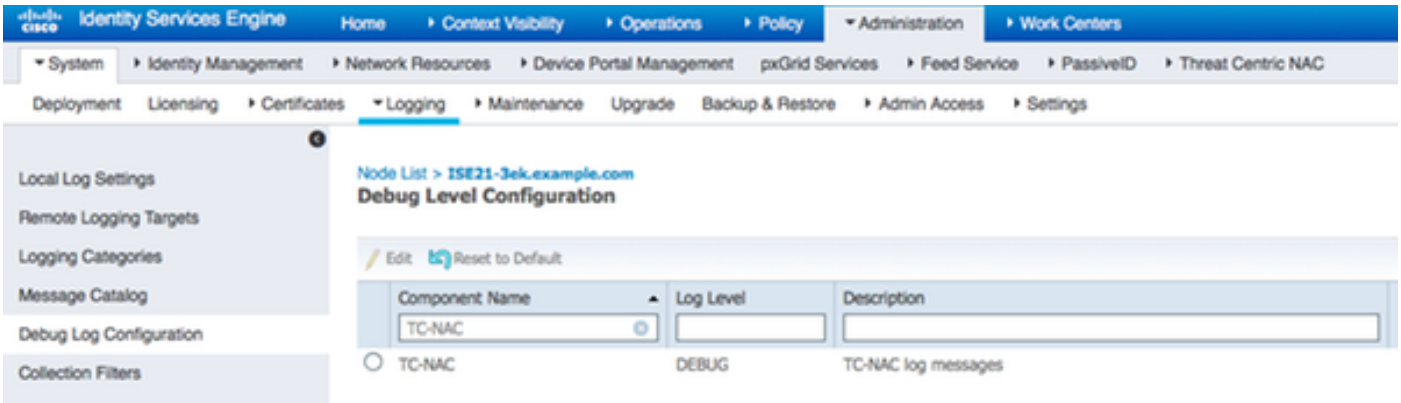
Si la session Terminate CoA est sélectionnée, ISE envoie le débranchement CoA et le client perd l'accès au réseau.

Other Attributes

ConfigVersionId	72
Acct-Terminate-Cause	Admin Reset
Event-Timestamp	1467305830
NetworkDeviceProfileName	Cisco
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
IsThirdPartyDeviceFlow	false
AcsSessionID	cfec88ac-6d2c-4b54-9fb6-716914f18744
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
Device IP Address	10.62.148.120
CiscoAVPair	audit-session-id=0a3e9478000009ab5775481d

Dépanner

Afin d'activer met au point sur ISE naviguent vers la gestion > le système > se connectant > configuration de log de debug, noeud choisi TC-NAC et changent le **niveau de log du** composant TC-NAC **POUR DÉBUGGER**



Logs à vérifier - irf.log. Vous pouvez le suivre directement d'ISE CLI :

```
ISE21-3ek/admin# show logging application irf.log tail
```

La menace même est reçue du nuage d'AMP

2016-06-30 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 de 18:27:48,617 - : : : : : : -
appelant le message du gestionnaire
com.cisco.cpm.irf.service.IrfNotificationHandler$MyNotificationHandler@3fac8043 de notification
{messageType=NOTIFICATION, messageId=THREAT_EVENT, content= {« **c0:4a:00:14:8d:4b"** :
[{« incident » : {« Impact_Qualification » : « Douloureux »}, « groupe date/heure » :
1467304068599, « constructeur » : « AMP », « titre » : « **Menace détectée** »}]} ', priority=0,
timestamp=Thu 30 juin 18:27:48 CEST 2016, amqpEnvelope=Envelope(deliveryTag=79, redeliver=false,
exchange=irf.topic.events, routingKey=irf.events.threat), amqpProperties=#contentHeader<basic>
(content-type=application/json, content-encoding=null, headers=null, delivery-mode=null,
priority=0, correlation-id=null, reply-to=null, expiration=null, message-id=THREAT_EVENT,
timestamp=null, type=NOTIFICATION, user-id=null, app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4,
cluster-id=null)}
2016-06-30 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.service.IrfNotificationHandler:handle:140 de 18:27:48,617 - : : : : : - ajouté à
la file d'attente en attente : Message {messageType=NOTIFICATION, messageId=THREAT_EVENT,
content= {« **c0:4a:00:14:8d:4b"** : [{« incident » : {« Impact_Qualification » : « **Douloureux** »},
« groupe date/heure » : 1467304068599, « constructeur » : « **AMP** », « titre » : « Menace
détectée »}]} ', priority=0, timestamp=Thu 30 juin 18:27:48 CEST 2016,
amqpEnvelope=Envelope(deliveryTag=79, redeliver=false, exchange=irf.topic.events,
routingKey=irf.events.threat), amqpProperties=#contentHeader<basic> (content-
type=application/json, content-encoding=null, headers=null, delivery-mode=null, priority=0,
correlation-id=null, reply-to=null, expiration=null, message-id=THREAT_EVENT, timestamp=null,
type=NOTIFICATION, user-id=null, app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=null)}
2016-06-30 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:59 de 18:27:48,617 - : : : : : : - FAIT
traitant la notification : #contentHeader<basic> Envelope(deliveryTag=79, de redeliver=false,
exchange=irf.topic.events, routingKey=irf.events.threat) (content-type=application/json,
content-encoding=null, headers=null, delivery-mode=null, priority=0, correlation-id=null, reply-
to=null, expiration=null, message-id=THREAT_EVENT, timestamp=null, type=NOTIFICATION, user-
id=null, app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=null)
2016-06-30 DEBUG [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:parseNotification:221 de 18:27:48,706 - : : : : : : -
analysant la notification : Message {messageType=NOTIFICATION, messageId=THREAT_EVENT,
content='{"c0:4a:00:14:8d:4b" : [{« incident » : {« Impact_Qualification » : « Douloureux »},
« groupe date/heure » : 1467304068599, « constructeur » : « AMP », « titre » : « Menace
détectée »}]} ', priority=0, timestamp=Thu 30 juin 18:27:48 CEST 2016,
amqpEnvelope=Envelope(deliveryTag=79, redeliver=false, exchange=irf.topic.events,
routingKey=irf.events.threat), amqpProperties=#contentHeader<basic> (content-
type=application/json, content-encoding=null, headers=null, delivery-mode=null, priority=0,
correlation-id=null, reply-to=null, expiration=null, message-id=THREAT_EVENT, timestamp=null,
type=NOTIFICATION, user-id=null, app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=null)}

Des informations sur la menace sont envoyées POUR FILTRER

2016-06-30 DEBUG [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:storeEventsInES:366 de 18:27:48,724 - : : : : : : -
ajoutant les informations sur l'événement de menace pour envoyer POUR FILTRER -
c0:4a:00:14:8d:4b {incident= {Impact_Qualification=Painful}, time-stamp=1467304068599,
vendor=AMP, title=Threat détectés}