Services de posture sur le guide de configuration de Cisco ISE

Contenu

Introduction

Ce document décrit des services de posture, le ravitaillement de client, la création de stratégie de posture, et la configuration de politique d'accès pour le Logiciel Cisco Identity Services Engine (ISE). Des résultats d'estimation de point final pour des clients câblés (connectés à Cisco des Commutateurs) et des clients sans fil (connectés à Cisco des contrôleurs sans-fil) sont discutés.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Logiciel Cisco Identity Services Engine (ISE)
- Configuration de commutateur de logiciel de Cisco IOS®
- Configuration Sans fil du contrôleur LAN de Cisco (WLC)

Composants utilisés

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

- Version 1.1.3 de Cisco ISE
- Version 15.0(2) SE2 de commutateur de gamme Cisco Catalyst 3560
- Version 7.4.100.0 de la gamme Cisco 2504 WLC

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Services de posture ISE

Le processus de services de posture est composé de trois sections de configuration principale :

- Ravitaillement de client
- Stratégie de posture
- Stratégie d'autorisation

Ravitaillement de client

Afin d'exécuter l'estimation de posture et déterminer l'état de conformité d'un point final, il est nécessaire de provision le point final avec un agent. L'agent de Contrôle d'admission au réseau (NAC) peut être persistant, par lequel l'agent soit installé et soit automatiquement chargés chaque fois les logins d'un utilisateur. Alternativement, l'agent NAC peut être temporel, par lequel un agent basé sur le WEB soit dynamiquement téléchargé au point final pour chaque nouvelle session et alors retiré après le processus d'estimation de posture. Les agents NAC également facilitent la correction et fournissent une politique d'utilisation acceptable facultative (AUP) à l'utilisateur final.

Par conséquent, une des premières étapes dans le processus est de récupérer les fichiers d'agent du site Web Cisco et de créer les stratégies qui déterminent quels agent et fichiers de configuration sont téléchargés aux points finaux, basés sur des attributs tels que le type d'identité de l'utilisateur et de SYSTÈME D'EXPLOITATION de client.

Stratégie de posture

La stratégie de posture définit l'ensemble de conditions requises pour qu'un point final soit conforme considéré basé sur la présence de fichier, clé de registre, processus, application, Windows, et le (AS) de l'antivirus (poids du commerce) /anti-spyware vérifie et ordonne. La stratégie de posture est appliquée aux points finaux basés sur un ensemble de conditions défini tel que le type d'identité de l'utilisateur et de SYSTÈME D'EXPLOITATION de client. Le statut de conformité (posture) d'un point final peut être :

- Inconnu : Aucune donnée n'a été collectée afin de déterminer l'état de posture.
- Noncompliant : Une estimation de posture a été exécutée, et un ou plusieurs conditions requises ont manqué.
- Conforme : Le point final est conforme avec toutes les conditions obligatoires.

Des conditions requises de posture sont basées sur un ensemble configurable d'un ou plusieurs conditions. Les conditions simples incluent un contrôle simple d'estimation. Les conditions composées sont un groupe logique d'un ou plusieurs conditions simples. Chaque condition requise est associée avec une action de correction qui aide des points finaux à répondre à l'exigence, telle que la mise à jour de signature poids du commerce.

Stratégie d'autorisation

La stratégie d'autorisation définit les niveaux de l'accès au réseau et des services en option à livrer à un point final basé sur l'état de posture. Des points finaux qui sont considérés non conformes avec la stratégie de posture peuvent être sur option mis en quarantaine jusqu'à ce que le point final devienne conforme ; par exemple, une stratégie typique d'autorisation peut limiter l'accès au réseau d'un utilisateur pour poser et les ressources en correction seulement. Si la correction par l'agent ou l'utilisateur final est réussie, alors la stratégie d'autorisation peut accorder l'accès au réseau privilégié à l'utilisateur. La stratégie est souvent imposée avec les listes téléchargeables de contrôle d'accès (dACLs) ou l'affectation dynamique VLAN. Dans cet exemple de configuration, des dACLs sont utilisés pour l'application d'accès de point final.

Processus d'exemple de posture

Dans ces fichiers persistants (agent NAC) et temporels d'exemple de configuration, de Web (d'agent) d'agent sont téléchargés à ISE, et des stratégies de ravitaillement de client sont définies qui exigent des utilisateurs de domaine de télécharger les utilisateurs d'agent et d'invité NAC pour télécharger l'agent de Web.

Avant estimation de posture des stratégies et les conditions requises sont configurées, la stratégie d'autorisation est mise à jour pour s'appliquer des profils d'autorisation aux utilisateurs et aux invités de domaine qui sont signalés comme noncompliant. Le nouveau profil d'autorisation défini dans cette configuration limite l'accès pour poser et les ressources en correction. On permet à des employés et les utilisateurs d'invité signalés en tant que conforme l'accès au réseau régulier. Une fois que des services de ravitaillement de client ont été vérifiés, des conditions requises de posture sont configurées afin de vérifier l'installation d'antivirus, les mises à jour de définition de virus, et les mises à jour essentielles de Windows.

> **Note**: Vérifiez tous les éléments sur des ces point final et listes de contrôle ISE avant que vous tentiez de configurer la posture.

Liste de contrôle de point final

1. Le nom de domaine complet ISE (FQDN) doit être résoluble par le périphérique d'extrémité.
2. Vérifiez que le navigateur de point final est configuré comme affiché ici :

   Firefox ou Chrome : Le module d'extension de Javas doit être activé sur les navigateurs.**Internet Explorer** : ActiveX doit être activé en configurations du navigateur.**Internet Explorer 10** :**Importer le certificat Auto-signé** : Si vous utilisez un certificat auto-signé pour ISE, exécutez l'Internet Explorer 10 en mode d'administrateur afin d'installer ces Certificats.**Mode compatible** : Le mode compatible doit être changé sur des configurations de l'Internet Explorer 10 afin de permettre le téléchargement d'agent NAC. Afin de changer cette configuration, cliquez avec le bouton droit la barre bleue en haut de l'écran de l'Internet Explorer 10, et choisissez la **barre de commande**. Naviguez vers des **outils >** des configurations de **vue de compatibilité**, et ajoutez l'IP ou le FQDN ISE à la liste de site.
   Activation du contrôle ActiveX : Cisco ISE installe l'agent de Cisco NAC et l'agent de Web avec le contrôle ActiveX. En Internet Explorer 10, l'option d'inciter pour des contrôles d'ActiveX est désactivée par défaut. Prenez ces mesures afin d'activer cette option : Naviguez vers des **outils > des options Internet**.Naviguez vers l'**onglet Sécurité**, et cliquez sur le **niveau d'Internet** et de **coutume**.Dans les contrôles et les modules d'extension d'ActiveX sectionnez, activez l'**incitation automatique pour des contrôles d'ActiveX**.
3. Si un Pare-feu existe localement sur le client ou le long du chemin réseau à l'ISE, vous devez ouvrir ces ports pour la transmission ISE NAC :

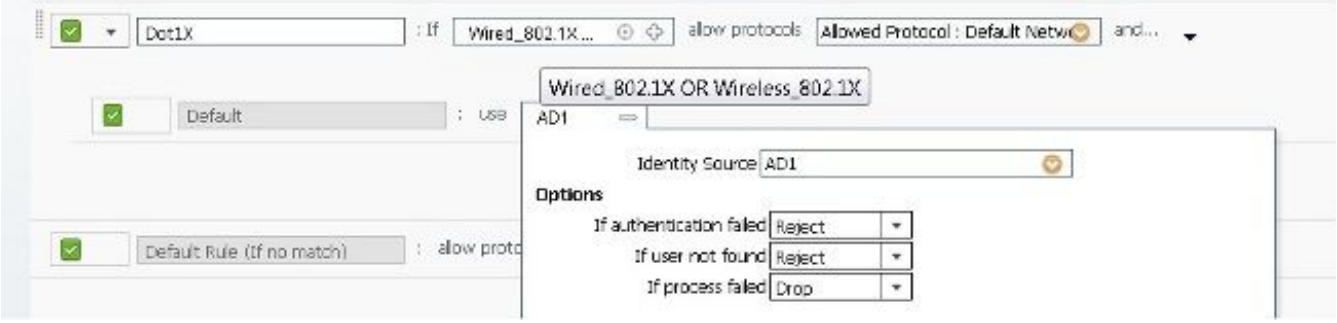
   UDP/TCP 8905 : Utilisé pour la transmission de posture entre l'agent NAC et l'ISE (port de Suisse).UDP/TCP 8909 : Utilisé pour le ravitaillement de client.TCP 8443 : Utilisé pour l'invité et la détection de posture.**Note**: ISE n'utilise plus le TCP existant 8906 de port.
4. Si le client fait configurer un serveur proxy, modifiez les paramètres de proxy afin d'exclure l'adresse IP de l'ISE. Le manque de faire casse ainsi les transmissions exigées pour l'authentification Web centrale (CWA) et le ravitaillement de client.

Liste de contrôle ISE

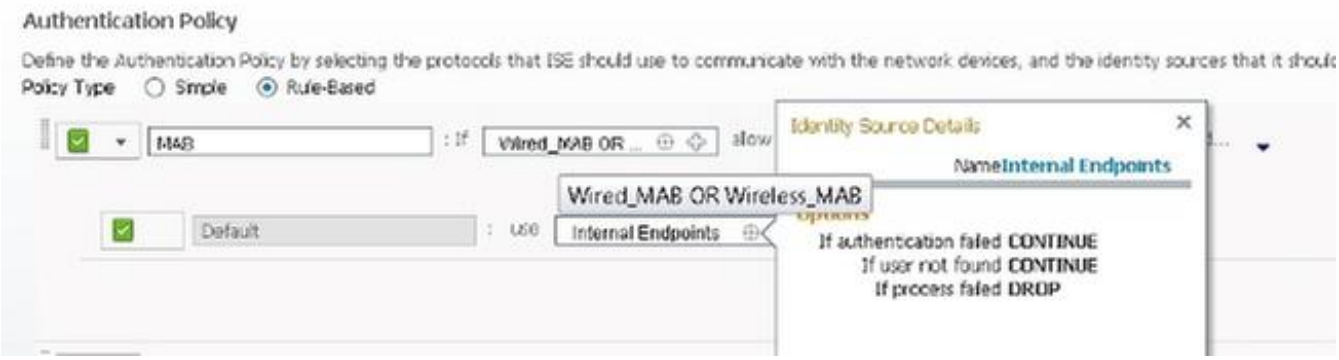
- Naviguez vers la **gestion > les sources extérieures > le Répertoire actif d'identité**, et vérifiez qu'ISE est joint au domaine de Répertoire actif (AD).

- Cliquez sur l'onglet de **groupes**, et le vérifiez que les users group de domaine sont ajoutés à la configuration d'AD.
- Naviguez vers la **gestion > les ressources de réseau > les périphériques de réseau**, et vérifiez que le commutateur et les WLC sont définis comme périphériques d'accès au réseau (NAD).
- Sous la **stratégie > l'authentification**, assurez que le dot1x et les règles de dérivation d'authentification MAC (MAB) sont configurés comme décrit ici :

  Des authentifications de dot1x pour de câble et des clients sans fil sont envoyées à la mémoire d'identité d'AD.



  Des authentifications de MAB pour de câble et des périphériques sans fil sont envoyées aux points finaux internes ; soyez sûr de vérifier l'option **si l'utilisateur non trouvé CONTINUENT**.



Configurez ISE

Aperçu de configuration ISE

Cette configuration de l'exemple ISE est composée de ces étapes :

1. Configurez et déployez les services de ravitaillement de client.
2. Configurez les stratégies d'autorisation.
3. Configurez les stratégies de posture.
4. Configurez la correction du service de mise à jour de Windows Server (WSUS).

Configurez et déployez les services de ravitaillement de client

1. Vérifiez la configuration de proxy ISE.

Naviguez vers la **gestion > le système > les configurations > le proxy**. Si un proxy est exigé pour l'accès Internet, terminez-vous le serveur et mettez en communication les détails.

2. La posture prête à l'emploi de téléchargement vérifie AV/AS et Microsoft Windows.

   Naviguez vers la **gestion > le système > les configurations > la posture > les mises à jour**. L'information de mise à jour dans le volet droit inférieur devrait être vide puisqu'aucune mise à jour n'a été téléchargée encore. Configurez ces valeurs :

   Cliquez sur la **mise à jour maintenant**, et reconnaissez l'avertissement que les mises à jour peuvent prendre un certain temps de se terminer.

   Note: S'ISE n'a pas l'accès Internet, les mises à jour hors ligne de posture sont disponibles pour le téléchargement sur Cisco.com.

3. (Facultatif) configurez les paramètres généraux pour le comportement d'agent.

   La gestion > le système > les configurations > la posture > les paramètres généraux choisis, et passent en revue les valeurs par défaut pour le temporisateur de correction, le retard de transition de réseau, et l'état par défaut de posture. Placez le temporisateur de correction à 8 minutes.Vérifiez (enable) l'**écran automatiquement étroit de succès de procédure de connexion après** case à cocher, et le set time à 5 secondes comme affiché ici :

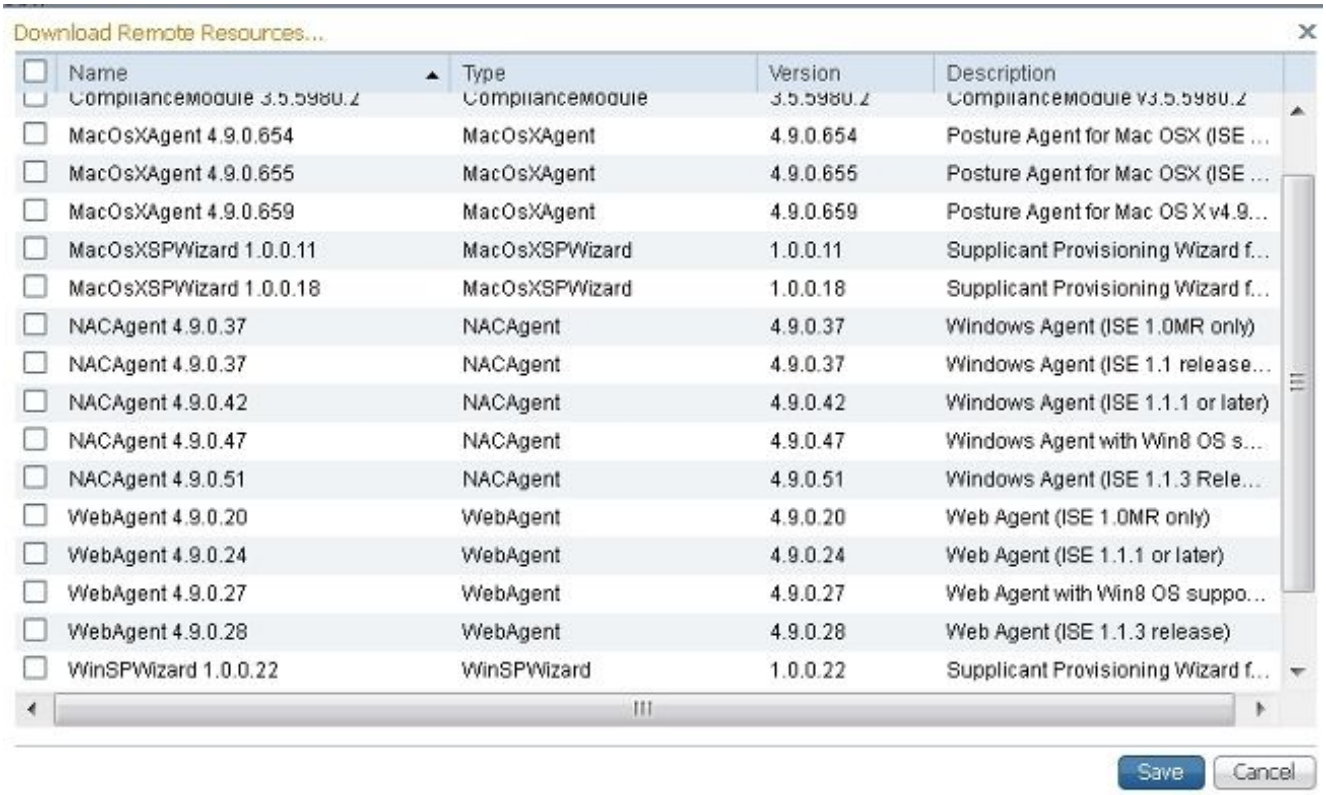
   Cliquez sur **Save**.
   Note: Valeurs assignées par le dépassement de profil d'agent ces paramètres généraux. L'état par défaut de posture définit l'état pour les clients qui ne font pas installer un agent NAC. Si le ravitaillement de client n'est pas utilisé, cette valeur peut être placée à noncompliant.

4. Placez l'emplacement et la stratégie pour télécharger des mises à jour de ravitaillement de client.

   Cliquez sur la **gestion > le système > les configurations > le ravitaillement de client du** volet gauche, et les vérifiez que ces valeurs par défaut sont placées :

5. Téléchargez les fichiers d'agent.

   Naviguez vers la **stratégie > les éléments > les résultats de stratégie**, développez le répertoire de **ravitaillement de client**, et sélectionnez les **ressources**.Du volet droit, cliquez sur Add > des **ressources en agent de site de Cisco de la** liste déroulante. Une fenêtre externe affiche les ressources distantes :



Au minimum, sélectionnez l'agent du courant NAC, l'agent de Web, et le module de conformité (module de support AV/AS) de la liste, et de la **sauvegarde de** clic. Les types de fichier de ravitaillement de client sont :

Agent NAC : Agent intermédiaire persistant pour des PC de client Windows.**Agent de Mac OS X** : Agent intermédiaire persistant pour des PC de client de Mac OS X.**Agent de Web** : Agent intermédiaire temporel pour des PC de Windows seulement.**Module de conformité** : Module OPSWAT qui fournit des mises à jour au support technique du constructeur en cours AV/AS pour l'agent NAC et l'agent de Mac OS X. Pas applicable à l'agent de Web.**Profils** : Fichiers de configuration d'agent pour l'agent NAC et l'agent de Mac OS X. Les mises à jour localement ont installé des fichiers XML sur des PC de client. Pas applicable à l'agent de Web.Attendez jusqu'à ce que les fichiers soient téléchargés à l'appliance ISE.

6. (Facultatif) créez un profil de configuration d'agent NAC pour vos clients.

   Du volet droit, cliquez sur Add, puis sélectionnez le **profil d'agent intermédiaire ISE de la** liste déroulante. Modifiez le profil afin de répondre aux exigences de déploiement.

   L'option de fusion met à jour le paramètre en cours de profil d'agent seulement si aucune autre valeur n'est définie.L'option d'écraser mette à jour la valeur de paramètre, qu'explicitement défini ou pas.Pour une liste complète de paramètres configurables d'agent NAC, référez-vous au guide utilisateur de Logiciel Cisco Identity Services Engine, la release 1.1.x.
7. Définissez la stratégie de ravitaillement de client pour des utilisateurs de domaine et des utilisateurs d'invité.

   Naviguez vers la **stratégie > le ravitaillement de client**. Ajoutez deux nouvelles règles de ravitaillement de client conformément à cette table. Cliquez sur les **ACTIONS** se boutonnent à la droite de n'importe quelle entrée de règle afin d'insérer ou reproduire des règles.

Note: Si des plusieurs versions du même type de fichier (module de conformité d'agent de Web d'agent NAC) étaient téléchargées au référentiel de ravitaillement de client, sélectionnez la version la plus en cours disponible quand vous configurez la règle.**Sauvegarde de** clic une fois terminé.

8. Configurez le portail d'authentification Web afin de télécharger l'agent intermédiaire comme défini par la stratégie de ravitaillement de client.

   Naviguez vers la **gestion > la Gestion > les configurations de portail web**, développez le répertoire d'**invité**, des **configurations Multi-portailes** choisies, et sélectionnez **DefaultGuestPortal**.Sous l'onglet d'**exécution**, permettez à l'option afin de permettre à des utilisateurs d'invité pour télécharger des agents et au registre d'individu.

   Définissez un profil de temps d'enregistrement de rôle et d'individu d'invité d'enregistrement d'individu comme affiché ici. Le self service d'invité est une configuration facultative qui permet des utilisateurs de créer des comptes sans intervention de sponsor. Cet exemple permet au self service afin de simplifier la procédure d'enregistrement d'invité.

   (Facultatif) placez l'AUP pour des utilisateurs d'invité comme affiché ici :

   Sauvegarde de clic une fois terminé.

Configurez la stratégie d'autorisation pour le ravitaillement et la posture de client

La stratégie d'autorisation place les types de l'accès et de services à accorder aux points finaux basés sur leurs attributs tels que l'identité, la méthode d'accès, et la conformité aux stratégies de posture. Les stratégies d'autorisation dans cet exemple s'assurent que des points finaux qui ne sont pas posture conforme sont mis en quarantaine ; c'est-à-dire, les points finaux sont accordés l'accès limité suffisamment pour provision le logiciel agent et au remediate ont manqué des conditions requises. Seulement on accorde des points finaux conformes de posture l'accès au réseau privilégié.

1. (Facultatif). Définissez un dACL qui limite l'accès au réseau pour les points finaux qui ne sont pas posture conforme.

   Naviguez vers la **stratégie > les éléments > les résultats de stratégie**, développez le répertoire d'**autorisation**, et sélectionnez **ACLs téléchargeable**.Cliquez sur Add du volet droit sous la Gestion DACL, et écrivez ces valeurs pour le nouveau dACL.

   C'est un dACL de posture d'échantillon. Passez en revue les entrées de dACL pour la précision, parce qu'ISE 1.1.x ne prend en charge pas actuellement la validation de syntaxe

d'ACL.

Cliquez sur Submit une fois terminé.

2. Définissez un nouveau profil d'autorisation pour des utilisateurs de l'agent 802.1X-authenticated/NAC nommés **Posture_Remediation**. Le profil accroît le nouveau dACL pour le contrôle d'accès de port et l'URL réorientent l'ACL pour la redirection du trafic.

   Naviguez vers la **stratégie > les éléments > les résultats > l'autorisation de stratégie**, et sélectionnez les **profils d'autorisation**.Cliquez sur Add du volet droit, et écrivez ces valeurs pour le profil d'autorisation :

   Ces détails résultants d'attribut devraient apparaître au bas de page :

   Type d'Access = ACCESS_ACCEPT
   DACL = POSTURE_REMEDIATION
   Cisco : la POSTURE de cisco-av-pair=url-redirect-acl=ACL- RÉORIENTENT
   Cisco : cisco-av-pair=url-redirect = https://
   ip:8443/guestportal/gateway?sessionId=SessionIdValue@action=cppCliquez sur Submit afin d'appliquer vos modifications.

   Note: L'ACL ACL-POSTURE-REDIRECT doit être configuré localement sur le commutateur ou le WLC. L'ACL est mis en référence de nom dans la stratégie d'autorisation ISE. Pour le commutateur réorientez l'ACL, les entrées d'autorisation déterminent quel trafic devrait être réorienté à ISE tandis que, sur un WLC, les entrées d'autorisation définissent quel trafic ne devrait pas être réorienté.

3. Définissez un nouveau profil d'autorisation pour les utilisateurs Web-authentifié/de Web agent nommés **CWA_Posture_Remediation**. Le profil accroît le nouveau dACL pour le contrôle d'accès de port et l'URL réorientent l'ACL pour la redirection du trafic.

   Naviguez vers la **stratégie > les éléments > les résultats > l'autorisation de stratégie**, et sélectionnez les **profils d'autorisation**.Cliquez sur Add du volet droit, et écrivez ces valeurs pour le profil d'autorisation :

   Ces détails résultants d'attribut devraient apparaître au bas de page :

   Type d'Access = ACCESS_ACCEPT
   DACL = POSTURE_REMEDIATION
   Cisco : la POSTURE de cisco-av-pair=url-redirect-acl=ACL- RÉORIENTENT
   Cisco : cisco-av-pair=url-redirect
   =https://ip:8443/guestportal/gateway?sessionId=SessionIdValue@action=cwaCliquez sur Submit afin d'appliquer vos modifications.

   Note: La différence entre les deux profils est l'URL réorientent l'attribut de Cisco-poids du commerce-paires. Des utilisateurs qui doivent être authentifiés sont réorientés au portail d'invité pour CWA. Une fois qu'authentifiés, des utilisateurs sont automatiquement réorientés à CPP comme nécessaires. Des utilisateurs authentifiés par le 802.1X sont réorientés

directement à CPP.

4. Mettez à jour la stratégie d'autorisation afin de prendre en charge la conformité de posture.

   Naviguez vers la **stratégie > l'autorisation**. Mettez à jour la stratégie existante d'autorisation avec ces valeurs. Utilisez le sélecteur à l'extrémité d'une entrée de règle afin d'insérer ou reproduire des règles :

   Sauvegarde de clic afin d'appliquer vos modifications.

   Note: Ce profil d'autorisation est appliqué à l'accès câblé et d'utilisateur de sans fil. Le WLC ne prend pas en compte le dACL. La caractéristique de dACL est prise en charge seulement sur des Commutateurs. Pour la radio, l'ACL de réorientation est assez pour refuser tout le trafic excepté le serveur de correction et la posture ISE.

Configurez la stratégie de posture poids du commerce

Cet exemple affiche comment définir une stratégie poids du commerce avec ces états de posture :

- Posez la stratégie pour que des utilisateurs de domaine fassent installer ClamWin poids du commerce et courant.
- Posez la stratégie pour que les utilisateurs d'invité installent ClamWin poids du commerce si aucun antivirus n'est installé.

1. Définissez un état de posture poids du commerce qui valide l'installation de ClamWin poids du commerce sur un point final. Ce contrôle sera utilisé dans des conditions requises de posture appliquées aux employés.

   Naviguez vers la **stratégie > les éléments > les états de stratégie**, développez le répertoire de **posture**, et sélectionnez l'**état de composé poids du commerce**.Cliquez sur Add du menu droit de volet. Si Produits poids du commerce n'apparaît pas sous le champ de **constructeur**, des mises à jour de posture n'ont pas été encore téléchargées ou le téléchargement ne s'est pas encore terminé. Écrivez ces valeurs :

   Cliquez sur Submit au bas de page.
2. Définissez un état de posture poids du commerce qui valide la version de signature de ClamWin poids du commerce sur un point final. Ce contrôle sera utilisé dans des conditions requises de posture appliquées aux employés.

   L'état de composé choisi **poids du commerce du** volet gauche, et cliquent sur Add du menu droit de volet. Écrivez ces valeurs :

   Cliquez sur Submit au bas de page.
3. Définissez un état de posture poids du commerce qui valide l'installation de n'importe quel poids du commerce pris en charge sur un point final. Ce contrôle sera utilisé pour des conditions requises de posture appliquées aux utilisateurs d'invité.

   L'état de composé choisi **poids du commerce du** volet gauche, et cliquent sur Add du menu droit de volet. Écrivez ces valeurs :

Cliquez sur Submit au bas de page.

4. Définissez une action de correction de posture qui installe ClamWin poids du commerce sur un point final.

   Naviguez vers la **stratégie > les éléments > les résultats de stratégie**, et développez le répertoire de **posture**.Développez le contenu des **actions de correction**.Sélectionnez la **correction de lien**, et cliquez sur Add du menu droit de volet. Écrivez ces valeurs :

   Cliquez sur **Submit**.

   Note: *L'IP de SERVEUR rem* représente l'adresse IP de votre serveur de correction où l'installation de ClamWin existe. Le fichier exécutable dans cet exemple a été mis en place préalablement sur le serveur de correction. Pour que la correction fonctionne, assurez-vous que l'IP de serveur de mise à jour de ClamWin est inclus dans le dACL précédemment configuré et réorientez l'ACL.
5. Définissez une action de correction de posture cette les mises à jour ClamWin poids du commerce sur un point final.

   La correction choisie **AV/AS du** volet gauche, et cliquent sur Add du menu droit de volet. Écrivez ces valeurs :

   Cliquez sur **Submit**.
6. Définissez les conditions requises de posture qui seront appliquées aux employés et aux utilisateurs d'invité.

   Les conditions requises choisies de la **stratégie > des éléments de stratégie > résulte > posture**. Écrivez ces entrées dans la table. Utilisez le sélecteur à l'extrémité d'une entrée de règle afin d'insérer ou reproduire des règles :

   Sauvegarde de clic une fois terminé.

   Note: Si un état préconfiguré n'affiche pas sous la liste d'états, vérifiez que le SYSTÈME D'EXPLOITATION approprié a été sélectionné pour l'état aussi bien que la règle de condition requise. Seulement conditions qui sont identiques ou sont un sous-ensemble du SYSTÈME D'EXPLOITATION sélectionné pour l'affichage de règle dans la liste de sélection de conditions.
7. Configurez la stratégie de posture afin de s'assurer que ClamWin poids du commerce est installé et le courant sur des ordinateurs des employés avec le Windows 7 et que n'importe quel poids du commerce pris en charge est installé et courant sur des ordinateurs d'utilisateur d'invité.

   Naviguez vers la **stratégie > la posture**, et créez les règles de nouvelle stratégie avec les valeurs fournies dans cette table. Afin de spécifier une condition requise de posture comme obligatoire, facultatif, ou l'audit, cliquez sur l'icône à la droite du nom de condition requise, et choisissez une option de la liste déroulante.

   Sauvegarde de clic afin d'appliquer vos modifications.

Configurez la correction WSUS

Cet exemple affiche comment s'assurer que tous les ordinateurs des employés avec le Windows 7 ont les derniers correctifs essentiels installés. Les services de mise à jour de Windows Server (WSUS) sont intérieurement gérés.

1. Définissez une action de correction de posture qui vérifie et installe les derniers correctifs de Windows 7.

   Naviguez vers la **stratégie > les éléments > les résultats de stratégie**, et développez le répertoire de **posture**.Développez le contenu des **actions de correction**.**La correction** choisie de **mise à jour de Windows Server**, et cliquent sur Add du menu droit de volet. Écrivez ces valeurs, et cliquez sur Submit :

   Note: Si vous voulez employer des règles de Cisco afin de valider la mise à jour de Windows, créez vos états de posture, et définissez vos conditions dans l'étape 2.
2. Définissez les conditions requises de posture qui seront appliquées aux employés.

   Naviguez vers la **stratégie > les éléments > les résultats > la posture de stratégie**, et sélectionnez les **conditions requises**. Écrivez ces entrées dans la table. Utilisez le sélecteur à l'extrémité d'une entrée de règle afin d'insérer ou reproduire des règles :

   Note: Vous pouvez trouver le **pr_WSUSRule de** condition sous **Cisco avez défini la condition > état composé régulier**. (C'est une règle factice choisie parce que Step1 a placé les mises à jour de Windows à valider par le niveau d'importance.)
3. Configurez la stratégie de posture afin de s'assurer que les ordinateurs des employés avec le Windows 7 ont les derniers correctifs essentiels de Windows 7.

   Naviguez vers la **stratégie > la posture**, et créez les règles de nouvelle stratégie avec les valeurs dans cette table :

   Sauvegarde de clic afin d'appliquer vos modifications.

Configuration de commutateur témoin

Cette section fournit un extrait de la configuration de commutateur. On le destine pour la référence seulement et ne devrait pas être copié ou collé dans un commutateur de production.

Radius global et configuration de dot1x

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
dot1x system-auth-control
ip radius source-interface Vlan (x)
```

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-acce ss-req
radius-server attribute 25 access-request include
radius-server host <ISE IP> key <pre shared key>
radius-server vsa send accounting
radius-server vsa send authentication
```

ACL par défaut à appliquer sur le port

```
ip access-list extended permitany
permit ip any any
```

Modification de Radius d'enable de l'autorisation

```
aaa server radius dynamic-author
client <ISE IP> server-key <pre share d key>
```

Redirection et se connecter URL d'enable

```
Ip device tracking
Epm logging
Ip http server
Ip http secure server
```

ACL de redirection

```
ip access-list extended ACL-POSTURE-REDIRECT
deny udp any eq bootpc any eq bootps
deny udp any any eq domain
deny udp any host <ISE IP> eq 8905
deny tcp any host <ISE IP> eq 8905
deny tcp any host <ISE IP> eq 8909
deny udp any host <ISE IP> eq 8909
deny tcp any host <ISE IP> eq 8443
deny ip any host <REM SERVER IP>
deny ip any host 192.230.240.8           (one of the ip of CLAMwin database virus Definitions)
permit ip any any
```

> **Note**: L'adresse IP du périphérique d'extrémité doit être accessible de l'interface virtuelle de commutateur (SVI) pour que la redirection fonctionne.

Configuration switchport

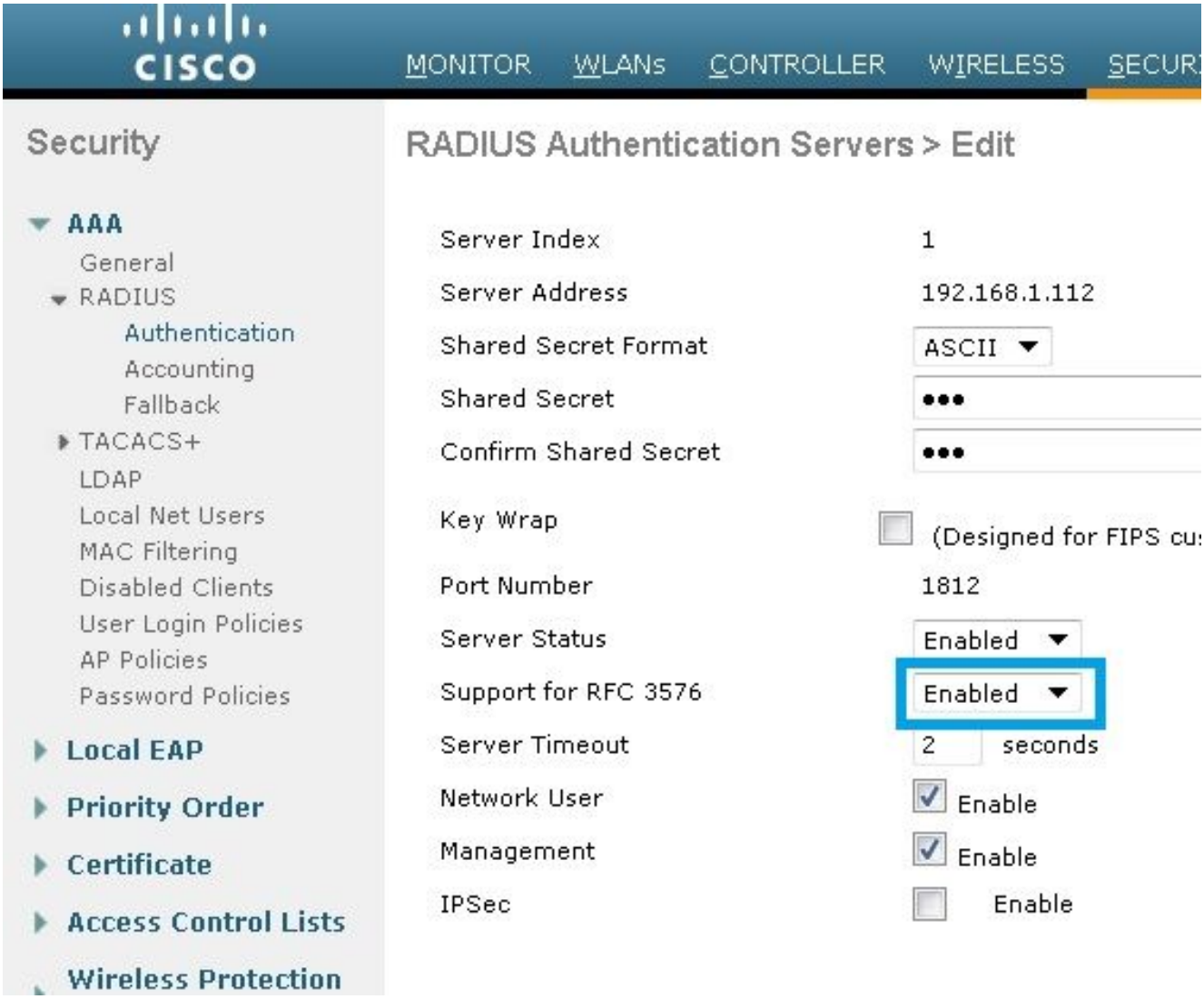
```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS earlier
than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
```

mab

Configuration de l'échantillon WLC

Configuration globale

1. Assurez-vous que le serveur de RADIUS fait activer RFC3576 (CoA) ; il n'est pas activé par défaut.



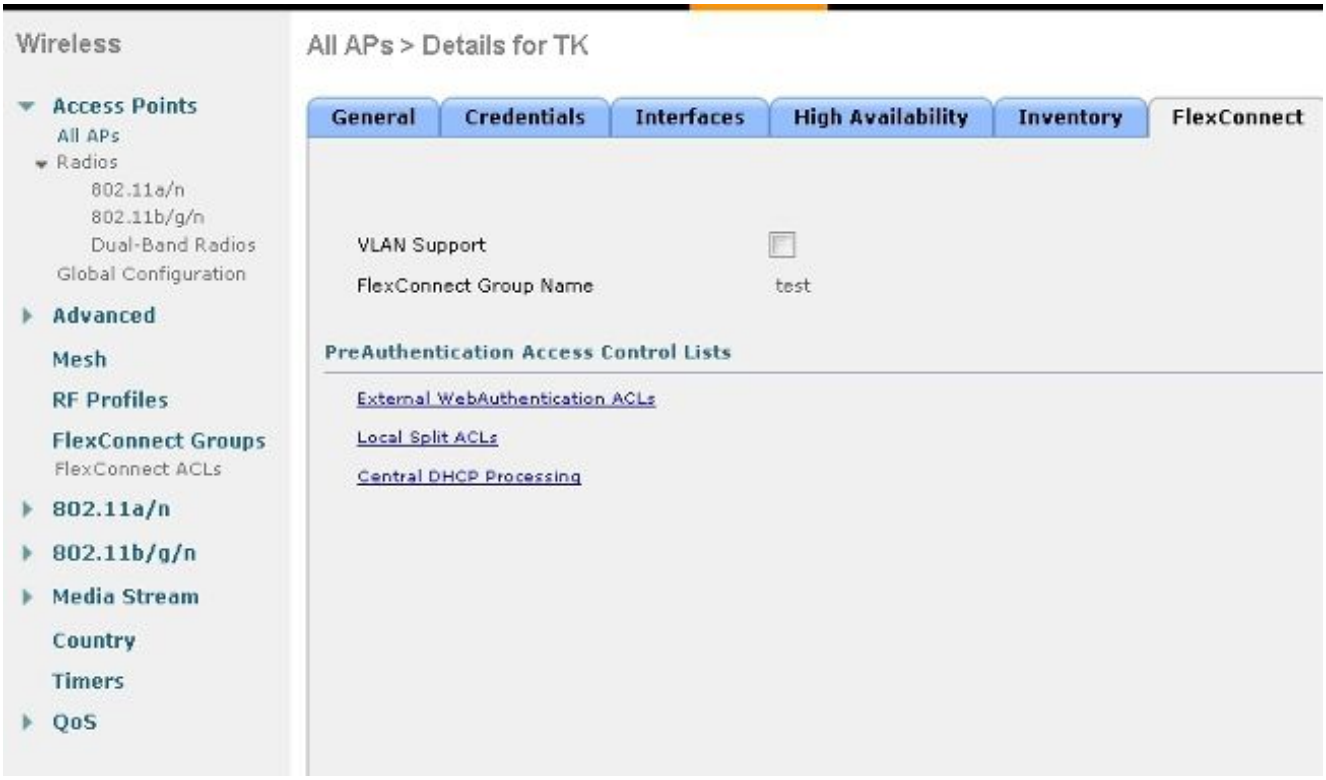
2. Naviguez vers la **Sécurité > les listes de contrôle d'accès**, créez un ACL sur le WLC et appelez-le « ACL-POSTURE-REDIRECT. »

15 et 16 sont utilisés dans cet exemple pour la mise à jour de ClamWin poids du commerce où 192.230.240.8 contient le fichier de définition de base de données.

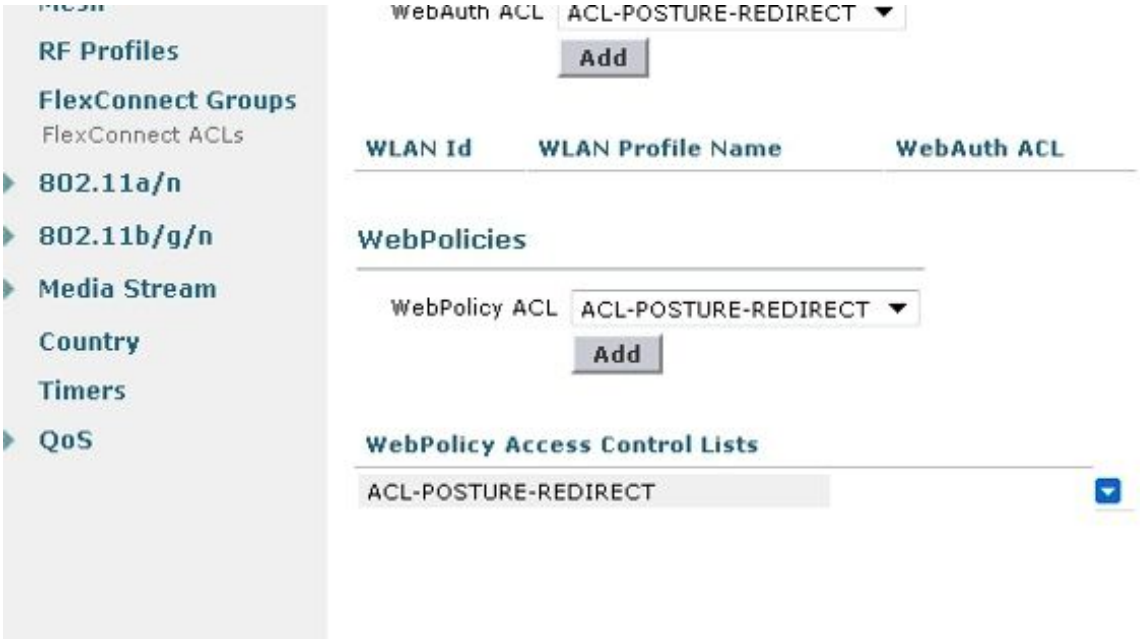
Pour FlexConnect avec la commutation locale, vous devez créer un ACL de FlexConnect, et vous appliquez l'à l'ACL de WebPolicy. L'ACL a le même nom que l'ACL sur le WLC et a les mêmes attributs.

1. Clic **FlexConnect ACLs**.

2. Clic **WebAuthentication externe ACLs**.



3. Ajoutez l'ACL de WebPolicy.



4. Cliquez sur **Apply**.

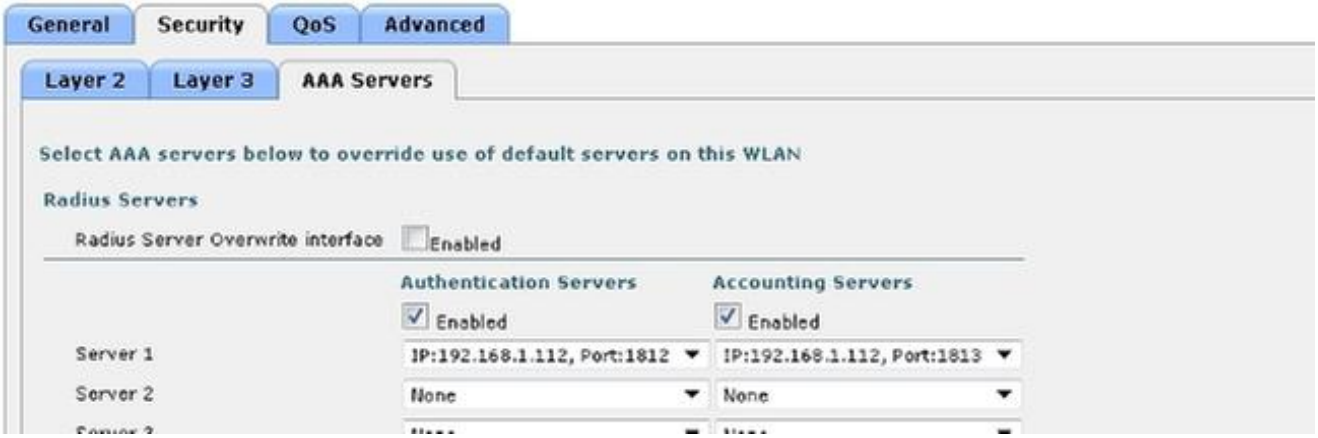
Configuration des employés SSID

Créez un nouvel Identifiant SSID (Service Set Identifier) des employés ou modifiez l'en cours.

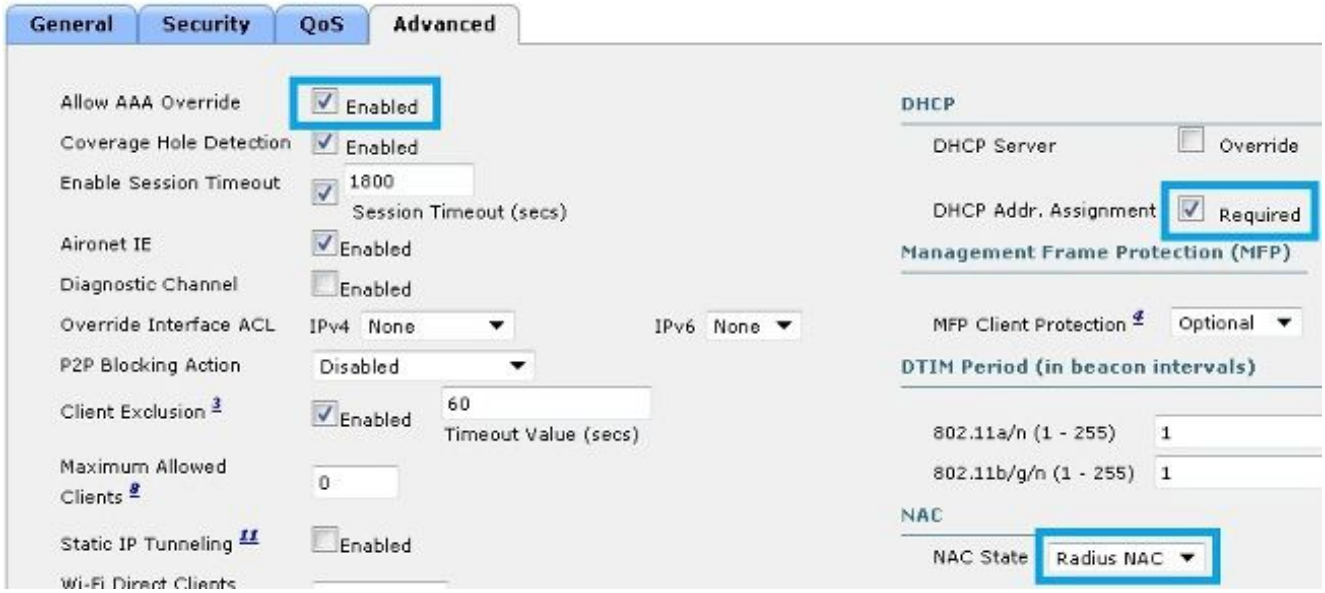
1. Dans l'onglet **WLAN**, le clic **créent nouveau** ou cliquent sur un WLAN existant.

2. Cliquez sur l'**onglet Sécurité**, cliquez sur l'onglet de la **couche 2**, puis placez la Sécurité appropriée. Voici une configuration de WPA avec le dot1x.

3. Cliquez sur l'**onglet AAA Servers**, et vérifiez (enable) l'ISE en tant que serveur de Radius pour l'authentification et la comptabilité.



4. Cliquez sur l'**onglet Avancé**, vérifiez (enable) l'**Allow AAA Override** et l'**adr DHCP.** Les cases à cocher d'**affectation**, et ont placé l'**état NAC à** Radius NAC.



Configuration de l'invité SSID

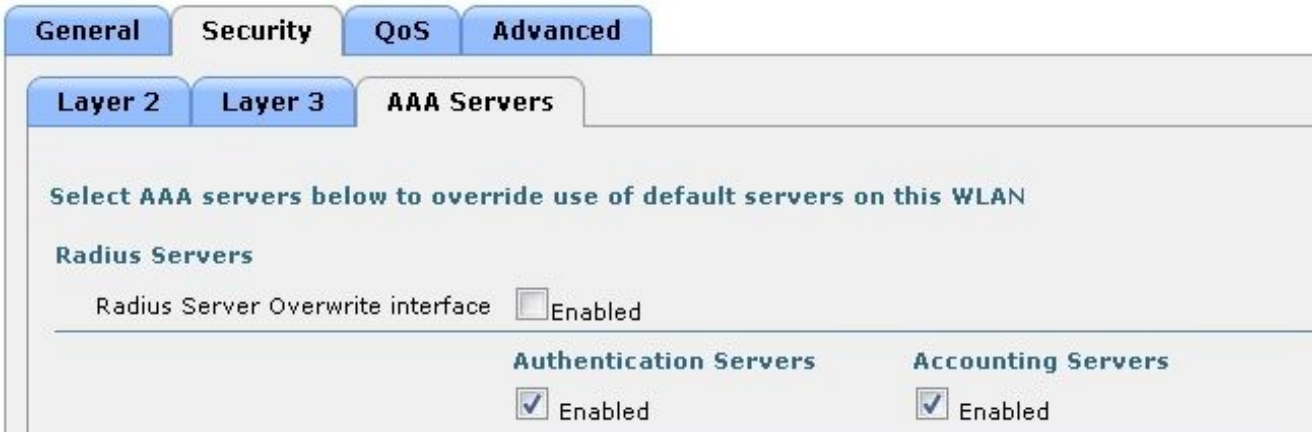
Créez un nouveau WLAN avec l'invité SSID ou modifiez en cours.

1. Dans l'onglet **WLAN**, le clic **créent nouveau** ou cliquent sur un WLAN existant.

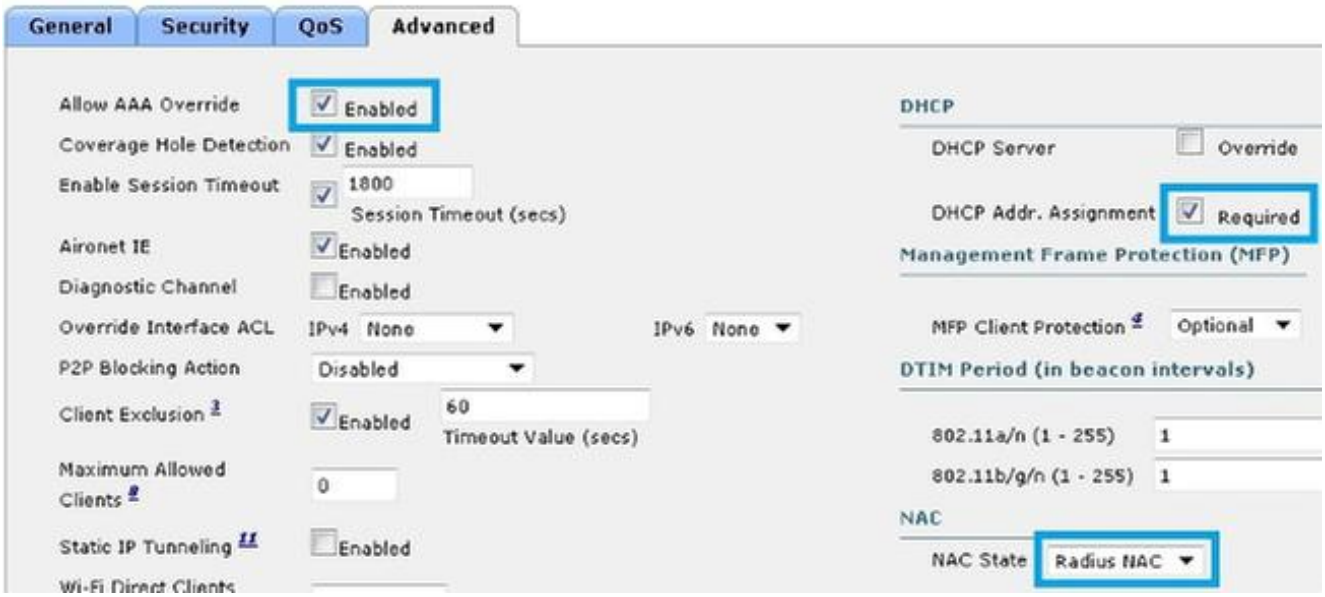
2. Cliquez sur l'**onglet Sécurité**, cliquez sur l'onglet de la **couche 2**, puis vérifiez (enable) la case à cocher de **filtrage MAC**.

3. Cliquez sur l'onglet de la **couche 3**, et l'assurez que toutes les options sont désactivées.

4. Cliquez sur l'**onglet AAA Servers**, et vérifiez (enable) l'ISE en tant qu'un serveur d'authentification et serveur de comptabilité.



5. Cliquez sur l'**onglet Avancé**, vérifiez (enable) l'**Allow AAA Override** et l'**adr DHCP.** Les cases à cocher d'**affectation**, et ont placé l'**état NAC à** Radius NAC.



Posture de dot1x des employés (agent NAC)

C'est la procédure de la posture elle-même d'un point de vue de client, une fois que le client se connecte aux WLAN précédemment configurés.

1. Configurez votre radio SSID (employé) ou réseau câblé pour PEAP MSCHAP V2, et connectez à un utilisateur d'AD au groupe d'utilisateurs de domaine.
2. Ouvrez un navigateur, et l'essai pour naviguer vers un site. Une demande de réorientation est affichée.
3. **Clic de** clic **pour installer l'agent**.

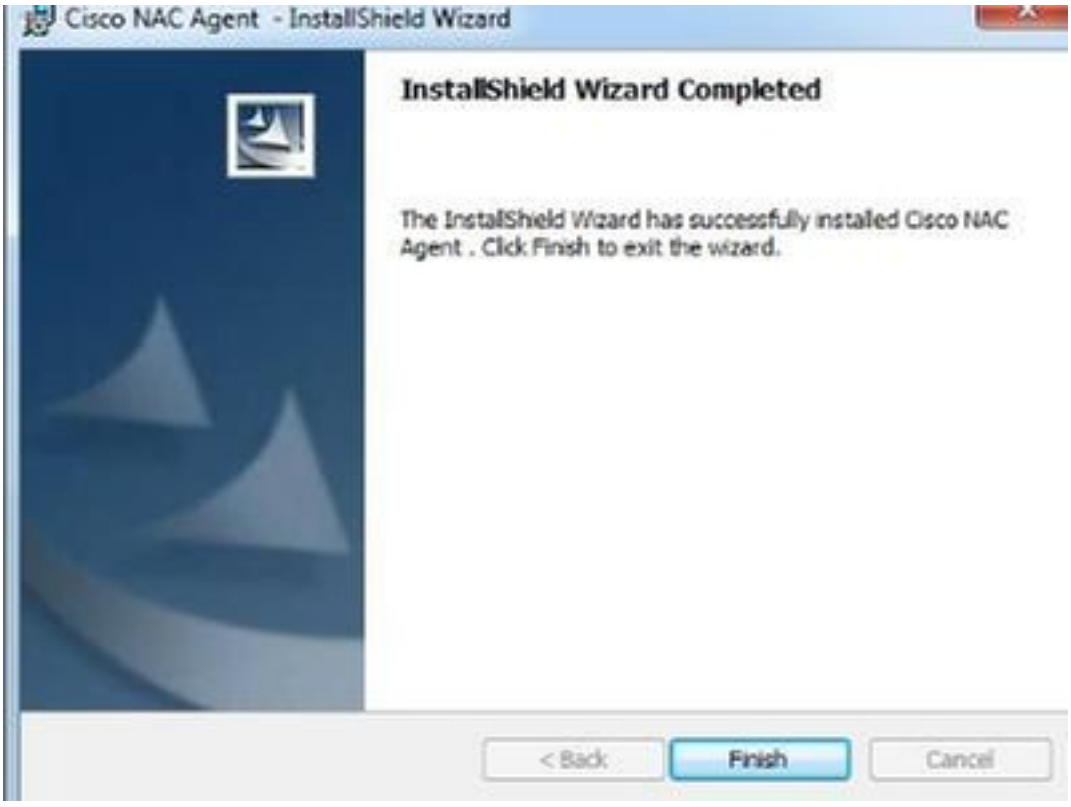
4. Cliquez sur **Next** (Suivant).

5. Le clic **I reçoivent les termes du contrat de licence**, et cliquent sur Next.

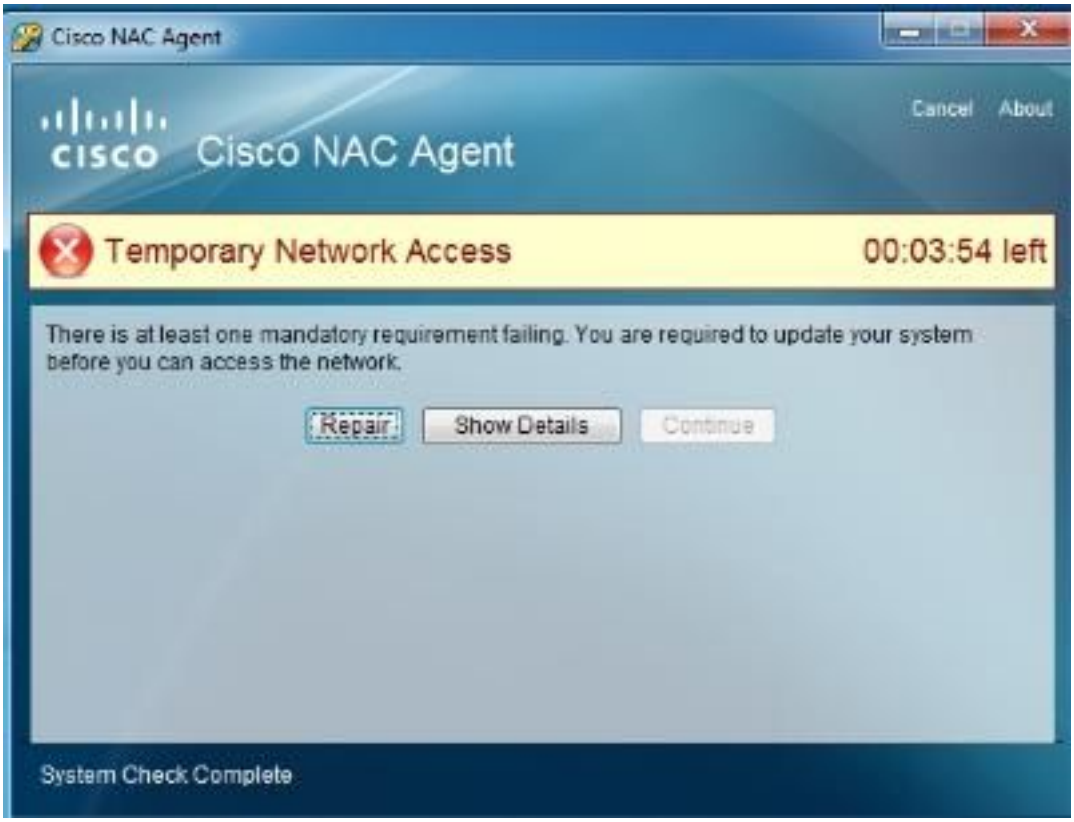
6. Cliquez sur **complet**, et cliquez sur Next.

7. Cliquez sur **Install**.

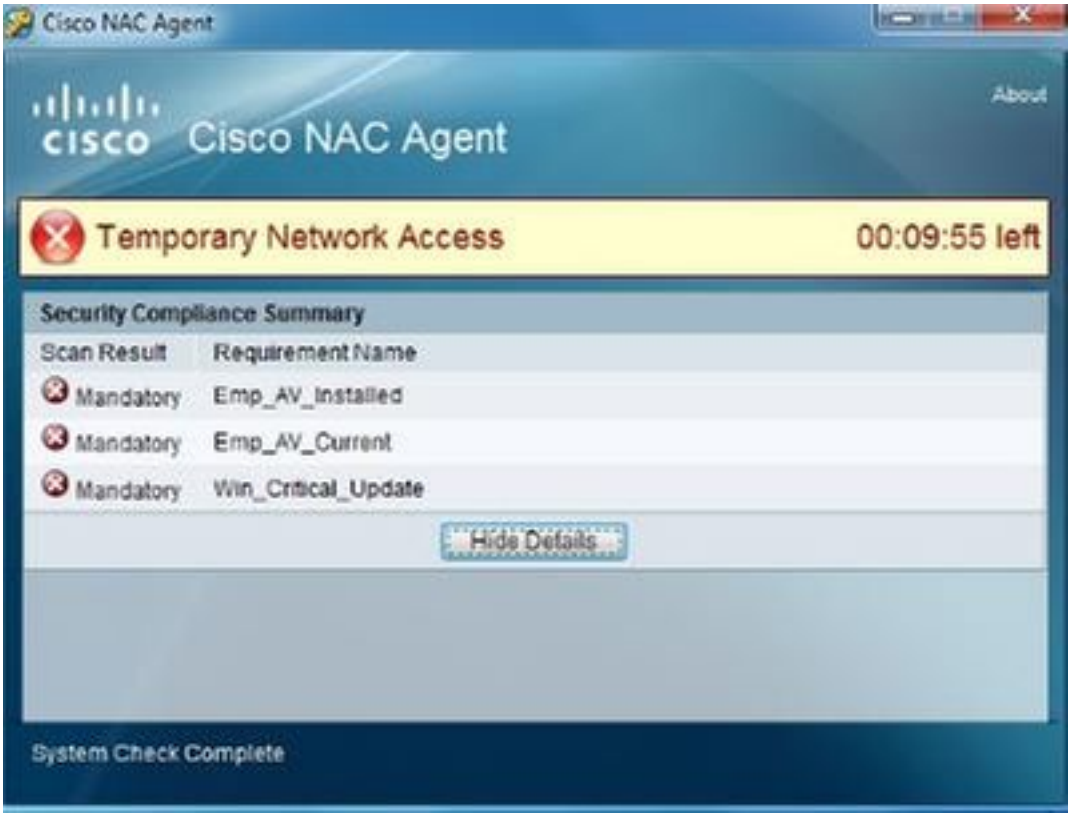
8. Sélectionnez la **finition**.



9. Une fois que l'installation est complète, l'agent NAC s'affiche. **Détails d'exposition de** clic.



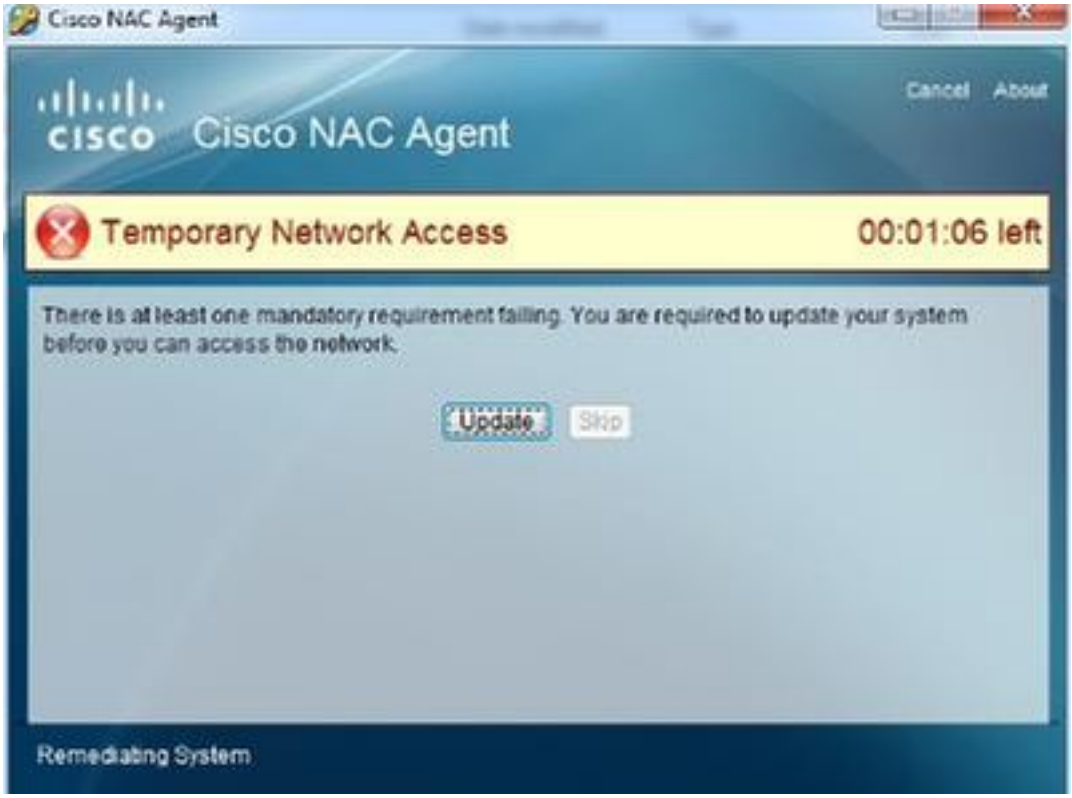
La sortie prouve que ClamWin n'est pas installé et n'est pas mise à jour. Quelques mises à jour essentielles de Windows ne sont pas installées.



10. Cliquez sur Go **pour joindre** afin d'installer l'antivirus du serveur de correction.

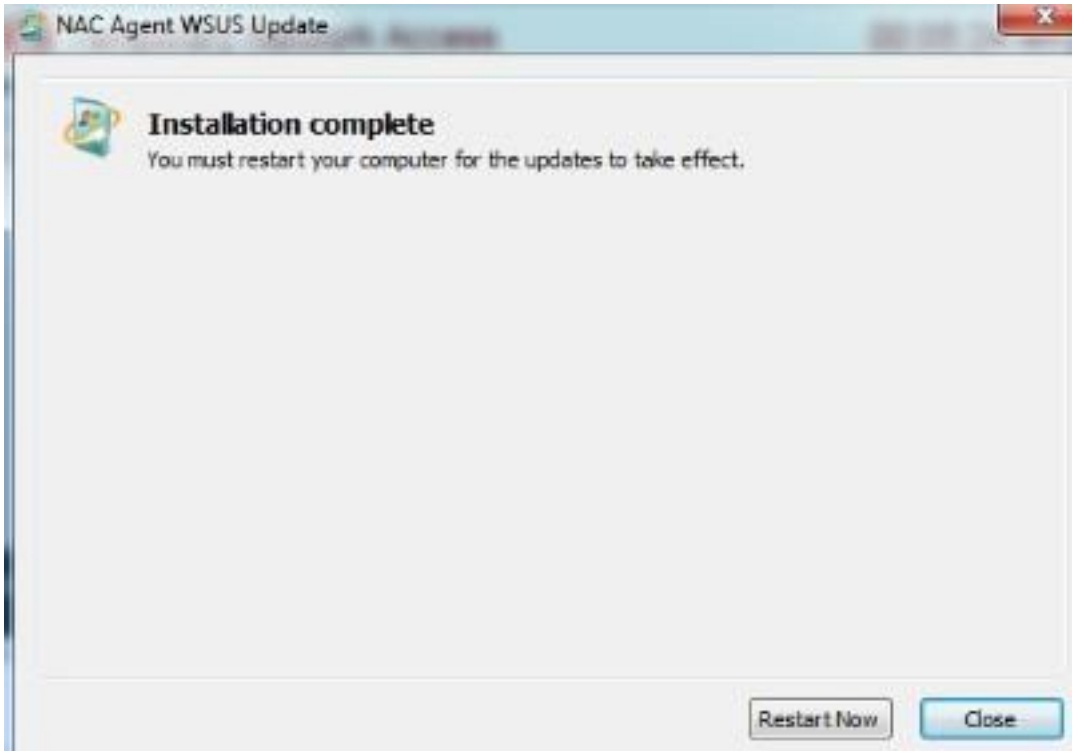
11. Cliquez sur Run, et procédez à l'installation de ClamWin poids du commerce.

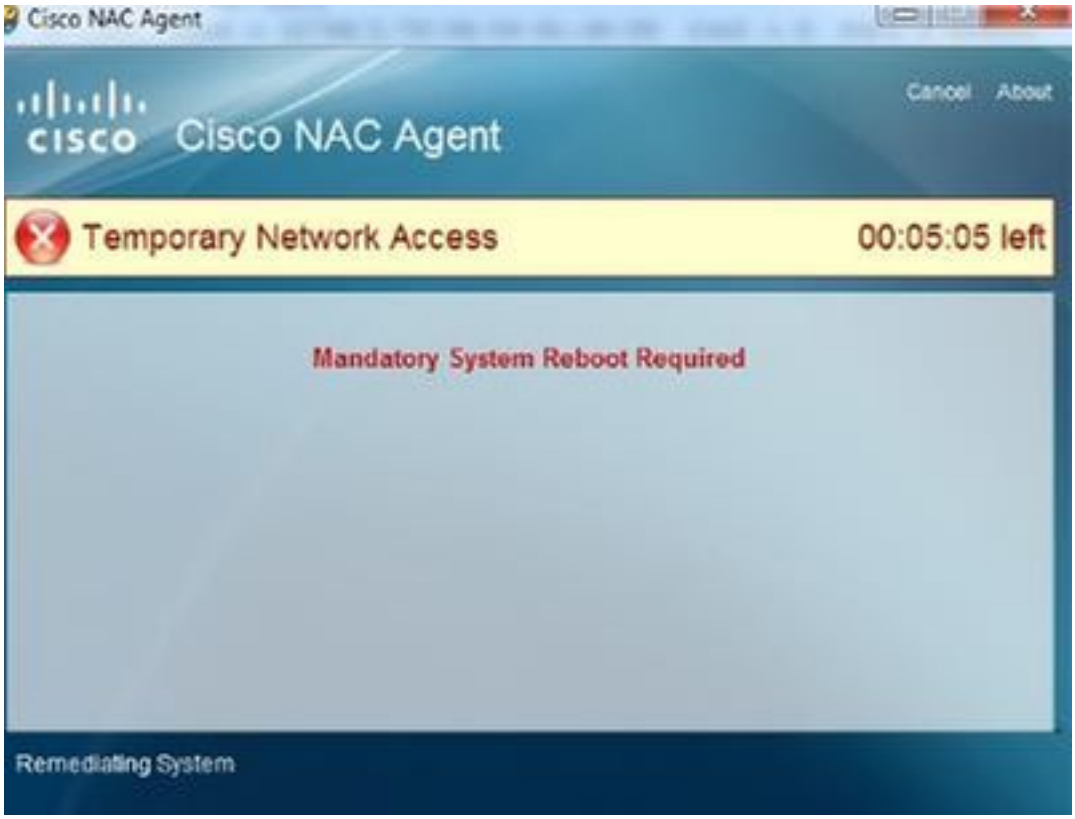
12. Après que l'antivirus soit installé, l'agent NAC incite pour des mises à jour. **Mise à jour de** clic afin d'obtenir le dernier fichier de définition de virus. Quand le même écran est présenté une deuxième fois, cliquez sur la **mise à jour** de nouveau afin d'installer les mises à jour de Windows.



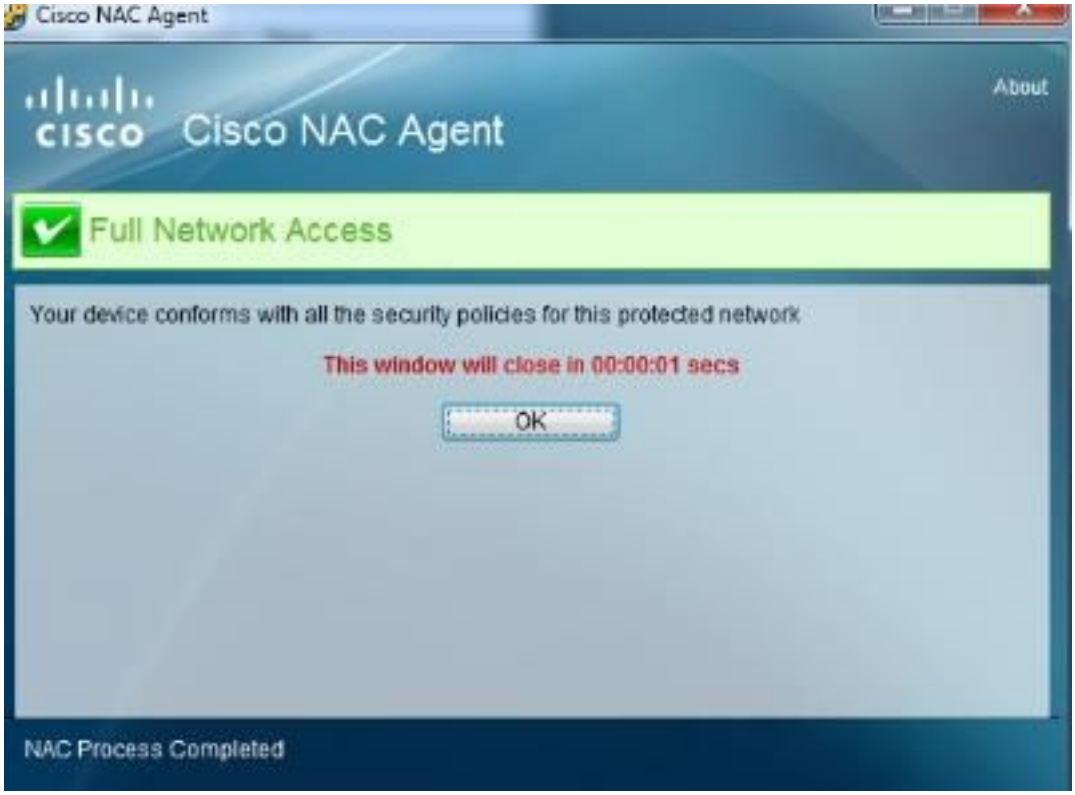
L'agent NAC entre en contact avec votre WSUS afin de vérifier et installer les dernières mises à jour essentielles.

13. **Reprise de** clic **maintenant** afin de se terminer la mise à jour.





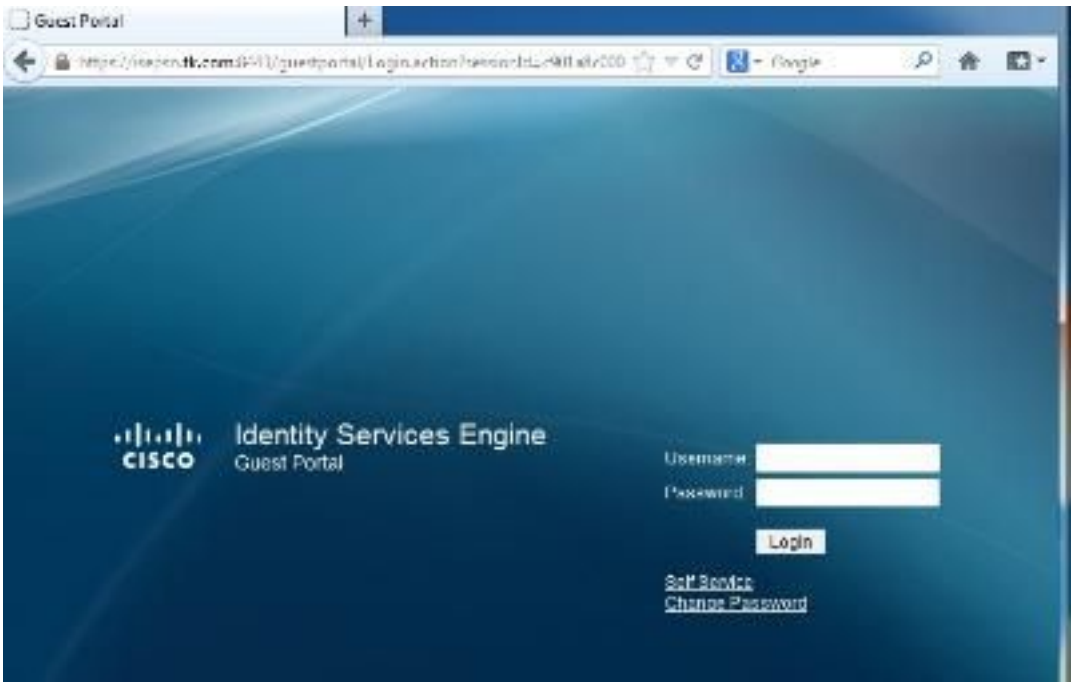
14. Après que la reprise, le système soit conforme.



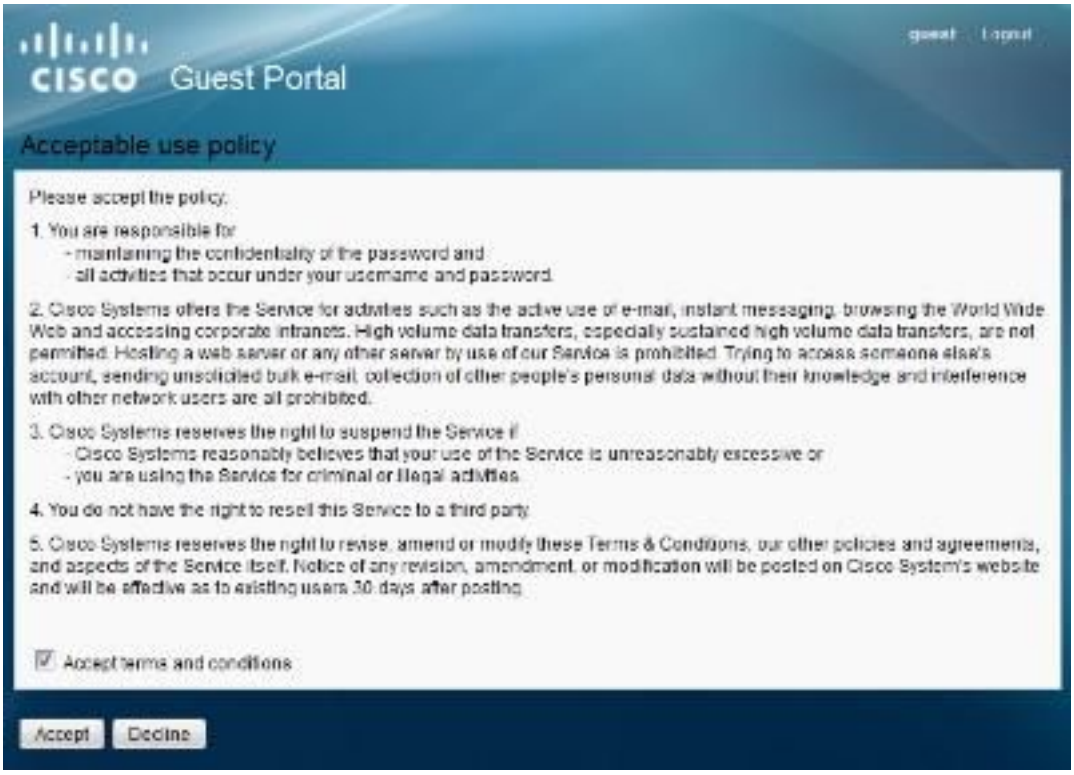
Posture de l'invité CWA (agent de Web NAC)

C'est la procédure que les utilisateurs exécutent, une fois qu'ils se connectent à l'invité SSID à la posture activée.

1. Connectez à votre invité SSID, ou ne configurez pas le dot1x sur votre réseau câblé.
2. Ouvrez un navigateur, et l'essai pour naviguer vers un site.
3. Le navigateur est réorienté au portail d'invité.
4. Cliquez sur l'**enregistrement d'individu**, et procédez à l'authentification.



5. Le clic **reçoivent** afin de recevoir l'AUP.

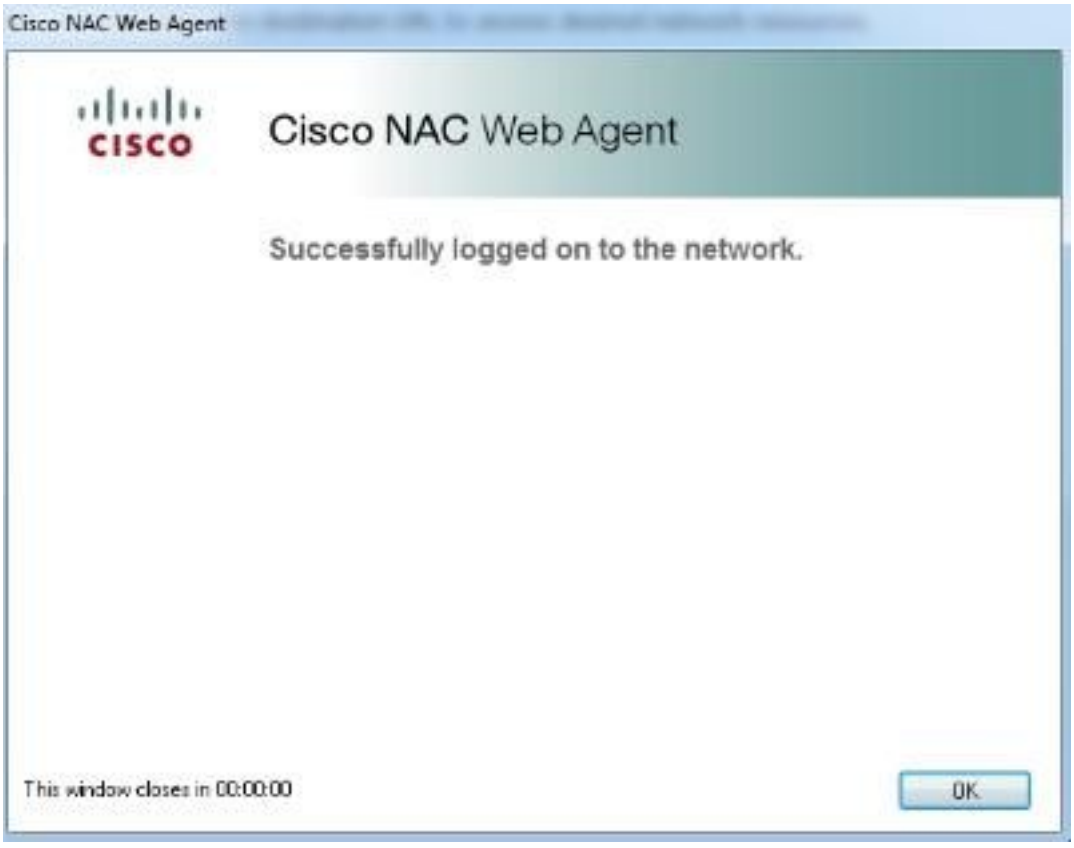


6. Sélectionnez le **clic pour installer l'agent**.

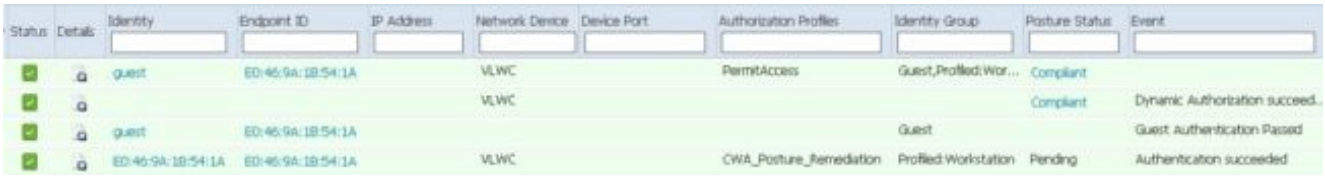
7. Le clic **a cliquez ici au remediate**.

8. Cliquez sur Run, et procédez à l'installation d'antivirus.

Le PC s'avère maintenant conforme.



9. Vérifiez la commande de logins d'authentification ISE pour vérifier que l'autorisation dynamique a réussi et que vous êtes assortie le profil d'autorisation avez rapporté à l'état conforme.



Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event
✓		guest	E0:46:9A:1B:54:1A		VLWC		PermitAccess	Guest,Profiled:Wor...	Compliant	
✓					VLWC				Compliant	Dynamic Authorization succeed...
✓		guest	E0:46:9A:1B:54:1A					Guest		Guest Authentication Passed
✓		E0:46:9A:1B:54:1A	E0:46:9A:1B:54:1A		VLWC		CWA_Posture_Remediation	Profiled:Workstation	Pending	Authentication succeeded

Forum aux questions

Options de déploiement autres que le ravitaillement de client

Référez-vous au guide de l'utilisateur de Logiciel Cisco Identity Services Engine, version 1.1x : Machines cliente de ravitaillement avec le MSI Installer d'agent de Cisco NAC.

Hôte de détection pour l'agent NAC

L'agent NAC atteint le bon point de décision politique ISE (PDP) dans différentes manières, selon si l'hôte de détection est défini :

1. Si aucun hôte de détection n'est défini : L'agent NAC envoie la demande de HTTP sur le port 80 à la passerelle ; ce trafic doit être réorienté au lien de détection de posture (CPP) pour que la détection fonctionne correctement.
2. Si un hôte de détection est défini : L'agent NAC envoie la demande de HTTP sur le port 80 à l'hôte ; ce trafic doit être réorienté au lien de détection de posture (CPP) pour que la détection fonctionne correctement. S'il y a un problème avec la redirection, les essais d'agent NAC pour entrer en contact avec directement l'hôte de détection ont défini sur le port 8905 ; la validation de posture n'est pas garantie, parce que les informations de session peuvent ne pas être disponibles sur ce PDP à moins que des groupes de noeud soient définis, et le PDP est dans le même groupe.
3. Si l'hôte de détection ne peut pas être atteint du tout, l'agent NAC retombe à la méthode 1, essaye ainsi d'entrer en contact avec la passerelle par défaut.

Choisissant l'hôte de détection, on devrait prendre en compte, qui le trafic initial de l'agent NAC vers l'hôte de détection devrait être visible au PDP. Ainsi, les bons choix ont pu être : Adresse PDP elle-même, hôte inexistant dans le même sous-réseau que des Noeuds PDP.

Des navigateurs des employés sont configurés avec le proxy

1. Si vous n'utilisez pas le ravitaillement de client et les PC des employés sont configurés avec le proxy, il n'y a aucun besoin de modifications puisque les paquets de détection de posture sont envoyés sur le port 80 et sautent les paramètres de proxy.
2. Si vous utilisez le service de ravitaillement de client, apportez ces modifications à la configuration de commutateur et au WLC afin d'intercepter le trafic http sur le port défini du proxy (ici 8080 dans cet exemple) si le proxy n'est pas sur le port 80.

   - Configuration de proxy sur le port 8080 sur le commutateur :

```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
```

```
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab

switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

- Configuration de proxy WLC. Par défaut, le WLC intercepte des demandes de HTTP avec le port TCP 80 de destination seulement. Cette commande doit être configurée par l'interface de ligne de commande (CLI) si vous voulez intercepter l'autre trafic http sur le port 8080 :

```
switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS
earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab
```

Note: Les Commutateurs permettent la redirection sur un port. Par conséquent, si vous spécifiez un autre port pour la redirection de commutateur, la détection de posture échoue, et le trafic de posture est envoyé à l'hôte de détection défini dans le NACAgentCFG.xml (le profil d'agent NAC).

ACL de dACL et de redirection

L'ACL de redirection est obligatoire pour le ravitaillement de client, l'authentification Web centrale, et la détection de posture. Cependant, le dACL est utilisé afin de limiter l'accès au réseau et est appliqué seulement au trafic non-réorienté.

Afin de résoudre cette situation, vous pouvez :

1. Définissez seulement un ACL de redirection, et réorientez tout le trafic que vous voulez être

lâché (comme fait dans l'exemple).
2. Définissez un ACL de redirection qui est moins restrictif, et appliquez un dACL qui filtre le trafic qui n'est pas réorienté.
3. Définissez un ACL de redirection, et appliquez un VLAN qui limite l'accès au réseau. C'est la meilleure approche parce que le trafic VLAN peut être filtré par un Pare-feu application-averti.

L'agent NAC ne s'affiche pas

1. Le contrôle ISE vivent authentification, et vérifient que l'authentification apparie votre profil d'autorisation de posture.
2. Du PC client, ouvrez le cmd. Tapez le **nslookup**, et vérifiez-vous peut résoudre l'adresse Internet ISE PDP.
3. De votre navigateur de client, ise-*adresse Internet de* **https:// de** type **: 8905/auth/discovery**, et vous veillent pour recevoir le FQDN ISE comme réponse.

Si toutes ces étapes sont réussies et si votre commutateur ou configuration WLC est conforme à ce document, vos étapes suivantes devraient être :

- Employez Wireshark afin de commencer une capture sur le PC.
- Service d'agent de la reprise NAC.
- Collectez le réalisateur de log de Cisco.
- Localisez NACAgentCFG.xml dans le répertoire d'agent NAC.

Contactez Cisco TAC une fois que vous avez recueilli la capture de paquet, des logs d'agent NAC, fichier de configuration de NACAgentCFG, et visualisateur d'événements de Windows se connecte.

Incapable d'accéder à WSUS pour la correction

Si vous utilisez WSUS 3.0 SP2 et l'agent NAC ne peut pas accéder à des mises à jour WSUS Windows, vérifiez que vous avez le dernier correctif de WSUS installé. Ce correctif est obligatoire pour des clients Windows afin de parcourir des mises à jour de WSUS.

Vérifiez que vous pouvez accéder à ce fichier : *wsus* **/selfupdate/iuident.cab d'***IP de* **http://**.

Référez-vous au guide SP2 pas à pas des services 3.0 de mise à jour de Windows Server pour information les informations complémentaires.

N'ayez pas un WSUS géré interne

Vous pouvez encore utiliser des serveurs de Windows Update tandis que vous configurez votre règle de correction de posture.

On doit permettre au client pour accéder à ces sites, ainsi ces l'URLs ne doit pas être réorienté :

- http://windowsupdate.microsoft.com
- http://*.windowsupdate.microsoft.com
- https://*.windowsupdate.microsoft.com
- http://*.update.microsoft.com
- https://*.update.microsoft.com

- http://*.windowsupdate.com
- http://download.windowsupdate.com
- http://*.download.windowsupdate.com
- http://wustat.windows.com
- http://ntservicepack.microsoft.com
- http://stats.microsoft.com
- https://stats.microsoft.com

Aucune authentification défaillante vue dans ISE ne vivent des logs

Vous pourriez être tenté pour créer une règle de stratégie d'autorisation que des déclencheurs sur l'état d'un client noncompliant afin de limiter l'accès. Cependant, vous ne verrez pas que la tentative d'authentification échoue jusqu'à ce que le temporisateur de correction expire, particulièrement quand vous utilisez l'agent de Web. En fait, l'agent note l'insoumission et met en marche le temporisateur de correction.

On annonce L'ISE que la posture était une panne seulement quand le temporisateur de correction expire ou les clics d'utilisateur **s'annulent**. Par conséquent, l'il est conseillé de donnent un accès par défaut à tous les clients qui tient compte de la correction mais bloquent n'importe quelle autre forme de l'accès.

Vérifiez

Quelques procédures de vérification sont incluses dans les sections précédentes.

Dépanner

Quelques procédures de dépannage sont incluses dans les sections précédentes.