

# Posture de la version 9.2.1 VPN ASA avec exemple de configuration de l'ISE

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme et flux du trafic du réseau](#)

[Configurations](#)

[ASA](#)

[ISE](#)

[Réévaluation Périodique](#)

[Vérifier](#)

[Dépannage](#)

[Débogages sur l'ISE](#)

[Débogages sur l'ASA](#)

[Débogages pour l'agent](#)

[Défaillance de la posture agent NAC](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment configurer l'appareil de sécurité adaptatif (ASA) Cisco version 9.2.1 afin de positionner les utilisateurs VPN par rapport à Cisco Identity Services Engine (ISE) sans avoir besoin d'un noeud de positionnement en ligne (IPN).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de la configuration CLI ASA et de la configuration VPN SSL (Secure Socket Layer)
- Connaissance de base de la configuration VPN d'accès à distance sur l'ASA

- Connaissances de base sur ISE et les services de posture

## Composants utilisés

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

- Logiciel Cisco ASA versions 9.2.1 et ultérieures
- Microsoft Windows version 7 avec Cisco AnyConnect Secure Mobility Client version 3.1
- Cisco ISE version 1.2 avec correctif 5 ou ultérieur

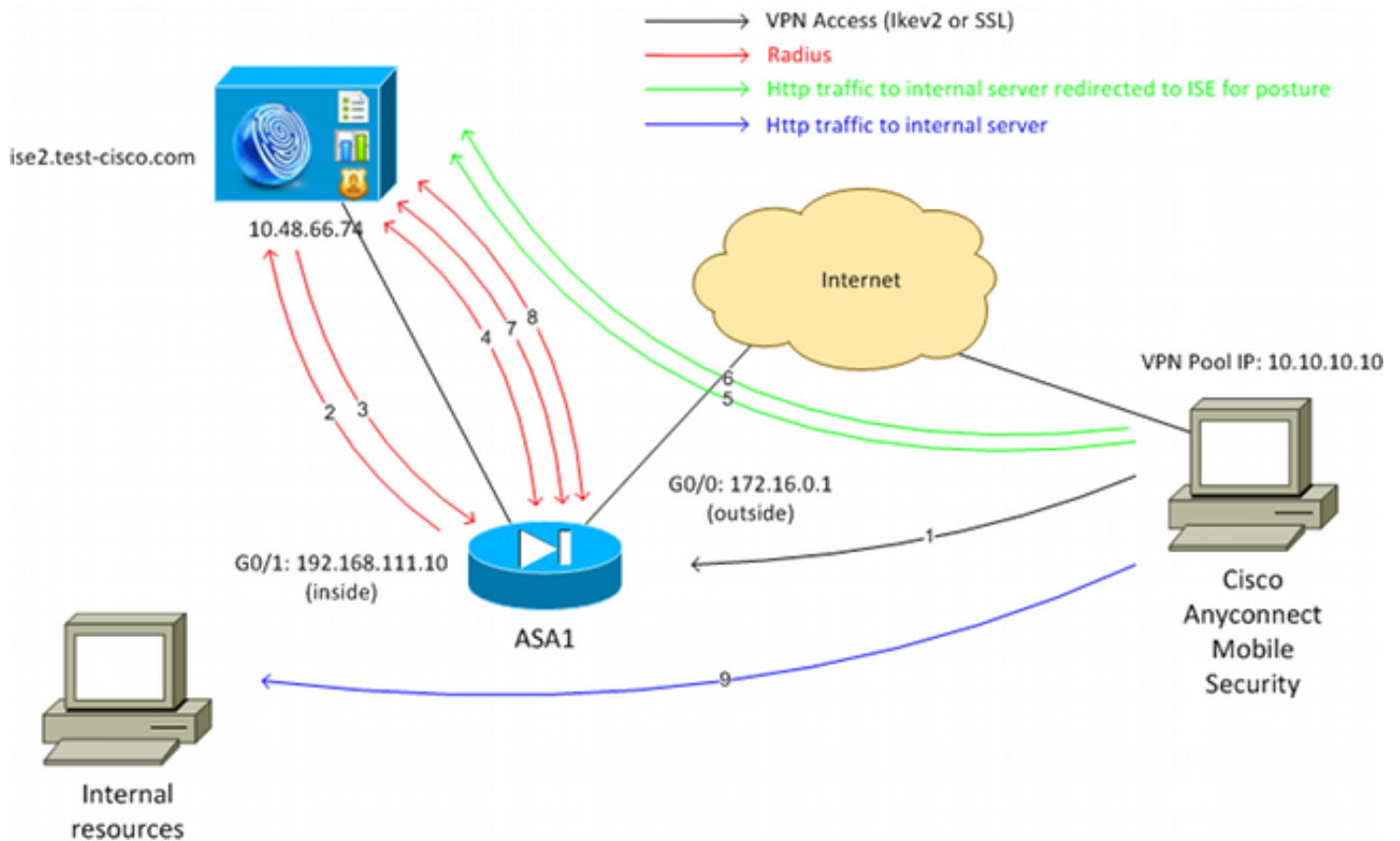
## Informations générales

La version 9.2.1 de Cisco ASA prend en charge le changement d'autorisation RADIUS (RFC 5176). Cela permet de positionner les utilisateurs VPN par rapport à Cisco ISE sans avoir besoin d'un IPN. Une fois qu'un utilisateur VPN se connecte, l'ASA redirige le trafic Web vers l'ISE, où l'utilisateur dispose d'un agent NAC (Network Admission Control) ou d'un agent Web. L'agent effectue des contrôles spécifiques sur la machine utilisateur afin de déterminer sa conformité par rapport à un ensemble configuré de règles de posture, telles que le système d'exploitation (OS), les correctifs, l'antivirus, le service, l'application ou les règles du registre.

Les résultats de la validation de posture sont ensuite envoyés à l'ISE. Si la machine est considérée comme conforme, alors l'ISE peut envoyer un RADIUS CoA à l'ASA avec le nouvel ensemble de politiques d'autorisation. Une fois la validation de la position et la CoA réussies, l'utilisateur est autorisé à accéder aux ressources internes.

## Configurer

### Diagramme et flux du trafic du réseau



Voici le flux de trafic, comme illustré dans le schéma du réseau :

1. L'utilisateur distant utilise Cisco Anyconnect pour l'accès VPN à l'ASA.
2. L'ASA envoie une requête d'accès RADIUS pour cet utilisateur à l'ISE.
3. Cette demande atteint la stratégie nommée **ASA92-posture** sur l'ISE. Par conséquent, le profil d'autorisation de **posture ASA92** est renvoyé. L'ISE envoie un message d'acceptation d'accès RADIUS avec deux paires attribut-valeur Cisco :

**url-redirect-acl=redirect** - il s'agit du nom de la liste de contrôle d'accès (ACL) qui est définie localement sur l'ASA, qui décide du trafic qui doit être redirigé.

**url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp** - il s'agit de l'URL vers laquelle l'utilisateur distant doit être redirigé. **Conseil** : les serveurs DNS (Domain Name System) affectés aux clients VPN doivent être en mesure de résoudre le nom de domaine complet (FQDN) renvoyé dans l'URL de redirection. Si les filtres VPN sont configurés afin de restreindre l'accès au niveau du groupe de tunnels, assurez-vous que le pool client est en mesure d'accéder au serveur ISE sur le port configuré (**TCP 8443** dans cet exemple).

4. L'ASA envoie un paquet de démarrage de demande de compte RADIUS et reçoit une réponse. Cela est nécessaire pour envoyer tous les détails relatifs à la session à l'ISE. Ces détails incluent l'ID de session, l'adresse IP externe du client VPN et l'adresse IP de l'ASA. L'ISE utilise l'ID de session afin d'identifier cette session. L'ASA envoie également des informations de compte intermédiaires périodiques, où l'attribut le plus important est l'adresse IP tramée avec l'adresse IP qui est attribuée au client par l'ASA (**10.10.10.10** dans

cet exemple).

5. Lorsque le trafic de l'utilisateur VPN correspond à la liste de contrôle d'accès définie localement (redirection), il est redirigé vers <https://ise2.test-cisco.com:8443>. En fonction de la configuration, l'ISE provisionne l'agent NAC ou l'agent Web.
6. Une fois l'agent installé sur l'ordinateur client, il effectue automatiquement des vérifications spécifiques. Dans cet exemple, il recherche le fichier `c:\test.txt`. Il envoie également un rapport de position à l'ISE, qui peut inclure plusieurs échanges avec l'utilisation du protocole SWISS et des ports TCP/UDP 8905 afin d'accéder à l'ISE.
7. Lorsque l'ISE reçoit le rapport de position de l'agent, il traite à nouveau les règles d'autorisation. Cette fois, le résultat de la posture est connu et une autre règle est atteinte. Il envoie un paquet RADIUS CoA :

Si l'utilisateur est conforme, un nom de liste de contrôle d'accès téléchargeable (DACL) autorisant un accès complet est envoyé (conforme à la règle AuthZ ASA92).

Si l'utilisateur n'est pas conforme, un nom DACL autorisant un accès limité est envoyé (règle AuthZ ASA92 non conforme). **Remarque** : RADIUS CoA est toujours confirmé, c'est-à-dire que l'ASA envoie une réponse à l'ISE afin de confirmer.

8. ASA supprime la redirection. Si les listes de contrôle d'accès ne sont pas mises en cache, il doit envoyer une requête d'accès afin de les télécharger à partir de l'ISE. La liste de contrôle d'accès spécifique est attachée à la session VPN.
9. La prochaine fois que l'utilisateur VPN essaiera d'accéder à la page Web, il pourra accéder à toutes les ressources autorisées par la liste de contrôle d'accès d'ASA.  
Si l'utilisateur n'est pas conforme, seul un accès limité lui est accordé.  
**Remarque** : ce modèle de flux diffère de la plupart des scénarios qui utilisent RADIUS CoA. Pour les authentifications 802.1x filaires/sans fil, RADIUS CoA n'inclut aucun attribut. Elle déclenche uniquement la deuxième authentification dans laquelle tous les attributs, tels que DACL, sont associés. Pour la posture VPN ASA, il n'y a pas de deuxième authentification. Tous les attributs sont renvoyés dans la CoA RADIUS. La session VPN est active et il n'est pas possible de modifier la plupart des paramètres utilisateur VPN.

## Configurations

Utilisez cette section afin de configurer l'ASA et l'ISE.

### ASA

Voici la configuration ASA de base pour l'accès Cisco AnyConnect :

```
ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0
```

```
interface GigabitEthernet0/0  
nameif outside
```

```

security-level 0
ip address xxxx 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.111.10 255.255.255.0

aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.48.66.74
key cisco

webvpn
enable outside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
anyconnect enable
tunnel-group-list enable

group-policy GP-SSL internal
group-policy GP-SSL attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
address-pool POOL
authentication-server-group ISE
default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
group-alias RA enable

```

Pour l'intégration d'ASA avec la position ISE, assurez-vous que vous :

- Configurez le serveur AAA (Authentication, Authorization, and Accounting) pour l'autorisation dynamique afin d'accepter CoA.
- Configurez la gestion des comptes en tant que groupe de tunnels afin d'envoyer les détails de la session VPN vers l'ISE.
- Configurez la comptabilité intermédiaire qui enverra l'adresse IP attribuée à l'utilisateur et mettez régulièrement à jour l'état de la session sur ISE
- Configurez la liste de contrôle d'accès de redirection, qui décide si le trafic DNS et ISE est autorisé. Tous les autres trafics HTTP sont redirigés vers l'ISE pour la posture.

Voici l'exemple de configuration :

```

access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www

aaa-server ISE protocol radius
authorize-only
interim-accounting-update periodic 1
dynamic-authorization
aaa-server ISE (inside) host 10.48.66.74
key cisco

tunnel-group RA general-attributes

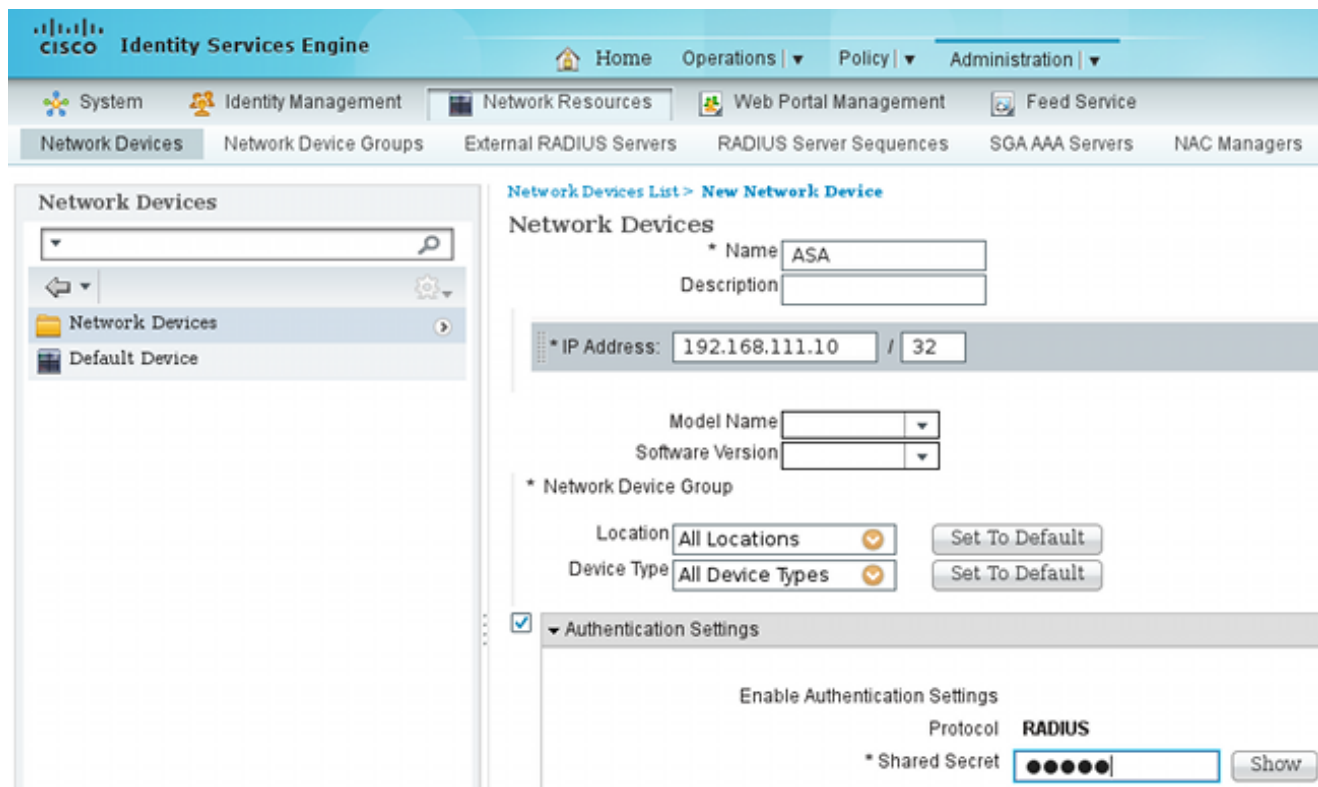
```

address-pool POOL  
authentication-server-group ISE  
**accounting-server-group ISE**  
default-group-policy GP-SSL

## ISE

Complétez ces étapes afin de configurer l'ISE :

1. Accédez à **Administration > Network Resources > Network Devices** et ajoutez l'ASA en tant que périphérique réseau :



The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The main menu shows 'System', 'Identity Management', 'Network Resources', 'Web Portal Management', and 'Feed Service'. Under 'Network Resources', the 'Network Devices' tab is selected, showing a list of 'Network Devices', 'Network Device Groups', 'External RADIUS Servers', 'RADIUS Server Sequences', 'SGA AAA Servers', and 'NAC Managers'. The 'Network Devices' list is expanded to show 'Network Devices' and 'Default Device'. The main content area is titled 'Network Devices List > New Network Device' and contains the following configuration fields:

- Name:** ASA
- Description:** (empty)
- IP Address:** 192.168.111.10 / 32
- Model Name:** (dropdown menu)
- Software Version:** (dropdown menu)
- Network Device Group:**
  - Location:** All Locations (dropdown menu) with a 'Set To Default' button.
  - Device Type:** All Device Types (dropdown menu) with a 'Set To Default' button.
- Authentication Settings:** (checked)
  - Enable Authentication Settings:** (checked)
  - Protocol:** RADIUS
  - \* Shared Secret:** (masked with dots) with a 'Show' button.

2. Accédez à **Policy > Results > Authorization > Downloadable ACL** et configurez la DACL de sorte qu'elle autorise un accès complet. La configuration de liste de contrôle d'accès par défaut autorise tout le trafic IP sur ISE :

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. At the top, the navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, a secondary menu shows 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Security Group Access'. The 'Results' tab is selected in the main navigation. On the left, a tree view shows the configuration hierarchy, with 'Downloadable ACLs' highlighted. The main content area shows the configuration for a specific Downloadable ACL named 'PERMIT\_ALL\_TRAFFIC'. The description is 'Allow all Traffic'. The DACL content is shown in a table with 10 rows, where the first row contains the command '1 permit ip any any'. A 'Check DACL Syntax' button is located at the bottom of the configuration area.

3. Configurez une liste de contrôle d'accès similaire qui fournit un accès limité (pour les utilisateurs non conformes).
4. Accédez à **Policy > Results > Authorization > Authorization Profiles** et configurez le profil d'autorisation nommé **ASA92-posture**, qui redirige les utilisateurs vers posture. Cochez la case **Web Redirection**, sélectionnez **Client Provisioning** dans la liste déroulante, et assurez-vous que la **redirection** apparaît dans le champ ACL (que l'ACL est définie localement sur l'ASA) :

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Security Group Access'. The 'Results' tab is active. On the left, a tree view shows the configuration hierarchy: Authentication, Authorization, Authorization Profiles, Downloadable ACLs, Inline Posture Node Profiles, Profiling, Posture, Client Provisioning, and Security Group Access. The main configuration area is titled 'Authorization Profile' and shows the following settings:

- \* Name: ASA92-posture
- Description: (empty)
- \* Access Type: ACCESS\_ACCEPT
- Service Template:
- Common Tasks:
  - Voice Domain Permission
  - Web Redirection (CWA, DRW, MDM, NSP, CPP)
- Client Provisioning (Posture): (dropdown menu)
- ACL: redirect
- Static IP/Host name

- Configurez le profil d'autorisation nommé **ASA92-compliance**, qui ne doit retourner que la DACL nommée **PERMIT\_ALL\_TRAFFIC** qui fournit un accès complet pour les utilisateurs conformes :

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for an Authorization Profile named 'ASA92-compliant'. The navigation and tabs are the same as in the previous screenshot. The configuration area is titled 'Authorization Profile' and shows the following settings:

- \* Name: ASA92-compliant
- Description: (empty)
- \* Access Type: ACCESS\_ACCEPT
- Service Template:
- Common Tasks:
  - DACL Name: PERMIT\_ALL\_TRAFFIC

- Configurez un profil d'autorisation similaire nommé **ASA92-noncompliance**, qui devrait retourner la DACL avec un accès limité (pour les utilisateurs non conformes).

- Accédez à **Policy > Authorization** et configurez les règles d'autorisation :



Créez une règle qui autorise un accès complet si les résultats de la posture sont conformes. Il en résulte une politique d'autorisation **conforme à ASA92**.

Créez une règle qui autorise un accès limité si les résultats de la position ne sont pas conformes. Le résultat est la politique d'autorisation **ASA92-noncompliance**.

Assurez-vous que si aucune des deux règles précédentes n'est atteinte, alors la règle par défaut retourne la **posture ASA92**, qui force une redirection sur l'ASA.

<input checked="" type="checkbox"/>	ASA92 compliant	if Session:PostureStatus EQUALS Compliant	then ASA92-compliant
<input checked="" type="checkbox"/>	ASA92 non compliant	if Session:PostureStatus EQUALS NonCompliant	then ASA92-noncompliant
<input checked="" type="checkbox"/>	ASA92 redirect	if Radius:NAS-IP-Address EQUALS 192.168.111.10	then ASA92-posture

- Les règles d'authentification par défaut vérifient le nom d'utilisateur dans le magasin d'identités interne. Si cela doit être modifié (coché dans Active Directory (AD), par exemple), alors naviguez vers **Policy > Authentication** et faites la modification :

**Authentication Policy**

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use.

Policy Type  Simple  Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	: use Internal Endpoints	
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	: use Internal Users	
<input checked="" type="checkbox"/>	Default Rule (if no match)	: Allow Protocols : Default Network Access and use : Internal Users	

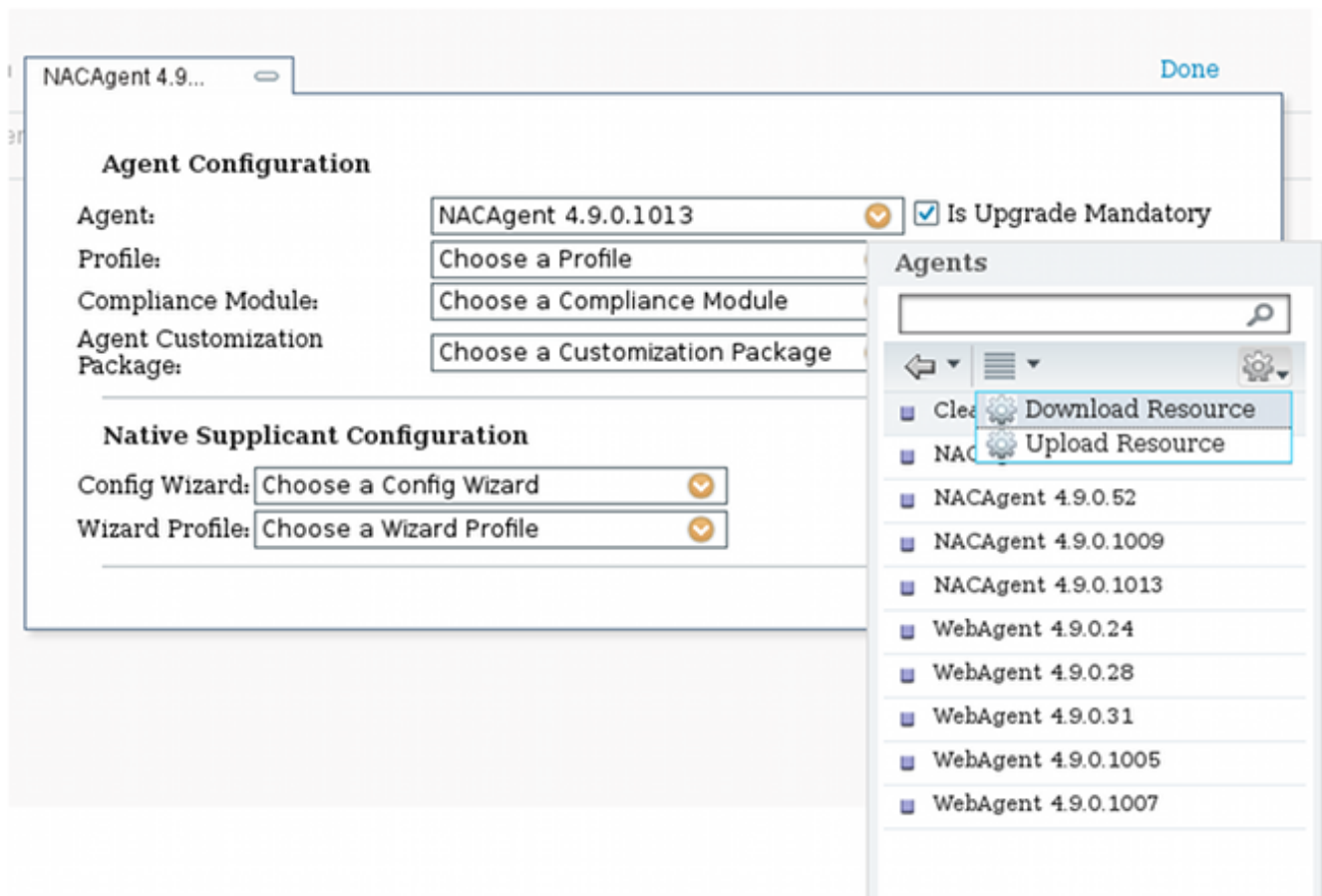
- Accédez à **Policy > Client Provisioning** et configurez les règles de provisioning. Il s'agit des règles qui déterminent le type d'agent à provisionner. Dans cet exemple, une seule règle simple existe et l'ISE sélectionne l'agent NAC pour tous les systèmes Microsoft Windows :

**Client Provisioning Policy**

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:  
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.  
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

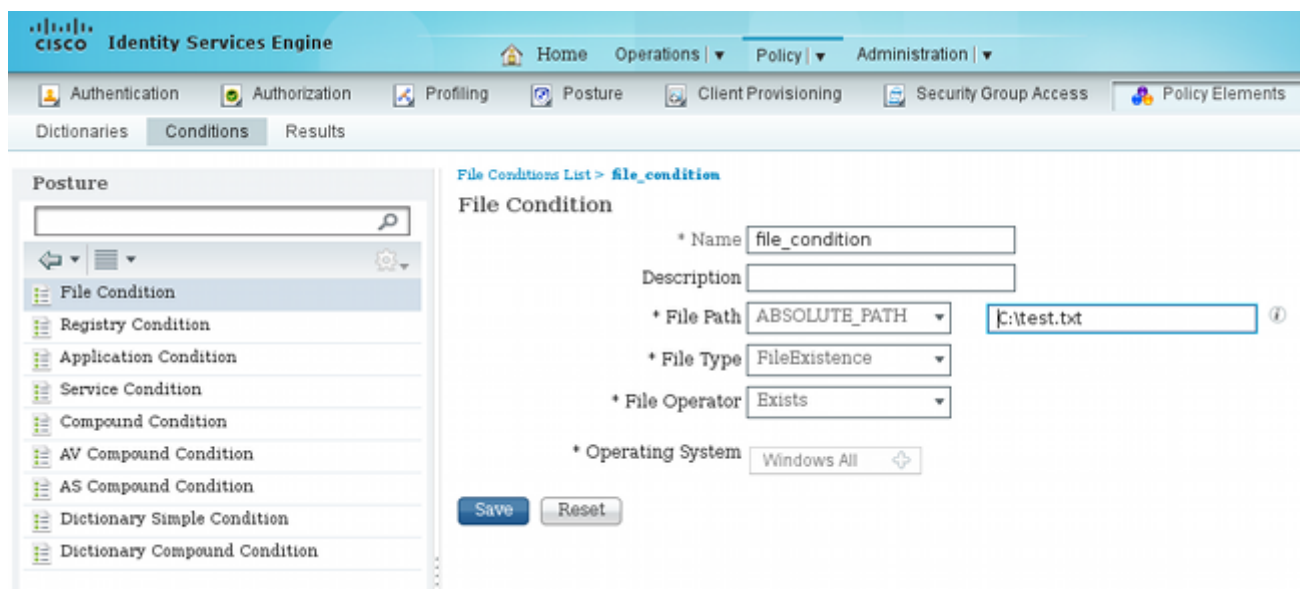
Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> ASA92-posture	if Any	and Windows All	and Condition(s)	then NACAgent 4.9.0.1013

Lorsque les agents ne sont pas sur l'ISE, il est possible de les télécharger :

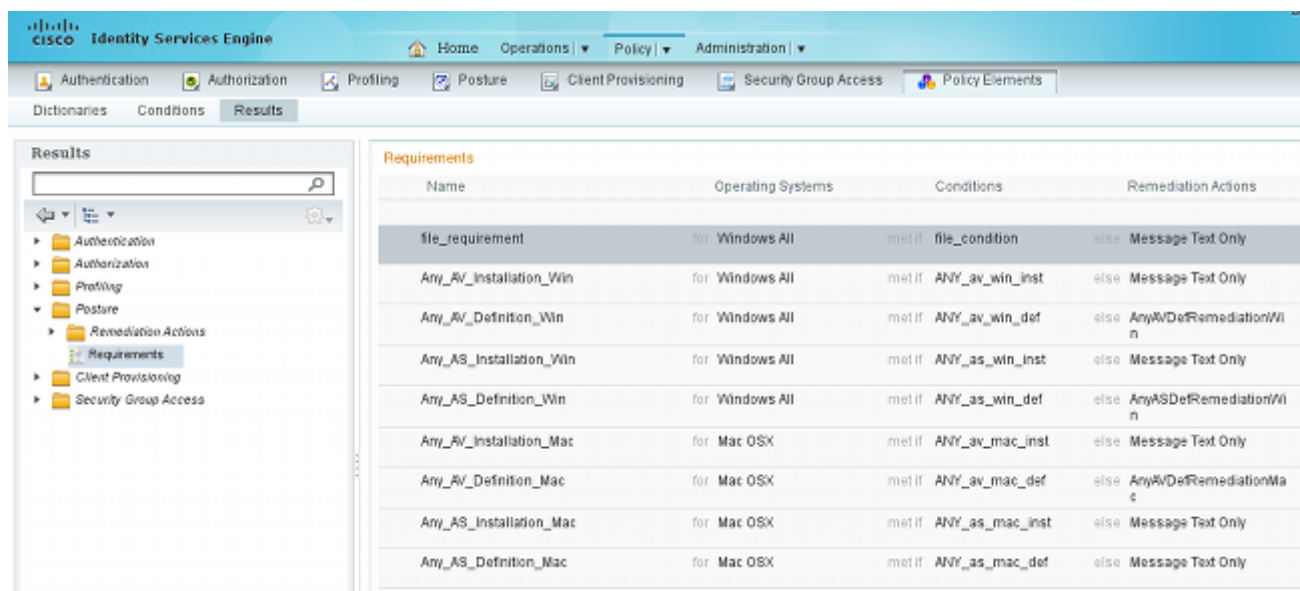


10. Si nécessaire, vous pouvez naviguer vers **Administration > System > Settings > Proxy** et configurer le proxy pour l'ISE (pour accéder à Internet).
11. Configurez les règles de posture, qui vérifient la configuration du client. Vous pouvez configurer des règles qui vérifient :
  - fichiers** - existence, version, date
  - Registre** - clé, valeur, existence
  - application** - nom du processus, en cours d'exécution, non en cours d'exécution
  - service** - nom du service, en cours d'exécution, non en cours d'exécution
  - antivirus** - plus de 100 fournisseurs pris en charge, version, lorsque les définitions sont mises à jour
  - logiciel anti-espion** - plus de 100 fournisseurs pris en charge, version, lorsque les définitions sont mises à jour
  - condition composée** - mélange de tous
  - conditions du dictionnaire personnalisé** - utilisation de la plupart des dictionnaires ISE
12. Dans cet exemple, seule une simple vérification de l'existence d'un fichier est effectuée. Si

le fichier **c:\test.txt** est présent sur l'ordinateur client, il est conforme et l'accès complet est autorisé. Accédez à **Policy > Conditions > File Conditions** et configurez la condition du fichier :

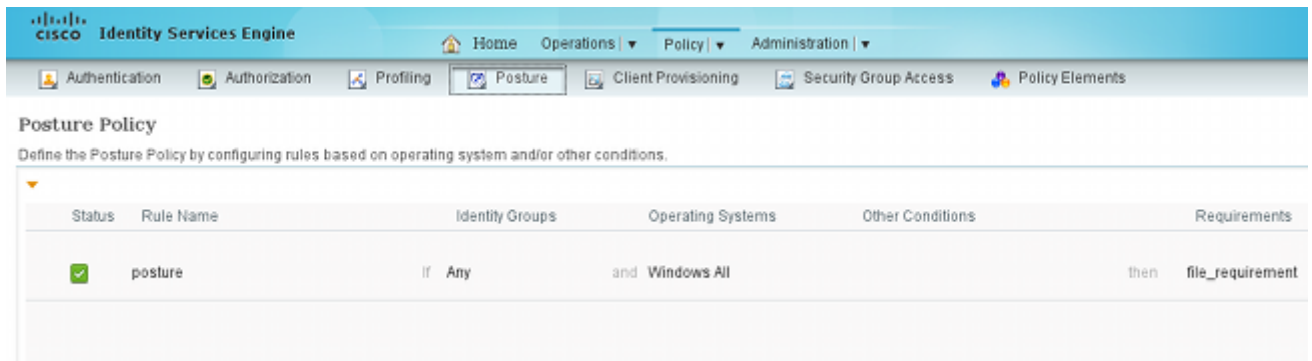


- Accédez à **Policy > Results > Posture > Requirements** et créez un besoin. Cette condition doit être remplie lorsque la condition précédente est remplie. Si ce n'est pas le cas, une action corrective est exécutée. De nombreux types d'actions correctives peuvent être disponibles, mais dans cet exemple, la plus simple est utilisée : un message spécifique s'affiche.



**Remarque** : dans un scénario normal, l'action de correction de fichier peut être utilisée (l'ISE fournit le fichier téléchargeable).

- Navigation jusqu'à **Policy > Posture** et utilisez la condition que vous avez créée à l'étape précédente (nommée **file\_requirements**) dans les règles de position. La seule règle de posture exige que tous les systèmes Microsoft Windows répondent à la **condition file\_requirements**. Si cette exigence est satisfaite, la station est conforme ; si elle ne l'est pas, la station n'est pas conforme.

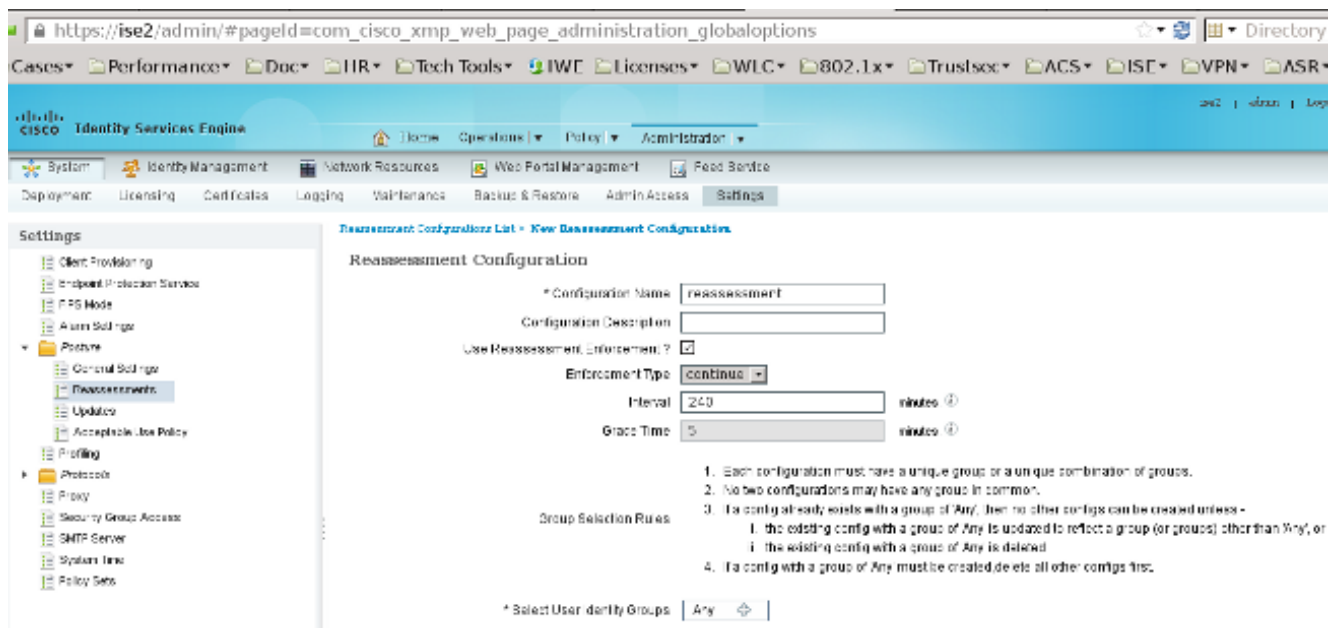


## Réévaluation Périodique

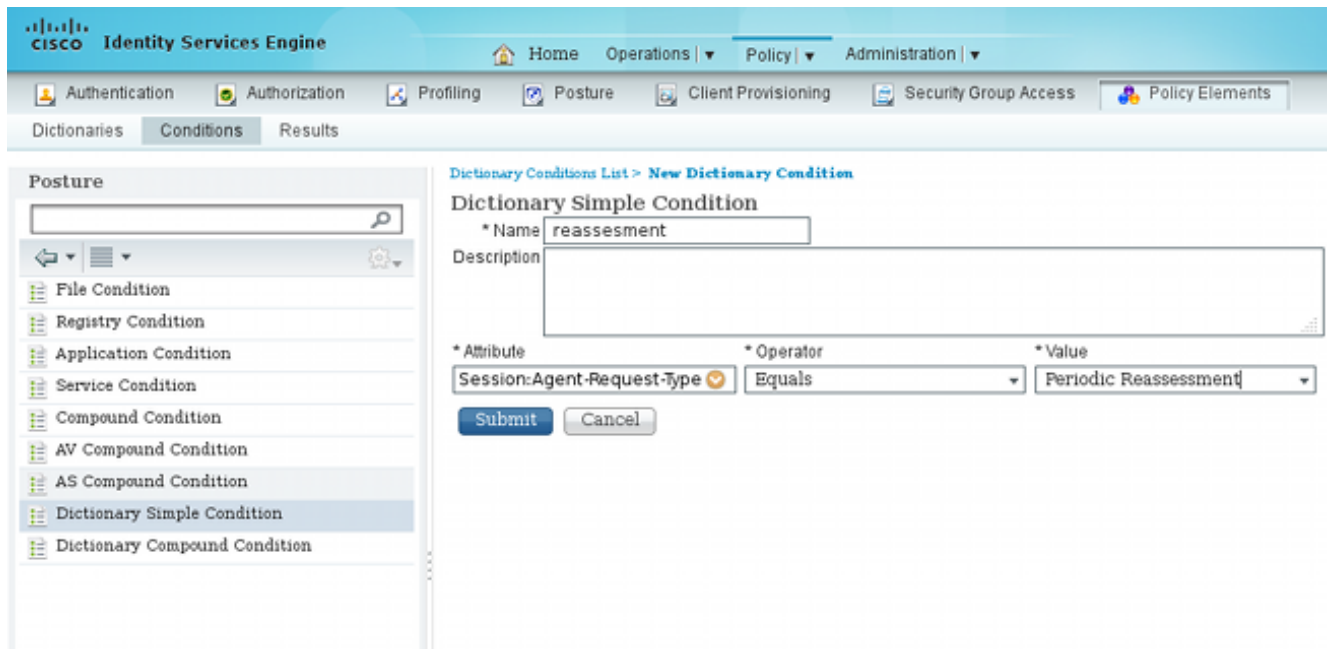
Par défaut, la posture est un événement ponctuel. Cependant, il est parfois nécessaire de vérifier périodiquement la conformité de l'utilisateur et d'ajuster l'accès aux ressources en fonction des résultats. Ces informations sont transmises via le protocole SWISS (NAC Agent) ou codées dans l'application (Web Agent).

Complétez ces étapes afin de vérifier la conformité de l'utilisateur :

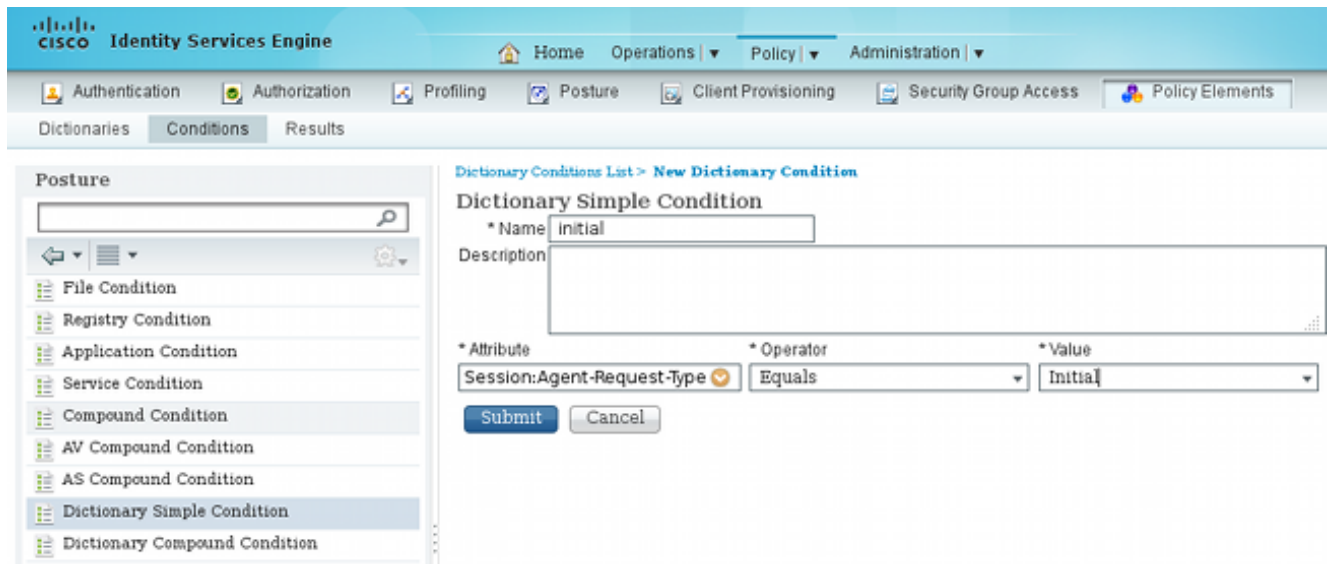
1. Accédez à **Administration > Settings > Posture > Reassessment** et activez la réévaluation globalement (par configuration de groupe d'identité) :



2. Créez une condition de posture qui correspond à toutes les réévaluations :



3. Créez une condition similaire qui correspond uniquement aux évaluations initiales :



Ces deux conditions peuvent être utilisées dans les règles de posture. La première règle correspond uniquement aux évaluations initiales et la seconde correspond à toutes les évaluations suivantes :

Posture Policy

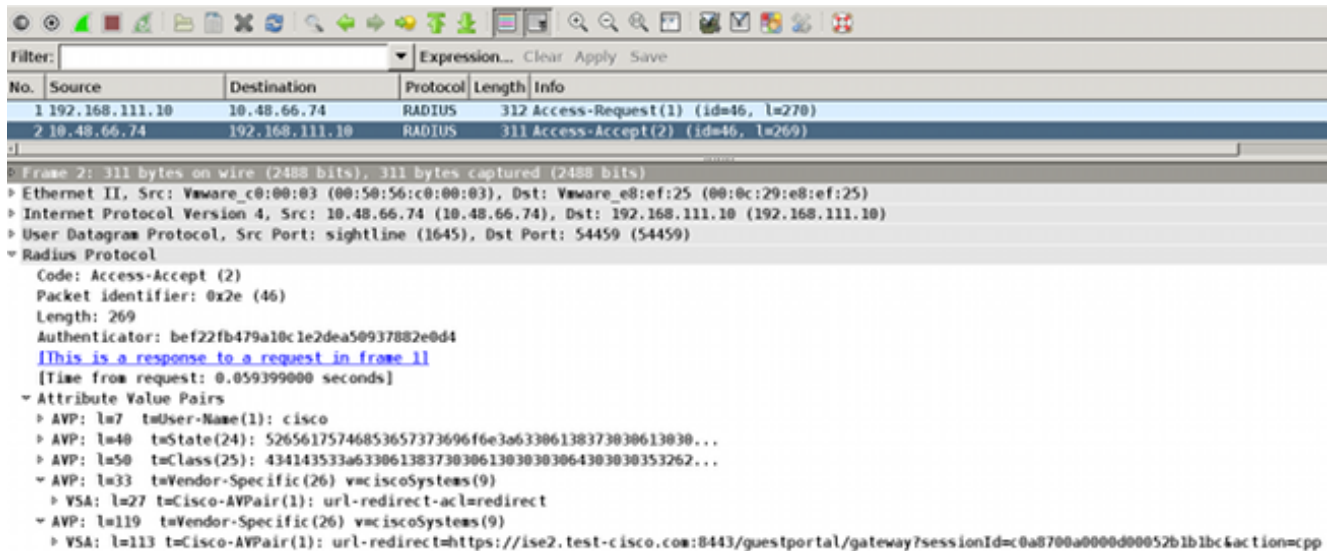
Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
<input checked="" type="checkbox"/>	posture_initial	if Any	and Windows All	initial	then file_requirement
<input checked="" type="checkbox"/>	posture_reassessment	if Any	and Windows All	reassessment	then file_requirement

**Vérifier**

Afin de confirmer que votre configuration fonctionne correctement, assurez-vous que ces étapes sont effectuées comme décrit ci-dessous :

1. L'utilisateur VPN se connecte à l'ASA.
2. L'ASA envoie une requête RADIUS et reçoit une réponse avec les attributs `url-redirect` et `url-redirect-acl` :



3. Les journaux ISE indiquent que l'autorisation correspond au profil de posture (la première entrée du journal) :

Check	IP	Host	Policy	Status	Device
<input checked="" type="checkbox"/>		#ACSACL#-IP-P	ASA9-2	Compliant	ise2
<input checked="" type="checkbox"/>	192.168.10.67		ASA9-2	ASA92-compliant	ise2
<input checked="" type="checkbox"/>	0	cisco	192.168.10.67	Compliant	ise2
<input checked="" type="checkbox"/>		cisco	192.168.10.67	ASA92-posture	User Identity Gro... Pending ise2

4. L'ASA ajoute une redirection à la session VPN :

```
aaa_url_redirect: Added url redirect:https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
acl:redirect for 10.10.10.10
```

5. L'état de la session VPN sur l'ASA indique que la position est requise et redirige le trafic HTTP :

```
ASA# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username      : cisco                               Index      : 9
Assigned IP   : 10.10.10.10                          Public IP   : 10.147.24.61
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Essentials
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 16077                               Bytes Rx   : 19497
Pkts Tx       : 43                                 Pkts Rx   : 225
Pkts Tx Drop  : 0                                 Pkts Rx Drop : 0
Group Policy  : GP-SSL                               Tunnel Group : RA
Login Time    : 14:55:50 CET Mon Dec 23 2013
Duration      : 0h:01m:34s
```

Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : c0a8700a0000900052b840e6  
Security Grp : 0

AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 9.1  
Public IP : **10.147.24.61**  
Encryption : none Hashing : none  
TCP Src Port : 50025 TCP Dst Port : 443  
Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes  
Client OS : win  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040  
Bytes Tx : 5204 Bytes Rx : 779  
Pkts Tx : 4 Pkts Rx : 1  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 9.2  
Assigned IP : **10.10.10.10** Public IP : **10.147.24.61**  
Encryption : RC4 Hashing : SHA1  
Encapsulation: TLSv1.0 TCP Src Port : 50044  
TCP Dst Port : 443 Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040  
Bytes Tx : 5204 Bytes Rx : 172  
Pkts Tx : 4 Pkts Rx : 2  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 9.3  
Assigned IP : **10.10.10.10** Public IP : **10.147.24.61**  
Encryption : AES128 Hashing : SHA1  
Encapsulation: DTLSv1.0 UDP Src Port : 63296  
UDP Dst Port : 443 Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040  
Bytes Tx : 5669 Bytes Rx : 18546  
Pkts Tx : 35 Pkts Rx : 222  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

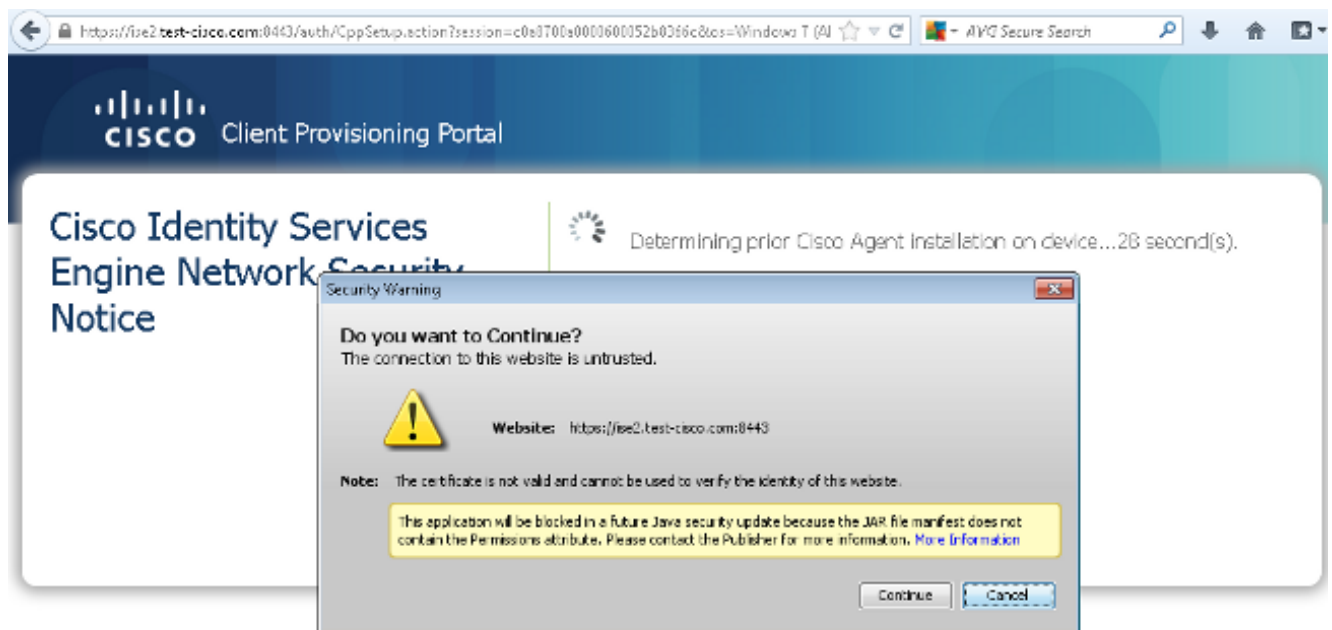
ISE Posture:

Redirect URL : **https://ise2.test-cisco.com:8443/guestportal/gateway?  
sessionId=c0a8700a0000900052b840e6&action=cpp**  
Redirect ACL : **redirect**

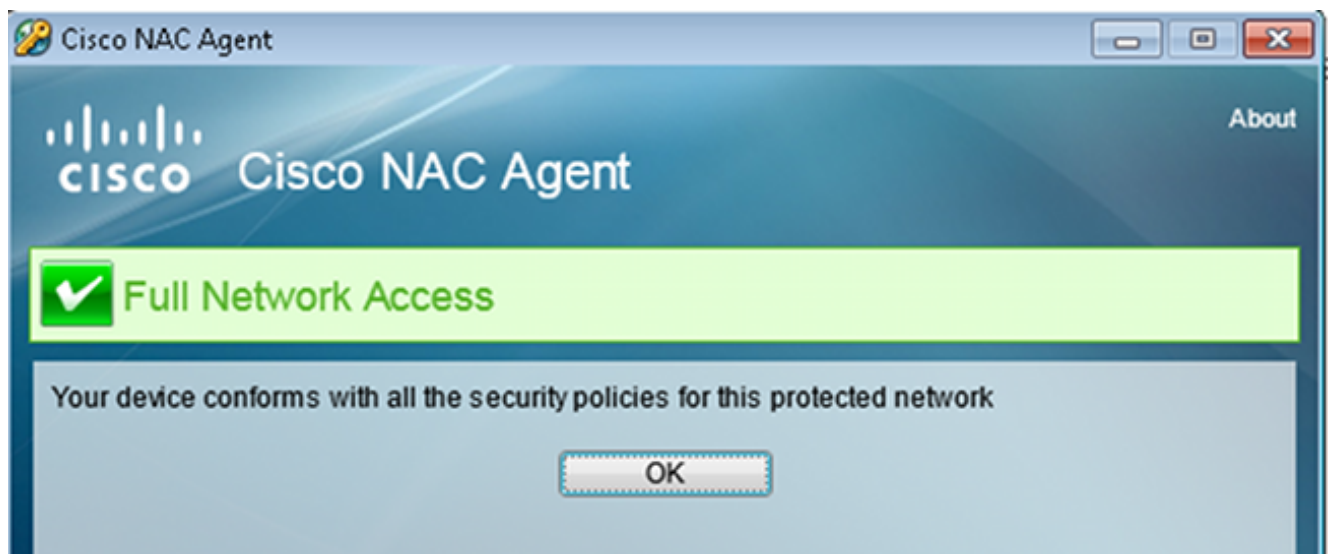
6. Le client qui initie le trafic HTTP correspondant à la liste de contrôle d'accès de redirection est redirigé vers l'ISE :

aaa\_url\_redirect: Created proxy for 10.10.10.10  
aaa\_url\_redirect: **Sending url redirect:**https://ise2.test-cisco.com:8443/  
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp  
for **10.10.10.10**

7. Le client est redirigé vers l'ISE pour la posture :



8. L'agent NAC est installé. Une fois l'agent NAC installé, il télécharge les règles de posture via le protocole SWISS et effectue des contrôles afin de déterminer la conformité. Le rapport de position est ensuite envoyé à l'ISE.



9. L'ISE reçoit le rapport de position, réévalue les règles d'autorisation et (si nécessaire) modifie l'état d'autorisation et envoie un CoA. Ceci peut être vérifié dans **ise-psc.log** :

```
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8700a0000900052b840e6
:::- Decrypting report
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- User cisco belongs to groups NAC Group:NAC:IdentityGroups:User Identity
Groups:Employee,NAC Group:NAC:IdentityGroups:An
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- Posture report token for endpoint mac 08-00-27-CD-E8-A2 is Healthy
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
:::- Posture state is compliant for endpoint with mac 08-00-27-CD-E8-A2
cisco.cpm.posture.runtime.PostureCoA -:cisco:c0a8700a0000900052b840e6
:::- Posture CoA is triggered for endpoint [null] with session
```



[c0a8700a0000900052b840e6]

10. L'ISE envoie une liste de contrôle d'accès RADIUS qui inclut l'**ID de session** et le nom de la liste de contrôle d'accès DACL qui autorise un accès complet :

No.	Source	Destination	Protocol	Length	Info
7	10.48.66.74	192.168.111.10	RADIUS	231	CoA-Request(43) (id=11, l=189)
8	192.168.111.10	10.48.66.74	RADIUS	62	CoA-ACK(44) (id=11, l=20)

```
> Frame 7: 231 bytes on wire (1848 bits), 231 bytes captured (1848 bits)
> Ethernet II, Src: Vmware_c0:00:03 (00:50:56:c0:00:03), Dst: Vmware_e8:ef:25 (00:0c:29:e8:ef:25)
> Internet Protocol Version 4, Src: 10.48.66.74 (10.48.66.74), Dst: 192.168.111.10 (192.168.111.10)
> User Datagram Protocol, Src Port: 44354 (44354), Dst Port: mps-raft (1700)
v Radius Protocol
  Code: CoA-Request (43)
  Packet identifier: 0xb (11)
  Length: 189
  Authenticator: d20817c6ca828ce7db4ee54f15177b8d
  [The response to this request is in frame 8]
v Attribute Value Pairs
  > AVP: l=6 t=NAS-IP-Address(4): 10.147.24.61
  > AVP: l=15 t=Calling-Station-Id(31): 192.168.10.67
  > AVP: l=6 t=Event-Timestamp(55): Dec 18, 2013 15:32:10.000000000 CET
  > AVP: l=18 t=Message-Authenticator(80): 1ee29f1d83e5f3aa4934d60aa617ebeb
  v AVP: l=75 t=Vendor-Specific(26) v=ciscoSystems(9)
    > VSA: l=69 t=Cisco-AVPair(1): ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
  v AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)
    > VSA: l=43 t=Cisco-AVPair(1): audit-session-id=c0a8700a0000d00052b1b1bc
```

Ceci est reflété dans les journaux ISE :

La première entrée de journal est pour l'authentification initiale qui renvoie le profil de posture (avec redirection).

La deuxième entrée de journal est renseignée après la réception du rapport SWISS conforme.

La troisième entrée du journal est renseignée lors de l'envoi de la CoA, avec la confirmation (décrite comme Autorisation dynamique réussie).

L'entrée de journal finale est créée lorsque l'ASA télécharge la DACL.

Statut	Source	Destination	Protocole	Info	Statut	Source	
✓	#ACSACL#-IP-F		ASA9-2		Compliant	ise2	
✓		192.168.10.67	ASA9-2	ASA92-compliant	Compliant	ise2	
●	0 cisco	192.168.10.67			Compliant	ise2	
✓	cisco	192.168.10.67	ASA9-2	ASA92-posture	User Identity Gro...	Pending	ise2

11. Les débogages sur l'ASA montrent que la CoA est reçue et que la redirection est supprimée. L'ASA télécharge les DACL si nécessaire :

```
ASA# Received RAD_COA_REQUEST
```

```
RADIUS packet decode (CoA-Request)
```

```
Radius: Value (String) =
```

```
41 43 53 3a 43 69 73 63 6f 53 65 63 75 72 65 2d | ACS:CiscoSecure-
44 65 66 69 6e 65 64 2d 41 43 4c 3d 23 41 43 53 | Defined-ACL=#ACS
41 43 4c 23 2d 49 50 2d 50 45 52 4d 49 54 5f 41 | ACL#-IP-PERMIT_A
4c 4c 5f 54 52 41 46 46 49 43 2d 35 31 65 66 37 | LL_TRAFFIC-51ef7
64 62 31 | db1
```

Got AV-Pair with value audit-session-id=c0a8700a0000900052b840e6

Got AV-Pair with value ACS:CiscoSecure-Defined-ACL=

**#ACSACL#-IP-PERMIT\_ALL\_TRAFFIC-51ef7db1**

aaa\_url\_redirect: **Deleted url redirect** for **10.10.10.10**

## 12. Après la session VPN, Cisco applique la liste de contrôle d'accès (DACL) à l'utilisateur :

ASA# **show vpn-sessiondb detail anyconnect**

Session Type: AnyConnect Detailed

Username : cisco Index : 9  
Assigned IP : **10.10.10.10** Public IP : **10.147.24.61**  
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License : AnyConnect Essentials  
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1  
Bytes Tx : 94042 Bytes Rx : 37079  
Pkts Tx : 169 Pkts Rx : 382  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : GP-SSL Tunnel Group : RA  
Login Time : 14:55:50 CET Mon Dec 23 2013  
Duration : 0h:05m:30s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : c0a8700a0000900052b840e6  
Security Grp : 0

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 9.1  
Public IP : **10.147.24.61**  
Encryption : none Hashing : none  
TCP Src Port : 50025 TCP Dst Port : 443  
Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes  
Client OS : win  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040  
Bytes Tx : 5204 Bytes Rx : 779  
Pkts Tx : 4 Pkts Rx : 1  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 9.2  
Assigned IP : **10.10.10.10** Public IP : **10.147.24.61**  
Encryption : RC4 Hashing : SHA1  
Encapsulation: TLSv1.0 TCP Src Port : 50044  
TCP Dst Port : 443 Auth Mode : userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040  
Bytes Tx : 5204 Bytes Rx : 172  
Pkts Tx : 4 Pkts Rx : 2  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Filter Name : **#ACSACL#-IP-PERMIT\_ALL\_TRAFFIC-51ef7db1**

DTLS-Tunnel:

Tunnel ID : 9.3

```
Assigned IP   : 10.10.10.10           Public IP    : 10.147.24.61
Encryption   : AES128                Hashing      : SHA1
Encapsulation: DTLSv1.0             UDP Src Port : 63296
UDP Dst Port : 443                  Auth Mode    : userPassword
Idle Time Out: 30 Minutes           Idle TO Left : 29 Minutes
Client OS     : Windows
Client Type   : DTLS VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx      : 83634                Bytes Rx     : 36128
Pkts Tx       : 161                  Pkts Rx      : 379
Pkts Tx Drop  : 0                    Pkts Rx Drop : 0
Filter Name   : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

**Remarque** : l'ASA supprime toujours les règles de redirection, même lorsque la liste de contrôle d'accès n'est associée à aucune liste de contrôle d'accès.

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

### Débogages sur l'ISE

Accédez à **Administration > Logging > Debug Log Configuration** afin d'activer les débogages. Cisco recommande d'activer les débogages temporaires pour :

- SUISSE
- Transfert sans interruption (NSF)
- NSF-Session
- Approvisionnement
- Posture

Entrez cette commande dans la CLI afin d'afficher les débogages :

```
ise2/admin# show logging application ise-psc.log tail count 100
```

Accédez à **Operations > Reports > ISE Reports > Endpoints and Users > Posture Details Assessment** afin d'afficher les rapports de posture :

**Posture Detail Assessment**

From 12/23/2013 12:00:00 AM to 12/23/2013 03:57:31 PM

Logged At	Status	Detail	PRA	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2013-12-23 15:21:34.9	continue		continue	cisco	08:00:27:CD:E8:A2	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 15:08:58.3	continue		continue	cisco	08:00:27:CD:E8:A2	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:59:34.3	continue		continue	cisco	08:00:27:CD:E8:A2	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:55:28.6	N/A		N/A	cisco	08:00:27:CD:E8:A2	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 14:44:45.0	N/A		N/A	cisco	08:00:27:CD:E8:A2	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 13:34:30.3	N/A		N/A	cisco	08:00:27:7F:5F:6...	10.147.24.92	Windows 7 Ultimate 64-bit	Cisco NAC A...	Received a posture report from an endpoint
2013-12-23 13:27:10.3	N/A		N/A	cisco	08:00:27:7F:5F:6...	10.147.24.92	Windows 7 Ultimate 64-bit	Cisco NAC A...	Received a posture report from an endpoint

Sur la page Posture More Detail Assessment, un nom de stratégie et un nom de condition s'affichent, ainsi que les résultats :

### Posture More Detail Assessment

Time Range: From 12/23/2013 12:00:00 AM to 12/23/2013 03:57:31 PM  
 Generated At: 2013-12-23 15:57:31.248

#### Client Details

Username:	cisco
Mac Address:	08:00:27:CD:E8:A2
IP address:	10.147.24.92
Session ID:	c0a8700a0000b00052b846c0
Client Operating System:	Windows 7 Enterprise 64-bit
Client NAC Agent:	Cisco NAC Agent for Windows 4.9.0.1013
PRA Enforcement:	1
CoA:	Received a posture report from an endpoint
PRA Grace Time:	
PRA Interval:	240
PRA Action:	continue
User Agreement Status:	NotEnabled
System Name:	MGARCARZ-WS01
System Domain:	cisco.com
System User:	mgarcarz
User Domain:	CISCO
AV Installed:	McAfee VirusScan Enterprise;8.8.0.975;7227;10/13/2013;McAfeeAV,Cisco Security Agent;6.0.2.130;;;CiscoAV
AS Installed:	Windows Defender;6.1.7600.16385;1.95.191.0;11/19/2010;MicrosoftAS

#### Posture Report

Posture Status:	Compliant
Logged At:	2013-12-23 15:21:34.902

#### Posture Policy Details

Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions
posture_initial	file_require...	Mandatory		file_condition		

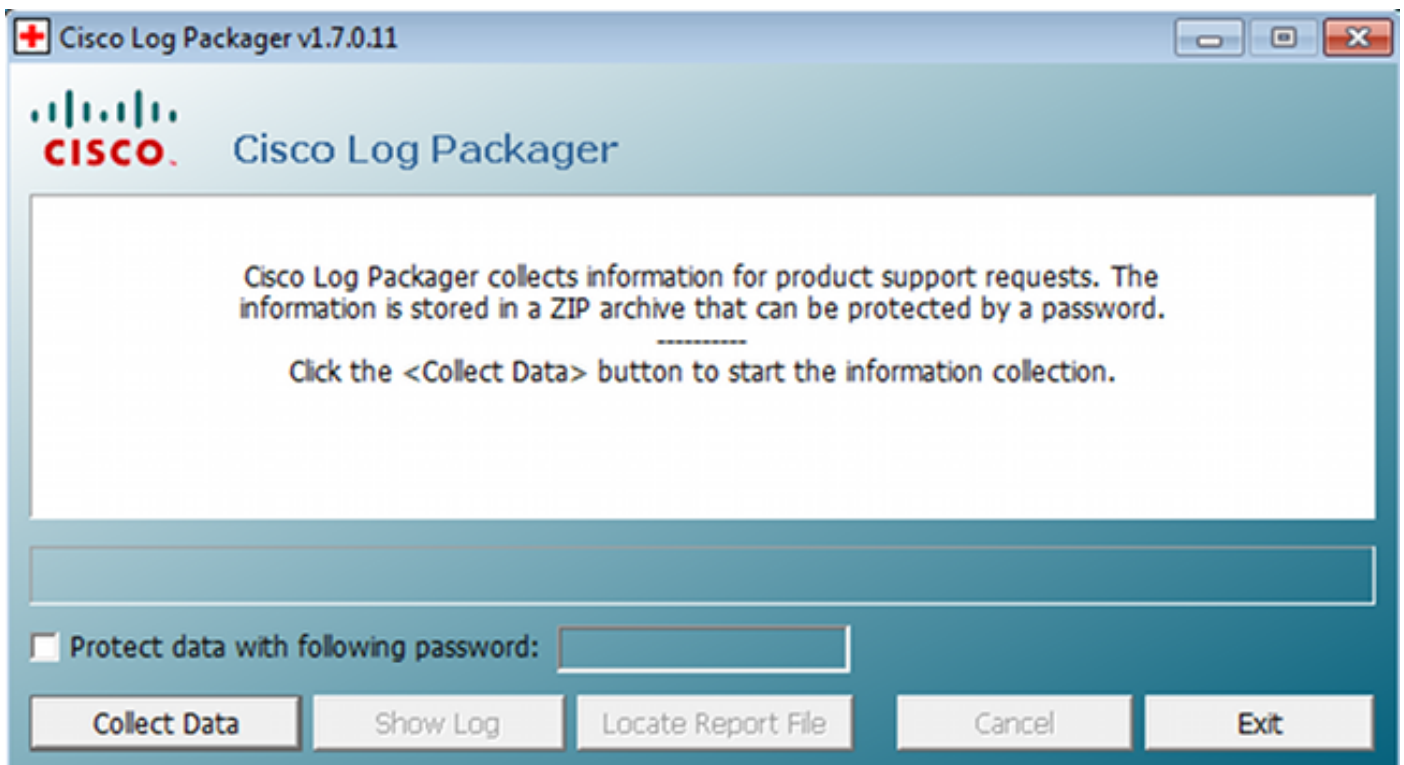
## Débogages sur l'ASA

Vous pouvez activer ces débogages sur l'ASA :

- debug aaa url-redirect
- debug aaa authorization
- debug radius dynamic-authorization
- debug radius decode
- debug radius user cisco

## Débogages pour l'agent

Pour l'agent NAC, il est possible de collecter les débogages avec Cisco Log Packager, qui est lancé à partir de l'interface graphique utilisateur ou avec l'interface de ligne de commande : CCAgentLogPackager.app.



**Conseil** : vous pouvez décoder les résultats à l'aide de l'outil Centre d'assistance technique (TAC).

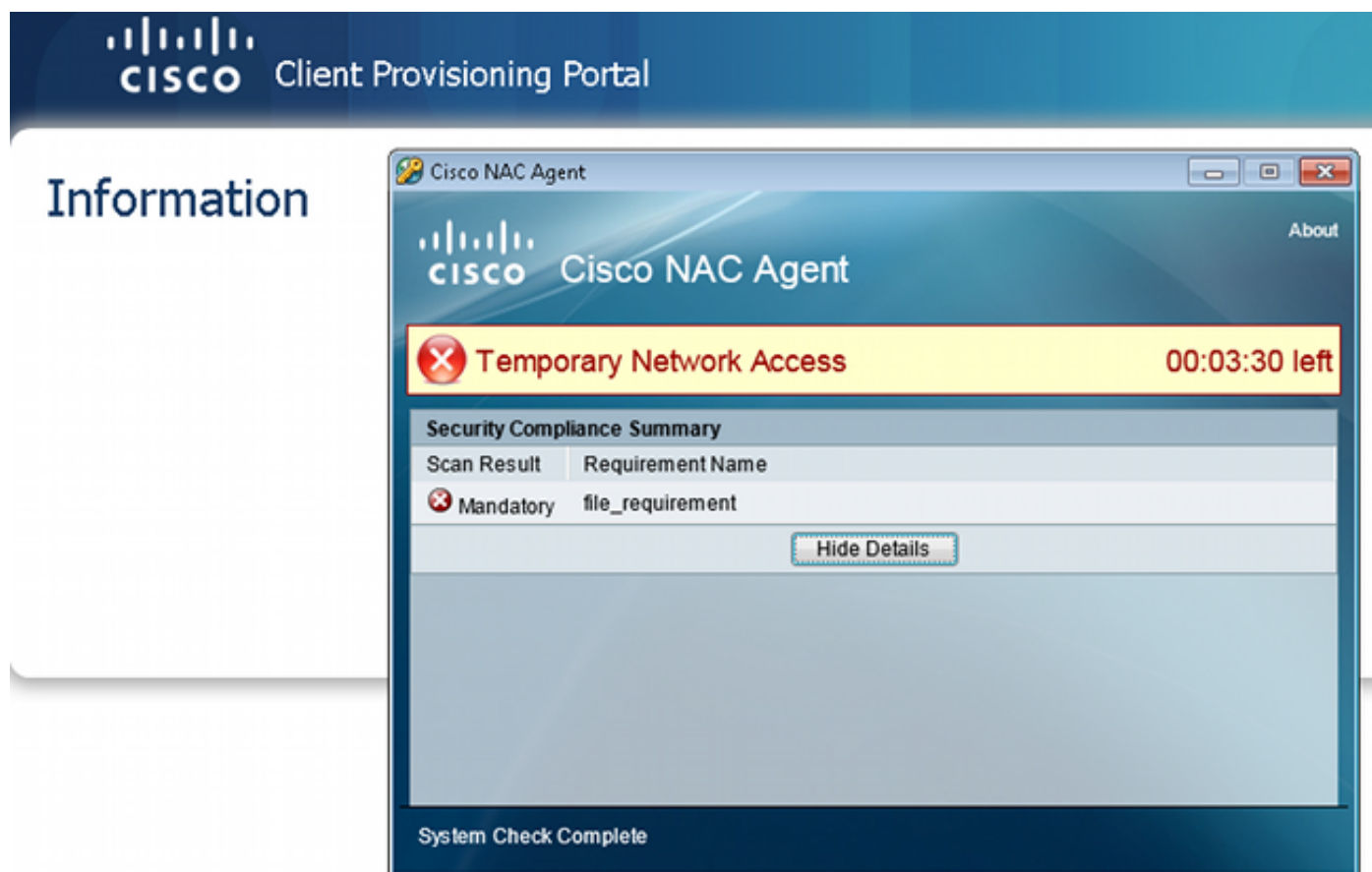
Pour récupérer les journaux de l'agent Web, accédez aux emplacements suivants :

- C: > Document and Settings > <user> > Local Settings > Temp > webagent.log (décodé avec l'outil TAC)
- C: > Document and Settings > <user> > Local Settings > Temp > webagentsetup.log

**Remarque** : si les journaux ne se trouvent pas à ces emplacements, vérifiez la variable d'environnement TEMP.

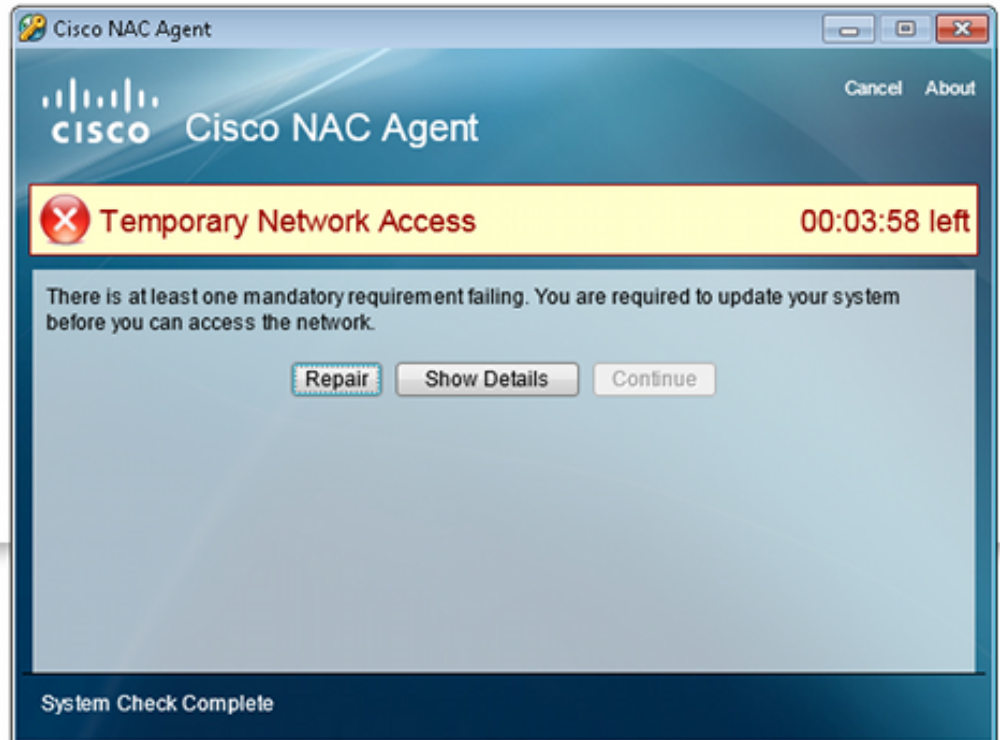
## Défaillance de la posture agent NAC

Si la posture échoue, l'utilisateur est présenté avec la raison :



L'utilisateur est alors autorisé à effectuer des actions correctives si elles sont configurées :

## Information



## Informations connexes

- [Configuration d'un serveur externe pour l'autorisation de l'utilisateur de l'appareil de sécurité](#)
- [Guide de configuration du CLI VPN de la série Cisco ASA, 9.1](#)
- [Guide de l'utilisateur de la plateforme de services d'identité de Cisco, version 1.2](#)
- [Technical Support & Documentation - Cisco Systems](#)

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.