

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Écoulement détaillé](#)

[Configurez le nuage d'AMP](#)

[Étape 1. Connecteur de téléchargement de nuage d'AMP](#)

[Configurez ISE](#)

[Étape 1. Configurez les stratégies et les états de posture](#)

[Étape 2. Configurez le profil de posture](#)

[Étape 3. Configurez le profil d'AMP](#)

[Étape 2. Applications de téléchargement et profil XML à ISE](#)

[Étape 3. Module de conformité d'AnyConnect de téléchargement](#)

[Étape 4. Ajoutez la configuration d'AnyConnect](#)

[Étape 5. Configurez les règles de ravitaillement de client](#)

[Étape 6. Configurez les stratégies d'autorisation](#)

[Étape 7. Services de l'enable TC-NAC](#)

[Étape 8. Configurez l'adaptateur d'AMP](#)

[Vérifier](#)

[Point final](#)

[Nuage d'AMP](#)

[ISE](#)

[Dépanner](#)

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.

The screenshot shows the Cisco AMP for Endpoints web interface. At the top, there's a navigation bar with 'Dashboard', 'Analysis', 'Outbreak Control', 'Reports', 'Management', and 'Accounts'. A search bar is on the right. The main heading is 'Download Connector'. Below it, a 'Group' dropdown menu is set to 'Audit'. There are four connector cards:

- FireAMP Windows**: Shows 'No computers require updates' and 'Audit Policy' settings: 'Flash Scan on Install' (checked) and 'Redistributable' (checked). Buttons: 'Show URL', 'Download'.
- FireAMP Mac**: Shows 'Audit Policy for FireAMP Mac' settings: 'Flash Scan on Install' (checked). Buttons: 'Show URL', 'Download'.
- FireAMP Linux**: Shows 'Audit Policy for FireAMP Li...' settings: 'Flash Scan on Install' (checked). Buttons: 'Show GPG Public Key', 'Show URL', 'Download'.
- FireAMP Android**: Shows 'Default FireAMP Android' settings: 'Activation Codes'. Buttons: 'Show URL', 'Download'.

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 :

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

File Conditions List > File_Condition

File Condition

* Name: File_Condition

Description:

* Operating System: Windows All

Compliance Module: Any version

* File Type: FileExistence

* File Path: ABSOLUTE_PATH

* File Operator: Exists

C:\test.bt

Save Reset

- Authentication
- Authorization
- Profiling
- Posture
 - Anti-Malware Condition
 - Anti-Spyware Condition
 - Anti-Virus Condition
 - Application Condition
 - Compound Condition
 - Disk Encryption Condition
 - File Condition
 - Patch Management Condition
 - Registry Condition
 - Service Condition
 - USB Condition
 - Dictionary Simple Condition
 - Dictionary Compound Condition
- Guest
- Common

Cette condition est utilisée pour une condition requise :

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

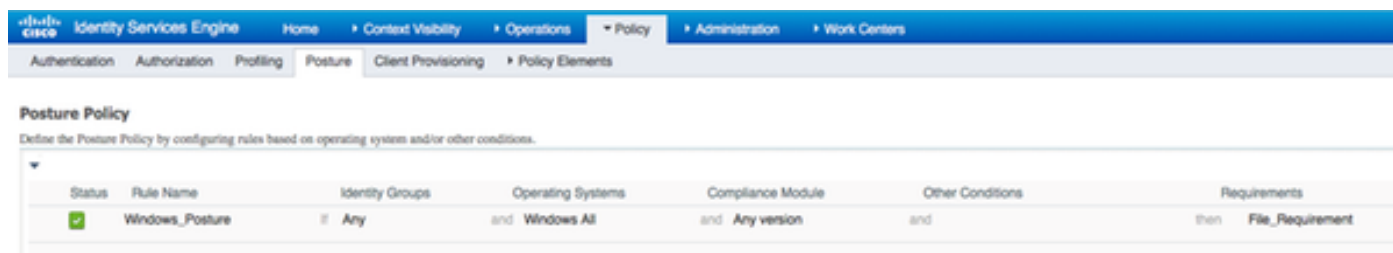
Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Requirements

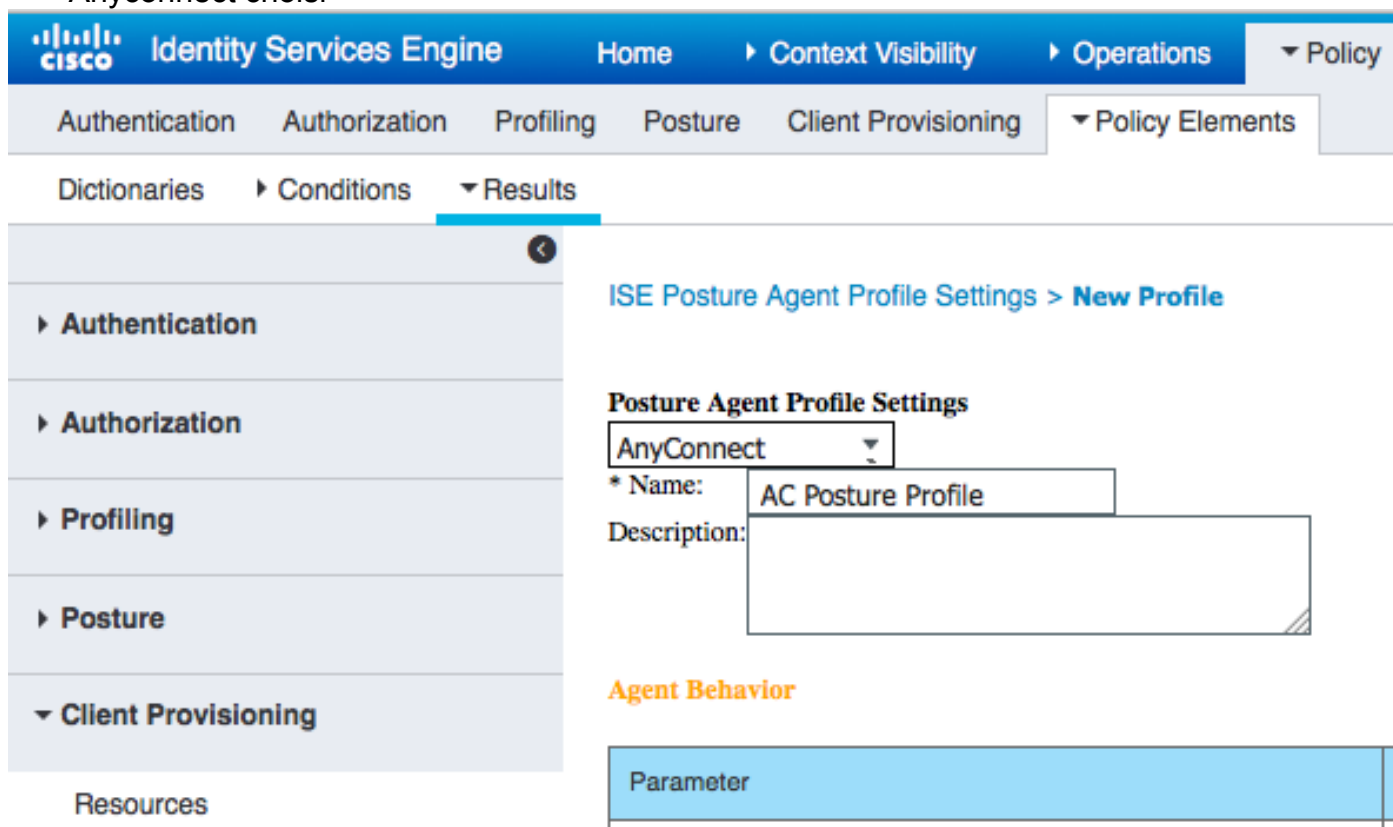
Name	Operating Systems	Compliance Module	Conditions	Remediation Actions
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	met if ANY_av_win_inst	then Message Text Only
File_Requirement	for Windows All	using Any version	met if File_Condition	then Message Text Only
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	met if ANY_av_win_def	then AnyAVDefRemediationWin
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	met if ANY_am_mac_inst	then Message Text Only
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	met if ANY_as_win_inst	then Message Text Only
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	met if ANY_as_win_def	then AnyASDefRemediationWin
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	met if ANY_av_mac_inst	then Message Text Only
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	met if ANY_av_mac_def	then AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	met if ANY_as_mac_inst	then Message Text Only
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	met if ANY_as_mac_def	then AnyASDefRemediationMac
Any_AM_Installation_Win	for Windows All	using 4.x or later	met if ANY_am_win_inst	then Message Text Only
Any_AM_Definition_Win	for Windows All	using 4.x or later	met if ANY_am_win_def	then AnyAMDefRemediationWin
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	met if ANY_am_mac_def	then AnyAMDefRemediationMac
USB_Block	for Windows All	using 4.x or later	met if USB_Check	then USB_Block

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

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all

Étape 3. Configurez le profil d'AMP

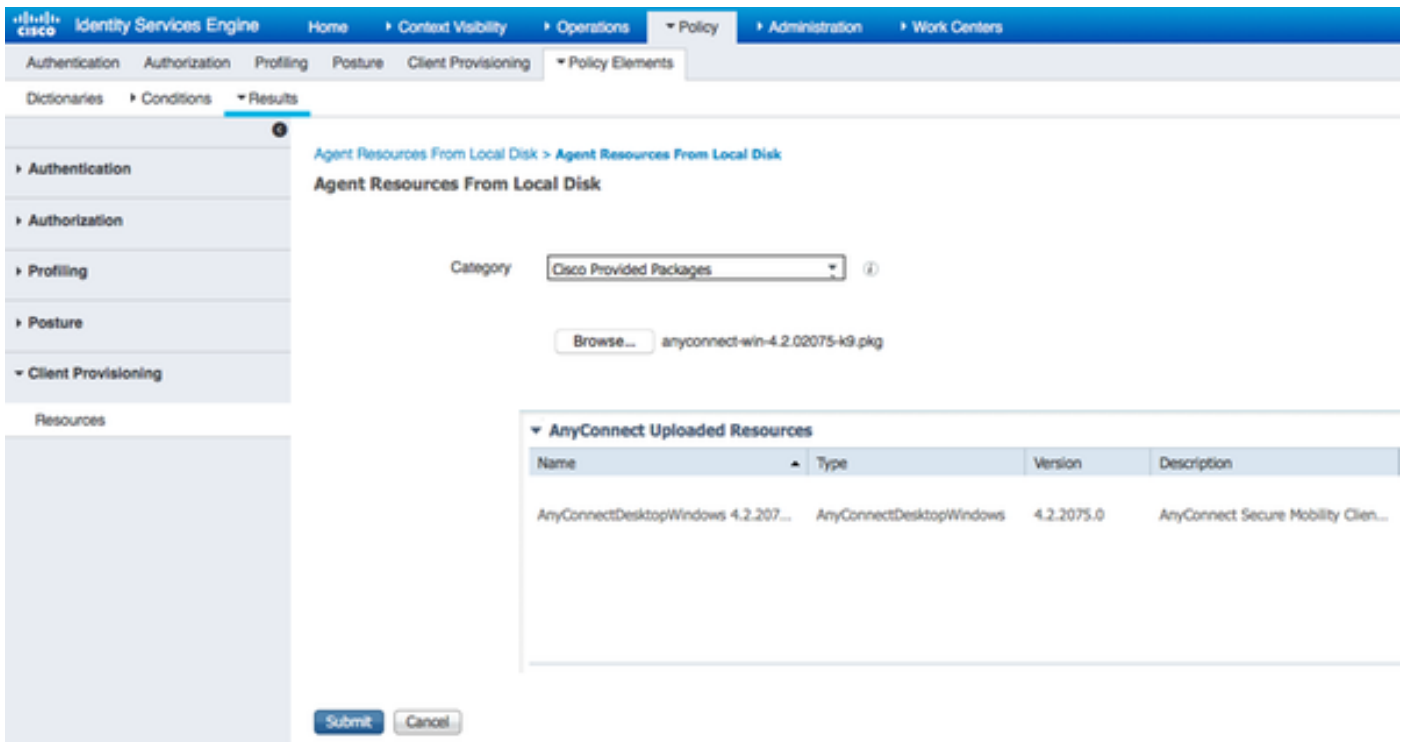
Le profil d'AMP contient les informations où l'installer windows se trouve. L'installer windows a été téléchargé plus tôt du nuage d'AMP. Il devrait être accessible de la machine cliente. Le certificat du serveur HTTPS, où l'installateur se trouve devrait sont de confiance par la machine cliente aussi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

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The 'Results' tab is selected. The left sidebar contains a navigation menu with 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', and 'Resources'. The main content area is titled 'AMP Enabler Profile Settings > New Profile' and 'AMP Enabler Profile'. It contains the following fields and options:

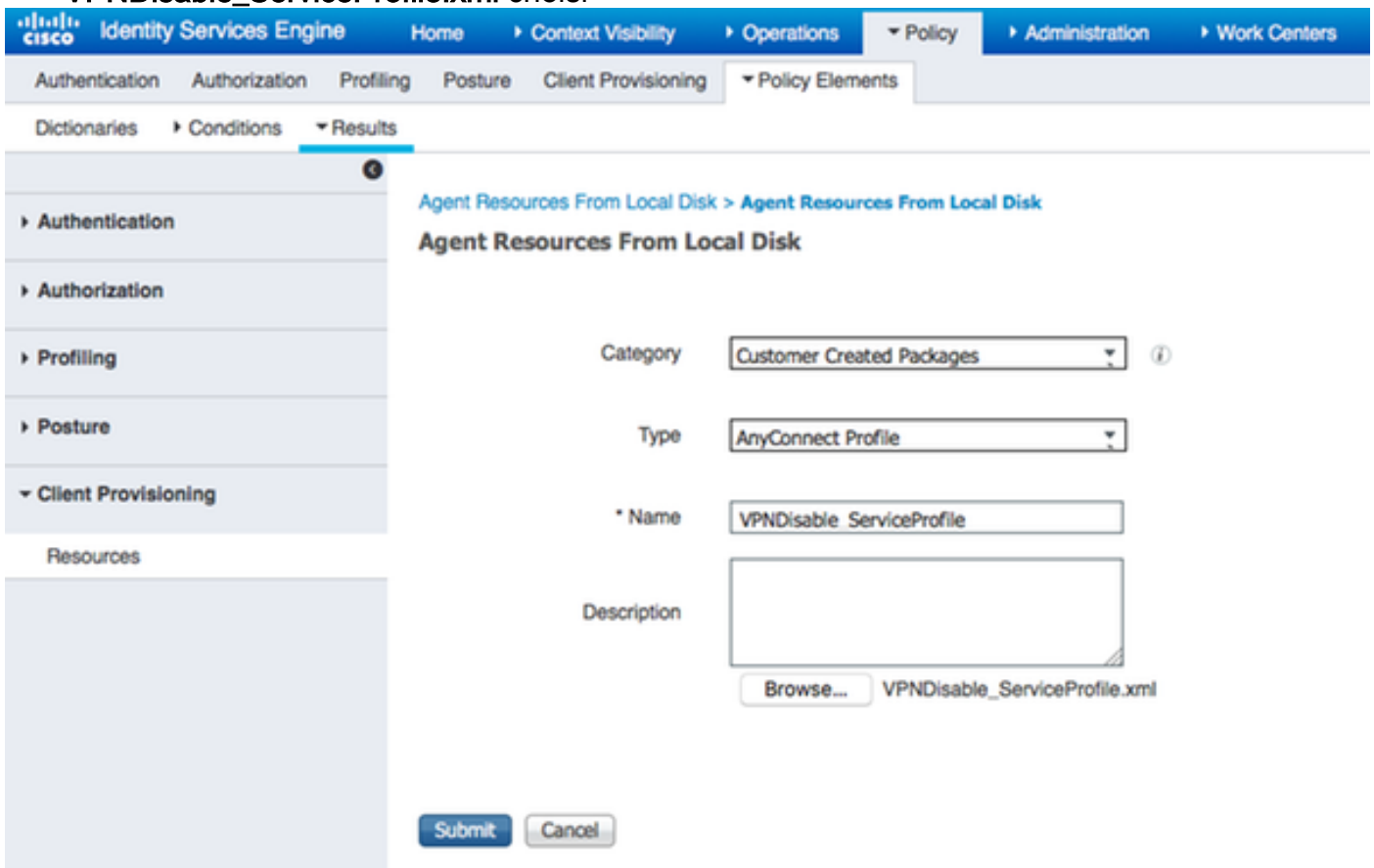
- * Name: AMP Profile
- Description:
- Install AMP Enabler Uninstall AMP Enabler
- Windows Installer: https://win2012ek.example.com/Downloads/Audit_FireAMPSetup.
- MAC Installer: <https://>
- Windows Settings:
 - Add to Start Menu
 - Add to Desktop
 - Add to Context Menu
- Submit Cancel

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**

Download Remote Resources ✕

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 3.6.10591.2	AnyConnect OS X Compliance Module 3.6.10591.2
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 3.6.10591.2	AnyConnect Windows Compliance Module 3.6.10591.2
<input type="checkbox"/>	ComplianceModule 3.6.10591.2	NACAgent ComplianceModule v3.6.10591.2 for Windows
<input type="checkbox"/>	MACComplianceModule 3.6.10591.2	MACAgent ComplianceModule v3.6.10591.2 for MAC OSX
<input type="checkbox"/>	MacOsXAgent 4.9.0.1006	NAC Posture Agent for Mac OSX (ISE 1.2 release)
<input type="checkbox"/>	MacOsXAgent 4.9.0.1007	NAC Posture Agent for Mac OSX v4.9.0.1007 (with CM 3.6.7873.2)- ISE
<input type="checkbox"/>	MacOsXAgent 4.9.0.655	NAC Posture Agent for Mac OSX (ISE 1.1.1 or later)
<input type="checkbox"/>	MacOsXAgent 4.9.0.661	NAC Posture Agent for Mac OS X v4.9.0.661 with CM v3.5.7371.2 (ISE
<input type="checkbox"/>	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Abov
<input type="checkbox"/>	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3 rel
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1.3 Release)
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE 1.2 release
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 release
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 release
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE 1.2 Patch
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.36	Supplicant Provisioning Wizard for Mac OsX 1.0.0.36 (for ISE 1.2 Patch

For AnyConnect software, please download from <http://cisco.com/go/anyconnect>. Use the "Agent resource from local disk" add option, to import into ISE

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Profiling

Posture

Client Provisioning

Resources

AnyConnect Configuration > AnyConnect Configuration AMP

* Select AnyConnect Package: AnyConnectDesktopWindows 4.2.2075.0

* Configuration Name: AnyConnect Configuration AMP

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 3.6.10591.2

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AC Posture Profile

VPN: VPNDisable_ServiceProfile

Network Access Manager

Web Security

AMP Enabler: AMP Profile

Network Visibility

Customer Feedback

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

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"/> Windows_Posture_AMP	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration AMP

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > AMP_Profile

Authorization Profile

* Name AMP_Profile

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL ACL_WEBAUTH_REDIRECT Value Client Provisioning Portal (defa

Display Certificates Renewal Message

Static IP/Host name/FQDN

Advanced Attributes Settings

Select an item =

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on Identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

Exceptions (1)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
2. <input checked="" type="checkbox"/>	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
1. <input checked="" type="checkbox"/>	Non_Compliant_Devices_Access	if Session:PostureStatus NOT_EQUALS Compliant	then AMP_Profile
<input type="checkbox"/>	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD
<input type="checkbox"/>	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD
<input checked="" type="checkbox"/>	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then VA_Scan
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

Étape 7. Services de l'enable TC-NAC

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

Deployment Nodes List > ISE21-3ek

Edit Node

General Settings Profiling Configuration

Hostname **ISE21-3ek**
FQDN **ISE21-3ek.example.com**
IP Address **10.62.145.25**
Node Type **Identity Services Engine (ISE)**

Personas

Administration Role **STANDALONE**

Monitoring Role **PRIMARY** Other Monitoring Node

Policy Service

Enable Session Services Include Node in Node Group **None**

Enable Profiling Service

Enable Threat Centric NAC Service

Étape 8. Configurez l'adaptateur d'AMP

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

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassiveID > Threat Centric NAC

Third Party Vendors

Vendor Instances > New
Input fields marked with an asterisk (*) are required.

Vendor * AMP : THREAT

Instance Name * AMP_THREAT

Cancel Save

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

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassiveID > Threat Centric NAC

Third Party Vendors

Vendor Instances
0 Selected

Refresh + Add Trash Edit Filter

Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
QualysVA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active
AMP_THREAT	AMP	THREAT		Disconnected	Ready to configure

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

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > PassiveID > Threat Centric NAC

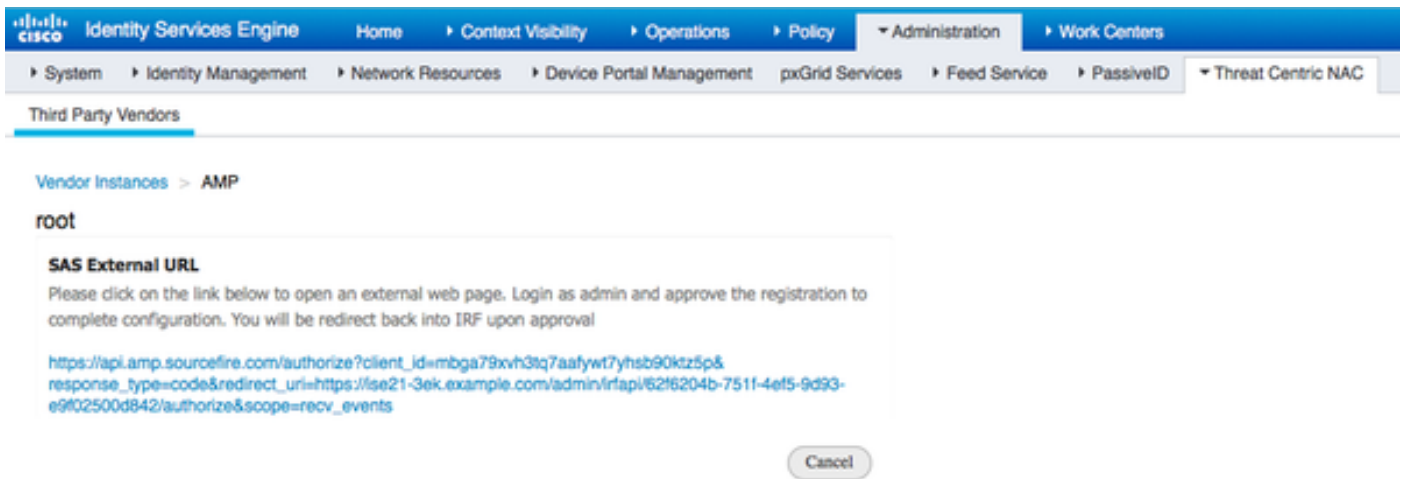
Third Party Vendors

Vendor Instances > AMP

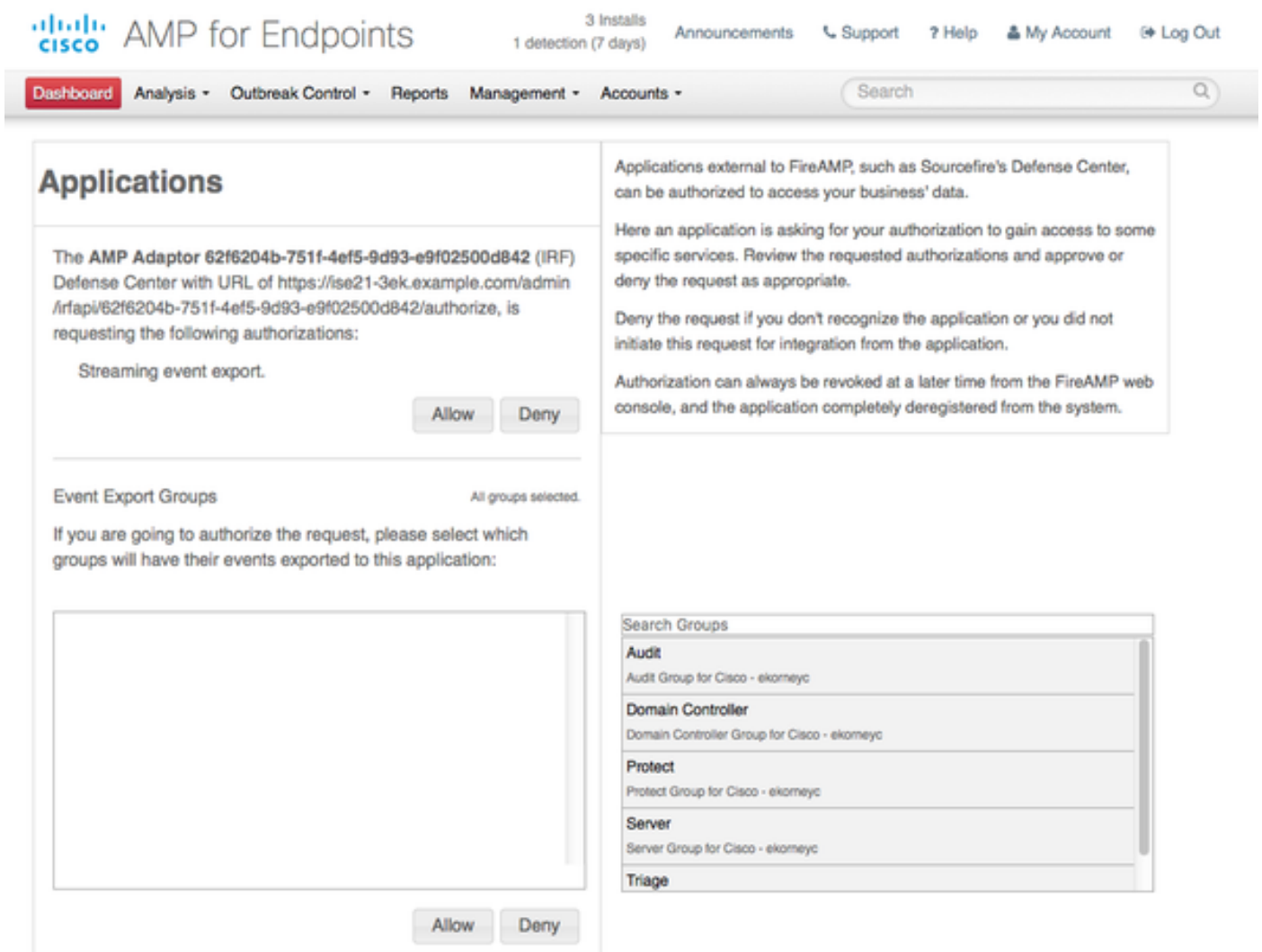
Cloud
US Cloud
Which public cloud would you like to connect to

Cancel Next

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



Le clic **autoriser** 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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Third Party Vendors

Vendor Instances

0 Selected

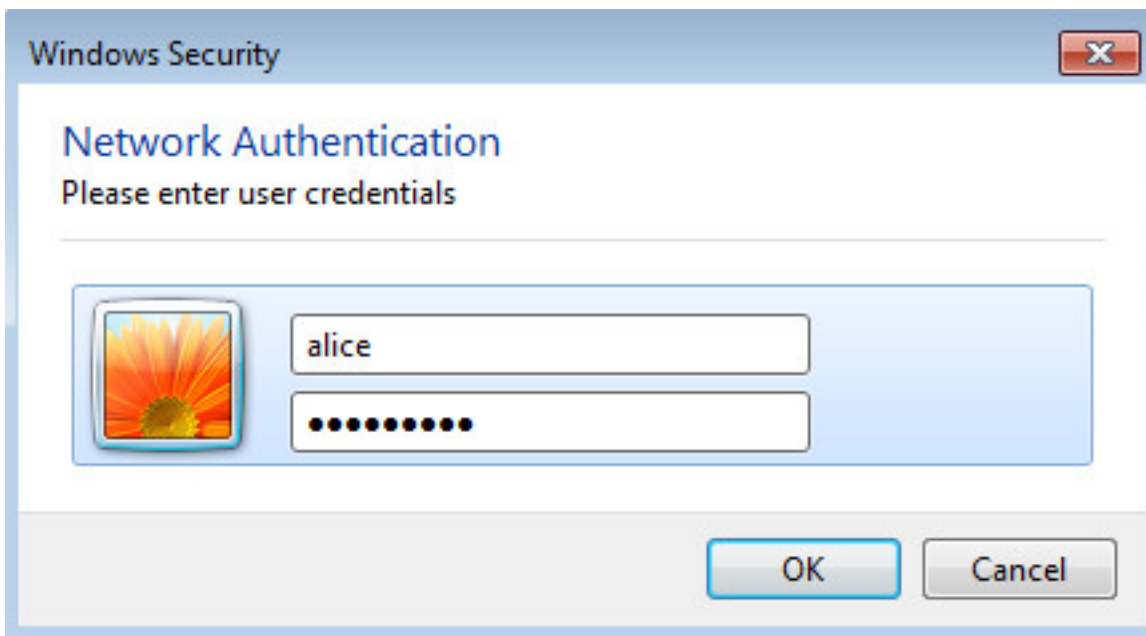
Refresh Add Trash Edit Filter Settings

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
QUALYS_VA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active

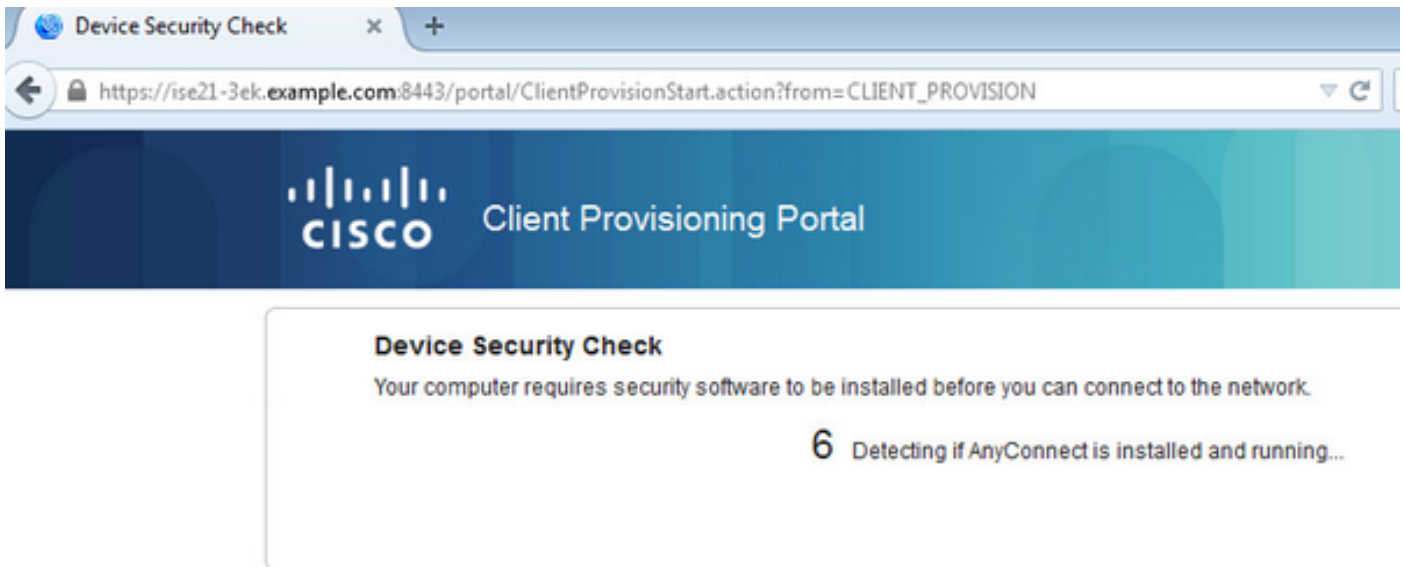
Vérifiez

Point final

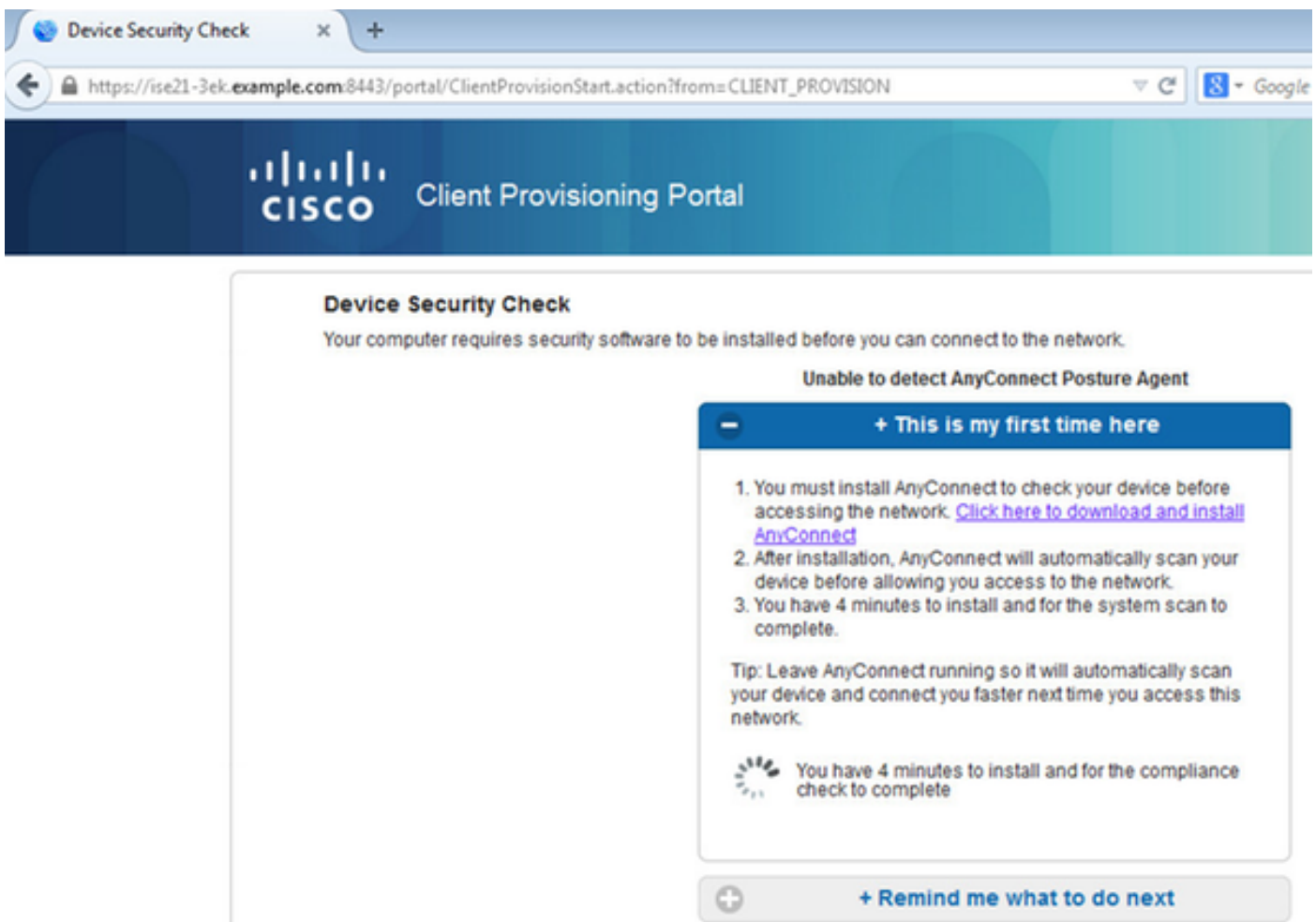
Connectez au réseau Sans fil par l'intermédiaire de PEAP (MSCHAPv2).



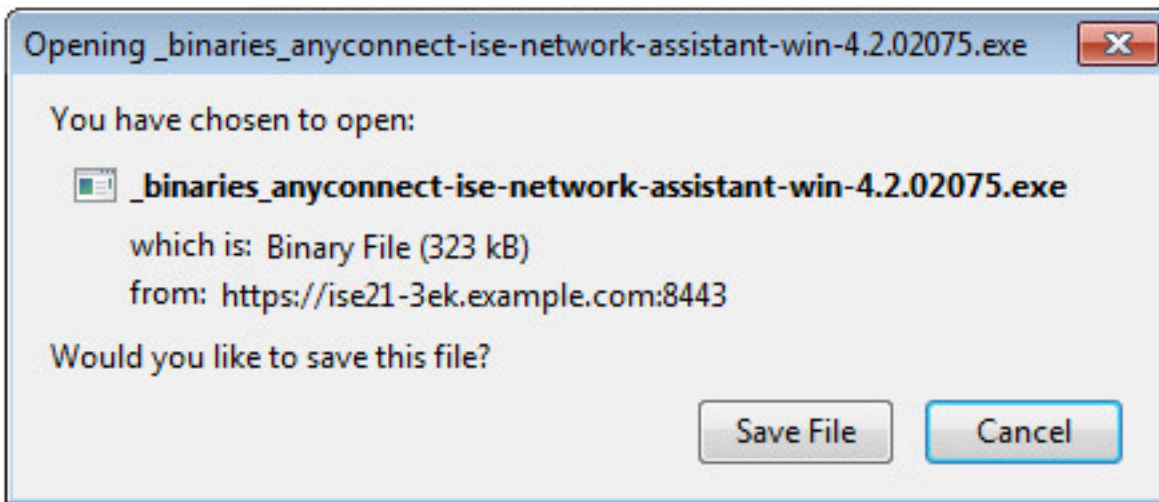
Une fois que connecté la redirection au portail de ravitaillement de client a lieu.



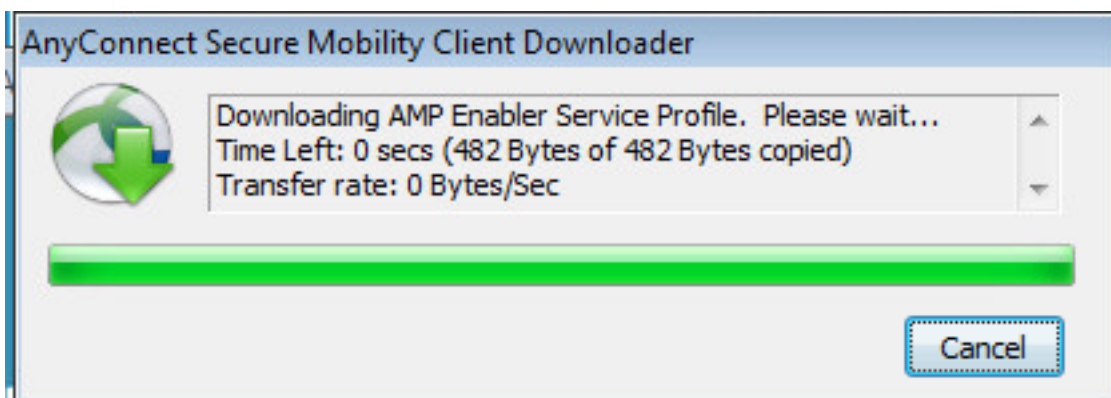
Puisqu'il n'y a rien installé sur la machine cliente, ISE incite pour l'installation de client d'AnyConnect.

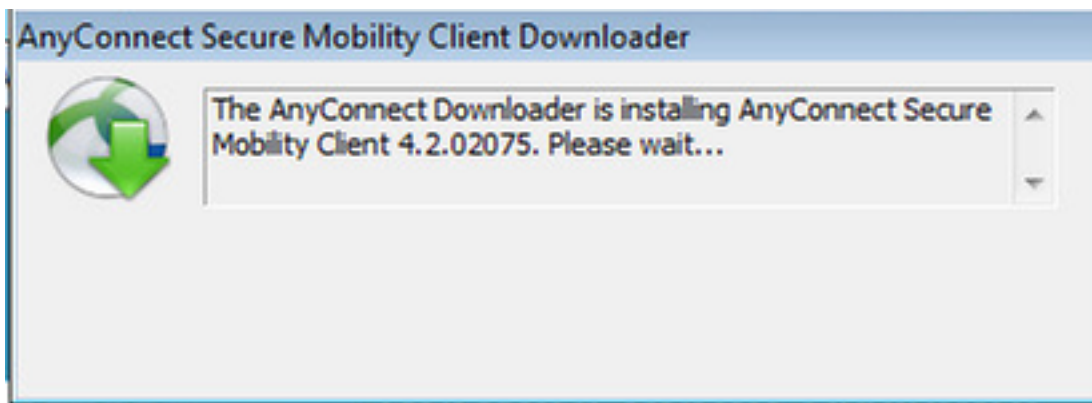


L'application auxiliaire de configuration réseau (NSA) devrait être téléchargée et passage de machine cliente.

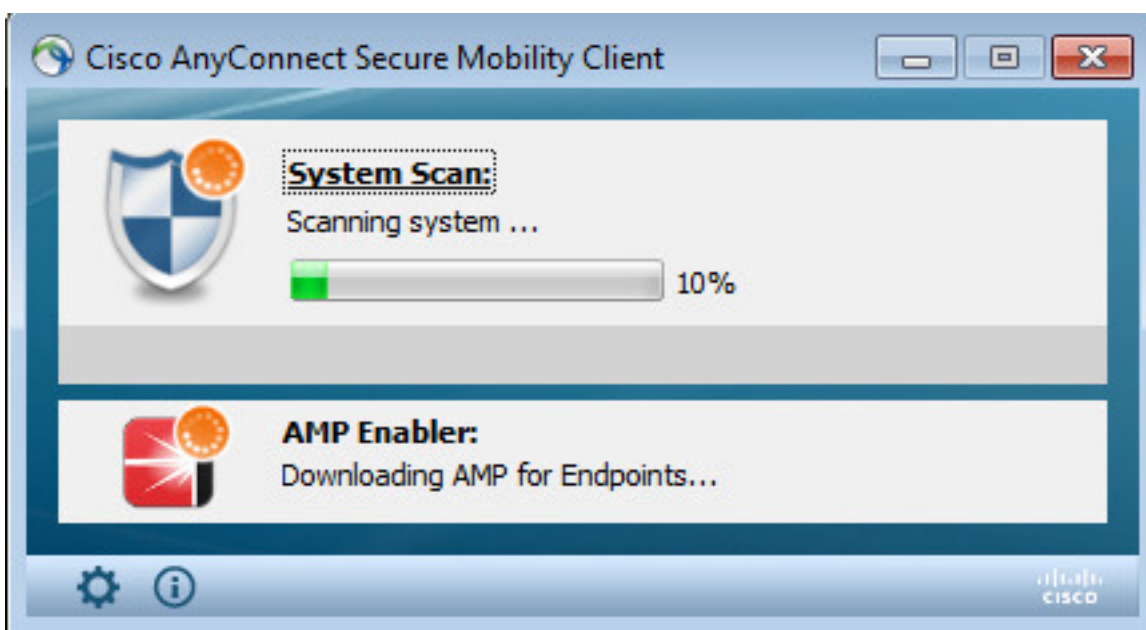
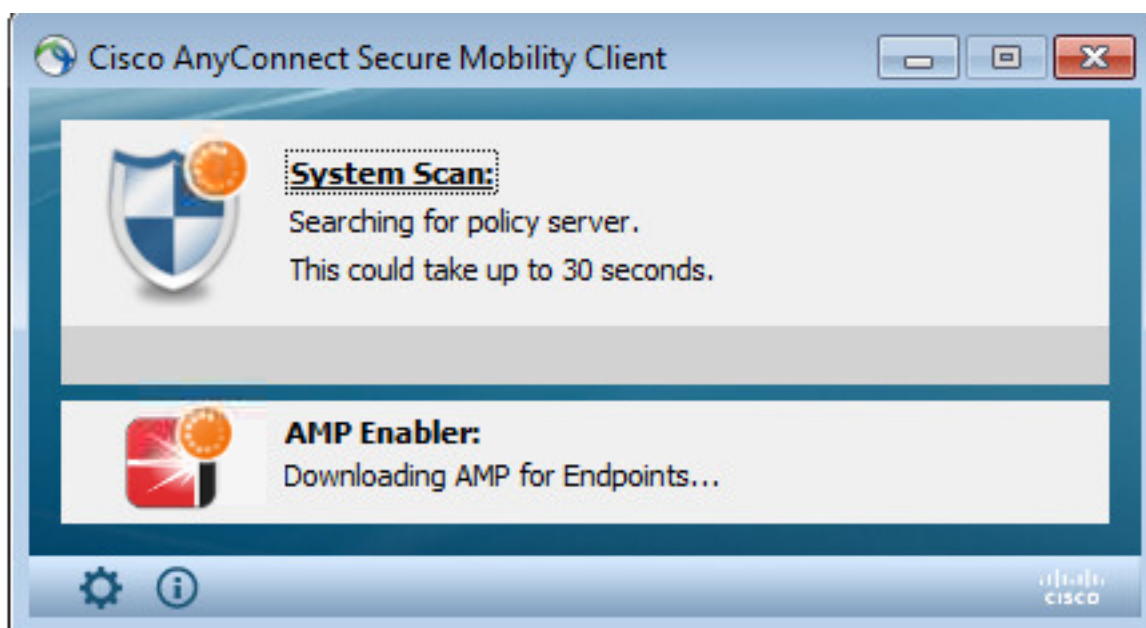


Le NSA prend soin d'installer des éléments requis et des profils.

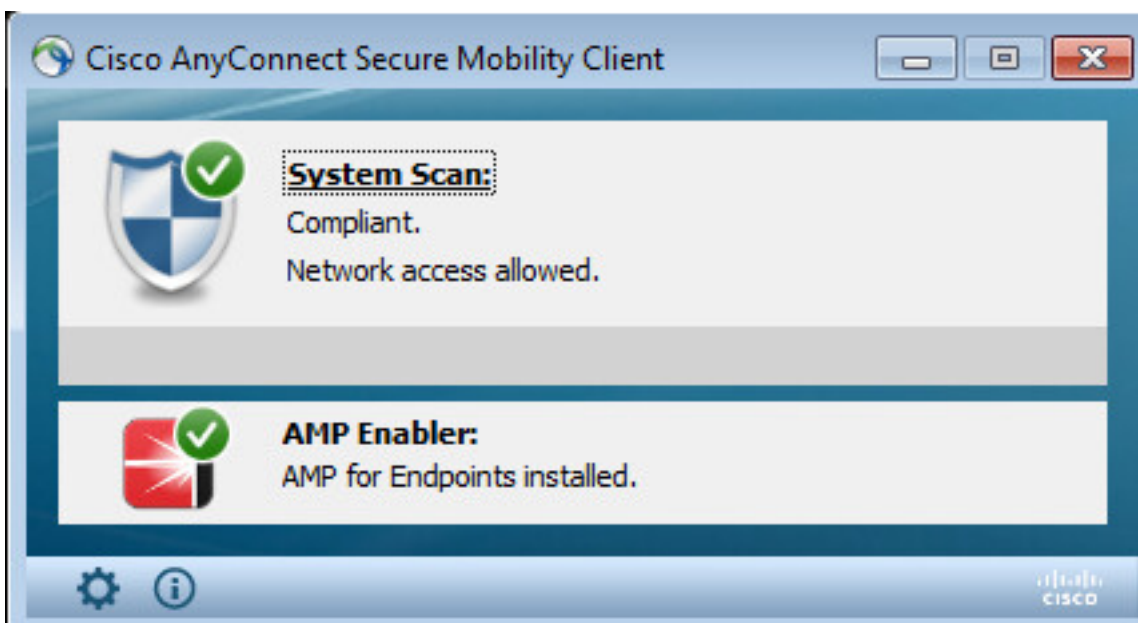
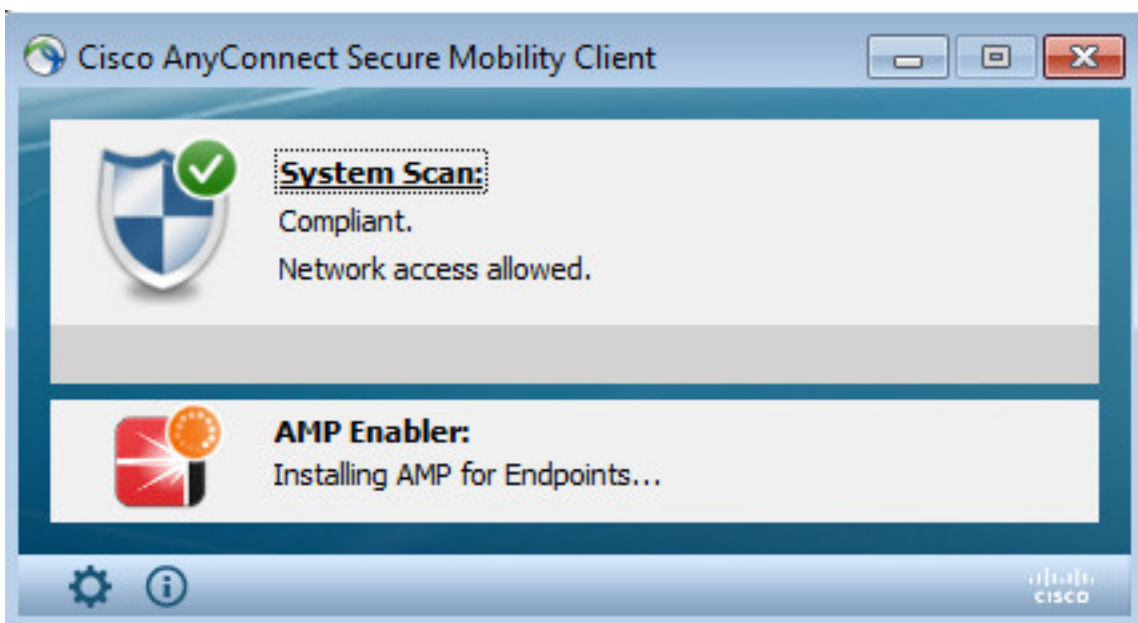
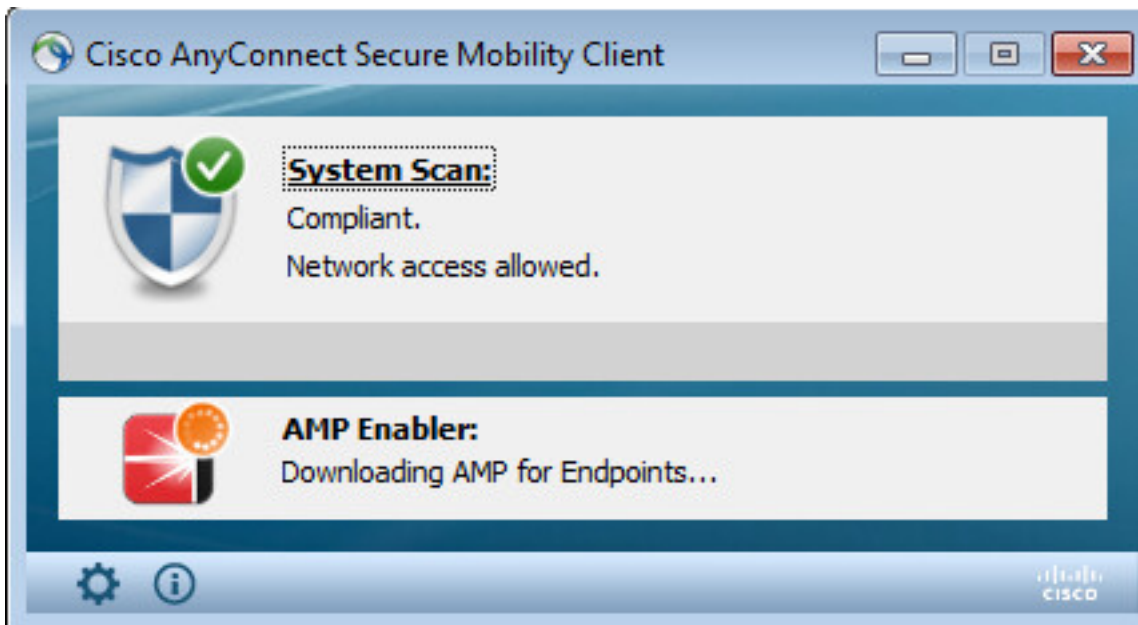




Une fois que l'installation est de finition, le module de posture d'AnyConnect exécute le contrôle de conformité.



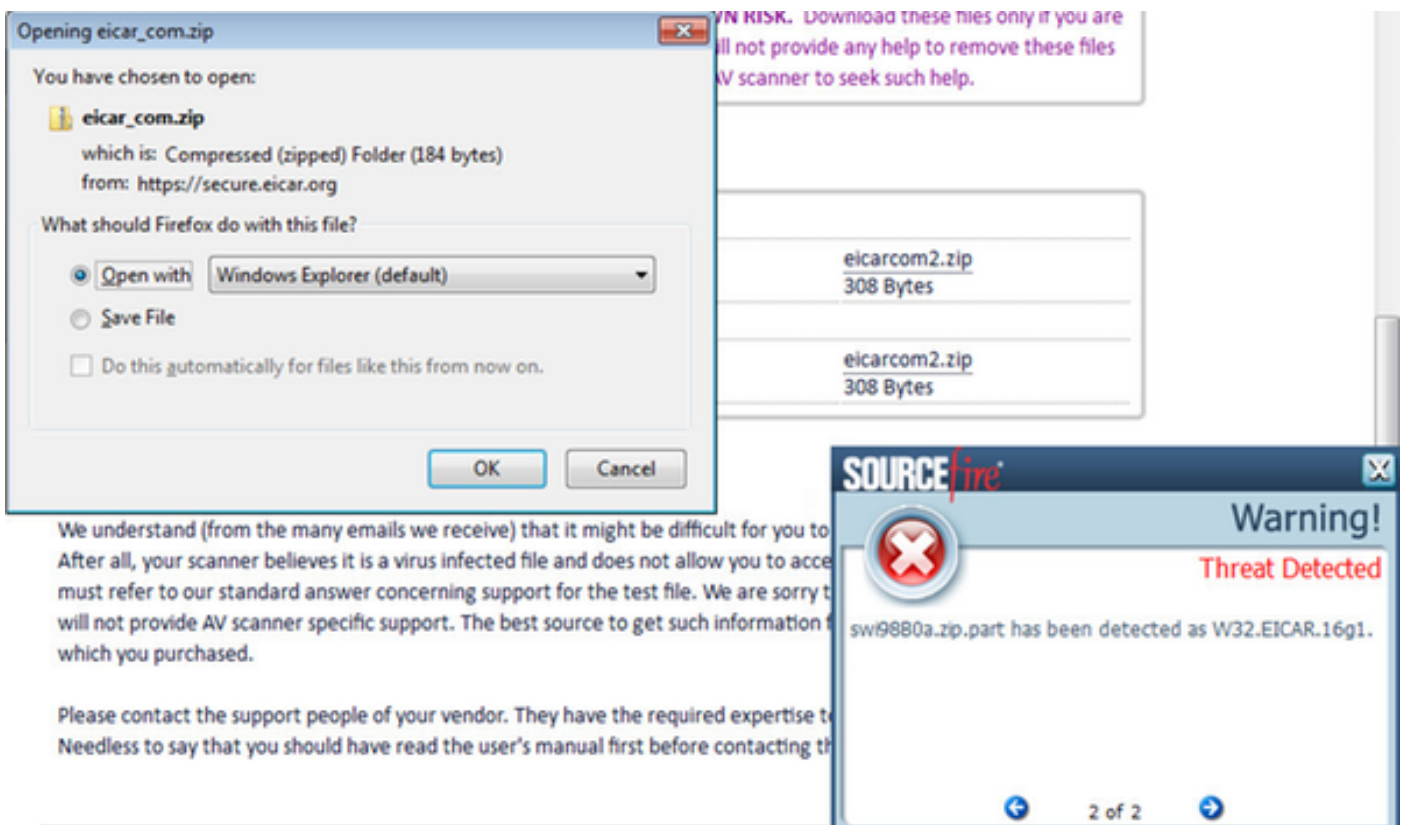
Car l'accès complet est donné, si le point final est conforme, l'AMP est téléchargé et installé du web server spécifié plus tôt dans le profil d'AMP.



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.

4 Installs
5 detections (7 days)

Announcements Support Help My Account Log Out

Dashboard Analysis - Outbreak Control - Reports Management - Accounts -

Search

Group Filter Select Groups

Dashboard

Overview Events Heat Map

Refresh All Auto Refresh

Indications of Compromise

ekorneyc-PC.example.com Mark Resolved

Threat Detected

Hosts Detecting Malware (7 days)

Computer	Count
ekorneyc-PC.example.com	4
HARISHA-PC.example.com	1

Hosts Detecting Network Threats (7 days)

Computer Count

There are no recent network threat detections to display.

Malware Threats (7 days)

Detection Name	Count
W32.EICAR.16g1	5

Network Threats (7 days)

Remote IP Count

There are no recent network threat detections to display.

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

4 Installs
5 detections (7 days)

Announcements Support Help My Account Log Out

Dashboard Analysis - Outbreak Control - Reports Management - Accounts -

Search

Dashboard

Overview Events Heat Map

Filter: (New) Select a Filter

Event Type Threat Detected Group All Groups

Filters Computer: e8c02e6a-a885-47ba-aeec-2ac03bea4241

Sort Time

Not Subscribed Reset Save filter as...

ekorneyc-PC.example.com detected 0M90PRxO.zip.part as W32.EICAR.16g1

Quarantine: Not Seen 2016-05-30 16:27:30 UTC

File Detection	Detection	W32.EICAR.16g1
Connector Info	Fingerprint (SHA-256)	2546dcf...6e9eedad
Comments	Filename	0M90PRxO.zip.part
	Filepath	C:\Users\admin\AppData\Local\Temp\0M90PRxO.zip.part
	File Size (bytes)	184
	Parent Fingerprint (SHA-256)	3147bd8...32de89c2
	Parent Filename	Firefox.exe

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

Applications

AMP Adaptor 4d4047dc-4791-477d-955f-6a0f182ae65b IRF	Edit Deregister
AMP Adaptor fe80e16e-cde8-4d7f-a836-545416ae56f4 IRF	Edit Deregister

These are applications external to FireAMP, such as Sourcefire's Defense Center, that you have authorized to access your business' data.

Here you can deauthorize registered applications, thus revoking their access to specific functionality, or you can deregister the applications, thus deauthorizing them and completely removing them from the FireAMP system.

You can currently authorize Defense Center appliances to receive streaming FireAMP events for integration with the Defense Center.

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.

Time	Status	Details	Repeat	Identify	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Jun 30, 2016 05:50:18.728 PM	●		0	alice	02:4A:00:14:8D:4B	Windows7...	Default >> Dot1X >> Default	Default >> Compliant_Device_A...	PermitAccess	10.62.148.26
Jun 30, 2016 05:49:26.479 PM	●			alice	02:4A:00:14:8D:4B	Windows7...	Default >> Dot1X >> Default	Default >> Compliant_Device_A...	PermitAccess	
Jun 30, 2016 05:49:34.437 PM	●				02:4A:00:14:8D:4B					
Jun 30, 2016 05:42:56.536 PM	●			alice	02:4A:00:14:8D:4B	Windows7...	Default >> Dot1X >> Default	Default >> Non-Compliant_Devis...	AMP_Profile	

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

COMPROMISED ENDPOINTS BY INCIDENTS

All endpoints | Connected | Disconnected

Incident Type	Count
Unknown	0
Insignificant	0
Distracting	0
Painful	1
Damaging	0
Catastrophic	0

IMPACT LEVEL

COMPROMISED ENDPOINTS BY INDICATORS

All endpoints | Connected | Disconnected

Indicator	Count
Unknown	0
None	0
Low	0
Medium	0
High	0

LIKELY IMPACT LEVEL

MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity
02:4A:00:14:8D:4B	alice	10.62.148.26	Threat Detected	AMP	Painful	Location/FBI Locations	Connected

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

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main menu has 'Endpoints' and 'Network Devices'. The breadcrumb trail is 'Endpoints > C0:4A:00:14:8D:4B'. The endpoint details are: MAC Address: C0:4A:00:14:8D:4B, Username: alice, Endpoint Profile: Windows7-Workstation, Current IP Address: 10.62.148.26, Location: . The 'Threats' tab is selected, showing a 'Threat Detected' event. The event details are: Type: INCIDENT, Severity: Painful, Reported by: AMP, Reported at: 2016-06-30 11:27:48.

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.

The screenshot shows the 'Compromised Endpoints' page in the Cisco Identity Services Engine (ISE) interface. The page displays two bar charts: 'COMPROMISED ENDPOINTS BY INCIDENTS' and 'COMPROMISED ENDPOINTS BY INDICATORS'. Below the charts is a table of endpoints. The table has columns for 'Source', 'Threat Severity', 'Logical NAD Location', 'Connectivity', 'Hostname', 'Identity Group', and 'Endpoint OS'. The table contains two rows of data. A context menu is open over the first row, showing options like 'CoA Session Result', 'CoA Session Terminate', 'CoA Port Bounce', 'CoA SNAet Session Query', 'CoA Session termination with port bounce', and 'CoA Session termination with port shutdown'. The 'Change Authorization' option is selected.

Source	Threat Severity	Logical NAD Location	Connectivity	Hostname	Identity Group	Endpoint OS
AMP	Painful	Location#A1 Locations	Disconnected		Workstation	
AMP	Painful	Location#A1 Locations	Connected		Workstation	

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**

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Logging' selected. The main content area is titled 'Node List > ISE21-3ek.example.com Debug Level Configuration'. It features an 'Edit' button and a 'Reset to Default' button. Below this is a table with columns for 'Component Name', 'Log Level', and 'Description'. The table contains one entry: TC-NAC with a log level of DEBUG and a description of 'TC-NAC log messages'. There is a radio button next to the TC-NAC component name.

Component Name	Log Level	Description
TC-NAC	DEBUG	TC-NAC log messages

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 » : « Dououreux »}, « 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 » : « Dououreux »},
« 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 » : « Dououreux »},
« 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}
```