تكوين ISE 2.1 NAC الذي يركز على التهديد (TC-NAC) مع AMP وخدمات Posture

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين NAC الذي يركز على التهديد باستخدام الحماية المتقدمة من البرامج الضارة (AMP) على محرك خدمات الهوية (ISE) 2.1. يمكن إستخدام مستويات خطورة التهديد ونتائج تقييم الثغرات الأمنية للتحكم بشكل ديناميكي في مستوى الوصول لنقطة نهاية أو مستخدم ما. يتم تغطية خدمات Posture أيضا كجزء من هذا المستند.

> **ملاحظة**: الغرض من الوثيقة هو وصف تكامل ISE 2.1 مع AMP، تظهر خدمات Posture كما هو مطلوب عندما نوفر AMP من ISE.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- محرك خدمة الهوية من Cisco
- الحماية المتقدمة من البرامج الضارة

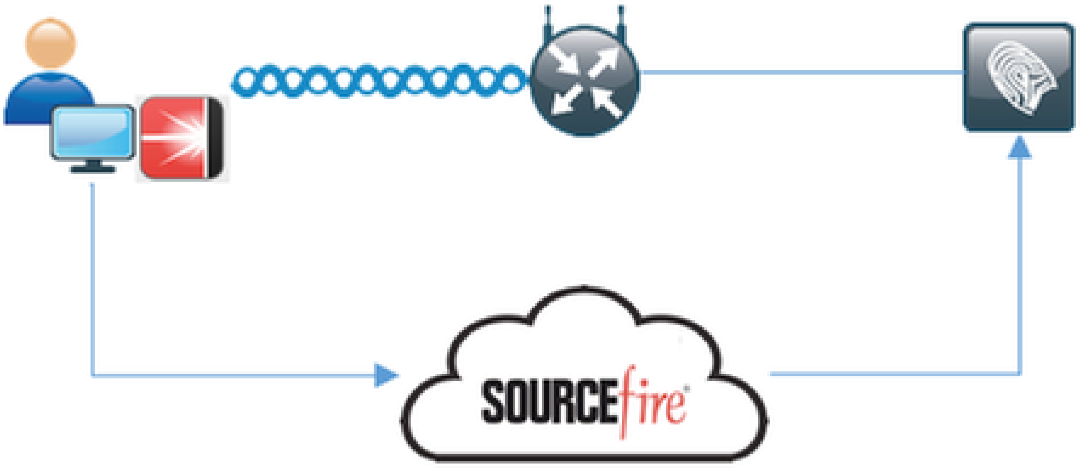
المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Identity Service Engine، الإصدار 2.1
- وحدة التحكم في شبكة LAN اللاسلكية (WLC) 8.0.121.0
- AnyConnect VPN Client 4.2.02075
- حزمة الخدمة 1 لنظام التشغيل Windows 7

التكوين

الرسم التخطيطي للشبكة



جريان تفصيلي

1. يتصل العميل بالشبكة، ويتم تعيين **AMP_Profile** وإعادة توجيه المستخدم إلى مدخل إمداد AnyConnect. إذا لم يتم اكتشاف AnyConnect على الجهاز، فسيتم تثبيت جميع الوحدات النمطية التي تم تكوينها (VPN، AMP، Posture). يتم دفع التهيئة لكل وحدة نمطية مع ملف التعريف هذا

2. بمجرد تثبيت AnyConnect، يتم تشغيل تقييم الوضع

3. تقوم الوحدة النمطية AMP Enabler (أداة تمكين AMP) بتثبيت موصل FireAMP

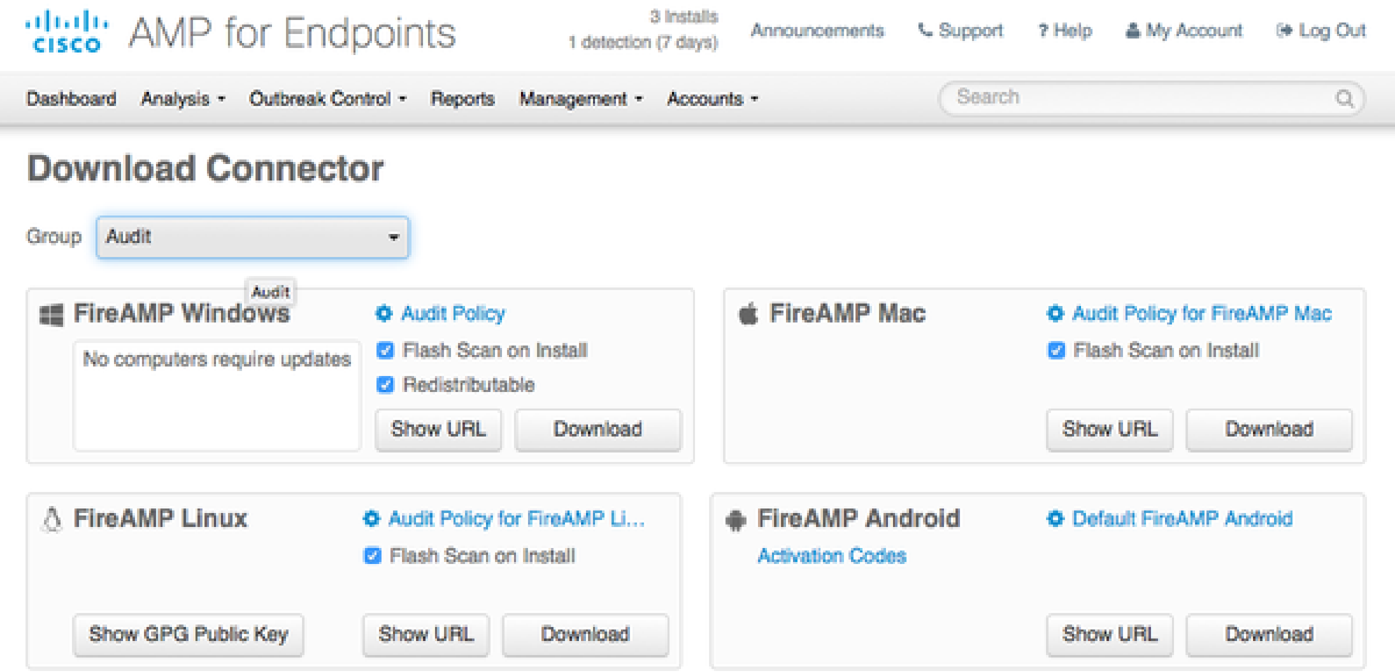
4. عندما يحاول العميل تنزيل برامج ضارة، يقوم موصل AMP برمي رسالة تحذير وإبلاغها إلى سحابة AMP

5. ترسل سحابة AMP هذه المعلومات إلى ISE

تكوين سحابة AMP

الخطوة 1. تنزيل الموصل من سحابة AMP

لتنزيل الموصل، انتقل إلى الإدارة > تنزيل الموصل. ثم حدد الكتابة وقم **بتنزيل** FireAMP (Windows و Android و Mac و Linux). في هذه الحالة تم تحديد **تدقيق** وملف تثبيت FireAMP لـ Windows.

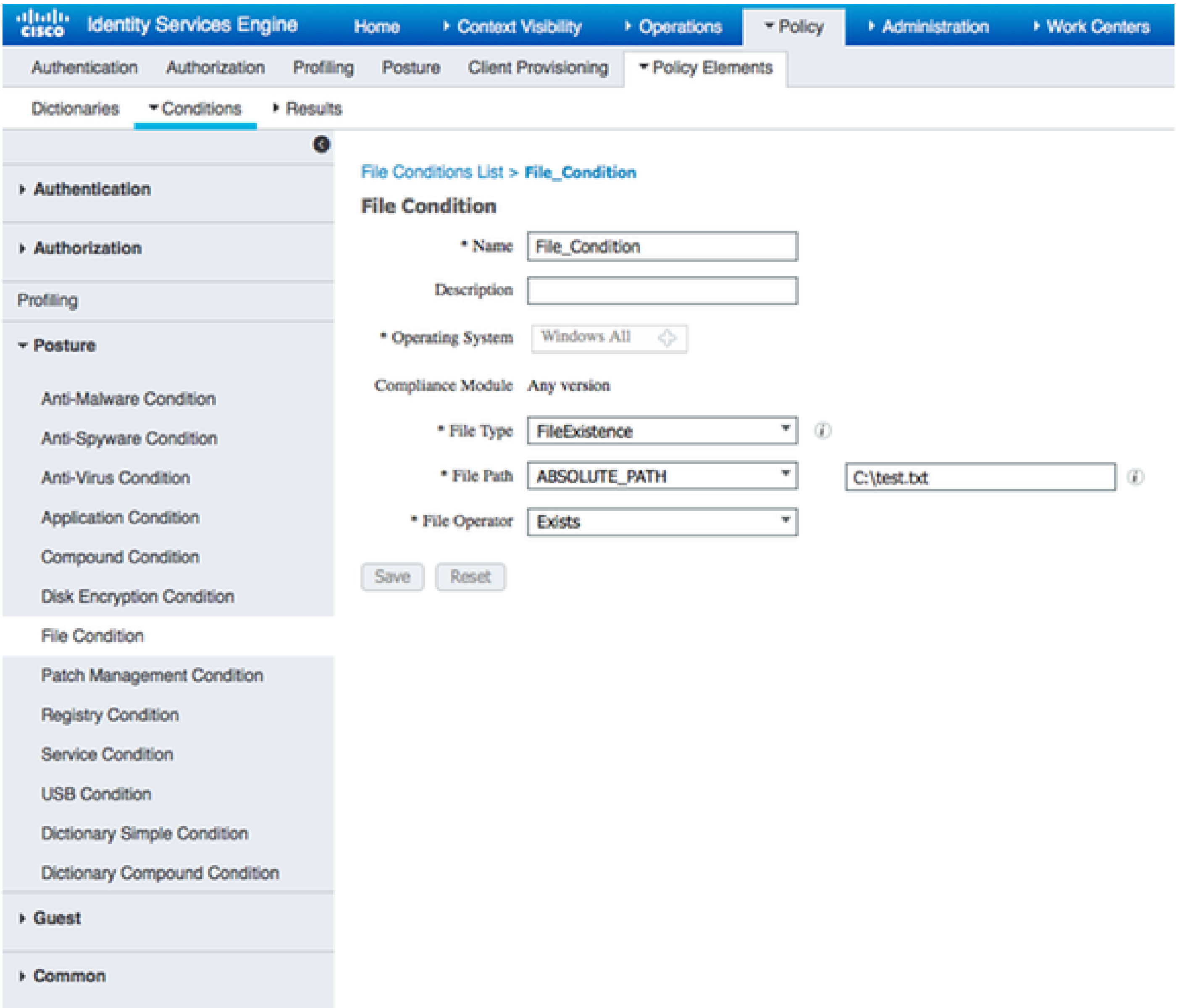


> **ملاحظة**: يؤدي تنزيل هذا الملف إلى إنشاء ملف .exe يسمى **Audit_FireAMPSetup.exe** في المثال. تم إرسال هذا الملف إلى خادم الويب ليكون متوفرا بمجرد أن يطلب المستخدم تكوين AMP.

تكوين ISE

الخطوة 1. تكوين سياسات وشروط الوضع

انتقل إلى السياسة > عناصر السياسة > الشروط > الوضع > حالة الملف.يمكنك أن ترى أنه تم إنشاء شرط بسيط لوجود الملف. يجب أن يكون الملف موجودا إذا كانت نقطة النهاية متوافقة مع السياسة التي تم التحقق منها بواسطة الوحدة النمطية للوضع:



File Conditions List > File_Condition

File Condition

* Name: File_Condition

Description:

* Operating System: Windows All

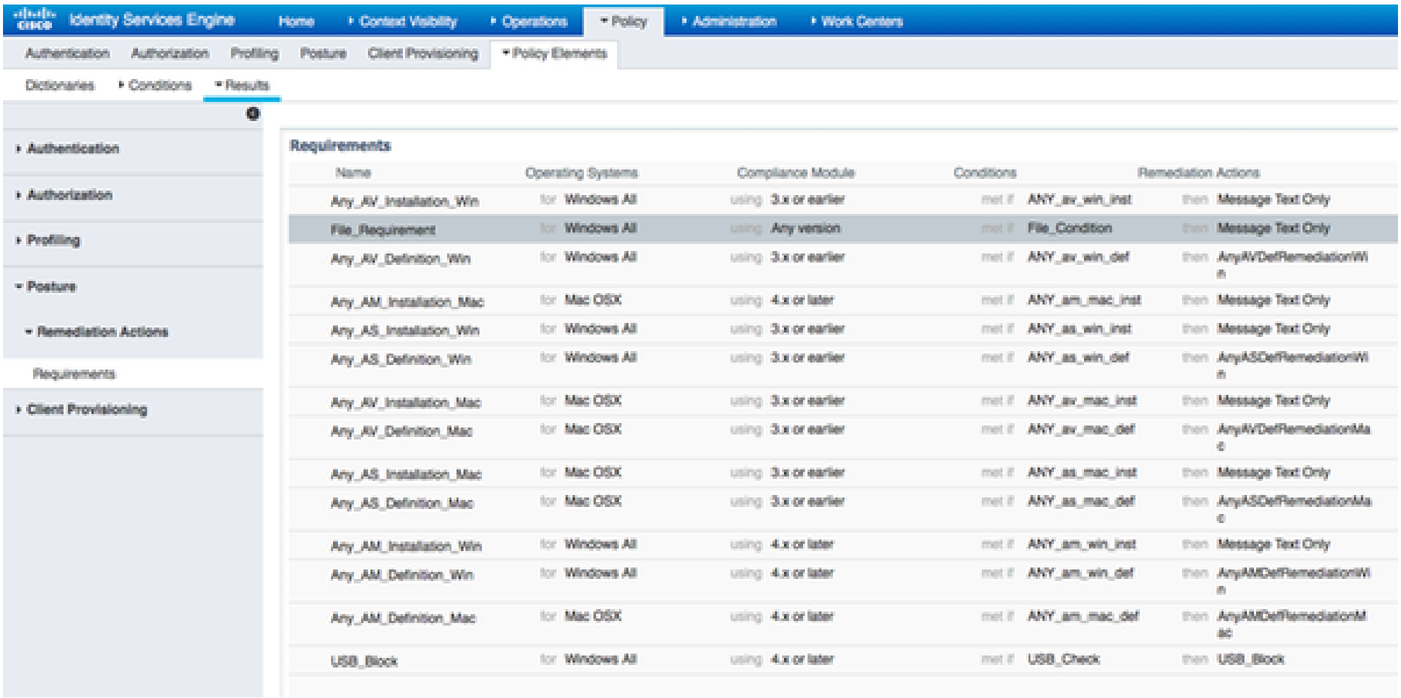
Compliance Module: Any version

* File Type: FileExistence

* File Path: ABSOLUTE_PATH C:\test.txt

* File Operator: Exists

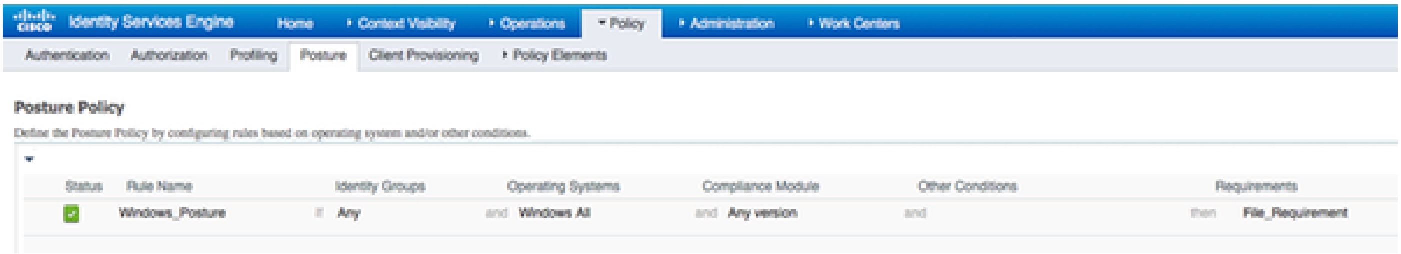
يتم إستخدام هذا الشرط لمتطلب:



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

يتم إستخدام هذا المتطلب في نهج الوضع لأنظمة Microsoft Windows:



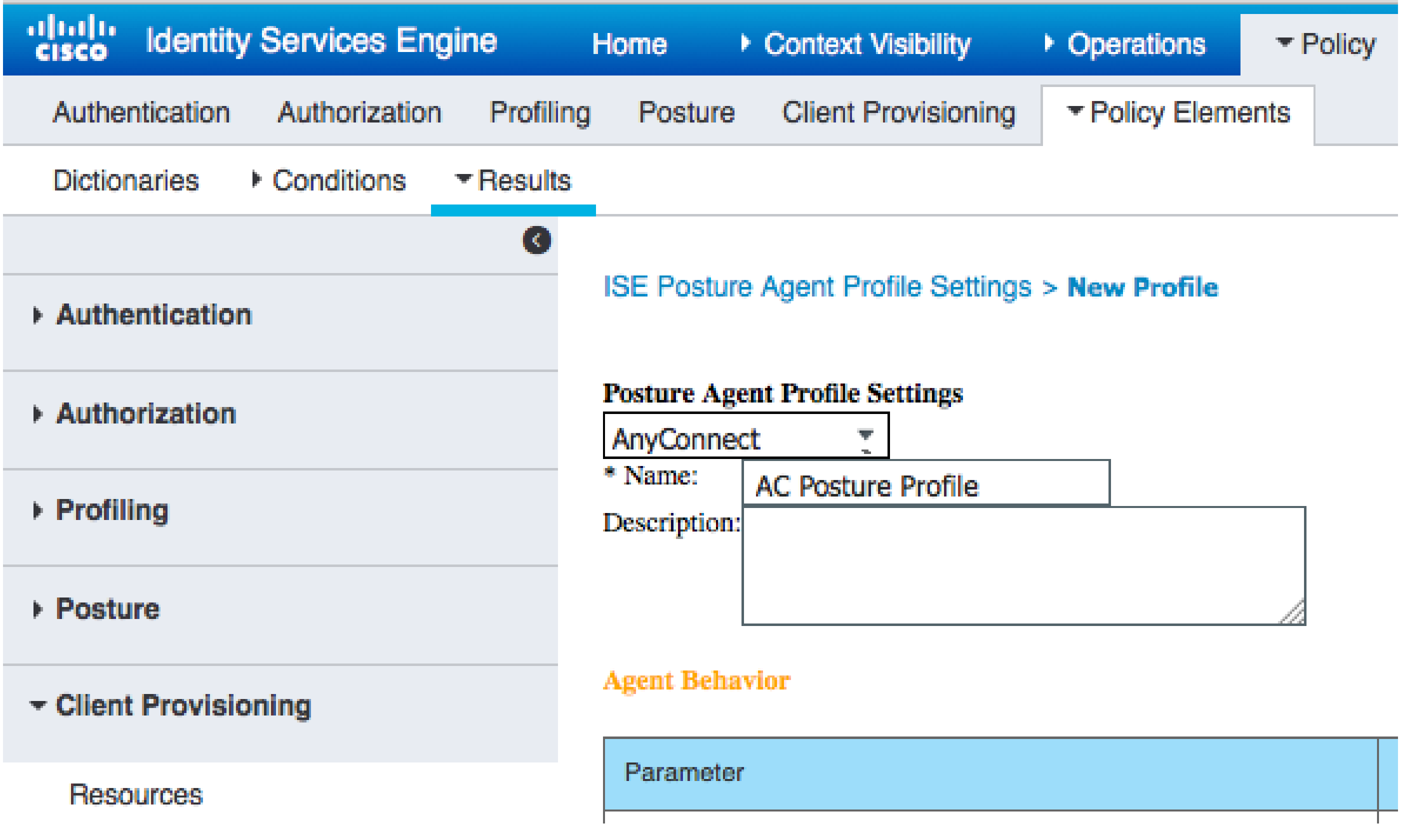
Posture Policy

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

Status	Rule Name		Identity Groups		Operating Systems		Compliance Module		Other Conditions		Requirements
✓	Windows_Posture	If	Any	and	Windows All	and	Any version	and		then	File_Requirement

الخطوة 2. تكوين ملف تعريف الوضع

- انتقل إلى السياسة > عناصر السياسة > النتائج > إمداد العميل > الموارد وقم بإضافة عامل التحكم في الدخول إلى الشبكة (NAC) أو ملف تعريف وضعية وكيل AnyConnect
- تحديد AnyConnect



ISE Posture Agent Profile Settings > New Profile

Posture Agent Profile Settings

AnyConnect

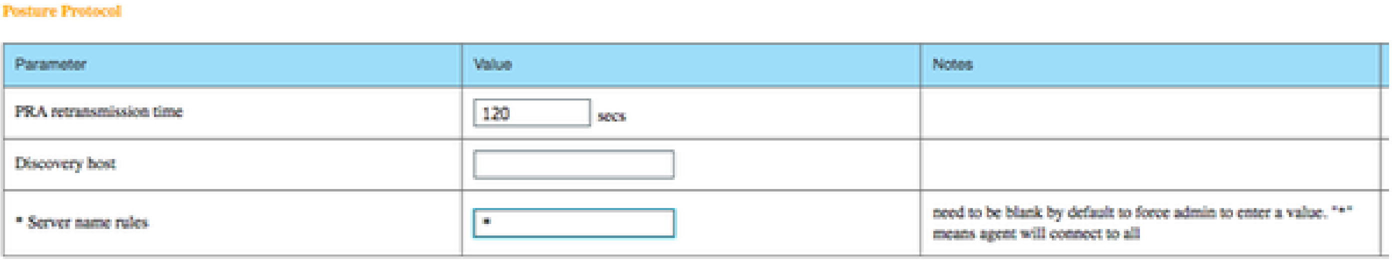
* Name: AC Posture Profile

Description:

Agent Behavior

Parameter

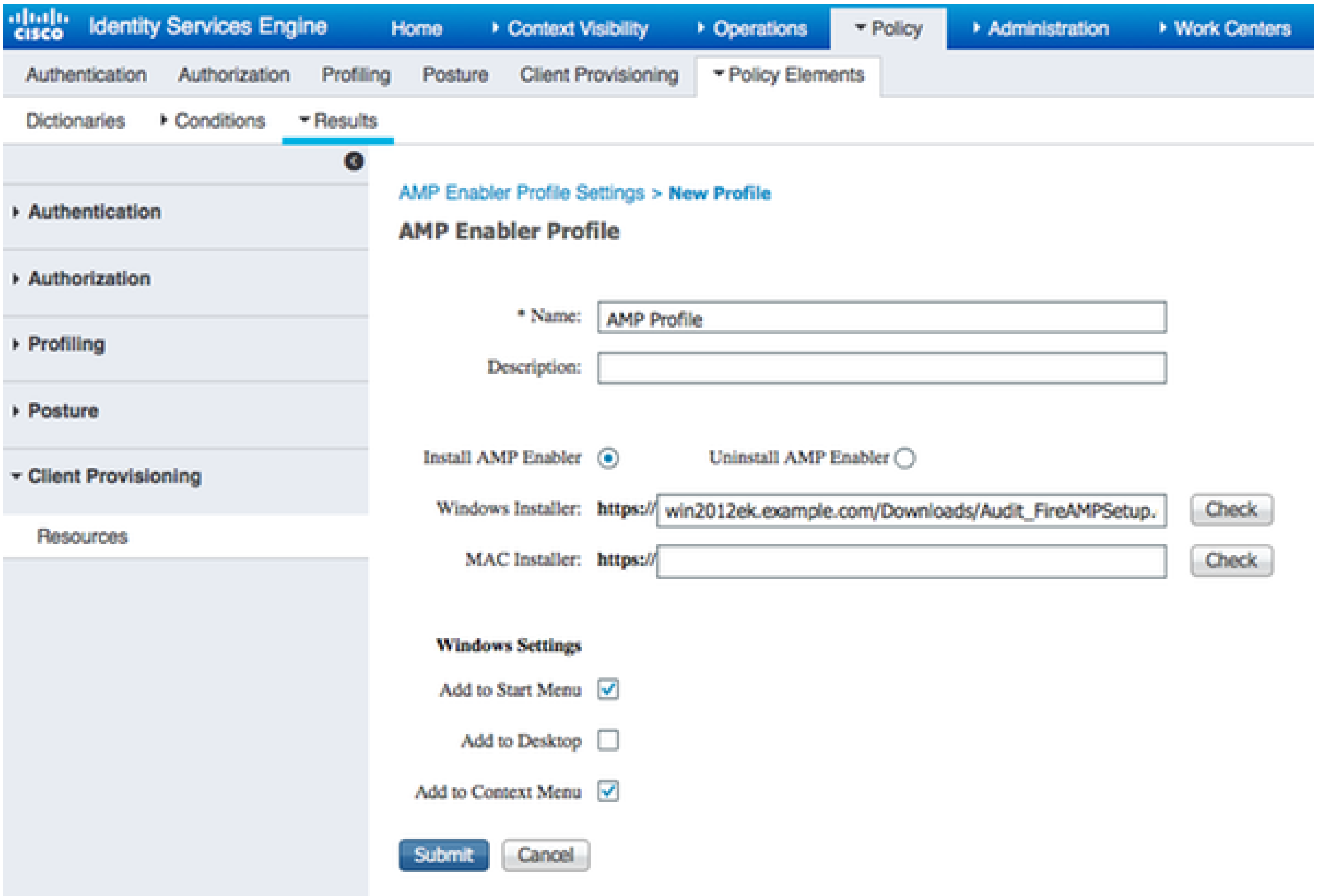
- من قسم بروتوكول الوضع، أضف * للسماح للوكيل بالاتصال بجميع الخوادم


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

الخطوة 3. تكوين ملف تعريف AMP

يحتوي ملف تعريف AMP على معلومات حول موقع Windows Installer. تم تنزيل Windows Installer في وقت سابق من سحابة AMP. يجب الوصول إليها من جهاز العميل. يجب أن تكون شهادة خادم HTTPS، حيث يوجد المثبت، موثوق بها بواسطة جهاز العميل أيضا.



AMP Enabler Profile Settings > New Profile

AMP Enabler Profile

* Name: AMP Profile

Description:

Install AMP Enabler ● Uninstall AMP Enabler ○

Windows Installer: https:// win2012ek.example.com/Downloads/Audit_FireAMPSetup.

MAC Installer: https://

Windows Settings

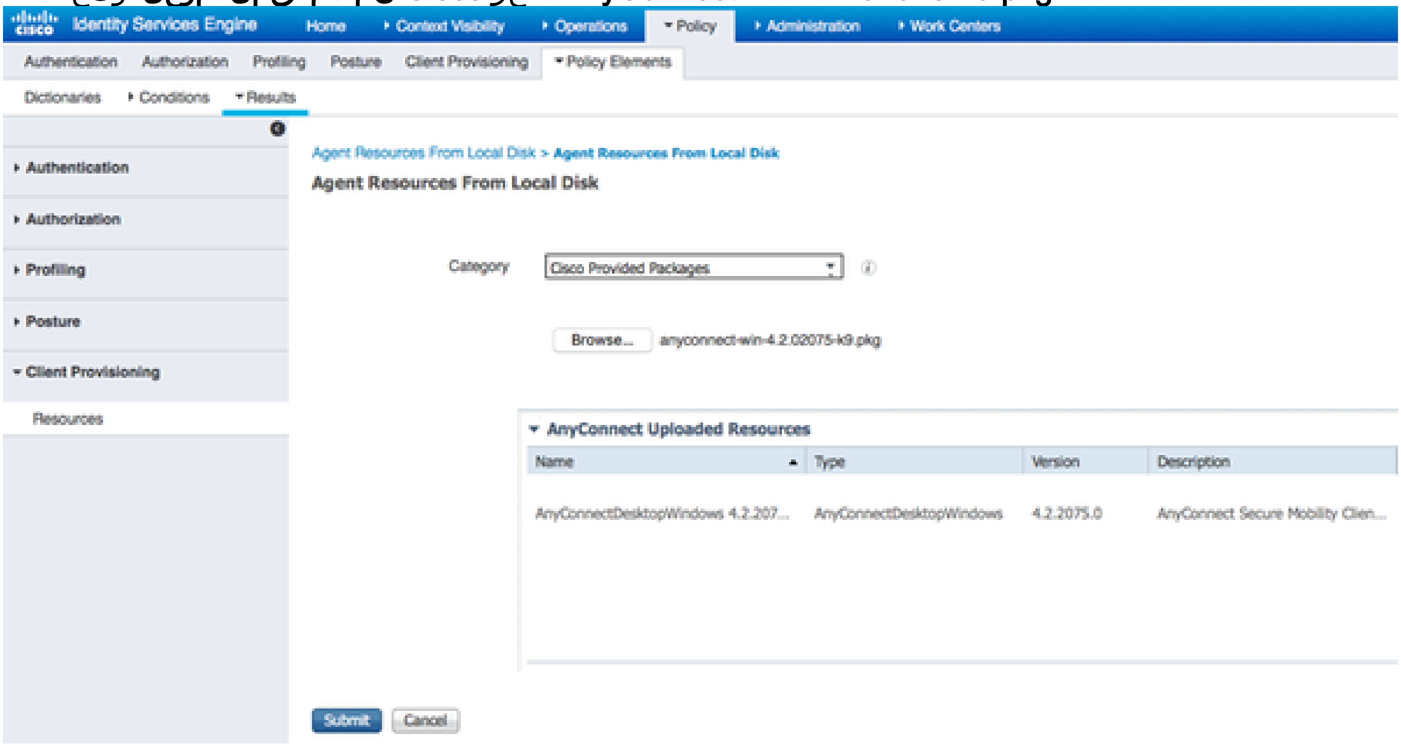
Add to Start Menu ☑

Add to Desktop □

Add to Context Menu ☑

الخطوة 2. تحميل التطبيقات وملف تعريف XML إلى ISE

- تنزيل التطبيق يدويا من موقع Cisco الرسمي: **AnyConnect-win-4.2.02075-k9.pkg**
- على ISE، انتقل إلى السياسة > عناصر السياسة > النتائج > إمداد العميل > الموارد، وقم بإضافة **موارد الوكيل من القرص المحلي**
- أختر **الحزم المقدمة من Cisco** وحدد **AnyConnect-win-4.2.02075-k9.pkg**



Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

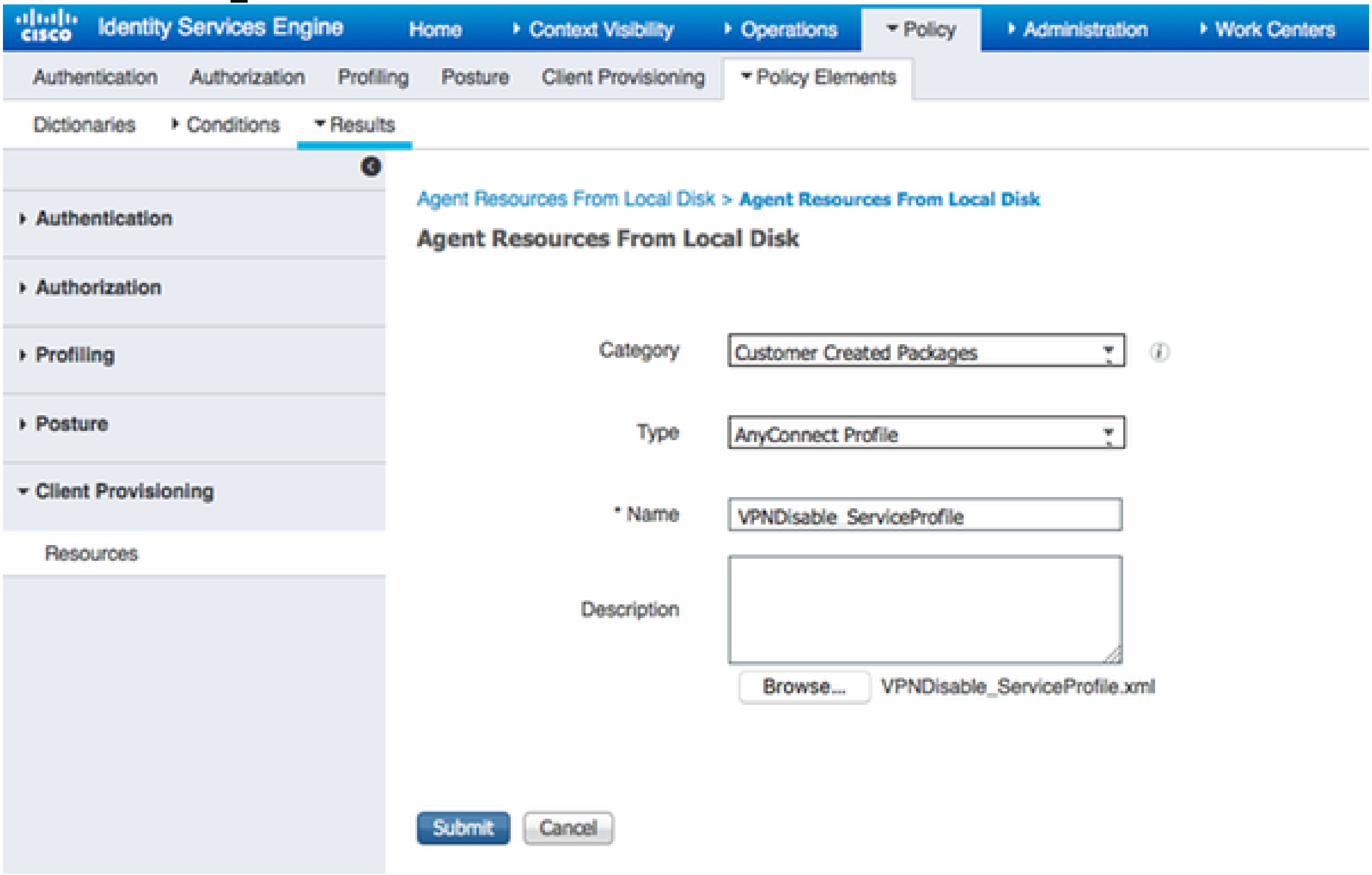
Category: Cisco Provided Packages

anyconnect-win-4.2.02075-k9.pkg

AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.2.207...	AnyConnectDesktopWindows	4.2.2075.0	AnyConnect Secure Mobility Clien...

- انتقل إلى السياسة > عناصر السياسة > النتائج > إمداد العميل > الموارد وأضف **موارد الوكيل من القرص المحلي**
- أختر **الحزم التي أنشأها العميل** واكتب **توصيف AnyConnect**. حدد **VPNDisable_ServiceProfile.xml**



Category: Customer Created Packages

Type: AnyConnect Profile

* Name: VPNDisable_ServiceProfile

Description:

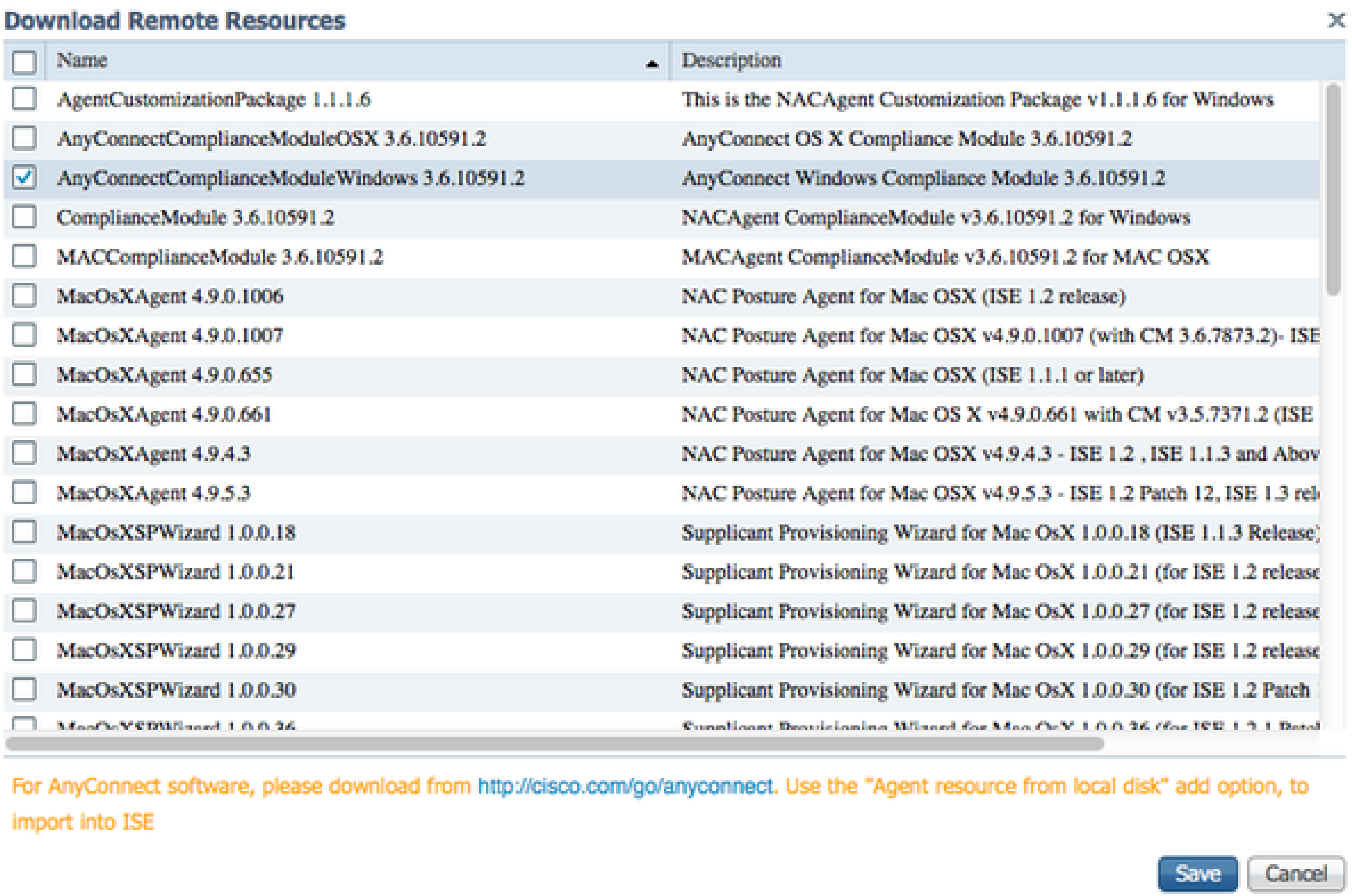
Browse... VPNDisable_ServiceProfile.xml

ملاحظة: يتم إستخدام **VPNDisable_ServiceProfile.xml** لإخفاء عنوان VPN، نظرا لأن هذا المثال لا يستخدم وحدة VPN النمطية. هذا هو محتوى **VPNDisable_ServiceProfile.xml**:

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

الخطوة 3. تنزيل وحدة توافق AnyConnect

- انتقل إلى السياسة > عناصر السياسة > النتائج > إمداد العميل > الموارد وأضف **موارد الوكيل من موقع Cisco**
- حدد **AnyConnect Windows Compliance Module 3.6.10591.2** وانقر فوق **حفظ**



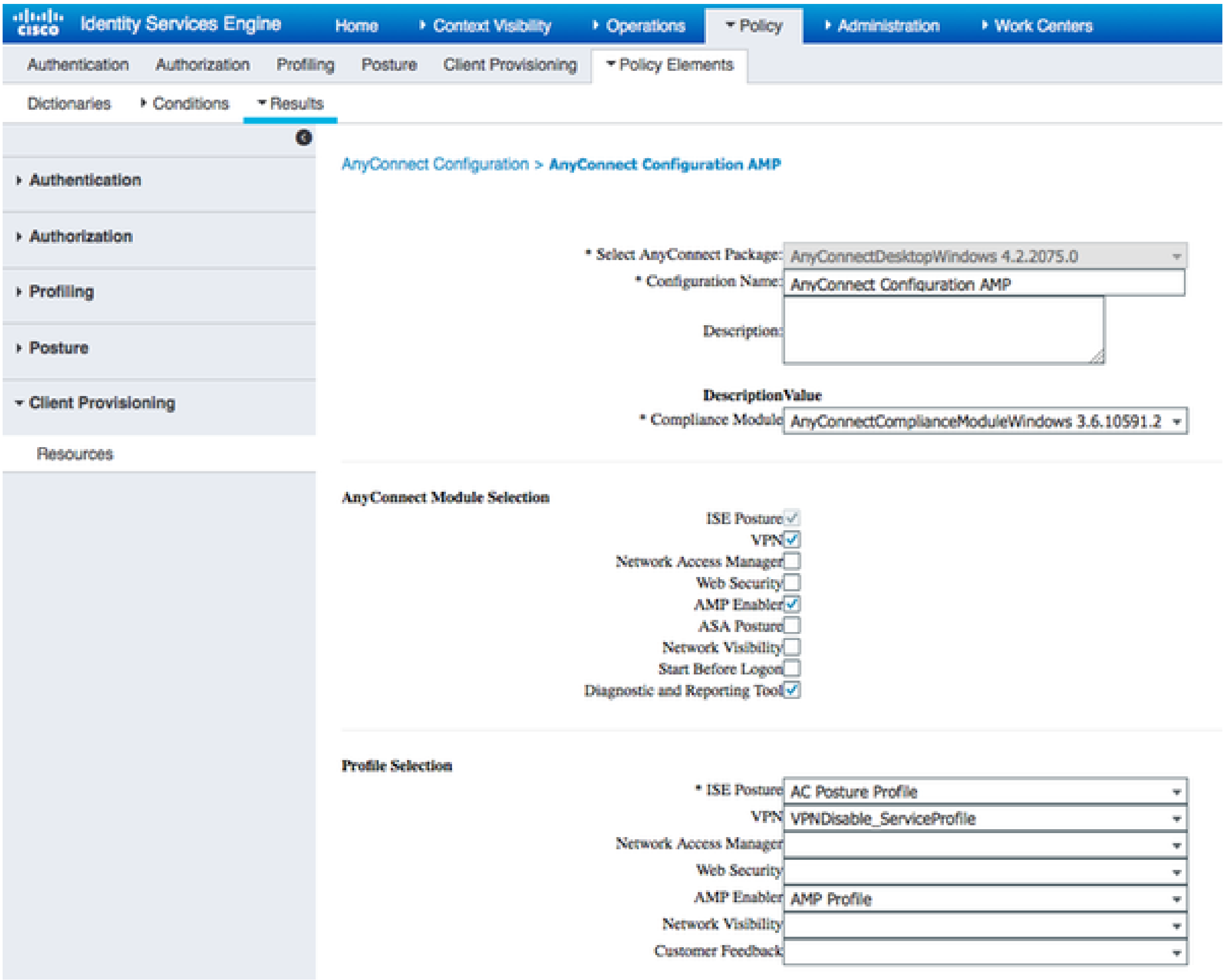
Download Remote Resources

☐	Name	Description
☐	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
☐	AnyConnectComplianceModuleOSX 3.6.10591.2	AnyConnect OS X Compliance Module 3.6.10591.2
☑	AnyConnectComplianceModuleWindows 3.6.10591.2	AnyConnect Windows Compliance Module 3.6.10591.2
☐	ComplianceModule 3.6.10591.2	NACAgent ComplianceModule v3.6.10591.2 for Windows
☐	MACComplianceModule 3.6.10591.2	MACAgent ComplianceModule v3.6.10591.2 for MAC OSX
☐	MacOsXAgent 4.9.0.1006	NAC Posture Agent for Mac OSX (ISE 1.2 release)
☐	MacOsXAgent 4.9.0.1007	NAC Posture Agent for Mac OSX v4.9.0.1007 (with CM 3.6.7873.2)- ISE
☐	MacOsXAgent 4.9.0.655	NAC Posture Agent for Mac OSX (ISE 1.1.1 or later)
☐	MacOsXAgent 4.9.0.661	NAC Posture Agent for Mac OS X v4.9.0.661 with CM v3.5.7371.2 (ISE
☐	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Abov
☐	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3 rel
☐	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1.3 Release)
☐	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE 1.2 release
☐	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 release
☐	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 release
☐	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE 1.2 Patch
☐	MacOsXSPWizard 1.0.0.36	Supplicant Provisioning Wizard for Mac OsX 1.0.0.36 (for ISE 1.2.1 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

الخطوة 4. إضافة تكوين AnyConnect

- انتقل إلى السياسة > عناصر السياسة > النتائج > إمداد العميل > الموارد، وقم بإضافة **تكوين AnyConnect**
- قم بتكوين الاسم وحدد وحدة التوافق النمطية وجميع وحدات AnyConnect النمطية المطلوبة (VPN، AMP، و Posture)
- في **تحديد التوصيف**، أختر التوصيف الذي تم تكوينه سابقا لكل وحدة نمطية



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

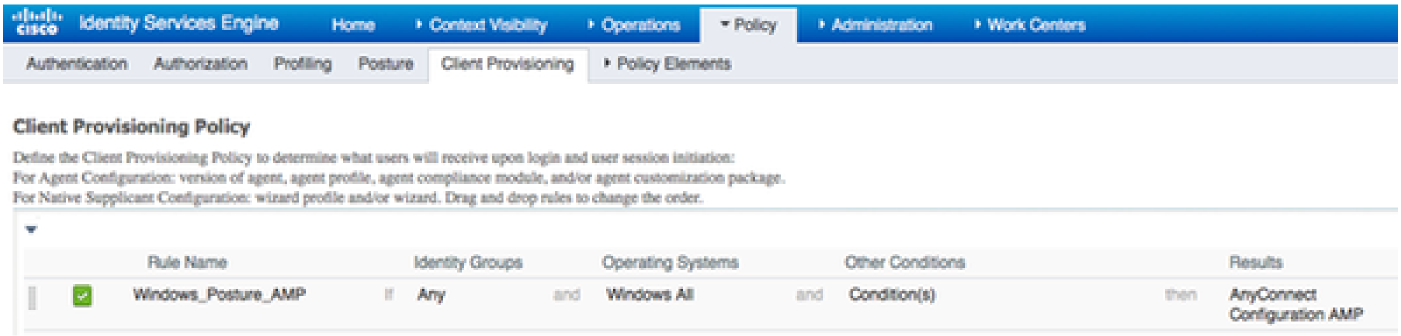
ISE Posture ☑
VPN ☑
Network Access Manager □
Web Security □
AMP Enabler ☑
ASA Posture □
Network Visibility □
Start Before Logon □
Diagnostic and Reporting Tool ☑

Profile Selection

* ISE Posture AC Posture Profile
VPN VPNDisable_ServiceProfile
Network Access Manager
Web Security
AMP Enabler AMP Profile
Network Visibility
Customer Feedback

الخطوة 5. تكوين قواعد إمداد العميل

تتم الإشارة إلى تكوين AnyConnect الذي تم إنشاؤه مسبقا في قواعد **إمداد العميل**



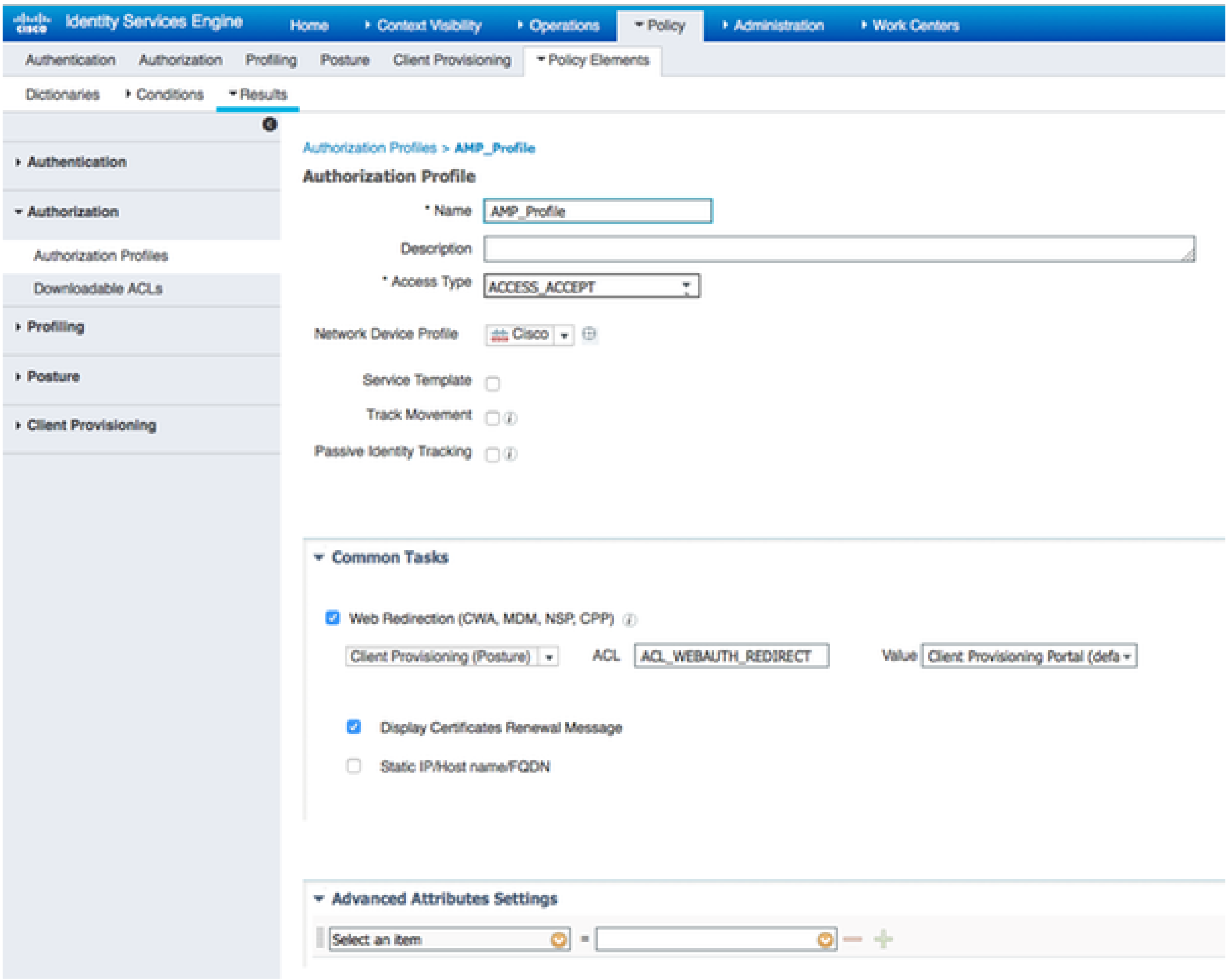
Client Provisioning Policy

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
☑	Windows_Posture_AMP	If	Any	and	Windows All	and	Condition(s)	then	AnyConnect Configuration AMP

الخطوة 6. تكوين سياسات التخويل

يتم أولا إعادة التوجيه إلى مدخل توفير العميل. يتم إستخدام سياسات التخويل القياسية للوضع.



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

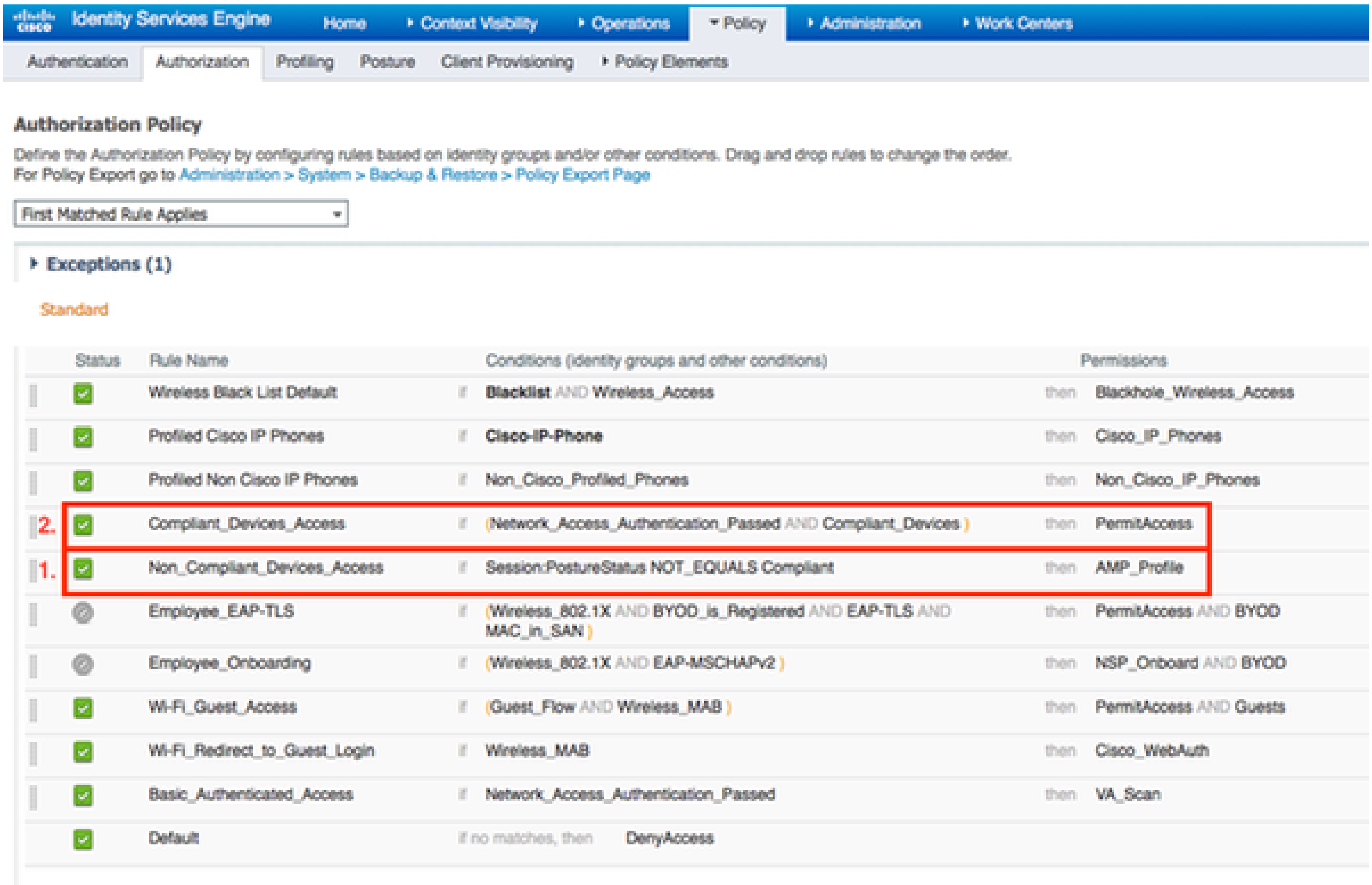
☑ Display Certificates Renewal Message

□ Static IP/Host name/FQDN

Advanced Attributes Settings

Select an item =

بعد ذلك، وبمجرد التوافق، يتم تعيين الوصول الكامل



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

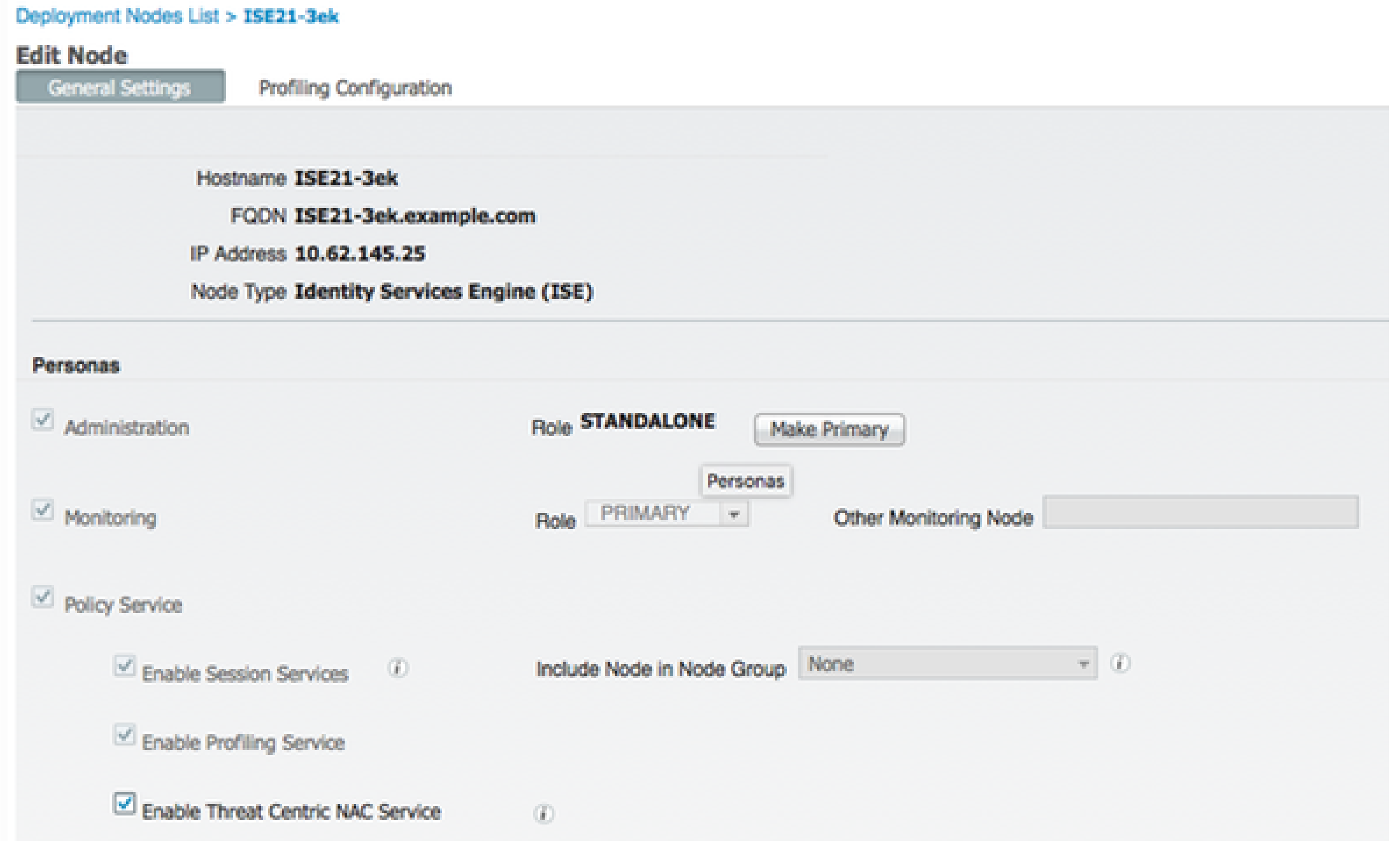
▸ Exceptions (1)

Standard

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

الخطوة 7. تمكين خدمات TC-NAC

تمكين خدمات TC-NAC تحت الإدارة > النشر > عقدة التحرير. حدد خانة الاختيار **تمكين خدمة NAC التي ترتكز على التهديد**.


Deployment Nodes List > **ISE21-3ek**

Edit Node

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

Personas

☑ Administration — Role **STANDALONE** [Make Primary]

☑ Monitoring — Role PRIMARY ▾ — Other Monitoring Node

☑ Policy Service

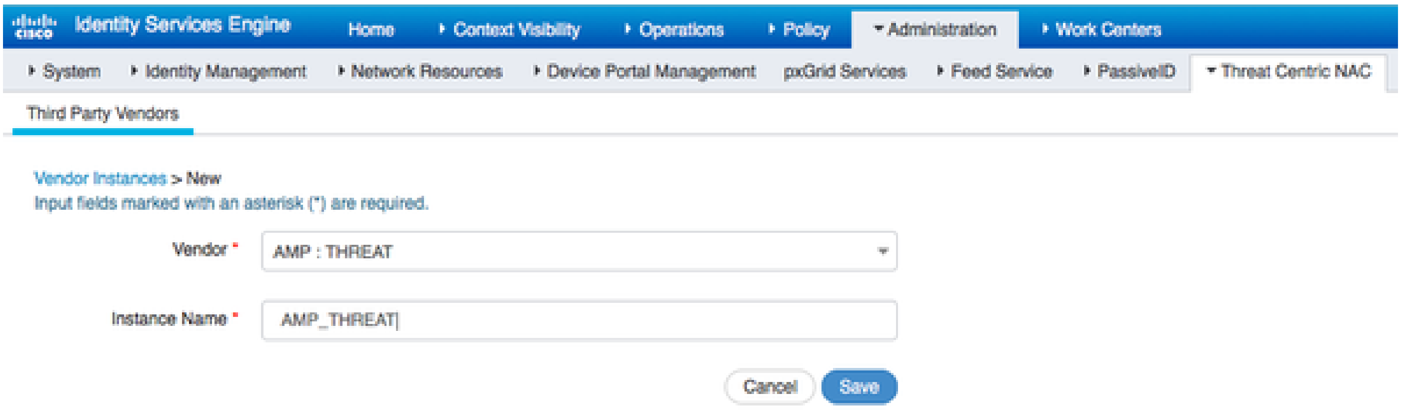
☑ Enable Session Services — Include Node in Node Group None ▾

☑ Enable Profiling Service

☑ Enable Threat Centric NAC Service

الخطوة 8. تكوين مهايئ AMP

انتقل إلى الإدارة > NAC الذي يركز على التهديدات > موردي الجهات الخارجية > إضافة. انقر على **حفظ**



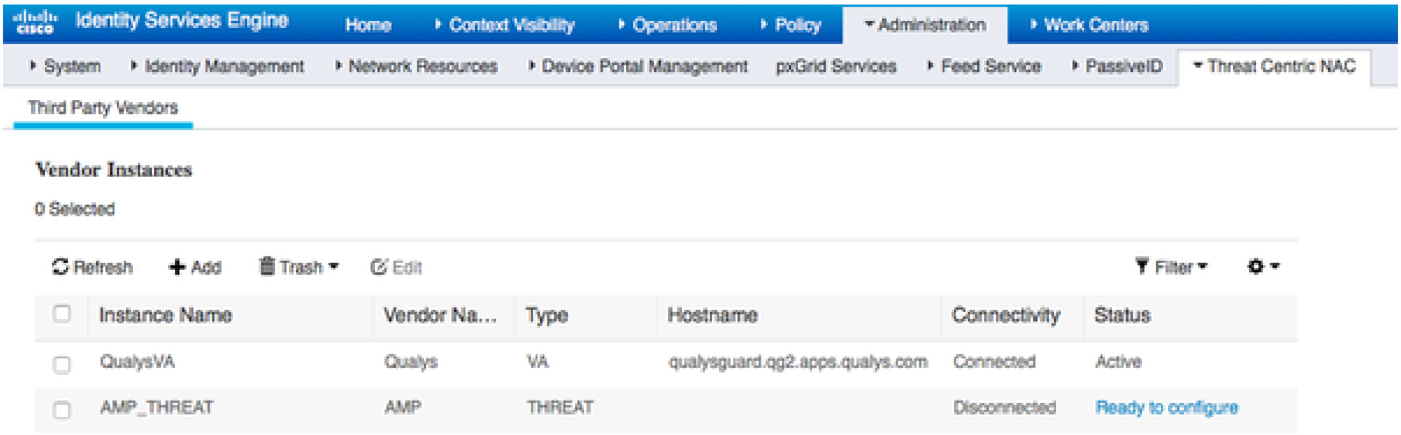
Vendor Instances > New

Input fields marked with an asterisk (*) are required.

Vendor * AMP : THREAT

Instance Name * AMP_THREAT

يجب الانتقال إلى **حالة "جاهز للتكوين"**. انقر فوق **جاهز للتكوين**

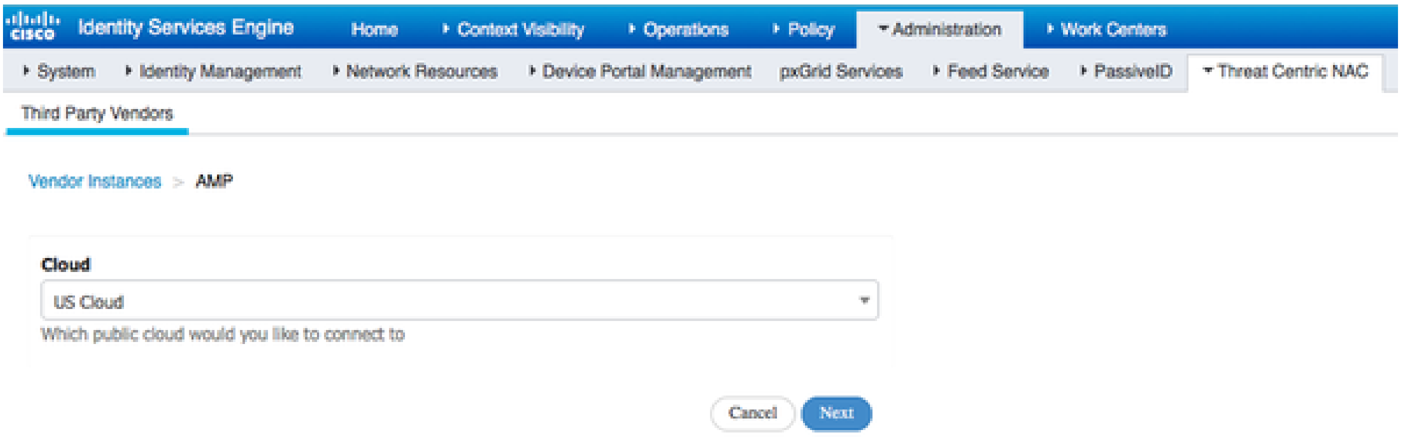


Vendor Instances

0 Selected

	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

حدد **سحابة** وانقر على **التالي**



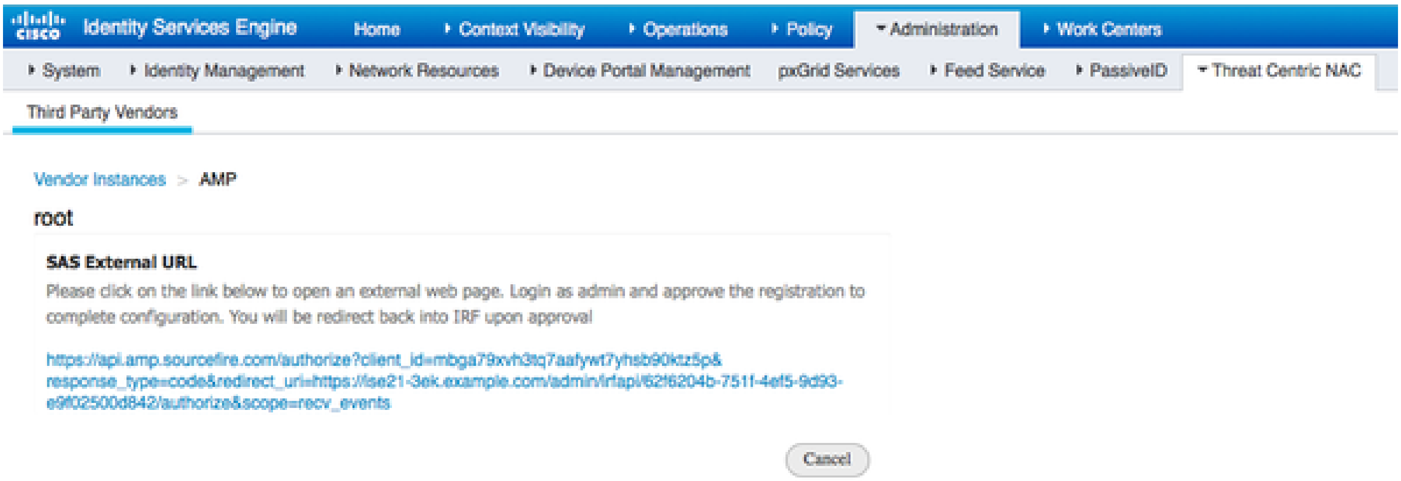
Vendor Instances > AMP

Cloud

US Cloud

Which public cloud would you like to connect to

انقر فوق إرتباط FireAMP وتسجيل الدخول كمسؤول في FireAMP.



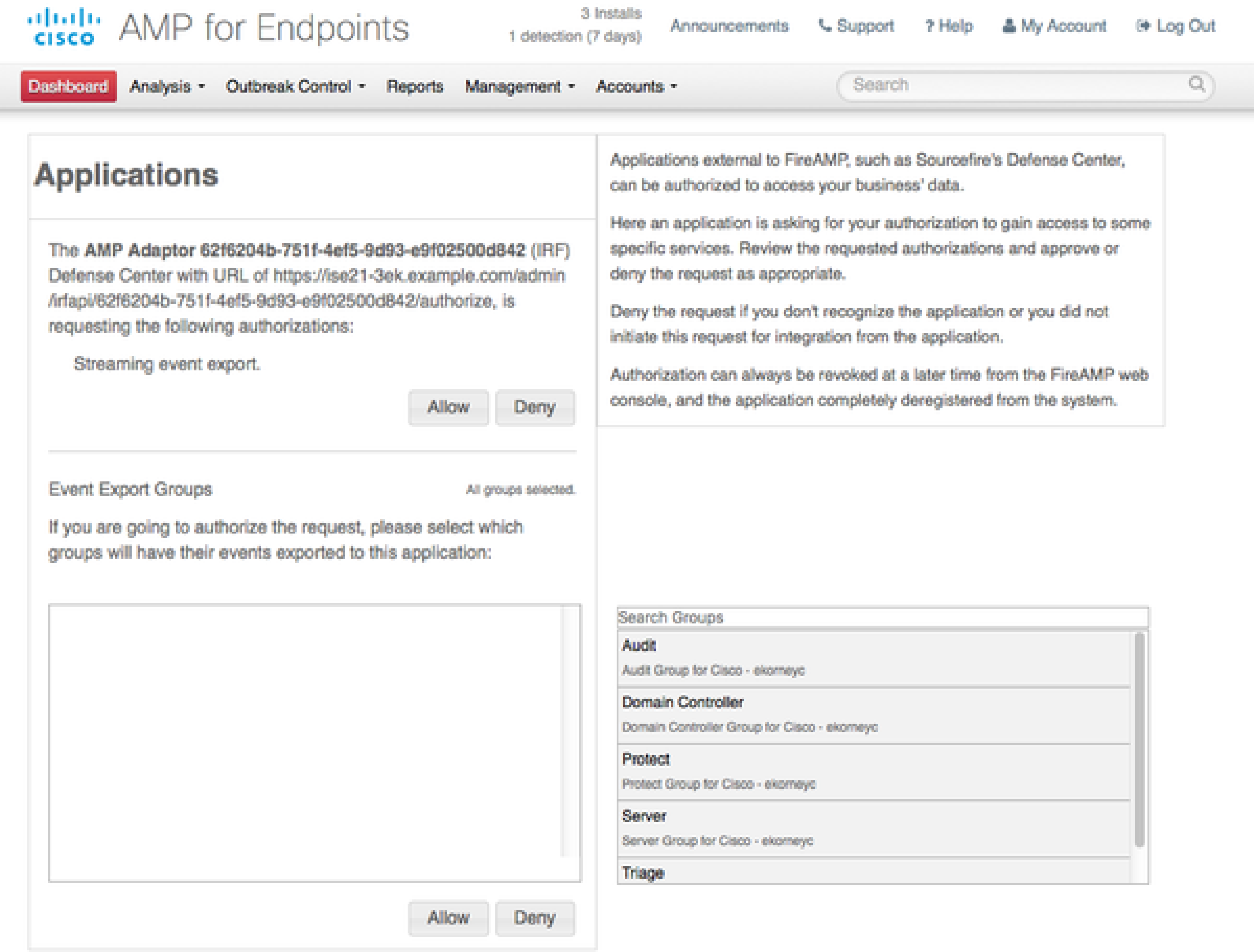
root

SAS External URL

Please click on the link below to open an external web page. Login as admin and approve the registration to complete configuration. You will be redirect back into IRF upon approval

https://api.amp.sourcefire.com/authorize?client_id=mbga79xvh3tq7aafywt7yhsb90ktz5p&response_type=code&redirect_uri=https://ise21-3ek.example.com/admin/irfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize&scope=recv_events

انقر فوق **السماح** في لوحة **التطبيقات** لتخويل طلب تصدير حدث الدفق. بعد هذا الإجراء، تتم إعادة توجيهك إلى Cisco ISE



Applications

The **AMP Adaptor 62f6204b-751f-4ef5-9d93-e9f02500d842** (IRF) Defense Center with URL of https://ise21-3ek.example.com/admin/irfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize, is requesting the following authorizations:

Streaming event export.

Applications external to FireAMP, such as Sourcefire's Defense Center, can be authorized to access your business' data.

Here an application is asking for your authorization to gain access to some specific services. Review the requested authorizations and approve or deny the request as appropriate.

Deny the request if you don't recognize the application or you did not initiate this request for integration from the application.

Authorization can always be revoked at a later time from the FireAMP web console, and the application completely deregistered from the system.

Event Export Groups

All groups selected.

If you are going to authorize the request, please select which groups will have their events exported to this application:

Audit
Audit Group for Cisco - ekorneyc

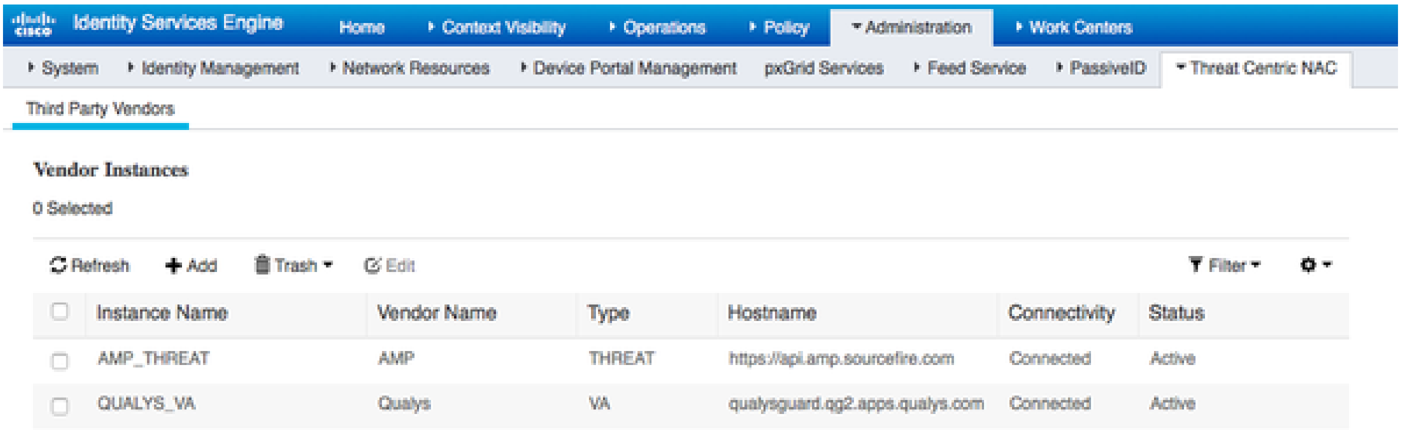
Domain Controller
Domain Controller Group for Cisco - ekorneyc

Protect
Protect Group for Cisco - ekorneyc

Server
Server Group for Cisco - ekorneyc

Triage

حدد الأحداث (على سبيل المثال، التنزيل المريب، الاتصال بمجال مريب، البرامج الضارة المنفذة، تطبيق Java Compromise) التي ترغب في مراقبتها. يتم عرض ملخص تكوين مثيل المحول في صفحة ملخص التكوين. انتقالات مثيل المحول إلى حالة الاتصال/النشاط.



Vendor Instances

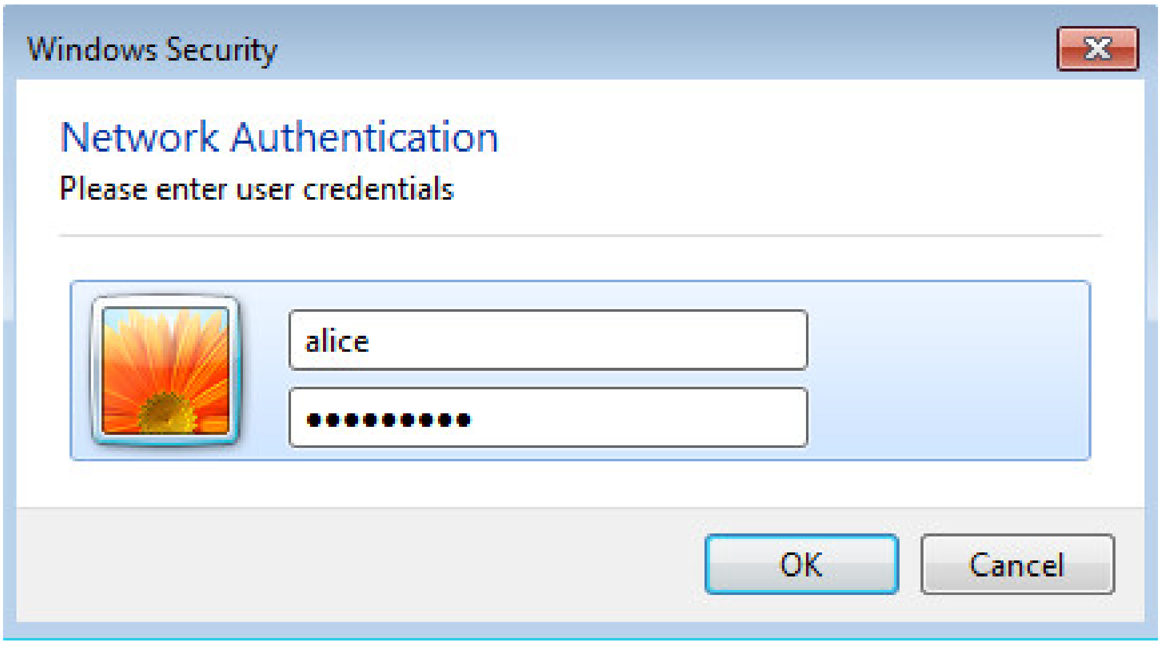
0 Selected

□	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

التحقق من الصحة

نقطة النهاية

الاتصال بالشبكة اللاسلكية عبر PEAP (MSCHAPv2).



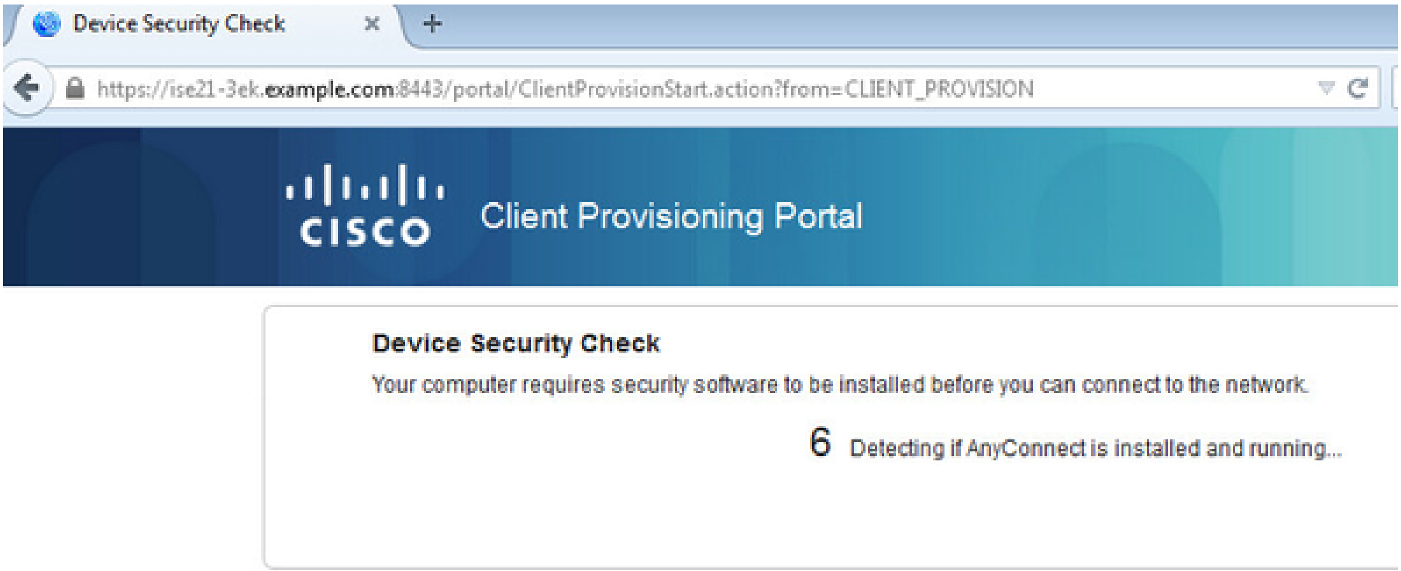
Network Authentication

Please enter user credentials

alice

••••••••••

بمجرد إجراء عملية إعادة التوجيه المتصلة إلى مدخل إمداد العميل.



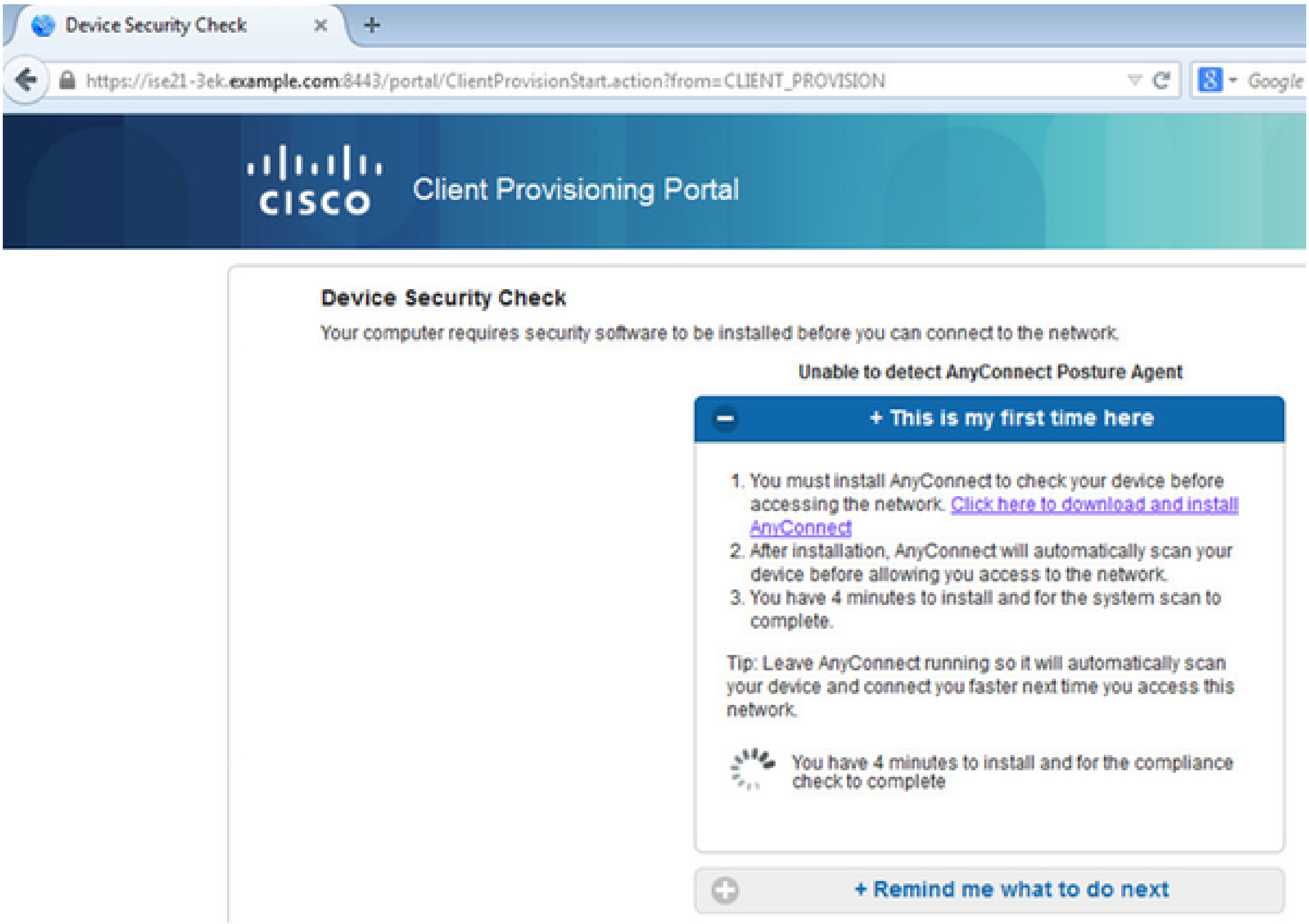
Device Security Check
https://ise21-3ek.example.com:8443/portal/ClientProvisionStart.action?from=CLIENT_PROVISION
CISCO
Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

6 Detecting if AnyConnect is installed and running...

وانظر لأنه لم يتم تثبيت أي شيء على جهاز العميل، تطلب ISE تثبيت عميل AnyConnect.



Device Security Check
https://ise21-3ek.example.com:8443/portal/ClientProvisionStart.action?from=CLIENT_PROVISION
Google
CISCO
Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect AnyConnect Posture Agent

+ This is my first time here

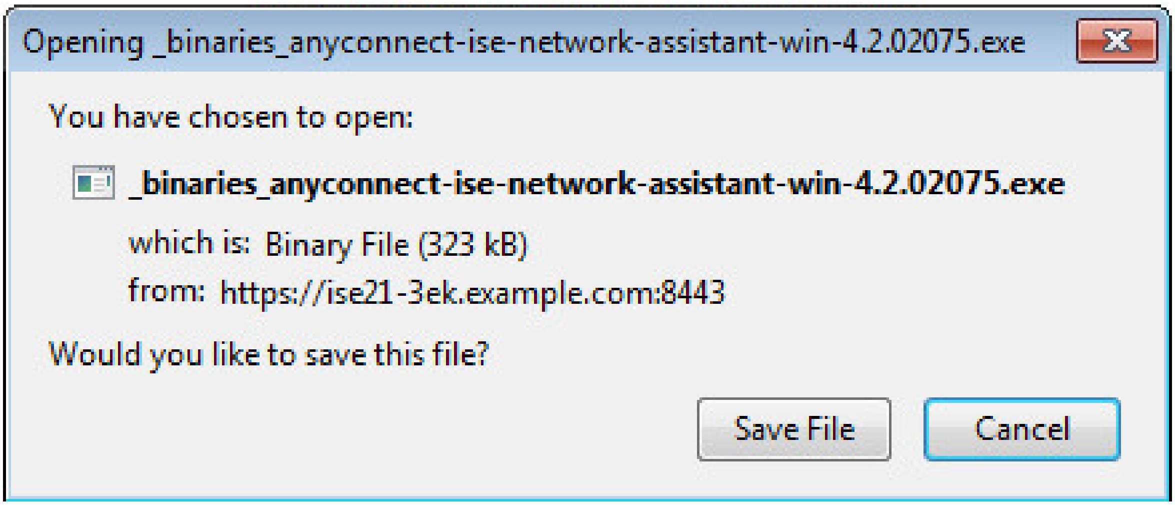
1. You must install AnyConnect to check your device before accessing the network. Click here to download and install AnyConnect
2. After installation, AnyConnect will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave AnyConnect running so it will automatically scan your device and connect you faster next time you access this network.

You have 4 minutes to install and for the compliance check to complete

+ Remind me what to do next

يجب تنزيل تطبيق مساعد إعداد الشبكة (NSA) وتشغيله من جهاز العميل.



Opening _binaries_anyconnect-ise-network-assistant-win-4.2.02075.exe

You have chosen to open:

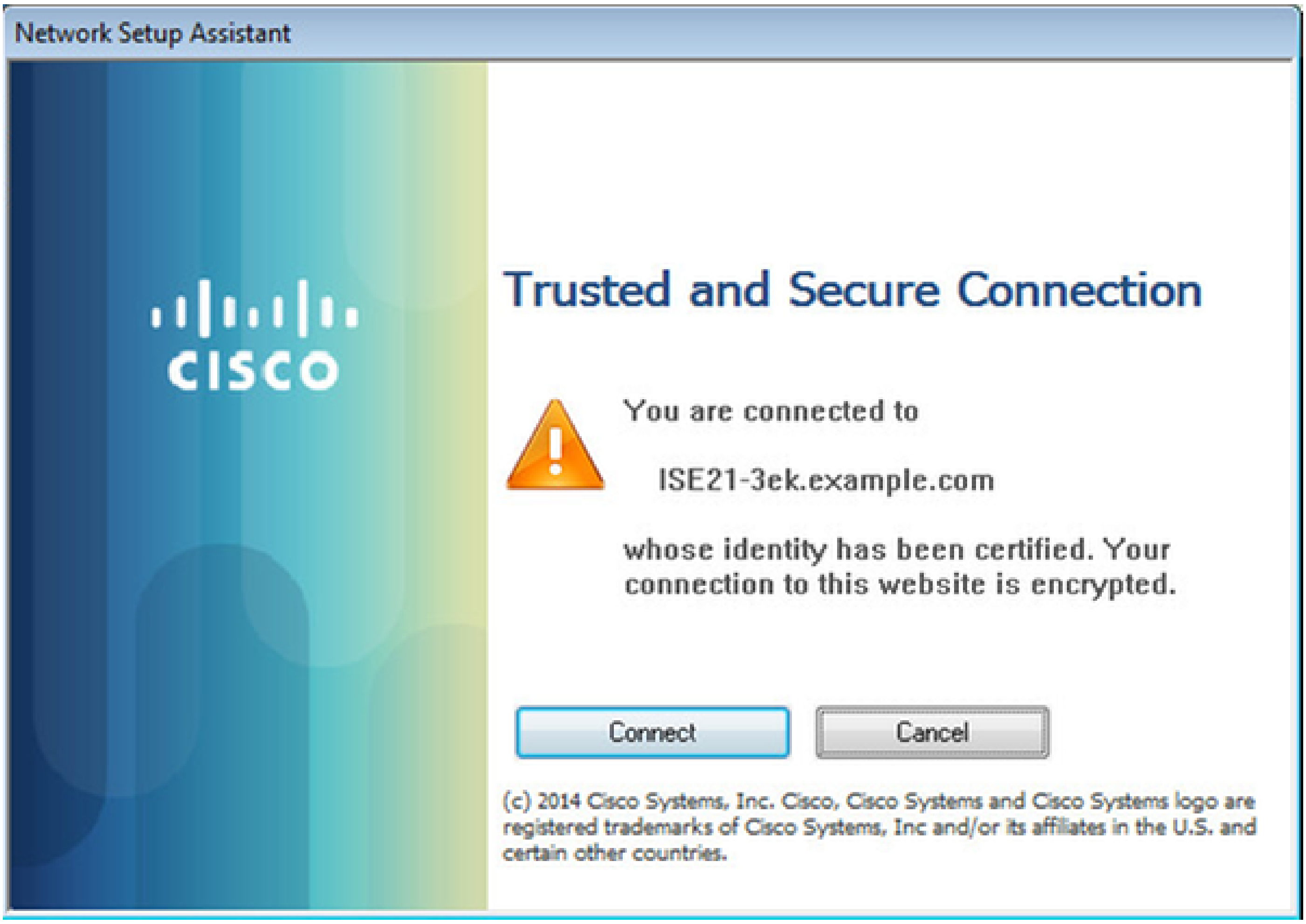
_binaries_anyconnect-ise-network-assistant-win-4.2.02075.exe

which is: Binary File (323 kB)

from: https://ise21-3ek.example.com:8443

Would you like to save this file?

تتم الإدارة بتركيب المكونات وملفات التعريف المطلوبة.



Network Setup Assistant

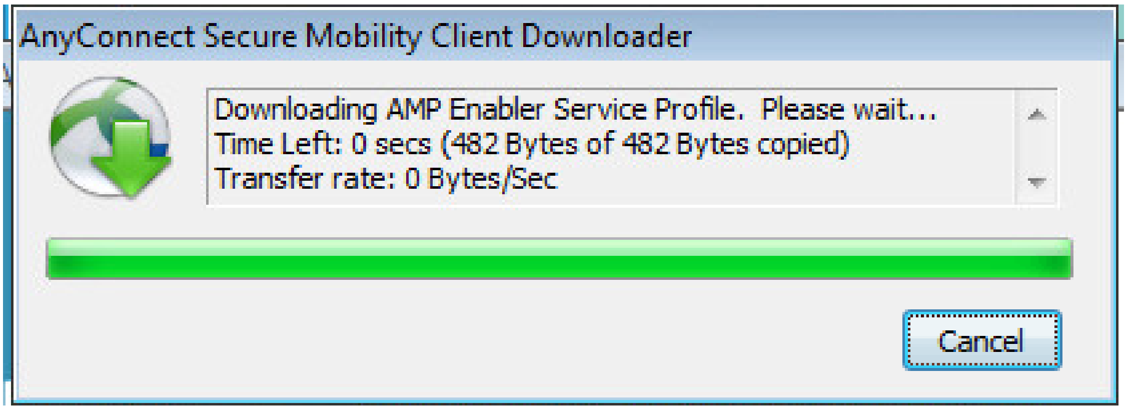
Trusted and Secure Connection

You are connected to

ISE21-3ek.example.com

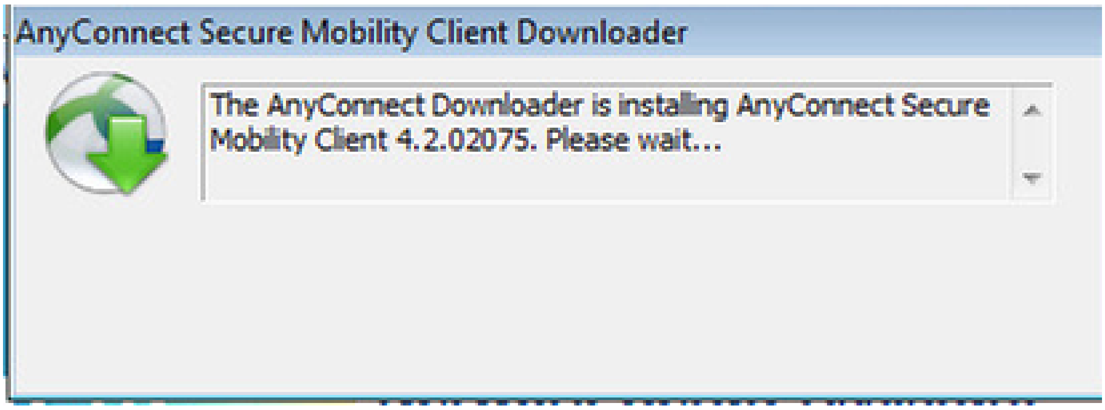
whose identity has been certified. Your connection to this website is encrypted.

(c) 2014 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



AnyConnect Secure Mobility Client Downloader

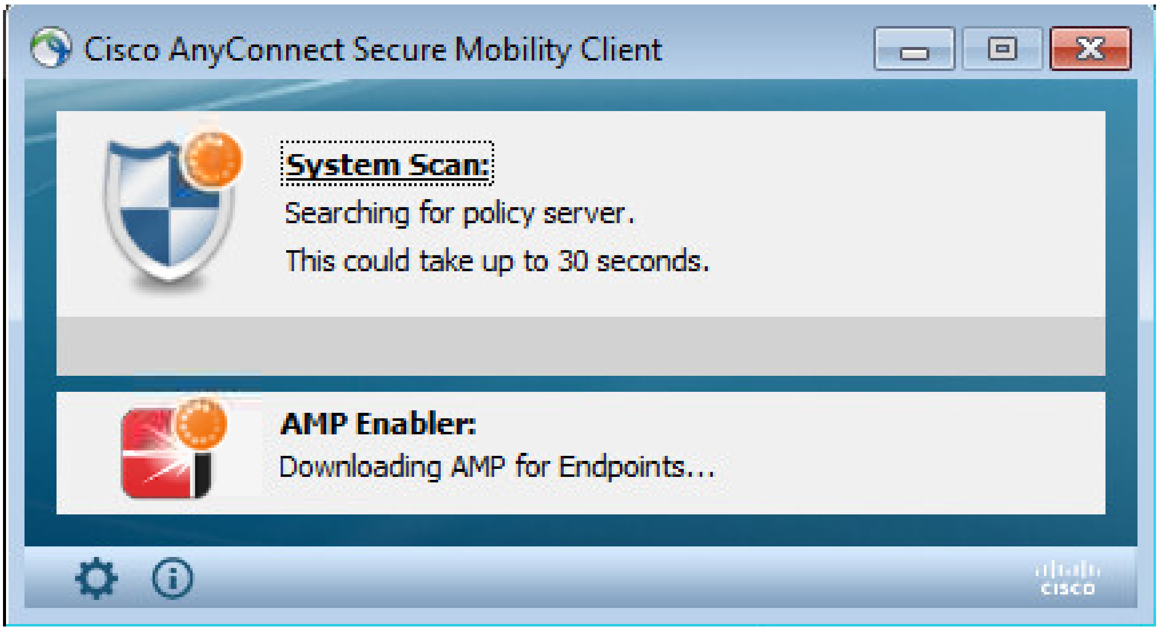
Downloading AMP Enabler Service Profile. Please wait...
Time Left: 0 secs (482 Bytes of 482 Bytes copied)
Transfer rate: 0 Bytes/Sec



AnyConnect Secure Mobility Client Downloader

The AnyConnect Downloader is installing AnyConnect Secure Mobility Client 4.2.02075. Please wait...

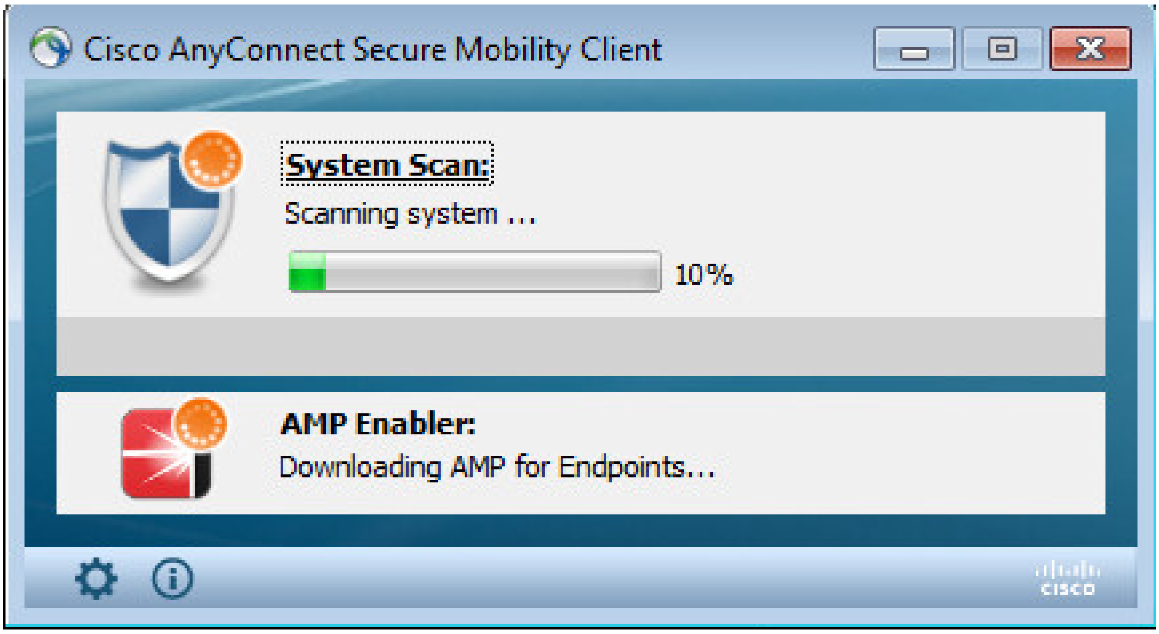
بمجرد انتهاء التثبيت، تقوم الوحدة النمطية AnyConnect Posture (وضعية AnyConnect) بإجراء فحص التوافق.



Cisco AnyConnect Secure Mobility Client

System Scan:
Searching for policy server.
This could take up to 30 seconds.

AMP Enabler:
Downloading AMP for Endpoints...

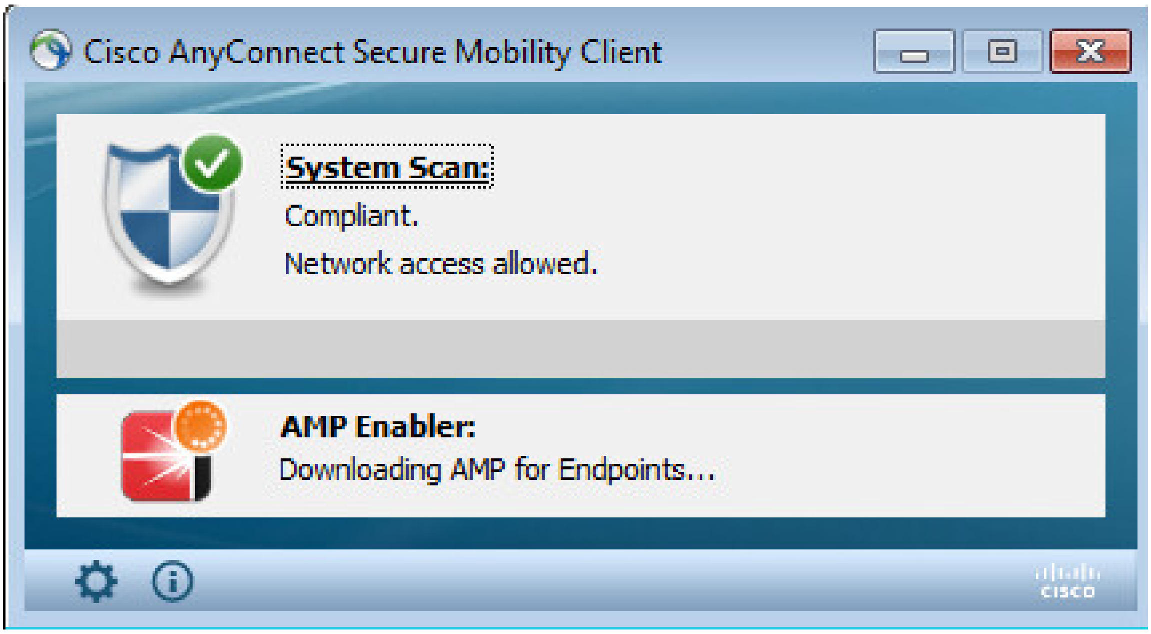


Cisco AnyConnect Secure Mobility Client

System Scan:
Scanning system ...
10%

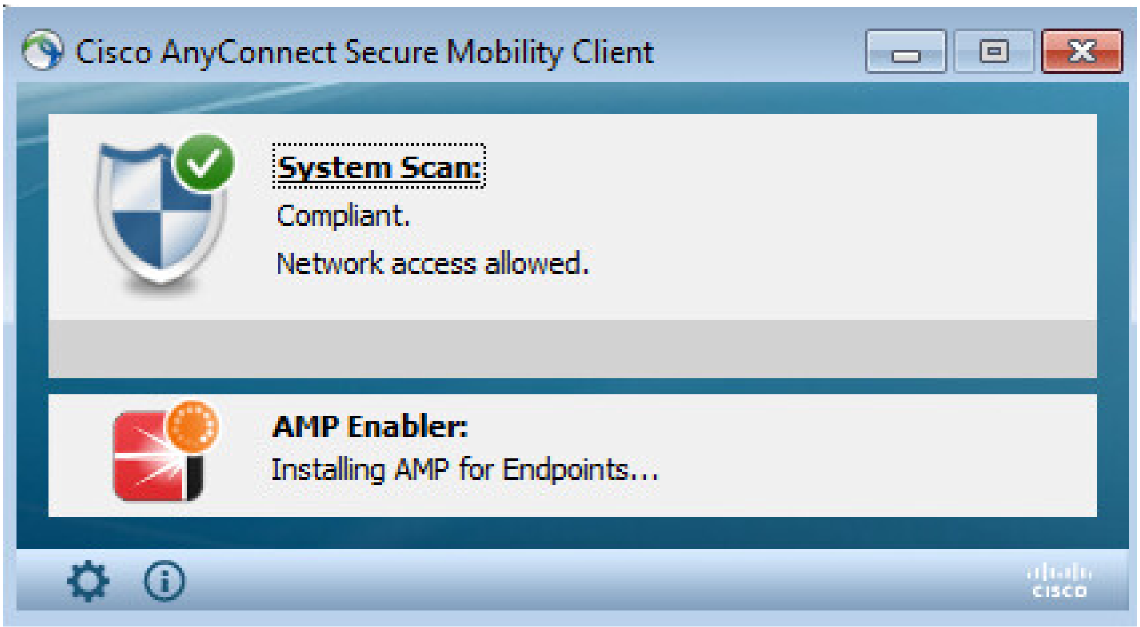
AMP Enabler:
Downloading AMP for Endpoints...

مع توفير الوصول الكامل، إذا كانت نقطة النهاية متوافقة، فإنه يتم تنزيل AMP وتثبيته من خادم الويب المحدد سابقا في ملف تعريف AMP.



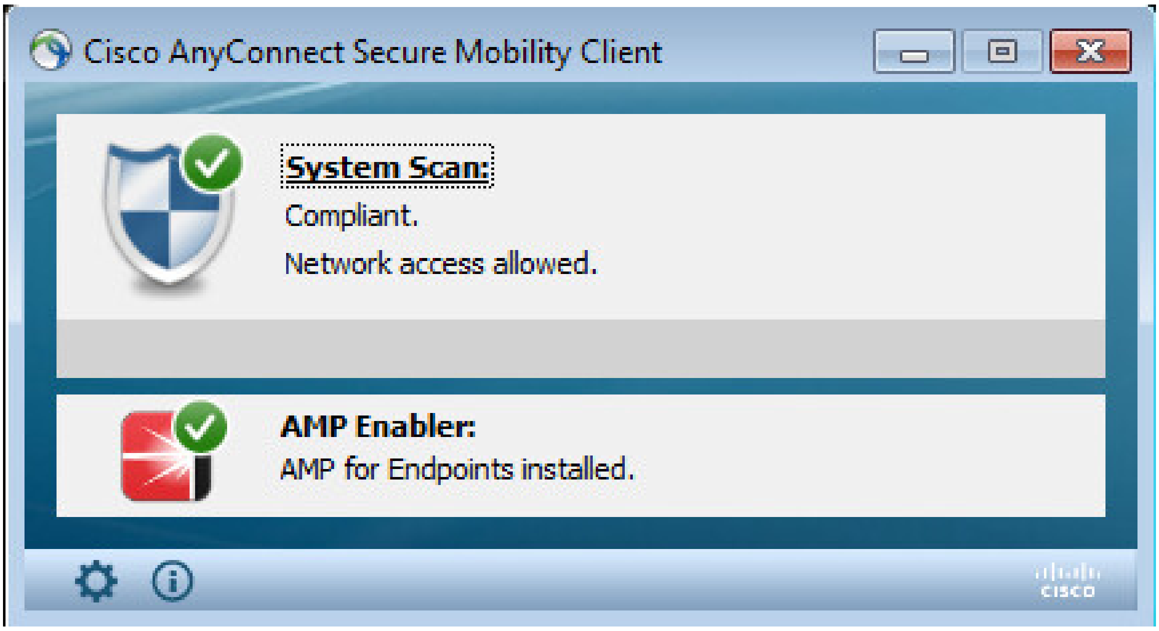
System Scan:
Compliant.
Network access allowed.

AMP Enabler:
Downloading AMP for Endpoints...



System Scan:
Compliant.
Network access allowed.

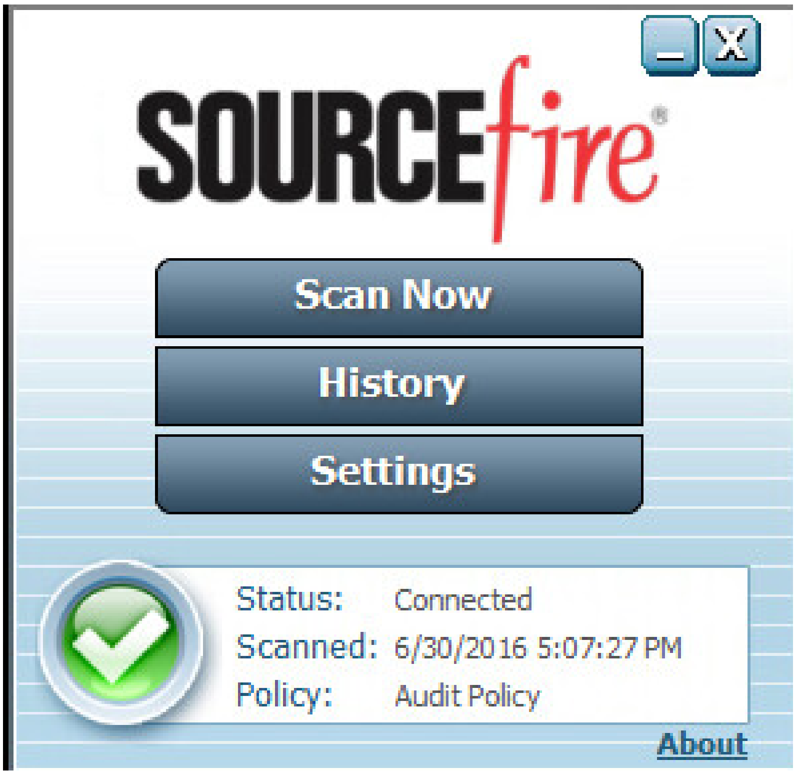
AMP Enabler:
Installing AMP for Endpoints...



System Scan:
Compliant.
Network access allowed.

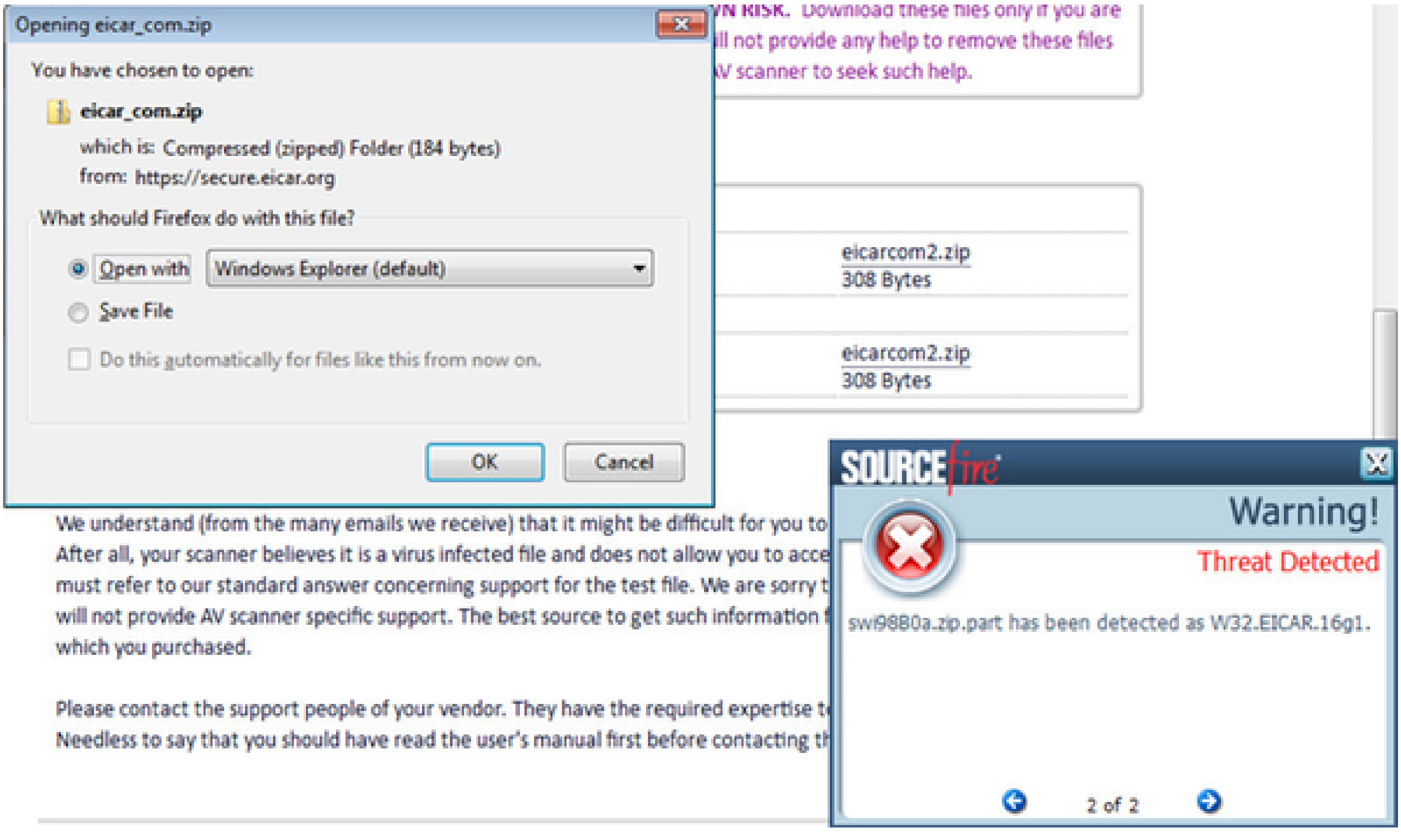
AMP Enabler:
AMP for Endpoints installed.

يظهر موصل AMP.



Status: Connected
Scanned: 6/30/2016 5:07:27 PM
Policy: Audit Policy

لاختبار AMP قيد التشغيل يتم تنزيل سلسلة EICAR المضمنة في ملف zip. يتم اكتشاف التهديد، ويتم الإبلاغ عنه إلى سحابة AMP.



WN RISK. Download these files only if you are
ill not provide any help to remove these files
V scanner to seek such help.

You have chosen to open:

eicar_com.zip

which is: Compressed (zipped) Folder (184 bytes)
from: https://secure.eicar.org

What should Firefox do with this file?

● Open with Windows Explorer (default)

□ Do this automatically for files like this from now on.

eicarcom2.zip
308 Bytes

eicarcom2.zip
308 Bytes

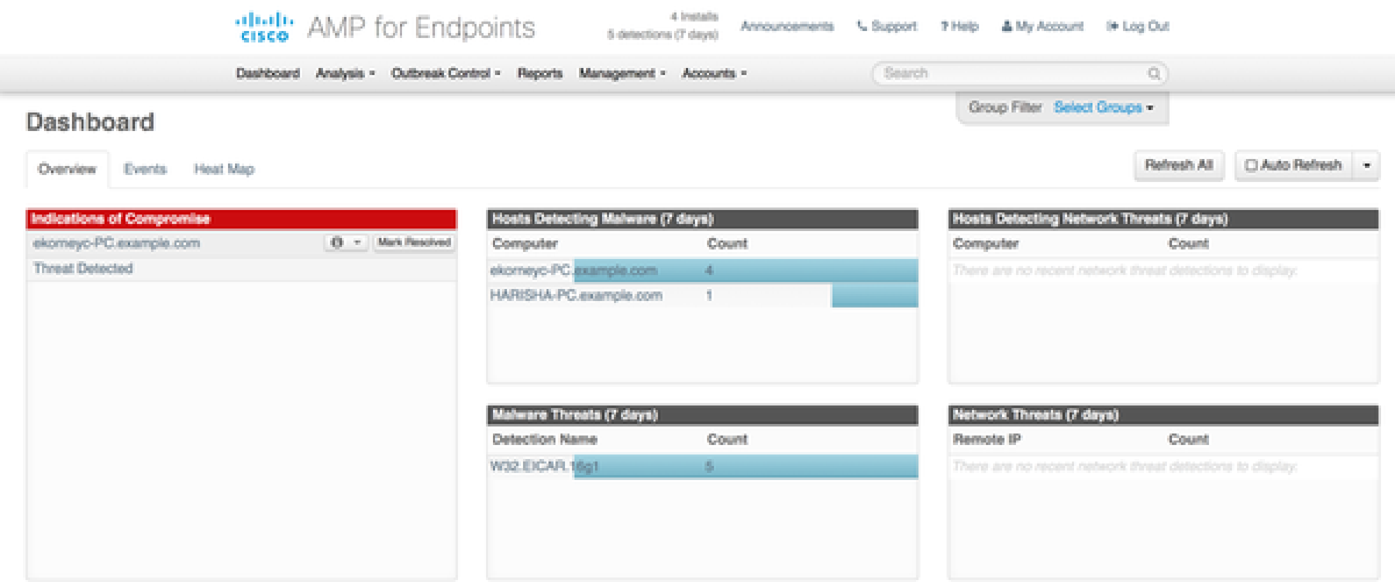
We understand (from the many emails we receive) that it might be difficult for you to
After all, your scanner believes it is a virus infected file and does not allow you to acce
must refer to our standard answer concerning support for the test file. We are sorry t
will not provide AV scanner specific support. The best source to get such information f
which you purchased.

Please contact the support people of your vendor. They have the required expertise t
Needless to say that you should have read the user's manual first before contacting th

swi9880a.zip.part has been detected as W32.EICAR.16g1.

AMP Cloud

للتحقق من تفاصيل لوحة معلومات التهديد الخاصة بسحابة AMP يمكن إستخدامها.



Dashboard

Indications of Compromise

ekorneyc-PC.example.com

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)

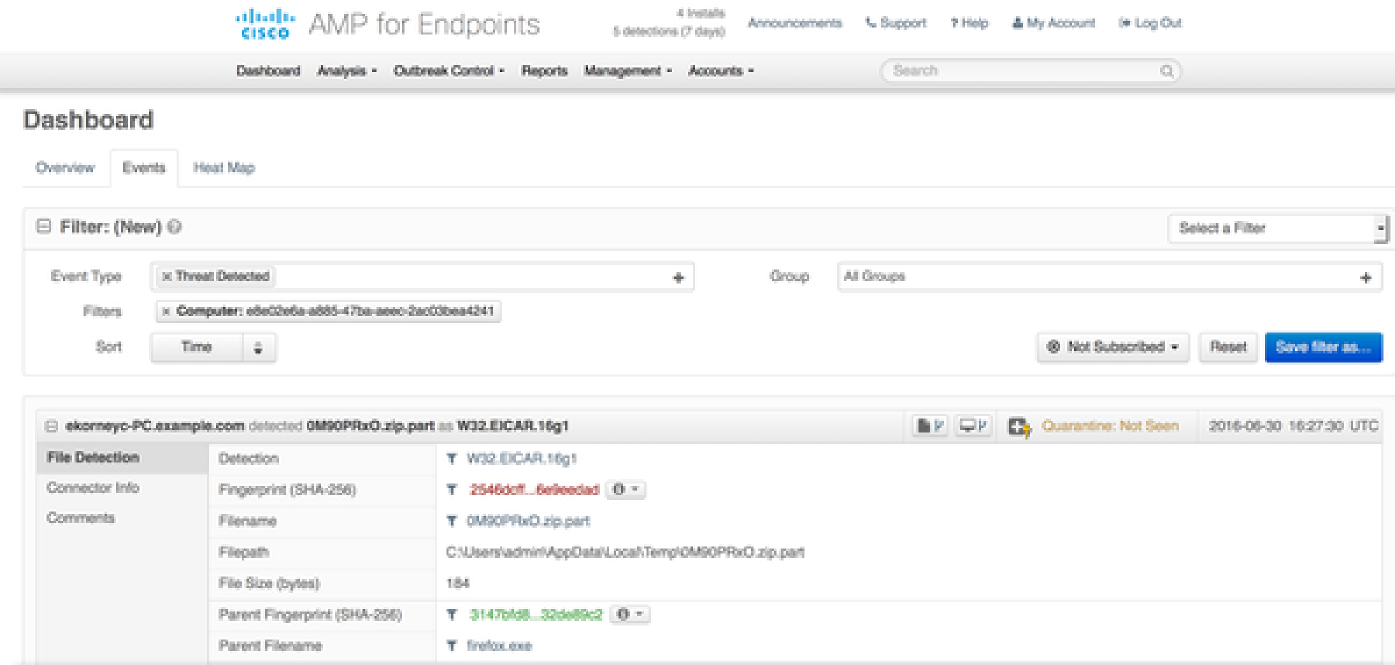
Detection Name	Count
W32.EICAR.16g1	5

Network Threats (7 days)

Remote IP	Count

There are no recent network threat detections to display.

من أجل الحصول على مزيد من التفاصيل حول التهديد والمصفوفة وأصابع الاتهام، يمكنك النقر فوق المضيف، حيث تم اكتشاف برامج ضارة.



Dashboard

Filter: (New)

Event Type: Threat Detected

Group: All Groups

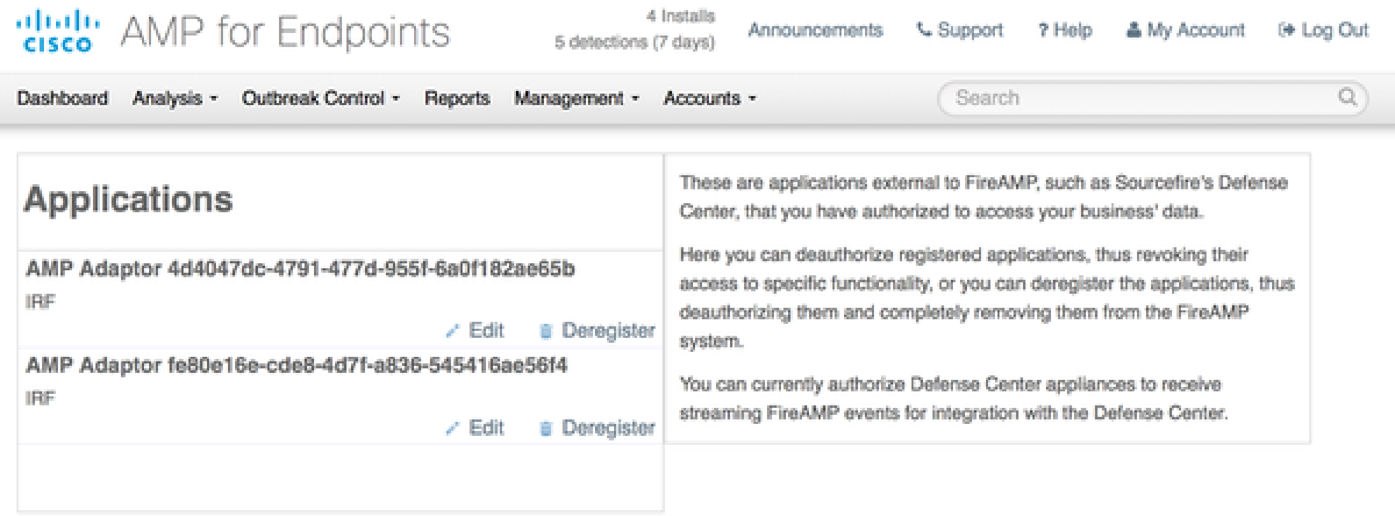
Filters: Computer: e8e02e6a-a885-47ba-aeec-2ac03bea4241

Sort: Time

ekorneyc-PC.example.com detected 0M90PRxO.zip.part as W32.EICAR.16g1 Quarantine: Not Seen 2016-06-30 16:27:30 UTC

Detection	W32.EICAR.16g1
Fingerprint (SHA-256)	2546dcff...6e9eedad
Filename	0M90PRxO.zip.part
Filepath	C:\Users\admin\AppData\Local\Temp\0M90PRxO.zip.part
File Size (bytes)	184
Parent Fingerprint (SHA-256)	3147bfd8...32de89c2
Parent Filename	firefox.exe

لعرض مثيل ISE أو إلغاء تسجيله، يمكنك الانتقال إلى الحسابات > التطبيقات



Applications

AMP Adaptor 4d4047dc-4791-477d-955f-6a0f182ae65b

IRF

AMP Adaptor fe80e16e-cde8-4d7f-a836-545416ae56f4

IRF

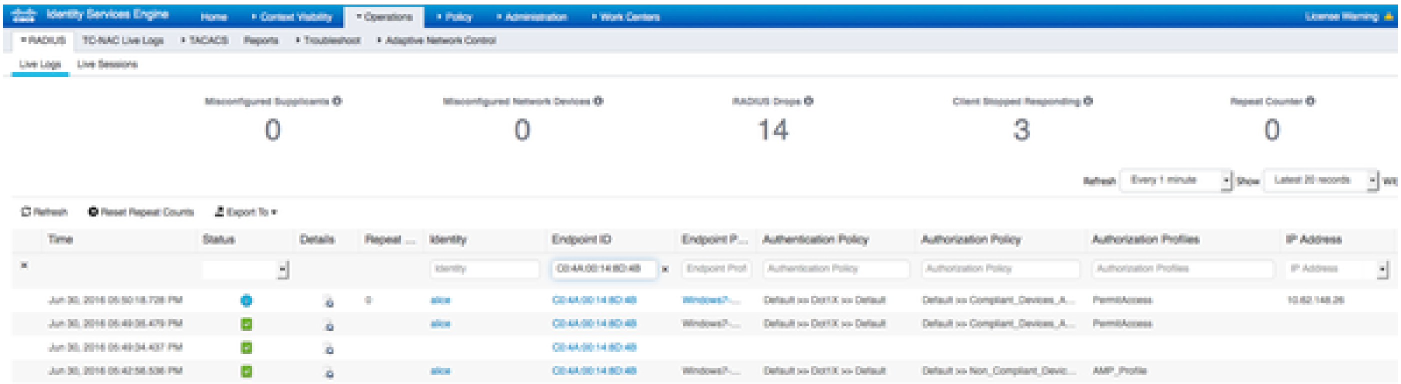
These are applications external to FireAMP, such as Sourcefire's Defense Center, that you have authorized to access your business' data.

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.

محرك خدمات كشف الهوية (ISE)

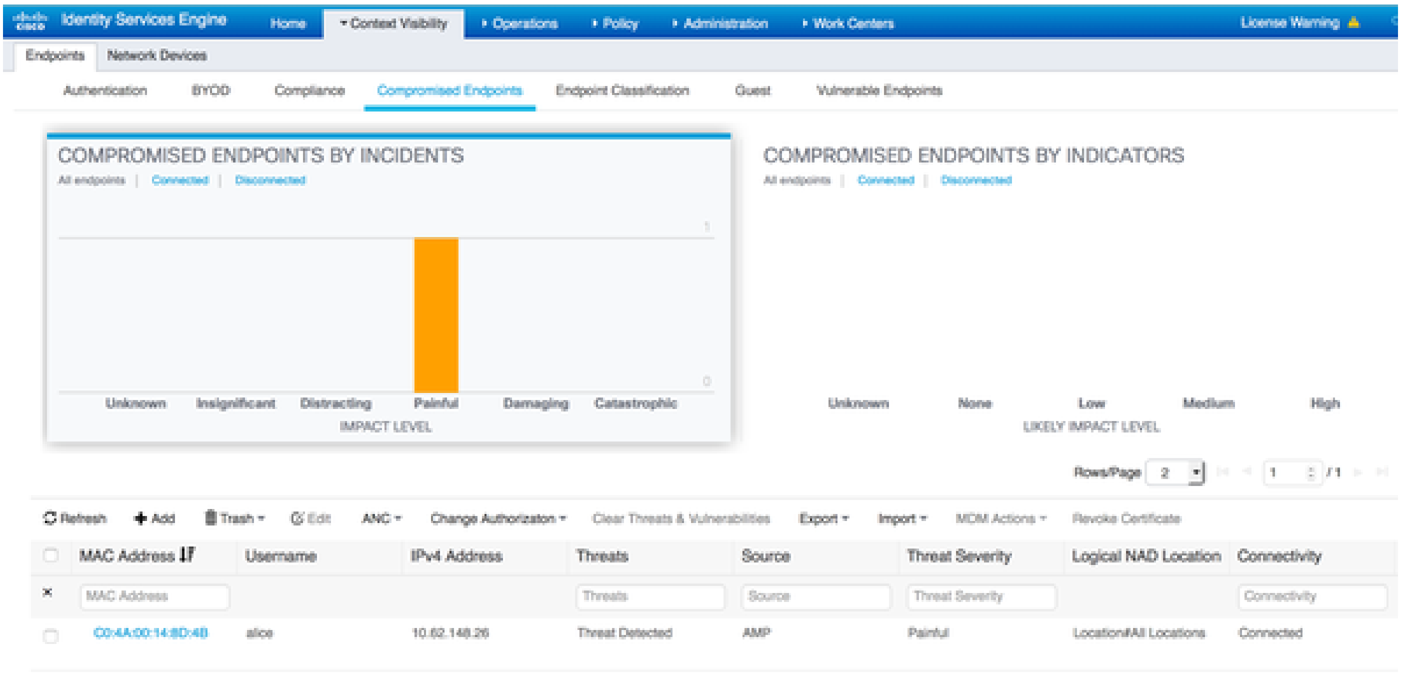
على ISE نفسه يتم رؤية تدفق الوضع العادي، تحدث عملية إعادة التوجيه أولا للتحقق من توافق الشبكة. بمجرد أن تكون نقطة النهاية متوافقة، يتم إرسال CoA Reauth ويتم تعيين ملف تعريف جديد مع PermitAccess.



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	14	3	0

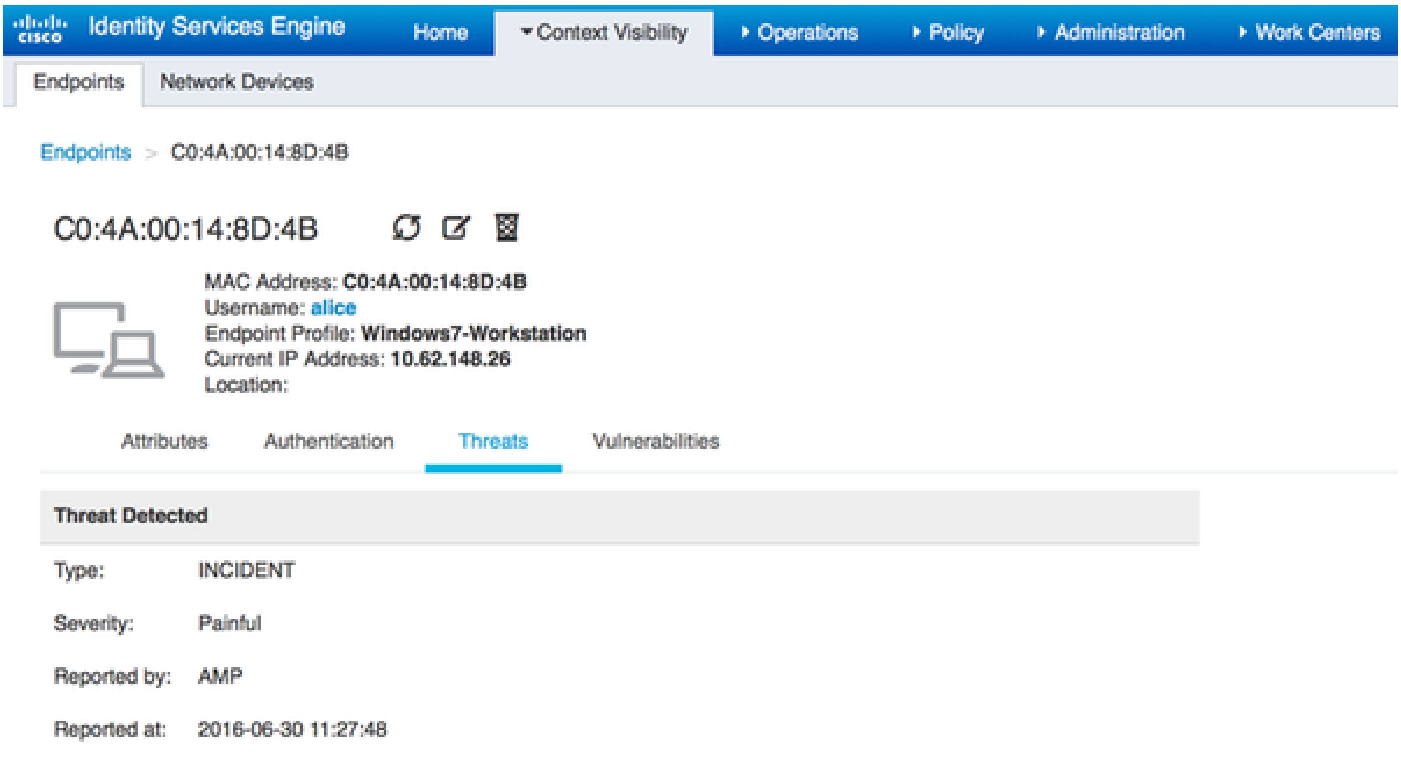
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
				Identity	C0:4A:00:14:8D:4B	Endpoint Prof	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Jun 30, 2016 05:50:18.728 PM	●		0	alice	C0:4A:00:14:8D:4B	Windows7-...	Default >> Dot1X >> Default	Default >> Compliant_Devices_A...	PermitAccess	10.62.148.26
Jun 30, 2016 05:49:26.479 PM	✓			alice	C0:4A:00:14:8D:4B	Windows7-...	Default >> Dot1X >> Default	Default >> Compliant_Devices_A...	PermitAccess	
Jun 30, 2016 05:49:34.437 PM	✓				C0:4A:00:14:8D:4B					
Jun 30, 2016 05:42:56.536 PM	✓			alice	C0:4A:00:14:8D:4B	Windows7-...	Default >> Dot1X >> Default	Default >> Non_Compliant_Devic...	AMP_Profile	

لعرض التهديدات التي تم اكتشافها، يمكنك الانتقال إلى حالة رؤية السياق > نقاط النهاية > نقاط النهاية التي تم إختراقها



□	MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity
×	MAC Address			Threats	Source	Threat Severity		Connectivity
□	C0:4A:00:14:8D:4B	alice	10.62.148.26	Threat Detected	AMP	Painful	Location#All Locations	Connected

إذا قمت بتحديد نقطة النهاية وانتقلت إلى علامة التبويب تهديد، سيتم عرض المزيد من التفاصيل.



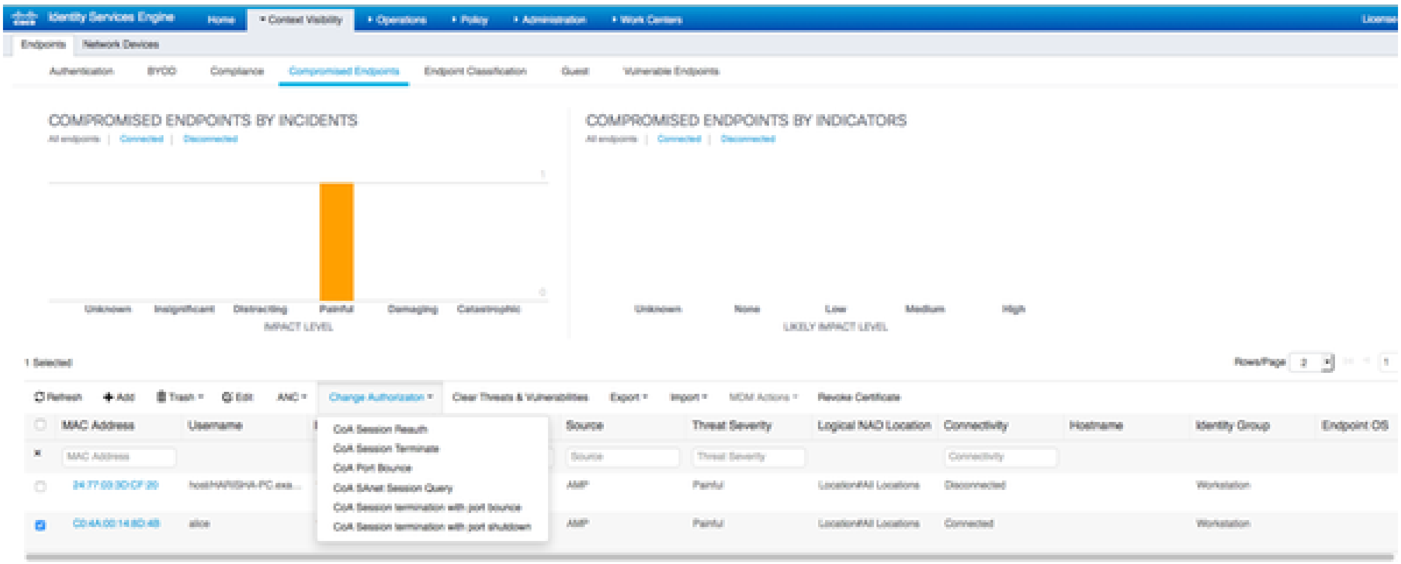
C0:4A:00:14:8D:4B

MAC Address: **C0:4A:00:14:8D:4B**
Username: **alice**
Endpoint Profile: **Windows7-Workstation**
Current IP Address: **10.62.148.26**
Location:

Threat Detected

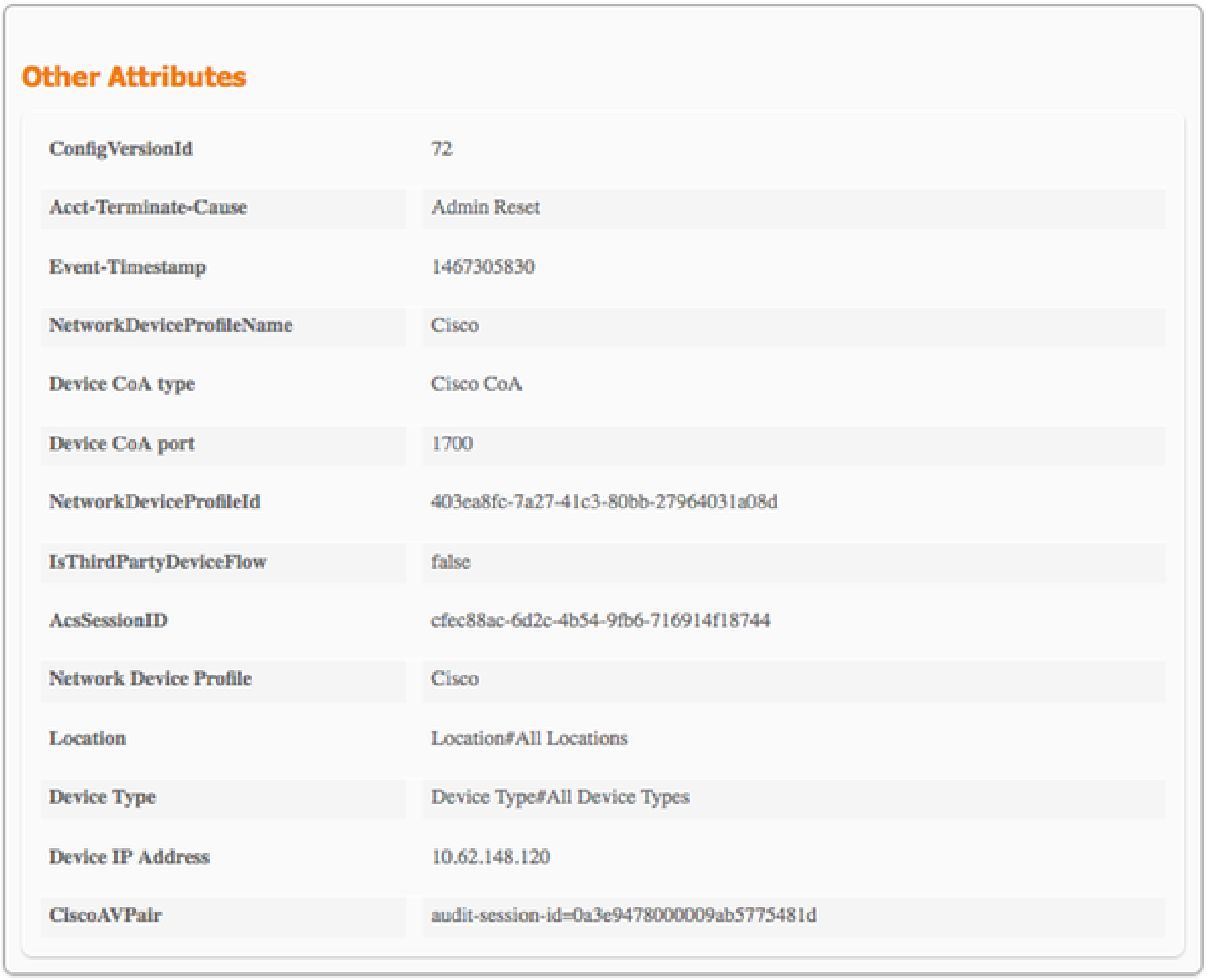
Type:	INCIDENT
Severity:	Painful
Reported by:	AMP
Reported at:	2016-06-30 11:27:48

عندما يتم الكشف عن حدث تهديد لنقطة نهاية، يمكنك تحديد عنوان MAC لنقطة النهاية على صفحة نقاط النهاية التي تم إختراقها وتطبيق سياسة ANC (في حالة تكوينها، على سبيل المثال عزل). بدلا من ذلك يمكنك إصدار تغيير التفويض لإنهاء الجلسة.



	MAC Address	Username	Source	Threat Severity	Logical NAD Location	Connectivity	Hostname	Identity Group	Endpoint OS
○	24:77:03:3D:CF:20	host/HARISHA-PC.exa...	AMP	Painful	Location#All Locations	Disconnected		Workstation	
☑	C0:4A:00:14:8D:4B	alice	AMP	Painful	Location#All Locations	Connected		Workstation	

إذا تم تحديد إنهاء جلسة عمل CoA، فإن ISE يرسل قطع اتصال CoA ويفقد العميل الوصول إلى الشبكة.

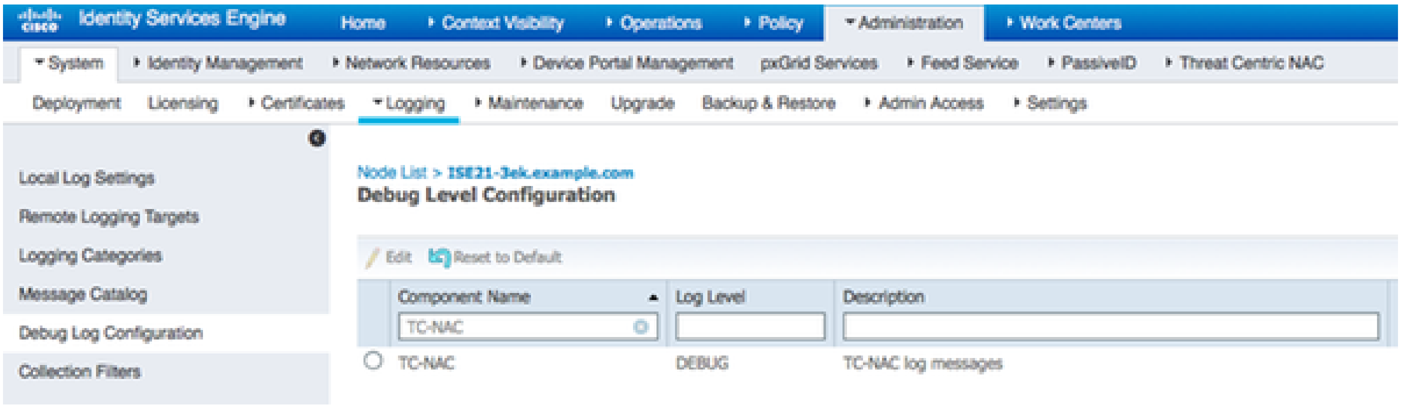


Other Attributes

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

استكشاف الأخطاء وإصلاحها

لتمكين تصحيح الأخطاء على ISE الانتقال إلى الإدارة > النظام > التسجيل > تكوين سجل تصحيح الأخطاء، حدد عقدة TC-NAC وقم بتغيير **مستوى السجل** لمكونات TC-NAC إلى **تصحيح الأخطاء**



Node List > ISE21-3ek.example.com

Debug Level Configuration

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

السجلات المطلوب فحصها - irf.log. يمكنك الحصول عليها مباشرة من واجهة سطر أوامر ISE:

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

بل إن التهديد يتم تلقيه من سحابة AMP

```
2016-06-30 18:27:48617   [IRF-AMQP-Dispatch-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 -:::-
.cisco.cpm.irf.service.irf.NotificationHandler$MyNotificationHandler@3fac8043
Message{Type=Notification messageId=THREAT_EVENT ='{"c0:00:401:8d:4b": [{"incident":
{"impact_qualification": "Painful"} "timestamp": 1467304068599 "vendor": "amp" "title": "
"}]}' priority=0 timestamp=thu June 30 18:27:48 CEST 2016 amqpEnvelope=envelope(deliveryTag=79
redelivery=false exchange=irf.topic routingKey=irf.topic f.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-
a836-54416ae5f4 cluster-id=null)}
2016-06-30 18:27:48617   [IRF-AMQP-Dispatch-Notification-0][]
cisco.cpm.irf.service.irfNotificationHandler:140 -::::---      :
Message{messageType=Notification messageId=THREAT_EVENT content='{"c0:4a:00:14:8d:4b" [""
{_impact: ": "Painful"} " ": 1467304068599 "": "AMP" "": "   "}]}' priority=0  =Thu Jun 30
18:27:48 CEST 2016 amqpEnvelope=envelope(deliveryTag=79 redelivery=false
exchange=irf.topic.events routingKey=irf.threat.threat) ampProperties#content=Envelope
header<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-a836-54416ae56f4
cluster-id=null)}
2016-06-30   [IRF-AMQP-Dispatch-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:59 -:::-    : envelope(deliveryTag=79
redelivery=false exchange=irf.topic.events routingKey=irf.events.threat)
#contentHeader<basic>(content-type=application/json encoding-content=null 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 18:27:48706   [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:parseNotification:221 -::::-  :
Message{Type=Notification messageId=THREAT_EVENT content='{"c0:4a:00:14:8d:4b": ["":
{"impact_qualification": "painful" "time"} : 1467304068599 "": "AMP" "title": "   "}]}'
priority=0 timestamp=thu  30 18:27:48 CEST 2016 amqpEnvelope=envelope(deliveryTag=79
redelivery=false exchange=irf.topic.events routingKey=irf.events.threat)
amqpProperties=#contentHeader<basic>(content-type=application/json content-encoding=null =null
=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)}
```

يتم إرسال معلومات حول التهديد إلى PAN

```
2016-06-30 18:27:48724   [IRF-EventProcessor-0][]
cisco.cpm.irf.service.irfEventProcessor:storeEventsInES:366 -::-       PAN - c0:4a:00:14:8d:4b
{incident={impact_qualification=painful} timestamp=146730 068599 vendor=amp title=threat
detected}
```

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية
والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم
بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما
هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco
Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى
المستند الإنجليزي الأصلي (الرابط متوفر).