使用AMP和狀態服務配置ISE 2.1以威脅為中心的NAC(TC-NAC)

目錄

簡介

本文描述如何在身份服務引擎(ISE)2.1上配置具有高級惡意軟體防護(AMP)的以威脅為中心的NAC。威脅嚴重性級別和漏洞評估結果可用於動態控制終端或使用者的訪問級別。安全評估服務也將在本文檔中介紹。

> **附註**：本文檔的目的是描述ISE 2.1與AMP的整合，說明我們從ISE調配AMP時需要安全評估服務。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 思科身分識別服務引擎
- 高級惡意軟體防護

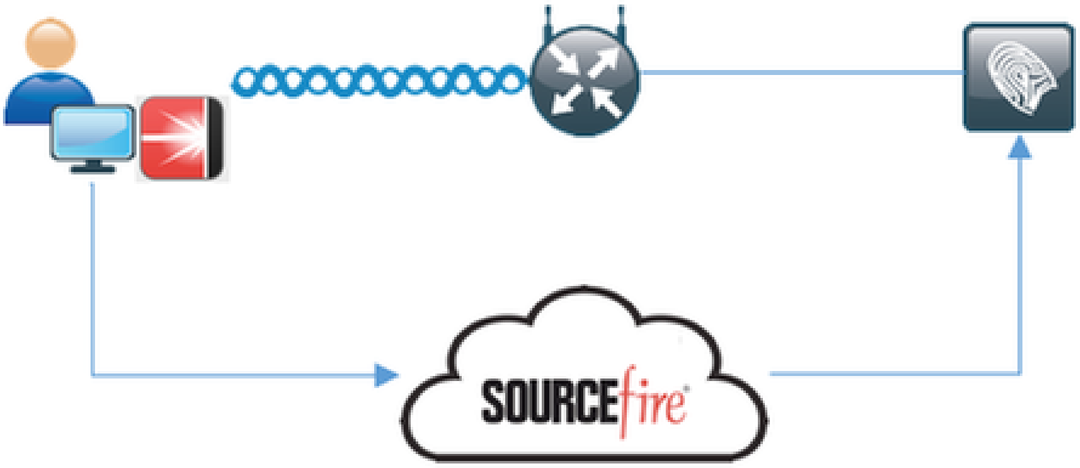
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎版本2.1
- 無線區域網路控制器(WLC)8.0.121.0
- AnyConnect VPN客戶端4.2.02075
- Windows 7 Service Pack 1

設定

網路圖表



詳細流程

1.客戶端連線到網路，分配**AMP_Profile**並將使用者重定向到Anyconnect調配門戶。如果在電腦上未檢測到Anyconnect，則安裝所有配置的模組（VPN、AMP、安全狀態）。每個模組的配置與該配置檔案一起推送

2.安裝Anyconnect後，運行狀態評估

3. AMP Enabler模組安裝FireAMP聯結器

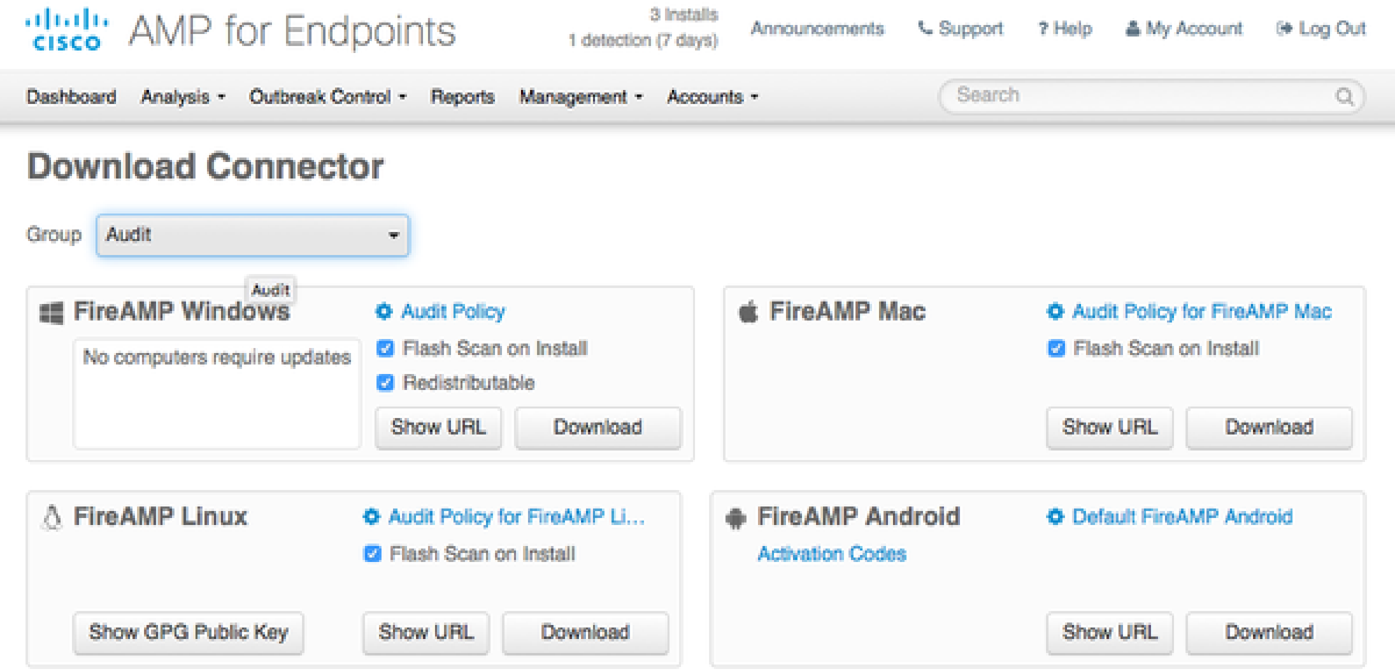
4.當客戶端嘗試下載惡意軟體時，AMP聯結器會拋出警告消息並將其報告給AMP雲

5. AMP雲將此資訊傳送到ISE

配置AMP雲

步驟1.從AMP雲下載聯結器

若要下載聯結器，請導覽至Management > Download Connector。然後選擇type和**Download** FireAMP(Windows、Android、Mac、Linux)。 在這種情況下，選擇了**Audit**，並且選擇了FireAMP for Windows的安裝檔案。



Group: Audit

FireAMP Windows: Audit Policy
☑ Flash Scan on Install
☑ Redistributable

FireAMP Mac: Audit Policy for FireAMP Mac
☑ Flash Scan on Install

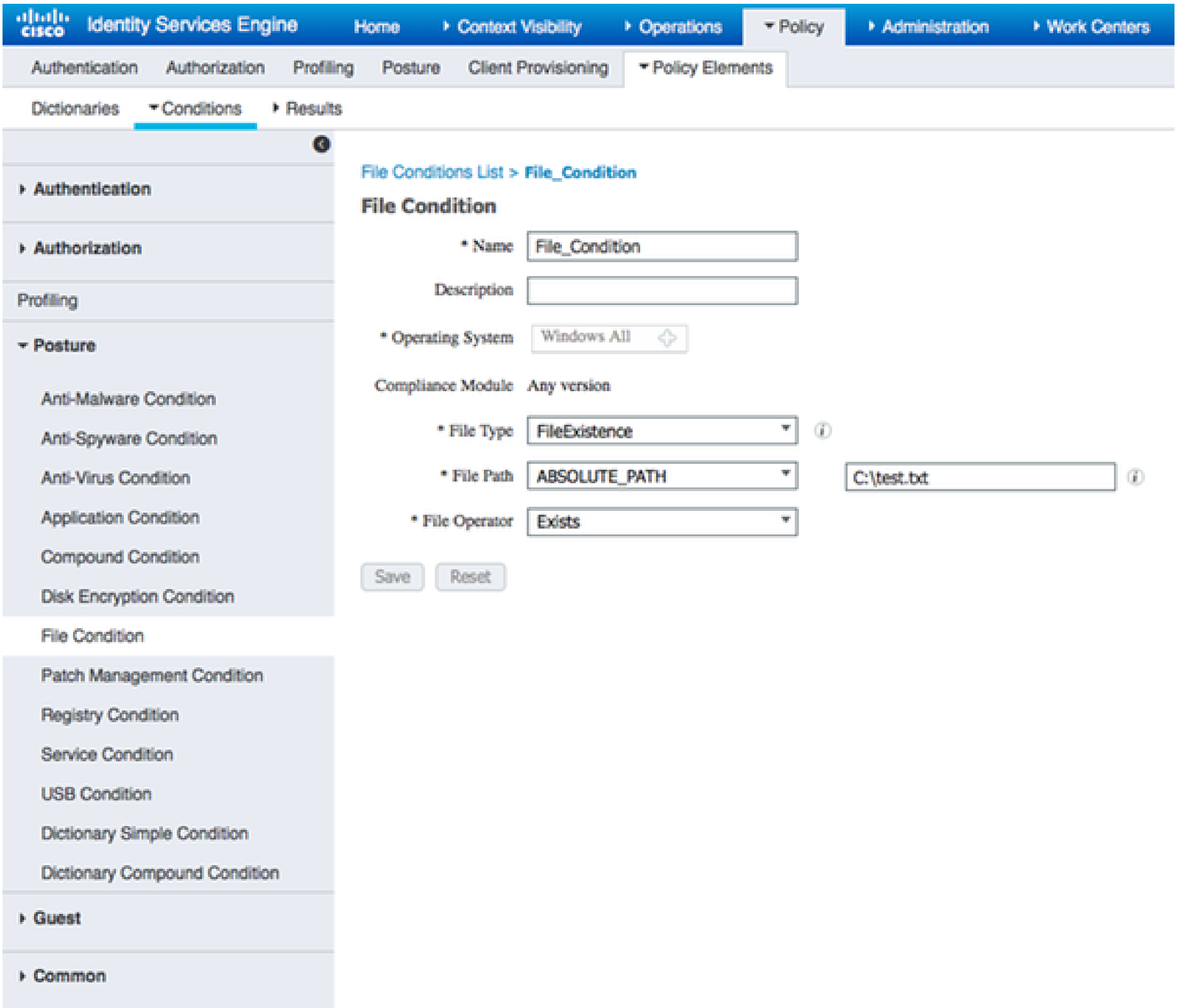
FireAMP Linux: Audit Policy for FireAMP Li...
☑ Flash Scan on Install

> **附註**：下載此檔案會生成一個在示例中名為**Audit_FireAMPSetup.exe**的.exe檔案。在使用者要求配置AMP後，此檔案被傳送到Web伺服器以供使用。

配置ISE

步驟1.配置狀態策略和條件

導航到Policy > Policy Elements > Conditions > Posture > File Condition。您可以看到已建立了一個簡單的檔案存在條件。如果端點要符合狀態模組驗證的策略，則檔案必須存在：

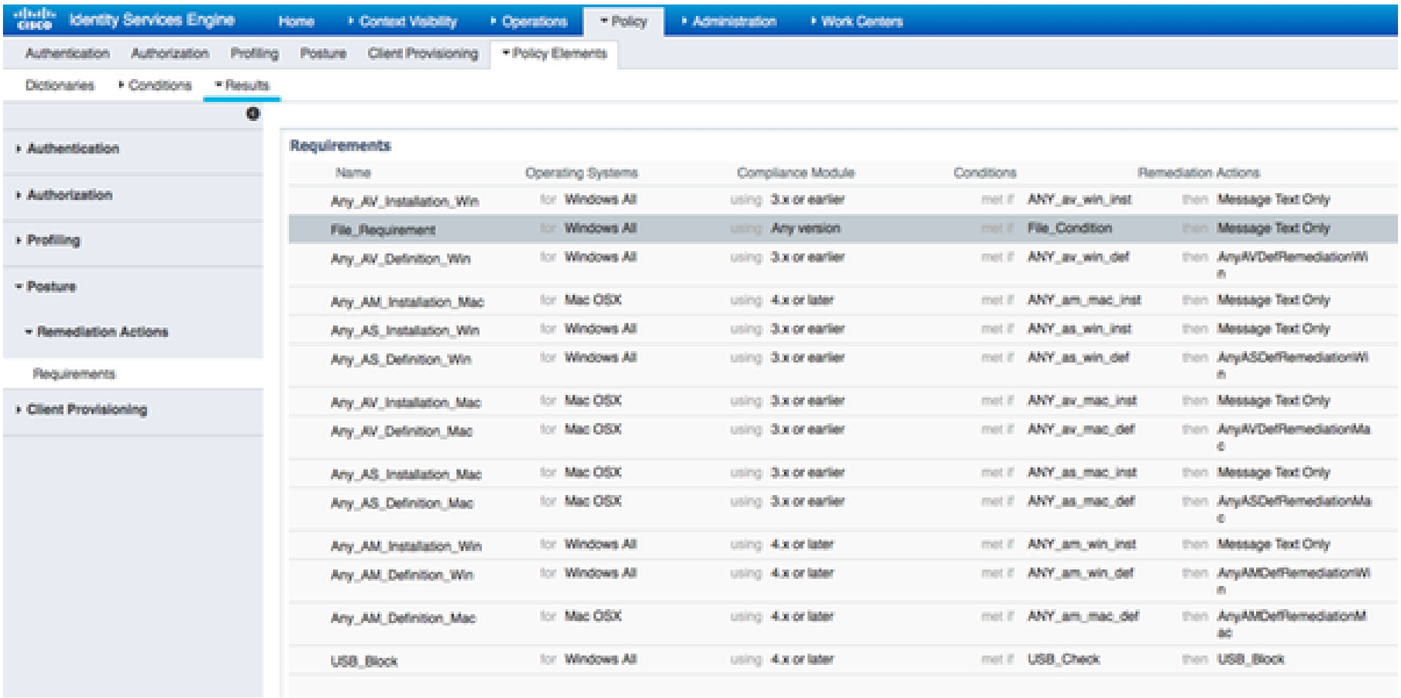


File Conditions List > **File_Condition**

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

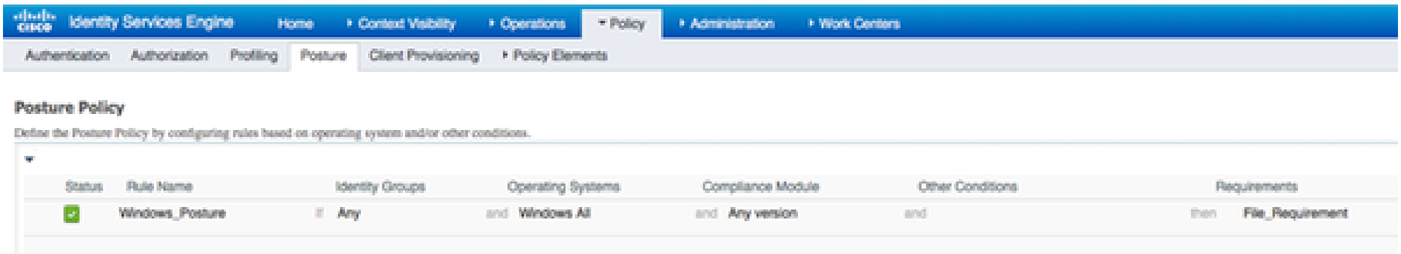
此條件用於需求：



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

此要求用於Microsoft Windows系統的終端安全評估策略：



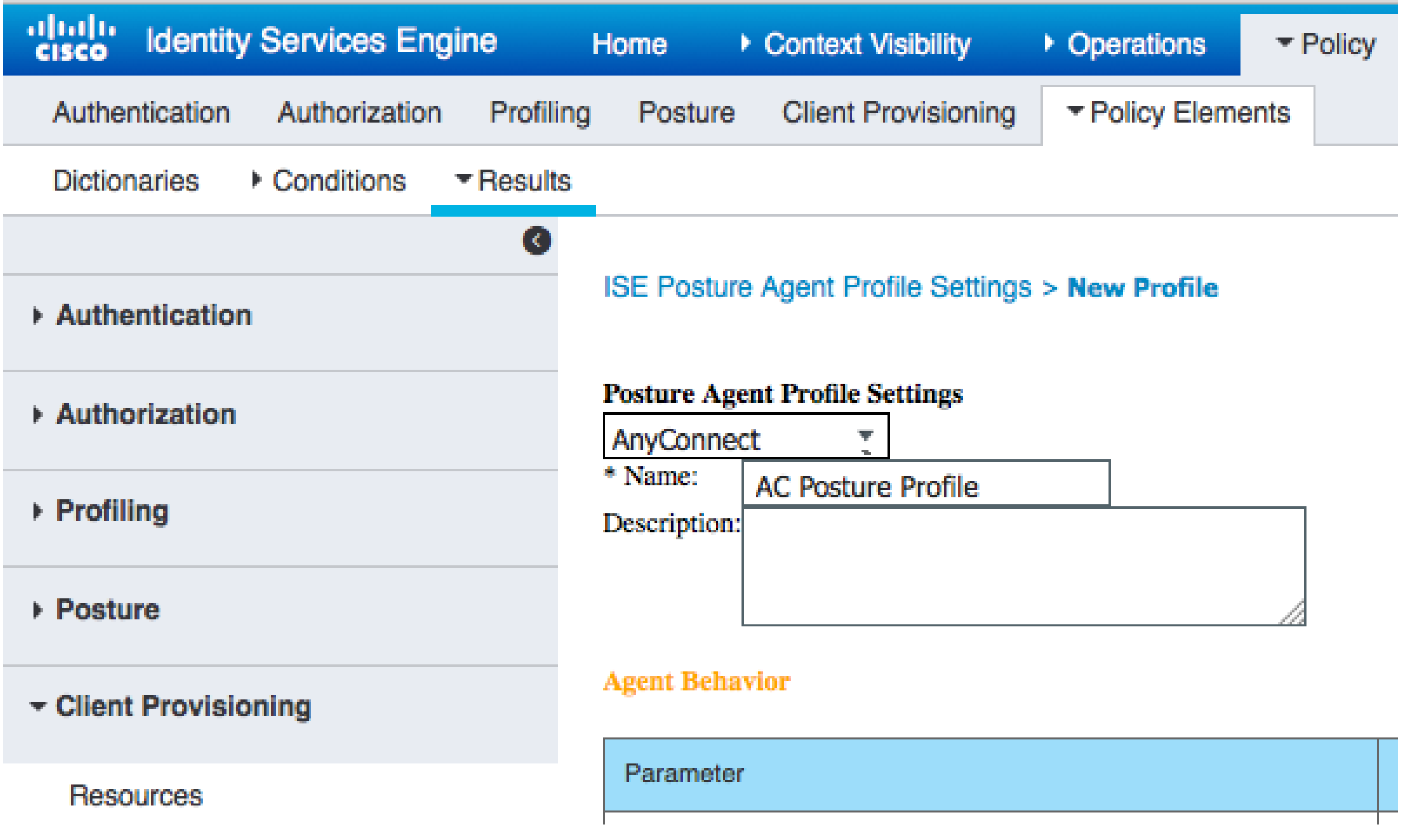
Posture Policy

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

步驟2.配置狀態配置檔案

- 導航到Policy > Policy Elements > Results > Client Provisioning > Resources並新增網路准入控制(NAC)代理或AnyConnect代理狀態配置檔案
- 選擇Anyconnect



ISE Posture Agent Profile Settings > New Profile

Posture Agent Profile Settings

AnyConnect

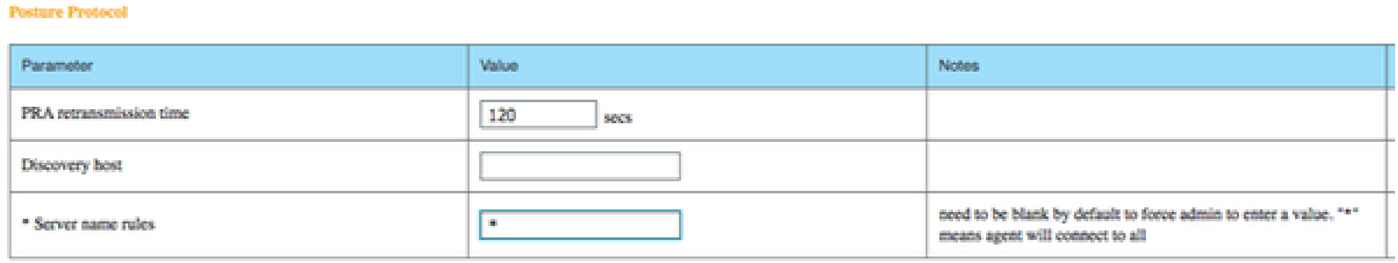
* Name: AC Posture Profile

Description:

Agent Behavior

Parameter

- 在Posture Protocol部分新增*以允許代理連線到所有伺服器

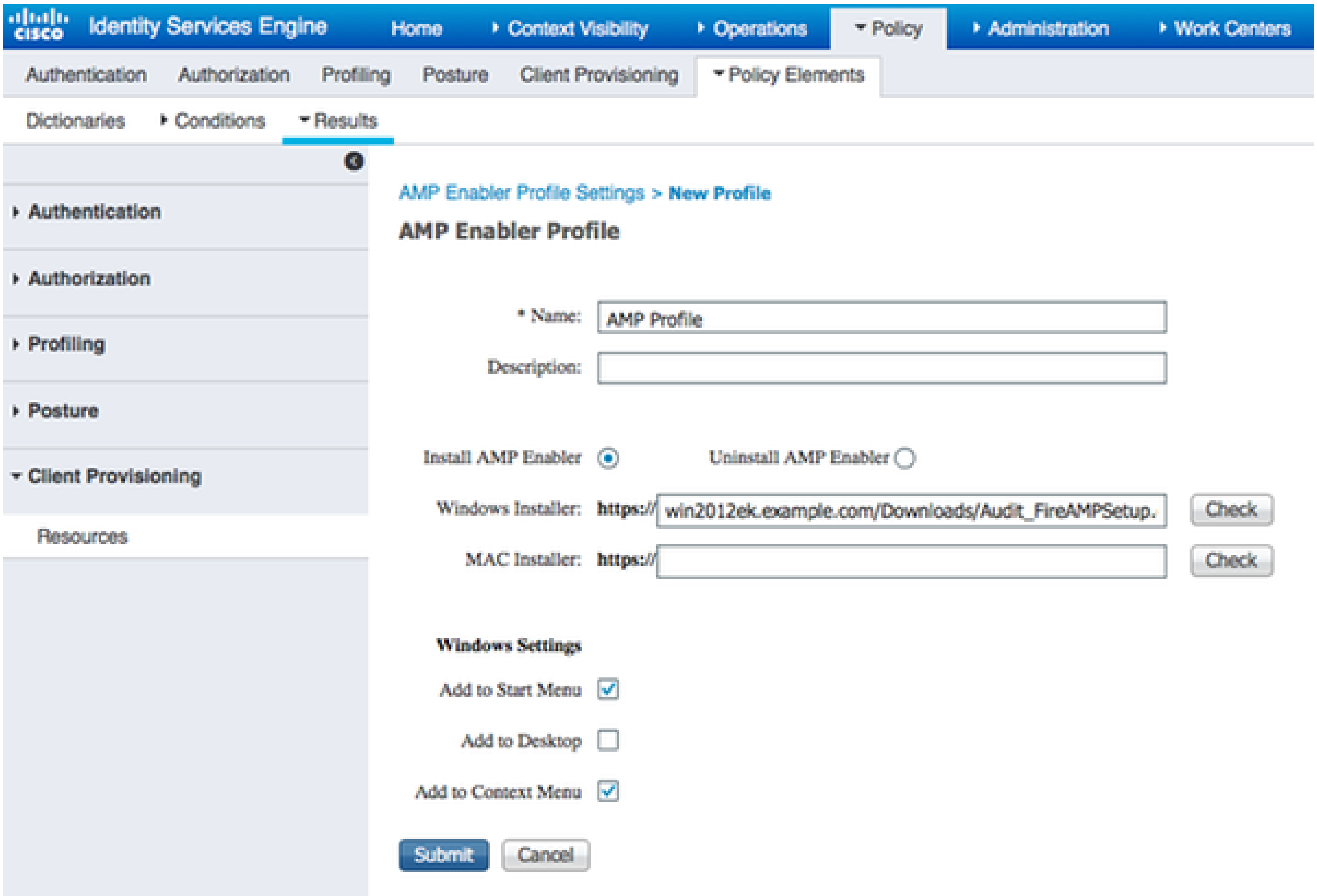


Posture Protocol

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

步驟3.配置AMP配置檔案

AMP配置檔案包含Windows Installer所在位置的資訊。Windows Installer先前從AMP雲下載。它應該可以從客戶端電腦訪問。安裝程式所在的HTTPS伺服器的證書也應受客戶端電腦信任。



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

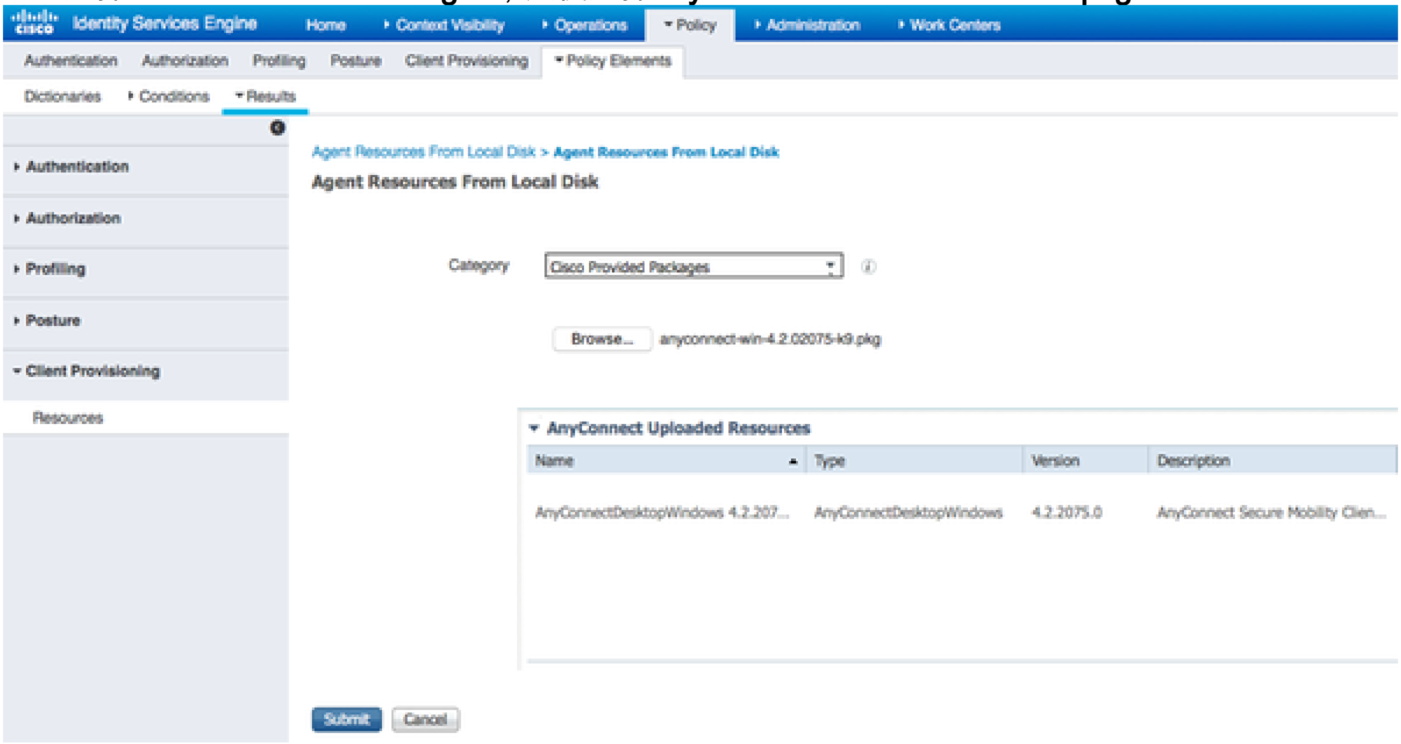
Add to Start Menu ☑

Add to Desktop □

Add to Context Menu ☑

步驟2.將應用和XML配置檔案上傳到ISE

- 從思科官方網站手動下載該應用：**anyconnect-win-4.2.02075-k9.pkg**
- 在ISE上，導航到Policy > Policy Elements > Results > Client Provisioning > Resources，並從本地磁**盤新增代理資源**
- 選擇**Cisco Provided Packages**，然後選擇**anyconnect-win-4.2.02075-k9.pkg**



Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

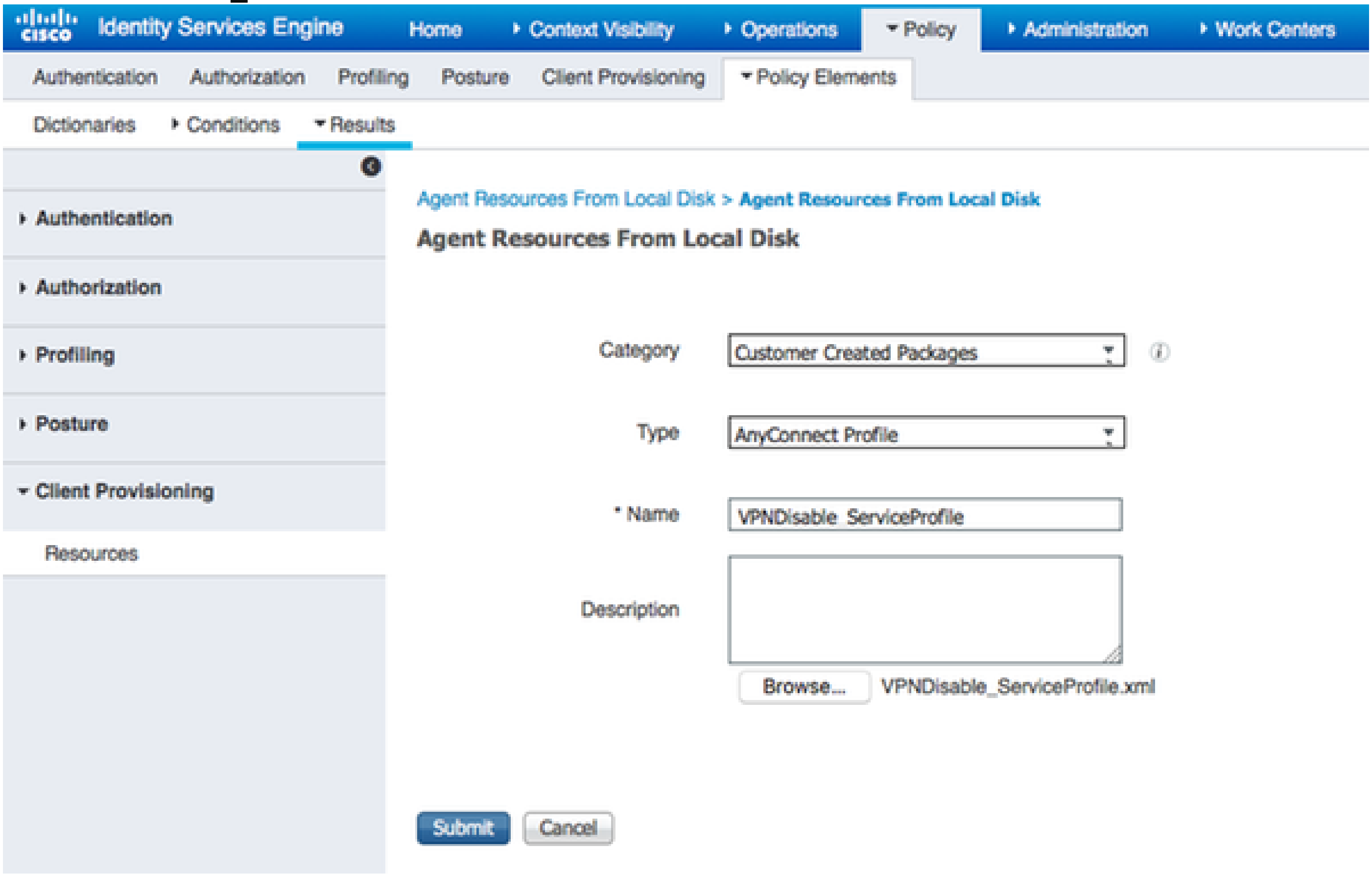
Category: Cisco Provided Packages

Browse... 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...

- 導航到Policy > Policy Elements > Results > Client Provisioning > Resources，並從本地磁盤**新增代理資源**
- 選擇**Customer Created Packages**，然後鍵入**AnyConnect Profile**。選擇**VPNDisable_ServiceProfile.xml**



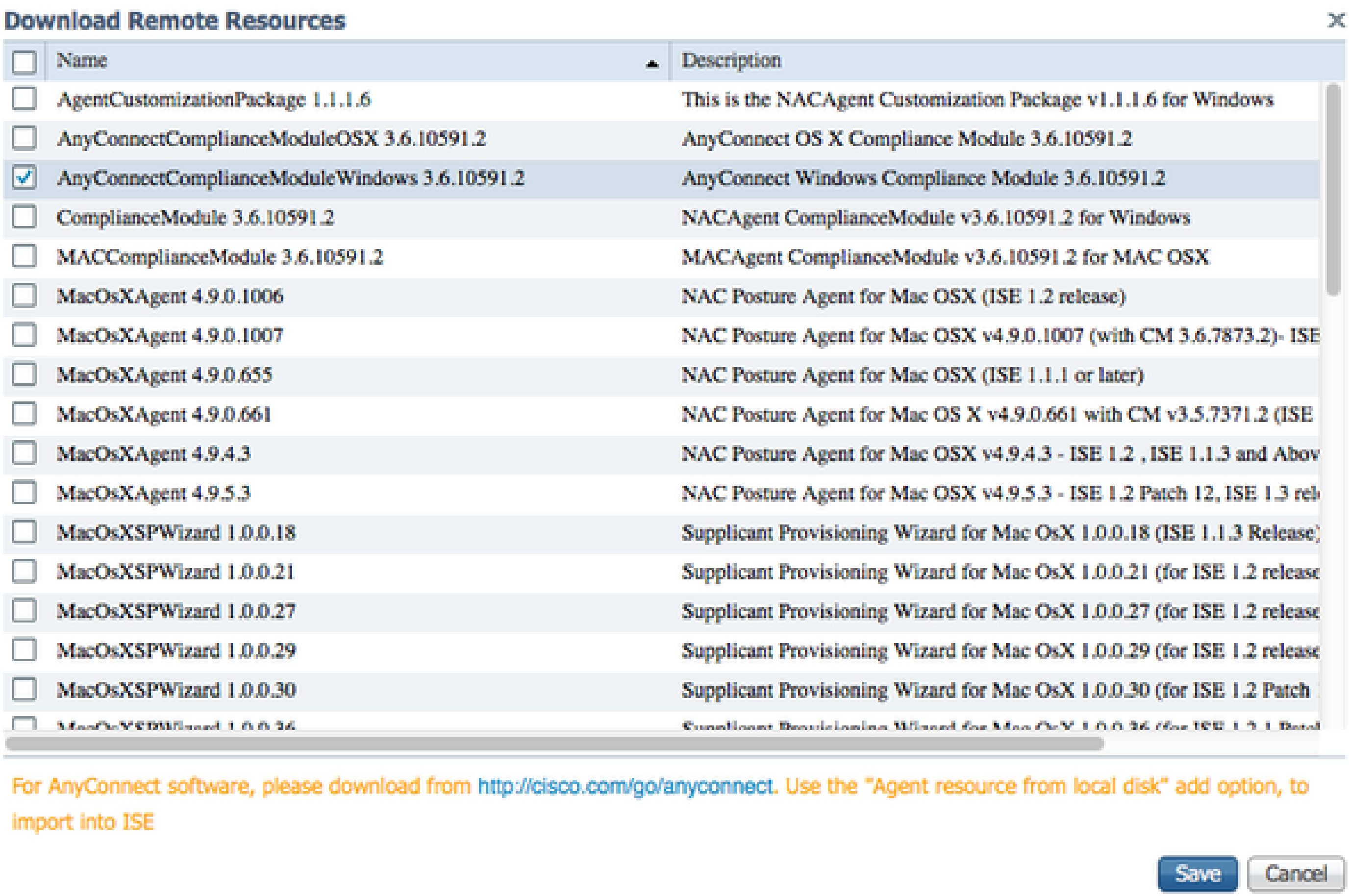
Category: Customer Created Packages
Type: AnyConnect Profile
* Name: VPNDisable_ServiceProfile
Description:
VPNDisable_ServiceProfile.xml

附註：**VPNDisable_ServiceProfile.xml**用於隱藏VPN標題，因為此示例不使用VPN模組。以下是**VPNDisable_ServiceProfile.xml**的內容：

```
<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">
 <客戶端初始化>
 <ServiceDisable>true</ServiceDisable>
 </ClientInitialization>
</AnyConnectProfile>
```

步驟3.下載AnyConnect合規性模組

- 導航到Policy > Policy Elements > Results > Client Provisioning > Resources，然後從Cisco站**點新增代理資源**
- 選擇**AnyConnect Windows Compliance Module 3.6.10591.2**，然後按一下**Save**



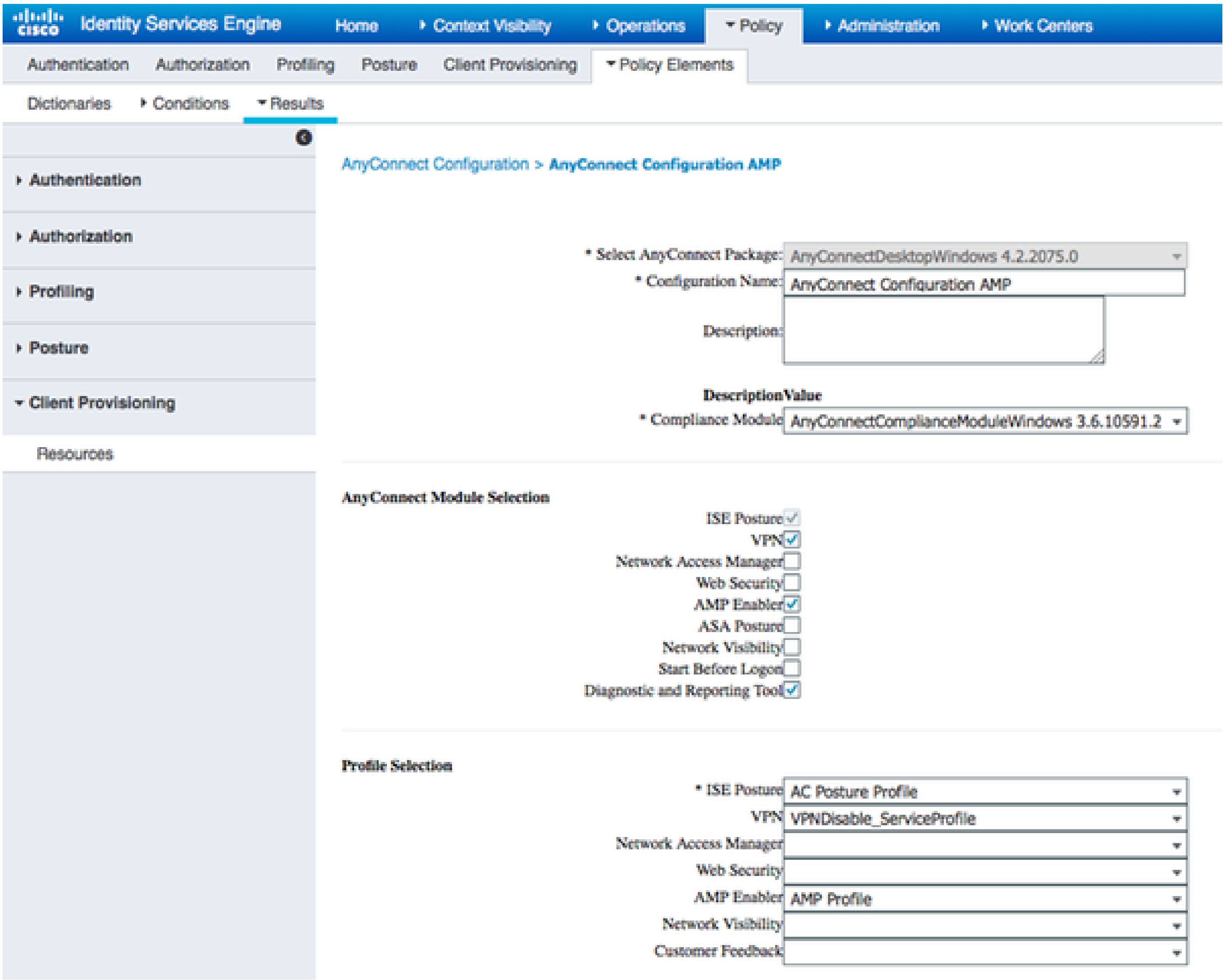
Download Remote Resources

☐	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

步驟4.新增AnyConnect配置

- 導航到Policy > Policy Elements > Results > Client Provisioning > Resources，然後新增**AnyConnect Configuration**
- 配置名稱並選擇合規性模組和所有所需的AnyConnect模組（VPN、AMP和安全狀態）
- 在**設定檔選擇**中，選擇之前為每個模組設定的設定檔



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

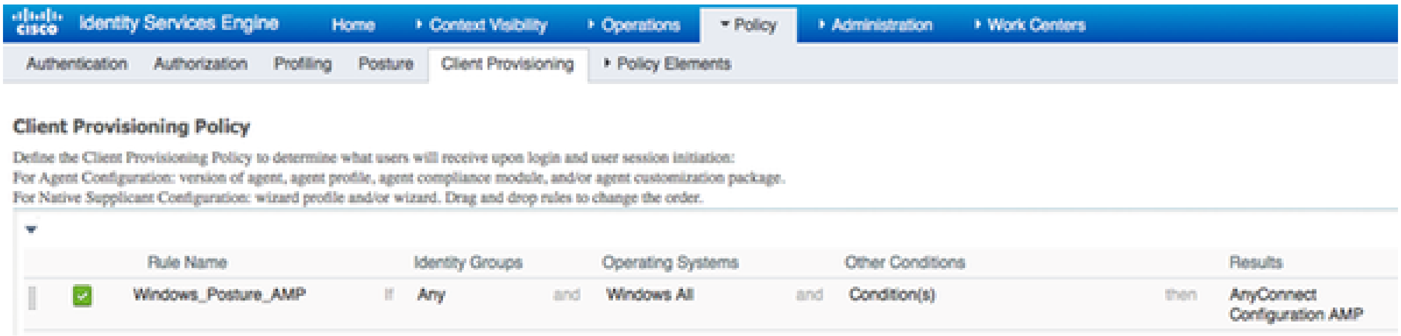
ISE Posture ☑
VPN ☑
Network Access Manager □
Web Security □
AMP Enabler ☑
ASA Posture □
Network Visibility □
Start Before Logon □
Diagnostic and Reporting Tool ☑

Profile Selection

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

步驟5.配置客戶端調配規則

在客戶端調配規則中引用之前建立**的AnyConnect配**置



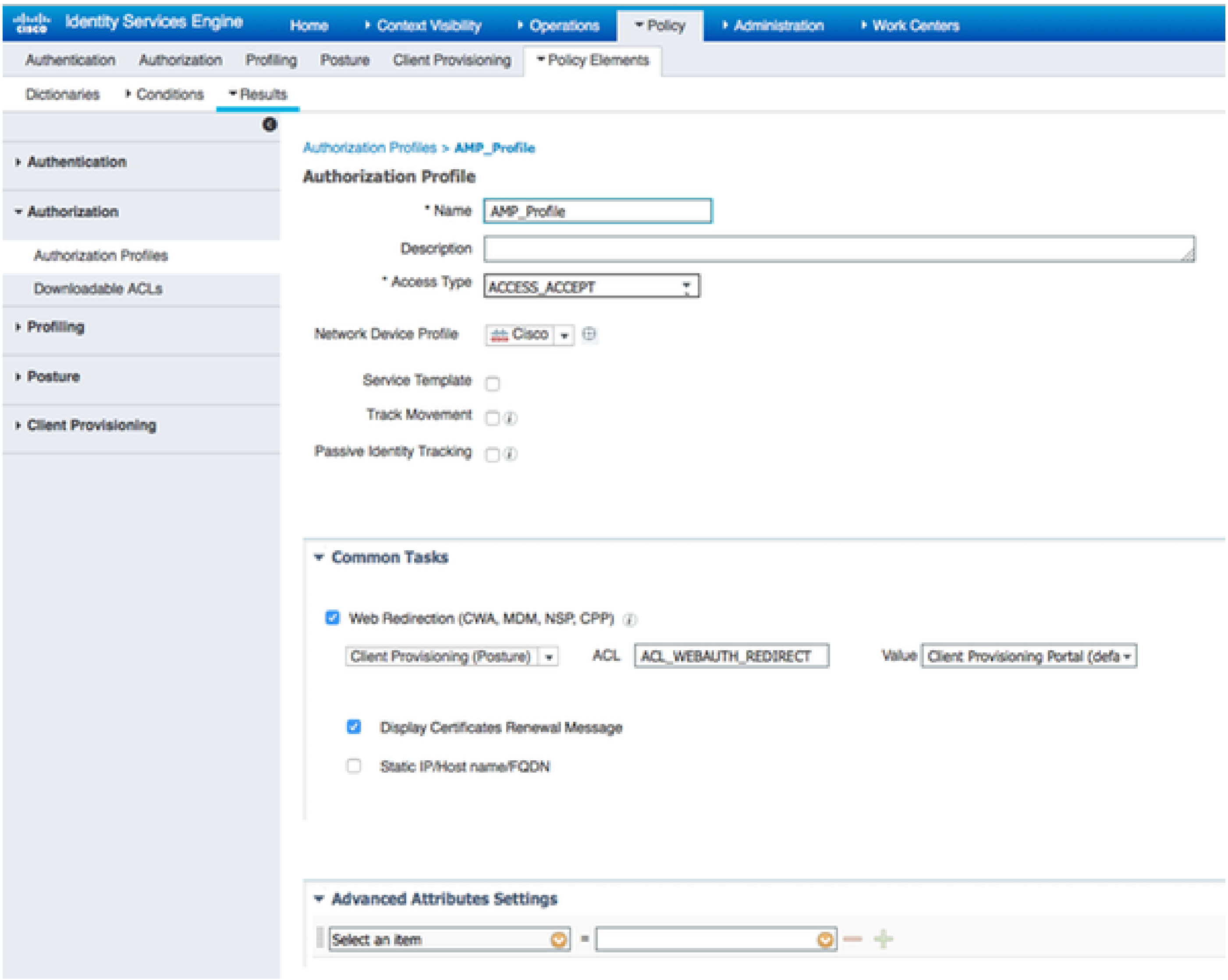
Client Provisioning Policy

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

步驟6.配置授權策略

首先，重定向到客戶端調配門戶。使用安全狀態的標準授權策略。



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

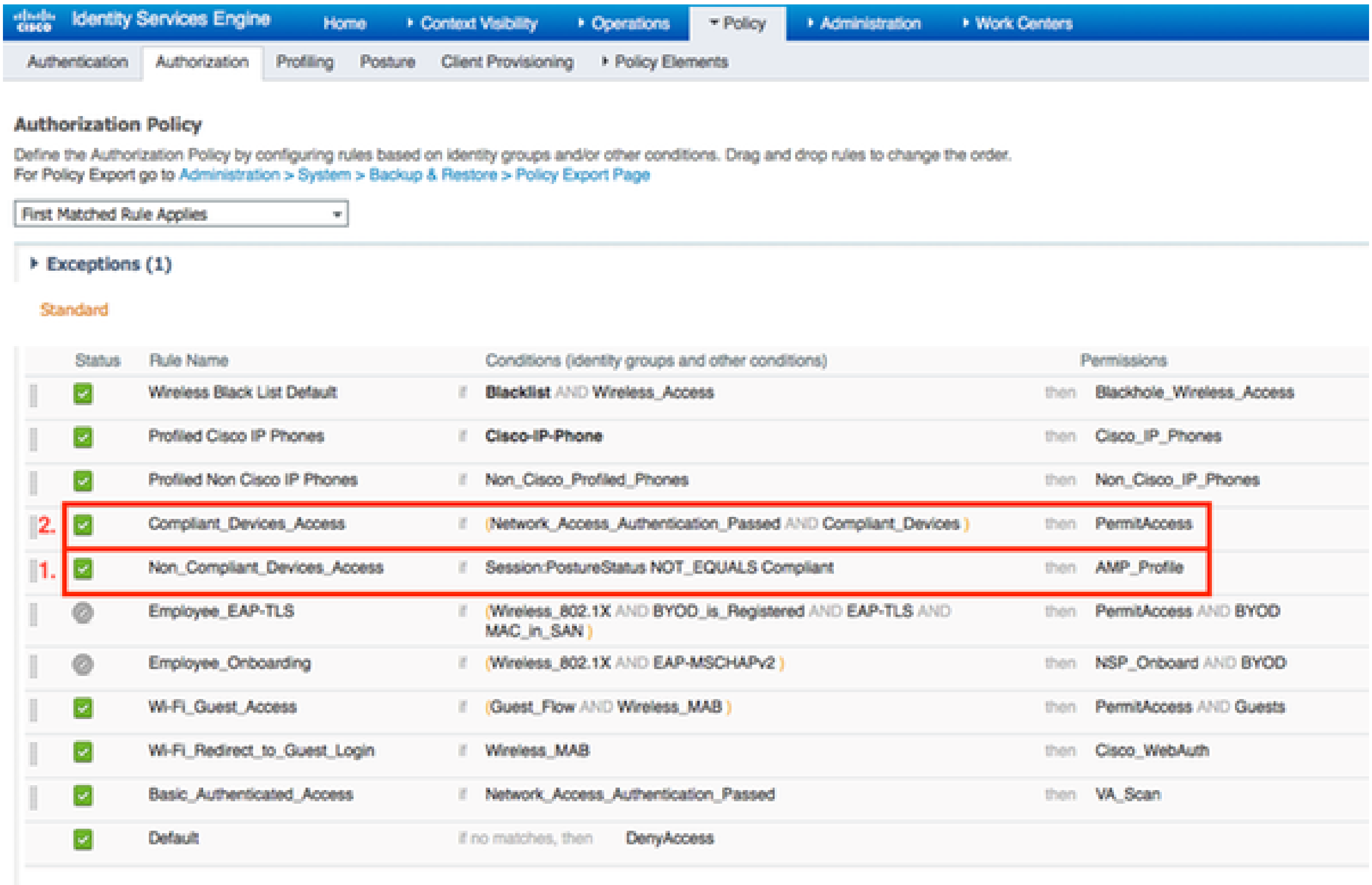
☑ Display Certificates Renewal Message

□ Static IP/Host name/FQDN

Advanced Attributes Settings

Select an item =

之後，一旦符合要求，就會分配完全訪問許可權



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

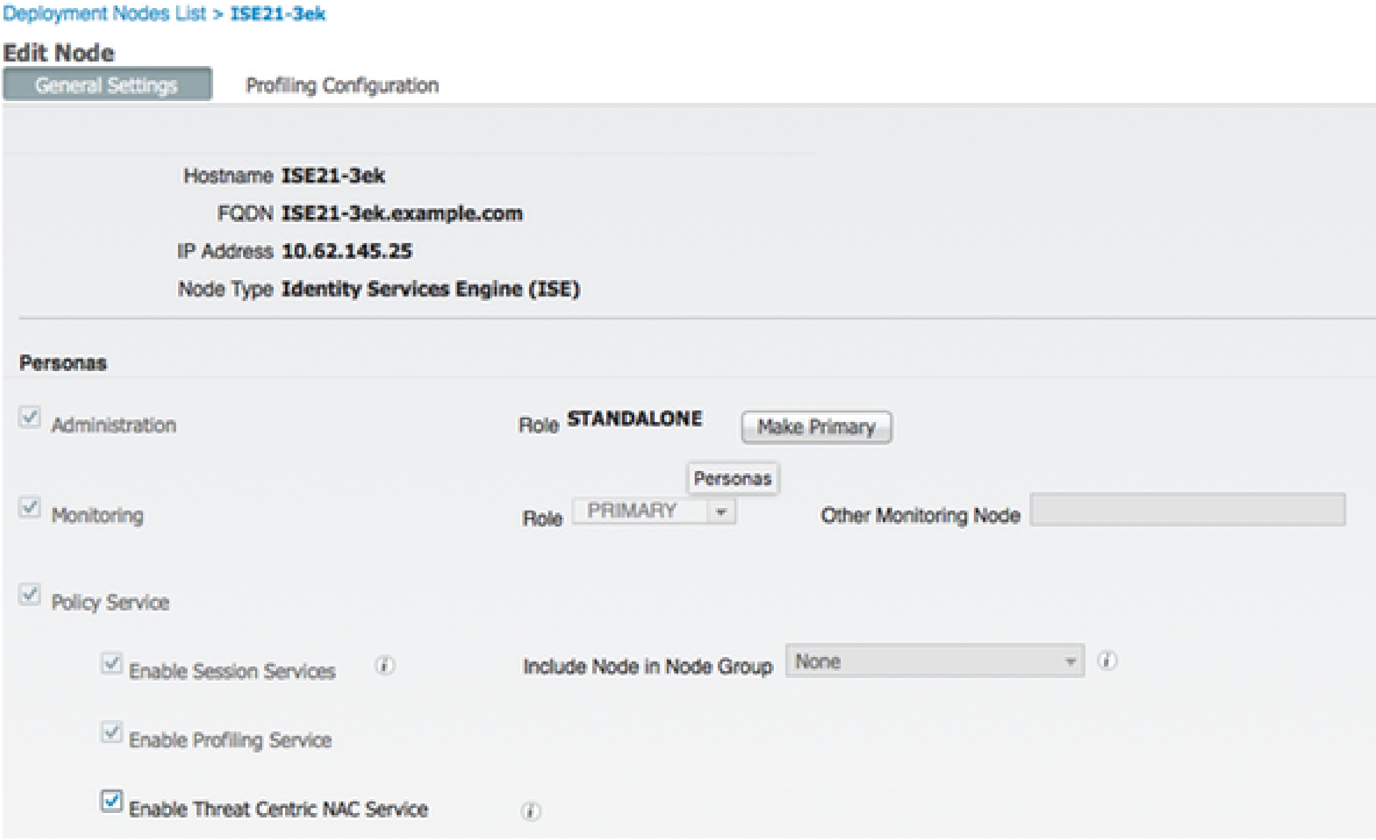
▸ Exceptions (1)

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		

步驟7.啟用TC-NAC服務

在管理>部署>編輯節點下啟用TC-NAC服務。選中**啟用以威脅為中心的NAC服務**覈取方塊。


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]

[Personas]

☑ Monitoring — Role PRIMARY ▾ — Other Monitoring Node

☑ Policy Service

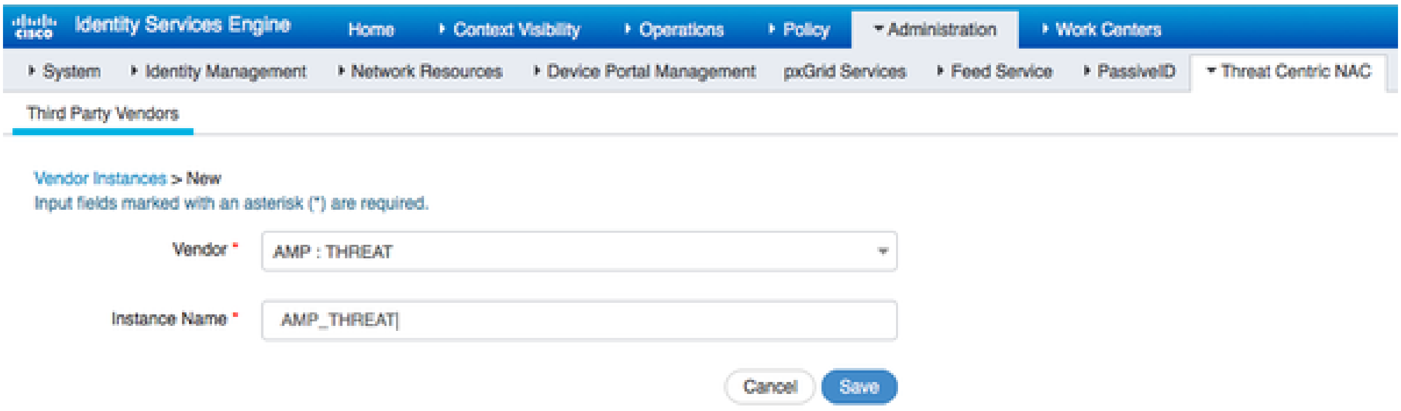
☑ Enable Session Services ⓘ — Include Node in Node Group None ▾ ⓘ

☑ Enable Profiling Service

☑ Enable Threat Centric NAC Service ⓘ

步驟8.配置AMP介面卡

導航到Administration > Threat Centric NAC > Third Party Vendors > Add。按一下**Save**



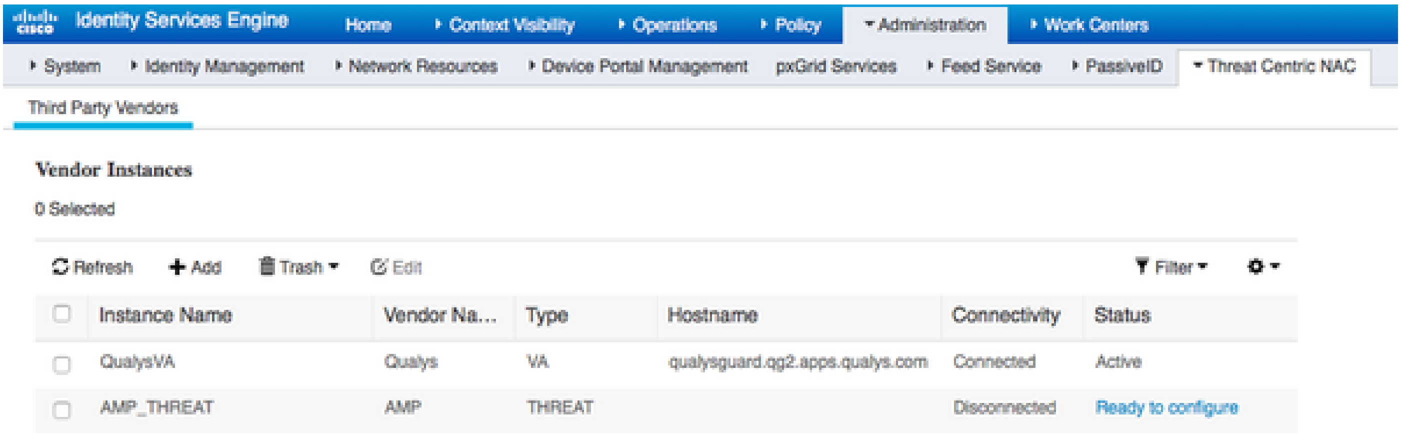
Vendor Instances > New

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

Vendor * AMP : THREAT

Instance Name * AMP_THREAT

它應過渡到**Ready to Configure**狀態。按一下**Ready to Configure**

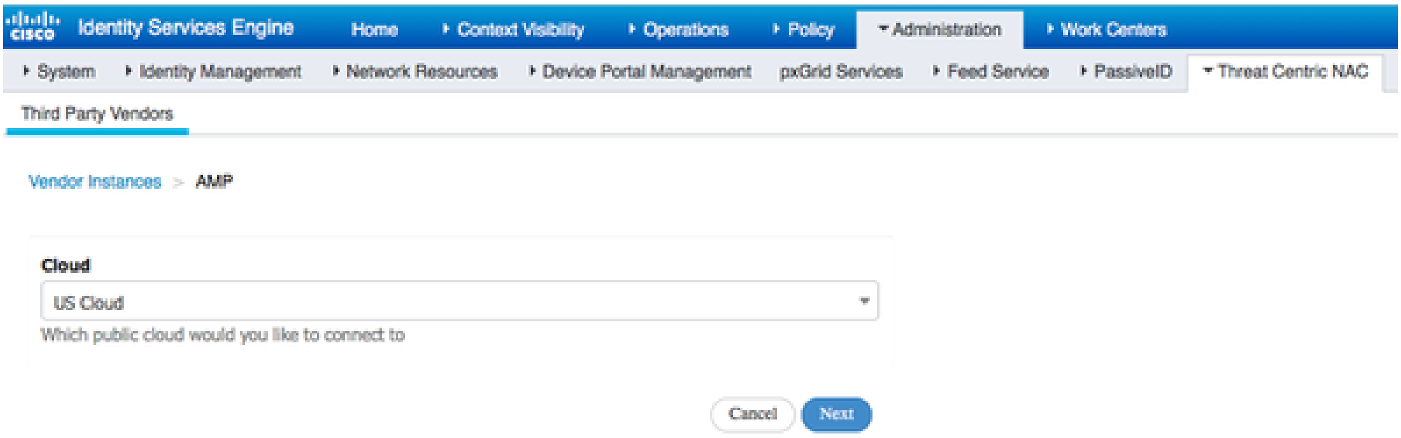


Vendor Instances

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

選擇**Cloud**，然後按一下**Next**



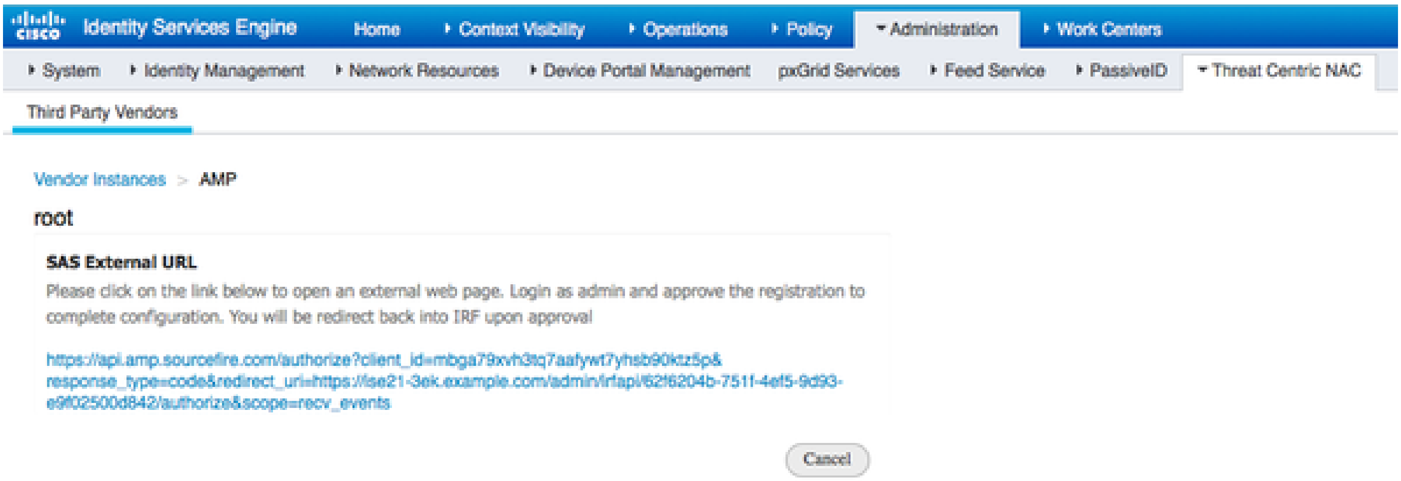
Vendor Instances > AMP

Cloud

US Cloud

Which public cloud would you like to connect to

按一下FireAMP連結並在FireAMP中以admin身份登入。

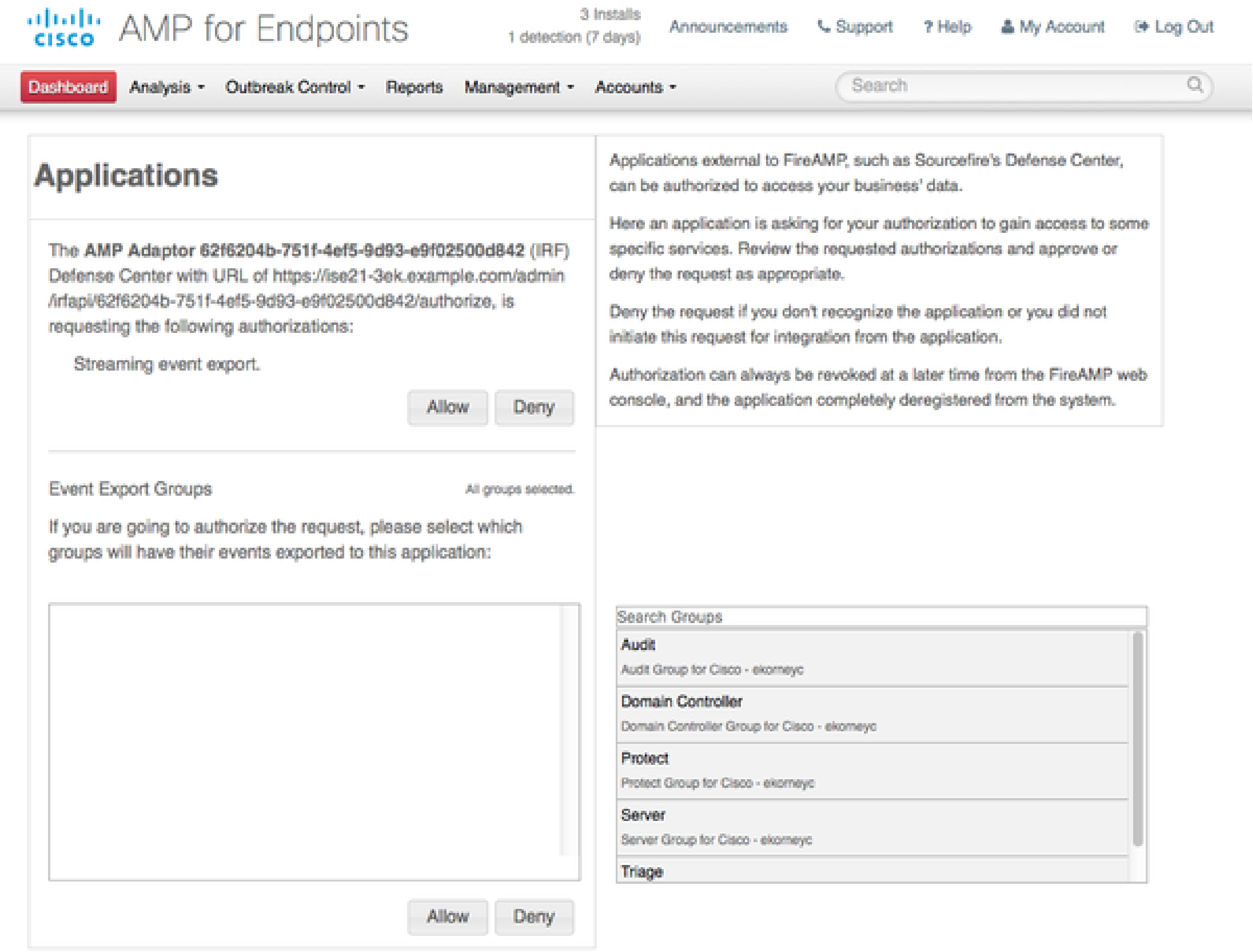


SAS External URL

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

在Applications面板中按一下Allow以授權流事件匯出請求。執行此操作後，您將重定向回思科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.

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:

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.

Audit
Audit Group for Cisco - ekorneyc

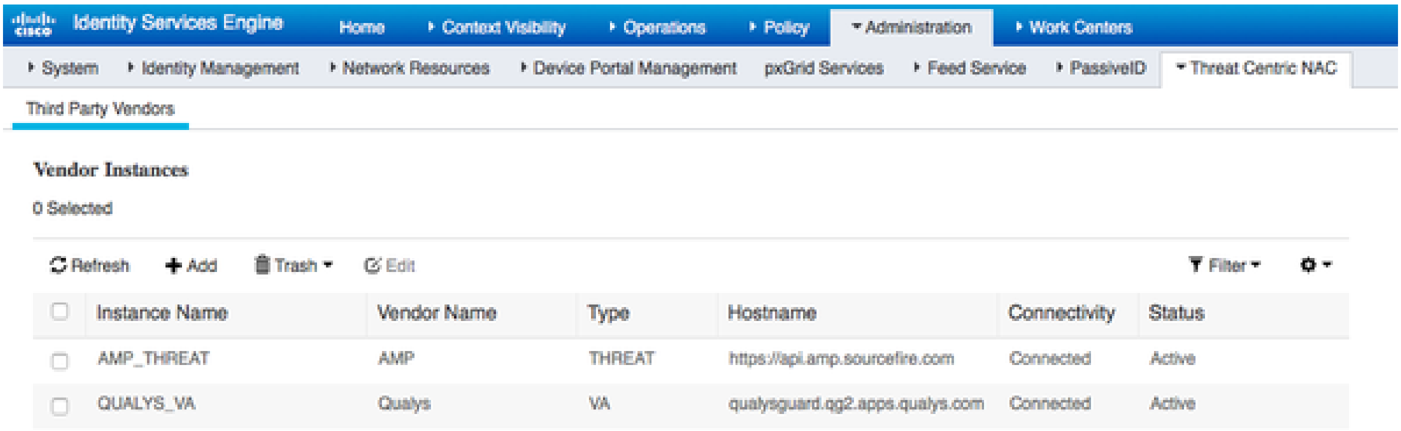
Domain Controller
Domain Controller Group for Cisco - ekorneyc

Protect
Protect Group for Cisco - ekorneyc

Server
Server Group for Cisco - ekorneyc

Triage

選擇要監控的事件（例如，可疑下載、與可疑域的連線、執行的惡意軟體、Java危害）。介面卡例項配置的摘要顯示在配置摘要頁面中。介面卡例項轉變為「已連線/活動」狀態。



Vendor Instances

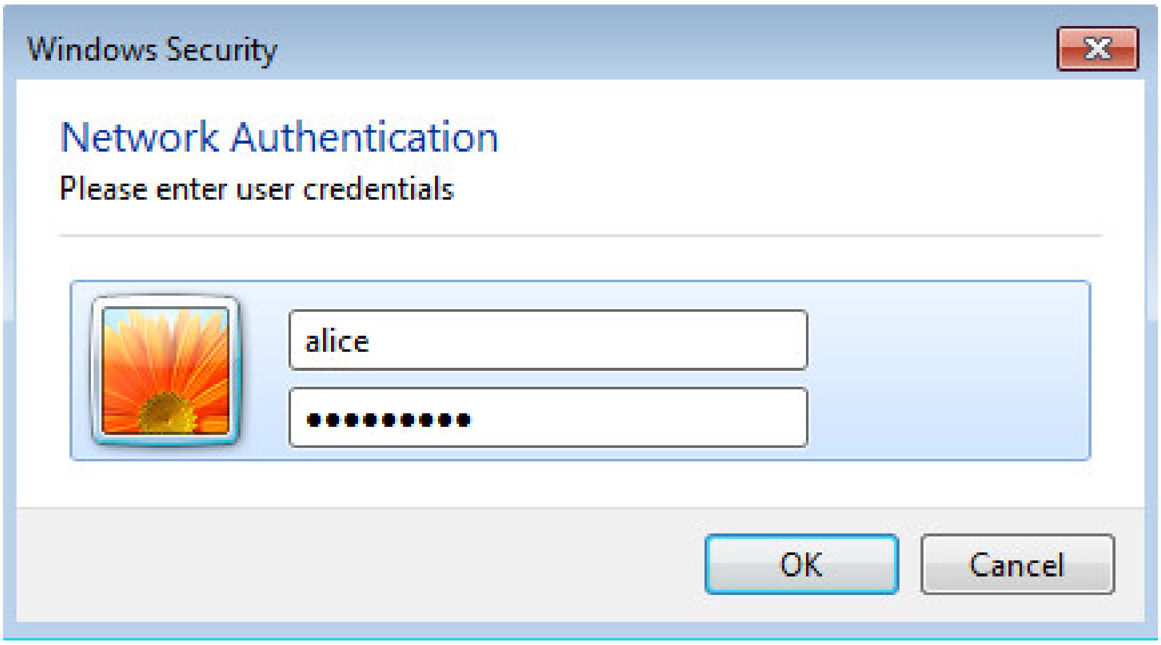
0 Selected

□	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

驗證

終端

通過PEAP(MSCHAPv2)連線到無線網路。



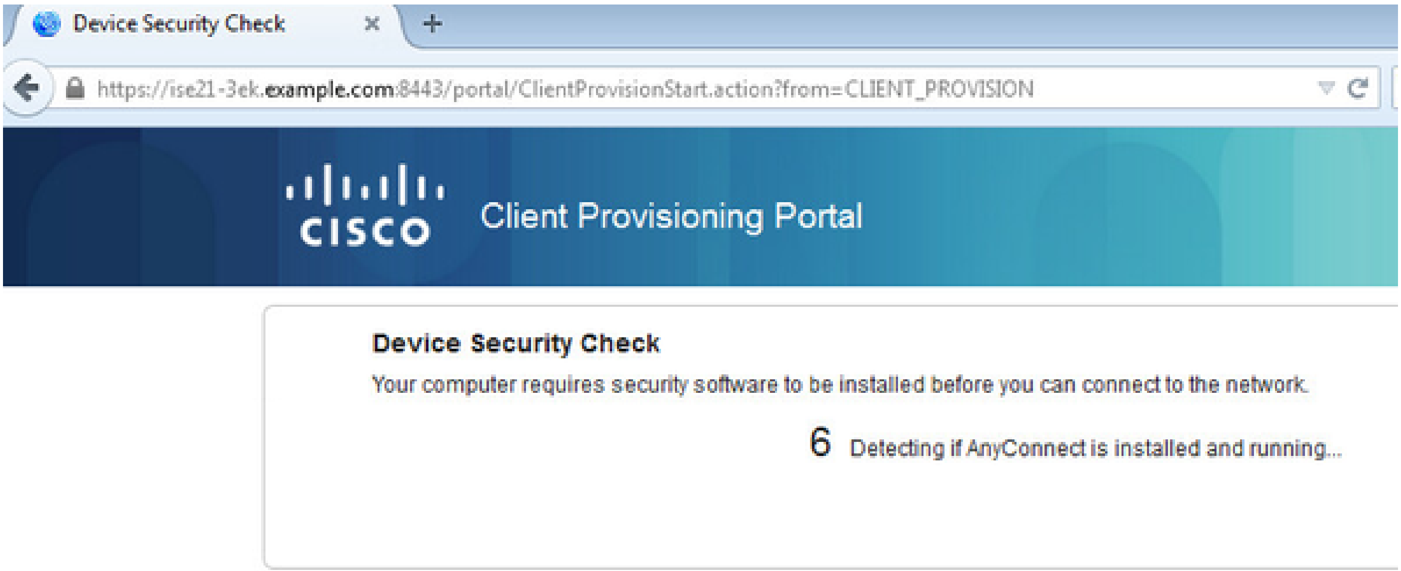
Network Authentication

Please enter user credentials

alice

●●●●●●●●●●

連線到客戶端調配門戶之後。

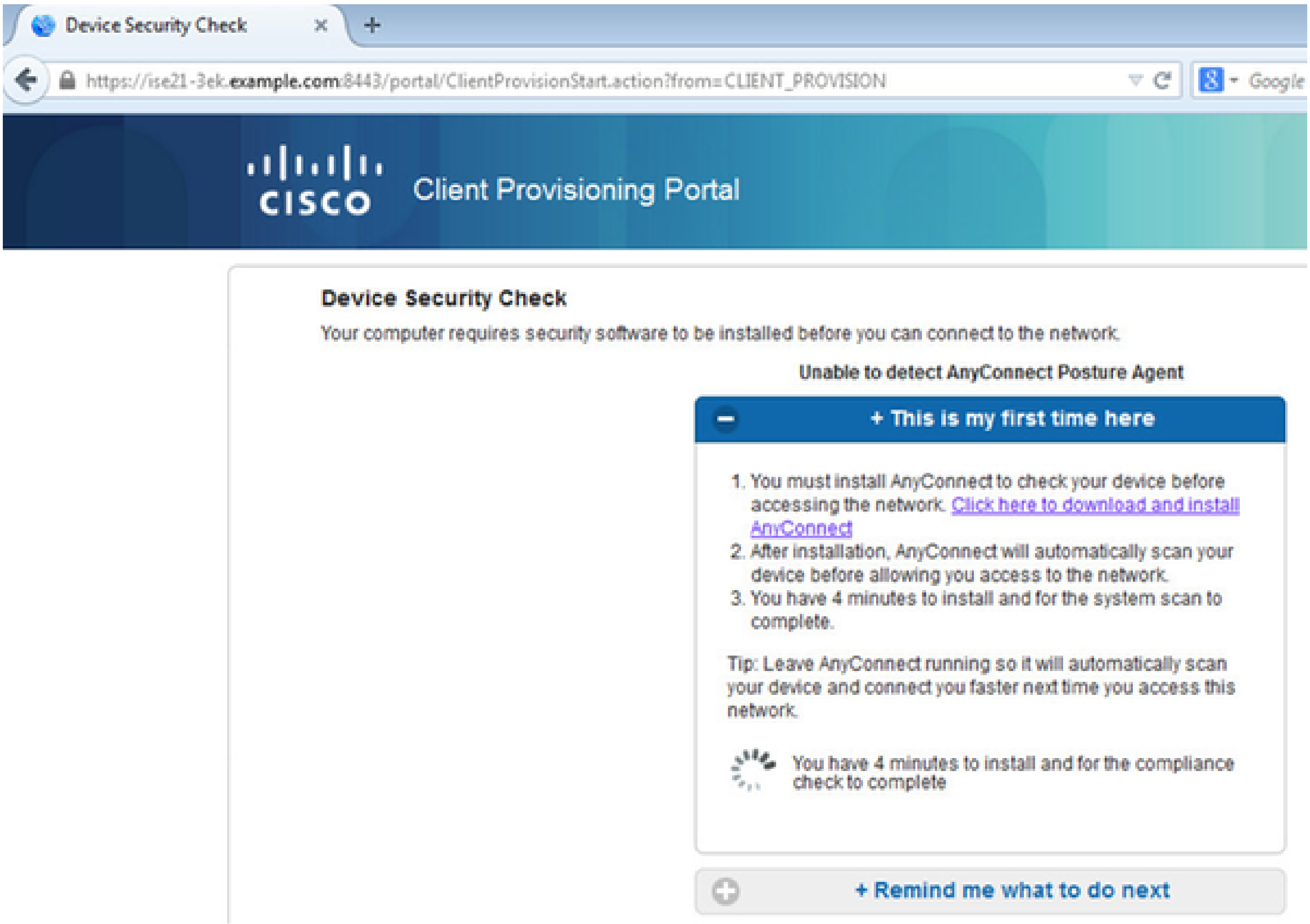

Device Security Check
https://ise21-3ek.example.com:8443/portal/ClientProvisionStart.action?from=CLIENT_PROVISION
Client Provisioning Portal

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...

由於客戶端電腦上未安裝任何內容，因此ISE會提示AnyConnect客戶端安裝。


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

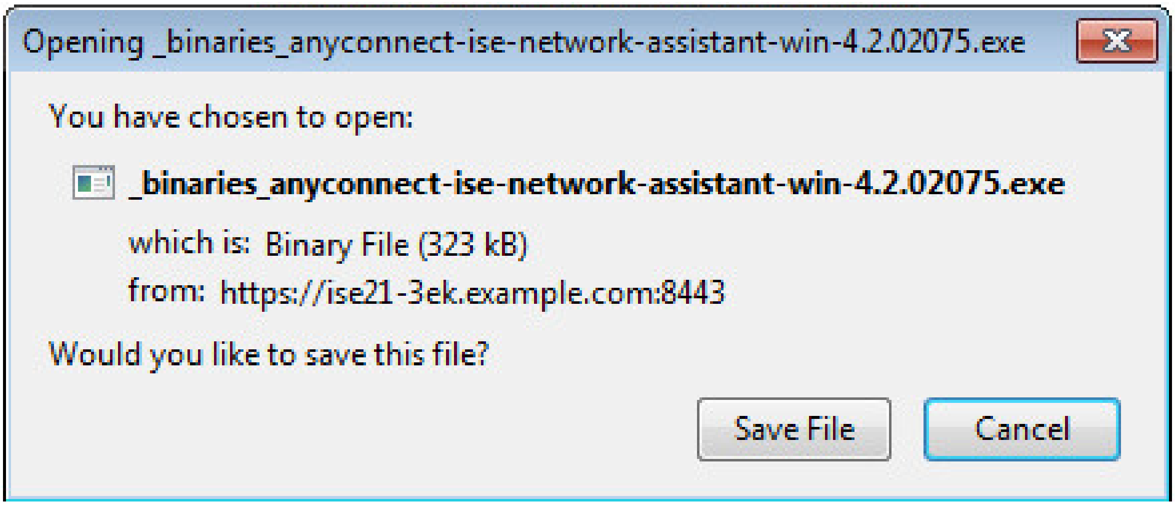
1. You must install AnyConnect to check your device before accessing the network. Click here to download and install AnyConnect
2. After installation, AnyConnect will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to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

應從客戶端電腦下載並運行網路設定助理(NSA)應用程式。



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

You have chosen to open:

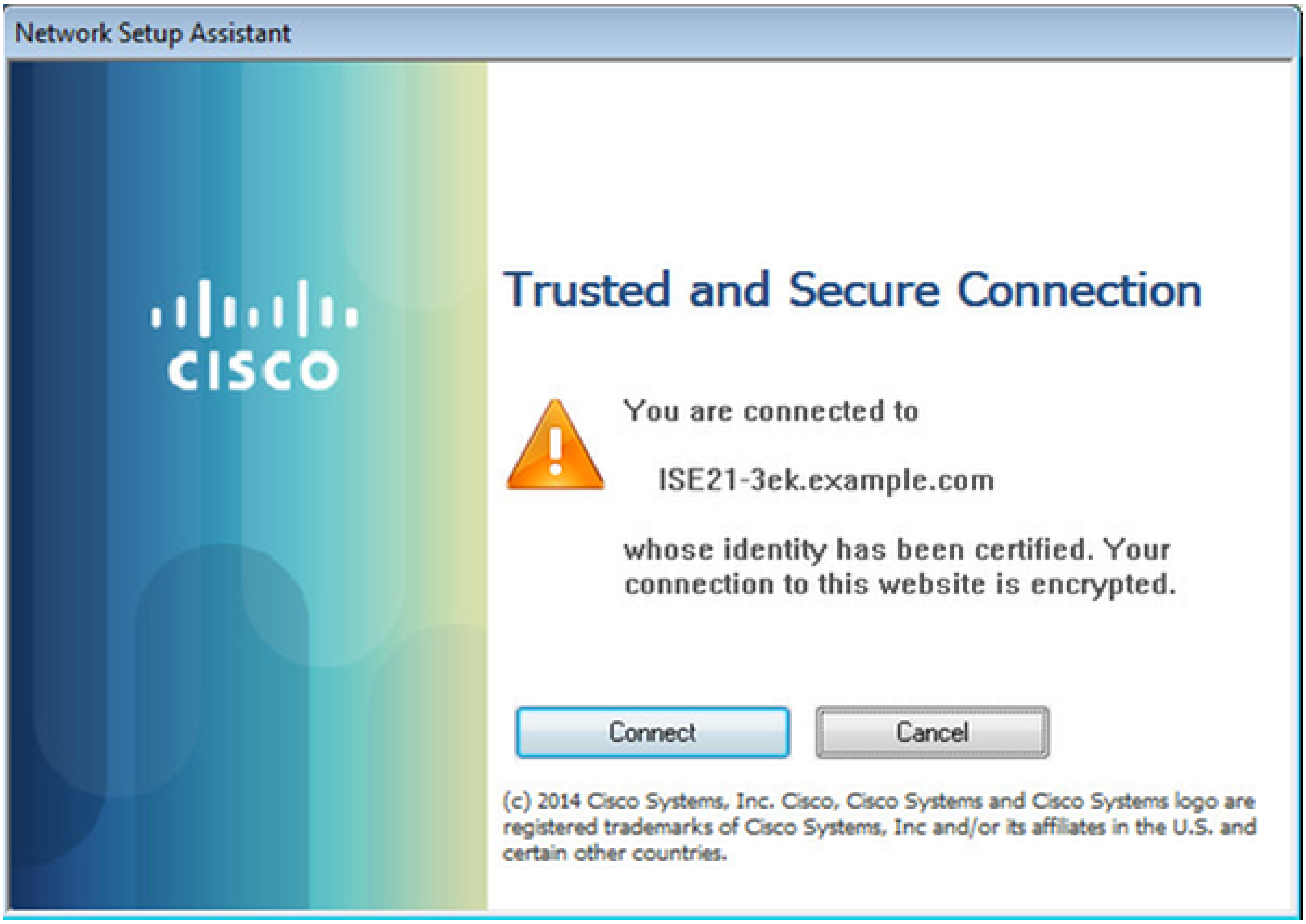
_binaries_anyconnect-ise-network-assistant-win-4.2.02075.exe

which is: Binary File (323 kB)

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

Would you like to save this file?

NSA負責安裝所需的元件和配置檔案。



Network Setup Assistant

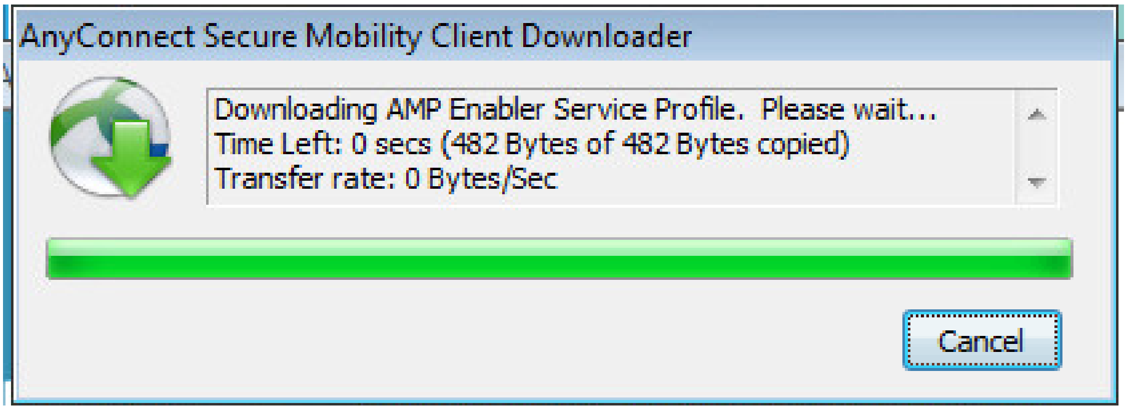
Trusted and Secure Connection

You are connected to

ISE21-3ek.example.com

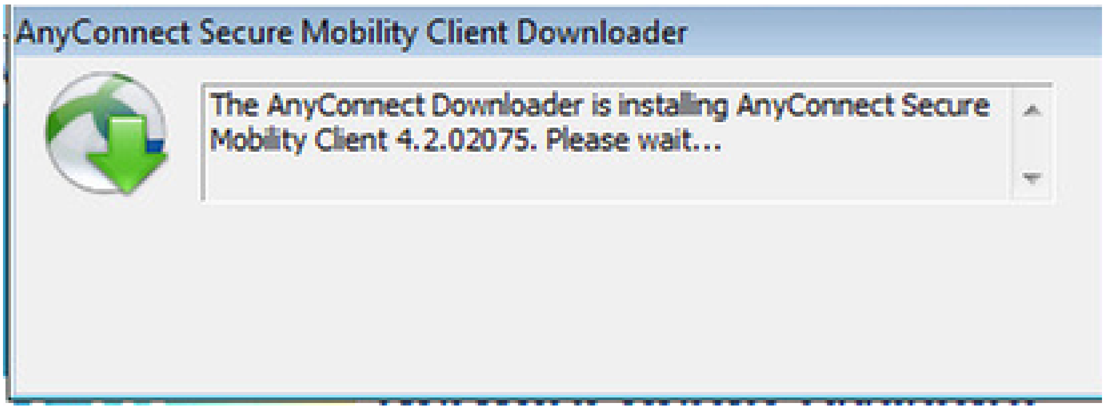
whose identity has been certified. Your connection to this website is encrypted.

(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

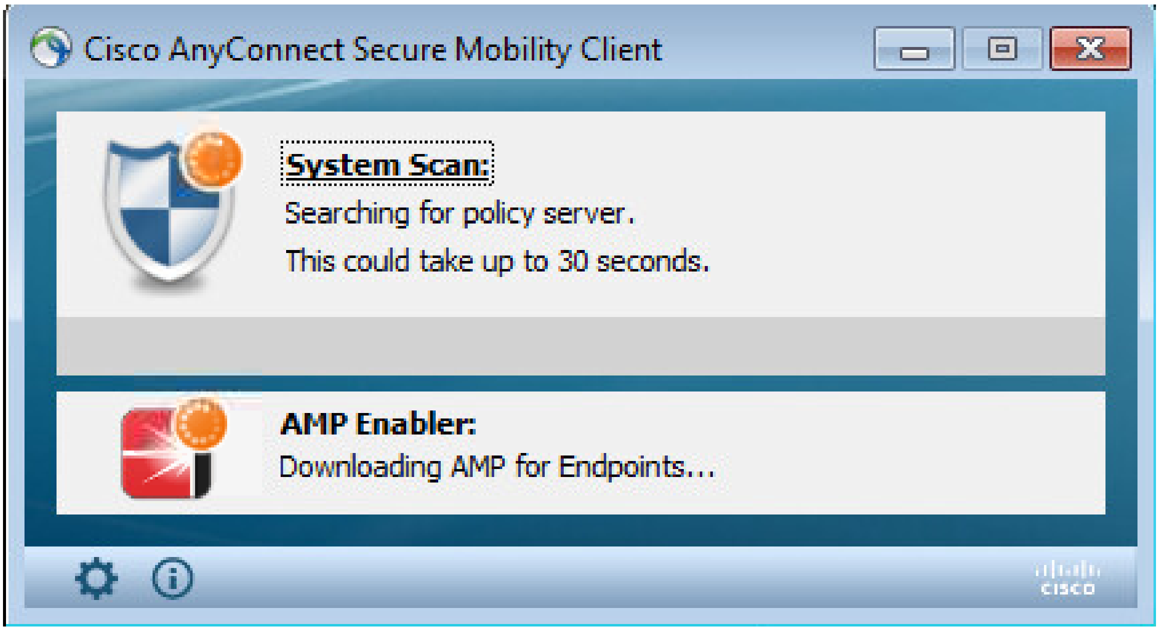
```
Downloading AMP Enabler Service Profile.  Please wait...
Time Left: 0 secs (482 Bytes of 482 Bytes copied)
Transfer rate: 0 Bytes/Sec
```



AnyConnect Secure Mobility Client Downloader

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

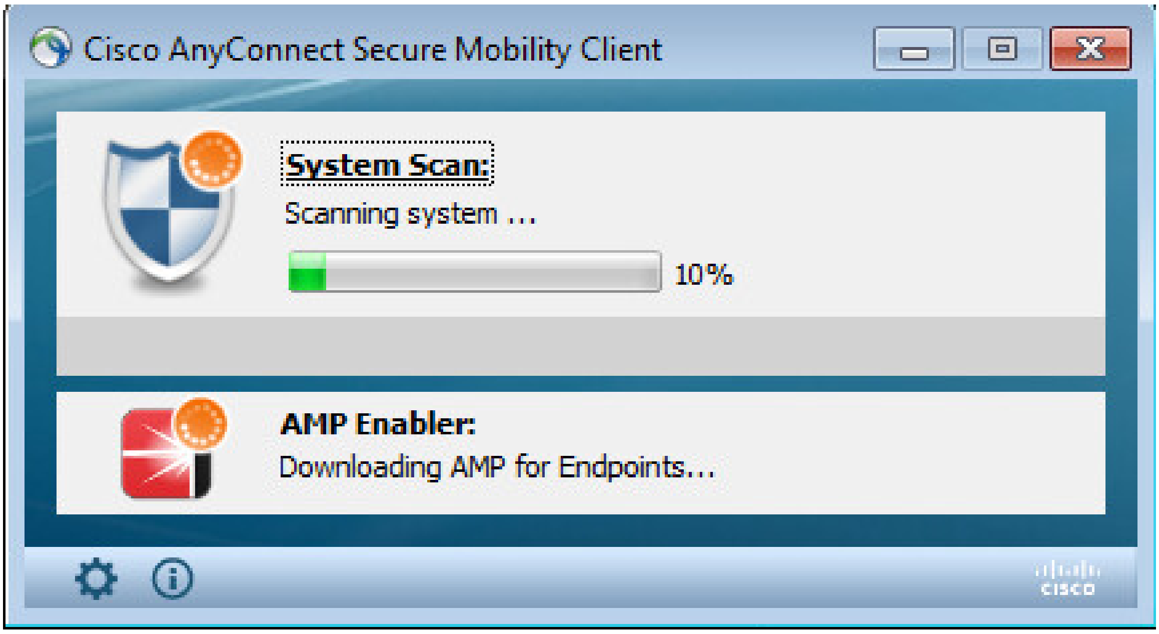
安裝完成後，AnyConnect狀態模組將執行合規性檢查。



Cisco AnyConnect Secure Mobility Client

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

AMP Enabler:
Downloading AMP for Endpoints...

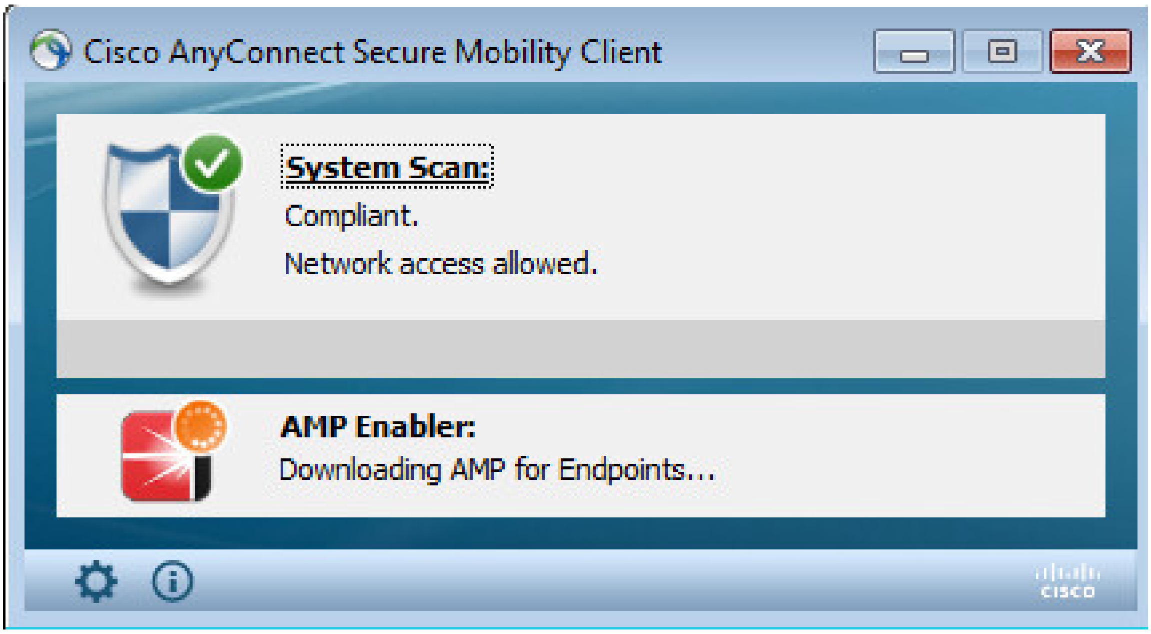


Cisco AnyConnect Secure Mobility Client

System Scan:
Scanning system ...
10%

AMP Enabler:
Downloading AMP for Endpoints...

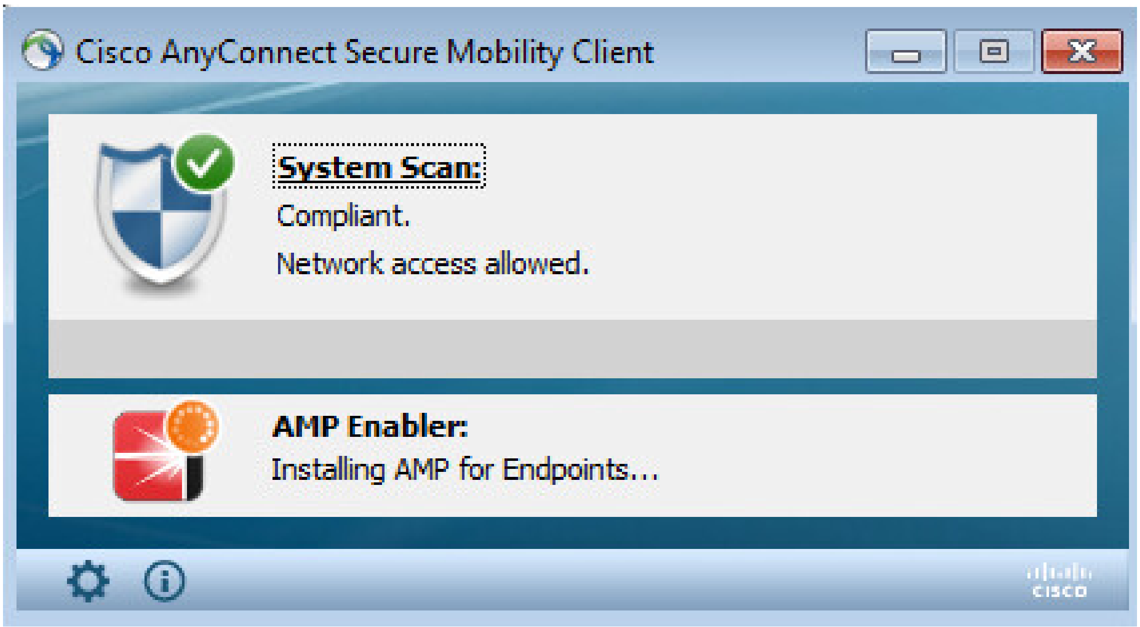
當提供完全訪問許可權時，如果終端符合要求，則從AMP配置檔案中前面指定的Web伺服器下載並安裝AMP。



Cisco AnyConnect Secure Mobility Client

System Scan:
Compliant.
Network access allowed.

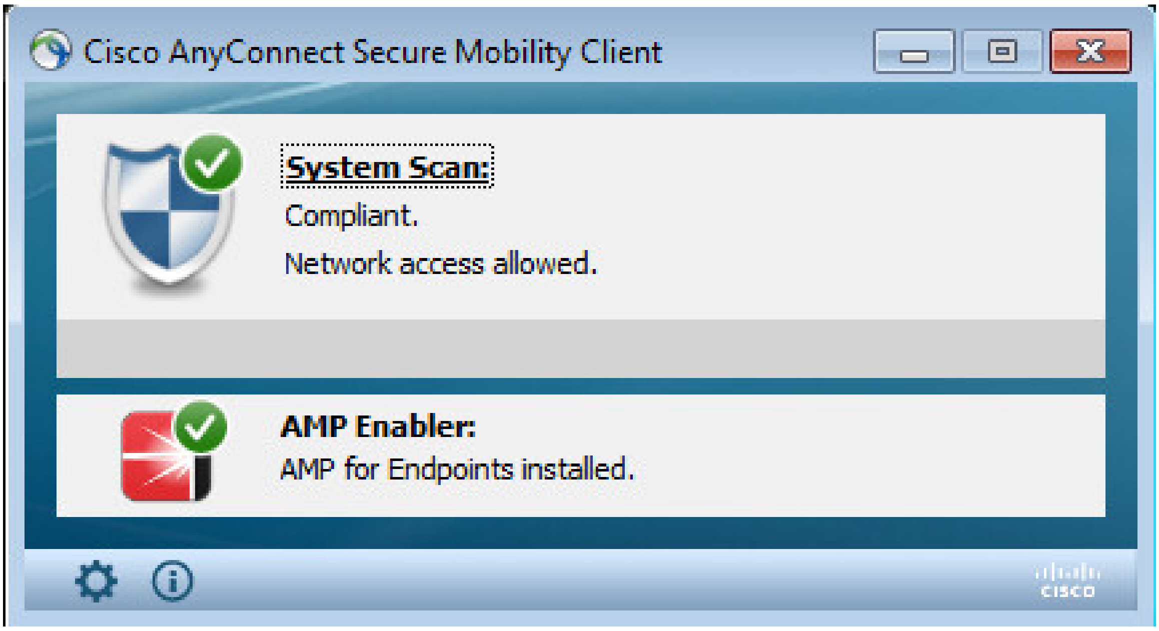
AMP Enabler:
Downloading AMP for Endpoints...



Cisco AnyConnect Secure Mobility Client

System Scan:
Compliant.
Network access allowed.

AMP Enabler:
Installing AMP for Endpoints...

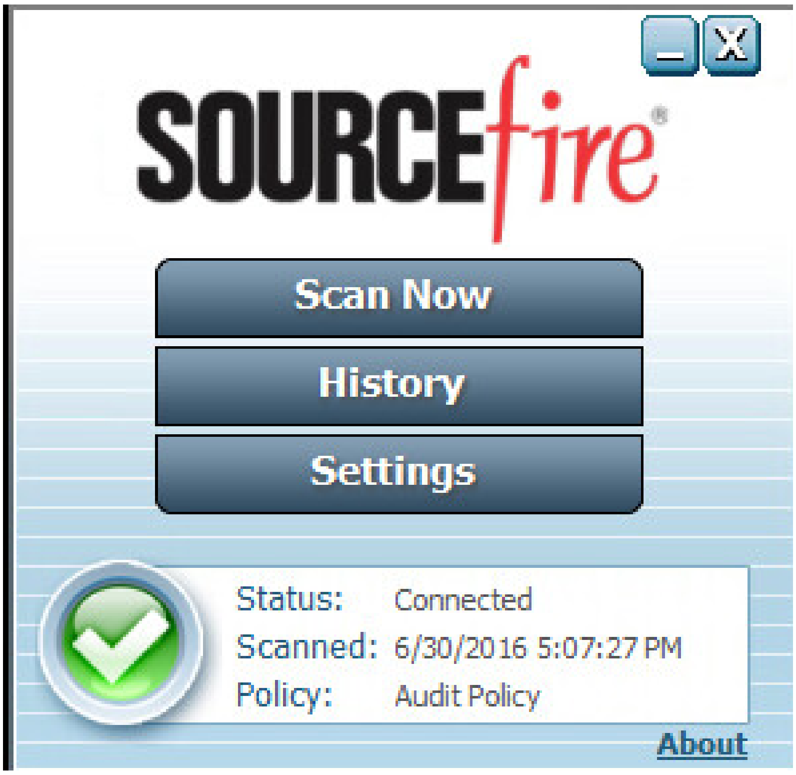


Cisco AnyConnect Secure Mobility Client

System Scan:
Compliant.
Network access allowed.

AMP Enabler:
AMP for Endpoints installed.

AMP聯結器顯示。

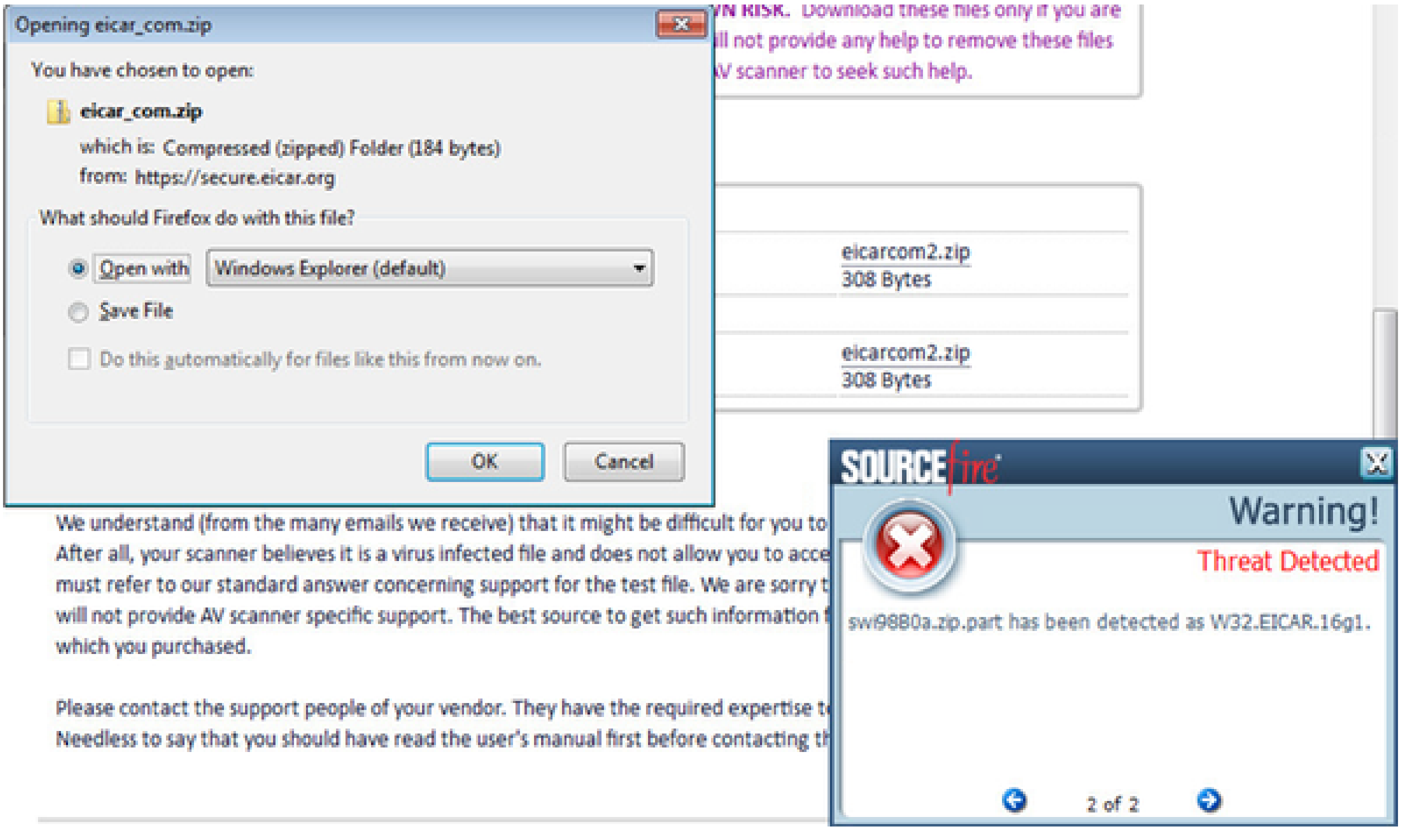


Status: Connected

Scanned: 6/30/2016 5:07:27 PM

Policy: Audit Policy

要測試AMP的實際應用，需要下載zip檔案中包含的Eicar字串。檢測到威脅並將其報告給AMP雲。



Opening eicar_com.zip

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)

○ Save File

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

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

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

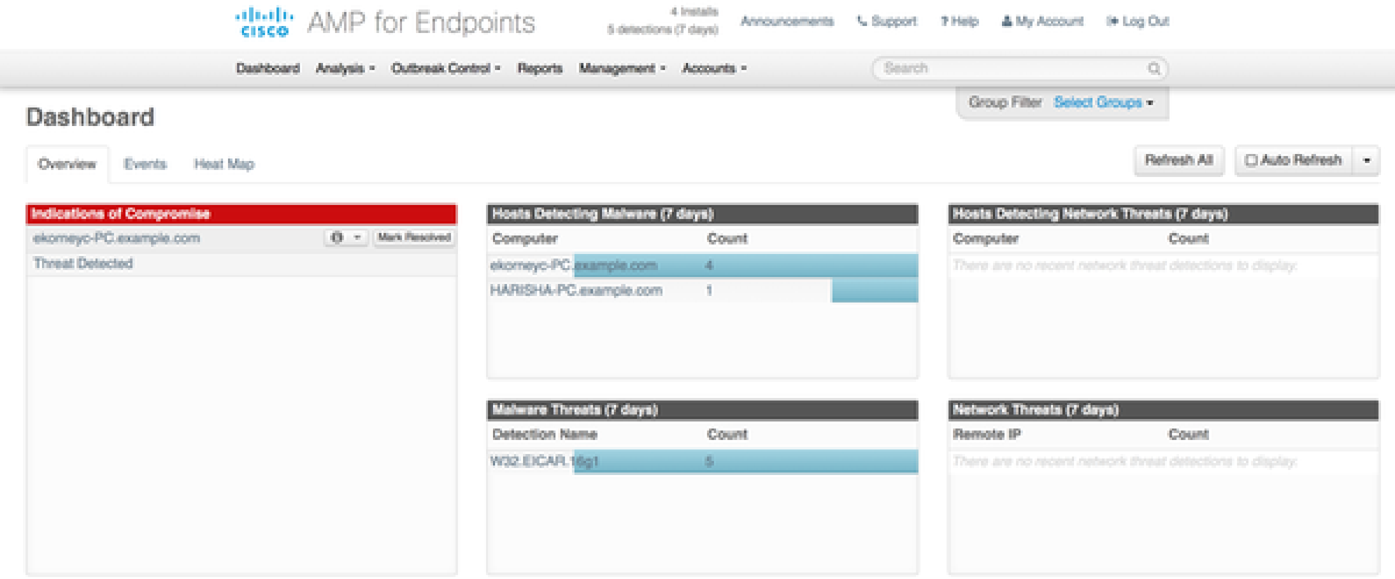
Warning!

Threat Detected

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

AMP雲端

驗證可以使用AMP雲威脅控制面板的詳細資訊。



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.	

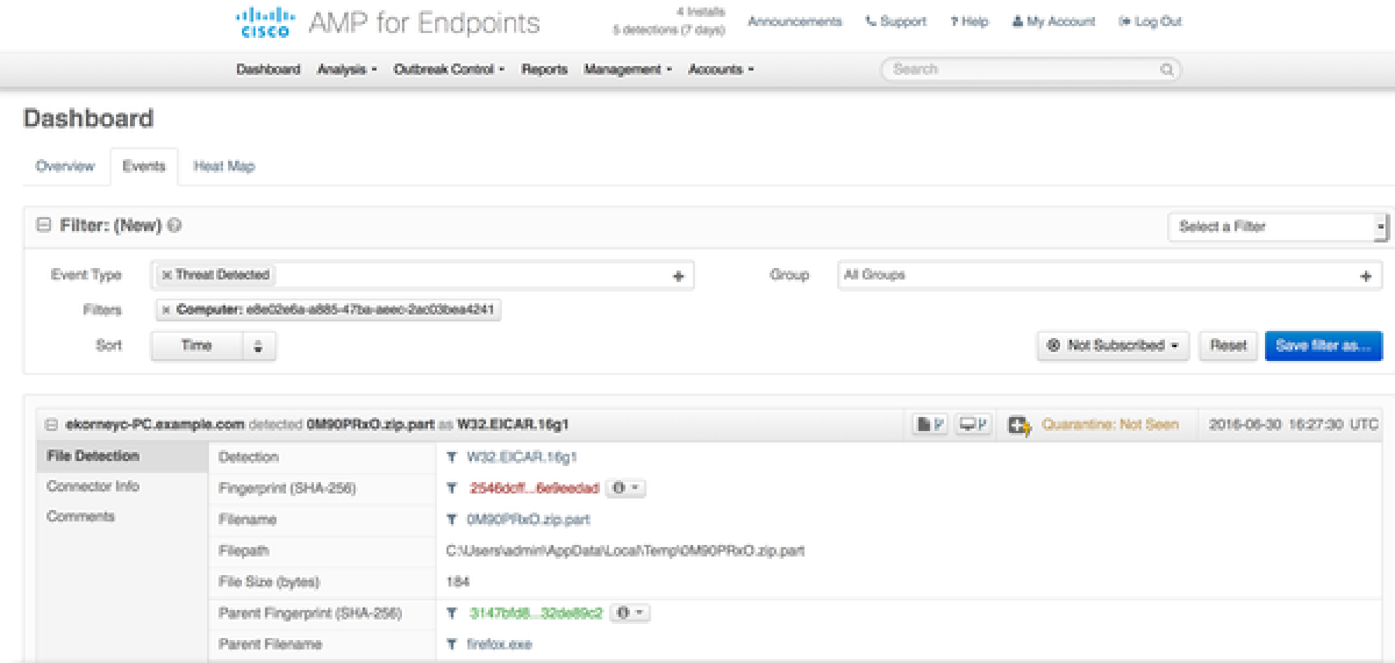
Malware Threats (7 days)

Detection Name	Count
W32.EICAR.16g1	5

Network Threats (7 days)

Remote IP	Count
There are no recent network threat detections to display.	

要獲取有關威脅、檔案路徑和指紋的詳細資訊，可以按一下檢測到惡意軟體的主機。



Filter: (New)

Event Type: × Threat Detected

Group: All Groups

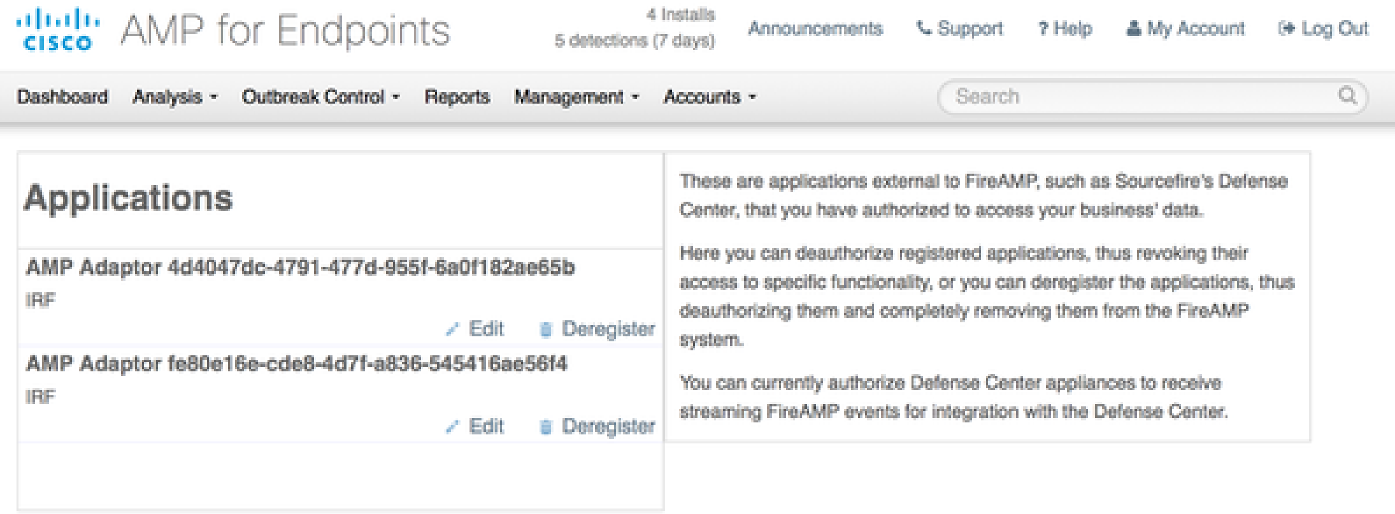
Filters: × Computer: e8e02e6a-a885-47ba-aeec-2ac03bea4241

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

要檢視或註銷ISE例項，您可以導航到Accounts > Applications



Applications

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

IRF

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

IRF

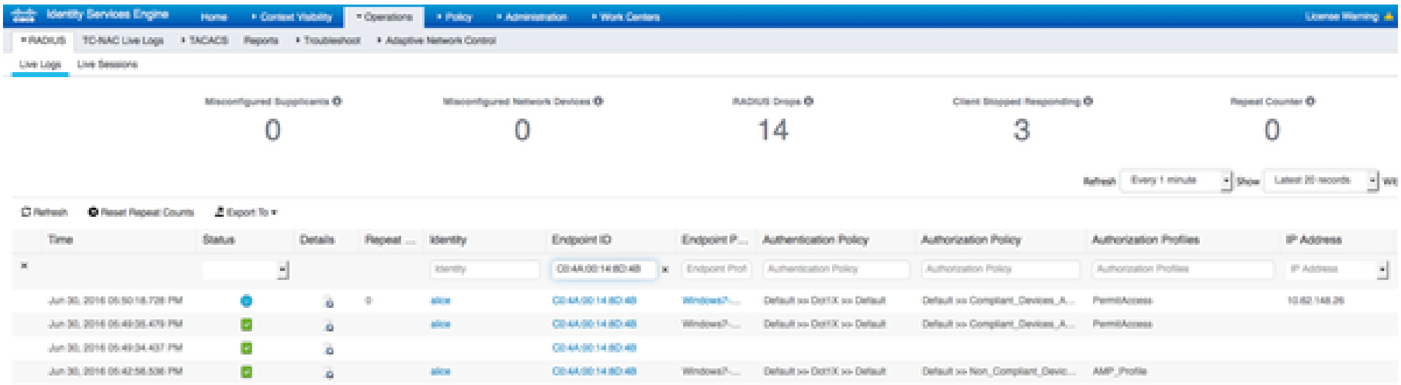
These are applications external to FireAMP, such as Sourcefire's Defense Center, that you have authorized to access your business' data.

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.

ISE

在ISE本身上看到常規狀態流程，首先進行重定向以檢查網路合規性。只要終端符合要求，就會傳送CoA Reauth並分配具有PermitAccess的新配置檔案。

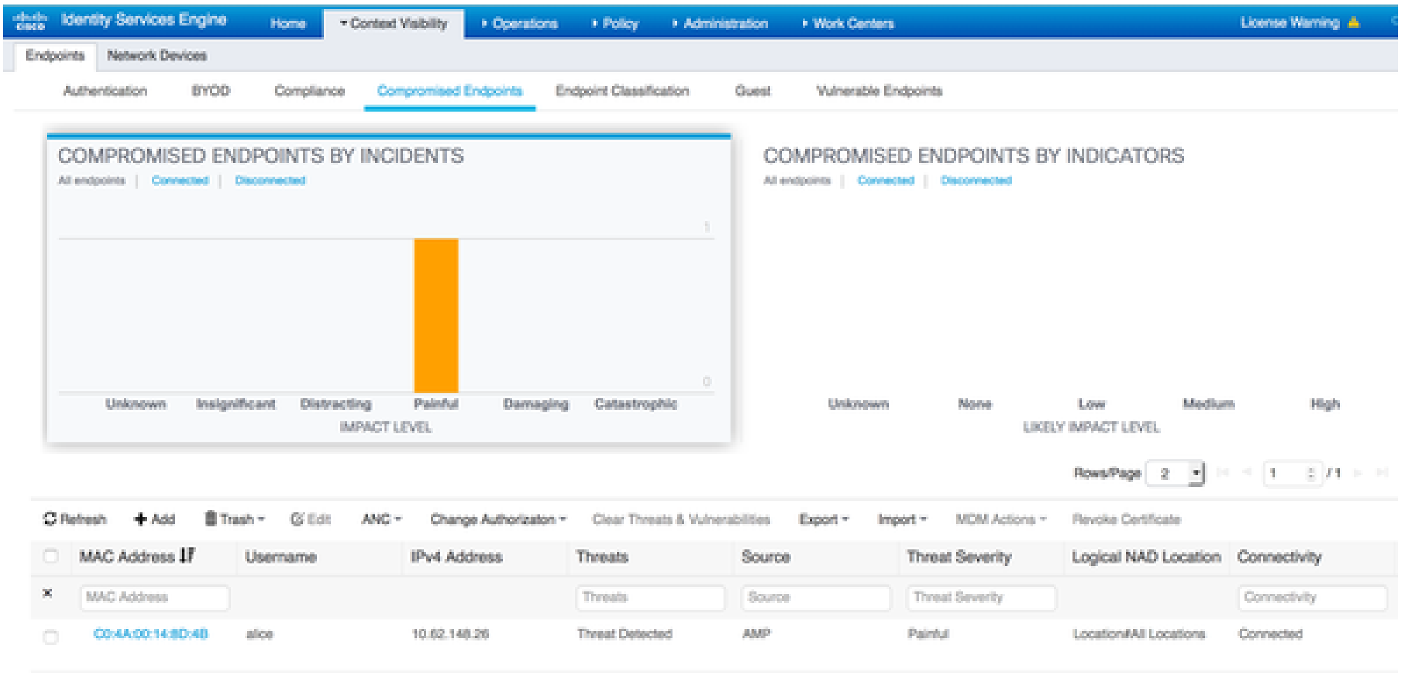


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	14	3	0

Refresh: Every 1 minute; Show: Latest 20 records

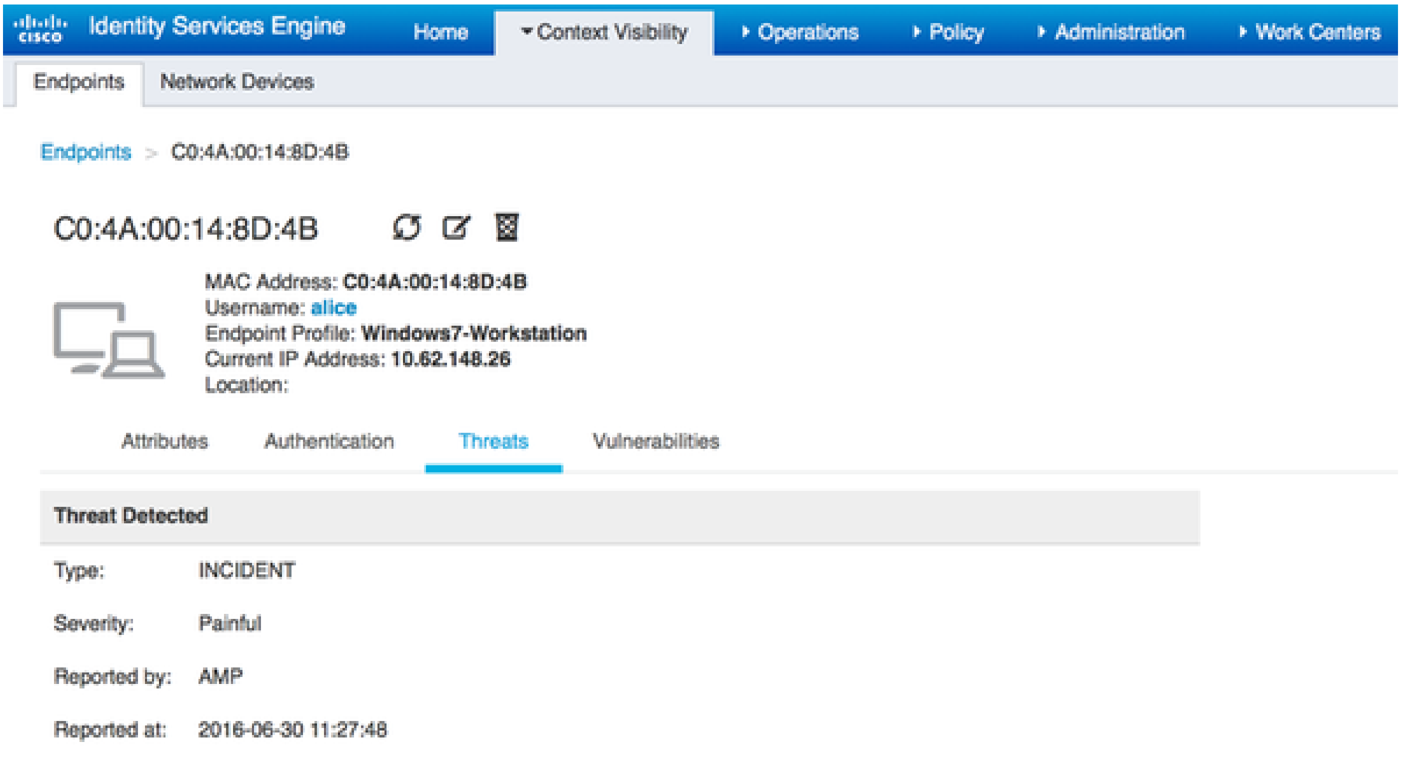
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
				Identity	C0:4A:00:14:8D:4B	Endpoint Prof	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Jun 30, 2016 05:50:18.728 PM	●		0	alice	C0:4A:00:14:8D:4B	Windows7-...	Default >> Dot1X >> Default	Default >> Compliant_Devices_A...	PermitAccess	10.62.148.26
Jun 30, 2016 05:49:35.479 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 05:42:58.536 PM	✓			alice	C0:4A:00:14:8D:4B	Windows7-...	Default >> Dot1X >> Default	Default >> Non_Compliant_Devic...	AMP_Profile	

要檢視檢測到的威脅，您可以導航到Context Visibility > Endpoints > Compressed Endpoints



□	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

如果選擇終端並導航到Threat頁籤，將顯示更多詳細資訊。



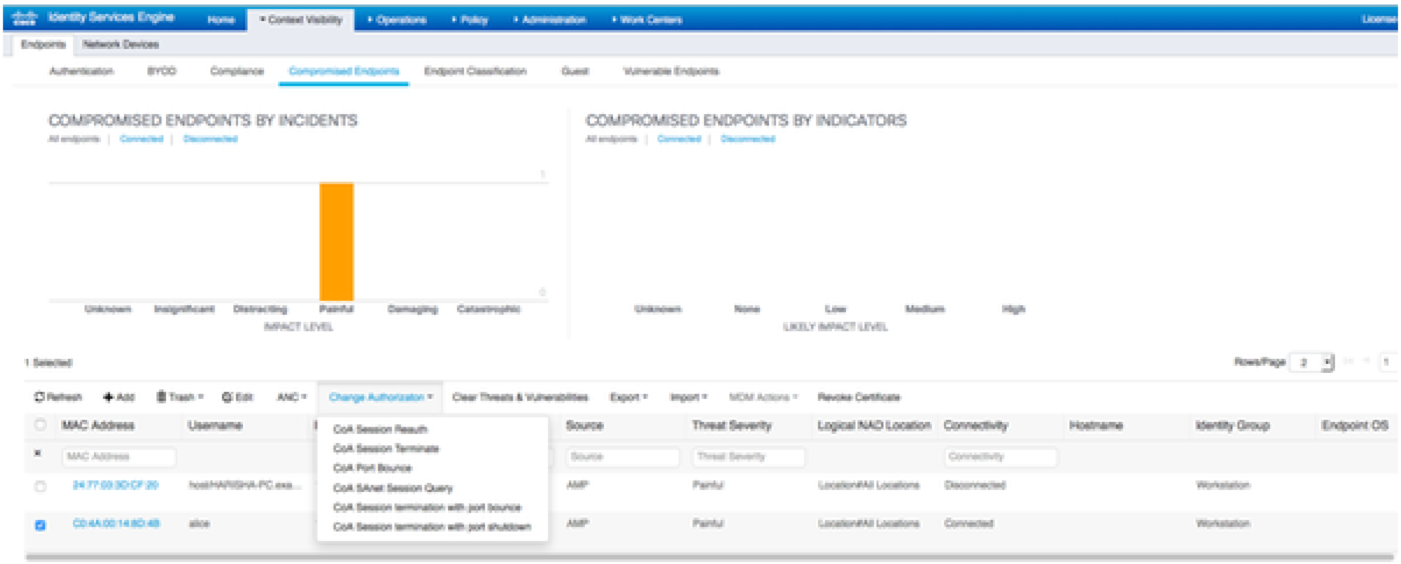
C0:4A:00:14:8D:4B

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

Threat Detected

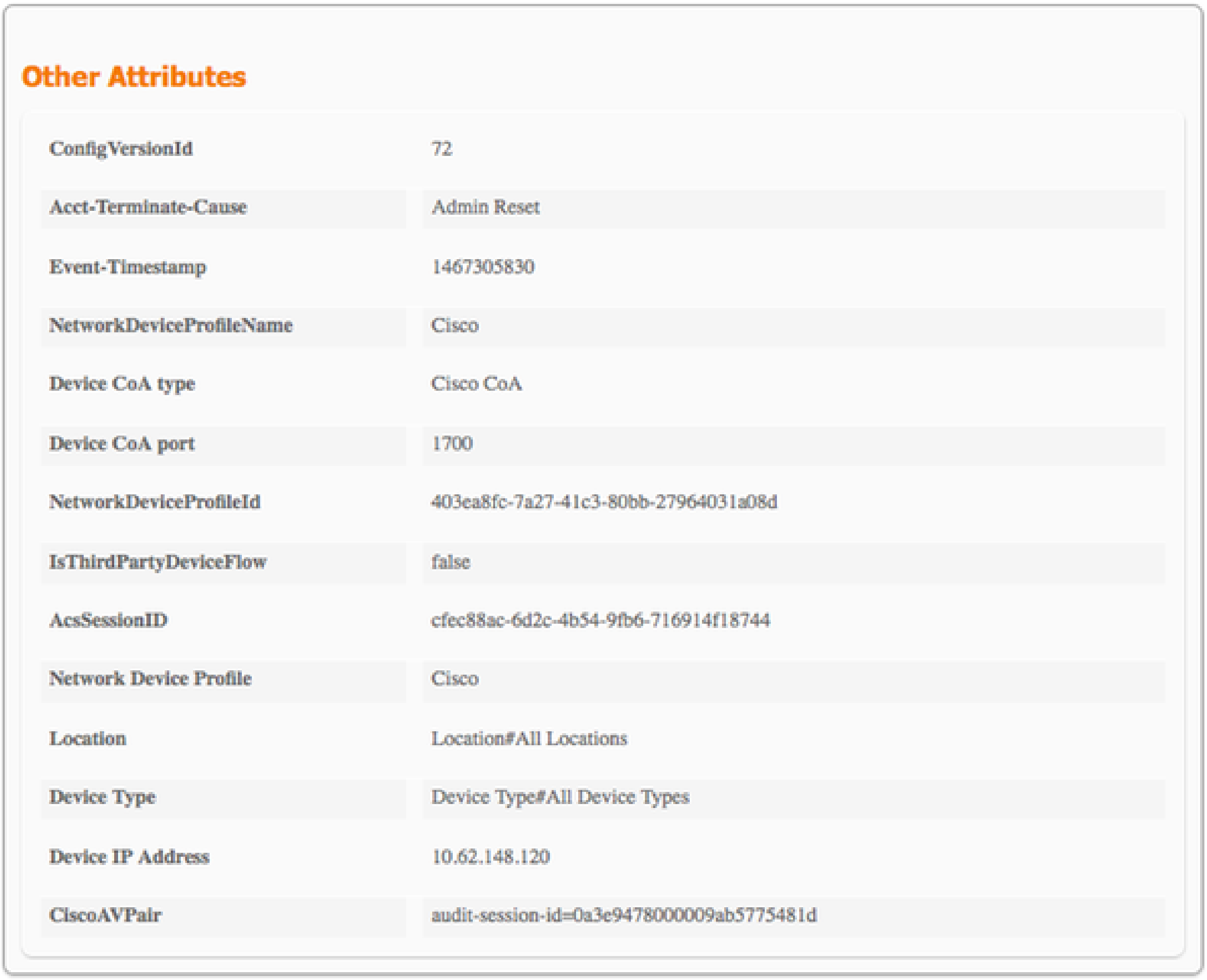
Type:	INCIDENT
Severity:	Painful
Reported by:	AMP
Reported at:	2016-06-30 11:27:48

當檢測到終端的威脅事件時，您可以在「受危害的終端」頁面上選擇終端的MAC地址並應用ANC策略（如果已配置，例如隔離）。 或者，您可以發出「更改授權」以終止會話。



	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	

如果選擇了CoA Session Terminate，ISE會傳送CoA Disconnect，客戶端將失去對網路的訪問許可權。

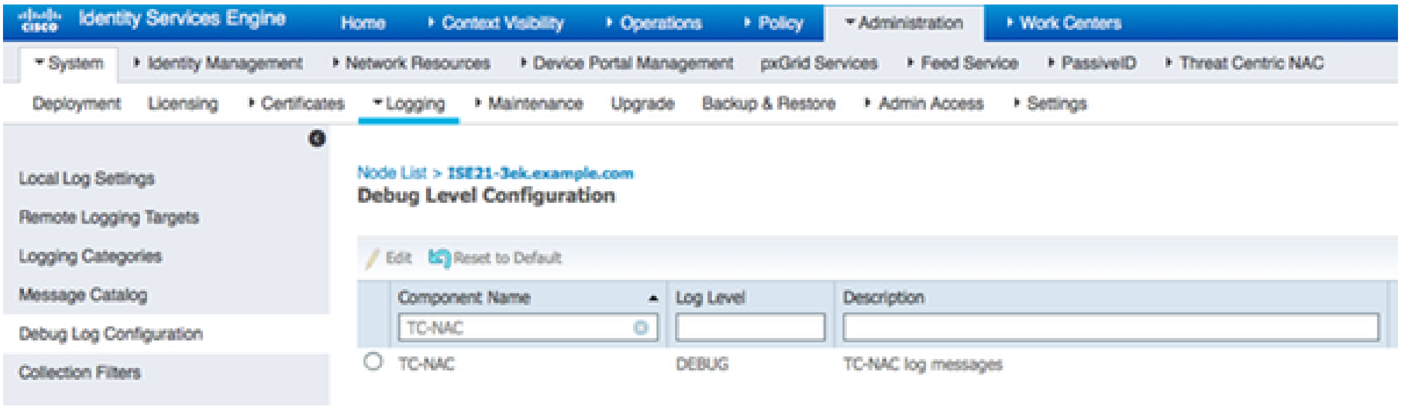


Other Attributes

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

疑難排解

若要在ISE上啟用調試，請導航到Administration > System > Logging > Debug Log Configuration，選擇TC-NAC Node，並將**Log Level** of TC-NAC元件更改為**DEBUG**



Node List > ISE21-3ek.example.com

Debug Level Configuration

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

要檢查的日誌 — irf.log。您可以直接從ISE CLI對其進行跟蹤：

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

威脅甚至從AMP雲接收

```
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 -::: –
com.cisco.cpm.irf.service.IrfNotificationHandler$MyNotificationHandler@3fac8043
Message{messageType=NOTIFICATION messageId=THREAT content='{:c0:4a 00:14:8d:4b[{"
":{"Impact_Qualification":""},"":1467304068599vendor"AMP""":"Threat Detected"}]}', priority=0,
timestamp=Thu Jun 30 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
headts=null headts=null rement-mode=null priority=0, correlation-id=null EVENT timestamp=null
type=NOTIFICATION user-id=null app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=null)}
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.service.IrfNotificationHandler:handle:140 -::::: –
Message{messageType=NOTIFICATION messageId=THREAT_EVENT content='{"c0:4a:00:14:8d:4b":[{"
":{"Impact_Qualification":"Paulse"},"":1467304068599vendor"AMP", "":Threat Detected"}]}',
priority=0, timestamp=Thu Jun 30 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
headts=null delivery-mode=null priority=0, correlation-id=null reply – to=null timestamp=null
type=NOTIFICATION user-id=null app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=null)}
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:59 -::::: – 545416
Envelope(deliveryTag=79, redeliver=false exchange=irf.topic.events
routingKey=irf.events.threat)#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-a88836-a556, id=
2016-06-30 18:27:48,706 DEBUG [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:parseNotification:221 -:::: –
Message{messageType=NOTIFICATION messageId=THREAT_EVENT content='{"c0:4a:00:14:8d:4b":[{"
":{"Impact_Qualification":""},"":1467304068599vendor"AMP""":Threat Detected"}]}', priority=0,
timestamp=Thu Jun 30 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
headts=null delivery-mode=null priority=0, correlation-id=null reply – to=null timestamp=null
type=NOTIFICATION user-id=null app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=null)}
```

有關威脅的資訊將傳送到PAN

```
2016-06-30 18:27:48,724 DEBUG [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:storeEventsInES:366 -:::: – PAN - c0:4a:00:14:8d:4b
{incident={Impact_Qualification=Pain},time-amp=1467304068599=PAN Title=}
```