

AMP とポスチャ サービスの ISE 2.1 脅威中心型 NAC (TC-NAC) を設定する

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[詳細フロー](#)

[AMP クラウドの設定](#)

[手順 1 : AMP クラウドからコネクタをダウンロードする](#)

[ISE の設定](#)

[手順 1 : ポスチャ ポリシーと条件の設定](#)

[手順 2 : ポスチャ プロファイルの設定](#)

[手順 3 : AMP プロファイルの設定](#)

[手順 2 : ISE にアプリケーションと XML プロファイルをアップロードする](#)

[手順 3 : AnyConnect コンプライアンス モジュールをダウンロードする](#)

[手順 4 : AnyConnect 設定の追加](#)

[手順 5 : クライアント プロビジョニング ルールの設定](#)

[手順 6 : 許可ポリシーの設定](#)

[手順 7 : TC-NAC サービスの有効化](#)

[手順 8 : AMP アダプタの設定](#)

[確認](#)

[エンドポイント](#)

[AMP クラウド](#)

[ISE](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Identity Services Engine (ISE) 2.1 で Advanced Malware Protection (AMP) を使用して脅威中心型 NAC を設定する方法について説明します。脅威の重大度と脆弱性アセスメントの結果を使用することで、エンドポイントまたはユーザのアクセスレベルを動的に制御することができます。ポスチャ サービスについてもこのドキュメントの一部として説明します。

注: 本書の目的は、ISE 2.1 と AMP の統合について説明することであり、ポスチャ サービスは、AMP を ISE からプロビジョニングする際に必要であるために示しています。

前提条件

要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- Cisco Identity Service Engine
- 高度なマルウェア対策

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Identity Service Engine バージョン 2.1
- ワイヤレス LAN コントローラ (WLC) 8.0.121.0
- AnyConnect VPN クライアント 4.2.02075
- Windows 7 Service Pack 1

設定

ネットワーク図



詳細フロー

1. クライアントがネットワークに接続し、AMP_Profile が割り当てられます。ユーザは Anyconnect のプロビジョニング ポータルにリダイレクトされます。Anyconnect がマシンで検出されなかった場合、設定されたすべてのモジュール (VPN、AMP、ポスチャ) がインストールされます。設定は、そのプロファイルとともに、各モジュールにプッシュされます。

2. Anyconnect がインストールされたら、ポスチャ アセスメントが実行されます。

3. AMP イネーブラ モジュールが FireAMP コネクタをインストールします。
4. クライアントが悪意のあるソフトウェアをダウンロードしようとする時、AMP コネクタは警告メッセージを投げ、AMP クラウドにそれを報告します。
5. AMP クラウドは、ISE にこの情報を送信します。

AMP クラウドの設定

手順 1 : AMP クラウドからコネクタをダウンロードする

コネクタをダウンロードするには、[Management] > [Download Connector] に移動します。タイプを選択し、FireAMP (Windows、Android、Mac、Linux) をダウンロードします。この場合、[Audit] が選択され、Windows 用の FireAMP のインストール ファイルがダウンロードされます。

注: このファイルをダウンロードすると、には、この例で **Audit_FireAMPSetup.exe** と呼ばれる .exe ファイルが生成されます。このファイルは、ユーザが AMP の設定を依頼したときに使用できるように Web サーバに送られました。

ISE の設定

手順 1 : ポスチャ ポリシーと条件の設定

[Policy] > [Policy Elements] > [Conditions] > [Posture] > [File Condition] に移動します。ファイルの存在に関するシンプルな条件が作成されたことがわかります。エンドポイントがポスチャ モジュールによって検証済みのポリシーに準拠する場合、ファイルは存在しなければなりません。

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

Description

* Operating System

Compliance Module Any version

* File Type ⓘ

* File Path ⓘ

* File Operator

- 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

この条件は要件に使用されます。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

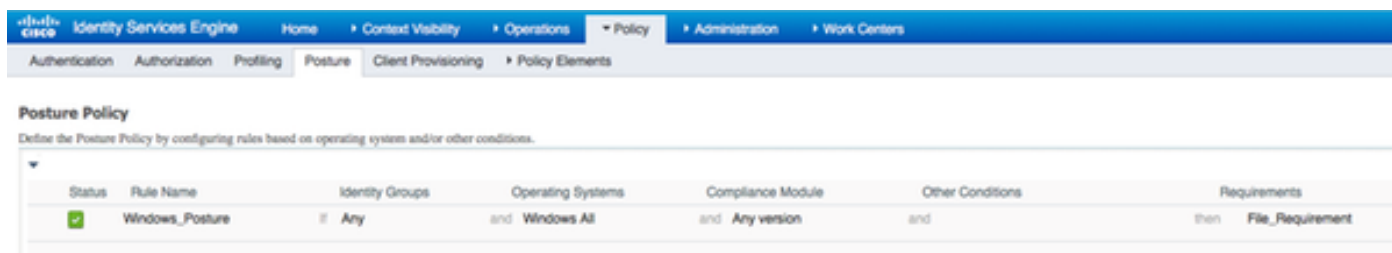
Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Requirements

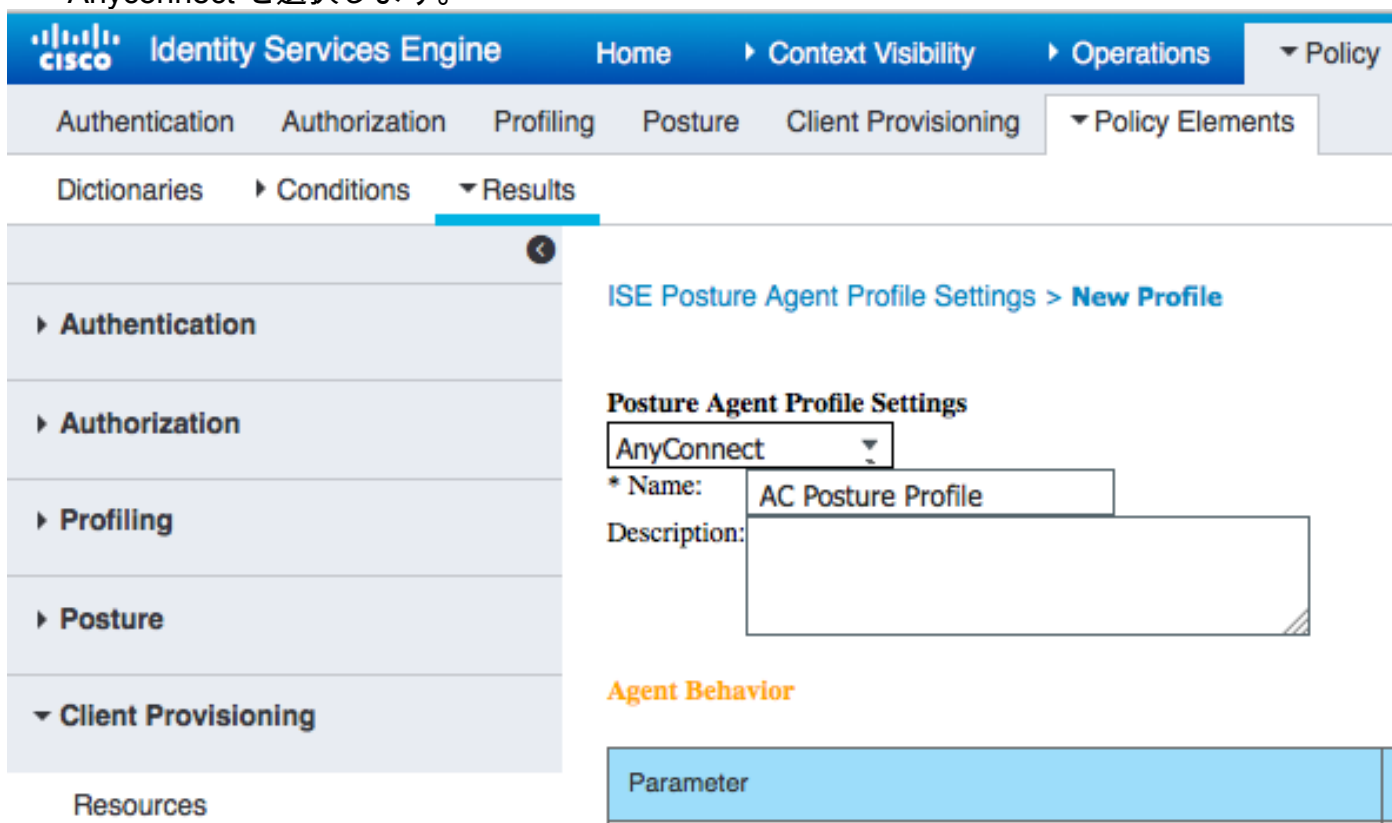
Name	Operating Systems	Compliance Module	Conditions	Remediation Actions
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	met if ANY_av_win_inst	then Message Text Only
File_Requirement	for Windows All	using Any version	met if File_Condition	then Message Text Only
Any_AV_Definition_Win	for 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

要件は、Microsoft Windows システムのポスチャ ポリシーで使用されます。



手順 2 : ポスチャ プロファイルの設定

- [Policy] > [Policy Elements] > [Results] > [Client Provisioning] > [Resources] に移動し、ネットワーク アドミッション コントロール (NAC) エージェントまたは AnyConnect エージェント ポスチャ プロファイルを追加します。
- Anyconnect を選択します。



- [Posture Protocol] セクションから * を追加し、エージェントがすべてのサーバに接続できるようにします。

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

手順 3 : AMP プロファイルの設定

AMP プロファイルには、Windows インストーラが配置された場所の情報が含まれます。

Windows インストーラ、AMP クラウドから前もってダウンロードされています。クライアントマシンからアクセスできるはずですが、インストーラが配置された場所にある HTTPS サーバの証明書も、クライアントマシンによって信頼されます。

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Elements > Results > AMP Enabler Profile Settings > New Profile. The page title is "AMP Enabler Profile".

On the left, there is a navigation menu with the following items: Authentication, Authorization, Profiling, Posture, Client Provisioning (selected), and Resources.

The main configuration area includes the following fields and options:

- * Name: AMP Profile
- Description: (empty field)
- Install AMP Enabler: (selected)
- Uninstall AMP Enabler:
- Windows Installer: [https://win2012ek.example.com/Downloads/Audit_FireAMPSetup.](https://win2012ek.example.com/Downloads/Audit_FireAMPSetup) [Check]
- MAC Installer: <https://> [Check]
- Windows Settings:
 - Add to Start Menu:
 - Add to Desktop:
 - Add to Context Menu:

At the bottom, there are "Submit" and "Cancel" buttons.

手順 2 : ISE にアプリケーションと XML プロファイルをアップロードする

- Cisco のオフィシャル サイトからアプリケーションを手動でダウンロードします。
anyconnect-win-4.2.02075-k9.pkg
- ISE で、[Policy] > [Policy Elements] > [Results] > [Client Provisioning] > [Resources] に移動し、[Agent Resources From Local Disk] を追加します。
- [Cisco Provided Packages] を選択し、anyconnect-win-4.2.02075-k9.pkg を選択します。

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

- [Policy] > [Policy Elements] > [Results] > [Client Provisioning] > [Resources] に移動し、[Agent Resources From Local Disk] を追加します。
- [Customer Created Packages] を選択し、AnyConnect Profile と入力します。
VPNDisable_ServiceProfile.xml を選択します。

注: VPNDisable_ServiceProfile.xml は、VPN のタイトルを非表示にするために使用されます (この例では VPN モジュールを使用しないため)。VPNDisable_ServiceProfile.xml の内容は次のとおりです。


```

<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">
  <ClientInitialization>
    <ServiceDisable>true</ServiceDisable>
  </ClientInitialization>
</AnyConnectProfile>

```

手順 3 : AnyConnect コンプライアンス モジュールをダウンロードする

- [Policy] > [Policy Elements] > [Results] > [Client Provisioning] > [Resources] に移動し、[Agent Resources from Cisco site] を追加します。
- [AnyConnect Windows Compliance Module 3.6.10591.2] を選択し、[Save] をクリックします

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

手順 4 : AnyConnect 設定の追加

- [Policy] > [Policy Elements] > [Results] > [Client Provisioning] > [Resources] に移動し、[AnyConnect Configuration] を追加します。
- 名前を設定し、コンプライアンス モジュールおよび AnyConnect のすべての必須モジュール (VPN、AMP、ポスチャ) を選択します。
- [Profile Selection] で、各モジュール用に先ほど設定したプロファイルを選択します。

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for 'AnyConnect Configuration AMP'. The breadcrumb navigation is 'AnyConnect Configuration > AnyConnect Configuration AMP'. The configuration includes:

- Select AnyConnect Package:** AnyConnectDesktopWindows 4.2.2075.0
- Configuration Name:** AnyConnect Configuration AMP
- Description:** (Empty text box)
- Description Value:** (Empty text box)
- 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: (Empty dropdown)
 - Web Security: (Empty dropdown)
 - AMP Enabler: AMP Profile
 - Network Visibility: (Empty dropdown)
 - Customer Feedback: (Empty dropdown)

手順 5 : クライアント プロビジョニング ルールの設定

先ほど作成した AnyConnect 設定は、クライアント プロビジョニング ルールで参照されます。

The screenshot shows the 'Client Provisioning Policy' configuration page in Cisco ISE. The page title is 'Client Provisioning Policy' and it includes instructions: '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

手順 6 : 許可ポリシーの設定

最初にクライアント プロビジョニング ポータルへのリダイレクトが行われます。ポスチャの標準認可ポリシーが使用されます。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys 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 =

その後、[Compliant]になると、フルアクセスが指定されます。

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

手順 7 : TC-NAC サービスの有効化

[Administration] > [Deployment] > [Edit Node] で、TC-NAC サービスを有効化します。 [Enable Threat Centric NAC Service] チェックボックスを選択します。

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** Make Primary

Monitoring Role **PRIMARY** Persons Other Monitoring Node

Policy Service

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

Enable Profiling Service

Enable Threat Centric NAC Service i

手順 8 : AMP アダプタの設定

[Administration] > [Threat Centric NAC] > [Third Party Vendors] > [Add] の順に移動します。
[Save] をクリックします。

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

Vendor * AMP : THREAT

Instance Name * AMP_THREAT

Cancel Save

[Ready to Configure] 状態に移行するはずですが、[Ready to Configure] をクリックします。

Vendor Instances
0 Selected

Refresh Add Trash Edit Filter Settings

<input type="checkbox"/>	Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
<input type="checkbox"/>	QualysVA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active
<input type="checkbox"/>	AMP_THREAT	AMP	THREAT		Disconnected	Ready to configure

[Cloud] を選択し、[Next] をクリックします。

Vendor Instances > AMP

Cloud
US Cloud

Which public cloud would you like to connect to

Cancel Next

FireAMP のリンクをクリックして、admin ユーザとして FireAMP にログインします。

Third Party Vendors

Vendor Instances > AMP

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/vrfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize&scope=recv_events

Cancel

[Applications] パネルで [Allow] をクリックし、Streaming Event Export 要求を認可します。このアクションが終わると、Cisco ISE へリダイレクトされます。

AMP for Endpoints 3 Installs 1 detection (7 days) Announcements Support Help My Account Log Out

Dashboard Analysis Outbreak Control Reports Management Accounts Search

Applications

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

- Streaming event export.

Allow Deny

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 - ekomeyc
- Domain Controller: Domain Controller Group for Cisco - ekomeyc
- Protect: Protect Group for Cisco - ekomeyc
- Server: Server Group for Cisco - ekomeyc
- Triage

Allow Deny

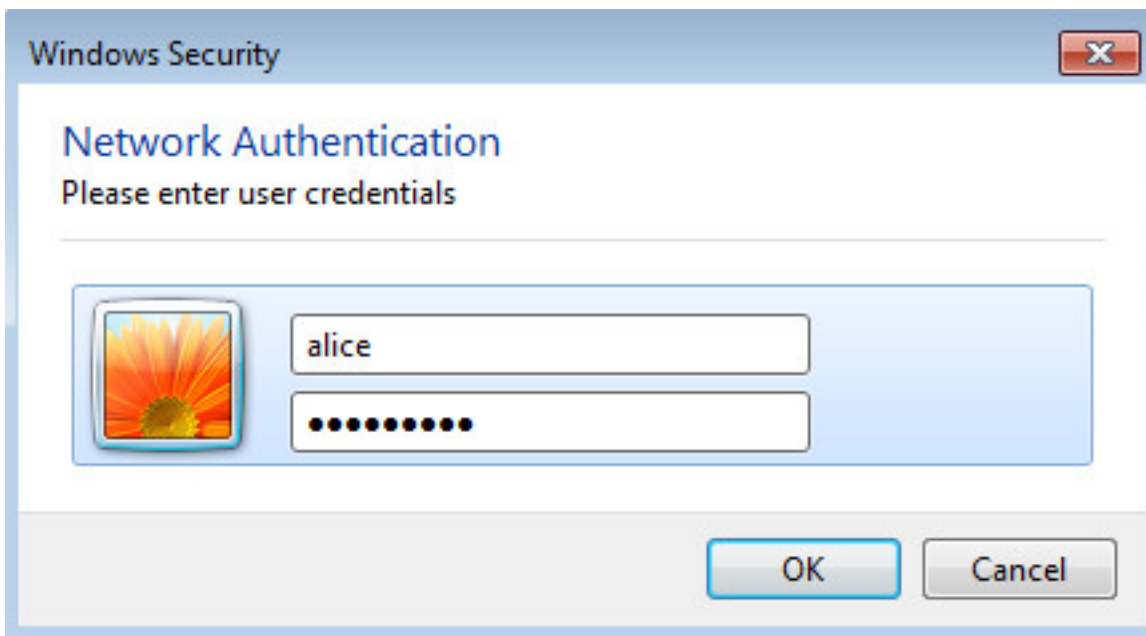
モニタするイベント (疑わしいダウンロード、疑わしいドメインへの接続、実行されたマルウェア、Java のセキュリティ侵害など) を選択します。アダプタ インスタンス設定の概要が、設定概要ページに表示されます。アダプタ インスタンスが [Connected/Active] 状態に移行します。

Cisco 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
<input type="checkbox"/>	Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
<input type="checkbox"/>	AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
<input type="checkbox"/>	QUALYS_VA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active

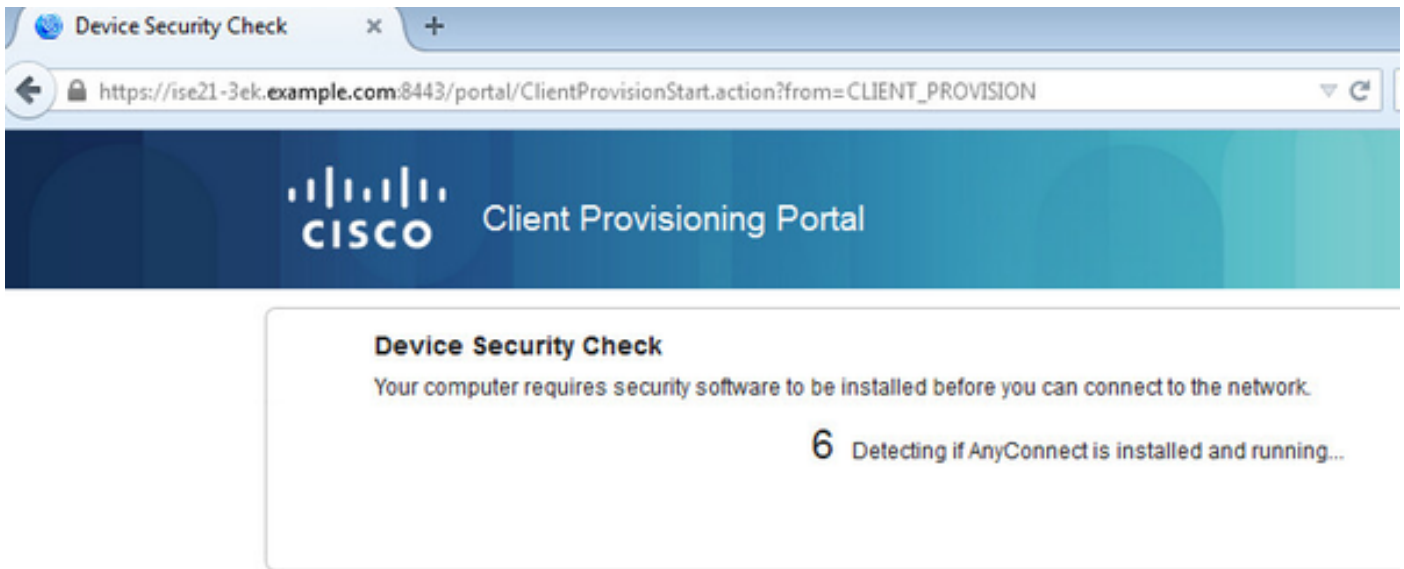
確認

Endpoint

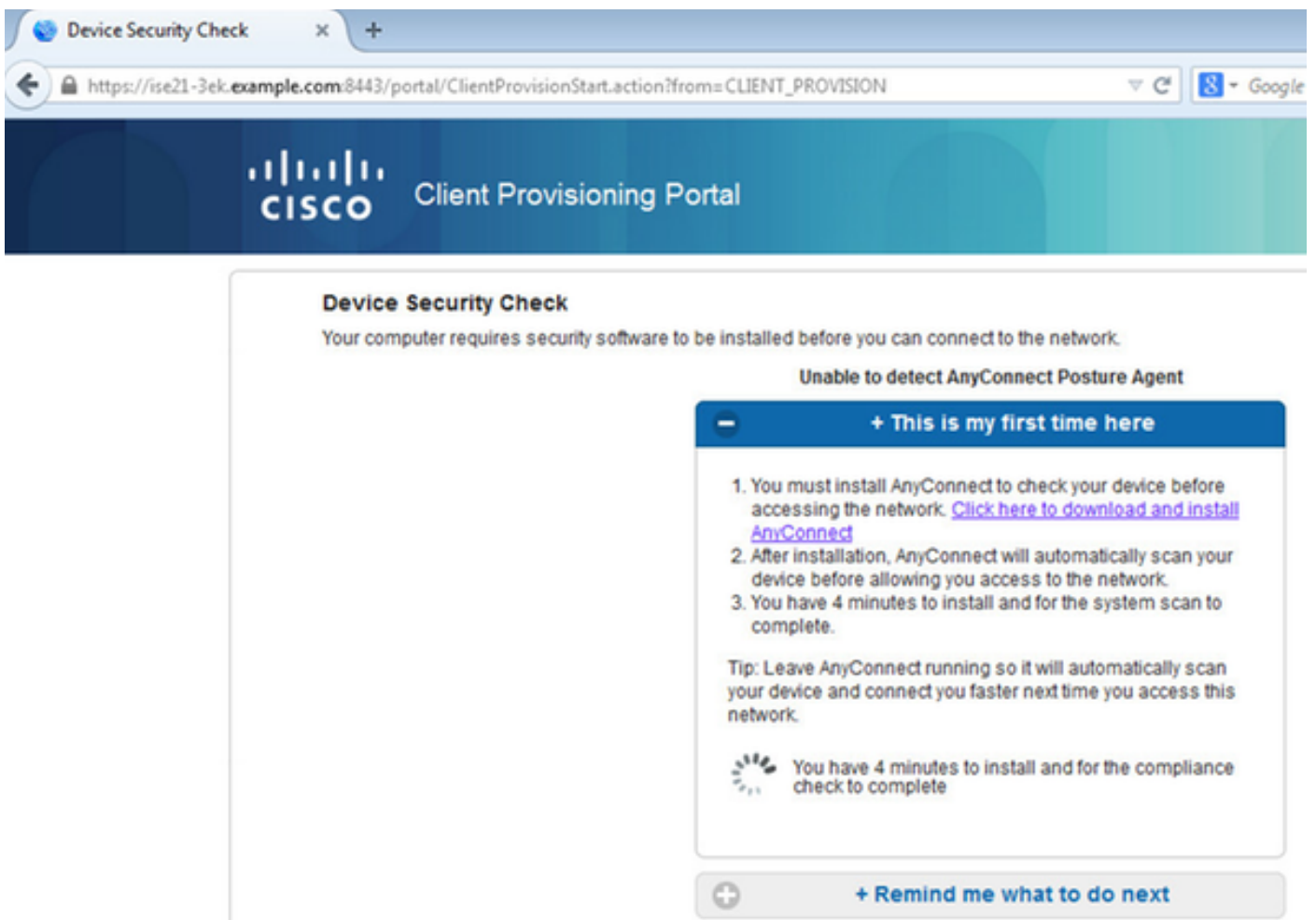
PEAP (MSCHAPv2) 経由でワイヤレス ネットワークに接続します。



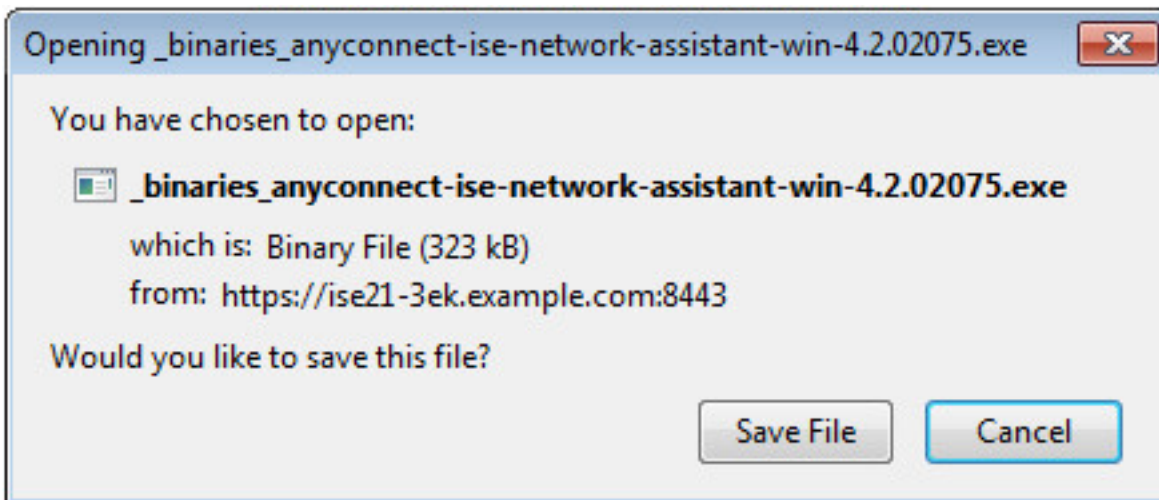
接続されると、クライアント プロビジョニング ポータルへのリダイレクトが行われます。



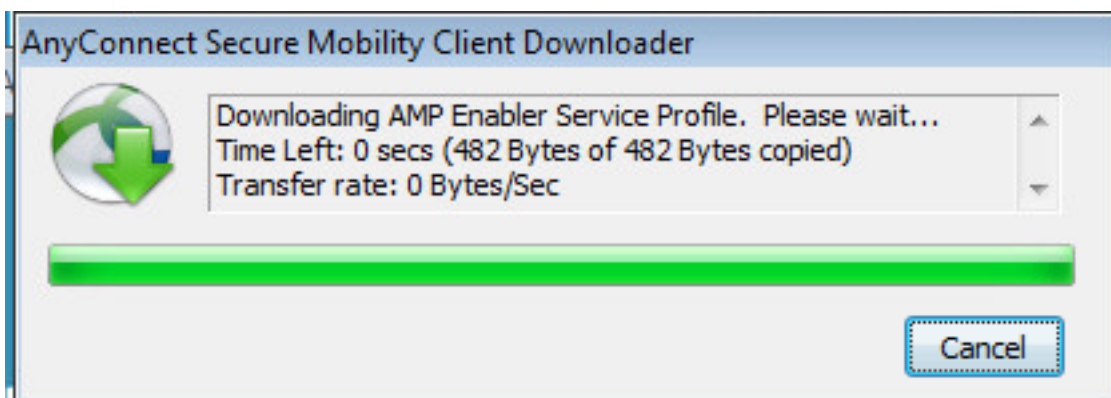
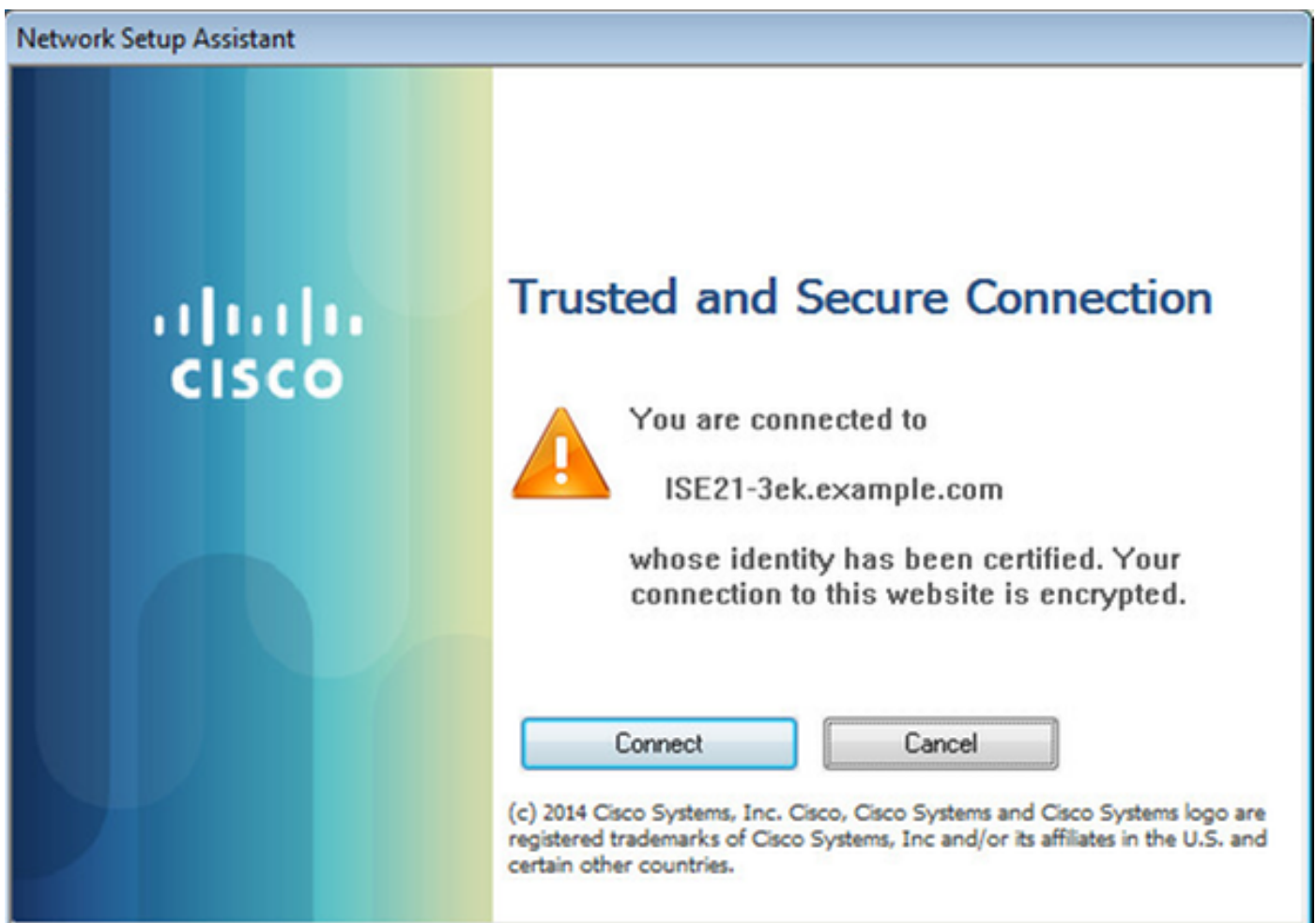
クライアント マシンに何もインストールされてないため、ISE が AnyConnect クライアントのインストールを求めます。

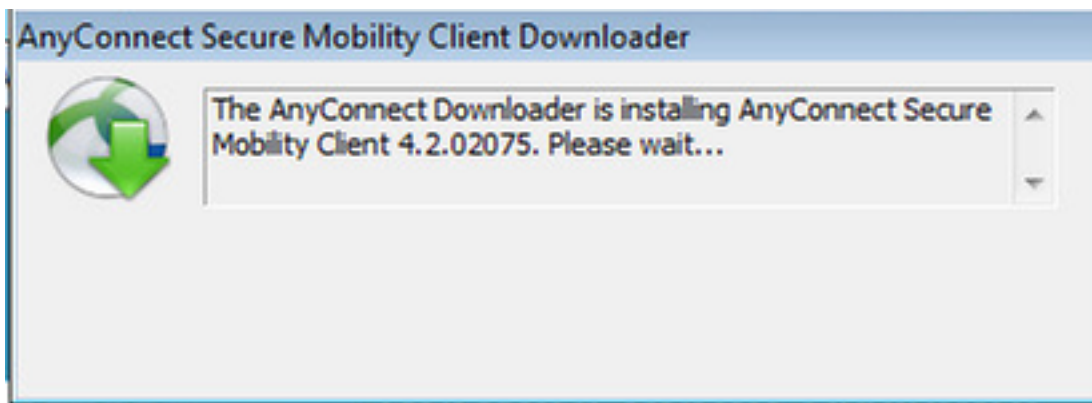


ネットワーク設定アシスタント (NSA) アプリケーションをダウンロードし、クライアント マシンから実行してください。

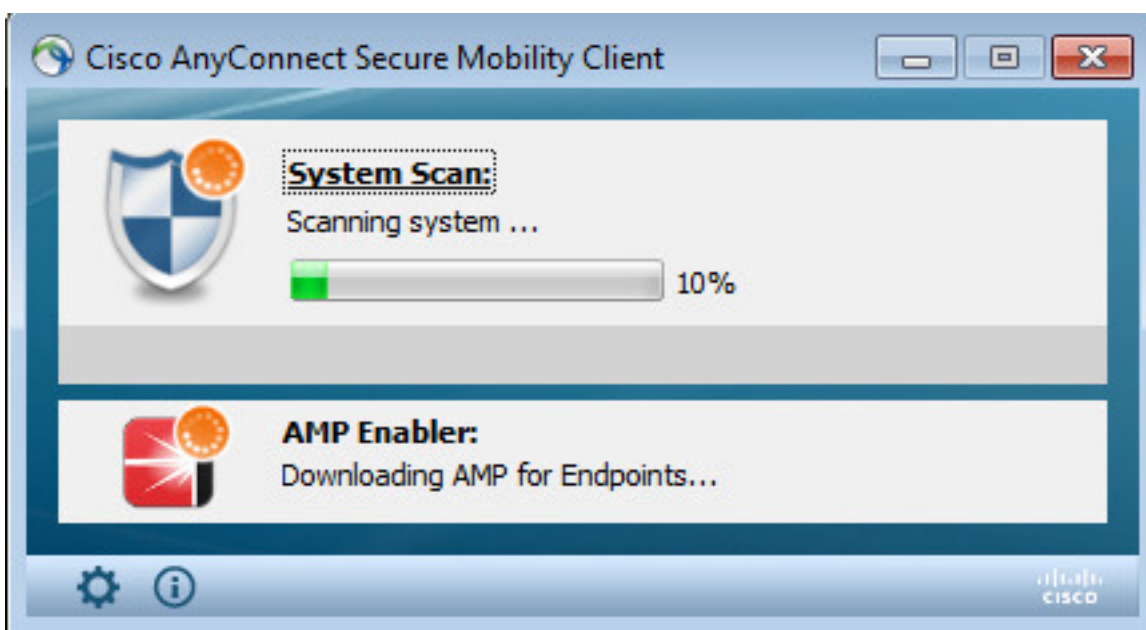
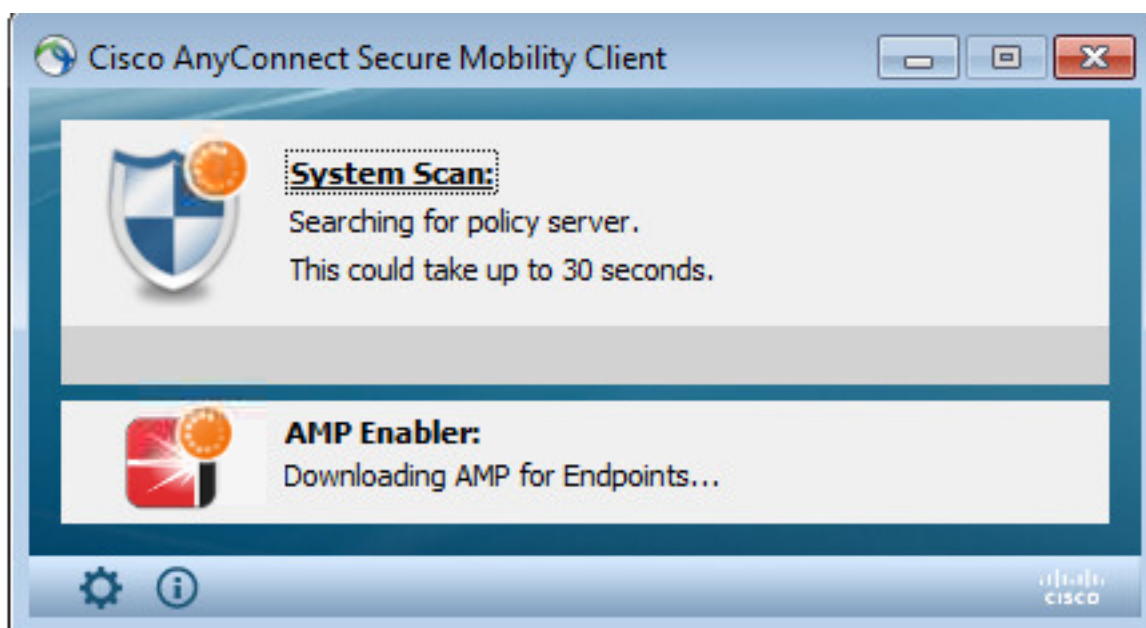


NSA が必要なコンポーネントとプロファイルのインストールを処理します。

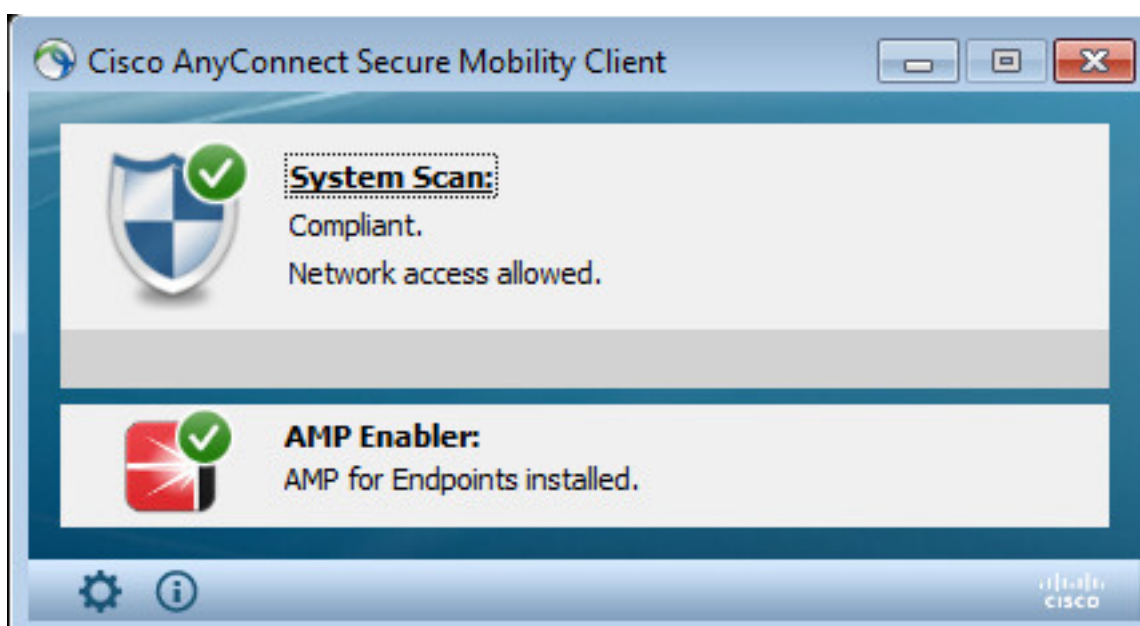
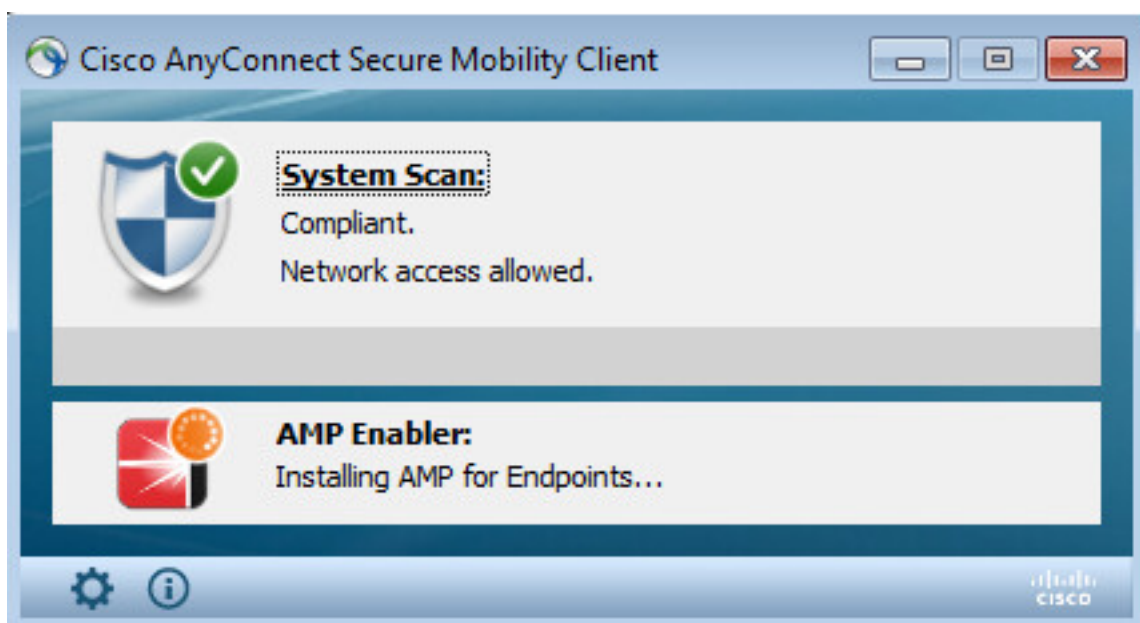
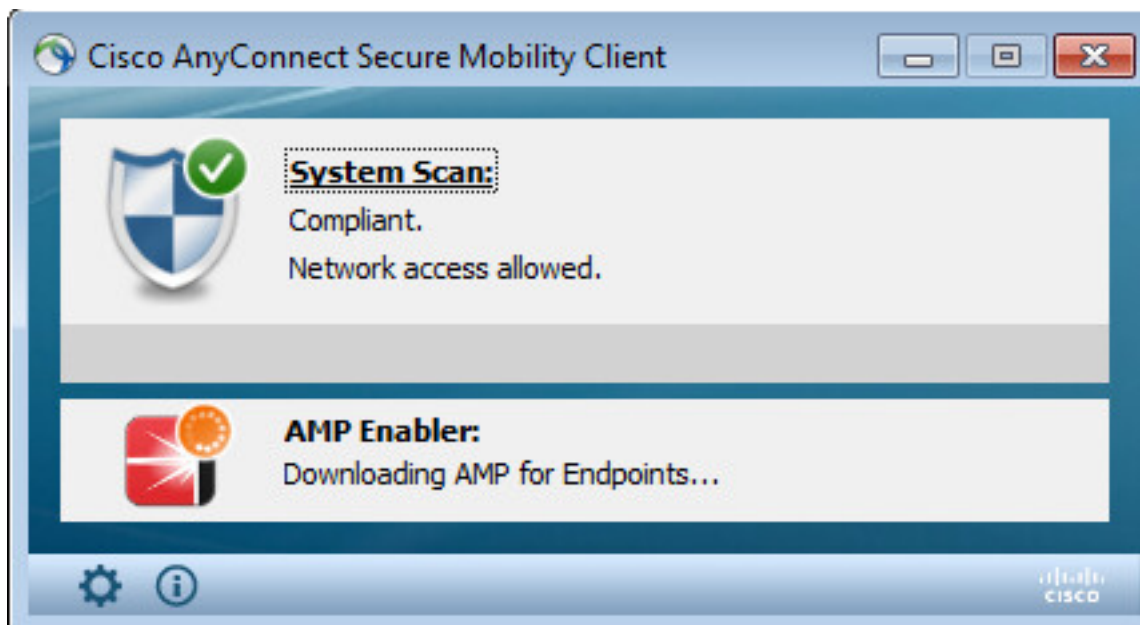




インストールが完了すると、AnyConnect ポスチャ モジュールがコンプライアンスチェックを行います。



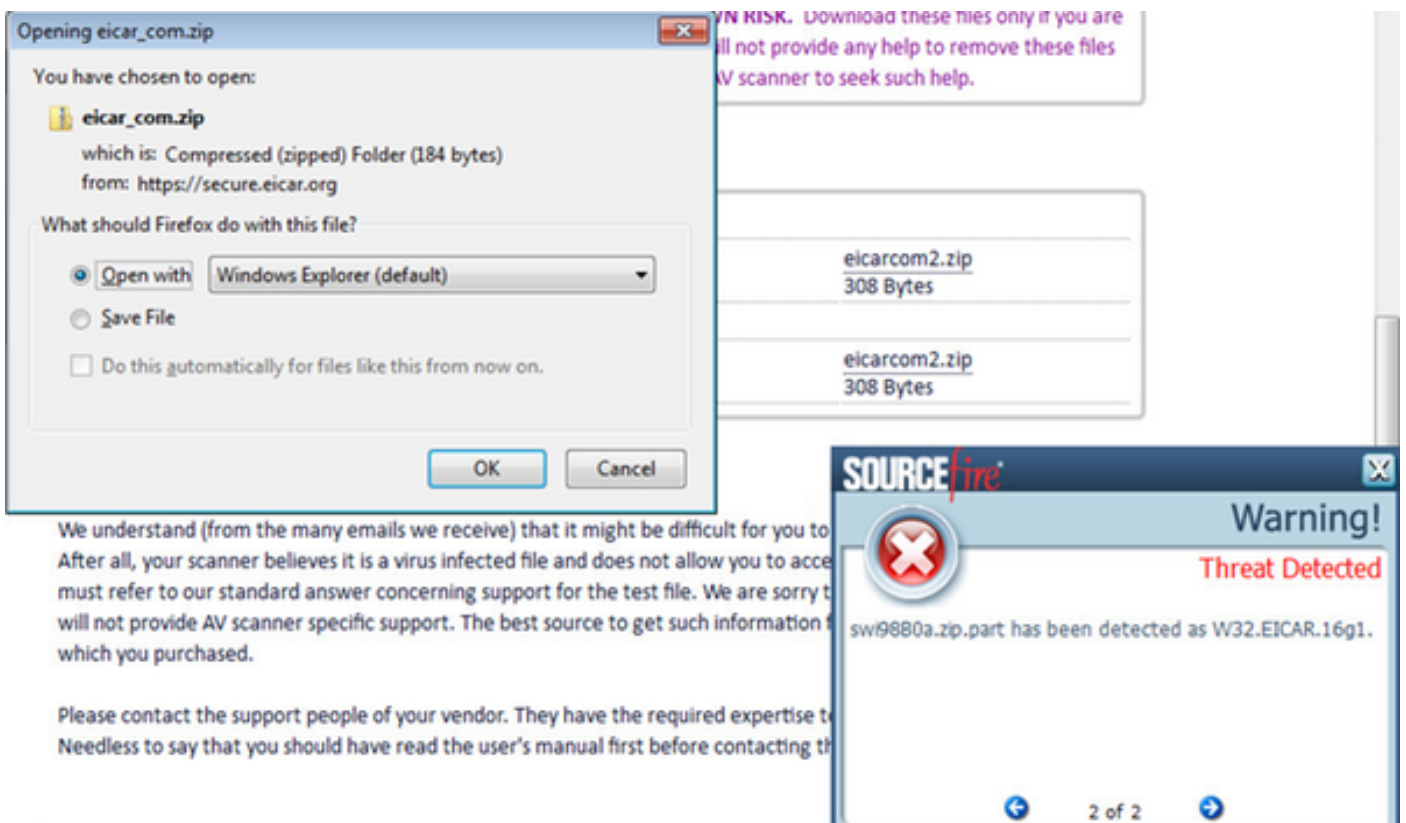
フルアクセスが与えられているため、エンドポイントが適合している場合、AMP プロファイルで先ほど指定した Web サーバから AMP がダウンロードされ、インストールされます。



AMP コネクタが表示されます。



動作中の AMP をテストするため、ZIP ファイルに格納されている Eicar 文字列がダウンロードされます。脅威が検出され、AMP クラウドに報告されます。



AMP クラウド

脅威の詳細を確認するには、AMP クラウドのダッシュボードを使用できます。

The screenshot shows the Cisco AMP for Endpoints dashboard. At the top, there are navigation links for Dashboard, Analysis, Outbreak Control, Reports, Management, and Accounts. The dashboard is divided into several sections:

- Indications of Compromise:** Shows a threat detected on ekorneyc-PC.example.com.
- Hosts Detecting Malware (7 days):** A table showing the number of malware detections for different hosts.

Computer	Count
ekorneyc-PC.example.com	4
HARISHA-PC.example.com	1
- Malware Threats (7 days):** A table showing the number of malware threats detected.

Detection Name	Count
W32.EICAR.16g1	5
- Hosts Detecting Network Threats (7 days):** Shows no recent network threat detections.
- Network Threats (7 days):** Shows no recent network threat detections.

脅威、ファイルパスおよびフィンガープリントについての詳細を得るには、マルウェアが検出されたホストをクリックします。

The screenshot shows a detailed view of a malware detection event. The event type is 'Threat Detected' and the host is 'ekorneyc-PC.example.com'. The detection is for the malware 'W32.EICAR.16g1'. The event details are as follows:

File Detection	Detection	W32.EICAR.16g1
Connector Info	Fingerprint (SHA-256)	2546dcf...6e9eedad
Comments	Filename	0M90PRx0.zip.part
	Filepath	C:\Users\admin\AppData\Local\Temp\0M90PRx0.zip.part
	File Size (bytes)	184
	Parent Fingerprint (SHA-256)	3147bd8...32d689c2
	Parent Filename	Firefox.exe

ISE のインスタンスを表示 (View) または登録解除 (Deregister) するには、[Accounts] > [Applications] に移動します。

Applications

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.

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

ISE

ISE 自体で定期的なポスチャ フローが見られ、ネットワークのコンプライアンスを確認するため、最初にリダイレクトが行われます。エンドポイントが適合するとすぐに、CoA 再認証が送信され、PermitAccess を持つ新しいプロファイルが割り当てられます。

Summary Metrics:

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

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	●			alice	02-4A:00:14:8D:4B	Windows7...	Default >> Dot1X >> Default	Default >> Non_Compliant_Devis...	AMP_Profile	
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	

検出された脅威を表示するには、[Context Visibility] > [Endpoints] > [Compromised Endpoints] に移動します。

COMPROMISED ENDPOINTS BY INCIDENTS

COMPROMISED ENDPOINTS BY INDICATORS

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

エンドポイントを選択し、[Threats] タブに移動すると、より多くの詳細が表示されます。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below this, there are tabs for 'Endpoints' and 'Network Devices'. The main content area shows the endpoint details for MAC address C0:4A:00:14:8D:4B, including Username: alice, Endpoint Profile: Windows7-Workstation, and Current IP Address: 10.62.148.26. The 'Threats' tab is selected, displaying a 'Threat Detected' section with the following details: Type: INCIDENT, Severity: Painful, Reported by: AMP, and Reported at: 2016-06-30 11:27:48.

エンドポイントで脅威イベントが検出されると、[Compromised Endpoints] ページでエンドポイントの MAC アドレスを選択し、ANC ポリシーを適用することができます (設定されている場合、隔離 (Quarantine) など)。または、認可変更 (Change of Authorization) を発行してセッションを終了することができます。

The screenshot shows the Cisco Identity Services Engine (ISE) interface for 'Compromised Endpoints'. The top navigation bar is the same as in the previous screenshot. Below it, there are tabs for 'Authentication', 'BYOD', 'Compliance', 'Compromised Endpoints', 'Endpoint Classification', 'Guest', and 'Vulnerable Endpoints'. The 'Compromised Endpoints' tab is selected, displaying two charts: 'COMPROMISED ENDPOINTS BY INCIDENTS' and 'COMPROMISED ENDPOINTS BY INDICATORS'. The 'By Incidents' chart shows a bar for 'Painful' with an impact level of 1. The 'By Indicators' chart shows a bar for 'Low' with a likely impact level of 1. Below the charts, there is a table with columns for 'Source', 'Threat Severity', 'Logical NAD Location', 'Connectivity', 'Hostname', 'Identity Group', and 'Endpoint OS'. The table contains one row with the following data: Source: AMP, Threat Severity: Painful, Logical NAD Location: Location#A1 Locations, Connectivity: Connected, Hostname: Workstation, Identity Group: Workstation, Endpoint OS: Workstation. A dropdown menu is open over the table, showing options: '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'.

[CoA Session Terminate] を選択すると、ISE は CoA Disconnect を送信し、クライアントはネットワークへのアクセスを失います。

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

トラブルシューティング

ISE でデバッグを有効にするには、[Administration] > [System] > [Logging] > [Debug Log Configuration] に移動し、[TC-NAC Node] を選択して TC-NAC コンポーネントの [Log Level] を [DEBUG] に変更します。

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Administration > System > Logging > Debug Log Configuration. The page title is "Node List > ISE21-3ek.example.com Debug Level Configuration". There are two buttons: "Edit" and "Reset to Default". Below the buttons is a table with columns for Component Name, Log Level, and Description. The table has one row for "TC-NAC" with "DEBUG" selected in the Log Level column and "TC-NAC log messages" in the Description column. There is also a radio button next to "TC-NAC".

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

チェックするログ : irf.log。ISE CLI から直接次の tail コマンドを発行します。

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

AMP クラウドから脅威イベントが届きます。

```
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][  
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 -:::: -- calling notification  
handler com.cisco.cpm.irf.service.IrfNotificationHandler$MyNotificationHandler@3fac8043  
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":  
[{"incident": {"Impact_Qualification": "Painful"}, "time-stamp": 1467304068599, "vendor":  
"AMP", "title": "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, 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 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][  
cisco.cpm.irf.service.IrfNotificationHandler:handle:140 -:::: -- Added to the pending queue:  
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":  
[{"incident": {"Impact_Qualification": "Painful"}, "time-stamp": 1467304068599, "vendor":  
"AMP", "title": "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, 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 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][  
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:59 -:::: -- DONE processing  
notification: 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-a836-545416ae56f4, cluster-id=null)  
2016-06-30 18:27:48,706 DEBUG [IRF-EventProcessor-0][  
cisco.cpm.irf.service.IrfEventProcessor:parseNotification:221 -:::: -- parsing notification:  
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":  
[{"incident": {"Impact_Qualification": "Painful"}, "time-stamp": 1467304068599, "vendor":  
"AMP", "title": "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, 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)}
```

脅威が PAN に送信されたことに関する情報

```
2016-06-30 18:27:48,724 DEBUG [IRF-EventProcessor-0][  
cisco.cpm.irf.service.IrfEventProcessor:storeEventsInES:366 -:::: -- Adding threat event info  
to send to PAN - c0:4a:00:14:8d:4b {incident={Impact_Qualification=Painful}, time-  
stamp=1467304068599, vendor=AMP, title=Threat Detected}
```