

ISE 2.1 Threat-Centric NAC (TC-NAC) configureren met AMP- en posteringsservices

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Gedetailleerde Flow](#)

[AMP-cloud configureren](#)

[Stap 1. Download connector van AMP Cloud](#)

[ISE configureren](#)

[Stap 1. Het beleid en de voorwaarden voor de posteringen configureren](#)

[Stap 2. Postprofiel configureren](#)

[Stap 3. AMP-profiel configureren](#)

[Stap 2. Uploadtoepassingen en XML-profiel naar ISE](#)

[Stap 3. Download AnyConnect-nalevingsmodule](#)

[Stap 4. Voeg AnyConnect-configuratie toe](#)

[Stap 5. Instellen van regels voor clientprovisioning](#)

[Stap 6. Instellen van het vergunningsbeleid](#)

[Stap 7. Schakel TC-NAC-services in](#)

[Stap 8. AMP-adapter configureren](#)

[Verifiëren](#)

[Endpoint](#)

[AMP-cloud](#)

[ISE](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u Threat-Centric NAC kunt configureren met Advanced Malware Protection (AMP) op Identity Services Engine (ISE) 2.1. Er kunnen gegevens over de ernst van de vervuiling en de kwetsbaarheidsassessments worden gebruikt om het toegangsniveau van een eindpunt of een gebruiker dynamisch te controleren. Postdiensten vallen ook onder dit document.

Opmerking: Het doel van het document is ISE 2.1 Integratie met AMP te beschrijven. Postdiensten worden getoond zoals ze nodig zijn wanneer we AMP van ISE leveren.

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- Cisco Identity Services Engine
- Advanced Malware Protection

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine versie 2.1
- Draadloze LAN-controller (WLC) 8.0.121.0
- AnyConnect VPN-client 4.2.2075
- Windows 7 Service Pack 1

Configureren

Netwerkdigram



Gedetailleerde Flow

1. Clientverbindingen met het netwerk, de **AMP_Profile** worden toegewezen en de gebruiker wordt terugverwezen naar Any-Connect Provisioning Portal. Als AnyConnect niet op de machine wordt gedetecteerd, worden alle geconfigureerde modules (VPN, AMP, Posture) geïnstalleerd. De configuratie wordt voor elke module samen met dat profiel ingedrukt
2. Zodra AnyConnect is geïnstalleerd, wordt de beoordeling van de positie uitgevoerd

3. AMP Enabler-module installeert een FireAMP-connector

4. Wanneer een cliënt probeert kwaadaardige software te downloaden, stuurt de AMP-connector een waarschuwingsbericht en meldt het aan de AMP Cloud

5. AMP Cloud stuurt deze informatie naar ISE

AMP-cloud configureren

Stap 1. Download connector van AMP Cloud

Ga naar Management > Download connector om de connector te downloaden. Selecteer vervolgens type en **Download** FirePOWER (Windows, Android, Mac, Linux). In dit geval is **Audit** geselecteerd en het installatiebestand van FireAMP voor Windows.

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

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

Opmerking: Het downloaden van dit bestand genereert een .exe-bestand dat **Audit_FireAMPSetup.exe** heet in het voorbeeld. Dit bestand is naar de webserver gestuurd zodat het beschikbaar is zodra de gebruiker om de configuratie van de Advanced Malware Protection vraagt.

ISE configureren

Stap 1. Het beleid en de voorwaarden voor de posturien configureren

Navigeren in op Policy > Policy Elementen > Voorwaarden > Posture > File Condition. U kunt zien dat er een eenvoudige voorwaarde voor het bestaan van bestanden is gemaakt. Bestand moet bestaan indien het eindpunt in overeenstemming is met het door de Postmodule geverifieerde beleid:

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

Deze voorwaarde wordt gebruikt voor een vereiste:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

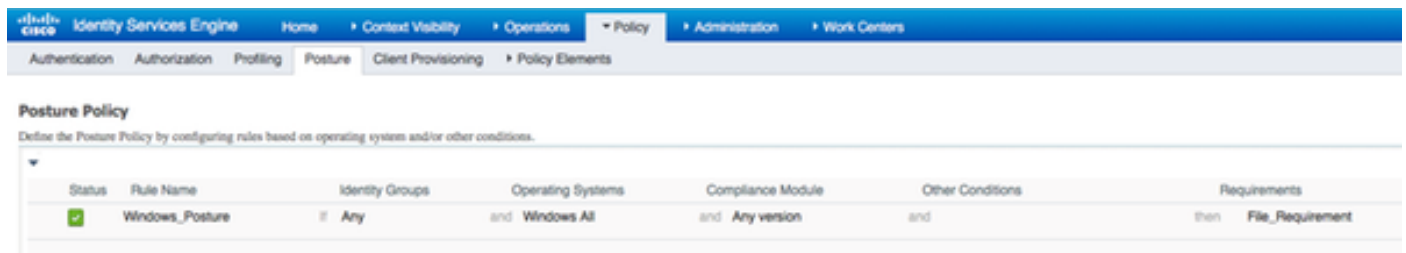
Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Requirements

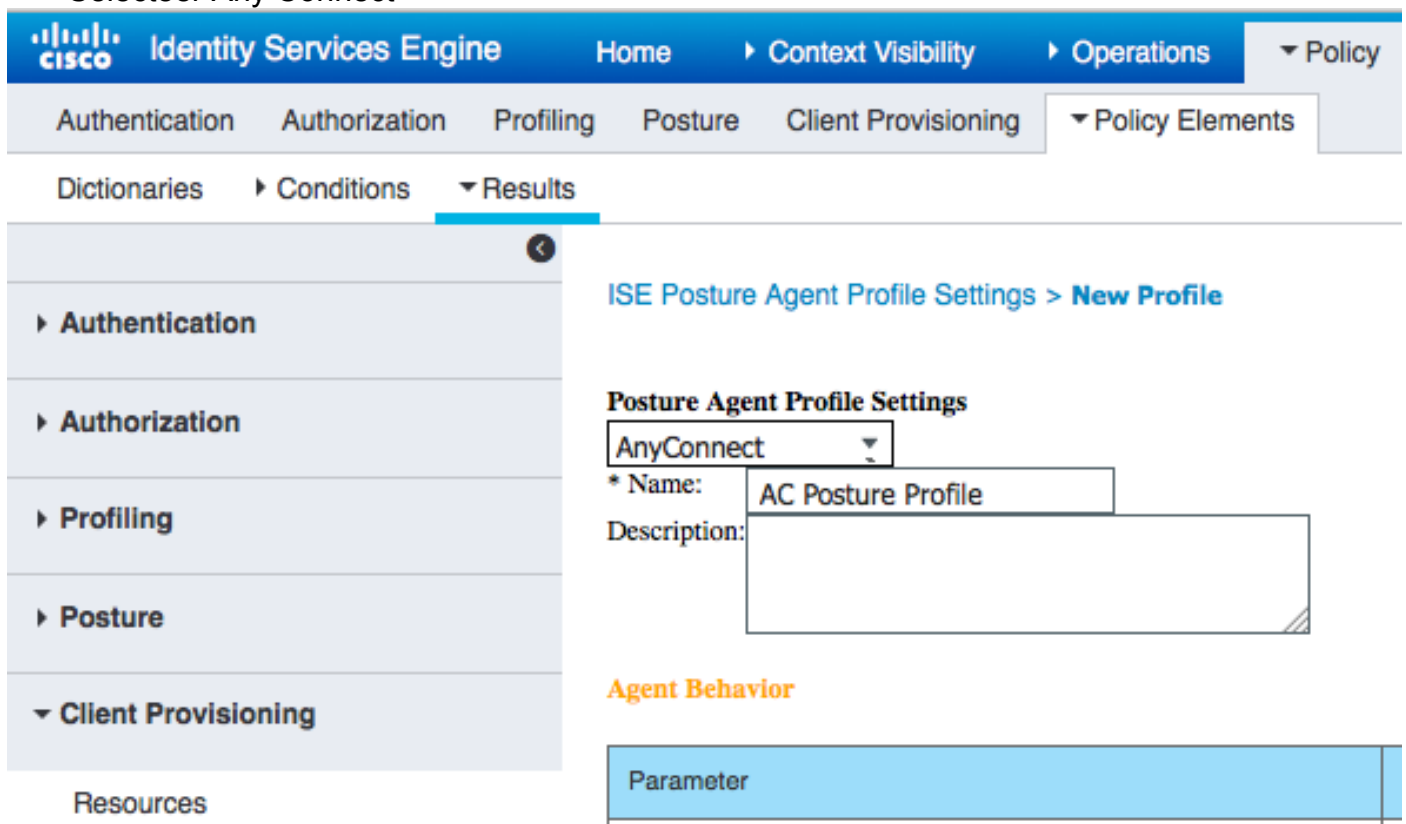
Name	Operating Systems	Compliance Module	Conditions	Remediation Actions
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	met if ANY_av_win_inst	then Message Text Only
File_Requirement	for Windows All	using Any version	met if File_Condition	then Message Text Only
Any_AV_Definition_Win	for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

Dit vereiste wordt gebruikt in het Posture-beleid voor Microsoft Windows-systemen:



Stap 2. Postprofiel configureren

- Navigeren in naar beleid > Beleidselementen > Resultaten > Clientprovisioning > Resources en netwerktoegangscontrole (NAC) Agent of AnyConnect Agent Posture Profile
- Selecteer Any Connect



- Toevoegen van het gedeelte Posture Protocol * om de Agent in staat te stellen verbinding te maken met alle servers

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

Stap 3. AMP-profiel configureren

AMP Profile bevat informatie waar het Windows-installatieprogramma zich bevindt. Windows Installer is eerder gedownload van de Advanced Malware Protection Cloud. Het moet toegankelijk zijn vanaf de klant. Certificaat van de HTTPS Server, waar Installer zich bevindt, zou ook door

client machine moeten worden vertrouwd.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main navigation bar includes: Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. Under Policy Elements, there are sub-menus for Dictionaries, Conditions, and Results. The left sidebar shows a tree view with Authentication, Authorization, Profiling, Posture, and Client Provisioning (selected). Under Client Provisioning, there is a Resources section. The main content area is titled 'AMP Enabler Profile Settings > New Profile' and 'AMP Enabler Profile'. It contains the following fields and options:

- * Name: AMP Profile
- Description: (empty field)
- 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:
- Buttons: Submit, Cancel

Stap 2. Uploadtoepassingen en XML-profiel naar ISE

- Download de toepassing handmatig van de officiële website van Cisco: **anyconnect-win-4.2.02075-k9.pkg**
- Op ISE, navigeer naar Beleidselementen > Resultaten > Clientprovisioning > Resources en voeg **Agent resources toe van lokale schijf**
- Kies **Cisco meegeleverde pakketten** en selecteer **elke connect-win-4.2.02075-k9.pkg**

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

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 4.2.2075...	AnyConnectDesktopWindows	4.2.2075.0	AnyConnect Secure Mobility Clie...

Submit Cancel

- Navigeren in op beleid > Beleidselementen > Resultaten > Clientprovisioning > Resources en Agent-bronnen van lokale schijf toevoegen
- Kies door de klant gemaakte pakketten en type AnyConnect Profile. Selecteer VPNisable_ServiceProfile.xml

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

Category: Customer Created Packages

Type: AnyConnect Profile

* Name: VPNDisable_ServiceProfile

Description:

Browse... VPNDisable_ServiceProfile.xml

Submit Cancel

Opmerking: **VPNDisable_ServiceProfile.xml** wordt gebruikt om de titel van VPN te verbergen, aangezien dit voorbeeld geen VPN-module gebruikt. Dit is de inhoud van **VPNisable_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">
  <Client-initialisatie>
  <ServiceOff>ware</ServiceOff>
  Initialisatie </client>
</AnyConnect-profiel>

```

Stap 3. Download AnyConnect-nalevingsmodule

- Navigeren in naar beleid > Beleidselementen > Resultaten > Clientprovisioning > Resources en **Agent Resources van Cisco-site toevoegen**
- Selecteer **AnyConnect Windows-8-nalevingsmodule 3.6.10591.2** en klik op Opslaan

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

Stap 4. Voeg AnyConnect-configuratie toe

- Navigatie in naar beleid > Beleidselementen > Resultaten > Clientprovisioning > Resources en add **AnyConnect-configuratie**
- Configuratie van de naam en selecteer de nalevingsmodule en alle vereiste modules van AnyConnect (VPN, AMP en Posture)
- Kies in **de selectie van het profiel** het profiel dat eerder voor elke module is geconfigureerd

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Profiling

Posture

Client Provisioning

Resources

AnyConnect Configuration > AnyConnect Configuration AMP

* Select AnyConnect Package: AnyConnectDesktopWindows 4.2.2075.0

* Configuration Name: AnyConnect Configuration AMP

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 3.6.10591.2

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AC Posture Profile

VPN: VPNDisable_ServiceProfile

Network Access Manager

Web Security

AMP Enabler: AMP Profile

Network Visibility

Customer Feedback

Stap 5. Instellen van regels voor clientprovisioning

De AnyConnect-configuratie die eerder is gemaakt, wordt vermeld in de regels voor de clientprovisioning

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Client Provisioning Policy

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

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> Windows_Posture_AMP	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration AMP

Stap 6. Instellen van het vergunningsbeleid

Eerst wordt de omleiding naar Client Provisioning Portal uitgevoerd. Er wordt gebruikgemaakt van standaard autorisatiebeleid voor de houding.

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 =

Daarna wordt volledige toegang toegewezen zodra dit voldoet

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

Stap 7. Schakel TC-NAC-services in

Schakel TC-NAC-services in onder Beheer > Implementatie > Knooppunt bewerken. Controleer het selectieteken voor bedreigingscentrifuge NAC-service inschakelen.

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

Stap 8. AMP-adapter configureren

Navigatie in naar Administratie > Bedreigingscentrifuge NAC > Verkopers van derden > Toevoegen. Klik op **Opslaan**

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

Third Party Vendors

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

Vendor * AMP : THREAT

Instance Name * AMP_THREAT

Cancel Save

Het zou moeten overschakelen naar **Klaar om staat te configureren**. Klik op **Klaar om te configureren**

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

Third Party Vendors

Vendor Instances

0 Selected

Refresh Add Trash Edit Filter Settings

<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

Selecteer **Cloud** en klik op **Volgende**

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

Third Party Vendors

Vendor Instances > AMP

Cloud

US Cloud

Which public cloud would you like to connect to

Cancel Next

Klik op de koppeling FirePOWER en loggen in als beheerder van FireAMP.

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

Klik op **Sta** in het paneel **Toepassingen** toe om het verzoek van de Uitvoer van de Streaminggebeurtenis goed te keuren. Na die actie wordt u terugverwezen naar Cisco ISE

The screenshot shows the Cisco AMP for Endpoints dashboard. At the top, it displays '3 Installs' and '1 detection (7 days)'. The main navigation bar includes 'Dashboard', 'Analysis', 'Outbreak Control', 'Reports', 'Management', and 'Accounts'. A search bar is also present.

The 'Applications' section is active, showing a request from 'The AMP Adaptor 62f6204b-751f-4ef5-9d93-e9f02500d842 (IRF) Defense Center'. The request is for 'Streaming event export' and includes a URL: <https://ise21-3ek.example.com/admin/vrfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize>. There are 'Allow' and 'Deny' buttons for this request.

Below this, there is a section for 'Event Export Groups' with the text 'All groups selected.' and a note: 'If you are going to authorize the request, please select which groups will have their events exported to this application:'. There is a large empty box for selecting groups and 'Allow'/'Deny' buttons.

On the right side, there is a 'Search Groups' dropdown menu with the following options:

- 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**

Selecteer de gebeurtenissen (bijvoorbeeld verdachte download, verbinding met verdachte domein, uitgevoerde malware, java-compromis) die u wilt controleren. De samenvatting van de configuratie van de adapterinstantie wordt weergegeven in de summiere pagina van de configuratie. Adapterinstantie overschakelt naar Connected/Active State.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

Third Party Vendors

Vendor Instances

0 Selected

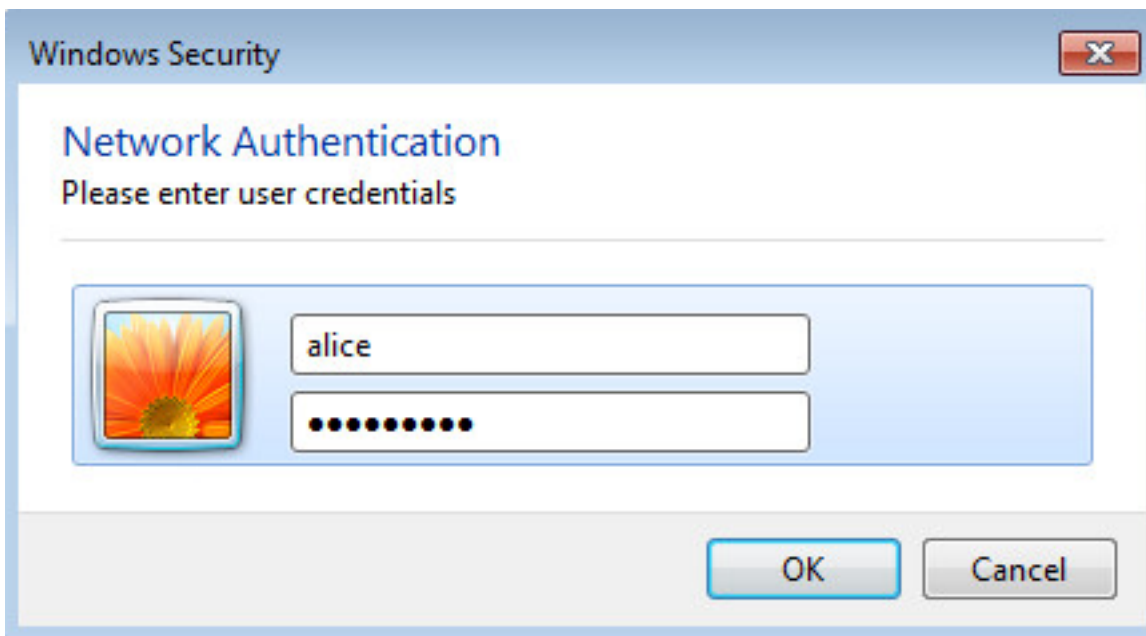
Refresh Add Trash Edit Filter Settings

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

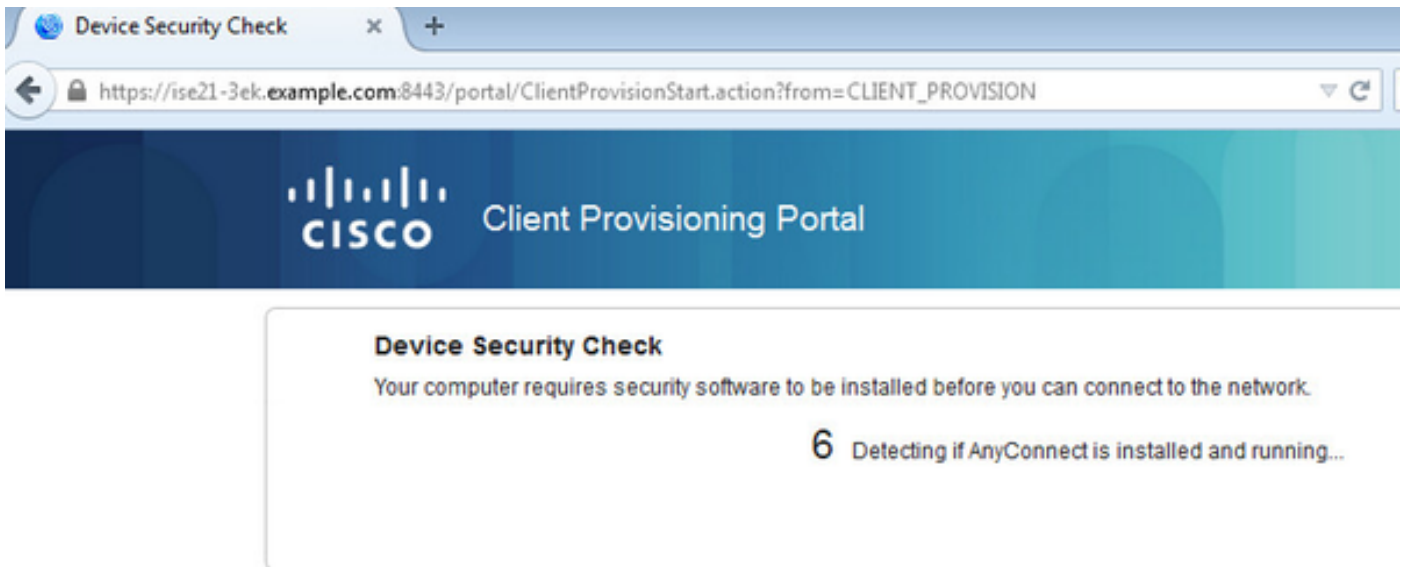
Verifiëren

Endpoint

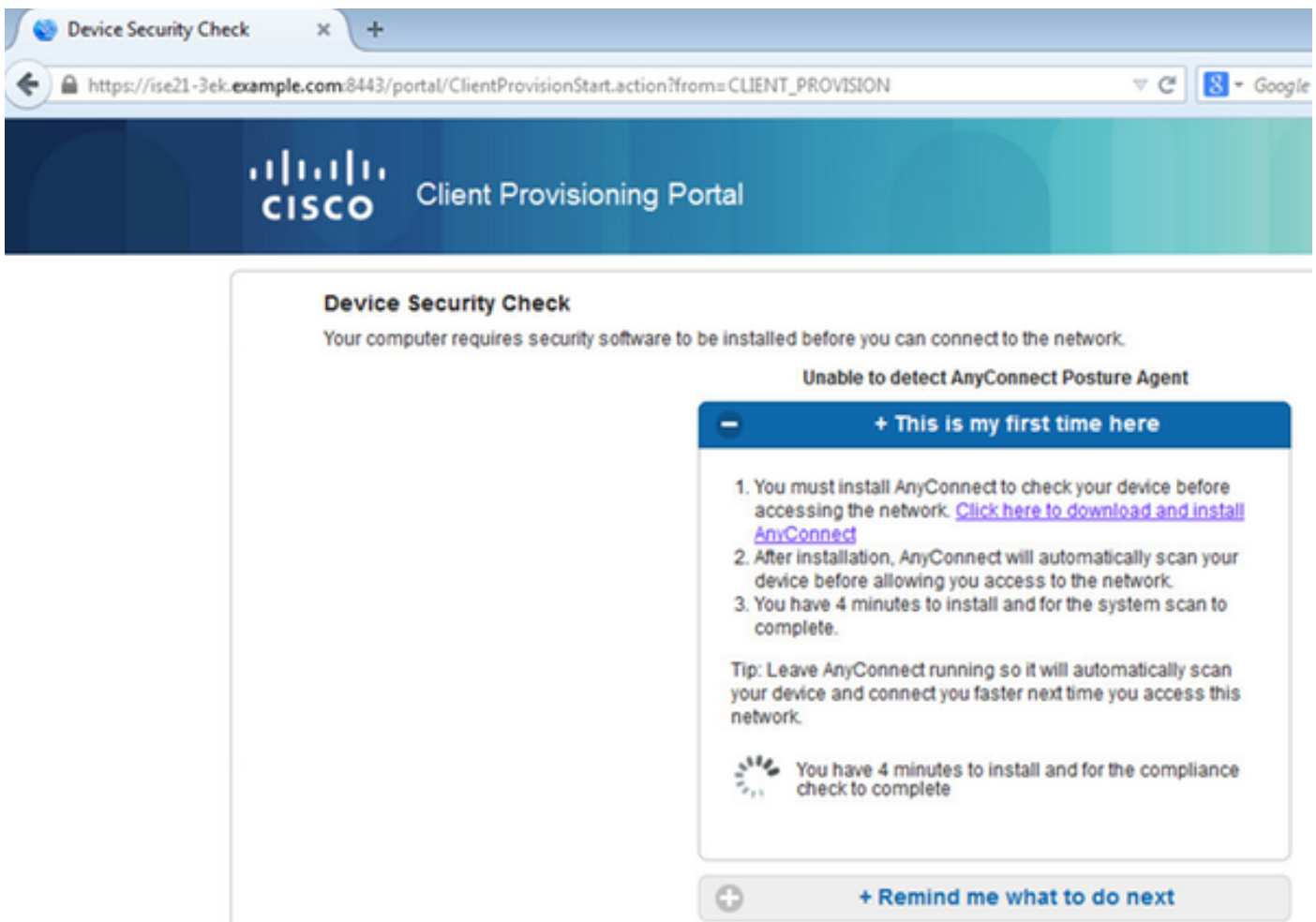
Verbinding aan een draadloos netwerk via PEAP (MSCHAPv2).



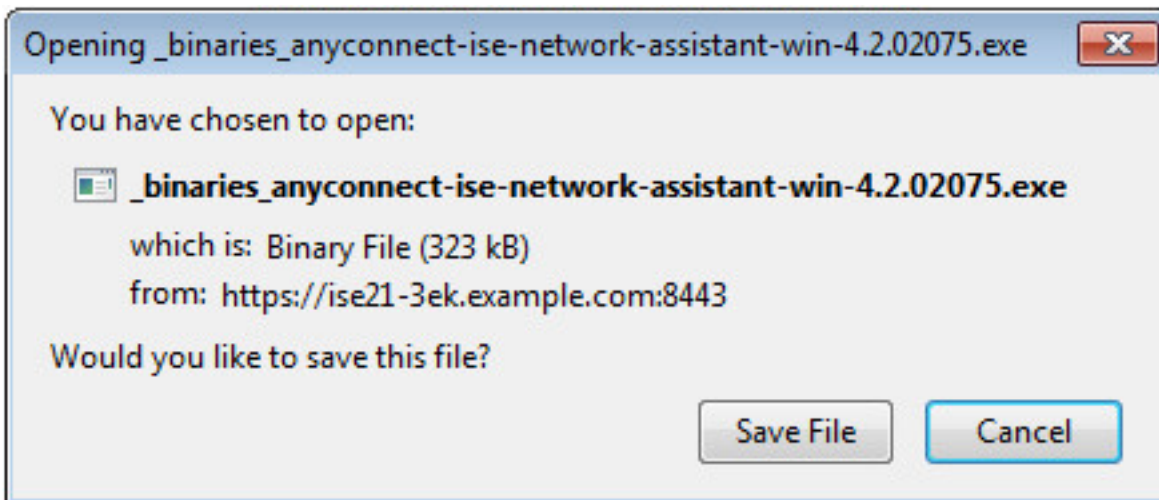
Zodra deze is aangesloten, wordt er verwezen naar Client Provisioning Portal.



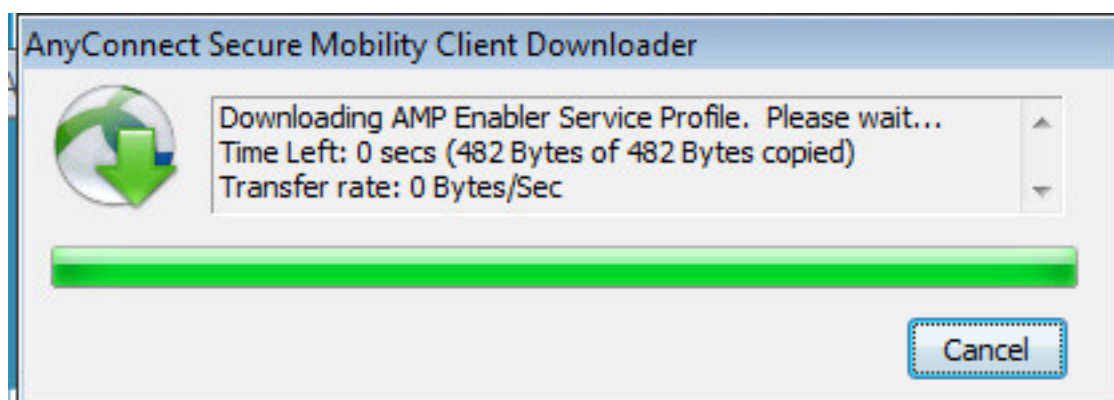
Aangezien er niets op de clientmachine is geïnstalleerd, vraagt ISE om een AnyConnect-client.

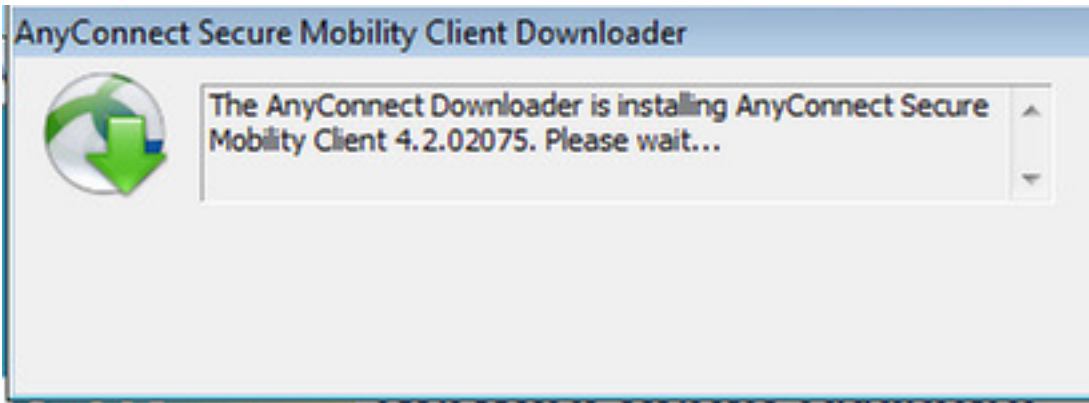


Network Setup Assistant-toepassing (NSA) dient te worden gedownload en te starten vanaf een clientmachine.

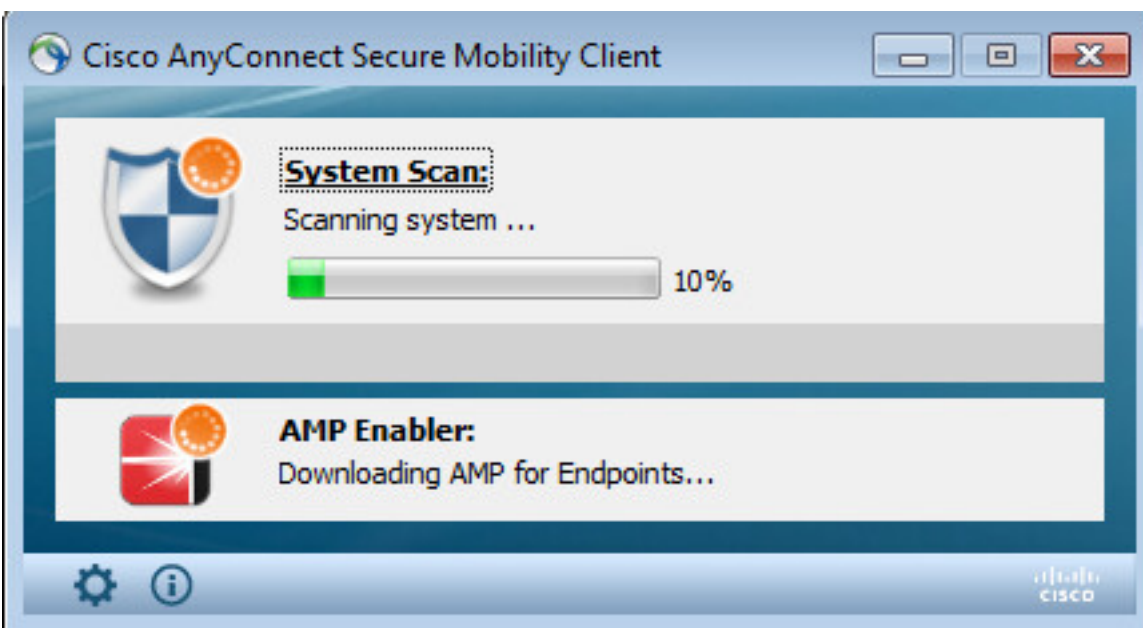
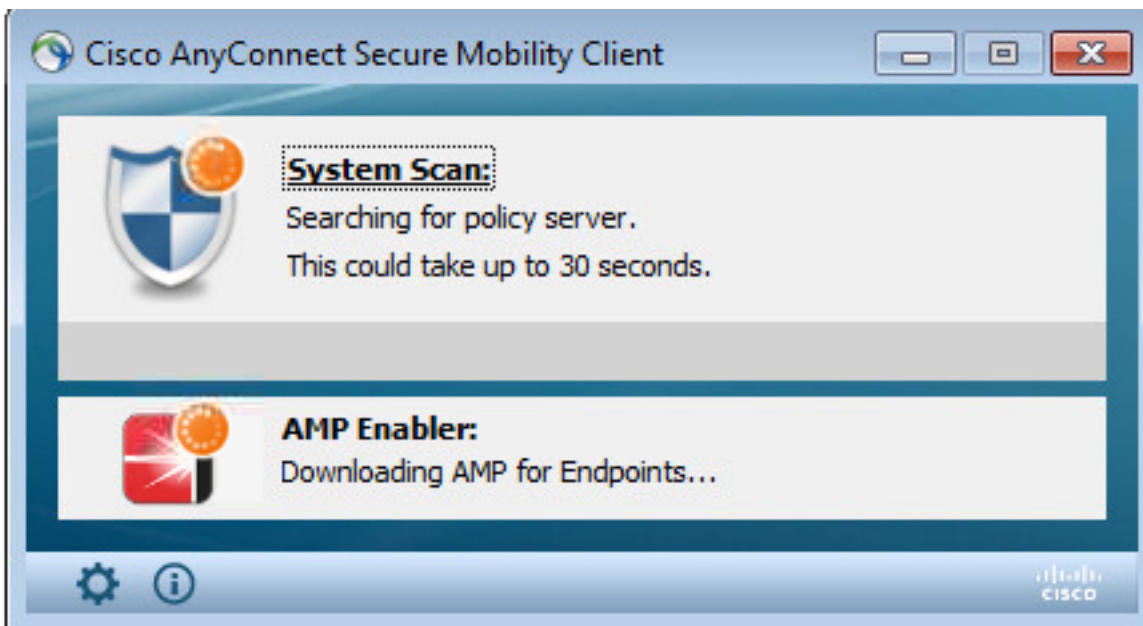


NSA zorgt voor het installeren van vereiste componenten en profielen.

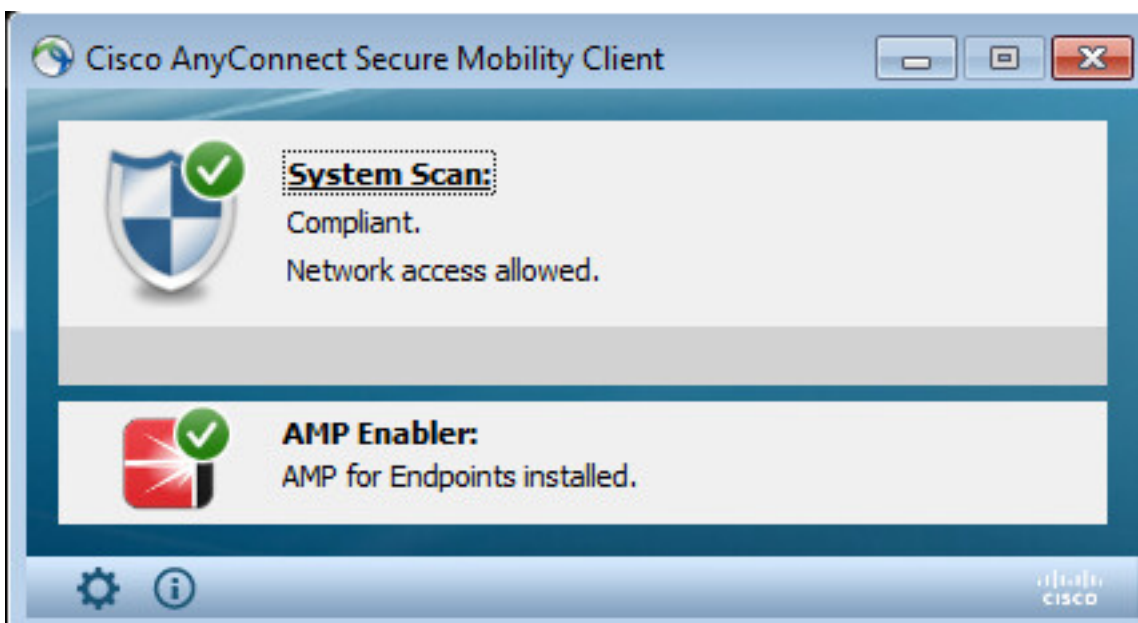
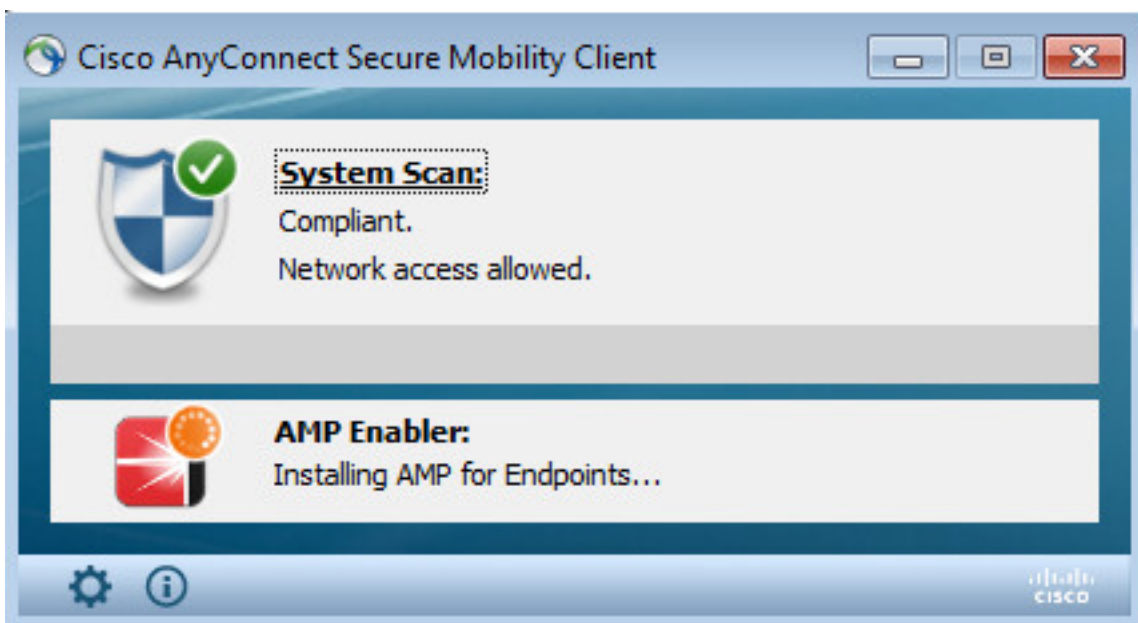
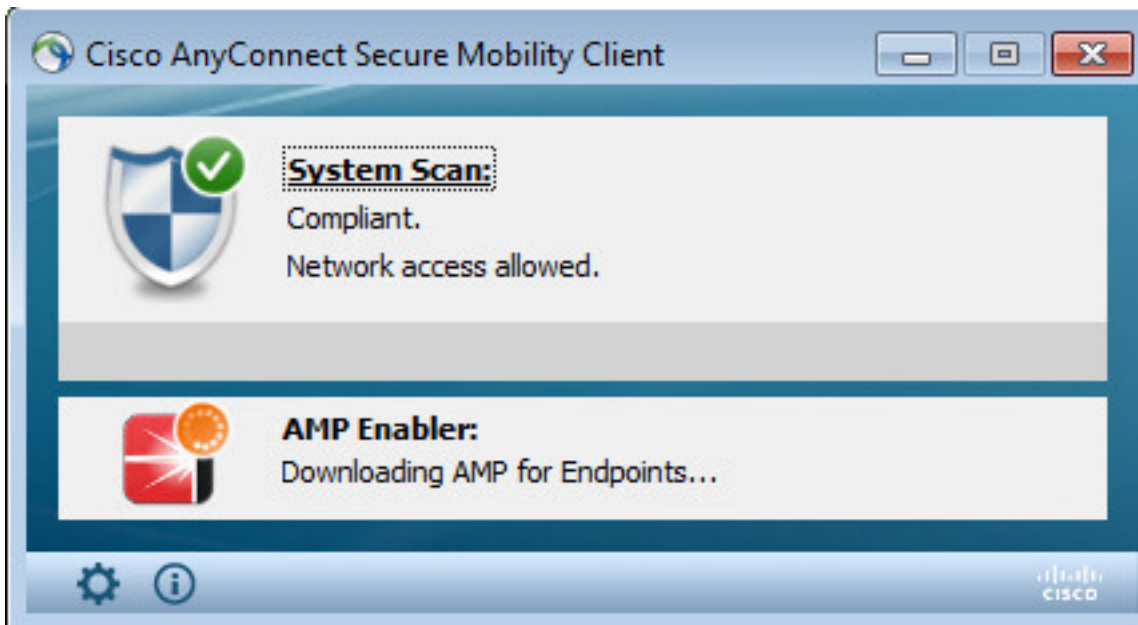




Nadat de installatie is voltooid, controleert de AnyConnect Posture-module de naleving van de voorschriften.



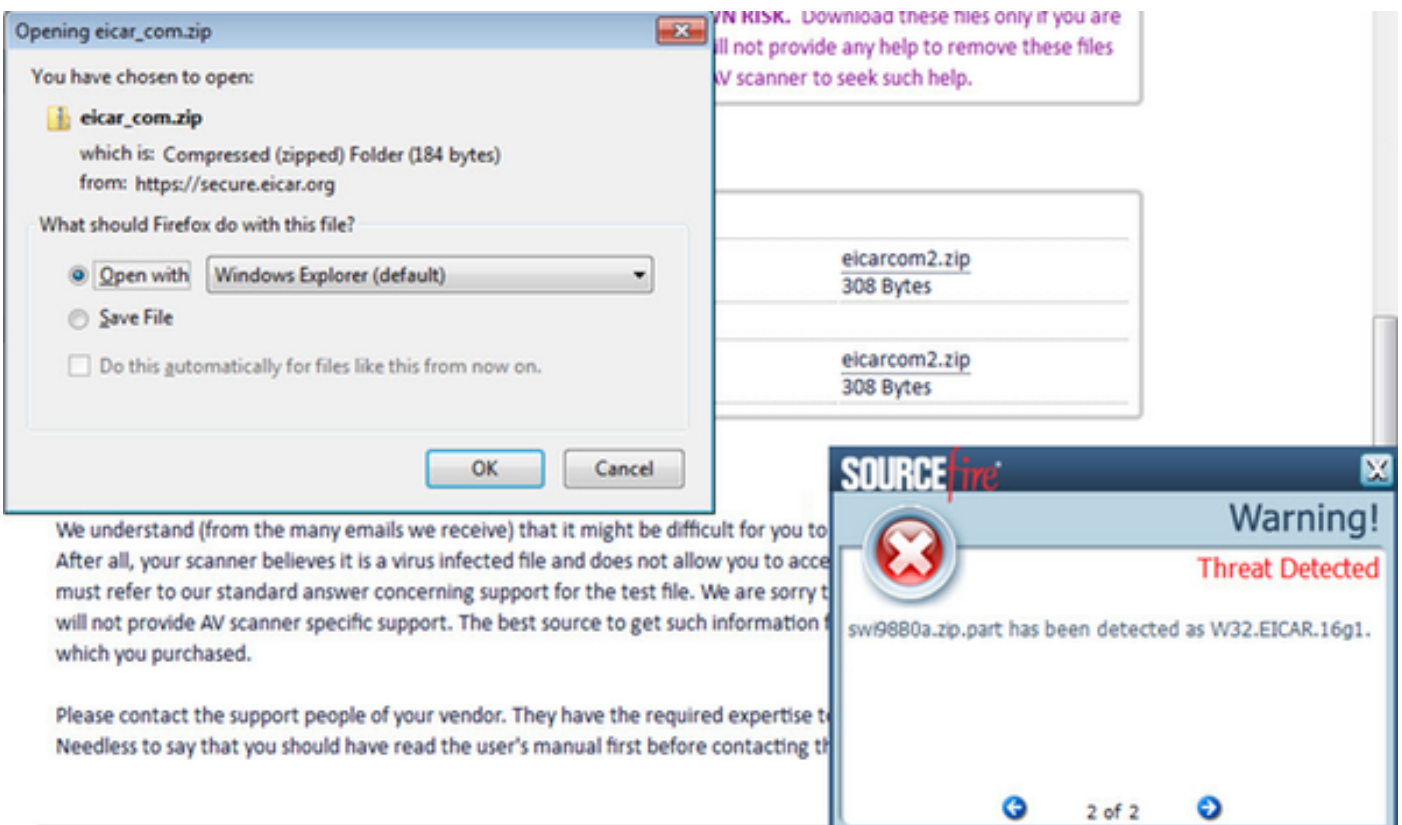
Aangezien volledige toegang wordt gegeven, als het eindpunt in overeenstemming is, wordt AMP gedownload en geïnstalleerd van de webserver die eerder in het AMP Profile is gespecificeerd.



AMP-connector verschijnt.



Om AMP in actie te testen wordt de Eicar string in een zip bestand gedownload. De dreiging wordt gedetecteerd en aan AMP Cloud gerapporteerd.



AMP-cloud

Om de details van het bedreigingsdashboard van de AMP cloud te controleren kan worden gebruikt.

The dashboard displays several key metrics:

- Indications of Compromise:** Shows a threat detected on `ekorneyc-PC.example.com`.
- Hosts Detecting Malware (7 days):**

Computer	Count
ekorneyc-PC.example.com	4
HARISHA-PC.example.com	1
- Malware Threats (7 days):**

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

Om meer informatie te krijgen over de dreiging, het pad en de vingerafdrukken, kunt u op de host klikken waar malware werd gedetecteerd.

The detailed view shows the following information:

- Event Type:** Threat Detected
- Filters:** Computer: `e8c02e6a-a885-47ba-aeec-2ac03bea4241`
- Sort:** Time
- Event Details:**
 - Host: `ekorneyc-PC.example.com`
 - Detection: `0M90PRxO.zip.part` as `W32.EICAR.16g1`
 - Quarantine: Not Seen
 - Timestamp: 2016-05-30 16:27:30 UTC
- File Detection Details:**

Field	Value
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)	3147bd8...32d689c2
Parent Filename	firefox.exe

Om geval van ISE te bekijken of te registreren kunt u naar accounts > Toepassingen navigeren

Applications

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

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

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

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

ISE

Op ISE zelf wordt een regelmatige posteringsstroom gezien, wordt eerst omleiding uitgevoerd om de netwerkconformiteit te controleren. Zodra het eindpunt in overeenstemming is, wordt CoA Reauth verzonden en wordt het nieuwe profiel met PermitAccess toegewezen.

Dashboard showing network statistics:

- 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 05:50:18.729 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	

Om de gedetecteerde bedreigingen te bekijken kunt u navigeren naar Context Visibility and > Endpoints > Combelloofde endpoints

Dashboard showing compromised endpoints:

COMPROMISED ENDPOINTS BY INCIDENTS

Bar chart showing impact levels: Unknown, Insignificant, Distracting, Painful, Damaging, Catastrophic. The 'Painful' category shows the highest number of incidents.

COMPROMISED ENDPOINTS BY INDICATORS

Bar chart showing likely impact levels: Unknown, None, Low, Medium, High. The 'Low' category shows the highest number of indicators.

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

Als u het eindpunt selecteert en naar het tabblad Threat navigeert, worden meer details weergegeven.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Endpoints Network Devices

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

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:

Attributes Authentication **Threats** Vulnerabilities

Threat Detected

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

Wanneer een bedreigingsgebeurtenis voor een eindpunt wordt gedetecteerd, kunt u het MAC-adres van het eindpunt op de pagina Compressed Endpoints selecteren en een ANC-beleid toepassen (indien geconfigureerd, bijvoorbeeld Quarantine). U kunt ook een wijziging van de vergunning geven om de sessie te beëindigen.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Endpoints Network Devices

Authentication BYOD Compliance **Compromised Endpoints** Endpoint Classification Guest Vulnerable Endpoints

COMPROMISED ENDPOINTS BY INCIDENTS
All endpoints | Connected | Disconnected

Unknown Indifferent Distressing **Painful** Damaging Catastrophic
IMPACT LEVEL

COMPROMISED ENDPOINTS BY INDICATORS
All endpoints | Connected | Disconnected

Unknown None **Painful** Low Medium High
LIKELY IMPACT LEVEL

1 Selected Rows/Page 2

Network Add Train Edit ANC Change Authorization Clear Threats & Vulnerabilities Export Import SCM Actions Revoke Certificate

MAC Address	Username	Source	Threat Severity	Logical NAD Location	Connectivity	Hostname	Identity Group	Endpoint OS
24:77:69:3D:CF:20	hostNARISHA-PC.ens...	AMP	Painful	Location#A1 Locations	Disconnected		Workstation	
C0:4A:00:14:8D:4B	alice	AMP	Painful	Location#A1 Locations	Connected		Workstation	

Als CoA Session Terminate is geselecteerd, stuurt ISE CoA Disconnect en verliest client toegang tot het netwerk.

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

Problemen oplossen

Om debugs op ISE in te schakelen, navigeer naar Administratie > Systeem > Vastlegging > Loggen > Logconfiguratie van het Debug Logbestand, selecteer TC-NAC Node en wijzig het logniveau van de TC-NAC component in **DEBUG**

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Debug Log Configuration' selected. The main content area displays the 'Debug Level Configuration' page for the 'TC-NAC' component. The page includes an 'Edit' button and a 'Reset to Default' button. A table shows the configuration for the 'TC-NAC' component, with the 'Log Level' set to 'DEBUG' and the 'Description' as 'TC-NAC log messages'.

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

Aanmelden om te controleren - irf.log. U kunt deze direct staart vanaf ISE CLI:

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

Bedreiging wordt zelfs ontvangen van de AMP Cloud

```
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-notification-0][  
cisco.cpm.amqp.notificationDispatcher:processDelivery:53 - :  
m.irf.service.IrfnotificationHandler$MyNotificationHandler@3fac8043 Message  
{messageType=NOTIFICATION, messageID=THREAT_EVENT, content='\"c0:4a:00:14:8d:4b\": [  
{"Impact_Qualification": "Pijnlijk"}, "tijdstempel": 1467304068599, "verkoper": AMP, "titel":  
"Threat Detected"]]', Priority=0, timestamp=Thu jun 30 18:27:48 CEST 2016, amqpEnvelope=Envelope  
(deliveryTag=79, remake=vals, exchange=irf.topic.events, RoutingKey=irf.events.dreigement),  
qpProperties=#contentHeader<basic>(content-type=application/json, content-encoding=ongeldige,  
headers=zero, delivery-mode=ongeldige, Priority=0, correlatie-id=ongeldige, response-to=Nut,  
expiration=nul, bericht-id=THREAT_EVENT, timestamp=ongeldige, type=NOTIFICATION, user-  
id=ongeldige, app-id=o8fe e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=ongeldige)}  
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-notification-0][  
cisco.cpm.irf.service.IrfnotificationHandler:handle:handle:140 -:- toegevoegd aan de wachtrij:  
Bericht {berichtType=NOTIFICATION, messageID=THREAT_EVENT, content='<\"c0:4a:00:14:8d:4b\":  
[<\"incident\": {\"Impact_Qualification\": \"Pijnlijk\"}, \"tijdstempel\": 1467304068599, \"verkoper\":  
\"AMP\", \"titel\": \"Bedreigingsdetectie\"}]', prioriteit=0, timestamp=Thu jun 30 18:27:48 CEST 2016,  
amqpEnvelope=Envelope (deliveryTag=79, redelivery=irf.topic.events,  
RoutingKey=irf.events.dreigen), amqpProperties= #contentHeader<basic>(content-  
type=application/json, content-encoding=ongeldige, headers=nul, delivery-mode=0, prioritaair-  
id=ongeldige, correlatie-id=ongeldige, response-to=Nul, expiration=nul, bericht-id=THREAT_EVENT,  
timestamp=ongeldige, type=NOTIFICATION, user-id=ongeldige, app-id=fe80e16e e-cde8-4d7f-a836-  
545416ae56f4, cluster-id=ongeldige)}  
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-notification-0][  
cisco.cpm.irf.amqp.notificationDispatcher:processDelivery:59 -:: Envelope (deliveryTag=79,  
redelivery=false, exchange=irf.topic.events, RoutingKey=irf.events.dreigen)  
#contentHeader<basic>(content-type=application/json, content-encoding=zero, content-headers=nul,  
delivery-mode=nul, correlatie-id=Nul, antwoord-to=default, expiration=nul, bericht-id=DN  
REAT_EVENT, timestamp=DN, type=NOTIFICATION, user-id=DN, app-id=fe80e16e-cde8-4d7f-a836-  
545416ae56f4, cluster-id=ongeldige)  
2016-06-30 18:27:48,706 DEBUG [IRF-EventProcessor-0][  
cisco.cpm.irf.service.IrfEventProcessor:parsenotification:221 -:: - parsing notification:  
Bericht {berichtType=NOTIFICATION, messageID=THREAT_EVENT, content='\"c0:4a:00:14:8d:4b\":  
[<\"incident\": {\"Impact_Qualification\": \"Pijnlijk\"}, \"tijdstempel\": 1467304068599, \"verkoper\":  
AMP, \"titel\": \"Bedreigingsdetectie\"}]', prioriteit=0, timestamp=Thu jun 30 18:27:48 CEST 2016,  
amqpEnvelope=Envelope (deliveryTag=79, redelivery=irf.topic.events,  
RoutingKey=irf.events.dreigen), amqpProperties= #contentHeader<basic>(content-  
type=application/json, content-encoding=ongeldige, headers=nul, delivery-mode=0, prioritaair-  
id=ongeldige, correlatie-id=ongeldige, response-to=Nul, expiration=nul, bericht-id=THREAT_EVENT,  
timestamp=ongeldige, type=NOTIFICATION, user-id=ongeldige, app-id=fe80e16e e-cde8-4d7f-a836-  
545416ae56f4, cluster-id=ongeldige)}
```

Informatie over de bedreiging wordt naar PAN verzonden

```
2016-06-30 18:27:48,724 DEBUG [IRF-EventProcessor-0][  
cisco.cpm.irf.service.IrfEventProcessor:StoreEventsInES:366 -:: - bedreigingsinformatie toe te  
zenden aan PHP AN - c0:4a:00:14:8d:4b {incident= {Impact_Qualification=Pijnlijk},  
tijdstempel=1467304068599, seller=AMP, title=Threat Detected}
```