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

Inhoud

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

Netwerkdiagram

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

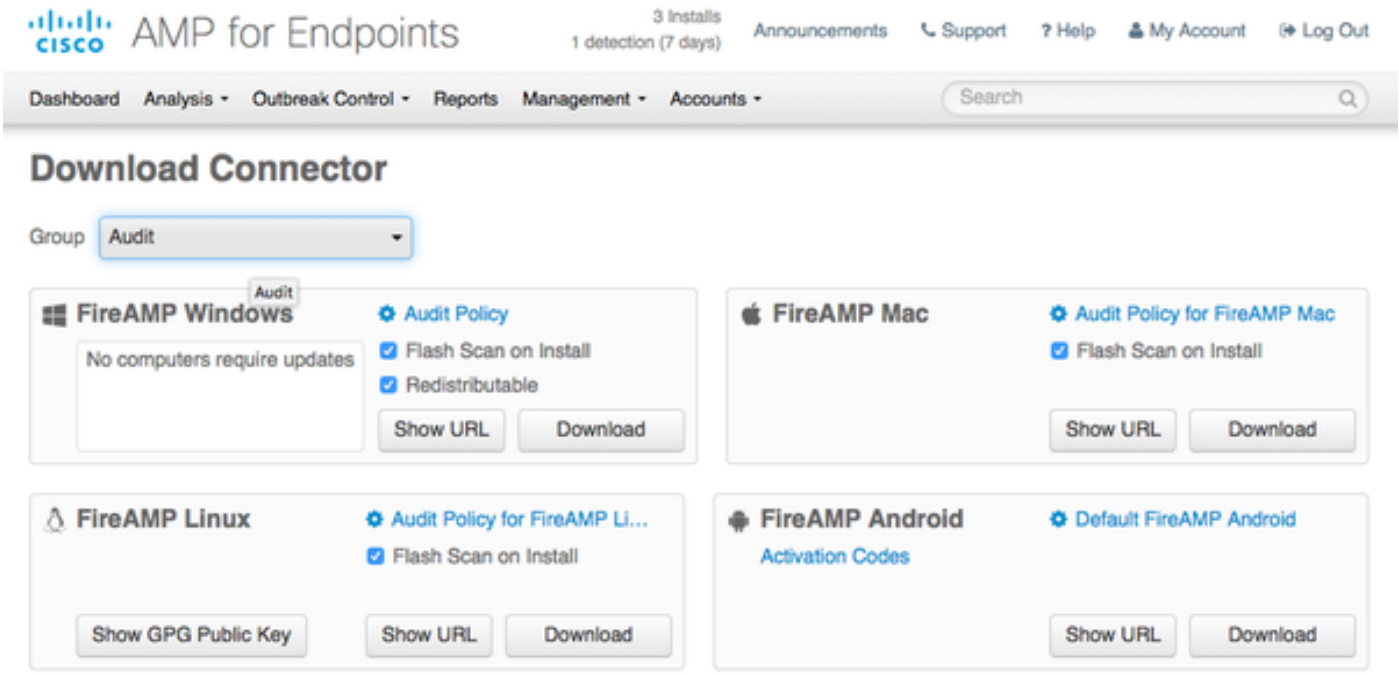
4. Wanneer een cliënt probeert kwaadaardige software te downloaden, stuurt de AMP-connector een waarschuwingsbericht en meldt het aan de AMP Cloud

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.

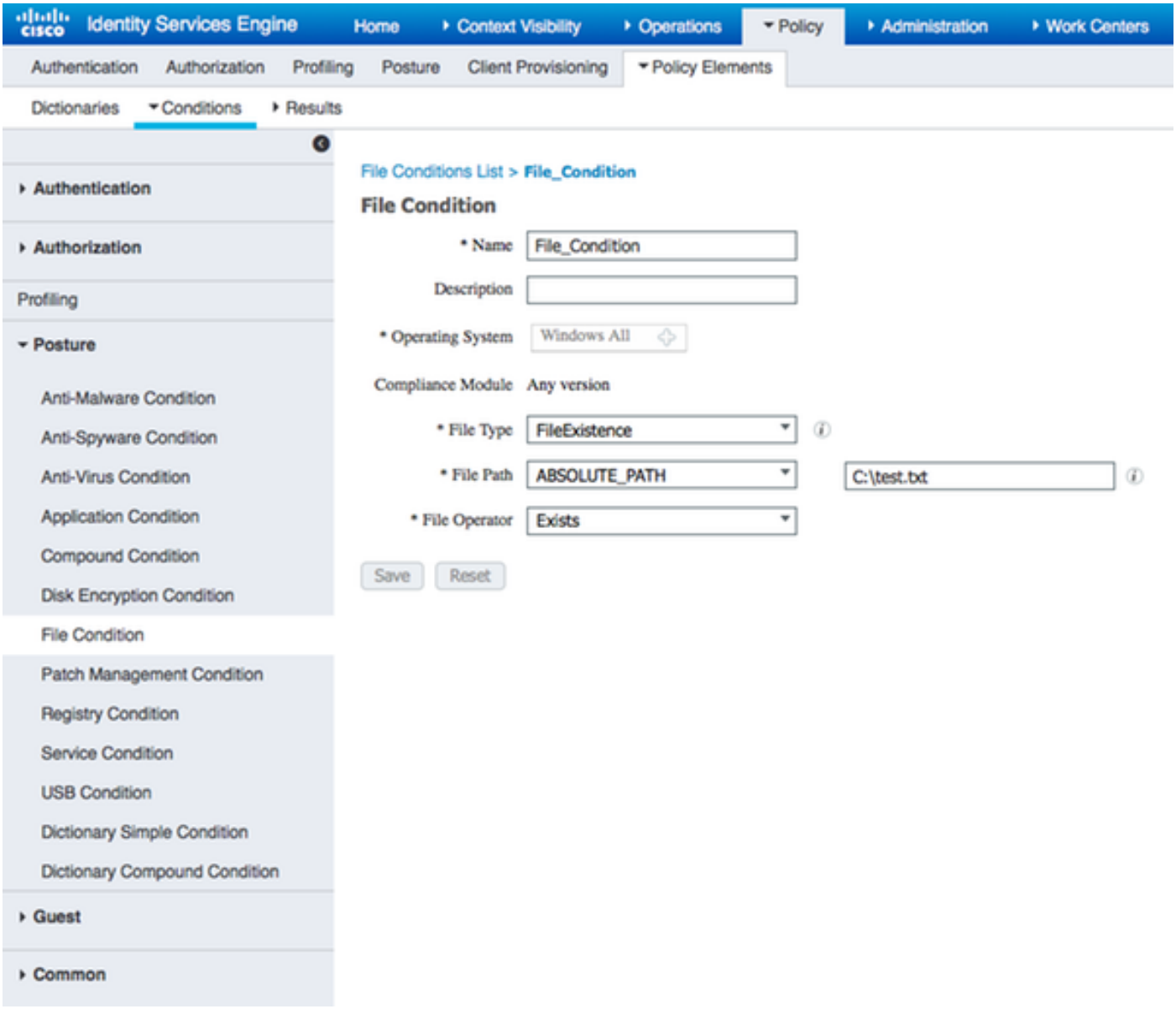


> Opmerking: Het downloaden van dit bestand genereert een .exe-bestand dat **Audit_FireAMPSetup.exe** heet in het voorbeeld. Dit bestand is naar de webserver gestuurd zodat het beschikbaar is zodra de gebruiker om de configuratie van de Advanced Malware Protection vraagt.

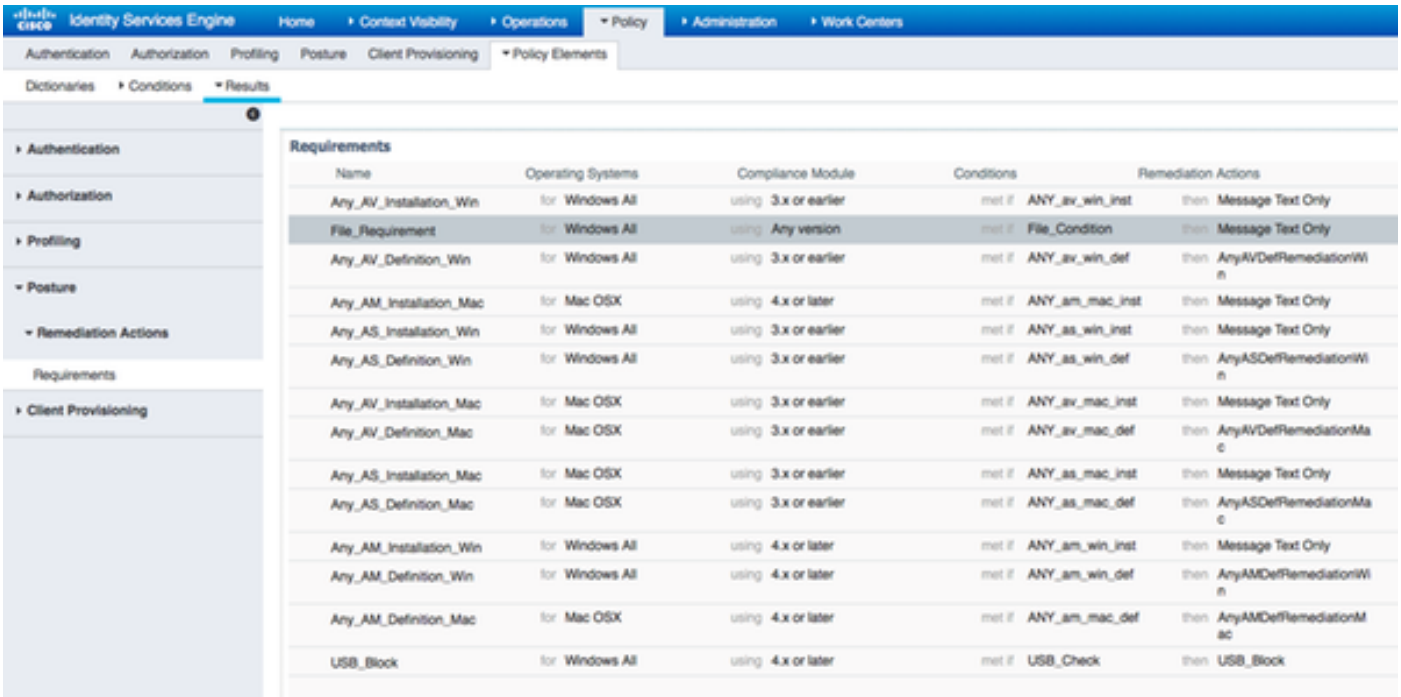
ISE configureren

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

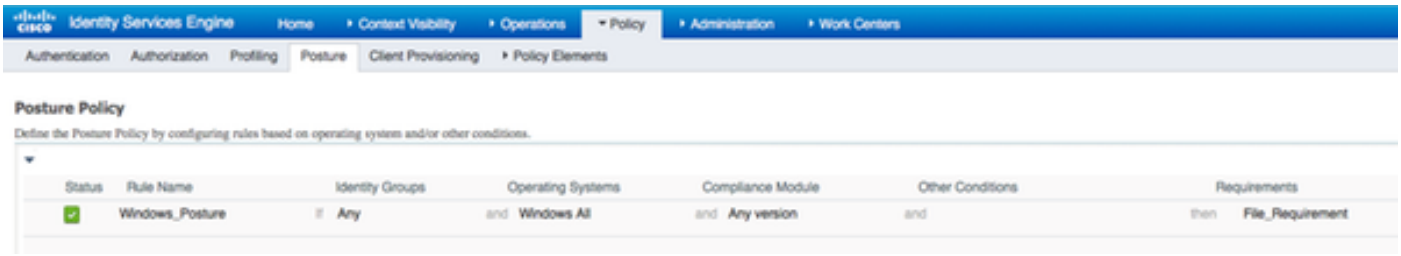
Navigeren in op Policy > Policy Elementen > Voorwaarden > Posture > File Condition.U kunt zien dat er een eenvoudige voorwaarde voor het bestaan van bestanden is gemaakt. Bestand moet bestaan indien het eindpunt in overeenstemming is met het door de Postmodule geverifieerde beleid:



Deze voorwaarde wordt gebruikt voor een vereiste:

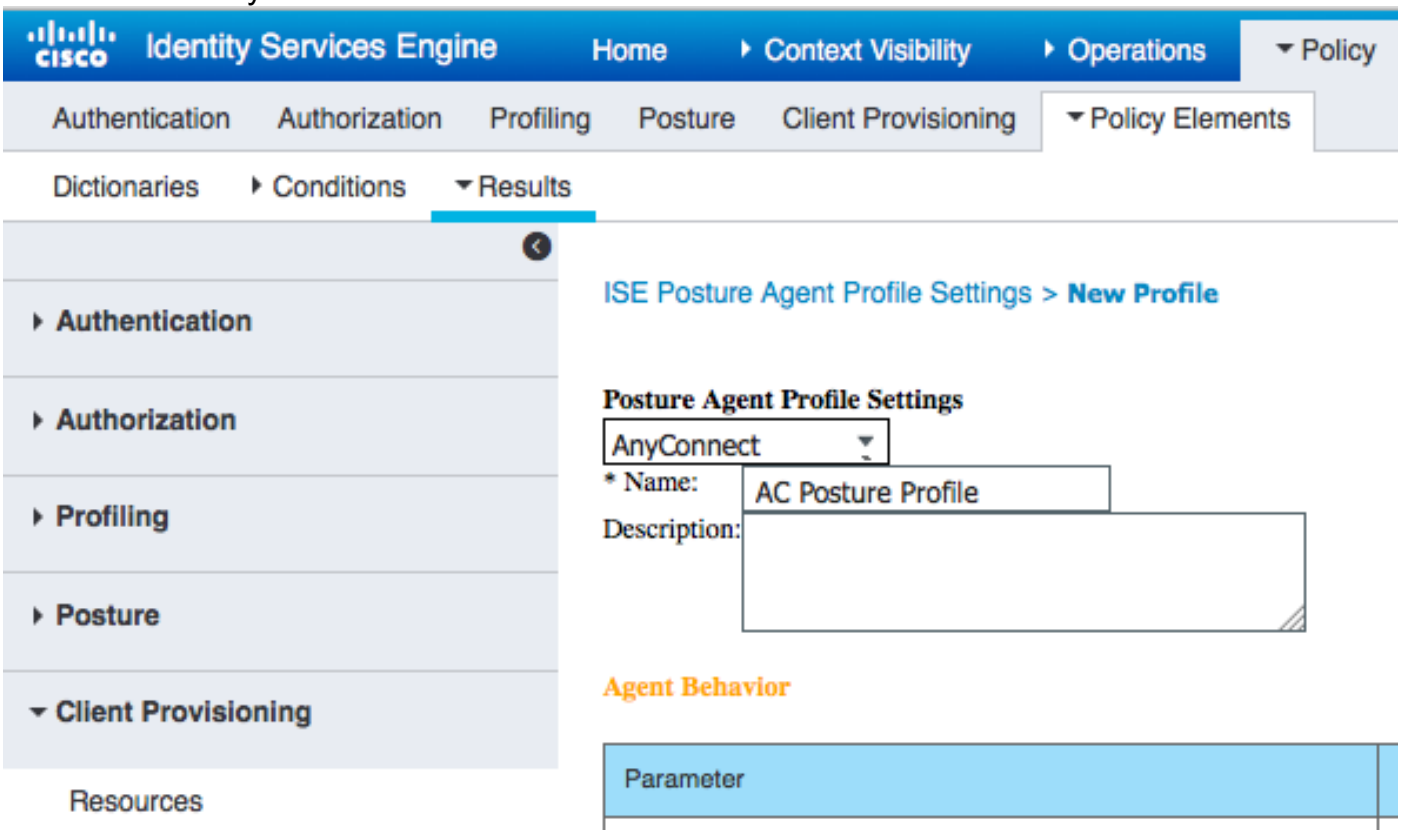


Dit vereiste wordt gebruikt in het Posture-beleid voor Microsoft Windows-systemen:

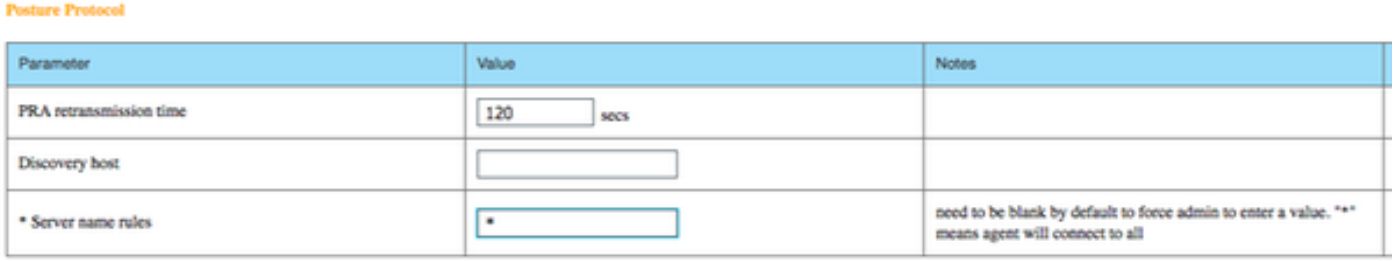


Stap 2. Postprofiel configureren

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



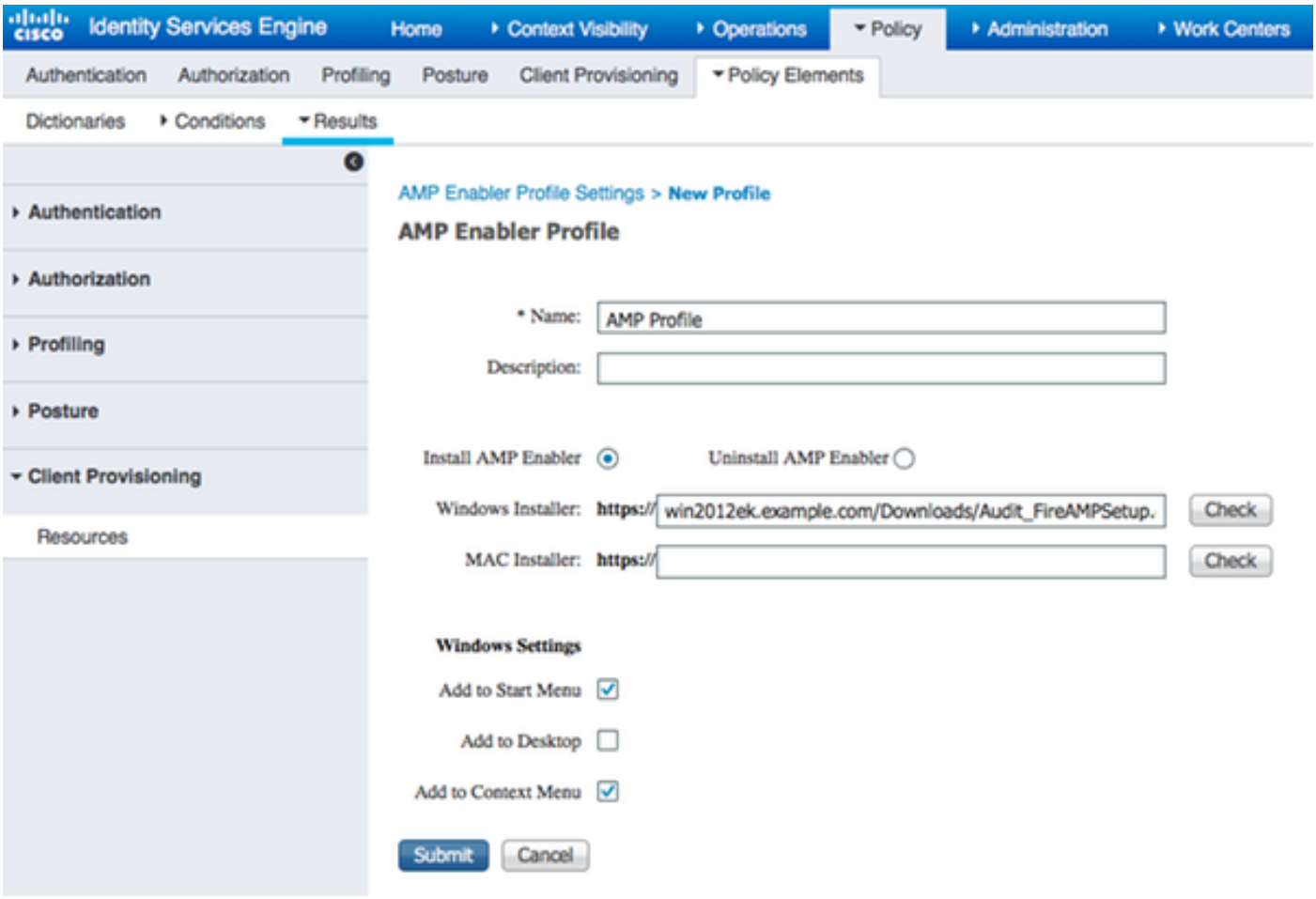
- Toevoegen van het gedeelte Posture Protocol * om de Agent in staat te stellen verbinding te maken met alle servers



Stap 3. AMP-profiel configureren

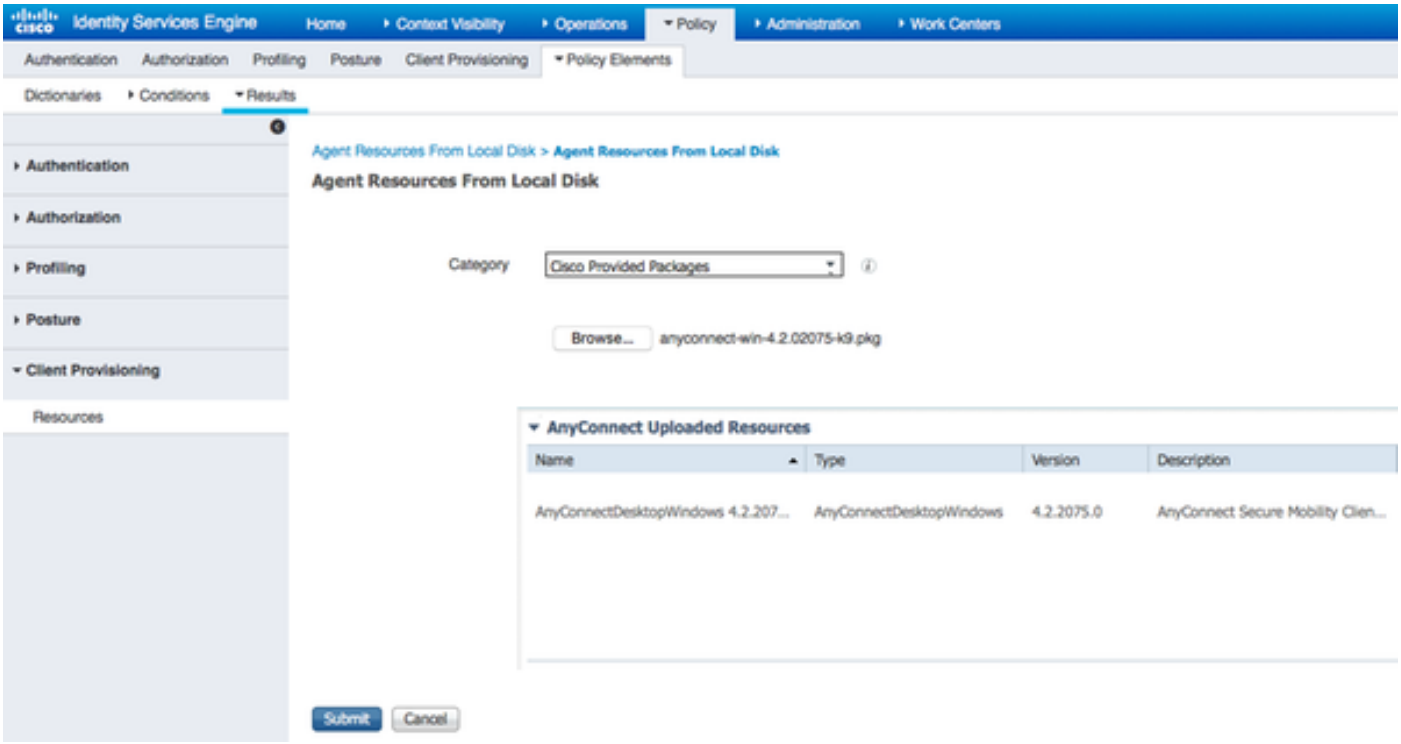
AMP Profile bevat informatie waar het Windows-installatieprogramma zich bevindt. Windows Installer is eerder gedownload van de Advanced Malware Protection Cloud. Het moet toegankelijk zijn vanaf de klant. Certificaat van de HTTPS Server, waar Installer zich bevindt, zou ook door

client machine moeten worden vertrouwd.

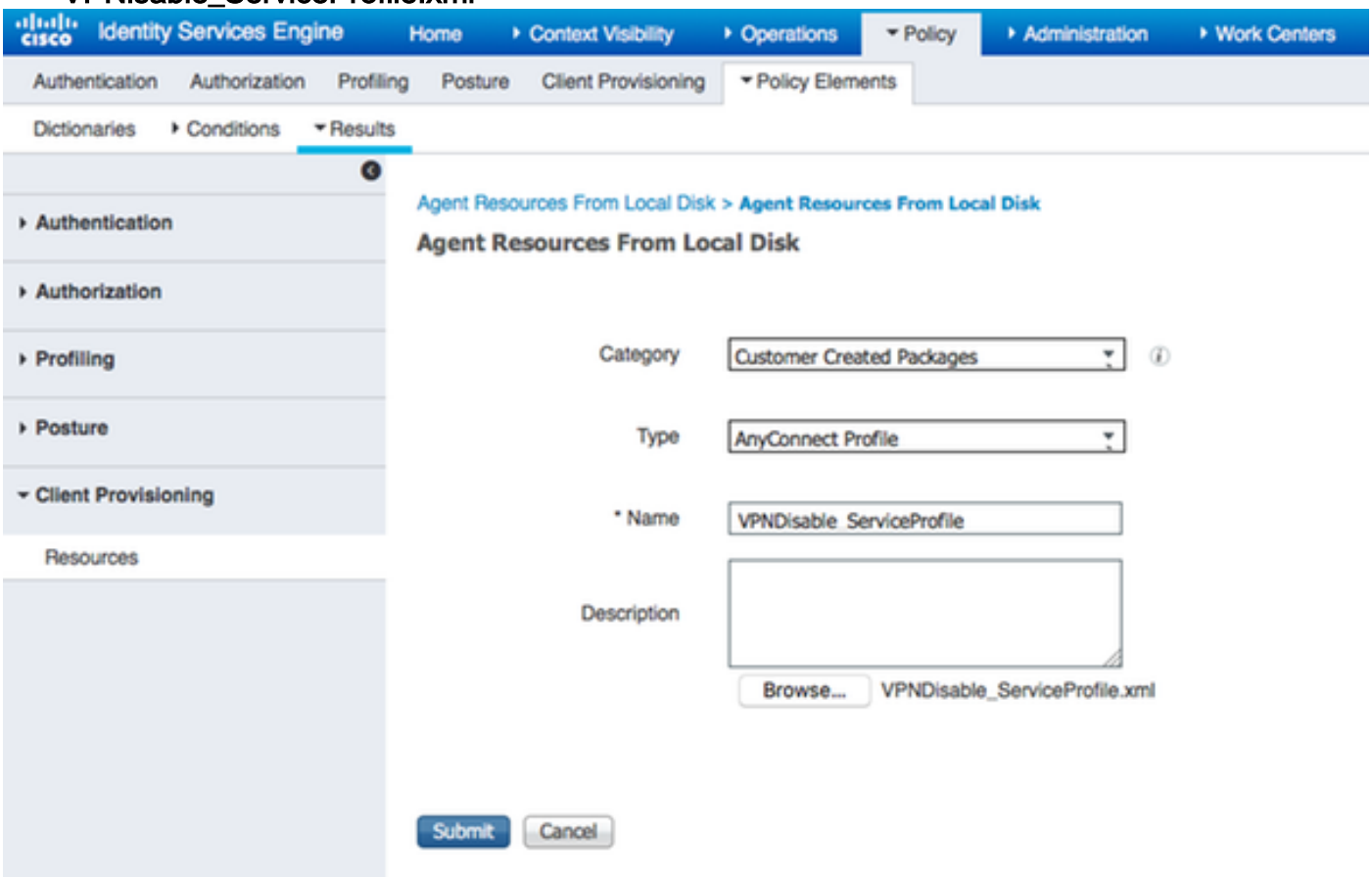


Stap 2. Uploadtoepassingen en XML-profiel naar ISE

- 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**



- 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**

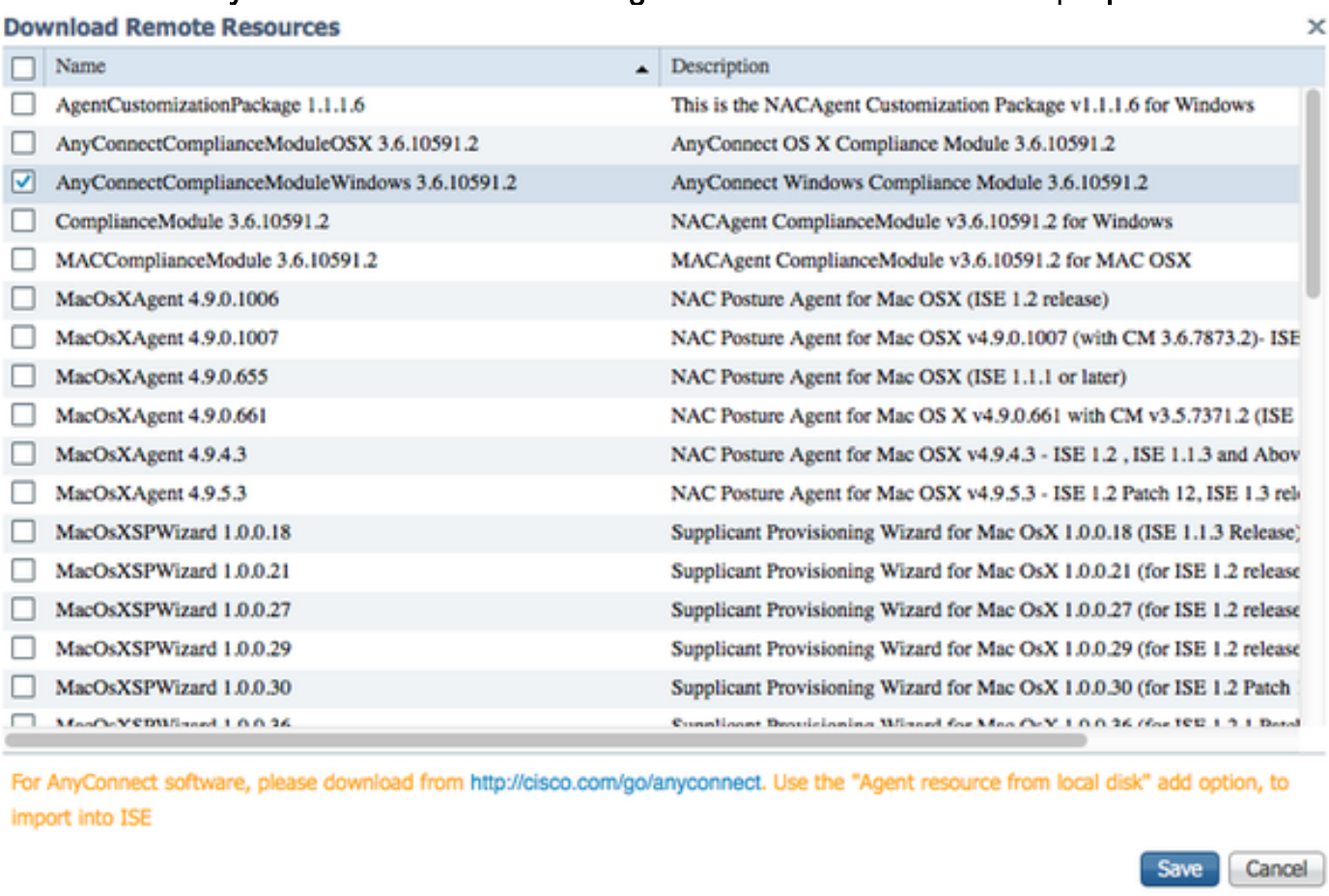


Opmerking: **VPNDisable_ServiceProfile.xml** wordt gebruikt om de titel van VPN te verbergen, aangezien dit voorbeeld geen VPN-module gebruikt. Dit is de inhoud van **VPNisable_ServiceProfile.xml**:

```
<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>
```

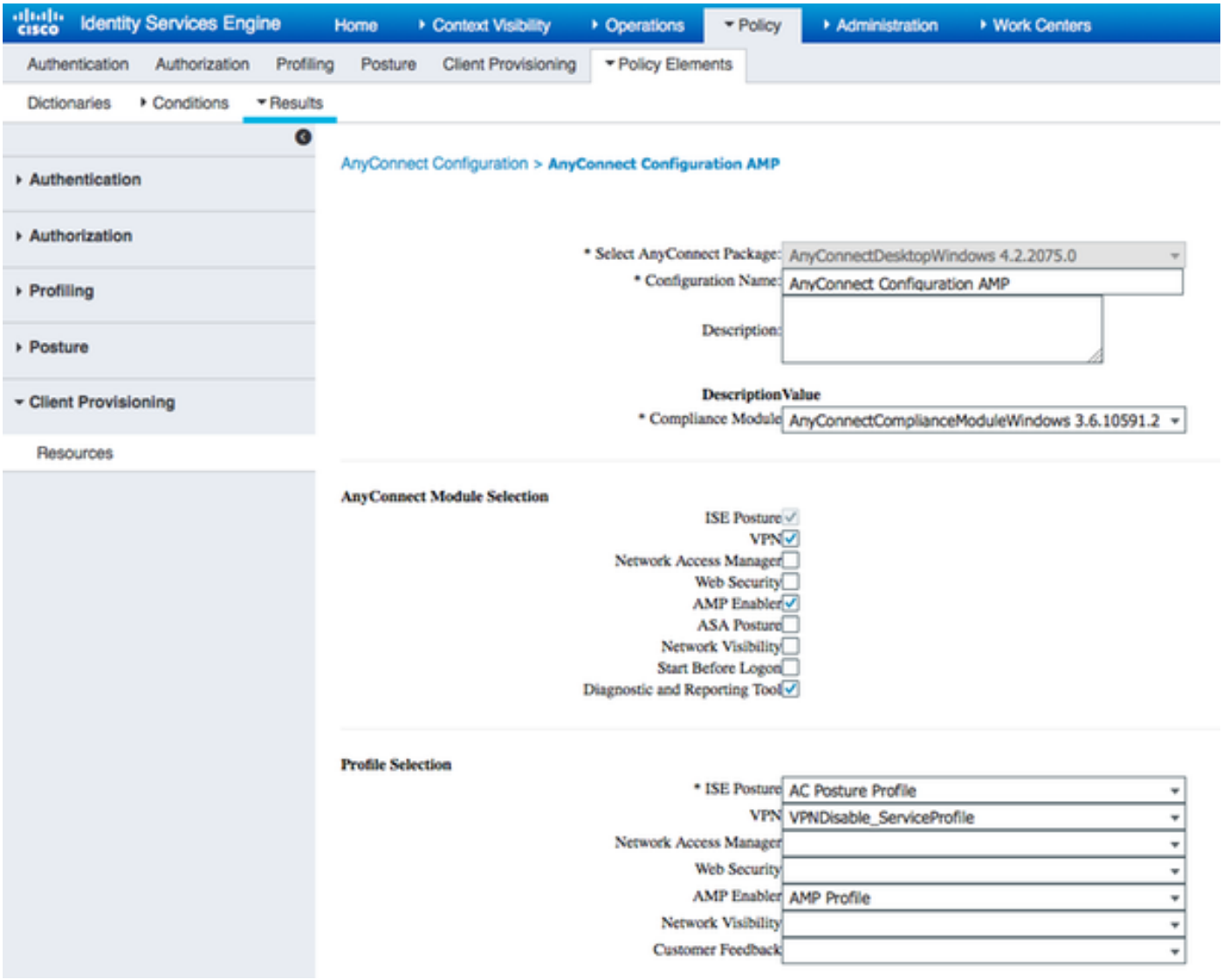
Stap 3. Download AnyConnect-nalevingsmodule

- 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**



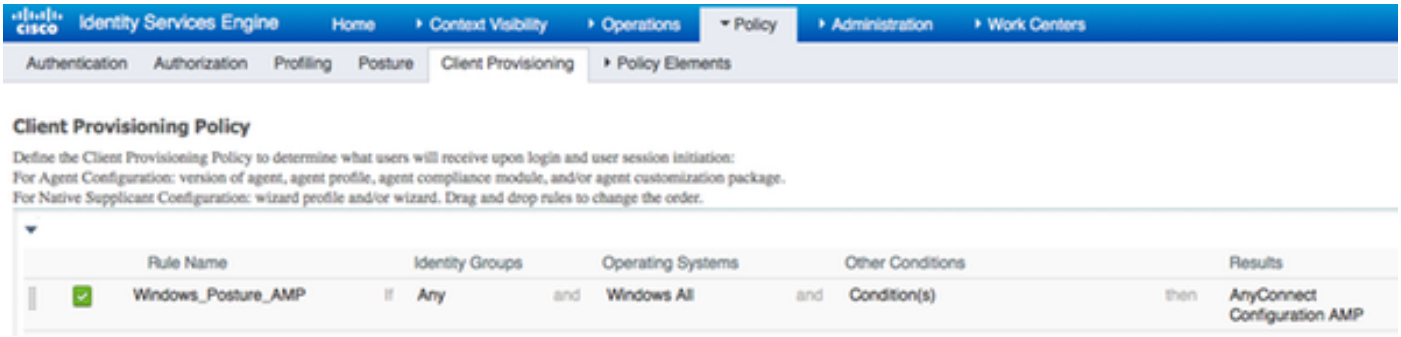
Stap 4. Voeg AnyConnect-configuratie toe

- 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



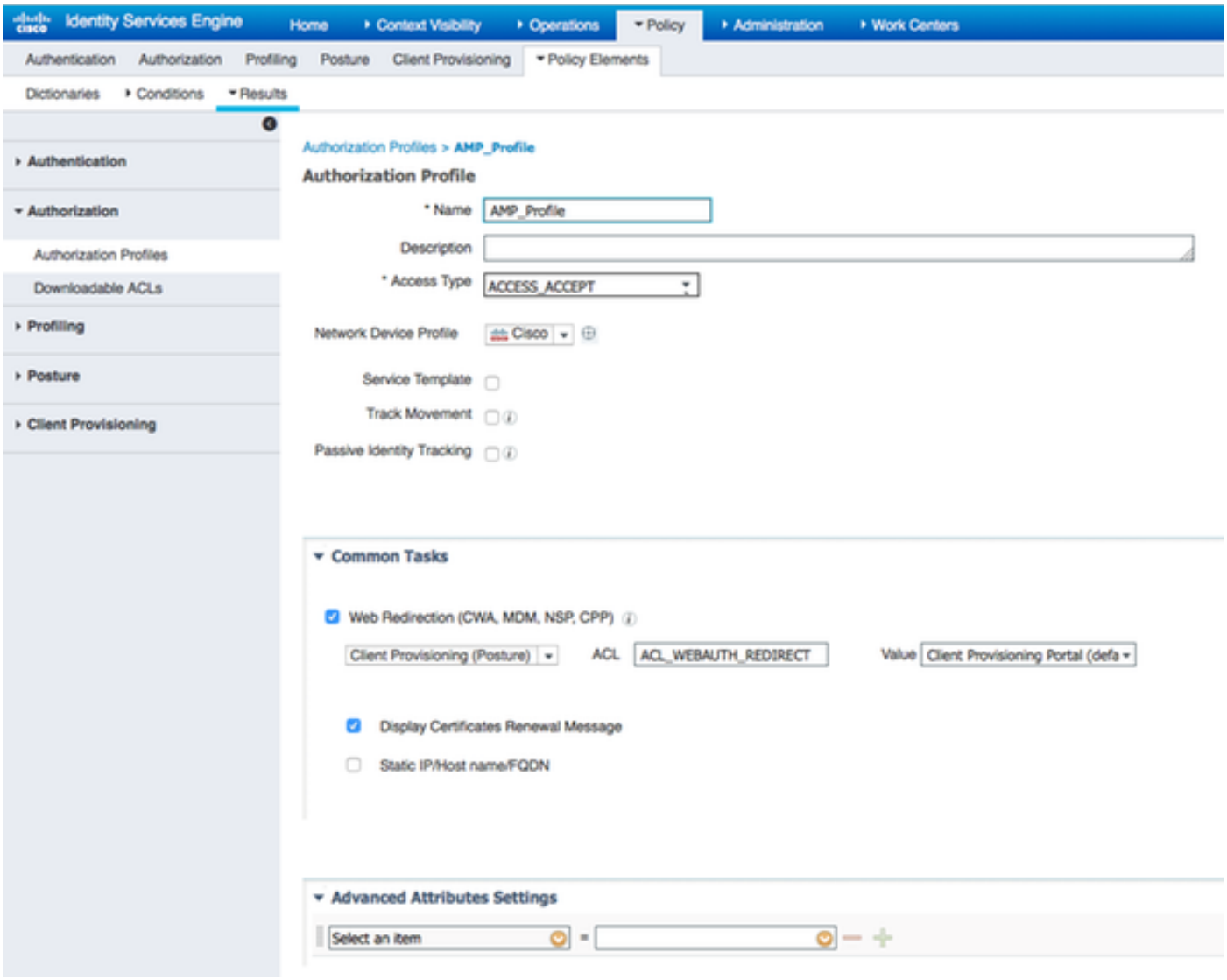
Stap 5. Instellen van regels voor clientprovisioning

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

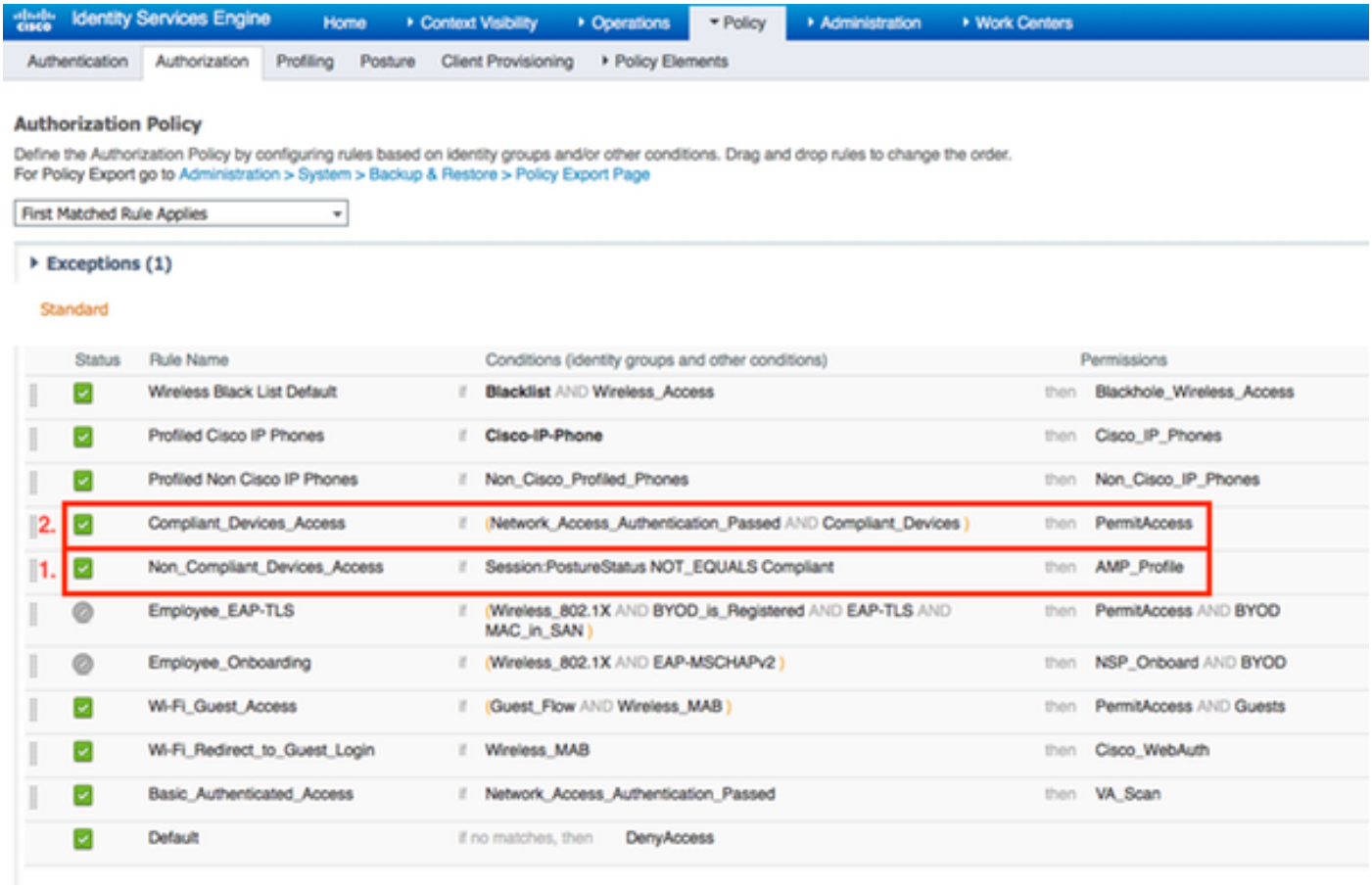


Stap 6. Instellen van het vergunningsbeleid

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

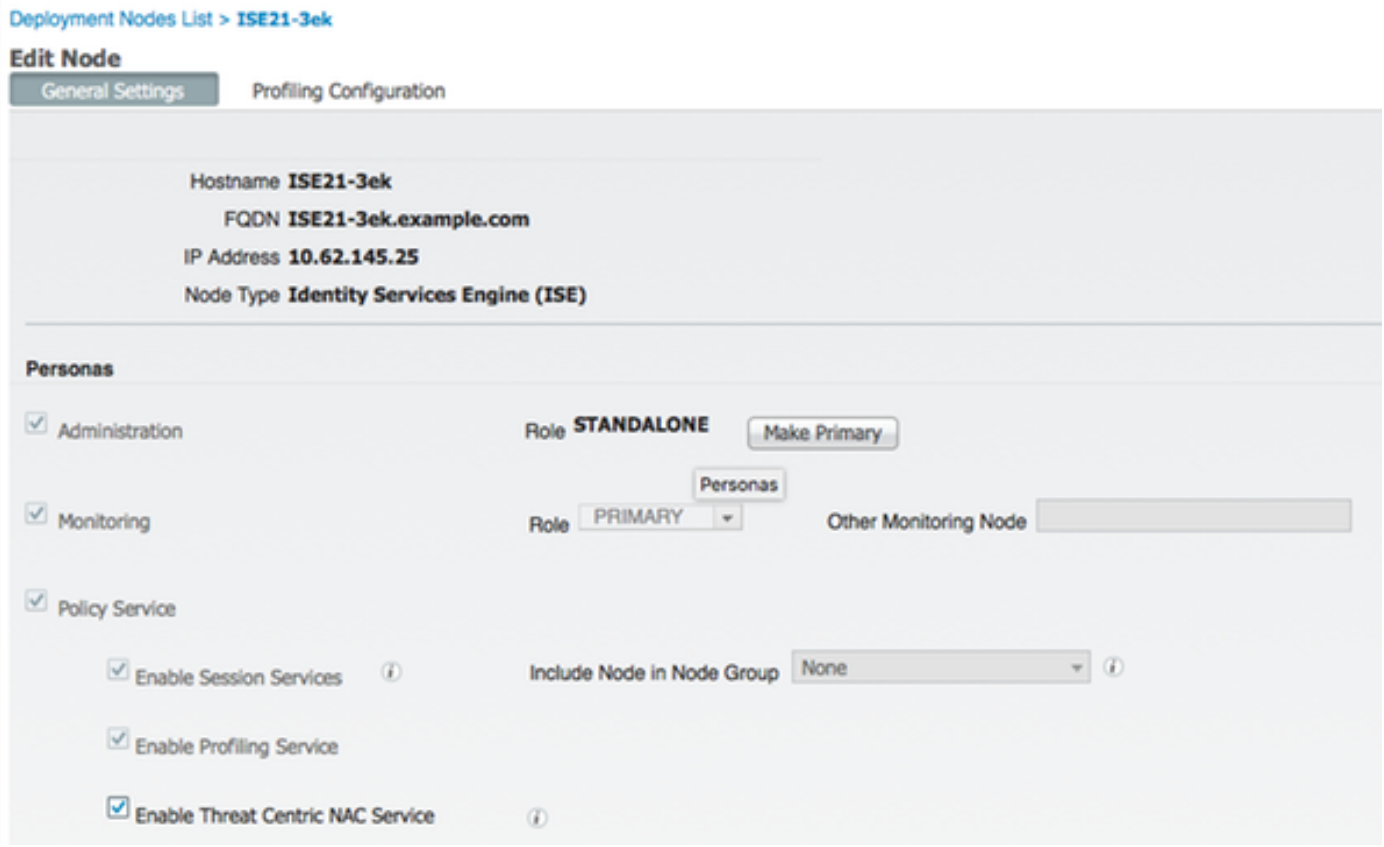


Daarna wordt volledige toegang toegewezen zodra dit voldoet



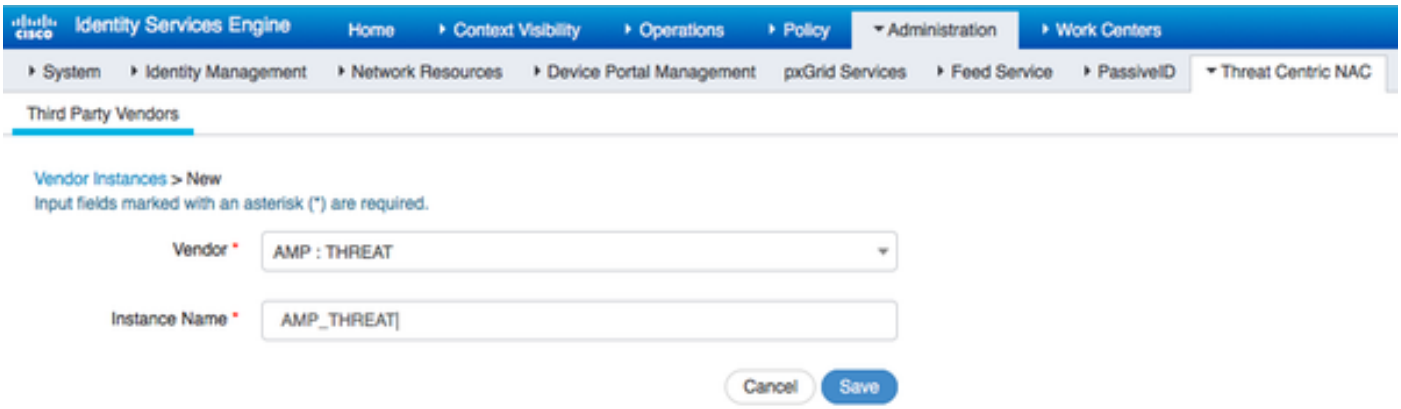
Stap 7. Schakel TC-NAC-services in

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

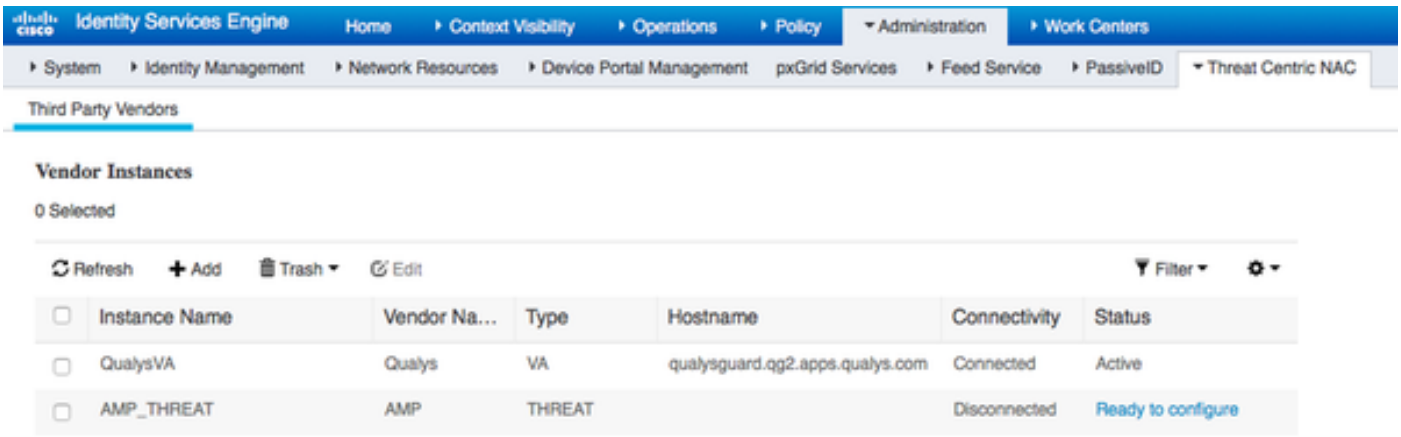


Stap 8. AMP-adapter configureren

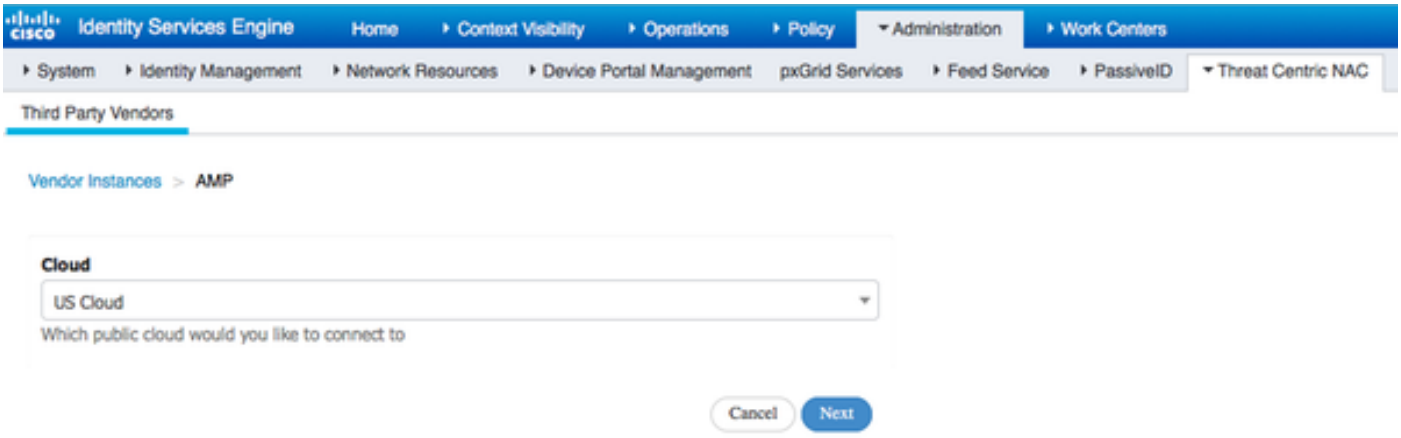
Navigatie in naar Administratie > Bedreigingscentrifuge NAC > Verkopers van derden > Toevoegen. Klik op **Opslaan**



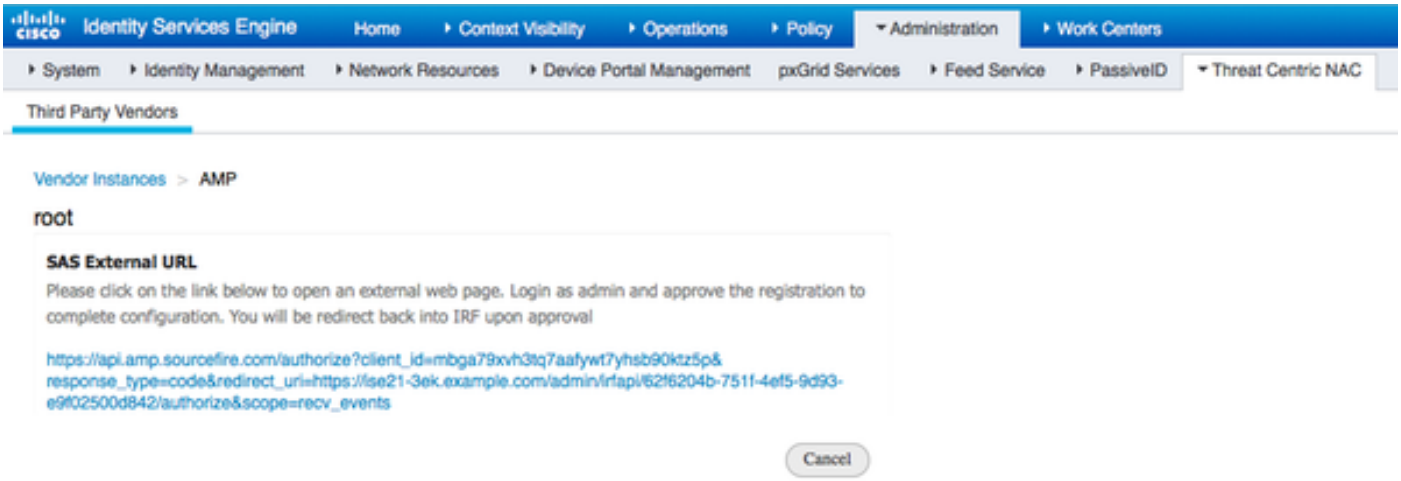
Het zou moeten overschakelen naar **Klaar om** staat **te configureren**. Klik op **Klaar om te configureren**



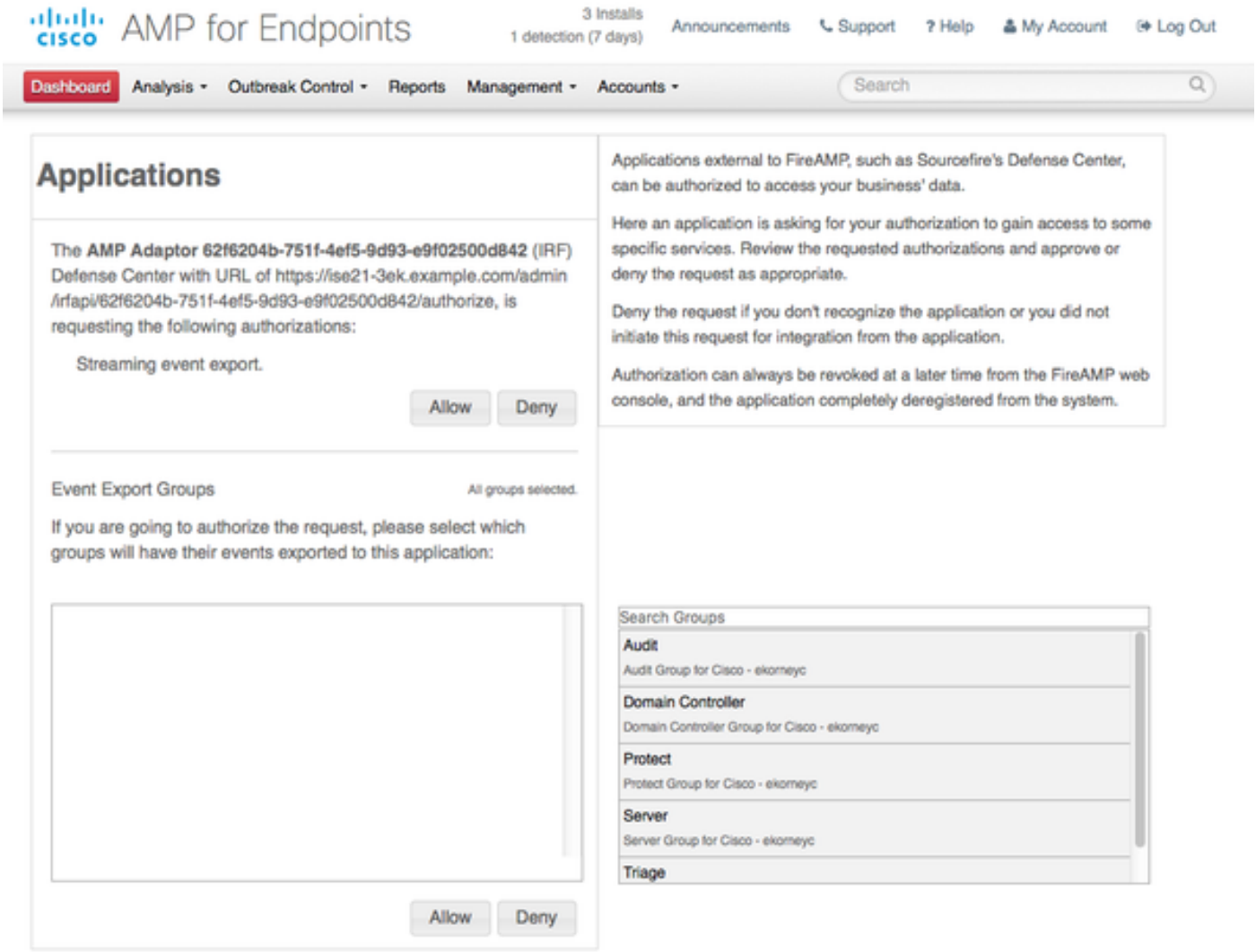
Selecteer **Cloud** en klik op **Volgende**



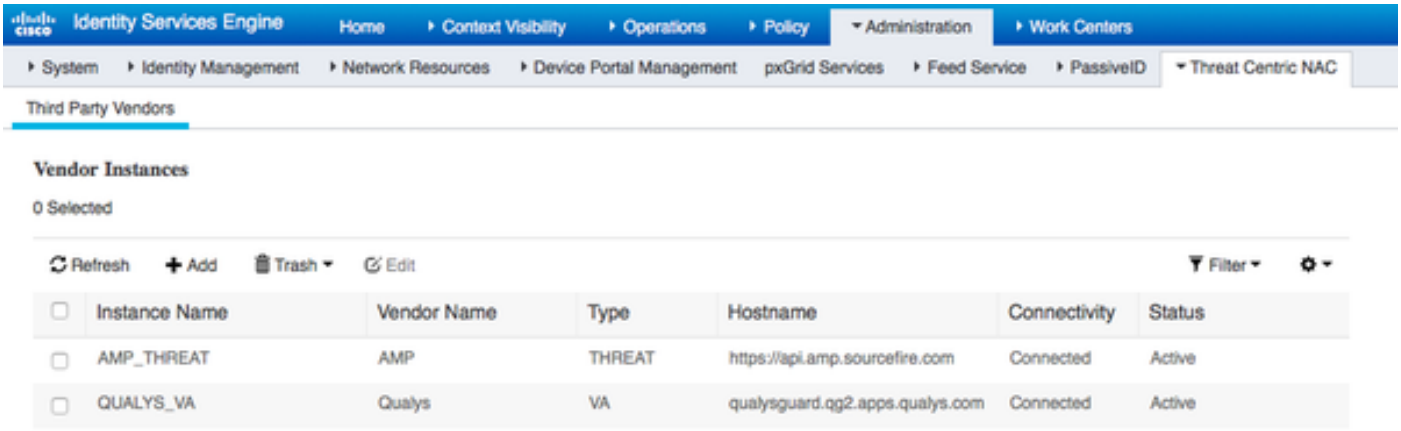
Klik op de koppeling FirePOWER en loggen in als beheerder van FireAMP.



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



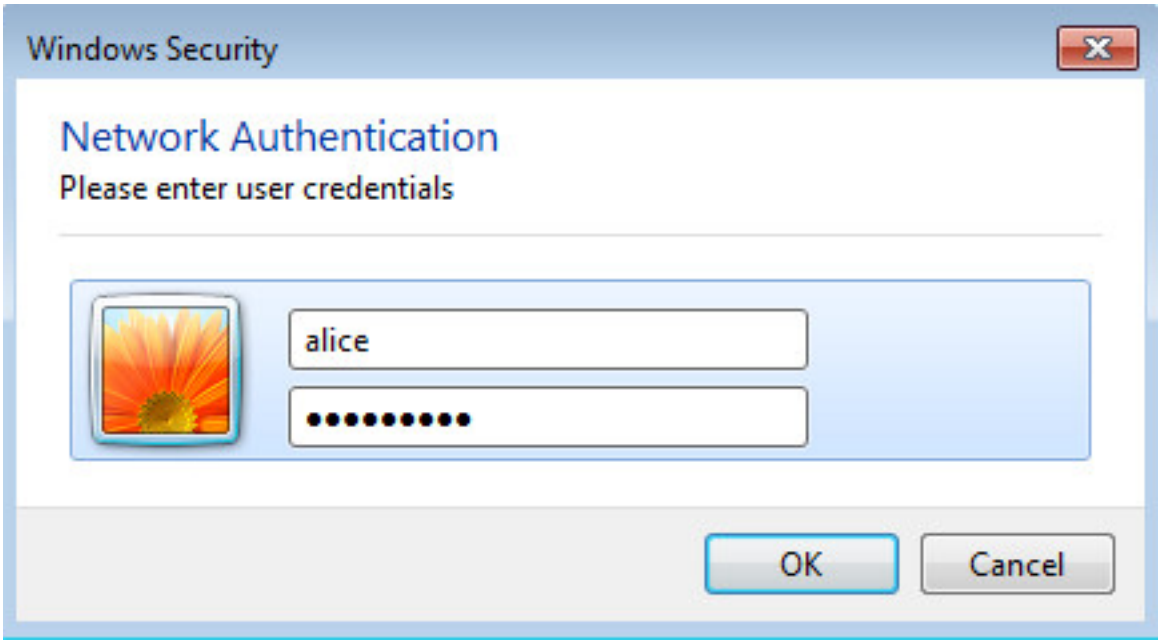
Selecteer de gebeurtenissen (bijvoorbeeld verdachte download, verbinding met verdachte domein, uitgevoerde malware, java-compromis) die u wilt controleren. De samenvatting van de configuratie van de adapterinstantie wordt weergegeven in de summiere pagina van de configuratie. Adapter-instantie overschakelt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



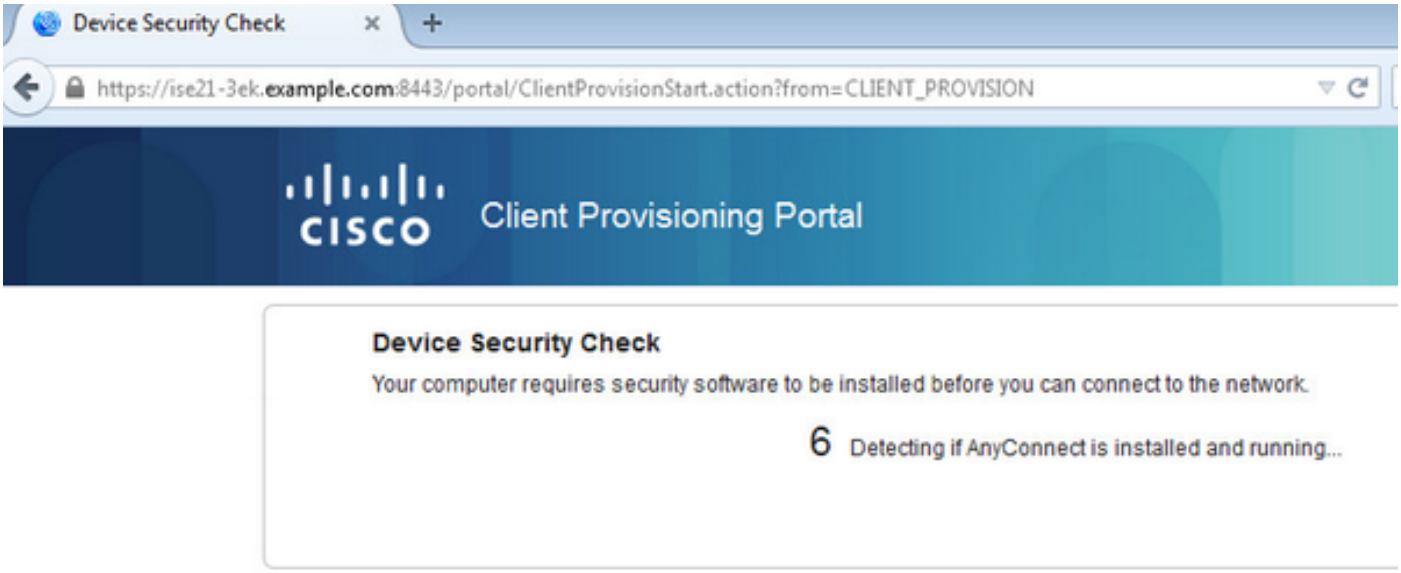
Verifiëren

Endpoint

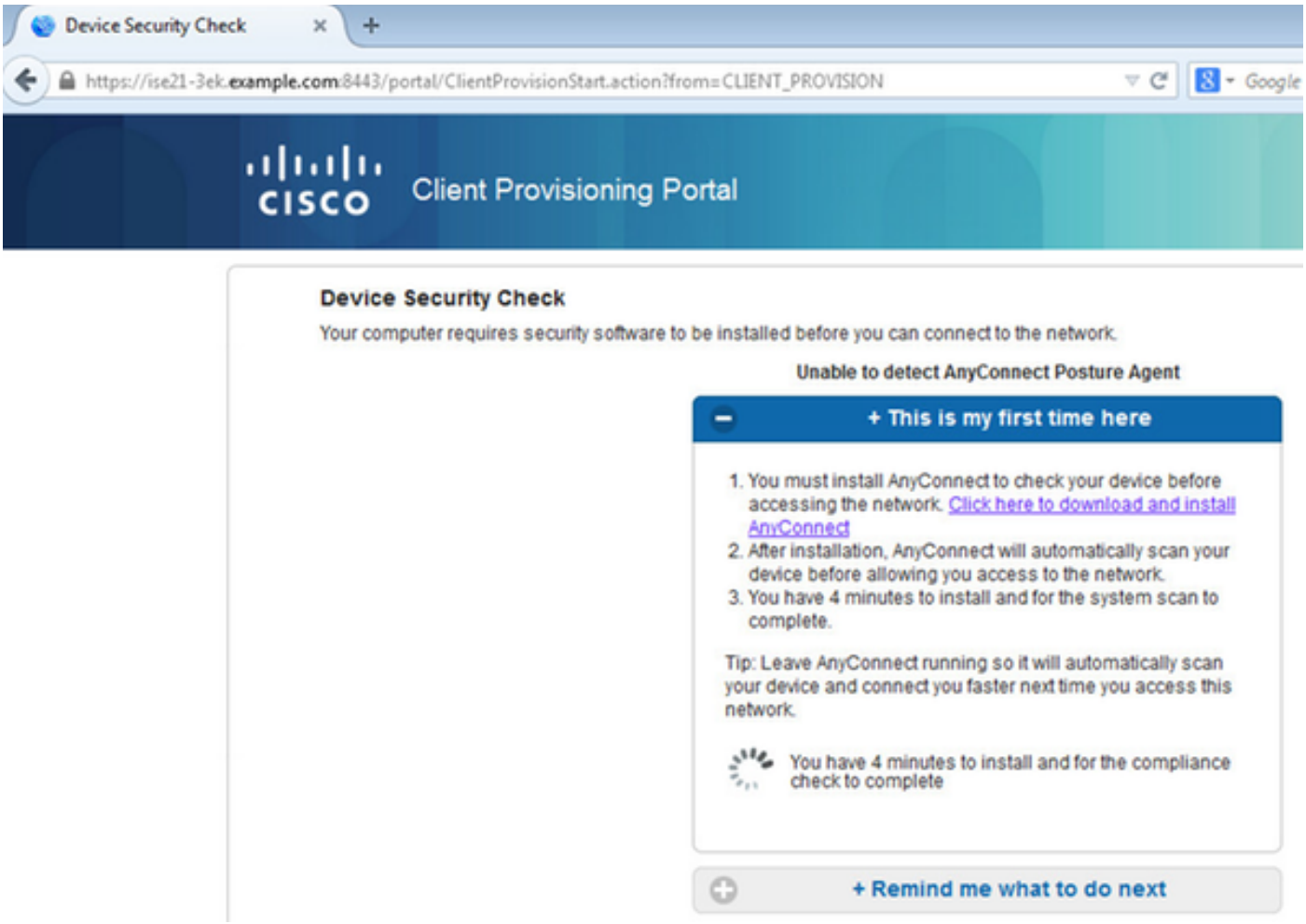
Verbinding aan een draadloos netwerk via PEAP (MSCHAPv2).



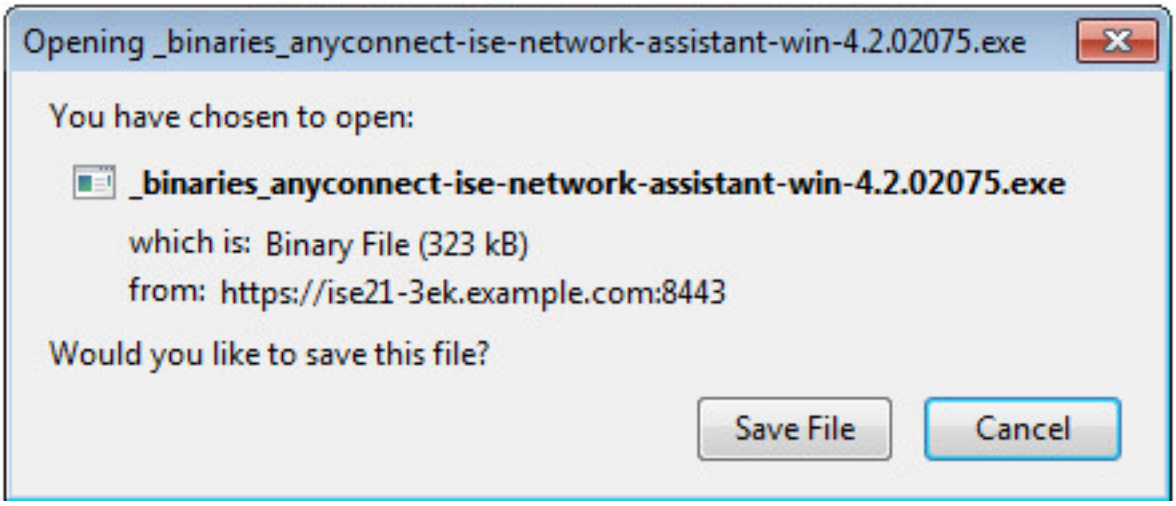
Zodra deze is aangesloten, wordt er verwezen naar Client Provisioning Portal.



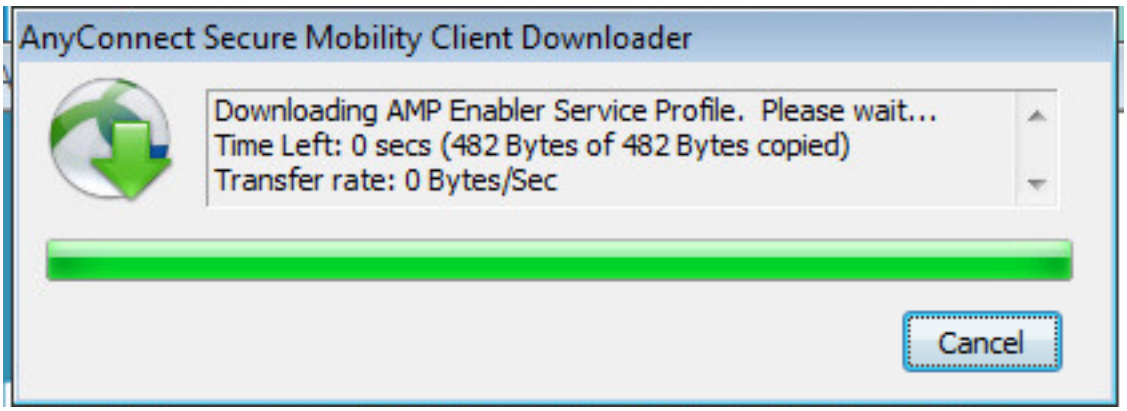
Aangezien er niets op de clientmachine is geïnstalleerd, vraagt ISE om een AnyConnect-client.

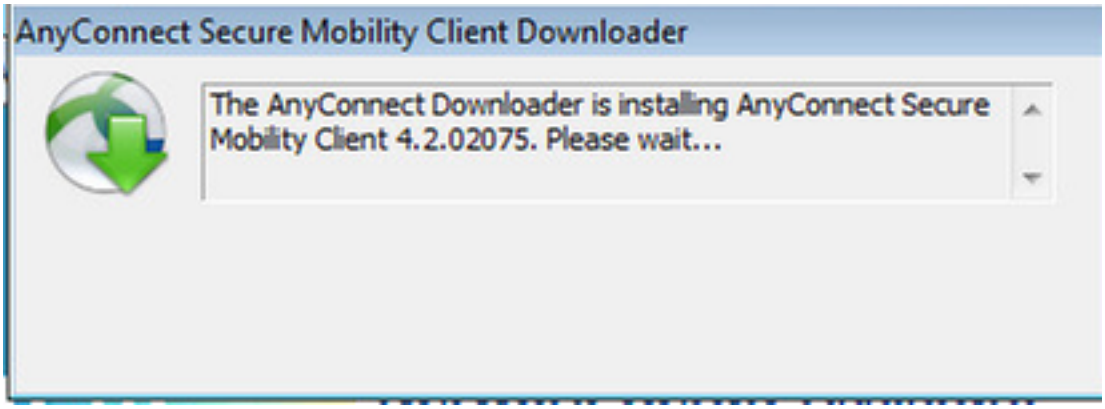


Network Setup Assistant-toepassing (NSA) dient te worden gedownload en te starten vanaf een clientmachine.

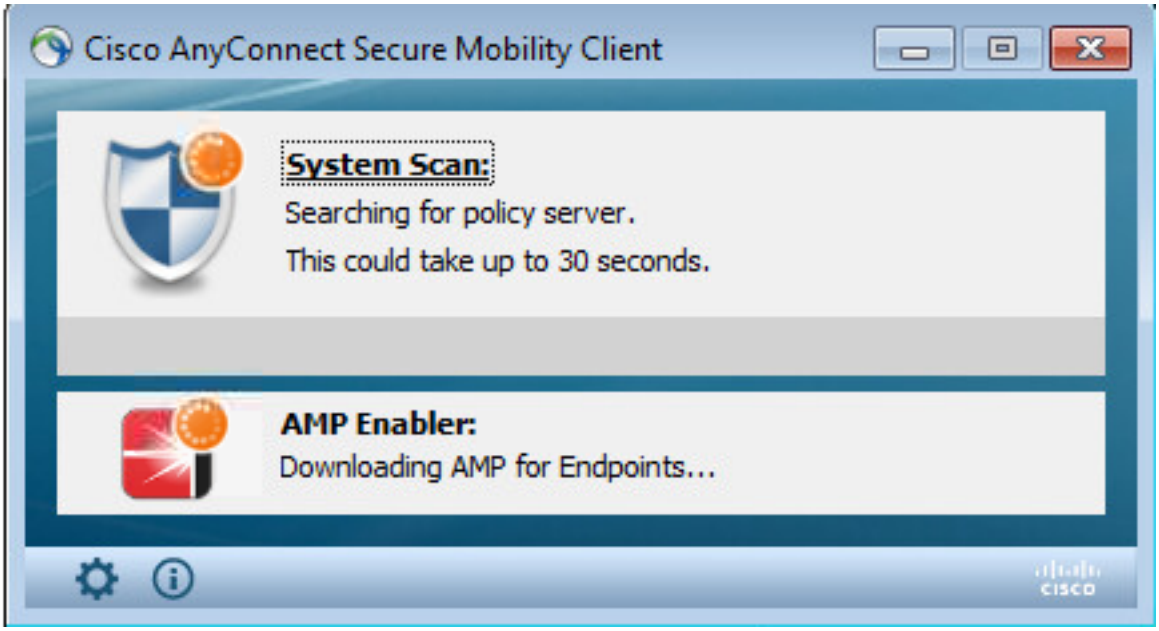


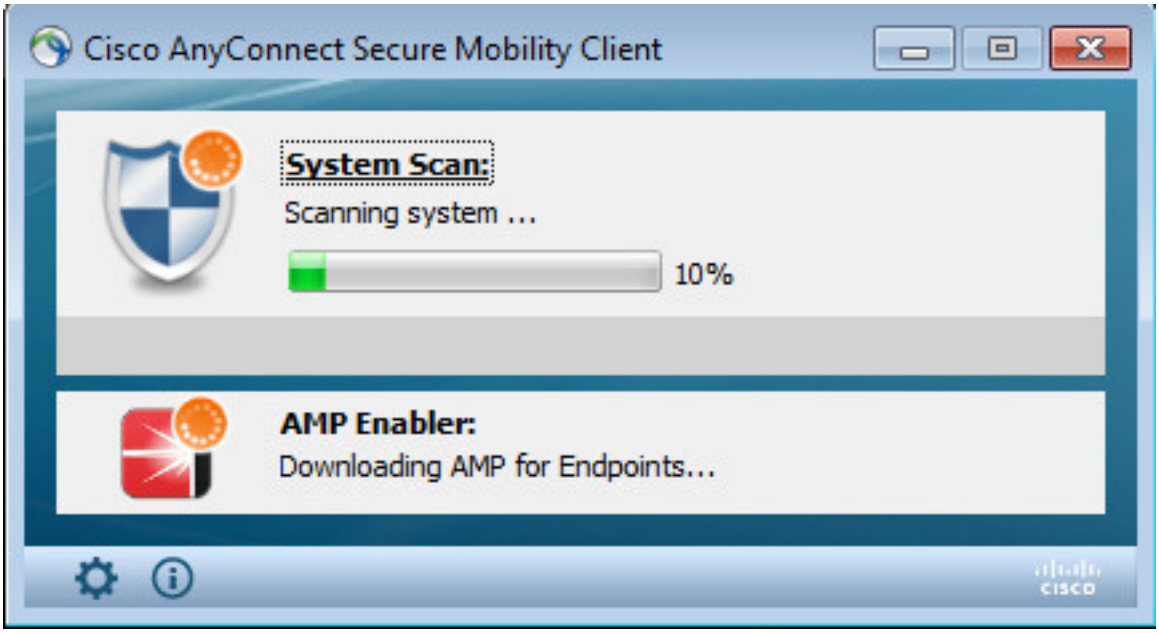
NSA zorgt voor het installeren van vereiste componenten en profielen.



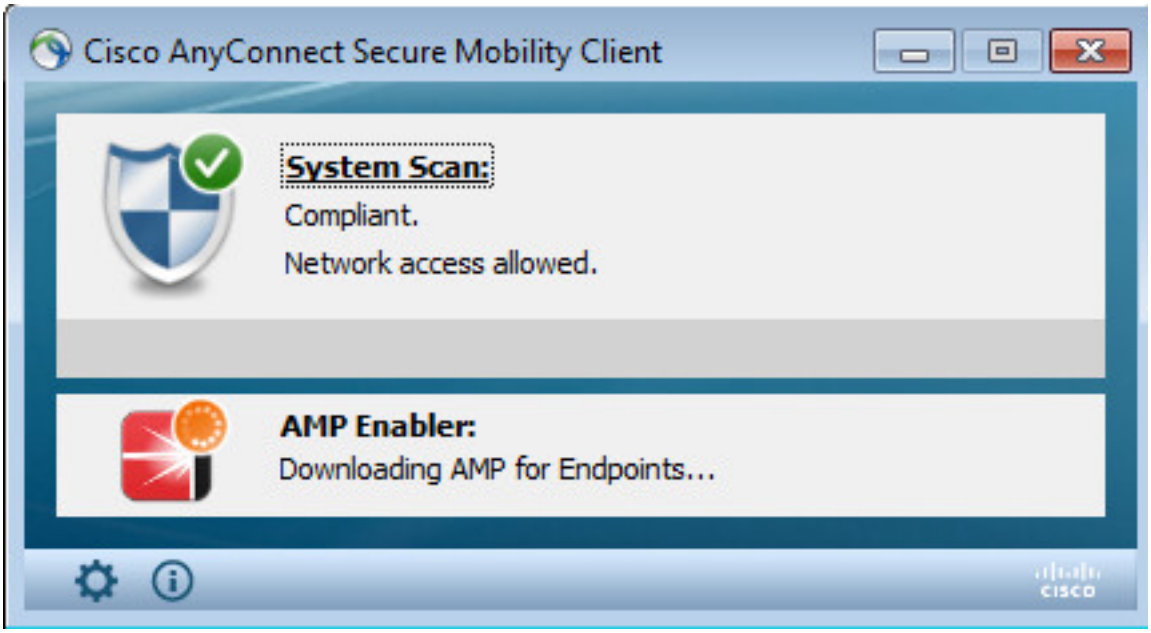


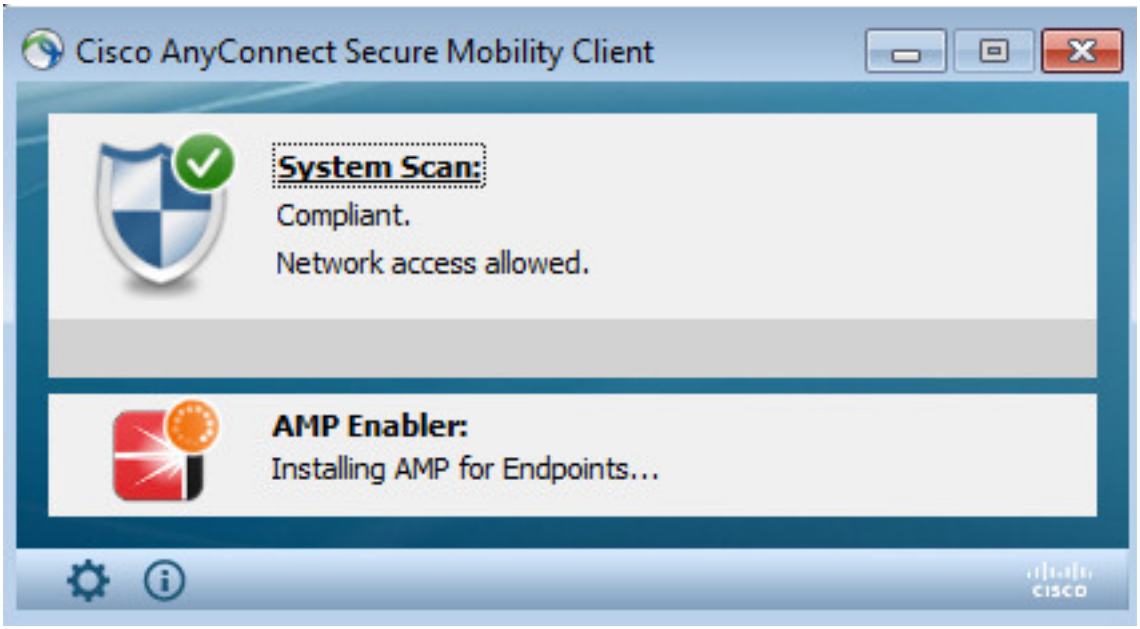
Nadat de installatie is voltooid, controleert de AnyConnect Posture-module de naleving van de voorschriften.

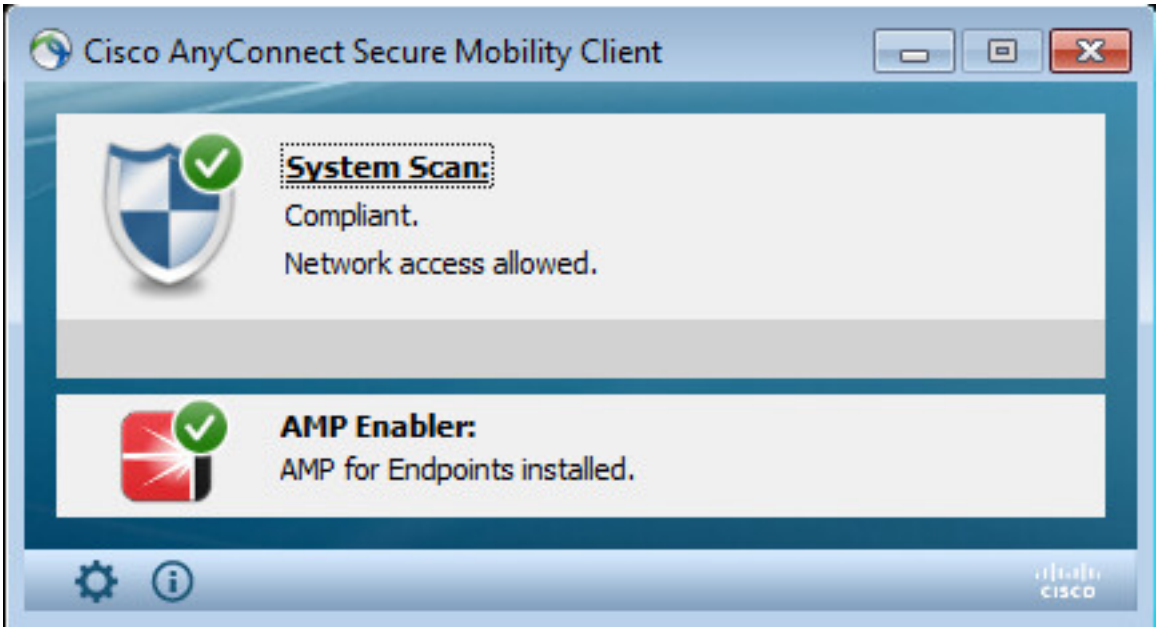




Aangezien volledige toegang wordt gegeven, als het eindpunt in overeenstemming is, wordt AMP gedownload en geïnstalleerd van de webserver die eerder in het AMP Profile is gespecificeerd.

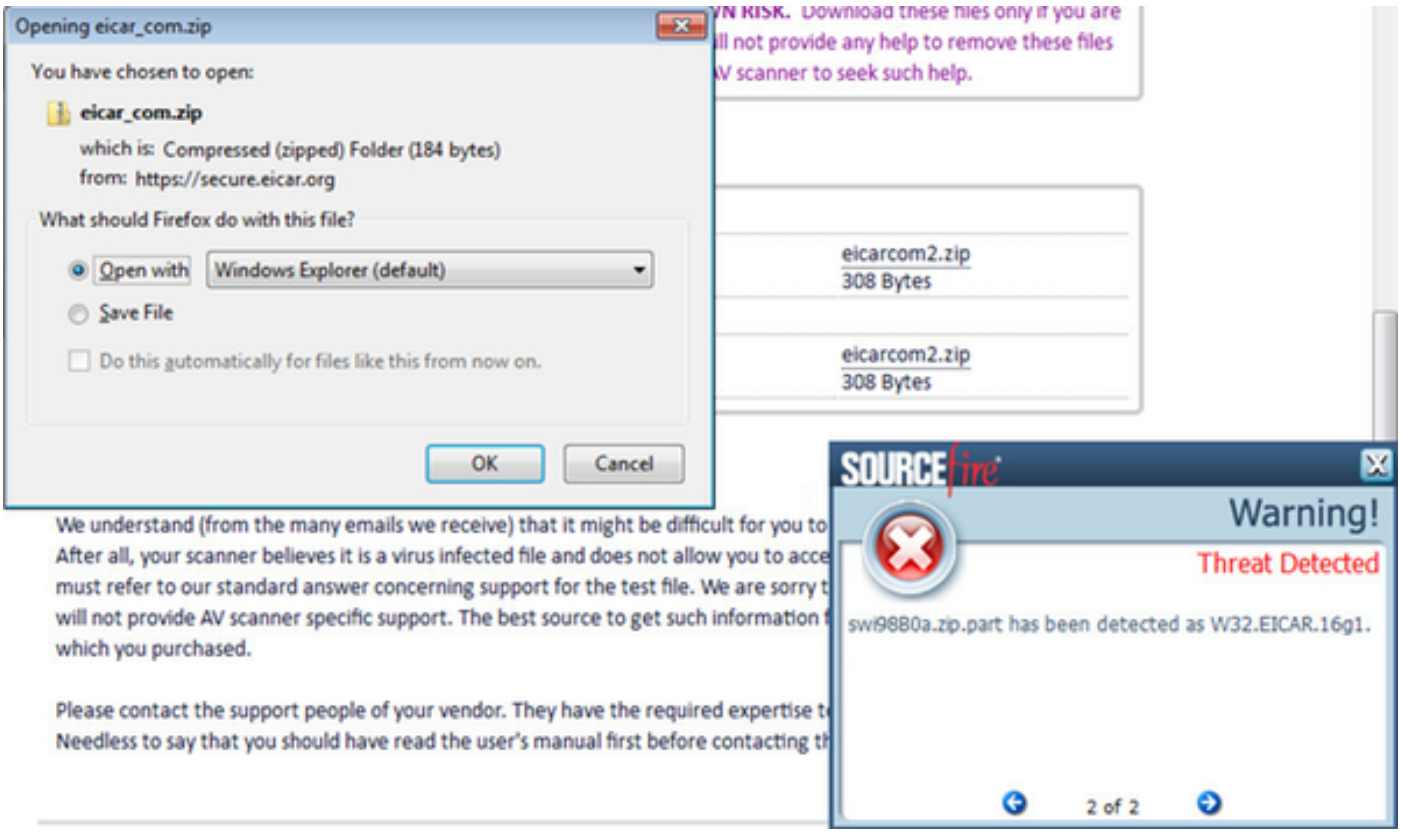






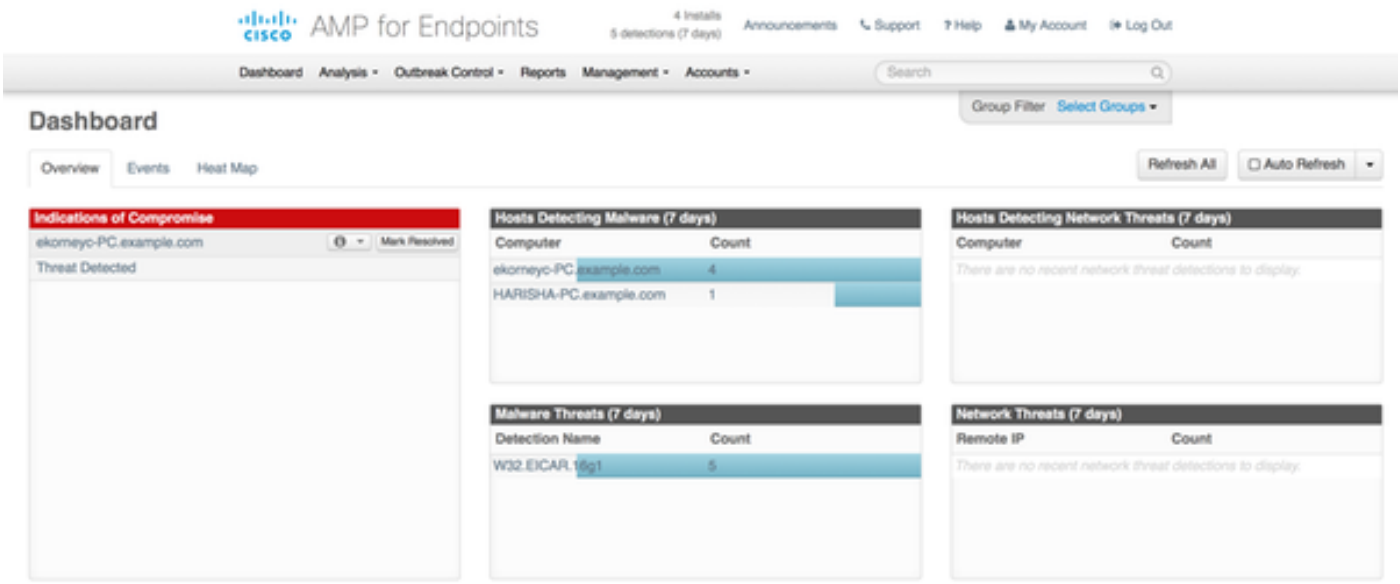
AMP-connector verschijnt.

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

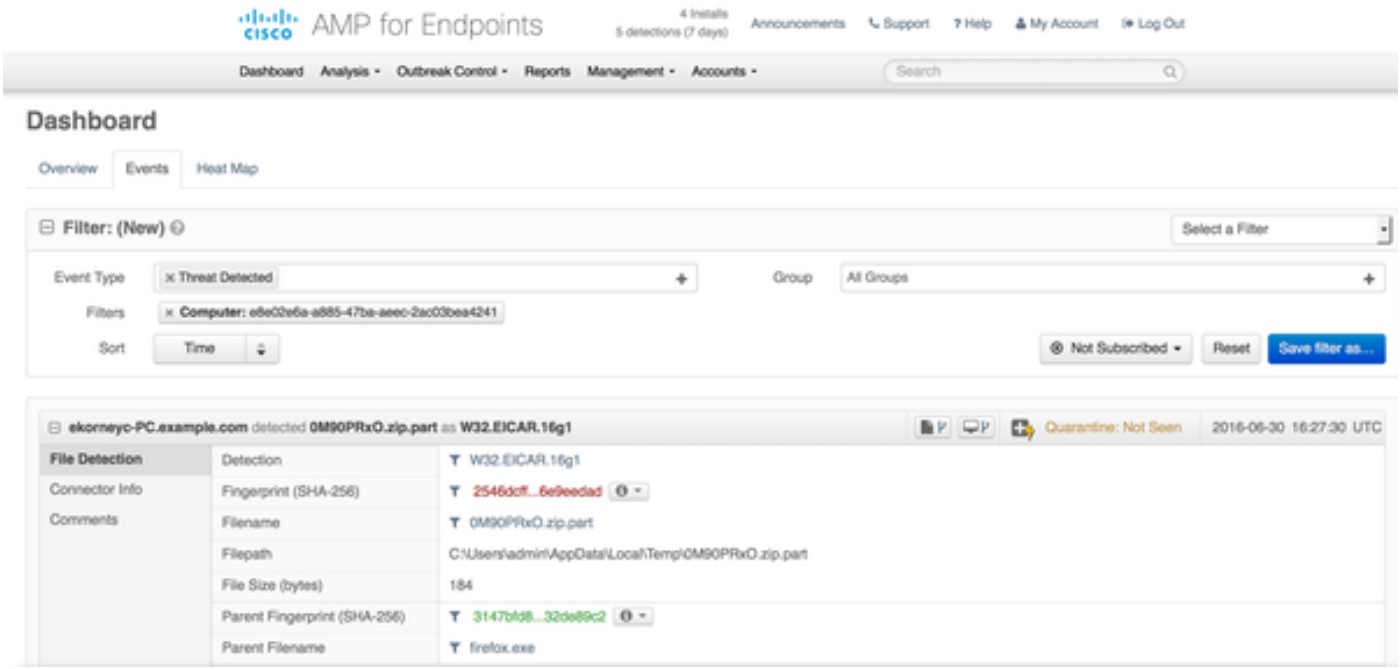


AMP-cloud

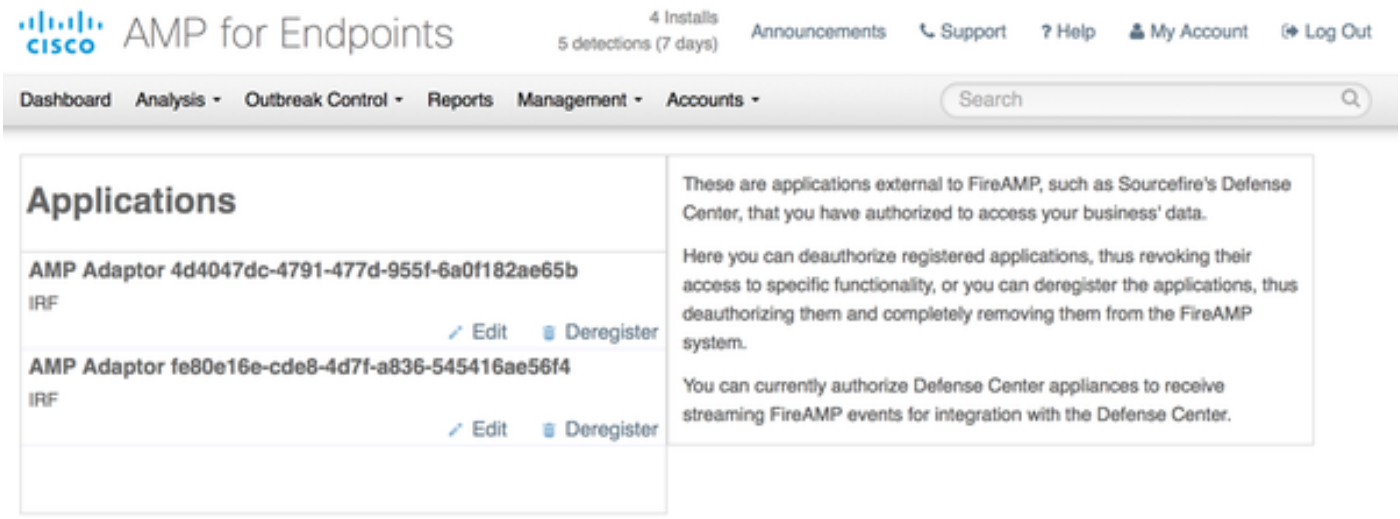
Om de details van het bedreigingsdashboard van de AMP cloud te controleren kan worden gebruikt.



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

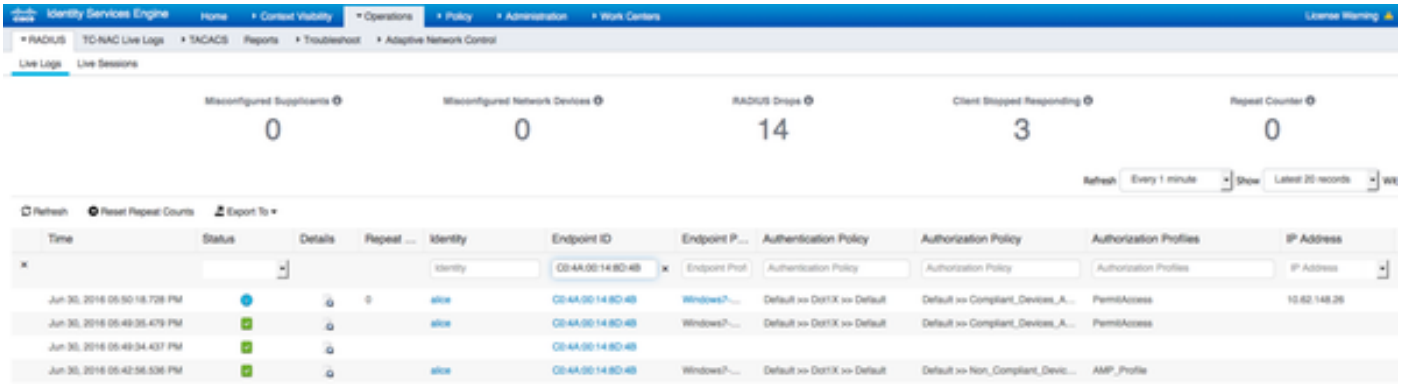


Om geval van ISE te bekijken of te registreren kunt u naar accounts > Toepassingen navigeren

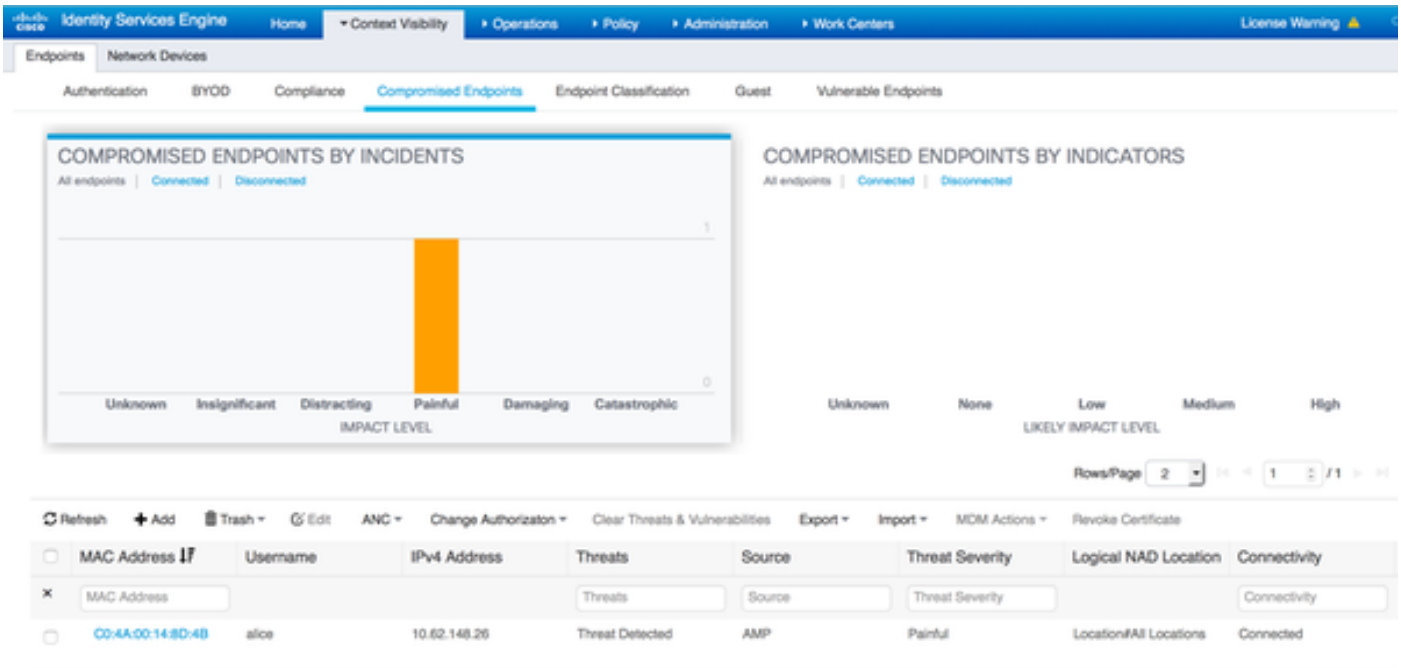


ISE

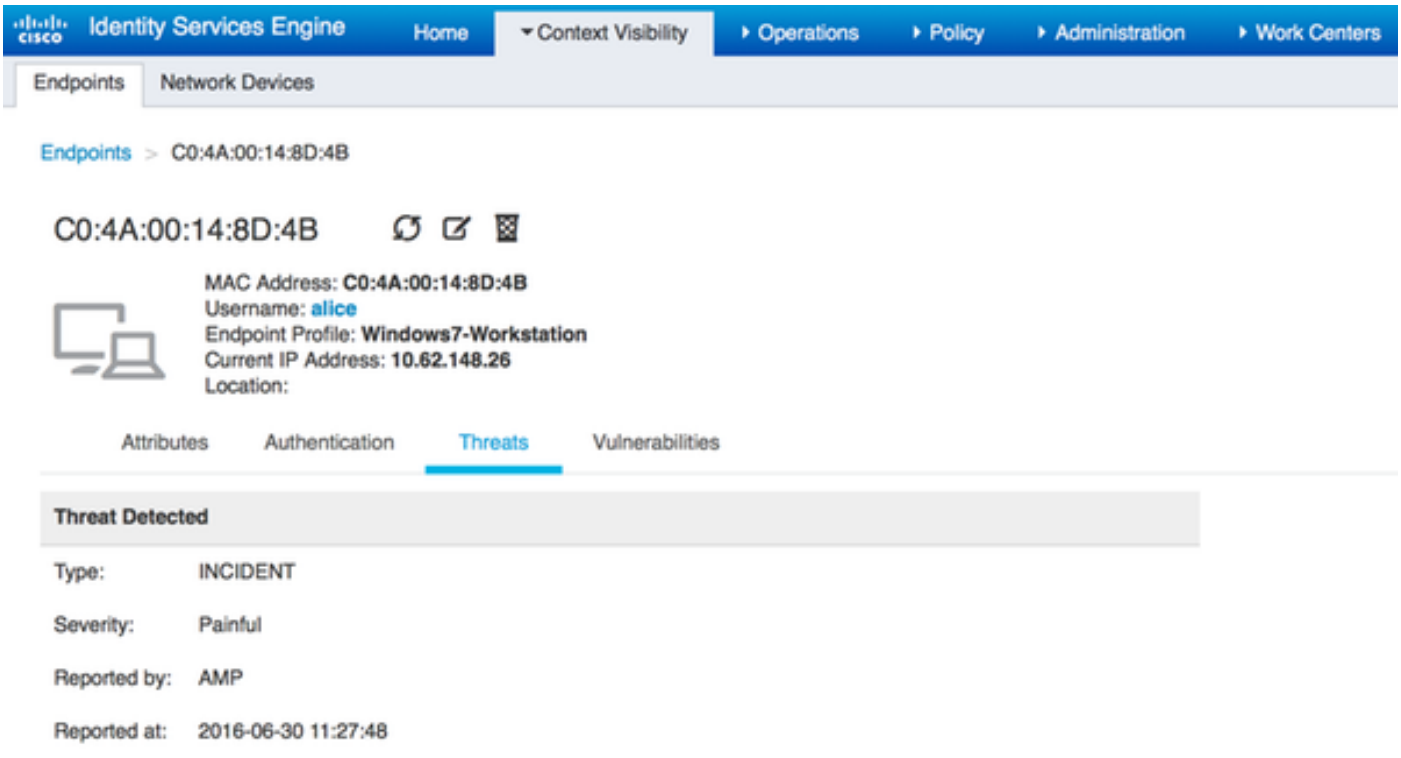
Op ISE zelf wordt een regelmatige posteringsstroom gezien, wordt eerst omleiding uitgevoerd om de netwerkconformiteit te controleren. Zodra het eindpunt in overeenstemming is, wordt CoA Reauth verzonden en wordt het nieuwe profiel met PermitAccess toegewezen.



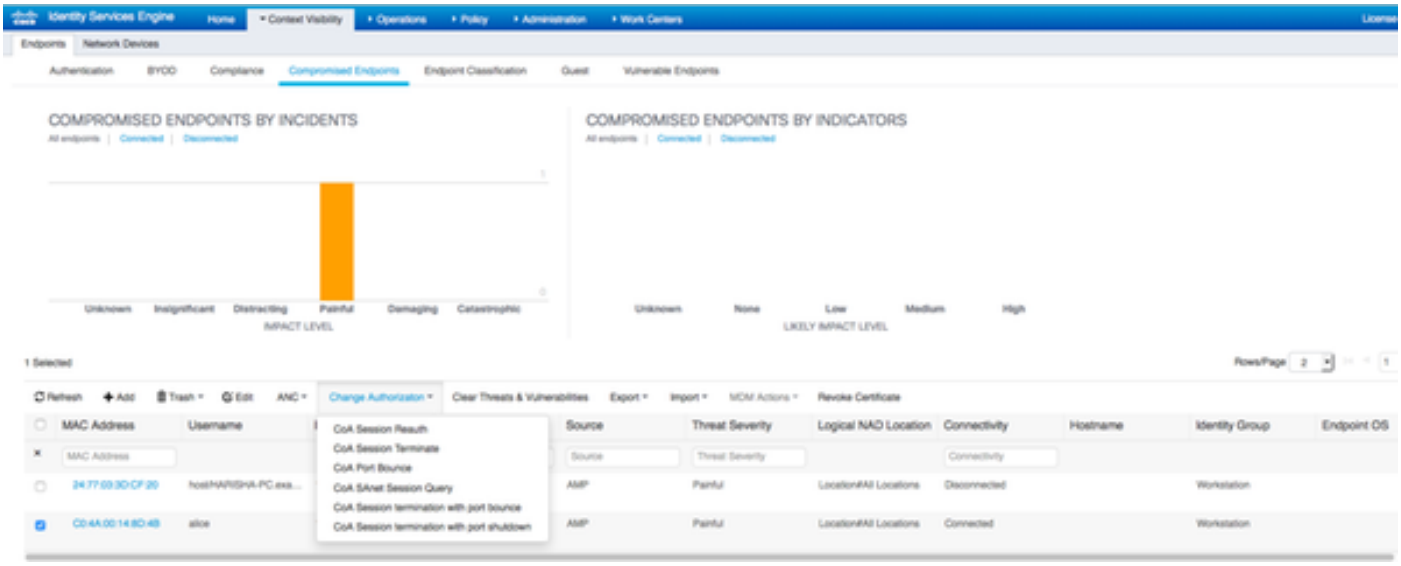
Om de gedetecteerde bedreigingen te bekijken kunt u navigeren naar Context Visibility and > Endpoints > Combeloofde endpoints



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



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.



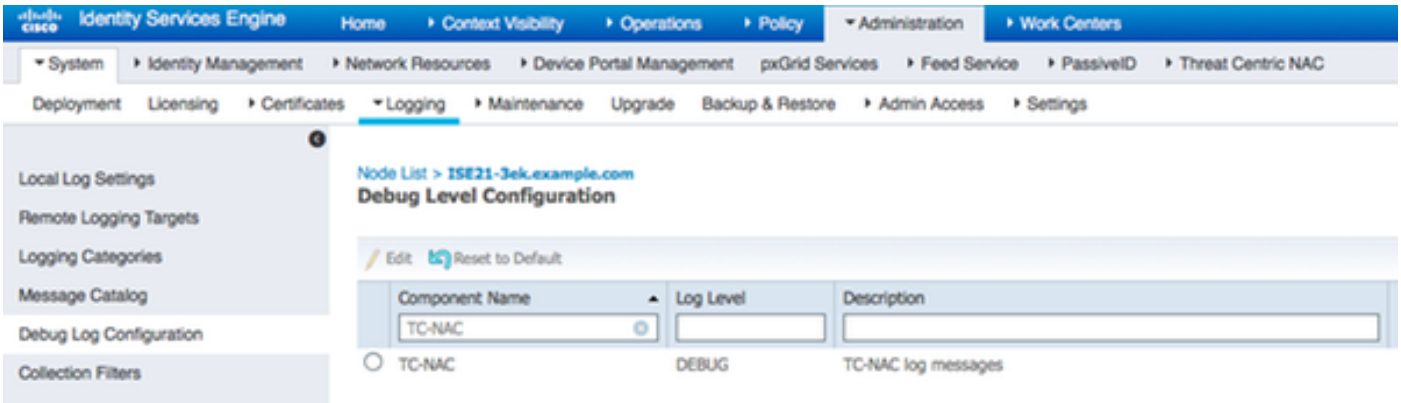
Als CoA Session Terminate is geselecteerd, verstuurt ISE CoA Disconnect en verliest client toegang tot het netwerk.

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**



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**": [<"incident":
{"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-encodering=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, prioritair-
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=valse, 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, prioritair-
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=Ppijnlijk},
tijdstempel=1467304068599, seller=AMP, title=Threat Detected}