

2.2 Clientprovisioning en -toepassing configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Configuraties](#)

[Sectie 1: Clientprovisie configureren](#)

[Stap 1. Upload AnyConnect](#)

[Stap 2. Download AnyConnect-nalevingsmodule](#)

[Stap 3. Postprofiel maken](#)

[Stap 4. Maak AnyConnect-configuratie](#)

[Stap 5. Het beleid voor clientprovisioning configureren](#)

[Stap 6. Maak een vergunningsprofiel voor CP](#)

[Stap 7. Instellen van het vergunningsbeleid](#)

[Sectie 2: Postvorm instellen](#)

[Stap 1: Postgegevens bijwerken](#)

[Stap 2. Maak een toepassingsvoorwaarde](#)

[Stap 3. Vereiste vertraging maken](#)

[Stap 4. Postbeleid maken](#)

[Stap 5 \(optioneel\). Verandering van continue bewaking](#)

[Stap 6 \(optioneel\). Toepassingsnaleving maken](#)

[Verifiëren](#)

[LiveLogs](#)

[Endpoint](#)

[Elementen van het postbeleid](#)

[Rapporten](#)

[Postbeoordeling per conditionering](#)

[Postbeoordeling door eindpunt](#)

[Problemen oplossen](#)

[Van ISE](#)

[Van AnyConnect](#)

[Gemeenschappelijke kwesties](#)

[AnyConnect kan ISE niet bereiken](#)

[ISE werpt "ongeldige" fout af bij het maken van App-naleving vanuit EP-weergave](#)

Inleiding

Dit document beschrijft hoe u toepassingen die op endpoints zijn geïnstalleerd kunt configureren

en oplossen. Toepassingszichtbaarheid op Identity Services Engine (ISE) 2.2.

Toepassingszichtbaarheid geeft u de mogelijkheid om toepassingen te controleren die op endpoints zijn geïnstalleerd, beleid te maken op basis van die informatie en toepassingen tijdens postcontroles te doden of te verwijderen als ze aan bepaalde voorwaarden voldoen. AnyConnect stuurt regelmatig informatie naar ISE met een lijst van geïnstalleerde/actieve toepassingen en processen. AnyConnect kan informatie over alle toepassingen en toepassingen van bepaalde categorieën verzamelen (browsers, encryptie, enz.).

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- Cisco Identity Services Engine
- Clientprovisioning
- ISE Posture

Gebruikte componenten

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

- Cisco Identity Services Engine versie 2.2.0.470
- Cisco AnyConnect 4.4.00243
- AnyConnect-nalevingsmodule 4.2.468.0
- Windows 7 Service Pack 1

Configureren

Configuraties

Sectie 1: Clientprovisie configureren

Stap 1. Upload AnyConnect

1. Navigeer naar **Beleidselementen > Resultaten > Clientprovisioning > Resultaten** op ISE. Klik op **Add > Agent resources van lokale disk**:

2. Selecteer **Category** als Cisco Provided Packages en **Kies Bestand** (AnyConnect-pakket):

Agent Resources From Local Disk

Category ⓘ

anyconnect-w...ploy-k9.pkg

▼ AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.4.24...	AnyConnectDesktopWindows	4.4.243.0	AnyConnect Secure Mobility Clie...

Klik op **Inzenden** om wijzigingen op te slaan.

U dient te worden gevraagd de bedragen van het geüploade pakket te controleren. Vergelijk ze met controlemiddelen die op een website van Cisco worden verstrekt om te verzekeren dat het pakket niet gecorrumped is.

Stap 2. Download AnyConnect-nalevingsmodule

Op een Resultaten-pagina van Client Provisioning klikt u op **Add > Agent resources van Cisco-site**, zodat een venster met beschikbare modules wordt geopend. Selecteer de gewenste **AnyConnect-nalevingsmodule** voor Windows en klik op **Opslaan**.

Als u geen internetverbinding hebt op uw ISE, kunt u de nieuwste nalevingsmodule van cisco.com downloaden en op dezelfde manier naar uw ISE uploaden als AnyConnect-pakket.

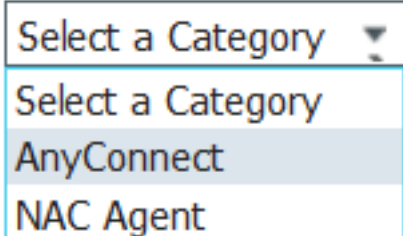
Als u een proxy in uw netwerk hebt, moet u deze configureren op **Beheer > System >**

Instellingen > proxy-pagina.

Stap 3. Postprofiel maken

Op het Resultaten op de pagina Clientprovisioning klik op **Add > NAC Agent of AnyConnect Posture Profile** en selecteer **AnyConnect** vanuit Posture Agent Profile-instellingen:

Posture Agent Profile Settings

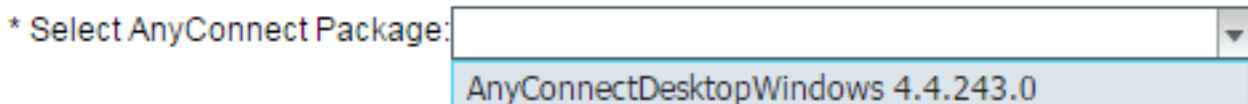


Select a Category ▼
Select a Category
AnyConnect
NAC Agent

Geef het profiel een naam en vul de vereiste velden in. Klik op **Inzenden** om profiel op te slaan.

Stap 4. Maak AnyConnect-configuratie

Klik op een Resultaten-pagina van Client Provisioning op **Add > AnyConnect Configuration** en selecteer het pakket dat in Stap 1 is geüpload:



* Select AnyConnect Package: []
AnyConnectDesktopWindows 4.4.243.0

Extra opties moeten worden geladen. Vul alle vereiste velden in en klik op **Indienen** om wijzigingen op te slaan:

* Select AnyConnect Package: AnyConnectDesktopWindows 4.4.243.0
* Configuration Name: AnyConnect Configuration
Description:
DescriptionValue
* Compliance Module: AnyConnectComplianceModuleWindows 4.2.468.0

AnyConnect Module Selection

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Umbrella Roaming Security
- Start Before Logon
- Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AnyConnect Posture
VPN
Network Access Manager
Web Security
AMP Enabler
Network Visibility
Umbrella Roaming Security
Customer Feedback

Customization Bundle
Localization Bundle

Configuratiennaam - naam van de configuratie. Dit wordt gebruikt in het beleid voor clientprovisioning (volgende stap).

Nalevingsmodule - selecte nalevingsmodule die in stap 2 is gedownload.

ISE Posture - selecteer AnyConnect Posture Profile dat in Stap 3 is gemaakt.

Stap 5. Het beleid voor clientprovisioning configureren

Navigeer naar **beleid > Clientprovisioning**. Maakt nieuw beleid of bewerk een bestaand beleid voor Windows. Selecteer hiermee de optie AnyConnect Configuration:

Stap 6. Maak een vergunningsprofiel voor CP

Navigeer in **Beleidselementen > Resultaten > Resultaten > Vergunningsprofielen > autorisatieprofielen** en klik op **Toevoegen** om een nieuw profiel te maken. Configureer het voor omleiding naar clientprovisioningportal:

Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

ACL Value

Static IP/Host name/FQDN

Auto Smart Port

Advanced Attributes Settings

= - +

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ISE-REDIRECT
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=4cb1f740-e371-11e6-92ce-005056873bd0&action=cpp
```

Klik op **Inzenden** om het profiel op te slaan.

Houd in gedachten dat redirect-ACL (in dit voorbeeld **wordt** genoemd **ISE-REDIRECT**) op

NAD (Network Access Devices) moet worden gemaakt om juiste omleiding te hebben. Basis omgekeerde ACL moet geen verkeer van en naar ISE PSN-knooppunten, DNS en DHCP onderscheppen. En moet HTTP- en HTTPS-verkeer omleiden. In deze documenten zijn voorbeelden van ACL's te vinden: [Central-webverificatie op het WLC- en ISE-configuratievoorbeeld](#) en [Central-webverificatie met een Configuratievoorbeeld van Switch- en Identity Services Engine](#)

Stap 7. Instellen van het vergunningsbeleid

Navigeren in **Policy > Authorization**, creëer 2 beleid met check of Posture status:

<input checked="" type="checkbox"/>	POSTURED	if Session:PostureStatus EQUALS Compliant	then PermitAccess
<input checked="" type="checkbox"/>	CPP_REDIRECT	if Session:PostureStatus NOT_EQUALS Compliant	then CPP_REDIRECT

Als op een dergelijke configuratie geen AnyConnect is geïnstalleerd of nog niet is voltooid, wordt de configuratie opnieuw gericht op Client Provisioning Portal. De eindgebruiker kan AnyConnect van ISE installeren en AnyConnect kan ISE detecteren en de houding controleren.

Klik op **Opslaan**.

Sectie 2: Postvorm instellen

Stap 1: Postgegevens bijwerken

Navigeer naar **Administratie > Instellingen > Posture > Uploads** en klik op **Nu bijwerken** om Post bij te werken. Het bevat OPSWAT-kaarten en definities voor toepassingen en is vereist voor het maken van beleid.

Posture Updates

Web Offline

* Update Feed URL

Proxy Address

Proxy Port HH MM SS

Automatically check for updates starting from initial delay every hours ⓘ

Als u geen internetverbinding hebt op uw ISE, kunt u ook de nieuwste postupdates downloaden via <https://www.cisco.com/web/secure/pmbu/posture-offline.html> en vervolgens naar **Administratie > Systeem > Instellingen > Posture > Update** navigeren, **Offline** selecteren en naar gedownload bestand met postupdates selecteren. Klik op **Nu bijwerken** om het bestand te uploaden en postupdates te installeren.

Stap 2. Maak een toepassingsvoorwaarde

AnyConnect verzamelt informatie over geïnstalleerde toepassingen uitsluitend met 4.x (of hoger)

nalevingsmodule.

Met de versie van 3.x van de nalevingsmodule kunnen alleen procescontroles worden uitgevoerd (dit betekent dat AnyConnect-controles kunnen worden uitgevoerd als het gespecificeerde proces al dan niet wordt uitgevoerd).

In de **toepassingsfase** kunnen deze combinaties worden geconfigureerd:

- Geïnstalleerd + actief - AnyConnect verzamelt informatie over de momenteel actieve processen om informatie over de installatie te verzamelen
- Geïnstalleerd + niet actief - AnyConnect verzamelt alleen installatieinformatie

Met deze **bepaling** kunnen worden gekozen: **Alles**, **naam** en **categorie**:

- Als **Alles** is geselecteerd, probeert AnyConnect informatie te verzamelen over alle geïnstalleerde toepassingen
- Als de **naam** is geselecteerd, kan de specifieke toepassing voor het beleid worden geselecteerd. Bijvoorbeeld:

Provision by

At least one category must be selected *

<input type="checkbox"/> Unclassified	<input type="checkbox"/> Data Loss Prevention	<input type="checkbox"/> Data Storage
<input type="checkbox"/> Browser	<input type="checkbox"/> Backup	<input type="checkbox"/> Patch Management
<input type="checkbox"/> Encryption	<input checked="" type="checkbox"/> Antiphishing	<input type="checkbox"/> VPN Client
<input type="checkbox"/> Anti-Malware	<input type="checkbox"/> Virtual Machine	<input type="checkbox"/> Firewall
<input type="checkbox"/> Messenger	<input type="checkbox"/> Public File Sharing	<input type="checkbox"/> Health Agent

Vendor *

At least one product must be selected *

| Selected Rows/Page / 1 / 1 3 Total Rows

<input type="checkbox"/>	Product Name	Version
<input checked="" type="checkbox"/>	Anvi Smart Defender	1.x
<input type="checkbox"/>	Anvi Smart Defender	2.x
<input type="checkbox"/>	Anvi Smart Defender	ANY

- Als **Category** is geselecteerd, verzamelt AnyConnect informatie over alle toepassingen van een bepaalde categorie. Bijvoorbeeld:

Provision by

At least one category must be selected *

- | | | |
|--|---|---|
| <input type="checkbox"/> Unclassified | <input type="checkbox"/> Data Loss Prevention | <input type="checkbox"/> Data Storage |
| <input type="checkbox"/> Browser | <input type="checkbox"/> Backup | <input type="checkbox"/> Patch Management |
| <input type="checkbox"/> Encryption | <input type="checkbox"/> Antiphishing | <input type="checkbox"/> VPN Client |
| <input checked="" type="checkbox"/> Anti-Malware | <input type="checkbox"/> Virtual Machine | <input type="checkbox"/> Firewall |
| <input type="checkbox"/> Messenger | <input type="checkbox"/> Public File Sharing | <input type="checkbox"/> Health Agent |

Als u informatie wilt verzamelen over geïnstalleerde en toepassingen die actief zijn op **Policy > Policy Elementen > Voorwaarden > Posture > Application Condition**, klikt u op **Add** om nieuwe conditie te creëren en de vereiste velden zoals getoond te vullen:

[Application Condition > New](#)

Name *	<input type="text" value="Apps_Collection"/>
Description	<input type="text" value="Condition for all applications"/>
Operating System *	<input type="text" value="Windows All"/>
Compliance module	<input type="text" value="4.x or later"/>
Check By *	<input type="text" value="Application"/>
Application State *	<input checked="" type="checkbox"/> Installed <input checked="" type="checkbox"/> Running
Provision by	<input type="text" value="Everything"/>

Cancel

Submit

Stap 3. Vereiste vertraging maken

In **Policy > Policy Elementen > Resultaten > Posture > Requirements** creëren u nieuwe vereisten met gedefinieerde toepassingsvoorwaarden:

Name	Operating Systems	Compliance Module	Stealth Mode	Conditions	Remediation Actions
USB_Block	for Windows All	using 4.x or later	using Disabled	met if USB_Check	then USB_Block
Apps_collection	for Windows All	using 4.x or later	using Disabled	met if Apps_Collection	then Message Text Only
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	using Disabled	met if ANY_av_mac_inst	then Message Text Only
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using Disabled	met if ANY_av_mac_def	then AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using Disabled	met if ANY_as_mac_inst	then Message Text Only
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using Disabled	met if ANY_as_mac_def	then AnyASDefRemediationMac

Stap 4. Postbeleid maken

Om ISE en AnyConnect in staat te stellen informatie over toepassingen te verzamelen, moet in het Postbeleid een vereiste met een toepassingsvoorwaarde worden opgenomen. Postbeleid kan worden gecreëerd bij **Policy > Posture**. De vereiste kan worden ingesteld als **Audit**, indien u informatie wenst te verzamelen voor verder gebruik.

Posture Policy

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

Stap 5 (optioneel). Verandering van continue bewaking

Met ISE kunt u configureren hoe vaak AnyConnect updates over toepassingen naar ISE moet doorsturen. De standaardinstelling is dat het interval wordt ingesteld op 5 minuten en kan worden gewijzigd bij **Administratie > Instellingen > Post > Algemene instellingen**:

Posture General Settings

Remediation Timer Minutes *i*

Network Transition Delay Seconds *i*

Default Posture Status *i*

Automatically Close Login Success Screen After Seconds *i*

Continuous Monitoring Interval Minutes *i*

Acceptable Use Policy in Stealth Mode

Posture Lease

- Perform posture assessment every time a user connects to the network
- Perform posture assessment every Days *i*

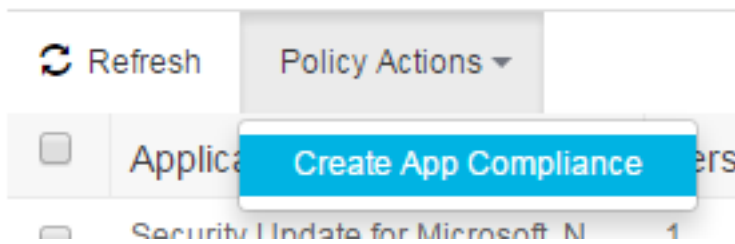
Stap 6 (optioneel). Toepassingsnaleving maken

Nadat gegevens vanuit het Endpoint zijn verzameld, kan de naleving van de app worden gecreëerd bij **Context Visibility > Endpoints > [ENDPOINT]**:

1. Selecteer een toepassing:

<input type="checkbox"/>	Windows Media Player	1.2.0.1001.23377	Microsoft Corporation	Unclassified	C:\Program Files\Win...
<input checked="" type="checkbox"/>	FileZilla	3.8.1.0	FileZilla Project	FileShare	C:\Program Files (x86)...
<input type="checkbox"/>	Security Update for Microsoft N...	2	Microsoft Corporation	Unclassified	

2. Klik op **Beleidsacties > Naleving van app maken**



3. Vul de velden in een pop-upvenster op:

Create Posture Application Compliance

Application Names *

Version 3.8.1.0 ANY

Compliance Name *

Description

Operating System * MacOSX Windows

Compliance module

Condition

Application State * Installed Running

Remediation

Remediation Type

Interval *

Retry Count *

Remediation Option * Uninstall Kill Process

Note: By default the above Condition & Remediation would be linked as a requirement.

4. Klik op **Opslaan beleid**. Deze items moeten worden aangemaakt: Toepassingsvoorwaarden voor uitstelHandeling voor uitstel van toepassingPostvereistenPostbeleid

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

LiveLogs

In RADIUS LiveLogs ziet de stroom eruit als een normale postuur: **Verificatie + omleiding naar provisioningportal > Wijzigen van autorisatie (CoA) > Overeenkomstige houding van conforme posterijen.**

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Posture St...	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address
x				Identity	Endpoint ID	Posture Status	Endpoint Profil	Authentication	Authorization F	Authorization F	IP Address
Jan 04, 2017 07:59:07.655 PM			1	cisco	C0-4A:00:15:75:C8	Compliant	Microsoft-W...	Default >> D...	Default >> p...	PermitAccess	10.62.148.162
Jan 04, 2017 07:19:16.732 PM				cisco	C0-4A:00:15:75:C8	Compliant	Microsoft-W...	Default >> D...	Default >> p...	PermitAccess	
Jan 04, 2017 07:19:16.097 PM					C0-4A:00:15:75:C8	Compliant					
Jan 04, 2017 07:19:02.205 PM				cisco	C0-4A:00:15:75:C8	Pending	Microsoft-W...	Default >> D...	Default >> C...	CPP	

Endpoint

Na clientprovisioning (als AnyConnect niet eerder was voorzien) en voortdurende bewaking van de configuratie van interfaces, kan het proces van gegevensverzameling worden geverifieerd bij **Context Visibility and > Endpoints**. Klik op het adres van MAC van het eindpunt, zou de pagina van het eindpunt moeten openen. Deze informatie bevat informatie over toepassingen die op het eindpunt zelf zijn geïnstalleerd:

Refresh Policy Actions Filter ▼

Application Name	Version	Vendor	Running process	Category	Install Path
<input type="checkbox"/> Security Update for Microsoft .N...	1	Microsoft Corporation		Unclassified	
<input type="checkbox"/> Security Update for Microsoft .N...	1	Microsoft Corporation		Unclassified	
<input type="checkbox"/> Microsoft .NET Framework 4.6.1	4.6.01005	Microsoft Corporation		Unclassified	C:\Windows\Microsoft...
<input type="checkbox"/> Google Update Helper	1.3.24.15	Google Inc.		Unclassified	
<input type="checkbox"/> Windows Update Agent	7.6.7601.19161	Microsoft Corporation		PatchManagement	C:\Windows\System32\
<input type="checkbox"/> Cisco AnyConnect ISE Complia...	4.2.468.0	Cisco Systems, Inc		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> DAEMON Tools Lite	4.49.1.0356	Disc Soft Ltd		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Tlpad32 Standalone Edition (re...	0.0			Unclassified	
<input type="checkbox"/> Security Update for Microsoft .N...	1	Microsoft Corporation		Unclassified	
<input type="checkbox"/> VMware Tools	9.4.15.2827462	VMware, Inc.	2	Unclassified	C:\Program Files\VMw...
<input type="checkbox"/> BitLocker Drive Encryption	6.1.7600.16385	Microsoft Corporation		DiskEncryption	C:\Windows\System32\
<input type="checkbox"/> Cisco AnyConnect Diagnostics ...	4.4.00209	Cisco Systems, Inc.		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Cisco AnyConnect Secure Mobi...	4.4.00209	Cisco Systems, Inc.	5	Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Java Auto Updater	2.8.91.15	Oracle Corporation		Unclassified	
<input type="checkbox"/> Mozilla Firefox	47.0.2	Mozilla Corporation		AntiPhishing.Browser	C:\Program Files (x86)...
<input type="checkbox"/> Microsoft Visual C++ 2008 Redi...	9.0.30729.4148	Microsoft Corporation		Unclassified	
<input type="checkbox"/> Java 8 Update 91	8.0.910.15	Oracle Corporation		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Google Chrome	55.0.2883.87	Google Inc.		AntiPhishing.Browser	C:\Program Files (x86)...
<input type="checkbox"/> Cisco AnyConnect Profile Editor	4.1.08005	Cisco Systems, Inc.		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Java	8.0.910.15	Oracle Corporation		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Internet Explorer	11.0.9600.18524	Microsoft Corporation		AntiPhishing.Browser	C:\Program Files\Inter...
<input type="checkbox"/> Wireshark	1.10.7	The Wireshark developer comm...		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Windows Backup and Restore	6.1.7600.16385	Microsoft Corporation		BackupClient	C:\Windows\System32\
<input type="checkbox"/> Windows Media Player	12.0.7601.23517	Microsoft Corporation	1	Unclassified	C:\Program Files\Wind...
<input type="checkbox"/> FileZilla	3.8.1.0	FileZilla Project		FileShare	C:\Program Files (x86)...
<input type="checkbox"/> Security Update for Microsoft .N...	2	Microsoft Corporation		Unclassified	
<input type="checkbox"/> Java 7 Update 79	7.0.790	Oracle		Unclassified	C:\Program Files (x86)...

Vanwege [CSCve82743](#) moet u het eindpunt twee keer benaderen en op Vernieuwen klikken om de tabel van toepassingen weer te geven.

Elementen van het postbeleid

Deze elementen moeten met de optie **App-naleving maken** worden gemaakt:

- Toepassingsvoorwaarden voor uitstel
- Handeling voor uitstel van toepassing
- Postvereisten
- Postbeleid

Elk van deze kan worden geverifieerd door ISE GUI. **De voorwaarden** bevinden zich op **Policy > Policy Elementen > Voorwaarden > Posture > Application Condition**:

Application Condition

Rows/Page 25 1 / 1 Go 11 Total Rows

<input type="checkbox"/>	Name	Description	Application State	Compliance module	Categories	Check
<input type="checkbox"/>	Apps_Collection		Installed	4.x or later	Anti-Malware	APPLIC
<input type="checkbox"/>	FileZilla-Uninstall		Installed	4.x or later	Public File Sharing	APPLIC
<input type="checkbox"/>	Notepadplus		Installed and Running	4.x or later	Unclassified	APPLIC

Herschikkingen zijn te vinden op **Policy > Policy Elementen > Resultaten > Posture > Remediation actions > Application Remediations:**

Application Remediation

Rows/Page 2 1 / 1 Go 2 Total Rows

<input type="checkbox"/>	Name	Description	Application State	Compliance module	Categories
<input type="checkbox"/>	Notepadplus_Remediation			4.x or later	
<input type="checkbox"/>	FileZilla-Uninstall_Remediation			4.x or later	

Vereisten zijn te vinden op **Policy > Policy Elementen > Resultaten > Posture > Requirements:**

Name	Identity Groups	Operating Systems	Compliance Module	Stealth mode	Other Conditions	Requirements
FileZilla-Uninstall_Requirement	for Windows All	using 4.x or later	using Standard	met if FileZilla-Uninstall	then FileZilla-Uninstall_Remediation	Edit

Het beleid wordt gevoerd op **Policy > Posture:**

Posture Policy

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

Status	Rule Name	Identity Groups	Operating Systems	Compliance Module	Stealth mode	Other Conditions	Requirements
<input checked="" type="checkbox"/>	FileZilla-Uninstall_Policy	Any	and Windows All	and 4.x or later	and Disabled	and	then FileZilla-Uninstall_Requirement
<input checked="" type="checkbox"/>	Notepadplus_Online	Any	and Windows All	and 4.x or later	and Disabled	and	then Notepadplus_Remediation

Rapporten

Elk Postrapport van elk EndPoint wordt opgeslagen op ISE en kan worden gecontroleerd bij **Operations > Rapporten**. Er zijn te verschillende Postrapporten:

- Beoordeling van de positie door Endpoint - het bevat details over de overeenstemming van de positie voor een bepaald eindpunt.
- Postbeoordeling door middel van conditionering - het bevat details over posteringspolitieke voorwaarden. Hieruit blijkt welke voorwaarden zijn mislukt en welke voorwaarden zijn vervuld. Alleen de verplichte en facultatieve voorwaarden zijn vermeld.

Postbeoordeling per conditionering

Postbeoordeling door middel van conditiontie ziet er uit zoals aangegeven. In dit voorbeeld faalt een van de verplichte voorwaarden, zodat de status van postuur naar niet-conforme voorwaarden gaat:

Timestamp	Status	User	IP	Result	Condition	IP	Location
2017-01-24 17:20:57...	●	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 17:05:59...	●	alice	C0:4A:00:15:75:C8	Failed	fs_visInst_v4_FileZilla_ANY	10.62.148.136	All Locations
2017-01-24 17:05:59...	●	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 17:01:22...	●	alice	C0:4A:00:15:75:C8	Failed	fs_visInst_v4_FileZilla_ANY	10.62.148.136	All Locations
2017-01-24 17:01:22...	●	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 16:56:44...	●	alice	C0:4A:00:15:75:C8	Failed	fs_visInst_v4_FileZilla_ANY	10.62.148.136	All Locations
2017-01-24 16:56:44...	●	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 16:52:08.77	●	alice	C0:4A:00:15:75:C8	Failed	fs_visInst_v4_FileZilla_ANY	10.62.148.136	All Locations
2017-01-24 16:52:08.77	●	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 16:17:24.78	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 15:46:33.24	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 15:45:57...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 13:45:04...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 12:43:45...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 12:43:10...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 12:42:35...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 12:41:59.22	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 11:41:14...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations


Rows/Page: 100 / 11 / 12 / Go 1116 Total Rows

Postbeoordeling door eindpunt

Postbeoordeling per eindpunt:

Timestamp	Status	User	IP	Result	Condition	IP	Location
2017-01-24 18:17:40.993	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 18:10:44.127	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 18:00:57.393	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:55:39.642	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:46:25.969	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:40:35.05	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:25:38.766	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:20:57.331	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:05:59.534	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:01:22.737	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 16:56:44.516	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 16:52:08.77	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 16:17:24.78	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 15:46:33.24	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 15:45:57.783	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 13:45:04.109	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 12:43:45.326	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 12:43:10.551	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit

Rows/Page: 100 / 6 / Go 580 Total Rows

Details van elke postcontrole kunnen worden gecontroleerd door op het pictogram **Details Report** te klikken - 

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Van ISE

ise-psc.log bevat alle informatie over houding, inclusief debugs. Pas de uitwerpselen kunnen worden ingeschakeld bij **Beheer > Systeem > Vastlegging > Logconfiguratie van het bug-logbestand**. componentnaam is **postuur**:

- Local Log Settings
- Remote Logging Targets
- Logging Categories
- Message Catalog
- Debug Log Configuration
- Collection Filters

Node List > ise22-pri.example.com
Debug Level Configuration

Component Name	Log Level	Description
PassiveID	INFO	PassiveID events and messages
policy-engine	INFO	Policy Engine 2.0 related messages
portal	INFO	Portal (Guest, Hotspot, BYOD, CP) debug messages
portal-session-manager	INFO	Portal Session Manager debug messages
portal-web-action	INFO	Base Portal debug messages
posture	DEBUG	Posture debug messages
previewportal	INFO	Preview Portal debug messages

Zodra een eindpunt op het netwerk is aangesloten en AnyConnect bereik op de ISE, controleert ISE of EP moet worden gecontroleerd aan de hand van de ingestelde posteringcontroles en detecteert zij de versie van de nalevingsmodule die op het EP is geïnstalleerd. Op basis van verzamelde informatie genereert ISE een vraagstelling voor de EP - **NAC agent xml** en versleutel het. Later stuurt ISE deze zoekopdracht naar AnyConnect.

```

2017-01-04 19:19:13,686 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PostureHandlerImpl --:cisco::-- About to query posture policy for user
cisco with endpoint mac C0-4A-00-15-75-C8
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PostureManager --:cisco::-- agentCMVersion=4.2.468.0,
agentType=AnyConnect Posture Agent, groupName=OESIS_V4_Agents -> found agent group with
displayName=4.x or later
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::-- User cisco belongs to groups NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation,NAC
Group:NAC:IdentityGroups:Any
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::-- About to retrieve posture policy
resources for os 7 Enterprise, agent group 4.x or later and identity groups [NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation, NAC
Group:NAC:IdentityGroups:Any]
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::-- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:Apps by agent group with FQN NAC
Group:NAC:AgentGroupRoot:ALL:OESIS_V4_Agents
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::-- The evaluation result by agent group for
resourceId NAC Group:NAC:Posture:PosturePolicies:Apps is Permit
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::-- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:Apps by OS group with FQN NAC
Group:NAC:OsGroupRoot:ALL:WINDOWS_ALL:WINDOWS_7_ALL:WINDOWS_7_ENTERPRISE_ALL
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::-- stealth mode is 0
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::-- The evaluation result by os group for
resourceId NAC Group:NAC:Posture:PosturePolicies:Apps is Permit
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::-- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:Apps by Stealth mode NSF group with FQN NAC
Group:NAC:StealthModeStandard
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::-- Procesing obligation with posture policy
resource with id NAC Group:NAC:Posture:PosturePolicies:Apps
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco::-- Found obligation id

```



```
urn:cisco:cepm:3.3:xacml:response-qualifier for posture policy resource with id NAC
Group:NAC:Posture:PosturePolicies:Apps
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Found obligation id PostureReqs for
posture policy resource with id NAC Group:NAC:Posture:PosturePolicies:Apps
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Posture policy resource id Apps has
following associated requirements []
2017-01-04 19:19:13,720 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco::- policy enforcemnt is 2
2017-01-04 19:19:13,720 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco::- simple condition: [Name=Apps_Collection,
Description=null, Application State =installed,running, Provision By =Everything, monitory
Categories = []]
2017-01-04 19:19:13,720 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco::- check type is ApplicationVisibility
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco::- NAC agent xml <?xml version="1.0"
encoding="UTF-8"?><cleanmachines>
  <version>ISE: 2.2.0.423</version>
  <encryption>0</encryption>
  <package>
    <id>l2</id>
    <name>Apps_collection</name>
    <description>Apps Check</description>
    <version/>
    <type>3</type>
    <optional>2</optional>
    <action>3</action>
    <check>
      <id>Apps_Collection</id>
      <category>l2</category>
      <type>l202</type>
      <monitor>ALL</monitor>
      <evaluation>periodic</evaluation>
    </check>
    <criteria>(Apps_Collection)</criteria>
  </package>
</cleanmachines>

2017-01-04 19:19:13,800 INFO [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil -:cisco::- StatusUtil - getPosturePolicyHTML
[<cleanmachines><version>ISE:
2.2.0.423</version><encryption>0</encryption><package><id>l2</id><name>Apps_collection</name><de
scription>Apps
Check</description><version/><type>3</type><optional>2</optional><action>3</action><check><id>Ap
ps_Collection</id><category>l2</category><type>l202</type><monitor>ALL</monitor><evaluation>peri
odic</evaluation></check><criteria>(Apps_Collection)</criteria></package></cleanmachines>]
2017-01-04 19:19:13,800 INFO [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil -:cisco::- StatusUtil -getPosturePolicyHTML - do encrypt
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil -:cisco::- Encrypting policy using AES key.
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.CipherUtil -:cisco::- Encrypting message using AES.
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil -:cisco::- IV Base 64: AeUQGbj6CP/jMB+cTIGIGQ==
2017-01-04 19:19:13,801 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil -:cisco::- StatusUtil.getPosturePolicyHTML() returns <!--X-
Perfigo-UserKey=--><!--X-Perfigo-Provider=Device Filter--><!--X-Perfigo-UserName=cisco--><!--
error=1010--><!--X-Perfigo-DM-Error=1010--><!--user role=--><!--X-Perfigo-OrigRole=--><!--X-
Perfigo-DM-Scan-Req=0--><!--X-ISE-IV=AeUQGbj6CP/jMB+cTIGIGQ==--><!--X-Perfigo-DM-Software-
List=f5aGq8rU5wx7hFS9WnugNhy/6HaSxNtKesoqAjYkecEk56t+I/J93PtAYU0XLq451NXQhReuFktImYEPENWwOslbV5o
OTuTsY3kEbcuR4p5Sp0cfz/j98YEubNtSKDCUGt5U8dhpOJqMYTV4UcaSP/D0FXym10gFEjPxpPghyWcplzYwcpehIX+2vOY
OSzPTEvM2kDdHTkof+/UYvBfGv8Y7YkK9P6lupfSedIqdynyxUbeqknXkoCaWvUawJLVWiXAJs2atsCwJjXitwNHyzCuH/mB
```

```
z/Y9AUvblCB/cutCeyVCl7ij8wtXUAt2NpKqeEj0COOxnp5B35JTBfOSXHFVjL29E5JALaun6RR8yJlkd4apk7qflnjsu451
CHY/SbKTMnqjV5bNwXfuCBf++X6X/mh0nwk+r2iWhJjFyqmNxBm2BvcJAjXOKOV7xHIhgmLj+etF4Sss/zwnFT4+WTzKI+Bp
brVdnZjUP7+uvbQbIPtRFqJVI5StjZlIP4vLzFWKbWxI+itTX6hjqvNhiT2zwtvIboUzXaBV6yS5/+5cYMU3+EhWxIx/UVO
0o7sX--><!--X-Perfigo-DM-Session-Time=240-->
2017-01-04 19:19:13,801 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco:::- User cisco belongs to groups NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation,NAC
Group:NAC:IdentityGroups:Any
2017-01-04 19:19:13,801 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PostureHandlerImpl --:cisco:::- Sending response to endpoint C0-4A-00-
15-75-C8 http response [[ <!--X-Perfigo-UserKey=--><!--X-Perfigo-Provider=Device Filter--><!--X-
Perfigo-UserName=cisco--><!--error=1010--><!--X-Perfigo-DM-Error=1010--><!--user role=--><!--X-
Perfigo-OrigRole=--><!--X-Perfigo-DM-Scan-Req=0--><!--X-ISE-IV=AeUQGbj6CP/jMB+cTIGIGQ=---><!--X-
Perfigo-DM-Software-
List=f5aGq8rU5wx7hFS9WnugNhy/6HaSxNtKesoqAjYkecEk56t+I/J93PtAYU0XLq451NXQhReuFktImYEPENWwOs1bV5o
OTuTsY3kEbcuR4p5Sp0cfz/j98YEubNtSKDCUGt5U8dhpOJqMYTV4UcaSP/D0FXym10gFEjPxpPghyWcplzYwcpheIX+2vOY
OSzPTEvM2kDdHTkof+/UYvBfGv8Y7YkK9P61upfSedIqdynyxUbeqknXkoCaWvUawJLVWiXAJ2atsCwJjXitwNHyzCuH/mB
z/Y9AUvblCB/cutCeyVCl7ij8wtXUAt2NpKqeEj0COOxnp5B35JTBfOSXHFVjL29E5JALaun6RR8yJlkd4apk7qflnjsu451
CHY/SbKTMnqjV5bNwXfuCBf++X6X/mh0nwk+r2iWhJjFyqmNxBm2BvcJAjXOKOV7xHIhgmLj+etF4Sss/zwnFT4+WTzKI+Bp
brVdnZjUP7+uvbQbIPtRFqJVI5StjZlIP4vLzFWKbWxI+itTX6hjqvNhiT2zwtvIboUzXaBV6yS5/+5cYMU3+EhWxIx/UVO
0o7sX--><!--X-Perfigo-DM-Session-Time=240--> ]]
2017-01-04 19:19:13,959 DEBUG [http-bio-10.48.26.60-8443-exec-5][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- receiving request from client
C0:4A:00:15:75:C8 10.62.148.162 bcu5ksw0
2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Found the ipAddress that matched the http
request remote address 10.62.148.162 and corresponding client mac address C0-4A-00-15-75-C8
2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for Radius session with input
values : sessionId: 0a3e94650000066586d3c42, MacAddr: C0-4A-00-15-75-C8, ipAddr: 10.62.148.162
2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- looking for session using session ID:
0a3e94650000066586d3c42, IP addrs: [10.62.148.162], mac Addrs [C0-4A-00-15-75-C8]
2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][]
cisco.cpm.posture.runtime.PostureRuntimeFactory -::::- Found session using sessionId
0a3e94650000066586d3c42
Het volledige rapport van AnyConnect. Dit rapport bevat informatie over alle gevonden
toepassingen die overeenkomen met de geconfigureerde toepassingsvoorwaarden.
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- UDID is
766bb955e51e4ab063fd478c63acee81260ca592 for end point C0-4A-00-15-75-C8
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- os version from user agent is 1.2.1.6.1.4
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Received posture request [parameters:
reqtype=, userip=10.62.148.162, clientmac=C0-4A-00-15-75-C8, os=, osVerison=1.2.1.6.1.4,
architecture=, provider=, state=, userAgent=Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.4;
AnyConnect Posture Agent v.4.4.00209), session_id=
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Found a session info for endpoint C0-4A-00-
15-75-C8 cisco
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Got userid cisco from cache for endpoint C0-
4A-00-15-75-C8/
2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Report IV in Base64:
JjneGgZcJbmjqMKQcy8kJg==
2017-01-04 19:19:37,359 DEBUG [http-bio-10.48.26.60-8443-exec-3][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Using AES shared secret to decrypt report.
2017-01-04 19:19:37,359 DEBUG [http-bio-10.48.26.60-8443-exec-3][]
cisco.cpm.posture.util.CipherUtil -::::- Decrypting message using AES.
```

2017-01-04 19:19:37,359 DEBUG [http-bio-10.48.26.60-8443-exec-3][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -:::- **Decrypted report** [[
<report><version>1000</version><package><id>12</id><status>1</status><check><chk_id>Apps_Collect
ion</chk_id><diff>0</diff><application><diff>0</diff><id></id><name>Adobe Flash Player 23
NPAPI</name><vendor>Adobe Systems
Incorporated</vendor><version>23.0.0.207</version><category>Unclassified</category></application
><application><diff>0</diff><id>104</id><name>Adobe Flash Player</name><vendor>Adobe Systems
Inc.</vendor><version>23.0.0.207</version><path>C:\Windows\SysWOW64\Macromed\F\nash\</path><category>Unclassified</category></application><application><diff>0</diff><id>873</id><name>BitLocker
Drive Encryption</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32\</path><category>
DiskEncryption</category></application><application><diff>0</diff><id></id><name>Cisco
AnyConnect Diagnostics and Reporting Tool</name><vendor>Cisco Systems,
Inc.</vendor><version>4.4.00209</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Secure Mobility
Client\DART\</path><category>Unclassified</category></application><application><diff>0</diff><id
></id><name>Cisco AnyConnect ISE Compliance Module</name><vendor>Cisco Systems,
Inc</vendor><version>4.2.468.0</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Secure Mobility
Client\opswat\</path><category>Unclassified</category></application><application><diff>0</diff><
id></id><name>Cisco AnyConnect ISE Posture Module</name><vendor>Cisco Systems,
Inc.</vendor><version>4.4.00209</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Secure Mobility
Client\opswat\</path><category>Unclassified</category></process><diff>0</diff><pid>704</pid><path>c:\pro
gram files (x86)\cisco\cisco anyconnect secure mobility
client\vpnagent.exe</path><hash>7D7502DE53F0282A7AFC98BE89F54D39FDEC3FAC2A1F32674C76967ADC695E09
</hash></process><process><diff>0</diff><pid>1296</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseagent.exe</path><hash>7E156520C184334D473506FFE8A482997581ACF6ABD34231FDEDC2B9A3A120
66</hash></process><process><diff>0</diff><pid>3076</pid><path>c:\program files
(x86)\cisco\cisco anyconnect secure mobility
client\vpnui.exe</path><hash>0131258625A16B78125EB2081E8D5678671B6DE52DDA9E0813D4674618177DC3</h
ash></process><process><diff>0</diff><pid>3384</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\acise.exe</path><hash>8636F5761663A0EB9EDE263609B6AEF0EA52292E5B093AD4C453097583F365DD</h
ash></process><process><diff>0</diff><pid>15924</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseposture.exe</path><hash>7FA4B3B6F688642E800AD53B865DBDCC163FBCA92D83482248DB068BA421
92EA</hash></process></application><application><diff>0</diff><id></id><name>Cisco AnyConnect
Profile Editor</name><vendor>Cisco Systems,
Inc.</vendor><version>4.1.08005</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Profile
Editor\</path><category>Unclassified</category></application><application><diff>0</diff><id></id
><name>Cisco AnyConnect Secure Mobility Client </name><vendor>Cisco Systems,
Inc.</vendor><version>4.4.00209</version><category>Unclassified</category></application><applica
tion><diff>0</diff><id></id><name>Cisco AnyConnect Secure Mobility Client</name><vendor>Cisco
Systems, Inc.</vendor><version>4.4.00209</version><path>C:\Program Files (x86)\Cisco\Cisco
AnyConnect Secure Mobility
Client\</path><category>Unclassified</category></process><diff>0</diff><pid>704</pid><path>c:\pro
gram files (x86)\cisco\cisco anyconnect secure mobility
client\vpnagent.exe</path><hash>7D7502DE53F0282A7AFC98BE89F54D39FDEC3FAC2A1F32674C76967ADC695E09
</hash></process><process><diff>0</diff><pid>1296</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseagent.exe</path><hash>7E156520C184334D473506FFE8A482997581ACF6ABD34231FDEDC2B9A3A120
66</hash></process><process><diff>0</diff><pid>3076</pid><path>c:\program files
(x86)\cisco\cisco anyconnect secure mobility
client\vpnui.exe</path><hash>0131258625A16B78125EB2081E8D5678671B6DE52DDA9E0813D4674618177DC3</h
ash></process><process><diff>0</diff><pid>3384</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\acise.exe</path><hash>8636F5761663A0EB9EDE263609B6AEF0EA52292E5B093AD4C453097583F365DD</h
ash></process><process><diff>0</diff><pid>15924</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseposture.exe</path><hash>7FA4B3B6F688642E800AD53B865DBDCC163FBCA92D83482248DB068BA421
92EA</hash></process></application><application><diff>0</diff><id></id><name>Cisco NAC Agent

</name><vendor>Cisco Systems, Inc.</vendor><version>4.9.5.10</version><path>C:\Program Files (x86)\Cisco\Cisco NAC Agent\</path><category>Unclassified</category><process><diff>0</diff><pid>1444</pid><path>c:\program files (x86)\cisco\cisco nac agent\nacagent.exe</path><hash>502EF2A864254A2DF555E029BE2C39E94B111E8B01534D7161826650DE4CEB4D</hash></process><process><diff>0</diff><pid>2320</pid><path>c:\program files (x86)\cisco\cisco nac agent\nacagentui.exe</path><hash>DC617419F082BEAF26521E48CB410282631F93F1359E604A4D3D181A04FEE1FB</hash></process></application><application><diff>0</diff><id>293</id><name>DAEMON Tools Lite</name><vendor>Disc Soft Ltd</vendor><version>4.49.1.0356</version><path>C:\Program Files (x86)\DAEMON Tools Lite\</path><category>Unclassified</category></application><application><diff>0</diff><id></id><name>Digital Operatives PAINT Beta</name><vendor></vendor><version>0.0</version><category>Unclassified</category></application><application><diff>0</diff><id></id><name>FileZilla Server</name><vendor>FileZilla Project</vendor><version>beta 0.9.44</version><path>C:\Program Files (x86)\FileZilla Server\</path><category>Unclassified</category><process><diff>0</diff><pid>1408</pid><path>c:\program files (x86)\filezilla server\filezilla server.exe</path><hash>E8DB1409DB694A90C759F418346AE5D71014AE3513A8B865B50923AD0DFEE395</hash></process><process><diff>0</diff><pid>2348</pid><path>c:\program files (x86)\filezilla server\filezilla server interface.exe</path><hash>F57B0A7F4A9EBAACC1A67323EBB93D96FA910524FAE842953551DBA103EF71C5</hash></process></application><application><diff>0</diff><id>180</id><name>FileZilla</name><vendor>FileZilla Project</vendor><version>3.8.1.0</version><path>C:\Program Files (x86)\FileZilla FTP Client\</path><category>FileShare</category></application><application><diff>0</diff><id>39</id><name>Google Chrome</name><vendor>Google Inc.</vendor><version>55.0.2883.87</version><path>C:\Program Files (x86)\Google\Chrome\Application\</path><category>AntiPhishing, Browser</category></application><application><diff>0</diff><id></id><name>Google Update Helper</name><vendor>Google Inc.</vendor><version>1.3.24.15</version><category>Unclassified</category></application><application><diff>0</diff><id>100</id><name>Internet Explorer</name><vendor>Microsoft Corporation</vendor><version>11.0.9600.18524</version><path>C:\Program Files\Internet Explorer\</path><category>AntiPhishing, Browser</category></application><application><diff>0</diff><id></id><name>Java 7 Update 79</name><vendor>Oracle</vendor><version>7.0.790</version><path>C:\Program Files (x86)\Java\jre7\</path><category>Unclassified</category></application><application><diff>0</diff><id></id><name>Java 8 Update 91</name><vendor>Oracle Corporation</vendor><version>8.0.910.15</version><path>C:\Program Files (x86)\Java\jre1.8.0_91\</path><category>Unclassified</category></application><application><diff>0</diff><id></id><name>Java Auto Updater</name><vendor>Oracle Corporation</vendor><version>2.8.91.15</version><category>Unclassified</category></application><application><diff>0</diff><id>111</id><name>Java</name><vendor>Oracle Corporation</vendor><version>7.0.790.15</version><path>C:\Program Files (x86)\Java\jre7\bin\</path><category>Unclassified</category></application><application><diff>0</diff><id>111</id><name>Java</name><vendor>Oracle Corporation</vendor><version>8.0.910.15</version><path>C:\Program Files (x86)\Java\jre1.8.0_91\bin\</path><category>Unclassified</category></application><application><diff>0</diff><id></id><name>Microsoft .NET Framework 4.6.1</name><vendor>Microsoft Corporation</vendor><version>4.6.01055</version><path>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SetupCache\v4.6.01055\</path><category>Unclassified</category></application><application><diff>0</diff><id></id><name>Microsoft Network Monitor 3.4</name><vendor>Microsoft Corporation</vendor><version>3.4.2350.0</version><category>Unclassified</category></application><application><diff>0</diff><id></id><name>Microsoft Network Monitor: NetworkMonitor Parsers 3.4</name><vendor>Microsoft Corporation</vendor><version>3.4.2350.0</version><category>Unclassified</category></application><application><diff>0</diff><id></id><name>Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148</name><vendor>Microsoft Corporation</vendor><version>9.0.30729.4148</version><category>Unclassified</category></application><application><diff>0</diff><id></id><name>Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148</name><vendor>Microsoft Corporation</vendor><version>9.0.30729.4148</version><category>Unclassified</category></application><application><diff>0</diff><id>44</id><name>Mozilla Firefox</name><vendor>Mozilla Corporation</vendor><version>47.0.2</version><path>C:\Program Files (x86)\Mozilla Firefox\</path><category>AntiPhishing, Browser</category><process><diff>0</diff><pid>8292</pid><p

ath>c:\program files (x86)\mozilla
firefox\firefox.exe</path><hash>47F80E4FC4C43FAF468D94F5D51AAC78A125CC720FCBEA0B88B5F29D06719CE9
</hash></process></application><application><diff>0</diff><id></id><name>Mozilla Maintenance
Service</name><vendor>Mozilla</vendor><version>47.0.2.6148</version><category>Unclassified</cate
gory></application><application><diff>0</diff><id>298</id><name>Notepad++</name><vendor>Notepad+
+ Team</vendor><version>6.63</version><path>C:\Program Files
(x86)\Notepad++\</path><category>Unclassified</category></application><application><diff>0</diff
><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3122661)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3127233)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3136000v2)</name><vendor>Microsoft
Corporation</vendor><version>2</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3142037)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3143693)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3164025)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>TP-LINK TL-WDN3200 Driver</name><vendor>TP-
LINK</vendor><version>1.1.0</version><path>C:\Program Files (x86)\TP-LINK\TP-LINK Wireless
Configuration Utility and
Driver\</path><category>Unclassified</category></application><application><diff>0</diff><id></id
><name>Tftpd32 Standalone Edition (remove
only)</name><vendor></vendor><version>0.0</version><category>Unclassified</category></applicatio
n><application><diff>0</diff><id></id><name>VMware Tools</name><vendor>VMware,
Inc.</vendor><version>9.4.15.2827462</version><path>C:\Program Files\VMware\VMware
Tools\</path><category>Unclassified</category><process><diff>0</diff><pid>952</pid><path>c:\prog
ram files\vmware\vmware
tools\vmtoolsd.exe</path><hash>5C642EF7F4EF65A0445B2C2CD227F9431835712EE7F1BD4D01D1F7472199DE47<
</hash></process><process><diff>0</diff><pid>1516</pid><path>c:\program files\vmware\vmware
tools\vmtoolsd.exe</path><hash>5C642EF7F4EF65A0445B2C2CD227F9431835712EE7F1BD4D01D1F7472199DE47<
</hash></process></application><application><diff>0</diff><id></id><name>WinPcap
4.1.3</name><vendor>Riverbed Technology,
Inc.</vendor><version>4.1.0.2980</version><category>Unclassified</category></application><applic
ation><diff>0</diff><id>300</id><name>WinPcap</name><vendor>Riverbed Technology,
Inc.</vendor><version>4.1.0.2980</version><path>C:\Program Files
(x86)\WinPcap\</path><category>Unclassified</category></application><application><diff>0</diff><
id>923</id><name>Windows Backup and Restore</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32\</path><category>
BackupClient</category></application><application><diff>0</diff><id>362</id><name>Windows
Defender</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Program Files\Windows
Defender\</path><category>AntiMalware</category></application><application><diff>0</diff><id>283
</id><name>Windows Firewall</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32\</path><category>
FireWall</category></application><application><diff>0</diff><id>1612</id><name>Windows Media
Player</name><vendor>Microsoft
Corporation</vendor><version>12.0.7601.23517</version><path>C:\Program Files\Windows Media
Player\</path><category>Unclassified</category><process><diff>0</diff><pid>1596</pid><path>c:\pr
ogram files\windows media
player\wmpnetwk.exe</path><hash>306467D280E99D0616E839278A4DB5BED684F002AE284C3678CABB5251459CB3
</hash></process></application><application><diff>0</diff><id>1587</id><name>Windows Security
Health Agent</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32\</path><category>
HealthAgent</category></application><application><diff>0</diff><id>1090</id><name>Windows Update
Agent</name><vendor>Microsoft
Corporation</vendor><version>7.6.7601.19161</version><path>C:\Windows\System32\</path><category>

```
PatchManagement</category></application><application><diff>0</diff><id>1106</id><name>Windows
VPN Client</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32</path><category>
VPNClient</category></application><application><diff>0</diff><id>207</id><name>Wireshark</name><
vendor>The Wireshark developer community</vendor><version>1.10.7</version><path>C:\Program Files
(x86)\Wireshark</path><category>Unclassified</category></application></check></package></report
> ]]
```

...

Alle rapporten zijn XML strings. Rapport voorbeeldopmaak:

```
<report>
<version>1000</version>
<package>
<id>12</id>
<status>1</status>
<check>
<chk_id>Apps_Collection</chk_id>
<diff>0</diff>
<application>
<diff>0</diff>
<id>104</id>
<name>Adobe Flash Player</name>
<vendor>Adobe Systems Inc.</vendor>
<version>23.0.0.207</version>
<path>C:\Windows\SysWOW64\Macromed\Flash</path>
<category>Unclassified</category>
</application>
...
<application>
<diff>0</diff>
<id></id>
<name>Cisco AnyConnect ISE Posture Module</name>
<vendor>Cisco Systems, Inc.</vendor>
<version>4.4.00209</version>
<path>C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client</path>
<category>Unclassified</category>
<process>
<diff>0</diff>
<pid>704</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\vpnagent.exe</path>
<hash>7D7502DE53F0282A7AFC98BE89F54D39FDEC3FAC2A1F32674C76967ADC695E09</hash>
</process>
<process>
<diff>0</diff>
<pid>1296</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\aciseagent.exe</path>
<hash>7E156520C184334D473506FFE8A482997581ACF6ABD34231FDEDC2B9A3A12066</hash>
</process>
<process>
<diff>0</diff>
<pid>3076</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\vpnui.exe</path>
<hash>0131258625A16B78125EB2081E8D5678671B6DE52DDA9E0813D4674618177DC3</hash>
</process>
<process>
<diff>0</diff>
<pid>3384</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\acise.exe</path>
<hash>8636F5761663A0EB9EDE263609B6AEF0EA52292E5B093AD4C453097583F365DD</hash>
</process>
<process>
<diff>0</diff>
```

```
<pid>15924</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility
client\aciseposture.exe</path>
<hash>7FA4B3B6F688642E800AD53B865DBDCC163FBCA92D83482248DB068BA42192EA</hash>
</process>
</application>
... </check> </package> </report>
```

AnyConnect stuurt alleen volledige rapporten over de eerste verbinding. Verder worden er alleen maar veranderingen aangebracht. Zo werd bijvoorbeeld Kladblok++ na een tijdje gestart:

```
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Received posture request [parameters:
reqtype=, userip=10.62.148.162, clientmac=C0-4A-00-15-75-C8, os=, osVerison=1.2.1.6.1.4,
architecture=, provider=, state=, userAgent=Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.4;
AnyConnect Posture Agent v.4.4.00209), session_id=
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Found a session info for endpoint C0-4A-00-
15-75-C8 cisco
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Got userid cisco from cache for endpoint C0-
4A-00-15-75-C8/
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Report IV in Base64:
JjneGgZcJbmjqMKQcy8kJg==
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Using AES shared secret to decrypt report.
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.util.CipherUtil -::::- Decrypting message using AES.
2017-01-04 19:24:37,930 DEBUG [http-bio-10.48.26.60-8443-exec-7][[]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Decrypted report [[
<report><version>1000</version><package><id>12</id><status>1</status><check><chk_id>Apps_Collect
ion</chk_id><diff>1</diff><application><diff>2</diff><id>298</id>
```

```
<vendor>Notepad++ Team</vendor><version>6.63</version><path>C:\Program Files
(x86)\Notepad++\</path><category>Unclassified</category><process><diff>0</diff>
```

```
<path>c:\program files
(x86)\notepad++\notepad++.exe</path><hash>43E9F528CD2405E6DD117857D440A634769C6E11C4D986605354C2
605B6E7D84</hash></process></application></check></package></report> ]]
```

Opgemaakt:

```
<report>
<version>1000</version>
<package>
<id>12</id>
<status>1</status>
<check>
<chk_id>Apps_Collection</chk_id>
<diff>1</diff>
<application>
<diff>2</diff>
<id>298</id>
```

```
<vendor>Notepad++ Team</vendor>
<version>6.63</version>
<path>C:\Program Files (x86)\Notepad++\</path>
<category>Unclassified</category>
<process>
<diff>0</diff>
```

```
<path>c:\program files (x86)\notepad++\notepad++.exe</path>
<hash>43E9F528CD2405E6DD117857D440A634769C6E11C4D986605354C2605B6E7D84</hash>
</process>
</application>
</check>
</package>
</report>
```

Van AnyConnect

Bestand **AnyConnect_ISEPosture.txt** bevat alle bijbehorende stammen en uiteinden. Dit bestand is te vinden in DART-bundel op een eindpunt. Hier is een voorbeeld van een periodiek rapport, dat met AES256 is versleuteld:

```
Date       : 01/04/2017
Time       : 19:34:38
Type       : Unknown
Source     : acise
```

```
Description : Function: Authenticator::bldMonitorReport
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 724
Level: info
```

Monitor Report:

```
&user_key=dummykey&cm=10&ops=1&mac_list=C0%3a4A%3a00%3a15%3a75%3aC8&ip_list=10%2e62%2e148%2e162&
hostname=TSOPREK%2dWIN7%2dl&udid=766bb955e51e4ab063fd478c63acee81260ca592&dm_report_client_IV=Jj
neGgZcJbmjqMKQcy8kJg%3d%3d&dm_report=2yWwY7QzHWCY%2fdVEESSAabEZtYltxNE7Qgy00a85Dgo2Ts4ok8sIrBM37
S2%2fe2Hs0URCP4KkfY4Ap8%2bh%2fqS%2biw50CZeJkG%2bVbF7RTRqZyrg2veWAwvEDsSb%2bqWRRdzvZfSjS3G4ApQi07
qnfExwN1IvCqrVOp1j17TAcVXEht8NkDg00T9jM%2fTNH%2fMK1lc0o6Ha5juJo4YtWDWY%2bnOancw%3d%3d.
```

```
Date       : 01/04/2017
Time       : 19:34:38
Type       : Unknown
Source     : acise
```

```
Description : Function: Authenticator::buildAndSendHttpMsg
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 196
Level: debug
```



```
MSG_SN_HTTP_REQUEST, {{url="https://ise22-pri.example.com:8443/auth/perfigo_validate.jsp"},
{server="ise22-pri.example.com"}, {method="post"}, {object_path=""}, {reuse_existing=1},
{close_when_done=0},
{pkt="&user_key=dummykey&cm=10&ops=1&mac_list=C0%3a4A%3a00%3a15%3a75%3aC8&ip_list=10%2e62%2e148%
2e162&hostname=TSOPREK%2dWIN7%2d1&udid=766bb955e51e4ab063fd478c63acee81260ca592&dm_report_client
_IV=JjneGgZcJbmjqMKQcy8kJg%3d%3d&dm_report=2yWwY7QzHWCY%2fDVEESSAabEZtYltxNE7Qgy0Oa85Dgo2Ts4ok8s
IrBM37S2%2fe2Hs0URCP4KkfY4Ap8%2bh%2fqS%2biw50CZe jKG%2bVbF7RTRqZyrg2veWAwwEDsSb%2bqWRRdzvZfSjS3G4
ApQi07qnfExwN1IvCqrVOp1j17TAcVXEht8NkDg00T9jM%2fTNH%2fMK1lc0o6Ha5juJo4YtWDWY%2bnOancw%3d%3d"},
{path=""}, {type=1}}.
```

```
Date      : 01/04/2017
Time      : 19:34:39
Type      : Unknown
Source    : acise
```

```
Description : Function: HttpHandler::createOutgoingHTTPSMessage
Thread Id: 0xD3C
File: HttpHandler.cpp
Line: 295
Level: debug
```

```
MSG_NS_HTTP_RESPONSE, {{success=1}, {pkt="<!--error=0--><!--X-Perfigo-DM-Error=0--><!--X-
Perfigo-Monitoring-Interval=5-->"}, {type=1}}.
```

Gemeenschappelijke kwesties

AnyConnect kan ISE niet bereiken

In dit geval bevat `AnyConnect_ISEPosture.txt` fouten:

```
Date      : 01/04/2017
Time      : 20:04:40
Type      : Unknown
Source    : acise
```

```
Description : Function: Authenticator::buildAndSendHttpMsg
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 196
Level: debug
```

```
MSG_SN_HTTP_REQUEST, {{url="https://ise22-pri.example.com:8443/auth/perfigo_validate.jsp"},
{server="ise22-pri.example.com"}, {method="post"}, {object_path=""}, {reuse_existing=1},
{close_when_done=0},
{pkt="&user_key=dummykey&cm=10&ops=1&mac_list=C0%3a4A%3a00%3a15%3a75%3aC8&ip_list=10%2e62%2e148%
2e162&hostname=TSOPREK%2dWIN7%2d1&udid=766bb955e51e4ab063fd478c63acee81260ca592&dm_report_client
_IV=JjneGgZcJbmjqMKQcy8kJg%3d%3d&dm_report=2yWwY7QzHWCY%2fDVEESSAabEZtYltxNE7Qgy0Oa85Dgo2Ts4ok8s
IrBM37S2%2fe2Hs0URCP4KkfY4Ap8%2bh%2fqS%2biw50CZe jKG%2bVbF7RTRqZyrg2veWAwwEDsSb%2bqWRRdzvZfSjS3G4
ApQi07qnfExwN1Pdu7AztTn%2f3VYph9WNF1jG1jXSuTFmr38e%2bVDXQnx7avYHs9meVItYqA6MecAJK3WdkBNSrK1bYjmI
vzkAPqR2LuoflnA9IcNOTZQ9iN%2fknOj1LqsiV5eV6j1MSUeOakKsTwylgbPsFz99eKdtaCMv1F%2fSAmvLApjpk0IMKor
XXkvpJURtAtOMK751tXdykC85ihgHcI10JW7mlpvIppk5MbcZjIhQbXldr5%2fQVdpB8eRqMhF1iCK1gx961wwdzBSfr%2bg
rcF4072fYYNOa9cYnTFShgU%2bxrnBDcJ1GUoYE9K5nTfGQ01p4NrCbLjpm79e14v14YgfQhmSfktwxFA8pY7A6jml3BIp30
9gmQVnoTgaaccqkW76uT%2bPkjvOyrOgdG0CYuUwUMVqpctGKorxx1C3IwXhBWUmvRY9p2LRdePRqncN8hpiesyk%2bzTnyX
00aNdHD6%2bGEMGo9QjQvwrL9dcvrUxxHtlQcJPekXajXPfn98FpC8z%2b966tcz4DfMN6giSlEfK6y5%2bMpk0oAL%2fV4X
Mg296PDocGaeTK1OUR7Qkl%2b7S2fv%2fCfZdiQaTndZ6zHWuimq5JBRElmuKI9hWRN2cPERcDn64ISZZSiz9yPoJPLPPpFs
fggkc2PdS00EETmim%2bBjNKcFz2Tcsq76eYfDtvDq9tGzjST8opInlIixdAzdbeWsjCAerCvS73xg2vd2DHfpFlrd51Va3q
```

wo3Vov3nFiAz4l3IrIlfOHjAE7rCZTy2dWU455icOjm0%2bCVAS3SzwCea4fZu3fAhmIhAVQKElcfZ4CyyBv8934OVw62Bxu
5ij0wbH0StA8TSbxJXyuGBw8cqTPfuUtqPLx6nWtcrZ6p13MuQTq%2bKZLZ7hwY2Urf1o1Gi9OPGyo5zuJZAUQInU%2bkJKU
6ycXHZo17Uti3DITCy0%2fG%2bQ2gixzBIpmJctekKJO243rZiU1wbOUPWLzGum8ydRu3im2LiDisXquAu7ipY5P0D475AZN
3Cd6nlIPP5MORA493QhX4I139q%2birT1%2f5F7tI%2fKLv20FWFC%2fjKbfu%2bFe4QIbdtiSCvLkyZ%2bWdWBMWSXHGE11
CoErbj4LJP3h4oqLto17riGcYmb%2bRHZXXNJA2bwjcfgy4w2FE4hrL0cC6D3YgZxHHpUeT4gMxOxj0EJwODxQwElc9yfoe%2
bdGj4Fy6%2fXc0ymDFYU7oOouAc0nwPKZwhZn43mMzIG5aeOFcx9IM6M47IcMMbo0r78aUk8M94h5f4sK6JxHz75B6JyTx3
H%2bxFDJ3j5UtUYjloir4CLQJgR8AbhMDGxqhAN4c4wa4y790bh2F5PxxVXMGYb4ghFNt3jIHGXRMENPTYkelnd0falMmhJ
UXE%2fVashJ8aZwcGCU%2fNhSkCATRXb5UDameaSkwe3m4bcRtFbBNZ115CNQVH8ZPZsK1GCNpD6dOYkSxa%2ffErYqImEzm
9itwSzUujQXI%2f8%2f%2fKewc9jeBujwHqnjuIYg5sJbjk%2bqc%2fwy5hKHTbxFacnFJ1gvJhHt3mht8oRC9EbbSULOAK1
fvLe4%2fe%2bqfJ0e02bw4sQuu1ssMKxLsNQMCTIZFzh10K6BZdfolRonKGOMEg1K%2ftSDNC4eyQw9ewYhgzopzDVHwlyprp
VY9UgcTvFVSh0Vy%2bwde4b0dtmPdhhQhvvsQOSgnxIX6a8GN4AwXEOE7CoP6%2fFZiTAJTuxUKMjC1m8iAsrAurJugnEgaK
KugSNk19y7bgSiYB6zkthDclEyBFWclrAecfH6oMJs59aJodXnPSAA9FuyqLCWB%2f3WFZ03efhTviz2101G8%2fSWMxR0w%
2fR56oNH2wzUwkmh9oczFaYLPJpZg6k47ohlzmDJraqyVwGzzfPIipa7EKK8Yvsu04BCFGMrDZtYZnCO6B9CFoKDCNJE9Wxl
%2bhTdzFCA4GpeLE4nT7y1j113iTV%2faWyImNLARMU2ZiwuKy%2bd2OH55LqnLBCxrUUMH7Ku4Mhd%2fYvwlNVpcZZ0L%2
bWOkMoephk2XXE4OQAY7Rk%2f%2fRncbbHlFOVQmEVOoxNneBElleajK%2fxX6C0BZBaebAVYluwdGkkktvgQ5gUvzMiyyqbs
vzyUMzq%2fhqKY7vVMWUeyCsBnybuGPSILJIKMgdgjiz%2baUZsOyZsUE%2b7PPyiqphqXNRfQ6tj8wTzq7a2Z5XgCYI10Pi
qjlmg6hY1TiRYuPanyBqh61LfkxblkpQJX2339ppqB4RBOzF4%2f3CsvfjU302NSU9fypX5dBYubAZt80DOBe84FSnQIX3pfX
2%2fW9LqclyWbxC2QSOfoHoe6TgkCiOall%2fqUHWqeOogbgLO5s5ffBoNmUCxhJW%2fH1EqKcsFzA%2ba%2f2Q0%2bs2m99R
qlxdd55bg67LXVPGfKh2dbVHjghXj090nLEtVwCfs8oMUIg%2bmnip%2fdA7wDz4Nsma2W0ugEh0jpfFbL2TxHLhE0r%2bwY
3t%2bosvtaxNJZg84LJKpt3J%2bmc0pnIBH5S5H7zrNDKUnIYXY8BD5n1clzi4wwkRIp62avJw7lN22zNHs.jp7NUjTYw9X%2
f1Iti1TKxjPZuitU%2bITeCRRHzeoaeGbzE1E%2bGSSqemw7F1wx4w9JXHDAjH%2bY4iX7z2Y4OrY1JQQleeS9KWzw5HdiCp
uHmhMtLMSpz%2fGagw7KeaLEe9FwxrOYILS%2fXuBSTzIXOpbQHILH0ZdQbv2I%2bA%2f3j3GvalSul%2f0YVWlPPPIC2Ogk
SSbd4HyXXh9TEB8dhDmfucy5VEZ5MsuOTgytkALNSK0t9cyvsAcWTQf0uVAMnyBeaMPJAvdE9fXUiH628eMD9PHvt3cL0GYd
RR9WBUCszIFTJNIA5AXj7abdbbc6VZ8DqX4YfJ1xgTgg2qKSJqXvtbi5BJU49BGaxu01Ta6eBo2ABLTgBxKzb8DYNyqyqRB%2
bYkgr5YdU6z6va15jQJYGUJYVwZ8xDsKvYH1z1UFAHldzxxkq44myNAjD1H0DoYhQaXU120UXkg09w5kBqTfmKj9DOJhs5Q88
ilebAbHHxm3GTZSJP51jQjsPSU13doX3Mz8E7W5pYptxtW1XPwcSHhkxuhWjbVKKQRTgM5uSXCPQ0PDAqcc6NybV2t1BK3G
hQSPzsQ5k3wklDK7CYUWMPKTMNLZDVF8i25DoGpA0K5m5s3VMAukLA9Gob5ysU%2fsu2TVBrJZD0sa3L%2bNoF2b01f8BC3
2e.

Date : 01/04/2017
Time : 20:04:41
Type : Unknown
Source : acise

Description : Function: hs_transport_winhttp_post
Thread Id: 0xD3C
File: hs_transport_winhttp.c
Line: 5776
Level: debug

unable to send request: 12029.

Date : 01/04/2017
Time : 20:04:41
Type : Unknown
Source : acise

Description : Function: HttpHandler::createOutgoingHTTPSMessage
Thread Id: 0xD3C
File: HttpHandler.cpp
Line: 295
Level: debug

MSG_NS_HTTP_RESPONSE, {{success=0}, {pkt=""}, {type=1}}.

Date : 01/04/2017
Time : 20:04:41
Type : Error

Source : acise

Description : Function: Authenticator::parsePostureData
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 257
Level: error

Failed to communicate with CAS..

Date : 01/04/2017
Time : 20:04:41
Type : Error
Source : acise

Description : Function: SMNavPosture::SMP_handleMonitorResp
Thread Id: 0xD3C
File: SMNavPosture.cpp
Line: 495
Level: error

Failed to parse monitor response.

ISE werpt "ongeldige" fout af bij het maken van App-naleving vanuit EP-weergave

De meest voorkomende reden om tijdens de creatie van App-conformiteit vanuit EP-oogpunt "nul" te hebben, is het ontbreken van vereiste OPSWAT-kaarten. Los dit probleem op in de meest recente versie.