تكوين إعداد العميل وتطبيقه 2.2

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين إمكانية رؤية التطبيق على Identity Service Engine (ISE) 2.2 واستكشاف أخطائها وإصلاحها. تتيح لك إمكانية رؤية التطبيقات إمكانية مراقبة التطبيقات المثبتة على نقاط النهاية، وإنشاء سياسات تستند إلى هذه المعلومات،

وقل التطبيقات أو إزالة تثبيتها أثناء عمليات التحقق من الوضع إذا كانت تفي بشروط محددة. يرسل AnyConnect بشكل دوري معلومات إلى ISE باستخدام قائمة بالتطبيقات والعمليات المثبتة/الجارية تشغيلها. يمكن ل AnyConnect جمع معلومات حول جميع التطبيقات أو التطبيقات من فئات محددة (المستعرضات والتشفير، وما إلى ذلك).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بالمواضيع التالية:

- محرك خدمة الهوية من Cisco
- إمداد العميل
- ISE Posture

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Identity Service Engine، الإصدار 2.2.0.470
- Cisco AnyConnect 4.4.00243
- وحدة التوافق مع AnyConnect 4.2.468.0
- حزمة الخدمة 1 لنظام التشغيل Windows 7

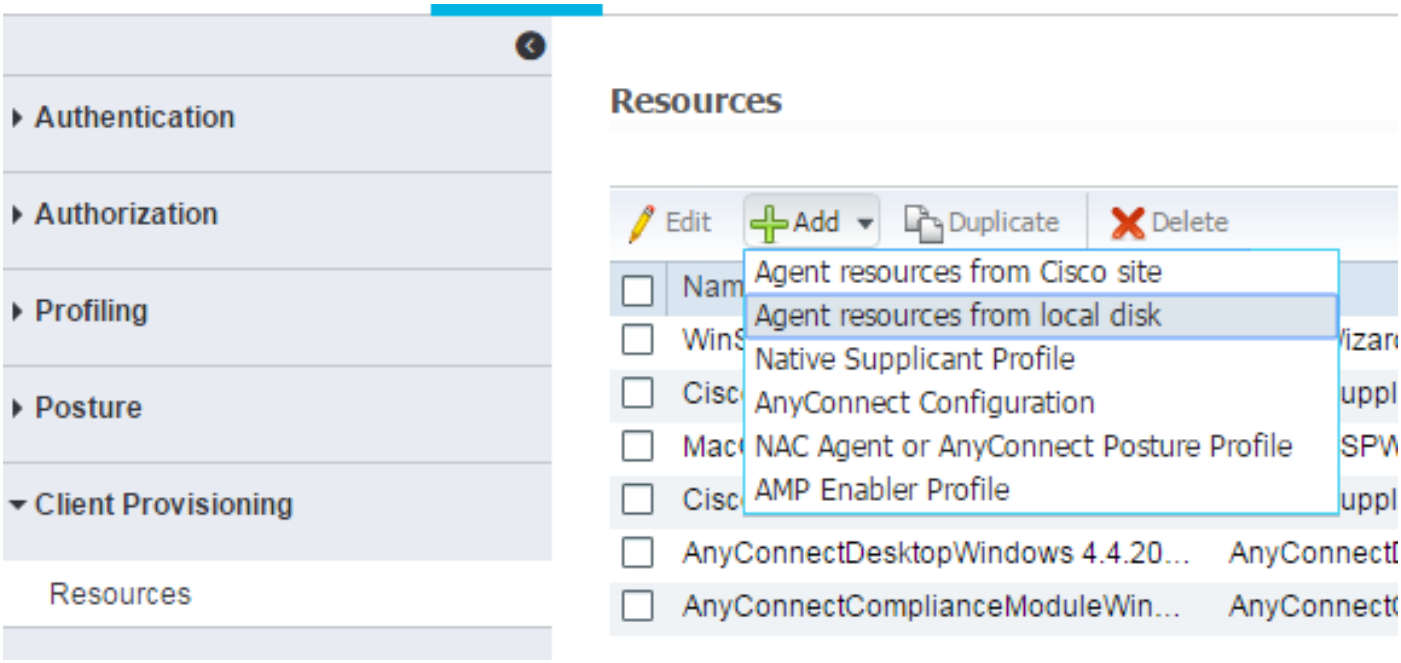
التكوين

التكوينات

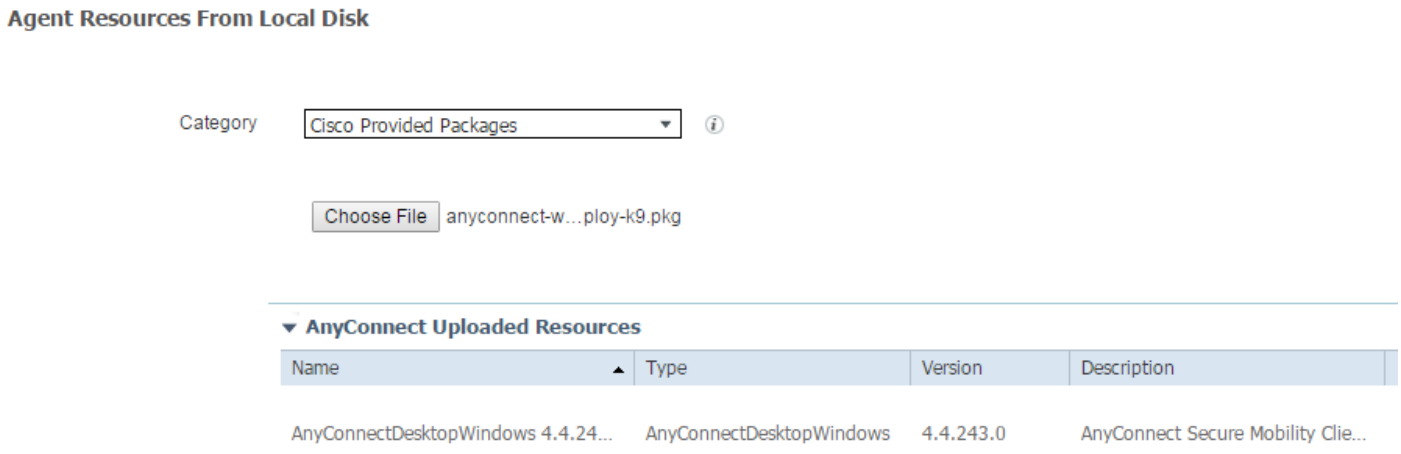
الباب 1. تكوين إمداد العميل

الخطوة 1. تحميل حزمة AnyConnect

1. انتقل إلى **السياسة > عناصر السياسة > النتائج > إمداد العميل > النتائج** على ISE. انقر فوق **إضافة > موارد الوكيل من القرص المحلي**:



2. حدد **الفئة** كحزم مقدمة من Cisco **واختر ملف** (حزمة AnyConnect):



انقر فوق **إرسال** لحفظ التغييرات.

> يجب أن يطلب منك تأكيد المبالغ المرجعية للحزمة التي تم تحميلها. قارنهم بمبالغ التحقق المقدمة على موقع Cisco على الويب لضمان عدم تلف الحزمة.

الخطوة 2. تنزيل وحدة توافق AnyConnect

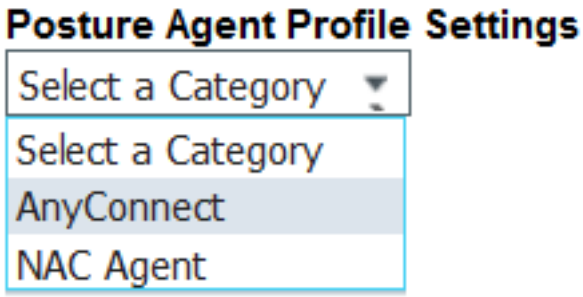
في صفحة نتائج توفير العميل، انقر فوق **إضافة > موارد الوكيل من موقع Cisco**، حتى تتمكن من تحديد الوحدات النمطية المتوفرة. حدد **وحدة التوافق النمطية** المطلوبة **لـ AnyConnect** لنظام التشغيل Windows وانقر فوق **حفظ**.

> بدلاً من ذلك، إذا لم يكن لديك اتصال بالإنترنت على نظام التشغيل ISE الخاص بك، فيمكنك تنزيل أحدث وحدة نمطية للتوافق من Cisco.com وتحميلها إلى نظام التشغيل ISE الخاص بك بنفس طريقة حزمة AnyConnect.

> إذا كان لديك وكيل في شبكتك، فقم بتكوينها في **الإدارة > النظام > الإعدادات > صفحة الوكيل**.

الخطوة 3. إنشاء ملف تعريف الوضع

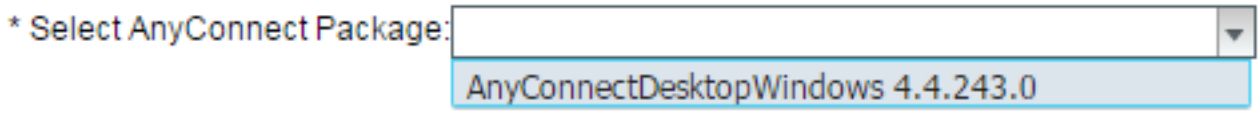
على صفحة نتائج إمداد العميل انقر على **إضافة > وكيل NAC أو توصيف AnyConnect** وحدد **Posture** من إعدادات ملف تعريف وكيل الوضع:



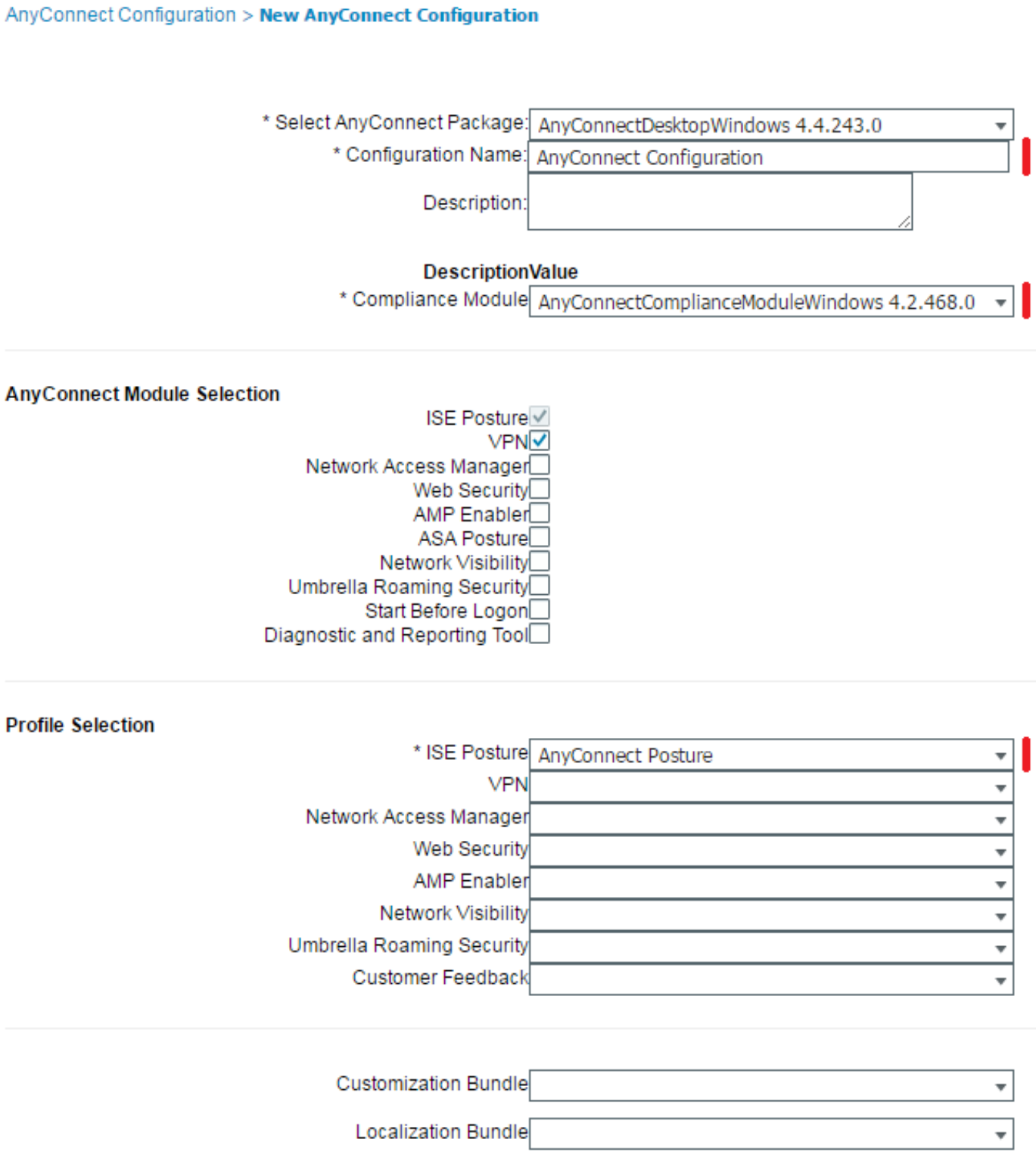
قم بتسمية حقول ملف التخصيص والتعبئة المطلوبة. انقر على **إرسال** لحفظ ملف التعريف.

الخطوة 4. إنشاء تكوين AnyConnect

في صفحة نتائج توفير العميل انقر على **إضافة > تكوين AnyConnect** وحدد الحزمة التي تم تحميلها في الخطوة 1:



يجب تحميل الخيارات الإضافية. قم بتعبئة كل الحقول المطلوبة وانقر فوق **إرسال** لحفظ التغييرات:



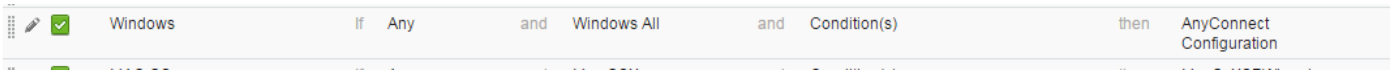
اسم التكوين - اسم التكوين. يتم إستخدام هذا في نهج إعداد العميل (الخطوة التالية).

وحدة التوافق - وحدة التوافق المحددة التي تم تنزيلها في الخطوة 2.

ISE Posture (وضعية محرك خدمات الهوية (ISE)) - حدد ملف تعريف AnyConnect Posture (وضعية محرك خدمات الهوية (ISE)) الذي تم إنشاؤه في الخطوة 3.

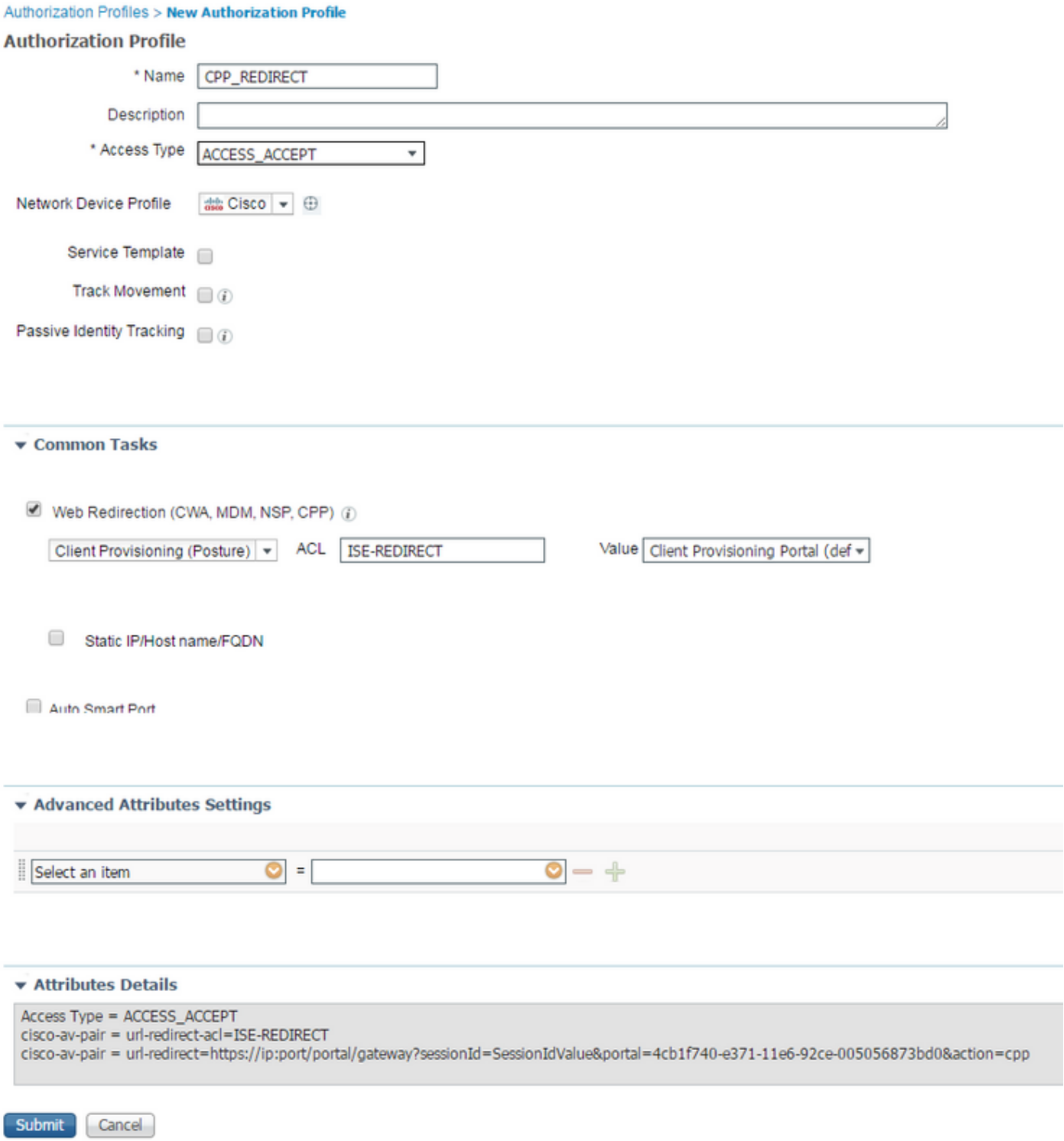
الخطوة 5. تكوين سياسات إمداد العميل

انتقل إلى **السياسة > إمداد العميل**. إنشاء نهج جديد أو تحرير نهج موجود ل Windows، وتحديد تكوين AnyConnect الذي تم إنشاؤه نتيجة لذلك:



الخطوة 6. إنشاء ملف تعريف التخويل ل CP

انتقل إلى **السياسة > عناصر السياسة > النتائج > التخويل > توصيفات التخويل** وانقر **إضافة** لإنشاء ملف تخصيص جديد. قم بتكوينه لإعادة التوجيه إلى مدخل إمداد العميل:



انقر على **إرسال** لحفظ التوصيف.

تذكر أنه يجب إنشاء قائمة التحكم في الوصول لإعادة التوجيه (في هذا المثال الذي يسمى **ISE-Redirect**) على NAD (جهاز الوصول إلى الشبكة) للحصول على إعادة التوجيه

المناسبة. يجب أن تعترض قائمة التحكم في الوصول الأساسية إعادة التوجيه حركة HTTP و HTTPS. يمكن العثور على عينة قوائم التحكم في الوصول (ACL) في هذه المستندات: [المركزية للويب مع مصادقة المركزية للويب على مثال تكوين WLC و ISE](#) و[مصادقة المركزية للويب مع محول مثال تكوين محرك خدمات الهوية](#)

الخطوة 7. تكوين سياسات التخويل

انتقل إلى **سياسة > تفويض**، وقم بإنشاء إثنين من السياسات مع التحقق من حالة الوضع:

☑	POSTURED	if	Session:PostureStatus EQUALS Compliant	then	PermitAccess
☑	CPP_REDIRECT	if	Session:PostureStatus NOT_EQUALS Compliant	then	CPP_REDIRECT

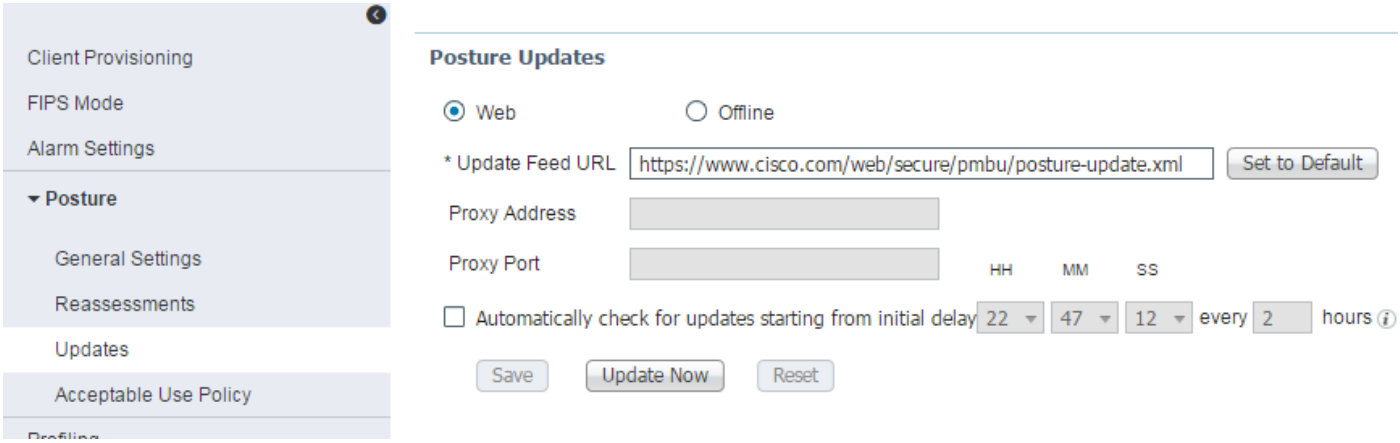
باستخدام هذا التكوين، إذا لم يتم تثبيت AnyConnect على نقطة نهاية أو لم تنتهِ من الوضع بعد، فسيتم إعادة توجيهها إلى مدخل إمداد العميل. يمكن للمستخدم النهائي تثبيت AnyConnect من ISE ويمكن لـ AnyConnect اكتشاف ISE والتحقق من وضع ISE.

طقطقة **حفظ**.

الباب 2. تكوين الوضع

الخطوة 1. تحديث الوضع

انتقل إلى **إدارة > إعدادات > وضعية > تحديثات** وانقر **تحديث الآن** لتحديث الحالة. وهو يحتوي على مخططات وتعريفات لنظام OPSWAT للتطبيقات وهو مطلوب لوضع السياسات.



بدلاً من ذلك، إذا لم يكن لديك اتصال إنترنت على ISE الخاص بك، فيمكنك تنزيل آخر تحديثات الوضع من https://www.cisco.com/web/secure/pmbu/posture-offline.html ثم الانتقال إلى **الإدارة > النظام > الإعدادات > الوضع > التحديثات**، حدد **غير متصل** وحدد الملف الذي تم تنزيله مع تحديثات الوضع. انقر فوق **تحديث الآن** لتحميل الملف وتثبيت تحديثات الوضع.

الخطوة 2. إنشاء شرط تطبيق

يقوم AnyConnect بجمع معلومات حول التطبيقات المثبتة فقط مع وحدة التوافق مع معيار 4.x (أو الأحدث).

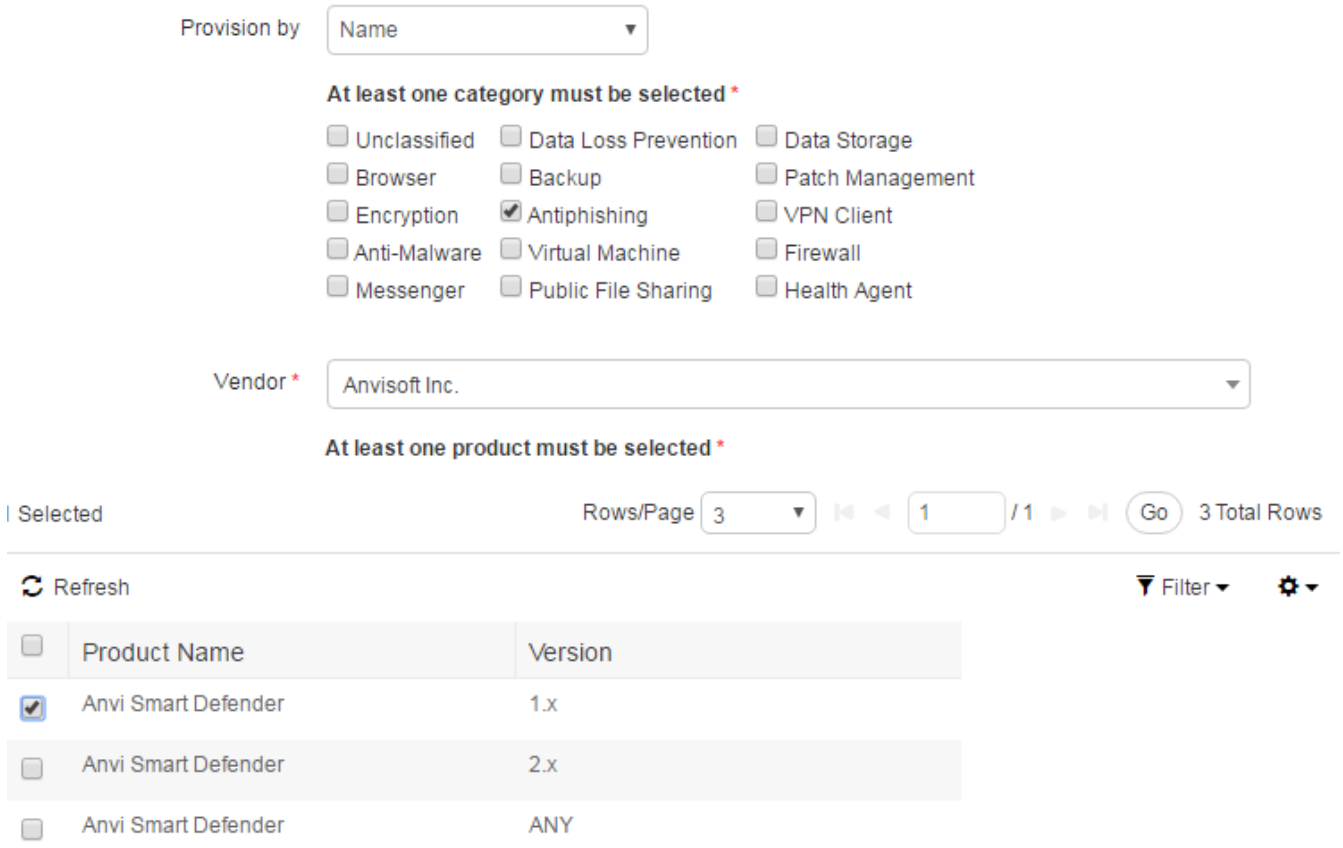
مع الإصدار 3.x من Compliance Module يمكن إجراء عمليات التحقق فقط (وهذا يعني أن AnyConnect يتحقق ما إذا كانت العملية المحددة قيد التشغيل أم لا).

مع **حالة التطبيق** يمكن تكوين هذه المجموعات:

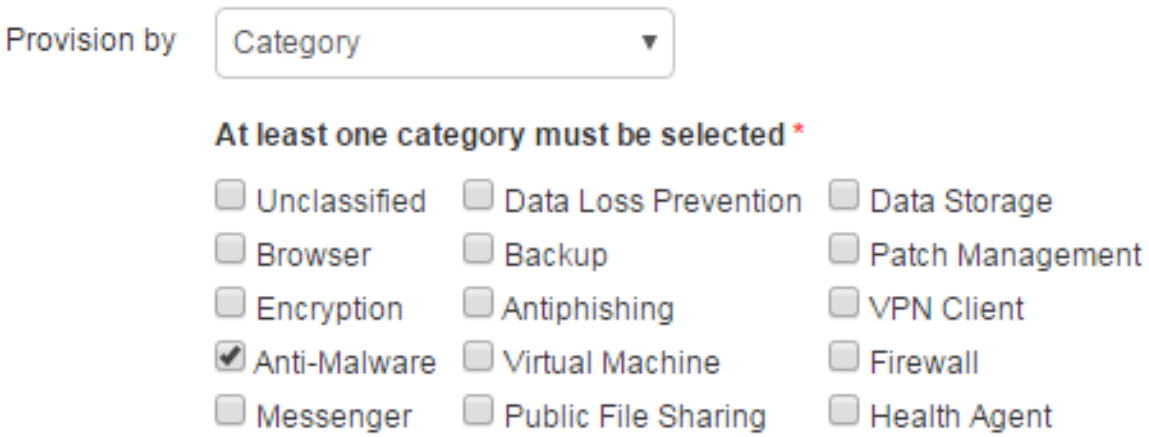
- مثبت + قيد التشغيل - يقوم AnyConnect بتجميع معلومات حول العمليات الجاري تشغيلها حاليا من خلال جمع معلومات التثبيت
- مثبت + لا يعمل - AnyConnect يجمع معلومات التثبيت فقط

مع **توفير حسب** لكل الفئة: **كل شيء**، **الاسم** و**الفئة**:

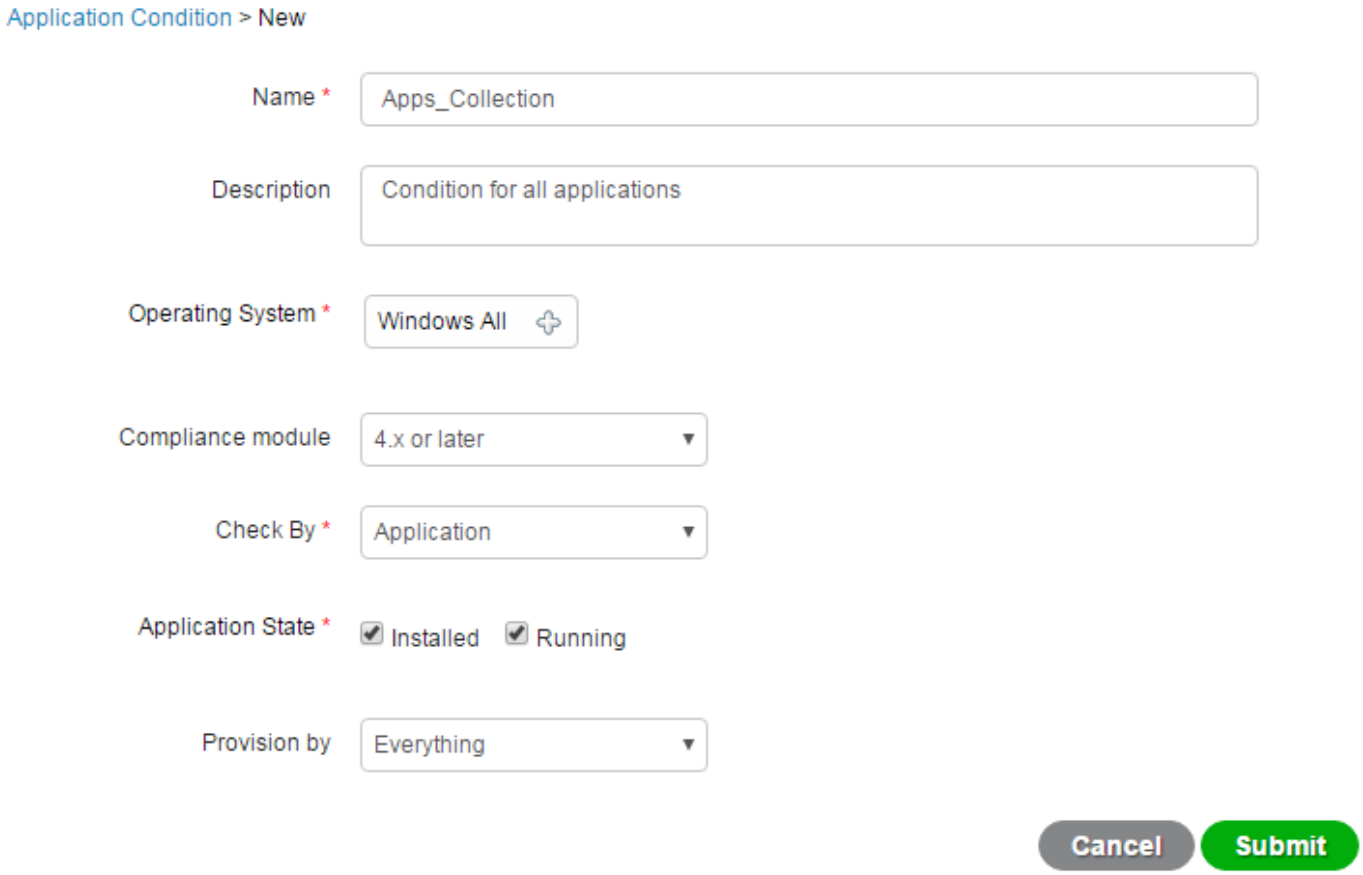
- في حالة تحديد **كل شيء** فسيحاول AnyConnect جمع معلومات حول جميع التطبيقات المثبتة
- في حالة تحديد **الاسم**، يمكن تحديد تطبيق معين للنهج. على سبيل المثال:



- إذا تم تحديد **فئة**، فإن AnyConnect يقوم بتجميع معلومات حول جميع الأجهزة من الفئة المحددة. على سبيل المثال:



من أجل جمع معلومات حول التطبيقات المثبتة التي يتم تشغيلها في **النهج > عناصر النهج > الشروط > الوضع > حالة التطبيق**، انقر فوق **إضافة** لإنشاء شرط جديد وتعبئة الحقول المطلوبة كما هو موضح:



الخطوة 3. إنشاء متطلبات الوضع

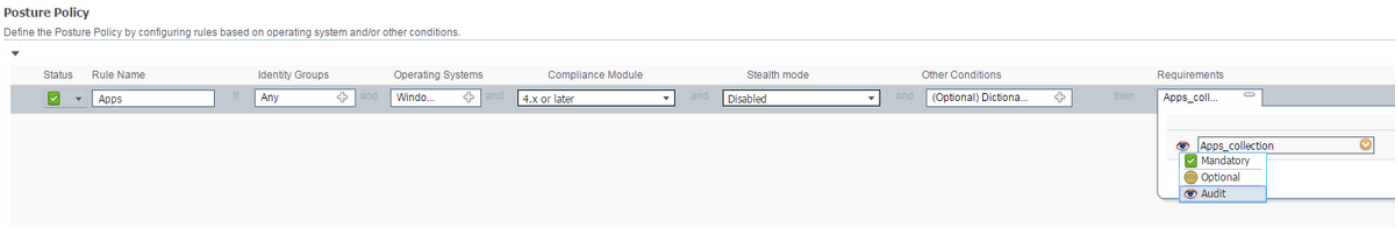
في **السياسة > عناصر السياسة > النتائج > الوضع > المتطلبات** قم بإنشاء متطلب جديد مع حالة التطبيق التي تم إنشاؤها:

Requirements

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

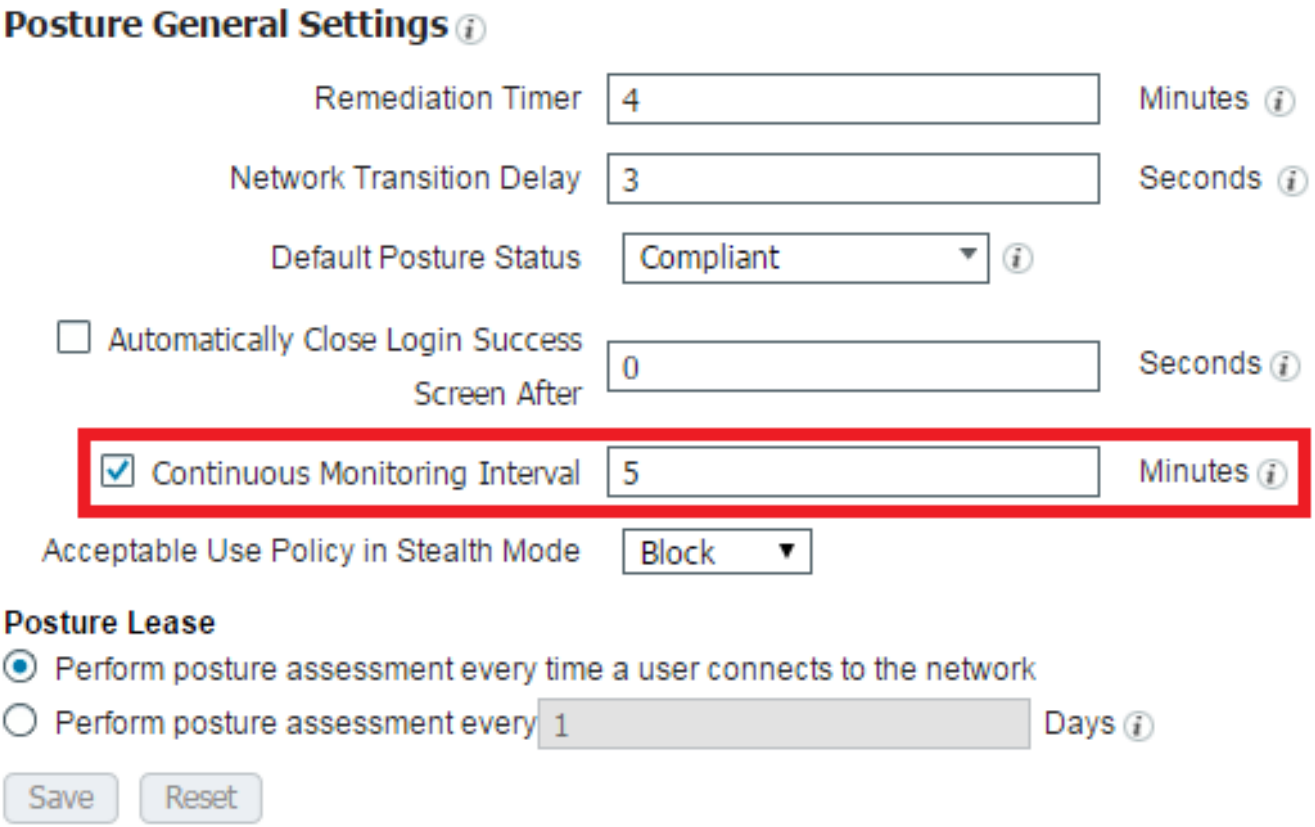
الخطوة 4. إنشاء نهج الوضع

لتمكين ISE و AnyConnect من جمع معلومات حول التطبيقات، يجب تضمين أحد المتطلبات مع أحد شروط التطبيق في نهج الوضع. يمكن إنشاء نهج الوضع في **النهج > Posture**. قد يتم تعيين المتطلب على أنه **تدقيق** إذا كنت ترغب في جمع معلومات لمزيد من الاستخدام.



الخطوة 5 (اختيارية). تغيير الفاصل الزمني للمراقبة المستمرة

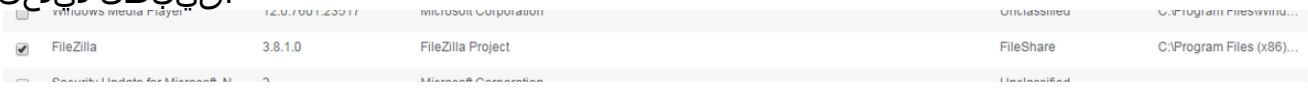
يسمح ISE لك بتكوين عدد المرات التي يجب فيها على AnyConnect إرسال تحديثات حول التطبيقات إلى ISE. بشكل افتراضي يتم تعيين الفاصل الزمني إلى 5 دقائق ويمكن تغييره في **إدارة > إعدادات > وضعية > إعدادات عامة**:



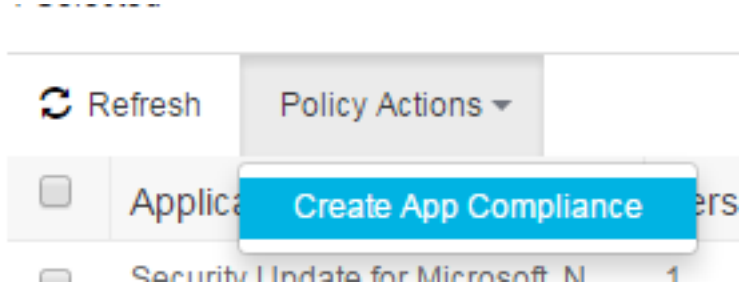
الخطوة 6 (اختيارية). إنشاء توافق مع التطبيقات

بعد تجميع البيانات من نقطة النهاية، يمكن إنشاء التوافق مع التطبيقات في **رؤية السياق > نقاط النهاية > [نقطة النهاية]**:

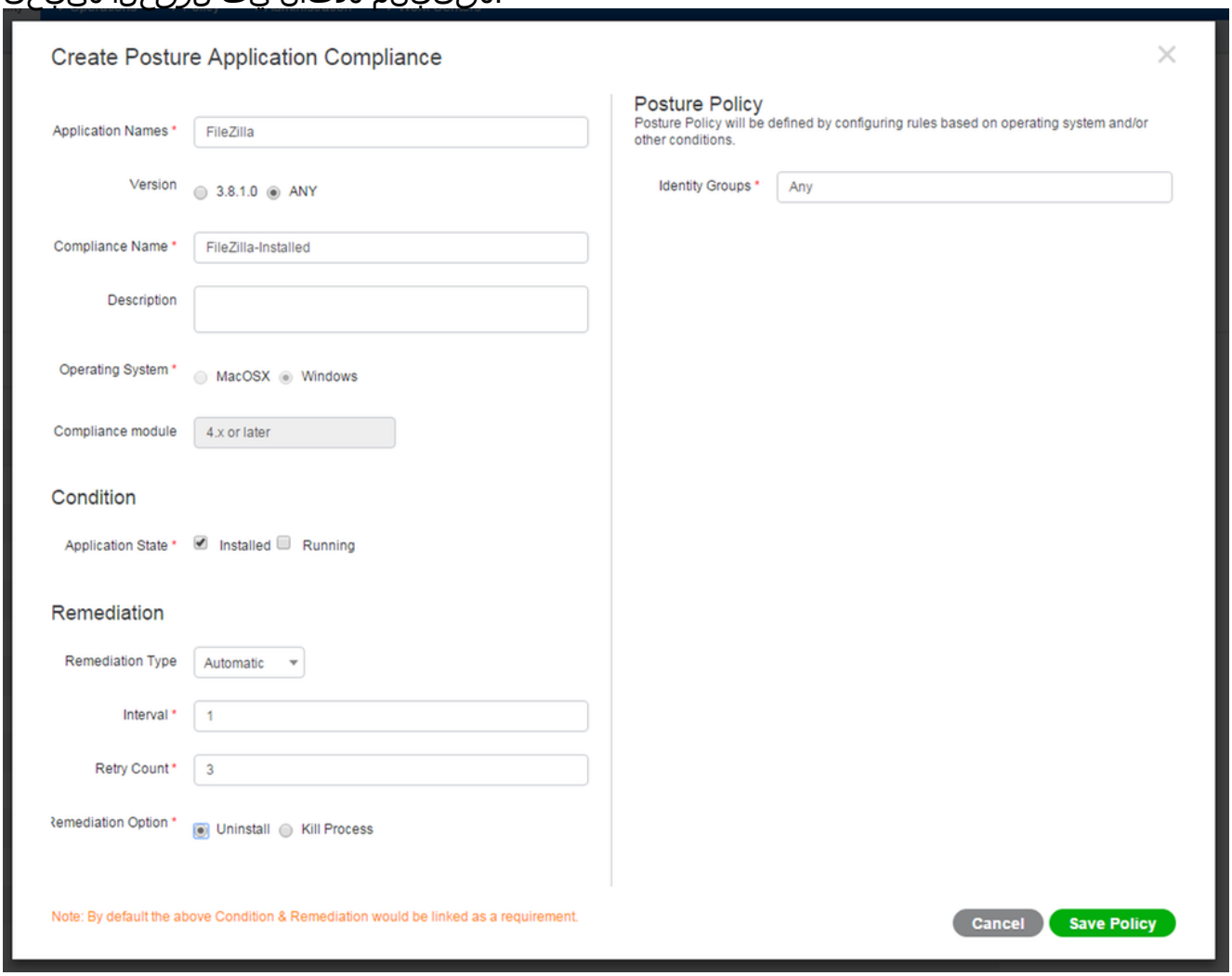
1. تحديد تطبيق:



2. انقر فوق **إجراءات النهج > إنشاء توافق مع التطبيقات**



3. تعبئة الحقول في نافذة منبثقة:



4. انقر فوق **حفظ النهج**، يجب إنشاء العناصر التالية: شرط تطبيق الوضعإجراء معالجة تطبيق الوضعمتطلب الوضعنهج الوضع

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

LiveLog

في RADIUS LiveLog يبدو التدفق مثل تدفق الوضع المعتاد: **المصادقة + إعادة التوجيه إلى مدخل التزويد > تغيير التفويض (CoA) > مطابقة سياسة الوضع المتوافق.**

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Posture St...	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address
				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	

نقطة النهاية

بعد إمداد العميل (إذا لم يتم توفير AnyConnect من قبل) وتكوين فترة المراقبة المستمرة، يمكن التحقق من عملية جمع البيانات في **رؤية السياق > نقاط النهاية**. انقر فوق عنوان MAC لنقطة النهاية، ويجب أن تفتح صفحة نقطة النهاية. يحتوي على معلومات حول التطبيقات المثبتة على نقطة النهاية نفسها:

C0:4 :8

MAC Address: C0:4 :8
Username: cisco
Endpoint Profile: Microsoft-Workstation
Current IP Address: 10 62
Location: Location ➔ All Locations

Applications | Attributes | Authentication | Threats | Vulnerabilities

Refresh | Policy Actions | Filter

Application Name	Version	Vendor	Running process	Category	Install Path
Security Update for Microsoft .N...	1	Microsoft Corporation		Unclassified	
Security Update for Microsoft .N...	1	Microsoft Corporation		Unclassified	
Microsoft .NET Framework 4.6.1	4.6.01055	Microsoft Corporation		Unclassified	C:\Windows\Microsoft....
Google Update Helper	1.3.24.15	Google Inc.		Unclassified	
Windows Update Agent	7.6.7601.19161	Microsoft Corporation		PatchManagement	C:\Windows\System32\
Cisco AnyConnect ISE Complia...	4.2.468.0	Cisco Systems, Inc		Unclassified	C:\Program Files (x86)...
DAEMON Tools Lite	4.49.1.0356	Disc Soft Ltd		Unclassified	C:\Program Files (x86)...
Tftpd32 Standalone Edition (re...	0.0			Unclassified	
Security Update for Microsoft .N...	1	Microsoft Corporation		Unclassified	
VMware Tools	9.4.15.2827462	VMware, Inc.	2	Unclassified	C:\Program Files\VMw...
BitLocker Drive Encryption	6.1.7600.16385	Microsoft Corporation		DiskEncryption	C:\Windows\System32\
Cisco AnyConnect Diagnostics ...	4.4.00209	Cisco Systems, Inc.		Unclassified	C:\Program Files (x86)...
Cisco AnyConnect Secure Mobi...	4.4.00209	Cisco Systems, Inc.	5	Unclassified	C:\Program Files (x86)...
Java Auto Updater	2.8.91.15	Oracle Corporation		Unclassified	
Mozilla Firefox	47.0.2	Mozilla Corporation		AntiPhishing,Browser	C:\Program Files (x86)...
Microsoft Visual C++ 2008 Redi...	9.0.30729.4148	Microsoft Corporation		Unclassified	
Java 8 Update 91	8.0.910.15	Oracle Corporation		Unclassified	C:\Program Files (x86)...
Google Chrome	55.0.2883.87	Google Inc.		AntiPhishing,Browser	C:\Program Files (x86)...
Cisco AnyConnect Profile Editor	4.1.08005	Cisco Systems, Inc.		Unclassified	C:\Program Files (x86)...
Java	8.0.910.15	Oracle Corporation		Unclassified	C:\Program Files (x86)...
Internet Explorer	11.0.9600.18524	Microsoft Corporation		AntiPhishing,Browser	C:\Program Files\Inter...
Wireshark	1.10.7	The Wireshark developer comm...		Unclassified	C:\Program Files (x86)...
Windows Backup and Restore	6.1.7600.16385	Microsoft Corporation		BackupClient	C:\Windows\System32\
Windows Media Player	12.0.7601.23517	Microsoft Corporation	1	Unclassified	C:\Program Files\Wind...
FileZilla	3.8.1.0	FileZilla Project		FileShare	C:\Program Files (x86)...
Security Update for Microsoft .N...	2	Microsoft Corporation		Unclassified	
Java 7 Update 79	7.0.790	Oracle		Unclassified	C:\Program Files (x86)...

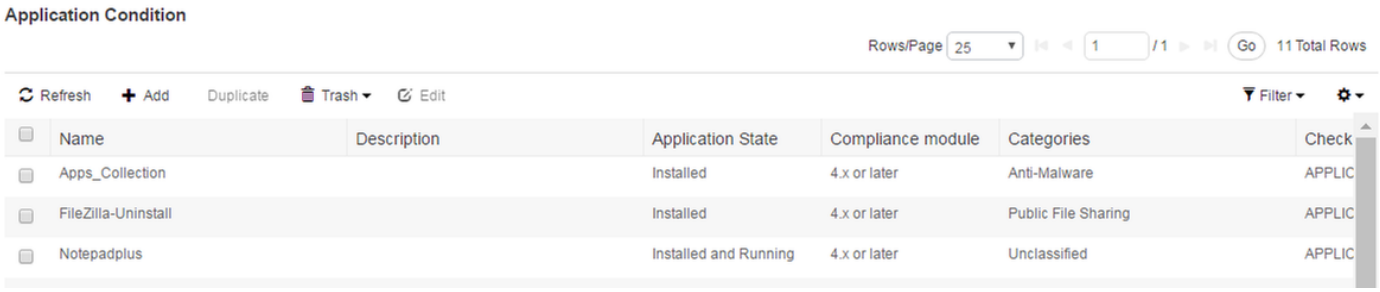
بسبب CSCve82743، ستحتاج إلى الوصول إلى نقطة النهاية مرتين واضغط على تحديث لتقديم جدول التطبيقات.

عناصر سياسة الوضع

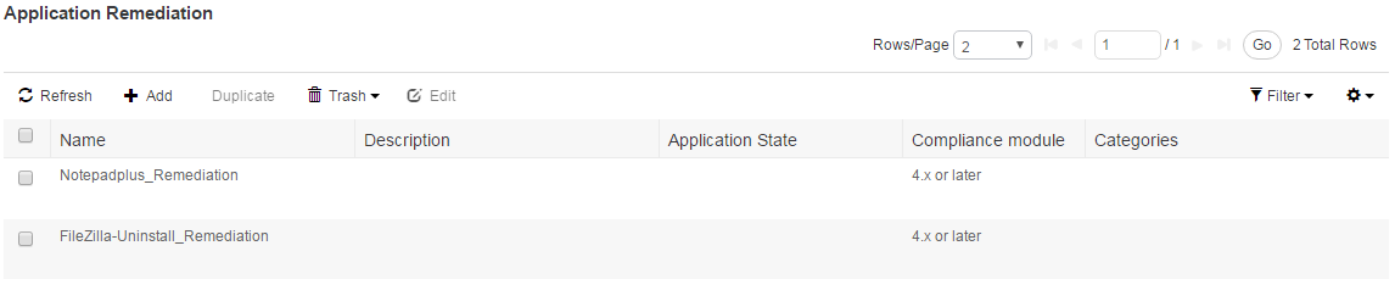
يجب إنشاء هذه العناصر باستخدام خيار **إنشاء التوافق مع التطبيقات**:

- شرط تطبيق الوضع
- إجراء معالجة تطبيق الوضع
- متطلب الوضع
- نهج الوضع

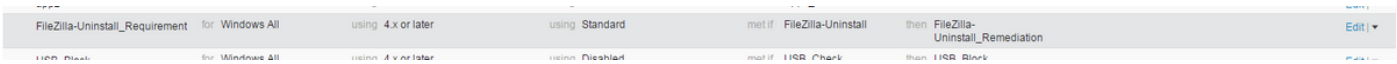
ويمكن التحقق من كل منها من واجهة المستخدم الرسومية ISE GUI. توجد **الشروط** في **السياسة > عناصر السياسة > الشروط > الوضع > حالة التطبيق**:



العلاج موجود في **السياسة > عناصر السياسة > النتائج > الوضع > إجراءات المعالجة > إصلاح التطبيق**:



توجد **المتطلبات** في **السياسة > عناصر السياسة > النتائج > الوضع > المتطلبات**:



توجد **السياسات** في **السياسة > الوضع**:

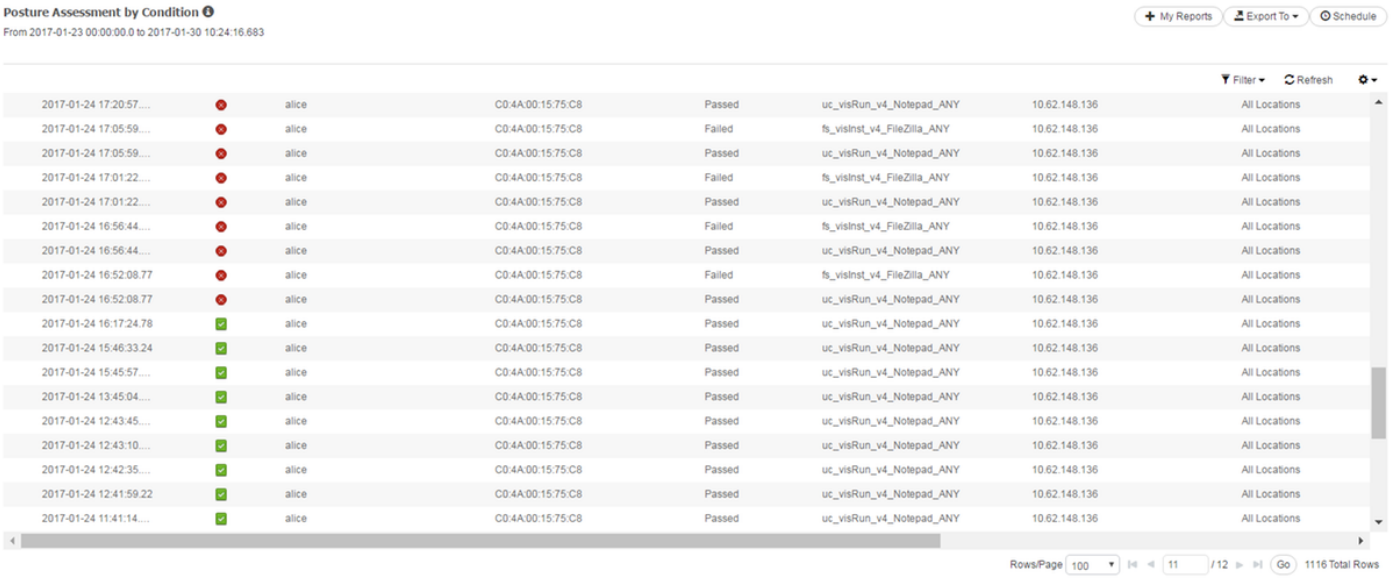
تقارير

يتم تخزين كل تقرير حالة من كل EndPoint على ISE ويمكن فحصه من **العمليات > التقارير**. هناك أشكال مختلفة من تقارير الوضع:

- تقييم الوضع حسب نقطة النهاية - يوفر تفاصيل حول توافق الوضع لنقطة نهاية معينة.
- تقييم الوضع حسب الحالة - يوفر تفاصيل حول شروط سياسة الوضع. فهو يعرض الشروط التي فشلت والشروط التي تم تمريرها. يتم عرض الشروط الإلزامية والاختيارية فقط.

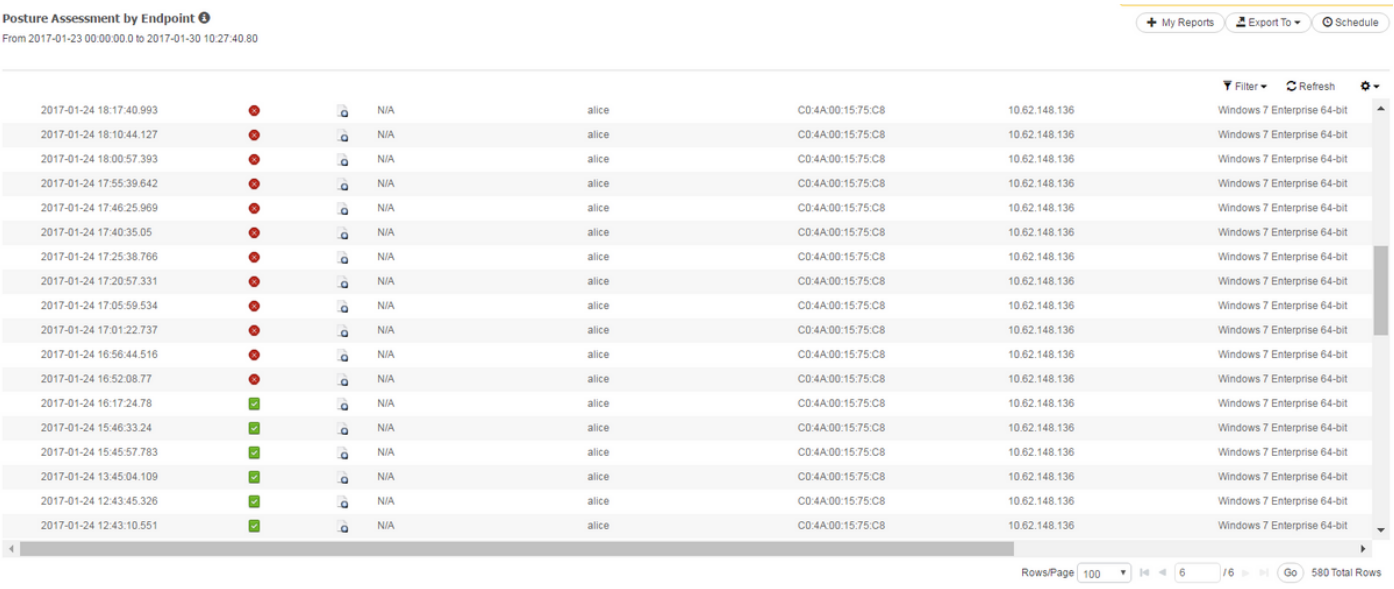
تقييم الوضع حسب الحالة

يظهر تقييم الوضع حسب الحالة كما هو موضح. في هذا المثال، يفشل أحد الشروط الإلزامية حتى تذهب حالة الوضع إلى غير متوافق:



تقييم الوضع حسب نقطة النهاية

تقييم الوضع حسب نقطة النهاية:



يمكن التحقق من تفاصيل كل تحقق للوضع بالنقر على أيقونة **تقرير التفاصيل** -

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

من ISE

يحتوي ISE-psc.log على جميع المعلومات المتعلقة بالوضع، بما في ذلك تصحيح الأخطاء.

يمكن تمكين تصحيح أخطاء الوضع في **الإدارة > النظام > التسجيل > تكوين سجل التصحيح**. اسم المكون هو **posture**:

بمجرد توصيل نقطة نهاية بالشبكة واتصال AnyConnect بشبكة إيثرنت، يتحقق ISE من أنه يجب فحص EP مقابل عمليات فحص الوضع التي تم تكوينها، كما يكتشف إصدار وحدة التوافق النمطية التي تم تثبيتها على EP. استنادا إلى المعلومات المجمعة، يقوم ISE بإنشاء استعلام الوضع ل EP - **عميل NAC xml** وتشفيره. لاحقا، يرسل ISE هذا الاستعلام إلى 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,runnning, 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>12</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>12</category>
      <type>1202</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>12</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>12</category><type>1202</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 - 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/J93PtAYU0XLq451NXQhReuFktImYEPEnWwOs1bV5oOTuTsY3kEbcuR4p5Sp0cfz/j98YEubNtSKDCUGt5U8dhpOJqMYTV4UcaSP/D0FXYm10gFEjPxpPghyWcplzYwcpehIX+2vOYOSzPTEvM2kDdHTkof+/UYvBfGv8Y7YkK9P61upfSedIqdynyxUbeqknXkoCaWvUawJLVWiXAJs2atsCwJjXitwNHYzCuH/mBz/Y9AUvbLCB/cutCeyVCl7ij8wtXUAt2NpKqeEj0COOxnp5B35JTBfOSXHfVjL29E5JALaun6RR8yJlkd4apk7qflnjsu451CHY/SbKTMnqjV5bNwXfuCBf++X6X/mh0nwk+r2iWhJJFyqmNxBm2BvcJAJXOKOV7xHIhgmLj+etF4Sss/zwnFT4+WTzKI+BpbrVdnZjUP7+uvbQbIPtRFqJVI5StjZlIP4vLzFWKbWXI+itTX6hjqvNhiT2zwktvIboUZXaBV6yS5/+5cYMU3+EhWxIx/UVo0o7sX--><!--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:::- S**ending 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/J93PtAYU0XLq451NXQhReuFktImYEPEnWwOs1bV5oOTuTsY3kEbcuR4p5Sp0cfz/j98YEubNtSKDCUGt5U8dhpOJqMYTV4UcaSP/D0FXYm10gFEjPxpPghyWcplzYwcpehIX+2vOYOSzPTEvM2kDdHTkof+/UYvBfGv8Y7YkK9P61upfSedIqdynyxUbeqknXkoCaWvUawJLVWiXAJs2atsCwJjXitwNHYzCuH/mBz/Y9AUvbLCB/cutCeyVCl7ij8wtXUAt2NpKqeEj0COOxnp5B35JTBfOSXHfVjL29E5JALaun6RR8yJlkd4apk7qflnjsu451CHY/SbKTMnqjV5bNwXfuCBf++X6X/mh0nwk+r2iWhJJFyqmNxBm2BvcJAJXOKOV7xHIhgmLj+etF4Sss/zwnFT4+WTzKI+BpbrVdnZjUP7+uvbQbIPtRFqJVI5StjZlIP4vLzFWKbWXI+itTX6hjqvNhiT2zwktvIboUZXaBV6yS5/+5cYMU3+EhWxIx/UVo0o7sX--><!--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: 0a3e946500000066586d3c42, 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: 0a3e946500000066586d3c42, 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 0a3e946500000066586d3c42

التقرير الكامل من AnyConnect. يحتوي هذا التقرير على معلومات حول كافة التطبيقات التي تم العثور عليها والتي تطابق حالة التطبيق التي تم تكوينها.

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\Flash\</path><categ
ory>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\</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>7FA4B3B6F688642E800AD53B865DBDCC163FBCA92D83482248DB068BA42192EA</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><path>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</category></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><application><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><application><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><application><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><application><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><application><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><application><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></application><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:\program 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><application><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:\program 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
>]]
...

كافة التقارير هي سلاسل XML. نموذج تقرير منسق:


```
<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>
```

يرسل AnyConnect تقاريك املة عند أول اتصال فقط. كما أنها ترسل التغييرات فقط. على سبيل المثال، تم بدء تشغيل Notepad++ بعد بعض الوقت:

```
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> ]]
```

منسق:

```
<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>
```

من AnyConnect

يحتوي الملف AnyConnect_ISEPosture.txt على جميع السجلات ذات الصلة وتصحيح الأخطاء. يمكن العثور على هذا الملف في حزمة DART التي تم تجميعها على نقطة نهاية. هنا مثال لتقرير دوري، يتم تشفيره باستخدام AES256:

```
****************************************

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%2d1&udid=766bb955e51e4ab063fd478c63acee81260ca592&dm_report_client_IV=Jj
neGgZcJbmjqMKQcy8kJg%3d%3d&dm_report=2yWwY7QzHWCY%2fDVEESSAabEZtYLtxNE7QgyOOa85Dgo2Ts4ok8sIrBM37
S2%2fe2Hs0URCP4KkfY4Ap8%2bh%2fqS%2biw50CZejKG%2bVbF7RTRqZyrg2veWAwvEDsSb%2bqWRRdzvZfSjS3G4ApQi07
qnfExwN1IvCqrVOplj17TAcVXEht8NkDg0OT9jM%2fTNH%2fMKllc0o6Ha5juJo4YtWDWY%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%2fDVEESSAabEZtYLtxNE7QgyOOa85Dgo2Ts4ok8s
IrBM37S2%2fe2Hs0URCP4KkfY4Ap8%2bh%2fqS%2biw50CZejKG%2bVbF7RTRqZyrg2veWAwvEDsSb%2bqWRRdzvZfSjS3G4
ApQi07qnfExwN1IvCqrVOplj17TAcVXEht8NkDg0OT9jM%2fTNH%2fMKllc0o6Ha5juJo4YtWDWY%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}}.
```

المشكلات الشائعة

يتعذر على AnyConnect الوصول إلى ISE

في هذه الحالة يحتوي AnyConnect_ISEPosture.txt على أخطاء:

```
****************************************

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%2fDVEESSAabEZtYLtxNE7QgyOOa85Dgo2Ts4ok8s
IrBM37S2%2fe2Hs0URCP4KkfY4Ap8%2bh%2fqS%2biw50CZejKG%2bVbF7RTRqZyrg2veWAwvEDsSb%2bqWRRdzvZfSjS3G4
ApQi07qnfExwN1Pdu7AztTn%2f3VYph9WNF1jGljXSuTFmr38e%2bvDXQnx7avYHs9meVItYqA6MecAJK3WdkBNSrK1bYjmI
vzkAPqR2LuoflnA9IcNOTZQ9iN%2fknOjlLqsiV5eV6jlMSUeOakKsTwy1gbPsFz99eKdtaCMv1F%2fsAmvLApjpke0IMKor
XXkvpJURtAtOMK75ltXdykC85ihgHcI10JW7mlpvIppk5MbCZjihQbXldr5%2fQVdpB8eRqMHF1iCK1gx96lwwdzBSfr%2bg
rcF4072fYYNOa9cYnTFShgU%2bxrnBDcJ1GUoYE9K5nTfGQ01p4NrcbLjpM79e14v14YgfQhmSfktwxfA8pY7A6jmL3BIp3O
```

9gmQVnoTqaaccqkW76uT%2bPkjVOyrOgdG0CYwUwUMVqpctGKorxx1C3IwXhBWUmvRY9p2LRdePRqnCN8hpiesyk%2bzTnyX
0OaNdHD6%2bGEMGo9QjQvwrL9dcvrUxxHtlQcJPekXajXPfn98FpC8z%2b966tcz4DfMN6giSlEfK6y5%2bMpk0oAL%2fV4X
Mg296PDocGaeTK1OUR7Qkl%2b7S2fv%2fCfZdiQaTndZ6zHWuimq5JBRElmuKI9hWRN2cPERcDn64ISZZSiz9yPoJPlPPpFs
fggkc2PdS0OEEtMiM%2bBjNKcFx2Tcsq76eYfDtvDq9tGzjST8opInlIiXdAzdbeWsjCAerCvS73xg2vd2DHfpFlrd5lVa3q
wo3Vov3nFiAz4l3IrI1fOHjAE7rCZTy2dWU455icOjmO%2bCVAS3SzWCea4fZu3fAhmIhAVQKE1cFZ4CyyBv8934OVw62Bxu
5ij0wbHOStA8TSbxJXyuGBw8cqTPfuUtqPLx6nWtcRZ6p13MuQTq%2bKZLZ7hwY2Urf1o1Gi9OPGyo5zuJZAuQInU%2bkJKU
6ycXHZo17Uti3DITCy0%2fG%2bQ2gixzBIpmJctekKJO243rZiU1wbOUPWLzGum8ydRu3im2LiDisXquAu7ipY5P0D475AZN
3Cd6nlIPP5MOra493QhX4Il39q%2birT1%2f5F7tI%2fKLv20fWFC%2fjKbfu%2bFe4QIbdtiSCvLkyZ%2bWDwBMWSXHGE11
CoErbj4LJP3h4oqLto17riGCYMb%2bRHZXNJA2bwjcfgY4w2FE4hrL0cC6D3YgZxHHpUeT4gMXoXj0EJwODxQwElc9yfoe%2
bDgJ4Fy6%2fXc0ymDFYU7oOouAc0nwPKZwhZn4Q3mMZIG5aeOFcx9IM6M47IcMMbo0r78aUk8M94h5f4sK6JxHz75B6JyTx3
H%2bxFDJ3j5UtUYj1oir4CLQJgR8ABhMDGxqhAN4c4wA4y790bh2F5PxkVXMGYb4ghFNt3jIHGXRMENPTYkelnD0fa1mMmhJ
UXE%2fVAshJ8aZwcGCU%2fNhSkCATRXb5UDAmeaSkwe3m4bcRtfBbNZ1l5CNQVH8ZPZsKlGCNpD6dOYkSxa%2ffErYqImEzm
9itwSzUujQXI%2f8%2f%2fKewc9jeBujwHqnjuIYg5sJbjk%2bqc%2fwy5hKHTbxFacnFJlgvJhHt3mht8oRC9EbbsULoAK1
fvLe4%2fE%2bqFjOe02bw4sQuu1ssMKxLsNQMCTIZFzhl0K6BZdfo1RonKG0MEG1K%2ftSDNC4eyQw9ewYhgpozDVHW1yprp
VY9UgcTvFVSh0Vy%2bWde4b0dtmPdhbQhvvsQOSgnxIX6a8GN4AwXEoE7CoP6%2fFZiTAJTuxUKMjC1m8iAsrAurJugnEgaK
KugSNkl9y7bgSiYB6zkthDclEyBFWc1rAEcfH6oMJs59aJodXnPSAA9FuyqLCWB%2f3WFZ03efhTviz2101G8%2fsWMxR0w%
2fR56oNH2wzUwkmh9oczFaYLpJPzg6k47oh1zmDJraqyvWgzzfPIipa7EKK8YvsuO4BCFgMrDZtYZnCO6B9CFoKDCNJE9Wxl
%2bhTdzFCA4GpeLE4nT7y1j113iTV%2faWyImNLaRMU2ZiwuKy%2bd2OH55LqnLBCxrUUIMH7Ku4Mhd%2fYvw1NVpcZZ0L%2
bWOkMoephk2XXE4OQAY7Rk%2f%2fRnCbbHlFOVQmEVOoxNneBElleajK%2fxX6C0BZBaebAVYluwdGkkktvgQ5gUvzMiyqbs
vzyUMzq%2fhqKY7vVMWUeyCsBnybuGPSILJIkMgdgjiz%2baUZsOyZsUE%2b7PPyiqphqXNRfQ6tj8wTzq7a2Z5XgCYI10Pi
qj1mg6hY1TiRYuPanyBqh61LFKxblkpQJX2339pqB4RBOzF4%2f3CsvfjU302NSU9fypX5dBYubAZt80DOBe84FSnQIX3pfX
2%2fW9LqclyWbxC2QSOfHoe6TgkCiOall%2fqUHWqeOogbgLO5s5ffBoNmUCxhJW%2fH1EqKcsFzA%2ba%2f2Q0%2bs2m99R
qlxdd55bg67LXVPGfKh2dbVHjghXjO90nLEtVwCfs8oMUIg%2bmnip%2fdA7wDz4Nsma2W0ugEhOjpfFbL2TxHLhE0r%2bwy
3t%2bosvtaXNJZg84LJKpt3J%2bmc0pnIBH5S5H7zrNDKUnIYXY8BD5n1clZi4wwkRIp62avJw7lN22zNHsjp7NUjTYw9X%2
f1Iti1TKxjPZuitU%2bITeCRRHzeoaeGbzE1E%2bGSSqemw7F1wx4w9JXHDajH%2bY4iX7z2Y4OrY1JQQleeS9KWzw5HdiCp
uHmhMtLMSpz%2fGagw7KeaLEe9FxwrOYILS%2fXuBStZ1XOpbQHIlH0ZdQbv2I%2bA%2f3j3GvalSul%2f0YVWlPPPIC2Ogk
SSbd4HyXXh9TEB8dhDmfucy5VEZ5MsuOTgytkALNSK0t9cyvsAcWTQf0uVAMnyBeaMPJAvdE9fXUiH628eMD9PHvt3cL0GYd
RR9WBUcszIFtJNIA5AXj7abdbc6VZ8DqX4YfJ1xgTqg2qKSJqXvtbi5BJU49BGaxu01Ta6eBo2ABLtgBxKzb8DYNYqyqRB%2
bYkgr5YdU6z6va15jQJYGUJYVwZ8xDsKvYHz1fUFAHldzxkq44myNAjD1H0DoYhQaXUl20UXkgO9w5kBqTfmKj9DOJhs5Q88
ilebAbHHxm3GTZSJpP51jQjsPSUi3doX3Mz8E7W5pYptxtW1XPwcSHhkxuhWjbVKKQRTgM5uSXCPQ0PDAqcc6NybV2t1BK3G
hQSPzsQ5k3wkldK7CYuUWMpKTMNLZDVF8i25DoGpA0K5m5s3VMAukLA9Gob5ysU%2fsu2TVBrJZDOsa3L%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.

****************************************
```

يلقي ISE بخطأ "خال" عند إنشاء التوافق مع التطبيقات من طريقة عرض EP

السبب الأكثر شيوعا لوجود رسالة "خالية" أثناء إنشاء التوافق مع التطبيقات من طريقة عرض EP وهو غياب مخططات OPSWAT المطلوبة. يجب أن يقوم تحديث الوضع إلى أحدث إصدار بإصلاح هذه المشكلة.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).