

AnyConnect 4.2 ريفش ت و ISE 2.0 نيوكت ريفش ت لل Posture BitLocker

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [ASA](#)
- [Windows 7 على BitLocker](#)
- [محرك خدمات كشف الهوية \(ISE\)](#)
- [الخطوة 1. جهاز الشبكة](#)
- [الخطوة 2. حالة الوضع والنهج](#)
- [الخطوة 3. موارد إعداد العميل وساسته](#)
- [الخطوة 4. قواعد التحويل](#)
- [التحقق من الصحة](#)
- [الخطوة 1. إنشاء جلسة VPN](#)
- [الخطوة 2. إمداد العميل](#)
- [الخطوة 3. Posture Check and CoA](#)
- [حشرات](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يصف هذا المستند كيفية تشفير قسم قرص نقطة النهاية باستخدام Microsoft BitLocker وكيفية تكوين محرك خدمات الهوية من (ISE) Cisco لتوفير الوصول الكامل إلى الشبكة، فقط عند تكوين التشفير الصحيح. يدعم Cisco ISE الإصدار 2.0 مع AnyConnect Secure Mobility Client 4.2 الوضع لتشفير القرص.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين واجهة سطر الأوامر (CLI) القابل للتكيف (ASA) وتكوين طبقة مأخذ التوصيل الآمنة (VPN SSL)
- تكوين VPN للوصول عن بعد على ASA
- خدمات ISE و Posture (وضعية محرك خدمات الهوية (ISE))

المكونات المستخدمة

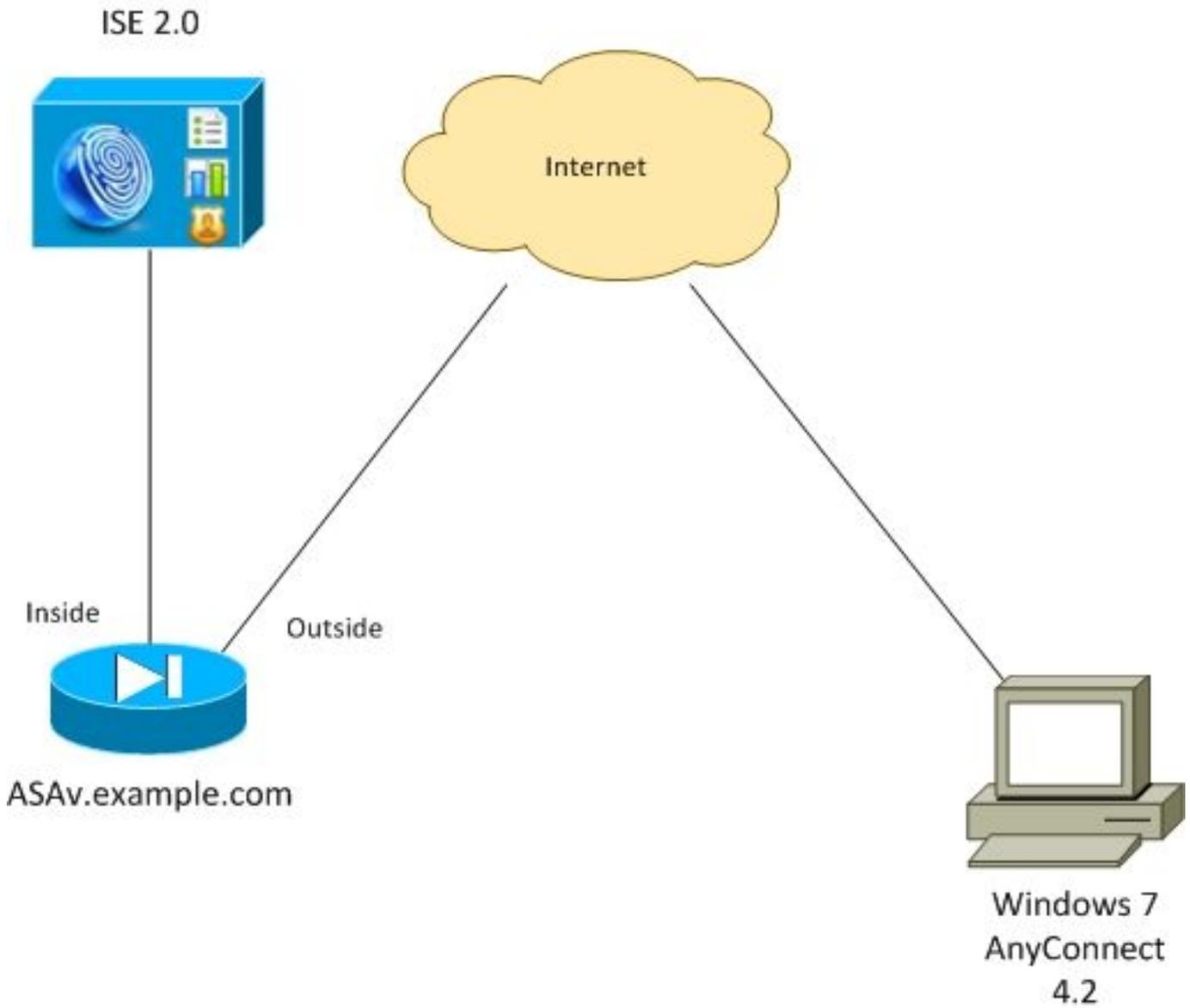
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- برنامج ASA الإصدارات 9.2.1 من Cisco والإصدارات الأحدث
- Microsoft Windows الإصدار 7 مع Cisco AnyConnect Secure Mobility Client الإصدار 4.2 والإصدارات الأحدث
- Cisco ISE، الإصدار 2.0 والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة



التدفق هو كما يلي:

- تتم مصادقة جلسة عمل الشبكة الخاصة الظاهرية (VPN) التي تم بدؤها بواسطة عميل AnyConnect عبر ISE. حالة الوضع لنقطة النهاية غير معروفة، يتم الوصول إلى قاعدة ASA VPN غير المعروفة، ونتيجة لذلك يتم إعادة توجيه الجلسة إلى ISE للتوفير

- يقوم المستخدم بفتح مستعرض الويب، تتم إعادة توجيه حركة مرور بيانات HTTP بواسطة ASA إلى ISE. يدفع ISE أحدث إصدار من AnyConnect مع الوضع ووحدة التوافق إلى نقطة النهاية
- بمجرد تنفيذ وحدة الوضع، فإنها تتحقق مما إذا كان القسم E: مشفرا بالكامل بواسطة BitLocker. إذا كانت الإجابة بنعم، يتم إرسال التقرير إلى ISE التي تقوم بتشغيل تغيير RADIUS للتحويل (CoA) بدون أي قائمة تحكم في الوصول (الوصول الكامل)
- يتم تحديث جلسة عمل VPN على ASA، ويتم إزالة قائمة التحكم في الوصول (ACL) المعاد توجيهها وتتوفر للجلسة إمكانية الوصول الكامل
- يتم تقديم جلسة عمل شبكة VPN كمثال. تعمل وظيفة الوضع بشكل جيد بالنسبة لأنواع الأخرى من الوصول.

ASA

تم تكوينها من وصول SSL VPN البعيد باستخدام ISE كخادم المصادقة والتفويض والمحاسبة (AAA). يلزم تكوين RADIUS CoA مع قائمة التحكم في الوصول (ACL) لإعادة التوجيه:

```

aaa-server ISE20 protocol radius
                        authorize-only
interim-accounting-update periodic 1
                        dynamic-authorization
aaa-server ISE20 (inside) host 10.48.17.235
                        key cisco

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
                        address-pool POOL
                        authentication-server-group ISE20
                        accounting-server-group ISE20
default-group-policy AllProtocols
tunnel-group TAC webvpn-attributes
                        group-alias TAC enable

group-policy AllProtocols internal
group-policy AllProtocols attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
                        anyconnect enable
tunnel-group-list enable
error-recovery disable

access-list REDIRECT extended deny udp any any eq domain
access-list REDIRECT extended deny ip any host 10.48.17.235
                        access-list REDIRECT extended deny icmp any any
                        access-list REDIRECT extended permit tcp any any eq www

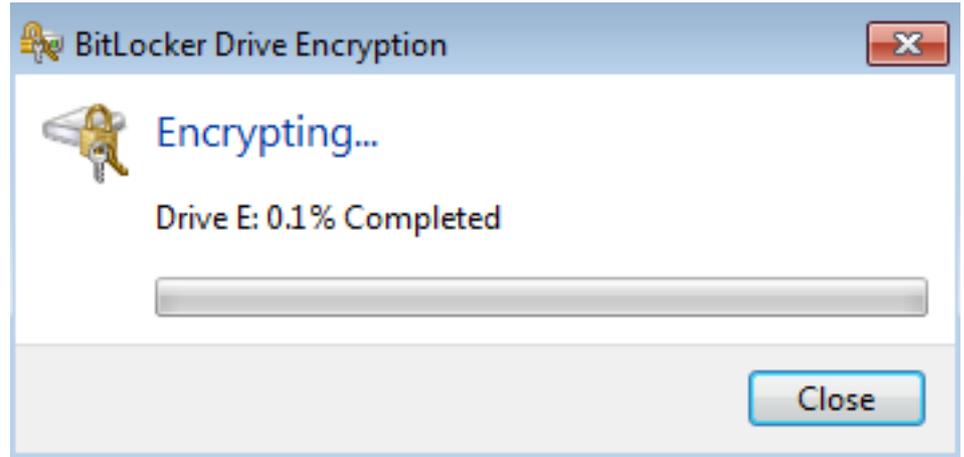
ip local pool POOL 172.16.31.10-172.16.31.20 mask 255.255.255.0
لمزيد من التفاصيل، راجع:

```

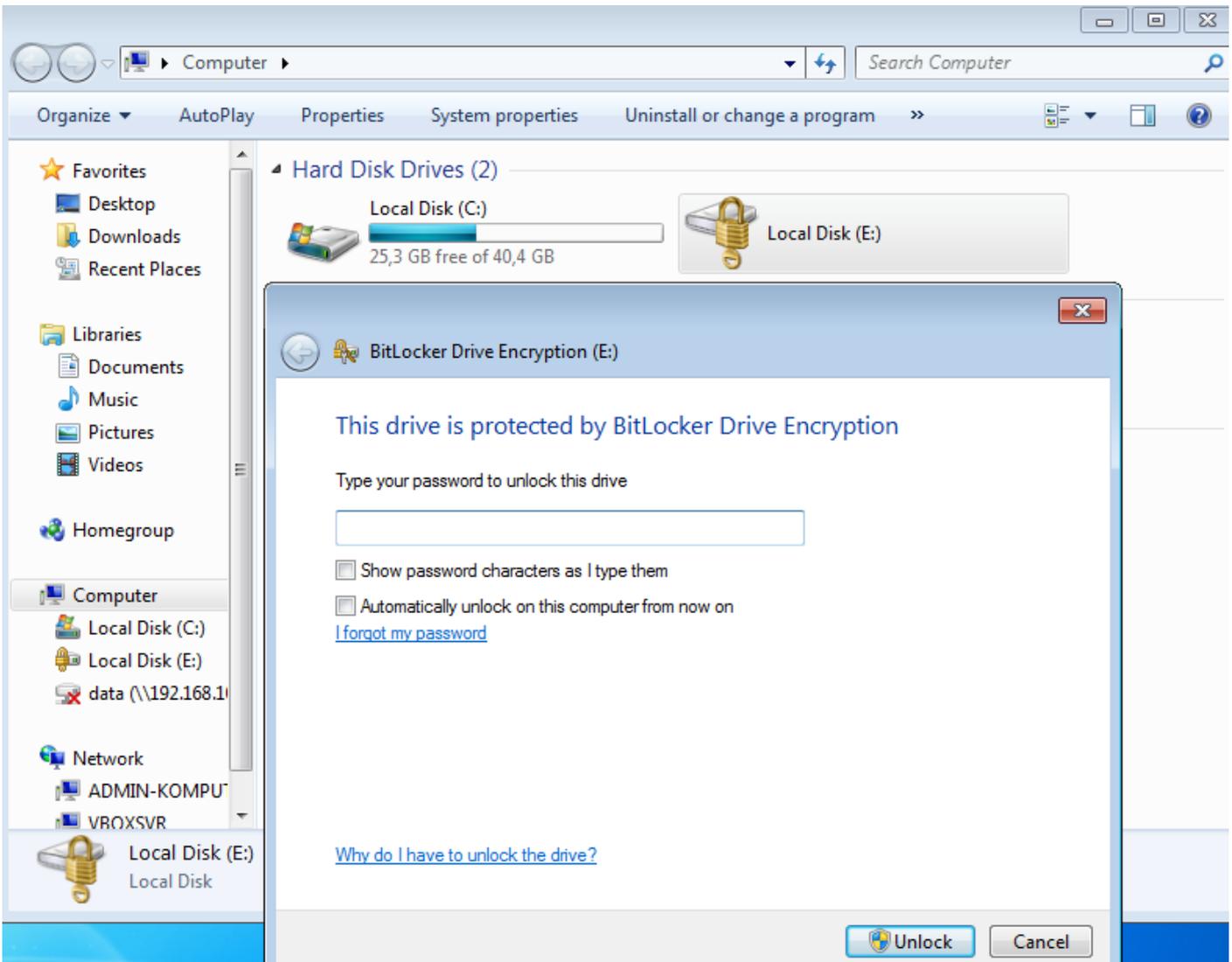
[تكملة AnyConnect 4.0 مع ISE، الإصدار 1.3 مثال التكوين](#)

Windows 7 على BitLocker

انتقل إلى لوحة التحكم < النظام والأمان > تشفير المحركات باستخدام BitLocker، قم بتمكين تشفير E: التقسيم. قم بحمايته بكلمة مرور (PIN) كما هو موضح في الصورة.



بمجرد تشفيره، قم بتركيبه (مع توفير كلمة المرور) وتأكد من إمكانية الوصول إليه كما هو موضح في الصورة.



لمزيد من التفاصيل، اتبع وثائق Microsoft:

[الدليل بالتفصيل لتشغيل محرك أقراص Windows BitLocker](#)

محرك خدمات كشف الهوية (ISE)

الخطوة 1. جهاز الشبكة

انتقل إلى إدارة < موارد الشبكة > أجهزة الشبكة، أضف ASA مع نوع الجهاز = ASA. يتم استخدام هذا كشرط في قواعد التحويل ولكنه ليس إلزاميا (يمكن استخدام أنواع أخرى من الشروط).

إن أمكن، لا توجد مجموعة أجهزة الشبكة. انتقل إلى الإدارة < موارد الشبكة > مجموعات أجهزة الشبكة من أجل الإنشاء.

الخطوة 2. حالة الوضع والنهج

تأكد من تحديث شروط الوضع: انتقل إلى الإدارة < النظام < الإعدادات < الوضع < التحديثات < التحديث الآن.

انتقل إلى سياسة < عناصر السياسة < الشروط < الوضع < شرط تشفير القرص، وقم بإضافة شرط جديد كما هو موضح في الصورة.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The 'Policy Elements' menu is expanded to show Dictionaries, Conditions, and Results. The 'Conditions' menu is selected, and the 'Disk Encryption Condition' configuration page is displayed. The page title is 'Disk-Encryption Conditions List > bitlocker'. The configuration fields are: Name: bitlocker, Description: (empty), Operating System: Windows All, Vendor Name: Microsoft Corp. Below these fields is a table titled 'Products for Selected Vendor' with the following data:

	Product Name	Version	Encryption State Check	Minimum Compliant Module Supp...
<input type="checkbox"/>	BitLocker Drive Encryption	10.x	YES	3.6.10146.2
<input checked="" type="checkbox"/>	BitLocker Drive Encryption	6.x	YES	3.6.10146.2

At the bottom of the page, there is a checkbox for 'Encryption State' which is checked. Below it, there is a field for 'Location' with a dropdown menu set to 'Specific Locatic' and a text box containing 'E:'. To the right of this field, there are three radio buttons: 'Fully Encrypted OR', 'Pending Encryption OR', and 'Partially Encrypted'.

يتحقق هذا الشرط ما إذا كان BitLocker الخاص بنظام التشغيل Windows 7 مثبتا وما إذا كان القسم E: مشفرا بالكامل.

ملاحظة: BitLocker هو تشفير على مستوى القرص ولا يعتمد الموقع المحدد بوسيلة المسار، بل حرف القرص فقط.

انتقل إلى السياسة < عناصر السياسة < النتائج < الوضع < المتطلبات لإنشاء متطلب جديد يستخدم الشرط كما هو موضح في الصورة.

Name	Operating Systems	Conditions	Remediation Actions
Bitlocker	for Windows All	met if bitlocker	else Message Text Only
Any_AV_Definition_Mac	for Mac OSX	met if ANY_av_mac_def	else AnyAVDefRemediationMac
Any_AS_Definition_Win_copy	for Windows All	met if ANY_as_win_def	else AnyASDefRemediationWin
Any_AV_Installation_Win	for Windows All	met if ANY_av_win_inst	else Message Text Only
Any_AV_Definition_Win	for Windows All	met if ANY_av_win_def	else AnyAVDefRemediationWin

انتقل إلى نهج < Posture (وضعية)، وقم بإضافة شرط لكل Windows لاستخدام المتطلب كما هو موضح في الصورة.

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Bitlocker	if Any	and Windows All		then Bitlocker

الخطوة 3. موارد إعداد العميل وسياسته

انتقل إلى السياسة < عناصر السياسة < إمداد العميل < الموارد، قم بتنزيل وحدة التوافق النمطية من Cisco.com وتحميل حزمة AnyConnect 4.2 يدويا كما هو موضح في الصورة.

Resources

Name	Type	Version	Last Update	Description
<input type="checkbox"/> MacOSXSPWizard 1.0.0.36	MacOsXSPWizard	1.0.0.36	2015/10/08 09:24:15	ISE 2.0 Supplicant Provisioning ...
<input type="checkbox"/> WinSPWizard 1.0.0.43	WinSPWizard	1.0.0.43	2015/10/29 17:15:02	Supplicant Provisioning Wizard f...
<input type="checkbox"/> ComplianceModule 3.6.10231.2	ComplianceModule	3.6.10231.2	2015/11/06 17:49:36	NACAgent ComplianceModule ...
<input checked="" type="checkbox"/> AnyConnectDesktopWindows 4.2.96.0	AnyConnectDesktopWindows	4.2.96.0	2015/11/14 12:24:47	AnyConnect Secure Mobility Cli...
<input checked="" type="checkbox"/> AnyConnectComplianceModuleWindows 3.6.10231.2	AnyConnectComplianceMo...	3.6.10231.2	2015/11/06 17:50:14	AnyConnect Windows Complian...
<input type="checkbox"/> AnyConnectPosture	AnyConnectProfile	Not Applicable	2015/11/14 12:26:16	
<input type="checkbox"/> Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2015/10/29 22:10:20	Pre-configured Native Supplica...
<input type="checkbox"/> AnyConnect Configuration	AnyConnectConfig	Not Applicable	2015/11/14 12:26:42	
<input type="checkbox"/> WinSPWizard 1.0.0.46	WinSPWizard	1.0.0.46	2015/10/08 09:24:16	ISE 2.0 Supplicant Provisioning ...

انتقل إلى إضافة < وكيل NAC أو ملف تعريف AnyConnect Posture، قم بإنشاء ملف تعريف AnyConnect Posture (الاسم: AnyConnectPosture) بإعدادات افتراضية.

انتقل إلى إضافة < تكوين AnyConnect، ثم أضف ملف تعريف AnyConnect (الاسم: تكوين AnyConnect) كما هو موضح في الصورة.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

AnyConnect Configuration > AnyConnect Configuration

* Select AnyConnect Package: AnyConnectDesktopWindows 4.2.96.0

* Configuration Name: AnyConnect Configuration

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 3.6.1

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AnyConnectPosture

VPN

Network Access Manager

Web Security

AMP Enabler

Network Visibility

Customer Feedback

انتقل إلى سياسة < إمداد العميل وعدل السياسة الافتراضية ل Windows لاستخدام ملف تعريف AnyConnect الذي تم تكوينه كما هو موضح في الصورة.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Client Provisioning Policy

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

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> IOS	If Any and	Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
<input checked="" type="checkbox"/> Android	If Any and	Android	and Condition(s)	then Cisco-ISE-NSP
<input checked="" type="checkbox"/> Windows	If Any and	Windows All	and Condition(s)	then AnyConnect Configuration
<input checked="" type="checkbox"/> MAC OS	If Any and	Mac OSX	and Condition(s)	then MacOSXSPWizard 1.0.0.36 And Cisco-ISE-NSP

الخطوة 4. قواعد التحويل

انتقل إلى السياسة < عناصر السياسة < النتائج < التفويض، وقم بإضافة ملف تعريف التفويض (الاسم: RedirectForPosture) الذي يعيد التوجيه إلى مدخل إمداد عميل افتراضي كما هو موضح في الصورة.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > RedirectForPosture

Authorization Profile

* Name: RedirectForPosture

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: REDIRECT Value: Client Provisioning Portal

Static IP/Host name/FQDN

يتم تحديد قائمة التحكم في الوصول (ACL) المعاد توجيهها على ASA.

انتقل إلى نهج < تفويض، قم بإنشاء 3 قواعد تخويل كما هو موضح في الصورة.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	ASA VPN compliant	if (DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS Compliant)	then PermitAccess
<input checked="" type="checkbox"/>	ASA VPN unknown	if (DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS Unknown)	then RedirectForPosture
<input checked="" type="checkbox"/>	ASA VPN non compliant	if (DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS NonCompliant)	then RedirectForPosture

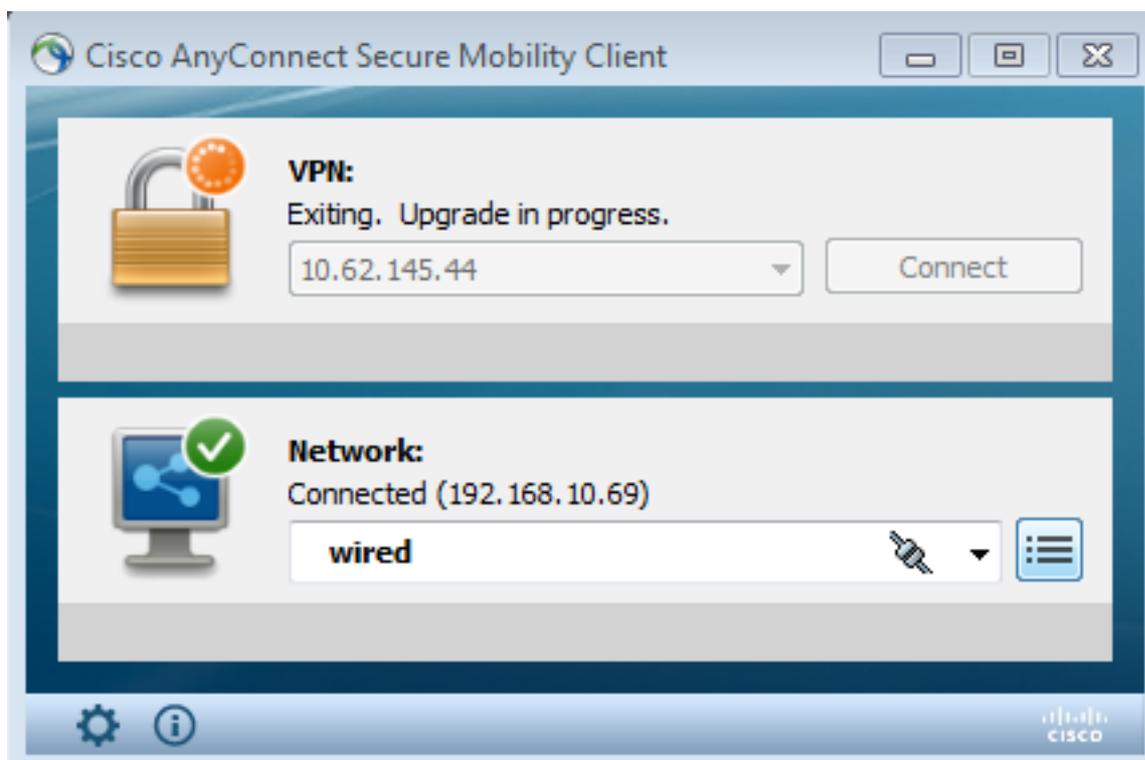
إذا كانت نقطة النهاية متوافقة، يتم توفير الوصول الكامل. إذا كانت الحالة غير معروفة أو غير متوافقة، يتم إرجاع إعادة التوجيه ل Client Provisioning.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

الخطوة 1. إنشاء جلسة VPN

بمجرد إنشاء جلسة عمل الشبكة الخاصة الظاهرية (VPN)، قد يرغب ASA في إجراء ترقية لوحات AnyConnect النمطية كما هو موضح في الصورة.



في ISE، يتم الوصول إلى القاعدة الأخيرة، نتيجة لإرجاع أذونات RedirectForPosture كما هو موضح في الصورة.

Identity Services Engine									
Home									
Operations									
Policy									
Guest Access									
Administration									
Work Centers									
RADIUS LiveLog									
TACACS LiveLog									
Reports									
Troubleshoot									
Adaptive Network Control									
Misconfigured Supplicants			Misconfigured Network Devices			RADIUS Drops			
0			0			3			
Show Live Sessions									
Add or Remove Columns									
Refresh									
Reset Repeat Counts									
Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Event
2015-11-14 14:59:06...	✓				10.229.20.45		PermitAccess	ASA	Dynamic Authorization succeeded
2015-11-14 14:59:04...	✓		0	cisco	08:00:27:81:50:86	Default >> ASA VP...	RedirectForPosture		Session State is Postured
2015-11-14 14:58:22...	✓			cisco	08:00:27:81:50:86	Default >> ASA VP...	RedirectForPosture	ASA	Authentication succeeded

بمجرد انتهاء ASA من إنشاء جلسة عمل الشبكة الخاصة الظاهرية (VPN)، يشير إلى أنه يجب إجراء إعادة التوجيه:

```
ASA# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
Username      : cisco                               Index      : 32
Assigned IP   : 172.16.31.10                       Public IP   : 10.61.90.226
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 53201                               Bytes Rx   : 122712
Pkts Tx       : 134                                Pkts Rx   : 557
Pkts Tx Drop  : 0                                  Pkts Rx Drop : 0
Group Policy  : AllProtocols                        Tunnel Group : TAC
```

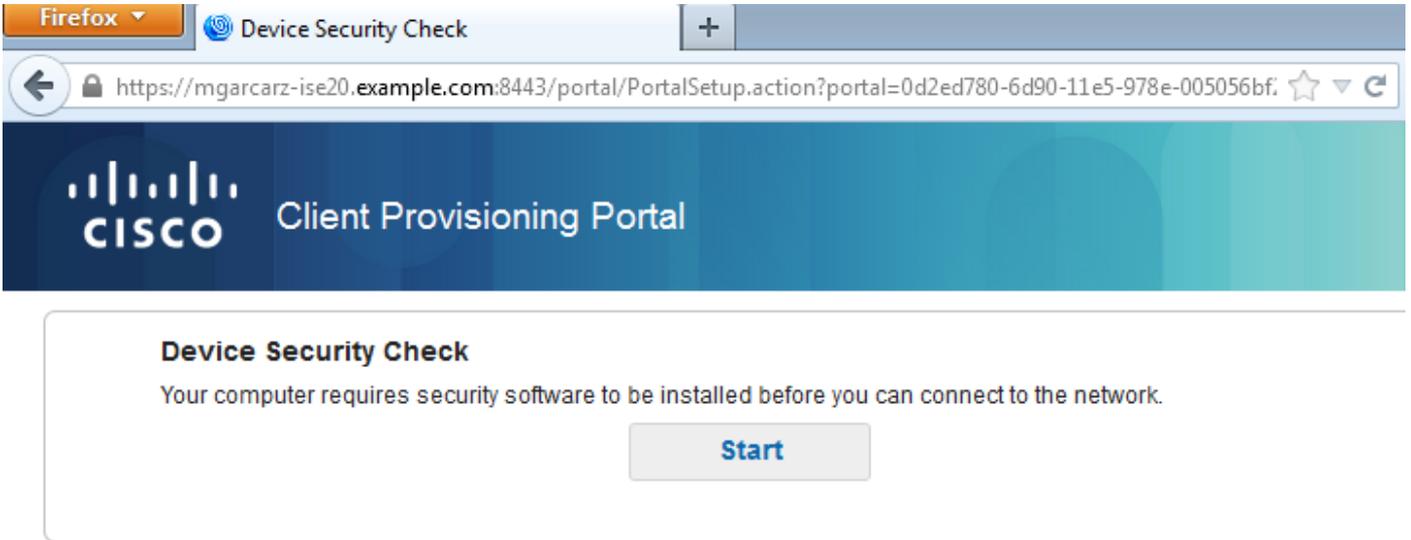
Login Time : 21:29:50 UTC Sat Nov 14 2015
Duration : 0h:56m:53s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a80101000200005647a7ce
Security Grp : none

<some output omitted for clarity>

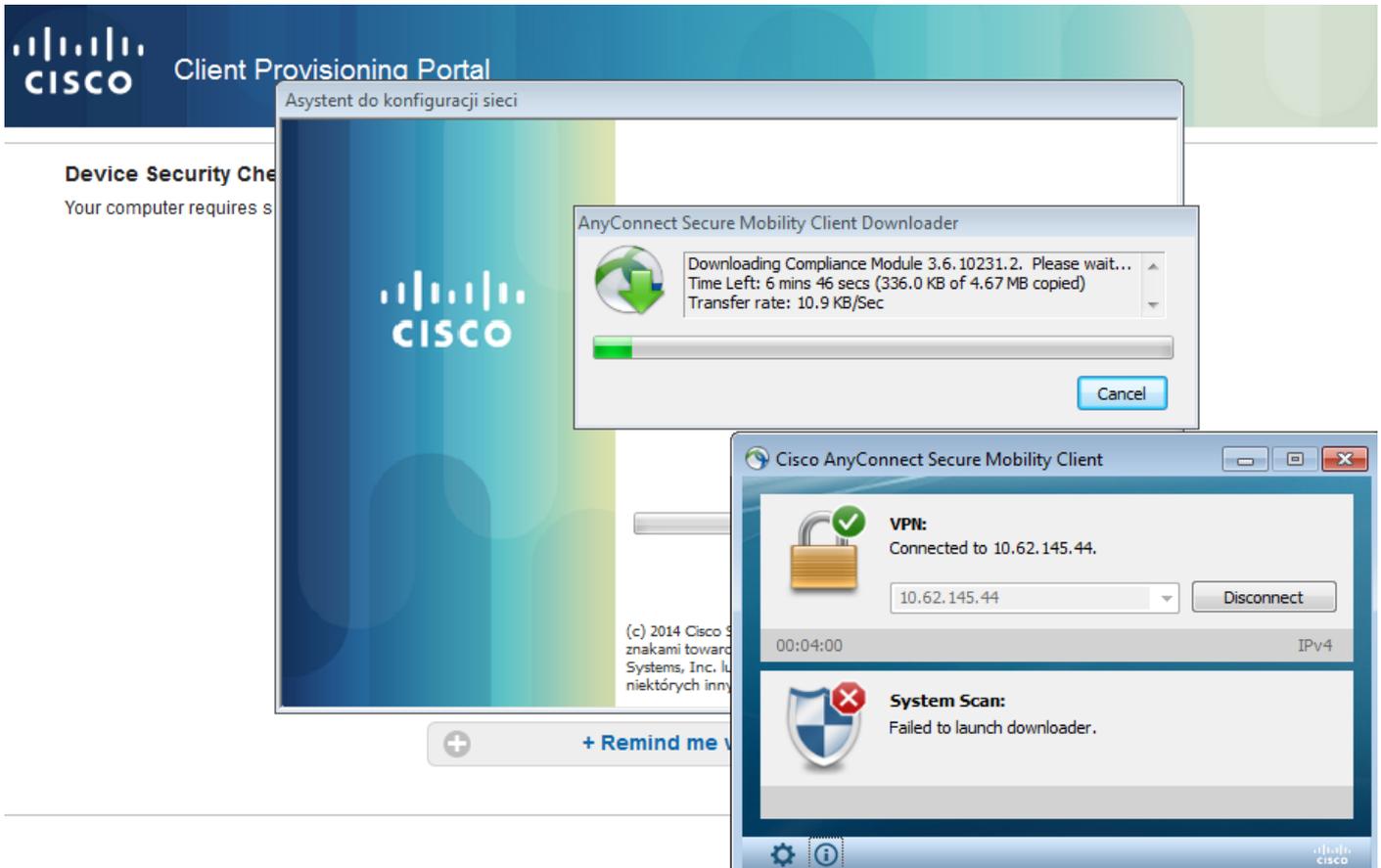
:ISE Posture
Redirect URL : https://mgarcarz-
...ise20.example.com:8443/portal/gateway?sessionId=&portal=0d2ed780-6d90-11e5-978e-00505
Redirect ACL : REDIRECT

الخطوة 2. إمداد العميل

في تلك المرحلة، تتم إعادة توجيه حركة مرور مستعرض ويب لنقطة النهاية إلى ISE لتوفير العميل كما هو موضح في الصورة.

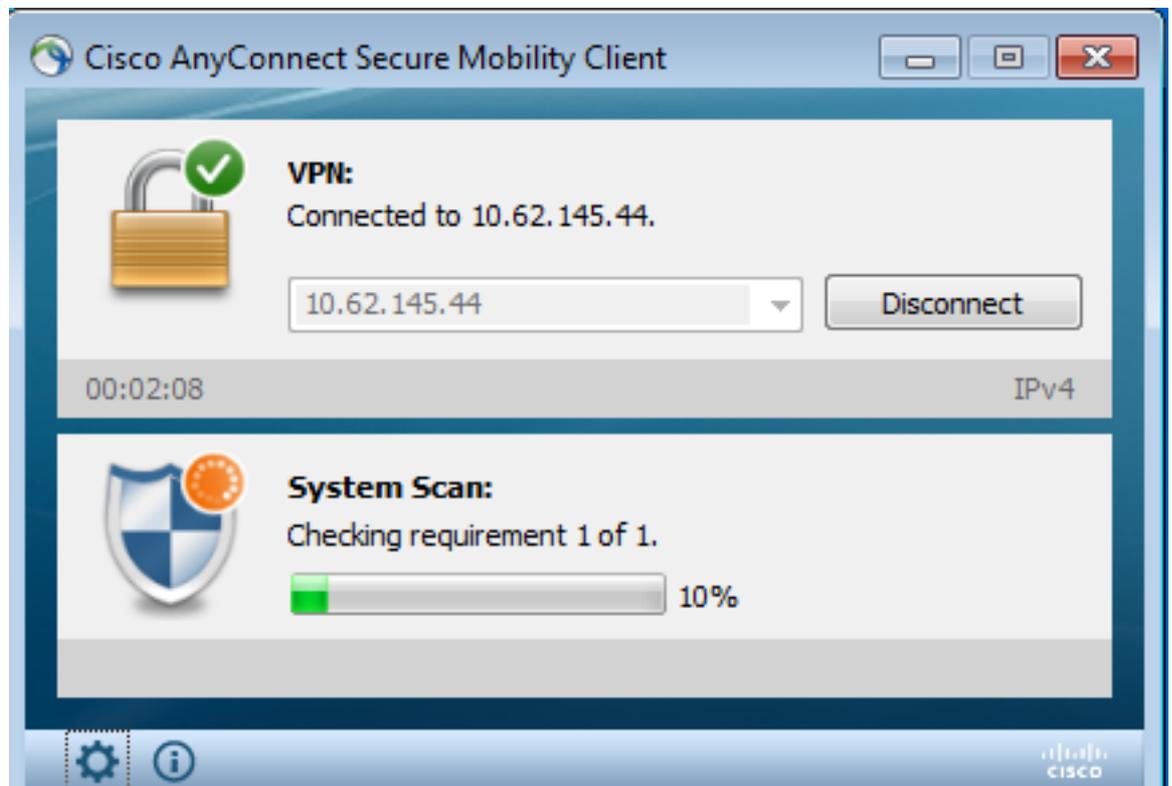


إذا تطلب الأمر، يتم تحديث AnyConnect مع Posture (الحالة والتوافق) النمطية كما هو موضح في الصورة.

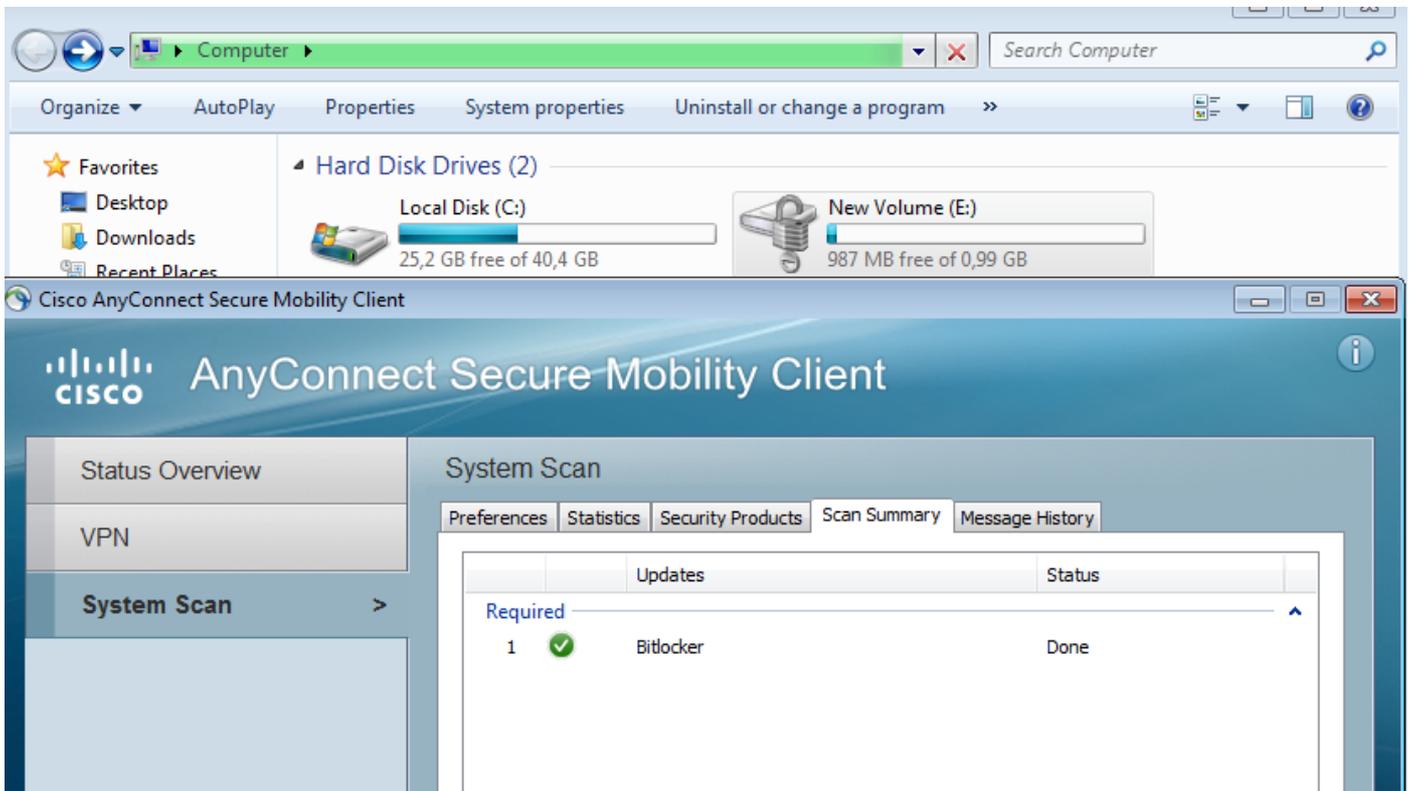


الخطوة 3. Posture Check and CoA

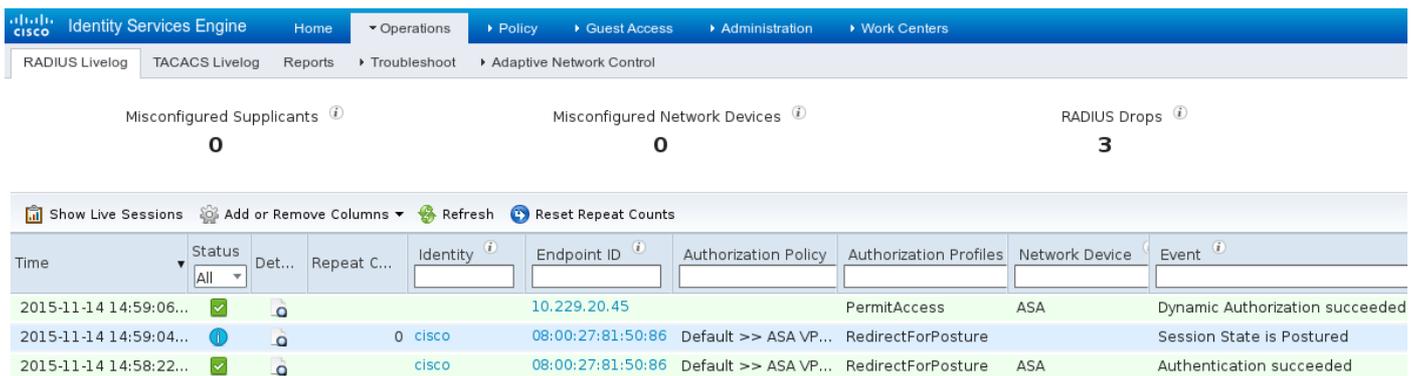
يتم تنفيذ وحدة Posture النمطية، واكتشف ISE (قد يتطلب الأمر أن يكون لديك سجل DNS لـ enroll.cisco.com لكي ينجح)، قم بتنزيل وفحص شروط الوضع كما هو موضح في الصورة.



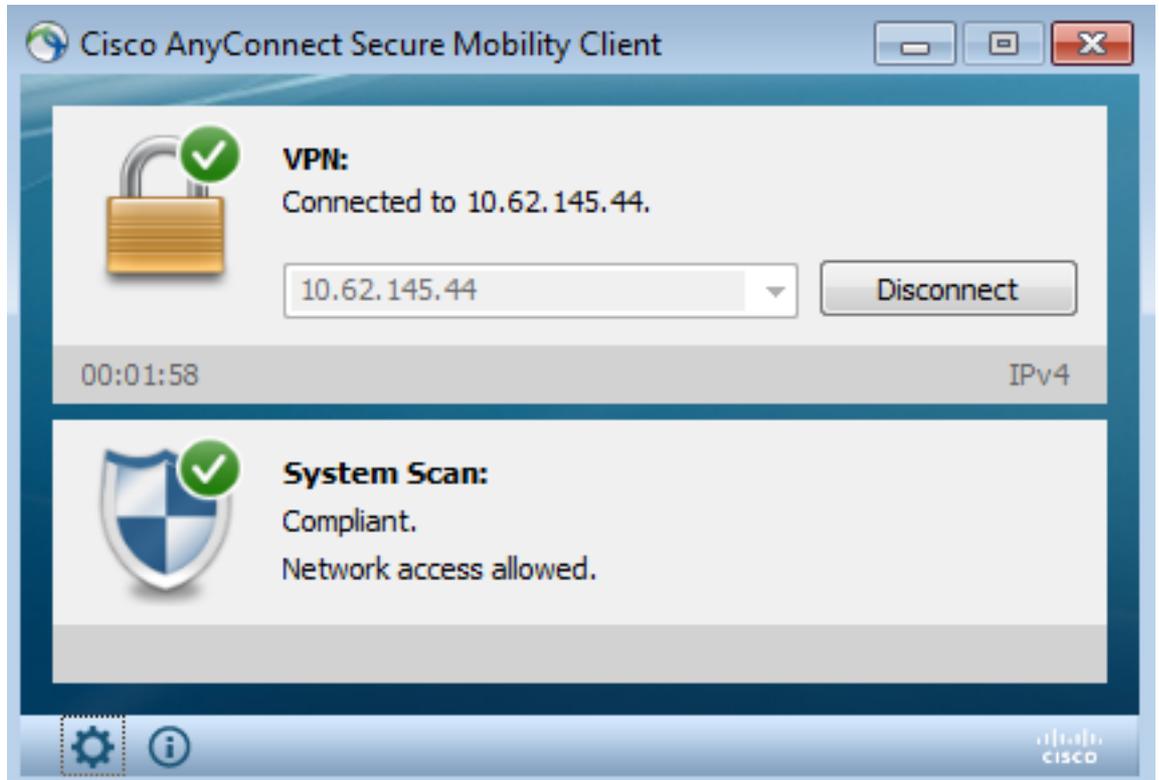
بمجرد التأكد من تشفير القسم E: بالكامل بواسطة BitLocker، يتم إرسال التقرير الصحيح إلى ISE كما هو موضح في الصورة.



يؤدي هذا إلى تشغيل CoA لإعادة تخويل جلسة VPN، كما هو موضح في الصورة.



يزيل ASA قائمة التحكم في الوصول لإعادة التوجيه التي توفر الوصول الكامل. يبلغ AnyConnect عن التوافق كما هو موضح في الصورة.



كما يمكن أن تؤكد التقارير التفصيلية على ISE استيفاء كلا الشرطين (تقييم الوضع حسب الحالة هو تقرير ISE 2.0 الجديد الذي يظهر كل شرط). يقوم الشرط الأول (HD_inst_BitLockerDriveEncryption_6_x) بالتحقق من عملية التثبيت/التثبيت، بينما يقوم الشرط الثاني (HD_loc_bitlocker_specific_1) بالتحقق من إذا ما كان موقع معين (E:) مشغرا بالكامل كما هو موضح في الصورة.

Report Selector	Posture Assessment by Condition									
From 11/14/2015 12:00:00 AM to 11/14/2015 02:59:15 PM	Logged At	Postur	Identity	Endpoint ID	IP Address	Endpoint OS	Policy	Enforcement	Condition Status	Condition name
	2015-11-14 14:59:04.8	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_loc_bitlocker_specific_1
	2015-11-14 14:59:04.8	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:42:25.7	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:42:25.7	✓	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:41:52.4	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:41:52.4	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:41:52.4	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_loc_bitlocker_specific_1
	2015-11-14 14:38:46.1	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:38:46.1	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_loc_bitlocker_specific_1
	2015-11-14 14:37:23.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Passed	hd_inst_BitLockerDriveEncryption_6_x
	2015-11-14 14:37:23.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:37:23.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_loc_bitlocker_specific_2
	2015-11-14 14:35:32.3	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:35:32.3	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_loc_bitlocker_specific_1
	2015-11-14 14:32:07.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
	2015-11-14 14:32:07.0	✗	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_loc_bitlocker_specific_1

يؤكد تقرير تقييم وضعية ISE حسب نقطة النهاية أن جميع الشروط مستوفاة، كما هو موضح في الصورة.

Posture More Detail Assessment

Time Range: From 11/14/2015 12:00:00 AM to 11/14/2015 11:42:08 PM
Generated At: 2015-11-14 23:42:08.257

Client Details

Username:	cisco
Mac Address:	08:00:27:81:50:86
IP address:	10.62.145.44
Session ID:	c0a801010001700056473ebe
Client Operating System:	Windows 7 Ultimate 64-bit
Client NAC Agent:	AnyConnect Posture Agent for Windows 4.2.00096
PRA Enforcement:	0
CoA:	Received a posture report from an endpoint
PRA Grace Time:	0
PRA Interval:	0
PRA Action:	N/A
User Agreement Status:	NotEnabled
System Name:	ADMIN-KOMPUTER
System Domain:	n/a
System User:	admin
User Domain:	admin-Komputer
AV Installed:	
AS Installed:	Windows Defender;6.1.7600.16385;1.141.3676.0;01/11/2013;

Posture Report

Posture Status:	Compliant
Logged At:	2015-11-14 14:59:04.827

ويمكن تأكيد نفس الإجراء من تصحيح أخطاء ISE-PSC.log. تم تلقي طلب Posture من قبل ISE والاستجابة:

```
DEBUG [portal-http-service28][] 14:59:01,963 2015-11-14
cisco.cpm.posture.runtime.PostureHandlerImpl -::c0a801010001700056473ebe::- Received posture
request [parameters: reqtype=validate, userip=10.62.145.44, clientmac=08-00-27-81-50-86,
os=WINDOWS, osVerison=1.2.1.6.1.1, architecture=9, provider=Device Filter, state=, ops=1,
avpid=, avpname=Microsoft Corp.:!::!::!::, avpname=Windows Defender:!::!::!::,
avpversion=6.1.7600.16385:!::!::!::, avpfeature=AS:!::!::!::, userAgent=Mozilla/4.0 (compatible;
WINDOWS; 1.2.1.6.1.1; AnyConnect Posture Agent v.4.2.00096), session_id=c0a801010001700056473ebe
DEBUG [portal-http-service28][] 14:59:01,963 2015-11-14
cisco.cpm.posture.runtime.PostureHandlerImpl -::cisco:c0a801010001700056473ebe::- Creating a new
session info for mac 08-00-27-81-50-86
DEBUG [portal-http-service28][] 14:59:01,963 2015-11-14
cisco.cpm.posture.runtime.PostureHandlerImpl -::cisco:c0a801010001700056473ebe::- Turning on
encryption for endpoint with mac 08-00-27-81-50-86 and os WINDOWS, osVersion=1.2.1.6.1.1
DEBUG [portal-http-service28][] 14:59:01,974 2015-11-14
```

```
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco:c0a801010001700056473ebe::- Agent criteria
      for rule [Name=bitlocker, Description=, Operating Systems=[Windows All],
      Vendor=com.cisco.cpm.posture.edf.AVASVendor@96b084e, Check Type=Installation, Allow older def
date=0, Days Allowed=Undefined, Product Name=[com.cisco.cpm.posture.edf.AVASProduct@44870fea]] -
      ( ( ( ( hd_inst_BitLockerDriveEncryption_6_x) ) & (hd_loc_bitlocker_specific_1
```

:XML الاستجابة مع متطلبات الوضع (الشرط + الإصلاح) بتنسيق XML:

```
DEBUG [portal-http-service28][] 14:59:02,052 2015-11-14
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- NAC agent xml
      <<?xml version="1.0" encoding="UTF-8"?><cleanmachines
      <version>2</version>
      <encryption>0</encryption>
      <package>
      <id>10</id>

      </version>

      <type>3</type>
      <optional>0</optional>
      <action>3</action>
      <check>
      <id>hd_loc_bitlocker_specific_1</id>
      <category>10</category>
      <type>1002</type>
      <param>180</param>

      <value_type>2</value_type>
      <check/>
      <check>

      <category>10</category>
      <type>1001</type>
      <param>180</param>
      <operation>regex match</operation>
```

```
<value>^6\..+$|^6$/value>
<value_type>3</value_type>
<check/>
criteria>( ( (hd_inst_BitLockerDriveEncryption_6_x) ) &and;
<(hd_loc_bitlocker_specific_1) )</criteria>
<package/>
<cleanmachines/>
```

بعد إستلام التقرير المشفر بواسطة ISE:

```
DEBUG [portal-http-service28][ ] 14:59:04,816 2015-11-14
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Decrypting
report
DEBUG [portal-http-service28][ ] 14:59:04,817 2015-11-14
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Decrypted
report [[
<report><version>1000</version><encryption>0</encryption><key></key><os_type>WINDOWS</os_type><os
version>1.2.1.6.1.1</osversion><build_number>7600</build_number><architecture>9</architecture><
user_name>[device-filter-AC]</user_name><agent>x.y.z.d-todo</agent><sys_name>ADMIN-
KOMPUTER</sys_name><sys_user>admin</sys_user><sys_domain>n/a</sys_domain><sys_user_domain>admin-
Komputer</sys_user_domain><av><av_vendor_name>Microsoft
Corp.</av_vendor_name><av_prod_name>Windows
Defender</av_prod_name><av_prod_version>6.1.7600.16385</av_prod_version><av_def_version>1.141.36
76.0</av_def_version><av_def_date>01/11/2013</av_def_date><av_prod_features>AS</av_prod_features
<></av><package><id>10</id><status>1</status><check><chk_id>hd_loc_bitlocker_specific_1</chk_id
```

```
check><check><chk_id>hd_inst_BitLockerDriveEncryption_6_x</chk_id><chk_status>1</check></pack/>
[[ <age></report
```

يتم وضع علامة على المحطة كمتوافقة ويقوم ISE بإرسال CoA

```
INFO [portal-http-service28][ ] 14:59:04,823 2015-11-14
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a801010001700056473ebe::- Posture state is
compliant for endpoint with mac 08-00-27-81-50-86
DEBUG [pool-5399-thread-1][ ] cisco.cpm.posture.runtime.PostureCoA - 14:59:06,825 2015-11-14
:cisco:c0a801010000f0005647358b::- Posture CoA is triggered for endpoint [08-00-27-81-50-86]
with session [c0a801010001700056473ebe
كما يتم إرسال التكوين النهائي بواسطة ISE:
```

```
DEBUG [portal-http-service28][ ] 14:59:04,827 2015-11-14
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Sending
response to endpoint 08-00-27-81-50-86 http response [[ <!--X-Perfigo-DM-Error=0--><!--error=0--
><!--X-Perfigo-DmLogoff-Exit=0--><!--X-Perfigo-Gp-Update=0--><!--X-Perfigo-Auto-Close-Login-
Scr=0--><!--X-Perfigo-Auto-Close-Login-Scr-Time=0--><!--user role=--><!--X-Perfigo-OrigRole=--
><!--X-Perfigo-UserKey=dummykey--><!--X-Perfigo-RedirectUrl=--><!--X-Perfigo-ShowInfo=--><!--X-
Perfigo-Session=--><!--X-Perfigo-SSO-Done=1--><!--X-Perfigo-Provider=Device Filter--><!--X-
Perfigo-UserName=cisco--><!--X-Perfigo-DHCP-Release-Delay=4--><!--X-Perfigo-DHCP-Renew-Delay=1--
[[ <><!--X-Perfigo-Client-MAC=08:00:27:81:50:86--
```

يمكن أيضا تأكيد هذه الخطوات من جانب العميل (AnyConnect DART)

```
Date : 11/14/2015
Time : 14:58:41
Type : Warning
Source : acvpnui
```

```
Description : Function: Module::UpdateControls
File: .\Module.cpp
Line: 344
```

```
No matching element found for updating: [System Scan], [label], [nac_panel_message_history],
[ ... [Scanning system
```

Date : 11/14/2015
Time : 14:58:43
Type : Warning
Source : acvpnui

Description : Function: Module::UpdateControls
File: .\Module.cpp
Line: 344

No matching element found for updating: [System Scan], [label], [nac_panel_message_history],
[.][Checking requirement 1 of 1

Date : 11/14/2015
Time : 14:58:46
Type : Warning
Source : acvpnui

Description : Function: CNacApiShim::PostureNotification
File: .\NacShim.cpp
Line: 461

.Clearing Posture List

للجلسة الناجحة، تقارير مسح نظام واجهة المستخدم ل AnyConnect / محفوظات الرسائل:

.Searching for policy server 14:41:59
...Checking for product updates 14:42:03
...The AnyConnect Downloader is performing update checks 14:42:03
...Checking for profile updates 14:42:04
...Checking for product updates 14:42:04
...Checking for customization updates 14:42:04
...Performing any required updates 14:42:04
.The AnyConnect Downloader updates have been completed 14:42:04
.Update complete 14:42:03
... Scanning system 14:42:03
.Checking requirement 1 of 1 14:42:05
.Updating network settings 14:42:05
.Compliant 14:42:10

حشرات ISE 2.0 - [CSCux15941](#) و AC4.2 تشفير BitLocker في الوضع مع فشل الموقع (char \ / غير

مدعوم) استكشاف الأخطاء وإصلاحها يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها. إذا كانت نقطة النهاية غير متوافقة، يتم الإبلاغ عنها بواسطة واجهة مستخدم AnyConnect (يتم تنفيذ عملية الإصلاح التي تم تكوينها أيضا) كما هو موضح في الصورة.

Cisco AnyConnect Secure Mobility Client

System Scan Summary

Update Details

30%

1 Update(s) Required
Updates are needed on your computer before you can join the network.

Updates	Status
Required	
1 Bitlocker	Click Start to begin

Bitlocker (Required)
Bitlocker encryption not enabled on the endpoint. Station not compliant.

Start

Time Remaining: 00:03:29

Hide Cancel

ويستطيع ISE توفير تفاصيل عن حالات الفشل، كما هو موضح في الصورة.

Identity Services Engine

Home Operations Policy Guest Access Administration Work Centers

RADIUS Livelog TACACS Livelog Reports Troubleshoot Adaptive Network Control

Report Selector

Favorites

ISE Reports

Audit 10 reports

Device Administration 4 reports

Diagnostics 10 reports

Endpoints and Users

Authentication Summary

Client Provisioning

Current Active Sessions

External Mobile Device Management

Identity Mapping

Manual Certificate Provisioning

Posture Assessment by Condition

Filters

Time Range Today

Run

Posture Assessment by Condition

From 11/14/2015 12:00:00 AM to 11/14/2015 02:36:59 PM

Logged At	Postur	Identit	Endpoint ID	IP Address	Endpoint OS	Policy	Enforcement	Condition	Condition name
2015-11-14 14:35:32.3	✘	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
2015-11-14 14:35:32.3	✘	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_loc_bitlocker_specific_1
2015-11-14 14:32:07.0	✘	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Failed	hd_inst_BitLockerDriveEncryption_10_x
2015-11-14 14:32:07.0	✘	cisco	08:00:27:81:50:8	10.62.145.44	Windows 7 Ulti	Bitlocker	Mandatory	Skipped	hd_loc_bitlocker_specific_1

ال نفسه يستطيع كنت فحصت من ال CLI سجل (مثال من ال log في قسم دقت). معلومات ذات صلة

- [تكوين خادم خارجي لتفويض مستخدم جهاز الأمان](#)
- [دليل تكوين واجهة سطر الأوامر Cisco ASA Series VPN الإصدار 9.1](#)
- [دليل مسؤول محرك خدمات الهوية من Cisco، إصدار 2.0](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل