

# 設定 ISE 2.0 および暗号化 AnyConnect 4.2 ポスチャ BitLocker 暗号化

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[ASA](#)

[Windows 7 の BitLocker](#)

[ISE](#)

[ステップ 1. ネットワーク デバイス](#)

[ステップ 2. ポスチャ状態およびポリシー](#)

[ステップ 3. クライアント プロビジョニング リソースおよびポリシー](#)

[ステップ 4. 承認規則](#)

[確認](#)

[ステップ 1. VPN セッション確立](#)

[ステップ 2. クライアント プロビジョニング](#)

[ステップ 3. ポスチャ チェックおよび CoA](#)

[バグ](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

正しい暗号化が設定される時だけこの資料に Microsoft BitLocker の使用のエンドポイントのディスクのパーティションを暗号化する方法をおよびネットワークにフル アクセスを提供するために Cisco Identity Services Engine ( ISE ) を設定する方法を記述されています。 AnyConnect セキュア モビリティ クライアント 4.2 サポートと共に Cisco ISE バージョン 2.0 はディスク暗号化のためにポーズをとります。

## 前提条件

### 要件

次の項目に関する知識が推奨されます。

- 適応型セキュリティ アプライアンス ( ASA ) ソフトウェア ( ASA ) CLI 設定およびセキュア ソケット レイヤ ( SSL ) VPN 設定
- ASA のリモートアクセス VPN 設定
- ISE およびポスチャ サービス

## 使用するコンポーネント

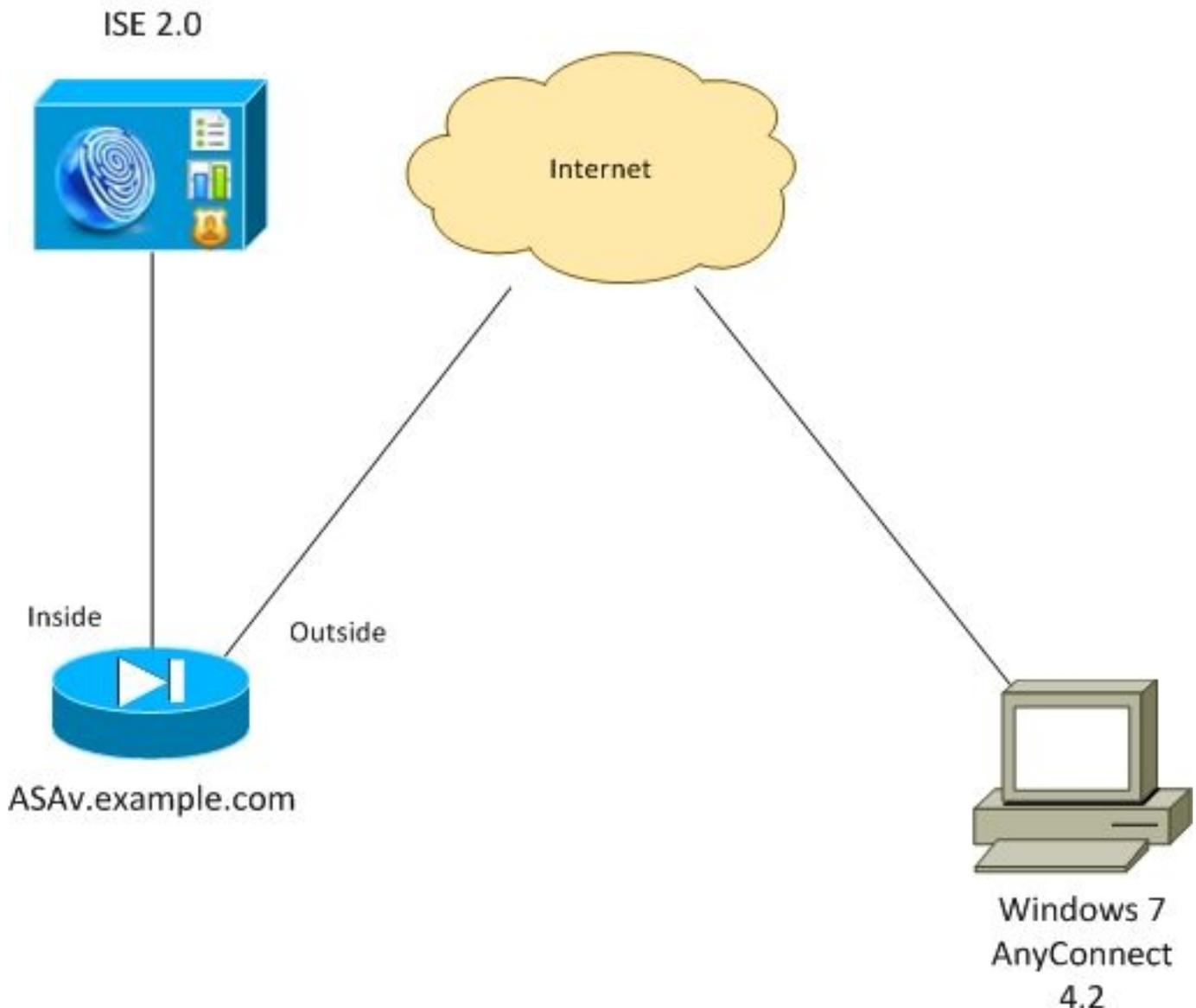
このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco ASA ソフトウェア バージョン 9.2.1 および以降
- Cisco AnyConnect セキュア モビリティ クライアント バージョン 4.2 を搭載している Microsoft Windows バージョン 7
- Cisco ISE リリース 2.0 以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

## 設定

### ネットワーク図



フローは次の通りです:

- AnyConnect クライアントから開始された VPN セッションが ISE を介して認証されます。エンドポイントのポスチャ ステータスは知られません、ルール **ASA VPN 未知数**は見つかリ、その結果セッションは提供のための ISE にリダイレクトされます
- ユーザが Web ブラウザを開き、HTTP トラフィックが ASA によって ISE にリダイレクトされます。ISE が、ポスチャとコンプライアンス モジュールとともに、AnyConnect の最新バージョンをエンドポイントにプッシュします。
- ポスチャ モジュールが実行されれば、パーティション E かどうか確認します:十分に BitLocker によって暗号化されます。Yes の場合は、レポートは ACL なしで許可 (CoA) の Radius 変更を誘発する ISE に送られます (フル アクセス)
- ASA の VPN セッションは更新済です、リダイレクト ACL は取除かれ、セッションにフル アクセスがあります

VPN セッションは一例として行なわれます。ポスチャ 機能性はアクセスの他の型のために余りにうまく働きます。

## ASA

それは認証、許可、アカウントイング (AAA) サーバで ISE の使用でリモート SSL VPN アクセスから設定されます。RADIUS CoA、およびリダイレクト ACL は、次のように設定する必要があります。

```

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

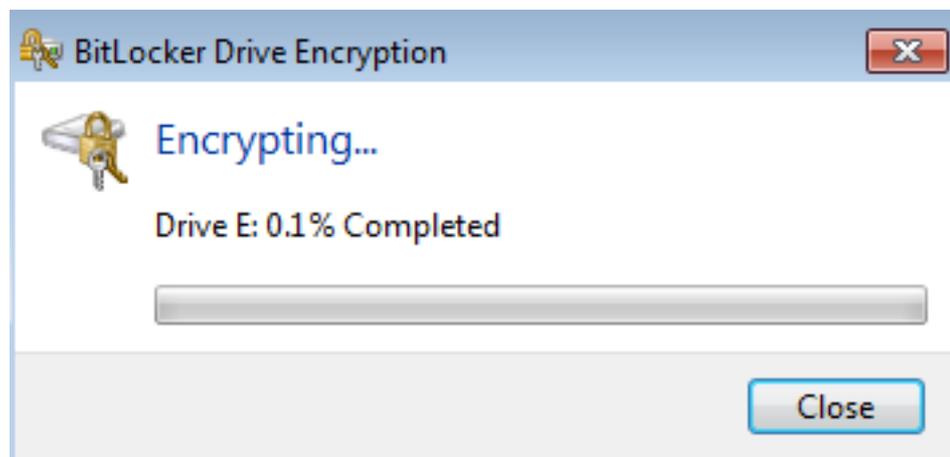
```

詳細については参照して下さい:

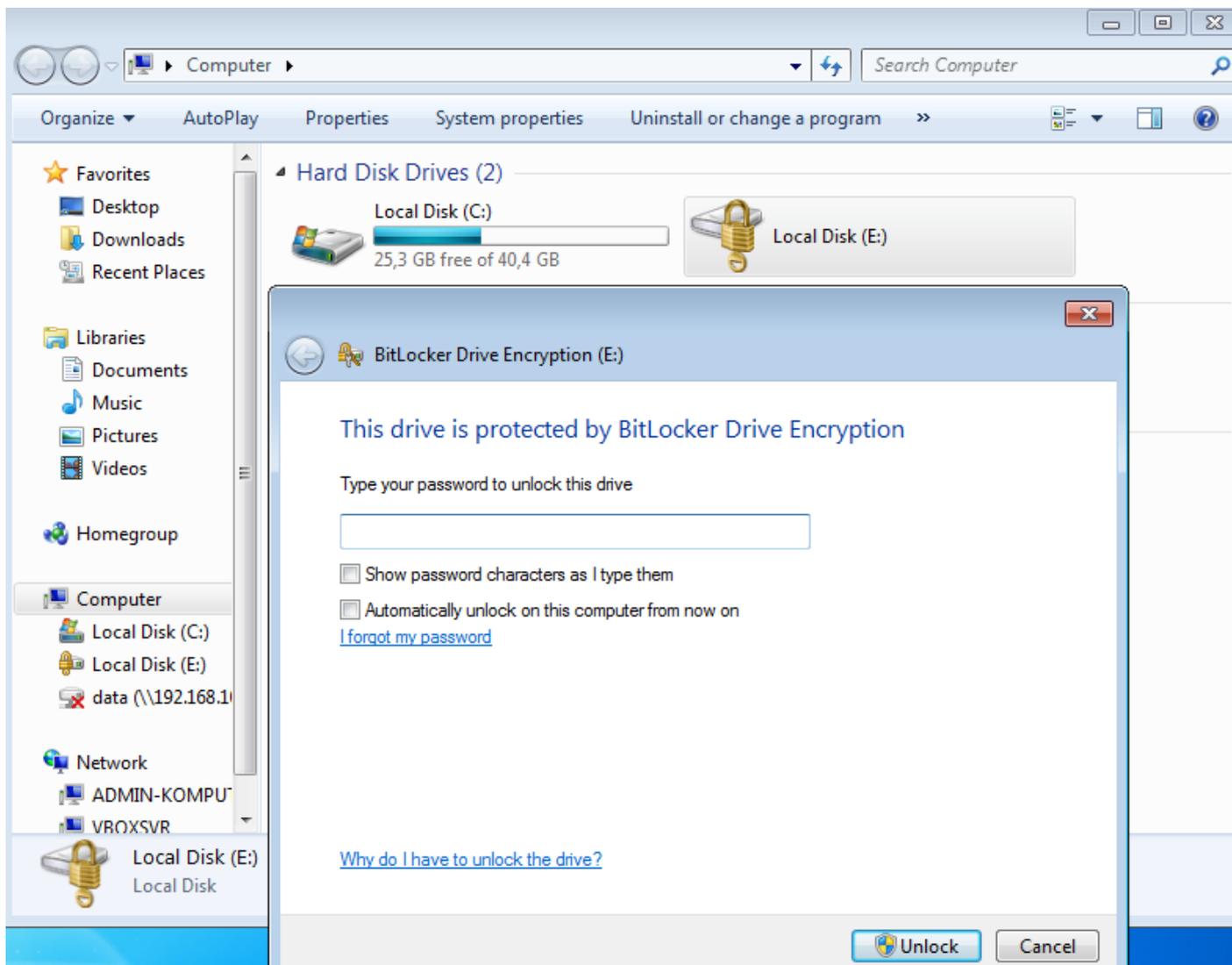
[AnyConnect 4.0 と ISE バージョン 1.3 統合の設定例](#)

## Windows 7 の BitLocker

コントロール パネル > システムへの移動およびセキュリティ > BitLocker ドライブ暗号化、有効 E: パーティションの暗号化を有効にします。イメージに示すようにパスワード (PIN) によってそれを保護して下さい。



暗号化されたら、それを (パスワードのプロビジョニングすると) マウントし、イメージに示すようにアクセス可能であることが確認して下さい。



詳細については、Microsoft ドキュメントに続いて下さい:

[Windows BitLocker Drive Encryption Step-by-Step Guide](#)

## ISE

### ステップ 1. ネットワーク デバイス

Administration > ネットワーク リソース > ネットワーク デバイスへの移動は、**装置タイプ = ASA** が付いている **ASA** を追加します。これは承認規則その条件が必須ではないが、ので使用されます (条件の他の型は使用することができます)。

適切であれば、ネットワーク デバイス グループはありません。作成するため、Administration > ネットワーク リソース > ネットワーク デバイス グループにナビゲートするため。

### ステップ 2. ポスチャ状態およびポリシー

ポスチャ状態をです更新確認して下さい: Administration > システム > 設定 > ポスチャ > 更新 > アップデートに今ナビゲートして下さい。

ポリシー > ポリシー要素 > 条件 > ポスチャ > ディスク暗号化状態にナビゲートして下さい、イメージに示すように新しい状態を追加して下さい。

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Disk-Encryption Conditions List > bitlocker

### Disk Encryption Condition

\* Name: bitlocker

Description:

\* Operating System: Windows All

\* Vendor Name: Microsoft Corp.

Products for Selected Vendor

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

Encryption State

Location: Specific Locatio E: is Fully Encrypted OR Pending Encryption OR Partially Encrypted

この状態点検 E Windows 7 のための BitLocker がインストールされていれば、そして:パーティションが完全に暗号化されているかどうかをチェックします。

注: BitLocker はディスク水平な暗号化であり、パス 引数の特定の Location を、ディスク文字だけサポートしません。

イメージに示すように条件を使用するポリシー > ポリシー要素 > 結果 > ポスチャ > 必要条件への移動新しい要件を作成するため。

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

### Requirements

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

ポリシー > ポスチャへの移動は、イメージに示すように要件を使用するためにすべての Windows のための条件を追加します。

### Posture Policy

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

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

## ステップ 3.クライアント プロビジョニング リソースおよびポリシー

ポリシー > ポリシー要素 > クライアント プロビジョニング > リソースにナビゲートし、Cisco.com から **準拠性モジュール** をダウンロードし、イメージに示すように手動で AnyConnect 4.2 パッケージをアップロードして下さい。

### Resources

<a href="#">Edit</a> <a href="#">+ Add</a> <a href="#">Duplicate</a> <a href="#">Delete</a>					
<input type="checkbox"/>	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 ...

追加するために > NAC エージェント ナビゲートすれば AnyConnect ポスチャ プロファイルは、AnyConnect ポスチャ プロファイル (名前を作成します: *AnyConnectPosture*) 。

追加するために > AnyConnect 設定ナビゲートして下さい、AnyConnect プロファイル (名前を追加して下さい: イメージに示すように **AnyConnect 設定**) 。

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

ポリシー > クライアント プロビジョニングへの移動および Windows のための修正する デフォルトポリシー AnyConnect 設定されたプロファイルをイメージに示すように使用するため。

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 <a href="#">AnyConnect Configuration</a>
<input checked="" type="checkbox"/> MAC OS	If Any and	Mac OSX	and Condition(s)	then MacOSXSPWizard 1.0.0.36 And Cisco-ISE-NSP

#### ステップ 4.承認規則

ポリシー > ポリシー要素への移動は >> 許可、追加します許可 プロファイル (名前を生じます: リダイレクトするかどれがイメージに示すように既定のクライアント提供ポータルに RedirectForPosture )。

The screenshot shows the Cisco 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 left sidebar shows a tree view with Authentication, Authorization (selected), Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profile' and shows the configuration for 'RedirectForPosture'. The configuration includes:
 

- Name: RedirectForPosture
- Description: (empty)
- Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Service Template: (disabled)
- Track Movement: (disabled)

 Below the configuration is a 'Common Tasks' section with a checked checkbox for 'Web Redirection (CWA, MDM, NSP, CPP)'. Under this checkbox, there are three fields: 'Client Provisioning (Posture)' set to 'Client Provisioning (Posture)', 'ACL' set to 'REDIRECT', and 'Value' set to 'Client Provisioning Portal'. There is also an unchecked checkbox for 'Static IP/Host name/FQDN'.

[REDIRECT] ACL は ASA で定義されます。

ポリシー > 許可にナビゲートして下さい、イメージに示すように 3 つの承認規則を作成して下さい。

The screenshot shows the 'Authorization Policy' configuration page in Cisco ISE. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The main menu includes Authentication, Authorization (selected), Profiling, Posture, Client Provisioning, and Policy Elements. The page title is 'Authorization Policy'. Below the title is a description: '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'. There is a dropdown menu set to 'First Matched Rule Applies'. Below this is a section for 'Exceptions (0)' with a sub-section for 'Standard'. A table lists three rules:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	ASA VPN compliant	if (DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS Compliant )	then PermitAccess
✓	ASA VPN unknown	if (DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS Unknown )	then RedirectForPosture
✓	ASA VPN non compliant	if (DEVICE:Device Type EQUALS All Device Types#ASA AND Session:PostureStatus EQUALS NonCompliant )	then RedirectForPosture

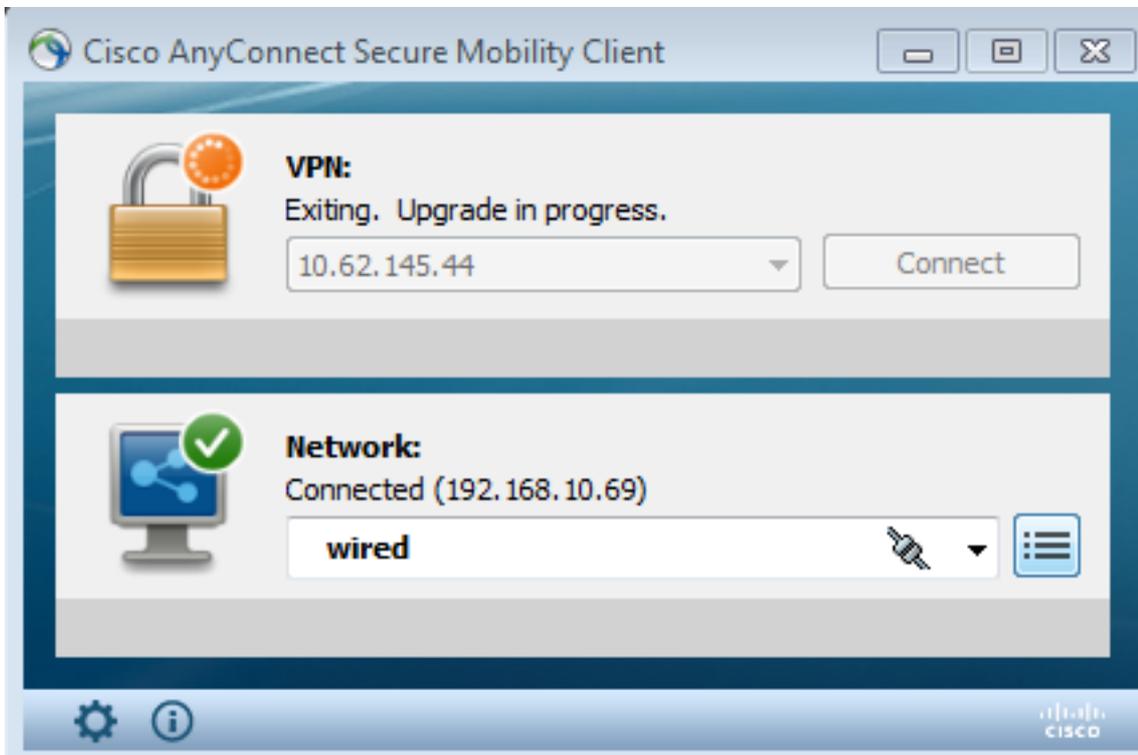
エンドポイントがルールに準拠している場合は、フル アクセスが許可されます。ステータスが不明または非対応である場合、クライアント プロビジョニングのためのリダイレクションは戻ります。

## 確認

このセクションでは、設定が正常に機能していることを確認します。

## ステップ 1. VPN セッション確立

VPN セッションが設定されれば、ASA はイメージに示すように AnyConnect モジュールのアップグレードを行いたいと思うかもしれません。



ISE で最後のルールは見つかります、その結果 **RedirectForPosture** 権限はイメージに示すように戻ります。

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

ASA が VPN セッションを構築することを終わればリダイレクションが発生する必要があることを報告します:

```
ASAv# 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
```

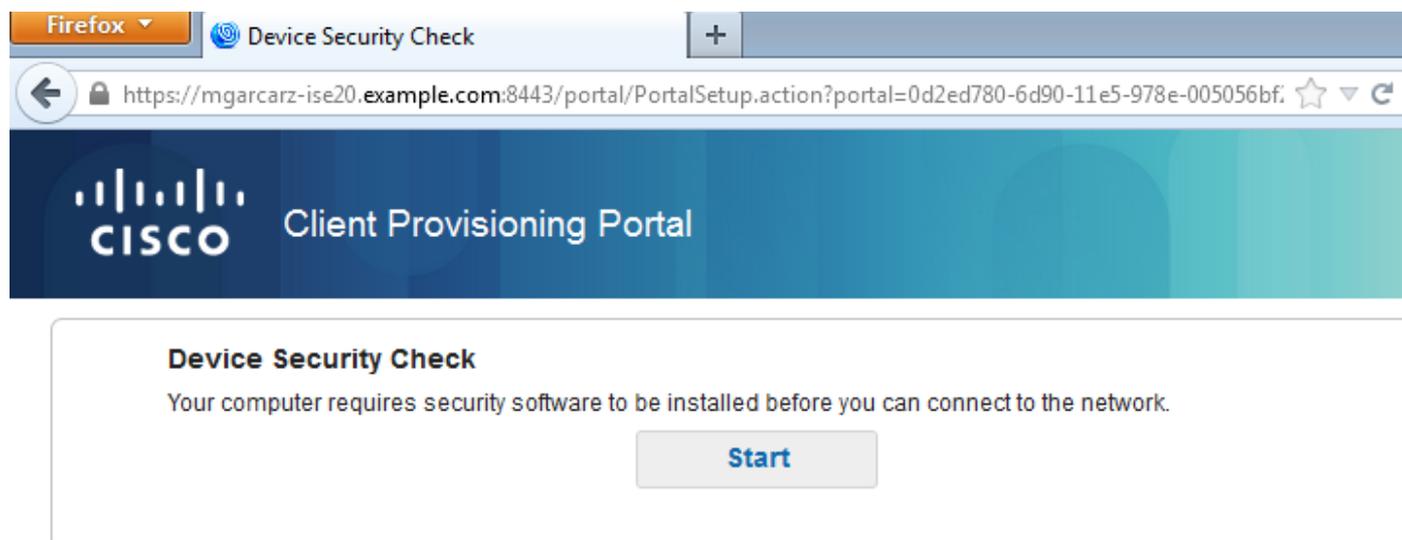
<some output omitted for clarity>

#### ISE Posture:

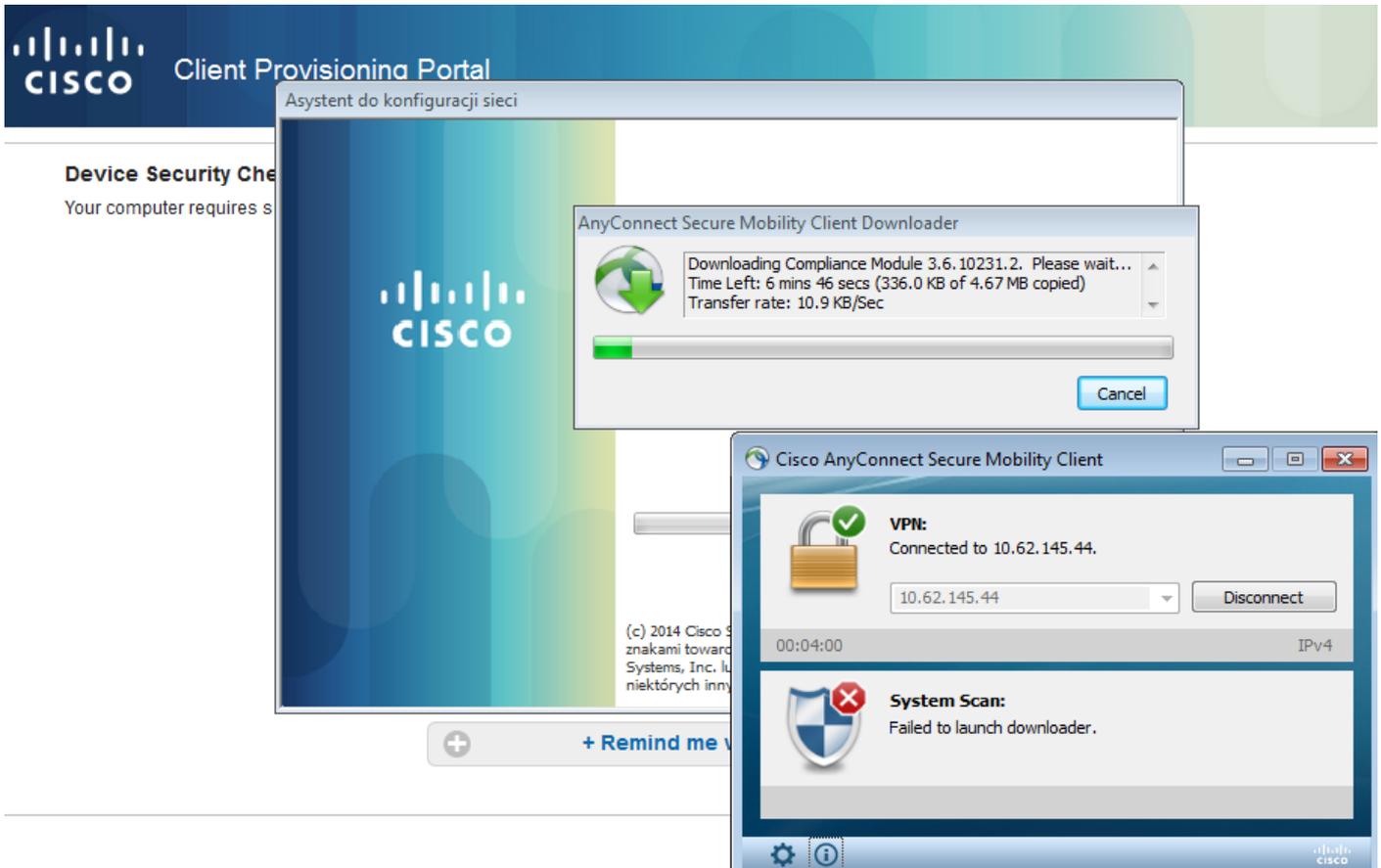
```
Redirect URL : https://mgarcarz-
ise20.example.com:8443/portal/gateway?sessionId=&portal=0d2ed780-6d90-11e5-978e-00505...
Redirect ACL : REDIRECT
```

## ステップ 2.クライアント プロビジョニング

そのステージで、エンドポイント Webブラウザ トラフィックはイメージに示すようにクライアント プロビジョニングのための ISE にリダイレクトされます。

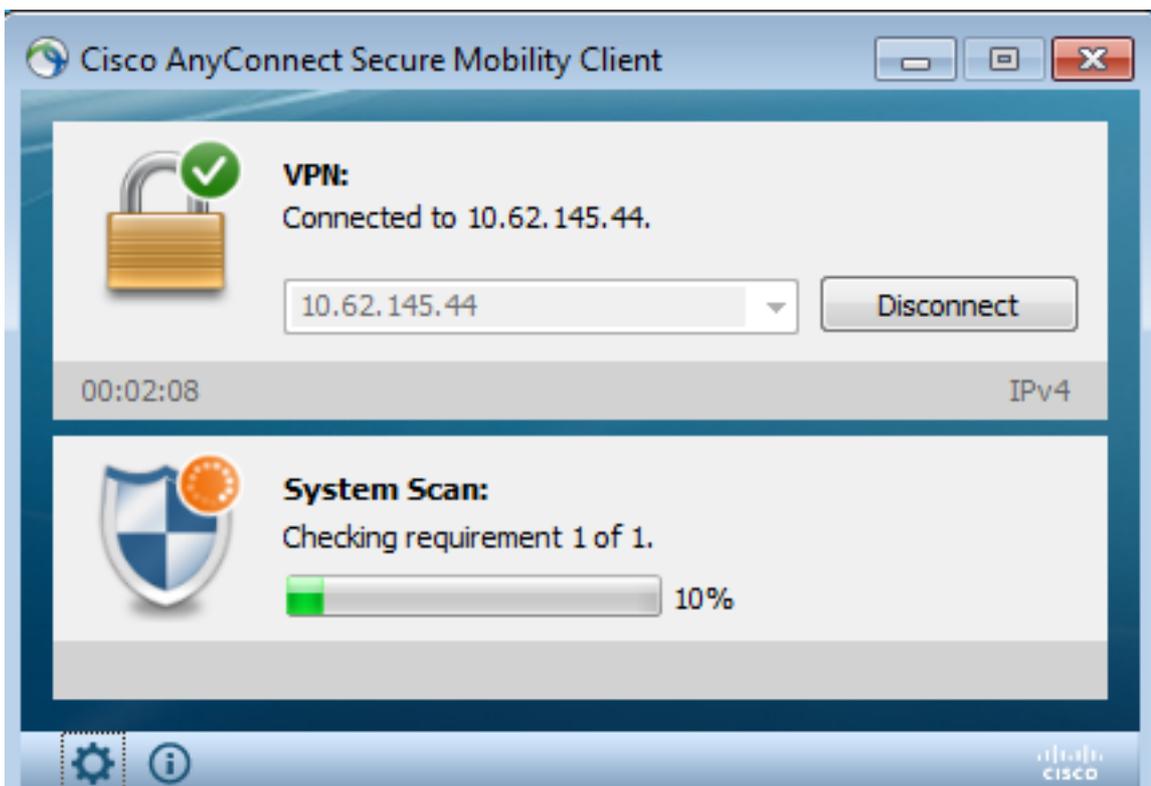


もし必要なら、ポスチャおよび準拠性モジュールと共に AnyConnect はイメージに示すように更新済です。



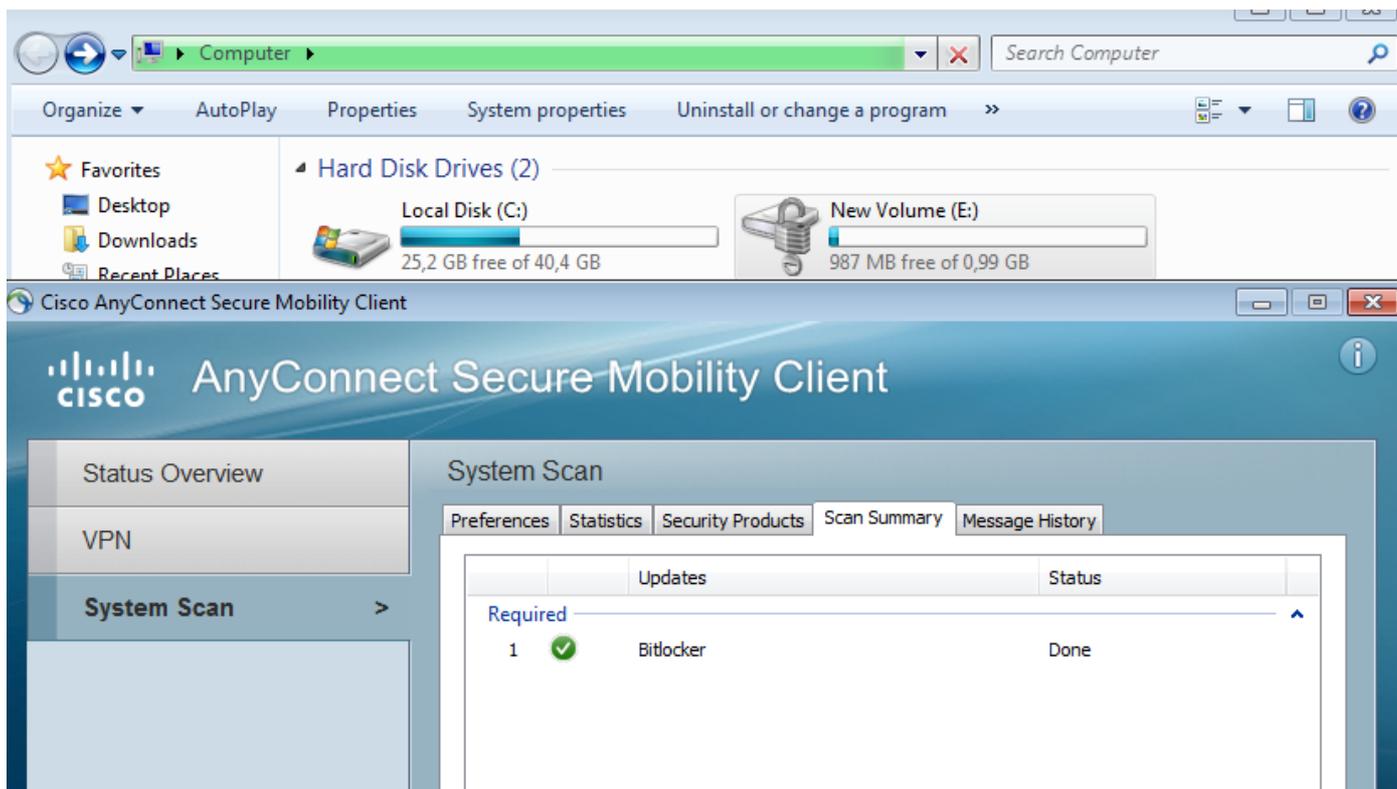
### ステップ 3. ポスチャ チェックおよび CoA

ポスチャ モジュールはポスチャ状態実行され、検出する、ISE ( enroll.cisco.com のための DNS A レコードがあるために成功するため必要となるかもしれません )、イメージに示すようにダウンロード、チェック。

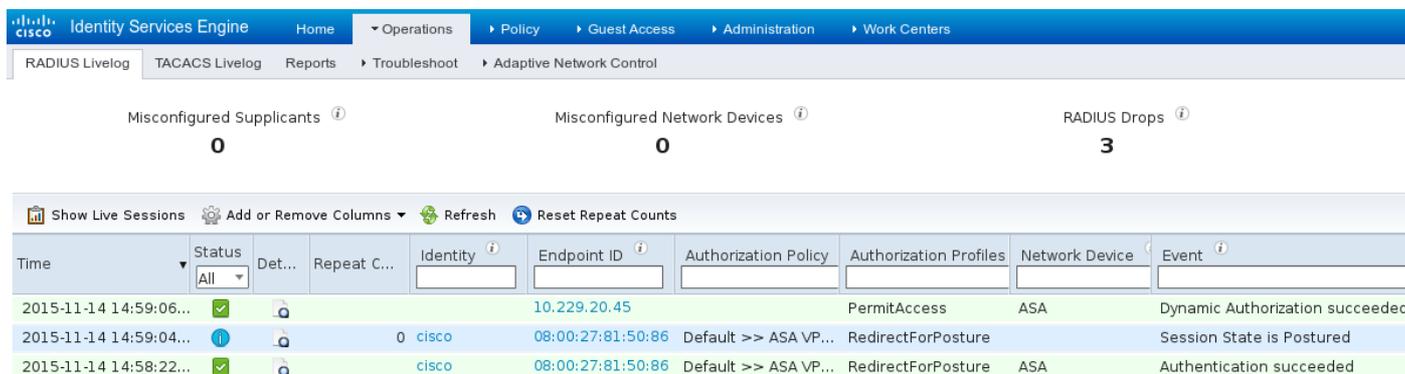


E ことが確認されれば: パーティションはイメージに示すように ISE に BitLocker によって十分に

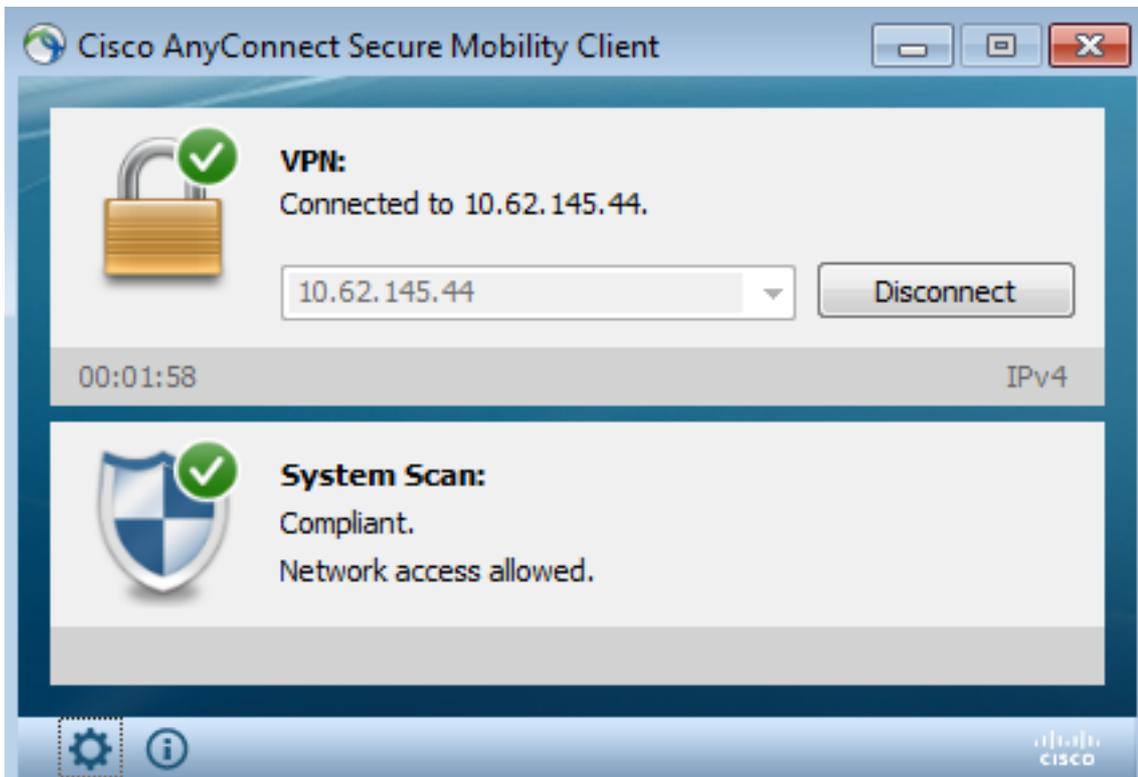
、正しいレポート送信 されず暗号化されます。



これはイメージに示すように VPN セッションを、reauthorize ために CoA を誘発します。



ASA はフル アクセスを提供するリダイレクション ACL を取除きます。AnyConnect はイメージに示すように準拠性を報告します。



また、ISE の Detailed レポートは条件が両方とも満足することを確認できます ( 条件によるポスチャ Assessment は各条件を示す ) 新しい ISE 2.0 レポートです。最初の状態 ( hd\_inst\_BitLockerDriveEncryption\_6\_x ) はインストール/プロセスがあるように、第 2 1 ( hd\_loc\_bitlocker\_specific\_1 ) チェック確認します特定の場所 ( E が: ) イメージに示すように十分に暗号化されます。

Report Selector	Posture Assessment by Condition									
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 * Time Range Today Run Posture Assessment by Endpoint	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

すべての条件が満足することをエンドポイント レポートによる ISE ポスチャ Assessment は、確認しますイメージに示すように。

## 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

同じ ise-psc.log デバッグから確認することができます。ISE で受信されたポスチャ要求、および応答は次のとおりです。

```
2015-11-14 14:59:01,963 DEBUG [portal-http-service28][  
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=, avvname=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  
2015-11-14 14:59:01,963 DEBUG [portal-http-service28][  
cisco.cpm.posture.runtime.PostureHandlerImpl -::cisco:c0a801010001700056473ebe::- Creating a new  
session info for mac 08-00-27-81-50-86  
2015-11-14 14:59:01,963 DEBUG [portal-http-service28][  
cisco.cpm.posture.runtime.PostureHandlerImpl -::cisco:c0a801010001700056473ebe::- Turning on  
enryption for endpoint with mac 08-00-27-81-50-86 and os WINDOWS, osVersion=1.2.1.6.1.1
```

```
2015-11-14 14:59:01,974 DEBUG [portal-http-service28][  
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) )
```

ポスチャ要件 ( 条件 + 修復 ) 付きの応答は XML 形式になります。

```
2015-11-14 14:59:02,052 DEBUG [portal-http-service28][  
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>  
<name>Bitlocker</name>  
<version/>  
<description>Bitlocker encryption not enabled on the endpoint. Station not  
compliant.</description>  
<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>  
<path>E:</path>  
<value>full</value>  
<value_type>2</value_type>  
</check>  
<check>  
<id>hd_inst_BitLockerDriveEncryption_6_x</id>  
<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) ) & ;  
(hd_loc_bitlocker_specific_1) ) )</criteria>  
</package>  
</cleanmachines>
```

暗号化されたレポートが ISE で受信された後 :

```
2015-11-14 14:59:04,816 DEBUG [portal-http-service28][  
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Decrypting  
report  
2015-11-14 14:59:04,817 DEBUG [portal-http-service28][  
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a801010001700056473ebe::- Decrypted  
report [[  
<report><version>1000</version><encryption>0</encryption><key></key><os_type>WINDOWS</os_type><os  
sversion>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><
chk_status>1</chk_status></check><check><chk_id>hd_inst_BitLockerDriveEncryption_6_x</chk_id><ch
k_status>1</chk_status></check></package></report> ]]
```

ステーションは対応および ISE 送信 CoA としてマークされます:

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

また、最終的な設定は ISE によって送信 されます:

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

これらのステップはまたクライアント側 ( AnyConnect 投げ矢 ) から確認することができます:

```
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.
```

成功したセッションに関しては、AnyConnect UI システム スキャン/メッセージ履歴は報告します  
:

```
14:41:59    Searching for policy server.
14:42:03    Checking for product updates...
14:42:03    The AnyConnect Downloader is performing update checks...
14:42:04    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.
14:42:03    Update complete.
14:42:03    Scanning system ...
14:42:05    Checking requirement 1 of 1.
14:42:05    Updating network settings.
14:42:10    Compliant.
```

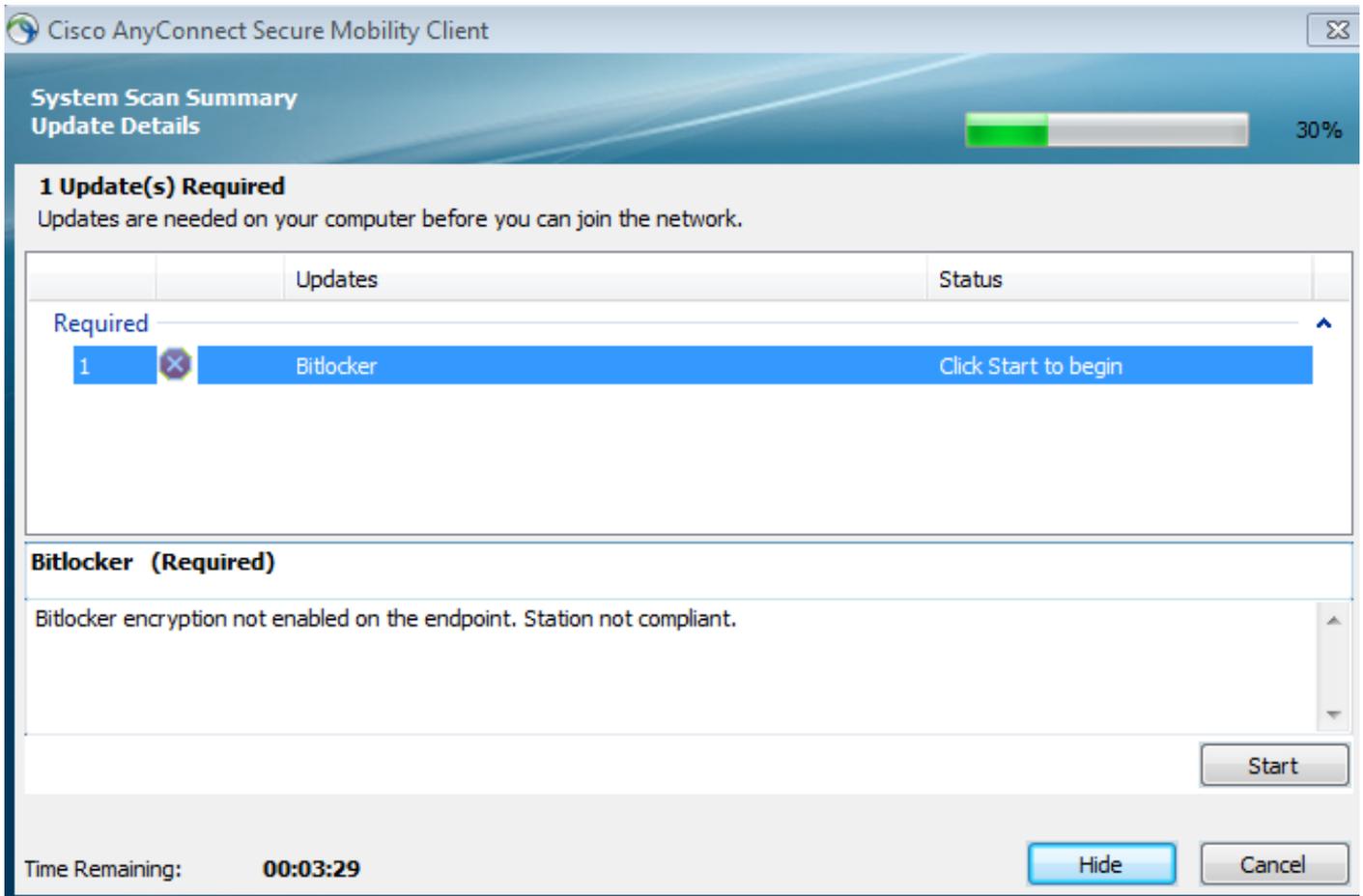
## バグ

[CSCux15941 : 場所指定による ISE 2.0 および AC4.2 Posture BitLocker 暗号化の失敗 \( 文字列「\ /」はサポート対象外 \)](#)

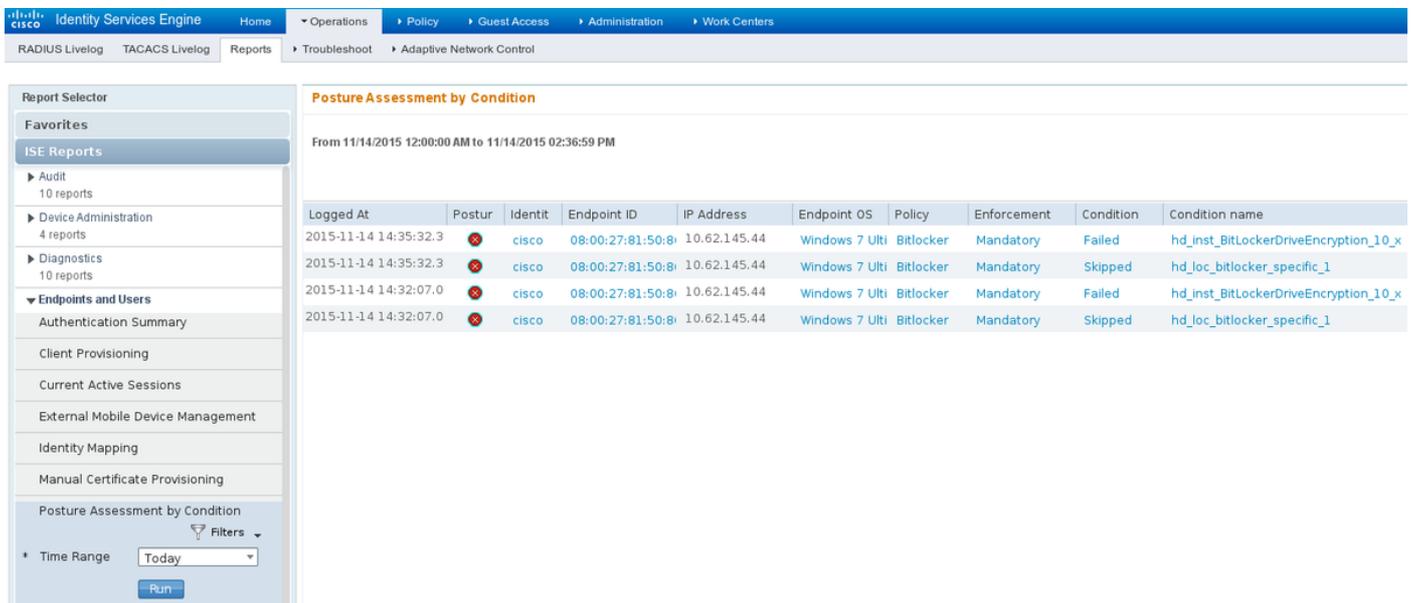
## トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

エンドポイントが不適合である場合、AnyConnect UI によってイメージに示すように ( また設定された治療は実行されず ) 報告されます。



ISE はイメージに示すように壊れる条件で詳細を、提供できます。



同じ CLI ログからチェックすることができます ( の例はセクションを確認しますログオンします ) 。

## 関連情報

- [セキュリティ アプライアンスのユーザ承認用の外部サーバの設定](#)
- [Cisco ASA シリーズ VPN CLI 構成ガイド 9.1](#)
- [Cisco Identity Services Engine 管理者ガイド リリース 2.0](#)

- [テクニカル サポートとドキュメント - Cisco Systems](#)