

AnyConnect 4.0 と ISE バージョン 1.3 統合の設定例

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トポロジとフロー](#)

[設定](#)

「[AeroScout RFID タグ](#)

[ISE](#)

[手順 1 : WLC の追加](#)

[手順 2 : VPN プロファイルの設定](#)

[手順 3 : NAM プロファイルの設定](#)

[ステップ 4 : アプリケーションのインストール](#)

[ステップ 5 : VPN/NAM プロファイルのインストール](#)

[手順 6 : ポスチャの設定](#)

[手順 7 : AnyConnect の設定](#)

[ステップ 8 : クライアント プロビジョニング ルール](#)

[手順 9 : 認可プロファイル](#)

[手順 10 : 認可ルール](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、複数の AnyConnect セキュア モビリティ クライアント モジュールを設定し、それらをエンドポイントに自動的にプロビジョニングできる、Cisco Identity Services Engine (ISE) バージョン 1.3 の新機能について説明します。このドキュメントでは、ISE 上での VPN、ネットワーク アクセス マネージャ (NAM)、ポスチャ モジュールの設定方法と、それを社内ユーザにプッシュする方法を説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- ISE の導入、認証、および許可
- ワイヤレス LAN コントローラ (WLC) の設定
- 基本的な VPN および 802.1x の情報

- AnyConnect を使用した VPN および NAM プロファイルの設定

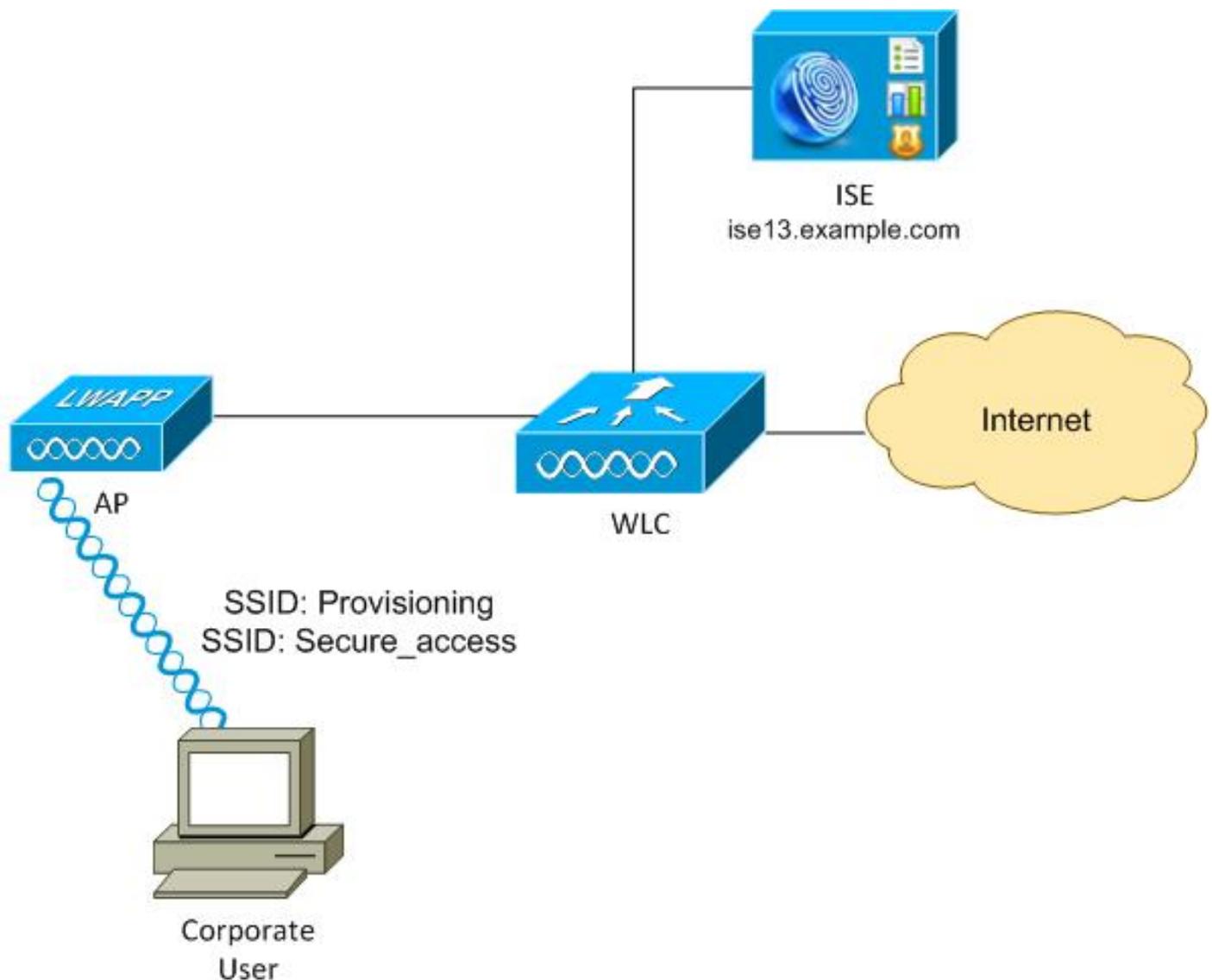
使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Microsoft Windows 7
- Cisco WLC バージョン 7.6 以降
- Cisco ISE ソフトウェア バージョン 1.3 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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

トポロジとフロー



ここで、フローを示します。

手順 1: 社内ユーザ アクセスのサービス セット識別子 (SSID) : プロビジョニング。
Extensible Authentication Protocol-Protected EAP (EAP-PEAP) を使用して 802.1x 認証を実行

します。 **Provisioning** 認証ルールが ISE 上で検出され、ユーザは AnyConnect プロビジョニングに ([Client Provisioning Portal] を介して) リダイレクトされます。 AnyConnect がマシン上で検出されない場合、すべての設定済みモジュール (VPN、NAM、ポスチャ) がインストールされます。 そのプロファイルとともに、各モジュールの設定がプッシュされます。

ステップ 2 : AnyConnect がインストールされたら、ユーザは PC を再起動する必要があります。 AnyConnect が再起動して稼働すると、SSID は設定済みの各 NAM プロファイル (Secure_access) で自動的に使用されます。 EAP-PEAP が使用されます (たとえば、Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) も使用できます)。 同時に、ポスチャ モジュールは、ステーションが準拠しているかどうかを検査します (c:\test.txt ファイルが存在しているかを検査)。

ステップ 3 : ステーション ポスチャの状態が不明である (ポスチャ モジュールからのレポートがない) 場合は、 **Unknown** 認証ルールが ISE で検出されるため、引き続きプロビジョニングのためにリダイレクトされます。 ステーションが準拠すると、ISE は認可変更 (CoA) をワイヤレス LAN コントローラに送信し、そこで再認証がトリガーされます。 2 番目の認証が実行され、 **Compliant** ルールが ISE に適用されます。 これによりユーザには、ネットワークへのフルアクセスが提供されます。

この結果、ユーザに対して、ネットワークへのユニファイド アクセスを許可する AnyConnect の VPN、NAM、ポスチャの各モジュールがプロビジョニングされたことになります。 同様の機能は、VPN アクセス用の適応型セキュリティ アプライアンス (ASA) でも使用できます。 現在、ISE は非常に詳細なアプローチにより、任意のタイプのアクセスについて同じことを行えます。

この機能は社内ユーザのみに制限されていませんが、そのグループのユーザ用に導入する機能としてはおそらくかなり一般的なものとなっています。

設定

WLC

WLC は、次の 2 つの SSID で設定されます。

- Provisioning - [WPA + WPA2][Auth(802.1X)]. この SSID は、AnyConnect のプロビジョニング用に使用されます。
- Secure_access - [WPA + WPA2][Auth(802.1X)]. この SSID は、セキュアなアクセス用に、その SSID に対して設定されている NAM モジュールでエンドポイントがプロビジョニングされた後に使用されます。

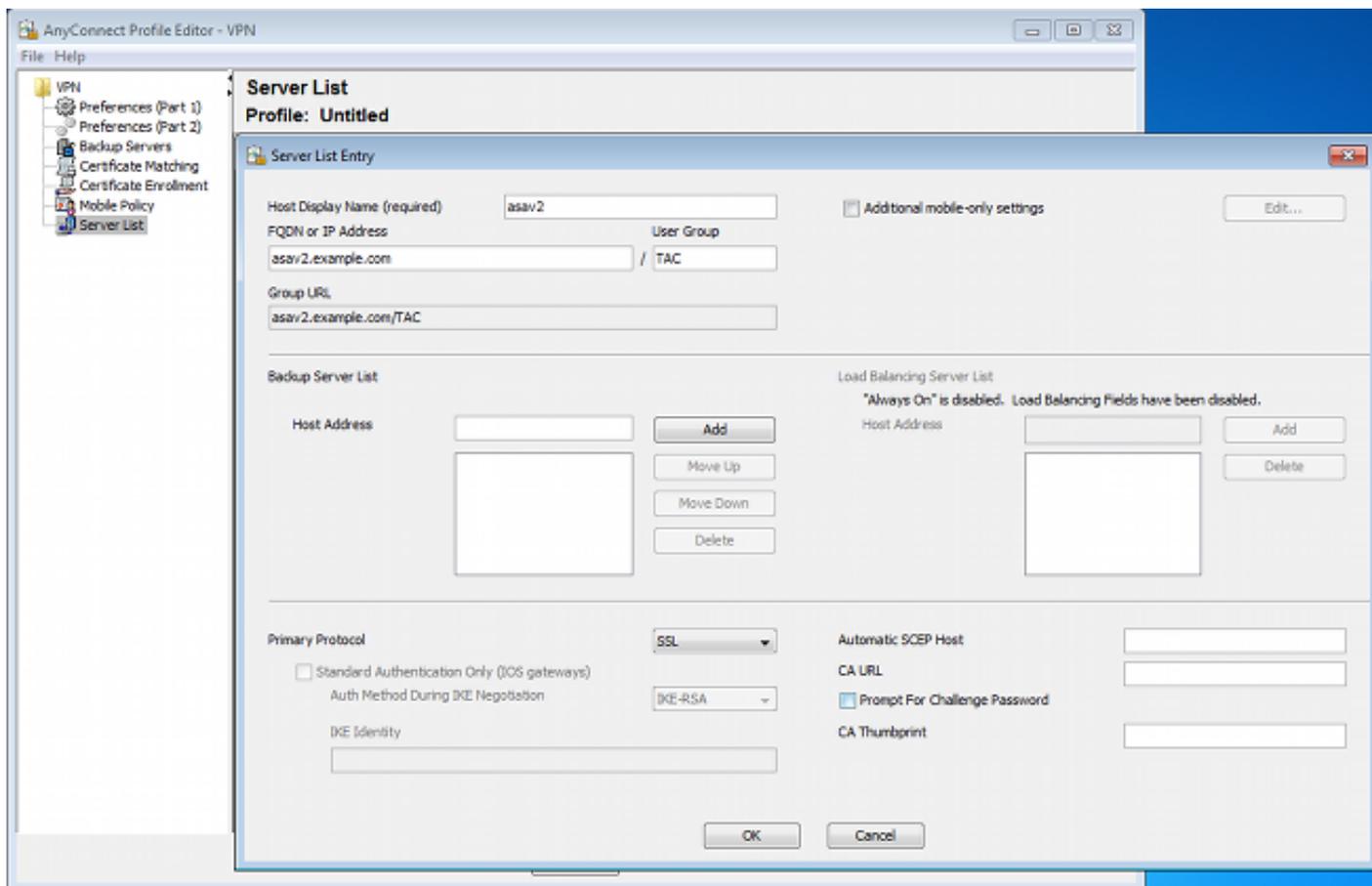
ISE

ステップ 1 : WLC の追加

WLC を ISE 上のネットワーク デバイスに追加します。

手順 2 : VPN プロファイルの設定

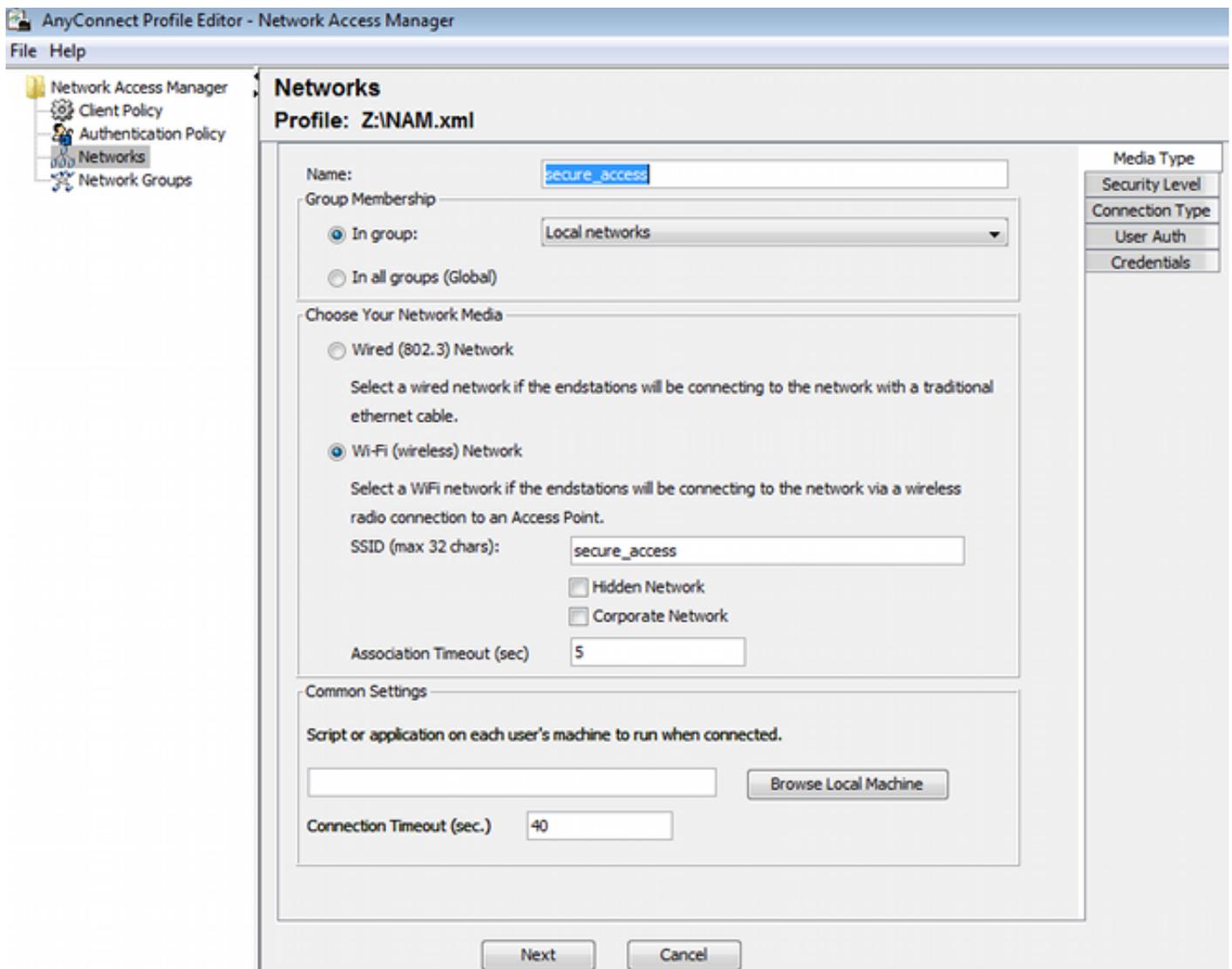
VPN プロファイルを、VPN 用の AnyConnect プロファイル エディタを使用して設定します。



VPN アクセス用に追加されているのは 1 エントリのみです。XML ファイルを VPN.xml に保存します。

手順 3 : NAM プロファイルの設定

NAM プロファイルを、NAM 用の AnyConnect プロファイル エディタを使用して設定します。



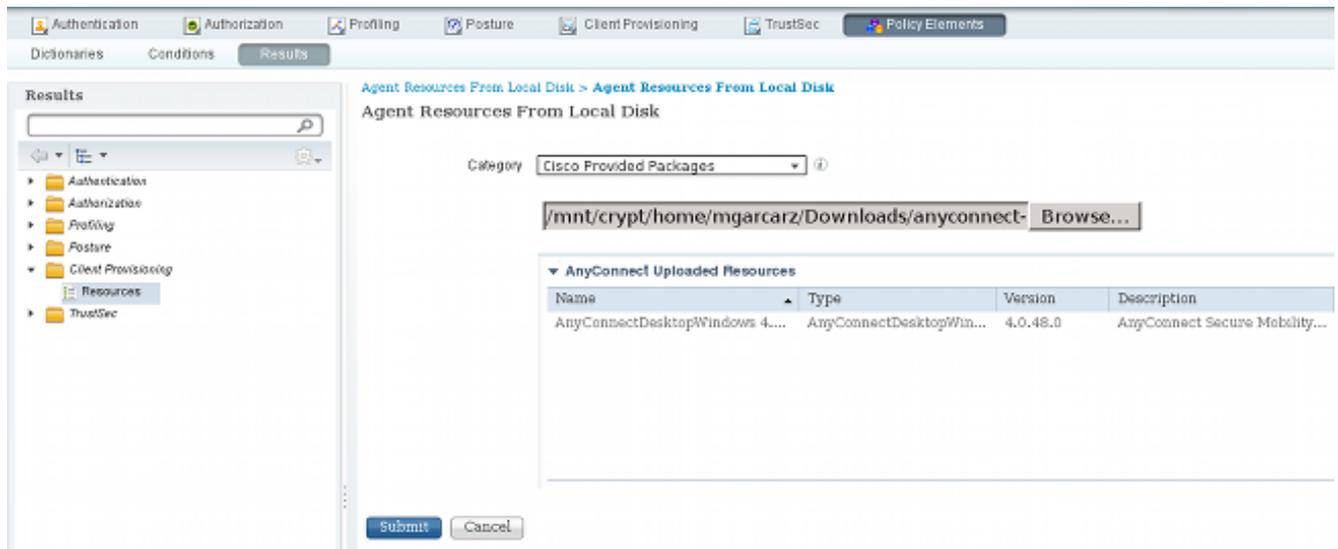
設定されるのは次の1つのSSID、**secure_access**のみです。XML ファイルを **NAM.xml** に保存します。

手順4：アプリケーションのインストール

1. Cisco.com から手動でアプリケーションをダウンロードします。

anyconnect-win-4.0.00048-k9.pkg
anyconnect-win-compliance-3.6.9492.2.pkg

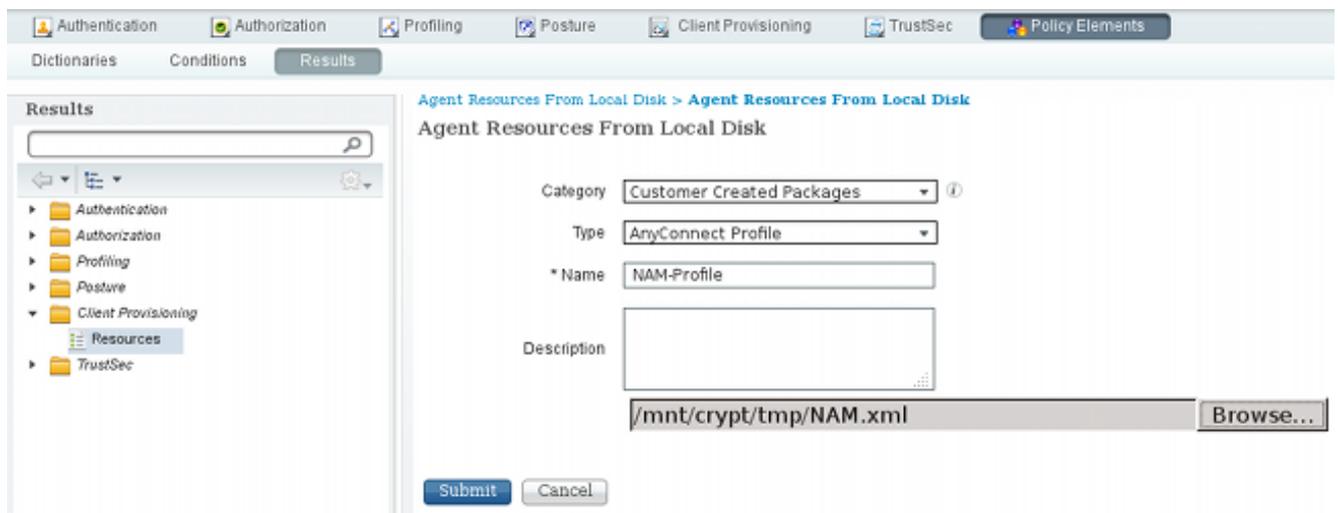
2. ISE 上で、[Policy] > [Results] > [Client Provisioning] > [Resources] と移動し、[Agent Resources From Local Disk] を追加します。
3. [Cisco Provided Packages] を選択して、[anyconnect-win-4.0.00048-k9.pkg] を選択します。



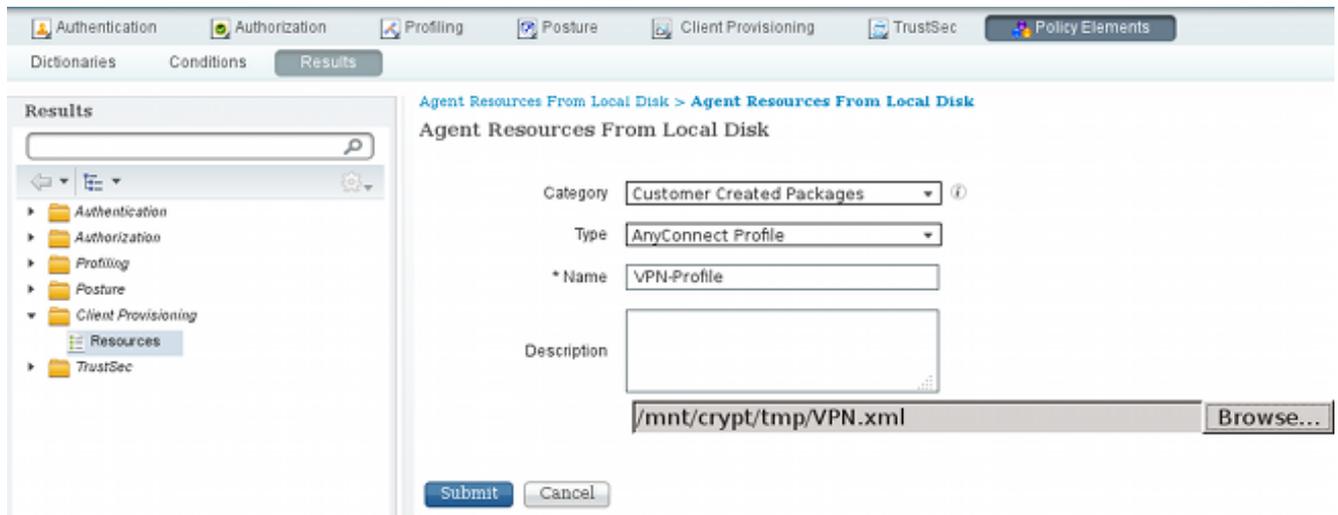
4. コンプライアンス モジュールに対して手順 4 を繰り返します。

ステップ 5 : VPN/NAM プロファイルのインストール

1. [Policy] > [Results] > [Client Provisioning] > [Resources] と移動し、[Agent Resources From Local Disk] を追加します。
2. [Customer Created Packages] を選択し、**AnyConnect Profile** と入力します。以前に作成した NAM プロファイル (XML ファイル) を選択します。



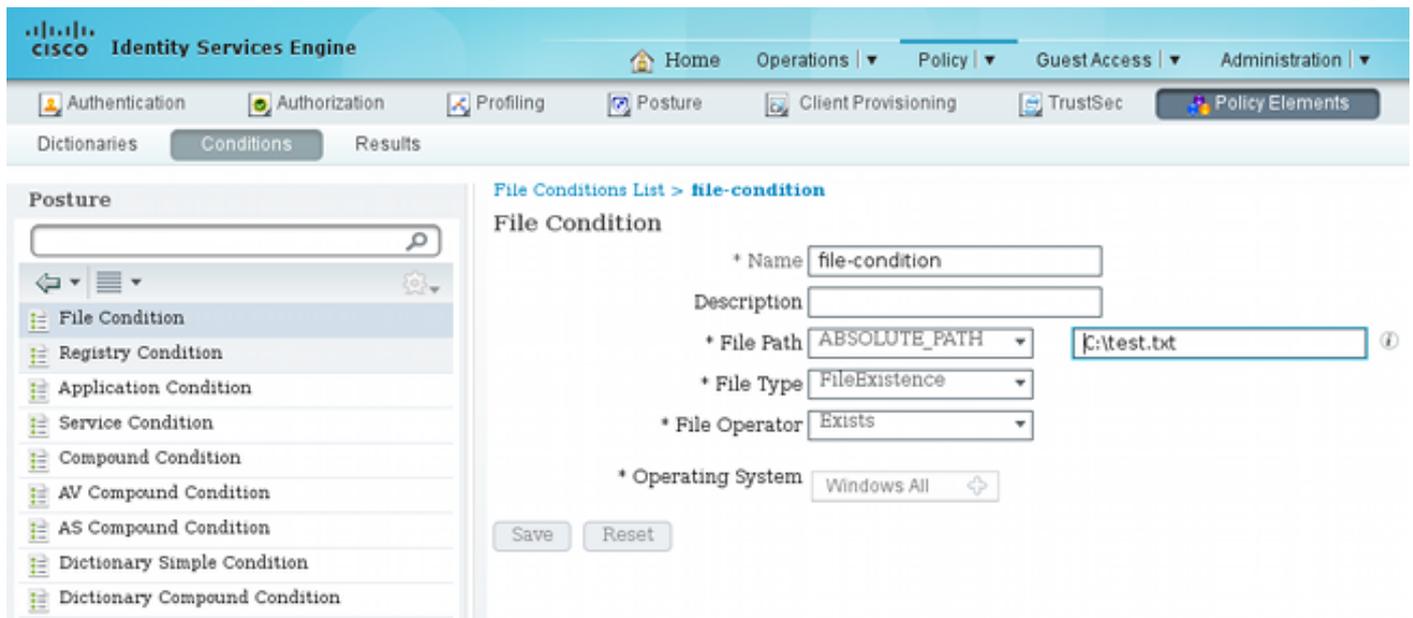
3. VPN プロファイルに対して同様のステップを繰り返します。



ステップ 6 : ポスチャの設定

NAM および VPN プロファイルは、AnyConnect プロファイル エディタにより外部で設定され、ISE にインポートされる必要があります。しかし、ポスチャはすべて ISE 上で設定されます。

[Policy] > [Conditions] > [Posture] > [File Condition] と移動します。ファイル存在のための簡単な条件が作成されていることを確認できます。そのファイルは、ポスチャ モジュールにより検証されるポリシーとの互換性を保つために必要です。



この条件は要件に使用されます。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Operations, Policy, Guest Access, and Administration. Below the navigation bar, there are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy Elements. The main content area is divided into two sections: Results (left) and Requirements (right). The Requirements section displays a table with the following data:

Name	Operating Systems	Conditions	Remediation Actions
FileRequirement	for Windows All	met if file-condition	else Message Text Only
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
Any_AS_Installation_Win	for Windows All	met if ANY_as_win_inst	else Message Text Only
Any_AS_Definition_Win	for Windows All	met if ANY_as_win_def	else AnyASDefRemediationWin
Any_AV_Installation_Mac	for Mac OSX	met if ANY_av_mac_inst	else Message Text Only
Any_AV_Definition_Mac	for Mac OSX	met if ANY_av_mac_def	else AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	met if ANY_as_mac_inst	else Message Text Only
Any_AS_Definition_Mac	for Mac OSX	met if ANY_as_mac_def	else AnyASDefRemediationMac

さらにこの要件は、Microsoft Windows システム用のポスチャ ポリシーで使用されます。

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a Posture Policy. The top navigation bar includes Home, Operations, Policy, Guest Access, and Administration. Below the navigation bar, there are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy Elements. The main content area is titled "Posture Policy" and includes the instruction: "Define the Posture Policy by configuring rules based on operating system and/or other conditions." Below this instruction is a table with the following data:

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
✓	File	if Any	and Windows All		then FileRequirement

ポスチャ設定の詳細については、「[Cisco ISE コンフィギュレーションガイドのポスチャ サービス](#)」を参照してください。

ポスチャ ポリシーの準備ができたら、ポスチャ エージェント設定を追加します。

1. [Policy] > [Results] > [Client Provisioning] > [Resources] と移動し、ネットワーク アドミッション コントロール (NAC) エージェントまたは AnyConnect エージェント ポスチャ プロファイルを追加します。
2. [AnyConnect] を選択します (ISE バージョン 1.3 からの新しいポスチャ モジュールが、古い NAC エージェントの代わりに使用されています)。

3. [Posture Protocol] セクションでは、エージェントがすべてのサーバに接続できるようにするために、**?**を忘れずに追加してください。

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	<input type="text" value="120"/> secs	
Discovery host	<input type="text"/>	
* Server name rules	<input type="text" value="*"/>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all

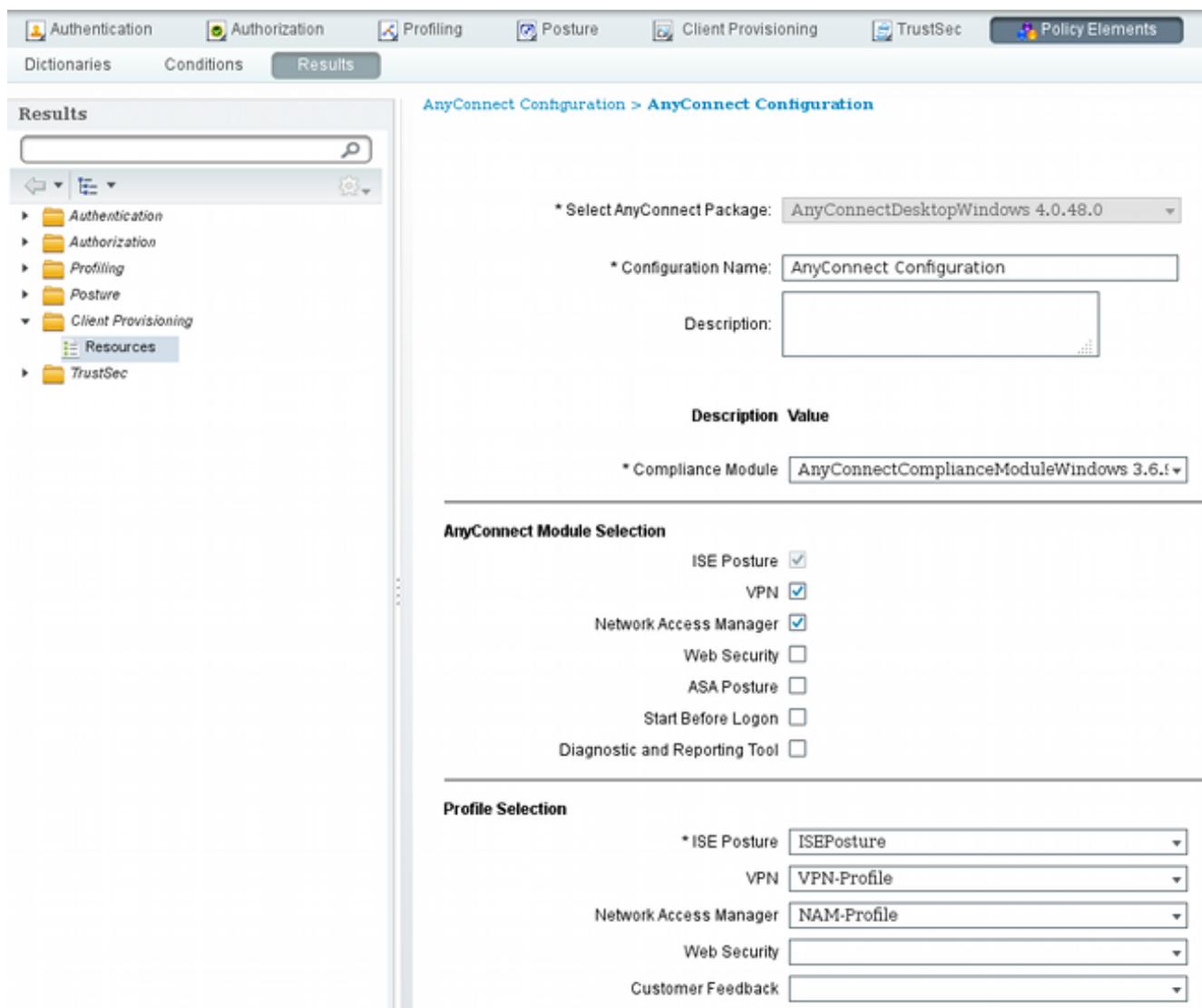
4. [Server name rules] フィールドを空のままにしておくと、ISE は設定を保存せず、次のエラーを報告します。

Server name rules: valid value is required

ステップ 7 : AnyConnect の設定

この段階で、すべてのアプリケーション (AnyConnect) と、すべてのモジュール (VPN、NAM、およびポスチャ) のプロファイル設定は、設定済みとなっています。ここでバインドを実行します。

1. [Policy] > [Results] > [Client Provisioning] > [Resources] と移動し、AnyConnect 設定を追加します。
2. 名前を設定し、コンプライアンス モジュールと、AnyConnect のすべての必須モジュール (VPN、NAM、ポスチャ) を選択します。
3. [Profile Selection] では、各モジュールに対して前に設定したプロファイルを選択します。



4. VPN モジュールは、他のすべてのモジュールが正しく機能するために必須です。VPN モジュールは、インストール用に選択されない場合でも、クライアントにプッシュされてインストールされます。VPN を使用しない場合には、VPN モジュール用のユーザ インターフェイスを非表示にする、VPN 用の特別なプロファイルを設定する可能性があります。これらの行は、VPN.xml ファイルに追加する必要があります。

```
<ClientInitialization>
<ServiceDisable>true</ServiceDisable>
</ClientInitialization>
```

5. さらに、iso パッケージ (anyconnect-win-3.1.06073-pre-deploy-k9.iso) からの Setup.exe を使用する場合にも、この種のプロファイルがインストールされます。それから、VPN 用の VPNDisable_ServiceProfile.xml プロファイルが設定とともにインストールされます。これにより VPN モジュール用のユーザ インターフェイスは無効になります。

ステップ 8： クライアント プロビジョニング ルール

手順 7 で作成された AnyConnect 設定は、次のクライアント プロビジョニング ルールに従って参照される必要があります。

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
AnyconnectWin	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration

クライアントプロビジョニングルールは、どのアプリケーションがクライアントにプッシュされるかを決定します。ここで必要になるのは、手順7で作成した設定を指す結果と、1つのルールのみです。このようにすると、クライアントプロビジョニングにリダイレクトされるすべてのMicrosoft Windows エンドポイントは、AnyConnect 設定をすべてのモジュールとプロファイルを用いて使用します。

手順9：認可プロファイル

クライアントプロビジョニング用の認可プロファイルを作成する必要があります。この場合は次のデフォルトの [Client Provisioning Portal] を使用します。

Authorization Profiles > GuestProvisioning

Authorization Profile

* Name: GuestProvisioning

Description: [Empty]

* Access Type: ACCESS_ACCEPT

Service Template:

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) | ACL: GuestRedirect | Value: Client Provisioning Portal

このプロファイルは、ユーザをプロビジョニングのために、デフォルトの [Client Provisioning Portal] に強制的にリダイレクトします。このポータルは、クライアントプロビジョニングポリシー（手順8で作成されたルール）を評価します。認可プロファイルは、手順10で設定した認証ルールの結果として生成されます。

GuestRedirect アクセスコントロールリスト (ACL) は、WLC 上で定義されている ACL の名前です。この ACL は、どのトラフィックを ISE にリダイレクトするかを決定します。詳細については、「[スイッチおよび Identity Services Engine を使用した中央 Web 認証の設定例](#)」を参照してください。

また、非標準ユーザに限定的なネットワークアクセス (DAACL) を提供する、さらに別の認可プ

ロファイルもあります (LimitedAccess と呼ばれている)。

ステップ 10 : 認可ルール

これらすべては、次の 4 つの認証ルールに結合されます。

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
✓	Compliant	if (Radius:Called-Station-ID CONTAINS secure_access AND Session:PostureStatus EQUALS Compliant)	then PermitAccess
✓	NonCompliant	if (Radius:Called-Station-ID CONTAINS secure_access AND Session:PostureStatus EQUALS NonCompliant)	then LimitedAccess
✓	Unknown	if (Radius:Called-Station-ID CONTAINS secure_access AND Session:PostureStatus EQUALS Unknown)	then GuestProvisioning
✓	Provisioning	if (Radius:Called-Station-ID CONTAINS provisioning AND Session:PostureStatus EQUALS Unknown)	then GuestProvisioning

まずプロビジョニング SSID に接続すると、そこからプロビジョニングのために、デフォルトの [Client Provisioning Portal] にリダイレクトされます (Provisioning という名前のルール)。 Secure_access SSID に接続すると、ポスチャ モジュールからのレポートを ISE が受け取っていない場合には、さらにプロビジョニングのためにリダイレクトされます (Unknown という名前のルール)。エンドポイントが完全に準拠すると、フル アクセスが許可されます (Compliant という名前のルール)。エンドポイントが非準拠と報告されると、ネットワーク アクセスが制限されます (NonCompliant という名前のルール)。

確認

プロビジョニング SSID との関連付けを行い、任意の Web ページへのアクセスを試行すると、[Client Provisioning Portal] にリダイレクトされます。

Firefox Device Security Check

https://ise13.example.com:8443/portal/PortalSetup.action?portal=19f9d160-5e4e-11e4-b905-005056bf2f0a&sessionId=0a3e478500000

CISCO Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Start

AnyConnect が検出されないので、インストールするように求められます。

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect AnyConnect Posture Agent

+ This is my first time here

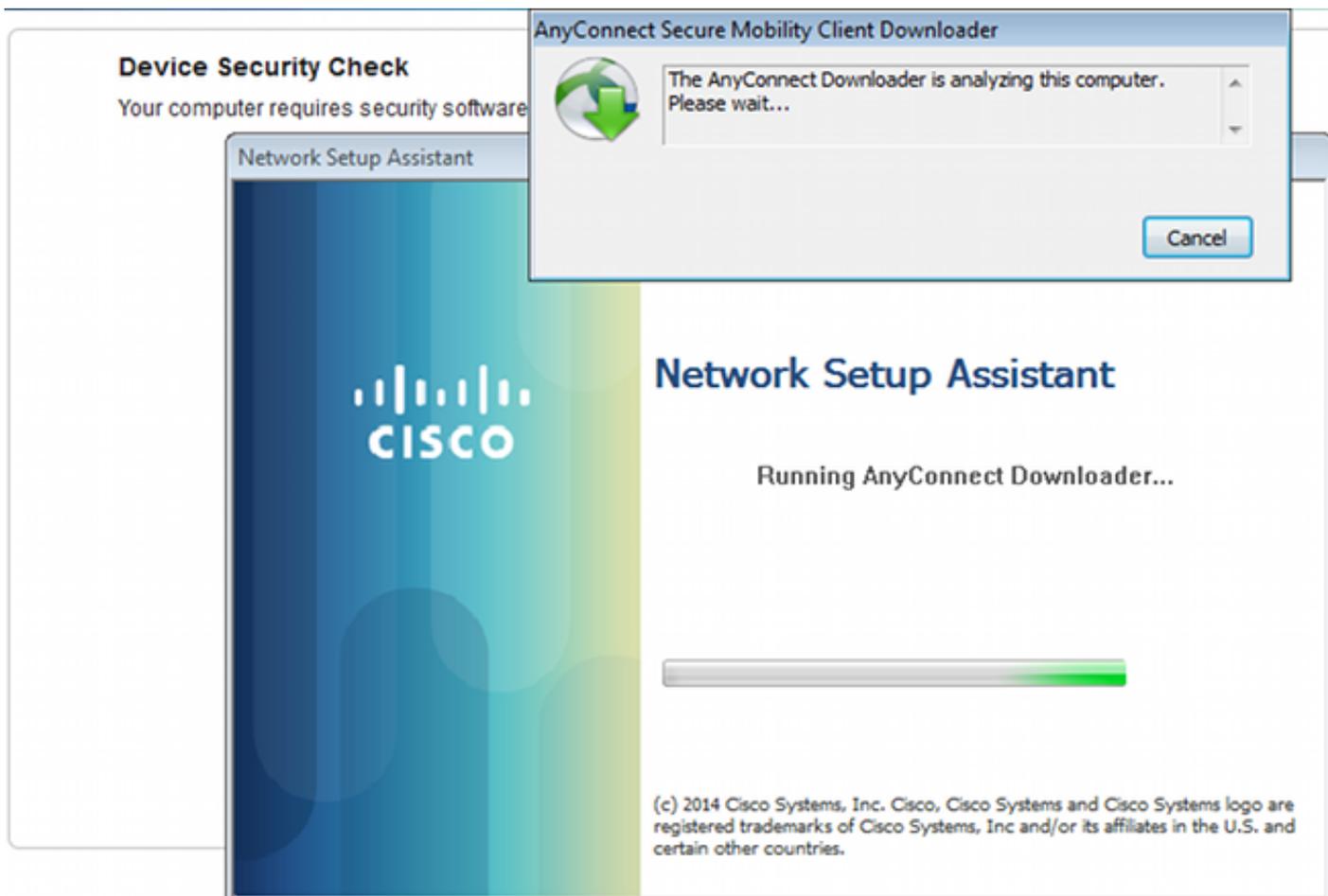
1. You must install AnyConnect to check your device before accessing the network. [Click here to download and install AnyConnect](#)
2. After installation, AnyConnect will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave AnyConnect running so it will automatically scan your device and connect you faster next time you access this network.

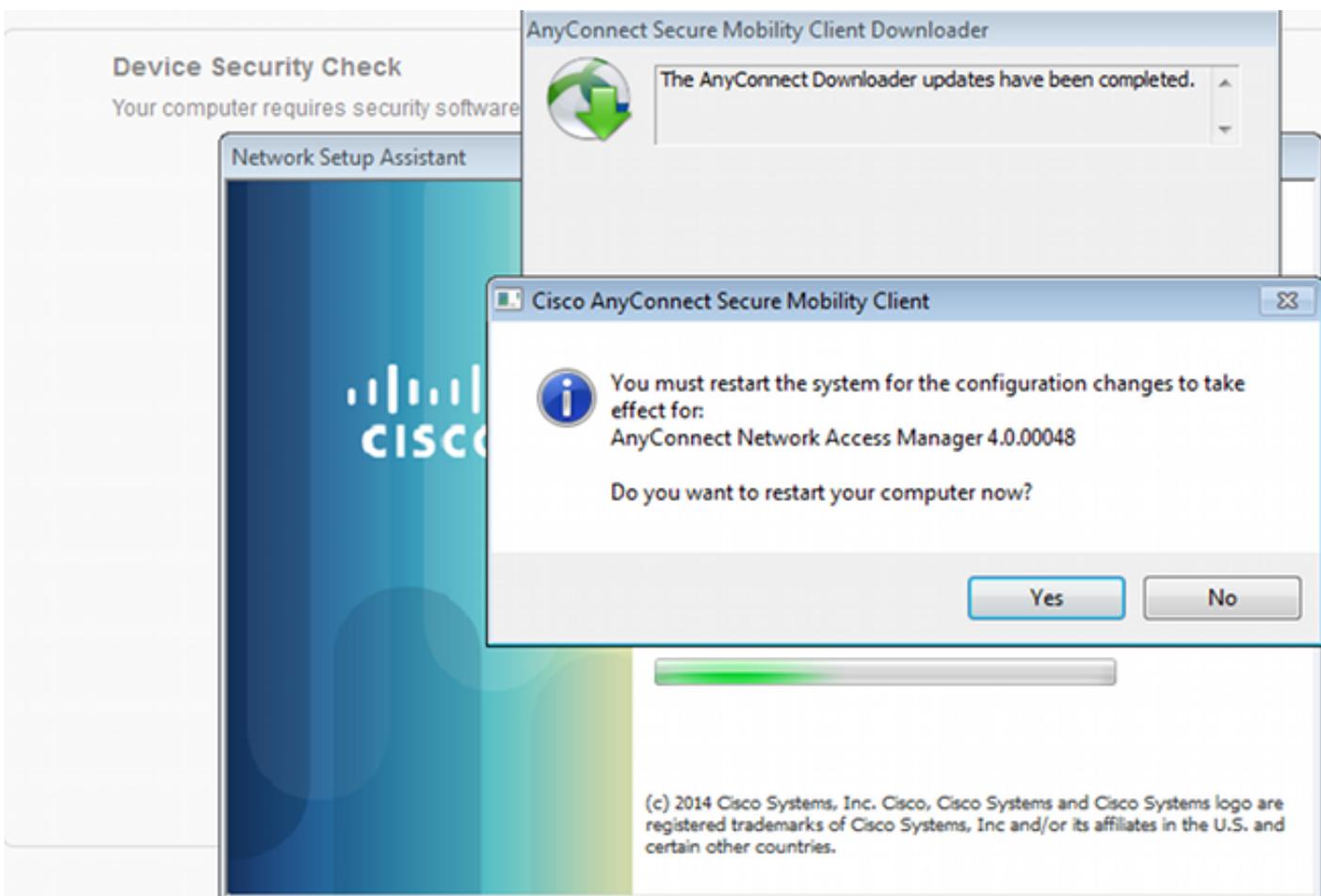
 You have 4 minutes to install and for the compliance check to complete

+ Remind me what to do next

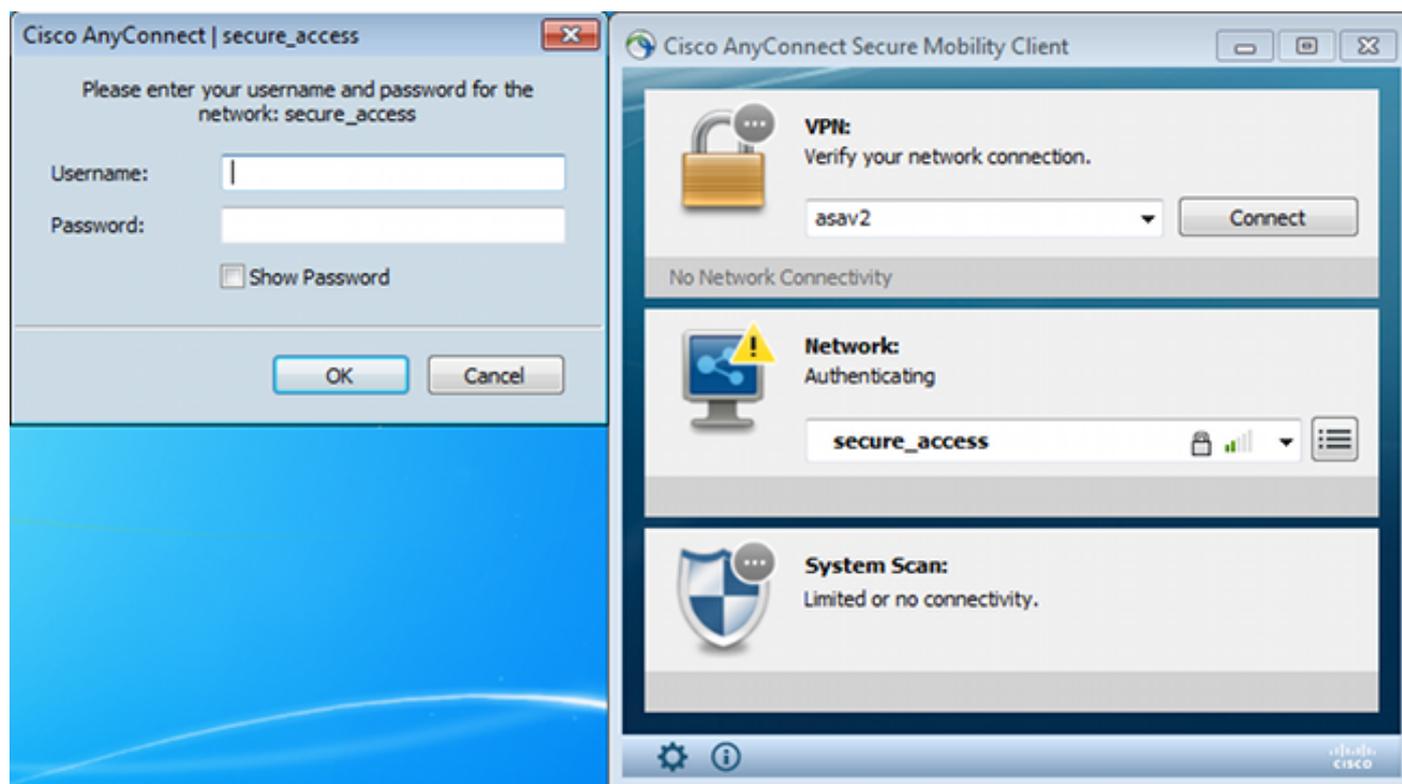
インストール プロセス全体を管理する Network Setup Assistant という小規模なアプリケーションがダウンロードされます。これは、バージョン 1.2 の Network Setup Assistant とは異なっていることに注意してください。



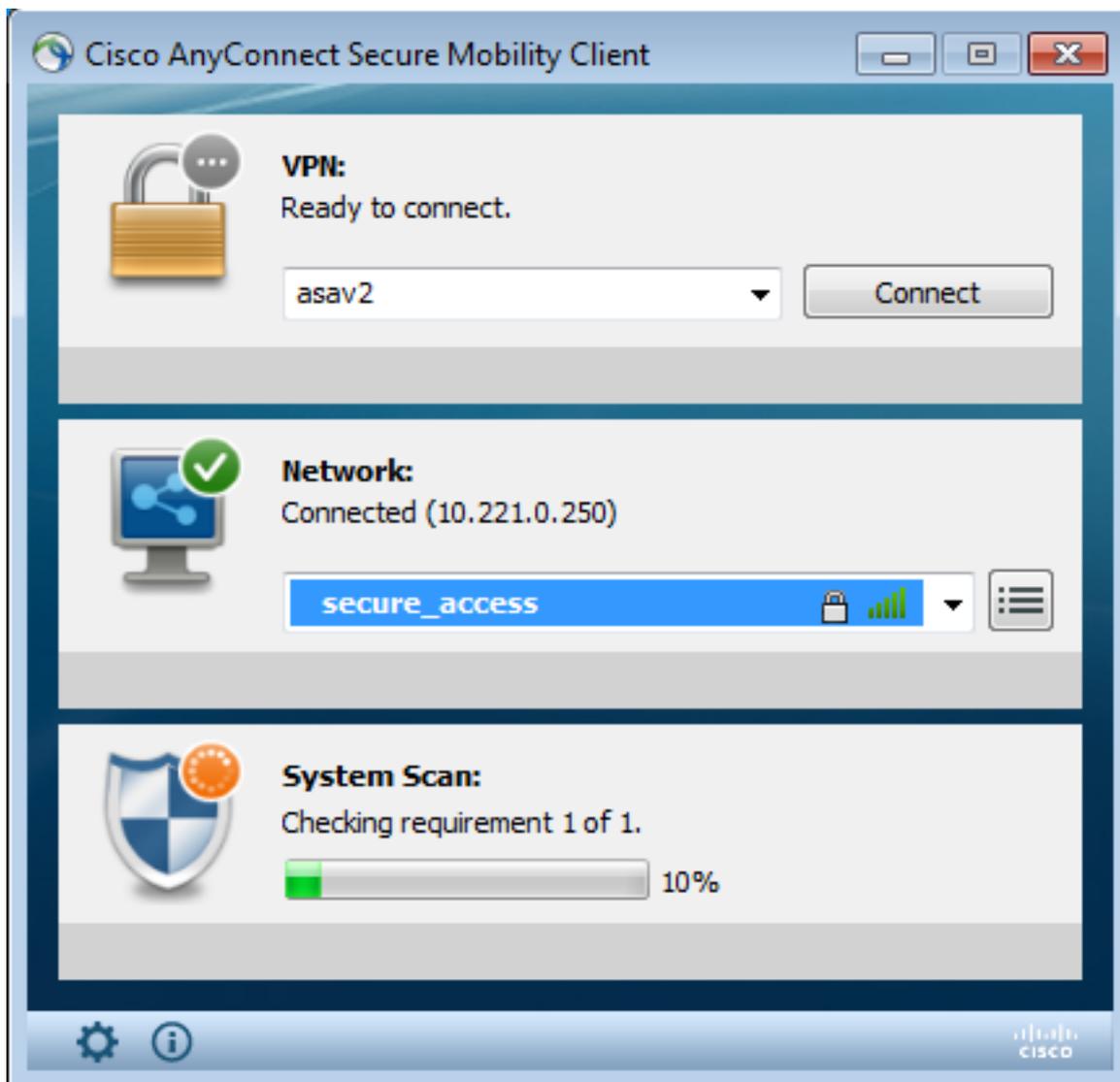
すべてのモジュール（VPN、NAM、ポスチャ）は、インストールされて設定されます。PCを再起動する必要があります。



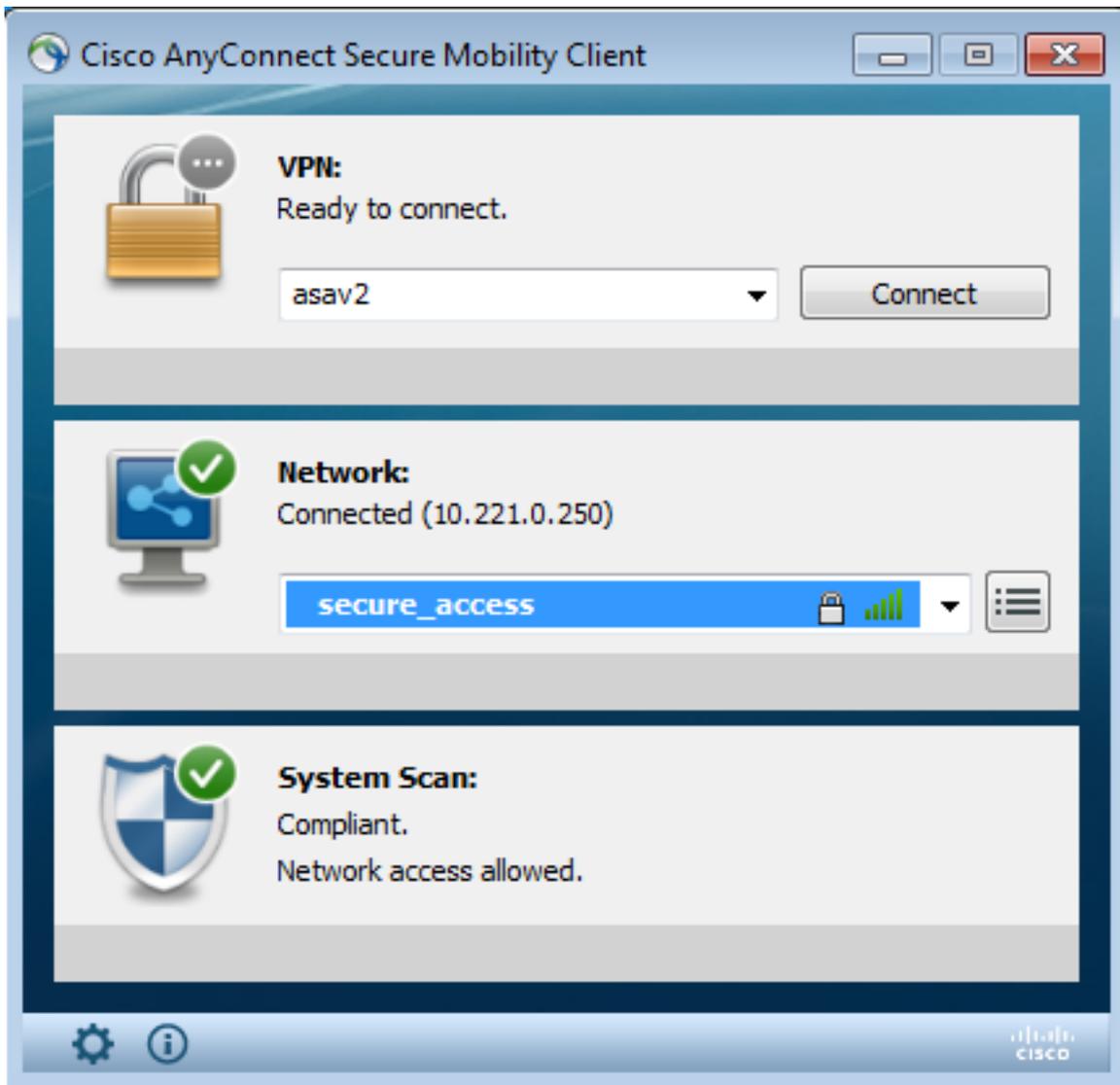
AnyConnect は再起動すると自動的に実行され、NAM は secure_access SSID との関連付けを（設定済みのプロファイルごとに）試行します。VPN プロファイルが正しくインストールされていることに注目してください（VPN のエントリ asav2）。



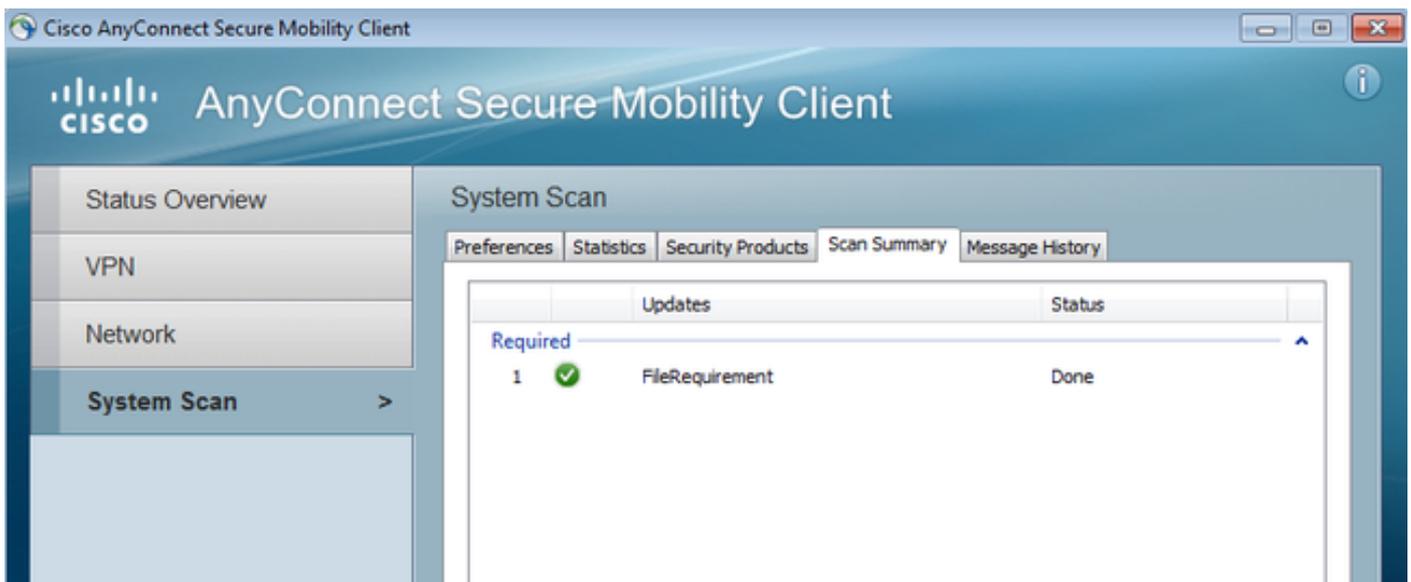
認証後に、AnyConnect は更新をダウンロードし、検証を実行するポスチャルールもダウンロードします。



この段階では、まだアクセス制限がある可能性があります (ISE 上で Unknown 認証ルールが表示されます)。ステーションが準拠すれば、そのことがポスチャ モジュールで報告されます。



詳細も確認できます (FileRequirement は条件を満たしています)。



メッセージ履歴には、次のように詳細な手順が表示されます。

```
9:18:38 AM The AnyConnect Downloader is performing update checks...
9:18:38 AM Checking for profile updates...
9:18:38 AM Checking for product updates...
```

9:18:38 AM Checking for customization updates...
 9:18:38 AM Performing any required updates...
 9:18:38 AM The AnyConnect Downloader updates have been completed.
 9:18:38 AM Update complete.
 9:18:38 AM Scanning system ...
 9:18:40 AM **Checking requirement 1 of 1.**
 9:18:40 AM Updating network settings ...
 9:18:48 AM **Compliant.**

正常なレポートは ISE に送信され、そこで認可変更がトリガーされます。2 番目の認証では Compliant ルールが検出され、ネットワークへのフル アクセスが許可されます。プロビジョニング SSID との関連付けがまだ有効であるときにポスチャレポートを送信すると、それらのログは ISE 上で表示できます。

Time	Status	Det...	R...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Posture Status	Server	Event
2014-11-16 09:32:07...	●	●	●	cisco	CB-4A-00:15-6A-DC				Compliant	ise13	Session State is Started
2014-11-16 09:32:07...	●	●	●	cisco	CB-4A-00:15-6A-DC	Default => Compliant	PermitAccess	WLC1	Compliant	ise13	Authentication succeeded
2014-11-16 09:32:07...	●	●	●	cisco	CB-4A-00:15-6A-DC			WLC1	Compliant	ise13	Dynamic Authorization succeeded
2014-11-16 09:31:35...	●	●	●	admin	CB-4A-00:15-6A-DC			WLC1	Pending	ise13	Authentication failed
2014-11-16 09:29:34...	●	●	●	cisco	CB-4A-00:15-6A-DC	Default => Provisioning	GuestProvisioning	WLC1	Pending	ise13	Authentication succeeded

ポスチャレポートは、次のような内容を示します。

Logged At	Status	Detail	PRA	Identity	Endpoint ID	IP Address	Endpoint OS	Agent	Message
2014-11-16 09:23:25.8	●	●	N/A	cisco	CB-4A-00:15-6A-D	10.221.0.250	Windows 7 Ultimate 64-bit	AnyConnect...	Received a posture report from an endpoint
2014-11-16 09:18:42.2	●	●	N/A	cisco	CB-4A-00:15-6A-D	10.221.0.250	Windows 7 Ultimate 64-bit	AnyConnect...	Received a posture report from an endpoint
2014-11-16 09:16:59.6	●	●	N/A	cisco	CB-4A-00:15-6A-D	10.221.0.250	Windows 7 Ultimate 64-bit	AnyConnect...	Received a posture report from an endpoint
2014-11-16 09:15:17.4	●	●	N/A	cisco	CB-4A-00:15-6A-D	10.221.0.250	Windows 7 Ultimate 64-bit	AnyConnect...	Received a posture report from an endpoint

詳細レポートは、条件が満たされた FileRequirement を示します。

Posture More Detail Assessment

Time Range: From 11/16/2014 12:00:00 AM to 11/16/2014 09:28:48 AM
Generated At: 2014-11-16 09:28:48.404

Client Details

Username:	cisco
Mac Address:	C0:4A:00:15:6A:DC
IP address:	10.221.0.250
Session ID:	0a3e4785000002a354685ee2
Client Operating System:	Windows 7 Ultimate 64-bit
Client NAC Agent:	AnyConnect Posture Agent for Windows 4.0.00048
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-PC
System Domain:	n/a
System User:	admin
User Domain:	admin-PC
AV Installed:	
AS Installed:	Windows Defender;6.1.7600.16385;1.147.1924.0;04/16/2013;

Posture Report

Posture Status:	Compliant
Logged At:	2014-11-16 09:23:25.873

Posture Policy Details

Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions
File	FileRequirement	Mandatory		file-condition		

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [Cisco ISE コンフィギュレーション ガイドのポスチャ サービス](#)
- [Cisco ISE 1.3 アドミニストレータ ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)