AnyConnect 4.0과 ISE 버전 1.3 통합 컨피그레이션 예

목차

소개

이 문서에서는 여러 AnyConnect Secure Mobility Client 모듈을 구성하고 엔드포인트에 자동으로 프로비저닝할 수 있는 Cisco ISE(Identity Services Engine) 버전 1.3의 새로운 기능에 대해 설명합니다.이 문서에서는 ISE에서 VPN, NAM(Network Access Manager) 및 Posture 모듈을 구성하고 이를 기업 사용자에게 푸시하는 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE 구축, 인증 및 권한 부여
- WLC(Wireless LAN Controller) 구성
- 기본 VPN 및 802.1x 지식
- AnyConnect 프로파일 편집기로 VPN 및 NAM 프로파일 구성

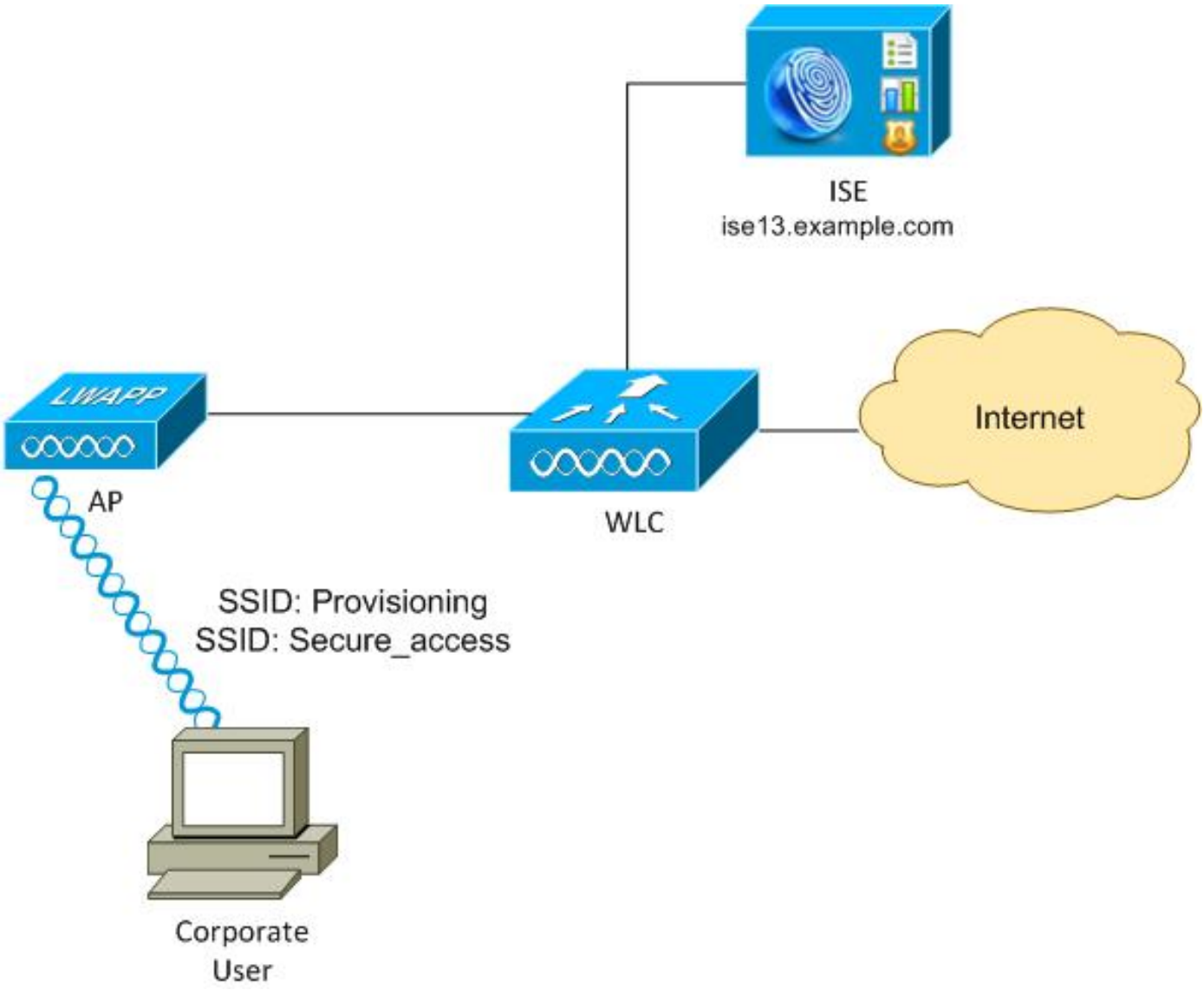
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7
- Cisco WLC 버전 7.6 이상
- Cisco ISE 소프트웨어, 버전 1.3 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

토폴로지 및 흐름



플로우는 다음과 같습니다.

1단계. 회사 사용자가 SSID(Service Set Identifier)에 액세스합니다.프로비저닝.EAP-PEAP(Extensible Authentication Protocol-Protected EAP)를 사용하여 802.1x 인증을 수행합니다. 프로비저닝 **권한 부여** 규칙이 ISE에서 발견되고 사용자가 AnyConnect 프로비저닝을 위해 리디렉션됩니다(클라이언트 프로비저닝 포털을 통해). AnyConnect가 시스템에서 탐지되지 않으면 구성된 모든 모듈이 설치됩니다(VPN, NAM, Posture). 해당 프로필과 함께 각 모듈에 대한 컨피그레이션이 푸시됩니다.

2단계. AnyConnect가 설치되면 사용자가 PC를 재부팅해야 합니다.재부팅 후 AnyConnect가 실행되며 구성된 NAM 프로파일(Secure_access)에 따라 올바른 SSID가 자동으로 사용됩니다.EAP-PEAP가 사용됩니다(예: EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)도 사용할 수 있음). 동시에 Posture 모듈은 스테이션이 호환되는지 확인합니다(c:\test.txt **파일**이 있는지 확인).

3단계. 스테이션 상태 상태를 알 수 없는 경우(포스처 모듈에서 보고서가 없는 경우), ISE에서 **알 수 없는** Authz 규칙이 발견되었기 때문에 프로비저닝을 위해 리디렉션됩니다.스테이션이 호환 되면 ISE는 CoA(Change of Authorization)를 무선 LAN 컨트롤러에 전송하여 재인증을 트리거합니다.두 번째 인증이 발생하고 **Compliant** 규칙이 ISE에 적용되어 사용자에게 네트워크에 대한 전체 액세스 권한을 제공합니다.

따라서 사용자가 네트워크에 대한 통합 액세스를 허용하는 AnyConnect VPN, NAM 및 Posture 모듈로 프로비전되었습니다. VPN 액세스를 위해 ASA(Adaptive Security Appliance)에서 유사한 기능을 사용할 수 있습니다.현재 ISE는 매우 세분화된 접근 방식을 통해 모든 액세스 유형에 대해 동일한 작업을 수행할 수 있습니다.

이러한 기능은 기업 사용자에게만 국한되지 않지만, 해당 사용자 그룹에 대해 배포하는 것이 가장 일반적일 수 있습니다.

구성

WLC

WLC는 두 개의 SSID로 구성됩니다.

- 프로비저닝 - [WPA + WPA2][Auth(802.1X)].이 SSID는 AnyConnect 프로비저닝에 사용됩니다.
- Secure_access - [WPA + WPA2][Auth(802.1X)].이 SSID는 엔드포인트가 해당 SSID에 대해 구성된 NAM 모듈로 프로비저닝된 후 보안 액세스에 사용됩니다.

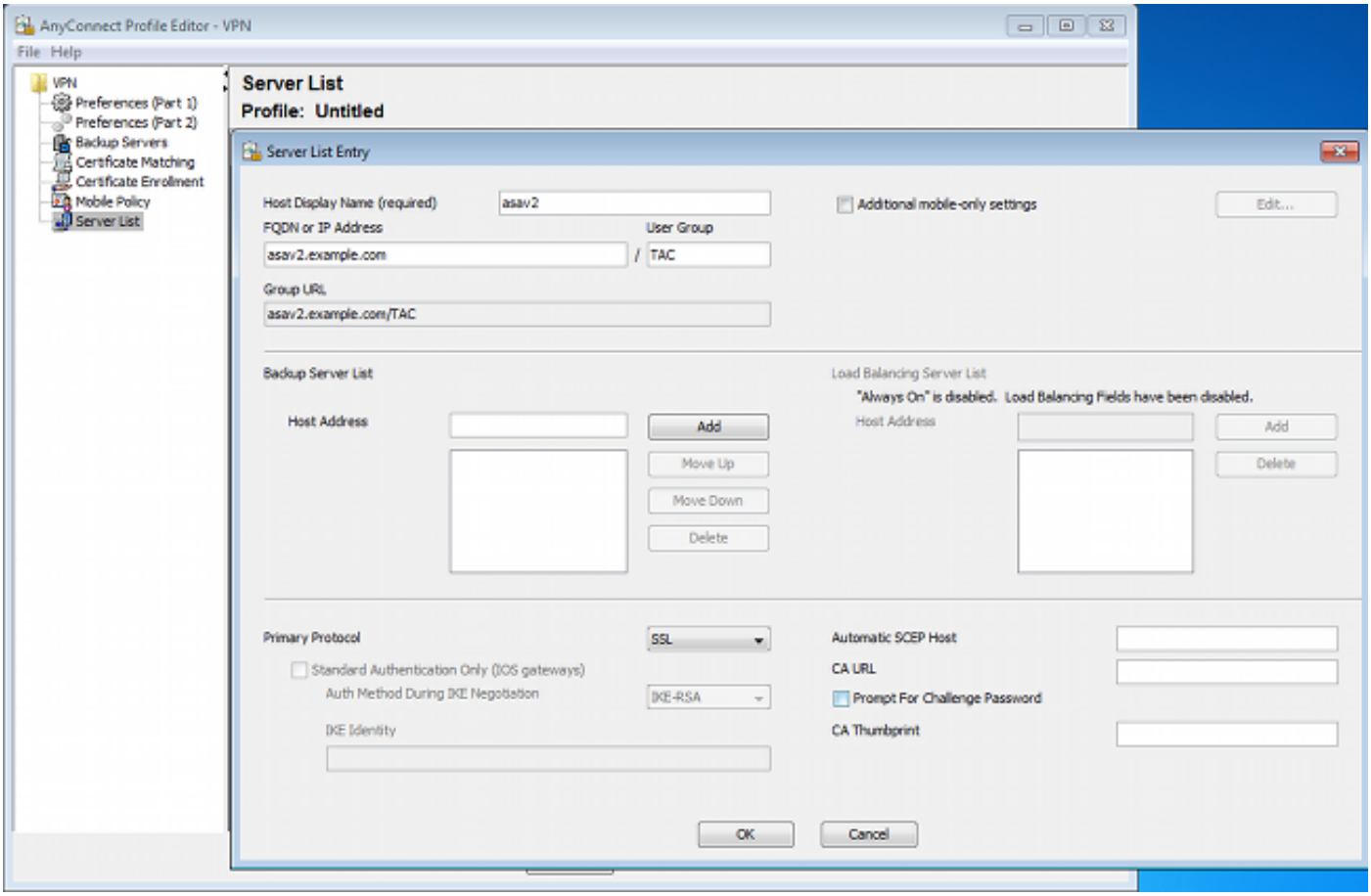
ISE

1단계. WLC를 추가합니다.

ISE의 네트워크 디바이스에 WLC를 추가합니다.

2단계. VPN 프로파일 구성

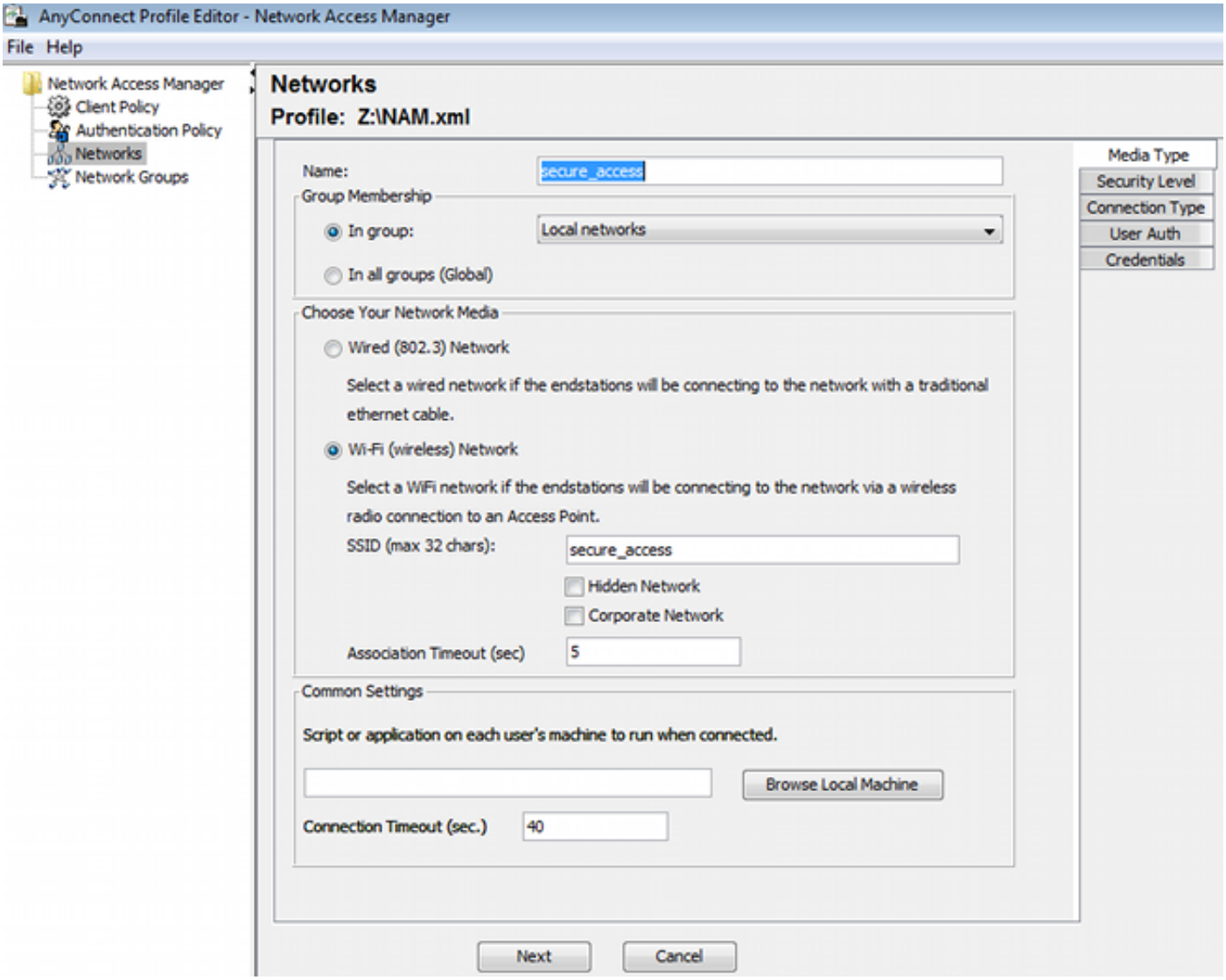
VPN용 AnyConnect 프로파일 편집기를 사용하여 VPN 프로파일을 구성합니다.



VPN 액세스에 대해 하나의 항목만 추가되었습니다.해당 XML 파일을 **VPN.xml에 저장합니다**.

3단계. NAM 프로필 구성

NAM용 AnyConnect 프로파일 편집기를 사용하여 NAM 프로파일을 구성합니다.



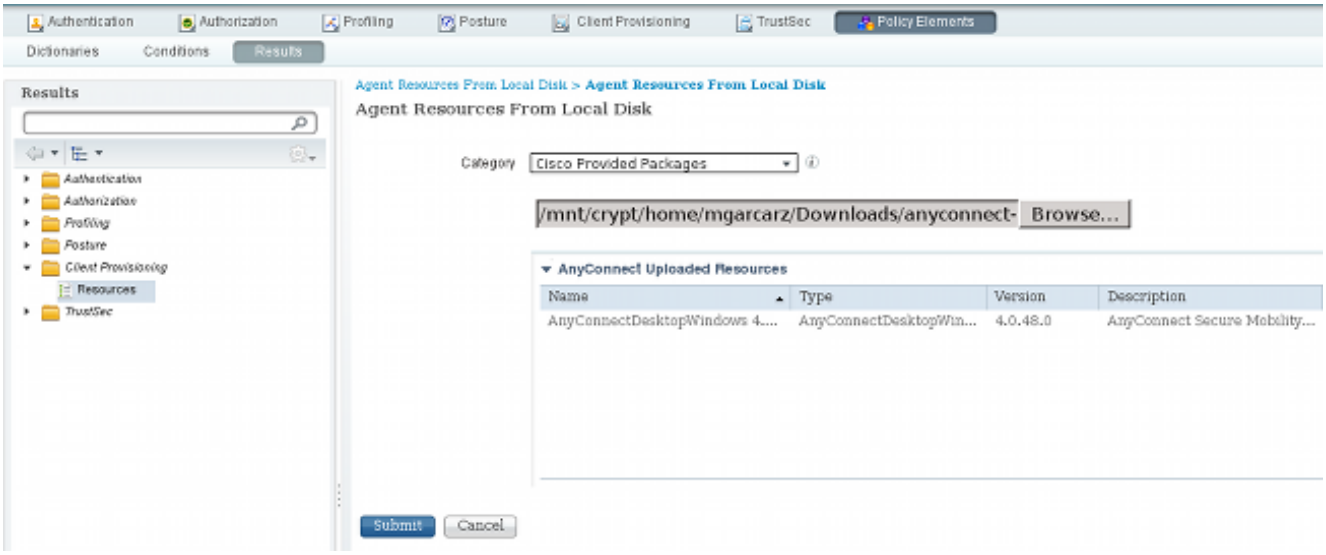
하나의 SSID만 구성되었습니다.**secure_access**.해당 XML 파일을 **NAM.xml에 저장합니다**.

4단계. 응용 프로그램 설치

1. Cisco.com에서 애플리케이션을 수동으로 다운로드합니다.

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

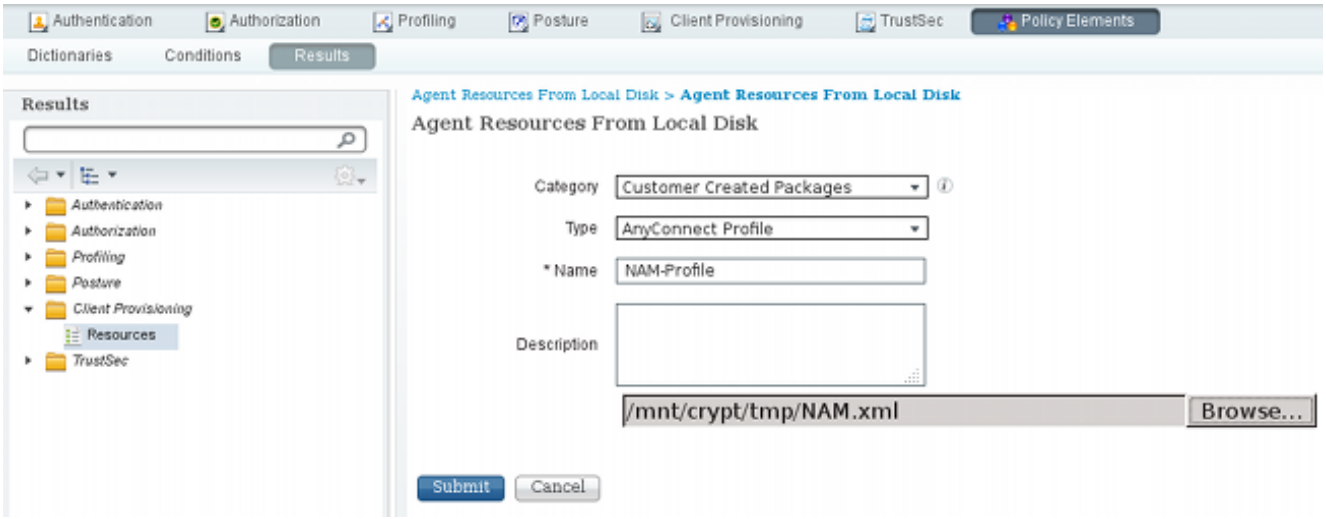
2. ISE에서 **Policy(정책) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동하고** Agent Resources From Local Disk(로컬 디스크에서 에이전트 리소스)를 추가합니다.
3. Cisco Provided Packages(Cisco 제공 패키지)를 선택하고 **anyconnect-win-4.0.00048-k9.pkg을 선택합니다**.



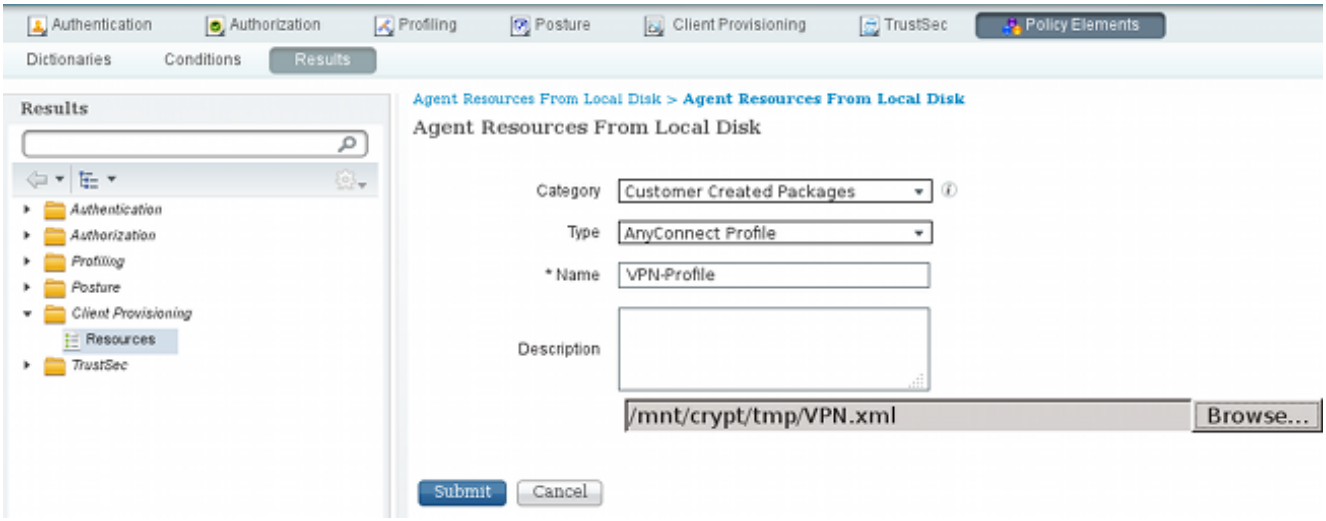
4. 규정 준수 모듈에 대해 4단계를 반복합니다.

5단계. VPN/NAM 프로파일 설치

1. Policy(**정책) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)**로 이동하고 로컬 디스크에서 에이전트 리소스를 추가합니다.
2. Customer Created Packages(고객 생성 패키지)를 선택하고 AnyConnect **Profile(AnyConnect 프로파일)을 입력합니다**.이전에 생성한 NAM 프로필(XML 파일)을 선택합니다.



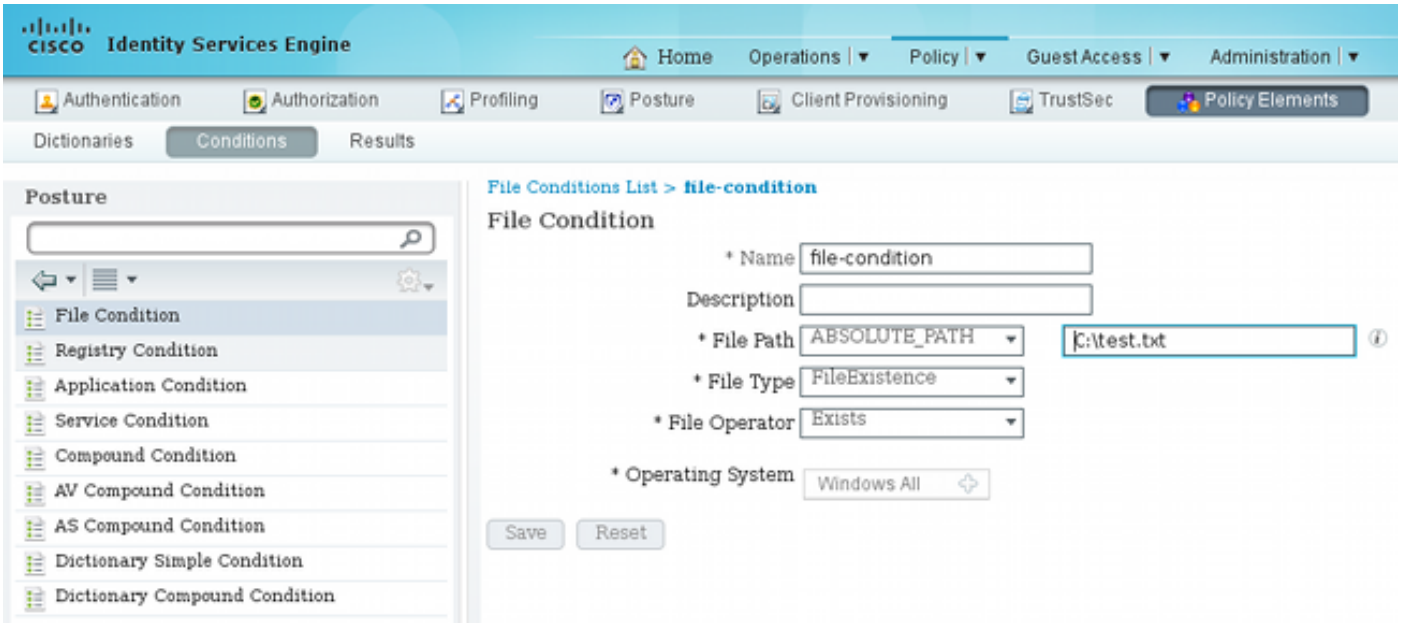
3. VPN 프로필에 대해 유사한 단계를 반복합니다.



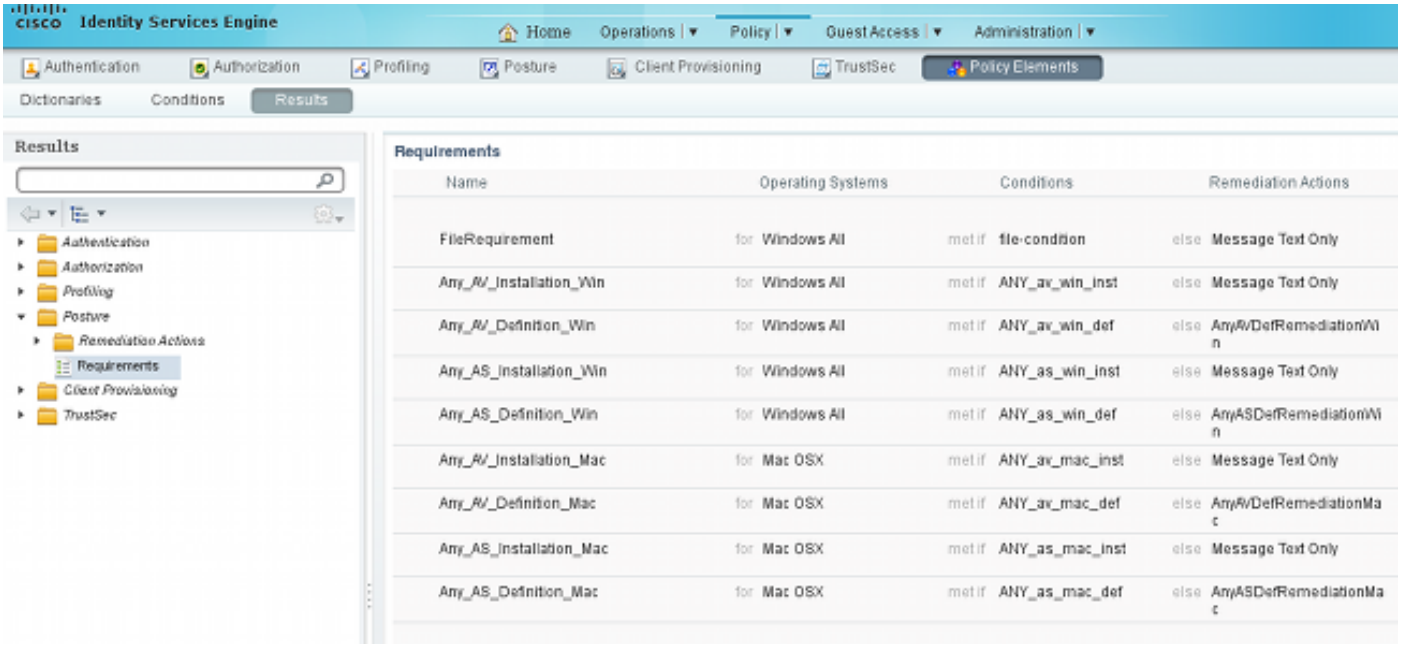
6단계. 상태 구성

NAM 및 VPN 프로파일은 AnyConnect 프로파일 편집기로 외부에서 구성하고 ISE로 가져와야 합니다.그러나 Posture는 ISE에서 완전히 구성됩니다.

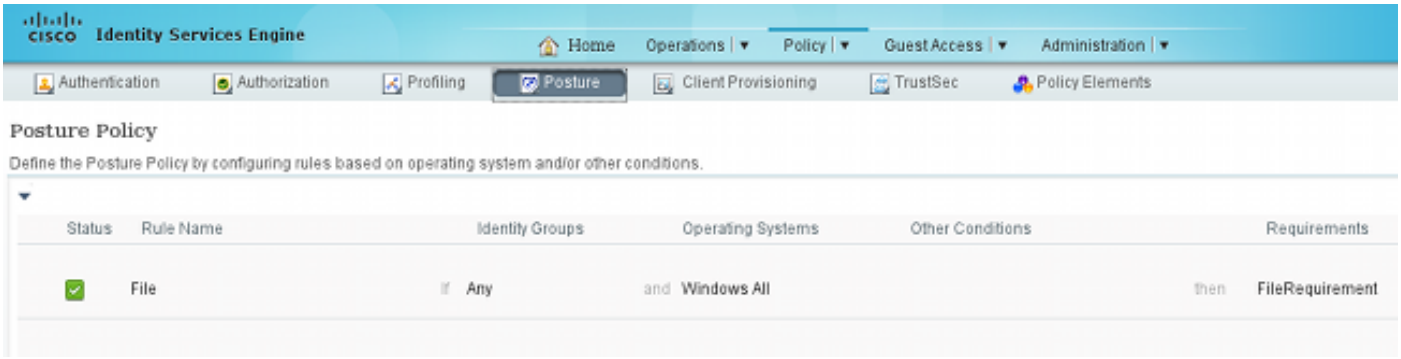
Policy(**정책) > Conditions(조건) > Posture(포스처) > File Condition(파일 조건)으로 이동합니다**.파일 존재에 대한 간단한 조건이 생성되었음을 확인할 수 있습니다.Posture 모듈에서 확인한 정책을 준수하려면 해당 파일이 있어야 합니다.



이 조건은 요구 사항에 사용됩니다.



Microsoft Windows 시스템의 상태 정책에 요구 사항이 사용됩니다.

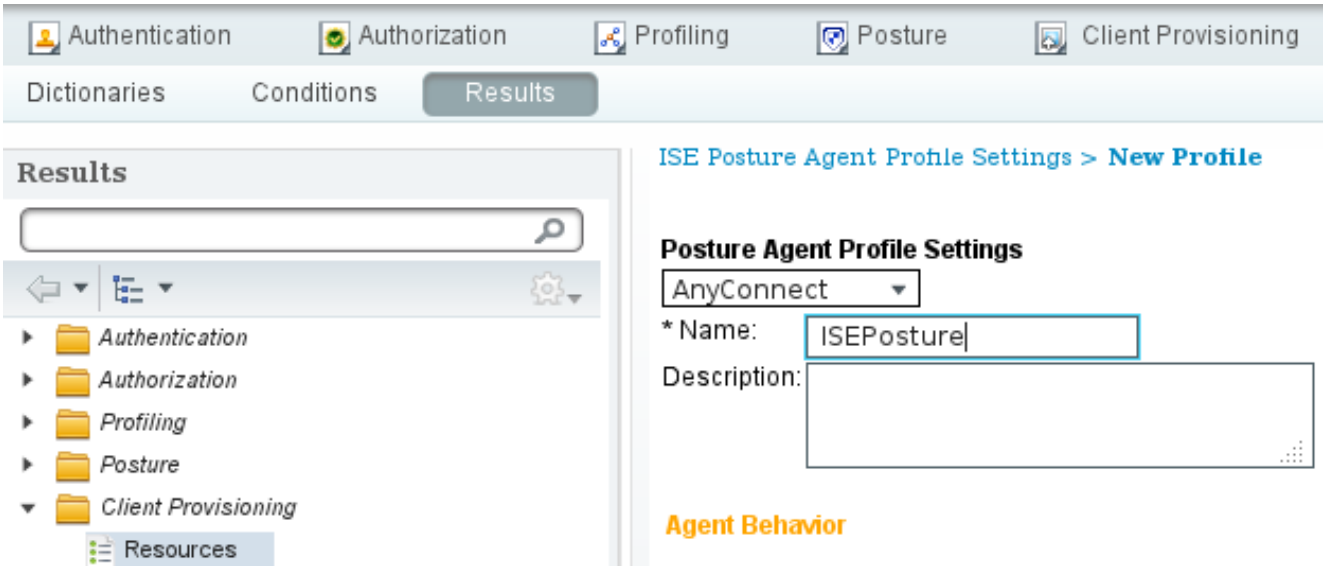


Posture 컨피그레이션에 대한 자세한 내용은 Cisco ISE 컨피그레이션 가이드에서 포스처 서비스를 참조하십시오.

포스처 정책이 준비되면 포스처 에이전트 컨피그레이션을 추가할 차례입니다.

1. Policy(**정책) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스)로 이동하고** NAC(Network Admission Control) Agent 또는 AnyConnect Agent Posture Profile(NAC(Network Admission Control) 또는 AnyConnect 에이전트 포스처 프로파일)을 추가합니다.

2. AnyConnect 선택(이전 NAC Agent 대신 ISE 버전 1.3의 새 포스처 모듈이 사용됨):



3. Posture Protocol 섹션에서 에이전트가 모든 서버에 연결할 수 있도록 *를 추가하는 것을 잊지 마십시오.

Posture Protocol

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

4. Server name rules(서버 이름 규칙) 필드가 비어 있으면 ISE는 설정을 저장하지 않고 다음 오류를 보고합니다.

```
Server name rules: valid value is required
```

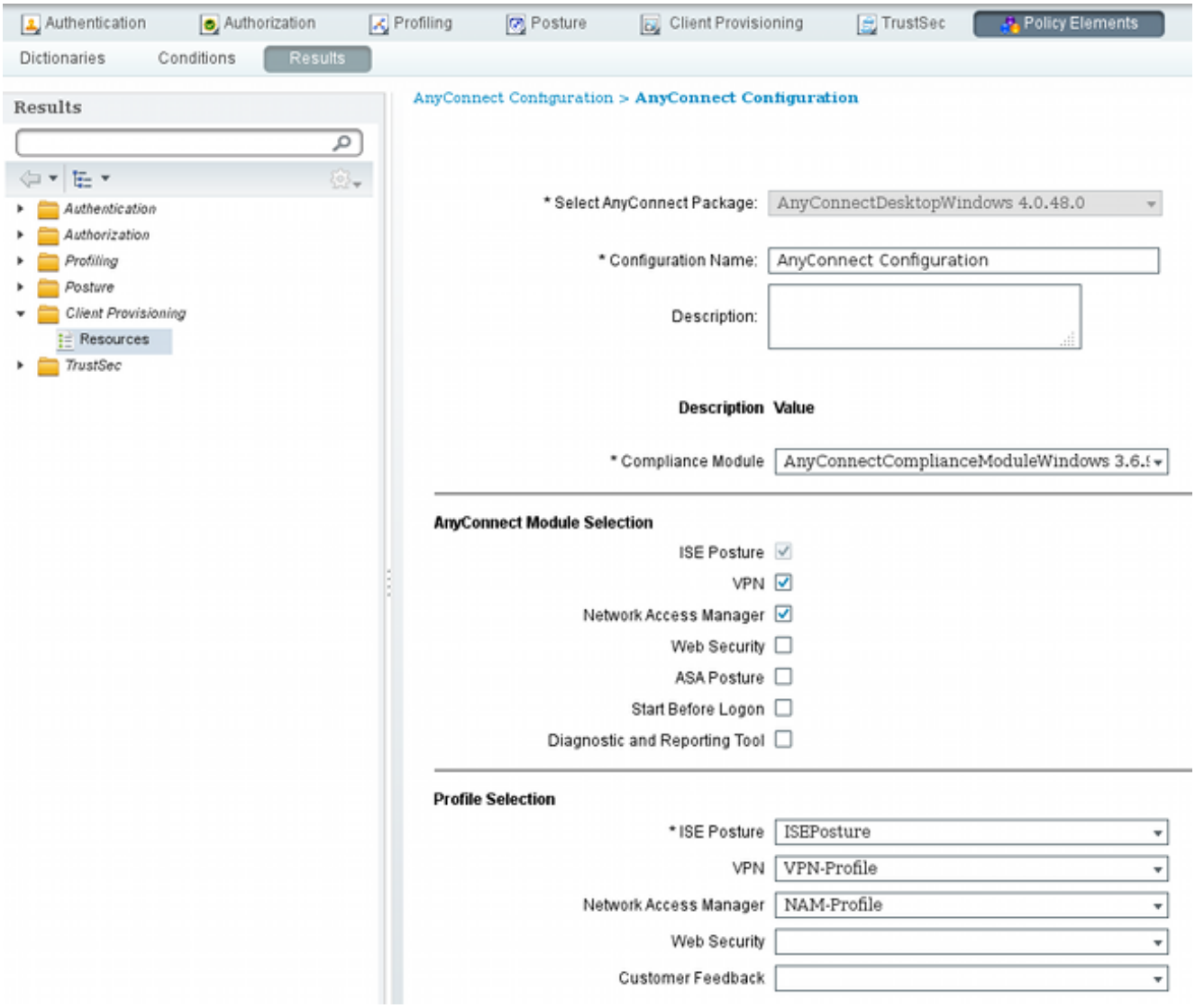
7단계. AnyConnect 구성

이 단계에서는 모든 애플리케이션(AnyConnect) 및 모든 모듈(VPN, NAM 및 Posture)에 대한 프로파일 컨피그레이션이 구성되었습니다.그것을 함께 묶어야 할 때이다.

1. Policy(**정책) > Results(결과) > Client Provisioning(클라이언트 프로비저닝) > Resources(리소스**)로 이동하고 AnyConnect Configuration(AnyConnect 컨피그레이션)을 추가합니다.

2. 이름을 구성하고 규정 준수 모듈 및 필요한 모든 AnyConnect 모듈(VPN, NAM 및 Posture)을 선택합니다.

3. Profile Selection(프로필 선택)에서 각 모듈에 대해 이전에 구성된 프로필을 선택합니다.



4. 다른 모든 모듈이 올바르게 작동하려면 VPN 모듈이 필수입니다.VPN 모듈을 설치하도록 선택하지 않은 경우에도 클라이언트에 푸시되어 설치됩니다.VPN을 사용하지 않으려는 경우 VPN 모듈의 사용자 인터페이스를 숨기는 VPN에 대해 특수 프로필을 구성할 수 있습니다.다음 행은 **VPN.xml 파일**에 추가해야 합니다.

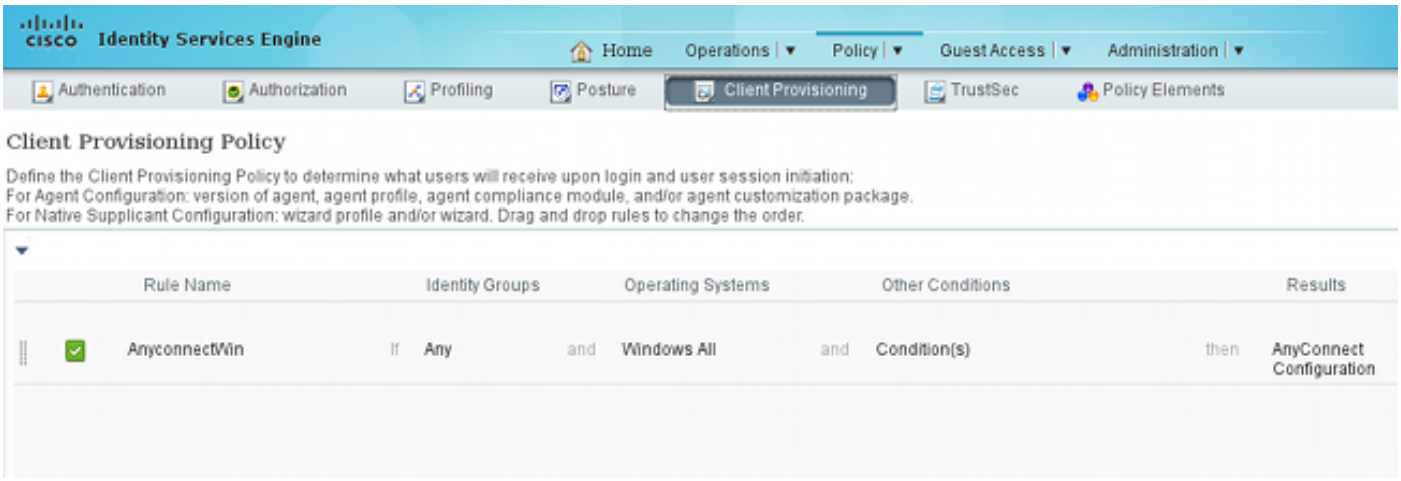
```
<ClientInitialization>

</ClientInitialization>
```

5. 이러한 종류의 프로필은 iso 패키지(anyconnect-win-3.1.06073-pre-deploy-k9.iso)에서 **Setup.exe**를 사용할 때도 설치됩니다. 그런 다음 VPN용 **VPNDisable_ServiceProfile.xml** 프로파일이 컨피그레이션과 함께 설치되며, 이는 VPN 모듈에 대한 사용자 인터페이스를 비활성화합니다.

8단계. 클라이언트 프로비저닝 규칙

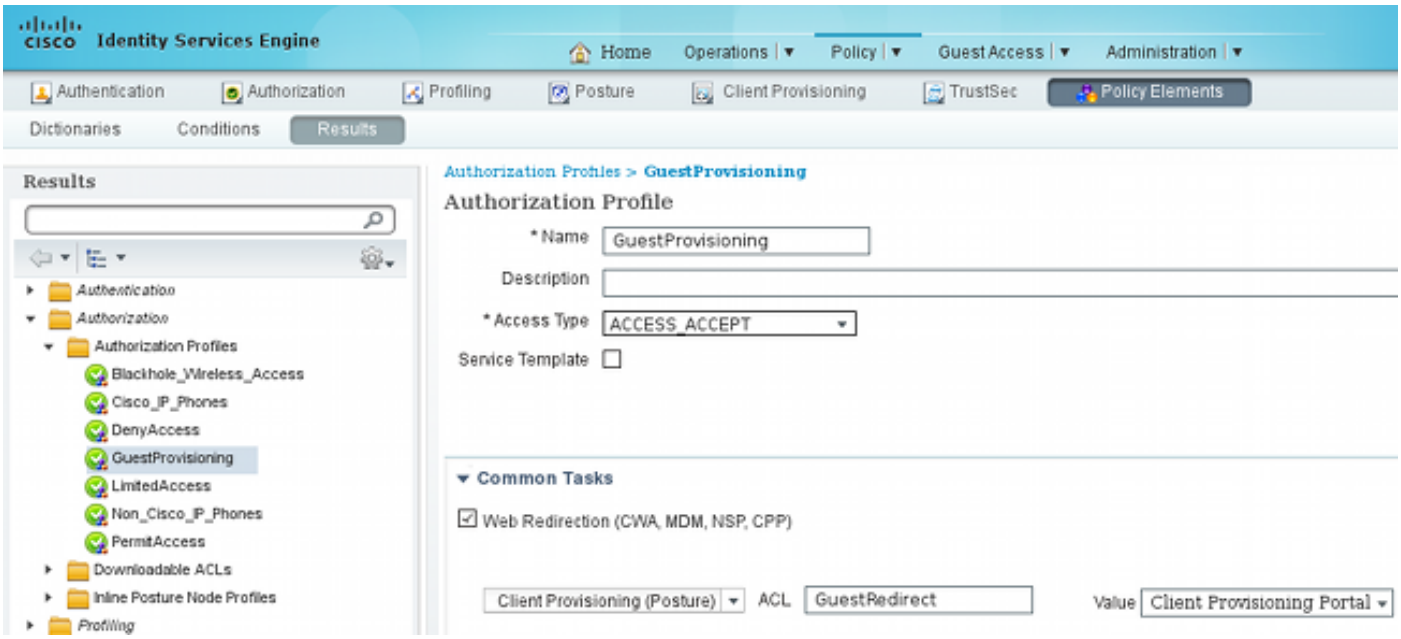
7단계에서 생성한 AnyConnect 컨피그레이션은 클라이언트 프로비저닝 규칙에서 참조되어야 합니다.



클라이언트 프로비저닝 규칙은 클라이언트에 푸시될 애플리케이션을 결정합니다.7단계에서 만든 구성을 가리키는 결과 하나의 규칙만 필요합니다. 이렇게 하면 클라이언트 프로비저닝을 위해 리디렉션되는 모든 Microsoft Windows 엔드포인트는 모든 모듈과 프로필과 함께 AnyConnect 구성을 사용합니다.

9단계. 권한 부여 프로파일

클라이언트 프로비저닝을 위한 권한 부여 프로파일을 만들어야 합니다.기본 클라이언트 프로비저닝 포털이 사용됩니다.



이 프로파일은 기본 클라이언트 프로비저닝 포털로 프로비저닝하기 위해 사용자를 리디렉션합니다.이 포털은 클라이언트 프로비저닝 정책(8단계에서 생성된 규칙)을 평가합니다. 권한 부여 프로파일은 10단계에서 구성된 권한 부여 규칙의 결과입니다.

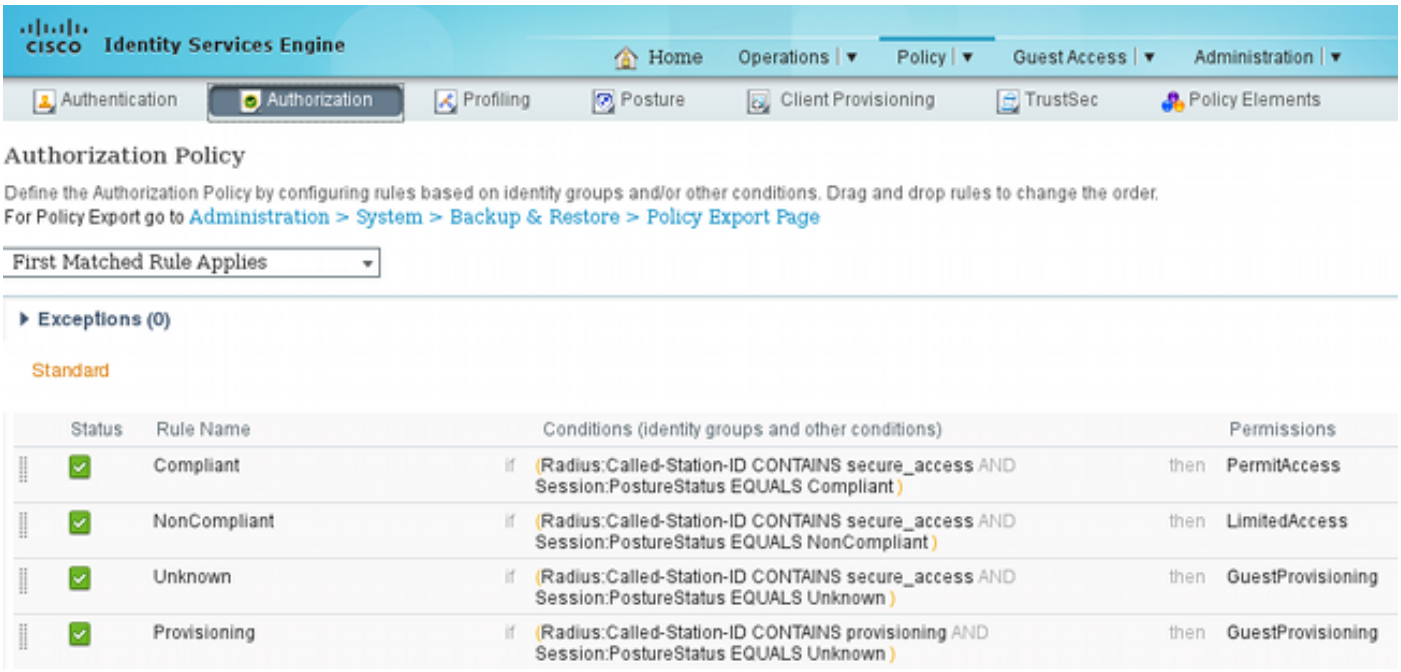
GuestRedirect ACL(Access Control List)은 WLC에 정의된 ACL의 이름입니다.이 ACL은 어떤 트래픽을 ISE로 리디렉션할지 결정합니다.자세한 내용은 스위치 및 Identity Services Engine 컨피그레이션을 사용한 중앙 웹 인증 예를 참조하십시오.

또한 규정 미준수 사용자(LimitedAccess라고 함)를 위한 제한된 네트워크 액세스(DACL)를 제공하

는 또 다른 권한 부여 프로파일이 있습니다.

10단계. 권한 부여 규칙

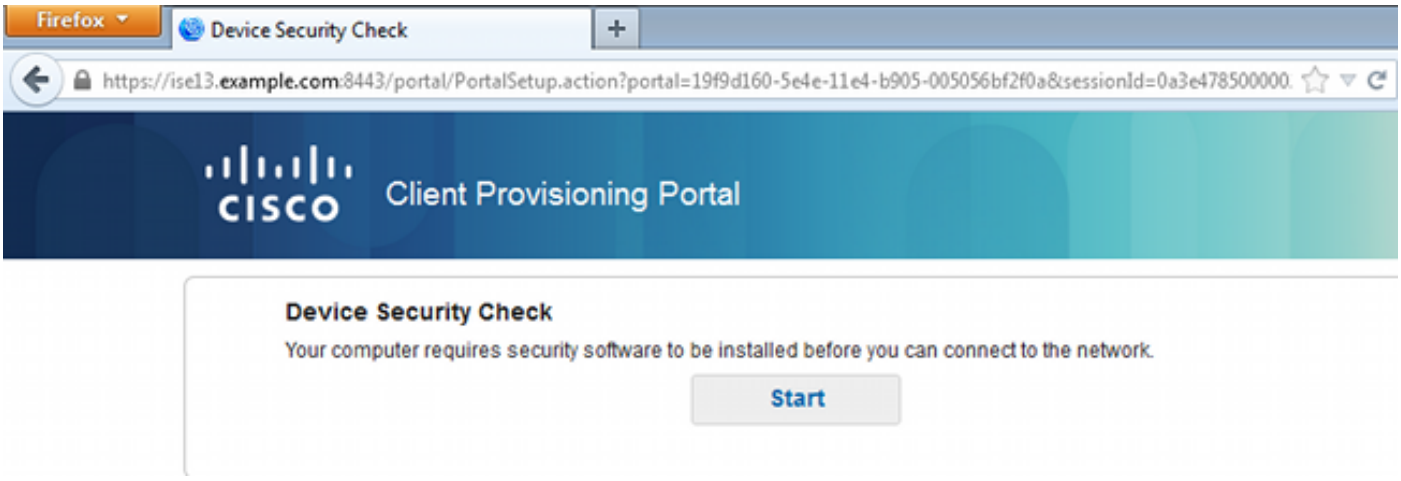
이 모든 항목은 4개의 권한 부여 규칙으로 통합됩니다.



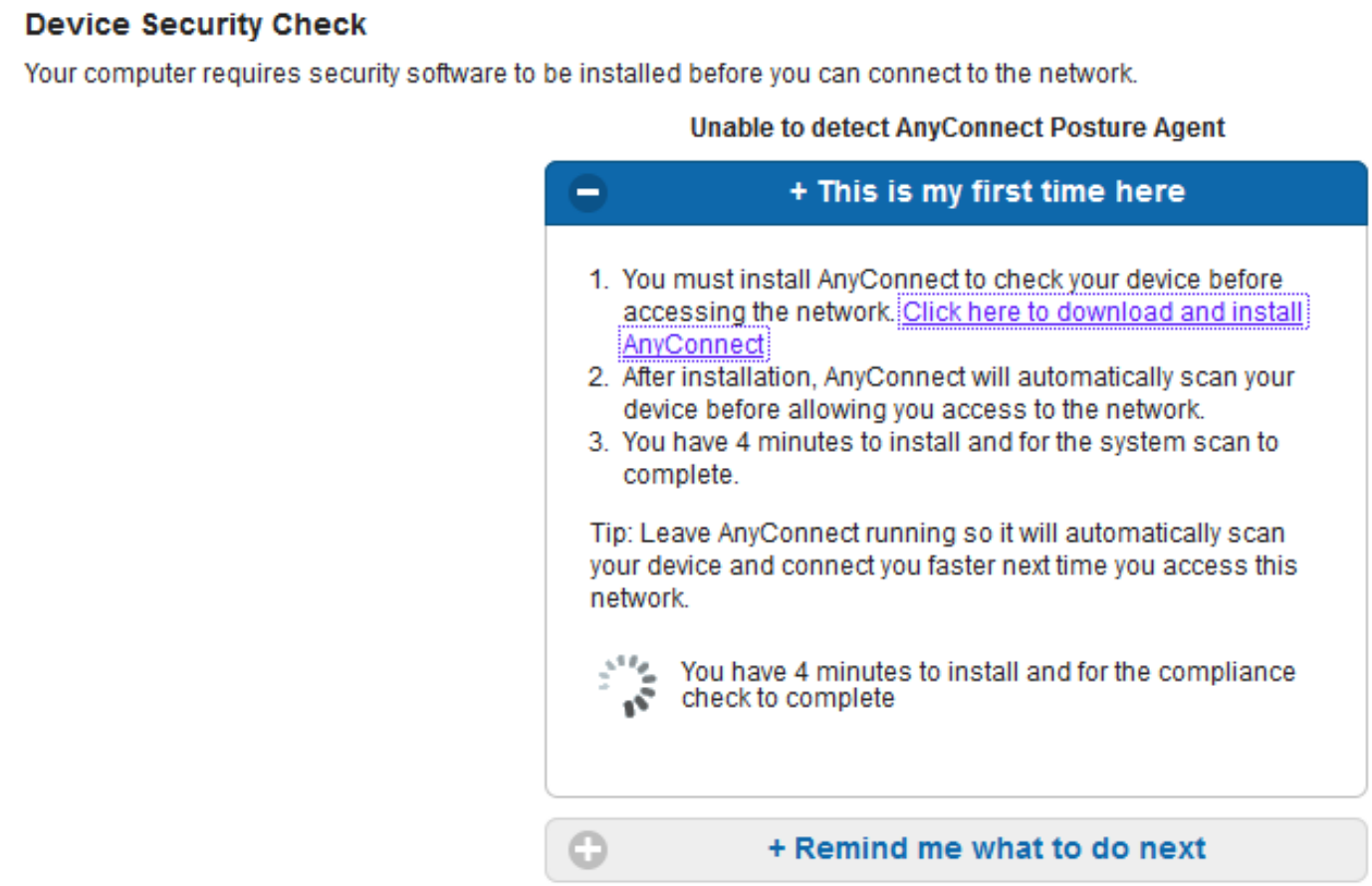
먼저 프로비저닝 SSID에 연결하고 기본 클라이언트 프로비저닝 포털(프로비저닝 규칙)에 프로비저닝하기 위해 리디렉션됩니다. Secure_access SSID에 연결하면 Posture 모듈에서 ISE에 의해 보고서를 받지 못한 경우 프로비저닝에 대해 리디렉션됩니다(Unknown이라는 규칙). 엔드포인트가 완전히 준수되면 전체 액세스 권한이 부여됩니다(규칙 이름 Compliant). 엔드포인트가 규정을 준수하지 않는 것으로 보고되면 네트워크 액세스가 제한됩니다(NonCompliant라는 규칙).

다음을 확인합니다.

프로비저닝 SSID와 연결하고 웹 페이지에 액세스하려고 하면 클라이언트 프로비저닝 포털로 리디렉션됩니다.

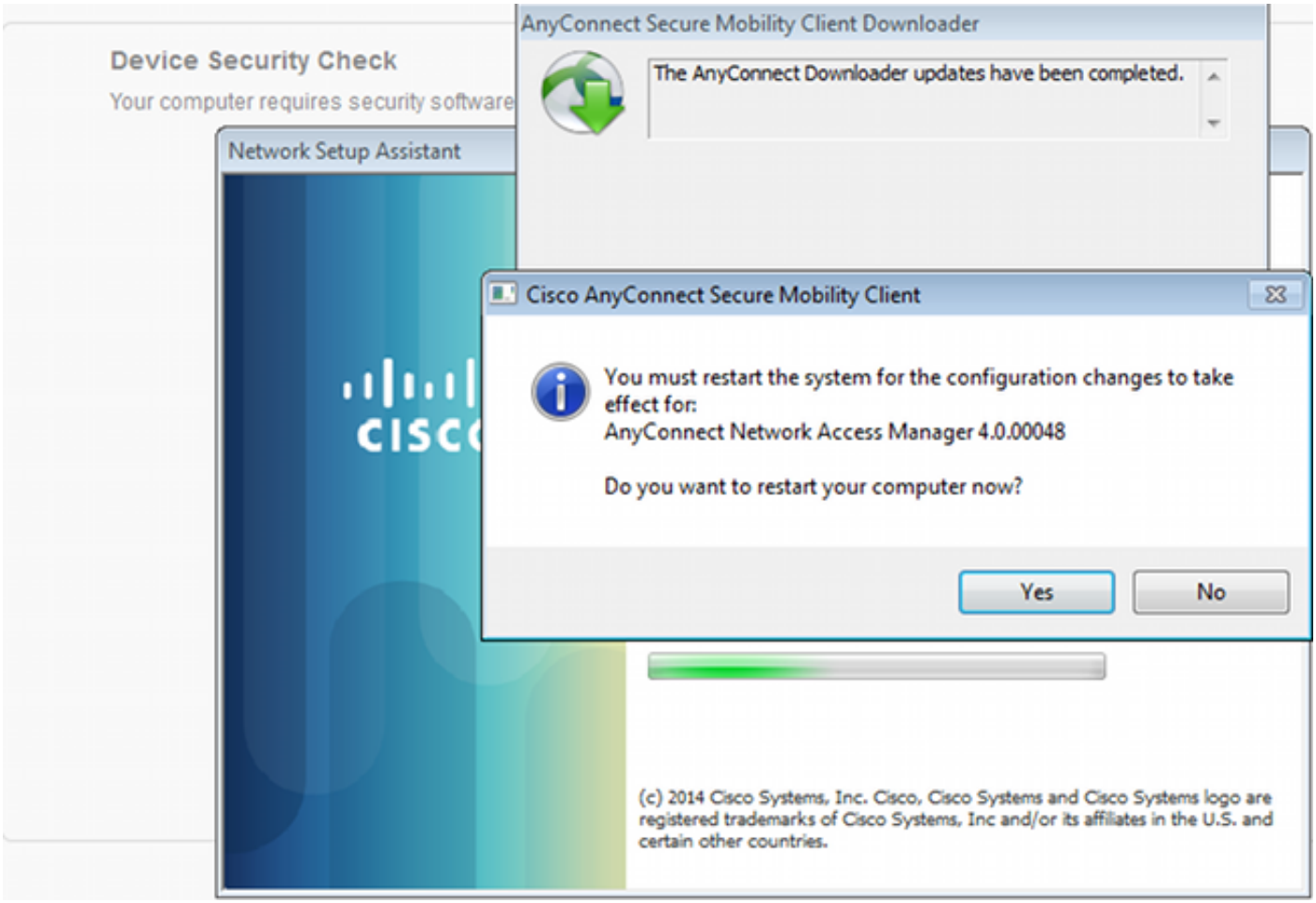


AnyConnect가 검색되지 않으므로 다음 명령을 사용하여 설치하라는 메시지가 표시됩니다.

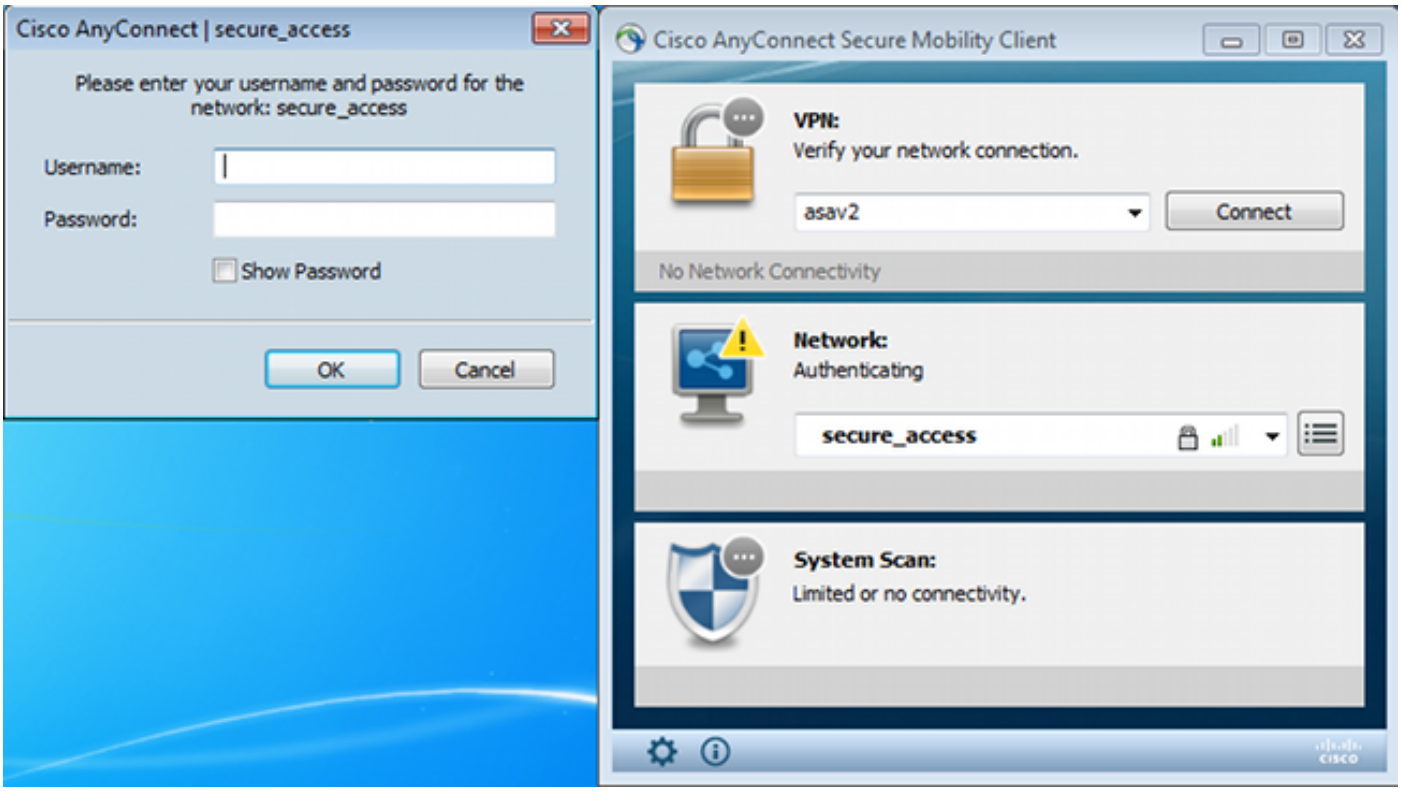


전체 설치 프로세스를 담당하는 Network Setup Assistant라는 작은 애플리케이션이 다운로드됩니다.버전 1.2의 Network Setup Assistant와 다릅니다.

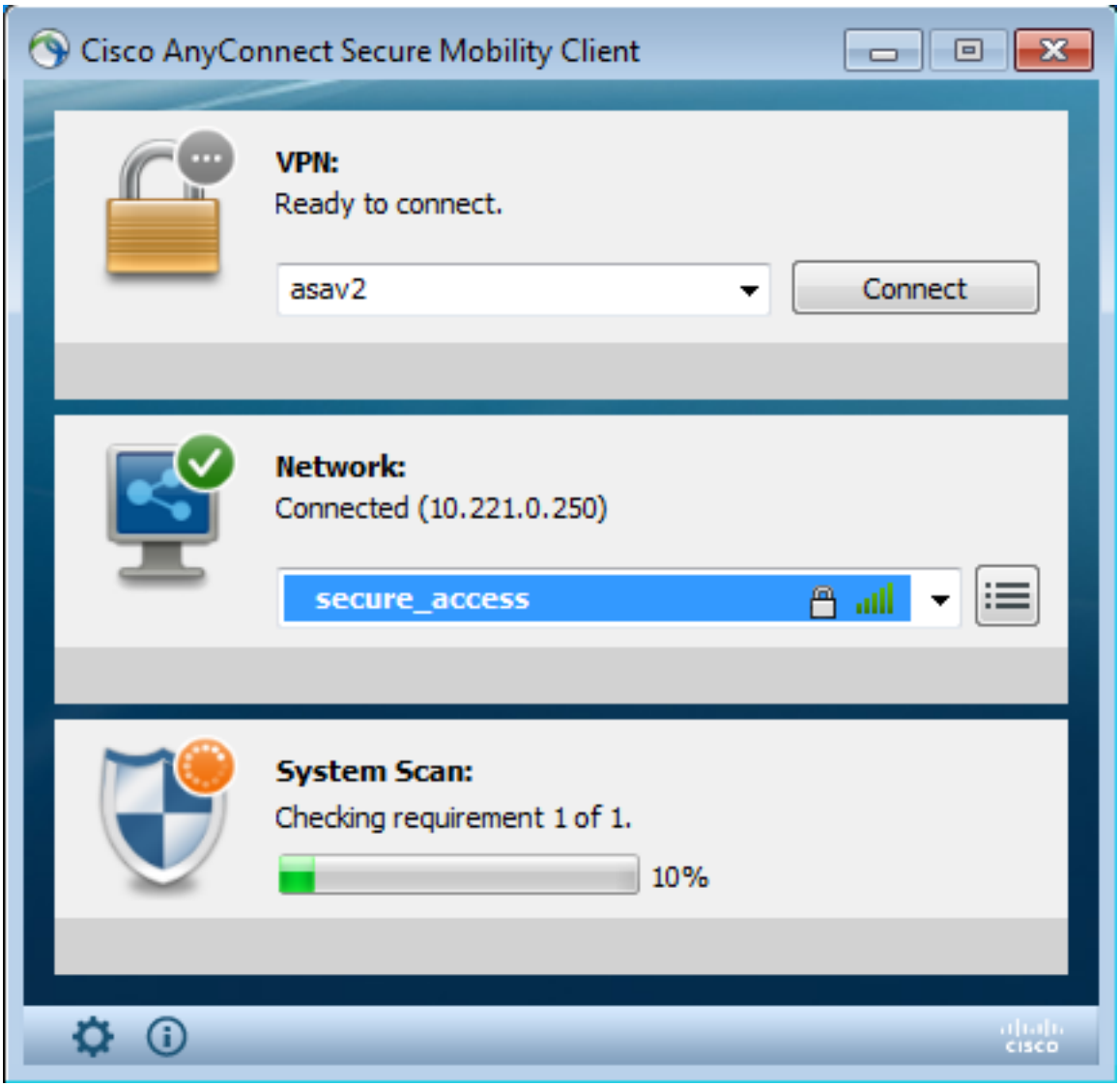
모든 모듈(VPN, NAM 및 Posture)이 설치 및 구성됩니다.PC를 재부팅해야 합니다.



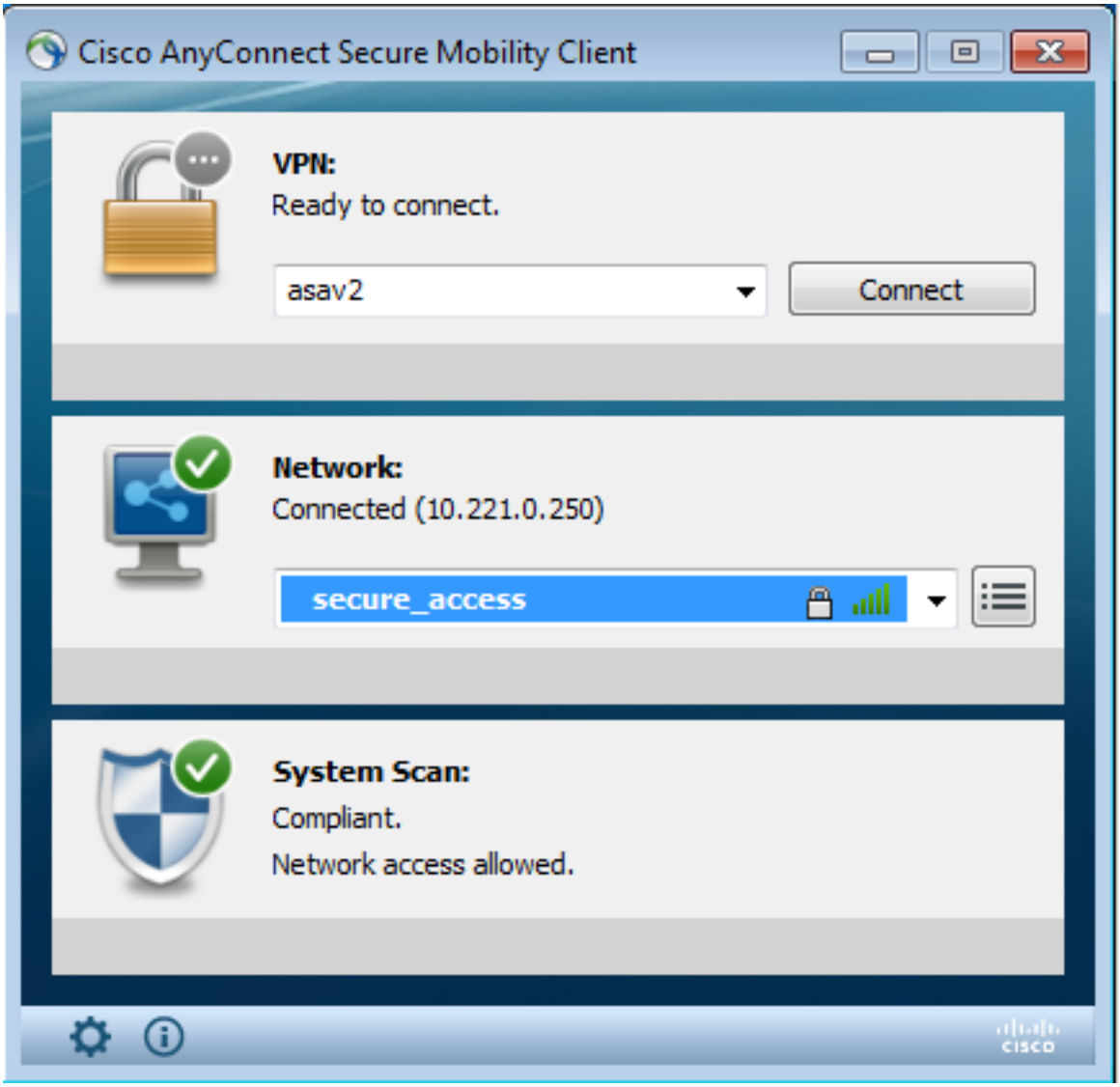
재부팅 후 AnyConnect가 자동으로 실행되며 NAM은 구성된 프로파일에 따라 secure_access SSID와 연결을 시도합니다. VPN 프로파일이 올바르게 설치되어 있는지 확인합니다(VPN의 경우 asav2 항목).



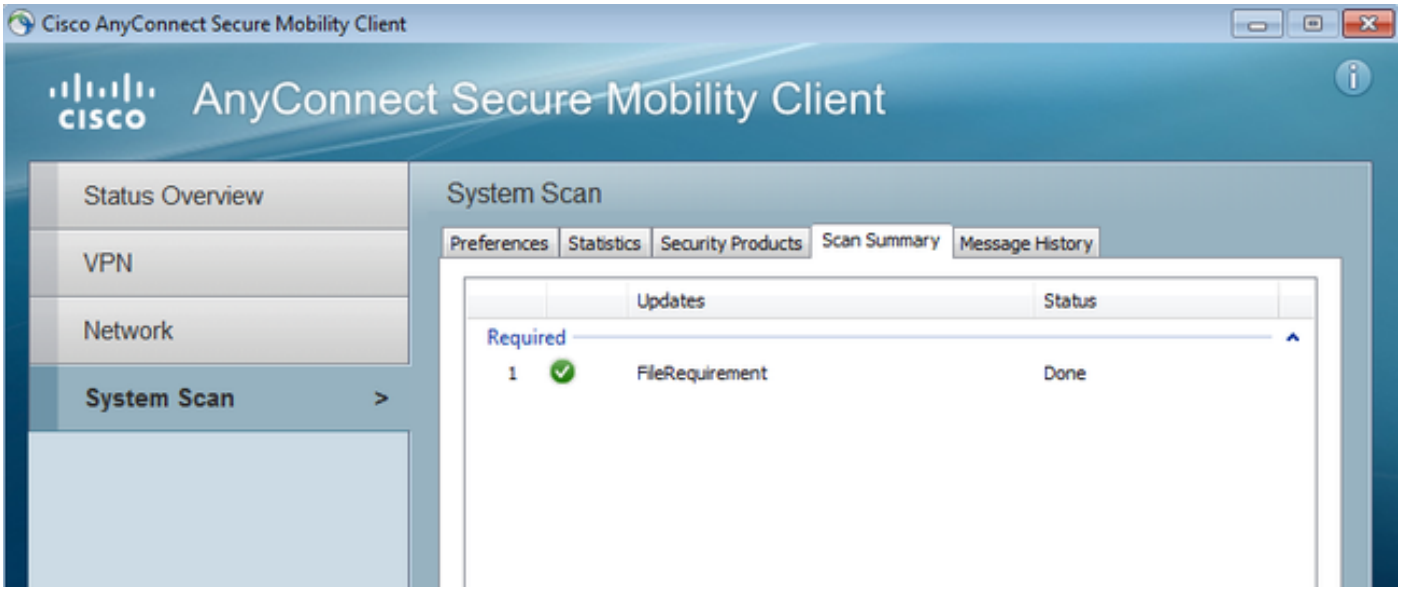
인증 후 AnyConnect는 업데이트 및 확인이 수행되는 상태 규칙을 다운로드합니다.



이 단계에서는 액세스가 제한될 수 있습니다(ISE에서 알 수 없는 권한 부여 규칙이 발생함). 스테이션이 호환 되면 포스처 모듈에서 보고 됩니다.



세부 정보도 확인할 수 있습니다(FileRequirement가 충족됨).

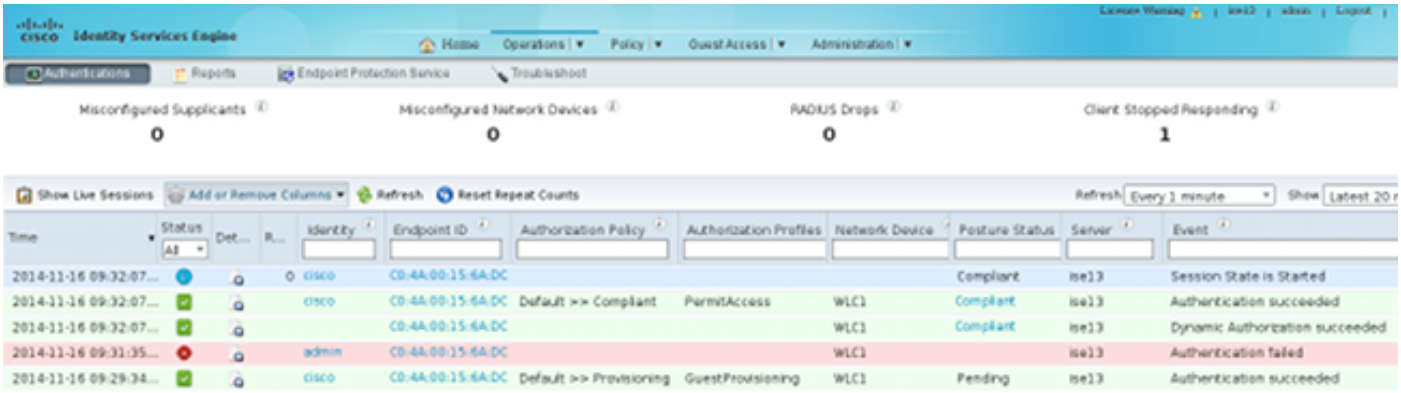


Message History(메시지 기록)에는 다음과 같은 자세한 단계가 표시됩니다.

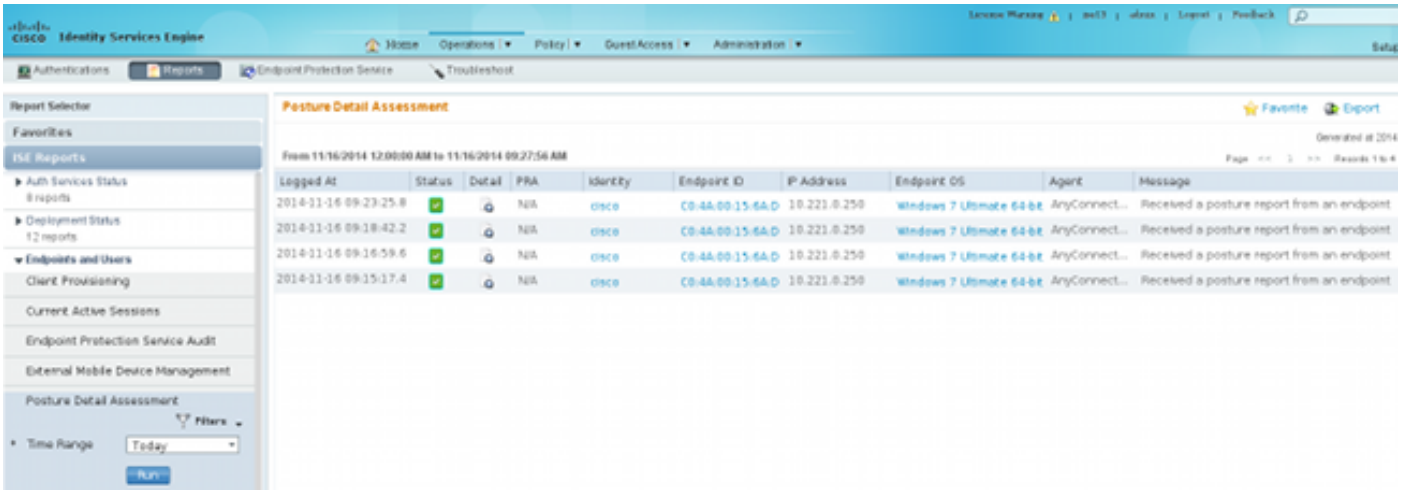
```
9:18:38 AM The AnyConnect Downloader is performing update checks...
9:18:38 AM Checking for profile updates...
9:18:38 AM Checking for product updates...
```

```
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.
```

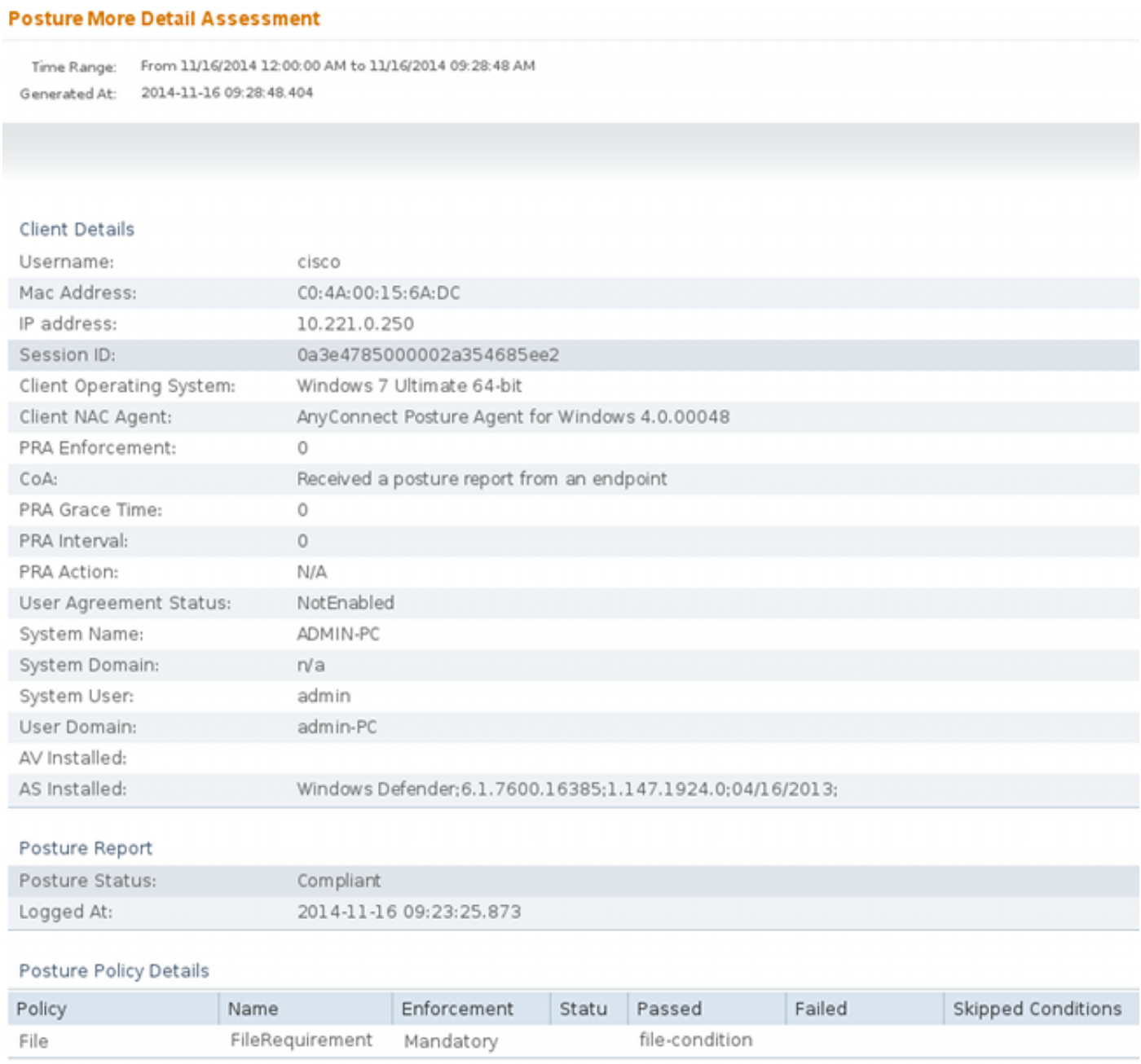
성공 한 보고서가 ISE로 전송 되어 권한 변경 이 시작 됩니다.두 번째 인증은 Compliant(호환) 규칙을 발견하면 전체 네트워크 액세스가 부여됩니다.프로비저닝 SSID에 계속 연결되어 있는 동안 상태 보고서가 전송되면 다음 로그가 ISE에서 표시됩니다.



상태 보고서는 다음을 나타냅니다.



자세한 보고서는 다음 조건을 충족하는 FileRequirement를 보여 줍니다.



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		

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco ISE 컨피그레이션 가이드의 포스처 서비스
- Cisco ISE 1.3 관리자 가이드
- 기술 지원 및 문서 – Cisco Systems