Cisco Secure Client ISE Posture 모듈 및 Cisco Secure Firewall Management Center를 사용하여 엔드포인트 컴플라이언스 평가

초판: 2023년 7월 27일

Cisco Secure Client ISE Posture 모듈 및 Cisco Secure Firewall Management Center를 사용하여 엔드포인트 컴플라이언스 평가

소개

Cisco Secure Client의 ISE(Identity Services Engine) Posture 모듈을 사용하면 엔드포인트의 네트워크 연결을 허용하기 전에 엔드포인트의 컴플라이언스를 평가할 수 있습니다. 평가는 안티바이러스, 안티스파이웨어, 파일, 레지스트리 키 등의 특정 버전에 대한 것일 수 있습니다. 포스처 평가 중에 네트워크에 연결하는 모든 클라이언트는 준수해야 하는 필수 요구 사항을 충족해야 합니다.

ISE Posture 모듈은 클라이언트 측 평가를 실시합니다. 클라이언트는 ISE에서 포스처 요건 정책을 수신하고 포스처 데이터 수집을 수행하며 결과를 정책과 비교하여 평가 결과를 ISE로 반송합니다.

포스처 서비스는 포스처 상태를 다음과 같이 분류합니다.

포스처 컴플라이언스 상태	설명
규정 준수	엔드포인트에 대해 일치하는 포스처 정책이 정의된 경우 엔드포인트의 포스처 규정 준수 상태를 컴플라이언스로 설정할 수 있습니다. 포스처 평가가 수행되면 엔드포인트는 일치 포스처 정책에 정의된 모든 필수 요구 사항을 충족하고 네트워크에서 권한 있는 네트워크 액세스 권한이 부여됩니다.
규정 미준수	엔드포인트에 대해 일치하는 포스처 정책이 정의되었으나 포스처 평가 중에 모든 필수 요건을 충족하지 못할 경우 엔드포인트의 포스처 컴플라이언스 상태는 규정 미준수가 됩니다. 규정 미준수 엔드포인트는 포스처 요구 사항을 교정 작업과 일치시키며, 자체 교정하려면 교정 리소스에 대한 제한된 네트워크 액세스 권한이 부여되어야 합니다.

포스처 컴플라이언스 상태	설명
알 수 없음	엔드포인트에 대해 일치하는 포스처 정책이 정의되지 않은 경우 엔드포인트의 포스처 컴플라이언스 상태를 알 수 없음으로 설정할 수 있습니다. 일치하는 포스처 정책이 활성화되었으나 해당 엔드포인트에 대한 포스처 평가가 아직 진행되지 않았으며 클라이언트 에이전트에서 컴플라이언스 보고서가 제공되지 않은 경우, 엔드포인트의 상태가 Unknown(알 수 없음)이 될 수 있습니다.

장점

Threat Defense를 사용하여 ISE Posture 모듈을 구성하면 다음과 같은 상당한 이점이 제공됩니다.

- 각 엔드포인트에서 ISE Posture 모듈과 프로파일을 쉽게 배포하고 관리할 수 있습니다.
- 엔드포인트를 기업 네트워크에 연결하기 전에 엔드포인트의 컴플라이언스를 쉽게 평가할 수 있습니다.

가이드의 적합성 확인

이 활용 사례는 주로 엔드포인트 컴플라이언스 평가를 위해 Management Center를 사용하여 ISE Posture 모듈을 구성하려는 네트워크 관리자를 대상으로 합니다.

시스템 요구 사항

다음 테이블에는 이 기능이 지원되는 플랫폼이 나와 있습니다.

제품	버전	이 문서에 사용된 버전
Cisco Secure Firewall Threat Defense(구 Firepower Threat Defense/FTD)	6.3 이상	7.3
Cisco Secure Firewall Management Center(구 Firepower Management Center/FMC)	6.7 이상	7.3
Cisco Secure Client(구 AnyConnect)	4.0 이상	5.0
Cisco ISE	2.0 이상	3.1

사전 요건

다음을 확인하십시오.

- 관리자 권한으로 Cisco ISE 서버에 액세스할 수 있어야 합니다.
- Cisco 소프트웨어 다운로드 센터에서 로컬 호스트로 Secure Client 패키지 및 Secure Client 프로파일 편집기를 다운로드해야 합니다.
- 로컬 호스트에 Secure Client 프로파일 편집기를 설치해야 합니다.
- Cisco 소프트웨어 다운로드 센터에서 로컬 호스트로 ISE Compliance 모듈을 다운로드해야 합니다.
- 매니지드 Threat Defense에서 ISE 서버 세부 정보를 구성해야 합니다. Management Center에서 ISE 구성을 참조하십시오.
- Management Center에서 원격 액세스 VPN을 설정해야 합니다.

라이선스

- ISE Premier 라이선스.
- 다음 Secure Client 라이선스 중 하나:

  Secure Client Premier, Secure Client Advantage 또는 Secure Client VPN Only.
- Management Center Essentials(구 Base) 라이선스는 내보내기 제어 기능을 허용해야 합니다.

  System(시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 선택하여 Management Center에서 이 기능을 확인합니다.

Management Center에서 ISE 구성

다음을 수행하려면 Management Center에 ISE 서버를 구성해야 합니다.

- 원격 액세스 VPN에 대한 Threat Defense의 AAA 요청을 허용합니다.
- ISE에서 포스처 요건 정책을 수신합니다.
- 평가 결과를 ISE로 전송합니다.

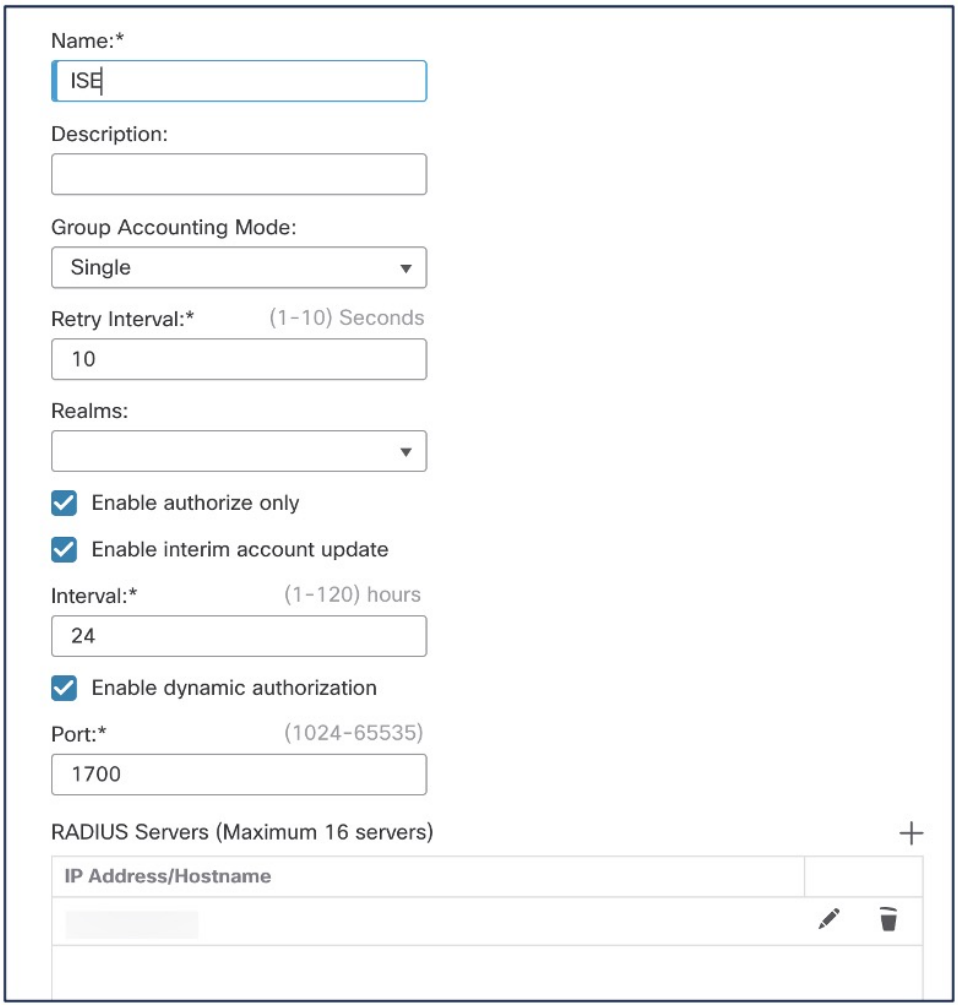
RADIUS 서버 개체를 생성하고 ISE 서버 세부 정보로 구성해야 합니다.

프로시저

단계 **1** **Object(**개체**)** > **Object Management(**개체 관리**)** > **AAA Server(AAA** 서버**)** > **RADIUS Server Group(RADIUS** 서버 그룹**)**을 선택합니다.

단계 **2** **Add RADIUS Server Group(RADIUS** 서버 그룹 추가**)**을 클릭합니다.

단계 **3** 이름과 재시도 간격을 입력합니다.



단계 **4** 포트를 1700으로 구성합니다.

단계 **5** +를 클릭하여 ISE 서버를 추가합니다.

단계 **6** ISE 서버의 IP 주소를 입력하십시오.

단계 **7** **Authentication Port(**인증 포트**)**는 1812로 둡니다.

단계 **8** 키를 구성합니다.

매니지드 디바이스(클라이언트)와 ISE 서버 간에 데이터를 암호화하려면 공유 암호를 입력합니다.

단계 **9** **Confirm Key(**확인 키**)** 필드에 키를 다시 입력합니다.

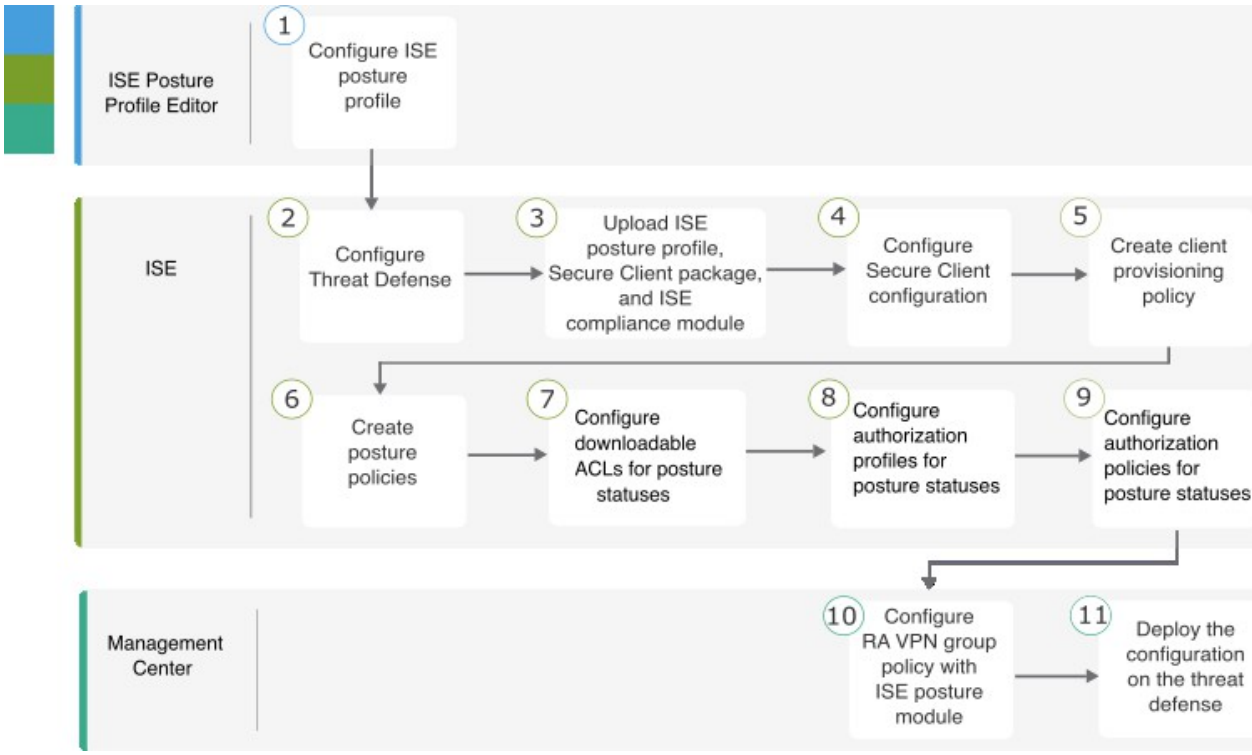
ISE에서 Threat Defense를 추가할 때 이 키가 필요합니다.

단계 **10** 나머지 매개변수에 대해서는 기본값을 사용합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

Management Center를 사용하여 ISE Posture 모듈을 구성하기 위한 엔드 투 엔드 절차

다음 순서도에는 Management Center를 사용하여 Secure Client ISE Posture 모듈을 구성하는 워크플로우가 나와 있습니다.



단계	애플리케이션	설명
1	ISE Posture 프로파일 편집기	ISE Posture 프로파일 편집기를 사용하여 포스처 프로파일 구성, 6 페이지
2	ISE	ISE에서 Threat Defense 구성, 8 페이지
3	ISE	ISE에 ISE Posture 프로파일, Secure Client 패키지 및 ISE Compliance 모듈 업로드, 9 페이지
4	ISE	ISE에서 보안 클라이언트 구성 설정, 11 페이지
5	ISE	ISE에서 클라이언트 프로비저닝 정책 생성, 12 페이지

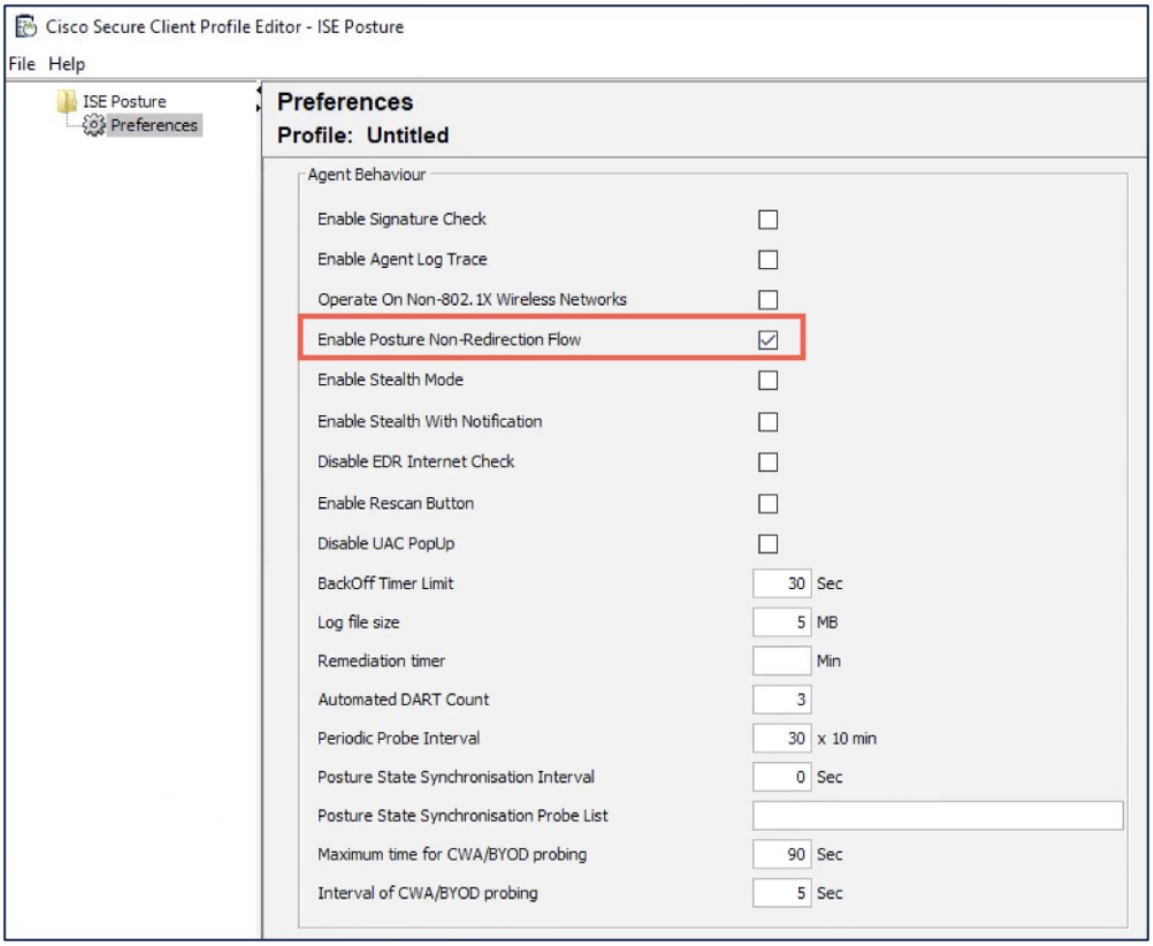
단계	애플리케이션	설명
6	ISE	ISE에서 포스처 정책 구성, 13 페이지
7	ISE	ISE의 포스처 상태에 대해 다운로드 가능한 ACL 구성, 16 페이지
8	ISE	ISE에서 포스처 상태에 대한 권한 부여 프로파일 구성, 17 페이지
9	ISE	ISE에서 포스처 상태에 대한 권한 부여 정책 구성, 18 페이지
10	Management Center	Management Center에서 ISE Posture 모듈을 사용하여 원격 액세스 VPN 그룹 정책 구성, 19 페이지
11	Management Center	Management Center 메뉴 모음에서 **Deploy(**구축**)**를 클릭한 다음 **Deployment(**구축**)**를 선택합니다.

ISE Posture 프로파일 편집기를 사용하여 포스처 프로파일 구성

독립형 Secure Client 프로파일 편집기 패키지에는 ISE Posture 프로파일 편집기가 포함되어 있습니다. 이 편집기를 사용하여 ISE Posture 프로파일을 생성한 다음 ISE 및 Management Center에 업로드합니다.

프로시저

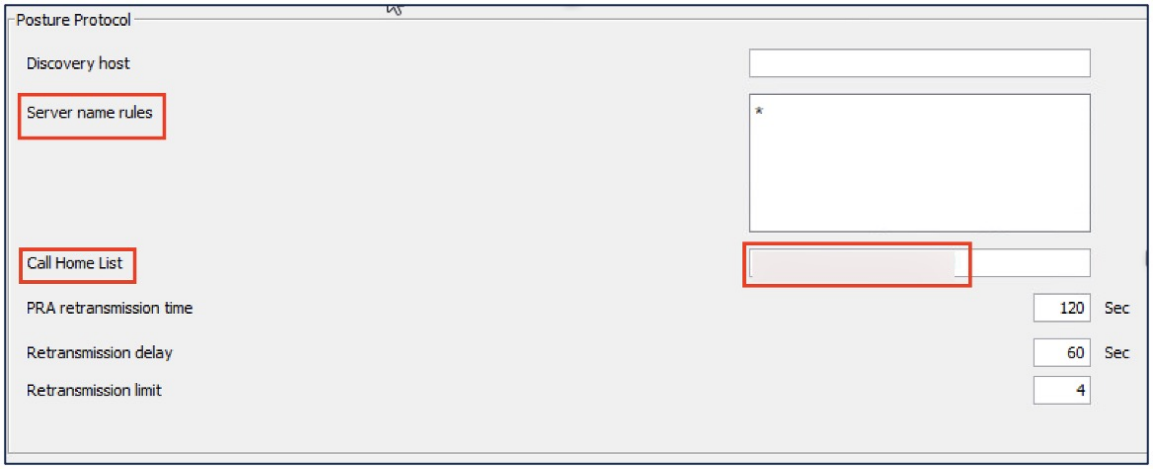
단계 **1** **Enable posture non-redirection flow(**포스처 비 리디렉션 플로우 활성화**)** 체크 박스를 선택합니다.



단계 **2** **Server name rules(**서버 이름 규칙**)**에 *를 입력합니다.

이러한 규칙에는 에이전트가 연결할 수 있는 서버를 정의하는 와일드카드의 쉼표로 구분된 이름 목록이 포함될 수 있습니다. example1.cisco.com 또는 *.cisco.com을 예로 들 수 있습니다.

단계 **3** FQDN 또는 ISE의 IP 주소로 **Call Homes List(Call Home** 목록**)**를 구성합니다.



다음에 수행할 작업

ISE에서 Threat Defense 구성, 8 페이지

ISE에서 Threat Defense 구성

프로시저

단계 **1** ISE에 로그인합니다.

단계 **2** **Administration(관리)** > **Network Resources(네트워크 리소스)** > **Network Devices(네트워크 디바이스)**를 선택합니다.

단계 **3** **Add(추가)**를 클릭합니다.

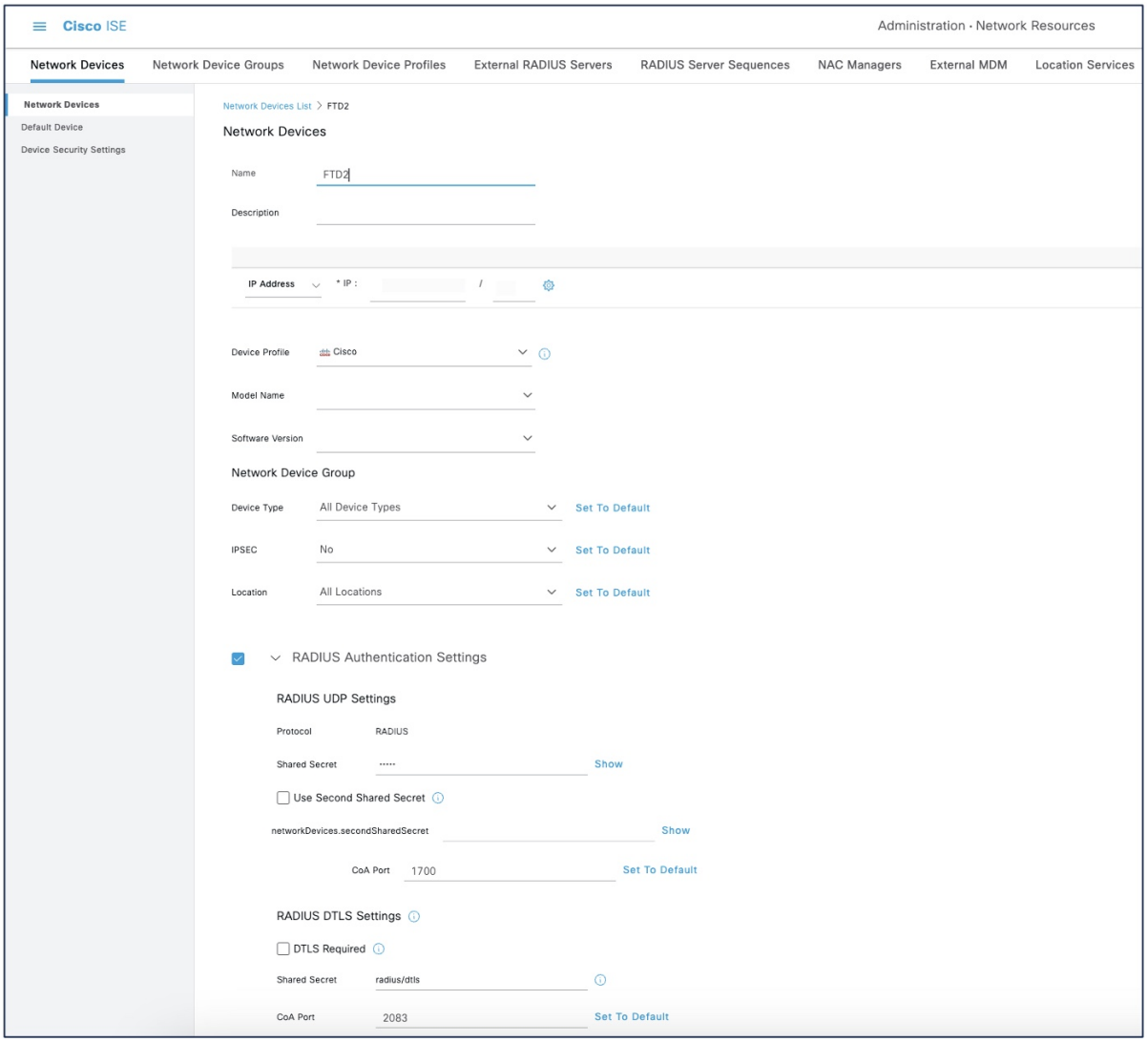
단계 **4** Threat Defense의 이름, 설명 및 IP 주소를 입력합니다.

단계 **5** **Device Profile(디바이스 프로파일)** 드롭다운 목록에서 **Cisco**를 선택합니다.

단계 **6** **RADIUS Authentication Settings(RADIUS 인증 설정)**를 확장합니다.

단계 **7** **Shared Secret(공유 암호)** 및 **CoA Port(CoA 포트)**를 구성합니다.

Threat Defense에서 ISE를 구성하는 데 사용한 포트와 암호를 사용합니다. 자세한 정보는 Management Center에서 ISE 구성을 참조하십시오.



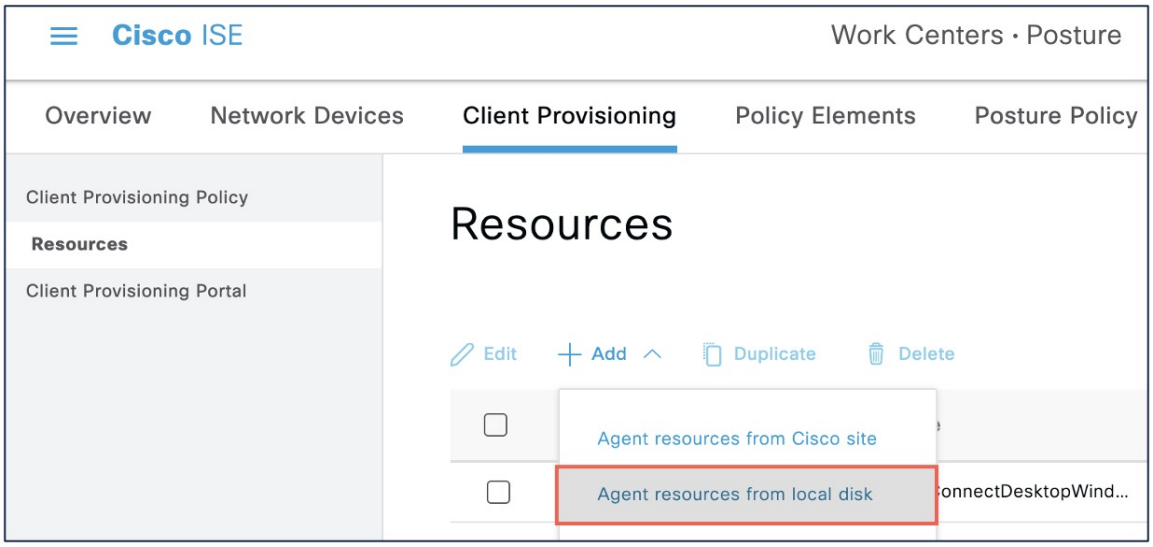
단계 **8** **Save(**저장**)**를 클릭합니다.

ISE에 ISE Posture 프로파일, Secure Client 패키지 및 ISE Compliance 모듈 업로드

프로시저

단계 **1** **Work Centers(**작업 센터**)** > **Posture(**포스처**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하고 **Agent resources from local disk(**로컬 디스크의 에이전트 리소스**)**를 선택합니다.



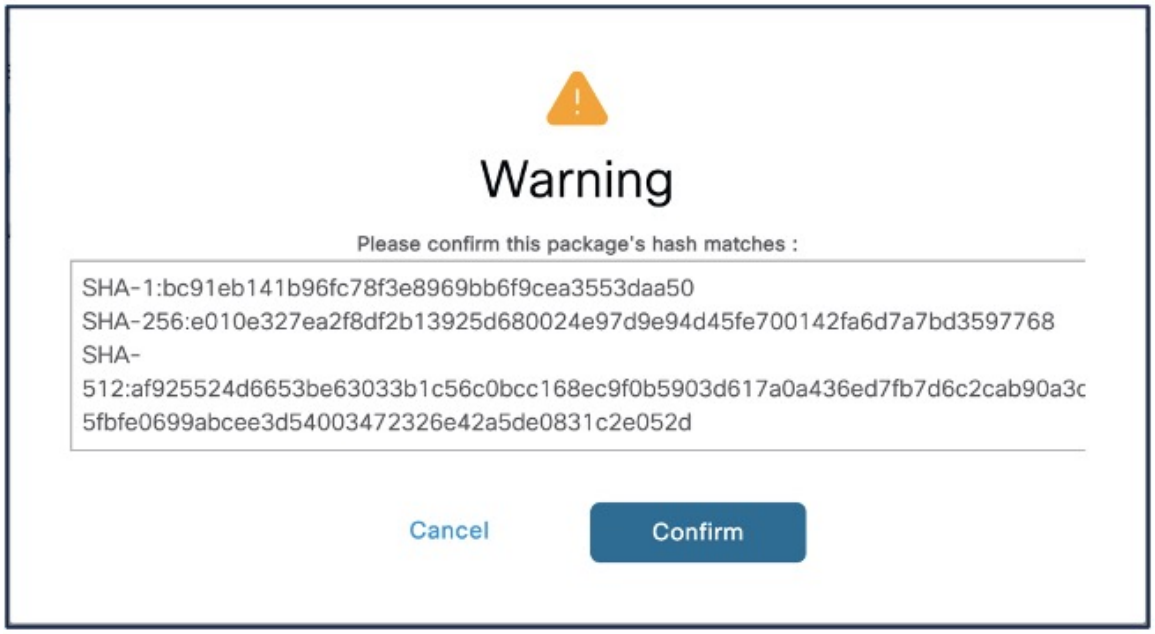
단계 **3** **Category(**범주**)** 드롭다운 목록에서 **Cisco Provided Packages(Cisco** 제공 패키지**)**를 선택합니다.

단계 **4** **Choose File(**파일 선택**)**을 클릭하고 로컬 호스트에서 다음 중 하나를 선택합니다.

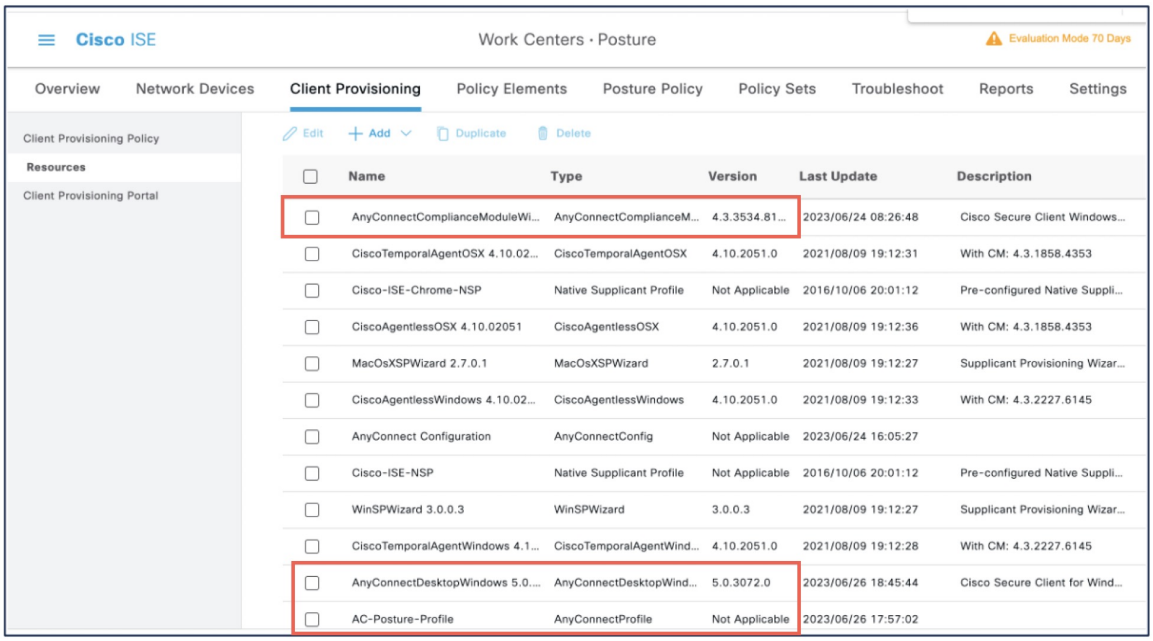
1. ISE Posture 프로파일(ISEPostureCFG.xml)
2. Secure Client 패키지
3. ISE Compliance 모듈

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** 체크섬을 확인하려면 **Confirm(**확인**)**을 클릭합니다.



단계 **7** 나머지 2개 파일을 업로드하려면 2~6단계를 반복합니다.



ISE에서 보안 클라이언트 구성 설정

Secure Client 구성(ISE의 AnyConnect 구성)은 Secure Client 소프트웨어 및 해당 구성 파일(예: 클라이언트용 Secure Client 바이너리 패키지, ISE Compliance 모듈, ISE 모듈 프로파일, 맞춤화 및 AnyConnect용 언어 패키지)입니다.

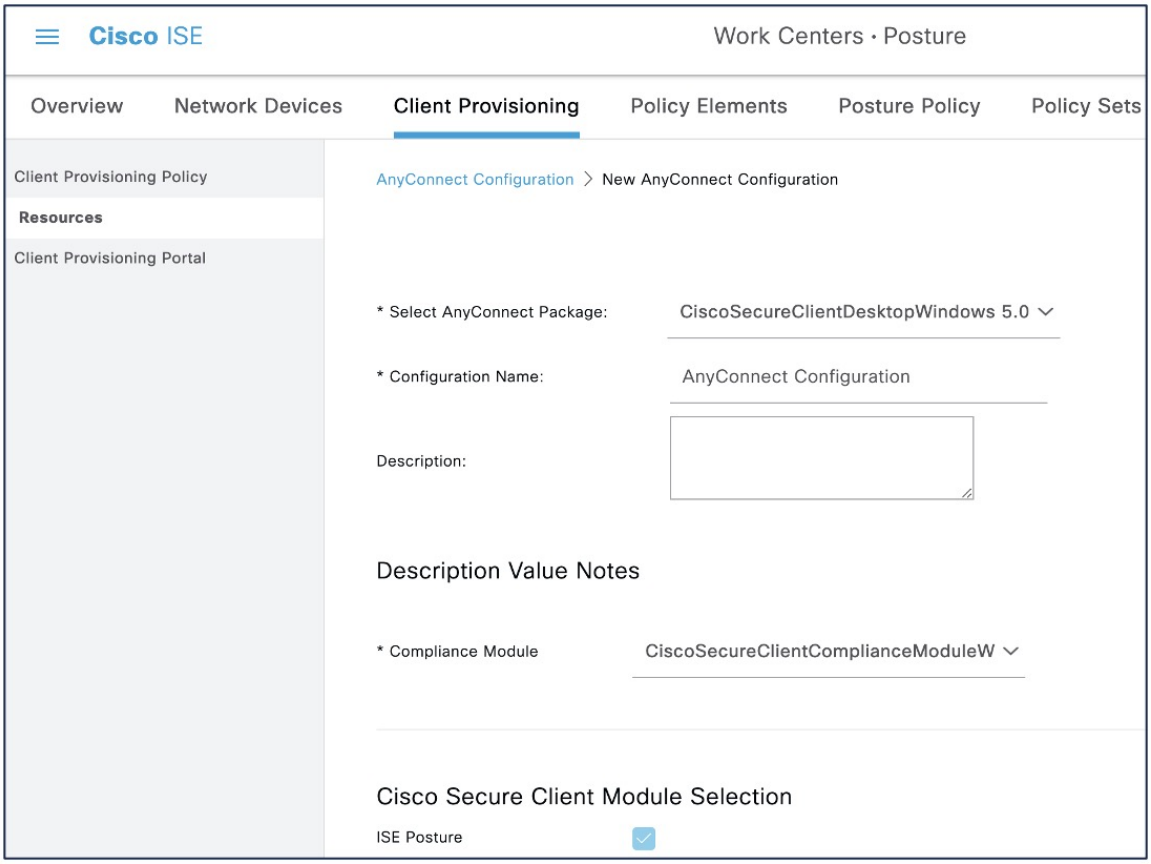
프로시저

단계 **1** **Work Centers**(작업 센터) > **Posture**(포스처) > **Client Provisioning**(클라이언트 프로비저닝) > **Resources**(리소스)를 선택합니다.

단계 **2** **Add**(추가)를 클릭하고 **AnyConnect Configuration**(**AnyConnect** 구성)을 선택합니다.

단계 **3** **Select AnyConnect Package**(**AnyConnect** 패키지 선택) 드롭다운 목록에서 Secure Client 패키지를 선택합니다.

단계 **4** **Compliance Module**(컴플라이언스 모듈) 드롭다운 목록에서 ISE Compliance Module(ISE Compliance 모듈)을 선택합니다.



단계 **5** **Cisco Secure Client Module Selection(Cisco Secure Client** 모듈 선택**)**에서는 기본적으로 ISE Posture가 활성화되어 있습니다.

단계 **6** **Profile Selection(**프로파일 선택**)**의 **ISE Posture** 드롭다운 목록에서 ISE Posture 파일을 선택합니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

ISE에서 클라이언트 프로비저닝 정책 생성

사용자는 클라이언트 프로비저닝 정책에 따라 ISE에서 에이전트, 에이전트 컴플라이언스 모듈 또는 에이전트 맞춤형 프로파일과 같은 특정 버전의 리소스를 수신합니다.

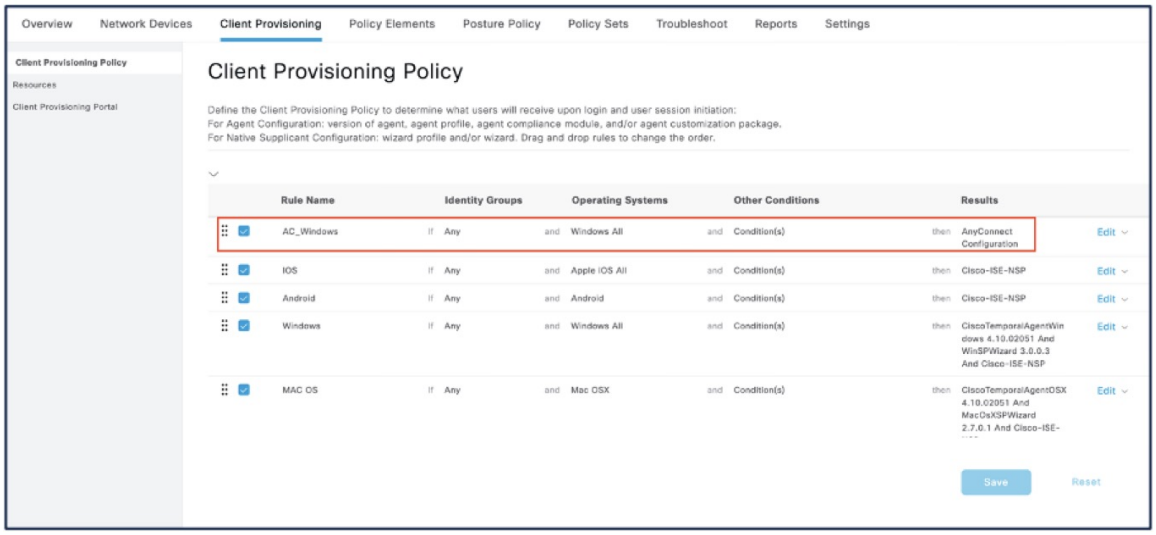
프로시저

단계 **1** **Policy(**정책**)** > **Client Provisioning(**클라이언트 프로비저닝**)**을 선택합니다.

단계 **2** **Edit(**편집**)**을 클릭하고 **Insert new policy above(**위에서 새 정책 삽입**)**를 선택합니다.

단계 **3** 정책 이름을 입력하고 운영 체제를 선택합니다.

단계 **4** **Results(**결과**)**에서 +를 클릭하고 **Agent(**에이전트**)** 드롭다운 목록에서 AnyConnect Configuration(AnyConnect 구성)을 선택합니다.



단계 **5** **Save(**저장**)**를 클릭합니다.

ISE에서 포스처 정책 구성

포스처 정책, 포스처 요건 및 포스처 조건은 엔드포인트의 컴플라이언스 상태를 결정합니다.

프로시저

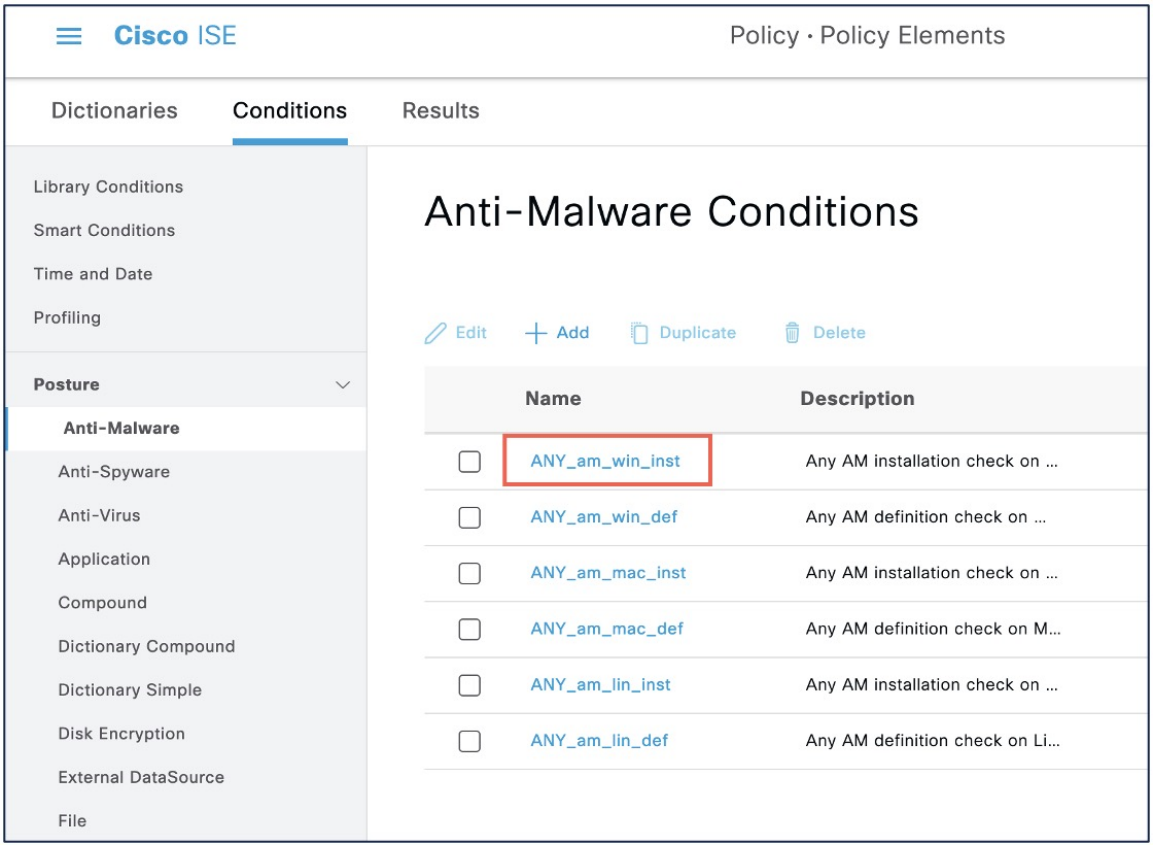
단계 **1** 포스처 조건을 구성합니다.

1. **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)**를 선택합니다.

   하나 이상의 포스처 조건을 선택할 수 있습니다.

2. **Anti-Malware(**안티 맬웨어**)**를 클릭하여 안티 맬웨어 조건을 선택합니다.

   사전 정의된 안티 맬웨어 조건을 선택하거나 새로 생성할 수 있습니다. Windows의 경우에는 'ANY_am_win_inst' 안티 맬웨어 포스처 조건을 선택할 수 있습니다.

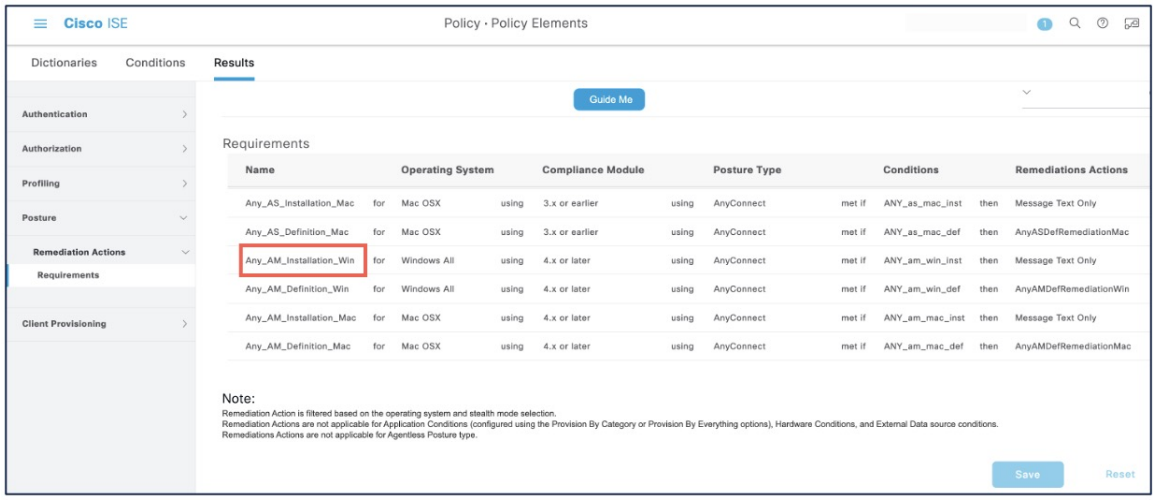


단계 **2** 포스처 요건을 구성합니다.

Policy(정책) > **Policy Elements**(정책 요소) > **Results**(결과) > **Posture**(포스처) > **Requirements**(요건)를 선택합니다.

포스처 요건은 교정 작업과 관련된 포스처 조건 집합입니다. 여러 기본 또는 사전 정의된 포스처 요건 중 하나를 선택하거나 새로 생성할 수 있습니다.

Windows의 경우에는 'Any_AM_Installation_Win' 안티 맬웨어 포스처 요건을 선택할 수 있습니다.

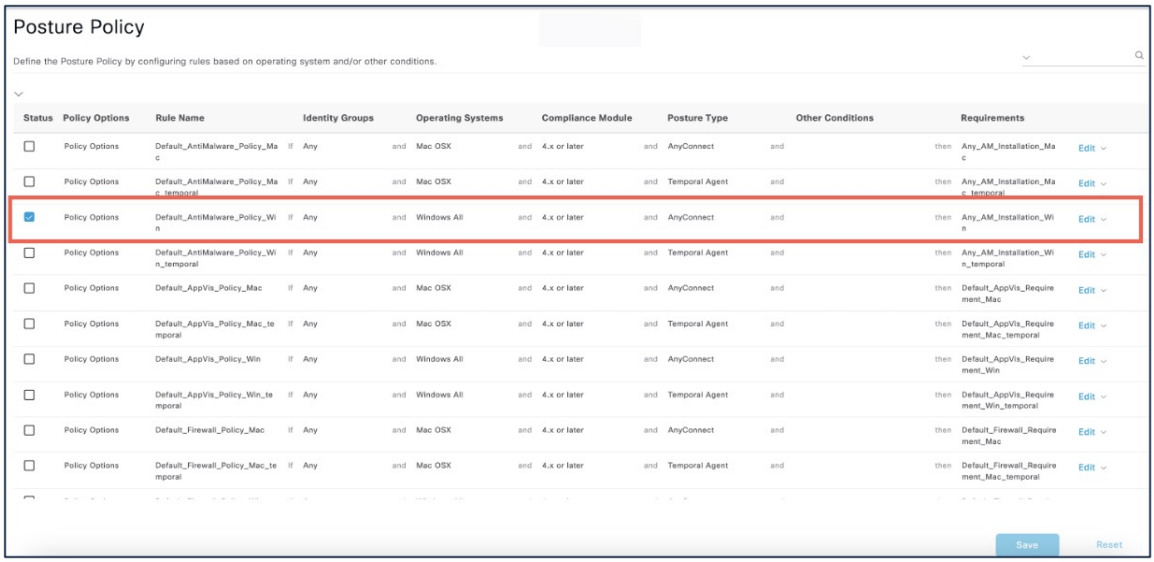


단계 **3** 포스처 정책을 구성합니다.

1. **Policy(**정책**)** > **Posture(**포스처**)**를 선택합니다.

   운영 체제 및 하나 이상의 포스처 요건을 기반으로 규칙을 구성하여 포스처 정책을 정의해야 합니다.

   Windows의 경우 'Default_AntiMalware_Policy_Win' 안티 맬웨어 포스처 정책을 선택할 수 있습니다.



2. 포스처 정책을 활성화하려면 **Status(**상태**)** 체크 박스를 선택합니다.
3. **Save(**저장**)**를 클릭합니다.

ISE의 포스처 상태에 대해 다운로드 가능한 ACL 구성

Unknown(알 수 없음), Noncompliant(규정 미준수) 및 Compliant(규정 준수) 포스처 상태에 대한 DACL(다운로드 가능 ACL)을 구성해야 합니다. 기본 권한 부여 DACL도 사용할 수 있습니다.

프로시저

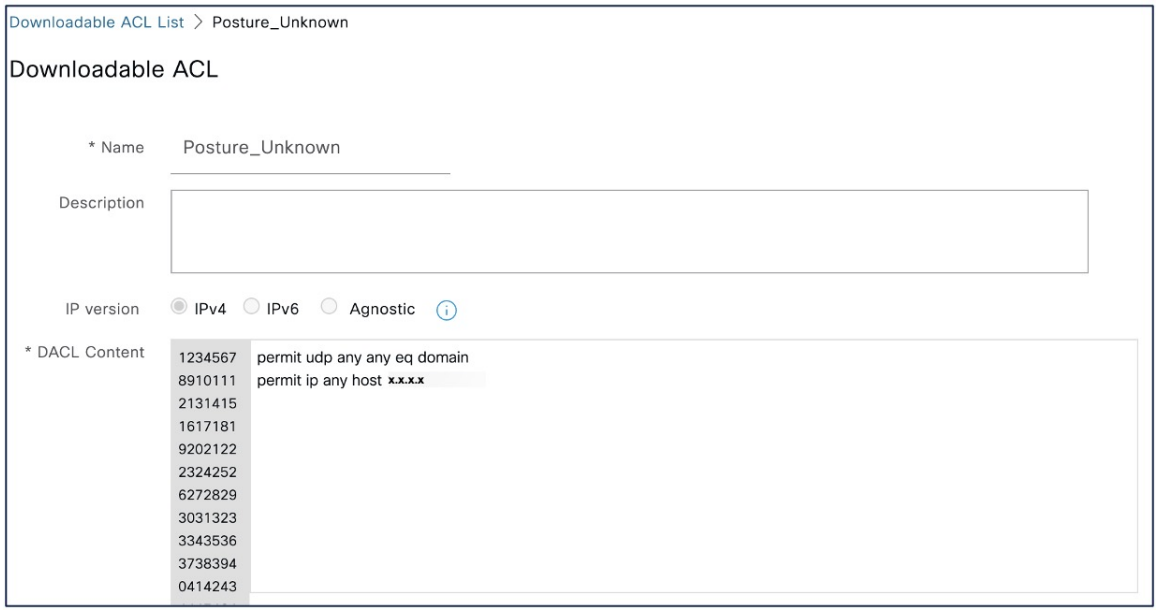
단계 **1** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Downloadable ACLs(**다운로드 가능한 **ACL)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 이름과 설명을 입력합니다.

단계 **4** 필요한 IP 버전의 라디오 버튼을 클릭합니다.

단계 **5** DACL 값을 입력합니다.



단계 **6** **Submit(**제출**)**을 클릭합니다.

단계 **7** 나머지 포스처 상태에 대한 DACL을 생성하려면 2~6단계를 반복합니다.

DACL에서 Unknown(알 수 없음), Noncompliant(규정 미준수) 및 Compliant(규정 준수) 포스처 상태의 예는 다음과 같습니다.

DACL 유형	설명	**DACL**
알 수 없는 DACL 포스처	DNS 및 Policy Service(PSN)에 대한 트래픽을 허용합니다.	permit udp any any eq domain ip any host x.x.x.x 허용

DACL 유형	설명	DACL
규정 미준수 DACL 포스처	프라이빗 서브넷에 대한 액세스를 거부하고 인터넷 트래픽만 허용합니다.	ip any x.x.x.x 255.255.255.0 거부 permit ip any any
규정 준수 DACL 포스처	모든 트래픽을 허용합니다.	permit ip any any

다음에 수행할 작업

이러한 DACL을 사용하여 권한 부여 프로파일을 구성합니다. 자세한 내용은 ISE에서 포스처 상태에 대한 권한 부여 프로파일 구성을 참조하십시오.

ISE에서 포스처 상태에 대한 권한 부여 프로파일 구성

Unknown(알 수 없음), Noncompliant(규정 미준수) 및 Compliant(규정 준수) 포스처 상태에 대한 세 가지 권한 부여 프로파일을 생성해야 합니다.

프로시저

단계 **1** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다.

단계 **2** 각 포스처 상태에 대한 권한 부여 프로파일을 생성합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** 이름을 입력합니다.

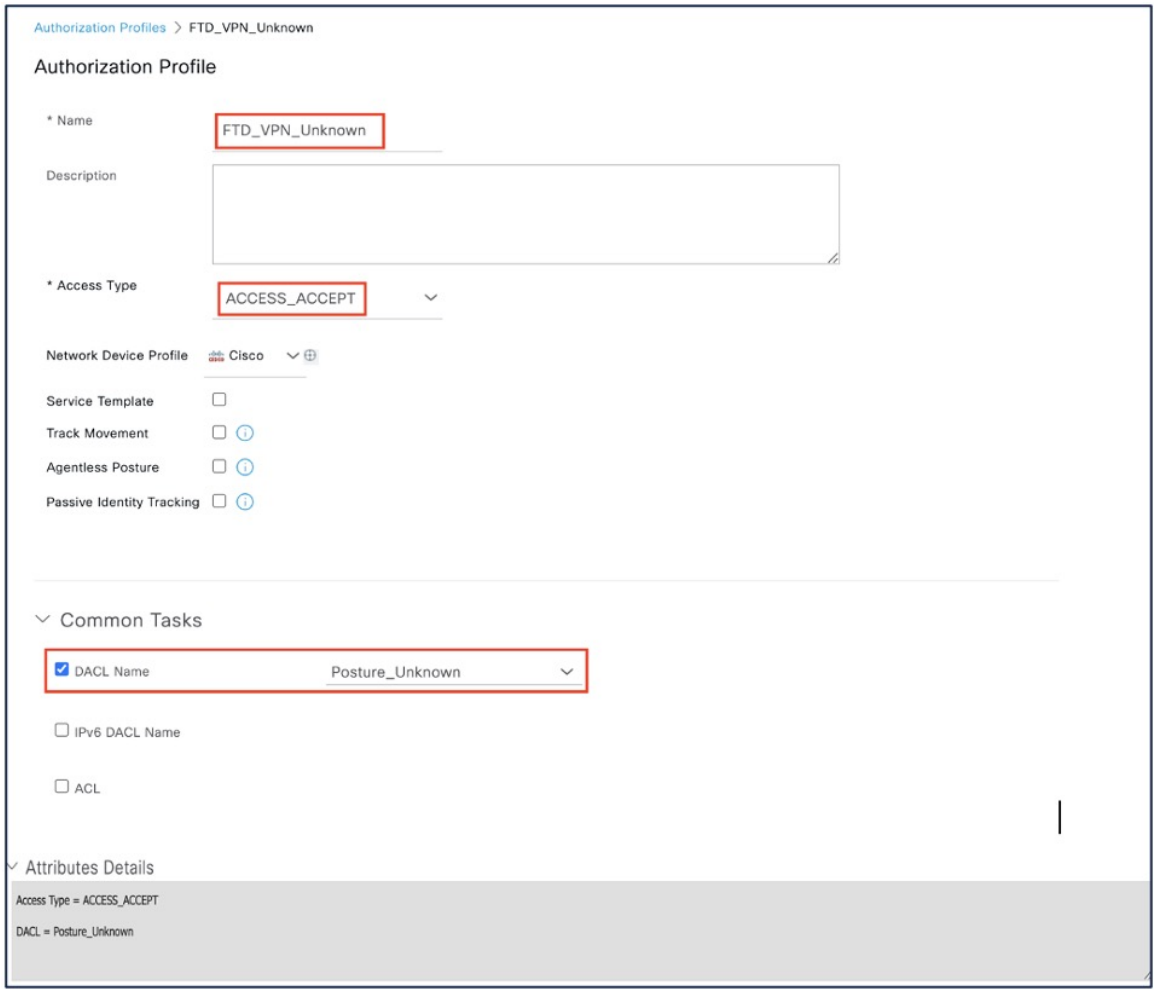
단계 **5** **Access Type(**액세스 유형**)** 드롭다운 목록에서 **ACCESS_ACCEPT**를 선택합니다.

단계 **6** **Network Device Profile(**네트워크 디바이스 프로파일**)** 드롭다운 목록에서 **Cisco**를 선택합니다.

단계 **7** **Common Tasks(**일반 작업**)**에서 **DACL Name(DACL** 이름**)** 체크 박스를 선택하고 드롭다운 목록에서 포스처 상태에 대한 DACL을 선택합니다.

Attributes Details(속성 세부 정보**)**에서 구성된 속성을 볼 수 있습니다.

아래 예에는 Unknown(알 수 없음) 상태에 대한 권한 부여 프로파일이 나와 있습니다.



단계 **8** **Submit(**제출**)**을 클릭합니다.

단계 **9** 나머지 포스처 상태에 대한 권한 부여 프로파일을 생성하려면 3~8단계를 반복합니다.

다음에 수행할 작업

이러한 권한 부여 프로파일을 사용하여 권한 부여 정책을 구성합니다. 자세한 내용은 ISE에서 포스처 상태에 대한 권한 부여 정책 구성을 참조하십시오.

ISE에서 포스처 상태에 대한 권한 부여 정책 구성

각 포스처 상태에 대한 권한 부여 정책을 생성해야 합니다.

프로시저

단계 **1** **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택합니다.

단계 **2** **View(**보기**)** 열에서 Default(기본값) 정책 옆에 있는 화살표 아이콘을 클릭합니다.

단계 **3** **Authorization Policy(**권한 부여 정책**)**를 확장합니다.

단계 **4** **Status(**상태**)** 열 옆의 +를 클릭합니다.

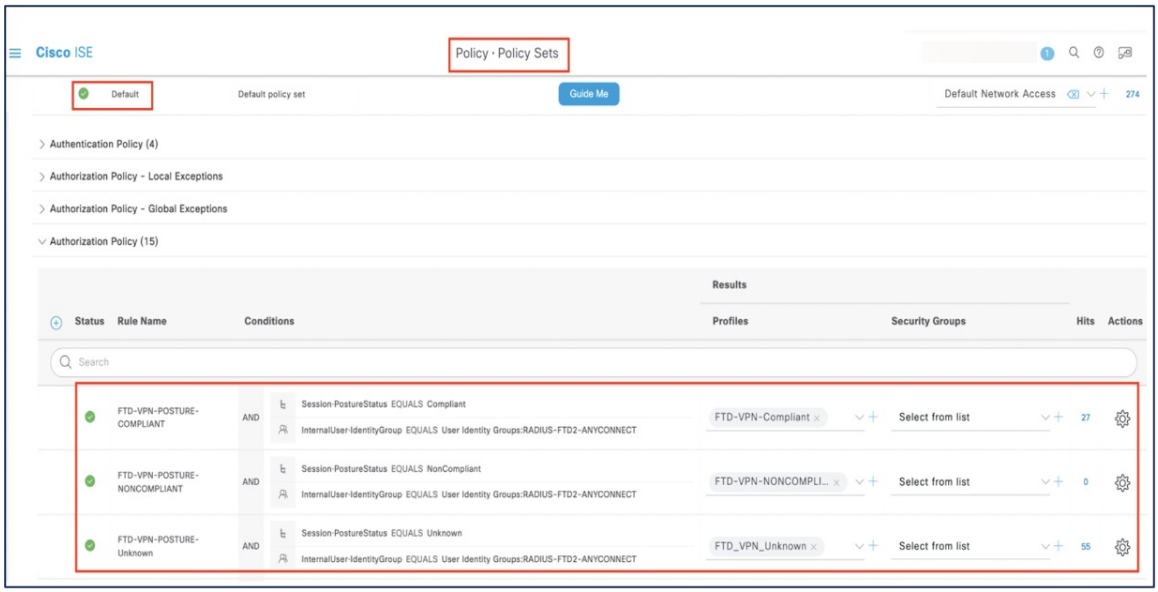
단계 **5** **Posture Status(**포스처 상태**)** 및 **Identity Group(ID** 그룹**)**을 정책의 조건으로 사용합니다.

단계 **6** 포스처 상태의 드롭다운 목록에서 적절한 권한 부여 프로파일을 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** 나머지 권한 부여 정책에 대해 4~7단계를 반복합니다.

아래 이미지에는 포스처에 대한 권한 부여 정책이 나와 있습니다.



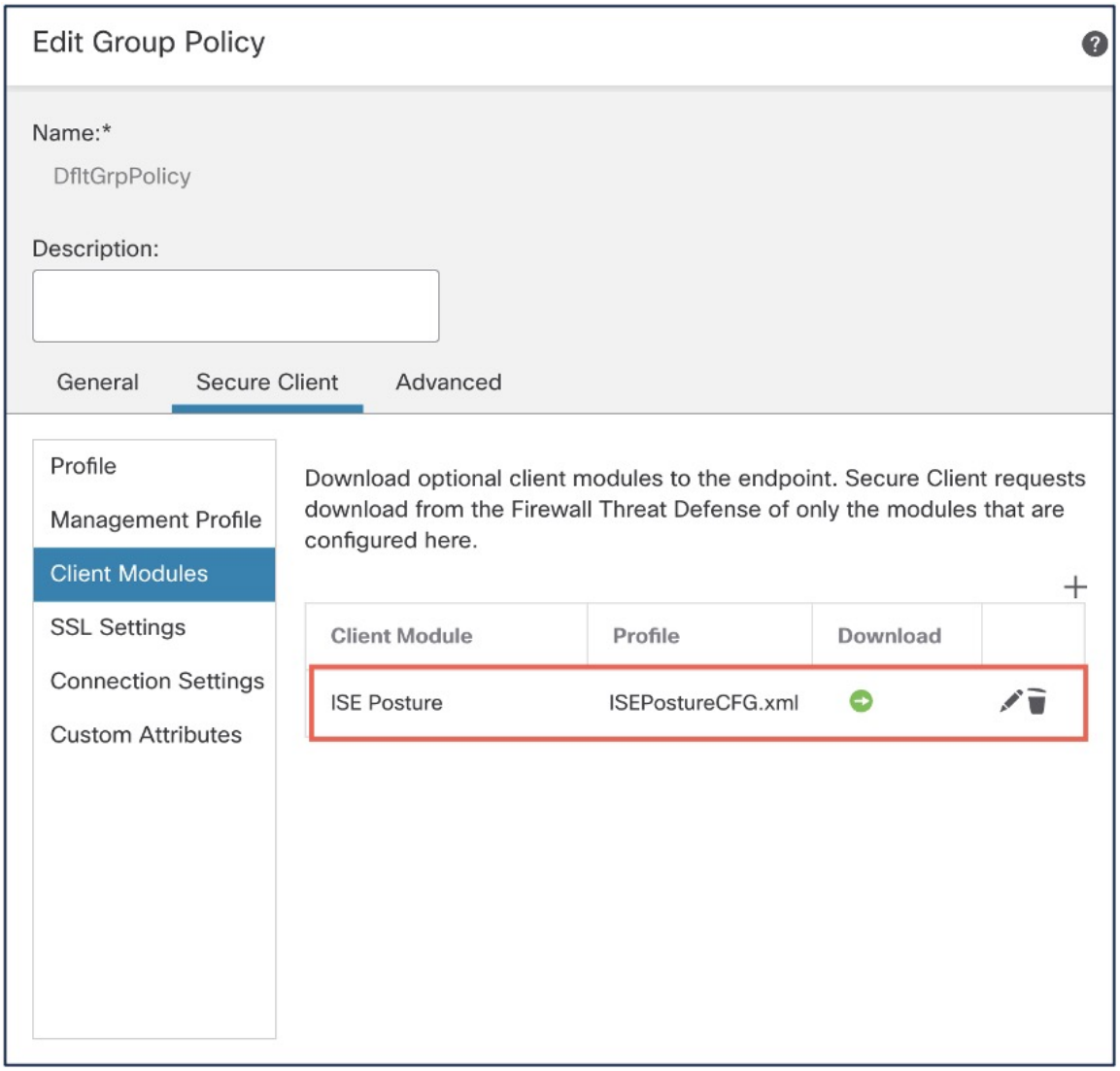
Management Center에서 ISE Posture 모듈을 사용하여 원격 액세스 VPN 그룹 정책 구성

시작하기 전에

Management Center에서 원격 액세스 VPN 정책을 구성합니다.

프로시저

단계 **1** Management Center 웹 인터페이스에 로그인합니다.
단계 **2** **Devices(**디바이스**)** > **Remote Access(**원격 액세스**)**를 선택합니다.
단계 **3** 원격 액세스 VPN 정책을 선택하고 **Edit(**편집**)**을 클릭합니다.
단계 **4** Connection Profile(연결 프로파일)을 선택하고 **Edit(**편집**)**을 클릭합니다.
단계 **5** **Edit Group Policy(**그룹 정책 편집**)**를 클릭합니다.
단계 **6** **Secure Client** 탭을 클릭합니다.
단계 **7** **Client Module(**클라이언트 모듈**)**과 **+**를 차례로 클릭합니다.
단계 **8** **Client Module(**클라이언트 모듈**)** 드롭다운 목록에서 ISE Posture 모듈을 선택합니다.
단계 **9** **Profile to download(**다운로드할 프로파일**)** 드롭다운 목록에서 ISE 프로파일을 선택합니다.
단계 **10** **Enable module download(**모듈 다운로드 활성화**)** 체크 박스를 선택합니다.
단계 **11** **Add(**추가**)**를 클릭합니다.



단계 **12** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

1. 구성을 Threat Defense에 구축합니다. Management Center 메뉴 모음에서 **Deploy(**구축**)**를 클릭한 다음 **Deployment(**구축**)**를 선택합니다.
2. Secure Client를 사용하여 Threat Defense에 대한 VPN 연결을 설정합니다.
3. ISE Posture 모듈 구성을 확인합니다.

ISE Posture 모듈 구성 확인

Threat Defense에서

Threat Defense CLI에서 다음 명령을 사용하여 ISE Posture 모듈 구성을 확인합니다.

show run webvpn: Secure Client 구성의 세부 정보를 확인합니다.

```
> show run webvpn
webvpn
 enable Outside
 http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
  x-content-type-options
  x-xss-protection
  content-security-policy
 anyconnect image disk0:/csm/cisco-secure-client-win-5.0.03072-
webdeploy-k9.pkg 1 regex "Windows"
 anyconnect profiles ISEPostureCFG.xml disk0:/csm/ISEPostureCFG.xml
 anyconnect profiles raftd1.xml disk0:/csm/raftd1.xml
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
```

show run group-policy <*ravpn_group_policy_name*>: Secure Client에 대한 RA VPN 그룹 정책의 세부 정보를 확인합니다.

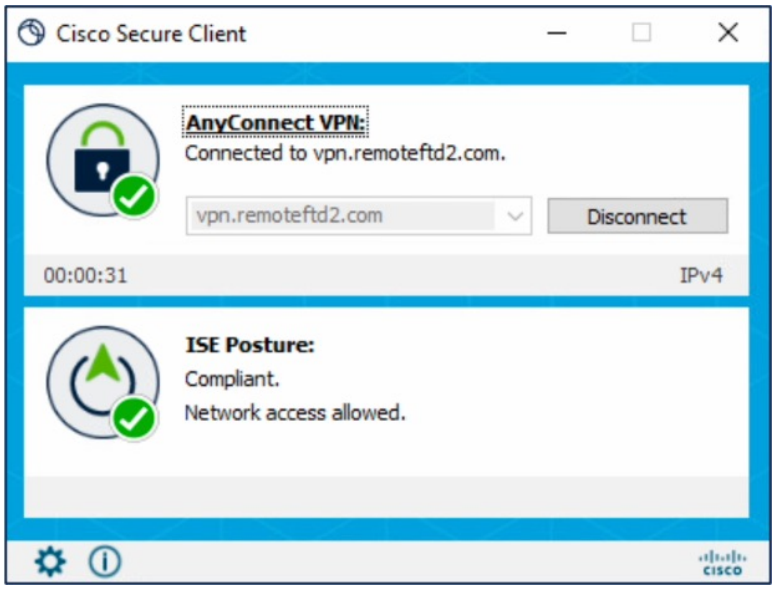
```
> show run group-policy AC-Posture
group-policy AC-Posture internal
group-policy AC-Posture attributes
 banner none
 wins-server none
 dns-server none
 dhcp-network-scope none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelall
 ipv6-split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain none
 split-dns none
 split-tunnel-all-dns disable
 client-bypass-protocol disable
 vlan none
 address-pools none
 webvpn
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface public none
  anyconnect firewall-rule client-interface private none
  anyconnect ssl keepalive 20
  anyconnect ssl rekey time none
  anyconnect ssl rekey method none
  anyconnect dpd-interval client 30
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression none
  anyconnect modules value iseposture
  anyconnect profiles value ISEPostureCFG.xml type iseposture
  anyconnect ask none default anyconnect
  anyconnect ssl df-bit-ignore disable
```

show run aaa-server: ISE 서버의 세부 정보를 확인합니다.

```
> show run aaa-server
aaa-server ISE protocol radius
 authorize-only
 interim-accounting-update periodic 24
 dynamic-authorization
aaa-server ISE (Inside) host 1[redacted]
 key *****
 authentication-port 1812
 accounting-port 1813
```

엔드포인트

Secure Client를 사용하여 Threat Defense에 대한 VPN 연결을 설정하고 ISE Posture 모듈 설치를 확인합니다.



관련 설명서:

- Cisco Identity Services Engine 관리자 설명서
- Secure Firewall Management Center 관리 및 디바이스 구성 가이드
- Cisco Secure Client 관리 가이드