규정 준수

포스처 유형

다음 포스처 에이전트는 Cisco ISE 포스처 정책을 모니터링하고 적용합니다.

- **AnyConnect**: AnyConnect 에이전트를 구축하여 클라이언트와의 상호 작용이 필요한 Cisco ISE Posture 포스처 정책을 모니터링하고 시행합니다. AnyConnect 에이전트는 클라이언트에서 유지됩니다. Cisco ISE에서 AnyConnect를 사용하는 방법에 대한 자세한 내용은 Cisco AnyConnect Secure Mobility, 111 페이지을 참조하십시오.

- **AnyConnect Stealth**: 사용자 인터페이스 없이 포스처를 서비스로 실행합니다. 에이전트는 클라이언트에서 유지됩니다.

  포스처 요건에서 AnyConnect Stealth 포스처 유형을 선택하면 일부 조건, 교정 또는 조건의 속성이 비활성화됩니다(회색으로 표시됨). 예를 들어 AnyConnect Stealth 요건을 활성화하면 클라이언트측 상호 작용이 필요하므로 수동 교정 유형이 비활성화됩니다(회색으로 표시됨).

  포스처 프로파일을 AnyConnect 컨피그레이션에 매핑한 다음 AnyConnect Stealth 모드 구축 시에 Anyconnect 컨피그레이션을 클라이언트 프로비저닝 창에 매핑하면 다음이 지원됩니다.

  - AnyConnect가 포스처 프로파일을 읽고 원하는 모드로 설정할 수 있습니다.
  - AnyConnect가 초기 상태 요청 중에 선택한 모드와 관련된 정보를 Cisco ISE로 전송할 수 있습니다.

- Cisco ISE가 모드와 기타 요소(ID 그룹, OS 및 규정 준수 모듈 등)를 기반으로 올바른 정책을 일치시킬 수 있습니다.

참고 AnyConnect Stealth 모드를 사용하려면 AnyConnect 버전 4.4 이상이 필요합니다.

Cisco ISE에서 AnyConnect Stealth를 구성하는 방법에 대한 자세한 내용은 AnyConnect 스텔스 모드 워크플로우 구성, 78 페이지을 참조하십시오.

- **Temporal Agent**: 클라이언트가 신뢰할 수 있는 네트워크에 액세스하려고 하면 Cisco ISE가 클라이언트 프로비저닝 포털을 엽니다. 포털은 사용자에게 에이전트를 다운로드 및 설치하고 에이전트를 실행하도록 지시합니다. 임시 에이전트는 규정 준수 상태를 확인하고 Cisco ISE에 상태를 전송합니다. 그 결과에 따라 Cisco ISE가 작동합니다. 규정 준수 처리가 완료되면 임시 에이전트가 클라이언트에서 스스로를 제거합니다. 임시 에이전트는 사용자 맞춤화 교정을 지원하지 않습니다. 기본 교정은 메시지 텍스트만 지원합니다.

  Temporal Agent는 다음 조건을 지원하지 않습니다.

  - 서비스 조건 MAC—시스템 데몬 확인
  - 서비스 조건-MAC—데몬 또는 사용자 에이전트 검사
  - PM—최신 상태 확인
  - PM - 활성화 검사
  - DE—암호화 확인
  - **Posture Types(**포스처 유형**) Temporal Agent(**임시 에이전트**)** 및 **Compliance Module(**규정 준수 모듈**) 4.x** 이상을 사용해 포스처 정책을 구성합니다. 규정 준수 모듈을 **3.x or earlier(3.x** 이하**)** 또는 **Any Version(**모든 버전**)**으로 구성하지 마십시오.
  - Termporal Agent의 경우, **Requirements(**요건**)** 창에서 **Installation(**설치**)** 확인 유형을 포함하는 패치 관리 조건만 볼 수 있습니다.
  - Cisco ISE는 Mac OSX용 Temporal Agent에서 VLAN 제어 포스처를 지원하지 않습니다. 기존 VLAN에서 새 VLAN으로 네트워크 액세스를 변경하면 VLAN 변경 전에 사용자의 IP 주소가 해제됩니다. 사용자가 새 VLAN에 연결할 때 클라이언트는 DHCP를 통해 새 IP 주소를 가져옵니다. 새 IP 주소를 인식하려면 루트 권한이 필요하지만 Temporal Agent는 사용자 프로세스로 실행됩니다.
  - Cisco ISE는 ACL로 제어되는 포스처 환경을 지원하며 여기에서는 엔드포인트의 IP 주소의 새로고침이 필요하지 않습니다.
  - Cisco ISE에서 Temporal Agent를 구성하는 방법에 대한 자세한 내용은 Cisco 임시 에이전트 구성 워크플로우, 83 페이지을 참조하십시오.

- **AMP Enabler**—AMP Enabler는 엔터프라이즈 내의 로컬로 호스팅되는 서버에서 엔드포인트 하위 집합으로 엔드포인트용 AMP 소프트웨어를 푸시하고 기존 사용자 기반에 대해 AMP 서비스

를 설치합니다. AMP 프로파일러에 대한 설명은 AMP Enabler 프로파일 설정, 94 페이지에 제시되어 있습니다.

- **Agentless Posture(**에이전트리스 포스처**)**—에이전트리스 포스처는 클라이언트에서 얻는 포스처 정보를 제공하며 작업이 완료되면 스스로 완전히 제거됩니다. 최종 사용자 측에서 취해야 할 작업은 없습니다. Temporal Agent와 달리 Agentless Posture는 관리 사용자로 클라이언트에 연결합니다. Cisco ISE에서 에이전트리스 포스처를 사용하는 방법에 대한 자세한 내용은 에이전트리스 포스처, 4 페이지를 참조하십시오.

클라이언트 프로비저닝 페이지(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Client Provisioning(**클라이언트 프로비저닝**) > Resources(**리소스**)**와 포스처 요건 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Posture(**포스처**) > Requirements(**요건**)**에서 포스처 유형을 사용합니다. 모범 사례는 클라이언트 프로비저닝 창에서 포스처 프로파일을 프로비저닝하는 것입니다.

관련 항목

AnyConnect 스텔스 모드 워크플로우 구성, 78 페이지
Cisco 임시 에이전트 구성 워크플로우, 83 페이지

에이전트리스 포스처

Agentless Posture(에이전트리스 포스처)는 클라이언트에서 얻는 포스처 정보를 제공하며 작업이 완료되면 스스로 완전히 제거됩니다. 최종 사용자 측에서 취해야 할 작업은 없습니다.

요구 사항

- 클라이언트는 IP 주소로 연결할 수 있어야 하며, RADIUS 계정 관리에서 해당 IP 주소를 사용할 수 있어야 합니다.
- 현재 Windows 및 Mac 클라이언트가 지원됩니다.
  - Windows 클라이언트의 경우, 클라이언트에서 Powershell에 액세스하기 위한 포트 5985가 열려 있어야 합니다. Powershell은 버전 5.1 이상이어야 합니다. 클라이언트는 cURL 버전 7.34 이상이어야 합니다.
  - Mac OSX 클라이언트의 경우 SSH에 액세스하기 위한 포트 22가 열려 있어야 클라이언트에 액세스할 수 있습니다. 클라이언트는 cURL 버전 7.34 이상이어야 합니다.
- 셸 로그인에 대한 클라이언트 자격 증명에는 로컬 관리자 권한이 있어야 합니다.
- 컨피그레이션 단계에 설명된 대로 포스처 피드 업데이트를 실행하여 최신 클라이언트를 가져옵니다.
- 엔드포인트에서 인증서 설치 실패를 방지하려면 sudoers 파일에서 다음 항목이 업데이트되었는지 확인합니다.

```
<macadminusername> ALL = (ALL) NOPASSWD: /usr/bin/security, /usr/bin/osascript
```

- Mac OSX의 경우 구성된 사용자 계정은 관리자 계정이어야 합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Endpoint Scripts(**엔

드포인트 스크립트**)** > **Login Configuration(**로그인 구성**)** > **MAC Local User(MAC** 로컬 사용자**)**. 추가 권한을 부여하더라도 Mac OSX 용 에이전트리스 포스처는 다른 계정 유형에서 작동하지 않습니다.

지원되는 포스처 조건

- 파일 조건
- 서비스 조건
- 애플리케이션 조건
- 외부 데이터 소스 조건
- 복합 조건
- 안티멀웨어 조건
- 패치 관리 조건
- 방화벽 조건
- 디스크 암호화 조건

참고 Mac OSX에서는 서비스 조건이 지원되지 않습니다.

지원되지 않는 포스처 조건

- 교정
- 유예 기간
- 정기적 재평가
- 허용되는 사용 정책

지원되는 클라이언트 운영체제

- Microsoft Windows versions: 10
- Mac OSX versions: 10.13, 10.14, 10.15

Agentless Posture Process Flow

1. 클라이언트가 네트워크에 연결됩니다.
2. Cisco ISE는 클라이언트가 사용하는 권한 부여 프로파일에서 에이전트리스 포스처가 활성화되어 있는지를 탐지합니다.
3. 활성화되어 있을 경우 Cisco ISE는 에이전트리스 포스처 작업 요청을 Cisco ISE 메시징 큐로 전송합니다.

4. Cisco ISE는 메시징 큐에서 작업을 가져오고 에이전트리스 포스처 플로우를 시작합니다.
5. Cisco ISE는 전원 셸 또는 SSH를 통해 클라이언트에 연결합니다.
6. Cisco ISE는 인증서가 아직 클라이언트의 신뢰 인증 기관 저장소에 없는 경우 해당 인증서를 푸시합니다.
7. Cisco ISE는 클라이언트 프로비저닝 정책을 실행합니다.
8. Cisco ISE는 에이전트리스 플러그인을 클라이언트에 푸시하고 플러그인을 시작합니다.
9. 포스처 평가가 클라이언트에서 실행되며 Cisco ISE로 상태를 전송합니다.
10. Cisco ISE는 클라이언트에서 에이전트리스 플러그인을 제거합니다. 포스처 플로우 로그는 클라이언트에 24시간 동안 또는 클라이언트가 삭제할 때까지 유지됩니다.

에이전트리스 포스처 컨피그레이션

1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)> Policy Elements(**정책 요소**) > Results(**결과**) > Posture(**포스처**) > Requirements(**요건**)**에서 요건을 확인하기 위해서 에이전트리스 포스처를 사용하는 하나 이상의 포스처 요건을 생성합니다.
2. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > Posture(**포스처**) > Posture Policy(**포스처 정책**)**에서 해당 포스처 요건에 대해 에이전트리스 포스처를 사용하는 하나 이상의 지원되는 포스처 정책 규칙을 생성합니다. 사용하려는 규칙을 복제하고 포스처 유형을 에이전트리스로 변경할 수 있습니다.
3. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Authorization(**권한 부여**) > Authorization Profiles(**권한 부여 프로파일**)**에서 에이전트리스 포스처의 결과를 평가하는 권한 부여 프로파일을 생성할 수 있습니다.
   - 권한 부여 프로파일에서 에이전트리스 포스처를 활성화합니다.
   - 이 프로파일은 에이전트리스 포츠처에만 사용합니다. 다른 포스처 유형에는 이 값을 사용하지 마십시오.
   - 에이전트리스 포스처에는 CWA 및 리디렉션 ACL이 필요하지 않습니다. VLAN, DACL 또는 ACL을 세그멘테이션 규칙의 일부로 사용할 수 있습니다.
4. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**) > Client Provisioning(**클라이언트 프로비저닝**)**을 선택하고 클라이언트 프로비저닝 정책을 추가합니다. Cisco Agent Configuration(Cisco Agent 컨피그레이션)에서 구성한 운영체제에 대한 에이전트리스 플러그인을 선택합니다. Windows의 경우 플러그인은 CiscoAgentlessWindows 4.9.01095입니다. MacOS의 경우 플러그인은 CiscoAgentlessOSX 4.9.01095입니다. 이 규칙이 확인하는 포스처 조건을 선택합니다. Active Directory를 사용하는 경우 정책에서 Active Directory 그룹을 사용할 수 있습니다.

참고 MACOSX 10.14 및 10.15 버전에 대한 에이전트리스 포스처 컨피그레이션은 포스처 피드를 업데이트할 때까지 사용할 수 없습니다. 포스처 피드를 실행하기 전에 포스처 피드 URL을 업데이트하십시오. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Posture(**포스처**)** > **Settings(**설정**)** > **Software Updates(**소프트웨어 업데이트**)** > **Posture Updates(**포스처 업데이트**)**. **Posture Updates(**포스처 업데이트**)** 창에서 **Update Feed URL(**피드 **URL** 업데이트**)** 필드에 URL(https://www.cisco.com/web/secure/spa/posture-update.xml)를 입력하고 **Update Now(**지금 업데이트**)**를 클릭합니다.

5. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**에서 권한 부여 정책을 확장합니다. 다음 3가지 권한 부여 정책을 활성화하고 구성합니다.
   - **Unknown_Compliance_Redirect**: Configure conditions Network_Access_Authentication_Passed AND Compliance_Unknown_Devices with result Agentless Posture.
   - **NonCompliant_Devices_Redirect**: Configure conditions Network_Access_Authentication_Passed and Non_Compliant_Devices with result DenyAccess.
   - **Compliant_Devices_Access**: Configure conditions Network_Access_Authentication_Passed and Compliant_Devices with result PermitAccess.
6. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Settings(**설정**)** > **Endpoint Scripts(**엔드포이트 스크립트**)** > **Endpoint Login Configuration(**엔드포인트 로그인 구성**)**에서클라이언트 자격 증명을 구성하고 클라이언트에 로그인합니다. 동일한 자격증명이 엔드포인트 스크립트에서도 사용됩니다. 자세한 내용은 를 참고하십시오.<Link to Endpoint Scripts topic>>.
7. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Settings(**설정**)** > **Endpoint Scripts(**엔드포인트 스크립트**)** > **Settings(**설정**)**에서 **OS** 식별을 위한 최대 재시도 횟수와 **OS** 식별을 위한 재시도 간 지연 시간을 구성합니다. 이러한 설정에 따라 연결 문제를 얼마나 빨리 확인할 수 있는지가 결정됩니다. 예를 들어 PowerShell 포트가 열려 있지 않다는 오류는 재시도가 다 사용되지 않은 경우에로그에 표시되지 않습니다.
8. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **General Settings(**일반 설정**)**에서 에이전트리스 포스처 설정을 구성합니다. 포스처 일반 설정, 16 페이지을(를) 참조하십시오.
9. 클라이언트가 에이전트리스 포스처에 연결되면 라이브 로그에서 확인할 수 있습니다.

디버깅 및 문제 해결

다음에 대해 디버그 로그 레벨을 활성화합니다.

- 인프라
- 클라이언트 프로비저닝
- 포스처

디버그 로그는 *ise-psc.log*에 있습니다.

에이전트리스 포스처 문제 해결은 다음에서 사용할 수 있습니다.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Live Logs(**라이브 로그**)**—포스처 상태 열 아래에 있는 점 세 개로 에이전트리스 포스처 문제 해결을 엽니다.
- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Troubleshoot(**문제 해결**) > Diagnostics(**진단**) > General Tools(**일반 도구**)**

에이전트리스 포스처 문제 해결에 대한 자세한 내용은 유지 관리 및 모니터링 장을 참조하십시오.

에이전트리스 포스처 문제 해결

에이전트리스 포스처 보고서는 에이전트가 없는 포스처가 정상적으로 작동하지 않을 때 활용할 수 있는 기본 문제 해결 도구입니다. 이 보고서에는 스크립트 업로드 완료, 스크립트 업로드 실패, 스크립트 실행 완료 등의 이벤트를 포함하는 에이전트리스 플로우 단계와 알려진 실패 이유가 표시됩니다.

다음 두 위치에서 에이전트리스 포스처 문제 해결에 액세스할 수 있습니다.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Live Logs(**라이브 로그**)**: 문제를 해결하려는 클라이언트의 Posture Status(포스처 상태) 열에서 3개의 세로 점을 클릭합니다.
- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Troubleshoot(**문제 해결**) > Diagnostics(**진단**) > General Tools(**일반 도구**) > Agentless Posture Troubleshooting(**에이전트리스 포스처 문제 해결**)**을 선택합니다.

에이전트리스 포스처 문제 해결 도구는 지정된 클라이언트에 대한 에이전트리스 포스처 활동을 수집합니다. **Agentless Posture Flow(**에이전트리스 포스처 플로우**)**는 포스처를 시작하고 현재 활성 상태인 클라이언트와 Cisco ISE 간의 모든 상호 작용을 표시합니다. **Only Download Client Logs(**클라이언트 로그만 다운로드**)**에서는 클라이언트에서 지난 24시간 동안의 포스처 플로우가 포함된 로그를 생성합니다. 클라이언트는 언제든지 로그를 삭제할 수 있습니다. 수집이 완료되면 로그의 ZIP 파일을 내보낼 수 있습니다.

보고서

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Reports(**보고서**) > Reports(**보고서**) > Endpoints and Users(**엔드포인트 및 사용자**) > Agentless Posture(**에이전트리스 포스처**)**를 선택하여 에이전트리스 포스처를 실행하는 모든 엔드포인트를 확인합니다.

포스처 관리 설정

포스처 서비스에 맞게 전역적으로 관리 포털을 구성할 수 있습니다. 웹을 통해 Cisco에서 Cisco ISE 서버로 업데이트를 자동 다운로드할 수 있습니다. 또한 나중에 오프라인에서 Cisco ISE를 수동으로 업데이트할 수도 있습니다. 또한 AnyConnect, 또는 웹 에이전트와 같은 에이전트를 클라이언트에 설치하면 Posture Assessment 및 교정 서비스를 클라이언트에게 제공할 수 있습니다. 클라이언트 에이전트는 Cisco ISE에 대한 클라이언트의 규정 준수 상태를 정기적으로 업데이트합니다. 로그인 및 포

스처에 대한 성공적인 요건 평가가 완료되면 최종 사용자가 네트워크 사용 약관을 준수하도록 요구하는 링크가 포함된 대화 상자가 클라이언트 에이전트에 표시됩니다. 이 링크를 사용하여 엔터프라이즈 네트워크에 대한 네트워크 사용 정보를 정의할 수 있습니다. 이 정보는 최종 사용자가 네트워크에 액세스하려면 동의해야 하는 정보입니다.

클라이언트 포스처 요건

포스처 요건을 생성하려면 다음을 따릅니다.

1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Posture(포스처) > Requirements(요건)**를 선택합니다.
2. 아무 요건 행 끝에 있는 **Edit(편집)** 드롭다운 목록에서 **Insert New Requirement(새 요건 삽입)**를 선택합니다.
3. 필요한 세부정보를 입력하고 **Done(완료)**을 클릭합니다.

다음 표에서는 **Client Posture Requirements(클라이언트 포스처 요건)** 창의 필드에 대해 설명합니다.

표 *1:* 포스처 요건

필드 이름	사용 지침
Name(이름)	요건의 이름을 입력합니다.
Operating Systems(운영체제)	운영체제를 선택합니다. 정책에 여러 운영체제를 연결하려면 더하기 [+]를 클릭합니다. 정책에서 운영체제를 제거하려면 빼기 [-]를 클릭합니다.
규정 준수 모듈**(Compliance Module)**	**Compliance Module(규정 준수 모듈)** 드롭다운 목록에서 필요한 규정 준수 모듈을 선택합니다. • 4.x 이상: 안티멀웨어, 디스크 암호화, 패치 관리 및 USB 조건을 지원합니다. • 3.x 이하: 안티바이러스, 안티스파이웨어, 디스크 암호화 및 패치 관리 조건을 지원합니다. • 모든 버전: 파일, 서비스, 레지스트리, 애플리케이션 및 복합 조건을 지원합니다. 규정 준수 모듈에 대한 자세한 내용은 규정 준수 모듈, 27 페이지에서 참조하십시오.

필드 이름	사용 지침
포스처 유형**(Posture Type)**	**Posture Type(**포스처 유형**)** 드롭다운 목록에서 필요한 포스처 유형을 선택합니다. • AnyConnect: AnyConnect 에이전트를 구축하여 클라이언트 상호 작용이 필요한 Cisco ISE 정책을 모니터링하고 시행합니다. • AnyConnect Stealth: AnyConnect 에이전트를 구축하여 클라이언트 상호 작용 없이 Cisco ISE 포스처 정책을 모니터링하고 시행합니다. • Temporal Agent(임시 에이전트): 규정 준수 상태를 확인하기 위해 클라이언트에서 실행되는 임시 실행 파일입니다.
Conditions(조건**)**	목록에서 조건을 선택합니다. Action(작업) 아이콘을 클릭하여 사용자 맞춤화 조건을 생성하고 요건과 연결할 수도 있습니다. 사용자 맞춤화 조건을 생성하는 경우 연결된 상위 운영체제를 편집할 수 없습니다. pr_WSUSRule은 더미 복합 조건으로, WSUS(Windows Server Update Services) 교정이 연결되어 있는 포스처 요건에 사용됩니다. 연결된 WSUS 교정 작업은 심각도 레벨 옵션을 사용해 Windows 업데이트를 검증하도록 구성해야 합니다. 이 요건이 충족되지 않으면 Windows 클라이언트에 설치된 Agent는 WSUS 교정에 정의된 심각도 레벨에 따라 WSUS 교정 작업을 시행합니다. 복합 조건 목록 페이지에서는 pr_WSUSRule을 볼 수 없습니다. pr_WSUSRule은 조건 위젯에서만 선택 가능합니다.

필드 이름	사용 지침
Remediation Actions(교정 작업**)**	목록에서 교정을 선택합니다. 교정 작업을 생성하고 이를 요건과 연결할 수도 있습니다. 에이전트 사용자와의 통신에 사용할 수 있는 모든 교정 유형에 대해서는 텍스트 상자가 있습니다. 교정 작업 외에도, 메시지를 사용하여 클라이언트의 규정 미준수에 대해 에이전트 사용자에게 통신할 수 있습니다. **Message Text Only(**메시지 텍스트 전용**)** 옵션을 사용하면 에이전트 사용자에게 규정 미준수에 대해 알릴 수 있습니다. 헬프 데스크에 연결하여 자세한 정보를 얻거나 클라이언트를 수동으로 교정하기 위한 선택적 지침을 사용자에게 제공하기도 합니다. 이 시나리오에서 NAC 에이전트는 교정 작업을 트리거하지 않습니다.

관련 항목

Posture Assessment용 사용 제한 정책 구성, 22 페이지
클라이언트 포스처 요건 생성, 73 페이지

클라이언트용 타이머 설정

사용자가 교정을 수행하고 상태 간을 전환하고 로그인 성공 화면을 제어하도록 타이머를 설정할 수 있습니다.

이러한 설정이 정책을 기반으로 지정되도록 교정 타이머 및 네트워크 전환 지연 타이머와 클라이언트의 로그인 성공 화면을 제어하는 데 사용되는 타이머를 모두 사용하여 에이전트 프로파일을 구성하는 것이 좋습니다. **AnyConnect Posture Profile(AnyConnect** 포스처 프로파일**)** 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)** > **Add(**추가**)** > **AnyConnect Posture Profile(AnyConnect** 포스처 프로파일**)**)에서 클라이언트 프로비저닝 리소스의 에이전트에 대해 이러한 모든 타이머를 구성할 수 있습니다.

그러나 클라이언트 프로비저닝 정책과 일치하도록 구성된 에이전트 프로파일이 없는 경우 **General Settings(**일반 설정**)** 구성 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **General Settings(**일반 설정**)**)의 설정을 사용할 수 있습니다.

지정된 시간 내에 클라이언트를 교정하기 위한 교정 타이머 설정

지정된 시간 내에 클라이언트 교정을 수행하기 위한 타이머를 구성할 수 있습니다. 클라이언트가 초기 평가에서 구성된 Posture Policies를 충족하지 못하면 에이전트는 클라이언트가 교정 타이머에 구성된 시간 이내에 교정되도록 대기합니다. 클라이언트가 이 지정된 시간 이내에 교정되지 않으면 클

라이언트 에이전트는 포스처 런타임 서비스에 보고서를 보내며, 그리고 나면 클라이언트는 미준수 상태로 전환됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **General Settings(**일반 설정**)**

단계 **2** **Remediation Timer(**교정 타이머**)** 필드에 시간 값을 분 단위로 입력합니다.

기본값은 4분입니다. 유효 범위는 1~300분입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

클라이언트를 전환할 네트워크 전환 지연 타이머 설정

네트워크 전환 지연 타이머를 사용하여 지정된 시간 이내에 클라이언트가 특정 상태에서 다른 상태로 전환되도록 타이머를 구성할 수 있습니다. CoA(Change of Authorization)를 완료하려면 이 타이머를 구성해야 합니다. 클라이언트가 포스처 성공 및 실패 시에 새 VLAN IP 주소를 가져오기 위한 시간이 필요한 경우 지연 시간을 더 길게 설정해야 할 수 있습니다. 포스처가 정상적으로 완료되면 Cisco ISE는 클라이언트가 네트워크 전환 지연 타이머에 지정된 시간 이내에 알 수 없음 모드에서 준수 모드로 전환할 수 있도록 허용합니다. 포스처가 실패하면 Cisco ISE는 클라이언트가 타이머에 지정된 시간 이내에 알 수 없음 모드에서 미준수 모드로 전환할 수 있도록 허용합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **General Settings(**일반 설정**)**

단계 **2** **Network Transition Delay(**네트워크 전환 지연**)** 필드에 시간 값을 초 단위로 입력합니다.

기본값은 3초입니다. 유효 범위는 2초~30초입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

로그인 성공 창이 자동으로 닫히도록 설정

Posture Assessment가 정상적으로 수행되고 나면 클라이언트 에이전트에 임시 네트워크 액세스 화면이 표시됩니다. 사용자는 로그인 창을 닫으려면 해당 화면에서 **OK(**확인**)** 버튼을 클릭해야 합니다. 지정된 시간이 지나면 이 로그인 화면을 자동으로 닫도록 타이머를 설정할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **General Settings(**일반 설정**)**

단계 **2** **Automatically Close Login Success Screen After(**다음 시간 이후 자동으로 로그인 성공 화면 닫기**)** 확인란을 선택합니다.

단계 **3** **Automatically Close Login Success Screen After(**다음 시간 이후 자동으로 로그인 성공 화면 닫기**)** 확인란 옆의 필드에 시간 값을 초 단위로 입력합니다.

유효 범위는 0~300초입니다. 시간을 0으로 설정하면 AnyConnect에 로그인 성공 화면이 표시되지 않습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

에이전트가 아닌 디바이스의 포스처 상태 설정

에이전트가 아닌 디바이스에서 실행되는 엔드포인트의 포스처 상태를 구성할 수 있습니다. Android 디바이스와 iPod, iPhone, iPad 등의 Apple 디바이스는 Cisco ISE가 활성화된 네트워크에 연결할 때 Default Posture Status(기본 포스처 상태) 설정을 사용합니다.

포스처 실행 시간 중에 일치하는 정책을 찾을 수 없을 때는 Windows 및 Macintosh 운영체제에서 실행되는 엔드포인트에도 이러한 설정을 적용할 수 있습니다.

시작하기 전에

엔드포인트에서 정책을 시행하려면 해당하는 클라이언트 프로비저닝 정책(에이전트 설치 패키지)을 구성해야 합니다. 그렇지 않으면 엔드포인트의 포스처 상태가 기본 설정을 자동으로 반영합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **General Settings(**일반 설정**)**

단계 **2** **Default Posture Status(**기본 포스처 상태**)** 드롭다운 목록에서 옵션을 **Compliant(**준수**)** 또는 **Noncompliant(**미준수**)**로 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

포스처 임대

사용자가 네트워크에 로그인할 때마다 Posture Assessment를 수행하도록 Cisco ISE를 구성할 수도 있고 지정된 간격으로 Posture Assessment를 수행할 수도 있습니다. 유효 범위는 1~365일입니다.

이 컨피그레이션은 포스처 평가에 AnyConnect 에이전트를 사용하는 사용자에게만 적용됩니다.

포스처 임대가 활성 상태이면 Cisco ISE는 마지막으로 알려진 포스처 상태를 사용하며, 엔드포인트에 연결하여 규정 준수를 확인하지 않습니다. 그러나 포스처 임대가 만료되면 Cisco ISE는 엔드포인트에 대한 재인증 또는 포스처 재평가를 자동으로 트리거하지 않습니다. 엔드포인트는 동일한 세션이 사용되고 있으므로 동일한 규정 준수 상태로 유지됩니다. 엔드포인트가 다시 인증되면 포스처가 실행되고 포스처 임대 시간이 재설정됩니다.

활용 사례 시나리오 예:

- 사용자가 엔드포인트에 로그온하면 포스처가 1일로 설정된 포스처 임대를 따르게 됩니다.
- 4시간 후 사용자가 엔드포인트에서 로그오프합니다. 이제 포스처 임대는 20시간 남았습니다.
- 1시간 후 사용자가 다시 로그온합니다. 이제 포스처 임대가 19시간 남았습니다. 마지막으로 확인한 포스처 상태가 규정 준수 상태입니다. 따라서 엔드포인트에서 실행되는 포스처 없이도 사용자에게 액세스 권한이 제공됩니다.

- 4시간 후 사용자가 로그오프합니다. 이제 포스처 임대는 15시간 남았습니다.
- 14시간 후 사용자가 로그온합니다. 포스처 임대가 1시간 남았습니다. 마지막으로 확인한 포스처 상태가 규정 준수 상태입니다. 엔드포인트에서 실행되는 포스처 없이도 사용자에게 액세스 권한이 제공됩니다.
- 1시간 후 포스처 임대가 만료됩니다. 동일한 사용자 세션이 사용 중이므로 사용자는 여전히 네트워크에 연결되어 있습니다.
- 1시간 후 사용자가 로그오프합니다. 세션은 사용자와 연결되어 있지만, 시스템과는 연결되지 않으므로 시스템이 네트워크에 남아 있을 수 있습니다.
- 1시간 후 사용자가 로그온합니다. 포스처 임대가 만료되고 새 사용자 세션이 시작되었으므로, 시스템은 포스처 평가를 수행합니다. 결과가 Cisco ISE로 전송되고, 이 활용 사례의 경우 포스처 임대 타이머가 1일로 재설정됩니다.

정기적 재평가

PRA(Periodic reassessment)는 규정을 준수하도록 이미 포스처되어 있는 클라이언트에만 수행할 수 있습니다. 클라이언트가 네트워크에서 규정을 준수하지 않을 경우에는 PRA가 발생할 수 없습니다.

엔드포인트가 규정 준수 상태인 경우에만 PRA가 유효하고 적용 가능합니다. 정책 서비스 노드가 관련 정책을 확인하고 컨피그레이션에 PRA를 시행하도록 정의되어 있는 클라이언트 역할에 따라 요건을 컴파일합니다. PRA 컨피그레이션 일치 항목이 발견되면 정책 서비스 노드가 CoA 요청을 실행하기 전에 컨피그레이션에 클라이언트에 대해 정의된 PRA 속성을 사용하여 클라이언트 에이전트에 응답합니다. 클라이언트 에이전트는 정기적으로 컨피그레이션에 지정된 간격을 기준으로 PRA 요청을 보냅니다. 클라이언트는 PRA에 성공하면 규정 준수 상태를 유지하고 PRA 컨피그레이션에 구성된 작업이 계속 진행됩니다. 클라이언트가 PRA를 충족하지 못하면 클라이언트가 규정 준수 상태에서 규정 미준수 상태로 전환됩니다.

PRA 요청에서 PostureStatus 속성은 포스처 재평가 요청인 경우에도 현재 포스처 상태를 알 수 없는 상태가 아니라 규정 준수 상태로 표시합니다. PostureStatus는 모니터링 보고서에서도 업데이트됩니다.

포스처 리스가 만료되지 않은 경우 엔드포인트는 ACL(Access Control List, 액세스 제어 목록)을 기반으로 규정을 준수하며 PRA가 시작됩니다. PRA에 장애가 발생할 경우 엔드포인트가 규정 비준수 상태로 간주되며 포스처 리스가 재설정됩니다.

정기 재평가 구성

규정 준수를 위해 이미 정상적으로 포스처된 클라이언트에 대해서만 정기 재평가를 구성할 수 있습니다. 시스템에 정의되어 있는 사용자 ID 그룹에 대해 각 PRA를 구성할 수 있습니다.

시작하기 전에

- 각 PRA(Periodic reassessment) 컨피그레이션이 컨피그레이션에 할당된 사용자 ID 그룹의 고유한 조합 또는 고유한 그룹을 포함하고 있는지 확인합니다.

- PRA 컨피그레이션에 대한 두 가지 고유 역할인 role_test_1 및 role_test_2를 할당할 수 있습니다. 논리 연산자로 이 두 역할을 결합하고 두 역할의 고유한 조합으로 PRA 컨피그레이션을 할당할 수 있습니다. 예를 들면 role_test_1 OR role_test_2와 같이 조합할 수 있습니다.
- 두 PRA 컨피그레이션에 공통된 사용자 ID 그룹이 포함되어 있지 않은지 확인합니다.
- 사용자 ID 그룹 *Any*를 포함하는 PRA 컨피그레이션이 이미 있는 경우에는 다음의 작업을 수행하지 않으면 다른 PRA 컨피그레이션을 생성할 수 없습니다.
  - *Any* 이외의 사용자 ID 그룹을 반영하도록 Any 사용자 ID 그룹이 포함된 기존 PRA 컨피그레이션을 업데이트합니다.
  - 사용자 ID 그룹 "*Any*"를 포함하는 기존 PRA 컨피그레이션을 삭제합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **Reassessments(**재평가**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **New Reassessment Configuration(**새 재평가 컨피그레이션**)** 창의 값을 수정하여 새 PRA를 생성합니다.

단계 **4** **Submit(**제출**)**을 클릭하여 PRA 컨피그레이션을 생성합니다.

포스처 문제 해결 설정

다음 표에서는 네트워크의 포스처 문제를 찾고 해결하는 데 사용할 수 있는 포스처 문제 해결 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Posture Troubleshooting(**포스처 문제해결**)**입니다.

표 ***2:*** 포스처 문제 해결 설정

필드 이름	사용 지침
문제 해결을 위한 포스처 이벤트 검색 및 선택	
Username(사용자 이름**)**	필터 기준으로 사용할 사용자 이름을 입력합니다.
MAC Address(MAC 주소**)**	필터 기준으로 사용할 MAC 주소를 xx-xx-xx-xx-xx-xx 형식으로 입력합니다.
Posture Status(포스처 상태**)**	필터 기준으로 사용할 인증 상태를 선택합니다.
Failure Reason(실패 이유**)**	실패 이유를 입력하거나 **Select(**선택**)**를 클릭하고 목록에서 실패 이유를 선택합니다. 실패 이유를 지우려면 **Clear(**지우기**)**를 클릭합니다.

필드 이름	사용 지침
Time Range(시간 범위**)**	시간 범위를 선택합니다. 이 시간 범위 동안 생성되는 RADIUS 인증 기록이 사용됩니다.
Start Date-Time(시작 날짜/시간**):**	(Custom Time Range(사용자 맞춤화 시간 범위)를 선택할 때만 사용 가능) 시작 날짜와 시간을 입력하거나 달력 아이콘을 클릭하고 시작 날짜와 시간을 선택합니다. 날짜는 *mm/dd/yyyy* 형식이어야 하며 시간은 *hh:mm* 형식이어야 합니다.
End Date-Time(종료 날짜/시간**):**	(Custom Time Range(사용자 맞춤화 시간 범위)를 선택할 때만 사용 가능) 종료 날짜와 시간을 입력하거나 달력 아이콘을 클릭하고 시작 날짜와 시간을 선택합니다. 날짜는 *mm/dd/yyyy* 형식이어야 하며 시간은 *hh:mm* 형식이어야 합니다.
Fetch Number of Records(가져올 기록 수**)**	표시할 기록 수를 10, 20, 50, 100, 200, 500개 중에서 선택합니다.
Search Result(검색 결과**)**	
Time(시간**)**	이벤트의 시간
Status(상태**)**	포스처 상태
Username(사용자 이름**)**	이벤트와 관련된 사용자 이름
MAC Address(MAC 주소**)**	시스템의 MAC 주소
Failure Reason(실패 이유**)**	이벤트의 실패 이유

관련 항목

포스처 문제 해결 도구, 85 페이지

포스처 일반 설정

다음 표에서는 교정 시간 및 포스처 상태 등의 일반 포스처 설정을 구성하는 데 사용할 수 있는 Posture General Settings(포스처 일반 설정) 페이지의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **General Settings(**일반 설정**)**입니다.

이러한 설정은 포스 처의 기본 설정이며 포스처 프로파일로 재정의할 수 있습니다.

일반 포스처 설정

- **Remediation Timer(**교정 타이머**)**: 교정을 시작하기 전에 대기 할 시간을 입력합니다. 기본값은 4분입니다. 유효 범위는 1~300분입니다.

- **Network Transition Delay(**네트워크 전환 지연**)**: 시간 값을 초 단위로 입력합니다. 기본값은 3초입니다. 유효 범위는 2초~30초입니다.
- **Default Posture Status(**기본 포스처 상태**)**: **Compliant(**준수**)** 또는 **Noncompliant(**미준수**)**를 선택합니다. 비에이전트 디바이스는 네트워크에 액세스할 때 이 상태로 지정됩니다.
- **Automatically Close Login Success Screen After(**다음 시간 이후 자동으로 로그인 성공 화면 닫기**)**: 지정된 시간이 지난 후 로그인 성공 화면을 자동으로 닫으려면 확인란을 선택합니다. 로그인 화면을 자동으로 닫도록 타이머를 구성할 수 있습니다. 유효 범위는 0~300초입니다. 시간을 0으로 설정하면 클라이언트의 에이전트에 로그인 성공 화면이 표시되지 않습니다.
- **Continuous Monitoring Interval(**연속 모니터링 간격**)**: 시간 간격을 지정하면 이 간격 이후에 AnyConnect가 모니터링 데이터 전송을 시작합니다. 애플리케이션 및 하드웨어 조건의 경우 기본값은 5분입니다.
- **Agentless posture client timeout(**에이전트리스 포스처 클라이언트 시간 초과**)**: 여기에서 지정한 시간이 지나면 포스처 확인이 실패한 것으로 간주됩니다.
- **Remove Agentless Plugin after each run(**매 실행 후 에이전트리스 플러그인 제거**)**: 이 설정을 활성화하면 에이전트리스 포스처의 실행 후 클라이언트에서 에이전트가 제거됩니다. 새 버전이 이용 가능해질 때까지는 다운로드한 플러그인을 재사용할 수 있도록 이 기능을 비활성화한 상태로 두는 것이 좋습니다. 이 설정을 비활성해 두면 네트워크 트래픽을 줄일 수 있습니다.
- **Acceptable Use Policy in Stealth Mode(**스텔스 모드의 허용 가능 사용 정책**)**: 회사의 네트워크 사용 조건이 충족되지 않는 경우 클라이언트를 미준수 포스처 상태로 전환하려면 스텔스 모드에서 **Block(**차단**)**을 선택합니다.

포스처 임대

- **Perform posture assessment every time a user connects to the network(**사용자가 네트워크에 연결할 때마다 포스처 평가 수행**)**: 사용자가 네트워크에 연결할 때마다 포스처 평가를 시작하려면 이 옵션을 선택합니다.
- **Perform posture assessment every n days(n**일마다 포스처 평가 수행**)**: 클라이언트의 포스처 상태가 이미 Compliant(준수)이더라도 지정된 기간(일) 이후 포스처 평가를 시작하려면 이 옵션을 선택합니다.
- **Cache Last Known Posture Compliant Status(**마지막으로 알려진 포스처 준수 상태 캐시**)**: Cisco ISE가 포스처 평가 결과를 캐시하도록 하려면 이 확인란을 선택합니다. 기본적으로 이 필드는 비활성화되어 있습니다.
- **Last Known Posture Compliant Status(**마지막으로 알려진 포스처 준수 상태**)**:이 설정은 **Cache Last Known Posture Compliant Status(**마지막으로 알려진 포스처 준수 상태 캐시**)**를 선택한 경우에만 적용됩니다. Cisco ISE는이 필드에 지정된 시간 동안 포스처 평가 결과를 캐시합니다. 유효한 값은 1~30 일, 1~720 시간 또는 1~43200 분입니다.

관련 항목

포스처 관리 설정, 8 페이지
포스처 임대, 13 페이지

Cisco ISE에 포스처 업데이트 다운로드

포스처 업데이트에는 Windows 및 Macintosh 운영체제용 안티바이러스 및 안티스파이웨어용으로 사전 정의된 확인, 규칙 및 지원 차트 집합과 Cisco에서 지원하는 운영체제 정보가 포함되어 있습니다. 업데이트의 최신 아카이브가 포함된 로컬 시스템의 파일에서 오프라인으로 Cisco ISE를 업데이트할 수도 있습니다.

네트워크에서 Cisco ISE를 처음 구축할 때 웹에서 포스처 업데이트를 다운로드할 수 있습니다. 이 프로세스는 보통 20분 정도 걸립니다. 초기 다운로드 후에는 Cisco ISE가 증분 업데이트 확인 및 다운로드를 자동으로 수행하도록 구성할 수 있습니다.

Cisco ISE는 초기 포스처 업데이트 중에 기본 포스처 정책, 요건 및 교정을 한 번만 생성합니다. 이러한 항목을 삭제하면 Cisco ISE는 후속 수동 업데이트 또는 예약된 업데이트 중에 해당 항목을 다시 생성하지 않습니다.

시작하기 전에

Cisco ISE에 포스처 리소스를 다운로드할 수 있는 적절한 원격 위치에 액세스하려면 Cisco ISE에서 프록시 설정 지정에 나온 대로 네트워크에 대해 올바른 프록시 설정을 구성했는지 확인해야 할 수 있습니다.

포스처 업데이트 창을 사용하여 웹에서 업데이트를 동적으로 다운로드할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Postur(**포스처**)** > **Updates(**업데이트**)**를 선택합니다.

단계 **2** 업데이트를 동적으로 다운로드하려면 **Web(**웹**)** 옵션을 선택합니다.

단계 **3** **Update Feed URL(**업데이트 피드 **URL)** 필드에 대해 Cisco 기본값을 설정하려면 **Set to Default(**기본값으로 설정**)**를 클릭합니다.

네트워크에서 프록시 서버 등을 통한 URL 리디렉션 기능을 제한하는 경우 위 URL에 액세스하는 데 문제가 있으면 Cisco ISE가 관련 항목에 나와 있는 대체 URL을 가리키도록 지정해 보십시오.

단계 **4** **Posture Updates(**포스처 업데이트**)** 창의 값을 수정합니다.

단계 **5** **Update Now(**지금 업데이트**)**를 클릭하여 Cisco에서 업데이트를 다운로드합니다.

Cisco ISE가 업데이트되고 나면 Posture Updates(포스처 업데이트) 창의 Update Information(업데이트 정보) 섹션 아래에 업데이트를 확인할 수 있도록 현재 Cisco 업데이트 버전 정보가 표시됩니다.

단계 **6** **Yes(**예**)**를 클릭하여 계속합니다.

Cisco ISE 오프라인 업데이트

이 오프라인 업데이트 옵션을 사용하면 Cisco ISE를 사용하는 디바이스에서 Cisco.com에 대한 직접 인터넷 액세스를 사용할 수 없거나 보안 정책에 따라 허용되지 않는 경우 클라이언트 프로비저닝 및 포스처 업데이트를 다운로드할 수 있습니다.

클라이언트 프로비저닝 리소스를 다운로드하려면 다음 단계를 수행합니다.

단계 **1** https://software.cisco.com/download/home/283801620/type/283802505/release/3.0.0으로 이동합니다.

단계 **2** 로그인 자격 증명을 입력합니다.

단계 **3** Cisco Identity Services Engine 다운로드 창으로 이동하여 릴리스를 선택합니다.

다음과 같은 오프라인 설치 패키지를 다운로드할 수 있습니다.

- **win_spw-**<*version*>**-isebundle.zip** - Windows용 오프라인 SPW 설치 패키지
- **mac-spw-**<*version*>**.zip** - Mac OS X용 오프라인 SPW 설치 패키지
- **compliancemodule-**<*version*>**-isebundle.zip** - 오프라인 규정 준수 모듈 설치 패키지
- **macagent-**<*version*>**-isebundle.zip** - 오프라인 Mac 에이전트 설치 패키지
- **webagent-**<*version*>**-isebundle.zip** - 오프라인 웹 에이전트 설치 패키지

단계 **4** **Download(**다운로드**)** 또는 **Add to Cart(**장바구니에 추가**)**를 클릭합니다.

Cisco ISE에 다운로드한 설치 패키지를 추가하는 방법에 대한 자세한 내용은 Cisco Identity Services Engine 관리자 가이드의 "로컬 머신에서 클라이언트 프로비저닝 리소스 추가" 섹션을 참조하십시오.

포스처 업데이트를 사용하여 로컬 시스템의 아카이브에서 오프라인으로 Windows 및 Mac 운영체제에 대한 검사, 운영체제 정보, 안티바이러스 및 안티스파이웨어 지원 차트를 업데이트할 수 있습니다.

오프라인 업데이트의 경우 아카이브 파일의 버전이 컨피그레이션 파일의 버전과 일치하는지 확인합니다. Cisco ISE를 구성하고 포스처 정책 서비스에 대해 동적 업데이트를 활성화하려는 경우 오프라인 상태 업데이트를 사용합니다.

오프라인 포스처 업데이트를 다운로드하려면 다음 단계를 수행합니다.

단계 **1** https://www.cisco.com/web/secure/spa/posture-offline.html로 이동합니다.

단계 **2** 로컬 시스템에 **posture-offline.zip** 파일을 저장합니다. 이 파일은 Windows 및 Mac 운영체제의 운영체제 정보, 검사, 규칙, 안티바이러스 및 안티스파이웨어 지원 차트를 업데이트하는 데 사용됩니다.

단계 **3** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Posture(**포스처**)**를 선택합니다.

단계 **4** 포스처에 대한 설정을 보려면 화살표를 클릭합니다.

단계 **5** **Updates(**업데이트**)**를 클릭합니다.
Posture Updates(포스처 업데이트**)** 창이 표시됩니다.

단계 **6** **Offline(**오프라인**)** 옵션을 클릭합니다.

단계 **7** **Browse(**찾아보기**)**를 클릭하여 시스템의 로컬 폴더에서 아카이브 파일(posture-offline.zip)을 찾습니다.

참고 **File to Update(**업데이트할 파일**)** 필드는 필수 필드입니다. 적절한 파일을 포함하는 아카이브 파일(.zip)을 하나만 선택할 수 있습니다. .tar, .gz와 같은 .zip 이외의 아카이브 파일은 지원되지 않습니다.

단계 **8** **Update Now(**지금 업데이트**)**를 클릭합니다.

자동으로 포스처 업데이트 다운로드

초기 업데이트를 완료한 후 Cisco ISE가 업데이트를 자동으로 확인하고 다운로드하도록 구성할 수 있습니다.

시작하기 전에

- 포스처 업데이트를 처음으로 다운로드하여 Cisco ISE가 업데이트를 자동으로 확인하고 다운로드하도록 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Postur(**포스처**)** > **Updates(**업데이트**)**를 선택합니다.

단계 **2** **Posture Updates(**포스처 업데이트**)** 창에서 **Automatically check for updates starting from initial delay(**초기 지연 시간부터 업데이트 자동 확인**)** 확인란을 선택합니다.

단계 **3** 초기 지연 시간을 hh:mm:ss 형식으로 입력합니다.

Cisco ISE는 초기 지연 시간이 종료된 후 업데이트 확인을 시작합니다.

단계 **4** 시간 간격을 시간 단위로 입력합니다.

Cisco ISE는 초기 지연 시간부터 지정된 간격으로 구축에 업데이트를 다운로드합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

포스처 사용 제한 정책 컨피그레이션 설정

다음 표에서는 포스처용 사용 제한 정책을 구성하는 데 사용할 수 있는 포스처 사용 제한 정책 컨피그레이션 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **Acceptable Use Policy(**허용 가능 사용 정책**)**입니다.

표 ***3:*** 포스처 ***AUP*** 컨피그레이션 설정

필드 이름	사용 지침
Configuration Name(컨피그레이션 이름**)**	생성할 AUP 컨피그레이션의 이름을 입력합니다.
Configuration Description(컨피그레이션 설명**)**	생성할 AUP 컨피그레이션의 설명을 입력합니다.
에이전트 사용자에게 **AUP** 표시**(Windows**만 해당**)**	선택하면 인증 및 포스처 평가에 성공 시 네트워크의 네트워크 사용 약관 링크가 사용자에게 표시됩니다.
Use URL for AUP message(AUP 메시지에 **URL** 사용**)**	선택하면 AUP URL 필드에 AUP 메시지의 URL을 입력해야 합니다.
Use URL for AUP message(AUP 메시지에 파일 사용**)**	선택하면 압축된 형식의 파일이 있는 위치로 이동하여 해당 파일을 업로드해야 합니다. 파일은 최상위 레벨에서 index.html을 포함해야 합니다. .zip 파일은 index.html 파일 이외의 다른 파일과 하위 디렉토리를 포함할 수 있습니다. 이러한 파일은 HTML 태그를 사용하여 서로를 참조할 수 있습니다.
AUP URL	클라이언트가 인증 및 포스처 평가 성공 시 액세스해야 하는 AUP의 URL을 입력합니다.
AUP File(AUP 파일**)**	파일을 찾아 Cisco ISE 서버에 업로드합니다. 이 파일은 압축 파일이어야 하며, 압축 파일의 최상위 레벨에는 index.html이 포함되어 있어야 합니다.

필드 이름	사용 지침
Select User Identity Groups(사용자 **ID** 그룹 선택**)**	AUP 컨피그레이션에 대해 고유한 사용자 ID 그룹 또는 고유한 사용자 ID 그룹 조합을 선택합니다. AUP 컨피그레이션을 생성하는 동안에는 다음 사항에 유의해 주십시오. • 게스트 흐름에는 포스처 AUP가 적용되지 않습니다. • 두 컨피그레이션에 같은 사용자 ID 그룹을 포함할 수는 없습니다. • "모두" 사용자 ID 그룹을 사용하여 AUP 컨피그레이션을 생성하려는 경우 먼저 다른 AUP 컨피그레이션을 모두 삭제해야 합니다. • "모두" 사용자 ID 그룹을 사용하여 AUP 컨피그레이션을 생성하는 경우에는 하나 이상의 고유한 사용자 ID 그룹을 사용하여 다른 AUP 컨피그레이션을 생성할 수 없습니다. "모두" 이외의 사용자 ID 그룹을 사용하여 AUP 컨피그레이션을 생성하려면 "모두" 사용자 ID 그룹이 포함된 기존 AUP 컨피그레이션을 먼저 삭제하거나, "모두" 사용자 ID 그룹이 포함된 기존 AUP 컨피그레이션을 하나 이상의 고유한 사용자 ID 그룹으로 업데이트합니다.
Acceptable use policy configurations—Configurations list(사용 제한 정책 컨피그레이션 - 컨피그레이션 목록**)**	AUP 컨피그레이션과 연결된 기존 AUP 컨피그레이션 및 최종 사용자 ID 그룹이 나열됩니다.

관련 항목

Posture Assessment용 사용 제한 정책 구성, 22 페이지

Posture Assessment용 사용 제한 정책 구성

클라이언트가 로그인하여 Posture Assessment를 정상적으로 수행하고 나면 임시 네트워크 액세스 화면이 표시됩니다. 이 화면에는 AUP(Acceptable Use Policy)에 대한 링크가 포함되어 있습니다. 사용자가 링크를 클릭하면 네트워크 사용 약관이 표시되는 페이지로 리디렉션되며, 해당 약관을 읽고 내용에 동의해야 합니다.

각 사용 제한 정책 컨피그레이션에는 고유한 사용자 ID 그룹 또는 고유한 사용자 ID 그룹 조합이 있어야 합니다. Cisco ISE는 AUP에서 일치하는 첫 번째 사용자 ID 그룹을 찾은 다음 AUP를 표시하는 클라이언트 에이전트에 해당 그룹을 전송합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **Acceptable Use Policy(**사용 제한 정책**)**을 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **New Acceptable Use Policy Configuration(**새 사용 제한 정책 컨피그레이션**)** 창의 값을 수정합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

포스처 조건

포스처 조건은 파일, 레지스트리, 애플리케이션, 서비스 또는 사전 조건의 단순 조건 중 하나일 수 있습니다. 이러한 단순 조건 중 하나 이상의 조건은 포스처 요건과 연결될 수 있는 복합 조건을 형성합니다.

네트워크에서 Cisco ISE를 처음 구축할 때 웹에서 포스처 업데이트를 다운로드할 수 있습니다. 이러한 프로세스를 초기 포스처 업데이트라고 합니다.

초기 포스처 업데이트가 완료되면 Cisco ISE는 Cisco에서 정의한 단순 및 복합 조건도 생성합니다. Cisco에서 정의한 단순 조건의 접두사는 pc_ as이고 복합 조건의 접두사는 pr_ as입니다.

동적 포스처 업데이트의 결과로 Cisco에서 정의한 조건을 정기적으로 다운로드하도록 Cisco ISE를 구성할 수도 있습니다. Cisco에서 정의한 포스처 조건은 삭제하거나 편집할 수 없습니다.

사용자 맞춤화 조건 또는 Cisco에서 정의한 조건에는 단순 조건과 복합 조건이 모두 포함됩니다.

단순 포스처 조건

Posture Navigation(포스처 탐색**)** 창을 사용하여 다음과 같은 단순 조건을 관리할 수 있습니다.

- 파일 조건 - 클라이언트에서 파일의 존재 여부, 파일 날짜 및 파일 버전을 확인하는 조건입니다.
- 레지스트리 조건 - 클라이언트에서 레지스트리 키의 존재 여부 또는 레지스트리 키 값을 확인하는 조건입니다.
- 애플리케이션 조건 - 애플리케이션 또는 프로세스가 클라이언트에서 실행 중인지 여부를 확인하는 조건입니다.

참고 프로세스가 설치되어 실행중인 경우 사용자는 규정을 준수하는 것입니다. 그러나 애플리케이션 조건은 역 논리에서 작동합니다. 애플리케이션이 설치되어 있지 않고 실행되지 않는 경우 최종 사용자가 불만을 제기합니다. 애플리케이션이 설치되어 실행중인 경우 최종 사용자는 불만을 제기하지 않습니다.

- 서비스 조건: 서비스가 클라이언트에서 실행되고 있는지 여부를 확인하는 조건입니다.

- 사전 조건: 특정 값을 사용하여 사전 속성을 확인하는 조건입니다.
- USB 조건: USB 대량 스토리지 디바이스가 있는지 여부를 확인하는 조건입니다.

단순 포스처 조건 생성

Posture Policies 또는 기타 복합 조건에서 사용할 수 있는 파일, 레지스트리, 애플리케이션, 서비스 및 사전 단순 조건을 생성할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)**를 선택합니다.

단계 **2** **File(**파일**)**, **Registry(**저장소**)**, **Application(**애플리케이션**)**, **Service(**서비스**)**, **Dictionary Simple Condition(**사전 단순 조건**)** 중에서 하나를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** 필드에 해당하는 값을 입력합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

복합 포스처 조건

복합 조건은 하나 이상의 단순 조건 또는 복합 조건으로 이루어집니다. 포스처 정책을 정의하면서 다음 복합 조건을 사용할 수 있습니다.

- 복합 조건: 하나 이상의 단순 조건, 또는 파일, 레지스트리, 애플리케이션 또는 서비스 조건 유형의 복합 조건을 포함합니다.
- 안티바이러스 복합 조건: 하나 이상의 AV 조건 또는 AV 복합 조건을 포함합니다.
- 안티스파이웨어 복합 조건: 하나 이상의 AS 조건 또는 AS 복합 조건을 포함합니다.
- 사전 복합 조건: 하나 이상의 사전 단순 조건 또는 사전 복합 조건을 포함합니다.
- 안티 멀웨어 조건: 하나 이상의 AM 조건을 포함합니다.

복합 포스처 조건 생성

Posture Assessment 및 검증을 위해 Posture Policies에서 사용할 수 있는 복합 조건을 생성할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **Compound Conditions(**복합 조건**)** > **Add(**추가**)**를 선택합니다.

단계 **2** 필드에 해당하는 값을 입력합니다.

단계 **3** 조건을 검증하려면 **Validate Expression(**식 검증**)**을 클릭합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

사전 복합 조건 설정

표 ***4:*** 사전 복합 조건 설정

필드 이름	사용 지침
Name(이름**)**	생성할 사전 복합 조건의 이름을 입력합니다.
Description(설명**)**	생성할 사전 복합 조건에 대한 설명을 입력합니다.
Select Existing Condition from Library(라이브러리에서 기존 조건 선택**)**	정책 요소 라이브러리에서 사전 정의된 조건을 선택하여 식을 정의하거나 후속 단계에서 임시 속성/값 쌍을 식에 추가할 수 있습니다.
Condition Name(조건 이름**)**	정책 요소 라이브러리에서 이미 생성한 사전 단순 조건을 선택합니다.
Expression(식**)**	Condition Name(조건 이름) 드롭다운 목록에서 선택한 항목에 따라 식이 업데이트됩니다.
AND or OR operator(AND 또는 **OR** 연산자**)**	라이브러리에서 추가할 수 있는 사전 단순 조건을 논리적으로 결합하려면 AND 또는 OR 연산자를 선택합니다. **Action(**작업**)** 아이콘을 클릭하여 다음을 수행합니다. • 속성/값 추가 • 라이브러리의 조건 추가 • 삭제
Create New Condition (Advance Option)(새 조건 생성**(**고급 옵션**))**	다양한 시스템 또는 사용자 맞춤화 사전에서 속성을 선택합니다. 후속 단계에서 정책 요소 라이브러리의 사전 정의된 조건을 추가할 수도 있습니다.
Condition Name(조건 이름**)**	이미 생성한 사전 단순 조건을 선택합니다.

필드 이름	사용 지침
Expression(식)	Expression(식) 드롭다운 목록에서 사전 단순 조건을 생성할 수 있습니다.
Operator(연산자)	값을 속성에 연결할 연산자를 선택합니다.
Value(값)	사전 속성과 연결할 값을 입력하거나 드롭다운 목록에서 값을 선택합니다.

관련 항목

복합 포스처 조건, 24 페이지
복합 포스처 조건 생성, 24 페이지

Windows 클라이언트에서 자동 업데이트를 사용할 수 있도록 사전 정의된 조건

pr_AutoUpdateCheck_Rule은 Cisco에서 미리 정의한 조건으로 Compound Conditions(복합 조건) 창으로 다운로드됩니다. 이 조건을 사용하면 Windows 클라이언트에서 자동 업데이트 기능이 활성화되었는지 확인할 수 있습니다. Windows 클라이언트가 이 요건을 충족하지 않으면 NAC(Network Access Control) Agent가 강제로 Windows 클라이언트에서 자동 업데이트 기능을 활성화(교정)합니다. 이 교정이 완료되고 나면 Windows 클라이언트는 포스처를 따르게 됩니다. Windows 클라이언트에서 자동 업데이트 기능이 활성화되지 않은 경우 포스처 정책에서 연결한 Windows 업데이트 교정이 Windows 관리자 설정을 재정의합니다.

미리 구성된 안티바이러스 및 안티스파이웨어 조건

Cisco ISE는 AV 및 AS 복합 조건 창에서 미리 구성된 안티바이러스 및 안티스파이웨어 복합 조건을 로드합니다. 이 조건은 Windows 및 Macintosh 운영체제용 안티바이러스 및 안티스파이웨어 지원 차트에 정의되어 있습니다. 이러한 복합 조건을 사용하면 모든 클라이언트에서 지정된 안티바이러스 및 안티스파이웨어 제품이 있는지 확인할 수 있습니다, Cisco ISE에서 새 안티바이러스 및 안티스파이웨어 복합 조건을 생성할 수도 있습니다.

안티바이러스 및 안티스파이웨어 지원 차트

Cisco ISE에서는 안티바이러스 및 안티스파이웨어 지원 차트를 사용하여 각 벤더 제품의 정의 파일에 최신 버전과 날짜를 제공합니다. 사용자는 안티바이러스 및 안티스파이웨어 지원 차트에 업데이트 정보가 있는지 자주 확인해야 합니다. 안티바이러스 및 안티스파이웨어 벤더는 안티바이러스 및 안티스파이웨어 정의 파일을 빈번하게 업데이트하므로 각 벤더 제품의 정의 파일에서 최신 버전과 날짜를 찾아보십시오.

안티바이러스 및 안티스파이웨어 지원 차트가 업데이트되어 새 안티바이러스 및 안티스파이웨어 벤더, 제품 및 해당 릴리스에 대한 지원을 반영할 때마다 NAC Agent는 새 안티바이러스 및 안티스파이웨어 라이브러리를 받게 됩니다. 이를 통해 NAC Agent는 새 버전을 지원할 수 있습니다. NAC Agent에서 이러한 지원 정보를 발견하면, 정기적으로 업데이트되는 se-checks.xml 파일(se-templates.tar.gz

압축 파일로 se-rules.xml 파일과 함께 게시됨)에서 최신 정의 정보를 확인하고 클라이언트가 포스처 정책을 따르는지 여부를 확인합니다. 특정 안티바이러스 또는 안티스파이웨어 제품의 안티바이러스 및 안티스파이웨어 라이브러리에서 지원하는 사항에 따라, 해당 요건이 NAC Agent로 전송되어 포스처 검증 과정에서 클라이언트에 그러한 요건이 있는지 검증하고 특정 안티바이러스 및 안티스파이웨어 제품의 상태를 확인합니다.

ISE Posture 에이전트에서 지원하는 안티바이러스 및 안티멀웨어 제품에 대한 자세한 내용은 Cisco AnyConnect ISE Posture 지원 차트: Cisco ISE 호환성 가이드를 참조하십시오.

안티멀웨어 포스처 조건을 생성하는 동안 최소 컴플라이언스 모듈 버전을 확인할 수 있습니다. 포스처 피드가 업데이트된 후 **Work Centers(**작업 센터**) > Posture(**포스처**) > Policy Elements(**정책 요소**) > Anti-Malware Condition(**안티멀웨어 조건**)**을 선택한 다음 **Operating System(**운영체제**)** 및 **Vendor(**벤더**)**를 선택하여 지원 차트를 확인합니다.

참고 일부 안티멀웨어 엔드포인트 보안 솔루션(예: FireEye, Cisco AMP, Sophos 등)이 작동하려면 해당 중앙 집중식 서비스에 대한 네트워크 액세스가 필요합니다. 이러한 제품의 경우 AnyConnect ISE Posture 모듈(또는 OESIS 라이브러리)에서 엔드포인트가 인터넷에 연결되어 있어야 합니다. 이러한 온라인 에이전트에 대해 사전 포스처(오프라인 탐지가 활성화되지 않은 경우) 동안 해당 엔드포인트가 인터넷에 액세스할 수 있도록 허용하는 것이 좋습니다. 이러한 경우 서명 정의 조건이 적용되지 않을 수 있습니다.

규정 준수 모듈

규정 준수 모듈에는 Cisco ISE 포스처 조건을 지원하는 OPSWAT에서 제공하는 벤더 이름, 제품 버전, 제품 이름, 속성 등의 필드 목록이 포함되어 있습니다.

벤더는 정의 파일의 제품 버전과 날짜를 빈번하게 업데이트하므로 규정 준수 모듈에서 업데이트를 자주 폴링하여 각 벤더 제품의 정의 파일에서 최신 버전 및 날짜를 확인해야 합니다. 새 벤더, 제품 및 해당 릴리스에 대한 지원을 반영하기 위해 규정 준수 모듈이 업데이트될 때마다 AnyConnect 에이전트는 새 라이브러리를 수신합니다. 이를 통해 AnyConnect 에이전트는 최신 추가 기능을 지원할 수 있습니다. AnyConnect 에이전트는 이 지원 정보를 검색하는 경우, 정기적으로 업데이트되는 se-checks.xml 파일(se-templates.tar.gz 압축 파일로 se-rules.xml 파일과 함께 게시됨)에서 최신 정의 정보를 확인하고 클라이언트가 보안 상태 정책을 준수하는지 여부를 확인합니다. 특정 안티바이러스, 안티스파이웨어, 악성코드 차단, 디스크 암호화 또는 패치 관리 제품용 라이브러리에서 지원하는 사항에 따라 적절한 요건이 AnyConnect 에이전트로 전송되어 보안 상태를 검증하는 동안 클라이언트에서 해당 요건의 유무와 특정 제품의 상태를 검증합니다.

규정 준수 모듈은 Cisco.com에서 이용 가능합니다.

아래 표에는 ISE 포스처 정책을 지원하는 및 지원하지 않는 OPSWAT API 버전이 나와 있습니다. 버전 3 및 4를 지원하는 에이전트별로 정책 규칙이 다릅니다.

표 ***5: OPSWAT API*** 버전

보안 상태 조건	규정 준수 모듈 버전
OPSWAT	
안티바이러스	3.x 이하
안티스파이웨어	3.x 이하
악성코드 차단	4.x 이상
디스크 암호화	3.x 이하 및 4.x 이상
패치 관리	3.x 이하 및 4.x 이상
USB	4.x 이상
OPSWAT 이외	
파일	모든 버전
애플리케이션	모든 버전
복합	모든 버전
레지스트리	모든 버전
서비스	모든 버전

참고

- 위의 버전 중 하나를 설치한 클라이언트가 있을 수 있으므로 버전 3.x 이하 및 버전 4.x 이상용으로 별도의 보안 상태 정책을 생성해야 합니다.
- OESIS 버전 4는 규정 준수 모듈 4.x 및 Cisco AnyConnect 4.3 이상에 대해 제공됩니다. 그러나 AnyConnect 4.3은 OESIS 버전 3 및 버전 4 정책을 모두 지원합니다.
- 버전 4 규정 준수 모듈은 ISE 2.1 이상에서 지원됩니다.

포스처 규정 준수 확인

단계 **1** Cisco ISE에 로그인하여 대시보드에 액세스합니다.

단계 **2** **Posture Compliance(**포스처 규정 준수**)** dashlet에서 커서로 스택 막대 또는 스파크라인을 가리킵니다.

도구 설명에 자세한 정보가 제공됩니다.

단계 **3** 자세한 내용을 확인하려면 데이터 범주를 확장합니다.

단계 **4** **Posture Compliance(**포스처 규정 준수**)** dashlet을 확장합니다.

자세한 실시간 보고서가 표시됩니다.

참고 **Context Visibility(**상황 가시성**)** 창에서 포스처 규정 준수 보고서를 볼 수 있습니다. **Context Visibility(**상황 가시성**) > Endpoints(**엔드포인트**) > Compliance(**규정 준수**)**로 이동합니다. 이 창에는 규정 준수 상태, 위치, 엔드포인트 및 범주별 애플리케이션에 따라 다른 차트가 표시됩니다.

활성 세션이 없는 엔드포인트에 대한 포스처 상태가 표시될 수 있습니다. 예를 들어 엔드포인트에 대해 마지막으로 확인된 포스처 상태가 **Compliant(**규정 준수**)**인 경우 엔드포인트 세션이 종료된 경우에도 엔드포인트에 대한 다음 업데이트가 수신될 때까지 **Context Visibility(**상황 가시성**)** 창에 상태가 **Compliant(**규정 준수**)**로 유지됩니다. 엔드포인트가 삭제되거나 제거될 때까지 포스처 상태가 **Context Visibility(**상황 가시성**)** 창에 유지됩니다.

패치 관리 조건 생성

선택한 벤더의 패치 관리 제품 상태를 확인하는 정책을 생성할 수 있습니다.

예를 들어 Microsoft SCCM(System Center Configuration Manager) 클라이언트 버전 4.x 소프트웨어 제품이 엔드포인트에 설치되어 있는지를 확인하는 조건을 생성할 수 있습니다.

참고 Cisco ISE 및 AnyConnect의 지원되는 버전은 다음과 같습니다.

- Cisco ISE 버전 1.4 이상
- AnyConnect 버전 4.1 이상

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **Patch Management Condition(**패치 관리 조건**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 및 **Description(**설명**)** 필드에 조건 이름과 설명을 입력합니다.

단계 **4** **Operating System(**운영체제**)** 드롭 다운 필드에서 적절한 운영체제를 선택합니다.

단계 **5** 드롭다운 목록에서 **Compliance Module(**컴플라이언스 모듈**)**을 선택합니다.

단계 **6** 드롭다운 목록에서 **Vendor Name(**벤더 이름**)**을 선택합니다.

단계 **7** **Check Type(**확인 유형**)**을 선택합니다.

단계 **8** **Check patches installed(**패치 설치 확인**)** 드롭 다운 목록에서 적절한 패치를 선택합니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

관련 항목

패치 관리 조건 설정, 51 페이지
패치 관리 교정 추가, 70 페이지

디스크 암호화 조건 생성

엔드포인트가 지정된 데이터 암호화 소프트웨어의 규정을 준수하는지를 확인하는 정책을 생성할 수 있습니다.

예를 들어 C: 드라이브가 엔드포인트에서 암호화되는지를 확인하는 조건을 생성할 수 있습니다. C: 드라이브가 암호화되지 않으면 엔드포인트는 규정 미준수 알림을 수신하며 ISE는 메시지를 기록합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다. AnyConnect ISE 포스처 에이전트를 사용할 때만 디스크 암호화 조건을 포스처 요건과 연결할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처 > **Disk Encryption Condition(**디스크 암호화 조건**)**

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Disk Encryption Condition(**디스크 암호화 조건**)** 창에서 필드에 해당하는 값을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

포스처 조건 설정

이 섹션에서는 포스처에 사용되는 단순 및 복합 조건에 대해 설명합니다.

파일 조건 설정

다음 표에서는 File Conditions(파일 조건) 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **File Condition(**파일 조건**)**입니다.

표 ***6:*** 파일 조건 설정

필드 이름	**Windows OS**의 사용 지침	**Mac OSX**의 사용 지침
Name(이름**)**	파일 조건의 이름을 입력합니다.	파일 조건의 이름을 입력합니다.

필드 이름	**Windows OS**의 사용 지침	**Mac OSX**의 사용 지침
Description(설명**)**	파일 조건에 대한 설명을 입력합니다.	파일 조건에 대한 설명을 입력합니다.
Operating System(운영체제**)**	파일 조건을 적용해야 하는 Windows 운영체제를 선택합니다.	파일 조건을 적용해야 하는 Mac OSX를 선택합니다.
File Type(파일 유형**)**	미리 정의된 설정 중 하나를 선택합니다. • **FileDate**: 특정 파일 생성 또는 파일 수정 날짜의 파일이 시스템에 있는지 여부를 확인합니다. • **FileExistence**: 파일이 시스템에 있는지 여부를 확인합니다. • **FileVersion**: 특정 파일 버전이 시스템에 있는지 여부를 확인합니다. • **CRC32**: 체크섬 기능을 사용하여 파일의 데이터 무결성을 확인합니다. • **SHA-256**: 해시 기능을 사용하여 파일의 데이터 무결성을 확인합니다.	미리 정의된 설정 중 하나를 선택합니다. • **FileDate**: 특정 파일 생성 또는 파일 수정 날짜의 파일이 시스템에 있는지 여부를 확인합니다. • **FileExistence**: 파일이 시스템에 있는지 여부를 확인합니다. • **CRC32**: 체크섬 기능을 사용하여 파일의 데이터 무결성을 확인합니다. • **SHA-256**: 해시 기능을 사용하여 파일의 데이터 무결성을 확인합니다. • **PropertyList**: loginwindow.plist와 같은 plist 파일의 속성 값을 확인합니다.

필드 이름	**Windows OS**의 사용 지침	**Mac OSX**의 사용 지침
Data Type & Operator(데이터 유형 및 연산자**)**	해당 없음	(File Type(파일 유형)으로 **PropertyList**를 선택하는 경우에만 사용 가능함) plist 파일에서 검색할 키의 값이나 데이터 유형을 선택합니다. 각 데이터 유형에는 연산자 집합이 포함되어 있습니다. • **Unspecified(**지정되지 않음**)**: 지정한 키의 유무를 확인합니다. 연산자(Exists, DoesNotExist)를 입력합니다. • **Number(**숫자**)**: 숫자 데이터 유형의 지정된 키를 확인합니다. 연산자(같음, 같지 않음, 큼, 작음, 크거나 같음, 작거나 같음)와 값을 입력합니다. • **String(**문자열**)**: 문자열 데이터 유형의 지정된 키를 확인합니다. 연산자(같음, 같지 않음, 같음(대소문자 무시), 다음으로 시작, 다음으로 시작 안 함, 포함, 포함 안 함, 다음으로 끝남, 다음으로 끝나지 않음)와 값을 입력합니다. • **Version(**버전**)**: 버전 문자열로 지정된 키의 값을 확인합니다. 연산자(이전, 이후, 같음)와 값을 입력합니다.
속성 이름	해당 없음	(File Type(파일 유형)으로 **PropertyList**를 선택하는 경우에만 사용 가능함) BuildVersionStampAsNumber와 같은 키의 이름을 입력합니다.

필드 이름	**Windows OS**의 사용 지침	**Mac OSX**의 사용 지침
File Path(파일 경로**)**	미리 정의된 설정 중 하나를 선택합니다. • **ABSOLUTE_PATH**: 파일의 인증된 경로에서 파일을 확인합니다. 예를 들면 C:\<directory>\file name과 같습니다. 기타 설정의 경우에는 파일 이름만 입력합니다. • **SYSTEM_32**: C:\WINDOWS\system32 디렉토리에서 파일을 확인합니다. 파일 이름을 입력합니다. • **SYSTEM_DRIVE**: C:\ 드라이브에서 파일을 확인합니다. 파일 이름을 입력합니다. • **SYSTEM_PROGRAMS**: C:\Program Files에서 파일을 확인합니다. 파일 이름을 입력합니다. • **SYSTEM_ROOT**: Windows 시스템의 루트 경로에서 파일을 확인합니다. 파일 이름을 입력합니다. • **USER_DESKTOP**: Windows 사용자의 데스크톱에 지정한 파일이 있는지를 확인합니다. 파일 이름을 입력합니다. • **USER_PROFILE**: Windows 사용자의 로컬 프로파일 디렉토리에 파일이 있는지를 확인합니다. 파일 경로를 입력합니다.	미리 정의된 설정 중 하나를 선택합니다. • **Root**: 루트(/) 디렉토리에서 파일을 확인합니다. 파일 경로를 입력합니다. • **Home**: 홈(~) 디렉토리에서 파일을 확인합니다. 파일 경로를 입력합니다.
File Date Type(파일 날짜 유형**)**	(File Type(파일 유형)으로 **FileDate**를 선택하는 경우에만 사용 가능함) **Creation Date(**생성 날짜**)** 또는 **Modification Date(**수정 날짜**)**를 선택합니다.	(File Type(파일 유형)으로 **FileDate**를 선택하는 경우에만 사용 가능함) **Creation Date(**생성 날짜**)** 또는 **Modification Date(**수정 날짜**)**를 선택합니다.

필드 이름	**Windows OS**의 사용 지침	**Mac OSX**의 사용 지침
File Operator(파일 연산자**)**	File Operator(파일 운영자) 옵션은 File Type(파일 유형)에서 선택하는 설정에 따라 달라집니다. 다음 설정 중에서 적절하게 선택합니다. FileDate • EarlierThan • LaterThan • EqualTo • Within: 지난 *n*일을 지정합니다. 유효한 값의 범위는 0~300일입니다. FileExistence • Exists • DoesNotExist FileVersion • EarlierThan • LaterThan • EqualTo	File Operator(파일 운영자) 옵션은 File Type(파일 유형)에서 선택하는 설정에 따라 달라집니다. 다음 설정 중에서 적절하게 선택합니다. FileDate • EarlierThan • LaterThan • EqualTo • Within: 지난 *n*일을 지정합니다. 유효한 값의 범위는 0~300일입니다. FileExistence • Exists • DoesNotExist
File CRC Data(파일 **CRC** 데이터**)**	(File Type(파일 유형)으로 **CRC32**를 선택하는 경우에만 사용 가능함) 파일 무결성을 확인하기 위해 0x3c37fec3과 같은 체크섬 값을 입력할 수 있습니다. 체크섬 값은 16진수 정수인 0x로 시작해야 합니다.	(File Type(파일 유형)으로 **CRC32**를 선택하는 경우에만 사용 가능함) 파일 무결성을 확인하기 위해 0x3c37fec3과 같은 체크섬 값을 입력할 수 있습니다. 체크섬 값은 16진수 정수인 0x로 시작해야 합니다.
File SHA-256 Data(파일 **SHA-256** 데이터**)**	(File Type(파일 유형)으로 **SHA-256**을 선택하는 경우에만 사용 가능함) 파일 무결성을 확인하기 위해 64바이트 16진수 해시 값을 입력할 수 있습니다.	(File Type(파일 유형)으로 **SHA-256**을 선택하는 경우에만 사용 가능함) 파일 무결성을 확인하기 위해 64바이트 16진수 해시 값을 입력할 수 있습니다.

필드 이름	**Windows OS**의 사용 지침	**Mac OSX**의 사용 지침
날짜 및 시간	(File Type(파일 유형)으로 **FileDate**를 선택하는 경우에만 사용 가능함) 클라이언트 시스템의 날짜와 시간을 mm/dd/yyyy 및 hh:mm 형식으로 입력합니다.	(File Type(파일 유형)으로 **FileDate**를 선택하는 경우에만 사용 가능함) 클라이언트 시스템의 날짜와 시간을 mm/dd/yyyy 및 hh:mm 형식으로 입력합니다.

관련 항목

단순 포스처 조건, 23 페이지
복합 포스처 조건, 24 페이지
포스처 조건 생성, 81 페이지

방화벽 조건 설정

방화벽 조건은 특정 방화벽 제품이 엔드포인트에서 실행 중인지 확인합니다. 지원되는 방화벽 제품 목록은 OPSWAT 지원 차트를 기반으로 합니다. 초기 포스처 및 PRA(주기적 재평가) 중에 정책을 시행할 수 있습니다.

Cisco ISE는 Windows 및 Mac OS에 대한 기본 방화벽 조건을 제공합니다. 이러한 조건은 기본적으로 비활성화되어 있습니다.

필드 이름	사용 지침
Name(이름**)**	방화벽 조건의 이름을 입력합니다.
Description(설명**)**	방화벽 조건에 대한 설명을 입력합니다.
규정 준수 모듈**(Compliance Module)**	필요한 규정 준수 모듈을 선택합니다. • 4.x 이상 • 3.x 이상 • 모든 버전
Operating System(운영체제**)**	필수 방화벽 제품이 엔드포인트에 설치되어 있는지 확인합니다. Windows OS 또는 Mac OSX를 선택할 수 있습니다.
벤더	드롭다운 목록에서 벤더 이름을 선택합니다. 벤더의 방화벽 제품과 확인 유형이 검색되어 **Products for Selected Vendor(**선택한 벤더의 제품**)** 표에 표시됩니다. 표의 목록은 선택한 운영체제에 따라 변경됩니다.

필드 이름	사용 지침
Check Type(확인 유형**)**	Enabled(활성화됨): 특정 방화벽이 엔드포인트에서 실행 중인지 확인합니다. **Products for Selected Vendor(**선택한 벤더의 제품**)** 목록을 참조하여 벤더의 제품이 선택한 확인 유형을 지원하는지를 확인합니다.

레지스트리 조건 설정

다음 표에서는 Registry Conditions(레지스트리 조건) 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **Registry Condition(**레지스트리 조건**)**입니다.

표 *7:* 레지스트리 조건 설정

필드 이름	사용 지침
Name(이름**)**	레지스트리 조건의 이름을 입력합니다.
Description(설명**)**	레지스트리 조건에 대한 설명을 입력합니다.
Registry Type(레지스트리 유형**)**	미리 정의된 설정 중 하나를 레지스트리 유형으로 선택합니다.
Registry Root Key(레지스트리 루트 키**)**	미리 정의된 설정 중 하나를 레지스트리 루트 키로 선택합니다.
Sub Key(하위 키**)**	레지스트리 루트 키에 지정된 경로에서 레지스트리 키를 확인하기 위한 하위 키를 백슬래시("\") 없이 입력합니다. 예를 들어 SOFTWARE\Symantec\Norton AntiVirus\version을 입력하면 다음 경로에서 키를 확인합니다. HKLM\SOFTWARE\Symantec\NortonAntiVirus\version
Value Name(값 이름**)**	(레지스트리 유형으로 **RegistryValue** 또는 **RegistryValueDefault**를 선택하는 경우에만 사용 가능함) **RegistryValue**에 대해 확인할 레지스트리 키 값의 이름을 입력합니다. 이 항목은 **RegistryValueDefault**의 기본 필드입니다.

필드 이름	사용 지침
Value Data Type(값 데이터 유형**)**	(레지스트리 유형으로 **RegistryValue** 또는 **RegistryValueDefault**를 선택하는 경우에만 사용 가능함) 다음 설정 중 하나를 선택합니다. • **Unspecified(**지정되지 않음**)**: 레지스트리 키 값의 유무를 확인합니다. 이 옵션은 **RegistryValue**에 대해서만 사용 가능합니다. • **Number(**번호**)**: 레지스트리 키 값에 지정된 번호를 확인합니다. • **String(**문자열**)**: 레지스트리 키 값의 문자열을 확인합니다. • **Version(**버전**)**: 레지스트리 키 값의 버전을 확인합니다.
Value Operator(값 연산자**)**	설정을 적절하게 선택합니다.
Value Data(값 데이터**)**	(레지스트리 유형으로 **RegistryValue** 또는 **RegistryValueDefault**를 선택하는 경우에만 사용 가능함) **Value Data Type(**값 데이터 유형**)**에서 선택한 데이터 유형에 따라 레지스트리 키의 값을 입력합니다.
Operating System(운영체제**)**	레지스트리 조건을 적용해야 하는 운영체제를 선택합니다.

관련 항목

단순 포스처 조건, 23 페이지
복합 포스처 조건, 24 페이지

지속적인 엔드포인트 속성 모니터링

Cisco AnyConnect 에이전트를 사용하여 다양한 엔드포인트 속성을 지속적으로 모니터링하여 상태 평가 중에 동적 변경 사항이 관찰되는지 확인할 수 있습니다. 이렇게 하면 엔드포인트의 전반적인 가시성이 향상되고 그 동작을 기반으로 포스처 정책을 생성할 수 있습니다. Cisco AnyConnect 에이전트는 엔드포인트에 설치되어 실행중인 애플리케이션을 모니터링합니다. 기능을 켜고 끄고 데이터를 모니터링할 빈도를 구성할 수 있습니다. 기본적으로 데이터는 5분마다 수집되며 데이터베이스에 저장됩니다. 초기 포스처 중에 Cisco AnyConnect는 실행중인 애플리케이션과 설치된 애플리케이션의 전체 목록을 보고합니다. 초기 상태가 유지되면 Cisco AnyConnect 에이전트는 X분마다 애플리케이션을 검사하고 마지막 검사에서 서버로 차이를 전송합니다. 서버는 실행 중인 애플리케이션과 설치된 애플리케이션의 전체 목록을 표시합니다.

애플리케이션 조건 설정

애플리케이션 조건은 엔드포인트에 설치된 애플리케이션을 쿼리합니다. 이를 통해 엔드포인트에 분산된 소프트웨어를 종합적으로 파악할 수 있습니다. 예를 들어 정보에 근거하여 정책을 생성하고 데스크톱 팀과 함께 소프트웨어 라이선스를 줄일 수 있습니다.

다음 표에서는 **Application Conditions(**애플리케이션 조건**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Posture(**포스처**)** > **Policy Elements(**정책 요소**)** > **Application Condition(**애플리케이션 조건**)** > **Add(**추가**)**입니다.

필드 이름	사용 지침
Name(이름**)**	애플리케이션 조건의 이름을 입력합니다.
Description(설명**)**	애플리케이션 조건에 대한 설명을 입력합니다.
Operating System(운영체제**)**	애플리케이션 조건을 적용해야 하는 Windows OS 또는 MAC OSX를 선택합니다.
규정 준수 모듈**(Compliance Module)**	다음 옵션 중 하나를 선택합니다. • **4.x** 이상 • **3.x** 이하 • 모든 버전
확인 기준	다음 옵션 중 하나를 선택합니다. • **Process(**프로세스**)**: 프로세스가 엔드포인트에서 실행 중인지 확인하려면 이 옵션을 선택합니다. • **Application(**애플리케이션**)**: 엔드포인트에서 애플리케이션이 실행 중인지 확인하려면 이 옵션을 선택합니다.
Process Name(프로세스 이름**)**	(**Check By(**확인 기준**)** 옵션으로 **Process(**프로세스**)**를 선택한 경우에만 사용 가능) 필요한 프로세스 이름을 입력합니다.

필드 이름	사용 지침
Application Operator(애플리케이션 운영자**)**	(**Check By(**확인 기준**)** 옵션으로 **Process (**프로세스**)**를 선택한 경우에만 사용 가능) 다음 옵션 중 하나를 선택합니다. • **Running(**실행 중**)**: 애플리케이션이 엔드포인트에서 실행 중인지 확인하려면 이 옵션을 선택합니다. • **Not Running(**실행 중 아님**)**: 애플리케이션이 엔드포인트에서 실행되고 있지 않은지 확인하려면 이 옵션을 선택합니다.
애플리케이션 상태	(**Check By(**확인 기준**)** 옵션으로 **Application(**애플리케이션**)**을 선택한 경우에만 사용 가능) 다음 옵션 중 하나를 선택합니다. • **Installed(**설치됨**)**: 클라이언트에 악성 애플리케이션이 설치되어 있는지 확인하려면 이 옵션을 선택합니다. 악성 애플리케이션이 발견되면 교정 작업이 트리거됩니다. • **Running(**실행 중**)**: 애플리케이션이 엔드포인트에서 실행 중인지 확인하려면 이 옵션을 선택합니다.
프로비저닝 기준	(**Check By(**확인 기준**)** 옵션으로 **Application(**애플리케이션**)**을 선택한 경우에만 사용 가능) 다음 옵션 중 하나를 선택합니다. • **Everything(**모두**)**: 브라우저, 패치 관리 등 나열된 모든 범주를 선택할 수 있습니다. • **Name(**이름**)**: 하나 이상의 범주를 선택해야합니다. 예를 들어 **Browser(**브라우저**)** 범주를 선택하면 **Vendor(**벤더**)** 드롭다운 목록에 해당 벤더가 표시됩니다. • **Category(**범주**)**: 안티멀웨어, 백업, 브라우저 또는 데이터 스토리지와 같은 하나 이상의 범주를 확인할 수 있습니다. 참고 범주는 OPSWAT 라이브러리에서 동적으로 업데이트됩니다.

Context Visibility(상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Compliance(**규정 준수**)** 창에서 각 엔드포인트에 대해 설치되어 실행중인 애플리케이션의 수를 볼 수 있습니다.

Home(홈**)** > **Summary(**요약**)** > **Compliance(**규정 준수**)** 창에는 포스처 평가가 적용되고 규정을 준수하는 엔드포인트의 백분율이 표시됩니다.

서비스 조건 설정

다음 표에서는 **Service Conditions(**서비스 조건**)** 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **Service Condition(**서비스 조건**)**입니다.

표 ***8:*** 서비스 조건 설정

필드 이름	사용 지침
Name(이름**)**	서비스 조건의 이름을 입력합니다.
Description(설명**)**	서비스 조건에 대한 설명을 입력합니다.
Operating Systems(운영체제**)**	서비스 조건을 적용해야 하는 운영체제를 선택합니다. 다양한 Windows OS 또는 Mac OSX 버전을 선택할 수 있습니다.
Service Name(서비스 이름**)**	루트로 실행되는 데몬 또는 사용자 에이전트 서비스의 이름(예: com.apple.geod)을 입력합니다. AnyConnect 에이전트는 **sudo launchctl list** 명령을 사용하여 서비스 조건을 검증합니다.
Service Type(서비스 유형**)**	클라이언트가 규정을 준수하는지를 확인하기 위해 AnyConnect가 확인해야 하는 서비스의 유형을 선택합니다. • **Daemon(**데몬**)**: 클라이언트 디바이스에서 악성코드를 스캔하는 등의 지정된 서비스가 클라이언트 내 데몬 서비스의 지정된 목록에 있는지를 확인합니다. • **User Agent(**사용자 에이전트**)**: 악성코드가 탐지되면 실행되는 서비스 등의 지정된 서비스가 클라이언트 내 사용자 서비스의 지정된 목록에 있는지를 확인합니다. • **Daemon or User Agent(**데몬 또는 사용자 에이전트**)**: 지정된 서비스가 데몬 또는 사용자 에이전트 서비스 목록에 있는지를 확인합니다.

필드 이름	사용 지침
Service Operator(서비스 운영자**)**	클라이언트에서 확인할 서비스 상태를 선택합니다. • **Windows OS**: 서비스가 **Running(**실행 중**)** 상태인지 아니면 **Not Running(**실행 중이 아님**)** 상태인지를 확인합니다. • **Mac OSX**: 서비스가 **Loaded(**로드됨**)**, **Not Loaded(**로드되지 않음**)**, **Loaded and Running(**로드되어 실행 중**)**, **Loaded with Exit Code(**로드되었으며 종료 코드 생성됨**)**, **Loaded and running or with Exit code(**로드되어 실행 중 또는 종료 코드 생성됨**)** 상태인지를 확인합니다.

관련 항목

단순 포스처 조건, 23 페이지
복합 포스처 조건, 24 페이지

포스처 복합 조건 설정

다음 표에서는 **Compound Conditions(**복합 조건**)** 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **Compounde Condition(**복합 조건**)**입니다.

표 ***9:*** 포스처 복합 조건 설정

필드 이름	사용 지침
Name(이름**)**	생성할 복합 조건의 이름을 입력합니다.
Description(설명**)**	생성할 복합 조건의 설명을 입력합니다.
Operating System(운영체제**)**	하나 이상의 Windows 운영체제를 선택합니다. 그러면 조건이 적용되는 Windows 운영체제를 연결할 수 있습니다.
Parentheses ( )(괄호( ))**	괄호를 클릭하면 단순 조건 유형(파일, 레지스트리, 애플리케이션 및 서비스 조건)에서 단순 조건 두 개를 결합할 수 있습니다.
(&): AND operator((&): AND 연산자)(AND 연산자로는 따옴표 없이 "&" 사용)	복합 조건에서 AND 연산자(앰퍼샌드[&])를 사용할 수 있습니다. 예를 들어 **Condition1 & Condition2**와 같이 입력할 수 있습니다.

필드 이름	사용 지침
(|): OR operator((|): OR 연산자(OR 연산자로는 따옴표 없이 "|" 사용))	복합 조건에서 OR 연산자(가로 막대[|])를 사용할 수 있습니다. 예를 들어 **Condition1 & Condition2**와 같이 입력할 수 있습니다.
(!): NOT operator((!): NOT 연산자)(NOT 연산자로는 따옴표 없이 "!" 사용)	복합 조건에서 NOT 연산자(느낌표[!])를 사용할 수 있습니다. 예를 들어 **Condition1 & Condition2**와 같이 입력할 수 있습니다.
Simple Conditions(단순 조건**)**	단순 조건 목록에서 파일, 레지스트리, 애플리케이션 및 서비스 조건 유형의 조건을 선택합니다. 개체 선택기에서 단순 조건인 파일, 레지스트리, 애플리케이션 및 서비스 조건을 생성할 수도 있습니다. **Action(**작업**)** 버튼의 빠른 선택기(아래쪽 화살표)를 클릭하여 단순 조건인 파일, 레지스트리, 애플리케이션 및 서비스 조건을 생성합니다.

관련 항목

포스처 조건, 23 페이지
복합 포스처 조건 생성, 24 페이지

안티바이러스 조건 설정

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **Anti-Virus Condition(**안티바이러스 조건**)**.

필드 이름	사용 지침
Name(이름**)**	생성할 안티바이러스 복합 조건의 이름을 입력합니다.
Description(설명**)**	생성할 안티바이러스 조건에 대한 설명을 입력합니다.
Operating System(운영체제**)**	운영체제를 선택하면 클라이언트에서 안티바이러스 프로그램의 설치를 확인하거나 조건이 적용된 최신 안티바이러스 정의 파일 업데이트를 확인할 수 있습니다.
Vendor(벤더**)**	드롭다운 목록에서 벤더를 선택합니다. Vendor(벤더)를 선택하면 해당 안티바이러스 제품 및 버전이 검색되어 선택한 벤더의 제품 표에 표시됩니다.

필드 이름	사용 지침
Check Type(확인 유형**)**	클라이언트에서 설치를 확인할지, 아니면 최신 정의 파일 업데이트를 확인할지 선택합니다.
Installation(설치**)**	클라이언트에서 안티바이러스 프로그램의 설치만 확인하려면 이 필드를 선택합니다.
Definition(정의**)**	클라이언트에서 안티바이러스 제품의 최신 정의 파일 업데이트만 확인하려면 이 필드를 선택합니다.

Products for Selected Vendor(선택한 벤더의 제품**)**

표에서 안티바이러스 제품을 선택합니다. 새 안티바이러스 조건 페이지에서 선택한 벤더에 따라 안티바이러스 제품 및 버전, 제공하는 교정 지원, 최신 정의 파일 날짜 및 버전에 대한 정보가 표에 표시됩니다.

표에서 제품을 선택하면 안티바이러스 프로그램의 설치를 확인하거나 최신 안티바이러스 정의 파일 날짜 및 최신 버전을 확인할 수 있습니다.

참고 **Baseline Condition(**베이스라인 조건**)** 또는 **Advance Condition(**고급 조건**)**에서 각 안티바이러스 제품에 대해 하나의 조건만 구성할 수 있습니다.

베이스라인 조건

필드 이름	지침
Minimum Version(최소 버전**)**	(운영체제 및 벤더를 업데이트할 때만 사용 가능) 드롭다운 목록에서 안티바이러스의 최소 버전을 선택합니다. 확인을 수행할 때 네트워크의 모든 엔드포인트에서 네트워크 정책은 이 최소 안티바이러스 버전을 준수해야 합니다.
Maximum Version(최대 버전**)**	포스처 피드를 업데이트할 때 안티바이러스의 최대 버전이 자동으로 수정됩니다.
최소 규정 준수 모듈 버전**(Minimum Compliance Module Version)**	최소 규정 준수 모듈 버전은 AnyConnect에서 업데이트됩니다.

고급 조건**(Advance Condition)**

필드 이름	지침
Check against latest AV definition file version, if available(가능한 경우 최신 **AV** 정의 파일 버전을 기준으로 확인**)**	(정의 확인 유형을 선택한 경우에만 사용 가능) Cisco ISE에서 포스처 업데이트의 결과로 사용 가능한 경우 최신 안티바이러스 정의 파일 버전과 비교하여 클라이언트의 안티바이러스 정의 파일 버전을 확인하려면 이 필드를 선택합니다. 그렇지 않은 경우 이 옵션을 사용하면 Cisco ISE에서 최신 정의 파일 날짜를 기준으로 클라이언트의 정의 파일 날짜를 확인할 수 있습니다.
Allow virus definition file to be(바이러스 정의 파일을 활성화하도록 허용**)(**활성화**)**	(정의 확인 유형을 선택한 경우에만 사용 가능) 클라이언트에서 안티바이러스 정의 파일 버전 및 최신 안티바이러스 정의 파일 날짜를 확인하려면 이 필드를 선택합니다. 최신 정의 파일 날짜는 제품의 최신 안티바이러스 정의 파일 날짜 또는 현재 시스템 날짜를 기준으로 다음 필드(days older than(다음보다 오래됨(일) 필드)에 정의한 날짜보다 이전일 수 없습니다. 선택하지 않는 경우 Cisco ISE는 Check against latest AV definition file version, if available(가능한 경우 최신 AV 정의 파일 버전을 기준으로 확인) 옵션을 사용하여 안티스파이웨어 정의 파일의 버전만 확인할 수 있습니다.
Days Older Than(다음보다 오래됨**(**일**))**	클라이언트의 최신 안티바이러스 정의 파일 날짜가 제품의 최신 안티바이러스 정의 파일 날짜 또는 현재 시스템 날짜를 기준으로 얼마나 더 이전 날짜(일)가 될 수 있는지 정의합니다. 기본값은 영(0)입니다.
Latest File Date(최신 파일 날짜**)**	클라이언트의 안티바이러스 정의 파일 날짜를 확인하려면 선택합니다. 이 날짜는 days older than(다음보다 오래됨(일)) 필드에 정의한 기간(일)만큼 이전 날짜일 수 있습니다. 기간(일)을 기본값(0)으로 설정하는 경우 클라이언트의 안티바이러스 정의 파일 날짜는 제품의 최신 안티바이러스 정의 파일 날짜 이전일 수 없습니다.

필드 이름	지침
Current System Date(현재 시스템 날짜**)**	클라이언트의 안티바이러스 정의 파일 날짜를 확인하려면 선택합니다. 이 날짜는 days older than(다음보다 오래됨(일)) 필드에 정의한 기간(일)만큼 이전 날짜일 수 있습니다. 기간(일)을 기본값(0)으로 설정하는 경우 클라이언트의 안티바이러스 정의 파일 날짜는 현재 시스템 날짜 이전일 수 없습니다.

관련 항목

복합 포스처 조건, 24 페이지
미리 구성된 안티바이러스 및 안티스파이웨어 조건, 26 페이지
안티바이러스 및 안티스파이웨어 지원 차트, 26 페이지

안티스파이웨어 복합 조건 설정

다음 표에서는 **AS Compound Conditions(AS** 복합 조건**)** 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **AS Compounde Condition(**복합 조건**)**입니다.

표 ***10:*** 안티스파이웨어 복합 조건 설정

필드 이름	사용 지침
Name(이름**)**	생성할 안티스파이웨어 복합 조건의 이름을 입력합니다.
Description(설명**)**	생성할 안티스파이웨어 복합 조건에 대한 설명을 입력합니다.
Operating System(운영체제**)**	운영체제를 선택하면 클라이언트에서 안티스파이웨어 프로그램의 설치를 확인하거나 조건이 적용된 최신 안티스파이웨어 정의 파일 업데이트를 확인할 수 있습니다.
Vendor(벤더**)**	드롭다운 목록에서 벤더를 선택합니다. Vendor(벤더)를 선택하면 해당 안티스파이웨어 제품 및 버전이 검색되어 선택한 벤더의 제품 표에 표시됩니다.
Check Type(확인 유형**)**	클라이언트에서 설치를 확인할지, 아니면 최신 정의 파일 업데이트를 확인할지 유형을 선택하려면 이 필드를 선택합니다.

필드 이름	사용 지침
Installation(설치**)**	클라이언트에서 안티스파이웨어 프로그램의 설치만 확인하려면 이 필드를 선택합니다.
Definition(정의**)**	클라이언트에서 안티스파이웨어 제품의 최신 정의 파일 업데이트만 확인하려면 이 필드를 선택합니다.
Allow Virus Definition File to be(바이러스 정의 파일을 활성화하도록 허용**)(**활성화**)**	안티스파이웨어 정의 확인 유형을 생성하는 경우 이 확인란을 선택하고, 안티스파이웨어 설치 확인 유형을 생성하는 경우에는 비활성화합니다. 선택하는 경우 클라이언트에서 안티스파이웨어 정의 파일 버전 및 최신 안티스파이웨어 정의 파일 날짜를 확인할 수 있습니다. 최신 정의 파일 날짜는 현재 시스템 날짜를 기준으로 days older than(다음보다 오래됨(일)) 필드에 정의한 날짜보다 이전일 수 없습니다. 선택하지 않는 경우, Allow virus definition file to be(바이러스 정의 파일 허용) 확인란을 선택하지 않았으므로 안티스파이웨어 정의 파일의 버전만 확인할 수 있습니다.
days older than(다음보다 오래됨**(**일**))**	클라이언트의 최신 안티스파이웨어 정의 파일 날짜가 현재 시스템 날짜를 기준으로 얼마나 더 이전 날짜(일)가 될 수 있는지 정의합니다. 기본값은 영(0)입니다.
Current System Date(현재 시스템 날짜**)**	클라이언트의 안티스파이웨어 정의 파일 날짜를 확인하려면 선택합니다. 이 날짜는 days older than(다음보다 오래됨(일)) 필드에 정의한 기간(일)만큼 이전 날짜일 수 있습니다. 기간(일)을 기본값(0)으로 설정하는 경우 클라이언트의 안티스파이웨어 정의 파일 날짜는 현재 시스템 날짜 이전일 수 없습니다.
Products for Selected Vendor(선택한 벤더의 제품**)**	표에서 안티스파이웨어 제품을 선택합니다. 새 안티스파이웨어 복합 조건 페이지에서 선택한 벤더에 따라 안티스파이웨어 제품 및 버전, 제공하는 교정 지원, 최신 정의 파일 날짜 및 버전에 대한 정보가 표에 표시됩니다. 표에서 제품을 선택하면 안티스파이웨어 프로그램의 설치를 확인하거나 최신 안티스파이웨어 정의 파일 날짜 및 최신 버전을 확인할 수 있습니다.

관련 항목

복합 포스처 조건, 24 페이지
미리 구성된 안티바이러스 및 안티스파이웨어 조건, 26 페이지
안티바이러스 및 안티스파이웨어 지원 차트, 26 페이지

안티 멀웨어 조건 설정

안티스파이웨어 및 안티바이러스 조건의 조합인 안티 멀웨어 조건은 OESIS 버전 4.x 이상 규정 준수 모듈에 의해 지원됩니다.

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **Antimalware Condition(**안티멀웨어 조건**)**.

참고 설치된 안티멀웨어 제품을 최소한 한 번은 수동으로 업데이트하여 최신 정의를 받는 것이 좋습니다. 그러지 않으면 AnyConnect를 사용하여 안티멀웨어 정의에 대해 포스처를 확인할 때 실패할 수 있습니다.

필드 이름	사용 지침
Name(이름**)**	안티 멀웨어 조건의 이름을 입력합니다.
Description(설명**)**	안티 멀웨어 조건에 대한 설명을 입력합니다.
Operating System(운영체제**)**	운영체제를 선택하면 클라이언트에서 안티 멀웨어 프로그램의 설치를 확인하거나 조건이 적용된 최신 안티 멀웨어 정의 파일 업데이트를 확인할 수 있습니다. MAC 및 Windows OS를 모두 지원합니다
Vendor(벤더**)**	드롭다운 목록에서 벤더를 선택합니다. 선택한 벤더의 안티 멀웨어 제품, 버전, 최신 정의 날짜, 최신 정의 버전 및 최소 규정 준수 모듈 버전이 **Products for Selected Vendor(**선택한 벤더의 제품**)** 표에 표시됩니다.
Check Type(확인 유형**)**	다음 옵션 중 하나를 선택합니다. • **Installation(**설치**)**: 클라이언트에서 멀웨어 프로그램의 설치만 확인하려면 이 옵션을 선택합니다. • **Definition(**정의**)**: 클라이언트에서 안티 멀웨어 제품의 최신 정의 파일 업데이트만 확인하려면 이 옵션을 선택합니다.

필드 이름	사용 지침
Check against latest AV definition file version, if available(가능한 경우 최신 **AV** 정의 파일 버전을 기준으로 확인**)**	**(Definition(**정의**)** 확인 유형을 선택한 경우에만 사용 가능) Cisco ISE에서 포스처 업데이트의 결과로 사용 가능한 경우 최신 안티 멀웨어 정의 파일 버전과 비교하여 클라이언트의 안티 멀웨어 정의 파일 버전을 확인하려면 이 옵션을 선택합니다. 그렇지 않은 경우 이 옵션을 사용하면 Cisco ISE에서 최신 정의 파일 날짜를 기준으로 클라이언트의 정의 파일 날짜를 확인할 수 있습니다. 이 확인은 선택한 제품의 **Latest Definition Date(**최신 정의 날짜**)** 또는 **Latest Definition Version(**최신 정의 버전**)** 필드에 대해 Cisco ISE에 나열된 값이 있는 경우에만 작동합니다. 그렇지 않은 경우 **Current System Date(**현재 시스템 날짜**)** 필드를 사용해야 합니다.
Allow Virus Definition File to be(바이러스 정의 파일을 활성화하도록 허용**)**	(**Definition(**정의**)** 확인 유형을 선택한 경우에만 사용 가능) 클라이언트에서 안티 멀웨어 정의 파일 버전 및 최신 안티 멀웨어 정의 파일 날짜를 확인하려면 선택합니다. 최신 정의 파일 날짜는 **Days Older Than(**다음보다 오래됨**(**일**))** 필드에 정의한 날짜보다 이전일 수 없습니다. 이 필드를 선택하지 않는 경우 Cisco ISE는 **Check against latest AV definition file version(**최신 **AV** 정의 파일 버전을 기준으로 확인**)** 옵션을 사용하여 안티 멀웨어 정의 파일의 버전만 확인할 수 있습니다.
Days Older Than(다음보다 오래됨**(**일**))**	클라이언트의 최신 안티 멀웨어 정의 파일 날짜가 제품의 최신 안티 멀웨어 정의 파일 날짜 또는 현재 시스템 날짜를 기준으로 얼마나 더 이전 날짜(일)가 될 수 있는지 정의합니다. 기본값은 0입니다.

필드 이름	사용 지침
Latest File Date(최신 파일 날짜**)**	클라이언트의 최신 안티 멀웨어 정의 파일 날짜가 제품의 최신 안티 멀웨어 정의 파일 날짜를 기준으로 얼마나 더 이전 날짜(일)가 될 수 있는지 정의하려면 이 옵션을 선택합니다. 기간(일)을 기본값으로 설정하는 경우 클라이언트의 안티 멀웨어 정의 파일 날짜는 제품의 최신 안티 멀웨어 정의 파일 날짜 이전일 수 없습니다. 이 확인은 선택한 제품의 **Latest Definition Date(**최신 정의 날짜**)** 필드에 대해 Cisco ISE에 나열된 값이 있는 경우에만 작동합니다. 그렇지 않은 경우 **Current System Date(**현재 시스템 날짜**)** 필드를 사용해야 합니다.
Current System Date(현재 시스템 날짜**)**	클라이언트의 최신 안티멀웨어 정의 파일 날짜가 현재 시스템 날짜를 기준으로 얼마나 더 이전 날짜(일)가 될 수 있는지 정의하려면 이 옵션을 선택합니다. 기간(일)을 기본값으로 설정하는 경우 클라이언트의 안티 멀웨어 정의 파일 날짜는 현재 시스템 날짜 이전일 수 없습니다.

Products for Selected Vendor(선택한 벤더의 제품**)**

표에서 안티 멀웨어 제품을 선택합니다. **New Antimalware Condition(**새 안티 멀웨어 조건**)** 페이지에서 선택한 벤더에 따라 안티 멀웨어 제품 및 버전, 제공하는 치료 지원, 최신 정의 파일 날짜 및 버전이 이 표에서 표시됩니다.

참고 **Baseline Condition(**베이스라인 조건**)** 또는 **Advance Condition(**고급 조건**)**에서 각 안티멀웨어 제품에 대해 하나의 조건 만 구성 할 수 있습니다.

베이스라인 조건

필드 이름	사용 지침
Minimum Version(최소 버전**)**	(운영체제 및 벤더 필드를 업데이트할 때만 사용 가능) 안티멀웨어의 최소 버전을 엔드포인트에 설치해야 합니다.
Maximum Version(최대 버전**)**	포스처 피드를 업데이트할 때 안티멀웨어의 최대 버전이 자동으로 수정됩니다.
최소 규정 준수 모듈 버전**(Minimum Compliance Module Version)**	최소 규정 준수 모듈 버전은 AnyConnect를 기반으로 업데이트됩니다.

고급 조건**(Advance Condition)**
관련 항목
복합 포스처 조건, 24 페이지

사전 단순 조건 설정

다음 표에서는 **Dictionary Simple Conditions(**사전 단순 조건**)** 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **Dictionary Simple Condition(**사전 단순 조건**)**입니다.

표 ***11:*** 사전 단순 조건 설정

필드 이름	사용 지침
Name(이름**)**	생성할 사전 단순 조건의 이름을 입력합니다.
Description(설명**)**	생성할 사전 단순 조건에 대한 설명을 입력합니다.
Attribute(속성**)**	사전에서 속성을 선택합니다.
Operator(연산자**)**	선택한 속성에 값을 연결할 연산자를 선택합니다.
Value(값**)**	사전 속성과 연결할 값을 입력하거나 드롭다운 목록에서 미리 정의된 값을 선택합니다.

관련 항목
단순 포스처 조건, 23 페이지
단순 포스처 조건 생성, 24 페이지

사전 복합 조건 설정

표 ***12:*** 사전 복합 조건 설정

필드 이름	사용 지침
Name(이름**)**	생성할 사전 복합 조건의 이름을 입력합니다.
Description(설명**)**	생성할 사전 복합 조건에 대한 설명을 입력합니다.
Select Existing Condition from Library(라이브러리에서 기존 조건 선택**)**	정책 요소 라이브러리에서 사전 정의된 조건을 선택하여 식을 정의하거나 후속 단계에서 임시 속성/값 쌍을 식에 추가할 수 있습니다.
Condition Name(조건 이름**)**	정책 요소 라이브러리에서 이미 생성한 사전 단순 조건을 선택합니다.

필드 이름	사용 지침
Expression(식**)**	Condition Name(조건 이름) 드롭다운 목록에서 선택한 항목에 따라 식이 업데이트됩니다.
AND or OR operator(AND 또는 **OR** 연산자**)**	라이브러리에서 추가할 수 있는 사전 단순 조건을 논리적으로 결합하려면 AND 또는 OR 연산자를 선택합니다. **Action(**작업**)** 아이콘을 클릭하여 다음을 수행합니다. • 속성/값 추가 • 라이브러리의 조건 추가 • 삭제
Create New Condition (Advance Option)(새 조건 생성**(**고급 옵션**))**	다양한 시스템 또는 사용자 맞춤화 사전에서 속성을 선택합니다. 후속 단계에서 정책 요소 라이브러리의 사전 정의된 조건을 추가할 수도 있습니다.
Condition Name(조건 이름**)**	이미 생성한 사전 단순 조건을 선택합니다.
Expression(식**)**	Expression(식) 드롭다운 목록에서 사전 단순 조건을 생성할 수 있습니다.
Operator(연산자**)**	값을 속성에 연결할 연산자를 선택합니다.
Value(값**)**	사전 속성과 연결할 값을 입력하거나 드롭다운 목록에서 값을 선택합니다.

관련 항목

복합 포스처 조건, 24 페이지
복합 포스처 조건 생성, 24 페이지

패치 관리 조건 설정

다음 표에서는 **Patch Management Conditions(**패치 관리 조건**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **Patch Management Condition(**패치 관리 조건**)**입니다.

표 ***13:*** 패치 관리 조건

필드 이름	사용 지침
Name(이름**)**	패치 관리 조건의 이름을 입력합니다.

필드 이름	사용 지침
Description(설명**)**	패치 관리 조건의 설명을 입력합니다.
Operating System(운영체제**)**	엔드포인트의 패치 관리 소프트웨어 설치를 확인할 운영 체제를 선택하거나, 조건이 적용되는 최신 패치 관리 조건 파일 업데이트를 확인합니다. Windows OS 또는 Mac OSX를 선택할 수 있습니다. 패치 관리 조건을 생성할 운영체제 버전을 여러 개 선택할 수도 있습니다.
Vendor Name(벤더 이름**)**	드롭다운 목록에서 **Vendor Name(**벤더 이름**)**을 선택합니다. 선택한 항목에 따라 패치 관리 제품 및 지원되는 버전, 검사 유형 및 최소 준수 모듈 지원 세부 정보가 **Products for Selected Vendor(**선택한 벤더의 제품**)** 표에 표시됩니다. 표의 목록은 선택한 운영체제에 따라 변경됩니다.

필드 이름	사용 지침
Check Type(확인 유형**)**	다음 옵션 중 하나를 선택합니다. • **Installation(**설치**)**: 엔드포인트에 선택한 제품이 설치되어 있는지를 확인합니다. 모든 벤더에서 이 확인 유형을 지원합니다. 참고 CiscoTermporal Agent의 경우, **Requirements(**요건**)** 창에서 **Installation(**설치**)** 확인 유형을 포함하는 패치 관리 조건만 볼 수 있습니다. • **Enable(**활성화**)**: 엔드포인트에서 선택한 제품이 활성화되어 있는지를 확인합니다. **Products for Selected Vendor(**선택한 벤더의 제품**)** 목록을 참조하여 벤더의 제품이 선택한 확인 유형을 지원하는지를 확인합니다. • **Up to Date(**최신 상태**)**: 선택한 제품에 누락된 패치가 없는지를 확인합니다. **Products for Selected Vendor(**선택한 벤더의 제품**)** 목록을 참조하여 벤더의 제품이 선택한 확인 유형을 지원하는지를 확인합니다. **Products for Selected Vendor(**선택한 벤더의 제품**)** 드롭다운 목록을 클릭하여 **Vendor Name(**벤더 이름**)**에서 지정한 벤더가 지원하는 제품 목록을 확인합니다. 제품 1과 제품 2의 두 제품을 제공하는 벤더 A를 선택한 경우를 예로 들어 보겠습니다. 제품 1은 **Enabled(**활성화됨**)** 옵션을 지원하는 반면 제품 2는 지원하지 않을 수도 있습니다. 또는 제품 1이 어떤 확인 유형도 지원하지 않는 경우 제품 1은 회색으로 표시됩니다. 참고 (Cisco ISE 2.3 이상 및 AnyConnect 4.5 이상에 적용 가능) SCCM에 대해 패치 관리 조건에서 최신 상태 확인 유형을 선택하면 Cisco ISE가 1. Microsoft API를 사용하여 지정된 심각도 레벨에 대해 현재 보안 패치를 확인합니다. 2. 누락된 보안 패치에 대한 패치 관리 교정을 트리거합니다.

필드 이름	사용 지침
Check Patches Installed(설치된 패치 확인**)**	(**Up To Date(**최신 상태**)** 확인 유형을 선택한 경우에만 사용 가능합니다.) 누락된 패치에 대한 심각도 레벨을 구성할 수 있으며, 추후 해당 심각도를 기반으로 구축됩니다. 다음 옵션 중 하나를 선택합니다. • **Critical Only(**심각 전용**)**: 심각 소프트웨어 패치가 구축의 엔드포인트에 설치되었는지 확인합니다. • **Important and Critical(**중요 및 심각**)**: 중요 및 심각 소프트웨어 패치가 구축의 엔드포인트에 설치되었는지 확인합니다. • **Moderate, Important, and Critical(**보통**,** 중요 및 심각**)**: 구축의 엔드 포인트에 보통, 중요 및 심각 소프트웨어 패치가 설치되어 있는지 확인합니다. • **Low To Critical(**낮음부터 심각까지**)**: 구축의 엔드 포인트에 낮음, 보통, 중요 및 심각 소프트웨어 패치가 설치되어 있는지 확인합니다. • **All(**모두**)**: 모든 심각도 레벨에 대해 누락된 패치를 설치합니다.

관련 항목

패치 관리 조건 생성, 29 페이지

디스크 암호화 조건 설정

다음 표에서는 **Disk Encryption Condition(**디스크 암호화 조건**)** 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **Disk Encryption Condition(**디스크 암호화 조건**)**입니다.

표 ***14:*** 디스크 암호화 조건 설정

필드 이름	사용 지침
Name(이름**)**	생성할 디스크 암호화 조건의 이름을 입력합니다.
Description(설명**)**	디스크 암호화 조건에 대한 설명을 입력합니다.

필드 이름	사용 지침
Operating System(운영체제**)**	엔드포인트의 운영체제를 선택합니다. 이 엔드포인트의 디스크에서 암호화를 확인합니다. Windows OS 또는 Mac OSX를 선택할 수 있습니다. 디스크 암호화 조건을 생성할 운영체제 버전을 두 개 이상 선택할 수도 있습니다.
Vendor Name(벤더 이름**)**	드롭다운 목록에서 벤더 이름을 선택합니다. 벤더의 데이터 암호화 제품과 지원되는 버전, 암호화 상태 확인 및 최소 준수 모듈이 검색되어 **Products for Selected Vendor(**선택한 벤더의 제품**)** 표에 표시됩니다. 표의 목록은 선택한 운영체제에 따라 변경됩니다.
Location(위치**)**	**Products for Selected Vendor(**선택한 벤더의 제품**)** 섹션에서 옵션을 선택하는 경우에만 활성화됩니다. 다음 옵션 중 하나를 선택합니다. • **Specific Location(**특정 위치**)**: 지정된 디스크 드라이브(예: Windows OS의 경우 C:)가 엔드포인트에서 암호화되는지 아니면 지정된 볼륨 레이블(예: Mac OSX용 Mackintosh HD)이 암호화되는지를 확인합니다. • **System Location(**시스템 위치**)**: 기본 Windows OS 시스템 드라이브 또는 Mac OSX 하드 드라이브가 엔드포인트에서 암호화되는지를 확인합니다. • **All Internal Drives(**모든 내부 드라이브**)**: 내부 드라이브를 확인합니다. 마운트 및 암호화된 모든 하드 디스크와 모든 내부 파티션을 포함합니다. 읽기 전용 드라이브, 시스템 복구 디스크 / 파티션, 부팅 파티션, 네트워크 파티션 및 엔드포인트 외부에 있는 다른 물리적 디스크 드라이브(USB 및 썬더볼트를 통해 연결된 디스크 드라이브를 포함하나 이에 국한되지 않음)는 제외합니다. 검증된 암호화 소프트웨어 제품은 다음과 같습니다. • Bit-locker-6.*x*/10.*x* • Checkpoint 80.*x* on Windows 7

필드 이름	사용 지침
Encryption State(암호화 상태**)**	선택한 제품이 암호화 상태 확인을 지원하지 않으면 Encryption State(암호화 상태) 확인란은 비활성화됩니다. 이 확인란을 선택해야 리피터가 표시됩니다. Fully Encrypted(완전히 암호화됨) 옵션을 선택하여 클라이언트의 디스크 드라이브가 완전히 암호화되는지를 확인할 수 있습니다. TrendMicro 등에 대해 조건을 생성하고 벤더 두 개를 선택하여 하나는 Encryption State(암호화 상태)를 "Yes(예)"로, 다른 하나는 Encryption State(암호화 상태)를 "No(아니요)"로 설정하는 경우 Vendor Encryption State(벤더 암호화 상태) 중 하나가 "No(아니요)"이므로 Encryption State(암호화 상태)가 비활성화됩니다. 참고 리피터를 클릭해 위치를 더 추가할 수 있으며 각 위치 간의 관계는 논리적 AND 연산자입니다.

관련 항목

디스크 암호화 조건 생성, 30 페이지

USB 조건 설정

다음 표에서는 **USB Condition(USB** 조건**)** 창의 필드에 대해 설명합니다. 이동할 수도 있습니다.Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Posture(**포스처**)** > **Policy Elements(**정책 요소**)** > **USB**. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **USB Condition(USB** 조건**)**.

USB 확인은 사전 정의된 조건이며 Windows OS만 지원합니다.

표 ***15: USB*** 조건 설정

필드 이름	사용 지침
Name(이름**)**	USB_Check
Description(설명**)**	사전 정의된 Cisco 확인
Operating System(운영체제**)**	(Windows용)
규정 준수 모듈**(Compliance Module)**	버전 4.x(및 이상)에 대한 ISE 포스처 규정 준수 모듈 지원의 표시 전용 필드입니다.

관련 항목

단순 포스처 조건, 23 페이지

하드웨어 속성 조건 설정

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(정책)** > **Policy Elements(정책 요소)** > **Hardware Attributes Condition(하드웨어 속성 조건)**을 선택하여 **Hardware Attributes Condition(하드웨어 속성 조건)** 창에 액세스합니다. 다음 표에서는 **Hardware Attributes Condition(하드웨어 속성 조건)** 창의 필드에 대해 설명합니다.

필드 이름	사용 지침
Name(이름)	Hardware_Attributes_Check: 조건에 할당된 기본 이름입니다.
Description(설명)	클라이언트로부터 하드웨어 속성을 수집하는 Cisco 사전 정의 검사입니다.
Operating System(운영체제)	모든 Windows 및 Mac OS
규정 준수 모듈**(Compliance Module)**	4.x 이상

포스처 외부 데이터 소스 조건

엔드포인트 UDID를 외부 데이터 소스와 일치시키는 조건을 구성할 수 있습니다. 현재는 Active Directory만 지원됩니다. Active Directory에 UDID를 전송하기 위해 포스처 에이전트에 필요한 스크립트는 ISE에 포함되어 있지 않습니다.

포스처 정책 구성

포스처 정책은 하나 이상의 ID 그룹 및 운영체제와 연결된 포스처 요건의 모음입니다. 사전 속성은 ID 그룹 및 운영체제와 함께 디바이스에 대해 여러 정책을 정의하는 데 사용할 수 있는 선택적 조건입니다.

Cisco ISE는 규정을 준수하지 않는 디바이스에 대해 유예 기간을 구성하는 옵션을 제공합니다. 디바이스가 규정을 준수하지 않는 것으로 확인되면 Cisco ISE는 포스처 평가 결과 캐시에서 이전에 알려진 정상 상태를 찾아 그에 따라 디바이스에 유예 기간을 제공합니다. 유예 기간 동안 디바이스에 네트워크에 액세스할 수 있는 권한이 부여됩니다. 유예 기간을 분, 시간 또는 일(최대 30일)로 구성할 수 있습니다.

자세한 내용은 ISE Posture 규범 구축 가이드의 "포스처 정책" 섹션을 참조하십시오.

참고 '엔드 포인트 정책' 및 '논리적 프로파일'이 모두**Policy(정책)** > **Posture(포스처)**의 기타 조건에 구성된 경우 프로파일러 정책 평가가 작동하지 않습니다.

참고

- 유예 기간이 늘어나거나 줄어들면 디바이스가 포스처 플로우를 다시 통과하는 경우(예: **Delayed Notification(**지연 알림**)** 옵션이 활성화된 경우 **Re-Scan(**다시 스캔**)** 옵션이 선택되고, 디바이스의 연결이 끊기거나 네트워크에 다시 연결됨) 새 유예 기간 및 지연 알림이 적용됩니다.
- 임시 에이전트에는 유예 기간이 적용되지 않습니다.
- 디바이스가 여러 포스처 정책과 일치하는 경우 각 정책의 유예 기간이 서로 다르면 디바이스는 여러 정책에 걸쳐 구성된 최대 유예 기간을 가져옵니다.
- 디바이스가 유예 기간에 있는 경우 AUP(Acceptable Use Policy)가 표시되지 않습니다.

시작하기 전에

- AUP(Acceptable Use Policy)를 이해하고 있어야 합니다.
- PRA(Periodic Reassessments)에 대해 알고 있어야 합니다.
- 규정 준수 관련 알림을 보려면 AnyConnect 에이전트 4.7 이상을 사용해야 합니다. AnyConnect 에이전트 구성에 대한 자세한 내용은 AnyConnect 컨피그레이션 생성, 112 페이지를 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Posture(**포스처**)** 또는 **Work Centers(**작업 센터**)** > **Posture(**포스처**)** > **Posture Policy(**포스처 정책**)**를 선택합니다.

단계 **2** 드롭다운 화살표를 사용하여 새 정책을 추가합니다.

단계 **3** 프로파일을 편집하려면 정책을 더블 클릭하거나 행 끝에서 Edit(편집)를 클릭합니다.117

단계 **4** **Rule Status(**규칙 상태**)** 드롭다운 목록에서 **Enabled(**활성화됨**)** 또는 **Disabled(**비활성화됨**)**를 선택합니다.

단계 **5** **Policy Options(**정책 옵션**)** 아래의 드롭다운을 선택하고 **Grace Period Settings(**유예 기간 설정**)**를 분, 시간 또는 일 단위로 지정합니다.

유효한 값은 다음과 같습니다.

- 1~30일
- 1~720시간
- 1~43200분

기본적으로 이 설정은 비활성화되어 있습니다.

참고 포스처 평가 결과가 규정을 준수하지 않더라도 디바이스가 이전에 규정을 준수하는 것으로 확인되었고 캐시가 아직 만료되지 않은 경우 디바이스에 **Grace Period Settings(**유예 기간 설정**)**에 지정된 시간 동안 액세스 권한이 부여됩니다.

단계 **6** (선택 사항) 유예 기간이 일정 비율 경과할 때까지 유예 기간 프롬프트가 사용자에게 표시되지 않도록 하려면 **Delayed Notification(**지연 알림**)**이라는 슬라이더를 드래그합니다. 예를 들어 알림 지연 기간이 50%로 지정되고 유예 기간을 10분으로 구성한 경우 Cisco ISE는 5분 후에 포스처 상태를 확인하고 엔드포인트가 미준수로 확인되

면 유예 기간 알림을 표시합니다. 엔드포인트 상태가 규정을 준수하는 경우 유예 기간 알림이 표시되지 않습니다. 알림 지연 기간을 0%로 설정하면 유예 기간이 시작되자마자 사용자에게 문제를 해결하라는 메시지가 표시됩니다. 단, 유예 기간이 만료될 때까지는 엔드포인트에 액세스 권한이 부여됩니다. 이 필드의 기본값은 0%입니다. 유효 범위는 0~95%입니다.

단계 **7** **Rule Name(**규칙 이름**)** 필드에 정책의 이름을 입력합니다.

참고 예기치 않은 결과를 방지하기 위해 각 요건을 별도의 규칙으로 사용하여 포스처 정책을 구성하는 것이 가장 좋습니다.

단계 **8** **Identity Groups(ID** 그룹**)** 열에서 원하는 ID 그룹을 선택합니다.

사용자 또는 엔드포인트 ID 그룹을 기반으로 포스처 정책을 생성할 수 있습니다.

단계 **9** **Operating Systems(**운영체제**)** 열에서 운영체제를 선택합니다.

단계 **10** **Compliance Module(**규정 준수 모듈**)** 열에서 필요한 규정 준수 모듈을 선택합니다.

- **4.x** 이상: 안티멀웨어, 디스크 암호화, 패치 관리 및 USB 조건을 지원합니다.
- **3.x** 이하: 안티바이러스, 안티스파이웨어, 디스크 암호화 및 패치 관리 조건을 지원합니다.
- 모든 버전: 파일, 서비스, 레지스트리, 애플리케이션 및 복합 조건을 지원합니다.

단계 **11** **Posture Type(**포스처 유형**)** 열에서 Posture Type(포스처 유형)을 선택합니다.

- **AnyConnect** - 클라이언트 상호 작용이 필요한 Cisco ISE 정책을 모니터링하고 시행하기 위해 AnyConnect 에이전트를 구축합니다.
- **AnyConnect** 스텔스 - 클라이언트 상호 작용 없이 Cisco ISE 포스처 정책을 모니터링하고 시행하기 위해 AnyConnect 에이전트를 구축합니다.
- 임시 에이전트 - 규정 준수 상태를 확인하기 위해 클라이언트에서 실행되는 임시 실행 파일입니다.

단계 **12** **Other Conditions(**기타 조건**)**에서는 사전 속성을 하나 이상 추가하여 사전에 단순 조건 또는 복합 조건으로 저장할 수 있습니다.

참고 **Posture Policy(**포스처 정책**)** 창에서 생성하는 사전 단순 조건과 사전 복합 조건은 권한 부여 정책을 구성하는 동안에는 표시되지 않습니다.

단계 **13** **Requirements(**요건**)** 필드에 요건을 지정합니다.

단계 **14** **Save(**저장**)**를 클릭합니다.

AnyConnect 워크플로우 구성

AnyConnect 에이전트를 구성하려면 Cisco ISE에서 다음 단계를 수행합니다.

단계 **1** AnyConnect 에이전트 프로파일을 생성합니다.

단계 **2** AnyConnect 패키지의 AnyConnect 컨피그레이션을 생성합니다.
단계 **3** 클라이언트 프로비저닝 정책을 생성합니다.
단계 **4** (선택 사항) 사용자 맞춤화 포스처 조건을 생성합니다.
단계 **5** (선택 사항) 사용자 맞춤화 교정 작업을 생성합니다.
단계 **6** (선택 사항) 사용자 맞춤화 포스처 요건을 생성합니다.
단계 **7** 포스처 정책을 생성합니다.
단계 **8** 클라이언트 프로비저닝 정책을 구성합니다.
단계 **9** 권한 부여 프로파일을 생성합니다.
단계 **10** 권한 부여 정책을 구성합니다.

참고 Cisco ISE는 AnyConnect 포스 처 플로우에 대해 ARM64 버전의 AnyConnect를 지원하지 않습니다. 클라이언트 프로비저닝 정책에서 ARM64 버전의 AnyConnect이 사용되지 않는지 확인합니다. 그러지 않으면 클라이언트 측에서 장애가 발생할 수 있습니다. 이 문제 때문에 Anyconnect가 제대로 작동하지 않으면 클라이언트를 재시작합니다.

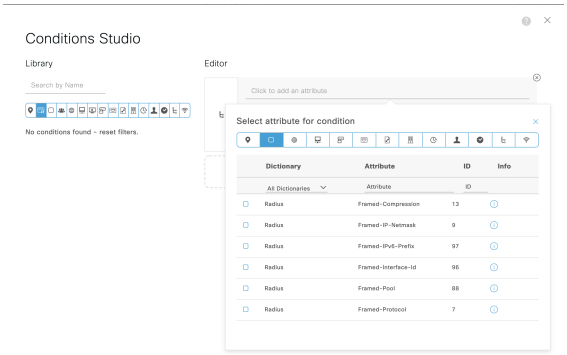
인증서 기반 조건의 사전 요건

클라이언트 프로비저닝 및 포스처 정책 규칙에는 인증서 속성에 기반한 조건이 포함될 수 있습니다. 클라이언트 프로비저닝 또는 포스처 정책의 인증서 기반 조건에 대한 사전 요건은 동일한 인증서 속성을 바탕으로 일치하는 권한 부여 정책 규칙이 있는지 확인하는 것입니다.

예를 들어 그림에 나와 있는 것과 동일한 속성을 사용해야합니다. Issuer – Common Name(발급자 - 공통 이름) 속성은 클라이언트 프로비저닝 또는 포스처 및 권한 부여 정책에 모두 사용됩니다.

그림 ***1: Cisco*** 프로비저닝 정책

그림 ***2: Condition Studio***



참고 ISE 서버 인증서는 AnyConnect 4.6 MR2 이상의 시스템 인증서 저장소에서 신뢰할 수 있어야 합니다. 서버를 신뢰할 수 없는 경우 보다 높은 권한이 필요한 포스처 확인 또는 교정이 이루어지지 않습니다.

- Windows OS: 서버 인증서를 시스템 인증서 저장소에 추가해야 합니다.
- MAC OS: 서버 인증서를 시스템 키체인에 추가해야 합니다. 명령줄 유틸리티를 사용하여 인증서를 신뢰하는 것이 좋습니다. Keychain Access 앱을 사용하여 시스템 키체인에 인증서를 추가하는 경우 로그인 키체인에 인증서가 이미 있으면 작동하지 않을 수 있습니다.

기본 포스처 정책

Cisco ISE 소프트웨어에는 다수의 사전 구성된 포스처 정책(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Posture(**포스처**)**)이 포함되어 있으므로 포스처 정책과 프로파일을 보다 쉽게 생성할 수 있습니다. 이러한 정책은 기본적으로 비활성화되어 있습니다. 요건에 따라 이러한 정책을 활성화할 수 있습니다. 다음은 몇 가지 기본 포스처 정책입니다.

규칙 이름	설명	요건
Default_Antimalware_Policy_Mac	엔드포인트에서, 지원되는 벤더의 디바이스에 설치되어 실행 중인 안티멀웨어 소프트웨어(AnyConnect에서 인식)가 있는지 확인합니다.	Any_AM_Installation
Default_Antimalware_Policy_Win	엔드포인트에서, 지원되는 벤더의 디바이스에 설치되어 실행 중인 안티멀웨어 소프트웨어(AnyConnect에서 인식)가 있는지 확인합니다.	Any_AM_Installation_Win

규칙 이름	설명	요건
Default_AppVis_Policy_Mac	정보를 수집하고 해당 엔드포인트에 설치된 모든 애플리케이션을 보고합니다.	Default_AppVis_Requirement_Mac
Default_AppVis_Policy_Win	정보를 수집하고 해당 엔드포인트에 설치된 모든 애플리케이션을 보고합니다.	Default_AppVis_Requirement_Win
Default_Firewall_Policy_Mac	엔드포인트에서, 지원되는 벤더의 설치된 방화벽 프로그램(AnyConnect에서 인식)이 있는지 확인합니다.	Default_Firewall_Requirement_Mac
Default_Firewall_Policy_Win	엔드포인트에서, 지원되는 벤더의 설치된 방화벽 프로그램(AnyConnect에서 인식)이 있는지 확인합니다.	Default_Firewall_Requirement_Win
Default_USB_Block_Win	엔드포인트 디바이스에서 연결되어 있는 USB 스토리지 디바이스가 없음을 확인합니다.	USB_Block

Client Posture 평가

네트워크 보안 수단을 적절하고 효율적으로 적용할 수 있도록 Cisco ISE에서는 보호된 네트워크에 액세스하는 모든 클라이언트 머신의 보안 기능을 검증하고 유지 관리할 수 있습니다. Cisco ISE 관리자는 클라이언트 머신에서 최신 보안 설정 또는 애플리케이션을 활성화하도록 설계된 포스처 정책을 사용하는 방식으로, 네트워크에 액세스하는 모든 클라이언트 머신이 엔터프라이즈 네트워크 액세스를 위해 정의된 보안 표준을 충족하고 있으며 앞으로도 계속 충족하는지 확인할 수 있습니다. 포스처 규정 준수 보고서는 사용자가 로그인하는 시점, 그리고 정기적인 재평가가 발생하는 경우에 클라이언트 머신의 규정 준수 수준에 대한 스냅샷을 Cisco ISE에 제공합니다.

포스처 평가 및 규정 준수는 Cisco ISE에서 사용 가능한 다음 에이전트 유형 중 하나를 사용하여 발생합니다.

- AnyConnect ISE Agent: Windows 또는 Mac OS X 클라이언트에 설치되어 포스처 규정 준수 기능을 수행하는 영구 에이전트입니다.
- Cisco Temporal Agent: 규정 준수 상태를 확인하기 위해 클라이언트에서 실행되는 임시 실행 파일입니다. 로그인 세션이 종료된 후 클라이언트 머신에서 에이전트가 제거됩니다. 기본적으로 에이전트는 Cisco ISE ISO 이미지에 있으며 설치 중에 Cisco ISE에 업로드됩니다.

Posture Assessment 옵션

다음 표에는 Windows/Macintosh용 Cisco ISE Posture Agent와 Windows용 Web Agent에서 지원하는 Posture Assessment(포스처 조건) 옵션의 목록이 나와 있습니다.

표 ***16: Posture Assessment*** 옵션

Windows용 ISE Posture Agent	**Windows용 Cisco Temporal Agent**	**Macintosh OS X용 ISE Posture Agent**	**Macintosh OS X용 Cisco Temporal Agent**
운영체제/서비스 팩/핫픽스	—	—	—
서비스 확인	서비스 확인(Temporal Agent 4.5 및 ISE 2.3)	서비스 확인(AC 4.1 및 ISE 1.4)	데몬 확인은 지원되지 않음
레지스트리 확인	레지스트리 확인(Temporal Agent 4.5 및 ISE 2.3)	—	—
파일 확인	파일 확인(Temporal Agent 4.5 및 ISE 2.3)	파일 확인(AC 4.1 및 ISE 1.4)	파일 확인(Temporal Agent 4.5 및 ISE 2.3)
애플리케이션 확인	애플리케이션 확인(Temporal Agent 4.5 및 ISE 2.3)	애플리케이션 확인(AC 4.1 및 ISE 1.4)	애플리케이션 확인(Temporal Agent 4.5 및 ISE 2.3)
안티바이러스 설치	안티멀웨어 설치	안티바이러스 설치	안티멀웨어 설치
안티바이러스 버전/안티바이러스 정의 날짜	OPSWAT 버전 4가 사용되므로 안티바이러스/안티스파이웨어가 지원되지 않음, 안티멀웨어만 지원	안티바이러스 버전/안티바이러스 정의 날짜	OPSWAT 버전 4가 사용되므로 안티바이러스/안티스파이웨어가 지원되지 않음, 안티멀웨어만 지원
안티스파이웨어 설치	OPSWAT 버전 4가 사용되므로 안티바이러스/안티스파이웨어가 지원되지 않음, 안티멀웨어만 지원	안티스파이웨어 설치	OPSWAT 버전 4가 사용되므로 안티바이러스/안티스파이웨어가 지원되지 않음, 안티멀웨어만 지원
안티스파이웨어 버전/안티스파이웨어 정의 날짜	OPSWAT 버전 4가 사용되므로 안티바이러스/안티스파이웨어가 지원되지 않음, 안티멀웨어만 지원	안티스파이웨어 버전/안티스파이웨어 정의 날짜	OPSWAT 버전 4가 사용되므로 안티바이러스/안티스파이웨어가 지원되지 않음, 안티멀웨어만 지원

Windows용 ISE Posture Agent	Windows용 Cisco Temporal Agent	Macintosh OS X용 ISE Posture Agent	Macintosh OS X용 Cisco Temporal Agent
패치 관리 확인(AC 4.1 및 ISE 1.4)	패치 관리 설치만 확인	패치 관리 확인(AC 4.1 및 ISE 1.4)	—
Windows 업데이트 실행	—	—	—
Windows 업데이트 컨피그레이션	—	—	—
WSUS 규정 준수 설정	—	—	—

포스처 교정 옵션

다음 표에는 Windows/Macintosh용 Cisco ISE 포스처 에이전트와 Windows용 웹 에이전트에서 지원하는 포스처 교정 옵션의 목록이 나와 있습니다.

표 ***17:*** 포스처 교정 옵션

ISE Posture 에이전트 (Windows용)	ISE Posture 에이전트 (Macintosh OS X용)
메시지 텍스트(로컬 확인)	메시지 텍스트(로컬 확인)
URL 링크(링크 배포)	URL 링크(링크 배포)
파일 배포	—
프로그램 시작	—
안티바이러스 정의 업데이트	안티바이러스 실시간 업데이트
안티스파이웨어 정의 업데이트	안티스파이웨어 실시간 업데이트
패치 관리 치료(AC 4.1 및 ISE 1.4)	—
Windows 업데이트	—
WSUS	—

ISE 커뮤니티 리소스

Cisco ISE and SCCM integration Reference Guide

포스처를 위한 사용자 맞춤화 조건

포스처 조건은 파일, 레지스트리, 애플리케이션, 서비스 또는 사전 조건의 단순 조건 중 하나일 수 있습니다. 이러한 단순 조건 중 하나 이상의 조건은 포스처 요건과 연결될 수 있는 복합 조건을 형성합니다.

초기 포스처 업데이트가 완료되면 Cisco ISE는 Cisco에서 정의한 단순 및 복합 조건도 생성합니다. Cisco에서 정의한 단순 조건에서는 pc_ as를 사용하고, 복합 조건에서는 pr_ as를 사용합니다.

사용자 맞춤화 조건 또는 Cisco에서 정의한 조건은 단순 조건과 복합 조건을 모두 포함합니다.

포스처 서비스에서는 AV/AS(Antivirus and Antispyware) 복합 조건에 따라 내부 검사를 사용합니다. 따라서 포스처 보고서에는 관리자가 생성한 정확한 AV/AS 복합 조건 이름이 반영되지 않습니다. 보고서에는 AV/AS 복합 조건의 내부 검사 이름만 표시됩니다.

예를 들어 벤더 및 제품을 확인하기 위해 "MyCondition_AV_Check"라는 AV 복합 조건을 생성한 경우 포스처 보고서에는 조건 이름으로 "MyCondition_AV_Check"가 아니라 내부 검사, 즉 "av_def_ANY"가 표시됩니다.

포스처 엔드포인트 사용자 맞춤화 속성

포스처 엔드포인트 사용자 맞춤화 속성을 사용하여 클라이언트 프로비저닝 및 포스처 정책을 생성할 수 있습니다. 최대 100개의 엔드포인트 맞춤형 속성을 생성할 수 있습니다. 지원되는 엔드포인트 사용자 맞춤화 속성 유형은 Int, String, Long, Boolean, Float, IP 및 Date.

엔드포인트 사용자 맞춤화 속성은 특정 속성에 따라 디바이스를 허용 또는 차단하거나 포스처 또는 클라이언트 프로비저닝 정책에 따라 특정 권한을 할당하는 데 사용할 수 있습니다.

엔드포인트 맞춤형 속성을 사용한 포스처 정책 생성

엔드포인트 맞춤형 속성을 사용하여 포스처 정책을 생성하려면 다음을 따릅니다.

단계 **1** 엔드포인트 맞춤형 속성을 생성합니다.

a)

b) **Attribute Name(**속성 이름**)**(예: deviceType)과 데이터 유형(예: String)을 **Endpoint Custom Attributes(**엔드포인트 맞춤형 속성**)** 영역에 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **2** 맞춤형 속성에 값을 할당합니다.

a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)**.

b) 맞춤형 속성 값을 할당합니다.

- 필요한 MAC 주소 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

- 또는 필요한 MAC 주소를 클릭하고 **Endpoints(**엔드포인트**)** 페이지에서 **Edit(**편집**)**를 클릭합니다.

c) 생성한 맞춤형 속성이 **Edit Endpoint(**엔드포인트 편집**)** 대화 상자의 **Custom Attributes(**맞춤형 속성**)** 영역에 표시되는지 확인합니다.

d) **Edit(**편집**)**를 클릭하고 필요한 속성 값(예: deviceType = Apple-iPhone)을 입력합니다.

e) **Save(**저장**)**를 클릭합니다.

단계 **3** 맞춤형 속성 및 값을 사용하여 포스처 정책을 생성합니다.

a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Posture(**포스처**)** > **Posture Policy(**포스처 정책**)**.

b) 필요한 정책을 생성합니다. **Other Conditions(**기타 조건**)**를 클릭하여 맞춤형 속성을 선택하고 필요한 사전을 선택합니다(예: Endpoints(엔드 포인트) > deviceType, 즉 1단계에서 생성한 맞춤형 속성 선택). 자세한 내용은 Cisco 임시 에이전트 구성 워크플로우, 83 페이지을 참조하십시오.

c) **Save(**저장**)**를 클릭합니다.

엔드포인트 맞춤형 속성을 사용하여 클라이언트 프로비저닝 정책을 생성하려면 다음을 따릅니다.

1. **Work Centers(**작업 센터**)** > **Posture(**포스처**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Client Provisioning Policy(**클라이언트 프로비저닝 정책**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .
2. 필요한 정책을 생성합니다.
   - 필요한 규칙을 생성합니다(예: Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117).
   - **Other Conditions(**기타 조건**)**를 클릭하고 필요한 사전을 선택하여 맞춤형 속성을 선택합니다.

사용자 맞춤화 포스처 교정 작업

사용자 맞춤화 포스처 교정 작업은 프로그램, Windows 업데이트 또는 WSUS(Windows Server Update Services) 교정 유형을 실행하는 파일, 링크, 안티바이러스 또는 안티스파이웨어 정의 업데이트입니다.

안티스파이웨어 교정 추가

안티스파이웨어 교정을 설치할 수 있습니다. 그러면 교정 후 규정 준수를 위해 최신 파일 정의를 사용하여 클라이언트를 업데이트합니다.

AS 교정 페이지에는 모든 안티바이러스 교정과 해당 이름/설명 및 교정 모드가 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**포스처**)**를 선택합니다.

단계 **2** **Remediation Actions(**교정 작업**)**를 선택합니다.

단계 **3** **AS Remediation(AS** 교정**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **New AS Remediations(**새 **AS** 교정**)** 페이지의 값을 수정합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

안티바이러스 교정 추가

안티바이러스 교정을 설치할 수 있습니다. 그러면 교정 후 규정 준수를 위해 최신 파일 정의를 사용하여 클라이언트를 업데이트합니다.

AV Remediations(AV 교정) 창에는 모든 안티바이러스 교정과 해당 이름/설명 및 교정 모드가 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**포스처**)**를 선택합니다.

단계 **2** **Remediation Actions(**교정 작업**)**를 선택합니다.

단계 **3** **AV Remediation(AV** 교정**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **New AV Remediation(**새 **AV** 교정**)** 창의 값을 수정합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

파일 교정 추가

파일 교정을 사용하면 클라이언트가 규정 준수를 위해 필요한 파일 버전을 다운로드할 수 있습니다. 클라이언트 에이전트는 규정 준수를 위해 클라이언트에 필요한 파일을 사용하여 엔드포인트를 교정합니다.

File Remediations(파일 교정) 창에서 파일 교정을 필터링, 확인, 추가 또는 삭제할 수는 있지만 편집할 수는 없습니다. 파일 교정(File Remediation) 창에는 모든 파일 교정과 해당 이름/설명 및 교정에 필요한 파일이 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**포스처**)**를 선택합니다.

단계 **2** **Remediation Actions(**교정 작업**)**를 선택합니다.

단계 **3** **File Remediation(**파일 교정**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **Name(**이름**)** 및 **Description(**설명**)** 필드에 파일 교정의 이름과 설명을 입력합니다.

단계 **6** **New File Remediation(**새 파일 교정**)** 창의 값을 수정합니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

프로그램 시작 교정 추가

클라이언트 에이전트가 규정 준수를 위해 하나 이상의 애플리케이션을 시작하여 클라이언트를 교정하는 프로그램 시작 교정을 생성할 수 있습니다.

프로그램 시작 교정 페이지에는 모든 프로그램 시작 교정과 해당 이름/설명 및 교정 모드가 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**포스처**)**를 선택합니다.

단계 **2** **Remediation Actions(**교정 작업**)**를 선택합니다.

단계 **3** **Launch Program Remediation(**프로그램 시작 교정**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **New Launch Program Remediation(**새 프로그램 시작 교정**)** 페이지의 값을 수정합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

프로그램 시작 치료 문제 해결

문제

Launch Program Remediation(프로그램 시작 치료)을 사용하여 치료를 위해 시작하는 애플리케이션은 정상적으로 시작되며 Windows Task Manager에 표시되지만 애플리케이션 UI는 보이지 않습니다.

해결책

프로그램 UI 시작 애플리케이션은 시스템 권한을 사용하여 실행되며 ISD(Interactive Service Detection) 윈도우에서 볼 수 있습니다. 프로그램 UI 시작 애플리케이션을 보려면 다음 OS에 대해 ISD를 활성화해야 합니다.

- Windows Vista: ISD는 기본적으로 중지 상태입니다. services.msc에서 ISD 서비스를 시작하여 ISD를 활성화합니다.
- Windows 7: ISD 서비스는 기본적으로 활성화되어 있습니다.
- Windows 8/8.1: 레지스트리 \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows에서 "NoInteractiveServices"를 1에서 0으로 변경하여 ISD를 활성화합니다.

링크 교정 추가

링크 교정을 사용하면 클라이언트가 URL을 클릭하여 Remediation(교정) 창또는 리소스에 액세스할 수 있습니다. 클라이언트 에이전트는 링크를 사용하여 브라우저를 열고 클라이언트가 규정 준수를 위해 직접 교정을 수행하도록 허용합니다.

Link Remediation(링크 교정) 창에는 모든 링크 교정과 해당 이름/설명 및 교정 모드가 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**포스처**)**를 선택합니다.

단계 **2** **Remediation Actions(**교정 작업**)**를 선택합니다.

단계 **3** **Link Remediation(**링크 교정**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **New Link Remediation(**새 링크 교정**)** 창의 값을 수정합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

패치 관리 교정 추가

패치 관리 교정을 설치할 수 있습니다. 그러면 교정 후 규정 준수를 위해 최신 파일 정의를 사용하여 클라이언트를 업데이트합니다.

패치 관리 교정 창에는 교정 유형, 패치 관리 벤더 이름 및 다양한 교정 옵션이 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**포스처**)**를 선택합니다.

단계 **2** **Remediation Actions(**교정 작업**)**를 선택합니다.

단계 **3** **Patch Mangement Remediation(**패치 관리 교정**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **Patch Management Remediation(**패치 관리 교정**)** 창의 값을 수정합니다.

단계 **6** **Submit(**제출**)**을 클릭하여 교정 작업을 **Patch Management Remediation(**패치 관리 교정**)** 창에 추가합니다.

Windows Server Update Services 교정 추가

규정 준수를 위해 Windows 클라이언트가 로컬에서 관리되거나 Microsoft에서 관리하는 WSUS 서버에서 최신 WSUS 업데이트를 받도록 구성할 수 있습니다. WSUS(Windows Server Update Services) 교정은 로컬에서 관리되는 WSUS 서버 또는 Microsoft에서 관리하는 WSUS 서버에서 최신 Windows 서비스 팩, 핫픽스 및 패치를 설치합니다.

클라이언트 에이전트가 로컬 WSUS 에이전트와 통합되는 WSUS 교정을 생성하여 WSUS 업데이트를 위해 엔드포인트가 최신 상태인지를 확인할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**포스처**)**를 선택합니다.

단계 **2** **Remediation Actions(**교정 작업**)**를 선택합니다.

단계 **3** **Windows Server Update Services Remediation(Windows Server Update Services** 교정**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **New Windows Server Update Services Remediation(**새 **Windows Server Update Services** 교정**)** 창의 값을 수정합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

Windows 업데이트 교정 추가

Windows 업데이트 교정 페이지에는 모든 Windows 업데이트 교정과 해당 이름/설명 및 교정 모드가 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > > **Posture(**포스처**)**를 선택합니다. .

단계 **2** **Remediation Actions(**교정 작업**)**를 선택합니다.

단계 **3** **Windows Update Remediation(Windows** 업데이트 교정**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **New Windows Update Remediation(**새 **Windows** 업데이트 교정**)** 창의 값을 수정합니다.

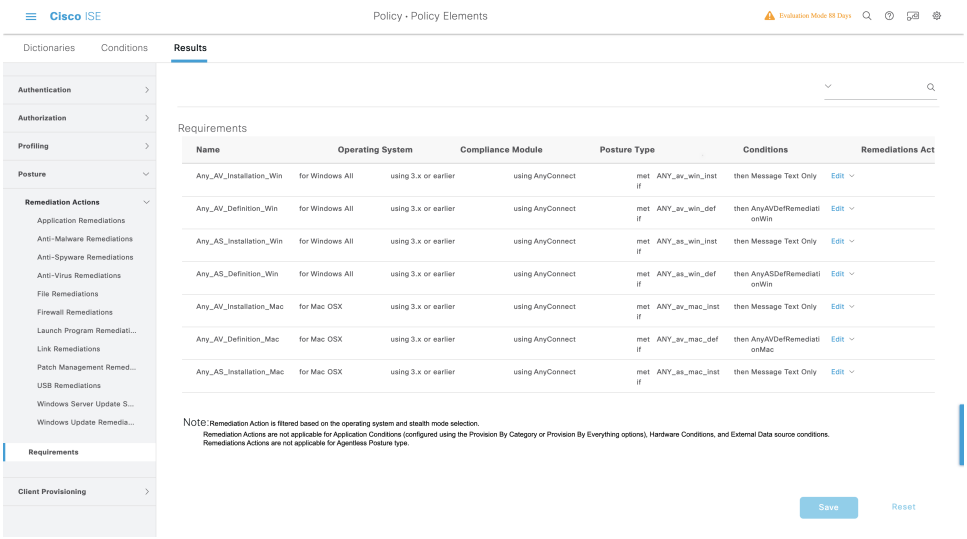
단계 **6** **Submit(**제출**)**을 클릭합니다.

Posture Assessment 요건

포스처 요건은 역할 및 운영체제와 연결할 수 있는 관련 교정 작업이 포함된 복합 조건 집합입니다. 네트워크에 연결하는 모든 클라이언트는 포스처 평가 중에 필수 요건을 충족해야 네트워크에서 준수 상태가 됩니다.

Posture Policies에서 포스처 정책 요건을 필수, 선택 또는 감사 유형으로 설정할 수 있습니다. 요건이 선택인 경우에는 클라이언트가 해당 요건을 충족하지 못하더라도 엔드포인트 평가 중에 해당 평가를 계속 진행할 수 있는 옵션이 제공됩니다.

그림 ***3: Posture Policy*** 요건 유형



필수 요건

정책 평가 중에 에이전트는 Posture Policy에 정의되어 있는 필수 요건을 충족하지 못하는 클라이언트에 대해 치료 옵션을 제공합니다. 최종 사용자는 치료를 수행하여 치료 타이머 설정에 지정된 시간 이내에 요건을 충족해야 합니다.

절대 경로에 C:\temp\text.file이 있는지를 확인하기 위해 사용자 맞춤화 조건을 사용하여 필수 요건을 지정한 경우를 예로 들어 보겠습니다. 해당 파일이 없으면 필수 요건은 충족되지 않으며 사용자는 Non-Compliant(미준수) 상태로 전환됩니다.

선택 요건

정책 평가 중에 에이전트는 Posture Policy에 지정되어 있는 선택적 요건을 충족하지 못하는 클라이언트에 대해 평가를 계속하도록 옵션을 제공합니다. 최종 사용자는 지정된 선택적 요건을 건너뛸 수 있습니다.

Calc.exe와 같이 클라이언트 머신에서 실행되고 있는 애플리케이션을 확인하기 위해 사용자 맞춤화 조건을 사용하여 선택적 요건을 지정한 경우를 예로 들어 보겠습니다. 클라이언트가 조건을 충족하지 못하더라도 에이전트는 계속할지를 묻는 옵션 메시지를 표시합니다. 계속하도록 선택하면 선택적 요건을 건너뛰며 최종 사용자는 Compliant(준수) 상태로 전환됩니다.

감사 요건

감사 요건은 내부용으로 지정되며, 에이전트는 정책 평가 중의 통과 또는 장애 상태에 관계없이 최종 사용자의 입력이나 메시지를 표시하지 않습니다.

최종 사용자가 안티바이러스 프로그램의 최신 버전을 사용하고 있는지를 확인하기 위해 필수 정책 조건을 생성하는 프로세스를 예로 들어 보겠습니다. 해당 조건을 정책 조건으로 실제로 시행하기 전에 미준수 최종 사용자를 찾으려는 경우 이 조건을 감사 요건으로 지정할 수 있습니다.

가시성을 위한 요구 사항

정책 평가 중에 에이전트는 5~10분마다 가시성 요건에 대한 규정 준수 데이터를 보고합니다.

규정 미준수 상태로 중단된 클라이언트 시스템

필수 요건을 충족하도록 클라이언트를 교정할 수 없는 경우에는 포스처 상태가 "미준수"로 변경되며 에이전트 세션이 격리됩니다. 클라이언트 머신에서 이 "규정 미준수" 상태를 벗어나려면 에이전트가 클라이언트 머신에서 다시 Posture Assessment를 시작하도록 포스처 세션을 다시 시작해야 합니다. 다음과 같이 포스처 세션을 다시 시작할 수 있습니다.

- 802.1X 환경의 유선 및 무선 CoA(Change of Authorization)에서
  - 새 권한 부여 프로파일 페이지에서 새 권한 부여 프로파일을 생성할 때 특정 권한 부여 정책에 대한 재인증 타이머를 구성할 수 있습니다. 자세한 내용은 20-11페이지의 "다운로드 가능한 ACL에 대한 권한 구성" 섹션을 참고해 주십시오.
  - 유선 사용자는 연결을 끊은 후 네트워크에 다시 연결하면 격리 상태를 벗어날 수 있습니다. 무선 환경에서 사용자는 WLC(Wireless LAN Controller)에서 연결을 끊고, 네트워크에 대한 재연결을 시도하기에 앞서 사용자 유휴 시간 초과 기간이 만료할 때까지 기다려야 합니다.
- VPN 환경에서 VPN 터널 연결을 끊고 다시 연결합니다.

클라이언트 포스처 요건 생성

요건 창에서 요건을 생성할 수 있습니다. 이 창에서는 사용자 맞춤화 조건과 Cisco 정의 조건 및 교정 작업을 연결할 수 있습니다. 요건 창에서 생성하여 저장한 사용자 맞춤화 조건과 교정 작업은 개별 목록 창에서 확인할 수 있습니다.

시작하기 전에

- 포스처에 대한 AUP(Acceptable Use Policy)를 이해해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**포스처**)** > **Requirements(**요건**)**.

단계 **2** **Requirements(**요건**)** 창에서 값을 입력합니다.

단계 **3** **Done(**완료**)**을 클릭하여 포스처 요건을 읽기 전용 모드로 저장합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

Posture Reassessment 컨피그레이션 설정

다음 표에서는 Posture Reassessment를 구성하는 데 사용할 수 있는 Posture Reassessment Configurations(Posture Reassessment 컨피그레이션) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **Reassessments(**재평가**)**입니다.

표 ***18: Posture Reassessment*** 컨피그레이션 설정

필드 이름	사용 지침
Configuration Name(컨피그레이션 이름**)**	PRA 컨피그레이션의 이름을 입력합니다.
Configuration Description(컨피그레이션 설명**)**	PRA 컨피그레이션에 대한 설명을 입력합니다.
Use Reassessment Enforcement?(재평가 시행 사용**?)**	사용자 ID 그룹에 대해 PRA 컨피그레이션을 적용하려면 확인란을 선택합니다.

필드 이름	사용 지침
Enforcement Type(시행 유형**)**	시행할 작업을 선택합니다. • **Continue(**계속**)**: 사용자가 포스처 요건에 관계없이 별도의 작업을 수행하지 않고도 클라이언트를 교정할 수 있는 권한 있는 액세스 권한을 계속 소유합니다. • **Logoff(**로그오프**)**: 클라이언트가 규정을 준수하지 않으면 사용자가 네트워크에서 강제로 로그오프됩니다. 클라이언트가 다시 로그인할 때의 규정 준수 상태는 Unknown(알 수 없음)입니다. • **Remediate(**교정**)**: 클라이언트가 규정을 준수하지 않으면 에이전트가 지정된 시간 동안 교정이 수행되기를 기다립니다. 클라이언트가 교정되면 에이전트는 정책 서비스 노드에 PRA 보고서를 보냅니다. 클라이언트에서 교정이 무시되면 에이전트는 정책 서비스 노드에 로그오프 요청을 보내 네트워크에서 클라이언트를 강제로 로그오프합니다. 포스처 요건이 필수로 설정되어 있는 경우 PRA 실패 작업의 결과로 RADIUS 세션이 해제되며, 클라이언트를 다시 포스처하려면 새 RADIUS 세션을 시작해야 합니다. 포스처 요건이 선택으로 설정되어 있는 경우 클라이언트의 에이전트를 통해 사용자는 에이전트에서 Continue(계속) 옵션을 클릭할 수 있습니다. 이 경우 사용자는 제한 없이 현재 네트워크를 계속 사용할 수 있습니다.
Interval(간격**)**	첫 번째 로그인 성공 이후 클라이언트에서 PRA를 시작할 시간 간격을 분 단위로 입력합니다. 기본값은 240분입니다. 최소값은 60분이고 최대값은 1,440분입니다.

필드 이름	사용 지침
Grace time(유예 시간**)**	클라이언트가 교정을 완료할 수 있는 시간 간격을 분 단위로 입력합니다. 유예 시간은 0일 수 없으며 PRA 간격보다 커야 합니다. 이 시간의 범위는 기본 최소 간격(5분)에서 최소 PRA 간격 사이입니다. 최소값은 5분이고 최대값은 60분입니다. 참고 클라이언트에 대한 Posture Reassessment가 실패한 후의 시행 유형이 교정 작업으로 설정되어 있는 경우에만 유예 시간이 활성화됩니다.
Select User Identity Groups(사용자 **ID** 그룹 선택**)**	PRA 컨피그레이션에 대해 고유한 그룹 또는 고유한 그룹 조합을 선택합니다.
PRA configurations(PRA 컨피그레이션**)**	기존 PRA 컨피그레이션 및 PRA 컨피그레이션에 연결된 사용자 ID 그룹이 표시됩니다.

관련 항목

포스처 임대, 13 페이지
정기적 재평가, 14 페이지
Posture Assessment 옵션, 64 페이지
포스처 교정 옵션, 65 페이지
포스처를 위한 사용자 맞춤화 조건, 66 페이지
사용자 맞춤화 포스처 교정 작업, 67 페이지
정기 재평가 구성, 14 페이지

포스처를 위한 사용자 맞춤화 권한

사용자 맞춤화 권한은 Cisco ISE에서 정의하는 표준 권한 부여 프로파일입니다. 표준 권한 부여 프로파일은 엔드포인트의 일치하는 규정 준수 상태에 따라 액세스 권한을 설정합니다. 포스처 서비스는 포스처를 포괄적으로 알 수 없음, 규정 준수 및 규정 미준수 프로파일로 분류합니다. Posture Policies 및 포스처 요건은 엔드포인트의 규정 준수 상태를 결정합니다.

다른 VLAN, DACL 및 다른 속성 값 쌍 집합을 가질 수 있는 엔드포인트의 알 수 없음, 규정 준수 및 규정 미준수 포스처 상태에 대해 3가지 서로 다른 권한 부여 프로파일을 생성해야 합니다. 이러한 프로파일은 3가지 권한 부여 정책에 연결될 수 있습니다. 이러한 권한 부여 정책을 구분하려면 다른 조건과 함께 Session:PostureStatus 속성을 사용해 주십시오.

알 수 없는 프로파일

엔드포인트에 대해 일치하는 Posture Policy가 정의되지 않은 경우 엔드포인트의 포스처 규정 준수 상태를 알 수 없음으로 설정할 수 있습니다. 알 수 없음 포스처 규정 준수 상태는 일치하는 Posture Policy가 활성화되어 있지만 엔드포인트에 대해 아직 Posture Assessment가 발생하지 않은 엔드포인트에 적용될 수 있습니다. 그러므로 클라이언트 에이전트에서 규정 준수 보고서를 제공하지 않은 상태입니다.

참고 모든 Cisco Network Access 디바이스에 대해 포스처를 리디렉션과 함께 사용하는 것이 좋습니다.

규정 준수 프로파일

엔드포인트에 대해 일치하는 Posture Policy가 정의된 경우 엔드포인트의 포스처 규정 준수 상태를 규정 준수로 설정할 수 있습니다. Posture Assessment가 발생하는 경우 일치하는 Posture Policy에 정의된 엔드포인트는 모든 필수 요건을 충족합니다. 포스처 규정 준수 상태인 엔드포인트의 경우 네트워크 액세스 권한이 부여될 수 있습니다.

규정 미준수 프로파일

엔드포인트에 대해 일치하는 Posture Policy가 정의되었지만 Posture Assessment 중에 모든 필수 요건을 충족하지 못할 경우 엔드포인트의 포스처 규정 준수 상태는 규정 미준수로 설정됩니다. 포스처 규정 미준수 상태의 엔드포인트가 교정 작업이 있는 포스처 요건과 일치하는 경우 자신을 교정하려면 교정 리소스에 대해 제한된 네트워크 액세스 권한이 부여되어야 합니다.

표준 권한 부여 정책 구성

권한 부여 정책 창에서 표준 권한 부여 정책과 예외 권한 부여 정책의 두 가지 권한 부여 정책 유형을 정의할 수 있습니다. 포스처 전용인 표준 권한 부여 정책은 엔드포인트의 규정 준수 상태를 기준으로 정책을 결정하는 데 사용됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**.

단계 **2** **View(**보기**)** 열에서 해당하는 Default Policy(기본 정책) 옆의 화살표 아이콘을 클릭합니다.

단계 **3** **Actions(**작업**)** 열에서 톱니바퀴 아이콘을 클릭한 다음 드롭다운 목록에서 새 권한 부여 정책을 선택합니다. **Policy Sets(**정책 집합**)** 표에 새 행이 표시됩니다.

단계 **4** 규칙 이름을 입력합니다.

단계 **5** **Conditions(**조건**)** 열에서 (+) 기호를 클릭합니다.

단계 **6** **Conditions Studio Page(**조건 스튜디오 페이지**)**에 필수 조건을 생성합니다. **Editor(**편집기**)** 섹션에서 **Click To Add an Attribute(**클릭해서 속성 추가**)** 텍스트 상자를 클릭하고 필수 사전 및 속성을 선택합니다.

Click To Add An Attribute(클릭해서 속성 추가**)** 텍스트 상자에 라이브러리 조건을 끌어다 놓을 수 있습니다.

단계 **7** **Use(**사용**)**를 클릭하여 새 표준 권한 부여 정책을 읽기 전용 모드로 저장합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

포스처를 통한 네트워크 드라이브 매핑 모범 사례

Windows 엔드포인트의 포스처 평가 중에 엔드포인트 사용자가 데스크톱에 액세스하는 데 지연이 발생할 수 있습니다. 이는 Windows가 사용자에게 데스크톱 액세스를 제공하기 전에 파일 서버 드라이브 문자 매핑을 복원하려고 시도하기 때문일 수 있습니다. 포스처 중에 지연을 방지하는 모범 사례는 다음과 같습니다.

- 엔드포인트가 Active Directory 서버에 연결할 수 있어야 합니다. AD에 연결하지 않으면 파일 서버 드라이브 문자를 매핑할 수 없기 때문입니다. 포스처(AnyConnect ISE Posture 에이전트 사용)가 트리거되면 AD에 대한 액세스가 차단되어 로그인이 지연됩니다. 포스처 완료 전에 포스처 교정 ACL을 사용하여 AD 서버에 대한 액세스를 제공합니다.
- 포스처가 완료될 때까지 로그인 스크립트에 대한 지연을 설정한 다음 Persistence(지속) 속성을 NO(아니요)로 설정해야 합니다. Windows는 로그인 중에 모든 네트워크 드라이브를 다시 연결하려고 시도하는데 AnyConnect ISE Posture 에이전트가 전체 네트워크 액세스 권한을 얻을 때까지 이 작업을 수행할 수 없습니다.

AnyConnect 스텔스 모드 워크플로우 구성

스텔스 모드에서 AnyConnect를 구성하는 프로세스에는 일련의 단계가 포함됩니다. Cisco ISE에서 다음 단계를 수행하십시오.

단계 **1** AnyConnect 에이전트 프로파일을 생성합니다(AnyConnect 에이전트 프로파일을 생성합니다. 참조).

단계 **2** AnyConnect 패키지용 AnyConnect 컨피그레이션을 생성합니다(AnyConnect 패키지의 AnyConnect 컨피그레이션 생성 참조).

단계 **3** Cisco ISE에서 Open DNS 프로파일을 업로드합니다(Cisco ISE에서 Open DNS 프로파일 업로드 참조).

단계 **4** 클라이언트 프로비저닝 정책을 생성합니다(클라이언트 프로비저닝 정책 생성 참조).

단계 **5** 포스처 조건을 생성합니다(포스처 조건 생성 참조).

단계 **6** 포스처 교정을 생성합니다(포스처 교정 생성 참조).

단계 **7** 클라이언트리스 모드에서 포스처 요건을 생성합니다(스텔스 모드에서 포스처 요건 생성 참조).

단계 **8** 포스처 정책을 생성합니다(포스처 정책 생성 참조).

단계 **9** 권한 부여 프로파일을 구성합니다.

a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**인증**)** > **Authorization Profiles(**인증 프로파일**)**을 선택합니다.

b) **Add(**추가**)**를 클릭하고 프로파일의 **Name(**이름**)**을 입력합니다.

c) Common Tasks(일반 작업)에서 **Web Redirection(**웹 리디렉션**)(CWA, MDM, NSP, CPP)**을 활성화하고 드롭다운 목록에서 **Client provisioning (Posture)(**클라이언트 프로비저닝**(**포스처**))**을 선택합니다. 그런 다음 리디렉

션 **ACL** 이름을 입력하고 클라이언트 프로비저닝 포털 값을 선택합니다. **Work Centers(**작업 센터**)** > **Posture(**포스처**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Client Provisioning Portal(**클라이언트 프로비저닝 포털**)**에서 새로운 클라이언트 프로비저닝 포털을 편집하거나 생성할 수 있습니다.

단계 **10** 권한 부여 정책을 구성합니다.

a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**

b) > 기호를 클릭하여 **Authorization Policy(**권한 부여 정책**)**를 선택합니다. 그런 다음 + 아이콘을 클릭하여 **Session:Posture Status EQUALS Unknown** 조건과 이전에 구성된 권한 부여 프로파일을 특징으로 하는 새 권한 부여 규칙을 생성합니다.

c) 이전 규칙 위에 **Session:Posture Status EQUALS NonCompliant** 조건을 갖춘 권한 부여 규칙과 **Session:Posture Status EQUALS Compliant** 조건을 특징으로 하는 다른 권한 부여 규칙을 새로 생성합니다.

AnyConnect 에이전트 프로파일을 생성합니다.

시작하기 전에

MAC 및 Windows OS용 AnyConnect Cisco 패키지와 AnyConnect 컴플라이언스 모듈을 업로드해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**.

단계 **2** **Add(**추가**)** 드롭 다운 목록에서 **AnyConnect ISE Posture Profile(AnyConnect IST** 포스처 프로파일**)**을 선택합니다.

단계 **3** **Posture Agent Profile Settings(**포스처 에이전트 프로파일 설정**)** 드롭다운 목록에서 **AnyConnect**를 선택합니다.

단계 **4** **Name(**이름**)** 필드에 필요한 이름(예: AC_Agent_Profile)을 입력합니다.

단계 **5** **Agent Behavior(**에이전트 동작**)** 섹션에서 **Stealth Mode(**스텔스 모드**)** 매개 변수를 **Enabled(**사용**)** 로 선택합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

AnyConnect 패키지용 AnyConnect 구성을 생성해야 합니다.

AnyConnect 패키지의 AnyConnect 컨피그레이션 생성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**.

단계 **2** **Add(**추가**)** 드롭다운 목록에서 **AnyConnect Configuration(AnyConnect** 컨피그레이션**)**을 선택합니다.

단계 **3** **Select AnyConnect Package(AnyConnect** 패키지 선택**)** 드롭다운 목록에서 필요한 AnyConnect 패키지(예: AnyConnectDesktopWindows 4.4.117.0)를 선택합니다.

단계 4 **Configuration Name(**컨피그레이션 이름**)** 텍스트 상자에 원하는 이름(예: AC_Win_44117)을 입력합니다.

단계 5 **Compliance Module(**컴플라이언스 모듈**)** 드롭다운 목록에서 필요한 규정 준수 모듈(예: AnyConnectComplianceModuleWindows 4.2.437.0)을 선택합니다.

단계 6 **AnyConnect Module Selection(AnyConnect** 모듈 선택**)** 섹션에서 **ISE Posture** 및 **Network Access Manager** 확인란을 선택합니다.

단계 7 **Profile Selection(**프로파일 선택**)** 섹션의 **ISE Posture**) 드롭다운 목록에서 AnyConnect 에이전트 프로파일(예: AC_Agent_Profile)을 선택합니다.

단계 8 **Network Access Manager** 드롭다운 목록에서 필요한 AnyConnect 에이전트 프로파일(예: AC_Agent_Profile)을 선택합니다.

다음에 수행할 작업

Open DNS 프로파일을 업로드하여 클라이언트에 푸시해야 합니다.

Cisco ISE에서 Open DNS 프로파일 업로드

Open DNS 프로파일이 클라이언트에 푸시됩니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**.

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

단계 3 **Category(**범주**)** 드롭다운 목록에서 **Customer Created Packages(**고객이 생성한 패키지**)**를 선택합니다.

단계 4 **Type(**유형**)** 드롭다운 목록에서 **AnyConnect Profile(AnyConnect** 프로파일**)**을 선택합니다.

단계 5 **Name(**이름**)** 텍스트 상자에, 필요한 이름(예: OpenDNS)을 입력합니다.

단계 6 **Browse(**찾아보기**)**를 클릭하고 로컬 디스크에서 JSON 파일을 찾습니다.

단계 7 **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

클라이언트 프로비저닝 정책을 생성해야 합니다.

클라이언트 프로비저닝 정책 생성

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Client Provisioning(**클라이언트 프로비저닝**)**.

단계 2 필요한 규칙을 생성합니다(예: Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117).

다음에 수행할 작업

포스처 조건을 생성해야 합니다.

포스처 조건 생성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **File Condition(**파일 조건**)**.

단계 **2** 필요한 이름(예: filechk)을 입력합니다.

단계 **3** **Operating Systems(**운영체제**)** 드롭다운 목록에서 Windows 7(All)(Windows 7(모두))을 선택합니다.

단계 **4** **File Type(**파일 유형**)** 드롭다운 목록에서 FileExistence를 선택합니다.

단계 **5** **File Path(**파일 경로**)** 드롭다운 목록에서 ABSOLUTE_PATH C:\test.txt를 선택합니다.

단계 **6** **File Operator(**파일 연산자**)** 드롭다운 목록에서 DoesNotExist를 선택합니다.

다음에 수행할 작업

포스처 교정을 생성해야 합니다.

포스처 교정 생성

파일 조건은 엔드포인트에 test.txt 파일이 있는지 확인합니다. 해당 파일이 없는 경우 교정에서 USB 포트를 차단하고 USB 디바이스를 사용하여 파일을 설치하지 못하게 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Remediation Actions(**교정 작업**)** > **USB Remediations(USB** 교정**)**로 이동합니다.

단계 **2** 원하는 이름(예: clientless_mode_block)을 입력합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

포스처 요건을 생성해야 합니다.

스텔스 모드에서 포스처 요건 생성

요건 페이지에서 교정 작업을 생성하면 스텔스 모드에 적용 가능한 교정(안티멀웨어, 프로그램 실행, 패치 관리, USB, Windows Server Update Services 및 Windows Update)만 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**.

단계 **2** 필요한 포스처 요건을 생성합니다(예: Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Posture Type=AnyConnect Stealth met if Condition=filechk then Remediation Actions=clientless_mode_block).

다음에 수행할 작업

포스처 정책을 생성해야 합니다.

포스처 정책 생성

시작하기 전에

포스처 정책 요건을 확인하고 정책이 클라이언트리스 모드에서 생성되었는지 파악합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Posture(**포스처**)**를 선택합니다.

단계 **2** 필요한 규칙을 생성합니다. 예를 들어 ID 그룹=모두, 운영체제=Windows 7(전체) 및 규정 준수 모듈=4.x 이상이고, 포스처 유형=AnyConnect 스텔스면 요건=win7Req입니다.

참고 URL 리디렉션이 없는 클라이언트 프로비저닝의 경우 네트워크 액세스 또는 Radius 관련 속성으로 조건을 구성해도 작동하지 않으며, Cisco ISE 서버에서 특정 사용자에 대한 세션 정보를 사용할 수 없어 클라이언트 프로비저닝 정책의 일치가 실패할 수 있습니다. 그러나 Cisco ISE에서는 외부에서 추가된 ID 그룹에 대한 조건을 구성할 수 있습니다.

AnyConnect 스텔스 모드 알림 활성화

Cisco ISE는 AnyConnect 스텔스 모드 구축을 위한 몇 가지 새로운 실패 알림을 제공합니다. 스텔스 모드에서 실패 알림을 활성화하면 유선, 무선 또는 VPN 연결의 문제를 식별하는 데 도움이 됩니다. 스텔스 모드에서 알림을 활성화하려면

참고 AnyConnect 4.5.0.3040 이상 버전은 스텔스 모드 알림을 지원합니다.

시작하기 전에

스텔스 모드에서 AnyConnect를 구성합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**를 선택합니다.

단계 **2** **Add(**추가**)** > **AnyConnect ISE Posture Profile(AnyConnect IST** 포스처 프로파일**)**을 선택합니다.

단계 **3** **Select a Category(**범주 선택**)** 드롭다운 목록에서 **AnyConnect**를 선택합니다.

단계 **4** **Agent Behavior(**에이전트 동작**)** 섹션에서 **Enable notifications in stealth mode(**스텔스 모드에서 알림 활성화**)** 옵션에 대해 **Enabled(**활성화됨**)**를 선택합니다.

Cisco 임시 에이전트 구성 워크플로우

Cisco Temporal Agent를 구성하는 프로세스에는 일련의 단계가 포함됩니다. Cisco ISE에서 다음 단계를 수행하십시오.

단계 **1** 포스처 조건 생성

단계 **2** 포스처 요건 생성

단계 **3** 포스처 정책 생성

단계 **4** 클라이언트 프로비저닝 정책 구성

단계 **5** 권한 부여 프로파일을 구성합니다.

a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책 요소**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**.

b) **Add(**추가**)**를 클릭하고 프로파일의 **Name(**이름**)**을 입력합니다.

c) Common Tasks(일반 작업)에서 **Web Redirection(**웹 리디렉션**)(CWA, MDM, NSP, CPP)**을 활성화하고 드롭다운 목록에서 **Client provisioning (Posture)(**클라이언트 프로비저닝(포스처)**)**을 선택합니다. 그런 다음 리디렉션 **ACL** 이름을 입력하고 클라이언트 프로비저닝 포털 값을 선택합니다. **Work Centers(**작업 센터**)** > **Posture(**포스처**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Client Provisioning Portal(**클라이언트 프로비저닝 포털**)**에서 새로운 클라이언트 프로비저닝 포털을 편집하거나 생성할 수 있습니다.

단계 **6** 권한 부여 정책을 구성합니다.

a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**.

b) > 기호를 클릭하여 **Authorization Policy(**권한 부여 정책**)**를 선택합니다. 그런 다음 + 아이콘을 클릭하여 **Session:Posture Status EQUALS Unknown** 조건과 이전에 구성된 권한 부여 프로파일을 특징으로 하는 새 권한 부여 규칙을 생성합니다.

c) 이전 규칙 위에 **Session:Posture Status EQUALS NonCompliant** 조건을 갖춘 권한 부여 규칙과 **Session:Posture Status EQUALS Compliant** 조건을 특징으로 하는 다른 권한 부여 규칙을 새로 생성합니다.

단계 **7** Cisco Temporal Agent 다운로드 및 실행

포스처 조건 생성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** > **File Condition(**파일 조건**)**.

단계 **2** 필요한 이름(예: filecondwin)을 입력합니다.

단계 **3** **Operating Systems(**운영체제**)** 드롭다운 목록에서 Windows 7(All)(Windows 7(모두))을 선택합니다.

단계 **4** **File Type(**파일 유형**)** 드롭다운 목록에서 FileExistence를 선택합니다.

단계 **5** **File Path(**파일 경로**)** 드롭다운 목록에서 ABSOLUTE_PATH C:\test.txt를 선택합니다.

단계 **6** **File Operator(**파일 연산자**)** 드롭다운 목록에서 DoesNotExist를 선택합니다.

포스처 요건 생성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Posture(**포스처**)** > **Requirements(**요건**)**.

단계 **2** **Edit(**편집**)** 드롭다운 목록에서 **Insert New Requirement(**새 요건 삽입**)**를 선택합니다.

단계 **3** **Name(**이름**)**, **Operating Systems(**운영체제**)**, **Compliance Module(**규정 준수 모듈**)**(예: Name(이름): filereqwin, Operating Systems(운영체제): Windows All, Compliance Module(규정 준수 모듈): 4.x or later(4.x 이상))을 입력합니다.

단계 **4** **Posture Type(**포스처 유형**)** 드롭다운에서 **Temporal Agent**를 선택합니다.

단계 **5** 필요한 조건(예: filecondwin)을 선택합니다.

참고 Cisco Termporal Agent의 경우, **Requirements(**요건**)** 페이지에서 **Installation(**설치**)** 확인 유형을 포함하는 패치 관리 조건만 볼 수 있습니다.

단계 **6** **Message Text Only(**메시지 텍스트 전용**)** 교정 작업을 선택합니다.

참고 Temporal Agent는 AnyConnect 4.x 이상에서 지원됩니다.

포스처 정책 생성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Posture(**포스처**)**.

단계 **2** 필수 규칙을 생성합니다(예: Name=filepolicywin, Identity Groups=Any, Operating Systems=Windows All, Compliance Module=4.x or later, Posture Type=Temporal Agent, and Requirements=filereqwin).

클라이언트 프로비저닝 정책 구성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Client Provisioning(**클라이언트 프로비저닝**)**.

단계 **2** 필요한 규칙을 생성합니다(예: Rule Name=Win, Identity Groups=Any, Operating Systems=Windows All, Other Conditions=Conditions, Results=CiscoTemporalAgentWindows4.5).

Cisco Temporal Agent 다운로드 및 실행

단계 **1** SSID에 연결합니다.

단계 **2** 브라우저를 실행하면 클라이언트 프로비저닝 포털로 리디렉션됩니다.

단계 **3** **Start(**시작**)**를 클릭합니다. 이를 통해 Cisco Temporal Agent가 설치되어 실행 중인지가 확인됩니다.

단계 **4** **This My First Time Here(**처음 사용하는 경우**)**를 클릭합니다.

단계 **5** **Click Here to Download and Launch Cisco Temporal Agent(Cisco Temporal Agent**를 다운로드하고 실행하려면 여기를 클릭**)**를 선택합니다.

단계 **6** Windows 또는 Mac OSX에서 각각 Cisco Temporal Agent의 .exe 또는 .dmg 파일을 저장합니다. Windows의 경우 .exe 파일을 실행하고 Mac OSX의 경우 .dmg 파일을 두 번 클릭한 다음 acisetempagent 앱을 실행합니다.
Cisco Temporal Agent는 클라이언트를 검사하며, 규정 미준수 확인에서 적십자 마크와 같은 결과를 표시합니다.

포스처 문제 해결 도구

포스처 문제 해결 도구는 포스처 검사 실패의 원인을 찾아 다음 사항을 식별하는 데 도움이 됩니다.

- 포스처에서 성공한 엔드포인트와 실패한 엔드포인트
- 엔드포인트가 포스처에서 실패한 경우 포스처 프로세스에서 실패한 단계
- 통과 및 실패한 필수 검사와 선택적 검사

사용자 이름, MAC 주소 및 포스처 상태와 같은 매개변수에 따라 요청을 필터링하여 이러한 정보를 확인할 수 있습니다.

엔드포인트 로그인 자격 증명 구성

Endpoint Login Configuration(엔드포인트 로그인 컨피그레이션**)** 창에서는 Cisco ISE가 클라이언트에 로그인할 수 있도록 로그인 자격 증명을 구성할 수 있습니다. 이 창에 구성된 로그인 자격 증명은 다음 Cisco ISE 기능에서 사용됩니다.

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Endpoint Scripts(**엔드포인트 스크립트**)** > **Settings(**설정**)**를 선택합니다.

다음 탭이 표시됩니다.

- **Windows Domain User(Windows** 도메인 사용자**)**: Cisco ISE가 SSH를 통해 클라이언트에 로그인하는 데 사용해야 하는 도메인 자격 증명을 구성합니다. 더하기 아이콘을 클릭하고 필요한 만큼 Windows 로그인을 입력합니다. 각 도메인에 대해 **Domain(**도메인**)**, **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 필요한 값을 입력합니다. 도메인 자격 증명을 구성하는 경우 **Windows Local User(Windows** 로컬 사용자**)** 탭에 구성된 로컬 사용자 자격 증명이 무시됩니다.

- **Windows Local User(Windows** 로컬 사용자**)**: Cisco ISE가 SSH를 통해 클라이언트에 액세스하는 데 사용하는 로컬 계정을 구성합니다. 로컬 계정은 Powershell 및 Powershell 원격을 실행할 수 있어야 합니다.
- **MAC Local User(MAC** 로컬 사용자**)**: Cisco ISE가 SSH를 통해 클라이언트에 액세스하는 데 사용하는 로컬 계정입니다. 로컬 계정은 Powershell 및 Powershell 원격을 실행할 수 있어야 합니다.

엔드포인트 스크립트 설정

이 페이지에서는 엔드포인트 스크립트 및 에이전트리스 포스처에 대한 옵션을 구성합니다.

- **Upload endpoint script execution logs to ISE(**엔드포인트 스크립트 실행 로그를 **ISE**에 업로드**)**: 기본적으로 활성화되어 있으며, Cisco ISE에 엔드포인트 스크립트를 업로드할 수 있습니다. 이 기능을 비활성화하면 엔드포인트 스크립트가 비활성화되므로 엔드포인트 스크립트를 업로드하거나 실행할 수 없습니다.
- **Endpoint script execution verbose logging(**엔드포인트 스크립트 실행에 대한 자세한 정보 로깅**)**: 디버깅을 위해 자세한 정보 로깅을 활성화합니다.
- **Endpoint processor batch size(**엔드포인트 프로세서 배치 크기**)**: 네트워크 로드 및 시스템 성능에 맞게 이를 조정할 수 있습니다.
- **Endpoints processing concurrency for MAC(MAC**의 경우 엔드포인트 처리 동시성**)**
- **Endpoints processing concurrency for Windows(Windows**의 경우 엔드포인트 처리 동시성**)**
- **Maximum retry attempts for OS identification(OS** 식별을 위한 재시도의 최대 횟수**)**
- **Delay between retries for OS identification (msec)(OS** 식별을 위한 재시도 간 지연**(**밀리초**))**
- **Endpoint pagination batch size(**엔드포인트 페이지 매김 배치 크기**)**
- **Log retention period on Endpoints (Days)(**엔드포인트의 로그 보존 기간**(**일**))**
- **Connection Time out (sec)(**연결 시간 초과**(**초**))**
- **Max-retry attempts for Connection(**연결 재시도 최대 횟수**)**
- **Port Number for Powershell(Powershell**용 포트 번호**)**: 표준이 아닌 포트 번호를 사용하려면 이 값을 변경합니다.
- **Port Number for SSH Connection(SSH** 연결용 포트 번호**)**: 표준이 아닌 포트 번호를 사용하려면 이 값을 변경합니다.

Cisco ISE에서 클라이언트 프로비저닝 구성

사용자가 클라이언트 프로비저닝 리소스를 다운로드하고 에이전트 프로파일을 구성할 수 있도록 허용하려면 클라이언트 프로비저닝을 활성화합니다. Windows 클라이언트, Mac OS X 클라이언트, 용

에이전트 프로파일과 개인 디바이스용 기본 신청자 프로파일을 구성할 수 있습니다. 클라이언트 프로비저닝을 비활성화하면 네트워크 액세스를 시도하는 사용자에게 클라이언트 프로비저닝 리소스를 다운로드할 수 없음을 나타내는 경고 메시지가 표시됩니다.

시작하기 전에

프록시를 사용하고 원격 시스템에서 클라이언트 프로비저닝 리소스를 호스팅하는 경우 프록시가 클라이언트가 해당 원격 위치에 액세스하도록 허용하는지 확인합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Client Provisioning(**클라이언트 프로비저닝**)** 또는 **Work Centers(**작업 센터**)** > **Posture(**포스처**)** > **Settings(**설정**)** > **Software Updates(**소프트웨어 업데이트**)** > **Client Provisioning(**클라이언트 프로비저닝**)**.

단계 **2** **Enable Provisioning(**프로비저닝 활성화**)** 드롭다운 목록에서 **Enable(**활성화**)** 또는 **Disable(**비활성화**)**을 선택합니다.

단계 **3** **Enable Automatic Download(**자동 다운로드 활성화**)** 드롭다운 목록에서 **Enable(**활성화**)**을 선택합니다.

피드 다운로드에는 사용 가능한 모든 클라이언트 프로비저닝 리소스가 포함됩니다. 이러한 리소스 중 일부는 구축과 관련이 없을 수 있습니다. Cisco에서는 이 옵션을 설정하는 대신 가능한 경우 항상 리소스를 수동으로 다운로드할 것을 권장합니다.

단계 **4** 업데이트 피드 **URL** 텍스트 상자에 Cisco ISE가 시스템 업데이트를 검색하는 URL을 지정합니다. 예를 들어 클라이언트 프로비저닝 리소스 다운로드를 위한 기본 URL은 https://www.cisco.com/web/secure/spa/provisioning-update.xml입니다.

단계 **5** 디바이스에 대한 클라이언트 프로비저닝 리소스가 없는 경우 다음 옵션 중 하나를 선택합니다.

- **Allow Network Access(**네트워크 액세스 허용**)**: 사용자가 기본 신청자 마법사를 설치 및 시작하지 않고도 네트워크에서 디바이스를 등록할 수 있습니다.
- **Apply Defined Authorization Policy(**정의된 권한 부여 정책 적용**)**: 사용자가 기본 신청자 프로비저닝 프로세스에 포함되지 않는 표준 인증 및 권한 부여 정책 애플리케이션을 통해 Cisco ISE 네트워크에 액세스해야 합니다. 이 옵션을 활성화하는 경우 사용자 ID에 적용된 클라이언트 프로비저닝 정책에 따라 사용자 디바이스에서 표준 등록이 진행됩니다. 사용자 디바이스가 Cisco ISE 네트워크에 액세스하려면 인증서가 필요한 경우, 사용자 맞춤화 가능한 사용자용 텍스트 필드를 사용하여 유효한 인증서를 얻고 적용하는 방법을 설명하는 자세한 지침도 사용자에게 제공해야 합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

클라이언트 프로비저닝 리소스 정책을 구성합니다.

클라이언트 프로비저닝 리소스

엔드포인트가 네트워크에 연결되고 나면 클라이언트 프로비저닝 리소스가 엔드포인트에 다운로드됩니다. 클라이언트 프로비저닝 리소스는 데스크톱용 규정 준수 및 포스처 에이전트와 휴대폰 및 태

블릿용 기본 신청자 프로파일로 구성됩니다. 클라이언트 프로비저닝 정책은 네트워크 세션을 시작하기 위해 이러한 프로비저닝 리소스를 엔드포인트에 할당합니다.

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**에 나열됩니다. **Add(**추가**)** 버튼을 클릭하여 다음 리소스 유형을 목록에 추가할 수 있습니다.

- **Agent resources from Cisco Site(Cisco** 사이트의 에이전트 리소스**)**: 클라이언트 프로비저닝 정책에 사용하려는 AnyConnect 및 Supplicant Provisioning(신청자 프로비저닝) 마법사를 선택합니다. Cisco는 새 리소스를 추가하고 기존 리소스를 업데이트하여 이 리소스 목록을 정기적으로 업데이트합니다. 또한 모든 Cisco 리소스 및 리소스 업데이트를 자동으로 다운로드하도록 ISE를 설정할 수도 있습니다. 더 자세한 내용은 Cisco ISE에서 클라이언트 프로비저닝 구성, 86 페이지를 참고하십시오.
- **Agent resources from local disk(**로컬 디스크의 에이전트 리소스**)**: ISE에 업로드할 PC의 리소스를 선택합니다. 로컬 머신에서 Cisco 제공 클라이언트 프로비저닝 리소스 추가, 89 페이지를 참고하십시오.
- **AnyConnect Configuration(AnyConnect** 컨피그레이션**)**: 클라이언트 프로비저닝에 사용하려는 AnyConnect PC 클라이언트를 선택합니다. 자세한 내용은 AnyConnect 컨피그레이션 생성을 참고하십시오.
- **Native Supplicant Profile(**기본 신청자 프로파일**)**: 네트워크의 설정이 포함된 휴대폰 및 태블릿용 신청자 프로파일을 구성합니다. 자세한 내용은 기본 신청자 프로파일 생성을 참고하십시오.
- **AnyConnect ISE Posture Profile(AnyConnect ISE Posture** 프로파일**)**: 에이전트 XML 프로파일을 생성 및 배포하지 않으려는 경우 여기서 AnyConnect ISE Posture를 구성합니다. AnyConnect ISE Posture 에이전트 및 ISE 포스처 프로파일 편집기에 대한 자세한 내용은 사용자의 AnyConnect 버전에 대한 AnyConnect 관리자 설명서를 참고하십시오https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html.

클라이언트 프로비저닝 리소스를 생성한 후에는 엔드포인트에 클라이언트 프로비저닝 리소스를 적용하는 클라이언트 프로비저닝 정책을 생성합니다. 클라이언트 프로비저닝 리소스 정책 구성, 117 페이지를 참고하십시오.

관련 항목

Cisco ISE에서 클라이언트 프로비저닝 구성, 86 페이지
Cisco의 클라이언트 프로비저닝 리소스 추가, 88 페이지
로컬 머신에서 Cisco 제공 클라이언트 프로비저닝 리소스 추가, 89 페이지
로컬 머신에서 AnyConnect용으로 고객이 생성한 리소스 추가, 90 페이지

Cisco의 클라이언트 프로비저닝 리소스 추가

Cisco.com에서 Windows 및 Mac OSX 클라이언트용 AnyConnect Cisco Web Agent에 대한 클라이언트 프로비저닝 리소스를 추가할 수 있습니다. 선택한 리소스 및 사용 가능한 네트워크 대역폭에 따라 Cisco ISE로 클라이언트 프로비저닝 리소스를 다운로드하는 데 몇 분이 걸릴 수 있습니다.

시작하기 전에

- Cisco ISE에 올바른 프록시 설정이 구성되어 있는지 확인합니다.
- Cisco ISE에서 클라이언트 프로비저닝을 활성화합니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(정책)** > **Policy Elements(정책 요소)** > **Results(결과)** > **Client Provisioning(클라이언트 프로비저닝)** > **Resources(리소스)**.

단계 2 **Add(추가)** > **Agent resources from Cisco site(Cisco 사이트의 에이전트 리소스)**를 선택합니다.

단계 3 **Download Remote Resources(원격 리소스 다운로드)** 대화 상자의 사용 가능한 목록에서 필수 클라이언트 프로비저닝 리소스를 하나 이상 선택합니다.

단계 4 **Save** 버튼을 클릭합니다.

다음에 수행할 작업

Cisco ISE에 클라이언트 프로비저닝 리소스를 정상적으로 추가하고 나면 클라이언트 프로비저닝 리소스 정책 구성을 시작할 수 있습니다.

로컬 머신에서 Cisco 제공 클라이언트 프로비저닝 리소스 추가

이전에 Cisco에서 다운로드한 클라이언트 프로비저닝 리소스를 로컬 디스크에서 추가할 수 있습니다.

시작하기 전에

지원되는 최신 리소스만 Cisco ISE에 업로드해야 합니다. 오래되고 지원되지 않는 리소스는 클라이언트 액세스에 심각한 문제를 일으킬 수 있습니다.

Cisco.com에서 리소스 파일을 수동으로 다운로드하는 경우 Cisco ISE 릴리스 노트에서 "Cisco ISE 오프라인 업데이트" 섹션을 참고해 주십시오.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(정책)** > **Policy Elements(정책 요소)** > **Results(결과)** > **Client Provisioning(클라이언트 프로비저닝)** > **Resources(리소스)**.

단계 2 **Add(추가)** > **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 **Browse(찾아보기)**를 클릭하여 Cisco ISE로 다운로드할 리소스 파일이 있는 로컬 머신의 디렉토리로 이동합니다.

이전에 Cisco에서 로컬 시스템에 다운로드한 AnyConnect 또는 Cisco Web Agent 리소스를 추가할 수 있습니다.

단계 5 **Submit(제출)**을 클릭합니다.

다음에 수행할 작업

Cisco ISE에 클라이언트 프로비저닝 리소스를 정상적으로 추가하고 나면 클라이언트 프로비저닝 리소스 정책을 구성할 수 있습니다.

로컬 머신에서 **AnyConnect**용으로 고객이 생성한 리소스 추가

AnyConnect 맞춤화 및 현지화 패키지와 AnyConnect 프로파일 등의 고객이 생성한 리소스를 로컬 머신에서 Cisco ISE에 추가합니다.

시작하기 전에

AnyConnect용으로 고객이 생성한 리소스가 압축 파일이며 로컬 디스크에서 사용 가능한지 확인합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**.

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

단계 **3** **Customer Created Packages(**고객이 생성한 패키지**)**를 **Category(**범주**)** 드롭다운 목록에서 선택합니다.

단계 **4** AnyConnect 리소스의 이름과 설명을 입력합니다.

단계 **5** **Browse(**찾아보기**)**를 클릭하여 Cisco ISE로 다운로드할 리소스 파일이 있는 로컬 머신의 디렉토리로 이동합니다.

단계 **6** Cisco ISE로 업로드할 다음 AnyConnect 리소스를 선택합니다.

- AnyConnect 사용자 맞춤화 번들
- AnyConnect 현지화 번들
- AnyConnect 프로파일
- AMP(Advanced Malware Protection) Enabler 프로파일

단계 **7** **Submit(**제출**)**을 클릭합니다.
Cisco ISE에 추가한 AnyConnect 리소스가 업로드한 AnyConnect 리소스 표에 표시됩니다.

다음에 수행할 작업

AnyConnect 에이전트 프로파일을 생성합니다.

기본 신청자 프로파일 생성

사용자가 Cisco ISE 네트워크에서 자신의 디바이스를 사용할 수 있도록 기본 신청자 프로파일을 생성할 수 있습니다. 사용자가 로그인하면 Cisco ISE는 필요한 신청자 프로비저닝 마법사를 선택하기 위해 해당 사용자의 권한 부여 요건과 연결한 프로파일을 사용합니다. 마법사는 네트워크에 액세스할 수 있도록 해당 사용자의 개인 디바이스를 실행 및 설정합니다.

참고 프로비저닝 마법사는 활성화된 인터페이스만 구성합니다. 이러한 이유로 유선 및 무선 연결을 사용하는 사용자는 두 인터페이스가 모두 활성화되어 있지 않는 한 두 인터페이스 모두에 대해 프로비저닝되지 않습니다.

시작하기 전에

- Cisco AnyConnect Agent, Cisco Web Agent 및 신청자 프로비저닝 마법사 설치를 활성화하려면 TCP 포트 8905를 엽니다. 포트 사용에 대한 자세한 내용은 *Cisco Identity Services Engine* 하드웨어 설치 설명서에서 "Cisco ISE 어플라이언스 포트 참조" 부록을 참고하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(정책)** > **Policy Elements(정책 요소)** > **Results(결과)** > **Client Provisioning(클라이언트 프로비저닝)** > **Resources(리소스)**.

단계 **2** **Add(추가)** > **Native Supplicant Profile(기본 신청자 프로파일)**을 선택합니다.

단계 **3** 다음 내용의 설명에 따라 프로파일을 생성합니다. 기본 신청자 프로파일 설정, 91 페이지

다음에 수행할 작업

여러 게스트 포털 지원 섹션의 설명에 따라 직원이 개인 디바이스를 네트워크에 직접 연결할 수 있는 셀프 프로비저닝 기능을 활성화합니다.

기본 신청자 프로파일 설정

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(정책)** > **Policy Elements(정책 요소)** > **Results(결과)** > **Client Provisioning Resources(클라이언트 프로비저닝 리소스)**를 선택하고 기본 신청자 프로파일을 추가하면 다음과 같은 설정이 나타납니다.

- **Name(이름)**: 생성 중인 기본 신청자 프로파일의 이름입니다. 이 프로파일이 적용할 운영체제를 선택합니다. 각 프로파일은 ISE가 클라이언트의 기본 신청자에 적용할 네트워크 연결에 대한 설정을 정의합니다.

무선 프로파일

하나 이상의 무선 프로파일(클라이언트가 사용할 수 있도록 각 SSID에 하나씩)을 구성합니다.

- **SSID Name(SSID 이름)**: 클라이언트가 연결할 SSID의 이름입니다.
- **Proxy Auto-Config File URL(프록시 자동 컨피그레이션 파일 URL)**: 클라이언트가 신청자에 대한 네트워크 컨피그레이션을 가져오기 위해 프록시에 연결할 경우 해당 프록시 서버의 URL을 입력합니다.
- **Proxy Host/IP(프록시 호스트/IP)**
- **Proxy Port(프록시 포트)**

- **Security(**보안**)**: 클라이언트가 WPA 또는 WPA2를 사용하도록 구성합니다.
- **Allowed Protocol(**허용된 프로토콜**)**: 클라이언트가 인증 서버에 연결하는 데 사용해야 하는 프로토콜(PEAP 또는 EAP-TLS)을 구성합니다.
- **Certificate Template(**인증서 템플릿**)**: TLS의 경우**Administration(**관리**)** > **System Certificates(**시스템 인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Templates(**인증서 템플릿**)**에 정의된 인증서 템플릿 중 하나를 선택합니다.

선택적 설정은 선택적 설정 - *Windows*용 섹션에 설명되어 있습니다.

iOS 설정

- **Enable if target network is hidden(**대상 네트워크가 숨겨진 경우 활성화**)**

유선 프로파일

- **Allowed Protocol(**허용된 프로토콜**)**: 클라이언트가 인증 서버에 연결하는 데 사용해야 하는 프로토콜(PEAP 또는 EAP-TLS)을 구성합니다.
- **Certificate Template(**인증서 템플릿**)**: TLS의 경우 Administration(관리) > System Certificates(시스템 인증서) > Certificate Authority(인증 기관) > Certificate Templates(인증서 템플릿)에 정의된 인증서 템플릿 중 하나를 선택합니다.

선택적 설정 **- Windows**용

Optional(선택**)**을 펼치면 Windows 클라이언트에 대해 다음 필드도 사용 가능합니다.

- **Authentication Mode(**인증 모드**)**: 권한 부여용 자격 증명으로 User(사용자) 또는 Machine(머신)을 사용할지 아니면 둘 다 사용할지를 결정합니다.
- **Automatically use logon name and password (and domain if any)(**로그온 이름 및 비밀번호를 자동으로 사용**(**도메인이 있는 경우 도메인도 사용**))**: 인증 모드로 User(사용자)를 선택한 경우 로그온 및 비밀번호를 사용할 수 있으면 사용자에게 메시지를 표시하지 않고 해당 정보를 사용합니다.
- **Enable Fast Reconnect(**빠른 재연결 활성화**)**: **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **PEAP**에 구성되어 있는 PEAP 프로토콜 옵션에서 세션 재개 기능이 활성화되어 있으면 사용자 자격 증명을 확인하지 않고 PEAP 세션 재개를 허용합니다.
- **Enable Quarantine Checks(**격리 확인 활성화**)**: 클라이언트가 격리되었는지를 확인합니다.
- **Disconnect if server does not present cryptobinding TLV(**서버가 암호화 바인딩 **TLV**를 제공하지 않는 경우 연결 끊기**)**: 네트워크 연결을 위해 암호화 바인딩 TLV가 지원되지 않으면 연결을 끊습니다.
- **Do not prompt user to authorize new servers or trusted certification authorities(**새 서버 또는 신뢰할 수 있는 인증 기관 권한 부여 메시지를 사용자에게 표시하지 않음**)**: 사용자 인증서를 자동으로 수락하고, 사용자에게 메시지를 표시하지 않습니다.

- **Connect even if the network is not broadcasting its name (SSID)(**네트워크가 이름**(SSID)**을 브로드캐스트하지 않아도 연결**)**: 무선 프로파일에만 해당됩니다.

다른 네트워크의 **URL** 리디렉션 없는 클라이언트 프로비저닝

서드 파티 NAC가 CoA를 지원하지 않는 경우 URL 리디렉션 없는 클라이언트 프로비저닝이 필요합니다. URL 리디렉션을 사용하거나 사용하지 않고 클라이언트 프로비저닝을 수행할 수 있습니다.

참고 URL 리디렉션을 사용하는 클라이언트 프로비저닝의 경우 클라이언트 머신에 프록시 설정이 구성된 경우 브라우저 설정의 예외 목록에 Cisco ISE를 추가해야 합니다. 이 설정은 URL 리디렉션을 사용하는 모든 플로우, BYOD, MDM, 게스트 및 포스처에 적용됩니다. 예를 들어 Windows 시스템에서 다음을 수행합니다.

1. 제어판에서 **Internet Properties(**인터넷 속성**)**을 클릭합니다.
2. **Connections(**연결**)** 탭을 선택합니다.
3. **LAN settings(LAN** 설정**)**를 클릭합니다.
4. Proxy server(프록시 서버) 영역에서 **Advanced(**고급**)**를 클릭합니다.
5. **Exceptions(**예외**)** 상자에 Cisco ISE 노드의 IP 주소를 입력합니다.
6. **OK(**확인**)**를 클릭합니다.

아래에는 여러 네트워크에 대한 리디렉션 없이 엔드포인트를 프로비저닝하기 위해 수행하는 단계가 나와 있습니다.

Dot1X EAP-TLS

1. 프로비저닝된 인증으로 Cisco ISE 네트워크 연결
2. 브라우저 창을 열고 프로비저닝 URL provisioning.cisco.com을 입력합니다.
3. 내부 사용자, AD, LDAP 또는 SAML을 통해 CP 포털에 로그인합니다.

   AnyConnect가 포스처를 수행합니다. 엔트포인트가 포스처 컴플라이언스에 따라 바른 네트워크로 이동합니다.

Dot1X PEAP

1. NSP를 통해 사용자 이름 및 비밀번호로 Cisco ISE 네트워크 연결
2. 브라우저 창을 열고 프로비저닝 URL provisioning.cisco.com을 입력합니다.
3. 내부 사용자, AD, LDAP 또는 SAML을 통해 CP 포털에 로그인합니다.

AnyConnect가 포스처를 수행합니다. 엔트포인트가 포스처 컴플라이언스에 따라 바른 네트워크로 이동합니다.

MAB(유선 네트워크)

1. Cisco ISE 네트워크 연결
2. 브라우저 창을 열고 프로비저닝 URL provisioning.cisco.com을 입력합니다.
3. 내부 사용자, AD, LDAP 또는 SAML을 통해 CP 포털에 로그인합니다.

   AnyConnect가 포스처를 수행합니다. 엔트포인트가 포스처 컴플라이언스에 따라 바른 네트워크로 이동합니다.

MAB(무선 네트워크)

1. Cisco ISE 네트워크 연결
2. 브라우저 창을 열고 프로비저닝 URL provisioning.cisco.com을 입력합니다.
3. 내부 사용자, AD, LDAP 또는 SAML을 통해 CP 포털에 로그인합니다.

   AnyConnect가 포스처를 수행합니다. 포스처는 무선 802.1X에만 시작됩니다.

AMP Enabler 프로파일 설정

다음 표에서는 AMP(Advanced Malware Protection) Enabler 프로파일 창의 필드에 대해 설명합니다.Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**입니다.

Add(추가**)** 드롭다운 화살표를 클릭하고 **AMP Enabler Profile(AMP Enabler** 프로파일**)**을 선택합니다.

표 ***19: AMP Enabler*** 프로파일 페이지

필드 이름	사용 지침
Name(이름**)**	생성할 AMP Enabler 프로파일의 이름을 입력합니다.
Description(설명**)**	AMP Enabler 프로파일에 대한 설명을 입력합니다.

필드 이름	사용 지침
Install AMP Enabler(AMP Enabler 설치**)**	• **Windows Installer(Windows** 설치 관리자**)**: Windows OS용 AMP 소프트웨어를 호스팅하는 로컬 서버의 URL을 지정합니다. AnyConnect 모듈은 이 URL을 사용하여 .exe 파일을 엔드포인트로 다운로드합니다. 파일 크기는 약 25MB입니다. • **Mac Installer(MAC** 설치 관리자**)**: Mac OSX용 AMP 소프트웨어를 호스팅하는 로컬 서버의 URL을 지정합니다. AnyConnect 모듈은 이 URL을 사용하여 .pkg 파일을 엔드포인트로 다운로드합니다. 파일 크기는 약 6MB입니다. **Check(**확인**)** 버튼을 누르면 서버와 통신하여 URL이 유효한지 확인할 수 있습니다. URL이 유효하면 "파일 발견" 메시지가 표시됩니다. 그렇지 않으면 오류 메시지가 표시됩니다.
Uninstall AMP Enabler(AMP Enabler 제거**)**	엔드포인트에서 AMP for Endpoint 소프트웨어를 제거합니다.
Add to Start Menu(시작 메뉴에 추가**)**	AMP for Endpoint 소프트웨어를 엔드포인트에 설치한 후에 엔드포인트의 Start(시작) 메뉴에서 AMP for Endpoint 소프트웨어에 대한 바로가기를 추가합니다.
Add to Desktop(데스크톱에 추가**)**	AMP for Endpoint 소프트웨어를 엔드포인트에 설치한 후에 엔드포인트의 바탕 화면에 AMP for Endpoint 소프트웨어 아이콘을 추가합니다.
Add to Context Menu(상황에 맞는 메뉴에 추가**)**	AMP for Endpoint 소프트웨어를 엔드포인트에 설치한 후에 엔드포인트의 오른쪽 클릭 상황에 맞는 메뉴에 Scan Now(지금 스캔) 옵션을 추가합니다.

내장 프로파일 편집기를 사용하여 **AMP Enabler** 프로파일 생성

Cisco ISE 내장 프로파일 편집기 또는 독립형 편집기를 사용하여 AMP Enabler 프로파일을 생성할 수 있습니다.

Cisco ISE 내장 프로파일 편집기에서 AMP Enabler 프로파일을 생성하려면 다음을 수행합니다.

시작하기 전에

- SOURCEfire 포털에서 AMP for Endpoint 소프트웨어를 다운로드하여 로컬 서버에서 호스트합니다.
- AMP for Endpoint 소프트웨어를 호스트하는 서버의 인증서를 ISE 인증서 저장소로 가져옵니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Certificates(**인증서**)** > **Trusted certificates(**신뢰할 수 있는 인증서**)**
- **AMP Enabler** 옵션이 **AnyConnect Configuration** 창(**Policy(**정책**)** > **Policy Elements(**정책 요소**)** > Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Results(**결과**)** > **Client provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)** > **Add(**추가**)** > **AnyConnect Configuration(AnyConnect** 컨피그레이션**)** > **Select AnyConnect Package(AnyConnect** 패키지 선택**)**)의 **AnyConnect Module Selection(AnyConnect** 모듈 선택**)** 및 **Profile Selection(**프로파일 선택**)** 섹션에서 선택되어 있는지 확인합니다.
- SOURCEfire 포털에 로그인하고 엔드포인트 그룹을 위한 정책을 생성하고 엔드포인트 소프트웨어용 AMP를 다운로드해야 합니다. 소프트웨어는 선택한 정책이 미리 구성되어 있는 상태로 제공됩니다. 두 개의 이미지, 즉 Windows OS를 위한 재배포 가능한 AMP for Endpoint 소프트웨어 버전과 Mac OSX용 AMP for Endpoint 소프트웨어를 다운로드해야 합니다. 다운로드된 소프트웨어는 엔터프라이즈 네트워크를 통해 액세스 가능한 서버에서 호스팅됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**.

단계 **2** **Add(**추가**)** 드롭다운을 클릭합니다.

단계 **3** **AMP Enabler Profile(AMP Enabler** 프로파일**)**을 선택하여 새 AMP Enabler 프로파일을 생성합니다.

단계 **4** 필드에 해당하는 값을 입력합니다.

독립형 편집기를 사용하여 **AMP Enabler** 프로파일 생성

AnyConnect 독립형 편집기에서 AMP Enabler 프로파일을 생성하려면 다음 단계를 수행합니다.

시작하기 전에

AnyConnect 4.1 독립형 편집기를 사용하여 프로파일의 XML 형식을 업로드해 AMP Enabler 프로파일을 생성할 수 있습니다.

- Cisco.com에서 Windows 및 Mac OS용 AnyConnect 독립형 프로파일 편집기를 다운로드합니다.
- 독립형 프로파일 편집기를 시작하고 AMP Enabler 프로파일 설정에 지정된 대로 필드에 내용을 입력합니다.
- 프로파일을 로컬 디스크에 XML 파일로 저장합니다.
- **AMP Enabler** 옵션이 **AnyConnect Configuration** 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client provisioning(**클라이언

트 프로비저닝**)** > **Resources(**리소스**)** > **Add(**추가**)** > **AnyConnect Configuration(AnyConnect** 컨피그레이션**)** > **Select AnyConnect Package(AnyConnect** 패키지 선택**))**의 **AnyConnect Module Selection(AnyConnect** 모듈 선택**)** 및 **Profile Selection(**프로파일 선택**)** 섹션에서 선택되어 있는지 확인합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Agent resources from local disk(**로컬 디스크의 에이전트 리소스**)**를 선택합니다.

단계 **4** **Customer Created Packages(**고객이 생성한 패키지**)**를 **Category(**범주**)** 드롭다운에서 선택합니다.

단계 **5** **AMP Enabler Profile(AMP Enabler** 프로파일**)**을 **Type(**유형**)** 드롭다운에서 선택합니다.

단계 **6** 이름과 설명을 입력합니다.

단계 **7** **Browse(**찾아보기**)**를 클릭하고 로컬 디스크에서 저장된 프로파일(XML 파일)을 선택합니다. 아래 예에는 사용자 맞춤화된 설치 파일이 나와 있습니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Install>
 <WindowsConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</WindowsConnectorLocation>
 <MacConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</MacConnectorLocation>
 <StartMenu>true</StartMenu>
 <DesktopIcon>false</DesktopIcon>
 <ContextIcon>true</ContextIcon>
 </Install>
 </FAConfiguration>
</FAProfile>
```

아래 예에는 사용자 맞춤화된 제거 파일이 나와 있습니다.

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Uninstall>
 </Uninstall>
 </FAConfiguration>
</FAProfile>
```

단계 **8** **Submit(**제출**)**을 클릭합니다.
새로 생성한 AMP Enabler 프로파일이 **Resources(**리소스**)** 페이지에 표시됩니다.

일반 **AMP Enabler** 설치 오류 문제 해결

Windows 또는 MAC 설치 관리자 텍스트 상자에 SOURCEfile URL을 입력하고 **Check(**확인**)**를 클릭하면 다음 오류 중 하나가 표시될 수 있습니다.

- 오류 메시지: Mac/Windows 설치 관리자 파일이 포함된 서버의 인증서를 ISE가 신뢰하지 않습니다. **Administration(**관리**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**에 신뢰 인증서를 추가해 주십시오.

  Cisco ISE 인증서 저장소로 SOURCEfire 신뢰할 수 있는 인증서를 가져오지 않은 경우 이 오류 메시지가 표시됩니다. SOURCEfire 신뢰할 수 있는 인증서를 얻어서 Cisco ISE 신뢰할 수 있는 인증서 저장소(Administration(관리) > Certificates(인증서) > Trusted Certificates(신뢰할 수 있는 인증서))로 가져옵니다.

- 오류 메시지: 이 위치에 설치 관리자 파일이 없습니다. 연결 문제 때문일 수 있습니다. 설치 관리자 텍스트 상자에 유효한 경로를 입력하거나 연결을 확인해 주십시오.

  AMP for Endpoint 소프트웨어를 호스트하는 서버가 다운되었거나 Windows 설치 관리자 또는 MAC 설치 관리자 텍스트 상자에 입력한 내용에 오타가 있으면 이 오류 메시지가 표시됩니다.

- 오류 메시지: Windows/Mac 설치 관리자 텍스트 상자에 유효한 URL이 포함되어 있지 않습니다.

  구문이 잘못된 URL 형식을 입력하면 이 오류 메시지가 표시됩니다.

Cisco ISE의 **Chromebook** 디바이스 온보딩 지원

Chromebook 디바이스는 여느 디바이스(Apple, Windows, Android)와 달리 Google 도메인에서 관리하는 디바이스이며 온보딩 지원이 제한됩니다. Cisco ISE는 네트워크에서 Chromebook 디바이스 온보딩을 지원합니다. 온보딩이란 엔드포인트가 Cisco ISE에 인증한 후 네트워크에 안전하게 연결할 수 있도록 엔드포인트로 필요한 설정 및 파일을 전달하는 프로세스를 지칭합니다. 이 프로세스에서는 인증서 프로비저닝 및/또는 기본 신청자 프로비저닝을 수행합니다. 그러나 Chromebook 디바이스에서는 인증서 프로비저닝만 수행할 수 있습니다. 기본 신청자 프로비저닝은 Google Admin Console을 통해 수행됩니다.

관리되지 않는 Chromebook 디바이스는 보안 네트워크로 온보딩할 수 없습니다.

Chromebook 온보딩 프로세스에서 사용되는 엔터티는 다음과 같습니다.

- Google 관리자
- ISE 관리자
- Chromebook 사용자/디바이스
- Google 관리자가 관리하는 Google Admin Console

Google 관리자는 다음을 수행합니다.

- 다음 라이선스 보호:

1. Google Admin Console 컨피그레이션용 Google 앱 관리자 라이선스 - URL: https://admin.google.com. 관리자는 Google Admin Console에서 조직의 사용자를 위한 Google 서비스를 관리할 수 있습니다.
2. Chromebook 디바이스 관리 라이선스 - URL: https://support.google.com/chrome/a/answer/2717664?hl=en. Chromebook 디바이스 관리 라이선스는 특정 Chromebook 디바이스에 대한 설정을 구성하고 정책을 시행하는 데 사용됩니다. 이 라이선스는 사용자 액세스 제어, 기능 맞춤화, 네트워크 액세스 구성 등을 위해 디바이스 설정에 대한 액세스 권한을 Google 관리자에게 제공합니다.

- Google 디바이스 라이선스를 사용한 Chromebook 디바이스 프로비저닝 및 등록을 원활하게 수행할 수 있도록 합니다.
- Google Admin Console을 통해 Chromebook 디바이스를 관리합니다.
- 각 Chromebook 사용자에 대해 Wi-Fi 네트워크 컨피그레이션을 설정하고 관리합니다.
- Chromebook 디바이스에 설치할 애플리케이션 및 강제 익스텐션을 구성하여 Chromebook 디바이스를 관리합니다. Chromebook 디바이스를 온보딩하려면 Chromebook 디바이스에 Cisco Network Setup Assistant 익스텐션을 설치해야 합니다. 그러면 Chromebook 디바이스가 Cisco ISE에 연결하여 ISE 인증서를 설치할 수 있습니다. 인증서 설치 작업은 관리되는 디바이스에 대해서만 허용되므로 익스텐션은 강제로 설치됩니다.
- 서버 검증 및 보안 연결 기능을 제공하려면 Cisco ISE 인증서가 Google Admin Console에 설치되어 있는지 확인합니다. 디바이스 또는 사용자에 대해 인증서를 생성해야 하는지 여부는 Google 관리자가 결정합니다. Cisco ISE는 다음을 수행할 수 있는 옵션을 제공합니다.
  - Chromebook 디바이스를 공유하지 않는 단일 사용자용으로 인증서를 생성합니다.
  - 여러 사용자가 공유하는 Chromebook 디바이스용으로 인증서를 생성합니다. 필요한 추가 컨피그레이션은 Google Admin Console에서 네트워크 및 강제 익스텐션 구성 섹션의 5단계를 참고하십시오.

  Chromebook 디바이스에서 인증서 프로비저닝을 수행하도록 ISE를 신뢰하고, EAP-TLS 인증서 기반 인증을 허용하기 위해 Google 관리자는 ISE 서버 인증서를 설치합니다. Google Chrome 버전 37 이상은 Chromebook 디바이스에 대한 인증서 기반 인증을 지원합니다. Google 관리자는 Google Admin Console에서 ISE 프로비저닝 애플리케이션을 로딩해야 하며 ISE에서 인증서를 가져오도록 Chromebook 디바이스에 해당 애플리케이션을 제공해야 합니다.
- 권장 Google 호스트 이름이 SSL 보안 연결을 위해 WLC에 구성된 ACL 정의 목록에서 허용되는지 확인합니다. Google Support(Google 지원) 페이지의 허용되는 권장 호스트 이름을 참고하십시오.

ISE 관리자는 다음을 수행합니다.

- 인증서 템플릿 구조를 포함하는 Chromebook OS에 대한 기본 신청자 프로파일 정의
- Chromebook 사용자를 위해 Cisco ISE에서 필요한 권한 부여 규칙 및 클라이언트 프로비저닝 정책 생성

Chromebook 사용자는 다음을 수행합니다.

- Google 관리자가 정의한 시행된 정책을 보호하기 위해 Chromebook 디바이스를 지우고 Google 도메인에 등록
- Google Admin Console이 설치한 Cisco Network Setup Assistant 강제 익스텐션 및 Chromebook 디바이스 정책 수신
- Google 관리자가 정의한 대로 프로비저닝된 SSID에 연결하고 브라우저를 열어 BYOD 페이지를 표시한 다음 온보딩 프로세스 시작
- Cisco Network Setup Assistant는 Chromebook 디바이스에서 클라이언트 인증서를 설치하므로 디바이스가 EAP-TLS 인증서 기반 인증을 수행할 수 있습니다.

Google Admin Console은 다음을 수행합니다.

Google Admin Console은 Chromebook 디바이스 관리를 지원하며, 보안 네트워크를 구성하고 Chromebook으로 Cisco Network Setup Assistant 인증서 관리 익스텐션을 푸쉬할 수 있도록 허용합니다. 익스텐션은 Cisco ISE에 SCEP 요청을 보내고 클라이언트 인증서를 설치하여 네트워크 액세스 및 보안 연결을 허용합니다.

공유 환경에서 **Chromebook** 디바이스 사용을 위한 모범 사례

학교, 도서관 등의 공유 환경에서 Chromebook 디바이스를 사용할 때는 여러 사용자가 Chromebook 디바이스를 공유하게 됩니다. Cisco가 권장하는 몇 가지 모범 사례는 다음과 같습니다.

- 특정 사용자(학생 또는 교수) 이름을 사용하는 Chromebook 디바이스를 온보딩하는 경우 인증서 Subject(주체) 필드의 CN(Common Name)에 해당 사용자 이름이 입력됩니다. 또한 공유 Chromebook은 특정 사용자의 My Devices(내 디바이스) 포털에 나열됩니다. 따라서 디바이스가 특정 사용자의 My Devices(내 디바이스) 포털 목록에만 표시되도록 온보딩 시 공유 디바이스에서 공유 자격 증명을 사용하는 것이 좋습니다. 공유 계정을 관리자 또는 교수가 별도의 계정으로 관리하며 공유 디바이스를 제어할 수 있습니다.
- Cisco ISE 관리자는 공유 Chromebook 디바이스용 사용자 맞춤화 인증서 템플릿을 생성하여 정책에서 사용할 수 있습니다. 예를 들어 주체-CN(Common Name) 값과 일치하는 표준 인증서 템플릿을 사용하는 대신 인증서에 이름(예: chrome-shared-grp1)을 지정할 수 있으며 동일한 이름을 Chromebook 디바이스에 할당할 수 있습니다. 이 이름과 일치하는지 여부에 따라 Chromebook 디바이스에 대한 액세스를 허용하거나 거부하는 정책을 설계할 수 있습니다.
- Cisco ISE 관리자는 Chromebook 온보딩을 거쳐야 하는 모든 Chromebook 디바이스(액세스를 제한해야 하는 디바이스)의 MAC 주소를 사용하여 엔드포인트 그룹을 생성할 수 있습니다. 권한 부여 규칙에서 디바이스 유형 Chromebook과 함께 이를 호출해야 합니다. 이렇게 하면 액세스를 NSP로 리디렉션할 수 있습니다.

Chromebook 온보딩 프로세스

Chromebook 온보딩 프로세스에서는 다음과 같은 일련의 단계가 포함되어 있습니다.

단계 **1** Google Admin Console에서 네트워크 및 강제 익스텐션 구성 .

단계 **2** Chromebook 온보딩용으로 Cisco ISE 구성.

단계 **3** Chromebook 디바이스 초기화.

단계 **4** Google Admin Console에 Chromebook 등록.

단계 **5** BYOD 온보딩을 위해 Chromebook을 Cisco ISE 네트워크에 연결.

Google Admin Console에서 네트워크 및 강제 익스텐션 구성

다음 단계는 Google 관리자가 수행합니다.

단계 **1** Google Admin Console에 로그인합니다.

a) 브라우저에서 URL https://admin.google.com을 입력합니다.

b) 필요한 사용자 이름 및 비밀번호를 입력합니다.

c) **Welcome to Admin Console**(관리 콘솔 시작) 창에서 **Device Management**(디바이스 관리)를 클릭합니다.

d) **Device Management**(디바이스 관리) 창에서 **Network**(네트워크)를 클릭합니다.

단계 **2** 관리되는 디바이스용으로 Wi-Fi 네트워크를 설정합니다.

a) **Networks**(네트워크) 창에서 **Wi-Fi**를 클릭합니다.

b) **Add Wi-Fi**(Wi-Fi 추가)를 클릭하여 필요한 SSID를 추가합니다. 자세한 내용은 Google Admin Console - Wi-Fi 네트워크 설정을 참고하십시오.

MAB 플로우의 경우 2개의 SSID를, 하나는 개방형 네트워크용으로 그리고 다른 하나는 인증서 인증용으로 생성합니다. 개방형 네트워크에 연결할 때 Cisco ISE ACL은 인증을 위해 사용자를 자격 증명이 있는 게스트 포털로 리디렉션하며, 인증에 성공하면 BYOD 포털로 리디렉션합니다.

중간 CA에서 ISE 인증서를 발급한 경우에는 중간 인증서를 루트 CA가 아닌 "서버 CA"에 매핑해야 합니다.

c) **Add**(추가)를 클릭합니다.

단계 **3** 강제 익스텐션을 생성합니다.

a) **Device Management**(디바이스 관리) 창의 **Device Settings**(디바이스 설정)에서 **Chrome Management**(Chrome 관리)를 클릭합니다.

b) **User Settings**(사용자 설정)를 클릭합니다.

c) 아래로 스크롤한 다음 **Apps and Extensions**(앱 및 확장) 섹션의 **Force-Installed Apps and Extensions**(강제 설치된 앱 및 확장) 옵션에서 **Manage Force-Installed Apps**(강제 설치된 앱 관리)를 클릭합니다.

단계 **4** 강제 익스텐션을 설치합니다.

a) **Force-Installed Apps and Extensions**(강제 설치된 앱 및 확장) 창에서 **Chrome Web Store**(Chrome 웹 스토어)를 클릭합니다.

b) **Search**(검색) 텍스트 상자에 "Cisco Network Setup Assistant"를 입력하여 이 확장 프로그램을 찾습니다.

Chromebook 디바이스의 강제 Cisco Network Setup Assistant 확장 프로그램이 Cisco ISE에서 인증서를 요청한 다음 Chromebook 디바이스에 ISE 인증서를 설치합니다. 인증서 설치는 관리되는 디바이스에 대해서만 허용되므로, 이 확장 프로그램은 강제 설치로 구성해야 합니다. 등록 프로세스 중에 이 확장 프로그램이 설치되지 않으면 Cisco ISE 인증서를 설치할 수 없습니다.

이 확장 프로그램에서 지원되는 언어에 대한 자세한 내용은 의 Cisco ISE 국제화 및 현지화 섹션을 참고하십시오.

c) 앱을 강제 설치하려면 **Add(**추가**)**를 클릭합니다.
d) **Save(**저장**)**를 클릭합니다.

단계 **5** (선택 사항) 여러 사용자가 공유하는 Chromebook 디바이스에서 인증서를 설치하려면 구성 파일을 정의합니다.

a) 다음 코드를 복사하여 메모장 파일에 붙여 넣은 다음 로컬 디스크에 저장합니다.

```
{
  "certType": {
    "Value": "system"
  }
}
```

b) **Device Management(**디바이스 관리**)** > **Chromebook Management(Chromebook** 관리**)** > **App Management(**앱 관리**)**를 선택합니다.
c) **Cisco Network Setup Assistant** 익스텐션을 클릭합니다.
d) **User Settings(**사용자 설정**)**를 클릭하고 도메인을 선택합니다.
e) **Upload Configuration File(**구성 파일 업로드**)**을 클릭하고 로컬 디스크에 저장한 .txt 파일을 선택합니다.

참고 Cisco Network Setup Assistant에서 여러 사용자가 공유하는 디바이스에 대한 인증서를 생성하려는 경우 Google Admin Console에서 메모장 파일을 추가해야 합니다. 이렇게 하지 않으면 Cisco NSA는 단일 사용자에 대한 인증서를 생성합니다.

f) **Save(**저장**)**를 클릭합니다.

단계 **6** (선택 사항) Chromebook을 공유하지 않는 단일 사용자용으로 인증서를 설치합니다.

a) **Device Management(**디바이스 관리**)** > **Network(**네트워크**)** > **Certificates(**인증서**)**를 선택합니다.
b) **Certificates(**인증서**)** 창에서 **Add Certificate(**인증서 추가**)**를 클릭하고 Cisco ISE 인증서 파일을 업로드합니다.

다음에 수행할 작업

Chromebook 온보딩용으로 Cisco ISE 구성

Chromebook 온보딩용으로 Cisco ISE 구성

시작하기 전에

Cisco ISE 관리자는 필수 정책을 생성해야 합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)** 창.

아래는 권한 부여 정책의 예입니다.

Rule Name: Full_Access_After_Onboarding, Conditions: If RegisteredDevices AND Wireless_802.1x AND Endpoints:BYODRegistration EQUALS Yes AND Certificate: Subject Alternative Name Equals RadiusCalling-Station-ID AND Network Access: EAP-Authentication EQUALS EAP-TLS Then CompliantNetworkAccess.

CompliantNetworkAccess는 구성된 권한 부여 결과입니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(정책)** > **Policy Elements(정책 요소)** > **Results(결과)** > **Authorization(권한 부여)** > **Authorization Profiles(권한 부여 프로파일)** 창.

단계 **1** Cisco ISE에서 NSP(Native Supplicant Profile)를 구성합니다.

a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(정책)** > **Policy Elements(정책 요소)** > **Results(결과)** > **Client Provisioning(클라이언트 프로비저닝)** > **Resources(리소스)**.

Chromebook 디바이스는 새로 Cisco ISE를 설치하는 경우 클라이언트 프로비저닝 페이지에 표시됩니다. 그러나 업그레이드의 경우에는 포스처 업데이트를 다운로드해야 합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Settings(설정)** > **Posture(포스처)** > **Updates(업데이트)** 창.

b) **Add(추가)** > **Native Supplicant Profile(기본 신청자 프로파일)**을 클릭합니다.

c) **Name(이름)** 및 **Description(설명)**을 입력합니다.

d) **Operating System(운영체제)** 필드에서 **Chrome OS All(Chrome OS 모두)**을 선택합니다.

e) **Certificate Template(인증서 템플릿)** 필드에서 필요한 인증서 템플릿을 선택합니다.

f) **Submit(제출)**을 클릭합니다. SSID가 기본 신청자 프로비저닝 플로우를 통해서가 아닌 Google Admin Console을 통해 프로비저닝되는지 확인합니다.

단계 **2** Client Provisioning(클라이언트 프로비저닝) 페이지에서 NSP를 매핑합니다.

a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 을 선택합니다.

b) 결과를 정의합니다.

- 클라이언트 프로비저닝 정책의 **Results(결과)**에서 기본 제공 기본 신청자 컨피그레이션(Cisco-ISE-Chrome-NSP)을 선택합니다.
- 또는 새 규칙을 생성하고 Chromebook 디바이스용으로 생성된 **Result(결과)**를 선택합니다.

Chromebook 디바이스 초기화

Google 관리자가 Google Admin Console을 구성하고 나면 Chromebook 디바이스를 초기화해야 합니다. Chromebook 사용자는 일회성 프로세스인 디바이스 초기화를 수행하여 익스텐션을 강제로 수행하고 네트워크 설정을 구성해야 합니다. 자세한 내용은 URL https://support.google.com/chrome/a/answer/1360642에서 참고할 수 있습니다.

Chromebook 사용자는 다음 단계를 수행합니다.

단계 **1** **Esc+**새로 고침**+**전원 키 조합을 누릅니다. 화면에 노란색 느낌표(!)가 표시됩니다.

단계 **2** **Ctrl+D** 키 조합을 눌러 개발자 모드를 시작한 다음 **Enter** 키를 누릅니다. 화면에 빨간색 느낌표가 표시됩니다.

단계 **3** **Ctrl+D** 키 조합을 누릅니다. Chromebook이 로컬 데이터를 삭제하고 초기 상태로 돌아갑니다. 삭제에는 약 15분이 소요됩니다.

단계 **4** 전환이 완료되면 스페이스바 키를 누른 다음 **Enter** 키를 눌러 확인된 모드로 돌아갑니다.

단계 **5** 로그인하기 전에 Chromebook을 등록합니다.

다음에 수행할 작업

Google Admin Console에 Chromebook을 등록합니다.

Google Admin Console에 Chromebook 등록

Chromebook 디바이스를 프로비저닝하려면 Chromebook 사용자는 먼저 Google Admin Console 페이지에서 등록을 하고 디바이스 정책 및 강제 익스텐션을 받아야 합니다.

단계 **1** Chromebook 디바이스를 켜고 로그인 화면이 보일 때까지 화면의 지침을 따릅니다. 아직 로그인하지 마십시오.

단계 **2** Chromebook 디바이스에 로그인하기 전에 **Ctrl+Alt+E** 키 조합을 누릅니다. **Enterprise Enrolment(**기업 등록**)** 화면이 나타납니다.

단계 **3** 이메일 주소를 입력하고 **Next(**다음**)**를 클릭합니다.
그러면 Your device has successfully been enrolled for enterprise management.(디바이스가 기업 관리용으로 등록되었습니다.)라는 메시지가 표시됩니다.

단계 **4** **Done(**완료**)**을 클릭합니다.

단계 **5** 등록 자격이 있는 계정에 Google 관리자의 환영 서신에 포함된 사용자 이름과 비밀번호 또는 기존 Google 앱 사용자의 사용자 이름과 비밀번호를 입력합니다.

단계 **6** **Enroll Device(**디바이스 등록**)**를 클릭합니다. 디바이스가 등록되었다는 확인 메시지가 표시됩니다.

Chromebook 등록은 일회용 프로세스입니다.

BYOD 온보딩을 위해 Chromebook을 Cisco ISE 네트워크에 연결

이 절차는 듀얼 SSID를 위한 절차입니다. EAP-TLS 프로토콜을 사용하여 802.x 네트워크에 연결하기 위해 Chromebook 사용자는 다음 단계를 수행합니다.

참고 듀얼 SSID를 사용하는 경우-802.x PEAP에서 EAP-TLS 네트워크에 연결할 때 웹 브라우저가 아닌 네트워크 신청자에 자격 증명을 입력하여 네트워크에 연결합니다.

단계 **1** Chromebook에서 **Settings(**설정**)**를 클릭합니다.

단계 **2** **Internet Connection(**인터넷 연결**)** 섹션에서 **Provisioning Wi-Fi Network(Wi-Fi** 네트워크 프로비저닝**)**를 클릭하고 네트워크를 클릭합니다.

단계 **3** 자격증명이 있는 게스트 포털이 열립니다.

1. Sign On(로그인) 페이지에서 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)**를 입력합니다.

2. **Sign-on(**로그인**)**을 클릭합니다.

단계 **4** BYOD Welcome(BYOD 시작) 페이지에서 **Start(**시작**)**를 클릭합니다.

단계 **5** **Device Information(**디바이스 정보**)** 필드에서 디바이스의 이름과 설명을 입력합니다. 예를 들어 "개인 디바이스: 학교에서 사용하는 Jane의 Chromebook" 또는 "공유 디바이스: 도서관 Chromebook 1번 또는 강의실 1 Chromebook 1번".

단계 **6** **Continue(**계속**)**를 클릭합니다.

단계 **7** **Cisco Network Setup Assistant** 대화 상자에서 **Yes(**예**)**를 클릭하여 보안 네트워크 액세스를 위한 인증서를 설치합니다.

Google 관리자가 보안 Wi-Fi를 구성한 경우 네트워크 연결이 자동으로 수행됩니다. 그렇지 않은 경우 사용 가능한 네트워크 목록에서 보안 SSID를 선택합니다.

도메인에 이미 등록되었으며 Cisco Network Setup Assistant 익스텐션을 소유하고 있는 Chromebook 사용자는 자동 업데이트를 기다리지 않고 익스텐션을 업데이트할 수 있습니다. 다음 단계를 수행하여 익스텐션을 수동으로 업데이트합니다.

1. Chromebook에서 브라우저를 열고 **URL: chrome://Extensions**를 입력합니다.
2. **Developer Mode(**개발자 모드**)** 확인란을 선택합니다.
3. **Update Extensions Now(**지금 익스텐션 업데이트**)**를 클릭합니다.
4. Cisco Network Setup Assistant 익스텐션 버전이 2.1.0.35 이상인지 확인합니다.

Google Admin Console - Wi-Fi 네트워크 설정

Wi-Fi 네트워크 컨피그레이션은 고객 네트워크에서 SSID를 구성하거나 인증서 속성을 사용하여 인증서 일치 여부를 확인하는 데 사용됩니다(EAP-TLS의 경우). 인증서가 Chromebook에 설치되어 있는 경우 해당 인증서는 Google 관리 설정과 동기화됩니다. 정의된 인증서 속성 중 하나가 SSID 컨피그레이션과 일치해야 연결이 설정됩니다.

아래에는 EAP-TLS, PEAP 및 개방형 네트워크플로우우와 관련된 필수 필드가 나열되어 있습니다. 이 필드로 Google 관리자가 각 Chromebook 사용자에 대해 Google Admin Console 페이지(**Device Management(**디바이스 관리**) > Network(**네트워크**) > Wi-Fi > Add Wi-Fi(Wi-Fi** 추가**)**)에서 Wi-Fi 네트워크를 설정하도록 구성할 수 있습니다.

필드	**EAP-TLS**	**PEAP**	개방형
Name(이름)	네트워크 연결의 이름을 입력합니다.	네트워크 연결의 이름을 입력합니다.	네트워크 연결의 이름을 입력합니다.
Service Set Identifier (SSID)(SSID(Service Set Identifier))	SSID(예: tls_ssid)를 입력합니다.	SSID(예: tls_ssid)를 입력합니다.	SSID(예: tls_ssid)를 입력합니다.

필드	**EAP-TLS**	**PEAP**	개방형
This SSID Is Not Broadcast(이 SSID는 브로드캐스트가 아님)	옵션을 선택합니다.	옵션을 선택합니다.	옵션을 선택합니다.
Automatically Connect(자동으로 연결)	옵션을 선택합니다.	옵션을 선택합니다.	옵션을 선택합니다.
보안 유형	WPA/WPA2 Enterprise (802.1x)	WPA/WPA2 Enterprise (802.1x)	개방형
Extensible Authentication Protocol	EAP-TLS	PEAP	—
Inner Protocol(내부 프로토콜)	—	• 자동 • MSCHAP v2(옵션 선택) • MD5 • PAP • MSCHAP • GTC	—
Outer Identity(외부 ID)	—	—	—
Username(사용자 이름)	(선택 사항) 고정 값을 설정하거나 사용자 로그인의 변수(${LOGIN_ ID} 또는 ${LOGIN_EMAIL})를 사용합니다.	ISE(내부 ISE 사용자/AD/기타 ISE ID) 및 Password(비밀번호) 필드에 대해 인증하는 데 사용할 PEAP 자격 증명을 입력합니다.	—
Server Certificate Authority(서버 인증 기관)	ISE 인증서(Device Management(디바이스 관리) > Network(네트워크) > Certificates(인증서))를 선택합니다.	ISE 인증서(Device Management(디바이스 관리) > Network(네트워크) > Certificates(인증서))를 선택합니다.	—
Restrict Access to this Wi-Fi Network by Platform(플랫폼을 기준으로 이 Wi-Fi 네트워크에 대한 액세스 제한)	• Mobile Devices(모바일 디바이스)를 선택합니다. • Chromebooks(Chromebook)를 선택합니다.	• Mobile Devices(모바일 디바이스)를 선택합니다. • Chromebooks(Chromebook)를 선택합니다.	—

필드	**EAP-TLS**	**PEAP**	개방형
Client Enrollment URL(클라이언트 등록 URL)	등록되지 않은 사용자에 대해 Chromebook 디바이스 브라우저가 리디렉션되는 URL을 입력합니다. 등록되지 않은 사용자 리디렉션을 위해 무선 LAN 컨트롤러에서 ACL을 구성합니다.	—	—

필드	**EAP-TLS**	**PEAP**	개방형
Issuer Pattern(발급자 패턴)	인증서의 속성입니다. Issuer Pattern(발급자 패턴) 또는 Subject Pattern(주체 패턴)에서 설치된 인증서 속성과 일치해야 하는 속성을 하나 이상 선택합니다. 인증서를 수락하기 위해 Chromebook 디바이스와의 일치 여부를 확인할 인증서 속성을 지정합니다. • Common Name(공용 이름): 인증서의 Subject(주체) 필드 또는 인증서 Subject(주체) 필드의 와일드카드 도메인을 참조합니다. 인증서는 노드의 FQDN과 일치해야 합니다. • Locality(지역): 인증서 주체와 연결된 테스트 지역(구/군/시)을 참조합니다. • Organization(조직): 인증서 주체와 연결된 조직 이름을 참조합니다. • Organization Unit(조직 단위): 인증서 주체와 연결된 조직 단위 이름을 참조합니다.	—	—

필드	**EAP-TLS**	**PEAP**	개방형
Subject Pattern(주체 패턴)	인증서의 속성입니다. Issuer Pattern(발급자 패턴) 또는 Subject Pattern(주체 패턴)에서 설치된 인증서 속성과 일치해야 하는 속성을 하나 이상 선택합니다. 인증서를 수락하기 위해 Chromebook 디바이스와의 일치 여부를 확인할 인증서 속성을 지정합니다. • Common Name(공용 이름): 인증서의 Subject(주체) 필드 또는 인증서 Subject(주체) 필드의 와일드카드 도메인을 참조합니다. 인증서는 노드의 FQDN과 일치해야 합니다. • Locality(지역): 인증서 주체와 연결된 테스트 지역(구/군/시)을 참조합니다. • Organization(조직): 인증서 주체와 연결된 조직 이름을 참조합니다. • Organization Unit(조직 단위): 인증서 주체와 연결된 조직 단위 이름을 참조합니다.	—	—

필드	EAP-TLS	PEAP	개방형
프록시 설정	• Direct Internet Connection(직접 인터넷 연결)(선택됨) • Manual Proxy Configuration(수동 프록시 컨피그레이션) • Automatic Proxy Configuration(자동 프록시 컨피그레이션)	• Direct Internet Connection(직접 인터넷 연결)(선택됨) • Manual Proxy Configuration(수동 프록시 컨피그레이션) • Automatic Proxy Configuration(자동 프록시 컨피그레이션)	—
Apply Network(네트워크 적용)	By User(사용자별)	By User(사용자별)	—

Cisco ISE에서 Chromebook 디바이스 활동 모니터링

Cisco ISE는 Chromebook 디바이스의 인증 및 권한 부여와 관련된 정보를 확인할 수 있는 다양한 보고서와 로그를 제공합니다. 온디맨드로 또는 정기적으로 이러한 보고서를 실행할 수 있습니다. 인증 방법(예: 802.1x) 및 인증 프로토콜(예: EAP-TLS)을 확인할 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)** 창을 선택합니다. 또한 Chromebook 디바이스로 분류되는 엔드포인트의 수를 식별할 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)** 창을 선택합니다.

Chromebook 디바이스 온보딩 문제 해결

이 섹션에서는 Chromebook 디바이스를 온보딩하는 동안 발생할 수 있는 문제에 대해 설명합니다.

- 오류: 웹 스토어에서 익스텐션을 설치할 수 없음 - 웹 스토어에서는 익스텐션을 설치할 수 없습니다. 익스텐션은 네트워크 관리자에 의해 Chromebook 디바이스에 자동으로 설치됩니다.
- 오류: 인증서 설치를 완료했으나 보안 네트워크에 연결할 수 없음 - 설치한 인증서가 정의된 발급자/주체 속성 패턴과 일치하는지 관리 콘솔을 확인하십시오. chrome://settings/certificates에서 설치된 인증서에 대한 정보를 가져올 수 있습니다.
- 오류: Chromebook에서 보안 네트워크에 수동으로 연결하려고 할 때 "Obtain Network Certificate(네트워크 인증서 가져오기)" 오류 메시지가 표시됨 - Get New Certificate(새 인증서 가져오기)를 클릭하면 브라우저가 열리고 인증서 설치를 위한 ISE BYOD 플로우로 리디렉션됩니다. 그러나 보안 네트워크에 연결할 수 없는 경우에는 설치한 인증서가 정의된 발급자/주체 속성 패턴과 일치하는지 관리 콘솔을 확인하십시오.

- 오류: Get New Certificate(새 인증서 가져오기)를 클릭했는데 www.cisco.com 사이트로 이동됨 - ISE로 리디렉션되어 인증서 설치 프로세스를 시작하려면 사용자가 프로비저닝 SSID에 연결되어 있어야 합니다. 이 네트워크에 대해 올바른 액세스 목록이 정의되어 있는지 확인하십시오.
- 오류: "Only managed devices can use this extension. Contact helpdesk or network administrator(관리되는 디바이스만 이 익스텐션을 사용할 수 있습니다. 헬프 데스크 또는 네트워크 관리자에게 문의하십시오.)" 오류 메시지가 표시됨 - Chromebook은 관리되는 디바이스이며, 디바이스에 인증서를 설치하기 위해 Chrome OS API 액세스 권한을 얻으려면 익스텐션이 강제 설치 항목으로 구성되어 있어야 합니다. Google 웹 스토어에서 익스텐션을 다운로드하여 수동으로 설치할 수는 있지만 등록되지 않은 Chromebook 사용자는 인증서를 설치할 수 없습니다.

  사용자가 도메인 사용자 그룹에 속하는 경우 등록되지 않은 Chromebook 디바이스가 인증서를 보호할 수 있습니다. 익스텐션은 모든 디바이스에서 도메인 사용자를 추적합니다. 그러나 도메인 사용자는 등록되지 않은 디바이스용으로 사용자 기반 인증 키를 생성할 수 있습니다.
- 오류: Google 관리 콘솔에서 SSID가 연결되는 순서가 명확하지 않음 -
  - Google 관리 콘솔에 여러 SSID(PEAP 및 EAP-TLS)가 구성되어 있는 경우 인증서를 설치하고 속성 일치 여부를 확인하고 나면 Chrome OS가 SSID를 구성한 순서에 관계없이 인증서 기반 인증을 사용하여 SSID에 자동으로 연결합니다.
  - EAP-TLS SSID 2개가 같은 속성과 일치하면 신호 강도 및 기타 네트워크 레벨 신호 등의 다른 요인에 따라 연결되는데, 이러한 요인은 사용자나 관리자가 제어할 수 없습니다.
  - Chromebook 디바이스에 여러 EAP-TLS 인증서가 설치되어 있으며 모든 인증서가 관리 콘솔에 구성된 인증서 패턴과 일치하는 경우 최신 인증서가 연결에 사용됩니다.

Cisco AnyConnect Secure Mobility

Cisco ISE는 Cisco ISE 포스처 요건을 위해 AnyConnect에 통합된 모듈을 사용합니다.

참고 Cisco AnyConnect는 CWA 플로우를 지원하지 않습니다. 게스트 포털에서 **Work Centers(**작업 센터**)Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Guest Device Compliance Settings(**게스트 디바이스 규정 준수 설정**)** 창에서 **Require guest device compliance(**게스트 디바이스 규정 준수 필요**)** 필드를 사용하여 Cisco AnyConnect를 프로비저닝할 수 없습니다. 대신 클라이언트 프로비저닝 포털에서 Cisco AnyConnect를 프로비저닝합니다. 이렇게 하면 권한 부여 권한에 구성된 대로 리디렉션이 수행됩니다.

참고 네트워크 미디어를 전환할 때, Cisco AnyConnect ISE 포스처 모듈이 변경된 네트워크를 감지하고 클라이언트를 재평가 할 수 있도록 기본 게이트웨이를 변경해야 합니다.

Cisco ISE를 Cisco AnyConnect 에이전트와 통합할 때 Cisco ISE는 다음을 수행합니다.

- Cisco AnyConnect 버전 4.0 이상의 릴리스를 구축할 수 있는 스테이징 서버 역할
- Cisco ISE 포스처 요건을 위해 AnyConnect 포스처 구성 요소와 상호작용
- Windows 및 Mac OS X 운영체제에 대해 AnyConnect 프로파일, 사용자 맞춤화 및 언어 패키지 및 OPSWAT 라이브러리 업데이트를 배포할 수 있도록 지원
- Cisco AnyConnect와 레거시 에이전트를 동시에 지원

AnyConnect 컨피그레이션 생성

AnyConnect 컨피그레이션에는 AnyConnect 소프트웨어 및 관련 구성 파일이 포함됩니다. 사용자가 클라이언트에서 AnyConnect 리소스를 다운로드하여 설치하도록 허용하는 클라이언트 프로비저닝 정책에서 이 컨피그레이션을 사용할 수 있습니다. ISE와 ASA를 모두 사용하여 AnyConnect를 구축하는 경우에는 두 헤드엔드에서 컨피그레이션이 일치해야 합니다.

VPN에 연결되어있을 때 ISE 포스처 모듈을 푸시하려면 Cisco ASDM(Adaptive Security Device Manager) GUI 툴을 사용하는 Cisco ASA(Adaptive Security Appliance)를 통해 AnyConnect 에이전트를 설치하는 것이 좋습니다. ASA는 VPN 다운로더를 사용하여 설치를 수행합니다. 다운로드된 ISE Posture 프로파일은 ASA를 통해 푸시되며, 이후 프로파일 프로비저닝에 필요한 검색 호스트는 ISE Posture 모듈이 ISE에 연결하기 전에 제공됩니다. 반면 ISE 사용 시에는 ISE가 검색된 후에만 ISE Posture 모듈이 프로파일을 가져오므로 오류가 발생할 수 있습니다. 따라서 VPN에 연결할 때 ISE Posture 모듈을 푸시하려면 ASA를 사용하는 것이 좋습니다.

참고 Cisco ISE가 ASA와 통합된 경우 ASA에서 계정 관리 모드가 **Single(**단일**)**로 설정되어 있는지 확인합니다. 계정 관리 데이터는 단일 모드에서 하나의 계정 관리 서버로만 전송됩니다.

시작하기 전에

AnyConnect 구성 개체를 구성하기 전에 다음을 수행하십시오.

1. Cisco 소프트웨어 다운로드 페이지에서 AnyConnect Headend Deployment 패키지 및 규정 준수 모듈을 다운로드합니다.
2. Cisco ISE에 이러한 리소스를 업로드합니다(로컬 머신에서 Cisco 제공 클라이언트 프로비저닝 리소스 추가, 89 페이지 참고).
3. (선택 사항) 사용자 맞춤화 및 현지화 번들을 추가합니다(로컬 머신에서 AnyConnect용으로 고객이 생성한 리소스 추가, 90 페이지 참고).
4. AnyConnect 포스처 에이전트 프로파일을 구성합니다(포스처 에이전트 프로파일 생성, 113 페이지 참고).

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**.

단계 **2** **Add(**추가**)**를 클릭하여 AnyConnect 컨피그레이션을 생성합니다.

단계 **3** **AnyConnect Configuration(AnyConnect** 컨피그레이션**)**을 선택합니다.

단계 **4** 이전에 업로드한 AnyConnect 패키지를 선택합니다. AnyConnectDesktopWindows xxx.x.xxxxx.x 등을 예로 들 수 있습니다.

단계 **5** 현재 AnyConnect 컨피그레이션의 이름을 입력합니다. 예를 들면 AC Config xxx.x.xxxxx.x와 같이 입력할 수 있습니다.

단계 **6** 이전에 업로드한 규정 준수 모듈을 선택합니다. AnyConnectComplianceModulewindows x.x.xxxx.x 등을 예로 들 수 있습니다.

단계 **7** 하나 이상의 AnyConnect 모듈 확인란을 선택합니다. 예를 들어 ISE Posture, VPN, Network Access Manager, Web Security, AMP Enabler, ASA Posture, Start Before Log on(로그온하기 전에 시작)(Windows OS의 경우만 해당함), Diagnostic and Reporting Tool(진단 및 보고 도구) 중에서 하나 이상의 모듈을 선택합니다.

참고 AnyConnect 모듈 선택에서 VPN 모듈의 선택을 취소해도 프로비저닝되는 클라이언트에서 VPN 타일이 비활성화되지는 않습니다. AnyConnect GUI에서 VPN 타일을 비활성화하려면 VPNDisable_ServiceProfile.xml을 구성해야 합니다. AnyConnect가 기본 위치에 설치된 시스템의 경우 C:\Program Files\Cisco에서 이 파일을 찾을 수 있습니다. AnyConnect가 다른 위치에 설치된 경우 파일은 <AnyConnect Installed path>\Cisco에 있습니다.

단계 **8** 선택한 AnyConnect 모듈에 대해 AnyConnect 프로파일을 선택합니다. 예를 들어 ISE Posture, VPN, NAM, Web Security 등을 선택할 수 있습니다.

단계 **9** AnyConnect 사용자 맞춤화 및 현지화 번들을 선택합니다.

단계 **10** **Submit(**제출**)**을 클릭합니다.

포스처 에이전트 프로파일 생성

이 절차를 참조하여 AnyConnect 포스처 에이전트 프로파일을 생성합니다. 여기서 포스처 프로토콜에 대한 에이전트 동작을 정의하는 매개변수를 지정할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **AnyConnect Posture Profile(AnyConnect** 포스처 프로파일**)**을 선택합니다.

단계 **4** 프로파일의 이름을 입력합니다.

단계 **5** 다음에 대해 매개변수를 구성합니다.

- Cisco ISE Posture 에이전트 동작
- 클라이언트 IP 주소 변경
- Cisco ISE Posture 프로토콜

단계 **6** **Submit(**제출**)**을 클릭합니다.

클라이언트 IP 주소 새로 고침 컨피그레이션

다음 표에서는 NAC AnyConnect Posture Profile(NAC AnyConnect 포스처 프로파일) 창의 필드에 대해 설명합니다. 이 창에서는 클라이언트가 VLAN 변경 후 IP 주소를 갱신하거나 새로 고칠 수 있는 매개변수를 구성할 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)** > **Add(**추가**)** > **NAC or AnyConnect Posture Profile(NAC** 또는 **AnyConnect** 포스처 프로파일**)**을 선택합니다.

필드 이름	기본값	사용 지침
VLAN detection interval(VLAN 탐지 간격**)**	0, 5	이 설정은 에이전트가 VLAN 변경을 확인하는 간격입니다. Mac OS X 에이전트의 기본값은 5입니다. 기본적으로 Mac OS X에서는 VlanDetectInteval이 5초로 설정된 상태로 인증 VLAN 변경 기능에 대한 액세스가 활성화되어 있습니다. 유효 범위는 5~900초입니다. 0 - 인증 VLAN 변경 기능에 대한 액세스가 비활성화됩니다. 1~5 - Agent가 5초마다 한 번씩 ICMP(Internet Control Message Protocol) 또는 ARP(Address Resolution Protocol) 쿼리를 보냅니다. 6~900 - ICMP 또는 ARP 쿼리가 x초마다 한 번씩 전송됩니다.
UI 없이 **VLAN** 탐지 활성화**(Mac OS X** 클라이언트에는 해당되지 않음**)**	No(아니요)	이 설정은 사용자가 로그인되지 않은 경우에도 VLAN 탐지를 활성화하거나 비활성화합니다. 아니요 - VLAN 탐지 기능이 비활성화됩니다. 예 - VLAN 탐지 기능이 활성화됩니다.

필드 이름	기본값	사용 지침
Retry detection count(재시도 탐지 횟수**)**	3	ICMP(Internet Control Message Protocol) 또는 ARP(Address Resolution Protocol) 폴링이 실패하는 경우 이 설정은 클라이언트 IP 주소를 새로 고치기 전까지 에이전트가 x회 재시도하도록 구성합니다.
Ping 또는 **ARP**	0 유효 범위는 0~2입니다.	이 설정은 클라이언트 IP 주소 변경을 탐지하는 데 사용되는 방법을 지정합니다. 0 - ICMP를 사용하여 폴링 1 - ARP를 사용하여 폴링 2 - ICMP를 먼저 사용한 다음 (ICMP가 실패하는 경우) ARP를 사용하여 폴링
Maximum timeout for ping(최대 **ping** 시간 초과**)**	1 유효 범위는 1~10초입니다.	ICMP를 사용하여 폴링하고 지정된 시간 내에 응답이 없는 경우 ICMP 폴링 실패를 선언합니다.
Enable agent IP refresh(에이전트 **IP** 새로 고침 활성화**)**	Yes(예)(기본값)	이 설정은 스위치(또는 WLC)가 각 스위치 포트에서 클라이언트의 로그인 세션에 대한 VLAN을 변경한 후에 클라이언트 머신이 IP 주소를 갱신할지, 아니면 새로 고칠지를 지정합니다.
DHCP renew delay(DHCP 갱신 지연**)**	0 유효 범위는 0~60초입니다.	이 설정은 클라이언트 머신이 네트워크 DHCP 서버에서 새 IP 주소에 대한 요청을 시도하기 전에 대기하도록 지정합니다.
DHCP release delay(DHCP 릴리스 지연**)**	0 유효 범위는 0~60초입니다.	이 설정은 클라이언트 머신이 현재 IP 주소를 해제하기 전에 대기하도록 지정합니다.

참고 매개변수 값을 기존 에이전트 프로파일 설정과 병합하거나 Windows 및 Mac OS X 클라이언트에서 해당 값을 덮어써 IP 주소를 새로 고칩니다.

포스처 프로토콜 설정

다음 표에서는 Cisco ISE에서 AnyConnect의 포스처 프로토콜 설정을 구성하는 데 사용할 수 있는 NAC AnyConnect 프로파일 페이지의 필드에 대해 설명합니다. Anyconnect용 포스처 프로토콜 설정의 기타 필드에 대한 자세한 내용은 사용중인 AnyConnect 버전의 Cisco AnyConnect Secure Mobility Client Administrator Guide를 참조하십시오.

필드 이름	기본값	사용 지침
Call Home 리스트	—	IP 주소와 포트 사이에 콜론이 있는 IP 주소 및 포트의 쉼표로 구분된 목록을 입력합니다.
Back-off Timer (백오프 타이머)	30초	이 설정을 통해 Anyconnect 에이전트는 이 최대 시간 제한에 도달할 때까지 검색 패킷을 전송하여 검색 대상(리디렉션 대상 및 이전에 연결한 PSN)에 지속적으로 연결할 수 있습니다. 유효 범위는 1 ~ 600초입니다.

지속적인 엔드포인트 속성 모니터링

Cisco AnyConnect 에이전트를 사용하여 다양한 엔드포인트 속성을 지속적으로 모니터링하여 상태 평가 중에 동적 변경 사항이 관찰되는지 확인할 수 있습니다. 이렇게 하면 엔드포인트의 전반적인 가시성이 향상되고 그 동작을 기반으로 포스처 정책을 생성할 수 있습니다. Cisco AnyConnect 에이전트는 엔드포인트에 설치되어 실행중인 애플리케이션을 모니터링합니다. 기능을 켜고 끄고 데이터를 모니터링할 빈도를 구성할 수 있습니다. 기본적으로 데이터는 5분마다 수집되며 데이터베이스에 저장됩니다. 초기 포스처 중에 Cisco AnyConnect는 실행중인 애플리케이션과 설치된 애플리케이션의 전체 목록을 보고합니다. 초기 상태가 유지되면 Cisco AnyConnect 에이전트는 X분마다 애플리케이션을 검사하고 마지막 검사에서 서버로 차이를 전송합니다. 서버는 실행 중인 애플리케이션과 설치된 애플리케이션의 전체 목록을 표시합니다.

Cisco Web Agent

Cisco Web Agent는 클라이언트 머신에 대한 임시 포스처 평가를 제공합니다.

사용자는 ActiveX 컨트롤 또는 Java 애플릿을 통해 웹 에이전트 파일을 클라이언트 머신의 임시 디렉토리에 설치하는 Cisco Web Agent 실행 파일을 시작할 수 있습니다.

사용자가 Cisco Web Agent에 로그인하고 나면, 웹 에이전트는 Cisco ISE 서버에서 사용자 역할 및 운영체제에 대해 구성된 요건을 가져오고, 호스트 레지스트리, 프로세스, 애플리케이션 및 서비스에서 필수 패키지를 확인하고, 보고서를 다시 Cisco ISE 서버로 보냅니다. 클라이언트 머신에서 요건이 충족되면 사용자는 네트워크 액세스가 허용됩니다. 요건이 충족되지 않으면 웹 에이전트는 충족되지 않은 각 요건에 해당하는 대화 상자를 사용자에게 제공합니다. 대화 상자에서는 클라이언트 머신이

요건을 충족하기 위해 수행해야 할 작업 및 지침을 사용자에게 제공합니다. 또는 지정된 요건이 충족되지 않은 경우 사용자는 사용자 로그인 역할에 대한 요건을 충족하도록 클라이언트 시스템을 교정하는 동안 제한된 네트워크 액세스를 허용하도록 선택할 수 있습니다.

참고 ActiveX는 32비트 버전의 Internet Explorer에서만 지원됩니다. Firefox 웹 브라우저 또는 64비트 버전의 Internet Explorer에는 ActiveX를 설치할 수 없습니다.

Cisco Web Agent

Cisco Web Agent는 클라이언트 머신에 대한 임시 포스처 평가를 제공합니다.

사용자는 ActiveX 컨트롤 또는 Java 애플릿을 통해 웹 에이전트 파일을 클라이언트 머신의 임시 디렉토리에 설치하는 Cisco Web Agent 실행 파일을 시작할 수 있습니다.

사용자가 Cisco Web Agent에 로그인하고 나면, 웹 에이전트는 Cisco ISE 서버에서 사용자 역할 및 운영체제에 대해 구성된 요건을 가져오고, 호스트 레지스트리, 프로세스, 애플리케이션 및 서비스에서 필수 패키지를 확인하고, 보고서를 다시 Cisco ISE 서버로 보냅니다. 클라이언트 머신에서 요건이 충족되면 사용자는 네트워크 액세스가 허용됩니다. 요건이 충족되지 않으면 웹 에이전트는 충족되지 않은 각 요건에 해당하는 대화 상자를 사용자에게 제공합니다. 대화 상자에서는 클라이언트 머신이 요건을 충족하기 위해 수행해야 할 작업 및 지침을 사용자에게 제공합니다. 또는 지정된 요건이 충족되지 않은 경우 사용자는 사용자 로그인 역할에 대한 요건을 충족하도록 클라이언트 시스템을 교정하는 동안 제한된 네트워크 액세스를 허용하도록 선택할 수 있습니다.

참고 ActiveX는 32비트 버전의 Internet Explorer에서만 지원됩니다. Firefox 웹 브라우저 또는 64비트 버전의 Internet Explorer에는 ActiveX를 설치할 수 없습니다.

클라이언트 프로비저닝 리소스 정책 구성

클라이언트의 경우 클라이언트 프로비저닝 리소스 정책은 각 사용자가 로그인 및 사용자 세션 시작 시에 Cisco ISE에서 수신하는 리소스(에이전트, 에이전트 규정 준수 모듈 및 에이전트 사용자 맞춤화 패키지 또는 프로파일)의 버전 하나 이상을 결정합니다.

AnyConnect의 경우에는 클라이언트 프로비저닝 리소스 창에서 리소스를 선택하여 클라이언트 프로비저닝 정책 창에서 사용할 수 있는 AnyConnect 컨피그레이션을 생성할 수 있습니다. AnyConnect 컨피그레이션은 구성 파일이 각기 다른 AnyConnect 소프트웨어 및 해당 연결입니다. 구성 파일에는 Windows 및 Mac OS X 클라이언트용 AnyConnect 이진 패키지, 규정 준수 모듈, 모듈 프로파일, AnyConnect용 사용자 맞춤화 및 언어 패키지가 포함되어 있습니다.

시작하기 전에

- 유효한 클라이언트 프로비저닝 리소스 정책을 생성하기 전에 리소스를 Cisco ISE에 추가했는지 확인해 주십시오. 에이전트 규정 준수 모듈을 다운로드할 때는 항상 시스템에서 사용 가능한 기존 모듈(있는 경우)을 덮어씁니다.
- 클라이언트 프로비저닝 정책에 사용된 기본 신청자 프로파일을 확인하고 무선 SSID가 올바른지 확인합니다. iOS 디바이스의 경우 연결하려는 네트워크가 숨겨져 있으면 **iOS Settings(iOS** 설정**)** 영역에서 **Enable if target network is hidden(**대상 네트워크가 숨겨져 있는 경우 활성화**)** 확인란을 선택합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Client Provisioning(**클라이언트 프로비저닝**)**.

단계 **2** **Behavior(**동작**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Enable(**활성화**)**: 사용자가 네트워크에 로그인할 때 Cisco ISE가 이 정책을 사용해 클라이언트 프로비저닝 기능을 수행하고 클라이언트 프로비저닝 정책 지침을 준수할 수 있도록 합니다.
- **Disable(**비활성화**)**: Cisco ISE가 클라이언트 프로비저닝 기능을 수행하기 위해 지정된 리소스 정책을 사용하지 않습니다.
- **Monitor(**모니터**)**: 정책을 비활성화하고 클라이언트 프로비저닝 세션 요청을 "감시"하여 Cisco ISE가 "모니터링되는" 정책을 기준으로 호출을 시도하는 횟수를 확인합니다.

단계 **3** **Rule Name(**규칙 이름**)** 텍스트 상자에 새 리소스 정책의 이름을 입력합니다.

단계 **4** Cisco ISE에 로그인하는 사용자가 속해 있을 수 있는 ID 그룹을 하나 이상 지정합니다.

Any(모두**)** ID 그룹 유형을 지정하도록 선택할 수도 있고, 자신이 구성한 기존 ID 그룹 목록에서 그룹을 하나 이상 선택할 수도 있습니다.

단계 **5** **Operating Systems(**운영체제**)** 필드를 사용하여 클라이언트 머신 또는 디바이스에서 실행 중일 수 있는 운영체제를 하나 이상 지정합니다. 사용자는 이러한 운영체제를 통해 Cisco ISE에 로그인합니다.

Android, Mac iOS, Mac OSX 등의 단일 운영체제를 지정하도록 선택할 수도 있고 Windows XP (All)(Windows XP(모두)) 또는 Windows 7 (All)(Windows 7(모두))과 같이 여러 클라이언트 머신 운영체제를 포함하는 umbrella 운영체제 지정 방식을 선택할 수도 있습니다.

참고 MAC OS 10.6, 10.7 및 10.8을 선택하는 옵션은 Cisco ISE GUI의 클라이언트 프로비저닝 창에서 사용할 수 있지만, 이러한 버전은 AnyConnect에서 지원되지 않습니다.

단계 **6** **Other Conditions(**기타 조건**)** 필드에서 이 특정 리소스 정책에 대해 생성할 새 식을 지정합니다.

단계 **7** 클라이언트 머신의 경우 **Agent Configuration(**에이전트 컨피그레이션**)** 옵션을 사용하여 클라이언트 머신에서 제공 및 프로비저닝할 에이전트 유형, 규정 준수 모듈, 에이전트 사용자 맞춤화 패키지 및 프로파일을 지정합니다.

클라이언트 머신에서 Agent가 팝업으로 표시될 수 있도록 권한 부여 정책에는 클라이언트 프로비저닝 URL을 반드시 포함해야 합니다. 이렇게 하면 임의의 클라이언트가 보내는 요청이 차단되며 적절한 리디렉션 URL을 알고 있는 클라이언트만 포스처 평가를 요청할 수 있습니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

하나 이상의 클라이언트 프로비저닝 리소스 정책을 정상적으로 구성한 후에는 Cisco ISE 구성을 시작하여 로그인 중에 클라이언트 머신에서 포스처 평가를 수행할 수 있습니다.

클라이언트 프로비저닝 정책에서 **Cisco ISE Posture** 에이전트 구성

클라이언트 머신의 경우 클라이언트 머신에서 사용자가 다운로드하고 설치할 수 있도록 제공 및 프로비저닝할 에이전트 유형, 규정 준수 모듈, 에이전트 사용자 맞춤화 패키지 및/또는 프로파일을 구성합니다.

시작하기 전에

Cisco ISE에서 AnyConnect용 클라이언트 프로비저닝 리소스를 추가해야 합니다.

단계 **1** **Agent** 드롭다운 목록에서 사용 가능한 에이전트를 선택하고 **Is Upgrade Mandatory** 옵션을 적절하게 활성화하거나 비활성화하여 여기에 정의된 에이전트 업그레이드(다운로드)가 클라이언트 시스템에 대해 필수적인지 지정합니다.

Is Upgrade Mandatory 설정은 에이전트 다운로드에만 적용됩니다. 에이전트 프로파일, 규정 준수 모듈 및 에이전트 사용자 맞춤화 패키지 업데이트는 항상 필수 항목입니다.

단계 **2** **Profile** 드롭다운 목록에서 기존 에이전트 프로파일을 선택합니다.

단계 **3** **Compliance Module** 드롭다운 목록을 사용하여 클라이언트 머신에 다운로드할 사용 가능한 규정 준수 모듈을 선택합니다.

단계 **4** **Agent Customization Package** 드롭다운 목록에서 클라이언트 머신에 대해 사용 가능한 에이전트 사용자 맞춤화 패키지를 선택합니다.

개인 디바이스의 기본 신청자 구성

그러면 직원이 Windows, Mac OS, iOS 및 Android 디바이스에 대해 제공되는 기본 신청자를 사용하여 개인 디바이스를 네트워크에 직접 연결할 수 있습니다. 개인 디바이스에 대해 등록된 개인 디바이스에서 제공하고 프로비저닝할 기본 신청자 컨피그레이션을 지정합니다.

시작하기 전에

사용자가 로그인할 때 해당 사용자 권한 부여 요건과 연결한 프로파일에 따라 Cisco ISE가 네트워크 액세스를 위해 사용자 개인 디바이스를 설정하는 데 필요한 신청자 프로비저닝 마법사를 제공하도록 하려면 기본 신청자 프로파일을 생성합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Client Provisioning(**클라이언트 프로비저닝**)**을 선택합니다.

단계 **2** 동작 드롭다운 목록에서 **Enable**, **Disable** 또는 **Monitor**을 선택합니다.

단계 **3** 규칙 이름 텍스트 상자에 새 리소스 정책의 이름을 입력합니다.

단계 **4** 다음 항목을 지정합니다.

- Identity Groups(ID 그룹) 필드를 사용하여 Cisco ISE에 로그인하는 사용자가 속해 있을 수 있는 ID 그룹을 하나 이상 지정합니다.
- Operating Systems(운영체제) 필드를 사용하여 개인 디바이스에서 실행 중일 수 있는 운영체제를 하나 이상 지정합니다. 사용자는 이러한 운영체제를 통해 Cisco ISE에 로그인합니다.
- Other Conditions(기타 조건) 필드를 사용하여 이 특정 리소스 정책에 대해 생성할 새 식을 지정합니다.

단계 **5** 개인 디바이스의 경우 **Native Supplicant Configuration(**기본 **supplicant** 구성**)**을 사용하여 이러한 개인 디바이스로 배포할 특정 **Configuration Wizard**를 선택합니다.

단계 **6** 지정된 개인 디바이스 유형에 대해 해당하는 **Wizard Profile**을 지정합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

클라이언트 프로비저닝 보고서

Cisco ISE 모니터링 및 문제 해결 기능에 액세스하여 성공 또는 실패한 사용자 로그인 세션에 대한 전반적인 트렌드를 확인하거나, 지정된 기간 동안 네트워크에 로그인하는 클라이언트 머신의 수와 유형에 대한 통계를 수집하거나, 클라이언트 프로비저닝 리소스에서의 최근 컨피그레이션 변경 사항을 확인할 수 있습니다.

클라이언트 프로비저닝 요청

Operations(작업**)** > **Reports(**보고서**)** > **ISE Reports(ISE** 보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **Client provisioning(**클라이언트 프로비저닝**)** 보고서에서는 성공 및 실패한 클라이언트 프로비저닝 요청에 대한 통계를 표시합니다. **Run**을 선택하고 사전 설정 기간 중 하나를 지정하는 경우 Cisco ISE는 데이터베이스를 결합하고 결과 클라이언트 프로비저닝 데이터를 표시합니다.

신청자 프로비저닝 요청

Operations(작업**)** > **Reports(**보고서**)** > **ISE Reports(ISE** 보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **Supplicant Provisioning(**신청자 프로비저닝**)** 창에서는 최근의 성공 및 실패한 사용자 디바이스 등록 및 신청자 프로비저닝 요청에 대한 정보를 표시합니다. **Run**을 선택하고 사전 설정 기간 중 하나를 지정하는 경우 Cisco ISE는 데이터베이스를 결합하고 결과 신청자 프로비저닝 데이터를 표시합니다.

신청자 프로비저닝 보고서에서는 로깅 날짜 및 시간, ID(사용자 ID), IP 주소, MAC 주소(엔드포인트 ID), 서버, 프로파일, 엔드포인트 운영체제, SPW 버전, 실패 이유(있는 경우) 및 등록 상태와 같은 데이터를 비롯하여 특정 기간 동안 디바이스 등록 포털을 통해 등록된 엔드포인트 목록에 대한 정보를 제공합니다.

클라이언트 프로비저닝 이벤트 로그

클라이언트 로그인 동작에 대한 가능한 문제를 쉽게 진단하기 위해 이벤트 로그 항목을 검색할 수 있습니다. 예를 들어 네트워크의 클라이언트 머신이 로그인할 때 클라이언트 프로비저닝 리소스 업데이트를 가져올 수 없는 문제의 원인을 판단해야 할 수 있습니다. Client Provisioning Audit and Posture(포스처 및 클라이언트 프로비저닝 감사 및 포스처) 및 Client Provisioning Diagnostics(클라이언트 프로비저닝 진단) 로깅 항목을 사용할 수 있습니다.

클라이언트 프로비저닝 포털의 포털 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Client Provisioning Portals(**클라이언트 프로비저닝 포털**)** > **Create, Edit, Duplicate, or Delete(**생성**,** 편집**,** 복제 또는 삭제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 입니다.

포털 설정

- **HTTPS Port(HTTPS** 포트**)**: 8000에서 8999 사이의 포트 값을 입력합니다. 기본값은 모든 기본 포털의 경우 8443이고 차단 목록 포털의 경우에는 8444입니다. 이 범위를 벗어나는 포트 값으로 업그레이드한 경우에는 이 페이지에서 설정을 변경할 때까지 해당 값이 적용됩니다. 이 페이지에서 설정을 변경하는 경우에는 이 제한을 준수하도록 포트 설정을 업데이트해야 합니다.
- **Allowed interfaces(**허용된 인터페이스**)**: 포털을 실행할 수 있는 PSN 인터페이스를 선택합니다. PSN에서 사용 가능한 허용된 인터페이스가 있는 PSN만 포털을 생성할 수 있습니다. 물리적 인터페이스와 결합형 인터페이스의 조합을 구성할 수 있습니다. 이는 PSN 전체에 적용되는 컨피그레이션입니다. 즉, 모든 포털은 이러한 인터페이스에서만 실행할 수 있으며 모든 PSN에 이 인터페이스 컨피그레이션이 푸쉬됩니다.
  - 다른 서브넷의 IP 주소를 사용하여 이더넷 인터페이스를 구성해야 합니다.
  - 여기서 활성화하는 인터페이스는 정책 서비스가 켜져 있는 경우의 VM 기반 PSN을 포함한 모든 PSN에서 사용할 수 있어야 합니다. 이는 게스트 세션 시작 시 이러한 PSN이 리디렉션에 사용될 수 있기 때문에 필요합니다.
  - 포털 인증서 주체 이름/대체 주체 이름에서는 인터페이스 IP를 확인해야 합니다.
  - 보조 인터페이스 IP를 FQDN에 매핑하려면 ISE CLI에서 ip host x.x.x.x yyy.domain.com을 구성합니다. 이는 인증서 주체 이름/대체 주체 이름과의 일치 여부를 확인하는 데 사용됩니다.
  - 결합형 NIC만 선택하는 경우 - PSN은 포털을 구성을 시도할 때 결합 인터페이스 구성을 먼저 시도합니다. 해당 PSN에서 결합이 설정되어 있지 않은 등의 이유로 인해 이 시도가 성공하지 못하면 PSN은 오류를 기록하고 종료됩니다. 물리적 인터페이스에서 포털을 시작하려고 시도하지는 않습니다.
  - **NIC Teaming(NIC** 팀**)** 또는 결합은 O/S 컨피그레이션 옵션으로, 이를 통해 고가용성(내결함성)을 위해 개별 NIC 2개를 구성할 수 있습니다. NIC 중 하나에서 장애가 발생하면 결합

형 연결의 일부분인 다른 NIC가 연결을 계속 진행합니다. 포털 설정 컨피그레이션을 기준으로 하여 포털에 대해 NIC를 선택합니다.

- 물리적 NIC와 해당하는 결합형 NIC가 모두 구성되어 있는 경우 - PSN은 포털을 구성할 때 결합 인터페이스 연결을 먼저 시도합니다. 해당 PSN에서 결합이 설정되어 있지 않은 등의 이유로 인해 이 시도가 성공하지 못하면 PSN은 물리적 인터페이스에서 포털을 시작하려고 시도합니다.

- **Certificate Group Tag(**인증서 그룹 태그**)**: 포털의 HTTPS 트래픽에 사용할 인증서 그룹의 그룹 태그를 선택합니다.
- **Authentication Method(**인증 방법**)**: 사용자 인증에 사용할 ISS(Identity Source Sequence) 또는 IdP(Identity Provider)를 선택합니다. ISS는 사용자 자격 증명을 확인하기 위해 순서대로 검색하는 ID 저장소 목록입니다. ISS의 예로는 내부 게스트 사용자, 내부 사용자, Active Directory, LDAP 등이 있습니다.

  Cisco ISE에는 클라이언트 프로비저닝 포털, Certificate_Request_Sequence에 대한 기본 클라이언트 프로비저닝 ID 소스 시퀀스가 포함되어 있습니다.

- **FQDN(Fully Qualified Domain Name)(FQDN(**정규화된 도메인 이름**))**: 클라이언트 프로비저닝 포털에 대해 고유한 FQDN 및/또는 호스트 이름을 하나 이상 입력합니다. 예를 들어 provisionportal.yourcompany.com을 입력할 수 있습니다. 그러면 사용자가 브라우저에 이 중 하나를 입력하는 경우 클라이언트 프로비저닝 포털에 연결할 수 있습니다.

  - 새 URL의 FQDN이 유효한 PSN(Policy Services Node) IP 주소로 확인되도록 DNS를 업데이트합니다. 필요한 경우 이 주소가 PSN 풀을 제공하는 로드 밸런서 가상 IP 주소를 가리키도록 지정할 수 있습니다.
  - 이름 불일치로 인한 인증서 경고 메시지가 표시되지 않도록 하려면 사용자 맞춤화된 URL의 FQDN 또는 와일드카드를 Cisco ISE PSN의 로컬 서버 인증서 SAN(Subject Alternative Name) 속성에 포함합니다.

  참고 URL 리디렉션 없는 클라이언트 프로비저닝의 경우 FQDN(Fully Qualified Domain Name) 필드에 입력된 포털 이름을 DNS 컨피그레이션에서 구성해야 합니다. URL 리디렉션 없이 클라이언트 프로비저닝을 활성화하려면 이 URL을 사용자에게 전달해야 합니다.

- **Idle Timeout(**유휴 시간 초과**)**: 포털에서 작업이 수행되지 않는 경우 Cisco ISE가 사용자를 로그아웃 처리할 때까지 대기하도록 할 시간을 분 단위로 입력합니다. 유효 범위는 1분~30분입니다.

참고 클라이언트 프로비저닝 포털에서 호스트가 클라이언트 프로비저닝 및 포스처에 대해 동일한 인증서를 다운로드할 수 있도록 포트 번호 및 인증서를 정의할 수 있습니다. 공식 인증 기관에서 포털 인증서를 서명한 경우 보안 경고가 표시되지 않습니다. 인증서가 자체 서명된 경우 포털과 Cisco AnyConnect Posture 구성 요소 모두에 대해 보안 경고가 한 번 표시됩니다.

로그인 페이지 설정

- Enable Login(로그인 활성화): 클라이언트 프로비저닝 포털에서 로그인 단계를 활성화하려면 이 확인란을 선택합니다.
- Maximum failed login attempts before rate limiting(속도 제한 전의 최대 로그인 시도 실패 횟수): Cisco ISE에서 로그인을 시도할 수 있는 속도를 인위적으로 늦춰 추가 로그인 시도를 차단할 때까지 단일 브라우저 세션에서 허용되는 로그인 시도 실패 횟수를 지정합니다. 이 로그인 실패 횟수에 도달한 이후의 로그인 시도 간 시간은 **Time between login attempts when rate limiting(**속도 제한 시의 로그인 시도 간 시간**)**에서 지정합니다.
- Time between login attempts when rate limiting(속도 제한 시의 로그인 시도 간 시간): 로그인이 **Maximum failed login attempts before rate limiting(**속도 제한 전의 최대 로그인 시도 실패 횟수**)** 에 정의된 횟수만큼 실패한 후 다시 로그인을 시도할 때까지 사용자가 대기해야 하는 시간을 분 단위로 설정합니다.
- Include an AUP (on page/as link)(AUP 포함(페이지에/링크로)): 회사의 네트워크 사용 약관을 사용자에게 현재 표시된 페이지에 텍스트로 보여주거나 AUP 텍스트가 포함된 새 탭 또는 창을 여는 링크로 표시합니다.
- Require acceptance(수락 필요): 사용자가 AUP를 수락해야 포털에 액세스할 수 있도록 지정합니다. 사용자가 AUP를 수락하지 않으면 **Login(**로그인**)** 버튼은 활성화되지 않습니다. AUP를 수락하지 않는 사용자는 포털에 액세스할 수 없습니다.
- Require scrolling to end of AUP(APU 끝으로 스크롤해야 함): 이 옵션은 **Include an AUP on page(**페이지에 **AUP** 포함**)**를 활성화하는 경우에만 표시됩니다. 사용자가 AUP의 전체 내용을 확인해야 하도록 지정합니다. 사용자가 AUP 끝으로 스크롤해야 **Accept(**수락**)** 버튼이 활성화됩니다.

AUP(Acceptable Use Policy) 페이지 설정

- Include an AUP(AUP 포함): 회사의 네트워크 사용 약관을 별도의 페이지에서 사용자에게 표시합니다.
- Require scrolling to end of AUP(APU 끝으로 스크롤해야 함): 사용자가 AUP의 전체 내용을 확인해야 하도록 지정합니다. 사용자가 AUP 끝으로 스크롤해야 Accept(수락) 버튼이 활성화됩니다.
- On first login only(첫 로그인 시에만): 사용자가 네트워크 또는 포털에 처음 로그인할 때 AUP를 표시합니다.
- On every login(로그인할 때마다): 사용자가 네트워크 또는 포털에 로그인할 때마다 AUP를 표시합니다.
- Every _____ days (starting at first login)(첫 로그인부터 _____일마다): 사용자가 네트워크 또는 포털에 처음 로그인한 후 정기적으로 AUP를 표시합니다.

Post-Login Banner(로그인 후 배너**)** 페이지 설정

Include a Post-Login Banner page(로그인 후 배너 페이지 포함): 사용자가 정상적으로 로그인하여 네트워크 액세스 권한을 부여받기 전에 추가 정보를 표시합니다.

비밀번호 변경 설정

Allow internal users to change their own passwords(내부 사용자의 비밀번호 변경 허용): 직원이 클라이언트 프로비저닝 포털에 로그인한 후 비밀번호를 변경하도록 허용합니다. 이 옵션은 Cisco ISE 데이터베이스에 계정이 저장되어 있는 직원에게만 적용되며 Active Directory 또는 LDAP와 같은 외부 데이터베이스에 계정이 저장되어 있는 직원에게는 적용되지 않습니다.

클라이언트 프로비저닝 포털 언어 파일을 위한 HTML 지원

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Client Provisioning Portals** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**입니다. 미니 편집기에서 **View HTML Source(HTML** 소스 보기**)** 아이콘을 사용하여 콘텐츠에 HTML 코드를 추가할 수 있습니다.

텍스트에서 HTML을 지원하는 포털 언어 속성 파일의 사전 키는 다음과 같습니다.

참고 이 목록은 파일 내 사전 키의 전체 목록이 아닙니다.

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2

- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message