위협 억제

Threat Centric NAC 서비스

TC-NAC(위협 중심 네트워크 액세스 제어) 기능을 사용하면 위협 및 취약점 어댑터에서 수신되는 위협 및 취약점 속성을 기준으로 권한 부여 정책을 생성할 수 있습니다. 위협 심각도 레벨 및 취약점 평가 결과를 사용하여 엔드포인트나 사용자의 액세스 레벨을 동적으로 제어할 수 있습니다.

취약성 및 위협 어댑터가 고품질 IoC(High Fidelity Indications of Compromise), 위협 탐지 이벤트 및 CVSS 점수를 Cisco ISE에 전송하도록 구성할 수 있으며 이를 통해 위협 중심 액세스 정책이 생성되어 엔드포인트의 권한 및 상황이 적절하게 변경될 수 있습니다.

Cisco ISE는 다음 어댑터를 지원합니다.

- SourceFire FireAMP
- CTA(Cognitive Threat Analytics) 어댑터
- Qualys

참고 현재 TC-NAC 플로우에서는 Qualys Enterprise Edition만 지원됩니다.

- Rapid7 Nexpose
- Tenable Security Center

엔드포인트에 대한 위협 이벤트가 탐지되면 **Compromised Endpoints(**침해 엔드포인트**)** 창에서 그 엔드포인트의 MAC 주소를 선택한 뒤 ANC 정책(예 : 격리)을 적용할 수 있습니다. Cisco ISE는 이 엔드포인트에 대해 CoA를 트리거하고 해당 ANC 정책을 적용합니다. ANC 정책을 사용할 수 없는 경우 Cisco ISE는 해당 엔드포인트에 대해 CoA를 트리거하고 원래 권한 부여 정책을 적용합니다. **Compromised Endpoints(**침해 엔드 포인트**)** 창에서 **Clear Threat and Vulnerabilities(**위협 및 취약점

지우기**)** 옵션을 사용하여 Cisco ISE 시스템 데이터베이스에서 엔드포인트와 관련된 위협 및 취약점을 지울 수 있습니다.

위협 사전 아래에는 다음 속성이 나열됩니다.

- CTA-Course_Of_Action(내부 차단, 근절 또는 모니터링을 값으로 사용할 수 있음)
- Qualys-CVSS_Base_Score
- Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

유효 범위는 기본 점수와 임시 점수 속성 모두 0~10입니다.

엔드포인트에 대한 취약점 이벤트가 수신되면 Cisco ISE는 해당 엔드포인트에 대해 CoA를 트리거합니다. 그러나 위협 이벤트가 수신되면 CoA는 트리거되지 않습니다.

취약성 속성을 사용하여 속성 값을 기반으로 취약한 엔드포인트를 자동으로 격리함으로써 권한 부여 정책을 생성할 수 있습니다. 예를 들면 다음과 같습니다.

```
Any Identity Group & Threat:Qualys-CVSS_Base_Score > 7.0 -> Quarantine
```

CoA 이벤트 중에 자동으로 격리되는 엔드포인트의 로그를 보려면 **Operations(**작업**)** > **Threat-Centric NAC Live Logs(Threat-Centric NAC** 라이브 로그**)**를 선택합니다. 수동으로 격리되는 엔드포인트의 로그를 보려면 **Operations(**작업**)** > **Reports(**보고서**)** > **Audit(**감사**)** > **Change Configuration Audit(**컨피그레이션 변경 감사**)**를 선택합니다.

Threat Centric NAC 서비스를 활성화할 때는 다음 사항에 유의하십시오.

- Threat Centric NAC 서비스에는 Cisco ISE Advantage 라이선스가 필요합니다.
- Threat Centric NAC 서비스는 구축 내 한 개 노드에서만 활성화할 수 있습니다.
- 취약점 평가 서비스에 벤더별로 어댑터 인스턴스를 하나만 추가할 수 있습니다. 그러나 FireAMP 어댑터의 인스턴스는 여러 개 추가할 수 있습니다.
- 컨피그레이션을 잃지 않고도 어댑터를 중지했다가 다시 시작할 수 있습니다. 어댑터를 구성한 후에는 언제든지 어댑터를 중지할 수 있습니다. 어댑터는 ISE 서비스가 재시작될 때도 이 상태를 유지합니다. 어댑터를 선택하고 **Restart(**재시작**)**을 클릭하여 어댑터를 다시 시작합니다.

참고 어댑터가 중지 상태인 동안에는 어댑터 인스턴스의 이름만 편집할 수 있습니다. 어댑터 컨피그레이션 또는 고급 설정은 편집할 수 없습니다.

다음 페이지에서 엔드포인트에 대한 위협 정보를 볼 수 있습니다.

- 홈 페이지 > 위협 대시보드
- 상황 가시성 > 엔드포인트 > 침해 엔드포인트

Threat Centric NAC 서비스는 다음 경보를 트리거합니다.

- Adapter not reachable(어댑터에 연결할 수 없음)(syslog ID: 91002): 어댑터에 연결할 수 없음을 나타냅니다.
- Adapter Connection Failed(어댑터 연결 실패)(syslog ID: 91018): 어댑터에 연결할 수 있지만 어댑터와 소스 서버 간의 연결이 끊겼음을 나타냅니다.
- Adapter Stopped Due to Error(오류로 인해 어댑터가 중지됨)(syslog ID: 91006): 어댑터가 바람직한 상태가 아닌 경우 이 경보가 트리거됩니다. 이 경보가 표시되면 어댑터 컨피그레이션 및 서버 연결을 확인합니다. 자세한 내용은 어댑터 로그를 참조하십시오.
- Adapter Error(어댑터 오류)(syslog ID: 91009): Qualys 어댑터가 Qualys 사이트와 연결을 설정할 수 없거나 Qualys 사이트에서 정보를 다운로드 할 수 없음을 나타냅니다.

Threat Centric NAC 서비스에 대해 다음 보고서를 이용할 수 있습니다.

- **Adapter Status(**어댑터 상태**)**: 어댑터 상태 보고서에는 위협 및 취약점 어댑터의 상태가 표시됩니다.
- **COA Events(COA** 이벤트**)**: 엔드포인트에 대한 취약점 이벤트가 수신되면 Cisco ISE는 해당 엔드포인트에 대해 CoA를 트리거합니다. CoA 이벤트 보고서에는 이러한 CoA 이벤트의 상태가 표시됩니다. 또한 이전 권한 부여 규칙 및 새 권한 부여 규칙과 이러한 엔드포인트에 대한 프로파일 세부정보도 표시됩니다.
- **Threat Events(**위협 이벤트**)**: Threat Events(위협 이벤트) 보고서는 Cisco ISE가 사용자가 구성한 다양한 어댑터에서 수신하는 모든 위협 이벤트의 목록을 제공합니다. 취약점 평가 이벤트는 이 보고서에 포함되지 않습니다.
- **Vulnerability Assessment(**취약점 평가**)**: 취약점 평가 보고서는 엔드포인트에 대해 수행되는 평가와 관련된 정보를 제공합니다. 이 보고서를 보고 구성된 정책을 기준으로 평가가 수행되는지를 확인할 수 있습니다.

Operations(작업**) > Reports(**보고서**) > Diagnostics(**진단**) > ISE Counters(ISE** 카운터**) > Threshold Counter Trends(**임계값 카운터 트렌드**)**에서 다음 정보를 볼 수 있습니다.

- 수신한 총 이벤트 수
- 총 위협 이벤트 수
- 총 취약점 이벤트 수
- PSN에 발급된 총 CoA 수

이러한 속성의 값은 5분마다 수집되므로 마지막 5분 동안의 수를 나타냅니다.

위협 대시보드에는 다음 대시릿이 포함되어 있습니다.

- **Total Compromised Endpoints(**총 침해 엔드포인트**)** 대시릿에는 현재 네트워크에서 영향을 받은 총 엔드포인트(연결된 엔드포인트와 연결되지 않은 엔드포인트 모두)의 수가 표시됩니다.
- **Compromised Endpoints Over Time(**시간별 침해 엔드포인트**)** 대시릿에는 지정된 기간 동안 엔드포인트에 미친 영향에 대한 기록 보기가 표시됩니다.

- **Top Threats(**상위 위협**)** 대시릿에는 영향 받은 엔드포인트 수와 위협의 심각도를 기반으로 상위 위협이 표시됩니다.
- **Threats Watchlist(**위협 감시 목록**)** 대시릿을 사용하여 선택한 이벤트의 추세를 분석할 수 있습니다.

Top Threats(상위 위협**)** 대시릿의 거품 방울 크기는 영향 받는 엔드포인트의 수를 나타내며, 밝은 음영 영역은 연결이 끊긴 엔드포인트의 수를 나타냅니다. 색상 및 세로 눈금은 위협의 심각도를 나타냅니다. 위협의 범주는 지표와 인시던트로 두 가지가 있습니다. 지표의 심각도 속성은 "Likely_Impact"이고 인시던트의 심각도 속성은 "Impact_Qualification"입니다.

Compromised Endpoint(침해 엔드포인트) 창에는 영향 받는 엔드포인트의 매트릭스 보기와 각 위협 범주에 대한 영향의 심각도가 표시됩니다. 디바이스 링크를 클릭하여 엔드포인트에 대한 자세한 위협 정보를 볼 수 있습니다.

Action Of Action(조치 과정) 차트에는 CTA 어댑터에서 수신한 CTA-Course_Of_Action 속성을 기반으로 위협 인시던트에 대해 취해진 조치(내부 차단, 근절 또는 모니터링)가 표시됩니다.

홈 페이지의 취약점 대시보드에는 다음 대시릿이 포함되어 있습니다.

- **Total Vulnerable Endpoints(**총 취약 엔드포인트**)** 대시릿에는 CVSS 점수가 지정된 값보다 큰 총 엔드포인트 수가 표시됩니다. 또한 CVSS 점수가 지정된 값보다 큰 연결된 및 연결되지 않은 엔드포인트의 총 개수도 표시됩니다.
- **Top Vulnerability(**상위 취약점**)** 대시릿에는 영향 받는 엔드포인트의 수 또는 취약점의 심각도를 기반으로 상위 취약점이 표시됩니다. Top Vulnerability(상위 취약점) 대시릿의 거품 방울 크기는 영향 받는 엔드포인트의 수를 나타내며, 밝은 음영 영역은 연결되지 않은 엔드포인트의 수를 나타냅니다. 색상 및 세로 눈금은 취약점의 심각도를 나타냅니다.
- **Vulnerability Watchlist(**취약점 감시**)** 대시릿을 사용하면 선택한 취약점에 대한 일정 기간 동안의 추세를 분석할 수 있습니다. 대시릿에서 검색 아이콘을 클릭하고 벤더별 ID(Qualys ID 번호의 경우 "qid")를 입력하여 해당 특정 ID 번호의 트렌드를 선택하고 볼 수 있습니다.
- **Vulnerable Endpoints Over Time(**시간별 취약 엔드포인트**)** 대시릿에는 엔드포인트에 미치는 영향에 대한 시간 경과에 따른 기록 보기가 표시됩니다.

Vulnerable Endpoints(취약 엔드포인트**)** 창의 CVSS별 엔드포인트 수 그래프에는 영향 받는 엔드포인트의 수와 해당 CVSS 점수가 표시됩니다. **Vulnerable Endpoints(**취약 엔드포인트**)** 창에서 영향 받는 엔드포인트의 목록도 볼 수 있습니다. 디바이스 링크를 클릭하여 각 엔드포인트에 대한 세부적인 취약점 정보를 볼 수 있습니다.

Threat Centric NAC 서비스 로그는 지원 번들에 포함되어 있습니다(Cisco ISE 로그 파일 다운로드 참조). Threat Centric NAC 서비스 로그는 support/logs/TC-NAC/에 있습니다.

Threat Centric NAC 서비스 활성화

취약점 및 위협 어댑터를 구성하려면 먼저 Threat Centric NAC 서비스를 활성화해야 합니다. 이 서비스는 구축의 정책 서비스 노드 하나에서만 활성화할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Deployment(구축)**를 선택합니다.

단계 **2** Threat Centric NAC 서비스를 활성화할 PSN 옆의 확인란을 선택하고 **Edit(편집)**를 클릭합니다.

단계 **3** **Enable Threat Centric NAC Service(Threat Centric NAC 서비스 활성화)** 확인란을 선택합니다.

단계 **4** **Save(저장)**를 클릭합니다.

관련 항목

SourceFire FireAMP 어댑터 추가, 5 페이지
Cognitive Threat Analytics 어댑터 구성, 6 페이지
CTA 어댑터를 위한 권한 부여 프로파일 구성, 8 페이지
작업 과정 속성을 사용하여 권한 부여 정책 구성, 8 페이지
Threat Centric NAC 서비스, 1 페이지

SourceFire FireAMP 어댑터 추가

시작하기 전에

- SourceFire FireAMP가 있는 계정이 있어야 합니다.
- 모든 엔드포인트에서 FireAMP 클라이언트를 구축해야 합니다.
- 구축 노드에서 Threat Centric NAC 서비스를 활성화해야 합니다(Threat Centric NAC 서비스 활성화, 4 페이지 참고).
- FireAMP 어댑터는 AMP 클라우드에 대한 REST API 호출에 SSL을 사용하고 이벤트를 수신하는 데 AMQP를 사용합니다. 또한 프록시 사용을 지원합니다. FireAMP 어댑터는 통신에 포트 443을 사용합니다.

단계 **1** **Administration(관리)** > **Threat Centric NAC** > **Third Party Vendors(**서드파티 벤더**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Add(추가)**를 클릭합니다.

단계 **3** **Vendor(벤더)** 드롭다운 목록에서 **AMP: Threat**를 선택합니다.

단계 **4** 어댑터 인스턴스의 이름을 입력합니다.

단계 **5** **Save(저장)**를 클릭합니다.

단계 **6** Vendor Instances(벤더 인스턴스) 목록 창을 새로 고칩니다. Vendor Instances(벤더 인스턴스) 목록 창에서 어댑터 상태가 **Ready to Configure(구성 준비)**로 변경된 후에만 어댑터를 구성할 수 있습니다.

단계 **7** **Ready to Configure(구성 준비)** 링크를 클릭합니다.

단계 **8** (선택 사항) 모든 트래픽을 라우팅하도록 SOCKS 프록시 서버를 구성한 경우 프록시 서버의 호스트 이름 및 포트 번호를 입력합니다.

단계 **9** 연결하려는 클라우드를 선택합니다. US 클라우드 또는 EU 클라우드를 선택할 수 있습니다.

단계 **10** 구독할 이벤트 소스를 선택합니다. 다음 옵션을 사용할 수 있습니다.

- **AMP** 이벤트만
- **CTA** 이벤트만
- **CTA** 및 **AMP** 이벤트

단계 **11** FireAMP 링크를 클릭하고 FireAMP에서 관리자로 로그인합니다. **Applications(**애플리케이션**)** 창에서 **Allow(**허용**)**를 클릭하여 스트리밍 이벤트 내보내기 요청에 권한을 부여합니다.
Cisco ISE로 다시 리디렉션됩니다.

단계 **12** 모니터링하려는 이벤트(예: 의심스러운 다운로드, 의심스러운 도메인으로의 연결, 실행된 악성코드, java 보안 침해)를 선택합니다.

고급 설정을 변경하거나 어댑터를 재구성할 때 AMP 클라우드에 새 이벤트가 추가된 경우 해당 이벤트도 **Events Listing(**이벤트 목록**)** 창에 나열됩니다.

어댑터의 로그 레벨을 선택할 수 있습니다. 사용 가능한 옵션은 **Error**, **Info**, **Debug**입니다.

어댑터 인스턴스 구성의 요약이 **Configuration Summary(**구성 요약**)** 창에 표시됩니다.

Cognitive Threat Analytics 어댑터 구성

시작하기 전에

- 구축 노드에서 Threat Centric NAC 서비스를 활성화해야 합니다(Threat Centric NAC 서비스 활성화, 4 페이지 참고).
- http://cognitive.cisco.com/login을 통해 Cisco CTA(Cognitive Threat Analytics) 포털에 로그인하고 CTA STIX/TAXII 서비스를 요청합니다. 자세한 내용은 Cisco ScanCenter Center 관리자 가이드를 참조하십시오.
- CTA(Cognitive Threat Analytics) 어댑터는 SSL과 함께 TAXII 프로토콜을 사용하여, 탐지된 위협에 대해 CTA 클라우드를 폴링합니다. 또한 프록시의 사용을 지원합니다.
- 신뢰할 수 있는 인증서 저장소로 어댑터 인증서를 가져옵니다. 인증서를 가져오려면 **Administration(**관리**) > System(**시스템**) > Certificates(**인증서**) > Trusted Certificates(**신뢰할 수 있는 인증서**) > Import(**가져오기**)**를 선택합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Threat Centric NAC > Third Party Vendors(**서드파티 벤더**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Vendor(**벤더**)** 드롭다운 목록에서 **CTA : Threat**를 선택합니다.

단계 **4** 어댑터 인스턴스의 이름을 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** Vendor Instances(벤더 인스턴스) 목록 페이지를 새로 고칩니다. Vendor Instances(벤더 인스턴스) 목록 페이지에서 어댑터 상태가 **Ready to Configure(**구성 준비**)**로 변경된 후에만 어댑터를 구성할 수 있습니다.

단계 **7** **Ready to Configure(**구성 준비**)** 링크를 클릭합니다.

단계 **8** 다음 세부정보를 입력합니다.

- **CTA STIX/TAXII service URL(CTA STIX/TAXII** 서비스 **URL)**: CTA 클라우드 서비스의 URL. 기본적으로 https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService/ URL이 사용됩니다.
- **CTA feed name(CTA** 피드 이름**)**: CTA 클라우드 서비스의 피드 이름을 입력합니다.
- **CTA username and password(CTA** 사용자 이름 및 비밀번호**)**: CTA 클라우드 서비스의 사용자 이름 및 비밀번호를 입력합니다.
- **Proxy host and port (optional)(**프록시 호스트 및 포트**(**선택 사항**))**: 모든 트래픽을 라우팅하도록 프록시 서버를 구성한 경우 프록시 서버의 호스트 이름 및 포트 번호를 입력합니다.
- **Polling interval(**폴링 간격**)**: 각 폴링 사이의 시간 간격. 기본값은 30분입니다.
- **First Poll Duration in hours(**첫 번째 폴링 기간**(**시간**))**: 첫 번째 폴링에서 가져올 데이터의 기간. 기본값은 2시간입니다. 최대 값은 12시간입니다.
- **Incident Type(**인시던트 유형**)**: 다음 옵션을 사용할 수 있습니다.
  - **CTA** 이벤트만
  - **AMP** 이벤트만
  - **CTA** 및 **AMP** 이벤트

단계 **9** **Next(**다음**)**를 클릭합니다.

단계 **10** **Advanced Settings(**고급 설정**)** 탭에서 다음 옵션을 구성합니다.

- **Impact Qualification(**영향 자격**)**: 폴링할 인시던트의 심각도 레벨을 선택합니다. 다음 옵션을 사용할 수 있습니다.
  - **1 -** 중요하지 않음
  - **2 -** 주의 분산
  - **3 -** 영향 있음
  - **4 -** 손상 있음
  - **5 -** 치명

  예를 들어 "3-영향 있음"을 선택한 경우 이 심각도 레벨(3-영향 있음)과 그보다 높은 심각 도레벨(이 예에서는 4-손상 있음 및 5-치명)이상의 인시던트가 폴링됩니다.
- **Logging level(**로깅 레벨**)**: 어댑터의 로그 레벨을 선택합니다. 사용 가능한 옵션은 Error, Info, Debug입니다.

단계 **11** **Finish(**종료**)**를 클릭합니다.

참고 CTA는 웹 프록시 로그에 나열된 사용자 ID를 IP 주소 또는 사용자 이름으로 사용합니다. 특히 IP 주소의 경우 프록시 로그를 통해 사용 가능한 디바이스의 IP 주소가 내부 네트워크에있는 다른 디바이스의 IP 주소와 충돌할 수 있습니다. 예를 들어 AnyConnect와 스플릿 터널링을 통해 연결되는 사용자를 인터넷에 직접 로밍하면 로컬 IP 범위 주소(예: 10.0.0.X 주소)를 가져올 수 있습니다. 이 주소는 내부 네트워크에서 사용되는 중복 개인 IP 범위의 주소와 충돌할 수 있습니다. 불일치 디바이스에 격리 작업이 적용되지 않도록 정책을 정의하는 동시에 논리적 네트워크 아키텍처를 함께 고려하는 것이 좋습니다.

CTA 어댑터를 위한 권한 부여 프로파일 구성

각 위협 이벤트에 대해 CTA 어댑터는 Course of Action(작업 과정) 속성에 대해 Internal Blocking(내부 차단), Monitoring(모니터링) 또는 Eradication(제거) 값 중 하나를 반환합니다. 이러한 값을 기준으로 권한 부여 프로파일을 생성할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**) > Policy Elements(**정책 요소**) > Authorization(**권한 부여**) > Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 권한 부여 프로파일의 이름과 설명을 입력합니다.

단계 **4** 액세스 유형을 선택합니다.

단계 **5** 필요한 세부정보를 입력하고 **Submit(**제출**)**을 클릭합니다.

작업 과정 속성을 사용하여 권한 부여 정책 구성

CTA-Course_Of_Action 속성을 사용하여 위협 이벤트가 보고되는 엔드포인트에 대한 권한 부여 정책을 구성할 수 있습니다. 이러한 속성은 Threat(위협) 디렉토리에서 사용할 수 있습니다.

CTA-Course_Of_Action 속성을 기반으로 예외 규칙을 생성할 수도 있습니다.

단계 **1** **Policy(**정책**) > Policy Sets(**정책 집합**)**를 선택합니다.
위협 이벤트가 있는 엔드포인트에 대해 기존 정책 규칙을 수정하거나 새 예외 규칙을 생성할 수 있습니다.

단계 **2** CTA-Course_Of_Action 속성 값을 확인하고 적절한 권한 부여 프로파일을 할당하는 조건을 생성합니다. 예를 들면 다음과 같습니다.

Network_Access_Authentication_Passed AND ThreatCTA-Course_Of_Action CONTAINS Internal Blocking then blocking (authorization profile)

참고 "Internal Blocking(내부 차단)"은 엔드포인트를 격리하는 데 사용할 권장되는 Course of Action(작업 과정) 속성입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

엔드포인트에 대한 위협 이벤트가 수신되면 Cisco ISE는 엔드포인트에 일치하는 권한 부여 정책이 있는지 확인하고 엔드포인트가 활성 상태인 경우에만 CoA를 트리거합니다. 엔드포인트가 오프라인 상태인 경우 위협 이벤트 세부정보가 위협 이벤트 보고서에 추가됩니다(Operations(운영)> Reports(보고서)> Threat Centric NAC > Threat Events(위협 이벤트)).

참고 경우에 따라 CTA는 하나의 사고에서 여러 리스크 및 이와 관련된 Course of Action(작업 과정) 속성을 전송하기도 합니다. 예를 들어 하나의 사고에서 "Internal Blocking(내부 차단)"및 "Monitoring(모니터링)"(작업 과정 속성)을 전송할 수 있습니다. 이 경우 "Equals(같음)" 연산자를 사용하여 엔드포인트를 격리하도록 권한 부여 정책을 구성하면 엔드포인트가 격리되지 않습니다. 예를 들면 다음과 같습니다.

```
CTA-Course_Of_Action EQUALS Internal Blocking then Quarantine_Systems (authorization profile)
```

이러한 경우 권한 부여 정책에서 "Contains(포함)" 연산자를 사용하여 엔드포인트를 격리해야 합니다. 예를 들면 다음과 같습니다.

```
CTA-Course_Of_Action CONTAINS Internal Blocking then Quarantine_Systems
```

Cisco ISE의 취약점 평가 지원

Cisco ISE는 다음의 VA(취약점 평가) 에코시스템 파트너와 통합되어 Cisco ISE 네트워크에 연결된 엔드포인트의 취약점 결과를 가져옵니다.

- Qualys: Qualys는 네트워크에 스캐너 어플라이언스가 구축된 클라우드 기반 평가 시스템입니다. Cisco ISE에서는 Qualys와 통신하여 VA 결과를 가져오는 어댑터를 구성할 수 있습니다. 관리 포털에서 어댑터를 구성할 수 있습니다. 어댑터를 구성하려면 슈퍼 관리자 권한이 있는 Cisco ISE 관리자 계정이 필요합니다. Qualys 어댑터는 REST API를 사용하여 Qualys Cloud Service와 통신합니다. Qualys에서 REST API에 액세스 가능한 관리자 권한이 있는 사용자 계정이 필요합니다. Cisco ISE는 다음과 같은 Qualys REST API를 사용합니다.
  - 호스트 탐지 목록 API: 엔드포인트의 마지막 스캔 결과를 확인합니다.
  - API 스캔 : 엔드포인트의 온디맨드 스캔을 트리거합니다.

  Qualys는 가입된 사용자가 수행할 수 API 호출 수에 대해 제한을 적용합니다. 기본 속도 제한 수는 24시간당 300회입니다. Cisco ISE는 Qualys API 2.0 버전을 사용하여 Qualys에 연결합니다. 이러한 API 기능에 대한 자세한 내용은 Qualys API V2 사용 설명서를 참조하십시오.
- Rapid7 Nexpose: Cisco ISE는 취약점 관리 솔루션인 Rapid 7 Nexpose와 통합되어 취약점을 탐지하고 이러한 위협에 신속하게 대응하는 데 도움을 줍니다. Cisco ISE는 Nexpose에서 취약점 데이터를 수신하며, ISE에서 구성한 정책에 따라 영향을 받는 엔드포인트를 격리합니다. Cisco ISE 대시 보드에서 영향 받는 엔드포인트를 보고 적절한 조치를 취할 수 있습니다.

  Cisco ISE는 Nexpose 릴리스 6.4.1에서 테스트되었습니다.

- Tenable SecurityCenter(Nessus 스캐너) : Cisco ISE는 Tenable SecurityCenter와 통합되고 Tenable Nessus 스캐너(Tenable SecurityCenter에서 관리)에서 취약점 데이터를 수신하며 ISE에서 구성한 정책에 따라 영향받는 엔드포인트를 격리합니다. Cisco ISE 대시 보드에서 영향 받는 엔드포인트를 보고 적절한 조치를 취할 수 있습니다.

  Cisco ISE는 Tenable SecurityCenter 5.3.2에서 테스트되었습니다.

에코시스템 파트너의 결과는 STIX(Structured Threat Information Expression) 표현으로 변환되며, 이 값을 기반으로 CoA(Change of Authorization)가 트리거되고 필요한 경우 엔드포인트에 대한 적절한 액세스 레벨이 부여됩니다.

엔드포인트의 취약점을 평가하는 데 걸리는 시간은 다양한 요인에 따라 달라지므로 VA를 실시간으로 수행할 수 없습니다. 엔드포인트의 취약점을 평가하는 데 걸리는 시간에 영향을 미치는 요인은 다음과 같습니다.

- 취약점 평가
- 스캔되는 취약점의 유형
- 활성화되는 스캔 유형
- 에코시스템에서 스캐너 어플라이언스에 대해 할당한 네트워크 및 시스템 리소스

이 Cisco ISE 릴리스에서는 IPv4 주소가있는 엔드 포인트 만 취약점을 평가할 수 있습니다.

취약점 평가 서비스 활성화 및 구성

Cisco ISE에서 취약점 평가 서비스를 활성화하고 구성하려면 다음 작업을 수행합니다.

단계 **1** Threat Centric NAC 서비스 활성화, 4 페이지.

단계 **2** 구성하려면 다음을 따릅니다.

- Qualys 어댑터는 Qualys 어댑터 구성, 11 페이지를 참조하십시오.
- Nexpose 어댑터는 Nexpose 어댑터 구성, 14 페이지를 참조하십시오.
- Tenable 어댑터는 Tenable 어댑터 구성, 17 페이지를 참조하십시오.

단계 **3** 권한 부여 프로파일 구성, 20 페이지.

단계 **4** 취약한 엔드포인트 격리를 위한 예외 규칙 구성, 21 페이지.

Threat Centric NAC 서비스 활성화

취약점 및 위협 어댑터를 구성하려면 먼저 Threat Centric NAC 서비스를 활성화해야 합니다. 이 서비스는 구축의 정책 서비스 노드 하나에서만 활성화할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Deployment(구축)**를 선택합니다.

단계 **2** Threat Centric NAC 서비스를 활성화할 PSN 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Enable Threat Centric NAC Service(Threat Centric NAC** 서비스 활성화**)** 확인란을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

관련 항목

SourceFire FireAMP 어댑터 추가, 5 페이지
Cognitive Threat Analytics 어댑터 구성, 6 페이지
CTA 어댑터를 위한 권한 부여 프로파일 구성, 8 페이지
작업 과정 속성을 사용하여 권한 부여 정책 구성, 8 페이지
Threat Centric NAC 서비스, 1 페이지

Qualys 어댑터 구성

Cisco ISE는 Qualys Vulnerability Assessment Ecosystem을 지원합니다. Cisco ISE가 Qualys와 통신하고 VA 결과를 얻도록 하려면 Qualys 어댑터를 생성해야 합니다.

시작하기 전에

- 다음 사용자 계정이 있어야 합니다.
  - 벤더 어댑터를 구성할 수 있도록 슈퍼 관리자 권한이 있는 Cisco ISE의 관리 사용자 계정
  - 관리자 권한이 있는 Qualys의 사용자 계정
- 적절한 Qualys 라이선스 구독이 있는지 확인합니다. Qualys Report Center, KBX(Knowledge Base) 및 API 액세스 권한이 필요합니다. 자세한 내용은 Qualys 어카운트 매니저에게 문의하십시오.
- Cisco ISE(**Administration(**관리**) > Certificates(**인증서**) > Certificate Management(**인증서 관리**) > Trusted Certificates(**신뢰할 수 있는 인증서**) > Import(**가져오기**)**)에서 Qualys 서버 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다. Cisco ISE 신뢰할 수 있는 인증서 저장소에서 적절한 루트 및 중간 인증서를 가져왔는지 또는 해당 인증서가 있는지 확인합니다.
- 다음 컨피그레이션은 Qualys API 가이드를 참조하십시오.
  - Qualys(**Reports(**보고서**) > Setup(**설정**) > CVSS Scoring(CVSS** 점수**) > Enable CVSS Scoring(CVSS** 점수 활성화**)**)에서 CVSS 점수를 활성화했는지 확인합니다.
  - Qualys(**Assets(**자산**) > Host Assets(**호스트 자산**)**)에서 엔드포인트의 IP 주소 및 서브넷 마스크를 추가해야 합니다.
  - Qualys 옵션 프로파일의 이름이 있는지 확인합니다. 옵션 프로파일은 Qualys에서 스캔에 사용할 스캐너 템플릿입니다. 인증된 스캔을 포함하는 옵션 프로파일을 사용하는 것이 좋습니다. 이 옵션은 엔드포인트의 MAC 주소도 확인합니다.
- Cisco ISE는 HTTPS/SSL(포트 443)을 통해 Qualys와 통신합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Threat Centric NAC** > **Third Party Vendors(**서드파티 벤더**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Vendor(**벤더**)** 드롭다운 목록에서 **Qualys:VA**를 선택합니다.

단계 **4** 어댑터 인스턴스의 이름을 입력합니다. Qualys_Instance를 예로 들 수 있습니다.

구성된 어댑터 인스턴스 목록과 함께 목록 창이 나타납니다.

단계 **5** Vendor Instances(벤더 인스턴스) 목록 창을 새로 고칩니다. 새로 추가된 Qualys_Instance 어댑터의 상태가 **Ready to Configure(**구성 준비**)**로 변경되어야 합니다.

단계 **6** **Ready to Configure(**구성 준비**)** 링크를 클릭합니다.

단계 **7** Qualys 컨피그레이션 화면에서 다음 값을 입력하고 **Next(**다음**)**를 클릭합니다.

필드 이름	설명
REST API Host(REST API 호스트**)**	Qualys 클라우드를 호스팅하는 서버의 호스트 이름입니다. 자세한 내용은 Qualys 담당자에게 문의하십시오.
REST API Port(REST API 포트**)**	443
Username(사용자 이름**)**	관리자 권한이 있는 Qualys의 사용자 계정입니다.
Password(비밀번호**)**	Qualys 사용자 계정의 비밀번호입니다.
HTTP Proxy Host(HTTP 프록시 호스트**)**	모든 인터넷 트래픽을 라우팅하도록 프록시 서버를 구성한 경우 프록시 서버의 호스트 이름을 입력합니다.
HTTP Proxy Port(HTTP 프록시 포트**)**	프록시 서버에서 사용하는 포트 번호를 입력합니다.

Qualys 서버에 대한 연결이 설정된 경우 Qualys 스캐너 목록과 함께 Scanner Mappings(스캐너 매핑) 창이 나타납니다. 사용 중인 네트워크의 Qualys 스캐너가 이 창에 표시됩니다.

단계 **8** Cisco ISE가 온디맨드 스캔에 사용할 기본 스캐너를 선택합니다.

단계 **9** **PSN to Scanner Mapping(PSN-**스캐너 매핑**)** 영역에서 PSN노드에 Qualys 스캐너 어플라이언스를 하나 이상 선택하고 **Next(**다음**)**를 클릭할 수 있습니다.

Advanced Settings(고급 설정**)** 창이 나타납니다.

단계 **10** **Advanced Setting(**고급 설정**)** 창에서 다음 값을 입력합니다. 이 창의 설정에 따라 VA에 대해 마지막 스캔 결과가 사용되는지 아니면 온디맨드 스캔이 트리거되는지가 결정됩니다.

필드 이름	설명
Option Profile(옵션 프로파일**)**	Qualys에서 엔드포인트를 스캔하는 데 사용하도록 할 옵션 프로파일을 선택합니다. 기본 옵션 프로파일인 Initial Options(초기 옵션)를 선택할 수 있습니다.
마지막 스캔 결과 - 설정 확인	
Last scan results check interval in minutes(마지막 스캔 결과 확인 간격**(**분**))**	(호스트 탐지 목록 API의 액세스 속도에 영향을 줌) 마지막 스캔 결과를 다시 확인해야 할 때까지의 시간 간격(분)입니다. 유효 범위는 1~2880입니다.
Maximum results before last scan results are checked(마지막 스캔 결과를 확인할 때까지의 최대 결과 수**)**	(호스트 탐지 목록 API의 액세스 속도에 영향을 줌) 대기열에 있는 스캔 요청 수가 여기서 지정한 최대 수를 초과하면 **Last scan results check interval in minutes(**마지막 스캔 결과 확인 간격**(**분**))** 필드에서 지정한 시간 간격이 되기 전에 마지막 스캔 결과를 확인합니다. 유효 범위는 1~1000입니다.
Verify MAC address(MAC 주소 확인**)**	True 또는 False입니다. true로 설정하면 엔드포인트의 MAC 주소가 포함되어 있는 경우에만 Qualys의 마지막 스캔 결과를 사용합니다.
Scan Settings(스캔 설정**)**	
Scan trigger interval in minutes(스캔 트리거 간격**(**분**))**	(스캔 API의 액세스 속도에 영향을 줌) 온디맨드 스캔이 트리거될 때까지의 시간 간격(분)입니다. 유효 범위는 1~2880입니다.
Maximum requests before scan is triggered(스캔을 트리거할 때까지의 최대 요청 수**)**	(스캔 API의 액세스 속도에 영향을 줌) 대기열에 있는 스캔 요청 수가 여기서 지정한 최대 수를 초과하면 **Scan trigger interval in minutes(**스캔 트리거 간격**(**분**))** 필드에서 지정한 시간 간격이 되기 전에 온디맨드 스캔이 트리거됩니다. 유효 범위는 1~1000입니다.
Scan status check interval in minutes(스캔 상태 확인 간격**(**분**))**	Cisco ISE가 Qualys와 통신하여 스캔 상태를 확인할 때까지의 시간 간격(분)입니다. 유효 범위는 1~60입니다.
Number of scans that can be triggered concurrently(동시에 트리거할 수 있는 스캔 수**)**	(이 옵션은 Scanner Mappings(스캐너 매핑) 화면에서 각 PSN에 매핑한 스캐너 수에 따라 달라짐) 각 스캐너는 요청을 한 번에 하나씩만 처리할 수 있습니다. PSN에 둘 이상의 스캐너를 매핑한 경우에는 선택한 스캐너 수에 따라 이 값을 증가시킬 수 있습니다. 유효 범위는 1~200입니다.

필드 이름	설명
Scan timeout in minutes(스캔 시간 초과**(**분**))**	스캔 요청이 시간 초과될 때까지의 시간(분)입니다. 스캔 요청이 시간 초과되면 경보가 생성됩니다. 유효 범위는 20~1440입니다.
Maximum number of IP addresses to be submitted per scanner(스캐너당 제출할 최대 **IP** 주소 수**)**	처리를 위해 Qualys로 전송하도록 단일 요청에 대기시킬 수 있는 요청의 수를 나타냅니다. 유효 범위는 1~1000입니다.
Choose the log level for adapter log files(어댑터 로그 파일의 로그 레벨 선택**)**	어댑터의 로그 레벨을 선택합니다. 사용 가능한 옵션은 ERROR, INFO, DEBUG 및 TRACE입니다.

단계 **11** 컨피그레이션 설정을 검토하려면 **Next(**다음**)**를 클릭합니다.

단계 **12** **Finish(**종료**)**를 클릭합니다.

Nexpose 어댑터 구성

Cisco ISE가 Nexpose와 통신하고 VA 결과를 얻도록 하려면 Nexpose 어댑터를 생성해야 합니다.

시작하기 전에

- Cisco ISE에서 위협 중심 NAC 서비스를 활성화했는지 확인합니다.
- Nexpose 보안 콘솔에 로그인하여 다음 권한으로 사용자 계정을 생성합니다.
  - 사이트 관리
  - 보고서 생성
- Nexpose 서버 인증서를 Cisco ISE의 신뢰할 수 있는 인증서 저장소로 가져옵니다(**Administration(**관리**) > Certificates(**인증서**) > Certificate Management(**인증서 관리**) > Trusted Certificates(**신뢰할 수 있는 인증서**) > Import(**가져오기**)**). Cisco ISE 신뢰할 수 있는 인증서 저장소에서 적절한 루트 및 중간 인증서를 가져왔는지 또는 해당 인증서가 있는지 확인합니다.
- Cisco ISE는 HTTPS/SSL(포트 3780)을 통해 Nexpose와 통신합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Threat Centric NAC** > **Third Party Vendors(**서드파티 벤더**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Vendor(**벤더**)** 드롭다운 목록에서 **Rapid7 Nexpose:VA**를 선택합니다.

단계 **4** 어댑터 인스턴스의 이름을 입력합니다. 예를 들어 Nexpose를 입력합니다.

구성된 어댑터 인스턴스 목록과 함께 목록 창이 나타납니다.

단계 **5** Vendor Instances(벤더 인스턴스) 목록 창을 새로 고칩니다. 새로 추가된 Nexpose 어댑터의 상태가 **Ready to Configure(**구성 준비**)**로 변경되어야 합니다.

단계 **6** **Ready to Configure(**구성 준비**)** 링크를 클릭합니다.

단계 **7** Nexpose 컨피그레이션 화면에서 다음 값을 입력하고 **Next(**다음**)**를 클릭합니다.

필드 이름	설명
Nexpose Host(Nexpose 호스트**)**	Nexpose 서버의 호스트 이름입니다.
Nexpose Port(Nexpose 포트**)**	3780입니다.
Username(사용자 이름**)**	Nexpose 관리 사용자 계정입니다.
Password(비밀번호**)**	Nexpose 관리 사용자 계정의 비밀번호입니다.
HTTP Proxy Host(HTTP 프록시 호스트**)**	모든 인터넷 트래픽을 라우팅하도록 프록시 서버를 구성한 경우 프록시 서버의 호스트 이름을 입력합니다.
HTTP Proxy Port(HTTP 프록시 포트**)**	프록시 서버에서 사용하는 포트 번호를 입력합니다.

단계 **8** **Next(**다음**)**를 클릭하여 고급 설정을 구성합니다.

단계 **9** **Advanced Setting(**고급 설정**)** 창에서 다음 값을 입력합니다. 이 창의 설정에 따라 VA에 대해 마지막 스캔 결과가 사용되는지 아니면 온디맨드 스캔이 트리거되는지가 결정됩니다.

필드 이름	설명
최신 스캔 결과 확인 설정	
Interval between checking the latest scan results in minutes(최신 스캔 결과 확인 간격**(**분**))**	마지막 스캔 결과를 다시 확인해야 할 때까지의 시간 간격(분)입니다. 유효 범위는 1~2880입니다.

필드 이름	설명
최신 스캔 결과 확인 설정	
Number of pending requests that can trigger checking the latest scan results(최신 스캔 결과 확인을 트리거할 수 있는 보류 중인 요청 수**)**	대기열에 있는 스캔 요청 수가 여기서 지정한 최대 수를 초과하면 Interval between checking the latest scan results in minutes(최신 스캔 결과 확인 간격(분)) 필드에서 지정한 시간 간격이 되기 전에 마지막 스캔 결과를 확인합니다. 유효 범위는 1~1000입니다.
Verify MAC address(MAC 주소 확인**)**	True 또는 False입니다. true로 설정하면 엔드포인트의 MAC 주소가 포함되어 있는 경우에만 Nexpose의 마지막 스캔 결과를 사용합니다.
Scan settings(스캔 설정**)**	
Scan trigger interval for each site in minutes(각 사이트별 스캔 트리거 간격**(**분**))**	스캔이 트리거되는 시간 간격(분)입니다. 유효 범위는 1~2880입니다.
Number of pending requests before a scan is triggered for each site(스캔이 각 사이트에 트리거되기 전에 보류 중인 요청 수**)**	대기열에 있는 스캔 요청 수가 여기서 지정한 최대 수를 초과하면 **Scan timeout in minutes(**스캔 시간 초과**(**분**))** 필드에서 지정한 시간 간격이 되기 전에 스캔이 트리거됩니다. 유효 범위는 1~1000입니다.
Scan timeout in minutes(스캔 시간 초과**(**분**))**	스캔 요청이 시간 초과될 때까지의 시간(분)입니다. 스캔 요청이 시간 초과되면 경보가 생성됩니다. 유효 범위는 20~1440입니다.
Number of sites for which scans could be triggered concurrently(동시에 스캔을 트리거할 수 있는 사이트 수**)**	스캔을 동시에 실행할 수 있는 사이트 수입니다. 유효 범위는 1~200입니다.
Timezone(표준 시간대**)**	Nexpose 서버에 구성된 표준 시간대를 기준으로 표준 시간대를 선택합니다.
Http timeout in seconds(Http 시간 초과**(**초**))**	Cisco ISE가 Nexpose의 응답을 기다리는 시간 간격(초)입니다. 유효 범위는 5~1200입니다.

필드 이름	설명
최신 스캔 결과 확인 설정	
Choose the log level for adapter log files(어댑터 로그 파일의 로그 레벨 선택**)**	어댑터의 로그 레벨을 선택합니다. 사용 가능한 옵션은 ERROR, INFO, DEBUG 및 TRACE입니다.

단계 **10** 컨피그레이션 설정을 검토하려면 **Next(**다음**)**를 클릭합니다.

단계 **11** **Finish(**종료**)**를 클릭합니다.

Tenable 어댑터 구성

Cisco ISE가 Tenable SecurityCenter(Nessus 스캐너)와 통신하고 VA 결과를 얻도록 하려면 Tenable 어댑터를 생성해야 합니다.

시작하기 전에

참고 Cisco ISE에서 Tenable 어댑터를 구성하려면 먼저 Tenable SecurityCenter에서 다음을 설정해야 합니다. Tenable SecurityCenter 설명서에서 관련 컨피그레이션을 참조하십시오.

- Tenable SecurityCenter 및 Tenable Nessus 취약점 스캐너가 설치되어 있어야 합니다. Tenable Nessus 스캐너를 등록하는 동안 **Registration(**등록**)** 필드에서 **Managed by SecurityCenter(SecurityCenter**에서 관리됨**)**를 선택했는지 확인합니다.
- Tenable SecurityCenter에서 보안 매니저 권한이 있는 사용자 계정을 생성합니다.
- 관리자 자격 증명으로 Tenable SecurityCenter에 로그인하고 **Repository(**저장소**) > Add(**추가**)**를 선택하여 SecurityCenter에서 저장소를 생성합니다.
- 저장소에서 스캔할 엔드포인트 IP 범위를 추가합니다.
- Nessus 스캐너를 추가합니다.
- 스캔 영역을 생성하고 해당 스캔 영역에 매핑된 스캔 영역 및 스캐너에 IP 주소를 할당합니다.
- ISE에 대한 스캔 정책을 생성합니다.
- 활성 스캔을 추가하고 ISE 스캔 정책과 연결합니다. 설정 및 대상(IP/DNS 이름)을 구성합니다.
- Tenable SecurityCenter에서 시스템 및 루트 인증서를 내보낸 후 Cisco ISE의 신뢰할 수 있는 인증서 저장소로 가져옵니다**(Administration(**관리**) > Certificates(**인증서**) > Certificate Management(**인증서 관리**) > Trusted Certificates(**신뢰할 수 있는 인증서**) > Import(**가져오기**)**). Cisco ISE 신뢰할 수 있는 인증서 저장소에서 적절한 루트 및 중간 인증서를 가져왔는지 또는 해당 인증서가 있는지 확인합니다.

• Cisco ISE는 HTTPS/SSL(포트 443)을 통해 Tenable SecurityCenter와 통신합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Threat Centric NAC** > **Third Party Vendors(**서드파티 벤더**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Vendor(**벤더**)** 드롭다운 목록에서 **Tenable SecurityCenter:VA**를 선택합니다.

단계 **4** 어댑터 인스턴스의 이름을 입력합니다. 예를 들어 Tenable을 입력합니다.

구성된 어댑터 인스턴스 목록과 함께 목록 창이 나타납니다.

단계 **5** Vendor Instances(벤더 인스턴스) 목록 창을 새로 고칩니다. 새로 추가된 Tenable 어댑터의 상태가 **Ready to Configure(**설정 준비**)**로 변경되어야 합니다.

단계 **6** **Ready to Configure(**구성 준비**)** 링크를 클릭합니다.

단계 **7** Tenable SecurityCenter 설정창에서 다음 값을 입력하고 **Next(**다음**)**를 클릭합니다.

필드 이름	설명
Tenable SecurityCenter Host(Tenable SecurityCenter호스트**)**	Tenable SecurityCenter의 호스트 이름입니다.
Tenable SecurityCenter Port(Tenable SecurityCenter 포트**)**	443
Username(사용자 이름**)**	Tenable SecurityCenter에서 보안 매니저 권한이 있는 사용자 계정의 사용자 이름입니다.
Password(비밀번호**)**	Tenable SecurityCenter에서 보안 매니저 권한이 있는 사용자 계정의 비밀번호입니다.
HTTP Proxy Host(HTTP 프록시 호스트**)**	모든 인터넷 트래픽을 라우팅하도록 프록시 서버를 구성한 경우 프록시 서버의 호스트 이름을 입력합니다.
HTTP Proxy Port(HTTP 프록시 포트**)**	프록시 서버에서 사용하는 포트 번호를 입력합니다.

단계 **8** **Next(**다음**)**를 클릭합니다.

단계 **9** **Advanced Setting(**고급 설정**)** 창에서 다음 값을 입력합니다. 이 창의 설정에 따라 VA에 대해 마지막 스캔 결과가 사용되는지 아니면 온디맨드 스캔이 트리거되는지가 결정됩니다.

필드 이름	설명
Repository(저장소**)**	Tenable SecurityCenter에서 생성한 저장소를 선택합니다.
Scan Policy(스캔 정책**)**	Tenable SecurityCenter에서 ISE에 대해 생성한 스캔 정책을 선택합니다.
최신 스캔 결과 확인 설정	
Interval between checking the latest scan results in minutes(최신 스캔 결과 확인 간격**(**분**))**	마지막 스캔 결과를 다시 확인해야 할 때까지의 시간 간격(분)입니다. 유효 범위는 1~2880입니다.
Number of pending requests that can trigger checking the latest scan results(최신 스캔 결과 확인을 트리거할 수 있는 보류 중인 요청 수**)**	대기열에 있는 스캔 요청 수가 여기서 지정한 최대 수를 초과하면 **Interval between checking the latest scan results in minutes(**최신 스캔 결과 확인 간격**(**분**))** 필드에서 지정한 시간 간격이 되기 전에 마지막 스캔 결과를 확인합니다. 유효 범위는 1~1000입니다. 기본값은 10입니다.
Verify MAC address(MAC 주소 확인**)**	True 또는 False입니다. true로 설정하면 엔드포인트의 MAC 주소가 포함되어 있는 경우에만 Tenable SecurityCenter의 마지막 스캔 결과를 사용합니다.
Scan Settings(스캔 설정**)**	
Scan trigger interval for each site in minutes(각 사이트별 스캔 트리거 간격**(**분**))**	온디맨드 스캔이 트리거될 때까지의 시간 간격(분)입니다. 유효 범위는 1~2880입니다.
Number of pending requests before a scan is triggered(스캔이 트리거되기 전에 보류 중인 요청 수**)**	대기열에 있는 스캔 요청 수가 여기서 지정한 최대 수를 초과하면 **Scan trigger interval for each site in minutes(**각 사이트별 스캔 트리거 간격**(**분**))** 필드에서 지정한 시간 간격이 되기 전에 온디맨드 스캔이 트리거됩니다. 유효 범위는 1~1000입니다.
Scan timeout in minutes(스캔 시간 초과**(**분**))**	스캔 요청이 시간 초과할 때까지의 시간(분)입니다. 스캔 요청이 시간 초과되면 경보가 생성됩니다. 유효 범위는 20~1440입니다.

필드 이름	설명
Number of scans that could run in parallel(동시에 실행할 수 있는 스캔 수**)**	동시에 실행할 수 있는 스캔 수입니다. 유효 범위는 1~200입니다.
Http timeout in seconds(Http 시간 초과**(**초**))**	Cisco ISE가 Tenable SecurityCenter의 응답을 기다리는 시간 간격(초)입니다. 유효 범위는 5~1200입니다.
Choose the log level for adapter log files(어댑터 로그 파일의 로그 레벨 선택**)**	어댑터의 로그 레벨을 선택합니다. 사용 가능한 옵션은 ERROR, INFO, DEBUG 및 TRACE입니다.

단계 **10** 컨피그레이션 설정을 검토하려면 **Next(**다음**)**를 클릭합니다.

단계 **11** **Finish(**종료**)**를 클릭합니다.

권한 부여 프로파일 구성

이제 Cisco ISE의 권한 부여 프로파일에는 엔트포인트의 취약점을 스캔하는 옵션이 포함되어 있습니다. 정기적으로 스캔을 실행하도록 선택할 수 있으며 이러한 스캔의 시간 간격도 지정할 수 있습니다. 권한 부여 프로파일을 정의한 후 기존 권한 부여 정책 규칙에 적용하거나 새 권한 부여 정책 규칙을 생성할 수 있습니다.

시작하기 전에

Threat Centric NAC 서비스를 활성화하고 벤더 어댑터를 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다.

단계 **2** 새 권한 부여 프로파일을 생성하거나 기존 프로파일을 편집합니다.

단계 **3** **Common Tasks(**일반 작업**)** 영역에서 **Assess Vulnerabilities(**취약점 평가**)** 확인란을 선택합니다.

단계 **4** **Adapter Instance(**어댑터 인스턴스**)** 드롭다운 목록에서, 구성한 벤더 어댑터를 선택합니다. Qualys_Instance를 예로 들 수 있습니다.

단계 **5** 마지막 스캔 이후 경과된 시간이 텍스트 상자의 값보다 크면 Trigger scan(스캔 트리거)에 스캔 간격을 시간 단위로 입력합니다. 유효 범위는 1~9999입니다.

단계 **6** **Assess periodically using above interval(**위의 간격을 사용하여 정기적으로 평가**)** 확인란을 선택합니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

취약한 엔드포인트 격리를 위한 예외 규칙 구성

다음 취약점 평가 속성을 사용하여 예외 규칙을 구성하고 취약한 엔드포인트에 대한 제한된 액세스를 제공할 수 있습니다.

- Threat:Qualys-CVSS_Base_Score
- Threat:Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

이러한 속성은 Threat 디렉토리에서 사용할 수 있습니다. 유효한 값의 범위는 0~10입니다.

엔드포인트를 격리하거나, 제한된 액세스를 제공하거나(다른 포털로 리디렉션) 요청을 거부하도록 선택할 수 있습니다.

단계 **1** **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택합니다.
VA 속성 확인을 위해 기존 정책 규칙을 수정하거나 새 예외 규칙을 생성할 수 있습니다.

단계 **2** Qualys 점수를 확인하고 적절한 권한 부여 프로파일을 할당하는 조건을 생성합니다. 예를 들면 다음과 같습니다.

Any Identity Group & Threat:Qualys-CVSS_Base_Score > 5 -> Quarantine (authorization profile)

단계 **3** **Save(**저장**)**를 클릭합니다.

취약점 평가 로그

Cisco ISE는 VA 서비스 문제 해결을 위해 다음 로그를 제공합니다.

- vaservice.log - VA 코어 정보를 포함하며, TC-NAC 서비스를 실행하는 노드에서 사용할 수 있습니다.
- varuntime.log - 엔드포인트 및 VA 플로우에 대한 정보를 포함하며, 모니터링 노드 및 TC-NAC 서비스를 실행하는 노드에서 사용할 수 있습니다.
- vaaggregation.log - 엔드포인트 취약점에 대한 시간별 집계 세부정보를 포함하며, 기본 관리 노드에서 사용할 수 있습니다.

네트워크 리소스

SAnet(Session Aware Networking) 지원

Cisco ISE는 SAnet(Session Aware Networking)을 제한적으로 지원합니다. SAnet은 여러 Cisco 스위치에서 실행되는 세션 관리 프레임워크입니다. SAnet은 가시성, 인증 및 권한 부여를 포함한 액세스 세션을 관리합니다. SAnet은 RADIUS 권한 부여 속성이 포함된 서비스 템플릿을 사용합니다. Cisco ISE는 권한 부여 프로파일 내에 서비스 템플릿을 포함합니다. Cisco ISE는 프로파일을 "서비스 템플릿"과 호환되는 것으로 식별하는 플래그를 사용하여 권한 부여 프로파일에서 서비스 템플릿을 식별합니다.

Cisco ISE 권한 부여 프로파일에는 속성 목록으로 변환되는 RADIUS 권한 부여 속성이 포함되어 있습니다. SAnet 서비스 템플릿에는 RADIUS 권한 부여 속성도 포함되지만, 이러한 속성은 목록으로 변환되지 않습니다.

SAnet 디바이스의 경우 Cisco ISE는 서비스 템플릿의 이름을 전송합니다. 캐시 또는 정적으로 정의된 컨피그레이션에 해당 콘텐츠가 없는 경우 디바이스는 서비스 템플릿의 콘텐츠를 다운로드합니다. 서비스 템플릿이 RADIUS 속성을 변경하면 Cisco ISE가 디바이스에 CoA 알림을 보냅니다.

네트워크 디바이스

이들 창에서 Cisco ISE에 네트워크 디바이스를 추가하고 관리할 수 있습니다.

네트워크 디바이스 정의 설정

다음 표에서는 Cisco ISE에서 네트워크 액세스 디바이스를 구성하는 데 사용할 수 있는 **Network Devices(**네트워크 디바이스**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**입니다. 그런 다음 **Add(**추가**)**를 클릭합니다.

네트워크 디바이스 설정

다음 표에서는 **New Network Devices(**새 네트워크 디바이스**)** 창의 필드에 대해 설명합니다.

표 ***1:*** 네트워크 디바이스 설정

필드 이름	설명
Name(이름**)**	네트워크 디바이스의 이름을 입력합니다. 디바이스의 호스트 이름과 다른, 네트워크 디바이스를 설명하는 이름을 입력할 수 있습니다. 디바이스 이름은 논리적 식별자입니다. 참고 디바이스를 구성한 후에는 그 이름을 편집할 수 없습니다.

필드 이름	설명
Description(설명**)**	디바이스에 대한 설명을 입력합니다.
IP 주소 또는 **IP** 범위	드롭다운 목록에서 다음 중 하나를 선택하고 표시되는 필드에 필요한 값을 입력합니다. • **IP Address(IP** 주소**)**: 단일 IP 주소(IPv4 또는 IPv6 주소)와 서브넷 마스크를 입력합니다. • **IP Range(IP** 범위**)**: 필요한 IPv4 주소 범위를 입력합니다. 인증 중에 IP 주소를 제외하려면 **Exclude(**제외**)** 필드에 IP 주소 또는 IP 주소 범위를 입력합니다. IP 주소 및 서브넷 마스크 또는 IP 주소 범위를 정의할 때의 지침은 다음과 같습니다. • 특정 IP 주소를 정의하거나 서브넷 마스크가 포함된 IP 범위를 정의할 수 있습니다. 디바이스 A에 IP 주소 범위가 정의되어 있으면 디바이스 A에 정의된 범위의 개별 주소를 사용하여 다른 디바이스 B를 구성할 수 있습니다. • 모든 옥텟에서 IP 주소 범위를 정의할 수 있습니다. IP 주소 범위를 지정하는 경우 하이픈(-)을 사용하거나 별표(*)를 와일드카드로 사용할 수 있습니다. 예를 들어 *.*.*.*, 1-10.1-10.1-10.1-10 또는 10-11.*.5.10-15와 같이 지정할 수 있습니다. • IP 주소 범위의 일부가 이미 추가된 경우에는 구성된 범위에서 이를 제외할 수 있습니다. 예를 들어 10.197.65.*/10.197.65.1과 같이 지정하여 10.197.65.*에서 10.197.65.1를 제외할 수 있습니다. • 동일한 특정 IP 주소를 사용하여 두 개의 디바이스를 정의할 수는 없습니다. • 동일한 IP 범위를 사용하여 두 개의 디바이스를 정의할 수는 없습니다. IP 범위가 일부분 또는 완전히 겹쳐서는 안 됩니다.

필드 이름	설명
Device Profile(디바이스 프로파일**)**	드롭다운 목록에서 네트워크 디바이스의 벤더를 선택합니다. 드롭다운 목록 옆의 툴팁을 사용하여 선택한 벤더의 네트워크 디바이스가 지원하는 플로우 및 서비스를 확인할 수 있습니다. 툴팁에는 디바이스에서 사용되는 URL 리디렉션의 유형 및 RADIUS CoA 포트도 표시됩니다. 이러한 속성은 디바이스 유형의 네트워크 디바이스 프로파일에 정의되어 있습니다.
Model Name(모델 이름**)**	드롭다운 목록에서 디바이스 모델을 선택합니다. 규칙 기반 정책에서 조건을 확인하는 동안 모델 이름을 매개변수 중 하나로 사용합니다. 이 속성은 디바이스 사전에 있습니다.
Software Version(소프트웨어 버전**)**	드롭다운 목록에서 네트워크 디바이스에서 실행되는 소프트웨어의 버전을 선택합니다. 규칙 기반 정책에서 조건을 확인하는 동안 소프트웨어 버전을 매개변수 중 하나로 사용할 수 있습니다. 이 속성은 디바이스 사전에 있습니다.
Network Device Group(네트워크 디바이스 그룹**)**	**Network Device Group(**네트워크 디바이스 그룹**)** 영역의 **Location(**위치**)**, **IPSEC** 및 **Device Type(**디바이스 유형**)** 드롭다운 목록에서 필요한 값을 선택합니다. 그룹에 구체적으로 할당하지 않는 디바이스는 기본 디바이스 그룹(루트 네트워크 디바이스 그룹)에 포함됩니다. 기본 디바이스 그룹은 위치 기준 **All Locations(**모든 위치**)** 및 디바이스 유형 기준 **All Device Types(**모든 디바이스 유형**)**입니다.

RADIUS 인증 설정

다음 표에서는 **RADIUS** 인증 설정 영역의 필드에 대해 설명합니다.

표 ***2: RADIUS*** 인증 설정 영역의 필드

필드 이름	사용 지침
RADIUS UDP Settings(RADIUS UDP 설정**)**	
Protocol(프로토콜**)**	**RADIUS**를 선택한 프로토콜로 표시합니다.

필드 이름	사용 지침
Shared Secret(공유 암호**)**	네트워크 디바이스의 공유 암호를 입력합니다. 공유 암호는 **radius-host** 명령(**pac** 옵션 포함)을 사용하여 네트워크 디바이스에 구성된 키입니다. 참고 공유 암호 길이는 **Device Security Settings(**디바이스 보안 설정**)** 창(**Administration(**관리**) > Network Resources(**네트워크 리소스**) > Network Devices(**네트워크 디바이스**) > Device Security Settings(**네트워크 보안 설정**))** 창의 **Minimum RADIUS Shared Secret Length(**최소 **RADIUS** 공유 암호 길이**)** 필드에 구성된 값보다 크거나 같아야 합니다. RADIUS 서버의 경우 모범 사례는 22자입니다. 신규 설치 및 업그레이드된 구축의 경우 공유 암호 길이는 기본적으로 4자입니다. **Device Security Settings(**디바이스 보안 설정**)** 창에서 이 값을 변경할 수 있습니다.

필드 이름	사용 지침
Use Second Shared Secret(두 번째 공유 암호 사용**)**	네트워크 디바이스 및 Cisco ISE에서 사용할 두 번째 공유 암호를 지정합니다. 참고 Cisco TrustSec 디바이스는 이중 공유 암호(키)를 활용할 수 있지만 Cisco ISE에서 전송되는 Cisco TrustSec CoA 패킷은 항상 첫 번째 공유 암호(키)를 사용합니다. 두 번째 공유 암호를 활성화하려면 Cisco TrustSec CoA 패킷을 Cisco TrustSec 디바이스로 전송할 Cisco ISE 노드를 선택합니다. **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Add(**추가**)** > **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)** 창에 있는 **Send From(**전송 위치**)** 드롭다운 목록에서 이 작업에 사용할 Cisco ISE 노드를 구성합니다. PAN(Primary Administration Node) 또는 PSN(Policy Service Node)을 선택할 수 있습니다. 선택한 PSN 노드가 작동 중지된 경우 PAN은 Cisco TrustSec CoA 패킷을 Cisco TrustSec 디바이스로 전송합니다. 참고 RADIUS 액세스 요청에 대한 두 번째 공유 암호 기능은 **Message-Authenticator** 필드를 포함하는 패킷에 대해서만 작동합니다.

필드 이름	사용 지침
CoA Port(CoA 포트**)**	RADIUS CoA에 사용할 포트를 지정합니다. 디바이스의 기본 CoA 포트는 네트워크 디바이스에 대해 구성된 네트워크 디바이스 프로파일(**Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일)에 정의됩니다. 기본 CoA 포트를사용하려면 **Set To Default(**기본값으로 설정**)** 버튼을 클릭합니다. 참고 **Network Devices(**네트워크 디바이스**)** 창(**Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**))**의 **RADIUS Authentication Settings(RADIUS** 인증 설정**)**에 지정된 CoA 포트를 수정하는 경우 **Network Device Profile(**네트워크 디바이스 프로파일**)** 창(**Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**))**의 해당 프로파일에도 동일한 CoA 포트를 지정하십시오.
RADIUS DTLS Settings(RADIUS DTLS 설정**)**	
DTLS Required(DTLS 필수**)**	**DTLS Required(DLTS** 필수**)** 확인란을 선택하면 Cisco ISE에서 이 디바이스의 DTLS 요청만 처리합니다. 이 옵션을 비활성화하면 Cisco ISE에서 이 디바이스의 UDP 요청과 DTLS 요청을 모두 처리합니다. RADIUS DTLS는 SSL(Secure Sockets Layer) 터널 설정 및 RADIUS 통신을 위한 향상된 보안을 제공합니다.
Shared Secret(공유 암호**)**	RADIUS DTLS에 사용되는 공유 암호를 표시합니다. 이 값은 고정되어 있으며 MD5(Message Digest 5) 무결성 확인을 처리하는 데 사용됩니다.
CoA Port(CoA 포트**)**	RADIUS DTLS CoA에 사용할 포트를 지정합니다.
Issuer CA of ISE Certificates for CoA(CoA의 **ISE** 인증서에 대한 발급자 **CA)**	드롭다운 목록에서 RADIUS DTLS CoA에 사용할 CA(Certificate Authority)를 선택합니다.

필드 이름	사용 지침
DNS Name(DNS 이름**)**	네트워크 디바이스의 DNS 이름을 입력합니다. **RADIUS Settings(RADIUS** 설정**)** 창 (**Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **RADIUS**) 에서 **Enable RADIUS/DTLS Client Identity Verification(RADIUS/DTLS** 클라이언트 **ID** 확인 활성화**)** 옵션이 활성화된 경우 Cisco ISE는 이 DNS 이름을 클라이언트 인증서에 지정된 DNS 이름과 비교하여 네트워크 디바이스의 ID를 확인합니다.
General Settings(일반 설정**)**	
Enable KeyWrap(KeyWrap 활성화**)**	네트워크 디바이스에서 KeyWrap 알고리즘이 지원되는 경우에만 **Enable KeyWrap(KeyWrap** 활성화**)** 확인란을 선택합니다. 이 옵션은 AES KeyWrap 알고리즘을 통해 RADIUS 보안을 강화하는 데 사용됩니다. 참고 FIPS 모드에서 Cisco ISE를 실행할 때는 네트워크 디바이스에서 KeyWrap을 활성화해야 합니다.
Key Encryption Key(키 암호화 키**)**	세션 암호화(비밀 유지)에 사용되는 암호화 키를 입력합니다.
Message Authenticator Code Key(메시지 인증자 코드 키**)**	RADIUS 메시지에 대한 키 HMAC(Hashed Message Authentication Code) 계산에 사용되는 키를 입력합니다.

필드 이름	사용 지침
Key Input Format(키 입력 형식**)**	다음 형식 중 하나에 해당하는 라디오 버튼을 클릭합니다. • **ASCII**: **Key Encryption Key(**키 암호화 키**)** 필드에 입력하는 값의 길이는 16자(바이트)여야 하며 **Message Authenticator Code Key(**메시지 인증자 코드 키**)** 필드에 입력하는 값의 길이는 20자(바이트)여야 합니다. • **Hexadecimal**: **Key Encryption Key(**키 암호화 키**)** 필드에 입력하는 값의 길이는 32자(바이트)여야 하며 **Message Authenticator Code Key(**메시지 인증자 코드 키**)** 필드에 입력하는 값의 길이는 40자(바이트)여야 합니다. Cisco ISE FIPS 암호화 키를 입력하는 데 사용할 키 입력 형식을 무선 LAN 컨트롤러에서 사용 가능한 구성과 일치하도록 지정할 수 있습니다. 이 값은 키의 정확한(전체) 길이로 지정해야 하며 더 짧은 값은 지정할 수 없습니다.

TACACS 인증 설정

표 ***3: TACACS*** 인증 설정 영역의 필드

필드 이름	사용 지침
Shared Secret(공유 암호**)**	TACACS+ 프로토콜을 활성화할 때 네트워크 디바이스에 할당된 텍스트 문자열입니다. 네트워크 디바이스가 사용자 이름과 비밀번호를 인증하기 전에 사용자가 텍스트를 입력해야 합니다. 사용자가 공유 암호를 제공할 때까지는 연결이 거부됩니다.
Retired Shared Secret is Active(사용 중단된 공유 암호가 활성 상태임**)**	사용 중단 기간이 활성인 경우 표시됩니다.
Retire(사용 중단**)**	기존 공유 암호를 종료하는 대신 사용 중단합니다. **Retire(**사용 중단**)**를 클릭하면 메시지 상자가 표시됩니다. **Yes(**예**)** 또는 **No(**아니요**)**를 클릭할 수 있습니다.

필드 이름	사용 지침
Remaining Retired Period(남은 사용 중단 기간**)**	(**Retire(**사용 중단**)** 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Settings(**설정**)** > **Connection Settings(**연결 설정**)** > **Default Shared Secret Retirement Period(**기본 공유 암호 사용 중단 기간**)** 탐색 경로에 지정되어 있는 기본값이 표시됩니다. 기본값은 변경할 수 있습니다. 그러면 새 공유 암호를 입력할 수 있습니다. 이전 공유 암호는 지정된 기간(일) 동안 활성 상태로 유지됩니다.
End(종료**)**	(**Retire(**사용 중단**)** 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) 사용 중단 기간을 종료하고 이전 공유 암호 사용을 중단합니다.
Enable Single Connect Mode(단일 연결 모드 활성화**)**	네트워크 디바이스와의 모든 TACACS+ 통신에 단일 TCP 연결을 사용하려면 **Enable Single Connect Mode(**단일 연결 모드 활성화**)** 확인란을 선택합니다. 다음 중 하나의 옵션에 해당하는 라디오 버튼을 클릭합니다. • **Legacy Cisco Devices(**레거시 **Cisco** 디바이스**)** • **TACACS Draft Compliance Single Connect Support(TACACS+** 초안 규정 준수 단일 연결 지원**)** **Single Connect Mode(**단일 연결 모드**)**를 비활성화하면 Cisco ISE는 모든 TACACS 요청에 대해 새 TCP 연결을 사용합니다.

SNMP 설정

다음 표에서는 **SNMP Settings(SNMP** 설정**)** 섹션의 필드에 대해 설명합니다.

표 ***4: SNMP*** 설정 영역의 필드

필드 이름	사용 지침
SNMP Version(SNMP 버전**)**	**SNMP Version(SNMP** 버전**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • **1**: SNMPv1에서는 알림이 지원되지 않습니다. • **2c** • **3**: SNMPv3은 이후 단계에서 **Priv(**개인**)** 보안 레벨 선택 시 패킷 암호화를 허용하므로 가장 안전한 모델입니다. 참고 SNMPv3 매개변수를 사용하여 네트워크 디바이스를 구성한 경우에는 모니터링 서비스(**Operations(**운영**)** > **Reports(**보고서**)** > **Diagnostics(**진단**)** > **Network Device Session Status(**네트워크 디바이스 세션 상태**))**에서 제공되는 **Network Device Session Status(**네트워크 디바이스 세션 상태**)** 요약 보고서를 생성할 수 없습니다. 네트워크 디바이스가 SNMPv1 또는 SNMPv2c 매개변수로 구성된 경우 이 보고서를 정상적으로 생성할 수 있습니다.
SNMP RO Community(SNMP RO 커뮤니티**)**	(SNMP 버전 1 및 2c에 대해서만 적용됨) 디바이스에 대한 특정 액세스 유형을 Cisco ISE에 제공하는 읽기 전용 커뮤니티 문자열을 입력합니다. 참고 캐럿(circumflex ^) 기호는 허용되지 않습니다.
SNMP Username(SNMP 사용자 이름**)**	(SNMP 버전 3에만 적용됨) SNMP 사용자 이름을 입력합니다.

필드 이름	사용 지침
Security Level(보안 레벨**)**	(SNMP 버전 3에만 적용됨) **Security Level(**보안 레벨**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • **Auth(**인증**)**: MD5 또는 SHA(Secure Hash Algorithm) 패킷 인증을 활성화합니다. • **No Auth(**인증 안 함**)**: 인증 및 개인 보안 레벨을 사용하지 않습니다. • **Priv(**개인**)**: DES(Date Encryption Standard, 데이터 암호화 표준) 패킷 암호화를 활성화합니다.
Auth Protocol(인증 프로토콜**)**	(보안 레벨로 **Auth(**인증**)** 또는 **Priv(**개인**)**를 선택하는 경우 SNMP 버전 3에만 적용됨) 네트워크 디바이스가 사용하도록 할 인증 프로토콜을 **Auth Protocol(**인증 프로토콜**)** 드롭다운 목록에서 선택합니다. • **MD5** • **SHA**
Auth Password(인증 비밀번호**)**	(보안 레벨로 **Auth(**인증**)** 및 **Priv(**개인**)**를 선택하는 경우 SNMP 버전 3에만 적용됨) 인증 키를 입력합니다. 8자 이상이어야 합니다. **Show(**표시**)**를 클릭하면 디바이스에 대해 이미 구성된 인증 비밀번호가 표시됩니다. 참고 캐럿(circumflex ^) 기호는 사용할 수 없습니다.
Privacy Protocol(프라이버시 프로토콜**)**	(**Priv(**개인**)** 보안 레벨이 선택된 경우 SNMP 버전 3에만 적용됨) **Privacy Protocol(**프라이버시 프로토콜**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • **DES** • **AES128** • **AES192** • **AES256** • **3DES**

필드 이름	사용 지침
Privacy Password(프라이버시 비밀번호**)**	(보안 레벨로 **Priv(**개인**)**를 선택하는 경우 SNMP 버전 3에만 적용됨) 프라이버시 키를 입력합니다. **Show(**표시**)**를 클릭하면 디바이스에 대해 이미 구성된 프라이버시 비밀번호가 표시됩니다. 참고 캐럿(circumflex ^) 기호는 사용할 수 없습니다.
Polling Interval(폴링 간격**)**	폴링 간격을 초 단위로 입력합니다. 기본값은 3600초입니다.
Link Trap Query(링크 트랩 쿼리**)**	SNMP 트랩을 통해 수신되는 linkup 및 linkdown 알림을 수신하고 해석하려면 **Link Trap Query(**링크 트랩 쿼리**)** 확인란을 선택합니다.
Mac Trap Query(Mac 트랩 쿼리**)**	SNMP 트랩을 통해 수신되는 MAC 알림을 수신하고 해석하려면 **Link Trap Query(**링크 트랩 쿼리**)** 확인란을 선택합니다.
Originating Policy Service Node(원래 정책 서비스 노드**)**	**Originating Policy Services Node(**원래 정책 서비스 노드**)** 드롭다운 목록에서 SNMP 데이터 폴링에 사용할 Cisco ISE 서버를 선택합니다. 이 필드의 기본값은 **Auto(**자동**)**입니다. 드롭다운 목록에서 특정 값을 선택하여 설정을 덮어 씁니다.

Advanced TrustSec Settings(Advanced TrustSec 설정)

다음 표에서는 **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)** 섹션의 필드에 대해 설명합니다.

표 *5:* 고급 *TrustSec* 설정 영역의 필드

필드 이름	사용 지침
Device Authentication Settings(디바이스 인증 설정**)**	
Use Device ID for TrustSec Identification(TrustSec 식별에 디바이스 **ID** 사용**)**	디바이스 이름이 **Device ID(**디바이스 **ID)** 필드에 디바이스 식별자로 나열되도록 하려면 **Use Device ID for TrustSec Identification(TrustSec** 식별에 디바이스 **ID** 사용**)** 확인란을 선택합니다.
Device ID(디바이스 **ID)**	**Use Device ID for TrustSec Identification(TrustSec** 식별에 디바이스 **ID** 사용**)** 확인란을 선택하지 않은 경우에만 이 필드에 디바이스 ID를 입력할 수 있습니다.

필드 이름	사용 지침
Password(비밀번호**)**	Cisco TrustSec 디바이스를 인증하기 위해 Cisco TrustSec 디바이스 CLI에서 구성한 비밀번호를 입력합니다. 비밀번호를 표시하려면 **Show(**표시**)**를 클릭합니다.
HTTP REST API Settings(HTTP REST API 설정**)**	
Enable HTTP REST API(HTTP REST API 활성화**)**	HTTP REST API를 사용하여 필요한 Cisco TrustSec 정보를 네트워크 디바이스에 제공하려면 **Enable HTTP REST API(HTTP REST API** 활성화**)** 확인란을 선택합니다. 이렇게 하면 RADIUS 프로토콜에 비해 짧은 시간에 대규모 구성을 다운로드할 수 있고 효율성이 향상됩니다. 또한 TCP over UDP를 사용하여 안정성이 향상됩니다.
Username(사용자 이름**)**	Cisco TrustSec 디바이스를 인증하기 위해 Cisco TrustSec 디바이스 CLI에서 구성한 사용자 이름을 입력합니다. 사용자 이름에는 특수 문자를 포함할 수 없습니다. 예: 공백 ! % ^ : ; , [{ | }] ` " = < > ?
Password(비밀번호**)**	Cisco TrustSec 디바이스를 인증하기 위해 Cisco TrustSec 디바이스 CLI에서 구성한 비밀번호를 입력합니다.
TrustSec 디바이스 알림 및 업데이트	
Device ID(디바이스 **ID)**	**Use Device ID for TrustSec Identification(TrustSec** 식별에 디바이스 **ID** 사용**)** 확인란을 선택하지 않은 경우에만 이 필드에 디바이스 ID를 입력할 수 있습니다.
Password(비밀번호**)**	Cisco TrustSec 디바이스를 인증하기 위해 Cisco TrustSec 디바이스 CLI에서 구성한 비밀번호를 입력합니다. 비밀번호를 표시하려면 **Show(**표시**)**를 클릭합니다.
Download Environment Data Every <...>(환경 데이터 다운로드 간격**)**	이 영역의 드롭다운 목록에서 필요한 값을 선택하여 디바이스가 Cisco ISE에서 환경 데이터를 다운로드하는 시간 간격을 지정합니다. 초, 분, 시간, 일 또는 주 단위로 시간 간격을 선택할 수 있습니다. 기본값은 1일입니다.

필드 이름	사용 지침
Download Peer Authorization Policy Every <...>(피어 권한 부여 정책 다운로드 간격**)**	이 영역의 드롭다운 목록에서 필요한 값을 선택하여 디바이스가 Cisco ISE에서 피어 권한 부여 정책을 다운로드하는 시간 간격을 지정합니다. 초, 분, 시간, 일 또는 주 단위로 시간 간격을 지정할 수 있습니다. 기본값은 1일입니다.
Reauthentication Every <...>(재인증 간격**)**	이 영역의 드롭다운 목록에서 필요한 값을 선택하여 디바이스가 초기 인증 후 Cisco ISE에 대해 재인증되는 시간 간격을 지정합니다. 초, 분, 시간, 일 또는 주 단위로 시간 간격을 구성할 수 있습니다. 예를 들어 1,000초를 입력하면 디바이스가 Cisco ISE에 대해 1,000초마다 자체적으로 재인증됩니다. 기본값은 1일입니다.
Download SGACL Lists Every <...>(SGACL 목록 다운로드 간격**)**	이 영역의 드롭다운 목록에서 필요한 값을 선택하여 디바이스가 Cisco ISE에서 SGACL 목록을 다운로드하는 시간 간격을 지정합니다. 초, 분, 시간, 일 또는 주 단위로 시간 간격을 구성할 수 있습니다. 기본값은 1일입니다.
Other TrustSec Devices to Trust This Device (TrustSec Trusted)(다른 **TrustSec** 디바이스가 이 디바이스를 신뢰함**(TrustSec** 신뢰**))**	모든 피어 디바이스가 이 Cisco TrustSec 디바이스를 신뢰하도록 허용하려면 **Other TrustSec Devices to Trust This Device(**다른 **TrustSec** 디바이스가 이 디바이스를 신뢰함**)** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 피어 디바이스가 이 디바이스를 신뢰하지 않으며 이 디바이스에서 도착하는 모든 패킷에 그에 따른 색상 또는 태그가 지정됩니다.

필드 이름	사용 지침
구성 변경 사항을 디바이스에 전송	Cisco ISE가 CoA 또는 CLI(SSH)를 사용하여 Cisco TrustSec 디바이스에 Cisco TrustSec 구성 변경 사항을 보내도록 하려면 **Send Configuration Changes to Device(**구성 변경 사항을 디바이스에 전송**)** 확인란을 선택합니다. 필요에 따라 **CoA** 또는 **CLI(SSH)** 라디오 버튼을 클릭합니다. Cisco ISE가 CoA를 사용하여 Cisco TrustSec 디바이스에 구성 변경 사항을 전송하도록 하려면 **CoA** 옵션을 선택합니다. Cisco ISE가 CLI(SSH 연결)를 사용하여 Cisco TrustSec 디바이스에 구성 변경 사항을 전송하도록 하려면 **CLI (SSH)** 옵션을 선택합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 세그멘테이션의 "CoA 미지원 디바이스에 구성 변경 푸시"섹션을 참고하십시오 참고.
Send From(전송 위치**)**	이 드롭다운 목록에서 구성 변경 사항을 Cisco TrustSec 디바이스로 전송할 Cisco ISE 노드를 선택합니다. PAN 또는 PSN 노드를 선택할 수 있습니다. 선택한 PSN 노드가 작동 중지된 경우 PAN을 사용하여 구성 변경 사항이 Cisco TrustSec 디바이스로 전송됩니다.
연결 테스트	이 옵션을 사용하여 Cisco TrustSec 디바이스와 선택한 Cisco ISE 노드(PAN 또는 PSN) 간의 연결을 테스트할 수 있습니다.
SSH Key(SSH 키**)**	이 기능을 사용하려면 Cisco ISE에서 네트워크 디바이스로의 SSHv2 터널을 연 다음 디바이스의 CLI를 사용해 SSH 키를 검색합니다. 검증을 위해 이 키를 복사하여 **SSH Key(SSH** 키**)** 필드에 붙여넣어야 합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 세그멘테이션의 "SSH 키 확인" 섹션을 참고하십시오.
디바이스 구성 구축	
Include this device when deploying Security Group Tag Mapping Updates(보안 그룹 태그 매핑 업데이트 구축 시 이 디바이스 포함**)**	Cisco TrustSec 디바이스가 디바이스 인터페이스 자격 증명을 사용하여 IP-SGT 매핑을 가져오도록 하려면 **Include this device when deploying Security Group Tag Mapping Updates(**보안 그룹 태그 매핑 업데이트 구축 시 이 디바이스 포함**)** 확인란을 선택합니다.

필드 이름	사용 지침
Exec Mode Username(실행 모드 사용자 이름**)**	Cisco TrustSec 디바이스에 로그인하는 데 사용하는 사용자 이름을 입력합니다.
Exec Mode Password(실행 모드 비밀번호**)**	디바이스 비밀번호를 입력합니다. 비밀번호를 보려면 **Show(**표시**)**를 클릭합니다. 참고 보안 취약점을 방지하려면 EXEC 모드 및 활성화 모드 비밀번호를 포함하여 비밀번호에 % 문자를 사용하지 않는 것이 좋습니다.
Enable Mode Password(활성화 모드 비밀번호**)**	(선택 사항) 특별 권한 모드에서 Cisco TrustSec 디바이스의 구성을 편집하는 데 사용되는 활성화 비밀번호를 입력합니다. 비밀번호를 보려면 **Show(**표시**)**를 클릭합니다.
OOB TrustSec PAC	
Issue Date(발급 날짜**)**	Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성된 Cisco TrustSec PAC의 발급 날짜를 표시합니다.
만료일	Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성된 Cisco TrustSec PAC의 만료일을 표시합니다.
Issued By(발급자**)**	Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성된 Cisco TrustSec PAC의 발급자 이름(Cisco TrustSec 관리자)을 표시합니다.
Generate PAC(PAC 생성**)**	**Generate PAC(PAC** 생성**)** 버튼을 클릭하여 Cisco TrustSec 디바이스에 대한 OOB(Out of Band) Cisco TrustSec PAC를 생성합니다.

기본 네트워크 디바이스 정의 설정

다음 표에서는 **Default Network device(**기본 네트워크 디바이스**)** 창의 필드에 대해 설명합니다. 이 창에서는 Cisco ISE가 RADIUS 또는 TACACS+ 인증에 사용할 수 있는 기본 네트워크 디바이스를 구성할 수 있습니다. 다음 탐색 경로 중 하나를 선택합니다.

- **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Default Device(**기본 디바이스**)**
- **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Default Devices(**기본 디바이스**)**

표 ***6: Default Network Device(***기본 네트워크 디바이스***)*** 창의 필드

필드 이름	사용 지침
Default Network Device Status(기본 네트워크 디바이스 상태**)**	**Default Network Device Status(**기본 네트워크 디바이스 상태**)** 드롭다운 목록에서 **Enable(**활성화**)**를 선택하여 기본 네트워크 디바이스 정의를 활성화합니다. 참고 기본 디바이스를 활성화하는 경우 이 창에서 RADIUS 또는 TACACS+ 인증 설정의 해당 확인란을 선택하여 활성화해야 합니다.
디바이스 프로파일**(Device Profile)**	**Cisco**를 기본 디바이스 벤더로 표시합니다.
RADIUS 인증 설정**(RADIUS Authentication Settings)**	
Enable RADIUS(RADIUS 활성화**)**	디바이스에 대한 RADIUS 인증을 활성화하려면 **Enable RADIUS(RADIUS** 활성화**)** 확인란을 선택합니다.
RADIUS UDP 설정**(RADIUS UDP Settings)**	
Shared Secret(공유 암호**)**	공유 암호를 입력합니다. 공유 암호의 최대 길이는 127자입니다. 공유 암호는 **radius-host** 명령(**pac** 옵션 포함)을 사용하여 네트워크 디바이스에서 구성한 키입니다. 참고 공유 암호 길이는 **Device Security Settings(**디바이스 보안 설정**)** 창(**Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Device Security Settings(**네트워크 보안 설정**))** 창의 **Minimum RADIUS Shared Secret Length(**최소 **RADIUS** 공유 암호 길이**)** 필드에 구성된 값보다 크거나 같아야 합니다. 기본적으로 이 값은 신규 설치 및 업그레이드된 구축의 경우 4자입니다. RADIUS 서버의 경우 모범 사례는 22자입니다.
RADIUS DTLS Settings(RADIUS DTLS 설정**)**	

필드 이름	사용 지침
DTLS Required(DTLS 필수**)**	**DTLS Required(DLTS** 필수**)** 확인란을 선택하면 Cisco ISE에서 이 디바이스의 DTLS 요청만 처리합니다. 이 옵션을 비활성화하면 Cisco ISE에서 이 디바이스의 UDP 요청과 DTLS 요청을 모두 처리합니다. RADIUS DTLS는 SSL 터널 설정 및 RADIUS 통신을 위한 향상된 보안을 제공합니다.
Shared Secret(공유 암호**)**	RADIUS DTLS에 사용되는 공유 암호를 표시합니다. 이 값은 고정되어 있으며 MD5 무결성 확인을 컴퓨팅하는 데 사용됩니다.
Issuer CA of ISE Certificates for CoA(CoA의 **ISE** 인증서에 대한 발급자 **CA)**	**Issuer CA of ISE Certificates for CoA(CoA**의 **ISE** 인증서에 대한 발급자 **CA)** 드롭다운 목록에서 RADIUS DTLS CoA에 사용할 인증 기관을 선택합니다.
General Settings(일반 설정**)**	
Enable KeyWrap(KeyWrap 활성화**)**	네트워크 디바이스에서 KeyWrap 알고리즘이 지원되는 경우에만 **Enable KeyWrap(KeyWrap** 활성화**)** 확인란을 선택합니다. 확인란을 선택하면 AES KeyWrap 알고리즘을 통해 RADIUS 보안이 개선됩니다.
Key Encryption Key(키 암호화 키**)**	KeyWrap을 활성화하는 경우 세션 암호화(비밀 유지)에 사용할 암호화 키를 입력합니다.
Message Authenticator Code Key(메시지 인증자 코드 키**)**	KeyWrap을 활성화하는 경우 RADIUS 메시지에 대한 키 HMAC(Hashed Message Authentication Code) 계산에 사용되는 키를 입력합니다.
Key Input Format(키 입력 형식**)**	다음 형식 중 하나의 해당 라디오 버튼을 클릭하여 선택하고 **Key Encryption Key(**키 암호화 키**)** 및 **Message Authenticator Code Key(**메시지 인증자 코드 키**)** 필드에 값을 입력합니다. • **ASCII**: 키 암호화 키의 길이는 16자(바이트)여야 하며 메시지 인증자 코드 키의 길이는 20자(바이트)여야 합니다. • **Hexadecimal(16**진수**)**: 키 암호화 키의 길이는 32바이트여야 하며 메시지 인증자 코드 키의 길이는 40바이트여야 합니다.
TACACS Authentication Settings(TACACS 인증 설정**)**	

필드 이름	사용 지침
Shared Secret(공유 암호**)**	TACACS+ 프로토콜을 활성화할 때 네트워크 디바이스에 할당된 텍스트 문자열입니다. 네트워크 디바이스가 사용자 이름과 비밀번호를 인증하기 전에 사용자가 텍스트를 입력해야 합니다. 사용자가 공유 암호를 제공할 때까지는 연결이 거부됩니다.
Retired Shared Secret is Active(사용 중단된 공유 암호가 활성 상태임**)**	사용 중단 기간이 활성인 경우 표시됩니다.
Retire(사용 중단**)**	기존 공유 암호를 종료하는 대신 사용 중단합니다. **Retire(**사용 중단**)**를 클릭하면 메시지 상자가 표시됩니다. **Yes(**예**)** 또는 **No(**아니요**)**를 클릭합니다.
Remaining Retired Period(남은 사용 중단 기간**)**	(위의 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Settings(**설정**)** > **Connection Settings(**연결 설정**)** > **Default Shared Secret Retirement Period(**기본 공유 암호 사용 중단 기간**)** 탐색 경로에 지정되어 있는 기본값이 표시됩니다. 기본값은 변경할 수 있습니다. 그러면 새 공유 암호를 입력할 수 있으며, 이전 공유 암호는 지정된 기간(일) 동안 활성 상태로 유지됩니다.
End(종료**)**	(위의 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) 사용 중단 기간을 종료하고 이전 공유 암호 사용을 중단합니다.
Enable Single Connect Mode(단일 연결 모드 활성화**)**	네트워크 디바이스와의 모든 TACACS+ 통신에 단일 TCP 연결을 사용하려면 **Enable Single Connect Mode(**단일 연결 모드 활성화**)** 확인란을 선택합니다. 다음 중 하나의 옵션에 해당하는 라디오 버튼을 클릭합니다. • **Legacy Cisco Devices(**레거시 **Cisco** 디바이스**)** • **TACACS Draft Compliance Single Connect Support(TACACS+** 초안 규정 준수 단일 연결 지원**)**. 이 옵션을 비활성화하면 Cisco ISE는 모든 TACACS+ 요청에 대해 새 TCP 연결을 사용합니다.

디바이스 보안 설정

RADIUS 공유 암호의 최소 길이를 지정합니다. 신규 설치 및 업그레이드된 구축의 경우 이 값은 기본적으로 4자입니다. RADIUS 서버의 경우 모범 사례는 22자입니다.

참고 Network Devices(네트워크 디바이스) 페이지에 입력한 공유 암호 길이는 Device Security Settings(디바이스 보안 설정) 창의 Minimum RADIUS Shared Secret Length(최소 RADIUS 공유 암호 길이) 필드에 구성된 값보다 크거나 같아야 합니다.

관련 항목

네트워크 디바이스 정의 설정

네트워크 디바이스 가져오기 설정

다음 표에서는 Cisco ISE로 네트워크 디바이스 세부정보를 가져오는 데 사용할 수 있는 네트워크 디바이스 가져오기 페이지의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** 입니다.

표 *7:* 네트워크 디바이스 가져오기 설정

필드 이름	사용 지침
Generate a Template(템플릿 생성**)**	쉼표로 구분된 값(CSV) 템플릿 파일을 생성하려면 **Generate a Template(**템플릿 생성**)**을 클릭합니다. 동일한 형식의 네트워크 디바이스 정보로 템플릿을 업데이트하고 로컬에 저장합니다. 그런 다음 편집된 템플릿을 사용하여 네트워크 디바이스를 Cisco ISE 구축으로 가져옵니다.
파일	**Choose File(**파일 선택**)**을 클릭하여, 최근에 직접 생성했거나 이전에 Cisco ISE 구축에서 내보냈을 수 있는 CSV 파일을 선택합니다. **Import(**가져오기**)** 옵션을 사용하면 신규/업데이트된 네트워크 디바이스 정보가 포함된 다른 Cisco ISE 구축의 네트워크 디바이스를 가져올 수 있습니다.

필드 이름	사용 지침
Overwrite Existing Data with New Data(새 데이터로 기존 데이터 덮어쓰기**)**	Cisco ISE가 기존 네트워크 디바이스를 가져오기 파일의 디바이스로 교체하도록 하려면 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 가져오기 파일에서 사용 가능한 새 네트워크 디바이스 정의가 네트워크 디바이스 저장소에 추가됩니다. 중복 엔트리는 무시됩니다.
Stop Import on First Error(첫 번째 오류에서 가져오기 중지**)**	가져오기 중에 오류가 발생하는 경우 Cisco ISE가 가져오기를 중단하게 하려면 **Stop Import on First Error(**첫 번째 오류에서 가져오기 중지**)** 확인란을 선택합니다. 그러면 Cisco ISE는 오류가 발생할 때까지 네트워크 디바이스를 가져옵니다. 이 확인란을 선택하지 않은 상태에서 발생하는 오류는 보고되며 Cisco ISE는 나머지 디바이스 가져오기를 계속합니다.

네트워크 디바이스 그룹 관리

다음 창에서는 네트워크 디바이스 그룹을 구성하고 관리할 수 있습니다.

네트워크 디바이스 그룹 설정

다음 표에서는 네트워크 디바이스 그룹을 생성하는 데 사용할 수 있는 **Network Device Groups(**네트워크 디바이스 그룹**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)** > **All Groups(**모든 그룹**)**입니다.

Work Centers(작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)** > **All Groups(**모든 그룹**)** 창에서 네트워크 디바이스 그룹을 생성할 수도 있습니다.

표 ***8: Network Device Group(***네트워크 디바이스 그룹***)*** 창의 필드

필드 이름	사용 지침
Name(이름**)**	루트 네트워크 디바이스 그룹의 이름을 입력합니다. 루트 네트워크 디바이스 그룹에 추가된 모든 후속 자식 네트워크 디바이스 그룹에 대해서는 새롭게 생성된 네트워크 디바이스 그룹의 이름을 입력합니다. 루트 노드를 포함하여 네트워크 디바이스 그룹 계층 구조에 최대 6개의 노드를 포함할 수 있습니다. 각 네트워크 디바이스 그룹의 이름은 최대 32자까지 지정할 수 있습니다.
Description(설명**)**	루트 또는 자식 네트워크 디바이스 그룹에 대한 설명을 입력합니다.
No. of Network Devices(네트워크 디바이스 수**)**	이 열에 네트워크 그룹의 네트워크 디바이스 수가 표시됩니다.

네트워크 디바이스 그룹 가져오기 설정

다음 표에서는 **Network Device Group(**네트워크 디바이스 그룹**)** 창의 **Import(**가져오기**)** 대화 상자에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)**입니다.

표 ***9: Network Device Groups Import(***네트워크 디바이스 그룹 가져오기***)*** 창의 필드

필드 이름	사용 지침
Generate a Template(템플릿 생성**)**	링크를 클릭하여 CSV 템플릿 파일을 다운로드합니다. 네트워크 디바이스 그룹 정보가 포함된 템플릿을 같은 형식으로 업데이트하여 로컬에 저장하면 해당 네트워크 디바이스 그룹을 Cisco ISE 구축으로 가져올 수 있습니다.
File(파일**)**	업로드할 CSV 파일의 위치로 **Choose File(**파일 선택**)**을 클릭합니다. 이 파일은 새로 생성된 파일이거나 다른 Cisco ISE 구축에서 이전에 내보낸 파일일 수 있습니다. Cisco ISE 구축에서 신규/업데이트된 네트워크 디바이스 그룹 정보가 포함된 다른 구축으로 네트워크 디바이스 그룹을 가져올 수 있습니다.

필드 이름	사용 지침
Overwrite Existing Data with New Data(새 데이터로 기존 데이터 덮어쓰기**)**	Cisco ISE가 기존 네트워크 디바이스 그룹을 가져온 파일의 디바이스 그룹으로 교체하도록 하려면 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 가져온 파일에서 새 네트워크 디바이스 그룹이 네트워크 디바이스 그룹 저장소에 추가됩니다. 중복 엔트리는 무시됩니다.
Stop Import on First Error(첫 번째 오류에서 가져오기 중지**)**	가져오기 중에 오류가 발생한 첫 번째 인스턴스에서 가져오기를 중단하려면 **Stop Import on First Error(**첫 번째 오류에서 가져오기 중지**)** 확인란을 선택합니다. 이 확인란을 선택하지 않은 상태에서 오류가 발생하면 Cisco ISE가 오류를 보고하고 디바이스 그룹에 속한 나머지를 계속 가져옵니다.

네트워크 디바이스 프로파일 설정

다음 표에서는 Network Device Profiles(네트워크 디바이스 프로파일) 창의 필드에 대해 설명합니다. 이러한 필드를 사용하면 디바이스의 프로토콜 지원, 리디렉션 URL 및 CoA 설정과 같은 특정 벤더의 네트워크 디바이스 유형에 대한 기본 설정을 구성할 수 있습니다. 그런 다음 프로파일을 사용하여 특정 네트워크 디바이스를 정의합니다.

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**)**입니다.

네트워크 디바이스 프로파일 설정

다음 표에서는 Network Device Profile(네트워크 디바이스 프로파일) 섹션의 필드에 대해 설명합니다.

표 ***10:*** 네트워크 디바이스 프로파일 설정

필드 이름	설명
Name(이름**)**	네트워크 디바이스 프로파일의 이름을 입력합니다.
Description(설명**)**	네트워크 디바이스 프로파일에 대한 설명을 입력합니다.

필드 이름	설명
Icon(아이콘**)**	네트워크 디바이스 프로파일에 사용할 아이콘을 선택합니다. 기본적으로는 선택한 벤더의 아이콘이 사용됩니다. 선택하는 아이콘은 16 x 16 PNG 파일이어야 합니다.
Vendor(벤더**)**	네트워크 디바이스 프로파일의 벤더를 선택합니다.
Supported Protocols(지원되는 프로토콜**)**	
RADIUS	이 네트워크 디바이스 프로파일이 RADIUS를 지원하는 경우 이 확인란을 선택합니다.
TACACS+	이 네트워크 디바이스 프로파일이 TACACS+를 지원하는 경우 이 확인란을 선택합니다.
TrustSec	이 네트워크 디바이스 프로파일이 TrustSec을 지원하는 경우 이 확인란을 선택합니다.
RADIUS Dictionaries(RADIUS 사전**)**	이 프로파일에서 지원되는 하나 이상의 RADIUS 사전을 선택합니다. 프로파일을 생성하기 전에 모든 벤더별 RADIUS 사전을 가져옵니다.

인증**/**권한 부여 템플릿 설정

다음 표에서는 Authentication/Authorization(인증/권한 부여) 섹션의 필드에 대해 설명합니다.

표 ***11:*** 인증/권한 부여 설정

필드 이름	설명
Flow Type Conditions(플로우 유형 조건**)**	Cisco ISE는 유선 네트워크와 무선 네트워크 둘 다를 통해 기본 사용자 인증 및 액세스를 위한 802.1X, MAB(MAC Authentication Bypass) 및 브라우저 기반 웹 인증 로그인을 지원합니다. 이 네트워크 디바이스 유형이 지원하는 인증 로그인에 대한 확인란을 선택합니다. 이러한 로그인은 다음 중 하나 이상일 수 있습니다. • 유선 MAB(MAC Authentication Bypass) • 무선 MAB • 유선 802.1X • 무선 802.1X • 유선 웹 인증 • 무선 웹 인증 네트워크 디바이스 프로파일이 지원하는 인증 로그인을 선택한 후 로그인의 조건을 지정합니다.
Attribute Aliasing(속성 별칭**)**	디바이스의 SSID(Service Set Identifier)를 정책 규칙에서 Friendly Name으로 사용하려면 SSID 확인란을 선택합니다. 그러면 정책 규칙에서 사용할 일관된 이름을 생성할 수 있습니다.
호스트 조회**(MAB)**	
Process Host Lookup(프로세스 호스트 조회**)**	네트워크 디바이스 프로파일에 사용되는 호스트 조회용 프로토콜을 정의하려면 이 확인란을 선택합니다. 여러 벤더의 네트워크 디바이스는 각기 다른 방식으로 MAB 인증을 수행합니다. 디바이스 유형에 따라 사용 중인 프로토콜에 대해 **Check Password(**비밀번호 확인**)** 또는 **Checking Calling-Station-Id equals MAC Address(Calling-Station-Id**가 **MAC** 주소와 같은지 확인**)** 확인란 중 하나를 선택하거나 두 확인란을 모두 선택합니다.
Via PAP/ASCII(PAP/ASCII 사용**)**	Cisco ISE가 네트워크 디바이스 프로파일로부터의 PAP 요청을 호스트 조회 요청으로 탐지하도록 구성하려면 이 확인란을 선택합니다.

필드 이름	설명
Via CHAP(CHAP 사용**)**	Cisco ISE가 네트워크 디바이스로부터의 이 요청 유형을 호스트 조회 요청으로 탐지하도록 구성하려면 이 확인란을 선택합니다. 이 옵션은 CHAP 인증을 활성화합니다. CHAP는 비밀번호 암호화와 함께 시도 응답 메커니즘을 사용합니다. Microsoft Active Directory에서는 CHAP가 작동하지 않습니다.
Via EAP-MD5(EAP-MD5 사용**)**	네트워크 디바이스 프로파일에 대해 EAP 기반 MD5 해시 인증을 활성화하려면 이 확인란을 선택합니다.

권한

이 네트워크 디바이스 프로파일에 사용할 VLAN 및 ACL 권한을 정의할 수 있습니다. 프로파일을 저장하고 나면 Cisco ISE는 구성된 각 권한에 대해 권한 부여 프로파일을 자동으로 생성합니다.

표 ***12:*** 권한

필드 이름	설명
Set VLAN(VLAN 설정**)**	이 네트워크 디바이스 프로파일에 대한 VLAN 권한을 설정하려면 이 확인란을 선택하고 다음 옵션 중 하나를 선택합니다. • IETF 802.1X Attributes(IETF 802.1X 속성). Internet Engineering Task Force에서 정의한 기본 RADIUS 속성 집합입니다. • Unique Attributes(고유한 속성). 여러 RADIUS 속성-값 쌍을 지정할 수 있습니다.
Set ACL(ACL 설정**)**	네트워크 디바이스 프로파일에서 ACL에 대해 설정할 RADIUS 속성을 선택하려면 이 확인란을 선택합니다.

CoA(Change of Authorization) 템플릿 설정

이 템플릿은 이 네트워크 디바이스 유형으로 CoA가 전송되는 방법을 정의합니다. 다음 표에서는 Change of Authorization (CoA) 섹션의 필드에 대해 설명합니다.

표 ***13: CoA(Change of Authorization)*** 설정

필드 이름	정의
CoA by(CoA 전달 프로토콜**)**	다음 옵션 중 하나를 선택합니다. • RADIUS • SNMP • 지원되지 않음
RADIUS 사용 **CoA(CoA by RADIUS)**	
Default CoA Port(기본 CoA 포트)	RADIUS CoA를 전송할 포트입니다. 기본적으로 이는 Cisco 디바이스의 경우 포트 1700이고 Cisco 이외의 벤더 디바이스의 경우에는 포트 3799입니다. Network Device(네트워크 디바이스) 창에서 이를 재정의할 수 있습니다.
Timeout Interval(시간 초과 간격**)**	Cisco ISE가 CoA를 전송한 후 응답을 대기하는 시간(초)입니다.
Retry Count(재시도 횟수**)**	Cisco ISE가 첫 번째 시간 초과 후 CoA 전송을 시도하는 횟수입니다.
Disconnect(연결 끊기**)**	이러한 디바이스에 연결 끊기 요청을 전송할 방법을 선택합니다. • **RFC 5176**: RFC 5176에 정의된 대로 표준 세션 종료를 수행하고 새 세션에 준비된 상태로 포트를 유지하려면 이 확인란을 선택합니다. • **Port Bounce(**포트 바운스**)**: 세션을 종료하고 포트를 재시작하려면 이 확인란을 선택합니다. • **Port Shutdown(**포트 종료**)**: 세션을 종료하고 포트를 종료하려면 이 확인란을 선택합니다.

필드 이름	정의
Re-authenticate(재인증**)**	네트워크 디바이스에 재인증 요청을 전송할 방법을 선택합니다. 이는 현재 Cisco 디바이스에서만 지원됩니다. • **Basic(**기본**)**: 표준 세션 재인증을 수행하려면 이 확인란을 선택합니다. • **Rerun(**재실행**)**: 인증 방법을 처음부터 실행하려면 이 확인란을 선택합니다. • **Last(**최근**)**: 세션에 대해 마지막으로 성공한 인증 방법을 사용합니다.
CoA Push(CoA 푸시**)**	네트워크 디바이스가 Cisco의 TrustSec CoA 기능을 지원하지 않는 경우 Cisco ISE가 컨피그레이션 변경 사항을 디바이스에 푸시할 수 있도록 허용하려면 이 옵션을 선택합니다.
CoA by SNMP(SNMP 사용 **CoA)**	
Timeout Interval(시간 초과 간격**)**	Cisco ISE가 CoA를 전송한 후 응답을 대기하는 시간(초)입니다.
Retry Count(재시도 횟수**)**	Cisco ISE가 CoA 전송을 시도하는 횟수입니다.
NAD Port Detection(NAD 포트 탐지**)**	현재 Relevant RADIUS Attribute(관련 RADIUS 속성)만이 유일한 옵션입니다.
Relevant RADIUS Attribute(관련 **RADIUS** 속성**)**	NAD 포트를 탐지하는 방법을 선택합니다. • Nas-Port • Nas-Port-ID
Disconnect(연결 끊기**)**	이러한 디바이스에 연결 끊기 요청을 전송할 방법을 선택합니다. • **Reauthenticate(**재인증**)**: 세션을 종료하고 포트를 재시작하려면 이 확인란을 선택합니다. • **Port Bounce(**포트 바운스**)**: 세션을 종료하고 포트를 재시작하려면 이 확인란을 선택합니다. • **Port Shutdown(**포트 종료**)**: 세션을 종료하고 포트를 종료하려면 이 확인란을 선택합니다.

리디렉션 템플릿 설정

네트워크 디바이스가 권한 부여 프로파일의 일부로 구성되어 있는 경우 네트워크 디바이스는 클라이언트의 HTTP 요청을 리디렉션할 수 있습니다. 이 템플릿은 이 네트워크 디바이스 프로파일이 URL 리디렉션을 지원하는지 여부를 지정합니다. 디바이스 유형과 관련된 URL 파라미터 이름을 사용합니다.

다음 표에서는 Redirect(리디렉션) 섹션의 필드에 대해 설명합니다.

표 ***14:*** 리디렉션 설정

필드 이름	정의
Type(유형**)**	네트워크 디바이스 프로파일이 정적 URL 리디렉션을 지원할지 아니면 동적 URL 리디렉션 지원할지를 선택합니다. 디바이스가 어느 것도 지원하지 않는 경우 **Not Supported(**지원되지 않음**)**를 선택하고 **Settings(**설정**)** > **DHCP & DNS Services(DHCP** 및 **DNS** 서비스**)**에서 VLAN을 설정합니다.
Redirect URL Parameter Names(리디렉션 **URL** 파라미터 이름**)**	
Client IP Address(클라이언트 **IP** 주소**)**	네트워크 디바이스가 클라이언트의 IP 주소에 사용하는 파라미터 이름을 입력합니다.
Client MAC Address(클라이언트 **MAC** 주소**)**	네트워크 디바이스가 클라이언트의 MAC 주소에 사용하는 파라미터 이름을 입력합니다.
Originating URL(원래 **URL)**	네트워크 디바이스가 원래 URL에 사용하는 파라미터 이름을 입력합니다.
Session ID(세션 **ID)**	네트워크 디바이스가 세션 ID에 사용하는 파라미터 이름을 입력합니다.
SSID	네트워크 디바이스가 SSID(Service Set Identifier)에 사용하는 파라미터 이름을 입력합니다.
Dynamic URL Parameters(동적 **URL** 파라미터**)**	
Parameter(파라미터**)**	리디렉션에 Dynamic URL(동적 URL)을 사용하도록 선택하는 경우 이러한 네트워크 디바이스가 리디렉션 URL을 생성하는 방법을 지정해야 합니다. 또한 리디렉션 URL이 세션 ID를 사용할지 아니면 클라이언트 MAC 주소를 사용할지를 지정할 수도 있습니다.

고급 설정

Network Device Profile(네트워크 디바이스 프로파일)을 사용하여 정책 규칙에서 네트워크 디바이스를 쉽게 사용하기 위해 여러 정책 요소를 생성할 수 있습니다. 이러한 요소에는 복합 조건, 권한 부여 프로파일 및 허용된 프로토콜이 포함됩니다.

이러한 요소를 생성하려면 **Generate Policy Elements(**정책 요소 생성**)**를 클릭합니다.

외부 **RADIUS** 서버 설정

다음 표에서는 RADIUS 서버를 구성하는 데 사용할 수 있는 External RADIUS Server(외부 RADIUS 서버) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External RADIUS Servers(**외부 **RADIUS** 서버**)**입니다.

표 ***15:*** 외부 ***RADIUS*** 서버 설정

필드 이름	사용 지침
Name(이름**)**	외부 RADIUS 서버의 이름을 입력합니다.
Description(설명**)**	외부 RADIUS 서버에 대한 설명을 입력합니다.
Host IP(호스트 **IP)**	외부 RADIUS 서버의 IP 주소를 입력합니다. IPv4 주소를 입력할 때 범위 및 서브넷 마스크를 사용할 수 있습니다. IPv6용 범위는 지원되지 않습니다.
Shared Secret(공유 암호**)**	외부 RADIUS 서버를 인증하는 데 사용되는 Cisco ISE와 외부 RADIUS 서버 간 공유 암호를 입력합니다. 공유 암호는 네트워크 디바이스가 사용자 이름 및 비밀번호를 인증할 수 있도록 사용자가 제공해야 하는 필요한 텍스트 문자열입니다. 사용자가 공유 암호를 제공할 때까지는 연결이 거부됩니다. 공유 암호의 최대 길이는 128자입니다.
Enable KeyWrap(KeyWrap 활성화**)**	AES KeyWrap 알고리즘을 통해 RADIUS 프로토콜 보안을 개선하려면 이 옵션을 활성화합니다.
Key Encryption Key(키 암호화 키**)**	(Enable KeyWrap(KeyWrap 활성화) 확인란을 선택하는 경우에만 해당함) 세션 암호화(비밀 유지)에 사용되는 키를 입력합니다.
Message Authenticator Code Key(메시지 인증자 코드 키**)**	(Enable KeyWrap(KeyWrap 활성화) 확인란을 선택하는 경우에만 해당함) RADIUS 메시지에 대한 키 HMAC 계산에 사용되는 키를 입력합니다.

필드 이름	사용 지침
Key Input Format(키 입력 형식**)**	Cisco ISE 암호화 키를 입력하는 데 사용할 입력 형식을 WLAN 컨트롤러에서 사용 가능한 컨피그레이션과 일치하도록 지정합니다. 이 값은 아래에 정의되어 있는 것처럼 키의 정확한 (전체) 길이로 지정해야 하며 더 짧은 값은 지정할 수 없습니다. • ASCII: 키 암호화 키의 길이는 16자(바이트)여야 하며, 메시지 인증자 코드 키의 길이는 20자(바이트)여야 합니다. • Hexadecimal(16진수): 키 암호화 키의 길이는 32바이트여야 하며, 메시지 인증자 코드 키의 길이는 40바이트여야 합니다.
Authentication Port(인증 포트**)**	RADIUS 인증 포트 번호를 입력합니다. 유효 범위는 1~65535입니다. 기본값은 1,812입니다.
Accounting Port(계정 관리 포트**)**	RADIUS 계정 관리 포트 번호를 입력합니다. 유효 범위는 1~65535입니다. 기본값은 1,813입니다.
Server Timeout(서버 시간 초과**)**	Cisco ISE가 외부 RADIUS 서버로부터의 응답을 대기할 시간을 초 단위로 입력합니다. 기본값은 5초입니다. 유효한 값은 5~120입니다.
Connection Attempts(연결 시도 횟수**)**	Cisco ISE가 외부 RADIUS 서버에 대한 연결을 시도하는 횟수를 단위로 입력합니다. 기본값은 3회입니다. 유효한 값은 1~9입니다.
RADIUS Proxy Failover Expiration(RADIUS 프록시 페일오버 만료**)**	연결이 실패한 후에 해당 서버에 대한 연결을 다시 시도할 때까지의 경과 시간을 입력합니다. 유효 범위는 1~600입니다. 서버 시간 초과를 건너뛰고 바로 페일오버로 넘어가도록 하려면 이 매개변수를 구성합니다.

RADIUS 서버 시퀀스

다음 표에서는 RADIUS 서버 시퀀스를 생성하는 데 사용할 수 있는 RADIUS Server Sequences(RADIUS 서버 시퀀스) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **RADIUS Server Sequences** > **Add(RADIUS** 서버 시퀀스 > 추가**)**입니다.

표 ***16: RADIUS*** 서버 시퀀스

필드 이름	사용 지침
Name(이름**)**	RADIUS 서버 시퀀스의 이름을 입력합니다.
Description(설명**)**	필요에 따라 설명을 입력합니다.
Host IP(호스트 **IP)**	외부 RADIUS 서버의 IP 주소를 입력합니다.
User Selected Service Type(사용자가 선택한 서비스 유형**)**	정책 서버로 사용할 외부 RADIUS 서버를 사용 가능 목록 상자에서 선택한 다음 선택됨 목록 상자로 이동합니다.
Remote Accounting(원격 계정 관리**)**	원격 정책 서버에서 계정 관리 기능을 활성화하려면 이 확인란을 선택합니다.
Local Accounting(로컬 계정 관리**)**	Cisco ISE의 계정 관리를 활성화하려면 이 확인란을 선택합니다.
Advanced Attribute Settings(고급 속성 설정**)**	
Strip Start of Subject Name up to the First Occurrence of the Separator(처음으로 나타나는 구분 기호까지 주체 이름 시작 부분 분리**)**	접두사에서 사용자 이름을 분리하려면 이 확인란을 선택합니다. 예를 들어 주체 이름이 acme\userA이고 구분 기호가 \이면 사용자 이름은 userA가 됩니다.
Strip End of Subject Name from the Last Occurrence of the Separator(마지막으로 나타나는 구분 기호부터 주체 이름 끝 부분 분리**)**	접미사에서 사용자 이름을 분리하려면 이 확인란을 선택합니다. 예를 들어 주체 이름이 userA@abc.com이고 구분 기호가 @이면 사용자 이름은 userA가 됩니다. • NetBIOS 또는 UPN(사용자 계정 이름) 형식 사용자 이름(user@domain.com 또는 /domain/user)에서 사용자 이름을 추출하려면 분리 옵션을 활성화해야 합니다. 사용자를 인증하기 위해 사용자 이름만 RADIUS 서버로 전달되기 때문입니다. • \ 및 @ 분리 기능을 모두 활성화하고 Cisco AnyConnect를 사용 중이면 Cisco ISE는 문자열에서 첫 번째 \를 정확하게 자르지 않습니다. 그러나 개별적으로 사용되는 각 분리 기능은 Cisco AnyConnect에서도 정상적으로 작동합니다.

필드 이름	사용 지침
Modify Attributes in the Request to the External RADIUS Server(외부 **RADIUS** 서버에 대한 요청의 속성 수정**)**	Cisco ISE가 인증된 RADIUS 서버에서 보내거나 받는 속성을 조작할 수 있도록 하려면 이 확인란을 선택합니다. 속성 조작 작업은 다음과 같습니다. • **Add(**추가**)**: 전체 RADIUS 요청/응답에 속성을 더 추가합니다. • **Update(**업데이트**)**: 속성 값(고정/정적)을 변경하거나 속성을 다른 속성 값(동적)으로 대체합니다. • **Remove(**제거**)**: 속성 또는 속성-값 쌍을 제거합니다. • **RemoveAny(**모두 제거**)**: 모든 속성 항목을 제거합니다.
Continue to Authorization Policy(권한 부여 정책 계속 진행**)**	ID 저장소 그룹 및 속성 검색을 기준으로 하여 추가 의사 결정을 위해 프록시 흐름을 전환하여 권한 부여 정책을 실행하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 외부 RADIUS 서버의 응답에 포함된 속성이 인증 정책 선택 시 적용됩니다. 상황에 이미 있는 속성은 AAA 서버 수락 응답 속성의 적절한 값으로 업데이트됩니다.
Modify Attributes before send an Access-Accept(액세스 수락 전송 전에 속성 수정**)**	디바이스로 응답을 다시 보내기 전에 속성을 수정하려면 이 확인란을 선택합니다.

NAC Manager 설정

다음 표에서는 NAC Manager를 추가하는 데 사용할 수 있는 새 NAC Manager 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **NAC Managers(NAC Manager)**입니다.

표 ***17: NAC Manager*** 설정

필드	사용 지침
Name(이름)	CAM(Cisco Access Manager)의 이름을 입력합니다.
Status(상태)	CAM에 대한 연결을 인증하는 Cisco ISE 프로파일러에서 REST API 통신을 활성화하려면 Status(상태) 확인란을 클릭합니다.

필드	사용 지침
Description(설명)	CAM에 대한 설명을 입력합니다.
IP Address(IP 주소)	CAM의 IP 주소를 입력합니다. Cisco ISE에서 CAM를 생성하여 저장한 후에는 CAM의 IP 주소를 편집할 수 없습니다. 0.0.0.0 및 255.255.255.255는 Cisco ISE에서 CAM의 IP 주소를 검증할 때 제외되므로 사용할 수 없습니다. 즉, 이 두 IP 주소는 CAM의 IP Address(IP 주소) 필드에 사용할 수 있는 유효한 IP 주소가 아닙니다. 참고 고가용성 컨피그레이션에서 CAM 쌍이 공유하는 가상 서비스 IP 주소를 사용할 수 있습니다. 이렇게 하면 고가용성 컨피그레이션에서 CAM의 페일오버가 지원됩니다.
Username(사용자 이름)	CAM의 사용자 인터페이스에 로그온하는 데 사용할 수 있는 CAM 관리자의 사용자 이름을 입력합니다.
Password(비밀번호)	CAM의 사용자 인터페이스에 로그온하는 데 사용할 수 있는 CAM 관리자의 비밀번호를 입력합니다.

디바이스 포털 관리

디바이스 포털 설정 구성

디바이스 포털의 포털 ID 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Managment(**디바이스 포털 관리**)** > **Blocked List Portal, Client Provisioning Portals, BYOD Portals, MDM Portals, or My Device Portals(**차단 목록 포털**,** 클라이언트 프로비저닝 포털**, BYOD** 포털**, MDM** 포털 또는 내 디바이스 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portals Settings and Customization(**포털 설정 및 사용자 맞춤화**)**입니다.

- **Portal Name(**포털 이름**)**: 이 포털에 액세스하는 데 사용할 고유한 포털 이름을 입력합니다. 차단 목록, BYOD(Bring Your Own Device), 클라이언트 프로비저닝, MDM(Mobile Device Management), 내 디바이스 포털 등 기타 모든 스폰서 포털, 게스트 포털 및 비게스트 포털에 대해서는 이 이름을 포털 이름을 사용하지 마십시오.

이 이름은 리디렉션 선택을 위한 권한 부여 프로파일 포털 선택 항목에 표시됩니다. 이는 다른 포털과 쉽게 식별할 수 있도록 포털 목록에 적용됩니다.

- **Description(**설명**)**: 선택 사항입니다.
- **Portal test URL(**포털 테스트 **URL)**: **Save(**저장**)**를 클릭하면 시스템에서 생성된 URL이 링크로 표시됩니다. 이 URL을 사용하여 포털을 테스트합니다.

  링크를 클릭하여, 이 포털의 URL을 표시하는 새 브라우저 탭을 열 수 있습니다. 정책 서비스가 있는 PSN(정책 서비스 노드)은 반드시 활성화해야 합니다. 정책 서비스가 비활성화되면 PSN이 관리자 포털만 표시합니다.

  참고 테스트 포털은 RADIUS 세션을 지원하지 않으므로 모든 포털의 전체 포털 플로우를 볼 수 없습니다. RADIUS 세션을 사용하는 포털의 예로는 BYOD 및 클라이언트 프로비저닝이 있습니다. 예를 들어 외부 URL로의 리디렉션은 작동하지 않습니다. PSN이 한 개보다 많은 경우 Cisco ISE는 첫 번째 활성 상태의 PSN을 선택합니다.

- **Language File(**언어 파일**)**: 각 포털 유형은 기본적으로 15개 언어를 지원합니다. 이러한 언어는 단일 압축(zip) 언어 파일에 함께 번들링된 개별 속성 파일로 사용할 수 있습니다. 포털에서 사용할 압축 언어 파일을 내보내거나 가져옵니다. 압축 언어 파일에는 포털의 텍스트를 표시하는 데 사용할 수 있는 모든 개별 언어 파일이 포함되어 있습니다.

  언어 파일은 특정 브라우저 로캘 설정에 대한 매핑 및 해당 언어로 된 전체 포털에 대한 모든 문자열 설정을 포함합니다. 단일 언어 파일은 변환 및 지역화를 위해 쉽게 사용할 수 있도록 지원되는 모든 언어를 포함합니다.

  언어 하나에 대한 브라우저 로캘 설정을 변경하면 기타 모든 최종 사용자 웹 포털에 변경 사항이 적용됩니다. 예를 들어 핫스팟 게스트 포털에서 French.properties 브라우저 로캘을 fr,fr-fr,fr-ca에서 fr,fr-fr로 변경하면 내 디바이스 포털에도 변경 사항이 적용됩니다.

  Portal Page **Customizations(**포털 페이지 사용자 맞춤화**)** 탭에서 포털 페이지 텍스트를 사용자 맞춤화하면 경고 아이콘이 표시됩니다. 이 경고 메시지는 포털을 사용자 맞춤화하는 동안 한 언어에 적용한 변경 사항을 지원되는 모든 언어 속성 파일에도 추가해야 한다는 알림을 표시합니다. 드롭다운 목록 옵션을 사용하여 경고 아이콘을 수동으로 해제할 수 있습니다. 또는 업데이트된 압축 언어 파일을 가져오고 나면 아이콘은 자동으로 해제됩니다.

BYOD 및 MDM 포털에 대한 포털 설정

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

포털 페이지 작업을 정의하려면 이러한 설정을 구성합니다.

- **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 업

그레이드한 경우에는 이 창에서 설정을 변경할 때까지 해당 값이 적용됩니다. 이 창을 변경하는 경우에는 이 제한을 준수하도록 포트 설정을 업데이트해야 합니다.

내 디바이스 등의 게스트 포털이 아닌 포털에서 사용하는 포트를 게스트 포털에 할당하면 오류 메시지가 표시됩니다.

포스처 평가 및 교정에 한해 클라이언트 프로비저닝 포털은 포트 8905 및 8909도 사용하며, 그 외의 경우에는 게스트 포털에 할당된 것과 같은 포털을 사용합니다.

동일한 HTTPS 포트에 할당된 포털은 같은 기가비트 인터페이스 또는 다른 인터페이스를 사용할 수 있습니다. 동일한 포트 및 인터페이스 조합을 사용하는 포털은 동일한 인증서 그룹 태그를 사용해야 합니다. 예를 들면 다음과 같습니다.

- 스폰서 포털을 예로 들 때 유효한 조합은 다음을 포함합니다.
  - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 태그 **A**/내 디바이스 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**
  - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**/내 디바이스 포털: 포트 **8445**, 인터페이스 **0**, 인증서 그룹 **B**
  - 스폰서 포털: 포트 **8444**, 인터페이스 **1**, 인증서 그룹 **A**/차단 목록 포털: 포트 **8444**, 인터페이스 **0**, 인증서 그룹 **B**
- 잘못된 조합은 다음과 같습니다.
  - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**/내 디바이스 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **B**
  - 스폰서 포털: 포트 **8444**, 인터페이스 **0**, 인증서 태그 **A**/차단 목록 포털: 포트 **8444**, 인터페이스 **0**, 인증서 그룹 **A**

참고 최상의 성능을 위해서는 게스트 서비스에 인터페이스 0을 사용하는 것이 좋습니다. **Portal Settings(**포털 설정**)**에서 인터페이스 0만 구성하거나 CLI 명령 **ip host**를 사용하여 호스트 이름 또는 FQDN을 인터페이스 0의 IP 주소에 매핑 할 수 있습니다.

- **Allowed Interfaces(**허용된 인터페이스**)**: PAN이 포털을 실행하는 데 사용할 수 있는 PSN 인터페이스를 선택합니다. PAN에서 포털 열기 요청이 수행되면 PAN은 PSN에서 사용 가능한 허용된 포트를 찾습니다. 다른 서브넷의 IP 주소를 사용하여 이더넷 인터페이스를 구성해야 합니다.

  이러한 인터페이스는 정책 서비스가 설정된 VM 기반 PSN을 포함하여 모든 PSN에서 사용할 수 있어야 합니다. 이 요건이 적용되는 이유는 게스트 세션 시작 시 리디렉션에 이러한 PSN을 사용할 수 있기 때문입니다.

  - 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 IP 주소를 확인해야 합니다.
- 보조 인터페이스 IP 주소를 FQDN에 매핑하려면 Cisco ISE CLI에서 **ip host x.x.x.x yyy.domain.com**을 구성합니다. 이 항목은 인증서 주체 이름 또는 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. PSN은 물리적 인터페이스에서 포털을 시작하려고 시도하지 않습니다.
- NIC 팀 또는 결합은 컨피그레이션 옵션으로, 이를 통해 고가용성(내결함성)을 위해 개별 NIC 2개를 구성할 수 있습니다. NIC 중 하나에서 장애가 발생하면 결합형 연결의 일부분인 다른 NIC가 연결을 계속 진행합니다. NIC는 **Portal Settings(**포털 설정**)** 컨피그레이션에 기반하여 포털에 대해 선택됩니다. 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 인증서를 지정하는 인증서 그룹 태그를 선택합니다.
- **Endpoint Identity Group(**엔드포인트 **ID** 그룹**)**: 게스트 디바이스를 추적하기 위한 엔드포인트 ID 그룹을 선택합니다. Cisco ISE는 기본값으로 사용할 **GuestEndpoints** 엔드포인트 ID 그룹을 제공합니다. 기본값을 사용하지 않으려는 경우에는 엔드포인트 ID 그룹을 추가로 생성할 수도 있습니다.

  직원 디바이스를 추적하기 위한 엔드포인트 ID 그룹을 선택합니다. Cisco ISE는 기본값으로 사용할 **RegisteredDevices** 엔드포인트 ID 그룹을 제공합니다. 기본값을 사용하지 않으려는 경우에는 엔드포인트 ID 그룹을 추가로 생성할 수도 있습니다.
- **Display Language(**표시 언어**)**
  - **Use Browser Local(**브라우저 로캘 사용**)**: 클라이언트 브라우저의 로캘 설정에 지정된 언어를 포털의 표시 언어로 사용합니다. 브라우저 로캘의 언어가 Cisco ISE에서 지원되지 않는 경우 **Fallback Language(**대체 언어**)**가 언어 포털로 사용됩니다.
  - **Fallback Language(**대체 언어**)**: 브라우저 로캘에서 언어를 가져올 수 없거나 Cisco ISE에서 브라우저 로캘 언어를 지원하지 않는 경우 사용할 언어를 선택합니다.
  - **Always Use(**항상 사용**)**: 포털에 사용할 표시 언어를 선택합니다. 이 설정은 **User Browser Locale(**사용자 브라우저 로캘**)** 옵션을 재정의합니다.

BYOD 포털에 대한 BYOD 설정

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

이 설정을 사용하면 개인 디바이스를 사용하여 기업 네트워크에 액세스하려는 직원을 위해 BYOD(Bring Your Own Device) 기능을 활성화할 수 있습니다.

필드 이름	사용 지침
Include an AUP(AUP 포함**)(**페이지에/링크로**)**	회사의 네트워크 사용 약관을 사용자에 대해 현재 표시되어 있는 창에 텍스트로 표시하거나, AUP 텍스트가 포함된 새 탭 또는 창을 여는 링크로 표시합니다.
Require Acceptance(수락 필요**)**	직원이 AUP를 수락해야 계정이 완전히 활성화되도록 지정합니다. 사용자가 AUP를 수락하지 않으면 **Login(**로그인**)** 버튼은 활성화되지 않습니다. AUP를 수락하지 않는 게스트에게는 네트워크 액세스 권한이 제공되지 않습니다.
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.
Display Device ID Field During Registration(등록 중에 디바이스 **ID** 필드 표시**)**	디바이스 ID가 미리 구성되어 있어 BYOD 포털 사용 중에 변경할 수 없는 상태이더라도 등록 프로세스 중에 사용자에게 디바이스 ID를 표시합니다.
Originating URL(원래 **URL)**	네트워크에 정상적으로 인증한 후 사용자 브라우저를 사용자가 액세스하려고 하는 원래 웹사이트(사용 가능한 경우)로 리디렉션합니다. 이 웹사이트를 사용할 수 없는 경우에는 인증 성공 창이 표시됩니다. 리디렉션 URL이 NAD의 액세스 제어 목록 및 해당 NAD에 대해 Cisco ISE에 구성된 권한 부여 프로파일에 의해 PSN의 포트 8443에서 작동하도록 허용되어야 합니다. Windows, Mac 및 Android 디바이스의 경우에는 프로비저닝을 수행하는 셀프 프로비저닝 마법사 앱에 제어권이 제공됩니다. 따라서 이러한 디바이스는 원래 URL로 리디렉션되지 않습니다. 그러나 iOS(dot1X) 및 네트워크 액세스가 허용되는 지원되지 않는 디바이스의 경우 이 URL로 리디렉션됩니다.
Success page(성공 페이지)	디바이스 등록에 성공했음을 나타내는 페이지를 표시합니다.
URL	네트워크에 정상적으로 인증한 후 사용자 브라우저를 회사 웹사이트 등의 지정된 URL로 리디렉션합니다.

참고 인증 후 게스트를 외부 URL로 리디렉션하는 경우 URL 주소가 확인되고 세션이 리디렉션되는 동안 지연이 발생할 수 있습니다.

인증서 프로비저닝 포털의 포털 설정

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

- **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 창에서 설정을 변경할 때까지 해당 값이 적용됩니다. 이 창을 변경하는 경우에는 이 제한을 준수하도록 포트 설정을 업데이트해야 합니다.

  내 디바이스 등의 게스트 포털이 아닌 포털에서 사용하는 포트를 게스트 포털에 할당하면 오류 메시지가 표시됩니다.

  포스처 평가 및 교정에 한해 클라이언트 프로비저닝 포털은 포트 8905 및 8909도 사용하며, 그 외의 경우에는 게스트 포털에 할당된 것과 같은 포털을 사용합니다.

  동일한 HTTPS 포트에 할당된 포털은 같은 기가비트 인터페이스 또는 다른 인터페이스를 사용할 수 있습니다. 동일한 포트 및 인터페이스 조합을 사용하는 포털은 동일한 인증서 그룹 태그를 사용해야 합니다. 예를 들면 다음과 같습니다.

  - 스폰서 포털을 예로 들 때 유효한 조합은 다음을 포함합니다.
    - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 태그 **A**/내 디바이스 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**
    - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**/내 디바이스 포털: 포트 **8445**, 인터페이스 **0**, 인증서 그룹 **B**
    - 스폰서 포털: 포트 **8444**, 인터페이스 **1**, 인증서 그룹 **A**/차단 목록 포털: 포트 **8444**, 인터페이스 **0**, 인증서 그룹 **B**
  - 잘못된 조합은 다음과 같습니다.
    - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**/내 디바이스 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **B**
    - 스폰서 포털: 포트 **8444**, 인터페이스 **0**, 인증서 태그 **A**/차단 목록 포털: 포트 **8444**, 인터페이스 **0**, 인증서 그룹 **A**

참고 최상의 성능을 위해서는 게스트 서비스에 인터페이스 0을 사용하는 것이 좋습니다. **Portal Settings(**포털 설정**)**에서 인터페이스 0만 구성하거나 CLI 명령 **ip host**를 사용하여 호스트 이름 또는 FQDN을 인터페이스 0의 IP 주소에 매핑 할 수 있습니다.

- **Allowed Interfaces(**허용된 인터페이스**)**: PAN이 포털을 실행하는 데 사용할 수 있는 PSN 인터페이스를 선택합니다. PAN에서 포털 열기 요청이 수행되면 PAN은 PSN에서 사용 가능한 허용된 포트를 찾습니다. 다른 서브넷의 IP 주소를 사용하여 이더넷 인터페이스를 구성해야 합니다.

  이러한 인터페이스는 정책 서비스가 설정된 VM 기반 PSN을 포함하여 모든 PSN에서 사용할 수 있어야 합니다. 이 요건이 적용되는 이유는 게스트 세션 시작 시 리디렉션에 이러한 PSN을 사용할 수 있기 때문입니다.

  - 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 IP 주소를 확인해야 합니다.
  - 보조 인터페이스 IP 주소를 FQDN에 매핑하려면 Cisco ISE CLI에서 **ip host x.x.x.x yyy.domain.com**을 구성합니다. 이 항목은 인증서 주체 이름 또는 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. PSN은 물리적 인터페이스에서 포털을 시작하려고 시도하지 않습니다.
  - NIC 팀 또는 결합은 컨피그레이션 옵션으로, 이를 통해 고가용성(내결함성)을 위해 개별 NIC 2개를 구성할 수 있습니다. NIC 중 하나에서 장애가 발생하면 결합형 연결의 일부분인 다른 NIC가 연결을 계속 진행합니다. NIC는 **Portal Settings(**포털 설정**)** 컨피그레이션에 기반하여 포털에 대해 선택됩니다. 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 인증서를 지정하는 인증서 그룹 태그를 선택합니다.
- **Authentication Method(**인증 방법**)**: 사용자 인증에 사용할 ID 소스 시퀀스 또는 IdP(ID 제공자)를 선택합니다. ID 소스 시퀀스는 사용자 자격 증명을 확인하기 위해 순서대로 검색되는 ID 저장소 목록입니다.

  Cisco ISE에는 스폰서 포털용 기본 ID 소스 시퀀스인 Sponsor_Portal_Sequence가 포함되어 있습니다.

IdP를 구성하려면 **Administration(**관리**) > Identity Management(ID** 관리**) > External Identity Sources(**외부 **ID** 소스**) > SAML Id Providers(SAML ID** 제공자**)**를 선택합니다.

ID 소스 시퀀스를 구성하려면 **Administration(**관리**) > Identity Management(ID** 관리**) > Identity Source Sequences(ID** 소스 시퀀스**)**를 선택합니다.

- **Configure authorized groups(**권한 부여된 그룹 구성**)**: 인증서 생성 권한을 부여할 사용자 ID 그룹을 선택하여 Chosen(선택됨) 상자로 이동합니다.
- **Fully Qualified Domain Name (FQDN)(FQDN(**정규화된 도메인 이름**))** - 스폰서 또는 내 디바이스 포털에 대해 고유한 FQDN 및/또는 호스트 이름을 하나 이상 입력합니다. 예를 들어 **`sponsorportal.yourcompany.com,sponsor`**를 입력할 수 있습니다. 그러면 사용자가 브라우저에 해당 이름 중 하나를 입력하면 스폰서 포털이 표시됩니다. 이름은 쉼표로 구분하되 엔트리 사이에 공백은 포함하지 마십시오.

  기본 FQDN를 변경하는 경우 다음 작업도 수행해야 합니다.

  - 새 URL의 FQDN이 유효한 PSN(정책 서비스 노드) 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. 스폰서 포털에 대해 **Allow Kerberos SSO(Kerberos SSO** 허용**)** 옵션이 활성화된 경우 Cisco ISE PSN의 FQDN 또는 와일드카드를 포털에서 사용하는 로컬 서버 인증서의 SAN 특성에 포함해야 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.

로그인 페이지 설정

- **Maximum Failed Login Attempts Before Rate Limiting(**속도 제한 전의 최대 로그인 시도 실패 횟수**)**: Cisco ISE가 해당 계정 제한을 시작하기 전에 단일 브라우저 세션에서 로그인 시도 장애 횟수를 지정합니다. 이 횟수까지는 로그인을 시도해도 계정이 잠기지 않습니다. 조절된 속도는 **Time between login attempts when rate limiting(**속도 제한 시의 로그인 시도 간 시간**)**에서 구성됩니다.
- **Include an AUP(AUP** 포함**)**: 허용되는 사용 정책 창을 플로우에 추가합니다. AUP를 창에 추가하거나 다른 창으로 연결할 수 있습니다.

AUP(Acceptable Use Policy) 페이지 설정

- **Include an AUP Page(AUP** 페이지 포함**)**: 회사의 네트워크 사용 약관을 별도의 페이지에서 사용자에게 표시합니다.
- **Use Different AUP for Employees(**직원에 대해 다른 **AUP** 사용**)**: 직원에 한해 다른 AUP 및 네트워크 사용 약관을 표시합니다. 이 옵션을 선택하는 경우 **Skip AUP for employees(**직원에 대해 **AUP** 건너뛰기**)**도 함께 선택할 수는 없습니다.

- **Skip AUP for Employees(**직원에 대해 **AUP** 건너뛰기**)**: 직원들이 네트워크에 액세스하기 전에 AUP를 수락할 필요가 없습니다. 이 옵션을 선택하는 경우 **Use different AUP for employees(**직원에 대해 다른 **AUP** 사용**)**도 함께 선택할 수는 없습니다.
- **Require Acceptance(**수락 필요**)**: 직원이 AUP를 수락해야 계정이 완전히 활성화되도록 지정합니다. 사용자가 AUP를 수락하지 않으면 **Login(**로그인**)** 버튼은 활성화되지 않습니다. AUP를 수락하지 않는 게스트에게는 네트워크 액세스 권한이 제공되지 않습니다.
- **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. AUP가 사용자에게 표시되는 시점을 구성합니다.

  - **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**)**: 용자가 네트워크 또는 포털에 처음 로그인한 후 해당 기간마다 정기적으로 AUP를 표시합니다.

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 결합형 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.

MDM 포털의 직원 모바일 디바이스 관리 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **MDM Portals(MDM** 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 흐름 설정**)** > **Employee Mobile Device Management Settings(**직원 모바일 디바이스 관리 설정**)**입니다.

다음과 같은 설정을 사용하여 MDM 포털을 사용하는 직원에 대해 MDM(Mobile Device Managemen) 기능을 활성화하고 해당 AUP 환경을 정의합니다.

필드 이름	사용 지침
Include an AUP(AUP 포함**)(**페이지에/링크로**)**	회사의 네트워크 사용 약관을 사용자에 대해 현재 표시되어 있는 창에 텍스트로 표시하거나, AUP 텍스트가 포함된 새 탭 또는 창을 여는 링크로 표시합니다.
Require Acceptance(수락 필요**)**	직원이 AUP를 수락해야 계정이 완전히 활성화되도록 지정합니다. 사용자가 AUP를 수락하지 않으면 **Login(**로그인**)** 버튼은 활성화되지 않습니다. AUP를 수락하지 않는 게스트에게는 네트워크 액세스 권한이 제공되지 않습니다.
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.

내 디바이스 포털의 포털 설정

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

- **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 창에서 설정을 변경할 때까지 해당 값이 적용됩니다. 이 창을 변경하는 경우에는 이 제한을 준수하도록 포트 설정을 업데이트해야 합니다.

  내 디바이스 등의 게스트 포털이 아닌 포털에서 사용하는 포트를 게스트 포털에 할당하면 오류 메시지가 표시됩니다.

  포스처 평가 및 교정에 한해 클라이언트 프로비저닝 포털은 포트 8905 및 8909도 사용하며, 그 외의 경우에는 게스트 포털에 할당된 것과 같은 포털을 사용합니다.

  동일한 HTTPS 포트에 할당된 포털은 같은 기가비트 인터페이스 또는 다른 인터페이스를 사용할 수 있습니다. 동일한 포트 및 인터페이스 조합을 사용하는 포털은 동일한 인증서 그룹 태그를 사용해야 합니다. 예를 들면 다음과 같습니다.

  - 스폰서 포털을 예로 들 때 유효한 조합은 다음을 포함합니다.
    - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 태그 **A**/내 디바이스 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**
    - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**/내 디바이스 포털: 포트 **8445**, 인터페이스 **0**, 인증서 그룹 **B**
    - 스폰서 포털: 포트 **8444**, 인터페이스 **1**, 인증서 그룹 **A**/차단 목록 포털: 포트 **8444**, 인터페이스 **0**, 인증서 그룹 **B**
  - 잘못된 조합은 다음과 같습니다.
    - 스폰서 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **A**/내 디바이스 포털: 포트 **8443**, 인터페이스 **0**, 인증서 그룹 **B**
    - 스폰서 포털: 포트 **8444**, 인터페이스 **0**, 인증서 태그 **A**/차단 목록 포털: 포트 **8444**, 인터페이스 **0**, 인증서 그룹 **A**

참고 최상의 성능을 위해서는 게스트 서비스에 인터페이스 0을 사용하는 것이 좋습니다. **Portal Settings(**포털 설정**)**에서 인터페이스 0만 구성하거나 CLI 명령 **ip host**를 사용하여 호스트 이름 또는 FQDN을 인터페이스 0의 IP 주소에 매핑 할 수 있습니다.

- **Allowed Interfaces(**허용된 인터페이스**)**: PAN이 포털을 실행하는 데 사용할 수 있는 PSN 인터페이스를 선택합니다. PAN에서 포털 열기 요청이 수행되면 PAN은 PSN에서 사용 가능한 허용된 포트를 찾습니다. 다른 서브넷의 IP 주소를 사용하여 이더넷 인터페이스를 구성해야 합니다.

  이러한 인터페이스는 정책 서비스가 설정된 VM 기반 PSN을 포함하여 모든 PSN에서 사용할 수 있어야 합니다. 이 요건이 적용되는 이유는 게스트 세션 시작 시 리디렉션에 이러한 PSN을 사용할 수 있기 때문입니다.

  - 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 IP 주소를 확인해야 합니다.
  - 보조 인터페이스 IP 주소를 FQDN에 매핑하려면 Cisco ISE CLI에서 **ip host x.x.x.x yyy.domain.com**을 구성합니다. 이 항목은 인증서 주체 이름 또는 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. PSN은 물리적 인터페이스에서 포털을 시작하려고 시도하지 않습니다.
  - NIC 팀 또는 결합은 컨피그레이션 옵션으로, 이를 통해 고가용성(내결함성)을 위해 개별 NIC 2개를 구성할 수 있습니다. NIC 중 하나에서 장애가 발생하면 결합형 연결의 일부분인 다른 NIC가 연결을 계속 진행합니다. NIC는 **Portal Settings(**포털 설정**)** 컨피그레이션에 기반하여 포털에 대해 선택됩니다. 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 인증서를 지정하는 인증서 그룹 태그를 선택합니다.

- **Fully Qualified Domain Name (FQDN)(FQDN(**정규화된 도메인 이름**))** - 스폰서 또는 내 디바이스 포털에 대해 고유한 FQDN 및/또는 호스트 이름을 하나 이상 입력합니다. 예를 들어 **`sponsorportal.yourcompany.com,sponsor`**를 입력할 수 있습니다. 그러면 사용자가 브라우저에 해당 이름 중 하나를 입력하면 스폰서 포털이 표시됩니다. 이름은 쉼표로 구분하되 엔트리 사이에 공백은 포함하지 마십시오.

  기본 FQDN를 변경하는 경우 다음 작업도 수행해야 합니다.

  - 새 URL의 FQDN이 유효한 PSN(정책 서비스 노드) 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. 스폰서 포털에 대해 **Allow Kerberos SSO(Kerberos SSO** 허용**)** 옵션이 활성화된 경우 Cisco ISE PSN의 FQDN 또는 와일드카드를 포털에서 사용하는 로컬 서버 인증서의 SAN 특성에 포함해야 합니다.

- **Authentication Method(**인증 방법**)**: 사용자 인증에 사용할 ID 소스 시퀀스 또는 IdP(ID 제공자)를 선택합니다. ID 소스 시퀀스는 사용자 자격 증명을 확인하기 위해 순서대로 검색되는 ID 저장소 목록입니다.

  Cisco ISE에는 스폰서 포털용 기본 ID 소스 시퀀스인 Sponsor_Portal_Sequence가 포함되어 있습니다.

  IdP를 구성하려면 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **SAML Id Providers(SAML ID** 제공자**)**를 선택합니다.

  ID 소스 시퀀스를 구성하려면 **Administration(**관리**) > Identity Management(ID** 관리**) > Identity Source Sequences(ID** 소스 시퀀스**)**를 선택합니다.

- **Endpoint Identity Group(**엔드포인트 **ID** 그룹**)**: 게스트 디바이스를 추적하기 위한 엔드포인트 ID 그룹을 선택합니다. Cisco ISE는 기본값으로 사용할 **GuestEndpoints** 엔드포인트 ID 그룹을 제공합니다. 기본값을 사용하지 않으려는 경우에는 엔드포인트 ID 그룹을 추가로 생성할 수도 있습니다.

  직원 디바이스를 추적하기 위한 엔드포인트 ID 그룹을 선택합니다. Cisco ISE는 기본값으로 사용할 **RegisteredDevices** 엔드포인트 ID 그룹을 제공합니다. 기본값을 사용하지 않으려는 경우에는 엔드포인트 ID 그룹을 추가로 생성할 수도 있습니다.

- **Purge Endpoints in this Identity Group when they Reach __ Days(__**일 후 이 **ID** 그룹의 엔드포인트 비우기**)**: 기간(일)을 지정하면 이 기간 이후에 Cisco ISE 데이터베이스에서 디바이스가 비워집니다. 비우기는 매일 수행되며 비우기 활동은 전체 비우기 타이밍과 동기화됩니다. 변경 사항은 이 엔드포인트 ID 그룹에 대해 전역적으로 적용됩니다.

  다른 정책 조건에 따라 엔드포인트 비우기 정책이 변경되는 경우에는 이 설정을 더 이상 사용할 수 없습니다.

- **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.

- **Display Language(**표시 언어**)**

  - **Use Browser Local(**브라우저 로캘 사용**)**: 클라이언트 브라우저의 로캘 설정에 지정된 언어를 포털의 표시 언어로 사용합니다. 브라우저 로캘의 언어가 Cisco ISE에서 지원되지 않는 경우 **Fallback Language(**대체 언어**)**가 언어 포털로 사용됩니다.

  - **Fallback Language(**대체 언어**)**: 브라우저 로캘에서 언어를 가져올 수 없거나 Cisco ISE에서 브라우저 로캘 언어를 지원하지 않는 경우 사용할 언어를 선택합니다.

  - **Always Use(**항상 사용**)**: 포털에 사용할 표시 언어를 선택합니다. 이 설정은 **User Browser Locale(**사용자 브라우저 로캘**)** 옵션을 재정의합니다.

내 디바이스 포털용 로그인 페이지 설정

- **Maximum Failed Login Attempts Before Rate Limiting(**속도 제한 전의 최대 로그인 시도 실패 횟수**)**: Cisco ISE가 해당 계정 제한을 시작하기 전에 단일 브라우저 세션에서 로그인 시도 장애 횟수를 지정합니다. 이 횟수까지는 로그인을 시도해도 계정이 잠기지 않습니다. 조절된 속도는 **Time between login attempts when rate limiting(**속도 제한 시의 로그인 시도 간 시간**)**에서 구성됩니다.
- **Maximum Failed Login Attempts Before Rate Limiting(**속도 제한 전의 최대 로그인 시도 실패 횟수**)**: Cisco ISE가 해당 계정 제한을 시작하기 전에 단일 브라우저 세션에서 로그인 시도 장애 횟수를 지정합니다. 이 횟수까지는 로그인을 시도해도 계정이 잠기지 않습니다. 조절된 속도는 **Time between login attempts when rate limiting(**속도 제한 시의 로그인 시도 간 시간**)**에서 구성됩니다.
- **Include an AUP(AUP** 포함**)**: 허용되는 사용 정책 창을 플로우에 추가합니다. AUP를 창에 추가하거나 다른 창으로 연결할 수 있습니다.

내 디바이스 포털의 허용되는 사용 정책 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **My Devices Portals(**내 디바이스 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Acceptable Use Policy (AUP) Page Settings(AUP** 페이지 설정**)**입니다.

다음과 같은 설정을 사용하여 사용자(게스트, 스폰서 또는 직원 중 해당하는 사용자)의 AUP 경험을 정의합니다.

필드	사용 지침
Include an AUP Page(AUP 페이지 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 때만 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 해당 기간마다 정기적으로 AUP를 표시합니다.

내 디바이스 포털용 로그인 후 배너 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **My Devices Portals(**내 디바이스 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는

복제) > **Portal Behavior and Flow Settings(**포털 동작 및 흐름 설정**)** > **Post-Login Banner Page Settings(**로그인 후 배너 페이지 설정**)**입니다.

다음과 같은 설정을 사용하여 사용자(게스트, 스폰서 또는 직원 중 해당하는 사용자)가 정상적으로 로그인한 후 추가 정보에 대한 알림을 표시합니다.

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

내 디바이스 포털용 직원 비밀번호 변경 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **My Devices Portals(**내 디바이스 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Employee Change Password Settings(**직원 비밀번호 변경 설정**)**입니다. 다음과 같은 설정을 사용하여 내 디바이스 포털을 사용 중인 직원에 대한 비밀번호 요건을 정의합니다.

직원 비밀번호 정책을 설정하려면 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Username Password Policy(**사용자 이름 비밀번호 정책**)**를 선택합니다.

필드 이름	사용 지침
Allow internal users to change password(내부 사용자의 비밀번호 변경 허용**)**	직원이 내 디바이스(My Device) 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.

내 디바이스 포털의 디바이스 관리 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **My Devices Portals(**내 디바이스 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Manage Devices(**디바이스 관리**)**입니다.

Page Customizations(페이지 사용자 맞춤화**)**에서 내 디바이스 포털의 **Manage Accounts(**계정 관리**)** 탭에 나타나는 메시지, 제목, 내용, 지침 및 필드/버튼 레이블을 사용자 맞춤화할 수 있습니다.

Settings(설정**)**에서는 이 포털을 사용하는 직원들이 등록된 개인 디바이스에서 수행할 수 있는 작업을 지정할 수 있습니다.

표 ***18:*** 내 디바이스 포털의 디바이스 관리 설정

필드 이름	사용 지침
Lost(분실**)**	직원들이 디바이스를 분실했음을 표시할 수 있습니다. 이 작업을 수행하면 내 디바이스 포털에서 디바이스 상태가 Lost(분실)로 업데이트되며 디바이스가 차단 목록 엔드포인트 ID 그룹에 추가됩니다.
Reinstate(복구**)**	이 작업을 수행하면 차단 목록에 추가되었거나 분실했거나 도난당한 디바이스가 복구되며 해당 상태가 마지막으로 확인된 값으로 재설정됩니다. 도난당한 디바이스의 상태는 등록되지 않음으로 재설정됩니다. 도난당한 디바이스는 추가 프로비저닝을 수행해야 네트워크에 연결할 수 있기 때문입니다. 차단 목록에 추가된 디바이스를 직원들이 복구하지 못하도록 하려면 내 디바이스 포털에서 이 옵션을 활성화하지 마십시오.
Delete(삭제**)**	등록된 디바이스의 최대 수에 도달하면 직원들이 내 디바이스 포털에서 등록된 디바이스를 삭제하거나 사용하지 않는 디바이스를 삭제하고 새 디바이스를 추가할 수 있도록 합니다. 이 작업을 수행하면 내 디바이스 포털에 표시된 목록에서 디바이스가 제거되지만, 해당 디바이스는 Cisco ISE 데이터베이스에 계속 남아 있으며 엔드포인트 목록에 계속 나열됩니다. 직원들이 BYOD 또는 내 디바이스 포털을 사용하여 등록할 수 있는 개인 디바이스의 최대 수를 정의하려면 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Settings(**설정**)** > **Employee Registered Devices(**직원 등록 디바이스**)**를 선택합니다. Cisco ISE 데이터베이스에서 디바이스를 영구적으로 삭제하려면 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**를 선택합니다.
Stolen(도난**)**	직원들이 디바이스를 도난당했음을 표시할 수 있습니다. 이 작업을 수행하면 내 디바이스 포털에서 디바이스 상태가 Stolen(도난)으로 업데이트되고 디바이스가 차단 목록 엔드포인트 ID 그룹에 추가되며 해당 인증서가 제거됩니다.
Device lock(디바이스 잠금**)**	MDM에 등록된 디바이스에 한해서만 적용됩니다. 직원들이 디바이스를 분실하거나 도난당한 경우 내 디바이스 포털에서 원격으로 디바이스를 즉시 잠글 수 있도록 합니다. 이 작업을 수행하면 디바이스를 무단으로 사용할 수 없게 됩니다. 그러나 PIN은 내 디바이스 포털에서 설정할 수 없으므로 직원이 모바일 디바이스에서 미리 구성해 두어야 합니다.

필드 이름	사용 지침
Unenroll(등록 취소**)**	MDM에 등록된 디바이스에 한해서만 적용됩니다. 직원들이 회사에서 디바이스를 더 이상 사용할 필요가 없는 경우 이 옵션을 선택할 수 있습니다. 이 작업을 수행하면 회사에서 설치한 애플리케이션 및 설정만 제거되고 직원의 모바일 디바이스에 포함된 기타 앱 및 데이터는 유지됩니다.
Full wipe(완전 삭제**)**	MDM에 등록된 디바이스에 한해서만 적용됩니다. 직원들이 디바이스를 분실했거나 새 디바이스로 교체하는 경우 이 옵션을 선택할 수 있습니다. 이 작업을 수행하면 직원 모바일 디바이스가 기본 초기 설정으로 재설정되며 설치된 앱과 데이터가 제거됩니다.

내 디바이스 포털의 디바이스 맞춤화 추가, 편집 및 찾기

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **My Devices Portals(**내 디바이스 포털**)** > **Create, Edit or Duplicate(**생성, 편집 또는 복제**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Add Devices, Edit Devices or Locate Devices(**디바이스 추가, 편집 또는 찾기**)**입니다.

Page Customizations(페이지 사용자 맞춤화**)**에서 내 디바이스 포털의 Add(추가), Edit(편집) 및 Locate(찾기) 탭에 나타나는 메시지, 제목, 내용, 지침 및 필드/버튼 레이블을 사용자 맞춤화할 수 있습니다.

디바이스 포털용 지원 정보 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **BYOD Portals, Client Provisioning Portals, MDM Portals, or My Devices Portals(BYOD** 포털, 클라이언트 프로비저닝 포털, **MDM** 포털 또는 내 디바이스 포털**)** > **Create, Edit, or Duplicate(**생성, 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Support Information Page Settings(**지원 정보 페이지 설정**)**입니다.

다음과 같은 설정을 사용하여 헬프 데스크에서 사용자(게스트, 스폰서 또는 직원 중 해당하는 사용자)에게 발생한 액세스 문제를 해결하는 데 사용할 수 있는 정보를 표시합니다.

필드 이름	사용 지침
Include a Support Information Page(지원 정보 페이지 포함**)**	포털에 대해 활성화된 모든 창에 **Contact Us(Cisco**에 문의**)** 등의 정보 창 링크를 표시합니다.
MAC Address(MAC 주소**)**	지원 정보 창에 디바이스의 MAC 주소를 기재합니다.
IP Address(IP 주소**)**	지원 정보 창에 디바이스의 IP 주소를 기재합니다.
Browser User Agent(브라우저 사용자 에이전트**)**	지원 정보 창에 요청을 시작한 사용자 에이전트의 버전, 레이아웃 엔진 및 제품 이름/버전과 같은 브라우저 세부정보를 기재합니다.

필드 이름	사용 지침
Policy Server(정책 서버**)**	지원 정보 창에 이 포털에 서비스를 제공하는 ISE PSN(정책 서비스 노드)의 IP 주소를 기재합니다.
Failure Code(장애 코드**)**	사용 가능한 경우 로그 메시지 카탈로그의 해당 번호를 기재합니다. 메시지 카탈로그를 보려면 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Message Catalog(**메시지 카탈로그**)**를 선택합니다.
Hide Field(필드 숨기기**)**	포함되어 있어야 하는 정보가 없는 경우 지원 정보 창의 필드 레이블을 표시하지 않습니다. 예를 들어 장애 코드가 확인할 수 없는 상태여서 비어 있으면 **Failure Code(**장애 코드**)**가 선택되어 있더라도 장애 코드를 표시하지 않습니다.
Display Label with no Value(값 없이 레이블 표시**)**	포함되어 있어야 하는 정보가 없더라도 지원 정보 창에서 선택한 모든 필드 레이블을 표시합니다. 예를 들어 장애 코드가 확인할 수 없는 상태여서 비어 있어도 **Failure Code(**장애 코드**)**를 표시하지 않습니다.
Display Label with Default Value(기본값으로 레이블 표시**)**	포함되어 있어야 하는 정보가 없는 경우 지원 정보 창에서 선택한 필드 레이블에 이 텍스트를 표시합니다. 예를 들어 이 필드에 사용할 수 없음을 입력하는 경우 장애 코드를 확인할 수 없으면 **Failure Code(**장애 코드**)** 필드가 **Not Available(**사용할 수 없음**)**로 표시됩니다.