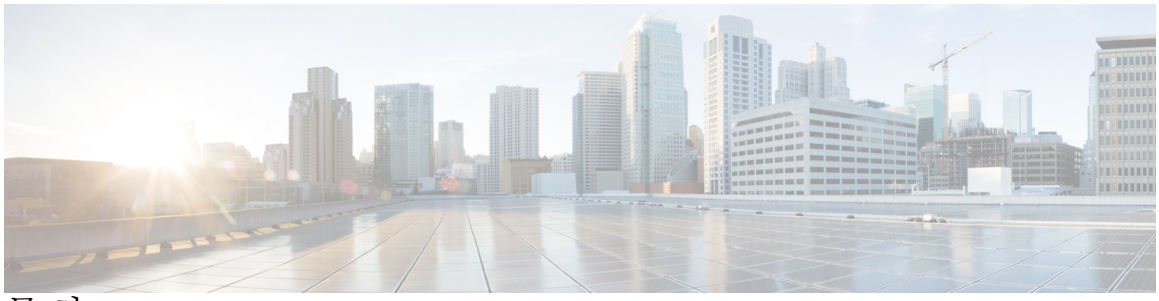
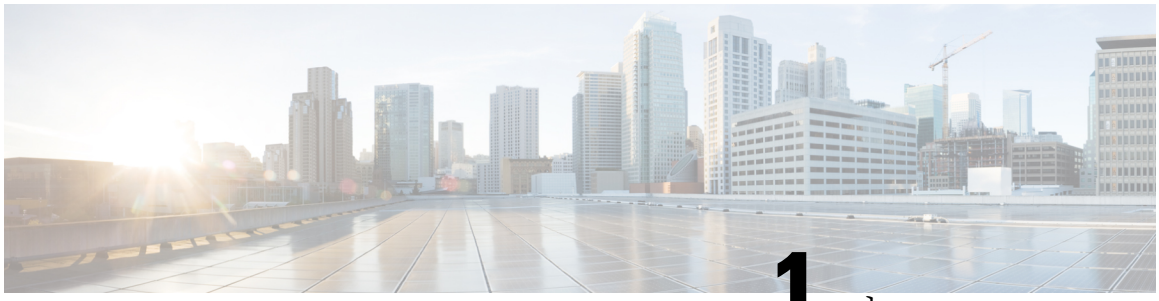
Cisco ID 서비스 엔진 관리자 설명서, 릴리스 3.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

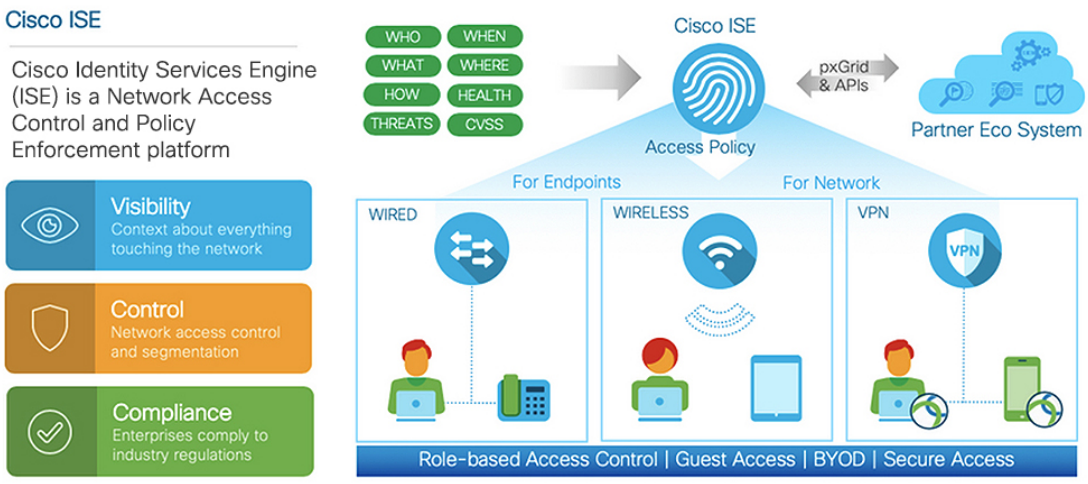


1 장

개요

참고 이 제품에 대한 문서 세트는 편견 없는 언어를 사용하기 위해 노력합니다. 이 설명서 세트의 목적상, 편향이 없는 언어는 나이, 장애, 성별, 인종 정체성, 민족 정체성, 성적 지향성, 사회 경제적 지위 및 교차성에 기초한 차별을 의미하지 않는 언어로 정의됩니다. 제품 소프트웨어의 사용자 인터페이스에서 하드코딩된 언어, RFP 설명서에 기초한 언어 또는 참조된 타사 제품에서 사용하는 언어로 인해 설명서에 예외가 있을 수 있습니다.

Cisco ISE 개요



Cisco ISE(Identity Services Engine)는 ID 기반 네트워크 액세스 제어 및 정책 시행 시스템입니다. 이는 기업의 엔드포인트 액세스 제어 및 네트워크 디바이스 관리를 지원하는 공통 정책 엔진으로 작동합니다.

Cisco ISE를 활용하면 규정 준수를 유지하고 인프라의 보안을 향상하며 서비스 운영을 간소화할 수 있습니다.

Cisco ISE 관리자는 사용자 및 사용자 그룹(누가?), 디바이스 유형(무엇을?), 액세스 시간(언제?), 액세스 위치(어디서?), 액세스 유형(유선, 무선 또는 VPN)(어떻게?), 네트워크 위협 및 취약점을 비롯하여 네트워크에 대한 실시간 상황 데이터를 수집할 수 있습니다.

Cisco ISE 관리자는 이 정보를 사용하여 네트워크 거버넌스(Governance) 의사 결정을 내릴 수 있습니다. 또한 ID 데이터를 다양한 네트워크 요소에 연결하여 네트워크 액세스 및 사용을 제어하는 정책을 생성할 수 있습니다.

Cisco ISE의 기능

Cisco ISE 소프트웨어는 있는 그대로 설치해야 합니다. 기본 운영 체제 레벨에서는 다른 타사 애플리케이션을 설치할 수 없습니다.

Cisco ISE는 다음과 같은 기능을 제공합니다.

- 디바이스 관리: Cisco ISE는 TACACS+ 보안 프로토콜을 사용하여 네트워크 디바이스의 컨피그레이션을 제어하고 감사합니다. 따라서 어떤 사용자가 어떤 네트워크 디바이스에 액세스하고 관련 네트워크 설정을 변경할 수 있는지를 세분화된 방식으로 제어할 수 있습니다. Cisco ISE에서 디바이스 관리자 작업의 인증 및 권한 부여를 쿼리하도록 네트워크 디바이스를 구성할 수 있습니다. 이러한 디바이스는 Cisco ISE에 계정 관리 메시지를 보내 관련 작업을 로깅합니다.
- 게스트 및 보안 무선: Cisco ISE를 사용하면 방문자, 계약업체, 컨설턴트 및 고객에게 보안 네트워크 액세스를 제공할 수 있습니다. 웹 기반 및 모바일 포털을 사용하여 게스트를 회사 네트워크 및 내부 리소스에 온보딩할 수 있습니다. 다양한 게스트 유형에 대한 액세스 권한을 정의하고, 게스트 계정을 생성하고 관리할 스폰서를 할당할 수 있습니다.
- **BYOD(Bring Your Own Device)**: Cisco ISE를 사용하면 직원과 게스트가 엔터프라이즈 네트워크에서 안전하게 개인 디바이스를 사용할 수 있습니다. BYOD 기능 최종 사용자는 구성된 경로를 사용하여 디바이스를 추가하고 미리 정의된 인증 및 네트워크 액세스 레벨을 프로비저닝할 수 있습니다.
- 자산 가시성: Cisco ISE는 무선, 유선 및 VPN 연결을 통해 네트워크에 있는 사람과 대상을 일관적으로 파악하고 제어할 수 있습니다. Cisco ISE는 프로브 및 디바이스 센서를 사용하여 디바이스가 네트워크에 연결되는 방식을 수신합니다. 그런 다음 광범위한 Cisco ISE 프로파일 데이터베이스가 디바이스를 분류합니다. 이를 통해 적절한 수준의 네트워크 액세스 권한을 부여하는 데 필요한 가시성과 상황 정보가 제공됩니다.
- 보안 유선 액세스: Cisco ISE는 광범위한 인증 프로토콜을 사용하여 네트워크 디바이스 및 엔드포인트에 보안 유선 네트워크 액세스를 제공합니다. 여기에는 802.1X, RADIUS, MAB, 웹 기반, EasyConnect 및 외부 에이전트 지원 인증 방법이 포함되며 이에 국한되지는 않습니다.

- 세분화: Cisco ISE는 네트워크 디바이스 및 엔드포인트에 대한 상황 데이터를 사용하여 네트워크 세분화를 지원합니다. 보안 그룹 태그, 액세스 제어 목록, 네트워크 액세스 프로토콜, 권한 부여와 액세스 및 인증을 정의하는 정책 집합으로, Cisco ISE는 안전하게 네트워크를 세분화할 수 있습니다.
- 포스처 또는 규정 준수: Cisco ISE에서는 네트워크에 연결하기 전에 엔드포인트의 규정 준수(포스처라고도 함)를 확인할 수 있습니다. 엔드포인트가 포스처 서비스에 적합한 포스처 에이전트를 수신하도록 할 수 있습니다.
- 위협 억제: Cisco ISE가 엔드포인트에서 위협이 되거나 취약한 속성을 탐지하는 경우 적응형 네트워크 제어 정책이 전송되어 엔드포인트의 액세스 레벨을 동적으로 변경합니다. 위협 또는 취약점을 평가하고 해결하면 엔드포인트에 원래 액세스 정책이 다시 적용됩니다.
- 보안 에코시스템 통합: pxGrid 기능을 통해 Cisco ISE는 연결된 네트워크 디바이스, 타사 벤더 또는 Cisco 파트너 시스템과 상황에 맞는 정보, 정책 및 컨피그레이션 데이터 등을 안전하게 공유할 수 있습니다.

Cisco ISE 관리자

관리자는 관리 포털을 사용하여 다음을 수행할 수 있습니다.

- 구축, 헬프 데스크 작업, 네트워크 디바이스 및 노드 모니터링, 문제 해결을 관리합니다.
- Cisco ISE 서비스, 정책, 관리자 계정 및 시스템 컨피그레이션 및 작업을 관리합니다.
- 관리자 및 사용자 비밀번호를 변경합니다.

CLI 관리자는 Cisco ISE 애플리케이션을 시작 및 중지하고, 소프트웨어 패치를 적용하고, Cisco ISE 어플라이언스를 업그레이드, 다시 로드 또는 종료하고, 모든 시스템 및 애플리케이션 로그를 볼 수 있습니다. CLI 관리자에게는 특수 권한이 부여되므로 Cisco ISE 구축을 구성하고 관리하기 위해서는 CLI 관리자 자격 증명을 보호하고 웹 기반 관리자를 생성하는 것이 좋습니다.

설치 중에 구성하는 사용자 이름 및 비밀번호는 CLI에 대한 관리 액세스 용도로만 사용됩니다. 이 역할은 CLI 관리자라고도 하는 CLI 관리 사용자로 간주됩니다. 기본적으로 CLI 관리 사용자의 사용자 이름은 admin이고 비밀번호는 설치 과정에서 정의됩니다. 비밀번호는 기본값이 없습니다. 이 CLI 관리 사용자는 기본 관리 사용자이며 이 사용자 계정은 삭제할 수 없습니다. 그러나 다른 관리자는 해당 계정에 대한 비밀번호를 활성화, 비활성화 또는 변경하는 옵션을 포함하여 해당 계정을 편집할 수 있습니다.

관리자를 만들 수도 있고 기존 사용자를 관리자 역할로 승격시킬 수도 있습니다. 또한 해당 관리 권한을 비활성화하여 관리자를 단순 네트워크 사용자 상태로 강등시킬 수도 있습니다.

관리자는 컨피그레이션에 대한 로컬 권한이 있으며 Cisco ISE 시스템을 운영하는 사용자입니다.

관리자는 하나 이상의 관리 그룹에 할당됩니다.

관련 항목

Cisco ISE 관리자 그룹, 6 페이지

CLI 관리자의 외부 ID 저장소 사용 강제 적용

외부 ID 소스를 사용한 인증은 내부 데이터베이스를 사용하는 것보다 더 안전합니다. CLI 관리자의 RBAC(역할 기반 액세스 제어)는 외부 ID 저장소를 지원합니다.

사전 요건

관리자를 정의하고 관리자 그룹에 추가해야 합니다. 관리자는 슈퍼 관리자여야 합니다.

Active Directory 사용자 디렉토리에 사용자 속성 정의

Active Directory를 실행하는 Windows 서버를 사용하여 CLI 관리자로 구성하려는 각 사용자의 속성을 수정합니다.

1. Server Manager(서버 관리자) 창에서 **Server Manager(**서버 관리자**)** > **Roles(**역할**)** > **Active Directory Domain Services(Active Directory** 도메인 서비스**)** > **Active Directory Users and Computers(Active Directory** 사용자 및 컴퓨터**) > [ad.adserver] <*ad_server*>.local**을 선택합니다.
2. 사용자 속성을 편집할 수 있도록 **View(**보기**)** 메뉴에서 **Advanced Features(**고급 기능**)**를 활성화합니다.
3. 모든 관리자 사용자 목록이 포함된 Active Directory 그룹으로 이동하여 해당 사용자를 선택합니다.
4. 사용자를 두 번 클릭하여 **Properties(**속성**)** 창을 엽니다.
5. **Attribute Editor(**속성 편집기**)**를 선택합니다.
6. 임의의 속성을 클릭하고 "gid"를 입력하여 *gidNumber*를 찾습니다. gidNumber 속성을 찾을 수 없는 경우 **Filter(**필터**)** 버튼을 클릭하고 **Show only attributes that have values(**값이 있는 속성만 표시**)**의 선택을 취소합니다.
7. 각 속성을 편집하려면 해당 속성 이름을 두 번 클릭합니다. 각 사용자에 대해 다음을 수행합니다.
   - 60000보다 큰 *uidNumber*를 할당하고 숫자가 고유한지 확인합니다. 할당 후에는 uidNumber를 변경하지 마십시오.
   - *gidNumber*를 110 또는 111로 할당합니다. 110은 관리자 사용자를 나타내고 111은 읽기 전용 사용자를 나타냅니다. gidNumber를 수정하는 경우 SSH 연결을 수행하기 전에 5분 이상 기다립니다.

Active Directory 도메인에 관리자 CLI 사용자 가입

Cisco ISE CLI에 연결하고 **identity-store** 명령을 실행 한 다음 ID 저장소에 관리자 사용자를 할당합니다. 예를 들어 CLI 관리자 사용자를 ISE에 adpool1로 정의된 Active Directory에 매핑하려면 **identity-store active-directory domain-name adpool1 user admincliuser** 명령을 실행합니다.

가입이 완료되면 Cisco ISE CLI에 연결하고 관리자 CLI 사용자로 로그인하여 컨피그레이션을 확인합니다.

이 명령에서 사용하는 도메인이 이전에 ISE 노드에 연결되었던 경우 관리자 콘솔에서 도메인에 다시 가입해야 합니다.

1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Identity Management(ID** 관리**) > External Identity Sources(**외부 **ID** 소스**)**로 이동합니다.
2. 왼쪽 창에서 **Active Directory**를 클릭하고 Active Directory 이름을 선택합니다.

참고 MS-RPC 또는 Kerberos를 사용하여 테스트 사용자와의 연결을 테스트하는 경우 Active Directory 연결의 상태가 **Operational(**운영**)**로 표시될 수 있지만 오류 메시지가 표시됩니다.

3. Cisco ISE CLI에 여전히 관리자 CLI 사용자로 로그인 할 수 있는지 확인합니다.

새 관리자 생성

Cisco ISE 관리자에게는 특정 관리 작업을 수행하기 위한 특정 역할이 할당된 계정이 있어야 합니다. 여러 관리자 계정을 생성하고 이러한 관리자가 수행해야 하는 관리 작업을 기준으로 해당 관리자에게 하나 이상의 역할을 할당할 수 있습니다.

Admin Users(관리자 사용자**)** 창을 사용하여 Cisco ISE 관리자의 특성에 대해 확인/생성/수정/삭제/상태 변경/복제/검색을 수행합니다.

참고 관리자 사용자의 도메인이 CLI와 GUI에서 모두 동일할 경우 GUI에 가입하기 전에 Active Directory 액세스를 먼저 구성하는 것이 좋습니다. 그러지 않을 경우, GUI에서 도메인에 다시 가입해야 해당 도메인에 대한 인증 실패를 방지할 수 있습니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Users(**관리자 사용자**)** > **Add(**추가**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Users(**관리자 사용자**)** > **Add(**추가**)**

단계 **3** **Add(**추가**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 관리자 사용자 생성

  Create an Admin User(관리자 사용자 생성**)**를 선택하면 새 관리자 사용자에 대한 계정 정보를 구성할 수 있는 **New Administrator(**새 관리자**)** 창이 나타납니다.

- **Select from Network Access Users(**네트워크 액세스 사용자 중에서 선택**)**

  Select from Network Access Users(네트워크 액세스 사용자 중에서 선택**)**를 선택하면 현재 사용자 목록이 나타납니다. 이 목록에서 사용자를 클릭하여 선택할 수 있습니다. 그러면, 이 사용자에 해당하는 **Admin User(**관리자 사용자**)** 창이 나타납니다.

단계 **4** 필드에 값을 입력합니다. **Name(**이름**)** 필드에 입력할 수 있는 문자는 # $ ' ( ) * + - 입니다. / @ _ 입니다.

관리자 이름은 고유해야 합니다. 이미 존재하는 사용자 이름을 입력한 경우 오류 팝업 창에 다음 메시지가 표시됩니다.

```
User can't be created. A User with that name already exists.
```

단계 **5** **Submit(**제출**)**을 클릭하여 Cisco ISE 내부 데이터베이스에 새 관리자를 생성합니다.

관련 항목

읽기 전용 관리 정책, 22 페이지
읽기 전용 관리자를 위한 메뉴 액세스 사용자 맞춤화, 22 페이지

Cisco ISE 관리자 그룹

관리자 그룹은 Cisco ISE의 RBAC(Role-based Access Control) 그룹입니다. 같은 그룹에 속하는 모든 관리자는 공통 ID를 공유하고 동일한 권한을 갖습니다. 특정 관리 그룹의 멤버인 관리자의 ID는 권한 부여 정책에서 조건으로 사용될 수 있습니다. 한 관리자는 여러 관리자 그룹에 속할 수 있습니다.

모든 액세스 수준을 가진 관리자 계정을 사용하여 액세스할 수 있는 창에서 권한을 가진 개체를 수정하거나 삭제할 수 있습니다.

Cisco ISE 보안 모델에서 관리자는 자신이 가진 것과 동일한 권한 집합을 포함하는 관리 그룹만 생성할 수 있습니다. 부여된 권한은 Cisco ISE 데이터베이스에 정의된 사용자의 관리 역할에 따라 달라집니다. 이런 방식으로 관리 그룹은 Cisco ISE 시스템에 액세스하기 위한 권한을 정의하는 기준을 형성합니다.

다음 표에는 Cisco ISE에 미리 정의된 관리자 그룹과 함께 해당 그룹의 멤버가 수행할 수 있는 작업이 나열되어 있습니다.

표 ***1: Cisco ISE*** 관리자 그룹, 액세스 레벨, 권한 및 제한 사항

관리자 그룹 역할	액세스 레벨	권한	제한 사항
사용자 맞춤화 관리자	스폰서, 게스트 및 개인 디바이스 포털 관리	• 게스트 및 스폰서 액세스 구성 • 게스트 액세스 설정 관리 • 최종 사용자 웹 포털 사용자 맞춤화	• Cisco ISE에서 정책 관리, ID 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가 • 보고서 조회 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
헬프 데스크 관리자	쿼리 모니터링 및 문제 해결 작업	• 모든 보고서 실행 • 모든 문제 해결 플로우 실행 • Cisco ISE 대시보드 및 라이브 로그 조회 • 경보 확인	보고서, 문제 해결 플로우, 라이브 인증 또는 경보의 생성, 업데이트 또는 삭제 불가
ID 관리자	• 사용자 계정 및 엔드포인트 관리 • ID 소스 관리	• 사용자 계정 및 엔드포인트 추가, 편집 및 삭제 • ID 소스 추가, 편집 및 삭제 • ID 소스 시퀀스 추가, 편집 및 삭제 • 사용자 계정에 대한 일반 설정 구성(속성 및 비밀번호 정책) • Cisco ISE 대시보드, 라이브 로그, 경보 및 보고서 조회 • 모든 문제 해결 플로우 실행	Cisco ISE에서 정책 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가
MnT 관리자	모든 모니터링 및 문제 해결 작업 수행	• 모든 보고서 관리(실행, 생성 및 삭제) • 모든 문제 해결 플로우 실행 • Cisco ISE 대시보드 및 라이브 로그 조회 • 경보 관리(생성, 업데이트, 보기 및 삭제)	Cisco ISE에서 정책 관리, ID 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
네트워크 디바이스 관리자	Cisco ISE 네트워크 디바이스 및 네트워크 디바이스 저장소 관리	• 네트워크 디바이스에 대한 읽기 및 쓰기 권한 • 네트워크 디바이스 그룹 및 모든 네트워크 리소스 개체 유형에 대한 읽기 및 쓰기 권한 • Cisco ISE 대시보드, 라이브 로그, 경보 및 보고서 조회 • 모든 문제 해결 플로우 실행	Cisco ISE에서 정책 관리, ID 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
정책 관리자	네트워크에서 인증, 권한 부여, 포스처, 프로파일러, 클라이언트 프로비저닝 및 작업 센터와 관련된 모든 Cisco ISE 서비스에 대한 정책 생성 및 관리	• 정책에 사용되는 모든 요소(예: 권한 부여 프로파일, NDG(네트워크 디바이스 그룹) 및 조건)에 대한 읽기 및 쓰기 권한 • ID, 엔드포인트 및 ID 그룹(사용자 ID 그룹 및 엔드포인트 ID 그룹)에 대한 읽기 및 쓰기 권한 • 서비스 정책 및 설정에 대한 읽기 및 쓰기 권한 • Cisco ISE 대시보드, 라이브 로그, 경보 및 보고서 조회 • 모든 문제 해결 플로우 실행 • 디바이스 관리 - 디바이스 관리 작업 센터 액세스, TACACS 정책 조건 및 결과에 대한 권한, TACACS 프록시 및 시퀀스에 대한 네트워크 디바이스 권한	Cisco ISE에서 ID 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가 디바이스 관리 - 작업 센터에 대한 액세스는 하위 링크에 대한 액세스를 보장하지 않음

관리자 그룹 역할	액세스 레벨	권한	제한 사항
RBAC 관리자	Endpoint Protection Services(엔드포인트 보호 서비스) Adaptive Network Control(적응형 네트워크 제어)을 제외한 **Operations(**운영**)** 메뉴 아래의 모든 작업 및 **Administration(**관리**)** 아래의 일부 메뉴 항목에 대한 부분 액세스	• 인증 세부정보 조회 • Endpoint Protection Services(엔드포인트 보호 서비스) Adaptive Network Control(적응형 네트워크 제어) 활성화 또는 비활성화 • 경보 생성, 편집 및 삭제, 보고서 생성 및 조회, Cisco ISE를 사용하여 네트워크의 문제 해결 • 관리자 계정 설정 및 관리자 그룹 설정에 대한 읽기 권한 • **RBAC policy(RBAC** 정책**)** 창에서 관리자 액세스에 대한 권한을 봅니다. • Cisco ISE 대시보드, 라이브 로그, 경보 및 보고서 조회 • 모든 문제 해결 플로우 실행	Cisco ISE에서 ID 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
읽기 전용 관리자	ISE GUI에 대한 읽기 전용 액세스		

관리자 그룹 역할	액세스 레벨	권한	제한 사항
		• 데이터 필터링, 쿼리, 옵션 저장, 인쇄, 데이터 내보내기와 같은 대시보드, 보고서, 라이브 로그 또는 세션 기능 조회 및 사용 • 본인의 계정 비밀번호 변경 • 전역 검색, 보고서, 라이브 로그 또는 세션을 통한 ISE 쿼리 • 속성을 기반으로 데이터 필터링 및 저장 • 인증 정책, 프로파일 정책, 사용자, 엔드포인트, 네트워크 디바이스, 네트워크 디바이스 그룹, ID(그룹 포함) 및 기타 컨피그레이션과 관련된 데이터 내보내기 • 보고서 쿼리 맞춤 설정, 저장, 인쇄 및 내보내기 • 맞춤형 보고서 쿼리를 생성하고, 결과를 저장, 인쇄 또는 내보내기 • 추후 참조를 위해 GUI 설정 저장 • **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)** 창에서	• 권한 부여 정책, 인증 정책, 포스처 정책, 프로파일러 정책, 엔드포인트 및 사용자와 같은 개체의 생성, 업데이트, 삭제, 가져오기, 격리 및 MDM(Mobile Device Management) 작업 등 컨피그레이션 변경 수행 • 백업 및 복구, 노드 등록 또는 등록 취소, 노드 동기화, 노드 그룹 생성, 편집, 삭제, 패치 업그레이드 및 설치와 같은 시스템 작업 수행 • 정책, 네트워크 디바이스, 네트워크 디바이스 그룹, ID(그룹 포함) 및 기타 컨피그레이션과 관련된 데이터 가져오기 • CoA, 엔드포인트 디버깅, 수집 필터 수정, 라이브 세션 데이터 삭제 무시, PAN-HA 페일오버 설정 수정, Cisco ISE 노드의 페르소나 또는 서비스 편집 등의 작업 수행 • 성능에 큰 영향을 미칠 수있는 명령 실행 (예: **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** >

관리자 그룹 역할	액세스 레벨	권한	제한 사항
		ise-psc-log와 같은 로그 다운로드	**General Tools(**일반 도구**)** 창의 **TCP** 덤프에 대한 액세스 제한) • 지원 번들 생성
슈퍼 관리자	모든 Cisco ISE 관리 기능. 기본 관리자 계정이 이 그룹에 속함	모든 Cisco ISE 리소스에 대한 생성, 읽기, 업데이트, 삭제 및 실행(CRUDX) 권한 참고 슈퍼 관리 사용자는 시스템에서 생성된 기본 RBAC 정책 및 권한을 수정할 수 없습니다. 이를 위해서는 사용자 요구 사항에 따라 필요한 권한으로 새 RBAC 정책을 생성하고 해당 정책을 관리자 그룹에 매핑해야 합니다. 디바이스 관리 - 디바이스 관리 작업 센터 액세스, TACACS 정책 조건 및 결과에 대한 권한, TACACS 프록시 및 시퀀스에 대한 네트워크 디바이스 권한 및 TACACS 전역 프로토콜 설정을 활성화하는 권한	• 디바이스 관리 - 작업 센터에 대한 액세스는 하위 링크에 대한 액세스를 보장하지 않음 • 기본 슈퍼 관리자 그룹의 관리 사용자만 다른 관리 사용자를 수정 또는 삭제 가능, 슈퍼 관리자 그룹의 메뉴 및 데이터 액세스 권한으로 복제된 관리자 그룹의 일부인 외부에서 매핑된 사용자도 관리 사용자 수정 또는 삭제 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
시스템 관리자	모든 Cisco ISE 컨피그레이션 및 유지 관리 작업	**Operations(**운영**)** 탭 아래의 모든 활동을 수행할 수 있는 전체 액세스(읽기 및 쓰기 권한) 및 **Administration(**관리**)** 탭 아래의 일부 메뉴 항목에 대한 부분 액세스 • 관리자 계정 설정 및 관리자 그룹 설정에 대한 읽기 권한 • 관리자 액세스에 대한 읽기 권한 및 **RBAC policy(RBAC** 정책**)** 창과 함께 데이터 액세스 권한 • **Administration(**관리**)** > **System(**시스템**)** 아래의 모든 옵션에 대한 읽기 및 쓰기 권한 • 인증 세부정보 조회 • Endpoint Protection Services(엔드포인트 보호 서비스) Adaptive Network Control(적응형 네트워크 제어) 활성화 또는 비활성화 • 경보 생성, 편집 및 삭제, 보고서 생성 및 조회, Cisco ISE를 사용하여 네트워크의 문제 해결 • 디바이스 관리 - TACACS 전역 프로토콜 설정을 활성화하는 권한	Cisco ISE에서 정책 관리 또는 시스템 레벨 컨피그레이션 작업 수행 불가

관리자 그룹 역할	액세스 레벨	권한	제한 사항
승격 시스템 관리자 (Cisco ISE, 릴리스 2.6, 패치 2 이상에서 지원)	모든 Cisco ISE 컨피그레이션 및 유지 관리 작업	시스템 관리자의 모든 권한 외에도 승격 시스템 관리자는 관리 사용자 생성 가능	• 슈퍼 관리자 사용자 생성 또는 삭제 불가 • 슈퍼 관리자 그룹 관리 불가
ERS(External RESTful Services) 관리자	GET, POST, DELETE, PUT 등 모든 ERS API 요청에 대한 전체 액세스	• ERS API 요청 생성, 읽기, 업데이트 및 삭제	내부 사용자, ID 그룹, 엔드포인트, 엔드포인트그룹 및 SGT를 지원하는 ERS 인증 전용 역할
ERS(External RESTful Services) 운영자	ERS API에 대한 읽기 전용, GET만	• ERS API 요청 읽기만 가능	내부 사용자, ID 그룹, 엔드포인트, 엔드포인트그룹 및 SGT를 지원하는 ERS 인증 전용 역할
TACACS+ 관리자	전체 액세스 권한	액세스: • 디바이스 관리 작업 센터 • 구축 - TACACS+ 서비스 활성화용 • 외부 ID 저장소 • **Operations(운영) > TACACS Live Logs(TACACS 라이브 로그)** 창	—

관련 항목

Cisco ISE 관리자, 3 페이지

관리자 그룹 생성

Admin Groups(관리자 그룹) 창에서는 Cisco ISE 네트워크 관리자 그룹 확인/생성/수정/삭제/복제/필터링을 수행할 수 있습니다.

시작하기 전에

외부 관리자 그룹 유형을 구성하려면 하나 이상의 외부 ID 저장소가 이미 지정되어 있어야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Groups(**관리자 그룹**)**.

단계 **2** **Add(**추가**)**를 클릭하고 이름과 설명을 입력합니다.

Name(이름**)** 필드에 입력할 수 있는 특수 문자는 공백, # $ & ‘ ( ) * + - . / @ _입니다.

단계 **3** 해당 확인란을 선택하여 구성 중인 관리자 그룹 유형을 지정합니다.

- **Internal(**내부**)**: Cisco ISE 내부 데이터베이스에 저장되어 있는 자격 증명을 기준으로 하여 이 그룹 유형에 할당되는 관리자를 인증합니다.
- **External(**외부**)**: 이 그룹에 할당된 관리자는 **Administration(**관리**) > System(**시스템**) > Admin Access(**관리 액세스**) > Authentication(**인증**) > Authentication Method(**인증 방법**)** 창에서 선택하는 외부 ID 저장소에 저장된 자격 증명을 기준으로 인증합니다. 필요한 경우 외부 그룹을 지정할 수 있습니다.

참고 내부 사용자가 인증을 위해 외부 ID 저장소로 구성된 경우, ISE 관리 포털에 로그인하는 동안 내부 사용자는 외부 ID 저장소를 **ID** 소스로 선택해야 합니다. 내부 **ID** 소스를 선택하면 인증이 실패합니다.

단계 **4** **Member Users(**멤버 사용자**)** 영역에서 **Add(**추가**)**를 클릭하여 관리자 그룹에 사용자를 추가합니다. 관리자 그룹에서 사용자를 삭제하려면 삭제할 사용자에 해당하는 확인란을 선택하고 **Remove(**제거**)**를 클릭합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

Cisco ISE에 대한 관리 액세스

Cisco ISE 관리자는 자신이 속해 있는 관리 그룹에 따라 다양한 관리자 업무를 수행할 수 있습니다. 이러한 관리자 업무는 매우 중요합니다. 네트워크에서 Cisco ISE를 관리할 권한이 있는 사용자에게만 관리 액세스 권한을 부여하십시오.

Cisco ISE에서는 여기에서 설명한 옵션을 통해 웹 인터페이스에 대한 관리 액세스를 제어할 수 있습니다. .

참고 Cisco ISE 서버가 네트워크에 추가되는 경우 해당 웹 인터페이스가 작동한 후 실행 중인 상태로 표시됩니다. 그러나 포스처 서비스와 같은 일부 고급 서비스를 사용하려면 시간이 더 오래 걸릴 수 있으므로 모든 서비스가 완전히 작동하는 데 시간이 추가로 소요될 수 있습니다.

관리 액세스 방법

여러 방법으로 Cisco ISE 서버에 연결할 수 있습니다. PAN(정책 관리 노드)은 관리자 포털을 실행합니다. 로그인하려면 관리자 비밀번호가 필요합니다. 다른 ISE 페르소나 서버는 SSH 또는 CLI를 실행하는 콘솔을 통해 액세스할 수 있습니다. 이 섹션에서는 각 연결 유형에 사용 가능한 프로세스 및 비밀번호 옵션에 대해 설명합니다.

- **Admin password(관리자 비밀번호)**: 설치하는 동안 생성한 Cisco ISE 관리 사용자는 기본적으로 45일 후에 시간 초과됩니다. **Administration(관리)** > **System(시스템)** > **Admin Settings(관리자 설정)**에서 비밀번호 수명 주기를 끄는 방식으로 이를 방지할 수 있습니다. **Password Policy(비밀번호 정책)** 탭을 클릭하고 **Password Lifetime(비밀번호 수명 주기)** 아래에서 **Administrative passwords expire(관리자 비밀번호 만료)** 확인란을 선택 취소합니다.

  아니면 비밀번호가 만료되고 나서 **application reset-passwd** 명령을 실행하여 CLI에서 관리자 비밀번호를 재설정할 수 있습니다. 콘솔에 연결하여 CLI에 액세스하거나 ISE 이미지 파일을 재부팅하고 부팅 옵션 메뉴에 액세스하여 관리자 비밀번호를 재설정할 수 있습니다.

- **CLI password(CLI 비밀번호)**: 설치 중에 CLI 비밀번호를 입력해야 합니다. 잘못된 비밀번호로 인해 CLI에 로그인하는 데 문제가 있는 경우 CLI 비밀번호를 재설정할 수 있습니다. 콘솔에 연결하고 **password** CLI 명령을 실행하여 비밀번호를 재설정합니다. 자세한 내용은 Cisco Identity Services Engine CLI Reference Guide를 참고해 주십시오.

- **SSH access to the CLI(CLI에 대한 SSH 액세스)**: **service sshd** 명령을 사용하여 설치 중 또는 이후에 SSH 액세스를 활성화할 수 있습니다. SSH 연결에서 키를 사용하도록 강제할 수도 있습니다. 이 작업을 수행할 때 모든 네트워크 디바이스에 대한 SSH 연결에서도 해당 키를 사용합니다. Cisco ISE 관리 가이드: 세그멘테이션의 "SSH 키 확인 섹션을 참고하십시오. SSH 키가 Diffie-Hellman 알고리즘을 사용하도록 강제할 수 있습니다. ECDSA 키는 SSH 키에 대해 지원되지 않습니다.

Cisco ISE의 역할 기반 관리자 액세스 제어

Cisco ISE는 관리 권한을 제한하여 보안을 보장하는 RBAC(Role-based Access Control) 정책을 제공합니다. RBAC 정책은 역할 및 권한을 정의할 수 있도록 기본 관리 그룹과 연결됩니다. 표준 권한 집합(메뉴 및 데이터 액세스용)은 각각의 미리 정의된 관리 그룹과 쌍을 이루며 연결된 역할 및 작업 기능에 맞게 조정됩니다.

사용자 인터페이스의 일부 기능을 사용하려면 특정 권한이 필요합니다. 특정 기능을 사용할 수 없거나 특정 작업을 수행하도록 허용되지 않는 경우 관리 그룹에 기능을 활용하는 작업을 수행하는 데 필요한 권한이 없을 수도 있습니다.

액세스 레벨에 관계없이 모든 관리자 계정은 액세스할 수 있는 창에 대해 권한을 가진 객체를 수정하거나 삭제할 수 있습니다.

참고 슈퍼 관리자 또는 읽기 전용 권한이 있는 시스템 정의 관리 사용자만 사용자 그룹에 속하지 않은 ID 기반 사용자를 확인할 수 있습니다. 이러한 권한 없이 생성된 관리자는 해당 사용자를 볼 수 없습니다.

역할 기반 권한

Cisco ISE에서는 메뉴 및 데이터 레벨에서 권한을 구성할 수 있는데, 이를 메뉴 액세스 및 데이터 액세스 권한이라고 합니다.

메뉴 액세스 권한을 통해 Cisco ISE 관리 인터페이스의 메뉴 및 하위 메뉴 항목을 보이거나 숨길 수 있습니다. 이 기능을 사용하면 메뉴 레벨에서 액세스를 제한하거나 활성화할 수 있도록 권한을 생성할 수 있습니다.

데이터 액세스 권한을 통해 Cisco ISE 인터페이스에서 관리자 그룹, 사용자 ID 그룹, 엔드포인트 ID 그룹, 위치 및 디바이스 유형 데이터에 대한 읽기 및 쓰기 또는 읽기 전용 권한을 부여하거나 액세스 권한을 부여하지 않을 수 있습니다.

RBAC 정책

RBAC 정책에 따라 메뉴 항목 또는 다른 ID 그룹 데이터 요소에 대한 특정 액세스 유형을 관리자에게 부여할 수 있는지 결정됩니다. RBAC 정책을 사용하여 관리자 그룹에 따라 관리자에게 메뉴 항목 또는 ID 그룹 데이터 요소에 대한 액세스를 부여하거나 거부할 수 있습니다. 관리자가 관리 포털에 로그인하면 연결된 관리자 그룹용으로 정의된 정책 및 권한에 따라 메뉴 및 데이터에 액세스할 수 있습니다.

RBAC 정책은 관리자 그룹을 메뉴 액세스 및 데이터 액세스 권한에 매핑합니다. 예를 들어 네트워크 관리자가 Admin Access(관리자 액세스) 작업 메뉴 및 정책 데이터 요소를 보지 못하게 차단할 수 있습니다. 이렇게 하려면 네트워크 관리자가 연결되어 있는 관리자 그룹에 대한 사용자 맞춤화 RBAC 정책을 생성합니다.

참고 관리자 액세스를 위해 사용자 맞춤화 RBAC 정책을 사용하는 경우 해당 데이터 액세스 권한과 관련된 모든 메뉴 액세스를 제공해야 합니다. 예를 들어 ID 또는 정책 관리자의 데이터 액세스 권한으로 엔드포인트를 추가하거나 삭제하려면 **Work Center(**작업 센터**) > Network Access(**네트워크 액세스**)** 및 **Administration(**관리**) > Identity Management(ID** 관리**)**에 대한 메뉴 액세스를 제공해야 합니다.

기본 메뉴 액세스 권한

Cisco ISE는 미리 정의된 관리자 그룹 집합과 연결되어 있고 즉시 사용 가능한 권한 집합을 제공합니다. 관리자 그룹 권한이 미리 정의되어 있으므로 권한을 설정할 수 있습니다. 그러면 관리자 그룹의 멤버가 관리 인터페이스 내의 메뉴 항목에 대한 전체 또는 제한된 액세스 권한(메뉴 액세스라고 함)을 가질 수 있으며 관리자 그룹이 다른 관리자 그룹의 데이터 액세스 요소를 사용(데이터 액세스라고 함)하도록 위임할 수 있습니다. 이러한 권한은 다양한 관리자 그룹에 대한 RBAC 정책을 입안하기 위해 더 사용할 수 있는 다시 사용할 수 있는 엔티티입니다. Cisco ISE는 기본 RBAC 정책에서 이미 사용되는 시스템 정의 메뉴 액세스 권한 집합을 제공합니다. 미리 정의된 메뉴 접속 권한 외에, Cisco ISE는 또한 RBAC 정책에서 사용할 수 있는 사용자 맞춤화 메뉴 액세스 권한을 만들 수 있습니다. 열쇠 아이콘은 메뉴와 하위 메뉴에 대한 메뉴 액세스 권한을 나타내고 닫기 아이콘이 있는 열쇠는 각기 다른 RBAC 그룹에 대한 액세스 권한이 없음을 나타냅니다.

참고 슈퍼 관리 사용자의 경우 모든 메뉴 항목을 사용할 수 있습니다. 다른 관리 사용자는 **Menu Access Privileges(**메뉴 액세스 권한**)** 열의 모든 메뉴 항목을 독립형 구축과 함께 분산형 구축의 기본 노드에서 사용할 수 있습니다. 분산형 구축의 보조 노드에서 **Administration(**관리**)** 탭 아래의 메뉴 항목은 사용할 수 없습니다.

메뉴 액세스 권한 구성

Cisco ISE에서는 RBAC 정책에 매핑할 수 있는 맞춤화 메뉴 액세스 권한을 생성할 수 있습니다. 관리자가 역할에 따라 특정 메뉴 옵션에만 액세스하도록 허용할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authorization(**권한 부여**)** > **Permissions(**권한**)** > **Menu Access(**메뉴 액세스**)**

단계 **2** **Add(**추가**)**를 클릭하고 **Name(**이름**)** 및 **Description(**설명**)** 필드에 값을 입력합니다.

a) **ISE Navigation Structure(ISE** 탐색 구조**)** 메뉴를 원하는 수준으로 확장하고 권한을 생성할 옵션을 클릭합니다.

b) **Permissions for Menu Access(**메뉴 액세스에 대한 권한**)** 패널에서 **Show(**표시**)**를 클릭합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

데이터 액세스 권한 부여 사전 요건

RBAC 관리자가 개체(예: 사용자 ID 그룹 데이터 유형의 직원)에 대한 모두 전체 액세스을 가진 경우 관리자는 해당 그룹에 속한 사용자를 보고, 추가하고, 업데이트하고, 삭제할 수 있습니다. 관리자에게 **Users(**사용자**)** 창(**Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**)**)에 대해 부여된 메뉴 액세스 권한이 있는지 확인합니다. 이는 네트워크 디바이스 그룹 및 엔드포인트 ID 그룹 데이터 유형에 부여된 권한을 기준으로 네트워크 디바이스 및 엔드포인트 개체에 적용됩니다.

기본 네트워크 디바이스 그룹 개체(모든 디바이스 유형 및 모든 위치)에 속하는 네트워크 디바이스에 대해 데이터 액세스를 활성화하거나 제한할 수 없습니다. 이러한 기본 네트워크 디바이스 그룹 개체에서 생성된 개체에 전체 액세스 데이터 사용 권한이 부여된 경우 모든 네트워크 디바이스가 표시됩니다. 따라서 기본 네트워크 디바이스 그룹 개체와 무관한 네트워크 디바이스 그룹 데이터 유형에 대해 별도의 계층 구조를 생성하는 것이 좋습니다. 제한된 액세스 권한을 생성하려면 새로 생성된 네트워크 디바이스 그룹에 네트워크 디바이스 개체를 할당해야 합니다.

참고 관리 그룹이 아닌 사용자 ID 그룹, 네트워크 디바이스 그룹 및 엔드포인트 ID 그룹에 대해서만 데이터 액세스 권한을 활성화하거나 제한할 수 있습니다.

기본 데이터 액세스 권한

Cisco ISE에는 미리 정의된 데이터 액세스 권한이 제공됩니다. 데이터 액세스 권한을 사용하면 여러 관리자가 동일한 사용자 집단 내에서 데이터 액세스 권한을 가질 수 있습니다. 하나 이상의 관리자 그룹에 대한 데이터 액세스 권한을 사용하는 기능을 활성화하거나 제한할 수 있습니다. 이 프로세스에서는 선택적 연결을 통해 선택한 관리자 그룹의 데이터 액세스 권한을 재사용할 수 있도록 한 관리자 그룹의 관리자에 대한 자율 위임 제어가 가능합니다. 데이터 액세스 권한의 범위는 선택한 관리자 그룹 또는 네트워크 디바이스 그룹을 볼 수 있는 전체 액세스 권한부터 액세스 권한 없음까지입니다. RBAC 정책은 관리자 (RBAC) 그룹, 메뉴 액세스 및 데이터 액세스 권한에 기초 하여 정의 됩니다. 먼저 메뉴 액세스 및 데이터 액세스 권한을 생성한 다음 관리자 그룹을 해당 메뉴 액세스 및 데이터 액세스 권한에 연결하는 RBAC 정책을 생성해야 합니다. RBAC 정책의 형식은 If admin_group=Super

Admin then assign SuperAdmin Menu Access permission + SuperAdmin Data Access permission과 같습니다. 미리 정의된 데이터 접속 권한 외에, Cisco ISE는 또한 RBAC 정책과 연결할 수 있는 사용자 맞춤화 데이터 액세스 권한을 만들 수 있습니다.

관리자 그룹에 부여할 수 있는 데이터 액세스 권한은 세 가지로, Full Access(전체 액세스), No Access(액세스 없음) 및 Read Only(읽기 전용) 액세스 권한입니다.

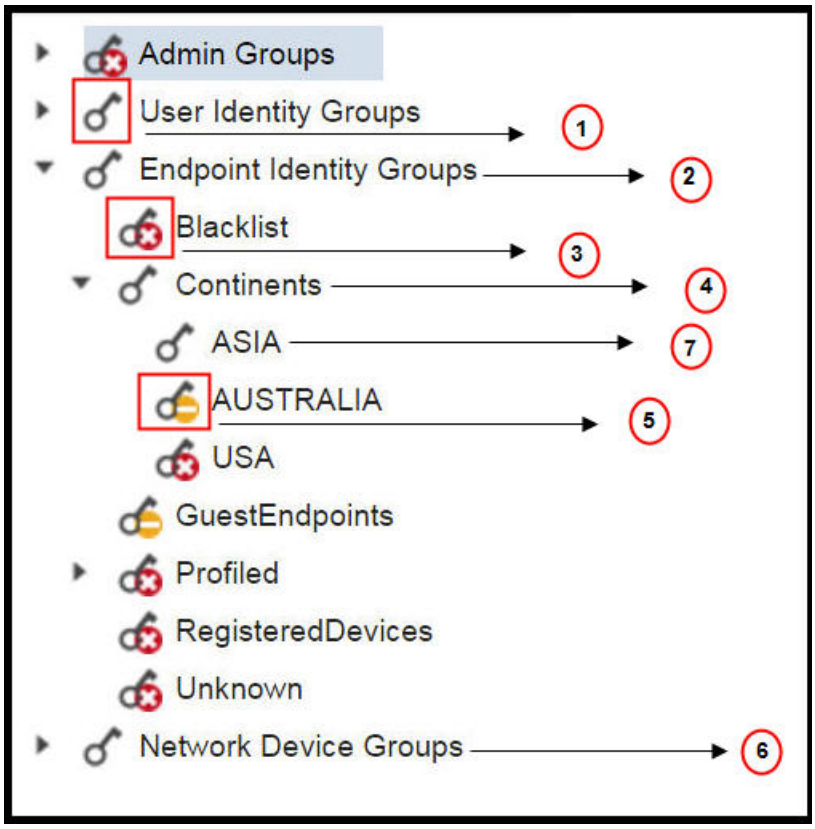
다음의 관리자 그룹에 읽기 전용 권한을 부여할 수 있습니다.

- Administration(관리) > Admin Access(관리 액세스) > Administrators(관리자) > Admin Groups(관리자 그룹)
- Administration(관리) > Groups(그룹) > User Identity Group(사용자 ID 그룹)
- Administration(관리) > Groups(그룹) > Endpoint Identity Group(엔드포인트 ID 그룹)
- 네트워크 가시성 > 엔드포인트
- Administration(관리) > Network Resources(네트워크 리소스) > Network Device Groups(네트워크 디바이스 그룹)
- Administration(관리) > Network Resources(네트워크 리소스) > Network Device Groups(네트워크 디바이스 그룹)
- Administration(관리) > Identity Management(아이덴티티 관리) > Identities(아이덴티티)
- Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹)
- Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > Endpoint Identity Groups(엔드포인트 ID 그룹)

데이터 유형에 대해 읽기 전용 권한이 있는 경우(예: 엔드포인트 ID 그룹) 해당 데이터 유형에 대해 CRUD 작업을 수행할 수 없습니다. 개체에 대해 읽기 전용 권한이 있는 경우(예: 게스트 엔드포인트) 해당 개체에 대해 편집 또는 삭제 작업을 수행할 수 없습니다.

다음의 이미지는 각기 다른 RBAC 그룹에 대한 추가 하위 메뉴 또는 옵션을 포함하는 두 번째 또는 세 번째 레벨 메뉴에서 데이터 액세스 권한이 적용되는 과정을 설명한 것입니다.

그림 *1:* 데이터 액세스 권한



라벨	설명
1	사용자 ID 그룹 데이터 유형에 대한 전체 액세스를 나타냅니다.
2	엔드포인트 ID 그룹이 하위 항목(아시아)에 부여된 최대 권한(전체 액세스)을 얻는다는 것을 나타냅니다.
3	개체(차단된 목록)에 대한 액세스가 없음을 나타냅니다.
4	상위 항목(대륙)이 하위 항목(아시아)에 부여된 최대 액세스 권한을 얻는다는 것을 나타냅니다.
5	개체(호주)에 대한 읽기 전용 액세스를 나타냅니다.
6	상위 항목(네트워크 디바이스 그룹)에 전체 액세스 권한이 부여되면 하위 항목이 자동으로 권한을 상속받는다는 것을 나타냅니다.

라벨	설명
7	상위 항목(아시아)에 전체 액세스 권한이 부여되면 개체들은 권한을 명시적으로 부여받지 않는 한 전체 액세스 권한을 상속받는다는 것을 나타냅니다.

데이터 액세스 권한 구성

Cisco ISE에서는 RBAC 정책에 매핑할 수 있는 사용자 맞춤화 데이터 액세스 권한을 생성할 수 있습니다. 관리자가 역할에 따라 선택적인 데이터에 대한 액세스 권한만 제공할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authorization(**권한 부여**)** > **Permissions(**권한**)**

단계 **2** **Permissions(**권한**)** > **Data Access(**데이터 액세스**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하고 **Name(**이름**)** 및 **Description(**설명**)** 필드에 값을 입력합니다.

a) 관리 그룹을 클릭하여 확장하고 해당 관리 그룹을 선택합니다.

b) **Full Access(**전체 액세스 권한**)**, **Read Only Access(**읽기 전용 액세스 권한**)** 또는 **No Access(**액세스 권한 없음**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

읽기 전용 관리 정책

기본 읽기 전용 관리 정책은 **Administration(**관리**) > System(**시스템**) > Admin Access(**관리자 액세스**) > Authorization(**권한 부여**) > RBAC Policy(RBAC** 정책**)** 창에서 제공됩니다. 이 정책은 신규 설치 및 업그레이드된 구축에 모두 사용할 수 있습니다. 읽기 전용 관리자 정책은 읽기 전용 관리자 그룹에 적용됩니다. 기본적으로 슈퍼 관리자 메뉴 액세스 및 읽기 전용 데이터 액세스 권한은 읽기 전용 관리자에게 부여됩니다. 이 정책은 복제할 수 없으며 연결된 **Data Access(**데이터 액세스**)** 권한을 수정할 수 없습니다.

참고

- 기본 읽기 전용 정책은 읽기 전용 관리자 그룹에 매핑됩니다. 읽기 전용 관리자 그룹을 사용하여 사용자 맞춤화 RBAC 정책을 생성할 수 없습니다.
- Cisco ISE는 읽기 전용 관리자 그룹의 정적 확인을 기반으로 하는 읽기 전용 기능을 지원합니다.

읽기 전용 관리자를 위한 메뉴 액세스 사용자 맞춤화

기본적으로 읽기 전용 관리자에게는 슈퍼 관리자 메뉴 액세스 및 읽기 전용 관리자 데이터 액세스 권한이 부여됩니다. 그러나 슈퍼 관리자가 읽기 전용 관리자에게 **Home(**홈**)** 및 **Administration(**관리**)** 탭만 표시하도록 요구하는 경우 슈퍼 관리자는 맞춤형 메뉴 액세스를 생성하거나 MnT 관리자 메뉴 액

세스 또는 정책 관리자 메뉴 액세스와 같은 기본 권한을 사용자 맞춤화할 수 있습니다. 슈퍼 관리자는 읽기 전용 관리 정책에 매핑된 읽기 전용 데이터 액세스를 수정할 수 없습니다.

단계 **1** 관리 포털에 슈퍼 관리자로 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authorization(**권한 부여**)** > **Permissions(**권한**)** > **Menu Access(**메뉴 액세스**)**

단계 **3** **Add(**추가**)**를 클릭하고 이름(예: MyMenu) 및 설명을 입력합니다.

단계 **4** **Menu Access Privileges(**메뉴 액세스 권한**)** 섹션에서 **Show/Hide(**표시/숨기기**)** 옵션을 선택하여 읽기 전용 관리자에게 표시해야 하는 필수 옵션(예: **Home(**홈**)** 및 **Administration (**관리**)** 탭)을 선택할 수 있습니다.

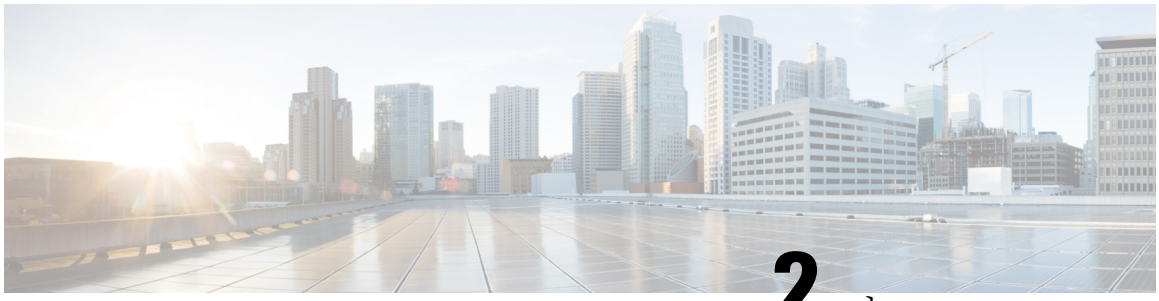
단계 **5** **Submit(**제출**)**을 클릭합니다.
맞춤형 메뉴 액세스 권한은 **Administration(**관리**) > System(**시스템**) > Admin Access(**관리자 액세스**) > Authorization(**권한 부여**) > Policy(**정책**)** 창에 나와 있는 읽기 전용 관리 정책에 해당하는 **Permissions(**권한**)** 드롭다운에 표시됩니다.

단계 **6** **Administration(**관리**) > System(**시스템**) > Admin Access(**관리자 액세스**) > Authorization(**권한 부여**) > RBAC Policy(**정책**)** 창을 선택합니다.

단계 **7** **Read-Only Admin Policy(**읽기 전용 관리 정책**)**에 해당하는 **Permissions(**권한**)** 드롭다운을 클릭하고 **Administration(**관리**) > System(**시스템 **)> Admin Access(**관리자 액세스**) > Authorization(**권한 부여**) > Permissions(**권한**) > Menu Access(**메뉴 액세스**)** 창에서 생성한 기본(MnT 관리자 메뉴 액세스) 또는 맞춤형 메뉴 액세스 권한(MyMenu)을 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

참고
- 읽기 전용 관리 정책에 대해 데이터 액세스 권한을 선택하면 오류가 발생합니다.
- 읽기 전용 관리 포털에 로그인하면 Read-Only(읽기 전용) 아이콘이 창 상단에 나타나며 데이터 액세스 없이 지정된 메뉴 옵션만 볼 수 있습니다.



2 장

라이선싱

Cisco ISE 라이선스

Cisco ISE 릴리스 3.0 이상 릴리스는 Cisco ISE 릴리스 2.x에서 사용된 레거시 라이선스(예: Base, Plus 및 Apex 라이선스)를 지원하지 않습니다. Cisco ISE 릴리스 3.0 라이선스는 전적으로 CSSM(Cisco Smart Software Manager)이라는 중앙 데이터베이스를 통해 관리됩니다. 단일 토큰 등록으로 모든 라이선스를 쉽고 효율적으로 등록, 활성화 및 관리할 수 있습니다.

고객의 경제성을 최대화하기 위해 Cisco ISE의 라이선싱이 다음 패키지로 제공됩니다.

- 계층 라이선스

  Cisco ISE 릴리스 3.0부터는 릴리스 3.0 이전에 사용된 Base, Apex 및 Plus 라이선스를 계층 라이선스라고 하는 새로운 라이선스 집합으로 대체합니다. 리이선싱 계층에는 Essentials, Advantage 및 Premier의 3가지가 포함됩니다.

  현재 Base, Apex 또는 Plus 라이선스가 있는 경우 CSSM을 사용하여 새 라이선스 유형으로 변환합니다.

- 디바이스 관리 라이선스

  TACACS+ 페르소나가 활성화된 PSN(정책 서비스 노드)은 디바이스 관리 라이선스를 사용합니다.

- 가상 어플라이언스 라이선스

  가상 어플라이언스 라이선스는 VM Small, VM Medium 및 VM Large의 세 가지 형식으로 제공됩니다.

- 평가판 라이선스

평가판 라이선스는 Cisco ISE 릴리스 3.0을 처음 설치할 때 기본적으로 활성화됩니다. 평가판 라이선스는 모든 Cisco ISE 기능에 액세스할 수 있는 90일 라이선스입니다. 평가 기간 동안에는 라이선스 사용이 CSSM에 보고되지 않습니다.

기존 스마트 라이선스를 사용하여 Cisco ISE 릴리스 3.0으로 업그레이드하는 경우, 라이선스를 CSSM의 새로운 스마트 라이선스 유형으로 변환합니다. 그러나 Cisco ISE 릴리스 3.0에서 라이선스를 활성화하려면 CSSM에 새 라이선스 유형을 등록해야 합니다.

기존 Cisco ISE 라이선스를 소유한 경우, Cisco ISE 릴리스 3.0에서 라이선스 사용을 활성화하려면 스마트 라이선스로 변환해야 합니다. Cisco ISE 2.x 라이선스를 새 라이선스 유형으로 변환하려면 Support Case Manager(지원 케이스 매니저)(http://cs.co/scmswl)를 통해 온라인으로 케이스를 열거나 http://cs.co/TAC-worldwide에 제시된 연락처 정보를 사용하십시오.

모든 활성 Cisco ISE 라이선스의 경우 라이선스 만료에 대한 알림이 만료 전 90일, 60일, 30일 전에 Cisco ISE에 표시됩니다. 비준수 라이선스 사용에 대한 알림도 Cisco ISE에 표시됩니다. 라이선스 사용이 45일 동안 컴플라이언스를 준수하지 않는 경우, 필요한 라이선스를 구매하여 활성화할 때까지 Cisco ISE의 모든 관리 제어 기능에 액세스할 수 없게 됩니다.

하나의 라이선싱 패키지에서 다른 라이선싱 패키지로 업그레이드할 경우 Cisco ISE는 업그레이드 전에 이전 패키지에서 제공되었던 모든 기능을 계속 제공합니다. 이미 구성한 설정은 다시 구성해야 합니다. 예를 들어, 현재 Essentials 라이선스를 사용 중이고 나중에 Advantage 라이선스를 추가하는 경우 Essentials 라이선스를 사용하여 이미 구성된 기능은 변경되지 않습니다.

다음과 같은 경우 라이선스 계약을 업데이트해야 합니다.

- 평가 기간이 종료되었으며 아직 라이선스를 등록하지 않았습니다.
- 라이선스가 만료되었습니다.
- 엔드포인트 사용량이 라이선스 계약을 초과합니다.

Cisco ISE 커뮤니티 리소스

Cisco Identity Services Engine 주문 설명서

평가 라이선스를 구하는 방법에 대한 자세한 내용은 ISE 평가 라이선스 취득 방법에서 확인할 수 있습니다.

계층 라이선스

다음 표에는 새 계층 라이선스로 활성화되는 기능이 나와 있습니다.

표 *2: Cisco ISE* 계층 라이선스

라이선스 이름	이 라이선스로 활성화되는 기능
Essentials	• 802.1X, MAC Authentication Bypass 및 Easy Connect, 웹 인증을 포함하는 RADIUS 인증, 권한 부여 및 계정 관리 • MACsec • SSO(Single Sign-On), SAML(Security Assertion Markup Language) 및 ODBC(Open DataBase Connectivity) 표준을 기반으로 하는 인증 • 게스트 액세스 및 스폰서 서비스 • 모니터링을 위한 REST(Representational State Transfer) API 및 CRUD 작업을 위한 외부 RESTful 서비스 API • 패시브 ID 서비스. • 보안 유선 및 무선 액세스
Advantage	• Cisco ISE Essentials 라이선스로 활성화되는 모든 기능 • 기본 제공되는 CA(Certification Authority)를 사용한 BYOD(Bring Your Own Device) 디바이스 등록 및 프로비저닝. 디바이스 등록은 구성된 내 디바이스 포털을 통해 수행됩니다. • 보안 그룹 태그 지정, TrustSec 및 Cisco ACI(Application Centric Infrastructure) 통합 • 기본 에셋 가시성 및 시행 기능을 포함한 프로파일링 서비스 • 고급 에셋 가시성 및 시행 기능을 포함한 엔드포인트 분석 • 피드 서비스. • 위치 기반 서비스의 가시성 및 시행 • 상황 공유(예: pxGrid) 및 보안 에코시스템 통합

라이선스 이름	이 라이선스로 활성화되는 기능
Premier	• Cisco ISE Essentials 및 Advantage 라이선스로 활성화되는 모든 기능 • 엔드포인트 보호 서비스 • 적응형 네트워크 제어 및 상황 공유 서비스를 사용한 빠른 위협 억제 • 포스처 가시성 및 시행 • 엔터프라이즈 이동성 관리 및 모바일 디바이스 관리를 통한 규정 준수 가시성 및 시행 • 위협 중심 네트워크 액세스 제어 가시성 및 시행

디바이스 관리 라이선스

디바이스 관리 라이선스를 사용하면 정책 서비스 노드에서 TACACS 서비스를 사용할 수 있습니다. 고가용성 독립형 구축에서는 디바이스 관리 라이선스를 통해 고가용성 쌍의 단일 정책 서비스 노드에서 TACACS 서비스를 사용할 수 있습니다.

가상 어플라이언스 라이선스

Cisco ISE는 가상 어플라이언스로도 판매됩니다. 네트워크의 VM 노드 수와 CPU 및 메모리와 같은 각 VM 노드의 리소스 사양에 따라 VM(Virtual Machine) 라이선스를 선택합니다. 제공되는 VM 라이선스의 카테고리는 세 가지, 즉 VM Small, VM Medium 및 VM Large입니다.

다음 표에는 카테고리별 최소 VM 리소스가 나와 있습니다.

표 ***3:*** 카테고리별 최소 ***VM*** 리소스

VM 라이선스	**VM** 노드의 **RAM** 용량	**VM** 노드의 **CPU** 수
VM Small	16GB	CPU 12개
VM Medium	64GB	CPU 16개
VM Large	256GB	CPU 16개

예를 들어 CPU 16개, RAM 64GB의 3595형 VM 노드를 사용하는 경우 이 VM 노드에서 Cisco ISE 서비스를 활성화하려면 VM Medium 라이선스가 필요합니다. VM Small 라이선스만 등록하고 활성화한 경우에도 Cisco ISE는 VM 노드별로 VM Medium 라이선스의 사용을 등록합니다. 이는 사용된 라이선스가 VM 노드의 RAM 및 CPU 사양에 따라 결정되기 때문입니다.

그러면 필요한 VM 라이선스를 조달하고 설치할 때까지 비준수 라이선스 사용에 대한 경고 및 알림을 받게 됩니다. 그러나 Cisco ISE 서비스는 중단되지 않습니다.

구축의 VM 수와 리소스에 따라 여러 VM 라이선스를 설치할 수 있습니다.

VM 라이선스는 인프라 라이선스입니다. 따라서 구축에서 사용 가능한 엔드포인트 라이선스에 관계없이, VM 라이선스를 설치할 수 있습니다. 그러나 계층 라이선스에서 활성화된 기능을 사용하려면 적절한 계층 라이선스도 설치해야합니다.

Cisco ISE 릴리스 2.4 이상 릴리스를 설치하거나 업그레이드한 후, 구축된 VM 노드 수와 설치된 VM 라이선스 수가 일치하지 않으면 14일마다 홈 페이지의 **Alarms(**경보**)** 대시릿에 경보가 표시됩니다. VM 노드의 리소스가 변경되고 VM 노드가 등록 또는 등록 취소된 경우에도 경보가 표시됩니다.

VM 라이선스는 영구 라이선스입니다. VM 라이선스 변경 사항은 Cisco ISE GUI에 로그인할 때마다 대화 상자에서 **Do not show this message again(**이 메시지를 다시 표시하지 않음**)** 확인란을 선택할 때까지 표시됩니다.

평가판 라이선스

평가판 라이선스는 Cisco ISE 릴리스 3.0을 설치하거나 업그레이드할 때 기본적으로 활성화됩니다. 평가판 라이선스는 90일 동안 활성화되며 이 기간 동안 모든 Cisco ISE 기능에 액세스할 수 있습니다. 평가 라이선스를 사용 중인 경우 Cisco ISE는 평가 모드로 간주됩니다.

Cisco ISE 관리 포털의 오른쪽 상단에 평가 모드가 유지되는 기간(일)이 포함된 메시지가 표시됩니다. 필요한 Cisco ISE 기능을 계속 사용하려면 평가 모드 종료 시까 지 구매한 Cisco ISE 라이선스를 등록해야 합니다.

Cisco ISE 스마트 라이선싱

스마트 라이선스 토큰이 활성 상태이고 Cisco ISE 관리 포털에 등록된 경우 CSSM은 제품 라이선스마다 각 엔드포인트 세션별로 라이선스 사용을 모니터링합니다. 스마트 라이선싱은 Cisco ISE의 간단한 표 레이아웃에서 엔드포인트 세션별 라이선스 사용에 대해 관리자에게 알립니다. 스마트 라이선싱은 활성화된 각 라이선스의 최고 사용량을 매일 중앙 집중식 데이터베이스에 보고합니다. 라이선스가 사용 가능하지만 사용되지 않는 경우 관리자는 사용 가능한 라이선스에 대해 알림을 받고 사용량을 계속 모니터링할 수 있습니다. 사용량이 사용 가능한 라이선스 수를 초과하면 경보가 활성화되고 경보 및 알림을 통해 관리자에게 이 정보가 전달됩니다.

스마트 라이선싱을 사용하면 Cisco 스마트 어카운트를 통해 포함된 다양한 라이선스 엔타이틀먼트(예: Essentials, Advantage, Premium 또는 Device Admin)를 관리할 수 있습니다. Cisco ISE에서 라이선스 엔타이틀먼트당 기본 사용량 통계를 모니터링할 수 있습니다. CSSM 계정에서 추가 정보, 통계 및 알림을 볼 수 있을 뿐만 아니라 계정 및 엔타이틀먼트도 변경할 수 있습니다.

참고 CSSM 위성은 Cisco ISE 릴리스 3.0 패치 1 이하에서는 지원되지 않습니다.

Cisco ISE는 30분마다 내부의 라이선스 사용 샘플을 가져옵니다. 라이선스 규정 준수 및 사용량이 그에 따라 업데이트됩니다. Cisco ISE의 **Licenses(**라이선스**)** 표에서 이 정보를 보려면 메인 메뉴에서

Administration(관리**)** > **System(**시스템**)** > **Licensing(**라이선싱**)**을 선택하고 **Refresh(**새로 고침**)**를 클릭합니다.

Cisco ISE PAN(Cisco ISE Primary Administration Node)을 CSSM에 등록할 때부터 Cisco ISE는 6시간마다 CSSM 서버에 최고 라이선스 사용 수를 보고합니다. 최고 개수 보고서는 Cisco ISE의 라이선스 사용량이 구매 및 등록된 라이선스를 준수하는지 확인하는 데 도움이 됩니다. Cisco ISE는 CSSM 인증서의 로컬 복사본을 저장하여 CSSM 서버와 통신합니다. CSSM 인증서는 일별 동기화 중에 그리고 **Licenses(**라이선스**)** 표를 새로 고칠 때 자동으로 다시 권한이 부여됩니다. 일반적으로 CSSM 인증서는 6개월간 유효합니다.

Cisco ISE가 CSSM 서버와 동기화할 때 규정 준수 상태가 변경되면 **Licenses(**라이선스**)** 표의 **Last Authorization(**마지막 권한 부여**)** 열이 그에 따라 업데이트됩니다. 또한 엔타이틀먼트가 더 이상 규정을 준수하지 않는 경우, 규정을 준수하지 않는 기간(일)이 **Days Out of Compliancy(**규정을 준수하지 않은 일수**)** 열에 표시됩니다. 규정 미준수는 **Licensing(**라이선싱**)** 영역 상단의 알림 및 Cisco ISE 툴바의 **License Warning(**라이선스 경고**)** 링크 옆에도 표시됩니다. 알림 외에도 경보를 볼 수 있습니다.

참고 디바이스 관리 라이선스는 Cisco ISE가 CSSM 서버와 통신할 때 권한이 부여되지만, 세션 기반이 아니므로 **Licenses(**라이선스**)** 표에 이와 관련된 사용량이 표시되지 않습니다.

Licenses(라이선스**)** 표의 규정 준수 열에 다음 값 중 하나가 표시됩니다.

- **In Compliance(**규정 준수**)**: 이 라이선스의 사용이 규정을 준수합니다.
- **Released Entitlement(**릴리스된 엔타이틀먼트**)**: 라이선스가 구매되어 사용하도록 릴리스되었지만 이 Cisco ISE 구축에서는 지금까지 사용된 것이 없습니다. 이 경우 라이선스의 **Consumption Count(**사용 개수**)**가 0입니다.
- **Evaluation(**평가판**)**: 평가판 라이선스를 사용할 수 있습니다.

스마트 라이선스 등록 및 활성화

시작하기 전에

- 기존 Cisco ISE 라이선스가 있는 경우 스마트 라이선스로 변환해야 합니다.
- 기존 스마트 라이선스를 사용하여 Cisco ISE 릴리스 3.0으로 업그레이드하는 경우, 라이선스를 CSSM의 새로운 스마트 라이선스 유형으로 변환합니다.
- 등록 토큰을 받으려면 CSSM의 새 스마트 라이선스 유형을 등록합니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Licensing(**라이선싱**)**을 선택합니다.

단계 **2** **Registration Details(**등록 세부정보**)**를 클릭합니다.

단계 **3** 표시되는 **Registration Details(**등록 세부정보**)** 영역에서 **Registration Token(**등록 토큰**)** 필드에 CSSM으로부터 받은 등록 토큰을 입력합니다.

단계 **4** **Connection Method(**연결 방법**)** 드롭다운 목록에서 연결 방법을 선택합니다.

- 인터넷에 대한 직접 연결을 구성한 경우 **Direct HTTPS(**직접 **HTTPS)**입니다.
- 인터넷에 직접 연결되어 있지 않고 프록시 서버를 사용해야 하는 경우 **HTTPS Proxy(HTTPS** 프록시**)**입니다. Cisco ISE 스마트 라이선스를 등록한 후 프록시 서버 구성을 변경하는 경우 **Licensing(**라이선싱**)** 창에서 스마트 라이선스 구성을 업데이트해야 합니다. Cisco ISE는 업데이트된 프록시 서버를 사용하여 CSSM과의 연결을 설정하므로 Cisco ISE 서비스가 중단되지 않습니다.
- **Transport Gateway(**전송 게이트웨이**)**가 권장 옵션입니다. 전송 게이트웨이를 구성한 경우 이 연결이 기본적으로 선택됩니다. 다른 연결 방법을 선택하려면 전송 게이트웨이 구성을 제거해야 합니다.
- 구성된 SSM 온 프레미스 서버에 연결하기 위한 **SSM** 온프레미스 서버. 이 옵션은 Cisco ISE 릴리스 3.0 패치 2 이상에서 사용할 수 있습니다. Air-Gapped 네트워크용 스마트 라이선싱, 32 페이지를 참조하십시오.

단계 **5** **Tier(**계층**)** 및 **Virtual Appliance(**가상 어플라이언스**)** 영역에서 활성화해야 하는 모든 라이선스의 확인란을 선택합니다. 선택한 라이선스가 활성화되며 그 사용량이 CSSM에서 추적됩니다.

단계 **6** **Register(**등록**)**를 클릭합니다.

Cisco ISE에서 스마트 라이선싱 관리

스마트 라이선싱 토큰을 활성화하고 등록한 후에는 다음을 통해 Cisco ISE에서 라이선스 엔타이틀먼트를 관리할 수 있습니다.

- 라이선스 엔타이틀먼트 인증서 활성화, 비활성화 및 새로 고침
- 스마트 라이선싱 등록 업데이트
- 라이선싱 준수 및 비준수 문제 식별

시작하기 전에

스마트 라이선싱 토큰을 활성화하고 등록했는지 확인하십시오.

단계 **1** Cisco ISE 릴리스 3.0을 처음 설치하면 모든 라이선스 엔타이틀먼트가 평가 모드의 일부로 자동으로 활성화됩니다. 라이선스 토큰을 등록한 후 CSSM 계정에 특정 엔타이틀먼트가 포함되어 있지 않고 등록 중 이를 비활성화하지 않은 경우 Cisco ISE에 비준수 알림이 표시됩니다. 비준수 알림을 제거하고 관련 기능을 계속 사용하려면 CSSM 계정에 해당 엔타이틀먼트를 추가(도움이 필요하면 CSM 계정 담당자에게 문의)한 후에 **Licenses(**라이선스**)** 표에서 **Refresh(**새로 고침**)**를 클릭합니다. 권한 부여를 새로 고친 후에는 Cisco ISE에서 로그아웃했다가 다시 로그인해야 관련 비준수 메시지가 제거됩니다.

단계 **2** 일별 자동 권한 부여가 어떤 이유로 실패할 경우 비준수 메시지가 나타날 수 있습니다. 엔타이틀먼트에 다시 권한을 부여하려면 **Refresh(**새로 고침**)**를 클릭합니다. 권한 부여를 새로 고친 후에는 Cisco ISE에서 로그아웃했다가 다시 로그인해야 관련 비준수 메시지가 제거됩니다.

단계 **3** Cisco ISE 릴리스 3.0을 처음 설치하면 모든 라이선스 엔타이틀먼트가 평가 기간의 일부로 자동으로 활성화됩니다. 라이선스 토큰을 등록한 후 CSSM 계정에 특정 엔타이틀먼트가 포함되어 있지 않고 등록 중 이를 비활성화하지 않은 경우에도 불필요한 비준수 알림을 방지하기 위해 ISE의 스마트 라이선싱에서 해당 엔타이틀먼트를 비활성화할 수 있습니다. **Licenses(**라이선스**)** 표에서 토큰에 포함되지 않은 라이선스 엔타이틀먼트의 확인란을 선택하고 툴바에서 **Disable(**비활성화**)**을 클릭합니다. 라이선스 엔타이틀먼트를 비활성화한 후 로그아웃한 다음 다시 Cisco ISE에 로그인하면 관련 기능이 메뉴에서 제거되고 비준수 메시지가 제거됩니다.

단계 **4** 계정에 엔타이틀먼트를 추가한 후에는 해당 엔타이틀먼트를 활성화합니다. **Licenses(**라이선스**)** 표에서 필요한 비활성화된 라이선스의 확인란을 선택하고 툴바에서 **Enable(**활성화**)**을 클릭합니다.

단계 **5** 등록 인증서는 6개월마다 자동으로 새로 고쳐집니다. 스마트 라이선싱 인증서 등록을 수동으로 새로 고치려면 **Licensing(**라이선싱**)** 창 상단에서 **Renew Registration(**등록 갱신**)**을 클릭합니다.

단계 **6** 스마트 어카운트에서 Cisco ISE 등록(UDI로 표시됨)을 제거하고 평가 기간이 끝날 때까지 스마트 라이선싱을 계속 사용하려면 **Cisco Smart Licensing(Cisco** 스마트 라이선싱**)** 영역 상단에서 **Deregister(**등록 취소**)**를 클릭합니다. 예를 들어 등록 프로세스의 일부로 지정한 UDI를 변경해야 하는 경우 이 작업을 수행할 수 있습니다. 평가 기간이 남아있는 경우 Cisco ISE에서 스마트 라이선싱을 유지합니다. 평가 기간이 종료되면 브라우저를 새로 고칠 때 알림이 표시됩니다. 스마트 라이선스 등록을 취소한 후에는 등록 프로세스를 다시 수행하여 동일하거나 다른 UDI로 등록할 수 있습니다.

단계 **7** 스마트 어카운트에서 Cisco ISE 등록(UDI로 표시됨)을 완전히 제거하고 기존 라이선싱으로 되돌리려면 **Cisco Smart Licensing(Cisco** 스마트 라이선싱**)** 영역 상단에서 **Disable(**비활성화**)**을 클릭합니다. 예를 들어 등록 프로세스의 일부로 지정한 UDI를 변경해야 하는 경우 이 작업을 수행할 수 있습니다. 스마트 라이선스를 비활성화한 후에는 등록 프로세스를 다시 수행하여 동일하거나 다른 UDI를 활성화하고 등록합니다.

Air-Gapped 네트워크용 스마트 라이선싱

Cisco ISE 스마트 라이선싱을 사용하려면 Cisco ISE를 CSSM에 연결해야 합니다. 네트워크가 무선으로 연결되어 있으면 Cisco ISE는 CSSM에 라이선스 사용량을 보고할 수 없습니다. 이러한 보고 기능 부족으로 인해 Cisco ISE에 대한 관리 액세스가 손실되고 Cisco ISE 기능이 제한됩니다.

Air-Gap 네트워크에서 라이선싱 문제를 방지하고 전체 Cisco ISE 기능을 활성화하려면 Smart Software Manager(SSM) 온 프레미스를 구성합니다. 이 라이선싱 방법은 Cisco ISE 릴리스 3.0 패치 2 이상에서 사용할 수 있습니다. 구축의 노드에서 SSM 온 프레미스 서버를 구성하고 Cisco ISE가이 서버에 연결할 수 있는지 확인할 수 있습니다. 이 서버는 필요에 따라 라이선스 자격을 릴리스하고 사용량 메트릭을 추적하여 무선 게이트 네트워크에서 CSSM의 역할을 수행합니다. SSM 온 프레미스 서버는 라이선싱 소비 및 유효성과 관련된 알림, 알람 및 경고 메시지도 전송합니다.

라이선스 구매를 구입하거나 수정하는 경우 SSM 온 프레미스를 CSSM에 연결해야 로컬 서버에서 변경 사항을 사용할 수 있습니다.

참고

- SSM 온 프레미스 라이선싱 솔루션을 활성화하면 Cisco ISE에서 프록시 서비스를 사용할 수 없습니다. 또한 외부 CA 인증서로 활성화된 Cisco ISE 서비스를 사용할 수 없습니다.
- ISE-PIC 3.0은 스마트 라이선싱을 지원하지 않습니다.

스마트 라이선싱을 위한 Smart Software Manager 온프레미스 구성

시작하기 전에

구축의 노드에서 SSM 온프레미스 서버를 구성하고 Cisco ISE가 이 서버에 연결할 수 있는지 확인합니다. 이 노드는 전용 서버여야 합니다. 이 노드에서 Cisco ISE 페르소나를 활성화하지 마십시오.

Smart Software Manager 온프레미스 리소스를 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리) > System(시스템) > Licensing(라이센싱)**.

단계 **2** **Registration Details(등록 세부정보)**를 클릭합니다.

단계 **3** 표시되는 **Registration Details(등록 세부정보)** 영역에서 **Registration Token(등록 토큰)** 필드에 CSSM으로부터 받은 등록 토큰을 입력합니다.

단계 **4** **Connection Method(연결 방법)** 드롭다운 목록에서 **SSM On-Prem Server(SSM 온 프레미스 서버)**를 선택합니다.

SSM 온 프레미스 포털의 **Certificate(인증서)** 창에는 연결된 SSM 온 프레미스 서버의 IP 주소 또는 호스트 이름(또는 FQDN)이 표시됩니다.

단계 **5** **SSM On-Prem server Host(SSM 온 프레미스 서버 호스트)** 필드에 구성된 IP 주소 또는 호스트 이름(또는 FQDN)을 입력합니다.

단계 **6** **Tier(계층)** 및 **Virtual Appliance(가상 어플라이언스)** 영역에서 활성화해야 하는 모든 라이선스의 확인란을 선택합니다. 선택한 라이선스가 활성화되며 그 사용량이 CSSM에서 추적됩니다.

단계 **7** **Register(등록)**를 클릭합니다.

등록되지 않은 라이선스 사용

문제

엔드포인트와 일치하는 권한 부여 정책에서 사용되는 속성에 따라 각기 다른 엔드포인트 라이선스가 사용됩니다.

시스템에서 90일 평가 라이선스는 삭제하고 Cisco ISE Essentials 라이선스만 등록했다고 가정해 보겠습니다. 이 경우 Cisco ISE Essentials 라이선스에 해당하는 메뉴 항목 및 기능을 보고 구성할 수 있습니다.

Advantage 라이선스가 필요한 기능(예: Session:PostureStatus 속성을 사용하는 경우)을 사용하도록 권한 부여 정책을 구성하는 경우 엔드포인트가 해당 권한 부여 정책과 일치하면 다음과 같은 결과가 발생합니다.

- Cisco ISE Advantage 라이선스가 시스템에 등록되어 있지 않아도 엔드포인트가 Advantage 라이선스를 사용합니다.
- 로그인할 때마다 비준수 라이선스 사용에 대한 알림이 표시됩니다.

- Cisco ISE가 `Exceeded license usage than allowed(허용된 라이선스 사용이 허용됨)` 메시지와 함께 알림 및 알람을 표시합니다. 이는 Cisco ISE용 CSSM에 등록된 Cisco ISE Advantage 라이센스가 없지만 엔드포인트가 라이센스를 사용하기 때문입니다.

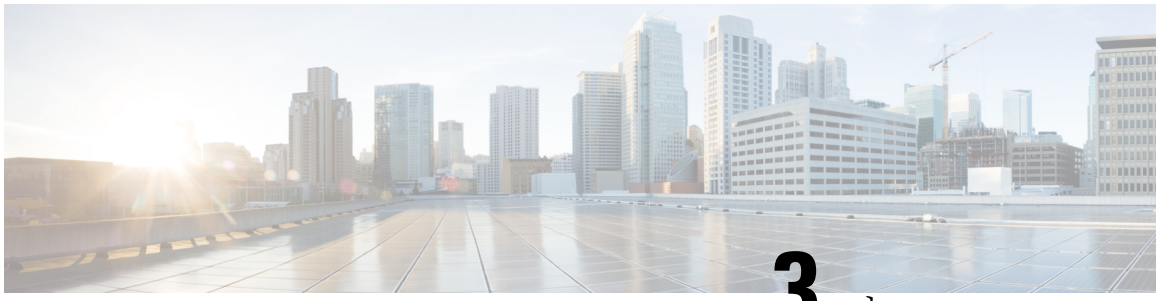
45일 동안 규정을 위반하여 3가지 계층 라이선스 모두를 사용할 경우 올바른 라이선스 파일이 업로드될 때까지 Cisco ISE의 모든 관리 제어 권한을 잃게 됩니다. 올바른 라이선스가 등록될 때까지 Cisco ISE 관리 포털의 **Licensing(**라이선싱**)** 창에만 액세스할 수 있습니다. 그러나 Cisco ISE에서는 계속 인증을 처리합니다.

가능한 원인

권한 부여 정책 구성으로 인해 **Licensing(**라이선싱**)** 표에 Cisco ISE가 구매 및 등록하지 않은 라이선스를 사용 중이라는 메시지가 표시됩니다. Advantage 또는 Premier 라이선스를 구매하기 전까지는 해당 라이선스에서 제공되는 기능이 Cisco ISE 관리 포털에 표시되지 않습니다. 그러나 이러한 라이선스를 구매한 후에는 라이선스가 만료되었거나 라이선스의 엔드포인트 사용이 설정된 제한을 초과한 후에도 GUI에서 활성화하는 기능이 계속 표시됩니다. 따라서 현재 유효한 라이선스가 없더라도 기능을 구성할 수 있습니다.

해결책

Cisco ISE 관리 포털에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택하여 등록된 라이선스가 없는 기능을 사용 중인 권한 부여 규칙을 확인한 후 해당 규칙을 재구성합니다.



3 장

구축

Cisco ISE 구축 용어

Cisco ISE 구축 시나리오에 대해 설명할 때 일반적으로 사용되는 용어는 다음과 같습니다.

- 서비스: 서비스는 네트워크 액세스, 프로파일러, 포스처, 보안 그룹 액세스, 모니터링, 문제 해결 등 페르소나가 제공하는 특정 기능입니다.
- 노드: 노드는 Cisco ISE 소프트웨어를 실행하는 개별 인스턴스입니다. Cisco ISE는 어플라이언스는 물론 VMware에서 실행될 수 있는 소프트웨어로도 사용 가능합니다. Cisco ISE 소프트웨어를 실행하는 각 인스턴스(어플라이언스 또는 VMware)를 노드라고 합니다.
- 페르소나: 노드 페르소나는 노드에서 제공하는 서비스를 결정합니다. Cisco ISE 노드는 관리, 정책 서비스, 모니터링 및 pxGrid 페르소나 중 하나를 취할 수 있습니다. 관리 포털을 통해 사용할 수 있는 메뉴 옵션은 Cisco ISE 노드에서 맡는 역할 및 페르소나에 따라 달라집니다.
- 구축 모델: 분산형 구축인지, 독립형 구축인지, 아니면 기본 2노드 구축에 해당하는 독립형 모드의 고가용성 구축인지 결정합니다.

분산형 Cisco ISE 구축의 페르소나

Cisco ISE 노드는 관리, 정책 서비스 또는 모니터링 페르소나를 취할 수 있습니다.

Cisco ISE 노드는 그 페르소나에 따라 다양한 서비스를 제공할 수 있습니다. 구축의 각 노드는 관리, 정책 서비스 및 모니터링 페르소나를 취할 수 있습니다. 분산형 구축에서는 네트워크에 다음과 같은 노드 조합이 있을 수 있습니다.

- 고가용성을 위한 기본 PAN(Policy Administration Node) 및 보조 PAN(Policy Administration Node)
- 고가용성을 위한 기본 MnT 노드(Monitoring Node) 및 보조 MnT 노드(Monitoring Node)
- 기본 PAN 자동 페일오버를 위한 상태 확인 노드 쌍 또는 단일 상태 확인 노드
- 세션 페일오버를 위한 하나 이상의 PSN(Policy Service Node)

환경 다운로드에 성공했으며, 결과에는 가동 및 실행 중인 Cisco ISE 노드만 포함됩니다.

Cisco ISE 노드 구성

Cisco ISE 노드를 설치하고 나면 관리, 정책 서비스 및 모니터링 페르소나가 제공하는 모든 기본 서비스가 해당 노드에서 실행됩니다. 이 노드는 독립형 상태가 됩니다. Cisco ISE 노드를 구성하려면 해당 노드의 관리 포털에 로그인해야 합니다. 독립형 Cisco ISE 노드의 페르소나 또는 서비스는 편집할 수 없습니다. 그러나 기본/보조 Cisco ISE 노드의 페르소나 및 서비스는 편집할 수 있습니다. 먼저 기본 ISE 노드를 구성한 후 기본 ISE 노드에 보조 ISE 노드를 등록해야 합니다.

노드에 처음 로그인하는 경우에는 기본 관리자 비밀번호를 변경하고 유효한 라이선스를 설치해야 합니다.

운영 환경에서 Cisco ISE에 구성된 호스트 이름 및 도메인 이름은 변경하지 않는 것이 좋습니다. 이러한 이름을 변경해야 하는 경우에는 어플라이언스를 재이미지화하고 변경한 다음, 초기 구축 중에 세부정보를 구성합니다.

시작하기 전에

Cisco ISE에서 분산형 구축이 설정되는 방식을 기본적으로 파악해야 합니다. 분산형 구축을 설정하기 위한 지침을 참조하십시오.

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

단계 **2** 구성할 Cisco ISE 노드 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** 필요한 대로 값을 입력하고 **Save(**저장**)**를 클릭합니다.

기본 PAN(Policy Administration Node) 구성

분산형 구축을 설정하려면 먼저 Cisco ISE 노드를 기본 PAN으로 구성해야 합니다.

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

처음에는 Register(등록) 버튼이 비활성화되어 있습니다. 이 버튼을 활성화하려면 기본 PAN을 구성해야 합니다.

단계 **2** 현재 노드 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Make Primary(**기본으로 설정**)**를 클릭하여 기본 PAN을 구성합니다.

단계 **4** **Save(**저장**)**를 클릭하여 노드 컨피그레이션을 저장합니다.

다음에 수행할 작업

1. 구축에 보조 노드를 추가합니다.
2. 필요한 경우 프로파일러 서비스를 활성화하고 프로브를 구성합니다.

보조 Cisco ISE 노드 등록

Cisco ISE 노드를 기본 PAN에 등록하여 멀티 노드 구축을 구성할 수 있습니다. 구축에서 기본 PAN이 아닌 노드들은 보조 노드라고 합니다. 노드를 등록하는 동안 노드에서 활성화해야하는 페르소나 및 서비스를 선택할 수 있습니다. 등록된 노드는 기본 PAN에서 관리할 수 있습니다(예: 노드 페르소나, 서비스, 인증서, 라이선스 관리, 패치 적용 등 관리).

노드를 등록할 때 기본 PAN이 보조 노드로 컨피그레이션 데이터를 전달하며 보조 노드의 애플리케이션 서버가 재시작됩니다. 전체 데이터가 전달되고 나면 기본 PAN에 적용한 추가 컨피그레이션 변

경 사항이 보조 노드에 복제됩니다. 보조 노드에 변경 사항을 복제하는 데 걸리는 시간은 네트워크 지연, 시스템의 로드 등 다양한 요인에 따라 달라집니다.

시작하기 전에

기본 PAN과 등록 대상 노드가 서로 DNS로 확인 가능한지 확인합니다. 등록 대상 노드에서 신뢰할 수 없는 자체 서명 인증서를 사용하는 경우 인증서 세부정보가 포함된 인증서 경고가 표시됩니다. 인증서를 수락하면 노드와의 TLS 통신을 활성화하기 위해 기본 PAN의 신뢰할 수 있는 인증서 저장소에 인증서가 추가됩니다.

노드가 자체 서명되지 않은 인증서(예: 외부 CA에서 서명하는 경우)를 사용하는 경우 해당 노드의 관련 인증서 체인을 기본 PAN의 신뢰할 수 있는 인증서 저장소에 수동으로 가져와야 합니다. 보조 노드의 인증서를 신뢰할 수 있는 인증서 저장소로 가져올 때는 PAN이 보조 노드의 인증서를 검증하도록 **Trusted Certificates(**신뢰할 수 있는 인증서**)** 창에서 **Trust for Authentication within ISE(ISE** 내의 인증 신뢰**)** 확인란을 선택합니다.

네트워크 액세스, 게스트, 포스처 등의 세션 서비스가 활성화된 노드를 등록하는 동안에는 이를 노드 그룹에 추가 할 수 있습니다. 자세한 내용은 정책 서비스 노드 그룹 생성, 92 페이지를 참조하십시오.

단계 **1** 기본 PAN에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**.

단계 **3** 보조 노드 등록을 시작하려면 **Register(**등록**)**를 클릭합니다.

단계 **4** 등록하려는 독립형 노드의 DNS 확인 가능 FQDN(Fully Qualified Domain Name)을 입력합니다(abc.xyz.com과 같이 호스트 이름.도메인 이름의 형식). 기본 PAN과 등록 대상 노드가 서로 확인 가능한지 확인합니다.

단계 **5** **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 보조 노드의 GUI 기반 관리자 자격 증명을 입력합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

기본 PAN이 등록 대상 노드와의 (최초) TLS 통신 설정을 시도합니다.

- 노드가 신뢰할 수 있는 인증서를 사용하는 경우 7단계를 진행할 수 있습니다.
- 노드에서 신뢰할 수 없는 자체 서명 인증서를 사용하는 경우 인증서 경고 메시지에는 인증서에 대한 세부정보(예: 발급 대상, 발급자, 일련번호 등)가 표시되며 이 정보를 노드의 실제 인증서와 비교하여 확인할 수 있습니다. **Import Certificate and Proceed(**인증서 가져 오기 및 진행**)** 옵션을 선택하여 이 인증서를 신뢰하고 등록을 계속할 수 있습니다. Cisco ISE는 해당 노드의 기본 자체 서명 인증서를 기본 PAN의 신뢰할 수 있는 인증서 저장소로 가져옵니다. 기본 자체 서명 인증서를 사용하지 않으려면 **Cancel Registration(**등록 취소**)**을 클릭하고 해당 노드의 관련 인증서 체인을 기본 PAN의 신뢰할 수 있는 인증서 저장소에 수동으로 가져옵니다. 보조 노드의 인증서를 신뢰할 수 있는 인증서 저장소로 가져올 때는 PAN이 보조 노드의 인증서를 검증하도록 **Trust for Authentication within ISE(ISE** 내의 인증 신뢰**)** 확인란을 선택합니다.
- 노드가 CA 서명 인증서를 사용하는 경우, 인증서 신뢰가 설정될 때까지 등록을 진행할 수 없다는 오류 메시지가 표시됩니다.

단계 **7** 노드에서 활성화할 페르소나 및 서비스를 선택하고 **Save(**저장**)**를 클릭합니다.

노드가 등록되면 노드 구축에 노드가 추가되었음을 확인하는 경보가 기본 PAN에 생성됩니다. Cisco ISE GUI **Dashboard(**대시보드**)**의 **Alarms(**경보**)** 대시릿에서 이 경보를 볼 수 있습니다. 등록된 노드가 동기화되고 재시작된 후, 기본 PAN에 사용된 동일한 자격 증명을 사용하여 보조 노드 GUI에 로그인할 수 있습니다.

다음에 수행할 작업

- 게스트 사용자, 액세스/권한 부여, 로깅 등 시간이 중요한 작업의 경우에는 노드의 시스템 시간이 동기화되는지 확인합니다.
- 보조 PAN을 등록했으며 내부 Cisco ISE CA 서비스를 사용하려는 경우에는 기본 PAN에서 Cisco ISE CA 인증서와 키를 백업한 다음 보조 PAN에서 이를 복원해야 합니다.

  Cisco ISE CA 인증서 및 키의 백업 및 복구 장의 *Cisco ISE CA* 인증서 및 키 백업 및 복원 섹션을 참조하십시오.

여러 구축 시나리오 지원

Cisco ISE는 802.1X 유선, 무선 및 VPN(Virtual Private Network)을 지원하는 엔터프라이즈 인프라 전반에 구축될 수 있습니다.

Cisco ISE 아키텍처는 독립형 및 분산형(고가용성 또는 리던던시*(redundancy)*라고도 함) 구축을 모두 지원합니다. 여기서 한 머신은 기본 역할을 맡고 다른 백업 머신은 보조 역할을 맡습니다. Cisco ISE는 구성 가능한 고유한 페르소나, 서비스 및 역할을 제공하며, 관리자는 이를 통해 네트워크에서 필요한 Cisco ISE 서비스를 생성하고 적용할 수 있습니다. 그 결과 완전한 기능을 갖춘 통합 시스템으로 작동하는 포괄적인 Cisco ISE 구축을 실현할 수 있습니다.

Cisco ISE 노드는 하나 이상의 관리, 모니터링 및 정책 서비스 페르소나를 사용하여 구축할 수 있습니다. 각 페르소나는 전반적인 네트워크 정책 관리 토폴로지에서 서로 다른 중요한 부분을 수행합니다. 관리 페르소나 역할의 Cisco ISE를 설치하면 중앙 집중식 포털에서 네트워크를 구성 및 관리하여 효율성과 사용 편의성을 높일 수 있습니다.

Cisco ISE 분산형 구축

여러 Cisco ISE 노드가 있는 구축을 분산형 구축이라고 합니다. 페일오버를 지원하고 성능을 개선하기 위해 분산된 형태로 여러 Cisco ISE 노드가 포함된 구축을 설정할 수 있습니다. Cisco ISE 분산 구축에서는 관리 및 모니터링 활동이 중앙 집중식으로 이루어지며 처리 작업은 PSN에 분산됩니다. 성능 요구 사항에 따라 구축을 확장할 수 있습니다. 구축의 각 Cisco ISE 노드는 관리, 정책 서비스 및 모니터링 페르소나를 취할 수 있습니다.

Cisco ISE 구축 설정

Cisco Identity Services Engine 하드웨어 설치 설명서에 설명된 것처럼 모든 노드에 Cisco ISE를 설치하고 나면 노드가 독립형 상태로 표시됩니다. 그러면 하나의 노드를 기본 PAN으로 정의해야 합니다. 기본 PAN을 정의하면서 해당 노드에서 관리 및 모니터링 페르소나를 활성화해야 합니다. 기본 PAN

에서 선택적으로 정책 서비스 페르소나를 활성화할 수 있습니다. 기본 PAN에서 페르소나를 정의하는 작업을 완료한 후에는 다른 보조 노드를 기본 PAN에 등록하고 보조 노드에 대한 페르소나를 정의할 수 있습니다.

모든 Cisco ISE 시스템 및 기능 관련 컨피그레이션은 기본 PAN에서만 수행되어야 합니다. 기본 PAN에서 수행한 컨피그레이션 변경 사항은 구축 환경의 모든 보조 노드로 복제됩니다.

분산형 구축에는 MnT 노드가 하나 이상 있어야 합니다. 기본 PAN을 구성할 때 모니터링 페르소나를 활성화해야 합니다. 구축에서 MnT 노드를 등록한 후 필요에 따라 기본 PAN을 편집하여 모니터링 페르소나를 비활성화할 수 있습니다.

기본 ISE 노드에서 보조 ISE 노드로의 데이터 복제

Cisco ISE 노드를 보조 노드로 등록하는 경우 Cisco ISE에서는 즉시 기본 노드에서 보조 노드로 연결되는 데이터 복제 채널을 생성하고 복제 프로세스를 시작합니다. 복제는 기본 노드에서 보조 노드로 Cisco ISE 컨피그레이션 데이터를 공유하는 프로세스입니다. 복제를 통해 구축의 일부에 해당하는 모든 Cisco ISE 노드에 있는 컨피그레이션 데이터 간에 일관성을 유지할 수 있습니다.

전체 복제는 일반적으로 Cisco ISE 노드를 처음 보조 노드로 등록하는 경우에 발생합니다. 증분 복제는 전체 복제 후에 발생하고, PAN 컨피그레이션 데이터의 추가, 수정 또는 삭제와 같이 새롭게 변경된 내용이 보조 노드에 반영되도록 합니다. 복제 프로세스를 사용하면 구축의 모든 Cisco ISE 노드를 동기화할 수 있습니다. Cisco ISE 관리 포털의 **Deployment(**구축**)** 창에 있는 **Node Status(**노드 상태**)** 열에서 복제 상태를 확인할 수 있습니다. Cisco ISE 노드를 보조 노드로 등록하거나 PAN과의 수동 동기화를 수행하는 경우 노드 상태에는 요청한 작업이 진행 중임을 의미하는 주황색 아이콘이 표시됩니다. 동기화 작업이 완료되면 노드 상태는 보조 노드가 PAN과 동기화되었음을 나타내는 녹색으로 바뀝니다.

Cisco ISE 노드 등록 취소

구축에서 노드를 제거하려면 노드 등록을 취소해야 합니다. 기본 PAN에서 보조 노드를 등록 취소하면 등록 취소된 노드의 상태가 독립형으로 변경되고 기본 노드와 보조 노드 간 연결이 끊어집니다. 업데이트는 더 이상 등록 취소된 독립형 노드로 전송되지 않습니다.

PSN의 등록을 취소하면 엔드포인트 데이터가 손실됩니다. PSN이 독립형 노드가 된 후 엔드포인트 데이터를 유지하도록 하려는 경우 다음 중 하나를 수행할 수 있습니다.

- 기본 PAN에서 백업을 가져온 다음 PSN이 독립형 노드가 되면 해당 노드에서 이 데이터 백업을 복구합니다.
- PSN의 페르소나를 관리(보조 PAN)로 변경하고 관리 포털의 **Deployment(**구축**)** 창에서 데이터를 동기화한 다음 노드 등록을 취소합니다. 이제 이 노드에 모든 데이터가 포함됩니다. 그런 다음 보조 PAN을 기존 구축에 추가할 수 있습니다.

참고 기본 PAN은 등록 취소할 수 없습니다.

분산형 구축을 설정하기 위한 지침

분산형 환경에서 Cisco ISE를 설정하기 전에 다음 정보를 신중히 읽어보십시오.

- Cisco ISE 서버에 대한 노드 유형을 선택합니다. 관리, 정책 서비스 및 모니터링 기능을 사용하려면 Cisco ISE 노드를 선택해야 합니다.
- 모든 노드에 대해 동일한 NTP(Network Time Protocol) 서버를 선택합니다. 노드 사이의 시간대 문제를 방지하려면 각 노드 설정 시 동일한 NTP 서버 이름을 제공해야 합니다. 이 설정을 사용하면 구축의 다양한 노드에서 제공하는 보고서 및 로그가 항상 타임스탬프와 동기화될 수 있습니다.
- Cisco ISE 설치 시 Cisco ISE 관리자 비밀번호를 구성합니다. 이전의 Cisco ISE 관리자 기본 로그인 자격 증명(admin/cisco)은 더 이상 유효하지 않습니다. 초기 설정 중에 생성된 사용자 이름 및 비밀번호나 현재 비밀번호(나중에 변경된 경우)를 사용합니다.
- DNS 서버 구성 DNS 서버에서 분산형 구축에 포함되는 모든 Cisco ISE 노드의 IP 주소 및 FQDN(Fully Qualified Domain Name)을 입력합니다. 그렇지 않으면 노드 등록이 실패합니다.
- DNS 서버의 분산형 구축에 있는 모든 Cisco ISE 노드에 대한 정방향 및 역방향 DNS 조회를 구성합니다. 그렇지 않으면 Cisco ISE 노드를 등록하고 다시 시작할 때 구축 관련 문제가 발생할 수 있습니다. 모든 노드에 대해 역방향 DNS 조회가 구성되지 않은 경우 성능이 저하될 수 있습니다.
- (선택 사항) Cisco ISE를 기본 PAN에서 제거하려면 보조 Cisco ISE 노드를 PAN에서 등록 취소합니다.
- 기본 MnT를 백업하고 데이터를 새 보조 MnT로 복구합니다. 이렇게 하면 새 변경 사항이 복제될 때 기본 MnT의 기록이 새 MnT와 동기화됩니다.
- 기본 PAN 및 보조 노드로 등록하려는 독립형 노드에서 동일한 버전의 Cisco ISE를 실행하고 있는지 확인합니다.
- 구축에 새 노드를 추가하는 동안 와일드카드 인증서의 발급자 인증서 체인이 새 노드에 대한 신뢰할 수 있는 인증서의 일부인지 확인합니다. 새 노드가 구축에 추가되면 와일드카드 인증서가 새 노드에 복제됩니다.
- Cisco TrustSec을 지원하도록 Cisco ISE 구축을 구성하거나 Cisco ISE가 Cisco DNA 센터와 통합된 경우 PSN을 SXP 전용으로 구성하지 마십시오. SXP는 Cisco TrustSec과 비 Cisco TrustSec 디바이스 간의 인터페이스입니다. SXP는 Cisco TrustSec 지원 네트워크 디바이스와 통신하지 않습니다.

기본 및 보조 노드에서 사용할 수 있는 메뉴 옵션

분산형 구축의 일부인 Cisco ISE 노드에서 사용할 수 있는 메뉴 옵션은 활성화되어 있는 페르소나에 따라 달라집니다. 모든 관리 및 모니터링 활동은 PAN(Primary Administration Node)을 통해 수행해야 합니다. 다른 작업은 보조 노드를 사용해야 합니다. 그러므로 보조 노드의 사용자 인터페이스는 해당 노드에 활성화되어 있는 페르소나에 따라 제한된 메뉴 옵션을 제공합니다.

한 노드에서 여러 페르소나를 맡고 있는 경우(예: 정책 서비스 페르소나 및 활성 역할이 있는 모니터링 페르소나) PSN 및 기본 Mnt에 대해서 나열된 메뉴 옵션을 해당 노드에서 사용할 수 있습니다.

다음 표에는 여러 페르소나를 맡고 있는 Cisco ISE 노드에서 사용할 수 있는 메뉴 옵션이 나와 있습니다.

표 ***4: Cisco ISE*** 노드 및 사용 가능한 메뉴 옵션

Cisco ISE 노드	사용 가능한 메뉴 옵션
모든 노드	• 시스템 시간 및 NTP 서버 설정을 보고 구성합니다. • 서버 인증서를 설치하고 인증서 서명 요청을 관리합니다. 모든 서버 인증서를 중앙에서 관리하는 기본 PAN을 통해 구축의 모든 노드에 대해 서버 인증서 작업을 수행할 수 있습니다. 참고 개인 키는 로컬 데이터베이스에 저장되지 않으며 관련 노드에서 복사되지도 않습니다. 개인 키는 로컬 파일 시스템에 저장됩니다.
기본 PAN(Policy Administration Node)	모든 메뉴 및 하위 메뉴
기본 모니터링 노드(기본 MnT 노드)	• 모니터링 데이터에 대한 액세스 제공 참고 **Operations(**운영**)** 메뉴는 기본 PAN에서만 볼 수 있습니다. Cisco ISE 2.1 이상의 모니터링 노드에는 **Operations(**운영**)** 메뉴가 표시되지 않습니다.
PSN(Policy Service Node)	Active Directory 도메인에 가입하거나 나가고 Active Directory 연결을 테스트할 수 있는 옵션이 있습니다. 각 PSN은 Active Directory 도메인에 개별적으로 가입해야 합니다. 먼저 도메인 정보를 정의하고 PAN을 Active Directory 도메인에 가입시킬 수 있습니다. 그런 다음 다른 PSN을 개별적으로 Active Directory 도메인에 가입시킬 수 있습니다.

Cisco ISE 노드	사용 가능한 메뉴 옵션
보조 PAN(Policy Administration Node)	보조 PAN을 기본 PAN으로 승격하는 옵션 참고 보조 노드를 기본 PAN으로 등록한 후에 보조 노드의 관리 포털에 로그인하는 동안 기본 PAN의 로그인 자격 증명을 사용해야 합니다.

구축 및 노드 설정

Deployment Nodes(구축 노드**)** 창에서는 Cisco ISE(PAN, PSN, MnT) 노드를 구성하고 구축을 설정할 수 있습니다.

구축 노드 목록 창

다음 표에서는 구축 환경에서 Cisco ISE 를 구성하는 데 사용할 수 있는 **Deployment Nodes List(**구축 노드 목록**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**입니다.

표 *5:* 구축 노드 목록

필드 이름	사용 지침
Hostname(호스트 이름**)**	노드의 호스트 이름을 표시합니다.
Personas(역할 분담**)**	(노드 유형이 Cisco ISE인 경우에만 나타남) Cisco ISE 노드가 맡은 페르소나를 나열합니다. 예: Administration(관리), Policy Service(정책 서비스), Monitoring(모니터링) 또는 pxGrid 예: **Administration(**관리**)**, **Policy Service(**정책 서비스**)**, **Monitoring(**모니터링**)** 또는 **pxGrid**
역할	현재 노드에서 이러한 페르소나가 활성화된 경우 관리 및 모니터링 페르소나가 맡은 역할 (기본, 보조 또는 독립형)을 나타냅니다. 역할은 다음 중 하나 이상일 수 있습니다. • **PRI(A)**: 기본 PAN을 나타냅니다. • **SEC(A)**: 보조 PAN을 나타냅니다. • **PRI(M)**: 기본 MnT를 나타냅니다. • **SEC(M)**: 보조 MnT를 나타냅니다.

필드 이름	사용 지침
서비스	(정책 서비스 페르소나가 활성화된 경우에만 나타남) 이 Cisco ISE 노드에서 실행되는 서비스를 나열합니다. 포함되는 서비스는 다음과 같습니다. • **ID** 매핑 • 세션 • 프로파일링 • 모두
Node Status(노드 상태**)**	구축 환경에서 데이터 복제에 대한 각 Cisco ISE 노드의 상태를 나타냅니다. • 녹색(연결됨): 구축 환경에 이미 등록되어 있는 Cisco ISE 노드가 기본 PAN과 동기화되어 있음을 표시합니다. • 빨간색(연결 끊김): Cisco ISE 노드가 연결할 수 없거나 작동 중지되었거나 데이터 복제가 발생하지 않음을 나타냅니다. • 주황색(진행 중): Cisco ISE 노드가 기본 PAN에 새로 등록되었거나 수동 동기화 작업을 수행했거나 Cisco ISE 노드가 기본 PAN과 동기화되지 않았음(동기화 중단)을 나타냅니다. 자세한 내용을 보려면 각 Cisco ISE 노드의 **Node Status(**노드 상태**)** 열에서 간단히 보기 아이콘을 클릭해 주십시오.

관련 항목

Cisco ISE 분산형 구축, 39 페이지
Cisco ISE 구축 용어, 36 페이지
Cisco ISE 노드 구성, 36 페이지
보조 Cisco ISE 노드 등록, 37 페이지

일반 노드 설정

다음 표에서는 Cisco ISE 노드의 **General Settings(**일반 설정**)** 창에 있는 필드에 대해 설명합니다. 이 창에서 노드에 페르소나를 할당하고 노드에서 실행할 서비스를 구성할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** > **Deployment Node(**구축 노드**)** > **Edit(**편집**)** > **General Settings(**일반 설정**)**입니다.

표 *6:* 일반 노드 설정

필드 이름	사용 지침
Hostname(호스트 이름**)**	Cisco ISE 노드의 호스트 이름을 표시합니다.
FQDN	Cisco ISE 노드의 인증된 도메인 이름(예: ise1.cisco.com)을 표시합니다.
IP Address(IP 주소**)**	Cisco ISE 노드의 IP 주소를 표시합니다.
Node Type(노드 유형**)**	노드 유형을 표시합니다.
Personas(역할 분담**)**	
Administration(관리**)**	Cisco ISE 노드가 관리 페르소나 역할을 하도록 지정하려면 이 토클 버큰을 활성화합니다. 관리 서비스 제공 라이선스가 있는 노드에서만 관리 페르소나를 활성화할 수 있습니다. **Role(**역할**)**: 구축에서 관리 페르소나에 대해 지정된 역할을 표시합니다. 페르소나는 **Standalone(**독립형**)**, **Primary(**기본**)**, **Secondary(**보조**)** 중 하나의 값을 가질 수 있습니다. **Make Primary(**기본으로 지정**)**: 이 노드를 기본 Cisco ISE 노드로 지정하려면 이 버튼을 클릭합니다. 기본 Cisco ISE 노드는 구축당 하나만 포함할 수 있습니다. 이 창의 다른 옵션은 이 노드를 기본으로 지정해야 활성화됩니다. 관리 노드는 구축당 두 개만 포함할 수 있습니다. 노드가 **Standalone(**독립형**)** 역할을 갖는 경우 노드 옆에 **Make Primary(**기본으로 지정**)** 버튼이 표시됩니다. 노드가 **Secondary(**보조**)** 역할을 갖는 경우 노드 옆에 **Promote to Primary(**기본으로 승격**)** 버튼이 표시됩니다. 노드가 **Primary(**기본**)** 역할을 갖고 등록된 다른 노드가 없는 경우 노드 옆에 **Make Standalone(**독립형으로 지정**)** 버튼이 표시됩니다. **Make Standalone(**독립형으로 지정**)** 버튼을 클릭하여 기본 노드를 독립형 노드로 지정할 수 있습니다.

필드 이름	사용 지침
Monitoring(모니터링**)**	

필드 이름	사용 지침
	Cisco ISE 노드가 모니터링 페르소나 역할을 하고 로그 컬렉터로 작동하도록 지정하려면 이 토글 버튼을 활성화합니다. 분산형 구축에는 모니터링 노드가 하나 이상 있어야 합니다. 기본 PAN을 구성할 때 모니터링 페르소나를 활성화해야 합니다. 구축에서 보조 모니터링 노드를 등록한 후 필요에 따라 기본 PAN을 편집하여 모니터링 페르소나를 비활성화할 수 있습니다. VMware 플랫폼에서 Cisco ISE 노드를 로그 컬렉터로 구성하려면 다음 지침을 참조하여 필요한 최소 디스크 공간(네트워크의 엔드포인트당 180KB, 네트워크의 Cisco ISE 노드당 매일 2.5MB)을 결정해 주십시오. 모니터링 노드에 포함할 데이터의 양(월 단위)을 기준으로 하여 필요한 최대 디스크 공간을 계산할 수 있습니다. 구축에 모니터링 노드가 하나뿐이면 독립형 역할이 지정됩니다. 구축에 모니터링 노드가 두 개인 경우 Cisco ISE에는 기본-보조 역할을 구성할 수 있도록 다른 모니터링 노드의 이름이 표시됩니다. 이러한 역할을 구성하려면 다음 중 하나를 선택합니다. • **Primary(**기본**)**: 현재 노드를 기본 모니터링 노드로 지정합니다. • **Secondary(**보조**)**: 현재 노드를 보조 모니터링 노드로 지정합니다. • **None(**없음**)**: 모니터링 노드에 기본-보조 역할을 지정하지 않으려는 경우에 선택합니다. 모니터링 노드 중 하나를 기본 또는 보조로 구성하는 경우 다른 모니터링 노드는 그에 따라 각각 보조 또는 기본 노드로 자동 지정됩니다. 기본 및 보조 모니터링 노드는 모두 관리 및 정책 서비스 로그를 수신합니다. 노드를 모니터링 노드로 지정한 후 모니터링 노드 하나의 역할을 **None(**없음**)**으로 변경하면 다른 모니터링 노드의 역할도 **None(**없음**)**이 되어 고가용성 페어가 취소됩니다. 이 노드는 **Remote Logging Targets(**원격 로깅 대상**)** 창에서 시스템 로그 대상으로 나열됩니다.. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Remote Logging Targets(**원격 로

필드 이름	사용 지침
	깅 대상**)**.

필드 이름	사용 지침
Policy Service(정책 서비스**)**	

필드 이름	사용 지침
	다음과 같은 서비스 중 하나 또는 전체를 활성화하려면 이 토글 버튼을 활성화합니다. • **Enable Session Services(**세션 서비스 활성화**)**: 네트워크 액세스, 포스처, 게스트 및 클라이언트 프로비저닝 서비스를 활성화하려면 이 확인란을 선택합니다. **Include Node in Node Group(**노드 그룹의 노드 포함**)** 드롭다운 목록에서 이 정책 서비스 노드가 속하는 그룹을 선택합니다. CA(Certificate Authority) 및 EST(Enrollment over Secure Transport) 서비스는 세션 서비스가 활성화된 정책 서비스 노드에서만 실행할 수 있습니다. **Include Node in Node Group(**노드 그룹의 노드 포함**)**에서 이 정책 서비스 노드를 그룹에 포함하지 않으려는 경우에는 **None(**없음**)**을 선택합니다. 동일한 노드 그룹 내의 모든 노드는 NAD(Network Access Device)에서 RADIUS 클라이언트로 구성되어야 하며 CoA에 대해 권한이 부여되어야 합니다. 이러한 노드 중 하나가 노드 그룹의 노드를 통해 설정된 세션에 대해 CoA 요청을 발급할 수 있기 때문입니다. 로드 밸런서를 사용하지 않는 경우 노드 그룹의 노드는 NAD에서 구성한 RADIUS 서버 및 클라이언트와 동일하거나 해당 서버 및 클라이언트의 하위 집합이어야 합니다. 이러한 노드는 RADIUS 서버로도 구성됩니다. 여러 Cisco ISE 노드를 사용하여 단일 NAD 노드를 RADIUS 서버 및 동적 권한 부여 클라이언트로 구성할 수는 있지만 모든 노드가 동일한 노드 그룹에 있을 필요는 없습니다. 노드 그룹의 멤버는 기가비트 이더넷과 같은 고속 LAN 연결을 사용하여 서로 연결되어야 합니다. 노드 그룹 멤버가 L2에 인접해 있을 필요는 없지만 충분한 대역폭과 연결 가능성을 보장하려면 L2에 인접하는 것이 좋습니다. 섹션을 참고하십시오. • **Enable Profiling Service(**프로파일링 서비스 활성화**)**: 프로파일링 서비스를 활성화하려면 이 확인란을 선택합니다. 프로파일링 서비스를 활성화하는 경우 **Profiling**

필드 이름	사용 지침
	Configuration(프로파일링 구성**)** 탭을 클릭하고 필요한 세부정보를 입력해야 합니다. 정책 서비스 노드에서 실행되는 서비스를 활성화/비활성화하거나 이 노드를 변경하는 경우에는 해당 서비스가 실행되는 애플리케이션 서버 프로세스가 재시작됩니다. 이러한 서비스가 다시 시작되는 동안에는 작업이 지연됩니다. CLI에서 **show application status ise** 명령을 사용하여 노드에서 애플리케이션 서버가 재시작된 시간을 확인할 수 있습니다. • **Enable Threat-Centric NAC Service(Threat Centric NAC** 서비스 활성화**)**: TC-NAC(Threat-Centric Network Access Control) 기능을 활성화하려면 이 체크 박스를 선택합니다. 이 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. • **Enable SXP Service(SXP** 서비스 활성화**)**: 노드에서 SXP 서비스를 활성화하려면 이 확인란을 선택합니다. SXP 서비스에 사용할 인터페이스도 지정해야 합니다. NIC 결합 또는 팀을 구성한 경우 결합된 인터페이스도 **Use Interface(**인터페이스 사용**)** 드롭다운 목록에 물리적 인터페이스와 함께 나열됩니다. • **Enable Device Admin Service(**디바이스 관리 서비스 활성화**)**: 네트워크 디바이스 구성을 제어하고 감사하기 위해 TACACS 정책 집합, 정책 결과 등을 생성하려면 이 확인란을 선택합니다.

필드 이름	사용 지침
	• **Enable Passive Identity Service(**패시브 **ID** 서비스 활성화**)**: ID 매핑 기능을 활성화하려면 이 확인란을 선택합니다. 이 기능을 사용하면 Cisco ISE가 아닌 도메인 컨트롤러에 의해 인증되는 사용자를 모니터링할 수 있습니다. Cisco ISE가 네트워크 액세스를 위해 사용자를 능동적으로 인증하지 않는 네트워크에서 ID 매핑 기능을 사용하여 Active Directory 도메인 컨트롤러에서 사용자 인증 정보를 수집할 수 있습니다.
pxGrid	pxGrid 페르소나를 활성화하려면 이 확인란을 선택합니다. Cisco pxGrid는 Cisco ISE 세션 디렉토리에서 Cisco ASA(Adaptive Security Appliance) 등의 다른 정책 네트워크 시스템으로 상황 민감 정보를 공유하는 데 사용됩니다. 또한 pxGrid 프레임워크를 사용하여 노드 간에 정책 및 구성 데이터를 교환하고(예: Cisco ISE와 서드파티 벤더 간에 태그 및 정책 개체 공유) 위협 정보와 같은 ISE와 관련이 없는 정보도 교환할 수 있습니다.

관련 항목

분산형 Cisco ISE 구축의 페르소나, 36 페이지
관리 노드, 62 페이지
정책 서비스 노드, 71 페이지
모니터링 노드, 75 페이지
Cisco pxGrid 노드, 83 페이지
기본 및 보조 Cisco ISE 노드 동기화, 90 페이지
정책 서비스 노드 그룹 생성, 92 페이지
Cisco pxGrid 노드 구축, 84 페이지
노드 페르소나 및 서비스 변경, 91 페이지
자동 페일오버용 MnT 노드 구성, 82 페이지

프로파일링 노드 설정

다음 표에서는 프로파일러 서비스용으로 프로브를 구성하는 데 사용할 수 있는 **Profiling Configuration(**프로파일링 컨피그레이션**)** 창의 필드에 대해 설명합니다. 이 창에 액세스하려면 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** > **ISE Node(ISE** 노드**)** > **Edit(**편집**)** > **Profiling Configuration(**프로파일링 컨피그레이션**)**을 클릭합니다.

표 *7:* 프로파일링 노드 설정

필드 이름	사용 지침
NetFlow	이 토글 버튼을 활성화하여 라우터에서 전송된 NetFlow 패킷을 수신하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 NetFlow를 사용하도록 설정합니다. 다음 옵션에 필요한 값을 입력합니다. • **Interface(**인터페이스**)**: Cisco ISE 노드의 인터페이스를 선택합니다. • **Port(**포트**)**: NetFlow에서 내보낸 패킷이 라우터에서 수신되는 NetFlow 리스너 포트 번호를 입력합니다. 기본 포트는 9996입니다.
DHCP	이 토글 버튼을 활성화하여 IP 도우미에서 DHCP 패킷을 수신하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 DHCP를 사용하도록 설정합니다. 다음 옵션에 필요한 값을 입력합니다. • **Interface(**인터페이스**)**: Cisco ISE 노드의 인터페이스를 선택합니다. • **Port(**포트**)**: DHCP 서버 UDP 포트 번호를 입력합니다. 기본 포트는 67입니다.
DHCP SPAN	이 토글 버튼을 활성화하여 DHCP 패킷을 수집하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 DHCP SPAN을 사용하도록 설정합니다. • **Interface(**인터페이스**)**: Cisco ISE 노드의 인터페이스를 선택합니다.
HTTP	이 토글 버튼을 활성화하여 HTTP 패킷을 수신하고 구문 분석하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 HTTP를 사용하도록 설정합니다. • **Interface(**인터페이스**)**: Cisco ISE 노드의 인터페이스를 선택합니다.
RADIUS	정책 서비스 페르소나가 지정된 ISE 노드 당 RADIUS가 Cisco ISO 센서 활성화 디바이스에서 RADIUS 세션 특성 및 CDP, LLDP 특성을 수집하도록 하려면 이 토글 버튼을 활성화합니다.

필드 이름	사용 지침
NMAP(Network Scan)	이 토글 버튼을 활성화하여 NMAP 프로브를 사용하도록 설정합니다.
DNS	이 토글 버튼을 활성화하여 FQDN에 대한 DNS 조회를 수행하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 DNS를 사용하도록 설정합니다. 시간 초과 기간을 초 단위로 입력합니다. 참고 분산형 구축의 특정 Cisco ISE 노드에서 DNS 프로브가 작동하도록 하려면 DHCP, DHCP SPAN, HTTP, RADIUS 또는 SNMP 프로브 중 하나를 활성화해야 합니다. DNS 조회의 경우에는 이러한 프로브 중 하나를 DNS 프로브와 함께 시작해야 합니다.
SNMP Query(SNMP 쿼리**)**	이 토글 버튼을 활성화하여 지정된 간격으로 네트워크 디바이스를 폴링하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 SNMP 쿼리를 사용하도록 설정합니다. **Retries(**재시도**)**, **Timeout(**시간 초과**)**, **Event Timeout(**이벤트 시간 초과**)** (필수) 및 **Description**(설명) (선택 사항)에 값을 입력합니다. 참고 이처럼 SNMP 쿼리 프로브를 구성해야 할 뿐 아니라**Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** 위치에서 다른 SNMP 설정도 구성해야 합니다. 네트워크 디바이스에서 SNMP 설정을 구성할 때는 네트워크 디바이스에서 CDP 및 LLDP를 전역적으로 활성화해야 합니다.

필드 이름	사용 지침
SNMP Trap(SNMP 트랩)	이 토글 버튼을 활성화하여 네트워크 디바이스에서 linkUp, linkDown 및 MAC 알림 트랩을 수신하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 SNMP 트랩 프로브를 사용하도록 설정합니다. 다음 정보를 제공하거나 활성화합니다. • **Link Trap Query(**링크 트랩 쿼리**)**: 이 토글 버튼을 활성화하여 SNMP 트랩을 통해 수신된 알림을 수신하고 해석합니다. • **MAC Trap Query(MAC** 트랩 쿼리**)**: 이 토글 버튼을 활성화하여 SNMP 트랩을 통해 수신된 MAC 알림을 수신하고 해석합니다. • **Interface(**인터페이스**)**: Cisco ISE 노드의 인터페이스를 선택합니다. • **Port(**포트**)**: 사용할 호스트의 UDP 포트를 입력합니다. 기본 포트는 162입니다.
Active Directory	이 토글 버튼을 활성화하여 정의된 Active Directory 서버에서 Windows 사용자에 대한 정보를 스캔합니다. • **Days before rescan(**다시 스캔할 때까지의 기간**(**일**))**: 스캔을 다시 실행할 날짜를 선택합니다.
pxGrid	이 토글 버튼을 활성화하여 Cisco ISE가 pxGrid를 통해 엔드포인트 속성을 수집(프로파일)할 수 있도록 허용합니다.

관련 항목

Cisco ISE 프로파일링 서비스, 688 페이지
프로파일링 서비스에 사용되는 네트워크 프로브, 692 페이지
Cisco ISE 노드에서 프로파일링 서비스 구성, 691 페이지

로깅 설정

다음 섹션에서는 디버그 로그의 심각도를 구성하고, 외부 로그 대상을 생성하고, Cisco ISE가 이러한 외부 로그 대상에 로그 메시지를 보낼 수 있도록 설정하는 방법에 대해 설명합니다.

원격 로깅 대상 설정

다음 표에서는 로깅 메시지를 저장하기 위한 외부 위치(시스템 로그 서버)를 생성하는 데 사용할 수 있는 **Remote Logging Targets(**원격 로깅 대상**)** 창의 필드에 대해 설명합니다. 이 창에 액세스하려면 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Remote Logging Targets(**원격 로깅 대상**)** 에서 **Add(**추가**)**를 클릭합니다.

표 ***8:*** 원격 로깅 대상 설정

필드 이름	사용 지침
Name(이름**)**	새 시스템 로그 대상의 이름을 입력합니다.
Target Type(대상 유형**)**	드롭다운 목록에서 대상 유형을 선택합니다. 기본값은 **UDP** 시스템 로그입니다.
Description(설명**)**	새 대상의 간략한 설명을 입력합니다.
IP Address(IP 주소**)**	로그를 저장할 대상 머신의 IP 주소 또는 호스트 이름을 입력합니다. Cisco ISE는 로깅에 IPv4 및 IPv6 형식을 지원합니다.
Port(포트**)**	대상 머신의 포트 번호를 입력합니다.
Facility Code(시설 코드**)**	드롭다운 목록에서 로깅에 사용할 시스템 로그 시설 코드를 선택합니다. 유효한 옵션은 Local0~Local7입니다.
Maximum Length(최대 길이**)**	원격 로그 대상 메시지의 최대 길이를 입력합니다. 유효한 값은 200~1024바이트입니다.
Buffer Message When Server Down(서버 다운 시 메시지 버퍼링**)**	이 확인란은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **TCP** 시스템 로그 또는 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. TCP 시스템 로그 대상 및 보안 시스템 로그 대상을 사용할 수 없을 때 Cisco ISE가 시스템 로그 메시지를 버퍼링하도록 하려면 이 확인란을 선택합니다. Cisco ISE는 대상에 연결을 재개할 때 대상에 대한 메시지 전송을 다시 시도합니다. 연결이 재개되면 메시지는 가장 오래된 것부터 시작하여 최신순으로 전송됩니다. 버퍼링된 메시지는 항상 새 메시지보다 먼저 전송됩니다. 버퍼가 가득 차면 오래된 메시지는 폐기됩니다.
Buffer Size (MB)(버퍼 크기**(MB))**	각 대상의 버퍼 크기를 설정합니다. 기본적으로 버퍼 크기는 100MB로 설정됩니다. 버퍼 크기를 변경하면 버퍼가 지워지며 특정 대상에 대해 기존에 버퍼링된 모든 메시지는 손실됩니다.

필드 이름	사용 지침
Reconnect Timeout (Sec)(다시 연결 시간 초과**(**초**))**	서버가 다운되었을 때 TCP 및 보안 시스템 로그를 폐기할 때까지 저장할 시간을 초 단위로 입력합니다.
Select CA Certificate(CA 인증서 선택**)**	이 드롭다운 목록은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. 드롭다운 목록에서 클라이언트 인증서를 선택합니다.
Ignore Server Certificate Validation(서버 인증서 검증 무시**)**	이 확인란은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. Cisco ISE가 서버 인증서 인증을 무시하고 모든 시스템 로그 서버를 수락하도록 하려면 이 확인란을 선택합니다.

로깅 범주 구성

다음 표에서는 로깅 범주를 구성하는 데 사용할 수 있는 필드에 대해 설명합니다. 로그 심각도 레벨을 설정하고 로깅 범주의 로그에 대한 로깅 대상을 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**입니다.이 창에 액세스하려면 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 클릭합니다.

보고자 하는 범주 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다. 다음 표에서는 로깅 범주의 편집 창에 표시되는 필드에 대해 설명합니다.

표 ***9:*** 로깅 범주 설정

필드 이름	사용 지침
Name(이름**)**	로깅 범주의 이름을 표시합니다.

필드 이름	사용 지침
Log Severity Level(로그 심각도 레벨**)**	일부 로깅 범주의 경우이 값은 기본적으로 설정되며 수정할 수 없습니다. 일부 로깅 범주의 경우 드롭다운 목록에서 다음 심각도 레벨 중 하나를 선택할 수 있습니다. • **FATAL**: 긴급 범주입니다. 이 레벨은 Cisco ISE를 사용할 수 없으며 필요한 조치를 즉시 수행해야 함을 의미합니다. • **ERROR**: 이 레벨은 심각한 오류 상태를 나타냅니다. • **WARN**: 이 레벨은 정상적이기는 하지만 중요한 상태를 나타냅니다. 이 레벨은 여러 로깅 범주에 대해 설정되는 기본 수준입니다. • **INFO**: 이 레벨은 정보 메시지를 나타냅니다. • **DEBUG**: 이 레벨은 진단 버그 메시지를 나타냅니다.
Local Logging(로컬 로깅**)**	로컬 노드의 범주에 대한 이벤트 로깅을 활성화하려면 이 확인란을 선택합니다.
Targets(대상**)**	이 영역에서는 왼쪽 및 오른쪽 화살표 아이콘을 사용하여 **Available(**사용 가능**)** 영역과 **Selected(**선택됨 **)** 영역 간에 대상을 전송하는 방식으로 로깅 범주에 대한 대상을 변경할 수 있습니다. **Available(**사용 가능**)** 상자에는 기존 로깅 대상이 포함되어 있습니다. 여기에는 미리 정의된 로컬 대상과 사용자가 정의한 외부 대상이 모두 포함됩니다. **Selected(**선택됨**)** 영역은 처음에는 비어 있으며, 이후에 이 범주에 대해 선택된 대상을 표시됩니다.

관리자 액세스 설정

이 섹션에서는 관리자용 액세스 설정을 구성할 수 있습니다.

관리자 비밀번호 정책 설정

다음 표에서는 **Password Policy(**비밀번호 정책**)** 탭의 필드에 대해 설명합니다. 이 탭을 사용하여 관리자 비밀번호가 충족해야 하는 기준을 정의할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Authentication(**인증**)** > **Password Policy(**비밀번호 정책**)** .

표 ***10:*** 관리자 비밀번호 정책 설정

필드 이름	사용 지침
최소 길이	최소 비밀번호 길이를 문자 단위로 지정합니다. 기본값은 6자입니다.

필드 이름	사용 지침
비밀번호는 다음을 포함할 수 없습니다.	관리자 이름 또는 그 문자를 역순으로 배열한 단어: 관리자 이름 또는 그 문자를 역순으로 배열한 단어의 사용을 제한하려면 이 확인란을 선택합니다.
	Cisco 또는 그 문자를 역순으로 배열한 단어: Cisco 또는 그 문자를 비밀번호의 역순으로 배열한 단어의 사용을 제한하려면 이 체크 박스를 선택합니다.
	이 단어 또는 그 문자를 역순으로 배열한 단어: 사용자가 정의한 특정 단어 또는 그 문자를 비밀번호의 역순으로 배열한 단어의 사용을 제한하려면 이 체크 박스를 선택합니다.
	4번 이상 반복되는 문자: 비밀번호에 4번 이상 반복되는 문자를 연속으로 사용하는 것을 제한하려면 이 체크 박스를 선택합니다.
	사전 단어**,** 반대 순서의 문자 또는 다른 문자로 교체 된 문자: 사전 단어의 비밀번호 사용을 제한하거나 반대 순서로 문자를 교체하거나 문자를 다른 문자로 교체하려면 이 확인란을 선택합니다. s를 $, a를 @, o를 0, l를 1, i를 !, e를 3으로 대체할 수 없습니다. 예를 들어 Pa$$w0rd는 허용되지 않습니다. • **Default Dictionary(**기본 사전**)**: Cisco ISE에서 기본 Linux 사전을 사용하려면 이 옵션을 선택합니다. 기본 사전에는 약 480,000개의 영어 단어가 포함되어 있습니다. 이 옵션은 기본적으로 선택되어 있습니다. • **Custom Dictionary(**맞춤형 사전**)**: 맞춤 설정한 사전을 사용하려면 이 옵션을 선택합니다. **Choose File(**파일 선택**)**을 클릭하여 맞춤형 사전 파일을 선택합니다. 텍스트 파일은 새 줄 구분된 단어, .dic 확장자여야 하며 크기가 20MB 미만이어야 합니다.

필드 이름	사용 지침
Password must contain at least one character of each of the selected types(비밀번호는 선택한 유형별로 하나 이상의 문자를 포함해야 함**)**	관리자 비밀번호에 포함해야 하는 문자 유형에 대한 확인란을 선택합니다. 다음 옵션 중 하나 이상을 선택합니다. • 소문자 알파벳 문자 • 대문자 알파벳 문자 • 숫자 • 영숫자 이외의 문자
Password History(비밀번호 기록**)**	같은 비밀번호를 반복적으로 사용하지 못하도록 하기 위해, 새로 입력하는 비밀번호와 달라야 하는 이전 비밀번호의 수를 지정합니다. **Password must be different from the previous *n*versions(**비밀번호는 이전 **n** 버전과 달라야 함**)** 확인란을 선택하고 해당 필드에 번호를 입력합니다. 비밀번호를 재사용할 수 있을 때까지의 기간을 일 단위로 입력합니다. **Cannot reuse password within *n* days(n**일 이내에 비밀번호를 재사용 할 수 없음**)** 확인란을 선택하고 해당 필드에 번호를 입력합니다.
Password Lifetime(비밀번호 수명**)**	사용자가 지정된 기간 이후 비밀번호를 변경해야 하도록 강제 지정하려면 확인란을 선택합니다. • 관리자 비밀번호는 생성 또는 마지막 변경 이후 ***n***일 후에 만료: 비밀번호를 변경하지 않으면 관리자 계정을 비활성화할 때까지의 시간(일))입니다. 유효한 범위는 1일~3650일입니다. • 비밀번호 만료 ***n***일 전에 관리자에게 이메일 알림 보내기: 비밀번호가 만료 될 것임을 관리자에게 알리기 전까지의 시간(일)입니다. 유효한 범위는 1일~3650일입니다.
네트워크 디바이스 민감한 데이터 표시	
Require Admin Password(관리자 비밀번호 필요**)**	공유 암호 및 비밀번호와 같은 네트워크 디바이스의 민감한 데이터를 확인하기 위해 관리 사용자가 로그인 비밀번호를 입력해야 하도록 지정하려면 이 체크 박스를 선택합니다.

필드 이름	사용 지침
Password cached for *n* Minutes(n분 동안 비밀번호 캐시**)**	관리 사용자가 입력한 비밀번호가 이 기간 동안 캐시됩니다. 이 기간 동안에는 관리 사용자가 네트워크 디바이스의 민감한 데이터를 볼 때 비밀번호를 다시 입력하라는 메시지가 표시되지 않습니다. 유효 범위는 1분~60분입니다.

관련 항목

Cisco ISE 관리자, 3 페이지
새 관리자 생성, 5 페이지

세션 시간 초과 및 세션 정보 설정

다음 표에서는 세션 시간 초과를 정의하고 활성 관리 세션을 종료하는 데 사용할 수 있는 **Session(**세션**)** 창의 필드에 대해 설명합니다. 이 창에 액세스하려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Settings(**설정**)** > **Session(**세션**)**을 선택합니다.

표 ***11:*** 세션 시간 초과 및 세션 정보 설정

필드 이름	사용 지침
세션 시간 초과	
Session Idle Timeout(세션 유휴 시간 초과**)**	작업을 수행하지 않는 경우 관리자가 로그아웃될 때까지 Cisco ISE가 대기하도록 할 시간을 분 단위로 입력합니다. 기본값은 60분입니다. 유효 범위는 6분~100분입니다.
세션 정보	
Invalidate(무효화**)**	종료할 세션 ID 옆의 확인란을 선택하고 **Invalidate(**무효화**)**를 클릭합니다.

관련 항목

관리자 액세스 설정, 242 페이지
관리자에 대한 세션 시간 초과 구성, 246 페이지
활성 관리 세션 종료, 246 페이지

관리 노드

관리 페르소나의 Cisco ISE 노드에서는 Cisco ISE에 대한 모든 관리 작업을 수행할 수 있습니다. 인증, 권한 부여, 감사 등과 같은 기능과 관련된 모든 시스템 관련 컨피그레이션을 처리합니다. 분산형 환경에서는 최대 두 개의 노드에서 관리 페르소나를 실행할 수 있습니다. 관리 페르소나는 독립형, 기본 또는 보조 역할 중 하나를 맡을 수 있습니다.

관리 노드의 고가용성

고가용성 구성에서 기본 PAN(Policy Administration Node)은 활성 상태입니다. 보조 PAN은 대기 상태입니다. 즉, 기본 PAN에서 모든 구성 업데이트를 수신하지만 Cisco ISE 네트워크에서는 활성 상태가 아닙니다.

Cisco ISE는 수동 및 자동 페일오버를 지원합니다. 자동 페일오버를 사용하는 경우 기본 PAN이 다운되면 보조 PAN의 자동 승격이 시작됩니다. 자동 페일오버에는 비관리 보조 노드(상태 확인 노드라고 함)가 필요합니다. 상태 확인 노드는 기본 PAN의 상태를 확인합니다. 기본 PAN이 작동 중지되거나 연결 불가능한 상태로 탐지될 경우 상태 확인 노드는 보조 PAN을 승격하여 기본 역할을 인계하도록 합니다.

자동 페일오버 기능을 구축하려면 노드가 3개 이상 있어야 합니다. 여기서 노드 2개는 관리 페르소나이고 노드 1개는 상태 확인 노드로 작동합니다. 상태 확인 노드는 비관리 노드이며 PSN, MnT 또는 pxGrid 노드이거나 이러한 노드의 조합일 수 있습니다. 기본 PAN과 보조 PAN이 서로 다른 데이터 센터에 있는 경우 각 PAN에 대해 상태 확인 노드가 있어야 합니다.

다음 표에는 PAN이 작동 중지될 경우 보조 PAN에서 인계해야 하는 영향을 받는 기능이 나와 있습니다.

기능 이름	기본 **PAN**이 작동 중지된 경우 사용 가능한지 여부 **(**예**/**아니요**)**
기존 내부 사용자 RADIUS 인증	예
기존 또는 신규 AD 사용자 RADIUS 인증	예
프로파일이 변경되지 않은 기존 엔드포인트	예
프로파일이 변경된 기존 엔드포인트	아니요
프로파일링을 통해 학습된 신규 엔드포인트	No(아니요)
기존 게스트: LWA(Local Web Authentication)	예
기존 게스트: CWA(Central Web Authentication)	예(자동 디바이스 등록 기능이 있는 핫스팟, BYOD 및 CWA와 같이 디바이스 등록용으로 활성화된 플로우는 제외)
게스트 변경 비밀번호	아니요
게스트: AUP	No(아니요)
게스트: 실패한 최대 로그인 횟수	아니요
새 게스트(스폰서 또는 셀프 등록)	아니요
포스처	예
내부 CA가 있는 BYOD	아니요

기능 이름	기본 **PAN**이 작동 중지된 경우 사용 가능한지 여부 **(**예**/**아니요**)**
기존에 등록된 디바이스	예
MDM 온보딩	아니요
pxGrid 서비스	아니요
보조 노드의 GUI 로그인	예(마지막 로그인 세부정보를 업데이트하기 위해 PAN에 대한 차단 호출이 시도되어 로그인 프로세스가 지연되며, 이 호출이 시간 초과되면 로그인이 진행됨)

내부 CA(Certificate Authority)를 사용하는 인증서 프로비저닝을 지원하기 위해 승격 후 원래 기본 PAN 및 해당 키가 포함된 루트 인증서를 새 기본 노드로 가져와야 합니다. 보조 노드가 기본 PAN으로 승격된 이후에 추가된 PSN 노드가 자동으로 페일오버될 경우 인증서 프로비저닝이 작동하지 않습니다.

고가용성 상태 확인 노드

기본 PAN의 상태 확인 노드를 활성 상태 확인 노드라고 합니다. 보조 PAN의 상태 확인 노드를 비활성 상태 확인 노드라고 합니다. 활성 상태 확인 노드는 기본 PAN의 상태를 확인하고 관리 노드의 자동 페일오버를 관리합니다. 2 개의 비-관리 ISE 노드를 상태 확인 노드로 사용하는 것이 좋습니다. 하나는 기본, 다른 하나는 보조 PAN용입니다. 상태 확인 노드를 하나만 사용하는 경우 해당 노드가 다운되면 자동 페일오버가 수행되지 않습니다.

두 PAN이 동일한 데이터 센터에 있는 경우, 단일 비-관리 ISE 노드를 기본 PAN 및 보조 PAN 모두에 대한 상태 확인 노드로 사용할 수 있습니다. 단일 상태 확인 노드가 기본 및 보조 PAN의 상태를 모두 확인하는 경우 활성 역할과 비활성 역할을 동시에 수행합니다.

상태 확인 노드는 비관리 노드이며 정책 서비스, 모니터링 또는 pxGrid 노드이거나 이러한 노드의 조합일 수 있습니다. 관리 노드와 같은 데이터 센터에 있는 PSN 노드를 상태 확인 노드로 지정하는 것이 좋습니다. 그러나 관리 노드 두 개가 같은 위치(LAN 또는 데이터 센터)에 있는 소규모 또는 중앙 집중식 구축의 경우에는 관리 페르소나를 포함하지 않는 모든 노드(PSN/pxGrid/MnT)를 상태 확인 노드로 사용할 수 있습니다.

자동 페일오버를 활성화하지 않기로 하고 기본 PAN에 장애가 발생했을 때 보조 노드의 수동 승격에 의존하는 경우에는 확인 노드가 필요하지 않습니다.

보조 **PAN**의 상태 확인 노드

보조 PAN의 상태 확인 노드는 비활성 모니터입니다. 이 노드는 보조 PAN이 기본 PAN으로 승격될 때까지 아무 조치도 수행하지 않습니다. 보조 PAN이 기본 PAN으로 승격되면 관련 상태 확인 노드가 관리 노드의 자동 페일오버를 관리하는 활성 역할을 하게 됩니다. 그러면 이전 기본 PAN의 상태 확인 노드는 이제 보조 PAN의 상태 확인 노드로서 비활성 모니터링을 수행하게 됩니다.

상태 확인 비활성화 및 재시작

상태 확인 역할에서 노드가 제거되거나 자동 페일오버 컨피그레이션이 비활성화되면 해당 노드에서 상태 확인 서비스가 중지됩니다. 지정된 고가용성 상태 확인 노드에서 자동 페일오버 컨피그레이션을 활성화하면 노드가 관리 노드의 상태 확인을 다시 시작합니다. 노드에서 고가용성 상태 확인 역할을 지정하거나 제거할 때는 해당 노드에서 애플리케이션이 다시 시작되지 않으며 상태 확인 작업만 시작되거나 중지됩니다.

고가용성 상태 확인 노드는 다시 시작되는 경우 기본 PAN의 이전 다운타임을 무시하고 상태 확인을 새로 시작합니다.

상태 확인 노드

활성 상태 확인 노드는 구성된 폴링 간격으로 기본 PAN의 상태를 확인합니다. 상태 확인 노드는 기본 PAN에 요청을 보내며, 수신되는 응답이 컨피그레이션과 일치하면 기본 PAN을 정상 상태로 간주하고 그렇지 않은 경우에는 기본 PAN을 비정상 상태로 간주합니다. 기본 PAN의 상태가 구성된 페일오버 기간을 초과해서 계속 비정상인 경우 상태 확인 노드가 보조 PAN에 대한 페일오버를 시작합니다.

상태 확인 중에 언제든지 이전에 페일오버 기간 내에 비정상으로 보고된 상태가 정상으로 확인된 경우 상태 확인 노드는 기본 PAN 상태를 정상으로 표시하고 상태 확인 주기를 재설정합니다.

기본 PAN의 상태 확인 응답은 상태 확인 노드에서 사용할 수 있는 컨피그레이션 값을 기준으로 검증됩니다. 응답이 해당 값과 일치하지 않으면 경보가 발생됩니다. 단, 승격 요청은 보조 PAN으로 전송됩니다.

상태 노드 변경

상태 확인에 사용 중인 Cisco ISE 노드를 변경할 수 있지만, 몇 가지 사항을 고려해야 합니다.

상태 확인 노드(H1)가 동기화되지 않은 상태에서 다른 노드(H2)가 기본 PAN의 상태 확인 노드로 지정되는 경우를 예로 들어 보겠습니다. 이러한 경우 기본 PAN이 다운되면 H1은 다른 노드(H2)가 같은 기본 PAN을 확인 중인지 알 수 없습니다. 이후 H2도 다운되거나 네트워크에서 연결이 끊기면 실제로 페일오버를 수행해야 합니다. 그러나 보조 PAN에는 승격 요청을 거부할 권한이 있습니다. 따라서 보조 PAN이 기본 역할로 승격되면 H2의 승격 요청이 오류와 함께 거부됩니다. 기본 PAN의 상태 확인 노드는 동기화되지 않은 상태이더라도 기본 PAN의 상태를 계속 확인합니다.

보조 **PAN**에 대한 자동 페일오버

기본 PAN을 사용할 수 없을 때 보조 PAN을 자동으로 승격하도록 Cisco ISE를 구성할 수 있습니다. 컨피그레이션은 **Deployment(**구축**)** 창의 기본 정책 관리 노드(기본 PAN)에서 수행됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다. 페일오버 기간은 **Number of Failure Polls Before Failover(**페일오버 전의 오류 폴링 횟수**)**에서 구성된 횟수에 **Polling Interval(**폴링 간격**)**에 설정된 시간(초)으로 정의됩니다. 기본 컨피그레이션의 경우 10분입니다. 보조 PAN을 기본 PAN으로 승격하는 데 10분이 더 소요됩니다. 따라서 기본 PAN 오류에서 보조 PAN 작동까지 걸리는 총 시간은 대개 20분입니다.

보조 PAN이 페일오버 호출을 받으면 실제 페일오버를 진행하기 전에 먼저 다음과 같은 검증을 수행합니다.

- 기본 PAN은 네트워크에서 사용할 수 없습니다.
- 페일오버 요청이 유효한 상태 확인 노드에서 발생했습니다.
- 이 PAN에 대한 페일오버 요청입니다.

모든 검증을 통과한 경우 보조 PAN은 자신을 기본 역할로 승격시킵니다.

다음은 보조 PAN의 자동 페일오버가 시도되는 몇 가지 샘플 시나리오입니다(이에 국한되지 않음).

- 기본 PAN의 상태는 폴링 기간 동안 **Number of failure polls before failover(**페일오버 전의 오류 폴링 횟수**)** 값에 대해 지속적으로 양호하지 않습니다.
- 기본 PAN의 Cisco ISE 서비스는 수동으로 중지되며 페일오버 기간 동안 중지된 상태로 유지됩니다.
- 기본 PAN은 소프트 중지 또는 재부팅 옵션을 통해 종료되며 구성된 페일오버 기간 동안 종료된 상태로 유지됩니다.
- 기본 PAN이 갑작스레 다운(전원 꺼짐)되고 페일오버 기간 동안 다운된 상태로 유지됩니다.
- 기본 PAN의 네트워크 인터페이스가 다운(네트워크 포트 종료 또는 네트워크 서비스 다운)되거나 다른 이유로 상태 확인 노드에서 연결할 수 없으며, 설정된 페일오버 기간 동안 다운된 상태로 유지됩니다.

상태 확인 노드 재시작

다시 시작하면 고가용성 상태 확인 노드가 기본 PAN의 이전 다운타임을 무시하고 상태 확인을 새로 시작합니다.

보조 **PAN**에 대한 자동 페일오버가 수행된 경우의 **BYOD(Bring Your Own Device)**

기본 PAN이 다운되더라도 기본 PAN 루트 CA 체인에서 이미 발급한 인증서가 있는 엔드포인트에 대한 인증은 중단되지 않습니다. 이는 구축의 모든 노드가 신뢰 및 검증을 위해 전체 인증서 체인을 가지고 있기 때문입니다.

그러나 보조 PAN이 기본으로 승격될 때까지 새 BYOD 디바이스는 온보딩되지 않습니다. BYOD 온보딩에는 활성 기본 PAN이 필요합니다.

원래의 기본 PAN이 복구되거나 보조 PAN이 승격되면 새 BYOD 엔드포인트가 문제없이 온보딩됩니다.

장애가 발생한 기본 PAN을 기본 PAN으로 재참가시킬 수 없는 경우 새로 승격된 기본 PAN(원래 보조 PAN)에서 루트 CA 인증서를 다시 생성합니다.

기존 인증서 체인의 경우 새 루트 CA 인증서를 트리거하면 하위 CA 인증서가 자동으로 생성됩니다. 새 하위 인증서가 생성되는 경우에도 이전 체인에서 생성된 엔드포인트 인증서는 계속 유효합니다.

자동 페일오버가 차단되는 샘플 시나리오

아래에서는 상태 확인 노드에 의한 자동 페일오버가 차단되거나 보조 노드로의 승격 요청이 거부되는 사례를 나타내는 몇 가지 샘플 시나리오가 나와 있습니다.

- 승격 요청을 수신하는 노드가 보조 노드가 아님
- 보조 PAN에서 수신한 승격 요청에 올바른 기본 PAN 정보가 포함되어 있지 않음
- 승격 요청이 잘못된 상태 확인 노드에서 수신됨
- 승격 요청이 수신되었지만 기본 PAN이 작동 중이며 정상 상태임
- 승격 요청을 수신하는 노드가 동기화되지 않은 상태임

PAN 자동 페일오버 기능의 영향을 받는 기능

다음 표에는 구축에서 PAN 자동 페일오버 구성이 활성화되어 있는 경우 차단되거나 구성을 추가로 변경해야 하는 기능이 나와 있습니다.

기능	영향 세부정보
차단되는 작업	
업그레이드	CLI를 통한 업그레이드가 차단됩니다. 이전 버전의 Cisco ISE에서 릴리스 1.4로 업그레이드하고 나면 PAN 자동 페일오버 기능의 구성이 가능해집니다. 이 기능은 기본적으로 비활성화됩니다. 자동 페일오버 기능을 구축하려면 노드가 3개 이상 있어야 합니다. 여기서 노드 2개는 관리 페르소나로 지정되며 노드 1개는 상태 확인 노드로 작동합니다. 상태 확인 노드는 비관리 노드이며 PSN, MnT 또는 pxGrid 노드이거나 이러한 노드의 조합일 수 있습니다. PAN이 서로 다른 데이터 센터에 있는 경우 각 PAN의 상태 확인 노드가 있어야 합니다.
백업의 복원	CLI 및 사용자 인터페이스를 통한 복원이 차단됩니다. 복구 전에 PAN 자동 페일오버 구성을 활성화한 경우에는 정상적인 복구 이후에 PAN 자동 페일오버를 재구성해야 합니다.

기능	영향 세부정보
노드 페르소나 변경	사용자 인터페이스를 통한 다음 노드 페르소나 변경이 차단됩니다. • 기본 및 보조 PAN의 관리 페르소나 • PAN의 페르소나 • PAN 자동 페일오버 기능 활성화 이후의 상태 확인 노드 등록 취소
기타 CLI 작업	CLI를 통한 다음 관리 작업이 차단됩니다. • 패치 설치 및 롤백 • DNS 서버 변경 • eth1, eth2 및 eth3 인터페이스의 IP 주소 변경 • eth1, eth2 및 eth3 인터페이스의 호스트 별칭 변경 • 표준 시간대 변경
기타 관리 포털 작업	사용자 인터페이스를 통한 다음 관리 작업이 차단됩니다. • 패치 설치 및 롤백 • HTTPS 인증서 변경 • 비밀번호 기반 인증과 인증서 기반 인증 간의 관리 인증 유형 변경
최대 수의 디바이스가 연결된 사용자는 연결할 수 없음	일부 세션 데이터가 장애가 발생한 PAN에 저장되며 PSN에서 업데이트될 수 없습니다.
PAN 자동 페일오버를 비활성화해야 하는 작업	

기능	영향 세부정보
CLI 작업	PAN 자동 페일오버 구성이 활성화되어 있는 경우 CLI를 통해 다음 관리 작업을 수행할 때 경고 메시지가 표시됩니다. 이러한 작업을 수행할 때 페일오버 기간 이내에 서비스 또는 시스템을 다시 시작하지 않으면 자동 페일오버가 트리거될 수 있습니다. 따라서 다음 작업을 수행하는 동안에는 PAN 자동 페일오버 구성을 비활성화하는 것이 좋습니다. • Cisco ISE 서비스 수동 중지 • 관리 CLI를 사용한 Cisco ISE 소프트 재로드(재부팅)

자동 페일오버를 위한 기본 **PAN** 구성

시작하기 전에

자동 페일오버 기능을 구축하려면 노드가 3개 이상 있어야 합니다. 여기서 노드 2개는 관리 페르소나로 지정되며 노드 1개는 상태 확인 노드로 작동합니다. 상태 확인 노드는 비관리 노드이며 PSN, MnT 또는 pxGrid 노드이거나 이러한 노드의 조합일 수 있습니다. PAN이 서로 다른 데이터 센터에 있는 경우 각 PAN의 상태 확인 노드가 있어야 합니다.

단계 **1** 기본 PAN의 사용자 인터페이스에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** > **PAN Failover(PAN** 페일오버**)**를 선택합니다.

단계 **3** **Enable PAN Auto Failover(PAN** 자동 페일오버 활성화**)** 확인란을 선택하여 기본 PAN의 자동 페일오버를 활성화합니다.

보조 PAN만 기본 PAN으로 승격할 수 있습니다. PSN, MnT, pxGrid 노드 또는 이러한 노드의 조합으로만 지정된 Cisco ISE 노드는 기본 PAN으로 승격할 수 없습니다.

단계 **4** 사용 가능한 모든 보조 노드가 포함되어 있는 **Primary Health Check Node(**기본 상태 확인 노드**)** 드롭다운 목록에서 기본 PAN의 상태 확인 노드를 선택합니다.

이 노드는 기본 PAN과 동일한 위치 또는 데이터 센터에 있는 것이 좋습니다.

단계 **5** 사용 가능한 모든 보조 노드가 포함되어 있는 **Secondary Health Check Node(**보조 상태 확인 노드**)** 드롭다운 목록에서 보조 PAN용 상태 확인 노드를 선택합니다.

이 노드는 보조 PAN과 동일한 위치 또는 데이터 센터에 있는 것이 좋습니다.

단계 **6** **Polling Interval(**폴링 간격**)** 시간을 입력합니다. 이 시간이 지나면 PAN 상태를 확인합니다. 유효 범위는 30~300초입니다.

단계 **7** **Number of Failure Polls before Failover(**페일오버 전의 오류 폴링 횟수**)**에 대한 횟수를 입력합니다.

지정한 오류 폴링 횟수 동안 PAN의 상태가 정상이 아닌 경우 페일오버가 수행됩니다. 유효 범위는 2~60개입니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

보조 PAN을 기본 PAN으로 승격한 후 다음을 수행합니다.

- 이전 기본 PAN을 수동으로 동기화하여 구축으로 다시 가져옵니다.
- 동기화 상태가 아닌 다른 보조 노드를 수동으로 동기화하여 구축으로 다시 가져옵니다.

보조 PAN을 기본으로 수동 승격

PAN 자동 페일오버를 구성하지 않은 상태에서 기본 PAN에 오류가 발생하는 경우 보조 PAN을 수동으로 승격하여 새 기본 PAN으로 지정해야 합니다.

시작하기 전에

기본 PAN으로 승격하려는 관리 페르소나가 지정된 두 번째 Cisco ISE 노드를 구성했는지 확인해 주십시오.

단계 **1** 보조 PAN의 사용자 인터페이스에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

단계 **3** **Edit Node(**노드 편집**)** 창에서 **Promote to Primary(**기본으로 승격**)**를 클릭합니다.

보조 PAN만 기본 PAN으로 승격할 수 있습니다. 정책 서비스 또는 모니터링 페르소나 중 하나 또는 두 가지가 모두 지정된 Cisco ISE 노드는 기본 PAN으로 승격할 수 없습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

원래 기본 PAN이었던 노드가 다시 작동하면 승격된 노드는 자동으로 강등되며 보조 PAN이 됩니다. 이 노드(원래 기본 PAN)에서 수동 동기화를 수행하여 구축으로 다시 가져와야 합니다.

보조 노드의 노드 편집 창에서는 옵션이 비활성화되어 있으므로 페르소나 또는 서비스를 수정할 수 없습니다. 변경을 수행하려면 관리 포털에 로그인해야 합니다.

기존 Cisco ISE 구축 노드를 새 Cisco ISE 구축을 위한 기본 PAN으로 재사용

기존 Cisco ISE 구축의 노드를 새 Cisco ISE 구축의 기본 PAN으로 재사용하려는 경우 다음 단계를 수행해야 합니다.

단계 **1** 먼저 사용중인 Cisco ISE 버전에 대한 Cisco ISE 설치 가이드에 설명된 대로 Cisco ISE 유틸리티 "Perform System Erase"를 실행합니다. https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

단계 **2** Cisco ISE 설치 가이드에 설명된 대로 Cisco ISE를 새로 설치합니다.

단계 **3** 기본 PAN(Policy Administration Node) 구성, 37 페이지를 참조하여 독립형 노드를 기본 정책 관리 노드로 구성합니다.

기본 PAN에 서비스 복원

Cisco ISE에서는 원래 기본 PAN으로의 자동 대체를 지원하지 않습니다. 보조 PAN에 대한 자동 페일오버가 시작된 후 원래의 기본 PAN을 네트워크로 다시 가져오는 경우에는 보조 PAN으로 구성해야 합니다.

관리 노드에 대한 자동 페일오버 지원

Cisco ISE는 관리 페르소나에 대한 자동 페일오버를 지원합니다. 자동 페일오버 기능을 활성화하려면 분산 설정에서 적어도 2개의 노드를 관리 페르소나로 지정하고 한 노드를 비관리 페르소나로 지정해야 합니다. 기본 PAN이 다운되면 보조 PAN의 자동 승격이 시작됩니다. 이런 이유로 비관리 보조 노드가 각 PAN에 대한 상태 확인 노드로 지정됩니다. 상태 확인 노드가 구성한 간격으로 기본 PAN의 상태를 확인합니다. 디바이스가 다운되었거나 연결할 수 없는 등의 이유로 기본 PAN에 대해 수신된 상태 확인 응답이 정상 상태가 아닌 경우 상태 확인 노드는 구성한 임계치만큼 기다렸다가 기본 역할을 인계받을 수 있도록 보조 PAN의 승격을 시작합니다. 보조 PAN의 자동 페일오버 이후에 사용할 수 없는 몇 가지 기능이 있습니다. Cisco ISE는 원래 기본 PAN으로의 대체를 지원하지 않습니다. 자세한 내용은 관리 노드의 고가용성 섹션을 참고하십시오.

정책 서비스 노드

PSN(Policy Service Node)은 정책 서비스 페르소나의 Cisco ISE 노드이며 네트워크 액세스, 포스처, 포스처, 게스트 액세스, 클라이언트 프로비저닝, 프로파일링 서비스를 제공합니다.

분산 설정에서 하나 이상의 노드가 정책 서비스 페르소나를 맡아야 합니다. 이 페르소나는 정책을 평가하고 모든 결정을 내립니다. 일반적으로 분산형 구축에는 두 개 이상의 PSN이 있습니다.

같은 고속 LAN(Local Area Network)이나 로드 밸런서 뒤에 있는 모든 PSN은 함께 그룹화하여 하나의 노드 그룹을 만들 수 있습니다. 노드 그룹의 노드 중 하나에 장애가 발생하면 다른 노드가 장애를 탐지하고 URL로 리디렉션된 세션을 재설정합니다.

정책 서비스 노드의 고가용성

노드 장애를 탐지하고 장애가 발생한 노드에서 URL이 리디렉션된 모든 세션을 재설정하려는 경우에는 같은 노드 그룹에 둘 이상의 PSN을 배치할 수 있습니다. 노드 그룹에 속한 노드에 장애가 발생하면 동일한 노드 그룹의 다른 노드가 장애 발생 노드의 URL이 리디렉션된 모든 세션에 대해 CoA(Change of Authorization)를 실행합니다.

동일한 노드 그룹 내의 모든 노드는 NAD(Network Access Device)에서 RADIUS 클라이언트로 구성되어야 하며 CoA에 대해 권한이 부여되어야 합니다. 이러한 노드 중 하나가 노드 그룹의 노드를 통해 설정된 세션에 대해 CoA 요청을 발급할 수 있기 때문입니다. 로드 밸런서를 사용하지 않는 경우 노드 그룹의 노드는 NAD에서 구성한 RADIUS 서버 및 클라이언트와 동일하거나 해당 서버 및 클라이언트의 하위 집합이어야 합니다. 이러한 노드는 RADIUS 서버로도 구성됩니다.

여러 Cisco ISE 노드를 사용하여 단일 NAD 노드를 RADIUS 서버 및 동적 권한 부여 클라이언트로 구성할 수는 있지만 모든 노드가 동일한 노드 그룹에 있을 필요는 없습니다.

노드 그룹의 멤버는 기가비트 이더넷과 같은 고속 LAN 연결을 사용하여 서로 연결되어야 합니다. 노드 그룹 멤버가 L2에 인접해 있을 필요는 없지만 충분한 대역폭과 연결 가능성을 보장하려면 L2에 인접하는 것이 좋습니다. 자세한 내용은 정책 서비스 노드 그룹 생성, 92 페이지 섹션을 참고하십시오.

PSN 간에 요청을 균일하게 분산시키는 로드 밸런서

구축에 여러 PSN이 있을 때는 로드 밸런서를 사용하여 요청을 균일하게 분산시킬 수 있습니다. 로드 밸런서는 요청을 작동하는 여러 노드로 분산시킵니다. 로드 밸런서 뒤에서 PSN을 구축하는 방법에 대한 자세한 내용과 모범 사례는 Cisco 및 F5 구축 설명서: BIG-IP를 사용한 ISE 로드 밸런싱을 참고하십시오.

정책 서비스 노드의 세션 페일오버

노드 그룹의 PSN은 세션 정보를 공유합니다. 노드는 하트 비트 메시지를 교환하여 노드 장애를 탐지합니다. 노드에 장애가 발생하면 노드 그룹의 피어 중 하나가 장애가 발생한 PSN의 세션을 인식하고 CoA를 실행하여 그러한 세션의 연결을 끊습니다. 대부분의 클라이언트는 자동으로 다시 연결되고 새 세션을 설정합니다.

일부 클라이언트는 자동으로 다시 연결되지 않습니다. 예를 들어 클라이언트가 VPN을 통해 연결되는 경우 해당 클라이언트가 CoA를 인식하지 못할 수 있습니다. IP 폰, 멀티 호스트 802.1X 포트 또는 가상 머신인 클라이언트도 CoA를 인식하거나 CoA에 응답하지 않을 수 있습니다. URL 리디렉션 클라이언트(webauth)도 자동으로 연결할 수 없습니다. 이러한 클라이언트는 수동으로 다시 연결해야 합니다.

타이밍 문제로 재연결이 안 될 수도 있습니다. PSN 페일오버 시 포스처 상태가 보류 중인 경우를 예로 들 수 있습니다.

PSN 세션 공유에 대한 자세한 내용은 라이트 데이터 배포, 73 페이지를 참고하십시오.

정책 서비스 노드 그룹의 노드 수

노드 그룹에 포함될 수 있는 노드 수는 구축 요건에 따라 다릅니다. 노드 그룹은 노드 장애가 탐지되고 피어가 권한 부여되었지만 아직 포스처되지는 않은 세션에 CoA를 실행하도록 합니다. 노드 그룹 크기는 그리 크지 않아도 됩니다.

노드 그룹 크기가 커지면 노드 간에 교환되는 메시지 및 하트비트의 수가 크게 증가합니다. 결과적으로 트래픽도 증가하게 됩니다. 노드 그룹의 노드 수가 적을수록 트래픽도 줄어들며, 그와 동시에 PSN 장애를 탐지하기 위한 이중화를 충분히 제공할 수 있습니다.

노드 그룹 클러스터에서 가질 수 있는 PSN의 수에는 제한이 없습니다.

라이트 데이터 배포

라이트 데이터 배포는 사용자 세션 정보를 저장하여 구축의 모든 PSN 전반에 복제하는 데 사용되므로, 사용자 세션 세부정보를 위해 PAN 또는 MnT 노드에 의존할 필요가 없습니다.

라이트 데이터 배포는 다음 두 디렉토리로 구성됩니다.

- Radius 세션 디렉토리
- 엔드포인트 소유자 디렉토리

또한 **Advanced Settings(**고급 설정**)**에서 다음 옵션을 구성 할 수 있습니다.

- **Batch Size(**배치 크기**)**: 세션 업데이트를 일괄 적으로 전송할 수 있습니다. 이 값은 라이트 데이터 배포 인스턴스에서 구축의 다른 PSN으로 각 배치에서 전송되는 기록 수를 지정합니다. 이 필드를 1로 설정하면 세션 업데이트가 일괄적으로 전송되지 않습니다. 기본값은 기록 10개입니다.
- **TTL**: 이 값은 라이트 데이터 배포를 업데이트하기 전에 세션이 배치가 완료될 때까지 기다리는 최대 시간을 지정합니다. 기본값은 1000밀리초입니다.

PSN간에 연결 문제가 발생하는 경우(예: PSN이 다운된 경우) 세션 세부정보는 MnT 세션 디렉토리에서 검색되며, 나중에 사용할 수 있도록 저장됩니다.

대규모 구축에서는 최대 2,000,000개의 세션 기록을 저장할 수 있습니다. 소규모 구축에서는 1,000,000개의 세션 기록을 저장할 수 있습니다. 세션에 대한 계정 관리 중지 요청이 수신되면 모든 라이트 데이터 배포 인스턴스에서 해당 세션 데이터가 삭제됩니다. 저장된 기록의 수가 최대 한도를 초과하면 타임스탬프를 기준으로 가장 오래된 세션이 삭제됩니다.

참고

- 세션의 IPv6 접두사 길이가 128 비트보다 작고 인터페이스 ID가 지정되지 않은 경우 IPv6 접두사가 거부되어 여러 세션이 동일한 키를 가질 수 없습니다.
- 라이트 데이터 배포는 노드 간 통신에 ISE 메시징 서비스를 사용합니다. Cisco ISE 메시징 서비스는 다른 인증서 (내부 CA 체인에서 서명)를 사용합니다. Cisco ISE 메시징 서비스에 문제가 있는 경우 ISE 메시징 서비스 인증서를 다시 생성해야 합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다. **Certificate(s) will be used for(**사용될 인증서**)** 섹션에서 **ISE Messaging service(ISE** 메시징 서비스**)**를 선택합니다. **Generate ISE messaging service certificate(ISE** 메시징 서비스 인증서 생성**)**을 클릭합니다.

Radius 세션 디렉토리

RADIUS 세션 디렉토리는 사용자 세션 정보를 저장하고 이를 구축의 PSN 전체에 복제하는 데 사용됩니다. **RADIUS** 세션 디렉토리는 CoA(Change of Authorization)에 필요한 세션 속성만 저장합니다.

이 기능은 Cisco ISE 릴리스 2.7에서 기본적으로 활성화됩니다. **Light Data Distribution(**라이트 데이터 배포**)** 창에서 **RADIUS Session Directory (RADIUS** 세션 디렉토리**)** 확인란을 선택하거나 선택 취소하여 이 기능을 활성화하거나 비활성화 할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Light Data Distribution(**라이트 데이터 배포**)**입니다.

엔드포인트 소유자 디렉토리

Cisco ISE 릴리스 2.6까지는 특정 엔드포인트에 대한 요청을 원래 처리한 것과 다른 PSN(Policy Service Node)에서 엔드포인트 프로브가 수신되면 엔드포인트 소유자가 새 PSN으로 변경됩니다. 이로 인해 엔드포인트 소유권이 플래핑됩니다.

Cisco ISE 릴리스 2.7부터는 **Endpoint Owner Directory(**엔드포인트 소유자 디렉토리를 사용하여 Cisco ISE에 연결하는 각 MAC 주소의 PSN FQDN을 저장하고 구축에서 PSN 전체에 걸쳐 이 데이터를 복제합니다. 이렇게 하면 모든 PSN이 이제 엔드포인트 소유자를 전부 인식하므로 엔드포인트 소유권 플래핑을 방지할 수 있습니다. 엔드포인트 소유권은 다른 PSN에서 해당 엔드포인트의 RADIUS 인증에 성공한 경우에만 변경됩니다.

또한 정적 엔드포인트 할당은 동일한 엔드포인트에 대해 수신 프로브가 받게 되는 속성에 우선되므로, 속성 재정의 문제가 발생하지 않습니다.

이 기능은 Cisco ISE 릴리스 2.7에서 기본적으로 활성화됩니다. 필요한 경우 비활성화하여 엔드포인트 소유자 디렉토리를 사용하지 않는 이전 메커니즘으로 되돌릴 수 있습니다. 엔드포인트 소유자 디렉토리는 프로파일링에도 사용되며, 이 옵션을 비활성화하면 레거시 프로파일러 소유자의 디렉토리가 사용됩니다. **Light Data Distribution(**라이트 데이터 배포**)** 창에서 **Enable Endpoint Owner Directory(**엔드포인트 소유자 디렉토리 활성화**)** 확인란을 선택하거나 선택 취소하여 해당 기능을 활

성화하거나 비활성화할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Light Data Distribution(**라이트 데이터 배포**)**입니다.

모니터링 노드

모니터링 페르소나를 사용하는 Cisco ISE 노드는 로그 컬렉터로 작동하며, 네트워크에 있는 PAN 및 PSN의 로그 메시지를 저장합니다. 이 페르소나는 네트워크 및 리소스를 효율적으로 관리하는 데 사용할 수 있는 고급 모니터링 및 문제 해결 도구를 제공합니다. 이 페르소나를 사용하는 노드는 관리자가 수집하여 보고서 형식으로 의미 있는 정보를 제공하는 데이터를 집계하고 상관관계를 지정합니다.

Cisco ISE에서는 이 페르소나를 사용하는 노드를 두 개까지 가질 수 있으며, 그러한 노드는 고가용성을 위해 기본 또는 보조 역할을 맡을 수 있습니다. 기본 및 보조 MnT 노드 모두 로그 메시지를 수집합니다. 기본 MnT가 다운되면 기본 PAN이 보조 노드를 가리키며 모니터링 데이터를 수집합니다. 그러나 보조 노드는 기본 노드로 자동 승격되지 않습니다. 이 작업은 수동으로 MnT 역할 수정.

분산 설정에서 하나 이상의 노드가 모니터링 페르소나를 맡아야 합니다. 동일한 Cisco ISE 노드에서 모니터링 페르소나와 정책 서비스 페르소나를 함께 활성화하지 않는 것이 좋습니다. 최적의 성능을 위해서는 모니터링 전용 노드를 사용하는 것이 좋습니다.

구축의 기본 모니터링 노드

참고 pxGrid를 활성화한 경우 pxGrid 노드에 대한 새 인증서를 생성해야 합니다. 디지털 서명을 사용하여 인증서 템플릿을 생성하고 새 pxGrid 인증서를 생성합니다.

수동으로 MnT 역할 수정

기본 PAN에서 MnT 역할을 수동으로 수정(기본에서 보조로, 보조에서 기본으로)할 수 있습니다.

단계 **1** 기본 PAN의 사용자 인터페이스에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**.

단계 **3** 노드 목록에서 역할을 변경할 MnT 노드 옆의 확인란을 선택합니다.

단계 **4** **Edit(**편집**)**를 클릭합니다.

단계 **5** **Monitoring(**모니터링**)** 섹션에서 역할을 **Primary(**기본**)** 또는 **Secondary(**보조**)**로 변경합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

참고 해당 노드에서 활성화된 다른 모든 페르소나 및 서비스를 비활성화하려는 경우 **Dedicated MnT(**전용 **MnT)** 옵션을 활성화할 수 있습니다. 이 옵션을 활성화하면 해당 노드에서 컨피그레이션 데이터 복제 프로세스가 중지됩니다. 이는 MnT 노드의 성능을 개선하는 데 도움이 됩니다. 해당 옵션을 비활성화하면 수동 동기화가 트리거됩니다.

Cisco ISE 메시징 서비스의 시스템 로그

Cisco ISE 릴리스 2.6에서는 기본 내장 UDP 시스템 로그 수집 대상인 LogCollector 및 LogCollector2에 대한 MnT WAN 지속 가능성을 제공합니다. 이 지속 가능성은 **Use "ISE Messaging Service" for UDP Syslogs delivery to MnT(MnT**로의 **UDP** 시스템 로그 전달 시 **"ISE** 메시징 서비스**"** 사용**)**(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **System(**시스템**)** > **Logging(**로깅**)** > **Log Settings(**로그 설정**)**) 옵션을 통해 활성화됩니다. 이 옵션을 활성화하면 UDP 시스템 로그가 TLS(Transport Layer Security)로 보호됩니다.

Use "ISE Messaging Service" for UDP Syslogs delivery to MnT(MnT로의 **UDP** 시스템 로그 전달 시 **"ISE** 메시징 서비스**"** 사용**)** 옵션은 Cisco ISE 릴리스 2.6, FCS(First Customer Ship)에서 기본적으로 비활성화되어 있습니다. 이 옵션은 Cisco ISE 릴리스 2.6 누적 패치 2 이상 릴리스에서 기본적으로 활성화되어 있습니다.

UDP 시스템 로그에 Cisco ISE 메시징 서비스를 사용하면 MnT 노드에 연결할 수 없는 경우에도 제한된 기간 동안 운영 데이터가 유지됩니다. MnT WAN 지속 가능성 기간은 약 2시간 30분입니다.

이 서비스는 TCP 포트 8671을 사용합니다. 이에 따라 네트워크를 구성하고, 구축에서 다른 모든 Cisco ISE 노드의 각 Cisco ISE 노드에서 TCP 포트 8671로의 연결을 허용합니다. Light Session Directory(*Cisco ID* 서비스 엔진 관리자 가이드에서 "배포된 환경에서의 Cisco ISE 설정" 장의 "Light Session Directory" 섹션 참조)와 Profiler Persistence Queue 기능도 Cisco ISE 메시징 서비스를 사용합니다. .

참고 구축에서 Cisco ISE 구축에 TCP 또는 보안 시스템 로그를 사용하는 경우 기능은 이전 릴리스와 동일하게 유지됩니다.

대기열 링크 경보

Cisco ISE 메시징 서비스는 내부 CA 체인에서 서명한 다른 인증서를 사용합니다. Cisco ISE GUI 대시보드의 **Alarms(**경보**)** 대시릿에서 대기열 링크 경보를 가져올 수 있습니다. 이 경보는 구축에 노드를 등록하거나, 기본 PAN에서 노드를 수동으로 동기화하거나, 노드가 동기화되지 않은 상태이거나, 노드에서 애플리케이션 서비스가 다시 시작되는 등의 구축 작업을 수행하는 경우에 발생합니다. 다음을 확인하여 경보를 해결합니다.

- 모든 노드가 연결되어 있고 동기화됩니다.
- 모든 노드 및 Cisco ISE 메시징 서비스가 제대로 기능합니다.
- Cisco ISE 메시징 서비스 포트는 방화벽과 같은 외부 엔티티에 의해 차단되지 않습니다.
- 각 노드의 Cisco ISE 메시징 인증서 체인이 손상되지 않았으며 인증서 상태가 양호합니다.

위에 나열된 전제 조건이 충족되면 다음 작업으로 인해 대기열 링크 경보가 트리거됩니다.

- PAN 또는 PSN의 도메인 이름 또는 호스트 이름 변경
- 새 구축에서 백업 복원
- 업그레이드 후 이전 기본 PAN을 새 기본 PAN으로 승격

대기열 링크 경보를 해결하려면 Cisco ISE 루트 CA 체인을 다시 생성합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다. **Generate Certificate Signing Requests (CSR)(CSR(**인증서 서명 요청**)** 생성**)**를 클릭합니다. **Certificate(s) will be used for(**인증서 사용 대상**)** 드롭다운 목록에서 **ISE Root CA(ISE** 루트 **CA)**를 선택합니다. **Replace ISE Root CA Certificate Chain(ISE** 루트 **CA** 인증서 체인 교체**)**을 클릭합니다.

다음 시나리오로 인해 **Queue Link Error(**대기열 링크 오류**)** 경보가 생성 될 수 있습니다.

- 시간 초과 : Cisco ISE 구축에서 두 노드간에 네트워크 문제가있는 경우 **Timeout(**시간 초과**)** 원인이 있는 **Queue Link Error(**대기열 링크 오류**)** 경보가 발생합니다. 이 오류를 해결하려면 포트 8671에서 연결을 확인합니다.
- 알 수 없는 CA: **System Certificates(**시스템 인증서**)** 창(이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**))**창 손상된 Cisco ISE 메시징 인증서가 있는 경우 **Unknown CA(**알 수 없는 **CA** 원인**)**이 있는 **Queue Link Error(**대기열 링크 오류**)** 경보가 발생합니다. 이 문제는 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Signing Requests(**인증서 서명 요청**)**을 선택한 다음 Cisco ISE GUI에서 **Generate Certificate Signing Request (CSR)(CSR(**인증서 서명 요청**)** 생성**)**에서 생성을 클릭하여 Cisco ISE 메시징 인증서를 재생성하여 해결할 수 있습니다. Cisco ISE 루트 CA 인증서 체인을 이미 교체한 경우에는 재생성이 필요하지 않습니다.

Cisco ISE 루트 CA 체인을 교체하면 Cisco ISE 메시징 서비스 인증서도 교체됩니다. 그 후에는 약 2분의 다운타임이 지나고 Cisco ISE 메시징 서비스가 재시작됩니다. 따라서 이 다운타임 중에 시스템 로그가 손실됩니다. 다운타임 중에 시스템 로그가 손실되지 않도록 하려면 Cisco ISE 메시징 서비스를 잠시 비활성화할 수 있습니다.

MnT로의 UDP 시스템 로그 전달 시 Cisco ISE 메시징 서비스를 활성화하거나 비활성화하려면 다음을 따릅니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **System(**시스템**)** > **Logging(**로깅**)** > **Log Settings(**로그 설정**)**.

단계 **2** **Use "ISE Messaging Service" for UDP Syslogs delivery to MnT(MnT**로의 **UDP** 시스템 로그 전달 시 **"ISE** 메시징 서비스**"** 사용**)** 확인란을 선택하거나 선택 취소하여 ISE 메시징 서비스 사용을 활성화 또는 비활성화합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

MnT 노드의 자동 페일오버

MnT 노드는 고가용성을 제공하지 않지만 활성-대기 구성을 지원합니다. PSN은 운영 감사 데이터를 기본 및 보조 MnT 노드에 복사합니다.

자동 페일오버 프로세스

기본 MnT 노드의 작동이 중지되면 보조 MnT 노드가 모든 모니터링 및 문제 해결 정보를 인계받습니다.

보조 노드를 기본 노드로 수동 전환하려면 수동으로 MnT 역할 수정을 참고하십시오. 보조 노드가 승격된 후에 기본 노드가 복구되면 보조 역할을 맡습니다. 보조 노드가 승격되지 않은 경우에는 기본 MnT 노드가 복구되고 나면 기본 역할을 다시 수행합니다.

⚠

주의 페일오버 이후에 기본 노드가 복구되면 보조 노드의 백업을 확보하고 데이터를 복구하여 기본 노드를 업데이트합니다.

MnT 노드의 활성-대기 페어를 설정하기 위한 지침

Cisco ISE 네트워크에서 MnT 노드 2개를 지정하고 활성-대기 페어로 구성할 수 있습니다. 기본 MnT 노드를 백업하고 데이터를 새 보조 MnT 노드로 복구하는 것이 좋습니다. 이렇게 하면 기본 노드에서 새 데이터를 복제할 때 기본 MnT 노드의 기록이 새 보조 노드와 동기화됩니다. 활성-대기 페어에 적용되는 규칙은 다음과 같습니다.

- 모든 변경 사항이 기본 MnT 노드에 기록됩니다. 보조 노드는 읽기 전용입니다.
- 기본 노드에 적용된 변경 사항은 자동으로 보조 노드에 복제됩니다.
- 기본 노드와 보조 노드는 다른 모든 노드가 로그를 전송하는 로그 컬렉터로 나열됩니다.
- Cisco ISE 대시보드는 모니터링 및 문제 해결을 위한 기본 시작점입니다. 모니터링 정보는 PAN의 대시보드에 표시됩니다. 기본 노드가 작동 중지되면 보조 노드에서 모니터링 정보가 제공됩니다.
- MnT 데이터를 백업하고 비우기하는 작업은 표준 Cisco ISE 노드 백업 프로세스에 포함되지 않습니다. 기본 및 보조 MnT 노드에서 백업 및 데이터 비우기를 위한 저장소를 구성하고 각각에 동일한 저장소를 사용해야 합니다.

MnT 노드 페일오버 시나리오

다음 시나리오는 MnT 노드에 해당하는 활성-대기 또는 단일 노드 구성에 적용됩니다.

- MnT 노드의 활성-대기 구성에서 기본 PAN은 항상 모니터링 데이터를 수집하기 위해 기본 MnT 노드를 가리킵니다. 기본 MnT 노드에 장애가 발생한 경우 PAN은 대기 MnT 노드를 가리킵니다. 기본 노드에서 보조 노드로의 페일오버는 5분 이상 작동이 중지된 후에 이루어집니다.

  그러나 기본 노드에서 장애가 발생한 후에는 보조 노드가 기본 노드가 되지 않습니다. 기본 노드가 복구되면 PAN은 재개된 기본 노드에서 다시 모니터링 데이터 수집을 시작합니다.

- 기본 MnT 노드가 작동 중지된 상태에서 대기 MnT 노드를 활성 상태로 승격하려는 경우 수동으로 MnT 역할 수정하거나 기존 기본 MnT 노드를 등록 취소하면 됩니다. 기존의 기본 MnT 노드를 등록 취소하면 대기 노드가 기본 MnT 노드가 되고, PAN은 자동으로 새로 승격된 기본 노드를 가리키게 됩니다.
- 활성-대기 페어에서 보조 MnT 노드를 등록 취소하거나 보조 MnT 노드가 작동 중지되면 기존의 기본 MnT 노드는 기본 노드로 유지됩니다.
- Cisco ISE 구축 환경에 MnT 노드가 하나만 있는 경우 이 노드는 PAN에 모니터링 데이터를 제공하는 기본 MnT 노드로 작동합니다. 그러나 새 MnT 노드를 등록하고 구축 환경에서 이를 기본 노드로 전환하면 기존의 기본 MnT 노드는 자동으로 대기 노드가 됩니다. PAN은 모니터링 데이터를 수집하기 위해 새로 등록된 기본 MnT 노드를 가리킵니다.

모니터링 데이터베이스

모니터링 기능에 사용되는 데이터 비율과 양에 따라 전용 노드에서 이러한 용도로 사용할 별도의 데이터베이스가 필요합니다.

PSN처럼 MnT 노드에는 이 섹션에서 설명하는 항목과 같이 유지 관리 작업을 수행해야 하는 전용 데이터베이스가 있습니다.

모니터링 데이터베이스 백업 및 복구

모니터링 데이터베이스는 대량의 데이터를 처리합니다. 시간의 경과할수록 MnT 노드의 성능과 효율성은 해당 데이터를 얼마나 잘 관리하느냐에 따라 달라집니다. 효율성을 높이기 위해서는 데이터를 백업하여 정기적으로 원격 저장소로 전송하는 것이 좋습니다. 자동 백업을 예약하여 이 작업을 자동화할 수 있습니다.

참고 제거 작업이 진행 중인 경우 백업을 수행해서는 안 됩니다. 제거 작업 중에 백업을 시작하면 제거 작업이 중단되거나 실패합니다.

보조 MnT 노드를 등록하는 경우에는 먼저 기본 MnT 노드를 백업한 다음, 데이터를 새 보조 MnT 노드에 복구하는 것이 좋습니다. 이렇게 하면 새 변경 사항이 복제될 때 기본 MnT 노드의 기록이 새 보조 노드와 동기화됩니다.

Monitoring(모니터링) Database Purge(데이터베이스 비우기)

비우기 프로세스를 사용하면 비우기하는 동안 데이터를 유지할 개월 수를 지정하여 모니터링 데이터베이스의 크기를 관리할 수 있습니다. 기본값은 3개월입니다. 이 값은 비우기를 위한 디스크 공간 사용 임계값(디스크 공간의 백분율)을 충족할 때 사용됩니다. 이 옵션에서 각 달은 30일로 구성됩니다. 3개월의 기본값은 90일입니다.

모니터링 데이터베이스 비우기를 위한 지침

다음은 모니터링 데이터베이스 디스크 사용량과 관련하여 따라야 하는 지침입니다.

- 모니터링 데이터베이스 디스크 사용량이 임계값 설정의 80%를 초과하는 경우에는 데이터베이스 크기가 할당된 디스크 크기를 초과했음을 나타내는 중요 경보가 생성됩니다. 디스크 사용량이 90%를 초과하면 또 다른 경보가 생성됩니다.

  비우기 프로세스가 실행되면 **Data Purging Audit(**데이터 비우기 감사**)** 창에서 볼 수 있는 상태 기록 보고서가 생성됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Audit(**감사**)** > **Data Purging Audit(**데이터 비우기 감사**)**입니다. 비우기가 완료되면 정보(INFO) 경보가 생성됩니다.

- 비우기는 데이터베이스의 사용된 디스크 공간 백분율도 기반으로 합니다. 모니터링 데이터베이스의 사용된 디스크 공간이 임계값(기본값: 80%) 이상이면 비우기 프로세스가 시작됩니다. 이 프로세스에서는 관리 포털에서 구성된 값에 관계없이 모니터링 데이터의 가장 오래된 7일 분량만 삭제합니다. 사용된 디스크 공간이 80% 미만이 될 때까지 루프에서 이 프로세스가 계속 진행됩니다. 비우기를 계속하기 전에 항상 모니터링 데이터베이스 디스크 공간을 확인합니다.

운영 데이터 비우기

Cisco ISE 모니터링 운영 데이터베이스에는 Cisco ISE 보고서로 생성되는 정보가 포함되어 있습니다. 최신 Cisco ISE 릴리스에는 Cisco ISE 관리 CLI 명령 **application configure ise**를 실행한 후 모니터링 운영 데이터를 제거하고 모니터링 데이터베이스를 재설정하는 옵션이 있습니다.

제거 옵션은 데이터를 정리하는 데 사용되며 보존 기간(일)을 지정하라는 메시지를 표시합니다. 재설정 옵션은 데이터베이스를 출고 시 기본값으로 재설정하는 데 사용되며 백업된 모든 데이터를 영구적으로 삭제합니다. 파일이 너무 많은 파일 시스템 공간을 사용하는 경우 데이터베이스를 재설정할 수 있습니다.

참고 재설정 옵션을 사용하면 재시작 전까지 Cisco ISE 서비스를 일시적으로 사용할 수 없게 됩니다.

Operational Data Purging(운영 데이터 비우기**)** 창에는 **Database Utilization(**데이터베이스 사용률**)** 및 **Purge Data Now(**지금 데이터 비우기**)** 영역이 포함되어 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Maintenance(**유지 관리**)** > **Operational Data Purging(**운영 데이터 비우기**)**입니다. **Database Utilization(**데이터베이스 사용률**)** 영역에 저장된 RADIUS 및 TACACS 데이터 및 총 가용 데이터베이스 공간을 볼 수 있습니다. 상태 표시줄 위에 마우스를 올려 놓으면 사용 가능한 디스크 공간과 기존 데이터가 데이터베이스에 저장된 일수가 표시됩니다. **Data Retention Period(**데이터 보존 기간**)** 영역에서 RADIUS 및 TACACS 데이터를 보존할 기간을 지정할 수 있습니다. 데이터는 매일 오전 4시에 제거되며, 보존 기간(일)을 지정하여 제거하기 전에 저장소에 데이터를 내보내도록 구성할 수 있습니다. **Enable Export Repository(**내보내기 저장소 활성화**)** 확인란을 선택하여 저장소를 선택 및 생성하고 **Encryption Key(**암호화 키**)**를 지정할 수 있습니다.

Purge Data Now(지금 데이터 제거**)** 영역에서 모든 RADIUS 및 TACACS 데이터를 제거하거나 특정 기간이 경과되면 데이터를 제거하도록 일수를 지정할 수 있습니다.

참고 비우기하기 전에 RADIUS 인증 및 계정 관리, TACACS 권한 부여 및 계정 관리, RADIUS 오류 및 잘못 구성된 supplicant 표을 저장소로 내보낼 수 있습니다.

관련 항목

이전 운영 데이터 비우기, 81 페이지

이전 운영 데이터 비우기

운영 데이터는 일정 기간 동안 서버에 수집되며, 즉시 또는 정기적으로 비울 수 있습니다. **Data Purging Audit(**데이터 비우기 감사**)** 보고서를 확인하여 데이터 비우기 성공 여부를 확인할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Maintenance(**유지 관리**)** > **Operational Data Purging(**운영 데이터 비우기**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 다음 중 하나를 수행합니다.

- **Data Retention Period(**데이터 보존 기간**)** 영역에서 다음을 수행합니다.
  1. RADIUS 및 TACACS 데이터를 보존할 기간을 일 단위로 지정합니다. 지정한 기간 이전의 모든 데이터는 저장소로 내보내집니다.
  2. **Repository(**저장소**)** 영역에서 **Enable Export Repository(**내보내기 저장소 활성화**)** 확인란을 선택하여 데이터를 저장할 저장소를 선택합니다.
  3. **Encryption Key(**암호화 키**)** 텍스트 상자에 필요한 비밀번호를 입력합니다.
  4. **Save(**저장**)**를 클릭합니다.

     참고 구성된 보존 기간이 진단 데이터에 해당하는 기존 보존 임계값보다 작으면 구성된 값이 기존 임계값을 재정의합니다. 예를 들어 보존 기간을 3일로 구성했는데 이 값이 진단 표의 기존 임계값(예: 기본값인 5일)보다 작은 경우에는 이 창에서 구성한 값(3일)에 따라 데이터를 제거합니다.

- **Purge Data Now(**지금 데이터 제거**)** 영역에서 다음을 수행합니다.
  1. 모든 데이터를 제거할지 아니면 지정된 기간(일)보다 오래된 데이터를 제거할지 선택합니다. 데이터는 어떤 저장소에도 저장되지 않습니다.
  2. **Purge(**제거**)**를 클릭합니다.

자동 페일오버용 **MnT** 노드 구성

구축에 MnT 노드가 두 개인 경우에는 Cisco ISE 모니터링 서비스 다운타임을 방지하기 위해 자동 페일오버용으로 기본-보조 쌍을 구성할 수 있습니다. 이처럼 기본-보조 쌍을 구성하면 기본 노드에서 오류가 발생하는 경우 보조 MnT 노드가 모니터링 기능을 자동으로 제공합니다.

시작하기 전에

- 자동 페일오버용 MnT 노드를 구성하려면 해당 노드를 Cisco ISE 노드로 등록해야 합니다.
- 두 노드에서 모두 모니터링 역할과 서비스를 구성한 다음 기본 및 보조 역할에 맞게 적절한 이름을 지정합니다.
- 기본 및 보조 MnT 노드 둘 다에서 백업 및 데이터 비우기용 저장소를 구성합니다. 백업 및 비우기 기능이 정상적으로 작동하도록 하려면 두 노드에 대해 동일한 저장소를 사용합니다. 비우기는 이중화 쌍의 기본 및 보조 노드 둘 다에서 수행됩니다. 예를 들어 기본 MnT 노드가 백업과 비우기용으로 두 개 저장소를 사용하는 경우 보조 노드에 대해서도 동일한 저장소를 지정해야 합니다.

  시스템 CLI에서 **repository** 명령을 사용하여 MnT 노드에 대해 데이터 저장소를 구성합니다.

  ⚠ 주의 모니터링 이중화 쌍의 노드에서 예약된 백업 및 비우기가 정상적으로 작동하도록 하려면 CLI를 사용하여 기본 노드와 보조 노드 둘 다에서 동일한 저장소를 하나 이상 구성합니다. 저장소는 두 노드 간에 자동으로 동기화되지 않습니다.

Cisco ISE 대시보드에서 MnT 노드가 준비되었는지 확인합니다. **System Summary(**시스템 요약**)** dashlet에서 서비스가 준비된 MnT 노드의 왼쪽에는 녹색 확인 표시가 표시됩니다.

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

단계 **2** **Deployment Nodes(**구축 노드**)** 창에서 기본으로 지정할 MnT 노드 옆의 확인란을 선택하고 **Edit**를 클릭합니다.

단계 **3** **General Settings(**일반 설정**)** 탭을 클릭하고 **Role(**역할**)** 드롭다운 목록에서 **Primary(**기본**)**를 선택합니다.

MnT 노드를 기본으로 선택하면 나머지 MnT 노드는 자동으로 보조가 됩니다. 독립형 구축의 경우에는 기본 및 보조 역할 컨피그레이션이 비활성화됩니다.

단계 **4** **Save** 버튼을 클릭합니다. 기본 노드와 보조 노드가 모두 재시작됩니다.

Cisco pxGrid 노드

Cisco pxGrid는 Cisco ISE 세션 디렉토리에서 다른 네트워크 시스템(예: Cisco ISE 에코시스템 파트너 시스템 및 기타 Cisco 플랫폼)과 상황 민감 정보를 공유하는 데 사용됩니다. 또한 pxGrid 프레임워크를 사용하여 노드 간에 정책 및 컨피그레이션 데이터를 교환하고(예: ISE와 서드파티 벤더 간에 태그 및 정책 객체 공유) 다른 정보도 교환할 수 있습니다. 또한 Cisco pxGrid에서는 서드파티 시스템이 네트워크 또는 보안 이벤트에 대한 응답으로 사용자나 장치 또는 둘 다를 격리하기 위해 EPS(적응형 네트워크 제어 작업)를 호출할 수 있습니다. 태그 정의, 값 및 설명과 같은 TrustSec 정보는 Cisco TrustSec 토픽을 통해 Cisco ISE에서 다른 네트워크로 전달될 수 있습니다. FQN(Fully Qualified Names)을 사용하는 엔드포인트 프로파일은 엔드포인트 프로파일 메타 토픽을 통해 Cisco ISE에서 다른 네트워크로 전달될 수 있습니다. Cisco pxGrid는 태그 및 엔드포인트 프로파일의 대량 다운로드도 지원합니다.

Cisco pxGrid를 통해 SXP 바인딩(IP-SGT 매핑)을 게시하고 구독할 수 있습니다. SXP 바인딩에 대한 자세한 내용은 *Cisco ISE* 관리 가이드*:* 세그멘테이션의 보안 그룹 태그 교환 프로토콜 섹션을 참조하십시오. 참조.

고가용성 컨피그레이션에서 Cisco pxGrid 서버는 PAN을 통해 노드 간에 정보를 복제합니다. PAN이 다운되면 Cisco pxGrid 서버는 클라이언트 등록 및 서브스크립션 처리를 중단합니다. Cisco pxGrid 서버가 활성화되도록 하려면 PAN을 수동으로 승격해야 합니다. Cisco pxGrid 서비스 창(Administration(관리) > pxGrid Services(pxGrid 서비스))에서 Cisco pxGrid 노드가 현재 활성 상태인지 아니면 대기 상태인지를 확인할 수 있습니다.

pxGrid 페르소나가 있는 활성 Cisco 노드에서 이러한 프로세스는 **Running(**실행 중**)**으로 표시됩니다. 대기 중인 Cisco pxGrid 노드에서는 **Standby(**대기**)**로 표시됩니다. 활성 pxGrid 노드가 다운되면 대기 중인 pxGrid 노드가 이를 탐지하고 4개의 pxGrid 프로세스를 시작합니다. 몇 분 내에 이러한 프로세스가 **Running(**실행 중**)**으로 표시되고 대기 노드는 활성 노드가 됩니다. CLI 명령 **show logging application pxgrid/pxgrid.state**를 실행하여 Cisco pxGrid 서비스가 해당 노드에서 대기 중인지 확인할 수 있습니다.

XMPP(Extensible Messaging and Presence Protocol) 클라이언트의 경우 Cisco pxGrid 노드는 활성 노드에서 활성-대기 고가용성 모드로 작동합니다. 즉, Cisco pxGrid Service는 활성 노드에서는 실행 중 상태이며 대기 모드에서는 비활성화됨 상태입니다.

참고 고가용성 Cisco ISE 구축에서 활성-대기 설정에서 작동하는 pxGrid 개인 설정 노드는 pxGrid 서비스가 활성 노드에서 실행 중 상태이며 대기 노드에서는 대기 상태임을 표시합니다.

Cisco ISE 노드에서 pxGrid 서비스의 상태를 확인하려면 다음 CLI 명령을 사용합니다.

```
show logging application pxgrid/pxgrid.state
```

보조 Cisco pxGrid 노드에 대한 자동 페일오버가 시작된 후 원래 기본 Cisco pxGrid 노드가 네트워크에 다시 연결되면, 원래 기본 Cicsco pxGrid 노드는 계속 보조 역할로 지정되며 현재 기본 노드가 강등되지 않는 한 기본 역할로 다시 승격되지 않습니다.

참고 간혹 원래 기본 Cisco pxGrid 노드가 자동으로 기본 역할로 다시 승격되기도 합니다.

고가용성 구축의 경우 기본 Cisco pxGrid 노드가 강등되면 보조 Cicsco pxGrid 노드로 전환하는 데 3~5분 정도 걸릴 수 있습니다. 기본 Cisco pxGrid 노드 장애가 발생하는 경우 클라이언트는 되도록 전환이 완료될 때까지 기다린 다음 캐시 데이터를 지워야 합니다.

Cisco pxGrid 노드에 사용할 수 있는 로그는 다음과 같습니다.

- pxgrid.log: 상태 변경 알림입니다.
- pxgrid-cm.log: 클라이언트와 서버 간의 게시자 또는 가입자 또는 둘 다에 대한 및 데이터 교환 활동에 대한 업데이트입니다.
- pxgrid-controller.log: 클라이언트 기능, 그룹 및 클라이언트 권한 부여 세부정보를 표시합니다.
- pxgrid-jabberd.log: 시스템 상태 및 인증 관련 전체 로그입니다.
- pxgrid-pubsub.log: 게시자 및 가입자 이벤트 관련 정보입니다.

참고 노드에서 pxGrid 서비스가 비활성화된 경우, 포트 5222는 작동하지 않지만 (Web Clients(웹 클라이언트)에서 사용하는) 포트 8910은 작동하며 요청에 계속 응답합니다.

참고 Cisco ISE Advantage 라이선스로 Cisco pxGrid 및 Cisco pxGrid 페르소나를 활성화 할 수 있습니다.

참고 Passive ID Work Center(패시브 ID 작업 센터)를 이용하려면 Cisco pxGrid를 정의해야 합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 자산 가시성의 PassiveID 작업 센터 섹션을 참조하십시오 .

Cisco pxGrid 노드 구축

독립형 노드와 분산형 구축 노드에서 모두 Cisco pxGrid 페르소나를 활성화할 수 있습니다.

시작하기 전에

- Cisco pxGrid 페르소나를 활성화하려면 Cisco ISE Advantage 라이선스가 있어야 합니다.
- 라이선싱 요건은 ISE 라이선싱/주문을 참조하십시오.
- 모든 노드는 Cisco pxGrid 서비스 사용 시 CA 인증서를 사용합니다. 업그레이드 전에 Cisco pxGrid 서비스에 기본 인증서를 사용한 경우에는 업그레이드 시 해당 인증서가 내부 CA 인증서로 대체됩니다.

- Websockets(pxGrid 2.0)에 대해서는 포트 8910이 열려 있고 XMPP(pxGrid V1.0)에 대해서는 포트 5222가 열려 있어야 합니다. 노드에서 pxGrid 서비스가 비활성화된 경우, 포트 5222는 작동하지 않지만 포트 8910은 작동하며 요청에 계속 응답합니다.

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

단계 **2** **Deployment Nodes(**구축 노드**)** 창에서 Cisco pxGrid 서비스를 활성화할 노드 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **General Settings(**일반 설정**)** 탭을 클릭하고 **pxGrid** 토글 버튼을 활성화.

단계 **4** **Save(**저장**)**를 클릭합니다.

이전 버전에서 업그레이드하는 경우 **Save(**저장**)** 옵션이 비활성화되어 있을 수 있습니다. 브라우저 캐시가 이전 버전 Cisco ISE의 오래된 파일을 참고하는 경우 이러한 현상이 발생합니다. **Save(**저장**)** 옵션을 활성화하려면 브라우저 캐시를 지우십시오.

Cisco pxGrid 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **Settings(**설정**)**를 선택합니다.

단계 **2** 요건에 따라 다음 옵션을 선택합니다.

- **Automatically approve new certificate-based accounts(**새 인증서 기반 계정 자동 승인**)**: 새 Cisco pxGrid 클라이언트의 연결 요청을 자동으로 승인하려면 이 확인란을 선택합니다.
- **Allow password based account creation(**비밀번호 기반 계정 생성 허용**)**: Cisco pxGrid 클라이언트에 대해 사용자 이름 또는 비밀번호 기반 인증을 활성화하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 Cisco pxGrid 클라이언트를 자동으로 승인할 수 없습니다.

  Cisco pxGrid 클라이언트는 REST API를 통해 사용자 이름을 전송하여 Cisco pxGrid 컨트롤러에 자체적으로 등록할 수 있습니다. Cisco pxGrid 컨트롤러는 클라이언트 등록 중에 Cisco pxGrid 클라이언트의 비밀번호를 생성합니다. 관리자는 연결 요청을 승인하거나 거부할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

Cisco pxGrid **Settings(**설정**)** 창의 **Test(**테스트**)** 옵션을 사용하여 Cisco pxGrid 노드에서 상태 확인을 실행할 수 있습니다. pxgrid 또는 pxgrid-test.log 파일에서 세부정보를 볼 수 있습니다.

Cisco pxGrid 인증서 생성

시작하기 전에

일부 Cisco ISE 버전에는 NetscapeCertType을 사용하는 Cisco pxGrid용 인증서가 있습니다. 새 인증서를 생성하는 것이 좋습니다.

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- 기본 PAN에서 Cisco pxGrid 인증서를 생성해야 합니다.
- Cisco pxGrid 인증서가 SAN(Subject Alternative Name) 확장을 사용하는 경우, 주체 ID의 FQDN을 DNS 이름 항목으로 포함해야 합니다.
- 디지털 서명을 사용하여 인증서 템플릿을 생성하고 이를 사용하여 새 Cisco pxGrid 인증서를 생성합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **Client Management(**클라이언트 관리**)** > **Certificates(**인증서**)**.

단계 **2** **I want to(**수행할 작업**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)**: 이 옵션을 선택하면 CN(Common Name)을 입력해야 합니다.
- **Generate a single certificate without a certificate signing request(**인증서 서명 요청을 이용해 단일 인증서 생성**)**: 이 옵션을 선택하면 Certificate Signing Request(인증서 서명 요청) 세부정보를 입력해야 합니다.
- **Generate bulk certificates(**대량 인증서 생성**)**: 필수 세부정보를 포함하는 CSV 파일을 업로드할 수 있습니다.
- **Download Root Certificate Chain(**루트 인증서 체인 다운로드**)**: 루트 인증서를 다운로드하여 신뢰할 수 있는 인증서 저장소에 추가합니다. 호스트 이름 및 인증서 다운로드 형식을 지정해야 합니다.

단계 **3** **CN(Common Name)**: **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)** 옵션을 선택하는 경우에 필요합니다. pxGrid 클라이언트의 FQDN을 입력합니다.

단계 **4** **Certificate Signing Request Details(**인증서 서명 요청 세부정보**)**: **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)** 옵션을 선택하는 경우에 필요합니다. 전체 인증서 서명 요청 세부정보를 입력합니다.

단계 **5** **Description(**설명**)**: (선택 사항) 이 인증서에 대한 설명을 입력합니다.

단계 **6** **Certificate Template(**인증서 템플릿**)**: **pxGrig_Certificate_Template** 링크를 클릭하여 인증서 템플릿을 다운로드하고 요구 사항에 따라 템플릿을 편집합니다.

단계 **7** **SAN(Subject Alternative Name)**: 여러 SAN을 추가할 수 있습니다. 다음 옵션을 사용할 수 있습니다.

- **IP address(IP** 주소**)**: 인증서에 연결할 Cisco pxGrid 클라이언트의 IP 주소를 입력합니다.
- **FQDN**: pxGrid 클라이언트의 정규화된 도메인 이름을 입력합니다.

참고 **Generate Bulk Certificate(**대량 인증서 생성**)** 옵션을 선택했다면 이 필드는 표시되지 않습니다.

단계 **8** **Certificate Download Format(**인증서 다운로드 형식**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **PEM(Private Enhanced Electronic Mail)** 형식의 인증서**, PKCS8 PEM** 형식의 키**(**인증서 체인 포함**))**: 루트 인증서, 중간 CA 인증서 및 최종 엔티티 인증서는 PEM 형식으로 표시됩니다. PEM 형식 인증서는 BASE64 인코딩 ASCII 파일입니다. 각 인증서는 "--------BEGIN CERTIFICATE-----" 태그로 시작하고 "-------END CERTIFICATE----" 태그로 끝납니다. 최종 엔티티의 개인 키는 PKCS * PEM을 사용하여 저장됩니다. "-----BEGIN ENCRYPTED PRIVATE KEY----" 태그로 시작하고 "-----END ENCRYPTED PRIVATE KEY----" 태그로 끝납니다.
- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)(PKCS12** 형식**(**인증서 체인 포함**,** 인증서 체인과 모두를 위한 단일 파일**))**: 루트 CA 인증서, 중간 CA 인증서, 최종 엔티티의 인증서 및 개인 키를 단일 암호화 파일에 저장하는 이진 형식입니다.

단계 **9** **Certificate Password(**인증서 비밀번호**)**: 인증서의 비밀번호를 입력하고 다음 필드에 비밀번호를 다시 입력하여 확인합니다.

단계 **10** **Create(**생성**)**를 클릭합니다.

생성한 인증서는 Cisco ISE의 **Issued Certificates(**발급된 인증서**)** 창에 표시됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Issued Certificates(**발급된 인증서**)**입니다. 인증서는 브라우저의 다운로드 디렉터리에도 다운로드됩니다.

참고 Cisco ISE 2.4 패치 13부터는 pxGrid 서비스에 대한 인증서 요건이 더욱 엄격해졌습니다. Cisco ISE의 기본 SSC(Self-Signed Certificate, 자가서명 인증서)를 pxGrid 인증서로 사용하는 경우 Cisco ISE 2.4 패치 13 이상 버전을 적용한 후 Cisco ISE에서 해당 인증서를 거부할 수 있습니다. 해당 인증서의 이전 버전에서 **Netscape Cert Type(Netscape** 인증서 유형**)** 확장이 **SSL Server(SSL** 서버**)**로 지정되었기 때문에 실패하는 것입니다(이제 클라이언트 인증서도 필요함).

규정 미준수 인증서가 있는 클라이언트는 Cisco ISE와 통합되지 않습니다. 내부 CA에서 발급한 인증서를 사용하거나 적절한 사용 확장을 사용하여 새 인증서를 생성합니다.

- 인증서의 키 사용**(Key Usage)** 확장에는 **Digital Signature(**디지털 서명**)** 및 **Key Encipherment(**키 암호화**)** 필드가 포함되어야 합니다.
- 인증서의 **Extended Key Usage(**확장 키 사용**)** 확장에는 **Client Authentication(**클라이언트 인증**)** 및 **Server Authentication(**서버 인증**)** 필드가 포함되어야 합니다.
- **Netscape Certificate Type(Netscape** 인증서 유형**)** 확장은 필요하지 않습니다. 해당 확장을 포함하려면 확장에 **SSL Client(SSL** 클라이언트**)** 및 **SSL Server(SSL** 서버**)**를 모두 포함해야 합니다.
- 자가서명 인증서를 사용하는 경우 **Basic Constraints CA** 기본 제약 조건 **CA)** 필드를 True로 설정하고 **Key Usage(**키 사용**)** 확장에 **Key Cert Sign(**키 인증서 서명**)** 필드를 포함해야 합니다.

Cisco pxGrid 클라이언트에 대한 권한 제어

Cisco pxGrid 클라이언트에 대한 권한을 제어하기 위한 Cisco pxGrid 권한 부여 규칙을 생성할 수 있습니다. Cisco pxGrid 클라이언트에 제공되는 서비스를 제어하려면 이 규칙을 사용합니다.

서로 다른 유형의 그룹을 생성하고 Cisco pxGrid 클라이언트에 제공된 서비스를 이러한 그룹에 매핑할 수 있습니다. **Client Management(**클라이언트 관리**)** 창에서 **Groups(**그룹**)** 옵션을 사용하여 새 그룹을 추가합니다. **Client Management(**클라이언트 관리**)** > **Policies(**정책**)** 창에서 사전 정의된 그룹(예: EPS 및 ANC)을 사용하는 사전 정의된 권한 부여 규칙을 확인할 수 있습니다. 사전 정의된 규칙에 대해 **Custom Operations(**사용자 맞춤화 작업**)** 필드만 업데이트할 수 있습니다.

pxGrid 클라이언트에 대한 권한 부여 규칙을 생성하려면

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **Client Management(**클라이언트 관리**)** > **Policy(**정책**)**.

단계 **2** **Service(**서비스**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

단계 **3** **Operation(**운영**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **<ANY>**
- **publish**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**

  참고 이 옵션을 선택하면 사용자 맞춤화 작업을 지정할 수 있습니다.

단계 **4** **Groups(**그룹**)** 드롭다운 목록에서 이 서비스에 매핑할 그룹을 선택합니다.

사전 정의된 그룹(예: EPS 및 ANC) 및 수동으로 추가한 그룹이 이 드롭다운 목록에 나열됩니다.

구축 노드 확인

Deployment Nodes(구축 노드**)** 창에서는 구축에 포함된 모든 Cisco ISE 노드(기본 및 보조 노드)를 확인할 수 있습니다.

단계 **1** 기본 Cisco ISE 관리 포털에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

단계 **3** 왼쪽 탐색창에서 **Deployment(**구축**)**를 클릭합니다.

구축에 속하는 모든 Cisco ISE 노드가 나열됩니다.

MnT 노드에서 엔드포인트 통계 데이터 다운로드

MnT 노드에서 네트워크에 연결하는 엔드포인트에 대한 통계 데이터를 다운로드할 수 있습니다. 로드, CPU 사용량, 인증 트래픽 데이터가 포함되어 있는 KPM(Key Performance Metrics)는 네트워크의 문제를 모니터링하고 해결하는 데 사용할 수 있습니다. Cisco ISE CLI(Command Line Interface)에서 **application configure ise** 명령을 사용하여 옵션 12 또는 13을 선택하여 일일 KPM 통계 또는 최근 8주 동안의 KPM 통계를 각각 다운로드할 수 있습니다.

이 명령의 출력은 엔드포인트에 대한 다음 데이터를 제공합니다.

- 네트워크의 총 엔드포인트 수
- 성공적인 연결을 설정한 엔드포인트 수
- 인증에 실패한 엔드포인트 수
- 매일 연결된 새로운 총 엔드포인트 수
- 매일 온보드된 총 엔드포인트 수

출력에는 타임스탬프 세부정보, 구축에서 각 PSN(Policy Service Node)을 통해 연결된 총 엔드포인트 수, 총 엔드포인트 수, 활성 엔드포인트, 로드 및 인증 트래픽 세부정보도 포함됩니다.

이 명령에 대한 자세한 내용은 *Cisco Identity Services Engine CLI Reference Guide*를 참고해 주십시오.

데이터베이스 충돌 또는 파일 손상 문제

정전이 발생하거나 그 외에 데이터가 손실되는 이유로 인해 Oracle 데이터베이스 파일이 손상된 경우 Cisco ISE가 충돌할 수 있습니다. 사고 유형에 따라 아래 단계를 수행하여 데이터 손실을 복구합니다.

- 구축 시 PAN이 손상된 경우에는 보조 PAN을 기본 PAN으로 승격해야 합니다.
- 소규모 구축 또는 기타 이유로 인해 보조 PAN의 승격이 불가능한 경우 사용 가능한 최신 백업을 복원합니다.
- PSN이 손상된 경우, 등록을 취소하고 컨피그레이션을 재설정한 다음 노드를 다시 등록하는 단계를 수행합니다.
- 독립형 디바이스의 경우 사용 가능한 최신 백업을 복원합니다.

참고 최신 컨피그레이션 변경 사항이 손실되지 않도록 독립형 상자에서 정기적으로 백업을 가져옵니다.

모니터링을 위한 디바이스 컨피그레이션

MnT 노드는 대시보드 화면을 채우기 위해 네트워크의 디바이스에서 데이터를 수신하여 사용합니다. MnT 노드와 네트워크 디바이스 간 통신을 위해서는 스위치 및 NAD를 올바르게 구성해야 합니다.

기본 및 보조 Cisco ISE 노드 동기화

기본 PAN을 통해서만 Cisco ISE의 구성을 변경할 수 있습니다. 컨피그레이션 변경사항은 모든 보조 노드로 복제됩니다. 복제가 정상적으로 수행되지 않는 경우에는 보조 PAN을 기본 PAN과 수동으로 동기화할 수 있습니다.

단계 **1** 기본 PAN에 로그인합니다.

단계 **2** **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **3** 기본 PAN과 동기화할 노드 옆의 확인란을 선택하고 **Syncup**을 클릭하여 전체 데이터베이스 복제를 강제로 수행합니다.

노드 페르소나 및 서비스 변경

Cisco ISE 노드 컨피그레이션을 편집하여 노드에서 실행되는 페르소나 및 서비스를 변경할 수 있습니다.

시작하기 전에

- PSN에서 실행되는 서비스를 활성화/비활성화하거나 PSN을 변경하는 경우에는 해당 서비스가 실행되는 애플리케이션 서버 프로세스가 다시 시작됩니다. 이러한 서비스가 다시 시작되는 동안에는 작업이 지연됩니다.
- 서비스가 다시 시작될 때의 이러한 지연으로 인해 구축에서 활성화된 경우 자동 페일오버가 시작될 수 있습니다. 이를 방지하려면 자동 페일오버 컨피그레이션이 꺼져 있는지 확인합니다.

단계 **1** 기본 PAN에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**.

단계 **3** 페르소나 또는 서비스를 변경하려는 노드 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** 원하는 페르소나 및 서비스를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 기본 PAN에서 경보가 수신되는지 확인하여 페르소나 또는 서비스 변경을 확인합니다. 페르소나 또는 서비스 변경 사항이 정상적으로 저장되지 않으면 경보가 생성되지 않습니다.

Cisco ISE에서 노드 수정의 효과

Cisco ISE의 노드를 다음과 같이 변경하면 해당 노드가 다시 시작되어 지연이 발생하게 됩니다.

- 노드 등록(독립형에서 보조로)
- 노드 등록 취소(보조에서 독립형으로)
- 기본 노드를 독립형으로 변경(다른 노드가 등록되지 않은 경우, 기본에서 독립형으로)
- 관리 노드 승격(보조에서 기본으로)
- 페르소나 변경(정책 서비스 또는 모니터링 페르소나를 노드에서 할당하거나 제거하는 경우)
- 정책 서비스 노드에서 서비스 수정(세션 및 프로파일러 서비스 활성화 또는 비활성화)
- 기본 노드에서 백업을 복원하면 동기화 작업이 트리거되어 기본 노드에서 보조 노드로 데이터 복제

정책 서비스 노드 그룹 생성

둘 이상의 PSN(Policy Service Node)이 같은 고속 LAN(Local Area Network)에 연결되어 있을 때 해당 노드를 같은 노드 그룹에 배치하는 것이 좋습니다. 이 설계를 사용하는 경우 중요도가 낮은 속성을 그룹에 로컬로 유지하고 네트워크에서 원격 노드로 복제되는 정보를 줄여 엔드포인트 프로파일링 데이터 복제를 최적화할 수 있습니다. 노드 그룹 멤버는 피어 그룹 멤버의 가용성도 확인합니다. 그룹은 멤버에 장애가 발생했음을 탐지하면 장애가 발생한 노드에서 URL로 리디렉션된 모든 세션의 재설정 및 복구를 시도합니다.

참고 모든 PSN을 같은 노드 그룹의 동일 로컬 네트워크 부분에서 만드는 것이 좋습니다. PSN이 같은 노드 그룹에 가입하기 위해 로드 밸런싱된 클러스터의 일부분일 필요는 없습니다. 그러나 로드 밸런싱된 클러스터의 각 로컬 PSN은 일반적으로 같은 노드 그룹의 일부분이어야 합니다.

참고 노드 그룹은 URL 리디렉션(포스처 서비스, 게스트 서비스 및 MDM)이 적용된 세션의 PSN 페일오버에 사용됩니다.

PSN을 노드 그룹에 멤버로 추가하기 전에 노드 그룹을 먼저 생성해야 합니다. 관리 포털의 **Depolyment(**구축**)** 창에서 PSN 그룹을 생성, 편집 및 삭제할 수 있습니다.

시작하기 전에

노드 그룹 멤버는 TCP/7800을 통해 통신할 수 있습니다.

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

단계 **2** 왼쪽 탐색창 상단에서 **Settings(**설정**)** 아이콘을 클릭합니다.

단계 **3** **Create Node Group(**노드 그룹 생성**)**을 클릭합니다.

단계 **4** 노드 그룹의 고유한 이름을 입력합니다.

참고 노드 등록에서 바람직하지 않은 문제가 발생할 수 있으므로 이름이 **None**인 노드 그룹을 구성하지 않는 것이 좋습니다.

단계 **5** (선택 사항) 노드 그룹에 대한 설명을 입력합니다.

단계 **6** (선택 사항) **Enable MAR Cache Distribution(MAR** 캐시 배포 활성화**)** 확인란을 선택하고 다른 옵션을 입력합니다. 이 옵션을 활성화하기 전에 **Active Directory** 창에서 MAR이 활성화되어 있는지 확인하십시오.

단계 **7** **Submit(**제출**)**을 클릭하여 노드 그룹을 저장합니다.

저장한 노드 그룹은 왼쪽 탐색 창에 표시됩니다. 왼쪽 창에 노드 그룹이 표시되지 않는 경우 해당 그룹이 숨겨져 있는 것일 수 있습니다. 숨겨진 개체를 보려면 탐색창에서 **Expand(**확장**)** 버튼을 클릭합니다.

다음에 수행할 작업

노드 그룹에 노드를 추가합니다. **Policy Service(**정책 서비스**)**에 있는 **Include node in node group(**노드 그룹의 노드 포함**)** 드롭다운 목록에서 노드 그룹을 선택하여 노드를 편집합니다.

구축에서 노드 제거

구축에서 노드를 제거하려면 노드 등록을 취소해야 합니다. 등록 취소된 노드는 독립형 Cisco ISE 노드로 설정됩니다.

이 노드는 기본 PAN에서 받은 마지막 컨피그레이션을 유지하며 독립형 노드의 기본 페르소나(관리, 정책 서비스, 모니터링)로 지정됩니다. MnT 노드는 등록 취소하는 경우 더 이상 시스템 로그 대상으로 사용되지 않습니다.

기본 PSN의 등록을 취소하면 엔드포인트 데이터가 손실됩니다. PSN이 독립형 노드가 된 후 엔드포인트 데이터를 유지하도록 하려는 경우 다음 중 하나를 수행할 수 있습니다.

- 기본 PAN에서 백업을 가져온 다음 PSN이 독립형 노드가 되면 해당 노드에서 이 데이터 백업을 복구합니다.
- PSN의 페르소나를 관리(보조 PAN)로 변경하고 관리 포털의 **Deployment(**구축**)** 창에서 데이터를 동기화한 다음 노드 등록을 취소합니다. 이제 이 노드에 모든 데이터가 포함됩니다. 그런 다음 보조 PAN을 기존 구축에 추가할 수 있습니다.

기본 PAN의 구축 창에서 이러한 변경사항을 확인할 수 있습니다. 그러나 이러한 변경사항이 적용되어 구축 창에 표시될 때까지는 5분 정도 지연될 수 있습니다.

시작하기 전에

구축에서 보조 노드를 제거하기 전에 Cisco ISE 컨피그레이션의 백업을 수행해 주십시오. 필요한 경우 나중에 이 백업을 복원할 수 있습니다.

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

단계 **2** 제거할 보조 노드 옆의 확인란을 선택하고 **Deregister(**등록 취소**)**를 클릭합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 기본 PAN에서 경보가 수신되는지 확인하여 보조 노드가 정상적으로 등록 취소되었음을 확인합니다. 보조 노드가 기본 PAN에서 등록 취소되지 않으면 경보는 생성되지 않습니다.

Cisco ISE 노드 종료

Cisco ISE CLI(Command Line Interface)에서 `halt` 명령을 실행하기 전에 Cisco ISE 애플리케이션 서비스를 중지하고 백업, 복구, 설치, 업그레이드 또는 제거 작업을 수행하지 않는 것이 좋습니다. Cisco ISE에서 이러한 작업 중 하나를 수행 중일 때 halt 명령을 실행하는 경우, 다음 경고 메시지 중 하나가 표시됩니다.

```
WARNING: A backup or restore is currently in progress! Continue with halt?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

halt 명령을 사용 중일 때 프로세스를 실행하고 있지 않은 경우 또는 표시되는 경고 메시지에 대한 응답에 `Yes`를 입력하는 경우, 다음 질문에 응답해야 합니다.

```
Do you want to save the current configuration?
```

기존 Cisco ISE 구성을 저장하기 위해 `Yes`를 입력하는 경우 다음 메시지가 표시됩니다.

```
Saved the running configuration to startup successfully.
```

참고 어플라이언스를 재부팅하기 전에 애플리케이션 프로세스를 중지하는 것이 좋습니다.

이는 Cisco ISE 재부팅에도 적용됩니다. 자세한 내용은 Cisco Identity Services Engine CLI Reference Guide를 참고해 주십시오.

독립형 Cisco ISE 노드의 호스트 이름 또는 IP 주소 변경

독립형 Cisco ISE 노드의 호스트 이름, IP 주소 또는 도메인 이름을 변경할 수 있습니다. 노드의 호스트 이름으로 `localhost`를 사용할 수 없습니다.

시작하기 전에

Cisco ISE 노드가 분산형 구축의 일부분인 경우에는 구축에서 해당 노드를 제거하고 독립형 노드인지를 확인해야 합니다.

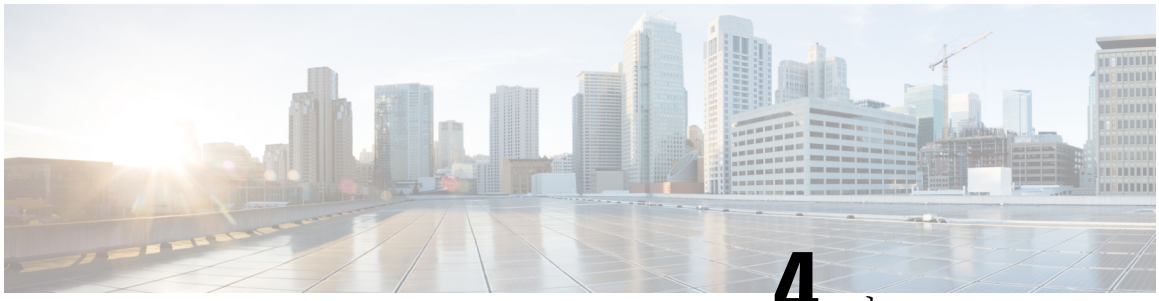
단계 **1** Cisco ISE CLI에서 **hostname**, **ip address,** 또는 **ip domain-name** 명령을 사용하여 Cisco ISE 노드의 호스트 이름이나 IP 주소를 변경합니다.

단계 **2** 모든 서비스를 다시 시작하려면 Cisco ISE CLI에서 **application stop ise** 명령을 사용하여 Cisco ISE 애플리케이션 구성을 재설정합니다.

단계 **3** Cisco ISE 노드가 분산형 구축의 일부분인 경우에는 기존 PAN에 해당 노드를 등록합니다.

참고 Cisco ISE 노드를 등록하는 동안 호스트 이름을 사용하는 경우에는 *abc.xyz.com*과 같이 등록하려는 독립형 노드의 FQDN(Fully Qualified Domain Name)이 기본 PAN의 DNS 확인 가능 이름이어야 합니다. 그렇지 않으면 노드 등록이 실패합니다. DNS 서버에서 분산형 구축의 일부분인 Cisco ISE 노드의 IP 주소와 FQDN을 입력해야 합니다.

Cisco ISE 노드를 보조 노드로 등록하고 나면 기본 PAN이 IP 주소, 호스트 이름 또는 도메인 이름의 변경사항을 구축의 다른 Cisco ISE 노드로 복제합니다.



4 장

기본 설정

관리 포털

그림 ***2: Cisco ISE*** 관리 포털

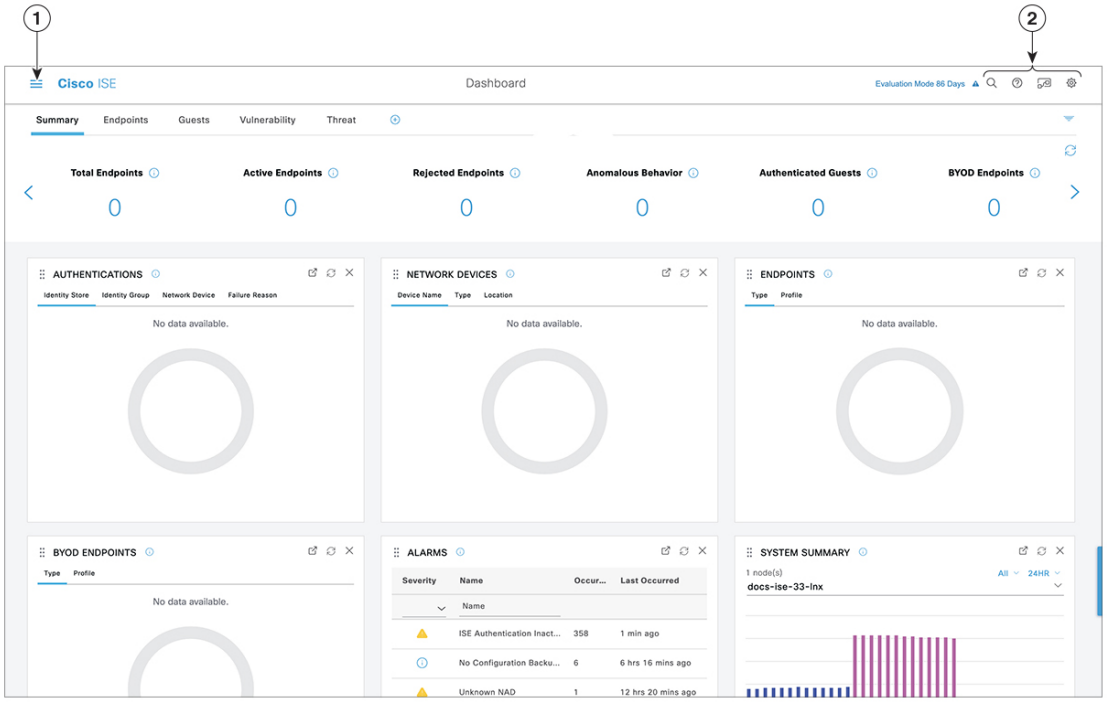
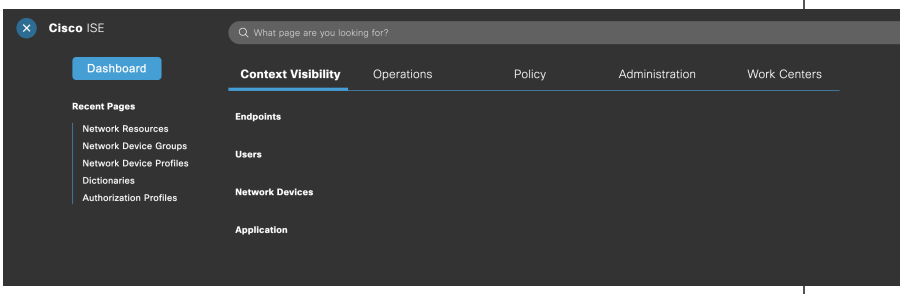


표 ***12: Cisco ISE*** 관리 포털의 구성 요소

1	메뉴 아이콘	다음 메뉴가 있는 슬라이드식 창에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭합니다. 슬라이드식 메뉴 창에는 필요한 창을 찾을 수 있는 검색 창도 포함되어 있습니다. 홈 페이지의 **Dashboard(**대시보드**)**를 클릭합니다. 그림 ***3: Cisco ISE*** 주 메뉴  • **Context Visibility(**상황 가시성**)**: 상황 가시성 창에는 엔드포인트, 사용자 및 NAD(Network Access Device)에 대한 정보가 표시됩니다. 상황 가시성 정보는 등록한 라이선스에 따라 기능, 애플리케이션, BYOD(Bring Your Own Device) 및 기타 범주별로 구분됩니다. 상황 가시성 창은 중앙 데이터베이스를 사용하며 데이터베이스 표, 캐시 및 버퍼에서 정보를 수집합니다. 따라서 상황 가시성 dashlet 및 목록의 콘텐츠가 빠르게 업데이트됩니다. 상황 가시성 창은 상단의 dashlet과 하단의 정보 목록으로 구성되어 있습니다. 목록에서 열 속성을 수정하여 데이터를 필터링하면 dashlet이 새로 고침되어 변경된 콘텐츠가 보여집니다. • **Policy(**정책**)**: 정책 창은 인증, 권한 부여, 프로파일링, 포스처 및 클라이언트 프로비저닝 영역에서 네트워크 보안을 관리할 수 있는 도구를 포함합니다. • **Administration(**관리**)**: 관리 창은 Cisco ISE 노드, 라이선스, 인증서, 네트워크 디바이스, 사용자, 엔드포인트 및 게스트 서비스를 관리할 수 있는 도구를 포함합니다.

2	오른쪽 상단 메뉴 아이콘	

-

  이 아이콘을 이용해 엔드포인트를 검색하고 프로파일, 장애, ID 저장소, 위치, 디바이스 유형 등을 기준으로 배포를 표시할 수 있습니다.

-

  아이콘을 클릭하면 여러 리소스에 대한 액세스를 제공하는 대화형 도움말 메뉴가 표시됩니다.

-

  다음 옵션에 액세스하려면 이 아이콘을 클릭합니다.

  - **PassiveID Setup(PassiveID** 설정**)**: **PassiveID Setup(PassiveID** 설정**)** 옵션은 Active Directory를 사용하여 수동 ID를 설정하기 위해 **PassiveID Setup(PassiveID** 설정**)** 마법사를 실행합니다. 외부 인증 서버에서 사용자 ID 및 IP 주소를 수집하고 인증된 IP 주소를 해당 가입자에게 전달하도록 서버를 구성합니다.

  - **Visibility Setup(**가시성 설정 **)**: **Visibility Setup(**가시성 설정 **)**은 애플리케이션, 하드웨어 인벤토리, USB 상태, 방화벽 상태 및 Windows 엔드포인트의 전체 규정 준수 상태와 같은 엔드포인트 데이터를 수집하는 PoV(Proof of Value) 서비스입니다. 수집된 데이터는 이후 Cisco ISE로 전송됩니다. **ISE Visibility Setup(ISE** 가시성 설정**)** 마법사를 실행할 때, 네트워크의 선호되는 세그먼트 또는 엔드포인트 그룹에 대해 엔드포인트 검색을 실행할 IP 주소 범위를 지정할 수 있습니다.

    PoV 서비스는 Cisco Stealth Temporal 에이전트를 사용하여 엔드포인트 포스처 데이터를 수집합니다. Cisco ISE는 관리자 계정 유형으로 Windows를 실행하는 컴퓨터에 Cisco Stealth Temporal 에이전트를 푸시합니다. 에이전트는 자동으로 임시 실행 파일을 실행하여 상황을 수집합니다. 그 후 에이전트가 자동으로 제거됩니다. Cisco Stealth Temporal 에이전트의 디버그 기능(선택 사항)을 사용하려면 **Endpoint Logging(**엔드포인트 로깅**)** 확인란을 선택(**Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Visibility Setup(**가시성 설정**)** > **Posture(**포스처**)** 선택) 하여 디버그 로그를 엔드포인트 또는 여러 엔드 포인트에 저장합니다. 다음 위치 중 하나에서 로그를 볼 수 있습니다.

    - C:\WINDOWS\syswow64\config\systemprofile\ (64비트 운영체제)
    - C:\WINDOWS\system32\config\systemprofile\ (32비트 운영체제)

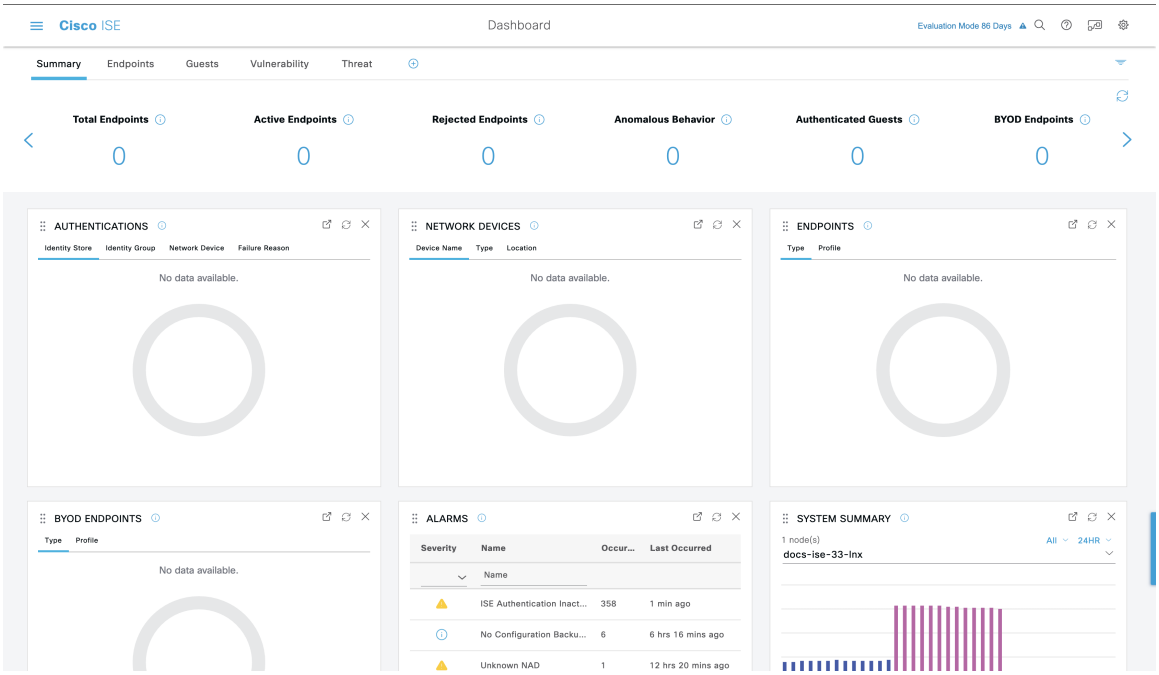
  - **Run Endpoint Scripts(**엔드포인트 스크립트 실행**)**: 연결된

		엔드 포인트에서 스크립트를 실행하여 조직의 요건을 준수하는 관리 작업을 수행하려면 이 옵션을 선택합니다. 여기에는 더 이상 사용되지 않는 소프트웨어 제거, 프로세스 또는 애플리케이션의 시작 또는 종료, 특정 서비스의 활성화 또는 비활성화 작업이 포함됩니다. •  온라인 도움말 실행 및 어카운트 설정 구성 등 시스템 활동에 대한 메뉴를 보려면 이 아이콘을 클릭합니다.

Cisco ISE 홈 대시보드

Cisco ISE Home(홈) 대시보드에는 상관 통계가 지정된 실시간 통합 데이터가 표시되는데, 이는 효과적인 모니터링 및 문제 해결을 위해 필수적입니다. 대시보드 요소는 일반적으로 24시간 동안의 활동을 표시합니다. 다음 그림에는 Cisco ISE 대시보드에서 사용할 수 있는 정보의 예가 나와 있습니다. 기본 PAN(Policy Administration Node) 포털에서만 Cisco ISE 대시보드 데이터를 볼 수 있습니다.

그림 ***4: Cisco ISE*** 홈 대시보드



홈 페이지에는 Cisco ISE 데이터를 표시하는 5개의 기본 대시보드가 있습니다. 이러한 각 대시보드에는 사전 정의된 여러 dashlet이 있습니다.

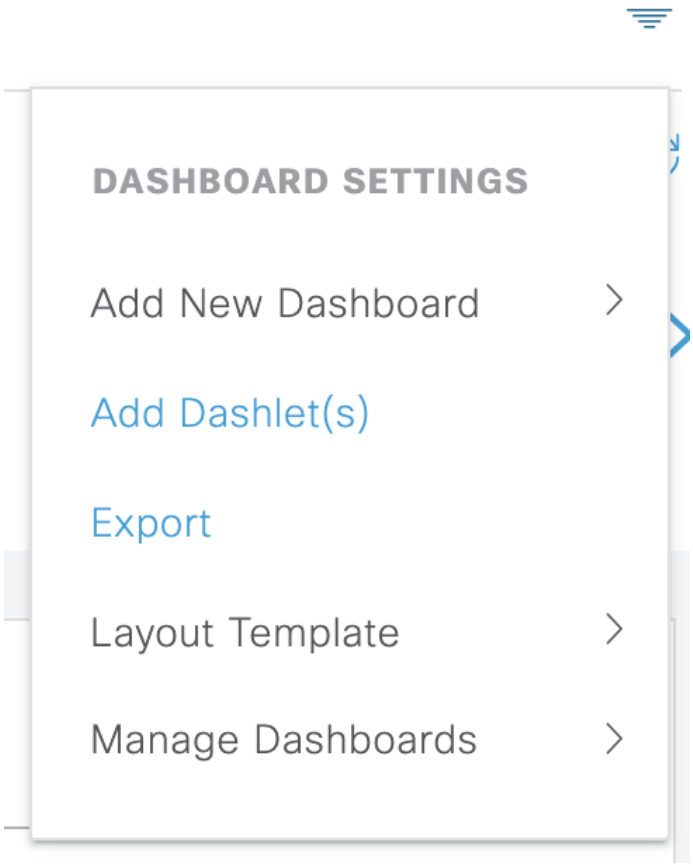
- **Summary(**요약**)**: 이 대시보드에는 선형 메트릭 dashlet, 원형 차트 dashlet 및 목록 dashlet이 포함됩니다. 메트릭 dashlet은 구성할 수 없습니다. 기본적으로 이 대시보드에는 **Status(**상태**) Endpoints(**엔드포인트**)**, **Endpoint Categories(**엔드포인트 범주**)** 및 **Network Devices(**네트워크 디바이스**)** dashlet이 포함됩니다.

- **Endpoints(**엔드포인트**)**: 기본적으로 이 대시보드에는 **Status(**상태**)**, **Endpoints(**엔드포인트**)**, **Endpoint Categories(**엔드포인트 범주**)** 및 **Network Devices(**네트워크 디바이스**)** dashlet이 포함됩니다.
- **Guests(**게스트**)**: 이 대시보드에는 게스트 사용자 유형, 로그인 실패 및 활동 위치에 대한 정보를 제공하는 dashlet이 포함됩니다.
- **Vulnerability(**취약점**)**: 이 대시보드에는 취약점 서버가 Cisco ISE에 보고하는 정보가 표시됩니다.
- **Threat(**위협**)**: 이 대시보드에는 Cisco ISE로 전송한 위협 서버 보고서의 정보가 표시됩니다.

홈 대시보드 구성

창 오른쪽 상단에 있는 **Inverted Pyramid(**역 피라미드**)** 아이콘를 클릭하여 홈 페이지 대시보드를 사용자 맞춤화할 수 있습니다.

그림 ***5:*** 대시보드 사용자 맞춤화



드롭다운 목록에 다음과 같은 옵션이 표시됩니다.

- **Add New Dashboard(**새 대시보드 추가**)**를 통해 새 대시보드를 추가할 수 있습니다. 표시되는 필드에 값을 입력하고 **Apply(**적용**)**를 클릭합니다.
- **Add Dashlet(s)(dashlet** 추가**)**를 선택하면 사용 가능한 dashlet 목록이 포함된 대화 상자가 표시됩니다. 대시보드에서 dashlet을 추가하거나 제거하려면 dashlet 이름 옆에 있는 **Add(**추가**)** 또는 **Remove(**제거**)**를 클릭합니다.
- **Export(**내보내기**)**를 사용하면 선택한 홈 페이지 보기가 PDF로 저장됩니다.
- **Layout Template(**레이아웃 템플릿**)**을 통해 이 보기에 표시되는 열 수를 구성할 수 있습니다.
- **Manage Dashboards(**대시 보드 관리**)**에는 두 가지 옵션이 있습니다.
  - **Mark as Default Dashboard(**기본 대시보드로 표시**)**: 현재 대시보드를 Home(홈)에 표시되는 기본 보기로 설정하려면 이 옵션을 선택합니다.
  - **Reset All Dashboards(**모든 대시보드 재설정**)**: 모든 대시보드를 재설정하고 모든 홈 대시보드에서 기존 구성을 제거하려면 이 옵션을 사용합니다.

상황 가시성 보기

Context Visibility(상황 가시성**)** 창의 구조는 다음을 제외하고 홈 페이지와 유사합니다.

- 표시된 데이터를 필터링할 때 현재 상황(브라우저 창) 유지
- 보다 사용자 맞춤화 가능
- 엔드포인트 데이터에 중점

기본 PAN에서만 상황 가시성 데이터를 볼 수 있습니다.

Context Visibility(상황 가시성**)** 창의 dashlet에는 엔드포인트 및 NAD에 대한 엔드포인트 연결 정보가 표시됩니다. 현재 표시되는 정보는 각 창의 dashlet 아래에 있는 데이터 목록 내용을 기반으로 합니다. 각 창에는 탭 이름을 기반으로 엔드포인트 데이터가 표시됩니다. 데이터를 필터링하면 목록과 dashlet이 모두 업데이트됩니다. 하나 이상의 원형 그래프 부분을 클릭하거나 표의 행을 필터링하거나 이러한 작업을 조합하여 데이터를 필터링할 수 있습니다. 필터를 선택하면 캐스케이딩 필터라고도 하는 효과가 추가로 표시되며, 이를 통해 원하는 특정 데이터를 찾을 수 있습니다. 또한 목록에서 엔드포인트를 클릭하면 해당 엔드포인트의 세부정보 보기가 표시됩니다.

Context Visibility(상황 가시성**)** 아래에는 4가지 기본 메뉴 옵션이 있습니다.

- **Endpoints(**엔드포인트**)**: 디바이스 유형, 규정 준수 상태, 인증 유형, 하드웨어 인벤토리 등에 따라 표시할 엔드포인트를 필터링합니다. 자세한 내용은 하드웨어 대시보드, 108 페이지의 내용을 참조하십시오.

참고 NAD(네트워크 액세스 디바이스)에서 계정 관리 설정을 활성화하여 계정 관리 시작 및 업데이트 정보가 Cisco ISE로 전송되도록 하는 것이 좋습니다.

Cisco ISE는 계정 관리가 활성화된 경우에만 최신 IP 주소, 세션 상태(연결됨, 연결 해제됨 또는 거부됨), 엔드포인트가 비활성화된 일 수 등과 같은 계정 관리 정보를 수집할 수 있습니다. 이 정보는 Cisco ISE 관리 포털의 **Live Logs(**라이브 로그**)**, **Live Sessions(**라이브 세션**)** 및 **Context Visibility(**상황 가시성**)** 창에 표시됩니다. NAD에서 계정 관리가 비활성화된 경우 **Live Sessions(**라이브 세션**)**, **Live Logs(**라이브 로그**)** 및 **Context Visibility(**상황 가시성**)** 창 간에 계정 관리 정보가 누락되거나, 부정확하거나, 일치하지 않을 수 있습니다.

참고 Cisco ISE 관리 포털 홈 페이지에서 사용 가능한 **Visibility Setup(**가시성 설정**)** 워크플로우를 사용하면 엔드포인트 검색을 위한 IP 주소 범위 목록을 추가할 수 있습니다. 이 워크플로우를 구성하고 나면 Cisco ISE에서 엔드포인트를 인증하지만 구성된 IP 주소 범위에 포함되지 않은 엔드포인트가 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** 창 및 **Endpoints(**엔드포인트**)** 목록 페이지(**Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**))**에 표시되지 않습니다.

- **Users(**사용자**)**: 사용자 ID 소스의 사용자 기반 정보를 표시합니다

  사용자 이름 또는 비밀번호 속성이 변경된 경우 인증 상태가 변경되면 **Users(**사용자**)** 창에 반영됩니다.

  Microsoft Active Directory에서 사용자 이름 이외의 속성이 변경된 경우에는 재인증 24시간 후에 업데이트된 속성이 **Users(**사용자**)** 창에 표시됩니다.

  Microsoft Active Directory에서 사용자 이름 및 기타 속성을 변경하면 재인증 후 업데이트된 변경 사항이 즉시 **Users(**사용자**)** 창에 표시됩니다.

- **Network Devices(**네트워크 디바이스**)**: 이 창은 엔드포인트가 연결된 NAD의 목록을 표시합니다. NAD의 경우 해당 **# of endpoints(**엔드포인트 수**)** 열에 표시되는 엔드포인트 수를 클릭합니다. 해당 NAD로 필터링된 모든 디바이스를 나열하는 창이 표시됩니다.

참고 SNMPv3 매개변수를 사용하여 네트워크 디바이스를 구성한 경우에는 Cisco ISE 모니터링 서비스의 **Operations(**작업**)** > **Reports(**보고서**)** > **Catalog(**카탈로그**)** > **Network Device(**네트워크 디바이스**)** > **Session Status Summary(**세션 상태 요약**)**에서 제공되는 **Network Device Session Status Summary(**네트워크 디바이스 세션 상태 요약**)** 보고서를 생성할 수 없습니다. 네트워크 디바이스가 SNMPv1 또는 SNMPv2c 매개변수로 구성된 경우 이 보고서를 정상적으로 생성할 수 있습니다.

- **Application(**애플리케이션**)**: 이 창을 사용하여 특정 애플리케이션이 설치된 엔드포인트 수를 확인할 수 있습니다. 결과는 그래픽 및 표 형식으로 표시됩니다. 그래픽 표현은 비교 분석을 수행하는 데 유용합니다. 예를 들어 Google Chrome 소프트웨어가 있는 엔드포인트의 수와 버전, 벤더 및 범주(안티 피싱, 브라우저 등)를 표와 막대 그래프로 확인할 수 있습니다. 자세한 내용은 애플리케이션 대시보드을 참고하십시오.

Context Visibility(상황 가시성**)** 창에서 새 탭을 생성하여 추가 필터링을 위한 사용자 맞춤화 목록을 생성할 수 있습니다. 사용자 맞춤화 보기에서는 dashlet이 지원되지 않습니다.

dashlet에서 원형 그래프의 섹션을 클릭하여 해당 dashlet에서 필터링된 데이터가 포함된 새 창을 표시합니다. 이 새 창에서 보기에서 표시되는 데이터 필터링, 112 페이지에 설명된 대로 표시된 데이터를 계속 필터링할 수 있습니다.

Context Visibility(상황 가시성) 창을 사용하여 엔드포인트 데이터를 찾는 방법에 대한 자세한 내용은 ISE 2.1을 사용하는 Cisco YouTube 비디오(https://www.youtube.com/watch?v=HvonGhrydfg)를 참고하십시오.

관련 항목

하드웨어 대시보드, 108 페이지

상황 가시성의 속성

상황 가시성에 대한 속성을 제공하는 시스템 및 서비스는 동일한 속성 이름에 대해 서로 다른 값을 가질 수 있습니다. 몇 가지 예를 들면 다음과 같습니다.

운영체제

- *OperatingSystem*: 포스처 운영체제
- *operating-system*: NMAP 운영체제
- *operating-system-result*: 프로파일러 통합 운영체제

참고 Cisco ISE에서 엔드포인트에 대해 여러 프로브가 활성화된 경우 상황 가시성 창에 표시되는 엔드포인트 운영체제 데이터에 일부 불일치가 있을 수 있습니다.

포털 이름

- *Portal.Name*: 디바이스 등록이 설정되어 있을 때의 게스트 포털 이름입니다.
- *PortalName*: 디바이스 등록이 설정되어 있지 않을 때의 게스트 포털 이름입니다.

포털 사용자의 경우

- *User-Name*: RADIUS 인증의 사용자 이름
- *GuestUserName*: 게스트 사용자
- *PortalUser*: 포털 사용자

애플리케이션 대시보드

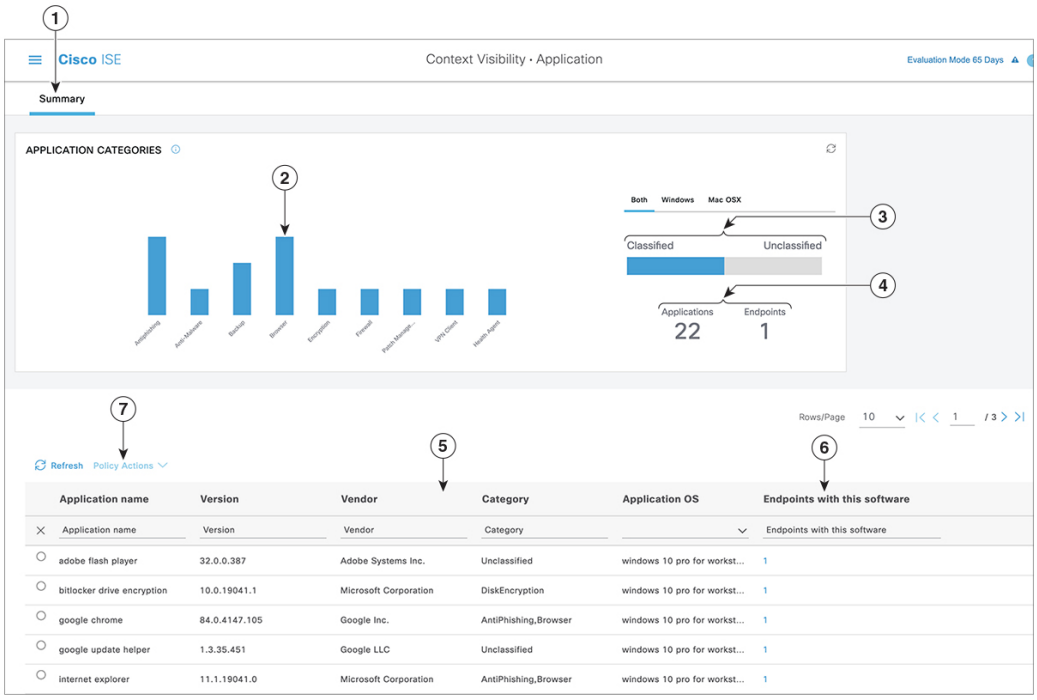


표 ***13:*** 애플리케이션 대시보드에 대한 설명

라벨	설명
1	**Summary(**요약**)** 탭은 홈 페이지에 기본적으로 표시됩니다. 막대 차트가 포함된 **Application Categories(**애플리케이션 범주**)** 대시릿이 표시됩니다. 애플리케이션은 13개 범주로 분류됩니다. 이러한 범주에 속하지 않는 애플리케이션은 미분류로 그룹화됩니다. 사용 가능한 범주는 안티멀웨어, 안티피싱, 백업, 브라우저, 데이터 손실 방지, 데이터 스토리지, 암호화, 방화벽, 메신저, 패치 관리, 공용 파일 공유, 가상 머신 및 VPN 클라이언트입니다.
2	각 막대는 분류 범주를 나타냅니다. 각 막대 위로 마우스를 올려 선택한 애플리케이션 범주에 해당하는 총 애플리케이션 및 엔드포인트 수를 확인합니다.

<table>
<tr><th>라벨</th><th>설명</th></tr>
<tr><td>3</td><td>분류 범주에 속하는 애플리케이션 및 엔드포인트는 파란색으로 표시됩니다. 미분류 애플리케이션 및 엔드포인트는 회색으로 표시됩니다. 분류 또는 미분류 범주 막대 위에 마우스를 올려 해당 범주에 속하는 총 애플리케이션 및 엔드포인트 수를 확인합니다. Classified(분류)를 클릭하고 막대 그래프 및 창의 표에서 결과를 볼 수 있습니다. Unclassified(미분류)를 클릭하면 막대 차트가 비활성화되고 결과가 창의 표에 표시됩니다.</td></tr>
<tr><td>4</td><td>선택한 필터에 따라 애플리케이션 및 엔드포인트가 표시됩니다. 다양한 필터를 클릭하여 Breadcrumb Trail을 볼 수 있습니다. Clear All Filters(모든 필터 지우기)를 클릭하여 모든 적용된 필터를 제거할 수 있습니다.</td></tr>
<tr><td>5</td><td>여러 막대를 클릭하면 해당하는 분류 애플리케이션 및 엔드포인트가 표에 표시됩니다. 예를 들어 안티멀웨어 및 패치 관리 범주를 선택하면 다음 결과가 표시됩니다.
<table>
<tr><th>애플리케이션 이름</th><th>Version(버전)</th><th>Vendor(벤더)</th><th>카테고리</th><th>애플리케이션 OS</th><th>이 소프트웨어를 사용하는 엔드포인트</th></tr>
<tr><td>게이트키퍼</td><td>9.9.5</td><td>Apple Inc.</td><td>악성코드 차단</td><td>windows 7 64 비트, mac osx 10.10, mac osx 8, mac osx 9</td><td>5</td></tr>
<tr><td>게이트키퍼</td><td>10.9.5</td><td>Apple Inc.</td><td>악성코드 차단</td><td>Windows 8 64 비트, mac osx 10.10</td><td>3</td></tr>
<tr><td>소프트웨어 업데이트</td><td>2.3</td><td>Apple Inc.</td><td>패치 관리</td><td>Windows 7 64 비트, mac osx 10.10, mac osx 8, mac osx 9</td><td>5</td></tr>
</table></td></tr>
<tr><td>6</td><td>표의 Endpoints With This Software(이 소프트웨어를 사용하는 엔드포인트) 열에서 엔드포인트를 클릭하면 Mac 주소, NAD IP 주소, NAD 포트 ID/SSID, IPv4 주소 등의 엔드포인트 세부정보가 표시됩니다.</td></tr>
<tr><td>7</td><td>애플리케이션 이름을 선택하고 Policy Actions(정책 작업) 드롭다운 목록에서 Create App Compliance(앱 규정 준수 생성) 옵션을 선택하여 애플리케이션 규정 준수 조건 및 교정을 생성할 수 있습니다.</td></tr>
</table>

하드웨어 대시보드

Context Visibility(상황 가시성) 아래의 Endpoint Hardware(엔드포인트 하드웨어) 탭을 사용하면 짧은 시간 내에 엔드포인트 하드웨어 인벤토리 정보를 수집, 분석 및 보고할 수 있습니다. 메모리 용량이 낮은 엔드포인트, 엔드포인트의 BIOS 모델/버전을 찾는 등 원하는 정보를 수집할 수 있습니다. 이러한 결과를 기반으로 메모리 용량을 늘리거나 BIOS 버전을 업그레이드할 수 있습니다. 자산 구매를

계획하기 전에 요건을 평가할 수 있습니다. 적시에 리소스를 교체할 수 있습니다. 모듈을 설치하거나 엔드포인트와 상호 작용하지 않고도 해당 정보를 수집할 수 있습니다. 요약하면, 자산 라이프 사이클의 효과적인 관리가 가능해집니다.

Context Visibility(상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Hardware(**하드웨어**)** 페이지는 **Manufacturers(**제조업체**)** 및 **Endpoint Utilizations(**엔드포인트 사용률**)** dashlet에 표시됩니다. 이러한 dashlet에는 선택한 필터에 따라 변경사항이 반영됩니다. **Manufacturers(**제조업체**)** dashlet에는 Windows 및 Mac OS가 있는 엔드포인트의 하드웨어 인벤토리 세부정보가 표시됩니다. **Endpoint Utilizations(**엔드포인트 사용률**)** dashlet에는 엔드포인트의 CPU, 메모리 및 디스크 사용률이 표시됩니다. 3가지 옵션 중 하나를 선택하여 사용률을 백분율로 볼 수 있습니다.

- n% 이상의 CPU 사용량을 보이는 디바이스
- n% 이상의 메모리 사용량을 보이는 디바이스
- n% 이상의 디스크 사용량을 보이는 디바이스

참고 하드웨어 인벤토리 데이터가 ISE GUI에 표시되는 데 120초가 걸립니다. 포스처 규정 준수 및 규정 미준수 상태에 대해 하드웨어 인벤토리 데이터가 수집됩니다.

참고
- Hardware Visibility(하드웨어 가시성) 페이지의 빠른 필터를 적용하려면 3자 이상이어야 합니다. 빠른 필터가 효율적으로 작동하도록 하는 또 다른 방법은 문자를 입력한 후 다른 열 속성의 필터를 클릭하는 것입니다.
- 이 표는 하드웨어 관련 속성을 기준으로 필터링하는 데만 사용되므로 일부 열 속성은 회색으로 표시됩니다.
- 운영체제 필터는 **Manufacturers(**제조업체**)** 차트에만 적용됩니다. 아래 표와는 관련이 없습니다.

엔드포인트 및 연결된 외부 디바이스의 하드웨어 속성이 표 형식으로 표시됩니다. 다음과 같은 하드웨어 속성이 표시됩니다.

- MAC 주소
- BIOS 제조업체
- BIOS 일련 번호
- BIOS 모델
- 연결된 디바이스
- CPU 이름
- CPU 속도(GHz)
- CPU 사용량(%)

- 코어 수
- 프로세스 수
- 메모리 크기(GB)
- 메모리 사용량(%)
- 총 내부 디스크 크기(GB)
- 사용 가능한 총 내부 디스크 크기(GB)
- 총 내부 디스크 사용량(%)
- 내부 디스크 수
- NAD 포트 ID
- 상태
- 네트워크 디바이스 이름
- 위치
- UDID
- IPv4 주소
- 사용자 이름
- 호스트 이름
- OS 유형
- 비정상적 동작
- 엔드포인트 프로파일
- 설명
- 엔드포인트 유형
- ID 그룹
- 등록 날짜
- ID 저장소
- 권한 부여 프로파일

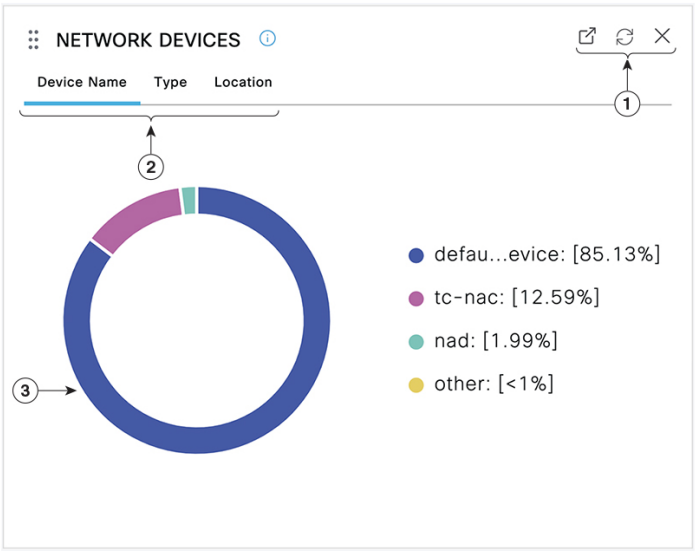
엔드포인트에 해당하는 **Attached Devices(**연결된 디바이스**)** 열의 번호를 클릭하면 현재 엔드포인트에 연결된 USB 디바이스의 이름, 범주, 제조업체, 유형, 제품 ID 및 벤더 ID를 볼 수 있습니다.

참고 Cisco ISE는 클라이언트 시스템의 하드웨어 속성을 프로파일링하지만, Cisco ISE가 프로파일링하지 않는 몇 가지 하드웨어 속성이 있을 수 있습니다. 이러한 하드웨어 속성은 Hardware Context Visibility(하드웨어 상황 가시성) 페이지에 나타나지 않을 수 있습니다.

하드웨어 인벤토리 데이터 수집 간격은 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **General Settings(**일반 설정**)** 페이지에서 제어할 수 있습니다. 기본 간격은 5분입니다.

Dashlet

다음 이미지는 dashlet의 예입니다.



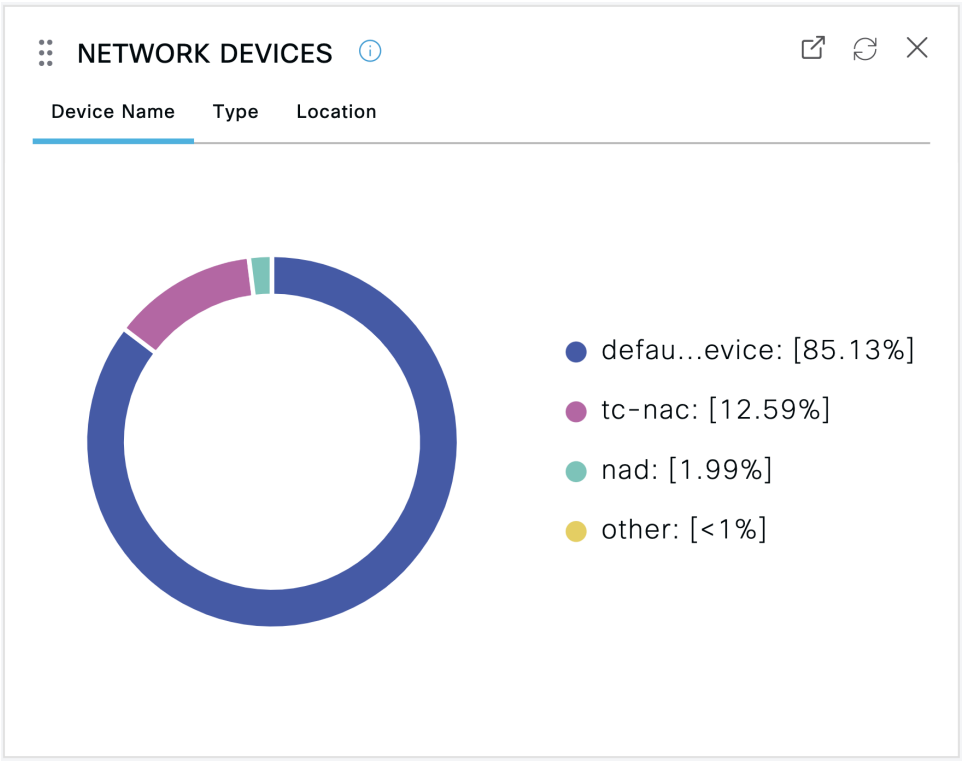
1. 열린 새 창 아이콘을 클릭하면 새 브라우저 창에서 이 dashlet이 열립니다. 파이 차트가 새로 고쳐집니다. 이 dashlet을 삭제하려면 **X**를 클릭합니다. 이 옵션은 홈 페이지에서만 사용할 수 있습니다. 화면 오른쪽 상단의 기어 기호를 사용하면 상황 가시성 창에서 dashlet이 삭제됩니다.
2. 일부 dashlet은 데이터 범주가 서로 다릅니다. 해당 데이터 집합이 포함된 원형 차트를 보려면 범주를 클릭합니다.
3. 원형 차트에는 선택한 데이터가 표시됩니다. 원 세그먼트 중 하나를 클릭하면 해당 원 세그먼트를 기준으로 필터링된 데이터를 포함한 새 탭이 열립니다.

홈 페이지 대시보드에서 원도표의 섹션을 클릭하여 새 브라우저 창에서 차트를 엽니다. 새 창에는 클릭한 원도표의 섹션을 기준으로 필터링된 데이터가 표시됩니다.

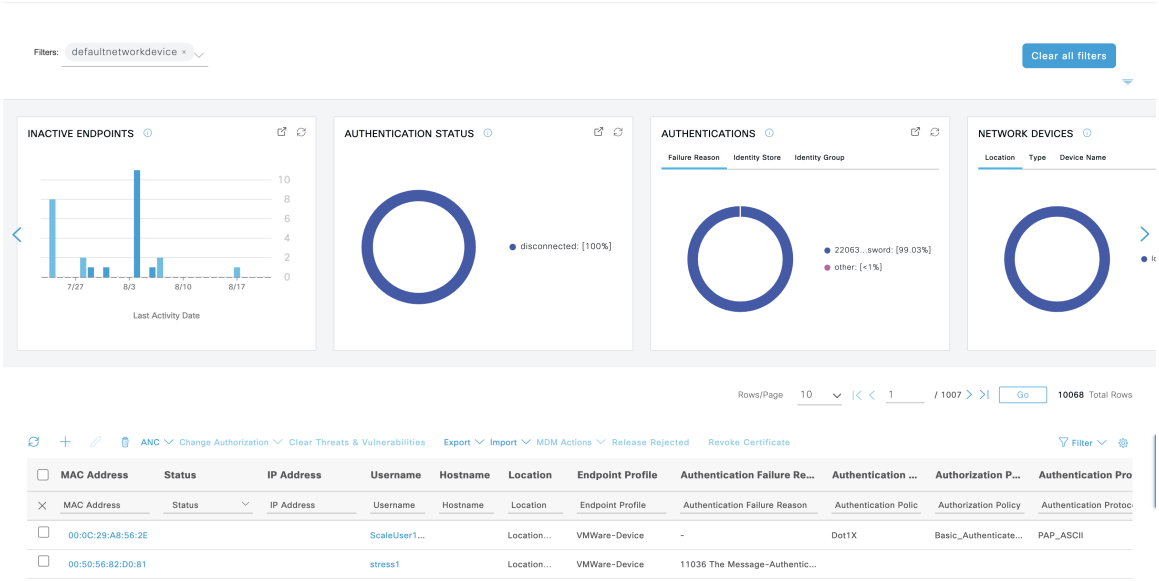
Context Visibility(상황 가시성) 창에서 원도표의 섹션을 클릭하면 표시되는 데이터는 필터링되지만 상황은 변경되지 않습니다. 필터링된 데이터를 동일한 브라우저 창에서 볼 수 있습니다.

보기에서 표시되는 데이터 필터링

Context Visibility(상황 가시성) 창에서 dashlet을 클릭하면 클릭하여 표시하는 항목을 기준으로 해당 데이터가 필터링됩니다. 예를 들어, 원도표의 섹션을 클릭하면 선택한 섹션의 데이터가 필터링되어 표시됩니다.



Network Devices(네트워크 디바이스**)**dashlet에서 **defau...evice**를 클릭하는 경우 다음 이미지와 같이 새 창이 데이터와 함께 나타납니다.



원도표의 추가 섹션을 클릭하여 데이터를 추가로 필터링합니다. **Filter(**필터**)** 드롭다운 목록 또는 데이터 목록의 오른쪽 상단 모서리에 있는 기어 아이콘을 사용하여 표시되는 데이터를 관리할 수도 있습니다.

맞춤형 필터를 저장합니다.

사용자 맞춤화 필터 생성

나만 액세스할 수 있는 사용자별 맞춤형 필터를 생성하고 저장합니다. Cisco ISE에 로그인하는 다른 사용자는 사용자가 생성하는 맞춤형 필터를 볼 수 없습니다. 사용자 정의 필터는 Cisco ISE 데이터베이스에 저장되지 않습니다. Cisco ISE에 로그인하는 모든 컴퓨터 또는 브라우저에서 액세스할 수 있습니다.

단계 **1** **Filter(**필터**)**를 클릭하고 **Advanced Filter(**고급 필터**)** 드롭다운 목록을 선택합니다.

단계 **2** 필터 메뉴에서 필드, 연산자, 값 등의 검색 속성을 지정합니다.

단계 **3** 조건을 더 추가하려면 **+**를 클릭합니다.

단계 **4** **Go(**이동**)**를 클릭하여 지정한 속성과 일치하는 엔트리를 표시합니다.

단계 **5** 필터를 저장하려면 **Save(**저장**)**를 클릭합니다.

단계 **6** 이름을 입력하고 **Save(**저장**)**를 클릭합니다. 이제 필터가 **Filter(**필터**)** 드롭다운 목록에 표시됩니다.

고급 필터를 사용하여 조건별로 데이터 필터링

고급 필터를 사용하면 이름 = Mike, 사용자 그룹 = 직원과 같이 지정된 조건에 따라 정보를 필터링할 수 있습니다. 조건은 여러 개 지정할 수 있습니다.

단계 **1** **Filter(**필터**)**를 클릭하고 **Advanced Filter(**고급 필터**)** 드롭다운 목록을 선택합니다.
단계 **2** Filter(필터) 메뉴에서 필드, 연산자, 값 등의 검색 속성을 지정합니다.
단계 **3** 조건을 더 추가하려면 +를 클릭합니다.
단계 **4** **Go(**이동**)**를 클릭하여 지정한 속성과 일치하는 엔트리를 표시합니다.

빠른 필터를 사용하여 필드 속성을 기준으로 데이터 필터링

빠른 필터를 사용하면 목록 페이지에 표시되는 필드 속성에 대해 값을 입력하고, 페이지를 새로 고치고, 필터 기준과 일치하는 기록만 나열할 수 있습니다.

단계 **1** **Filter(**필터**)**를 클릭하고 드롭다운 목록에서 **Quick Filter(**빠른 필터**)**를 선택합니다.
단계 **2** 속성 필드 중 하나 이상에 검색 기준을 입력하면 지정한 속성과 일치하는 엔트리가 자동으로 표시됩니다.

Dashlet 보기의 엔드포인트 작업

목록 상단의 툴바를 사용하면 선택한 목록의 엔드포인트에 대한 작업을 수행할 수 있습니다. 모든 목록에 대해 모든 작업이 활성화되는 것은 아닙니다. 일부 작업은 사용하도록 설정된 기능에 따라 달라집니다. 다음 목록에는 Cisco ISE에서 사용하기 전에 활성화해야 하는 두 가지 엔드포인트 작업이 나와 있습니다.

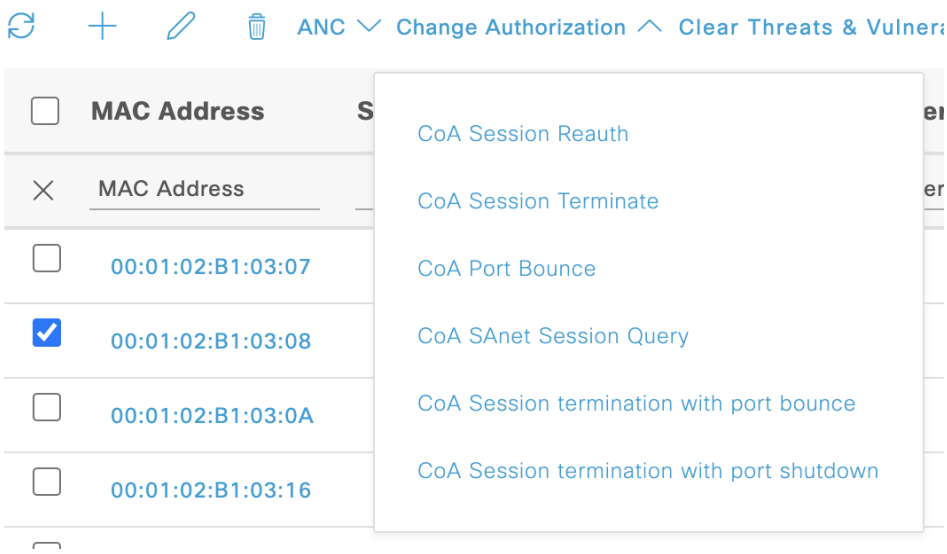
- **Adaptive Network Control Actions(**적응형 네트워크 제어 작업**)**

  적응형 네트워크 제어가 활성화된 경우 목록에서 엔드포인트를 선택하고 네트워크 액세스를 할당하거나 취소할 수 있습니다. CoA(Change of Authorization)를 실행할 수도 있습니다.

  Adaptive Network Service(적응형 네트워크 서비스**)** 창에서 Cisco ISE의 적응형 네트워크 서비스 또는 엔드포인트 보호 서비스를 활성화합니다. Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고**Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Endpoint Protection Service(**엔드포인트 보호 서비스**)** > **Adaptive Network Control(**적응형 네트워크 제어**)**를 선택합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 유지 관리 및 모니터링의 Cisco ISE에서 적응형 네트워크 제어 활성화 섹션을 참고하십시오 참고.

  홈 페이지 dashlet에서 원도표를 클릭하면 표시되는 새 창에 **ANC** 및 **Change Authorization(**인증 변경**)** 옵션이 포함됩니다. 작업을 수행할 엔드포인트의 확인란을 선택하고 **ANC** 및 **Change Authorization(**인증 변경**)** 드롭다운 목록에서 필요한 작업을 선택합니다.

그림 *6: Dashlet* 보기의 엔드포인트 작업



- **MDM** 작업

  MDM 서버를 Cisco ISE에 연결하는 경우 선택한 엔드포인트에서 MDM 작업을 수행할 수 있습니다. **MDM Actions(MDM** 작업**)** 드롭다운 목록에서 필요한 작업을 선택합니다.

Cisco ISE 대시보드

Cisco ISE 대시보드 또는 홈 페이지(**Menu(**메뉴**)** 아이콘(☰)을 클릭하고 대시보드를 선택)는 Cisco ISE 관리 포털에 로그인한 후에 표시되는 랜딩 페이지입니다. 대시보드는 창 위쪽에 메트릭 측정기가 표시되고 아래에는 dashlet이 구성된 중앙 집중식 관리 콘솔입니다. 기본 대시보드는 **Summary(**요약**)**, **Endpoints(**엔드포인트**)**, **Guests(**게스트**)**, **Vulnerability(**취약점**)** 및 **Threat(**위협**)**입니다. Cisco ISE 홈 대시보드, 102 페이지를 참조하십시오.

참고 Cisco ISE 기본 PAN 포털에서만 이 대시보드 데이터를 볼 수 있습니다.

대시보드의 실시간 데이터는 네트워크에 액세스하는 디바이스 및 사용자의 상태와 함께 시스템 상태 개요를 한눈에 볼 수 있도록 제공합니다.

대시보드 설정에 대한 드롭다운 목록을 보려면 두 번째 레벨 메뉴 모음에서 기어 아이콘을 클릭합니다. 다음 표에는 드롭다운 목록에서 사용 가능한 대시보드 설정 옵션에 대한 설명이 포함되어 있습니다.

드롭다운 목록 옵션	설명
Add New Dashboard(새 대시보드 추가**)**	기본 대시보드 5개를 포함하여 최대 20개의 대시보드를 구성할 수 있습니다.

드롭다운 목록 옵션	설명
Rename Dashboard(대시보드 이름 바꾸기**)**	(이 옵션은 사용자 지정 대시보드에만 사용 가능) 대시보드 이름을 바꾸려면 다음을 수행합니다. **1.** **Rename Dashboard(**대시보드 이름 바꾸기**)**를 클릭합니다. **2.** 새 이름을 지정합니다. **3.** **Apply(**적용**)**를 클릭합니다.
Add Dashlet(Dashlet 추가**)**	홈페이지 대시보드에 dashlet을 추가하려면 다음 단계를 수행합니다. **1.** **Add Dashlet(s)(dashlet** 추가**)**를 클릭합니다. **2.** **Add Dashlets(dashlet** 추가**)** 창에서 추가할 dashlet 옆에 있는 **Add(**추가**)**를 클릭합니다. **3.** **Save(**저장**)**를 클릭합니다. 참고 대시보드당 최대 9개의 dashlet을 추가할 수 있습니다.

드롭다운 목록 옵션	설명
Export(내보내기**)**	대시보드 데이터를 PDF 또는 CSV 파일로 내보낼 수 있습니다. 1. **Export(**내보내기**)**를 클릭합니다. 2. **Export(**내보내기**)** 대화 상자에서 다음 파일 형식 중 하나의 옆에 있는 라디오 버튼을 선택합니다. • **PDF**: 선택한 dashlet의 스냅샷을 볼 수 있는 PDF 형식을 선택합니다. • **CSV**: 선택한 대시보드 데이터를 zip 파일로 다운로드할 수 있는 CSV 형식을 선택합니다. 3. **Export(**내보내기**)** 대화 상자에서 내보낼 dashlet 옆에 있는 확인란을 선택합니다. 4. **Export(**내보내기**)**를 클릭합니다. zip 파일에는 선택한 대시보드의 개별 dashlet CSV 파일이 포함됩니다. dashlet의 각 탭과 관련된 데이터는 해당 dashlet CSV 파일에서 별도의 섹션으로 표시됩니다. 맞춤형 대시보드를 내보내면 zip 파일이 같은 이름으로 내보내집니다. 예를 들어 이름이 MyDashboard인 맞춤형 대시보드를 내보내는 경우 내보낸 파일 이름은 MyDashboard.zip입니다.
Layout Template(레이아웃 템플릿**)**	dashlet이 표시되는 템플릿의 레이아웃을 변경할 수 있습니다. 레이아웃을 변경하려면 다음을 수행합니다. 1. **Layout Template(**레이아웃 템플릿**)**을 클릭합니다. 2. 사용 가능한 옵션에서 원하는 레이아웃을 선택합니다.

드롭다운 목록 옵션	설명
Manage Dashboards(대시보드 관리**)**	**Manage Dashboards(**대시보드 관리**)**를 클릭하고 다음 옵션 중 하나를 선택합니다. • **Mark as Default Dashboard(**기본 대시보드로 지정**)**: 대시보드를 기본 대시보드(홈페이지)로 설정하려면 이 옵션을 사용합니다. • **Reset all Dashboards(**모든 대시보드 재설정**)**: 모든 대시보드를 원래 설정으로 재설정하려면 이 옵션을 사용합니다.

해당하는 맞춤형 대시보드 옆의 닫기(**x**) 아이콘을 클릭하여 생성한 대시보드를 삭제할 수 있습니다.

참고 기본 대시보드는 이름을 바꾸거나 삭제할 수 없습니다.

각 dashlet의 오른쪽 상단에는 다음 작업을 수행할 수 있는 도구 모음이 있습니다.

- Detach(분리): dashlet을 별도의 창에서 확인합니다.
- Refresh(새로 고침): dashlet을 새로 고칩니다.
- Remove(제거): 대시보드에서 dashlet을 제거합니다.

dashlet의 왼쪽 상단 모서리에 있는 위치 조정 아이콘을 사용하여 dashlet을 끌어다 놓을 수 있습니다.

알람 dashlet에는 **Severity(**심각도**)** 열에 대한 빠른 필터가 포함되어 있습니다. **Severity(**심각도**)** 드롭다운 목록에서 **Critical(**위험**)**, **Warning(**경고**)** 또는 **Info(**정보**)**를 선택하여 심각도별로 알람을 필터링할 수 있습니다.

Cisco ISE 국제화 및 현지화

Cisco ISE 국제화를 통해 지원되는 언어에 맞게 사용자 인터페이스가 변경됩니다. 사용자 인터페이스의 현지화는 위치별 구성 요소와 번역된 텍스트를 통합합니다. Windows, MAC OSX 및 Android 디바이스에서는 기본 신청자 프로비저닝 마법사를 지원되는 다음 언어로 사용할 수 있습니다.

Cisco ISE의 국제화 및 현지화 지원에서는 최종 사용자가 접하는 포털 및 관리 포털의 선택적 필드에 대해 영어가 아닌 텍스트를 UTF-8 인코딩으로 지원하는 데 초점을 맞춥니다.

지원되는 언어

Cisco ISE는 다음 언어 및 브라우저 로캘에 대한 국제화와 현지화를 지원합니다.

표 ***14:*** 지원되는 언어 및 로캘

언어	브라우저 로캘
중국어(번체)	zh-tw
중국어(간체)	zh-cn
체코어	cs-cz
네덜란드어	nl-nl
영어	en
프랑스어	fr-fr
독일어	de-de
헝가리어	hu-hu
이탈리아어	it-it
일본어	ja-jp
한국어	ko-kr
폴란드어	pl-pl
포르투갈어(브라질)	pt-br
러시아어	ru-ru
스페인어	es-es

최종 사용자 웹 포털 현지화

게스트, 스폰서, 내 디바이스 및 클라이언트 프로비저닝 포털은 지원되는 모든 언어 및 로캘로 현지화됩니다. 현지화되는 항목에는 텍스트, 레이블, 메시지, 필드 이름 및 버튼 레이블이 포함됩니다. 클라이언트 브라우저가 Cisco ISE의 템플릿으로 매핑되지 않는 로캘을 요청하는 경우 포털에서는 영어 템플릿을 사용하여 콘텐츠를 표시합니다.

관리 포털을 사용하여 각 언어에 대해 게스트, 스폰서 및 내 디바이스 포털에 사용되는 필드를 수정할 수 있습니다. 다른 언어를 추가할 수도 있습니다. 현재 클라이언트 프로비저닝 포털의 경우에는 이러한 필드를 사용자 맞춤화할 수 없습니다.

Cisco ISE에 HTML 페이지를 업로드하여 게스트 포털을 추가로 사용자 맞춤화할 수 있습니다. 사용자 맞춤화된 페이지를 업로드할 때는 구축에 대해 적절한 현지화를 지원해야 합니다. Cisco ISE는 지침으로 사용 가능한 샘플 HTML 페이지가 포함된 현지화 지원 예제를 제공합니다. Cisco ISE는 사용자 맞춤화 다국어 HTML 페이지를 업로드, 저장 및 렌더링하는 기능도 제공합니다.

참고 NAC 및 MAC Agent 설치 프로그램과 WebAgent 페이지는 현지화되지 않습니다.

UTF-8 문자 데이터 입력 지원

Cisco 클라이언트 에이전트나 supplicant 또는 스폰서/게스트/내 디바이스/클라이언트 프로비저닝 포털을 통해 최종 사용자에게 표시되는 Cisco ISE 필드는 모든 언어에 대해 UTF-8 문자 집합을 지원합니다. UTF-8은 히브리어, 산스크리트어, 아랍어 등의 여러 언어 문자 집합을 포함하는 유니코드 문자 집합용 멀티바이트 문자 인코딩입니다.

문자 값은 관리 컨피그레이션 데이터베이스에 UTF-8로 저장되며 UTF-8 문자는 보고서 및 사용자 인터페이스 구성 요소에 올바르게 표시됩니다.

UTF-8 인증서 인증

네트워크 액세스 인증에서는 UTF-8 사용자 이름 및 비밀번호 자격 증명을 지원합니다. 여기에는 게스트 및 관리 포털 로그인 인증에서 사용되는 RADIUS, EAP(Extensible Authentication Protocol), RADIUS 프록시, RADIUS 토큰 및 웹 인증이 포함됩니다. 사용자 이름 및 비밀번호에 대한 UTF-8 지원은 로컬 ID 저장소에 대한 인증 및 외부 ID 저장소에 대한 인증에 모두 적용됩니다.

UTF-8 인증은 네트워크 로그인에 사용되는 클라이언트 신청자에 따라 달라집니다. 일부 Windows 기본 신청자는 UTF-8 자격 증명을 지원하지 않습니다.

참고 RSA는 UTF-8 사용자를 지원하지 않으므로 RSA를 사용하는 UTF-8 인증은 지원되지 않습니다. 또한 Cisco ISE와 호환되는 RSA 서버도 UTF-8을 지원하지 않습니다.

UTF-8 정책 및 Posture Assessment

속성 값에서 조건이 지정된 Cisco ISE의 정책 규칙은 UTF-8 텍스트를 포함할 수 있습니다. 규칙 평가에서는 UTF-8 속성 값이 지원됩니다. 또한 관리 포털을 통해 UTF-8 값으로 조건을 구성할 수 있습니다.

포스처 요건은 UTF-8 문자배열을 기준으로 파일, 애플리케이션 및 서비스 조건으로 수정할 수 있습니다.

신청자에게 전송되는 메시지에 대한 UTF-8 지원

RSA 프롬프트와 메시지는 RADIUS 속성 REPLY-MESSAGE를 사용하거나 EAP 데이터 내에 포함되어 신청자에게 전달됩니다. UTF-8 데이터를 포함하는 텍스트는 클라이언트의 로컬 운영체제 언어 지원을 기반으로 하여 신청자에게 표시됩니다. 일부 Windows 기본 신청자는 UTF-8 자격 증명을 지원하지 않습니다.

Cisco ISE 프롬프트 및 메시지는 supplicant를 실행 중인 클라이언트 운영체제의 로캘과 동기화되지 않을 수 있습니다. 그러므로 Cisco ISE에서 지원하는 언어에 맞게 최종 사용자 신청자 로캘을 조정해야 합니다.

보고서 및 경보 **UTF-8** 지원

모니터링 및 문제 해결 보고서와 경보는 Cisco ISE에서 지원하는 언어에 대해 관련 속성의 UTF-8 값을 지원합니다. 다음 활동이 지원됩니다.

- 라이브 인증 보기.
- 보고서 기록의 세부 페이지 보기.
- 보고서 내보내기 및 저장.
- Cisco ISE 대시보드 보기.
- 경보 정보 보기.
- tcpdump 데이터 보기.

포털의 **UTF-8** 문자 지원

Cisco ISE 필드에서는 포털 및 최종 사용자 메시지 현지화에 대해 현재 지원되는 것보다 훨씬 더 많은 문자 집합(UTF-8)이 지원됩니다. 예를 들어 Cisco ISE에서는 히브리어, 아랍어 등 오른쪽에서 왼쪽 방향의 언어를 지원하지 않습니다(해당 문자 집합 자체는 지원됨).

다음 표에는 데이터 입력 및 보기에 대해 UTF-8 문자를 지원하는 관리 및 최종 사용자 포털의 필드와 관련 제한 사항이 나와 있습니다.

- Cisco ISE는 UTF-8 문자를 포함하는 게스트 사용자 이름 및 비밀번호를 지원하지 않습니다.
- Cisco ISE는 인증서의 UTF-8 문자를 지원하지 않습니다.

표 ***15:*** 관리 포털 ***UTF-8*** 문자 필드

관리 포털 요소	**UTF-8** 필드
네트워크 액세스 사용자 컨피그레이션	• **Username(**사용자 이름**)** 사용자 이름에는 대문자, 소문자, 숫자, 공백 및 특수 문자를 포함할 수 있습니다(`, %, ^, ;, :, [, {, |, },], \, ‘, “, =, <, >, ?, !, 그리고 제어문자는 제외) 공백만 포함된 사용자 이름은 제출할 수 없습니다. • 이름 • 성 • 이메일
사용자 목록	• 모든 필터 필드 • User List(사용자 목록) 창에 값이 표시됩니다. • 왼쪽 탐색 간단히 보기에 표시되는 값

관리 포털 요소	**UTF-8** 필드
사용자 비밀번호 정책	비밀번호는 대문자, 소문자, 숫자, 특수 문자를 포함할 수 있습니다(!, @, #, $, ^, &, *, (, and 포함). 비밀번호 필드는 UTF-8 문자를 포함한 모든 문자를 허용하지만 제어문자는 허용하지 않습니다. 일부 언어의 경우 대문자 또는 소문자 알파벳이 없습니다. 사용자 비밀번호 정책상 사용자가 대문자 또는 소문자로 비밀번호를 입력해야 하는데 사용자 언어가 이러한 문자를 지원하지 않는 경우 사용자는 비밀번호를 설정할 수 없습니다. 사용자 비밀번호 필드에서 UTF-8 문자를 지원하도록 하려면 사용자 비밀번호 정책 페이지(**Menu(**메뉴**)** 아이콘을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **User Authentication Settings(**사용자 인증 설정**)** > **Password Policy(**비밀번호 정책**)**선택)에서 다음 확인란을 선택 취소해야 합니다. • 소문자 알파벳 문자 • 대문자 알파벳 문자 사전상의 단어, 그 문자를 역순으로 배열한 단어 또는 그 문자를 다른 문자로 대체한 단어는 사용할 수 없습니다.
관리자 목록	• 모든 필터 필드 • 관리자 목록 창에 표시되는 값. • 왼쪽 탐색 간단히 보기에 표시되는 값
관리자 로그인 페이지	• **Username(**사용자 이름**)**
RSA	• Messages(메시지) • Prompts(프롬프트)
RADIUS 토큰	• Authentication(인증) 탭 > Prompt(프롬프트)
포스처 요건	• Name(이름) • Remediation action(교정 작업) > Message shown to Agent User(에이전트 사용자에게 표시되는 메시지) • Requirement(요건) 목록 표시

관리 포털 요소	**UTF-8** 필드
포스처 조건	**Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Posture(**포스처**)** 창의 다음 필드: • **File Condition(**파일 조건**)** > **Add(**추가**)** > **File Path(**파일 경로**)**. • **Application Condition(**애플리케이션 조건**)** > **Add(**추가**)** > **Process Name(**프로세스 이름**)**. • **Service Condition(**서비스 조건**)** > **Add(**추가**)** > **Service Name(**서비스 이름**)**. • Conditions(조건) 목록 표시
게스트 및 내 디바이스 설정	• Sponsor(스폰서) > Language Template(언어 템플릿): 지원되는 모든 언어/모든 필드 • Guest(게스트) > Language Template(언어 템플릿): 지원되는 모든 언어/모든 필드 • My Devices(내 디바이스) >Language Template(언어 템플릿): 지원되는 모든 언어/모든 필드
시스템 설정	• SMTP Server(SMTP 서버) > Default e-mail address(기본 이메일 주소)
Operations(작업) > Alarms(경보) > Rule(규칙)	• Criteria(기준) > User(사용자) • Notification(알림) > e-mail Notification(이메일 알림) 사용자 목록
Operations(작업) > Reports(보고서)	• Operations(작업) > Live Authentications(라이브 인증) > Filter(필터) 필드 • Operations(작업) > Reports(보고서) > Catalog(카탈로그) > Report(보고서) 필터 필드
Operations(작업) > Troubleshoot(문제 해결)	• General Tools(일반 도구) > RADIUS Authentication Troubleshooting(RADIUS 인증 문제 해결) > Username(사용자 이름)

관리 포털 요소	UTF-8 필드
정책	• Authentication(인증) > 정책 조건 내의 안티바이러스식의 값 • Authorization or posture or client provisioning(권한 부여, 포스처, 또는 클라이언트 프로비저닝) > other conditions(기타 조건) > 정책 조건 내의 안티바이러스식의 값
정책 라이브러리 조건의 속성 값	• Authentication(인증) > simple condition or compound condition(단순 조건 또는 복합 조건) > 안티바이러스식의 값 • Authentication(인증) > simple condition(단순 조건) 목록 표시 • Authentication(인증) > simple condition(단순 조건) 목록 > left navigation quick view(왼쪽 탐색 간단히 보기) 표시 • Authorization(권한 부여) > simple condition or compound condition(단순 조건 또는 복합 조건) > 안티바이러스식의 값 • Authorization(권한 부여) > simple condition(단순 조건) 목록 > left navigation quick view(왼쪽 탐색 간단히 보기) 표시 • Posture(포스처) > Dictionary simple condition or Dictionary compound condition(사전 단순 조건 또는 사전 복합 조건) > 안티바이러스식의 값 • Guest(게스트) > simple condition or compound condition(단순 조건 또는 복합 조건) > 안티바이러스식의 값

Cisco ISE 사용자 인터페이스 외부에서 UTF-8 지원

이 섹션에서는 UTF-8을 지원하는 Cisco ISE 사용자 인터페이스 외부의 영역에 대해 설명합니다.

디버그 로그 및 CLI 관련 UTF-8 지원

일부 디버그 로그에서는 속성 값 및 포스처 조건 세부정보가 표시됩니다. 모든 디버그 로그는 UTF-8 값을 허용합니다. 원시 UTF-8 데이터가 포함된 디버그 로그를 다운로드할 수 있으며, UTF-8을 지원하는 뷰어에서 이 로그를 볼 수 있습니다.

Cisco Secure ACS 마이그레이션 UTF-8 지원

Cisco ISE에서는 Cisco Secure ACS(Access Control Server) UTF-8 구성 개체와 값을 마이그레이션할 수 있습니다. 일부 UTF-8 개체의 마이그레이션은 Cisco ISE UTF-8 언어에서 지원되지 않을 수도 있으므로 관리 포털 또는 보고서를 사용하는 방법으로는 마이그레이션 중에 제공되는 일부 UTF-8 데이터를 읽지 못할 수 있습니다. Cisco Secure ACS에서 마이그레이션되는 읽을 수 없는 UTF-8 값을 ASCII 텍스트로 변환합니다. Cisco Secure ACS에서 Cisco ISE 로의 마이그레이션에 대한 자세한 내용은 사용 중인 Cisco ISE 버전의 Cisco Secure ACS to Cisco ISE Migration Tool을 참고하십시오.

UTF-8 값 가져오기 및 내보내기 지원

관리 및 스폰서 포털에서는 사용자 계정 세부정보를 가져올 때 UTF-8 값을 포함하는 .csv 파일과 일반 텍스트를 사용할 수 있습니다. 내보낸 파일은 csv 파일로 제공됩니다.

REST에 대한 UTF-8 지원

외부 REST(Representational State Transfer) 통신은 UTF-8 값을 지원합니다. 이 지원은 Cisco ISE 사용자 인터페이스에서 UTF-8이 지원되는 구성 가능한 항목(관리자 인증은 제외)에 적용됩니다. REST의 관리자 인증에서는 로그인에 ASCII 텍스트 자격 증명을 사용해야 합니다.

ID 저장소 권한 부여 데이터에 대한 UTF-8 지원

Cisco ISE에서는 Active Directory 및 LDAP(Active Directory 및 LDAP)가 정책 처리를 위해 권한 부여 정책에 UTF-8 데이터를 사용할 수 있도록 허용합니다.

MAC 주소 정규화

Cisco ISE는 다음 형식으로 입력되는 MAC 주소의 정규화를 지원합니다.

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

다음 Cisco ISE 창에서는 전체 또는 부분 MAC 주소를 제공합니다.

- **Policy(**정책**)** > **Policy Sets(**정책 집합**)**
- **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > Authorization(권한 부여)
- Authentications(인증) > Filters(필터)(엔드포인트 및 ID 열)
- 글로벌 검색
- **Operations(**작업**)** > **Reports(**보고서**)** > Reports Filters(보고서 필터)

- **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Endpoint Debug(**엔드포인트 디버그**)**.

다음 Cisco ISE 창에서 전체 MAC 주소(':' 또는 '-' 또는 '.'로 구분된 6개 옥텟)를 제공합니다.

- Operations(작업) > Endpoint Protection Services(엔드포인트 보호 서비스) Adaptive Network Control(적응형 네트워크 제어)
- **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **RADIUS Authentication Troubleshooting(RADIUS** 인증 문제 해결**)**
- **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Posture Troubleshooting(**포스처 문제 해결**)**
- Administration(관리) > Identities(ID) > Endpoints(엔드포인트)
- **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**
- **Administration(**관리**)** > **Logging(**로깅**)** > **Collection Filter(**수집 필터**)**

REST API는 전체 MAC 주소의 정규화도 지원합니다.

옥텟의 유효 범위는 0~9, a~f 또는 A~F입니다.

Cisco ISE 구축 업그레이드

Cisco ISE는 관리 포털에서 GUI 기반 중앙 집중식 업그레이드를 제공합니다. 업그레이드 진행률 및 노드의 상태가 Cisco ISE GUI에 표시됩니다. 사전 및 사후 업그레이드 작업에 대한 자세한 내용은 업그레이드하려는 Cisco ISE 릴리스에 대한 *Cisco Identity Services Engine* 업그레이드 가이드를 참고하십시오.

업그레이드 **Overview(**개요**)** 창(**Administration(**관리**)** > **System(**시스템**)** > **Upgrade(**업그레이드**)** > **Overview(**개요**)**) 구축의 모든 노드, 해당 노드에서 활성화된 페르소나, 현재 사용 중인 Cisco ISE 버전 및 각 노드의 상태(노드가 활성 상태인지 비활성 상태인지를 나타냄)가 나열됩니다. 노드가 **Active(**활성**)** 상태여야 업그레이드를 시작할 수 있습니다.

관리자 액세스 콘솔

다음 단계에서는 관리 포털에 로그인하는 방법을 설명합니다.

단계 **1** 브라우저의 주소 표시줄에서 Cisco ISE URL을 입력합니다(예: https://<ise 호스트 이름 또는 IP 주소>/admin/).

단계 **2** 초기 Cisco ISE 설정 시 지정 및 구성한 대/소문자를 구분하는 비밀번호와 사용자 이름을 입력합니다.

단계 **3** **Login(**로그인**)**을 클릭하거나 **Enter**를 누릅니다.

로그인이 실패하면 로그인 페이지에서 **Problem logging in?(**로그인하는 데 문제가 있나요**?)** 링크를 클릭하여 지침을 따릅니다.

관리자 로그인 브라우저 지원

Cisco ISE 관리 포털은 다음의 HTTPS 사용 가능 브라우저를 지원합니다.

- Mozilla Firefox 79 이하 버전
- Mozilla Firefox ESR 60.9 이하 버전
- Google Chrome 84 이하 버전

ISE 커뮤니티 리소스

Adblock Plus 사용 시 ISE 페이지가 완전히 로드되지 않는 경우

실패한 로그인 시도 이후에 관리자 잠금

관리 사용자 ID의 비밀번호를 여러 번 잘못 입력하면 지정된 시간 동안 구성에 따라 계정이 일시 중단되거나 잠기게 됩니다. Cisco ISE가 사용자를 잠그도록 구성한 경우 관리 포털이 시스템에서 사용자를 잠급니다. Cisco ISE는 서버 관리자 로그인 보고서에 로그 항목을 추가하고 해당 관리자 ID의 자격 증명을 일시 중단합니다. Cisco Identity Services Engine 설치 가이드의 "관리자 잠금에 따라 비활성화된 비밀번호 재설정" 섹션에 설명된 대로 해당 관리자 ID의 비밀번호를 재설정합니다. 관리자 계정을 비활성화하기 전에 허용되는 로그인 시도 실패 횟수는 *Cisco Identity Services Engine* 관리자 가이드의 "Cisco ISE에 대한 관리 액세스" 섹션에 설명된 대로 구성됩니다. 관리 사용자 계정이 잠기면 Cisco ISE는 해당 정보가 구성된 경우 연결된 사용자에게 이메일을 보냅니다.

슈퍼 관리자 역할(Microsoft Active Directory 사용자 포함)의 관리자만 관리자 액세스 비활성화 옵션을 구성할 수 있습니다.

Cisco ISE의 프록시 설정 구성

기존 네트워크 토폴로지에서 프록시 서버를 사용해 Cisco ISE를 활성화하는 경우 클라이언트 프로비저닝 및 포스처 관련 리소스를 찾을 수 있는 원격 다운로드 사이트와 같은 외부 리소스에 액세스하려면 관리 포털을 사용하여 프록시 설정을 구성할 수 있습니다.

프록시 설정은 다음 Cisco ISE 기능에 영향을 줍니다.

- 파트너 모바일 관리
- 엔드포인트 프로파일러 피드 서비스 업데이트
- 엔드포인트 포스처 업데이트
- 엔드포인트 포스처 에이전트 리소스 다운로드

- CRL(인증서 해지 목록) 다운로드
- 게스트 알림
- SMS 메시지 전송
- 소셜 로그인

Cisco ISE 프록시 컨피그레이션은 프록시 서버에 대한 기본 인증을 지원합니다. NTLM(NT LAN Manager) 인증은 지원되지 않습니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Proxy(**프록시**)**를 선택합니다.

단계 **2** 프록시 IP 주소 또는 DNS 확인 가능 호스트 이름을 입력하고, 프록시 트래픽이 Cisco ISE에서/Cisco ISE로 이동할 때 사용되는 포트를 **Proxy host server : port(**프록시 호스트 서버**:** 포트**)** 필드에 지정합니다.

단계 **3** 필요한 경우 **Password required(**비밀번호 필요**)** 확인란을 선택합니다.

단계 **4** 프록시 서버에 인증하는 데 사용되는 사용자 이름과 비밀번호를 **User Name(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 입력합니다. **Confirm Password(**비밀번호 확인**)** 필드에 비밀번호를 다시 입력합니다.

단계 **5** 바이패스해야 하는 호스트나 도메인의 IP 주소 또는 주소 범위를 **Bypass proxy for these hosts and domain(**다음 호스트 및 도메인에 대해 프록시 바이패스**)** 텍스트 상자에 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

관리 포털에서 사용하는 포트

관리 포털은 HTTP 포트 80 및 HTTPS 포트 443을 사용하며 이러한 설정은 변경할 수 없습니다. 최종 사용자 포털은 어느 것도 직접 구성할 수 없으며 이는 관리 포털에 대한 위험을 줄이기 위함입니다.

Cisco ISE 애플리케이션 프로그래밍 인터페이스 게이트웨이 설정

Cisco ISE API 게이트웨이는 여러 Cisco ISE 서비스 API에 대한 단일 엔트리 포인트 역할을 하여 더 우수한 보안 및 트래픽 관리를 제공하는 API 관리 솔루션입니다. 외부 클라이언트의 API 요청은 Cisco ISE의 API 게이트웨이로 라우팅됩니다. 요청은 내부 알고리즘을 기반으로 서비스 API가 실행 중인 Cisco ISE 노드로 전달됩니다.

Cisco ISE 릴리스 3.0에서는 MnT(모니터링) API만 API 게이트웨이를 통해 라우팅됩니다.

API 게이트웨이를 활성화하려는 Cisco ISE 노드를 선택할 수 있습니다. Cisco ISE 구축의 2개 이상의 노드에서 API 게이트웨이를 실행하는 것이 좋습니다.

단계 **1** 기본 PAN에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **API Gateway Settings(API** 게이트웨이 설정**)**.

단계 **3** **ISE API Gateway Nodes List(ISE API** 게이트웨이 노드 목록**)** 영역에서 API 게이트웨이를 활성화할 노드 옆의 확인란을 선택합니다.

단계 **4** **Enable(**활성화**)**을 클릭합니다.

문제 해결

API 게이트웨이와 관련된 문제를 해결하려면 **Debug Log Configuration(**디버그 로그 컨피그레이션**)** 창에서 다음 구성 요소의 **Log Level(**로그 레벨**)**을 **DEBUG**로 설정합니다. (이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Debug Wizard(**디버그 마법사**)** > **Debug Log Configuration(**디버그 로그 컨피그레이션**)**을 선택합니다.)

- **ise-kong**
- **kong**

로그는 **Download Logs(**로그 다운로드**)** 창에서 다운로드할 수 있습니다. (이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Dowload Logs(**로그 다운로드**)**.) **Support Bundle(**지원 번들**)** 탭에 있는 **Download(**다운로드**)** 버튼을 클릭하여 지원 번들을 다운로드하거나 **Debug Logs(**디버그 로그**)** 탭에서 **kong** 디버그 로그의 로그 파일 값을 클릭하여 kong 디버그 로그를 다운로드할 수 있습니다.

확인

언제든지 Cisco ISE 기본 PAN에 로그인할 수 있다면 API 게이트웨이 설정이 정상적으로 작동하는 것입니다.

참고 UI가 로그인된 동일한 웹 브라우저의 다른 탭에서 API 게이트웨이를 통해 REST API에 액세스하는 경우 UI가 로그아웃됩니다.

이는 API 게이트웨이 노드가 아닌 원격 노드에서 API를 제공하는 경우에만 발생합니다.

외부 **RESTful** 서비스 애플리케이션 프로그래밍 인터페이스 활성화

외부 RESTful 서비스 API는 HTTPS 프로토콜 및 REST 방법론을 기반으로 하며 포트 9060을 사용합니다.

외부 RESTful 서비스 API는 기본 인증을 지원합니다. 인증 자격 증명은 암호화되어 있으며 요청 헤더의 일부입니다.

JAVA, cURL linux 명령, Python 또는 기타 모든 클라이언트와 같은 모든 REST 클라이언트를 사용하여 외부 RESTful 서비스 API 호출을 수행할 수 있습니다.

참고 ERS API는 TLS 1.1 및 TLS 1.2를 지원합니다. ERS API는 **Security Settings(**보안 설정**)** 창 (**Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Security Settings(**보안 설정**)**)에서 TLS 1.0을 활성화하더라도 TLS 1.0을 지원하지 않습니다. **Security Settings(**보안 설정**)** 창에서 TLS 1.0을 활성화하면 EAP 프로토콜에만 관련이 있으며 ERS API에는 영향을 주지 않습니다.

사용자에게 외부 RESTful 서비스 API를 사용하여 작업을 수행하도록 특수 권한을 할당해야 합니다. Cisco ISE 릴리스 2.6 이상에서 외부 RESTful 서비스 사용자는 내부 사용자이거나 외부 Microsoft Active Directory 그룹에 속할 수 있습니다. 외부 사용자가 속한 Active Directory 그룹은 **ERS** 관리자 또는 **ERS** 운영자 그룹에 매핑되어야 합니다.

- **ERS** 관리자: 이 사용자는 외부 RESTful 서비스 API 요청을 생성, 읽기, 업데이트 및 삭제할 수 있습니다. 이들은 모든 외부 RESTful 서비스 API(GET, POST, DELETE, PUT) 전체에 액세스할 수 있습니다.
- **ERS** 운영자: 이 사용자에게는 읽기 전용 액세스 권한이 있습니다(GET 요청만 해당).

참고 슈퍼 관리자 역할의 사용자는 모든 외부 RESTful 서비스 API에 액세스할 수 있습니다.

ERS 세션 유휴 시간 초과은 60초입니다. 이 기간 동안 여러 요청이 전송되는 경우 동일한 CSRF(Cross-Site Request Forgery) 토큰과 함께 동일한 세션이 사용됩니다. 세션이 60초 이상 유휴 상태인 경우 세션이 재설정되고 새 CSRF 토큰이 사용됩니다.

외부 RESTful 서비스 API는 기본적으로 활성화되어 있지 않습니다. 활성화하지 않고 외부 RESTful 서비스 API 호출을 시도하는 경우 오류 응답이 표시됩니다. Cisco ISE REST API용으로 개발된 애플리케이션에서 Cisco ISE에 액세스할 수 있도록 Cisco ISE REST API를 활성화합니다. Cisco REST API는 기본적으로 HTTPS 포트 9060을 사용합니다. Cisco ISE REST API가 Cisco ISE 관리자 서버에서 활성화되지 않은 경우, 클라이언트 애플리케이션은 모든 게스트 REST API 요청에 대해 서버에서 시간 초과 오류를 수신합니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **ERS Settings(ERS** 설정**)**를 선택합니다.

단계 **2** Enable ERS for Read / Write (읽기 / 쓰기를 위해 ERS 활성화) 라디오 버튼을 클릭하여 PAN (Primary Administration Node)에서 외부 RESTful 서비스를 활성화합니다.

단계 **3** 구축에 보조 노드가 있는 경우 **Enable ERS for Read for All Other Nodes(**모든 기타 노드에서 읽기 위한 **ERS** 활성화**)** 라디오 버튼을 클릭합니다.

모든 유형의 외부 RESTful 서비스 요청은 기본 ISE 노드에만 유효합니다. 보조 노드에는 읽기-액세스 권한(GET 요청)이 있습니다.

단계 **4** **CSRF** 확인 영역에서 다음 중 하나의 옵션에 해당하는 라디오 버튼을 클릭합니다.

- **Use CSRF Check for Enhanced Security(**보안 강화를 위해 **CSRF** 확인 사용**)**: 이 옵션을 활성화하면 외부 RESTful 서비스 클라이언트는 GET 요청을 전송하여 Cisco ISE에서 CSRF 토큰을 가져오고 Cisco ISE로 전송되는 요청에 CSRF 토큰을 포함해야 합니다. Cisco ISE는 외부 RESTful 서비스 클라이언트에서 요청이 수신되면 CSRF 토큰을 검증합니다. Cisco ISE는 토큰이 유효한 경우에만 요청을 처리합니다. 이 옵션은 Cisco ISE 릴리스 2.3 이전의 외부 RESTful 서비스 클라이언트에는 적용되지 않습니다.
- **Disable CSRF for ERS Request(ERS** 요청에 대해 **CSRF** 비활성화**)**: 이 옵션을 활성화하면 CSRF 검증이 수행되지 않습니다. 이 옵션은 Cisco ISE 2.3 이전의 외부 RESTful 서비스 클라이언트에 사용할 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

모든 REST 작업이 감사되며 로그는 시스템 로그에 기록됩니다. 외부 RESTful 서비스 API에는 디버그 로깅 범주가 있으며 이는 Cisco ISE GUI의 디버그 로깅 창에서 활성화할 수 있습니다.

Cisco ISE에서 외부 RESTful 서비스를 비활성화하면 포트 9060은 열린 상태로 유지되지만 포트를 통한 통신은 허용되지 않습니다.

관련 항목

외부 RESTful 서비스 소프트웨어 개발 키트 , 132 페이지

외부 **RESTful** 서비스 애플리케이션 프로그래밍 인터페이스에 대한 외부 **AD** 액세스 활성화

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** 외부 사용자가 속한 Active Directory 그룹을 외부 ID 소스로 추가합니다.

*Cisco ISE Administrator Guide*의 "자산 가시성"장에서 "외부 ID 소스로서의 Active Directory"섹션을 참조하십시오.

단계 **3** Active Directory에서 사용자 그룹을 추가합니다.

*Cisco ISE Administrator Guide*의 "자산 가시성"장에서 "사용자 추가"섹션을 참조하십시오.

단계 **4** Cisco ISE GUI 메뉴에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭한 뒤 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)** > **Authentication Method(**인증 방법**)**.

단계 **5** **Identity Source(ID** 소스**)** 드롭 다운 목록에서 **AD:<Join Point Name> ID**을 선택합니다.

단계 **6** 해당 라디오 버튼을 클릭하여 **Password Based(**비밀번호 기반**)** 또는 **Client Certificate Based(**클라이언트 인증서 기반**)** 인증을 선택합니다.

단계 **7** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Groups(**관리자 그룹**)**를 선택합니다.

단계 **8** 관리 그룹 목록에서 **ERS Admin group(ERS** 관리자 그룹**)** 또는 **ERS Operator(ERS** 운영자**)**를 클릭합니다.

단계 **9** **Add (**추가**)**를 클릭하고 외부 사용자를 관리자 그룹에 구성원 사용자로 추가합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

Cisco ISE 관리자는 사용자에게 외부 RESTful 서비스 API를 사용하여 작업을 수행하도록 특수 권한을 할당해야 합니다. Cisco ISE 릴리스 2.6 이상에서 외부 RESTful 서비스 사용자는 내부 사용자이거나 외부 Active Directory에 속할 수 있습니다. 외부 사용자가 속한 Active Directory 그룹은 ERS 관리자 또는 ERS 운영자 그룹에 매핑되어야 합니다.

- **ERS** 관리자: 이 사용자는 외부 RESTful 서비스 API 요청을 생성, 읽기, 업데이트 및 삭제할 수 있습니다. 이들은 모든 외부 RESTful 서비스 API(GET, POST, DELETE, PUT) 전체에 액세스할 수 있습니다.
- **ERS** 운영자: 이 사용자에게는 읽기 전용 액세스 권한이 있습니다(GET 요청만 해당).

참고 슈퍼 관리자 역할의 사용자는 모든 외부 RESTful 서비스 API에 액세스할 수 있습니다.

외부 **RESTful** 서비스 소프트웨어 개발 키트

ERS(외부 RESTful 서비스) SDK(소프트웨어 개발 키트)를 사용하여 고유한 툴을 구축할 수 있습니다. https://<ISE-ADMIN-NODE>:9060/ers/sdk URL에서 외부 RESTful 서비스 SDK에 액세스할 수 있습니다. **ERS Admin(ERS** 관리자**)** 역할의 사용자만 외부 RESTful 서비스 SDK에 액세스 할 수 있습니다.

SDK는 다음 구성 요소로 구성됩니다.

- 빠른 참조 API 설명서.
- 사용 가능한 모든 API 작업의 전체 목록.
- 다운로드에 사용 가능한 스키마 파일.
- 다운로드에 사용 가능한 Java의 샘플 애플리케이션.
- cURL 스크립트 형식의 활용 사례.
- Python 스크립트 형식의 활용 사례.
- Chrome Postman 사용에 대한 지침.

시스템 시간 및 네트워크 시간 프로토콜 서버 설정 지정

Cisco ISE에서는 최대 3개의 NTP 서버를 구성할 수 있습니다. NTP 서버를 사용하면 정확한 시간을 유지하고 서로 다른 표준 시간대 간에 시간을 동기화할 수 있습니다. 또한 Cisco ISE가 인증된 NTP 서버만 사용해야 하는지 여부를 지정할 수 있으며 이를 위해 인증 키를 하나 이상 입력할 수 있습니다.

모든 Cisco ISE 노드는 UTC(협정 세계시) 표준 시간대로 설정하는 것이 좋습니다. 특히 Cisco ISE 노드가 분산형 구축에 설치되어 있는 경우에는 반드시 UTC 표준 시간대를 설정해야 합니다. 이 절차를 수행하면 구축 내 여러 노드의 보고서 및 로그의 타임스탬프가 항상 동기화됩니다.

Cisco ISE는 또한 NTP 서버에 대한 공개 키 인증을 지원합니다. NTPv 버전 4는 대칭 키 암호화를 사용하며, 공개 키 암호화를 기반으로 하는 새로운 Autokey 보안 모델도 제공합니다. 공개 키 암호화는 대칭 키 암호화보다 안전한 것으로 간주됩니다. 이 보안은 각 서버에서 생성되고 절대 공개되지 않는 개인 값을 기반으로 하기 때문입니다. Autokey 보안 모델을 사용하면 모든 키 배포 및 관리 기능에 공개 값만 포함되며, 따라서 키 배포 및 저장이 대폭 간소화됩니다.

Configuration Mode(구성 모드)에서 Cisco ISE CLI의 NTP 서버용 Autokey 보안 모델을 구성할 수 있습니다. 가장 많이 사용하는 IFF(Friend 또는 Foe 식별) 시스템을 이 시스템으로 사용하는 것이 좋습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리 관리자 역할이 할당되어 있어야 합니다.

기본 및 보조 Cisco ISE 노드가 둘 다 있는 경우에는 각 노드의 사용자 인터페이스에 로그인한 다음 시스템 시간과 NTP(네트워크 시간 프로토콜) 서버 설정을 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭한 다음 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **System Time(**시스템 시간**)** .

단계 **2** **NTP Server Configuration(NTP** 서버 컨피그레이션**)** 영역에서 NTP 서버의 고유한 IP 주소(IPv4 또는 IPv6 또는 FQDN(Fully Qualified Domain Name) 값)를 입력합니다.

단계 **3** (선택 사항) 개인 키를 이용하여 NTP 서버를 인증하고 싶다면 **NTP Authentication Keys(NTP** 인증 키**)** 탭을 클릭하고, 지정하는 서버에서 인증 키를 통한 인증을 수행해야 하는 경우 인증 키를 하나 이상 지정합니다. 다음 단계를 수행합니다.

a) **Add(**추가**)**를 클릭합니다.

b) **Key ID(**키 **ID)** 및 **Key Value(**키 값**)** 필드에 필요한 값을 입력합니다. **HMAC** 드롭다운 목록에서 필요한 HMAC(해시 메시지 인증 코드) 값을 선택합니다.**Key ID(**키 **ID)** 필드에는 1~65,535 사이의 숫자 값을 입력할 수 있으며 **Key Value(**키 값**)** 필드에는 영숫자 문자를 15자까지 입력할 수 있습니다.

c) **OK(**확인**)**를 클릭합니다.

d) **NTP Server Configuration(NTP** 서버 컨피그레이션**)** 탭으로 돌아갑니다.

단계 **4** (선택 사항) 공개 키 인증을 사용하여 NTP 서버를 인증하려는 경우 CLI에서 Cisco ISE에 대해 Autokey 보안 모델을 구성합니다. 해당되는 Cisco ISE 릴리스의 Cisco Identity Services Engine CLI 참조 가이드에서 **ntp server** 및 **crypto** 명령을 참조하십시오.

참고 Cisco ISE에서는 2개의 NTP 서버만 사용하지 않을 것을 권장합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

시스템 표준 시간대 변경

표준 시간대는 설정하고 나면 관리 포털에서 편집할 수 없습니다. 표준 시간대 설정을 변경하려면 Cisco ISE CLI에서 다음 명령을 입력하십시오.

clock timezone *timezone*

clock timezone 명령에 대한 자세한 내용은 Cisco Identity Services Engine CLI Reference Guide에서 확인하십시오.

참고 Cisco ISE는 표준 시간대 이름 및 출력 약어에서 POSIX(Portable Operating System Interface) 스타일 기호를 사용합니다. 따라서 그리니치 서부 시간대에는 양수 기호가 붙고 그리니치 동부 시간대에는 음수 기호가 붙습니다. 예를 들어 TZ='Etc/GMT+4'는 UT(Universal Time)보다 4시간 늦은 시간에 해당합니다.

주의 설치 후에 Cisco ISE 어플라이언스에서 표준 시간대를 변경하려면 특정 노드에서 ISE 서비스를 다시 시작해야 합니다. 따라서 유지 관리 기간 내에 이러한 변경을 수행하는 것이 좋습니다. 또한 단일 Cisco ISE 구축의 모든 노드는 같은 표준 시간대로 구성해야 합니다. 지리적 위치나 표준 시간대가 다른 Cisco ISE 노드가 있는 경우에는 모든 Cisco ISE 노드에서 UTC 등의 전 세계 표준 시간대를 사용해야 합니다.

알림을 지원하도록 SMTP 서버 구성

Cisco ISE가 다음 목적으로 이메일 알림을 보낼 수 있도록 SMTP 서버를 구성합니다.

- 경보
- 스폰서가 로그인 자격 증명 및 비밀번호 재설정 지침이 포함된 이메일 알림을 게스트에게 전송
- 게스트가 자신을 성공적으로 등록한 후 자동으로 로그인 자격 증명을 수신하고 게스트 계정이 만료되기 전에 필요한 작업 수행

경보 알림의 수신자는 **Include system alarms in emails(**이메일에 시스템 경보 포함**)** 옵션이 활성화된 모든 내부 관리 사용자가 될 수 있습니다. 경보 알림을 보내기 위한 보낸 사람의 이메일 주소는 ise@<호스트 이름>으로 하드 코드됩니다.

다음 표에는 분산 Cisco ISE 환경에서 이메일을 전송하는 노드가 나와 있습니다.

표 ***16:*** 이메일을 전송하는 ***Cisco ISE*** 노드

이메일의 목적	이메일을 전송하는 노드
게스트 액세스 만료	기본 PAN(Policy Administration Node)

이메일의 목적	이메일을 전송하는 노드
경보	활성 MnT(Monitoring and Troubleshooting) 노드
게스트 및 스폰서 포털의 스폰서 및 게스트 알림	PSN(Policy Service Node)
비밀번호 만료	기본 PAN

SMTP(Simple Mail Transfer Protocol) 서버를 구성하려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **SMTP Server(SMTP** 서버**)**. 다음 필드를 구성합니다.

- **SMTP Server Settings(SMTP** 서버 설정**)** 영역에서 다음을 수행합니다.
  - **SMTP server(SMTP** 서버**)**: 아웃바운드 SMTP 서버의 호스트 이름을 입력합니다.
  - **SMTP Port(SMTP** 포트**)**: SMTP 포트 번호를 입력합니다. SMTP 서버에 연결하려면 이 포트를 열어야 합니다.
  - **Connection Timeout(**연결 시간 초과**)**: Cisco ISE가 새 연결을 시작하기 전에 SMTP 서버에 대한 연결을 대기하는 최대 시간을 입력합니다. 시간 초과 값은 초 단위로 구성됩니다.
- 보안 SMTP 서버와 통신하도록 **Encryption Settings(**암호화 설정**)** 영역에서 **Use TLS/SSL Encryption(TLS/SSL** 암호화 사용**)** 확인란을 선택합니다. SSL(Secure Sockets Layer)을 사용하는 경우 SMTP 서버의 루트 인증서를 Cisco ISE의 신뢰할 수 있는 인증서에 추가합니다.
- SSL 대신 인증에 사용자 이름과 비밀번호를 사용하도록 **Authentication Settings(**인증 설정**)** 영역에서 **Use Password Authentication(**비밀번호 인증 사용**)** 확인란을 선택합니다.

대화형 도움말

사용자는 인터랙티브 도움말을 사용하여 작업을 쉽게 완료 할 수있는 팁과 단계별 지침을 제공하여 Cisco ISE를 효율적으로 사용할 수 있습니다.

이 기능은 기본적으로 활성화되어 있습니다. 이 기능을 비활성화하려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Interactive Help(**대화형 도움말**)**를 선택하고 **Enable Interactive Help(**대화형 도움말 활성화**)** 확인란의 선택을 취소합니다.

대화형 도움말 메뉴를 보려면 **Show(**표시**)** 버튼을 클릭합니다.

보안 잠금 해제 클라이언트 메커니즘 활성화

Secure Unlock Client 메커니즘은 특정 시간 동안 Cisco ISE CLI에서 루트 쉘(shell) 액세스를 제공합니다. 세션을 종료하거나 닫으면 루트 액세스도 취소됩니다.

Secure Unlock Client 기능은 Consent Token 툴을 사용하여 구현됩니다. Consent Token은 Cisco 제품에 대한 권한 있는 액세스를 신뢰할 수 있는 방식으로 안전하게 부여하기 위한 통합된 다단계 인증 스키마이며, 고객과 Cisco의 상호 동의가 있어야 합니다.

Cisco ISE CLI에서 루트 쉘(shell)을 활성화하려면 다음 단계를 수행합니다.

단계 **1** Cisco ISE CLI에서 **permit rootaccess**를 입력합니다.

```
ise/admin# permit rootaccess
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
```

단계 **2** 옵션 **1**을 선택하여 Consent Token 챌린지를 생성합니다.

```
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
1
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
********************************************************************************
GLCX7gAAQEBAAQAAAAPAgAFAAAAAAMACImJxgubOhitBAAQiUwv+XeD3pnJ4HLnJy3OXQIABAAADhAGAANUUUHAAZJUUVfQlQIAANUUUACcJIDU2NGQ3NjgwLTFmZmEtOWI0ZS0wZjY1LTdlZDllMGQlM2UzNQo=
********************************************************************************
Starting background timer of 15mins
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
```

단계 **3** Consent Token 챌린지를 Cisco TAC(Technical Assistance Center)에 전송합니다.

Cisco TAC는 사용자가 제공하는 Consent Token 챌린지를 사용하여 Consent Token 응답을 생성합니다.

단계 **4** 옵션 **2**를 선택한 다음 Cisco TAC에서 제공하는 Consent Token 응답을 입력합니다.

```
Enter CLI Option:
2
Please input the response when you are ready .....................
[redacted]
Response Signature Verified successfully !
Granting shell access
sh-4.2# ls
```

참고 응답 서명 확인에 성공하면 권한 있는 액세스가 활성화됩니다.

다음에 수행할 작업

쉘(shell) 모드를 종료하려면 **exit** 명령을 실행합니다.

```
sh-4.2# exit
exit
Root shell exited
```

옵션 **3**을 선택하여 루트 액세스 세션의 기록을 확인합니다.

```
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
3
**********************************
        SN No : 1
**********************************
Challenge
3Wc[redacted]
 generated at 2019-06-12 15:40:01.000
**********************************
        SN No : 2
**********************************
```

FIPS(연방 정보 처리 표준) 모드 지원

Cisco ISE FIPS(연방 정보 처리 표준) 140 모드는 Cisco FIPS 개체 모듈 암호화 모듈을 FIPS 140-2 모드로 초기화합니다. Cisco ISE는 임베디드 FIPS 140-2 검증 암호화 모듈을 사용합니다. FIPS 규정 준수 클레임에 대한 자세한 내용은 FIPS 규정 준수 공문을 참고해 주십시오.

FIPS 모드가 활성화되면 Cisco ISE 관리자 인터페이스에서는 창 오른쪽 상단 모서리에 있는 노드 이름 왼쪽에 FIPS 모드 아이콘이 표시됩니다.

Cisco ISE에서 FIPS 140-2 표준으로 지원되지 않는 프로토콜 또는 인증서의 사용을 탐지하면 규정을 준수하지 않는 프로토콜 또는 인증서의 이름과 함께 경고가 표시되고, FIPS 모드가 활성화되지 않습니다. FIPS 모드를 활성화하기 전에 FIPS 규정 준수 프로토콜만 선택하고 비 FIPS 규정 준수 인증서를 변경해야 합니다.

FIPS에서 인증서에 사용된 암호화 방법을 지원하지 않는 경우 Cisco ISE에 설치된 인증서를 다시 발급받아야 합니다.

FIPS 모드를 활성화하는 경우 영향을 받는 기능은 다음과 같습니다.

- SSL(Secure Sockets Layer)을 통한 LDAP(Lightweight Directory Access Protocol)

Cisco ISE는 RADIUS 공유 암호 및 키 관리 수단을 통해 FIPS 140-2 규정 준수를 지원합니다. FIPS 모드가 활성화되면 비 FIPS 규정 준수 알고리즘을 사용하는 기능이 실패합니다.

FIPS 모드를 활성화하는 경우:

- 모든 비 FIPS 규정 준수 암호 그룹은 EAP-TLS, PEAP 및 EAP-FAST에 대해 비활성화됩니다.
- 모든 비 FIPS 규정 준수 암호 그룹은 SSH에서 비활성화됩니다.
- 인증서 및 개인 키는 FIPS 규정 준수 해시 및 암호화 알고리즘만 사용해야 합니다.
- RSA 개인 키는 2048 비트 이상이어야 합니다.

- ECDSA 개인 키는 224 비트 이상이어야 합니다.
- ECDSA 서버 인증서는 TLS 1.2에서만 사용할 수 있습니다.
- DHE 암호는 모든 ISE TLS 클라이언트에 대해 2048 비트 이상의 DH 매개변수와 함께 사용할 수 있습니다.
- 3DES 암호는 Cisco ISE에서 서버로 사용할 수 없습니다.
- SHA-1은 인증서 생성에 사용할 수 없습니다.
- SHA-1은 클라이언트 인증서에서 사용할 수 없습니다.
- EAP-FAST의 익명 PAC 프로비저닝 옵션이 비활성화되었습니다.
- 로컬 SSH 서버는 FIPS 모드에서 작동합니다.
- 다음 프로토콜은 RADIUS에서 지원되지 않습니다.
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

FIPS 모드가 활성화되면 구축의 모든 노드가 자동으로 재부팅됩니다. Cisco ISE는 먼저 기본 PAN을 다시 시작하고 나서 각 보조 노드를 한 번에 하나씩 다시 시작하는 방식으로 점진적 재시작을 자동 수행합니다. 따라서 컨피그레이션을 변경하기 전에 다운타임을 계획하는 것이 좋습니다.

팁 데이터베이스 마이그레이션 프로세스를 완료하기 전에 FIPS 모드를 활성화하는 것은 권장되지 않습니다.

Cisco ISE에서 연방 정보 처리 표준 모드 활성화

Cisco ISE에서 FIPS 모드를 활성화하려면

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **FIPS Mode(FIPS** 모드**)**를 선택합니다.

단계 **2** **FIPS Mode(FIPS** 모드**)** 드롭다운 목록에서 **Enabled(**활성화됨**)** 옵션을 선택합니다.

단계 **3** **Save(**저장**)**를 클릭하고 머신을 다시 시작합니다.

다음에 수행할 작업

FIPS 모드를 활성화한 후 다음의 FIPS 140-2 준수 기능을 활성화하고 구성합니다.

- 셀프 서명 인증서 생성, 163 페이지.
- 인증서 서명 요청을 생성하고 인증 기관에 제출, 184 페이지.
- 네트워크 디바이스 정의 설정, 821 페이지에서 RADIUS 인증 설정을 구성합니다.

또한 CAC(Common Access Card) 기능을 사용하여 관리자 계정 권한 부여를 활성화할 수도 있습니다. 권한 부여용으로 CAC 기능을 사용하는 것은 엄밀히 말하자면 FIPS 140-2 요건은 아니지만, FIPS 140-2 규정 준수를 강화하기 위해 다양한 환경에서 사용되는 널리 알려진 보안 액세스 방식입니다.

관리자 CAC(Common Access Car) 인증을 위한 Cisco ISE 구성

시작하기 전에

- Cisco ISE에서 Active Directory에 대해 DNS(Domain Name Server)가 설정되어 있는지 확인합니다.
- 각 관리자 인증서에 대해 Active Directory 사용자 및 사용자 그룹 멤버십이 정의되었는지 확인합니다.

Cisco ISE가 브라우저에서 제출된 CAC(Common Access Card) 기반 클라이언트 인증서를 기반으로 관리자를 인증하고 권한을 부여할 수 있도록 하려면 다음을 구성합니다.

- 외부 ID 소스(다음 예에서는 Active Directory)
- 관리자가 속한 Active Directory의 사용자 그룹
- 인증서에서 사용자 ID를 찾는 방법
- Cisco ISE RBAC 권한에 대한 Active Directory 사용자 그룹 매핑
- 클라이언트 인증서에 서명을 하는 인증 기관(신뢰) 인증서
- 클라이언트 인증서가 인증 기관에 의해 취소되었는지를 확인하는 방법

Cisco ISE에 로그인할 때 CAC(Common Access Card)를 사용하여 자격 증명을 인증할 수 있습니다.

단계 **1** Cisco ISE에서 Active Directory ID 소스를 구성 하고 모든 Cisco ISE 노드를 Active Directory에 가입시킵니다.

단계 **2** 지침에 따라 인증서 인증 프로파일을 구성합니다.

Principal Name X.509 Attribute(보안 주체 이름 **X.509** 속성**)** 필드에 관리자 사용자 이름이 포함되어 있는 인증서의 속성을 선택해야 합니다. CAC(Common Access Card) 카드의 경우 보통 카드의 서명 인증서를 사용하여 Active Directory의 사용자를 조회합니다. 이 인증서에서는 **Subject Alternative Name(**주체 대체 이름**)** 확장(구체적으로는 해당 확장 내의 **Other Name(**기타 이름**)** 필드)에서 보안 주체 이름을 확인할 수 있습니다. 그러므로 여기서는 **Subject Alternative Name - Other Name(**주체 대체 이름 **-** 기타 이름**)** 속성을 선택해야 합니다.

사용자의 Active Directory 기록에 사용자 인증서가 포함되어 있으며 브라우저에서 수신된 인증서를 AD의 인증서와 비교하려는 경우 **Binary Certificate Comparison(**이진 인증서 비교**)** 확인란을 선택하고 앞에서 지정한 Active Directory 인스턴스 이름을 선택합니다.

단계 **3** 비밀번호 기반 관리자 인증에 대해 Active Directory를 활성화합니다. 앞에서 Cisco ISE에 연결하고 가입시킨 Active Directory 인스턴스 이름을 선택합니다.

참고 다른 컨피그레이션을 완료할 때까지는 비밀번호 기반 인증을 사용해야 합니다. 그런 후에는 이 절차의 마지막 작업에 따라 인증 유형을 클라이언트 인증서로 변경할 수 있습니다.

단계 **4** 외부 관리자 그룹을 생성하여 Active Directory 그룹에 매핑합니다. Cisco ISE GUI 메뉴에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭한 뒤 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Groups(**관리자 그룹**)**를 선택합니다. 외부 시스템 관리자 그룹을 생성합니다.

단계 **5** 외부 관리자 그룹에 대한 RBAC 권한을 할당할 관리자 권한 부여 정책을 구성합니다.

주의 외부 슈퍼 관리자 그룹을 생성하여 Active Directory 그룹에 매핑하고, 슈퍼 관리자 권한(메뉴 액세스 및 데이터 액세스)으로 관리자 권한 부여 정책을 구성한 후에 해당 Active Directory 그룹에서 사용자를 한 명 이상 생성하는 것이 좋습니다. 이 매핑을 사용하는 경우 **Client Certificate-Based Authentication(**클라이언트 인증서 기반 인증**)**을 활성화하면 외부 관리자 한 명 이상이 슈퍼 관리자 권한을 가지게 됩니다. 이렇게 하지 않으면 Cisco ISE 관리자가 관리 포털에서 중요한 기능을 사용하지 못하게 될 수도 있습니다.

단계 **6** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Store(**인증서 저장소**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** 인증 기관 인증서를 Cisco ISE 인증서 신뢰 저장소로 가져옵니다.

클라이언트 인증서 신뢰 체인의 인증 기관 인증서를 Cisco ISE 인증서 저장소에 저장하지 않으면 Cisco ISE는 클라이언트 인증서를 수락하지 않습니다. 적절한 인증 기관 인증서를 Cisco ISE 인증서 저장소로 가져와야 합니다.

a) **Import(**가져 오기**)**를 클릭하고 **Certificate File(**인증서 파일**)** 영역에서 **Choose File(**파일 선택**)**을 클릭합니다.
b) **Trust for client authentication and Syslog(**클라이언트 인증 및 시스템 로그용으로 신뢰**)** 확인란을 선택합니다.
c) **Submit(**제출**)**을 클릭합니다.

인증서를 가져오고 나면 구축의 모든 노드를 재시작하라는 메시지가 표시됩니다. 모든 인증서를 가져올 때까지 재시작을 연기할 수 있습니다. 그러나 모든 인증서를 가져온 후에는 계속 진행하기 전에 Cisco ISE를 재시작해야 합니다.

단계 **7** 취소 상태 확인용으로 인증 기관 인증서를 구성합니다.

a) **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **OSCP Client Profile(OSCP** 클라이언트 프로파일**)**.
b) **Add(**추가**)**를 클릭합니다.
c) OCSP 서버의 이름, 설명(선택 사항) 및 서버의 URL을 해당 필드에 입력합니다.
d) **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Store(**인증서 저장소**)**.
e) 클라이언트 인증서에 서명을 할 수 있는 각 CA 인증서에 대해 해당 CA의 취소 상태 확인을 수행할 방법을 지정합니다. 목록에서 인증 기관 인증서를 선택하고 Edit(편집)를 클릭합니다. 편집 페이지에서 OCSP 또는 CRL(인증서 해지 목록) 검증 또는 둘 다를 선택합니다. OCSP를 선택하는 경우 해당 인증 기관에 사용할 OCSP 서비스를 선택합니다. CRL을 선택하는 경우에는 CRL 배포 URL 및 기타 컨피그레이션 파라미터를 지정합니다.

단계 **8** 클라이언트 인증서 기반 인증을 활성화합니다. **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)**을 선택합니다.

a) **Authentication Method(**인증 방법**)** 탭에서 **Client Certificate Based(**클라이언트 인증서 기반**)** 라디오 버튼을 클릭합니다.
b) 이전에 구성한 인증서 인증 프로파일을 **Certificate Authentication Profile(**인증서 인증 프로파일**)** 드롭다운 목록에서 선택합니다.
c) **Identity Source(ID** 소스**)** 드롭 다운 목록에서 Active Directory 인스턴스 이름을 선택합니다.
d) **Save(**저장**)**를 클릭합니다.

여기서 패스워드 기반 인증을 클라이언트 인증서 기반 인증으로 전환합니다. 이전에 구성한 인증서 인증 프로파일에 따라 관리자 인증서를 인증하는 방법이 결정됩니다. 외부 ID 소스(이 예에서는 Active Directory)를 사용하여 관리자에게 권한을 부여합니다.

인증서 인증 프로파일의 보안 주체 이름 속성을 사용하여 Active Directory의 관리자를 조회합니다.

지원되는 **CAC(Common Access Card)** 표준

Cisco ISE는 CAC(Common Access Card) 인증 디바이스를 사용하여 자신을 인증하는 미국 정부 사용자를 지원합니다. CAC는 특정 직원을 식별하는 X.509 클라이언트 인증서 집합이 포함된 전자 칩을 사용하는 ID 배지입니다. CAC를 통해 액세스하려면 카드를 삽입하고 PIN을 입력할 수 있는 카드 판독기가 필요합니다. 그러면 카드에 있는 인증서가 Windows 인증서 저장소로 전송되어 Cisco ISE를 실행하는 로컬 브라우저 같은 애플리케이션에서 사용할 수 있게 됩니다.

Cisco ISE의 **CAC(Common Access Card)** 작업

Cisco ISE 인증이 클라이언트 인증서를 통해서만 발생하도록 관리 포털을 구성할 수 있습니다. 사용자 ID 또는 비밀번호가 필요한 자격 증명 기반 인증은 허용되지 않습니다. 클라이언트 인증서 기반 인증에서 CAC(Common Access Card) 카드를 삽입하고 PIN을 입력한 다음 Cisco ISE 관리 포털 URL을 브라우저 주소 필드에 입력합니다. 브라우저는 인증서를 Cisco ISE에 전달하며, Cisco ISE는 인증서 내용을 기반으로 로그인 세션을 인증하고 권한을 부여합니다. 이 프로세스에 성공한 경우 Cisco ISE 모니터링 및 문제 해결 홈 페이지가 표시되고 적절한 RBAC 권한이 부여됩니다.

Diffie-Hellman 알고리즘을 사용하여 **SSH** 키 교환 보호

Diffie-Hellman-Group14-SHA1 SSH 키 교환만 허용하도록 Cisco ISE를 구성할 수 있습니다. Cisco ISE CLI 구성 모드에서 다음 명령을 입력합니다.

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

예를 들면 다음과 같습니다.

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

보안 시스템 로그를 전송하도록 Cisco ISE 구성

시작하기 전에

Cisco ISE가 Cisco ISE 노드 간에, 그리고 모니터링 노드에 TLS로 보호되는 보안 시스템 로그만 전송하도록 구성하려면 다음 작업을 수행합니다.

- 구축의 모든 Cisco ISE 노드가 적절한 서버 인증서를 사용하여 구성되어 있는지 확인해 주십시오.
- 기본 네트워크 액세스 인증 정책이 모든 SSL 프로토콜 버전을 허용하지 않도록 합니다.
- 구축의 모든 노드가 기본 PAN에 등록되어 있는지 확인합니다. 또한 구축 환경에 있는 하나 이상의 노드가 보안 시스템 로그 수신기(TLS 서버)로 작동하도록 모니터링 페르소나가 활성화되어 있는지 확인합니다.
- 시스템 로그에 지원되는 RFC 표준을 확인합니다. 사용 중인 Cisco ISE 릴리스에 대한 Cisco Identity Services Engine 네트워크 구성 요소 호환성을 참고하십시오.

단계 **1** 보안 시스템 로그 원격 로깅 대상을 구성합니다.

단계 **2** 보안 시스템 로그 원격 로깅 대상으로 감사 가능한 이벤트를 보내도록 로깅 범주를 활성화합니다.

단계 **3** TCP 시스템 로그 및 UDP 시스템 로그 컬렉터를 비활성화합니다. TLS로 보호되는 시스템 로그 컬렉터만 활성화해야 합니다.

참고 Cisco ISE Release 2.6 이상 릴리스에서는 UDP 시스템 로그를 MnT 노드로 전달하기 위해 Cisco ISE 메시징 서비스를 사용하도록 설정할 경우 TLS로 보호되는 UDP 시스템 로그가 포함됩니다.

보안 시스템 로그 원격 로깅 대상 구성

Cisco ISE 시스템 로그는 다양한 용도로 사용할 수 있도록 로그 컬렉터에 의해 수집되어 저장됩니다. 보안 시스템 로그 대상을 구성하려면 모니터링 페르소나가 활성화되어있는 Cisco ISE 노드를 로그 컬렉터로 선택합니다.

단계 **1** Cisco ISE 관리 포털에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration**(관리) > **System**(시스템) > **Logging**(로깅) > **Remote Logging Targets**(원격 로깅 대상)을 선택합니다.

단계 **3** **Add**(추가)를 클릭합니다.

단계 **4** 보안 시스템 로그 서버의 이름을 입력합니다.

단계 **5** **Target Type**(대상 유형) 드롭다운 목록에서 **Secure Syslog**(보안 시스템 로그)를 선택합니다.

단계 **6** **Status**(상태) 드롭다운 목록에서 **Enabled**(활성화됨)를 선택합니다.

단계 **7** **Host / IP Address(**호스트/**IP** 주소**)** 필드에서 구축의 Cisco ISE 모니터링 노드 호스트 이름 또는 IP 주소를 입력합니다.

단계 **8** **Port(**포트**)** 필드에서 포트 번호를 *6514*로 입력합니다. 보안 시스템 로그 수신기는 TCP 포트 6514에서 수신 대기합니다.

단계 **9** **Facility Code(**기능 코드**)** 드롭다운 목록에서 시스템 로그 기능 코드를 선택합니다. 기본값은 **LOCAL6**입니다.

단계 **10** 다음 확인란을 선택하여 해당 컨피그레이션을 활성화합니다.

a) **Include Alarms For This Target(**이 대상에 대한 경보 포함**)**

b) **Comply to RFC 3164(RFC 3164** 준수**)**

c) **Enable Server Identity Check(**서버 **ID** 확인 활성화**)**

단계 **11** **Buffer Messages When Server Down(**서버가 다운되면 메시지 버퍼링**)** 확인란을 선택합니다. 이 옵션을 선택하면 Cisco ISE는 보안 시스템 로그 수신기에 연결할 수 없는 경우 로그를 저장하고, 보안 시스템 로그 수신기를 주기적으로 확인하며, 보안 시스템 로그 수신기가 작동하면 로그를 전달합니다.

a) **Buffer Size (MB)(**버퍼 크기**(MB))** 필드에 버퍼 크기를 입력합니다.

b) Cisco ISE가 보안 시스템 로그 수신기를 정기적으로 확인하도록 하려면 **Reconnect Time (Sec)(**다시 연결 시간 초과**(**초**))** 필드에서 다시 연결 시간 초과 값을 입력합니다. 시간 초과 값은 초 단위로 구성됩니다.

단계 **12** **Select CA Certificate(CA** 인증서 선택**)** 드롭다운 목록에서 Cisco ISE가 보안 시스템 로그 서버에 제공해야 하는 CA 인증서를 선택합니다.

단계 **13** 보안 시스템 로그를 구성할 때 **Ignore Server Certificate validation(**서버 인증서 검증 무시**)** 확인란이 선택되지 않았는지 확인합니다.

단계 **14** **Submit(**제출**)**을 클릭합니다.

원격 로깅 대상 설정

다음 표에서는 로깅 메시지를 저장하기 위한 외부 위치(시스템 로그 서버)를 생성하는 데 사용할 수 있는 **Remote Logging Targets(**원격 로깅 대상**)** 창의 필드에 대해 설명합니다. 이 창에 액세스하려면 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Remote Logging Targets(**원격 로깅 대상**)**에서 **Add(**추가**)**를 클릭합니다.

표 ***17:*** 원격 로깅 대상 설정

필드 이름	사용 지침
Name(이름**)**	새 시스템 로그 대상의 이름을 입력합니다.
Target Type(대상 유형**)**	드롭다운 목록에서 대상 유형을 선택합니다. 기본값은 **UDP** 시스템 로그입니다.
Description(설명**)**	새 대상의 간략한 설명을 입력합니다.
IP Address(IP 주소**)**	로그를 저장할 대상 머신의 IP 주소 또는 호스트 이름을 입력합니다. Cisco ISE는 로깅에 IPv4 및 IPv6 형식을 지원합니다.

필드 이름	사용 지침
Port(포트**)**	대상 머신의 포트 번호를 입력합니다.
Facility Code(시설 코드**)**	드롭다운 목록에서 로깅에 사용할 시스템 로그 시설 코드를 선택합니다. 유효한 옵션은 Local0~Local7입니다.
Maximum Length(최대 길이**)**	원격 로그 대상 메시지의 최대 길이를 입력합니다. 유효한 값은 200~1024바이트입니다.
Buffer Message When Server Down(서버 다운 시 메시지 버퍼링**)**	이 확인란은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **TCP** 시스템 로그 또는 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. TCP 시스템 로그 대상 및 보안 시스템 로그 대상을 사용할 수 없을 때 Cisco ISE가 시스템 로그 메시지를 버퍼링하도록 하려면 이 확인란을 선택합니다. Cisco ISE는 대상에 연결을 재개할 때 대상에 대한 메시지 전송을 다시 시도합니다. 연결이 재개되면 메시지는 가장 오래된 것부터 시작하여 최신순으로 전송됩니다. 버퍼링된 메시지는 항상 새 메시지보다 먼저 전송됩니다. 버퍼가 가득 차면 오래된 메시지는 폐기됩니다.
Buffer Size (MB)(버퍼 크기**(MB))**	각 대상의 버퍼 크기를 설정합니다. 기본적으로 버퍼 크기는 100MB로 설정됩니다. 버퍼 크기를 변경하면 버퍼가 지워지며 특정 대상에 대해 기존에 버퍼링된 모든 메시지는 손실됩니다.
Reconnect Timeout (Sec)(다시 연결 시간 초과**(**초**))**	서버가 다운되었을 때 TCP 및 보안 시스템 로그를 폐기할 때까지 저장할 시간을 초 단위로 입력합니다.
Select CA Certificate(CA 인증서 선택**)**	이 드롭다운 목록은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. 드롭다운 목록에서 클라이언트 인증서를 선택합니다.
Ignore Server Certificate Validation(서버 인증서 검증 무시**)**	이 확인란은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. Cisco ISE가 서버 인증서 인증을 무시하고 모든 시스템 로그 서버를 수락하도록 하려면 이 확인란을 선택합니다.

보안 시스템 로그 대상으로 감사 가능 이벤트를 전송하기 위한 로깅 범주 활성화

감사 가능 이벤트를 보안 시스템 로그 대상으로 보내려면 Cisco ISE에 대해 로깅 범주를 활성화해야 합니다.

단계 **1** Cisco ISE 관리 포털에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**을 선택합니다.

단계 **2** **Administrative and Operational Audit(**관리 및 운영 감사**)** 로깅 범주 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Log Severity Level(**로그 심각도 레벨**)** 드롭다운 목록에서 **WARN**을 선택합니다.

단계 **4** **Targets(**대상**)** 영역에서 앞서 생성한 보안 시스템 로그 원격 로깅 대상을 **Selected(**선택된**)** 영역으로 이동합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 이 절차를 반복하여 다음 로깅 범주를 활성화합니다. 이 두 로깅 범주 모두 기본 로그 심각도 레벨로 **INFO**를 가지며 수정할 수 없습니다.

- **AAA** 감사.
- **Posture and Client Provisioning Audit(**포스처 및 클라이언트 프로비저닝 감사**)**.

로깅 범주 구성

다음 표에서는 로깅 범주를 구성하는 데 사용할 수 있는 필드에 대해 설명합니다. 로그 심각도 레벨을 설정하고 로깅 범주의 로그에 대한 로깅 대상을 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**입니다.이 창에 액세스하려면 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 클릭합니다.

보고자 하는 범주 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다. 다음 표에서는 로깅 범주의 편집 창에 표시되는 필드에 대해 설명합니다.

표 ***18:*** 로깅 범주 설정

필드 이름	사용 지침
Name(이름**)**	로깅 범주의 이름을 표시합니다.

필드 이름	사용 지침
Log Severity Level(로그 심각도 레벨**)**	일부 로깅 범주의 경우이 값은 기본적으로 설정되며 수정할 수 없습니다. 일부 로깅 범주의 경우 드롭다운 목록에서 다음 심각도 레벨 중 하나를 선택할 수 있습니다. • **FATAL**: 긴급 범주입니다. 이 레벨은 Cisco ISE를 사용할 수 없으며 필요한 조치를 즉시 수행해야 함을 의미합니다. • **ERROR**: 이 레벨은 심각한 오류 상태를 나타냅니다. • **WARN**: 이 레벨은 정상적이기는 하지만 중요한 상태를 나타냅니다. 이 레벨은 여러 로깅 범주에 대해 설정되는 기본 수준입니다. • **INFO**: 이 레벨은 정보 메시지를 나타냅니다. • **DEBUG**: 이 레벨은 진단 버그 메시지를 나타냅니다.
Local Logging(로컬 로깅**)**	로컬 노드의 범주에 대한 이벤트 로깅을 활성화하려면 이 확인란을 선택합니다.
Targets(대상**)**	이 영역에서는 왼쪽 및 오른쪽 화살표 아이콘을 사용하여 **Available(**사용 가능**)** 영역과 **Selected(**선택됨 **)** 영역 간에 대상을 전송하는 방식으로 로깅 범주에 대한 대상을 변경할 수 있습니다. **Available(**사용 가능**)** 상자에는 기존 로깅 대상이 포함되어 있습니다. 여기에는 미리 정의된 로컬 대상과 사용자가 정의한 외부 대상이 모두 포함됩니다. **Selected(**선택됨**)** 영역은 처음에는 비어 있으며, 이후에 이 범주에 대해 선택된 대상을 표시됩니다.

TCP 시스템 로그 및 UDP 시스템 로그 컬렉터 비활성화

Cisco ISE가 노드 간에 보안 시스템 로그만 전송하도록 하려는 경우 TCP 및 UDP 시스템 로그 컬렉터를 비활성화하고 보안 시스템 로그 컬렉터만 활성화하십시오.

참고 Cisco ISE Release 2.6 이상 릴리스에서는 UDP 시스템 로그를 MnT 노드로 전달하기 위해 Cisco ISE 메시징 서비스를 사용하도록 설정할 경우 TLS로 보호되는 UDP 시스템 로그가 포함됩니다. Cisco ISE 메시징 서비스의 시스템 로그, 76 페이지의 내용을 참조하십시오.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Remote Logging Targets(**원격 로깅 대상**)**를 선택합니다.

단계 **2** TCP 또는 UDP 시스템 로그 컬렉터 옆의 라디오 버튼을 클릭합니다.

단계 **3** **Edit(**편집**)**를 클릭합니다.

단계 **4** **Status(**상태**)** 드롭다운 목록에서 **Disabled(**비활성화됨**)**를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 이 절차를 반복하여 모든 TCP 또는 UDP 시스템 로그 컬렉터를 비활성화합니다.

기본 보안 시스템 로그 컬렉터

Cisco ISE는 MnT 노드에 대한 기본 보안 시스템 로그 컬렉터를 제공합니다. 기본적으로 로깅 범주는 이러한 기본 보안 시스템 로그 컬렉터에 매핑되지 않습니다. 기본 보안 시스템 로그 컬렉터의 이름은 다음과 같습니다.

- 기본 MnT node: SecureSyslogCollector
- 보조 MnT node: SecureSyslogCollector2

이 정보는 **Remote Logging Targets(**원격 로그인 대상**)** 창에서 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로그인**)** > **Remote Logging Targets(**원격 로그인 대상**)**을 선택합니다 에서 확인할 수 있습니다. 기본 시스템 로그 컬렉터는 삭제할 수 없으며 기본 시스템 로그 컬렉터에 대해서는 다음 필드를 업데이트할 수 없습니다.

- **Name(**이름**)**
- **Target Type(**대상 유형**)**
- **IP /** 호스트 주소
- **Port(**포트**)**

Cisco ISE를 새로 설치할 때 **Default Self-signed Server Certificate(**기본 자체 서명 서버 인증서**)**라는 이름의 인증서가 신뢰할 수 있는 인증서 저장소에 추가됩니다. 이 인증서는 **Trust for Client authentication and Syslog(**클라이언트 인증 및 시스템 로그에 대한 신뢰**)** 사용으로 표시되어 있으므로 안전한 시스템 로그 사용에 적용할 수 있습니다. 구축을 구성하거나 인증서를 업데이트하는 동안 보안 시스템 로그 대상에 관련 인증서를 할당해야 합니다.

Cisco ISE 업그레이드 중에 포트 6514의 MnT 노드를 가리키는 기존 보안 시스템 로그 대상이 있는 경우 대상의 이름과 컨피그레이션이 유지됩니다. 업그레이드 후에는 이러한 시스템 로그 대상을 삭제할 수 없으며 다음 필드를 편집할 수 없습니다.

- **Name(**이름**)**
- **Target Type(**대상 유형**)**
- **IP /** 호스트 주소
- **Port(**포트**)**

업그레이드 시점에 이러한 대상이 없는 경우 인증서 설치 없이 기본 보안 시스템 로그 대상이 신규 설치 시나리오와 유사하게 생성됩니다. 이러한 시스템 로그 대상에 관련 인증서를 할당할 수 있습니다. 인증서에 매핑되지 않은 보안 시스템 로그 대상을 로깅 범주에 매핑하려고 하면 Cisco ISE는 다음 메시지를 표시합니다.

Please configure the certificate for *log_target_name*

오프라인 유지 관리

유지 관리 기간이 1시간 미만인 경우 Cisco ISE 노드를 오프라인으로 전환하고 유지 관리 작업을 수행합니다. 노드를 다시 온라인 상태로 전환하면 PAN 노드는 유지 관리 기간 동안 발생한 모든 변경 사항을 자동으로 동기화합니다. 변경 사항이 자동으로 동기화되지 않으면 PAN과 수동으로 동기화할 수 있습니다.

유지 관리 기간이 1시간을 초과하는 경우 유지 관리 시 노드를 등록 취소하고 노드를 다시 구축에 추가할 때 재등록합니다.

활동이 적은 기간에 유지 관리를 예약하는 것이 좋습니다.

참고

1. 큐에 1,000,000개가 넘는 메시지가 포함되어 있거나 Cisco ISE 노드가 6시간 이상 오프라인 상태인 경우 데이터 복제 문제가 발생할 수 있습니다.
2. 기본 MnT 노드에서 유지 관리를 수행하는 경우 유지 관리 활동을 수행하기 전에 MnT 노드의 운영 백업을 수행하는 것이 좋습니다.

엔드포인트 로그인 자격 증명 구성

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

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

다음 탭이 표시됩니다.

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

Cisco ISE에서의 인증서 관리

인증서는 개인, 서버, 회사 또는 다른 엔터티를 식별하고 해당 엔터티를 공용 키에 연결하는 전자 문서입니다. 자가서명 인증서는 해당 생성자가 서명합니다. 인증서는 자가 서명하거나 외부 CA(Certificate Authority)가 디지털 서명할 수 있습니다. CA 서명 디지털 인증서는 업계 표준으로 자가서명 인증서보다 보안성이 더 높은 것으로 간주됩니다.

인증서는 네트워크에서 보안 액세스를 제공하기 위해 사용됩니다. 인증서는 엔드포인트에 대한 Cisco ISE 노드를 식별하고 엔드포인트와 Cisco ISE 노드 간 통신을 보호합니다.

Cisco ISE는 다음 용도로 인증서를 사용합니다.

- Cisco ISE 노드 간의 통신.
- Cisco ISE와 시스템 로그 및 피드 서버와 같은 외부 서버 간의 통신.
- Cisco ISE와 최종 사용자 포털(예: 게스트, 스폰서 및 BYOD 포털) 간의 통신.

관리 포털을 사용하여 구축 환경의 모든 노드에 대한 인증서를 관리할 수 있습니다.

Cisco ISE에서 보안 액세스를 위한 인증서 구성

Cisco ISE는 PKI(Public Key Infrastructure)를 사용하여 엔드포인트 및 관리자 모두와의 보안 통신은 물론 다중 노드 구축 환경에서 Cisco ISE 노드 간 보안 통신을 제공합니다. PKI는 X.509 디지털 인증서를 사용하여 메시지의 암호화 및 암호 해독을 위한 공용 키를 전송하고 사용자 및 디바이스를 나타내는 다른 인증서의 신뢰성을 확인합니다. Cisco ISE 관리 포털을 통해 두 가지 X.509 인증서 범주를 관리할 수 있습니다.

- 시스템 인증서: 이는 클라이언트 애플리케이션에 대한 Cisco ISE 노드를 식별하는 서버 인증서입니다. 각 Cisco ISE 노드는 고유한 시스템 인증서를 가지고 있으며 각 인증서는 해당 개인 키와 함께 노드에 저장됩니다.
- 신뢰할 수 있는 인증서: 이는 사용자 및 디바이스로부터 받은 공개 키에 대한 신뢰 관계를 설정하는 데 사용되는 CA 인증서입니다. 신뢰할 수 있는 인증서 저장소에는 엔터프라이즈 네트워크에 모바일 디바이스를 등록할 수 있게 해주는 SCEP(Simple Certificate Enrollment Protocol)를 통해 배포된 인증서가 포함되어 있습니다. 신뢰할 수 있는 인증서는 기본 PAN에서 관리되며 Cisco ISE 구축 환경의 다른 모든 노드로 자동 복제됩니다.

분산형 구축 환경에서는 인증서를 PAN의 CTL(Certificate Trust List)로만 가져올 수 있습니다. 인증서는 보조 노드로 복제됩니다.

Cisco ISE의 인증서 인증이 인증서 기반 확인 기능의 소소한 차이에 따른 영향을 받지 않게 하려면 네트워크에 구축된 모든 Cisco ISE 노드에 대해 소문자 호스트 이름을 사용해 주십시오.

인증서 사용

Cisco ISE로 인증서를 가져오는 경우 인증서를 사용할 용도를 지정해야 합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**시스템 관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**) Import(**가져오기**)**를 클릭합니다.

다음 용도 중 하나 이상을 선택합니다.

- **Admin(**관리**)**: 노드 간 통신 및 관리 포털 인증에 사용됩니다.
- **EAP Authentication(EAP** 인증**)**: TLS 기반 EAP 인증에 사용됩니다.
- **RADIUS DTLS**: RADIUS DTLS 서버 인증에 사용됩니다.
- **Portal(**포털**)**: 모든 Cisco ISE 최종 사용자 포털과의 통신에 사용됩니다.
- **SAML**: SAML 응답이 올바른 ID 제공자로부터 수신되고 있는지 확인하는 데 사용됩니다.
- **pxGrid**: pxGrid 컨트롤러와의 통신에 사용됩니다.

각 노드의 다양한 인증서를 관리 포털(관리자 사용), pxGrid 컨트롤(pxGrid 사용) 및 TLS 기반 EAP 인증(EAP 인증 사용)과 통신할 수 있도록 연결할 수 있습니다. 그러나 각 노드에서 이러한 용도로 하나의 인증서만 연결할 수 있습니다.

구축에서 웹 포털 요청을 처리할 수 있는 PSN이 여러 개 있는 경우 Cisco ISE에는 포털 통신에 사용할 인증서를 식별할 수 있는 고유 식별자가 필요합니다. 포털에서 사용하도록 지정된 인증서를 추가하거나 가져오는 경우 인증서 그룹 태그를 정의하고 이를 구축의 각 노드에 있는 해당 인증서와 연결해야 합니다. 이 인증서 그룹 태그를 해당 최종 사용자 포털(게스트, 스폰서 및 개인 디바이스 포털)에 연결해야 합니다. 이 인증서 그룹 태그는 Cisco ISE가 이러한 각 포털과 통신할 때 사용해야 하는 인증서를 식별하도록 도와주는 고유 식별자입니다. 포털마다 각 노드의 인증서를 하나씩만 지정할 수 있습니다.

참고 EAP-TLS 클라이언트 인증서에는 다음 암호에 대해 KeyUsage=Key Agreement 및 ExtendedKeyUsage=Client Authentication이 있어야 합니다.

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

EAP-TLS 클라이언트 인증서에는 다음 암호에 대해 KeyUsage=Key Encipherment 및 ExtendedKeyUsage=Client Authentication이 있어야 합니다.

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

Cisco ISE에서의 인증서 일치

구축에서 Cisco ISE 노드를 설정할 때 노드는 서로 통신합니다. 시스템은 각 Cisco ISE 노드의 FQDN이 일치하는지 확인합니다(예: ise1.cisco.com 및 ise2.cisco.com 또는 와일드카드 인증서를 사용하는 경우 *.cisco.com). 또한 외부 머신에서 Cisco ISE 서버에 인증서를 제공할 경우 Cisco ISE 서버의 인증서와 비교하여 인증을 위해 제공되는 외부 인증서를 확인하거나 일치시킵니다. 두 인증서가 일치하면 인증이 성공합니다.

Cisco 의 경우 노드 간(2개가 있는 경우), 그리고 Cisco 와 pxGrid 간에 일치가 수행됩니다.

Cisco ISE에서는 다음과 같이 일치하는 주체 이름을 확인합니다.

1. Cisco ISE에서 인증서의 대체 주체 이름 확장을 확인합니다. 대체 주체 이름에 하나 이상의 DNS 이름이 있는 경우 DNS 이름 중 하나를 Cisco ISE 노드의 FQDN과 일치시켜야 합니다. 와일드카드 인증서를 사용하는 경우 와일드카드 도메인 이름을 Cisco ISE 노드 FQDN의 도메인과 일치시켜야 합니다.
2. 대체 주체 이름에 DNS 이름이 없거나 대체 주체 이름이 완전히 누락된 경우 인증서의 **Subject(**주체**)** 필드에 있는 공용 이름 또는 인증서의 **Subject(**주체**)** 필드에 있는 와일드카드 도메인을 노드의 FQDN과 일치시켜야 합니다.
3. 일치 항목이 발견되지 않으면 인증서가 거부됩니다.

참고 Cisco ISE로 가져온 X.509 인증서는 PEM(Privacy-Enhanced Mail) 또는 식별 부호화 규칙 형식이어야 합니다. 인증서 체인(시스템 인증서와 여기에 서명하는 신뢰 인증서 시퀀스)이 포함된 파일은 특정 제한 사항에 따라 가져올 수 있습니다.

X.509 인증서의 유효성

X.509 인증서는 특정 날짜까지 유효합니다. 시스템 인증서가 만료되면 해당 인증서를 사용하는 Cisco ISE 기능이 영향을 받게 됩니다. Cisco ISE에서는 만료 날짜까지 남은 기간이 90일 미만이면 시스템 인증서의 보류 중인 만료에 대한 알림을 표시합니다. 이 알림은 다음과 같은 여러 가지 방법으로 표시됩니다.

- **System Certificates(**시스템 인증서**)** 창에 색상이 지정된 만료 상태 아이콘이 나타납니다. 이 창을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificate Management(**시스템 관리**)** > **Certificates(**시스템 인증서**)**를 선택합니다.
- Cisco ISE 시스템 진단 보고서에 만료 메시지가 나타납니다. 이 창을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Diagnostics(**진단**)** > **System Diagnostics(**시스템 진단**)**를 선택합니다.
- 만료 전 90일, 60일, 그리고 30일 시점에 만료 경보가 생성됩니다. 만료 전 30일부터는 매일 만료 경보가 생성됩니다.

만료되는 인증서가 셀프 서명 인증서인 경우에는 인증서를 편집하여 만료 날짜를 연장할 수 있습니다. 인증 기관이 서명한 인증서의 경우에는 만료 전에 충분한 여유를 두고 인증 기관으로부터 교체 인증서를 받아야 합니다.

Cisco ISE에서 공개 키 인프라 활성화

PKI는 보안 통신을 수행할 수 있도록 하고 디지털 서명을 사용 중인 사용자의 신원을 확인하는 암호화 기술입니다.

단계 **1** 구축의 각 노드에서 다음을 위해 시스템 인증서를 구성합니다.

- EAP-TLS와 같은 TLS 지원 인증 프로토콜
- 관리 포털 인증
- 브라우저 및 REST 클라이언트에서 Cisco ISE 웹 포털에 액세스할 수 있도록 허용
- pxGrid 컨트롤러에 대한 액세스 허용

기본적으로 Cisco ISE 노드는 EAP 인증과 관리 포털, 최종 사용자 포털 및 pxGrid 컨트롤러 액세스에 사용되는 SSC(자가서명 인증서)와 함께 미리 설치됩니다. 일반적인 엔터프라이즈 환경에서 이 자가서명 인증서는 신뢰할 수 있는 CA가 서명한 서버 인증서로 교체됩니다.

단계 **2** 사용자와의 신뢰 관계를 설정하는 데 필요한 CA 인증서 및 Cisco ISE에 제공할 디바이스 인증서를 신뢰할 수 있는 인증서 저장소에 저장합니다.

루트 CA 인증서 하나와 중간 CA 인증서 하나 이상으로 구성된 인증서 체인을 사용하여 사용자 또는 디바이스 인증서의 신뢰성을 검증하려면 다음을 수행하십시오.

- 루트 CA에 대해 관련 신뢰 옵션을 활성화합니다.

  Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** >**Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다. 이 창에서 루트 CA 인증서의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다. **Usage(**사용**)** 영역의 **Trusted For(**신뢰 대상**)** 영역에서 필요한 확인란을 선택합니다.

- 루트 CA에 대해 신뢰 옵션을 활성화하지 않으려면 전체 CA 서명 인증서 체인을 신뢰할 수 있는 인증서 저장소로 가져옵니다.

노드 간 통신의 경우에는 Cisco ISE 구축에 포함된 각 노드의 관리자 시스템 인증서를 검증하는 신뢰 인증서를 신뢰할 수 있는 인증서 저장소에 저장해야 합니다. 기본 자가서명 인증서를 노드 간 통신에 사용하려는 경우에는 각 Cisco ISE 노드의 System Certificates(시스템 인증서) 페이지에서 이 인증서를 내보낸 다음 신뢰할 수 있는 인증서 저장소로 가져옵니다. 자가서명 인증서를 CA에서 서명한 인증서로 교체하는 경우에는 적절한 루트 CA 및 중간 CA 인증서만 신뢰할 수 있는 인증서 저장소에 저장하면 됩니다. 이 단계를 완료할 때까지는 Cisco ISE 구축에서 노드를 등록할 수 없습니다.

구축의 클라이언트와 PSN 간 통신을 보호하기 위해 자가서명 인증서를 사용하는 경우 BYOD 사용자가 한 위치에서 다른 위치로 이동하면 EAP-TLS 사용자 인증이 실패합니다. 몇 개의 PSN 간에 서비스를 받아야 하는 인증 요청

의 경우에는 외부에서 서명한 CA 인증서를 사용하여 클라이언트와 PSN 간의 통신을 보호하거나 외부 CA가 서명한 와일드카드 인증서를 사용해야 합니다.

참고 독립형 Cisco ISE 노드 또는 PAN에서 백업을 가져온 후 구축의 노드 하나 이상에서 인증서 컨피그레이션을 변경하는 경우에는 다른 백업을 가져와서 데이터를 복원해야 합니다. 이렇게 하지 않는 경우 이전 백업을 사용하여 데이터를 복원하려고 하면 노드 간의 통신이 실패할 수 있습니다.

와일드카드 인증서

와일드카드 인증서는 와일드카드 표기법(별표 및 도메인 이름 앞의 마침표)을 사용하므로 조직의 여러 호스트 간에 인증서를 공유할 수 있습니다. 예를 들어 인증서 주체의 **CN** 값은 aaa.ise.local과 같은 일반 호스트 이름이고, SAN 필드에는 동일한 일반 호스트 이름과 함께 DNS.1=aaa.ise.local 및 DNS.2=*.ise.local과 같은 와일드카드 표기법이 포함된다고 가정합니다.

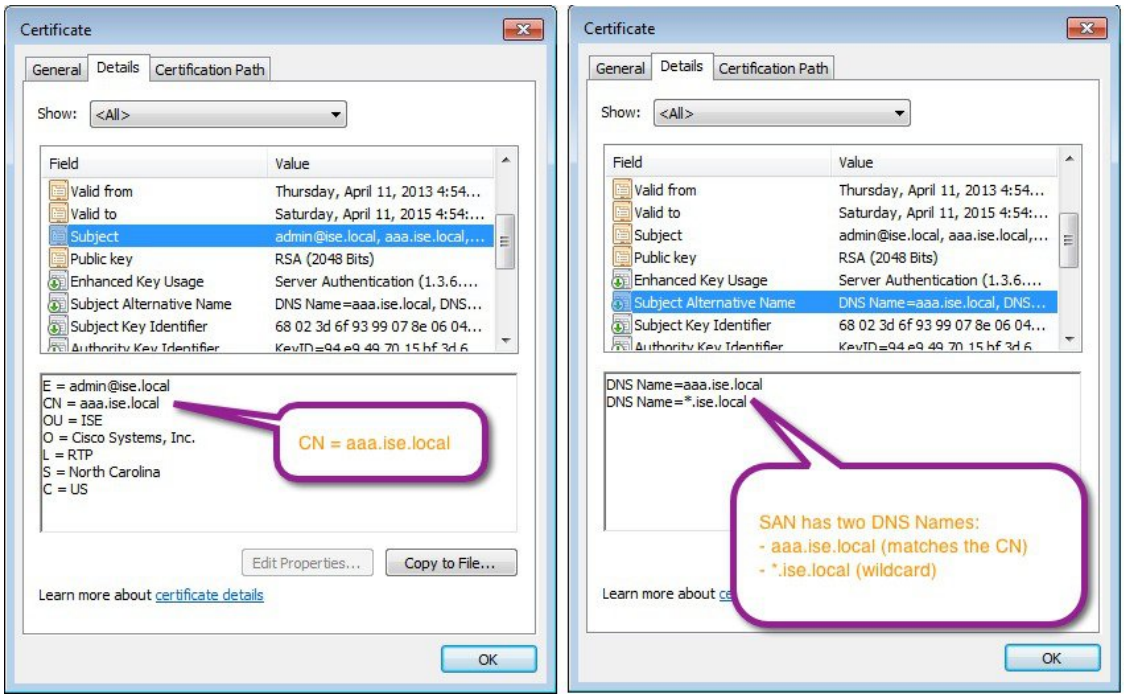
*.ise.local을 사용하도록 와일드카드 인증서를 구성하는 경우 동일한 인증서를 사용하여 DNS 이름이과 같이 ".ise.local"로 끝나는 다른 모든 호스트를 보호할 수 있습니다.:

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

와일드카드 인증서는 일반 인증서와 동일한 방법으로 통신을 보호하며 요청은 동일한 검증 방법을 사용하여 처리됩니다.

다음 그림에는 웹사이트를 보호하는 데 사용되는 와일드카드 인증서의 예가 나와 있습니다.

그림 7: 와일드카드 인증서 예



Cisco ISE의 와일드카드 인증서 지원

Cisco ISE는 와일드카드 인증서를 지원합니다. 이전 릴리스에서 Cisco ISE는 HTTPS용으로 활성화된 모든 인증서를 확인하여 CN 필드가 호스트의 FQDN과 정확하게 일치하는지를 확인했습니다. 이 필드가 일치하지 않으면 인증서를 HTTPS 통신에 사용할 수 없었습니다.

이전 릴리스에서 Cisco ISE는 해당 CN 값을 사용하여 url-redirect A-V 쌍 문자열의 변수를 교체했습니다. 모든 CWA(Centralized Web Authentication), 온보딩, 포스처 리디렉션 등에 대해 CN 값이 사용되었습니다.

Cisco ISE는 ISE 노드의 호스트 이름을 CN으로 사용합니다.

HTTPS 및 Extensible Authentication Protocol 통신용 와일드카드 인증서

SSL 또는 TLS 터널링을 이용하는 EAP 프로토콜 및 관리용 Cisco ISE(웹 기반 서비스)에서 와일드카드 서버 인증서를 사용할 수 있습니다. 와일드카드 인증서를 사용하는 경우에는 각 Cisco ISE 노드에 대해 고유한 인증서를 생성하지 않아도 됩니다. 또한 인증서 경고가 표시되지 않도록 하기 위해 여러 FQDN 값을 SAN 필드에 입력할 필요도 없습니다. SAN 필드에 별표(*)를 사용하면 구축의 여러 노드 간에 단일 인증서를 공유할 수 있으며, 인증서 이름 불일치 경고가 표시되지 않습니다. 그러나 와일드카드 인증서를 사용하는 방식은 각 Cisco ISE 노드에 고유한 서버 인증서를 할당하는 방식보다 보안성이 낮은 것으로 간주됩니다.

공개 와일드카드 인증서를 게스트 포털에 할당하고 루트 CA 인증서가 포함된 하위 CA를 가져오는 경우 Cisco ISE 서비스가 재시작될 때까지 인증서 체인이 전송되지 않습니다.

참고 와일드카드 인증서를 사용하는 경우에는 보안 향상을 위해 도메인 공간을 분할하는 것이 좋습니다. 예를 들어 *.example.com 대신 *.amer.example.com으로 도메인을 분할할 수 있습니다. 도메인을 분할하지 않으면 심각한 보안 문제가 발생할 수 있습니다.

와일드카드 인증서에서는 도메인 이름 앞에 별표(*)와 기간이 사용됩니다. 인증서 주체 이름의 공용 이름 값은 aaa.ise.local과 같은 일반 호스트 이름이고 SAN 필드에 *.ise.local과 같은 와일드카드 문자를 사용하는 경우를 예로 들 수 있습니다. Cisco ISE는 와일드카드 문자(*)가 표시되는 식별자의 맨 왼쪽 문자인 와일드카드 인증서를 지원합니다. *.example.com 또는 *.ind.example.com 등을 예로 들 수 있습니다. Cisco ISE는 표시되는 식별자가 와일드카드 문자와 함께 다른 문자를 포함하는 인증서를 지원하지 않습니다. abc*.example.com, a*b.example.com, *abc.example.com 등을 예로 들 수 있습니다.

URL 리디렉션의 인증된 도메인 이름

중앙 웹 인증, 디바이스 등록 웹 인증, 기본 신청자 프로비저닝, 모바일 디바이스 관리, 클라이언트 프로비저닝 및 포스처 서비스용으로 권한 부여 프로파일 리디렉션이 수행됩니다. Cisco ISE가 권한 부여 프로파일 리디렉션을 구축할 때 결과로 생성된 cisco-av-pair에는 다음과 유사한 문자열이 포함됩니다.

url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa와 같은 문자열이 포함됩니다.

이 요청을 처리할 때 Cisco ISE는 이 문자열의 일부 키워드를 실제 값으로 대체합니다. 예를 들어 SessionIdValue는 요청의 실제 세션 ID로 바뀝니다. eth0 인터페이스의 경우 Cisco ISE는 URL의 IP를 Cisco ISE 노드의 FQDN으로 바꿉니다. eth0가 아닌 인터페이스의 경우 Cisco ISE는 URL의 IP 주소를 사용합니다. eth1~eth3 인터페이스에 대해 호스트 별칭(이름)을 할당할 수 있습니다. Cisco ISE는 URL 리디렉션 중에 IP 주소를 이러한 별칭으로 대체할 수 있습니다.

이렇게 하려는 경우 Cisco ISE CLI ISE /admin(config)# 프롬프트의 컨피그레이션 모드에서 **ip host** 명령을 사용하면 됩니다.

ip host *IP_address host-alias FQDN-string*

여기서 *IP_address*는 네트워크 인터페이스의 IP 주소(eth1, eth2 또는 eth3)이고 *host-alias*는 네트워크 인터페이스에 할당하는 이름입니다. *FQDN-string*은 네트워크 인터페이스의 인증된 도메인 이름입니다. 이 명령을 사용하여 *host-alias* 또는 *FQDN-string* 중 하나 또는 둘 다를 네트워크 인터페이스에 할당할 수 있습니다.

ip host 명령을 사용하는 예는 ip host a.b.c.d sales sales.amerxyz.com과 같습니다.

eth0이 아닌 인터페이스에 호스트 별칭을 할당한 후에는 **application start ise** 명령을 사용하여 Cisco ISE에서 애플리케이션 서비스를 재시작해야 합니다.

네트워크 인터페이스와 호스트 별칭의 연결을 제거하려면 이 명령의 **no** 형식을 사용합니다.

no ip host *IP_address host-alias FQDN-string*

호스트 별칭 정의를 보려면 **show running-config** 명령을 사용합니다.

*FQDN-string*을 제공하는 경우 Cisco ISE는 URL의 IP 주소를 FQDN으로 바꿉니다. 호스트 별칭만 제공하는 경우 Cisco ISE는 호스트 별칭을 구성된 IP 도메인 이름과 결합하여 완전한 FQDN을 만든 다음 URL의 IP 주소를 FQDN으로 바꿉니다. 네트워크 인터페이스를 호스트 별칭에 매핑하지 않으면 Cisco ISE는 URL에 포함된 네트워크 인터페이스의 IP 주소를 사용합니다.

클라이언트 프로비저닝이나 기본 신청자 또는 게스트 플로우용으로 eth0이 아닌 인터페이스를 사용할 때는 PSN 인증서의 SAN 필드에서 eth0이 아닌 인터페이스의 IP 주소 또는 호스트 별칭을 적절하게 구성해야 합니다.

와일드카드 인증서를 사용하는 경우의 이점

- 비용 절감: 서드 파티 CA에서 서명한 인증서는 비용이 많이 들며 특히 서버 수가 증가할수록 비용이 큽니다. 와일드카드 인증서는 Cisco ISE 구축의 여러 노드에서 사용할 수 있습니다.
- 운영 효율성: 와일드카드 인증서를 사용하면 모든 PSN이 EAP 및 웹 서비스에 대해 동일한 인증서를 공유할 수 있습니다. 막대한 비용 절감 효과를 거둘 수 있을 뿐 아니라, 인증서를 한 번 생성하여 모든 PSN에 적용하는 방식으로 인증서 관리 작업도 간소화할 수 있습니다.
- 인증 오류 감소: 와일드카드 인증서는 클라이언트가 프로파일에 신뢰할 수 있는 인증서를 저장하지만 서명 루트를 신뢰할 수 있는 iOS 키 체인을 따르지 않는 Apple iOS 디바이스에서 발생하는 문제를 해결해 줍니다. PSN과 처음 통신하는 iOS 클라이언트는 신뢰할 수 있는 CA가 인증서에 서명한 경우에도 PSN 인증서를 명시적으로 신뢰하지 않습니다. 와일드카드 인증서를 사용하면 인증서가 모든 PSN에서 동일하게 유지되므로 사용자가 인증서를 수락하기만 하면 여러 PSN에 대한 이후의 인증은 오류 또는 메시지 없이 진행됩니다.
- 신청자 컨피그레이션 간소화: 예를 들어 PEAP-MSCHAPv2 및 신뢰할 수 있는 서버 인증서가 있는 Microsoft Windows 신청자에서는 각 서버 인증서를 신뢰하도록 지정해야 합니다. 아니면 클라이언트가 다른 PSN을 사용하여 연결할 때 사용자에게 각 PSN 인증서를 신뢰하는지 묻는 메시지가 표시될 수 있습니다. 와일드카드 인증서를 사용하면 각 PSN의 개별 인증서가 아니라 단일 서버 인증서를 신뢰할 수 있습니다.
- 와일드카드 인증서를 사용하면 메시지 수를 줄이고 원활한 연결을 진행할 수 있으므로 사용자 환경을 개선할 수 있습니다.

와일드카드 인증서를 사용하는 경우의 단점

다음은 와일드카드 인증서 사용과 관련된 몇 가지 보안 고려 사항입니다.

- 감사 기능 손실 및 미거부
- 개인 키의 노출 증가
- 일반적이지 않거나 관리자가 이해할 수 없음

와일드카드 인증서는 각 Cisco ISE 노드의 고유 서버 인증서보다 보안성이 낮은 것으로 간주됩니다. 그러나 보안 위험 문제보다 비용 및 다른 운영 관련 이점이 훨씬 큽니다.

Cisco Adaptive Security Appliance와 같은 보안 디바이스도 와일드카드 인증서를 지원합니다.

와일드카드 인증서를 구축할 때에는 주의해야 합니다. 예를 들어 *.company.local을 사용하여 인증서를 생성하는 경우 공격자가 개인 키를 복구할 수 있으면 공격자는 company.local 도메인의 서버를 스푸핑할 수 있습니다. 그러므로 이러한 종류의 문제를 방지하려면 도메인 공간을 분할하는 것이 좋습니다.

이러한 문제를 해결하고 사용 범위를 제한하려면 조직의 특정 하위 도메인을 보호하도록 와일드카드 인증서를 사용할 수 있습니다. 와일드카드를 지정하려는 공통 이름의 하위 도메인 영역에 별표(*)를 추가합니다.

예를 들어 *.ise.company.local에 대한 와일드카드 인증서를 구성하는 경우 다음과 같이 DNS 이름이 ".ise.company.local"로 끝나는 다른 모든 호스트를 해당 인증서를 사용하여 보호할 수 있습니다.

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

와일드카드 인증서 호환성

와일드카드 인증서는 일반적으로 인증서 주체의 CN(Common Name)으로 나열되는 와일드카드를 사용하여 생성됩니다. Cisco ISE에서는 이러한 생성 유형을 지원합니다. 그러나 모든 엔드포인트 신청자가 인증서 주체의 와일드카드 문자를 지원하는 것은 아닙니다.

테스트를 거친 모든 Microsoft 기본 신청자(현재 중단된 Windows Mobile 포함)는 인증서 주체에서 와일드카드 문자를 지원하지 않습니다.

Subject(주체) 필드에서 와일드카드 문자 사용을 허용할 수 있는 Cisco AnyConnect NAM(Network Access Manager) 등의 다른 신청자를 사용할 수 있습니다.

또한 인증서의 주체 대체 이름에 특정 하위 도메인을 포함하여 호환되지 않는 디바이스에서 사용 가능한 DigiCert의 Wildcard Plus와 같은 특수 와일드카드 인증서를 사용할 수도 있습니다.

Microsoft 신청자 제한으로 인해 와일드카드 인증서를 사용할 수 없다고 생각할 수도 있지만, Microsoft 기본 신청자를 포함하여 보안 액세스용으로 테스트된 모든 디바이스에서 사용할 수 있는 와일드카드 인증서를 생성하는 대체 방법이 있습니다.

이러한 인증서를 생성하려면 주체에 와일드카드 문자를 사용하는 대신 SAN(Subject Alterative Name) 필드에 와일드카드 문자를 사용해야 합니다. SAN 필드에서 도메인 이름(DNS 이름) 확인용 확장을 유지 관리할 수 있습니다. 자세한 내용은 RFC 6125 및 2128을 참고해 주십시오.

인증서 계층 구조

관리 포털에서 모든 엔드포인트, 시스템 및 신뢰할 수 있는 인증서의 인증서 계층 구조 또는 인증서 신뢰 체인을 확인할 수 있습니다. 인증서 계층 구조에는 인증서, 모든 중간 CA 인증서 및 루트 인증서가 포함됩니다. 예를 들어 관리 포털에서 시스템 인증서를 보도록 선택하면 해당 시스템 인증서의 세부정보가 표시됩니다. 인증서 계층 구조는 인증서의 상단에 나타납니다. 계층 구조에서 인증서를 클릭하면 해당 세부정보를 볼 수 있습니다. 셀프 서명 인증서에는 계층 구조 또는 신뢰 체인이 없습니다.

인증서 목록 창의 **Status(**상태**)** 열에는 다음 아이콘 중 하나가 표시됩니다.

- 녹색 아이콘: 유효한 인증서(유효한 신뢰 체인)를 나타냅니다.
- 빨간색 아이콘: 오류(예: 신뢰 인증서가 누락되었거나 만료됨)를 나타냅니다.
- 노란색 아이콘: 인증서가 곧 만료된다고 경고하며 갱신하라는 메시지가 표시됩니다.

시스템 인증서

Cisco ISE 시스템 인증서는 구축의 다른 노드 및 클라이언트 애플리케이션에 대해 Cisco ISE 노드를 식별하는 서버 인증서입니다. 시스템 인증서는 다음과 같이 사용됩니다.

- Cisco ISE 구축에서 노드 간 통신에 사용됩니다. 이러한 인증서의 **Usage(**사용**)** 영역에서 **Admin(**관리**)** 확인란을 선택합니다.
- 브라우저 및 Cisco ISE 웹 포털에 연결되는 REST 클라이언트에 사용됩니다. 이러한 인증서의 **Usage(**사용**)** 영역에서 **Portal(**포털**)** 확인란을 선택합니다.
- PEAP 및 EAP-FAST와 함께 외부 TLS 터널을 형성하는 데 사용됩니다. **Usage(**사용**)** 영역에서 EAP-TLS, PEAP 및 EAP-FAST와의 상호 인증을 위한 **EAP Authentication(EAP** 인증**)** 확인란을 선택합니다.
- RADIUS DTLS 서버 인증에 사용됩니다.
- SAML IdP(Identity Provider)와 통신하는 데 사용됩니다. 이러한 인증서의 **Usage(**사용**)** 영역에서 **SAML** 확인란을 선택합니다. SAML 옵션을 선택하는 경우 다른 서비스에 이 인증서를 사용할 수 없습니다.
- pxGrid 컨트롤러와의 통신에 사용됩니다. 이러한 인증서의 **Usage(**사용**)** 영역에서 **pxGrid** 확인란을 선택합니다.

Cisco ISE 구축의 각 노드에 유효한 시스템 인증서를 설치합니다. 기본적으로 설치 중에 Cisco ISE 노드에 자체 서명 인증서 2개와 내부 Cisco ISE CA에서 서명 1개가 생성됩니다.

- EAP, 관리자, 포털, RADIUS DTLS (키 크기는 2048이며 1년 동안 유효함)
- SAML IdP와의 통신을 보호하는 데 사용할 수 있는 자체 서명 SAML 서버 인증서(키 크기는 2048이며 1년 동안 유효함)
- pxGrid 클라이언트와의 통신을 보호하는 데 사용할 수 있는 내부 Cisco ISE CA 서명 서버 인증서(키 크기가 4096이고 1년 동안 유효함).

구축을 설정하고 보조 노드를 등록하면 pxGrid 컨트롤러용으로 지정된 인증서가 기본 노드의 CA에서 서명한 인증서로 자동 교체됩니다. 따라서 모든 pxGrid 인증서는 동일한 PKI 신뢰 계층 구조의 일부가 됩니다.

참고 가져온 와일드카드 시스템 인증서를 다른 노드(노드 간 통신을 위해)로 내보내는 경우 인증서 및 개인 키를 내보내고 암호화 비밀번호를 지정해야 합니다. 가져오는 동안 인증서, 개인 키 및 암호화 비밀번호가 필요합니다.

참고 릴리스에 대해 지원되는 키 및 암호 정보를 찾으려면 Cisco Identity Services Engine Network Component Compatibility의 해당 버전을 확인하십시오.

보안을 향상하기 위해 셀프 서명 인증서는 CA 서명 인증서로 대체하는 것이 좋습니다. CA 서명 인증서를 가져오려면 다음을 수행해야 합니다.

1. 인증서 서명 요청을 생성하고 인증 기관에 제출, 184 페이지
2. 신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 177 페이지
3. 인증서 서명 요청에 대한 CA 서명 인증서 바인딩, 185 페이지

ISE 커뮤니티 리소스

방법: ISE 서버 측 인증서 구현

Certificate Renewal on Cisco Identity Services Engine Configuration Guide

시스템 인증서 보기

System Certificate(시스템 인증서**)** 창에는 Cisco ISE에 추가된 모든 시스템 인증서가 나열됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다.

단계 **2** 다음 열이 **System Certificates(**시스템 인증서**)** 창에 표시됩니다.

- **Friendly Name(**식별 이름**)**: 인증서의 이름입니다.
- **Usage(**사용**)**: 이 인증서가 사용되는 서비스입니다.
- **Portal group tag(**포털 그룹 태그**)**: 포털에서 사용하도록 지정된 인증서에만 해당되며, 이 필드가 포털에 사용해야 하는 인증서를 지정합니다.
- **Issued To(**발급 대상**)**: 인증서 주체의 공용 이름입니다.
- **Issued By(**발급자**)**: 인증서 발급자의 공용 이름입니다.
- **Valid From(**유효 기간 시작**)**: 인증서가 생성된 날짜이며, "Not Before" 인증서 속성이라고도 합니다.
- **Valid To (Expiration)(**만료 날짜**)**: 인증서의 만료 날짜이며, "Not After" 인증서 속성이라고도 합니다. 만료 날짜 옆에 다음 아이콘이 표시됩니다.
  - 녹색 아이콘: 만료 날짜까지 남은 기간이 90일 이상입니다.
  - 파란색 아이콘: 90일 이내에 만료됩니다.
  - 노란색 아이콘: 60일 이내에 만료됩니다.

- 주황색 아이콘: 30일 이내에 만료됩니다.
- 빨간색 아이콘: 만료되었습니다.

시스템 인증서 가져오기

관리 포털에서 Cisco ISE 노드의 시스템 인증서를 가져올 수 있습니다.

참고 기본 PAN 노드에서 관리 역할 인증서의 인증서를 변경하면 다른 모든 노드에서 서비스가 재시작됩니다. 시스템은 기본 PAN이 재시작되고 나면 노드를 한 번에 한 개씩 재시작합니다.

시작하기 전에

- 클라이언트 브라우저를 실행 중인 시스템에 시스템 인증서 및 개인 키 파일이 있는지 확인합니다.
- 가져오는 시스템 인증서에 외부 CA가 서명을 한 경우 관련 루트 및 중간 CA 인증서를 신뢰할 수 있는 인증서 저장소(**Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**)로 가져옵니다.
- 가져오는 시스템 인증서에 CA 플래그가 true로 설정된 기본 제한 확장명이 포함되어 있으면 키 사용 확장이 있는지 확인하고, keyEncipherment 비트나 keyAgreement 중 하나 또는 두 비트가 모두 설정되어 있는지 확인합니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1**

단계 **2** **Import(**가져오기**)**를 클릭합니다.
Import Server Certificate(서버 인증서 가져오기**)** 창이 표시됩니다.

단계 **3** 가져올 인증서에 대한 값을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

시스템 인증서 가져오기 설정

다음 표에서는 서버 인증서를 가져오는 데 사용할 수 있는 **Import System Certificate(**시스템 인증서 가져오기**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**입니다. **Import(**가져오기**)**를 클릭합니다.

표 ***19:*** 시스템 인증서 가져오기 설정

필드 이름	설명
Select Node(노드 선택**)**	(필수) 드롭다운 목록에서 시스템 인증서를 가져올 Cisco ISE 노드를 선택합니다.
Certificate File(인증서 파일**)**	(필수) **Choose File(**파일 선택**)**을 클릭하고 로컬 시스템에서 인증서 파일을 선택합니다.
Private Key File(개인 키 파일**)**	(필수) **Choose File(**파일 선택**)**을 클릭하고 로컬 시스템에서 개인 키 파일을 선택합니다.
Password(비밀번호**)**	(필수) 개인 키 파일의 암호를 해독하기 위한 비밀번호를 입력합니다.
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다. 이름을 지정하지 않으면 Cisco ISE는 다음 형식으로 이름을 자동으로 생성합니다. <common name> # <issuer> # <nnnnn>에서 <nnnnn>은 고유한 5자리 숫자입니다.
Allow Wildcard Certificates(와일드카드 인증서 허용**)**	와일드카드 인증서를 가져오려면 이 확인란을 선택합니다. 와일드카드 인증서에서는 와일드카드 표기법(도메인 이름 앞에 별표와 기간)이 사용됩니다. 와일드카드 인증서는 조직의 여러 호스트에서 공유됩니다. 이 확인란을 선택하는 경우 Cisco ISE는 구축의 기타 모든 노드로 이 인증서를 가져옵니다.
Validate Certificate Extensions(인증서 확장명 검증**)**	Cisco ISE가 인증서 확장명을 검증하도록 지정하려면 이 확인란을 선택합니다. 이 확인란을 선택하는 경우 가져오는 인증서에 CA 플래그가 true로 설정된 기본 제한 확장명이 포함되어 있으면 키 사용 확장이 있는지 확인합니다. keyEncipherment 비트나 keyAgreement 비트 중 하나 또는 둘 모두 설정되어야 합니다.

필드 이름	설명
Usage(사용**)**	이 시스템 인증서를 사용할 서비스를 선택합니다. • **Admin(**관리**)**: 구축의 Cisco ISE 노드 간 통신 및 관리 포털과의 통신을 보호하는 데 사용되는 서버 인증서입니다. 참고 기본 PAN에서 관리자 역할 인증서의 인증서를 변경하면 다른 모든 Cisco ISE 노드에서 서비스가 재시작됩니다. • **EAP Authentication(EAP** 인증**)**: SSL 또는 TLS 터널링용 EAP 프로토콜을 사용하는 인증에 사용되는 서버 인증서입니다. • **RADIUS DTLS**: RADIUS DTLS 인증에 사용되는 서버 인증서입니다. • **pxGrid**: pxGrid 클라이언트와 서버 간의 통신을 보호하기 위한 클라이언트 및 서버 인증서입니다. • **ISE Messaging Service(ISE** 메시징 서비스**)**: 내장 UDP 시스템 로그 수집 대상(LogCollector 및 LogCollector2)에 대해 MnT WAN 지속성을 지원하는 **Syslog Over Cisco ISE Messaging(Cisco ISE** 메시징을 통한 시스템 로그**)**에서 사용됩니다. • **SAML**: SAML ID 제공자와의 통신을 보호하는 데 사용되는 서버 인증서입니다. SAML에 사용하도록 지정된 인증서는 관리, EAP 인증 등의 기타 서비스에는 사용할 수 없습니다. • **Portal(**포털**)**: 모든 Cisco ISE 웹 포털과의 통신을 보호하는 데 사용되는 서버 인증서입니다.

관련 항목

시스템 인증서, 159 페이지
시스템 인증서 보기, 160 페이지
시스템 인증서 가져오기, 161 페이지

셀프 서명 인증서 생성

SSC(자가서명 인증서)를 생성하여 새 로컬 인증서를 추가할 수 있습니다. Cisco에서는 내부 테스트 및 평가에 필요한 SSC(자가서명 인증서)만 사용하기를 권장합니다. 생산 환경에서 Cisco ISE를 구축하려는 경우에는 생산 네트워크 전체에서 보다 균일하게 수락될 수 있도록 가능하면 항상 CA 서명 인증서를 사용하십시오.

참고 SSC(자가서명 인증서)를 사용 중일 때 Cisco ISE 노드의 호스트 이름을 변경해야 하는 경우에는 Cisco ISE 노드의 관리 포털에 로그인하여 이전 호스트 이름이 지정된 SSC(자가서명 인증서)를 삭제한 다음 새 SSC(자가서명 인증서)를 생성해야 합니다. 이렇게 하지 않으면 Cisco ISE는 이전 호스트 이름이 지정된 SSC(자가서명 인증서)를 계속 사용합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

셀프 서명 인증서 설정

다음 표에서는 셀프 서명 인증서 생성 창의 필드에 대해 설명합니다. 이 창에서는 노드 간 통신, EAP-TLS 인증, Cisco ISE 웹 포털용 시스템 인증서를 생성하고 pxGrid 컨트롤러와 통신할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**입니다. 셀프 서명 인증서 생성을 클릭합니다.

표 ***20:*** 셀프 서명 인증서 설정

필드 이름	사용 지침
Select Node(노드 선택**)**	(필수) 시스템 인증서를 생성할 노드입니다.
Common Name(공통 이름**) (CN)**	(SAN을 지정하지 않는 경우 필수) 기본적으로 일반 이름은 셀프 서명 인증서를 생성하는 Cisco ISE 노드의 FQDN입니다.
Organizational Unit(OU)(조직 단위**)**	조직 단위의 이름입니다. Engineering 등을 예로 들 수 있습니다.
Organization(O)(조직**)**	조직의 이름입니다. Cisco 등을 예로 들 수 있습니다.
City (L)(L(구/군/시**))**	(약어로 표기하지 않음) 구/군/시의 이름입니다. San Jose 등을 예로 들 수 있습니다.
State(ST)(시/도**)**	(약어로 표기하지 않음) 시/도의 이름입니다. California 등을 예로 들 수 있습니다.
Country(C)(국가**)**	국가의 이름입니다. 2자리 ISO 국가 코드를 입력해야 합니다. US 등을 예로 들 수 있습니다.
SAN(Subject Alternative Name)	인증서와 연결된 IP 주소, DNS 이름 또는 URI(Uniform Resource Identifier)
Key Type(키 유형**)**	공개 키(RSA 또는 ECDSA)를 생성하는 데 사용할 알고리즘입니다.

필드 이름	사용 지침
Key Length(키 길이**)**	공개 키의 비트 크기입니다. RSA를 위한 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • 512 • 1024 • 2048 • 4096 ECDSA를 위한 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • 256 • 384 참고 RSA 및 ECDSA 공개 키는 동일한 보안 레벨에서 키 길이가 다를 수 있습니다. 공용 CA 서명 인증서를 가져오거나 FIPS 호환 정책 관리 시스템으로 Cisco ISE를 구축하려면 2048을 선택합니다.
Digest to Sign With(서명에 사용할 다이제스트**)**	드롭다운 목록에서 다음 해싱 알고리즘 중 하나를 선택합니다. • SHA-1 • SHA-256
인증서 정책	인증서가 준수해야 하는 인증서 정책 OID 또는 OID 목록을 입력합니다. 쉼표나 공백을 사용하여 OID를 구분합니다.
Expiration TTL(만료 **TTL)**	인증서가 만료될 때까지의 기간(일)을 지정합니다. 드롭다운 목록에서 필요한 값을 선택합니다.
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다. 이름을 지정하지 않으면 Cisco ISE가 <common name> # <issuer> # <nnnnn> 형식으로 이름을 자동 생성합니다. 여기서 <nnnnn>은 고유한 5자리 숫자입니다.
Allow Wildcard Certificates(와일드카드 인증서 허용**)**	셀프 서명 와일드카드 인증서를 생성하려면 이 확인란을 선택합니다. 와일드카드 인증서는 와일드카드 표기법(별표 및 도메인 이름 앞의 마침표)을 사용하므로 조직의 여러 호스트 간에 인증서를 공유할 수 있습니다.

필드 이름	사용 지침
Usage(사용)	이 시스템 인증서를 사용할 서비스를 선택합니다. • **Admin(관리)**: 구축의 Cisco ISE 노드 간 통신 및 관리 포털과의 통신을 보호하는 데 사용되는 서버 인증서입니다. • **EAP Authentication(EAP 인증)**: SSL 또는 TLS 터널링용 EAP 프로토콜을 사용하는 인증에 사용되는 서버 인증서입니다. • **RADIUS DTLS**: RADIUS DTLS 인증에 사용되는 서버 인증서입니다. • **pxGrid**: pxGrid 클라이언트와 서버 간의 통신을 보호하기 위한 클라이언트 및 서버 인증서입니다. • **SAML**: SAML ID 제공자와의 통신을 보호하는 데 사용되는 서버 인증서입니다. SAML에 사용하도록 지정된 인증서는 관리, EAP 인증 등의 기타 서비스에는 사용할 수 없습니다. • **Portal(포털)**: 모든 Cisco ISE 웹 포털과의 통신을 보호하는 데 사용되는 서버 인증서입니다.

관련 항목

시스템 인증서, 159 페이지
시스템 인증서 보기, 160 페이지
셀프 서명 인증서 생성, 163 페이지

시스템 인증서 편집

이 창을 사용하여 시스템 인증서를 편집하고 셀프 서명 인증서를 갱신할 수 있습니다. 와일드카드 인증서를 편집하면 변경사항이 구축의 모든 노드로 복제됩니다. 와일드카드 인증서를 삭제하면 구축의 모든 노드에서 해당 와일드카드 인증서가 제거됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** 선택Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Certificates(인증서)** > **System Certificates(시스템 인증서)**를 선택합니다.

단계 **2** 편집할 인증서 옆의 확인란을 선택하고 **Edit(편집)**를 클릭합니다.

단계 **3** 셀프 서명 인증서를 갱신하려면 **Renewal Period(갱신 기간)** 확인란을 선택하고 만료 TTL(Time to Live)를 일, 주, 월 또는 연도 단위로 입력합니다. 드롭다운 목록에서 필요한 값을 를 선택합니다.

단계 **4** **Save(저장)**를 클릭합니다.

Admin(관리**)** 확인란을 선택하면 Cisco ISE 노드의 애플리케이션 서버가 다시 시작됩니다. 또한 Cisco ISE 노드가 구축의 PAN인 경우에는 구축 내 기타 모든 노드의 애플리케이션 서버도 다시 시작됩니다. 시스템은 기본 PAN이 재시작되고 나면 노드를 한 번에 한 개씩 재시작합니다.

참고 Chrome 65 이상을 사용하여 Cisco ISE를 시작하면 URL이 성공적으로 리디렉션되어도 브라우저에서 BYOD 포털 또는 게스트 포털이 시작되지 않을 수 있습니다. 이는 모든 인증서에 주체 대체 이름 필드를 요구하는 Google의 새로운 보안 기능 때문입니다. Cisco ISE 릴리스 2.4 이상의 경우 Subject Alternative Name(주체 대체 이름) 필드를 입력해야 합니다.

Chrome 65 이상에서 실행하려면 다음 단계를 수행합니다.

1. Subject Alternative Name(주체 대체 이름) 필드를 입력해 Cisco ISE GUI에서 새 자체 서명 인증서를 생성합니다. DNS 및 IP 주소를 모두 입력해야 합니다.

2. Cisco ISE 서비스가 다시 시작됩니다.

3. Chrome 브라우저에서 포털을 리디렉션합니다.

4. 브라우저에서 View Certificate(인증서보기)>Details(세부정보)>Copy the certificate by selecting base-64 encoded(base-64 인코딩을 선택하여 인증서 복사)를 실행합니다.

5. 신뢰할 수 있는 경로에 인증서를 설치합니다.

6. Chrome 브라우저를 닫고 포털 리디렉션을 시도합니다.

참고 운영체제 Win RS4 또는 RS5에서 브라우저 Firefox 64 이상 릴리스에 대해 무선 BYOD 설정을 구성할 때 인증서 예외를 추가하지 못할 수 있습니다. 이 동작은 Firefox 64 이상 릴리스를 새로 설치하는 경우에 예상되며, 이전 버전에서 Firefox 64 이상으로 업그레이드하는 경우에는 발생하지 않습니다. 이 경우 다음과 같은 단계를 통해 인증서 예외를 추가할 수 있습니다.

1. BYOD 플로우 단일 또는 이중 PEAP 또는 TLS를 구성합니다.
2. Windows ALL 옵션을 사용해 CP 정책을 구성합니다.
3. 엔드 클라이언트 Windows RS4 또는 Windows RS5에서 Dot1.x 또는 MAB SSID를 연결합니다.
4. 게스트 또는 BYOD 포털로의 리디렉션을 위해 FF64 브라우저에 1.1.1.1을 입력합니다.
5. **Add Exception(**예외 추가**)** > **Unable to add certificate(**인증서 추가 불가능**)**을 클릭한 다음 플로우를 진행합니다.

이를 해결하는 방법으로, Firefox 64용 인증서를 수동으로 추가합니다. Firefox 64 브라우저에서 **Options(**옵션**)** > **Privacy & Settings(**개인 정보 및 설정**)** > **View Certificates(**인증서 보기**)** > **Servers(**서버**)** > **Add Exception(**예외 추가**)**을 선택합니다.

시스템 인증서 삭제

더 이상 사용하지 않는 시스템 인증서는 삭제할 수 있습니다.

시스템 인증서 저장소에서 한 번에 여러 인증서를 삭제할 수는 있지만, 이 경우 관리 및 EAP 인증에 사용할 수 있는 인증서가 하나 이상 있어야 합니다. 또한 관리, EAP 인증, 포털 또는 pxGrid 컨트롤러에 사용되는 인증서는 삭제할 수 없습니다. 단, 서비스를 비활성화하는 경우 pxGrid 인증서는 삭제할 수 있습니다.

와일드카드 인증서를 삭제하도록 선택하는 경우에는 구축의 모든 Cisco ISE 노드에서 인증서가 제거됩니다.

단계 **1** 선택Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다.

단계 **2** 삭제할 인증서 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

경고 메시지가 표시됩니다.

단계 **3** **Yes(**예**)**를 클릭하여 인증서를 삭제합니다.

시스템 인증서 내보내기

시스템 인증서 또는 인증서와 그 연결된 개인 키를 내보낼 수 있습니다. 인증서 및 해당 개인 키를 백업용으로 내보내는 경우 나중에 필요하면 인증서와 키를 다시 가져올 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** 선택Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **3** 인증서만 내보낼지 아니면 인증서 및 연결된 개인 키를 내보낼지를 선택합니다.

팁 인증서와 연결된 개인 키의 값이 노출될 수 있으므로 개인 키는 내보내지 않는 것이 좋습니다. 노드 간 통신용으로 와일드카드 시스템 인증서를 다른 Cisco ISE 노드로 가져오기 위해 내보내는 등의 경우와 같이 개인 키를 내보내야 하는 경우에는 개인 키용 암호화 비밀번호를 지정합니다. 개인 키의 암호를 해독하려면 이 인증서를 다른 Cisco ISE 노드로 가져오는 동안 이 비밀번호를 지정해야 합니다.

단계 **4** 개인 키를 내보내도록 선택한 경우 비밀번호를 입력합니다. 비밀번호는 8자 이상이어야 합니다.

단계 **5** **Export(**내보내기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 파일 시스템에 인증서를 저장합니다.

인증서만 내보내는 경우에는 PEM 형식으로 인증서가 저장됩니다. 인증서와 개인 키를 모두 내보내는 경우에는 PEM 형식 인증서와 암호화된 개인 키 파일을 포함하는 .zip 파일로 인증서가 내보내집니다.

신뢰할 수 있는 인증서 저장소

신뢰할 수 있는 인증서 저장소에는 신뢰 및 SCEP(Simple Certificate Enrollment Protocol)에 사용되는 X.509 인증서가 포함되어 있습니다.

신뢰할 수 있는 인증서 저장소의 인증서는 기본 PAN에서 관리되고 Cisco ISE 구축의 각 노드에 복제됩니다. Cisco ISE는 와일드카드 인증서를 지원합니다.

Cisco ISE는 다음과 같은 용도로 신뢰할 수 있는 인증서를 사용합니다.

- 인증서 기반 관리자 인증을 사용하여 ISE-PIC관리 포털에 액세스하는 Cisco ISE 관리자 및 엔드포인트에서 인증을 위해 사용하는 클라이언트 인증서 확인
- 구축에 있는 Cisco ISE 노드 간의 통신 보호 활성화. 신뢰할 수 있는 인증서 저장소는 구축의 각 노드에 있는 시스템 인증서와의 신뢰 관계를 설정하는 데 필요한 CA 인증서 체인을 포함해야 합니다.
  - 셀프 서명 인증서는 시스템 인증서에 사용되고 각 노드의 셀프 서명 인증서는 PAN의 신뢰할 수 있는 인증서 저장소에 위치해야 합니다.
  - CA 서명 인증서가 시스템 인증서로 사용되는 경우 CA 루트 인증서와 함께 신뢰 체인의 중간 인증서는 PAN의 신뢰할 수 있는 인증서 저장소에 위치해야 합니다.
- 보안 LDAP 인증을 활성화하려면 SSL을 통해 액세스하는 LDAP ID 소스를 정의할 때는 인증서 저장소의 인증서를 선택해야 합니다.
- 개인 디바이스 포털을 사용하여 네트워크에 등록할 수 있도록 개인 디바이스에 배포. Cisco ISE는 개인 디바이스 등록을 지원하기 위해 PSN에 SCEP를 구현합니다. 등록 디바이스는 SCEP 프로토콜을 사용하여 PSN에서 클라이언트 인증서를 요청할 수 있습니다. PSN에는 중개자 역할을 하는 RA(Registration Authority)가 포함되어 있습니다. RA는 등록 디바이스로부터 요청을 받고 검증한 다음 요청을 외부 CA 또는 내부 Cisco ISE CA로 전달하는데, 이 CA에서 클라이언트 인증서를 발급합니다. CA는 인증서를 다시 RA로 보내고 RA에서 디바이스로 인증서를 반환합니다.

  Cisco ISE에 사용되는 각 SCEP CA는 SCEP RA 프로파일로 정의됩니다. SCEP RA 프로파일이 생성되면 다음 두 개의 인증서가 자동으로 신뢰할 수 있는 인증서 저장소에 추가됩니다.

  - CA 인증서(셀프 서명 인증서)
  - CA가 서명한 RA 인증서(인증서 요청 에이전트 인증서)

  SCEP 프로토콜 요건에 따라 RA에서 이러한 두 인증서를 등록 디바이스에 제공해야 합니다. 신뢰할 수 있는 인증서 저장소에서 이러한 두 인증서를 대체하면 해당 노드의 RA에 사용되도록 인증서가 모든 PSN 노드로 복제됩니다.

참고 SCEP RA 프로파일이 제거되면 연결된 CA 체인도 신뢰할 수 있는 인증서 저장소에서 제거됩니다. 그러나 보안 시스템 로그, LDAP, 시스템 또는 신뢰 인증서에서 동일한 인증서를 참조하는 경우 SCEP 프로파일만 삭제됩니다.

참고

- Cisco ISE로 가져온 X.509 인증서는 PEM(Privacy-Enhanced Mail) 또는 DER(Distinguished Encoding Rule) 형식이어야 합니다. 인증서 체인, 시스템 인증서와 여기에 서명하는 신뢰 인증서 시퀀스를 포함하는 파일은 특정 제한 사항에 따라 가져올 수 있습니다.
- 공개 와일드카드 인증서를 게스트 포털에 할당하고 루트 CA 인증서가 포함된 하위 CA를 가져오는 경우 Cisco ISE 서비스가 재시작될 때까지 인증서 체인이 전송되지 않습니다.

ISE 커뮤니티 리소스

ISE 2.0에 타사 CA 인증서 설치

신뢰할 수 있는 인증서 저장소의 인증서

신뢰할 수 있는 인증서 저장소는 신뢰할 수 있는 인증서, 즉 Manufacturing 인증서, 루트 인증서, 및 다른 신뢰할 수 있는 인증서로 미리 채워져 있습니다. 루트 인증서(Cisco 루트 CA)는 Manufacturing (Cisco CA Manufacturing) 인증서에 서명합니다. 이 인증서는 기본적으로 비활성화되어 있습니다. 구축에서 Cisco IP Phone을 엔드포인트로 사용하는 경우 이러한 두 인증서를 활성화해야 IP Phone에 대한 Cisco 서명 클라이언트 인증서를 인증할 수 있습니다.

신뢰할 수 있는 인증서 목록

다음 표에서는 관리 노드에 추가된 신뢰할 수 있는 인증서 목록이 표시되는 **Trusted Certificates(**신뢰할 수 있는 인증서**)** 창의 열에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**입니다.

표 ***21:*** 신뢰할 수 있는 인증서 창의 열

필드 이름	사용 지침
Friendly Name(식별 이름**)**	인증서의 이름을 표시합니다.
Status(상태**)**	이 열에는 **Enabled(**활성화됨**)** 또는 **Disabled(**비활성화됨**)**가 표시됩니다. 인증서가 비활성화되면 Cisco ISE가 신뢰를 설정하는 데 인증서를 사용하지 않습니다.
Trusted for(신뢰 대상**)**	인증서를 사용하는 다음 서비스를 하나 이상 표시합니다. • **Infrastructure(**인프라**)** • **Cisco Services(**시스코 서비스**)** • **Endpoints(**엔드포인트**)**

필드 이름	사용 지침
Issued To(발급 대상**)**	인증서 주체의 CN(Common Name)을 표시합니다.
Issued By(발급자**)**	인증서 발급자의 CN(Common Name)을 표시합니다.
Valid From(유효 기간 시작**)**	인증서가 발급된 날짜와 시간을 표시합니다. 이 값은 "Not Before" 인증서 속성이라고도 합니다.
Expiration Date(만료일**)**	인증서가 만료되는 날짜와 시간을 표시합니다. 이 값은 "Not After" 인증서 속성이라고도 합니다.
Expiration Status(만료 상태**)**	인증서 만료의 상태에 대한 정보를 제공합니다. 이 열에는 정보 메시지의 범주와 5개 아이콘이 표시됩니다. • 녹색: 만료일까지 남은 기간이 90일 이상입니다. • 파란색: 90일 이내에 만료됩니다. • 노란색: 60일 이내에 만료됩니다. • 주황색: 30일 이내에 만료됩니다. • 빨간색: 만료되었습니다.

관련 항목

신뢰할 수 있는 인증서 저장소, 169 페이지
신뢰할 수 있는 인증서 보기, 172 페이지
신뢰할 수 있는 인증서 저장소의 상태 변경, 173 페이지
신뢰할 수 있는 인증서 저장소에 인증서 추가, 173 페이지

신뢰할 수 있는 인증서 명명 제한

CTL의 신뢰할 수 있는 인증서는 이름 제한 확장명을 포함할 수 있습니다. 이 확장명은 인증서 체인 내 후속 인증서의 모든 주체 이름 및 대체 주체 이름 필드 값에 대한 네임스페이스를 정의합니다. Cisco ISE는 루트 인증서에 지정된 제한을 확인하지 않습니다.

Cisco ISE에서 지원되는 이름 제한은 다음과 같습니다.

- 디렉토리 이름

  Subject(주체) 또는 Subject Alternative Name(대체 주체 이름) 필드에서 디렉토리 이름 접두사를 디렉토리 이름 제한으로 사용해야 합니다. 예를 들면 다음과 같습니다.

  - 올바른 주체 접두사:

    CA 인증서 이름 제한: Permitted: O=Cisco

    클라이언트 인증서 주체: O=Cisco,CN=Salomon

- 잘못된 주체 접두사:

  CA 인증서 이름 제한: Permitted: O=Cisco

  클라이언트 인증서 주체: CN=Salomon,O=Cisco

- DNS
- 이메일
- URI(URI 제한은 http://, https://, ftp:// 또는 ldap://와 같은 URI 접두사로 시작되어야 함)

Cisco ISE는 다음 이름 제약 조건을 지원하지 않습니다.

- IP 주소
- 기타 이름

신뢰할 수 있는 인증서에 지원되지 않는 제약 조건이 있고 확인 중인 인증서에 적절한 필드가 없는 경우 Cisco ISE는 지원되지 않는 제약 조건을 확인할 수 없으므로 인증서를 거부합니다.

신뢰할 수 있는 인증서 내의 이름 제한 정의 예제는 다음과 같습니다.

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.abcde.at
                  email:.abcde.be
                  email:.abcde.bg
                  email:.abcde.by
                  DNS:.dir
                  DirName: DC = dir, DC = emea
                  DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
                  DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
                  DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
                  DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100
                  URI:.dir
                  IP:172.23.0.171/255.255.255.255
                Excluded:
                  DNS:.dir
                  URI:.dir
```

위의 정의와 일치하는 허용되는 클라이언트 인증서 주체는 다음과 같습니다.

```
           Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

신뢰할 수 있는 인증서 보기

Trusted Certificates(신뢰할 수 있는 인증서**)** 창에는 Cisco ISE에서 사용 가능한 신뢰할 수 있는 인증서가 모두 나열됩니다. 신뢰할 수 있는 인증서를 보려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** 모든 인증서를 보려면 메뉴 아이콘(☰)을 클릭합니다. 그런 다음**Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다. Trusted Certificates(신뢰할 수 있는 인증서) 창이 표시되고 신뢰할 수 있는 인증서가 모두 나열됩니다.

단계 **2** 신뢰할 수 있는 인증서의 확인란을 선택하고 **Edit(**편집**)**, **View(**보기**)**, **Export(**내보내기**)** 또는 **Delete(**삭제**)**를 클릭하여 필요한 작업을 수행합니다.

신뢰할 수 있는 인증서 저장소의 상태 변경

Cisco ISE가 신뢰를 설정하는 데 인증서를 사용할 수 있도록 인증서의 상태를 활성화해야 합니다. 인증서는 신뢰할 수 있는 인증서 저장소로 가져올 때 자동으로 활성화됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **3** 활성화하거나 비활성화할 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **Status(**상태**)** 드롭다운 목록에서 상태를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

신뢰할 수 있는 인증서 저장소에 인증서 추가

신뢰할 수 있는 인증서 저장소 창에서 Cisco ISE에 CA 인증서를 추가할 수 있습니다.

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- 브라우저를 실행 중인 컴퓨터의 파일 시스템에 추가하고자 하는 인증서가 있어야 합니다. 인증서는 PEM 또는 DER 형식이어야 합니다.
- 관리자 또는 EAP 인증용으로 인증서를 사용하려는 경우 인증서에 기본 제한을 정의하고 CA 플래그를 true로 설정합니다.

신뢰할 수 있는 인증서 편집

신뢰할 수 있는 인증서 저장소에 추가한 인증서는 **Edit(**편집**)** 옵션을 사용하여 추가로 편집할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** 선택Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2** 편집할 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** (선택 사항) **Friendly Name(**식별 이름**)** 필드에 인증서의 이름을 입력합니다. 식별 이름을 지정하지 않으면 기본 이름이 다음 형식으로 생성됩니다.

common-name#issuer#nnnnn

단계 **4** **Trusted For(**신뢰 대상**)** 영역에서 필요한 확인란을 선택하여 인증서 사용을 정의합니다.

단계 **5** (선택 사항) **Description(**설명**)** 필드에 인증서 설명을 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

신뢰할 수 있는 인증서 설정

다음 표에서는 신뢰할 수 있는 인증서의 **Edit(**편집**)** 창에 있는 필드에 대해 설명합니다. 이 창에서 CA 인증서 속성을 편집합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**입니다. 편집할 신뢰할 수 있는 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

표 ***22:*** 신뢰할 수 있는 인증서 편집 설정

필드 이름	사용 지침
인증서 발급자	
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다. 선택적 필드로, 식별 이름을 입력하지 않으면 기본 이름이 다음 형식으로 생성됩니다. *common-name # issuer # nnnnn*
Status(상태**)**	드롭다운 목록에서 **Enabled(**활성화됨**)** 또는 **Disabled(**비활성화됨**)**를 선택합니다. 인증서가 비활성화되면 Cisco ISE가 신뢰를 설정하는 데 인증서를 사용하지 않습니다.
Description(설명**)**	(선택 사항) 설명을 입력합니다.
사용	
Trust for authentication within ISE(ISE 내의 인증 신뢰**)**	이 인증서가 다른 Cisco ISE 노드 또는 LDAP 서버의 서버 인증서를 확인하도록 하려면 이 확인란을 선택합니다.

필드 이름	사용 지침
Trust for client authentication and Syslog(클라이언트 인증 및 시스템 로그 신뢰**)**	(Trust for authentication within **ISE**(ISE 내의 인증 신뢰) 확인란을 선택하는 경우에만 해당함) 다음 용도로 이 인증서를 사용하려는 경우 확인란을 선택합니다. • EAP 프로토콜을 사용하여 Cisco ISE에 연결하는 엔드포인트 인증 • 시스템 로그 서버 신뢰
Trust for authentication of Cisco Services(Cisco 서비스의 인증 신뢰**)**	피드 서비스와 같은 외부 Cisco 서비스를 신뢰하는 데 이 인증서를 사용하려는 경우 이 확인란을 선택합니다.
Certificate Status Validation(인증서 상태 검증**)**	Cisco ISE는 특정 CA가 발급한 클라이언트 또는 서버 인증서의 취소 상태를 확인하는 두 가지 방법을 지원합니다. 첫 번째 방법은 OCSP(Online Certificate Status Protocol)를 사용하여 인증서를 검증하는 것입니다. 이 경우 CA가 유지 관리하는 OCSP 서비스에 요청을 하게 됩니다. 두 번째 방법은 CA에서 Cisco ISE로 다운로드할 수 있는 CRL과 대조하여 인증서를 검증하는 것입니다. 이 두 방법은 모두 활성화할 수 있으며 이 경우 OCSP가 먼저 사용됩니다. 상태를 확인할 수 없는 경우에만 CRL이 사용됩니다.
Validate Against OCSP Service(OCSP 서비스와 대조하여 검증**)**	OCSP 서비스와 대조하여 인증서를 검증하려면 확인란을 선택합니다. 먼저 OCSP 서비스를 생성해야 이 확인란을 선택할 수 있습니다.
Reject the request if OCSP returns UNKNOWN status(OCSP에서 **UNKNOWN** 상태를 반환하는 경우 요청 거부**)**	OCSP 서비스에서 인증서 상태를 확인할 수 없는 경우 요청을 거부하려면 확인란을 선택합니다. 이 확인란을 선택하면 OCSP 서비스에서 알 수 없는 상태 값을 반환하는 경우 Cisco ISE가 현재 평가 중인 클라이언트 또는 서버 인증서를 거부합니다.
Reject the request if OCSP Responder is unreachable(OCSP 응답자에 연결할 수 없는 경우 요청 거부**)**	OCSP 응답자에 연결할 수 없는 경우 Cisco ISE가 요청을 거부하도록 하려면 이 확인란을 선택합니다.
Download CRL(CRL 다운로드**)**	Cisco ISE가 CRL을 다운로드하도록 하려면 확인란을 선택합니다.

필드 이름	사용 지침
CRL Distribution URL(CRL 배포 **URL)**	CA에서 CRL를 다운로드할 URL을 입력합니다. 인증 기관 인증서에 URL이 지정되어 있으면 이 필드는 자동으로 채워집니다. URL은 " http", "https" 또는 "ldap"로 시작해야 합니다.
Retrieve CRL(CRL 검색**)**	CRL은 자동으로 다운로드할 수도 있고 정기적으로 다운로드할 수도 있습니다. 이 필드에서 다운로드 간의 시간 간격을 구성합니다.
If download failed, wait(다운로드 실패 시 대기**)**	Cisco ISE가 다시 CRL 다운로드를 시도할 때까지 대기할 시간 간격을 구성합니다.
Bypass CRL Verification if CRL is not Received(CRL이 수신되지 않으면 **CRL** 확인 바이패스**)**	CRL이 수신되기 전에 클라이언트 요청을 수락하려면 이 확인란을 선택합니다. 이 확인란의 선택을 취소하면 선택한 CA가 서명을 한 인증서를 사용하는 모든 클라이언트 요청은 Cisco ISE가 CRL 파일을 받을 때까지 거부됩니다.
Ignore that CRL is not yet valid or expired(CRL 이 아직 유효하지 않거나 만료된 경우 시작일/만료 날짜 무시**)**	Cisco ISE가 시작일과 만료 날짜를 무시하고 아직 활성화되지 않았거나 만료된 CRL을 계속 사용하도록 하고, CRL의 내용에 따라 EAP-TLS 인증을 허용하거나 거부하도록 하려면 이 확인란을 선택합니다. Cisco ISE가 CRL 파일에서 Effective Date(유효 날짜) 필드의 시작일과 Next Update(다음 업데이트) 필드의 만료 날짜를 확인하도록 하려면 이 확인란의 선택을 취소합니다. CRL이 아직 활성화되지 않았거나 만료된 경우에는 이 CA가 서명을 한 인증서를 사용하는 모든 인증은 거부됩니다.

관련 항목

신뢰할 수 있는 인증서 저장소, 169 페이지
신뢰할 수 있는 인증서 편집, 173 페이지

신뢰할 수 있는 인증서 삭제

더 이상 필요하지 않은 신뢰할 수 있는 인증서는 삭제할 수 있습니다. 그러나 Cisco ISE 내부 CA 인증서를 삭제해서는 안 됩니다. Cisco ISE 내부 CA 인증서는 전체 구축에 대해 Cisco ISE 루트 인증서 체인을 교체할 때만 삭제할 수 있습니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2** 삭제할 인증서 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

경고 메시지가 표시됩니다. Cisco ISE 내부 CA 인증서를 삭제하려면 다음 옵션 중 하나를 클릭합니다.

- **Delete(**삭제**)**: Cisco ISE 내부 CA 인증서를 삭제합니다. 이 경우 Cisco ISE 내부 CA가 서명한 모든 엔드포인트 인증서는 무효화되며 엔드포인트가 네트워크에 가입할 수 없게 됩니다. 엔드포인트가 네트워크에 다시 가입할 수 있게 하려면 신뢰할 수 있는 인증서 저장소에 동일한 Cisco ISE 내부 CA 인증서를 가져옵니다.
- **Delete & Revoke(**삭제 및 취소**)**: Cisco ISE 내부 CA 인증서를 삭제 및 취소합니다. 이 경우 Cisco ISE 내부 CA가 서명한 모든 엔드포인트 인증서는 무효화되며 엔드포인트가 네트워크에 연결할 수 없게 됩니다. 이 작업은 취소할 수 없으며, 전체 구축에 대해 Cisco ISE 루트 인증서 체인을 교체해야 합니다.

단계 **3** **Yes(**예**)**를 클릭하여 인증서를 삭제합니다.

신뢰할 수 있는 인증서 저장소에서 인증서 내보내기

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

참고 내부 CA에서 인증서를 내보내는 경우 해당 내보내기를 사용하여 백업에서 복원하려는 경우 CLI 명령 `application configure ise`를 사용해야 합니다. Cisco ISE CA 인증서 및 키 내보내기, 214 페이지의 내용을 참조하십시오.

단계 **1** 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2**

단계 **3** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다. 인증서는 한 번에 하나씩만 내보낼 수 있습니다.

단계 **4** 선택한 인증서가 PEM 형식으로 클라이언트 브라우저를 실행중인 파일 시스템에 다운로드됩니다.

신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기

루트 CA 및 중간 CA 인증서를 가져오는 동안 신뢰할 수 있는 CA 인증서를 사용할 서비스를 지정할 수 있습니다.

시작하기 전에

인증서 서명 요청에 서명하고 디지털 서명 CA 인증서를 반환한 CA의 루트 인증서와 기타 중간 인증서가 있어야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2**

단계 **3** **Import(**가져오기**)**를 클릭합니다.

단계 **4** 표시되는 **Import a new Certificate into the Certificate Store(**인증서 저장소에 새 인증서 가져오기**)** 창에서 **Choose File(**파일 선택**)**을 클릭하여 CA에서 서명하고 반환한 루트 CA 인증서를 선택합니다.

단계 **5** 식별 이름을 입력합니다.

식별 이름을 입력하지 않으면 Cisco ISE는 *common-name#issuer#nnnnn* 형식의 이름을 이 필드에 자동으로 채웁니다. 여기서 *nnnnn*은 고유한 번호입니다. 추후 인증서를 편집하여 식별 이름을 변경할 수 있습니다.

단계 **6** 이 신뢰할 수 있는 인증서를 사용할 서비스 옆의 확인란을 선택합니다.

단계 **7** (선택 사항) **Description(**설명**)** 필드에 인증서 설명을 입력합니다.

단계 **8** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

해당하는 경우 신뢰할 수 있는 인증서 저장소로 중간 CA 인증서를 가져옵니다.

신뢰할 수 있는 인증서 가져오기 설정

다음 표에서는 Cisco ISE에 CA 인증서를 추가하는 데 사용할 수 있는 Trusted Certificate Import(신뢰할 수 있는 인증서 가져오기) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** > **Import(**가져오기**)** 입니다.

표 ***23:*** 신뢰할 수 있는 인증서 가져오기 설정

필드 이름	설명
Certificate File(인증서 파일**)**	브라우저를 실행 중인 컴퓨터에서 인증서 파일을 선택하려면 **Browse(**찾아보기**)**를 클릭합니다.
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다. 이름을 지정하지 않으면 Cisco ISE에서 <common name>#<issuer>#<nnnnn> 형식으로 이름을 자동 생성합니다. 여기서 <nnnnn>은 고유한 5자리 숫자입니다.
Trust for authentication within ISE(ISE 내의 인증 신뢰**)**	다른 ISE 노드 또는 LDAP 서버의 서버 인증서를 확인하는 데 이 인증서를 사용하려는 경우 확인란을 선택합니다.

필드 이름	설명
Trust for client authentication and Syslog(클라이언트 인증 및 시스템 로그 신뢰**)**	(Trust for authentication within ISE(ISE 내의 인증 신뢰) 확인란을 선택하는 경우에만 해당함) 다음 용도로 이 인증서를 사용하려는 경우 확인란을 선택합니다. • EAP 프로토콜을 사용하여 ISE에 연결하는 엔드포인트 인증 • 시스템 로그 서버 신뢰
Trust for authentication of Cisco Services(Cisco 서비스의 인증 신뢰**)**	피드 서비스와 같은 외부 Cisco 서비스를 신뢰하는 데 이 인증서를 사용하려는 경우 이 확인란을 선택합니다.
Validate Certificate Extensions(인증서 확장명 검증**)**	(Trust for client authentication(클라이언트 인증 신뢰) 및 Enable Validation of Certificate Extensions(인증서 확장명 검증 활성화) 옵션을 둘 다 선택하는 경우에만 해당함) "keyUsage" 확장명이 있고 "keyCertSign" 비트가 설정되어 있으며 CA 플래그가 true로 설정된 기본 제한 확장명이 있는지 확인합니다.
Description(설명**)**	필요에 따라 설명을 입력합니다.

관련 항목

신뢰할 수 있는 인증서 저장소, 169 페이지
인증서 체인 가져오기, 179 페이지
신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 177 페이지

인증서 체인 가져오기

인증서 저장소에서 수신한 인증서 체인이 들어 있는 단일 파일에서 여러 인증서를 가져올 수 있습니다. 파일의 모든 인증서는 PEM 형식이어야 하며, 인증서는 다음 순서로 정렬되어야 합니다.

- 파일의 마지막 인증서는 CA에서 발급된 클라이언트 또는 서버 인증서여야 합니다.
- 이전의 모든 인증서는 루트 CA 인증서이자 발급된 인증서의 서명 체인에 있는 중간 CA 인증서여야 합니다.

2단계 프로세스로 인증서 체인 가져오기:

1. Cisco ISE 관리 포털의 신뢰할 수 있는 인증서 저장소로 인증서 체인 파일을 가져옵니다. 이 작업은 마지막 인증서를 제외한 파일의 모든 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다.
2. CA 서명 인증서 바인딩 작업을 사용하여 인증서 체인 파일을 가져옵니다. 이 작업은 파일에서 마지막 인증서를 로컬 인증서로 가져옵니다.

Cisco ISE 노드 간 통신용으로 신뢰할 수 있는 인증서 설치

구축을 설정할 때는 보조 노드를 등록하기 전에 보조 노드의 관리 인증서를 검증하는 데 사용되는 적절한 CA 인증서를 PAN의 CTL에 입력해야 합니다. PAN의 CTL에 인증서를 입력하는 절차는 시나리오마다 다릅니다.

- 보조 노드가 CA 서명 인증서를 사용하여 Cisco ISE 관리 포털과 통신하는 경우 보조 노드의 CA 서명 인증서, 관련 중간 인증서(있는 경우) 및 보조 노드 인증서에 서명을 한 CA의 루트 CA 인증서를 PAN의 CTL로 가져와야 합니다.
- 보조 노드가 SSC(자가서명 인증서)를 사용하여 Cisco ISE 관리 포털과 통신하는 경우에는 보조 노드의 해당 인증서를 PAN의 CTL로 가져올 수 있습니다.

참고

- 등록된 보조 노드에서 관리 인증서를 변경하는 경우에는 보조 노드 관리 인증서를 검증하는 데 사용할 수 있는 적절한 CA 인증서를 얻은 다음 PAN의 CTL로 가져와야 합니다.
- 구축의 클라이언트와 PSN 간 통신을 보호하기 위해 SSC(자가서명 인증서)를 사용하는 경우 BYOD 사용자가 한 위치에서 다른 위치로 이동하면 EAP-TLS 사용자 인증이 실패합니다. 몇 개의 PSN 간에 서비스를 받아야 하는 인증 요청의 경우에는 외부에서 서명한 CA 인증서로 클라이언트와 PSN 간의 통신을 보호하거나 외부 CA가 서명한 와일드카드 인증서를 사용해야 합니다.

외부 CA가 발급한 인증서에 기본 제한이 정의되어 있으며 CA 플래그가 true로 설정되어 있는지 확인합니다. 노드 간 통신을 위해 CA 서명 인증서를 설치하려면 다음 단계를 수행합니다. 이러한 작업에 대한 자세한 내용은 *Cisco ISE* 관리자 가이드의 "기본 설정" 장을 참조하십시오.

단계 **1** CSR(Certificate Signing Request)을 생성하고 CSR을 인증 기관에 제출합니다.

단계 **2** 신뢰할 수 있는 인증서 저장소로 루트 인증서를 가져옵니다.

단계 **3** CSR에 CA 서명 인증서를 바인딩합니다.

Cisco ISE의 기본 신뢰할 수 있는 인증서

Cisco ISE의 신뢰할 수 있는 인증서 저장소(**Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**)에는 기본적으로 사용 가능한 일부 인증서가 포함되어 있습니다. 이러한 인증서는 보안 요구 사항을 충족하기 위해 저장소로 자동으로 가져옵니다. 그러나 이 모두를 사용해야 하는 것은 아닙니다. 아래 표에서 달리 언급되지 않는 한, 이미 사용 가능한 인증서 대신 원하는 인증서를 사용할 수 있습니다.

표 *24:*

신뢰할 수 있는 인증서 이름	**Serial Number**(일련 번호)	인증서의 목적	인증서가 포함된 **Cisco ISE** 릴리스
Baltimore CyberTrust Root CA	02 00 00 B9	이 인증서는 일부 지역에서 cisco.com이 사용하는 CA 체인의 루트 CA 인증서로 사용할 수 있습니다. 인증서는 https://s3.amazonaws.com에서 호스팅될 때 ISE 2.4 Posture / CP 업데이트 XML 파일에도 사용되었습니다.	릴리스 2.4 이상.
DST Root CA X3 Certificate Authority	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	이 인증서는 cisco.com에서 사용하는 CA 체인의 루트 CA 인증서 역할을 할 수 있습니다.	릴리스 2.4 이상.
Thawte Primary Root CA	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	이 인증서는 루트 CA 역할을 할 수 있습니다. cisco.com 및 perfigo.com에서 사용하는 CA 체인용 인증서입니다.	릴리스 2.4 이상.
VeriSign Class 3 Public Primary Certification Authority	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	이 인증서는 VeriSign Class 3 Secure Server CA-G3의 루트 CA 인증서 역할을 합니다. Cisco ISE에서 프로파일러 피드 서비스를 구성할 때 이 인증서를 사용해야 합니다.	릴리스 2.4 이상.
VeriSign Class 3 Secure Server CA - G3	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	이는 2020년 2월 7일에 만료되는 중간 CA 인증서입니다. 이 인증서는 갱신할 필요가 없습니다. 아래 작업에 따라 인증서를 제거 할 수 있습니다.	릴리스 2.4 이상.

신뢰할 수 있는 인증서 이름	**Serial Number**(일련 번호)	인증서의 목적	인증서가 포함된 **Cisco ISE** 릴리스
Cisco CA Manufacturing	6A 69 67 B3 00 00 00 00 00 03	이 인증서는 Cisco ISE에 연결하는 특정 Cisco 디바이스에서 사용할 수 있습니다. 이 인증서는 기본적으로 비활성화되어 있습니다.	릴리스 2.4 및 2.6.
Cisco Manufacturing CA SHA2	02	이 인증서는 CA 체인에서 관리자 인증, 엔드포인트 인증 및 구축 인프라 흐름에 사용할 수 있습니다.	릴리스 2.4 이상.
Cisco Root CA 2048	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	이 인증서는 Cisco ISE에 연결하는 특정 Cisco 디바이스에서 사용할 수 있습니다. 이 인증서는 기본적으로 비활성화되어 있습니다.	릴리스 2.4 이상.
Cisco Root CA M2	01	이 인증서는 CA 체인에서 관리자 인증, 엔드포인트 인증 및 구축 인프라 흐름에 사용할 수 있습니다.	릴리스 2.4 이상.
DigiCert Root CA	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	Facebook으로 게스트 로그인을 사용하는 플로우에 이 인증서를 사용해야 합니다.	릴리스 2.4 이상.
DigiCert SHA2 High Assurance Server CA	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	Facebook으로 게스트 로그인을 사용하는 플로우에 이 인증서를 사용해야 합니다.	릴리스 2.4 이상.
HydrantID SSL ICA G2	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	Cisco 서비스에 대해 신뢰됩니다.	릴리스 2.4 및 2.6.
QuoVadis Root CA 2	05 09	프로파일러, 포스처 및 클라이언트 프로비저닝 플로우에서 이 인증서를 사용해야 합니다.	릴리스 2.4 이상.

신뢰할 수 있는 인증서 이름	**Serial Number(**일련 번호**)**	인증서의 목적	인증서가 포함된 **Cisco ISE** 릴리스
Cisco ECC Root CA	01	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6.
Cisco Licensing Root CA	01	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상
Cisco Root CA 2099	01 9A 33 58 78 CE 16 C1 C1	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상
Cisco Root CA M1	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상
Cisco RXC-R2	01	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상
DigiCert Global Root CA	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상
Cisco ECC Root CA 2099	03	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상

Cisco ISE에서 신뢰할 수 있는 기본 인증서 제거

- Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.
- 필요한 경우 다시 가져올 수 있도록 삭제할 인증서를 내보내고 저장합니다.

  내보낼 인증서 확인란을 선택하고 위의 메뉴 모음에서 **Export(**내보내기**)**를 클릭합니다. 키 체인이 시스템에 다운로드됩니다.

- 인증서를 삭제합니다. 삭제할 인증서 확인란을 선택하고 위의 메뉴 모음에서 **Delete(**삭제**)**를 클릭합니다. CA 체인, 보안 시스템 로그 또는 보안 LDAP에서 인증서를 사용 중인 경우 해당 인증서를 삭제할 수 없습니다.
- CA 체인, 보안 시스템 로그 및 그 일부인 시스템 로그에서 인증서를 제거하기 위래 필요한 컨피그레이션을 변경합니다. 그런 다음 인증서를 삭제합니다.
- 인증서를 삭제한 후 관련 서비스(인증서의 목적 참조)가 정상적으로 작동하는지 확인합니다.

인증서 서명 요청

서명된 인증서를 발급하는 CA의 경우 인증서 서명 요청을 생성하고 CA에 제출해야 합니다.

생성한 인증서 서명 요청 목록은 **Certificate Signing Requests(**인증서 서명 요청**)** 창에서 확인할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다. CA에서 서명을 받으려면 인증서 서명 요청을 내보낸 다음, 인증서를 CA로 보내야 합니다. CA는 인증서에 서명하고 반환합니다.

Cisco ISE 관리 포털을 통해 중앙에서 인증서를 관리할 수 있습니다. 구축의 모든 노드에 사용할 인증서 서명 요청을 생성하고 내보낼 수 있습니다. 그런 다음 인증서 서명 요청을 CA에 제출하고, CA에서 CA 서명 인증서를 받고, CA에서 반환된 루트 및 중간 CA 인증서를 신뢰할 수 있는 인증서 저장소로 가져온 다음, CA 서명 인증서를 인증서 서명 요청에 바인딩해야 합니다.

인증서 서명 요청을 생성하고 인증 기관에 제출

CSR(Certificate Signing Request)을 생성하여 구축의 노드용으로 CA에서 서명한 인증서를 가져올 수 있습니다. 구축의 특정 노드 또는 구축의 모든 노드에 대해 CSR을 생성할 수 있습니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

단계 **2** **Generate Certificate Signing Requests(CSR)(**인증서 서명 요청 생성**)** 클릭하여 인증서 서명 요청을 생성합니다.

단계 **3** 인증서 서명 요청 생성에 대한 값 입력 표시된 창의 각 필드에 대한 자세한 내용은 인증서 서명 요청 설정을 참조하십시오.

단계 **4** 서명 요청 확인란을 선택하고 **Export(**내보내기**)**를 클릭하여 인증서 서명 요청을 다운로드합니다.

단계 **5** **"-----BEGIN CERTIFICATE REQUEST-----"**부터 **"-----END CERTIFICATE REQUEST-----"**까지의 모든 텍스트를 복사합니다."

단계 **6** CSR의 내용을 선택한 CA의 인증서 요청에 붙여 넣습니다.

단계 **7** 서명된 인증서를 다운로드합니다.

일부 CA의 경우 서명된 인증서를 이메일로 전송할 수 있습니다. 서명된 인증서는 zip 파일 형식이며 새로 발급된 인증서와 CA의 공개 서명 인증서가 들어 있습니다. 이러한 인증서를 Cisco ISE 신뢰할 수 있는 인증서 저장소에 추가

해야 합니다. 디지털 서명된 CA 인증서, 루트 CA 인증서 및 기타 중간 CA 인증서(해당하는 경우)가 클라이언트 브라우저를 실행 중인 로컬 시스템에 다운로드됩니다.

인증서 서명 요청에 대한 **CA** 서명 인증서 바인딩

CA가 디지털 서명된 인증서를 반환하고 나면 해당 인증서를 CSR(Certificate Signing Request)에 바인딩해야 합니다. 관리 포털에서 구축의 모든 노드에 대해 바인딩 작업을 수행할 수 있습니다.

시작하기 전에

- 디지털 서명된 인증서와 CA가 반환한 관련 루트 중간 CA 인증서가 있어야 합니다.
- 관련 루트 및 중간 CA 인증서를 신뢰할 수 있는 인증서 저장소(**Menu(**메뉴**)** 아이콘(☰) 클릭 후 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** 선택)로 가져옵니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

CA 서명 인증서에 바인딩해야 하는 인증서 서명 요청 옆의 확인란을 선택합니다.

단계 **2** **Bind Certificate(**인증서 바인딩**)**를 클릭합니다.

단계 **3** **Bind CA Signed Certificate(CA** 서명 인증서 바인딩**)** 창에서 **Choose File(**파일 선택**)**을 클릭하여 CA 서명 인증서를 선택합니다.

단계 **4** **Friendly Name(**식별 이름**)** 필드에 값을 입력합니다.

단계 **5** Cisco ISE가 인증서 확장명을 검증하도록 하려면 **Validation of Certificate Extensions(**인증서 확장명 검증**)** 확인란을 선택합니다.

Validation of Certificate Extensions(인증서 확장명 검증**)** 옵션을 활성화하는 경우 가져오는 인증서에 CA 플래그가 true로 설정된 기본 제한 확장명이 포함되어 있으면 키 사용 확장이 있는지 확인하고, keyEncipherment 비트나 keyAgreement 중 하나 또는 두 비트가 모두 설정되어 있는지도 확인합니다.

참고 Cisco ISE는 EAP-TLS 클라이언트 인증서가 있어야 디지털 서명 키 사용 확장명을 보유할 수 있습니다.

단계 **6** (선택 사항) **Usage(**사용**)** 영역에서 이 인증서를 사용할 서비스를 확인합니다.

인증서 서명 요청을 생성하는 중에 **Usage(**사용**)** 옵션을 활성화한 경우 이 정보는 자동으로 채워집니다. 나중에 인증서를 편집하여 사용을 지정할 수도 있습니다.

기본 PAN에서 **Admin(**관리자**)** 사용 인증서를 변경하면 다른 모든 노드에서 서비스가 재시작됩니다. 시스템은 기본 PAN이 재시작한 뒤에 노드를 한 번에 한 개씩 재시작합니다.

단계 **7** CA 서명 인증서에 인증서 서명 요청을 바인딩하려면 **Submit(**제출**)**을 클릭합니다.

이 인증서가 Cisco ISE 노드 간 통신 사용에 대해 표시되어 있는 경우 Cisco ISE 노드의 애플리케이션 서버가 다시 시작됩니다.

구축에서 다른 노드에 대해 이 프로세스를 반복하여 인증서 서명 요청을 CA 서명 인증서와 바인딩할 수 있습니다.

다음에 수행할 작업

신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 177 페이지

인증서 서명 요청 내보내기

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **3** 인증서 서명 요청이 로컬 파일 시스템에 다운로드됩니다.

인증서 서명 요청 설정

Cisco ISE에서는 관리 포털에서 단일 요청으로 구축의 모든 노드에 대한 인증서 서명 요청을 생성할 수 있습니다. 또한 필요에 따라 구축의 단일 노드 또는 여러 모든 노드에 대한 인증서 서명 요청도 생성할 수 있습니다. 여러 노드에 대한 인증서 서명 요청을 생성하도록 선택하는 경우 ISE는 인증서 주체의 CN= 필드에서 특정 노드의 FQDN(Fully Qualified Domain Name)을 자동으로 대체합니다. 인증서의 SAN(Subject Alternative Name) 필드에 항목을 포함하도록 선택하는 경우 다른 SAN 속성과 함께 ISE 노드의 FQDN을 입력해야 합니다. 구축의 모든 노드에 대해 인증서 서명 요청을 생성하도록 선택하는 경우 Allow Wildcard Certificates(와일드카드 인증서 허용) 확인란을 선택하고 SAN 필드(DNS 이름)에 와일드카드 FQDN 표기법(예: *.amer.example.com)을 입력합니다. EAP 인증에 인증서를 사용하려는 경우 CN= 필드에 와일드카드 값을 입력하지 마십시오.

와일드카드 인증서를 사용하는 경우에는 각 Cisco ISE 노드에 대해 고유한 인증서를 더 이상 생성하지 않아도 됩니다. 또한 인증서 경고가 표시되지 않도록 하기 위해 여러 FQDN 값을 SAN 필드에 입력할 필요도 없습니다. SAN 필드에 별표(*)를 사용하면 구축의 여러 모든 노드에 걸쳐 단일 인증서를 공유할 수 있으며, 인증서 이름 불일치 경고가 표시되지 않습니다. 그러나 와일드카드 인증서를 사용하는 방식은 각 Cisco ISE 노드용으로 고유한 서버 인증서를 할당하는 방식보다 보안성이 낮은 것으로 간주됩니다.

다음 표에서는 인증서 서명 요청 창의 필드에 대해 설명합니다. 이 창은 CA(Certificate Authority)에 의해 서명될 수 있는 인증서 서명 요청을 생성하는 데 사용할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Signing Request(**인증서 서명 요청**)** 입니다.

표 ***25:*** 인증서 서명 요청 설정

필드	사용 지침
Certificate(s) will be used for(인증서 사용 대상**)**	

필드	사용 지침
	인증서를 사용할 서비스를 선택합니다. **Cisco ISE ID** 인증서 • **Multi-Use(**다용도**)**: 여러 서비스(관리, EAP-TLS 인증, pxGrid 및 포털)에 사용됩니다. 다용도 인증서는 클라이언트 및 서버 키 사용을 모두 지원합니다. 서명 CA의 인증서 템플릿은 컴퓨터 또는 머신 인증서 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 및 TLS 웹 클라이언트 인증(1.3.6.1.5.5.7.3.2) • **Admin(**관리**)**: 구축의 ISE 노드 간 통신 및 관리 포털과의 통신을 보호하기 위한 서버 인증에 사용됩니다. 서명 CA의 인증서 템플릿은 웹 서버 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) • **EAP Authentication(EAP** 인증**)**: 서버 인증에 사용됩니다. 서명 CA의 인증서 템플릿은 컴퓨터 또는 머신 인증서 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 참고 EAP-TLS 클라이언트 인증서에는 디지털 서명 키를 사용해야 합니다. • **RADIUS DTLS**: RADIUS DTLS 서버 인증에 사용됩니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) • **ISE Messaging Service(ISE** 메시징 서비스**)**: Syslog Over Cisco ISE Messaging(Cisco ISE 메시징을 통한 시스템 로그) 기능에서 사용되며, 구축 당시 기본으로 내장된 UDP 시스템 로그 수집 대상(LogCollector 및 LogCollector2)에 대해 MnT WAN 존속성을 활성화합니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) • **Portal(**포털**)**: 모든 ISE 웹 포털과의 통신을 보호하기 위한 서버 인증에 사

필드	사용 지침
	용됩니다. 서명 CA의 인증서 템플릿은 컴퓨터 또는 머신 인증서 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) • **pxGrid**: pxGrid 클라이언트와 서버 간의 통신을 보호하기 위해 클라이언트 및 서버 인증에 사용됩니다. 서명 CA의 인증서 템플릿은 컴퓨터 또는 머신 인증서 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 및 TLS 웹 클라이언트 인증(1.3.6.1.5.5.7.3.2) • **SAML**: SAML IdP(Identity Provider)와의 통신을 보호하는 데 사용되는 서버 인증서입니다. SAML에 사용하도록 지정된 인증서는 관리, EAP, 인증 등의 기타 서비스에는 사용할 수 없습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 참고 Extended Key Usage(확장 키 사용) 속성의 모든 용도 개체 식별자에 대해 2.5.29.37.0 값을 포함하는 인증서를 사용하지 않는 것이 좋습니다. Extended Key Usage(확장 키 사용) 속성에서 모든 용도 개체 식별자에 대해 2.5.29.37.0 값을 포함하는 인증서를 사용하는 경우 인증서가 유효하지 않은 것으로 간주되고, 다음 오류 메시지가 표시됩니다. `source=local ; type=fatal ; message="unsupported certificate"` **Cisco ISE** 인증 기관 인증서

필드	사용 지침

	• **ISE Root CA(ISE** 루트 **CA)**: (내부 CA 서비스에만 해당함) 기본 PAN의 루트 CA 및 PSN의 하위 CA를 비롯하여 전체 내부 CA 인증서 체인을 재생성하는 데 사용됩니다.
	• **ISE Intermediate CA(ISE** 중간 **CA)**: (ISE가 외부 PKI의 중간 CA로 작동하는 경우 내부 CA 서비스에만 해당함) 기본 PAN의 중간 CA 인증서 및 PSN의 하위 CA 인증서를 생성하는 데 사용됩니다. 서명 CA의 인증서 템플릿은 하위 인증 기관이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다.
	  • 기본 제한: 위험, 인증 기관 여부
	  • 키 사용: 인증서 서명, 디지털 서명
	  • 확장 키 사용: OCSP 서명(1.3.6.1.5.5.7.3.9)
	• **Renew ISE OCSP Responder Certificates(ISE OCSP** 응답자 인증서 갱신**)**: (내부 CA 서비스에만 해당함) 전체 구축에 대한 ISE OCSP 응답자 인증서를 갱신하는 데 사용되며, 인증서 서명 요청과는 다릅니다. 보안을 위해 ISE OCSP 응답자 인증서는 6개월에 한 번씩 갱신하는 것이 좋습니다.

Allow Wildcard Certificates(와일드카드 인증서 허용**)**	인증서의 SAN 필드에서 CN 및/또는 DNS 이름에 와일드카드 문자(*)를 사용하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 구축의 모든 노드가 자동으로 선택됩니다. 맨 왼쪽 레이블 위치에 별표(*) 와일드카드 문자를 사용해야 합니다. 와일드카드 인증서를 사용하는 경우에는 보안 향상을 위해 도메인 공간을 분할하는 것이 좋습니다. 예를 들어 *.example.com 대신 *.amer.example.com으로 도메인을 분할할 수 있습니다. 도메인을 분할하지 않으면 심각한 보안 문제가 발생할 수 있습니다.
Generate CSRs for these Nodes(이 노드에 대해 **CSR** 생성**)**	인증서를 생성할 노드 옆에 있는 확인란을 선택합니다. 구축의 선택 노드에 대해 CSR을 생성하려면 Allow Wildcard Certificates(와일드카드 인증서 허용) 옵션의 선택을 취소해야 합니다.
Common Name(CN)(공용 이름**)**	기본적으로 공용 이름은 인증서 서명 요청을 생성하는 ISE 노드의 FQDN입니다. $FQDN$은 ISE 노드의 FQDN을 나타냅니다. 구축의 여러 노드에 대해 인증서 서명 요청을 생성하는 경우 인증서 서명 요청의 Common Name(공통 이름) 필드가 해당 ISE 노드의 FQDNdmfh 대체됩니다.
Organizational Unit(OU)(조직 단위**)**	조직 단위의 이름입니다. Engineering 등을 예로 들 수 있습니다.
Organization(O)(조직**)**	조직의 이름입니다. Cisco 등을 예로 들 수 있습니다.
City(L)(구/군/시**)**	(약어로 표기하지 않음) 구/군/시의 이름입니다. San Jose 등을 예로 들 수 있습니다.

필드	사용 지침
State(ST)(시/도**)**	(약어로 표기하지 않음) 시/도의 이름입니다. California 등을 예로 들 수 있습니다.
Country(C)(국가**)**	국가의 이름입니다. 2자리 ISO 국가 코드를 입력해야 합니다. US 등을 예로 들 수 있습니다.
SAN(Subject Alternative Name)	IP 주소, DNS 이름, URI(Uniform Resource Identifier) 또는 인증서와 연결된 디렉토리 이름 • **DNS** 이름: DNS 이름을 선택하는 경우 ISE 노드의 정규화된 도메인 이름을 입력합니다. Allow Wildcard Certificates(와일드카드 인증서 허용) 옵션을 활성화한 경우 와일드카드 표기법(별표 및 도메인 이름 앞의 마침표)을 지정합니다. 예: *.amer.example.com • **IP** 주소: 인증서와 연결할 ISE 노드의 IP 주소입니다. • **Uniform Resource Identifier**: 인증서와 연결할 URI입니다. • 디렉토리 이름: RFC 2253에 따라 정의된 DN(Distinguished Name)의 문자열 표현입니다. 쉼표(,)를 사용하여 DN을 구분합니다. "dnQualifier" RDN의 경우 쉼표를 이스케이프하고 구분 기호로 백슬래시와 쉼표, 즉 "\,"를 사용합니다. 예: CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL
Key Type(키 유형**)**	공개 키를 생성하는 데 사용할 알고리즘을 RSA 또는 ECDSA로 지정합니다.
Key Length(키 길이**)**	공개 키의 비트 크기를 지정합니다. RSA에는 다음 옵션을 사용할 수 있습니다. • 512 • 1024 • 2048 • 4096 ECDSA에는 다음 옵션을 사용할 수 있습니다. • 256 • 384 참고 RSA 및 ECDSA 공개 키는 동일한 보안 레벨에서 키 길이가 다를 수 있습니다. 공용 CA 서명 인증서를 가져오거나 하려면 2048 이상을 선택합니다.

필드	사용 지침
Digest to Sign With(서명에 사용할 다이제스트**)**	SHA-1 또는 SHA-256 해싱 알고리즘 중 하나를 선택합니다.
인증서 정책	인증서가 준수해야 하는 인증서 정책 OID 또는 OID 목록을 입력합니다. 쉼표나 공백을 사용하여 OID를 구분합니다.

관련 항목

인증서 서명 요청, 184 페이지
인증서 서명 요청을 생성하고 인증 기관에 제출, 184 페이지
인증서 서명 요청에 대한 CA 서명 인증서 바인딩, 185 페이지

포털 사용을 위한 인증서 설정

구축에서 웹 포털 요청을 처리할 수 있는 PSN이 여러 개 있는 경우 Cisco ISE에는 포털 통신에 사용할 인증서를 식별할 수 있는 고유 식별자가 필요합니다. 포털에서 사용하도록 지정된 인증서를 추가하거나 가져오는 경우 인증서 그룹 태그를 정의하고 이를 구축의 각 노드에 있는 해당 인증서와 연결해야 합니다. 이 인증서 그룹 태그를 해당 최종 사용자 포털(게스트, 스폰서 및 개인 디바이스 포털)에 연결해야 합니다. 이 인증서 그룹 태그는 Cisco ISE가 이러한 각 포털과 통신할 때 사용해야 하는 인증서를 식별하도록 도와주는 고유 식별자입니다. 포털마다 각 노드의 인증서를 하나씩만 지정할 수 있습니다.

참고 Cisco ISE는 TCP 포트 8443(또는 포털 사용을 위해 구성한 포트)에서 포털 인증서를 제공합니다.

단계 **1** 인증서 서명 요청을 생성하고 인증 기관에 제출, 184 페이지.

이미 정의한 인증서 그룹 태그를 선택하거나 포털용으로 새 태그를 생성해야 합니다. 예를 들어 mydevicesportal과 같은 태그를 생성할 수 있습니다.

단계 **2** 신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 177 페이지.

단계 **3** 인증서 서명 요청에 대한 CA 서명 인증서 바인딩, 185 페이지.

CA 서명 인증서에 기본 포털 인증서 그룹 태그 재할당

기본적으로 모든 Cisco ISE 포털은 셀프 서명 인증서를 사용합니다. 포털에 CA 서명 인증서를 사용하려는 경우 CA 서명 인증서에 기본 포털 인증서 그룹 태그를 할당할 수 있습니다. 기존의 CA 서명 인증서를 사용할 수도 있고, CSR을 생성하여 포털에서 사용할 새 CA 서명 인증서를 얻을 수도 있습니다. 인증서 간에 포털 그룹 태그를 재할당할 수 있습니다.

참고 기존 인증서를 편집할 때 해당 인증서에 연결되어 있는 포털 태그(게스트)를 이미 사용 중인 포털이 있으면 기본 포털 인증서 그룹 태그 또는 기타 포털 그룹 태그를 이 인증서에 재할당할 수 없습니다. 시스템에는 "게스트" 포털 태그를 사용하는 포털 목록이 나열됩니다.

다음 절차에서는 CA 서명 인증서에 기본 포털 인증서 그룹 태그를 재할당하는 방법을 설명합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다.

기본 포털 인증서 그룹 태그 옆의 i 아이콘을 마우스로 가리키면 해당 태그를 사용하는 포털 목록을 확인할 수 있습니다. 이 태그가 할당된 포털 인증서가 있는 구축 내 ISE 노드도 확인할 수 있습니다.

단계 **2** 포털에 사용할 CA 서명 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

포털에서 사용하고 있지 않은 CA 서명 인증서를 선택해야 합니다.

단계 **3** **Usage(**사용**)** 영역에서 **Portal(**포털**)** 확인란을 선택하고 기본 포털 인증서 그룹 태그를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

경고 메시지가 표시됩니다.

단계 **5** **Yes(**예**)**를 클릭하여 기본 포털 인증서 그룹 태그를 CA 서명 인증서에 재할당합니다.

노드 등록 전에 포털 인증서 태그 연결

구축의 모든 포털에 대해 "기본 포털 인증서 그룹" 태그를 사용하는 경우에는 새 ISE 노드를 등록하기 전에 관련 CA 서명 인증서를 가져오고 서비스로 "Portal(포털)"을 선택한 다음 "기본 포털 인증서 그룹" 태그를 이 인증서와 연결해야 합니다.

구축에 새 노드를 추가하면 기본 셀프 서명 인증서가 "기본 포털 인증서 그룹" 태그와 연결되며 이 태그를 사용하도록 포털이 구성됩니다.

새 노드를 등록한 후에는 인증서 그룹 태그 연결을 변경할 수 없습니다. 그러므로 구축에 노드를 등록하기 전에 다음을 수행해야 합니다.

단계 **1** 셀프 서명된 인증서를 생성하고 서비스로 "Portal(포털)"을 선택한 후 tempportaltag 등의 다른 인증서 그룹 태그를 할당합니다.

단계 **2** 새로 생성한 인증서 그룹 태그(tempportaltag)를 사용하도록 포털 컨피그레이션을 변경합니다.

단계 **3** 기본 셀프 서명 인증서를 편집하여 Portal(포털) 역할을 제거합니다.

이 옵션을 사용하는 경우 기본 셀프 서명 인증서와의 "기본 포털 인증서 그룹" 태그 연결이 제거됩니다.

단계 **4** 다음 중 하나를 수행합니다.

옵션	설명
Generate a CSR(CSR 생성)	CSR 생성 시: **1.** 이 인증서를 사용할 서비스로 "Portal(포털)"을 선택하고 "기본 포털 인증서 그룹" 태그를 연결합니다. **2.** CA에 CSR을 보내고 서명된 인증서를 가져옵니다. **3.** 인증서에 서명을 한 CA의 루트 및 기타 중간 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다. **4.** CA 서명 인증서를 CSR에 바인딩합니다.
Import the private key and the CA-signed certificate(개인 키 및 CA 서명 인증서 가져오기)	CA 서명 인증서를 가져올 때는 다음을 수행합니다. **1.** 이 인증서를 사용할 서비스로 "Portal(포털)"을 선택하고 "기본 포털 인증서 그룹" 태그를 연결합니다. **2.** 인증서에 서명을 한 CA의 루트 및 기타 중간 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다.
기존 CA 서명 인증서를 편집합니다.	기존 CA 서명 인증서를 편집할 때는 다음을 수행합니다. 이 인증서를 사용할 서비스로 "Portal(포털)"을 선택하고 "기본 포털 인증서 그룹" 태그를 연결합니다.

단계 **5** 구축에 ISE 노드를 등록합니다.
구축의 포털 컨피그레이션이 "기본 포털 인증서 그룹" 태그로 구성되고 포털이 새 노드에서 "기본 포털 인증서 그룹" 태그와 연결된 CA 서명 인증서를 사용하도록 구성됩니다.

사용자 및 엔드포인트 인증서 갱신

기본적으로 Cisco ISE는 인증서가 만료된 디바이스에서 발생하는 요청을 거부합니다. 그러나 이 기본 동작을 변경하여 그러한 요청을 처리하고 사용자에게 인증서를 갱신할지 묻는 메시지를 표시하도록 ISE를 구성할 수 있습니다.

사용자가 인증서를 갱신하도록 허용하는 경우 요청을 추가로 처리하기 전에 인증서가 갱신되었는지 확인하는 권한 부여 정책 규칙을 구성하는 것이 좋습니다. 인증서가 만료된 디바이스에서 오는 요청을 처리하면 잠재적 보안 위협이 발생할 수 있습니다. 따라서 조직의 보안이 손상되지 않도록 적절한 권한 부여 프로파일 및 규칙을 구성해야 합니다.

일부 디바이스에서는 인증서가 만료되기 전과 후에 인증서를 갱신할 수 있습니다. 그러나 Windows 디바이스에서는 인증서가 만료되기 전에만 갱신할 수 있습니다. Apple iOS, Mac OSX 및 Android 디바이스에서는 인증서가 만료되기 전과 후에 인증서를 갱신할 수 있습니다.

인증서 갱신을 위해 정책 조건에 사용되는 사전 속성

Cisco ISE 인증서 사전에는 정책 조건에 사용되는 다음과 같은 속성이 있습니다. 사용자는 그러한 정책 조건을 통해 인증서를 갱신할 수 있습니다.

- Days to Expiry(만료될 때까지 남은 일 수): 이 속성은 인증서가 유효한 기간(일)을 제공합니다. 이 속성을 사용하여 권한 부여 정책에 사용할 수 있는 조건을 생성할 수 있습니다. 이 속성은 0~15 범위의 값을 사용할 수 있습니다. 값 0은 인증서가 이미 만료되었음을 나타냅니다. 값 1은 인증서가 만료되기까지 1일이 채 남지 않았음을 나타냅니다.
- Is Expired(만료됨): 이 부울 속성은 인증서가 만료되었는지 여부를 나타냅니다. 인증서 만료가 다가오는 경우 인증서가 만료되기 전에만 인증서 갱신을 허용하려면, 권한 부여 정책 조건에서 이 속성을 사용합니다.

인증서 갱신을 위한 권한 부여 정책 조건

권한 부여 정책에서 CertRenewalRequired 단순 조건(기본적으로 사용 가능)을 사용하여 Cisco ISE에서 요청을 추가로 처리하기에 앞서 인증서(만료됨 또는 만료 예정)가 갱신되었는지 확인할 수 있습니다.

인증서 갱신을 위해 **CWA** 리디렉션

사용자 인증서가 만료되기 전에 취소되면 Cisco ISE가 CA에서 게시한 CRL을 확인하고 인증 요청을 거부합니다. 취소된 인증서가 만료된 경우 CA는 CRL에 이 인증서를 게시하지 않을 수 있습니다. 이 시나리오에서 Cisco ISE는 취소된 인증서를 갱신할 수 있습니다. 이런 문제를 방지하려면 인증서를 갱신하기 전에 전체 인증을 위해 요청이 CWA(Centralized Web Authentication)로 리디렉션되는지 확인해 주십시오. 사용자를 CWA로 리디렉션하려면 권한 부여 프로파일을 생성해야 합니다.

사용자가 인증서를 갱신할 수 있도록 **Cisco ISE** 구성

사용자가 인증서를 갱신할 수 있도록 Cisco ISE를 구성하려면 이 절차에 나와 있는 작업을 완료해야 합니다.

시작하기 전에

CWA 요청을 리디렉션하도록 WLC에서 제한된 액세스 ACL을 구성합니다.

단계 **1** 허용되는 프로토콜 컨피그레이션 업데이트, 196 페이지
단계 **2** CWA 리디렉션용 권한 부여 정책 프로파일 생성, 196 페이지
단계 **3** 인증서 갱신용 권한 부여 정책 규칙 생성, 197 페이지
단계 **4** 게스트 포털에서 BYOD 설정 활성화, 198 페이지

허용되는 프로토콜 컨피그레이션 업데이트

단계 **1** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authentication(**인증**)** > **Allowed Protocols(**허용되는 프로토콜**)** > **Default Network Access(**기본 네트워크 액세스**)**를 선택합니다.

단계 **2** EAP-TLS 프로토콜 아래에서 **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy(**만료된 인증서 인증을 허용하여 권한 부여 정책에서 인증서 갱신 허용**)** 확인란을 선택하고 PEAP 및 EAP-FAST 프로토콜용 EAP-TLS 내부 메서드를 선택합니다.

그러면 EAP-TLS를 사용하는 요청이 NSP 플로우를 통과하게 됩니다.

PEAP 및 EAP-FAST 프로토콜의 경우 Cisco ISE가 요청을 처리하도록 Cisco AnyConnect를 수동으로 구성해야 합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

CWA 리디렉션용 권한 부여 정책 프로파일 생성, 196 페이지

CWA 리디렉션용 권한 부여 정책 프로파일 생성

시작하기 전에

WLC에서 제한된 액세스 ACL을 구성했는지 확인합니다.

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

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 권한 부여 프로파일의 이름을 입력합니다. 예를 들어 CertRenewal_CWA와 같이 입력합니다.

단계 **4** 일반 작업 영역에서 **Web Redirection (CWA, DRW, MDM, NSP, CPP)(**웹 리디렉션**(CWA, DRW, MDM, NSP, CPP))** 확인란을 선택합니다.

단계 **5** 드롭다운 목록에서 **Centralized Web Auth(**중앙 웹 인증**)**를 선택하고 제한된 액세스 ACL을 선택합니다.

단계 **6** **Display Certificates Renewal Message(**인증서 갱신 메시지 표시**)** 확인란을 선택합니다.

URL-redirect 속성 값이 변경되어 인증서가 유효한 기간(일)이 포함됩니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

참고 Cisco ISE 1.2에서 무선 디바이스용으로 다음과 같은 DRW(Device Registration WebAuth) 정책을 구성한 경우:

- 조건 = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) 및 프로파일 = Wireless-drw-redirect가 포함된 DRW-Redirect 정책
- 조건 = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) 및 프로파일 = Wireless-Permit이 포함된 DRW-Allow 정책

ISE 1.3 이상 버전으로 업그레이드한 후 DRW-Allow 정책 조건을 다음과 같이 업데이트해야 합니다.

- 조건 = (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow) 및 프로파일 = Wireless-Permit

다음에 수행할 작업

인증서 갱신용 권한 부여 정책 규칙 생성, 197 페이지

인증서 갱신용 권한 부여 정책 규칙 생성

시작하기 전에

중앙 웹 인증 리디렉션용 권한 부여 프로파일을 생성했는지 확인합니다.

Administration(관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Policy Settings(**정책 집합**)**에서 정책 집합을 활성화합니다.

단계 **1** **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Sets(**정책 집합**)**를 선택합니다.

단계 **2** **Create Above(**위에 생성**)**를 클릭합니다.

단계 **3** 새 규칙의 이름을 입력합니다.

단계 **4** 다음의 단순 조건 및 결과를 선택합니다.

CertRenewalRequired=True인 경우 권한에 대해 앞에서 생성한 권한 부여 프로파일(CertRenewal_CWA)을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

참고 Cisco ISE에서는 한 번에 최대 50개의 권한 부여 정책을 로드할 수 있으며, 다음 정책 집합을 로드하는 데 약 10초가 지연됩니다.

참고 생성된 정책 목록에서 특정 권한 부여 정책을 검색하는 경우 검색 창에 제공된 정책 이름이 아래 정책 목록에서 강조 표시되지만 필터링되지는 않습니다.

다음에 수행할 작업

인증서가 만료된 디바이스를 사용하여 회사 네트워크에 액세스할 때는 **Renew(**갱신**)**를 클릭하여 디바이스를 재구성합니다.

게스트 포털에서 **BYOD** 설정 활성화

사용자가 개인 디바이스 인증서를 갱신할 수 있도록 하려면 선택한 게스트 포털에서 BYOD 설정을 활성화해야 합니다.

단계 **1** **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals and Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)**를 선택합니다.

a) 선택한 CWA 포털을 고르고 **Edit(**편집**)**를 클릭합니다.

단계 **2** BYOD Settings(BYOD 설정)에서 **Allow employees to use personal devices on the network(**네트워크에서 직원의 개인 디바이스 사용 허용**)** 확인란을 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

Apple iOS 디바이스용 인증서 갱신 실패

ISE를 사용하여 Apple iOS 디바이스에서 엔드포인트 인증서를 갱신하는 경우 "Profiled Failed to Install(프로파일링 설치 실패)" 오류 메시지가 표시될 수 있습니다. 이 오류 메시지는 만료 예정이거나 만료된 네트워크 프로파일이 동일한 PSN(Policy Service Node)에서, 또는 다른 PSN에서 갱신 처리에 사용되는 것과 다른 관리 HTTPS 인증서로 서명된 경우에 나타납니다.

문제 해결을 위해서는 일반적으로 UCC(Unified Communications Certificate)라고 하는 다중 도메인 SSL 인증서, 또는 구축의 모든 PSN에서 관리 HTTPS에 대해 와일드카드 인증서를 사용해 주십시오.

인증서 정기 확인 설정

Cisco ISE는 CRL(Certificate Revocation List)을 정기적으로 확인합니다. 이 창에서는 자동으로 다운로드되는 CRL에 대해 진행 중인 세션을 확인하도록 Cisco ISE를 구성할 수 있습니다. 매일 OCSP 또는 CRL 확인을 시작해야 하는 시간과 Cisco ISE가 OCSP 서버 또는 CRL을 다시 확인할 때까지 대기하는 시간 간격을 시간 단위로 지정할 수 있습니다.

다음 표에서는 인증서(OCSP 또는 CRL)의 상태를 확인할 시간 간격을 지정할 수 있는 Certificate Periodic Check Settings(인증서 정기 확인 설정) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Periodic Check Settings(**인증서 정기 확인 설정**)**입니다.

표 ***26:*** 인증서 정기 확인 설정

필드 이름	사용 지침
Certificate Check Settings(인증서 확인 설정**)**	

필드 이름	사용 지침
Check ongoing sessions against automatically retrieved CRL(자동으로 검색된 **CRL**에 대해 진행 중인 세션 확인**)**	Cisco ISE가 자동으로 다운로드되는 CRL에 대해 진행 중인 세션을 확인하도록 지정하려면 이 확인란을 선택합니다.
CRL/OCSP Periodic Certificate Checks(CRL/OCSP 정기 인증서 확인**)**	
First check at(첫 확인 시간**)**	매일 CRL 또는 OCSP 확인을 시작할 시간을 지정합니다. 00:00~23:59시간 사이의 값을 입력합니다.
Check every(확인 간격**)**	Cisco ISE가 CRL 또는 OCSP 서버를 다시 확인할 때까지 대기하는 시간 간격을 시간 단위로 지정합니다.

관련 항목

OCSP 서비스, 235 페이지
OCSP 클라이언트 프로파일 추가, 237 페이지

Cisco ISE CA 서비스

인증서는 자체 서명되거나 외부 CA(Certificate Authority)에 의해 디지털 서명될 수 있습니다. Cisco ISE Internal Certificate Authority(ISE CA)는 엔드포인트에 대한 디지털 인증서를 발급하고 중앙 집중식 콘솔에서 관리하므로 직원이 회사 네트워크에서 개인 디바이스를 사용할 수 있습니다. CA 서명 디지털 인증서는 업계 표준으로 보안성이 더 높은 것으로 간주됩니다. 기본 PAN은 루트 CA입니다. PSN(Policy Service Nodes)은 기본 PAN(SCEP RA)에 대한 하위 CA입니다. ISE CA는 다음과 같은 기능을 제공합니다.

- Certificate Issuance: 네트워크에 연결되는 엔드포인트에 대한 CSR(Certificate Signing Requests)을 검증하고 서명합니다.
- Key Management: 키와 인증서를 생성하고 PAN 및 PSN 노드에서 모두 안전하게 저장합니다.
- Certificate Storage: 사용자 및 디바이스에 발급된 인증서를 저장합니다.
- Support OCSP(Online Certificate Status Protocol): 인증서의 유효성을 확인하도록 OCSP 응답자를 제공합니다.

기본 관리 노드에서 CA 서비스가 비활성화된 경우에도 보조 관리 노드의 CLI에서 실행 중인 것으로 간주됩니다. CA 서비스는 비활성화된 상태로 표시하는 것이 가장 좋습니다. 이는 알려진 Cisco ISE 문제입니다.

Cisco ISE 인증서 핑거프린트

인증서 핑거프린트 프로세스는 신뢰할 수 있는 인증서와 일치하도록 인증서 즉시 발급 핑거프린트 SHA256을 평가하는 데 사용됩니다. 이렇게 하면 여러 CA가 서로 다른 도메인을 지원하도록 보안 메커니즘이 적용되며 802.1x 프로토콜용으로 신뢰할 수 있는 CA를 잠글 수도 있습니다.

정책 조건에서 인증서를 업데이트하기 전에 발급자 핑거프린트 SHA-256 인증서가 Cisco ISE 구축에 추가되었는지 확인하십시오.

참고 신뢰할 수 있는 인증서가 정책으로 구성된 후에는 인증서를 삭제할 수 없습니다. 다음 메시지가 **Trusted Certificates(**신뢰할 수 있는 인증서**)** 창의 **This Trusted Certificate Refered by Policy Sets(**정책 집합에서 참조하는 신뢰할 수 있는 인증서**)**에 표시됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

인증서가 정책에서 사용되므로 인증서를 삭제할 수 없습니다. 인증서를 삭제하려면 먼저 정책 조건을 수정하십시오.

Cisco ISE용 인증서 핑거프린트를 구성하려면 아래 단계를 순서대로 수행합니다.

1. 내부 사용자를 생성합니다. 자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드, 릴리스 *3.0*의 "자산 가시성" 장에서 "사용자 추가" 섹션을 참조하십시오.
2. 네트워크 디바이스를 추가합니다. 자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드, 릴리스 *3.0*의 "기본 설정" 장에서 "Cisco ISE에서 네트워크 디바이스 추가" 섹션을 참조하십시오.
3. **External Certificates(**외부 인증서**)**에서 외부 CA를 가져옵니다. 자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드, 릴리스 *3.0*의 "기본 설정" 장에서 "시스템 인증서 가져오기" 섹션을 참조하십시오.

   SCEP 프로토콜을 사용하여 발급자 핑거프린트 SHA-256 인증서를 가져올 수도 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authorit(**인증 기관**)** > **External CA Settings(**외부 **CA** 설정**)**를 선택합니다. 표시되는 **Add SCEP RA Profile(SCEP RA** 프로파일 추가**)** 창에서 **Add(**추가**)**를 클릭합니다. **Name(**이름**)** 필드에 인증서 이름을 입력합니다. **URL** 필드에 CA 서버 URL을 입력합니다. **Test Connection(**테스트 연결**)**을 클릭합니다.
4. SHA-256 핑거프린트로 정책 생성
5. SHA-256 핑거프린트를 사용하여 인증 정책 생성 및 매핑
6. 권한 부여 정책 생성.
7. PRRT 로그 확인

SHA-256 핑거프린트로 정책 생성

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

단계 2 표시되는 **Policy Set(정책 집합)** 창에서 **Settings(설정)**를 클릭하고 드롭다운 목록에서 **Insert a new row(새 행 삽입)**를 선택합니다.

단계 3 **New Policy Name(새 정책 이름)** 필드에 이름을 입력합니다.

단계 4 이 정책에 대한 설명을 입력합니다.

단계 5 **Conditions(조건)** 열 아래에서 새 **Policy Set Name(정책 집합 이름)** 옆의 **Add(추가)(+)** 아이콘을 클릭합니다.

단계 6 표시되는 **Condition Studio** 창에서 **Click to Add Attribute(속성을 추가하려면 클릭)** 필드를 클릭합니다.

단계 7 **All Dictionary(모든 사전)** 드롭다운 목록에서 **Network Access-Protocol(네트워크 액세스-프로토콜)**(**Dictionary-Attribute(사전-속성)**) 조합을 선택합니다.

단계 8 논리 조건을 작성하기 위해 **Equals(같음)** 연산자를 선택합니다.

단계 9 **Choose from List or Type(목록 또는 유형 선택)** 드롭다운 목록에서 **RADIUS**를 선택합니다.

단계 10 **Use(사용)**를 클릭합니다.

단계 11 표시되는 **Policy Set(정책 집합)** 창의 **Allowed Protocols/Server Sequence(허용되는 프로토콜/서버 시퀀스)** 드롭다운 목록에서 **Default Network Access(기본 네트워크 액세스)**를 선택합니다.

단계 12 **Save(저장)**를 클릭합니다.

SHA-256 핑거프린트를 사용하여 인증 정책 생성 및 매핑

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

단계 2 **Authentication Policy(인증 정책)**를 클릭합니다.

단계 3 Settings(설정) 아이콘을 클릭하고 **Insert a new row(새 행 삽입)**를 선택합니다.

단계 4 **Authentication Rule Name(인증 규칙 이름)** 창에서 이름을 입력합니다.

단계 5 규칙 이름 옆에 있는 **Add(추가)(+)** 아이콘을 클릭합니다.

단계 6 표시되는 **Condition Studio** 창에서 **Click to add Attributes(클릭하여 속성 추가)** 필드를 클릭합니다.

단계 7 **All Dictionary(모든 사전)** 드롭다운 목록에서 **CERTIFICATE-Issuer- Fingerprint SHA-256**(**Dictionary-Attribute**) 조합을 선택합니다.

단계 8 논리 조건을 작성하기 위해 **Equals(같음)** 연산자를 선택합니다.

단계 9 **Choose from List or Type(목록 또는 유형에서 선택)** 드롭다운 목록에서 **Cisco Manufacturing CA SHA2 fingerprint sha256**을 선택합니다.

단계 10 **Use(사용)**를 클릭합니다.

단계 11 표시되는 **Policy Set(정책 집합)** 창의 **Allowed Protocols/Server Sequence(허용되는 프로토콜/서버 시퀀스)** 드롭다운 목록에서 **Preloaded_Certificate_Profile**을 선택합니다.

단계 12 **Save(저장)**를 클릭합니다.

권한 부여 정책 생성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Set(**정책 집합**)** > **Default(**기본값**)**를 선택합니다.

단계 **2** **Authorization Policy(**권한 부여 정책**)**을 클릭합니다.

단계 **3** 설정 아이콘을 클릭하고 드롭 다운 목록에서 **Insert a new row(**새 행 삽입**)**를 선택합니다.

단계 **4** **Authorization Rule Name(**권한 부여 규칙 이름**)** 창에서 이름을 입력합니다.

단계 **5** 규칙 이름 옆에 있는 **Add(**추가**)**(+) 아이콘을 클릭합니다.

단계 **6** 표시되는 **Condition Studio** 창에서 **Click to add Attributes(**클릭하여 속성 추가**)** 필드를 클릭합니다.

단계 **7** **All Dictionary(**모든 사전**)** 드롭다운 목록에서 **CERTIFICATE-Issuer- Fingerprint SHA-256(Dictionary-Attribute)** 조합을 선택합니다.

단계 **8** 논리 조건을 작성하기 위해 **Equals(**같음**)** 연산자를 선택합니다.

단계 **9** 목록 또는 유형 드롭 다운 목록에서 **Cisco Root CA 2099** 핑거프린트 **sha**를 선택합니다.

단계 **10** **Use(**사용**)**를 클릭합니다.

단계 **11** 표시되는 **Policy Set(**정책 집합**)** 창의 **Allowed Protocols/Server Sequence(**허용되는 프로토콜/서버 시퀀스**)** 드롭다운 목록에서 **PermitAccess(**액세스 허용**)**를 선택합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

PRRT 로그 확인

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operation(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**.

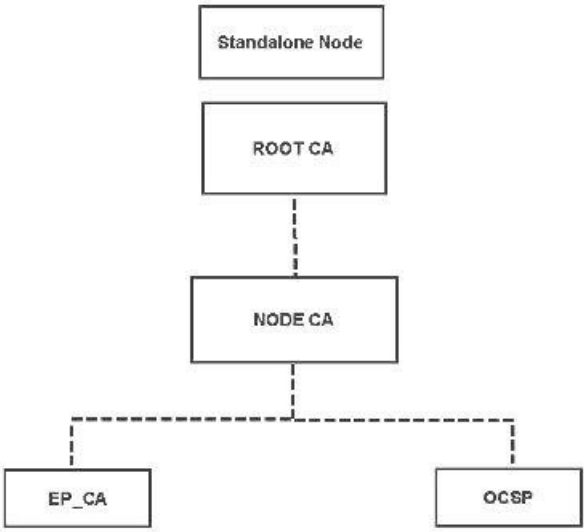
단계 **2** 표시되는 **Live Logs(**라이브 로그**)** 창에서 최신 로그 세부정보를 클릭합니다.

단계 **3** 표시되는 **Authentication Details(**인증 세부정보**)** 창에서 **Issuer- Fingerprint SHA-256(**발급자- 핑거프린트 **SHA-256)** 열의 SHA-256 값을 확인하여 **Issuer- Fingerprint SHA-256(**발급자- 핑거프린트 **SHA-256)** 인증서가 성공적으로 추가 및 검증되었는지 확인합니다.

관리 및 정책 서비스 노드에 프로비저닝된 **ISE CA** 인증서

설치 후 Cisco ISE 노드에는 엔드포인트용 인증서를 관리할 수 있도록 루트 CA 인증서와 노드 CA 인증서가 프로비저닝됩니다.

그림 ***8:*** 독립형 노드에 프로비저닝된 ***ISE CA*** 인증서

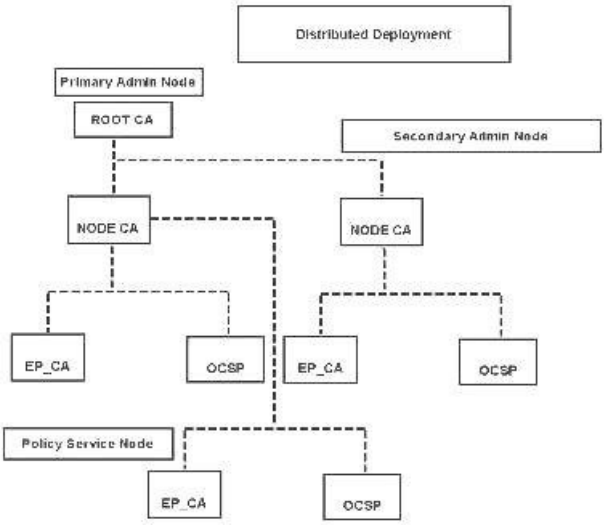


구축을 설정할 때는 PAN(Primary Administration Node)으로 지정하는 노드가 루트 CA가 됩니다. PAN에는 루트 CA 인증서 및 루트 CA가 서명한 노드 CA 인증서가 있습니다.

보조 관리 노드를 PAN에 등록하면 노드 CA 인증서가 생성되며, 기본 관리 노드의 루트 CA가 이 인증서에 서명합니다.

PAN에 등록하는 모든 PSN(Policy Service Node)에는 PAN의 노드 CA가 서명한 OCSP 인증서 및 엔드포인트 CA가 프로비저닝됩니다. PSN(Policy Service Node)은 PAN의 하위 CA입니다. ISE CA를 사용할 때는 PSN의 엔드포인트 CA가 네트워크에 액세스하는 엔드포인트에 대해 인증서를 발급합니다.

그림 ***9:*** 구축의 관리 및 정책 서비스 노드에 프로비저닝된 ***ISE CA*** 인증서



CA와 Cisco ISE의 상호운용성을 위한 요구 사항

CA 서버와 Cisco ISE를 함께 사용할 때는 다음 요구 사항이 충족되어야 합니다.

- 키 크기는 1024, 2048 또는 그 이상이어야 합니다. CA 서버에서 키 크기는 인증서 템플릿을 사용하여 정의됩니다. Cisco ISE에서 서플리컨트 프로파일을 사용하여 키 크기를 정의할 수 있습니다.
- 키를 사용하면 확장 프로그램에서 서명 및 암호화가 지원됩니다.
- SCEP 프로토콜을 통해 GetCACapabilities를 사용하면 암호화 알고리즘과 요청 해시가 지원됩니다. RSA 및 SHA1을 사용하는 것이 권장됩니다.
- OCSP(Online Certificate Status Protocol)가 지원됩니다. 이 프로토콜은 BYOD에서 직접적으로 사용되지는 않지만, 인증 철회 시 OCSP 서버처럼 작동하는 CA가 사용될 수 있습니다.

참고 Cisco ISE는 PEAP, EAP-TLS 등의 표준 EAP 인증을 위해 EJBCA(Enterprise Java Beans Certificate Authority)를 지원합니다. 프록시 SCEP에 대한 EJBCA 지원을 활성화하려면 EJBCA에서 **System(**시스템**) > Basic Configurations(**기본 컨피그레이션**)**에 있는 **Enable End Entity Profile Limitations(**종료 엔터티 프로파일 제한 활성화**)** 옵션을 비활성화해야합니다.

- 엔터프라이즈 PKI를 사용하여 Apple iOS 디바이스용 인증서를 발급하는 경우 SCEP 템플릿에서 키 사용을 구성하고 **Key Encipherment(**키 암호화**)** 옵션을 활성화해야 합니다.

  Microsoft CA를 사용하는 경우 인증서 템플릿에서 키 사용 확장을 편집합니다. **Encryption(**암호화**)** 영역에서 **Allow Key Exchange only with Key Encryption (Key encipherment)(**키 암호화를 사용하여 키 교환만 허용**(**키 암호화**))** 라디오 버튼을 클릭하고 **Allow Encryption of User Data(**사용자 데이터 암호화 허용**)** 확인란을 선택합니다.

- Cisco ISE는 EAP-TLS 인증을 위한 신뢰할 수 있는 인증서 및 엔드포인트 인증서에 대해 RSASSA-PSS 알고리즘 사용을 지원합니다. 인증서를 볼 때 서명 알고리즘은 알고리즘 이름 대신 1.2.840.113549.1.1.10으로 나열됩니다.

참고 BYOD 플로우에 Cisco ISE 내부 CA를 사용하는 경우 외부 CA에서 RSASSA-PSS 알고리즘을 통해 관리자 인증서에 서명해서는 안 됩니다. Cisco ISE 내부 CA는 해당 알고리즘을 사용하여 서명된 관리자 인증서를 확인할 수 없으며, 요청이 실패합니다.

인증서 기반 인증을 위한 클라이언트 인증서 요건

Cisco ISE를 통한 인증서 기반 인증의 경우 클라이언트 인증서가 다음 요건을 충족해야 합니다.

표 ***27: RSA*** 및 ***ECC***에 대한 클라이언트 인증서 요건

RSA

지원되는 키 크기	1024, 2048 및 4096 비트	
지원되는 SHA(Secure Hash Algorithms)	SHA-1 및 SHA-2(SHA-256 포함)	
ECC [1] [2]		
지원되는 커브 유형	P-192, P-256, P-384 및 P-521	
지원되는 SHA(Secure Hash Algorithm)	SHA-256	
클라이언트 머신 운영체제 및 지원되는 커브 유형		
Windows	8 이상	P-256, P-384 및 P-521
Android	4.4 이상 참고 Android 6.0에서 ECC 인증서를 지원하려면 2016년 5월 패치가 필요합니다.	모든 커브 유형(P-192 커브 유형을 지원하지 않는 Androidv6.0 제외)

[1] Windows 7 및 Apple iOS는 기본적으로 EAP-TLS 인증에 대해 ECC를 지원하지 않습니다.
[2] Cisco ISE의 이 릴리스에서는 MAC OS X 디바이스에서 ECC 인증서 사용을 지원하지 않습니다.

ISE CA 체인 재생성

Cisco ISE CA 체인을 재생성하면 루트 CA, 노드 CA 및 엔드포인트 CA 인증서를 포함한 모든 인증서가 재생성됩니다. PAN 또는 PSN의 도메인 이름이나 호스트 이름을 변경할 때는 ISE CA 체인을 재생성해야 합니다. 이전 릴리스에서 릴리스 2.0 이상으로 업그레이드할 때는 2개의 루트 계층 구조에서 단일 루트 계층 구조로 이동하도록 ISE CA 체인을 재생성하는 것이 좋습니다.

루트 CA이든 중간 CA 인증서이든 시스템 인증서를 재생성하면 ISE 메시징 서비스가 재시작되어 새 인증서 체인이 로드됩니다. ISE 메시징 서비스를 다시 사용할 수 있을 때까지 감사 로그가 손실됩니다.

참고 구축에서 Cisco ISE 내부 CA를 교체할 때마다 ISE 메시징 서비스도 업데이트해야 전체 인증서 체인을 검색할 수 있습니다.

Cisco ISE 내부 CA 체인을 재생성할 경우, 체인에 있는 모든 인증서의 **Valid From(**유효 기간 시작**)** 필드에 재생성 1일 전의 날짜가 표시됩니다.

Elliptical Curve Cryptography 인증서 지원

Cisco ISE CA 서비스는 ECC(Elliptical Curve Cryptography) 알고리즘을 기반으로 하는 인증서를 지원합니다. ECC는 훨씬 작은 키 크기를 사용하는 경우에도 다른 암호화 알고리즘보다 더 우수한 보안 및 성능을 제공합니다.

다음 표에서는 ECC 및 RSA의 키 크기와 보안 수준을 비교합니다.

ECC 키 크기**(**비트**)**	**RSA** 키 크기**(**비트**)**
160	1024
224	2048
256	3072
384	7680
521	15360

키 크기가 더 작기 때문에 암호화가 더 빠릅니다.

Cisco ISE는 다음과 같은 ECC 커브 유형을 지원합니다. 커브 유형 또는 키 크기가 클수록 보안이 우수합니다.

- P-192
- P-256
- P-384
- P-521

ISE는 인증서의 EC 부분에서 명시적 매개변수를 지원하지 않습니다. 명시적 매개변수를 사용하여 인증서를 가져오려고 하면 Validation of certificate failed: Only named ECParameters(인증서 검증 실패: 명명된 EC 매개변수만 지원됨)라는 오류가 표시됩니다.

Cisco ISE CA 서비스는 BYOD 플로우를 통해 연결하는 디바이스용 ECC 인증서를 지원합니다. 인증서 프로비저닝 포털에서 ECC 인증서를 생성할 수도 있습니다.

참고 다음 표에는 ECC를 사용할 수 있는 운영체제 및 버전이 지원되는 커브 유형과 함께 나와 있습니다. 디바이스가 지원되는 운영체제를 실행하고 있지 않거나 지원되는 버전에서 실행되고 있지 않은 경우에는 RSA 기반 인증서를 대신 사용할 수 있습니다.

Operating System(운영 체제**)**	지원되는 버전	지원되는 커브 유형
Windows	8 이상	P-256, P-384 및 P-521
Android	4.4 이상 참고 Android 6.0에서 ECC 인증서를 지원하려면 2016년 5월 패치가 필요합니다.	모든 커브 유형(Android 6.0은 P-192 커브 유형을 지원하지 않으므로 제외).

Windows 7 및 Apple iOS는 기본적으로 EAP-TLS를 통한 인증에 ECC를 지원하지 않습니다. Cisco ISE의 이 릴리스에서는 MAC OS X 디바이스에서 ECC 인증서 사용을 지원하지 않습니다.

EST(Enrollment over Secure Transport) 프로토콜을 사용하는 BYOD 플로우가 정상적으로 작동하지 않으면 다음 사항을 확인하십시오.

- 인증서 서비스 엔드포인트 하위 CA 인증서 체인이 완료 되었습니다. 인증서 체인이 완료되었는지 확인하려면 다음을 수행합니다.
  1. **Administration(**관리**) > System(**시스템**) > Certificates(**인증서**) > Certificate Authority(**인증 기관**) > Certificate Authority Certificates(**인증 기관 인증서**)**를 선택합니다.
  2. 확인할 인증서 옆의 확인란을 선택하고 **View(**보기**)**를 클릭합니다.
- CA 및 EST 서비스가 작동되어 실행 중인지 확인합니다. 서비스가 실행되지 않으면 **Administration(**관리**) > System(**시스템**) > Certificates(**인증서**) > Certificate Authority(**인증 기관**) > Internal CA Settings(**내부 **CA** 설정**)**로 이동하여 CA 서비스를 활성화합니다.
- 2.0 이전의 ISE 버전에서 Cisco ISE 2.x로 업그레이드한 경우 업그레이드 후에 ISE 루트 CA 인증서 체인을 교체합니다. 방법은 다음과 같습니다.
  1. **Administration(**관리**) > System(**시스템**) > Certificates(**인증서**) > Certificate Management(**인증서 관리**) > Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.
  2. **Generate Certificate Signing Requests (CSR)(CSR** 생성**)**를 클릭합니다.
  3. Choose ISE Root CA from one or more Certificates(하나 이상의 인증서에서 ISE 루트 CA 선택)는 드롭다운 목록에 사용됩니다.
  4. **Replace ISE Root CA Certificate Chain(ISE** 루트 **CA** 인증서 체인 교체**)**을 클릭합니다.

참고 이 Cisco ISE 릴리스에서는 EST 클라이언트가 Cisco ISE 내에 있는 EST 서버에 대해 직접 인증하는 것을 지원하지 않습니다.

Android 또는 Windows 엔드포인트를 온보딩하는 동안 ECC 기반 인증서에 대한 요청이 있는 경우 ISE는 EST 플로우를 트리거합니다.

Cisco ISE 인증 기관 인증서

CA(인증기관) 인증서 페이지에는 내부 Cisco ISE CA와 관련된 모든 인증서가 나열됩니다. 이전 릴리스에서 이러한 CA 인증서는 Trusted Certificates(신뢰할 수 있는 인증서) 저장소에서 제공되었지만 이제는 CA Certificates(CA 인증서) 페이지로 이동되었습니다. 이러한 인증서는 이 페이지에 노드별로 나열됩니다. 노드를 펼쳐서 해당 특정 노드의 모든 ISE CA 인증서를 확인할 수 있습니다. 기본 및 보조 관리 노드에는 루트 CA, 노드 CA, 하위 CA 및 OCSP 응답자 인증서가 있습니다. 구축의 다른 노드에는 엔드포인트 하위 CA 및 OCSP 인증서가 있습니다.

Cisco ISE CA 서비스를 활성화하면 이러한 인증서가 생성되어 모든 노드에 자동으로 설치됩니다. 또한 전체 ISE 루트 CA 체인을 교체하면 이러한 인증서가 재생성되어 모든 노드에 자동으로 설치됩니다. 수동 개입이 필요하지 않습니다.

Cisco ISE CA 인증서는 **Certificate Services** <***Endpoint Sub CA/Node CA/Root CA/OCSP Responder***>-<*node_hostname*>#*certificate_number* 명명 규칙을 따릅니다.

CA 인증서 페이지에서 Cisco ISE CA 인증서의 편집, 가져오기, 내보내기, 삭제 및 보기가 가능합니다.

Cisco ISE CA 인증서 편집

Cisco ISE CA 인증서 저장소에 인증서를 추가한 뒤에는 설정 편집을 사용하여 추가로 편집할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Authority Certificates(**인증 기관 인증서**)**를 선택합니다. .

단계 **2** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 를 선택합니다.

단계 **3** 편집할 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** 편집 가능한 필드를 필요한 대로 수정합니다. 필드에 대한 설명은 신뢰할 수 있는 인증서 설정을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭하여 인증서 저장소에 대한 변경사항을 저장합니다.

Cisco ISE CA 인증서 내보내기

Cisco ISE 루트 CA 및 노드 CA 인증서를 내보내려면 다음을 수행합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 1 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Authority Certificates(**인증 기관 인증서**)**를 선택합니다.

단계 2 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 3 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다. 인증서는 한 번에 하나씩만 내보낼 수 있습니다.

단계 4 클라이언트 브라우저를 실행 중인 파일 시스템에 프라이버시가 강화된 메일 파일을 저장합니다.

Cisco ISE CA 인증서 가져오기

엔드포인트가 다른 의 Cisco ISE CA에서 발급한 인증서를 사용하여 네트워크에 인증하려고 하는 경우에는 해당 구축의 Cisco ISE 루트 CA, 노드 CA 및 엔드포인트 하위 CA 인증서를 Cisco ISE 신뢰할 수 있는 인증서 저장소로 가져와야 합니다.

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- 엔드포인트 인증서가 서명된 구축에서 ISE 루트 CA, 노드 CA 및 엔드포인트 하위 CA 인증서를 내보낸 다음 브라우저를 실행 중인 컴퓨터의 파일 시스템에 저장합니다.

단계 1 엔드포인트가 인증되는 구축의 관리 포털에 로그인합니다.

단계 2 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 3

단계 4 **Import(**가져오기**)**를 클릭합니다.

단계 5 필요한 대로 필드 값을 구성합니다. 자세한 내용은 신뢰할 수 있는 인증서 가져오기 설정을 참조하십시오.

클라이언트 인증서 기반 인증이 활성화되어 있으면 Cisco ISE는 구축의 각 노드에서 애플리케이션 서버를 다시 시작합니다. 이때 PAN에서 애플리케이션 서버부터 시작한 다음 각 추가 노드의 애플리케이션 서버를 하나씩 시작합니다.

인증서 템플릿

인증서 템플릿은 해당 템플릿을 기준으로 CA(Certificate Authority)에서 발급한 모든 인증서에 일반적인 속성을 포함합니다. 인증서 템플릿은 사용해야 하는 주체, SAN(Subject Alternative Name), 키 크기, SCEP RA 프로파일, 인증서의 유효 기간, 그리고 클라이언트 또는 서버 인증이나 두 인증에 모두 인증서를 사용해야 하는지 여부를 지정하는 EKU(Extended Key Usage: 확장 키 사용)를 정의합니다. 내

부 Cisco ISE CA(ISE CA)는 인증서 템플릿을 사용하여 해당 템플릿을 기준으로 인증서를 발급합니다.

Cisco ISE에서는 다음과 같은 ISE CA용 기본 인증서 템플릿이 제공됩니다. 필요한 경우 추가 인증서 템플릿을 생성할 수 있습니다. 기본 인증서 템플릿은 다음과 같습니다.

- CA_SERVICE_Certificate_Template - ISE CA(Certificate Authority)를 사용하는 기타 네트워크 서비스용입니다. 예를 들어 ASA VPN 사용자를 위한 인증서를 발급하도록 ISE를 구성하는 동안 이 인증서 템플릿을 사용합니다. 이 인증서 템플릿에서는 유효 기간만 수정할 수 있습니다.
- EAP_Authentication_Certificate_Template - EAP 인증용입니다.
- pxGrid_Certificate_Template - Certificate Provisioning Portal(인증서 프로비저닝 포털)에서 인증서를 생성하는 동안 pxGrid 컨트롤러에 사용됩니다.

인증서 템플릿 이름 익스텐션

Cisco ISE 내부 CA에는 엔드포인트 인증서를 생성하는 데 사용된 인증서 템플릿을 나타내는 익스텐션이 포함되어 있습니다. 내부 CA에서 발급한 모든 엔드포인트 인증서에는 인증서 템플릿 이름 익스텐션이 포함됩니다. 이 익스텐션은 해당 엔드포인트 인증서를 생성하는 데 사용된 인증서 템플릿을 나타냅니다. 익스텐션 ID는 1.3.6.1.4.1.9.21.2.5입니다. 권한 부여 정책 조건에서 CERTIFICATE: Template Name(인증서: 템플릿 이름) 속성을 사용하여 평가 결과에 따라 적절한 액세스 권한을 할당할 수 있습니다.

권한 부여 정책 조건에서 인증서 템플릿 이름 사용

권한 부여 정책 규칙에서 인증서 템플릿 이름 익스텐션을 사용할 수 있습니다.

단계 **1** **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택하고 기본 정책 집합을 확장하여 권한 부여 정책 규칙을 확인합니다.

단계 **2** 새 규칙을 추가하거나 기존 규칙을 편집합니다. 이 예에서는 Compliant_Device_Access 규칙 편집에 대해 설명합니다.

a) Compliant_Device_Access 규칙을 편집합니다.
b) **Add Attribute/Value(**속성/값 추가**)**를 선택합니다.
c) Dictionaries(사전)에서 **CERTIFICATE: Template Name(**인증서**:** 템플릿 이름**)** 속성과 **Equals(**같음**)** 연산자를 선택합니다.
d) 인증서 템플릿 이름의 값을 입력합니다. 예를 들어 EAP_Authentication_Certificate_Template을 입력합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

---

pxGrid 컨트롤러용 **Cisco ISE CA** 인증서 구축

Cisco ISE CA는 pxGrid 컨트롤러가 인증서 프로비저닝 포털에서 인증서를 생성하도록 인증서 템플릿을 제공합니다.

시작하기 전에

pxGrid 클라이언트용 CSR(Certificate Signing Request)을 생성하고 CSR의 내용을 클립보드에 복사합니다.

단계 **1** 네트워크 액세스 사용자 계정을 생성(Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자) > Add(추가))합니다.

사용자가 할당된 사용자 그룹을 적어 둡니다.

단계 **2** 인증서 프로비저닝 포털 설정을 편집(Administration(관리) > Device Portal Management(디바이스 포털 관리) > Certificate Provisioning(인증서 프로비저닝))합니다.

a) 인증서 프로비저닝 포털을 선택하고 **Edit(**편집**)**를 클릭합니다.

b) **Portal Settings(**포털 설정**)** 드롭다운 목록을 클릭합니다. 권한 부여된 그룹 구성의 사용 가능 목록에서 네트워크 액세스 사용자가 속하는 사용자 그룹을 선택하고 선택됨 목록으로 이동합니다.

c) **Certificate Provisioning Portal Settings(**인증서 프로비저닝 포털 설정**)** 드롭다운 목록을 클릭합니다. pxGrid_Certificate_Template을 선택합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 게스트 및 *BYOD*의 인증서 프로비저닝 포털 포털 설정 섹션을 참고하십시오.

d) 포털 설정을 저장합니다.

단계 **3** 인증서 프로비저닝 포털을 시작합니다. Portal Test URL(포털 테스트 URL) 링크를 클릭합니다.

a) 1단계에서 생성한 사용자 계정을 사용하여 인증서 프로비저닝 포털에 로그인합니다.

b) AUP를 수락하고 **Continue(**계속**)**를 클릭합니다.

c) **I want to(**수행할 작업**)** 드롭다운 목록에서 **Generate a single certificate (with certificate signing request)(**인증서 서명 요청을 사용하여 단일 인증서 생성**)**를 선택합니다.

d) Certificate Signing Request Details(인증서 서명 요청 세부정보) 필드에 클립보드의 CSR 내용을 붙여 넣습니다.

e) **Certificate Download Format(**인증서 다운로드 형식**)** 드롭다운 목록에서 **PKCS8 format(PKCS8** 형식**)**을 선택합니다.

참고 PKCS12 형식을 선택하는 경우 단일 인증서 파일을 별도의 인증서 및 키 파일로 변환해야 합니다. 인증서 및 키 파일은 이진 DER로 인코딩되거나 PEM 형식이어야만 Cisco ISE로 가져올 수 있습니다.

f) **Choose Certificate Template(**인증서 템플릿 선택**)** 드롭다운 목록에서 **pxGrid_Certificate_Template**을 선택합니다.

g) 인증서 비밀번호를 입력합니다.

h) **Generate(**생성**)**를 클릭합니다.

인증서가 생성됩니다.

i) 인증서를 내보냅니다.

인증서가 인증서 체인과 함께 내보내기됩니다.

단계 **4** pxGrid 클라이언트의 신뢰할 수 있는 인증서 저장소로 Cisco ISE CA 체인을 가져옵니다.

Simple Certificate Enrollment Protocol 프로파일

사용자가 네트워크에 등록할 수 있는 다양한 모바일 디바이스에 대한 인증서 프로비저닝 기능을 활성화하기 위해, Cisco ISE에서는 Cisco ISE가 여러 CA 위치를 가리키도록 하나 이상의 SCEP(Simple Certificate Enrollment Protocol) CA(Certificate Authority) 프로파일(Cisco ISE 외부 CA 설정이라고 함)을 구성할 수 있습니다. 여러 프로파일을 허용하는 경우의 이점은 고가용성을 보장하고 지정한 CA 위치 전체에서 로드 밸런싱을 수행할 수 있다는 것입니다. 특정 SCEP CA에 대한 요청이 3번 연속으로 응답이 없는 경우 Cisco ISE는 특정 서버가 사용 불가능하다고 선언하고 로드 및 응답 시간이 다음으로 가장 낮은 것으로 알려진 CA로 자동으로 전환합니다. 그런 다음 서버가 다시 온라인으로 복구되면 주기적 폴링을 시작합니다.

Cisco ISE와 상호 운용되도록 Microsoft SCEP 서버를 설정하는 방법에 대한 자세한 내용은

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf

를 참고해 주십시오.

Issued Certificates(발급된 인증서)

관리 포털은 내부 ISE CA에서 엔드포인트에 발급한 모든 인증서가 나열됩니다(Administration(관리) > System(시스템) > Certificates(인증서) > Endpoint Certificates(엔드포인트 인증서)). Issued Certificates(발급된 인증서) 페이지에서는 인증서 상태를 한 눈에 볼 수 있습니다. 인증서가 취소된 경우 상태 열 위에 마우스를 놓으면 취소 이유를 확인할 수 있습니다. Certificate Template(인증서 템플릿) 열 위에 마우스를 놓으면 인증서의키 유형, 키 크기 또는 커브 유형, 주체, SAN(Subject Alternative Name) 및 유효성과 같은 추가 세부정보를 볼 수 있습니다. 엔드포인트 인증서를 클릭하여 인증서를 볼 수 있습니다.

ISE CA에서 발급한 모든 인증서(BYOD 플로우를 통해 자동으로 프로비저닝된 인증서 및 인증서 프로비저닝 포털에서 가져온 인증서)는 Endpoint Certificates(엔드포인트 인증서) 페이지에 나열됩니다. 이 페이지에서 이러한 인증서를 관리할 수 있습니다.

예를 들어 user7에게 발급된 인증서를 보려면 Friendly Name(식별 이름) 필드 아래 표시되는 텍스트 상자에 user7을 입력합니다. 그러면 Cisco ISE에서 이 사용자에게 발급한 모든 인증서가 표시됩니다. 필터를 취소하려면 텍스트 상자에서 검색어를 제거합니다. 또한 고급 필터 옵션을 사용하여 다양한 검색 기준에 따라 기록을 볼 수도 있습니다.

이 엔드포인트 인증서 페이지에는 필요한 경우 엔드포인트 인증서를 취소할 수 있는 옵션도 제공됩니다.

인증서 관리 개요 페이지에는 구축 환경의 각 PSN 노드에서 발급된 총 엔드포인트 인증서 수가 표시됩니다. 노드별로 취소된 총 인증서 수와 실패한 총 인증서 수도 확인할 수 있습니다. 이 페이지에서 특정한 속성에 따라 데이터를 필터링할 수 있습니다.

발급 및 취소된 인증서

다음 표에서는 Overview of Issued and Revoked Certificates(발급 및 취소된 인증서 개요) 창의 필드에 대해 설명합니다. 구축의 PSN 노드는 엔드포인트에 인증서를 발급합니다. 이 창에서는 구축의 각 PSN 노드에서 발급한 엔드포인트 인증서 관련 정보를 제공합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Certificates(인증서)** > **Overview(개요)**입니다.

표 28: 발급 및 취소된 인증서

필드	사용 지침
Node Name(노드 이름)	인증서를 발급한 PSN(Policy Service Node)의 이름입니다.
Certificates Issued(발급된 인증서)	PSN 노드에서 발급한 엔드포인트 인증서의 수입니다.
Certificates Revoked(취소된 인증서)	취소된 엔드포인트 인증서의 수입니다(PSN 노드에서 발급한 인증서).
Certificates Requests(인증서 요청)	PSN 노드에서 처리한 인증서 기반 인증 요청 수입니다.
Certificates Failed(인증서 실패)	PSN 노드에서 처리한 인증 요청 중 실패한 인증 요청 수입니다.

관련 항목

Issued Certificates(발급된 인증서), 212 페이지
사용자 및 엔드포인트 인증서 갱신, 194 페이지
개인 디바이스 인증에 인증서를 사용하도록 Cisco ISE 구성, 216 페이지
사용자가 인증서를 갱신할 수 있도록 Cisco ISE 구성, 195 페이지
엔드포인트 인증서 취소, 234 페이지

Cisco ISE CA 인증서 및 키의 백업 및 복구

Cisco ISE CA 인증서 및 키를 안전하게 백업해야 PAN 장애 발생 시 외부 PKI의 루트 CA 또는 중간 CA로 작동하도록 보조 관리 노드를 승격시키려는 경우 보조 관리 노드에서 다시 복구할 수 있습니다. Cisco ISE 컨피그레이션 백업에는 CA 인증서 및 키가 포함되지 않습니다. 대신 CLI(Command Line Interface)를 사용하여 CA 인증서 및 키를 저장소로 내보냈다가 가져와야 합니다. **application configure ise** 명령에는 이제 CA 인증서 및 키를 백업하고 복원할 수 있는 Export(내보내기) 및 Import(가져오기) 옵션이 포함되어 있습니다.

신뢰할 수 있는 인증서 저장소의 다음 인증서가 보조 관리 노드에서 복원됩니다.

- Cisco ISE 루트 CA 인증서
- Cisco ISE 하위 CA 인증서
- Cisco ISE 엔드포인트 RA 인증서
- Cisco ISE OCSP Responder 인증서

다음과 같은 경우에 Cisco ISE CA 인증서 및 키를 백업하고 복원해야 합니다.

- 구축 환경에 보조 관리 노드가 있는 경우
- 전체 Cisco ISE CA 루트 체인을 바꾸는 경우

- 외부 PKI의 하위 CA 역할을 하도록 Cisco ISE 루트 CA를 구성하는 경우
- 릴리스 1.2에서 이후 릴리스로 업그레이드하는 경우
- 컨피그레이션 백업에서 데이터를 복원하는 경우 (이 경우에는 먼저 Cisco ISE CA 루트 체인을 다시 생성한 다음, ISE CA 인증서 및 키를 백업하고 복원해야 합니다.)

참고 구축에서 Cisco ISE 내부 CA를 교체할 때마다 ISE 메시징 서비스도 업데이트해야 전체 인증서 체인을 검색할 수 있습니다.

Cisco ISE CA 인증서 및 키 내보내기

PAN에서 CA 인증서 및 키를 내보내야 보조 관리 노드에서 해당 인증서와 키를 가져올 수 있습니다. 이 옵션을 사용하는 경우 PAN이 다운되면 보조 관리 노드가 엔드포인트에 대해 인증서를 발급하고 관리할 수 있으며, 이 경우 보조 관리 노드를 PAN으로 승격합니다.

시작하기 전에

CA 인증서와 키를 저장할 저장소를 생성했는지 확인합니다.

단계 **1** Cisco ISE CLI에서 **application configure ise** 명령을 입력합니다.

단계 **2** 7을 입력하여 인증서와 키를 내보냅니다.

단계 **3** 저장소 이름을 입력합니다.

단계 **4** 암호화 키를 입력합니다.

내보내진 인증서 목록 및 주체, 발급자, 일련 번호가 포함된 성공 메시지가 나타납니다.

예제**:**

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

Cisco ISE CA 인증서 및 키 가져오기

보조 관리 노드를 등록한 후에는 PAN에서 CA 인증서와 키를 내보낸 다음 보조 관리 노드로 가져와야 합니다.

단계 **1** Cisco ISE CLI의 **application configure ise** 명령을 입력합니다.

단계 **2** CA 인증서와 키를 가져오려면 8을 입력합니다.

단계 **3** 저장소 이름을 입력합니다.

단계 **4** 가져올 파일의 이름을 입력합니다. 파일 이름은 **ise_ca_key_pairs_of_<vm hostname>** 형식이 되어야 합니다.

단계 **5** 파일 암호를 해독할 암호화 키를 입력합니다.

성공 메시지가 나타납니다.

예제**:**

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

참고 내 보낸 키 파일의 암호화는 Cisco ISE 릴리스 2.6에 도입되었습니다. Cisco ISE 릴리스 2.4 이하 버전에서 키를 내보내고 Cisco ISE 릴리스 2.6 이상 버전에서 키를 가져오면 성공하지 못합니다.

기본 PAN 및 PSN에서 루트 CA 및 하위 CA 생성

구축을 설정할 때 Cisco ISE는 Cisco ISE CA 서비스용으로 기본 PAN에 루트 CA를 생성하고 PSN에 하위 CA 인증서를 생성합니다. 그러나 기본 PAN 또는 PSN의 도메인 이름이나 호스트 이름을 변경할 때는 기본 PAN에서 루트 CA를, PSN에서 하위 CA를 각각 재생성해야 합니다.

PSN에서 호스트 이름을 변경하려는 경우에는 기본 PAN과 PSN에서 각각 루트 CA와 하위 CA를 재생성하는 대신 호스트 이름을 변경하기 전에 PSN 등록을 취소했다가 변경 후 다시 등록할 수 있습니다. 그러면 새 하위 인증서가 PSN에 자동으로 프로비저닝됩니다.

단계 1 를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**.

단계 2 **Generate Certificate Signing Requests (CSR)(CSR** 생성**)**를 클릭합니다.

단계 3 **Certificate(s) will be used for(**인증서 사용 대상**)** 드롭다운 목록에서 ISE Root CA(ISE 루트 CA)를 선택합니다.

단계 4 **Replace ISE Root CA Certificate chain(ISE** 루트 **CA** 인증서 체인 교체**)**을 클릭합니다.

루트 CA 및 하위 CA 인증서가 구축의 모든 노드에 대해 생성됩니다.

외부 PKI의 하위 CA로 Cisco ISE 루트 CA 구성

기본 PAN의 루트 CA가 외부 PKI의 하위 CA로 작동하도록 하려면 ISE 중간 CA 인증서 서명 요청을 생성하여 외부 CA로 보낸 다음 루트 및 CA 서명 인증서를 받습니다. 그런 다음 루트 CA 인증서는 신뢰할 수 있는 인증서 저장소로 가져오고 CA 서명 인증서는 CSR에 바인딩합니다. 이 경우 외부 CA는 루트 CA이고 기본 PAN은 외부 CA의 하위 CA이며 PSN은 기본 PAN의 하위 CA입니다.

단계 1 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

단계 2 **Generate Certificate Signing Requests (CSR)(CSR** 생성**)**를 클릭합니다.

단계 3 **Certificate(s) will be used for(**인증서 사용 대상**)** 드롭다운 목록에서 ISE Intermediate CA(ISE 중간 CA)를 선택합니다.

단계 4 **Generate(**생성**)**를 클릭합니다.

단계 5 CSR을 내보내 외부 CA로 보낸 다음 CA 서명 인증서를 받습니다.

단계 6 외부 CA의 루트 CA 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다.

단계 7 CA 서명 인증서를 CSR에 바인딩합니다.

다음에 수행할 작업

구축에 보조 PAN이 있는 경우 기본 PAN에서 Cisco ISE CA 인증서와 키의 백업을 가져온 다음 보조 PAN에서 복원합니다. 그러면 서버 및 루트 인증서가 보조 PAN에 자동으로 복제됩니다. 그러면 관리 노드 장애 시 보조 PAN이 외부 PKI의 하위 CA로 작동할 수 있습니다.

개인 디바이스 인증에 인증서를 사용하도록 Cisco ISE 구성

네트워크에 연결하는 엔드포인트(개인 디바이스)용 인증서를 발급하고 관리하도록 Cisco ISE를 구성할 수 있습니다. 내부 Cisco ISE CA 서비스를 사용하여 엔드포인트에서 CSR(Certificate Signing Request)에 서명을 하거나 CSR을 외부 CA에 전달할 수 있습니다.

시작하기 전에

- 기본 PAN에서 Cisco ISE CA 인증서와 키의 백업을 받아 재해 복구용으로 안전한 위치에 저장합니다.

단계 **1** 직원 사용자 그룹에 사용자 추가, 217 페이지

내부 ID 저장소 또는 Microsoft Active Directory 등의 외부 ID 저장소에 사용자를 추가할 수 있습니다.

단계 **2** TLS 기반 인증용 인증서 인증 프로파일 생성, 218 페이지

단계 **3** TLS 기반 인증용 인증서 ID 소스 시퀀스 생성, 218 페이지

단계 **4** 클라이언트 프로비저닝 정책을 생성합니다.

a) 인증 기관 설정 구성, 219 페이지
b) CA 템플릿 생성, 220 페이지
c) 클라이언트 프로비저닝 정책에서 사용할 기본 신청자 프로파일 생성, 222 페이지
d) Cisco 사이트에서 Windows 및 MAC OS X 운영체제용 에이전트 리소스 다운로드, 223 페이지
e) Apple iOS, Android 및 MACOSX 디바이스용 클라이언트 프로비저닝 정책 규칙 생성, 224 페이지

단계 **5** TLS 기반 인증용 Dot1X 인증 정책 규칙 구성, 224 페이지

단계 **6** TLS 기반 인증용 인증 정책 규칙을 구성합니다.

a) 중앙 웹 인증 및 신청자 프로비저닝 흐름용 권한 부여 프로파일 생성, 225 페이지
b) 권한 부여 정책 규칙 생성, 226 페이지

ECDHE-RSA 기반 인증서를 사용하는 경우 개인 디바이스에서 무선 SSID에 연결하는 동안 비밀번호를 다시 입력하라는 프롬프트가 표시됩니다.

직원 사용자 그룹에 사용자 추가

다음 절차에서는 Cisco ISE ID 저장소의 직원 사용자 그룹에 사용자를 추가하는 방법을 설명합니다. 외부 ID 저장소를 사용하는 경우에는 사용자를 추가할 수 있는 직원 사용자 그룹이 있는지 확인해 주십시오.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 사용자 세부정보를 입력합니다.

단계 **4** **Passwords(**비밀번호**)** 섹션에서 **Login Password(**로그인 비밀번호**)** 및 TACACS+ **Enable Password(**활성화 비밀번호**)**를 선택하여 네트워크 디바이스에 대한 액세스 레벨을 설정합니다.

단계 **5** 사용자 그룹 드롭다운 목록에서 Employee(직원)를 선택합니다.

직원 사용자 그룹에 속하는 모든 사용자는 동일한 권한 집합을 공유합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

TLS 기반 인증용 인증서 인증 프로파일 생성, 218 페이지

TLS 기반 인증용 인증서 인증 프로파일 생성

인증서를 사용하여 네트워크에 연결하는 엔드포인트를 인증하려면 Cisco ISE에서 인증서 인증 프로파일을 정의하거나 기본 프로파일인 Preloaded_Certificate_Profile을 편집해야 합니다. 인증서 인증 프로파일에는 보안 주체 사용자 이름으로 사용해야 하는 인증서 필드가 포함됩니다. 예를 들어 Common Name(일반 이름) 필드에 사용자 이름이 포함되어 있으면 보안 주체 사용자 이름이 주체 - 일반 이름인 인증서 인증 프로파일을 정의할 수 있으며 이 이름을 ID 저장소에 대해 확인할 수 있습니다.

단계 1 **Administration(관리)** > **Identity Management(ID 관리)** > **External Identity Sources(외부 ID 소스)** > **Certificate Authentication Profile(인증서 인증 프로파일)**을 선택합니다.

단계 2 인증서 인증 프로파일의 이름을 입력합니다. 예를 들어 CAP 등을 입력할 수 있습니다.

단계 3 주체 - 일반 이름을 **Principal Username X509 Attribute(보안 주체 사용자 이름 X509 속성)**로 선택합니다.

단계 4 **Save(저장)**를 클릭합니다.

다음에 수행할 작업

TLS 기반 인증용 인증서 ID 소스 시퀀스 생성, 218 페이지

TLS 기반 인증용 인증서 ID 소스 시퀀스 생성

인증서 인증 프로파일을 생성한 후에는 Cisco ISE가 인증서에서 속성을 가져온 다음 ID 소스 시퀀스에서 정의한 ID 소스와 해당 속성이 일치하는지를 확인할 수 있도록 ID 소스 시퀀스에 해당 프로파일을 추가해야 합니다.

시작하기 전에

다음 작업을 완료했는지 확인합니다.

- 직원 사용자 그룹에 사용자 추가
- 인증서 기반 인증용 인증서 인증 프로파일 생성

단계 1 **Administration(관리)** > **Identity Management(ID 관리)** > **Identity Source Sequences(ID 소스 시퀀스)**를 선택합니다.

단계 2 **Add(추가)**를 클릭합니다.

단계 3 ID 소스 시퀀스의 이름을 입력합니다. 예를 들어 Dot1X와 같이 입력할 수 있습니다.

단계 4 **Select Certificate Authentication Profile(인증서 인증 프로파일 선택)** 확인란을 선택하고 이전에 생성한 인증서 인증 프로파일(CAP)을 선택합니다.

단계 5 사용자 정보가 포함된 ID 소스를 인증 검색 목록 영역의 **Selected(선택됨)** 목록 상자로 이동합니다.

ID 소스를 더 추가할 수 있으며, 그러면 Cisco ISE는 일치하는 항목을 찾을 때까지 이러한 데이터 저장소를 순차적으로 검색합니다.

단계 **6** **Treat as if the user was not found and proceed to the next store in the sequence(**사용자를 찾지 못한 것으로 간주하여 다음 저장소로 순차 진행**)** 라디오 버튼을 클릭합니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

인증 기관 설정 구성, 219 페이지

인증 기관 설정 구성

외부 CA를 사용하여 CSR에 서명을 하려는 경우 외부 CA 설정을 구성해야 합니다. Cisco ISE의 이전 릴리스에서는 외부 CA 설정의 명칭이 SCEP RA 프로파일이었습니다. Cisco ISE CA를 사용하는 경우에는 CA 설정을 명시적으로 구성할 필요가 없습니다. Administration(관리) > System(시스템) > Certificates(인증서) > Internal CA Settings(내부 CA 설정)에서 내부 CA 설정을 검토할 수 있습니다.

사용자 디바이스가 수신한 검증된 인증서는 다음 표에서 설명하는 것처럼 디바이스에 상주하게 됩니다.

표 ***29:*** 디바이스 인증서 위치

디바이스	인증서 저장 위치	액세스 방법
iPhone/iPad	표준 인증서 저장소	Settings(설정) > General(일반) > Profile(프로파일)
Android	암호화된 인증서 저장소	최종 사용자에게 표시되지 않습니다. 참고 Settings(설정) > Location & Security(위치 및 보안) > Clear Storage(저장소 지우기)를 사용하면 인증서를 제거할 수 있습니다.
Windows	표준 인증서 저장소	**/cmd** 프롬프트에서 mmc.exe를 시작하거나 인증서 스냅인에서 확인합니다.
Mac	표준 인증서 저장소	Application(애플리케이션) > Utilities(유틸리티) > Keychain Access(키 체인 액세스)

시작하기 전에

외부 CA(Certificate Authority)를 사용하여 CSR(Certificate Signing Request)에 서명을 하려는 경우에는 외부 CA의 URL이 있어야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **External CA Settings(**외부 **CA** 설정**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 외부 CA 설정의 이름을 입력합니다. EXTERNAL_SCEP 등을 예로 들 수 있습니다.

단계 **4** URL 텍스트 상자에 외부 CA 서버 URL을 입력합니다.

Test Connection(연결 테스트**)**을 클릭하여 외부 CA에 연결할 수 있는지 확인합니다. 추가 CA 서버 URL을 입력하려면 + 버튼을 클릭합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

CA 템플릿 생성, 220 페이지

CA 템플릿 생성

인증서 템플릿은 내부 또는 외부 CA에 대해 사용해야 하는 SCEP RA 프로파일, 키 유형, 키 크기 또는 커브 유형,주체, SAN(Subject Alternative Name), 인증서의 유효 기간 및 확장 키 사용을 정의합니다. 이 예제에서는 내부 Cisco ISE CA를 사용한다고 가정합니다. 외부 CA 템플릿의 경우 유효 기간은 외부 CA에 의해 결정되며 지정할 수 없습니다.

새 CA 템플릿을 생성할 수도 있고 기본 인증서 템플릿인 EAP_Authentication_Certificate_Template을 편집할 수도 있습니다.

기본적으로 Cisco ISE에서는 다음 CA 템플릿을 사용할 수 있습니다.

- CA_SERVICE_Certificate_Template - ISE CA를 사용하는 기타 네트워크 서비스용입니다. 예를 들어 ASA VPN 사용자를 위한 인증서를 발급하도록 ISE를 구성하는 동안 이 인증서 템플릿을 사용합니다.
- EAP_Authentication_Certificate_Template - EAP 인증용입니다.
- pxGrid_Certificate_Template—Certificate Provisioning Portal(인증서 프로비저닝 포털)에서 인증서를 생성하는 동안 pxGrid 컨트롤러에 사용됩니다.

참고 ECC 키 유형을 사용하는 인증서 템플릿은 내부 Cisco ISE CA에서만 사용할 수 있습니다.

시작하기 전에

CA 설정을 구성했는지 확인합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **CA Service(CA** 서비스**)** > **Internal CA Certificate Template(**내부 **CA** 인증서 템플릿**)**을 선택합니다.

단계 **2** 내부 CA 템플릿의 이름을 입력합니다. 예를 들어 Internal_CA_Template과 같이 입력할 수 있습니다.

단계 **3** (선택 사항) Organizational Unit(조직 단위), Organization(조직), City(구/군/시), State(시/도) 및 Country(국가) 필드에 값을 입력합니다.

UTF-8 문자는 인증서 템플릿 필드(조직 단위, 조직, 구/군/시, 시/도 및 국가)에서 지원되지 않습니다. 인증서 템플릿에 UTF-8 문자를 사용하면 인증서 프로비저닝이 실패합니다.

인증서를 생성하는 내부 사용자의 사용자 이름이 인증서의 공용 이름으로 사용됩니다. Cisco ISE 내부 CA는 Common Name(공용 이름) 필드에서 "+" 또는 "*" 문자를 지원하지 않습니다. 사용자 이름에는 특수 문자 "+" 또는 "*"가 포함되어 있지 않아야 합니다.

단계 **4** 인증서의 유효 기간과 SAN(Subject Alternative Name)을 지정합니다.

단계 **5** 키 유형을 지정합니다. RSA 또는 ECC를 선택합니다.

다음 표에는 ECC를 지원하는 운영체제 및 버전과 지원되는 커브 유형이 나열되어 있습니다. 디바이스가 지원되는 운영체제를 실행하고 있지 않거나 지원되는 버전에서 실행되고 있지 않은 경우에는 RSA 기반 인증서를 대신 사용할 수 있습니다.

Operating System(운영체제**)**	지원되는 버전	지원되는 커브 유형
Windows	8 이상	P-256, P-384 및 P-521
Android	4.4 이상 참고 Android 6.0에서 ECC 인증서를 지원하려면 2016년 5월 패치가 필요합니다.	모든 커브 유형(Android 6.0은 P-192 커브 유형을 지원하지 않으므로 제외).

Windows 7 및 Apple iOS는 기본적으로 EAP-TLS 인증에 ECC를 지원하지 않습니다. Cisco ISE의 이 릴리스에서는 MAC OS X 디바이스에서 ECC 인증서 사용을 지원하지 않습니다.

네트워크의 디바이스가 지원되지 않는 운영체제(Windows 7, MAC OS X 또는 Apple iOS)를 실행하는 경우에는 키 유형으로 RSA를 선택하는 것이 좋습니다.

단계 **6** (RSA 키 유형을 선택하는 경우에 해당함) 키 크기를 지정합니다. 1024 이상의 키 크기를 선택해야 합니다.

단계 **7** (ECC 키 유형을 선택하는 경우에만 해당함) 커브 유형을 지정합니다. 기본 값은 P-384 입니다.

단계 **8** ISE Internal CA를 SCEP RA 프로파일로 선택합니다.

단계 **9** 유효 기간을 일 단위로 입력합니다. 기본값은 730일입니다. 유효 범위는 1~730입니다.

단계 **10** 확장 키 사용을 지정합니다. 클라이언트 인증에 인증서를 사용하려면 **Client Authentication(**클라이언트 인증**)** 확인란을 선택합니다. 서버 인증에 인증서를 사용하려면 **Server Authentication(**서버 인증**)** 확인란을 선택합니다.

단계 **11** **Submit(**제출**)**을 클릭합니다.

내부 CA 인증서 템플릿이 생성되어 클라이언트 프로비저닝 정책에 사용됩니다.

다음에 수행할 작업

클라이언트 프로비저닝 정책에서 사용할 기본 신청자 프로파일 생성, 222 페이지

내부 CA 설정

다음 표에서는 내부 CA 설정 창의 필드에 대해 설명합니다. 이 창에서 내부 CA 설정을 확인하고 내부 CA 서비스를 비활성화할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Certificates(인증서)** > **Certificate Authority(인증 기관)** > **Internal CA Settings(내부 CA 설정)**입니다.

표 *30:* 내부 *CA* 설정

필드 이름	사용 지침
Disable Certificate Authority(인증 기관 비활성화)	내부 CA 서비스를 비활성화하려면 이 버튼을 클릭합니다.
Host Name(호스트 이름)	CA 서비스를 실행 중인 Cisco ISE 노드의 호스트 이름입니다.
Personas(역할 분담)	CA 서비스를 실행 중인 노드에서 활성화된 Cisco ISE 노드 페르소나입니다. Administration(관리), Policy Service(정책 서비스) 등을 예로 들 수 있습니다.
Role(s)(역할)	CA 서비스를 실행 중인 Cisco ISE 노드에 지정된 역할입니다. Standalone(독립형), Primary(기본), Secondary(보조) 등을 예로 들 수 있습니다.
CA, EST & OCSP Responder Status(CA, EST 및 OCSP 응답기 상태)	Enabled(활성화됨) 또는 Disabled(비활성화됨)입니다.
OCSP Responder URL(OCSP 응답기 URL)	OCSP 서버에 액세스하는 Cisco ISE 노드의 URL입니다.
SCEP URL	SCEP 서버에 액세스하는 Cisco ISE 노드의 URL입니다.

관련 항목

Cisco ISE CA 서비스, 199 페이지
개인 디바이스 인증에 인증서를 사용하도록 Cisco ISE 구성, 216 페이지

클라이언트 프로비저닝 정책에서 사용할 기본 신청자 프로파일 생성

사용자가 회사 네트워크에서 개인 디바이스를 사용할 수 있도록 기본 신청자 프로파일을 생성할 수 있습니다. Cisco ISE는 각 운영체제에 대해 서로 다른 정책 규칙을 사용합니다. 각 클라이언트 프로비

저닝 정책 규칙에는 기본 신청자 프로파일이 포함되어 있으며, 이 프로파일은 각 운영체제에 대해 사용할 프로비저닝 마법사를 지정합니다.

시작하기 전에

- Cisco ISE에서 CA 인증서 템플릿을 구성합니다.
- TCP 포트 8905 및 UDP 포트 8905를 열어 클라이언트 에이전트 및 supplicant 프로비저닝 마법사 설치를 활성화합니다. 포트 사용에 대한 자세한 내용은 *Cisco Identity Services Engine* 하드웨어 설치 설명서에서 "Cisco ISE 어플라이언스 포트 참조" 부록을 참고하십시오.

단계 **1** **Policy**(정책) > **Policy Elements**(정책 요소) > **Results**(결과) > **Client Provisioning**(클라이언트 프로비저닝) > **Resources**(리소스)를 선택합니다.

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

단계 **3** 기본 신청자 프로파일의 이름을 입력합니다. 예를 들어 EAP_TLS_INTERNAL과 같이 입력할 수 있습니다.

단계 **4** **Operating System**(운영체제) 드롭다운 목록에서 ALL(모두)을 선택합니다.

참고 MAC OS 버전 10.10 사용자는 듀얼 SSID PEAP 플로우용으로 프로비저닝된 SSID에 수동으로 연결해야 합니다.

단계 **5** **Wired**(유선) 또는 **Wireless**(무선) 확인란을 선택합니다.

단계 **6** **Allowed Protocol**(허용되는 프로토콜) 드롭다운 목록에서 TLS를 선택합니다.

단계 **7** 앞에서 생성한 CA 인증서 템플릿을 선택합니다.

단계 **8** **Submit**(제출)을 클릭합니다.

다음에 수행할 작업

Cisco 사이트에서 Windows 및 MAC OS X 운영체제용 에이전트 리소스 다운로드, 223 페이지

Cisco 사이트에서 Windows 및 MAC OS X 운영체제용 에이전트 리소스 다운로드

Windows 및 MAC OS X 운영체제의 경우에는 Cisco 사이트에서 원격 리소스를 다운로드해야 합니다.

시작하기 전에

네트워크의 프록시 설정이 올바르게 구성되어 있는지 확인하여 Cisco ISE에 클라이언트 프로비저닝 리소스를 다운로드하기 위한 적절한 원격 위치에 액세스할 수 있는지 확인합니다.

단계 **1** **Policy**(정책) > **Policy Elements**(정책 요소) > **Resources**(리소스) > **Client Provisioning**(클라이언트 프로비저닝) > **Resources**(리소스)를 선택합니다.

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

단계 **3** **Windows** 및 **MAC OS X** 패키지 옆의 확인란을 선택합니다. 최신 버전을 포함해야 합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

Apple iOS, Android 및 MACOSX 디바이스용 클라이언트 프로비저닝 정책 규칙 생성, 224 페이지

Apple iOS, Android 및 MACOSX 디바이스용 클라이언트 프로비저닝 정책 규칙 생성

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

에이전트 규정 준수 모듈을 다운로드할 때는 항상 시스템에서 사용 가능한 기존 모듈(있는 경우)을 덮어씁니다.

직원이 iOS, Android 및 MACOSX 디바이스를 사용할 수 있도록 하려면 클라이언트 프로비저닝 정책 페이지에서 이러한 각 디바이스에 대해 정책 규칙을 생성해야 합니다.

시작하기 전에

클라이언트 프로비저닝 정책 페이지에서 필수 기본 신청자 프로파일을 구성하고 필수 에이전트를 다운로드해야 합니다.

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

단계 **2** Apple iOS, Android 및 MACOSX 디바이스용 클라이언트 프로비저닝 정책 규칙을 생성합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

TLS 기반 인증용 Dot1X 인증 정책 규칙 구성, 224 페이지

TLS 기반 인증용 Dot1X 인증 정책 규칙 구성

이 작업에서는 TLS 기반 인증에 대해 Dot1X 인증 정책 규칙을 업데이트하는 방법을 보여줍니다.

시작하기 전에

TLS 기반 인증용으로 인증서 인증 프로파일을 생성했는지 확인합니다.

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

단계 **2** **View(**보기**)** 열에서 화살표 › 아이콘을 클릭하여 Set view(보기 설정) 화면을 열어 인증 정책을 보고, 관리하고, 업데이트합니다.

기본 규칙 기반 인증 정책에는 Dot1X 인증용 규칙이 포함되어 있습니다.

단계 **3** Dot1X 인증 정책 규칙의 조건을 편집하려면 **Conditions(**조건**)** 열의 셀 위에 마우스를 올려놓고 아이콘을 클릭합니다. Condition Studio가 열립니다.

단계 **4** Dot1X 정책 규칙의 **Actions(**작업**)** 열에서 톱니바퀴 아이콘을 클릭한 다음, 드롭다운 메뉴에서 필요에 따라 Insert(삽입) 또는 Duplicate(중복) 옵션을 선택하여 새 정책 집합을 삽입합니다.
정책 집합 표에 새 행이 표시됩니다.

단계 **5** 규칙의 이름을 입력합니다. 예를 들어 eap-tls와 같이 입력할 수 있습니다.

단계 **6** **Conditions(**조건**)** 열에서 (+) 기호를 클릭합니다.

단계 **7** **Conditions Studio** 페이지에 필수 조건을 생성합니다. **Editor(**편집기**)** 섹션에서 **Click To Add an Attribute(**클릭하여 속성 추가**)** 텍스트 상자를 클릭하고 필요한 사전 및 속성(예: Network Access:UserName Equals User1)을 선택합니다.

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

단계 **8** **Use**를 클릭합니다.

단계 **9** 기본 규칙은 그대로 유지합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

중앙 웹 인증 및 신청자 프로비저닝 흐름용 권한 부여 프로파일 생성, 225 페이지

중앙 웹 인증 및 신청자 프로비저닝 흐름용 권한 부여 프로파일 생성

인증서 기반 인증이 성공한 후 사용자에게 부여해야 하는 액세스 권한을 결정하려면 권한 부여 프로파일을 정의해야 합니다.

시작하기 전에

WLC(Wireless LAN Controller)에서 필요한 ACL(Access Control Lists)을 구성했는지 확인합니다. WLC에서 ACL을 생성하는 방법에 대한 자세한 내용은 *TrustSec* 사용 방법 설명서*:* 구별된 액세스를 위해 인증서 사용을 참고해 주십시오.

이 예제에서는 WLC에서 다음 ACL을 생성했다고 가정합니다.

- NSP-ACL - 기본 신청자 프로비저닝용
- BLACKHOLE - 차단 목록에 포함된 디바이스에 대한 액세스 제한용
- NSP-ACL-Google - Android 디바이스 프로비저닝용

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

단계 **2** **Add(**추가**)**를 클릭하여 새 권한 부여 프로파일을 생성합니다.

단계 **3** 권한 부여 프로파일의 이름을 입력합니다.

단계 **4** **Access Type(**액세스 유형**)** 드롭다운 목록에서 ACCESS_ACCEPT를 선택합니다.

단계 **5** **Add(**추가**)**를 클릭하여 중앙 웹 인증용 권한 부여 프로파일, Google Play용 중앙 웹 인증, 기본 신청자 프로비저닝 및 Google용 기본 신청자 프로비저닝을 추가합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

권한 부여 정책 규칙 생성, 226 페이지

권한 부여 정책 규칙 생성

Cisco ISE는 권한 부여 정책 규칙을 평가하여 정책 규칙에 지정된 권한 부여 프로파일을 기준으로 사용자에게 네트워크 리소스 액세스 권한을 부여합니다.

시작하기 전에

필요한 권한 부여 프로파일을 생성했는지 확인합니다.

단계 **1** **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택하고 정책 집합을 확장하여 권한 부여 정책 규칙을 확인합니다.

단계 **2** 기본 규칙 위에 추가 정책 규칙을 삽입합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

CA 서비스 정책 참조

이 섹션에서는 Cisco ISE CA 서비스를 활성화하기 전에 먼저 생성해야 하는 권한 부여 및 클라이언트 프로비저닝 정책 규칙에 대한 참조 정보를 제공합니다.

인증서 서비스용 클라이언트 프로비저닝 정책 규칙

이 섹션에는 Cisco ISE 인증서 서비스를 사용하는 동안 생성해야 하는 클라이언트 프로비저닝 정책 규칙이 나와 있습니다. 다음 표에는 세부정보가 나와 있습니다.

규칙 이름	**ID** 그룹	운영체제	기타 조건	결과
iOS	모든	모든 Apple iOS	조건	EAP_TLS_INTERNAL(이전에 생성한 기본 신청자 프로파일). 외부 CA를 사용하는 경우 외부 CA에 대해 생성한 기본 신청자 프로파일을 선택합니다.

규칙 이름	ID 그룹	운영체제	기타 조건	결과
Android	모든	Android	조건	EAP_TLS_INTERNAL(이전에 생성한 기본 신청자 프로파일). 외부 CA를 사용하는 경우 외부 CA에 대해 생성한 기본 신청자 프로파일을 선택합니다.
MACOSX	모든	MACOSX	조건	Native Supplicant Configuration(기본 신청자 컨피그레이션)에서 다음을 지정합니다. 1. Config Wizard(컨피그레이션 마법사): Cisco 사이트에서 다운로드한 MACOSX 신청자 마법사를 선택합니다. 2. Wizard Profile(마법사 프로파일): 이전에 생성한 EAP_TLS_INTERNAL 기본 신청자 프로파일을 선택합니다. 외부 CA를 사용하는 경우 외부 CA에 대해 생성한 기본 신청자 프로파일을 선택합니다.

인증서 서비스용 권한 부여 프로파일

이 섹션에는 Cisco ISE에서 인증서 기반 인증을 활성화하기 위해 생성해야 하는 권한 부여 프로파일이 나와 있습니다. WLC(Wireless LAN Controller)에서 이미 ACL(NSP-ACL 및 NSP-ACL-Google)을 생성한 상태여야 합니다.

- CWA - 이 프로파일은 중앙 웹 인증 흐름을 진행하는 디바이스에 사용됩니다. **Web Authentication(**웹 인증**)** 확인란을 선택하고 드롭다운 목록에서 Centralized(중앙 집중식)를 선택하고 ACL 텍스트 상자에 NSP-ACL을 입력합니다.
- CWA_GooglePlay - 이 프로파일은 중앙 웹 인증 흐름을 진행하는 디바이스에 사용됩니다. 이 프로파일은 Android 디바이스가 Google Play 스토어에 액세스하고 Cisco Network Setup Assistant를 다운로드하도록 합니다. **Web Authentication(**웹 인증**)** 확인란을 선택하고 드롭다운 목록에서 Centralized(중앙 집중식)를 선택하고 ACL-Google 텍스트 상자에 NSP-ACL을 입력합니다.
- NSP - 이 프로파일은 신청자 프로비저닝 흐름을 진행하는, Android 이외의 디바이스에 사용됩니다. **Web Authentication(**웹 인증**)** 확인란을 선택하고 드롭다운 목록에서 Supplicant Provisioning(신청자 프로비저닝)을 선택하고 ACL 텍스트 상자에 NSP-ACL을 입력합니다.
- NSP-Google - 이 프로파일은 신청자 프로비저닝 흐름을 진행하는, Android 이외의 디바이스에 사용됩니다. **Web Authentication(**웹 인증**)** 확인란을 선택하고 드롭다운 목록에서 Supplicant Provisioning(신청자 프로비저닝)을 선택하고 ACL 텍스트 상자에 NSP-ACL-Google을 입력합니다.

기본 Blackhole_Wireless_Access 권한 부여 프로파일을 검토합니다. 필수적인 고급 속성 설정은 다음과 같습니다.

- Cisco:cisco-av-pair = url-redirect=https://*ip:port*/blockedlistportal/gateway?portal=*PortalID*
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

인증서 서비스용 권한 부여 정책 규칙

이 섹션에는 Cisco ISE CA 서비스를 활성화하는 동안 생성해야 하는 권한 부여 정책 규칙이 나와 있습니다.

- 기업 자산 - 이 규칙은 802.1X 및 MSCHAPV2 프로토콜을 사용하여 회사 무선 SSID에 연결되는 회사 디바이스에 사용됩니다.
- Android_SingleSSID - 이 규칙은 Google Play 스토어에 액세스하여 프로비저닝용 Cisco Network Setup Assistant를 다운로드하는 Android 디바이스에 사용됩니다. 이 규칙은 단일 SSID 설정과 관련이 있습니다.
- Android_DualSSID - 이 규칙은 Google Play 스토어에 액세스하여 프로비저닝용 Cisco Network Setup Assistant를 다운로드하는 Android 디바이스에 사용됩니다. 이 규칙은 이중 SSID 설정과 관련이 있습니다.
- CWA - 이 규칙은 중앙 웹 인증 흐름을 진행하는 디바이스에 사용됩니다.
- NSP - 이 규칙은 EAP-TLS 인증에 인증서를 사용하여 기본 신청자 프로비저닝 흐름을 진행하는 디바이스에 사용됩니다.
- EAP-TLS - 이 규칙은 신청자 프로비저닝 흐름을 완료하고 인증서로 프로비저닝된 디바이스에 사용됩니다. 네트워크에 대한 액세스가 부여됩니다.

다음 표에는 Cisco ISE CA 서비스에 대한 권한 부여 정책 규칙을 구성하면서 선택해야 하는 속성 및 값이 나와 있습니다. 이 예에서는 Cisco ISE에서 해당 권한 부여 프로파일을 구성했다고 가정합니다.

규칙 이름	조건	권한(적용될 권한 부여 프로파일)
기업 자산	Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	PermitAccess
Android_SingleSSID	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	NSP_Google
Android_DualSSID	(Wireless_MAB AND Session:Device-OS EQUALS Android)	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	NSP
EAP-TLS	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI	PermitAccess

ASA VPN 사용자에 대한 ISE CA의 인증서 발급

ISE CA는 ASA VPN을 통해 연결하는 클라이언트 머신에 인증서를 발급합니다. 이 기능을 사용하면 ASA VPN을 통해 연결하는 엔드 디바이스에 인증서를 자동으로 프로비저닝할 수 있습니다.

Cisco ISE는 인증서를 클라이언트 머신에 등록하고 프로비저닝하기 위해 SCEP(Simple Certificate Enrollment Protocol)를 사용합니다. AnyConnect 클라이언트는 HTTPS 연결을 통해 ASA에 SCEP 요청을 보냅니다. ASA는 Cisco ISE와 ASA 간에 설정된 HTTP 연결을 통해 Cisco ISE로 요청을 릴레이하기 전에 요청을 평가하고 정책을 시행합니다. Cisco ISE CA의 응답은 클라이언트로 다시 릴레이됩니다. ASA는 SCEP 메시지의 내용을 읽을 수 없으며 Cisco ISE CA에 대한 프록시로 작동합니다. Cisco ISE CA는 클라이언트에서 SCEP 메시지를 암호 해독하고 응답을 암호화된 형식으로 보냅니다.

ISE CA SCEP URL은 http://<*ISE CA* 서버의 *IP* 주소 또는 *FQDN*>:9090/auth/caservice/pkiclient.exe입니다. ISE 노드의 FQDN을 사용하는 경우 ASA에 연결된 DNS 서버가 FQDN을 확인할 수 있어야 합니다.

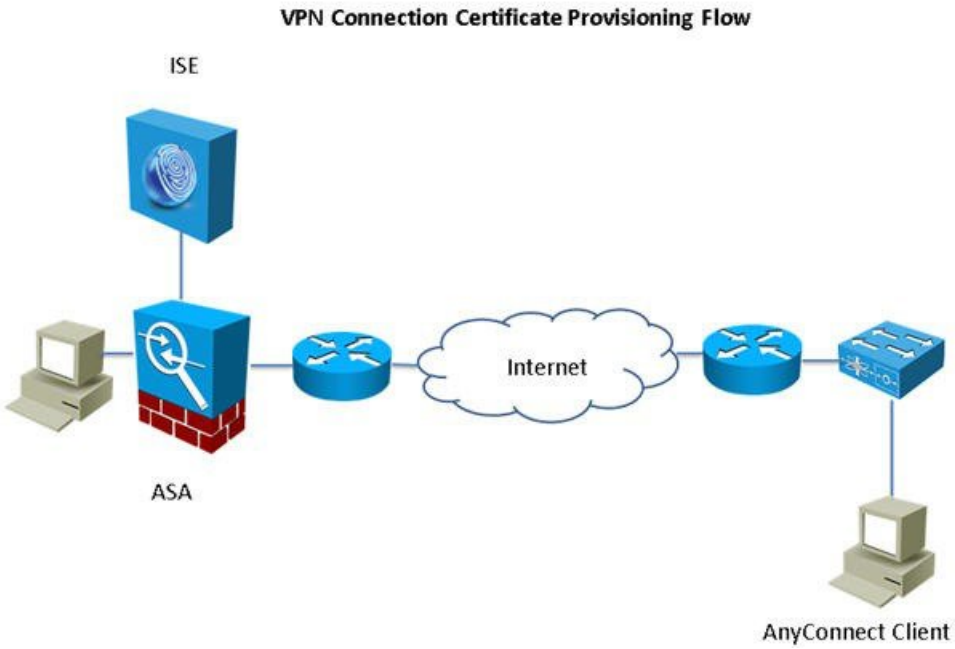
AnyConnect 클라이언트 프로파일에서 만료 전에 인증서 갱신을 구성할 수 있습니다. 인증서가 이미 만료된 경우 갱신 플로우는 새 등록과 비슷합니다.

지원되는 버전은 다음과 같습니다.

- 소프트웨어 버전 8.x를 실행하는 Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco AnyConnect VPN 버전 2.4 이상

VPN 연결 인증서 프로비저닝 플로우

그림 *10: ASA VPN* 사용자를 위한 인증서 프로비저닝



1. 사용자가 VPN 연결을 시작합니다.
2. AnyConnect 클라이언트는 클라이언트 머신을 스캔하고 고유한 디바이스 식별자(예: IMEI)와 같은 속성을 ASA에 전송합니다.
3. ASA는 클라이언트에서 인증서 기반 인증을 요청합니다. 인증서가 없으므로 인증에서 장애가 발생합니다.
4. ASA는 계속해서 사용자 이름/비밀번호를 사용하여 기본 사용자 인증(AAA)을 진행하고 정보를 인증 서버(ISE)에 전달합니다.
    1. 인증에서 장애가 발생하면 연결이 즉시 종료됩니다.
    2. 인증에 통과하면 제한적 액세스 권한이 부여됩니다. aaa.cisco.sceprequired 속성을 사용하여 인증서를 요청하는 클라이언트 머신에 대해 DAP(Dynamic Access Policy)를 구성할 수 있습니다. 이 속성의 값을 "true"로 설정하고 ACL 및 웹 ACL을 적용할 수 있습니다.
5. 관련 정책과 ACL이 적용된 후 VPN 연결이 설정됩니다. AAA 인증이 성공하고 VPN 연결이 설정되어야 클라이언트가 SCEP용 키 생성을 시작합니다.
6. 클라이언트가 SCEP 등록을 시작하고 HTTP를 통해 SCEP 요청을 ASA로 보냅니다.
7. ASA는 요청의 세션 정보를 조회하여 세션 등록이 허용되면 요청을 ISE CA로 릴레이합니다.
8. ASA가 ISE CA의 응답을 클라이언트로 다시 릴레이합니다.

9. 등록에 성공하면 클라이언트는 구성 가능한 메시지를 사용자에게 제공하고 VPN 세션과의 연결을 끊습니다.
10. 사용자는 인증서를 사용하여 다시 인증할 수 있으며, 그러면 정상 VPN 연결이 설정됩니다.

ASA VPN 사용자에게 인증서를 발급하도록 Cisco ISE CA 구성

ASA VPN 사용자에게 인증서를 프로비저닝하려면 Cisco ISE 및 ASA에서 다음 컨피그레이션을 수행해야 합니다.

시작하기 전에

- Cisco ISE 내부 또는 외부 ID 소스에 VPN 사용자 계정이 있는지 확인합니다.
- ASA 및 Cisco ISE 정책 서비스 노드가 동일한 NTP 서버를 사용하여 동기화되는지 확인합니다.

단계 **1** Cisco ISE에서 ASA를 네트워크 액세스 디바이스로 정의합니다. ASA를 네트워크 디바이스로 추가하는 방법에 대한 자세한 내용은 Cisco ISE에서 네트워크 디바이스 추가, 231 페이지을 참고하십시오.

단계 **2** ASA에서 그룹 정책 구성, 232 페이지.

단계 **3** SCEP 등록용 AnyConnect 연결 프로파일 구성, 232 페이지.

단계 **4** ASDM에서 VPN 클라이언트 프로파일 구성, 233 페이지.

단계 **5** ASA로 Cisco ISE CA 인증서 가져오기.

Cisco ISE에서 네트워크 디바이스 추가

Cisco ISE에서 네트워크 디바이스를 추가하거나 기본 네트워크 디바이스를 사용할 수 있습니다.

Network Devices(네트워크 디바이스)(**Work Centers**(작업 센터) > **Device Administration**(디바이스 관리) > **Network Resources**(네트워크 리소스) > **Network Devices**(네트워크 디바이스)) 창에서 네트워크 디바이스를 추가할 수도 있습니다.

시작하기 전에

추가할 네트워크 디바이스에서 AAA 기능을 활성화해야 합니다. 릴리스에 대한 *Cisco ISE* 관리자 가이드의 "통합" 장에서 "AAA 기능을 활성화하는 명령" 섹션을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration**(관리) > **Network Resources**(네트워크 리소스) > **Network Devices**(네트워크 디바이스)를 선택합니다.

단계 **2** **Add**(추가)를 클릭합니다.

단계 **3** **Name**(이름), **Description**(설명) 및 **IP Address**(IP 주소) 필드에 해당 값을 입력합니다.

단계 **4** 드롭다운 목록에서 **Device Profile**(디바이스 프로파일), **Model Name**(모델 이름), **Software Version**(소프트웨어 버전) 및 **Network Device Group**(네트워크 디바이스 그룹) 필드에 필요한 값을 선택합니다.

단계 **5** (선택 사항) 인증용 RADIUS 프로토콜을 구성하려면 **RADIUS Authentication Settings(RADIUS** 인증 설정**)** 확인란을 선택합니다.

단계 **6** (선택 사항) 인증용 TACACS 프로토콜을 구성하려면 **TACACS Authentication Settings(TACACS** 인증 설정**)** 확인란을 선택합니다.

단계 **7** (선택 사항) 네트워크 디바이스에서 정보를 수집하기 위해 Cisco ISE 프로파일링 서비스용으로 SNMP를 구성하려면 **SNMP Settings(SNMP** 설정**)** 확인란을 선택합니다.

단계 **8** (선택 사항) Cisco TrustSec이 활성화된 디바이스를 구성하려면 **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)** 확인란을 선택합니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

ASA에서 그룹 정책 구성

AnyConnect가 SCEP 등록 요청을 전달하도록 할 ISE CA URL을 정의하려면 ASA에서 그룹 정책을 구성합니다.

단계 **1** Cisco ASA ASDM에 로그인합니다.

단계 **2** 좌측의 Remote Access VPN(원격 액세스 VPN) 탐색창에서 **Group Policies(**그룹 정책**)**를 클릭합니다.

단계 **3** 그룹 정책을 생성하려면 **Add(**추가**)**를 클릭합니다.

단계 **4** 그룹 정책의 이름을 입력합니다. ISE_CA_SCEP를 예로 들 수 있습니다.

단계 **5** SCEP forwarding URL(SCEP 전달 URL) 필드에서 **Inherit(**상속**)** 확인란 선택을 취소하고 포트 번호와 함께 ISE SCEP URL을 입력합니다.

ISE 노드의 FQDN을 사용하는 경우 ASA에 연결된 DNS 서버가 ISE 노드의 FQDN을 확인할 수 있어야 합니다.

예제**:**

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe

단계 **6** 그룹 정책을 저장하려면 **OK(**확인**)**를 클릭합니다.

SCEP 등록용 AnyConnect 연결 프로파일 구성

ISE CA 서버, 인증 방법 및 ISE CA SCEP URL을 지정하려면 ASA에서 AnyConnect 연결 프로파일을 구성합니다.

단계 **1** Cisco ASA ASDM에 로그인합니다.

단계 **2** 좌측의 Remote Access VPN(원격 액세스 VPN) 탐색창에서 **AnyConnect Connection Profiles(AnyConnect** 연결 프로파일**)**를 클릭합니다.

단계 **3** 연결 프로파일을 생성하려면 **Add(**추가**)**를 클릭합니다.

단계 **4** 연결 프로파일의 이름을 입력합니다. 예를 들어 Get-Group과 같이 입력합니다.

단계 **5** (선택 사항) Aliases(별칭) 필드에 연결 프로파일의 설명을 입력합니다. 예를 들어 SCEP-Call-ASA와 같이 입력합니다.

단계 **6** Authentication(인증) 영역에서 다음을 지정합니다.

- Method(방법) - **Both(**둘 다**)** 라디오 버튼을 클릭합니다.
- AAA Server Group(AAA 서버 그룹) - **Manage(**관리**)**를 클릭하고 ISE 서버를 선택합니다.

단계 **7** Client Address Assignment(클라이언트 주소 할당) 영역에서, 사용할 DHCP 서버 및 클라이언트 주소 풀을 선택합니다.

단계 **8** Default Group Policy(기본 그룹 정책) 영역에서 **Manage(**관리**)**를 클릭하고 ISE SCEP URL 및 포트 번호로 생성한 그룹 정책을 선택합니다.

예제**:**

ISE_CA_SCEP를 예로 들 수 있습니다.

단계 **9** **Advanced(**고급**)** > **General(**일반**)**을 선택하고 이 연결 프로파일에 대해 **Enable Simple Certificate Enrollment Protocol(Simple Certificate Enrollment Protocol** 활성화**)** 확인란을 선택합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.
AnyConnect 연결 프로파일이 생성되었습니다.

다음에 수행할 작업

ASDM에서 VPN 클라이언트 프로파일 구성

SCEP 등록을 위해 AnyConnect에서 VPN 클라이언트 프로파일을 구성합니다.

단계 **1** Cisco ASA ASDM에 로그인합니다.

단계 **2** 좌측의 Remote Access VPN(원격 액세스 VPN) 탐색창에서 **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 클릭합니다.

단계 **3** 사용할 클라이언트 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** 좌측의 Profile(프로파일) 탐색창에서 **Certificate Enrollment(**인증서 등록**)**를 클릭합니다.

단계 **5** **Certificate Enrollment(**인증서 등록**)** 확인란을 선택합니다.

단계 **6** 다음 필드에 값을 입력합니다.

- Certificate Expiration Threshold(인증서 만료 임계값) - AnyConnect에서 사용자에게 인증서가 만료될 예정임을 경고하는 인증서 만료 전 남은 날짜 수입니다(SCEP가 활성화되어 있으면 지원되지 않음). 기본값은 영(0)(표시된 경고 없음)입니다. 값의 범위는 영(0)부터 180일까지입니다.
- Automatic SCEP Host(자동 SCEP 호스트) - SCEP 인증서 검색이 구성되어 있는 ASA의 호스트 이름과 연결 프로파일(터널 그룹)을 입력합니다. ASA의 FQDN(Fully Qualified Domain Name, 정규화된 도메인 이름) 또는 연결 프로파일 이름을 입력합니다. 예를 들어 호스트 이름인 asa.cisco.com과 연결 프로파일 이름인 Cert_Group을 입력합니다.
- CA URL - SCEP CA 서버를 식별합니다. ISE 서버의 FQDN 또는 IP 주소를 입력합니다. 예를 들어 http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe와 같이 입력합니다.

단계 **7** 클라이언트가 인증서의 콘텐츠를 요청하는 방법을 정의하는 Certificate Contents(인증서 콘텐츠)의 값을 입력합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.
AnyConnect 클라이언트 프로파일이 생성되었습니다. 자세한 내용은 해당 AnyConnect 버전의 Cisco AnyConnect Secure Mobility 클라이언트를 참고하십시오.

ASA로 Cisco ISE CA 인증서 가져오기

Cisco ISE 내부 CA 인증서를 ASA로 가져옵니다.

시작하기 전에

Cisco ISE 내부 CA 인증서를 내보냅니다. **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Authority Certificates(**인증 기관 인증서**)**를 선택합니다. **Certificate Services Node CA(**인증서 서비스 노드 **CA)** 및 **Certificate Services Root CA(**인증서 서비스 루트 **CA)** 인증서 옆의 확인란을 선택하여 해당 인증서를 한 번에 하나씩 내보냅니다.

단계 **1** Cisco ASA ASDM에 로그인합니다.

단계 **2** 왼쪽의 Remote Access VPN(원격 액세스 VPN) 탐색창에서 **Certificate Management(**인증서 관리**)** > **CA Certificates(CA** 인증서**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭한 다음 Cisco ISE 내부 CA 인증서를 선택하여 ASA로 가져옵니다.

엔드포인트 인증서 취소

직원의 개인 디바이스로 발급된 인증서를 취소해야 하는 경우 엔드포인트 인증서 페이지에서 해당 인증서를 취소할 수 있습니다. 예를 들어 직원 디바이스가 도난당하거나 분실된 경우 Cisco ISE 관리 포털에 로그인한 다음 엔드포인트 인증서 페이지에서 해당 디바이스에 발급된 인증서를 취소할 수 있습니다. 식별 이름, 디바이스 고유 ID 또는 일련 번호를 기준으로 이 페이지에서 데이터를 필터링할 수 있습니다.

PSN(하위 CA)이 노출된 경우에는 엔드포인트 인증서 페이지에서 Issued By(발급자) 필드를 기준으로 필터링하여 해당 PSN에서 발급한 모든 인증서를 취소할 수 있습니다.

직원에게 발급된 인증서를 취소할 때 해당 인증서를 사용하여 인증된 활성화된 세션이 있으면 해당 세션이 즉시 종료됩니다. 인증서를 취소하면 권한이 부여되지 않은 사용자가 인증서 취소 즉시 리소스에 액세스할 수 없게 됩니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Issued Certificates(**발급된 인증서**)**를 선택합니다.

단계 **2** 취소할 엔드포인트 인증서 옆의 확인란을 선택하고 **Revoke(**취소**)**를 클릭합니다.
식별 이름 및 디바이스 유형을 기준으로 인증서를 검색할 수 있습니다.

단계 **3** 인증서 취소 사유를 입력합니다.

단계 **4** **Yes(**예**)**를 클릭합니다.

OCSP 서비스

OCSP(Online Certificate Status Protocol)는 x.509 디지털 인증서의 상태를 확인하는 데 사용되는 프로토콜입니다. CRL(Certificate Revocation List) 대신 사용 가능한 이 프로토콜은 CRL 처리로 인해 발생하는 문제를 해결합니다.

Cisco ISE에는 HTTP를 통해 OCSP 서버와 통신하여 인증에서 인증서의 상태를 검증하는 기능이 있습니다. Cisco ISE에 구성되어 있는 모든 CA(Certificate Authority) 인증서에서 참조할 수 있는 재사용 가능한 컨피그레이션 객체에서 OCSP 컨피그레이션을 구성합니다.

CA별로 CRL 및/또는 OCSP 확인을 구성할 수 있습니다. CRL과 OCSP를 모두 선택하면 Cisco ISE는 OCSP를 통해 먼저 확인을 수행합니다. 기본 및 보조 OCSP 서버에서 모두 통신 문제가 탐지되거나 지정된 인증서에 대해 알 수 없는 상태가 반환되면 Cisco ISE는 CRL을 확인하도록 전환됩니다.

Cisco ISE CA Service Online Certificate Status Protocol 응답자

Cisco ISE CA OCSP 응답자는 OCSP 클라이언트와 통신하는 서버입니다. Cisco ISE CA용 OCSP 클라이언트에는 내부 Cisco ISE OCSP 클라이언트 및 ASA(Adaptive Security Appliance)의 OCSP 클라이언트가 있습니다. OCSP 클라이언트는 RFC 2560, 5019에 정의된 OCSP 요청/응답 구조를 사용하여 OCSP 응답자와 통신해야 합니다.

Cisco ISE CA는 OCSP 응답자에 인증서를 발급합니다. OCSP 응답자는 포트 2560에서 모든 들어오는 요청을 수신 대기합니다. 이 포트는 OCSP 트래픽만 허용하도록 구성되어 있습니다.

OCSP 응답자는 RFC 2560, 5019에 정의된 구조를 따르는 요청을 수락합니다. OCSP 요청에서는 Nonce 확장이 지원됩니다. OCSP 응답자는 인증서 상태를 확보하여 OCSP 응답을 생성하고 서명합니다. 최대 기간인 24시간 동안 클라이언트에서 OCSP 응답을 캐시할 수 있지만 OCSP 응답자에서 OCSP 응답은 캐시되지 않습니다. OCSP 클라이언트는 OCSP 응답의 서명을 검증해야 합니다.

PAN의 셀프 서명된 CA 인증서(또는 ISE가 외부 CA의 중간 CA로 작동하는 경우 중간 CA 인증서)는 OCSP 응답자 인증서를 발급합니다. PAN의 이 CA 인증서는 PAN 및 PSN에서 OCSP 인증서를 발급합니다. 이 셀프 서명된 CA 인증서는 전체 구축의 루트 인증서이기도 합니다. 구축 전체의 모든 OCSP 인증서는 이러한 인증서를 사용하여 서명된 응답을 검증하기 위해 ISE의 신뢰할 수 있는 인증서 저장소에 배치됩니다.

OCSP 인증서 상태 값

OCSP 서비스는 지정된 인증서 요청에 대해 다음 값을 반환합니다.

- 정상 - 상태 질의에 대한 긍정적 응답을 나타냅니다. 이는 인증서가 취소되지 않았으며 상태가 다음 시간 간격(Time to Live) 값까지만 정상이라는 것을 의미합니다.
- 취소됨 - 인증서가 취소되었습니다.

- 알 수 없음 - 인증서 상태를 알 수 없습니다. 이 OCSP 응답자의 CA에 의해 인증서가 발급되지 않은 경우 OCSP 서비스에서 이 값을 반환합니다.
- 오류 - OCSP 요청에 대한 응답이 수신되지 않았습니다.

OCSP 고가용성

Cisco ISE는 CA당 최대 2대의 OCSP 서버를 구성할 수 있으며, 이러한 서버를 각각 기본 및 보조 OCSP 서버라고 합니다. 각 OCSP 서버 컨피그레이션에는 다음 매개변수가 포함됩니다.

- URL - OCSP 서버 URL입니다.
- Nonce - 요청에서 전송되는 난수입니다. 이 옵션을 사용하는 경우 재생 공격에서 이전 통신을 사용할 수 없습니다.
- Validate response - Cisco ISE는 OCSP 서버에서 수신되는 응답 서명을 검증합니다.

Cisco ISE는 기본 OCSP 서버와 통신할 때 시간 초과(5초)이 발생하면 보조 OCSP 서버로 전환합니다.

Cisco ISE는 구성 가능한 시간 동안 보조 OCSP 서버를 사용한 후 기본 서버 사용을 다시 시도합니다.

OCSP 실패

3가지 일반 OCSP 실패 시나리오는 다음과 같습니다.

- 실패한 OCSP 캐시 또는 OCSP 클라이언트 측(Cisco ISE) 장애
- 실패한 OCSP 응답자 시나리오. 예를 들어 다음과 같습니다.

  첫 번째 기본 OCSP 응답자가 응답하지 않고 보조 OCSP 응답자가 Cisco ISE OCSP 요청에 응답함

  Cisco ISE OCSP 요청에서 수신되지 않은 응답 또는 오류

  OCSP 응답자가 Cisco ISE OCSP 요청에 대한 응답을 또는 제공하지 않거나 OCSP 응답 상태를 실패한 상태로 반환할 수 있습니다. OCSP 응답 상태 값은 다음과 같습니다.

  - tryLater
  - signRequired
  - unauthorized
  - internalError
  - malformedRequest

    OCSP 요청에는 여러 가지 날짜 및 시간 검사, 서명 유효성 검사 등이 있습니다. 자세한 내용은 *RFC 2560 X.509* 인터넷 공개 키 인프라 *OCSP(Online Certificate Status Protocol)*를 참고하십시오. 여기에서는 오류 상태를 포함한 모든 가능한 상태를 설명합니다.

- 실패한 OCSP 보고서

OCSP 클라이언트 프로파일 추가

OCSP 클라이언트 프로파일 페이지를 사용하여 Cisco ISE에 새 OCSP 클라이언트 프로파일을 추가할 수 있습니다.

시작하기 전에

CA(Certificate Authority)가 비표준 포트(80 또는 443 이외의 포트)에서 OCSP 서비스를 실행 중인 경우 Cisco ISE와 해당 포트의 CA 간에 통신을 허용하도록 스위치에서 ACL을 구성해야 합니다. 예를 들면 다음과 같습니다.

permit tcp <*source ip*> <*destination ip*> **eq** <*OCSP port number*>

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **OCSP Client Profile(OSCP** 클라이언트 프로파일**)**을 선택합니다 .

단계 **2** 값을 입력하여 OCSP 클라이언트 프로파일을 추가합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

OCSP 클라이언트 프로파일 설정

다음 표에서는 OCSP 클라이언트 프로파일을 구성하는 데 사용할 수 있는 OSCP Client Profile(OCSP 클라이언트 프로파일) 페이지의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **OCSP Client Profile(OCSP** 클라이언트 프로파일**)**입니다.

표 ***31: OCSP*** 클라이언트 프로파일 설정

필드 이름	사용 지침
Name(이름**)**	OCSP 클라이언트 프로파일의 이름입니다.
Description(설명**)**	필요에 따라 설명을 입력합니다.
OCSP 응답자 구성	
Enable Secondary Server(보조 서버 활성화**)**	고가용성을 위해 보조 OCSP 서버를 활성화하려면 이 확인란을 선택합니다.
Always Access Primary Server First(항상 기본 서버에 먼저 액세스**)**	보조 서버로 이동하기 전에 기본 서버를 확인하려면 이 옵션을 사용합니다. 이전에 기본 서버를 확인한 결과 응답하지 않았더라도 Cisco ISE는 보조 서버로 이동하기 전에 기본 서버로의 요청 전송을 시도합니다.

필드 이름	사용 지침
Fallback to Primary Server After Interval *n* Minutes(n분 간격 이후 기본 서버로 대체**)**	Cisco ISE가 보조 서버로 이동했다가 기본 서버로 다시 대체하도록 하려면 이 옵션을 사용합니다. 이 경우 다른 요청은 모두 건너뛰며 텍스트 상자에서 구성하는 시간 동안 보조 서버가 사용됩니다. 사용할 수 있는 시간 범위는 1~999분입니다.
Primary and Secondary Servers(기본 서버 및 보조 서버**)**	
URL	기본 및/또는 보조 OCSP 서버의 URL을 입력합니다.
Enable Nonce Extension Support(nonce 확장 지원 활성화**)**	OCSP 요청의 일부분으로 nonce를 전송하도록 구성할 수 있습니다. nonce에는 OCSP 요청의 의사 난수가 포함됩니다. 이 옵션을 사용하는 경우 응답에서 수신된 숫자가 요청에 포함된 숫자와 동일한지를 확인합니다. 이 옵션을 사용하는 경우 재생 공격에서 이전 통신을 사용할 수 없습니다.
Validate Response Signature(응답 서명 검증**)**	OCSP 응답자는 다음 인증서 중 하나를 사용하여 응답을 표시합니다. • CA 인증서 • CA 인증서와 다른 인증서 Cisco ISE가 응답 서명을 검증하도록 하려면 OCSP 응답자가 인증서와 함께 응답을 보내야 합니다. 그렇지 않으면 응답 확인이 실패하며 인증서의 상태를 신뢰할 수 없습니다. RFC에 따르면 OCSP는 서로 다른 여러 인증서를 사용하여 응답에 서명을 할 수 있습니다. 단, OCSP는 Cisco ISE가 검증할 수 있도록 응답에 서명을 하는데 사용한 인증서를 보내야 합니다. OCSP가 Cisco ISE에 구성되어 있지 않은 다른 인증서로 응답에 서명을 하는 경우에는 응답 확인이 실패합니다.
Use OCSP URLs specified in Authority Information Access (AIA)(AIA(Authority Information Access)에 지정된 **OCSP URL** 사용**)**	Authority Information Access 익스텐션에 지정된 OCSP URL을 사용하려면 라디오 버튼을 클릭합니다.
응답 캐시	

필드 이름	사용 지침
Cache Entry Time To Live *n* Minutes(캐시 엔트리 **Time To Live n**분**)**	캐시 엔트리가 만료될 때까지의 시간을 분 단위로 입력합니다. OCSP 서버의 각 응답은 nextUpdate 값을 포함합니다. 서버에서 다음 번에 인증서 상태를 업데이트하면 이 값이 표시됩니다. OCSP 응답을 캐시할 때는 두 값, 즉 컨피그레이션의 값과 응답의 값을 비교하며 이 두 값 중 더 작은 기간에 대해 응답이 캐시됩니다. nextUpdate 값이 0이면 응답은 캐시되지 않습니다. Cisco ISE는 구성된 시간 동안 OCSP 응답을 캐시합니다. 캐시는 복제되거나 영구적으로 저장되지 않으므로 Cisco ISE를 재시작하면 캐시가 지워집니다. OCSP 캐시는 OCSP 응답을 유지 관리하는 데 사용되며, 다음과 같은 이유로도 사용됩니다. • 이미 알려진 인증서에 대한 OCSP 서버의 네트워크 트래픽 및 로드 감소 • 이미 알려진 인증서 상태를 캐시하여 Cisco ISE의 성능 개선 기본적으로 캐시는 내부 CA OCSP 클라이언트 프로파일에 대해 2분으로 설정됩니다. 엔드포인트가 첫 번째 인증 후 2분 이내에 두 번째 인증을 수행하는 경우 OCSP 캐시가 사용되고 OCSP 응답자가 쿼리되지 않습니다. 엔드포인트 인증서가 캐시 기간 내에 취소된 경우 이전 OCSP 상태인 Good이 사용되며 인증이 성공합니다. 캐시를 0분으로 설정하면 응답이 캐시되지 않습니다. 이 옵션을 사용하면 보안이 개선되지만 인증 성능은 저하됩니다.
Clear Cache(캐시 지우기**)**	OCSP 서비스에 연결된 모든 인증 기관의 엔트리를 지우려면 **Clear Cache(**캐시 지우기**)**를 클릭합니다. 구축에서 **Clear Cache(**캐시 지우기**)**는 모든 노드와 상호 작용하여 작업을 수행합니다. 이러한 메커니즘은 구축의 모든 노드를 업데이트합니다.

관련 항목

OCSP 서비스, 235 페이지
Cisco ISE CA Service Online Certificate Status Protocol 응답자, 235 페이지
OCSP 인증서 상태 값, 235 페이지
OCSP 고가용성, 236 페이지
OCSP 실패, 236 페이지
OCSP 통계 카운터, 239 페이지
OCSP 클라이언트 프로파일 추가, 237 페이지

OCSP 통계 카운터

Cisco ISE는 OCSP 카운터를 사용하여 OCSP 서버의 데이터와 상태를 기록하고 모니터링합니다. 5분마다 로깅됩니다. Cisco ISE는 시스템 로그 메시지를 모니터링 노드로 보내며, 이 메시지는 로컬 저장

소에 보존됩니다. 로컬 저장소에는 지난 5분 동안의 데이터가 포함되어 있습니다. Cisco ISE가 시스템 로그 메시지를 보내고 나면 다음 간격에 대해 카운터가 다시 계산됩니다. 즉, 5분이 지나면 새로운 5분 시간 간격이 다시 시작됩니다.

다음 표에는 OCSP 시스템 로그 메시지와 해당 설명이 나와 있습니다.

표 ***32: OCSP*** 시스템 로그 메시지

메시지	설명
OCSPPrimaryNotResponsiveCount	응답하지 않는 기본 요청의 수
OCSPSecondaryNotResponsiveCount	응답하지 않는 보조 요청의 수
OCSPPrimaryCertsGoodCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '정상' 인증서의 수
OCSPSecondaryCertsGoodCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '정상' 상태의 수
OCSPPrimaryCertsRevokedCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '취소된' 상태의 수
OCSPSecondaryCertsRevokedCount	보조 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '취소된' 상태의 수
OCSPPrimaryCertsUnknownCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '알 수 없는' 상태의 수
OCSPSecondaryCertsUnknownCount	보조 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '알 수 없는' 상태의 수
OCSPPrimaryCertsFoundCount	기본 원본의 캐시에서 발견된 인증서의 수
OCSPSecondaryCertsFoundCount	보조 원본의 캐시에서 발견된 인증서의 수
ClearCacheInvokedCount	간격 이후 일반 캐시가 트리거된 횟수
OCSPCertsCleanedUpCount	간격 이후 정리된 캐시된 엔트리의 수
NumOfCertsFoundInCache	캐시에서 이행된 요청의 수
OCSPCacheCertsCount	OCSP 캐시에서 발견된 인증서의 수

관리자 액세스 정책 구성

RBAC 정책은 if-then 형식으로 표현됩니다. 여기서 "if"는 RBAC 관리자 그룹 값이고 "then"은 RBAC 권한 값입니다.

RBAC 정책 창(**Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authorization(**권한 부여**)** > **RBAC Policy(RBAC** 정책**)** 선택)에는 기본 정책 목록이 포함되어 있습니다. 이러한 기본 정책은 편집하거나 삭제할 수 없습니다. 그러나 읽기 전용 관리 정책에 대한 데이터 액세스 권한은 편집할 수 있습니다. 또한 RBAC 정책 페이지에서는 직장 전용 관리자 그룹에 대해 사용자 맞춤화 RBAC 정책을 생성하여 개인 설정된 관리자 그룹에 적용할 수 있습니다.

제한된 메뉴 액세스를 할당할 경우 관리자가 데이터 액세스 권한을 통해 지정된 메뉴를 사용하는 데 필요한 데이터에 액세스할 수 있는지 확인하십시오. 예를 들어, MyDevices 포털에 대한 메뉴 액세스는 제공하지만 엔드포인트 ID 그룹에 대한 데이터 액세스는 허용하지 않는 경우 해당 관리자는 포털을 수정할 수 없습니다.

참고 관리자는 엔드포인트 MAC 주소를 읽기 전용 액세스 권한이 있는 엔드포인트 ID 그룹에서 전체 액세스 권한이 있는 엔드포인트 ID 그룹으로 이동할 수 있습니다. 다른 방법으로는 불가능합니다.

시작하기 전에

- RBAC(Role-Based Access Control) 정책을 정의하려는 모든 관리자 그룹을 생성합니다.
- 이러한 관리자 그룹이 개별 관리 사용자에게 매핑되어 있는지 확인합니다.
- 메뉴 액세스 및 데이터 액세스 권한과 같은 RBAC 권한을 구성했는지 확인합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Authorization(**권한 부여**)** > **RBAC Policy(RBAC** 정책**)**를 선택합니다.

RBAC 정책 페이지에는 기본 관리자 그룹에 대해 즉시 사용 가능한 미리 정의된 정책이 포함되어 있습니다. 이러한 기본 정책은 편집하거나 삭제할 수 없습니다. 그러나 기본 읽기 전용 관리 정책에 대한 데이터 액세스 권한을 편집할 수 있습니다.

단계 **2** 기본 RBAC 정책 규칙 옆의 **Actions(**작업**)**를 클릭합니다.

여기서 새 RBAC 정책을 삽입하고 기존 RBAC 정책을 복제/삭제할 수 있습니다.

단계 **3** **Insert new policy(**새 정책 삽입**)**를 클릭합니다.

단계 **4** Rule Name(규칙 이름), RBAC Group(s)(RBAC 그룹) 및 Permissions(권한) 필드에 값을 입력합니다.

RBAC 정책을 생성할 때는 여러 메뉴 액세스 및 데이터 액세스 권한을 선택할 수 없습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

관리자 액세스 설정

Cisco ISE를 사용하면 관리자 계정에 대한 일부 규칙을 정의하여 보안을 개선할 수 있습니다. 관리 인터페이스에 대한 액세스를 제한하여 관리자가 강력한 비밀번호를 사용하거나 비밀번호를 정기적으로 변경하는 등의 작업을 하도록 강제할 수 있습니다. Cisco ISE의 관리자 계정 설정에서 정의하는 비밀번호 정책은 모든 관리자 계정에 적용됩니다.

Cisco ISE는 UTF-8 문자를 포함하는 관리자 비밀번호를 지원합니다.

동시 관리 세션 및 로그인 배너의 최대 수 구성

관리자에게 관리 웹 또는 CLI 인터페이스에 액세스하는 사용자를 알려 주는 동시 관리 GUI 또는 CLI(SSH) 세션 및 로그인 배너의 최대 수를 구성할 수 있습니다. 관리자 로그인 전과 후에 표시되는 로그인 배너를 구성할 수 있습니다. 이러한 로그인 배너는 기본적으로 비활성화됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration**(관리) > **System**(시스템) > **Admin Access**(관리자 액세스) > **Settings**(설정) > **Access**(액세스) > **Session**(세션)을 선택합니다.

단계 **2** GUI 및 CLI 인터페이스를 통해 허용하려는 동시 관리 세션의 최대 수를 입력합니다. 동시 관리 GUI 세션의 유효 범위는 1~20입니다. 동시 관리 CLI 세션의 유효 범위는 1~10입니다.

단계 **3** 관리자 로그인 전에 Cisco ISE가 메시지를 표시하도록 하려면 **Pre-login banner**(로그인 전 배너) 확인란을 선택하고 텍스트 상자에 메시지를 입력합니다.

단계 **4** 관리자 로그인 후에 Cisco ISE가 메시지를 표시하도록 하려면 **Post-login banner**(로그인 후 배너) 확인란을 선택하고 텍스트 상자에 메시지를 입력합니다.

단계 **5** **Save**(저장)를 클릭합니다.

관련 항목

선택한 IP 주소에서 Cisco ISE로의 관리 액세스 허용, 242 페이지

선택한 IP 주소에서 Cisco ISE로의 관리 액세스 허용

Cisco ISE에서는 관리자가 Cisco ISE 관리 인터페이스에 액세스할 수 있는 IP 주소 목록을 구성할 수 있습니다.

관리자 액세스 제어 설정은 관리, 정책 서비스 또는 모니터링 페르소나가 지정된 Cisco ISE 노드에만 적용 가능합니다. 이러한 제한은 기본 노드에서 보조 노드로 복제됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Settings(**설정**)** > **Access(**액세스**)** > **IP Access(IP** 주소**)**를 선택합니다.

단계 **2** **Allow only listed IP address to connect(**연결하도록 나열된 **IP** 주소만 허용**)** 라디오 버튼을 클릭합니다.

참고 포트 161(SNMP)에 대한 연결은 관리 액세스에 사용됩니다. 그러나 IP 액세스 제한이 구성된 경우, snmpwalk가 수행되는 출처 노드를 관리 액세스용으로 구성하지 않으면 snmpwalk는 실패합니다.

단계 **3** **Configure IP List for Access Restriction(**액세스 제한용 **IP** 목록 구성**)** 영역에서 **Add(**추가**)**를 클릭합니다.

단계 **4** **Add IP CIDR(IP CIDR** 추가**)** 대화 상자에서 **IP address(IP** 주소**)** 필드에 IP 주소를 CIDR(Classless Interdomain Routing) 형식으로 입력합니다.

참고 이 IP 주소는 IPv4 또는 IPv6 주소일 수 있습니다. 하나의 ISE 노드에 대해 여러 IPv6 주소를 구성할 수 있습니다.

단계 **5** **Netmask in CIDR format(CIDR**의 네트워크 마스크 형식**)** 필드에 서브넷 마스크를 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다. 단계 4~7을 반복하여 이 목록에 IP 주소 범위를 더 추가합니다.

단계 **7** **Save(**저장**)**를 클릭하여 변경사항을 저장합니다.

단계 **8** **Reset(**재설정**)**을 클릭하여 **IP Access(IP** 액세스**)** 창을 새로 고칩니다.

Cisco ISE의 MnT 섹션에 대한 액세스 허용

Cisco ISE에서는 관리자가 Cisco ISE의 Mnt 섹션에 액세스할 수 있는 노드의 목록을 구성할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE 홈페이지에서 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Access(**액세스**)**를 선택합니다.

단계 **2** **Mnt Access(Mnt** 액세스**)** 탭을 클릭합니다.

단계 **3** 구축 내에서 또는 구축 외부에서 시스템 로그를 MnT로 전송하도록 노드 또는 엔티티를 허용하려면 **Allow any IP address to connect to MnT(MnT**에 연결할 모든 **IP** 주소 허용**)** 라디오 버튼을 클릭합니다. 구축 내 노드 또는 엔티티만 시스템 로그를 MnT로 전송하도록 허용하려면 **Allow any IP address to connect to MnT (**구축 내의 노드만 **MnT** 에 연결 허용**)** 라디오 버튼을 클릭합니다.

참고 ISE 2.6 P2 이상 버전의 경우 Use ISE Messaging Service for UDP Syslogs delivery to MnT(UDP Syslogs를 Mnt로 전송하기 위해서 ISE 메시지 서비스만 사용)이 기본적으로 켜져 있습니다. 그러면 구축 외부의 다른 엔티티에서 오는 시스템 로그가 허용되지 않습니다.

관리자 계정의 비밀번호 정책 구성

Cisco ISE에서는 보안을 강화하기 위해 관리자 계정용 비밀번호 정책을 생성할 수도 있습니다. 비밀번호 기반 또는 클라이언트 인증서 기반 관리자 인증을 원하는지 정의할 수 있습니다. 여기에서 정의하는 비밀번호 정책은 Cisco ISE의 모든 관리자 계정에 적용됩니다.

참고

- 내부 관리자 사용자에 대한 이메일 알림은 root@host로 전송됩니다. 이메일 주소를 구성 할 수 없으며 많은 SMTP 서버가 이 이메일을 거부합니다.

  이메일 주소를 변경할 수 있는 개선된 오픈 결함 CSCui5583을 따릅니다.

- Cisco ISE는 UTF-8 문자를 포함하는 관리자 비밀번호를 지원합니다.

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- 구축에서 활성화되어 있는 경우 자동 페일오버 구성을 끕니다. 관리 노드에 대한 자동 페일오버 지원, 71 페이지의 내용을 참조하십시오.

  인증 방법을 변경하면 애플리케이션 서버 프로세스가 다시 시작됩니다. 이러한 서비스가 다시 시작되는 동안 작업이 지연될 수 있습니다. 서비스가 다시 시작될 때의 이러한 지연으로 인해 보조 관리 노드의 자동 페일오버가 시작될 수 있습니다.

단계 **1** Cisco ISE GUI 메뉴에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭한 뒤**Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)**를 선택합니다.

단계 **2** 다음 인증 방법 중 하나의 라디오 버튼을 클릭합니다.

- **Password Based(**비밀번호 기반**)**: 관리자 로그인에 표준 사용자 ID 및 비밀번호 자격 증명을 사용하려면 이 옵션을 선택합니다. **Identity Source** 드롭다운 목록에서 **Internal(**내부**)** 또는 **External(**외부**)**을 선택합니다.

  참고 LDAP 등의 외부 ID 소스를 구성했으며 관리자에게 액세스 권한을 부여하기 위한 인증 소스로 해당 소스를 사용하려는 경우에는 ID 소스 목록 상자에서 해당 특정 ID 소스를 선택해야 합니다.

- **Client Certificate Based(**클라이언트 인증서 기반**)**: 인증서 기반 정책을 지정하려면 이 옵션을 선택합니다. **Certificate Authentication Profile(**인증서 인증 프로파일**)** 드롭다운 목록에서 기존 인증 프로파일을 선택합니다. **Identity Source(ID** 소스**)** 드롭다운 목록에서 필요한 값을 선택합니다.

단계 **3** **Password Policy(**비밀번호 정책**)** 탭을 클릭하고 Cisco ISE GUI 및 CLI 비밀번호 요구 사항을 구성하는 데 필요한 값을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭하여 관리자 비밀번호 정책을 저장합니다.

참고 로그인 시 외부 ID 저장소를 사용하여 관리자를 인증하는 경우, 관리자 프로파일에 적용되는 비밀번호 정책에 대해 이 설정이 구성되어 있더라도 외부 ID 저장소는 관리자의 사용자 이름과 비밀번호를 계속 검증합니다.

관련 항목

관리자 비밀번호 정책 설정, 59 페이지
관리자 계정의 계정 비활성화 정책 구성, 245 페이지
관리자 계정에 대한 잠금 또는 일시 중단 설정 구성, 245 페이지

관리자 계정의 계정 비활성화 정책 구성

Cisco ISE에서는 구성된 연속 기간(일) 동안 관리자 계정이 인증되지 않은 경우 해당 관리자 계정을 비활성화할 수 있습니다.

단계 **1** Cisco ISE GUI 메뉴에서 **Menu**(메뉴) 아이콘(☰)을 클릭한 뒤 **Administration**(관리) > **System**(시스템) > **Admin Access**(관리자 액세스) > **Authentication**(인증) > **Account Disable Policy**(계정 비활성화 정책)를 선택합니다.

단계 **2** **Disable account after *n* days of inactivity**(n일 동안 비활성 상태였던 계정 비활성화) 확인란을 선택하고 해당 필드에 기간(일)을 입력합니다.

이 옵션을 사용하면 구성된 지정된 기간(일) 동안 관리자 계정이 비활성 상태인 경우 해당 관리자 계정을 비활성화할 수 있습니다. 그러나 **Inactive Account Never Disabled**(비활성화된 적 없는 계정 비활성화) 옵션(**Administration**(관리) > **System**(시스템) > **Admin Access**(관리 액세스) > **Administrators**(관리자) > **Admin Users**(관리 사용자) 창에서 사용 가능)을 사용하여 이 계정 비활성화 정책에서 개별 관리자 계정을 제외할 수 있습니다.

단계 **3** 관리자에 대한 전역 계정 비활성화 정책을 구성하려면 **Save**(저장)를 클릭합니다.

관리자 계정에 대한 잠금 또는 일시 중단 설정 구성

Cisco ISE에서는 실패한 로그인 시도 횟수가 지정된 횟수보다 많은 관리자 계정(비밀번호 기반 내부 관리자 계정 및 인증서 기반 관리자 계정 포함)을 잠그거나 일시 중지할 수 있습니다.

단계 **1** Cisco ISE GUI 메뉴에서 **Menu**(메뉴) 아이콘(☰)을 클릭한 뒤 **Administration**(관리) > **System**(시스템) > **Admin Access**(관리자 액세스) > **Authentication**(인증) > **Lock/Suspend Settings**(설정 잠금/일시 중지)를 선택합니다.

단계 **2** **Suspend or Lock Account With Incorrect Login Attempts**(잘못된 로그인 시도 시 계정 잠금 또는 일시 중지) 확인란을 선택하고 몇 번의 시도가 실패한 후 조치를 취할지 입력합니다. 유효 범위는 3~20입니다. 다음 중 하나의 옵션에 해당하는 라디오 버튼을 클릭합니다.

- **Suspend Account For *n* Minutes**(n분 동안 계정 일시 중지): 지정된 잘못된 로그인 시도 횟수를 초과하는 계정을 일시 중지하려면 이 옵션을 선택합니다. 유효 범위는 15~1440입니다.
- **Lock Account**(계정 잠금): 지정된 잘못된 로그인 시도 횟수를 초과하는 계정을 잠그려면 이 옵션을 선택합니다.

최종 사용자에게 헬프데스크에 문의하여 계정 잠금을 해제하도록 요청하는 등의 사용자 맞춤화 이메일 교정 메시지를 입력할 수 있습니다.

참고 Cisco ISE 릴리스 2.3 이하에서는 **Lock/Suspend Settings(**설정 잠금/일시 중지**)**은 **Password Policy(**비밀번호 정책**)** 탭(**Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Authentication(**인증**)** > **Password Policy(**비밀번호 정책**)**에서 사용할 수 있습니다.

관리자에 대한 세션 시간 초과 구성

Cisco ISE에서는 관리 GUI 세션이 비활성 상태로 계속 연결되어 있을 수 있는 시간을 결정할 수 있습니다. Cisco ISE가 관리자를 로그아웃 처리할 때까지의 시간을 분 단위로 지정할 수 있습니다. 세션 시간이 초과되고 나면 관리자는 다시 로그인해야 Cisco ISE 관리 포털에 액세스할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Session(**세션**)** > **Session Timeout(**세션 시간 초과**)**을 선택합니다.

단계 **2** 작업을 수행하지 않는 경우 관리자가 로그아웃될 때까지 Cisco ISE가 대기하도록 할 시간을 분 단위로 입력합니다. 기본값은 60분입니다. 유효 범위는 6분~100분입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

활성 관리 세션 종료

Cisco ISE는 필요한 경우 언제든지 세션을 선택하여 종료할 수 있도록 모든 활성 관리 세션을 표시합니다. 동시 관리 GUI 세션의 최대 수는 20개입니다. GUI 세션의 최대 수에 도달하면 슈퍼 관리자 그룹에 속하는 관리자가 로그인하여 일부 세션을 종료할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Session(**세션**)** > **Session Info(**세션 정보**)**를 선택합니다.

단계 **2** 종료할 세션 ID 옆의 확인란을 선택하고 **Invalidate(**무효화**)**를 클릭합니다.

관리자 이름 변경

Cisco ISE에서는 Cisco ISE GUI를 통해 사용자 이름을 변경할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE 관리 포털에 로그인합니다.

단계 **2** Cisco ISE GUI의 오른쪽 상단에서 기어 아이콘 ()을 클릭하고 드롭다운 목록에서 **Account Settings(**계정 설정**)**를 선택합니다.

단계 **3** 표시되는 **Admin User(**관리 사용자**)** 대화 상자에 새 사용자 이름을 입력합니다.

단계 **4** 변경할 계정에 대한 기타 세부정보를 편집합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

관리자 액세스 설정

이 섹션에서는 관리자용 액세스 설정을 구성할 수 있습니다.

관리자 비밀번호 정책 설정

다음 표에서는 **Password Policy(**비밀번호 정책**)** 탭의 필드에 대해 설명합니다. 이 탭을 사용하여 관리자 비밀번호가 충족해야 하는 기준을 정의할 수 있습니다. 이 창을 보려면 메뉴 아이콘()을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Authentication(**인증**)** > **Password Policy(**비밀번호 정책**)** .

표 ***33:*** 관리자 비밀번호 정책 설정

필드 이름	사용 지침
최소 길이	최소 비밀번호 길이를 문자 단위로 지정합니다. 기본값은 6자입니다.

필드 이름	사용 지침
비밀번호는 다음을 포함할 수 없습니다.	관리자 이름 또는 그 문자를 역순으로 배열한 단어: 관리자 이름 또는 그 문자를 역순으로 배열한 단어의 사용을 제한하려면 이 확인란을 선택합니다.
	Cisco 또는 그 문자를 역순으로 배열한 단어: Cisco 또는 그 문자를 비밀번호의 역순으로 배열한 단어의 사용을 제한하려면 이 체크 박스를 선택합니다.
	이 단어 또는 그 문자를 역순으로 배열한 단어: 사용자가 정의한 특정 단어 또는 그 문자를 비밀번호의 역순으로 배열한 단어의 사용을 제한하려면 이 체크 박스를 선택합니다.
	4번 이상 반복되는 문자: 비밀번호에 4번 이상 반복되는 문자를 연속으로 사용하는 것을 제한하려면 이 체크 박스를 선택합니다.
	사전 단어**,** 반대 순서의 문자 또는 다른 문자로 교체 된 문자: 사전 단어의 비밀번호 사용을 제한하거나 반대 순서로 문자를 교체하거나 문자를 다른 문자로 교체하려면 이 확인란을 선택합니다. s를 $, a를 @, o를 0, l를 1, i를 !, e를 3으로 대체할 수 없습니다. 예를 들어 Pa$$w0rd는 허용되지 않습니다. • **Default Dictionary(**기본 사전**)**: Cisco ISE에서 기본 Linux 사전을 사용하려면 이 옵션을 선택합니다. 기본 사전에는 약 480,000개의 영어 단어가 포함되어 있습니다. 이 옵션은 기본적으로 선택되어 있습니다. • **Custom Dictionary(**맞춤형 사전**)**: 맞춤 설정한 사전을 사용하려면 이 옵션을 선택합니다. **Choose File(**파일 선택**)**을 클릭하여 맞춤형 사전 파일을 선택합니다. 텍스트 파일은 새 줄 구분된 단어, .dic 확장자여야 하며 크기가 20MB 미만이어야 합니다.

필드 이름	사용 지침
Password must contain at least one character of each of the selected types(비밀번호는 선택한 유형별로 하나 이상의 문자를 포함해야 함**)**	관리자 비밀번호에 포함해야 하는 문자 유형에 대한 확인란을 선택합니다. 다음 옵션 중 하나 이상을 선택합니다. • 소문자 알파벳 문자 • 대문자 알파벳 문자 • 숫자 • 영숫자 이외의 문자
Password History(비밀번호 기록**)**	같은 비밀번호를 반복적으로 사용하지 못하도록 하기 위해, 새로 입력하는 비밀번호와 달라야 하는 이전 비밀번호의 수를 지정합니다. **Password must be different from the previous *n*versions(**비밀번호는 이전 **n** 버전과 달라야 함**)** 확인란을 선택하고 해당 필드에 번호를 입력합니다. 비밀번호를 재사용할 수 있을 때까지의 기간을 일 단위로 입력합니다. **Cannot reuse password within *n* days(n**일 이내에 비밀번호를 재사용 할 수 없음**)** 확인란을 선택하고 해당 필드에 번호를 입력합니다.
Password Lifetime(비밀번호 수명**)**	사용자가 지정된 기간 이후 비밀번호를 변경해야 하도록 강제 지정하려면 확인란을 선택합니다. • 관리자 비밀번호는 생성 또는 마지막 변경 이후 ***n***일 후에 만료: 비밀번호를 변경하지 않으면 관리자 계정을 비활성화할 때까지의 시간(일))입니다. 유효한 범위는 1일~3650일입니다. • 비밀번호 만료 ***n***일 전에 관리자에게 이메일 알림 보내기: 비밀번호가 만료 될 것임을 관리자에게 알리기 전까지의 시간(일)입니다. 유효한 범위는 1일~3650일입니다.
네트워크 디바이스 민감한 데이터 표시	
Require Admin Password(관리자 비밀번호 필요**)**	공유 암호 및 비밀번호와 같은 네트워크 디바이스의 민감한 데이터를 확인하기 위해 관리 사용자가 로그인 비밀번호를 입력해야 하도록 지정하려면 이 체크 박스를 선택합니다.

필드 이름	사용 지침
Password cached for *n* Minutes(n분 동안 비밀번호 캐시**)**	관리 사용자가 입력한 비밀번호가 이 기간 동안 캐시됩니다. 이 기간 동안에는 관리 사용자가 네트워크 디바이스의 민감한 데이터를 볼 때 비밀번호를 다시 입력하라는 메시지가 표시되지 않습니다. 유효 범위는 1분~60분입니다.

관련 항목

Cisco ISE 관리자, 3 페이지
새 관리자 생성, 5 페이지

세션 시간 초과 및 세션 정보 설정

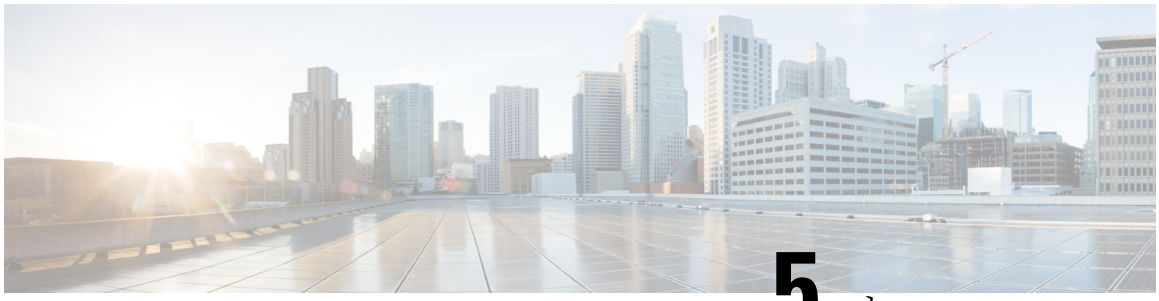
다음 표에서는 세션 시간 초과를 정의하고 활성 관리 세션을 종료하는 데 사용할 수 있는 **Session(**세션**)** 창의 필드에 대해 설명합니다. 이 창에 액세스하려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Settings(**설정**)** > **Session(**세션**)**을 선택합니다.

표 ***34:*** 세션 시간 초과 및 세션 정보 설정

필드 이름	사용 지침
세션 시간 초과	
Session Idle Timeout(세션 유휴 시간 초과**)**	작업을 수행하지 않는 경우 관리자가 로그아웃될 때까지 Cisco ISE가 대기하도록 할 시간을 분 단위로 입력합니다. 기본값은 60분입니다. 유효 범위는 6분~100분입니다.
세션 정보	
Invalidate(무효화**)**	종료할 세션 ID 옆의 확인란을 선택하고 **Invalidate(**무효화**)**를 클릭합니다.

관련 항목

관리자 액세스 설정, 242 페이지
관리자에 대한 세션 시간 초과 구성, 246 페이지
활성 관리 세션 종료, 246 페이지



5 장

유지 관리 및 모니터링

적응형 네트워크 제어

ANC(Adaptive Network Control)는 관리 노드에서 실행되는 서비스입니다. 이 서비스는 엔드포인트의 네트워크 액세스를 모니터링하고 제어합니다. ANC는 ISE 관리자가 관리자 GUI에서 호출하며 타사 시스템에서 pxGrid를 통해 호출할 수도 있습니다. ANC는 유선 및 무선 구축을 지원하며, 이를 위해서는 Premier 라이선스가 필요합니다.

ANC를 사용하여 시스템의 전체 권한 부여 정책을 수정하지 않고도 권한 부여 상태를 변경할 수 있습니다. ANC에서는 엔드포인트를 격리할 때 권한 부여 상태를 설정할 수 있습니다. 따라서 ANCPolicy를 확인하도록 정의된 권한 부여 정책은 네트워크 액세스를 제한하거나 거부할 수 있습니다. 전체 네트워크 액세스가 가능하도록 엔드포인트를 격리 해제할 수 있습니다. 네트워크에서 엔드포인트 연결이 끊어진 NAS(Network Attached System)의 포트를 종료할 수도 있습니다.

한 번에 격리할 수 있는 사용자 수에는 제한이 없습니다. 또한 격리 기간 길이에도 시간 제약 조건이 없습니다.

ANC를 통해 네트워크 액세스를 모니터링하고 제어하려면 다음 작업을 수행하십시오.

- 격리: 예외 정책(권한 부여 정책)을 사용하여 네트워크에 대한 엔드포인트 액세스를 제한하거나 거부할 수 있습니다. ANCPolicy에 따라 다른 권한 부여 프로파일(권한)을 할당하려면 예외 정책을 생성해야 합니다. 격리 상태로 설정하면 근본적으로 엔드포인트가 기본 VLAN에서 지정된 격리 VLAN으로 이동합니다. 엔드포인트와 동일한 NAS에서 지원되는 격리 VLAN을 먼저 정의해야 합니다.
- 격리 해제: 엔드포인트의 네트워크에 대한 전체 액세스를 허용하는 격리 상태를 되돌릴 수 있습니다. 이는 엔드포인트를 원래 VLAN으로 되돌리면 발생합니다.
- 종료: NAS의 포트를 비활성화하고 네트워크에서 엔드포인트 연결을 끊을 수 있습니다. 엔드포인트가 연결된 NAS에서 포트가 종료되면 NAS에서 포트를 다시 수동으로 재설정합니다. 이렇게 하면 엔드포인트를 네트워크에 연결할 수 있으며, 이는 무선 구축에 사용할 수 없습니다.

격리 및 격리 해제 작업은 활성 엔드포인트의 세션 디렉토리 보고서에서 트리거될 수 있습니다.

참고 격리된 세션이 격리 해제된 경우 새로 격리 해제된 세션의 시작 방법은 스위치 컨피그레이션에 지정된 인증 방법에 따라 달라집니다.

참고 Cisco ISE 1.4부터 ANC가 EPS(Endpoint Protection Services)를 대체합니다. ANC는 추가 분류 및 성능 개선을 제공합니다. 때때로 일부 ANC 작업에서 ERS 속성을 사용하는 것이 가능할 수도 있지만, ANC 속성을 사용하는 것이 좋습니다.

Cisco ISE에서 적응형 네트워크 제어 활성화

ANC는 기본적으로 비활성화되어 있습니다. ANC는 PxGrid가 활성화된 경우에만 활성화되며, 관리 포털에서 서비스를 수동으로 비활성화할 때까지 활성화된 상태로 유지됩니다.

네트워크 액세스 설정 구성

ANC를 사용하면 엔드포인트의 네트워크 액세스 상태를 격리, 격리 해제 또는 포트 종료로 재설정할 수 있습니다. 이는 네트워크의 엔드 포인트에 대한 권한 부여 정도를 정의합니다.

엔드포인트 IP 주소 또는 MAC 주소를 사용하여 엔드포인트가 연결되어 있는 NAS(Network Access Server) 포트를 종료하거나 엔드포인트를 격리 또는 격리 해제할 수 있습니다. 격리 및 격리 해제 작업은 동시에 수행하지 않는 경우 같은 엔드포인트에 대해 여러 번 수행할 수 있습니다. 네트워크에서 악의적인 엔드포인트가 검색되면 ANC를 사용해 NAS 포트를 닫는 방법으로 엔드포인트 액세스를 종료할 수 있습니다.

ANC 정책을 엔드포인트에 할당하려면 다음을 수행합니다.

시작하기 전에

- ANC를 활성화합니다.
- ANC용 권한 부여 프로파일 및 예외 유형 권한 권한 부여 정책을 생성합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Adaptive Network Control(**적응형 네트워크 제어**)** > **Policy List(**정책 목록**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** ANC 정책의 이름을 입력하고 EPS 작업을 지정합니다. 다음 옵션을 사용할 수 있습니다.

- 격리
- Shut_Down
- Port_Bounce

작업은 하나 또는 여러 개 선택할 수 있지만 Shut_Down 및 Port_Bounce는 다른 ANC 작업과 결합할 수 없습니다.

단계 **4** **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택하고 정책 집합을 확장합니다.

단계 **5** ANCPolicy 속성을 사용하여 ANC 정책을 해당하는 권한 부여 정책과 연결합니다.

단계 **6** **Operations(**작업**) > Adaptive Network Control(**적응형 네트워크 제어**) > Endpoint Assignment(**엔드포인트 할당**)**를 선택합니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** 엔드포인트의 IP 주소 또는 MAC 주소를 입력하고 **Policy Assignment(**정책 할당**)** 드롭다운 목록에서 정책을 선택합니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

ANC를 통해 네트워크 액세스에 대한 권한 부여 프로파일 생성

ANC에서 사용할 권한 부여 프로파일을 생성하십시오. 이렇게 하면 Standard Authorization Profiles(표준 권한 부여 프로파일) 목록에 해당 권한 부여 프로파일이 표시됩니다. 네트워크에서 엔드포인트를 인증하고 권한을 부여할 수 있지만, 해당 엔드포인트는 네트워크에만 액세스하도록 제한됩니다.

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

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 권한 부여 프로파일의 고유한 이름과 설명을 입력하고 **Access Type(**액세스 유형**)**은 **ACCESS_ACCEPT**로 업데이트합니다.

단계 **4** **DACL Name(DACL** 이름**)** 확인란을 선택하고 드롭다운 목록에서 **DENY_ALL_TRAFFIC**을 선택합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

예외 권한 부여 정책은 특수한 조건이나 권한 또는 즉각적인 요건에 대한 제한적 액세스 권한을 부여하는 데 사용됩니다. ANC 권한 부여의 경우에는 모든 표준 권한 부여 정책보다 먼저 처리되는 격리 예외 정책을 생성해야 합니다. 다음 조건을 사용하여 예외 규칙을 생성하십시오.

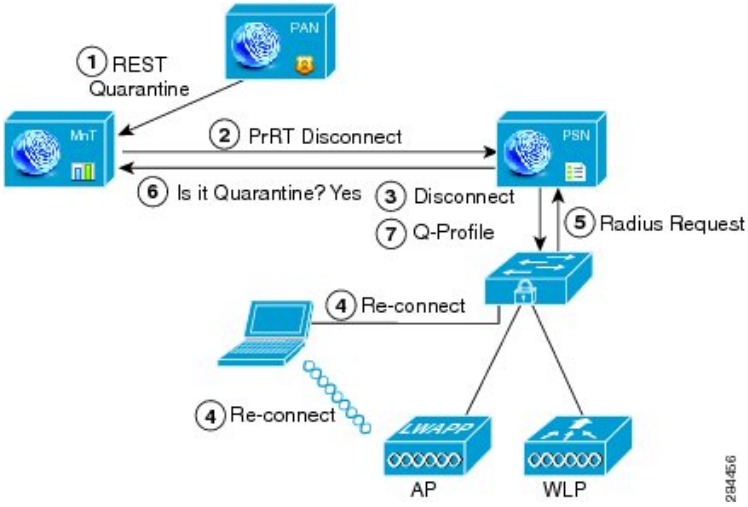
Session:ANCPolicy EQUALS Quarantine

ANC 격리 및 격리 해제 흐름

ANC를 사용하여 선택한 엔드포인트를 격리해 네트워크에 대한 액세스를 제한할 수 있습니다. 엔드포인트를 격리하고 상태에 따라 다른 권한 부여 프로파일을 할당하는 예외 권한 부여 정책을 설정할 수 있습니다. 권한 부여 프로파일은 지정된 네트워크 서비스에 대한 액세스를 허용하는 권한 부여 정책에 정의하는 권한의 컨테이너 역할을 합니다. 권한 부여가 완료되면 네트워크 액세스 요청에 대한 권한이 부여됩니다. 그런 다음 엔드포인트가 검증되면 네트워크에 대한 전체 액세스를 허용하도록 엔드포인트를 격리 해제할 수 있습니다.

이 그림에 나타난 격리 플로우에서는 권한 부여 규칙이 구성되었으며 ANC 세션이 설정된 것으로 가정합니다.

그림 ***11: ANC*** 격리 플로우



1. 클라이언트 디바이스가 무선 디바이스(WLC)를 통해 네트워크에 로그인하고, 관리 노드(PAP)에서 모니터링 노드(MnT)로 격리 REST API 호출이 실행됩니다.
2. 그런 다음 모니터링 노드는 정책 서비스 Cisco ISE 노드(PDP)를 통해 PrRT를 호출하여 CoA(Certificate of Authorization)를 불러옵니다.
3. 클라이언트 디바이스 연결이 끊어집니다.
4. 클라이언트 디바이스가 다시 인증되고 재연결됩니다.
5. 클라이언트 디바이스에 대한 RADIUS 요청이 모니터링 노드로 다시 보내집니다.
6. 확인이 진행되는 동안 클라이언트 디바이스가 격리됩니다.
7. Q-Profile 권한 부여 정책이 적용되고 클라이언트 디바이스가 검증됩니다.
8. 클라이언트 디바이스가 격리 해제되고 네트워크에 대한 전체 액세스가 제공됩니다.

ANC NAS 포트 종료 흐름

엔드포인트 IP 주소 또는 MAC 주소를 사용하여 엔드포인트가 연결되어 있는 NAS 포트를 종료할 수 있습니다.

종료하면 MAC 주소에 대해 지정된 IP 주소를 기반으로 NAS 포트를 닫을 수 있습니다. 엔드포인트를 네트워크에 다시 연결하려면 포트를 수동으로 복구해야 합니다. 이러한 복구는 유선 미디어를 통해 연결된 엔드포인트에만 적용됩니다.

일부 디바이스에서는 종료가 지원되지 않을 수도 있습니다. 그러나 대부분의 스위치는 종료 명령을 지원합니다. getResult() 명령을 사용하여 종료가 정상적으로 실행되는지를 확인할 수 있습니다.

아래 그림에는 ANC 종료 흐름이 나와 있습니다. 클라이언트 디바이스에서는 이 디바이스가 네트워크에 액세스하는 데 사용하는 NAS에서 종료 작업이 수행됩니다.

그림 ***12: ANC*** 종료 흐름

엔드포인트 제거 설정

ID 그룹 및 기타 조건을 기준으로 규칙을 구성하여 엔드포인트 제거 정책을 정의할 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Endpoint Purge(**엔드포인트 제거**)**를 선택합니다. 지정된 엔드포인트를 제거하지 않고 선택한 프로파일링 조건을 기준으로 하여 엔드포인트를 제거할 수 있습니다.

엔드포인트 제거 작업을 예약할 수 있습니다. 이 엔드포인트 제거 예약은 기본적으로 활성화되어 있습니다. Cisco ISE는 기본적으로 30일 초과하는 엔드포인트 및 등록된 디바이스를 삭제합니다. 제거 작업은 기본 PAN에서 구성한 표준 시간대를 기준으로 매일 오전 1시(자정)에 실행됩니다.

엔드포인트 제거는 3분마다 5천개가 넘는 엔드포인트를 삭제합니다.

아래에는 엔드포인트를 비우기하는 데 사용할 수 있는 몇 가지 조건이 예제와 함께 나와 있습니다.

- InactivityDays - 엔드포인트에 대한 마지막 프로파일링 활동 또는 업데이트 이후로 경과한 일 수입니다.
  - 이 조건 시간이 흐르면서 누적된 오래된 디바이스를 제거합니다. 여기에는 대게 일반적으로 임시 게스트 또는 개인 디바이스 또는 사용 중단된 디바이스가 포함됩니다. 이러한 엔드포인트는 더 이상 활성화되지 않거나 가까운 미래에 표시되지 않을 가능성이 높아 구축에서 문제가 발생할 소지가 있습니다. 혹시라도 다시 연결되는 경우 필요에 따라 재검색되거나 프로파일링되거나 등록됩니다.
  - 엔드포인트에서 업데이트가 있을 때는 프로파일링이 활성화된 경우에만 InactivityDays가 0으로 재설정됩니다.
- ElapsedDays - 객체가 생성된 이후로 경과한 일 수입니다.
  - 이 조건은 게스트 또는 계약자 엔드포인트 또는 네트워크 액세스에 WebAuth를 사용하는 직원과 같이 지정된 기간 동안 인증되지 않은 또는 조건부 액세스가 부여된 엔드포인트에 사용될 수 있습니다. 허용되는 연결 유예 기간이 지난 후에는 완전히 다시 인증되고 등록되어야 합니다.
- PurgeDate - 엔드포인트를 제거하는 날짜입니다.

- 이 옵션은 생성 시간 또는 시작 시간에 관계없이 특정 시간 동안 액세스가 부여된 특수 이벤트 또는 그룹에 사용할 수 있습니다. 이 경우 모든 엔드포인트를 동시에 제거할 수 있습니다. 예를 들어 무역 박람회, 컨퍼런스 또는 주간 교육 과정에서 각 주마다 새 멤버가 참여하는 경우 절대 일, 주, 월이 아니라 특정 주나 월에 액세스가 부여됩니다.

격리된 엔드포인트가 정책 변경 후 인증을 갱신하지 않음

문제

정책 변경 또는 ID 추가 후 인증이 실패하며 재인증이 수행되지 않습니다. 인증이 실패하거나 해당 엔드포인트가 네트워크에 계속 연결할 수 없습니다. 이 문제는 사용자 역할에 할당된 포스처 정책에 따라 포스처 평가를 수행할 수 없는 클라이언트 머신에서 발생하는 경우가 많습니다.

가능한 원인

클라이언트 머신의 인증 타이머 설정 또는 스위치의 인증 간격이 올바르게 설정되어 있지 않습니다.

해결책

이 문제를 해결할 수 있는 몇 가지 방법은 다음과 같습니다.

1. Cisco ISE의 세션 상태 요약 보고서에서 지정된 NAD 또는 스위치를 확인하여 인터페이스에 적절한 인증 간격이 구성되어 있는지 파악합니다.
2. NAD/스위치에서 "show running configuration"을 입력한 다음 인터페이스가 적절한 "authentication timer start" 설정으로 구성되어 있는지 확인합니다. "authentication timer restart 15" 및 "authentication timer reauthenticate 15" 등을 예로 들 수 있습니다.
3. Cisco ISE에서 수행되었을 수 있는 컨피그레이션 변경 이후 "interface shutdown" 및 "no shutdown"을 입력하여 NAD/스위치에서 포트를 반송하고 재인증을 강제로 수행해 봅니다.

참고 CoA에는 MAC 주소 또는 세션 ID가 필요하므로 네트워크 디바이스 SNMP 보고서에 표시되어 있는 포트는 반송하지 않는 것이 좋습니다.

IP 주소 또는 MAC 주소를 찾을 수 없으면 ANC 작업이 실패함

엔드포인트에 대한 활성 세션에 IP 주소 관련 정보가 포함되어 있지 않으면 엔드포인트에서 수행하는 ANC 작업이 실패합니다. 해당 엔드포인트의 MAC 주소 및 세션 ID에도 이 규칙이 적용됩니다.

참고 ANC를 통해 엔드포인트의 권한 부여 상태를 변경하려는 경우에는 해당 엔드포인트의 IP 주소 또는 MAC 주소를 제공해야 합니다. IP 주소 또는 MAC 주소를 엔드포인트에 대한 활성 세션에서 찾을 수 없는 경우 다음과 같은 오류 메시지가 표시됩니다.

No active session found for this MAC address, IP Address or Session ID(□ MAC □□, IP □□ □□ □□ ID□ □□ □□ □ □□ □□ □ □□□□).

.

외부에서 인증된 관리자가 **ANC** 작업을 수행할 수 없음

외부에서 인증된 관리자가 라이브 세션에서 CoA-격리를 실행하려고 하면 Cisco ISE에서 다음 오류 메시지가 반환됩니다.

xx:xx:xx:xx:xx:xx□ □□ CoA □□ □□□ □□□ □ □□□□. □□: □□□□ □□□□ □□ □ □□□□. □□□□ □□ □□□□ □□□ □□□□ □□□□ □ □□□□.

외부에서 인증된 관리자가 ANC 작업을 Cisco ISE의 **Operations(**작업**)**에서 엔드포인트의 IP 주소 또는 MAC 주소를 사용하여 수행하는 경우 Cisco ISE에서는 다음 오류 메시지가 반환됩니다.

□□ □□: □□□□ □□□□ □□ □ □□□□. □□□□ □□ □□□□ □□□ □□□□ □□□□ □ □□□□.

백업 데이터 유형

Cisco ISE에서는 기본 PAN 또는 모니터링 노드의 데이터를 백업할 수 있습니다. 백업은 CLI 또는 사용자 인터페이스에서 수행할 수 있습니다.

Cisco ISE에서는 다음 데이터 유형을 백업할 수 있습니다.

- 컨피그레이션 데이터 - 애플리케이션별 데이터와 Cisco ADE 운영체제 컨피그레이션 데이터를 모두 포함합니다. 백업은 GUI 또는 CLI를 사용하여 기본 PAN을 통해 수행할 수 있습니다.
- 작업 데이터 - 모니터링 및 문제 해결 데이터를 포함합니다. 백업은 기본 PAN GUI를 통해 또는 모니터링 노드용 CLI를 사용하여 수행할 수 있습니다.

Cisco ISE가 VMware에서 실행될 때는 ISE 데이터 백업용으로 VMware 스냅샷이 지원되지 않습니다.

참고 VMware 스냅샷은 지정된 시점에 VM의 상태를 저장하므로, Cisco ISE는 VMware 스냅샷으로 ISE 데이터를 백업하는 기능은 지원하지 않습니다. 멀티 노드 Cisco ISE 구축에서는 모든 노드의 데이터가 현재 데이터베이스 정보와 지속적으로 동기화됩니다. 스냅샷을 복원하면 데이터베이스 복제 및 동기화 문제가 발생할 수 있습니다. 데이터 보관 및 복구를 위해 Cisco ISE에 포함된 백업 기능을 사용하는 것이 좋습니다.

VMware 스냅샷 또는 서드파티 백업 서비스를 사용하여 Cisco ISE 데이터를 백업하면 Cisco ISE 서비스가 중단될 수 있습니다. VMware 또는 CommVault SAN 레벨 백업과 같은 기타 서드파티 백업 서비스에서 백업을 시작하면 충돌이 일관되게 유지되도록 파일 시스템이 정지되어 Cisco ISE 기능이 정지될 수 있습니다. Cisco ISE 구축에서 서비스를 다시 시작하려면 재부팅해야 합니다.

복원 작업은 이전 Cisco ISE 버전의 백업 파일을 사용하여 수행하고 이후 버전에서 복원할 수 있습니다. 예를 들어 Cisco ISE, 릴리스 1.3 또는 1.4의 ISE 노드 백업이 있는 경우 Cisco ISE, 릴리스 2.1에서 복원할 수 있습니다.

Cisco ISE, 릴리스 3.0은 릴리스 2.4 이상에서 가져온 백업을 복원하도록 지원합니다.

저장소 백업 및 복구

Cisco ISE에서는 관리 포털을 통해 저장소를 생성하거나 삭제할 수 있습니다. 다음과 같은 저장소 유형을 생성할 수 있습니다.

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

참고 저장소는 각 디바이스에 대해 로컬입니다.

모든 구축 유형(소규모, 중간 규모, 대규모)에 대해 저장소 크기를 최소 100GB로 설정하는 것이 좋습니다.

다음 표에는 Cisco ISE 작업과 외부 저장소 유형 간의 지원 가능성 정보가 나와 있습니다.

표 *35:* 외부 저장소에 대한 지원 가능성 매트릭스

Repository Type(저장소 유형**)**	컨피그레이션 백업	컨피그레이션 복원	업그레이드	운영 백업	운영 복원	지원 번들	사용자 인터페이스의 검증	사용자 인터페이스에서 보고서 내보내기	사용자 인터페이스에서 정책 내보내기
FTP	√	√	√	√	√	√	√	√	√
SFTP	√	√	√	√	√	√	√	√	√
TFTP	√	√	√	√	√	√	X	√	√
HTTP	X	X	√	X	X	X	X	X	X
HTTPS	X	*X*	√	X	X	X	X	X	X
NFS	√	√	√	√	√	√	√	√	√

저장소 생성

CLI 및 GUI를 사용하여 저장소를 생성할 수 있습니다. 다음과 같은 이유로 인해 GUI를 사용하는 것이 좋습니다.

- CLI를 통해 생성하는 저장소는 로컬에 저장되며 다른 구축 노드로 복제되지 않습니다. 이러한 저장소는 GUI의 저장소 페이지에 나열되지 않습니다.
- 기본 PAN에서 생성하는 저장소는 다른 구축 노드로 복제됩니다.

키는 GUI의 기본 PAN에서만 생성되므로 업그레이드 중에 새 기본 관리자의 GUI에서 키를 다시 생성하고 SFTP 서버로 내보내야 합니다. 구축 환경에서 노드를 제거하는 경우 비관리 노드의 GUI에서 키를 생성하고 SFTP 서버로 내보내야 합니다.

RSA 공개 키 인증을 사용하여 Cisco ISE에서 SFTP 저장소를 구성할 수 있습니다. 관리자가 생성한 비밀번호를 사용하여 데이터베이스 및 로그를 암호화하는 대신 보안 키를 사용하는 RSA 공개 키 인증을 선택할 수 있습니다. RSA 공개 키로 생성된 SFTP 저장소의 경우 GUI를 통해 생성된 저장소는 CLI에서 복제되지 않으며 CLI를 통해 생성된 저장소는 GUI에서 복제되지 않습니다. CLI 및 GUI에서 동일한 저장소를 구성하려면 CLI 및 GUI 모두에서 RSA 공개 키를 생성하고 두 키를 모두 SFTP 서버로 내보냅니다.

참고 Cisco ISE는 FIPS 모드가 ISE에서 활성화되지 않은 경우에도 FIPS 모드에서 아웃바운드 SSH 또는 SFTP 연결을 시작합니다. ISE와 통신하는 원격 SSH 또는 SFTP 서버가 FIPS 140-2 승인 암호화 알고리즘을 허용하는지 확인합니다.

Cisco ISE는 임베디드 FIPS 140-2 검증 암호화 모듈을 사용합니다. FIPS 규정 준수 클레임에 대한 자세한 내용은 FIPS 규정 준수 편지를 참고해 주십시오.

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자 권한이 있어야 합니다.
- RSA 공개 키 인증을 사용하여 SFTP 저장소를 생성하려면 다음 단계를 수행합니다.
  - SFTP 저장소에서 RSA 공개 키 인증을 활성화합니다.
  - **crypto host_key add** 명령을 사용하여 Cisco ISE CLI에서 SFTP 서버의 호스트 키를 입력합니다. 호스트 키 문자열은 저장소 구성 페이지의 **Path(**경로**)** 필드에 입력하는 호스트 이름과 일치해야 합니다.
  - 키 페어를 생성하고 GUI에서 공개 키를 로컬 시스템으로 내보냅니다. Cisco ISE CLI에서 **crypto key generate rsa passphrase** *test123* 명령을 사용하여 키 페어를 생성합니다. 여기서 passphrase는 4자보다 커야 하며 모든 저장소(로컬 디스크 또는 기타 구성된 저장소)로 내보내야 합니다.
  - 내보낸 RSA 공개 키를 PKI 지원 SFTP 서버에 복사하고 "authorized_keys" 파일에 추가합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Maintenance(**유지 관리**)** > **Repository(**저장소**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Maintenance(**유지 관리**)** > **Repository(**저장소**)**.

단계 **3** 새 저장소를 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 **4** 새 저장소를 설정하는 데 필요한 값을 입력합니다. 필드에 대한 설명은 저장소 설정, 262 페이지를 참고하십시오.

단계 **5** 저장소를 생성하려면 **Submit(**제출**)**을 클릭합니다.

단계 **6** 왼쪽의 **Operations(**운영**)** 탐색창에서 **Repository(**저장소**)**를 클릭하거나 **Repository(**저장소**)** 창 위쪽의 **Repository List(**저장소 목록**)** 링크를 클릭해 저장소 목록 페이지로 이동하여 저장소가 정상적으로 생성되었는지 확인합니다.

다음에 수행할 작업

- 생성한 저장소가 유효한지 확인합니다. **Repository Listing(**저장소 목록**)** 창에서 확인할 수 있습니다. 해당 저장소를 선택하고 **Validate(**검증**)**를 클릭합니다. 또는 Cisco ISE 명령줄 인터페이스에서 다음 명령을 실행할 수 있습니다.

  show repository *repository-name*

여기서 *repository_name*은 생성한 저장소의 이름입니다.

참고 저장소를 생성할 때 입력한 경로가 없으면 다음 오류가 표시됩니다.

```
%Invalid Directory
```

- 온디맨드 백업을 실행하거나 백업을 예약합니다.

저장소 설정

다음 표에서는 백업 파일을 저장하기 위한 저장소를 생성하는 데 사용할 수 있는 **Repository List(**저장소 목록**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Maintenance(**유지 관리**)** > **Repository(**저장소**)** 입니다.

표 ***36:*** 저장소 설정

필드	사용 지침
Repository(저장소**)**	저장소의 이름을 입력합니다. 영숫자 문자를 입력할 수 있으며 최대 길이는 80자입니다.
Protocol(프로토콜**)**	사용 가능한 프로토콜 중에서 사용하려는 프로토콜 하나를 선택합니다.
Server Name(서버 이름**)**	(TFTP, HTTP, HTTPS, FTP, SFTP 및 NFS의 경우 필수) 저장소를 생성할 서버의 호스트 이름 또는 IPv4 주소(IPv4 또는 IPv6)를 입력합니다. 참고 IPv6 주소를 사용해 저장소를 추가하는 경우 ISE eth0 인터페이스가 IPv6 주소로 구성되어야 합니다.
경로	저장소의 경로를 입력합니다. 경로는 유효해야 하며 저장소를 생성할 때 이미 있는 상태여야 합니다. 이 값은 서버의 루트 디렉토리를 나타내는 슬래시 두 개(//) 또는 하나(/)로 시작할 수 있습니다. 그러나 FTP 프로토콜의 경우 슬래시 하나(/)는 루트 디렉토리가 아닌 로컬 디바이스 홈 디렉토리의 FTP를 나타냅니다.
PKI 인증 활성화	(선택 사항, SFTP 저장소에만 적용 가능) SFTP 저장소에서 RSA 공개 키 인증을 활성화하려면 이 확인란을 선택합니다.

필드	사용 지침
사용자 이름	(FTP, SFTP 의 경우 필수) 지정한 서버에 대한 쓰기 권한이 있는 사용자 이름을 입력합니다. 영숫자 문자만 입력할 수 있습니다.
Password(비밀번호**)**	(FTP, SFTP 의 경우 필수) 지정한 서버에 액세스하는 데 사용할 비밀번호를 입력합니다. 비밀번호는 0~9, a~z, A~Z, -, ., |, @, #,$, ^, &, *, (,), +, = 문자를 포함할 수 있습니다.

관련 항목

저장소 백업 및 복구, 259 페이지
저장소 생성, 260 페이지

SFTP 저장소에서 RSA 공개 키 인증 활성화

SFTP 서버에서 각 노드에는 CLI와 GUI용으로 하나씩, 2개의 RSA 공개 키가 있어야 합니다. SFTP 저장소에서 RSA 공개 키 인증을 활성화하려면 다음 단계를 수행합니다.

단계 **1** */etc/ssh/sshd_config.file*을 편집할 권한이 있는 계정으로 SFTP 서버에 로그인합니다.

참고 *sshd_config* 파일의 위치는 운영체제 설치에 따라 달라질 수 있습니다.

단계 **2** **vi /etc/ssh/sshd_config** 명령을 입력합니다.

sshd_config 파일의 내용이 나열됩니다.

단계 **3** RSA 공개 키 인증을 활성화하려면 다음 줄에서 "#" 기호를 제거합니다.

- RSAAuthentication: yes(예)
- PubkeyAuthentication: yes(예)

  참고 공개 인증 키가 no인 경우 yes로 변경합니다.

- AuthorizedKeysFile ~/.ssh/authorized_keys

온디맨드 및 예약된 백업

기본 PAN 및 기본 모니터링 노드에 대한 온디맨드 백업을 구성할 수 있습니다. 데이터를 즉시 백업하려면 온디맨드 백업을 수행합니다.

Cisco ISE에서는 한 번, 매일, 매주, 매월 실행되도록 예약할 수 있는 시스템 레벨 백업을 예약할 수 있습니다. 백업 작업에는 시간이 오래 걸릴 수 있으므로 중단되지 않도록 백업을 예약할 수 있습니다. 관리 포털에서 백업을 예약할 수 있습니다.

참고 내부 CA를 사용하는 경우 CLI를 사용하여 인증서 및 키를 내보내야 합니다. 관리 포털에서 수행하는 백업은 CA 체인을 백업하지 않습니다.

자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드의 "기본 설정" 장에서 "Cisco ISE CA 인증서 및 키 내보내기" 섹션을 참고하십시오.

관련 항목

유지 관리 설정

온디맨드 백업 수행

온디맨드 백업을 수행하여 컨피그레이션 또는 모니터링(운영) 데이터를 즉시 백업할 수 있습니다. 복구 작업에서는 백업을 가져오는 시간의 컨피그레이션 상태로 Cisco ISE를 복원합니다.

중요 백업 및 복구를 수행 중인 경우, 복구는 대상 시스템의 신뢰할 수 있는 인증서 목록을 소스 시스템의 인증서 목록으로 덮어씁니다. 백업 및 복구 기능이 내부 CA(Certificate Authority) 인증서와 연계된 개인 키를 포함하지 않는다는 점이 매우 중요합니다.

한 시스템에서 다른 시스템으로 백업 및 복구하는 경우 오류를 방지하려면 다음 옵션 중 하나를 선택해야 합니다.

- 옵션 **1:**

  CLI를 통해 소스 ISE 노드에서 CA 인증서를 내보내고 대상 시스템에 가져옵니다.

  장점**:** 소스 시스템에서 엔드포인트에 발급한 모든 인증서는 계속해서 신뢰됩니다. 대상 시스템에서 발행된 모든 신규 인증서는 동일한 키를 사용하여 서명됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

- 옵션 **2:**

  복원 프로세스 이후에 내부 CA용으로 모든 신규 인증서를 생성합니다.

  장점**:** 원래 소스 인증서 또는 원래 대상 인증서가 모두 사용되지 않아 안전하기 때문에 권장되는 옵션입니다. 원래 소스 시스템에서 발급된 인증서는 계속해서 신뢰됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

시작하기 전에

- 온디맨드 백업을 수행하기 전에 Cisco ISE의 백업 데이터 유형에 대해 기본적으로 파악해야 합니다.
- 백업 파일을 저장할 저장소를 생성했는지 확인합니다.
- 로컬 저장소를 사용하여 백업해서는 안 됩니다. 원격 모니터링 노드의 로컬 저장소에는 모니터링 데이터를 백업할 수 없습니다.
- 백업을 가져오기 전에 모든 인증서 관련 변경을 수행해야 합니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

참고 CD-ROM, HTTP, HTTPS 또는 TFTP 저장소 유형은 백업 및 복구 작업에서 지원되지 않습니다. 이러한 저장소 유형은 읽기 전용이거나 프로토콜이 파일 나열을 지원하지 않기 때문입니다. 백업을 복원하려면 저장소를 선택하고 **Restore(**복원**)**를 클릭합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **3** 백업 유형을 Configuration(구성) 또는 Operational(운영) 중에서 선택합니다.

단계 **4** **Backup Now(**지금 백업**)**를 클릭합니다.

단계 **5** 필요한 값을 입력하여 백업을 수행합니다.

단계 **6** **Backup(**백업**)**을 클릭합니다.

단계 **7** 백업이 정상적으로 완료되었는지 확인합니다.

Cisco ISE는 백업 파일 이름에 타임스탬프를 추가하여 파일을 지정된 저장소에 저장합니다. Cisco ISE는 타임스탬프 외에 CFG 태그(구성 백업의 경우) 및 OPS 태그(운영 백업의 경우)도 추가합니다. 백업 파일이 지정된 저장소에 있는지 확인합니다.

분산형 구축에서는 백업을 실행할 때 노드를 승격하거나 노드의 역할을 변경하지 마십시오. 노드 역할을 변경해도 모든 프로세스가 종료되는 것은 아니며 백업을 동시에 실행하는 경우 데이터가 다소 불일치할 수도 있습니다. 백업이 완료될 때까지 기다린 후에 노드 역할을 변경해 주십시오.

백업이 실행 중일 때는 노드를 승격하지 마십시오. 이렇게 하면 모든 프로세스가 종료되며 백업을 동시에 실행하는 경우 데이터가 다소 불일치할 수도 있습니다. 백업이 완료될 때까지 기다린 후에 노드를 변경해 주십시오.

참고 백업이 실행 중일 때 높은 CPU 사용률이 관찰되고 높은 로드 평균 경보가 표시될 수 있습니다. 백업이 완료되면 CPU 사용률이 정상으로 돌아옵니다.

관련 항목

Cisco ISE 복원 작업, 270 페이지

인증 및 권한 부여 정책 컨피그레이션 내보내기, 276 페이지

온디맨드 백업 설정

다음 표에서는 임의의 시점에 백업을 가져오는 데 사용할 수 있는 **On-Demand Backup(**온디맨드 백업**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup & Restore(**백업 및 복구**)**입니다.

표 ***37:*** 온디맨드 백업 설정

필드 이름	사용 지침
Type(유형**)**	다음 중 하나를 선택합니다. • **Configuration Data Backup(**컨피그레이션 데이터 백업**)**: 애플리케이션별 데이터와 Cisco ADE 운영체제 컨피그레이션 데이터를 모두 포함합니다. • **Operational Data Backup(**운영 데이터 백업**)**: 모니터링 및 문제 해결 데이터를 포함합니다.
Backup Name(백업 이름**)**	백업 파일의 이름을 입력합니다.
Repository Name(저장소 이름**)**	백업 파일을 저장할 저장소입니다. 여기에 저장소 이름을 입력할 수는 없습니다. 드롭다운 목록에서 사용 가능한 저장소를 선택하는 것만 가능합니다. 백업을 실행하기 전에 저장소를 생성해야 합니다.
Encryption Key(암호화 키**)**	이 키는 백업 파일을 암호를 해독하는 데 사용됩니다.

관련 항목

백업 데이터 유형, 258 페이지
온디맨드 및 예약된 백업, 263 페이지
백업 기록, 269 페이지
백업 실패, 269 페이지
Cisco ISE 복원 작업, 270 페이지
인증 및 권한 부여 정책 컨피그레이션 내보내기, 276 페이지
분산형 환경에서 기본 및 보조 노드 동기화, 278 페이지
온디맨드 백업 수행, 264 페이지

백업 예약

온디맨드 백업을 수행하여 컨피그레이션 또는 모니터링(운영) 데이터를 즉시 백업할 수 있습니다. 복구 작업에서는 백업을 가져오는 시간의 컨피그레이션 상태로 Cisco ISE를 복원합니다.

중요 백업 및 복구를 수행 중인 경우, 복구는 대상 시스템의 신뢰할 수 있는 인증서 목록을 소스 시스템의 인증서 목록으로 덮어씁니다. 백업 및 복구 기능이 내부 CA(Certificate Authority) 인증서와 연계된 개인 키를 포함하지 않는다는 점이 매우 중요합니다.

한 시스템에서 다른 시스템으로 백업 및 복구하는 경우, 오류를 방지하려면 다음 옵션 중 하나를 선택해야 합니다.

- 옵션 **1:**

  CLI를 통해 소스 ISE 노드에서 CA 인증서를 내보내고 대상 시스템에 가져옵니다.

  장점**:** 소스 시스템에서 엔드포인트에 발급한 모든 인증서는 계속해서 신뢰됩니다. 대상 시스템에서 발행된 모든 신규 인증서는 동일한 키를 사용하여 서명됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

- 옵션 **2:**

  복원 프로세스 이후에 내부 CA용으로 모든 신규 인증서를 생성합니다.

  장점**:** 원래 소스 인증서 또는 원래 대상 인증서가 사용되므로 안전하기 때문에 권장되는 옵션입니다. 원래 소스 시스템에서 발행된 인증서는 계속해서 신뢰됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

시작하기 전에

- 백업을 예약하기 전에 Cisco ISE의 백업 데이터 유형에 대해 기본적으로 파악해야 합니다.
- 저장소를 구성했는지 확인합니다.
- 로컬 저장소를 사용하여 백업해서는 안 됩니다. 원격 모니터링 노드의 로컬 저장소에는 모니터링 데이터를 백업할 수 없습니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- Cisco ISE 1.1 이하 릴리스에서 Cisco ISE 1.2로 업그레이드한 경우에는 예약 백업을 재구성해야 합니다. *Cisco Identity Services Engine* 업그레이드 설명서 릴리스 *1.2*의 알려진 업그레이드 문제 섹션을 참고해 주십시오.

참고 CD-ROM, HTTP, HTTPS 또는 TFTP 저장소 유형은 백업 및 복구 작업에서 지원되지 않습니다. 이러한 저장소 유형은 읽기 전용이거나 프로토콜이 파일 나열을 지원하지 않기 때문입니다.

예약 백업 설정

다음 표에서는 전체 또는 증분 백업을 복구하는 데 사용할 수 있는 Scheduled Backup(예약 백업) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**입니다.

표 ***38:*** 예약 백업 설정

필드 이름	사용 지침
Type(유형**)**	다음 중 하나를 선택합니다. • **Configuration Data Backup(**컨피그레이션 데이터 백업**)**: 애플리케이션별 데이터와 Cisco ADE 운영체제 컨피그레이션 데이터를 모두 포함합니다. • **Operational Data Backup(**운영 데이터 백업**)**: 모니터링 및 문제 해결 데이터를 포함합니다.
Name(이름**)**	백업 파일의 이름을 입력합니다. 선택에 대한 설명이 포함된 이름을 입력할 수 있습니다. Cisco ISE는 백업 파일명에 타임스탬프를 추가하여 해당 파일을 저장소에 저장합니다. 일련의 백업을 구성하더라도 고유한 백업 파일명을 갖게 됩니다. Scheduled Backup(예약 백업) 목록 창에서 백업 파일명이 "backup_occur"로 추가되어 **kron** 수행 작업 파일임을 나타냅니다.
Description(설명**)**	백업의 설명을 입력합니다.
Repository Name(저장소 이름**)**	백업 파일이 저장되는 저장소를 선택합니다. 여기에 저장소 이름을 입력할 수는 없습니다. 드롭다운 목록에서 사용 가능한 저장소를 선택하는 것만 가능합니다. 백업을 실행하기 전에 저장소를 생성해야 합니다.
Encryption Key(암호화 키**)**	백업 파일을 암호화하고 암호를 해독하는 데 사용할 키를 입력합니다.
Schedule Options(예약 옵션**)**	예약 백업의 빈도를 선택하고 그에 따라 기타 옵션을 입력합니다.

관련 항목

백업 데이터 유형, 258 페이지
온디맨드 및 예약된 백업, 263 페이지
백업 기록, 269 페이지
백업 실패, 269 페이지
Cisco ISE 복원 작업, 270 페이지
인증 및 권한 부여 정책 컨피그레이션 내보내기, 276 페이지
분산형 환경에서 기본 및 보조 노드 동기화, 278 페이지
CLI를 사용한 복원, 269 페이지
백업 예약, 267 페이지

CLI를 사용한 복원

CLI와 GUI 둘 다에서 백업을 예약할 수 있지만 GUI를 사용하는 것이 좋습니다. 그러나 보조 모니터링 노드에 대한 운영 백업을 수행하려는 경우 CLI에서만 가능합니다.

백업 기록

백업 기록에서는 예약 백업 및 온디맨드 백업에 대한 기본 정보를 제공합니다. 백업 이름, 백업 파일 크기, 백업이 저장된 저장소 및 백업을 가져온 시점을 나타내는 타임스탬프가 나열됩니다. 이 정보는 운영 감사 보고서와 함께 Backup and Restore(백업 및 복구) 페이지의 History(기록) 표에서 사용할 수 있습니다.

실패한 백업의 경우 Cisco ISE가 경보를 트리거합니다. 백업 기록 페이지에 실패 이유가 제공됩니다. 실패 이유는 운영 감사 보고서에서도 확인할 수 있습니다. 실패 이유가 없거나 명확지 않은 경우 Cisco ISE CLI에서 **backup-logs** 명령을 실행하여 ADE.log에서 자세한 내용을 확인할 수 있습니다.

백업 작업이 진행 중인 경우 **show backup status** CLI 명령을 사용하여 백업 작업의 진행 상황을 확인할 수 있습니다.

백업 기록은 Cisco ADE 운영체제 컨피그레이션 데이터와 함께 저장됩니다. 이 기록은 애플리케이션이 업그레이드된 후에도 계속 해당 위치에 유지되며 PAN을 재이미지화하는 경우에만 제거됩니다.

백업 실패

백업이 실패하는 경우 다음 사항을 확인해 주십시오.

- NTP 동기화 또는 서비스 장애 문제가 있는지 확인합니다. Cisco ISE의 NTP 서비스가 작동하지 않으면 Cisco ISE에서 NTP 서비스 장애 경보를 생성합니다. Cisco ISE가 구성된 모든 NTP 서버와 동기화할 수 없는 경우 Cisco ISE에서 NTP 동기화 실패 경보를 생성합니다. NTP 서비스가 중지되었거나 동기화 문제가 있는 경우 Cisco ISE 백업이 실패할 수 있습니다. Alarms(경보) dashlet을 확인하고 NTP 동기화 또는 서비스 문제를 해결한 후에 백업 작업을 다시 시도하십시오.
- 다른 백업이 동시에 실행되고 있지 않은지 확인합니다.
- 구성한 저장소에 대해 사용 가능한 디스크 공간을 확인합니다.

- 모니터링 데이터가 할당된 모니터링 데이터베이스 크기의 75%를 사용한 경우 모니터링(운영) 백업이 실패합니다. 예를 들어 모니터링 노드에 600GB가 할당되어 있고 모니터링 데이터가 스토리지의 450GB 이상을 사용한 경우 모니터링 백업이 실패합니다.
- 데이터베이스 디스크 사용량이 90%를 초과하면 데이터베이스 크기를 할당된 크기의 75% 이하로 유지하기 위해 제거가 발생합니다.

- 제거가 진행 중인지 확인합니다. 제거가 진행 중일 때에는 백업 및 복구 작업이 수행되지 않습니다.
- 저장소가 올바르게 구성되었는지 확인합니다.

Cisco ISE 복원 작업

기본 또는 독립형 관리 노드에서 컨피그레이션 데이터를 복원할 수 있습니다. 기본 PAN에서 데이터를 복원한 후에는 보조 노드를 기본 PAN과 수동으로 동기화해야 합니다.

운영 데이터를 복원하는 프로세스는 구축 유형에 따라 다릅니다.

참고 Cisco ISE의 새 백업/복원 사용자 인터페이스에서는 백업 파일 이름에 메타데이터를 사용합니다. 그러므로 백업이 완료된 후에 백업 파일 이름을 수동으로 수정해서는 안 됩니다. 백업 파일 이름을 수동으로 수정할 경우 Cisco ISE 백업/복원 사용자 인터페이스에서 백업 파일을 인식할 수 없습니다. 백업 파일 이름을 수정해야 하는 경우 Cisco ISE CLI를 사용하여 백업을 복원해야 합니다.

데이터 복원 지침

다음은 Cisco ISE 백업 데이터를 복원할 때 따라야 하는 지침입니다.

- Cisco ISE를 사용하면 ISE 노드 (A)에서 백업을 가져와서 호스트네임이 동일한(IP 주소는 다름) 다른 ISE 노드 (B)에서 복구할 수 있습니다. 그러나 노드 B에서 백업을 복구한 후에는 인증서 및 포털 그룹 태그에 문제가 발생할 수 있으므로 노드 B의 호스트네임을 변경하지 마십시오.
- 특정 표준 시간대에서 기본 PAN의 백업을 가져온 다음 다른 표준 시간대에서 다른 Cisco ISE 노드에 해당 백업을 복원하려는 경우 복원 프로세스가 실패할 수 있습니다. 백업 파일의 타임스탬프가 백업을 복원하는 Cisco ISE 노드의 시스템 시간보다 이후이면 이러한 오류가 발생합니다. 백업을 가져오고 1일 후에 동일 백업을 복원하는 경우 백업 파일의 타임스탬프가 시스템 시간 이전에 되어 복원 프로세스가 정상적으로 진행됩니다.
- 백업을 가져온 호스트와 다른 호스트 이름으로 기본 PAN에서 백업을 복원하면 기본 PAN이 독립형 모드로 설정됩니다. 그러면 구축이 손상되고 보조 노드가 작동하지 않게 됩니다. 이 경우 독립형 모드를 기본 노드로 지정하고 보조 노드에서 컨피그레이션을 재설정한 후에 기본 노드에 보조 노드를 등록해야 합니다. Cisco ISE 노드에서 컨피그레이션을 재설정하려면 Cisco ISE CLI에서 다음 명령을 입력합니다.
  - **application reset-config ise**

- 초기 Cisco ISE 설치 및 설정 후에는 시스템 표준 시간대를 변경하지 않는 것이 좋습니다.
- 구축의 노드 하나 이상에서 인증서 컨피그레이션을 변경한 경우에는 다른 백업을 가져와 독립형 Cisco ISE 노드 또는 기본 PAN에서 데이터를 복원해야 합니다. 이렇게 하지 않는 경우 이전 백업을 사용하여 데이터를 복원하려고 하면 노드 간의 통신이 실패할 수 있습니다.
- 기본 PAN에서 컨피그레이션 백업을 복원한 후에는 이전에 내보낸 Cisco ISE CA 인증서 및 키를 가져올 수 있습니다.

참고 Cisco ISE CA 인증서 및 키를 내보내지 않은 경우 기본 PAN에서 컨피그레이션 백업을 복원한 후에 기본 PAN 및 PSN(Policy Service Nodes)에서 루트 CA 및 종속 CA를 생성합니다.

- 올바른 FQDN (플래티넘 데이터베이스의 FQDN)을 사용하지 않고 플래티넘 데이터베이스를 복원하려는 경우 CA 인증서를 다시 생성해야 합니다. (이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)** > **Replace ISE Root CA certificate chain(ISE** 루트 **CA** 인증서 체인 교체**)**을 선택합니다. 그러나 올바른 FQDN을 사용하여 플래티넘 데이터베이스를 복원하는 경우 CA 인증서가 자동으로 다시 생성됩니다.
- Cisco ISE가 백업 파일을 저장하는 위치인 데이터 저장소가 필요합니다. 온디맨드 또는 예약 백업을 실행하려면 저장소를 생성해야 합니다.
- 독립형 관리 노드에 오류가 발생하는 경우에는 컨피그레이션 백업을 실행하여 해당 노드를 복원해야 합니다. 기본 PAN에 오류가 발생하는 경우에는 분산형 설정을 통해 보조 관리 노드를 기본 노드로 승격할 수 있습니다. 기본 PAN이 작동하면 기본 PAN에서 데이터를 복원할 수 있습니다.

참고 Cisco ISE는 문제 해결용으로 로그 및 구성 파일을 수집하는 데 사용할 수 있는 **backup-logs** CLI 명령도 제공합니다.

CLI에서 컨피그레이션 또는 모니터링 백업 복원

Cisco ISE CLI를 통해 컨피그레이션 데이터를 복원하려면 EXEC 모드에서 **restore** 명령을 사용합니다. 컨피그레이션 또는 운영 백업에서 데이터를 복원하려면 다음 명령을 사용합니다.

filename repository-name encryption-key name **restore repository encryption-key hash|plain include-adeos**

구문 설명

restore	컨피그레이션 또는 운영 백업에서 데이터를 복원하려면 이 명령을 입력합니다.

filename	저장소에 있는 백업된 파일의 이름입니다. 최대 120개의 영숫자를 지원합니다. 참고 파일 이름 뒤에 .tar.gpg 확장자를 추가해야 합니다(예: myfile.tar.gpg).
repository	백업이 포함되어 있는 저장소를 지정합니다.
repository-name	복원할 백업이 있는 저장소의 이름입니다.
encryption-key	(선택 사항) 백업을 복원할 사용자 맞춤화 암호화 키를 지정합니다.
hash	백업을 복원하기 위해 해시된 암호 키입니다. 뒤에 오는 암호화된(해시된) 암호 키를 지정합니다. 최대 40자를 지원합니다.
plain	백업을 복원하기 위한 일반 텍스트 암호 키입니다. 뒤에 오는 암호화되지 않은 일반 텍스트 암호 키를 지정합니다. 최대 15자를 지원합니다.
encryption-key name	암호화 키를 입력합니다.
include-adeos	(선택 사항, 컨피그레이션 백업에만 해당함) 컨피그레이션 백업에서 ADE-OS 컨피그레이션을 복원하려는 경우 이 명령 연산자 매개변수를 입력합니다. 컨피그레이션 백업을 복원할 때 이 매개변수를 포함하지 않으면 Cisco ISE 애플리케이션 컨피그레이션 데이터만 복원됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

EXEC

사용 지침

Cisco ISE에서 restore 명령을 사용하는 경우 Cisco ISE 서버가 자동으로 다시 시작됩니다.

데이터를 복원할 때 암호화 키는 선택 사항입니다. 암호화 키를 제공하지 않은 이전 백업을 지원하려는 경우 암호화 키 없이 **restore** 명령을 사용하면 됩니다.

예

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key plain
 Lab12345
```

```
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

관련 명령

	Description(설명)
backup	백업을 수행하고(Cisco ISE 및 Cisco ADE OS) 저장소에 백업을 저장합니다.
backup-logs	시스템 로그를 백업합니다.
repository	백업 컨피그레이션을 위한 저장소 하위 모드로 진입합니다.
show repository	특정 저장소에 있는 사용 가능한 백업 파일을 표시합니다.
show backup history	시스템 백업 기록을 표시합니다.
show backup status	백업 작업의 상태를 표시합니다.
show restore status	복원 작업의 상태를 표시합니다.

보조 노드에 대한 애플리케이션 복원 후의 동기화 상태 및 복제 상태가 동기화되지 않음인 경우 해당 보조 노드의 인증서를 PAN으로 다시 가져온 다음 수동 동기화를 수행해야 합니다.

GUI에서 컨피그레이션 백업 복원

관리 포털에서 컨피그레이션 백업을 복원할 수 있습니다. GUI에는 현재 릴리스에서 생성한 백업만 나열됩니다. 이 릴리스 이전의 백업을 복원하려면 CLI에서 restore 명령을 사용해 주십시오.

시작하기 전에

기본 PAN 자동 페일오버 컨피그레이션이 구축에서 활성화되어 있는 경우 꺼져 있는지 확인합니다. 컨피그레이션 백업을 복원할 때는 애플리케이션 서버 프로세스가 다시 시작됩니다. 이러한 서비스

가 다시 시작되는 동안 작업이 지연될 수 있습니다. 서비스가 다시 시작될 때의 이러한 지연으로 인해 보조 관리 노드의 자동 페일오버가 시작될 수 있습니다.

구축 시 시간 컨피그레이션 백업의 듀얼 노드 구축인 경우 다음을 확인합니다.

- 복원의 소스 및 대상 노드는 컨피그레이션 백업에 사용된 것과 동일합니다. 대상 노드는 독립형 또는 기본 노드일 수 있습니다.
- 복원의 소스 및 대상 노드는 컨피그레이션 백업에 사용된 것과 다릅니다. 대상 노드는 독립형이어야 합니다.

참고 컨피그레이션 데이터베이스 백업을 복원하고 기본 PAN에서만 루트 CA를 다시 생성할 수 있습니다. 그러나 등록된 PAN에서는 컨피그레이션 데이터베이스 백업을 복원할 수 없습니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **3** 컨피그레이션 백업 목록에서 백업 이름을 선택하고 **Restore(**복원**)**를 클릭합니다.

단계 **4** 백업 중에 사용한 암호화 키를 입력합니다.

단계 **5** **Restore(**복원**)**를 클릭합니다.

다음에 수행할 작업

Cisco ISE CA 서비스를 사용하는 경우 다음을 수행해야 합니다.

1. 전체 Cisco ISE CA 루트 체인을 재생성합니다.
2. PAN에서 Cisco ISE CA 인증서와 키의 백업을 가져온 다음 보조 관리 노드에서 복원합니다. 그러면 기본 PAN 장애 시 보조 PAN이 루트 CA 또는 외부 PKI의 하위 CA로 작동할 수 있으며, 이 경우 보조 PAN을 기본 PAN으로 승격합니다.

모니터링 데이터베이스 복원

모니터링 데이터베이스를 복원하는 프로세스는 구축 유형에 따라 다릅니다. 다음 섹션에서는 독립형 및 분산형 구축에서 모니터링 데이터베이스를 복원하는 방법을 설명합니다.

CLI를 사용하여 이전 Cisco ISE 릴리스에서 온디맨드 모니터링 데이터베이스 백업을 복원해야 합니다. Cisco ISE 릴리스에서 예약 백업을 복원하는 기능은 지원되지 않습니다.

참고 데이터를 가져온 노드와 다른 노드로 데이터를 복원하려는 경우 새 노드를 가리키도록 로깅 대상 설정을 구성해야 합니다. 이렇게 하면 모니터링 시스템 로그가 적절한 노드로 전송됩니다.

독립형 환경에서 모니터링(운영) 백업 복원

GUI에는 현재 릴리스에서 생성한 백업만 나열됩니다. 이전 릴리스에서 가져온 백업을 복원하려면 CLI에서 restore 명령을 사용해 주십시오.

시작하기 전에

- 이전 모니터링 데이터를 비웁니다.
- 백업을 예약하거나 온디맨드 백업을 수행합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **3** 운영 백업 목록에서 백업 이름을 선택하고 **Restore(**복원**)**를 클릭합니다.

단계 **4** 백업 중에 사용한 암호화 키를 입력합니다.

단계 **5** **Restore(**복원**)**를 클릭합니다.

관리 및 모니터링 페르소나를 사용하여 모니터링 백업 복원

관리 및 모니터링 페르소나를 사용하여 분산형 환경의 모니터링 백업을 복구할 수 있습니다.

시작하기 전에

- 이전 모니터링 데이터를 비웁니다.
- 백업을 예약하거나 온디맨드 백업을 수행합니다.

단계 **1** 기본 및 보조 PAN을 사용하는 경우 PAN을 동기화합니다.

PAN을 동기화할 때 PAN을 선택하고, 이를 활성 기본 상태로 승격해야 합니다.

단계 **2** 모니터링 노드의 등록을 취소하기 전에 모니터링 페르소나를 구축의 다른 노드에 할당합니다.

모든 구축에는 작동하는 모니터링 노드가 하나 이상 있어야 합니다.

단계 **3** 백업할 모니터링 노드를 등록 취소합니다.

단계 **4** 새로 등록 취소한 노드로 모니터링 백업을 복원합니다.

단계 **5** 새로 복원한 노드를 현재 관리 노드에 등록합니다.

단계 **6** 새로 복구하고 등록한 노드를 활성 모니터링 노드로 승격합니다.

모니터링 페르소나를 사용하여 모니터링 백업 복원

모니터링 페르소나만 사용하여 분산형 환경의 모니터링 백업을 복원할 수 있습니다.

시작하기 전에

- 이전 모니터링 데이터를 비웁니다.
- 백업을 예약하거나 온디맨드 백업을 수행합니다.

단계 **1** 복구할 노드의 등록 취소를 준비합니다. 이 작업은 구축의 다른 노드에 모니터링 페르소나를 할당하여 수행됩니다.

구축에는 작동하는 모니터링 노드가 하나 이상 있어야 합니다.

단계 **2** 복원할 노드를 등록 취소합니다.

참고 등록 취소가 완료될 때까지 기다렸다가 복원을 진행합니다. 노드가 독립형 상태여야 복원을 계속할 수 있습니다.

단계 **3** 새로 등록 취소한 노드로 모니터링 백업을 복원합니다.

단계 **4** 새로 복원한 노드를 현재 관리 노드에 등록합니다.

단계 **5** 새로 복원하고 등록한 노드를 PAN으로 승격합니다.

복원 기록

운영 감사 보고서 창에서 모든 복원 작업, 로그 이벤트 및 상태에 대한 정보를 가져올 수 있습니다.

참고 그러나 운영 감사 보고서 창에서는 이전 복원 작업에 해당하는 시작 시간에 대한 정보를 제공하지 않습니다.

문제 해결 정보를 확인하려면 Cisco ISE CLI에서 **backup-logs** 명령을 실행하고 ADE.log 파일을 확인해야 합니다.

복원 작업이 진행 중인 동안에는 모든 Cisco ISE 서비스가 중지됩니다. **show restore status** CLI 명령을 사용하여 복구 작업의 진행률을 확인할 수 있습니다.

인증 및 권한 부여 정책 컨피그레이션 내보내기

컨피그레이션 오류를 식별하고 문제 해결용으로 사용하기 위해 오프라인에서 읽을 수 있는 XML 파일 형식으로 인증 및 권한 부여 정책 컨피그레이션을 내보낼 수 있습니다. 이 XML 파일은 인증 및 권한 부여 정책 규칙, 단순/복합 정책 조건, DACL(Discretionary Access Control Lists) 및 권한 부여 정책을 포함합니다. XML 파일을 이메일로 보내거나 로컬 시스템에 저장하도록 선택할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup & Restore(**백업 및 복구**)**를 선택합니다.

단계 **2** **Policy Export(**정책 내보내기**)**를 클릭합니다.

단계 **3** 필요한 대로 값을 입력합니다.

단계 **4** **Export(**내보내기**)**를 클릭합니다.

WordPad 등의 텍스트 편집기를 사용하여 XML 파일의 내용을 확인합니다.

정책 내보내기 예약 설정

다음 표에서는 **Schedule Policy Export(**정책 내보내기 예약**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)** > **Policy Export(**정책 내보내기**)**입니다.

표 ***39:*** 정책 내보내기 예약 설정

필드 이름	사용 지침
암호화	
Encryption Key(암호화 키**)**	내보내기 데이터를 암호화하고 암호를 해독하는 데 사용할 키를 입력합니다. 이 필드는 **Export with Encryption Key(**암호화 키를 사용해 내보내기**)** 옵션을 선택한 경우에만 활성화됩니다.
Destination(대상**)**	
Download file to local computer(파일을 로컬 컴퓨터에 다운로드**)**	정책 내보내기 파일을 로컬 시스템에 다운로드할 수 있습니다.
다음 사용자에게 이메일로 파일 보내기	이메일 주소가 여러 개인 경우 쉼표로 구분하십시오.
Repository(저장소**)**	정책 데이터를 내보낼 저장소를 선택합니다. 여기에 저장소 이름을 입력할 수는 없습니다. 드롭다운 목록에서 사용 가능한 저장소를 선택하는 것만 가능합니다. 정책 내보내기를 예약하기 전에 저장소를 생성해야 합니다.
Export Now(지금 내보내기**)**	데이터를 로컬 컴퓨터로 내보내거나 이메일 첨부 파일로 보내려면 이 옵션을 클릭합니다. 저장소로는 내보낼 수 없습니다. 저장소 내보내기만 예약이 가능합니다.

필드 이름	사용 지침
Schedule(일정**)**	
Schedule Options(예약 옵션**)**	내보내기 일정의 빈도를 선택하고 그에 따라 나머지 세부정보를 입력합니다.

분산형 환경에서 기본 및 보조 노드 동기화

분산형 환경에서는 PAN에서 백업 파일을 복원한 후 기본 노드와 보조 노드의 Cisco ISE 데이터베이스가 자동으로 동기화되지 않는 경우가 있습니다. 이러한 현상이 발생하는 경우 PAN에서 보조 ISE 노드로의 전체 복제를 수동으로 강제 수행할 수 있습니다. PAN에서 보조 노드로만 동기화를 강제 수행할 수 있습니다. syncup 작업 중에는 컨피그레이션을 변경할 수 없습니다. Cisco ISE에서는 동기화가 완료된 후에만 다른 Cisco ISE 관리 포털 페이지로 이동하여 컨피그레이션을 변경하도록 허용합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**

단계 **3** 복제 상태가 동기화되지 않음인 보조 ISE 노드 옆의 확인란을 선택합니다.

단계 **4** **Syncup**을 클릭하고 노드가 PAN과 동기화될 때까지 기다립니다. 이 프로세스가 완료될 때까지 기다려야 Cisco ISE 관리 포털에 다시 액세스할 수 있습니다.

분산형 구축에서 손실된 노드 복구

이 섹션에서는 분산형 구축에서 손실된 노드를 복구하는 데 사용할 수 있는 문제 해결 정보를 제공합니다. 다음 활용 사례 중 일부에서는 백업 및 복구 기능을, 다른 일부에서는 복제 기능을 사용하여 손실된 데이터를 복구합니다.

분산형구축에서 기존 **IP** 주소 및 호스트 이름을 사용한 손실 노드 복구

시나리오

분산형 구축에서 자연 재해로 인해 모든 노드가 손실되었습니다. 복구 후에 기존 IP 주소와 호스트 이름을 사용하려고 합니다.

예를 들어 N1(기본 정책 관리 노드 또는 기본 PAN) 및 N2(보조 정책 관리 노드 또는 보조 PAN)의 두 개 노드가 있다고 가정해 보겠습니다. 시간 T1에 만든 N1 노드의 백업을 사용할 수 있습니다. 그런데 나중에 자연 재해로 인해 N1 및 N2 노드 둘 다에서 장애가 발생합니다.

가정

구축의 모든 Cisco ISE 노드가 제거되었습니다. 같은 호스트 이름과 IP 주소를 사용하여 새 하드웨어가 이미지화되었습니다.

해결 단계

1. N1 및 N2 노드를 모두 대체해야 합니다. 이제 N1 및 N2 노드에 독립형 컨피그레이션이 사용됩니다.
2. N1 및 N2 노드의 UDI를 사용하여 라이선스를 가져온 다음 N1 노드에 설치합니다.
3. 그런 다음 교체된 N1 노드에서 백업을 복원해야 합니다. 복원 스크립트는 N2에서 데이터 동기화를 시도하지만 이제 N2는 독립형 노드이므로 동기화가 실패합니다. N1의 데이터는 T1 시간으로 재설정됩니다.
4. N1 관리 포털에 로그인하여 N2 노드를 삭제한 다음 다시 등록해야 합니다. N1 및 N2 노드 둘 다의 데이터가 T1 시간의 데이터로 재설정됩니다.

분산형구축에서 새 IP 주소 및 호스트 이름을 사용하여 손실된 노드 복구

시나리오

분산형 구축에서 자연 재해로 인해 모든 노드가 손실되었습니다. 새 위치에서 새 하드웨어를 재이미지화했으며 새 IP 주소와 호스트 이름이 필요합니다.

예를 들어 N1(기본 관리 노드/PAN) 및 N2(보조 정책 서비스 노드)의 두 개 ISE 노드가 있다고 가정해 보겠습니다. 시간 T1에 만든 N1 노드의 백업을 사용할 수 있습니다. 그런데 나중에 자연 재해로 인해 N1 및 N2 노드 둘 다에서 장애가 발생합니다. Cisco ISE 노드가 새 위치에서 대체되며, 새 호스트 이름은 N1A(PAN) 및 N2A(보조 정책 서비스 노드)입니다. 이 시점에서 N1A 및 N2A는 독립형 노드입니다.

가정

구축의 모든 Cisco ISE 노드가 제거되었습니다. 다른 위치에서 다른 호스트 이름과 IP 주소를 사용하여 새 하드웨어가 이미지화되었습니다.

해결 단계

1. N1 백업을 가져온 다음 N1A에서 복원합니다. 복원 스크립트는 호스트 이름 변경 및 도메인 이름 변경을 식별하여 현재 호스트 이름을 기반으로 구축 컨피그레이션에서 호스트 이름과 도메인 이름을 업데이트합니다.
2. 새 셀프 서명 인증서를 생성해야 합니다.

3. N1A에서 Cisco ISE 관리자 포털에 로그인해야합니다.Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** 에서 다음을 수행합니다.

   이전 N2 노드를 삭제합니다.

   새 N2A 노드를 보조 노드로 등록합니다. N1A 노드의 데이터가 N2A 노드로 복제됩니다.

독립형 구축에서 기존 IP 주소 및 호스트 이름을 사용하여 노드 복구

시나리오

독립형 관리 노드가 다운되었습니다.

예를 들어 독립형 관리 노드가 N1이라고 가정해 보겠습니다. 시간 T1에 N1 데이터베이스의 백업을 만들었습니다. N1 노드는 물리적 장애로 인해 다운되었으며 재이미지화해야 하거나 새 하드웨어를 사용해야 합니다. 같은 IP 주소와 호스트 이름을 사용하여 N1 노드를 다시 작동시켜야 합니다.

가정

이 구축은 독립형이며 새로 사용하거나 재이미지화되는 하드웨어의 IP 주소와 호스트 이름은 같습니다.

해결 단계

재이미지화 후에 N1 노드가 작동하거나 같은 IP 주소 및 호스트 이름을 사용하여 새 Cisco ISE 노드를 도입한 후에는 이전 N1 노드에서 만든 백업을 복구해야 합니다. 역할은 변경하지 않아도 됩니다.

독립형 구축에서 새 IP 주소 및 호스트 이름을 사용하여 노드 복구

시나리오

독립형 관리 노드가 다운되었습니다.

예를 들어 독립형 관리 노드가 N1이라고 가정해 보겠습니다. 시간 T1에 만든 N1 데이터베이스의 백업을 사용할 수 있습니다. N1 노드는 물리적 장애로 인해 다운되었으며, 다른 IP 주소와 호스트 이름을 사용하여 다른 위치에서 새 하드웨어로 해당 노드를 교체하려고 합니다.

가정

구축은 독립형이며 교체되는 하드웨어는 IP 주소와 호스트 이름이 다릅니다.

해결 단계

1. N1 노드를 새 하드웨어로 교체합니다. 이 노드는 독립형 상태가 되며 호스트 이름은 N1B입니다.
2. N1B 노드에서 백업을 복원할 수 있습니다. 역할은 변경하지 않아도 됩니다.

컨피그레이션 롤백

문제

실수로 컨피그레이션을 잘못 변경하는 경우가 있을 수 있습니다. 예를 들어 여러 NAD를 삭제하거나 일부 ADIUS 속성을 잘못 수정했지만, 몇 시간 후에야 이 문제를 깨달을 수 있습니다. 이 경우 변경하기 전에 작성한 백업을 복구하여 원래 컨피그레이션으로 되돌릴 수 있습니다.

가능한 원인

N1(기본 정책 관리 노드 또는 기본 PAN)과 N2(보조 정책 관리 노드 또는 보조 PAN)로 구성된 노드 2개와 N1 노드 백업이 지원됩니다. 일부 컨피그레이션을 잘못 변경하여 N1에서 변경 사항을 제거하고자 합니다.

해결책

잘못된 컨피그레이션 변경이 적용되기 전에 작성된 N1 노드 백업을 가져옵니다. N1 노드에서 이 백업을 복원합니다. 복원 스크립트는 N1의 데이터를 N2와 동기화합니다.

분산형 구축에서 장애 발생 시 기본 노드 복구

시나리오

다중 노드 구축에서 PAN에 장애가 발생했습니다.

예를 들어 N1(PAN) 및 N2(보조 관리 노드)라는 Cisco ISE 노드가 2개 있는데 하드웨어 문제로 인해 N1에 장애가 발생한다고 가정해 보겠습니다.

가정

분산형 구축의 기본 노드에만 장애가 발생했습니다.

해결 단계

1. N2 관리자 포털에 로그인합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** 를 선택하고 기본 노드로 N2를 구성합니다.

   N1 노드가 새 하드웨어로 교체되고 재이미지화되며 독립형 상태가 됩니다.

2. N2 관리자 포털에서 새 N1 노드를 보조 노드로 등록합니다.

   이제 N2 노드가 기본 노드가 되고 N1 노드가 보조 노드가 됩니다.

N1 노드를 다시 기본 노드로 지정하려면 N1 관리자 포털에 로그인하여 N1 노드를 기본 노드로 지정합니다. 그러면 N2는 자동으로 보조 서버가 됩니다. 데이터는 손실되지 않습니다.

분산형 구축에서 장애 발생 시 보조 노드 복구

시나리오

다중 노드 구축에서 단일 보조 노드에 장애가 발생했습니다. 복원은 수행하지 않아도 됩니다.

예를 들어 N1(기본 PAN), N2(보조 PAN), N3(보조 정책 서비스 노드), N4(보조 정책 서비스 노드)라는 여러 노드가 있는데 보조 노드 중 하나인 N3에서 장애가 발생한다고 가정해 보겠습니다.

해결 단계

1. 새 N3A 노드를 기본 독립형 상태로 재이미지화합니다.
2. N1 관리 포털에 로그인하여 N3 노드를 삭제합니다.
3. N3A 노드를 다시 등록합니다.

   데이터는 N1에서 N3A로 복제됩니다. 복원은 수행하지 않아도 됩니다.

Cisco ISE 로깅 메커니즘

Cisco ISE는 감사, 결함 관리 및 문제 해결에 사용되는 로깅 메커니즘을 제공합니다. 로깅 메커니즘은 구축된 서비스에서 결함 조건을 식별하고 문제를 효율적으로 해결하는 데 도움이 됩니다. 또한 모니터링 및 문제 해결 기본 노드에서 일관된 방식으로 로깅 출력을 생성하기도 합니다.

가상 루프백 주소를 사용하여 로컬 시스템의 로그를 수집하도록 Cisco ISE 노드를 구성할 수 있습니다. 외부에서 로그를 수집하려면 호출 대상인 외부 시스템 로그 서버를 구성해 주십시오. 로그는 미리 정의된 여러 범주로 분류됩니다. 대상, 심각도 레벨 등과 관련된 범주를 편집하여 로깅 출력을 사용자 맞춤화할 수 있습니다.

Cisco ISE 모니터링 및 문제 해결(MnT) 노드에 syslog를 전송하도록 네트워크 디바이스를 구성하지 않는 것이 모범 사례입니다. 이 경우 Cisco NISE(Network Access Device) syslog가 손실되고 MnT 서버가 오버로드되어 로드 문제가 발생할 수 있기 때문입니다. NAD Syslog가 MnT로 직접 전송되도록 구성된 경우 세션 관리 기능이 중단됩니다. 문제 해결을 위해 NAD 시스템 로그를 외부 시스템 로그 서버로 전송할 수 있지만 MnT로 보내서는 안 됩니다.

노드에서 ISE 메시징 서비스에 장애가 발생할 때 프로세스 중단 경보가 더 이상 트리거되지 않습니다. 노드에서 ISE 메시징 서비스에 장애가 발생하면 해당 노드에서 메시징 서비스가 다시 작동할 때까지 모든 시스템 로그 및 프로세스 중단 경보가 손실됩니다.

이 경우 관리자는 Cisco ISE **Home(**홈**)** 창의 **Alarms(**경보**)** dashlet에 나열되는 **Queue Link Error(**대기열 링크 오류**)** 경보를 찾아야 합니다. 경보를 클릭하면 **Suggested Actions(**추천 작업**)** 섹션이 포함된 새 창이 열립니다. 다음 지침에 따라 문제를 해결합니다.

참고 모니터링 노드가 네트워크 디바이스에 대한 시스템 로그 서버로 구성된 경우 로깅 소스가 올바른 NAS(Network Access Server) IP 주소를 다음 형식으로 전송하는지 확인합니다.

<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>

그렇지 않으면 NAS IP 주소에 의존하는 기능에 영향을 미칠 수 있습니다.

시스템 로그 제거 설정 구성

다음 프로세스를 사용하여 로컬 로그 저장 기간을 설정하고 특정 기간이 지난 후 로컬 로그를 삭제합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Local Log Settings(**로컬 로그 설정**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Local Log Settings(**로컬 로그 설정**)**.

단계 **3** **Local Log Storage Period(**로컬 로그 저장 기간**)** 필드에 로그 엔트리를 컨피그레이션 소스에 보관할 최대 기간을 일 단위로 입력합니다.

localStore 폴더의 크기가 97GB에 도달하면 구성된 **Local Log Storage Period(**로컬 로그 저장 기간**)**가 끝나기 전에 일찍 로그가 삭제될 수 있습니다.

단계 **4** 저장 기간이 만료되기 전에 언제든지 기존 로그 파일을 삭제하려면 **Delete Logs Now(**지금 로그 삭제**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Cisco ISE 시스템 로그

Cisco ISE에서 시스템 로그는 호출되는 로깅 대상이라고 하는 위치에서 수집됩니다. 대상이란 로그를 수집하고 저장하는 서버의 IP 주소를 나타냅니다. 로그는 로컬에서 생성하여 저장할 수도 있고, FTP 기능을 사용하여 외부 서버로 전송할 수도 있습니다. Cisco ISE에는 로컬 시스템의 루프백 주소에서 동적으로 구성되는 다음과 같은 기본 대상이 있습니다.

- LogCollector - 로그 컬렉터의 기본 시스템 로그 대상
- ProfilerRadiusProbe - 프로파일러 RADIUS 프로브의 기본 시스템 로그 대상

기본적으로 AAA Diagnostics(AAA 진단) 하위 범주 및 System Diagnostics(시스템 진단) 하위 범주 로깅 대상은 디스크 공간을 줄일 수 있도록 새로운 Cisco ISE 설치 또는 업그레이드 중에 비활성화됩니다. 이러한 하위 범주에 대해 수동으로 로깅 대상을 구성할 수 있지만 이러한 하위 범주의 로컬 로깅은 항상 활성화되어 있습니다.

Cisco ISE 설치 측에서 로컬로 구성한 기본 로깅 대상을 사용할 수 있습니다. 또는 외부 대상을 생성하여 로그를 저장할 수도 있습니다.

참고 시스템 로그 서버가 분산형 구축으로 구성된 경우 시스템 로그 메시지는 MnT 노드가 아닌 인증 PSN에서 직접 시스템 로그 서버로 전송됩니다.

관련 항목

Cisco ISE 메시지 코드, 285 페이지

원격 시스템 로그 컬렉션 위치 구성

웹 인터페이스를 사용하여 시스템 로그 메시지가 전송되는 원격 시스템 로그 서버 대상을 생성할 수 있습니다. 로그 메시지는 시스템 로그 프로토콜 표준에 따라 원격 시스템 로그 서버 타깃으로 전송됩니다(RFC-3164 참고). 시스템 로그 프로토콜은 비보안 UDP입니다.

이벤트가 발생하면 메시지가 생성됩니다. 이벤트는 프로그램 종료 시 표시되는 메시지와 같이 상태를 표시하는 항목 또는 경보일 수 있습니다. 커널, 메일, 사용자 레벨 등의 여러 기능에서 다양한 유형의 이벤트 메시지가 생성됩니다. 이벤트 메시지는 심각도 레벨과 연결되므로 관리자는 메시지를 필터링하고 우선순위를 설정할 수 있습니다. 기능과 심각도 레벨에는 숫자 코드가 할당됩니다. 시스템 로그 서버는 이벤트 메시지 컬렉터이며 이러한 기능에서 이벤트 메시지를 수집합니다. 관리자는 심각도 레벨에 따라 메시지를 전달할 이벤트 메시지 컬렉터를 선택할 수 있습니다.

기본 원격 로깅 대상은 UDP 시스템 로그(로그 컬렉터)입니다. 이 로깅 대상은 비활성화하는 경우 더 이상 로그 컬렉터로 작동하지 않으며 **Logging Categories(**로깅 범주**)** 창에서 제거되고, 활성화하는 경우 **Logging Categories(**로깅 범주**)** 창에서 로그 컬렉터로 지정됩니다.

참고 기본 원격 로깅 대상 **SecureSyslogCollector**를 변경하면 Cisco ISE 모니터링 및 문제 해결 로그 프로세서 서비스가 재시작됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Remote Logging Targets(**원격 로깅 대상**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 필요한 세부정보를 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 원격 로깅 대상 페이지로 이동하여 새 대상이 생성되었는지 확인합니다.

그런 다음 로깅 대상을 아래의 각 로깅 범주에 매핑할 수 있습니다. PSN 노드는 해당 노드에서 활성화된 서비스에 따라 관련 로그를 원격 로깅 대상으로 전송합니다.

- AAA 감사
- AAA 진단

- 어카운팅
- 외부 MDM
- 패시브 ID
- Posture and Client Provisioning Audit(포스처 및 클라이언트 프로비저닝 감사)
- 포스처 및 클라이언트 프로비저닝 진단
- 프로파일러

다음 범주의 로그는 구축 환경의 모든 노드에서 로깅 대상으로 전송됩니다.

- Administrative and Operational Audit(관리 및 운영 감사)
- 시스템 진단
- 시스템 통계

Cisco ISE 메시지 코드

로깅 범주는 기능, 흐름 또는 활용 사례를 설명하는 메시지 코드 번들입니다. Cisco ISE에서 각 로그는 로그 메시지 콘텐츠에 따라 로깅 범주와 함께 제공되는 메시지 코드와 연결되어 있습니다. 로깅 범주는 그 안에 포함된 메시지 콘텐츠를 설명하는 데 도움이 됩니다.

로깅 범주에서 로깅 컨피그레이션을 승격할 수 있습니다. 각 범주에는 애플리케이션 요건에 따라 설정할 수 있는 이름, 대상 및 심각도 레벨이 있습니다.

Cisco ISE는 포스처, 프로파일러, 게스트, AAA(Authentication, Authorization, and Accounting) 등과 같이 서비스에 대해 미리 정의된 로깅 범주를 제공하므로 여기에 로그 대상을 할당할 수 있습니다.

로깅 범주 **Passed Authentications(**통과된 인증**)**의 경우 로컬 로깅을 허용하는 옵션은 기본적으로 비활성화되어 있습니다. 이 범주에 대한 로컬 로깅을 활성화하면 운영 공간의 사용률이 높아지며 prrt-server.log와 iseLocalStore.log가 입력집니다.

Passed Authentications(통과된 인증**)**에 대해 로컬 로깅을 활성화하려면 범주 섹션에서 **Administration(**관리**) > System(**시스템**) > Logging(**로깅**) > Logging Categories(**로깅 범주**)**로 이동하여 **Passed Authentications(**통과된 인증**)**을 클릭한 다음 **Local Logging(**로컬 로깅**)**에 대한 확인란을 선택합니다.

관련 항목

메시지 코드에 대한 심각도 레벨 설정, 285 페이지

메시지 코드에 대한 심각도 레벨 설정

로그 심각도 레벨을 설정하고 선택한 범주의 로그를 저장할 로깅 대상을 선택할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**.

단계 **2** 편집할 범주 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** 필수 필드 값을 수정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 로깅 범주 페이지로 이동하여 특정 범주에 대해 수행된 컨피그레이션 변경사항을 확인합니다.

Cisco ISE 메시지 카탈로그

메시지 카탈로그 페이지를 사용하여 모든 가능한 로그 메시지와 설명을 볼 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Message Catalog(**메시지 카탈로그**)**를 선택합니다.

Log Message Catalog(로그 메시지 카탈로그) 페이지가 나타나면 로그 파일에 표시될 수 있는 잠재적인 로그 메시지를 모두 볼 수 있습니다. **Export(**내보내기**)**를 선택하여 모든 시스템 로그 메시지를 CSV 파일 형식으로 내보냅니다.

Cisco ISE에서 전송한 시스템 로그 메시지의 전체 목록, 의미 및 로컬 및 원격 대상에서 메시지가 기록되는 방식은 Cisco ISE 시스템 로그를 참조하십시오.

엔드포인트 디버그 로그 컬렉터

특정 엔드포인트 관련 문제를 해결하려면 IP 주소 또는 MAC 주소를 기준으로 특정 엔드포인트의 디버그 로그를 다운로드할 수 있습니다. 특정 엔드포인트 관련 구축 환경에 있는 다양한 노드의 로그는 단일 파일로 수집되므로 문제를 신속하고 효율적으로 해결하는 데 도움이 됩니다. 이 문제 해결 도구는 한 번에 하나의 엔드포인트에 대해서만 실행할 수 있습니다. 로그 파일은 GUI에 나열됩니다. 엔드포인트 로그는 단일 노드에서 다운로드할 수도 있고, 구축 환경의 모든 노드에서 다운로드할 수도 있습니다.

특정 엔드포인트에 대한 디버그 로그 다운로드

네트워크에서 특정 엔드포인트 관련 문제를 해결하려는 경우 관리 포털에서 엔드포인트 디버그 도구를 사용할 수 있습니다. 인증 페이지에서 이 도구를 실행할 수도 있습니다. 이렇게 하려면 인증 페이지에서 엔드포인트 ID를 마우스 오른쪽 버튼으로 클릭하고 **Endpoint Debug(**엔드포인트 디버그**)**를 클릭합니다. 이 도구는 특정 엔드포인트와 관련된 모든 서비스에 대한 모든 디버그 정보를 단일 파일에서 제공합니다.

시작하기 전에

디버그 로그를 수집하려는 엔드포인트의 IP 주소 또는 MAC 주소가 필요합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Endpoint Debug(**엔드포인트 디버그**)**.

단계 **2** **MAC Address(MAC** 주소**)** 또는 **IP** 라디오 버튼을 클릭하고 엔드포인트의 MAC 또는 IP 주소를 입력합니다.

단계 **3** 지정된 시간 후에 로그 수집을 중지하려면 **Automatic disable after *n* Minutes(n**분 후 자동 비활성화**)** 확인란을 선택합니다. 이 확인란을 선택하는 경우 1~60분 사이의 시간을 입력해야 합니다.

"엔드포인트 디버그를 사용하는 경우 구축 성능이 저하됩니다. 계속하시겠습니까?"라는 메시지가 표시됩니다.

단계 **4** 로그를 수집하려면 **Continue(**계속**)**를 클릭합니다.

단계 **5** 로그 수집을 수동으로 중지하려면 **Stop(**중지**)**을 클릭합니다.

관련 항목

엔드포인트 디버그 로그 컬렉터, 286 페이지

수집 필터

모니터링 및 외부 서버로 전송되는 시스템 로그 메시지를 표시하지 않도록 수집 필터를 구성할 수 있습니다. 표시 안 함은 다양한 속성 유형에 따라 정책 서비스 노드 수준에서 수행될 수 있습니다. 특정 속성 유형 및 해당 값을 사용하여 여러 필터를 정의할 수 있습니다.

Cisco ISE는 시스템 로그 메시지를 모니터링 노드 또는 외부 서버로 보내기 전에 먼저 이러한 값을 전송 대상 시스템 로그 메시지의 필드와 비교합니다. 일치하는 항목이 있는 경우 해당 메시지가 전송되지 않습니다.

수집 필터 구성

다양한 속성 유형을 기준으로 여러 수집 필터를 구성할 수 있습니다. 필터 수는 20개로 제한하는 것이 좋습니다. 수집 필터를 추가, 편집 또는 삭제할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Collection Filters(**수집 필터**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 다음 목록에서 **Filter Type(**필터 유형**)**을 선택합니다.

- 사용자 이름
- MAC 주소
- 정책 집합 이름
- NAS IP 주소
- 디바이스 IP 주소

단계 **4** 선택한 필터 유형에 해당하는 **Value(**값**)**를 입력합니다.

단계 **5** 드롭다운 목록에서 **Result(**결과**)**를 선택합니다. 결과는 모두, 통과 또는 실패일 수 있습니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

관련 항목

수집 필터, 287 페이지
이벤트 억제 무시 필터, 288 페이지

이벤트 억제 무시 필터

Cisco ISE에서는 수집 필터를 사용하여 시스템 로그 메시지가 모니터링 노드 및 다른 외부 서버로 전송되지 않도록 억제하는 필터를 설정할 수 있습니다. 때로는 이와 같이 숨겨진 로그 메시지에 액세스해야 하는 경우가 있습니다. Cisco ISE는 이제 구성 가능한 기간 동안 사용자 이름과 같은 특정 속성에 따라 이벤트 억제를 무시할 수 있는 옵션을 제공합니다. 기본값은 50분이지만 5분부터 480분(8시간)까지 기간을 구성할 수 있습니다. 이벤트 억제 무시를 구성하고 나면 효과가 즉시 적용됩니다. 설정한 기간이 경과되면 억제 무시 필터가 만료됩니다.

Cisco ISE 사용자 인터페이스의 수집 필터 페이지에서 억제 무시 필터를 구성할 수 있습니다. 이제 이 기능을 사용하여 특정 ID(사용자)의 모든 로그를 볼 수 있으며 해당 ID에 대한 문제를 실시간으로 해결할 수 있습니다.

필터는 활성화하거나 비활성화할 수 있습니다. 이벤트 무시 필터에 구성한 기간이 경과되면 관리자가 다시 활성화할 때까지 필터가 자동으로 비활성화됩니다.

Cisco ISE는 컨피그레이션 변경 감사 보고서에서 이러한 컨피그레이션 변경 사항을 캡처합니다. 이 보고서에서는 이벤트 억제 또는 억제 무시를 구성한 사용자 및 이벤트가 억제되었거나 억제가 무시된 기간에 대한 정보를 제공합니다.

Cisco ISE 보고서

Cisco ISE(Identity Services Engine) 보고서는 모니터링 및 문제 해결 기능과 함께 중앙 위치에서 트렌드를 분석하고 시스템 성능과 네트워크 활동을 모니터링하는 데 사용됩니다.

Cisco ISE는 네트워크에서 로그 및 컨피그레이션 데이터를 수집합니다. 그런 다음 보고 분석할 수 있도록 데이터를 보고서로 집계합니다. Cisco ISE는 미리 정의된 표준 보고서 집합을 제공하므로 사용자 요구 사항에 맞게 사용하고 사용자 맞춤화할 수 있습니다.

Cisco ISE 보고서는 미리 구성되어 있으며 인증, 세션 트래픽, 디바이스 관리 , 컨피그레이션 및 관리, 문제 해결과 관련된 정보를 사용하여 논리 범주로 그룹화됩니다.

관련 항목

보고서 실행 및 보기, 290 페이지
보고서 내보내기, 291 페이지
사용 가능한 보고서, 295 페이지

보고서 필터

단일 섹션 및 다중 섹션이라는 2가지 보고서 유형이 있습니다. 단일 섹션 보고서는 단일 그리드(Radius 인증 보고서)를 포함하고, 다중 섹션 보고서는 다수의 그리드(인증 요약 보고서)로 구성되며 차트 및 표 형식으로 데이터를 표시합니다. 단일 섹션 보고서의 Filter(필터) 드롭다운 메뉴는 **Quick Filter(**빠른 필터**)**와 **Advanced Filter(**고급 필터**)**로 구성되어 있습니다. 다중 섹션 보고서에서는 고급 필터만 지정할 수 있습니다.

다중 섹션 보고서에는 입력이 필요한 하나 이상의 필수 고급 필터가 포함될 수 있습니다. 예를 들어 상태 요약 보고서 클릭하면(**Operations(**운영**) > Reports(**보고서**) > Diagnostics(**진단**)** 페이지), Server(서버) 및 Time Range(시간 범위)라는 2가지 필수 고급 필터가 나타납니다. 연산자 명령, 서버 이름, 이 두 필터에 대한 필수 값을 지정하고 **Go(**이동**)**를 클릭하여 보고서를 생성해야 합니다. 더하기(+) 특수문자를 클릭하여 새 고급 필터를 추가할 수 있습니다. 다중 섹션 보고서는 PDF 형식으로만 내보낼 수 있습니다. Cisco ISE 다중 섹션 보고서가 특정 시간에 또는 일정 시간 간격으로 실행 및 재실행되도록 예약할 수는 없습니다.

참고 보고서를 클릭하면 현재 날짜의 데이터가 기본적으로 생성됩니다. 그러나 일부 다중 섹션 보고서에서는 시간 범위를 제외하고 사용자가 필수적으로 입력해야 하는 항목이 있습니다.

기본적으로 Quick Filter(빠른 필터)는 단일 섹션 보고서의 첫 번째 행으로 표시됩니다. 이 필드에는 검색 조건을 선택할 수 있는 드롭다운 목록이 포함되어 있거나 텍스트 상자일 수 있습니다.

Advanced Filter(고급 필터)에는 하나 이상의 내부 기준이 속한 외부 기준이 포함되어 있습니다. 외부 기준은 검색이 All(모두) 또는 Any(일부)로 지정된 내부 기준을 충족해야 하는지를 지정하는 데 사용됩니다. 내부 기준에는 조건에 대한 범주(엔드포인트 ID, ID 그룹), 방법(Contains(포함), Does Not Contain(포함하지 않음) 연산자 명령) 및 시간 범위를 지정하는 데 사용되는 하나 이상의 조건이 포함되어 있습니다.

빠른 필터를 사용하는 경우 **Logged At(**기록된 시간**)** 드롭다운 목록에서 날짜 또는 시간을 선택하여 지난 30일 이내에 기록된 데이터 집합에 대한 보고서를 생성할 수 있습니다. 30일 이전의 날짜 또는 시간에 대한 보고서를 생성하려면 고급 필터를 사용하여 드롭다운 목록의 **Custom(**맞춤 설정**)** 옵션의 **From(**시작**)** 및 **To(**종료**)** 필드에 원하는 기간을 설정하십시오.

빠른 필터 기준 생성

이 섹션에서는 빠른 필터 기준을 생성하는 방법을 설명합니다. 단일 섹션 보고서에 대해서만 빠른 필터 기준을 생성할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Reports(**보고서**)**를 선택하고 원하는 보고서를 클릭합니다.

단계 **2** **Settings(**설정**)** 드롭다운 목록에서 필수 필드를 선택합니다.

단계 **3** 필수 필드의 드롭다운 목록에서 선택하거나 특정 문자를 입력하여 데이터를 필터링할 수 있습니다. 검색에서는 Contains(포함) 연산자 명령을 사용합니다. 예를 들어 "K"로 시작하는 텍스트를 기준으로 필터링하려면 K를 입력하거나 텍스트에 "geo"가 있는 텍스트를 필터링하려면 geo를 입력합니다. *abc로 시작하고 *def로 끝나는 regex와 같이 별표(*)를 사용할 수도 있습니다.

빠른 필터는 포함, 다음으로 시작, 다음으로 종료, 다음으로 시작 또는 종료, OR 연산자를 사용한 다중 값 조건을 사용합니다.

단계 **4** **Enter** 키를 누릅니다.

고급 필터 기준 생성

이 섹션에서는 고급 필터 기준을 생성하는 방법을 설명합니다. 단일 섹션 및 다중 섹션 보고서에 대해 고급 필터를 생성할 수 있습니다. 단일 섹션 보고서의 Filter(필터) 드롭다운 메뉴는 **Quick Filter(**빠른 필터**)**와 **Advanced Filter(**고급 필터**)**로 구성되어 있습니다. 다중 섹션 보고서에서는 고급 필터만 지정할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)**를 선택하고 원하는 보고서를 클릭합니다.

단계 **2** **Filters(**필터**)** 섹션의 **Match(**일치**)** 드롭다운 목록에서 옵션 중 하나를 선택합니다.

a) **All(**모두**)**을 선택하여 지정된 모든 조건과 일치시킵니다.

b) **Any(**일부**)**를 선택하여 지정된 조건 중 하나와 일치시킵니다.

단계 **3** **Time Range(**시간 범위**)** 드롭다운 목록에서 원하는 범주를 선택합니다.

단계 **4** **Operator Commands(**운영자 명령**)** 드롭다운 목록에서 원하는 명령을 선택합니다. 예를 들어 특정 문자로 시작하는 텍스트(Begin With 사용) 또는 텍스트에 있는 특정 문자(Contains 사용)를 필터링할 수 있습니다. 또는 Logged Time(기록된 시간) 및 해당 Custom(맞춤 설정) 옵션을 선택하고 일정표에서 시작 및 종료 날짜와 시간을 지정하여 데이터를 필터링할 수 있습니다.

단계 **5** **Time Range(**시간 범위**)** 드롭다운 목록에서 원하는 옵션을 선택합니다.

단계 **6** **Go(**이동**)**를 클릭합니다.

필터링된 보고서를 저장하고 **Filter(**필터**)** 드롭다운 목록에서 검색하여 나중에 참조할 수 있습니다.

보고서 실행 및 보기

이 섹션에서는 보고서 보기를 사용하여 보고서를 실행, 확인 및 탐색하는 방법을 설명합니다. 보고서를 클릭하면 기본적으로 지난 7일 동안의 데이터가 생성됩니다. 각 보고서에는 페이지당 500개의 데이터 행이 표시됩니다. 보고서에서 데이터를 표시할 시간 단위를 지정할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **ISE Reports(ISE** 보고서**)**.

각 작업 센터 아래의 **Reports(**보고서**)** 링크로 이동하여 해당 작업 센터와 관련된 보고서 세트를 볼 수도 있습니다.

단계 **2** 사용 가능한 **report(**보고서**)** 범주에서 보고서를 클릭합니다.

단계 **3** 보고서를 실행하기 위한 필터를 하나 이상 선택합니다. 각 보고서에서는 서로 다른 필터를 사용할 수 있으며, 그 중에는 필수 필터도 있고 선택적 필터도 있습니다.

단계 **4** 필터에 해당하는 값을 입력합니다.

단계 **5** **Go(**이동**)**를 클릭합니다.

관련 항목

보고서 내보내기, 291 페이지
사용 가능한 보고서, 295 페이지

보고서 탐색

보고서 출력에서 자세한 정보를 얻을 수 있습니다. 예를 들어 5개월 동안의 보고서를 생성한 경우 그래프 및 표에는 수 개월 기간의 보고서에 대한 집계 데이터가 나열됩니다.

표에서 특정 값을 클릭하여 이 특정 필드와 관련된 다른 보고서를 볼 수 있습니다. 예를 들어 인증 요약(Authentication Summary) 보고서에는 사용자 또는 사용자 그룹에 대한 실패 횟수가 표시됩니다. 실패 횟수를 클릭하면 특정 실패 횟수에 해당하는 인증 요약(Authentication Summary) 보고서가 열립니다.

보고서 내보내기

다음 보고서는 PDF 파일 형식으로만 내보낼 수 있습니다.

- 인증 요약(Authentication Summary)
- 상태 요약
- RBACL 삭제 요약

참고 RBACL 삭제 패킷에 대한 플로우는 Cisco Catalyst 6500 시리즈 스위치에서만 사용할 수 있습니다.

- 게스트 스폰서 요약
- 엔드포인트 프로파일 변경
- 네트워크 디바이스 세션 상태

단계 **1** 보고서 실행 및 보기 섹션의 설명에 따라 보고서를 실행합니다.

단계 **2** 보고서 요약 페이지의 오른쪽 위에 있는 **Export To(**다음으로 내보내기**)**를 클릭합니다.

단계 **3** 다음 옵션 중 하나를 선택합니다.

- 저장소(CSV) : CSV 파일 형식으로 보고서를 저장소에 내보내려는 경우
- 로컬(CSV) : CSV 파일 형식으로 보고서를 로컬 디스크에 내보내려는 경우
- 로컬(PDF) : 보고서를 pdf 파일 형식으로 로컬 디스크에 내보내려는 경우

참고 로컬 CSV 또는 pdf 옵션을 선택하면 처음 500개 기록만 내보냅니다. Repository CSV(저장소 CSV) 옵션을 사용하여 모든 기록을 내보낼 수 있습니다.

Cisco ISE 보고서 예약 및 저장

보고서를 사용자 맞춤화하고 변경사항을 새 보고서로 저장하거나 Report Summary(보고서 개요) 페이지의 오른쪽 상단 모서리에 있는 **My Reports(**내 보고서**)**에서 기본 보고서 설정을 복구할 수 있습니다.

ISE 보고서를 맞춤화하여 특정 시간에 또는 특정 시간 간격으로 실행 및 다시 실행되도록 예약할 수도 있습니다. 보고서가 생성되면 이메일 알림을 보내고 받을 수도 있습니다.

시간별 빈도로 보고서를 예약할 경우 보고서를 여러 날에 걸쳐 실행할 수 있지만, 이틀에 걸쳐 기간을 설정할 수 없습니다.

예를 들어 2019년 5월 4일부터 5월 8일까지 시간별 보고서를 예약할 경우 시간 간격을 매일 오전 6시에서 오후 11시 사이로 설정할 수 있지만, 당일 오후 6시부터 익일 오전 11시까지로 설정할 수 없습니다. 후자의 경우 Cisco ISE에서 시간 범위가 유효하지 않다는 오류 메시지를 표시합니다.

참고 외부 관리자(예: Active Directory 관리자)가 email-id 필드를 채우지 않고 예약된 보고서를 생성하는 경우 이메일 알림이 전송되지 않습니다.

다음 보고서는 예약할 수 없습니다.

- 인증 요약(Authentication Summary)
- 상태 요약
- RBACL 삭제 요약
- 게스트 스폰서 요약
- Endpoint Profile Changes(엔드포인트 프로파일 변경)
- 네트워크 디바이스 세션 상태

참고 PAN에서만 Cisco ISE 보고서를 저장하거나 예약(맞춤화)할 수 있습니다.

참고 iI 기본 MnT가 다운되면 보조 MnT에서 예약된 보고서 작업을 실행합니다. 예약된 보고서 작업은 기본 MnT 및 보조 MnT에서 모두 실행됩니다. 보조 MnT에서는 내보내기 작업을 실행하기 전에 기본 MnT에 대해 ping을 시도합니다. ping이 실패할 경우 내보내기 작업만 실행되며, 그렇지 않으면 내보내기 작업을 건너뜁니다.

단계 **1** Running and Viewing Reports(보고서 실행 및 보기) 섹션의 설명에 따라 보고서를 실행합니다.

단계 **2** Report Summary(보고서 요약) 페이지의 오른쪽 상단에 있는 **My Reports(**내 보고서**)**를 클릭합니다.

단계 **3** 대화 상자에서 필요한 세부정보를 입력합니다.

단계 **4** **Save as New(**새 이름으로 저장**)**를 클릭합니다.

저장된 보고서로 돌아오면 모든 필터 옵션이 기본적으로 선택되어 있습니다. 사용하지 않으려는 필터는 선택을 취소하십시오.

My Reports(내 보고서**)** 범주에서 저장된 보고서를 제거할 수도 있습니다.

Cisco ISE 활성 RADIUS 세션

Cisco ISE는 라이브 세션을 위해 활성 RADIUS 세션을 동적으로 제어하는 데 사용할 수 있는 동적 CoA(Change of Authorization) 기능을 제공합니다. 다음 작업을 수행하도록 다시 인증 또는 연결 끊기 요청을 NAD(Network Access Device)로 보낼 수 있습니다.

- 인증과 관련된 문제 해결 - Session reauthentication(세션 재인증) 옵션을 사용하여 다시 재인증하려는 시도에 대한 후속 조치를 취할 수 있습니다. 그러나 이 옵션을 사용하여 액세스를 제한해서는 안 됩니다. 액세스를 제한하려면 종료 옵션을 사용해 주십시오.
- 문제가 있는 호스트 차단 - 네트워크를 통해 대량의 트래픽을 보내는 감염된 호스트를 차단하는 포트 종료 옵션과 함께 세션 종료를 사용할 수 있습니다. 그러나 RADIUS 프로토콜은 현재 종료된 포트를 다시 활성화하는 방법을 지원하지 않습니다.
- 엔드포인트가 IP 주소를 다시 가져오도록 강제 실행 - 신청자 또는 클라이언트가 없는 엔드포인트가 VLAN 변경 후 DHCP 요청을 생성하도록 포트 바운스 옵션과 함께 세션 종료를 사용할 수 있습니다.
- 업데이트된 권한 부여 정책을 엔드포인트에 푸시 - 세션 재인증 옵션을 사용하여 기존 세션에서 관리자 재량에 따른 권한 부여 정책의 변경과 같이 업데이트된 정책 컨피그레이션을 시행할 수 있습니다. 예를 들어 포스처 검증이 활성화된 경우 엔드포인트가 처음에 액세스 권한을 얻을 때 일반적으로 격리됩니다. 엔드포인트의 ID 및 포스처가 알려진 경우 엔드포인트가 해당 포스처

를 기준으로 실제 권한 부여 정책을 얻을 수 있도록 세션 재인증 명령을 엔드포인트로 보낼 수 있습니다.

CoA 명령이 디바이스에 인식되려면 옵션을 적절히 구성해야 합니다.

CoA가 제대로 작동하려면 동적 CoA(Change of Authorization)가 필요한 각 디바이스의 공유 암호를 구성해야 합니다. Cisco ISE는 공유 암호 컨피그레이션을 사용하여 디바이스에서 액세스를 요청하고 CoA 명령을 실행합니다.

참고 이 Cisco ISE 릴리스에서 표시될 수 있는 활성 인증 엔드포인트 세션의 최대 수는 100,000으로 제한됩니다.

관련 항목

RADIUS 세션에 대한 권한 부여 변경, 294 페이지

RADIUS 세션에 대한 권한 부여 변경

네트워크의 일부 네트워크 액세스 디바이스는 다시 로드한 후 계정 중지 또는 계정 끄기 패킷을 전송하지 않을 수도 있습니다. 이로 인해 세션 디렉토리 보고서에 세션이 두 개 표시될 수 있습니다. 두 세션 중 하나는 만료된 세션입니다.

활성 RADIUS 세션의 권한 부여를 동적으로 변경하거나 활성 RADIUS 세션의 연결을 끊으려면 가장 최근 세션을 선택해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **RADIUS Livelog(RADIUS** 라이브 로그**)**.

단계 **2** 보기를 **Show Live Session(**라이브 세션 표시**)**으로 전환합니다.

단계 **3** CoA를 실행할 RADIUS 세션의 CoA 링크를 클릭하고 다음 옵션 중 하나를 선택합니다.

- **SAnet Session Query(SAnet** 세션 쿼리**)** - SAnet 지원 디바이스에서 세션에 대한 정보를 쿼리하려면 이 옵션을 사용합니다.
- **Session reauthentication(**세션 재인증**)** - 세션을 재인증합니다. CoA를 지원하는 ASA 디바이스에서 설정된 세션에 대해 이 옵션을 선택하면 세션 정책 푸시 CoA가 호출됩니다.
- **Session reauthentication with last(**마지막 방법으로 세션 재인증**)** - 이 세션에 대해 마지막으로 성공한 인증 방법을 사용합니다.
- **Session reauthentication with rerun(**다시 실행하여 세션 재인증**)** - 구성된 인증 방법을 처음부터 실행합니다.

  참고 **Session reauthentication with last(**마지막 방법으로 세션 재인증**)** 및 **Session reauthentication with rerun(**다시 실행하여 세션 재인증**)** 옵션은 현재 Cisco iOS 소프트웨어에서 지원되지 않습니다.

- **Session termination(**세션 종료**)** - 세션을 종료합니다. 이 스위치를 선택하면 다른 세션에서 클라이언트가 재인증됩니다.
- **Session termination with port bounce(**포트를 반송하고 세션 종료**)** - 세션을 종료하고 포트를 다시 시작합니다.

- **Session termination with port shutdown(**포트를 종료하고 세션 종료**)** - 세션과 포트를 종료합니다.

단계 **4** **Run(**실행**)**을 클릭하여 선택한 재인증 또는 종료 옵션으로 CoA를 실행합니다.

CoA가 실패하는 경우 다음 원인 중 하나 때문일 수 있습니다.

- 디바이스가 CoA를 지원하지 않습니다.
- ID 또는 권한 부여 정책이 변경되었습니다.
- 공유 암호가 일치하지 않습니다.

사용 가능한 보고서

다음 표에는 미리 구성된 보고서가 범주에 따라 그룹화되어 있습니다. 보고서 기능 및 로깅 범주에 대한 설명도 제공됩니다.

로깅 범주에 대한 시스템 로그를 생성하려면 해당 **Log Severity Level(**로그 심각도 레벨**)**을 **Info(**정보**)**로 설정합니다.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > System(**시스템**) > Logging(**로깅**) > Logging Categories(**로깅 범주**)**.
- 시스템 로그를 생성해야 하는 로깅 범주를 클릭합니다.
- **Log Severity Level(**로그 심각도 레벨**)** 필드의 드롭다운 메뉴에서 **Info(**정보**)**를 선택합니다.
- **Save(**저장**)**를 클릭합니다.

참고 Cisco ISE 릴리스 2.6 이상에서는 IPv6 주소를 사용하는 사용자의 감사 보고서에 로그인/로그아웃, 비밀번호 변경, 운영 변경 사항과 같은 이벤트가 기록됩니다. Administrator Logins(관리자 로그인), User Change Password Audit(사용자 비밀번호 변경 감사) 및 Operations Audit(작업 감사) 보고서에서 이제 IPv4 및 IPv6 기록을 기준으로 로그를 필터링할 수 있습니다.

보고서 이름	설명	로깅 범주
감사		

보고서 이름	설명	로깅 범주
적응형 네트워크 제어 감사	적응형 네트워크 제어 감사 보고서는 RADIUS 계정 관리를 기반으로 합니다. 각 엔드포인트에 대한 모든 네트워크 세션의 기록 보고 정보를 표시합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Passed Authentications(통과한 인증) 및 RADIUS Accounting(RADIUS 계정 관리)을 선택합니다.
관리자 로그인	관리자 로그인 보고서는 모든 GUI 기반 관리자 로그인 이벤트와 성공한 CLI 로그인 이벤트에 대한 정보를 제공합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Administrative and Operational audit(관리 및 운영 감사).
컨피그레이션 변경 감사	컨피그레이션 변경 감사 보고서에서는 지정된 기간 내의 컨피그레이션 변경 사항에 대한 세부정보를 제공합니다. 특정 기능 문제를 해결해야 하는 경우 이 보고서를 통해 최근의 컨피그레이션 변경이 문제에 영향을 미쳤는지 확인할 수 있습니다.	

보고서 이름	설명	로깅 범주
데이터 비우기 감사	데이터 비우기 감사 보고서에서는 로깅 데이터가 비우기될 때 이를 기록합니다. 이 보고서에는 두 개의 데이터 비우기 소스가 반영됩니다. 매일 오전 4시에 Cisco ISE는 Administration(관리) > Maintenance(유지 관리) > Data Purging(데이터 비우기) 페이지에 설정한 기준을 충족하는 로깅 파일이 있는지 확인합니다. 있는 경우 파일이 삭제되고 이 보고서에 기록됩니다. 또한 Cisco ISE는 지속적으로 로그 파일의 저장 공간 중 사용된 공간을 최대 80%로 유지합니다. Cisco ISE는 매시간마다 이 비율을 확인하고 80% 임계값에 다시 도달할 때까지 가장 오래된 데이터를 삭제합니다. 이 정보도 이 보고서에 기록됩니다. 디스크 공간 사용률이 높은 경우 80% 임계값에 도달할 때 `ISE Monitor node(s) is about to exceed the maximum amount allocated`라는 알림 메시지가 표시됩니다. 그런 다음 90% 임계값에 도달할 때 `ISE Monitor node(s) has exceeded the maximum amount allocated`라는 알림 메시지가 표시됩니다.	—
엔드포인트 제거 활동	엔드포인트 제거 활동 보고서에서는 엔드포인트 제거 활동 기록을 검토할 수 있습니다. 이 보고서를 사용하려면 Profiler(프로파일러) 로깅 범주를 활성화해야 합니다. 이 범주는 기본적으로 활성화되어 있습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Profiler(프로파일러)를 선택합니다.

보고서 이름	설명	로깅 범주
내부 관리자 요약	내부 관리자 요약 보고서에서는 관리자 사용자의 자격을 확인할 수 있습니다. 이 보고서에서는 관리자 로그인 및 컨피그레이션 변경 감사 보고서에도 액세스할 수 있습니다. 이러한 보고서에서는 각 관리자에 대한 세부정보를 볼 수 있습니다.	—
운영 감사	운영 감사 보고서에서는 백업 실행, Cisco ISE 노드 등록 또는 애플리케이션 다시 시작 등 작동 변경에 대한 세부정보를 제공합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Administrative and Operational audit(관리 및 운영 감사).
pxGrid 관리자 감사	pxGrid 관리자 감사 보고서에서는 클라이언트 등록, 클라이언트 등록 취소, 클라이언트 승인, 항목 생성, 항목 삭제, 기본 PAN에서의 게시자-구독자 추가 및 게시자-구독자 삭제 등의 pxGrid 관리 작업에 대한 세부정보를 제공합니다. 각 기록에는 노드에 대한 작업을 수행한 관리자 이름이 있습니다. 관리자 및 메시지 기준에 따라 pxGrid 관리자 감사 보고서를 필터링할 수 있습니다.	—
보안 통신 감사	보안 통신 감사 보고서는 Cisco ISE 관리 CLI의 보안 관련 이벤트에 대한 감사 세부정보를 제공합니다. 여기에는 인증 장애, 침입 시도 가능성, SSH 로그인, 장애가 발생한 비밀번호, SSH 로그아웃, 잘못된 사용자 계정 등이 포함됩니다.	—
사용자 변경 비밀번호 감사	사용자 변경 비밀번호 감사 보고서에서는 직원의 비밀번호 변경에 대한 확인을 표시합니다.	Administrative and Operational audit(관리 및 운영 감사)

보고서 이름	설명	로깅 범주
Trustsec 감사	Trustsec 감사 로그에는 다음이 포함됩니다. • Trustsec 구성 요소의 관리(생성, 이름 변경, 업데이트 및 삭제) • Trustsec이 활성화된 NAD에 SGACL 및 SGT 구축 • Trustsec 세션. Cisco ISE가 Cisco DNA Center와 통합되어 있고 SD Access가 Cisco DNA Center에서 관리되는 경우 이 로그는 비어 있습니다.	—
디바이스 관리		
인증 요약(Authentication Summary)	TACACS Authentication Summary(TACACS 인증 요약) 보고서는 가장 일반적인 인증 및 인증 실패 이유에 대한 세부정보를 제공합니다.	—
TACACS 계정 관리	TACACS 계정 관리 보고서는 디바이스 세션에 대한 계정 관리 세부정보를 제공합니다. 사용자와 디바이스의 생성된 시간 및 기록된 시간 관련 정보가 표시됩니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 TACACS Accounting(TACACS 계정 관리)을 선택합니다.
Top N Authentication by Failure Reason(실패 이유별 상위 N 인증)	Top N Authentication by Failure Reason(실패 이유별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 실패 이유별 통과 및 실패한 인증 수가 표시됩니다.	—
Top N Authentication by Network Device(네트워크 디바이스별 상위 N 인증)	Top N Authentication by Network Device(네트워크 디바이스별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 네트워크 디바이스별 통과 및 실패한 인증 수가 표시됩니다.	—

보고서 이름	설명	로깅 범주
Top N Authentication by User(사용자별 상위 N 인증)	Top N Authentication by User(사용자별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 사용자 이름별 통과 및 실패한 인증 수가 표시됩니다.	—
Diagnostics(진단**)**		
AAA 진단	AAA 진단 보고서에서는 Cisco ISE와 사용자 간의 모든 네트워크 세션에 대한 세부정보를 제공합니다. 사용자가 네트워크에 액세스할 수 없는 경우 이 보고서를 검토하여 트렌드를 파악하고 문제를 특정 사용자와 격리할 수 있는지, 아니면 좀 더 광범위한 문제로 나타낼 수 있는지 식별할 수 있습니다. 참고 때때로 ISE는 사용자 인증이 진행 중인 경우에 엔드포인트의 계정 관리 중지 요청을 자동으로 취소합니다. 그러나 ISE는 사용자 인증이 완료되고 나면 모든 계정 관리 요청을 승인합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Policy Diagnostics(정책 진단), Identity Stores Diagnostics(ID 저장소 진단), Authentication Flow Diagnostics(인증 플로우 진단) 및 RADIUS Diagnostics(RADIUS 진단) 로깅 범주를 선택합니다.
AD Connector 운영	AD Connector 운영 보고서에서는 Cisco ISE 서버 비밀번호 새로 고침, Kerberos 티켓 관리, DNS 쿼리, DC 검색, LDAP 및 RPC 관리 관리 등 AD Connector에서 수행된 작업 로그를 제공합니다. 일부 AD 장애가 발생하면 이 보고서의 세부정보를 검토하여 가능한 원인을 식별할 수 있습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 AD Connector를 선택합니다.

보고서 이름	설명	로깅 범주
Endpoint Profile Changes(엔드포인트 프로파일 변경)	엔드포인트별 상위 권한 부여(MAC 주소) 보고서에서는 네트워크에 액세스할 수 있도록 Cisco ISE가 각 엔드포인트 MAC 주소에 대한 권한을 부여한 횟수를 표시합니다.	Passed authentications(통과한 인증), Failed Attempts(실패한 시도)
상태 요약	상태 요약 보고서에서는 대시보드와 유사한 세부정보를 제공합니다. 그러나 대시보드에는 지난 24시간 동안의 데이터만 표시되지만 이 보고서에서는 더 자세한 기록 데이터를 검토할 수 있습니다. 이 데이터를 평가하여 데이터의 일관된 패턴을 확인할 수 있습니다. 예를 들어 대부분의 직원이 하루 일과를 시작하는 시점에 CPU 사용량이 증가할 것을 예측할 수 있습니다. 이러한 트렌드의 불일치가 발견되는 경우 잠재적 문제를 식별할 수 있습니다. CPU Usage(CPU 사용량) 표에는 다양한 Cisco ISE 기능의 CPU 사용량 백분율이 나열됩니다. **show cpu usage** CLI 명령의 출력이 이 표에 나와 있으며, 이러한 값을 구축 내 문제와 연결하여 문제 원인을 식별할 수 있습니다.	—

보고서 이름	설명	로깅 범주
ISE 카운터	ISE Counters(ISE 카운터) 보고서에는 다양한 속성에 대한 임계값이 나열됩니다. 이러한 다양한 속성의 값은 서로 다른 간격으로 수집되며 데이터는 표 형식으로 표시됩니다. 하나는 5분 간격이고 다른 하나는 5분 초과 간격입니다. 이 데이터를 평가하여 추세를 확인할 수 있으며, 임계값보다 높은 값이 있는 경우 이 정보를 구축의 문제와 연관시켜 가능한 원인을 파악할 수 있습니다. Cisco ISE는 기본적으로 이러한 속성의 값을 수집합니다. Cisco ISE CLI에서 **application configure ise** 명령을 사용하여 이 데이터 수집을 비활성화하도록 선택할 수 있습니다. 옵션 14를 선택하여 카운터 속성 수집을 활성화하거나 비활성화하십시오.	—
핵심 성능 메트릭	Key Performance Metrics(핵심 성능 메트릭) 보고서는 구축에 연결되는 엔드포인트 수 및 각 PSN에서 시간 단위로 처리되는 RADIUS 요청 수에 대한 통계 정보를 제공합니다. 이 보고서는 서버의 평균 로드, 요청당 평균 레이턴시 및 초당 평균 트랜잭션을 나열합니다.	—

보고서 이름	설명	로깅 범주
잘못 구성된 NAS	잘못 구성된 NAS 보고서에서는 일반적으로 계정 관리 정보를 빈번하게 전송하는 경우 계정 관리 빈도가 부정확한 NAD에 대한 정보를 제공합니다. 정정 작업을 수행하고 잘못 구성된 NAD를 수정한 경우 보고서에는 수정 승인이 표시됩니다. 참고 이 보고서를 실행하려면 RADIUS 억제를 활성화해야 합니다.	—
잘못 구성된 신청자	잘못 구성된 신청자 보고서에서는 특정 신청자가 수행한 실패한 시도에 따른 통계와 함께 잘못 구성된 신청자 목록을 제공합니다. 정정 작업을 수행하고 잘못 구성된 신청자를 수정한 경우 보고서에는 수정 승인이 표시됩니다. 참고 이 보고서를 실행하려면 RADIUS 억제를 활성화해야 합니다.	—
네트워크 디바이스 세션 상태	네트워크 디바이스 세션 상태 요약 보고서를 사용하면 스위치에 직접 로그인하지 않고도 스위치 컨피그레이션을 표시할 수 있습니다. Cisco ISE는 SNMP 쿼리를 사용하여 이러한 세부정보에 액세스하므로 SNMP v1/v2c를 사용하여 네트워크 디바이스를 구성해야 합니다. 사용자에게 네트워크 문제가 발생하는 경우 이 보고서를 사용하면 해당 문제가 Cisco ISE가 아니라 스위치 컨피그레이션과 관련된 문제인지 쉽게 파악할 수 있습니다.	—

보고서 이름	설명	로깅 범주
OCSP 모니터링	OCSP 모니터링 보고서에서는 OCSP(Online Certificate Status Protocol) 서비스의 상태를 지정합니다. Cisco ISE가 성공적으로 인증서 서버에 연결하고 인증서 상태 감사를 제공할수 있는지 여부를 나타냅니다. Cisco ISE에서 수행하는 모든 OCSP 인증서 검증 작업에 대한 요약정보를 제공합니다. OCSP 서버에서 정상 상태 및 취소된 기본/보조 인증서와 관련된 정보를 검색합니다. Cisco ISE는 응답을 캐시하고 이를 이후의 OCSP 모니터링 보고서를 활용하는 데 활용합니다. 캐시가 지워지면 OCSP 서버에서 정보를 검색합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 System Diagnostics(시스템 진단).
RADIUS 오류	RADIUS Errors(RADIUS 오류) 보고서에서는 RADIUS 요청 삭제됨(알 수 없는 네트워크 액세스 디바이스에서 버려진 인증/계정 관리 요청), EAP 연결 시간 초과 및 알 수 없는 NAD를 확인할 수 있습니다. 참고 지난 5일 동안의 보고서만 볼 수 있습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Failed Attempts(실패한 시도)를 선택합니다.

보고서 이름	설명	로깅 범주
시스템 진단	시스템 진단 보고서에서는 Cisco ISE 노드의 상태에 대한 세부정보를 제공합니다. Cisco ISE 노드를 등록할 수 없는 경우 이 보고서를 검토하여 문제를 해결할 수 있습니다. 이 보고서를 사용하려면 먼저 여러 진단 로깅 범주를 활성화해야 합니다. 이러한 로그를 수집하는 경우 Cisco ISE 성능에 부정적 영향을 줄 수 있습니다. 그러므로 이러한 범주는 기본적으로 활성화되어 있지 않으므로 데이터를 수집하는 기간 동안만 활성화해야 합니다. 그렇지 않으면, 30분 후에 자동으로 비활성화됩니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택한 후에 Internal Operations Diagnostics(내부 운영 진단), Distributed Management(분산형 관리), Administrator Authentication and Authorization(관리자 인증 및 권한 부여) 로깅 범주를 선택합니다.
엔드포인트 및 사용자		
인증 요약(Authentication Summary)	인증 요약(Authentication Summary) 보고서는 RADIUS 인증을 기반으로 합니다. 가장 일반적인 인증과 함께 인증 실패에 대한 이유를 확인할 수 있습니다. 예를 들어 한 Cisco ISE 서버가 다른 서버에 비해 훨씬 많은 인증을 처리하고 있는 경우 향상된 로드 밸런싱을 위해 사용자를 다른 Cisco ISE 서버에 다시 할당해야 할 수 있습니다. 참고 인증 요약(Authentication Summary) 보고서 또는 대시보드에는 실패했거나 성공한 인증에 해당하는 최신 데이터가 수집되어 표시되므로, 보고서 내용이 표시될 때까지는 몇 분 정도 걸립니다.	—
에이전트리스 포스처	에이전트리스 포스처를 실행한 모든 엔드포인트를 나열합니다.	

보고서 이름	설명	로깅 범주
클라이언트 프로비저닝	클라이언트 프로비저닝 보고서에는 특정 엔드포인트에 적용된 클라이언트 프로비저닝 에이전트가 표시됩니다. 이 보고서를 사용하여 각 엔드포인트에 적용된 정책을 검토하여 엔드포인트가 올바르게 프로비저닝되었는지 여부를 확인할 수 있습니다. 참고 엔드포인트가 ISE와 연결되지 않거나(세션이 설정되지 않음) NAT(Network Address Translation) 주소가 세션에 사용되는 경우 엔드포인트의 MAC 주소가 엔드포인트 ID 열에 표시되지 않습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Client Provisioning Audit and Posture(포스처 및 클라이언트 프로비저닝 감사 및 포스처) 및 Client Provisioning Diagnostics(클라이언트 프로비저닝 진단)를 선택합니다.
현재 활성 세션	현재 활성 세션 보고서를 사용하면 지정된 기간 내에 현재 네트워크에 있는 사용자에 대한 세부정보가 포함된 보고서를 내보낼 수 있습니다. 사용자가 네트워크에 액세스하지 않은 경우에는 세션이 인증 또는 종료되었는지 확인하거나 세션에 다른 문제가 있는지 확인할 수 있습니다.	—
엔드포인트 스크립트 프로비저닝 요약	**Endpoint Scripts Provisioning Summary(**엔드포인트 스크립트 프로비저닝 요약**)** 창에는 지난 30일간 엔드포인트 스크립트 마법사를 통해 실행된 작업의 세부정보가 표시됩니다.	—

보고서 이름	설명	로깅 범주
외부 모바일 디바이스 관리	외부 모바일 디바이스 관리 보고서에서는 Cisco ISE와 외부 MDM(Mobile Device Management) 서버 간 통합에 대한 세부정보를 제공합니다. 이 보고서를 사용하면 MDM 서버에 직접 로그인하지 않고도 MDM 서버에서 프로비저닝된 엔드포인트를 확인할 수 있습니다. 등록 및 MDM 규정 준수 상태 등에 대한 정보도 표시됩니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 MDM을 선택합니다.
패시브 ID	Passive ID(패시브 ID) 보고서에서는 도메인 컨트롤러에 대한 WMI 연결의 상태를 모니터링하고 그와 관련된 통계(예: 수신된 알림 개수, 초당 사용자 로그인/로그아웃 수 등)를 수집할 수 있습니다. 참고 이 방법으로 인증된 세션의 보고서에는 인증 세부정보가 없습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Identity Mapping(ID 매핑)을 선택합니다.
수동 인증서 프로비저닝	수동 인증서 프로비저닝 보고서에는 인증서 프로비저닝 포털을 통해 수동으로 프로비저닝한 모든 인증서가 나열됩니다.	—
조건별 Posture Assessment	조건별 Posture Assessment 보고서를 사용하면 ISE에 구성되어 있는 포스처 정책 조건을 기준으로 기록을 확인하여 클라이언트 머신에서 최신 보안 설정 또는 애플리케이션을 사용할 수 있는지를 검증할 수 있습니다.	—

보고서 이름	설명	로깅 범주
엔드포인트별 Posture Assessment	Posture Assessment by Endpoint(엔드포인트별 포스처 평가) 보고서는 엔드포인트의 시간, 상태, PRA 작업 등의 자세한 정보를 제공합니다. **Details(**세부정보**)**를 클릭하여 엔드포인트에 대한 자세한 정보를 볼 수 있습니다. 참고 Posture Assessment by Endpoint(엔드포인트별 포스처 평가) 보고서는 엔드포인트의 애플리케이션 및 하드웨어 속성에 대한 포스처 정책 세부정보는 제공하지 않습니다. 이 정보는 Context Visibility(상황 가시성) 페이지에서만 볼 수 있습니다.	—
프로파일링된 엔드포인트 요약	프로파일링된 엔드포인트 요약 보고서는 네트워크에 액세스하는 엔드포인트에 대한 프로파일링 세부정보를 제공합니다. 참고 Cisco IP-Phone과 같이 세션 시간을 등록하지 않는 엔드포인트의 경우 Not Applicable(해당 없음)이 Endpoint session time(엔드포인트 세션 시간) 필드에 표시됩니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Profiler(프로파일러)를 선택합니다.

보고서 이름	설명	로깅 범주
RADIUS 계정 관리	RADIUS Accounting Report에서는 네트워크에서 사용자가 유지된 기간을 식별합니다. 사용자의 네트워크 액세스가 손실되면 이 보고서를 사용하여 Cisco ISE가 네트워크 연결 문제의 원인인지 확인할 수 있습니다. 참고 임시 업데이트에 지정된 세션의 IPv4 또는 IPv6 주소 변경 사항 정보가 포함되어 있는 경우 RADIUS 계정 관리 임시 업데이트가 RADIUS 계정 관리 보고서에 포함됩니다.	
RADIUS 인증	RADIUS 인증 보고서에서는 인증 실패 및 성공 기록을 검토할 수 있습니다. 사용자가 네트워크에 액세스할 수 없는 경우 이 보고서의 세부정보를 검토하여 가능한 원인을 식별할 수 있습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Passed Authentications(통과한 인증) 및 Failed Attempts(실패한 시도) 로깅 범주를 선택합니다.
등록된 엔드포인트	등록된 엔드포인트 보고서에는 직원이 등록한 모든 개인 디바이스를 표시합니다.	—
거부된 엔드포인트	Rejected Endpoints(거부된 엔드포인트) 보고서에는 직원이 등록하고 거부되거나 릴리스된 모든 개인 디바이스가 나열됩니다.	—
신청자 프로비저닝	신청자 프로비저닝 보고서에서는 직원의 개인 디바이스에 프로비저닝된 신청자에 대한 세부정보를 제공합니다.	Posture and Client Provisioning Audit(포스처 및 클라이언트 프로비저닝 감사)

보고서 이름	설명	로깅 범주
엔드포인트별 상위 권한 부여	엔드포인트별 상위 권한 부여(MAC 주소) 보고서에서는 네트워크에 액세스할 수 있도록 Cisco ISE가 각 엔드포인트 MAC 주소에 대한 권한을 부여한 횟수를 표시합니다.	Passed authentications(통과한 인증), Failed Attempts(실패한 시도)
사용자별 상위 권한 부여	사용자별 상위 권한 부여 보고서에서는 네트워크에 액세스할 수 있도록 Cisco ISE가 각 사용자에게 권한을 부여한 횟수를 표시합니다.	Passed authentications(통과한 인증), Failed Attempts(실패한 시도)
액세스 서비스별 상위 N 인증	Top N Authentication by Access Service(액세스 서비스별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 액세스 서비스 유형별 통과 및 실패한 인증 수가 표시됩니다.	—
Top N Authentication by Failure Reason(실패 이유별 상위 N 인증)	Top N Authentication by Failure Reason(실패 이유별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 실패 이유별 통과 및 실패한 인증 수가 표시됩니다.	—
Top N Authentication by Network Device(네트워크 디바이스별 상위 N 인증)	Top N Authentication by Network Device(네트워크 디바이스별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 네트워크 디바이스별 통과 및 실패한 인증 수가 표시됩니다.	—
Top N Authentication by User(사용자별 상위 N 인증)	Top N Authentication by User(사용자별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 사용자 이름별 통과 및 실패한 인증 수가 표시됩니다.	—
게스트		

보고서 이름	설명	로깅 범주
AUP 수락 상태	AUP 수락 상태 보고서에서는 모든 게스트 포털의 AUP 수락에 대한 세부정보를 제공합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Guest(게스트)를 선택합니다.
게스트 계정 관리	게스트 계정 보고서는 RADIUS 계정 보고서의 하위 집합입니다. 활성화된 게스트 또는 게스트 ID 그룹에 할당된 모든 사용자는 이 보고서에 표시됩니다.	—

보고서 이름	설명	로깅 범주
기본 게스트 보고서	Primary(기본) Guest(게스트) 보고서에는 다양한 게스트 액세스 보고서의 데이터가 결합되어 있으며 다양한 보고 소스의 데이터를 내보낼 수 있습니다. Primary(기본) Guest(게스트) 보고서에서는 게스트 사용자가 방문하는 웹사이트에 대한 세부정보도 제공합니다. 보안 감사용으로 이 보고서를 사용하여 게스트 사용자가 네트워크에 액세스한 시기, 그리고 어떤 작업을 수행했는지 살펴볼 수 있습니다. 또한 게스트 트래픽에 사용된 NAD(Network Access Device)에 대한 HTTP 검사도 활성화해야 합니다. 이 정보는 NAD에 의해 Cisco ISE로 다시 보내집니다. 클라이언트가 최대 동시 세션 제한에 도달하는 시기를 확인하려면 관리 포털에서 **Administration(**관리**) > System(**시스템**) > Logging(**로깅**) > Logging Categories(**로깅 범주**)**를 선택하고 다음을 수행합니다. **1.** "Authentication Flow Diagnostics(인증 플로우 진단)" 로깅 범주의 로그 레벨을 WARN에서 INFO로 높입니다. **2.** AAA Diagnostics(AAA 진단)의 "Logging Category(로깅 범주)"에서 LogCollector Target(LocCollector 타깃)을 Available(사용 가능한 항목)에서 Selected(선택한 항목)로 변경합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > System(**시스템**) > Logging(**로깅**) > Logging Categories(**로깅 범주**)**를 선택하고 Passed Authentications(통과한 인증)를 선택합니다.

보고서 이름	설명	로깅 범주
내 디바이스 로그인 및 감사	내 디바이스 로그인 및 감사 보고서에서는 내 디바이스 포털에서 디바이스에 대해 사용자가 수행한 로그인 활동 및 작업에 대한 세부정보를 제공합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 My Devices(내 디바이스)를 선택합니다.
스폰서 로그인 및 감사	스폰서 로그인 및 감사 보고서에서는 게스트 사용자의 로그인, 추가, 삭제, 활성화, 일시 중지 및 업데이트 작업과 함께 스폰서 포털에서의 스폰서의 로그인 활동에 대한 세부정보를 제공합니다. 게스트 사용자가 대량으로 추가된 경우 '게스트 사용자' 열 아래 표시됩니다. 이 열은 기본적으로 숨겨져 있습니다. 내보내기 시에 이러한 대량 사용자는 내보내는 파일에도 표시됩니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Guest(게스트)를 선택합니다.
SXP		
SXP 바인딩	SXP 바인딩 보고서는 SXP 연결을 통해 교환되는 IP-SGT 바인딩에 대한 정보를 제공합니다.	—
SXP 연결	이 보고서를 사용하여 SXP 연결의 상태를 모니터링하고 피어 IP, SXP 노드 IP, VPN 이름, SXP 모드 등 해당 연결과 관련된 정보를 수집할 수 있습니다.	—
TrustSec		

보고서 이름	설명	로깅 범주
RBACL 삭제 요약	RBACL 삭제 요약 보고서는 고급 Cisco ISE 라이선스가 있는 경우에만 사용할 수 있는 TrustSec 기능과 관련된 보고서입니다. 또한 이 보고서를 사용하려면 삭제된 이벤트에 해당하는 NetFlow 이벤트를 Cisco ISE로 보내도록 네트워크 디바이스를 구성해야 합니다. 사용자가 특정 정책 또는 액세스를 위반하는 경우 패킷이 삭제되고 이 보고서에 표시됩니다. 참고 RBACL 삭제 패킷 플로우는 Cisco Catalyst 6500 시리즈 스위치에서만 사용할 수 있습니다.	—
사용자별 상위 N개 RBACL 삭제	사용자별 상위 N개 RBACL 삭제 보고서는 고급 Cisco ISE 라이선스가 있는 경우에만 사용할 수 있는 TrustSec 기능과 관련된 보고서입니다. 또한 이 보고서를 사용하려면 삭제된 이벤트에 해당하는 NetFlow 이벤트를 Cisco ISE로 보내도록 네트워크 디바이스를 구성해야 합니다. 이 보고서에는 특정 사용자에 의한 정책 위반(패킷 삭제 기준)이 표시됩니다. 참고 RBACL 삭제 패킷 플로우는 Cisco Catalyst 6500 시리즈 스위치에서만 사용할 수 있습니다.	—

보고서 이름	설명	로깅 범주
TrustSec ACI	이 보고서에는 APIC의 IEPG, EEPG, 엔드포인트 및 서브넷 컨피그레이션과 동기화된 SGT 및 SXP 매핑이 나열됩니다. 이러한 세부정보는 TrustSec APIC 통합 기능이 활성화되어 있어야 표시됩니다.	—

보고서 이름	설명	로깅 범주
TrustSec 구축 확인		—

보고서 이름	설명	로깅 범주
	이 보고서를 사용하여 최신 TrustSec 정책이 모든 네트워크 디바이스에 구축되었는지 또는 Cisco ISE와 네트워크 디바이스에 구성된 정책 간에 불일치 사항이 있는지 확인할 수 있습니다. **Details(**세부정보**)** 아이콘을 클릭하여 확인 프로세스의 결과를 확인합니다. 다음과 같은 세부정보를 확인할 수 있습니다. • 확인 프로세스가 시작 및 완료된 시점 • 최신 TrustSec 정책이 네트워크 디바이스에 성공적으로 구축되었는지 여부. 최신 TrustSec 정책이 구축된 네트워크 디바이스의 이름 및 IP 주소도 볼 수 있습니다. • Cisco ISE와 네트워크 디바이스에 구성된 정책 간에 불일치사항이 있는지 여부. 각 정책 차이에 대해 디바이스 이름, IP 주소, 해당 오류 메시지가 표시됩니다. **Alarms(**경보**)** dashlet(**Work Centers(**작업 센터**) > TrustSec > Dashboard(**대시보드**)** 및 **Home(**홈**) > Summary(**요약**)**에 있음)에서 TrustSec Deployment Verification(TrustSec 구축 확인) 경보를 볼 수 있습니다. 참고 • 보고에 소요되는 시간은 구축에 포함된 네트워크 디바이스 및 TrustSec 그룹 수에 따라 달라집니다. • TrustSec Deployment	

보고서 이름	설명	로깅 범주
	Verification(TrustSec 구축 확인) 보고서의 오류 메시지 길이는 현재 480자로 제한됩니다. 480자를 초과하는 오류 메시지는 잘리고 처음 480자만 보고서에 표시됩니다.	
TrustSec 정책 다운로드	이 보고서에는 정책(SGT/SGACL) 다운로드를 위해 네트워크 디바이스에서 전송한 요청과 ISE에서 전송한 세부정보가 나열됩니다. 워크플로우 모드가 활성화되어 있으면 프로덕션 또는 스테이징 매트릭스에 대한 요청을 필터링할 수 있습니다.	이 보고서를 보려면 다음을 수행해야 합니다. 1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Logging(로깅)** > **Logging Categories(로깅 범주)**. 2. **AAA Diagnostics(AAA 진단)** > **RADIUS Diagnostics(RADIUS 진단)**를 선택합니다. 3. RADIUS 진단의 경우 Log Severity Level(로그 심각도 레벨)을 DEBUG로 설정합니다.
Threat Centric NAC 서비스		
어댑터 상태	어댑터 상태 보고서에는 위협 및 취약점 어댑터의 상태가 표시됩니다.	—
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.	—

보고서 이름	설명	로깅 범주
위협 이벤트	Threat Events(위협 이벤트) 보고서는 Cisco ISE가 사용자가 구성한 다양한 어댑터에서 수신하는 모든 위협 이벤트의 목록을 제공합니다.	—
취약점 평가	취약점 평가 보고서는 엔드포인트에 대해 수행되는 평가와 관련된 정보를 제공합니다. 이 보고서를 보고 구성된 정책을 기준으로 평가가 수행되는지를 확인할 수 있습니다.	—

RADIUS 라이브 로그

다음 표에서는 최근 RADIUS 인증이 표시되는 Live Logs(RADIUS 라이브 로그) 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(운영)** > **RADIUS** > **Live Logs(라이브 로그)**입니다. 기본 PAN에서만 RADIUS 라이브 로그를 볼 수 있습니다.

표 ***40: RADIUS*** 라이브 로그

필드 이름	설명
Time(시간)	모니터링 및 문제 해결 수집 에이전트가 로그를 수신한 시간을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Status(상태)	인증 성공 여부를 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다. 인증이 통과한 경우 녹색으로 표시되고, 인증이 실패한 경우 빨간색으로 표시됩니다.

필드 이름	설명
Details(세부정보**)**	Details(세부정보) 열 아래의 아이콘을 클릭하면 새 브라우저 창에서 **Authentication Detail Report(**인증 세부정보 보고서**)**가 열립니다. 이 보고서는 인증 및 관련 속성, 인증 플로우에 대한 정보를 제공합니다. **Authentication Details(**인증 세부정보**)** 상자에서 **Response Time(**응답 시간**)**은 Cisco ISE가 인증 플로우를 처리하는 데 걸리는 총 시간입니다. 예를 들어 인증이 3개의 왕복 메시지로 구성되어 있고 첫 메시지는 300ms, 그 다음 메시지는 150ms, 마지막 메시지는 100ms의 처리 시간이 소요된 경우 **Response Time(**응답 시간**)**은 300 + 150 + 100 = 550ms입니다. 참고 48시간 넘게 활성 상태인 엔드포인트의 세부정보는 볼 수 없습니다. 48시간 넘게 활성 상태인 엔드포인트의 **Details(**세부정보**)** 아이콘을 클릭하면 다음 메시지가 포함된 페이지가 표시될 수 있습니다. `No Data available for this record(이 기록에 데이터가 없습니다). Either the data is purged or authentication for this session record happened a week ago(데이터가 삭제되었거나이 세션 기록에 대한 인증이 일주일 전에 발생했습니다). Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session('PassiveID' 또는 'PassiveID Visibility' 세션인 경우에는 ISE가 아닌 세션에 대한 인증 세부정보만 포함됩니다).`
Repeat Count(반복 횟수**)**	지난 24시간 동안 ID, 네트워크 디바이스 및 권한 부여가 변경되지 않고 인증 요청이 반복된 횟수를 표시합니다.

필드 이름	설명
ID	인증과 연결된 로그인한 사용자 이름을 표시합니다. ID 저장소에 사용자 이름이 없는 경우 INVALID로 표시됩니다. 인증이 다른 이유로 인해 실패하는 경우 USERNAME으로 표시됩니다. 참고 이는 사용자에게만 적용되며, MAC 주소에는 적용되지 않습니다. 디버깅을 지원하기 위해 Cisco ISE가 잘못된 사용자 이름을 표시하도록 할 수 있습니다. 이렇게 하려면 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Security Settings(**보안 설정**)**에서 **Disclose Invalid Usernames(**잘못된 사용자 이름 공개**)** 확인란을 선택합니다. 또한 **Disclose Invalid Usernames(**잘못된 사용자 이름 공개**)** 옵션이 시간 초과되도록 구성하여 이 옵션을 수동으로 해제할 필요가 없게 할 수 있습니다.
Endpoint ID(엔드포인트 **ID)**	엔드포인트의 고유한 식별자(일반적으로는 MAC 또는 IP 주소)를 표시합니다.
Endpoint Profile(엔드포인트 프로파일**)**	iPhone, Android, MacBook, Xbox 등으로 프로파일이 지정된 엔드포인트 유형을 표시합니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.
Authorization Policy(권한 부여 정책**)**	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.
Authorization Profiles(권한 부여 프로파일**)**	인증에 사용된 권한 부여 프로파일을 표시합니다.
IP Address(IP 주소**)**	엔드포인트 디바이스의 IP 주소를 표시합니다.
Network Device(네트워크 디바이스**)**	네트워크 액세스 디바이스의 IP 주소를 표시합니다.
Device Port(디바이스 포트**)**	엔드포인트가 연결되어 있는 포트 번호를 표시합니다.
Identity Group(ID 그룹**)**	로그가 생성된 대상인 사용자나 엔드포인트에 할당되는 ID 그룹을 표시합니다.
Posture Status(포스처 상태**)**	포스처 검증의 상태 및 인증에 대한 세부정보를 표시합니다.

필드 이름	설명
Server(서버**)**	로그가 생성된 정책 서비스를 나타냅니다.
MDM Server Name(MDM 서버 이름**)**	MDM 서버의 이름을 표시합니다.
Event(이벤트**)**	이벤트 상태를 표시합니다.
Failure Reason(실패 이유**)**	인증이 실패한 경우 자세한 실패 이유를 표시합니다.
Auth Method(인증 방법**)**	MS-CHAPv2(Microsoft Challenge Handshake Authentication Protocol Version 2), IEE 802.1x 또는 dot1x 등과 같이 RADIUS 프로토콜에서 사용하는 인증 방법을 표시합니다.
Authentication Protocol(인증 프로토콜**)**	PEAP(Protected Extensible Authentication Protocol), EAP(Extensible Authentication Protocol) 등 사용되는 인증 프로토콜을 표시합니다.
Security Group(보안 그룹**)**	인증 로그로 식별된 그룹을 표시합니다.
Session ID(세션 **ID)**	세션 ID를 표시합니다.

참고 **RADIUS Live Logs(RADIUS** 라이브 로그**)** 및 **TACACS+ Live Logs(TACACS+** 라이브 로그**)** 창에는 각 정책 권한 부여 규칙의 첫 번째 속성에 대한 "Queried PIP" 항목이 표시됩니다. 권한 부여 규칙 내의 모든 속성이 이전 규칙에 대해 이미 쿼리된 사전과 관련된 경우 추가 "Queried PIP" 항목이 표시되지 않습니다.

RADIUS **Live Logs(**라이브 로그**)** 창에서는 다음을 수행할 수 있습니다.

- 데이터를 CSV 또는 PDF 형식으로 내보냅니다.
- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 사용자 맞춤화 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.
- 열 값을 정렬합니다.

참고 모든 사용자 맞춤 설정은 사용자 기본 설정으로 저장됩니다.

인증 레이턴시

인증 레이턴시는 인증 프로세스가 시작된 시점부터 RADIUS 인증 프로세스의 평균 응답 시간입니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Dashboard(**대시보드**)** > **System Summary(**시스템 요약**)** dashlet(대시릿).에서 Cisco ISE 인증 레이턴시를 확인할 수 있습니다.

드롭 다운 목록에서 다음 인증 레이턴시 기간을 선택할 수 있습니다.

- **60mins(60**분**)** :이 옵션은 지난 60분 동안 시작된 인증에 대한 인증 레이턴시를 제공합니다.
- **12hrs(12**시간**)** :이 옵션은 지난 24시간 동안 시작된 인증 프로세스에 대한 인증 레이턴시를 제공합니다.

표시되는 응답 시간은 밀리초(ms)입니다. 인증 레이턴시에 대한 자세한 보고서를 보려면 **Live Logs(**라이브 로그**)** 창에서 최신 로그를 클릭합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS**.

RADIUS 라이브 세션

다음 표에서는 라이브 인증을 표시하는, RADIUS **Live Sessions(**라이브 세션**)** 창의 필드를 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 RADIUS 라이브 세션의 Primary PAN(기본 PAN)에서만 볼 수 있습니다.

표 ***41: RADIUS*** 라이브 세션

필드 이름	설명
Initiated(시작됨**)**	세션이 시작된 타임스탬프를 표시합니다.
Updated(업데이트됨**)**	변경으로 인해 세션이 마지막으로 업데이트된 타임스탬프를 표시합니다.
Account Session Time(계정 세션 시간**)**	사용자 세션의 시간 범위를 초 단위로 표시합니다.
Session Status(세션 상태**)**	엔드포인트 디바이스의 현재 상태를 표시합니다.
Action(CoA 작업**)**	**Actions(**작업**)** 아이콘을 클릭하여 활성 RADIUS 세션을 다시 인증하거나 활성 RADIUS 세션의 연결을 끊습니다.
Repeat Count(반복 횟수**)**	사용자 또는 엔드포인트를 재인증하는 횟수를 표시합니다.
Endpoint ID(엔드포인트 **ID)**	엔드포인트의 고유한 식별자(일반적으로는 MAC 또는 IP 주소)를 표시합니다.

필드 이름	설명
ID	엔드포인트 디바이스의 사용자 이름을 표시합니다.
IP Address(IP 주소**)**	엔드포인트 디바이스의 IP 주소를 표시합니다.
Audit Session ID(감사 세션 **ID)**	고유 세션 ID를 표시합니다.
Account Session ID(계정 세션 **ID)**	네트워크 디바이스에서 제공하는 고유 ID를 표시합니다.
Endpoint Profile(엔드포인트 프로파일**)**	디바이스에 대한 엔드포인트 프로파일을 표시합니다.
Posture Status(포스처 상태**)**	포스처 검증의 상태 및 인증에 대한 세부정보를 표시합니다.
Security Group(보안 그룹**)**	인증 로그로 식별된 그룹을 표시합니다.
Server(서버**)**	로그가 생성된 정책 서비스 노드를 나타냅니다.
Auth Method(인증 방법**)**	PAP(Password Authentication Protocol), CHAP(Challenge Handshake Authentication Protocol), IEE 802.1x 또는 dot1x 등과 같이 RADIUS 프로토콜에서 사용하는 인증 방법을 표시합니다.
Authentication Protocol(인증 프로토콜**)**	PEAP(Protected Extensible Authentication Protocol), EAP(Extensible Authentication Protocol) 등 사용되는 인증 프로토콜을 표시합니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.
권한 부여 정책	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.
Authorization Profiles(권한 부여 프로파일**)**	인증에 사용된 권한 부여 프로파일을 표시합니다.
NAS IP Address(NAS IP 주소**)**	네트워크 디바이스의 IP 주소를 표시합니다.
Device Port(디바이스 포트**)**	네트워크 디바이스에 연결된 포트를 표시합니다.
PRA Action(PRA 작업**)**	네트워크에서 클라이언트가 규정 준수를 위해 올바르게 포스처된 후 클라이언트에 대해 수행되는 정기적 재평가 작업을 표시합니다.
ANC Status(ANC 상태**)**	디바이스의 적응형 네트워크 제어 상태를 Quarantine(격리), Unquarantine(격리 해제) 또는 Shutdown(종료)으로 표시합니다.

필드 이름	설명
WLC Roam(WLC 로밍**)**	로밍 중에 엔드포인트가 WLC 간에 전달되었음을 추적하는 데 사용되는 부울(Y/N)을 표시합니다. cisco-av-pair=nas-update의 값은 Y 또는 N입니다. 참고 Cisco ISE는 WLC의 nas-update=true 속성을 사용하여 세션이 로밍 상태인지 여부를 식별합니다. 원래 WLC가 nas-update=true인 계정 관리 중지 속성을 전송하는 경우 재인증을 방지하기 위해 ISE에서 세션이 삭제되지 않습니다. 로밍이 실패하는 경우 ISE는 5일 동안 활동이 없으면 세션을 지웁니다.
Packets In(수신 패킷**)**	수신된 패킷 수를 표시합니다.
Packets Out(전송 패킷**)**	전송된 패킷 수를 표시합니다.
Bytes In(수신 바이트**)**	수신된 바이트 수를 표시합니다.
Bytes Out(전송 바이트**)**	전송된 바이트 수를 표시합니다.
Session Source(세션 소스**)**	RADIUS 세션인지 아니면 패시브 ID 세션인지를 나타냅니다.
User Domain Name(사용자 도메인 이름**)**	사용자의 등록된 DNS 이름을 표시합니다.
Host Domain Name(호스트 도메인 이름**)**	호스트의 등록된 DNS 이름을 표시합니다.
User NetBIOS Name(사용자 **NetBIOS** 이름**)**	사용자의 NetBIOS 이름을 표시합니다.
Host NetBIOS Name(호스트 **NetBIOS** 이름**)**	호스트의 NetBIOS 이름을 표시합니다.
라이선스 유형	사용하는 라이선스 유형을 표시합니다.
라이선스 세부정보	라이선스 세부정보를 표시합니다.

필드 이름	설명
Provider(사업자**)**	엔드포인트 이벤트는 다양한 시스템 로그 소스에서 학습됩니다. 이러한 시스템 로그 소스를 제공자라고 합니다. • WMI(Windows Management Instrumentation)—WMI는 운영체제, 장치, 애플리케이션 및 서비스 관련 관리 정보에 액세스하기 위한 공통 인터페이스와 개체 모델을 제공하는 Windows 서비스입니다. • 에이전트: 클라이언트나 다른 프로그램을 대신하여 클라이언트에서 실행되는 프로그램입니다. • 시스템 로그: 클라이언트가 메시지를 전송하는 로깅 서버입니다. • REST: 클라이언트가 터미널 서버를 통해 인증됩니다. 이 시스템 로그 소스에 대한 TS Agent ID(TS 에이전트 ID), Source Port Start(소스 포트 시작), Source Port End(소스 포트 끝), Source First Port(소스 최초 포트) 값이 표시됩니다. • Span: 네트워크 정보가 span 프로브를 사용해 검색됩니다. • DHCP: DHCP 이벤트입니다. • 엔드포인트 참고 엔드포인트 세션에서 서로 다른 제공자에서 발생한 두 이벤트를 파악하면, 제공자는 라이브 세션 페이지에 쉼표로 구분된 값으로 표시됩니다.
MAC 주소**(MAC Address)**	클라이언트의 MAC 주소를 표시합니다.
엔드포인트 확인 시간	엔드포인트 프로브가 엔드포인트를 마지막으로 확인한 시간을 표시합니다.

필드 이름	설명
Endpoint Check Result(엔드포인트 확인 결과**)**	엔드포인트 프로브의 결과를 표시합니다. 가능한 값은 다음과 같습니다. • 연결 불가 • 사용자 로그아웃 • 활성 사용자
Source Port Start(소스 포트 시작**)**	(값은 REST 제공자에 대해서만 표시됨) 포트 범위의 첫 번째 포트 번호를 표시합니다.
Source Port End(소스 포트 종료**)**	(값은 REST 제공자에 대해서만 표시됨) 포트 범위의 마지막 포트 번호를 표시합니다.
Source First Port(소스 첫 번째 포트**)**	(값은 REST 제공자에 대해서만 표시됨) 터미널 서버 에이전트가 할당한 첫 번째 포트를 표시합니다. 터미널 서버는 모뎀이나 네트워크 인터페이스 없이도 여러 엔드포인트가 연결될 수 있고 여러 엔드포인트와 LAN 네트워크 간의 연결을 촉진하는 서버 또는 네트워크 디바이스를 말합니다. 여러 엔드포인트가 같은 IP 주소를 이용하는 것처럼 보이기 때문에 특정 사용자의 IP 주소를 식별하기가 어렵습니다. 따라서 특정 사용자를 식별하기 위해 각 사용자에 포트 범위를 할당하는 터미널 서버 에이전트가 서버에 설치됩니다. 이렇게 하면 IP 주소-포트-사용자 매핑을 만들 수 있습니다.
TS 에이전트 **ID**	(값은 REST 제공자에 대해서만 표시됨) 엔드포인트에 설치된 터미널 서버 에이전트의 고유 ID를 표시합니다.
AD User Resolved Identities(AD 사용자가 확인한 **ID)**	(값은 AD 사용자에 대해서만 표시됨) 일치하는 잠재적 계정을 표시합니다.
AD User Resolved DNs(AD 사용자가 확인한 **DN)**	(값은 AD 사용자에 대해서만 폿시됨) AD 사용자의 Distinguished Name(고유 이름) 을 표시합니다(예: CN=chris,CN=Users,DC=R1,DC=com).

TACACS 라이브 로그

다음 표에서는 TACACS+ AAA 세부정보가 표시되는 TACACS Live Logs(TACACS 라이브 로그) 페이지의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**입니다. 기본 PAN에서만 TACACS 라이브 로그를 볼 수 있습니다.

표 ***42: TACACS*** 라이브 로그

필드 이름	사용 지침
생성 시간	특정 이벤트가 트리거된 시간을 기준으로 시스템 로그 생성 시간을 표시합니다.
Logged Time(기록된 시간**)**	모니터링 노드에서 시스템 로그를 처리하고 저장한 시간을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Status(상태**)**	인증 성공 여부를 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다. 인증이 통과한 경우 녹색으로 표시되고, 인증이 실패한 경우 빨간색으로 표시됩니다.
Details(세부정보**)**	돋보기를 클릭하면 표시되는 보고서를 드릴다운하여 선택한 인증 시나리오에 대한 추가 세부정보를 확인할 수 있습니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Session Key(세션 키**)**	ISE가 네트워크 디바이스에 반환하는 세션 키(EAP 성공 또는 EAP 장애 메시지에서 확인 가능)를 표시합니다.
Username(사용자 이름**)**	디바이스 관리자의 사용자 이름을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Type(유형**)**	두 가지 유형인 Authentication(인증)과 Authorization(권한 부여)으로 구성됩니다. 인증, 권한 부여 또는 둘 다에서 통과했거나 장애가 발생한 사용자 이름을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.
권한 부여 정책	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.

필드 이름	사용 지침
ISE Node(ISE 노드**)**	액세스 요청이 처리되는 ISE 노드의 이름을 표시합니다.
Network Device Name(네트워크 디바이스 이름**)**	네트워크 디바이스의 이름을 표시합니다.
Network Device IP(네트워크 디바이스 **IP)**	액세스 요청이 처리되는 네트워크 디바이스의 IP 주소를 표시합니다.
네트워크 디바이스 그룹	네트워크 디바이스가 속한 해당 네트워크 디바이스 그룹의 이름을 표시합니다.
디바이스 유형	다른 네트워크 디바이스의 액세스 요청을 처리하는 데 사용되는 디바이스 유형 정책을 표시합니다.
Location(위치**)**	네트워크 디바이스의 액세스 요청을 처리하는 데 사용되는 위치 기반 정책을 표시합니다.
Device Port(디바이스 포트**)**	액세스 요청을 수행하는 디바이스 포트 번호를 표시합니다.
Failure Reason(실패 이유**)**	네트워크 디바이스에서 수행한 액세스 요청을 거부하는 이유를 표시합니다.
Remote Address(원격 주소**)**	최종 무선국을 고유하게 식별하는 IP 주소, MAC 주소 또는 기타 문자열을 표시합니다.
Matched Command Set(일치하는 명령 집합**)**	MatchedCommandSet 속성 값이 있으면 표시하고, MatchedCommandSet 속성 값이 비어 있거나 속성 자체가 시스템 로그에 없으면 빈 값을 표시합니다.
Shell Profile(셸 프로파일**)**	네트워크 디바이스에서 명령을 실행하기 위해 디바이스 관리자에게 부여된 권한을 표시합니다.

TACACS Live Logs(TACACS 라이브 로그) 페이지에서는 다음을 수행할 수 있습니다.

- 데이터를 csv 또는 pdf 형식으로 내보냅니다.
- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 맞춤형 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.
- 열 값을 정렬합니다.

참고 모든 사용자 맞춤 설정은 사용자 기본 설정으로 저장됩니다.

요약 내보내기

지난 7일 동안 모든 사용자가 내보낸 보고서의 세부정보를 상태와 함께 볼 수 있습니다. 내보내기 요약에는 수동 보고서와 예약 보고서가 모두 포함됩니다. 내보내기 요약 페이지는 2분마다 자동으로 새로 고쳐집니다. 내보내기 요약 페이지를 수동으로 새로 고치려면 새로 고침 아이콘을 클릭하십시오.

슈퍼 관리자는 진행 중이거나 대기열에 있는 내보내기를 취소할 수 있습니다. 다른 사용자는 본인이 시작한 내보내기 프로세스만 취소할 수 있습니다.

기본적으로는 특정 시점에 보고서를 3번만 수동으로 내보낼 수 있으며, 수동으로 트리거된 나머지 보고서는 대기열에 추가됩니다. 예약된 보고서 내보내기에는 이러한 제한이 없습니다.

참고 대기열에 있는 모든 보고서가 다시 예약되며, 진행 중이거나 취소 중인 상태의 보고서는 Cisco ISE 서버가 재시작되면 실패로 표시됩니다.

참고 기본 MnT 노드가 다운되면 예약된 보고서 내보내기 작업이 보조 MnT 노드에서 실행됩니다.

다음 표에서는 Export Summary(요약 내보내기) 페이지의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(운영)** > **Reports(보고서)** > **Export Summary(요약 내보내기)**입니다.

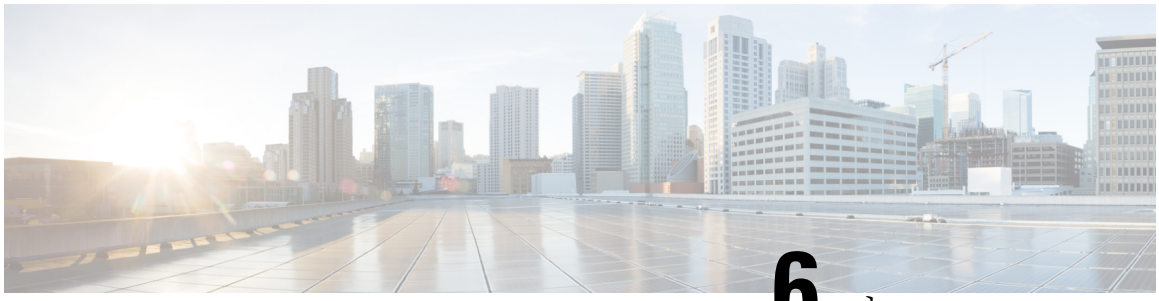
표 ***43:*** 요약 내보내기

필드 이름	설명
Report Exported(내보낸 보고서)	보고서의 이름을 표시합니다.
Exported By(내보낸 사람)	내보내기 프로세스를 시작한 사용자의 역할을 표시합니다.
Scheduled(예약됨)	보고서 내보내기가 예약된 내보내기인지 표시합니다.
Triggered On(트리거됨)	내보내기 프로세스가 시스템에서 트리거된 시간을 표시합니다.
Repository(저장소)	내보낸 데이터를 저장할 저장소 이름을 표시합니다.

필드 이름	설명
Filter Parameters(필터 파라미터**)**	보고서를 내보내는 동안 선택한 필터 파라미터를 표시합니다.
Status(상태**)**	내보낸 보고서의 상태를 표시합니다. 다음 중 하나일 수 있습니다. • 대기열에 있음 • 진행 중 • 완료됨 • 취소 중 • 취소됨 • 실패 • 건너뜀 참고 실패 상태에는 실패 이유가 표시됩니다. 건너뜀 상태는 기본 MnT 노드가 다운되어 예약된 보고서 내보내기를 건너뛰었음을 나타냅니다.

Export Summary(내보내기 요약) 페이지에서 다음을 수행할 수 있습니다.

- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 맞춤형 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.



6 장

디바이스 관리

TACACS+ 디바이스 관리

Cisco ISE는 네트워크 디바이스의 컨피그레이션을 제어하고 감사하기 위해 TACACS+(Terminal Access Controller Access-Control System) 보안 프로토콜을 사용하는 디바이스 관리를 지원합니다. 네트워크 디바이스는 디바이스 관리자 작업 인증 및 권한 부여를 Cisco ISE에 쿼리하고, 해당 작업을 기록하기 위해 Cisco ISE에 대한 계정 관리 메시지를 전송하도록 구성됩니다. 따라서 어떤 사용자가 어떤 네트워크 디바이스에 액세스하고 관련 네트워크 설정을 변경할 수 있는지를 세분화된 방식으로 제어할 수 있습니다. Cisco ISE 관리자는 디바이스 관리 액세스 서비스의 권한 부여 정책 규칙에서 명령 집합 및 쉘(shell) 프로파일과 같은 TACACS 결과를 선택하도록 허용하는 정책 집합을 생성할 수 있습니다. Cisco ISE 모니터링 노드는 디바이스 관리와 관련이 있는 향상된 보고서를 제공합니다. 작업 센터 메뉴에는 ISE 관리자에게 단일 시작점으로 작동하는 모든 디바이스 관리 페이지가 포함되어 있습니다.

Cisco ISE에서 TACACS+를 사용하려면 디바이스 관리 라이선스가 필요합니다.

디바이스 관리를 수행하는 관리자에는 다음 두 가지 유형이 있습니다.

- 디바이스 관리자
- Cisco ISE 관리자

디바이스 관리자는 스위치, 무선 액세스 포인트, 라우터, 게이트웨이와 같은 네트워크 디바이스에 로그인하여(일반적으로 SSH 사용) 관리 중인 디바이스의 구성 및 유지 관리를 수행하는 사용자입니다. Cisco ISE 관리자는 Cisco ISE에 로그인하여 디바이스 관리자가 로그인하는 디바이스를 구성하고 조정합니다.

Cisco ISE 관리자는 이 문서의 대상으로, 디바이스 관리자의 작업을 제어하는 설정을 구성하기 위해 Cisco ISE에 로그인합니다. Cisco ISE 관리자는 디바이스 관리 기능(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > Device Administration(**디바이스 관리**)**)을 사용하여 네트워크 디바이스의 구성을 제어 및 감사합니다. 디바이스는 TACACS(Terminal Access Controller Access-Control System) 보안 프로토콜을 사용하여 Cisco ISE 서버에 쿼리하도록 구성할 수 있습니다. Cisco ISE 모니터링 노드는 디바이스 관리와 관련이 있는 향상된 보고서를 제공합니다. Cisco ISE 관리자는 다음 작업을 수행할 수 있습니다.

- TACACS+ 세부정보(공유 암호)로 네트워크 디바이스를 구성합니다.
- 디바이스 관리자를 내부 사용자로 추가하고 필요에 따라 활성화 비밀번호를 설정합니다.
- 디바이스 관리 액세스 서비스의 권한 부여 정책 규칙에서 명령 집합 및 쉘(shell) 프로파일과 같은 TACACS 결과를 선택하도록 허용하는 정책 집합을 생성합니다.
- 디바이스 관리자가 정책 집합에 따라 디바이스에 액세스할 수 있도록 Cisco ISE에서 TACACS 서버를 구성합니다.

디바이스 관리자는 Cisco ISE 서버와 통신하도록 디바이스를 설정하는 작업을 수행합니다. 디바이스 관리자가 디바이스에 로그온하면 디바이스는 Cisco ISE 서버에 쿼리합니다. 그러면 Cisco ISE 서버가 내부 또는 외부 ID 저장소에 쿼리하여 디바이스 관리자의 세부정보를 검증합니다. Cisco ISE 서버에서 검증이 수행되면 디바이스는 Cisco ISE 서버에 계정 관리 및 감사를 위해 각 세션 또는 명령 권한 부여 작업의 최종 결과를 알립니다.

Cisco ISE 관리자는 TACACS 및 Cisco ISE 2.0 이상 릴리스를 사용하여 디바이스 관리를 수행할 수 있습니다. 디바이스 관리와 관련된 구성을 Cisco Secure Access Control System(ACS) 서버 5.5, 5.6, 5.7 및 5.8 버전에서 마이그레이션할 수도 있습니다. 마이그레이션 전에 이전 버전을 5.5 또는 5.6으로 업그레이드해야 합니다.

참고

TACACS+ 작업을 활성화하려면 **Administration(**관리**) > System(**시스템**) > Deployment(**구축**) > General Settings(**일반 설정**)** 페이지에서 **Enable Device Admin Service(**디바이스 관리 서비스 활성화**)** 확인란을 선택해야 합니다. 구축의 각 PSN에서 이 옵션이 활성화되어 있는지 확인합니다.

TACACS+ 프로토콜은 스위치 또는 라우터와 Cisco ISE 간의 보안 연결을 생성하는 데 알려진 제한이 있으므로 양측 간에 IPsec 프로토콜이 구축되었는지 확인하십시오.

ISE 커뮤니티 리소스

디바이스 관리 속성에 대한 자세한 내용은 ISE Device Administration Attributes를 참고하십시오.

무선 LAN 컨트롤러, IOS 네트워크 디바이스, Cisco NX-OS 네트워크 디바이스 및 네트워크 디바이스의 TACACS+ 구성에 대한 자세한 내용은 ISE Device Administration(TACACS+)을 참고하십시오.

디바이스 관리 작업 센터

작업 센터 메뉴에는 Cisco ISE 관리자에게 단일 시작점으로 작동하는 모든 디바이스 관리 페이지가 포함되어 있습니다. 그러나 Users(사용자), User Identity Groups(사용자 ID 그룹), Network Devices(네트워크 디바이스), Default Network Devices(기본 네트워크 디바이스), Network Device Groups(네트워크 디바이스 그룹), Authentication and Authorization Conditions(인증 및 권한 부여 조건) 등 디바이스 관리 조건이 없는 페이지는 다른 메뉴 옵션, 예를 들면 Administration(관리)에서도 액세스할 수 있습니다. Work Centers(작업 센터) 옵션은 올바른 TACACS+ 라이선스를 얻어 설치한 경우에만 사용할 수 있습니다.

Device Administration(디바이스 관리) 메뉴에는 Overview(개요), Identities(ID), User Identity Groups(사용자 ID 그룹), Ext ID Stores(Ext ID 저장소), Network Resources(네트워크 리소스 그룹), Policy Elements(정책 요소), Device Admin Policy Sets(디바이스 관리 정책 집합), Reports(보고서) 및 Settings(설정) 메뉴 옵션이 포함되어 있습니다.

디바이스 관리 구축 설정

Device Administration Deployment(디바이스 관리 구축 페이지)(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Overview(**개요**)** > **Deployment(**구축**)**)에서 Cisco ISE 관리자가 구축 섹션의 각 노드를 참조하지 않고 디바이스 관리 시스템을 중앙에서 볼 수 있습니다.

Device Administration Deployment(디바이스 관리 구축) 페이지에는 구축의 PSN이 나열됩니다. 이렇게 하면 구축의 각 PSN에서 개별적으로 디바이스 관리 서비스를 활성화하는 작업이 간소화됩니다. 아래의 옵션을 선택하여 여러 PSN에 대해 디바이스 관리 서비스를 한꺼번에 활성화할 수 있습니다.

옵션	설명
없음	기본적으로 디바이스 관리 서비스는 모든 노드에 대해 비활성화되어 있습니다.
모든 정책 서비스 노드	모든 PSN에서 디바이스 관리 서비스를 활성화합니다. 이 옵션을 사용하면 새 PSN이 추가될 때 디바이스 관리자에 대해 자동으로 활성화됩니다.
특정 노드	구축의 모든 PSN을 나열하는 ISE 노드 섹션을 표시합니다. 디바이스 관리 서비스를 활성화해야 하는 필수 노드를 선택할 수 있습니다.

참고 구축에 TACACS+용 라이선스가 없으면 위의 옵션은 비활성화됩니다.

TACACS Ports(TACACS 포트) 필드에서는 최대 4개의 TCP 포트를 쉼표로 구분하여 입력 할 수 있으며 포트 값 범위는 1 ~ 65535입니다. Cisco ISE 노드 및 해당 인터페이스는 지정된 포트에서 TACACS+

요청을 수신하며, 지정된 포트가 다른 서비스에서 사용되지 않도록해야 합니다. 기본 TACACS+ 포트값은 49입니다.

Save(저장**)**를 클릭하면 **Administration(**관리**)** > **System(**시스템**)** > **Deployment Listing(**구축 목록**)**창에 지정된 노드와 변경 사항이 동기화됩니다.

디바이스 관리 정책 집합

Device Admin Policy Sets(디바이스 관리 정책 집합) 창에는(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)> Device Administration(**디바이스 관리**) > Device Admin Policy Sets(**디바이스 관리 정책 집합**))**에는 Cisco ISE 관리자가 TACACS+ 디바이스 관리자의 인증 및 권한 부여를 제어하기 위해 관리하는 정책 집합 목록이 포함되어 있습니다. 각 정책은 일반 및 프록시 시퀀스의 두 가지 모드 중 하나일 수 있습니다.

일반 정책 집합은 인증 규칙 표과 권한 부여 규칙 표로 구성됩니다. 인증 규칙 표에는 네트워크 디바이스를 인증하는 데 필요한 작업을 선택하기 위한 규칙 집합이 포함되어 있습니다.

권한 부여 규칙 표에는 권한 부여 비즈니스 모델을 구현하는 데 필요한 특정 권한 부여 결과를 선택하는 규칙 집합이 포함되어 있습니다. 각 권한 부여 규칙은 참여할 규칙에 대해 일치해야 하는 하나 이상의 조건, 권한 부여 프로세스를 제어하기 위해 선택된 명령 집합 및/또는 셸 프로파일로 구성됩니다. 각 규칙 표은 특정 상황에서 규칙을 재정의하는 데 사용할 수 있는 예외 정책이 있으며, 종종 예외 표이 임시 상황에 사용됩니다.

참고 TACACS+ CHAP 아웃 바운드 인증은 지원되지 않습니다.

프록시 시퀀스 정책 집합에는 선택한 단일 프록시 시퀀스가 포함되어 있습니다. 정책 집합이 이 모드에 있으면 요청을 처리하는 데 하나 이상의 원격 프록시 서버가 사용됩니다(프록시 시퀀스에서 로컬 어카운팅을 구성할 수는 있음).

디바이스 관리 정책 집합 생성

디바이스 관리 정책 집합을 생성하려면 다음 단계를 수행합니다.

시작하기 전에

- TACACS + 작업에 대해 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Overview(**개요**)** > **Deployment(**구축**)** 창의 디바이스 관리가 활성화되어 있는지 확인합니다.
- 정책에 필요한 모든 사용자 ID 그룹(예: System_Admin, Helpdesk)이 생성되었는지 확인합니다. (Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **User Identity Groups(**사용자 **ID** 그룹**)** 페이지). 멤버 사용자(예: ABC, XYZ)가 해당 그룹에 할당되었는지 확인합니다. (Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Identities(ID)** > **Users(**사용자**)**창).

- 관리해야 하는 디바이스에서 TACACS 설정을 구성해야 합니다. (Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Add(**추가**)** > **TACACS Authentication Settings(TACACS+** 인증 설정**)** 확인란이 활성화되고 TACACS 및 디바이스의 공유 암호가 동일하여 디바이스가 Cisco ISE를 쿼리하도록 지원합니다.)
- 디바이스 유형 및 위치를 기반으로 네트워크 디바이스 그룹이 생성되었는지 확인합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Device Groups(**네트워크 디바이스 그룹**)** 창)

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리자 정책 집합**)**.

단계 **2** 아무 행의 **Actions(**작업**)** 열에서 톱니바퀴 아이콘을 클릭한 다음 드롭다운 메뉴에서 필요에 따라 삽입 또는 복제 옵션을 선택하여 새 정책 집합을 삽입합니다.
정책 집합 표에 새 행이 표시됩니다.

단계 **3** 정책 집합의 이름과 설명을 입력합니다.

단계 **4** 필요한 경우 Allowed Protocols/Server Sequence(허용되는 프로토콜/서버 시퀀스) 열에서 (+) 기호를 클릭하고 다음 중 하나를 선택합니다.

a) 새 허용되는 프로토콜 생성
b) TACACS 서버 시퀀스 생성

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

단계 **6** **Conditions Studio** 페이지에 필수 조건을 생성합니다. **Editor(**편집기**)** 섹션에서 **Click To Add an Attribute(**클릭해서 속성 추가**)** 텍스트 상자를 클릭하고 필수 사전 및 속성(예: Device-Location Equals Europe)을 선택합니다.

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

단계 **7** **Use**를 클릭합니다.

단계 **8** View(보기) 열에서 › 표시를 클릭하여 모든 정책 집합 세부정보에 액세스하고 인증 및 권한 부여 정책과 정책 예외를 생성합니다.

단계 **9** 필요 인증 정책을 생성합니다(예: Rule Name: ATN_Internal_Users, Conditions: DEVICE:Location EQUALS Location #All Locations#Europe—정책이 유럽 위치에 존재하는 디바이스에만 일치됨).

단계 **10** **Save(**저장**)**를 클릭합니다.

단계 **11** 필수 권한 부여 정책을 만듭니다.

예 1: 규칙 이름: Sys_Admin_rule, 조건: if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8—이 정책은 시스템 관리자를 사용자 이름 ABC와 일치시키고 지정된 명령을 실행하며 권한 레벨 8을 할당합니다.

예 2: 규칙 이름: HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1—이 정책은 시스템 관리자와 사용자 이름 XYZ를 매칭하고 지정된 명령을 실행하도록 허용하며 권한 레벨 1을 할당합니다.

위의 예에서

- 명령 집합 cmd_Sys_Admin 및 cmd_HDesk는 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **TACACS Command Sets(TACACS** 명령 집합**)** > **Add(**추가**)** 창에 생성됩니다.
- TACACS 프로파일 Profile_Priv_1 및 Profile_priv_8은 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **TACACS Command Sets(TACACS** 명령 집합**)** > **Add(**추가**)** 창에 생성됩니다.

참고 인증 및 권한 부여 정책에 사용되는 조건에서 디바이스 IP 주소 속성에 대해 IPv4 또는 IPv6 단일 주소를 추가할 수 있습니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

TACACS+ 인증 설정 및 공유 암호

다음 표에서는 네트워크 디바이스에 대한 TACACS+ 인증 설정을 구성하는 데 사용할 수 있는 Network Devices(네트워크 디바이스) 창의 필드를 설명합니다. 탐색 경로는 다음과 같습니다.

- (네트워크 디바이스의 경우) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Add(**추가**)** > **TACACS Authentication Settings(TACACS** 인증 설정**)**입니다.
- (기본 디바이스의 경우) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Default Devices(**기본 디바이스**)** > **TACACS Authentication Settings(TACACS** 인증 설정**)**입니다. 자세한 내용은 의 "Cisco ISE의 기본 네트워크 디바이스 정의"를 참조하십시오.

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. 이것은 필수 항목이 아닙니다.
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**)**	(위의 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **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 선택합니다. 다음 중 하나를 선택합니다. • 레거시 Cisco 디바이스 • 또는 TACACS+ 초안 규정 준수 단일 연결 지원. Single Connect Mode(단일 연결 모드)를 비활성화하면 ISE는 모든 TACACS+ 요청에 대해 새 TCP 연결을 사용합니다.

요약하면,

- 사용 종료 기간을 일수(범위: 1 ~ 99)로 지정하여 이전 공유 암호를 사용 종료하고 동시에 새 공유 암호를 설정합니다.
- 사용 종료 기간에는 이전 및 새 공유 암호를 사용합니다.
- 만료 기간이 만료되기 전에 이를 연장합니다.
- 이전 공유 암호는 사용 종료 기간이 끝날 때까지만 사용합니다.
- 만료되기 전에 사용 종료 기간을 종료합니다(End(종료)를 클릭한 다음 Submit(제출)을 클릭).

참고 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 창에서 TACACS+ 인증 설정 옵션에 액세스할 수 있습니다.

디바이스 관리-권한 부여 정책 결과

Cisco ISE 관리자는 TACACS+ 명령 집합 및 TACACS+ 프로파일(정책 결과)을 사용하여 디바이스 관리자에게 부여되는 권한 및 명령을 제어할 수 있습니다. 이 정책은 네트워크 디바이스와 함께 동작하므로 네트워크 디바이스에 대한 우발적 혹은 의도적인 구성 변경을 방지합니다. 만약 이런 상황이 발생한 경우, 디바이스 관리 감사 보고서를 사용하여 특정 명령이 실행된 네트워크 디바이스의 관리자가 누구인지를 확인할 수 있습니다.

TACACS + 디바이스 관리를 위해 **FIPS** 및 비 **FIPS** 모드에서 허용되는 프로토콜

Cisco ISE가 정책 결과를 생성하기 위해 제공하는 여러 허용되는 인증 프로토콜 서비스가 있습니다. 그러나 TACACS + 프로토콜에 적용할 수 있는 PAP/ASCII, CHAP 및 MS-CHAPv1과 같은 인증 프로토콜 서비스는 RADIUS용 FIPS 지원 Cisco ISE 어플라이언스에서 비활성화됩니다. 따라서 FIPS 지원 (**Administration(**관리**)** > **System Settings(**시스템 설정**)** > **FIPS Mode(FIPS** 모드**)**) Cisco ISE 어플라이언스를 사용하는 경우 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Allowed Protocols(**허용된 프로토콜**)** 창에서 프로토콜을 활성화하여 디바이스를 관리할 수 없습니다.

결과적으로 FIPS 및 비 FIPS 모드 모두에 대해 디바이스 관리 정책 결과에 PAP/ASCAP, CHAP 및 MS-CHAPv1 프로토콜을 구성하려면 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Allowed Protocols(**허용된 프로토콜**)** 창으로 이동해야 합니다. FIPS 모드가 활성화된 경우 기본 디바이스 관리자가 허용하는 프로토콜 설정만 사용할 수 있습니다. 이 옵션은 RADIUS에서 허용되지 않습니다.

TACACS+ 명령 집합

명령 집합은 디바이스 관리자가 실행할 수 있는 지정된 명령 목록을 적용합니다. 디바이스 관리자가 네트워크 디바이스에서 작동 명령을 실행하면 관리자가 이러한 명령을 실행할 권한이 있는지를 확인하기 위해 Cisco ISE가 쿼리됩니다. 이를 명령 권한 부여라고도 합니다.

명령 집합의 와일드카드 및 **Regex**

명령줄은 명령과 0개 이상의 인수로 구성됩니다. Cisco ISE는 명령줄(요청)을 수신하면 명령과 해당 인수를 다양한 방식으로 처리합니다.

- 이 명령은 와일드카드 일치 패러다임을 사용하여 명령 집합 목록에 지정된 명령과 요청의 명령을 일치시킵니다.

  예: Sh?? 또는 S*

- 정규식(regex) 일치 패러다임을 사용하여 요청의 인수를 명령 집합 목록에 지정된 인수와 일치시킵니다.

  예: Show interface[1-4] port[1-9]:tty*

명령 줄 및 명령 집합 목록 일치

요청된 명령 줄을 와일드카드 및 regex를 포함하는 명령 집합 목록에 일치시키려면 다음을 따릅니다.

1. 명령 집합 목록을 반복하여 일치하는 명령을 탐지합니다.

   와일드카드 일치는 다음을 허용합니다.

   - 대소문자 구분 안 함
   - 명령 집합에 있는 명령의 모든 문자는 "?"일 수 있으며, 이는 요청된 명령에 있어야 하는 모든 개별 문자와 일치함
   - 명령 집합에 있는 명령의 모든 문자는 "*"일 수 있으며, 이는 요청된 명령에 있는 0개 이상의 문자와 일치함

     예:

요청	명령 집합	일치	코멘트
show	show	예	—
show	표시	예	대소문자 구분 안 함
show	Sh??	예	모든 문자와 일치
show	Sho??	N	두 번째 "?" 존재하지 않는 문자와 교차
show	S*	예	"*" 문자는 모든 문자와 일치
show	S*w	예	"*"는 "ho" 문자와 일치
show	S*p	N	문자 "p"는 일치하지 않음

2. Cisco ISE는 일치하는 각 명령에 대해 인수를 검증합니다.

   명령 집합 목록에는 각 명령에 대해 공백으로 구분된 인수 집합이 포함됩니다.

   예: Show interface[1-4] port[1-9]:tty.*

   이 명령에는 두 개의 인수가 있습니다.

   1. 인수 1: interface[1-4]

   2. 인수 2: port[1-9]:tty. *

   이 요청의 명령 인수는 패킷에 나타나는 위치 중요 순서로 가져옵니다. 명령 정의의 모든 인수가 요청의 인수와 일치할 때 이 명령/인수가 일치한다고 합니다. 참고로 요청에서 관련 없는 인수는 모두 무시됩니다.

참고 표준 Unix 정규식을 인수에 사용합니다.

복수 명령 집합 처리 규칙

1. 명령 집합에 명령 및 해당 인수에 대한 일치가 포함되어 있고 일치에 Deny Always(항상 거부)가 있는 경우 Cisco ISE는 해당 명령 집합을 Commandset-DenyAlways로 지정합니다.
2. 명령 집합의 명령 일치에 Deny Always(항상 거부)가 없으면 Cisco ISE는 첫 번째 일치 항목에 대해 명령 집합의 모든 명령을 순차적으로 확인합니다.
    1. 첫 번째 일치 항목이 Permit(허용)인 경우 Cisco ISE는 명령 집합을 Commandset-Permit으로 지정합니다.
    2. 첫 번째 일치 항목이 Deny(거부)인 경우 Cisco ISE는 명령 집합을 Commandset-Deny로 지정합니다.
3. Cisco ISE는 모든 명령 집합을 분석한 후 다음 명령을 승인합니다.
    1. Cisco ISE가 Commandset-DenyAlways로 설정된 명령을 지정한 경우 Cisco ISE는 해당 명령을 거부합니다.
    2. Commandset-DenyAlways가 없는 경우 명령 집합이 Commandset-Permit이면 Cisco ISE는 해당 명령을 허용하고, 그렇지 않으면 Cisco ISE에서 명령을 거부합니다. 단, **Unmatched(**일치하지 않음**)** 확인란이 선택된 경우는 예외입니다.

TACACS+ 명령 집합 생성

TACACS + 명령 집합 정책 결과를 사용하여 정책 집합을 생성하려면,

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **TACACS Command Sets(TACACS** 명령 집합**)**

TACACS 명령 집합을 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리 정책 집합**)** 페이지에서도 구성할 수 있습니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 이름과 설명을 입력합니다.

단계 **4** 부여 권한, 명령 및 인수를 지정하려면 **Add(**추가**)**를 클릭합니다.

단계 **5** **Grant(**부여**)** 드롭다운 목록에서 다음을 선택합니다.

- **Permit(**허용**)**: 지정된 명령을 허용합니다(예: permit show, permit con * Argument terminal).
- **Deny(**거부**)**: 지정된 명령을 거부합니다(예: deny mtrace).
- **Deny Always(**항상 거부**)**: 다른 명령 집합에서 허용된 명령을 재정의합니다(예: clear auditlogs).

참고 작업 아이콘을 클릭하여 권한 부여, 명령 및 인수 필드의 열 너비를 늘리거나 줄입니다.

단계 **6** **Permit any command that is not listed below(**아래에 나열되지 않은 명령 허용**)** 확인란을 선택하여 Grant(허용) 열에서 Permit(허용), Deny(거부) 또는 Deny Always(항상 거부)로 지정되지 않은 명령 및 인수를 허용합니다.

TACACS+ 프로파일

TACACS+ 프로파일은 디바이스 관리자의 초기 로그인 세션을 제어합니다. 세션은 각 개별 인증, 권한 부여 또는 계정 관리 요청을 나타냅니다. 네트워크 디바이스에 대한 세션 권한 부여 요청은 Cisco ISE 응답을 유발합니다. 응답에는 네트워크 디바이스에서 해석되는 토큰이 포함되며, 이는 세션 기간 동안 실행될 수 있는 명령을 제한합니다. 디바이스 관리 액세스 서비스에 대한 권한 부여 정책은 단일 셸 프로파일 및 여러 명령 집합을 포함할 수 있습니다. TACACS+ 프로파일 정의는 두 가지 구성 요소로 나뉩니다.

- 공통 작업
- 사용자 맞춤화 속성

TACACS+ 프로파일 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **TACACS Profiles(TACACS** 프로파일**)**)에는 작업 속성 보기와 원시 보기의 두 가지 보기가 있습니다. 작업 속성 보기를 사용하여 일반 작업을 입력할 수 있으며, 작업 속성 보기 및 원시 보기에서 사용자 맞춤화 속성을 생성할 수 있습니다.

Common Tasks(일반 작업**)** 섹션에서는 프로파일에 대해 자주 사용되는 속성을 선택하고 구성할 수 있습니다. 여기에 포함된 속성은 TACACS+ 프로토콜 초안 사양에 정의된 속성입니다. 그러나 다른 서비스의 요청을 승인할 때 이 값을 사용할 수 있습니다. 작업 속성 보기에서 Cisco ISE 관리자는 디바이스 관리자에게 할당할 권한을 설정할 수 있습니다. 일반적인 작업 유형은 다음과 같습니다.

- Shell
- WLC
- Nexus
- Generic

Custom Attributes(사용자 맞춤화 속성**)** 섹션에서 추가 속성을 구성할 수 있습니다. 이 섹션은 **Common Tasks(**일반 작업**)** 섹션에서 인식되지 않는 속성 목록을 제공합니다. 각 정의는 속성 이름, 속성이 필수인지 아니면 선택인지에 대한 표시 및 속성의 값으로 구성됩니다.

참고 TACACS 사용 네트워크 디바이스에 대해 총 24개의 작업 속성을 정의 할 수 있습니다. 작업 속성을 24개보다 많이 정의하는 경우 TACACS 지원 네트워크 디바이스로 하나도 전송되지 않습니다.

Raw View(원시 보기**)**에서는 속성 이름과 해당 값 사이에 등호(=) 기호를 사용하여 필수 속성을 입력할 수 있으며, 선택 속성은 속성 이름과 해당 값 사이에 별표(*)를 사용하여 입력합니다. **Raw View(**원

시 보기) 섹션에 입력한 속성은 **Task Attribute View(**작업 속성 보기)의 **Custom Attributes(**사용자 맞춤화 속성) 섹션에 반영되며 그 반대의 경우도 마찬가지입니다. **Raw View(**원시 보기) 섹션은 클립 보드의 속성 목록(예 : 다른 제품의 속성 목록)을 복사하여 Cisco ISE에 붙여 넣는 데에도 사용됩니다. 비-셸 서비스에 대해 사용자 맞춤화 속성을 정의할 수 있습니다.

TACACS+ 프로파일 생성

TACACS+ 프로파일을 생성하려면

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터) > **Device Administration(**디바이스 관리) > **Policy Elements(**정책 요소) > **Results(**결과) > **TACACS Profiles(TACACS** 프로파일).

TACACS 명령 집합을 **Work Centers(**작업 센터) > **Device Administration(**디바이스 관리) > **Device Admin Policy Sets(**디바이스 관리 정책 집합) 페이지에서도 구성할 수 있습니다.

단계 **2** **Add(**추가)를 클릭합니다.

단계 **3** **TACACS Profile(TACACS** 프로파일) 섹션에서 프로파일 이름과 설명을 입력하십시오.

단계 **4** **Task Attribute View(**작업 속성 보기) 탭에서 필요한 **Common Tasks(**일반 작업)를 확인합니다. 일반 작업 설정, 344 페이지 페이지를 참조하십시오.

단계 **5** **Task Attribute View(**작업 속성 보기) 탭의 **Custom Attributes(**사용자 맞춤화 속성) 섹션에서 **Add(**추가)를 클릭하여 필요한 속성을 입력합니다.

일반 작업 설정

일반 작업 설정 창을 보려면 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터) > **Device Administration(**디바이스 관리) > **Policy Elements(**정책 요소) > **Results(**결과) > **TACACS Profiles(TACACS** 프로파일) > **Add(**추가)로 이동합니다. 일반 작업 유형은 셸, WLC, Nexus 및 일반입니다.

Shell

Cisco ISE 관리자가 디바이스 관리자 권한을 설정하는 데 사용할 수 있는 옵션은 다음과 같습니다.

옵션	설명
기본 권한	셸 권한 부여에 대해 디바이스 관리자의 기본(초기) 권한 수준을 활성화합니다. 다음 옵션 중 하나를 선택합니다. • 0~15의 범위 내에서 값을 선택합니다. • 필요한 ID 저장소 속성을 선택합니다.
최대 권한	인증 활성화에 대해 최대 권한 수준을 활성화합니다. 0~15의 범위 내에서 값을 선택할 수 있습니다.

옵션	설명
ACL(Access Control List)	ASCII 문자열(1-251*) 또는 필요한 ID 저장소 속성을 선택합니다.
자동 명령	ASCII 문자열(1-248*) 또는 필요한 ID 저장소 속성을 선택합니다.
이스케이프 없음	이스케이프 문자에 대해 다음 옵션 중 하나를 선택합니다. • True: 이스케이프 방지가 활성화되도록 지정합니다. • False: 이스케이프 방지가 활성화되지 않도록 지정합니다. • 필요한 ID 저장소 속성을 선택합니다.
시간 초과	0~9999의 범위 내에서 값을 선택하거나 필요한 ID 저장소 속성을 선택합니다.
유휴 시간	0~9999의 범위 내에서 값을 선택하거나 필요한 ID 저장소 속성을 선택합니다.

WLC

Cisco ISE 관리자는 다음 옵션을 사용해 WLC 애플리케이션 탭에 대한 디바이스 관리자의 액세스를 제어할 수 있습니다. WLC 애플리케이션에는 WLAN, Controller(컨트롤러), Wireless(무선), Security(보안), Management(관리), Commands(명령) 탭이 포함되어 있습니다.

옵션	설명
All(모두)	디바이스 관리자는 모든 WLC 애플리케이션 탭에 대한 전체 액세스 권한을 갖습니다.
모니터링	디바이스 관리자는 WLC 애플리케이션 탭에 대한 읽기 전용 액세스만 가능합니다.
로비	디바이스 관리자는 제한된 컨피그레이션 권한만 갖습니다.
선택됨	디바이스 관리자는 WLAN, Controller(컨트롤러), Wireless(무선), Security(보안), Management(관리), Commands(명령) 확인란에서 Cisco ISE 관리자가 선택한 대로 탭에 액세스 할 수 있습니다.

Nexus

Cisco ISE 관리자는 다음 옵션을 사용해 Cisco Nexus 스위치에 대한 디바이스 관리자의 액세스를 제어할 수 있습니다.

옵션	설명
다음으로 속성 값 설정	Cisco ISE 관리자는 일반 작업에서 생성된 Nexus 속성을 Optional(선택 사항) 또는 Mandatory(필수)로 지정할 수 있습니다.
네트워크 역할	Nexus가 Cisco ISE를 사용하여 인증하도록 구성된 경우 디바이스 관리자는 기본적으로 읽기 전용 액세스 권한을 갖습니다. 디바이스 관리자는 다음의 역할 중 하나에 할당될 수 있습니다. 각 역할은 허용되는 작업을 정의합니다. • 없음: 권한이 없습니다. • 운영자(읽기 전용): 전체 NX-OS 디바이스에 대해 전체 읽기 액세스가 가능합니다. • 관리자(읽기/쓰기): 전체 NX-OS 디바이스에 대해 전체 읽기 및 쓰기 액세스가 가능합니다.
VDC(Virtual Device Context)	없음: 권한이 없습니다. 운영자(읽기 전용): 읽기 액세스가 VDC로 제한됩니다. 관리자(읽기/쓰기): 읽기 및 쓰기 액세스가 VDC로 제한됩니다.

Generic

Cisco ISE 관리자는이 옵션을 사용하여, 일반 작업에서 사용할 수 없는 맞춤형 속성을 지정할 수 있습니다.

커맨드라인 인터페이스에 액세스하여 활성화 비밀번호 변경

활성화 비밀번호를 변경하려면 다음 단계를 수행하십시오.

시작하기 전에

일부 명령은 권한 모드로 할당됩니다. 따라서 이들 명령은 디바이스 관리자가 이 모드로 인증한 경우에만 실행될 수 있습니다.

디바이스 관리자가 권한 모드를 시작하려고 하면 디바이스에서 특수 활성화 인증 유형을 전송합니다. Cisco ISE는 이 특수 활성화 인증 유형을 검증하기 위해 별도의 활성화 비밀번호를 지원합니다. 별도의 활성화 비밀번호는 디바이스 관리자가 내부 ID 저장소로 인증될 때 사용됩니다. 외부 ID 저장소를 통한 인증의 경우 일반 로그인과 동일한 비밀번호가 사용됩니다.

단계 **1** 스위치에 로그인합니다.

단계 **2** Enter 키를 누르면 다음 프롬프트가 표시됩니다.

```
Switch>
```

단계 **3** 다음 명령을 실행하여 활성화 비밀번호를 설정합니다.

```
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```

참고 로그인 비밀번호 및 활성화 비밀번호에 사용 기간이 설정된 경우, 지정된 기간 내에 비밀번호가 변경되지 않으면 사용자 계정이 비활성화됩니다. Cisco ISE가 TACACS+ 서버로 설정되어 있고 **Enable Bypass(**우회 활성화**)** 옵션이 네트워크 디바이스에 설정된 경우 CLI에서(텔넷을 통해) 활성화 비밀번호를 변경할 수 없습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택해서 활성화 비밀번호를 변경합니다.

전역 **TACACS+** 설정 구성

전역 TACACS + 설정을 구성하려면 다음 단계를 따르십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Settings(**설정**)**를 선택합니다.

Connection Settings(연결 설정**)** 탭에서 필수 필드의 기본값을 변경할 수 있습니다.

- **Authorization cache timeout(**권한 부여 캐시 시간 초과**)** 필드에서 내부 사용자의 특정 속성이 첫 번째 권한 부여 요청 시 캐시되는 TTL(Time-To-Live) 값을 설정할 수 있습니다. 캐시된 속성에는 사용자 이름 및 UserGroup과 같은 사용자별 속성이 포함됩니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **System Administration(**시스템 관리**)** > **Configuration(**컨피그레이션**)** > **Dictionaries(**사전**)** > **Identity(ID)** > **Internal Users(**내부 사용자**)**를 선택하여 속성을 생성합니다. 기본값은 0이며, 이는 권한 부여 캐시가 비활성화되었음을 의미합니다.
- **Single Connect Support(**단일 연결 지원**)**: 단일 연결 모드를 비활성화하면 ISE는 모든 TACACS + 요청에 대해 새 TCP 연결을 사용합니다.

단계 **2** **Password Change Control(**비밀번호 변경 제어**)** 탭에서 TACACS+를 통해 비밀번호 업데이트를 허용할지를 제어하는 데 필요한 필드를 정의합니다.

Enable Telnet Change Password(Telnet 비밀번호 변경 활성화**)** 섹션의 프롬프트는 이 옵션을 선택한 경우에만 활성화됩니다. 아니면 **Disable Telnet Change Password(Telnet** 비밀번호 변경 비활성화**)**에서 프롬프트가 활성화됩니다. 비밀번호 프롬프트는 맞춤 설정이 가능하며 필요에 따라 수정할 수 있습니다.

새 비밀번호가 지정된 기준과 일치하지 않을 경우 **Password Policy Violation Message(**비밀번호 정책 위반 메시지**)** 필드에 내부 사용자가 설정한 비밀번호 관련 적절한 오류 메시지를 표시할 수 있습니다.

단계 **3** **Session Key Assignment(**세션 키 할당**)** 탭에서 TACACS+ 요청을 세션에 연결하는 데 필요한 필드를 선택합니다.

세션 키는 모니터링 노드에서 클라이언트의 AAA 요청을 연결하는 데 사용됩니다. 기본 설정은 NAS-주소, 포트, 원격-주소 및 사용자 필드를 활성화하는 것입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

관련 항목

TACACS+ 인증 설정 및 공유 암호, 338 페이지

Cisco Secure ACS에서 Cisco ISE로의 데이터 마이그레이션

마이그레이션 툴을 사용하여 ACS 5.5 이상에서 데이터를 가져오고, 모든 네트워크 디바이스에 대해 기본 TACACS + 암호를 설정할 수 있습니다. **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Overview(**개요**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Prepare(**준비**)** 섹션에서 소프트웨어 다운로드 웹페이지를 클릭하여 마이그레이션 툴을 다운로드합니다. 툴을 PC에 저장하고 migTool 폴더에서 migration.bat 파일을 실행하여 마이그레이션 프로세스를 시작합니다. 마이그레이션과 관련된 전체 정보는 Cisco ISE 버전에 대한 마이그레이션 가이드를 참조하십시오.

디바이스 관리 활동 모니터링

Cisco ISE는 TACACS+로 구성된 디바이스의 계정 관리, 인증, 권한 부여 및 명령 계정 관리와 관련된 정보를 볼 수 있는 다양한 보고서 및 로그를 제공합니다. 온디맨드 또는 예약 방식으로 이러한 보고서를 실행할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Reports(**보고서**)** > **ISE Reports(ISE** 보고서**)**를 선택합니다. .

다른 위치에서 보고서를 볼 수도 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)**페이지를 클릭하십시오.

단계 **2** **Report Selector(**보고서 선택기**)**에서 **Device Administration(**디바이스 관리**)**을 확장하여 **Authentication Summary(**인증 요약**)**, **TACACS Accounting(TACACS** 계정 관리**)**, **TACACS Authentication(TACACS** 인증**)**, **TACACS Authorization(TACACS** 권한 부여**)** **TACACS Command Accounting(TACACS** 명령 계정 관리**)**, **Top N Authentication by Failure Reason(**실패 이유별 상위 **N** 인증**)**, **Top N Authentication by Network Device(**네트워크 디바이스별 상위 **N** 인증**)**, **Top N Authentication by User(**사용자별 상위 **N** 인증**)** 보고서를 확인합니다.

단계 **3** 보고서를 선택하고 **Filters(**필터**)** 드롭다운 목록을 사용하여 검색할 데이터를 선택합니다.

단계 **4** 데이터를 확인할 **Time Range(**시간 범위**)**를 선택합니다.
단계 **5** **Run(**실행**)**을 클릭합니다.

TACACS 라이브 로그

다음 표에서는 TACACS+ AAA 세부정보가 표시되는 TACACS Live Logs(TACACS 라이브 로그) 페이지의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**입니다. 기본 PAN에서만 TACACS 라이브 로그를 볼 수 있습니다.

표 ***44: TACACS*** 라이브 로그

필드 이름	사용 지침
생성 시간	특정 이벤트가 트리거된 시간을 기준으로 시스템 로그 생성 시간을 표시합니다.
Logged Time(기록된 시간**)**	모니터링 노드에서 시스템 로그를 처리하고 저장한 시간을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Status(상태**)**	인증 성공 여부를 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다. 인증이 통과한 경우 녹색으로 표시되고, 인증이 실패한 경우 빨간색으로 표시됩니다.
Details(세부정보**)**	돋보기를 클릭하면 표시되는 보고서를 드릴다운하여 선택한 인증 시나리오에 대한 추가 세부정보를 확인할 수 있습니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Session Key(세션 키**)**	ISE가 네트워크 디바이스에 반환하는 세션 키(EAP 성공 또는 EAP 장애 메시지에서 확인 가능)를 표시합니다.
Username(사용자 이름**)**	디바이스 관리자의 사용자 이름을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Type(유형**)**	두 가지 유형인 Authentication(인증)과 Authorization(권한 부여)으로 구성됩니다. 인증, 권한 부여 또는 둘 다에서 통과했거나 장애가 발생한 사용자 이름을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.

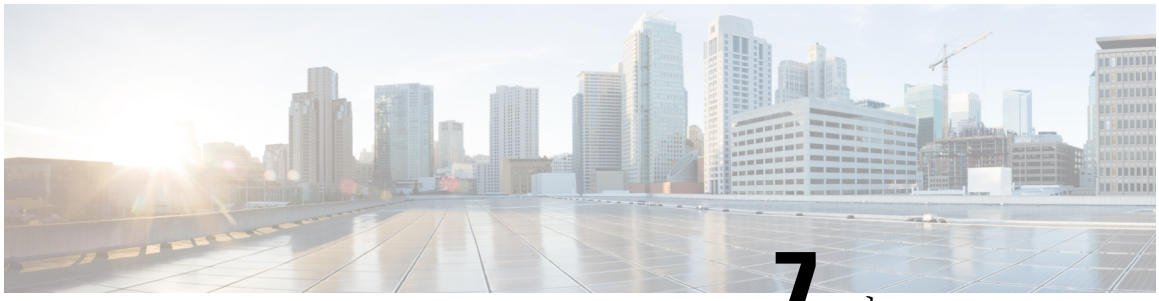
필드 이름	사용 지침
권한 부여 정책	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.
ISE Node(ISE 노드**)**	액세스 요청이 처리되는 ISE 노드의 이름을 표시합니다.
Network Device Name(네트워크 디바이스 이름**)**	네트워크 디바이스의 이름을 표시합니다.
Network Device IP(네트워크 디바이스 **IP)**	액세스 요청이 처리되는 네트워크 디바이스의 IP 주소를 표시합니다.
네트워크 디바이스 그룹	네트워크 디바이스가 속한 해당 네트워크 디바이스 그룹의 이름을 표시합니다.
디바이스 유형	다른 네트워크 디바이스의 액세스 요청을 처리하는 데 사용되는 디바이스 유형 정책을 표시합니다.
Location(위치**)**	네트워크 디바이스의 액세스 요청을 처리하는 데 사용되는 위치 기반 정책을 표시합니다.
Device Port(디바이스 포트**)**	액세스 요청을 수행하는 디바이스 포트 번호를 표시합니다.
Failure Reason(실패 이유**)**	네트워크 디바이스에서 수행한 액세스 요청을 거부하는 이유를 표시합니다.
Remote Address(원격 주소**)**	최종 무선국을 고유하게 식별하는 IP 주소, MAC 주소 또는 기타 문자열을 표시합니다.
Matched Command Set(일치하는 명령 집합**)**	MatchedCommandSet 속성 값이 있으면 표시하고, MatchedCommandSet 속성 값이 비어 있거나 속성 자체가 시스템 로그에 없으면 빈 값을 표시합니다.
Shell Profile(셸 프로파일**)**	네트워크 디바이스에서 명령을 실행하기 위해 디바이스 관리자에게 부여된 권한을 표시합니다.

TACACS Live Logs(TACACS 라이브 로그) 페이지에서는 다음을 수행할 수 있습니다.

- 데이터를 csv 또는 pdf 형식으로 내보냅니다.
- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 맞춤형 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.

- 열 값을 정렬합니다.

참고 모든 사용자 맞춤 설정은 사용자 기본 설정으로 저장됩니다.



7 장

게스트 및 보안 Wi-Fi

Cisco ISE 게스트 서비스

Cisco ISE(Identity Services Engine) 게스트 서비스를 사용하면 방문자, 계약자, 컨설턴트 및 고객과 같은 게스트에 대한 보안 네트워크 액세스를 제공할 수 있습니다. 기본 Cisco ISE 라이선스를 사용하여 게스트를 지원할 수 있으며, 회사의 인프라 및 기능 요구 사항에 따라 여러 구축 옵션 중에서 선택할 수 있습니다.

Cisco ISE에는 회사 네트워크와 내부 리소스 및 서비스를 대상으로 게스트 및 직원을 위한 온보딩 기능을 제공하는 웹 기반 및 모바일 포털이 있습니다.

관리 포털에서는 게스트 및 스폰서 포털을 생성 및 편집하고, 게스트 유형을 정의하여 게스트 액세스 권한을 구성하고, 게스트 계정을 생성하고 관리할 수 있는 스폰서 권한을 할당할 수 있습니다.

- 게스트 포털, 375 페이지
- 게스트 유형 및 사용자 ID 그룹, 355 페이지
- 스폰서 포털, 391 페이지
- 스폰서 그룹, 393 페이지

ISE 커뮤니티 리소스

ISE 게스트 및 웹 인증에 대한 ISE 커뮤니티 리소스의 전체 목록은 ISE Guest Access - ISE Guest and Web Authentication을 참고하십시오.

분산형 환경의 최종 사용자 게스트 및 스폰서 포털

Cisco ISE 최종 사용자 웹 포털에서는 관리, 정책 서비스 및 모니터링 페르소나를 사용하여 구성, 세션 지원 및 보고 기능을 제공합니다.

- **PAN(Policy Administration Node,** 정책 관리 노드**)**: 사용자, 디바이스 및 최종 사용자 포털에 적용하는 모든 구성 변경 사항은 PAN에 기록됩니다.
- **PSN(Policy Service node,** 정책 서비스 노드**)**: 네트워크 액세스, 클라이언트 프로비저닝, 게스트 서비스, 포스처 및 프로파일링을 비롯한 모든 세션 트래픽을 처리하는 PSN에서 최종 사용자 포털을 실행해야 합니다. PSN이 노드 그룹에 속해 있는 경우 노드에 장애가 발생하면 다른 노드에서 장애를 탐지하고 대기 중인 세션을 모두 재설정합니다.
- **MnT** 노드**(**모니터링 노드**)**: MnT 노드에서는 최종 사용자, 그리고 내 디바이스, 스폰서 및 게스트 포털의 디바이스 활동 관련 데이터를 수집, 집계 및 보고합니다. 기본 MnT 노드에 장애가 발생하면 보조 MnT 노드가 자동으로 기본 MnT 노드가 됩니다.

게스트 및 스폰서 계정

- 게스트 계정: 일반적으로 게스트는 권한이 부여된 방문자, 계약업체, 고객, 기타 사용자로서 네트워크에 대한 일시적인 액세스를 필요로 합니다. 게스트 구축 시나리오 중 하나를 사용하여 직원이 네트워크에 액세스할 수 있게 하려면 직원을 위해 게스트 계정을 사용할 수도 있습니다. 스폰서 포털에 액세스하여 스폰서 및 셀프 등록 게스트가 생성한 게스트 계정을 볼 수 있습니다.
- 스폰서 계정: 권한이 부여된 방문자가 기업 네트워크나 인터넷에 안전하게 액세스할 수 있도록 스폰서 포털을 사용하여 임시 계정을 생성합니다. 게스트 계정을 생성한 후에는 스폰서 포털을 사용하여 이러한 계정을 관리하고 게스트에게 계정 세부정보를 제공할 수도 있습니다.

게스트 계정은 다음과 같은 주체가 만들 수 있습니다.

- 스폰서: 관리 포털에서 스폰서 포털에 액세스하여 게스트 계정을 생성하고 관리할 수 있는 스폰서에 대한 액세스 권한 및 기능 지원을 정의할 수 있습니다.
- 게스트: 게스트는 셀프 등록 게스트 포털에서 직접 등록하여 본인의 계정을 생성할 수도 있습니다. 포털 컨피그레이션에 따라 이러한 셀프 등록 게스트의 경우 로그인 자격 증명을 얻으려면 스폰서 승인을 받아야 할 수 있습니다.

  게스트는 핫스팟 게스트 포털을 사용하여 네트워크에 액세스하도록 선택할 수도 있습니다. 이 경우 게스트 계정 및 로그인 자격 증명(예: 사용자 이름 및 비밀번호)을 생성할 필요가 없습니다.
- 직원: ID 저장소(예: Active Directory, LDAP, 내부 사용자)에 포함되어 있는 직원은 인증 게스트 포털(스폰서 게스트 및 셀프 등록 게스트 포털)을 구성한 경우 이를 통해서도 액세스 권한을 획득할 수 있습니다.

게스트 계정이 생성되고 나면 게스트는 스폰서 게스트 포털을 사용하여 로그인하고 네트워크에 대한 액세스 권한을 획득할 수 있습니다.

게스트 유형 및 사용자 ID 그룹

각 게스트 계정은 게스트 유형과 연결되어야 합니다. 게스트 유형을 통해 스폰서는 여러 수준의 액세스 및 게스트 계정에 대한 다양한 네트워크 연결 시간을 할당할 수 있습니다. 이러한 게스트 유형은 특정 네트워크 액세스 정책과 연결되어 있습니다. Cisco ISE에 포함되어 있는 기본 게스트 유형은 다음과 같습니다.

- 계약자: 최대 1년까지 오랜 시간 동안 네트워크에 액세스해야 하는 사용자
- 일별: 1~5일간만 네트워크의 리소스에 액세스해야 하는 게스트
- 주별: 몇 주간 네트워크에 액세스해야 하는 사용자

게스트 계정을 생성하는 경우 특정 게스트 유형을 사용하도록 특정 스폰서 그룹을 제한할 수 있습니다. 그러한 그룹의 멤버는 게스트 유형에 대해 지정된 기능만 사용하여 게스트를 생성할 수 있습니다. 예를 들어 스폰서 그룹, ALL_ACCOUNTS는 계약자 게스트 유형을 사용하여 설정될 수 있으며, 스폰서 그룹, OWN_ACCOUNTS 및 GROUP_ACCOUNTS는 일별 및 주별 게스트 유형을 사용하여 설정될 수 있습니다. 셀프 등록 게스트 포털을 사용하는 셀프 등록 게스트가 보통 하루 정도의 액세스 기간을 필요로 하는 경우 일별 게스트 유형을 할당할 수 있습니다.

게스트 유형에서는 게스트에 대한 사용자 ID 그룹을 정의합니다.

자세한 내용은 다음을 참고하십시오.

- 사용자 ID 그룹, 521 페이지
- 사용자 ID 그룹 생성, 531 페이지

게스트 유형 생성 또는 편집

기본 게스트 유형과 이 유형의 기본 액세스 권한 및 설정을 편집할 수도 있고 새 게스트 유형을 생성할 수도 있습니다. 수행하는 변경사항은 이 게스트 유형을 사용하여 생성한 기존 게스트 계정에 적용됩니다. 로그온되어 있는 게스트 사용자의 경우 로그오프했다가 다시 로그온할 때까지 이러한 변경사항이 표시되지 않습니다. 게스트 유형을 복제하여 동일한 액세스 권한으로 추가 게스트 유형을 생성할 수도 있습니다.

각 게스트 유형에는 이름, 설명 및 이 게스트 유형을 사용하여 게스트 계정을 생성할 수 있는 스폰서 그룹의 목록이 있습니다. 일부 게스트 유형은 셀프 등록 게스트에만 사용하도록 지정하거나 스폰서 그룹이 게스트 계정을 생성하는 데 사용하지 않도록 지정할 수 있습니다.

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Guest Access(**게스트 액세스**)** > **Configure(**구성**)** > **Guest Types(**게스트 유형**)**. 필요한 세부정보를 입력합니다.

다음과 같은 설정을 사용하여 네트워크에 액세스할 수 있는 게스트의 유형 및 게스트의 액세스 권한을 생성합니다. 이 게스트 유형을 생성할 수 있는 스폰서 그룹도 지정할 수 있습니다.

필드 이름	사용 지침
Guest type name(게스트 유형 이름**)**	이 게스트 유형과 기본 게스트 유형 및 직접 생성하는 다른 게스트 유형을 구분하는 이름을 1~256자로 입력합니다.
Description(설명**)**	이 게스트 유형의 권장 사용 방식(예: 셀프 등록 게스트에 사용, 게스트 계정 생성 시 사용 안 함 등)에 대한 추가 정보를 최대 2,000자까지 입력합니다.
Language File(언어 파일**)**	이 게스트 유형을 사용하는 포털에 사용할 언어 파일을 내보내거나 가져옵니다.
Collect Additional Data(추가 데이터 수집**)**	게스트에서 추가 정보를 수집하기 위한 사용자 맞춤화 필드를 선택합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Guest Access(**게스트 액세스**)** > **Settings(**설정**)** > **Custom Fields(**사용자 맞춤화 필드**)**.

필드 이름	사용 지침
Maximum Access Time—Account Duration Starts(최대 액세스 시간 - 계정 유지 기간 시작**)**	**From first login(**첫 번째 로그인**)**: 계정 시작 시간은 게스트 사용자가 게스트 포털에 처음 로그인하면 시작되며, 종료 시간은 지정된 기간의 시간과 동일합니다. 게스트 사용자가 로그인하지 않으면 계정은 게스트 계정 비우기 정책에 의해 제거될 때까지 Awaiting first login(첫 번째 로그인 대기 중) 상태로 유지됩니다. 셀프 등록 및 의뢰자 생성 사용자의 계정은 사용자가 계정을 생성하여 로그온하면 시작됩니다. 참고 **Allow access only on these days and times(**다음 요일과 시간에만 액세스 허용**)**을 사용하는 경우 해당 시간의 상황에 위치가 사용됩니다. From First Login(첫 번째 로그인) 액세스가 위치를 기반으로 하지 않도록 하려면 액세스할 날짜와 시간을 설정하지 마십시오. **From sponsor-specified date(**스폰서 지정 날짜**)**: 이 게스트 유형의 게스트가 네트워크에 액세스하고 네트워크에 연결된 상태를 유지할 수 있는 최대 시간을 일(1~999), 시간 또는 분 단위로 지정합니다. 이 설정을 변경하는 경우 이 게스트 유형을 사용하여 생성한 기존 게스트 계정에는 변경 사항이 적용되지 않습니다.
Allow access only on these days and times(다음 요일과 시간에만 액세스 허용**)**	시간 범위를 입력하고 요일을 선택하여 이 게스트 유형이 네트워크에 액세스할 수 있는 시간을 지정합니다. 이 게스트 유형은 이러한 시간 매개변수 범위를 벗어나 연결 상태를 유지하는 경우 로그아웃됩니다. 시간 범위는 이 게스트 유형을 사용하는 게스트에 할당된 위치에 의해 정의되는 표준 시간대와 연관됩니다. 제한된 액세스 시간을 추가하거나 삭제하려면 **+** 및 **-**를 클릭합니다.
Configure Guest Account Purge Policy(게스트 계정 비우기 정책 구성**)**	엔드포인트 제거 작업을 예약할 수 있습니다. 엔드포인트 비우기 일정은 기본적으로 활성화되며, Cisco ISE는 30일보다 오래된 엔드포인트를 삭제합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 유지 및 모니터링 의 "엔드포인트 제거 설정"섹션을 참조하십시오.
Login Options - Maximum simultaneous logins(로그인 옵션 - 최대 동시 로그인**)**	이 게스트 유형이 동시에 실행할 수 있는 최대 사용자 세션 수를 입력합니다.

필드 이름	사용 지침
When Guest Exceeds Limit(게스트의 제한 초과 시**)**	**Maximum simultaneous logins(**최대 동시 로그인 수**)**를 선택하는 경우에는 해당 제한에 도달한 후 사용자가 연결할 때 수행할 작업도 선택해야 합니다. 게스트의 제한 초과 시 수행할 작업의 옵션 • **Disconnect the oldest connection(**가장 오래된 연결 끊기**)** • **Disconnect the newest connection(**최신 연결 끊기**)** • **Redirect user to a portal page showing an error message(**오류 메시지가 표시되는 포털 페이지로 사용자 리디렉션**)**: 구성 가능한 시간 동안 오류 메시지가 표시되었다가 세션의 연결이 끊기며 사용자는 게스트 포털로 리디렉션됩니다. **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 대화 상자의 **Messages(**메시지**) > Error Messages(**오류 메시지**)** 탭에서 오류 페이지 내용을 구성합니다.
Maximum Devices Guests can Register(게스트가 등록할 수 있는 최대 디바이스 수**)**	각 게스트에게 등록할 수 있는 디바이스의 최대 수를 입력합니다. 이 게스트 유형의 게스트에 대해 이미 등록된 값보다 더 작은 숫자로 제한을 설정할 수 있습니다. 이 제한은 새로 생성하는 게스트 계정에만 적용됩니다.
Allow Guest to bypass the Guest portal(게스트의 게스트 포털 바이패스 허용**)**	사용자가 자격 증명이 지정된 게스트 종속 포털(웹 인증 페이지)을 바이패스하고 유/무선(dot1x) 신청자 또는 VPN 클라이언트에 자격 증명을 제공하여 네트워크에 액세스하도록 허용합니다. 게스트 계정은 초기 로그인 대기 중 상태와 AUP 페이지를 거쳐야 하는 경우에도 해당 상태 및 페이지를 바이패스하여 활성 상태가 됩니다. 이 설정을 활성화하지 않는 경우 사용자는 먼저 자격 증명이 지정된 게스트 종속 포털을 통해 로그인해야 네트워크의 다른 부분에 액세스할 수 있습니다.
Account Expiration Notification - Send account expiration notification __ days before account expires(계정 만료 알림 - 계정 만료 __일 전에 계정 만료 알림 전송**)**	게스트의 계정이 만료되기 전에 게스트에게 알림을 전송하고 만료 전에 알림을 보낼 기간을 일, 시간 또는 분 단위로 지정합니다.
View messages in(메시지 표시 언어**)**	이메일 또는 SMS 알림을 설정할 때 해당 알림을 표시하는 데 사용할 언어를 지정합니다.
Email(이메일**)**	계정 만료 알림에 사용할 방법으로 이메일을 선택합니다.

필드 이름	사용 지침
Use customization from(다음 위치의 사용자 맞춤화 내용 사용**)**	다른 포털의 이메일 사용자 맞춤화를 선택합니다.
Messages(메시지**)**	계정 만료 알림에 사용할 텍스트를 입력합니다.
Copy text from(다음 위치에서 텍스트 복사**)**	계정 만료 알림에 대해 다른 게스트 유형용으로 생성한 이메일 텍스트를 재사용합니다.
Send test email to me at(나에게 테스트 이메일 보내기**)**	자신의 이메일 주소로 이메일 알림을 전송하여 해당 알림이 올바르게 표시되는지 확인합니다.
SMS	계정 만료 알림에 사용할 방법으로 텍스트(SMS)를 선택합니다.
Messages(메시지**)**	계정 만료 알림에 사용할 텍스트를 입력합니다.
Copy text from(다음 위치에서 텍스트 복사**)**	다른 게스트 유형용으로 생성한 텍스트 메시지를 재사용합니다.
Send test SMS to me at(나에게 테스트 **SMS** 보내기**)**	자신의 휴대폰으로 텍스트 알림을 전송하여 해당 알림이 올바르게 표시되는지 확인합니다.
These sponsor groups can create this guest type(이 게스트 유형을 생성할 수 있는 스폰서 그룹**)**	이 게스트 유형의 게스트 계정을 생성할 수 있는 스폰서 그룹을 선택합니다. 이 게스트 유형의 사용을 비활성화하려는 경우 해당 유형을 스폰서 그룹에 할당하지 마십시오. 이 게스트 유형의 사용을 중단하려는 경우 나열된 스폰서 그룹을 삭제해 주십시오.

다음에 수행할 작업

- 이 게스트 유형을 사용할 스폰서 그룹을 생성하거나 수정합니다.
- 해당하는 경우 이 게스트 유형을 셀프 등록 게스트 포털의 셀프 등록 게스트에게 할당합니다.

게스트 유형 비활성화

마지막 남은 게스트 유형 또는 게스트 계정이 사용 중인 게스트 유형은 삭제할 수 없습니다. 사용 중인 게스트 유형을 삭제하려는 경우에는 먼저 해당 유형을 더 이상 사용할 수 없는지 확인합니다. 게스트 유형을 비활성화해도 해당 게스트 유형을 사용하여 생성한 게스트 계정에는 영향을 주지 않습니다.

다음의 단계들은 대상 게스트 유형을 준비하고 비활성화하는 방법을 설명합니다.

단계 1 스폰서가 대상 게스트 유형을 사용하여 게스트를 생성하도록 허용하는 스폰서 그룹을 식별합니다. . Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Configure(**구성**)** > **Portals and Components(**포털 및 구성 요소**)** > **Sponsor Groups(**스폰서 그룹**)**. 각 스폰서 그룹을 열어 **This sponsor group can create accounts using these guest types list(**이 스폰서 그룹이 계정을 생성하는 데 사용할 수 있는 게스트 유형**)** 목록을 검토합니다.

단계 2 대상 게스트 유형을 할당하는 셀프 등록 포털을 식별합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Configure(**구성**)** > **Portals and Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)**. 셀프 등록 게스트 포털을 엽니다. 포털에서 특정 게스트 유형을 사용하는 경우 **Portal Settings(**포털 설정**)**를 확장하여 **Employees using this portal as guests inherit login options from:(**이 포털을 게스트로 사용하는 직원이 로그인 옵션을 상속하는 원본**)** 필드의 할당된 게스트 유형을 변경합니다.

단계 3 삭제할 게스트 유형을 열고 이전 단계에서 식별한 모든 스폰서 그룹을 삭제합니다. 이 작업은 모든 스폰서가 이 게스트 유형으로 새 게스트 계정을 사용하지 못하도록 효과적으로 방지합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Configure(**구성**)** > **Portals and Components(**포털 및 구성 요소**)** > **Guest Type(**게스트 유형**)**.

엔드포인트 사용자에 대한 최대 동시 로그인 구성

게스트에게 허용되는 동시 로그인의 최대 수를 구성할 수 있습니다.

사용자가 게스트 포털에 로그인하고 정상적으로 인증될 때 해당 사용자의 기존 로그인 횟수가 확인되어 사용자의 최대 로그인 횟수에 이미 도달했는지 점검됩니다. 최대 로그인 횟수에 도달한 경우 게스트 사용자는 오류 페이지로 리디렉션됩니다. 오류 페이지가 표시되고 세션이 중지됩니다. 해당 사용자가 인터넷 액세스를 다시 시도하는 경우 사용자의 연결이 게스트 포털의 로그인 페이지로 리디렉션됩니다.

시작하기 전에

이 포털에 대한 권한 부여 정책에서 사용 중인 권한 부여 프로파일에 **Access Type(**액세스 유형**)**이 *Access_Accept*로 설정되어 있는지 확인하십시오. **Access Type(**액세스 유형**)**이 *Access_Reject*로 설정된 경우 최대 동시 로그인이 적용되지 않습니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 에서 다음을 수행합니다. **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Type(**게스트 유형**)**. **Login Options(**로그인 옵션**)**에서 다음을 수행합니다.

a) **Maximum simultaneous logins(**최대 동시 로그인 수**)** 확인란을 선택하고 허용되는 최대 동시 로그인 수를 입력합니다.

b) **When guests exceeds limit(**게스트의 제한 초과 시**)**에서 **Disconnect the newest connection(**최신 연결 끊기**)** 옵션을 클릭합니다.

c) **Redirect user to a portal page show an error message(**오류 메시지가 표시되는 포털 페이지로 사용자 리디렉션**)** 확인란을 선택합니다.

단계 2 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)**를 선택하고 권한 부여 프로파일을 생성합니다.

a) **Common Tasks(**일반 작업**)**에서 **Web Redirection(**웹 리디렉션**)**을 선택하고 다음을 수행합니다.

- 첫 번째 드롭다운에서 **Centralized Web Auth(**중앙 웹 인증**)**를 선택합니다.
- 사전 요건의 일부분으로 생성한 **ACL**을 입력합니다.
- **Value(**값**)**에서 리디렉션할 게스트 포털을 선택합니다.

b) **Common Tasks(**일반 작업**)**에서 아래로 스크롤하여 **Reauthentication(**재인증**)** 확인란을 선택하고 다음을 수행합니다.

- **Timer(**타이머**)**에서 사용자를 게스트 포털로 리디렉션할 때까지 오류 메시지를 표시할 시간을 입력합니다.
- **Maintain Connectivity During Reauthentication(**재인증 중에 연결 유지**)**에서 **Default(**기본값**)**를 선택합니다.

단계 **3** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**. NetworkAccess.SessionLimitExceeded 속성이 true이면 사용자가 포털로 리디렉션되도록 하는 권한 부여 정책을 생성합니다.

다음에 수행할 작업

Portal Page Customization(포털 페이지 사용자 맞춤화) 탭에서 오류 페이지의 텍스트를 사용자 맞춤화할 수 있습니다. **Messages(**메시지**)** > **Error Messages(**오류 메시지**)**를 선택하고 오류 메시지 키 *ui_max_login_sessions_exceeded_error*의 텍스트를 변경합니다.

만료된 게스트 계정을 비울 시기 예약

활성 또는 일시 중지된 게스트 계정의 계정 기간(계정 생성 시 스폰서가 정의함)이 종료되면 계정은 만료됩니다. 게스트 계정이 만료되면 이 계정에 해당하는 게스트가 네트워크에 액세스할 수 없습니다. 스폰서는 만료된 계정을 비우기 전에 연장할 수 있습니다. 그러나 계정이 비워진 후에는 스폰서가 새 계정을 생성해야 합니다.

만료된 게스트 계정을 비워도 연결된 엔드포인트와 보고 및 로깅 정보는 유지됩니다.

Cisco ISE는 기본적으로 15일마다 만료된 게스트 계정을 자동으로 비웁니다. **Date of next purge(**다음 비우기 날짜**)**는 다음 비우기가 수행되는 시기를 나타냅니다. 다음 작업도 가능합니다.

- X일마다 비우기가 수행되도록 예약합니다. 첫 번째 비우기는 X일 후의 **Time of Purge(**비우기 시간**)**에 수행되며, 그 이후에는 X일마다 비우기가 수행됩니다.
- X주마다 지정된 요일에 비우기를 예약합니다. 첫 번째 비우기는 다음 **Day of Week(**요일**)**의 **Time of Purge(**비우기 시간**)**에 수행되며, 그 이후에는 구성된 주의 수마다 해당 날짜와 시간에 비우기가 수행됩니다. 5주마다 목요일에 비우기가 수행되도록 월요일에 설정하는 경우를 예로 들어 보겠습니다. 다음 비우기는 지금부터 5주 후의 목요일이 아닌 이번 주의 목요일에 수행됩니다.
- **Purge Now(**지금 비우기**)**를 클릭하여 비우기를 강제로 즉시 수행할 수 있습니다.

비우기 실행이 예약된 시간에 Cisco ISE 서버가 다운되면 비우기는 실행되지 않습니다. 비우기 프로세스는 다음 예약된 비우기 시간에 해당 서버가 다시 작동한다고 가정하여 다시 실행됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Settings(**설정**)** > **Guest Account Purge Policy(**게스트 계정 제거 정책**)**.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 만료된 게스트 계정 기록을 즉시 비우려면 **Purge Now(**지금 비우기**)**를 클릭합니다.
- 비우기를 예약하려면 **Schedule purge of expired guest accounts(**만료된 게스트 계정 비우기 예약**)**를 선택합니다.

참고 각 비우기가 완료되고 나면 **Date of next purge(**다음 비우기 날짜**)**가 예약된 다음 비우기 시간으로 재설정됩니다.

단계 **3** **Expire portal-user information after(**다음 시간 후 포털-사용자 정보 만료**)**에서 사용자를 만료 처리할 비활성 기간(일)을 지정합니다. 이 설정을 사용하면, 사용된 적 없는 LDAP 및 Active Directory 계정이 ISE 데이터베이스에 무기한 보존되지 않습니다.

첫 번째 로그인이 수행되지 않은 경우 지정된 기간이 만료될 때 게스트 계정이 만료됨 상태로 전환된 다음 구성된 비우기 정책에 따라 비워집니다.

만료된 게스트 계정을 제거해야 하는 빈도(일 또는 주 단위)도 지정할 수 있습니다. **Purge occurs every _ weeks(_**주 간격으로 비우기**)** 옵션을 선택한 경우 만료된 계정을 삭제할 날짜와 시간도 지정할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다. 설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

게스트 계정 생성용 사용자 맞춤화 필드 추가

게스트 액세스 권한을 제공할 때 게스트의 이름, 이메일 주소 및 전화번호 이외의 정보도 수집하려는 경우가 있습니다. Cisco ISE는 회사 요건에 맞는 게스트에 대한 추가 정보를 수집하는 데 사용할 수 있는 사용자 맞춤화 필드를 제공합니다. 사용자 맞춤화 필드를 게스트 유형 및 셀프 등록 게스트 포털과 스폰서 포털에 연결할 수 있습니다. Cisco ISE는 기본 사용자 맞춤화 필드를 제공하지 않습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Guest Access(**게스트 액세스**)** > **Settings(**설정**)** > **Custom Fields(**사용자 맞춤화 필드**)**.

단계 **2** **Custom Field Name(**사용자 맞춤화 필드 이름**)**을 입력하고 드롭다운 목록에서 **Data Type(**데이터 유형**)**을 선택한 후에 사용자 맞춤화 필드에 대한 추가 정보를 제공할 수 있도록 **Tip Text(**팁 텍스트**)**를 입력합니다. 예를 들어 생년월일을 입력하는 경우 Date-MDY(날짜-MDY)를 선택하고 날짜 형식에 대한 팁을 YYYY/MM/DD로 입력합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

사용자 맞춤화 필드가 사전순으로 목록에 표시되거나 정렬된 순서로 상황에 맞게 표시됩니다.

단계 4 **Save(**저장**)**를 클릭합니다. 설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

참고 사용자 맞춤화 필드를 삭제하면 셀프 등록 게스트 및 스폰서 포털 설정과 게스트 유형에 대한 **Custom Fields(**사용자 맞춤화 필드**)** 목록에서 더 이상 해당 필드를 선택할 수 없습니다. 필드가 사용 중인 경우에는 **Delete(**삭제**)**가 비활성화됩니다.

다음에 수행할 작업

다음과 같은 경우 원하는 사용자 맞춤화 필드를 포함할 수 있습니다.

- 게스트 유형을 정의할 때 해당 게스트 유형을 사용하여 생성하는 계정에 사용자 맞춤화 필드의 정보가 포함되도록 하려는 경우. 게스트 유형 생성 또는 편집을 참고하십시오.
- 게스트 계정 생성 시 스폰서가 사용하도록 할 스폰서 포털을 구성하는 경우. 스폰서 포털 사용자 맞춤화, 402 페이지를 참고해 주십시오.
- 셀프 등록 게스트 포털을 사용하는 셀프 등록 게스트로부터 정보를 요청하는 경우. 셀프 등록 게스트 포털 생성, 384 페이지의 내용을 참조하십시오.

이메일 알림용 이메일 주소 및 SMTP 서버 지정

Cisco ISE에서는 스폰서와 게스트에게 이메일을 보내 정보와 지침을 알릴 수 있습니다. 이러한 이메일 알림을 배달하기 위한 SMTP 서버를 구성할 수 있습니다. 또한 게스트에게 알림을 보낼 이메일 주소도 지정할 수 있습니다.

참고 게스트 알림에는 UTF-8 호환 이메일 클라이언트가 필요합니다.

단일 클릭 스폰서 승인 기능을 사용하려면 HTML 지원 이메일 클라이언트(기능이 활성화됨)가 필요합니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Settings(**설정**)** > **Guest Email Settings(**게스트 이메일 설정**)**를 선택합니다.

단계 2 **Enable email notifications to guests(**게스트에 대한 이메일 알림 활성화**)**는 기본적으로 선택되어 있습니다. 이 설정을 비활성화하면 게스트 및 스폰서 포털을 구성할 때 활성화했을 수 있는 다른 설정에 관계없이 게스트가 이메일 알림을 받지 못하게 됩니다.

단계 3 게스트에게 이메일 알림을 보내도록 지정된 **Default** "**From**" **email address(**기본 "보낸 사람" 이메일 주소**)**를 입력합니다. 예를 들어 donotreply@ *yourcompany*.com과 같이 입력할 수 있습니다.

단계 4 다음 중 하나를 수행합니다.

- 게스트가 자신의 계정을 생성한 스폰서로부터 알림을 수신하도록 하려면 **Send notifications from sponsor's email address(if sponsored)(**스폰서가 지정된 경우 스폰서 이메일 주소에서 알림 보내기**)**를 선택합니다. 그러면 셀프 등록 게스트가 기본 이메일 주소에서 알림을 받게 됩니다.

- 스폰서가 지정된 게스트이든 셀프 등록 게스트이든 관계없이 모든 게스트가 알림을 받도록 하려면 **Always send notifications from the default email address(**항상 기본 이메일 주소에서 알림 보내기**)**를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. 설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

게스트 위치 및 **SSID** 할당

게스트 위치는 표준 시간대의 이름을 정의하며 ISE에서 로그온한 게스트의 시간 관련 설정을 시행하는 데 사용됩니다. 게스트 계정을 생성하는 스폰서와 셀프 등록 게스트가 게스트 위치를 게스트 계정에 할당합니다. 기본 게스트 위치는 산호세입니다. 다른 게스트 위치를 추가하지 않으면 모든 계정에 이 게스트 위치가 할당됩니다. 새 위치를 하나 이상 생성하지 않으면 산호세 게스트 위치를 삭제할 수 없습니다. 모든 게스트가 산호세와 같은 표준 시간대에 있는 경우가 아니면 필요한 표준 시간대를 사용하여 게스트 위치를 하나 이상 생성하십시오.

참고 게스트 액세스 시간은 게스트 위치의 표준 시간대를 기준으로 합니다. 게스트 위치의 표준 시간대가 시스템 표준 시간대와 일치하지 않으면 게스트 사용자가 로그인하지 못할 수 있습니다. 이 경우 게스트 사용자에게 "Authentication Failed(인증 실패)"오류가 발생할 수 있습니다. 디버그 보고서에 "Guest active time period not yet started(게스트 활성 기간이 아직 시작되지 않음)" 오류 메시지가 표시될 수 있습니다. 이를 해결하려면 Manage Accounts(계정 관리) 옵션을 사용하여 게스트 사용자의 현지 표준 시간대와 일치하도록 게스트 액세스 시작 시간을 조정하면 됩니다.

여기서 추가하는 SSID는 스폰서 포털에 제공되므로, 스폰서가 게스트에게 연결해야 하는 SSID를 알려줄 수 있습니다.

스폰서 포털에 구성되어 있거나 게스트 계정에 할당되어 있는 게스트 위치 또는 SSID는 삭제할 수 없습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Portals & Components(**포털 및 구성 요소**)** > **Settings(**설정**)** > **Guest Locations and SSIDs(**게스트 위치 및 **SSID)**를 선택합니다.

단계 **2** **Guest Locations(**게스트 위치**)**의 경우 다음을 수행합니다.

a) 지원해야 하는 각 표준 시간대에 대해 **Location name(**위치 이름**)**을 입력하고 드롭다운 목록에서 **Time zone(**표준 시간대**)**을 선택합니다.

b) **Add(**추가**)**를 클릭합니다.

참고 게스트 위치에서 장소의 이름, 표준 시간대의 이름 및 GMT 오프셋은 고정 값이므로 변경할 수 없습니다. 일광 절약 시간으로 인해 시간이 변경되어도 GMT 오프셋은 변경되지 않습니다. GMT 오프셋은 목록에 표시된 것과 반대입니다. 예를 들어 *Etc/GMT+3*은 실제로 GMT-3입니다.

참고 From First-login(첫 번째 로그인부터) 게스트 유형이라면 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Types(**게스트 유형**)** 페이지에서 액세스 시간 제한을 구성하려는 경우에만 게스트 위치(표준 시간대)를 구성해야 합니다.

단계 **3** **Guest SSIDs(**게스트 **SSID)**의 경우 다음을 수행합니다.

a) 게스트가 게스트 위치에서 사용할 수 있도록 할 네트워크의 **SSID** 이름을 입력합니다.

b) **Add(**추가**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다. 마지막으로 저장된 값으로 되돌리려면 **Reset(**재설정**)**을 클릭합니다.

다음에 수행할 작업

새 게스트 위치 또는 SSID를 추가한 경우 다음을 수행할 수 있습니다.

- 스폰서가 게스트 계정을 생성할 때 사용할 SSID를 제공합니다. 스폰서 포털용 포털 설정, 435 페이지를 참고해 주십시오.
- 스폰서 그룹에 게스트 위치를 추가합니다. 그러면 해당 그룹에 할당된 스폰서가 게스트 계정을 생성할 때 게스트 위치를 사용할 수 있습니다. 스폰서 그룹 구성, 394 페이지를 참고해 주십시오.
- 사용 가능한 게스트 위치를 셀프 등록 게스트 포털을 사용하는 셀프 등록 게스트에게 할당합니다. 셀프 등록 게스트 포털 생성, 384 페이지를 참고해 주십시오.
- 기존 게스트 계정의 경우 SSID 또는 위치를 추가하도록 수동으로 편집합니다.

게스트 비밀번호 정책에 대한 규칙

Cisco ISE에는 게스트 비밀번호에 대한 다음 규칙이 기본 제공됩니다.

- 게스트 비밀번호 정책은 스폰서 포털, 셀프 등록 포털, CSV 파일에 업로드된 계정, ERS API를 사용하여 생성된 비밀번호 및 사용자가 생성한 비밀번호에 적용됩니다.
- 게스트 비밀번호 정책의 변경 사항은 게스트 비밀번호가 만료되어 변경해야 될 때까지 기존 계정에 영향을 미치지 않습니다.
- 비밀번호는 대/소문자를 구분합니다.
- 특수 문자 <, >, /, 공백, 쉼표 및 %를 사용할 수 없습니다.
- 최소 길이 및 필요한 최소 문자 수는 모든 비밀번호에 적용됩니다.
- 비밀번호는 사용자 이름과 일치할 수 없습니다.
- 새 비밀번호는 현재 비밀번호와 일치해서는 안 됩니다.
- 게스트는 게스트 계정 만료와 달리 비밀번호 만료 전에는 알림을 받지 않습니다. 게스트 비밀번호가 만료되면 스폰서는 비밀번호를 임의 비밀번호로 재설정할 수 있습니다. 또는 게스트가 자신의 현재 로그인 자격 증명을 사용하여 로그인한 다음, 비밀번호를 변경할 수 있습니다.

참고 게스트 기본 사용자 이름은 4자리 영문이고, 비밀번호는 4자리 숫자입니다. 짧고 기억하기 쉬운 사용자 이름과 비밀번호는 단기 게스트에게 적합합니다. 필요하다면 ISE에서 사용자 이름과 비밀번호 길이를 변경할 수 있습니다.

게스트 비밀번호 정책 및 만료 설정

모든 게스트 포털에 대해 비밀번호 정책을 정의할 수 있습니다. 게스트 비밀번호 정책에 따라 모든 게스트 계정에 대해 비밀번호를 생성하는 방법이 결정됩니다. 비밀번호는 영문자, 숫자 또는 특수 문자의 조합일 수 있습니다. 게스트 비밀번호가 만료되어 게스트가 비밀번호를 재설정해야 할 때까지의 기간(일)을 설정할 수도 있습니다.

게스트 비밀번호 정책은 스폰서 포털, 셀프 등록 포털, CSV 파일에 업로드된 계정, ERS API를 사용하여 생성된 비밀번호 및 사용자가 생성한 비밀번호에 적용됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Guest Access(**게스트 액세스**)** > **Settings(**설정**)** > **Guest Password Policy(**게스트 비밀번호 정책**)**.

단계 **2** 게스트 비밀번호의 **Minimum password length(**최소 비밀번호 길이**)**를 문자 단위로 입력합니다.

단계 **3** 게스트가 비밀번호를 생성하는 데 사용할 수 있는 각 문자 집합의 문자를 지정합니다.

Allowed Characters and Minimums(허용되는 문자 및 최소값**)**에서 다음 옵션 중 하나를 선택하여 게스트에 대한 비밀번호 정책을 지정합니다.

- 각 문자 집합의 모든 문자를 사용합니다.
- 특정 문자를 사용하지 못하도록 지정하려면 드롭다운 메뉴에서 **Custom(**사용자 맞춤화**)**을 선택하고 미리 정의된 집합과 전체 집합에서 해당 문자를 삭제합니다.

단계 **4** 각 집합에 사용할 문자의 최소 수를 입력합니다.

4개 문자 집합 전체에서 필요한 문자의 총 수는 전체 **Minimum password length(**최소 비밀번호 길이**)**를 초과할 수 없습니다.

단계 **5** **Password Expiration(**비밀번호 만료**)**에서 다음 옵션 중 하나를 선택합니다.

- 게스트가 처음 로그인한 후 비밀번호를 변경해야 하는 빈도를 일 단위로 지정합니다. 비밀번호가 만료되기 전에 게스트가 비밀번호를 재설정하지 않으면 다음 번에 게스트가 원래 로그인 자격 증명을 사용하여 네트워크에 로그인할 때 비밀번호를 변경하라는 메시지가 표시됩니다.
- 비밀번호가 만료되지 않도록 설정합니다.

단계 **6** **Save(**저장**)**를 클릭합니다. 설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

다음에 수행할 작업

비밀번호 요건을 제공하려면 비밀번호 정책과 관련된 오류 메시지도 사용자 맞춤화해야 합니다.

1. **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsored-Guest Portals or Self-Registered Guest Portals(**스폰서 게스트 포털 또는 셀프 등록 게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Error Messages(**오류 메시지**)**를 선택합니다.
2. policy라는 키워드를 검색합니다.

게스트 사용자 이름 정책에 대한 규칙

Cisco ISE에서는 게스트 사용자 이름 정책에 대한 다음 규칙이 기본 제공됩니다.

- 게스트 사용자 이름 정책의 변경 사항은 게스트 계정이 만료되어 변경해야 될 때까지 기존 계정에 영향을 미치지 않습니다.
- 특수 문자 <, >, /, 공백, 쉼표 및 %를 사용할 수 없습니다.
- 최소 길이 및 필요한 최소 문자 수는 메일 주소를 기준으로 사용자 이름을 비롯하여 시스템에서 생성된 모든 사용자 이름에 적용됩니다.
- 비밀번호는 사용자 이름과 일치할 수 없습니다.

게스트 사용자 이름 정책 설정

게스트 사용자 이름이 생성되는 방법에 대한 규칙을 구성할 수 있습니다. 생성한 사용자 이름은 게스트의 이메일 주소 또는 이름과 성을 기준으로 생성할 수 있습니다. 스폰서가 여러 게스트를 생성할 때 또는 게스트 이름 및 이메일 주소를 사용할 수 없을 때 시간을 절약하기 위해 임의 수의 게스트 계정을 생성할 수도 있습니다. 임의로 생성된 게스트 사용자 이름은 영문자, 숫자 및 특수 문자의 조합으로 구성됩니다. 이러한 설정은 모든 게스트에 적용됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Portals & Components(**포털 및 구성 요소**)** > **Settings(**설정**)** > **Guest Username Policy(**게스트 사용자 이름 정책**)**.

단계 **2** 게스트 사용자 이름의 **Minimum username length(**최소 사용자 이름 길이**)**를 문자 단위로 입력합니다.

단계 **3** **Username Criteria for Known Guests(**알려진 게스트의 사용자 이름 기준**)**에서 옵션 중 하나를 선택하여 알려진 게스트의 사용자 이름 생성을 위한 정책을 지정합니다.

단계 **4** **Characters Allowed in Randomly-Generated Usernames(**임의 생성 사용자 이름에서 허용되는 문자**)**에서 다음 옵션 중 하나를 선택하여 임의 게스트의 사용자 이름 생성을 위한 정책을 지정합니다.

- 각 문자 집합의 모든 문자를 사용합니다.
- 특정 문자를 사용하지 못하도록 지정하려면 드롭다운 메뉴에서 **Custom(**사용자 맞춤화**)**을 선택하고 미리 정의된 집합과 전체 집합에서 해당 문자를 삭제합니다.

단계 **5** 각 집합에 사용할 문자의 최소 수를 입력합니다.

3개 문자 집합 전체의 총 문자 수는 **Minimum username length(**최소 사용자 이름 길이**)**에서 지정한 문자 수를 초과할 수 없습니다.

단계 **6** **Save(**저장**)**를 클릭합니다. 설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

다음에 수행할 작업

사용자 이름 요건을 제공하려면 사용자 이름 정책과 관련된 오류 메시지도 사용자 맞춤화해야 합니다.

1. **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsored-Guest Portals, Self-Registered Guest Portals, Sponsor Portals, or My Devices Portals(**스폰서 게스트 포털**,** 셀프 등록 게스트 포털**,** 스폰서 포털 또는 내 디바이스 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Error Messages(**오류 메시지**)**를 선택합니다.
2. `policy`라는 키워드를 검색합니다.

SMS 제공자 및 서비스

SMS 서비스는 자격 증명이 지정된 게스트 포털을 사용하는 게스트에게 SMS 알림을 보냅니다. SMS 메시지를 전송하려는 경우 이 서비스를 활성화합니다. 가능하면 회사의 비용을 절감할 수 있도록 무료 SMS 서비스 제공자를 구성하여 제공해 주십시오.

Cisco ISE는 구독자에게 무료 SMS 서비스를 제공하는 다양한 셀룰러 통신 사업자를 지원합니다. 서비스 계약 없이, Cisco ISE에서 계정 자격 증명을 구성하지 않고도 이러한 제공자를 사용할 수 있습니다. 여기에는 ATT, Orange, Sprint, TMobile 및 Verizon이 포함됩니다.

또한 무료 SMS 서비스를 제공하는 다른 셀룰러 서비스 제공자 또는 글로벌 SMS 서비스 제공자(예: Click-A-Tell)를 추가할 수도 있습니다. 기본 글로벌 SMS 서비스 제공자를 이용하려면 서비스 계약이 필요하며 Cisco ISE에서 계정 자격 증명을 구성해야 합니다.

- 셀프 등록 게스트가 셀프 등록 양식에서 무료 SMS 서비스 제공자를 선택할 경우 로그인 자격 증명이 포함된 SMS 알림을 무료로 받게 됩니다. SMS 서비스 제공자를 선택하지 않으면 회사에서 계약한 기본 글로벌 SMS 서비스 제공자를 사용하여 SMS 알림을 보내게 됩니다.
- 스폰서가 자신이 생성한 계정을 사용하는 게스트에게 SMS 알림을 보내도록 허용하는 경우에는 스폰서 포털을 사용자 맞춤화하고 이 스폰서가 사용할 수 있는 모든 적절한 SMS 서비스 제공자도 선택해야 합니다. 스폰서 포털에 사용할 SMS 서비스 제공자를 선택하지 않을 경우 회사에서 계약한 기본 글로벌 SMS 서비스 제공자가 SMS 서비스를 제공합니다.

SMS 제공자는 Cisco ISE에서 SMS 게이트웨이로 구성됩니다. Cisco ISE의 이메일은 SMS 게이트웨이에 의해 SMS로 변환됩니다. SMS 게이트웨이는 프록시 서버 뒤에 있을 수 있습니다.

게스트에게 **SMS** 알림을 보내도록 **SMS** 게이트웨이 구성

Cisco ISE에서 SMS 게이트웨이를 설정하여 다음 기능을 활성화해야 합니다.

- 스폰서가 로그인 자격 증명 및 비밀번호 재설정 지침이 포함된 SMS 알림을 게스트에게 수동으로 보내는 기능

- 게스트가 정상적으로 등록한 후 로그인 자격 증명이 포함된 SMS 알림을 자동으로 받는 기능
- 게스트 계정이 만료되기 전에 수행해야 하는 작업이 포함된 SMS 알림을 게스트가 자동으로 받는 기능

필드에 정보를 입력할 때는 [USERNAME], [PASSWORD], [PROVIDER_ID] 등 **[ ]** 내의 모든 텍스트를 SMS 제공자 계정과 관련된 정보로 업데이트해야 합니다.

시작하기 전에

SMS Email Gateway(SMS 이메일 게이트웨이) 옵션에 사용할 기본 SMTP 서버를 구성합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **SMS Gateway(SMS** 게이트웨이**)** > **SMS Gateway Providers(SMS** 게이트웨이 제공자**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** SMS 게이트웨이를 구성하려면 다음 세부정보를 입력합니다.

필드 이름	사용 지침
SMS Gateway Provider Domain(SMS 게이트웨이 제공자 도메인**)**	제공자 SMS/MMS 게이트웨이로 메시지를 보내기 위한 이메일 주소의 호스트 부분으로 사용되는 제공자 도메인과 사용자 부분으로 사용되는 게스트 계정 휴대폰 번호를 입력합니다.
Provider account address(제공자 계정 주소**)**	(선택 사항) **Default Email Address(**기본 이메일 주소**)** 전역 설정**(Guest Access(**게스트 액세스**)** > **Settings(**설정**)**에 있음)을 재정의하며 이메일의 보낸 사람 주소로 사용되는 계정 주소(일반적으로는 계정 주소)를 입력합니다.
SMTP API destination address(SMTP API 대상 주소**)**	(선택 사항) Clickatell SMTP API와 같이 특정 계정 수신자 주소가 필요한 SMTP SMS API를 사용 중인 경우 SMTP API 대상 주소를 입력합니다. 이 주소는 이메일의 받는 사람 주소로 사용되며, 메시지 본문 템플릿에서는 게스트 계정 휴대폰 번호가 대체 항목으로 사용됩니다.
SMTP API body template(SMTP API 본문 템플릿**)**	(선택 사항) Clickatell SMTP API와 같이 SMS를 전송할 때 특정 이메일 본문 템플릿이 필요한 SMTP SMS API를 사용 중인 경우 SMTP API 본문 템플릿을 입력합니다. 지원되는 동적 대체 항목은 $mobilenumber$, $timestamp$(형식: $YYYYMMDDHHHMISSmimi$) 및 $message$입니다. URL에 고유한 식별자가 필요한 SMS 게이트웨이에 $timestamp$$mobilenumber$를 사용할 수 있습니다.

다음과 같은 설정을 사용하여 HTTP API(GET 또는 POST 메서드)를 통한 게스트 및 스폰서로의 SMS 메시지 보내기를 구성합니다.

필드	사용 지침
URL	API의 URL을 입력합니다. 이 필드는 URL로 인코딩되지 않습니다. URL에서는 게스트 계정 휴대폰 번호가 대체 항목으로 사용됩니다. 지원되는 동적 대체 항목은 $mobilenumber$ 및 $message$입니다. HTTP API를 통한 HTTPS를 사용 중인 경우에는 URL 문자열에 HTTPS를 포함하고 제공자의 신뢰할 수 있는 인증서를 Cisco ISE에 업로드합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted certificates(**신뢰할 수 있는 인증서**)**.
Data(데이터)(URL로 인코딩되는 부분)	GET 또는 POST 요청에 대한 데이터(URL로 인코딩되는 부분)를 입력합니다. 이 필드는 URL로 인코딩됩니다. 기본 GET 메서드를 사용하는 경우 위에서 지정한 URL에 데이터가 추가됩니다.
Use HTTP POST method for data portion(데이터 부분에 HTTP POST 메서드 사용)	POST 메서드를 사용 중인 경우 이 옵션을 선택합니다. 위에서 지정한 데이터가 POST 요청의 내용으로 사용됩니다.
HTTP POST data content type(HTTP POST 데이터 콘텐츠 유형)	POST 메서드를 사용 중인 경우 "plain/text" 또는 "application/xml"과 같은 콘텐츠 유형을 지정합니다.
HTTPS Username(HTTPS 사용자 이름) HTTPS Password(HTTPS 비밀번호) HTTPS Host name(HTTPS 호스트 이름) HTTPS Port number(HTTPS 포트 번호)	해당 정보를 입력합니다.

단계 **4** (선택 사항) 휴대폰 번호를 SMS 제공자에게 보내기 전에 Javascript를 추가하여 휴대폰 번호를 형식화하려면 **Enable Mobile Number Format(**휴대폰 번호 형식 활성화**)** 확인란을 선택합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

새 SMS 게이트웨이를 구성하는 경우 다음을 수행할 수 있습니다.

- 만료 예정인 계정에 대한 SMS 알림을 게스트에게 보낼 때 사용할 SMS 통신 사업자 선택. 게스트 유형 생성 또는 편집을 참고하십시오.
- 셀프 등록 게스트가 선택할 수 있도록 셀프 등록 양식에 표시해야 하는 구성된 SMS 제공자 지정. 셀프 등록 게스트 포털 생성, 384 페이지의 내용을 참조하십시오.

셀프 등록 게스트의 소셜 로그인

게스트는 게스트 포털에서 사용자 이름과 비밀번호를 입력하는 대신 셀프 등록 게스트 자격 증명을 제공하는 방법으로 소셜 미디어 제공자를 선택할 수 있습니다. 이를 활성화하려면 소셜 미디어 사이트를 외부 ID 소스로 구성하고 사용자가 해당 외부 ID(소셜 미디어 제공자)를 사용할 수 있도록 포털을 구성합니다. Cisco ISE의 소셜 미디어 로그인에 대한 추가 정보는 여기에서 확인할 수 있습니다. https://community.cisco.com/t5/security-documents/how-to-configure-amp-use-a-facebook-social-media-login-on-ise/ta-p/3609532

소셜 미디어로 인증한 후 게스트는 소셜 미디어 사이트에서 가져온 정보를 수정할 수 있습니다. 소셜 미디어 자격 증명을 사용하더라도 소셜 미디어 사이트에서는 사용자가 해당 사이트의 정보를 사용하여 로그인했음을 알지 못합니다. Cisco ISE는 소셜 미디어 사이트에서 가져온 정보를 향후 추적을 위해 내부적으로 계속 사용합니다.

사용자가 소셜 미디어 사이트에서 가져온 정보를 변경하지 못하도록 게스트 포털을 구성하거나 등록 양식을 표시하지 않을 수도 있습니다.

소셜 로그인 게스트 플로우

로그인 플로우는 포털 설정을 구성하는 방법에 따라 달라집니다. 사용자 등록 없이, 사용자 등록과 함께 또는 사용자 등록 및 스폰서 승인을 통해 소셜 미디어 로그인을 설정할 수 있습니다.

1. 사용자가 셀프 등록 포털에 연결하고 소셜 미디어를 사용하여 로그인하도록 선택합니다. 액세스 코드를 구성한 경우 사용자는 로그인 페이지에도 액세스 코드를 입력해야 합니다.
2. 사용자가 인증을 위해 소셜 미디어 사이트로 리디렉션됩니다. 사용자는 소셜 미디어 사이트의 기본 프로파일 정보 사용을 승인해야 합니다.
3. 소셜 미디어 사이트 로그인에 성공하면 Cisco ISE는 소셜 미디어 사이트에서 사용자에 대한 추가 정보를 검색합니다. Cisco ISE는 소셜 미디어 정보를 사용하여 사용자를 로그온합니다.
4. 로그인 후 사용자는 컨피그레이션에 따라 AUP를 수락해야 할 수 있습니다.
5. 로그인 플로우의 다음 작업은 컨피그레이션에 따라 달라집니다.
   - 등록 불필요: 등록이 백그라운드에서 수행됩니다. Facebook은 로그인을 위해 Cisco ISE에 사용자 디바이스에 대한 토큰을 제공합니다.
   - 등록 필요: 소셜 미디어 제공자의 정보가 미리 입력된 등록 양식을 작성하라는 메시지가 사용자에게 표시됩니다. 이를 통해 사용자는 누락된 정보를 수정 및 추가하고 로그인을 위해 업데이트된 정보를 제출할 수 있습니다. Registration Form Settings(등록 양식 설정)에서 등록 코드를 구성한 경우 사용자는 등록 코드도 입력해야 합니다.
   - 등록 및 스폰서 승인 필요: 사용자에게 소셜 미디어에서 제공한 정보를 업데이트할 수 있을 뿐만 아니라 스폰서의 승인을 기다려야 한다는 메시지가 표시됩니다. 스폰서는 계정의 승인 또는 거부를 요청하는 이메일을 수신하게 됩니다. 스폰서가 계정을 승인하면 Cisco ISE는 액세스 권한이 있는 사용자에게 이메일을 보냅니다. 사용자가 게스트 포털에 접속하면 소셜 미디어 토큰으로 자동 로그인됩니다.

6. 등록이 완료됩니다. 사용자는 **Registration Form Settings(**등록 양식 설정**)**의 **After submitting the guest form for self-registration, direct guest to(**셀프 등록을 위해 게스트 양식 제출 후 다음으로 게스트 연결**)**에 구성된 옵션으로 연결됩니다. 사용자 계정이 포털의 게스트 유형에 대해 구성된 엔드포인트 ID 그룹에 추가됩니다.
7. 사용자는 게스트 계정이 만료되거나 사용자가 네트워크에서 연결을 끊을 때까지 액세스할 수 있습니다.

   계정이 만료된 경우 사용자가 로그인하도록 허용하는 유일한 방법은 계정을 다시 활성화하거나 삭제하는 것입니다. 사용자는 로그인 플로우를 다시 수행해야 합니다.

   사용자가 네트워크에서 연결을 끊고 다시 연결하는 경우 Cisco ISE는 권한 부여 규칙에 따라 다른 작업을 수행합니다. 사용자가 아래와 유사한 권한을 부여받고

   ```
   rule if guestendpoint then permit access
   ```

   사용자가 여전히 엔드포인트 그룹에 있으면 로그온 페이지로 리디렉션됩니다. 유효한 토큰이 있는 사용자는 자동으로 로그인됩니다. 그렇지 않은 경우 사용자는 등록을 다시 수행해야 합니다.

   사용자가 더 이상 엔드포인트 그룹에 속해 있지 않으면 사용자는 게스트 페이지로 리디렉션되어 등록을 진행합니다.

소셜 로그인 계정 기간

계정 재인증은 연결 방법에 따라 달라집니다.

- 802.1x의 경우 기본 권한 부여 규칙은

  ```
  if guestendpoint then permit access
  ```

  사용자 디바이스가 절전 상태로 전환되거나 사용자 디바이스가 다른 건물로 로밍되는 경우 게스트가 다시 연결할 수 있도록 합니다. 사용자가 다시 연결되면 토큰으로 자동 로그인하거나 등록을 재시작하는 게스트 페이지로 다시 리디렉션됩니다.

- MAB의 경우 사용자가 다시 연결할 때마다 게스트 포털로 리디렉션되며 소셜 미디어를 다시 클릭해야 합니다. Cisco ISE에서 해당 사용자의 계정에 대한 토큰을 여전히 보유한 경우(게스트 계정은 만료되지 않음) 소셜 미디어 제공자에 연결하지 않아도 플로우가 즉시 로그인 상태가 됩니다.

  모든 재연결이 다른 소셜 로그인으로 리디렉션되지 않도록 디바이스를 기억하고 계정이 만료될 때까지 액세스를 허용하는 권한 부여 규칙을 구성할 수 있습니다. 계정이 만료되면 엔드포인트 그룹에서 해당 계정이 제거되고 플로우는 게스트 리디렉션에 대한 규칙으로 다시 리디렉션됩니다. 예를 들면 다음과 같습니다.

  ```
  if wireless_mab and guest endpoint then permit access
  ```

  ```
  if wireless_mab then redirect to self-registration social media portal
  ```

보고 및 사용자 추적

Cisco ISE 라이브 로그 및 **Facebook**

- 인증 **ID** 저장소: Cisco ISE용 소셜 미디어 앱에서 생성한 애플리케이션의 이름입니다.

- **Facebook** 사용자 이름: Facebook에서 보고하는 사용자 이름입니다. 사용자가 등록 중에 사용자 이름을 변경할 수 있도록 허용하는 경우 Cisco ISE에서 보고하는 이름이 소셜 미디어 사용자 이름이 됩니다.
- **SocialMediaIdentifier**: 여기서

  ```
  https://facebook.com/<number>
  ```

  number는 소셜 미디어 사용자를 식별합니다.

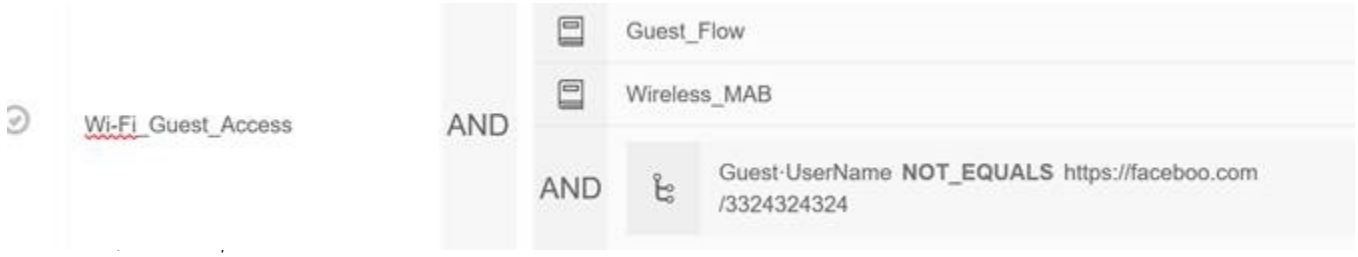
ISE 보고서: 게스트 사용자 이름은 소셜 미디어 사이트의 사용자 이름입니다.

Facebook 분석: Facebook의 분석을 사용하여 Facebook 소셜 로그온을 통해 게스트 네트워크를 사용 중인 대상을 확인할 수 있습니다.

무선 및 **Facebook**: 무선 컨트롤러의 사용자 이름은 고유한 Facebook ID이며, 라이브 로그의 **SocialMediaIdentifier**와 동일합니다. 무선 UI에서 설정을 보려면**Monitor(**모니터**)** > **Clients(**클라이언트**)** > **Detail(**상세 정보**)**을 선택하고 **User Name(**사용자 이름**)** 필드를 확인합니다.

소셜 미디어 인증 게스트 차단

개별 소셜 미디어 사용자를 차단하는 권한 부여 규칙을 생성할 수 있습니다. 이는 토큰이 만료되지 않았는데 인증에 Facebook을 사용하는 경우 유용할 수 있습니다. 다음 예에서는 Facebook 사용자 이름을 통해 차단된 Wi-Fi 연결 게스트 사용자를 보여줍니



소셜 로그인 구성에 대한 자세한 내용은 소셜 로그인 구성, 373 페이지를 참조하십시오.

소셜 로그인 구성

시작하기 전에

Cisco ISE가 소셜 미디어 사이트에 연결할 수 있도록 소셜 미디어 사이트를 구성합니다. 현재 Facebook만 지원됩니다.

Cisco ISE가 Facebook에 액세스할 수 있도록 다음 HTTPS 443 URL이 NAD를 통해 열려 있는지 확인하십시오.

```
facebook.co
akamaihd.net
akamai.co
fbcdn.net
```

참고 Facebook의 소셜 로그인 URL은 HTTPS입니다. 모든 NAD가 HTTPS URL로의 리디렉션을 지원하는 것은 아닙니다. https://communities.cisco.com/thread/79494?start=0&tstart=0&mobileredirect=true의 내용을 참조하십시오.

단계 **1** Facebook에서 Facebook 애플리케이션을 생성합니다.

a) https://developers.facebook.com에 개발자로 로그인하고 등록합니다.

b) 헤더에서 **Apps(**앱**)**를 선택하고 **Add a New App(**새 앱 추가**)**을 클릭합니다.

단계 **2** 새 **Product(**제품**)**, **Facebook Login(Facebook** 로그인**)**을 **Web(**웹**)** 유형으로 추가합니다. **Settings(**설정**)**를 클릭하고 다음 값을 설정합니다.

- **Client OAuth Login(**클라이언트 **OAuth** 로그인**)**: NO(아니요)
- **Web OAuth Login(**웹 **OAuth** 로그인**)**: YES(예)
- **Force Web OAuth Reauthentication(**강제 웹 **OAuth** 재인증**)**: NO(아니요)
- **Embedded Browser OAuth Login(**임베디드 브라우저 **OAuth** 로그인**)**: NO(아니요)
- **Valid OAuth redirect URIs(**유효한 **OAuth** 리디렉션 **URI)**: Cisco ISE에서 자동 리디렉션 URL 추가
- **Login from Devices(**디바이스에서 로그인**)**: NO(아니요)

단계 **3** **App Review(**앱 검토**)**를 클릭하고 **Your app is currently live and available to the public(**앱이 현재 라이브 상태이며 공개적으로 사용할 수 있음**)**에 *Yes(*예*)*를 선택합니다.

단계 **4** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Social Login(**소셜 로그인**)**으로 이동합니다. **Add(**추가**)**를 클릭하여 새 소셜 로그인 외부 ID 소스를 생성합니다.

- **Type(**유형**)**: 소셜 로그인 제공자의 유형을 선택합니다. 현재 Facebook이 유일한 옵션입니다.
- **App ID(**앱 **ID)**: Facebook 애플리케이션의 앱 ID를 입력합니다.
- **App Secret(**앱 암호**)**: Facebook 애플리케이션의 앱 암호를 입력합니다.

단계 **5** Cisco ISE의 셀프 등록 포털에서 **Social Media Login(**소셜 미디어 로그인**)**을 활성화합니다. 포털 페이지에서 **Portal & Page Settings(**포털 및 페이지 설정**)** > **Login Page Settings(**로그인 페이지 설정**)**를 선택하고 **Allow Social Login(**소셜 로그인 허용**)** 확인란을 선택한 후 다음 세부정보를 입력합니다.

- **Show registration form after social login(**소셜 로그인 후 등록 양식 표시**)**: 사용자가 Facebook에서 제공하는 정보를 변경할 수 있도록 합니다.
- **Require guests to be approved(**게스트 승인 필요**)**: 스폰서가 사용자의 계정을 승인해야 함을 사용자에게 알리며, 로그인을 위한 자격 증명을 사용자에게 전송합니다.

단계 **6** **Administration(**관리**)** > **External Identity Sources(**외부 **ID** 소스**)**를 선택하고 **Facebook Login(Facebook** 로그인**)** 창을 선택한 다음 Facebook 외부 ID 소스를 편집합니다.

이렇게 하면 리디렉션 URI가 생성됩니다. 이 URI를 Facebook 애플리케이션에 추가합니다.

단계 **7** Facebook에서, 이전 단계의 URI를 Facebook 애플리케이션에 추가합니다.

다음에 수행할 작업

Facebook에서 앱에 대한 데이터를 표시할 수 있습니다. 이 데이터는 Facebook 소셜 로그인을 이용한 게스트 활동을 보여줍니다.

게스트 포털

회사 방문자가 인터넷에 또는 회사 네트워크의 리소스 및 서비스에 액세스하기 위해 회사 네트워크를 사용하려 할 때 게스트 포털을 통해 네트워크 액세스 권한을 제공할 수 있습니다. 직원은 이러한 게스트 포털을 사용하여 회사의 네트워크에 액세스할 수 있습니다(구성된 경우).

세 가지 기본 게스트 포털이 있습니다.

- 핫스팟 게스트 포털 : 자격 증명 없이 네트워크 액세스가 허용됩니다. 일반적으로 네트워크 액세스 권한을 부여하기 전에 AUP(Acceptance of User Policy)를 수락해야 합니다.

  액세스 코드 로그온을 요구하는 것은 핫스팟 및 셀프 등록 포털에 대한 무선 설정에서 지원됩니다.

- Sponsored-Guest 포털: 게스트를 위해 계정을 생성하고 게스트에 로그인 자격 증명을 제공하는 스폰서가 네트워크 액세스를 부여합니다.

- 셀프 등록 게스트 포털: 게스트는 자신의 계정 자격 증명을 생성할 수 있으며 네트워크 액세스를 부여받기 전에 스폰서 승인을 받아야 합니다.

Cisco ISE는 미리 정의된 일련의 기본 포털을 포함하여 여러 게스트 포털을 호스팅할 수 있습니다.

게스트 포털의 자격 증명

Cisco ISE는 게스트가 다양한 자격 증명 유형을 사용하여 로그인하도록 요구하는 방식으로 보안 네트워크 액세스를 제공합니다. 관리자는 게스트가 이러한 자격 증명 하나 또는 여러 개의 조합을 사용하여 로그인하도록 설정할 수 있습니다.

- 사용자 이름은 필수입니다. 최종 사용자 포털(핫스팟 게스트 포털 제외)을 사용하는 모든 게스트에게 적용되며 사용자 이름 정책에서 파생됩니다. 사용자 이름 정책은 시스템에서 생성된 사용자 이름에만 적용되고 게스트 API 프로그래밍 인터페이스 또는 셀프 등록 프로세스를 사용하여 지정된 사용자 이름에는 적용되지 않습니다. **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Settings(**설정**)** > **Guest Username Policy(**게스트 사용자 이름 정책**)**에서 사용자 이름에 적용되는 정책 설정을 구성할 수 있습니다. 게스트는 이메일, SMS 또는 인쇄된 형태로 사용자 이름에 대한 알림을 받을 수 있습니다.

- 비밀번호는 필수입니다. 최종 사용자 포털(핫스팟 게스트 포털 제외)을 사용하는 모든 게스트에게 적용되며 비밀번호 정책에서 파생됩니다. **Work Centers(**작업 센터**)** > **Guest Access(**게스트

액세스**) > Settings(**설정**) > Guest Password Policy(**게스트 비밀번호 정책**)**에서 비밀번호에 적용되는 정책 설정을 구성할 수 있습니다. 게스트는 이메일, SMS 또는 인쇄된 형태로 비밀번호에 대한 알림을 받을 수 있습니다.

- 액세스 코드는 선택입니다. 핫스팟 게스트 및 자격 증명이 있는 게스트 포털을 사용하는 게스트에게 적용됩니다. 기본적으로 액세스 코드는 실제로 존재하는 게스트에게 제공되는 로컬에서 확인된 코드로, 화이트보드를 통해 시각적으로 또는 대기실 관리자에 의해 구두로 제공됩니다. 경계 외부의 사용자는 이 코드를 알 수 없어야 하며 네트워크에 액세스하는 데 이 코드를 사용해서는 안 됩니다. 액세스 코드 설정이 활성화된 경우:
  - 로그인 페이지에 액세스 코드(사용자 이름 및 비밀번호와 함께)를 입력하도록 스폰서 게스트에게 메시지가 표시됩니다.
  - 핫스팟 게스트 포털을 사용하는 게스트의 경우 AUP(Acceptable Use Policy) 페이지에 해당 액세스 코드를 입력하도록 메시지가 표시됩니다.
- 등록 코드는 선택입니다. 셀프 등록 게스트에 적용되고 셀프 등록 게스트에 제공되는 방식 차원에서 액세스 코드와 유사합니다. 등록 코드 설정이 활성화된 경우 셀프 등록 양식에 등록 코드를 입력하도록 셀프 등록 게스트에게 메시지가 표시됩니다.

사용자 이름 및 비밀번호는 회사의 스폰서(스폰서 게스트용)가 제공할 수 있습니다. 아니면 게스트가 자신을 등록하여 이러한 자격 증명을 얻을 수 있도록 자격 증명이 있는 게스트 포털을 구성할 수도 있습니다.

관련 항목

게스트 유형 및 사용자 ID 그룹, 355 페이지

핫스팟 게스트의 게스트 액세스 포털

Cisco ISE는 게스트가 로그인을 위한 자격 증명이 없어도 인터넷에 액세스하는 데 사용할 수 있는 액세스 포인트인 "핫스팟"이 포함된 네트워크 액세스 기능을 제공합니다. 게스트가 컴퓨터 또는 디바이스에서 웹 브라우저를 사용하여 핫스팟 네트워크에 연결하고 웹 사이트에 대한 연결을 시도하면 자동으로 핫스팟 게스트 포털로 리디렉션됩니다. 이 기능은 유선 및 무선(Wi-Fi) 연결에서 모두 지원됩니다.

핫스팟 게스트 포털은 게스트가 사용자 이름 및 비밀번호를 입력하지 않더라도 네트워크 액세스를 제공할 수 있는 대체 게스트 포털로, 게스트 계정을 관리해야 할 필요성을 줄여줍니다. 대신, Cisco ISE는 NAD(Network Access Device) 및 디바이스 등록 웹 인증(Device Registration WebAuth)과 함께 작동하여 게스트 디바이스에 직접 네트워크 액세스를 부여합니다. 가끔 게스트는 액세스 코드를 사용하여 로그인해야 하는 경우가 있습니다. 일반적으로 이는 회사 구내에 물리적으로 존재하는 게스트에게 로컬로 제공되는 코드입니다.

핫스팟 게스트 포털을 지원하는 경우:

- 핫스팟 게스트 포털 컨피그레이션 및 설정을 기반으로 게스트 액세스 조건이 충족되면 게스트에게 네트워크에 대한 액세스가 부여됩니다.
- Cisco ISE는 게스트 디바이스를 세밀하게 추적할 수 있게 해주는 기본 게스트 ID 그룹, GuestEndpoints를 제공합니다.

인증 게스트의 게스트 액세스 포털

자격 증명이 있는 게스트 포털을 사용하여 내부 네트워크 및 서비스에는 물론 인터넷에 대한 외부 사용자의 임시 액세스를 식별하고 권한을 부여할 수 있습니다. 스폰서는 포털의 로그인 페이지에 자격 증명을 입력하여 네트워크에 액세스할 수 있는 권한 부여된 방문자를 대신하여 임시 사용자 이름 및 비밀번호를 생성할 수 있습니다.

다음과 같이 게스트가 받은 사용자 이름과 비밀번호를 사용하여 로그인할 수 있도록 자격 증명이 있는 게스트 포털을 설정할 수 있습니다.

- 스폰서의 이 게스트 흐름에서 게스트는 회사 부지에 들어설 때의 대기실 관리자와 같이 스폰서의 인사를 받고 개별 게스트 계정으로 설정됩니다.
- 선택적 등록 코드 또는 액세스 코드를 사용하여 자신을 등록합니다. 이 게스트 흐름에서 게스트는 사람과의 상호 작용 없이 인터넷에 액세스할 수 있으며 Cisco ISE는 이 게스트에게 규정 준수에 사용할 수 있는 고유 식별자가 있는지 확인합니다.
- 선택적 등록 코드 또는 액세스 코드를 사용하여 자신을 등록하되 스폰서가 게스트 계정에 대한 요청을 승인한 이후에만 등록합니다. 이 게스트 흐름에서 게스트에게 네트워크에 대한 액세스가 제공되지만 추가적인 수준의 심사가 수행된 이후에만 제공됩니다.

로그인할 때 사용자가 새 비밀번호를 입력해야 하도록 할 수도 있습니다.

Cisco ISE에서는 여러 자격 증명이 있는 게스트 포털을 생성할 수 있습니다. 이 포털을 사용하여 여러 조건에 따라 게스트 액세스를 허용할 수 있습니다. 예를 들어 월간 계약자를 위한 포털을 구축할 수 있는데, 이는 일일 방문자를 위한 포털과는 다릅니다.

자격 증명이 있는 게스트 포털을 사용한 직원 액세스

직원은 자격 증명이 있는 게스트 포털용으로 구성된 ID 소스 시퀀스에서 자신의 자격 증명에 액세스할 수 있으면 직원 자격 증명을 사용하여 로그인하는 방식으로 해당 포털을 사용하여 네트워크에 액세스할 수도 있습니다.

게스트 디바이스 규정 준수

게스트 및 비게스트가 자격 증명이 있는 게스트 포털을 통해 네트워크에 액세스하는 경우 액세스가 허용되기 전에 관리자는 디바이스가 규정을 준수하는지 확인할 수 있습니다. 관리자는 해당 사용자를 Client Provisioning(클라이언트 프로비저닝) 창으로 보내어, 먼저 포스처 프로파일을 확인하고 디바이스가 규정을 준수하는지 검증하는 포스처 에이전트를 다운로드하도록 요구할 수 있습니다. 이를 위해서는 자격 증명이 있는 게스트 포털에서 **Guest Device Compliance Settings(**게스트 디바이스 규정 준수 설정**)**의 옵션을 선택하면 됩니다. 그러면 게스트 플로우의 일부로 Client Provisioning(클라이언트 프로비저닝) 창이 표시됩니다.

참고 게스트 플로우의 클라이언트 포스처 평가는 Temporal Agent만 지원합니다.

클라이언트 프로비저닝 서비스는 게스트를 위한 포스처 평가 및 교정 기능을 제공합니다. 클라이언트 프로비저닝 포털은 CWA(Central Web Authorization) 게스트 구축에서만 사용할 수 있습니다. 게스트 로그인 흐름에서는 CWA를 수행하고, acceptable-use-policy 및 change-password 검사가 완료되고 나면 자격 증명이 있는 게스트 포털이 클라이언트 프로비저닝 포털로 리디렉션됩니다. 포스처 하위 시스템은 네트워크 액세스 디바이스에 대해 CoA(Change of Authorization)를 수행하고 포스처가 평가된 경우 클라이언트 연결을 다시 인증합니다.

게스트 포털 컨피그레이션 작업

기본 포털 및 해당 기본 설정(예: 인증서, 엔드포인트 ID 그룹, ID 소스 시퀀스, 포털 테마, 이미지 및 Cisco ISE가 제공하는 기타 세부정보)을 사용할 수 있습니다. 기본 설정을 사용하지 않으려면 새 포털을 생성하거나 자신의 요구 사항에 맞게 기존 포털을 편집해야 합니다. 여러 포털을 생성하려는 경우 동일한 설정을 사용하여 포털을 복제할 수 있습니다.

새 포털을 생성하거나 기본 포털을 편집한 후에는 포털을 사용할 수 있는 권한을 부여해야 합니다. 포털을 사용할 수 있는 권한을 부여한 경우 이후의 컨피그레이션 변경 사항은 즉시 반영됩니다.

포털을 삭제하기로 선택한 경우에는 먼저 권한 부여 정책 규칙 및 이와 연결된 권한 부여 프로파일을 모두 삭제하거나 다른 포털을 사용하도록 수정해야 합니다.

여러 게스트 포털 구성과 관련된 작업에 대해서는 다음 표를 참고해 주십시오.

작업	핫스팟 게스트 포털	**Sponsored-Guest** 포털	셀프 등록 게스트 포털
정책 서비스 활성화, 379 페이지	필수	필수	필수
게스트 포털용 인증서 추가, 379 페이지	필수	필수	필수
외부 ID 소스 생성, 379 페이지	해당 없음	필수	필수
ID 소스 시퀀스 생성, 381 페이지	해당 없음	필수	필수
엔드포인트 ID 그룹 생성, 755 페이지	필수	필수 아님(게스트 유형으로 정의됨)	필수 아님(게스트 유형으로 정의됨)
핫스팟 게스트 포털 생성, 382 페이지	필수	해당 없음	해당 없음
Sponsored-Guest Portal 생성, 383 페이지	해당 없음	필수	해당 없음
셀프 등록 게스트 포털 생성, 384 페이지	해당 없음	해당 없음	필수
포털 권한 부여, 388 페이지	필수	필수	필수

작업	핫스팟 게스트 포털	**Sponsored-Guest** 포털	셀프 등록 게스트 포털
게스트 포털 사용자 맞춤화, 390 페이지	선택 사항	선택 사항	선택 사항

정책 서비스 활성화

Cisco ISE 최종 사용자 포털을 지원하려면 해당 포털을 호스트하려는 노드에서 포털 정책 서비스를 활성화해야 합니다.

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

단계 **2** 노드를 클릭하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **General Settings(**일반 설정**)** 탭에서 **Policy Service(**정책 서비스**)** 토글 버튼을 활성화합니다.

단계 **4** **Enable Session Services(**세션 서비스 활성화**)** 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

게스트 포털용 인증서 추가

기본 인증서를 사용하지 않으려는 경우 유효한 인증서를 추가하고 인증서 그룹 태그에 할당할 수 있습니다. 모든 최종 사용자 웹 포털에 사용되는 기본 인증서 그룹 태그는 기본 포털 인증서 그룹입니다.

단계 **1**

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

단계 **3** 시스템 인증서를 추가한 다음 포털에 사용하려는 인증서 그룹 태그에 할당합니다.

포털 생성 또는 편집 시에 이 인증서 그룹 태그를 선택할 수 있습니다.

단계 **4** **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create or Edit(**생성 또는 편집**)** > **Portal Settings(**포털 설정**)**를 선택합니다.

단계 **5** 새로 추가한 인증서와 연결된 특정 인증서 그룹 태그를 **Certificate Group Tag(**인증서 그룹 태그**)** 드롭다운 목록에서 선택합니다.

외부 **ID** 소스 생성

Cisco ISE는 Active Directory LDAP, RADIUS 토큰 및 RSA SecurID 서버와 같은 외부 ID 소스에 연결하여 인증 및 권한 부여를 위한 사용자 정보를 가져올 수 있습니다. 외부 ID 소스에는 인증서 기반 인증에 필요한 인증서 인증 프로파일도 포함되어 있습니다.

참고 인증된 사용자 ID를 수신하고 공유할 수 있는 패시브 ID 서비스를 사용하려면 추가 패시브 ID 서비스 제공자, 596 페이지의 내용을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **Identity Management(ID 관리)** > **External Identity Sources(**외부 **ID** 소스**)**를 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 인증서 기반 인증의 경우 **Certificate Authentication Profile(**인증서 인증 프로파일**)**을 선택합니다.
- 외부 ID 소스로 Active Directory에 연결하려는 경우 **Active Directory**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 Active Directory, 540 페이지를 참조하십시오.
- LDAP ID 소스를 추가하려는 경우 **LDAP**를 선택합니다. 자세한 내용은 LDAP, 640 페이지를 참조하십시오.
- RADIUS 토큰 서버를 추가하려는 경우 **RADIUS** 토큰을 선택합니다. 자세한 내용은 RADIUS 토큰 ID 소스, 665 페이지를 참조하십시오.
- RSA SecurID 서버를 추가하려는 경우 **RSA SecurID**를 선택합니다. 자세한 내용은 RSA ID 소스, 672 페이지를 참조하십시오.
- Oracle Access Manager 등의 IdP(Identity Provider)를 추가하려는 경우 **SAML Id Provider(SAML ID** 제공자**)**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 SAMLv2 ID 제공자, 679 페이지를 참조하십시오.
- 소셜 로그인(예: Facebook 등)을 외부 ID 소스로 추가하려면 **Social Login(**소셜 로그인**)**을 선택합니다. 자세한 내용은 셀프 등록 게스트의 소셜 로그인, 371 페이지을(를) 참조하십시오.

인증을 위해 게스트 포털이 **SAML IDP** 포털로 리디렉션되도록 구성

인증을 위해 사용자를 SAML IDP 포털로 리디렉션할 수 있도록 게스트 포털을 구성할 수 있습니다.

게스트 포털(셀프 등록 포털 또는 스폰서 게스트)에서 **Allow the following identity-provider guest portal to be used for login(**로그인에 다음 **ID** 제공자 게스트 포털 사용 허용**)** 옵션을 구성하면 해당 포털에서 새 로그인 영역이 활성화됩니다. 해당 로그인 옵션을 선택하는 사용자는 대체 ID 포털(사용자에게는 표시되지 않음)로 리디렉션된 다음 인증을 위해 SAML IDP 로그온 포털로 리디렉션됩니다.

예를 들어 게스트 포털에는 직원 로그인을 위한 링크가 있을 수 있습니다. 사용자는 기존 포털에서 로그인하는 대신 직원 로그온 링크를 클릭하며, 그러면 SAML IDP 단일 로그온 포털로 리디렉션됩니다. 직원은 이 SAML IDP의 마지막 로그온에 사용된 토큰을 사용하여 다시 연결되거나 해당 SAML 사이트에서 로그인합니다. 따라서 같은 포털이 단일 SSID에서 게스트와 직원을 모두 처리할 수 있습니다.

다음 단계에서는 인증을 위해 SAML IDP를 사용하도록 구성된 다른 포털을 호출하는 게스트 포털을 구성하는 방법을 보여줍니다.

단계 **1** 외부 ID 소스를 구성합니다. 자세한 내용은 외부 ID 소스로서의 SAMLv2 ID 제공자, 679 페이지를 참조하십시오.

단계 **2** SAML 제공자용 게스트 포털을 생성합니다. Portal Settings(포털 설정)에서 **Authentication method(**인증 방법**)**를 SAML 제공자로 설정합니다. 이 포털은 사용자에게는 보이지 않으며 SAML IDP 로그온 페이지로 사용자를 이동시

키기 위한 자리 표시자입니다. 아래에서 설명하는 것처럼 이 하위 포털로 리디렉션되도록 다른 포털을 구성할 수 있습니다.

단계 **3** 방금 생성한 SAML 제공자 포털에 대해 게스트 포털로 리디렉션하는 옵션을 사용하여 게스트 포털을 생성합니다. 이 포털은 하위 포털로 리디렉션되는 기본 포털입니다.

SAML 제공자처럼 표시되도록 이 포털의 외관을 맞춤화할 수 있습니다.

a) 기본 포털의 Login Page Settings(로그인 페이지 설정) 페이지에서 **Allow the following identity-provider guest portal to be used for login(**다음 **ID** 제공자 게스트 포털을 로그인에 사용하도록 허용**)**을 선택합니다.

b) SAML 제공자와 함께 사용하기 위해서 구성한 게스트 포털을 선택합니다.

ID 소스 시퀀스 생성

시작하기 전에

Cisco ISE에서 외부 ID 소스를 구성했는지 확인합니다.

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

게스트 사용자가 로컬 WebAuth를 통해 인증하도록 허용하려면 게스트 포털 인증 소스와 ID 소스 시퀀스가 동일한 ID 저장소를 포함하도록 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identity Source Sequences(ID** 소스 시퀀스**)** > **Add(**추가**)**를 선택합니다.

단계 **2** ID 소스 시퀀스의 이름을 입력합니다. 원하는 경우 설명을 입력할 수도 있습니다.

단계 **3** **Select Certificate Authentication Profile(**인증서 인증 프로파일 선택**)** 확인란을 선택하고 인증서 기반 인증용 인증서 인증 프로파일을 선택합니다.

단계 **4** ID 소스 시퀀스에 포함할 하나 이상의 데이터베이스를 **Selected List(**선택됨 목록**)** 필드에서 선택합니다.

단계 **5** Cisco ISE가 데이터베이스를 검색하도록 할 순서대로 **Selected List(**선택됨 목록**)** 필드의 데이터베이스를 다시 정렬합니다.

단계 **6** **Advanced Search List(**고급 검색 목록**)** 영역에서 다음 옵션 중 하나를 선택합니다.

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError(**시퀀스의 다른 저장소에 액세스하지 않고 **AuthenticationStatus** 속성을 **ProcessError**로 설정**)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 검색을 중지하도록 하려면 이 옵션을 선택합니다.
- **Treat as if the user was not found and proceed to the next store in the sequence(**사용자를 찾지 못한 것으로 간주하여 다음 저장소로 순차 진행**)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 시퀀스에서 선택한 다른 ID 소스에서 검색을 계속하도록 하려면 이 옵션을 선택합니다.

  요청을 처리하는 동안 Cisco ISE는 이러한 ID 소스를 순서대로 검색합니다. Selected list(선택됨 목록) 필드의 ID 소스가 Cisco ISE가 검색하도록 할 순서대로 나열되어 있는지 확인합니다.

단계 **7** ID 소스 시퀀스를 생성하려면 **Submit(**제출**)**을 클릭합니다. 생성된 시퀀스는 정책에서 사용할 수 있습니다.

엔드포인트 ID 그룹 생성

Cisco ISE는 검색되는 엔드포인트를 해당하는 엔드포인트 ID 그룹으로 그룹화합니다. Cisco ISE에서는 몇 가지 시스템 정의 엔드포인트 ID 그룹이 제공됩니다. 엔드포인트 **ID** 그룹 창에서 엔드포인트 ID 그룹을 추가로 생성할 수도 있습니다. 직접 생성한 엔드포인트 ID 그룹은 편집하거나 삭제할 수 있습니다. 시스템 정의 엔드포인트 ID 그룹의 경우 설명만 편집할 수 있습니다. 그 이름은 편집하거나 삭제할 수 없습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Endpoint Identity Groups(**엔드포인트 **ID** 그룹**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 생성할 엔드포인트 ID 그룹의 **Name(**이름**)**을 입력합니다(엔드포인트 ID 그룹의 이름에 공백 제외).

단계 **4** 생성할 엔드포인트 ID 그룹에 대한 **Description(**설명**)**을 입력합니다.

단계 **5** **Parent Group(**부모 그룹**)** 드롭다운 목록을 클릭하여 새로 생성한 엔드포인트 ID 그룹을 연결할 엔드포인트 ID 그룹을 선택합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

핫스팟 게스트 포털 생성

게스트가 로그인 시 사용자 이름과 비밀번호를 사용하지 않고도 네트워크에 연결할 수 있도록 핫스팟 게스트 포털을 제공할 수 있습니다. 로그인하려면 액세스 코드가 필요할 수 있습니다.

새 핫스팟 게스트 포털을 생성하거나 기존 포털을 편집 또는 복제할 수 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 핫스팟 게스트 포털을 삭제할 수 있습니다.

Portal Behavior and Flow Settings(포털 동작 및 흐름 설정**)** 탭의 페이지 설정에 적용하는 모든 변경 사항은 게스트 흐름도의 그래픽 흐름에 반영됩니다. AUP 페이지와 같은 페이지를 활성화하면 흐름에 표시되고 게스트가 포털에서 해당 페이지를 경험할 수 있습니다. 페이지를 비활성화하면 흐름에서 제거되고 다음에 활성화된 페이지가 게스트에게 표시됩니다.

인증 성공 설정를 제외한 모든 페이지 설정은 선택 사항입니다.

시작하기 전에

- 이 포털에 사용할 필수 인증서 및 엔드포인트 ID 그룹을 구성했는지 확인해 주십시오.
- 게스트가 핫스팟 포털용으로 연결하는 WLC를 Cisco ISE에서 지원하는지 확인합니다. 사용 중인 Cisco ISE 버전에 대해서는 Identity Services Engine 네트워크 구성 요소 호환성을 참조하십시오.

다음에 수행할 작업

포털을 사용하려면 권한을 부여해야 합니다. 포털 사용 권한을 부여하기 전이나 부여한 후에 포털을 사용자 맞춤화할 수도 있습니다.

Sponsored-Guest Portal 생성

지정한 스폰서가 게스트에게 액세스 권한을 부여할 수 있도록 Sponsored-Guest Portal을 제공할 수 있습니다.

새 Sponsored-Guest Portal을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 Sponsored-Guest Portal을 삭제할 수 있습니다.

Portal Behavior and Flow Settings(포털 동작 및 흐름 설정**)** 탭의 페이지 설정에 적용하는 모든 변경 사항은 게스트 흐름도의 그래픽 흐름에 반영됩니다. AUP 페이지와 같은 페이지를 활성화하면 흐름에 표시되고 게스트가 포털에서 해당 페이지를 경험할 수 있습니다. 페이지를 비활성화하면 흐름에서 제거되고 다음에 활성화된 페이지가 게스트에게 표시됩니다.

다음의 모든 페이지 설정을 사용하여 게스트에 대한 AUP(Acceptable Use Policy)를 표시하고 정책을 수락해야 하도록 지정할 수 있습니다.

- 로그인 페이지 설정
- AUP(Acceptable Use Policy) 페이지 설정
- BYOD 설정

시작하기 전에

이 포털에 사용할 필요한 인증서, 외부 ID 소스 및 ID 소스 시퀀스를 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)**.

단계 **2** 새 포털을 생성하는 경우 게스트 포털 생성 대화 상자에서 **Sponsored-Guest Portal**을 포털 유형으로 선택하고 **Continue(**계속**)**를 클릭합니다.

단계 **3** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **4** **Language File(**언어 파일**)** 드롭다운 메뉴를 사용하여 포털에 사용할 언어 파일을 내보내고 가져옵니다.

단계 **5** 포트, 이더넷 인터페이스, 인증서 그룹 태그, ID 소스 시퀀스, 인증 방법 등에 대한 기본값을 **Portal Settings(**포털 설정**)**에서 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 **6** 각각의 특정 페이지에 적용되는 다음 설정을 업데이트합니다.

- **Login Page Settings(**로그인 페이지 설정**)**: 게스트 자격 증명 및 로그인 지침을 지정합니다. **Allow guests to create their accounts(**게스트의 계정 생성 허용**)** 옵션을 선택하면 사용자가 게스트 계정을 직접 생성할 수 있습니다. 이 옵션을 선택하지 않으면 스폰서가 게스트 계정을 생성해야 합니다.

  참고 Authentication Method(인증 방법) 필드에서 IdP(Identity Provider)를 선택한 경우에는 Login Page Settings(로그인 페이지 설정) 옵션이 비활성화됩니다.

- **Acceptable Use Policy(AUP) Page Settings(AUP** 페이지 설정**)**: 별도의 AUP 페이지를 추가하고 자격 증명이 지정된 게스트 포털을 사용하는 직원을 포함하는 게스트에 대한 사용 제한 정책 동작을 정의합니다.

- **Employee Change Password Settings(**직원 비밀번호 변경 설정**)**: 게스트가 처음 로그인한 후 비밀번호를 변경해야 하도록 지정합니다.
- **Guest Device Registration Settings(**게스트 디바이스 등록 설정**)**: Cisco ISE가 게스트 디바이스를 자동으로 등록하는지 아니면 게스트가 디바이스를 수동으로 등록할 수 있는 페이지를 표시할지를 선택합니다.
- **BYOD Settings(BYOD** 설정**)**: 직원이 개인 디바이스를 사용하여 네트워크에 액세스하도록 허용합니다.
- **Post-Login Banner Page Settings(**로그인 후 배너 페이지 설정**)**: 게스트에게 네트워크 액세스 권한을 부여하기 전에 추가 정보를 알립니다.
- **Guest Device Compliance Settings(**게스트 디바이스 규정 준수 설정**)**: 게스트를 클라이언트 프로비저닝 페이지로 이동시키고 먼저 포스처 에이전트를 다운로드해야 하도록 지정합니다.
- **VLAN DHCP Release Page Settings(VLAN DHCP** 릴리스 페이지 설정**)**: 게스트 VLAN에서 게스트 디바이스 IP 주소를 릴리스하고 네트워크의 다른 VLAN에 액세스하도록 갱신합니다.
- **Authentication Success Settings(**인증 성공 설정**)**: 인증된 게스트에게 표시할 내용을 지정합니다.
- **Support Information Page Settings(**지원 정보 페이지 설정**)**: 헬프 데스크에서 네트워크 액세스 문제를 해결하는 데 사용할 수 있는 정보를 게스트가 제공할 수 있도록 합니다.

단계 **7** **Save(**저장**)**를 클릭합니다. 시스템에서 생성된 URL이 **Portal test URL(**포털 테스트 **URL)**로 표시됩니다. 이 URL을 사용하여 포털에 액세스한 다음 포털을 테스트할 수 있습니다.

다음에 수행할 작업

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 ISE는 첫 번째 활성 상태의 PSN을 선택합니다.

포털을 사용하려면 권한을 부여해야 합니다. 포털 사용 권한을 부여하기 전이나 부여한 후에 포털을 사용자 맞춤화할 수도 있습니다.

셀프 등록 게스트 포털 생성

게스트가 직접 등록을 하고 네트워크에 액세스하기 위한 계정을 직접 생성할 수 있도록 셀프 등록 게스트 포털을 제공할 수 있습니다. 하지만 액세스 권한을 부여하기 전에 스폰서가 이러한 계정을 계속 승인해야 하도록 지정할 수 있습니다.

새 셀프 등록 게스트 포털을 생성하거나 기존 포털을 편집 또는 복제할 수 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 셀프 등록 게스트 포털을 삭제할 수 있습니다.

Portal Behavior and Flow Settings(포털 동작 및 흐름 설정**)** 탭의 페이지 설정에 적용하는 모든 변경 사항은 게스트 흐름도의 그래픽 흐름에 반영됩니다. AUP 페이지와 같은 페이지를 활성화하면 흐름에 표시되고 게스트가 포털에서 해당 페이지를 경험할 수 있습니다. 페이지를 비활성화하면 흐름에서 제거되고 다음에 활성화된 페이지가 게스트에게 표시됩니다.

다음의 모든 페이지 설정을 사용하여 게스트에 대한 AUP(Acceptable Use Policy)를 표시하고 정책을 수락해야 하도록 지정할 수 있습니다.

- 로그인 페이지 설정
- 셀프 등록 페이지 설정
- 셀프 등록 성공 페이지 설정
- AUP(Acceptable Use Policy) 페이지 설정
- BYOD 설정

시작하기 전에

이 포털에 대해 필요한 인증서, 외부 ID 소스 및 ID 소스 시퀀스를 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers**(작업 센터) > **Guest Access**(게스트 액세스) > **Portals & Components**(포털 및 구성 요소) > **Guest Portals**(게스트 포털) > **Create, Edit or Duplicate**(생성, 편집 또는 복제).
.

단계 **2** 새 포털을 생성하는 경우 게스트 포털 생성 대화 상자에서 **Self-Registered Guest Portal**(셀프 등록 게스트 포털)을 포털 유형으로 선택하고 **Continue**(계속)를 클릭합니다.

단계 **3** 포털의 고유한 **Portal Name**(포털 이름) 및 **Description**(설명)을 입력합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **4** **Language File**(언어 파일) 드롭다운 메뉴를 사용하여 포털에 사용할 언어 파일을 내보내고 가져옵니다.

단계 **5** **Portal Settings**(포털 설정)에서 포트, 이더넷 인터페이스, 인증서 그룹 태그, ID 소스 시퀀스, 인증 방법 등에 대한 기본값과 이 포털의 동작을 정의하는 기타 설정을 업데이트합니다.

Portal Settings(포털 설정) 필드에 대한 자세한 내용은 자격 증명이 있는 게스트 포털에 대한 포털 설정, 419 페이지를 참고하십시오.

단계 **6** 각각의 특정 페이지에 적용되는 다음 설정을 업데이트합니다.

- **Login Page Settings**(로그인 페이지 설정): 게스트 자격 증명 및 로그인 지침을 지정합니다. 자세한 내용은 자격 증명이 있는 게스트 포털에 대한 로그인 페이지 설정, 422 페이지를 참고하십시오.
- **Self-Registration Page Settings**(셀프 등록 페이지 설정): 셀프 등록 게스트가 읽고 셀프 등록 양식에 입력해야 하는 정보와, 이러한 게스트가 양식을 제출한 후의 게스트 경험을 지정합니다.
- **Acceptable Use Policy (AUP) Page Settings**(AUP 페이지 설정): 별도의 AUP 페이지를 추가하고 자격 증명이 지정된 게스트 포털을 사용하는 직원을 포함하는 게스트에 대한 사용 제한 정책 동작을 정의합니다. 자세한 내용은 자격 증명이 있는 게스트 포털에 대한 AUP(Acceptable Use Policy) 페이지 설정, 428 페이지를 참고하십시오.
- **Employee Change Password Settings**(직원 비밀번호 변경 설정): 게스트가 처음 로그인한 후 비밀번호를 변경해야 하도록 지정합니다.
- **Guest Device Registration Settings**(게스트 디바이스 등록 설정): Cisco ISE가 게스트 디바이스를 자동으로 등록하는지 아니면 게스트가 디바이스를 수동으로 등록할 수 있는 페이지를 표시할지를 선택합니다.
- **BYOD Settings**(BYOD 설정): 직원이 개인 디바이스를 사용하여 네트워크에 액세스하도록 허용합니다. 자세한 내용은 자격 증명이 있는 게스트 포털에 대한 BYOD 설정, 429 페이지을(를) 참고하십시오.
- **Post-Login Banner Page Settings**(로그인 후 배너 페이지 설정): 사용자가 성공적으로 로그인한 후 사용자에게 네트워크 액세스 권한을 부여하기 전에 추가 정보를 표시합니다.

- **Guest Device Compliance Settings(**게스트 디바이스 규정 준수 설정**)**: 포스처 평가를 위해 게스트를 클라이언트 프로비저닝 페이지로 리디렉션합니다. 자세한 내용은 자격 증명이 있는 게스트 포털에 대한 게스트 디바이스 규정 준수 설정, 431 페이지를 참고하십시오.
- **VLAN DHCP Release Page Settings(VLAN DHCP** 릴리스 페이지 설정**)**: 게스트 VLAN에서 게스트 디바이스 IP 주소를 릴리스하고 네트워크의 다른 VLAN에 액세스하도록 갱신합니다. 자세한 내용은 자격 증명이 있는 게스트 포털에 대한 BYOD 설정, 429 페이지를 참고하십시오.
- **Authentication Success Settings(**인증 성공 설정**)**: 인증된 게스트를 보낼 곳을 지정합니다. 인증 후 게스트를 외부 URL로 리디렉션하는 경우 URL 주소가 확인되고 세션이 리디렉션되는 동안 지연이 발생할 수 있습니다. 자세한 내용은 게스트 포털용 인증 성공 설정, 432 페이지를 참고하십시오.
- **Support Information Page Settings(**지원 정보 페이지 설정**)**: 헬프 데스크에서 네트워크 액세스 문제를 해결하는 데 사용할 수 있는 정보를 게스트가 제공할 수 있도록 합니다.

단계 **7** **Save(**저장**)**를 클릭합니다. 시스템에서 생성된 URL이 **Portal test URL(**포털 테스트 **URL)**로 표시됩니다. 이 URL을 사용하여 포털에 액세스한 다음 포털을 테스트할 수 있습니다.

다음에 수행할 작업

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 ISE는 첫 번째 활성 상태의 PSN을 선택합니다.

포털을 사용하려면 권한을 부여해야 합니다. 포털 사용 권한을 부여하기 전이나 부여한 후에 포털을 사용자 맞춤화할 수도 있습니다.

스폰서의 셀프 등록 계정 승인

등록된 게스트가 계정의 승인을 요청하도록 구성하면 Cisco ISE는 승인자에게 이메일을 보내 계정을 승인합니다. 승인자는 방문자나 스폰서 사용자일 수 있습니다.

승인자가 스폰서인 경우 계정을 거부하거나 승인하는 링크를 포함하도록 이메일을 구성할 수 있습니다. 승인 링크에는 승인이 스폰서의 이메일 주소에 연결되는 토큰이 포함되어 있습니다. 스폰서에게 인증하도록 요구할 수 있으며, 이 경우 토큰이 무시됩니다. 토큰이 시간 초과될 수도 있습니다. 이 경우 계정을 승인하기 전에 스폰서가 인증해야 합니다.

셀프 등록 포털의 **Registration Form Settings(**등록 양식 설정**)**에서 계정 승인 옵션을 구성합니다. 이 기능을 단일 클릭 스폰서 승인이라고도 합니다.

스폰서가 이메일을 열고 승인 링크를 클릭할 때 승인자의 구성에 따라 작업이 달라집니다.

이메일 승인 요청 대상의 구성 및 해당 작업은 다음과 같습니다.

- 방문자
  - 그리고 게스트 계정에 인증이 필요하지 않음: 클릭 한 번으로 계정이 승인됩니다.

- 그리고 게스트 계정에 인증이 필요함: 스폰서는 스폰서 포털로 이동되며, 여기서 스폰서가 자격 증명을 입력해야 계정을 승인할 수 있습니다.

- 아래에 나온 스폰서 이메일 주소: Cisco ISE가 제공된 모든 이메일 주소로 이메일을 보냅니다. 이러한 스폰서 중 하나가 승인 또는 거부 링크를 클릭하면 스폰서 포털로 이동됩니다. 해당 스폰서가 자격 증명을 입력하고, 이 자격 증명이 확인됩니다. 스폰서가 속한 스폰서 그룹이 게스트 계정을 승인하도록 허용하는 경우 계정을 승인할 수 있습니다. 자격 증명 확인이 실패할 경우 Cisco ISE에서 스폰서에게 스폰서 포털에 로그온하여 계정을 수동으로 승인하도록 알립니다.

고려 사항

- 이전 버전의 Cisco ISE에서 데이터베이스를 업그레이드하거나 복구하는 경우에는 승인 또는 거부 링크를 수동으로 삽입해야 합니다. 셀프 등록 게스트 포털을 열고 Portal Page Customization(포털 페이지 사용자 맞춤화) 탭을 선택합니다. 아래로 스크롤하여 Approval Request Email(승인 요청 이메일) 창을 선택합니다. 해당 창의 **Email Body(**이메일 본문**)** 섹션에서 **Insert Approve/Deny Links(**승인/거부 링크 삽입**)**를 클릭합니다.
- Active Directory 및 LDAP로 인증하는 스폰서 포털만 지원됩니다. 스폰서가 매핑하는 스폰서 그룹은 스폰서가 속한 Active Directory 그룹을 포함해야 합니다.
- 스폰서 목록이 있으면 스폰서가 로그온한 포털이 아닌 경우에도 첫 번째 포털의 사용자 맞춤화이 사용됩니다.
- 스폰서가 승인 및 거부 링크를 사용하려면 HTM을 지원하는 이메일 클라이언트를 사용해야 합니다.
- 스폰서의 이메일 주소가 유효한 스폰서의 이메일 주소가 아닌 경우 승인 이메일이 전송되지 않습니다.

단일 클릭 스폰서 승인에 대한 자세한 내용은 Cisco ISE 커뮤니티 리소스 **ISE Single Click Sponsor Approval FAQ**를 참고하십시오. 이 문서에는 전체 프로세스를 설명하는 비디오에 대한 링크도 있습니다.

계정 승인 이메일 링크 구성

네트워크에 액세스하기 전에 셀프 등록 게스트를 승인해야 할 수 있습니다. Cisco ISE는 방문하는 사람의 이메일 주소를 사용하여 승인자에게 알립니다. 승인자는 방문 중인 사람 또는 스폰서입니다. 승인자 정의에 대한 자세한 내용은 스폰서의 셀프 등록 계정 승인, 386 페이지를 참고하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest(**게스트**)** > **Configure(**구성**)** > **Guest Portals(**게스트 포털**)**를 선택합니다. 이메일 계정 승인 링크에 대해 구성할 셀프 등록 포털을 선택합니다.

단계 **2** **Self-Registration Page Settings(**셀프 등록 페이지 설정**)** 탭을 확장합니다.

단계 **3** **Require self-registered guests to be approved(**셀프 등록한 게스트의 승인 필요**)**를 선택합니다.

Approve/Deny Link Settings(링크 설정 승인/거부**)** 섹션이 나타납니다. 또한 승인 요청 이메일의 이메일 컨피그레이션을 승인 및 거부 링크로 입력합니다.

다음 세부정보를 입력합니다.

- **Require self-registered guests to be approved(**셀프 등록한 게스트의 승인 필요**)**: 이 포털을 사용 중인 셀프 등록 게스트가 스폰서로부터 승인을 받아야 게스트 자격 증명을 받을 수 있도록 지정합니다. 이 옵션을 클릭하면 스폰서가 셀프 등록 게스트를 승인하는 방법에 대한 추가 옵션이 표시됩니다.
  - **Allow guests to login automatically from self-registration after sponsor's approval(**스폰서 승인 후 셀프 등록 게스트가 자동으로 로그인하도록 허용**)**: 스폰서가 승인하면 셀프 등록 게스트가 자동으로 로그인됩니다.
  - **Email approval request to(**승인 요청 이메일을 보낼 주소**)**:
    - **Sponsor email addresses listed below(**아래에 나와 있는 스폰서 이메일 주소**)**: 승인자로 지정된 스폰서의 이메일 주소를 하나 이상 입력하거나 모든 게스트 승인 요청을 보내야 하는 메일러를 입력합니다. 이메일 주소가 유효하지 않으면 승인이 실패합니다.
    - **Person being visited(**방문자**)**: **Require sponsor to provide credentials for authentication(**스폰서가 인증을 위해 자격 증명 제공 필요**)** 필드가 표시되며 **Fields to include(**포함할 필드**)**의 **Required(**필수**)** 옵션이 활성화됩니다(이전에 비활성화된 경우). 이러한 필드는 셀프 등록 게스트로부터 이 정보를 요청하는 셀프 등록 양식에 표시됩니다. 이메일 주소가 유효하지 않으면 승인이 실패합니다.
  - **Approve/Deny Link Settings(**링크 설정 승인/거부**)**:
    - **Links are valid for(**링크 유효 기간**)**: 계정 승인 링크의 만료 기간을 설정할 수 있습니다.
    - **Require sponsor to provide credentials for authentication(**스폰서가 인증을 위해 자격 증명 제공 필요**)**: 이 섹션의 구성에서 요구하지 않는 경우에도 스폰서가 계정 승인을 위해 자격 증명을 입력하도록 하려면 이 옵션을 선택합니다. 이 필드는 **Require self-registered guests to be approved(**셀프 등록한 게스트의 승인 필요**)**가 **person being visited(**방문자**)**로 설정된 경우에만 표시됩니다.
    - **Sponsor is matched to a Sponsor Portal to verify approval privileges(**스폰서 포털에서 스폰서의 승인 권한 확인**)**: **Details(**세부정보**)**를 클릭하여 스폰서가 유효한 시스템 사용자이고 스폰서 그룹의 멤버이며 해당 그룹의 멤버가 계정을 승인할 권한을 가졌는지 확인하기 위해 검색할 포털을 선택합니다. 각 스폰서 포털에는 스폰서를 식별하는 데 사용되는 ID 소스 시퀀스가 있습니다. 포털은 나열된 순서대로 사용됩니다. 목록의 첫 번째 포털에 따라 스폰서 포털에서 사용되는 스타일과 사용자 맞춤화이 결정됩니다.

포털 권한 부여

포털에 권한을 부여할 때는 네트워크 액세스를 위한 규칙과 네트워크 권한 부여 프로파일을 설정합니다.

시작하기 전에

포털에 권한을 부여하려면 먼저 포털을 생성해야 합니다.

단계 **1** 포털에 대해 특수 권한 부여 프로파일을 설정합니다.

단계 **2** 프로파일에 대한 권한 부여 정책 규칙을 생성합니다.

권한 부여 프로파일 생성

각 포털에서는 해당 포털용으로 특수 권한 부여 프로파일을 설정해야 합니다.

시작하기 전에

기본 포털을 사용하지 않으려는 경우에는 포털 이름을 권한 부여 프로파일과 연결할 수 있도록 먼저 포털을 생성해야 합니다.

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

단계 **2** 사용하기 위해 권한을 부여하려는 포털의 이름을 사용하여 권한 부여 프로파일을 생성합니다.

다음에 수행할 작업

새로 생성한 권한 부여 프로파일을 사용하는 포털 권한 부여 정책 규칙을 생성해야 합니다.

핫스팟 및 **MDM** 포털에 대한 권한 부여 정책 규칙 생성

사용자(게스트, 스폰서, 직원)의 액세스 요청에 응답할 때 포털에서 사용하도록 할 리디렉션 URL을 구성하려면 해당 포털용 권한 부여 정책 규칙을 정의합니다.

URL 리디렉션은 포털 유형에 따라 다음 형식을 사용합니다.

ip:*port*: IP 주소와 포트 번호입니다.

PortalID: 고유한 포털 이름입니다.

핫스팟 게스트 포털:
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

MDM(Mobile Device Management) 포털:
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

---

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택하여 **Standard(**표준**)** 정책 아래에 새 권한 부여 정책 규칙을 생성합니다.

단계 **2** **Conditions(**조건**)**에 대해 포털 검증에 사용할 엔드포인트 ID 그룹을 선택합니다. 예를 들어 핫스팟 게스트 포털의 경우 기본값인 **GuestEndpoints** 엔드포인트 ID 그룹을 선택하고 MDM 포털의 경우 기본값인 **RegisteredDevices** 엔드포인트 ID 그룹을 선택합니다.

참고 핫스팟 게스트 포털에서는 종료 CoA만 발급하므로 핫스팟 게스트 권한 부여 정책의 검증 조건 중 하나로 Network Access:UseCase EQUALS Guest Flow를 사용하지 마십시오. 대신 검증을 위해 엔드포인트가 속하는 ID 그룹을 일치시킵니다. 예를 들면 다음과 같습니다.

- `If GuestEndpoint + Wireless MAB then Permit Access`
- `If Wireless MAB then HotSpot Redirect`

단계 **3** **Permissions(**권한**)**에 대해 생성한 포털 권한 부여 프로파일을 선택합니다.

참고 MAC 옵션이 활성화된 사전 속성(예: RADIUS.Calling-Station-ID)을 사용하여 권한 부여 조건을 생성하는 동안 Mac 연산자(예: Mac_equals)로 다른 MAC 형식을 지원해야 합니다.

게스트 포털 사용자 맞춤화

포털 테마를 사용자 맞춤화하고, 포털 페이지의 UI 요소를 변경하고, 사용자에게 표시되는 오류 메시지와 알림을 편집하여 포털 모양과 사용자(해당하는 게스트, 스폰서 또는 직원) 환경을 사용자 맞춤화할 수 있습니다. 포털 사용자 맞춤화에 대한 자세한 내용은 의 최종 사용자 웹 포털 사용자 맞춤화 섹션을 참조하십시오.

정기 **AUP** 수락 구성

Policy(정책**)** > **Policy Sets(**정책 집합**)**를 선택한 다음 목록 맨 위에 새 권한 부여 규칙을 생성합니다. 이 규칙은 AUP 기간 만료 시 게스트 사용자를 자격 증명이 지정된 포털로 리디렉션합니다. 조건을 사용하여 LastAUPAcceptanceHours를 원하는 최대 시간과 비교합니다. 예를 들어 LastAUPAcceptanceHours > 8과 같이 설정합니다. 1~999시간 범위를 확인할 수 있습니다.

다음에 수행할 작업

엔드포인트가 AUP 설정을 수신했는지 확인하려면 다음을 수행합니다.

1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**.
2. 엔드포인트를 클릭하면 엔드포인트가 AUP를 마지막으로 수락한 시간(*AUPAcceptedTime*)으로 설정되어 있는지를 확인할 수 있습니다.

정기 **AUP** 강제 적용

정책에서 LastAUPAcceptance를 이용하여 사용자가 AUP를 수락하도록 강제할 수 있습니다.

```
If LastAUPAcceptance >= 24: Hotspot Redirect
If LastAUPacceptance < 24: PermitAccess
If Wireless_MAB: Hotspot Redirect
```

이 예에서는 24시간마다 핫스팟 포털에서 AUP를 강제 적용하는 방법을 보여줍니다.

1. 사용자가 24시간이 지난 후에 AUP를 수락했다면 AUP를 수락해야 합니다(다시 시작).
2. 사용자가 24시간 이내에 AUP를 수락한 경우 세션을 계속 진행합니다.
3. 네트워크에 첫 번째 액세스(MAB)하는 경우 AUP를 수락해야 합니다.

인증 포털에 대해 AUP를 활성화하는 경우 해당 포털에서 동일한 규칙을 사용할 수 있습니다.

게스트 이름 기억

이 기능을 사용하면 Cisco ISE가 보고서 및 로그에 MAC 주소 대신 게스트의 사용자 이름을 표시할 수 있습니다.

게스트가 처음 인증할 때 사용자 디바이스의 MAC 주소가 엔드포인트 그룹에 저장되고, 사용자 이름이 보고서에 사용됩니다. 사용자가 연결을 끊고 네트워크에 다시 연결하는 경우 MAC 주소가 이미 엔드포인트 그룹에 있으므로, 사용자가 다시 로그인(인증)할 필요가 없습니다. 이 경우 사용자 이름을 사용할 수 없으니 MAC 주소가 보고 및 로그에 사용됩니다.

Cisco ISE 2.3부터는 ISE가 포털 사용자 ID를 유지하고 릴리스에 따라 일부 보고에서 이를 사용합니다.

- Cisco ISE 2.3에서는 해당 기능을 구현했으나, 이 기능을 끌 수는 없습니다.
- Cisco ISE 2.4에는 **Guest(**게스트**)** > **Settings(**설정**)** > **Logging(**로깅**)**에 해당 기능을 비활성화하는 기능이 추가되었습니다. 새 설치에서는 이 기능이 기본적으로 활성화되며, 이전 릴리스를 업그레이드하거나 복구한 경우에는 비활성화됩니다.

내 정보 기억 로깅 문제에 대한 자세한 내용은 다음 Cisco ISE 커뮤니티 리소스 게스트 엔드포인트 그룹 로깅 표시를 사용한 ISE 2.3+ 내 정보 기억 게스트를 참조하십시오.

내 정보 기억 구성에 대한 자세한 내용은 다음의 Cisco ISE 게스트 액세스 구축 가이드를 참조하십시오. https://communities.cisco.com/docs/DOC-77590

각 릴리스에서 지원되는 보고 방법에 대한 자세한 내용은 해당 릴리스의 릴리스 노트를 참조하십시오.

스폰서 포털

스폰서 포털은 Cisco ISE 게스트 서비스의 주요 구성 요소 중 하나입니다. 스폰서는 스폰서 포털을 사용하여 권한 부여된 방문자가 기업 네트워크 또는 인터넷에 안전하게 액세스할 수 있도록 임시 계정을 생성하고 관리할 수 있습니다. 게스트 계정을 생성한 후 스폰서는 스폰서 포털을 사용하여 인쇄, 이메일 또는 문자 형식으로 계정 세부정보를 게스트에게 제공할 수도 있습니다. 회사 네트워크에 셀

프 등록 게스트 액세스를 제공하기 전에 먼저 스폰서는 이메일을 통해 게스트 계정을 승인해야 할 수 있습니다.

스폰서 포털에서 게스트 계정 관리

스폰서 포털 로그온 플로우

스폰서 그룹은 스폰서 사용자에게 할당되는 권한 집합을 지정합니다. 스폰서가 스폰서 포털에 로그인하는 경우 다음과 같은 작업이 발생합니다.

1. ISE가 스폰서의 자격 증명을 확인합니다.
2. 스폰서가 성공적으로 인증되면 Cisco ISE는 사용 가능한 모든 스폰서 그룹을 검색하여 스폰서가 속한 스폰서 그룹을 찾습니다. 다음의 경우 스폰서가 스폰서 그룹과 일치하거나 스폰서 그룹에 속합니다.
   - 스폰서는 구성된 멤버 그룹 중 하나의 멤버입니다.
   - 기타 조건을 사용하는 경우 해당 스폰서에 대해 모든 조건이 true로 평가됩니다.
3. 스폰서가 스폰서 그룹에 속한 경우 스폰서가 해당 그룹에서 권한을 가져옵니다. 스폰서는 둘 이상의 스폰서 그룹에 속할 수 있으며, 이 경우 해당 그룹들의 권한이 결합됩니다. 스폰서가 스폰서 그룹에 속하지 않으면 스폰서 포털에 로그인할 수 없습니다.

스폰서 그룹 및 해당 권한은 스폰서 포털과 무관합니다. 스폰서가 로그인하는 스폰서 포털에 관계없이 스폰서 그룹 일치에 동일한 알고리즘이 사용됩니다.

스폰서 포털 사용

권한이 부여된 방문자가 기업 네트워크나 인터넷에 안전하게 액세스할 수 있도록 스폰서 포털을 사용하여 임시 게스트 계정을 생성합니다. 게스트 계정을 생성한 후에는 스폰서 포털을 사용하여 이러한 계정을 관리하고 게스트에게 계정 세부정보를 제공할 수 있습니다.

스폰서 포털에서 스폰서는 새 게스트 계정을 개별적으로 생성하거나 파일에서 사용자 그룹을 가져올 수 있습니다.

참고 Active Directory와 같은 외부 ID 저장소에서 승인된 ISE 관리자도 스폰서 그룹에 속할 수 있습니다. 그러나 내부 관리자 계정(예: 기본 "admin" 계정)은 스폰서 그룹에 속할 수 없습니다.

다음과 같이 여러 방법으로 스폰서 포털을 열 수 있습니다.

- 관리자 콘솔에서 **Manage Accounts(**계정 관리**)** 링크를 사용합니다. 관리자 콘솔에서 **Guest Access(**게스트 액세스**) > Manage Accounts(**계정 관리**)**를 클릭합니다. **Manage Accounts(**계정 관리**)**를 클릭하면 ALL_ACCOUNTS에 대한 액세스 권한이 있는 기본 스폰서 그룹에 할당됩니다. 새 게스트 계정을 생성할 수는 있지만, 게스트로부터 계정 활성화 요청을 받을 수 있는 이메일 주소가 없으므로 해당 게스트에게 알림을 보내지는 못합니다. 스폰서 포털에 로그온하고 해당 계정을 검색하는 동일한 권한을 가진 스폰서는 알림을 보낼 수 있습니다.

이 단계에서는 스폰서 포털의 **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 창에서 구성한 FQDN이 DNS 서버에 있어야 합니다.

NAT 방화벽을 통해 스폰서 포털에 액세스하는 경우 연결에서 포트 9002를 사용합니다.

- 관리자 콘솔의 Sponsor Portal configuration(스폰서 포털 컨피그레이션) 창에서 **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)**를 클릭하여 스폰서 포털을 열고 **Description(**설명**)** 필드 오른쪽에 있는 **Portal Test URL(**포털 테스트 **URL)** 링크를 클릭합니다.
- 브라우저에서 스폰서 포털의 **Portal Settings(**포털 설정**)** 창에 구성된 URL(FQDN)을 열어 DNS 서버에서 정의해야 합니다.

향후 작업

스폰서 포털을 사용하는 방법에 대한 자세한 내용은 https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html에서 사용 중인 ISE 버전의 스폰서 포털 사용 설명서를 참조하십시오.

스폰서 계정 관리

스폰서 사용자는 스폰서 포털을 통해 guest-user 계정을 생성하고 관리하는 조직의 직원 또는 계약자입니다. Cisco ISE는 로컬 데이터베이스를 통해, 아니면 외부 LDAP(Lightweight Directory Access Protocol), Microsoft Active Directory 또는 SAML ID 저장소를 통해 스폰서를 인증합니다. 외부 소스를 사용하지 않는 경우 스폰서용 내부 사용자 계정을 생성해야 합니다.

스폰서 그룹

스폰서 그룹은 스폰서 포털을 사용할 때 스폰서에게 부여되는 권한을 제어합니다. 스폰서가 스폰서 그룹의 멤버인 경우 스폰서는 그룹에 정의된 권한을 갖게 됩니다.

다음 조건이 둘 다 해당될 경우 스폰서는 스폰서 그룹의 멤버로 간주됩니다.

1. 스폰서가 스폰서 그룹에 정의된 멤버 그룹 중 하나 이상에 속합니다. 멤버 그룹은 사용자 ID 그룹이거나 외부 ID 소스(예: Active Directory)에서 선택한 그룹일 수 있습니다.
2. 스폰서가 스폰서 그룹에 지정된 기타 조건을 모두 충족합니다. 기타 조건(선택 사항)은 사전 속성에 정의된 조건입니다. 이러한 조건은 권한 부여 정책에 사용되는 조건과 유사한 방식으로 적용됩니다.

스폰서는 둘 이상의 스폰서 그룹의 멤버가 될 수 있습니다. 그러한 경우 스폰서는 다음과 같이 모든 그룹에서 통합된 권한을 받습니다.

- 어떤 그룹에서든 활성화된 경우 "게스트 계정 삭제"와 같은 개별 권한이 부여됩니다.
- 스폰서는 어떤 그룹에서든 게스트 유형을 사용하여 게스트를 생성할 수 있습니다.
- 스폰서는 어떤 그룹에서든 해당 위치에 게스트를 생성할 수 있습니다.
- 배치 크기 제한과 같은 숫자 값의 경우 그룹에서 가장 큰 값이 사용됩니다.

스폰서가 어떤 스폰서 그룹이든 그 멤버가 아닌 경우 스폰서는 어떤 스폰서 포털로도 로그인할 수 없습니다.

- ALL_ACCOUNTS: 스폰서가 보류 중인 모든 게스트 계정을 관리 할 수 있습니다.
- GROUP_ACCOUNTS - 스폰서는 동일 스폰서 그룹에 속한 스폰서가 생성한 게스트 계정을 관리할 수 있습니다.
- OWN_ACCOUNTS: 스폰서는 자신이 생성한 게스트 계정만 관리할 수 있습니다.

특정 스폰서 그룹이 사용할 수 있는 기능을 사용자 맞춤화하여 스폰서 포털의 기능을 제한하거나 확장할 수 있습니다.

스폰서 계정을 생성하여 스폰서 그룹에 할당

내부 스폰서 사용자 계정을 생성하고 스폰서 포털을 사용할 수 있는 스폰서를 지정하려면 다음을 수행합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다. 적절한 사용자 ID 그룹에 내부 스폰서 사용자 계정을 할당합니다.

참고 기본 스폰서 그룹의 경우 기본 ID 그룹 Guest_Portal_Sequence가 할당됩니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Groups(**스폰서 그룹**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)**를 선택하고 **Members(**멤버**)**를 클릭합니다. 스폰서 사용자 ID 그룹을 스폰서 그룹에 매핑합니다.

다음에 수행할 작업

스폰서에 사용할 조직 전용 추가 사용자 ID 그룹을 생성할 수도 있습니다. 이렇게 하려면 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **User Identity Groups(**사용자 **ID** 그룹**)**를 선택합니다.

스폰서 그룹 구성

Cisco는 기본 스폰서 그룹을 제공합니다. 기본 옵션을 사용하지 않으려는 경우에는 새 스폰서 그룹을 생성하거나 기본 스폰서 그룹을 편집하여 설정을 변경할 수 있습니다. 또한 스폰서 그룹을 복제해 동일 설정 및 권한으로 스폰서 그룹을 생성할 수도 있습니다.

스폰서 그룹은 비활성화할 수 있으며, 이 경우 스폰서 그룹의 멤버가 스폰서 포털에 로그인할 수 없습니다. Cisco ISE에서 제공하는 기본 스폰서 그룹을 제외한 모든 스폰서 그룹은 삭제할 수 있습니다.

단계 **1** **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Groups(**스폰서 그룹**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Sponsor group name(**스폰서 그룹 이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **3** **Match Criteria(**일치 기준**)** 섹션에서 다음 세부정보를 입력합니다.

- **Member Groups(**멤버 그룹**)**: **Members(**멤버**)**를 클릭하여 외부 ID 소스에서 하나 이상의 사용자(ID) 그룹을 선택하고 해당 그룹을 추가합니다. 사용자가 이 스폰서 그룹의 멤버가 되려면 구성된 그룹 중 하나 이상에 속해야 합니다.
- **Other conditions(**기타 조건**)**: **Create New Condition(**새 조건 생성**)**을 클릭해, 스폰서가 이 스폰서 그룹에 포함시킬 수 있도록 일치시켜야 하는 한 개 이상의 조건을 설정합니다. Active Directory, LDAP, SAML, ODBC ID 저장소(RADIUS Token 또는 RSA SecurID 저장소는 불가능)의 인증 속성을 사용할 수 있습니다. 내부 사용자 속성을 사용할 수도 있습니다. 조건에는 속성, 연산자, 값이 있습니다.
  - 내부 사전 속성 *Name(*이름*)*을 사용해 조건을 생성하려면 사용자 ID 그룹을 ID 그룹 이름의 접두사로 사용해야 합니다. 예를 들면 다음과 같습니다.

    InternalUser:Name EQUALS bsmith

    즉, "bsmith"라는 이름을 가진 내부 사용자만 이 스폰서 그룹에 속할 수 있는 것입니다.
  - Active Directory 인스턴스의 ExternalGroups 속성을 사용하여 조건을 생성하려면 일치시킬 스폰서 사용자에 대해 AD "Primary Group"을 선택합니다. 예를 들어 사용자 이름이 Smith인 경우 *AD1:LastName EQUALS Smith*는 true입니다.

하나 이상의 구성된 멤버 그룹과 일치하는 것 외에도 스폰서는 여기에서 생성하는 모든 조건과 일치해야 합니다. 인증 스폰서 사용자가 여러 스폰서 그룹에 대한 일치 기준을 충족하는 경우 해당 사용자에게 다음과 같은 권한이 부여됩니다.

- 일치하는 그룹에서 활성화된 경우 게스트 계정 삭제와 같은 개별 권한이 부여됩니다.
- 스폰서는 일치하는 그룹에서 게스트 유형을 사용하여 게스트를 생성할 수 있습니다.
- 스폰서는 일치하는 그룹에서 게스트 유형을 사용하여 게스트를 생성할 수 있습니다.
- 스폰서는 일치하는 그룹에서 해당 위치에 게스트를 생성할 수 있습니다.
- 배치 크기 제한과 같은 숫자 값의 경우 일치하는 그룹에서 가장 큰 값이 사용됩니다.

멤버 그룹만 포함하거나 다른 조건만 포함하는 일치 기준을 생성 할 수 있습니다. Other Conditions(기타 조건)만 지정하는 경우 스폰서 그룹의 스폰서 자격은 일치하는 사전 속성에 의해 결정됩니다.

단계 **4** 이 스폰서 그룹을 기준으로 하는 스폰서가 생성할 수 있는 게스트 유형을 지정하려면 **This sponsor group can create accounts using these guest types(**이 스폰서 그룹이 계정을 생성하는 데 사용할 수 있는 게스트 유형**)**를 클릭하고 게스트 유형을 하나 이상 선택합니다.

Create Guest Types at(게스트 유형을 생성할 위치**)** 아래의 링크를 클릭하여 이 스폰서 그룹에 할당할 추가 게스트 유형을 생성할 수 있습니다. 새 게스트 유형을 생성한 후에는 스폰서 그룹을 저장하고 닫았다가 다시 열어야 해당 새 게스트 유형을 선택할 수 있습니다.

단계 **5** **Select the locations that guests will be visiting(**게스트가 방문할 위치 선택**)**을 사용하여 이 스폰서 그룹의 스폰서가 게스트 계정을 생성할 때 선택할 수 있는 위치(게스트 표준 시간대를 설정하는 데 사용됨)를 지정합니다.

Configure guest locations at(게스트 위치를 구성할 위치**)** 아래의 링크를 클릭하고 게스트 위치를 추가하여 선택할 수 있는 위치를 더 추가할 수 있습니다. 새 게스트 위치를 생성한 후에는 스폰서 그룹을 저장하고 닫았다가 다시 열어야 해당 새 게스트 위치를 선택할 수 있습니다.

이렇게 해도 게스트는 다른 위치에서 로그인할 수 있습니다.

단계 **6** 스폰서를 저장하려면 **Automatic guest notification(**자동 게스트 알림**)**에서 **Automatically email guests upon account creation if email address is available(**계정 생성 시 이메일 주소를 사용할 수 있는 경우 자동으로 게스트에게 이메일 보내기을 선택하고 사용자를 생성한 후 **Notify(**알림**)**를 클릭합니다. 그러면 이메일이 전송되었다는 팝업 창이 나타납니다. 또한 이 옵션을 선택하면 스폰서 포털에 게스트 알림이 자동으로 전송된다는 헤더가 추가됩니다.

단계 **7** **Sponsor Can Create(**스폰서가 생성할 수 있는 계정**)**에서 이 그룹의 스폰서가 게스트 계정 생성 시 사용할 수 있는 옵션을 구성합니다.

- **Multiple guest accounts assigned to specific guests (Import)(**특정 게스트에 할당되는 여러 게스트 계정**(**가져오기**))**: 스폰서가 이름, 성 등의 게스트 세부정보를 파일에서 가져와 여러 게스트 계정을 생성하는 기능을 활성화합니다.

  이 옵션을 활성화하면 **Import(**가져오기**)** 옵션이 스폰서 포털의 **Create Account(**계정 생성**)** 창에 표시됩니다. Import(가져오기) 옵션은 Internet Explorer, Firefox, Safari 등의 데스크톱 브라우저에서만 사용 가능하며 모바일에서는 사용할 수 없습니다.

- **Limit to batch of(**다음의 배치로 제한**)**: 이 스폰서 그룹이 여러 계정을 동시에 생성할 수 있는 경우 단일 가져오기 작업에서 생성할 수 있는 게스트 계정의 수를 지정합니다.

  스폰서는 최대 10,000개의 계정을 생성할 수 있지만 성능 문제가 발생할 가능성이 있으므로 생성하는 계정 수를 제한하는 것이 좋습니다.

- **Multiple guest accounts to be assigned to any guests (Random)(**임의의 게스트에 할당되는 여러 게스트 계정 **(**임의**))**: 스폰서가 아직 확인되지 않은 게스트에 대해 임의 게스트 계정을 자리 표시자로 생성하거나 많은 수의 계정을 빠르게 생성할 수 있도록 합니다.

  이 옵션을 활성화하면 **Random(**임의**)** 옵션이 스폰서 포털의 **Create Accounts(**계정 생성**)** 창에 표시됩니다.

- **Default username prefix(**기본 사용자 이름 접두사**)**: 여러 임의 게스트 계정을 생성할 때 스폰서가 사용할 수 있는 사용자 이름 접두사를 지정합니다. 이 접두사는 지정하는 경우 임의 게스트 계정을 생성할 때 스폰서 포털에 나타납니다. 또한 **Allow sponsor to specify a username prefix(**스폰서의 사용자 이름 접두사 지정 허용**)** 옵션의 설정에 따라 결과가 다음과 같이 달라집니다.

  - Enabled(활성화됨): 스폰서가 스폰서 포털에서 기본 접두사를 편집할 수 있습니다.
  - Not enabled(활성화 안 함): 스폰서가 스폰서 포털에서 기본 접두사를 편집할 수 없습니다.

  사용자 이름 접두사를 지정하지 않거나 스폰서가 접두사를 지정하도록 허용하지 않으면 스폰서는 스폰서 포털에서 사용자 이름 접두사를 할당할 수 없습니다.

- **Allow sponsor to specify a username prefix(**스폰서의 사용자 이름 접두사 지정 허용**)** 이 스폰서 그룹이 여러 계정을 동시에 생성할 수 있는 경우 단일 가져오기 작업에서 생성할 수 있는 게스트 계정의 수를 지정합니다.

  스폰서는 최대 10,000개의 계정을 생성할 수 있지만 성능 문제가 발생할 가능성이 있으므로 생성하는 계정 수를 제한하는 것이 좋습니다.

단계 **8** **Sponsor Can Manage(**스폰서가 관리할 수 있는 계정**)**에서는 이 스폰서 그룹의 멤버가 보고 관리할 수 있는 게스트 계정을 제한할 수 있습니다.

- **Only accounts sponsor has created(**스폰서가 생성한 계정만**)**: 이 그룹의 스폰서가 스폰서의 이메일 계정을 기준으로 하여 자신이 생성한 게스트 계정만 보고 관리할 수 있습니다.
- **Accounts created by members of this sponsor group(**이 스폰서 그룹의 멤버가 생성한 계정**)**: 스폰서가 이 스폰서 그룹의 모든 스폰서에 의해 생성된 게스트 계정을 보고 관리할 수 있습니다.
- **All guest accounts(**모든 게스트 계정**)**: 스폰서가 보류 중인 모든 게스트 계정을 관리 할 수 있습니다.

단계 **9** **Sponsor Can(**스폰서가 수행할 수 있는 작업**)**에서는 이 스폰서 그룹의 멤버에게 게스트 비밀번호 및 계정과 관련된 추가 권한을 제공할 수 있습니다.

- **Update guests' contact information (email, Phone Number)(**게스트 연락처 정보 업데이트**(**이메일**,** 전화 번호**))**: 스폰서가 관리할 수 있는 게스트 계정에 대해 게스트의 연락처 정보를 변경할 수 있도록 허용합니다.
- **View/print guests 'passwords(**게스트 비밀번호 보기/인쇄**)**: 이 옵션을 활성화하면 스폰서가 게스트의 비밀번호를 인쇄할 수 있습니다. 스폰서는 **Manage Accounts(**계정 관리**)** 창과 게스트의 세부정보에서 게스트의 비밀번호를 볼 수 있습니다. 이 옵션을 선택하지 않으면 스폰서는 비밀번호를 인쇄할 수 없지만 사용자는 그대로 이메일 또는 SMS를 통해 비밀번호를 가져올 수 있습니다(구성된 경우).
- **Send SMS notifications with guests' credentials(**게스트 자격 증명을 사용하여 **SMS** 알림 보내기**)**: 스폰서가 관리 가능한 게스트 계정에 대해 게스트의 계정 세부정보 및 로그인 자격 증명을 사용하여 게스트에게 SMS(텍스트) 알림을 보낼 수 있도록 허용합니다.
- **Reset guest account passwords(**게스트 계정 비밀번호 재설정**)**: 스폰서가 관리 가능한 게스트 계정에 대해 게스트의 비밀번호를 Cisco ISE에서 생성된 임의의 비밀번호로 재설정할 수 있도록 허용합니다.
- **Extend guests' accounts(**게스트 계정 연장**)**: 스폰서가 관리 가능한 게스트 계정을 만료 날짜 이후로 연장할 수 있도록 허용합니다. 스폰서는 계정 만료와 관련하여 게스트에게 전송되는 이메일 알림에 자동으로 복사됩니다.
- **Delete guests' accounts(**게스트 계정 삭제**)**: 스폰서가 관리 가능한 게스트 계정을 삭제하고 게스트의 회사 네트워크 액세스를 차단할 수 있도록 허용합니다.
- **Suspend guests' accounts(**게스트 계정 일시 중지**)**: 스폰서가 관리 가능한 게스트 계정을 일시 중지하여 게스트의 로그인을 일시적으로 차단할 수 있도록 허용합니다.

  이 동작을 수행하는 경우 CoA(Change of Authorization)도 실행되어 일시 중지된 게스트가 네트워크에서 제거됩니다.

  - **Require sponsor to provide a reason(**스폰서가 이유를 제공해야 함**)**: 스폰서가 게스트 계정 일시 중지에 대한 설명을 제공해야 합니다.

- **Approve and view requests from self-registering guests(**셀프 등록 게스트의 요청 승인 및 보기**)**: 이 스폰서 그룹에 포함되어 있는 스폰서는 셀프 등록 게스트(승인 필요)의 보류 중인 모든 계정 요청을 볼 수 있거나, 사용자가 방문 중인 사용자로서 스폰서 이메일 주소를 입력한 요청만 볼 수 있습니다. 이 기능을 사용하려면 셀프 등록 게스트가 사용하는 포털에서 **Require self-registered guests to be approved(**셀프 등록 게스트를 승인해야 함**)**를 선택해야 하며 스폰서의 이메일이 연락 대상으로 나열되어 있어야 합니다.

- 모든 보류 중인 계정: 이 그룹에 속한 스폰서는 모든 스폰서가 생성한 어카운트를 승인하고 검토합니다.
- 이 스폰서에게 할당된 보류 중인 계정만: 이 그룹에 속한 스폰서가 자신이 생성한 계정만 보고 승인할 수 있습니다.

- **Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)(**프로그래밍 인터페이스**(**게스트 **REST API)**를 사용하여 **Cisco ISE** 게스트 계정에 액세스**)**: 스폰서가 관리 가능한 게스트 계정에 대해 게스트 REST API 프로그래밍 인터페이스를 사용하여 게스트 계정에 액세스할 수 있도록 허용합니다.

단계 **10** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

스폰서 계정 생성을 위한 계정 콘텐츠 구성

게스트 및 스폰서가 새 게스트 계정을 생성하기 위해 제공해야 하는 사용자 데이터 유형을 구성할 수 있습니다. 일부 필드는 ISE 계정을 식별하는 데 필요하지만 그 외의 필드는 제거할 수 있으며 사용자 맞춤화 필드를 추가할 수도 있습니다.

스폰서가 계정을 생성하도록 필드를 구성하려면 다음을 수행하십시오.

1. **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)**를 선택하고 스폰서 포털을 편집합니다.Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고
2. **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 선택합니다.
3. 아래로 스크롤하여 **Create Account for Known Guest(**알려진 게스트의 계정 생성**)**를 선택합니다.
4. 오른쪽의 미리보기 화면에서 **Settings(**설정**)**를 선택합니다.

이러한 설정에 따라 스폰서 포털에서 생성 될 때 표시되는 필드와 게스트 계정에 필요한 필드가 결정됩니다. 이 구성은 알려진 게스트, 임의 게스트 및 가져온 게스트 유형에 적용됩니다. 스폰서가 새 사용자를 가져오기 위해 다운로드하는 템플릿은 동적으로 생성되므로 알려진 게스트에 설정된 필드만 포함됩니다.

계정의 사용자 이름 및 비밀번호 가져오기

스폰서는 사용자 이름과 비밀번호를 가져올 수 있지만, 스폰서가 CSV 템플릿을 다운로드할 때 해당 행이 템플릿에 추가되지 않습니다. 스폰서는 해당 제목을 추가할 수 있습니다. ISE가 열을 인식할 수 있도록 이름을 올바르게 지정해야 합니다.

- Username - *User Name* 또는 *UserName*이 될 수 있습니다.
- Password - **`password`**가 되어야 합니다.

스폰서 포털에 대한 특수 설정

다음 설정은 스폰서 포털의 Create Account for Imported Guest(가져온 게스트에 대해 계정 생성) 페이지에 있는 Portal Page Customization(포털 페이지 사용자 맞춤화) 탭에 고유한 설정입니다.

- **Allow sponsor to be copied in Guest Credentials email(**게스트 자격 증명 이메일을 스폰서에게 참조로 보낼 수 있음**)**: 이 옵션을 활성화하면 정상적으로 가져온 게스트에게 전송된 게스트 자격 증명의 각 이메일이 스폰서에게도 전송됩니다. 기본값은 스폰서에게 이메일을 보내지 않는 것입니다.
- **Allow sponsor to receive summary email(**스폰서가 요약 이메일을 수신할 수 있음**)**: 스폰서가 사용자 목록을 가져오면 ISE는 가져온 모든 사용자의 요약이 포함된 단일 이메일을 전송합니다. 이 옵션의 선택을 취소하면 스폰서는 가져온 각 사용자에 대해 별도의 이메일을 받습니다.

스폰서 포털 플로우 구성

기본 포털 및 해당 기본 설정(예: 인증서, 엔드포인트 ID 그룹, ID 소스 시퀀스, 포털 테마, 이미지 및 Cisco ISE가 제공하는 기타 세부정보)을 사용할 수 있습니다. 기본 설정을 사용하지 않으려면 새 포털을 생성하거나 자신의 요구 사항에 맞게 기존 포털을 편집해야 합니다. 여러 포털을 생성하려는 경우 동일한 설정을 사용하여 포털을 복제할 수 있습니다.

회사의 사무소 및 소매점 위치마다 브랜드가 각기 다르거나, 회사의 제품 브랜드가 여러 개이거나, 해당 구/군/시 사무소에서 소방서, 경찰서 및 기타 다른 부서에 대해 다른 테마가 지정된 포털을 사용하려는 경우 여러 스폰서 포털을 생성할 수 있습니다.

스폰서 포털 구성과 관련된 작업은 다음과 같습니다.

시작하기 전에

스폰서 그룹 구성, 394 페이지에 나온 대로 사이트에 대한 기존 스폰서 그룹을 구성하거나 수정합니다.

단계 **1** 정책 서비스 활성화, 399 페이지.
단계 **2** 게스트 서비스용 인증서 추가, 400 페이지.
단계 **3** 외부 ID 소스 생성, 400 페이지.
단계 **4** ID 소스 시퀀스 생성, 401 페이지.
단계 **5** 스폰서 포털 생성, 402 페이지.
단계 **6** (선택 사항) 스폰서 포털 사용자 맞춤화, 402 페이지.

정책 서비스 활성화

Cisco ISE 최종 사용자 포털을 지원하려면 해당 포털을 호스트하려는 노드에서 포털 정책 서비스를 활성화해야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .
단계 **2** 노드를 클릭하고 **Edit(**편집**)**를 클릭합니다.
단계 **3** **General Settings(**일반 설정**)** 탭에서 **Policy Service(**정책 서비스**)** 토글 버튼을 활성화합니다.

단계 4 **Enable Session Services(**세션 서비스 활성화**)** 확인란을 선택합니다.

단계 5 **Save(**저장**)**를 클릭합니다.

게스트 서비스용 인증서 추가

기본 인증서를 사용하지 않으려는 경우 유효한 인증서를 추가하고 인증서 그룹 태그에 할당할 수 있습니다. 모든 최종 사용자 웹 포털에 사용되는 기본 인증서 그룹 태그는 기본 포털 인증서 그룹입니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

단계 2 시스템 인증서를 추가한 다음 포털에 사용하려는 인증서 그룹 태그에 할당합니다.

포털 생성 또는 편집 시에 이 인증서 그룹 태그를 선택할 수 있습니다.

단계 3 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Create or Edit(**생성 또는 편집**)** > **Portal Settings(**포털 설정**)**를 선택합니다.

단계 4 새로 추가한 인증서와 연결된 특정 인증서 그룹 태그를 **Certificate Group Tag(**인증서 그룹 태그**)** 드롭다운 목록에서 선택합니다.

외부 ID 소스 생성

Cisco ISE는 Active Directory LDAP, RADIUS 토큰 및 RSA SecurID 서버와 같은 외부 ID 소스에 연결하여 인증 및 권한 부여를 위한 사용자 정보를 가져올 수 있습니다. 외부 ID 소스에는 인증서 기반 인증에 필요한 인증서 인증 프로파일도 포함되어 있습니다.

참고 인증된 사용자 ID를 수신하고 공유할 수 있는 패시브 ID 서비스를 사용하려면 추가 패시브 ID 서비스 제공자, 596 페이지의 내용을 참조하십시오.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)**를 선택합니다.

단계 2 다음 옵션 중 하나를 선택합니다.

- 인증서 기반 인증의 경우 **Certificate Authentication Profile(**인증서 인증 프로파일**)**을 선택합니다.
- 외부 ID 소스로 Active Directory에 연결하려는 경우 **Active Directory**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 Active Directory, 540 페이지를 참조하십시오.
- LDAP ID 소스를 추가하려는 경우 **LDAP**를 선택합니다. 자세한 내용은 LDAP, 640 페이지를 참조하십시오.
- RADIUS 토큰 서버를 추가하려는 경우 **RADIUS** 토큰을 선택합니다. 자세한 내용은 RADIUS 토큰 ID 소스, 665 페이지를 참조하십시오.

- RSA SecurID 서버를 추가하려는 경우 **RSA SecurID**를 선택합니다. 자세한 내용은 RSA ID 소스, 672 페이지를 참조하십시오.
- Oracle Access Manager 등의 IdP(Identity Provider)를 추가하려는 경우 **SAML Id Provider(SAML ID 제공자)**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 SAMLv2 ID 제공자, 679 페이지를 참조하십시오.
- 소셜 로그인(예: Facebook 등)을 외부 ID 소스로 추가하려면 **Social Login(소셜 로그인)**을 선택합니다. 자세한 내용은 셀프 등록 게스트의 소셜 로그인, 371 페이지을(를) 참조하십시오.

ID 소스 시퀀스 생성

시작하기 전에

Cisco ISE에서 외부 ID 소스를 구성했는지 확인합니다.

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

게스트 사용자가 로컬 WebAuth를 통해 인증하도록 허용하려면 게스트 포털 인증 소스와 ID 소스 시퀀스가 동일한 ID 저장소를 포함하도록 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **Identity Management(ID 관리)** > **Identity Source Sequences(ID 소스 시퀀스)** > **Add(추가)**를 선택합니다.

단계 **2** ID 소스 시퀀스의 이름을 입력합니다. 원하는 경우 설명을 입력할 수도 있습니다.

단계 **3** **Select Certificate Authentication Profile(인증서 인증 프로파일 선택)** 확인란을 선택하고 인증서 기반 인증용 인증서 인증 프로파일을 선택합니다.

단계 **4** ID 소스 시퀀스에 포함할 하나 이상의 데이터베이스를 **Selected List(선택됨 목록)** 필드에서 선택합니다.

단계 **5** Cisco ISE가 데이터베이스를 검색하도록 할 순서대로 **Selected List(선택됨 목록)** 필드의 데이터베이스를 다시 정렬합니다.

단계 **6** **Advanced Search List(고급 검색 목록)** 영역에서 다음 옵션 중 하나를 선택합니다.

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError(시퀀스의 다른 저장소에 액세스하지 않고 AuthenticationStatus 속성을 ProcessError로 설정)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 검색을 중지하도록 하려면 이 옵션을 선택합니다.
- **Treat as if the user was not found and proceed to the next store in the sequence(사용자를 찾지 못한 것으로 간주하여 다음 저장소로 순차 진행)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 시퀀스에서 선택한 다른 ID 소스에서 검색을 계속하도록 하려면 이 옵션을 선택합니다.

  요청을 처리하는 동안 Cisco ISE는 이러한 ID 소스를 순서대로 검색합니다. Selected list(선택됨 목록) 필드의 ID 소스가 Cisco ISE가 검색하도록 할 순서대로 나열되어 있는지 확인합니다.

단계 **7** ID 소스 시퀀스를 생성하려면 **Submit(제출)**을 클릭합니다. 생성된 시퀀스는 정책에서 사용할 수 있습니다.

스폰서 포털 생성

네트워크에 연결하여 인터넷 및 내부 리소스와 서비스에 액세스하려는 게스트를 위해 스폰서가 계정을 생성, 관리 및 승인할 수 있도록 스폰서 포털을 제공할 수 있습니다.

Cisco ISE는 다른 스폰서 포털을 생성하지 않고 사용할 수 있는 기본 스폰서 포털을 제공합니다. 그러나 새 스폰서 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. 기본 스폰서 포털을 제외한 모든 포털은 삭제할 수 있습니다.

Portal Behavior and Flow Settings(포털 동작 및 흐름 설정**)** 탭의 페이지 설정에서 수행하는 모든 변경사항은 스폰서 흐름 다이어그램의 그래픽 흐름에 반영됩니다. AUP 페이지 등의 페이지를 활성화하면 해당 페이지가 흐름에 나타나며, 스폰서가 포털에서 해당 페이지를 사용할 수 있습니다. 비활성화하는 페이지는 흐름에서 제거되며 다음으로 활성화하는 페이지가 스폰서에게 표시됩니다.

시작하기 전에

이 포털에 사용할 필요한 인증서, 외부 ID 소스 및 ID 소스 시퀀스를 구성했는지 확인해 주십시오.

단계 **1** **Portal Settings(**포털 설정**)** 페이지를 스폰서 포털용 포털 설정, 435 페이지의 설명에 따라 구성합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **2** **Login Settings(**로그인 설정**)** 페이지를 스폰서 포털용 로그인 설정, 438 페이지의 설명에 따라 구성합니다.

단계 **3** **Acceptable Use Policy (AUP) Page Settings(AUP** 페이지 설정**)** 페이지를 스폰서 포털용 AUP(Acceptable Use Policy) 설정, 439 페이지의 설명에 따라 구성합니다.

단계 **4** **Sponsor Change Password Settings(**스폰서 비밀번호 변경 설정**)** 옵션을 스폰서 포털용 스폰서 비밀번호 변경 설정, 439 페이지의 설명에 따라 구성합니다.

단계 **5** **Post-Login Banner Page Settings(**로그인 후 배너 페이지 설정**)** 페이지를 스폰서 포털용 로그인 후 배너 설정 , 440 페이지의 설명에 따라 구성합니다.

단계 **6** 포털을 사용자 맞춤화하려면 **Sponsor Portal Application Settings(**스폰서 포털 애플리케이션 설정**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

스폰서 포털 사용자 맞춤화

포털 테마를 사용자 맞춤화하고, 포털 페이지의 UI 요소를 변경하고, 사용자에게 표시되는 오류 메시지와 알림을 편집하여 포털 모양과 사용자 환경을 사용자 맞춤화할 수 있습니다. 웹 포털 맞춤화에 대한 자세한 내용은 최종 사용자 웹 포털의 사용자 맞춤화 , 449 페이지를 참고하십시오.

스폰서 계정 생성을 위한 계정 콘텐츠 구성

게스트 및 스폰서가 새 게스트 계정을 생성하기 위해 제공해야 하는 사용자 데이터 유형을 구성할 수 있습니다. 일부 필드는 ISE 계정을 식별하는 데 필요하지만 그 외의 필드는 제거할 수 있으며 사용자 맞춤화 필드를 추가할 수도 있습니다.

스폰서가 계정을 생성하도록 필드를 구성하려면 다음을 수행하십시오.

1. **Work Centers(**작업 센터**) > Guest Access(**게스트 액세스**) > Portals & Components(**포털 및 구성 요소**)**를 선택하고 스폰서를 편집합니다.
2. **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 선택합니다.
3. 아래로 스크롤하여 **Create Account for Known Guest(**알려진 게스트의 계정 생성**)**를 선택합니다.

   오른쪽의 Preview(미리보기) 화면에서 **Settings(**설정**)**를 선택합니다. 이러한 설정에 따라 스폰서 포털에서 게스트 계정을 생성하는 경우 게스트 계정에 표시되고 필요한 필드가 결정됩니다.

이 구성은 알려진 게스트, 임의 게스트 및 가져온 게스트 유형에 적용됩니다. 스폰서가 새 사용자를 가져오기 위해 다운로드하는 템플릿은 동적으로 생성되므로 알려진 게스트에 설정된 필드 만 포함됩니다.

스폰서 계정 사용자 이름 및 비밀번호 가져오기

스폰서는 사용자 이름과 비밀번호를 가져올 수 있지만, 스폰서가 템플릿을 다운로드할 때 해당 행이 템플릿에 추가되지 않습니다. 스폰서는 해당 제목을 추가할 수 있습니다. Cisco ISE가 열을 인식할 수 있도록 이름을 올바르게 지정해야 합니다.

- **Username**: **`User Name`** 또는 **`UserName`**이 될 수 있습니다.
- **Password**: password가 되어야 합니다.

스폰서가 사용할 수 있는 시간 설정 구성

스폰서가 새 게스트 계정을 생성할 때 계정이 활성화되는 시간을 구성합니다. 스폰서가 계정 유지 기간, 시작 및 종료 시간을 설정할 수 있도록 스폰서가 사용할 수 있는 옵션을 구성합니다. 이러한 옵션은 게스트 유형별로 구성됩니다. 스폰서는 **Access Information(**액세스 정보**)** 아래에서 결과를 볼 수 있습니다.

스폰서 포털 계정 시간 옵션을 제어하는 게스트 유형 설정은 **Maximum Access Time(**최대 액세스 시간**)**에 있습니다. 옵션 설명은 다음과 같습니다.

- **From first login(**첫 번째 로그인**)**: 스폰서 포털에 첫 번째 로그인 이후에 계정이 활성화된 기간이 표시됩니다.

  게스트 유형 설정 **Maximum Account Duration(**최대 계정 유지 기간**)**은 스폰서가 기간에 입력할 수 있는 값을 결정합니다.

- **From sponsor-specified date(**스폰서 지정 날짜**)(**또는 해당하는 경우 셀프 등록 날짜**)**: 스폰서는 기간을 영업일 종료로 설정하거나 해당 필드를 선택 취소하여 기간, 시작 및 종료 시간을 선택할 수 있습니다.

  기간 및 유효 날짜를 제어하기 위한 게스트 유형 설정은 **Allow access only on these days and times(**다음 요일과 시간에만 액세스 허용**)** 아래에 있습니다.

  - 선택한 요일은 스폰서의 일정표에서 고를 수 있는 날짜를 제한합니다.
  - 기간 및 날짜를 선택하면 스폰서 포털에 최대 계정 유지 기간이 적용됩니다.

스폰서 포털에 대한 **Kerberos** 인증

Kerberos를 사용하여 스폰서 포털에 액세스하기 위해 Windows에 로그온한 스폰서 사용자를 인증하도록 Cisco ISE를 구성할 수 있습니다. 이 프로세스에서는 Kerberos 티켓에 로그인한 스폰서 사용자의 Active Directory 자격 증명을 사용합니다. Kerberos SSO는 브라우저가 Cisco ISE와의 SSL 연결을 설정한 후 보안 터널 내부에서 수행됩니다.

다음 항목은 동일한 Active Directory 도메인에 있어야 합니다.

- 스폰서의 PC
- ISE PSN
- 이 스폰서 포털에 대해 구성된 FQDN

이 요구 사항은 Microsoft가 Active Directory 포리스트 전체에서 양방향 트러스트를 사용하는 Kerberos SSO를 지원하지 않기 때문입니다.

스폰서 사용자는 Windows에 로그온해야 합니다.

Kerberos 인증은 게스트 포털에 대해 지원되지 않습니다.

Kerberos 구성

스폰서 포털에서 Kerberos를 활성화하려면 **Sponsor Settings and Customization(**스폰서 설정 및 사용자 맞춤화**)** 창에서 **Allow Kerberos SSO(Kerberos SSO** 허용**)** 확인란을 선택합니다.

스폰서의 브라우저도 올바르게 구성해야 합니다. 다음 섹션에서는 각 브라우저를 수동으로 구성하는 방법을 설명합니다.

참고 Active Directory의 사용자 이름과 사용자 계정 이름이 일치해야 합니다. SSO는 사용자의 세션을 식별하는 데 사용자 계정 이름을 사용합니다.

참고 브라우저에서 스폰서 포털 FQDN을 사용하여 스폰서 포털에 액세스하는 동안 Cisco ISE는 구성된 스폰서 포털 FQDN 대신 PSN FQDN으로 요청을 리디렉션합니다.

예를 들어 스폰서 포털 FQDN이 `sponsor.example.com`이고 PSN FQDN이 `psn.example.com`인 경우 브라우저에서 `https://sponsor.example.com`에 액세스를 시도하면 `https://ise.example.com:8445/sponsorportal/PortalSetup.action?portal=b7e7d773-7bb3-442b-a50b-42837c12248a`로 리디렉션됩니다.

이 동작은 **Kerberos SSO** 허용 옵션을 활성화한 경우에만 발생합니다.

Firefox를 수동으로 구성하려면

1. 주소 표시줄에 `about:config`를 입력합니다.
2. 나타나는 경고를 무시하고 Continue(계속)를 클릭하여 진행합니다.

3. 검색 창에서 `negotiate`를 검색합니다.
4. `network.negotiate-auth.delegation-uris` 및 `network.negotiate-auth.trusted-uris`에 FQDN을 추가합니다. 각 속성의 URL 목록은 쉼표로 구분됩니다.
5. 탭을 닫습니다. 브라우저를 사용할 수 있으므로 재시작할 필요가 없습니다.

Internet Explorer를 수동으로 구성하려면

1. 오른쪽 상단의 기어를 클릭하고 **Internet Options(**인터넷 옵션**)**를 선택합니다.
2. **Security(**보안**)** 탭을 클릭합니다.
3. **Local Intranet(**로컬 인트라넷**)**을 클릭합니다.
4. **Sites(**사이트**)**를 클릭하고 **Advanced(**고급**)**를 클릭합니다.
5. `<mydomain>.com`이라는 문자열을 추가합니다. 여기서 `<mydomain>`은 스폰서 포털 FQDN의 와일드카드입니다. 또는 FQDN을 입력할 수도 있습니다.
6. **Close(**닫기**)**, **OK(**확인**)**를 차례로 클릭합니다.
7. **Advanced(**고급**)** 탭을 클릭합니다.
8. 아래로 스크롤하여 **Security(**보안**)** 섹션으로 이동해 **Enable Integrated Windows Authentication(**통합 **Windows** 인증 활성화**)** 확인란을 선택합니다.
9. 컴퓨터를 다시 시작합니다.

Chrome에서 Internet Explorer의 구성을 가져옵니다.

문제 해결

- 명령 프롬프트에서 `set user`를 실행하여 시스템이 적절한 AD 도메인에 연결되어 있는지 확인합니다.
- 캐시된 Kerberos 티켓 및 호스트 이름 목록을 보려면 명령 프롬프트에서 `klist`를 실행합니다.
- SPNEGO 토큰 데이터를 확인합니다. NTLM 비밀번호 기반 토큰 문자열은 Kerberos 토큰 문자열보다 훨씬 짧습니다. 올바른 토큰 문자열이라면 한 줄에 들어가지 않습니다.
- Kerberos 요청(있는 경우)을 캡처하려면 `kerberos` 필터를 통해 Wireshark를 사용합니다.

참고 Kerberos SSO 옵션이 활성화된 경우 Kerberos SSO가 제대로 작동하려면 노드 FQDN을 통해 스폰서 포털에 액세스해야 합니다. 스폰서 포털에 대해 포털 FQDN이 구성된 경우 사용자가 포털 FQDN에 연결하면 노드 FQDN에 의해 포털로 리디렉션됩니다.

스폰서가 스폰서 포털에 로그인할 수 없음

문제

스폰서가 스폰서 포털에 로그인하려고 하면 다음 오류 메시지가 표시됩니다.

"Invalid username or password. Please try again."

원인

- 스폰서가 잘못된 자격 증명을 입력했습니다.
- 데이터베이스(내부 사용자 또는 Active Directory)에 사용자 기록이 없으므로 스폰서가 유효하지 않습니다.
- 스폰서가 속하는 스폰서 그룹이 비활성화되었습니다.
- 스폰서의 사용자 계정이 활성/활성화된 스폰서 그룹의 멤버가 아니므로 스폰서 사용자의 ID 그룹이 스폰서 그룹의 멤버가 아닙니다.
- 스폰서의 내부 사용자 계정이 비활성화(일시 중지)되었습니다.

해결책

- 사용자 자격 증명을 확인합니다.
- 스폰서 그룹을 활성화합니다.
- 사용자 계정을 비활성화한 경우 복구합니다.
- 스폰서 사용자의 ID 그룹을 스폰서 그룹의 멤버로 추가합니다.

게스트 및 스폰서 활동 모니터링

Cisco ISE에서는 엔드포인트 및 사용자 관리 정보와 게스트 및 스폰서 활동을 확인할 수 있는 다양한 보고서 및 로그를 제공합니다.

온디맨드 또는 예약 방식으로 이러한 보고서를 실행할 수 있습니다.

단계 **1** **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 다양한 게스트, 스폰서 및 엔드포인트 관련 보고서를 보려면 **Guest(**게스트**)** 또는 **Endpoints and Users(**엔드포인트 및 사용자**)**를 선택합니다.

단계 **3** **Filters(**필터**)** 드롭다운 목록을 사용하여 검색에 사용할 데이터를 선택합니다.

단계 **4** 데이터를 확인할 **Time Range(**시간 범위**)**를 선택합니다.

단계 **5** **Run(**실행**)**을 클릭합니다.

메트릭 대시보드

Cisco ISE는 Cisco ISE 홈 페이지에 표시되는 메트릭 대시보드에서 네트워크의 **Authenticated Guests(**인증된 게스트**)** 및 **Active Endpoints(**활성 엔드포인트**)**를 한눈에 확인할 수 있는 보기를 제공합니다.

참고 핫스팟 플로우의 경우 엔드포인트가 **Authenticated Guests(**인증된 게스트**)** dashlet에 표시되지 않습니다.

AUP 수락 상태 보고서

AUP 수락 상태 보고서에는 모든 게스트 포털에서 게스트의 AUP(Acceptable Use Policy) 수락 상태가 표시됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Guest(**게스트**)** > **AUP Acceptance Status(AUP** 수락 상태**)**에서 확인할 수 있습니다.

이 보고서를 사용하여 지정된 기간 동안 수락 및 거부된 모든 AUP 연결을 추적할 수 있습니다.

게스트 계정 보고서

게스트 계정 보고서에는 지정된 기간 동안의 게스트 로그인 기록이 표시됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Guest(**게스트**)** > **Guest Accounting(**게스트 계정 관리**)**에서 확인할 수 있습니다.

기본 게스트 보고서

기본 게스트 보고서에서는 여러 보고서의 데이터가 단일 보기로 결합되므로, 여러 보고 소스의 데이터를 내보낼 수 있습니다. 데이터 열을 더 추가하고 보거나 내보내지 않을 열은 제거할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Guest(**게스트**)** > **Primary Guest Report(**기본 게스트 보고서**)**에서 이용할 수 있습니다.

이 보고서는 모든 게스트 활동을 수집하며 게스트 사용자가 방문하는 웹사이트에 대한 세부정보를 제공합니다. 보안 감사용으로 이 보고서를 사용하여 게스트 사용자가 네트워크에 액세스한 시간과 네트워크에서 수행한 작업을 확인할 수 있습니다. 게스트가 방문한 웹사이트의 URL 등 게스트의 인터넷 활동을 확인하려면 먼저 다음을 수행해야 합니다.

- 통과한 인증 로깅 범주를 활성화합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 Passed Authentications(통과한 인증)를 선택합니다.
- 게스트 트래픽에 사용되는 방화벽에서 다음 옵션을 활성화합니다.
  - Inspect HTTP traffic and send data to Cisco ISE Monitoring nod(HTTP 트래픽을 검사하여 Cisco ISE 모니터링 노드로 데이터를 보내기). 게스트 활동 보고서에는 IP 주소 및 액세스한 URL만 필요하므로 가능하면 이 정보만 포함하도록 데이터를 제한해 주십시오.
  - Send syslogs to Cisco ISE Monitoring node(Cisco ISE 모니터링 노드로 시스템 로그를 보내기)

스폰서 로그인 및 감사 보고서

스폰서 로그인 및 감사 보고서는 다음을 추적하는 결합된 보고서입니다.

- 스폰서 포털에서 스폰서가 수행하는 로그인 작업
- 스폰서 포털에서 스폰서가 수행하는 게스트 관련 작업

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Guest Access Reports(**게스트 액세스 보고서**)** > **Sponsor Login and Audit(**스폰서 로그인 및 감사**)**에서 사용 가능합니다.

게스트 및 스폰서 포털에 대한 감사 로깅

게스트 및 스폰서 포털 내에서 특정 작업 중에 감사 로그 메시지가 기본 감사 시스템으로 전송됩니다. 기본적으로 이러한 메시지는 /opt/CSCOcpm/logs/localStore/iseLocalStore.log 파일에 표시됩니다.

이러한 메시지가 시스템 로그에서 모니터링 및 문제 해결 시스템 및 로그 컬렉터로 전송되도록 구성할 수 있습니다. 모니터링 하위 시스템은 적절한 스폰서 및 디바이스 감사 로그와 게스트 활동 로그에 이러한 정보를 제공합니다.

게스트 로그인 흐름은 게스트 로그인의 성공 여부에 관계없이 감사 로그에 로그인합니다.

게스트 액세스 웹 인증 옵션

Cisco ISE 게스트 및 웹 인증 서비스는 보안 게스트 액세스를 사용하도록 설정하는 몇 가지 구축 옵션을 지원합니다. 로컬 또는 중앙 웹 인증 및 디바이스 등록 웹 인증을 사용하여 유선 또는 무선 게스트 연결을 제공할 수 있습니다.

- 중앙 웹 인증(중앙 WebAuth): 모든 게스트 포털에 적용됩니다. 유선 및 무선 연결 요청 모두에 대해 중앙 Cisco ISE RADIUS 서버에서 웹 인증을 사용합니다. 게스트는 핫스팟 게스트 포털에 선택적 액세스 코드를 입력하거나 인증 게스트 포털에 사용자 이름과 비밀번호를 입력하여 인증합니다.

  참고 리디렉션 중에 브라우저에서 둘 이상의 탭이 열리면 Cisco ISE가 모든 탭으로 리디렉션됩니다. 사용자는 포털에 로그인할 수 있지만, Cisco ISE에서는 세션을 인증할 수 없으며 사용자는 액세스 권한을 획득하지 못합니다. 이 문제를 해결하려면 사용자가 브라우저에서 탭 하나를 제외한 모든 탭을 닫아야 합니다.

- 로컬 웹 인증(로컬 WebAuth): 인증 게스트 포털에 적용됩니다. 게스트는 유선 연결의 경우 스위치에 연결하거나 무선 연결의 경우 WLC(무선 LAN 컨트롤러)에 연결합니다. NAD(Network Access Device)는 인증을 위해 웹페이지로 이동합니다. 게스트가 인증 게스트 포털에 사용자 이름과 비밀번호를 입력하여 인증합니다.

- 디바이스 등록 웹 인증(디바이스 등록 WebAuth): 핫스팟 게스트 포털에만 적용됩니다. Cisco ISE는 웹 인증 전에 게스트 디바이스를 등록하고 권한을 부여합니다. 게스트가 유선 또는 무선 NAD에 연결하면 핫스팟 게스트 포털로 연결됩니다. 게스트는 자격 증명(사용자 이름 및 비밀번호)을 제공하지 않고 네트워크에 액세스할 수 있습니다.

ISE 커뮤니티 리소스

게스트 액세스를 제공하도록 Cisco Wireless Controller로 Cisco ISE를 구성하는 방법에 대한 자세한 내용은 ISE 게스트 액세스 규범 구축 설명서에서 확인할 수 있습니다.

또한 기술 자료: ISE 무선 게스트 설정 가이드 및 마법사도 함께 참조하십시오.

NAD와 Central WebAuth 프로세스

이 시나리오에서 NAD(Network Access Device)는 알 수 없는 엔드포인트 연결에서 Cisco ISE RADIUS 서버에 대한 새 권한 부여 요청을 생성합니다. 그런 다음 엔드포인트는 Cisco ISE에 대한 url-redirect를 받습니다.

참고 webauth-vrf-aware 명령은 IOS XE 3.7E, IOS 15.2(4)E 이상 버전에서만 지원됩니다. 다른 스위치는 VRF(Virtual Routing and Forwarding, 가상 라우팅 및 포워딩) 환경에서 WebAuth URL 리디렉션을 지원하지 않습니다. 이러한 경우에는 해결 방법으로 전역 라우팅 표에 경로를 추가하여 트래픽을 VRF로 다시 유출할 수 있습니다.

게스트 디바이스가 NAD에 연결된 경우 게스트 서비스 상호 작용으로 MAB(MAC Authentication Bypass) 요청 양식을 가져오며 그에 따라 게스트 포털 Central WebAuth로 로그인하게 됩니다. 다음에는 이후의 중앙 웹 인증(Central WebAuth) 프로세스가 간략히 나와 있습니다. 이 프로세스는 무선 및 유선 네트워크 액세스 디바이스에 모두 적용됩니다.

1. 게스트 디바이스가 고정 연결을 통해 NAD에 연결됩니다. 게스트 디바이스에는 802.1X 신청자가 없습니다.
2. MAB용 서비스 유형과 함께 인증 정책을 사용하면 MAB 실패가 계속되고 Central WebAuth 사용자 인터페이스의 url-redirect가 포함된 제한된 네트워크 프로파일이 반환될 수 있습니다.
3. MAB 요청을 Cisco ISE RADIUS 서버에 대해 인증하도록 NAD가 구성됩니다.
4. Cisco ISE RADIUS 서버가 MAB 요청을 처리하지만 게스트 디바이스의 엔드포인트를 찾지 못합니다.

   이 MAB 실패가 제한된 네트워크 프로파일로 확인되고 프로파일의 url-redirect 값을 access-accept의 NAD에 반환합니다. 이 기능을 지원하려면 권한 부여 정책이 있으며 적절한 유선 또는 무선 MAB(복합 조건에 따라)를 제공하고 선택적으로 “Session:Posture Status=Unknown” 조건을 포함해야 합니다. NAD는 이 값을 사용하여 기본 포트 8443의 모든 게스트 HTTPS 트래픽을 url-redirect 값으로 리디렉션합니다.

이 경우 표준 URL 값은
`https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&portal=<PortalID>&action=cwa`
입니다.

5. 게스트 디바이스는 웹 브라우저를 통해 리디렉션 URL에 대한 HTTP 요청을 시작합니다.
6. NAD는 초기 access-accept에서 반환된 url-redirect 값으로 요청을 리디렉션합니다.
7. CWA 작업을 포함하는 게이트웨이 URL 값이 게스트 포털 로그인 페이지로 리디렉션됩니다.
8. 게스트가 로그인 자격 증명을 입력하고 로그인 양식을 제출합니다.
9. 게스트 서버가 로그인 자격 증명을 인증합니다.
10. 흐름 유형에 따라 다음과 같은 결과가 발생합니다.
    - 포스처 흐름(추가 검증 없는 인증)인 경우 클라이언트 프로비저닝을 수행하도록 게스트 포털이 구성되지 않았다면 게스트 서버가 CoA를 NAD에 보냅니다. 이 CoA는 NAD가 Cisco ISE RADIUS 서버를 사용하여 게스트 디바이스를 다시 인증하게 합니다. 새 access-accept가 네트워크 액세스가 구성되어 있는 NAD로 반환됩니다. 클라이언트 프로비저닝이 구성되지 않았으며 VLAN을 변경해야 하는 경우 게스트 포털은 VLAN IP 갱신을 수행합니다. 게스트는 로그인 자격 증명을 다시 입력하지 않아도 됩니다. 초기 로그인에 사용된 사용자 이름 및 비밀번호가 자동으로 사용됩니다.
    - 클라이언트 프로비저닝을 수행하도록 게스트 포털이 구성된 포스처 흐름인 경우 포스처 에이전트 설치 및 규정 준수를 위한 클라이언트 프로비저닝 페이지가 게스트 디바이스 웹 브라우저에 표시됩니다. 또한 선택적으로 클라이언트 프로비저닝 리소스 정책을 구성하여 "NetworkAccess:UseCase=GuestFlow" 조건을 포함할 수도 있습니다.

Linux를 위한 클라이언트 프로비저닝 또는 포스처 에이전트는 없으므로 게스트 포털은 클라이언트 프로비저닝 포털로 리디렉션되고 이는 다시 선택적 IP 릴리스/갱신을 수행한 다음 CoA를 수행하도록 게스트 인증 서블릿으로 리디렉션됩니다.

클라이언트 프로비저닝 포털로 리디렉션된 클라이언트 프로비저닝 서비스는 비영구적인 웹 에이전트를 게스트 디바이스로 다운로드하고 디바이스에 대한 포스처 검사를 수행합니다. 선택적으로 "NetworkAccess:UseCase=GuestFlow" 조건을 사용하여 포스처 정책을 구성할 수 있습니다.

게스트 디바이스가 규정을 준수하지 않는 경우 "NetworkAccess:UseCase=GuestFlow" 및 "Session:Posture Status=NonCompliant" 조건을 포함하는 권한 부여 정책을 구성했는지 확인해 주십시오.

게스트 디바이스가 규정을 준수하는 경우 "NetworkAccess:UseCase=GuestFlow" 및 "Session:Posture Status=Compliant" 조건을 사용하여 권한 부여 정책을 구성한 것입니다. 여기서 클라이언트 프로비저닝 서비스는 NAD에 대해 실행합니다. 이 CoA는 NAD가 Cisco ISE RADIUS 서버를 사용하여 게스트를 다시 인증하게 합니다. 새 access-accept가 네트워크 액세스가 구성되어 있는 NAD로 반환됩니다.

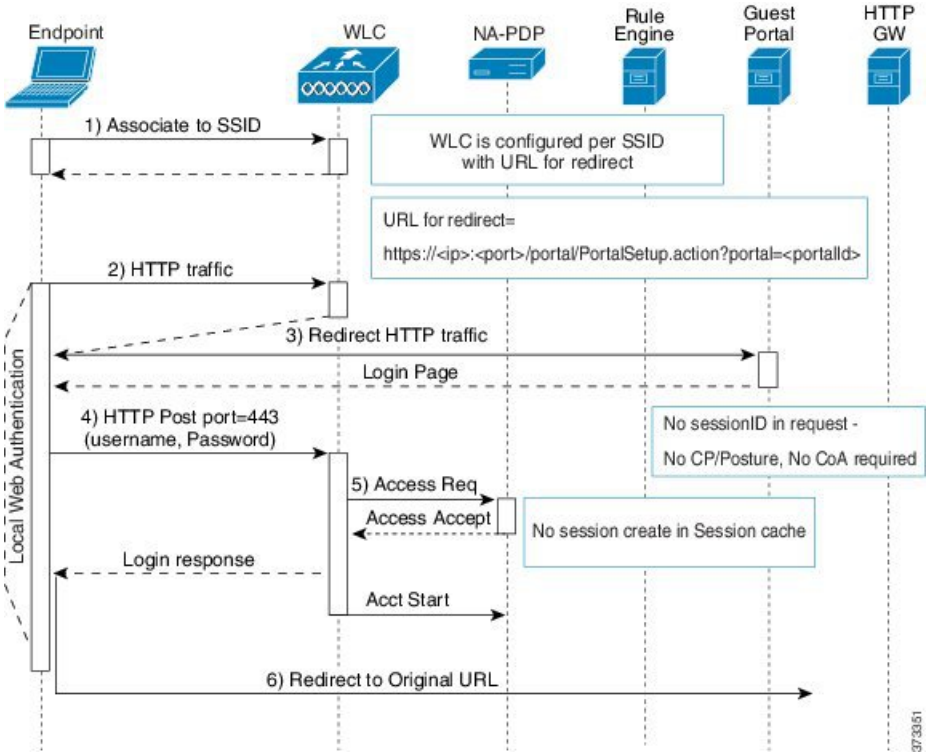
참고 "NetworkAccess:UseCase=GuestFlow"는 또한 게스트로 로그인하는 Active Directory 및 LDAP 사용자에게도 적용될 수 있습니다.

Local WebAuth를 사용하는 **Wireless LAN Controller** 프로세스

이 시나리오에서는 게스트가 로그인하고 WLC(Wireless LAN Controller)로 연결됩니다. 그런 다음 WLC는 게스트를 게스트 포털에 리디렉션합니다. 여기에서는 로그인 자격 증명을 입력하고 선택적 AUP(Acceptable Use Policy)를 수락하고 선택적 비밀번호 변경을 수행하도록 메시지가 표시됩니다. 이 과정이 완료되면 게스트 디바이스의 브라우저는 POST를 통해 로그인 자격 증명을 제공하도록 다시 WLC로 리디렉션됩니다.

이제 WLC는 Cisco ISE RADIUS 서버를 통해 게스트를 기록할 수 있습니다. 이 과정이 완료되면 WLC는 게스트 디바이스의 브라우저를 원래 URL 대상으로 리디렉션합니다. 게스트 포털에 대한 원래 URL 리디렉션을 지원하기 위한 WLC(Wireless LAN Controller) 및 NAD(Network Access Device) 요건은 IOS-XE 3.6.0.E 및 15.2(2)E 릴리스를 실행하는 WLC 5760과 Cisco Catalyst 3850, 3650, 2000, 3000, 4000 Series 액세스 스위치입니다.

그림 ***13: Local WebAuth*** 비포스처를 사용하는 ***WLC*** 흐름



Local WebAuth를 사용하는 유선 **NAD** 프로세스

이 시나리오에서 게스트 포털은 게스트 로그인 요청을 스위치(유선 NAD)로 리디렉션합니다. 로그인 요청은 스위치에 게시된 HTTPS URL 형식이며 로그인 자격 증명을 포함합니다. 스위치는 게스트 로그인 요청을 받고 구성한 Cisco ISE RADIUS 서버를 사용하여 게스트를 인증합니다.

1. HTML 리디렉션을 NAD에 업로드하려면 Cisco ISE에는 login.html 파일이 필요합니다. 이 login.html 파일은 HTTPS 요청에 대해 게스트 디바이스의 브라우저에 반환됩니다.

2. 게스트 디바이스의 브라우저는 게스트의 로그인 자격 증명이 입력되는 게스트 포털로 리디렉션됩니다.
3. AUP(Acceptable Use Policy) 및 비밀번호 변경(모두 선택 사항)이 처리되고 나면 NAD에 로그인 자격 증명을 게시하기 위해 게스트 포털에서 게스트 디바이스의 브라우저를 리디렉션합니다.
4. NAD는 게스트를 인증하고 권한을 부여할 수 있도록 Cisco ISE RADIUS 서버에 대한 RADIUS 요청을 실행합니다.

Login.html 페이지에 필요한 **IP** 주소 및 포트 값

login.html 페이지의 다음 HTML 코드에서 IP 주소 및 포트 값을 Cisco ISE 정책 서비스 노드에서 사용하는 값으로 변경해야 합니다. 기본 포트는 8443이지만 스위치에 할당하는 값이 Cisco ISE의 설정과 일치하도록 이 값을 변경할 수 있습니다.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<head>
<title>ISE Guest Portal</title>
<meta Http-Equiv="Cache-Control" Content="no-cache">
<meta Http-Equiv="Pragma" Content="no-cache">
<meta Http-Equiv="Expires" Content="0">
<meta http-equiv="content-type" content="text/html; charset=UTF-8">

<meta http-equiv="REFRESH"
content="0;url=https://ip:port/portal/PortalSetup.action?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/portal/PortalSetup.action?switch_url=wired">ISE Guest Portal</a>
</center>

</BODY>
</HTML>
```

사용자 맞춤화 로그인 페이지는 공용 웹 양식이므로 다음 지침을 고려해 주십시오.

- 로그인 양식은 사용자 이름 및 비밀번호에 대해 사용자가 입력하는 내용을 수락해야 하며 해당 엔트리를 **uname** 및 **pwd**로 표시해야 합니다.
- 사용자 맞춤화 로그인 페이지는 페이지 시간 초과, 숨겨진 비밀번호, 중복 제출 방지 등 웹 양식에 대한 모범 사례를 따라야 합니다.

NAD에서 **HTTPS** 서버 활성화

웹 기반 인증을 사용하려면 **ip http secure-server** 명령을 사용하여 스위치 내에서 HTTPS 서버를 활성화해야 합니다.

NAD의 사용자 맞춤화된 인증 프록시 웹 페이지 지원

성공, 만료 및 실패에 해당하는 사용자 맞춤화 페이지를 NAD에 업로드할 수 있습니다. Cisco ISE에서는 특정 사용자 맞춤화를 수행할 필요가 없으며 NAD에 포함된 표준 컨피그레이션 지침을 사용하여 이러한 페이지를 생성할 수 있습니다.

NAD에서 웹 인증 구성

기본 HTML 페이지를 사용자 맞춤화 파일로 교체하여 NAD에서 웹 인증을 완료해야 합니다.

시작하기 전에

웹 기반 인증 중에 스위치 기본 HTML 페이지 대신 사용할 대체 HTML 페이지 4개를 생성합니다.

단계 **1** 사용자 맞춤화 인증 프록시 웹 페이지 사용을 지정하려면 먼저 스위치 플래시 메모리에 사용자 맞춤화 HTML 파일을 저장합니다. 스위치 플래시 메모리에 HTML 파일을 복사하려면 스위치에서 다음 명령을 실행합니다.

copy tftp/ftp flash

단계 **2** 스위치에 HTML 파일을 복사한 후 전역 환경 설정 모드에서 다음 명령을 수행합니다.

ip admission proxy http login page file device:*login-filename*	기본 로그인 페이지 대신 사용할 사용자 맞춤화 HTML 파일의 스위치 메모리 파일 시스템 내 위치를 지정합니다. device:는 플래시 메모리입니다.
ip admission proxy http success page file device:*success-filename*	기본 로그인 성공 페이지 대신 사용할 사용자 맞춤화 HTML 파일 위치를 지정합니다.
ip admission proxy http failure page file device:*fail-filename*	기본 로그인 실패 페이지 대신 사용할 사용자 맞춤화 HTML 파일 위치를 지정합니다.
ip admission proxy http login expired page file device:*expired-filename*	기본 로그인 만료 페이지 대신 사용할 사용자 맞춤화 HTML 파일 위치를 지정합니다.

단계 **3** 스위치가 지원하는 지침에 따라 사용자 맞춤화된 인증 프록시 웹 페이지를 구성합니다.

단계 **4** 다음 예제에 나와 있는 대로 사용자 맞춤화 인증 프록시 웹 페이지의 컨피그레이션을 확인합니다.

```
Switch# show ip admission configuration
Authentication proxy webpage
 Login page           : flash:login.htm
 Success page         : flash:success.htm
 Fail Page            : flash:fail.htm
 Login expired Page   : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
```

```
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

디바이스 등록 웹 인증 프로세스

디바이스 등록 웹 인증(Device Registration WebAuth) 및 핫스팟 게스트 포털을 사용하여 사용자 이름과 비밀번호 없이도 게스트 디바이스를 개인 네트워크에 연결할 수 있습니다.

이 시나리오에서 게스트는 무선 연결을 통해 네트워크에 연결합니다. 디바이스 등록 웹 인증 프로세스 플로우의 예는 그림 14: 무선 디바이스 등록 웹 인증 흐름를 참고하십시오. 다음으로는 이후의 디바이스 등록 웹 인증 프로세스가 간략히 나와 있습니다. 프로세스는 무선 연결과 유선 연결 모두에서 유사합니다.

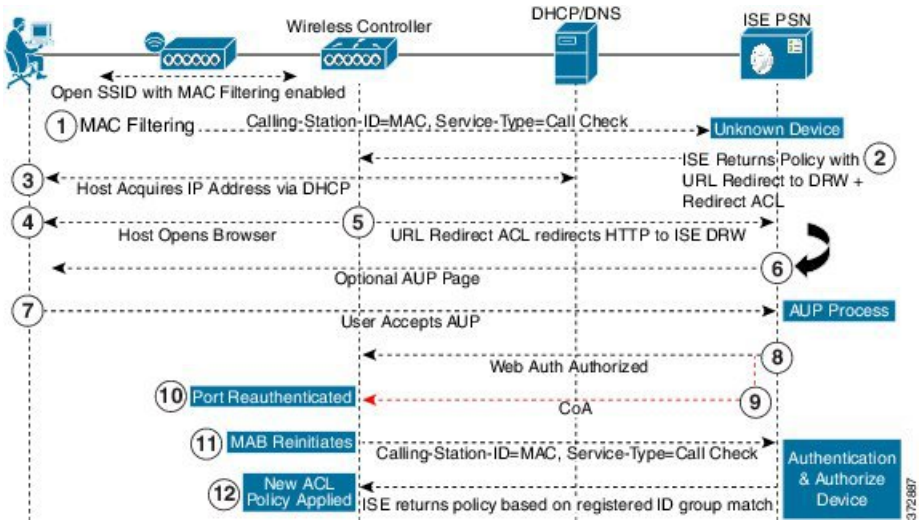
1. NAD(Network Access Device)가 핫스팟 게스트 포털에 대한 리디렉션을 보냅니다.
2. 게스트 디바이스의 MAC 주소가 엔드포인트 ID 그룹에 없거나 AUP(Acceptable Use Policy)에서 허용되는 속성이 true로 설정된 상태로 표시되지 않은 경우, Cisco ISE는 권한 부여 프로파일에 지정된 URL 리디렉션으로 응답합니다.
3. 게스트가 URL에 액세스하려고 하면 URL 리디렉션에서 게스트에 AUP 페이지(활성화된 경우)를 표시합니다.
   - 게스트가 AUP를 수락하면 디바이스 MAC 주소와 연결된 엔드포인트가 구성한 엔드포인트 ID 그룹에 할당됩니다. 이 엔드포인트는 이제 AUP에서 허용되는 속성이 true로 설정된 상태로 표시되어 AUP의 게스트 수락을 추적합니다.
   - 게스트가 AUP를 수락하지 않거나 오류가 발생하는 경우(예: 엔드포인트 생성 또는 업데이트) 오류 메시지가 표시됩니다.
4. 핫스팟 게스트 포털 컨피그레이션에 따라 추가 정보가 포함된 액세스 후 배너 페이지(활성화된 경우)가 표시될 수 있습니다.
5. 엔드포인트가 생성되거나 업데이트된 후에는 CoA(Change of Authorization) 종료가 NAD로 전송됩니다.
6. CoA 이후에 NAD는 새 MAB(MAC Auth Bypass) 요청을 통해 게스트 연결을 다시 인증합니다. 새 인증에서 엔드포인트 ID 그룹과 연결된 엔드포인트를 발견하면 구성한 액세스를 NAD로 반환합니다.
7. 핫스팟 게스트 포털 컨피그레이션에 따라, 게스트는 액세스를 요청한 URL, 관리자가 지정한 사용자 맞춤화 URL 또는 인증 성공 페이지로 연결됩니다.

유선과 무선 모두의 CoA 유형은 CoA 종료입니다. VLAN DHCP 릴리스(및 갱신)를 수행하여 유선 및 무선 CoA 유형의 Change of Auth에 대한 권한을 다시 부여하도록 핫스팟 게스트 포털을 구성할 수 있습니다.

VLAN DHCP 릴리스 지원은 Windows 디바이스에 한해 제공됩니다. 모바일 디바이스에는 사용할 수 없습니다. 등록된 디바이스가 모바일 디바이스이고 VLAN DHCP 릴리스 옵션이 활성화된 경우 게스

트는 해당 IP 주소를 수동으로 갱신해야 합니다. 모바일 디바이스 사용자는 WLC에서 VLAN을 사용하는 대신 ACL(Access Control Lists)을 사용하는 것이 좋습니다.

그림 ***14:*** 무선 디바이스 등록 웹 인증 흐름



게스트 포털 설정

포털 **ID** 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals or Sponsor Portals(**게스트 포털 또는 스폰서 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Guest Portals or Sponsor Portals Settings and Customization(**게스트 포털 또는 스폰서 포털 설정 및 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.

핫스팟 게스트 포털용 포털 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **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.

- **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.

- **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.

핫스팟 게스트 포털용 **AUP(Acceptable Use Policy)** 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Acceptable Use Policy (AUP) Page Settings(AUP(Acceptable Use Policy)** 페이지 설정**)**입니다.

- **Include an AUP Page(AUP** 페이지 포함**)**: 회사의 네트워크 사용 약관을 별도의 페이지에서 사용자에게 표시합니다.
- **Require an Access Code(**엑세스 코드 필요**)**: 여러 게스트가 네트워크에 액세스하기 위해 사용해야 하는 로그인 자격 증명로 액세스 코드를 할당합니다. 기본적으로 액세스 코드는 실제로 존재하는 게스트에게 제공되는 로컬에서 확인된 코드로, 화이트보드를 통해 시각적으로 또는 대기실 관리자에 의해 구두로 제공됩니다. 경계 외부의 사용자는 이 코드를 알 수 없어야 하며 네트워크에 액세스하는 데 이 코드를 사용해서는 안 됩니다.

  개별 게스트에게 로그인 자격 증명으로 제공되는 사용자 이름과 비밀번호와 함께 이 옵션을 사용할 수 있습니다.
- **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. AUP가 사용자에게 표시되는 시점을 구성합니다.

핫스팟 게스트 포털 플로우를 구성할 때 AUP 액세스 코드는 엔드포인트 ID 그룹 디바이스 등록에 의존합니다. 이는 AUP Last Acceptance and Network Access: Use Case EQUALS Guest Flow 플래그를 사용할 수 없음을 의미합니다. 사용자 세션이 NAD에서 제거되었다가 다시 연결되는 경우 사용자에게 AUP 페이지가 표시되지만 AUP 액세스 코드를 입력할 필요는 없습니다.

AUP 액세스 코드 페이지는 핫스팟 포털 구성에 연결된 엔드포인트 ID 그룹에서 MAC 주소가 제거된 후에만 표시됩니다. 엔드포인트는 Cisco ISE의 상황 가시성 페이지를 통해 데이터베이스에서 수동으로 삭제되거나 엔드포인트 제거 기능 및 구성된 엔드포인트 제거 정책을 통해 제거됩니다.

핫스팟 포털용 액세스 후 배너 페이지 설정

이 페이지의 탐색 경로는 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Post-Access Banner Page Settings(**액세스 후 배너 페이지 설정**)**입니다.

다음과 같은 설정을 사용하여 필요에 따라 게스트에게 액세스 상태 및 기타 추가 작업에 대한 알림을 표시합니다.

필드	사용 지침
Include a Post-Access Banner page(액세스 후 배너 페이지 포함**)**	게스트가 정상적으로 인증하여 네트워크 액세스 권한을 부여받기 전에 추가 정보를 표시합니다.

자격 증명이 있는 게스트 포털에 대한 포털 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **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.

- 포털 인증서 주체 이름/대체 주체 이름에서는 인터페이스 IP 주소를 확인해야 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.

- **Employees Using this Portal as Guests Inherit Login Options from(**이 포털을 게스트로 사용하는 직원이 로그인 옵션을 상속하는 원본**)**: 직원이 이 포털에 로그온할 때 직원에게 할당되는 게스트 유형을 선택합니다. 직원의 엔드포인트 데이터는 **Store device information in endpoint identity group(**엔드포인트 **ID** 그룹에 디바이스 정보 저장**)** 속성에서 해당 게스트 유형에 대해 구성되는 엔드포인트 ID 그룹에 저장됩니다. 연결된 게스트 유형의 다른 속성은 상속되지 않습니다.
- **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.

자격 증명이 있는 게스트 포털에 대한 로그인 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Login Page Settings(**로그인 페이지 설정**)**입니다.

- **Require an Access Code(**엑세스 코드 필요**)**: 여러 게스트가 네트워크에 액세스하기 위해 사용해야 하는 로그인 자격 증명로 액세스 코드를 할당합니다. 기본적으로 액세스 코드는 실제로 존재하는 게스트에게 제공되는 로컬에서 확인된 코드로, 화이트보드를 통해 시각적으로 또는 대기실 관리자에 의해 구두로 제공됩니다. 경계 외부의 사용자는 이 코드를 알 수 없어야 하며 네트워크에 액세스하는 데 이 코드를 사용해서는 안 됩니다.

  개별 게스트에게 로그인 자격 증명으로 제공되는 사용자 이름과 비밀번호와 함께 이 옵션을 사용할 수 있습니다.

- **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.

- **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(AUP** 포함**)**: 허용되는 사용 정책 창을 플로우에 추가합니다. AUP를 창에 추가하거나 다른 창으로 연결할 수 있습니다.

- **Allow Guests to Create their Own Accounts(**게스트의 계정 생성 허용**)**: 이 포털의 로그인 페이지에서 게스트가 직접 등록을 할 수 있는 옵션을 제공합니다. 이 옵션을 선택하지 않는 경우에는 스폰서가 게스트 계정을 생성합니다. 이 옵션을 활성화하면 이 페이지에서 **Self-Registration Page Settings(**셀프 등록 페이지 설정**)** 및 **Self-Registration Success Page Settings(**셀프 등록 성공 페이지 설정**)**를 구성할 수 있는 탭도 활성화됩니다.

  게스트는 이 옵션을 선택하면 표시되는 셀프 등록 양식에 요청된 정보를 입력하여 게스트 계정을 직접 생성할 수 있습니다.

- **Allow Guest to Recover the Password(**게스트의 비밀번호 복구 허용**)**: 이 옵션은 셀프 등록 게스트에 대해 게스트 포털에서 Reset Password(비밀번호 재설정) 버튼을 활성화합니다. 유효한 계정

이 있는 셀프 등록 게스트가 로그인 포털에 연결하고 비밀번호를 잊어버린 경우 **Reset Password(**비밀번호 재설정**)**를 클릭할 수 있습니다. 그러면 게스트는 셀프 등록 창으로 돌아가게 되며 여기에서 전화나 이메일(어느 것이든 게스트가 등록한 정보)을 입력하고 새 비밀번호를 입력할 수 있습니다.

- **Allow Social Login(**소셜 로그인 허용**)**: 소셜 미디어 사이트를 사용하여 이 포털의 사용자에 대한 로그인 자격 증명을 가져옵니다. 이 옵션을 선택하면 다음 설정이 표시됩니다.
  - **Show registration form after social login(**소셜 로그인 후 등록 양식 표시**)**: 사용자가 Facebook에서 제공하는 정보를 변경할 수 있도록 합니다.
  - **Require guests to be approved(**게스트 승인 필요**)**: 스폰서가 사용자의 계정을 승인해야 함을 사용자에게 알리며, 로그인을 위한 자격 증명을 사용자에게 전송합니다.
- **Allow guests to change password after login(**게스트의 로그인 후 비밀번호 변경 허용**)**: 게스트가 정상적으로 인증되고 AUP를 수락(필요 시)한 후 비밀번호를 변경하도록 허용합니다. 비밀번호를 변경한 게스트가 로그인 자격 증명을 잊어버리는 경우 스폰서는 자격 증명을 제공할 수 없으며, 게스트의 비밀번호를 다시 임의의 비밀번호로 재설정하는 작업만 가능합니다.
- **Allow the following identity-provider guest portal to be used for login(**다음 **ID** 제공자 게스트 포털을 로그인에 사용하도록 허용**)**: 이 옵션을 선택하고 SAML ID의 ID 제공자를 선택하면 해당 SAML ID의 링크가 이 포털에 추가됩니다. 이 하위 포털은 사용자가 자격 증명을 제공하는 SAML IDP처럼 보이도록 구성할 수 있습니다.
- **Allow social login(**소셜 로그인 허용**)**: 이 포털에서 사용자 로그인 시 소셜 미디어 유형을 사용할 수 있도록 합니다. 소셜 로그인 구성에 대한 자세한 내용은 셀프 등록 게스트의 소셜 로그인, 371 페이지을 참조하십시오.

셀프 등록 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portal & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Self Registration Page Settings(**셀프 등록 페이지 설정**)**입니다. 다음과 같은 설정을 사용하여 게스트의 셀프 등록 기능을 활성화하고 셀프 등록 양식에 입력해야 하는 정보를 지정합니다.

- **Assign self-registered guests to guest type(**게스트 유형에 셀프 등록된 게스트 할당**)**: 이 포털을 사용 중인 셀프 등록한 모든 게스트에 할당해야 하는 게스트 유형을 선택합니다.
- **Account valid for(**계정 유효 기간**)**: 계정의 유효 기간을 일/시/분 단위로 지정합니다. 계정 소유자나 스폰서가 스폰서 포털에서 계정 기간을 연장하지 않으면 이 기간이 지난 후 계정은 만료됩니다.
- **Require a registration code for self registration(**셀프 등록용 등록 코드 필요**)**: 셀프 등록 게스트가 셀프 등록 양식을 정상적으로 제출하려면 입력해야 하는 코드를 할당합니다. 경계 외부의 사용자가 시스템에 액세스하지 못하도록 하기 위해 등록 코드는 액세스 코드와 마찬가지로 게스트에게 오프라인으로 제공됩니다.

- **Fields to include(**포함할 필드**)**: 셀프 등록 양식에 표시할 필드를 선택합니다. 그런 다음 게스트가 양식을 제출하고 게스트 계정을 받으려면 반드시 작성해야 하는 필드를 선택합니다. **SMS Service Provider(SMS** 서비스 제공자**)** 및 **Person being Visited(**방문 중인 사용자**)**와 같은 필드를 필수로 지정하여 셀프 등록 게스트로부터 중요한 정보를 수집할 수 있습니다.
  - **Location(**위치**)**: 셀프 등록 게스트가 정의된 위치 목록을 사용하여 등록 시에 선택할 수 있는 위치를 입력합니다. 그러면 이러한 게스트에 대해 관련 표준 시간대가 유효한 액세스 시간으로 자동 할당됩니다. 선택 중에 혼선을 방지하기 위해 위치 이름을 Boston Office, 500 Park Ave New York, Singapore 등으로 명확하게 지정합니다.

    시간별로 게스트 액세스를 제한하려는 경우 표준 시간대를 사용하여 시간을 결정합니다. 시간별로 액세스가 제어되는 모든 게스트가 산호세 표준 시간대에 있지 않는 한 해당 로캘의 표준 시간대를 만듭니다. 위치를 하나만 제공하는 경우에는 해당 위치가 기본 위치로 자동 할당되며 게스트가 볼 수 있도록 이 필드가 포털에 표시되지 않습니다. 또한 **Location(**위치**)**은 **Fields to include(**포함할 필드**)** 목록에서 비활성화됩니다.
  - **SMS Service Provider(SMS** 서비스 제공자**)**: 셀프 등록 게스트가 SMS 제공자를 직접 선택할 수 있도록 셀프 등록 양식에 표시할 SMS 제공자를 선택합니다. 그런 다음 게스트의 SMS 서비스를 사용하여 게스트에게 SMS 알림을 보내면 회사 경비를 최소화할 수 있습니다. 게스트가 사용하도록 할 SMS 제공자를 하나만 선택한 경우에는 셀프 등록 양식에 이 필드가 표시되지 않습니다.
  - **Person being visited(**방문자**)**: 텍스트 필드이므로 이 필드를 사용하려면 게스트에게 이 필드에 입력할 정보 유형을 알려줍니다.
  - **Custom Fields(**사용자 맞춤화 필드**)**: 셀프 등록 게스트로부터 추가 데이터를 수집하기 위해 이전에 생성한 사용자 맞춤화 필드를 선택합니다. 그런 다음 게스트가 셀프 등록 양식을 제출하고 게스트 계정을 받으려면 반드시 작성해야 하는 필드를 선택합니다. 이러한 필드는 이름의 알파벳순으로 나열됩니다. 더 많은 사용자 맞춤화 필드를 추가하려면 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Settings(**설정**)** > **Custom Fields(**사용자 맞춤화 필드**)**에서 이러한 필드를 생성합니다.
  - **Include an AUP(AUP** 포함**)**: 회사의 네트워크 사용 약관을 사용자에 대해 현재 표시되어 있는 페이지에 텍스트로 표시하거나, AUP 텍스트가 포함된 새 탭 또는 창을 여는 링크로 표시합니다.
    - **Require acceptance(**수락 필요**)**: 사용자가 AUP의 전체 내용을 확인해야 하도록 지정합니다. 그러면 셀프 등록 페이지에서 **Accept(**수락**)** 버튼이 구성됩니다. 한 페이지로 AUP를 구성한 경우 사용자가 AUP의 끝으로 스크롤할 때까지 Accept(수락) 버튼을 비활성화할 수도 있습니다.

- **Only allow guests with an email address from(**다음 도메인의 이메일 주소를 사용하는 게스트만 허용**)**: 셀프 등록 게스트가 이메일 주소를 생성하기 위해 **Email Address(**이메일 주소**)**에서 사용할 수 있는 허용된 도메인(예: cisco.com) 목록을 지정합니다.

  이 필드를 비워두면 **Do not allow guests with an email address from(**다음 도메인의 이메일 주소를 사용하는 게스트 허용 안 함**)**에 나열된 도메인을 제외하고 모든 이메일 주소가 유효합니다.

- **Do not allow guests with an email address from(**다음 도메인의 이메일 주소를 사용하는 게스트 허용 안 함**)**: 셀프 등록 게스트가 이메일 주소를 생성하기 위해 **Email Address(**이메일 주소**)**에서 사용할 수 없는 차단된 도메인(예: czgtgj.com) 목록을 지정합니다.
- **Require self-registered guests to be approved(**셀프 등록한 게스트의 승인 필요**)**: 이 포털을 사용 중인 셀프 등록 게스트가 스폰서로부터 승인을 받아야 게스트 자격 증명을 받을 수 있도록 지정합니다. 이 옵션을 클릭하면 스폰서가 셀프 등록 게스트를 승인하는 방법에 대한 추가 옵션이 표시됩니다.
  - **Allow guests to login automatically from self-registration after sponsor's approval(**스폰서 승인 후 셀프 등록 게스트가 자동으로 로그인하도록 허용**)**: 스폰서가 승인하면 셀프 등록 게스트가 자동으로 로그인됩니다.
  - **Email approval request to(**승인 요청 이메일을 보낼 주소**)**:
    - **Sponsor email addresses listed below(**아래에 나와 있는 스폰서 이메일 주소**)**: 승인자로 지정된 스폰서의 이메일 주소를 하나 이상 입력하거나 모든 게스트 승인 요청을 보내야 하는 메일러를 입력합니다. 이메일 주소가 유효하지 않으면 승인이 실패합니다.
    - **Person being visited(**방문자**)**: **Require sponsor to provide credentials for authentication(**스폰서가 인증을 위해 자격 증명 제공 필요**)** 필드가 표시되며 **Fields to include(**포함할 필드**)**의 **Required(**필수**)** 옵션이 활성화됩니다(이전에 비활성화된 경우). 이러한 필드는 셀프 등록 게스트로부터 이 정보를 요청하는 셀프 등록 양식에 표시됩니다. 이메일 주소가 유효하지 않으면 승인이 실패합니다.
  - **Approve/Deny Link Settings(**링크 설정 승인/거부**)**:
    - **Links are valid for(**링크 유효 기간**)**: 계정 승인 링크의 만료 기간을 설정할 수 있습니다.
    - **Require sponsor to provide credentials for authentication(**스폰서가 인증을 위해 자격 증명 제공 필요**)**:이 섹션의 구성에서 요구하지 않는 경우에도 스폰서가 계정 승인을 위해 자격 증명을 입력하도록 하려면 이 옵션을 선택합니다. 이 필드는 **Require self-registered guests to be approved(**셀프 등록한 게스트의 승인 필요**)**가 **person being visited(**방문자**)**로 설정된 경우에만 표시됩니다.
    - **Sponsor is matched to a Sponsor Portal to verify approval privileges(**스폰서 포털에서 스폰서의 승인 권한 확인**)**: **Details(**세부정보**)**를 클릭하여 스폰서가 유효한 시스템 사용자이고 스폰서 그룹의 멤버이며 해당 그룹의 멤버가 계정을 승인할 권한을 가졌는지 확인하기 위해 검색할 포털을 선택합니다. 각 스폰서 포털에는 스폰서를 식별하는 데 사용되는 ID 소스 시퀀스가 있습니다. 포털은 나열된 순서대로 사용됩니다. 목록의 첫 번째 포털에 따라 스폰서 포털에서 사용되는 스타일과 사용자 맞춤화이 결정됩니다.
- **After registration submission, direct guest to(**등록 제출 후 게스트를 이동할 위치**)**: 정상적으로 등록한 후 셀프 등록 게스트를 이동할 위치를 선택합니다.
  - **Self Registration Success page(**셀프 등록 성공 페이지**)**: 정상적으로 셀프 등록한 게스트를 **Self Registration Success(**셀프 등록 성공**)** 창으로 이동시킵니다. 이 창에는 **Self Registration Success Page Settings(**셀프 등록 성공 페이지 설정**)**에서 지정한 필드와 메시지가 표시됩니다.

시스템이 계정 승인(이 창에서 활성화한 경우)을 대기 중이거나, 이 창에 지정된 허용 및 차단 목록 도메인을 기준으로 하여 이메일 주소 또는 전화번호로 로그인 자격 증명을 전달하는 중일 수도 있으므로 모든 정보를 표시하는 것은 적절하지 않을 수도 있습니다.

Allow guests to log in directly from the Self-Registration Success page(게스트가 셀프 등록 성공 페이지에서 직접 로그인할 수 있음**)**를 **Self-Registration Success Page Settings(**셀프 등록 성공 페이지 설정**)**에서 활성화한 경우 정상적으로 셀프 등록한 게스트가 이 창에서 직접 로그인할 수 있습니다. 이 옵션이 활성화되지 않은 경우에는 **Self-Registration Success(**셀프 등록 성공**)** 창이 표시된 후 게스트가 포털의 로그인 창으로 이동됩니다.

- **Login page with instructions about how to obtain login credentials(**로그인 자격 증명을 받는 방법에 대한 지침이 포함된 로그인 페이지**)**: 정상적으로 셀프 등록된 게스트를 포털 로그인 창으로 다시 이동시킨 다음 "Please wait for your guest credentials to be delivered either via email, SMS, or print format and proceed with logging in(게스트 자격 증명이 이메일, SMS 또는 인쇄 형식으로 전달될 때까지 기다렸다가 로그인을 진행해 주십시오)."과 같은 메시지를 표시합니다.

  기본 메시지를 사용자 맞춤화하려면 **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 클릭하고 **Self-Registration Page Settings(**셀프 등록 페이지 설정**)**를 선택합니다.

  시스템이 계정 승인(이 창에서 활성화한 경우)을 대기 중이거나, 이 창에 지정된 화이트리스트 및 블랙리스트 도메인을 기준으로 하여 이메일 주소 또는 전화번호로 로그인 자격 증명을 전달하는 중일 수도 있습니다.

- **URL**: 정상적으로 셀프 등록한 게스트가 계정 자격 증명이 전달될 때까지 기다리는 동안 지정된 URL로 이동시킵니다.

  시스템이 계정 승인(이 창에서 활성화한 경우)을 대기 중이거나, 이 창에 지정된 화이트리스트 및 블랙리스트 도메인을 기준으로 하여 이메일 주소 또는 전화번호로 로그인 자격 증명을 전달하는 중일 수도 있습니다.

- **Send credential notification automatically using(**다음을 사용하여 자격 증명 알림 자동 전송**):**
  - **Email(**이메일**)**:정상적으로 셀프 등록한 게스트가 로그인 자격 증명 정보를 받을 옵션으로 이메일을 선택합니다. 이 옵션을 선택하면 **Email address(**이메일 주소**)**가 **Fields to include(**포함할 필드**)** 목록에서 필수 필드가 되며 이 옵션을 더 이상 비활성화할 수 없습니다.
  - **SMS**: 정상적으로 셀프 등록한 게스트가 로그인 자격 증명 정보를 받을 옵션으로 SMS를 선택합니다. 이 옵션을 선택하면 **SMS Service Provider(SMS** 서비스 제공자**)**가 **Fields to include(**포함할 필드**)** 목록에서 필수 필드가 되며 이 옵션을 더 이상 비활성화할 수 없습니다.

셀프 등록 성공 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Self**

Registration Success Page Settings(셀프 등록 성공 페이지 설정**)**입니다. 다음과 같은 설정을 사용하여 정상적으로 셀프 등록한 게스트에게 네트워크 액세스 권한을 얻는 데 필요한 자격 증명을 알립니다.

필드	사용 지침
Include this information on the Self-Registration Success page(셀프 등록 성공 페이지에 이 정보 포함)	셀프 등록 성공 페이지에서 정상적으로 셀프 등록한 게스트에 대해 표시할 필드를 선택합니다. 스폰서의 게스트 승인이 필요하지 않은 경우에는 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)**를 선택하여 이러한 자격 증명을 게스트에 대해 표시합니다. 스폰서 승인이 필요한 경우에는 이러한 필드가 비활성화됩니다. 게스트가 승인된 후에만 자격 증명을 게스트에게 제공할 수 있기 때문입니다.
Allow guest to send information to self using(게스트가 다음 방법을 사용하여 자신에게 정보를 보내도록 허용)	정상적으로 셀프 등록한 게스트가 자신에게 자격 증명 정보를 보내는 데 사용할 수 있는 옵션을 **Print(**인쇄**)**, **Email(**이메일**)** 또는 **SMS** 중에서 선택합니다.
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**)**	**AUP on page(**페이지의 **AUP)** 옵션을 선택한 경우 이 필드가 표시됩니다. 사용자가 AUP의 전체 내용을 확인해야 하도록 지정합니다. 사용자가 AUP 끝으로 스크롤해야 **Accept(**수락**)** 버튼이 활성화됩니다.
Allow guests to log in directly from the Self-Registration Success page(게스트가 셀프 등록 성공 페이지에서 직접 로그인하도록 허용)	셀프 등록 성공 페이지의 아래쪽에 **Login(**로그인**)** 버튼을 표시합니다. 그러면 게스트가 로그인 페이지를 건너뛰고 로그인 자격 증명을 포털에 직접 제공하여 포털 흐름의 다음 페이지(예: AUP 페이지)를 표시할 수 있습니다.

자격 증명이 있는 게스트 포털에 대한 **AUP(Acceptable Use Policy)** 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Acceptable Use Policy (AUP) Page Settings(AUP(Acceptable Use Policy)** 페이지 설정**)**입니다.

- **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 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.

자격 증명이 있는 게스트 포털에 대한 게스트 변경 비밀번호 설정

게스트 비밀번호 변경 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Guest Change Password Settings(**게스트 비밀번호 변경 설정**)**입니다.

- **Allow guests to change password after login(**게스트의 로그인 후 비밀번호 변경 허용**)**: 게스트가 정상적으로 인증되고 AUP를 수락(필요 시)한 후 비밀번호를 변경하도록 허용합니다. 비밀번호를 변경한 게스트가 로그인 자격 증명을 잊어버리는 경우 스폰서는 자격 증명을 제공할 수 없으며, 게스트의 비밀번호를 다시 임의의 비밀번호로 재설정하는 작업만 가능합니다.

자격 증명이 있는 게스트 포털에 대한 게스트 디바이스 등록 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Guest Device Registration Settings(**게스트 디바이스 등록 설정**)**입니다.

다음과 같은 설정을 사용하여 게스트가 로그인할 때 Cisco ISE가 게스트 디바이스를 자동으로 등록하거나 게스트가 로그인한 후 디바이스를 수동으로 등록할 수 있도록 지정합니다.

각 게스트 유형의 최대 디바이스 수는 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Types(**게스트 유형**)**에 지정됩니다.

- **Automatically Register Guest Devices(**게스트의 디바이스 등록 허용**)**: 게스트가 이 포털에 액세스하는 데 사용하는 디바이스용 엔드포인트를 자동으로 생성합니다. 엔드포인트는 이 포털에 대해 지정된 엔드포인트 ID 그룹에 추가되며,.

  엔드포인트가 추가되면 권한 부여 규칙을 생성하여 해당 ID 그룹의 엔드포인트에 대한 액세스를 허용할 수 있습니다. 그러면 웹 인증이 더 이상 필요하지 않습니다.

  등록된 디바이스의 최대 수에 도달하면 시스템은 첫 번째로 등록한 디바이스를 자동으로 삭제하고 게스트가 로그인하는 데 사용 중인 디바이스를 등록한 후 게스트에게 알림을 표시합니다. 게스트가 등록할 수 있는 최대 디바이스 수를 변경하려면 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Types(**게스트 유형**)**를 선택합니다.

- **Allow Guests to Register Devices(**게스트의 디바이스 등록 허용**)**: 게스트가 이름, 설명 및 MAC 주소를 입력하여 디바이스를 수동으로 등록할 수 있습니다. MAC 주소는 엔드포인트 ID 그룹에 연결됩니다.

  등록된 디바이스의 최대 수에 도달하면 게스트는 디바이스를 하나 이상 삭제해야 다른 디바이스를 등록할 수 있습니다.

자격 증명이 있는 게스트 포털에 대한 **BYOD** 설정

이 페이지의 탐색 경로는 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **BYOD Settings(BYOD** 설정**)**입니다.

이러한 설정을 사용하여 비게스트(예: 직원)가 자격 증명이 지정된 게스트 포털을 사용하여 회사 네트워크에 액세스할 수 있도록 BYOD(Bring Your Own Device) 기능을 활성화할 수 있습니다.

필드	사용 지침
Allow Employees to use Personal Devices on the Network(네트워크에서 직원의 개인 디바이스 사용 허용**)**	이 포털에 BYOD(Bring Your Own Device) 등록 창을 추가하여 직원이 직원 디바이스 등록 프로세스를 진행할 수 있도록 허용합니다. 그리고 직원의 개인 디바이스 유형(예: iOS, Android, OSX)에 대한 클라이언트 프로비저닝 설정에 따라 기본 신청자 및 인증서 프로비저닝도 허용합니다.

필드	사용 지침
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.
Allow employees to choose to get guest access only(직원이 선택적으로 게스트 액세스만 가져오도록 허용**)**	직원이 게스트 네트워크에 액세스할 수 있지만 회사 네트워크에 액세스하는 데 필요할 수 있는 추가 프로비저닝 및 등록을 하지 못하게 합니다.
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.

자격 증명이 지정된 게스트 포털용 로그인 후 배너 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals or Sponsor Portals(**게스트 포털 또는 스폰서 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 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	사용 지침
Include a Post-Login Banner page(로그인 후 배너 페이지 포함**)**	사용자가 정상적으로 로그인하여 네트워크 액세스 권한을 부여받기 전에 추가 정보를 표시합니다.

자격 증명이 있는 게스트 포털에 대한 게스트 디바이스 규정 준수 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Guest Device Compliance Settings(**게스트 디바이스 규정 준수 설정**)**입니다. 게스트 포털을 사용하는 게스트 및 직원이 네트워크에 액세스하기 위해서는 디바이스의 클라이언트 프로비저닝을 수행하도록 지정하려면 다음과 같은 설정을 사용합니다.

- **Require guest device compliance(**게스트 디바이스 규정 준수 필요**)** - 게스트를 에이전트를 다운로드해야 하는 Client Provisioning(클라이언트 프로비저닝) 페이지로 리디렉션합니다. 이렇게 하면 게스트 플로우에 클라이언트 프로비저닝이 추가되며, 여기서 바이러스 방지 소프트웨어 확인과 같이 게스트에 대한 포스처 정책을 구성합니다.

  게스트가 인증 게스트 포털을 사용하여 네트워크에 액세스하는 직원인 경우와 아래의 경우 다음과 같은 작업이 수행됩니다.

  - **BYOD Settings(BYOD** 설정**)**에서 **Allow employees to use personal devices on the network(**네트워크에서 직원의 개인 디바이스 사용 허용**)**를 활성화한 경우 직원은 BYOD 플로우로 리디렉션되고 클라이언트 프로비저닝을 수행하지 않습니다.
  - **BYOD Settings(BYOD** 설정**)**에서 **Allow employees to use personal devices on the network(**네트워크에서 직원의 개인 디바이스 사용 허용**)** 및 **Allow employees to choose to get guest access only(**직원이 선택적으로 게스트 액세스만 가져오도록 허용**)**를 모두 활성화한 경우 직원이 게스트 액세스를 선택하면 직원은 Client provisioning(클라이언트 프로비저닝) 페이지로 연결됩니다.

게스트 포털용 **VLAN DHCP** 해제 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **VLAN DHCP Release Page Settings(VLAN DHCP** 릴리스 페이지 설정**)**입니다.

- **Enable VLAN DHCP release(VLAN DHCP** 릴리스 활성화**)**: 유선 환경과 무선 환경 둘 다에서 VLAN이 변경된 후 Windows 디바이스의 IP 주소를 새로 고치는 데 사용됩니다.

이 설정은 최종 권한 부여 중에 네트워크 액세스 시 게스트 VLAN이 새 VLAN으로 변경될 때의 CWA(Central WebAuth) 플로우에 영향을 줍니다. VLAN 변경 전에 게스트의 이전 IP 주소를 릴리스해야 하며, 게스트가 새 VLAN에 연결될 때 DHCP를 통해 새 게스트 IP 주소를 요청해야 합니다. IP 주소 릴리스 및 갱신 작업은 DirectX 컨트롤을 사용하는 Internet Explorer 브라우저에서만 지원됩니다.

모바일 디바이스에서는 VLAN DHCP 릴리스 옵션이 작동하지 않습니다. 대신 게스트가 수동으로 IP 주소를 재설정해야 합니다. 재설정 방법은 디바이스에 따라 다릅니다. 예를 들어 Apple iOS 디바이스에서는 게스트가 Wi-Fi 네트워크를 선택하고 **Renew Lease(**임대 갱신**)** 버튼을 클릭할 수 있습니다.

- **Delay to Release __ Seconds(**릴리스 __초 지연**)**: 릴리스 지연 시간을 입력합니다. 애플릿을 다운로드한 직후 Cisco ISE 서버가 CoA 요청을 통해 NAD에 재인증을 명령하기 전에 릴리스가 수행되어야 하므로, 이 시간 값은 짧은 것이 좋습니다.
- **Delay to CoA __ Seconds(CoA __**초 지연**)**: Cisco ISE의 CoA 실행을 지연할 시간을 입력합니다. 애플릿을 다운로드하고 클라이언트에서 IP 릴리스를 수행할 수 있도록 충분한 시간을 입력해야 합니다. 특별한 경우가 아니면 기본값을 사용하면 됩니다.
- **Delay to Renew __ Seconds(**갱신 __초 지연**)**: 값 갱신을 지연할 시간을 입력합니다. 이 시간은 IP 릴리스 값에 추가되며, 컨트롤을 다운로드할 때까지는 시간 측정이 시작되지 않습니다. CoA를 처리하고 새 VLAN 액세스 권한을 부여할 수 있도록 충분한 시간을 입력해야 합니다. 특별한 경우가 아니면 기본값을 사용하면 됩니다.

게스트 포털용 인증 성공 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Authentication Success Settings(**인증 성공 설정**)**입니다.

다음과 같은 설정을 사용하여 사용자(게스트, 스폰서 또는 직원 중 해당하는 사용자)에게 인증 성공을 알리거나 URL을 표시합니다. **Once authenticated, take guest to(**인증 후 게스트를 다음으로 이동**):** 에서 다음의 필드를 구성합니다.

- **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 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.

- **Authentication Success page(**인증 성공 페이지**)**: 사용자에게 인증이 성공했음을 알리는 페이지입니다.

- **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. 리디렉션 URL이 NAD의 액세스 제어 목록 및 해당 NAD에 대해 ISE에 구성된 권한 부여 프로파일에 의해 PSN의 포트 8443에서 작동하도록 허용되어야 합니다.

게스트 포털용 지원 정보 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **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	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.
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.

필드	사용 지침
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.

스폰서 포털 애플리케이션 설정

포털 ID 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals or Sponsor Portals(**게스트 포털 또는 스폰서 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Guest Portals or Sponsor Portals Settings and Customization(**게스트 포털 또는 스폰서 포털 설정 및 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.

스폰서 포털용 포털 설정

다음과 같은 설정을 구성하여 포털을 식별하고 모든 포털 페이지에 사용할 언어 파일을 선택합니다.

- **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.

- **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.
- **Allow Kerberos(Kerberos** 허용**)**: 스폰서 포털에 대한 스폰서의 액세스를 허용할 때 Kerberos를 사용해 스폰서를 인증합니다. Kerberos SSO는 브라우저가 ISE와의 SSL 연결을 설정한 후 보안 터널 내부에서 수행됩니다.

참고 Kerberos 인증을 사용하려면 다음 항목이 동일한 도메인에 있어야 합니다.

- 스폰서의 PC
- ISE PSN
- 이 스폰서 포털에 대해 구성된 FQDN

참고 Kerberos 인증은 게스트 포털에 대해 지원되지 않습니다.

- **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.
- **SSIDs Available to Sponsors(**스폰서가 사용할 수 있는 **SSID)**: 게스트의 방문 시 연결할 올바른 네트워크로 스폰서가 게스트에게 알릴 수 있는 네트워크의 SSID(Session Service Identifiers) 또는 이름을 입력합니다.

스폰서 포털용 로그인 설정

스폰서 포털용 로그인 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**게스트 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Login Page Settings(**로그인 페이지 설정**)**입니다.

- **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.
- **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 횟

수)에 정의된 횟수만큼 실패한 후 다시 로그인을 시도할 때까지 사용자가 대기해야 하는 시간을 분 단위로 설정합니다.

- **Include an AUP(AUP** 포함**)**: 허용되는 사용 정책 창을 플로우에 추가합니다. AUP를 창에 추가하거나 다른 창으로 연결할 수 있습니다.

스폰서 포털용 **AUP(Acceptable Use Policy)** 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 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(Acceptable Use Policy)** 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.

스폰서 포털용 스폰서 비밀번호 변경 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Create, Edit or Duplicate(**생성, 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Sponsor Change Password Settings(**스폰서 비밀번호 변경 설정**)**를 선택합니다. 이 설정은 스폰서 포털을 사용하여 스폰서에 대한 비밀번호 요건을 정의합니다.

필드	사용 지침
Allow sponsors to change their own passwords(스폰서의 비밀번호 변경 허용)	스폰서가 스폰서 포털에 로그인한 후 비밀번호를 변경하도록 허용합니다. 스폰서가 내부 사용자 데이터베이스에 포함되어 있는 경우에만 이 옵션을 선택하면 비밀번호 변경 페이지가 표시됩니다.

스폰서 포털용 로그인 후 배너 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals or Sponsor Portals(**게스트 포털 또는 스폰서 포털**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 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	사용 지침
Include a Post-Login Banner page(로그인 후 배너 페이지 포함**)**	사용자가 정상적으로 로그인하여 네트워크 액세스 권한을 부여받기 전에 추가 정보를 표시합니다.

스폰서 포털용 지원 정보 페이지 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 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	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.
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.

필드	사용 지침
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.

게스트에게 스폰서 포털의 맞춤화 알림

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Create, Edit or Duplicate(**생성, 편집 또는 복제**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Notify Guests(**게스트에게 알림**)**입니다.

Page Customizations(페이지 사용자 맞춤화**)**에서 스폰서가 스폰서 포털에서 게스트에게 보내는 알림에 나타나는 메시지, 제목, 내용, 지침 및 필드/버튼 레이블을 사용자 맞춤화할 수 있습니다.

Settings(설정**)**에서 스폰서가 이메일 또는 SMS를 사용하여 게스트에게 사용자 이름과 비밀번호를 별도로 보낼 수 있는지 여부를 지정할 수 있습니다. 또한 헬프 데스크에서 액세스 문제를 해결하는 데 사용할 수 있는 정보를 제공하기 위해 스폰서가 게스트에 대해 지원 정보 페이지를 표시할 수 있는지 여부도 지정할 수 있습니다.

스폰서 포털의 맞춤화 관리 및 승인

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Create, Edit or Duplicate(**생성, 편집 또는 복제**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Manage and Approve(**관리 및 승인**)**입니다.

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

사용자 맞춤화 가능한 항목에는 계정(등록된 계정 및 보류 중인 계정) 요약/상세 보기, 스폰서가 게스트 계정에 대해 수행하는 편집/연장/일시 중지 등의 작업을 기준으로 표시되는 팝업 대화 상자, 그리고 일반 포털 및 계정 작업 메시지가 포함됩니다.

게스트 및 스폰서 포털용 전역 설정

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Guest Access**(게스트 액세스) > **Settings**(설정)를 선택합니다. Cisco ISE에서 게스트/스폰서 포털, 게스트 유형 및 스폰서 그룹에 적용되는 다음 일반 설정을 구성할 수 있습니다.

- 게스트 계정을 비우기하고 사용자 이름과 비밀번호를 생성하기 위한 정책
- 게스트 및 스폰서에게 이메일과 SMS 알림을 보낼 때 사용할 SMTP 서버 및 SMS 게이트웨이
- 게스트 계정을 생성할 때와 셀프 등록 게스트 포털을 사용하여 게스트를 등록할 때 선택할 위치, 표준 시간대, SSID 및 사용자 맞춤화 필드

이러한 전역 설정을 구성하고 나면 특정 게스트/스폰서 포털, 게스트 유형 및 스폰서 그룹을 구성할 때 해당 설정을 필요한 대로 사용할 수 있습니다.

Portal Settings(포털 설정) 페이지에는 다음과 같은 탭이 있습니다.

- **Guest Account Purge Policy**(게스트 계정 제거 정책): 만료된 게스트 계정을 비울 시기를 예약합니다. 자세한 내용은 만료된 게스트 계정을 비울 시기 예약, 361 페이지를 참고하십시오.
- **Custom Fields**(맞춤형 필드): 사용자로부터 추가 정보를 검색하기 위해 게스트 포털에서 사용할 맞춤형 필드를 추가합니다. 자세한 내용은 게스트 계정 생성용 사용자 맞춤화 필드 추가, 362 페이지를 참고하십시오.
- **Guest Email Settings**(게스트 이메일 설정): 게스트에게 계정 변경 사항에 대한 알림을 이메일로 보낼지 여부를 결정합니다. 자세한 내용은 이메일 알림용 이메일 주소 및 SMTP 서버 지정, 363 페이지를 참고하십시오.
- **Guest Locations and SSIDs**(게스트 위치 및 **SSID**): 네트워크의 위치를 구성하고 이러한 위치에서 게스트가 사용할 수 있는 SSID(Service Set Identifier)를 구성합니다. 자세한 내용은 게스트 위치 및 SSID 할당, 364 페이지를 참고하십시오.
- **Guest Username Policy**(게스트 사용자 이름 정책): 게스트 사용자 이름 생성 방법을 구성합니다. 자세한 내용은 게스트 사용자 이름 정책 설정, 367 페이지 및 게스트 비밀번호 정책에 대한 규칙, 365 페이지를 참조하십시오.
- **Guest Password Policy**(게스트 비밀번호 정책): 모든 게스트 및 스폰서 포털에 대한 게스트 비밀번호 정책을 정의합니다. 자세한 내용은 게스트 비밀번호 정책 및 만료 설정, 366 페이지를 참고하십시오.
- **Logging**(로깅): 게스트 사용자가 디바이스의 MAC 주소로 추적됩니다. 게스트 사용자가 보고서에 표시될 때 사용자 이름은 MAC 주소입니다. 이 옵션을 선택하면 보고서에 포털 사용자 ID가 MAC 주소 대신 사용자 이름으로 표시됩니다. 이 옵션에 대한 자세한 내용은 게스트 이름 기억, 391 페이지를 참고하십시오.

게스트 유형 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Types(**게스트 유형**)**입니다. 다음과 같은 설정을 사용하여 네트워크에 액세스할 수 있는 게스트의 유형 및 게스트의 액세스 권한을 생성합니다. 이 게스트 유형을 생성할 수 있는 스폰서 그룹도 지정할 수 있습니다.

- **Guest type name(**게스트 유형 이름**)**: 이 게스트 유형과 다른 게스트 유형을 구분하는 이름을 1~256자로 입력합니다.
- **Description(**설명**)**: 이 게스트 유형의 권장 사용 방식(예: 셀프 등록 게스트에 사용)에 대한 추가 정보를 최대 2,000자까지 입력합니다.
- **Language File(**언어 파일**)**: 이 필드를 사용하면 지원되는 모든 언어의 이메일 제목, 이메일 메시지 및 SMS 메시지에 대한 콘텐츠가 포함된 언어 파일을 내보내고 가져올 수 있습니다. 이러한 언어 및 콘텐츠는 만료된 계정에 대한 알림에 사용되며 이 게스트 유형에 할당된 게스트에게 전송됩니다. 새 게스트 유형을 생성하는 경우에는 게스트 유형을 저장할 때까지 이 기능이 비활성화됩니다. 언어 파일 편집에 대한 자세한 내용은 포털 언어 사용자 맞춤화, 479 페이지를 참조하십시오.
- **Collect Additional Data(**추가 데이터 수집**)**: 이 게스트 유형을 사용하여 게스트로부터 추가 데이터를 수집하는 데 사용할 맞춤형 필드를 선택하려면 **Custom Fields(**맞춤형 필드**)** 옵션을 클릭합니다.

  Work Centers(작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Settings(**설정**)** > **Custom Fields(**맞춤형 필드**)**에서 맞춤형 필드를 관리합니다.
- **Maximum Access Time**
  - **Account duration starts(**계정 시간 시작**)**: **From first login(**첫 번째 로그인**)**을 선택한 경우 계정 시작 시간은 게스트 사용자가 게스트 포털에 처음 로그인하면 시작되며, 종료 시간은 지정된 기간의 시간과 동일합니다. 게스트 사용자가 로그인하지 않으면 계정은 게스트 계정 비우기 정책에 의해 제거될 때까지 `Awaiting first login(첫 번째 로그인 대기 중)` 상태로 유지됩니다.

    값은 1 ~ 999일, 시간 또는 분입니다.

    셀프 등록 사용자의 계정은 사용자가 계정을 생성하여 로그온하면 시작됩니다.

    From sponsor-specified date(스폰서 지정 날짜**)**를 선택한 경우 이 게스트 유형의 게스트가 네트워크에 액세스하고 네트워크에 연결된 상태를 유지할 수 있는 최대 시간을 일, 시간 또는 분 단위로 입력합니다.

    이 설정을 변경하는 경우 이 게스트 유형을 사용하여 생성한 기존 게스트 계정에는 변경 사항이 적용되지 않습니다.
  - **Maximum account duration(**최대 계정 기간**)**: 이 게스트 유형에 할당 된 게스트가 로그온 할 수있는 기간(일, 시간 또는 분)을 입력합니다.

참고 계정 삭제 정책은 만료된 게스트 계정을 확인하고 만료 알림을 보냅니다. 이 정책은 20분마다 실행되므로 계정 기간을 20분 미만으로 설정하면 계정이 삭제되기 전에 만료 알림이 전송되지 않을 수 있습니다.

Allow access only on these days and times(이 요일과 시간에만 액세스 허용**)** 옵션을 사용하여 이 게스트 유형의 게스트에게 액세스가 제공되는 기간과 요일을 지정할 수 있습니다.

- 선택한 요일은 스폰서의 일정표에서 고를 수 있는 날짜를 제한합니다.
- 기간 및 날짜를 선택하면 스폰서 포털에 최대 계정 유지 기간이 적용됩니다.

액세스 시간에 대해 여기서 설정하는 내용은 게스트 계정을 생성할 때 스폰서 포털에서 사용할 수 있는 시간 설정에 영향을 줍니다. 자세한 내용은 스폰서가 사용할 수 있는 시간 설정 구성 , 403 페이지을 참조하십시오.

- 로그온 옵션
  - **Maximum simultaneous logins(**최대 동시 로그인 수**)**: 사용자가 이 게스트 유형이 동시에 실행할 수 있도록 할당한 최대 사용자 세션 수를 입력합니다.
  - **When guest exceeds limit(**게스트가 한도를 초과할 때**)**: **Maximum simultaneous logins(**최대 동시 로그인 수**)**를 선택하면 사용자가 최대 로그인 수에 도달했을 때 취하는 조치도 선택해야 합니다.
    - **Disconnect the oldest connection(**가장 오래된 연결 끊기**)**
    - **Disconnect the newest connection(**최신 연결 끊기**)**: **Redirect user to a portal page showing an error message(**오류 메시지가 표시되는 포털 페이지로 사용자 리디렉션**)**를 선택하면 구성 가능한 시간 동안 오류 메시지가 표시되었다가 세션의 연결이 끊기며 사용자는 게스트 포털로 리디렉션됩니다. 포털 페이지 사용자 맞춤화 대화 상자의 **Messages(**메시지**)** > **Error Messages(**오류 메시지**)** 창에서 오류 페이지 내용을 구성합니다.
  - **Maximum devices guests can register(**게스트가 등록할 수 있는 최대 디바이스 수**)**: 각 게스트에게 등록할 수 있는 디바이스의 최대 수를 입력합니다. 이 게스트 유형의 게스트에 대해 이미 등록된 값보다 더 작은 숫자로 제한을 설정할 수 있습니다. 이 제한은 새로 생성하는 게스트 계정에만 적용됩니다. 새 디바이스가 추가되고 최대 값에 도달하면 가장 오래된 디바이스의 연결이 끊어집니다.
  - **Endpoint identity group for guest device registration(**게스트 디바이스 등록을 위한 엔드포인트 **ID** 그룹**)**: 게스트 디바이스에 할당할 수 있는 엔트포인트 ID 그룹을 선택합니다. Cisco ISE는 기본값으로 사용할 **GuestEndpoints** 엔드포인트 ID 그룹을 제공합니다. 기본값을 사용하지 않으려는 경우에는 엔드포인트 ID 그룹을 추가로 생성할 수도 있습니다.
  - **Allow guest to bypass the Guest portal(**게스트의 게스트 포털 바이패스 허용**)**: 사용자가 자격 증명이 지정된 게스트 종속 포털(웹 인증 페이지)을 바이패스하고 유/무선(dot1x) 신청자 또는 VPN 클라이언트에 자격 증명을 제공하여 네트워크에 액세스하도록 허용합니다. 게스

트 계정은 `Awaiting Initial Login(초기 로그인 대기)`를 바이패스 그리고 AUP가 필요해도 AUP 페이지를 바이패스해서 `Active(활성)` 상태로 변경됩니다.

이 설정을 활성화하지 않는 경우 사용자는 먼저 자격 증명이 지정된 게스트 종속 포털을 통해 로그인해야 네트워크의 다른 부분에 액세스할 수 있습니다.

- 계정 만료 알림
  - **Send account expiration notification __ days before account expires(**계정 만료 __일 전 계정 만료 알림 전송**)**: 게스트의 계정이 만료되기 전에 게스트에게 알림을 전송하고 만료 전에 알림을 보낼 기간을 일, 시간 또는 분 단위로 지정합니다.
  - **View messages in(**메시지 보기 언어**)**: 이메일 또는 SMS 알림을 설정할 때 해당 알림을 표시하는 데 사용할 언어를 지정합니다.
  - **Email(**이메일**)**: 이메일로 계정 만료 알림을 보냅니다.
  - **Use customization from(**사용자 맞춤화 선택**)**: 선택한 포털에 대해 구성한 것과 동일한 사용자 맞춤화을 이 게스트 유형의 계정 만료 이메일에 적용합니다.
  - **Copy text from(**텍스트 복사**)**: 계정 만료 알림에 대해 다른 게스트 유형용으로 생성한 이메일 텍스트를 재사용합니다.
  - **SMS**: SMS로 계정 만료 알림을 보냅니다.

    Send test SMS to me(나에게 테스트 **SMS** 보내기**)**의 경우 SMS 게이트웨이를 선택한다는 점을 제외하고 SMS에 대한 설정은 이메일 알림과 동일합니다.
- **Sponsor Groups(**스폰서 그룹**)**: 멤버가 이 게스트 유형을 사용하여 게스트 계정을 생성할 수 있는 스폰서 그룹을 지정합니다. 이 게스트 유형에 액세스하지 않으려는 스폰서 그룹을 삭제합니다.

스폰서 그룹 설정

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Groups(**스폰서 그룹**)**입니다. 다음과 같은 설정을 사용하여 스폰서 그룹에 멤버를 추가하고, 게스트 유형 및 위치 권한을 정의하고, 게스트 계정 생성 및 관리와 관련된 권한을 설정합니다.

- **Disable Sponsor Group(**스폰서 그룹 비활성화**)**: 이 스폰서 그룹 멤버의 스폰서 포털 액세스를 비활성화합니다.

  예를 들어 관리 포털에서 컨피그레이션을 변경하는 동안 스폰서가 스폰서 포털에 일시적으로 로그인하지 못하도록 할 수 있습니다. 또는 연간 회의에 대한 게스트 후원 등 자주 수행하지 않는 활동과 관련된 스폰서 그룹을 다시 활성화해야 할 때까지 비활성화할 수도 있습니다.
- **Sponsor group name(**스폰서 그룹 이름**)**: 고유한 이름(1~256자)을 입력합니다.
- **Description(**설명**)**: 이 스폰서 그룹에 사용되는 게스트 유형과 같은 유용한 정보(최대 2,000자)를 입력합니다.

- **Configure Guest Types(**게스트 유형 구성**)**: 필요한 게스트 유형을 사용할 수 없는 경우 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Types(**게스트 유형**)**를 클릭하고 새 게스트 유형을 생성하거나 기존 게스트 유형을 편집합니다.
- 매치 기준
  - **Members(**멤버**)**: 사용 가능한 사용자 ID 그룹(내부 및 외부 ID 저장소)을 선택하여 이 스폰서 그룹의 멤버로 추가할 수 있는 **Select Sponsor Group Members(**스폰서 그룹 멤버 선택**)** 상자를 표시하려면 클릭합니다.
    - **Sponsor Group Members(**스폰서 그룹 멤버**)**: 선택한 스폰서 그룹 목록을 검색 및 필터링하여 포함하지 않을 그룹을 삭제합니다.
  - **Other conditions(**기타 조건**)**: **Create New Condition(**새 조건 생성**)**을 클릭해, 스폰서가 이 스폰서 그룹에 포함시킬 수 있도록 일치시켜야 하는 한 개 이상의 조건을 설정합니다. Active Directory, LDAP, SAML, ODBC ID 저장소(RADIUS Token 또는 RSA SecurID 저장소는 불가능)의 인증 속성을 사용할 수 있습니다. 내부 사용자 속성을 사용할 수도 있습니다. 조건에는 속성, 연산자, 값이 있습니다.
    - 내부 사전 속성 *Name(*이름*)*을 사용해 조건을 생성하려면 사용자 ID 그룹을 ID 그룹 이름의 접두사로 사용해야 합니다. 예를 들면 다음과 같습니다.

      InternalUser:Name EQUALS bsmith

      즉, "bsmith"라는 이름을 가진 내부 사용자만 이 스폰서 그룹에 속할 수 있는 것입니다.
- **This sponsor group can create accounts using these guest types(**이 스폰서 그룹이 계정을 생성하는 데 사용할 수 있는 게스트 유형**)**: 이 스폰서 그룹의 멤버가 게스트 계정을 생성할 때 사용할 수 있는 게스트 유형을 지정합니다. 스폰서 그룹을 활성화하려면 사용 가능한 게스트 유형이 하나 이상 있어야 합니다.

  이 스폰서 그룹에 대해 게스트 유형을 하나만 할당하는 경우 스폰서 포털에서 해당 게스트 유형을 표시하지 않도록 선택할 수 있습니다. 포털에서 사용할 수 있는 유효한 게스트 유형이 해당 유형뿐이기 때문입니다. **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portal(**스폰서 포털**)** > **Page Customization(**페이지 사용자 맞춤화**)** > **Create Accounts(**계정 생성**)** > **Guest Types(**게스트 유형**)** > **Settings(**설정**)**를 선택합니다. **Hide guest type if only one is available to sponsor(**스폰서에 사용 가능한 게스트 유형이 하나뿐인 경우 게스트 유형 숨기기**)**를 선택하여 이 옵션을 활성화합니다.
- **Select the locations that guests will be visiting(**게스트가 방문할 위치 선택**)**: 게스트가 계정을 생성할 때 할당받을 수 있는 위치를 선택합니다. 이러한 위치를 선택하면 해당 게스트 계정에 대해 유효한 표준 시간대를 정의할 수 있으며, 유효한 액세스 시간 등 게스트에 적용되는 모든 시간 매개변수가 지정됩니다. 이 위치를 선택하더라도 게스트는 다른 위치의 네트워크에 연결할 수 있습니다.

  스폰서 그룹을 활성화하려면 사용 가능한 위치가 하나 이상 있어야 합니다.

이 스폰서 그룹에 위치를 하나만 할당하는 경우 스폰서 그룹의 멤버가 생성하는 게스트 계정에 대해 유효한 표준 시간대는 이 위치뿐입니다. 이 위치는 기본적으로 스폰서 포털에 표시되지 않습니다.

후원자가 생성할 수 있는 항목

- **Multiple guest accounts assigned to specific guests (Import)(**특정 게스트에 할당되는 여러 게스트 계정**(**가져오기**))**: 스폰서가 이름, 성 등의 게스트 세부정보를 파일에서 가져와 여러 게스트 계정을 생성하는 기능을 활성화합니다.

  이 옵션을 활성화하면 **Import(**가져오기**)** 옵션이 스폰서 포털의 계정 생성 페이지에 표시됩니다. Import(가져오기) 옵션은 Internet Explorer, Firefox, Safari 등의 데스크톱 브라우저에서만 사용 가능하며 모바일에서는 사용할 수 없습니다.

- **Limit to batch of(**다음의 배치로 제한**)**: 이 스폰서 그룹이 여러 계정을 동시에 생성할 수 있는 경우 단일 가져오기 작업에서 생성할 수 있는 게스트 계정의 수를 지정합니다.

  스폰서는 최대 10,000개의 계정을 생성할 수 있지만 성능 문제가 발생할 가능성이 있으므로 생성하는 계정 수를 제한하는 것이 좋습니다.

- **Multiple guest accounts to be assigned to any guests (Random)(**임의의 게스트에 할당되는 여러 게스트 계정**(**임의**))**: 게스트가 아직 확인되지 않았거나 많은 수의 계정을 빠르게 생성해야 하는 경우 스폰서가 여러 임의 게스트 계정을 자리 표시자로 생성하는 기능을 활성화합니다.

  이 옵션을 활성화하면 **Random(**임의**)** 옵션이 스폰서 포털의 계정 생성 창에 표시됩니다.

- **Default username prefix(**기본 사용자 이름 접두사**)**: 여러 임의 게스트 계정을 생성할 때 스폰서가 사용할 수 있는 사용자 이름 접두사를 지정합니다. 이 접두사는 지정하는 경우 임의 게스트 계정을 생성할 때 스폰서 포털에 나타납니다. 또한 **Allow sponsor to specify a username prefix(**스폰서의 사용자 이름 접두사 지정 허용**)** 옵션의 설정에 따라 결과가 다음과 같이 달라집니다.

  - Enabled(활성화됨): 스폰서가 스폰서 포털에서 기본 접두사를 편집할 수 있습니다.
  - Not enabled(활성화 안 함): 스폰서가 스폰서 포털에서 기본 접두사를 편집할 수 없습니다.

  사용자 이름 접두사를 지정하지 않거나 스폰서가 접두사를 지정하도록 허용하지 않으면 스폰서는 스폰서 포털에서 사용자 이름 접두사를 할당할 수 없습니다.

- **Allow sponsor to specify a username prefix(**스폰서의 사용자 이름 접두사 지정 허용**)** 이 스폰서 그룹이 여러 계정을 동시에 생성할 수 있는 경우 단일 가져오기 작업에서 생성할 수 있는 게스트 계정의 수를 지정합니다.

  스폰서는 최대 10,000개의 계정을 생성할 수 있지만 성능 문제가 발생할 가능성이 있으므로 생성하는 계정 수를 제한하는 것이 좋습니다.

- **Start date can be no more than __ days into the future(**시작 날짜는 앞으로 __일 이내여야 함**)**: 스폰서가 생성한 여러 게스트 계정에 대해, 여기에 지정한 기간(일수) 내로 시작 날짜를 설정해야 합니다.

스폰서가 관리할 수 있는 항목

- **Only accounts sponsor has created(**스폰서가 생성한 계정만**)**: 이 그룹의 스폰서가 스폰서의 이메일 계정을 기준으로 하여 자신이 생성한 게스트 계정만 보고 관리할 수 있습니다.
- **Accounts created by members of this sponsor group(**이 스폰서 그룹의 멤버가 생성한 계정**)**: 스폰서가 이 스폰서 그룹의 모든 스폰서에 의해 생성된 게스트 계정을 보고 관리할 수 있습니다.
- **All guest accounts(**모든 게스트 계정**)**: 스폰서가 보류 중인 모든 게스트 계정을 관리 할 수 있습니다.

참고 그룹 멤버십과 관계없이 모든 스폰서는 보류 중인 모든 계정을 볼 수 있습니다. 단, **Sponsor Can(**스폰서가 수행할 수 있는 작업**)** 아래에 **Only pending accounts assigned to this sponsor(**이 스폰서에게 할당된 보류 중인 계정만**)** 옵션과 함께 **Approve and view requests from self-registering guests(**셀프 등록 게스트의 요청 승인**)**를 선택한 경우는 예외입니다.

스폰서가 수행할 수 있는 작업

- **Update guests' contact information (email, Phone Number)(**게스트 연락처 정보 업데이트**(**이메일**,** 전화 번호**))**: 스폰서가 관리할 수 있는 게스트 계정에 대해 게스트의 연락처 정보를 변경할 수 있도록 허용합니다.
- **View/print guests 'passwords(**게스트 비밀번호 보기/인쇄**)**: 이 옵션을 활성화하면 스폰서가 게스트의 비밀번호를 인쇄할 수 있습니다. 스폰서는 **Manage Accounts(**계정 관리**)** 창과 게스트의 세부정보에서 게스트의 비밀번호를 볼 수 있습니다. 이 옵션을 선택하지 않으면 스폰서는 비밀번호를 인쇄할 수 없지만 사용자는 그대로 이메일 또는 SMS를 통해 비밀번호를 가져올 수 있습니다(구성된 경우).
- **Send SMS notifications with guests' credentials(**게스트 자격 증명을 사용하여 **SMS** 알림 보내기**)**: 스폰서가 관리 가능한 게스트 계정에 대해 게스트의 계정 세부정보 및 로그인 자격 증명을 사용하여 게스트에게 SMS(텍스트) 알림을 보낼 수 있도록 허용합니다.
- **Reset guest account passwords(**게스트 계정 비밀번호 재설정**)**: 스폰서가 관리 가능한 게스트 계정에 대해 게스트의 비밀번호를 Cisco ISE에서 생성된 임의의 비밀번호로 재설정할 수 있도록 허용합니다.
- **Extend guests' accounts(**게스트 계정 연장**)**: 스폰서가 관리 가능한 게스트 계정을 만료 날짜 이후로 연장할 수 있도록 허용합니다. 스폰서는 계정 만료와 관련하여 게스트에게 전송되는 이메일 알림에 자동으로 복사됩니다.
- **Delete guests' accounts(**게스트 계정 삭제**)**: 스폰서가 관리 가능한 게스트 계정을 삭제하고 게스트의 회사 네트워크 액세스를 차단할 수 있도록 허용합니다.
- **Suspend guests' accounts(**게스트 계정 일시 중지**)**: 스폰서가 관리 가능한 게스트 계정을 일시 중지하여 게스트의 로그인을 일시적으로 차단할 수 있도록 허용합니다.

  이 동작을 수행하는 경우 CoA(Change of Authorization)도 실행되어 일시 중지된 게스트가 네트워크에서 제거됩니다.

- **Require sponsor to provide a reason(**스폰서가 이유를 제공해야 함**)**: 스폰서가 게스트 계정 일시 중지에 대한 설명을 제공해야 합니다.

- **Approve and view requests from self-registering guests(**셀프 등록 게스트의 요청 승인 및 보기**)**: 이 스폰서 그룹에 포함되어 있는 스폰서는 셀프 등록 게스트(승인 필요)의 보류 중인 모든 계정 요청을 볼 수 있거나, 사용자가 방문 중인 사용자로서 스폰서 이메일 주소를 입력한 요청만 볼 수 있습니다. 이 기능을 사용하려면 셀프 등록 게스트가 사용하는 포털에서 **Require self-registered guests to be approved(**셀프 등록 게스트를 승인해야 함**)**를 선택해야 하며 스폰서의 이메일이 연락 대상으로 나열되어 있어야 합니다.
  - 모든 보류 중인 계정: 이 그룹에 속한 스폰서는 모든 스폰서가 생성한 어카운트를 승인하고 검토합니다.
  - 이 스폰서에게 할당된 보류 중인 계정만: 이 그룹에 속한 스폰서가 자신이 생성한 계정만 보고 승인할 수 있습니다.

- **Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)(**프로그래밍 인터페이스**(**게스트 **REST API)**를 사용하여 **Cisco ISE** 게스트 계정에 액세스**)**: 스폰서가 관리 가능한 게스트 계정에 대해 게스트 REST API 프로그래밍 인터페이스를 사용하여 게스트 계정에 액세스할 수 있도록 허용합니다.

최종 사용자 포털

Cisco ISE는 다음 3가지 기본 최종 사용자 집합에 대한 웹 기반 포털을 제공합니다.

- 게스트 포털(핫스팟 및 자격 증명이 있는 게스트 포털)을 사용하여 엔터프라이즈 네트워크에 일시적으로 액세스해야 하는 게스트
- 스폰서 포털을 사용하여 게스트 계정을 생성 및 관리하는 스폰서로 지정된 직원
- BYOD(Bring Your Own Device), MDM(Mobile Device Management) 및 내 디바이스 포털과 같은 다양한 비게스트 포털을 사용하여 엔터프라이즈 네트워크에서 개인 디바이스를 사용하는 직원

최종 사용자 웹 포털의 사용자 맞춤화

더 많은 포털을 편집, 복제 및 생성할 수 있습니다. 또한 포털 모양을 완전히 사용자 맞춤화할 수 있으므로 포털 환경 역시 사용자 맞춤화할 수 있습니다. 다른 포털에 영향을 미치지 않고 각 개별 포털을 사용자 맞춤화할 수 있습니다.

포털 인터페이스에서 다음과 같이 전체 포털에 적용되거나 포털의 특정 페이지에 적용되는 다양한 특성을 사용자 맞춤화할 수 있습니다.

- 테마, 이미지, 색상, 배너 및 바닥글
- 포털 텍스트, 오류 메시지 및 알림을 표시하는 데 사용되는 언어

- 제목, 콘텐츠, 지침 및 필드 및 버튼 레이블
- 이메일, SMS 및 프린터를 통해 게스트에게 전송되는 알림(셀프 등록 게스트 및 스폰서 포털에만 적용됨)
- 사용자에게 표시되는 오류 및 정보 메시지
- 셀프 등록 게스트 및 스폰서 포털의 경우 사용자 요구 사항에 따라 게스트 정보를 수집할 수 있는 사용자 맞춤화 필드를 생성할 수 있습니다.

ISE 커뮤니티 리소스

웹 포털 사용자 맞춤화에 대한 자세한 내용은 ISE Portal Builder 및 HowTo: ISE Web Portal Customization Options를 참고하십시오.

사용자 맞춤화 방법

최종 사용자 포털 페이지를 사용자 맞춤화할 수 있는 방법은 여러 가지가 있으며 각기 다른 지식 수준이 요구됩니다.

- **Basic(**기본**)**: 포털 사용자 맞춤화 페이지를 수정할 수 있습니다.
  - 배너 및 로고 업로드
  - 색상 변경(버튼 제외)
  - 화면의 텍스트 및 전체 포털에 사용되는 언어 변경
- 중급
  - 미니 편집기를 사용하여 HTML 및 Javascript 추가

  참고 미니 편집기에서 HTML을 입력하기 전에 HTML 아이콘을 클릭합니다.

  - jQuery 모바일 테마 롤러를 사용하여 모든 페이지 요소의 색상 변경
- 고급
  - 속성 및 CSS 파일을 수동으로 수정

포털을 사용자 맞춤화하고 나면 복제를 통해 여러 포털(동일한 유형)을 생성할 수 있습니다. 예를 들어 한 비즈니스 엔티티의 핫스팟 게스트 포털을 맞춤화한 경우 해당 포털을 복제하고 일부 내용을 변경하여 다른 비즈니스 엔티티를 위한 맞춤화 핫스팟 게스트 포털을 생성할 수 있습니다.

미니 편집기를 사용하여 포털을 사용자 맞춤화하기 위한 팁

- 미니 편집기 상자에 긴 단어를 입력하면 포털의 화면 영역 밖으로 스크롤될 수 있습니다. HTML 단락 속성 style="word-wrap: break-word"를 사용하여 줄을 바꿀 수 있습니다. 예를 들면 다음과 같습니다.

```
<p style="word-wrap:break-word">
thisisaverylonglineoftextthatwillexceedthewidthoftheplacethatyouwanttoputitsousethisstructure
</p>
```

- HTML 또는 javascript를 사용하여 포털 페이지를 사용자 맞춤화하는 경우 유효한 syntax(명령문)를 사용해야 합니다. 미니 편집기에 입력하는 태그와 코드는 ISE에서 검증되지 않습니다. 유효하지 않은 syntax(명령문)를 사용하면 포털 플로우 중에 문제가 발생할 수 있습니다.

포털 콘텐츠 유형

Cisco ISE는 "있는 그대로" 사용하거나, 기존 CSS 파일을 모델로 사용하여 새 사용자 맞춤화 파일을 생성하여 사용자 맞춤화할 수 있는 기본 포털 테마 집합을 제공합니다. 그러나 사용자 맞춤화된 CSS 파일을 사용하지 않고도 포털의 모양을 변경할 수 있습니다.

예를 들어 고유한 회사 로고 및 배너 이미지를 사용하려는 경우에는 새 이미지 파일을 업로드하여 사용하면 됩니다. 여러 가지 요소와 포털 영역의 색상을 변경하여 기본 색 구성표를 사용자 맞춤화할 수 있습니다. 자신이 변경하는 사용자 맞춤화 항목을 볼 때 사용할 언어를 선택할 수도 있습니다.

로고 및 배너를 대체할 이미지를 디자인하는 경우 다음 픽셀 크기에 최대한 가깝게 이미지를 작성해 주십시오.

배너	1724X133
데스크톱 로고	86X45
모바일 로고	80X35

ISE에서 포털에 맞게 이미지 크기를 조정하지만, 너무 작은 이미지는 크기를 조정해도 적절히 표시되지 않을 수 있습니다.

페이지 레이아웃 변경 또는 포털 페이지에 비디오 클립 또는 광고 추가 등의 고급 사용자 맞춤화를 수행하려는 경우 고유한 사용자 맞춤화 CSS 파일을 사용할 수 있습니다.

특정 포털에서 이러한 유형의 변경 사항은 해당 포털의 모든 페이지에 전역적으로 적용됩니다. 페이지 레이아웃 변경 사항은 전역적으로 적용될 수도 있고, 포털의 특정 한 페이지에만 적용될 수 있습니다.

포털 페이지 제목, 콘텐츠 및 레이블

제목, 텍스트 상자, 지침, 필드 및 버튼 레이블, 그리고 게스트가 최종 사용자 웹 포털 페이지에서 볼 수 있는 다른 시각적 요소를 사용자 맞춤화할 수 있습니다. 페이지를 사용자 맞춤화하면서 즉석에서 페이지 설정을 편집할 수도 있습니다.

이러한 변경 사항은 사용자 맞춤화하는 특정 페이지에만 적용됩니다.

포털의 기본 사용자 맞춤화

사용자 요구 사항에 부합되는 미리 정의된 테마를 선택하고 기본 설정을 대부분 사용할 수 있습니다. 그런 후 다음과 같은 기본 사용자 맞춤화를 수행할 수 있습니다.

- 포털 테마 색상 수정, 452 페이지
- 포털 아이콘, 이미지 및 로고 변경, 453 페이지
- 포털 배너 및 바닥글 요소 업데이트, 454 페이지
- 포털 표시 언어 변경, 453 페이지
- 제목, 지침, 버튼 및 레이블 텍스트 변경, 455 페이지
- 텍스트 상자 내용 서식 및 스타일 지정, 455 페이지

팁 업데이트하면서 사용자 맞춤화 내용 보기, 460 페이지 작업을 수행할 수 있습니다.

포털 테마 색상 수정

기본 포털 테마의 기본 색 구성표를 사용자 맞춤화하고 포털의 다양한 요소와 영역 색상을 변경할 수 있습니다. 이러한 변경사항은 사용자 맞춤화하는 전체 포털에 적용됩니다.

포털 색상을 변경하려는 경우 다음 사항에 유의해 주십시오.

- 이 옵션을 사용하여 해당 포털에 사용하기 위해 가져왔을 수 있는 사용자 맞춤화 포털 테마의 색 구성표를 변경할 수는 없습니다. 색상 설정을 변경하려면 사용자 맞춤화 테마 CSS 파일을 편집해야 합니다.
- 포털 테마에서 색상을 변경한 후 **Portal Theme(**포털 테마**)** 드롭다운 메뉴에서 다른 포털 테마를 선택하면 원래 포털 테마에서 변경사항이 손실되며 기본 색상으로 되돌아갑니다.
- 이미 수정한 색 구성표를 사용하여 포털 테마의 색상을 조정한 다음 테마를 저장하기 전에 색상을 재설정하면 색 구성표가 기본 색상으로 되돌아가며 이전 수정사항은 손실됩니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Configure(**구성**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Portal Theme(**포털 테마**)** 드롭다운 목록에서 기본 테마 중 하나를 선택합니다.

단계 **3** **Tweaks(**조정**)**를 클릭하여 선택한 기본 포털 테마의 색상 설정 중 일부를 재정의합니다.

a) 배너/페이지 배경, 텍스트 및 레이블의 색상 설정을 변경합니다.
b) 테마의 기본 색 구성표로 되돌리려면 **Reset Colors(**색상 재설정**)**를 클릭합니다.
c) **OK(**확인**)**를 클릭하면 **Preview(**미리 보기**)**에서 색상 변경사항을 확인할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

포털 표시 언어 변경

사용자 맞춤화 변경을 수행하면서 해당 변경사항을 확인할 언어를 선택할 수 있습니다. 이러한 변경사항은 사용자 맞춤화하는 전체 포털에 적용됩니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Global Customization(**전역 사용자 맞춤화**)**를 선택합니다.
- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Global Customization(**전역 사용자 맞춤화**)**를 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Global Customization(**전역 사용자 맞춤화**)**을 선택합니다.

단계 **2** **View In(**표시 언어**)** 드롭다운 목록에서 페이지를 사용자 맞춤화하는 동안 텍스트를 표시할 언어를 선택합니다.

이 드롭다운 목록에는 특정 포털과 연결된 언어 파일의 모든 언어가 포함되어 있습니다.

다음에 수행할 작업

포털 페이지를 사용자 맞춤화하는 동안 선택한 언어로 수행한 모든 변경사항을 지원되는 모든 언어 속성 파일에 업데이트해야 합니다.

포털 아이콘, 이미지 및 로고 변경

고유한 회사 로고, 아이콘 및 배너 이미지를 사용하려는 경우에는 사용자 맞춤화 이미지를 업로드하여 기존 이미지를 대체하기만 하면 됩니다. 지원되는 이미지 형식은 .gif, .jpg, .jpeg 및 .png입니다. 이러한 변경사항은 사용자 맞춤화하는 전체 포털에 적용됩니다.

시작하기 전에

포털 바닥글에 광고 등의 이미지를 포함하려면 이러한 이미지가 있는 외부 서버에 액세스할 수 있어야 합니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Configure(**구성**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Images(**이미지**)**에서 로고, 아이콘 및 이미지 버튼을 클릭하고 사용자 맞춤화 이미지를 업로드합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

포털 배너 및 바닥글 요소 업데이트

포털 내 모든 페이지의 배너 및 바닥글 섹션에 표시되는 정보를 사용자 맞춤화할 수 있습니다. 이러한 변경사항은 사용자 맞춤화하는 전체 포털에 적용됩니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** 모든 포털 페이지에 표시되는 **Banner title(**배너 제목**)**을 변경합니다.

단계 **3** 포털을 사용하는 게스트에 대해 다음 링크를 포함합니다.

- **Help(**도움말**)** - 온라인 도움말입니다. 스폰서 및 내 디바이스 포털에 대해서만 제공됩니다.
- **Contact(**연락처**)** - 기술 지원 정보입니다. 이 링크를 활성화하려면 지원 정보 페이지를 설정합니다.

단계 **4** 모든 포털 페이지의 아래쪽에 표시할 **Footer Elements(**바닥글 요소**)**에 고지 사항 또는 저작권 표시를 추가합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

제목, 지침, 버튼 및 레이블 텍스트 변경

포털에 표시되는 모든 텍스트를 업데이트할 수 있습니다. 사용자 맞춤화하는 페이지의 각 UI 요소에는 입력 가능한 문자 수에 대한 최소 및 최대 범위가 있습니다. 일부 텍스트 블록에서 제공되는 경우 미니 편집기를 사용하여 텍스트에 시각적 스타일을 적용할 수 있습니다. 이러한 변경사항은 사용자 맞춤화하는 특정 포털 페이지에만 적용됩니다. 이러한 페이지 요소는 이메일, SMS 및 인쇄 알림에 대해 각기 다릅니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Configure(**구성**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Pages(**페이지**)**에서 변경할 페이지를 선택합니다.

단계 **3** **Page Customizations(**페이지 사용자 맞춤화**)**에서 표시되는 UI 요소를 업데이트합니다. 모든 페이지에는 **Browser Page Title(**브라우저 페이지 제목**)**, **Content Title(**콘텐츠 제목**)**, **Instructional Text(**지침 텍스트**)**, **Content(**내용**)** 및 두 개의 **Optional Content(**선택적 콘텐츠**)** 텍스트 블록이 있습니다. **Content(**내용**)** 영역의 필드는 각 페이지별로 다릅니다.

텍스트 상자 내용 서식 및 스타일 지정

Instructional Text(지침 텍스트**)**, **Optional Content 1(**선택적 콘텐츠 **1)** 및 **Optional Content 2(**선택적 콘텐츠 **2)** 텍스트 상자에서 제공되는 미니 편집기를 사용하여 텍스트의 기본 서식 지정을 수행합니다. 이 방법으로 수행하는 변경사항은 사용자 맞춤화하는 특정 포털 페이지에만 적용됩니다.

텍스트 상자 사용 시 **Toggle Full Screen(**전체 화면 전환**)** 버튼을 사용하여 텍스트 상자의 크기를 늘리거나 줄일 수 있습니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Pages(**페이지**)**에서 변경할 페이지를 선택합니다.

단계 **3** **Page Customizations(**페이지 사용자 맞춤화**)**의 **Instructional Text(**지침 텍스트**)** 및 **Optional Content(**선택적 콘텐츠**)** 텍스트 블록에서 다음을 수행할 수 있습니다.

- 텍스트의 글꼴, 크기 및 색상 변경
- 텍스트에 굵게, 기울임꼴 또는 밑줄 스타일 지정
- 글머리 기호 및 번호 매기기 목록 생성

참고 **Toggle HTML Source(HTML** 소스 전환**)** 버튼을 사용하면 미니 편집기를 사용하여 서식을 지정한 텍스트에 적용된 HTML 태그를 확인할 수 있습니다. **HTML Source(HTML** 소스**)** 보기에서 텍스트를 편집하는 경우 **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 창에 변경 사항을 저장하기 전에 **Toggle HTML Source(HTML** 소스 전환**)** 버튼을 다시 클릭합니다.

포털 페이지 사용자 맞춤화를 위한 변수

이러한 포털 페이지 텍스트 상자의 탐색 경로는 다음과 같습니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**를 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**를 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**를 선택합니다.

포털 사용자(게스트, 스폰서 및 직원)에게 표시되는 정보의 일관성을 유지하기 위해 포털 콘텐츠 및 게스트 알림용 템플릿을 생성할 때 이러한 변수를 사용합니다. 각 포털에 대해 **Instructional Text(**지

침 텍스트**)**, **Optional Content 1(**선택적 콘텐츠 **1)** 및 **Optional Content 2(**선택적 콘텐츠 **2)** 텍스트 상자의 텍스트를 아래에 나와 있는 변수 이름으로 대체해 주십시오.

표 ***45:*** 게스트 포털용 변수 목록

표시 이름	대체할 변수 이름
Access code(액세스 코드) 이메일, 텍스트 또는 인쇄 알림을 사용하여 게스트에게 액세스 코드를 제공하는 데 사용됩니다.	ui_access_code
BYOD IOS SSID 듀얼 SSID 흐름에서 온보딩 후에 디바이스가 연결해야하는 네트워크를 지정하는 데 사용됩니다.	ui_byod_success_ios_ssid
Client Provisioning Agent Type(클라이언트 프로비저닝 에이전트 유형) AnyConnect Agent와 같이 클라이언트 프로비저닝 정책에 현재 구성되어 있는 에이전트를 지정하는 데 사용됩니다.	ui_client_provision_agent_type
Client Provisioning Agent URL(클라이언트 프로비저닝 에이전트 URL) 포스처 에이전트에 대한 다운로드 URL을 지정하는 데 사용됩니다.	ui_client_provision_agent_url
Client Provisioning agent install minutes(클라이언트 프로비저닝 에이전트 설치 시간(분)) 게스트가 클라이언트 프로비저닝 창의 설치 지침을 완료해야 하는 시간(교정 타이머에 의해 설정됨)을 알리는 데 사용됩니다. 타이머가 만료되기 전에 설치 지침을 완료하지 않는 게스트는 브라우저 페이지를 새로 고치고 로그인 프로세스를 다시 진행해야 합니다.	ui_client_provision_install_agent_mins
Company(회사)	ui_company
Email address(이메일 주소)	ui_email_address
End date and time(종료일 및 시간)	ui_end_date_time
First name(이름)	ui_first_name
Last name(성)	ui_last_name
Location name(위치 이름)	ui_location_name

표시 이름	대체할 변수 이름
Maximum registered devices(등록된 최대 디바이스 수)	ui_max_reg_devices
Maximum simultaneous logins(최대 동시 로그인 수)	ui_max_siml_login
Password(비밀번호)	ui_password
Person being visited (email)(방문 중인 사용자(이메일))	ui_person_visited
Phone number(전화번호)	ui_phone_number
Reason for visit(방문 사유)	ui_reason_visit
SMS Provider(SMS 제공자)	ui_sms_provider
SSID 게스트가 네트워크에 연결하는 데 사용할 수 있는 무선 네트워크를 지정하는 데 사용됩니다.	ui_ssid
Start date and time(시작일 및 시간)	ui_start_date_time
Time left(남은 시간)	ui_time_left
Username(사용자 이름)	ui_user_name

표 ***46:*** 스폰서 포털용 변수 목록

표시 이름	대체할 변수 이름
Guest - Company(게스트 - 회사)	ui_guest_company
Guest - Email address(게스트 - 이메일 주소)	ui_guest_email_address
Guest - End date and time(게스트 - 종료일 및 시간)	ui_guest_end_date_time
Guest - First name(게스트 - 이름)	ui_guest_first_name
Guest - Last name(게스트 - 성)	ui_guest_last_name
Guest - Location name(게스트 - 위치 이름)	ui_guest_location_name
Guest - Maximum registered devices(게스트 - 등록된 최대 디바이스 수)	ui_guest_max_reg_devices
Guest - Maximum simultaneous logins(게스트 - 최대 동시 로그인 수)	ui_guest_max_siml_login

표시 이름	대체할 변수 이름
Guest - Password(게스트 - 비밀번호)	ui_guest_password
Guest - Person being visited (email)(게스트 - 방문 중인 사용자(이메일))	ui_guest_person_visited
Guest - Phone number(게스트 - 전화번호)	ui_guest_phone_number
Guest - Reason for visit(게스트 - 방문 사유)	ui_guest_reason_visit
Guest - SMS Provider(게스트 - SMS 제공자)	ui_guest_sms_provider
Guest - SSID(게스트 - SSID) 게스트가 네트워크에 연결하는 데 사용할 수 있는 무선 네트워크를 지정하는 데 사용됩니다.	ui_guest_ssid
Guest - Start date and time(게스트 - 시작일 및 시간)	ui_guest_start_date_time
Guest - Time left(게스트 - 남은 시간)	ui_guest_time_left
Guest - Username(게스트 - 사용자 이름)	ui_guest_user_name
Username(사용자 이름) 포털에 로그인되어 있는 사용자 이름을 지정하는 데 사용됩니다.	ui_sponsor_user_name
Guest Access Information(게스트 액세스 정보**)** 창에서 "From(시작)"을 표시하는 데 사용됩니다.	ui_from_label
Guest Access Information(게스트 액세스 정보**)** 창에서 "First Login(첫 번째 로그인)"을 표시하는 데 사용됩니다.	ui_first_login_text
액세스 시간이 첫 번째 로그인에서 시작되는 경우 게스트 계정 알림 메시지를 표시하는 데 사용됩니다.	ui_notification_first_login_text
이메일 알림의 계정 기간을 나타내는 동적 변수입니다.	ui_access_duration
더 이상 사용할 수 없는 계정을 표시하는 동적 변수입니다. 시작-종료 계정의 경우 해당 날짜는 종료 날짜이고 첫 번째 로그인 계정의 경우 해당 날짜는 계정 생성 날짜에 비우기 기간(일)을 더한 날짜입니다.	ui_account_purge_date

표시 이름	대체할 변수 이름
게스트 사용자가 이전에 한 번 이상 로그인한 적이 있는 경우 스폰서가 게스트 유형을 첫 번째 로그인에서 시작-종료로 또는 그 반대로 변경하지 못하도록 제한하는 데 사용됩니다. 일반 스폰서 포털 메시지에 표시됩니다.	ui_guest_type_change_ffl_startend_not_allowed_error ui_guest_type_change_ startend_ffl_not_allowed_error

표 ***47: MDM*** 포털용 변수 목록

표시 이름	대체할 변수 이름
MDM - Vendor Name(MDM - 벤더 이름)	ui_mdm_vendor_name

표 ***48:*** 내 디바이스 포털용 변수 목록

표시 이름	대체할 변수 이름
MyDevices - Login Failure Rate Limit(내 디바이스 - 로그인 실패 비율 제한)	$user_login_failure_rate_limit$
MyDevices - Max Devices to Register(내 디바이스 - 등록할 최대 디바이스 수)	ui_max_register_devices
MyDevices - User Name(내 디바이스 - 사용자 이름) 포털에 로그인되어 있는 사용자 이름을 지정하는 데 사용됩니다.	$session_username$

사용자 맞춤화 내용 보기

사용자 맞춤화 내용이 포털 사용자(게스트, 스폰서 또는 직원)에게 어떻게 표시되는지를 확인할 수 있습니다.

단계 **1** 변경사항을 확인하려면 **Portal test URL(**포털 테스트 **URL)**을 클릭합니다.

단계 **2** (선택 사항) 여러 디바이스에서 변경사항이 어떻게 표시되는지를 동적으로 확인하려면 **Preview(**미리보기**)**를 클릭합니다.

- 모바일 디바이스: **Preview(**미리보기**)**에서 변경사항을 확인합니다.
- 데스크톱 디바이스: **Preview(**미리보기**)**를 클릭한 다음 **Desktop Preview(**데스크톱 미리보기**)**를 클릭합니다.

  변경사항이 표시되지 않으면 **Refresh Preview(**미리보기 새로 고침**)**를 클릭합니다. 표시되는 포털에서는 변경사항만 확인할 수 있으며 버튼을 클릭하거나 데이터를 입력할 수는 없습니다.

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. PSN이 한 개보다 많은 경우 Cisco ISE는 첫 번째 활성 상태의 PSN을 선택합니다.

사용자 맞춤화 포털 파일

Custom Portal Files(맞춤형 포털 파일) 메뉴를 사용하면 ISE 서버에 사용자 고유의 파일을 업로드할 수 있습니다. 이 메뉴를 사용하여 모든 대고객 포털을 맞춤 설정할 수 있습니다(관리 포털 제외). 업로드한 파일은 PSN에 저장되고 모든 PSN에 동기화됩니다.

지원되는 파일 유형은 다음과 같습니다.

- .png, .gif, .jpg, .jpeg, ico: 배경, 공지 사항 및 광고용
- .htm, .html, .js, .json, .css, .m4a, .m4v, .mp3, .mp4, .mpeg, .ogg, .wav: 고급 맞춤화(예: 포털 빌더)

파일 크기는 다음으로 제한됩니다.

- 파일당 20MB
- 200MB(모든 파일)

파일 목록의 경로 열에는 이 서버의 파일에 대한 URL이 표시됩니다. 이 URL을 사용하면 미니 편집기 외부에서 해당 파일을 참조할 수 있습니다. 파일이 이미지인 경우 링크를 클릭하면 이미지를 표시하는 새 창이 열립니다.

업로드된 파일은 **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 아래의 미니 편집기에서 관리 포털을 제외한 모든 포털 유형에서 참조할 수 있습니다. 미니 편집기에 파일을 삽입하려면 **Insert File(**파일 삽입**)**을 클릭합니다. HTML Source(HTML 소스) 보기로 전환하면 삽입된 파일이 적절한 HTML 태그로 묶여있는 것을 확인할 수 있습니다.

또한 테스트 목적으로 ISE 외부에서 브라우저에 표시 가능한 업로드된 파일을 볼 수도 있습니다. URL은 https://*ise_ip*:8443/portal/customFiles/*filename*입니다.

고급 포털 사용자 맞춤화

Cisco ISE에서 제공하는 기본 포털 테마를 사용하지 않으려는 경우 사용자 요구 사항에 맞게 포털을 사용자 맞춤화할 수 있습니다. 이를 위해서는 CSS 및 Javascript 파일과 jQuery Mobile ThemeRoller 애플리케이션에 대한 작업 경험이 있어야 합니다.

기본 포털 테마는 변경할 수 없지만 다음 사항은 수행할 수 있습니다.

- 포털의 기본 테마 CSS 파일 내보내기, 466 페이지 그리고 맞춤화 포털 테마를 생성하기 위한 기반으로 사용할 수 있습니다.
- 사용자 맞춤화 포털 테마 CSS 파일 생성, 467 페이지 - 기본 포털 테마를 편집하고 새 파일로 저장

- 사용자 맞춤화 포털 테마 CSS 파일 가져오기, 477 페이지 - 포털에 적용

전문 지식 및 요구 사항에 따라 다양한 유형의 고급 사용자 맞춤화을 수행할 수 있습니다. 미리 정의된 변수를 사용하여 표시되는 정보의 일관성 보장, 포털 페이지에 광고 추가, HTML, CSS 및 Javascript 코드를 사용하여 콘텐츠 사용자 맞춤화, 포털 페이지 레이아웃 수정 등을 할 수 있습니다.

각 포털의 **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭에 있는 콘텐츠 상자에 HMTL, CSS 및 javascript를 추가하여 포털을 수정합니다. 이 문서에는 HTML 및 CSS를 사용한 사용자 맞춤화 예가 포함되어 있습니다. javascript를 사용하는 예는 ISE 커뮤니티 (http://cs.co/ise-community)에 있습니다. 추가 HTML, CSS 및 Javascript 예는 ISE 커뮤니티 (https://community.cisco.com/t5/security-documents/how-to-ise-web-portal-customization-options/ta-p/3619042)에 있습니다.

참고 TAC는 Cisco ISE 포털의 Javascript 사용자 맞춤화을 지원하지 않습니다. Javascript 사용자 맞춤화에 문제가 있는 경우 질문을 ISE 커뮤니티 https://community.cisco.com/t5/identity-services-engine-ise/bd-p/5301j-disc-ise에 게시하십시오.

고급 포털 사용자 맞춤화 활성화

Cisco ISE에서는 최종 사용자 포털에 표시되는 콘텐츠를 사용자 맞춤화할 수 있습니다. **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 아래에 나열된 여러 페이지의 텍스트 상자에 HTML, CSS 및 Javascript 코드를 입력할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 을 선택합니다.

단계 **2** **Enable portal customization with HTML(HTML**을 사용한 포털 사용자 맞춤화 활성화**)**이 기본적으로 선택되어 있는지 확인합니다. 이 설정을 사용하면 **Instructional Text(**지침 텍스트**)**, **Optional Content 1(**선택적 콘텐츠 **1)** 및 **Optional Content 2(**선택적 콘텐츠 **2)** 텍스트 상자에 HTML 태그를 포함할 수 있습니다.

단계 **3** **Enable Portal Customization with HTML and JavaScript(HTML** 및 **Javascript**를 사용한 포털 사용자 맞춤화 활성화**)**를 선택합니다. 포함하여 고급 JavaScript 사용자 설정을 수행하려는 경우 <script> tags in the **Instructional Text(**지침 텍스트**)**, **Optional Content 1(**선택적 콘텐츠 **1)** 및 **Optional Content 2(**선택적 콘텐츠 **2)** 필드

포털 테마 및 구조 **CSS** 파일

CSS 파일로 작업한 경험이 있는 경우 포털 표시를 변경하도록 기본 포털 테마 CSS 파일을 사용자 맞춤화하고 페이지 레이아웃, 색상 및 글꼴과 같은 요소를 조작할 수 있습니다. CSS 파일을 사용자 맞춤화하면 표시 특성을 지정할 때 유연성과 제어력을 갖출 수 있으며 여러 페이지에서 서식을 공유할 수 있고, 구조 콘텐츠의 복잡성과 반복성을 완화할 수 있습니다.

Cisco ISE 최종 사용자 포털에서는 두 가지 고유한 유형의 CSS 파일, structure.css 및 *theme*.css를 사용합니다. 모든 포털 테마에는 고유한 *theme*.css 파일이 있으며, 포털 유형별로 하나의 structure.css 파일

이 있습니다. 예를 들어 게스트 포털에는 guest.structure.css, 스폰서 포털에는 sponsor.structure.css, 내 디바이스 포털에는 mydevices.structure.css가 있습니다.

structure.css는 페이지 레이아웃 및 구조 스타일을 제공합니다. 각 페이지에 대한 요소 배치를 정의하고 jQuery Mobile 구조 스타일도 포함합니다. structure.css 파일을 볼 수는 있지만 편집할 수는 없습니다. 그러나 *theme*.css 파일 내에서 페이지 레이아웃를 변경하고 이러한 파일을 포털로 가져와 적용하면 최신 변경 사항이 structure.css 스타일보다 우선 적용됩니다.

theme.css 파일은 글꼴, 버튼 색상 및 헤더 배경과 같은 스타일을 지정합니다. *theme*.css 파일을 내보내고 테마 설정을 변경하고 가져와 포털의 사용자 맞춤화 테마로 사용할 수 있습니다. *theme*.css 파일에 적용한 페이지 레이아웃 스타일 변경 사항이 structure.css 파일에 정의된 스타일보다 우선 적용됩니다.

Cisco에서 제공하는 기본 포털 *theme*.css 파일은 변경할 수 없습니다. 그러나 파일의 설정을 편집하여 새 사용자 맞춤화 *theme*.css*theme*.css 파일로 저장할 수는 있습니다. 사용자 맞춤화 *theme*.css 파일을 추가로 편집할 수 있지만 이를 다시 Cisco ISE로 가져오는 경우에는 원래 사용한 것과 동일한 테마 이름을 사용해야 합니다. 같은 *theme*.css 파일에 대해 서로 다른 두 테마 이름을 사용할 수는 없습니다.

예를 들어 기본 *green theme.css* 파일을 사용하여 새 맞춤화 *blue theme.css* 파일을 생성하고 이름을 *Blue*로 지정한다고 가정합니다. 그런 다음 blue *theme.css* 파일을 편집할 수 있지만 다시 가져올 때 동일한 *Blue* 테마 이름을 재사용해야 합니다. Cisco ISE에서 파일 이름과 테마 이름 사이의 관계와 테마 이름의 고유성을 확인하기 때문에 이름을 *Red*로 지정할 수 없습니다. 그러나 *blue theme.css* 파일을 편집하고 *red theme.css*로 저장한 다음 새 파일을 가져오고 이름을 *Red*로 지정할 수 있습니다.

jQuery Mobile을 사용한 테마 색상 변경 정보

Cisco의 최종 사용자 포털의 색 구성표는 jQuery ThemeRoller와 호환됩니다. ThemeRoller 웹 사이트를 사용하여 전체 포털의 색상을 쉽게 편집할 수 있습니다.

ThemeRoller 색상 "견본"에는 도구 모음, 콘텐츠 블록, 버튼, 목록 항목 및 글꼴 텍스트 그림자와 같이 본 UI 요소의 색상, 질감 및 글꼴 설정을 정의하는 고유한 색 구성표가 있습니다. 색 구성표에서는 버튼의 다양한 상호 작용 상태(기본, 가리키기 및 누름)에 대한 설정도 정의합니다.

Cisco에서는 다음 3가지 견본을 사용합니다.

- 견본 A - 기본 견본입니다.
- 견본 B - **Accept(**수락**)** 버튼과 같이 강조된 요소를 정의합니다.
- 견본 C - 경고, 오류 메시지, 유효하지 않은 입력 필드 및 삭제 버튼과 같은 중요한 요소를 정의합니다.

새로 추가한 견본을 사용하는 요소에서 HTML 코드를 추가(예를 들어, 선택적 콘텐츠에)하는 경우가 아니라면 추가 견본을 적용할 수 없습니다.

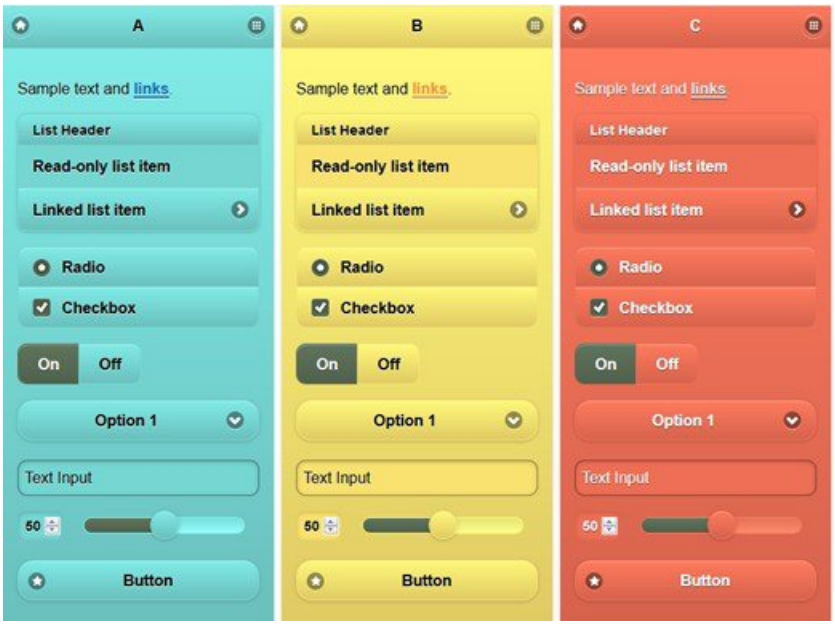
Cisco에서 제공하는 기본 CSS 파일을 편집하거나 기본 테마에 정의된 CSS 클래스 및 구조에 따라 새 파일을 생성하려면 필요한 jQuery Mobile ThemeRoller(릴리스 1.3.2) 버전을 사용해 주십시오.

jQuery Mobile ThemeRoller의 견본 및 테마에 대한 자세한 내용은 ThemeRoller를 사용하여 사용자 맞춤화 테마 생성의 "테마 설정 개요"를 참고해 주십시오. jQuery Mobile ThemeRoller의 온라인 도움말을 사용하여 사용자 맞춤화 테마를 다운로드, 가져오기 및 공유하는 방법을 알아보십시오.

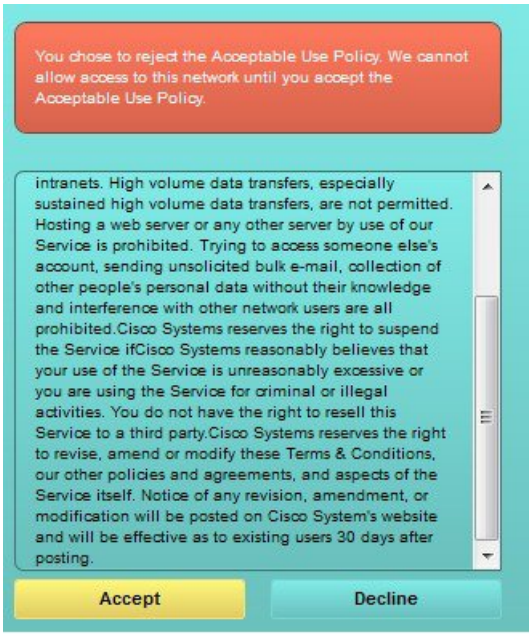
HTML, CSS 및 Javascript 코드를 사용하여 포털 페이지에 표시되는 텍스트 및 콘텐츠를 사용자 맞춤화하는 방법에 대한 튜토리얼을 보려면 Codecademy를 방문해 주십시오.

Cisco 견본을 보여주는 테마의 예

견본 사용 방법을 설명하기 위해 ThemeRoller에서 색상의 차이를 보여줄 수 있도록 게스트 포털의 기본 테마가 편집되었습니다.



다음 화면에는 게스트 포털 로그온 오류(견본 C)와 사용자의 동작을 요하는 버튼(견본 B)이 표시되어 있습니다. 화면의 나머지 부분은 견본 A입니다.



jQuery Mobile을 사용하여 테마 색상 변경

시작하기 전에

jQuery Mobile ThemeRoller의 버전 1.3.2를 사용 중인지 확인해 주십시오. 사용 중인 버전은 아래 그림에 나와 있는 것처럼 화면 왼쪽 위에 표시됩니다.

단계 **1** 포털의 **Configuration(**구성**)** 탭을 클릭하여 변경하려는 포털에서 기존 테마를 내보냅니다.

단계 **2** **Advanced Customization(**고급 사용자 맞춤화**)** > **Export/Import Themes(**테마 내보내기/가져오기**)**를 선택합니다.

단계 **3** **Custom Theming(**사용자 맞춤화 테마 설정**)** 대화 상자에서 업데이트할 테마를 내보냅니다.

단계 **4** 텍스트 편집기에서 해당 테마를 열어 모든 항목을 선택한 후에 복사합니다.

단계 **5** jQuery 웹사이트의 **Import Theme(**테마 가져오기**)** 상자에 해당 텍스트(CSS)를 붙여 넣습니다.

단계 **6** jQuery Mobil 웹 기반 애플리케이션에서 변경을 수행합니다.

단계 **7** jQuery 웹사이트에서 업데이트된 테마를 내보냅니다. 내보내기 형식은 ZIP입니다.

단계 **8** 업데이트된 테마의 압축을 풀고 themes 폴더의 업데이트된 테마를 PC에 추출합니다. 테마 이름은 jQuery 웹사이트에서 입력한 이름입니다.

단계 **9** 포털 구성 페이지의 **Custom Theming(**사용자 맞춤화 테마 설정**)** 대화 상자에서 추출된 CSS 테마 파일을 포털로 가져옵니다.

Portal Configuration(포털 구성**)** 창의 **Portal Theme(**포털 테마**)** 드롭다운을 클릭하여 이전 테마와 새 테마 간을 전환할 수 있습니다.

위치 기반 사용자 맞춤화

게스트 계정이 생성된 경우 이를 위치에 연결하고 SSID(Service Set Identifier) 속성을 지정할 수 있습니다. 게스트의 위치 및 SSID에 따라 포털 페이지에 다양한 CSS 스타일을 적용하는 데 사용할 수 있는 CSS 클래스로 위치 및 SSID를 활용할 수 있습니다.

예를 들면 다음과 같습니다.

- 게스트 위치 - 계정 위치가 *San Jose* 또는 *Boston*에 있는 게스트가 자격 증명이 있는 게스트 포털에 로그인하는 경우 모든 포털 페이지에서 **guest-location-san-jose** 또는 **guest-location-boston** 클래스 중 하나를 사용할 수 있습니다.
- 게스트 SSID - *Coffee Shop Wireless*라는 이름의 SSID의 경우 모든 포털 페이지에서 **guest-ssid-coffee-shop-wireless** CSS 클래스를 사용할 수 있습니다. 이 SSID는 게스트가 로그인할 때 연결된 SSID가 아니라 게스트 계정에 지정된 SSID입니다.

참고 이 정보는 게스트 로그인 이후의 자격 증명이 있는 게스트 포털에만 적용됩니다.

스위치 및 WLC(Wireless LAN Controller)와 같은 디바이스를 네트워크에 추가하는 경우에는 위치도 지정할 수 있습니다. 이 위치는 네트워크 디바이스의 위치에 따라 포털 페이지에 서로 다른 CSS 스타일을 적용하는 데 사용할 수 있는 CSS 클래스로도 이용 가능합니다.

예를 들어 WLC가 *Seattle*에 할당되고 게스트가 Seattle-WLC에서 Cisco ISE로 리디렉션되면 **device-location-my-locations-usa-seattle** CSS 클래스를 모든 포털 페이지에서 사용할 수 있습니다.

관련 항목

게스트 위치를 기반으로 인사말 맞춤화, 474 페이지

사용자 디바이스 유형 기반 사용자 맞춤화

Cisco ISE는 회사 네트워크 또는 최종 사용자 웹 포털(게스트, 스폰서 및 디바이스)에 액세스하는 클라이언트 디바이스 유형(게스트, 스폰서 또는 직원)을 탐지합니다. 그러한 디바이스는 모바일 디바이스(Android, iOS 등) 또는 데스크톱 디바이스(Windows, MacOS 등)로 탐지됩니다. 디바이스 유형은 사용자의 디바이스 유형을 기초로 서로 다른 CSS 스타일을 포털 페이지에 적용하는 데 사용할 수 있는 CSS 클래스로 제공됩니다.

사용자가 Cisco ISE 최종 사용자 웹 포털에 로그인하는 경우 **cisco-ise-mobile** 또는 **cisco-ise-desktop** 클래스를 포털 페이지에서 사용할 수 있습니다.

관련 항목

사용자 디바이스 유형을 기반으로 인사말 사용자 맞춤화, 475 페이지

포털의 기본 테마 CSS 파일 내보내기

Cisco에서 제공하는 기본 포털 테마를 다운로드한 다음 필요에 따라 사용자 맞춤화할 수 있습니다. 이 테마를 기준으로 하여 고급 사용자 맞춤화를 수행할 수 있습니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers**(작업 센터) > **Guest Access**(게스트 액세스) > **Portals & Components**(포털 및 구성 요소) > **Guest Portals**(게스트 포털) > **Edit**(편집) > **Portal Page Customization**(포털 페이지 사용자 맞춤화) > **Pages**(페이지)를 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers**(작업 센터) > **Guest Access**(게스트 액세스) > **Portals & Components**(포털 및 구성 요소) > **Sponsor Portals**(스폰서 포털) > **Edit**(편집) > **Portal Page Customization**(포털 페이지 사용자 맞춤화) > **Pages**(페이지)를 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration**(관리) > **Device Portal Management**(디바이스 포털 관리) > (임의의 포털) > **Edit**(편집) > **Portal Page Customization**(포털 페이지 사용자 맞춤화) > **Pages**(페이지)를 선택합니다.

단계 **2** **Advanced Customization**(고급 사용자 맞춤화) 드롭다운 목록에서 **Export/Import Themes**(테마 내보내기/가져오기)를 선택합니다.

단계 **3** 사용자 맞춤화 테마 지정 대화 상자에서 드롭다운 목록을 사용하여 사용자 맞춤화할 테마를 선택합니다.
단계 **4** **Export Theme CSS(**테마 **CSS** 내보내기**)**를 클릭하여 사용자 맞춤화할 기본 *theme.css* 파일을 다운로드합니다.
단계 **5** 파일을 데스크톱에 저장하려면 **Save(**저장**)**를 클릭합니다.

사용자 맞춤화 포털 테마 **CSS** 파일 생성

기존의 기본 포털 테마를 사용자 맞춤화한 다음 변경사항을 새 포털 *theme*.css 파일에 저장하여 사용자 맞춤화 포털 테마를 생성할 수 있습니다. 기본 테마 설정과 견본을 수정하여 선택한 포털을 전역적으로 변경할 수 있습니다.

시작하기 전에

- 사용자 맞춤화할 포털에서 *theme*.css 파일을 데스크톱에 다운로드합니다.
- 이 작업을 하려면 HTML, CSS 및 JavaScript 코드를 사용해 본 경험이 있어야 합니다.
- jQuery Mobile ThemeRoller 릴리스 1.3.2를 사용합니다.

단계 **1** 다운로드한 포털 *theme*.css 파일 콘텐츠를 jQuery Mobile ThemeRoller 도구로 가져옵니다.

팁 변경을 하면서 사용자 맞춤화 내용 보기, 478 페이지를 수행할 수 있습니다.

단계 **2** (선택 사항) 포털 콘텐츠에 링크 포함, 467 페이지
단계 **3** (선택 사항) 동적 텍스트 업데이트용 변수 삽입, 468 페이지
단계 **4** (선택 사항) 소스 코드를 사용하여 텍스트 서식 지정 및 링크 포함, 469 페이지
단계 **5** (선택 사항) 이미지를 광고로 추가, 470 페이지
단계 **6** (선택 사항) 게스트 위치를 기반으로 인사말 맞춤화, 474 페이지
단계 **7** (선택 사항) 사용자 디바이스 유형을 기반으로 인사말 사용자 맞춤화, 475 페이지
단계 **8** (선택 사항) 회전식 광고 설정, 471 페이지
단계 **9** (선택 사항) 포털 페이지 레이아웃 수정, 476 페이지
단계 **10** 사용자 맞춤화한 파일을 새 *theme*.css 파일로 저장합니다.

참고 기본 CSS 테마 파일에 대한 편집 내용은 저장할 수 없으며 적용한 편집 내용으로 새 사용자 맞춤화 파일을 생성하는 작업만 가능합니다.

단계 **11** 새 *theme*.css 파일이 준비되면 Cisco ISE로 가져올 수 있습니다.

포털 콘텐츠에 링크 포함

게스트가 포털 페이지에서 여러 웹사이트에 액세스할 수 있도록 링크를 추가할 수 있습니다. 이 방법으로 수행하는 변경사항은 사용자 맞춤화하는 특정 포털 페이지에만 적용됩니다.

필드 사용 시 **Toggle Full Screen(**전체 화면 전환**)** 옵션을 사용하여 필드의 크기를 늘리거나 줄일 수 있습니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals and Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals and Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 인증서 프로비저닝 포털의 경우메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Certificate Provisioning(**인증서 프로비저닝**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Pages(**페이지**)**에서 업데이트할 페이지를 선택합니다.

단계 **3** **Page Customizations(**페이지 사용자 맞춤화**)**에서 **Optional Content(**선택적 콘텐츠**)** 텍스트 상자에 제공된 미니 편집기를 사용해 포털 페이지에 링크를 추가합니다.

단계 **4** **Create Link(**링크 생성**)** 버튼을 클릭합니다.
Link Properties(링크 속성**)** 대화 상자가 나타납니다.

단계 **5** 하이퍼링크로 지정할 **URL** 및 텍스트를 URL의 **Description(**설명**)** 창에 입력합니다.

링크가 정상적으로 작동하도록 하려면 URL에 프로토콜 식별자를 포함합니다. 예를 들어 www.cisco.com 대신 http://www.cisco.com을 사용합니다.

단계 **6** **Set(**설정**)**을 클릭한 다음 **Save(**저장**)**를 클릭합니다.

Toggle HTML Source(HTML 소스 전환**)** 옵션을 사용하면 미니 편집기를 사용하여 서식을 지정한 텍스트에 적용된 HTML 태그를 확인할 수 있습니다.

동적 텍스트 업데이트용 변수 삽입

콘텐츠를 동적으로 업데이트하는 미리 정의된 변수($variable$)를 대체하여 포털에 표시되는 텍스트의 템플릿을 생성할 수도 있습니다. 그러면 게스트에게 표시되는 텍스트와 정보의 일관성을 유지할 수 있습니다. 이 방법으로 수행하는 변경사항은 사용자 맞춤화하는 특정 포털 페이지에만 적용됩니다.

필드 사용 시 **Toggle Full Screen(**전체 화면 전환**)** 옵션을 사용하여 필드의 크기를 늘리거나 줄일 수 있습니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals and Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals and Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Pages(**페이지**)**에서 업데이트할 페이지를 선택합니다.

단계 **3** **Page Customizations(**페이지 사용자 맞춤화**)**에서 **Instructional Text(**지침 텍스트**)**, **Optional Content 1(**선택적 콘텐츠 **1)** 및 **Optional Content 2(**선택적 콘텐츠 **2)** 필드에 제공된 미니 편집기를 사용해 포털 페이지용 텍스트 템플릿을 생성합니다.

예를 들어 여러 게스트에 대해 단일 환영 메시지 템플릿을 생성하되 게스트가 정상적으로 로그인하여 네트워크에 연결하고 나면 게스트에게 표시되는 메시지를 개인 설정할 수 있습니다.

단계 **4** 평소와 같이 필드에 정보를 입력합니다.

예를 들어 포털에 대한 환영 메시지를 입력할 수 있습니다.

```
Welcome to our company's Guest portal,
```

단계 **5** 텍스트를 변수로 대체하려는 지점에서 **Insert Variable(**변수 삽입**)**을 클릭합니다.
변수 목록이 팝업 메뉴에 나타납니다.

단계 **6** 텍스트에서 대체하려는 변수를 선택합니다.

예를 들어 환영 메시지에 각 게스트의 이름이 표시되도록 **First name(**이름**)**을 선택합니다. 커서 위치에 **ui_first_name** 변수가 삽입됩니다.

```
Welcome to our company's Guest portal,$ui_first_name$.
```

예를 들어 게스트 이름이 John일 때 포털 환영 페이지에 표시되는 환영 메시지는 다음과 같습니다. **Welcome to our company's Guest portal, John(John,** 저희 회사의 게스트 포털에 오신 것을 환영합니다**.)**

단계 **7** 필요한 대로 변수 목록을 계속 사용하여 텍스트 상자에 정보를 모두 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

Toggle HTML Source(HTML 소스 전환**)** 옵션을 사용하면 미니 편집기를 사용하여 서식을 지정한 텍스트에 적용된 HTML 태그를 확인할 수 있습니다.

소스 코드를 사용하여 텍스트 서식 지정 및 링크 포함

일반 텍스트에서 미니 편집기의 서식 및 링크 아이콘을 사용하는 방법 외에 HTML, CSS 및 Javascript 코드를 사용하여 포털 페이지에 표시되는 텍스트를 사용자 맞춤화할 수도 있습니다. 이 방법으로 수행하는 변경사항은 사용자 맞춤화하는 특정 포털 페이지에만 적용됩니다.

텍스트 상자 사용 시 **Toggle Full Screen(**전체 화면 전환**)** 옵션을 사용하여 텍스트 상자의 크기를 늘리거나 줄일 수 있습니다.

시작하기 전에

Enable portal customization with HTML(HTML을 사용한 포털 사용자 맞춤화 활성화**)**이 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Portal Customization(**포털 사용자 맞춤화**)**에서 기본적으로 활성화되어 있는지 확인합니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Pages(**페이지**)**에서 업데이트할 페이지를 선택합니다.

단계 **3** **Page Customizations(**페이지 사용자 맞춤화**)**에서 **Instructional Text(**지침 텍스트**)**, **Optional Content 1(**선택적 콘텐츠 **1)** 및 **Optional Content 2(**선택적 콘텐츠 **2)** 필드에 제공된 미니 편집기를 사용해 소스 코드를 입력하고 확인합니다.

단계 **4** **Toggle HTML Source(HTML** 소스 전환**)**를 클릭합니다.

단계 **5** 소스 코드를 입력합니다.

예를 들어 텍스트에 밑줄을 표시하려면 다음 코드를 입력합니다.

```
<p style="text-decoration:underline;">Welcome to Cisco!</p>
```

예를 들어 HTML 코드를 사용하여 링크를 포함하려면 다음 코드를 입력합니다.

```
<a href="http://www.cisco.com">Cisco</a>
```

중요 HTML 코드에 외부 URL을 삽입할 때는 "http" 또는 "https"를 포함한 절대(전체) URL 경로를 입력해야 합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

관련 항목

고급 포털 사용자 맞춤화 활성화, 462 페이지

이미지를 광고로 추가

포털 페이지의 특정 영역에 표시할 이미지와 광고를 포함할 수 있습니다.

텍스트 상자 사용 시 **Toggle Full Screen(**전체 화면 전환**)** 옵션을 사용하여 텍스트 상자의 크기를 늘리거나 줄일 수 있습니다.

시작하기 전에

Enable portal customization with HTML(HTML을 사용한 포털 사용자 맞춤화 활성화**)**이 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Portal Customization(**포털 사용자 맞춤화**)**에서 활성화되어 있는지 확인합니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Pages(**페이지**)**에서 업데이트할 페이지를 선택합니다.

단계 **3** **Page Customizations(**페이지 사용자 맞춤화**)**에서 **Instructional Text(**지침 텍스트**)**, **Optional Content 1(**선택적 콘텐츠 **1)** 및 **Optional Content 2(**선택적 콘텐츠 **2)** 필드에 제공된 미니 편집기를 사용해 소스 코드를 입력하고 확인합니다.

단계 **4** **Toggle HTML Source(HTML** 소스 전환**)**를 클릭합니다.

단계 **5** 소스 코드를 입력합니다.

예를 들어 핫스팟 게스트 포털 액세스 후 배너에 HTML 코드를 사용하여 제품 광고와 해당 이미지를 포함하려면 **Optional Content 1(**선택적 콘텐츠 **1)** 텍스트 상자에 다음 코드를 입력합니다. 이 텍스트 상자는 **Post-Access Banner(**액세스 후 배너**)** 페이지에 있습니다.

```
<p style="text-decoration:underline;">Optimized for 10/40/100 Campus Services!</p>
<img  src="http://www.static-cisco.com/assets/prod/root/catalyst_6800.jpg" width="100%" />
```

참고 HTML 코드에 외부 URL을 삽입할 때는 "http" 또는 "https"를 포함한 절대(전체) URL 경로를 입력해야 합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

회전식 광고 설정

회전식 광고는 여러 제품 이미지나 텍스트 설명이 배너 내의 반복되는 루프에서 표시되며 회전하는 광고 형식입니다. 회사에서 제공하는 여러 관련 제품 또는 다양한 제품을 홍보하려는 경우 게스트 포털에서 회전식 광고를 사용합니다.

텍스트 상자 사용 시 **Toggle Full Screen(**전체 화면 전환**)** 옵션을 사용하여 텍스트 상자의 크기를 늘리거나 줄일 수 있습니다.

시작하기 전에

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 을 선택하고 **Enable portal customization with HTML and Javascript(HTML** 및 **Javascript**를 사용한 포털 맞춤화 활성화)를 선택합니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Pages(**페이지**)**에서 업데이트할 페이지를 선택합니다.

단계 **3** **Page Customizations(**페이지 사용자 맞춤화**)**에서 **Instructional Text(**지침 텍스트**)**, **Optional Content 1(**선택적 콘텐츠 **1)** 및 **Optional Content 2(**선택적 콘텐츠 **2)** 필드에 제공된 미니 편집기를 사용해 소스 코드를 입력하고 확인합니다.

단계 **4** **Toggle HTML Source(HTML** 소스 전환**)**를 클릭합니다.

단계 **5** 소스 코드를 입력합니다.

예를 들어 게스트 포털에서 제품 이미지를 사용하여 회전식 광고를 구현하려면 핫스팟 포털의 경우 액세스 후 배너 필드에서, 자격 증명이 지정된 게스트 포털의 경우 로그인 후 배너 페이지에서 **Optional Content 1(**선택적 콘텐츠 **1)** 텍스트 상자에 다음 HTML 및 Javascript 코드를 입력합니다.

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 5000);

function changeBanner(){
var bannersArray = ["<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' width='100%'/>",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_0/
n21v1DrawerContainer.img.jpg/1400748629549.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_1/
n21v1DrawerContainer.img.jpg/1376556883237.jpg' width='100%'/>"

];
  var div = document.getElementById("image-ads");
  if(div){
     currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
      div.innerHTML = bannersArray[currentIndex];
   }
```

```
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
</style>
<div class="grey" id="image-ads">
<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/ content_parsys/overview/layout-
 overview/gd12v2/gd12v2-left/n21v1_cq/ n21v1DrawerContainer.img.jpg/1379452035953.jpg'/>
</div>
```

예를 들어 게스트 포털에서 제품 설명을 사용하여 회전식 광고를 구현하려면 핫스팟 포털의 경우 액세스 후 배너 필드에서, 자격 증명이 지정된 게스트 포털의 경우 로그인 후 배너 페이지에서 **Optional Content 1(**선택적 콘텐츠 **1)** 텍스트 상자에 다음 HTML 및 Javascript 코드를 입력합니다.

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 2000);

function changeBanner(){
var bannersArray = ["Optimize branch services on a single platform while delivering an optimal
application experience across branch and WAN infrastructure", "Transform your Network Edge to
deliver high-performance, highly secure, and reliable services to unite campus, data center,
and branch networks",  "Differentiate your service portfolio and increase revenues by delivering
end-to-end scalable solutions and subscriber-aware services"];

var colorsArray = ["grey", "blue",  "green"];
  var div = document.getElementById("text-ads");
  if(div){
     currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
      div.innerHTML = bannersArray[currentIndex];
               div.className = colorsArray[currentIndex];
   }
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
.blue{
color: black;
background-color: lightblue;
}
.green{
color: black;
background-color: lightgreen;
}
</style>
<div class="grey" id="text-ads">
Optimize branch services on a single platform while delivering an optimal application
experience across branch and WAN infrastructure
</div>
```

참고 HTML 코드에 외부 URL을 삽입할 때는 "http" 또는 "https"를 포함한 절대(전체) URL 경로를 입력해야 합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

게스트 위치를 기반으로 인사말 맞춤화

이 예에서는 게스트가 게스트 유형에 구성된 위치를 기준으로 하여 자격 증명이 있는 게스트 포털(핫스팟 아님)에 로그인하고 나면 보이는 로그인 성공 메시지를 맞춤화하는 방법을 보여줍니다.

필드 사용 시 **Toggle Full Screen(**전체 화면 전환**)** 옵션을 사용하여 필드의 크기를 늘리거나 줄일 수 있습니다.

단계 **1** 다음과 같이 포털 중 하나로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Pages(**페이지**)** 아래에서 **Authentication Success(**인증 성공**)**를 선택합니다.

단계 **3** **Page Customizations(**페이지 사용자 맞춤화**)**에서 **Optional Content 1(**선택적 콘텐츠 **1)** 필드에 제공된 미니 편집기를 사용하여 HTML 소스 코드를 입력하고 확인합니다.

단계 **4** **Toggle HTML Source(HTML** 소스 전환**)**를 클릭합니다.

단계 **5** 소스 코드를 입력합니다.

예를 들어 위치 기반 인사말을 포함하려면 **Optional Content 1(**선택적 콘텐츠 **1)**에 다음 코드를 입력합니다.

```
<style>
    .custom-greeting {
        display: none;
    }
    .guest-location-san-jose .custom-san-jose-greeting {
        display: block;
    }
    .guest-location-boston .custom-boston-greeting {
        display: block;
    }
</style>
<div class="custom-greeting custom-san-jose-greeting">
    Welcome to The Golden State!
</div>
<div class="custom-greeting custom-boston-greeting">
    Welcome to The Bay State!
</div>
```

게스트의 특정 위치에 따라 로그온 성공 후 각기 다른 메시지가 표시됩니다.

사용자 디바이스 유형을 기반으로 인사말 사용자 맞춤화

사용자의 클라이언트 디바이스 유형(모바일 또는 데스크톱)을 기반으로 하여 사용자(게스트, 스폰서 또는 직원)가 Cisco ISE 최종 사용자 웹 포털(게스트, 스폰서 및 디바이스)에 로그인하고 나면 사용자에게 전송할 인사말을 사용자 맞춤화할 수 있습니다.

필드 사용 시 **Toggle Full Screen(**전체 화면 전환**)** 옵션을 사용하여 필드의 크기를 늘리거나 줄일 수 있습니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Pages(**페이지**)**에서 업데이트할 페이지를 선택합니다.

단계 **3** **Page Customizations(**페이지 사용자 맞춤화**)**에서 **Optional Content 1(**선택적 콘텐츠 **1)** 필드에 제공된 미니 편집기를 사용하여 HTML 소스 코드를 입력하고 확인합니다.

단계 **4** **Toggle HTML Source(HTML** 소스 전환**)**를 클릭합니다.

단계 **5** 소스 코드를 입력합니다.

예를 들어 AUP 페이지에 디바이스 유형 기반 인사말을 포함하려면 AUP 창의 **Optional Content 1(**선택적 콘텐츠 **1)** 필드에 다음 코드를 입력합니다.

```
<style>
    .custom-greeting {
        display: none;
    }
    .cisco-ise-desktop .custom-desktop-greeting {
        display: block;
    }
    .cisco-ise-mobile .custom-mobile-greeting {
        display: block;
    }
</style>
<div class="custom-greeting custom-mobile-greeting">
    Try our New Dark French Roast! Perfect on the Go!
</div>
<div class="custom-greeting custom-desktop-greeting">
    We brough back our Triple Chocolate Muffin!
    Grab a seat and dig in!
</div>
```

사용자가 네트워크나 포털에 액세스하는 데 사용한 디바이스 유형에 따라 AUP 페이지에 각기 다른 인사말이 표시됩니다.

포털 페이지 레이아웃 수정

페이지의 전체 레이아웃을 조작할 수 있습니다. 예를 들어 추가 정보나 정보 링크를 제공하는 사이드바를 AUP 페이지에 추가할 수 있습니다.

단계 **1** 직접 생성하여 포털에 적용하려는 사용자 맞춤화 *theme*.css 파일의 맨 아래에 다음 CSS 코드를 추가합니다. 이렇게 하면 AUP 페이지 레이아웃이 변경됩니다. **Optional Content 1(**선택적 콘텐츠 **1)** 필드가 데스크톱 및 모바일 디바이스 모드에서 사이드바로 나타납니다.

```
#page-aup .cisco-ise-optional-content-1 {
        margin-bottom: 5px;
}
@media all and ( min-width: 60em ) {
        #page-aup .cisco-ise-optional-content-1 {
                float: left;
                margin-right: 5px;
                width: 150px;
        }
        #page-aup .cisco-ise-main-content {
                float: left;
                width: 800px;
        }
        #page-aup .cisco-ise-main-content h1,
        #page-aup .cisco-ise-main-content p {
                margin-right: auto;
                margin-left: -200px;
        }
}
```

그런 다음 해당 포털의 AUP 창에 대해 **Optional Content 1(**선택적 콘텐츠 **1)** 필드에서 HTML 코드를 사용하여 링크를 추가할 수 있습니다.

단계 **2** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portal & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **3** **Pages(**페이지**)**에서 사이드바를 포함할 페이지를 선택합니다.

단계 **4** **Page Customizations(**페이지 사용자 맞춤화**)**에서 **Optional Content 1(**선택적 콘텐츠 **1)** 필드에 제공된 미니 편집기를 사용하여 소스 코드를 입력하고 확인합니다.

단계 **5** **Toggle HTML Source(HTML** 소스 전환**)**를 클릭합니다.

단계 **6** 소스 코드를 입력합니다.

예를 들어 AUP 창에 사이드바를 포함하려면 AUP 창의 **Optional Content 1(**선택적 콘텐츠 **1)** 필드에서 다음 코드를 입력합니다.

```
<ul data-role="listview">
    <li>Rent a Car</li>
    <li>Top 10 Hotels</li>
    <li>Free Massage</li>
    <li>Zumba Classes</li>
</ul>
```

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

Optional Content(선택적 콘텐츠**)** 필드에 다른 텍스트나 HTML 코드를 입력하여 다른 페이지를 사용자 맞춤화할 수 있습니다.

사용자 맞춤화 포털 테마 **CSS** 파일 가져오기

직접 생성한 맞춤 *theme*.css 파일을 업로드하고 최종 사용자 포털에 적용할 수 있습니다. 이러한 변경 사항은 사용자 맞춤화하는 전체 포털에 적용됩니다.

사용자 맞춤화 *theme*.css 파일을 편집하여 Cisco ISE로 다시 가져올 때마다 해당 파일에 원래 사용했던 것과 같은 테마 이름을 사용해야 합니다. 같은 *theme*.css 파일에 대해 서로 다른 두 테마 이름을 사용할 수는 없습니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Configure(**구성**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Advanced Customization(**고급 사용자 맞춤화**)** 드롭다운 목록에서 **Export/Import Themes(**테마 내보내기/가져오기**)**를 선택합니다.

단계 **3** **Custom Theming(**사용자 맞춤화 테마 지정**)** 대화 상자에서 **Browse(**찾아보기**)**를 클릭하여 새 *theme*.css 파일을 찾습니다.

단계 **4** 새 파일의 **Theme Name(**테마 이름**)**을 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

사용자 맞춤화할 포털에 이 사용자 맞춤화 포털 테마를 적용할 수 있습니다.

1. **Portal Themes(**포털 테마**)** 드롭다운 목록에서 업데이트된 테마를 선택하여 전체 포털에 적용합니다.
2. **Save(**저장**)**를 클릭합니다.

사용자 맞춤화 포털 테마 삭제

Cisco ISE로 가져온 사용자 맞춤화 포털 테마가 포털 중 하나에서 사용되고 있지 않은 경우 삭제할 수 있습니다. Cisco ISE에서 제공하는 기본 테마는 삭제할 수 없습니다.

시작하기 전에

삭제하려는 포털 테마는 포털에서 사용되고 있지 않아야 합니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 선택합니다.

단계 **2** **Advanced Customization(**고급 사용자 맞춤화**)** 드롭다운 목록에서 **Delete Themes(**테마 삭제**)**를 선택합니다.

단계 **3** **Theme Name(**테마 이름**)** 드롭다운 목록에서 삭제할 포털 테마를 선택합니다.

단계 **4** **Delete(**삭제**)**, **Save(**저장**)**를 차례로 클릭합니다.

사용자 맞춤화 내용 보기

사용자 맞춤화 내용이 포털 사용자(게스트, 스폰서 또는 직원)에게 어떻게 표시되는지를 확인할 수 있습니다.

단계 **1** 변경사항을 확인하려면 **Portal test URL(**포털 테스트 **URL)**을 클릭합니다.

단계 **2** (선택 사항) 여러 디바이스에서 변경사항이 어떻게 표시되는지를 동적으로 확인하려면 **Preview(**미리보기**)**를 클릭합니다.

- 모바일 디바이스: **Preview(**미리보기**)**에서 변경사항을 확인합니다.
- 데스크톱 디바이스: **Preview(**미리보기**)**를 클릭한 다음 **Desktop Preview(**데스크톱 미리보기**)**를 클릭합니다.

변경사항이 표시되지 않으면 **Refresh Preview(**미리보기 새로 고침**)**를 클릭합니다. 표시되는 포털에서는 변경 사항만 확인할 수 있으며 버튼을 클릭하거나 데이터를 입력할 수는 없습니다.

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. PSN이 한 개보다 많은 경우 Cisco ISE는 첫 번째 활성 상태의 PSN을 선택합니다.

포털 언어 사용자 맞춤화

게스트, 스폰서, 내 디바이스 및 클라이언트 프로비저닝 포털은 지원되는 모든 언어 및 로캘로 현지화됩니다. 현지화되는 항목에는 텍스트, 레이블, 메시지, 필드 이름 및 버튼 레이블이 포함됩니다. 클라이언트 브라우저가 Cisco ISE의 템플릿으로 매핑되지 않는 로캘을 요청하는 경우 포털에서는 영어 템플릿을 사용하여 콘텐츠를 표시합니다.

관리 포털을 사용하여 각 언어에 대해 개별적으로 게스트, 스폰서 및 내 디바이스 포털에 사용되는 필드를 수정할 수 있으며 언어를 더 추가할 수 있습니다. 현재 클라이언트 프로비저닝 포털의 경우에는 이러한 필드를 사용자 맞춤화할 수 없습니다.

기본적으로 각 유형의 포털은 15개 언어를 지원합니다. **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 창에서 포털이 사용하는 언어를 선택하고 필요에 따라 해당 언어의 페이지 콘텐츠를 업데이트합니다. 참고로 한 언어의 페이지에서 글꼴과 콘텐츠를 변경할 경우 다른 언어에 변경 사항이 적용되지 않습니다. 해당 언어 파일을 내보낼 때 **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 창에서 변경한 사항이 포함됩니다.

지원되는 언어는 다음과 같습니다.

- 중국어(간체)
- 중국어 번체
- 체코어
- 네덜란드어
- 영어
- 프랑스어
- 독일어
- 헝가리어
- 이탈리아어
- 일본어
- 한국어
- 폴란드어

- 포르투갈어
- 러시아어
- 스페인어

포털에서 사용하는 언어를 편집하려면

1. 편집할 포털을 엽니 다.
2. **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭의 **view in(**표시 언어**)** 드롭다운 목록에서 편집할 언어를 선택합니다.
3. 원하는 대로 콘텐츠, 제목 및 글꼴을 변경합니다.
4. 해당 포털 구성을 저장하고 업데이트할 다른 언어에 대해 이 플로우를 반복합니다.

언어 파일을 내보내려면

각 **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 창에는 언어 파일도 제공됩니다. 언어 파일은 **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 창에서 사용자 맞춤화하는 데는 사용할 수 없지만 포털 플로우의 일부인 제목 및 텍스트를 사용자 맞춤화하는 데 사용할 수 있는 압축된 속성 파일(ZIP)입니다.

언어 파일은 특정 브라우저 로캘 설정에 대한 매핑 및 해당 언어로 된 전체 포털에 대한 모든 문자열 설정을 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.

새 언어 추가 또는 필요하지 않은 기존 언어 삭제를 비롯하여 압축 언어 파일을 내보내고 업데이트할 수 있습니다.

언어 파일을 업데이트하는 방법에 대한 지침은 다음을 참고하십시오.

- 언어 파일 내보내기, 480 페이지
- 언어 파일에서 언어 추가 또는 삭제, 481 페이지
- 업데이트된 언어 파일 가져오기, 482 페이지

언어 파일 내보내기

각 포털 유형에 대해 사용 가능한 언어 파일을 내보내 해당 파일에 지정되어 있는 기존 값을 편집하고 사용자 맞춤화할 수 있으며 언어를 추가하거나 삭제할 수 있습니다.

참고 언어 속성 파일 내 사전 키 중 일부만 값(텍스트)에서 HTML을 지원합니다.

단계 **1** 다음 포털로 이동합니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Edit(**편집**)**를 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Configure(**구성**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** 를 선택합니다.
- 디바이스 포털의 경우 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)**를 메뉴 아이콘(☰)을 클릭하고 합니다.

단계 **2** **Language File(**언어 파일**)**을 클릭하고 드롭다운 목록에서 **Export(**내보내기**)**를 선택합니다.

단계 **3** 사용자 데스크톱에 압축된 언어 파일을 저장합니다.

언어 파일에서 언어 추가 또는 삭제

포털 유형에 사용하려는 언어가 언어 파일에 없는 경우 새 언어 속성 파일을 생성한 다음 압축된 언어 파일에 추가하면 됩니다. 필요하지 않은 언어가 있는 경우에는 해당 언어 속성 파일을 삭제할 수 있습니다.

시작하기 전에

언어 속성 파일을 추가하거나 삭제하려면 각 포털 유형에서 사용 가능한 압축된 언어 파일을 내보냅니다.

단계 **1** 메모장 등의 UTF-8을 지원하는 편집기를 사용하여 언어를 추가하거나 삭제할 포털 유형에 대해 사전 정의된 언어 파일을 엽니다.

둘 이상의 포털 유형에 대해 언어를 추가하거나 삭제하려는 경우에는 해당하는 모든 포털 속성 파일을 사용합니다.

단계 **2** 새 언어를 추가하려면 압축된 언어 파일의 다른 파일과 같은 명명 규칙을 사용하여 기존 언어 속성 파일을 새 언어 속성 파일로 저장합니다. 예를 들어 새 일본어 언어 속성 파일을 생성하려면 해당 파일을 Japanese.properties(언어 이름.properties)로 저장합니다.

단계 **3** 새 언어 속성 파일의 첫 줄에서 브라우저 로컬 값을 지정하여 새 언어를 브라우저 로캘과 연결합니다. 예를 들어 Japanese.properties 파일의 첫 줄은 LocaleKeys= ja,ja-jp(LocaleKeys=브라우저 로캘 값)여야 합니다.

단계 **4** 새 언어 속성 파일에서 사전 키의 모든 값(텍스트)을 업데이트합니다.

사전 키는 변경할 수 없습니다. 해당 값만 업데이트할 수 있습니다.

참고 사전 키 중 일부만 값(텍스트)에서 HTML을 지원합니다.

다음에 수행할 작업

1. 모든 속성 파일(새 파일/기존 파일)을 압축하여 새 압축된 언어 파일을 생성합니다. 폴더나 디렉토리는 포함하지 마십시오.

참고 Mac을 사용하는 경우 ZIP 파일을 추출하면 DS 저장소가 생성됩니다. 편집 후 언어 파일을 압축할 때 ZIP에 DS 저장소를 포함해서는 안 됩니다. DS 저장소를 추출하는 방법을 알아보려면 https://superuser.com/questions/198569/compressing-folders-on-a-mac-without-the-ds-store를 참조하십시오.

2. 압축된 언어 파일에 대해 새 이름을 지정하거나 원래 이름을 사용합니다.
3. 압축된 언어 파일을 내보냈던 특정 포털로 가져옵니다.

업데이트된 언어 파일 가져오기

언어 속성 파일을 추가 또는 삭제하거나 기존 속성 파일의 텍스트를 업데이트하여 사용자 맞춤화한 편집된 언어 파일을 가져올 수 있습니다.

참고 Word 파일에서 맞춤 설정한 내용을 복사하여 붙여넣지 마십시오. 또는 **File(**파일**)** > **Save As(**다른 이름으로 저장**)**를 선택하고 Word 파일을 HTML 형식으로 저장합니다. 그런 다음 HTML 파일에서 맞춤 설정한 내용을 복사하여 붙여넣을 수 있습니다.

단계 **1** 다음 포털로 이동합니다.

- 스폰서 포털의 경우메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** 를 선택합니다.
- 디바이스 포털의 경우메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** 를 선택합니다.

단계 **2** **Language File(**언어 파일**)**을 클릭하고 드롭다운 목록에서 **Import(**가져오기**)**를 선택합니다.

단계 **3** 데스크톱을 검색하여 압축된 새 언어 파일을 찾습니다.

단계 **4** 해당 파일을 내보냈던 포털 유형용으로 파일을 다시 가져옵니다.

다음에 수행할 작업

추가한 새 언어 또는 변경된 텍스트를 표시하려면 **View In(**표시 언어**)** 드롭다운 목록에서 특정 언어를 선택합니다.

게스트 알림, 승인 및 오류 메시지 사용자 맞춤화

각 포털에서는 이메일, SMS 문자 메시지 및 인쇄를 통해 게스트가 알림을 수신하는 방법을 사용자 맞춤화할 수 있습니다. 이러한 알림을 통해 다음과 같은 경우 로그인 자격 증명을 이메일, 문자, 인쇄 형식으로 수신할 수 있습니다.

- 게스트가 셀프 등록 게스트 포털을 사용하여 정상적으로 등록하는 경우
- 스폰서가 게스트 계정을 생성한 후 게스트에게 세부정보를 제공하려는 경우. 스폰서 그룹을 생성할 때 스폰서에게 SMS 알림 사용 권한을 부여할지 여부를 결정할 수 있습니다. 이메일 및 인쇄 알림 기능을 사용할 수 있는 경우 항상 이메일 및 인쇄 알림을 사용할 수 있습니다.

또한 네트워크에 대한 액세스를 얻고자 하는 셀프 등록 게스트를 승인하도록 요청하는 스폰서에게 보내는 이메일 알림을 사용자 맞춤화할 수도 있습니다. 또한 게스트 및 스폰서에게 표시되는 기본 오류 메시지도 사용자 맞춤화할 수 있습니다.

이메일 알림 사용자 맞춤화

게스트에게 이메일을 통해 전송되는 정보를 사용자 맞춤화할 수 있습니다.

시작하기 전에

- 이메일 알림을 활성화하도록 SMTP 서버를 구성합니다. **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **SMTP Server(SMTP** 서버**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .
- 게스트에 대한 이메일 알림 지원을 구성합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Settings(**설정**)** > **Guest Email Settings(**게스트 이메일 설정**)**를 선택합니다. **Enable email notifications to guests(**게스트에 대한 이메일 알림 활성화**)**를 선택합니다.
- **Enable portal customization with HTML(HTML**을 사용한 포털 맞춤화 활성화**)**이 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Portal Customization(**포털 사용자 맞춤화**)**에서 기본적으로 활성화되어 있는지 확인합니다.

단계 **1** 셀프 등록 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Notify Guests(**게스트에게 알림**)** > **Email Notification(**이메일 알림**)**을 선택합니다.

단계 **2** **Global Page Customizations(**전역 페이지 사용자 맞춤화**)** 아래에 지정되어 있는 기본 **Logo (Email)(**로고**(**이메일**))**를 변경할 수 있습니다.

단계 **3** **Subject(**제목**)** 및 **Email body(**이메일 본문**)**를 지정합니다. 미리 정의된 변수를 사용하여 이메일 메시지에 포함할 게스트 계정 정보를 지정합니다. 미니 편집기와 HTML 태그를 사용하여 텍스트를 사용자 맞춤화합니다.

단계 **4** **Settings(**설정**)**에서 다음을 수행할 수 있습니다.

- 각기 다른 이메일로 **Send username and password separately(**사용자 이름과 비밀번호를 별도 전송**)**할 수 있습니다. 이 옵션을 선택하면 **Page Customizations(**페이지 사용자 맞춤화**)**에 **Username Email(**사용자 이름 이메일**)** 및 **Password Email(**비밀번호 이메일**)**을 사용자 맞춤화할 수 있는 두 개의 개별 탭이 표시됩니다.
- **Send Test Email(**테스트 이메일 보내기**)**을 사용하여 이메일 주소로 테스트 이메일을 보내 모든 디바이스에서 사용자 맞춤화 내용을 미리 보고 정상적으로 표시되는지 확인할 수 있습니다.

단계 **5** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

SMS 문자 메시지 알림 사용자 맞춤화

게스트에게 SMS 문자 메시지를 통해 전송되는 정보를 사용자 맞춤화할 수 있습니다.

시작하기 전에

- SMS 게이트웨이로 이메일을 전송하여 SMS 문자 메시지를 배달하는 데 사용되는 SMTP 서버를 구성합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **SMTP Server(SMTP** 서버**)**를 선택합니다.
- SMS 문자 알림을 지원하도록 스폰서 그룹을 구성합니다.
- 타사 SMS 게이트웨이를 사용하는 계정을 설정합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Systems(**시스템**)** > **Settings(**설정**)** > **SMS Gateway(SMS** 게이트웨이**)**를 선택합니다. Cisco ISE는 문자 메시지를 이메일 메시지로 게이트웨이에 전송하며, 그러면 게이트웨이는 SMS 제공자를 통해 지정된 사용자에게 메시지를 전달합니다.
- **Enable portal customization with HTML(HTML**을 사용한 포털 맞춤화 활성화**)**이 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Portal Customization(**포털 사용자 맞춤화**)**에서 기본적으로 활성화되어 있는지 확인합니다.

단계 **1** 셀프 등록 게스트 또는 스폰서 포털의 경우메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest or Sponsor Portals(**게스트 또는 스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **SMS Receipt or SMS Notification(SMS** 수신 또는 **SMS** 알림**)**을 선택합니다.

단계 **2** 미니 편집기와 HTML 태그를 사용하여 **Message Text(**메시지 텍스트**)**를 사용자 맞춤화합니다. 미리 정의된 변수를 사용하여 SMS 문자 메시지에 포함할 게스트 계정 정보를 지정합니다.

단계 **3** **Settings(**설정**)**에서 다음을 수행할 수 있습니다.

- 각기 다른 문자 메시지로 **Send username and password separately(**사용자 이름과 비밀번호를 별도 전송**)**할 수 있습니다. 이 옵션을 선택하면 **Page Customizations(**페이지 사용자 맞춤화**)**에 **Username Message(**사용자 이름 메시지**)** 및 **Password Message(**비밀번호 메시지**)**를 사용자 맞춤화할 수 있는 두 개의 개별 탭이 표시됩니다.
- **Send Test Message(**테스트 메시지 보내기**)**를 사용하여 휴대폰으로 테스트 메시지를 보내 사용자 맞춤화 내용을 미리 보고 정상적으로 표시되는지 확인할 수 있습니다. +1 ### ### ####, ###-###-####, (###) ### ####, ##########, 1########## 등의 전화번호 형식이 지원됩니다.

단계 **4** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

인쇄 알림 사용자 맞춤화

게스트에 대해 인쇄되는 정보를 사용자 맞춤화할 수 있습니다.

참고 각 포털 내에서 인쇄 알림 로고는 이메일 알림 로고 설정으로부터 상속됩니다.

시작하기 전에

Enable portal customization with HTML(HTML을 사용한 포털 사용자 맞춤화 활성화**)**이 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Portal Customization(**포털 사용자 맞춤화**)**에서 기본적으로 활성화되어 있는지 확인합니다.

단계 **1** 셀프 등록 게스트 및 스폰서 포털의 경우메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest or Sponsor Portals(**게스트 및 스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Print Receipt or Print Notification(**인쇄 수신 또는 인쇄 알림**)**을 선택합니다.

단계 **2** **Print Introduction Text(**인쇄 소개 텍스트**)**를 지정합니다. 미리 정의된 변수를 사용하여 이메일 메시지에 포함할 게스트 계정 정보를 지정합니다. 미니 편집기와 HTML 태그를 사용하여 텍스트를 사용자 맞춤화합니다.

단계 **3** 썸네일에서 사용자 맞춤화 내용을 미리 보거나 **Print Preview(**인쇄 미리보기**)**를 클릭합니다. 썸네일에서는 HTML 사용자 맞춤화 내용을 확인할 수 없습니다.
Print Preview(인쇄 미리보기**)** 옵션을 선택하는 경우 계정 세부정보를 인쇄하여 정보가 정상적으로 표시되는지를 확인할 수 있는 윈도우가 표시됩니다.

단계 **4** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

승인 요청 이메일 알림 사용자 맞춤화

셀프 등록 게스트의 계정이 생성되고 게스트가 로그인 자격 증명을 받기 전에 스폰서가 셀프 등록 게스트를 승인해야 하도록 지정할 수 있습니다. 승인을 요청하는 스폰서에게 이메일을 통해 전송되는 정보를 사용자 맞춤화할 수 있습니다. 셀프 등록 게스트 포털을 사용하는 셀프 등록 게스트가 네트워크 액세스 권한을 부여받기 전에 승인을 받아야 하도록 지정한 경우에만 이 알림이 표시됩니다.

시작하기 전에

- 이메일 알림을 활성화하도록 SMTP 서버를 구성합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Systems(**시스템**)** > **Settings(**설정**)** > **SMTP Server(SMTP** 서버**)**를 선택합니다.

- 게스트에 대한 이메일 알림 지원을 구성합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Settings(**설정**)** > **Guest Email Settings(**게스트 이메일 설정**)**를 선택합니다. **Enable email notifications to guests(**게스트에 대한 이메일 알림 활성화**)**를 선택합니다.
- 스폰서가 셀프 등록 계정 요청을 승인하도록 하려면 **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭의 **Self-Registration Page Settings(**셀프 등록 페이지 설정**)** 아래에서 **Require self-registered guests to be approved(**셀프 등록 게스트를 승인해야 함**)**를 선택합니다. 그러면 **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**의 **Notifications(**알림**)** 아래에서 **Approval Request Email(**승인 요청 이메일**)** 탭이 활성화되며, 이 탭에서 스폰서에게 전송되는 이메일을 맞춤화할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Configure(**구성**)** > **Self-Registered Guest Portals(**셀프 등록 게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Approval Request Email(**승인 요청 이메일**)**을 선택합니다. 여기서 다음을 수행할 수 있습니다.

단계 **2** 다음을 수행합니다.

a) **Global Page Customizations(**전역 페이지 사용자 맞춤화**)** 아래에 지정되어 있는 기본 **Logo(**로고**)**를 변경합니다.

b) **Subject(**제목**)** 및 **Email body(**이메일 본문**)**를 지정합니다. 미리 정의된 변수를 사용하여 이메일 메시지에 포함할 게스트 계정 정보를 지정합니다. 미니 편집기와 HTML 태그를 사용하여 텍스트를 사용자 맞춤화합니다. 예를 들어 요청 승인 이메일에서 스폰서 포털에 링크를 포함하려면 **Create a Link(**링크 생성**)**를 클릭하고 스폰서 포털에 FQDN을 추가합니다.

c) **Send Test Email(**테스트 이메일 보내기**)**을 사용하여 모든 디바이스에서 사용자 맞춤화 내용을 미리 보고 정상적으로 표시되는지 확인합니다.

d) **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

단계 **3** 스폰서가 보낸 승인 이메일의 내용을 맞춤화합니다.

a) **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)**를 선택합니다.

b) **Portal Page Customization(**포털 페이지 사용자 맞춤화**)**을 클릭합니다.

c) **Email Notification(**이메일 알림**)** 탭을 클릭하고 필요한 세부정보를 입력합니다.

오류 메시지 편집

게스트, 스폰서 및 직원에게 표시되는 오류 페이지에 나타나는 오류 메시지를 완전히 사용자 맞춤화할 수 있습니다. 오류 페이지는 차단 목록 포털을 제외한 모든 최종 사용자 웹 포털에서 제공됩니다.

단계 **1** 다음 중 하나를 수행합니다.

- 게스트 포털의 경우 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customizaiton(**포털 페이지 사용자 맞춤화**)** > **Messages(**메시지**)** > **Error Messages(**오류 메시지**)**메뉴 아이콘(☰)을 클릭하고 .

- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customizations(**포털 페이지 사용자 맞춤화**)** > **Messages(**메시지**)** > **Error Messages(**오류 메시지**)**를 선택합니다.
- 디바이스 포털의 경우 **Adminsitration(**관리**)** > **Device Portals Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customizations(**포털 페이지 사용자 맞춤화**)** > **Messages(**메시지**)** > **Error Messages(**오류 메시지**)**메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **View In(**표시 언어**)** 드롭다운 목록에서 메시지를 사용자 맞춤화하는 동안 텍스트를 표시할 언어를 선택합니다.

이 드롭다운 목록에는 특정 포털과 연결된 언어 파일의 모든 언어가 포함되어 있습니다. 포털 페이지를 사용자 맞춤화하는 동안 수행한 모든 변경사항을 지원되는 모든 언어 속성 파일에 업데이트해야 합니다.

단계 **3** 오류 메시지 텍스트를 업데이트합니다. **aup** 등의 키워드를 입력하여 AUP 관련 오류 메시지를 찾는 등 특정 오류 메시지를 검색할 수 있습니다.

단계 **4** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

포털 페이지 제목, 콘텐츠 및 레이블 문자 수 제한

제목, 텍스트 상자, 지침, 필드 및 버튼 레이블, 그리고 **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭의 다른 시각적 요소에 입력할 수 있는 최대 및 최소 문자 범위가 있습니다.

포털 페이지 제목, 콘텐츠 및 레이블에 대한 문자 수 제한

이러한 포털 페이지 UI 요소의 탐색 경로는 다음과 같습니다.

- 게스트 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**를 선택합니다.
- 스폰서 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**를 선택합니다.
- 디바이스 포털의 경우 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**를 선택합니다.

제목, 텍스트 상자, 지침, 필드 및 버튼 레이블, 그리고 사용자 맞춤화하는 포털 페이지의 다른 시각적 요소에 내용을 입력하는 경우에 이 정보를 사용합니다. 이러한 업데이트는 사용자 맞춤화하는 특정 페이지에만 적용됩니다.

참고 싱글바이트 또는 멀티바이트 문자를 입력하는 경우 필드에 지정된 최대 문자 수만 입력할 수 있습니다. 멀티바이트 문자는 문자 수 제한에 영향을 주지 않습니다.

필드 범주	필드	필드 레이블: 최소 문자 수	필드 레이블: 최대 문자 수	필드 입력 값: 최소 문자 수	필드 입력 값: 최대 문자 수
일반 페이지 요소	Banner title(배너 제목)				256
	Footer elements(바닥글 요소)			0	2000
	브라우저 페이지 제목			0	256
	Instructional Text(지침 텍스트)			0	2000
	Content Title(콘텐츠 제목)			0	256
	Optional Content 1(선택적 콘텐츠 1)			0	2000
	Optional Content 2(선택적 콘텐츠 2)			0	2000
	Button labels(버튼 레이블)	0	64		
	Check box labels(확인란 레이블)	0	64		
	Tab labels(탭 레이블)	0	64		
	Link labels(링크 레이블)	0	256		
AUP	AUP Text(AUP 텍스트)			0	50,000
메시지 텍스트	Message text(메시지 텍스트)(페이지에 표시됨)			0	2000
	Message text(메시지 텍스트)(팝업 창에 표시됨)			0	256
필드 레이블	All fields labels(모든 필드 레이블)	0	256		

필드 범주	필드	필드 레이블: 최소 문자 수	필드 레이블: 최대 문자 수	필드 입력 값: 최소 문자 수	필드 입력 값: 최대 문자 수
Field input (general)(필드 입력(일반))	Field input in general(일반적인 필드 입력)(특수한 경우는 아래 참조)			0	256
Field input (special cases)(필드 입력(특수한 경우))	Access Code(액세스 코드) 필드			1	20
	Registration Code(등록 코드) 필드			1	20
	Username(사용자 이름) 필드			1	64
	Password(비밀번호) 필드			1	256
	Phone Number(전화번호) 필드			0	64
	Device ID(디바이스 ID) 필드			12	17

포털 사용자 맞춤화

최종 사용자 웹 포털의 모양과 게스트 환경을 사용자 맞춤화할 수 있습니다. CSS(Cascading Style Sheet) 언어와 Javascript에 대한 경험이 있는 경우 jQuery Mobile ThemeRoller 애플리케이션을 사용하여 포털 페이지 레이아웃을 변경하여 포털 테마를 사용자 맞춤화할 수 있습니다.

필요한 포털 페이지에서 CSS 테마 또는 언어 속성을 내보내어 모든 필드를 확인할 수 있습니다. 자세한 내용은 포털의 기본 테마 CSS 파일 내보내기를 참고하십시오.

최종 사용자 포털 페이지 레이아웃에 대한 CSS 클래스 및 설명

다음과 같은 CSS 클래스를 사용하여 Cisco ISE 최종 사용자 웹 포털의 페이지 레이아웃을 정의 및 수정합니다.

CSS 클래스 이름	설명
cisco-ise-banner	로고, 배너 이미지 및 배너 텍스트를 포함합니다. 스폰서 및 내 디바이스 포털에서 이 클래스는 상황에 맞는 메뉴를 활성화할 수 있는 버튼도 포함합니다. 예를 들어 메뉴를 사용하면 **Log Out(**로그아웃**)**, **Change Password(**비밀번호 변경**)** 등의 옵션이 있는 팝업 창이 표시될 수 있습니다.
cisco-ise-body	배너에 포함되지 않은 모두 페이지 요소를 포함합니다.
cisco-ise-optional-content-1	기본적으로 비어 있습니다. 텍스트, 링크 및 HTML 및 Javascript 코드를 추가할 수 있습니다.
cisco-ise-main-content	지침 텍스트, 작업 버튼 및 cisco-ise-footer 컨테이너와 같은 포털 페이지의 기본 콘텐츠를 포함합니다.
cisco-ise-optional-content-2	기본적으로 비어 있습니다. 텍스트, 링크 및 HTML 및 Javascript 코드를 추가할 수 있습니다.
cisco-ise-footer	바닥글의 일부로, **Contact Support(**고객 지원**)** 및 온라인 **Help(**도움말**)**와 같은 링크 자리 표시자입니다.
cisco-ise-footer-text	기본적으로 비어 있습니다. 저작권 표시 또는 고지 사항 등 포털 페이지 아래쪽에 표시할 내용에 대한 자리 표시자입니다.

포털 언어 파일을 위한 HTML 지원

각 포털에 대한 압축된 언어 파일에는 해당 포털의 기본 언어 속성 파일이 들어 있습니다. 각 속성 파일에는 포털에 표시되는 콘텐츠를 정의하는 사전 키가 있습니다.

Instructional Text(지침 텍스트**)**, **Content(**콘텐츠**)**, **Optional Content 1(**선택적 콘텐츠 **1)** 및 **Optional Content 2(**선택적 콘텐츠 **2)** 필드의 콘텐츠를 비롯하여 포털에 표시되는 텍스트를 사용자 맞춤화할 수 있습니다. 이러한 일부 필드에는 기본 콘텐츠가 있지만 비어 있는 필드도 있습니다.

이러한 필드와 연결된 사전 키 중 일부만 그 값(텍스트)에서 HTML을 지원합니다.

차단 목록 포털 언어 파일을 위한 HTML 지원

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Blocked List Portal(**차단 목록 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포

털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**입니다. 미니 편집기에서 **View HTML Source(HTML** 소스 보기**)** 아이콘을 사용하여 콘텐츠에 HTML 코드를 추가할 수 있습니다.

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

참고 이 목록은 파일 내 사전 키의 전체 목록이 아닙니다.

- key.blacklist.ui_reject_message

BYOD(Bring Your Own Device) 포털 언어 파일을 위한 HTML 지원

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

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

참고 이 목록은 파일 내 사전 키의 전체 목록이 아닙니다.

- key.guest.ui_contact_instruction_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_byod_reg_limit_message
- key.guest.ui_byod_reg_content_message
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_byod_welcome_aup_text
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1

- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_error_instruction_message

인증서 프로비저닝 포털 언어 파일을 위한 **HTML** 지원

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

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

참고 이 목록은 파일 내 사전 키의 전체 목록이 아닙니다.

- key.manualcertprov.ui_login_instruction_message
- key.manualcertprov.ui_aup_instruction_message
- key.manualcertprov.ui_changepwd_instruction_message
- key.manualcertprov.ui_post_access_instruction_message
- key.manualcertprov.ui_status_csv_invalid_instruction_message
- key.manualcertprov.ui_login_optional_content_1
- key.manualcertprov.ui_login_optional_content_2
- key.manualcertprov.ui_aup_optional_content_1

- key.manualcertprov.ui_aup_optional_content_2
- key.manualcertprov.ui_changepwd_optional_content_1
- key.manualcertprov.ui_changepwd_optional_content_2
- key.manualcertprov.ui_post_access_optional_content_1
- key.manualcertprov.ui_post_access_optional_content_2
- key.manualcertprov.ui_landing_instruction_message
- key.manualcertprov.ui_status_page_single_generated_content
- key.manualcertprov.ui_status_generated_content

클라이언트 프로비저닝 포털 언어 파일을 위한 **HTML** 지원

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

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

참고 이 목록은 파일 내 사전 키의 전체 목록이 아닙니다.

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

- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_client_provision_posture_agent_scan_message

자격 증명 게스트 포털 언어 파일을 위한 **HTML** 지원

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**입니다. 미니 편집기에서 **View HTML Source(HTML** 소스 보기**)** 아이콘을 사용하여 콘텐츠에 HTML 코드를 추가할 수 있습니다.

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

참고 이 목록은 파일 내 사전 키의 전체 목록이 아닙니다.

- key.guest.ui_contact_instruction_message
- key.guest.ui_login_optional_content_1
- key.guest.ui_login_optional_content_2
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_device_reg_optional_content_2
- key.guest.ui_device_reg_optional_content_1
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_reg_optional_content_2

- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_max_devices_instruction_message
- key.guest.ui_max_devices_optional_content_1
- key.guest.ui_self_reg_results_instruction_message
- key.guest.notification_credentials_email_body
- key.guest.ui_max_devices_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_changepwd_instruction_message
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_aup_instruction_message
- key.guest.ui_changepwd_optional_content_2
- key.guest.ui_changepwd_optional_content_1
- key.guest.ui_self_reg_results_optional_content_2
- key.guest.ui_self_reg_results_optional_content_1
- key.guest.ui_device_reg_instruction_message
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_vlan_execute_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_client_provision_posture_check_non_compliant_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_device_reg_max_reached_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2

- key.guest.ui_aup_employee_text
- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_success_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_self_reg_optional_content_2
- key.guest.ui_self_reg_optional_content_1
- key.guest.ui_byod_reg_limit_message
- key.guest.notification_credentials_print_body
- key.guest.ui_byod_reg_content_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_aup_guest_text
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_self_reg_aup_text
- key.guest.ui_login_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_self_reg_results_aup_text
- key.guest.ui_device_reg_register_message
- key.guest.ui_byod_welcome_instruction_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_self_reg_instruction_message

- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_client_provision_posture_agent_scan_message

핫스팟 게스트 포털 언어 파일에 대한 **HTML** 지원

이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**입니다. 미니 편집기에서 **View HTML Source(HTML** 소스 보기**)** 아이콘을 사용하여 콘텐츠에 HTML 코드를 추가할 수 있습니다.

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

참고 이 목록은 파일 내 사전 키의 전체 목록이 아닙니다.

- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_success_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_vlan_unsupported_error_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_aup_instruction_message

- key.guest.ui_aup_hotspot_text
- key.guest.ui_vlan_execute_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1

모바일 디바이스 관리 포털 언어 파일에 대한 **HTML** 지원

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

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

- key.mdm.ui_contact_instruction_message
- key.mdm.ui_mdm_enrollment_after_message
- key.mdm.ui_error_optional_content_2
- key.mdm.ui_error_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_1
- key.mdm.ui_mdm_enroll_optional_content_2
- key.mdm.ui_mdm_enroll_instruction_message
- key.mdm.ui_error_instruction_message
- key.mdm.ui_mdm_enrollment_link_message
- key.mdm.ui_mdm_not_reachable_message
- key.mdm.ui_contact_optional_content_2
- key.mdm.ui_mdm_continue_message
- key.mdm.ui_contact_optional_content_1

내 디바이스 포털 언어 파일에 대한 **HTML** 지원

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

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

참고 이 목록은 파일 내 사전 키의 전체 목록이 아닙니다.

- key.mydevices.ui_add_optional_content_1
- key.mydevices.ui_add_optional_content_2
- key.mydevices.ui_post_access_instruction_message
- key.mydevices.ui_edit_instruction_message
- key.mydevices.ui_contact_optional_content_2
- key.mydevices.ui_contact_optional_content_1
- key.mydevices.ui_changepwd_optional_content_1
- key.mydevices.ui_changepwd_optional_content_2
- key.mydevices.ui_post_access_message
- key.mydevices.ui_home_instruction_message
- key.mydevices.ui_edit_optional_content_1
- key.mydevices.ui_edit_optional_content_2
- key.mydevices.ui_add_instruction_message
- key.mydevices.ui_post_access_optional_content_2
- key.mydevices.ui_post_access_optional_content_1
- key.mydevices.ui_error_instruction_message
- key.mydevices.ui_actions_instruction_message
- key.mydevices.ui_home_optional_content_2
- key.mydevices.ui_aup_optional_content_1
- key.mydevices.ui_aup_optional_content_2
- key.mydevices.ui_home_optional_content_1
- key.mydevices.ui_changepwd_instruction_message

- key.mydevices.ui_contact_instruction_message
- key.mydevices.ui_aup_employee_text
- key.mydevices.ui_login_optional_content_2
- key.mydevices.ui_login_optional_content_1
- key.mydevices.ui_login_instruction_message
- key.mydevices.ui_error_optional_content_1
- key.mydevices.ui_error_optional_content_2
- key.mydevices.ui_aup_instruction_message

스폰서 포털 언어 파일에 대한 **HTML** 지원

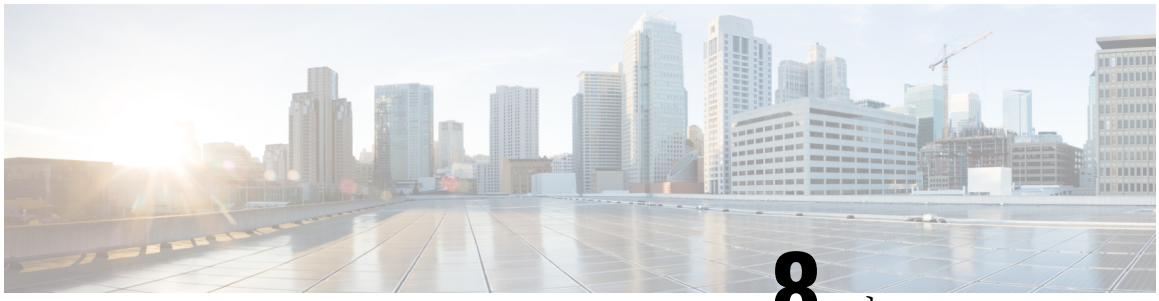
이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals & Components(**포털 및 구성 요소**)** > **Sponsor Portals(**스폰서 포털**)** > **Edit(**편집**)** > **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** > **Pages(**페이지**)**입니다. 미니 편집기에서 **View HTML Source(HTML** 소스 보기**)** 아이콘을 사용하여 콘텐츠에 HTML 코드를 추가할 수 있습니다.

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

참고 이 목록은 파일 내 사전 키의 전체 목록이 아닙니다.

- key.sponsor.ui_aup_instruction_message
- key.sponsor.ui_create_random_instruction_message
- key.sponsor.ui_home_instruction_message
- key.sponsor.ui_post_access_instruction_message
- key.sponsor.notification_credentials_print_body
- key.sponsor.ui_aup_sponsor_text
- key.sponsor.ui_create_accounts_access_info_instruction_message
- key.sponsor.ui_login_instruction_message
- key.sponsor.notification_credentials_email_body
- key.sponsor.ui_create_known_instruction_message
- key.sponsor.ui_create_import_instruction_message
- key.sponsor.ui_suspend_account_instruction_message
- key.sponsor.ui_post_access_message

- key.sponsor.ui_login_optional_content_2
- key.sponsor.ui_login_optional_content_1
- key.sponsor.notification_credentials_email_password_body
- key.sponsor.ui_contact_optional_content_2
- key.sponsor.ui_contact_optional_content_1
- key.sponsor.ui_login_aup_text
- key.sponsor.ui_changepwd_instruction_message
- key.sponsor.ui_create_accounts_guest_type_instruction_message
- key.sponsor.ui_changepwd_optional_content_1
- key.sponsor.ui_changepwd_optional_content_2
- key.sponsor.notification_credentials_email_username_body
- key.sponsor.ui_aup_optional_content_1
- key.sponsor.ui_aup_optional_content_2
- key.sponsor.ui_post_access_optional_content_1
- key.sponsor.ui_post_access_optional_content_2
- key.sponsor.ui_contact_instruction_message



8 장

자산 가시성

외부 ID 저장소를 사용하는 Cisco ISE에 대한 관리 액세스

Cisco ISE에서 Active Directory, LDAP 또는 RSA SecureID와 같은 외부 ID 저장소를 통해 관리자를 인증할 수 있습니다. 외부 ID 저장소를 통해 인증을 제공하는 데 사용할 수 있는 두 가지 모델이 있습니다.

- 외부 인증 및 권한 부여: 관리자를 위해 로컬 Cisco ISE 데이터베이스에 지정된 자격 증명이 없으며, 권한 부여는 외부 ID 저장소 그룹 멤버십만을 기반으로 합니다. 이 모델은 Active Directory 및 LDAP 인증에 사용됩니다.
- 외부 인증 및 내부 권한 부여: 관리자의 인증 자격 증명은 외부 ID 소스에서 가져오며, 권한 부여 및 관리자 역할 할당은 로컬 Cisco ISE 데이터베이스를 사용하여 발생합니다. 이 모델은 RSA SecurID 인증에 사용됩니다. 이 방법을 사용하려는 경우 외부 ID 저장 및 현지 Cisco ISE 데이터베이스에서 모두 동일한 사용자 이름을 구성해야 합니다.

Cisco ISE는 인증 프로세스 중에 외부 ID 저장소와의 통신이 설정되지 않았거나 통신이 실패할 경우 "대체"되어 내부 ID 데이터베이스에서 인증하려고 시도하도록 설계되었습니다. 또한 외부 인증을 설정한 관리자가 브라우저를 실행하고 로그인 세션을 시작하는 경우에도 여전히 관리자는 로그인 대화 상자의 **Identity Store(ID** 저장소**)** 드롭다운 목록에서 **Internal(**내부**)**을 선택하여 Cisco ISE 로컬 데이터베이스를 통해 인증을 요청할 수 있습니다.

슈퍼 관리자 그룹에 속하고 외부 ID 저장소를 사용하여 인증하고 권한을 부여하도록 구성된 관리자는 외부 ID 저장소로 인증하여 CLI(command-line interface) 액세스할 수도 있습니다.

참고 관리자 포털을 통해서만 외부 관리자 인증을 제공하는 이 방법을 구성할 수 있습니다. Cisco ISE CLI는 이러한 기능을 제공하지 않습니다.

네트워크에 하나 이상의 기존 외부 ID 저장소가 없는 경우 필요한 외부 ID 저장소를 설치하고 그러한 ID 저장소에 액세스하도록 Cisco ISE를 구성했는지 확인합니다.

외부 인증 및 권한 부여

기본적으로 Cisco ISE는 내부 관리자 인증을 제공합니다. 외부 인증을 설정하려면 외부 ID 저장소에 정의하는 외부 관리자 계정에 대한 비밀번호 정책을 생성해야 합니다. 그런 다음 이 정책을 외부 관리자 그룹에 적용할 수 있습니다. 그 결과 해당 정책은 외부 관리자 RBAC 정책에 포함됩니다.

외부 인증을 구성하려면 다음을 수행해야 합니다.

- 외부 ID 저장소를 사용하여 비밀번호 기반 인증을 구성합니다.
- 외부 관리자 그룹을 생성합니다.
- 메뉴 액세스 및 외부 관리자 그룹에 대한 데이터 액세스 권한을 구성합니다.
- 외부 관리자 인증을 위한 RBAC 정책을 생성합니다.

외부 ID 저장소를 통해 인증을 제공하는 것 외에 네트워크에서 CAC(Common Access Card) 인증 디바이스를 사용해야 할 수도 있습니다.

외부 **ID** 저장소를 사용하여 비밀번호 기반 인증 구성

Active Directory 또는 LDAP 등의 외부 ID 저장소를 사용하여 인증하는 관리자에 대해 먼저 비밀번호 기반 인증을 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)**을 선택합니다.

단계 **2** **Authentication Method(**인증 방법**)** 탭에서 **Password Based(**비밀번호 기반**)**를 클릭하고 이미 구성한 외부 ID 소스 중 하나를 선택합니다. 예를 들어 직접 생성한 Active Directory 인스턴스를 선택할 수 있습니다.

단계 **3** 외부 ID 저장소를 사용하여 인증하는 관리자에 대해 적용하려는 기타 특정 비밀번호 기반 정책 설정을 구성합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

외부 관리자 그룹 생성

외부 Active Directory 또는 LDAP 관리자 그룹을 생성해야 합니다. 그러면 Cisco ISE가 외부 Active Directory 또는 LDAP ID 저장소에 정의되어 있는 사용자 이름을 사용하여 로그인 시 사용자가 입력하는 관리자 사용자 이름 및 비밀번호를 검증합니다.

Cisco ISE는 외부 리소스에서 Active Directory 또는 LDAP 그룹 정보를 가져온 다음 사전 속성으로 저장합니다. 이러한 외부 관리자 인증 방법에 대해 RBAC 정책을 구성하는 동안 정책 구성 요소 중 하나로 해당 속성을 지정할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Groups(**관리자 그룹**)**를 선택합니다.

External Groups Mapped(외부 그룹 매핑됨**)** 열에 내부 RBAC 역할에 매핑된 외부 그룹 수가 표시됩니다. 관리자 역할에 해당하는 번호를 클릭하여 외부 그룹을 볼 수 있습니다. 예를 들어 Super Admin(슈퍼 관리자)에 대해 2를 클릭하면 두 개의 외부 그룹 이름이 표시됩니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 이름과 설명(선택 사항)을 입력합니다.

단계 **4** **External(**외부**)**을 클릭합니다.

Active Directory 도메인에 연결하고 조인한 경우에는 Active Directory 인스턴스 이름이 **Name(**이름**)** 필드에 표시됩니다.

단계 **5** **External Groups(**외부 그룹**)** 드롭다운 목록 상자에서 이 외부 관리자 그룹에 매핑할 Active Directory 그룹을 선택합니다.

"+" 기호를 클릭하여 추가 Active Directory 그룹을 이 외부 관리자 그룹에 매핑합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

내부 읽기 전용 관리자 생성

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Users(**관리 사용자**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Add(**추가**)**를 클릭하고 **Create An Admin User(**관리 사용자 생성**)**를 선택합니다.

단계 **3** 읽기 전용 관리자를 생성하려면 **Read Only(**읽기 전용**)** 확인란을 선택합니다.

읽기 전용 관리자 그룹에 외부 그룹 매핑

단계 **1** 외부 인증 소스를 구성하려면 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 필요한 외부 ID 소스(예: Active Directory 또는 LDAP)를 클릭한 다음 선택한 ID 소스에서 그룹을 검색합니다.

단계 **3** 관리자 액세스의 인증 방법을 ID 소스와 매핑하려면 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)**을 선택합니다.

단계 **4** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Groups(**관리자 그룹**)**를 선택한 다음 **Read Only Admin(**읽기 전용 관리자**)** 그룹을 선택합니다.

단계 **5** **External(**외부**)** 확인란을 선택하고 읽기 전용 권한을 제공해야 할 외부 그룹을 선택합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

읽기 전용 관리자 그룹에 매핑된 외부 그룹은 다른 관리자 그룹에 할당할 수 없습니다.

외부 관리자 그룹에 대한 메뉴 액세스 및 데이터 액세스 권한 구성

외부 관리자 그룹에 할당할 수 있는 메뉴 액세스 및 데이터 액세스 권한을 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 를 선택합니다.

단계 **2** 다음 중 하나를 클릭합니다.

- **Menu Access(**메뉴 액세스**)**: 외부 관리자 그룹에 속하는 모든 관리자에게 메뉴 또는 하위 메뉴 레벨에서 권한을 부여할 수 있습니다. 메뉴 액세스 권한에 따라 관리자가 액세스할 수 있는 메뉴 또는 하위 메뉴가 결정됩니다.
- **Data Access(**데이터 액세스**)**: 외부 관리자 그룹에 속하는 모든 관리자에게 데이터 레벨에서 권한을 부여할 수 있습니다. 데이터 액세스 권한에 따라 관리자가 액세스할 수 있는 데이터가 결정됩니다.

단계 **3** 외부 관리자 그룹에 대한 메뉴 액세스 또는 데이터 액세스 권한을 지정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

외부 관리자 인증을 위한 **RBAC** 정책 생성

외부 ID 저장소를 사용하여 관리자를 인증하는 동시에 사용자 맞춤화 메뉴 및 데이터 액세스 권한을 지정하려면 새 RBAC 정책을 구성해야 합니다. 이 정책은 외부 인증 및 권한 부여를 관리하기 위한 Cisco ISE 메뉴 및 데이터 액세스 권한과 인증용 외부 관리자 그룹을 포함해야 합니다.

참고 기존의 시스템 사전 설정 RBAC 정책을 수정하여 이러한 새 외부 속성을 지정할 수는 없습니다. 템플릿으로 사용하려는 기존 정책이 있는 경우에는 해당 정책을 복제하고 이름을 바꾼 후에 새 속성을 할당해야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authorization(**권한 부여**)** > **RBAC Policy(RBAC** 정책**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 규칙 이름, 외부 관리자 그룹 및 권한을 지정합니다.

적절한 외부 관리자 그룹을 올바른 관리자 사용자 ID에 할당해야 합니다. 관리자가 올바른 외부 관리자 그룹에 연결되어 있는지 확인합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

관리자로 로그인하는 경우 Cisco ISE RBAC 정책이 관리자 ID를 인증할 수 없으면 Cisco ISE에 "인증되지 않음" 메시지가 표시되며 관리 포털에 액세스할 수 없습니다.

내부 권한 부여를 사용하는 인증을 위해 외부 **ID** 저장소를 사용하여 관리자 액세스 구성

이 방법을 사용하려는 경우 외부 ID 저장 및 현지 Cisco ISE 데이터베이스에서 모두 동일한 사용자 이름을 구성해야 합니다. Cisco ISE가 외부 RSA SecurID ID 저장소를 사용하여 관리자 인증을 제공하도록 구성하면 RSA ID 저장소에 의해 관리자 자격 증명 인증이 수행됩니다. 그러나 권한 부여(정책 적용)는 계속해서 Cisco ISE 내부 데이터베이스에 따라 수행됩니다. 또한 외부 인증 및 권한 부여와는 다른 두 가지 중요한 요소가 있습니다.

- 관리자에 대해 특정 외부 관리자 그룹을 지정하지 않아도 됩니다.
- 외부 ID 저장소와 로컬 Cisco ISE 데이터베이스 둘 다에서 같은 사용자 이름을 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Users(**관리 사용자**)**를 선택합니다.

단계 **2** 외부 RSA ID 저장소의 관리 사용자 이름이 Cisco ISE에도 있는지 확인합니다. Password(비밀번호) 아래에서 **External(**외부**)** 옵션을 클릭해야 합니다.

참고 이 외부 관리자 사용자 ID에 대해서는 비밀번호를 지정할 필요가 없으며 구체적으로 구성된 외부 관리자 그룹을 연결된 RBAC 정책에 적용할 필요도 없습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

외부 인증 프로세스 플로우

관리자가 로그인하면 로그인 세션은 프로세스의 다음 단계를 거칩니다.

1. 관리자는 RSA SecurID 시도를 보냅니다.
2. RSA SecurID가 시도 응답을 반환합니다.
3. 관리자가 사용자 ID와 비밀번호를 입력하는 것처럼 Cisco ISE 로그인 대화 상자에 사용자 이름 및 RSA SecurID 시도 응답을 입력합니다.
4. 관리자가 지정된 ID 저장소가 외부 RSA SecurID 리소스인지 확인합니다.
5. 관리자가 **Login(**로그인**)**을 클릭합니다.

로그인되면 관리자에게는 메뉴 및 RBAC 정책에 지정된 데이터 액세스 항목만 표시됩니다.

외부 **ID** 소스

이러한 창에서는 Cisco ISE가 인증 및 권한 부여에 사용하는 사용자 데이터가 포함되어 있는 외부 ID 소스를 구성하고 관리할 수 있습니다.

LDAP ID 소스 설정

다음 표에서는 LDAP 인스턴스를 생성하고 해당 인스턴스에 연결하는 데 사용할 수 있는 LDAP ID 소스 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**입니다.

LDAP 일반 설정

다음 표에서는 **General(**일반**)** 탭의 필드에 대해 설명합니다.

표 ***49: LDAP*** 일반 설정

필드 이름	사용 지침
Name(이름**)**	LDAP 인스턴스 이름을 입력합니다. 이 값은 검색에서 주체 DN 및 속성을 가져오는 데 사용됩니다. 값은 문자열 유형이며 최대 길이는 64자입니다.
Description(설명**)**	LDAP 인스턴스에 대한 설명을 입력합니다. 이 값은 문자열 유형이며 최대 길이는 1,024자입니다.

필드 이름	사용 지침
Schema(스키마**)**	다음과 같은 내장 스키마 유형 중 하나를 선택하거나 사용자 맞춤화 스키마를 생성할 수 있습니다. • Active Directory • Sun Directory 서버 • Novell eDirectory Schema(스키마) 옆의 화살표를 클릭하여 스키마 세부정보를 확인할 수 있습니다. 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다.
참고 다음 필드는 사용자 맞춤화 스키마를 선택할 때만 편집할 수 있습니다.	
Subject Objectclass	검색에서 주체 DN 및 속성을 가져오기 위해 사용할 값을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.
Subject Name Attribute(주체 이름 속성**)**	요청의 사용자 이름이 포함된 속성의 이름을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.
Group Name Attribute(그룹 이름 속성**)**	• CN: 공용 이름을 기준으로 LDAP ID 저장소 그룹을 검색하려는 경우 입력합니다. • DN: 고유 이름을 기준으로 LDAP ID 저장소 그룹을 검색하려는 경우 입력합니다.
Certificate Attribute(인증서 속성**)**	인증서 정의를 포함하는 속성을 입력합니다. 인증서 기반 인증의 경우 이러한 정의는 클라이언트가 제공하는 인증서를 검증하는 데 사용됩니다.
Group Objectclass	검색에서 그룹으로 인식되는 객체를 지정하기 위해 사용할 값을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.
Group Map Attribute(그룹 맵 속성**)**	매핑된 정보를 포함하는 속성을 지정합니다. 이 속성은 선택한 참조 방향에 따라 사용자 또는 그룹 속성일 수 있습니다.
Subject Objects Contain Reference To Groups(주체 객체가 그룹에 대한 참조를 포함함**)**	주체 객체가 속한 그룹을 지정하는 속성이 주체 객체에 포함되어 있으면 이 옵션을 클릭합니다.

필드 이름	사용 지침
Group Objects Contain Reference To Subjects(그룹 객체가 주체에 대한 참조를 포함함**)**	그룹 객체가 주체를 지정하는 속성을 포함하고 있으면 이 옵션을 클릭합니다. 이 값이 기본값입니다.
Subjects in Groups Are Stored in Member Attribute As(그룹의 주체가 멤버 속성에 다른 이름으로 저장됨**)**	(**Group Objects Contain Reference To Subjects(**그룹 객체가 주체에 대한 참조를 포함함**)** 옵션을 활성화하는 경우에만 사용 가능함) 그룹 멤버 속성에서 멤버가 제공되는 방법을 지정하며, 기본값은 DN입니다.
User Info Attributes(사용자 정보 속성**)**	기본적으로, 사전 정의된 속성은 다음과 같은 내장 스키마 유형에 대한 사용자 정보(예: 이름, 성, 이메일, 전화 번호, 소재지 등)를 수집하는 데 사용됩니다. • Active Directory • Sun Directory 서버 • Novell eDirectory 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다. 스키마 드롭다운 목록에서 Custom(사용자 맞춤화) 옵션을 선택하여 요건에 따라 사용자 정보 속성을 편집할 수도 있습니다.

LDAP 연결 설정

다음 표에서는 **Connection Settings(**연결 설정**)** 탭의 필드에 대해 설명합니다.

표 ***50: LDAP*** 연결 설정

필드 이름	사용 지침
Enable Secondary Server(보조 서버 활성화**)**	기본 LDAP 서버에서 장애가 발생하는 경우 백업으로 사용할 보조 LDAP 서버를 활성화하려면 이 옵션을 선택합니다. 이 확인란을 선택하는 경우 보조 LDAP 서버에 대한 컨피그레이션 매개변수를 입력해야 합니다.
Primary and Secondary Servers(기본 서버 및 보조 서버**)**	

필드 이름	사용 지침
Hostname/IP(호스트 이름**/IP)**	LDAP 소프트웨어를 실행 중인 머신의 IP 주소 또는 DNS 이름을 입력합니다. 호스트 이름은 1~256자로 입력하거나 문자열로 표시되는 유효한 IP 주소를 포함할 수 있습니다. 호스트 이름에 사용할 수 있는 문자는 영숫자 문자(a~z, A~Z, 0~9)와 점(.), 하이픈(-)입니다.
Port(포트**)**	LDAP 서버가 수신 대기 중인 TCP/IP 포트 번호를 입력합니다. 유효한 값은 1~65,535입니다. 기본값은 LDAP 사양에 나와 있는 389입니다. 포트 번호를 모르는 경우 LDAP 서버 관리자에서 이 정보를 찾을 수 있습니다.
Specify server for each ISE node(각 **ISE** 노드에 대한 서버 지정**)**	각 PSN에 대해 기본 및 보조 LDAP 서버 호스트 이름/IP 및 해당 포트를 구성하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 구축의 모든 노드를 나열하는 표가 표시됩니다. 노드를 선택하고 선택한 노드에 대한 기본 및 보조 LDAP 서버 호스트 이름/IP 및 해당 포트를 구성해야 합니다.
Access(액세스**)**	**Anonymous Access(**익명 액세스**)**: LDAP 디렉토리의 검색이 익명으로 수행되도록 하려면 클릭합니다. 이 경우 서버는 클라이언트를 구분하지 않으며, 인증되지 않은 클라이언트가 액세스할 수 있도록 구성된 모든 데이터에 대한 읽기 권한을 클라이언트에 허용합니다. 서버로 인증 정보를 전송하도록 허용하는 특정 정책이 없는 경우 클라이언트는 익명 연결을 사용해야 합니다. **Authenticated Access(**인증된 액세스**)**: LDAP 디렉토리의 검색이 관리 자격 증명을 사용하여 수행되도록 하려면 클릭합니다. 이 설정을 클릭하는 경우 Admin DN(관리자 DN) 및 Password(비밀번호) 필드에 정보를 입력합니다.
Admin DN(관리자 **DN)**	관리자의 DN을 입력합니다. 관리자 DN은 사용자 디렉토리 서브트리에서 필요한 모든 사용자 및 그룹을 검색할 권한이 있는 LDAP 계정입니다. 지정된 관리자에게 검색에서 그룹 이름 속성을 확인할 권한이 없으면 해당 LDAP 서버에 의해 인증된 사용자에 대한 그룹 매핑이 실패합니다.
Password(비밀번호**)**	LDAP 관리자 계정 비밀번호를 입력합니다.

필드 이름	사용 지침
Secure Authentication(보안 인증**)**	SSL을 사용하여 Cisco ISE와 기본 LDAP 서버 간의 통신을 암호화하려면 클릭합니다. Port(포트) 필드에 LDAP 서버의 SSL에 사용되는 포트 번호가 포함되어 있는지 확인합니다. 이 옵션을 활성화하는 경우 루트 CA를 선택해야 합니다.
LDAP Server Root CA(LDAP 서버 루트 **CA)**	인증서를 사용한 보안 인증을 활성화하려면 드롭다운 목록에서 신뢰할 수 있는 루트 인증 기관을 선택합니다.
Server Timeout(서버 시간 초과**)**	기본 LDAP 서버와의 연결이나 인증이 실패했다고 결정할 때까지 Cisco ISE가 해당 서버로부터의 응답을 대기할 시간을 초 단위로 입력합니다. 유효한 값은 1~99입니다. 기본값은 10입니다.
Max. Admin Connections(최대 관리자 연결 수**)**	특정 LDAP 컨피그레이션에 대해 실행할 수 있는 LDAP 관리자 계정 권한이 있는 최대 동시 연결 수(0보다 큼)를 입력합니다. 이러한 연결은 디렉토리 검색 시 사용자 디렉토리 서브트리 및 그룹 디렉토리 서브트리에서 사용자와 그룹을 검색하는 데 사용됩니다. 유효한 값은 1~99입니다. 기본값은 20입니다.
Force reconnect every N seconds(N초마다 강제로 다시 연결**)**	서버가 지정된 시간 간격에 LDAP 연결을 갱신하도록 강제 지정하려면 이 확인란을 선택하고 **Seconds(**초**)** 필드에 원하는 값을 입력합니다. 유효 범위는 1분~60분입니다.
Test Bind to Server(서버에 대한 바인딩 테스트**)**	LDAP 서버 세부정보 및 자격 증명을 정상적으로 바인딩할 수 있는지를 테스트하고 확인하려면 클릭합니다. 테스트가 실패하는 경우 LDAP 서버 세부정보를 편집한 후에 다시 테스트해 주십시오.
Failover(페일오버**)**	
Always Access Primary Server First(항상 기본 서버에 먼저 액세스**)**	Cisco ISE가 인증 및 권한 부여를 위해 항상 기본 LDAP 서버에 먼저 액세스하도록 하려면 이 옵션을 클릭합니다.
Failback to Primary Server After(다음 시간 이후 기본 서버로 장애 복구**)**	Cisco ISE가 연결하려고 하는 기본 LDAP 서버에 연결할 수 없는 경우 Cisco ISE는 보조 LDAP 서버에 연결하려고 시도합니다. Cisco ISE가 기본 LDAP 서버를 다시 사용하도록 하려면 이 옵션을 클릭하고 텍스트 상자에 값을 입력합니다.

LDAP 디렉토리 조직 설정

다음 표에서는 **Directory Organization(**디렉토리 조직**)** 탭의 필드에 대해 설명합니다.

표 ***51: LDAP*** 디렉토리 조직 설정

필드 이름	사용 지침
Subject Search Base(주체 검색 기준**)**	모든 주체를 포함하는 서브트리의 DN을 입력합니다. 예를 들면 다음과 같습니다. o=corporation.com 주체를 포함하는 트리가 기본 DN인 경우 LDAP 컨피그레이션에 따라 o=corporation.com 또는 dc=corporation,dc=com 을 입력합니다. 자세한 내용은 LDAP 데이터베이스 설명서를 참고해 주십시오.
Group Search Base(그룹 검색 기준**)**	모든 그룹을 포함하는 서브트리의 DN을 입력합니다. 예를 들면 다음과 같습니다. ou=조직 단위, ou=다음 조직 단위, o=corporation.com 그룹을 포함하는 트리가 기본 DN인 경우 LDAP 컨피그레이션에 따라 o=corporation.com 또는 dc=corporation,dc=com 을 입력합니다. 자세한 내용은 LDAP 데이터베이스 설명서를 참고해 주십시오.

필드 이름	사용 지침
Search for MAC Address in Format(MAC 주소 검색 형식**)**	LDAP 데이터베이스에서 Cisco ISE가 검색에 사용할 MAC 주소 형식을 입력합니다. 내부 ID 소스의 MAC 주소는 xx-xx-xx-xx-xx-xx 형식으로 제공됩니다. LDAP 데이터베이스의 MAC 주소는 다른 형식으로 제공될 수 있습니다. 그러나 Cisco ISE는 호스트 조회 요청을 받으면 MAC 주소를 내부 형식에서 이 필드에 지정된 형식으로 변환합니다. 드롭다운 목록을 사용하여 특정 형식의 MAC 주소 검색을 활성화합니다. 여기서 <*format*>은 다음 중 하나일 수 있습니다. • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 선택한 형식은 LDAP 서버에서 제공되는 MAC 주소의 형식과 일치해야 합니다.
Strip Start of Subject Name Up To the Last Occurrence of the Separator(마지막으로 나타나는 구분 기호까지 주체 이름 시작 부분 분리**)**	사용자 이름에서 도메인 접두사를 제거하려면 적절한 텍스트를 입력합니다. Cisco ISE는 사용자 이름에서 이 필드에 지정된 구분 기호 문자를 찾으면 사용자 이름이 시작되는 부분부터 구분 기호 문자까지의 모든 문자를 분리합니다. <start_string> 상자에 지정된 문자 중 두 개 이상이 사용자 이름에 포함되어 있으면 Cisco ISE는 마지막으로 나타나는 구분 기호까지 문자를 분리합니다. 예를 들어 구분 기호 문자가 백슬래시(\)이고 사용자 이름이 DOMAIN\user1이면 Cisco ISE는 user1을 LDAP 서버에 제출합니다. 참고 <start_string>은 우물 정자(#), 물음표(?), 큰따옴표("), 별표(*), 오른쪽 꺾쇠 괄호(>) 및 왼쪽 꺾쇠 괄호(<)와 같은 특수 문자를 포함할 수 없습니다. Cisco ISE에서는 사용자 이름에 이러한 문자를 사용할 수 없습니다.

필드 이름	사용 지침
Strip End of Subject Name from the First Occurrence of the Separator(처음으로 나타나는 구분 기호부터 주체 이름 끝 부분 분리**)**	사용자 이름에서 도메인 접미사를 제거하려면 적절한 텍스트를 입력합니다. Cisco ISE는 사용자 이름에서 이 필드에 지정된 구분 기호 문자를 찾으면 구분 기호 문자부터 사용자 이름이 끝나는 부분까지의 모든 문자를 분리합니다. 이 필드에 지정된 문자 중 두 개 이상이 사용자 이름에 포함되어 있으면 Cisco ISE는 처음으로 나타나는 구분 기호부터 문자를 분리합니다. 예를 들어 구분 기호 문자가 @이고 사용자 이름이 *user1@domain*이면 Cisco ISE는 *user1*을 LDAP 서버에 제출합니다. 참고 <*end_string*> 상자에는 우물 정자(#), 물음표(?), 큰따옴표("), 별표(*), 오른쪽 꺾쇠 괄호(>) 및 왼쪽 꺾쇠 괄호(<)와 같은 특수 문자를 포함할 수 없습니다. Cisco ISE에서는 사용자 이름에 이러한 문자를 사용할 수 없습니다.

LDAP 그룹 설정

표 ***52: LDAP*** 그룹 설정

필드 이름	사용 지침
Add(추가**)**	새 그룹을 추가하려면 **Add(**추가**) > Add Group(**추가 그룹**)**을 선택합니다. 또는 LDAP 디렉토리에서 그룹을 선택하려면 **Add(**추가**) > Select Groups From Directory(**디렉토리에서 그룹 선택**)**를 선택합니다. 그룹을 추가하도록 선택하는 경우 새 그룹의 이름을 입력합니다. 디렉토리에서 선택하는 경우 필터 기준을 입력하고 **Retrieve Groups(**그룹 검색**)**를 클릭합니다. 선택할 그룹 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다. 선택한 그룹이 **Groups(**그룹**)** 창에 표시됩니다.

LDAP 속성 설정

표 *53: LDAP* 속성 설정

필드 이름	사용 지침
Add(추가)	새 속성을 추가하려면 **Add(추가) > Add Attribute(속성 추가)**를 선택합니다. 또는 LDAP 서버에서 속성을 선택하려면 **Add(추가) > Select Attributes From Directory(디렉토리에서 속성 선택)**를 선택합니다. 속성을 추가하도록 선택하는 경우 새 속성의 이름을 입력합니다. 디렉토리에서 선택하는 경우 사용자 이름을 입력하고 **Retrieve Attributes(속성 검색)**를 클릭하여 속성을 검색합니다. 선택할 속성 옆의 확인란을 선택하고 OK(확인)를 클릭합니다.

LDAP 고급 설정

다음 표에서는 Advanced Settings(고급 설정) 탭의 필드에 대해 설명합니다.

표 *54: LDAP* 고급 설정

필드 이름	사용 지침
Enable Password Change(비밀번호 변경 활성화)	디바이스 관리자에 PAP 프로토콜을 사용하고 네트워크 액세스에 RADIUS EAP-GTC 프로토콜을 사용하는 동안 비밀번호 만료 또는 비밀번호 재설정이 발생할 때 사용자가 비밀번호를 변경할 수 있도록하려면 이 확인란을 선택합니다. 지원되지 않는 프로토콜에 대한 사용자 인증은 실패합니다. 또한 이 옵션을 사용하면 사용자가 다음 로그인 시 비밀번호를 변경할 수 있습니다.

관련 항목

LDAP 디렉토리 서비스, 640 페이지
LDAP 사용자 인증, 642 페이지
LDAP 사용자 조회, 645 페이지
LDAP ID 소스 추가, 645 페이지

RADIUS 토큰 ID 소스 설정

다음 표에서는 외부 RADIUS ID 소스를 구성하고 해당 소스에 연결하는 데 사용할 수 있는 RADIUS 토큰 ID 소스 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > RADIUS Token(RADIUS 토큰)**입니다.

표 *55: RADIUS* 토큰 *ID* 소스 설정

필드 이름	사용 지침
Name(이름**)**	RADIUS 토큰 서버의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
Description(설명**)**	RADIUS 토큰 서버에 대한 설명을 입력합니다. 최대 문자 수는 1,024자입니다.
SafeWord Server(SafeWord 서버**)**	RADIUS ID 소스가 SafeWord 서버인 경우 이 확인란을 선택합니다.
Enable Secondary Server(보조 서버 활성화**)**	기본 서버에 오류가 발생하는 경우 백업으로 사용할 Cisco ISE용 보조 RADIUS 토큰 서버를 활성화하려면 이 확인란을 선택합니다. 이 확인란을 선택하는 경우 보조 RADIUS 토큰 서버를 구성해야 합니다.
Always Access Primary Server First(항상 기본 서버에 먼저 액세스**)**	Cisco ISE가 항상 기본 서버에 먼저 액세스하도록 하려면 이 옵션을 클릭합니다.
Fallback to Primary Server after(다음 시간 이후 기본 서버로 대체**)**	기본 서버에 연결할 수 없는 경우 Cisco ISE가 보조 RADIUS 토큰 서버를 사용하여 인증할 수 있는 시간(분)을 지정하려면 이 옵션을 클릭합니다. 이 시간이 경과하면 Cisco ISE는 기본 서버에 대한 인증을 재시도합니다.
기본 서버	
Host IP(호스트 **IP)**	기본 RADIUS 토큰 서버의 IP 주소를 입력합니다. 이 필드에는 문자열로 표시되는 유효한 IP 주소를 입력할 수 있습니다. 이 필드에 입력할 수 있는 문자는 숫자와 점(.)입니다.
Shared Secret(공유 암호**)**	이 연결에 대해 기본 RADIUS 토큰 서버에 구성된 공유 암호를 입력합니다.
Authentication Port(인증 포트**)**	기본 RADIUS 토큰 서버가 수신 대기 중인 포트 번호를 입력합니다.
Server Timeout(서버 시간 초과**)**	기본 RADIUS 토큰 서버가 다운되었다고 결정할 때까지 Cisco ISE가 기본 서버로부터의 응답을 대기할 시간을 초 단위로 지정합니다.
Connection Attempts(연결 시도 횟수**)**	Cisco ISE가 보조 서버(정의된 경우)로 이동하거나 보조 서버가 정의되어 있지 않은 경우 요청을 삭제하기 전에 기본 서버에 다시 연결을 시도해야 하는 횟수를 지정합니다.

필드 이름	사용 지침
보조 서버	
Host IP(호스트 **IP)**	보조 RADIUS 토큰 서버의 IP 주소를 입력합니다. 이 필드에는 문자열로 표시되는 유효한 IP 주소를 입력할 수 있습니다. 이 필드에 입력할 수 있는 문자는 숫자와 점(.)입니다.
Shared Secret(공유 암호**)**	이 연결에 대해 보조 RADIUS 토큰 서버에 구성된 공유 암호를 입력합니다.
Authentication Port(인증 포트**)**	보조 RADIUS 토큰 서버가 수신 대기 중인 포트 번호를 입력합니다. 유효한 값은 1~65,535입니다. 기본값은 1,812입니다.
Server Timeout(서버 시간 초과**)**	보조 RADIUS 토큰 서버가 다운되었다고 결정할 때까지 Cisco ISE가 보조 서버로부터의 응답을 대기할 시간을 초 단위로 지정합니다.
Connection Attempts(연결 시도 횟수**)**	Cisco ISE가 요청을 삭제하기 전에 보조 서버에 다시 연결을 시도해야 하는 횟수를 지정합니다.

관련 항목

RADIUS 토큰 ID 소스, 665 페이지
RADIUS 토큰 서버 추가, 671 페이지

RSA SecurID ID 소스 설정

다음 표에서는 RSA SecurID ID 소스를 생성하고 해당 소스에 연결하는 데 사용할 수 있는 RSA SecurID ID 소스 페이지의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID**입니다.

RSA 프롬프트 설정

다음 표에서는 **RSA Prompts(RSA** 프롬프트**)** 탭의 필드에 대해 설명합니다.

표 ***56: RSA*** 프롬프트 설정

필드 이름	사용 지침
Enter Passcode Prompt(암호 프롬프트 입력**)**	암호를 가져오기 위한 텍스트 문자열을 입력합니다.
Enter Next Token Code(다음 토큰 코드 입력**)**	다음 토큰을 요청하기 위한 텍스트 문자열을 입력합니다.

필드 이름	사용 지침
Choose PIN Type(PIN 유형 선택**)**	PIN 유형을 요청하기 위한 텍스트 문자열을 입력합니다.
Accept System PIN(시스템 **PIN** 수락**)**	시스템에서 생성된 핀 번호를 수락하기 위한 텍스트 문자열을 입력합니다.
Enter Alphanumeric PIN(영숫자 **PIN** 입력**)**	영숫자 PIN을 요청하기 위한 텍스트 문자열을 입력합니다.
Enter Numeric PIN(숫자 **PIN** 입력**)**	숫자 PIN을 요청하기 위한 텍스트 문자열을 입력합니다.
Re-enter PIN(PIN 다시 입력**)**	사용자에게 PIN을 다시 입력하도록 요청하기 위한 텍스트 문자열을 입력합니다.

RSA 메시지 설정

다음 표에서는 **RSA Messages(RSA** 메시지**)** 탭의 필드에 대해 설명합니다.

표 ***57: RSA*** 메시지 설정

필드 이름	사용 지침
Display System PIN Message(시스템 **PIN** 메시지 표시**)**	시스템 PIN 메시지에 레이블을 지정하기 위한 텍스트 문자열을 입력합니다.
Display System PIN Reminder(시스템 **PIN** 알림 표시**)**	사용자에게 새 PIN을 저장하도록 알리기 위한 텍스트 문자열을 입력합니다.
Must Enter Numeric Error(숫자를 입력해야 함 오류**)**	사용자에게 PIN에 숫자만 입력해야 하도록 지시하기 위한 메시지를 입력합니다.
Must Enter Alpha Error(영숫자를 입력해야 함 오류**)**	사용자에게 PIN에 영숫자 문자만 입력해야 하도록 지시하기 위한 메시지를 입력합니다.
PIN Accepted Message(PIN 수락됨 메시지**)**	사용자의 PIN이 시스템에서 수락되면 표시되는 메시지를 입력합니다.
PIN Rejected Message(PIN 거부됨 메시지**)**	시스템에서 사용자의 PIN을 거부하면 표시되는 메시지를 입력합니다.
User Pins Differ Error(사용자 **PIN**이 다름 오류**)**	사용자가 잘못된 PIN을 입력하면 표시되는 메시지를 입력합니다.
System PIN Accepted Message(시스템이 **PIN**을 수락함 메시지**)**	시스템에서 PIN을 수락하면 사용자에게 표시되는 메시지를 입력합니다.

필드 이름	사용 지침
Bad Password Length Error(잘못된 비밀번호 길이 오류**)**	사용자가 지정한 PIN이 PIN 길이 정책에 지정된 범위를 벗어나면 표시되는 메시지를 입력합니다.

관련 항목

RSA ID 소스, 672 페이지
Cisco ISE와 RSA SecurID 서버 통합, 673 페이지
RSA ID 소스 추가, 676 페이지

Cisco ISE 사용자

이 장에서 사용자란 용어는 네트워크에 정기적으로 액세스하는 직원 및 계약자, 그리고 스폰서 및 게스트 사용자를 가리킵니다. 스폰서 사용자는 스폰서 포털을 통해 guest-user 계정을 생성하고 관리하는 조직의 직원 또는 계약자입니다. 게스트 사용자는 제한된 기간 동안 조직의 네트워크 리소스에 액세스해야 하는 외부 방문자입니다.

사용자가 Cisco ISE 네트워크의 리소스 및 서비스에 대한 액세스를 얻으려면 관리자가 계정을 생성해야 합니다. 직원, 계약자 및 스폰서 사용자는 관리 포털에서 생성합니다.

사용자 ID

사용자 ID는 사용자에 대한 정보를 보유하는 컨테이너와 유사하며 네트워크 액세스 자격 증명을 형성합니다. 각 사용자의 ID는 데이터로 정의되며 사용자 이름, 이메일 주소, 비밀번호, 계정 설명, 연결된 관리 그룹, 사용자 그룹 및 역할을 포함합니다.

사용자 그룹

사용자 그룹은 특정 Cisco ISE 서비스 및 기능 집합에 액세스할 수 있게 해주는 공통 권한 집합을 공유하는 개인 사용자 컬렉션입니다.

사용자 ID 그룹

사용자의 그룹 ID는 동일 그룹에 속하는 특정 사용자 그룹을 식별하고 설명하는 요소로 이루어집니다. 그룹 이름은 이 그룹의 멤버가 지닌 기능적 역할에 대한 설명입니다. 그룹은 이 그룹에 속하는 사용자 목록입니다.

기본 사용자 ID 그룹

Cisco ISE에서는 다음과 같이 미리 정의된 사용자 ID 그룹이 제공됩니다.

- All_Accounts
- 직원

- Group_Accounts
- GuestType_Contractor
- GuestType_Daily
- GuestType_SocialLogin
- GuestType_Weekly
- Own_Accounts

사용자 역할

사용자 역할은 사용자가 수행할 수 있는 작업 및 Cisco ISE 네트워크에서 액세스할 수 있는 서비스를 결정하는 권한 집합입니다. 사용자 역할은 사용자 그룹과 연결됩니다(예: 네트워크 액세스 사용자).

사용자 계정 맞춤형 속성

Cisco ISE를 통해 네트워크 액세스 사용자와 관리자 모두의 사용자 속성에 따라 네트워크 액세스를 제한할 수 있습니다. Cisco ISE에서는 미리 정의된 사용자 속성 집합이 제공되며 이를 통해 사용자 맞춤화 속성을 생성할 수도 있습니다. 두 속성 유형을 모두 인증 정책을 정의하는 조건에 사용할 수 있습니다. 또한 비밀번호가 지정된 기준을 충족하도록 사용자 계정에 대한 비밀번호 정책을 정의할 수 있습니다.

사용자 맞춤화 사용자 속성

User Custom Attributes(사용자 맞춤화 속성**)** 창(**Administration(**관리**) > Identity Management(ID** 관리**) > Settings(**설정**) > User Custom Attributes(**사용자 맞춤화 속성**)**)에서 user-account 속성을 추가로 구성할 수 있습니다. 이 창에서 미리 정의된 사용자 속성 목록을 볼 수도 있습니다. 미리 정의된 사용자 속성은 수정할 수 없습니다.

User Custom Attributes(사용자 맞춤화 속성**)** 패널에 필요한 세부정보를 입력하여 새 맞춤화 속성을 추가합니다. **User Custom Attributes(**사용자 맞춤화 속성**)** 창에 추가한 맞춤화 속성 및 기본값이 네트워크 액세스 사용자(**Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**) > Add/Edit(**추가/편집**)**) 또는 관리 사용자(**Administration(**관리**) > System(**시스템**) > Admin Access(**관리자 액세스**) > Administrators(**관리자**) > Admin Users(**관리 사용자**) > Add/Edit(**추가/편집**)**)를 추가하거나 편집하는 동안 표시됩니다. 네트워크 액세스 또는 관리 사용자를 추가하거나 편집하는 동안 기본값을 변경할 수 있습니다.

User Custom Attributes(사용자 맞춤화 속성**)** 창에서 사용자 맞춤화 속성에 대해 다음 데이터 유형을 선택할 수 있습니다.

- 문자열: 최대 문자열 길이(문자열 속성 값에 허용되는 최대 길이)를 지정할 수 있습니다.
- 정수: 최솟값과 최댓값을 구성할 수 있습니다(허용되는 최저 및 최고 정수 값 지정).
- 열거형: 각 매개변수에 대해 다음 값을 지정할 수 있습니다.
    - 정수 값

- 표시 값

기본 매개변수를 지정할 수도 있습니다. 네트워크 액세스 또는 관리 사용자를 추가하거나 편집하는 동안 Display(표시) 필드에 추가한 값이 표시됩니다.

- 부동 소수점
- 비밀번호: 최대 문자열 길이를 지정할 수 있습니다.
- 길이: 최솟값과 최댓값을 구성할 수 있습니다.
- IP: 기본 IPv4 또는 IPv6 주소를 지정할 수 있습니다.
- 부울: True 또는 False를 기본값으로 설정할 수 있습니다.
- 날짜: 일정표에서 날짜를 선택하여 기본값으로 설정할 수 있습니다. 날짜는 yyyy-mm-dd 형식으로 표시됩니다.

네트워크 액세스 또는 관리 사용자를 추가하거나 편집하는 동안 속성을 필수로 지정하려면 **Mandatory(**필수**)** 확인란을 선택합니다. 사용자 맞춤화 속성에 대한 기본값을 설정할 수도 있습니다.

사용자 맞춤화 속성은 인증 정책에서도 사용 가능합니다. 사용자 맞춤화 속성에 대해 설정한 데이터 유형 및 허용 범위는 정책 조건의 사용자 맞춤화 속성 값에 적용됩니다.

사용자 인증 설정

일부 외부 ID 저장소에서는 네트워크 액세스 사용자가 비밀번호를 변경할 수 없습니다. 자세한 내용은 각 ID 소스에 대한 섹션을 참조하십시오.

네트워크 사용 비밀번호 규칙은 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **User Authentication Settings(**사용자 인증 설정**)**에 구성됩니다.

다음 섹션에는 **Password Policy(**비밀번호 정책**)** 탭의 일부 필드에 대한 추가 정보가 있습니다.

- **Required characters(**필수 문자**)**: 대문자나 소문자가 필요한 사용자 비밀번호 정책을 구성했는데 사용자의 언어가 이러한 문자를 지원하지 않는 경우 사용자는 비밀번호를 설정할 수 없습니다. UTF-8 문자를 지원하려면 다음 확인란의 선택을 취소하십시오.
  - 소문자 알파벳 문자
  - 대문자 알파벳 문자
- **Password Change Delta(**비밀번호 변경 델타**)**: 현재 비밀번호를 새 비밀번호로 변경할 때 수정해야 하는 최소 문자 수를 지정합니다. Cisco ISE에서는 문자 위치 변경을 수정으로 간주하지 않습니다.

  예를 들어 비밀번호 델타가 3이고 현재 비밀번호가 "?Aa1234?"인 경우 "?Aa1567?" (3개의 새 문자는 "5","6" 및 "7")이 유효한 새 비밀번호입니다. "?Aa1562?"는 현재 비밀번호에 사용된 "?","2" 및 "?"가 있으므로 설정할 수 없습니다. "Aa1234??" 역시 사용할 수 없는데, 문자 위치가 변경되었더라도 동일한 문자가 현재 비밀번호에 있기 때문입니다.

비밀번호 변경 델타도 이전 X 비밀번호를 고려합니다. 여기서 X는 비밀번호는 이전 버전과 달라야 함의 값입니다. 비밀번호 델타가 3이고 비밀번호 기록이 2라면 과거 2개의 비밀번호에 포함되지 않은 문자 4개를 변경해야 합니다.

- **Dictionary words(**사전 단어**)**: 사전 단어의 사용, 역순으로 된 문자 또는 다른 문자로 대체되는 문자를 제한하려면 이 확인란을 선택합니다.

  "s"를 "$", "a"를 "@", "o"를 "0", "l"을 "1", "i"를 "!", "e"를 "3"으로 대체할 수 없습니다. 예를 들면 "Pa$$w0rd"입니다.

  - **Default Dictionary(**기본 사전**)**: Cisco ISE에서 기본 Linux 사전을 사용하려면 이 옵션을 선택합니다. 기본 사전에는 약 480,000개의 영어 단어가 포함되어 있습니다.
  - **Custom Dictionary(**맞춤형 사전**)**: 맞춤 설정한 사전을 사용하려면 이 옵션을 선택합니다. **Choose File(**파일 선택**)**을 클릭하여 맞춤형 사전 파일을 선택합니다. 텍스트 파일은 새 줄 구분된 단어, .dic 확장자여야 하며 크기가 20MB 미만이어야 합니다.

- **Password Lifetime(**비밀번호 수명**)** 섹션을 사용하여 비밀번호 재설정 간격 및 알림을 업데이트할 수 있습니다. 비밀번호 수명을 설정하려면 **Disable user account after __ days if password was not changed(**비밀번호를 변경하지 않으면 __일 후 사용자 계정 비활성화**)** 확인란을 선택하고 입력 필드에 일 수를 입력합니다. 비밀번호 재설정을 위해 미리 알림 이메일을 전송하려면 **Display Reminder __ Days Before Password Expiration(**비밀번호 만료 전 __ 일 이전 비밀번호 표시**)** 확인란을 선택하고 네트워크 액세스 사용자에 대해 구성된 이메일 주소로 미리 알림 이메일을 전송해야 하는 기간(일)을 입력합니다. 네트워크 액세스 사용자를 생성하는 동안 **Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**) > Add Network Access User(**네트워크 액세스 사용자 추가**)** 창에서 이메일 주소를 추가하여 비밀번호 재설정을 위한 이메일 알림을 보낼 수 있습니다.

  참고

  - 다음 이메일 주소에서 미리 알림 이메일이 전송됩니다. iseadminportal@<ISE-Primary-FQDN>. 이 발신자에 대한 액세스를 명시적으로 허용해야 합니다.
  - 이메일 내용은 사용자 지정할 수 없습니다. 알림 이메일의 내용은 다음과 같습니다. 네트워크 액세스 비밀번호는 <비밀번호 만료 날짜 및 시간>에 만료됩니다. 도움이 필요한 경우 시스템 관리자에게 문의하십시오.

- **Lock/Suspend Account with Incorrect Login Attempts(**잘못된 로그인 시도 시 계정 잠금/일시 중지**)**: 로그인 시도가 지정된 횟수만큼 실패한 경우 이 옵션을 사용하여 계정을 일시 중지하거나 잠글 수 있습니다. 유효 범위는 3~20입니다.

- **Account Disable Policy(**계정 비활성화 정책**)** 탭에서는 기존 사용자 계정을 비활성화할 시기에 대한 규칙을 구성합니다. 자세한 내용은 전역적으로 사용자 계정 비활성화를 참조하십시오.

관련 항목

사용자 계정 맞춤형 속성, 522 페이지

사용자 추가, 525 페이지

사용자 및 관리자의 자동 비밀번호 생성

사용자 및 관리자 생성 창에서는 Cisco ISE 비밀번호 정책을 준수하는 인스턴트 비밀번호를 생성하는 **Generate Password(**비밀번호 생성**)** 옵션을 사용할 수 있습니다. 따라서 사용자나 관리자는 구성할 안전한 비밀번호를 생각하는 데 시간을 소비하는 대신 Cisco ISE에서 생성하는 비밀번호를 사용할 수 있습니다.

Generate Password(비밀번호 생성**)** 옵션은 다음 창에서 사용할 수 있습니다.

- **Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**)**
- **Administration(**관리**) > System(**시스템**) > Admin Access(**관리자 액세스**) > Administrators(**관리자**) > Admin Users(**관리자 사용자**)**.
- **Settings(**설정**) > Account Settings(**계정 설정**) > Change Password(**비밀번호 변경**)**.

내부 사용자 작업

사용자 추가

Cisco ISE에서는 Cisco ISE 사용자의 속성에 대해 확인/생성/수정/복제/삭제/상태 변경/가져오기/내보내기/검색을 수행할 수 있습니다.

Cisco ISE 내부 데이터베이스를 사용 중인 경우에는 Cisco ISE 네트워크의 리소스나 서비스에 액세스해야 하는 새 사용자에 대해 계정을 생성해야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다.

Work Centers(작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Identities(ID)** > **Users(**사용자**)** 페이지에 액세스하여 사용자를 생성할 수도 있습니다.

단계 **2** 새 사용자를 생성하려면 **Add (+)(**추가**(+))**를 클릭합니다.

단계 **3** 필드에 값을 입력합니다**.**

사용자 이름에 !, %, :, ;, [, {, |, },], `, ?, =, <, >, \ 문자와 제어 문자를 포함하지 마십시오. 공백으로만 구성된 사용자 이름도 허용되지 않습니다. BYOD용으로 Cisco ISE 내부 CA(Certificate Authority)를 사용하는 경우 여기에 입력하는 사용자 이름이 엔드포인트 인증서의 공용 이름으로 사용됩니다. Cisco ISE 내부 CA는 Common Name(공용 이름) 필드에서 "+" 또는 "*" 문자를 지원하지 않습니다.

단계 **4** 새 사용자를 Cisco ISE 내부 데이터베이스에 저장하려면 **Submit(**제출**)**을 클릭합니다.

Cisco ISE 사용자 데이터 내보내기

Cisco ISE 내부 데이터베이스에서 사용자 데이터를 내보내야 할 수 있습니다. Cisco ISE에서는 비밀번호로 보호된 csv 파일 형식으로 사용자 데이터를 내보낼 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다.

단계 **2** 데이터를 내보낼 사용자에 해당하는 확인란을 선택합니다.

단계 **3** **Export Selected(**선택 항목 내보내기**)**를 클릭합니다.

단계 **4** Key(키) 필드에 비밀번호를 암호화하는 키를 입력합니다.

단계 **5** users.csv 파일을 생성하려면 **Start Export(**내보내기 시작**)**를 클릭합니다.

단계 **6** users.csv 파일을 내보내려면 **OK(**확인**)**를 클릭합니다.

Cisco ISE 내부 사용자 가져오기

CSV 파일을 사용하여 새 사용자 데이터를 ICisco SE로 가져와 내부 계정을 새로 생성할 수 있습니다. 사용자 계정을 가져오는 동안 템플릿 CSV 파일 다운로드가 가능합니다. 스폰서는 스폰서 포털에서 사용자를 가져올 수 있습니다. 를 참조하십시오.

참고 CSV 파일에 맞춤형 속성이 포함되어 있으면 가져오는 동안 맞춤형 속성에 대해 설정한 데이터 유형 및 허용 범위가 맞춤형 속성 값에 적용됩니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다.

단계 **2** 쉼표로 구분된 텍스트 파일에서 사용자를 가져오려면 **Import(**가져오기**)**를 클릭합니다.

쉼표로 구분된 텍스트 파일이 없으면 **Generate a Template(**템플릿 생성**)**을 클릭하여 제목 행이 채워진 CSV 파일을 생성합니다.

단계 **3** File(파일) 텍스트 상자에 가져올 사용자가 포함된 파일명을 입력하거나 **Browse(**찾아보기**)**를 클릭하고 파일이 있는 위치로 이동합니다.

단계 **4** 새 사용자를 생성하는 동시에 기존 사용자를 업데이트하려면 **Create new user(s) and update existing user(s) with new data(**새 사용자를 생성하고 새 데이터로 기존 사용자 업데이트**)** 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

참고 모든 네트워크 액세스 사용자를 한 번에 삭제하지 않는 것이 좋습니다. 한 번에 삭제하면 CPU 사용량이 급증하여 서비스가 충돌할 수 있습니다(특히 매우 큰 데이터베이스를 사용하는 경우).

엔드포인트 설정

다음 표에서는 엔드포인트를 생성하고 엔드포인트용 정책을 할당하는 데 사용할 수 있는 **Endpoints(**엔드포인트**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**입니다.

표 ***58:*** 엔드포인트 설정

필드 이름	사용 지침
MAC Address(MAC 주소**)**	정적으로 엔드포인트를 생성하기 위한 MAC 주소를 16진수 형식으로 입력합니다. MAC 주소는 Cisco ISE가 활성화된 네트워크에 연결되어 있는 인터페이스의 디바이스 식별자입니다.
Static Assignment(정적 할당**)**	정적 할당 상태가 정적으로 설정되어 있을 때 엔드포인트 창에서 엔드포인트를 정적으로 생성하려면 이 확인란을 선택합니다. 엔드포인트의 정적 할당 상태는 정적에서 동적으로 또는 동적에서 정적으로 전환할 수 있습니다.
Policy Assignment(정책 할당**)**	(**Static Assignment(**정적 할당**)**가 선택되어 있지 않으면 기본적으로 비활성화됨) **Policy Assignment(**정책 할당**)** 드롭다운 목록에서 일치하는 엔드포인트 정책을 선택합니다. 다음 중 하나를 수행할 수 있습니다. • 일치하는 엔드포인트 정책을 선택하지 않고 기본 엔드포인트 정책인 Unknown(알 수 없음)을 사용하는 경우 엔드포인트의 동적 프로파일링을 허용하는 엔드포인트에 대해 정적 할당 상태가 동적으로 설정됩니다. • Unknown(알 수 없음) 이외의 일치하는 엔드포인트 정책을 선택하는 경우에는 해당 엔드포인트에 대해 정적 할당 상태가 정적으로 설정되며 **Static Assignment(**정적 할당**)** 확인란이 자동으로 선택됩니다.

필드 이름	사용 지침
Static Group Assignment(정적 그룹 할당**)**	엔드포인트를 ID 그룹에 정적으로 할당하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 이전에 다른 엔드포인트 ID 그룹에 동적으로 할당되었던 엔드포인트에 대해 다음 번에 엔드포인트 정책을 평가하는 동안 프로파일링 서비스가 엔드포인트 ID 그룹을 변경하지 않습니다. 이 확인란의 선택을 취소하면 정책 컨피그레이션에 따라 엔드포인트 ID 그룹이 ISE 프로파일러가 할당한 대로 동적으로 설정됩니다. Static Group Assignment(정적 그룹 할당) 옵션을 선택하지 않으면 다음 번에 엔드포인트 정책을 평가하는 동안 엔드포인트가 일치하는 ID 그룹에 자동으로 할당됩니다.

Identity Group Assignment(ID 그룹 할당**)**	엔드포인트를 할당할 엔드포인트 ID 그룹을 선택합니다.
	
	엔드포인트에 대한 엔드포인트 정책 평가 중에 **Create Matching Identity Group(**일치하는 **ID** 그룹 생성**)** 옵션을 사용하지 않으려는 경우 또는 엔드포인트를 정적으로 생성하는 경우 ID 그룹에 엔드포인트를 할당할 수 있습니다.
	
	Cisco ISE에는 시스템에서 생성된 다음과 같은 엔드포인트 ID 그룹이 포함되어 있습니다.
	• Blocked List
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

관련 항목

식별된 엔드포인트, 753 페이지
정책 및 ID 그룹을 정적으로 할당하여 엔드포인트 생성, 748 페이지

LDAP에서 엔드포인트 가져오기 설정

다음 표에서는 LDAP 서버에서 엔드포인트를 가져오는 데 사용할 수 있는 Import from LDAP(LDAP에서 가져오기) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**입니다.

표 ***59: LDAP***에서 엔드포인트 가져오기 설정

필드 이름	사용 지침
Connection Settings(연결 설정**)**	
Host(호스트**)**	LDAP 서버의 호스트 이름 또는 IP 주소를 입력합니다.
Port(포트**)**	LDAP 서버의 포트 번호를 입력합니다. LDAP 서버에서 가져오려는 경우 기본 포트인 389를 사용할 수 있으며, SSL을 통해 LDAP 서버에서 가져오려는 경우 기본 포트인 636을 사용할 수 있습니다. 참고 Cisco ISE는 구성된 모든 포트 번호를 지원합니다. 구성된 값은 LDAP 서버 연결 세부정보와 일치해야 합니다.
Enable Secure Connection(보안 연결 활성화**)**	SSL을 통해 LDAP 서버에서 가져오려면 **Enable Secure Connection(**보안 연결 활성화**)** 확인란을 선택합니다.
Root CA Certificate Name(루트 **CA** 인증서 이름**)**	신뢰할 수 있는 CA 인증서를 보려면 드롭다운 화살표를 클릭합니다. 루트 CA 인증서 이름은 LDAP 서버에 연결하는 데 필요한 신뢰할 수 있는 CA 인증서를 지칭합니다. Cisco ISE에서는 신뢰할 수 있는 CA 인증서를 추가(가져오기), 편집, 삭제 및 내보내기할 수 있습니다.
Anonymous Bind(익명 바인딩**)**	**Anonymous Bind(**익명 바인딩**)** 확인란을 활성화하거나 slapd.conf 구성 파일에서 LDAP 관리자 자격 증명을 입력해야 합니다.
Admin DN(관리자 **DN)**	slapd.conf 구성 파일에서 LDAP 관리자에 대해 구성된 DN(Distinguished Name)을 입력합니다. 관리자 DN 형식의 예제는 cn=Admin, dc=cisco.com, dc=com과 같습니다.
Password(비밀번호**)**	slapd.conf 구성 파일에서 LDAP 관리자에 대해 구성된 비밀번호를 입력합니다.

필드 이름	사용 지침
Base DN(기본 **DN)**	부모 엔트리의 고유 이름을 입력합니다. 기본 DN 형식의 예제는 dc=cisco.com, dc=com과 같습니다.
Query Settings(쿼리 설정**)**	
MAC Address objectClass(MAC 주소 **objectClass)**	MAC 주소를 가져오는 데 사용되는 쿼리 필터(예: ieee802Device)를 입력합니다.
MAC Address Attribute Name(MAC 주소 속성 이름**)**	가져오려는 반환된 속성 이름(예: macAddress)을 입력합니다.
Profile Attribute Name(프로파일 속성 이름**)**	LDAP 속성의 이름을 입력합니다. 이 속성은 LDAP 서버에 정의되어 있는 각 엔드포인트 엔트리에 대한 정책 이름을 포함합니다. **Profile Attribute Name(**프로파일 속성 이름**)** 필드를 구성할 때는 다음 사항을 고려합니다. • **Profile Attribute Name(**프로파일 속성 이름**)** 필드에서 이 LDAP 속성을 지정하지 않거나 이를 잘못 구성하는 경우에는 가져오기 작업 중에 엔드포인트가 "알 수 없음"으로 표시되며 이러한 엔드포인트는 일치하는 엔드포인트 프로파일링 정책으로 별도로 프로파일이 지정됩니다. • **Profile Attribute Name(**프로파일 속성 이름**)** 필드에서 이 LDAP 속성을 구성하면 속성 값을 검증하여 엔드포인트 정책이 Cisco ISE의 기존 정책과 일치하는지를 확인한 다음, 엔드포인트를 가져옵니다. 엔드포인트 정책이 기존 정책과 일치하지 않으면 해당 엔드포인트를 가져오지 않습니다.
Time Out(시간 초과**)**	시간을 초 단위로 입력합니다. 유효한 범위는 1초 ~ 60초입니다.

관련 항목

식별된 엔드포인트, 753 페이지
LDAP 서버에서 엔드포인트 가져오기, 752 페이지

ID 그룹 작업

사용자 ID 그룹 생성

사용자 ID 그룹을 생성해야 해당 그룹에 사용자를 할당할 수 있습니다.

단계 1 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Identity Groups(ID** 그룹**)** > **User Identity Groups(**사용자 **ID** 그룹**)** > **Add(**추가**)**를 선택합니다.

Work Centers(작업 센터**)** > **Device Administration(**디바이스 관리**)** > **User Identity Groups(**사용자 **ID** 그룹**)** > **Identity Groups(ID** 그룹**)** > **User Identity Groups(**사용자 **ID** 그룹**)** > **Add(**추가**)** 페이지에 액세스하여 사용자 ID 그룹을 생성할 수도 있습니다.

단계 2 Name(이름) 및 Description(설명) 필드에 값을 입력합니다. Name(이름) 필드에 입력할 수 있는 문자는 공백, # $ & ' ( ) * + - . / @ _입니다.

단계 3 **Submit(**제출**)**을 클릭합니다.

관련 항목

사용자 ID 그룹, 521 페이지

사용자 ID 그룹 내보내기

Cisco ISE에서는 로컬에 구성된 사용자 ID 그룹을 csv 파일 형식으로 내보낼 수 있습니다.

단계 1 **Administration(**관리**) > Identity Management(ID** 관리**) > Groups(**그룹**) > Identity Groups(ID** 그룹**) > User Identity Groups(**사용자 **ID** 그룹**)**를 선택합니다.

단계 2 내보낼 사용자 ID 그룹에 해당하는 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 3 **OK(**확인**)**를 클릭합니다.

사용자 ID 그룹 가져오기

Cisco ISE에서는 사용자 ID 그룹을 csv 파일 형식으로 가져올 수 있습니다.

단계 1 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Identity Groups(ID** 그룹**)** > **User Identity Groups(**사용자 **ID** 그룹**)**를 선택합니다.

단계 2 가져오기 파일에 사용할 템플릿을 가져오려면 **Generate a Template(**템플릿 생성**)**을 클릭합니다.

단계 3 쉼표로 구분된 텍스트 파일에서 네트워크 액세스 사용자를 가져오려면 Import(가져오기)를 클릭합니다.

단계 4 새 사용자 ID 그룹을 추가하는 동시에 기존 사용자 ID 그룹을 업데이트하려면 **Overwrite existing data with new data(**새 데이터로 기존 데이터 덮어쓰기**)** 확인란을 선택합니다.

단계 5 **Import(**가져오기**)**를 클릭합니다.

단계 6 변경사항을 Cisco ISE 데이터베이스에 저장하려면 **Save(**저장**)**를 클릭합니다.

엔드포인트 ID 그룹 설정

다음 표에서는 엔드포인트 그룹을 생성하는 데 사용할 수 있는 Endpoint Identity Groups(엔드포인트 ID 그룹) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Identity Management(ID** 관리**) > Groups(**그룹**) > Endpoint Identity Groups(**엔드포인트 **ID** 그룹**)**입니다.

표 *60:* 엔드포인트 *ID* 그룹 설정

필드 이름	사용 지침
Name(이름**)**	생성할 엔드포인트 ID 그룹의 이름을 입력합니다.
Description(설명**)**	생성할 엔드포인트 ID 그룹에 대한 설명을 입력합니다.
Parent Group(부모 그룹**)**	새로 생성하는 엔드포인트 ID 그룹을 연결할 엔드포인트 ID 그룹을 **Parent Group(**부모 그룹**)** 드롭다운 목록에서 선택합니다.

관련 항목

엔드포인트 ID 그룹에서 그룹화되어 식별된 엔드포인트, 755 페이지
엔드포인트 ID 그룹 생성, 755 페이지

최대 동시 세션 수 구성

최적의 성능을 위해 동시 사용자 세션 수를 제한할 수 있습니다. 사용자 레벨 또는 그룹 레벨에서 제한을 설정할 수 있습니다. 최대 사용자 세션 구성에 따라 세션 수가 사용자에게 적용됩니다.

ISE 노드당 각 사용자의 최대 동시 세션 수를 구성할 수 있습니다. 이 제한을 초과하는 세션은 거부됩니다.

단계 1 **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Max Sessions(**최대 세션 수**) > User(**사용자**)**를 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- **Maximum Sessions per User(**사용자당 최대 세션 수**)** 필드에 각 사용자에게 허용되는 최대 동시 세션 수를 입력합니다.

  또는

- 사용자가 무제한 세션을 사용하도록 하려면 **Unlimited Sessions(**무제한 세션**)** 확인란을 선택합니다. 이 옵션은 기본적으로 선택되어 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

최대 세션 수가 사용자 레벨과 그룹 레벨에서 모두 구성된 경우 더 작은 값이 우선합니다. 예를 들어 사용자의 최대 세션 값이 10으로 설정되어 있고 사용자가 속한 그룹의 최대 세션 값이 5로 설정된 경우 사용자는 최대 5개의 세션만 사용할 수 있습니다.

그룹의 최대 동시 세션 수

ID 그룹의 최대 동시 세션 수를 구성할 수 있습니다.

때때로 그룹의 일부 사용자가 모든 세션을 사용하고 있을 수 있습니다. 이 경우 세션 수가 이미 구성된 최대 값에 도달했으므로 다른 사용자의 새 세션 생성 요청이 거부됩니다. Cisco ISE에서는 그룹에 있는 각 사용자의 최대 세션 제한을 구성할 수 있습니다. 특정 ID 그룹에 속한 각 사용자는 동일한 그룹의 다른 사용자가 연 세션 수에 관계없이 세션 제한보다 많은 세션을 열 수 없습니다. 특정 사용자의 세션 제한을 계산할 때 사용자당 전역 세션 제한, 사용자가 속한 ID 그룹당 세션 제한, 그룹의 사용자당 세션 제한 중 가장 낮은 구성 값이 우선합니다.

ID 그룹의 최대 동시 세션 수를 구성하려면 다음을 수행하십시오.

단계 **1** **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Max Sessions(**최대 세션 수**) > Group(**그룹**)**을 선택합니다.

구성된 모든 ID 그룹이 나열됩니다.

단계 **2** 편집할 그룹 옆에있는 Edit(편집) 아이콘을 클릭하고 다음 값을 입력합니다.

- 해당 그룹에 허용되는 최대 동시 세션 수. 그룹의 최대 세션 수가 100으로 설정된 경우, 해당 그룹의 모든 멤버가 설정한 모든 세션의 총 개수는 100개를 초과할 수 없습니다.

  참고 그룹 레벨 세션 제한은 그룹 계층 구조에 따라 적용됩니다.

- 해당 그룹의 각 사용자에 허용되는 최대 동시 세션 수. 이 옵션은 그룹의 최대 세션 수를 재정의합니다.

그룹의 최대 동시 세션 수 또는 그룹 내 사용자의 최대 동시 세션 수를 Unlimited(무제한)로 설정하려면 **Max Sessions for Group/Max Sessions for User for Group(**그룹의 최대 세션 수/그룹 내 사용자의 최대 세션 수**)** 필드를 비워두고 체크 표시 아이콘을 클릭한 다음 Save(저장)를 클릭합니다. 기본적으로 이 두 값은 모두 Unlimited(무제한)로 설정됩니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

카운터 시간 제한 구성

동시 사용자 세션에 대한 시간 초과 값을 구성할 수 있습니다.

단계 **1** **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Max Sessions(**최대 세션 수**) > Counter Time Limit(**카운터 시간 제한**)**를 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- **Unlimited(**무제한**)**: 세션의 시간 초과 또는 시간 제한을 설정하지 않으려면 이 확인란을 선택합니다.
- **Delete sessions after(**다음 시간 초과 후 세션 삭제**)**: 동시 세션의 시간 초과 값을 분, 시간 또는 일 단위로 입력할 수 있습니다. 세션이 시간 제한을 초과하면 Cisco ISE는 카운터에서 세션을 삭제하고 세션 수를 업데이트하여 새 세션을 허용합니다. 세션이 시간 제한을 초과해도 사용자는 로그아웃되지 않습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

RADIUS Live Logs(RADIUS 라이브 로그) 창에서 세션 수를 재설정할 수 있습니다. Identity(ID), Identity Group(ID 그룹) 또는 Server(서버) 열에 표시된 Actions(작업) 아이콘을 클릭하여 세션 수를 재설정합니다. 세션을 재설정하면 카운터에서 세션이 삭제됩니다(이에 따라 새 세션 사용 가능). 카운터에서 세션이 삭제되어도 사용자의 연결은 끊어지지 않습니다.

계정 비활성화 정책

Cisco ISE는 사용자 또는 관리자를 인증하거나 쿼리하는 동안 **Administration(**관리**) > Identity Management(ID** 관리**) > Settings(**설정**) > User Authentication Settings(**사용자 인증 설정**)** 창에서 전역 계정 비활성화 정책 설정을 확인한 다음 컨피그레이션에 따라 결과를 인증하거나 반환합니다.

Cisco ISE는 다음의 3가지 정책을 확인합니다.

- 지정된 날짜(yyyy-mm-dd)를 초과하는 사용자 계정 비활성화: 지정된 날짜에 사용자 계정을 비활성화합니다. 그러나 **Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**) > Account Disable Policy(**계정 비활성화 정책**)**에 구성되어 있는 개별 네트워크 액세스 사용자에 대한 계정 비활성화 정책 설정이 전역 설정보다 우선적으로 적용됩니다.
- Disable user account after *n* days of account created or last enable(계정 생성 후 또는 마지막 활성화 후 n일 시점에 사용자 비활성화): 계정 생성 이후 또는 계정이 활성 상태였던 마지막 날짜 이후 특정 기간(일)이 지나면 사용자 계정을 비활성화합니다. **Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**) > Status(**상태**)**에서 사용자 상태를 확인할 수 있습니다.
- Disable accounts after n days of inactivity(*n*일 동안 비활성 상태 후 계정 비활성화): 구성된 연속 기간(일) 동안 인증되지 않은 관리자 및 사용자 계정을 비활성화합니다.

Cisco Secure ACS에서 Cisco ISE로 마이그레이션할 때, Cisco Secure ACS에서 네트워크 액세스 사용자에 대해 지정된 계정 비활성화 정책 설정은 Cisco ISE로 마이그레이션됩니다.

개별 사용자 계정 비활성화

Cisco ISE에서는 관리 사용자가 지정한 날짜가 사용자 레벨에서 초과되는 경우 각 개별 사용자의 사용자 계정을 비활성화할 수 있습니다.

단계 **1** **Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID)> Users(**사용자**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하여 새 사용자를 생성하거나 기존 사용자 옆에 있는 확인란을 선택하고 **Edit(**편집**)**를 클릭하여 기존 사용자 세부정보를 편집합니다.

단계 **3** **Disable account if the date exceeds(**날짜가 초과되는 경우 계정 비활성화**)** 확인란을 선택하고 날짜를 선택합니다.

이 옵션을 사용하면 구성된 날짜가 초과될 때 사용자 계정을 비활성화할 수 있습니다. 필요에 따라 서로 다른 사용자에 대해 서로 다른 만료 날짜를 구성할 수 있습니다. 이 옵션은 각 개별 사용자의 전역 컨피그레이션을 무효화합니다. 구성된 날짜는 현재 시스템 날짜일 수도 있고 이후의 날짜일 수도 있습니다.

참고 현재 시스템 날짜 이전의 날짜는 입력할 수 없습니다.

단계 **4** 개별 사용자에 대한 계정 비활성화 정책을 구성하려면 **Submit(**제출**)**을 클릭합니다.

전역적으로 사용자 계정 비활성화

특정 날짜, 계정 생성 또는 마지막 액세스 날짜 며칠 후, 계정이 비활성화되고 며칠 후 사용자 계정을 비활성화할 수 있습니다.

단계 **1** **Administration(**관리**) > Identity Management(ID** 관리**) > Settings(**설정**) > User Authentication Settings(**사용자 인증 설정**) > Account Disable Policy(**계정 비활성화 정책**)**를 선택합니다.

단계 **2** 다음 작업 중 하나를 수행합니다.

- **Disable account if date exceeds(**날짜가 초과되는 경우 계정 비활성화**)** 확인란을 선택하고 적절한 날짜를 yyyy-mm-dd 형식으로 선택합니다. 이 옵션을 사용하면 구성된 날짜가 지나고 사용자 계정을 비활성화할 수 있습니다. 사용자 레벨에서 **Disable account if date exceeds(**날짜가 초과되는 경우 계정 비활성화**)** 설정은 이 전역 컨피그레이션보다 우선합니다.
- **Disable account after n days of account creation or last enable(**계정 생성 또는 마지막 활성화 **n**일 후 계정 비활성화**)** 확인란을 선택하고 기간(일)을 입력합니다. 이 옵션을 사용하면 계정 생성 날짜 또는 마지막 액세스 날짜가 지정한 기간(일)을 초과하면 사용자 계정을 비활성화할 수 있습니다. 관리자는 비활성화된 사용자 계정을 수동으로 활성화할 수 있으며, 이후 일 수는 자동으로 재설정됩니다.
- **Disable account after n days of inactivity(n**일 동안 비활성 상태였던 계정 비활성화**)** 확인란을 선택하고 기간(일)을 입력합니다. 이 옵션을 사용하면 계정이 지정한 기간(일) 동안 비활성 상태일 때 사용자 계정이 비활성화됩니다.

단계 **3** 전역 계정 비활성화 정책을 구성하려면 **Submit(**제출**)**을 클릭합니다.

내부 및 외부 **ID** 소스

ID 소스는 사용자 정보를 저장하는 데이터베이스입니다. Cisco ISE는 ID 소스의 사용자 정보를 사용하여 인증 시 사용자 자격 증명을 검증합니다. 사용자 정보에는 그룹 정보 및 사용자와 연관된 기타 속성이 포함됩니다. ID 소스에서 사용자 정보를 추가 편집 및 삭제할 수 있습니다.

Cisco ISE는 내부 및 외부 ID 소스를 지원합니다. 두 소스를 모두 사용하여 스폰서 및 게스트 사용자를 인증할 수 있습니다.

내부 **ID** 소스

Cisco ISE에는 사용자 정보를 저장하는 데 사용할 수 있는 내부 사용자 데이터베이스가 있습니다. 내부 사용자 데이터베이스의 사용자는 내부 사용자라고 합니다. Cisco ISE에는 모든 디바이스 및 해당 디바이스에 연결되는 엔드포인트 관련 정보를 저장하는 내부 엔드포인트 데이터베이스도 있습니다.

외부 **ID** 소스

Cisco ISE에서는 사용자 정보가 포함된 외부 ID 소스를 구성할 수 있습니다. Cisco ISE는 인증을 위한 사용자 정보를 얻기 위해 외부 ID 소스에 연결합니다. 외부 ID 소스에는 Cisco ISE 서버 및 인증서 인증 프로파일의 인증서 정보도 포함됩니다. Cisco ISE는 외부 ID 소스와 통신하기 위해 인증 프로토콜을 사용합니다.

내부 사용자에 대한 정책을 구성할 때 다음 사항에 유의하십시오.

- 내부 ID 저장소에 대해 내부 사용자를 인증하도록 인증 정책을 구성합니다.
- 다음 옵션을 선택하여 내부 사용자 그룹에 대한 권한 부여 정책을 구성합니다.

  `Identitygroup.Name EQUALS User Identity Groups: Group_Name`

다음 표에는 인증 프로토콜과 해당 프로토콜에서 지원하는 외부 ID가 나와 있습니다.

표 ***61:*** 인증 프로토콜 및 지원되는 외부 ***ID*** 소스

프로토콜(인증 유형)	내부 데이터베이스	**Active Directory**	**LDAP**	**RADIUS** 토큰 서버 또는 **RSA**	**REST**	**ODBC**
EAP-GTC, PAP(일반 텍스트 비밀번호)	예	예	예	예	예	예
MS-CHAP 비밀번호 해시: MSCHAPv1/v2 EAP-MSCHAPv2(EAP, EAP-FAST, EAP-TTLS 또는 TEAP의 내부 방법) LEAP	예	예	아니요	아니요	아니요	예
EAP-MD5 CHAP	예	아니요	아니요	아니요	아니요	예

프로토콜(인증 유형)	내부 데이터베이스	Active Directory	LDAP	RADIUS 토큰 서버 또는 RSA	REST	ODBC
EAP-TLS PEAP-TLS (인증서 검색) 참고 TLS 인증(EAP-TLS 및 PEAP-TLS)에 ID 소스가 필요하지는 않지만 선택적으로 권한 부여 정책 조건에 대해 추가할 수 있습니다.	아니요	예	예	아니요	아니요	아니요

자격 증명은 외부 데이터 소스 연결 유형 및 사용된 기능에 따라 다르게 저장됩니다.

- Active Directory 도메인에 조인할 때(패시브 ID용이 아님) 조인하는 데 사용되는 자격 증명은 저장되지 않습니다. Cisco ISE는 AD 컴퓨터 계정이 없는 경우 이를 생성하고 해당 계정을 사용하여 사용자를 인증합니다.
- LDAP 및 패시브 ID의 경우 외부 데이터 소스에 연결하는 데 사용되는 자격 증명을 사용하여 사용자를 인증합니다.

외부 ID 소스 생성

Cisco ISE는 Active Directory LDAP, RADIUS 토큰 및 RSA SecurID 서버와 같은 외부 ID 소스에 연결하여 인증 및 권한 부여를 위한 사용자 정보를 가져올 수 있습니다. 외부 ID 소스에는 인증서 기반 인증에 필요한 인증서 인증 프로파일도 포함되어 있습니다.

참고 인증된 사용자 ID를 수신하고 공유할 수 있는 패시브 ID 서비스를 사용하려면 추가 패시브 ID 서비스 제공자, 596 페이지의 내용을 참조하십시오.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **Identity Management(ID 관리)** > **External Identity Sources(외부 ID 소스)**를 선택합니다.

단계 2 다음 옵션 중 하나를 선택합니다.

- 인증서 기반 인증의 경우 **Certificate Authentication Profile(인증서 인증 프로파일)**을 선택합니다.
- 외부 ID 소스로 Active Directory에 연결하려는 경우 **Active Directory**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 Active Directory, 540 페이지를 참조하십시오.
- LDAP ID 소스를 추가하려는 경우 **LDAP**를 선택합니다. 자세한 내용은 LDAP, 640 페이지를 참조하십시오.
- RADIUS 토큰 서버를 추가하려는 경우 **RADIUS** 토큰을 선택합니다. 자세한 내용은 RADIUS 토큰 ID 소스, 665 페이지를 참조하십시오.
- RSA SecurID 서버를 추가하려는 경우 **RSA SecurID**를 선택합니다. 자세한 내용은 RSA ID 소스, 672 페이지를 참조하십시오.
- Oracle Access Manager 등의 IdP(Identity Provider)를 추가하려는 경우 **SAML Id Provider(SAML ID 제공자)**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 SAMLv2 ID 제공자, 679 페이지를 참조하십시오.
- 소셜 로그인(예: Facebook 등)을 외부 ID 소스로 추가하려면 **Social Login(소셜 로그인)**을 선택합니다. 자세한 내용은 셀프 등록 게스트의 소셜 로그인, 371 페이지을(를) 참조하십시오.

외부 ID 저장소 비밀번호에 대해 내부 사용자 인증

Cisco ISE에서는 외부 ID 저장소 비밀번호에 대해 내부 사용자를 인증할 수 있습니다. Cisco ISE는 **Administration(관리)** > **Identity Management(ID 관리)** > **Identities(ID)** > **Users(사용자)** 창에서 내부 사용자에 대해 비밀번호 ID 저장소를 선택하는 옵션을 제공합니다. 관리자는 **Users(사용자)** 창에서 사용자를 추가하거나 편집하는 동안 Cisco ISE 외부 ID 소스 목록에서 ID 저장소를 선택할 수 있습니다. 내부 사용자의 기본 비밀번호 ID 저장소는 내부 ID 저장소입니다. Cisco Secure ACS 사용자의 경우 Cisco Secure ACS에서 Cisco ISE로 마이그레이션하는 중과 마이그레이션한 후에 비밀번호 ID 저장소가 동일하게 유지됩니다.

Cisco ISE는 비밀번호 유형에 대해 다음과 같은 외부 ID 저장소를 지원합니다.

- Active Directory
- LDAP
- ODBC
- RADIUS 토큰 서버
- RSA SecurID 서버

참고 현재 설계에 따라 외부 ID 저장소에 대해 인증이 수행되면 권한 부여 정책에서 내부 사용자 ID 그룹 이름을 구성할 수 없습니다. 권한 부여에 내부 사용자 ID 그룹을 사용하려면 내부 사용자 ID 저장소에 대해 인증하도록 인증 정책을 구성해야 하며 사용자 컨피그레이션에서 내부 또는 외부의 비밀번호 유형을 선택해야 합니다.

인증서 인증 프로파일

각 프로파일에 대해 보안 주체 사용자 이름으로 사용해야 하는 인증서 필드와 인증서의 이진 비교를 사용할지 여부를 지정해야 합니다.

인증서 인증 프로파일 추가

EAP-TLS(Extensible Authentication Protocol-Transport Layer Security) 인증서 기반 인증 방법을 사용하려는 경우 인증서 인증 프로파일을 생성해야 합니다. Cisco ISE는 기존 사용자 이름 및 비밀번호 방법을 통해 인증을 수행하는 대신 클라이언트로부터 받은 인증서를 서버의 인증서와 비교하여 사용자의 신뢰성을 확인합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Certificate Authentication Profile(**인증서 인증 프로파일**)** > **Add(**추가**)**를 선택합니다.

단계 **2** 인증서 인증 프로파일의 이름과 설명(선택 사항)을 입력합니다.

단계 **3** 드롭다운 목록에서 ID 저장소를 선택합니다.

기본 인증서 확인 시에는 ID 소스가 필요하지 않습니다. 인증서에 대해 이진 비교 확인을 수행하려면 ID 소스를 선택해야 합니다. ID 소스로 Active Directory를 선택하는 경우에는 주체 이름과 일반 이름 및 대체 주체 이름(모든 값)을 사용하여 사용자를 조회할 수 있습니다.

단계 **4** **Certificate Attribute(**인증서 속성**)** 또는 **Any Subject or Alternative Name Attributes in the Certificate(**인증서의 모든 주체 또는 대체 이름 속성**)**에서 ID 사용 여부를 선택합니다. 이 ID는 로그와 조회에서 사용됩니다.

Any Subject or Alternative Name Attributes in the Certificate(인증서의 모든 주체 또는 대체 이름 속성**)**를 선택하면 Active Directory UPN이 로그의 사용자 이름으로 사용되며 인증서의 모든 주체 이름 및 대체 이름을 사용하여 사용자를 조회합니다. 이 옵션은 Active Directory를 ID 소스로 선택하는 경우에만 사용할 수 있습니다.

단계 **5** **Match Client Certificate Against Certificate In Identity Store(ID** 저장소의 인증서와 클라이언트 인증서 일치 여부 확인**)**을 수행할 경우를 선택합니다. 인증서 일치 여부를 확인하려면 ID 소스(LDAP 또는 Active Directory)를 선택해야 합니다. Active Directory를 선택하는 경우 모호한 ID를 확인하기 위한 용도로만 인증서 일치 여부를 확인하도록 선택할 수 있습니다.

- **Never(**안 함**)**: 이 옵션을 선택하면 이진 비교를 수행하지 않습니다.
- **Only to resolve identity ambiguity(ID** 모호성만 해결**)**: 이 옵션을 선택하면 모호한 ID가 발견되는 경우에 한해 Active Directory의 계정에 대한 인증서와 클라이언트 인증서의 이진 비교를 수행합니다. 인증서의 ID 이름과 일치하는 Active Directory 계정이 여러 개 발견된 경우를 예로 들 수 있습니다.
- **Always perform binary comparison(**항상 이진 비교 수행**)**: 이 옵션을 선택하면 ID 저장소(Active Directory 또는 LDAP)의 계정에 대한 인증서와 클라이언트 인증서의 이진 비교를 항상 수행합니다.

단계 **6** **Submit(**제출**)**을 클릭하여 인증서 인증 프로파일을 추가하거나 변경사항을 저장합니다.

외부 ID 소스로서의 Active Directory

Cisco ISE는 사용자, 머신, 그룹 및 속성과 같은 리소스에 액세스하기 위한 외부 ID 소스로 Microsoft Active Directory를 사용합니다. Active Directory의 사용자 및 머신 인증을 통해 Active Directory에 나열된 사용자 및 디바이스에만 네트워크에서 액세스할 수 있습니다.

ISE 커뮤니티 리소스

AD 자격 증명을 사용하는 ISE 관리 포털 액세스 컨피그레이션 예

Active Directory에서 지원되는 인증 프로토콜 및 기능

Active Directory에서는 일부 프로토콜과 함께 Active Directory 사용자 비밀번호를 변경하여 사용자 및 머신 인증과 같은 기능을 지원합니다. 다음 표에는 Active Directory에서 지원되는 인증 프로토콜과 각 기능이 나와 있습니다.

표 ***62: Active Directory***에서 지원되는 인증 프로토콜

인증 프로토콜	기능
EAP-FAST 및 비밀번호 기반 PEAP(Protected Extensible Authentication Protocol)	사용자 및 머신 인증, 내부 MS-CHAPv2 및 EAP-GTC 방법과 함께 EAP-FAST 및 PEAP를 사용하여 비밀번호를 변경할 수 있는 기능 포함
PAP(Password Authentication Protocol)	사용자 및 머신 인증
MS-CHAPv1(Microsoft Challenge Handshake Authentication Protocol Version 1)	사용자 및 머신 인증
MS-CHAPv2(Microsoft Challenge Handshake Authentication Protocol Version 2)	사용자 및 머신 인증
EAP-GTC(Extensible Authentication Protocol-Generic Token Card)	사용자 및 머신 인증

인증 프로토콜	기능
EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)	• 사용자 및 머신 인증 • 그룹 및 속성 검색 • 이진 인증서 비교
EAP-FAST-TLS(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling-Transport Layer Security)	• 사용자 및 머신 인증 • 그룹 및 속성 검색 • 이진 인증서 비교
PEAP-TLS(Protected Extensible Authentication Protocol-Transport Layer Security)	• 사용자 및 머신 인증 • 그룹 및 속성 검색 • 이진 인증서 비교
LEAP(Lightweight Extensible Authentication Protocol)	사용자 인증

권한 부여 정책에 사용할 **Active Directory** 속성 및 그룹 검색

Cisco ISE는 Active Directory에서 권한 부여 정책 규칙에 사용할 사용자 또는 머신 속성 및 그룹을 검색합니다. 이러한 속성은 Cisco ISE 정책에 사용될 수 있으며 사용자 또는 머신의 권한 부여 수준을 결정합니다. 성공적인 인증이 이루어지고 나면 Cisco ISE는 사용자 및 머신 Active Directory 속성을 검색하고 인증과 관계없는 권한 부여를 위한 속성도 검색할 수 있습니다.

Cisco ISE는 외부 ID 저장소의 그룹을 사용하여 사용자 또는 컴퓨터에 권한을 할당(예: 사용자를 스폰서 그룹에 매핑하기 위해)할 수 있습니다. Active Directory에서 그룹 멤버십에 대한 다음 제한 사항에 유의해야 합니다.

- 정책 규칙 조건은 사용자 또는 컴퓨터의 기본 그룹, 사용자 또는 컴퓨터가 직접 멤버인 그룹 또는 간접(중첩된) 그룹 중 하나를 참조할 수 있습니다.
- 사용자 또는 컴퓨터의 계정 도메인 외부에 있는 도메인 로컬 그룹은 지원되지 않습니다.

참고 Active Directory 속성, msRadiusFramedIPAddress의 값을 IP 주소로 사용할 수 있습니다. 인증 프로파일에 이 IP 주소를 포함하여 NAS(Network Access Server)로 전송할 수 있습니다. msRADIUSFramedIPAddress 속성은 IPv4 주소만 지원합니다. 사용자 인증 시 사용자에 대해 가져오는 msRadiusFramedIPAddress 속성 값은 IP 주소 형식으로 변환됩니다.

속성 및 그룹은 가입 지점별로 검색되고 관리됩니다. 이는 권한 부여 정책에 사용(먼저 가입 지점을 선택한 다음 속성 선택)됩니다. 권한 부여의 경우 범위에 따라 속성 또는 그룹을 정의할 수 없지만 인증 정책에 범위를 사용할 수는 있습니다. 인증 정책에 범위를 사용하는 경우 사용자는 한 가입 지점

을 통해 인증되지만 속성 및/또는 그룹은 사용자의 계정 도메인에 대한 신뢰 경로를 가진 다른 가입 지점을 통해 인증될 수 있습니다. 인증 도메인을 사용하여 인증 도메인에서 범위가 하나인 두 가입 지점이 겹치는 문제가 발생하지 않도록 할 수 있습니다.

참고 다중 가입 포인트 컨피그레이션의 권한 부여 프로세스 중에 Cisco ISE는 특정 사용자가 발견될 때까지만 권한 부여 정책에 나열된 순서대로 가입 포인트를 검색합니다. 사용자가 발견되면 가입 포인트에서 사용자에게 할당된 속성 및 그룹을 사용해 권한 부여 정책을 평가합니다.

참고 사용 가능한 Active Directory 그룹의 최대 수에 대한 Microsoft의 제한을 참고해 주십시오. http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

규칙에 특수 문자(예: /, !, @, \, #, $, %, ^, &, *, (,), _, + 또는 ~)를 가진 Active Directory 그룹 이름이 포함되면 권한 부여 정책이 실패하게 됩니다.

관리자 사용자 이름에 $ 문자가 포함되어 있으면 Active Directory를 통한 관리자 로그인이 실패할 수 있습니다.

명시적 **UPN** 사용

Active Directory의 UPN(User-Principal-Name) 속성과 사용자 정보를 일치시킬 때 모호성을 줄이려면 명시적 UPN을 사용하도록 Active Directory를 구성해야 합니다. 두 사용자의 *sAMAccountName* 값이 동일한 경우 암시적 UPN을 사용하면 모호한 결과가 생성 될 수 있습니다.

Active Directory에서 명시적 UPN을 설정하려면 **Advanced Tuning(**고급 조정**)** 페이지를 열고 *REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN* 속성을 1로 설정합니다.

부울 속성 지원

Cisco ISE는 Active Directory 및 LDAP ID 저장소에서 부울 속성 검색을 지원합니다.

Active Directory 또는 LDAP에 대한 디렉토리 속성을 구성하는 동안 부울 속성을 구성할 수 있습니다. 이러한 속성은 Active Directory 또는 LDAP 인증 시 검색됩니다.

부울 속성은 정책 규칙 조건을 구성하는 데 사용할 수 있습니다.

부울 속성 값은 Active Directory 또는 LDAP 서버에서 문자열 유형으로 가져옵니다. Cisco ISE는 부울 속성에 대해 다음 값을 지원합니다.

부울 속성	지원되는 값
True(참)	t, T, true, TRUE, True, 1
거짓	f, F, false, FALSE, False, 0

참고 부울 속성에 대한 속성 대체는 지원되지 않습니다.

부울 속성(예: msTSAllowLogon)을 문자열 유형으로 구성하는 경우 Active Directory 또는 LDAP 서버 내 속성의 부울 값이 Cisco ISE의 문자열 속성에 대해 설정됩니다. 속성 유형을 부울로 변경하거나 수동으로 속성을 부울 유형으로 추가할 수 있습니다.

인증서 기반 인증을 위한 **Active Directory** 인증서 검색

Cisco ISE는 EAP-TLS 프로토콜을 사용하는 사용자 및 머신 인증을 위해 인증서 검색을 지원합니다. Active Directory의 사용자 또는 머신 기록는 이진 데이터 유형의 인증서 속성을 포함합니다. 이 인증서 속성에는 하나 이상의 인증서가 포함될 수 있습니다. Cisco ISE는 이 속성을 userCertificate로 식별하며 이 속성에 대해 다른 이름을 구성하는 것을 허용하지 않습니다. Cisco ISE는 이 인증서를 검색하여 이진 비교를 수행하는 데 사용합니다.

인증서 인증 프로파일에 따라 Active Directory에서 인증서를 검색하는 데 사용할 사용자를 조회하기 위해 사용자 이름(예: SAN(Subject Alternative Name) 또는 일반 이름)을 가져오는 필드가 결정됩니다. Cisco ISE가 인증서를 검색한 후에는 이 인증서와 클라이언트 인증서의 이진 비교를 수행합니다. 여러 인증서가 검색되면 Cisco ISE는 인증서를 비교하여 일치하는 항목을 확인합니다. 일치하는 인증서가 발견되면 사용자 또는 머신 인증이 통과됩니다.

Active Directory 사용자 인증 프로세스 플로우

사용자를 인증하거나 쿼리하는 경우 Cisco ISE는 다음을 확인합니다.

- MS-CHAP 및 PAP 인증에서는 사용자가 비활성화, 잠금 또는 만료되었거나 로그온 시간을 벗어났는지 확인하고 이러한 조건 중 어느 것이든 충족하는 경우 인증이 실패합니다.
- EAP-TLS 인증에서는 사용자가 비활성화 또는 잠금되었는지 확인하고 조건 중 어느 것이든 충족하는 경우 인증이 실패합니다.

Azure Active Directory를 사용하여 사용자를 인증하기 위한 리소스 소유자 비밀번호 인증서 플로우 구성

주의 Cisco ISE의 ROPC(Resource Owner Password Credentials) 플로우는 제어되는 도입 기능입니다. 이 기능은 프로덕션 환경에서 사용하기 전에 테스트 환경에서 철저하게 테스트하는 것이 좋습니다.

ROPC(Resource Owner Password Credentials)는 클라우드 기반 ID 제공자가 있는 네트워크에서 Cisco ISE가 권한 부여 및 인증을 수행할 수 있도록 하는 OAuth 2.0 권한 부여 유형입니다.

Cisco ISE는 ROPC 플로우를 사용하여 클라우드 기반 ID 소스로 사용자의 자격 증명을 검증합니다. ROPC 플로우는 일반 텍스트 인증 프로토콜을 지원합니다.

Cisco ISE는 현재 ROPC 플로우를 통해 Azure Active Directory를 지원합니다.

Azure Active Directory에서 리소스 소유자 비밀번호 자격 증명 플로우를 위한 애플리케이션 구성

단계 **1** Azure 포털에 로그인합니다.

단계 **2** 상단 내비게이션 바에서 **Directory+Application(**디렉토리+애플리케이션**)** 필터 아이콘을 클릭합니다. ROPC 사용 애플리케이션을 추가해야 할 Azure Active Directory 테넌트를 선택합니다.

단계 **3** 검색 창을 사용하여 **App Registrations(**앱 등록**)**를 찾아 선택합니다.

단계 **4** **+ New Registration(+** 새 등록**)**을 클릭합니다.

단계 **5** 표시되는 **Register an Application(**애플리케이션 등록**)** 창에서 **Name(**이름**)** 필드에 이 앱의 의미 있는 이름을 입력합니다.

단계 **6** **Supported account types(**지원되는 어카운트 유형**)** 영역에서 **Accounts in this organizational directory only(**이 조직 디렉토리에 있는 어카운트만**)**를 클릭합니다.

단계 **7** **Register(**등록**)**를 클릭합니다.

단계 **8** 표시되는 새 창의 왼쪽 메뉴 창에서 **Certificates & Secrets(**인증서 및 암호**)**를 클릭합니다.

단계 **9** **Client Secrets(**클라이언트 암호**)** 영역에서 **+ New Client Secret(+** 새 클라이언트 암호**)**을 클릭합니다.

단계 **10** **Add a Client Secret(**클라이언트 암호 추가**)** 대화 상자에서 **Description(**설명**)** 필드에 설명을 입력합니다.

단계 **11** **Expiry(**만료**)** 영역에서 **Never(**만료되지 않음**)**를 클릭합니다.

단계 **12** **Add(**추가**)**를 클릭합니다.

단계 **13** 클립보드에 복사 아이콘을 클릭하여 공유 암호를 복사합니다. Cisco ISE에서 ROPC 플로우를 구성할 때 이 값이 필요합니다.

단계 **14** 왼쪽 메뉴 창에서 **Overview(**개요**)**를 클릭하고, ROPC 플로우를 구성할 때 Cisco ISE에서 사용할 다음 값을 복사합니다.

- 애플리케이션(클라이언트) ID
- 디렉토리(테넌트) ID입니다

단계 **15** 이 애플리케이션에 대한 ROPC 플로우를 활성화하려면 왼쪽 메뉴 창에서 **Authentication(**인증**)**을 클릭합니다. **Advanced Settings(**고급 설정**)** 영역에서 토글 버튼이 **Yes(**예**)**로 설정되어 있는지 확인합니다.

단계 **16** 앱에 그룹 클레임을 추가하려면 왼쪽 메뉴 창에서 **Token Configuration(**토큰 컨피그레이션**)**을 클릭합니다.

단계 **17** **+ Add Groups Claim(+** 그룹 클레임 추가**)**을 클릭합니다.

단계 **18** **Edit Groups Claim(**그룹 클레임 편집**)** 대화 상자에서 **Security groups(**보안 그룹**)** 확인란을 선택합니다.

단계 **19** **Save(**저장**)**를 클릭합니다.

단계 **20** API 사용을 활성화하려면 왼쪽 메뉴 창에서 **API Permissions(API** 권한**)**를 클릭합니다.

단계 **21** **+ Add A Permission(+** 권한 추가**)**를 클릭합니다.

단계 **22** **Microsoft APIs** 영역에서 **Microsoft Graph**를 클릭합니다.

단계 **23** **Application Permissions(**애플리케이션 권한**)**를 클릭합니다.

단계 **24** **Group(**그룹**)** 드롭다운 영역에서 **Group.Read.All** 확인란을 선택합니다.

단계 **25** **Add Permissions(**권한 추가**)**를 클릭합니다.

단계 **26** **Grant Admin Consent for <user>(**<사용자>에 대해 관리자 동의 부여**)**를 클릭한 다음 **Yes(**예**)**를 클릭합니다.

Cisco ISE에서 리소스 소유자 비밀번호 자격 증명 플로우 구성

시작하기 전에

Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다. **DigiCert Global Root G2**가 신뢰할 수 있는 인증서 목록에 표시되는지 확인합니다.

이 인증서가 신뢰할 수 있는 인증서 저장소에 없는 경우 PEM 형식의 공용 루트 인증서 DigiCert Global Root G2를 Cisco ISE 신뢰할 수 있는 인증서 저장소로 가져옵니다.

https://www.digicert.com/kb/digicert-root-certificates.htm을 참고하십시오.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **REST ID Store Settings(REST ID** 저장소 설정**)**를 선택합니다.

단계 **2** **Enabled(**활성화됨**)**를 클릭한 다음 **Submit(**제출**)**을 클릭합니다.

단계 **3** ISE 노드에서 다음 CLI 명령을 통해 REST 인증 서비스의 상태를 확인합니다.

```
show application status ise
```

REST Auth Service running(REST 인증 서비스 실행 중**)** 메시지가 응답에 표시되면 REST ID 저장소 설정이 정상적으로 활성화된 것입니다. 이제 ROPC 플로우 구성을 진행할 수 있습니다.

단계 **4** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **REST(ROPC)**를 선택합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** 표시되는 새 창의 **Name(**이름**)** 필드에 값을 입력합니다.

단계 **7** **REST Identity Provider(REST ID** 제공자**)** 드롭다운 목록에서 구성할 ID 소스를 선택합니다.

단계 **8** 이전 작업 시 Azure Active Directory를 구성할 때 저장한 정보에서 **Client ID(**클라이언트 **ID)**, **Client Secret(**클라이언트 암호**)** 및 **Tenant ID(**테넌트 **ID)** 필드에 필요한 값을 입력합니다.

단계 **9** **Test Connection(**연결 테스트**)**을 클릭하여 Cisco ISE가 선택한 ID 소스에 연결할 수 있는지 확인합니다.

단계 **10** **Load Groups(**그룹 로드**)**를 클릭하여 연결된 ID 소스에서 사용자 그룹을 가져옵니다. 그런 다음 **Groups(**그룹**)** 드롭다운 목록에서 특정 그룹을 선택할 수 있습니다.

단계 **11** (선택 사항) 사용자 이름으로 Azure Active Directory 테넌트 사용자를 인증하려면 **Username Suffix(**사용자 이름 접미사**)** 필드에 값을 입력합니다.

예를 들어 사용자의 Azure Active Directory UPN(User Private Name)이 *example@myTest.onMicrosoft.com*인 경우 접미사는 구분 기호이고 도메인 이름은 *@myTest.onMicrosoft.com*입니다.

단계 **12** **Submit(**제출**)**을 클릭합니다.

Active Directory 다중 도메인 포리스트 지원

Cisco ISE는 다중 도메인 포리스트를 사용하는 Active Directory를 지원합니다. 각 포리스트 내의 Cisco ISE는 단일 도메인에 연결되지만 Cisco ISE가 연결된 도메인과 다른 도메인 간에 신뢰 관계가 설정된 경우에는 Active Directory 포리스트의 다른 도메인에 있는 리소스에 액세스할 수 있습니다.

Active Directory 디렉토리 서비스를 지원하는 Windows Server 운영체제 목록은 Cisco Identity Services Engine 릴리스 정보를 참고해 주십시오.

참고 Cisco ISE는 네트워크 주소 변환기 뒤에 배치되고 NAT(Network Address Translation) 주소를 사용하는 Microsoft Active Directory 서버를 지원하지 않습니다.

Active Directory와 Cisco ISE 통합을 위한 사전 요건

이 섹션에서는 Cisco ISE와 통합되도록 Active Directory를 구성하는 데 필요한 수동 단계를 설명합니다. 그러나 대부분의 경우 Cisco ISE가 Active Directory를 자동으로 구성할 수 있습니다. Active Directory와 Cisco ISE 통합의 사전 요건은 다음과 같습니다.

- Active Directory 도메인 구성을 변경하는 데 필요한 AD 도메인 관리자 자격 증명이 있어야 합니다.
- CIsco ISE에 슈퍼 관리자 또는 시스템 관리자 권한이 있어야 합니다.
- NTP(Network Time Protocol) 서버 설정을 사용하여 Cisco ISE 서버와 Active Directory 간에 시간을 동기화합니다. Cisco ISE CLI에서 NTP 설정을 구성할 수 있습니다.
- Cisco ISE는 양방향 신뢰를 가지지 않거나 서로 간에 신뢰가 없는 여러 Active Directory 도메인에 연결될 수 있습니다. 특정 조인 포인트에서 다른 도메인을 쿼리하는 경우, 액세스해야 하는 사용자 및 머신 정보가 있는 다른 도메인과 조인 포인트 간에 신뢰 관계가 존재해야 합니다. 신뢰 관계가 존재하지 않는다면 신뢰할 수 없는 도메인에 다른 조인 포인트를 생성해야 합니다. 신뢰 관계 설정에 대한 자세한 내용은 Microsoft Active Directory 설명서를 참고해 주십시오.
- Cisco ISE를 가입시키는 도메인에 Cisco ISE에서 액세스할 수 있으며 작동 가능한 글로벌 카탈로그 서버가 하나 이상 있어야 합니다.

다양한 작업을 수행하는 데 필요한 **Active Directory** 계정 권한

가입 작업	탈퇴 작업	**Cisco ISE** 머신 계정
가입 작업에는 다음 계정 권한이 필요합니다. • Active Directory 검색(Cisco ISE 머신 계정이 있는지 확인하는 용도) • 도메인에 Cisco ISE 머신 계정 생성(머신 계정이 아직 없는 경우) • 새 머신 계정에서 속성 설정(예: Cisco ISE 머신 계정 비밀번호, SPN, dnsHostname) 가입 작업을 수행하기 위해서는 반드시 도메인 관리자가 아니어도 됩니다.	탈퇴 작업에는 다음 계정 권한이 필요합니다. • Active Directory 검색(Cisco ISE 머신 계정이 있는지 확인하는 용도) • 도메인에서 Cisco ISE 머신 계정 제거 강제 탈퇴를 수행하는 경우(비밀번호 없이 탈퇴) 도메인에서 머신 계정이 제거되지 않습니다.	Active Directory 연결과의 통신에 사용되는 ISE 머신 계정에는 다음 권한이 필요합니다. • 비밀번호 변경 • 연락된 사용자 및 머신에 해당하는 사용자 및 머신 개체 읽기 • 정보(예: 신뢰할 수 있는 도메인, 대체 UPN 접미사 등)를 확인하기 위한 Active Directory 쿼리 • tokenGroups 속성 읽기 Active Directory에서 머신 계정을 미리 생성할 수 있습니다. SAM 이름이 Cisco ISE 어플라이언스 호스트 이름과 일치하는 경우 가입 작업 중에 해당 항목을 찾아서 재사용해야 합니다. 여러 가입 작업이 수행되는 경우 Cisco ISE 내에서 가입별로 하나씩 여러 머신 계정이 유지 관리됩니다.

참고 가입 또는 탈퇴 작업에 사용하는 자격 증명은 Cisco ISE에 저장되지 않습니다. 새로 생성된 Cisco ISE 머신 계정 자격 증명만 저장됩니다.

Microsoft Active Directory에서 네트워크 액세스**: SAM**에 대한 원격 호출을 허용하는 클라이언트 제한 보안 정책이 수정되었습니다. 따라서 Cisco ISE는 15일마다 머신 계정 암호를 업데이트하지 못할 수 있습니다. 머신 계정 암호가 업데이트되지 않으면 Cisco ISE는 Microsoft Active Directory를 통해 더 이상 사용자를 인증하지 않습니다. 이 이벤트에 대해 알 수 있도록 Cisco ISE 대시보드에서 **AD: ISE password update failed(AD: ISE** 비밀번호 업데이트 실패**)** 경보를 받게 됩니다.

사용자는 보안 정책을 통해 로컬 SAM(Security Accounts Manager) 데이터베이스 및 Microsoft Active Directory의 사용자 및 그룹을 열거할 수 있습니다. Cisco ISE가 머신 계정 비밀번호를 업데이트할 수 있도록 하려면 Microsoft Active Directory의 컨피그레이션이 정확한지 확인하십시오. 영향을 받는 Windows 운영체제 및 Windows 서버 버전, 네트워크에 미치는 영향 및 필요한 변경 사항에 대한 자세한 내용은 다음을 참조하십시오.

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

통신을 위해 열어 두어야 하는 네트워크 포트

프로토콜	포트(원격-로컬)	대상	인증 여부	참고
DNS(TCP/UDP)	49,152 이상의 난수	DNS 서버/AD 도메인 컨트롤러	아니요	—
MSRPC	445	도메인 컨트롤러	예	—
Kerberos(TCP/UDP)	88	도메인 컨트롤러	예(Kerberos)	MS AD/KDC
LDAP(TCP/UDP)	389	도메인 컨트롤러	예	—
LDAP(GC)	3268	글로벌 카탈로그 서버	예	—
NTP	123	NTP 서버/도메인 컨트롤러	아니요	—
IPC	80	구축의 다른 ISE 노드	예(RBAC 자격 증명 사용)	—

DNS 서버

DNS 서버를 구성하는 경우 주의해야 할 사항은 다음과 같습니다.

- Cisco ISE에 구성한 DNS 서버는 사용자가 사용하려는 도메인에 대한 정방향 및 역방향 DNS 쿼리를 모두 확인할 수 있어야 합니다.
- DNS 회귀는 지연을 유발하고 심각한 성능 저하를 유발할 수 있으므로, 권한 있는 DNS 서버를 통해 Active Directory 기록 확인하는 것이 좋습니다.
- 모든 DNS 서버는 추가 사이트 정보 사용 여부와 관계없이 DC, GC 및 KDC에 대한 SRV 쿼리에 응답할 수 있어야 합니다.
- Cisco에서는 성능 향상을 위해서는 서버 IP 주소를 SRV 응답에 추가하는 것을 권장합니다.
- DNS 서버를 사용하여 공용 인터넷에 쿼리하면 안 됩니다. 이 경우 알 수 없는 이름을 확인해야 할 때 네트워크 관련 정보가 유출될 수 있습니다.

외부 ID 소스로서의 Active Directory 구성

Easy Connect나 PassiveID 작업 센터 등의 기능에 대한 구성의 일부로, Active Directory를 외부 ID 소스로 구성합니다 . 이러한 기능에 관한 자세한 내용은 Easy Connect, 583 페이지 및 PassiveID 작업 센터 , 587 페이지 항목을 참조하십시오.

Active Directory를 외부 ID 소스로 구성하는 경우 다음을 확인해 주십시오.

- Microsoft Active Directory 서버가 네트워크 주소 변환기 뒤에 배치되지 않고 NAT(Network Address Translation) 주소를 갖지 않습니다.
- 가입 작업에 사용되는 Microsoft Active Directory 계정이 유효하며 Change Password on Next Login(다음 로그인 시 비밀번호 변경)을 사용하여 구성되지 않았습니다.
- ISE에 슈퍼 관리자 또는 시스템 관리자 권한이 있습니다.

참고 Cisco ISE가 Active Directory에 연결되어 있을 때 작동 문제가 발생한다면 **Operations(**작업**)** > **Reports(**보고서**)**의 AD Connector 운영 보고서를 참조하십시오.

다음 작업을 수행하여 Active Directory를 외부 ID 소스로 구성해야 합니다.

1. Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입, 549 페이지
2. 인증 도메인 구성, 555 페이지
3. Active Directory 사용자 그룹 구성, 556 페이지
4. Active Directory 사용자 및 머신 속성 구성, 556 페이지
5. (선택사항) 비밀번호 변경, 머신 인증 및 머신 액세스 제한 설정 수정, 557 페이지

Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입

시작하기 전에

Cisco ISE 노드가 NTP 서버, DNS 서버, 도메인 컨트롤러 및 전역 카탈로그 서버가 있는 네트워크와 통신할 수 있는지 확인합니다. 도메인 진단 도구를 실행하여 이러한 매개변수를 확인할 수 있습니다.

Active Directory에 더해 Passive ID Work Center(패시브 ID 작업 센터)의 에이전트, 시스템 로그, SPAN 및 엔드포인트 프로브까지 사용하려면 조인 포인트를 생성해야 합니다.

Active Directory와 통합할 때 IPv6을 사용하려면 관련 ISE 노드에 대해 IPv6 주소를 구성했는지 확인해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하고 **Active Directory Join Point Name(Active Directory** 가입 포인트 이름**)** 설정에서 도메인 이름과 ID 저장소 이름을 입력합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

새로 생성하는 가입 포인트를 도메인에 가입시킬지를 묻는 팝업 메시지가 표시됩니다. 가입 포인트를 도메인에 즉시 가입시키려면 **Yes(**예**)**를 클릭합니다.

No(아니오**)**를 클릭하고 컨피그레이션을 저장하면 Active Directory 도메인 컨피그레이션이 (기본 및 보조 정책 서비스 노드에) 전역적으로 저장되지만 Cisco ISE 노드가 도메인에 가입되지는 않습니다.

단계 **4** 새로 생성한 Active Directory 가입 포인트 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭하거나 왼쪽의 탐색창에서 새 Active Directory 가입 포인트를 클릭합니다. 모든 Cisco ISE 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 표이 표시됩니다.

단계 **5** 3단계를 진행하는 도중 가입 포인트가 도메인에 가입되지 않은 경우 관련 Cisco ISE 노드 옆의 확인란을 선택하고 **Join(**가입**)**을 클릭하여 Cisco ISE 노드를 Active Directory 도메인에 가입시킵니다.

컨피그레이션을 저장한 경우에도 이 작업을 명시적으로 수행해야 합니다. 단일 작업에서 도메인에 여러 Cisco ISE 노드를 가입시키려면 모든 가입 작업에 사용할 계정의 사용자 이름 및 비밀번호가 같아야 합니다. 각 Cisco ISE 노드를 가입시키는 데 필요한 사용자 이름 및 비밀번호가 다른 경우에는 각 Cisco ISE 노드에 대해 가입 작업을 개별적으로 수행해야 합니다.

단계 **6** **Join Domain(**도메인 가입**)** 대화 상자에서 Active Directory 사용자 이름 및 비밀번호를 입력합니다.

Store credentials(자격 증명 저장**)**는 되도록 선택하는 것이 좋습니다. 관리자의 사용자 이름이나 비밀번호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다.

가입 작업에 사용되는 사용자는 도메인 자체에 있어야 합니다. 사용자가 다른 도메인이나 하위 도메인에 있는 경우에는 jdoe@acme.com과 같이 UPN 표기법으로 사용자 이름을 표기해야 합니다.

단계 **7** (선택 사항) **Specify Organizational Unit(**조직 단위 지정**)** 확인란을 선택합니다.

CN=Computers,DC=someDomain,DC=someTLD 이외의 특정 조직 단위에 Cisco ISE 노드 머신 계정을 배치하려는 경우 이 확인란을 선택해야 합니다. Cisco ISE는 지정된 조직 단위에 머신 계정을 생성하거나, 머신 계정이 이미 있는 경우 이 위치로 이동합니다. 조직 단위를 지정하지 않으면 Cisco ISE에서는 기본 위치를 사용합니다. 값은 완전한 DN(Distinguished Name) 형식으로 지정해야 합니다. 구문은 Microsoft 지침을 따라야 합니다. /'+,;=<> 줄 바꿈, 공백, 캐리지 리턴 등의 특수 예약 문자는 백슬래시(\)로 이스케이프 처리해야 합니다. 예를 들면 OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ 및 Workstations,DC=someDomain,DC=someTLD와 같습니다. 머신 계정이 이미 생성된 경우에는 이 확인란을 선택하지 않아도 됩니다. Active Directory 도메인에 가입한 후 머신 계정의 위치를 변경할 수도 있습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

Active Directory 도메인에 가입시킬 노드를 두 개 이상 선택할 수 있습니다.

가입 작업이 실패하면 오류 메시지가 나타납니다. 각 노드에 대한 오류 메시지를 클릭하면 해당 노드의 상세 로그를 확인할 수 있습니다.

참고 조인이 완료되면 Cisco ISE는 자신의 AD 그룹과 대응하는 보안 식별자(SID)를 업데이트합니다. Cisco ISE는 SID 업데이트 프로세스를 자동으로 시작합니다. 이 프로세스를 완료할 수 있는지를 확인해야 합니다.

참고 DNS 서비스(SRV) 레코드가 없으면 Cisco ISE를 Active Directory 도메인에 가입시키지 못할 수도 있습니다. 가입시키려는 도메인에 대해 도메인 컨트롤러가 해당 SRV 레코드를 보급하지 않기 때문입니다. 문제 해결 관련 정보는 다음 Microsoft Active Directory 설명서를 참고해 주십시오.

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

참고 ISE에는 최대 200개의 도메인 컨트롤러만 추가할 수 있습니다. 제한을 초과하면 "Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200(<DC FQDN> 생성 오류 - DC 수가 허용된 최대 200개를 초과)" 오류가 표시됩니다.

다음에 수행할 작업

Active Directory 사용자 그룹 구성, 556 페이지

인증 도메인을 구성합니다.

도메인 컨트롤러 추가

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 창에서 **Active Directory**를 선택합니다.

단계 **2** 생성한 Active Directory 가입 포인트 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다. 모든 Cisco ISE 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 표이 표시됩니다.

단계 **3** 참고 Passive Identity(패시브 ID) 서비스용으로 새 DC(Domain Controller)를 추가하려면 해당 DC의 로그인 자격 증명이 필요합니다.

PassiveID(패시브 ID) 탭으로 이동하여 **Add DCs(DC** 추가**)**를 클릭합니다.

단계 **4** 모니터링을 위해 조인트 포인트에 추가할 도메인 컨트롤러 옆의 확인란을 선택하고 **OK (**확인)를 클릭합니다. 도메인 컨트롤러는 PassiveID(패시브 ID) 탭의 Domain Controller(도메인 컨트롤러) 목록에 표시됩니다.

단계 **5** 도메인 컨트롤러를 구성합니다.

a) 도메인 컨트롤러에 체크 표시하고 **Edit(**수정**)**를 클릭합니다. **Edit Item(**항목 수정**)** 화면이 나타납니다.

b) 선택 사항으로, 다른 도메인 컨트롤러 필드를 수정합니다. .

c) WMI 프로토콜을 선택했다면 **Configure(**구성**)**를 클릭하여 WMI를 자동으로 구성하고 **Test(**테스트**)**를 클릭하여 연결을 테스트합니다.

DC 페일오버 메커니즘은 페일오버 시 DC가 선택되는 순서를 지정하는 DC 우선 순위 목록을 기반으로 관리됩니다. DC가 오프라인 상태이거나 오류 때문에 연결할 수 없다면 우선 순위 목록에서 우선 순위가 감소합니다. DC가 다시 온라인 상태가 되면 우선 순위 목록에서 우선 순위가 조정(중가)됩니다.

참고 Cisco ISE는 인증 플로우에 대해 읽기 전용 도메인 컨트롤러를 지원하지 않습니다.

패시브 ID용 MSRPC 프로토콜

Cisco ISE 릴리스 3.0부터는 패시브 ID에 MS-Eventing API 또는 MSRPC(Microsoft Remote Procedure Call) 프로토콜을 사용할 수 있습니다. MSRPC 프로토콜은 Cisco ISE에서 노드 통신을 설정하고 노드 간 하트비트를 모니터링하는 데 사용됩니다. WMI 프로토콜에 추가로 이 옵션을 사용할 수 있습니다.

MSRPC 프로토콜은 Cisco ISE 또는 Cisco ISE-PIC가 여러 도메인 컨트롤러에서 이벤트를 수집하거나 모니터링할 때 신뢰할 수 있는 메커니즘을 제공합니다. 또한 Active Directory 도메인 컨트롤러 사용자 로그온 이벤트의 레이턴시를 줄입니다.

Cisco ISE 3.0 이상의 경우 MSRPC가 기본 프로토콜입니다. 기본 에이전트가 설치된 서버에 장애가 발생할 경우 보조 에이전트가 활성화되어 도메인 컨트롤러를 모니터링할 수 있도록 MSPRC의 고가용성 기능을 위해 기본 에이전트와 보조 에이전트를 활성화하는 것이 좋습니다.

에이전트를 생성하는 동안 MSPRC에 독립형 옵션을 사용하도록 선택할 수도 있습니다. 그러나 독립형 에이전트를 사용하는 경우 에이전트 장애 발생 시 보조 에이전트로 대체되지 않으므로 DC 이벤트를 모니터링할 수 없습니다.

Cisco ISE 2.x에서 3.0 버전으로 업그레이드하는 동안 멤버 서버가 기존 에이전트로 업데이트되는 경우 **Agents(**에이전트**)** 창의 **Version(**버전**)** 열에 에이전트 버전이 2.0.0.1로 표시됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Passive ID(**패시브 **ID)** > **Providers(**제공자**)** > **Agents(**에이전트**)** .

MSRPC용 에이전트 구축

시작하기 전에

Passive Identity Service를 활성화해야 합니다. 방법은 다음과 같습니다.

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택하고 구축 노드 옆의 확인란을 선택합니다. **Edit(**편집**)**를 클릭합니다. **Edit Node(**노드 편집**)** 창에서 **Enable Passive Identity Service(**패시브 **ID** 서비스 활성화**)** 확인란을 선택하고 **Save(**저장**)**를 클릭합니다.

Cisco ISE-PIC GUI에서 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택하고 구축 노드 옆의 확인란을 선택합니다. **Edit(**편집**)**를 클릭합니다. **Edit Node(**노드 편집**)** 창에서 **Enable Passive Identity Service(**패시브 **ID** 서비스 활성화**)** 확인란을 선택하고 **Save(**저장**)**를 클릭합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Passive ID(**패시브 **ID)** > **Providers(**제공자**)** > **Agents(**에이전트**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 새 에이전트를 구축하려면 **Agents(**에이전트**)** 창에서 **Deploy New Agent(**새 에이전트 구축**)**를 클릭하고, 기존 에이전트를 등록하려면 **Register Existing Agents(**기존 에이전트 등록**)**를 클릭합니다.

Register Existing Agent(기존 에이전트 등록**)** 옵션을 선택하면 지원되지 않는 프로토콜로 인해 지원 대상인 등록된 클라이언트의 요청이 삭제될 수 있습니다. 이러한 이벤트에서는 지원되는 프로토콜로 Cisco ISE 클라이언트를 구성해야 합니다.

단계 **4** **Name(**이름**)** 필드에 에이전트 이름을 입력합니다.

단계 **5** **Host FQDN(**호스트 **FQDN)** 필드에 호스트 FQDN URL을 입력합니다.

단계 **6** **User Name(**사용자 이름**)**과 **Password(**비밀번호**)**를 입력합니다.

단계 **7** **Protocol(**프로토콜**)** 드롭다운 목록에서 **MSRPC**를 선택합니다.

단계 **8** **High Availability Settings(**고가용성 설정**)** 섹션에서 **Primary(**기본**)**를 클릭합니다.

기본 에이전트가 성공적으로 구축된 후에는 **High Availability Settings(**고가용성 설정**)** 섹션에서 **Secondary(**보조**)** 옵션을 선택해 위의 단계를 반복하여 보조 에이전트를 구축해야 합니다. 보조 에이전트를 구축하는 동안 **Primary Agent(**기본 에이전트**)** 드롭다운 목록에서, 구성된 기본 에이전트를 선택합니다.

단계 **9** **Deploy(**구축**)**를 클릭합니다.

기본 에이전트로 도메인 컨트롤러 매핑

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Passive ID(**패시브 **ID)** > **Providers(**제공자**)** > **Active Directory**.

단계 **2** **Active Directory** 창에서 **Add(**추가**)**를 클릭합니다.

단계 **3** **Connection(**연결**)** 섹션에서 도메인 컨트롤러의 **Join Point Name(**조인 포인트 이름**)** 및 **Active Directory Domain(Active Directory** 도메인**)**을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

다음 메시지가 표시됩니다.

```
Would you like to Join all ISE Nodes to this Active Directory Domain?(모든 ISE 노드를 이 Active Directory 도메인에 조인하시겠습니까)
```

단계 **5** **Yes(**예**)**를 클릭하여 모든 ISE 노드를 조인시킵니다.

단계 **6** **Join Domain(**도메인 조인**)** 팝업 창에서 **AD User name(AD** 사용자 이름**)** 및 **Password(**비밀번호**)**를 입력합니다.

단계 **7** **Ok(**확인**)**를 클릭합니다.

단계 **8** **PassiveID(**패시브 **ID)** 탭을 클릭합니다.

단계 **9** **PassiveID Domain Controller(PassiveID** 도메인 컨트롤러**)** 창에서 매핑하려는 ISE 도메인 옆의 확인란을 클릭합니다.

다중 DC 매핑의 경우 **Use Existing Agent(**기존 에이전트 사용**)** 옵션에서 기존 에이전트를 선택할 수 있습니다.

단계 **10** **Edit(**편집**)**를 클릭합니다.

단계 **11** **Host FQDN(**호스트 **FQDN)** 필드에 호스트 FQDN URL을 입력합니다.

단계 **12** **AD User Name(AD** 사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 AD 자격 증명을 입력합니다.

단계 **13** **Protocol(**프로토콜**)** 드롭다운 목록에서 **Agent(**에이전트**)**를 선택합니다.

단계 **14** **Agent(**에이전트**)** 드롭다운 목록에서 해당 에이전트(고가용성을 위한 **Primary(**기본**)** 또는 **Standalone(**독립형**)**)를 선택합니다.

단계 **15** **Save(**저장**)**를 클릭합니다.

Dashboard(대시보드**)**에서 에이전트 매핑 상태, 도메인 컨트롤러를 모니터링하는 에이전트 및 에이전트 역할을 검토할 수 있습니다. (이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Overview(**개요**)**.)

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Sessions(**라이브 세션**)**를 선택하여 도메인 컨트롤러 이벤트 로그를 확인합니다.

패시브 ID용 WMI 구성

시작하기 전에

AD 도메인 컨피그레이션을 변경하려면 Active Directory 도메인 관리자 자격 증명이 있어야 합니다. **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**에서 이 노드에 대해 패시브 ID가 활성화되었는지 확인합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** 생성한 Active Directory 가입 포인트 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다. 모든 Cisco ISE 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 표이 표시됩니다.

단계 **3** Passive ID(패시브 ID) 탭으로 이동하여 관련 도메인 컨트롤러 옆에 있는 확인란을 선택하고 **Config WMI(WMI** 구성**)**를 클릭하여 ISE가 선택한 도메인 컨트롤러를 자동으로 구성하게 합니다.
Active Directory 및 도메인 컨트롤러를 수동으로 구성하거나 구성 문제를 해결하는 방법은 Active Directory와 Cisco ISE 통합을 위한 사전 요건 , 546 페이지 항목을 참조하십시오.

Active Directory 도메인 탈퇴

Active Directory 도메인 또는 이 가입 포인트에서 사용자나 머신을 더 이상 인증할 필요가 없으면, Active Directory 도메인에서 탈퇴할 수 있습니다.

명령줄 인터페이스에서 Cisco ISE 애플리케이션 컨피그레이션을 재설정하거나 백업 또는 업그레이드 이후 컨피그레이션을 복원하면 Cisco ISE는 탈퇴 작업을 수행하여 Cisco ISE 노드가 Active Directory 도메인에 이미 가입되어 있는 경우 해당 도메인에서 노드 연결을 끊습니다. 그러나 Cisco ISE 노드 계정은 Active Directory 도메인에서 제거되지 않습니다. 관리 포털에서 Active Directory 자격 증명을 사용하여 탈퇴 작업을 수행하는 것이 좋습니다. 이렇게 하면 Active Directory 도메인에서 노드 계정도 제거되기 때문입니다. Cisco ISE 호스트 이름을 변경할 때도 이 방법을 사용하는 것이 좋습니다.

시작하기 전에

Active Directory 도메인에서는 탈퇴했는데 Active Directory를 인증용 ID 소스로 계속 사용(직접 사용 또는 ID 소스 시퀀스의 일부분으로 사용)하면 인증이 실패할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** 생성한 Active Directory 조인 포인트 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다. 모든 Cisco ISE 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 표이 표시됩니다.

단계 **3** Cisco ISE 노드 옆의 확인란을 선택하고 **Leave(**탈퇴**)**를 클릭합니다.

단계 **4** Active Directory 사용자 이름 및 비밀번호를 입력하고 **OK(**확인**)**를 클릭하여 도메인을 탈퇴시킨 후 Cisco ISE 데이터베이스에서 머신 계정을 제거합니다.

Active Directory 자격 증명을 입력하는 경우 Active Directory 도메인에서 Cisco ISE 노드가 탈퇴되며 Active Directory 데이터베이스에서 Cisco ISE 머신 계정이 삭제됩니다.

참고 Active Directory 데이터베이스에서 Cisco ISE 머신 계정을 삭제하려면 여기서 입력하는 Active Directory 자격 증명에 도메인에서 머신 계정을 제거할 권한이 있어야 합니다.

단계 **5** Active Directory 자격 증명이 없는 경우에는 **No Credentials Available(**사용 가능한 자격 증명 없음**)**을 선택하고 **OK(**확인**)**를 클릭합니다.

Leave domain without credentials(자격 증명을 사용하지 않고 도메인 탈퇴**)** 확인란을 선택하면 기본 Cisco ISE 노드가 Active Directory 도메인에서 탈퇴됩니다. 이 경우에는 Active Directory 관리자가 가입 시 Active Directory에서 생성된 머신 계정을 수동으로 제거해야 합니다.

인증 도메인 구성

Cisco ISE가 가입된 도메인에서는 신뢰 관계가 설정된 다른 도메인을 확인할 수 있습니다. 기본적으로 Cisco ISE는 이러한 신뢰할 수 있는 모든 도메인에 대한 인증을 허용하도록 설정됩니다. Active Directory 구축과의 상호작용을 인증 도메인의 하위 집합으로 제한할 수 있습니다. 인증 도메인을 구성하면 선택한 도메인에 대해서만 인증이 수행되도록 각 가입 포인트에 대해 특정 도메인을 선택할 수 있습니다. 인증 도메인은 가입 포인트에서 신뢰되는 모든 도메인이 아닌 선택한 도메인의 사용자만 인증하도록 Cisco ISE에 명령하므로, 인증 도메인을 사용하는 경우 보안이 향상됩니다. 또한 인증 도메인은 검색 영역, 즉 인커밍 사용자 이름 또는 ID와 일치하는 계정을 검색하는 영역을 제한하므로 인증 요청 처리의 성능과 레이턴시도 개선됩니다. 인커밍 사용자 이름 또는 ID에는 도메인 태그(접두사 또는 접미사)가 포함되어 있지 않아야 합니다. 이러한 이유로 인해 인증 도메인을 구성하는 것이 모범 사례이므로 인증 도메인은 구성하는 것이 좋습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Active Directory** 조인 포인트를 클릭합니다.

단계 **3** **Authentication Domains(**인증 도메인**)** 탭을 클릭합니다.

신뢰할 수 있는 도메인 목록이 포함된 표가 표시됩니다. 기본적으로 Cisco ISE는 신뢰할 수 있는 모든 도메인에 대한 인증을 허용합니다.

단계 **4** 지정된 도메인만 허용하려면 **Use all Active Directory domains for authentication(**인증에 모든 **Active Directory** 도메인 사용**)** 확인란 선택을 취소합니다.

단계 **5** 인증을 허용할 도메인 옆의 확인란을 선택하고 **Enable Selected(**선택 항목 활성화**)**를 클릭합니다. **Authenticate(**인증**)** 열에서 이 도메인의 상태가 예로 변경됩니다.

선택한 도메인을 비활성화할 수도 있습니다.

단계 6 사용할 수 없는 도메인 목록을 보려면 **Show Unusable Domains(**사용할 수 없는 도메인 표시**)**를 클릭합니다. 사용할 수 없는 도메인은 단방향 신뢰, 선택적 인증 등의 이유로 인해 Cisco ISE가 인증에 사용할 수 없는 도메인입니다.

다음에 수행할 작업

Active Directory 사용자 그룹을 구성합니다.

Active Directory 사용자 그룹 구성

Active Directory 사용자 그룹을 구성해야 권한 부여 정책에서 해당 그룹을 사용할 수 있습니다. Cisco ISE는 내부적으로 SID(Security Identifiers)를 사용하여 모호한 그룹 이름 문제를 해결하고 그룹 매핑을 개선합니다. SID를 통해 정확하게 일치하는 그룹을 할당할 수 있습니다.

단계 1 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 2 **Groups(**그룹**)** 탭을 클릭합니다.

단계 3 다음 중 하나를 수행합니다.

a) **Add(**추가**)** > **Select Groups From Directory(**디렉토리에서 그룹 선택**)**를 선택하여 기존 그룹을 선택합니다.

b) **Add(**추가**)** > **Add Group(**그룹 추가**)**을 선택하여 그룹을 수동으로 추가합니다. 그룹 이름과 SID를 모두 입력하거나, 그룹 이름만 입력하고 **Fetch SID(SID** 가져오기**)**를 누를 수 있습니다.

사용자 인터페이스 로그인 시 그룹 이름에 큰따옴표(")를 사용하지 마십시오.

단계 4 그룹을 수동으로 선택하는 경우 필터를 사용하여 그룹을 검색할 수 있습니다. 예를 들어 필터 기준으로 **admin***를 입력하고 **Retrieve Groups(**그룹 검색**)**를 클릭하면 admin으로 시작하는 사용자 그룹을 확인할 수 있습니다. 별표(*) 와일드카드 문자를 입력하여 결과를 필터링할 수도 있습니다. 그룹은 한 번에 500개만 검색할 수 있습니다.

단계 5 권한 부여 정책에서 사용 가능하도록 지정할 그룹 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

단계 6 그룹을 수동으로 추가하도록 선택하는 경우 새 그룹의 이름과 SID를 입력합니다.

단계 7 **OK(**확인**)**를 클릭합니다.

단계 8 **Save(**저장**)**를 클릭합니다.

참고 그룹을 삭제하고 원본과 같은 이름으로 새 그룹을 생성하는 경우에는 **Update SID Values(SID** 값 업데이트**)**를 클릭하여 새로 생성한 그룹에 새 SID를 할당해야 합니다. 업그레이드 후 처음으로 가입하고 나면 SID가 자동으로 업데이트됩니다.

다음에 수행할 작업

Active Directory 사용자 속성을 구성합니다.

Active Directory 사용자 및 머신 속성 구성

Active Directory 사용자 및 머신 속성을 구성해야 권한 부여 정책의 조건에서 해당 속성을 사용할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Attributes(**속성**)** 탭을 클릭합니다.

단계 **3** **Add(**추가**)** > **Add Attribute(**속성 추가**)**를 클릭하여 속성을 수동으로 추가하거나 **Add(**추가**)** > **Select Attributes From Directory(**디렉터리에서 속성 선택**)**를 선택하여 디렉터리에서 속성 목록을 선택합니다.

Cisco ISE에서는 속성 유형 IP를 수동으로 추가할 때 사용자 인증에 IPv4 또는 IPv6 주소를 사용하도록 AD를 구성할 수 있습니다.

단계 **4** 디렉터리에서 속성을 추가하도록 선택하는 경우 **Sample User or Machine Account(**샘플 사용자 또는 머신 계정**)** 필드에 사용자의 이름을 입력하고 **Retrieve Attributes(**속성 검색**)**를 클릭하여 사용자에 대한 속성 목록을 가져옵니다. 예를 들어 관리자 속성 목록을 가져오려면 **administrator(**관리자**)**를 입력합니다. 별표(*) 와일드카드 문자를 입력하여 결과를 필터링할 수도 있습니다.

참고 예시 사용자 이름을 입력할 때는 Cisco ISE에 연결되는 Active Directory 도메인에 속한 사용자를 선택해야 합니다. 머신 속성을 얻고자 예시 머신을 선택할 때는 머신 이름 앞에 'host/'를 붙이거나 SAM$ 형식을 사용해야 합니다. 예를 들어 host/myhost를 사용할 수 있습니다. 속성을 검색할 때 표시되는 예제 값은 설명을 위해서만 제공되는 것이며 저장되지 않습니다.

단계 **5** 선택하려는 Active Directory의 속성 옆에 있는 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

단계 **6** 속성을 수동으로 추가하도록 선택하는 경우 새 속성의 이름을 입력합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

비밀번호 변경, 머신 인증 및 머신 액세스 제한 설정 수정

시작하기 전에

Active Directory 도메인에 Cisco ISE를 가입시켜야 합니다. 자세한 내용은 Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입, 549 페이지를 참고하십시오.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** Cisco ISE 노드 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다 .

단계 **3** **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

단계 **4** 비밀번호 변경, 머신 인증 및 MAR(Machine Access Restrictions) 설정을 필요한 대로 수정합니다.

단계 **5** 인증 또는 쿼리 중에 사용자의 다이얼인 권한을 확인하려면 **Enable dial-in check(**다이얼인 확인 활성화**)** 확인란을 선택합니다. 다이얼인 권한이 거부되는 경우 확인 결과에 따라 인증이 거부될 수 있습니다.

단계 **6** 인증 또는 쿼리 중에 서버가 사용자를 다시 호출하게 하려면 **Enable callback check for dial-in clients(**다이얼인 클라이언트용 콜백 확인 활성화**)** 확인란을 선택합니다. 서버에서 사용하는 IP 주소 또는 전화 번호는 발신자나 네트워크 관리자가 설정할 수 있습니다. 확인 결과는 RADIUS 응답의 장치로 반환됩니다.

단계 **7** 일반 텍스트 인증에 Kerberos를 사용하려는 경우 **Use Kerberos for Plain Text Authentications(**일반 텍스트 인증에 **Kerberos** 사용**)** 확인란을 선택합니다. 기본 및 권장 옵션은 MS-RPC입니다.

MAR(머신 액세스 제한) 캐시

애플리케이션 서비스를 수동으로 중지하면 Cisco ISE는 MAR 캐시 콘텐츠, 호출 스테이션 ID 목록 및 해당하는 타임스탬프를 로컬 디스크의 파일에 저장합니다. 런타임 서비스를 실수로 재시작하는 경우 Cisco ISE는 인스턴스의 MAR 캐시 엔트리를 저장하지 않습니다. Cisco ISE는 애플리케이션 서비스가 재시작될 때 캐시 엔트리 TTL(Time to Live)을 기준으로 하여 로컬 디스크의 파일에서 MAR 캐시 엔트리를 읽습니다. 재시작 후 애플리케이션 서비스가 작동하면 Cisco ISE는 해당 인스턴스의 현재 시간을 MAR 캐시 엔트리 시간과 비교합니다. 현재 시간과 MAR 엔트리 시간 사이의 차이가 MAR 캐시 엔트리 TTL(Time to Live)보다 크면 Cisco ISE는 디스크에서 해당 엔트리를 검색하지 않습니다. 그렇지 않은 경우 Cisco ISE는 해당 MAR 캐시 엔트리를 검색하고 MAR 캐시 엔트리 TTL(Time to Live)을 업데이트합니다.

MAR 캐시를 구성하는 방법

외부 ID 소스에 정의된 Active Directory의 **Advanced Settings(**고급 설정**)** 탭에서 다음 옵션이 선택되었는지 확인합니다.

- **Enable Machine Authentication(**머신 인증 활성화**)**: 머신 인증을 활성화합니다.
- **Enable Machine Access Restriction(**머신 액세스 제한 활성화**)**: 권한 부여 전에 사용자 및 머신 인증을 결합합니다.

MAR 캐시를 권한 부여에 사용하는 방법

권한 부여 정책에서 `WasMachineAuthenticated is True`를 사용합니다. 이 규칙과 자격 증명 규칙을 사용하여 이중 인증을 수행할 수 있습니다. 머신 인증은 AD 자격 증명보다 먼저 수행해야합니다.

System(시스템**) > Deployment(**구축**)** 페이지에서 노드 그룹을 생성 한 경우 MAR Cache Distribution(MAC 캐시 배포)을 활성화합니다. MAR 캐시 배포는 MAR 캐시를 동일한 노드 그룹의 모든 PSN에 복제합니다.

추가 정보

다음 Cisco ISE 커뮤니티 페이지를 참조하십시오.

- https://community.cisco.com/t5/policy-and-access/mar-why-is-it-useful/td-p/3213527
- https://community.cisco.com/t5/policy-and-access/ise-2-1-mar-aging-time-eap-tls/td-p/3209628

관련 항목

외부 ID 소스로서의 Active Directory 구성, 548 페이지

사용자 맞춤화 스키마 구성

시작하기 전에

Active Directory 도메인에 Cisco ISE를 가입시켜야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** 가입 포인트를 선택합니다.

단계 **3** **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

단계 **4** **Schema(**스키마**)** 섹션의 **Schema(**스키마**)** 드롭다운 목록에서 **Custom(**맞춤화**)** 옵션을 선택합니다. 필요에 따라 사용자 정보 속성을 업데이트할 수 있습니다. 이러한 속성은 이름, 성, 이메일, 전화, 지역 등의 사용자 정보를 수집하는 데 사용됩니다.

사전 정의된 속성은 Active Directory 스키마(구축 당시 기본으로 내장된 스키마)에 사용됩니다. 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다.

Active Directory 다중 가입 컨피그레이션 지원

Cisco ISE는 여러 Active Directory 도메인에 대한 다중 가입을 지원합니다. Cisco ISE는 최대 50개의 Active Directory 가입을 지원합니다. Cisco ISE는 양방향 신뢰를 가지지 않거나 서로 간에 신뢰가 없는 여러 Active Directory 도메인에 연결될 수 있습니다. Active Directory 다중 도메인 가입은 각 가입마다 일련의 개별 Active Directory 도메인과 함께 고유한 그룹, 속성 및 권한 부여 정책으로 구성됩니다.

동일한 포리스트에 여러 번 가입할 수 있습니다. 즉, 필요한 경우 동일 포리스트의 여러 도메인에 가입할 수 있습니다.

Cisco ISE는 이제 단방향 신뢰를 통한 도메인 가입을 지원합니다. 이 옵션을 사용하면 단방향 신뢰로 인해 발생하는 권한 문제를 피할 수 있습니다. 신뢰할 수 있는 도메인에 가입하여 양쪽 도메인을 모두 볼 수 있습니다.

- 가입 포인트: Cisco ISE에서 Active Directory 도메인에 대한 각각의 개별적 가입을 가입 포인트라고 합니다. Active Directory 가입 포인트는 Cisco ISE ID 저장소이며 인증 정책에 사용될 수 있습니다. 속성 및 그룹에 대한 사전이 연결되어 있으며, 이는 권한 부여 조건에 사용될 수 있습니다.
- 범위: 함께 그룹화된 Active Directory 가입 포인트의 하위 집합을 범위라고 합니다. 인증 정책에서 인증 결과로 단일 가입 포인트 대신 범위를 사용할 수 있습니다. 범위는 여러 가입 포인트에 대해 사용자를 인증하는 데 사용됩니다. 가입 포인트마다 여러 규칙을 사용하는 대신, 범위를 사용하면 단일 규칙으로 동일한 정책을 생성할 수 있으므로 요청을 처리하는 시간을 절약하고 성능을 높일 수 있습니다. 가입 포인트는 여러 범위로 존재할 수 있습니다. 범위는 ID 소스 시퀀스에 포함될 수 있습니다. 범위에는 사전이 연결되어 있지 않으므로 권한 부여 정책 조건에서 범위를 사용할 수 없습니다.

Cisco ISE를 새로 설치하는 경우 기본적으로 범위가 존재하지 않습니다. 이를 범위 없음 모드라고 합니다. 범위를 추가하면 Cisco ISE가 다중 범위 모드로 진입합니다. 필요한 경우 범위 없음 모드로 복귀할 수 있습니다. 모든 가입 포인트는 Active Directory 폴더로 이동합니다.

- Initial_Scope는 범위 없음 모드에서 추가된 Active Directory 가입 포인트를 저장하는 데 사용되는 암시적 범위입니다. 다중 범위 모드가 활성화되면 모든 Active Directory 가입 포인트가 자동으로 생성된 Initial_Scope로 이동합니다. Initial_Scope의 이름을 변경할 수 있습니다.
- All_AD_Instances는 Active Directory 컨피그레이션에 표시되지 않는 내장형 의사 범위입니다. 이는 정책 및 ID 시퀀스에서 인증 결과로 표시되는 유일한 항목입니다. Cisco ISE에 구성된 모든 Active Directory 가입 포인트를 선택하려는 경우 이 범위를 선택할 수 있습니다.

Active Directory 가입 포인트를 추가할 새 범위 생성

단계 1 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 2 **Scope Mode(**범위 모드**)**를 클릭합니다.
Initial_Scope라는 기본 범위가 생성되며 현재 가입 포인트가 모두 이 스코프에 배치됩니다.

단계 3 범위를 더 생성하려면 **Add(**추가**)**를 클릭합니다.

단계 4 새 범위의 이름과 설명을 입력합니다.

단계 5 **Submit(**제출**)**을 클릭합니다.

ID 다시 쓰기

ID 다시 쓰기는 ID가 외부 Active Directory 시스템으로 전달되기 전에 해당 ID를 조작하도록 Cisco ISE에 지시하는 고급 기능입니다. ID를 원하는 형식으로 변경하는 규칙을 생성하여 도메인 접두사 및/또는 접미사 또는 선택한 다른 추가 마크업을 포함하거나 제외시킬 수 있습니다.

ID 다시 쓰기 규칙은 클라이언트로부터 받은 사용자 이름 또는 호스트 이름에 적용됩니다. 그런 다음 그러한 이름은 주체 검색, 인증 및 권한 부여 쿼리와 같은 작업에 사용되도록 Active Directory로 전달됩니다. Cisco ISE는 조건 토큰과 일치시키고 첫 번째 일치 항목이 발견되면 Cisco ISE는 정책 처리를 중단하고 결과에 따라 ID 문자열을 다시 씁니다.

다시 쓰는 동안 대괄호 [ ]로 묶인 모든 항목(예: [IDENTITY])은 평가 측에서 평가되지 않지만 그 대신 문자열의 해당 위치와 일치하는 문자열이 추가되는 변수입니다. 대괄호가 없는 항목은 평가 측과 규칙을 다시 쓰기 측 모두에서 고정 문자열로 평가됩니다.

다음은 몇 가지 ID 다시 쓰기 사례로, 사용자가 ACME\jdoe를 ID로 입력한다고 가정합니다.

- ID가 **ACME\[IDENTITY]**와 일치하는 경우 **[IDENTITY]**로 다시 씁니다.

  결과는 jdoe가 됩니다. 이 규칙은 모든 사용자 이름에서 ACME 접두사를 제거하도록 Cisco ISE에 지시합니다.

- ID가 **ACME\[IDENTITY]**와 일치하는 경우 **[IDENTITY]@ACME.com**으로 다시 씁니다.

결과는 jdoe@ACME.com이 됩니다. 이 규칙은 접미사 표기법의 접두사 형식 또는 NetBIOS 형식을 UPN 형식으로 변경하도록 Cisco ISE에 지시합니다.

- ID가 **ACME\[IDENTITY]**와 일치하는 경우 **ACME2\[IDENTITY]**로 다시 씁니다.

  결과는 ACME2\jdoe가 됩니다. 이 규칙은 특정 접두사를 가진 모든 사용자 이름을 대체 접두사로 변경하도록 Cisco ISE에 지시합니다.

- ID가 **[ACME]\jdoe.USA**와 일치하는 경우 **[IDENTITY]@[ACME].com**으로 다시 씁니다.

  결과는 jdoe\ACME.com이 됩니다. 이 규칙은 점 뒤의 영역(이 경우, 국가)을 제거하고 올바른 도메인으로 대체하도록 ISE에 지시합니다.

- ID가 **E=[IDENTITY]**와 일치하는 경우 **[IDENTITY]**로 다시 씁니다.

  결과는 jdoe가 됩니다. 이 예제 규칙은 ID를 인증서에서 가져오고, 필드가 이메일 주소이며, 주체별로 검색하도록 Active Directory가 구성된 경우에 생성될 수 있습니다. 이 규칙은 Cisco ISE에 'E='를 제거하도록 지시합니다.

- ID가 **E=[EMAIL],[DN]**과 일치하는 경우 **[DN]**으로 다시 씁니다.

  이 규칙은 인증서 주체를 E=jdoe@acme.com, CN=jdoe, DC=acme, DC=com에서 pure DN, CN=jdoe, DC=acme, DC=com으로 변환합니다. 이 예제 규칙은 ID를 인증서 주체에서 가져오고 DN을 기준으로 사용자를 검색하도록 Active Directory가 구성된 경우에 생성될 수 있습니다. 이 규칙은 이메일 접두사를 제거하고 DN을 생성하도록 Cisco ISE에 지시합니다.

다음은 ID 다시 쓰기 규칙을 작성하는 동안 흔히 하는 몇 가지 실수입니다.

- ID가 **[DOMAIN]\[IDENTITY]**와 일치하는 경우 **[IDENTITY]@DOMAIN.com**으로 다시 씁니다.

  결과는 jdoe@DOMAIN.com이 됩니다. 이 규칙은 규칙 다시 쓰기 측에서 [DOMAIN]이 대괄호 [ ]로 묶이지 않았습니다.

- ID가 **DOMAIN\[IDENTITY]**와 일치하는 경우 **[IDENTITY]@[DOMAIN].com**으로 다시 씁니다.

  여기서는 결과가 다시 jdoe@DOMAIN.com이 됩니다. 이 규칙은 규칙 평가 측 [DOMAIN]이 대괄호 [ ]로 묶이지 않았습니다.

ID 다시 쓰기 규칙은 Active Directory 가입 지점 관점에서 항상 적용됩니다. 인증 정책의 결과로 특정 범위를 선택한 경우에도 각 Active Directory 가입 지점에 다시 쓰기 규칙이 적용됩니다. EAP-TLS가 사용 중인 경우 인증서에서 가져온 ID에도 이러한 다시 쓰기 규칙이 적용됩니다.

ID 재작성 활성화

참고 이 컨피그레이션 작업은 선택 사항입니다. 이 작업을 수행하면 모호한 ID 오류 등의 여러 원인으로 인해 발생할 수 있는 인증 실패를 줄일 수 있습니다.

시작하기 전에

Active Directory 도메인에 Cisco ISE를 가입시켜야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

단계 **3** **Identity Rewrite(ID** 재작성**)** 섹션에서 재작성 규칙을 적용하여 사용자 이름을 수정할지 여부를 선택합니다.

단계 **4** 일치 조건과 재작성 결과를 입력합니다. 표시되는 기본 규칙을 제거하고 요건에 따라 규칙을 입력할 수 있습니다. Cisco ISE는 정책을 순서대로 처리하며, 요청 사용자 이름과 일치하는 첫 번째 조건이 적용됩니다. 일치하는 토큰(대괄호 안의 텍스트)을 사용하여 원래 사용자 이름의 요소를 결과로 전송할 수 있습니다. 일치하는 규칙이 없으면 ID 이름은 변경되지 않고 그대로 유지됩니다. **Launch Test(**테스트 시작**)** 버튼을 클릭하여 재작성 처리를 미리 볼 수 있습니다.

ID 확인 설정

일부 ID 유형에는 접두사 또는 접미사와 같은 도메인 마크업이 포함되어 있습니다. 예를 들어 NetBIOS ID(예: ACME\jdoe) "ACME"는 UPN ID(예: jdoe@acme.com)에서와 마찬가지로 도메인 마크업 접두사이며, "acme.com"은 도메인 마크업 접미사입니다. 도메인 접두사는 조직 내 Active Directory 도메인의 NetBIOS(NTLM) 이름과 일치해야 하고 도메인 접미사는 Active Directory 도메인의 DNS 이름 또는 조직 내 대체 UPN 접미사와 일치해야 합니다. 예를 들어 gmail.com은 Active Directory 도메인의 DNS 이름이 아니므로 jdoe@gmail.com은 도메인 마크업 없이 처리됩니다.

ID 확인 설정을 사용하면 Active Directory 구축에 맞게 보안과 성능 사이에서 균형을 유지하도록 중요한 설정을 구성할 수 있습니다. 이러한 설정을 사용하여 도메인 마크업 없이 사용자 이름 및 호스트 이름에 대한 인증을 조정할 수 있습니다. Cisco ISE가 사용자 도메인을 인식하지 못하는 경우 모든 인증 도메인에서 사용자를 검색하도록 구성할 수 있습니다. 사용자가 한 도메인에서 발견되는 경우에도 Cisco ISE는 ID 모호성이 발생하지 않도록 모든 응답을 기다립니다. 이 프로세스는 도메인 수, 네트워크 레이턴시, 로드 등에 따라 오랜 시간이 소요될 수 있습니다.

ID 확인 문제 방지

인증 중에 사용자 및 호스트에 대한 정규화된 이름(즉, 도메인 마크업이 포함된 이름)을 사용하는 것이 좋습니다. 예를 들어 사용자의 경우 UPN 및 NetBIOS 이름을 사용하고 호스트의 경우 FQDN을 사용합니다. 이는 특히 들어오는 사용자 이름에 대한 여러 Active Directory 계정 일치(예: jdoe는 jdoe@emea.acme.com 및 jdoe@amer.acme.com과 일치함)와 같이 모호성 오류가 자주 발생하는 경우에 중요합니다. 경우에 따라 정규화된 이름을 사용하는 것이 유일한 문제 해결 방법일 수 있습니다. 다른 경우에는 사용자의 고유한 비밀번호를 사용하는 것만으로도 충분할 수 있습니다. 따라서 처음부터 고유 ID를 사용하면 효율성을 높이고 비밀번호 잠금 문제를 줄일 수 있습니다.

ID 확인 설정 구성

참고 이 컨피그레이션 작업은 선택 사항입니다. 이 작업을 수행하면 모호한 ID 오류 등의 여러 원인으로 인해 발생할 수 있는 인증 실패를 줄일 수 있습니다.

시작하기 전에

Active Directory 도메인에 Cisco ISE를 가입시켜야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

단계 **3** **Identity Resolution(ID** 확인**)** 섹션에서 사용자 이름 또는 머신 이름에 대한 ID 확인을 위해 다음 설정을 정의합니다. 이 설정은 사용자 검색 및 인증을 위한 고급 컨트롤을 제공합니다.

첫 번째 설정은 태그가 없는 ID용입니다. 이 경우에는 다음 옵션 중에서 선택할 수 있습니다.

- **Reject the request(**요청 거부**)**: 이 옵션을 사용하는 경우 SAM 이름 등의 도메인 태그가 없는 사용자의 인증이 실패합니다. Cisco ISE가 가입된 모든 글로벌 카탈로그에서 ID를 조회해야 하므로 안전하지 않을 수도 있는 다중 가입 도메인의 경우 이 옵션이 유용합니다. 이 옵션을 선택하면 사용자는 도메인 태그가 있는 이름을 사용해야 합니다.
- **Only search in the "Authentication Domains" from the joined forest(**조인된 포리스트의 "인증 도메인"만 검색**)**: 이 옵션을 사용하는 경우 인증 도메인 섹션에 지정되어 있는 조인 포인트의 포리스트 내 도메인에서만 ID를 검색합니다. 이 옵션은 기본값이며, SAM 계정 이름에 대한 Cisco ISE 1.2의 동작과 동일합니다.
- **Search in all the "Authentication Domains" sections(**모든 "인증 도메인" 섹션 검색**)**: 이 옵션을 사용하는 경우 신뢰할 수 있는 모든 포리스트 내 모든 인증 도메인에서 ID를 검색합니다. 따라서 레이턴시가 길어지고 성능이 저하될 수 있습니다.

Cisco ISE에서 인증 도메인이 구성되어 있는 방법에 따라 적절한 옵션을 선택합니다. 특정 인증 도메인만 선택하는 경우, 즉 두 번째 옵션과 세 번째 옵션을 선택하는 경우에는 해당 도메인만 검색합니다.

Cisco ISE가 "인증 도메인" 섹션에 지정된 컨피그레이션을 준수하기 위해 필요한 모든 GC(Global Catalogs)와 통신할 수 없는 경우에는 두 번째 설정이 사용됩니다. 이 경우에는 다음 옵션 중에서 선택할 수 있습니다.

- **Proceed with available domains(**사용 가능한 도메인으로 인증 진행**)**: 이 옵션을 사용하는 경우 사용 가능한 도메인 중에서 일치 항목을 찾으면 인증이 진행됩니다.
- **Drop the request(**요청 삭제**)**: 이 옵션을 사용하는 경우 ID 확인 과정에서 연결할 수 없거나 사용할 수 없는 도메인이 발견되면 인증 요청이 삭제됩니다.

Active Directory Authentication(인증)용 Test Users(사용자 테스트)

Test User(사용자 테스트) 도구를 사용하여 Active Directory에서 사용자 인증을 확인할 수 있습니다. 그룹과 속성을 가져와 검토할 수도 있습니다. 단일 가입 포인트 또는 범위에 대해 테스트를 실행할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 모든 가입 포인트에서 테스트를 실행하려면 **Advanced Tools(**고급 도구**)** > **Test User for All Join Points(**모든 가입 포인트에 대해 사용자 테스트**)**를 선택합니다.
- 특정 가입 포인트에 대해 테스트를 실행하려면 해당 가입 포인트를 선택하고 **Edit(**편집**)**를 클릭합니다. Cisco ISE 노드를 선택하고 **Test User(**사용자 테스트**)**를 클릭합니다.

단계 **3** Active Directory에서 사용자 또는 호스트의 사용자 이름 및 비밀번호를 입력합니다.

단계 **4** 인증 유형을 선택합니다. Lookup(조회) 옵션을 선택하는 경우에는 3단계에서 비밀번호를 입력하지 않아도 됩니다.

단계 **5** 모든 가입 포인트에 이 테스트를 실행하는 경우 이 테스트를 실행할 Cisco ISE 노드를 선택합니다.

단계 **6** Active Directory에서 그룹과 속성을 검색하고 싶다면 Retrieve Groups and Attributes(그룹과 속성 가져오기) 확인란을 선택합니다.

단계 **7** **Test(**테스트**)**를 클릭합니다.
테스트 작업의 결과 및 단계가 표시됩니다. 이러한 단계를 통해 실패 이유 및 문제 해결 상황을 파악할 수 있습니다.

Active Directory에서 각 처리 단계(인증, 조회 또는 그룹/속성 가져오기)를 수행하는 데 걸린 시간(밀리초)을 볼 수도 있습니다. 작업을 수행한 시간이 임계값을 초과하면 Cisco ISE에서 경고 메시지가 표시됩니다.

Active Directory 컨피그레이션 삭제

Active Directory 외부 ID 소스로 사용하지 않으려는 경우 Active Directory 컨피그레이션을 삭제해야 합니다. 다른 Active Directory 도메인에 가입하려는 경우에는 컨피그레이션을 삭제하지 마십시오. 현재 가입되어 있는 도메인은 그대로 두고 새 도메인에 가입할 수 있습니다.

시작하기 전에

Active Directory 도메인이 남아 있는지 확인합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** 구성되어 있는 Active Directory 옆의 확인란을 선택합니다.

단계 **3** 로컬 노드 상태가 가입되지 않음으로 나열되어 있는지 확인합니다.

단계 **4** **Delete(**삭제**)**를 클릭합니다.

Active Directory 데이터베이스에서 컨피그레이션이 제거되었습니다. 나중에 Active Directory를 사용하려는 경우 유효한 Active Directory 컨피그레이션을 다시 제출하면 됩니다.

노드의 Active Directory 가입 보기

Node View(노드 보기**)** 버튼(**Active Directory** 페이지)을 사용하면 지정된 Cisco ISE 노드에 대한 모든 Active Directory 가입 포인트의 상태나 모든 Cisco ISE 노드의 모든 가입 포인트를 확인할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Node View(**노드 보기**)**를 클릭합니다.

단계 **3** **ISE Node(ISE** 노드**)** 드롭다운 목록에서 노드를 선택합니다.
표에 노드별 Active Directory 상태가 나열됩니다. 구축에 가입 포인트와 Cisco ISE 노드가 여러 개 있는 경우 이 표이 업데이트되는 데 몇 분 정도 걸릴 수 있습니다.

단계 **4** 가입 포인트 **Name(**이름**)** 링크를 클릭하여 해당 Active Directory 가입 포인트로 이동한 후에 다른 특정 작업을 수행합니다.

단계 **5** **Diagnostic Summary(**진단 요약**)** 열에 있는 링크를 클릭하여 **Diagnostic Tools(**진단 도구**)** 페이지로 이동한 후에 특정 문제를 해결합니다. 진단 도구에는 노드당 각 가입 포인트에 대한 최신 진단 결과가 표시됩니다.

Active Directory 문제 진단

Diagnostic Tool(진단 도구)은 모든 Cisco ISE 노드에서 실행되는 서비스입니다. Active Directory 구축을 자동으로 테스트 및 진단할 수 있으며, 테스트 집합을 실행하여 Cisco ISE에서 Active Directory를 사용할 때 기능 또는 성능 오류를 발생시킬 수 있는 문제를 탐지할 수 있습니다.

Cisco ISE는 여러 이유로 Active Directory에 가입하거나 인증하지 못할 수 있습니다. 이 도구를 사용하면 Cisco ISE를 Active Directory에 연결하기 위한 사전 요건을 올바르게 구성할 수 있습니다. 그리고 네트워킹, 방화벽 컨피그레이션, 클록 동기화, 사용자 인증 등의 문제를 탐지할 수 있습니다. 이 도구는 단계별 설명서 방식으로 작동하며, 필요한 경우 중간에 모든 레이어의 문제를 해결할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Advanced Tools(**고급 도구**)** 드롭다운을 클릭하고 **Diagnostic Tools(**진단 도구**)**를 선택합니다.

단계 **3** 진단을 실행할 Cisco ISE 노드를 선택합니다.

Cisco ISE 노드를 선택하지 않으면 모든 노드에서 테스트가 실행됩니다.

단계 **4** 특정 Active Directory 가입 포인트를 선택합니다.

Active Directory 가입 포인트를 선택하지 않으면 모든 가입 포인트에서 테스트가 실행됩니다.

단계 **5** 진단 보고서는 온디맨드 또는 예약 방식으로 실행할 수 있습니다.

- 테스트를 즉시 실행하려면 **Run Tests Now(**지금 테스트 실행**)**를 선택합니다.
- 예약된 간격으로 테스트를 실행하려면 **Run Scheduled Tests(**예약된 테스트 실행**)** 확인란을 선택하여 테스트를 실행할 시작 시간과 간격(시간, 일 또는 주)을 지정합니다. 이 옵션을 활성화하면 모든 진단 테스트가 모든 노드 및 인스턴스에서 실행되며, **Home(**홈**)** 대시보드의 **Alarms(**경보**)** 데슬렛에서 장애가 보고됩니다.

단계 6 **View Test Details(**테스트 세부정보 보기**)**를 클릭하여 Warning(경고) 또는 Failed(장애) 상태의 테스트에 대한 세부 정보를 확인합니다.
이 표을 참조하여 특정 테스트를 다시 실행하고, 실행 중인 테스트를 중지하고, 특정 테스트의 보고서를 확인할 수 있습니다.

Active Directory 디버그 로그 활성화

Active Directory 디버그 로그는 기본적으로 기록되지 않습니다. 구축에서 정책 서비스 페르소나로 지정된 Cisco ISE 노드에 대해 이 옵션을 활성화해야 합니다. Active Directory 디버그 로그를 활성화하는 경우 ISE 성능에 영향을 줄 수 있습니다.

단계 1 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Debug Log Configuration(**디버그 로그 컨피그레이션**)**을 선택합니다.

단계 2 Active Directory 디버그 정보를 가져올 Cisco ISE Policy Service(정책 서비스) 노드 옆의 라디오 버튼을 클릭하고 **Edit(**수정**)**를 클릭합니다.

단계 3 **Active Directory** 라디오 버튼을 클릭하고 **Edit(**수정**)**를 클릭합니다.

단계 4 Active Directory 옆의 드롭다운 목록에서 **DEBUG**를 선택합니다. 여기에는 오류, 경고 및 자세한 정보 표시 로그가 포함됩니다. 전체 로그를 가져오려면 **TRACE**를 선택합니다.

단계 5 **Save(**저장**)**를 클릭합니다.

문제 해결을 위해 Active Directory 로그 파일 가져오기

발생했을 수 있는 문제를 해결하려면 Active Directory 디버그 로그를 다운로드하여 확인합니다.

시작하기 전에

Active Directory 디버그 로깅을 활성화해야 합니다.

단계 1 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)**를 선택합니다.

단계 2 Active Directory 디버그 로그 파일을 가져올 노드를 클릭합니다

단계 3 **Debug Logs(**디버그 로그**)** 탭을 클릭합니다.

단계 4 이 페이지를 스크롤하여 ad_agent.log 파일을 찾습니다. 이 파일을 클릭하여 다운로드합니다.

Active Directory 경보 및 보고서

Cisco ISE는 Active Directory 관련 활동을 모니터링하고 문제를 해결할 수 있는 다양한 경보 및 보고서를 제공합니다.

경보

Active Directory 오류 및 문제에 대해 다음 경보가 트리거됩니다.

- 구성된 네임서버를 사용할 수 없음
- 가입한 도메인 사용 불가능
- 인증 도메인을 사용할 수 없음
- Active Directory 포리스트를 사용할 수 없음
- AD Connector를 다시 시작해야 함
- AD: ISE 계정 비밀번호 업데이트 실패
- AD: 머신 TGT 새로 고침 실패

보고서

다음 두 보고서를 통해 Active Directory 관련 활동을 모니터링할 수 있습니다.

- RADIUS 인증 보고서: 이 보고서에는 Active Directory 인증 및 권한 부여에 대한 세부 단계가 표시됩니다. **Operations(**운영**)** > **Reports(**보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **RADIUS Authentications(RADIUS** 인증**)**에서 이 보고서를 찾을 수 있습니다.
- AD Connector 운영 보고서: AD Connector 운영 보고서는 Cisco ISE 서버 비밀번호 새로 고침, Kerberos 티켓 관리, DNS 쿼리, DC 검색, LDAP 및 RPC 연결 관리 등 AD Connector에서 수행하는 백그라운드 작업 로그를 제공합니다. Active Directory 오류가 발생하는 경우 이 보고서에서 세부 정보를 검토하여 가능한 원인을 파악할 수 있습니다. **Operations(**운영**)** > **Reports(**보고서**)** > **Diagnostics(**진단**)** > **AD Connector Operations(AD Connector** 운영**)**에서 이 보고서를 찾을 수 있습니다.

Active Directory 고급 조정

고급 조정 기능은 시스템에서 매개변수를 더 세부적으로 조정할 수 있도록 Cisco 지원 담당자의 감독하에 지원 작업에 사용되는 노드별 설정을 제공합니다. 이러한 설정은 일반적인 관리 흐름에는 사용되지 않으며 Cisco 지침에 따라서만 사용해야 합니다.

Active Directory ID 검색 속성

Cisco ISE는 SAM, CN 또는 두 속성 모두를 사용하여 사용자를 식별합니다. Cisco ISE, 릴리스 2.2 패치 5 이상 및 2.3 패치 2 이상에서는 sAMAccountName 속성을 기본 속성으로 사용합니다. 이전 릴리스에서는 기본적으로 SAM 및 CN 속성이 모두 검색되었습니다. 이 동작은 CSCvf21978 버그 수정의 일부로 릴리스 2.2 패치 5 이상 및 2.3 패치 2 이상에서 변경되었습니다. 이 릴리스에서는 sAMAccountName 속성만 기본 속성으로 사용됩니다.

사용자 환경에서 필요한 경우 SAM, CN 또는 둘 다를 사용하도록 Cisco ISE를 구성할 수 있습니다. SAM 및 CN이 사용되고 SAMAccountName 속성의 값이 고유하지 않은 경우 Cisco ISE는 CN 속성 값도 비교합니다.

참고 ID 검색 동작은 Cisco ISE 2.4에서 기본적으로 SAM 계정 이름만 검색하도록 변경되었습니다. 이 기본 동작을 수정하려면 "Active Directory ID 검색 속성 구성" 섹션에 설명된 대로 "IdentityLookupField" 플래그의 값을 변경합니다.

Active Directory ID 검색 속성 구성

1. **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다. **Active Directory** 창에서 **Advanced Tools(**고급 도구**)**를 클릭하고 **Advanced Tuning(**고급 조정**)**을 선택합니다. 다음 세부정보를 입력합니다.
   - **ISE Node(ISE** 노드**)** - Active Directory에 연결 중인 ISE 노드를 선택합니다.
   - **Name(**이름**)** - 변경 중인 레지스트리 키를 입력합니다. Active Directory 검색 속성을 변경하려면 `REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField`를 입력합니다.
   - **Value(**값**)** - ISE가 사용자를 식별하는 데 사용하는 속성을 입력합니다.
     - *SAM* - 쿼리에서 SAM만 사용하려는 경우(이 옵션이 기본값)
     - *CN* - 쿼리에서 CN만 사용하려는 경우
     - *SAMCN* - 쿼리에서 CN 및 SAM을 사용하려는 경우
   - **Comment(**설명**)** - 변경 사항에 대한 설명(예: Changing the default behavior to SAM and CN)을 입력합니다.
2. **Update Value(**값 업데이트**)**를 클릭하여 레지스트리를 업데이트합니다.

   팝업 창이 나타납니다. 메시지를 읽고 변경 사항을 수락합니다. ISE의 AD Connector 서비스가 다시 시작됩니다.

검색 문자열 예

다음 예에서는 사용자 이름이 *userd2only*라고 가정합니다.

- SAM 검색 문자열 -

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(|(cn=userd2only)(sAMAccountName=userd2only)))]
```

- SAM 및 CN 검색 문자열 -

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=userd2only))]
```

Active Directory를 사용하여 Cisco ISE를 설정하기 위한 보충 정보

Active Directory를 사용하여 Cisco ISE를 설정하려면 그룹 정책과 머신 인증용 신청자를 구성해야 합니다.

Active Directory에서 그룹 정책 구성

그룹 정책 관리 편집기에 액세스하는 방법에 대한 자세한 내용은 Microsoft Active Directory 설명서를 참고해 주십시오.

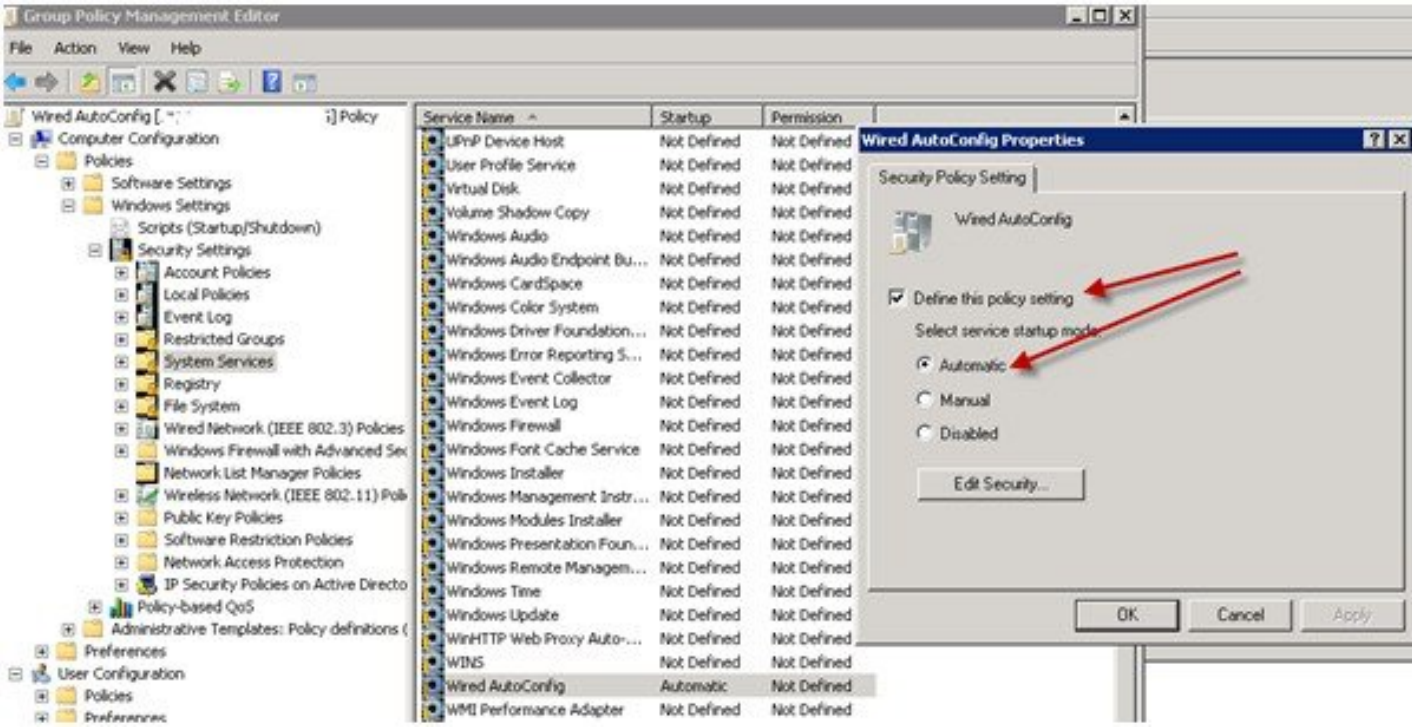
단계 **1** 다음 그림에 나와 있는 것처럼 그룹 정책(Group Policy) 관리 편집기를 엽니다.

그룹 정책 객체(Group Policy Object) 선택

단계 **2** 새 정책을 생성하고 해당 정책을 설명하는 이름을 입력하거나 기존 도메인 정책에 추가합니다.

아래 예에서는 정책 이름으로 Wired Autoconfiguration이 사용되었습니다.

단계 **3** 다음 그림에 나와 있는 것처럼 **Define this policy setting(**이 정책 설정 정의**)** 확인란을 선택하고 서비스 시작 모드로 **Automatic(**자동**)** 라디오 버튼을 클릭합니다.



단계 **4** 원하는 조직 단위 또는 도메인 Active Directory 레벨에 정책을 적용합니다.

Active Directory에 대한 EAP-TLS 머신 인증용 Odyssey 5.X 신청자 구성

Active Directory에 대한 EAP-TLS 머신 인증용으로 Odyssey 5.X 신청자를 사용 중인 경우에는 신청자에서 다음 항목을 구성해야 합니다.

단계 **1** Odyssey Access Client를 시작합니다.

단계 **2** 도구 메뉴에서 **Odyssey Access Client Administrator(Odyssey Access Client** 관리자**)**를 선택합니다.

단계 **3** **Machine Account(**머신 계정**)** 아이콘을 두 번 클릭합니다.

단계 **4** **Machine Account(**머신 계정**)** 창에서 EAP-TLS 인증용 프로파일을 구성해야 합니다.

a) **Configuration(**구성**)** > **Profiles(**프로파일**)**를 선택합니다.
b) EAP-TLS 프로파일의 이름을 입력합니다.
c) Authentication(인증) 탭에서 인증 방법으로 **EAP-TLS**를 선택합니다.
d) Certificate(인증서) 탭에서 **Permit login using my certificate(**내 인증서를 사용한 로그인 허용**)** 확인란을 선택하고 supplicant 머신의 인증서를 선택합니다.
e) **User Info(**사용자 정보**)** 탭에서 **Use machine credentials(**머신 자격 증명 사용**)** 확인란을 선택합니다.

이 옵션을 활성화하면 Odyssey 신청자가 host\<*machine_name*> 형식으로 머신 이름을 전송하며, Active Directory는 해당 요청이 머신에서 수신되는 것으로 식별하여 인증을 수행하기 위한 컴퓨터 객체를 조회합니다. 이 옵션을 비활성화하면 Odyssey 신청자는 host\ 접두사 없이 머신 이름을 전송하며, Active Directory는 사용자 객체를 조회하므로 인증이 실패합니다.

머신 인증용 AnyConnect 에이전트

머신 인증을 위해 AnyConnect 에이전트를 구성하는 경우 다음 중 하나를 수행할 수 있습니다.

- "host/" 접두사가 포함된 기본 머신 호스트 이름을 사용합니다.
- 새 프로파일을 구성합니다. 이 경우 "host/" 접두사와 머신 이름을 차례로 포함해야 합니다.

Easy Connect 및 패시브 ID 서비스 지원을 위한 Active Directory 요건

Easy Connect 및 패시브 ID 서비스는 Active Directory 도메인 컨트롤러에서 생성된 Active Directory 로그인 감사 이벤트를 사용하여 사용자 로그인 정보를 수집합니다. Active Directory 서버를 올바르게 구성해야 ISE 사용자가 서버에 연결하여 사용자 로그인 정보를 가져올 수 있습니다. 다음 섹션에서는 Easy Connect 및 패시브 ID 서비스를 지원하도록 Active Directory 도메인 컨트롤러를 구성하는 방법을 확인할 수 있습니다(Active Directory 측에서의 구성).

Easy Connect 및 패시브 ID 서비스를 지원하도록 Active Directory 도메인 컨트롤러를 구성하려면(Active Directory 측에서의 구성) 다음 단계를 수행합니다.

참고 도메인 전체에서 모든 도메인 컨트롤러를 구성해야 합니다.

1. ISE에서 Active Directory 조인 포인트 및 도메인 컨트롤러를 설정합니다. Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입, 549 페이지 및 도메인 컨트롤러 추가, 551 페이지를 참조하십시오.
2. 도메인 컨트롤러별 WMI를 구성합니다. 패시브 ID용 WMI 구성, 554 페이지를 참조하십시오.
3. Active Directory에서 다음 단계를 수행합니다.
   - 다음에 대한 Active Directory 설정 구성 패시브 ID 서비스, 571 페이지
   - Windows 감사 정책 설정, 575 페이지
4. (선택 사항) 다음 단계를 수행하여 Active Directory에서 ISE로 수행하는 자동 구성 문제를 해결합니다.
   - Microsoft Active Directory 사용자가 도메인 관리자 그룹에 있을 때의 권한 설정, 576 페이지
   - 도메인 관리자 그룹에 속하지 않은 Microsoft Active Directory 사용자에 대한 권한, 576 페이지
   - 도메인 컨트롤러에서 DCOM을 사용하기 위한 권한, 578 페이지
   - WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정, 580 페이지
   - AD 도메인 컨트롤러의 보안 이벤트 로그에 대한 액세스 권한 부여, 581 페이지

다음에 대한 **Active Directory** 설정 구성 패시브 **ID** 서비스

ISE Easy Connect 및 패시브 ID 서비스는 Active Directory 도메인 컨트롤러에서 생성된 Active Directory 로그인 감사 이벤트를 사용하여 사용자 로그인 정보를 수집합니다. ISE는 Active Directory에 연결하여 사용자 로그인 정보를 가져옵니다.

Active Directory 도메인 컨트롤러에서 다음 단계를 수행해야 합니다.

단계 **1** 관련 Microsoft 패치가 Active Directory 도메인 컨트롤러에 설치되어 있는지 확인합니다.

a) Windows Server 2008에는 다음 패치가 필요합니다.

- http://support.microsoft.com/kb/958124

  이 패치는 Microsoft의 WMI에서 메모리 누수를 수정하여, ISE가 도메인 컨트롤러와의 성공적인 연결을 설정할 수 없게 합니다.

- http://support.microsoft.com/kb/973995

이 패치는 때때로 Active Directory 도메인 컨트롤러가 도메인 컨트롤러의 보안 로그에 필요한 사용자 로그인 이벤트를 작성하지 못하도록 하는 Microsoft WMI의 다른 메모리 유출을 수정합니다.

b) Windows Server 2008 R2에는 다음 패치가 필요합니다(SP1이 설치되어 있지 않은 경우).

- http://support.microsoft.com/kb/981314

  이 패치는 때때로 Active Directory 도메인 컨트롤러가 도메인 컨트롤러의 보안 로그에 필요한 사용자 로그인 이벤트를 작성하지 못하도록 하는 Microsoft WMI의 메모리 유출을 수정합니다.

- http://support.microsoft.com/kb/2617858

  이 패치는 Windows Server 2008 R2에서 예기치 않게 발생하는 느린 시작 또는 로그인 프로세스를 수정합니다.

c) Windows 플랫폼의 WMI 관련 문제의 경우 다음 링크에 나열되어 있는 패치가 필요합니다.

- http://support.microsoft.com/kb/2591403

이러한 핫픽스는 WMI 서비스 및 관련 구성 요소의 작동 및 기능과 연관되어 있습니다.

단계 **2** Active Directory가 Windows 보안 로그에 사용자 로그인 이벤트를 기록하는지 확인합니다.

Audit Policy(감사 정책) 설정(Group Policy Management(그룹 정책 관리) 설정의 일부분)의 설정이 Windows 보안 로그에서 필요한 이벤트를 생성하기 위해 정상 로그온을 허용하는지 확인합니다(이는 기본 Windows 설정이지만 이 설정이 올바른지를 명시적으로 확인해야 함).

단계 **3** ISE가 Active Directory에 연결하려면 Active Directory 사용자에게 충분한 권한이 있어야 합니다. 다음 지침에서는 관리 도메인 그룹 사용자 또는 비관리 도메인 그룹 사용자에 대한 권한을 정의하는 방법을 보여줍니다.

- Active Directory 사용자가 도메인 관리자 그룹의 멤버인 경우 필요한 권한
- Active Directory 사용자가 도메인 관리자 그룹의 멤버가 아닌 경우 필요한 권한

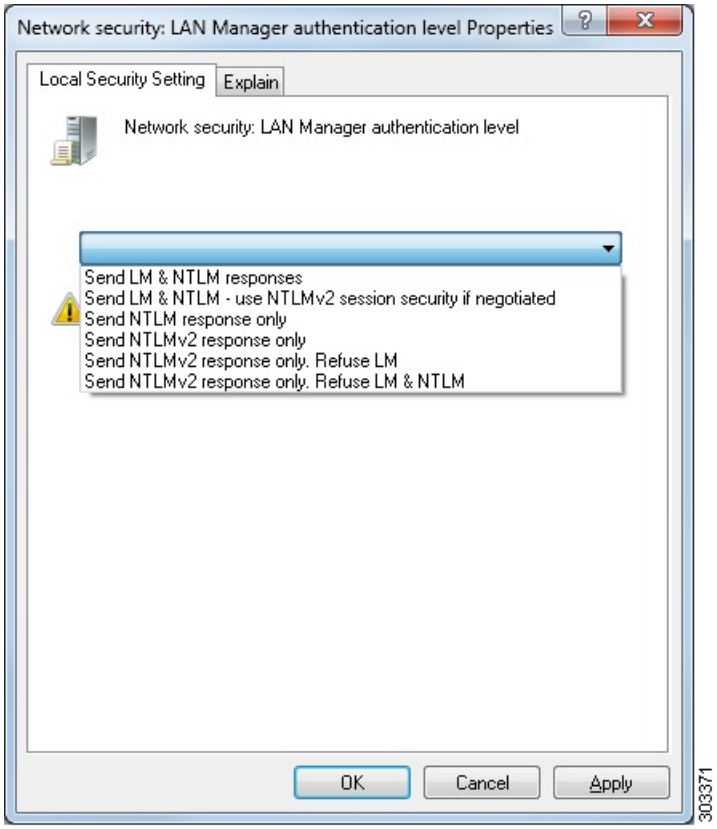
단계 **4** ISE에서 사용하는 Active Directory 사용자는 NTLM(NT LAN Manager) v1 또는 v2로 인증할 수 있습니다. ISE와 Active Directory 도메인 컨트롤러 간에 정상적으로 인증된 연결을 위해 Active Directory NTLM 설정이 ISE NTLM 설정과 일치하는지를 확인해야 합니다. 다음 표에는 모든 Microsoft NTLM 옵션과 지원되는 ISE NTLM 작업이 나와 있습니다. ISE가 NTLMv2로 설정되어 있으면 설명된 6개 옵션이 모두 지원됩니다. ISE가 NTLMv1을 지원하도록 설정되어 있으면 처음 5개 옵션만 지원됩니다.

표 ***63: ISE*** 및 ***AD NTLM*** 버전 설정에 따라 지원되는 인증 유형

ISE NTLM 설정 옵션**/AD(Active Directory) NTLM** 설정 옵션 **NTLMv1** 및 **NTLMv2**	**NTLMv1**	**NTLMv2**
Send LM & NTLM response(LM 및 NTLM 응답 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨

ISE NTLM 설정 옵션**/AD(Active Directory) NTLM** 설정 옵션 **NTLMv1** 및 **NTLMv2**	**NTLMv1**	**NTLMv2**
Send LM & NTLM - use NTLMv2 session security if negotiated(LM 및 NTLM 전송 - 협상 시 NTLMv2 세션 보안 사용) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLM response only(NTLM 응답만 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only(NTLMv2 응답만 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only. Refuse LM(NTLMv2 응답만 전송하고 LM은 거부) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only. Refuse LM & NTLM(NTLMv2 응답만 전송하고 LM 및 NTLM은 거부) 연결이 거부됨 연결이 허용됨	연결이 거부됨	연결이 허용됨

그림 ***15: MS NTLM*** 인증 유형 옵션



단계 **5** Active Directory 도메인 컨트롤러에서 `dllhost.exe`에 대한 트래픽을 허용하는 방화벽 규칙을 생성했는지 확인합니다.

방화벽을 끄거나, 특정 IP(ISE IP 주소)에서의 다음 포트에 대한 액세스를 허용할 수 있습니다.

- TCP 135: 일반 RPC 포트입니다. 비동기 RPC 호출을 수행하는 경우, 이 포트에서 수신 대기하는 서비스는 이 요청을 서비스하는 구성 요소에서 사용 중인 포트를 클라이언트에 알립니다.
- UDP 137: Netbios 이름 확인
- UDP 138: Netbios 데이터그램 서비스
- TCP 139: Netbios 세션 서비스
- TCP 445: SMB

더 많은 포트가 동적으로 할당됩니다. 또는 수동으로 구성할 수 있습니다. 대상으로 %SystemRoot%\System32\dllhost.exe를 추가하는 것을 권장합니다. 이 프로그램은 포트를 동적으로 관리합니다.

모든 방화벽 규칙을 특정 IP(ISE IP)에 할당할 수 있습니다.

Windows 감사 정책 설정

Audit Policy(감사 정책**)(Group Policy Management(**그룹 정책 관리**)** 설정의 일부분)가 정상 로그온을 허용하는지 확인합니다. 이는 AD 도메인 컨트롤러 머신의 Windows 보안 로그에서 필요한 이벤트를 생성하기 위해 필요합니다. 이는 기본 Windows 설정이지만 이 설정이 올바른지 확인해야 합니다.

단계 **1** **Start(**시작**)** > **Programs(**프로그램**)** > **Administrative Tools(**관리 도구**)** > **Group Policy Management(**그룹 정책 관리**)**를 선택합니다.

단계 **2** Domains(도메인) 아래의 관련 도메인으로 이동한 다음 탐색 트리를 펼칩니다.

단계 **3** **Default Domain Controller Policy(**기본 도메인 컨트롤러 정책**)**를 선택하고 마우스 오른쪽 버튼을 클릭한 후에 **Edit(**편집**)**를 선택합니다.

그룹 정책 관리 편집기가 나타납니다.

단계 **4** **Default Domain Controllers Policy(**기본 도메인 컨트롤러 정책**)** > **Computer Configuration(**컴퓨터 컨피그레이션**)** > **Policies(**정책**)** > **Windows Settings(Windows** 설정**)** > **Security Settings(**보안 설정**)**를 선택합니다.

- Windows Server 2003 또는 Windows Server 2008(R2 이외 버전)의 경우 **Local Policies(**로컬 정책**)** > **Audit Policy(**감사 정책**)**를 선택합니다. 두 개의 정책 항목, 즉 **Audit Account Logon Events(**계정 로그온 이벤트 감사**)** 및 **Audit Logon Events(**로그온 이벤트 감사**)**의 경우 해당하는 **Policy Setting(**정책 설정**)**에 **Success** 조건이 직접적 또는 간접적으로 포함되어 있는지 확인합니다. Success 조건을 간접적으로 포함하려면 **Policy Setting(**정책 설정**)**을 **Not Defined(**정의되지 않음**)**로 설정해야 하며, 이는 유효 값이 상위 레벨 도메인에서 상속됨을 나타냅니다. 그리고 해당 상위 레벨 도메인의 **Policy Setting(**정책 설정**)**은 **Success** 조건을 명시적으로 포함하도록 구성해야 합니다.
- Windows Server 2008 R2 및 Windows 2012의 경우 **Advanced Audit Policy Configuration(**고급 감사 정책 컨피그레이션**)** > **Audit Policies(**감사 정책**)** > **Account Logon(**계정 로그온**)**을 선택합니다. 두 개의 정책 항목, 즉 **Audit Kerberos Authentication Service(Kerberos** 인증 서비스 감사**)** 및 **Audit Kerberos Service Ticket Operations(Kerberos** 서비스 티켓 작업 감사**)**의 경우 위에서 설명한 대로 해당하는 Policy Setting(정책 설정)에 Success 조건이 직접적 또는 간접적으로 포함되어 있는지 확인합니다.

  참고 Cisco ISE는 Active Directory 도메인 컨트롤러 컨피그레이션에서 이 암호화 유형을 비활성화하지 않는 한 Active Directory와 통신하면서 Kerberos 프로토콜에서 RC4 암호를 사용합니다. Active Directory에서 **Network Security: Configure Encryption Types Allowed for Kerberos(**네트워크 보안**: Kerberos** 에 허용되는 암호화 유형 구성**)** 옵션을 사용하여 Kerberos 프로토콜에 대해 허용되는 암호화 유형을 구성할 수 있습니다.

단계 **5** 감사 정책 항목 설정이 변경된 경우에는 `gpupdate /force`를 실행하여 새 설정을 강제로 적용해야 합니다.

Microsoft Active Directory 사용자가 도메인 관리자 그룹에 있을 때의 권한 설정

Windows Server 2008 R2, Windows Server 2012 및 Windows Server 2012 R2의 경우 도메인 관리자 그룹에는 기본적으로 Windows 운영체제의 특정 레지스트리 키에 대한 모든 제어 권한이 없습니다. Microsoft Active Directory 관리자는 Microsoft Active Directory 사용자에게 다음 레지스트리 키에 대한 모든 제어 권한을 부여해야 합니다.

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

다음 Microsoft Active Directory 버전의 경우에는 레지스트리를 변경할 필요가 없습니다.

- Windows 2003
- Windows 2003R2
- Windows 2008

모든 제어 권한을 부여하려면 Microsoft Active Directory 관리자가 먼저 다음과 같이 키 소유권을 얻어야 합니다.

단계 **1** 키 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **Owner(**소유자**)** 탭을 선택합니다.

단계 **2** **Permissions(**권한**)**를 클릭합니다.

단계 **3** **Advanced(**고급**)**를 클릭합니다.

도메인 관리자 그룹에 속하지 않은 Microsoft Active Directory 사용자에 대한 권한

Windows 2012 R2의 경우 Microsoft AD 사용자에게 다음 레지스트리 키에 대한 모든 제어 권한을 부여합니다.

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Windows PowerShell에서 다음 명령을 사용하여 레지스트리 키에 대한 전체 권한이 부여되었는지 확인합니다.

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
  ```

- `get-acl -path "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list`

Microsoft AD 사용자가 도메인 관리자 그룹에는 없지만 도메인 사용자 그룹에는 있으면 다음 권한이 필요합니다.

- Cisco ISE가 도메인 컨트롤러에 연결할 수 있도록 레지스트리 키 추가
- 도메인 컨트롤러에서 DCOM을 사용하기 위한 권한, 578 페이지
- WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정, 580 페이지

이러한 권한은 다음 Microsoft AD 버전에만 필요합니다.

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

Cisco ISE가 도메인 컨트롤러에 연결할 수 있도록 레지스트리 키 추가

Cisco ISE가 도메인 사용자로 연결하여 로그인 인증 이벤트를 검색할 수 있게 하려면 도메인 컨트롤러에 일부 레지스트리 키를 수동으로 추가해야 합니다. 도메인 컨트롤러 또는 도메인의 머신에서 에이전트는 필요하지 않습니다.

다음 레지스트리 스크립트에는 추가할 키가 나와 있습니다. 이 스크립트를 복사하여 텍스트 파일에 붙여 넣고 파일을 .reg 확장자로 저장한 다음 파일을 더블 클릭하여 레지스트리를 변경합니다. 레지스트리 키를 추가하려면 사용자가 루트 키의 소유자여야 합니다.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

DllSurrogate 키의 값에는 공백이 두 개 포함되어야 합니다. 레지스트리를 수동으로 업데이트하는 경우 두 개의 공백만 포함하고 따옴표는 포함하지 않아야 합니다. 레지스트리를 수동으로 업데이트하는 동안 AppID, DllSurrogate 및 해당 값에 따옴표가 포함되지 않았는지 확인하십시오.

파일 맨 끝의 빈 줄을 포함하여 위 스크립트에 나와 있는 빈 줄은 그대로 유지합니다.

Windows 명령 프롬프트에서 다음 명령을 사용하여 레지스트리 키가 생성되었고 올바른 값을 가지고 있는지 확인합니다.

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

도메인 컨트롤러에서 **DCOM**을 사용하기 위한 권한

Cisco ISE 패시브 ID 서비스에 사용되는 Microsoft Active Directory 사용자는 도메인 컨트롤러 서버에서 DCOM을 사용할 권한이 있어야 합니다. **dcomcnfg** 명령줄 도구를 사용하여 권한을 구성하십시오.

단계 **1** 명령줄에서 **dcomcnfg** 도구를 실행합니다.

단계 **2** **Component Services(**구성 요소 서비스**)**를 펼칩니다.

단계 **3** **Computers(**컴퓨터**)** > **My Computer(**내 컴퓨터**)**를 펼칩니다.

단계 **4** 메뉴 모음에서 **Action(**작업**)**을 선택하고 **Properties(**속성**)**를 클릭한 후 **COM Security(COM** 보안**)**를 클릭합니다.

단계 **5** Cisco ISE가 액세스 및 실행에 모두 사용할 계정에 Allow(허용) 권한이 있는지 확인합니다. 해당 Microsoft Active Directory 사용자를 4개 옵션(**Access Permissions(**액세스 권한**)** 및 **Launch and Activation Permissions(**실행 및 활성화 권한**)** 모두에 대한 **Edit Limits(**제한 편집**)**와 **Edit Default(**기본값 편집**)**)에 모두 추가해야 합니다.

단계 **6** **Access Permissions(**액세스 권한**)** 및 **Launch and Activation Permissions(**실행 및 활성화 권한**)** 둘 다에 대해 로컬 액세스 및 Remote Access를 모두 허용합니다.

그림 ***16:*** 액세스 권한에 대한 로컬 및 ***Remote Access***

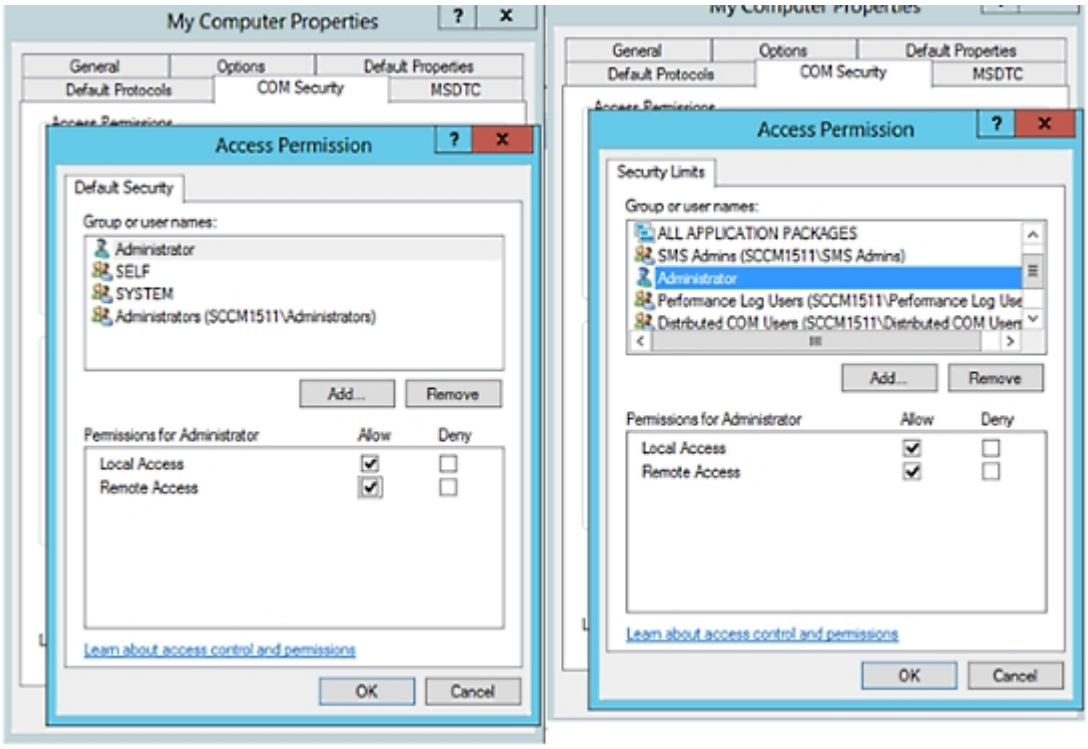
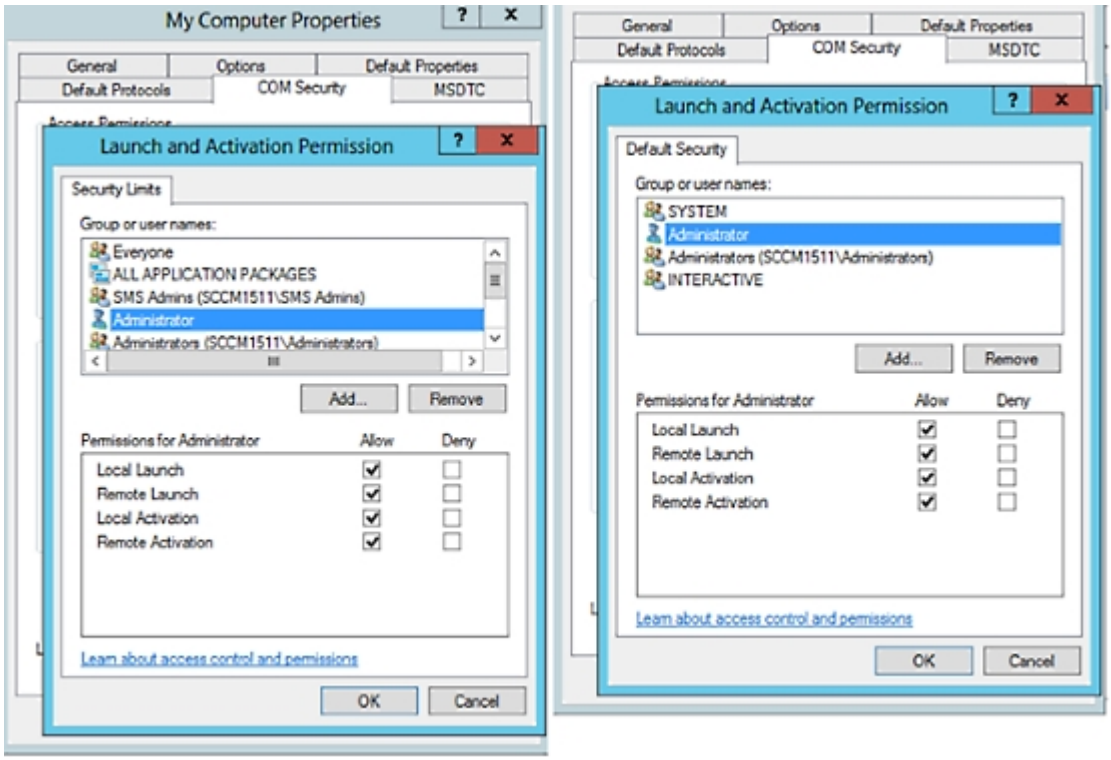


그림 *17:* 실행 및 활성화 권한에 대한 로컬 및 ***Remote Access***



WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정

기본적으로 Microsoft Active Directory 사용자에게는 방법 실행 및 원격 활성화에 대한 권한이 없습니다. wmimgmt.msc MMC 콘솔을 사용하여 액세스 권한을 부여할 수 있습니다.

단계 **1** **Start(**시작**)** > **Run(**실행**)**을 선택하고 `wmimgmt.msc`를 입력합니다.

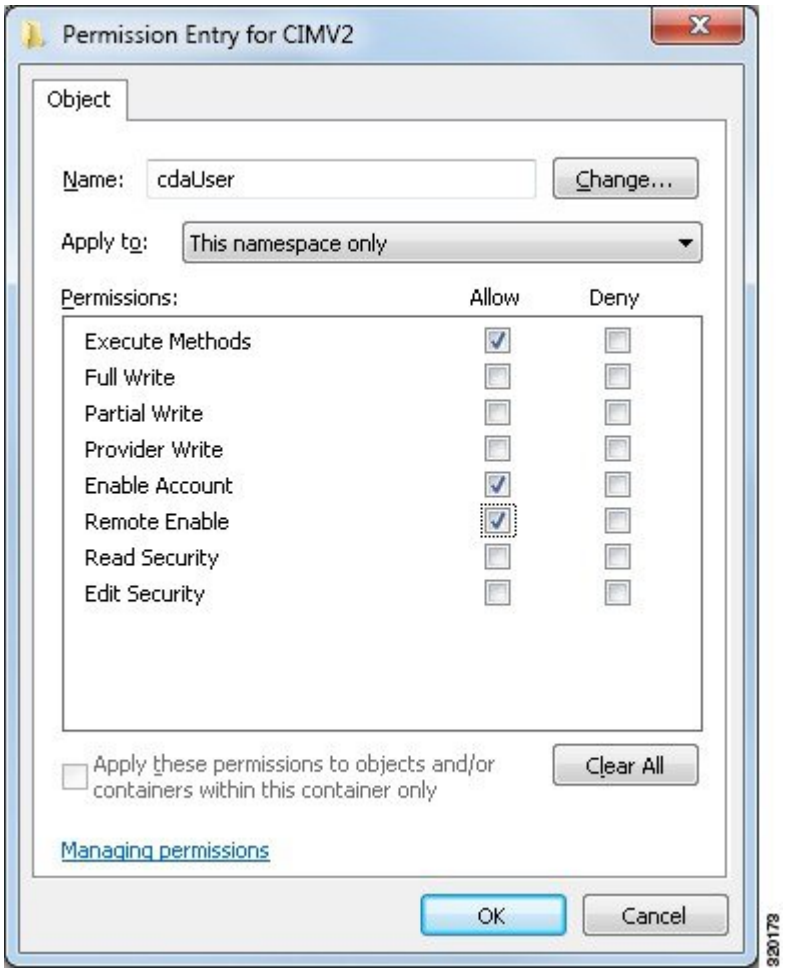
단계 **2** **WMI Control(WMI** 컨트롤**)**을 마우스 오른쪽 버튼으로 클릭하고 **Properties(**속성**)**를 클릭합니다.

단계 **3** **Security(**보안**)** 탭에서 **Root(**루트**)**를 펼치고 **CIMV2**를 선택합니다.

단계 **4** **Security(**보안**)**를 클릭합니다.

단계 **5** Active Directory 사용자를 추가하고 아래 이미지에 나와 있는 대로 필요한 권한을 구성합니다.

그림 ***18: WMI Root\CIMv2*** 이름 공간에 필요한 권한



AD 도메인 컨트롤러의 보안 이벤트 로그에 대한 액세스 권한 부여

Windows 2008 이상에서는 Event Log Readers라는 그룹에 ISE ID 매핑 사용자를 추가하여 AD 도메인 컨트롤러 로그에 대한 액세스 권한을 부여할 수 있습니다.

모든 이전 버전 Windows에서는 아래에 나와 있는 것처럼 레지스트리 키를 편집해야 합니다.

단계 **1** 보안 이벤트 로그에 대한 액세스 권한을 위임하려면 계정의 SID를 찾습니다.

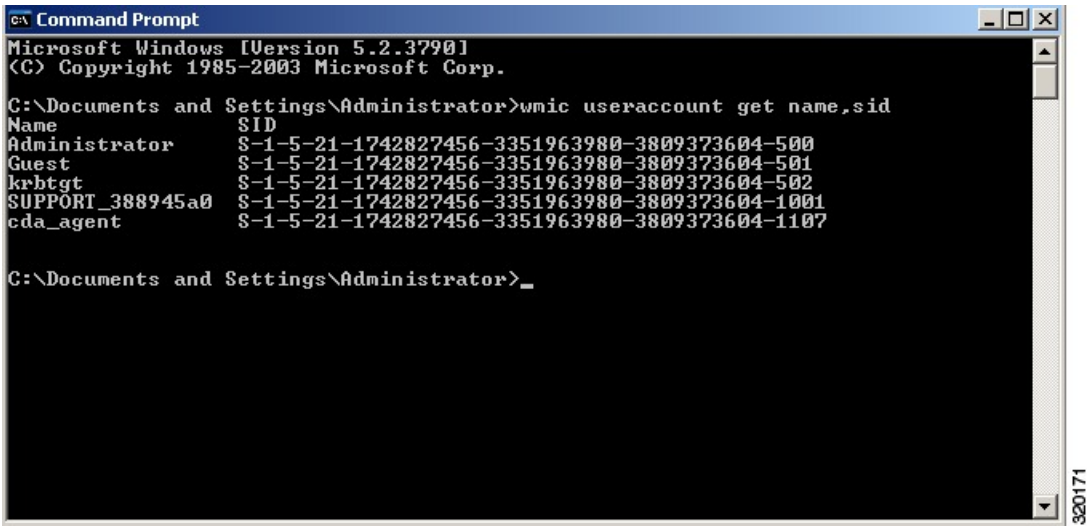
단계 **2** 명령줄에서 다음 명령을 사용하여 모든 SID 계정을 나열합니다. 이 명령은 아래 다이어그램에도 나와 있습니다.

```
wmic useraccount get name,sid
```

특정 사용자 이름 및 도메인의 경우 다음 명령을 사용할 수도 있습니다.

```
wmic useraccount where name="iseUser" get domain,name,sid
```

그림 *19:* 모든 *SID* 계정 나열



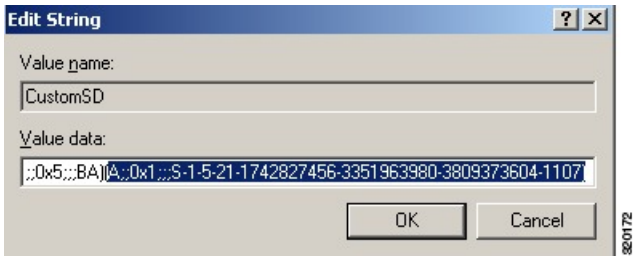
단계 **3** SID를 찾고 레지스트리 편집기를 연 후에 다음 위치로 이동합니다.

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog`

단계 **4** **Security(**보안**)**를 클릭하고 **CustomSD**를 두 번 클릭합니다.

예를 들어 ise_agent 계정 `(SID - S-1-5-21-1742827456-3351963980-3809373604-1107)`에 읽기 권한을 허용하려면 `(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`을 입력합니다.

그림 *20: CustomSD* 문자열 편집



단계 **5** 도메인 컨트롤러에서 WMI 서비스를 다시 시작합니다. 다음과 같이 두 가지 방법으로 WMI 서비스를 다시 시작할 수 있습니다.

a) CLI에서 다음 명령을 실행합니다.

net stop winmgmt

net start winmgmt

b) `Services.msc`를 실행합니다. 그러면 Windows 서비스 관리 툴이 열립니다. Windows 서비스 관리 윈도우에서 **Windows Management Instrumentation** 서비스를 찾아 마우스 오른쪽 버튼으로 클릭한 후에 **Restart(**다시 시작**)**를 선택합니다.

Easy Connect

Easy Connect를 사용하면 사용자를 유선 엔드포인트에서 네트워크로 안전하게 연결한 다음 Cisco ISE가 아닌 Active Directory 도메인 컨트롤러를 통해 사용자를 인증하여 모니터링할 수 있습니다. Easy Connect를 통해 Cisco ISE는 Active Directory 도메인 컨트롤러에서 사용자 인증 정보를 수집합니다. Easy Connect는 MS WMI 인터페이스를 사용하여 Windows 시스템(Active Directory)에 연결하며 Windows 이벤트 메시징에서 로그를 쿼리하므로 현재 Windows가 설치된 엔드포인트만 지원합니다. Easy Connect는 802.1X보다 훨씬 구성하기 쉬운 MAB를 사용하는 유선 연결을 지원합니다. 802.1X와는 달리 Easy Connect 및 MAB를 사용하는 경우:

- 신청자를 구성할 필요가 없습니다.
- PKI를 구성할 필요가 없습니다.
- 외부 서버(AD)가 사용자를 인증하고 나면 ISE에서 CoA를 발급합니다.

Easy Connect는 다음과 같은 작동 모드를 지원합니다.

- 시행 모드: ISE가 사용자 자격 증명을 기준으로 하는 시행을 위해 네트워크 디바이스에 권한 부여 정책을 실제로 다운로드합니다.
- 가시성 모드: Cisco ISE가 NAD 디바이스 센서에서 수신한 세션 병합 및 계정 관리 정보를 게시하여 해당 정보를 pxGrid로 전송합니다.

두 가지 경우 모두, AD(Active Directory)에서 인증된 사용자는 Cisco ISE 라이브 세션 보기에 표시되므로 서드파티 애플리케이션에서 Cisco pxGrid 인터페이스를 사용하여 세션 디렉토리에서 해당 사용자를 쿼리할 수 있습니다. 알려진 정보는 사용자 이름, IP 주소, AD DC 호스트 이름 및 AD DC NetBios 이름입니다. pxGrid에 대한 자세한 내용은 Cisco pxGrid 노드, 83 페이지를 참고하십시오.

Easy Connect를 설정하면 이름 또는 IP 주소를 기준으로 특정 사용자를 필터링할 수 있습니다. 예를 들어 엔드포인트를 이용해 일반 관리자를 지원하고자 엔드포인트에 로그인한 IT 서비스 관리자가 있다면, 관리자 활동을 필터링하여 Live Sessions(라이브 세션)에는 표시하지 않고 관련 엔드포인트의 일반 사용자에게만 표시되게 할 수 있습니다. 수동 ID 서비스를 필터링하는 방법은 패시브 ID 서비스 필터링, 633 페이지 항목을 참조하십시오.

Easy Connect 제한

- MAB(MAC Authentication Bypass)는 Easy Connect를 지원합니다. MAB와 802.1X를 둘 다 동일한 포트에 구성할 수는 있지만 각 서비스에 대해 서로 다른 ISE 정책을 사용해야 합니다.
- 현재는 MAB 연결만 지원됩니다. 연결에 대해 고유한 인증 정책이 필요하지 않습니다. 권한 부여 정책에 정의된 Easy Connect 조건에 의해 연결에 권한이 부여되며 사용 권한이 부여되기 때문입니다.
- Easy Connect는 고가용성 모드에서 지원됩니다. 수동 ID로 여러 노드를 정의하고 활성화할 수 있습니다. 그러면 ISE가 PSN 하나를 자동으로 활성화하며 나머지 노드는 스탠바이 상태로 유지됩니다.
- Cisco NAD(Network Access Device)만 지원됩니다.

- IPv6은 지원되지 않습니다.
- 무선 연결은 현재 지원되지 않습니다.
- Kerberos 인증 이벤트만 추적되며, 따라서 Easy Connect는 사용자 인증만 활성화하며 머신 인증은 지원하지 않습니다.

Easy Connect를 사용하려면 ISE에서 컨피그레이션을 수행해야 합니다. 또한 Active Directory 도메인 서버에도 Microsoft에서 발급한 지침에 따라 올바른 패치와 컨피그레이션을 적용해야 합니다. Cisco ISE용 Active Directory 도메인 컨트롤러 구성에 대한 자세한 내용은 다음 항목을 참고하십시오. Easy Connect 및 패시브 ID 서비스 지원을 위한 Active Directory 요건, 570 페이지

Easy Connect 시행 모드

Easy Connect를 사용하면 사용자는 MAB(MAC Address Bypass) 프로토콜을 사용하고 인증을 위해 AD(Active Directory)에 액세스하여 Windows 운영체제가 설치된 유선 엔드포인트(일반적으로 PC)에서 보안 네트워크에 로그온할 수 있습니다. Easy Connect는 인증된 사용자에 대한 정보를 위해 Active Directory 서버에서 WMI(Windows Management Instrumentation) 이벤트를 수신 대기합니다. AD가 사용자를 인증하면 도메인 컨트롤러는 사용자에 대해 할당된 사용자 이름과 IP 주소를 포함하는 이벤트 로그를 생성합니다. Cisco ISE는 AD에서 로그인 알림을 수신한 다음 RADIUS CoA(Change of Authorization)를 발급합니다.

참고 RADIUS 서버 유형이 통화 확인으로 설정되어 있는 경우 MAC 주소 조회는 MAB 요청에 대해 수행되지 않습니다. 따라서 요청에 대해 액세스 수락이 반환됩니다. 이 응답이 기본 구성입니다.

Easy Connect 시행 모드 프로세스 플로우

Easy Connect 시행 모드 프로세스는 다음과 같습니다.

1. 사용자가 유선 엔드포인트(예: PC 등)에서 NAD에 연결합니다.
2. MAB용으로 구성된 NAD가 Cisco ISE에 액세스 요청을 보냅니다. Cisco ISE는 사용자 구성을 기준으로 하는 액세스 권한으로 응답하여 사용자의 AD 액세스를 허용합니다. 구성은 최소한 DNS, DHCP 및 AD 액세스를 허용해야 합니다.
3. 사용자가 도메인에 로그인하면 보안 감사 이벤트가 Cisco ISE로 전송됩니다.
4. ISE가 RADIUS의 MAC 주소, IP 주소 및 도메인 이름을 수집하며 보안 감사 이벤트에서 사용자에 대한 계정 관리 정보(로그인 정보)도 수집합니다.
5. 모든 데이터가 수집되어 세션 디렉터리에 병합되면 Cisco ISE는 NAD에 CoA를 발급하며(정책 서비스 노드에서 관리되는 적절한 정책 기준), 해당 정책을 기준으로 NAD가 사용자에게 네트워크 액세스 권한을 제공합니다.

그림 ***21: Easy Connect*** 시행 모드 기본 플로우

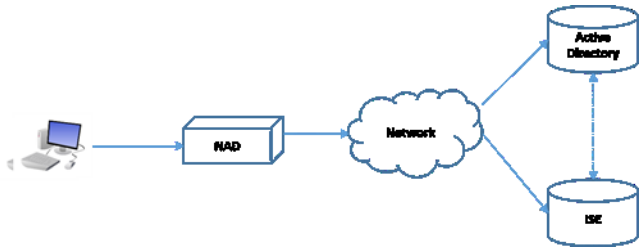
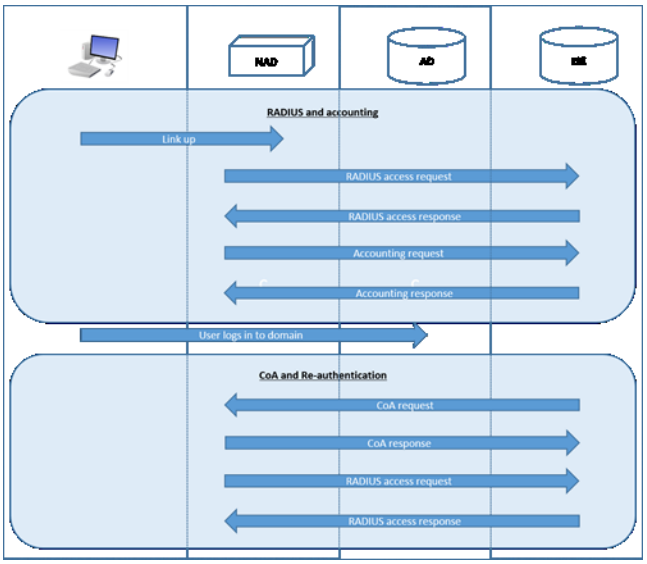


그림 ***22: Easy Connect*** 시행 모드 상세 플로우

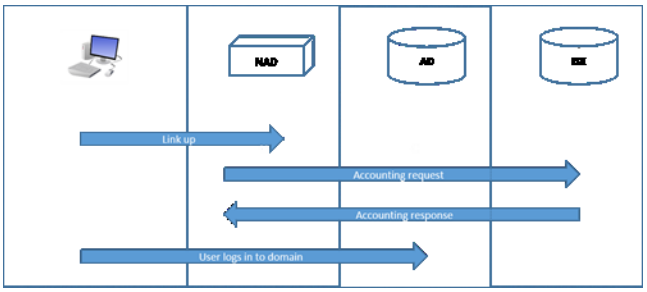


시행 모드 구성에 대한 자세한 내용은 Easy Connect 시행 모드 구성, 586 페이지를 참고하십시오.

Easy Connect 가시성 모드

가시성 모드에서는 Cisco ISE가 RADIUS(NAD의 디바이스 센서 기능의 일부분)에서 계정 관리 정보만을 모니터링하며 권한 부여는 수행하지 않습니다. Easy Connect는 RADIUS 계정 관리 및 WMI 이벤트를 수신 대기하며 해당 정보를 로그 및 보고서에 게시합니다(pxGrid에는 선택적으로 게시). pxGrid가 설정되어 있는 경우 Active Directory를 사용하는 사용자 로그인 중에 RADIUS 계정 관리 시작 및 세션 종료가 모두 pxGrid에 게시됩니다.

그림 ***23: Easy Connect*** 가시성 모드 플로우



Easy Connect 가시성 모드 구성에 대한 자세한 내용은 EasyConnect 가시성 모드 구성, 587 페이지를 참고하십시오.

Easy Connect 시행 모드 구성

시작하기 전에

- 최고의 성능을 위해서는 WMI 이벤트 수신 전용 PSN을 구축합니다.
- AD 로그인 이벤트를 수신하는 WMI 노드에 대해 Active Directory 도메인 컨트롤러 목록을 생성합니다.
- Cisco ISE가 Active Directory에서 사용자 그룹을 가져오려면 가입해야 하는 Microsoft 도메인을 확인합니다.
- 권한 부여 정책에서 참조로 사용되는 Active Directory 그룹을 확인합니다.
- pxGrid를 사용하여 네트워크 디바이스의 세션 데이터를 다른 pxGrid가 활성화된 시스템과 공유하는 경우에는 구축에서 pxGrid 페르소나를 정의합니다. pxGrid에 대한 자세한 내용은 다음을 참고하십시오. Cisco pxGrid 노드, 83 페이지
- MAB가 정상적으로 수행되고 나면 NAD는 제한적 액세스 프로파일을 제공해야 합니다. 그러면 개요의 설명과 같이 해당 포트의 사용자가 Active Directory 서버에 액세스할 수 있습니다.

참고 여러 노드에서 Passive Identity Service를 활성화할 수는 있지만 EasyConnect는 한 번에 한 노드에서만 작동할 수 있습니다. 여러 노드에 대해 서비스를 활성화하면 ISE는 활성화된 EasyConnect 세션에 사용할 노드를 자동으로 결정합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택한 후 노드를 열고 **General Settings(**일반 설정**)** 아래에서 **Enable Passive Identity Service(**패시브 **ID** 서비스 활성화**)**를 활성화합니다.

단계 **2** Easy Connect에서 사용할 Active Directory 조인 포인트와 도메인 컨트롤러를 구성합니다. 자세한 내용은 Easy Connect 및 패시브 ID 서비스 지원을 위한 Active Directory 요건, 570 페이지를 참고하십시오.

단계 **3** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다. **Groups(**그룹**)** 탭을 클릭하고 인증 정책에 사용할 Active Directory 그룹을 추가합니다.
도메인 컨트롤러에 대해 매핑하는 Active Directory 그룹은 PassiveID 사전에서 동적으로 업데이트되며, 정책 조건 규칙을 설정할 때 이러한 그룹을 사용할 수 있습니다.

단계 **4** 참고 EasyConnect 프로세스가 올바르게 실행하고 ISE가 CoA를 발급하도록 활성화하려면 EasyConnect 권한 부여에 사용되는 모든 프로파일에 대해 **Passive Identity Tracking(**수동 **ID** 추적**)**을 활성화해야 합니다.

Policy(정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다. EasyConnect에서 사용할 프로파일의 경우 해당 프로파일을 열고 **Passive Identify Tracking(**수동 **ID** 추적**)**을 활성화합니다.

단계 **5** 정책 규칙을 생성합니다. 이렇게 하려면 **Policy(정책)** > **Policy Elements(정책 요소)** > **Conditions(조건)** > **Authorization(권한 부여)** > **Simple Conditions(단순 조건)**를 선택하고 EasyConnect용 규칙을 생성합니다. **Add(추가)**를 클릭하고 조건을 정의합니다.

a) 이름과 설명을 입력합니다.

b) **Attribute(속성)**에서 PassiveID 사전으로 이동한 다음 PassiveID_Groups를 선택하여 도메인 컨트롤러 그룹용 조건을 생성하거나, PassiveID_user를 선택하여 개별 사용자용 조건을 생성합니다.

c) 올바른 작업을 입력합니다.

d) 정책에 포함할 사용자 이름 또는 그룹 이름을 입력합니다.

단계 **6** **Submit(제출)**을 클릭합니다.

EasyConnect 가시성 모드 구성

시작하기 전에

- 최고의 성능을 위해서는 WMI 이벤트 수신 전용 PSN을 구축합니다.
- AD 로그인 이벤트를 수신하는 WMI 노드에 대해 Active Directory 도메인 컨트롤러 목록을 생성합니다.
- Cisco ISE가 Active Directory에서 사용자 그룹을 가져오려면 가입해야 하는 Microsoft 도메인을 확인합니다.
- pxGrid를 사용하여 네트워크 디바이스의 세션 데이터를 다른 pxGrid가 활성화된 시스템과 공유하는 경우에는 구축에서 pxGrid 페르소나를 정의합니다. pxGrid에 대한 자세한 내용은 다음을 참고하십시오. Cisco pxGrid 노드, 83 페이지

단계 **1** **Administration(관리)** > **System(시스템)** > **Deployment(구축)**를 선택한 후 노드를 열고 **General Settings(일반 설정)** 아래에서 **Enable Passive Identity Service(패시브 ID 서비스 활성화)**를 활성화합니다.

단계 **2** Easy Connect에서 사용할 Active Directory 조인 포인트와 도메인 컨트롤러를 구성합니다. 자세한 내용은 Easy Connect 및 패시브 ID 서비스 지원을 위한 Active Directory 요건, 570 페이지를 참고하십시오.

PassiveID 작업 센터

Passive Identity Connector(PassiveID 작업 센터)는 중앙 집중식 원스톱 설치 및 구현을 제공하기 때문에, 사용자는 네트워크를 쉽고 간단하게 구성해 사용자 ID 정보를 받고 Cisco FMC(Firepower Management Center)나 Stealthwatch 같은 다양한 보안 제품 가입자와 공유할 수 있습니다. 수동 식별의 전체 브로커로서 PassiveID 작업 센터는 AD DC(Active Directory Domain Controller) 같은 다양한 제공자 소스로부터 사용자 ID를 수집하고, 사용자 로그인 정보를 사용 중인 관련 IP 주소에 매핑한 다음 매핑 정보를 사용자가 구성한 가입자 보안 제품과 공유합니다.

Passive Identity(패시브 ID)란?

Cisco Identity Services Engine(ISE)에서 제공하는 표준 흐름으로, AAA(인증, 권한 부여 및 계정 관리) 서버를 제공하며 802.1X나 Web Authentication(웹 인증) 같은 기술을 활용하고, 사용자 또는 엔드포인트와 직접 통신해 네트워크 액세를 요청한 다음 관련 로그인 자격 증명을 이용해 ID를 확인하고 활성 인증합니다.

패시브 ID 서비스는 사용자를 직접 인증하는 대신 서비스 제공자로 확인된 (Active Directory 같은) 외부 인증 서버에서 사용자 ID와 IP 주소를 수집한 다음 이 정보를 가입자와 공유합니다. PassiveID 작업 센터는 먼저 서비스 제공자로부터 (대부분 사용자 로그인 및 비밀번호를 바탕으로) 사용자 ID 정보를 수신한 다음 필요한 확인 작업과 서비스를 수행하여 사용자 ID를 관련 IP 주소와 매치함으로써 인증된 IP 주소를 가입자에게 전달합니다.

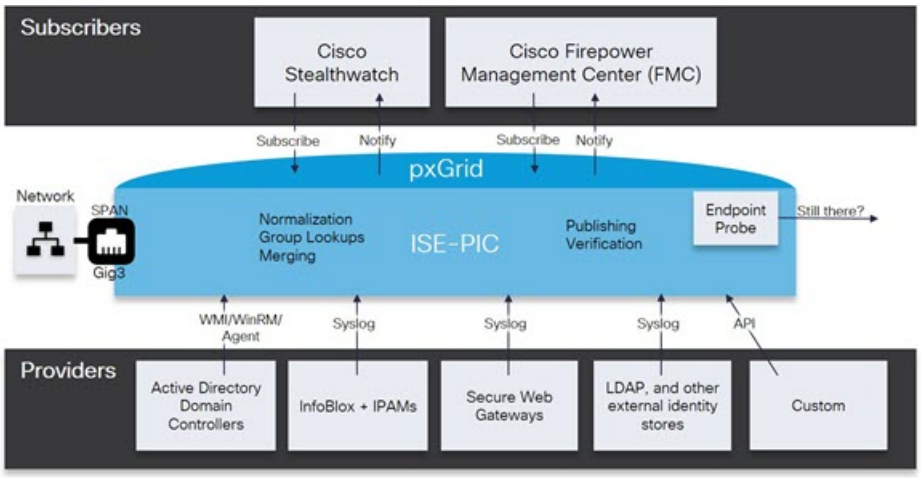
Passive Identity Connector(PassiveID 작업 센터) 플로우

PassiveID 작업 센터의 흐름은 다음과 같습니다.

1. 서비스 제공자가 사용자 또는 엔드포인트의 인증을 수행합니다.
2. 서비스 제공자가 인증된 사용자 정보를 Cisco ISE에 전송합니다.
3. Cisco ISE는 사용자 정보를 정규화하고 관련 조회와 병합 및 구문 분석을 수행하며 IP 주소에 매핑하고, 매핑한 세부정보를 pxGrid에 게시합니다.
4. pxGrid 가입자는 매핑된 사용자 세부정보를 수신합니다.

다음 다이어그램에서는 Cisco ISE에서 제공되는 개괄적인 플로우에 대해 설명합니다.

그림 *24:* 고수준 흐름



초기 설정 및 컨피그레이션

Cisco PassiveID 작업 센터를 빠르게 사용하려면 다음 흐름을 따르십시오.

1. DNS 서버를 올바르게 구성했는지 확인합니다(Cisco ISE에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). 자세한 내용은 DNS 서버, 548 페이지를 참고하십시오.

2. 패시브 ID 서비스에 사용할 전용 정책 서버(PSN)에서 패시브 ID 및 pxGrid 서비스를 활성화합니다. **Administration(관리)** > **System(시스템)** > **Deployment(구축)**를 선택한 후 노드를 열고 **General Settings(일반 설정)** 아래에서 **Enable Passive Identity Service(패시브 ID 서비스 활성화)** 및 **pxGrid**를 활성화합니다.
3. NTP 서버의 시계 설정을 동기화합니다.
4. ISE Passive Identity(ISE 패시브 ID) 설정을 사용하여 초기 서비스 제공자를 구성합니다. 자세한 내용은 다음을 참조하십시오. PassiveID(패시브 ID) 설정 시작하기 , 591 페이지
5. 단일 또는 다중 가입자를 구성합니다. 자세한 내용은 다음을 참조하십시오. 가입자, 636 페이지

최초 서비스 제공자와 가입자를 설정하면 추가 서비스 제공자를 쉽게 생성하고(추가 패시브 ID 서비스 제공자, 596 페이지 참조) PassiveID 작업 센터:에서 다른 서비스 제공자의 패시브 ID를 관리할 수 있습니다(PassiveID Work Center(패시브 ID 작업 센터)에서의 모니터링 및 문제 해결 PassiveID 작업 센터, 640 페이지 참조).

- RADIUS 라이브 세션, 323 페이지
- Cisco ISE 경보, 1314 페이지
- Cisco ISE 보고서, 288 페이지
- 들어오는 트래픽을 검증하는 TCP 덤프 유틸리티, 1359 페이지

PassiveID 작업 센터 Dashboard(대시보드)

Cisco PassiveID 작업 센터 대시보드에는 상관관계가 분석되고 통합된 요약 및 통계 데이터가 표시되는데, 이는 효과적인 모니터링 및 문제 해결을 위해서는 필수적이며 실시간으로 업데이트됩니다. dashlet에서는 별도의 설명이 없는 한 지난 24시간 동안의 활동을 표시합니다. 대시보드에 액세스하려면 **Work Centers(작업 센터)** > **PassiveID(패시브 ID)**를 선택한 다음 왼쪽 패널에서 **Dashboard(대시보드)**를 선택합니다. PAN(Primary Administration Node)에서만 Cisco PassiveID 작업 센터 대시보드를 볼 수 있습니다.

- **Main(기본)** 보기에는 선형 메트릭 대시보드, 차트 dashlet 및 목록 dashlet이 있습니다. PassiveID 작업 센터에서는 dashlet을 구성할 수 없습니다. 제공되는 dashlet은 다음과 같습니다.
  - **Passive Identity Metrics(패시브 ID 메트릭)**: 현재 추적 중인 총 고유 라이브 세션 수, 시스템에 구성된 총 ID 제공자 수, ID 데이터를 능동적으로 전달하는 총 에이전트 수, 현재 구성된 총 가입자 수를 표시합니다.
  - **Provider(제공자)**: 제공자는 사용자 ID 정보를 PassiveID 작업 센터에 제공합니다. 제공자 소스에서 정보를 수신하는 데 사용할 ISE 프로브(지정된 소스에서 데이터를 수집하는 메커니즘)를 구성합니다. 예를 들어 AD(Active Directory) 프로브와 에이전트 프로브는 각기 다른 기술을 사용하여 ISE-PIC가 AD에서 데이터를 수집하는 데 도움을 주는 한편, 시스템 로그 프로브는 시스템 로그 메시지를 읽는 구문 분석기에서 데이터를 수집합니다.
  - **Subscribers(가입자)**: 가입자는 사용자 ID 정보를 검색하기 위해 ISE에 연결합니다.

- **OS Types(OS** 유형**)**: 표시할 수 있는 OS 유형은 Windows뿐입니다. Windows 유형은 Windows 버전별로 표시됩니다. 제공자는 OS 유형을 보고하지 않지만 ISE는 Active Directory를 쿼리하여 해당 정보를 가져올 수 있습니다. dashlet에는 최대 1,000개의 항목이 표시됩니다.
- **Alarms(**경보**)**: 사용자 ID 관련 경보입니다.

프로브 및 제공자로서의 **Active Directory**

Active Directory(AD)는 사용자 이름, IP 주소 및 도메인 이름 같은 사용자 ID 정보를 수신할 수 있는 대단히 안전하고 정확한 소스입니다.

AD 프로브인 패시브 ID 서비스는 WMI 기술을 이용해 AD에서 사용자 ID 정보를 수신하지만, 다른 프로브는 다른 기술 과 방법을 이용해 AD를 사용자 ID 제공자로 사용합니다. ISE에서 제공하는 다른 프로브 및 제공자 유형에 관한 자세한 내용은 추가 패시브 ID 서비스 제공자, 596 페이지 항목을 참조하십시오.

Active Directory 프로브를 구성하면 (마찬가지로 Active Directory를 소스로 사용하는) 이러한 다른 프로브를 빠르게 구성하고 활성화할 수 있습니다.

- Active Directory 에이전트, 599 페이지

참고 Active Directory 에이전트는 Windows Server 2008 이상에서만 지원됩니다.

- SPAN, 609 페이지
- 엔드포인트 프로브, 633 페이지

또한 사용자 정보를 수집할 때 AD 사용자 그룹을 사용할 수 있도록 Active Directory 프로브를 구성합니다. AD 사용자 그룹을 AD, 에이전트, SPAN 및 시스템 로그 프로브에 사용할 수 있습니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성, 556 페이지 항목을 참조하십시오.

Active Directory(WMI) 프로브 설정

패시브 ID 서비스에 대해 Active Directory와 WMI를 구성하려면 Passive ID Work Center Wizard(패시브 ID 작업 센터 마법사)(PassiveID(패시브 ID) 설정 시작하기 , 591 페이지 참조)를 사용하거나 아래 단계를 따르십시오.

1. Active Directory 도메인을 구성합니다. Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입, 549 페이지를 참조하십시오.
2. AD 로그인 이벤트를 수신하는 WMI 구성 노드(또는 노드 모음)에 대한 Active Directory 도메인 컨트롤러 목록을 생성합니다. 도메인 컨트롤러 추가, 551 페이지를 참조하십시오.
3. ISE와 통합할 수 있도록 Active Directory를 구성합니다. 패시브 ID용 WMI 구성, 554 페이지를 참조하십시오.
4. (선택 사항) Active Directory 제공자 관리, 593 페이지.

자세한 내용은 Easy Connect 및 패시브 ID 서비스 지원을 위한 Active Directory 요건, 570 페이지를 참고하십시오.

PassiveID(패시브 ID) 설정 시작하기

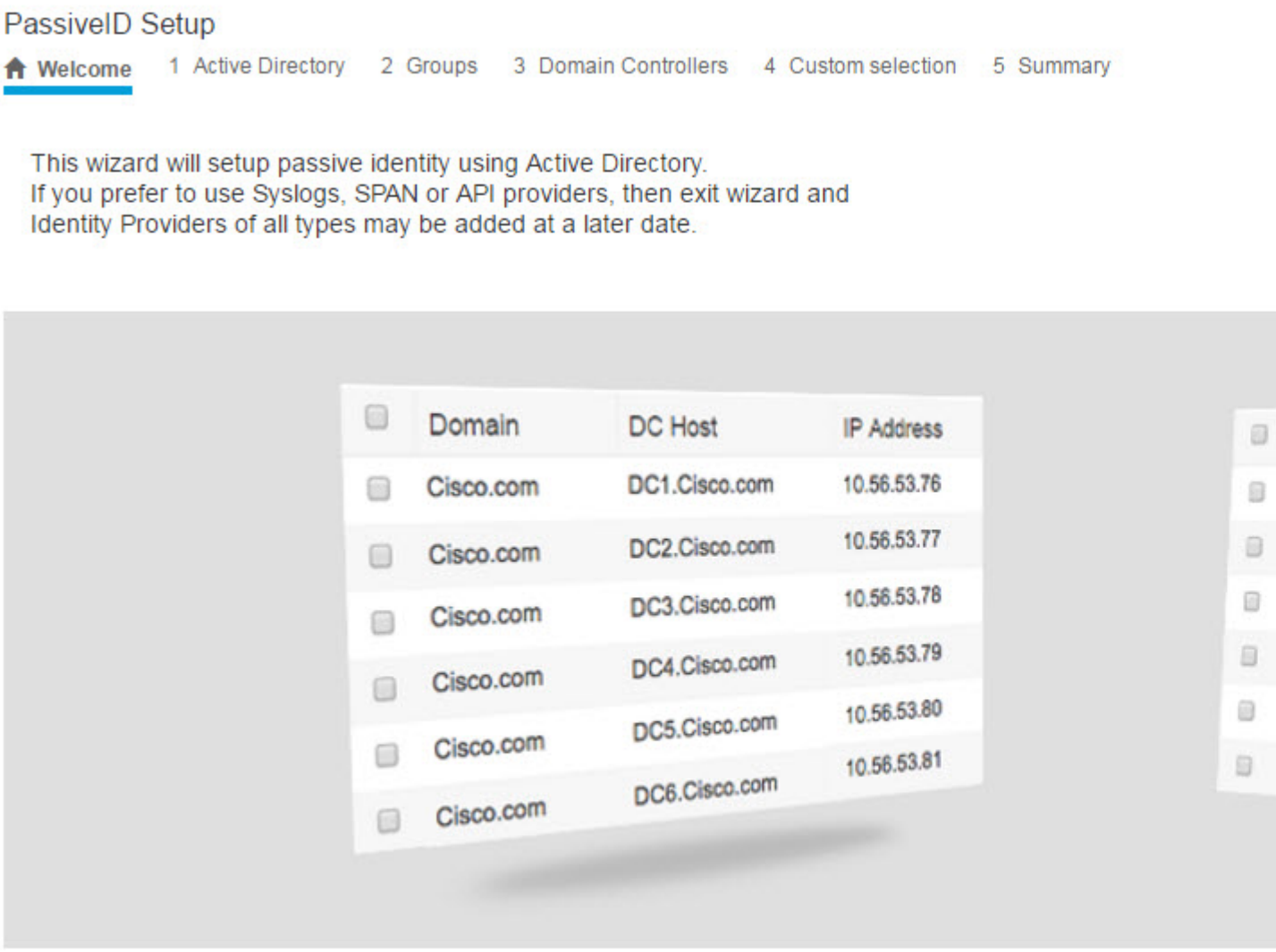
ISE-PIC Active Directory를 첫 번째 사용자 ID 제공자로 쉽고 빠르게 구성하여 Active Directory에서 사용자 ID를 수신할 수 있는 마법사를 제공합니다. ISE-PIC용으로 Active Directory를 구성하면, 나중에 다른 제공자 유형도 쉽게 구성할 수 있습니다. Active Directory를 구성한 후에는 가입자(isco FMC(Firepower Management Center) 또는 Stealthwatch 등)를 구성해야 사용자 데이터를 수신할 클라이언트를 정의할 수 있습니다. 가입자에 관한 자세한 내용은 가입자, 636 페이지 항목을 참조하십시오.

시작하기 전에

- Microsoft Active Directory 서버가 네트워크 주소 변환기 뒤에 배치되지 않고 NAT(Network Address Translation) 주소를 갖지 않는지 확인합니다.
- 가입 작업에 사용되는 Microsoft Active Directory 계정이 유효하며 Change Password on Next Login(다음 로그인 시 비밀번호 변경)을 사용하여 구성되지 않았는지 확인합니다.
- ISE에 슈퍼 관리자 또는 시스템 관리자 권한이 있어야 합니다.
- 패시브 ID 서비스에 사용할 전용 정책 서버(PSN)에서 패시브 ID 및 pxGrid 서비스를 활성화합니다. **Administration(관리)** > **System(시스템)** > **Deployment(구축)**를 선택한 후 노드를 열고 **General Settings(일반 설정)** 아래에서 **Enable Passive Identity Service(패시브 ID 서비스 활성화)** 및 **pxGrid**를 활성화합니다.
- ISE에 DNS(도메인 이름 서버)의 항목이 있는지 확인합니다. ISE에서 클라이언트 머신에 대 한 역방향 조회를 올바르게 구성했는지 확인합니다. 자세한 내용은 다음을 참조하십시오. DNS 서버, 548 페이지

단계 **1** **Work Centers(작업 센터)** > **PassiveID(패시브 ID)**를 선택합니다. Passive Identity Connector Overview(패시브 ID 커넥터 개요) 화면에서 **Passive Identity Wizard(패시브 ID 마법사)**를 클릭합니다.

그림 *25: PassiveID Setup(*패시브 *ID* 설정*)*



단계 **2** **Next(**다음**)**를 클릭하여 마법사를 시작합니다.

단계 **3** 이 Active Directory 조인 포인트의 고유한 이름을 입력합니다. 이 노드가 연결된 Active Directory 도메인의 도메인 이름을 입력하고 Active Directory 관리자의 사용자 이름과 비밀번호를 입력합니다. .

Store credentials(자격 증명 저장**)**는 되도록 선택하는 것이 좋습니다. 관리자의 사용자 이름이나 비밀번호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다.

단계 **4** **Next(**다음**)**를 클릭하여 Active Directory 그룹을 정의하고 포함 및 모니터링할 사용자 그룹을 확인합니다.
Active Directory 사용자 그룹은 이전 단계에서 구성한 Active Directory 조인 포인트에 따라 자동으로 표시됩니다.

단계 **5** **Next(**다음**)**를 클릭합니다. 모니터링할 DC를 선택합니다. Custom(사용자 맞춤화)을 선택했다면 다음 화면에서 모니터링할 특정 DC를 선택합니다. 모두 마쳤으면 **Next(**다음**)**를 클릭합니다.

단계 **6** **Exit(**종료**)**를 클릭하여 마법사를 완료합니다.

다음에 수행할 작업

Active Directory를 초기 제공자로 구성하는 작업이 끝나면, 추가 제공자 유형도 쉽게 구성할 수 있습니다. 자세한 내용은 추가 패시브 ID 서비스 제공자, 596 페이지를 참고하십시오. 나아가 정의한 제공자가 수집하는 사용자 ID 정보를 수신하도록 지정된 가입자를 구성할 수도 있습니다. 자세한 내용은 가입자, 636 페이지를 참고하십시오.

Active Directory 제공자 관리

Active Directory 조인 포인트를 생성하고 구성했다면, 이러한 작업을 이용해 Active Directory 프로브를 관리해야 합니다.

- Active Directory Authentication(인증)용 Test Users(사용자 테스트), 563 페이지
- 노드의 Active Directory 가입 보기, 564 페이지
- Active Directory 문제 진단, 565 페이지
- Active Directory 도메인 탈퇴, 554 페이지
- Active Directory 컨피그레이션 삭제, 564 페이지
- Active Directory 디버그 로그 활성화, 566 페이지

Active Directory 설정

Active Directory(AD)는 사용자 이름과 IP 주소 같은 사용자 정보를 수신할 수 있는 대단히 안전하고 정확한 소스입니다.

조인 포인트를 생성하고 수정하여 Active Directory 프로브를 생성하고 관리하려면 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)** > **Active Directory**를 선택합니다.

자세한 내용은 Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입, 549 페이지를 참고하십시오.

표 ***64: Active Directory*** 조인 포인트 이름 설정 및 도메인 조인 창

필드 이름	설명
조인 포인트 이름	구성한 조인 포인트를 빠르고 쉽게 구분할 수 있는 고유한 이름입니다.
Active Directory 도메인	이 노드가 연결된 Active Directory 도메인의 도메인 이름입니다.

필드 이름	설명
도메인 관리자	관리자 권한이 있는 Active Directory 사용자의 사용자 원이름 또는 사용자 계정 이름입니다.
Password(비밀번호**)**	Active Directory에 구성한 도메인 관리자의 비밀번호입니다.
조직 단위 지정	관리자의 조직 단위 정보를 입력합니다.
자격 증명 저장	**Store credentials(**자격 증명 저장**)**는 되도록 선택하는 것이 좋습니다. 관리자의 사용자 이름이나 비밀번호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다. 엔드포인트 프로브의 경우에는 **Store credentials(**자격 증명 저장**)**를 반드시 선택해야 합니다.

표 ***65: Active Directory*** 조인/탈퇴 창

필드 이름	설명
ISE Node(ISE 노드**)**	설치 내 특정 노드의 URL입니다.
ISE 노드 역할	노드가 설치 내 기본 노드인지 보조 노드인지를 나타냅니다.
Status(상태**)**	노드가 Active Directory 도메인에 적극적으로 가입했는지를 나타냅니다.
도메인 컨트롤러	Active Directory에 가입한 노드의 경우 이 열은 Active Directory 도메인에서 노드가 연결된 특정 도메인 컨트롤러를 나타냅니다.
사이트	Active Directory 포리스트가 ISE에 조인한 경우, 이 필드는 Active Directory Site & Services(Active Directory 사이트 및 서비스) 영역에 표시되는 포리스트 내의 특정 Active Directory 사이트를 나타냅니다.

표 ***66:*** 패시브 ***ID DC(***도메인 컨트롤러***)*** 목록

필드	설명
도메인	도메인 컨트롤러가 있는 서버의 정규화된 도메인 이름입니다.

필드	설명
DC 호스트	도메인 컨트롤러가 있는 호스트입니다.
사이트	Active Directory 포리스트가 ISE에 조인한 경우, 이 필드는 Active Directory Site & Services(Active Directory 사이트 및 서비스) 영역에 표시되는 포리스트 내의 특정 Active Directory 사이트를 나타냅니다.
IP Address(IP 주소**)**	도메인 컨트롤러의 IP 주소.
모니터링	다음 방법 중 하나를 사용하여 Active Directory 도메인 컨트롤러에서 사용자 ID 정보를 모니터링합니다. • WMI: WMI 인프라를 사용하여 Active Directory를 직접 모니터링합니다. • 에이전트 이름: Active Directory에서 사용자 정보를 모니터링하도록 에이전트를 정의한 경우, 에이전트 프로토콜을 선택하고 드롭다운 목록에서 사용할 에이전트를 선택합니다. 에이전트에 관한 자세한 내용은 Active Directory 에이전트, 599 페이지 항목을 참조하십시오.

표 ***67:*** 패시브 ***ID DC(Domain Controller,*** 도메인 컨트롤러***)*** 편집 화면

필드 이름	설명
호스트 **FQDN**	도메인 컨트롤러가 있는 서버의 정규화된 도메인 이름을 입력합니다.
Description(설명**)**	쉽게 식별할 수 있도록 이 도메인 컨트롤러에 관한 고유한 설명을 입력합니다.
사용자 이름	Active Directory에 액세스하는 데 사용하는 관리자의 사용자 이름입니다.
Password(비밀번호**)**	Active Directory에 액세스하는 데 사용하는 관리자의 비밀번호입니다.

필드 이름	설명
Protocol(프로토콜)	다음 방법 중 하나를 사용하여 Active Directory 도메인 컨트롤러에서 사용자 ID 정보를 모니터링합니다. • WMI: WMI 인프라를 사용하여 Active Directory를 직접 모니터링합니다. • 에이전트 이름: Active Directory에서 사용자 정보를 모니터링하도록 에이전트를 정의한 경우, 에이전트 프로토콜을 선택하고 드롭다운 목록에서 사용할 에이전트를 선택합니다. 에이전트에 관한 자세한 내용은 Active Directory 에이전트, 599 페이지 항목을 참조하십시오.

Active Directory 그룹은 Active Directory에서 정의하고 관리하며, 이 탭에서는 이 노드에 가입한 Active Directory의 그룹을 확인할 수 있습니다. Active Directory에 관한 자세한 내용은 https://msdn.microsoft.com/en-us/library/bb742437.aspx 항목을 참조하십시오.

표 ***68: Active Directory*** 고급 설정

필드 이름	설명
기록 간격	이미 수행된 사용자 로그인 정보를 패시브 ID 서비스에서 읽는 시간입니다. 패시브 ID 서비스를 시작하거나 재시작할 때 서비스를 사용할 수 없었던 시간 동안 생성된 이벤트를 확인하려면 이 시간을 설정해야 합니다. 활성 상태인 엔드포인트 프로브는 이 간격의 빈도를 유지합니다.
사용자 세션 에이징 타임	사용자가 로그인할 수 있는 시간입니다. 패시브 ID 서비스는 DC에서 새 사용자 로그인 이벤트를 식별하지만, DC는 사용자가 로그오프할 때는 보고하지 않습니다. 에이징 시간을 설정하면 Cisco ISE는 사용자가 로그인되어 있는 시간 간격을 확인할 수 있습니다.
NTLM 프로토콜 설정	Cisco ISE와 DC 간의 통신 프로토콜로는 NTLMv1 또는 NTLMv2를 선택할 수 있습니다. NTLMv2rk 권장 기본값입니다.

추가 패시브 ID 서비스 제공자

ISE가 서비스에 가입한 고객(가입자)에게 ID 정보를 제공하게 하려면(패시브 ID 서비스) , 먼저 ID 제공자에 연결되는 ISE 프로브를 구성해야 합니다.

매핑되고 ISE에 정보를 적극적으로 전달하는 제공자는 Live Sessions(라이브 세션) 메뉴의 세션 디렉토리에서 확인할 수 있습니다. Live Sessions(라이브 세션)에 관한 자세한 내용은 RADIUS 라이브 세션, 323 페이지 항목을 참조하십시오.

아래 표에는 ISE에서 사용 가능한 모든 제공자 및 프로브 유형에 대한 세부정보가 나와 있습니다. Active Directory에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 590 페이지 항목을 참조하십시오.

다음과 같은 제공자 유형을 정의할 수 있습니다.

표 69: 제공자 유형

제공자 유형(프로브)	설명	소스 시스템(제공자)	기술	수집한 사용자 ID 정보	문서 링크
AD(Active Directory)	대단히 안전하고 정확하며 가장 자주 사용하는 소스로, 사용자 정보를 수신하는 곳입니다. 프로브로서 AD는 WMI 기술을 이용해, 인증된 사용자 ID를 전달합니다. 프로브로서가 아닌 AD 자체는 다른 프로브가 사용자 데이터를 검색하는 소스 시스템(제공자) 역할을 합니다.	Active Directory 도메인 컨트롤러	WMI	• 사용자 이름 • IP 주소 • 도메인	프로브 및 제공자로서의 Active Directory, 590 페이지
에이전트	Active Directory 도메인 컨트롤러 또는 멤버 서버에 설치된 네이티브 32비트 애플리케이션입니다. 에이전트 프로브는 Active Directory를 사용하여 사용자 ID 정보를 확인하는 신속하고 효율적인 솔루션입니다.		도메인 컨트롤러 또는 멤버 서버에 설치된 에이전트입니다.	• 사용자 이름 • IP 주소 • 도메인	Active Directory 에이전트, 599 페이지
엔드포인트	다른 구성된 프로브와 함께 백그라운드에서 항상 실행되어 사용자가 여전히 연결되어 있는지를 확인합니다.		WMI	사용자가 계속 연결되어 있는지 여부	엔드포인트 프로브, 633 페이지
SPAN			SPAN(스위치에 설치됨) 및 Kerberos 메시지	• 사용자 이름 • IP 주소 • 도메인	SPAN, 609 페이지

제공자 유형(프로브)	설명	소스 시스템(제공자)	기술	수집한 사용자 ID 정보	문서 링크
	네트워크 트래픽을 수신 대기하기 위해 네트워크 스위치에 상주하며, Active Directory 데이터를 기반으로 사용자 ID 정보를 추출합니다.				
API 제공자	ISE가 제공하는 RESTful API 서비스를 이용하여, RESTful API 클라이언트와 통신하도록 프로그래밍된 모든 시스템에서 사용자 ID 정보를 수집합니다.	REST API 클라이언트와 통신하도록 프로그래밍된 모든 시스템입니다.	RESTful API. 가입자에게 전송된 JSON 형식의 사용자 ID.	• 사용자 이름 • IP 주소 • 포트 범위 • 도메인	API Providers(API 제공자), 604 페이지
Syslog	시스템 로그 메시지를 구문 분석하고 MAC 주소를 포함한 사용자 ID를 검색합니다.	• 일반 시스템 로그 메시지 제공자 • DHCP 서버	시스템 로그 메시지	• 사용자 이름 • IP 주소 • MAC 주소 • 도메인	Syslog Providers(시스템 로그 제공자), 611 페이지

Active Directory 에이전트

패시브 ID 서비스 작업 센터는 네이티브 32비트 애플리케이션인 Domain Controller(DC) 에이전트를 Active Directory(AD) 도메인 컨트롤러(DC) 또는 (컨피그레이션에 따라) 멤버 서버에 설치하여 AD에서 사용자 ID 정보를 검색한 다음, 이러한 ID를 사용자가 구성한 가입자에게 전송합니다. 에이전트 프로브는 Active Directory를 사용하여 사용자 ID 정보를 확인하는 신속하고 효율적인 솔루션입니다. 에이전트는 별도의 도메인 또는 AD 도메인에 설치할 수 있으며, 설치한 후에는 1분마다 한 번씩 ISE에 상태 업데이트를 제공합니다.

에이전트는 ISE가 자동으로 설치 및 구성하며, 사용자가 수동으로 설치할 수도 있습니다. 설치하면 다음과 같은 일이 발생합니다.

- 에이전트와 관련 파일이 **`Program Files/Cisco/Cisco ISE PassiveID Agent`** 경로에 설치됩니다.

- 에이전트의 로깅 수준을 보여주는 **PICAgent.exe.config**라는 구성 파일이 설치됩니다. 구성 파일에서 로깅 레벨을 수동으로 변경할 수 있습니다.
- CiscoISEPICAgent.log 파일은 모든 로깅 메시지와 함께 저장됩니다.
- nodes.txt 파일에는 에이전트가 통실할 수 있는 구축 내 모든 노드 목록이 있습니다. 에이전트가 목록의 첫 번째 노드에 접촉합니다. 노드에 접촉할 수 없는 경우 에이전트는 목록의 노드 순서에 따라 계속 통신을 시도합니다. 수동 설치의 경우에는 파일을 열고 노드 IP 주소를 입력해야 합니다. (수동 또는 자동으로) 설치가 끝난 후에는 파일을 변경하려면 수동으로 업데이트해야 합니다. 필요하다면 파일을 열고 노드 IP 주소를 추가, 변경 또는 삭제합니다.
- Cisco ISE PassiveID 에이전트 서비스는 Windows Services 대화 상자에서 관리할 수 있는 머신에서 실행됩니다.
- ISE는 도메인 컨트롤러를 100개까지 지원하며, 각 에이전트는 도메인 컨트롤러를 10개까지 모니터링할 수 있습니다.

참고 도메인 컨트롤러 100개를 모니터링하려면 에이전트 10개를 구성해야 합니다.

참고 Active Directory 에이전트는 Windows Server 2008 이상에서만 지원됩니다.

에이전트를 설치할 수 없는 경우에는 패시브 ID 서비스에 Active Directory 프로브를 사용합니다. 자세한 내용은 프로브 및 제공자로서의 Active Directory, 590 페이지를 참고하십시오.

Active Directory 에이전트 자동 설치 및 구축

도메인 컨트롤러에서 사용자 ID를 모니터링하도록 에이전트 제공자를 구성하는 경우 에이전트를 멤버 서버 또는 도메인 컨트롤러에 설치해야 합니다. 에이전트는 ISE에서 자동으로 설치하거나 사용자가 수동으로 설치할 수 있습니다. 자동 또는 수동 설치 후에는 기본 WMI가 아닌 지정된 도메인 컨트롤러를 모니터링하도록 설치된 에이전트를 구성해야 합니다. 이 프로세스에서는 자동 설치를 활성화하고 도메인 컨트롤러를 모니터링하도록 에이전트를 구성하는 방법을 설명합니다.

시작하기 전에

시작하기 전에

- 서버 측에서 관련 DNS 서버에 대한 역방향 조회를 구성합니다. ISE의 DNS 서버 구성 요구 사항에 관한 자세한 내용은 DNS 서버, 548 페이지 항목을 참조하십시오.
- 에이전트에 지정된 머신에서 Microsoft.NET Framework가 4.0 이상 버전으로 업데이트되었는지 확인합니다. .NET Framework에 대한 자세한 내용은 https://www.microsoft.com/net/framework 항목을 참고하십시오.

- 패시브 ID 및 pxGrid 서비스를 활성화합니다. 자세한 내용은 초기 설정 및 컨피그레이션, 588 페이지를 참고하십시오.
- AD 조인 포인트를 생성하고 하나 이상의 도메인 컨트롤러를 추가합니다. 조인 포인트에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 590 페이지 항목을 참고하십시오.

  AD 사용자 그룹을 AD, 에이전트, SPAN 및 시스템 로그 프로브에 사용합니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성, 556 페이지 항목을 참조하십시오.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Agents(**에이전트**)**를 선택합니다.

단계 **2** 새 에이전트를 추가하려면 표 상단에 있는 **Add(**추가**)**를 클릭합니다.

단계 **3** 새 에이전트를 생성하고 이 구성에서 지정한 호스트에 자동으로 설치하려면 **Deploy New Agent(**새 에이전트 구축**)**를 선택합니다.

단계 **4** 모든 필수 필드를 올바르게 작성하여 클라이언트를 올바르게 구성합니다. 자세한 내용은 Active Directory 에이전트 설정, 603 페이지를 참고하십시오.

단계 **5** **Deploy(**구축**)**를 클릭합니다.
에이전트는 구성에서 지정한 도메인에 따라 호스트에 자동으로 설치되며 설정이 저장됩니다. 이제 에이전트가 Agents(에이전트) 표에도 표시되며 다음 단계에 설명된 대로 지정된 도메인 컨트롤러를 모니터링하는 데 적용 가능합니다.

단계 **6** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Active Directory**를 선택하여 현재 구성된 모든 조인 포인트를 확인합니다.

단계 **7** 생성한 에이전트를 활성화할 조인 포인트의 링크를 클릭합니다.

단계 **8** **Passive ID(**패시브 **ID)** 탭을 선택하여 사전 요건에 따라 추가한 도메인 컨트롤러를 구성합니다.

단계 **9** 생성한 에이전트로 모니터링할 도메인 컨트롤러를 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **10** **Protocol(**프로토콜**)** 드롭다운 목록에서 **Agent(**에이전트**)**를 선택합니다.

단계 **11** **Agent(**에이전트**)** 드롭다운 목록에서 생성한 에이전트를 선택합니다. 에이전트에 대해 생성한 사용자 이름 및 비밀번호 자격 증명(있는 경우)을 입력하고 **Save(**저장**)**를 클릭합니다.

Active Directory 에이전트 수동 설치 및 구축

도메인 컨트롤러에서 사용자 ID를 모니터링하도록 에이전트 제공자를 구성하는 경우 에이전트를 멤버 서버 또는 도메인 컨트롤러에 설치해야 합니다. 에이전트는 ISE에서 자동으로 설치하거나 사용자가 수동으로 설치할 수 있습니다. 자동 또는 수동 설치 후에는 기본 WMI가 아닌 지정된 도메인 컨트롤러를 모니터링하도록 설치된 에이전트를 구성해야 합니다. 이 프로세스에서는 도메인 컨트롤러를 모니터링하도록 에이전트를 수동으로 설치하고 구성하는 방법을 설명합니다.

시작하기 전에

시작하기 전에

- 서버 측에서 관련 DNS 서버에 대한 역방향 조회를 구성합니다. ISE의 DNS 서버 구성 요구 사항에 관한 자세한 내용은 DNS 서버, 548 페이지 항목을 참조하십시오.

- 에이전트에 지정된 머신에서 Microsoft.NET Framework가 4.0 이상 버전으로 업데이트되었는지 확인합니다. .NET Framework에 대한 자세한 내용은 https://www.microsoft.com/net/framework 항목을 참고하십시오.
- 패시브 ID 및 pxGrid 서비스를 활성화합니다. 자세한 내용은 초기 설정 및 컨피그레이션, 588 페이지를 참고하십시오.
- AD 조인 포인트를 생성하고 하나 이상의 도메인 컨트롤러를 추가합니다. 조인 포인트에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 590 페이지 항목을 참고하십시오.

  AD 사용자 그룹을 AD, 에이전트, SPAN 및 시스템 로그 프로브에 사용합니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성, 556 페이지 항목을 참조하십시오.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Agents(**에이전트**)**를 선택합니다.

단계 **2** **Download Agent(**에이전트 다운로드**)**를 클릭하여 수동 설치를 위한 **`pxagent-installer.zip`** 파일을 다운로드합니다.
파일은 기본 Windows 다운로드 폴더에 다운로드됩니다.

단계 **3** 지정된 호스트 머신에 zip 파일을 배치하고 설치를 실행합니다.

단계 **4** ISE GUI에서 다시 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Agents(**에이전트**)**를 선택합니다.

단계 **5** 새 에이전트를 구성하려면 표 상단에 있는 **Add(**추가**)**를 클릭합니다.

단계 **6** 호스트 머신에 이미 설치한 에이전트를 구성하려면 **Register Existing Agent(**기존 에이전트 등록**)**를 선택합니다.

단계 **7** 모든 필수 필드를 올바르게 작성하여 클라이언트를 올바르게 구성합니다. 자세한 내용은 Active Directory 에이전트 설정, 603 페이지를 참고하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.
에이전트 설정이 저장됩니다. 이제 에이전트가 Agents(에이전트) 표에도 표시되며 다음 단계에 설명된 대로 지정된 도메인 컨트롤러를 모니터링하는 데 적용 가능합니다.

단계 **9** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Active Directory**를 선택하여 현재 구성된 모든 조인 포인트를 확인합니다.

단계 **10** 생성한 에이전트를 활성화할 조인 포인트의 링크를 클릭합니다.

단계 **11** **Passive ID(**패시브 **ID)** 탭을 선택하여 사전 요건에 따라 추가한 도메인 컨트롤러를 구성합니다.

단계 **12** 생성한 에이전트로 모니터링할 도메인 컨트롤러를 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **13** **Protocol(**프로토콜**)** 드롭다운 목록에서 **Agent(**에이전트**)**를 선택합니다.

단계 **14** **Agent(**에이전트**)** 드롭다운 목록에서 생성한 에이전트를 선택합니다. 에이전트에 대해 생성한 사용자 이름 및 비밀번호 자격 증명(있는 경우)을 입력하고 **Save(**저장**)**를 클릭합니다.

에이전트 제거

자동 또는 수동으로 설치된 에이전트는 Windows에서 직접 쉽게(수동으로) 제거할 수 있습니다.

단계 **1** Windows 대화 상자에서 **Programs and Features(**프로그램 및 기능**)**로 이동합니다.
단계 **2** 설치된 프로그램 목록에서 Cisco ISE PassiveID 에이전트를 찾아 선택합니다.
단계 **3** **Uninstall(**제거**)**을 클릭합니다.

Active Directory 에이전트 설정

서로 다른 DC(Domain Controller)에서 사용자 ID 정보를 검색하고 패시브 ID 서비스 가입자에게 해당 정보를 전달하려면 ISE가 네트워크의 지정된 호스트에 에이전트를 자동으로 설치하도록 허용합니다.

에이전트를 생성 및 관리하려면 **Providers(**제공자**)** > **Agents(**에이전트**)**를 선택합니다. Active Directory 에이전트 자동 설치 및 구축, 600 페이지의 내용을 참조하십시오.

표 ***70: Agents(***에이전트***)*** 창

필드 이름	설명
Name(이름**)**	구성한 에이전트 이름입니다.
Host(호스트**)**	에이전트가 설치된 호스트의 FQDN(Fully Qualified Domain Name)입니다.
Monitoring(모니터링**)**	지정된 에이전트가 모니터링 중인 도메인 컨트롤러의 쉼표로 구분된 목록입니다.

표 ***71:*** 에이전트 신규

필드	설명
새 에이전트 구축 또는 기존 에이전트 등록	• Deploy New Agent(새 에이전트 구축): 지정된 호스트에 새 에이전트를 설치합니다. • Register Existing Agent(기존 에이전트 등록): 호스트에 에이전트를 수동으로 설치한 다음 패시브 ID 서비스의 이 화면에서 해당 에이전트를 구성하여 서비스를 활성화합니다.
Name(이름**)**	에이전트를 쉽게 인식할 수 있는 이름을 입력합니다.
Description(설명**)**	에이전트를 쉽게 인식할 수 있는 설명을 입력합니다.
Host FQDN(호스트 **FQDN)**	이는 에이전트가 설치된(기존 에이전트 등록) 호스트가 설치될(자동 구축) 호스트의 FQDN(Fully Qualified Domain Name)입니다.

필드	설명
User Name(사용자 이름**)**	에이전트를 설치할 호스트에 액세스하려면 사용자 이름을 입력합니다. 패시브 ID 서비스는 이러한 인증서를 사용하여 에이전트를 설치합니다.
Password(비밀번호**)**	에이전트를 설치할 호스트에 액세스하려면 비밀번호를 입력합니다. 패시브 ID 서비스는 이러한 인증서를 사용하여 에이전트를 설치합니다.

API Providers(API 제공자)

Cisco ISE에서 API Providers(API 제공자) 기능을 이용하면 맞춤형 프로그램이나 터미널 서버(TS)-Agent에서 얻은 사용자 ID 정보를 내장된 ISE passive identity services(ISE 패시브 ID 서비스) REST API 서비스로 푸시할 수 있습니다. 이렇게 하면 네트워크에서 프로그램 가능 클라이언트를 맞춤화하여 아무 NAC(Network Access Control) 시스템에서 수집한 사용자 ID를 서비스로 전송할 수 있습니다. 또한 Cisco ISE API 제공자를 이용하면 모든 사용자가 IP 주소는 같지만 고유한 포트에 할당되는 Citrix 서버에서 TS-Agent 같은 네트워크 애플리케이션에 접속할 수 있습니다.

예를 들어 Active Directory(AD) 서버를 대상으로 인증된 사용자의 ID 매핑을 제공하는 Citrix 서버에서 실행하는 에이전트는 REST 요청을 ISE에 전송하여, 새 사용자가 로그인 또는 로그오프할 때마다 사용자 세션을 추가 또는 삭제할 수 있습니다. 그러면 ISE는 클라이언트에서 전달한, IP 주소와 할당된 포트를 포함한 사용자 ID 정보를 얻은 다음 Cisco FMC(Firepower Management Center) 같은 사전 구성한 가입자에 전송합니다.

ISE REST API 프레임워크는 HTTPS 프로토콜로 REST 서비스를 구현하며(클라이언트 인증서 검증 필요 없음), 사용자 ID 정보는 JSON(JavaScript Object Notation) 형식으로 제공됩니다. JSON에 관한 자세한 내용은 http://www.json.org/ 항목을 참조하십시오.

ISE REST API 서비스는 사용자 ID를 구문 분석하고, 이 정보를 포트 범위에 매핑하여 같은 시스템에 동시에 로그인한 사용자를 구분합니다. 포트가 사용자에게 할당될 때마다 API는 ISE에 메시지를 보냅니다.

REST API 제공자 흐름

클라이언트를 ISE의 제공자로 선언하고 해당하는 맞춤형 프로그램(클라이언트)이 RESTful 요청을 전송할 수 있도록 ISE에서 맞춤형 클라이언트로 이어지는 브리지를 구성하면, ISE REST 서비스는 다음 방식으로 작동하게 됩니다.

1. 클라이언트 인증의 경우 Cisco ISE는 인증 토큰을 요구합니다. 클라이언트 머신의 맞춤형 프로그램은 연락처를 초기화할 때 인증 토큰 요청을 전송하며, 이후에는 이전 토큰이 만료될 때마다 ISE가 이를 알립니다. 요청의 응답으로 토큰이 반환되어 클라이언트와 ISE 서비스 간에 진행 중인 통신을 활성화합니다.
2. 사용자가 네트워크에 로그인하면 클라이언트는 사용자 ID 정보를 검색하고 API Add 명령을 사용하여 ISE REST 서비스에 정보를 게시합니다.
3. Cisco ISE가 사용자 ID 정보를 수신하고 매핑합니다.

4. Cisco ISE가 매핑된 사용자 ID 정보를 가입자에게 전송합니다.
5. 맞춤형 머신은 필요할 때마다 Remove API 호출을 전송하고 전송한 Add 호출의 응답으로 수신한 사용자 ID를 포함하여, 사용자 정보 제거 요청을 전송할 수 있습니다.

ISE에서 REST API Providers(REST API 제공자)를 이용한 작업

ISE에서 REST 서비스를 활성화하려면 다음 단계를 따르십시오.

1. 클라이언트 측을 구성합니다. 자세한 내용은 클라이언트 사용 설명서를 참조하십시오.
2. 패시브 ID 및 pxGrid 서비스를 활성화합니다. 자세한 내용은 초기 설정 및 컨피그레이션, 588 페이지를 참고하십시오.
3. DNS 서버를 올바르게 구성했는지 확인합니다(ISE에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). 의 DNS 서버 구성 요건에 관한 자세한 내용은 DNS 서버, 548 페이지 항목을 참조하십시오.
4. 패시브 ID 서비스용 ISE REST 서비스에 대한 Bridge(브리지)를 구성합니다., 605 페이지를 참조하십시오.

참고 TS-Agent와 함께 작동하도록 API Provider(API 제공자)를 설정하려면, ISE와 에이전트를 연결하는 브리지를 만들 때 TS-Agent를 추가한 다음 TS-Agent 설명서에서 API 호출 전송 관련 정보를 참조하십시오.

5. 인증 토큰을 생성하고 추가 및 제거 요청을 API 서비스에 전송합니다.

패시브 ID 서비스용 ISE REST 서비스에 대한 Bridge(브리지)를 구성합니다.

ISE REST API 서비스가 특정 클라이언트의 정보를 수신하게 하려면, 먼저 Cisco ISE에서 특정 클라이언를 정의해야 합니다. 서로 다른 IP 주소를 사용하여 여러 REST API 클라이언트를 정의할 수 있습니다.

시작하기 전에

시작하기 전에

- Passive ID(패시브 ID) 및 pxGrid 서비스를 활성화해야 합니다. 자세한 내용은 초기 설정 및 컨피그레이션, 588 페이지를 참고하십시오.
- DNS 서버를 올바르게 구성했는지 확인합니다(Cisco ISE에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). Cisco ISE의 DNS 서버 구성 요구 사항에 관한 자세한 내용은 DNS 서버, 548 페이지 항목을 참고하십시오.

단계 1 **Work Centers(작업 센터)** > **PassiveID(패시브 ID)** > **Providers(제공자)**를 선택하고 왼쪽 패널에서 **API Providers(API 제공자)**를 선택합니다.

각 기존 클라이언트에 관한 상태 정보를 포함하는 API Providers(API 제공자) 표가 표시됩니다.

단계 2 새 클라이언트를 추가하려면 표 상단에 있는 **Add(추가)**를 클릭합니다.

단계 3 모든 필수 필드를 올바르게 작성하여 클라이언트를 올바르게 구성합니다. 자세한 내용은 API 제공자 설정, 606 페이지를 참고하십시오.

단계 4 **Submit(제출)**을 클릭합니다.
클라이언트 구성이 저장되고 화면에 업데이트된 API Providers(API 제공자) 표가 표시됩니다. 이제 클라이언트가 ISE REST 서비스에 게시물을 보낼 수 있습니다.

다음에 수행할 작업

ISE REST 서비스에 인증 토큰과 사용자 ID를 게시하도록 사용자 맞춤화 클라이언를 설정합니다. 패시브 ID REST Service로 API Calls(API 호출) 전송, 606 페이지의 내용을 참조하십시오.

패시브 ID REST Service로 API Calls(API 호출) 전송

시작하기 전에

패시브 ID 서비스용 ISE REST 서비스에 대한 Bridge(브리지)를 구성합니다., 605 페이지

단계 1 브라우저의 주소 표시줄에서 Cisco ISE URL을 입력합니다(예: *https://<ise* 호스트 이름 또는 *IP* 주소*>/admin/*).

단계 2 **API Providers(API 제공자)** 창에서 지정하고 구성한 사용자 이름과 비밀번호를 입력합니다. 자세한 내용은 패시브 ID 서비스용 ISE REST 서비스에 대한 Bridge(브리지)를 구성합니다., 605 페이지를 참고하십시오.

단계 3 **Enter** 키를 누릅니다.

단계 4 대상 노드의 URL Address(URL 주소) 필드에 API 호출을 입력합니다.

단계 5 **Send(전송)**을 클릭하여 API 호출을 실행합니다.

다음에 수행할 작업

디양한 API 호출과 관련 스키마 및 결과에 관한 자세한 내용과 세부정보는 API 호출, 607 페이지 항목을 참조하십시오.

API 제공자 설정

참고 전체 API 정의 및 개체 스키마는 다음과 같이 요청 호출을 사용하여 검색할 수 있습니다.

- 전체 API 사양의 경우(wadl)—https://YOUR_ISE:9094/application.wadl
- API 모델 및 개체 스키마의 경우—https://YOUR_ISE:9094/application.wadl/xsd0.xsd

표 *72: API* 제공자 설정

필드	설명
Name(이름)	이 클라이언트를 다른 클라이언트와 쉽고 빠르게 구별할 수 있는 고유한 이름을 입력합니다.
설명	이 클라이언트에 관한 명확한 설명을 입력합니다.
상태	**Enabled(**활성**)**를 선택하면 구성 완료와 동시에 클라이언트가 REST 서비스와 상호작용합니다.
호스트/IP	클라이언트 호스트 머신의 IP 주소를 입력합니다. DNS 서버를 올바르게 구성했는지 확인합니다(ISE에서의 클라이언트 머신에 대한 역방향 조회 구성 포함).
사용자 이름	REST 서비스에 게시할 때 사용할 고유한 사용자 이름을 생성합니다.
Password(비밀번호)	REST 서비스에 게시할 때 사용할 고유한 비밀번호를 생성합니다.

API 호출

Cisco ISE로 패시브 ID 서비스용 사용자 ID 이벤트를 관리하려면 이러한 API 호출을 사용합니다.

목적: 인증 토큰 생성

- 요청

  POST

  https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken

  요청에는 BasicAuth 권한 부여 헤더가 포함되어야 합니다. 이전에 ISE-PIC GUI에서 생성한 API 제공자의 자격 증명을 제공합니다. 자세한 내용은 API 제공자 설정, 606 페이지를 참조하십시오.

- 응답 헤더

  헤더에는 X-auth-access-token이 포함됩니다. 추가 REST 요청을 게시할 때 사용하는 토큰입니다.

- 응답 본문

  HTTP 204 No Content

목적: 사용자 추가

- 요청

  POST

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity

POST 요청 헤더에 X-auth-access-token을 추가합니다(예: 헤더: X-auth-access-token, 값: f3f25d81-3ac5-43ee-bbfb-20955643f6a7).

- 응답 헤더

  201 Created

- 응답 본문

  {

  "user": "<사용자 이름>",

  "srcPatRange": {

  "userPatStart": <사용자 PAT 시작 값>,

  "userPatEnd": <사용자 PAT 종료 값>,

  "patRangeStart": <PAT 범위 시작 값>

  },

  "srcIpAddress": "<src IP 주소>",

  "agentInfo": "<에이전트 이름>",

  "timestamp": "<ISO_8601 형식, 즉 “YYYY-MM-DDTHH:MM:SSZ" >",

  "domain": "<도메인>"

  }

- 메모
  - 위의 json에서 srcPatRange를 제거하면 단일 IP 사용자 바인딩을 생성할 수 있습니다.
  - 응답 본문에는 생성된 사용자 세션 바인딩에 대한 고유 식별자인 'ID'가 포함됩니다. DELETE 요청을 보낼 때 이 ID를 사용하여 제거 대상 사용자를 표시합니다.
  - 이 응답에는 새로 생성된 사용자 세션 바인딩의 URL인 자체 링크도 포함됩니다.

목적: 사용자 제거

- 요청

  DELETE

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

  <id>에는 Add(추가) 응답에서 수신한 ID를 입력합니다.

  DELETE 요청 헤더에 X-auth-access-token 토큰을 추가합니다(예: 헤더: X-auth-access-token, 값: f3f25d81-3ac5-43ee-bbfb-20955643f6a7).

- 응답 헤더

  200 OK

- 응답 본문

응답 본문에는 삭제된 사용자 세션 바인딩 관련 세부정보가 포함됩니다.

SPAN

SPAN은 패시브 ID 서비스Cisco ISE에서 직접 작동하도록 Active Directory를 구성하지 않고도 네트워크를 수신 대기하고 사용자 정보를 검색하도록 Cisco ISE를 빠르고 쉽게 활성화할 수 있는 입니다. SPAN은 네트워크 트래픽을, 특히 Kerberos 메시지를 검사하고 Active Directory에 저장된 사용자 ID 정보를 추출한 다음 정보를 ISE로 전송합니다. 그러면 ISE는 정보를 구문 분석하고, ISE에서 이전에 구성한 가입자에게 사용자 이름, IP 주소와 도메인 이름을 최종 전달합니다.

SPAN이 네트워크를 수신 대기하고 Active Directory 사용자 정보를 추출하려면, ISE와 Active Directory 모두가 네트워크에서 같은 스위치에 연결되어야 합니다. 이렇게 하면 SPAN은 Active Directory에서 모든 사용자 ID 데이터를 복사하고 미러링할 수 있습니다.

SPAN을 사용하면 사용자 정보를 다음 방법으로 검색합니다.

1. 사용자 엔드포인트에서 네트워크에 로그인합니다.
2. 로그인 및 사용자 데이터가 Kerberos 메시지에 저장됩니다.
3. 사용자가 로그인하고 사용자 데이터가 스위치를 통과하면, SPAN이 네트워크 데이터를 미러링합니다.
4. Cisco ISE가 네트워크에서 사용자 정보를 수신 대기하고 스위치에서 미러링된 데이터를 검색합니다.
5. Cisco ISE가 사용자 정보를 구문 분석하고 패시브 ID 매핑을 업데이트합니다.
6. Cisco ISE가 구문 분석된 사용자 정보를 가입자에게 전달합니다.

SPAN으로 작업

시작하기 전에

ISE가 네트워크 스위치에서 SPAN 트래픽을 수신하도록 설정하려면 먼저 스위치를 수신 대기할 노드와 노드 인터페이스를 정의해야 합니다. 설치된 서로 다른 ISE 노드를 SPAN이 수신 대기하도록 구성할 수 있습니다. 각 노드에 대해 하나의 인터페이스만 네트워크를 수신하도록 구성할 수 있으며, 수신하는 데 사용되는 인터페이스는 SPAN 전용이어야 합니다.

시작하기 전에 Passive ID(패시브 ID) 및 pxGrid 서비스를 활성화해야 합니다. SPAN 구성에 사용 가능한 인터페이스 목록에는 패시브 ID가 활성화된 노드만 나타납니다. 자세한 내용은 초기 설정 및 컨피그레이션, 588 페이지를 참고하십시오.

또한 다음을 수행해야 합니다.

- 네트워크에 Active Directory가 구성되어 있는지 확인합니다.
- 스위치가 ISE와 통신할 수 있도록, Active Directory에도 연결된 네트워크의 스위치에서 CLI를 실행합니다.
- AD에서 네트워크를 미러링하도록 스위치를 구성합니다.

- SPAN용 전용 ISE NIC(네트워크 인터페이스 카드)를 구성합니다. 이 NIC는 SPAN 트래픽에만 사용됩니다.
- SPAN 전용 NIC가 명령줄 인터페이스를 통해 활성화되었는지 확인합니다.
- Kerberos 트래픽만 SPAN 포트로 전송하는 VACL을 생성합니다.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 창에서 **SPAN**을 선택해 SPAN을 구성합니다.

단계 **2** 참고 GigabitEthernet0 NIC(네트워크 인터페이스 카드)는 계속 사용 가능한 상태로 유지하고 SPAN 구성 시에는 사용 가능한 다른 NIC를 선택하는 것이 좋습니다. GigabitEthernet0은 시스템 관리 목적으로 사용됩니다.

의미 있는 설명(선택 사항)을 입력하고 **Enabled(**활성화됨**)** 상태를 선택한 다음 네트워크 스위치를 수신하는 데 사용할 노드 및 관련 NIC를 선택합니다. 자세한 내용은 SPAN 설정, 610 페이지를 참고하십시오.

단계 **3** **Save(**저장**)**를 클릭합니다.
SPAN 컨피그레이션이 저장되고 ISE가 현재 네트워크 트래픽을 수신 대기하고 있습니다.ISE-PIC

SPAN 설정

구축한 각 노드에서 클라이언트 네트워크에 SPAN을 설치하여, ISE가 사용자 ID를 수신하도록 빠르고 쉽게 구성합니다.

표 ***73: SPAN*** 설정

필드	설명
Description(설명**)**	현재 활성화된 노드 및 인터페이스를 구별할 수 있는 고유한 설명을 입력합니다.
Status(상태**)**	**Enabled(**활성**)**를 선택하면 구성 완료와 동시에 클라이언트를 활성화합니다.
인터페이스 **NIC**	ISE에 설치된 노드를 하나 이상 선택한 다음, 선택한 각 노드에 대해 네트워크 정보를 수신할 노드 인터페이스를 선택합니다. 참고 GigabitEthernet0 NIC는 사용 가능한 상태로 유지하고 SPAN 구성에는 사용 가능한 다른 NIC를 선택하는 것이 좋습니다. GigabitEthernet0은 시스템 관리 목적으로 사용됩니다.

Syslog Providers(시스템 로그 제공자)

패시브 ID 서비스 (InfoBlox, Blue Coat, BlueCat, Lucent 등의 제공자가 보낸) 일반 시스템 로그와 DHCP 시스템 로그 메시지를 포함한 시스템 메시지를 전달하는 클라이언트(ID 데이터 제공자)가 보낸 시스템 로그 메시지를 구문 분석하고, MAC 주소를 포함한 사용자 ID 정보를 다시 전송합니다. 그러면 매핑된 사용자 ID 데이터가 가입자에게 전달됩니다.

사용자 ID 데이터를 수신할 시스템 로그 클라이언트를 지정할 수 있습니다(시스템 로그 클라이언트 구성, 611 페이지 참고). 제공자를 구성할 때 관리자는 연결 방법(TCP 또는 UDP)과 구문 분석에 사용할 시스템 로그 템플릿을 지정해야 합니다.

참고

TCP가 구성된 연결 유형이며 메시지 헤더에 문제가 있어 호스트 이름을 구문 분석할 수 없다면, ISE는 패킷에서 수신한 IP 주소를 ISE의 시스템 로그 메시지에 구성된 제공자 목록에 있는 IP 주소와 일치시킵니다. 이 목록을 보려면 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)** > **Syslog Providers(**시스템 로그 제공자**)**를 선택합니다. 구문 분석 성공을 보장하려면 메시지 헤더를 확인하고 필요하다면 사용자 맞춤화하는 것이 좋습니다. 헤더 사용자 맞춤화에 관한 자세한 내용은 시스템 로그 헤더 사용자 맞춤화, 618 페이지 항목을 참조하십시오.

시스템 로그 프로브는 수신한 메시지를 ISE 구문 분석기로 전송하고, 구문 분석기는 사용자 ID 정보를 매핑한 다음 정보를 ISE에 게시합니다. 그런 다음 ISE가 구분 분석과 매핑이 끝난 사용자 ID 정보를 패시브 ID 서비스 가입자에게 전달합니다.

ISE-PIC ISE에서 사용자 ID의 시스템 로그 메시지를 구문 분석하려면 다음을 수행하십시오.

- 사용자 ID 데이터를 받을 시스템 로그 클라이언트를 구성합니다. 시스템 로그 클라이언트 구성, 611 페이지의 내용을 참조하십시오.
- 단일 메시지 헤더를 사용자 맞춤화합니다. 시스템 로그 헤더 사용자 맞춤화, 618 페이지의 내용을 참조하십시오.
- 템플릿을 생성하여 메시지 본문을 사용자 맞춤화합니다. 시스템 로그 메시지 본문 사용자 맞춤화, 617 페이지의 내용을 참조하십시오.
- 시스템 로그 클라이언트를 구성할 때 ISE에서 미리 정의한 메시지 템플릿을 구문 분석용으로 사용하는 메시지 템플릿으로 사용하거나, 이러한 사전 정의 템플릿에서 사용자 맞춤화한 헤더나 본문 템플릿을 기반으로 사용합니다. 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지의 내용을 참조하십시오.

시스템 로그 클라이언트 구성

Cisco ISE가 특정 클라이언트에서 시스템 로그 메시지를 수신하게 하려면, 먼저 Cisco ISE에서 특정 클라이언를 정의해야 합니다. 여러 IP 주소를 사용하여 여러 공급자를 정의할 수 있습니다.

시작하기 전에

시작하기 전에 Passive ID(패시브 ID) 및 pxGrid 서비스를 활성화해야 합니다. 자세한 내용은 초기 설정 및 컨피그레이션, 588 페이지를 참고하십시오.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Syslog Providers(**시스템 로그 제공자**)**를 선택합니다.
각 기존 클라이언트에 관한 상태 정보를 포함하는 Syslog Providers(시스템 로그 제공자) 표가 표시됩니다.

단계 **2** 새 시스템 로그 클라이언트를 구성하려면 표 상단에 있는 **Add(**추가**)**를 클릭합니다.

단계 **3** 모든 필수 필드를 작성하고(자세한 내용은 시스템 로그 설정, 612 페이지 항목 참조) 필요하다면 메시지 템플릿을 생성하여(자세한 내용은 시스템 로그 메시지 본문 사용자 맞춤화, 617 페이지 항목 참조) 클라이언트를 올바르게 구성합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

시스템 로그 설정

특정 클라이언트가 보내는 시스템 로그 메시지를 이용해 사용자 IDMAC 주소 포함)를 수신하도록 Cisco ISE를 구성합니다. 여러 IP 주소를 사용하여 여러 공급자를 정의할 수 있습니다.

표 ***74: Syslog Providers(***시스템 로그 제공자***)***

필드 이름	설명
Name(이름**)**	구성한 클라이언트를 빠르고 쉽게 구분할 수 있는 고유한 이름을 입력합니다.
Description(설명**)**	이 시스템 로그 제공자에 대한 유의미한 설명입니다.
Status(상태**)**	**Enabled(**활성**)**를 선택하면 구성 완료와 동시에 클라이언트를 활성화합니다.
Host(호스트**)**	호스트 머신의 FQDN을 입력합니다.

필드 이름	설명
Connection Type(연결 유형**)**	UDP 또는 TCP를 입력하여 ISE가 시스템 로그 메시지를 수신 대기하는 채널을 표시합니다. 참고 TCP가 구성된 연결 유형이며 메시지 헤더에 문제가 있어 호스트 이름을 구문 분석할 수 없다면, Cisco ISE는 패킷에서 수신한 IP 주소를 Cisco ISE의 Syslog(시스템 로그) 메시지에 구성된 제공자 목록에 있는 IP 주소와 일치시킵니다. 이 목록을 보려면 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)** > **Syslog Providers(**시스템 로그 제공자**)** 를 선택합니다. 구문 분석 성공을 보장하려면 메시지 헤더를 확인하고 필요하다면 사용자 맞춤화하는 것이 좋습니다. 헤더 사용자 맞춤화에 관한 자세한 내용은 시스템 로그 헤더 사용자 맞춤화, 618 페이지 항목을 참조하십시오.

필드 이름	설명
Template(템플릿**)**	

필드 이름	설명
	템플릿은 구문 분석하고, 매핑하고, 전달해야 하는 시스템 로그 메시지 내 정보 부분을 구문 분석기가 식별할 수 있도록 정확한 본문 메시지 구조를 표시합니다. 예를 들어 템플릿은 구문 분석기가 모든 수신 메시지에서 사용자 이름을 찾을 수 있도록, 사용자 이름의 정확한 위치를 표시할 수 있습니다. 이 필드에는 시스템 로그 메시지를 인식하고 올바르게 구문 분석하는 데 사용할 (시스템 로그 메시지 본문용) 템플릿을 표시합니다. 사전 정의된 드롭다운 목록에서 선택하거나 **New(**새로 만들기**)**를 클릭하여 맞춤형 템플릿을 생성합니다. 템플릿 생성에 관한 자세한 내용은 시스템 로그 메시지 본문 사용자 맞춤화, 617 페이지 항목을 참조하십시오. 대부분의 사전 정의 템플릿은 정규식을 사용하며, 맞춤형 템플릿은 반드시 정규식을 사용해야 합니다. 참고 맞춤형 템플릿만 수정하거나 제거할 수 있으며, 드롭다운에 있는 사전 정의된 시스템 템플릿은 수정할 수 없습니다. ISE는 현재 다음과 같은 사전 정의된 DHCP 제공자 템플릿을 제공합니다. • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP 참고 DHCP 시스템 로그 메시지에는 사용자 이름이 포함되지 않습니다. 따라서 이러한 메시지는 구문 분석기에서 바로 전달되지 않으며, ISE는 올바른 구문 분석과 사용자 ID 정보 전달을 위해 (Live Sessionss(라이브 세션)에 표시되는) 로컬 세션 디렉토리에 등록된 사용자를 먼저 확인한 다음 해당 사용자의 IP 주소를 수신된 DHCP 시스템 로그 메시지에 나열된 IP 주소와 일치시킬 수 있습

필드 이름	설명
	니다. DHCP 시스템 로그 메시지에서 수신한 데이터를 현재 로그인한 사용자 중 누구와도 일치시킬 수 없다면, 메시지는 구문 분석되지 않고 사용자 ID가 전달되지 않습니다. Cisco ISE는 다음과 같은 사전 정의된 일반 시스템 로그 제공자 템플릿을 제공합니다. • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN 템플릿에 관한 자세한 내용은 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지 항목을 참조하십시오.
Default Domain(기본 도메인)	도메인이 특정 사용자의 시스템 로그 메시지에서 식별되지 않으면, 모든 사용자에게 도메인이 할당될 수 있도록 이 기본 도메인이 사용자에게 자동으로 할당됩니다. 기본 도메인이나 메시지에서 구문 분석한 도메인을 이용해, 사용자 이름은 username@domain 형식이 되며 사용자 및 사용자 그룹 관련 추가 정보를 얻을 수 있도록 해당 도메인을 포함합니다.

시스템 로그 메시지 구조 사용자 맞춤화(템플릿)

템플릿은 구문 분석하고, 매핑하고, 전달해야 하는 시스템 로그 메시지 내 정보 부분을 구문 분석기가 식별할 수 있도록 정확한 메시지 구조를 표시합니다. 예를 들어 템플릿은 구문 분석기가 모든 수신 메시지에서 사용자 이름을 찾을 수 있도록, 사용자 이름의 정확한 위치를 표시할 수 있습니다. 템플릿은 신규 및 제거 매핑 메시지 모두에서 지원되는 구조를 결정합니다.

Cisco ISE에서는 패시브 ID 구문 분석기에서 사용할 단일 메시지 헤더 및 여러 본문 구조를 사용자 맞춤화할 수 있습니다.

패시브 ID 구문 분석기가 사용자 ID 매핑 추가 메시지인지 제거 메시지인지를 정확하게 식별하고 사용자 세부정보를 올바르게 구문 분석하려면, 템플릿은 사용자 이름, IP 주소, MAC 주소와 도메인의 구조를 정의하는 정규식을 포함해야 합니다.

메시지 템플릿을 사용자 맞춤화할 때 사전 정의된 옵션 내에서 사용되는 정규식 및 메시지 구조를 참조하여 ISE-PIC ISE에 미리 정의된 메시지 템플릿을 기반으로 사용자 맞춤화를 수행할 수 있습니다. 사전 정의된 템플릿 정규식, 메시지 구조, 예제 등에 대한 자세한 내용은 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지을 참조하십시오.

다음을 사용자 맞춤화할 수 있습니다.

- 단일 메시지 헤더—시스템 로그 헤더 사용자 맞춤화, 618 페이지
- 복수 메시지 본문—시스템 로그 메시지 본문 사용자 맞춤화, 617 페이지

참고 DHCP 시스템 로그 메시지에는 사용자 이름이 포함되지 않습니다. 따라서 이러한 메시지는 구문 분석기에서 바로 전달되지 않으며, ISE는 올바른 구문 분석과 사용자 ID 정보 전달을 위해 (Live Sessionss(라이브 세션)에 표시되는) 로컬 세션 디렉토리에 등록된 사용자를 먼저 확인한 다음 해당 사용자의 IP 주소를 수신된 DHCP 시스템 로그 메시지에 나열된 IP 주소와 일치시킬 수 있습니다. DHCP 시스템 로그 메시지에서 수신한 데이터를 현재 로그인한 사용자 중 누구와도 일치시킬 수 없다면, 메시지는 구문 분석되지 않고 사용자 ID가 전달되지 않습니다.

DHCP 메시지를 올바르게 일치, 구문 분석 및 매핑하는 데 필요한 지연은 사용자 맞춤화 템플릿에는 적용되지 않으며, 따라서 DHCP 메시지 템플릿 사용자 맞춤화은 권장하지 않습니다. 대신 사전 정의된 DHCP 템플릿 중 하나를 사용하십시오.

시스템 로그 메시지 본문 사용자 맞춤화

Cisco ISE를 이용하면 (메시지 본문을 사용자 맞춤화하여) 자체 시스템 로그 메시지 템플릿을 패시브 ID 구문 분석기로 구문 분석하도록 사용자 맞춤화할 수 있습니다. 템플릿에는 사용자 이름, IP 주소, MAC 주소 및 도메인의 구조를 정의하는 정규식이 포함되어야 합니다.

참고 DHCP 시스템 로그 메시지에는 사용자 이름이 포함되지 않습니다. 따라서 이러한 메시지는 구문 분석기에서 바로 전달되지 않으며, Cisco ISE는 올바른 구문 분석과 사용자 ID 정보 전달을 위해 (Live Sessionss(라이브 세션)에 표시되는) 로컬 세션 디렉토리에 등록된 사용자를 먼저 확인한 다음, IP 주소를 기준으로 사용자를 수신한 DHCP 시스템 로그 메시지에 나열된 IP 주소와 일치시킬 수 있습니다. DHCP 시스템 로그 메시지에서 수신한 데이터를 현재 로그인한 사용자 중 누구와도 일치시킬 수 없다면, 메시지는 구문 분석되지 않고 사용자 ID가 전달되지 않습니다.

DHCP 메시지를 올바르게 일치, 구문 분석 및 매핑하는 데 필요한 지연은 사용자 맞춤화 템플릿에는 적용되지 않으며, 따라서 DHCP 메시지 템플릿 사용자 맞춤화은 권장하지 않습니다. 대신 사전 정의된 DHCP 템플릿 중 하나를 사용하십시오.

시스템 로그 클라이언트 구성 화면에서 시스템 로그 메시지 본문 템플릿을 생성하고 수정합니다.

참고 본인의 사용자 맞춤화 템플릿만 수정할 수 있습니다. 시스템에서 제공하는 사전 정의된 템플릿은 수정할 수 없습니다.

단계 1 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Syslog Providers(**시스템 로그 제공자**)**를 선택합니다.
각 기존 클라이언트에 관한 상태 정보를 포함하는 Syslog Providers(시스템 로그 제공자) 표가 표시됩니다.

단계 2 **Add(**추가**)**를 클릭하여 새 시스템 로그 클라이언트를 추가 하거나 **Edit(**수정**)**을 클릭하여 이미 구성된 클라이언트를 업데이트합니다. 시스템 로그 클라이언트 구성 및 업데이트에 관한 자세한 내용은 시스템 로그 클라이언트 구성, 611 페이지를 참조하십시오.

단계 3 **Syslog Providers(**시스템 로그 제공자**)** 창에서 **New(**새로 만들기**)**를 클릭하여 새 메시지 템플릿을 생성합니다. 기존 템플릿을 수정하려면 드롭다운 목록에서 템플릿을 선택하고 **Edit(**수정**)**를 클릭합니다.

단계 4 모든 필수 필드를 작성합니다.

올바른 값을 입력하는 자세한 방법은 시스템 로그 맞춤형 템플릿 설정 및 예시, 619 페이지 항목을 참조하십시오.

단계 5 **Test(**테스트**)**를 클릭하여, 입력된 문자열을 바탕으로 메시지가 올바르게 구문 분석되었는지 확인합니다.

단계 6 **Save(**저장**)**를 클릭합니다.

시스템 로그 헤더 사용자 맞춤화

시스템 로그 헤더에는 메시지가 생성된 호스트 이름도 포함됩니다. 시스템 로그 메시지를 Cisco ISE 메시지 구문 분석기가 인식하지 못한다면, 호스트 이름 앞에 오는 구분 기호를 구성하여 메시지 헤더를 사용자 맞춤화해야 Cisco ISE가 호스트 이름을 인식하고 메시지를 올바르게 구문 분석할 수 있습니다. 이 화면의 필드에 관한 자세한 내용은 시스템 로그 맞춤형 템플릿 설정 및 예시, 619 페이지 항목을 참조하십시오. 사용자 맞춤화 헤더 구성이 저장되며, 메시지가 수신될 때마다 구문 분석기에서 사용하는 헤더 유형에 추가됩니다.

참고 헤더 하나만 사용자 맞춤화할 수 있습니다. 헤더를 사용자 맞춤화한 후 **Custom Header(**사용자 맞춤화 헤더**)**를 클릭하고 템플릿을 생성하면 최신 구성만 저장됩니다.

단계 1 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Syslog Providers(**시스템 로그 제공자**)**를 선택합니다.
각 기존 클라이언트에 관한 상태 정보를 포함하는 Syslog Providers(시스템 로그 제공자) 표가 표시됩니다.

단계 2 **Custom Header(**사용자 맞춤화 헤더**)**를 클릭하여 Syslog Custom Header(시스템 로그 사용자 맞춤화 헤더)를 엽니다.

단계 3 **Paste sample syslog(**시스템 로그 예 붙여넣기**)**에 시스템 로그 메시지의 헤더 형식 예를 입력합니다. 예를 들어 다음 메시지 중 하나에서 이 헤더를 복사하여 붙여넣습니다. `< 181 > Oct 10 15:14:08 Cisco.com`

단계 **4** **Separator(**구분자**)** 필드에서 단어를 공백과 탭 중 무엇으로 구분할지를 지정합니다.

단계 **5** **Position of hostname in header(**헤더 내 호스트 이름 위치**)**필드에서 호스트 이름 내 헤더 위치를 지정합니다. 예를 들어 위의 헤더에서 호스트 이름은 헤더의 네 번째 단어입니다. 4를 입력하여 이를 표시합니다.

Hostname(호스트 이름**)** 필드는 처음 3개 필드에 표시된 세부정보를 기반으로 호스트 이름을 표시합니다. 예를 들어 **Paste sample syslog(**시스템 로그 예 붙여넣기**)**의 헤더 예가 다음과 같다면

<181>Oct 10 15:14:08 Cisco.com

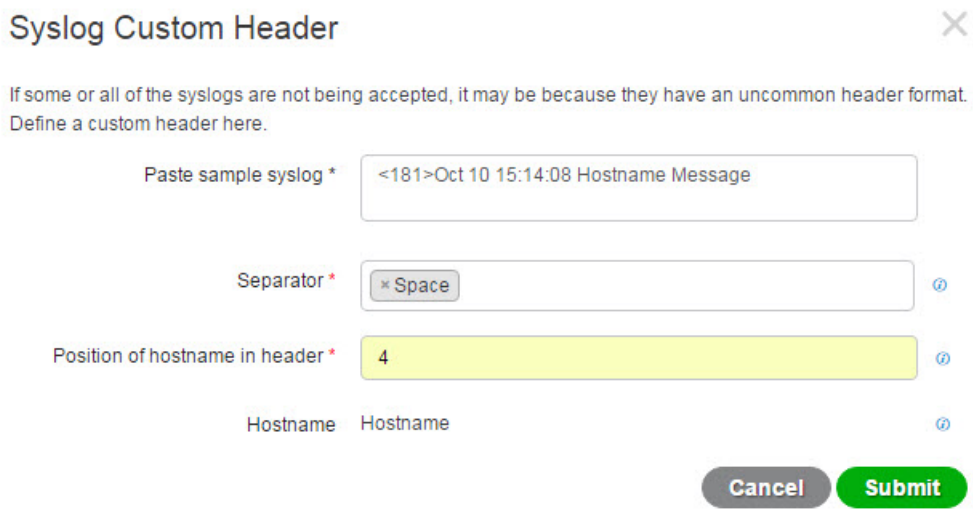
구분 기호는 공백으로 표시되며 헤더 내 호스트 이름 위치는 4로 입력됩니다.

Hostname(호스트 이름**)**은 **Paste sample syslog(**시스템 로그 예 붙여넣기**)** 필드에 붙여넣인 헤더 문구의 네 번째 단어인 Cisco.com으로 자동으로 표시됩니다.

호스트 이름이 잘못 표시된다면 **Seperator(**구분자**)** 및 **(Position of hostname in header(**헤더 내 호스트 이름 위치**)** 필드에 입력한 데이터를 확인하십시오.

이 예시는 다음 화면 캡처처럼 표시됩니다.

그림 ***26:*** 시스템 로그 헤더 사용자 맞춤화



단계 **6** **Submit(**제출**)**을 클릭합니다.
사용자 맞춤화 헤더 구성이 저장되며, 메시지가 수신될 때마다 구문 분석기에서 사용하는 헤더 유형에 추가됩니다.

시스템 로그 맞춤형 템플릿 설정 및 예시

Cisco ISE를 이용하면 자체 시스템 로그 메시지 템플릿을 패시브 ID 구문 분석기로 구문 분석하도록 사용자 맞춤화할 수 있습니다. 맞춤형 템플릿은 신규 및 제거 매핑 메시지 모두에서 지원되는 구조를 결정합니다. 패시브 ID 구문 분석기가 사용자 ID 매핑 추가 메시지인지 제거 메시지인지를 정확하게 식별하고 사용자 세부정보를 올바르게 구문 분석하려면, 템플릿은 사용자 이름, IP 주소, MAC 주소와 도메인의 구조를 정의하는 정규식을 포함해야 합니다.

참고 대부분의 사전 정의된 템플릿은 정규식을 사용합니다. 맞춤형 템플릿은 정규식을 사용해야 합니다.

시스템 로그 헤더 부분

호스트 이름 앞에 오는 구분 기호를 구성하면 시스템 로그 프로브에서 인식하는 단일 헤더를 사용자 맞춤화할 수 있습니다.

다음 표에서는 맞춤형 시스템 로그 헤더에 포함될 수 있는 다양한 부분 및 필드를 설명합니다. 정규식에 관한 자세한 내용은 표 77: 맞춤형 템플릿용 정규식, 622 페이지 항목을 참고하십시오.

표 ***75:*** 시스템 로그 맞춤형 헤더

필드	설명
샘플 시스템 로그 붙여넣기	시스템 로그 메시지에 헤더 형식 예를 입력합니다. 예를 들어 이 헤더를 복사하여 붙여넣습니다. **<181>Oct 10 15:14:08** 호스트 이름 메시지
구분자	단어가 공백과 탭 중 무엇으로 구분되는지를 나타냅니다.
헤더 내 호스트 이름 위치	헤더 내 호스트 위치를 표시합니다. 예를 들어 위의 헤더에서 호스트 이름은 헤더의 네 번째 단어입니다. 4를 입력하여 이를 표시합니다.
호스트 이름	처음 3개 필드에 표시된 세부정보를 기반으로 호스트 이름을 표시합니다. 예를 들어 샘플 시스템 로그 붙여넣기에 있는 헤더 예가 다음과 같다면 <181>Oct 10 15:14:08 호스트 이름 메시지 구분 기호는 공백으로 표시되며 헤더 내 호스트 이름 위치는 4로 입력됩니다. 호스트 이름은 자동으로 Hostname으로 표시됩니다. 호스트 이름이 잘못 표시된다면 구분자 및 헤더 내 호스트 이름 위치 필드에 입력한 데이터를 확인하십시오.

메시지 본문에 대한 시스템 로그 템플릿 부분 및 설명

다음 표에서는 맞춤형 시스템 로그 메시지 템플릿에 포함될 수 있는 다양한 부분 및 필드를 설명합니다. 정규식에 관한 자세한 내용은 표 77: 맞춤형 템플릿용 정규식, 622 페이지 항목을 참고하십시오.

표 ***76:*** 시스템 로그 템플릿

부분	필드	설명
	Name(이름)	이 템플릿의 용도를 인식하는 데 사용하는 고유한 이름입니다.
매핑 작업	새 매핑	새 사용자를 추가하기 위해 이 템플릿과 함께 사용하는 매핑 유형을 설명하는 정규식입니다. 예를 들어 F5 VPN에 로그인한 새 사용자를 나타내려면 이 필드에 'logged on from'을 입력합니다.
	제거된 매핑	사용자를 제거하기 위해 이 템플릿과 함께 사용하는 매핑 유형을 설명하는 정규식입니다. 예를 들어 ASA VPN에서 제거해야 하는 사용자를 나타내려면 이 필드에 'session disconnect'를 입력합니다.
사용자 데이터	IP 주소	캡처할 IP 주소를 나타내는 정규식입니다. 예를 들어 Bluecat 메시지의 경우 이 IP 주소 범위 내에서 사용자 ID를 캡처하려면 다음을 입력합니다. (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))
	사용자 이름	캡처할 사용자 이름 형식을 나타내는 정규식입니다.
	도메인	캡처할 도메인을 나타내는 정규식입니다.
	MAC 주소	캡처할 MAC 주소 형식을 나타내는 정규식입니다.

정규식 예

메시지 구문 분석에는 정규식을 사용합니다. 이 섹션에서는 IP 주소, 사용자 이름 및 매핑 추가 메시지를 구문 분석하는 정규식 예를 확인할 수 있습니다.

예를 들어 정규식을 사용하여 다음 메시지를 구문 분석할 수 있습니다.

<174>192.168.0.1 %ASA-4-722051: 그룹 <DfltGrpPolicy> 사용자 <user1> IP <192.168.0.10> IPv4 ㅈ주소 <192.168.0.6> IPv6 주소 <::> 세션에 할당됨

<174>192.168.0.1 %ASA-6-713228: 그룹 = xyz, 사용자 이름 = user1, IP = 192.168.0.12, 할당된 비공개 IP 주소 192.168.0.8 사용자 제거용

정규식은 다음 표에서처럼 정의됩니다.

표 77: 맞춤형 템플릿용 정규식

부분	정규식
IP 주소	주소 <([^\s]+)>|address ([^\s]+)
사용자 이름	사용자 <([^\s]+)>| 사용자 이름 = ([^\s]+)
매핑 메시지 추가	(%ASA-4-722051|%ASA-6-713228)

시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업

시스템 로그 메시지에는 헤더와 메시지 본문을 포함하는 표준 구조가 적용됩니다.

이 섹션에서는 Cisco ISE에서 제공하는 사전 정의 템플릿을 설명하며, 메시지 출처에 따라 지원되는 헤더용 콘텐츠 세부정보와 지원되는 본문 구조도 함께 설명합니다.

또한 시스템에서 사전 정의하지 않은 소스에 대한 맞춤형 본문 콘텐츠를 이용해 자체 템플릿을 만들 수도 있습니다. 이 섹션에서는 맞춤형 템플릿에 지원되는 구조에 대해서도 설명합니다. 메시지를 구문 분석할 때 시스템에 사전 정의된 헤더와 함께 사용할 단일 맞춤형 헤더를 구성할 수 있으며, 메시지 본문용으로 여러 맞춤형 템플릿을 구성할 수 있습니다. 헤더 사용자 맞춤화에 관한 자세한 내용은 시스템 로그 헤더 사용자 맞춤화, 618 페이지 항목을 참조하십시오. 본문 사용자 맞춤화에 관한 자세한 내용은 시스템 로그 메시지 본문 사용자 맞춤화, 617 페이지 항목을 참조하십시오.

참고 대부분의 사전 정의 템플릿은 정규식을 사용하며, 맞춤형 템플릿은 반드시 정규식을 사용해야 합니다.

메시지 헤더

모든 클라이언트 머신의 모든 메시지 유형에 대해, 구문 분석기는 두 가지 헤더 유형(신규 및 제거)을 인식합니다. 두 헤더는 다음과 같습니다.

- <171>호스트 메시지
- <171>Oct 10 15:14:08 호스트 메시지

수신된 헤더는 호스트 이름에 대해 구문 분석됩니다. IP 주소, 호스트 이름 또는 전체 FQDN이 될 수 있습니다.

헤더를 사용자 맞춤화할 수도 있습니다. 헤더를 사용자 맞춤화하는 방법은 시스템 로그 헤더 사용자 맞춤화, 618 페이지 항목을 참조하십시오.

시스템 로그 **ASA VPN** 사전 정의 템플릿

ASA VPN에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 ASA VPN 본문 메시지가 있습니다.

본문 메시지	구문 분석 예
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] 참고 이 메시지 유형의 구문 분석된 IP 주소는 메시지에 표시된 대로 개인 IP 주소입니다.
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] 참고 이 메시지 유형의 구문 분석된 IP 주소는 IPv4 주소입니다.

매핑 제거 본문 메시지

구문 분석기에서 ASA VPN에 대해 지원하는 매핑 제거 메시지는 이 섹션에 설명되어 있습니다.

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[UserA,10.1.1.1]

본문 메시지
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

시스템 로그 **Bluecat** 사전 정의 템플릿

Bluecat에서 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

이 섹션에서 설명한 대로 Bluecat 시스템 로그용 새 매핑에 대해 지원되는 메시지가 나와 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부정보에 대해 구문 분석됩니다.

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

본문
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

매핑 제거 메시지

Bluecat에 대해 알려진 매핑 제거 메시지가 없습니다.

시스템 로그 **F5 VPN** 사전 정의 템플릿

F5 VPN에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 F5 VPN 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부정보에 대해 구문 분석됩니다.

[user=UserA,ip=172.16.0.12]

본문
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

매핑 제거 메시지

현재 지원되는 F5 VPN에 대한 제거 메시지가 없습니다.

Syslog Infoblox 사전 정의 템플릿

Infoblox에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 ASA VPN 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

본문 메시지
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

매핑 제거 메시지

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

- MAC 주소가 포함된 경우:

  [00:0c:29:a2:18:34,10.0.10.100]

- MAC 주소가 포함되지 않은 경우:

  [10.0.10.100]

본문 메시지
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

시스템 로그 **Linux DHCPd3** 사전 정의 템플릿

Linux DHCPd3에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 메시지

다음 표에 설명된 대로 구문 분석기에서 인식하는 다양한 Linux DHCPd3 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

본문 메시지
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

매핑 제거 본문 메시지

이 섹션에서는 구문 분석기에서 Linux DHCPd3에 대해 지원하는 매핑 제거 메시지를 설명합니다.

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[00:0c:29:a2:18:34 ,10.0.10.100]

본문 메시지
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd : DHCPRELEASE of 10.0.10.100 from 00 : 0c : 29 : a2 : 18 : 34 (win10) via eth1

시스템 로그 **MS DHCP** 사전 정의 템플릿

MS DHCP에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 MS DHCP 본문 메시지가 있습니다.

구문 분석기는 수신된 데이터에서 쉼표(,)를 검색하여 데이터를 분할한 후 다음 예와 같이 이러한 형식의 메시지를 구문 분석합니다.

[macAddress=000C29912E5D,ip=10.0.10.123]

본문 메시지
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,0x4D53465420352E30,MSFT,5.0

매핑 제거 본문 메시지

이 섹션에서는 구문 분석기에서 MH DHCP에 대해 지원하는 매핑 제거 메시지를 설명합니다.

구문 분석기는 수신된 데이터에서 쉼표(,)를 검색하여 데이터를 분할한 후 다음 예와 같이 이러한 형식의 메시지를 구문 분석합니다.

[macAddress=000C29912E5D,ip=10.0.10.123]

본문 메시지
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

시스템 로그 **SafeConnect NAC** 사전 정의 템플릿

SafeConnect NAC에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 SafeConnect NAC 본문 메시지는 다양합니다.

본문은 수신된 후에 다음과 같이 사용자 세부정보에 대해 구문 분석됩니다.

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

본문 메시지
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

매핑 제거 메시지

현재 지원되는 안전 연결에 대한 제거 메시지가 없습니다.

시스템 로그 **Aerohive** 사전 정의 템플릿

Aerohive에서 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 Aerohive 본문 메시지가 있습니다.

본문에서 구문 분석된 세부정보에는 사용자 이름 및 IP 주소가 포함됩니다. 구문 분석에 사용되는 정규식은 다음 예와 같습니다.

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

본문은 수신된 후에 다음과 같이 사용자 세부정보에 대해 구문 분석됩니다.

[UserA,10.5.50.52]

본문 메시지
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

매핑 제거 메시지

현재 시스템은 Aerohive에서 매핑 제거 메시지를 지원하지 않습니다.

시스템 로그 **Blue Coat** 사전 정의 템플릿 **-** 기본 프록시**,** 프록시 **SG, Squid** 웹 프록시

시스템은 Blue Coat에 대해 다음 메시지 유형을 지원합니다.

- Bluecoat 메인 프록시
- BlueCoat Proxy SG
- BlueCoat Squid 웹 프록시

Bluecat 메시지에서 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 Blue Coat 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부정보에 대해 구문 분석됩니다.

[UserA, 192.168.10.24]

본문 메시지**(**이 예는 **BlueCoat** 프록시 **SG** 메시지에서 가져온 것임**)**
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

다음 표에서는 새 매핑 메시지용으로 클라이언트별로 사용되는 여러 정규 표현식 구조에 대해 설명합니다.

클라이언트	정규 표현식
Bluecoat 메인 프록시	새 매핑 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:(?:[a-zA-Z0-9]{1,4}:){1,7}[a-zA-Z0-9]{1,4}))\s** 사용자 이름 **\s\-\s([a-zA-Z0-9_]+)\s\-\s**

클라이언트	정규 표현식
BlueCoat Proxy SG	새 매핑 **(\-\sPROXIED){1}** IP **\s(?:[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\s(?:[a-zA-Z0-9]{1,4}:{1,2}){1,7}[a-zA-Z0-9]{1,4}\s([a-zA-Z0-9_]+)\s-** 사용자 이름 **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid 웹 프록시	새 매핑 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\s(?:[a-zA-Z0-9]{1,4}:{1,2}){1,7}[a-zA-Z0-9]{1,4})\sTCP** 사용자 이름 **\s([a-zA-Z0-9\._]+)\s\-\/**

매핑 제거 메시지

매핑 제거 메시지는 Blue Coat 클라이언트에 대해 지원되지만 현재 사용 가능한 예는 없습니다.

다음 표에서는 매핑 제거 메시지용으로 클라이언트별로 사용되는 여러 정규 표현식 구조 예에 대해 설명합니다.

클라이언트	정규 표현식
Bluecoat 메인 프록시	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat Proxy SG	현재 사용 가능한 예가 없습니다.
BlueCoat Squid 웹 프록시	**(TCP_MISS|TCP_NC_MISS){1}**

시스템 로그 **ISE** 및 **ACS** 사전 정의 템플릿

ISE 또는 ACS 클라이언트를 수신할 때 구문 분석기에서는 다음 메시지 유형을 받습니다.

- 인증 통과: ISE 또는 ACS에서 사용자를 인증하면 사용자 세부정보를 포함하여 인증에 성공했음을 알리는 암호 인증 메시지가 표시됩니다. 메시지가 구문 분석되고 사용자 세부정보 및 세션 ID가 해당 메시지에서 저장됩니다.
- Accounting start and accounting update messages (new mapping)(계정 관리 시작 및 계정 관리 업데이트 메시지(새 매핑)): 계정 관리 시작 또는 계정 관리 업데이트 메시지는 Pass Authentication(인증 통과) 메시지에서 저장한 사용자 세부 정보 및 세션 ID로 구문 분석되고 사용자가 매핑됩니다.
- Accounting stop (remove mapping)(계정 관리 중지(매핑 제거)): 사용자 매핑이 시스템에서 삭제됩니다.

ISE 및 ACS에서 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

인증 통과 메시지

다음 메시지는 인증 통과에 대해 지원됩니다.

- 헤더

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  예: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 본문

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=1.1.1.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- 구문 분석 예

  사용자 이름 및 세션 ID만 구문 분석됩니다.

  [UserA,5]

계정 관리 시작**/**업데이트**(**새 매핑**)** 메시지

다음 메시지는 새 매핑에 대해 지원됩니다.

- 헤더

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  예: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 본문

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- 구문 분석 예

  구문 분석된 세부정보에는 사용자 이름, 프레임 IP 주소 및 메시지에 포함된 MAC 주소가 포함됩니다.

  [UserA,10.0.0.16]

매핑 제거 메시지

다음 메시지는 매핑 제거에 대해 지원됩니다.

- 헤더

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

예: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 본문

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- 구문 분석 예

  구문 분석된 세부정보에는 사용자 이름, 프레임 IP 주소 및 메시지에 포함된 MAC 주소가 포함됩니다.

  [UserA,10.0.0.16]

시스템 로그 **Lucent QIP** 사전 정의 템플릿

Lucent QIP에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 622 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 설명된 대로 구문 분석기에서 인식하는 Lucent QIP 본문 메시지는 다양합니다.

이러한 메시지의 정규식 구조는 다음과 같습니다.

DHCP_GrantLease|:DHCP_RenewLease

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[00:0C:29:91:2E:5D,10.0.0.11]

본문 메시지
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

매핑 제거 본문 메시지

이러한 메시지의 정규식 구조는 다음과 같습니다.

Delete Lease:|DHCP Auto Release:

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[10.0.0.11]

본문 메시지
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

패시브 ID 서비스 필터링

이름 또는 IP 주소를 기준으로 특정 사용자를 필터링할 수 있습니다. 예를 들어 엔드포인트를 이용해 일반 관리자를 지원하고자 엔드포인트에 로그인한 IT 서비스 관리자가 있다면, 관리자 활동을 필터링하여 Live Sessions(라이브 세션)에는 표시하지 않고 관련 엔드포인트의 일반 사용자에게만 표시되게 할 수 있습니다. Live Session(라이브 세션)에는 Mapping Filters(매핑 필터)에 의해 필터링되지 않은 패시브 ID 서비스 구성 요소가 표시됩니다. 필터는 필요한 수만큼 추가할 수 있습니다. 필터 사이에는 "OR" 논리 연산자가 적용됩니다. 두 필드를 모두 단일 필터에서 지정하는 경우에는 이러한 필드 사이에 "AND" 논리 연산자가 적용됩니다.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 창에서 **Mapping Filters(**매핑 필터**)**를 선택합니다.

단계 **2** **Providers(**제공자**)** > **Mapping Filters(**매핑 필터**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하고 필터링할 사용자의 사용자 이름 및/또는 IP 주소를 입력한 후에 **Submit(**제출**)**을 클릭합니다.

단계 **4** 현재 모니터링 세션 디렉토리에 로그인되어 있는 필터링되지 않은 사용자를 확인하려면 **Operations(**운영**)** > **RADIUS Livelog(RADIUS** 라이브 로그**)**를 선택합니다.

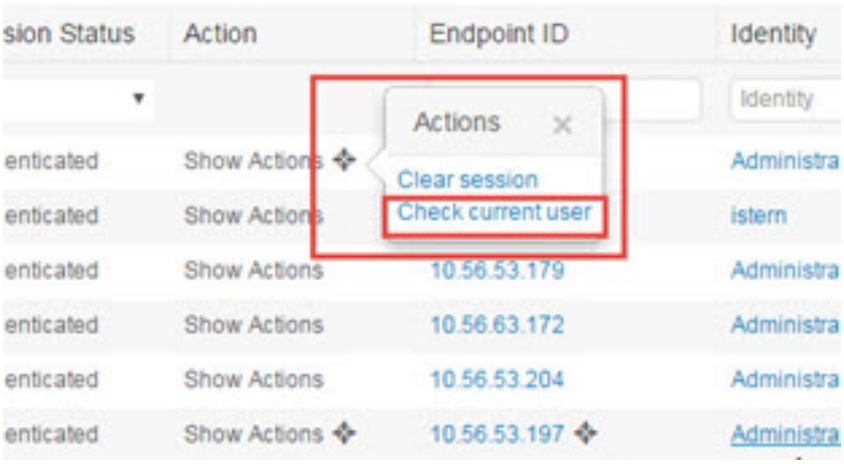
엔드포인트 프로브

사용자가 구성할 수 있는 맞춤형 제공자에 더해, ISE에서 활성화되도록 엔드포인트 프로브를 구성할 수도 있습니다. 단 설치 시 기본적으로 패시브 ID 서비스가 백그라운드에서 항상 실행되어야 합니다. 엔드포인트 프로브는 각 사용자가 여전히 시스템에 로그인해 있는지를 주기적으로 확인합니다.

참고 엔드포인트가 백그라운드에서 실행되게 하려면 먼저 초기 Active Directory 조인 포인트를 구성하고 **Store Credentials(**자격 증명 저장**)**을 선택해야 합니다. 엔드포인트 프로브 구성에 관한 자세한 내용은 엔드포인트 프로브 이용, 634 페이지 항목을 참조하십시오.

엔드포인트 상태를 수동으로 확인하려면 다음 그림에서처럼 **Live Sessions(**라이브 세션**)**로 이동한 다음 **Actions(**작업**)** 열에서 **Show Actions(**작업 표시**)**를 클릭하고 **Check current user(**현재 사용자 확인**)**를 선택합니다.

그림 *27:* 현재 사용자 확인



엔드포인트 사용자 상태에 관한 자세한 정보와 확인을 수동으로 실시하는 방법은 RADIUS 라이브 세션, 323 페이지 항목을 참조하십시오.

엔드포인트 프로브가 사용자가 연결되었음을 인식했고 특정 엔드포인트에 대한 세션이 업데이트된 후 4시간이 지났다면, 엔드포인트 프로브는 사용자가 아직도 로그인한 상태인지 확인하고 다음 데이터를 수집합니다.

- MAC 주소
- 운영체제 버전

확인 결과에 따라 프로브는 다음 작업을 수행합니다.

- 사용자가 여전히 로그인된 상태라면 프로브는 Cisco ISE를 Active User(활성 사용자)로 업데이트합니다.
- 사용자가 로그아웃했다면 세션 상태는 Terminated(종료됨)으로 업데이트되며, 15분이 지나면 사용자는 Session Directory에서 제거됩니다.
- 예를 들어 사용자에게 연락할 수 없을 때 방화벽에서 연결을 차단하거나 엔드포인트가 종료된다면, 상태는 Unreachable(연결 불가)로 업데이트되고 Subscriber(가입자) 정책에 따라 사용자 세션 처리 방법이 결정됩니다. 엔드포인트는 여전히 Session Directory에 남습니다.

엔드포인트 프로브 이용

시작하기 전에

서브넷 범위를 기반으로 엔드포인트 프로브를 생성하고 활성화합니다. PSN별로 엔드포인트 프로브 1개를 생성할 수 있습니다. 엔드포인트 프로브를 사용하려면 먼저 다음 항목을 구성했는지 확인해야 합니다.

- 엔드포인트는 포트 445에 네트워크로 연결되어야 합니다.

- ISE에서 초기 Active Directory 조인 포인트를 구성하고, 프롬프트가 표시되면 **Select Credentials(**자격 증명 선택**)**을 선택합니다. 조인 포인트에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 590 페이지 항목을 참조하십시오.

참고 엔드포인트가 백그라운드에서 실행되게 하려면 먼저 Active Directory 프로브를 완전히 구성하지 않은 경우에도 엔드포인트 프로브를 실행할 수 있도록 초기 Active Directory 조인 포인트를 구성해야 합니다.

단계 **1** **Work Centers(**작업 센터**)** > **Passive ID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 **Endpoint Probes(**엔드포인트 프로브**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하여 새 엔드포인트 프로브를 만듭니다.

단계 **3** 필수 필드를 작성합니다. **Status(**상태**)** 필드에서 **Enable(**활성화**)**을 선택하고 **Submit(**제출**)**을 클릭해야 합니다. 자세한 내용은 엔드포인트 프로브 설정, 635 페이지를 참조하십시오.

엔드포인트 프로브 설정

서브넷 범위를 기반으로 PSN별로 엔드포인트 프로브를 하나씩 생성합니다. 구축에 PSN이 여러 개 있다면 각 PSN을 별도의 서브넷 집합에 할당할 수 있습니다.

표 ***78:*** 엔드포인트 프로브 설정

필드 이름	설명
Name(이름**)**	이 프로브 사용 여부를 식별하는 데 사용하는 고유한 이름을 입력합니다.
Description(설명**)**	이 프로브 사용 방법을 설명하는 고유한 설명을 입력합니다.
Status(상태**)**	이 프로브를 활성화하려면 **Enable(**활성화**)**을 선택합니다.
Host Name(호스트 이름**)**	구축에서 사용 가능한 PSN 목록에서 이 프로브의 PSN을 선택합니다.

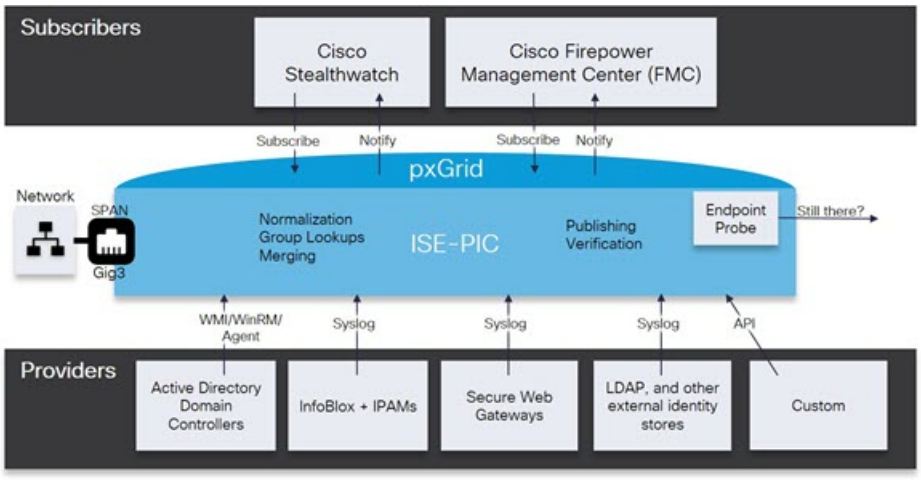
필드 이름	설명
Subnets(서브넷**)**	이 프로브로 확인해야 하는 엔드포인트 그룹의 서브넷 범위를 입력합니다. 표준 서브넷 마스크 범위를 사용하고 쉼표로 서브넷 주소를 구분합니다. 예: 10.56.14.111/32,1.1.1.1/24,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32 각 범위는 고유하며 다른 범위와 구분되어야 합니다. 예를 들어 동일한 프로브에 2.2.2.0/16,2.2.3.0/16을 입력해선 안 됩니다. 서로 겹치는 범위이기 때문입니다.

가입자

패시브 ID 서비스는 Cisco pxGrid 서비스를 사용하여 다양한 제공자로부터 수집하여 Cisco ISE 세션 디렉토리가 저장한 인증된 사용자 ID를 Cisco Stealthwatch나 Cisco FMC(Firepower Management Center) 같은 다른 네트워크 시스템으로 전달합니다.

다음 그림에서 pxGrid 노드는 외부 제공자로부터 사용자 ID를 수집합니다. 이러한 ID는 구문 분석, 매핑 및 형식화됩니다. pxGrid는 형식화된 사용자 ID를 가져와서 패시브 ID 서비스 가입자에게 전송합니다.

그림 ***28:*** 패시브 ***ID*** 서비스 ***Flow***



Cisco ISE에 연결된 가입자는 등록해야 pxGrid 서비스를 사용할 수 있습니다. 가입자는 pxGrid SDK를 통해 Cisco에서 사용 가능한 pxGrid 클라이언트 라이브러리를 채택해야 클라이언트가 될 수 있습니다. 가입자는 고유한 이름과 인증서 기반 상호 인증을 사용하여 pxGrid에 로그인할 수 있습니다. 유효한 인증서를 전송하면, Cisco pxGrid 가입자는 자동으로 ISE에 의해 승인됩니다.

가입자는 pxGrid 서버 호스트 이름 또는 IP 주소에 연결할 수 있습니다. Cisco에서는 불필요한 오류를 방지하기 위해, 특히 DNS 쿼리가 올바르게 작동할 수 있도록 호스트 이름 사용을 권장합니다. 기능

은 가입자가 게시 및 구독할 수 있도록 pxGrid에 생성되는 정보 토픽 또는 채널입니다. Cisco ISE에서는 SessionDirectory 및 IdentityGroup만 지원됩니다. 기능 정보는 **Capabilities(**기능**)** 탭의 **Subscribers(**가입자**)**로 이동하여 게시자로부터 게시, 직접 쿼리 또는 대량 다운로드 쿼리를 통해 사용할 수 있습니다.

가입자가 ISE에서 정보를 수신하게 하려면 다음 작업을 수행해야 합니다.

1. 선택 사항으로, 가입자 측에서 인증서를 생성합니다.
2. PassiveID work center(PassiveID 작업 센터)에서 가입자를 위한 pxGrid 인증서 생성, 637 페이지 작업을 수행합니다.
3. 가입자 활성화, 638 페이지에 전달하는 고성능 고속 어플라이언스입니다. 가입자가 ISE에서 사용자 ID를 수신하게 하려면 이 단계를 수행하거나 승인을 자동으로 활성화해야 합니다. 가입자 설정 구성, 639 페이지의 내용을 참조하십시오.

참고 Cisco ISE 릴리스 3.1부터 모든 pxGrid 연결은 pxGrid 2.0을 기반으로 해야 합니다. pxGrid 1.0 기반(XMPP 기반) 통합은 릴리스 3.1부터 Cisco ISE에서 작동하지 않습니다.

WebSockets를 기반으로 하는 pxGrid 버전 2.0은 Cisco ISE 릴리즈 2.4에서 소개되었습니다. 잠재적인 통합 중단을 방지하려면 다른 시스템을 pxGrid 2.0 호환 버전으로 계획 및 업그레이드하는 것이 좋습니다.

가입자를 위한 **pxGrid** 인증서 생성

시작하기 전에

pxGrid 가입자용 인증서를 생성하여 pxGrid와 가입자 간의 상호 신뢰를 보장하고, 그에 따라 사용자 ID가 ISE에서 가입자로 전달되게 할 수 있습니다. 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Subscribers(**가입자**)**를 선택하고 **Certificates(**인증서**)** 탭으로 이동합니다.

단계 **2** **I want to(**수행할 작업**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)**: 이 옵션을 선택하면 CN(Common Name)을 입력해야 합니다. Common Name(일반 이름) 필드에 pxGrid FQDN을 입력합니다(pxGrid는 접두사로 추가됩니다). (예: www.pxgrid-ise.ise.net) 와일드카드를 사용할 수도 있습니다. (예: *. ise.net)
- **Generate a single certificate with a certificate signing request(**인증서 서명 요청을 사용하여 단일 인증서 생성**)**: 이 옵션을 선택하면 인증서 서명 요청 세부정보를 입력해야 합니다.
- **Generate bulk certificates(**대량 인증서 생성**)**: 필수 세부정보를 포함하는 CSV 파일을 업로드할 수 있습니다.

- **Download Root Certificate Chain(**루트 인증서 체인 다운로드**)**: ISE 공용 루트 인증서를 다운로드하여 pxGrid 클라이언트의 신뢰할 수 있는 인증서 저장소에 추가합니다. ISE pxGrid 노드는 새로 서명한 pxGrid 클라이언트 인증서만 신뢰하며 반대의 경우도 마찬가지라, 외부 인증 기관을 이용하지 않아도 됩니다.

단계 **3** (선택 사항) 이 인증서에 대한 설명을 입력합니다.

단계 **4** 이 인증서가 기반으로 하는 pxGrid 인증서 템플릿을 보거나 수정합니다. 인증서 템플릿은 해당 템플릿을 기준으로 CA(Certificate Authority)에서 발급한 모든 인증서에 일반적인 속성을 포함합니다. 인증서 템플릿은 사용해야 하는 주체, SAN(Subject Alternative Name), 키 크기, SCEP RA 프로파일, 인증서의 유효 기간, 그리고 클라이언트 또는 서버 인증이나 두 인증에 모두 인증서를 사용해야 하는지 여부를 지정하는 EKU(Extended Key Usage: 확장 키 사용)를 정의합니다. 내부 Cisco ISE CA(ISE CA)는 인증서 템플릿을 사용하여 해당 템플릿을 기준으로 인증서를 발급합니다. 이 템플릿을 수정하려면 **Administration(**관리**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Templates(**인증서 템플릿**)**를 선택합니다.

단계 **5** SAN(대체 주체 이름)을 지정합니다. 여러 SAN을 추가해도 됩니다. 다음 옵션을 사용할 수 있습니다.

- **FQDN**: ISE 노드의 정규화된 도메인 이름을 입력합니다. (예: www.isepic.ise.net) FQDN에 와일드카드를 사용할 수도 있습니다. (예: *. ise.net)

  pxGrid FQDN을 입력할 수 있는 FQDN용 추가 회선을 추가할 수 있습니다. Common Name(일반 이름) 필드에 사용한 FQDN과 동일해야 합니다.

- **IP address(IP** 주소**)**: 인증서에 연결할 ISE 노드의 IP 주소를 입력합니다. 가입자가 FQDN 대신 IP 주소를 사용한다면 이 정보를 반드시 입력해야 합니다.

참고 Generate Bulk Certificate(대량 인증서 생성) 옵션을 선택했다면 이 필드는 표시되지 않습니다.

단계 **6** **Certificate Download Format(**인증서 다운로드 형식**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **PEM(Private Enhanced Electronic Mail)** 형식의 인증서**, PKCS8 PEM** 형식의 키**(**인증서 체인 포함**))**: 루트 인증서, 중간 CA 인증서 및 최종 엔티티 인증서는 PEM 형식으로 표시됩니다. PEM 형식 인증서는 BASE64 인코딩 ASCII 파일입니다. 각 인증서는 "--------BEGIN CERTIFICATE-----" 태그로 시작하고 "-------END CERTIFICATE----" 태그로 끝납니다. 최종 엔티티의 개인 키는 PKCS * PEM을 사용하여 저장됩니다. "-----BEGIN ENCRYPTED PRIVATE KEY----" 태그로 시작하고 "-----END ENCRYPTED PRIVATE KEY----" 태그로 끝납니다.

- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)(PKCS12** 형식**(**인증서 체인 포함**,** 인증서 체인과 모두를 위한 단일 파일**))**: 루트 CA 인증서, 중간 CA 인증서, 최종 엔티티의 인증서 및 개인 키를 단일 암호화 파일에 저장하는 이진 형식입니다.

단계 **7** 인증서 비밀번호를 입력합니다.

단계 **8** **Create(**생성**)**를 클릭합니다.

가입자 활성화

가입자가 Cisco ISE에서 사용자 ID를 수신하려면 이 작업을 수행하거나 승인을 자동으로 활성화해야 합니다. 가입자 설정 구성, 639 페이지를 참조하십시오.

시작하기 전에

- Cisco pxGrid 클라이언트에서 요청을 확인하려면 하나 이상의 노드에서 pxGrid 페르소나를 활성화합니다.
- Passive Identity Service를 활성화합니다. 자세한 내용은 Easy Connect, 583 페이지를 참고하십시오.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Subscribers(**가입자**)**를 선택하고 **Clients(**클라이언트**)** 탭이 표시되는지 확인합니다.

단계 **2** 가입자 옆의 확인란을 선택하고 **Approve(**승인**)**를 클릭합니다.

단계 **3** 최신 상태를 보려면 **Refresh(**새로 고침**)**를 클릭합니다.

Live Logs(라이브 로그)에서 가입자 이벤트 보기

Live Logs(라이브 로그) 페이지에는 모든 가입자 이벤트가 표시됩니다. 이벤트 정보에는 이벤트 유형 및 타임스탬프와 함께 가입자 및 기능 이름이 포함됩니다.

Subscribers(가입자**)**로 이동하고 **Live Log(**라이브 로그**)** 탭을 선택하여 이벤트 목록을 확인합니다. 로그를 지우고 목록을 다시 동기화하거나 새로 고칠 수도 있습니다.

가입자 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **Settings(**설정**)**를 선택합니다.

단계 **2** 요건에 따라 다음 옵션을 선택합니다.

- **Automatically Approve New Accounts(**새 계정 자동 승인**)**: 새 pxGrid 클라이언트의 연결 요청을 자동으로 승인하려면 이 확인란을 선택합니다.
- **Allow Password Based Account Creation(**암호 기반 계정 생성 허용**)**: pxGrid 클라이언트에 대해 사용자 이름/암호 기반 인증을 활성화하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 pxGrid 클라이언트를 자동으로 승인할 수 없습니다.

  pxGrid 클라이언트는 REST API를 통해 사용자 이름을 전송하여 pxGrid 컨트롤러에 자체적으로 등록할 수 있습니다. pxGrid 컨트롤러는 클라이언트 등록 중에 pxGrid 클라이언트의 비밀번호를 생성합니다. 관리자는 연결 요청을 승인하거나 거부할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

PassiveID Work Center(패시브 ID 작업 센터)에서의 모니터링 및 문제 해결 PassiveID 작업 센터

이 섹션에서는 모니터링, 문제 해결 및 보고 도구를 사용하여 PassiveID 작업 센터를 관리하는 .

- *Cisco ISE* 관리 가이드*:* 문제 해결의 RADIUS 라이브 세션 섹션을 참조하십시오.
- *Cisco ISE* 관리 가이드*:* 문제 해결의 Cisco ISE 경보 섹션을 참조하십시오.
- *Cisco ISE* 관리 가이드*:* 유지 관리 및 모니터링의 보고서 섹션을 참조하십시오.
- *Cisco ISE* 관리 가이드*:* 문제 해결의 들어오는 트래픽을 검증하는 TCP 덤프 유틸리티 섹션을 참조하십시오.

LDAP

LDAP(Lightweight Directory Access Protocol)는 RFC 2251에 정의된 네트워킹 프로토콜로, TCP/IP를 기반으로 실행되는 디렉토리 서비스를 쿼리하고 수정할 수 있습니다. LDAP는 X.500 기반 디렉토리 서버에 액세스하는 데 사용되는 경량 메커니즘입니다.

Cisco ISE는 LDAP 프로토콜을 사용하여 ID 소스라고도 하는 LDAP 외부 데이터베이스에 통합됩니다.

LDAP 디렉토리 서비스

LDAP 디렉토리 서비스는 클라이언트 서버 모델을 기반으로 합니다. 클라이언트는 LDAP 서버를 연결하고 작업 요청을 서버에 보내어 LDAP 세션을 시작합니다. 그런 다음 서버는 응답을 보냅니다. 하나 이상의 LDAP 서버에는 LDAP 디렉토리 트리 또는 LDAP 백엔드 데이터베이스의 데이터가 있습니다.

디렉토리 서비스는 정보가 포함된 데이터베이스에 해당하는 디렉토리를 관리합니다. 디렉토리 서비스는 정보를 저장하기 위해 분산형 모델을 사용하며 정보는 일반적으로 디렉토리 서버 간에 복제됩니다.

LDAP 디렉토리는 단순 트리 계층으로 구성되며 여러 서버 간에 분산될 수 있습니다. 각 서버에는 전체 디렉토리의 복제된 버전이 있을 수 있으며 이는 정기적으로 동기화됩니다.

트리 항목에는 속성 집합이 있으며, 각 속성에는 이름(속성 유형 또는 속성 설명)과 하나 이상의 값이 있습니다. 속성은 스키마로 정의됩니다.

각 항목에는 고유 식별자, 즉 DN(Distinguished Name)이 있습니다. 이 이름에는 항목의 속성과 상위 항목의 DN으로 구성된 RDN(Relative Distinguished Name)이 있습니다. DN을 전체 파일 이름으로, RDN을 폴더의 상대 파일 이름으로 간주할 수 있습니다.

여러 LDAP 인스턴스

서로 다른 IP 주소 또는 포트 설정을 사용하여 여러 LDAP 인스턴스를 생성하면 여러 LDAP 서버 또는 동일한 LDAP 서버의 여러 데이터베이스를 사용하여 인증하도록 Cisco ISE를 구성할 수 있습니다. 각각의 기본 서버 IP 주소 및 포트 컨피그레이션은 보조 서버 IP 주소 및 포트 컨피그레이션과 함께 하나의 Cisco ISE LDAP ID 소스 인스턴스에 해당하는 LDAP 인스턴스를 형성합니다.

Cisco ISE에서 각 LDAP 인스턴스가 고유한 LDAP 데이터베이스에 해당할 필요는 없습니다. 동일한 데이터베이스에 액세스하기 위해 여러 LDAP 인스턴스를 설정할 수 있습니다. 이 방법은 LDAP 데이터베이스에 사용자 또는 그룹의 서브트리가 여러 개 있는 경우에 유용합니다. 각 LDAP 인스턴스는 사용자와 그룹마다 각각 하나의 서브트리 디렉토리만 지원하므로 Cisco ISE가 인증 요청을 제출하는 각 사용자 디렉토리 및 그룹 디렉토리 서브트리 조합에 대해 별도의 LDAP 인스턴스를 구성해야 합니다.

LDAP 페일오버

Cisco ISE는 기본 LDAP 서버와 보조 LDAP 서버 간 페일오버를 지원합니다. 작동 중지되었거나 연결할 수 없는 이유로 Cisco ISE가 LDAP 서버에 연결할 수 없기 때문에 인증 요청에 실패하는 경우에 페일오버가 발생합니다.

페일오버를 설정한 상태에서 Cisco ISE가 연결하려고 하는 첫 번째 LDAP 서버에 연결할 수 없는 경우 Cisco ISE는 항상 두 번째 LDAP 서버에 연결하려고 시도합니다. Cisco ISE에서 첫 번째 LDAP 서버를 다시 사용하게 하려면 장애 복구 재시도 지연(Failback Retry Delay) 텍스트 상자에 값을 입력해야 합니다.

참고 Cisco ISE는 항상 기본 LDAP 서버를 사용하여 관리 포털에서 권한 부여 정책에 사용할 그룹 및 속성을 가져옵니다. 따라서 이러한 항목을 구성하는 경우 기본 LDAP 서버에 액세스할 수 있어야 합니다. Cisco ISE는 페일오버 컨피그레이션에 따라 런타임에 인증 및 권한 부여를 위해서만 보조 LDAP 서버를 사용합니다.

LDAP 연결 관리

Cisco ISE는 여러 동시 LDAP 연결을 지원합니다. 연결은 처음 LDAP 인증하는 시점에 온디맨드 방식으로 열립니다. 각 LDAP 서버마다 최대 연결 수가 구성되어 있습니다. 연결을 미리 열면 인증 시간이 단축됩니다. 동시 바인딩 연결에 사용할 최대 연결 수를 설정할 수 있습니다. 열린 연결 수는 각 LDAP 서버(기본 또는 보조)마다 다를 수 있으며 각 서버에 구성된 최대 관리 연결 수에 따라 결정됩니다.

Cisco ISE에는 Cisco ISE에 구성된 각 LDAP 서버의 열린 LDAP 연결 목록(바인딩 정보 포함)이 있습니다. 인증 프로세스 중에 연결 관리자는 풀에서 열린 연결을 찾으려고 합니다. 열린 연결이 없으면 새 연결이 열립니다.

LDAP 서버에서 연결이 닫히면 연결 관리자는 디렉토리를 검색하기 위한 첫 번째 호출 중에 오류를 보고하고 연결을 다시 시작하려고 시도합니다. 인증 프로세스가 완료되면 연결 관리자가 연결을 해제합니다.

LDAP 사용자 인증

LDAP를 외부 ID 저장소로 구성할 수 있습니다. Cisco ISE는 일반 비밀번호 인증을 지원합니다. 사용자 인증에는 다음과 같은 작업이 포함됩니다.

- LDAP 서버에서 요청의 사용자 이름과 일치하는 항목 검색
- LDAP 서버에서 발견된 비밀번호를 사용하여 사용자 비밀번호 확인
- 정책에 사용할 그룹의 멤버십 정보 검색
- 정책 및 권한 부여 프로파일에 사용할 지정된 속성 값 검색

Cisco ISE는 사용자 인증을 위해 바인딩 요청을 LDAP 서버에 보냅니다. 바인딩 요청에는 사용자의 DN 및 비밀번호가 일반 텍스트 형식으로 포함되어 있습니다. 사용자의 DN 및 비밀번호가 LDAP 디렉토리의 사용자 이름 및 비밀번호와 일치하면 사용자가 인증됩니다.

Active Directory가 LDAP로 사용되는 경우 UPN 이름이 사용자 인증에 사용됩니다. Sun ONE Directory Server를 LDAP로 사용하는 경우 SAM 이름이 사용자 인증에 사용됩니다.

참고 Cisco ISE는 모든 사용자 인증에 대해 두 개의 searchRequest 메시지를 전송합니다. 이는 Cisco ISE 권한 부여 또는 네트워크 성능에 영향을 주지 않습니다. 두 번째 LDAP 요청은 Ciso ISE가 올바른 ID와 통신하는지 확인하는 것입니다.

참고 Cisco ISE는 DNS 클라이언트로 DNS 응답에서 반환된 첫 번째 IP만 사용하여 LDAP 바인딩을 수행합니다.

SSL(Secure Sockets Layer)을 사용하여 LDAP 서버 연결을 보호하는 것이 좋습니다.

참고 비밀번호가 만료된 후 계정에 대한 유예 로그인이 남아 있는 경우에만 LDAP에 대한 비밀번호 변경이 지원됩니다. 비밀번호 변경이 성공하면 LDAP 서버의 bindResponse는 LDAP_SUCCESS이며, 나머지 유예 로그인 제어 필드를 bindResponse 메시지에 포함합니다. bindResponse 메시지에 추가 제어 필드(남은 유예 로그인 제외)가 포함되어 있으면 Cisco ISE가 메시지를 디코딩하지 못할 수 있습니다.

권한 부여 정책에 사용할 LDAP 그룹 및 속성 검색

Cisco ISE는 디렉토리 서버에 대해 바인딩 작업을 수행하여 주체를 찾아 인증하는 방식으로 LDAP ID 소스에 대해 주체(사용자 또는 호스트)를 인증할 수 있습니다. 인증에 성공한 후에 Cisco ISE는 필요하면 언제든지 그룹과 함께 주체에 속하는 속성을 검색할 수 있습니다. Cisco ISE 관리 포털에서 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**를 선택하여 검색할 속성을 구성할 수 있습니다. Cisco ISE에서 주체에 권한을 부여하는 데 이러한 그룹 및 속성을 사용할 수 있습니다

사용자를 인증하거나 LDAP ID 소스를 쿼리할 때 Cisco ISE는 LDAP 서버에 연결하고 연결 풀을 유지 관리합니다.

Active Directory를 LDAP 저장소로 구성한 경우 그룹 멤버십에 다음과 같은 제한 사항이 적용됩니다.

- 사용자 또는 컴퓨터는 정책 조건에 정의된 그룹의 직접 멤버여야 정책 규칙과 일치될 수 있습니다.
- 정의된 그룹은 사용자 또는 컴퓨터의 기본 그룹이 아닐 수 있습니다. 이 제한 사항은 Active Directory가 LDAP 저장소로 구성된 경우에만 적용됩니다.

LDAP 그룹 멤버십 정보 검색

사용자 인증, 사용자 조회 및 MAC 주소 조회에서 Cisco ISE는 LDAP 데이터베이스에서 그룹 멤버십 정보를 검색해야 합니다. LDAP 서버는 다음 중 한 가지 방법으로 주체(사용자 또는 호스트)와 그룹 간 연결을 나타냅니다.

- Groups Refer to Subjects(그룹이 주체를 참조함): 그룹 객체에 주체를 지정하는 속성이 포함되어 있습니다. 주체 식별자는 그룹에 다음과 같이 제공될 수 있습니다.
  - 고유 이름
  - 일반 사용자 이름
- Subjects Refer to Groups(주체가 그룹을 참조함): 주체 객체에 객체가 속하는 그룹을 지정하는 속성이 포함되어 있습니다.

LDAP ID 소스에는 그룹 멤버십 정보 검색을 위한 다음 매개변수가 포함되어 있습니다.

- Reference direction: 이 매개변수는 그룹 멤버십을 결정(그룹에서 주체로, 또는 주체에서 그룹으로)할 때 사용할 방법을 지정합니다.
- Group map attribute: 이 매개변수는 그룹 멤버십 정보가 들어 있는 속성을 나타냅니다.
- Group object class: 이 매개변수는 특정 객체가 그룹으로 인식되는지를 결정합니다.
- Group search subtree: 이 매개변수는 그룹 검색을 위한 검색 기준을 나타냅니다.
- Member type option: 이 매개변수는 멤버가 그룹 멤버 속성에 저장되는 방식(DN 또는 일반 사용자 이름으로)을 지정합니다.

LDAP 속성 검색

사용자 인증, 사용자 조회 및 MAC 주소 조회의 경우 Cisco ISE는 LDAP 데이터베이스에서 주체 속성을 검색해야 합니다. 각 LDAP ID 소스 인스턴스마다 ID 소스 사전이 생성됩니다. 이러한 사전은 다음과 같은 데이터 형식의 속성을 지원합니다.

- 문자열
- 서명되지 않은 정수 32
- IPv4 주소

서명되지 않은 정수 및 IPv4 속성의 경우 Cisco ISE는 검색된 문자열을 해당 데이터 형식으로 변환합니다. 변환이 실패하거나 속성 값이 검색되지 않으면 Cisco ISE는 디버깅 메시지를 기록하지만 인증 또는 조회 프로세스는 실패하지 않습니다.

변환이 실패하거나 Cisco ISE에서 속성 값이 검색되지 않으면, Cisco ISE가 사용할 수 있는 속성의 기본값을 선택적으로 구성할 수 있습니다.

LDAP 인증서 검색

사용자 조회의 일부로 인증서 검색을 구성한 경우 Cisco ISE는 LDAP에서 인증서 속성 값을 검색해야 합니다. LDAP에서 인증서 속성 값을 검색하려면 이전에 LDAP ID 소스를 구성하면서 액세스하는 속성 목록에서 인증서 속성을 구성해야 합니다.

LDAP 서버에서 반환하는 오류

인증 프로세스 중에는 다음 오류가 발생할 수 있습니다.

- 인증 오류 - Cisco ISE는 Cisco ISE 로그 파일에 인증 오류를 기록합니다.

  LDAP 서버가 바인딩(인증) 오류를 반환할 수 있는 원인은 다음과 같습니다.

  - 매개변수 오류 - 잘못된 매개변수를 입력했습니다.
  - 사용자 계정이 비활성화되었거나 잠겼거나 만료되었거나 비밀번호가 만료되는 등 계정이 제한되었습니다.
  - 초기화 오류 - LDAP 서버 시간 초과 설정을 사용하여 Cisco ISE가 LDAP 서버의 연결 또는 인증이 실패했다고 결정할 때까지 해당 서버에서 응답을 대기해야 하는 시간(초)을 구성합니다.

    LDAP 서버가 초기화 오류를 반환할 수 있는 이유는 다음과 같습니다.

    - LDAP가 지원되지 않습니다.
    - 서버가 다운되었습니다.
    - 서버의 메모리가 부족합니다.
    - 사용자에게 권한이 없습니다.
    - 관리자 자격 증명이 잘못 구성되었습니다.

LDAP 서버에 문제가 있을 수 있음을 나타내는 다음 오류가 외부 리소스 오류로 기록됩니다.

- 연결 오류가 발생했습니다.
- 시간 초과 기간이 만료되었습니다.
- 서버가 다운되었습니다.
- 서버의 메모리가 부족합니다.

다음 오류는 알 수 없는 사용자 오류로 기록됩니다.

- 사용자가 데이터베이스에 없습니다.

다음 오류는 사용자는 있지만 전송된 비밀번호는 잘못되었음을 나타내는 잘못된 비밀번호 오류로 기록됩니다.

- 잘못된 비밀번호를 입력했습니다.

LDAP 사용자 조회

Cisco ISE는 LDAP 서버를 사용한 사용자 조회 기능을 지원합니다. 이 기능을 사용하면 LDAP 데이터베이스에서 사용자를 검색하고 인증 없이 정보를 찾아올 수 있습니다. 사용자 조회 프로세스에는 다음과 같은 작업이 포함됩니다.

- LDAP 서버에서 요청의 사용자 이름과 일치하는 항목 검색
- 정책에 사용할 사용자의 그룹 멤버십 정보 검색
- 정책 및 권한 부여 프로파일에 사용할 지정된 속성 값 검색

LDAP MAC 주소 조회

Cisco ISE는 MAC 주소 조회 기능을 지원합니다. 이 기능을 사용하면 LDAP 데이터베이스에서 MAC 주소를 검색하고 인증 없이 정보를 찾아올 수 있습니다. MAC 주소 조회 프로세스에는 다음과 같은 작업이 포함됩니다.

- LDAP 서버에서 디바이스의 MAC 주소와 일치하는 항목 검색
- 정책에 사용할 디바이스의 MAC 주소 그룹 정보 검색
- 정책에 사용할 지정된 속성 값 검색

LDAP ID 소스 추가

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- Cisco ISE는 항상 기본 LDAP 서버를 사용하여 권한 부여 정책에서 사용할 그룹과 속성을 가져옵니다. 따라서 이러한 항목을 구성할 때 기본 LDAP 서버에 연결할 수 있어야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP** > **Add(**추가**)**를 선택합니다.

단계 **2** 값을 입력합니다.

단계 **3** **Submit(**제출**)**을 클릭하여 LDAP 인스턴스를 생성합니다.

LDAP ID 소스 설정

다음 표에서는 LDAP 인스턴스를 생성하고 해당 인스턴스에 연결하는 데 사용할 수 있는 LDAP ID 소스 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**입니다.

LDAP 일반 설정

다음 표에서는 **General(**일반**)** 탭의 필드에 대해 설명합니다.

표 ***79: LDAP*** 일반 설정

필드 이름	사용 지침
Name(이름**)**	LDAP 인스턴스 이름을 입력합니다. 이 값은 검색에서 주체 DN 및 속성을 가져오는 데 사용됩니다. 값은 문자열 유형이며 최대 길이는 64자입니다.
Description(설명**)**	LDAP 인스턴스에 대한 설명을 입력합니다. 이 값은 문자열 유형이며 최대 길이는 1,024자입니다.
Schema(스키마**)**	다음과 같은 내장 스키마 유형 중 하나를 선택하거나 사용자 맞춤화 스키마를 생성할 수 있습니다. • Active Directory • Sun Directory 서버 • Novell eDirectory Schema(스키마) 옆의 화살표를 클릭하여 스키마 세부정보를 확인할 수 있습니다. 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다.
참고 다음 필드는 사용자 맞춤화 스키마를 선택할 때만 편집할 수 있습니다.	
Subject Objectclass	검색에서 주체 DN 및 속성을 가져오기 위해 사용할 값을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.
Subject Name Attribute(주체 이름 속성**)**	요청의 사용자 이름이 포함된 속성의 이름을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.

필드 이름	사용 지침
Group Name Attribute(그룹 이름 속성**)**	• CN: 공용 이름을 기준으로 LDAP ID 저장소 그룹을 검색하려는 경우 입력합니다. • DN: 고유 이름을 기준으로 LDAP ID 저장소 그룹을 검색하려는 경우 입력합니다.
Certificate Attribute(인증서 속성**)**	인증서 정의를 포함하는 속성을 입력합니다. 인증서 기반 인증의 경우 이러한 정의는 클라이언트가 제공하는 인증서를 검증하는 데 사용됩니다.
Group Objectclass	검색에서 그룹으로 인식되는 객체를 지정하기 위해 사용할 값을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.
Group Map Attribute(그룹 맵 속성**)**	매핑된 정보를 포함하는 속성을 지정합니다. 이 속성은 선택한 참조 방향에 따라 사용자 또는 그룹 속성일 수 있습니다.
Subject Objects Contain Reference To Groups(주체 객체가 그룹에 대한 참조를 포함함**)**	주체 객체가 속한 그룹을 지정하는 속성이 주체 객체에 포함되어 있으면 이 옵션을 클릭합니다.
Group Objects Contain Reference To Subjects(그룹 객체가 주체에 대한 참조를 포함함**)**	그룹 객체가 주체를 지정하는 속성을 포함하고 있으면 이 옵션을 클릭합니다. 이 값이 기본값입니다.
Subjects in Groups Are Stored in Member Attribute As(그룹의 주체가 멤버 속성에 다른 이름으로 저장됨**)**	(**Group Objects Contain Reference To Subjects(**그룹 객체가 주체에 대한 참조를 포함함**)** 옵션을 활성화하는 경우에만 사용 가능함) 그룹 멤버 속성에서 멤버가 제공되는 방법을 지정하며, 기본값은 DN입니다.

필드 이름	사용 지침
User Info Attributes(사용자 정보 속성**)**	기본적으로, 사전 정의된 속성은 다음과 같은 내장 스키마 유형에 대한 사용자 정보(예: 이름, 성, 이메일, 전화 번호, 소재지 등)를 수집하는 데 사용됩니다. • Active Directory • Sun Directory 서버 • Novell eDirectory 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다. 스키마 드롭다운 목록에서 Custom(사용자 맞춤화) 옵션을 선택하여 요건에 따라 사용자 정보 속성을 편집할 수도 있습니다.

LDAP 연결 설정

다음 표에서는 **Connection Settings(**연결 설정**)** 탭의 필드에 대해 설명합니다.

표 ***80: LDAP*** 연결 설정

필드 이름	사용 지침
Enable Secondary Server(보조 서버 활성화**)**	기본 LDAP 서버에서 장애가 발생하는 경우 백업으로 사용할 보조 LDAP 서버를 활성화하려면 이 옵션을 선택합니다. 이 확인란을 선택하는 경우 보조 LDAP 서버에 대한 컨피그레이션 매개변수를 입력해야 합니다.
Primary and Secondary Servers(기본 서버 및 보조 서버**)**	
Hostname/IP(호스트 이름/**IP)**	LDAP 소프트웨어를 실행 중인 머신의 IP 주소 또는 DNS 이름을 입력합니다. 호스트 이름은 1~256자로 입력하거나 문자열로 표시되는 유효한 IP 주소를 포함할 수 있습니다. 호스트 이름에 사용할 수 있는 문자는 영숫자 문자(a~z, A~Z, 0~9)와 점(.), 하이픈(-)입니다.
Port(포트**)**	LDAP 서버가 수신 대기 중인 TCP/IP 포트 번호를 입력합니다. 유효한 값은 1~65,535입니다. 기본값은 LDAP 사양에 나와 있는 389입니다. 포트 번호를 모르는 경우 LDAP 서버 관리자에서 이 정보를 찾을 수 있습니다.

필드 이름	사용 지침
Specify server for each ISE node(각 **ISE** 노드에 대한 서버 지정**)**	각 PSN에 대해 기본 및 보조 LDAP 서버 호스트 이름/IP 및 해당 포트를 구성하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 구축의 모든 노드를 나열하는 표가 표시됩니다. 노드를 선택하고 선택한 노드에 대한 기본 및 보조 LDAP 서버 호스트 이름/IP 및 해당 포트를 구성해야 합니다.
Access(액세스**)**	**Anonymous Access(**익명 액세스**)**: LDAP 디렉토리의 검색이 익명으로 수행되도록 하려면 클릭합니다. 이 경우 서버는 클라이언트를 구분하지 않으며, 인증되지 않은 클라이언트가 액세스할 수 있도록 구성된 모든 데이터에 대한 읽기 권한을 클라이언트에 허용합니다. 서버로 인증 정보를 전송하도록 허용하는 특정 정책이 없는 경우 클라이언트는 익명 연결을 사용해야 합니다. **Authenticated Access(**인증된 액세스**)**: LDAP 디렉토리의 검색이 관리 자격 증명을 사용하여 수행되도록 하려면 클릭합니다. 이 설정을 클릭하는 경우 Admin DN(관리자 DN) 및 Password(비밀번호) 필드에 정보를 입력합니다.
Admin DN(관리자 **DN)**	관리자의 DN을 입력합니다. 관리자 DN은 사용자 디렉토리 서브트리에서 필요한 모든 사용자 및 그룹을 검색할 권한이 있는 LDAP 계정입니다. 지정된 관리자에게 검색에서 그룹 이름 속성을 확인할 권한이 없으면 해당 LDAP 서버에 의해 인증된 사용자에 대한 그룹 매핑이 실패합니다.
Password(비밀번호**)**	LDAP 관리자 계정 비밀번호를 입력합니다.
Secure Authentication(보안 인증**)**	SSL을 사용하여 Cisco ISE와 기본 LDAP 서버 간의 통신을 암호화하려면 클릭합니다. Port(포트) 필드에 LDAP 서버의 SSL에 사용되는 포트 번호가 포함되어 있는지 확인합니다. 이 옵션을 활성화하는 경우 루트 CA를 선택해야 합니다.
LDAP Server Root CA(LDAP 서버 루트 **CA)**	인증서를 사용한 보안 인증을 활성화하려면 드롭다운 목록에서 신뢰할 수 있는 루트 인증 기관을 선택합니다.

필드 이름	사용 지침
Server Timeout(서버 시간 초과**)**	기본 LDAP 서버와의 연결이나 인증이 실패했다고 결정할 때까지 Cisco ISE가 해당 서버로부터의 응답을 대기할 시간을 초 단위로 입력합니다. 유효한 값은 1~99입니다. 기본값은 10입니다.
Max. Admin Connections(최대 관리자 연결 수**)**	특정 LDAP 컨피그레이션에 대해 실행할 수 있는 LDAP 관리자 계정 권한이 있는 최대 동시 연결 수(0보다 큼)를 입력합니다. 이러한 연결은 디렉토리 검색 시 사용자 디렉토리 서브트리 및 그룹 디렉토리 서브트리에서 사용자와 그룹을 검색하는 데 사용됩니다. 유효한 값은 1~99입니다. 기본값은 20입니다.
Force reconnect every N seconds(N초마다 강제로 다시 연결**)**	서버가 지정된 시간 간격에 LDAP 연결을 갱신하도록 강제 지정하려면 이 확인란을 선택하고 **Seconds(**초**)** 필드에 원하는 값을 입력합니다. 유효 범위는 1분~60분입니다.
Test Bind to Server(서버에 대한 바인딩 테스트**)**	LDAP 서버 세부정보 및 자격 증명을 정상적으로 바인딩할 수 있는지를 테스트하고 확인하려면 클릭합니다. 테스트가 실패하는 경우 LDAP 서버 세부정보를 편집한 후에 다시 테스트해 주십시오.
Failover(페일오버**)**	
Always Access Primary Server First(항상 기본 서버에 먼저 액세스**)**	Cisco ISE가 인증 및 권한 부여를 위해 항상 기본 LDAP 서버에 먼저 액세스하도록 하려면 이 옵션을 클릭합니다.
Failback to Primary Server After(다음 시간 이후 기본 서버로 장애 복구**)**	Cisco ISE가 연결하려고 하는 기본 LDAP 서버에 연결할 수 없는 경우 Cisco ISE는 보조 LDAP 서버에 연결하려고 시도합니다. Cisco ISE가 기본 LDAP 서버를 다시 사용하도록 하려면 이 옵션을 클릭하고 텍스트 상자에 값을 입력합니다.

LDAP 디렉토리 조직 설정

다음 표에서는 **Directory Organization(**디렉토리 조직**)** 탭의 필드에 대해 설명합니다.

표 ***81: LDAP*** 디렉토리 조직 설정

필드 이름	사용 지침
Subject Search Base(주체 검색 기준**)**	모든 주체를 포함하는 서브트리의 DN을 입력합니다. 예를 들면 다음과 같습니다. o=corporation.com 주체를 포함하는 트리가 기본 DN인 경우 LDAP 컨피그레이션에 따라 o=corporation.com 또는 dc=corporation,dc=com 을 입력합니다. 자세한 내용은 LDAP 데이터베이스 설명서를 참고해 주십시오.
Group Search Base(그룹 검색 기준**)**	모든 그룹을 포함하는 서브트리의 DN을 입력합니다. 예를 들면 다음과 같습니다. ou=조직 단위, ou=다음 조직 단위, o=corporation.com 그룹을 포함하는 트리가 기본 DN인 경우 LDAP 컨피그레이션에 따라 o=corporation.com 또는 dc=corporation,dc=com 을 입력합니다. 자세한 내용은 LDAP 데이터베이스 설명서를 참고해 주십시오.

필드 이름	사용 지침
Search for MAC Address in Format(MAC 주소 검색 형식**)**	LDAP 데이터베이스에서 Cisco ISE가 검색에 사용할 MAC 주소 형식을 입력합니다. 내부 ID 소스의 MAC 주소는 xx-xx-xx-xx-xx-xx 형식으로 제공됩니다. LDAP 데이터베이스의 MAC 주소는 다른 형식으로 제공될 수 있습니다. 그러나 Cisco ISE는 호스트 조회 요청을 받으면 MAC 주소를 내부 형식에서 이 필드에 지정된 형식으로 변환합니다. 드롭다운 목록을 사용하여 특정 형식의 MAC 주소 검색을 활성화합니다. 여기서 <*format*>은 다음 중 하나일 수 있습니다. • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 선택한 형식은 LDAP 서버에서 제공되는 MAC 주소의 형식과 일치해야 합니다.
Strip Start of Subject Name Up To the Last Occurrence of the Separator(마지막으로 나타나는 구분 기호까지 주체 이름 시작 부분 분리**)**	사용자 이름에서 도메인 접두사를 제거하려면 적절한 텍스트를 입력합니다. Cisco ISE는 사용자 이름에서 이 필드에 지정된 구분 기호 문자를 찾으면 사용자 이름이 시작되는 부분부터 구분 기호 문자까지의 모든 문자를 분리합니다. <start_string> 상자에 지정된 문자 중 두 개 이상이 사용자 이름에 포함되어 있으면 Cisco ISE는 마지막으로 나타나는 구분 기호까지 문자를 분리합니다. 예를 들어 구분 기호 문자가 백슬래시(\)이고 사용자 이름이 DOMAIN\user1이면 Cisco ISE는 user1을 LDAP 서버에 제출합니다. 참고 <start_string>은 우물 정자(#), 물음표(?), 큰따옴표("), 별표(*), 오른쪽 꺾쇠 괄호(>) 및 왼쪽 꺾쇠 괄호(<)와 같은 특수 문자를 포함할 수 없습니다. Cisco ISE에서는 사용자 이름에 이러한 문자를 사용할 수 없습니다.

필드 이름	사용 지침
Strip End of Subject Name from the First Occurrence of the Separator(처음으로 나타나는 구분 기호부터 주체 이름 끝 부분 분리**)**	사용자 이름에서 도메인 접미사를 제거하려면 적절한 텍스트를 입력합니다. Cisco ISE는 사용자 이름에서 이 필드에 지정된 구분 기호 문자를 찾으면 구분 기호 문자부터 사용자 이름이 끝나는 부분까지의 모든 문자를 분리합니다. 이 필드에 지정된 문자 중 두 개 이상이 사용자 이름에 포함되어 있으면 Cisco ISE는 처음으로 나타나는 구분 기호부터 문자를 분리합니다. 예를 들어 구분 기호 문자가 @이고 사용자 이름이 *user1@domain*이면 Cisco ISE는 *user1*을 LDAP 서버에 제출합니다. 참고 <*end_string*> 상자에는 우물 정자(#), 물음표(?), 큰따옴표("), 별표(*), 오른쪽 꺾쇠 괄호(>) 및 왼쪽 꺾쇠 괄호(<)와 같은 특수 문자를 포함할 수 없습니다. Cisco ISE에서는 사용자 이름에 이러한 문자를 사용할 수 없습니다.

LDAP 그룹 설정

표 ***82: LDAP*** 그룹 설정

필드 이름	사용 지침
Add(추가**)**	새 그룹을 추가하려면 **Add(**추가**) > Add Group(**추가 그룹**)**을 선택합니다. 또는 LDAP 디렉토리에서 그룹을 선택하려면 **Add(**추가**) > Select Groups From Directory(**디렉토리에서 그룹 선택**)**를 선택합니다. 그룹을 추가하도록 선택하는 경우 새 그룹의 이름을 입력합니다. 디렉토리에서 선택하는 경우 필터 기준을 입력하고 **Retrieve Groups(**그룹 검색**)**를 클릭합니다. 선택할 그룹 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다. 선택한 그룹이 **Groups(**그룹**)** 창에 표시됩니다.

LDAP 속성 설정

표 *83: LDAP* 속성 설정

필드 이름	사용 지침
Add(추가)	새 속성을 추가하려면 **Add(추가) > Add Attribute(속성 추가)**를 선택합니다. 또는 LDAP 서버에서 속성을 선택하려면 **Add(추가) > Select Attributes From Directory(디렉토리에서 속성 선택)**를 선택합니다. 속성을 추가하도록 선택하는 경우 새 속성의 이름을 입력합니다. 디렉토리에서 선택하는 경우 사용자 이름을 입력하고 **Retrieve Attributes(속성 검색)**를 클릭하여 속성을 검색합니다. 선택할 속성 옆의 확인란을 선택하고 OK(확인)를 클릭합니다.

LDAP 고급 설정

다음 표에서는 Advanced Settings(고급 설정) 탭의 필드에 대해 설명합니다.

표 *84: LDAP* 고급 설정

필드 이름	사용 지침
Enable Password Change(비밀번호 변경 활성화)	디바이스 관리자에 PAP 프로토콜을 사용하고 네트워크 액세스에 RADIUS EAP-GTC 프로토콜을 사용하는 동안 비밀번호 만료 또는 비밀번호 재설정이 발생할 때 사용자가 비밀번호를 변경할 수 있도록하려면 이 확인란을 선택합니다. 지원되지 않는 프로토콜에 대한 사용자 인증은 실패합니다. 또한 이 옵션을 사용하면 사용자가 다음 로그인 시 비밀번호를 변경할 수 있습니다.

관련 항목

LDAP 디렉토리 서비스, 640 페이지
LDAP 사용자 인증, 642 페이지
LDAP 사용자 조회, 645 페이지
LDAP ID 소스 추가, 645 페이지

LDAP 스키마 구성

단계 **1** **Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > LDAP**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** LDAP 인스턴스를 선택합니다.

단계 **3** **General(일반)** 탭을 클릭합니다.

단계 **4** **Schema(스키마)** 옵션 근처의 드롭다운 화살표를 클릭합니다.

단계 **5** **Schema(스키마)** 드롭다운 목록에서 필요한 스키마를 선택합니다. **Custom(사용자 맞춤화)** 옵션을 선택하여 요구 사항에 따라 속성을 업데이트할 수 있습니다.

사전 정의된 속성은 Active Directory, Sun Directory Server, Novell eDirectory와 같은 기본 제공 스키마에 사용됩니다. 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다.

기본 및 보조 LDAP 서버 구성

LDAP 인스턴스를 생성한 후에는 기본 LDAP 서버에 대한 연결 설정을 구성해야 합니다. 보조 LDAP 서버는 필요에 따라 구성하면 됩니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**를 선택합니다.

단계 2 편집할 LDAP 인스턴스 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 3 **Connection(**연결**)** 탭을 클릭하여 기본 및 보조 서버를 구성합니다.

단계 4 LDAP ID 소스 설정의 설명에 따라 값을 입력합니다.

단계 5 **Submit(**제출**)**을 클릭하여 연결 매개변수를 저장합니다.

Cisco ISE가 LDAP 서버에서 속성을 가져오도록 설정

Cisco ISE가 LDAP 서버에서 사용자 및 그룹 데이터를 가져오도록 하려면 Cisco ISE에서 LDAP 디렉토리 세부정보를 구성해야 합니다. LDAP ID 소스에 대해 다음의 세 가지 검색을 수행할 수 있습니다.

- 관리용으로 그룹 서브트리의 모든 그룹 검색
- 사용자를 찾기 위해 주체 서브트리에서 사용자 검색
- 사용자가 멤버로 속한 그룹 검색

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**를 선택합니다.

단계 2 편집할 LDAP 인스턴스 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 3 **Directory Organization(**디렉토리 구성**)** 탭을 클릭합니다.

단계 4 LDAP ID 소스 설정의 설명에 따라 값을 입력합니다.

단계 5 컨피그레이션을 저장하려면 **Submit(**제출**)**을 클릭합니다.

LDAP 서버에서 그룹 멤버십 세부정보 검색

새 그룹을 추가하거나 LDAP 디렉토리에서 그룹을 선택할 수 있습니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**를 선택합니다.

단계 2 편집할 LDAP 인스턴스 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 3 **Groups(**그룹**)** 탭을 클릭합니다.

단계 4 **Add(**추가**)** > **Add Group(**그룹 추가**)**을 선택하여 새 그룹을 추가하거나 **Add(**추가**)** > **Select Groups From Directory(**디렉토리에서 그룹 선택**)**를 선택하여 LDAP 디렉토리에서 그룹을 선택합니다.

a) 그룹을 추가하도록 선택하는 경우 새 그룹의 이름을 입력합니다.

b) 디렉토리에서 선택하는 경우 필터 기준을 입력하고 **Retrieve Groups(**그룹 검색**)**를 클릭합니다. 검색 조건에는 별표(*) 와일드카드 문자를 포함할 수 있습니다.

단계 5 선택할 그룹 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

선택한 그룹이 그룹 페이지에 표시됩니다.

단계 6 **Submit(**제출**)**을 클릭하여 그룹 선택 사항을 저장합니다.

참고 Active Directory가 Cisco ISE에서 LDAP ID 저장소로 구성되어 있으면 Active Directory 내장 그룹은 지원되지 않습니다.

LDAP 서버에서 사용자 속성 검색

권한 부여 정책에서 사용할 사용자 속성을 LDAP 서버에서 가져올 수 있습니다.

단계 1 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**를 선택합니다.

단계 2 편집할 LDAP 인스턴스 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 3 **Attributes(**속성**)** 탭을 클릭합니다.

단계 4 새 속성을 추가하려면 **Add(**추가**)** > **Add Attribute(**속성 추가**)**를 선택합니다. 또는 LDAP 서버에서 속성을 선택하려면 **Add(**추가**)** > **Select Attributes From Directory(**디렉토리에서 속성 선택**)**를 선택합니다.

a) 속성을 추가하도록 선택하는 경우 새 속성의 이름을 입력합니다.

b) 디렉토리에서 선택하는 경우 예제 사용자를 입력하고 **Retrieve Attributes(**속성 검색**)**를 클릭하여 사용자 속성을 검색합니다. 별표(*) 와일드카드 문자를 사용할 수 있습니다.

Cisco ISE에서는 속성 유형 IP를 수동으로 추가할 때 사용자 인증에 IPv4 또는 IPv6 주소를 사용하도록 LDAP 서버를 구성할 수 있습니다.

단계 5 선택할 속성 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

단계 6 **Submit(**제출**)**을 클릭하여 속성 선택 사항을 저장합니다.

LDAP ID 소스를 사용한 보안 인증 활성화

LDAP 컨피그레이션 페이지의 Secure Authentication(보안 인증) 옵션을 선택하면 Cisco ISE는 SSL을 사용하여 LDAP ID 소스와의 통신을 보호합니다. LDAP ID 소스에 대한 보안 연결은 다음 항목을 사용하여 설정됩니다.

- SSL 터널: SSL v3 또는 TLS v1(LDAP 서버에서 지원하는 가장 강력한 버전)을 사용합니다.
- 서버 인증(LDAP 서버의 인증): 인증서를 기반으로 합니다.
- 클라이언트 인증(Cisco ISE의 인증): 사용되지 않습니다. SSL 터널 내부에서 관리자 바인딩이 사용됩니다.
- 암호 세트: Cisco ISE에서 지원하는 모든 암호 세트가 사용됩니다.

Cisco ISE가 지원하는 가장 강력한 암호화 및 암호를 제공하는 TLS v1을 사용하는 것이 좋습니다.

Cisco ISE가 LDAP ID 소스와 안전하게 통신할 수 있도록 설정하려면 다음을 수행합니다.

시작하기 전에

- Cisco ISE를 LDAP 서버에 연결해야 합니다.
- TCP 포트 636를 열어야 합니다.

단계 **1** LDAP 서버에 서버 인증서를 발급한 CA(Certificate Authority)의 전체 CA 체인을 Cisco ISE(**Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**)로 가져옵니다.

전체 CA 체인은 LDAP 서버 인증서가 아닌 루트 CA 및 중간 CA 인증서를 참고합니다.

단계 **2** LDAP ID 소스와 통신할 때 보안 인증을 사용하도록 Cisco ISE를 구성합니다(**Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**). 이때 Connection Settings(연결 설정) 탭에서 Secure Authentication(보안 인증) 확인란을 선택해야 합니다.

단계 **3** LDAP ID 저장소의 루트 CA 인증서를 선택합니다.

ODBC ID 소스

ODBC(Open Database Connectivity) 준수 데이터베이스를 외부 ID 소스로 사용하여 사용자와 엔드포인트를 인증할 수 있습니다. ODBC ID 소스는 ID 저장소 시퀀스에서, 그리고 게스트 및 스폰서 인증용으로 사용할 수 있습니다. 또한 BYOD 플로우에도 사용할 수 있습니다.

다음 데이터베이스 엔진이 지원됩니다.

- MySQL
- Oracle
- PostgreSQL

- Microsoft SQL Server
- Sybase

ODBC 준수 데이터베이스에 대해 인증하도록 Cisco ISE를 구성해도 데이터베이스 컨피그레이션에는 영향을 주지 않습니다. 데이터베이스를 관리하려면 데이터베이스 설명서를 참고하십시오.

참고 Cisco ISE는 ODBC를 사용한 암호화를 지원하지 않습니다. 따라서 ODBC 연결은 보호되지 않습니다.

ODBC 데이터베이스의 자격 증명 확인

Cisco ISE는 ODBC 데이터베이스에 대해 각기 다른 3가지 유형의 자격 증명 확인을 지원합니다. 각 자격 증명 확인 유형에 대해 적절한 SQL 저장 프로시저를 구성해야 합니다. Cisco ISE는 이 저장 프로시저를 이용해 ODBC 데이터베이스에서 적절한 표를 쿼리하고 ODBC 데이터베이스에서 출력 파라미터 또는 기록 집합을 수신합니다. 데이터베이스는 ODBC 쿼리에 대한 응답으로 기록 집합 또는 명명된 파라미터 집합을 반환할 수 있습니다.

비밀번호는 일반 텍스트 또는 암호화된 형식으로 ODBC 데이터베이스에 저장할 수 있습니다. 저장 절차는 Cisco ISE에서 호출될 때 비밀번호를 일반 텍스트로 다시 암호 해독할 수 있습니다.

자격 증명 확인 유형	**ODBC** 입력 파라미터	**ODBC** 출력 파라미터	자격 증명 확인	인증 프로토콜
ODBC 데이터베이스의 일반 텍스트 비밀번호 인증	사용자 이름 비밀번호	결과 그룹 계정 정보 오류 문자열	사용자 이름과 비밀번호가 일치하는 경우 관련 사용자 정보가 반환됩니다.	PAP EAP-GTC(PEAP 또는 EAP-FAST의 내부 방법) TACACS
ODBC 데이터베이스에서 가져오는 일반 텍스트 비밀번호	사용자 이름	결과 그룹 계정 정보 오류 문자열 비밀번호	사용자 이름이 있는 경우 해당 비밀번호와 관련 사용자 정보가 저장 절차에 의해 반환됩니다. Cisco ISE는 인증 방법에 근거해 비밀번호 해시를 계산한 다음 이를 클라이언트에서 수신한 비밀번호와 비교합니다.	CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2(PEAP 또는 EAP-FAST의 내부 방법) TACACS

자격 증명 확인 유형	ODBC 입력 파라미터	ODBC 출력 파라미터	자격 증명 확인	인증 프로토콜
조회	사용자 이름	결과 그룹 계정 정보 오류 문자열	사용자 이름이 있는 경우 관련 사용자 정보가 반환됩니다.	MAB PEAP, EAP-FAST 및 EAP-TTLS의 빠른 재연결

참고 ODBC가 권한 부여를 위한 조회 소스로 사용되는 경우, ODBC 데이터베이스와 수신 요청 MAB 형식이 동일한지 확인하십시오.

출력 파라미터에서 반환되는 그룹은 Cisco ISE에서 사용되지 않습니다. Fetch Groups(그룹 가져오기) 저장 절차에 의해 검색된 그룹만 Cisco ISE에서 사용됩니다. 계정 정보는 인증 감사 로그에만 포함됩니다.

다음 표에는 ODBC 데이터베이스 저장 프로시저에서 반환되는 결과 코드와 Cisco ISE 인증 결과 코드 간의 매핑이 나열되어 있습니다.

결과 코드(저장 프로시저에 의해 반환됨)	설명	Cisco ISE 인증 결과 코드
0	CODE_SUCCESS	NA(인증 통과됨)
1	CODE_UNKNOWN_USER	UnknownUser
2	CODE_INVALID_PASSWORD	Failed
3	CODE_UNKNOWN_USER_OR_INVALID_PASSWORD	UnknownUser
4	CODE_INTERNAL_ERROR	Error
10001	CODE_ACCOUNT_DISABLED	DisabledUser
10002	CODE_PASSWORD_EXPIRED	NotPerformedPasswordExpired

참고 Cisco ISE는 이 매핑된 인증 결과 코드를 기반으로 실제 인증 또는 조회 작업을 수행합니다.

저장 절차를 사용하여 ODBC 데이터베이스에서 그룹 및 속성을 가져올 수 있습니다.

일반 텍스트 비밀번호 인증용 기록 집합을 반환하는 샘플 절차(**Microsoft SQL Server**용)

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset]
        @username varchar(64), @password varchar(255)
AS
BEGIN
```

```
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

일반 텍스트 비밀번호 가져오기용 기록 집합을 반환하는 샘플 절차(Microsoft SQL Server용)

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error',password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

조회용 기록 집합을 반환하는 샘플 절차(Microsoft SQL Server용)

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

일반 텍스트 비밀번호 인증용 파라미터를 반환하는 샘플 절차(Microsoft SQL Server용)

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters]
       @username varchar(64), @password varchar(255), @result INT OUTPUT, @group varchar(255)
 OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc',  @errorString='ODBC Authen Error'
END
```

일반 텍스트 비밀번호 가져오기용 파라미터를 반환하는 샘플 절차(Microsoft SQL Server용)

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters]
        @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
varchar(255) OUTPUT, @errorString varchar(255) OUTPUT, @password varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
       SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error',
 @password=password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

조회용 파라미터를 반환하는 샘플 절차(Microsoft SQL Server용)

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters]
        @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

Microsoft SQL Server에서 그룹을 가져오는 샘플 절차

```
CREATE PROCEDURE [dbo].[ISEGroupsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                select 'accountants', 'engineers', 'sales','test_group2'
        end
        else
                set @result = 1
END
```

사용자 이름이 "*"인 경우 모든 사용자의 모든 그룹을 가져오는 샘플 절차(Microsoft SQL Server용)

```
ALTER PROCEDURE [dbo].[ISEGroupsH]
                @username varchar(64), @result int output
AS
BEGIN
                if @username = '*'
                begin
                                -- if username is equal to '*' then return all existing
groups
                                set @result = 0
                                select 'accountants', 'engineers',
'sales','test_group1','test_group2','test_group3','test_group4'
```

```
                end
                else
                if exists (select * from NetworkUsers where username = @username)
                begin
                                set @result = 0
                                select 'accountants'
                end
                else
                                set @result = 1
END
```

Microsoft SQL Server에서 속성을 가져오는 샘플 절차

```
CREATE PROCEDURE [dbo].[ISEAttrsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                                select phone as phone, username as username, department as
 department, floor as floor, memberOf as memberOf, isManager as isManager from NetworkUsers
 where username = @username
        end
        else
                set @result = 1
END
```

ODBC 컨피그레이션에 대한 추가적인 예

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/211581-Configure-ODBC-on-ISE-2-3-with-Oracle-Da.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200644-Configure-ODBC-on-ISE-2-1-with-PostgreSQ.html

ODBC ID 소스 추가

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **ODBC**를 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** **General(**일반**)** 탭에서 ODBC ID 소스의 이름과 설명을 입력합니다.

단계 **5** **Connection(**연결**)** 탭에서 다음 세부정보를 입력합니다.

- ODBC 데이터베이스의 호스트 이름 또는 IP 주소입니다. 데이터베이스에 비표준 TCP 포트를 사용 중인 경우, 호스트 이름 또는 IP 주소:포트 형식으로 포트 번호를 지정할 수 있습니다.
- ODBC 데이터베이스의 이름

- 관리자 사용자 이름 및 비밀번호(Cisco ISE는 이러한 자격 증명을 사용하여 데이터베이스에 연결함)
- 서버 시간 초과(초)(기본값은 5초)
- 연결 시도 횟수(기본값은 1)
- 데이터베이스 유형입니다. 다음 중 하나를 선택합니다.
  - **MySQL**
  - **Oracle**
  - **PostgreSQL**
  - **Microsoft SQL Server**
  - **Sybase**

단계 **6** ODBC 데이터베이스와의 연결을 확인하고 구성된 활용 사례에 대해 저장 절차가 있는지를 확인하려면 **Test Connection(**연결 테스트**)**을 클릭합니다.

단계 **7** **Stored Procedures(**저장 절차**)** 탭에서 다음 세부정보를 입력합니다.

- **Stored Procedure Type(**저장 절차 유형**)**: 데이터베이스가 제공하는 출력 유형을 선택합니다.
  - **Returns Recordset(**기록 집합 반환**)**: 데이터베이스가 ODBC 쿼리에 대한 응답으로 기록 집합을 반환합니다.
  - **Returns Parameters(**파라미터 반환**)**: 데이터베이스가 ODBC 쿼리에 대한 응답으로 명명된 파라미터 집합을 반환합니다.
- **Plain Text Password Authentication(**일반 텍스트 비밀번호 인증**)**: 일반 텍스트 비밀번호 인증을 위해 ODBC 서버에서 실행되는 저장 절차의 이름을 입력합니다. PAP, EAP-GTC 내부 방법 및 TACACS에 사용됩니다.
- **Plain Text Password Fetching(**일반 텍스트 비밀번호 가져오기**)**: 일반 텍스트 비밀번호를 가져오기 위해 ODBC 서버에서 실행되는 저장 절차의 이름을 입력합니다. CHAP, MS-CHAPv1/v2, LEAP, EAP-MD5, EAP-MSCHAPv2 내부 방법 및 TACACS에 사용됩니다.
- **Check Username or Machine Exists(**사용자 이름 또는 머신 유무 확인**)**: 사용자/MAC 주소 조회용으로 ODBC 서버에서 실행되는 저장 절차의 이름을 입력합니다. MAB 및 PEAP, EAP-FAST, EAP-TTLS의 빠른 재연결에 사용됩니다.
- **Fetch Groups(**그룹 가져오기**)**: ODBC 데이터베이스에서 그룹을 검색하는 저장 절차의 이름을 입력합니다.
- **Fetch Attributes(**속성 가져오기**)**: ODBC 데이터베이스에서 속성 및 해당 값을 검색하는 저장 절차의 이름을 입력합니다.
- **Advanced Settings(**고급 설정**)**: 이 옵션을 클릭하면 **Fetch Attributes(**속성 가져오기**)** 저장 절차에서 다음의 사전 아래에 있는 속성을 사용자 이름 및 비밀번호와 함께 입력 매개 변수로 사용할 수 있습니다.
  - **RADIUS**
  - 디바이스

- 네트워크 액세스

참고 **Network Access(**네트워크 액세스**)** 사전의 속성은 **AuthenticationMethod**, **Device IP Address**, **EapAuthentication**, **EapTunnel**, **ISE Host Name**, **Protocol**, **UserName**, **VN**, **WasMachineAuthenticated** 만 사용할 수 있습니다.

Attribute Name in Stored Procedure(저장된 절차의 속성 이름**)** 필드에서, 저장 절차에 사용되는 속성 이름을 지정합니다.

ODBC 데이터베이스에서 다음의 출력 매개 변수를 검색하도록 저장 절차를 구성할 수 있습니다.

- ACL
- Security Group(보안 그룹)
- VLAN(이름 또는 번호)
- 웹 리디렉션 ACL
- 웹 리디렉션 포털 이름

이러한 속성을 사용하여 권한 부여 프로파일을 구성할 수 있습니다. 이러한 속성은 **Authorization Profiles(**권한 부여 프로파일**)** 창의 **Common Tasks(**일반 작업**)** 섹션에 나열됩니다(**Policy (**정책**) > Policy Elements (**정책 요소**) > Results (**결과**)**). 다음은 이러한 속성을 사용할 수 있는 몇 가지 샘플 활용 사례 시나리오입니다.

- 각 권한 부여 프로파일에 대해 VLAN을 수동으로 지정하지 않고, 지정된 입력 속성(MAC 주소, 사용자 이름, called-station-ID 또는 디바이스 위치)을 기반으로 ODBC 데이터베이스에서 반환되는 VLAN을 사용하도록 권한 부여 프로파일을 구성하는 경우.
- ODBC ID 저장소에서 차단된 호출 스테이션 ID에 대한 액세스를 차단하도록 권한 부여 프로파일을 구성하는 경우.
- MAC 주소, 사용자 이름, called-station-ID 또는 디바이스 위치를 기반으로 ODBC 데이터베이스에서 웹 리디렉션 ACL 또는 웹 리디렉션 포털 이름을 검색하도록 권한 부여 프로파일을 구성하는 경우.

권한 부여 정책을 구성하는 동안, ODBC 데이터베이스에서 검색되는 보안 그룹을 **Policy Sets(**정책 집합**)** 창에서 선택할 수 있습니다.

참고 **Advanced Settings(**고급 설정**)** 옵션을 사용하는 동안에는 추가 세부정보를 저장하기 위해 user_attributes_detail이라는 새 표가 ODBC 데이터베이스에 생성됩니다. 모든 출력 매개 변수에 대해 데이터 유형을 VARCHAR2로 설정해야합니다. 그러지 않으면 통합 및 컴파일 프로세스 중에 저장 절차가 실패할 수 있습니다. 예를 들어 SGTNAME이 VARCHAR2로 설정되고 VLANNUMBER가 NUMBER로 설정된 경우 다음 저장 절차의 컴파일이 실패할 수 있습니다.

```
select  ATTR_NAME, value from ATTRIBUTES where user_id=userid
          union
         select 'SGTNAME', SGTNAME from user_attributes_detail where USER_ID = userid and
 user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE
          union
          select 'VLANNUMBER', VLANNUMBER from user_attributes_detail where USER_ID =
userid and user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE;
```

- **Search for MAC Address in Format(**다음 형식으로 **MAC** 주소 검색**)**: 선택한 MAC 형식을 기준으로 수신 MAC 주소가 정규화됩니다.

단계 **8** **Attributes(**속성**)** 탭에서 필요한 속성을 추가합니다. 속성을 추가할 때는 권한 부여 정책 규칙에서 속성 이름이 표시되어야 하는 방법을 지정할 수 있습니다.

또한 ODBC 데이터베이스에서 속성을 가져올 수도 있습니다. 이러한 속성은 권한 부여 정책에서 사용할 수 있습니다.

단계 **9** **Groups(**그룹**)** 탭에서 사용자 그룹을 추가합니다. 사용자 이름 또는 MAC 주소를 지정하여 ODBC 데이터베이스에서 그룹을 가져올 수도 있습니다. 이러한 그룹은 권한 부여 정책에서 사용할 수 있습니다.

그룹과 속성의 이름을 바꿀 수 있습니다. 기본적으로 **Name in ISE(ISE** 내 이름**)** 필드에 표시되는 이름은 ODBC 데이터베이스의 이름과 같지만 이 이름은 수정할 수 있습니다. 이 이름은 권한 부여 정책에서 사용 됩니다.

단계 **10** **Submit(**제출**)**을 클릭합니다.

ODBC ID 소스를 구성하는 방법에 대한 자세한 내용은 다음 링크를 참조하십시오.

- Oracle 데이터베이스를 사용하여 Cisco ISE에서 ODBC 구성
- ODBC를 사용하여 MS SQL로 Cisco ISE 구성
- PostgreSQL을 사용하여 Cisco ISE에서 ODBC 구성
- Cisco 서버와의 통합을 위한 Cisco ISE 구성

참고 입력 속성을 구성한 경우 ODBC ID 저장소를 복제하는 동안 다음을 수행해야 합니다. 그러지 않으면 중복된 ODBC ID 저장소에서 입력 매개 변수가 손실될 수 있습니다.

1. **Advanced Settings(**고급 설정**)**를 클릭합니다.
2. 입력 매개 변수가 올바르게 설정되었는지 확인합니다.
3. **OK(**확인**)**를 클릭하여 이러한 입력 매개 변수를 중복된 ODBC ID 저장소에 저장합니다.

RADIUS 토큰 ID 소스

RADIUS 프로토콜을 지원하고 사용자 및 디바이스에 AAA(Authentication, Authorization, and Accounting) 서비스를 제공하는 서버를 RADIUS 서버라고 합니다. RADIUS ID 소스는 주체 및 자격 증명 모음이 포함되어 있는 외부 ID 소스로, 통신에 RADIUS 프로토콜을 사용합니다. 예를 들어 Safeword 토큰 서버는 여러 사용자 및 자격 증명을 일회용 비밀번호로 포함할 수 있는 ID 소스로, RADIUS 프로토콜을 사용하여 쿼리할 수 있는 인터페이스를 제공합니다.

Cisco ISE는 외부 ID 소스로 RADIUS RFC 2865 준수 서버를 지원합니다. Cisco ISE는 여러 RADIUS 토큰 서버 ID(예: RSA SecurID 서버 및 SafeWord 서버)를 지원합니다. RADIUS ID 소스는 사용자를 인증하는 데 사용되는 모든 RADIUS 토큰 서버와 연동될 수 있습니다.

참고 MAB 인증을 위해 Process Host Lookup(프로세스 호스트 조회) 옵션을 활성화해야 합니다. MAB 인증을 사용하는 디바이스는 OTP 또는 RADIUS 토큰(RADIUS 토큰 서버 인증에 필요)을 생성 할 수 없으므로 MAB 인증을 위해 외부 ID 소스로 사용되는 RADIUS 토큰 서버를 구성하지 않는 것이 좋습니다. 따라서 인증이 실패합니다. 외부 RADIUS 서버 옵션을 사용하여 MAB 요청을 처리할 수 있습니다.

RADIUS 토큰 서버에서 지원되는 인증 프로토콜

Cisco ISE는 RADIUS ID 소스에 다음 인증 프로토콜을 지원합니다.

- RADIUS PAP
- 내부 EAP-GTC(Extensible Authentication Protocol-Generic Token Card)가 있는 PEAP(Protected Extensible Authentication Protocol)
- 내부 EAP-GTC가 있는 EAP-FAST

통신에 RADIUS 토큰 서버가 사용하는 포트

RADIUS 토큰 서버는 인증 세션에 UDP 포트를 사용합니다. 이 포트는 모든 RADIUS 통신에 사용됩니다. Cisco ISE에서 RADIUS OTP(One-Time Password) 메시지를 RADIUS 지원 토큰 서버로 보내려면 Cisco ISE와 RADIUS 지원 토큰 서버 사이의 게이트웨이 디바이스가 UDP 포트를 통한 통신을 허용하는지 확인해야 합니다. 관리 포털을 통해 UDP 포트를 구성할 수 있습니다.

RADIUS 공유 암호

Cisco ISE에서 RADIUS ID 소스를 구성하면서 공유 암호를 제공해야 합니다. 이 공유 암호는 RADIUS 토큰 서버에 구성된 공유 암호와 동일해야 합니다.

RADIUS 토큰 서버의 페일오버

Cisco ISE에서는 여러 RADIUS ID 소스를 구성할 수 있습니다. 각 RADIUS ID 소스마다 기본 및 보조 RADIUS 서버가 있을 수 있습니다. Cisco ISE가 기본 서버에 연결할 수 없는 경우에는 보조 서버를 사용합니다.

RADIUS 토큰 서버에서 구성 가능한 비밀번호 프롬프트

RADIUS ID 소스에서는 비밀번호 프롬프트를 구성할 수 있습니다. 관리 포털을 통해 비밀번호 프롬프트를 구성할 수 있습니다.

RADIUS 토큰 서버 사용자 인증

Cisco ISE는 사용자 자격 증명(사용자 이름 및 비밀번호)을 가져와 RADIUS 토큰 서버에 전달합니다. Cisco ISE는 또한 RADIUS 토큰 서버 인증 처리 결과를 사용자에게 릴레이합니다.

RADIUS 토큰 서버의 사용자 속성 캐시

RADIUS 토큰 서버는 기본적으로 사용자 조회를 지원하지 않습니다. 그러나 사용자 조회는 다음 Cisco ISE 기능에 필수적인 기능입니다.

- PEAP 세션 재개: 이 기능은 EAP 세션을 설정하는 중에 성공적인 인증이 이루어지면 PEAP 세션을 재개하도록 합니다.
- EAP/FAST 빠른 재연결: 이 기능은 EAP 세션을 설정하는 중에 성공적인 인증이 이루어지면 빠른 재연결을 허용합니다.
- TACACS + 권한 부여: TACACS + 인증에 성공한 후 발생합니다.

Cisco ISE는 성공적인 인증 결과를 캐시하여 이러한 기능에 대한 사용자 조회 요청을 처리합니다. 각각의 성공적인 인증에서 인증된 사용자의 이름 및 검색된 속성이 캐시됩니다. 실패한 인증은 캐시에 기록되지 않습니다.

런타임에 메모리에서 캐시를 사용할 수 있으며 캐시는 분산형 구축의 Cisco ISE 노드 간에 복제되지 않습니다. 관리 포털을 통해 TTL(Time to Live) 제한을 구성할 수 있습니다. ISE 2.6부터는 ID 캐싱 옵션을 활성화하고 에이징 타임을 분 단위로 설정할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있으며, 활성화된 경우 지정된 시간 동안 메모리에서 캐시를 사용할 수 있습니다.

ID 시퀀스의 RADIUS ID 소스

ID 소스 시퀀스에서 인증 시퀀스의 RADIUS ID 소스를 추가할 수 있습니다. 그러나 인증 없이 RADIUS ID 소스를 쿼리할 수 없으므로 속성 검색 시퀀스의 RADIUS ID 소스를 추가할 수 없습니다. Cisco ISE는 RADIUS 서버를 인증하는 동안 서로 다른 오류를 구분할 수 없습니다. RADIUS 서버는 모든 오류에 대해 Access-Reject 메시지를 반환합니다. 예를 들어 RADIUS 서버에 사용자가 없으면 RADIUS 서버는 사용자 알 수 없음 상태를 반환하는 대신 RADIUS 서버는 Access-Reject 메시지를 반환합니다.

RADIUS 서버가 모든 오류에 대해 같은 메시지를 반환함

RADIUS 서버에 사용자가 없으면 RADIUS 서버는 Access-Reject 메시지를 반환합니다. Cisco ISE는 관리 포털을 통해 이 메시지를 인증 실패 또는 사용자를 찾을 수 없음 메시지로 구성할 수 있는 옵션을 제공합니다. 그러나 이 옵션은 사용자를 확인할 수 없는 사례뿐 아니라 모든 오류 사례에 대해 사용자를 찾을 수 없음 메시지를 반환합니다.

다음 표에는 RADIUS ID 서버에서 발생할 수 있는 다양한 오류 사례가 나열되어 있습니다.

표 85: 오류 처리

오류 사례	오류 이유
인증 실패	• 사용자를 확인할 수 없습니다. • 사용자가 잘못된 암호로 로그인을 시도했습니다. • 사용자 로그인 시간이 만료 되었습니다.
처리 실패	• RADIUS 서버가 Cisco ISE에서 잘못 구성되어 있습니다. • RADIUS 서버를 사용할 수 없습니다. • RADIUS 패킷의 형식이 잘못된 것으로 탐지되었습니다. • RADIUS 서버에서 패킷을 보내거나 받는 동안 문제가 발생했습니다. • 시간이 초과되었습니다.
알 수 없는 사용자	인증이 실패했으며 Fail on Reject(거부 시 실패) 옵션이 false로 설정되어 있습니다.

SafeWord 서버의 특수 사용자 이름 형식 지원

SafeWord 토큰 서버는 다음 사용자 이름 형식을 사용하는 인증을 지원합니다.

사용자 이름 - 사용자 이름, OTP

Cisco ISE는 인증 요청을 받는 즉시 사용자 이름을 구문 분석하여 다음 사용자 이름으로 변환합니다.

사용자 이름 - 사용자 이름

SafeWord 토큰 서버는 이 두 가지 형식을 모두 지원합니다. Cisco ISE에서는 다양한 토큰 서버를 사용합니다. SafeWord 서버를 구성할 때는 Cisco ISE의 관리 포털에서 SafeWord Server(SafeWord 서버) 확인란을 선택하여 사용자 이름을 구문 분석하고 지정된 형식으로 변환해야 합니다. 요청이 RADIUS 토큰 서버로 전송되기 전에 RADIUS 토큰 서버 ID 소스에서 이 변환이 수행됩니다.

RADIUS 토큰 서버의 인증 요청 및 응답

Cisco ISE가 인증 요청을 RADIUS 지원 토큰 서버로 전달하는 경우 RADIUS 인증 요청에는 다음과 같은 속성이 포함됩니다.

- User-Name(RADIUS 속성 1)
- User-Password(RADIUS 속성 2)

- NAS-IP-Address(RADIUS 속성 4)

Cisco ISE가 수신을 기대하는 응답은 다음 중 하나입니다.

- Access-Accept: 속성이 필요하지 않습니다. 그러나 응답에는 RADIUS 토큰 서버 컨피그레이션에 따라 다양한 속성을 포함할 수 있습니다.
- Access-Reject: 속성이 필요하지 않습니다.
- Access-Challenge: RADIUS RFC마다 필요한 속성은 다음과 같습니다.
  - State(RADIUS 속성 24)
  - Reply-Message(RADIUS 속성 18)
  - 다음 속성 중 하나 이상: Vendor-Specific, Idle-Timeout(RADIUS 속성 28), Session-Timeout(RADIUS 속성 27), Proxy-State(RADIUS 속성 33)

    Access-Challenge에서 다른 속성은 허용되지 않습니다.

RADIUS 토큰 ID 소스 설정

다음 표에서는 외부 RADIUS ID 소스를 구성하고 해당 소스에 연결하는 데 사용할 수 있는 RADIUS 토큰 ID 소스 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RADIUS Token(RADIUS** 토큰**)**입니다.

표 ***86: RADIUS*** 토큰 ***ID*** 소스 설정

필드 이름	사용 지침
Name(이름**)**	RADIUS 토큰 서버의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
Description(설명**)**	RADIUS 토큰 서버에 대한 설명을 입력합니다. 최대 문자 수는 1,024자입니다.
SafeWord Server(SafeWord 서버**)**	RADIUS ID 소스가 SafeWord 서버인 경우 이 확인란을 선택합니다.
Enable Secondary Server(보조 서버 활성화**)**	기본 서버에 오류가 발생하는 경우 백업으로 사용할 Cisco ISE용 보조 RADIUS 토큰 서버를 활성화하려면 이 확인란을 선택합니다. 이 확인란을 선택하는 경우 보조 RADIUS 토큰 서버를 구성해야 합니다.
Always Access Primary Server First(항상 기본 서버에 먼저 액세스**)**	Cisco ISE가 항상 기본 서버에 먼저 액세스하도록 하려면 이 옵션을 클릭합니다.

필드 이름	사용 지침
Fallback to Primary Server after(다음 시간 이후 기본 서버로 대체**)**	기본 서버에 연결할 수 없는 경우 Cisco ISE가 보조 RADIUS 토큰 서버를 사용하여 인증할 수 있는 시간(분)을 지정하려면 이 옵션을 클릭합니다. 이 시간이 경과하면 Cisco ISE는 기본 서버에 대한 인증을 재시도합니다.
기본 서버	
Host IP(호스트 **IP)**	기본 RADIUS 토큰 서버의 IP 주소를 입력합니다. 이 필드에는 문자열로 표시되는 유효한 IP 주소를 입력할 수 있습니다. 이 필드에 입력할 수 있는 문자는 숫자와 점(.)입니다.
Shared Secret(공유 암호**)**	이 연결에 대해 기본 RADIUS 토큰 서버에 구성된 공유 암호를 입력합니다.
Authentication Port(인증 포트**)**	기본 RADIUS 토큰 서버가 수신 대기 중인 포트 번호를 입력합니다.
Server Timeout(서버 시간 초과**)**	기본 RADIUS 토큰 서버가 다운되었다고 결정할 때까지 Cisco ISE가 기본 서버로부터의 응답을 대기할 시간을 초 단위로 지정합니다.
Connection Attempts(연결 시도 횟수**)**	Cisco ISE가 보조 서버(정의된 경우)로 이동하거나 보조 서버가 정의되어 있지 않은 경우 요청을 삭제하기 전에 기본 서버에 다시 연결을 시도해야 하는 횟수를 지정합니다.
보조 서버	
Host IP(호스트 **IP)**	보조 RADIUS 토큰 서버의 IP 주소를 입력합니다. 이 필드에는 문자열로 표시되는 유효한 IP 주소를 입력할 수 있습니다. 이 필드에 입력할 수 있는 문자는 숫자와 점(.)입니다.
Shared Secret(공유 암호**)**	이 연결에 대해 보조 RADIUS 토큰 서버에 구성된 공유 암호를 입력합니다.
Authentication Port(인증 포트**)**	보조 RADIUS 토큰 서버가 수신 대기 중인 포트 번호를 입력합니다. 유효한 값은 1~65,535입니다. 기본값은 1,812입니다.
Server Timeout(서버 시간 초과**)**	보조 RADIUS 토큰 서버가 다운되었다고 결정할 때까지 Cisco ISE가 보조 서버로부터의 응답을 대기할 시간을 초 단위로 지정합니다.
Connection Attempts(연결 시도 횟수**)**	Cisco ISE가 요청을 삭제하기 전에 보조 서버에 다시 연결을 시도해야 하는 횟수를 지정합니다.

관련 항목

RADIUS 토큰 ID 소스, 665 페이지
RADIUS 토큰 서버 추가, 671 페이지

RADIUS 토큰 서버 추가

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** **External Identity Sources(**외부 **ID** 소스**)** > **RADIUS Token(RADIUS** 토큰**)** > **Add(**추가**)**를 선택합니다.

단계 **2** **General(**일반**)** 및 **Connection(**연결**)** 탭에 값을 입력합니다.

단계 **3** **Authentication(**인증**)** 탭을 클릭합니다.

이 탭에서는 RADIUS 토큰 서버의 Access-Reject 메시지에 대한 응답을 제어할 수 있습니다. 이 응답은 자격 증명이 잘못되었거나 사용자를 알 수 없다는 의미일 수 있습니다. Cisco ISE는 인증 실패 또는 사용자를 찾을 수 없음 응답 중 하나를 수락합니다. 또한 이 탭에서는 ID 캐싱을 활성화하고 캐시의 에이징 시간을 설정할 수도 있습니다. 그리고 비밀번호 요청 메시지도 구성할 수 있습니다.

a) RADIUS 토큰 서버의 Access-Reject 응답을 인증 실패로 처리하려는 경우 **Treat Rejects as 'authentication failed'(**거부를 '인증 실패'로 처리**)** 라디오 버튼을 클릭합니다.

b) RADIUS 토큰 서버의 Access-Reject 응답을 알 수 없는 사용자 오류로 처리하려는 경우 **Treat Rejects as 'user not found'(**거부를 '사용자를 찾을 수 없음'으로 처리**)** 라디오 버튼을 클릭합니다.

단계 **4** Cisco ISE가 RADIUS 토큰 서버를 사용한 첫 번째 인증에 성공한 후 캐시에 암호를 저장하고 구성된 기간 내에 발생하는 경우 후속 인증에 대해 캐시된 사용자 자격 증명을 사용하도록 하려면 **Enable Passcode Caching(**암호 캐싱 활성화**)** 확인란을 선택합니다.

Aging Time(에이징 시간**)** 필드의 캐시에 암호가 저장되어야 하는 시간을 초 단위로 입력합니다. 이 기간 동안에는 사용자가 동일한 암호를 사용하여 인증을 2회 이상 수행할 수 있습니다. 기본값은 30초입니다. 유효 범위는 1~300초입니다.

참고 Cisco ISE는 첫 번째 인증 실패 후 캐시를 지웁니다. 사용자는 새 유효 암호를 입력해야 합니다.

참고 이 옵션은 예를 들어 -FAST-GTC 같은 암호의 암호화를 지원하는 프로토콜을 사용할 때만 활성화하는 것이 좋습니다. RADIUS 토큰 서버에서 지원되는 인증 프로토콜에 대한 자세한 내용은 다음을 참조하십시오. RADIUS 토큰 서버에서 지원되는 인증 프로토콜, 666 페이지

단계 **5** 서버에 대해 인증을 수행하지 않는 요청을 처리하게 하려면 **Enable Identity Caching(ID** 캐싱 활성화**)** 확인란을 선택합니다.

ID 캐싱 옵션을 활성화하고 에이징 타임을 분 단위로 설정할 수 있습니다. 기본값은 120분입니다. 유효 범위는 1분~1440분입니다. 마지막으로 성공한 인증에서 얻은 결과와 속성은 지정된 기간 동안 캐시에 보관됩니다.

이 옵션은 기본적으로 비활성화되어 있습니다.

단계 **6** **Authorization(**권한 부여**)** 탭을 클릭합니다.

이 탭에서는 Cisco ISE로 Access-Accept 응답을 보내는 중에 RADIUS 토큰 서버에서 반환하는 속성에 대해 표시할 이름을 구성할 수 있습니다. 권한 부여 정책 조건에서 이 속성을 사용할 수 있습니다. 기본값은 CiscoSecure-Group-Id입니다.

참고 외부 ID 소스에서 Access-Accept의 속성을 보내려면 Ext ID 소스가 <ciscoavpair>를 속성 이름과 값으로 전송해야 합니다. 이때 ACS:<attrname>=<attrvalue> 형식을 사용해야 하며, 여기서 <attrname>은 **Authorization(**권한 부여**)** 탭에서 구성됩니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

RADIUS 토큰 서버 삭제

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- ID 소스 시퀀스의 일부분인 RADIUS 토큰 서버를 선택하지 않았는지 확인합니다. ID 소스 시퀀스의 일부분인 RADIUS 토큰 서버를 삭제하도록 선택하면 삭제 작업이 실패합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RADIUS Token(RADIUS** 토큰**)**을 선택합니다.

단계 **2** 삭제할 하나 이상의 RADIUS 토큰 서버 옆에 있는 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

단계 **3** **OK(**확인**)**를 클릭하여 선택한 하나 이상의 RADIUS 토큰 서버를 삭제합니다.

여러 RADIUS 토큰 서버를 삭제하도록 선택했는데 그 중 하나가 ID 소스 시퀀스에서 사용되는 경우에는 삭제 작업이 실패하며 모든 RADIUS 토큰 서버는 삭제되지 않습니다.

RSA ID 소스

Cisco ISE는 외부 데이터베이스로 RSA SecurID 서버를 지원합니다. RSA SecurID 2단계 인증은 사용자 PIN과 개별적으로 등록된 RSA SecurID 토큰으로 이루어집니다. 이 토큰은 시간 코드 알고리즘을 기반으로 하는 일회용 토큰 코드를 생성합니다. 고정 간격(일반적으로 30초 또는 60초마다)으로 다른 토큰 코드가 생성됩니다. RSA SecurID 서버는 이 동적 인증 코드를 검증합니다. 각 RSA SecurID 토큰은 고유하며 과거의 토큰을 기반으로 미래의 토큰 값을 예측할 수 없습니다. 따라서 PIN과 함께 올바른 토큰 코드를 제공하면 개인이 유효한 사용자임을 나타내는 확실성 수준이 높아집니다. 그러므로 RSA SecurID 서버는 기존의 재사용 가능한 비밀번호보다 안정적인 인증 메커니즘을 제공합니다.

Cisco ISE는 다음과 같은 RSA ID 소스를 지원합니다.

- RSA ACE/Server 6.x Series

- RSA Authentication Manager 7.x 및 8.0 Series

다음 방법 중 하나를 사용하여 RSA SecurID 인증 기술과 통합할 수 있습니다.

- RSA SecurID 에이전트 사용: RSA 기본 프로토콜을 통해 사용자 이름 및 암호를 사용하여 사용자가 인증됩니다.
- RADIUS 프로토콜 사용: RADIUS 프로토콜을 통해 사용자 이름 및 암호를 사용하여 사용자가 인증됩니다.

Cisco ISE의 RSA SecurID 토큰 서버는 RSA SEcurID 에이전트를 사용하여 RSA SecurID 인증 기술에 연결됩니다.

Cisco ISE는 하나의 RSA 영역만 지원합니다.

Cisco ISE와 RSA SecurID 서버 통합

Cisco ISE를 RSA SecurID 서버에 연결하는 데에는 두 가지 관리 역할이 관여합니다.

- RSA 서버 관리자: RSA 시스템 및 통합을 구성하고 유지 관리합니다.
- Cisco ISE 관리자: RSA SecurID 서버에 연결되도록 Cisco ISE를 구성하고 컨피그레이션을 유지 관리합니다.

이 섹션에서는 Cisco ISE를 RSA SecurID 서버에 외부 ID 소스로 연결하는 것과 관련된 프로세스에 설명합니다. RSA 서버에 대한 자세한 내용은 RSA 설명서를 참고해 주십시오.

Cisco ISE의 RSA 컨피그레이션

RSA 관리 시스템에서는 RSA 시스템 관리자가 사용자에게 제공하는 sdconf.rec 파일을 생성합니다. 이 파일을 사용하면 영역 내 RSA SEcurID 에이전트로 Cisco ISE 서버를 추가할 수 있습니다. 이렇게 하려면 Cisco ISE에서 이 파일을 찾아서 추가해야 합니다. 기본 Cisco ISE 서버는 복제 프로세스를 통해 모든 보조 서버에 이 파일을 배포합니다.

RSA SecurID 서버에 대한 RSA 에이전트 인증

모든 Cisco ISE 서버에 sdconf.rec 파일을 설치하고 나면 RSA 에이전트 모듈이 시작되며 RSA에서 생성한 자격 증명을 사용하는 인증이 각 Cisco ISE 서버에서 진행됩니다. 구축 내 각 Cisco ISE 서버의 에이전트가 정상적으로 인증되면 RSA 서버와 에이전트 모듈은 securid 파일을 함께 다운로드합니다. 이 파일은 Cisco ISE 파일 시스템에서 RSA 에이전트가 정의한 잘 알려진 위치에 있습니다.

분산형 Cisco ISE 환경의 RSA ID 소스

분산형 Cisco ISE 환경에서 RSA ID 소스를 관리할 때는 다음 작업을 수행합니다.

- 기본 서버에서 보조 서버로 sdconf.rec 및 sdopts.rec 파일 배포
- securid 및 sdstatus.12 파일 삭제

Cisco ISE 구축에서 RSA 서버 업데이트

Cisco ISE에서 sdconf.rec 파일을 추가하고 나면 RSA SecurID 관리자가 RSA 서버를 해제하거나 새 RSA 보조 서버를 추가할 때 sdconf.rec 파일을 업데이트할 수 있습니다. 이 경우 RSA SecurID 관리자는 업데이트된 파일을 제공합니다. 그러면 업데이트된 파일을 사용하여 Cisco ISE를 재구성할 수 있습니다. Cisco ISE의 복제 프로세스에서는 업데이트된 파일을 구축의 보조 Cisco ISE 서버로 배포합니다. Cisco ISE는 먼저 파일 시스템의 파일을 업데이트한 다음 RSA 에이전트 모듈과의 조정을 통해 다시 시작 프로세스의 단계를 적절하게 지정합니다. sdconf.rec 파일이 업데이트되면 sdstatus.12 및 securid 파일이 재설정(삭제)됩니다.

자동 RSA 라우팅 재정의

영역 내에 RSA 서버가 여러 개 있을 수 있습니다. sdopts.rec 파일은 로드 밸런서 역할을 수행합니다. Cisco ISE 서버 및 RSA SecurID 서버는 에이전트 모듈을 통해 작동합니다. Cisco ISE에 있는 에이전트 모듈은 영역 내 RSA 서버를 가장 효율적으로 사용하기 위해 비용 기반 라우팅 표을 유지 관리합니다. 그러나 관리 포털을 통해 sdopts.rec라는 텍스트 파일을 사용하면 영역의 각 Cisco ISE 서버에 대해 수동 컨피그레이션을 수행하여 이 라우팅을 재정의하도록 선택할 수 있습니다. 이 파일을 생성하는 방법에 대한 자세한 내용은 RSA 설명서를 참고해 주십시오.

RSA 노드 암호 재설정

securid 파일은 암호 노드 키 파일입니다. RSA는 처음 설정될 때 암호를 사용하여 에이전트를 검증합니다. Cisco ISE에 상주하는 RSA 에이전트는 처음으로 RSA 서버에 정상 인증되면 클라이언트 머신에 securid 파일을 생성한 다음 머신 간에 교환되는 데이터가 유효한지를 확인하는 데 사용합니다. RSA 서버에서 키를 재설정한 후와 같이 경우에 따라 구축의 특정 Cisco ISE 서버 또는 서버 그룹에서 securid 파일을 삭제해야 할 수 있습니다. Cisco ISE 관리 포털을 사용하여 해당 영역에 대해 Cisco ISE 서버에서 이 파일을 삭제할 수 있습니다. Cisco ISE의 RSA 에이전트는 다음 번에 정상 인증되면 새 securid 파일을 생성합니다.

참고 Cisco ISE의 최신 릴리스로 업그레이드한 후 인증이 실패하면 RSA 암호를 재설정해 주십시오.

RSA 자동 가용성 재설정

sdstatus.12 파일은 영역 내 RSA 서버의 가용성에 대한 정보를 제공합니다. 예를 들어 활성 상태인 서버와 다운된 서버에 대한 정보를 제공합니다. 에이전트 모듈은 영역 내 RSA 서버에서 작동하여 이 가용성 상태를 유지 관리합니다. 이 정보는 sdstatus.12 파일에서 연속으로 나열되며 Cisco ISE 파일 시스템의 잘 알려진 위치에서 제공됩니다. 이 파일이 오래되어 최신 상태가 이 파일에 반영되지 않는 경우도 있습니다. 이러한 경우에는 최신 상태가 다시 생성되도록 이 파일을 제거해야 합니다. 관리 포털을 사용하여 특정 영역에 대해 특정 Cisco ISE 서버에서 파일을 삭제할 수 있습니다. Cisco ISE는 RSA 에이전트와의 조정을 통해 올바른 다시 시작 단계를 지정합니다.

securid 파일이 재설정되거나 sdconf.rec 또는 sdopts.rec 파일이 업데이트될 때마다 sdstatus.12가 삭제됩니다.

RSA SecurID ID 소스 설정

다음 표에서는 RSA SecurID ID 소스를 생성하고 해당 소스에 연결하는 데 사용할 수 있는 RSA SecurID ID 소스 페이지의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID**입니다.

RSA 프롬프트 설정

다음 표에서는 **RSA Prompts(RSA** 프롬프트**)** 탭의 필드에 대해 설명합니다.

표 ***87: RSA*** 프롬프트 설정

필드 이름	사용 지침
Enter Passcode Prompt(암호 프롬프트 입력**)**	암호를 가져오기 위한 텍스트 문자열을 입력합니다.
Enter Next Token Code(다음 토큰 코드 입력**)**	다음 토큰을 요청하기 위한 텍스트 문자열을 입력합니다.
Choose PIN Type(PIN 유형 선택**)**	PIN 유형을 요청하기 위한 텍스트 문자열을 입력합니다.
Accept System PIN(시스템 **PIN** 수락**)**	시스템에서 생성된 핀 번호를 수락하기 위한 텍스트 문자열을 입력합니다.
Enter Alphanumeric PIN(영숫자 **PIN** 입력**)**	영숫자 PIN을 요청하기 위한 텍스트 문자열을 입력합니다.
Enter Numeric PIN(숫자 **PIN** 입력**)**	숫자 PIN을 요청하기 위한 텍스트 문자열을 입력합니다.
Re-enter PIN(PIN 다시 입력**)**	사용자에게 PIN을 다시 입력하도록 요청하기 위한 텍스트 문자열을 입력합니다.

RSA 메시지 설정

다음 표에서는 **RSA Messages(RSA** 메시지**)** 탭의 필드에 대해 설명합니다.

표 ***88: RSA*** 메시지 설정

필드 이름	사용 지침
Display System PIN Message(시스템 **PIN** 메시지 표시**)**	시스템 PIN 메시지에 레이블을 지정하기 위한 텍스트 문자열을 입력합니다.
Display System PIN Reminder(시스템 **PIN** 알림 표시**)**	사용자에게 새 PIN을 저장하도록 알리기 위한 텍스트 문자열을 입력합니다.

필드 이름	사용 지침
Must Enter Numeric Error(숫자를 입력해야 함 오류**)**	사용자에게 PIN에 숫자만 입력해야 하도록 지시하기 위한 메시지를 입력합니다.
Must Enter Alpha Error(영숫자를 입력해야 함 오류**)**	사용자에게 PIN에 영숫자 문자만 입력해야 하도록 지시하기 위한 메시지를 입력합니다.
PIN Accepted Message(PIN 수락됨 메시지**)**	사용자의 PIN이 시스템에서 수락되면 표시되는 메시지를 입력합니다.
PIN Rejected Message(PIN 거부됨 메시지**)**	시스템에서 사용자의 PIN을 거부하면 표시되는 메시지를 입력합니다.
User Pins Differ Error(사용자 **PIN**이 다름 오류**)**	사용자가 잘못된 PIN을 입력하면 표시되는 메시지를 입력합니다.
System PIN Accepted Message(시스템이 **PIN**을 수락함 메시지**)**	시스템에서 PIN을 수락하면 사용자에게 표시되는 메시지를 입력합니다.
Bad Password Length Error(잘못된 비밀번호 길이 오류**)**	사용자가 지정한 PIN이 PIN 길이 정책에 지정된 범위를 벗어나면 표시되는 메시지를 입력합니다.

관련 항목

RSA ID 소스, 672 페이지
Cisco ISE와 RSA SecurID 서버 통합, 673 페이지
RSA ID 소스 추가, 676 페이지

RSA ID 소스 추가

RSA ID 소스를 생성하려면 RSA 구성 파일(sdconf.rec)을 가져와야 합니다. sdconf.rec 파일은 RSA 관리자에게 받아야 합니다. 이 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

RSA ID 소스를 추가할 때는 다음 작업을 수행합니다.

RSA 구성 파일 가져오기

Cisco ISE에서 RSA ID 소스를 추가하려면 RSA 구성 파일을 가져와야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID** > **Add(**추가**)**를 선택합니다.

단계 **2** **Browse(**찾아보기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 신규 또는 업데이트된 sdconf.rec 파일을 선택합니다.

RSA ID 소스를 처음 생성할 때는 Import new sdconf.rec(새 sdconf.rec 파일 가져오기) 필드가 필수 필드로 지정됩니다. 그 이후에는 필요한 경우에 한해 기존 sdconf.rec 파일을 업데이트된 파일로 교체할 수 있습니다.

단계 **3** 서버 시간 초과 값을 초 단위로 입력합니다. Cisco ISE는 지정된 시간 동안 RSA 서버의 응답을 대기한 후 시간 초과됩니다. 이 값은 1~199 사이의 정수일 수 있습니다. 기본값은 30초입니다.

단계 **4** PIN 변경 시 재인증을 강제로 수행하려면 **Reauthenticate on Change PIN(PIN** 변경 시 재인증**)** 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Cisco ISE에서는 다음 시나리오도 지원합니다.

- Cisco ISE 서버의 옵션 파일을 구성하고 SecurID 및 sdstatus.12 파일 재설정
- RSA ID 소스에 대한 인증 제어 옵션 구성

Cisco ISE 서버의 옵션 파일을 구성하고 SecurID 및 sdstatus.12 파일 재설정

단계 **1** Cisco ISE 서버에 로그인합니다.

단계 **2** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소브**)** > **RSA SecurID** > **Add(**추가**)**를 선택합니다.

단계 **3** **RSA Instance Files(RSA** 인스턴스 파일**)** 탭을 클릭합니다.

이 페이지에는 구축 내 모든 Cisco ISE 서버의 sdopts.rec 파일이 나열됩니다.

사용자가 RSA SecurID 토큰 서버에 대해 인증되면 노드 암호 상태가 *Created(*생성됨*)*로 표시됩니다. 노드 암호 상태는 Create(생성됨) 또는 Not Created(생성되지 않음) 중 하나일 수 있습니다. 지워진 노드의 노드 암호 상태는 *Not Created(*생성되지 않음*)*로 표시됩니다.

단계 **4** 특정 Cisco ISE 서버의 sdopts.rec 파일 옆에 있는 라디오 버튼을 클릭하고 **Update Options File(**옵션 파일 업데이트**)**을 클릭합니다.

기존 파일이 현재 파일 영역에 표시됩니다.

단계 **5** 다음 중 하나를 선택합니다.

- Use the Automatic Load Balancing status maintained by the RSA agent(RSA 에이전트가 유지 관리하는 자동 로드 밸런싱 상태 사용) - RSA 에이전트가 로드 밸런싱을 자동으로 관리하도록 하려면 이 옵션을 선택합니다.
- Override the Automatic Load Balancing status with the sdopts.rec file selected below(아래에서 선택한 sdopts.rec 파일을 사용하여 자동 로드 밸런싱 상태 재정의) - 특정 요구에 따라 로드 밸런싱을 수동으로 구성하려면 이 옵션을 선택합니다. 이 옵션을 선택하는 경우 **Browse(**찾아보기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 새 sdopts.rec 파일을 선택해야 합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** Cisco ISE 서버에 해당하는 행을 클릭하여 해당 서버에 대한 securid 및 sdstatus.12 파일을 재설정합니다.

a) 드롭다운 화살표를 클릭하고 securid 파일 재설정 및 sdstatus.12 파일 재설정 열에서 **Remove on Submit(**제출 시 제거**)**을 선택합니다.

참고 Reset sdstatus.12 File(sdstatus.12 파일 재설정) 필드는 보기에서 숨겨져 있습니다. 이 필드를 표시하려면 맨 안쪽 프레임의 세로 및 가로 스크롤 막대를 사용하여 아래쪽과 오른쪽으로 차례로 스크롤합니다.

b) 변경사항을 저장하려면 이 행에서 **Save(**저장**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

RSA ID 소스에 대한 인증 제어 옵션 구성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID** > **Add(**추가**)**를 선택합니다.

단계 **2** **Authentication Control(**인증 제어**)** 탭을 클릭합니다.

단계 **3** 다음 중 하나를 선택합니다.

- Treat Rejects as "authentication failed"(거부를 "인증 실패"로 처리) - 거부된 요청을 실패한 인증으로 처리하려는 경우 이 옵션을 선택합니다.
- Treat Rejects as "user not found"(거부를 "사용자를 찾을 수 없음"으로 처리) - 거부된 요청을 사용자를 찾을 수 없음 오류로 처리하려는 경우 이 옵션을 선택합니다.

단계 **4** Cisco ISE가 첫 번째 인증에 성공한 후 캐시에 암호를 저장하고 구성된 기간 내에 발생하는 경우 후속 인증에 대해 캐싱된 사용자 자격 증명을 사용하도록 하려면 **Enable Passcode Caching(**암호 캐싱 활성화**)** 확인란을 선택합니다.

Aging Time(에이징 시간**)** 필드의 캐시에 암호가 저장되어야 하는 시간을 초 단위로 입력합니다. 이 기간 동안에는 사용자가 동일한 암호를 사용하여 인증을 2회 이상 수행할 수 있습니다. 기본값은 30초입니다. 유효 범위는 1~300초입니다.

참고 Cisco ISE는 첫 번째 인증 실패 후 캐시를 지웁니다. 사용자는 새 유효 암호를 입력해야 합니다.

참고 이 옵션은 예를 들어 -FAST-GTC 같은 암호의 암호화를 지원하는 프로토콜을 사용할 때만 활성화하는 것이 좋습니다.

단계 **5** 서버에 대해 인증을 수행하지 않는 요청을 처리하게 하려면 **Enable Identity Caching(ID** 캐싱 활성화**)** 확인란을 선택합니다.

ID 캐싱 옵션을 활성화하고 에이징 타임을 분 단위로 설정할 수 있습니다. 기본값은 120분입니다. 유효 범위는 1분~1440분입니다. 마지막으로 성공한 인증에서 얻은 결과와 속성은 지정된 기간 동안 캐시에 보관됩니다.

이 옵션은 기본적으로 비활성화되어 있습니다.

단계 **6** 컨피그레이션을 저장하려면 **Save(**저장**)**를 클릭합니다.

RSA 프롬프트 구성

Cisco ISE에서는 RSA SecurID 서버로 전송되는 요청을 처리하는 동안 사용자에게 제공되는 RSA 프롬프트를 구성할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Prompts(**프롬프트**)**를 클릭합니다.

단계 **3** RSA SecurID ID 소스 설정의 설명에 따라 값을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

RSA 메시지 구성

Cisco ISE에서는 RSA SecurID 서버로 전송되는 요청을 처리하는 동안 사용자에게 제공되는 메시지를 구성할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Prompts(**프롬프트**)**를 클릭합니다.

단계 **3** **Messages(**메시지**)** 탭을 클릭합니다.

단계 **4** RSA SecurID ID 소스 설정의 설명에 따라 값을 입력합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

외부 ID 소스로서의 SAMLv2 ID 제공자

SAML(Security Assertion Markup Language)은 관리자가 정의된 애플리케이션 중 하나에 로그인한 후에 해당 애플리케이션에 원활히 액세스하도록 해주는 XML 기반의 개방형 표준 데이터 형식입니다. SAML은 신뢰할 수 있는 비즈니스 파트너 간의 보안 관련 정보 교환에 대해 설명합니다. SAML은 IdP(Identity Provider)와 통신 사업자(이 경우 ISE) 간에 보안 인증 정보 교환을 가능하게 합니다.

SAML SSO(Single Sign On)는 메타데이터 및 인증서를 프로비저닝 프로세스의 일부로 IdP와 서비스 제공자 간에 교환하여 CoT(Circle of Trust)를 설정합니다. 서비스 제공자는 IdP의 사용자 정보를 신뢰하여 다양한 서비스 또는 애플리케이션에 대한 액세스를 제공합니다.

SAML SSO를 사용하면 다음과 같이 다양한 이점을 얻을 수 있습니다.

- 서로 다른 사용자 이름 및 비밀번호 조합을 입력하지 않아도 되므로 비밀번호를 사용하는 데 따르는 번거로움이 줄어듭니다.
- 동일한 ID에 대한 자격 증명을 다시 입력해야 하는 시간을 줄일 수 있으므로 생산성이 향상됩니다.
- 애플리케이션을 호스팅하는 시스템에서 인증을 타사 시스템으로 전송합니다.
- 비밀번호 재설정을 위한 헬프 데스크 호출 건수가 줄어들어 비용이 낮아지므로 더 많은 비용 절감 효과를 거둘 수 있습니다.

IdP는 사용자, 시스템 또는 서비스를 위한 ID 정보를 생성, 유지 및 관리하는 인증 모듈입니다. IdP는 사용자 자격 증명을 저장 및 검증하고, SAML 응답을 생성하므로 사용자는 서비스 제공자에 의해 보호된 리소스에 액세스할 수 있습니다.

참고 관리자는 IdP 서비스에 대해 잘 알고 있어야 하며, 현재 설치되어 작동 중인지 확인해야 합니다.

SAML SSO는 다음 포털에서 지원됩니다.

- 게스트 포털(스폰서 및 셀프 등록)
- 스폰서 포털
- 내 디바이스 포털
- 인증서 프로비저닝 포털

BYOD 포털의 외부 ID 소스로 IdP를 선택할 수 없지만, 게스트 포털에 사용할 IdP를 선택하고 BYOD 플로우를 활성화할 수 있습니다.

Cisco ISE는 SAMLv2를 준수하며 Base64 인코딩 인증서를 사용하는 모든 SAMLv2 준수 IdP를 지원합니다. 아래에는 Cisco ISE에서 테스트된 IdP가 나와 있습니다.

- OAM(Oracle Access Manager)
- OIF(Oracle Identity Federation)
- SecureAuth
- PingOne
- PingFederate
- Azure Active Directory

IdP는 ID 소스 시퀀스에 추가할 수 없습니다.

지정된 시간(기본값은 5분) 동안 활동이 없는 경우 SSO 세션이 종료되고 세션 시간 제한 오류 메시지가 표시됩니다.

포털의 오류 페이지에 Sign On Again(다시 로그인) 버튼을 추가하려면 포털 오류 페이지의 Optional Content(선택적 콘텐츠) 필드에 다음 JavaScript를 추가해 주십시오.

```
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b"
id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'"
type="button">SignOn Again</button>
```

Cisco ISE에서 SAML ID 제공자 구성

Cisco ISE에서 SAML ID 제공자를 구성하려면,

- Cisco ISE에서 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- IdP(ID 제공자)가 인증서에 셀프 서명을 하지 않은 경우 신뢰할 수 있는 인증서 저장소로 CA(Certificate Authority) 인증서를 가져옵니다.
- 구성중인 IdP 포털에 대한 관리자 액세스 권한이 있어야 합니다. 다음 작업에는 IdP 포털에서 수행해야 하는 몇 가지 단계가 포함되어 있습니다.

Cisco ISE에서 SAML ID 제공자를 구성하려면,

1. Cisco ISE에 SAML ID 제공자를 추가합니다.
2. 포털의 인증 방법으로 SAML ID 제공자를 추가합니다.
3. SAML ID 공급자를 구성합니다.

Cisco ISE에 SAML ID 제공자 추가

단계 **1** **Administration(**관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **SAML Id Providers(SAML ID** 제공자**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 표시된 **SAML Identity Provider(SAML ID** 제공자**)** 창의 **General(**일반**)** 탭에서 **Id Provider Name(ID** 제공자 이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

단계 **5** **Identity Provider Config(ID** 제공자 컨피그레이션**)** 탭에서 관련 메타 데이터 .xml 파일을 가져오고 **Submit(**제출**)**을 클릭합니다.

포털의 인증 방법으로 SAML ID 제공자 추가

방금 생성한 SAML ID 제공자를 다음 포털에 추가할 수 있습니다.

1. 셀프 등록 게스트 포털 및 스폰서 게스트 포털(**Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals and Components(**포털 및 구성 요소**)**)

2. 인증서 프로비저닝 포털(**Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Certificate Provisioning(**인증서 프로비저닝**)** > **Certificate Provisioning Portal(**인증서 프로비저닝 포털**)**)

단계 **1** 구성중인 포털의 포털 사용자 맞춤화 창에서 **Portal Settings(**포털 설정**)**를 클릭합니다.

단계 **2** 표시되는 드롭 다운 섹션에서 **Authentication Method(**인증 방법**)** 섹션으로 이동하여 메뉴를 사용하여 추가한 SAML IP 제공자를 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

SAML ID 제공자 구성

단계 **1** **Administration(**관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **SAML Id Providers(SAML ID** 제공자**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 . 해당 포털에 방금 연결한 IdP를 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **2** (선택 사항) Cisco ISE 노드의 로드를 최적화하기 위해 로드 밸런서를 사용하는 경우 IdP 구성을 간소화하기 위해 **Service Provider Info(**서비스 제공자 정보**)** 탭에서 세부정보를 추가할 수 있습니다. 소프트웨어 또는 하드웨어 로드 밸런서를 추가할 수 있습니다.

Portal Settings(포털 설정**)** 창에 지정된 포트를 사용하여 로드 밸런서에서 구축 환경의 Cisco ISE 노드로 요청을 전달할 수 있어야 합니다.

로드 밸런서를 추가한 경우에는 서비스 제공자 메타데이터 파일에서 로드 밸런서 URL만 제공됩니다. 로드 밸런서가 없으면 서비스 제공자 메타데이터 파일에 여러 **AssertionConsumerService** URL이 포함됩니다.

참고 포털 FQDN 설정에서 로드 밸런서에 대한 동일한 주소를 사용하지 않는 것이 권장됩니다.

단계 **3** **Service Provider Info(**통신 사업자 정보**)** 탭에서 **Export(**내보내기**)**를 클릭하여 통신 사업자 메타데이터 파일을 내보냅니다. 내보낸 메타데이터에는 Cisco ISE의 서명 인증서가 포함되어 있습니다. 이 서명 인증서는 선택한 포털의 인증서와 동일합니다.

내보낸 메타데이터 zip 폴더에는 각 IdP(Azure Active Directory, PingOne, PingFederate, SecureAuth, OAM 등)를 구성하기 위한 기본적인 지침이 포함된 추가 정보 파일이 들어 있습니다.

다음 사항이 변경된 경우에는 서비스 제공자 메타데이터를 다시 내보내야 합니다.

- 새 Cisco ISE 노드 등록
- 노드의 호스트 이름 또는 IP 주소
- 내 디바이스, 스폰서 또는 인증서 프로비저닝 포털의 FQDN(Fully Qualified Domain Name)
- 포트 또는 인터페이스 설정
- 연결된 로드 밸런서

업데이트된 메타데이터를 다시 내보내지 않으면 IdP 쪽에서 사용자 인증 요청을 거부할 수 있습니다.

단계 **4** IdP 포털로 이동하여 관리자로 로그인한 다음 방금 Cisco ISE에서 내보낸 서비스 제공자 메타데이터 파일을 가져옵니다. 먼저 포털 이름을 사용하여 내보낸 폴더와 메타데이터 파일의 압축을 풀어야 합니다. 메타데이터 파일에는 제공자 ID 및 바인딩 URI가 포함되어 있습니다.

단계 **5** Cisco ISE 포털로 돌아갑니다.

단계 **6** (선택 사항) **SAML Identity Provider(SAML ID** 제공자**)** 창의 **Groups(**그룹**)** 탭에서 필요한 사용자 그룹을 추가합니다.

Group Membership Attribute(그룹 멤버십 속성**)** 필드에 사용자의 그룹 멤버십을 지정하는 어설션 속성을 입력합니다.

단계 **7** (선택 사항) **Attributes(**속성**)** 탭에서 사용자 속성을 추가하여 IdP에서 반환된 어설션에 속성이 표시되는 방식을 지정합니다.

Name in ISE(ISE 내 이름**)** 필드에서 지정하는 이름이 정책 규칙에 표시됩니다.

다음 데이터 유형이 속성에 대해 지원됩니다.

- 문자열
- 정수
- IPv4
- 부울

단계 **8** **Advanced Settings(**고급 설정**)** 탭에서 다음 옵션을 구성합니다.

옵션	설명
ID 속성	표시된 옵션에 대해 라디오 버튼을 클릭하여 인증 중인 사용자의 ID를 지정하는 속성을 선택합니다. 참고 Cisco ISE는 SAML IdP 임시 또는 영구 형식의 주체 이름(NameID)을 포함하는 응답을 지원하지 않습니다. 이러한 방법을 사용할 경우 Cisco ISE는 사용자 이름 속성 어설션을 검색할 수 없으며 인증은 실패하게 됩니다.
이메일 속성	드롭다운 목록에서 사용자의 이메일 주소를 반환하는 어설션 속성을 선택합니다. 스폰서 하나에 대해 승인할 스폰서 게스트 목록을 필터링(제한)하려는 경우 이메일 속성을 구성해야 합니다.
다중 값 속성	다음 중 하나를 선택합니다. • **Each value in a separate XML(**개별 **XML**의 각 값**)**: IdP가 개별 XML 요소에서 속성이 같은 여러 값을 반환하는 경우 이 옵션을 클릭합니다. • **Multiple values in a single XML(**단일 **XML**의 여러 값**)**: IdP가 단일 XML 요소의 여러 값을 반환하는 경우 이 옵션을 클릭합니다. 텍스트 상자에서 구분 기호를 지정합니다.
로그아웃 설정	로그아웃 요청에 서명하려면 **Sign Logout Requests(**로그아웃 요청 서명**)** 확인란을 선택합니다. 구성 중인 IdP가 Oracle Access Manager 또는 Oracle Identity Federation인 경우 이 옵션은 표시되지 않습니다. 참고 SecureAuth에서는 SAML 로그아웃을 지원하지 않습니다.

옵션	설명
	다음 옵션은 Oracle Access Manager 또는 Oracle Identity Federation IdP를 구성하고 로드 밸런서를 구성하지 않은 경우에만 표시됩니다. • **Logout URL(**로그아웃 **URL)**: 사용자가 스폰서 또는 내 디바이스 포털에서 로그아웃할 때 SSO 세션을 종료하도록 리디렉션되는 페이지의 URL을 입력합니다. • **Redirect Parameter Name(**리디렉션 매개변수 이름**)**: SSO 세션이 종료되면 사용자가 IdP의 로그인 페이지로 돌아갑니다. 리디렉션 매개변수 이름은 IdP에 따라 다를 수 있습니다(예: **end_url** 또는 **returnURL**). 이 필드는 대/소문자를 구분합니다. 정상적으로 로그아웃되지 않는 경우 IdP 설명서에서 로그아웃 URL 및 리디렉션 매개변수 이름에 대한 세부정보를 확인하십시오.
인증 상황	이 섹션을 사용하여 SAML IdP 인증 상황 클래스 참조를 편집합니다. Cisco ISE SAML 요청은 일반적으로 SAML 요청 제목에서 **PasswordProtectedTransport** 인증 방법을 사용했습니다. 이로 인해 다중 인증이 사용되는 경우 인증이 실패하게 됩니다. 이를 방지하기 위해 **AuthnContextClassRef SAML Element** 섹션을 사용하여 인증 방법을 지정할 수 있습니다. 사용된 인증 방법을 잘 모를 경우 인증 실패를 방지하기 위해 이 섹션을 비워 두는 것이 좋습니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

ID 제공자 삭제

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

삭제할 IdP가 포털에 연결되어 있지 않은지 확인합니다. IdP가 포털에 연결되어 있으면 삭제 작업이 실패합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > Network Access(**네트워크 액세스**) > Ext Id Sources(**외부 **ID** 소스**) > SAML Id Providers(SAML ID** 제공자**)**를 선택합니다.

단계 **2** 삭제할 IdP 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

단계 **3** 선택한 IdP를 삭제하려면 **OK(**확인**)**를 클릭합니다.

인증 장애 로그

SAML ID 저장소에 대한 인증에서 장애가 발생하고 IdP가 SAML 응답을 통해 사용자를 다시 ISE 포털로 리디렉션하면 ISE는 인증 로그에 실패 이유를 보고하게 됩니다. 게스트 포털의 경우 BYOD 플

로우 활성화 여부에 관계없이 RADIUS 라이브 로그를 확인(Operations(운영) > RADIUS > Live Log(라이브 로그))하여 인증 실패 이유를 확인할 수 있습니다. 내 디바이스 포털 및 스폰서 포털의 경우 내 디바이스 로그인/감사 보고서 및 스폰서 로그인/감사 보고서를 확인(Operations(운영) > Reports(보고서) > Guest(게스트))하여 인증 실패 이유를 확인할 수 있습니다.

로그아웃 장애 발생 시 보고서와 로그를 확인하여 내 디바이스, 스폰서 및 게스트 포털에 대한 실패 이유를 확인할 수 있습니다.

인증은 다음과 같은 이유로 실패할 수 있습니다.

- SAML 응답 구문 분석 오류
- SAML 응답 검증 오류(예: 잘못된 발급자)
- SAML 어설션 검증 오류(예: 잘못된 대상)
- SAML 응답 서명 검증 오류(예: 잘못된 서명)
- IdP 인증서 서명 오류(예: 인증서 취소됨)

참고 Cisco ISE는 암호화된 어설션을 사용하는 SAML 응답을 지원하지 않습니다. IdP에서 이 기능이 구성된 경우 ISE에 다음 오류 메시지가 표시됩니다. `FailureReason=24803 Unable to find 'username' attribute assertion.`

인증이 실패하는 경우 인증 로그에서 "DetailedInfo" 속성을 확인하는 것이 좋습니다. 이 속성은 실패 원인에 대한 추가 정보를 제공합니다.

ID 소스 시퀀스

ID 소스 시퀀스는 Cisco ISE가 여러 데이터베이스에서 사용자 자격 증명을 찾는 순서를 정의합니다.

Cisco ISE에 연결된 여러 데이터베이스에 사용자 정보가 있는 경우 Cisco ISE가 이러한 ID 소스에서 정보를 찾는 순서를 정의할 수 있습니다. 일치 항목이 발견되면 Cisco ISE는 추가로 검색하지 않고 자격 증명을 평가한 후 사용자에게 결과를 반환합니다. 이는 처음 일치 정책입니다.

ID 소스 시퀀스 생성

시작하기 전에

Cisco ISE에서 외부 ID 소스를 구성했는지 확인합니다.

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

게스트 사용자가 로컬 WebAuth를 통해 인증하도록 허용하려면 게스트 포털 인증 소스와 ID 소스 시퀀스가 동일한 ID 저장소를 포함하도록 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identity Source Sequences(ID** 소스 시퀀스**)** > **Add(**추가**)**를 선택합니다.

단계 **2** ID 소스 시퀀스의 이름을 입력합니다. 원하는 경우 설명을 입력할 수도 있습니다.

단계 **3** **Select Certificate Authentication Profile(**인증서 인증 프로파일 선택**)** 확인란을 선택하고 인증서 기반 인증용 인증서 인증 프로파일을 선택합니다.

단계 **4** ID 소스 시퀀스에 포함할 하나 이상의 데이터베이스를 **Selected List(**선택됨 목록**)** 필드에서 선택합니다.

단계 **5** Cisco ISE가 데이터베이스를 검색하도록 할 순서대로 **Selected List(**선택됨 목록**)** 필드의 데이터베이스를 다시 정렬합니다.

단계 **6** **Advanced Search List(**고급 검색 목록**)** 영역에서 다음 옵션 중 하나를 선택합니다.

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError(**시퀀스의 다른 저장소에 액세스하지 않고 **AuthenticationStatus** 속성을 **ProcessError**로 설정**)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 검색을 중지하도록 하려면 이 옵션을 선택합니다.
- **Treat as if the user was not found and proceed to the next store in the sequence(**사용자를 찾지 못한 것으로 간주하여 다음 저장소로 순차 진행**)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 시퀀스에서 선택한 다른 ID 소스에서 검색을 계속하도록 하려면 이 옵션을 선택합니다.

  요청을 처리하는 동안 Cisco ISE는 이러한 ID 소스를 순서대로 검색합니다. Selected list(선택됨 목록) 필드의 ID 소스가 Cisco ISE가 검색하도록 할 순서대로 나열되어 있는지 확인합니다.

단계 **7** ID 소스 시퀀스를 생성하려면 **Submit(**제출**)**을 클릭합니다. 생성된 시퀀스는 정책에서 사용할 수 있습니다.

ID 소스 시퀀스 삭제

정책에서 더 이상 사용하지 않는 ID 소스 시퀀스를 삭제할 수 있습니다.

시작하기 전에

- 삭제하려는 ID 소스 시퀀스가 인증 정책에서 사용되지 않는지 확인합니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identity Source Sequences(ID** 소스 시퀀스**)**를 선택합니다.

단계 **2** 삭제할 하나 이상의 ID 소스 시퀀스 옆에 있는 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

단계 **3** **OK(**확인**)**를 클릭하여 하나 이상의 ID 소스 시퀀스를 삭제합니다.

보고서의 ID 소스 세부정보

Cisco ISE는 인증 dashlet 및 ID 소스 보고서에서 ID 소스에 대한 정보를 제공합니다.

인증 Dashlet

인증 dashlet에서 실패 이유를 비롯한 추가 정보를 드릴다운할 수 있습니다.

실시간 인증 요약을 확인하려면 Operations(작업) > RADIUS Livelog(RADIUS 라이브 로그)를 선택합니다. RADIUS 라이브 로그에 대한 자세한 내용은 RADIUS 라이브 로그, 319 페이지을 참고하십시오.

ID 소스 보고서

Cisco ISE는 ID 소스에 대한 정보가 포함된 다양한 보고서를 제공합니다. 이러한 보고서에 대한 설명은 사용 가능한 보고서 섹션을 참고해 주십시오.

네트워크에서 프로파일링된 엔드포인트

프로파일러 서비스는 디바이스 유형에 관계없이 네트워크의 모든 엔드포인트 기능(Cisco ISE에서 ID라고 함)을 식별하고 찾고 확인하는 데 도움이 됩니다. 이를 통해 엔터프라이즈 네트워크에 적절하게 액세스하는지 확인하고 이러한 액세스를 유지 관리할 수 있습니다. Cisco ISE 프로파일러 기능은 여러 프로브를 사용하여 네트워크의 모든 엔드포인트에 대한 속성을 수집하고 이를 프로파일러 분석기로 전달합니다. 여기서 알려진 엔드포인트는 연결된 정책 및 ID 그룹에 따라 분류됩니다.

Cisco ISE에서 프로파일러 피드 서비스를 사용하는 관리자는 지정된 Cisco 피드 서버에서 서브스크립션을 통해 신규 및 업데이트된 엔드포인트 프로파일링 정책 및 업데이트된 OUI 데이터베이스를 피드로 가져올 수 있습니다.

프로파일러 조건 설정

다음 표에서는 프로파일러 조건 창의 필드에 대해 설명합니다. 이 창의 탐색 경로는 **Policy(정책)** > **Policy Elements(정책 요소)** > **Conditions(조건)** > **Profiling(프로파일링)**입니다.

표 ***89:*** 프로파일러 조건 설정

필드 이름	사용 지침
Name(이름)	프로파일러 조건의 이름입니다.
Description(설명)	프로파일러 조건의 설명입니다.
Type(유형)	미리 정의된 유형 중 하나를 선택합니다.

필드 이름	사용 지침
Attribute Name(속성 이름**)**	프로파일러 조건의 기준으로 사용할 속성을 선택합니다.
Operator(연산자**)**	연산자를 선택합니다.
Attribute Value(속성 값**)**	선택한 속성에 대한 값을 입력합니다. 미리 정의된 속성 값을 포함하는 속성 이름의 경우 이 옵션에는 미리 정의된 값이 포함된 드롭다운 목록이 표시되며, 이 목록에서 값을 선택할 수 있습니다.
System Type(시스템 유형**)**	프로파일링 조건은 다음 유형 중 하나일 수 있습니다. • **Cisco** 제공: 구축 시 Cisco ISE에서 제공되는 프로파일링 조건은 Cisco 제공으로 식별됩니다. 이러한 조건은 시스템에서 삭제하거나 편집할 수 없습니다. • 관리자 생성: Cisco ISE의 관리자가 생성하는 프로파일링 조건은 관리자 생성으로 식별됩니다.

관련 항목

Cisco ISE 프로파일링 서비스, 688 페이지
프로파일러 조건, 716 페이지
프로파일러 피드 서비스, 758 페이지
프로파일러 조건 생성, 732 페이지

Cisco ISE 프로파일링 서비스

Cisco ISE(Identity Services Engine)의 프로파일링 서비스는 네트워크에 연결되는 디바이스와 해당 위치를 식별합니다. 엔드포인트는 Cisco ISE에서 구성한 엔드포인트 프로파일링 정책에 따라 프로파일링됩니다. 그런 다음 Cisco ISE는 정책 평가 결과를 기준으로 네트워크의 리소스에 액세스할 수 있는 권한을 엔드포인트에 부여합니다.

프로파일링 서비스:

- 다양한 규모와 복잡성을 지닌 모든 엔터프라이즈 네트워크에 IEEE 표준 802.1X 포트 기반 인증 액세스 제어, MAB(MAC Authentication Bypass) 인증 및 NAC(Network Admission Control)를 사용하여 효율적이고 효과적인 구축과 지속적인 인증 관리를 촉진합니다.
- 엔드포인트 유형에 관계없이 연결된 모든 네트워크 엔드포인트의 기능을 식별하거나 찾고 결정합니다.
- 일부 엔드포인트에 대한 액세스를 실수로 거부하지 못하게 보호합니다.

ISE 커뮤니티 리소스

ISE 엔드포인트 프로파일

방법: ISE 프로파일링 설계 가이드

프로파일러 작업 센터

프로파일러 작업 센터 메뉴(Work Centers[작업 센터] > Profiler[프로파일러])에는 ISE 관리자에게 단일 시작점 역할을 하는 모든 프로파일러 페이지가 포함되어 있습니다. 프로파일러 작업 센터 메뉴에는 Overview(개요), Ext ID Stores(외부 ID 저장소), Network Devices(네트워크 디바이스), Endpoint Classification(엔드포인트 분류), Node Config(노드 컨피그레이션), Feeds(피드), Manual Scans(수동 스캔), Policy Elements(정책 요소), Profiling Policies(프로파일링 정책), Authorization Policy(권한 부여 정책), Troubleshoot(문제 해결), Reports(보고서), Settings(설정) 및 Dictionaries(사전) 옵션이 포함되어 있습니다.

프로파일러 대시보드

프로파일러 대시보드(Work Centers[작업 센터] > Profiler[프로파일러] > Endpoint Classification[엔드포인트 분류])는 네트워크의 프로파일, 엔드포인트 및 자산용 중앙 집중식 모니터링 툴입니다. 대시보드에는 데이터가 그래픽 및 표 형식으로 표시됩니다. 프로파일 대시릿에는 네트워크에서 현재 활성 상태인 논리 프로파일과 엔드포인트 프로파일이 표시됩니다. 엔드포인트 대시릿에는 네트워크에 연결하는 엔드포인트의 ID 그룹, PSN 및 OS 유형이 표시됩니다. 자산 대시릿에는 Guest(게스트), BYOD, Corporate(기업) 등의 플로우가 표시됩니다. 표에는 연결된 다양한 엔드포인트가 표시되며, 새 엔드포인트를 추가할 수도 있습니다.

프로파일링 서비스를 사용하는 엔드포인트 인벤토리

프로파일링 서비스를 사용하여 네트워크에 연결된 모든 엔드포인트의 기능을 검색하고 찾고 확인할 수 있습니다. 그러면 디바이스 유형에 관계없이 엔드포인트가 엔터프라이즈 네트워크에 적절하게 액세스하는지 확인하고 이러한 액세스를 유지 관리할 수 있습니다.

프로파일링 서비스는 네트워크 디바이스와 네트워크에서 엔드포인트의 속성을 수집하고, 프로파일에 따라 엔드포인트를 특정 그룹으로 분류하고, 일치하는 프로파일과 함께 엔드포인트를 Cisco ISE 데이터베이스에 저장합니다. 프로파일링 서비스가 처리하는 모든 속성을 프로파일러 사전에서 정의해야 합니다.

프로파일링 서비스는 네트워크의 각 엔드포인트를 식별한 다음 프로파일에 따라 이러한 엔드포인트를 시스템의 기존 엔드포인트 ID 그룹이나 시스템에서 생성할 수 있는 새 그룹으로 그룹화합니다. 이와 같이 엔드포인트를 그룹화하고 엔드포인트 ID 그룹에 엔드포인트 프로파일링 정책을 적용하면 해당하는 엔드포인트 프로파일링 정책에 대한 엔드포인트의 매핑을 결정할 수 있습니다.

Cisco ISE 프로파일러 큐 제한 컨피그레이션

Cisco ISE 프로파일러는 짧은 시간 동안 네트워크에서 막대한 양의 엔드포인트 데이터를 수집합니다. 따라서 일부 느려진 Cisco ISE 구성 요소가 프로파일러에서 생성된 데이터를 처리할 때 누적된 백로그로 인해 JVM(Java Virtual Machine) 메모리 사용률이 높아지고 결과적으로 성능 저하 및 안정성 문제가 발생할 수 있습니다.

프로파일러에서 JVM 메모리 사용률이 증가하지 않고 JVM의 메모리가 부족해져 다시 시작되는 것을 방지하기 위해 프로파일러의 다음 내부 구성 요소에 제한이 적용됩니다.

- 엔드포인트 캐시: 크기가 제한을 초과하는 경우 주기적으로 (가장 최근에 사용한 전략에 따라) 제거되도록 내부 캐시의 크기가 제한됩니다.
- 전달자: 프로파일러에서 수집되는 엔드포인트 정보의 기본 인그레스 큐입니다.
- 이벤트 처리기: 느린 처리 구성 요소(일반적으로 데이터베이스 쿼리 관련)에 데이터를 공급하는 빠른 구성 요소의 연결을 끊는 내부 큐입니다.

엔드포인트 캐시

- maxEndPointsInLocalDb = 100000(캐시의 엔드포인트 객체)
- endPointsPurgeIntervalSec = 300(초당 엔드포인트 캐시 제거 스레드 간격)
- numberOfProfilingThreads = 8(스레드 수)

이 제한은 모든 프로파일러 내부 이벤트 처리기에 적용됩니다. 큐 크기 제한에 도달하면 모니터링 경보가 트리거됩니다.

Cisco ISE 프로파일러 큐 크기 제한

- forwarderQueueSize = 5000(엔드포인트 수집 이벤트)
- eventHandlerQueueSize = 10000(이벤트)

이벤트 처리기

- NetworkDeviceEventHandler: 이미 캐시된 중복 NAD(Network Access Device) IP 주소 필터링 외에 네트워크 디바이스 이벤트에 사용
- ARPCacheEventHandler: ARP 캐시 이벤트에 사용

화성 IP 주소

RADIUS 구문 분석기가 프로파일링 서비스에 도달하기 전에 화성 IP 주소를 제거하므로 해당 주소는 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** 및 **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Endpoint Classification(**엔드포인트 분류**)**창에 표시되지 않습니다. 화성 IP 주소는 공격에 취약하기 때문에 보안 문제가 됩니다. 그러나 화성 IP 주소는 감사 목적으로 MnT 로그에 표시됩니다. 이 동작은 멀티캐스트 IP 주소의 경우에도 마찬가지입니다. 화성 IP 주소에 대한 자세한 내용은

https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/250/index.html#page/tesla_250_olh/martian_addresses.html을 참조하십시오.

프로파일러 전환 지속성 대기열

프로파일러 전환 지속성 대기열은 프로파일러 모듈로 전송되기 전에 추후 처리에 사용할 수 있도록 이벤트를 저장합니다. 또한 증가된 이벤트 처리를 지원하기 위해 대기열에 저장 가능한 용량도 늘어났습니다. 이렇게 하면 이벤트 수가 갑자기 증가하여 손실되는 이벤트 수가 감소하게 됩니다. 대기열이 최대 한도에 도달하면 경보가 줄어듭니다.

이 기능은 기본적으로 활성화되어 있습니다. 필요한 경우 해당 기능을 비활성화하여 이벤트가 프로파일러 모듈로 직접 전송되는 원래 메커니즘으로 대체할 수 있습니다. 이 기능을 활성화하거나 비활성화하려면 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Profiling(**프로파일링**)**을 선택하고 **Enable Profiler Forwarder Persistence Queue(**프로파일러 전환 지속성 대기열**)** 확인란을 선택하거나 선택 취소합니다.

Cisco ISE 노드에서 프로파일링 서비스 구성

Cisco ISE가 활성화된 네트워크에서 네트워크 리소스를 사용하는 모든 엔드포인트의 상황별 인벤토리를 제공하는 프로파일링 서비스를 구성할 수 있습니다.

기본적으로 관리, 모니터링 및 정책 서비스 페르소나 역할을 모두 수행하는 단일 Cisco ISE 노드에서 실행되도록 프로파일링 서비스를 구성할 수 있습니다.

분산형 구축에서 프로파일링 서비스는 정책 서비스 페르소나 역할을 하는 Cisco ISE 노드에서만 실행되며, 관리 및 모니터링 페르소나 역할을 하는 기타 Cisco ISE 노드에서는 실행되지 않습니다.

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

단계 **2** 정책 서비스 페르소나 역할을 하는 Cisco ISE 노드를 선택합니다.

단계 **3** 구축 노드 페이지에서 **Edit(**편집**)**를 클릭합니다.

단계 **4** **General Settings(**일반 설정**)** 탭에서 **Policy Service(**정책 서비스**)** 확인란을 선택합니다. Policy Service(정책 서비스) 확인란 선택을 취소하면 세션 서비스와 프로파일링 서비스 확인란이 모두 비활성화됩니다.

단계 **5** 다음 작업을 수행합니다.

a) 네트워크 액세스, 포스처, 게스트 및 클라이언트 프로비저닝 세션 서비스를 실행하려면 **Enable Session Services(**세션 서비스 활성화**)** 확인란을 선택합니다.

b) 프로파일링 서비스를 실행하려면 **Enable Profiling Services(**프로파일링 서비스 활성화**)** 확인란을 선택합니다.

c) 디바이스 관리 서비스를 실행하여 기업의 네트워크 디바이스를 제어하고 감사하려면 **Enable Device Admin Service(**디바이스 관리 서비스 활성화**)** 확인란을 선택합니다.

단계 **6** **Save(**저장**)**를 클릭하여 노드 컨피그레이션을 저장합니다.

프로파일링 서비스에 사용되는 네트워크 프로브

네트워크 프로브는 네트워크의 엔드포인트에서 속성 또는 속성 집합을 수집하는데 사용되는 방법입니다. 프로브를 사용하면 엔드포인트를 생성하거나 Cisco ISE 데이터베이스에서 엔드포인트와 일치하는 프로파일로 엔드포인트를 업데이트할 수 있습니다.

Cisco ISE는 네트워크의 디바이스 동작을 분석하고 디바이스 유형을 확인하는 여러 네트워크 프로브를 사용하여 디바이스를 프로파일링할 수 있습니다. 네트워크 프로브는 네트워크를 보다 효과적으로 파악하도록 도와줍니다.

IP 주소와 MAC 주소 바인딩

엔터프라이즈 네트워크에서 엔드포인트의 MAC 주소를 사용하는 방법으로만 엔드포인트를 생성하거나 업데이트할 수 있습니다. ARP 캐시에서 엔트리를 찾을 수 없으면 Cisco ISE에서 NetFlow 패킷의 IN_SRC_MAC 및 HTTP 패킷의 L2 MAC 주소를 사용하여 엔드포인트를 생성하거나 업데이트할 수 있습니다. 엔드포인트가 1홉 거리에 있을 때는 L2 인접도에 따라 프로파일링 서비스가 달라집니다. 엔드포인트가 L2에 인접해 있으면 엔드포인트의 IP 주소와 MAC 주소는 이미 매핑되어 있으므로 IP-MAC 캐시 매핑을 수행할 필요가 없습니다.

엔드포인트가 L2에 인접해 있지 않으며 여러 홉 거리에 있으면 매핑이 안정적으로 수행되지 않을 수 있습니다. 수집하는 NetFlow 패킷의 알려진 속성으로는 PROTOCOL, L4_SRC_PORT, IPV4_SRC_ADDR, L4_DST_PORT, IPV4_DST_ADDR, IN_SRC_MAC, OUT_DST_MAC, IN_SRC_MAC, OUT_SRC_MAC 등이 있습니다. 엔드포인트가 L2에 인접해 있지 않으며 여러 L3 홉 거리에 있으면 IN_SRC_MAC 속성은 L3 네트워크 디바이스의 MAC 주소만 전달합니다. Cisco ISE에서 HTTP 프로브가 활성화되어 있으면 HTTP 패킷의 MAC 주소를 사용하는 방법으로만 엔드포인트를 생성할 수 있습니다. HTTP 요청 메시지가 페이로드 데이터에서 엔드포인트의 IP 주소 및 MAC 주소를 전달하지 않기 때문입니다.

엔드포인트의 IP 주소와 MAC 주소를 안정적으로 매핑할 수 있도록 Cisco ISE는 프로파일링 서비스에서 ARP 캐시를 구현합니다. ARP 기능이 작동하려면 DHCP 프로브 또는 RADIUS 프로브를 활성화해야 합니다. DHCP 및 RADIUS 프로브는 페이로드 데이터에서 엔드포인트의 IP 주소 및 MAC 주소를 전달합니다. DHCP 프로브의 dhcp-requested address 속성과 RADIUS 프로브의 Framed-IP-address 속성은 엔드포인트의 IP 주소를 해당 MAP 주소와 함께 전달하며, 이 IP 주소를 매핑하여 ARP 캐시에 저장할 수 있습니다.

NetFlow 프로브

Cisco ISE 프로파일러는 Cisco IOS NetFlow 버전 9를 구현합니다. Cisco ISE 프로파일링 서비스를 지원하기 위해 프로파일러를 개선하는 데 필요한 추가 기능이 포함되어 있는 NetFlow 버전 9를 사용하는 것이 좋습니다.

NetFlow가 활성화된 네트워크 액세스 디바이스에서 NetFlow 버전 9 속성을 수집하여 엔드포인트를 생성하거나 Cisco ISE 데이터베이스의 기존 엔드포인트를 업데이트할 수 있습니다. 엔드포인트의 소스 및 대상 MAC 주소를 연결하고 업데이트하도록 NetFlow 버전 9를 구성할 수 있습니다. 또한 NetFlow 기반 프로파일링을 지원하기 위해 NetFlow 속성 사전을 생성할 수도 있습니다.

NetFlow 버전 9 기록 형식에 대한 자세한 내용은 NetFlow 버전 9 흐름 기록 형식 문서의 표 6 "NetFlow 버전 9 필트 유형 정의"를 참고해 주십시오.

Cisco ISE는 버전 5 이전의 NetFlow 버전도 지원합니다. 네트워크에서 NetFlow 버전 5를 사용하는 경우, 다른 위치에서는 해당 버전이 작동하지 않으므로 액세스 레이어의 기본 NAD(Network Access Device)에서만 버전 5를 사용할 수 있습니다.

Cisco IOS NetFlow 버전 5 패킷은 엔드포인트의 MAC 주소를 포함하지 않습니다. NetFlow 버전 5에서 수집된 속성을 Cisco ISE 데이터베이스에 직접 추가할 수는 없습니다. IP 주소를 사용하여 엔드포인트를 검색하고 NetFlow 버전 5 속성을 엔드포인트에 추가할 수 있습니다. 이렇게 하려면 네트워크 액세스 디바이스의 IP 주소와 NetFlow 버전 5 속성에서 가져온 IP 주소를 결합합니다. 단, 이렇게 하려면 RADIUS 또는 SNMP 프로브를 사용하여 이러한 엔드포인트를 이전에 검색한 상태여야 합니다.

NetFlow 버전 5 이전의 버전에서는 MAC 주소가 IP 흐름의 일부분이 아니므로 엔드포인트 캐시에서 네트워크 액세스 디바이스로부터 수집한 속성 정보의 상관관계를 지정하여 IP 주소로 엔드포인트를 프로파일링해야 합니다.

NetFlow 버전 5 기록 형식에 대한 자세한 내용은 NetFlow 서비스 솔루션 설명서의 표 2 "Cisco ISO NetFlow 흐름 기록 및 내보내기 형식 콘텐츠 정보"를 참고해 주십시오.

DHCP 프로브

Cisco ISE 구축의 DHCP(Dynamic Host Configuration Protocol) 프로브를 사용하면 Cisco ISE 프로파일링 서비스에서 INIT-REBOOT 및 SELECTING 메시지 유형의 새 요청만을 기반으로 엔드포인트를 다시 프로파일링할 수 있습니다. RENEWING 및 REBINDING와 같은 다른 DHCP 메시지 유형도 처리되지만 프로파일링 엔드포인트에는 사용하지 않습니다. DHCP 패킷에서 구문 분석되는 속성은 엔드포인트 속성에 매핑됩니다.

INIT-REBOOT 상태에서 생성되는 **DHCPREQUEST** 메시지

DHCP 클라이언트가 이전에 할당 및 캐시된 컨피그레이션을 확인하는 경우 클라이언트는 서버 식별자(server-ip) 옵션을 채워서는 안 됩니다. 대신, 요청된 IP 주소(requested-ip) 옵션을 이전에 할당된 IP 주소로 채우고 DHCPREQUEST 메시지의 클라이언트 IP 주소(ciaddr) 필드를 0으로 채워야 합니다. 그러면 요청된 IP 주소가 잘못되었거나 클라이언트가 잘못된 네트워크에 있는 경우 DHCP 서버가 DHCPNAK 메시지를 클라이언트로 보냅니다.

SELECTING 상태에서 생성되는 **DHCPREQUEST** 메시지

DHCP 클라이언트는 선택한 DHCP 서버의 IP 주소를 서버 식별자(server-ip) 옵션에 삽입하고, 요청된 IP 주소(requested-ip) 옵션을 클라이언트가 선택한 DHCPOFFER의 IP 주소(yiaddr) 필드 값으로 채우고, "ciaddr" 필드를 0으로 채웁니다.

표 ***90:*** 여러 상태의 ***DHCP*** 클라이언트 메시지

—	**INIT-REBOOT**	**SELECTING**	**RENEWING**	**REBINDING**
broadcast/unicast	broadcast	broadcast	unicast	broadcast
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT

—	INIT-REBOOT	SELECTING	RENEWING	REBINDING
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	zero	zero	IP address	IP address

DHCP 브리징 모드의 Wireless LAN Controller 컨피그레이션

무선 클라이언트에서 Cisco ISE로 모든 DHCP(Dynamic Host Configuration Protocol) 패킷을 전달할 수 있는 DHCP 브리징 모드에서 WLC(Wireless LAN Controller)를 구성하는 것이 좋습니다. WLC 웹 인터페이스 **Controller(**컨트롤러**)** > **Advanced(**고급**)** > **DHCP Master Controller Mode(DHCP** 마스터 컨트롤러 모드**)** > **DHCP Parameters(DHCP** 매개변수**)**에서 사용 가능한 Enable DHCP Proxy(DHCP 프록시 활성화) 확인란의 선택을 취소해야 합니다. 또한 DHCP IP 헬퍼 명령이 Cisco ISE 정책 서비스 노드를 가리키는지도 확인해야 합니다.

DHCP SPAN 프로브

Cisco ISE 노드에서 초기화된 DHCP SPAN(Switched Port Analyzer) 프로브는 네트워크 액세스 디바이스의 특정 인터페이스에서 들어오는 네트워크 트래픽을 수신 대기합니다. DHCP 서버에서 오는 DHCP SPAN 패킷을 Cisco ISE 프로파일러로 전달하도록 네트워크 액세스 디바이스를 구성해야 합니다. 프로파일러는 이러한 DHCP SPAN 패킷을 받고 구문 분석하여 엔드포인트의 속성을 캡처합니다. 이러한 속성은 프로파일링 엔드포인트에 사용할 수 있습니다.

예:

```
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

HTTP 프로브

HTTP 프로브에서는 ID 문자열이 HTTP request-header 필드 사용자 에이전트로 전송됩니다. 이 문자열은 IP 유형의 프로파일링 조건을 생성하고 웹 브라우저 정보를 확인하는 데 사용할 수 있는 속성입니다. 프로파일러는 요청 메시지의 다른 HTTP 속성과 함께 사용자 에이전트 속성의 웹 브라우저 정보를 캡처한 다음 엔드포인트 속성 목록에 추가합니다.

Cisco ISE는 포트 80과 8080 둘 다에서 웹 브라우저로부터의 통신을 수신 대기합니다. Cisco ISE는 사용자 에이전트 속성을 기준으로 하여 엔드포인트를 식별하도록 시스템에 내장되어 있는 여러 기본 프로파일을 제공합니다.

HTTP 프로브는 기본적으로 활성화되어 있습니다. CWA, 핫스팟, BYOD, MDM 및 Posture와 같은 여러 ISE 서비스는 클라이언트 웹 브라우저의 URL 리디렉션을 사용합니다. 리디렉션된 트래픽에는 연결된 엔드포인트의 RADIUS 세션 ID가 포함됩니다. PSN이 이러한 URL 리디렉션 플로우를 종료하면 암호 해독된 HTTPS 데이터를 확인할 수 있습니다. HTTP 프로브가 PSN에서 비활성화된 경우에도 노드는 웹 트래픽에서 브라우저 사용자 에이전트 문자열을 구문 분석하고 연결된 세션 ID를 기반으로 데이터를 엔드포인트에 연결합니다. 이 방법을 통해 브라우저 문자열이 수집되면 데이터 소스가 HTTP 프로브가 아닌 게스트 포털 또는 CP(Client Provisioning)로 나열됩니다.

HTTP SPAN 프로브

Cisco ISE 구축의 HTTP 프로브를 SPAN(Switched Port Analyzer) 프로브와 함께 활성화하는 경우 프로파일러가 지정된 인터페이스에서 HTTP 패킷을 캡처할 수 있습니다. Cisco ISE가 웹 브라우저로부터의 통신을 수신 대기하는 포트 80에서 SPAN 기능을 사용할 수 있습니다.

HTTP SPAN에서는 IP 헤더(L3 헤더)의 IP 주소와 함께 HTTP 요청 헤더 메시지의 HTTP 속성을 수집합니다. L2 헤더의 엔드포인트 MAC 주소를 기준으로 하여 이 IP 주소를 엔드포인트에 연결할 수 있습니다. 이 정보는 운영체제가 각기 다른 컴퓨터와 Apple 디바이스 등의 여러 모바일 및 휴대용 IP 활성화 디바이스를 식별하는 데 유용합니다. Cisco ISE 서버는 게스트 로그인 또는 클라이언트 프로비저닝 다운로드 중에 캡처를 리디렉션하므로, 여러 모바일 및 휴대용 IP 활성화 디바이스를 보다 안정적으로 식별할 수 있습니다. 따라서 프로파일러가 요청 메시지에서 User-Agent 속성 및 기타 HTTP 속성을 수집한 다음 Apple 디바이스 등의 디바이스를 식별할 수 있습니다.

VMware에서 실행되는 Cisco ISE의 HTTP 속성을 수집할 수 없음

ESX 서버(VMware)에서 Cisco ISE를 구축하는 경우 Cisco ISE 프로파일러는 Dynamic Host Configuration Protocol 트래픽은 수집하지만 vSphere 클라이언트의 컨피그레이션 문제로 인해 HTTP 트래픽은 수집하지 않습니다. VMware 설정에서 HTTP 트래픽을 수집하려면 Cisco ISE 프로파일러에 대해 생성하는 가상 스위치의 Promiscuous Mode(무차별 모드)를 Accept(수락)에서 기본값인 Reject(거부)로 변경하여 보안 설정을 구성합니다. DHCP 및 HTTP의 SPAN(Switched Port Analyzer) 프로브가 활성화되어 있으면 Cisco ISE 프로파일러는 DHCP 및 HTTP 트래픽을 모두 수집합니다.

pxGrid 프로브

pxGrid 프로브는 외부 소스에서 엔드포인트 상황을 수신하기 위해 Cisco pxGrid를 활용합니다. Cisco ISE 2.4 이전에는 Cisco ISE가 게시자로만 사용되었으며 세션 ID 및 그룹 정보와 같은 다양한 상황 정보와 컨피그레이션 요소를 외부 가입자와 공유했습니다. Cisco ISE 2.4에 pxGrid 프로브가 도입됨에 따라 다른 솔루션도 게시자로 사용되며 Cisco ISE 정책 서비스 노드가 가입자가 됩니다.

pxGrid 프로브는 서비스 이름 *com.cisco.endpoint.asset*의 엔드포인트 자산 항목 */topic/com.cisco.endpoint.asset*를 사용하는 pxGrid v2 사양을 기반으로 합니다. 다음 표에는 접두사 자산을 갖는 모든 항목 속성이 표시됩니다.

표 ***91:*** 엔드포인트 자산 항목

속성 이름	**Type(**유형**)**	**Description(**설명**)**
자산 **ID**	길게	자산 ID
자산 이름	문자열	자산 이름
자산 **IP** 주소	문자열	IP 주소
자산 **Mac** 주소	문자열	MAC 주소
자산 벤더	문자열	Manufacturer
자산 제품 **ID**	문자열	제품 코드

자산 일련 번호	문자열	일련 번호
자산 디바이스 유형	문자열	디바이스 유형
자산 **SwRevision**	문자열	S/W 개정 번호
assetHwRevision	문자열	H/W 개정 번호
assetProtocol	문자열	프로토콜
assetConnectedLinks	어레이	네트워크 링크 개체의 어레이
assetCustomAttributes	어레이	맞춤형 이름-값 쌍 어레이

디바이스 MAC 주소(assetMacAddress) 및 IP 주소(assetIpAddress)와 같이 네트워크 자산을 추적하는 데 일반적으로 사용되는 속성 외에도 벤더는 고유 한 엔드포인트 정보를 맞춤형 속성(assetCustomAttributes)으로 게시할 수 있습니다. Cisco ISE에서 엔드포인트 사용자 맞춤화 속성을 사용하면 pxGrid를 통해 공유되는 고유한 각 벤더 속성 집합에 대한 스키마 업데이트 없이도 다양한 활용 사례로 항목을 확장할 수 있습니다.

RADIUS 프로브

RADIUS에 대한 인증을 수행하도록 Cisco ISE를 구성할 수 있습니다. 이때 클라이언트-서버 트랜잭션에 사용 가능한 공유 암호를 정의할 수 있습니다. 프로파일러는 RADIUS 서버에서 수신되는 RADIUS 요청 및 응답 메시지를 사용하여 RADIUS 속성을 수집할 수 있으며, 이러한 속성을 엔드포인트 프로파일링에 사용할 수 있습니다.

Cisco ISE는 RADIUS 서버로 작동할 수 있으며 다른 RADIUS 서버에 대한 RADIUS 프록시 클라이언트로도 작동할 수 있습니다. Cisco ISE는 프록시 클라이언트로 작동할 때 외부 RADIUS 서버를 사용하여 RADIUS 요청 및 응답 메시지를 처리합니다.

RADIUS 프로브는 디바이스 센서에 의해 RADIUS 계정 관리 패킷에서 전송된 속성도 수집합니다. 자세한 내용은 IOS 센서 내장 스위치에서의 속성 수집, 710 페이지 및 IOS 센서 지원 네트워크 액세스 디바이스의 컨피그레이션 체크리스트, 711 페이지를 참조하십시오.

RADIUS 프로브는 기본적으로 실행되며, ISE가 상황 가시성 서비스에 사용하기 위해 엔드포인트 인증 및 권한 부여 세부정보를 추적할 수 있도록 프로파일링 서비스가 구성되지 않은 시스템에서도 마찬가지로 실행됩니다. RADIUS 프로브 및 프로파일링 서비스는 제거 작업을 위해 등록된 엔드포인트의 생성 및 업데이트 시간을 추적하는 데에도 사용됩니다.

표 ***92: RADIUS*** 프로브를 사용하여 수집되는 일반적인 속성

User-Name	**Calling-Station-Id**	**Called-Station-Id**	**Framed-IP-Address**
NAS-IP-Address	NAS-Port-Type	NAS-Port-Id	NAS-Identifier
디바이스 유형(NAD)	위치(NAD)	인증 정책	권한 부여 정책

참고 계정 관리 중지가 수신될 경우 Cisco ISE에서 원래 IP 주소로 프로파일링된 엔드포인트를 다시 프로파일링합니다. 따라서 IP 주소로 프로파일링된 엔드포인트에 대한 사용자 맞춤화 프로파일이 있는 경우 이러한 프로파일의 전체 확실성 요인을 충족하는 유일한 방법은 해당 IP 주소에 일치시키는 것입니다.

네트워크 스캔(NMAP) 프로브

Cisco ISE를 사용하면 NMAP 보안 스캐너를 사용하여 서브넷에서 디바이스를 탐지할 수 있습니다. 프로파일링 서비스를 실행할 수 있는 정책 서비스 노드에서 NMAP 프로브를 활성화합니다. 엔드포인트 프로파일링 정책에서 해당 프로브의 결과를 사용합니다.

각 NMAP 수동 서브넷 스캔에는 고유한 숫자 ID가 있으며, 이는 엔드포인트 소스 정보를 해당 스캔 ID로 업데이트하는 데 사용됩니다. 엔드포인트가 탐지되면 네트워크 스캔 프로브로 검색되었음을 나타내도록 엔드포인트 소스 정보도 업데이트됩니다.

NMAP 수동 서브넷 스캔은 프린터와 같이 정적 IP 주소가 할당되어 있는 디바이스를 탐지하는 데 유용합니다. 정적 IP 주소는 Cisco ISE 네트워크에 지속적으로 연결되어 있는 디바이스에 할당되므로 이러한 디바이스는 다른 프로브에 의해 검색되지 않습니다.

NMAP 스캔 제한

서브넷을 스캔할 때는 리소스를 매우 많이 사용합니다. 서브넷 스캔은 오랫동안 진행되는 프로세스로, 시간은 서브넷의 크기와 밀도에 따라 달라집니다. 활성 스캔의 수는 항상 한 개 스캔으로 제한됩니다. 즉, 서브넷은 한 번에 하나씩만 스캔할 수 있습니다. 서브넷 스캔이 진행 중인 동안 언제든지 서브넷 스캔을 취소할 수 있습니다. **Click(**클릭**)**을 사용하여 최신 스캔 결과 링크를 표시하면 **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Manual Scans(**수동 스캔**)** > **Manual NMAP Scan Results(**수동 **NMAP** 스캔 결과**)**에 저장되어 있는 최신 네트워크 스캔 결과를 확인할 수 있습니다.

수동 **NMAP** 스캔

다음 NMAP 명령은 서브넷을 스캔하여 출력을 nmapSubnet.log로 보냅니다.

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

표 ***93:*** 수동 서브넷 스캔용 ***NMAP*** 명령

-O	OS 탐지를 활성화합니다.
-sU	UDP를 스캔합니다.
-p <포트 범위>	지정된 포트만 스캔합니다. 예를 들면 U:161, 162와 같이 입력합니다.
oN	일반 출력을 생성합니다.
oX	XML 출력을 생성합니다.

NMAP 수동 서브넷 스캔용 SNMP 읽기 전용 커뮤니티 문자열

NMAP 수동 서브넷 스캔 결과 엔드포인트에서 UDP 포트 161이 열려 있어 속성을 더 수집할 수 있는 것으로 검색될 때마다 해당 스캔에서 SNMP 쿼리가 추가로 수행됩니다. NMAP 수동 서브넷 스캔을 수행하는 동안 네트워크 스캔 프로브는 디바이스에서 SNMP 포트 161이 열려 있는지를 탐지합니다. 포트가 열려 있으면 SNMP 버전 2c를 통해 기본 커뮤니티 문자열(public)을 사용하여 SNMP 쿼리가 트리거됩니다.

디바이스가 SNMP를 지원하며 기본 읽기 전용 커뮤니티 문자열이 public으로 설정되어 있으면 MIB 값 "ifPhysAddress"에서 디바이스의 MAC 주소를 가져올 수 있습니다.

또한 **Profiler Configuration(**프로파일러 컨피그레이션**)** 창에서 쉼표로 구분된 추가 SNMP 읽기 전용 커뮤니티 문자열을 NMAP 수동 네트워크 스캔용으로 구성할 수도 있습니다. SNMP 버전 1 및 2c를 통한 SNMP MIB walk용으로 새 읽기 전용 커뮤니티 문자열을 지정할 수도 있습니다. SNMP 읽기 전용 커뮤니티 문자열 구성에 대한 자세한 내용은 CoA, SNMP RO 커뮤니티 및 엔드포인트 속성 필터 설정, 704 페이지를 참조하십시오.

수동 NMAP 스캔 결과

최신 네트워크 스캔 결과는 Work Centers (작업 센터)> Profiler (프로파일러)> Manual Scans (수동 스캔)> Manual NMAP Scan Results (수동 NMAP 스캔 결과)에 저장됩니다. 수동 NMAP 스캔 결과 페이지에는 서브넷에서 수행하는 수동 네트워크 스캔의 결과로 탐지된 최신 엔드포인트만 표시되며, 이러한 엔드포인트에 연결된 엔드포인트 프로파일, 해당 MAC 주소 및 정적 할당 상태가 함께 표시됩니다. 필요한 경우 이 페이지에서 보다 적절한 분류를 위해 엔드포인트 서브넷에서 탐지된 포인트를 편집할 수 있습니다.

Cisco ISE에서는 프로파일링 서비스를 실행하도록 활성화된 정책 서비스 노드에서 수동 네트워크 스캔을 수행할 수 있습니다. 정책 서비스 노드에서 수동 네트워크 스캔을 실행하려면 구축의 기본 관리 ISE 노드 사용자 인터페이스에서 정책 서비스 노드를 선택해야 합니다. 서브넷에서 수동 네트워크 스캔을 수행하는 동안 네트워크 스캔 프로브는 지정한 서브넷의 엔드포인트와 해당 운영체제를 탐지하고 UDP 포트 161 및 162에서 SNMP 서비스를 확인합니다.

아래에는 수동 NMAP 스캔 결과와 관련된 추가 정보가 나와 있습니다.

- 알 수 없는 엔드포인트를 탐지하려면 NMAP에서 NMAP 또는 지원되는 SNMP 스캔을 통해 IP/MAC 바인딩을 학습할 수 있어야 합니다.
- ISE는 Radius 인증 또는 DHCP 프로파일링을 통해 알려진 엔드포인트의 IP/MAC 바인딩을 학습합니다.
- IP/MAC 바인딩은 구축의 PSN 노드간에 복제되지 않습니다. 따라서 로컬 데이터베이스에 IP / MAC 바인딩이 있는 PSN에서 수동 스캔을 트리거해야 합니다(예: MAC 주소가 마지막으로 인증 된 PSN).
- NMAP 스캔 결과에는 NMAP가 이전에 수동으로 또는 자동으로 스캔한 엔드포인트와 관련된 정보가 표시되지 않습니다.

DNS 프로브

Cisco ISE 구축에서 DNS(Domain Name Service) 프로브를 사용하면 프로파일러가 엔드포인트를 조회하고 FQDN(Fully Qualified Domain Name)을 가져올 수 있습니다. Cisco ISE 지원 네트워크에서 엔드포인트가 탐지되고 나면 엔드포인트 속성 목록이 NetFlow, DHCP, DHCP SPAN, HTTP, RADIUS 또는 SNMP 프로브에서 수집됩니다.

독립형 환경 또는 분산형 환경에서 처음으로 Cisco ISE를 구축하는 경우 설치 유틸리티를 실행하여 Cisco ISE 어플라이언스를 구성하도록 메시지가 표시됩니다. 설치 유틸리티를 실행하는 경우 DNS(Domain Name System) 도메인 및 기본 네임서버(기본 DNS 서버)를 구성합니다. 설치 중에 하나 이상의 네임서버를 구성할 수 있습니다. 나중에 CLI 명령을 사용하여 Cisco ISE를 구축한 후에는 DNS 네임서버를 변경하거나 추가할 수 있습니다.

DNS 조회 FQDN

DNS 조회를 수행하려면 DHCP, DHCP SPAN, HTTP, RADIUS 또는 SNMP 프로브 중 하나를 DNS 프로브와 함께 시작해야 합니다. 이렇게 하면 프로파일러의 DNS 프로브가 Cisco ISE 구축에 정의하는 지정된 이름 서버에 대한 역방향 DNS 조회(FQDN 조회)를 수행할 수 있습니다. 새 속성은 엔드포인트 프로파일링 정책 평가에 사용할 수 있는 엔드포인트의 속성 목록에 추가됩니다. FQDN은 시스템 IP 사전에 있는 새 속성입니다. 엔드포인트 프로파일링 조건을 생성하여 프로파일링을 위해 FQDN 속성 및 해당 값을 검증할 수 있습니다. 다음은 DNS 조회에 필요한 특정 엔드포인트 속성 및 이러한 속성을 수집하는 프로브입니다.

- dhcp-requested-address 속성 - DHCP 및 DHCP SPAN 프로브에서 수집되는 속성
- SourceIP 속성 - HTTP 프로브에서 수집되는 속성
- Framed-IP-Address 속성 - RADIUS 프로브에서 수집되는 속성
- cdpCacheAddress 속성 - SNMP 프로브에서 수집되는 속성

WLC 웹 인터페이스에서 호출 스테이션 ID 유형 구성

WLC 웹 인터페이스를 사용하여 호출 스테이션 ID 유형 정보를 구성할 수 있습니다. WLC 웹 인터페이스의 Security(보안) 탭으로 이동하여 RADIUS 인증 서버 페이지에서 호출 스테이션 ID를 구성할 수 있습니다. WLC 사용자 인터페이스에서 MAC Delimiter(MAC 구분 기호) 필드는 기본적으로 콜론으로 설정됩니다.

WLC 웹 인터페이스에서 이 정보를 구성하는 방법에 대한 자세한 내용은 Cisco Wireless LAN Controller 컨피그레이션 설명서(릴리스 7.2)에서 6장 "보안 솔루션 구성"을 참고하십시오.

config radius callStationIdType 명령을 사용하여 WLC CLI에서 이 정보를 구성하는 방법에 대한 자세한 내용은 Cisco Wireless LAN Controller 명령 참조 설명서(릴리스 7.2)에서 2장 "컨트롤러 명령"을 참고하십시오.

단계 **1** Wireless LAN Controller 사용자 인터페이스에 로그인합니다.

단계 **2** **Security(**보안**)**를 클릭합니다.

단계 **3** **AAA**를 확장하고 **RADIUS** > **Authentication(**인증**)**을 선택합니다.

단계 **4** 호출 스테이션 ID 유형 드롭다운 목록에서 **System MAC Address(**시스템 **MAC** 주소**)**를 선택합니다.
단계 **5** MAC 구분 기호 드롭다운 목록에서 **Colon(**콜론**)**을 선택합니다.

SNMP 쿼리 프로브

노드 편집 페이지에서 SNMP 쿼리 프로브를 구성해야 할 뿐 아니라 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** 위치에서 다른 단순 관리 프로토콜 설정도 구성해야 합니다.

네트워크 디바이스 목록 페이지에서 새 NAD(Network Access Devices)의 SNMP 설정을 구성할 수 있습니다. 네트워크 액세스 디바이스의 SNMP 설정 또는 SNMP 쿼리 프로브에서 지정하는 폴링 간격에 따라 일정한 간격으로 NAD를 쿼리합니다.

다음 컨피그레이션에 따라 특정 NAD에 대해 SNMP 쿼리를 켜고 끌 수 있습니다.

- 링크 작동 및 새 MAC 알림에서 SNMP 쿼리 켜기/끄기
- 링크 작동 및 새 MAC 알림에서 Cisco Discovery Protocol 정보에 대한 SNMP 쿼리 켜기/끄기
- 각 스위치에 대한 SNMP 쿼리 타이머(기본적으로 1시간마다)

iDevice 및 SNMP를 지원하지 않는 기타 모바일 디바이스의 경우에는 ARP 표을 통해 MAC 주소를 검색할 수 있습니다. SNMP 쿼리 프로브를 사용하여 네트워크 액세스 디바이스에서 이 표을 쿼리할 수 있습니다.

SNMP 쿼리를 사용한 Cisco Discovery Protocol 지원

네트워크 디바이스에서 SNMP 설정을 구성하는 경우 네트워크 디바이스의 모든 포트에서 Cisco Discovery Protocol이 활성화(기본값)되어 있는지 확인해야 합니다. 네트워크 디바이스의 포트에서 Cisco Discovery Protocol을 비활성화하면 연결된 일부 엔드포인트의 Cisco Discovery Protocol 정보를 놓치게 되므로 올바르게 프로파일링하지 못할 수 있습니다. 네트워크 디바이스에 대해 cdp run 명령을 사용하여 Cisco Discovery Protocol을 전역적으로 활성화하고, 네트워크 액세스 디바이스의 인터페이스에 대해 cdp enable 명령을 사용하여 Cisco Discovery Protocol을 활성화할 수 있습니다. 네트워크 디바이스 및 인터페이스에서 Cisco Discovery Protocol을 비활성화하려면 명령 시작 부분에 no keyword를 사용해 주십시오.

SNMP 쿼리를 사용한 Link Layer Discovery Protocol 지원

Cisco ISE 프로파일러는 SNMP 쿼리를 사용하여 LLDP 속성을 수집합니다. RADIUS 프로브를 사용하여 네트워크 디바이스에 내장된 Cisco IOS 센서에서 LLDP 속성을 수집할 수도 있습니다. 아래 표에서 LLDP 전역 구성을 구성하는 데 사용할 수 있는 기본 LLDP 구성 설정과, 네트워크 액세스 디바이스의 LLDP 인터페이스 구성 명령을 확인해 주십시오.

표 ***94:*** 기본 ***LLDP*** 컨피그레이션

속성	설정
LLDP global state	비활성화

속성	설정
LLDP holdtime(폐기 전)	120초
LLDP timer(패킷 업데이트 빈도)	30초
LLDP reinitialization delay	2초
LLDP tlv-select	활성화됨(모든 TLV를 보내고 받을 수 있음)
LLDP interface state	활성화됨
LLDP receive	활성화됨
LLDP transmit	활성화됨
LLDP med-tlv-select	활성화됨(모든 LLDP-MED TLV를 보낼 수 있음)

단일 문자로 표시되는 **CDP** 및 **LLDP** 기능 코드

엔드포인트의 속성 목록에는 lldpCacheCapabilities 및 lldpCapabilitiesMapSupported 속성에 대한 단일 문자 값이 표시됩니다. 이 값은 CDP 및 LLDP를 실행하는 네트워크 액세스 디바이스에 대해 표시되는 기능 코드입니다.

예 **1**

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

예 **2**

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

예 **3**

```
Switch#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#

Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#
```

SNMP 트랩 프로브

SNMP 트랩은 MAC 알림, linkup, linkdown 및 알림을 지원하는 특정 네트워크 액세스 디바이스에서 정보를 수신합니다. SNMP 트랩 프로브는 포트가 작동하거나 작동이 중지될 때와 엔드포인트가 네트워크에 연결되거나 네트워크에서 연결이 끊길 때 특정 네트워크 액세스 디바이스에서 정보를 수신합니다.

SNMP 트랩이 완전히 작동하고 엔드포인트를 생성하도록 하려면 트랩 수신 시 SNMP 쿼리 프로브가 네트워크 액세스 디바이스의 특정 포트에서 폴링 이벤트를 트리거하도록 SNMP 쿼리를 활성화해야 합니다. 이 기능이 완전히 작동하도록 하려면 네트워크 액세스 디바이스 및 SNMP 트랩을 구성해야 합니다.

참고 Cisco ISE는 WLC(Wireless LAN Controller) 및 AP(Access Points)에서 수신된 SNMP 트랩을 지원하지 않습니다.

Active Directory 프로브

AD(Active Directory) 프로브:

- Windows 엔드포인트의 OS 정보의 신뢰도를 개선합니다. Microsoft AD는 버전 및 서비스 팩 레벨을 비롯하여 AD에 가입된 컴퓨터의 세부 OS 정보를 추적합니다. AD 프로브는 AD Runtime 커넥터를 사용하여 이 정보를 직접 검색하므로 신뢰도가 높은 클라이언트 OS 정보 소스를 제공합니다.
- 기업 자산과 그 외의 자산을 쉽게 구분할 수 있습니다. AD 프로브에서 사용할 수 있는 기본적이지만 중요한 속성은 AD에 엔드포인트가 있는지 여부입니다. 이 정보는 AD에 포함된 엔드포인트를 관리되는 디바이스 또는 기업 자산으로 분류하는 데 사용될 수 있습니다.

Administration(관리**)** > **System(**시스템**)** > **Deployment(**구축**)** > **Profiling Configuration(**프로파일링 컨피그레이션**)**에서 AD 프로브를 활성화할 수 있습니다. 이 프로브가 활성화되면 Cisco ISE는 호스트 이름을 수신하는 즉시 새 엔드포인트에 대한 AD 속성을 가져옵니다. 호스트 이름은 일반적으로 DHCP 또는 DNS 프로브에서 학습됩니다. 호스트 이름이 정상적으로 검색되면 ISE는 다시 스캔 타이머가 만료될 때까지 AD에서 같은 엔드포인트를 다시 쿼리하지 않습니다. 이는 속성 쿼리를 위한 AD의 로드를 제한하기 위한 것입니다. **Days Before Rescan(**다시 스캔할 때까지의 기간**(**일**))** 필드 (**Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** > **Profiling Configuration(**프로파일링 컨피그레이션**)** > **Active Directory**)에서 다시 스캔 타이머를 구성할 수 있습니다. 엔드포인트에서 추가 프로파일링 활동이 수행되는 경우 AD를 다시 쿼리합니다.

다음 AD 프로브 속성은 ACTIVEDIRECTORY 조건을 사용하여 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Profiling(**프로파일링**)**에서 일치 여부를 확인할 수 있습니다. AD 프로브를 사용하여 수집한 AD 속성은 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** 창의 엔드포인트 세부정보에 "AD" 접두사가 붙은 채로 표시됩니다.

- AD-Host-Exists
- AD-Join-Point

- AD-Operating-System
- AD-OS-Version
- AD-Service-Pack

Cisco ISE 노드별 프로브 구성

구축에서 정책 서비스 페르소나 역할을 하는 Cisco ISE 노드별로 Profiling Configuration(프로파일링 컨피그레이션) 탭에서 하나 이상의 프로브를 구성할 수 있습니다. 여기에는 다음과 같은 노드가 포함될 수 있습니다.

- 독립형 노드: 기본적으로 관리, 모니터링 및 정책 서비스 페르소나 역할을 모두 수행하는 단일 노드에서 Cisco ISE를 구축한 경우입니다.
- 여러 노드: 구축에서 정책 서비스 페르소나 역할을 하는 노드를 둘 이상 등록한 경우입니다.

참고 모든 프로브가 기본적으로 활성화되어 있지는 않습니다. 일부 프로브는 확인 표시로 명시적으로 활성화되지 않은 경우에도 부분적으로 활성화됩니다. 프로파일링 컨피그레이션은 현재 각 PSN에 고유합니다. 구축의 각 PSN은 동일한 프로파일러 컨피그레이션 설정으로 구성하는 것이 좋습니다.

시작하기 전에

Cisco ISE 노드별 프로브는 관리 노드에서만 구성할 수 있습니다. 분산형 구축의 보조 관리 노드에서는 이 구성 기능이 제공되지 않습니다.

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

단계 **2** 정책 서비스 페르소나 역할을 하는 Cisco ISE 노드를 선택합니다.

단계 **3** 구축 노드 페이지에서 **Edit(**편집**)**를 클릭합니다.

단계 **4** **General Settings(**일반 설정**)** 탭에서 **Policy Service(**정책 서비스**)** 확인란을 선택합니다. Policy Service(정책 서비스) 확인란 선택을 취소하면 세션 서비스와 프로파일링 서비스 확인란이 모두 비활성화됩니다.

단계 **5** **Enable Profiling Services(**프로파일링 서비스 활성화**)** 확인란을 선택합니다.

단계 **6** **Profiling Configuration(**프로파일링 컨피그레이션**)** 탭을 클릭합니다.

단계 **7** 각 프로브에 대한 값을 구성합니다.

단계 **8** 프로브 컨피그레이션을 저장하려면 **Save(**저장**)**를 클릭합니다.

CoA, SNMP RO 커뮤니티 및 엔드포인트 속성 필터 설정

Cisco ISE에서는 프로파일러 컨피그레이션 페이지에서 CoA(Change of Authorization)를 실행하는 전역 컨피그레이션을 사용할 수 있습니다. 그러면 프로파일링 서비스가 이미 인증된 엔드포인트를 보다 자세하게 제어할 수 있습니다.

또한 프로파일러 컨피그레이션 페이지에서 쉼표로 구분된 추가 SNMP 읽기 전용 커뮤니티 문자열을 NMAP 수동 네트워크 스캔용으로 구성할 수도 있습니다. SNMP RO 커뮤니티 문자열은 Current custom SNMP community strings(현재 맞춤 SNMP 커뮤니티 문자열) 필드에 표시되는 것과 같은 순서로 사용됩니다.

프로파일러 컨피그레이션 페이지에서 엔드포인트 속성 필터링을 구성할 수도 있습니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Profiling(**프로파일링**)**을 선택합니다.

단계 **2** 다음 설정 중 하나를 선택하여 CoA 유형을 구성합니다.

- **No CoA(CoA** 없음**)**(기본값) - 이 옵션을 사용하여 CoA 전역 컨피그레이션을 비활성화할 수 있습니다. 이 설정은 엔드포인트 프로파일링 정책별로 구성된 CoA를 재정의합니다. 목표가 가시성에 국한되어 있다면 기본값인 **No CoA(CoA** 없음**)**를 그대로 사용하십시오.
- **Port Bounce(**포트 반송**)** - 세션이 하나뿐인 스위치 포트가 있는 경우 이 옵션을 사용할 수 있습니다. 세션이 여러 개인 포트가 있는 경우에는 Reauth(재인증) 옵션을 사용합니다. 프로파일 변경 사항에 따라 액세스 정책을 즉시 업데이트하는 것이 목표라면 **Port Bounce(**포트 바운스**)** 옵션을 선택합니다. 그러면 클라이언트리스 엔드포인트가 다시 권한 부여되고 필요한 경우 IP 주소가 새로 고쳐집니다.
- **Reauth(**재인증**)** - 이 옵션을 사용하면 이미 인증된 엔드포인트를 프로파일링할 때 재인증을 시행할 수 있습니다. 현재 세션의 재인증 후에 VLAN 또는 주소가 변경되지 않을 경우 **Reauth(**재인증**)** 옵션을 선택합니다.

  참고 단일 포트에 여러 활성 세션이 있는 경우에는 **Port Bounce(**포트 반송**)** 옵션을 사용하여 CoA를 구성했더라도 프로파일링 서비스는 **Reauth(**재인증**)** 옵션을 사용하여 CoA를 실행합니다. 이 기능을 사용하면 **Port Bounce(**포트 반송**)** 옵션 사용 시 발생할 수 있는 상황인 다른 세션의 연결 끊김을 방지할 수 있습니다.

단계 **3** **Change Custom SNMP Community Strings(**맞춤 **SNMP** 커뮤니티 문자열 변경**)** 필드에 SNMP 수동 네트워크 스캔용 새 SNMP 커뮤니티 문자열을 쉼표로 구분하여 입력하고 **Confirm Custom SNMP Community Strings(**맞춤 **SNMP** 커뮤니티 문자열 확인**)** 필드에 확인을 위해 문자열을 다시 입력합니다.

기본 커뮤니티 문자열은 공개됩니다. 이를 확인하려면 **Current Custom SNMP Community Strings(**현재 맞춤 **SNMP** 커뮤니티 문자열**)** 섹션에서 **Show(**표시**)**를 클릭합니다.

단계 **4** **Endpoint Attribute Filter(**엔드포인트 속성 필터**)** 확인란을 선택하여 엔드포인트 속성 필터링을 활성화합니다.

EndPoint Attribute Filter(엔드포인트 속성 필터**)**를 활성화하면 Cisco ISE 프로파일러는 중요한 속성만 유지하고 다른 모든 속성은 버리게 됩니다. 자세한 내용은 엔드포인트 속성 필터링을 위한 전역 설정, 708 페이지 및 ISE 데이터베이스 지속성 및 성능의 속성 필터, 707 페이지 섹션을 참조하십시오. 모범 사례로서 프로덕션 구축에서 **Endpoint Attribute Filter(**엔드포인트 속성 필터**)**를 활성화하는 것이 좋습니다.

단계 **5** Cisco ISE가 ISE에서 엔드포인트 온보딩을 분류하기 위해 이 데이터가 필요한 pxGrid 가입자에게 엔드포인트 프로브 데이터를 게시하도록 하려면 **Enable Probe Data Publisher(**프로브 데이터 게시자 활성화**)** 확인란을 선택합니다. pxGrid 가입자는 초기 구축 단계에서 대량 다운로드를 사용하여 Cisco ISE에서 엔드포인트 기록을 가져올 수 있습니다. Cisco ISE는 PAN에서 업데이트될 때마다 pxGrid 가입자에게 엔드포인트 기록을 전송합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

이 옵션을 활성화할 경우 pxGrid 페르소나가 구축에서 활성화되어 있는지 확인합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

인증된 엔드포인트에 대한 **Change of Authorization**의 전역 컨피그레이션

전역 컨피그레이션 옵션을 사용하여 기본값인 No CoA(CoA 없음) 옵션을 통해 CoA(Change of Authorization)를 비활성화하거나, 포트 반송 및 재인증 옵션을 통해 CoA를 활성화할 수 있습니다. Cisco ISE에서 포트 반송을 구성한 경우에도 프로파일링 서비스는 "CoA 면제" 섹션에서 설명하는 기타 CoA를 계속 실행할 수 있습니다.

선택한 전역 컨피그레이션은 더 구체적인 설정이 없는 경우에만 기본 CoA 동작을 나타냅니다. 엔드포인트 프로파일링 정책별 CoA(Change of Authorization) 컨피그레이션, 741 페이지의 내용을 참조하십시오.

RADIUS 프로브 또는 모니터링 페르소나 REST API를 사용하여 엔드포인트를 인증할 수 있습니다. RADIUS 프로브를 활성화할 수 있으며, 그러면 성능이 개선됩니다. CoA를 활성화한 경우 성능 개선을 위해 Cisco ISE 애플리케이션에서 CoA 컨피그레이션과 함께 RADIUS 프로브를 활성화하는 것이 좋습니다. 그러면 프로파일링 서비스가 수집된 RADIUS 속성을 사용하여 엔드포인트에 대해 적절한 CoA를 실행할 수 있습니다.

Cisco ISE 애플리케이션에서 RADIUS 프로브를 비활성화한 경우에는 모니터링 페르소나 REST API를 사용하여 CoA를 실행할 수 있습니다. 이 경우 프로파일링 서비스가 보다 광범위한 엔드포인트를 지원할 수 있습니다. 분산형 구축에서는 모니터링 페르소나 REST API를 사용하여 CoA를 실행하려면 네트워크에 모니터링 페르소나로 지정된 Cisco ISE 노드가 하나 이상 있어야 합니다.

Cisco ISE는 분산형 구축 내 REST 쿼리의 기본 대상으로 기본 또는 보조 모니터링 노드를 임의 지정합니다. 기본 및 보조 모니터링 노드의 세션 디렉토리 정보는 동일하기 때문입니다.

Change of Authorization 실행을 위한 활용 사례

프로파일링 서비스는 다음과 같은 경우 Change of Authorization을 실행합니다.

- 엔드포인트가 삭제됨: 엔드포인트 페이지에서 엔드포인트가 삭제되었으며 네트워크에서 엔드포인트가 제거되었거나 연결이 끊긴 경우입니다.
- 예외 작업이 구성됨: 프로파일당 예외 작업을 구성하여 해당 엔드포인트에서 비정상적이거나 예기치 않은 이벤트가 발생하는 경우입니다. 이 경우 프로파일링 서비스는 CoA를 실행하여 해당하는 정적 프로파일로 엔드포인트를 이동합니다.
- 엔드포인트를 처음으로 프로파일링함: 정적으로 할당되어 있지 않은 엔드포인트를 처음으로 프로파일링하면 프로파일이 알 수 없는 프로파일에서 알려진 프로파일로 변경됩니다.

- 엔드포인트 ID 그룹이 변경됨: 권한 부여 정책에서 사용되는 엔드포인트 ID 그룹에서 엔드포인트를 추가하거나 제거하는 경우입니다.

  이 경우 프로파일링 서비스는 엔드포인트 ID 그룹이 변경될 때 CoA를 실행하며, 다음에 대해 권한 부여 정책에서 엔드포인트 ID 그룹이 사용됩니다.

  - 엔드포인트를 동적으로 프로파일링하면 해당 엔드포인트에 대해 엔드포인트 ID 그룹이 변경됩니다.
  - 동적 엔드포인트에 대해 정적 할당 플래그가 true로 설정되어 있으면 엔드포인트 ID 그룹이 변경됩니다.

- 엔드포인트 프로파일링 정책이 변경되었으며 권한 부여 정책에서 해당 정책이 사용됨: 엔드포인트 프로파일링 정책을 변경했는데 권한 부여 정책에서 사용되는 논리적 프로파일에 해당 정책이 포함되어 있는 경우입니다. 프로파일링 정책이 일치하거나, 엔드포인트가 논리적 프로파일에 연결된 엔드포인트 프로파일링 정책에 정적으로 할당되어 있으면 엔드포인트 프로파일링 정책이 변경될 수 있습니다. 두 가지 경우 모두에서 프로파일링 서비스는 엔드포인트 프로파일링 정책이 권한 부여 정책에서 사용될 때만 CoA를 실행합니다.

CoA(Change of Authorization) 발급 예외

엔드포인트 ID 그룹을 변경할 때 정적 할당이 이미 true이면 프로파일링 서비스는 CoA를 실행하지 않습니다.

Cisco ISE가 CoA를 실행하지 않는 이유는 다음과 같습니다.

- 엔드포인트의 네트워크 연결이 끊김 - 네트워크에서 연결이 끊긴 엔드포인트가 검색되는 경우입니다.
- 인증된 유선 EAP(Extensible Authentication Protocol) 가능 엔드포인트 - 인증된 유선 EAP 가능 엔드포인트가 검색되는 경우입니다.
- 포트당 활성 세션이 여러 개임 - 단일 포트의 활성 세션이 여러 개인 경우에는 Port Bounce(포트 바운스) 옵션을 사용하여 CoA를 구성했더라도 프로파일링 서비스는 Reauth 옵션을 사용하여 CoA를 실행합니다.
- 무선 엔드포인트 탐지 시 연결 끊김 패킷 CoA(세션 종료) - 무선 엔드포인트가 검색되면 포트 반송 CoA가 아닌 연결 끊김 패킷 CoA(세션 종료)가 실행됩니다. 이처럼 CoA가 변경되므로 WLC(Wireless LAN Controller) CoA가 지원된다는 이점이 있습니다.
- 프로파일러 CoA는 Authorization Profile(권한 부여 프로파일)에서 구성된 논리적 프로파일에 대해 **Suppress Profiler CoA for endpoints in Logical Profile(**논리적 프로파일에서 엔드포인트에 대해 프로파일러 **CoA** 표시 안 함**)** 옵션을 사용하는 경우 표시되지 않습니다. 프로파일러 CoA는 기본적으로 다른 모든 엔드포인트에 대해 트리거됩니다.
- 전역 CoA 없음 설정이 정책 CoA를 재정의함 - 전역 CoA 없음은 엔드포인트 프로파일링 정책의 모든 컨피그레이션 설정을 재정의합니다. 엔드포인트 프로파일링 정책별로 구성된 CoA에 관계없이 Cisco ISE에서는 CoA가 실행되지 않기 때문입니다.

참고 이 경우 CoA 없음 및 Reauth CoA 컨피그레이션은 영향을 받지 않으며 프로파일러 서비스는 유선 엔드포인트와 무선 엔드포인트에 대해 동일한 CoA 컨피그레이션을 적용합니다.

각 **CoA** 컨피그레이션 유형에 맞게 발급되는 **CoA(Change of Authorization)**

표 ***95:*** 각 ***CoA*** 컨피그레이션 유형에 맞게 발급되는 ***CoA(Change of Authorization)***

시나리오	**No CoA(CoA** 없음**)** 컨피그레이션	**Port Bounce(**포트 바운스**)** 컨피그레이션	**Reauth(**재인증**)** 컨피그레이션	추가 정보
Cisco ISE의 전역 CoA 컨피그레이션(일반 컨피그레이션)	CoA 없음	포트 바운스	Reauthentication(재인증)	—
네트워크에서 엔드포인트 연결이 끊어짐	No CoA(CoA 없음)	No CoA(CoA 없음)	No CoA(CoA 없음)	CoA(Change of Authorization)는 RADIUS 속성 Acct-Status -Type 값 Stop으로 확인됩니다.
동일한 스위치 포트에 여러 활성 세션이 있는 무선 엔드포인트	No CoA(CoA 없음)	Reauthentication(재인증)	Reauthentication(재인증)	재인증으로 다른 세션의 연결이 끊어지지 않도록 합니다.
무선 엔드포인트	No CoA(CoA 없음)	연결 끊김 패킷 CoA(세션 종료)	Reauthentication(재인증)	Wireless LAN Controller 지원
불완전 CoA 데이터	No CoA(CoA 없음)	No CoA(CoA 없음)	No CoA(CoA 없음)	RADIUS 속성 누락으로 인해

ISE 데이터베이스 지속성 및 성능의 속성 필터

Cisco ISE는 성능 저하 문제를 해결하는 NetFlow 프로브를 제외한 Dynamic Host Configuration Protocol(DHCP 헬퍼와 DHCP SPAN 모두), HTTP, RADIUS 및 Simple Network Management Protocol 프로브용 필터를 구현합니다. 각 프로브 필터는 엔드포인트 프로파일링과 무관한 임시적 속성 목록을 포함하며 프로브에서 수집된 속성에서 그러한 속성을 제거합니다.

isebootstrap 로그(isebootstrap-yyyymmdd-xxxxxx.log)는 사전 생성 및 사전에서의 속성 필터링을 처리하는 메시지를 포함합니다. 또한 엔드포인트에서 필터링 단계를 진행하여 필터링이 발생했음을 나타내는 경우 디버깅 메시지를 기록하도록 구성할 수 있습니다.

Cisco ISE 프로파일러는 다음과 같은 엔드포인트 속성 필터를 호출합니다.

- DHCP 헬퍼와 DHCP SPAN 모두에 사용되는 DHCP 필터는 필요한 속성이 아니어서 DHCP 패킷을 구문 분석한 후 제거되는 모든 속성을 포함합니다. 필터링된 속성은 엔드포인트의 엔드포인트 캐시에 있는 기존 속성과 병합됩니다.
- HTTP 필터는 필터링 후에도 속성 집합에 커다란 변화가 없는 HTTP 패킷에서 속성을 필터링하는 데 사용됩니다.
- RADIUS 필터는 시스템 로그 구문 분석이 완료되고 엔드포인트 속성이 프로파일링 용도로 엔드포인트 캐시에 병합된 경우에 사용됩니다.
- SNMP 쿼리용 SNMP 필터는 모두 SNMP-Query 프로브에 사용되는 별도의 CDP 및 LLDP 필터를 포함합니다.

엔드포인트 속성 필터링을 위한 전역 설정

수집 지점에서 자주 변경되지 않는 엔드포인트 속성 수를 줄여 지속성 이벤트 및 복제 이벤트 수를 줄일 수 있습니다. **EndPoint Attribute Filter(**엔드포인트 속성 필터**)**를 활성화하면 Cisco ISE 프로파일러는 중요한 속성만 유지하고 다른 모든 속성은 버리게 됩니다. 중요한 속성이란 Cisco ISE 시스템에 사용되는 속성 또는 특히 엔드포인트 프로파일링 정책 또는 규칙에 사용되는 속성을 말합니다.

Endpoint Attribute Filter(엔드포인트 속성 필터**)**를 활성화하려면 CoA, SNMP RO 커뮤니티 및 엔드포인트 속성 필터 설정, 704 페이지 섹션을 참고하십시오.

허용 목록은 엔드포인트 프로파일링을 위한 사용자 맞춤화 엔드포인트 프로파일링 정책에 사용되는 일련의 속성 및 CoA(Change of Authorization), BYOD(Bring Your Own Device), DRW(Device Registration WebAuth) 등이 Cisco ISE에서 정상적으로 작동하기 위해 반드시 필요한 속성 집합입니다. 허용 목록은 엔드포인트의 소유권이 변경(여러 정책 서비스 노드에서 속성이 수집될 때)되는 경우에 항상 조건으로 사용되며, 비활성화된 경우에도 마찬가지입니다.

기본적으로 허용 목록은 비활성화되어 있으며 속성은 속성 필터가 활성화된 경우에만 삭제됩니다. 허용 목록은 프로파일링 정책에 새 속성을 포함시키는 피드를 비롯하여 엔드포인트 프로파일링 정책이 변경되면 동적으로 업데이트됩니다. 허용 목록에 없는 속성은 수집 시 즉시 삭제되며 그러한 속성은 엔드포인트 프로파일링에 사용되지 않습니다. 버퍼링과 함께 사용되는 경우 지속성 이벤트의 수는 감소할 수 있습니다.

다음 두 소스에서 확인된 속성 집합이 허용 목록에 포함되어 있는지 확인해야 합니다.

- 엔드포인트를 프로파일과 일치시킬 수 있도록 기본 프로파일에 사용되는 속성 집합
- CoA(Change of Authorization), BYOD(Bring Your Own Device), DRW(Device Registration WebAuth) 등이 정상적으로 작동하기 위해 반드시 필요한 속성 집합

참고 허용 목록에 새 속성을 추가하려면 관리자가 해당 속성을 사용하는 새 프로파일러 조건 및 정책을 생성해야 합니다. 이 새 속성은 저장 및 복제된 속성의 허용 목록에 자동으로 추가됩니다.

표 ***96:*** 허용 속성

AAA-Server	BYODRegistration
Calling-Station-ID	인증서 만료 날짜
인증서 발급 날짜	인증서 발급자 이름
인증서 일련 번호	설명
DestinationIPAddress	디바이스 식별자
디바이스 이름	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
FQDN	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS 버전	OUI
PolicyVersion	PortalUser
PostureApplicable	제품
RegistrationTimeStamp	—
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress

cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities
lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	—

IOS 센서 내장 스위치에서의 속성 수집

IOS 센서 통합을 통해 Cisco ISE 런타임 및 Cisco ISE 프로파일러에서 스위치로부터 전송된 속성의 일부 또는 전부를 수집할 수 있습니다. RADIUS 프로토콜을 사용하여 스위치에서 직접 DHCP, CDP 및 LLDP 속성을 수집할 수 있습니다. DHCP, CDP 및 LLDP에 대해 수집된 속성은 구문 분석되고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionary(**사전**)** 위치에서 프로파일러 사전의 속성에 매핑됩니다.

디바이스 센서에서 지원되는 Catalyst 플랫폼에 대한 자세한 내용은 https://communities.cisco.com/docs/DOC-72932를 참고하십시오.

IOS 센서 내장 네트워크 액세스 디바이스

IOS 센서 내장 네트워크 액세스 디바이스를 Cisco ISE와 통합하면 다음 구성 요소가 통합됩니다.

- IOS 센서
- DHCP, CDP 및 LODP 데이터 수집을 위해 네트워크 액세스 디바이스(스위치)에 내장되어 있는 데이터 컬렉터
- 데이터를 처리하고 엔드포인트의 디바이스 유형을 확인하기 위한 분석기

  분석기는 두 가지 방식으로 구축할 수 있지만 이 두 방식을 함께 사용할 수는 없습니다.

  - Cisco ISE에서 분석기를 구축할 수 있습니다.
  - 스위치에 센서로 분석기를 내장할 수 있습니다.

IOS 센서 지원 네트워크 액세스 디바이스의 컨피그레이션 체크리스트

이 섹션에는 스위치로부터 직접 DHCP, CDP 및 LLDP 속성을 수집하도록 IOS 센서 지원 스위치 및 Cisco ISE에서 구성해야 하는 작업 목록이 요약되어 있습니다.

- Cisco ISE에서 RADIUS 프로브가 활성화되어 있는지 확인합니다.
- 네트워크 액세스 디바이스가 DHCP, CDP 및 LLDP 정보 수집용 IOS 센서를 지원하는지 확인합니다.
- 네트워크 액세스 디바이스가 다음 CDP 및 LLDP 명령을 실행하여 엔드포인트에서 CDP 및 LLDP 정보를 캡처하는지 확인합니다.

```
cdp enable
lldp run
```

- 세션 계정 관리가 표준 AAA 및 RADIUS 명령을 사용해 개별적으로 활성화되어 있는지 확인합니다.

  예를 들어 다음 명령을 사용합니다.

```
aaa new-model
aaa accounting dot1x default start-stop group radius

radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
radius-server vsa send accounting
```

- IOS 센서별 명령을 실행해야 합니다.
  - 계정 관리 확대 활성화

    IOS 센서 프로토콜 데이터를 RADIUS 계정 관리 메시지에 추가하고 새 센서 프로토콜 데이터를 탐지할 때 추가적인 계정 관리 이벤트를 생성하려면 네트워크 액세스 디바이스를 활성화해야 합니다. 즉, RADIUS 계정 관리 메시지에 모든 CDP, LLDP 및 DHCP 속성이 포함되어야 합니다.

    다음 전역 명령을 입력합니다.

    device-sensor accounting

  - 계정 관리 확대 비활성화

    (계정 관리) 네트워크 액세스 디바이스를 비활성화하고 지정된 포트에서 호스팅되는 세션에 대한 IOS 센서 프로토콜 데이터를 RADIUS 계정 관리 메시지에 추가하려면(계정 관리 기능이 전역적으로 활성화된 경우) 적절한 포트에 대해 다음 명령을 입력합니다.

    no device-sensor accounting

  - TLV 변경 추적

    기본적으로 지원되는 각 피어 프로토콜의 경우, 지정된 세션 상황에서 이전에 수신하지 않은 TLV(Type, Length, Value)가 인커밍 패킷에 포함되어 있는 경우에만 클라이언트 알림 및 계정 관리 이벤트가 생성됩니다.

새 TLV가 있거나 이전에 수신한 TLV의 값이 서로 다른 모든 TLV 변경 사항에 대해 클라이언트 알림 및 계정 관리 이벤트를 활성화해야 합니다. 다음의 명령을 입력합니다.

device-sensor notify all-changes

- 네트워크 액세스 디바이스에서 IOS Device Classifier(로컬 분석기)를 비활성화해야 합니다.

  다음의 명령을 입력합니다.

```
no macro auto monitor
```

참고 이 명령은 네트워크 액세스 디바이스에서 변경당 두 개의 동일한 RADIUS 계정 관리 메시지가 전송되는 것을 차단합니다.

ISE 프로파일러를 통한 Cisco IND 컨트롤러 지원

Cisco ISE는 Cisco IND(Industrial Network Device)에 연결된 디바이스의 상태를 프로파일링하고 표시할 수 있습니다. PxGrid는 Cisco ISE와 Cisco Industrial Network Director를 연결하여 엔드포인트(IoT) 데이터와 통신합니다. Cisco ISE의 pxGrid는 Cisco IND 이벤트를 사용하고 Cisco IND를 쿼리하여 엔드포인트 유형을 업데이트합니다.

Cisco ISE 프로파일러에는 사물 인터넷(IoT) 디바이스에 대한 사전 속성이 있습니다. **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**)**를 선택하고 시스템 사전 목록에서 *IOTASSET*를 선택하여 사전 속성을 확인합니다.

지침 및 권장 사항

프로파일링을 위해 여러 ISE 노드를 구성한 경우 한 노드에서만 Cisco IND에 대해 pxGrid를 활성화하는 것이 좋습니다.

여러 Cisco IND 디바이스를 단일 ISE에 연결할 수 있습니다.

둘 이상의 게시자(Cisco IND)에서 동일한 엔드포인트가 수신되는 경우 Cisco ISE는 해당 엔드포인트에 대한 마지막 게시자의 데이터만 유지합니다.

Cisco ISE는 pxGrid의 서비스 이름 *com.cisco.endpoint.asset* 및 */topic/com.cisco.endpoint.asset*에서 Cisco IND 데이터를 가져옵니다.

Cisco IND 프로파일링 프로세스 플로우

Cisco IND 에셋 검색은 IoT 디바이스를 찾고 해당 디바이스의 엔드포인트 데이터를 pxGrid에 게시합니다. Cisco ISE는 pxGrid에서 이벤트를 확인하고 엔드포인트 데이터를 가져옵니다. Cisco ISE의 프로파일러 정책은 디바이스 데이터를 ISE 프로파일러 사전의 속성에 할당하고 해당 속성을 Cisco ISE의 엔드포인트에 적용합니다.

Cisco ISE의 기존 속성을 충족하지 않는 IoT 엔드포인트 데이터는 저장되지 않습니다. 그러나 Cisco ISE에서 더 많은 속성을 생성하여 Cisco IND에 등록할 수 있습니다.

Cisco ISE는 pxGrid를 통해 Cisco IND에 대한 연결이 처음 설정될 때 엔드포인트를 대량으로 다운로드합니다. 네트워크 장애가 발생할 경우 Cisco ISE는 누적된 엔드포인트 변경 사항을 다시 한 번 대량으로 다운로드합니다.

IND 프로파일링을 위한 Cisco ISE 및 Cisco IND 구성

참고 Cisco IND에서 pxGrid를 활성화하기 전에 Cisco IND에 Cisco ISE 인증서를 설치하고 ISE에 Cisco IND 인증서를 설치해야 합니다.

1. **Administration(**관리**)** > **Deployment(**구축**)**를 선택합니다. pxGrid 사용자로 사용할 PSN을 편집하고 pxGrid를 활성화합니다. 이 PSN은 Cisco IND 및 프로파일링에서 게시한 pxGrid 데이터에서 엔드포인트를 생성합니다.
2. **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)**를 선택하여 pxGrid가 실행 중인지 확인합니다. 그런 다음 **Certificates(**인증서**)** 탭을 클릭하고 인증서 필드에 내용을 입력합니다. **Create(**생성**)**를 클릭하여 인증서를 발급하고 인증서를 다운로드합니다.
   - **I want to(**원하는 옵션**)**에서 **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**), CN(Common Name)**을 선택하고 연결하는 Cisco IND의 이름을 입력합니다.
   - **Certificate Download Format(**인증서 다운로드 형식**)**에서 **`PKS12 format(PKS12` 형식`)`**을 선택합니다.
   - **Certificate Password(**인증서 비밀번호**)**에서 비밀번호를 생성합니다.

참고 ISE 내부 CA를 활성화해야 합니다. 브라우저에서 팝업을 차단한 경우 인증서를 다운로드할 수 없습니다. 다음 단계에서 PEM 파일을 사용할 수 있도록 인증서의 압축을 풉니다.

3. Cisco IND에서 **Settings(**설정**)** > **pxGrid**를 선택하고 **`Download .pem IND certificate(.pem IND` 인증서 다운로드`)`**를 클릭합니다. 이 창을 열어 둡니다.
4. Cisco ISE에서 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **All Clients(**모든 클라이언트**)**를 선택합니다. Cisco IND pxGrid 클라이언트가 표시되면 승인합니다.
5. Cisco IND에서 슬라이더를 이동하여 pxGrid를 활성화합니다. 다른 화면이 열리면 ISE 노드의 위치, ISE에서 이 pxGrid 서버에 대해 입력한 인증서의 이름 및 입력한 비밀번호를 지정합니다. **Upload Certificate(**인증서 업로드**)**를 클릭하고 ISE pxGrid PEM 파일을 찾습니다.
6. ISE에서 **Administration(**관리**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다. **Import(**가져오기**)**를 클릭하고 Cisco IND에서 가져온 인증서의 경로를 입력합니다.
7. Cisco IND에서 **Activate(**활성화**)**를 클릭합니다.

8. Cisco ISE에서 **Administation(**관리**)> Deployment(**구축**)**를 선택합니다. Cisco IND 연결에 사용 중인 PSN을 선택하고 Profiling(프로파일 링) 창을 선택한 다음 pxGrid 프로브를 활성화합니다.
9. 이제 ISE와 Cisco IND 간의 pxGrid 연결이 활성화됩니다. Cisco IND에서 찾은 IoT 엔드포인트를 표시하여 확인합니다.

IND 프로파일링을 위한 속성 추가

Cisco IND는 ISE 사전에 없는 속성을 반환할 수 있습니다. Cisco ISE에 속성을 더 추가하여 해당 IoT 디바이스를 더욱 정확하게 프로파일링할 수 있습니다. 새 속성을 추가하려면 Cisco ISE에서 사용자 맞춤화 속성을 생성하고 해당 속성을 pxGrid를 통해 Cisco IND로 전송합니다.

1. **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)**를 선택한 다음 **Endpoint Custom Attributes(**엔드포인트 사용자 맞춤화 속성**)**를 선택합니다. 속성 엔드포인트 속성을 생성합니다.
2. 이제 프로파일러 정책에서 이 속성을 사용하여 새 속성으로 에셋을 식별할 수 있습니다. **Policy(**정책**)** > **Profiling(**프로파일링**)**을 선택하고 새 프로파일러 정책을 생성합니다. **Rules(**규칙**)** 섹션에서 새 규칙을 생성합니다. 속성/값을 추가할 때 **CUSTOMATTRIBUTE** 폴더 및 생성한 사용자 맞춤화 속성을 선택합니다.

MUD에 대한 ISE 지원

제조업체 사용 설명자(MUD)는 온보드(on-board) IoT 디바이스에 대한 방법을 정의하는 IETF 표준입니다. 이는 사물 인터넷 디바이스에 대한 완벽한 가시성 및 세그멘테이션 자동화를 제공합니다. MUD는 IETF 프로세스에서 승인되었으며 RFC8520으로 릴리스되었습니다. 자세한 내용은 https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/를 참조하십시오.

Cisco ISE, 릴리스 2.6 이상에서는 IoT 디바이스 식별을 지원합니다. Cisco ISE는 프로파일링 정책 및 엔드포인트 ID 그룹을 자동으로 생성합니다. MUD는 IoT 디바이스 프로파일링, 동적으로 프로파일링 정책을 생성, 정책 및 엔드포인트 ID 그룹을 생성하는 전체 프로세스 자동화를 지원합니다. 관리자는 이러한 프로파일링 정책을 사용하여 권한 부여 정책 및 프로파일을 수동으로 생성할 수 있습니다. DHCP 및 LLDP 패킷으로 MUD URL을 전송하는 사물 인터넷 디바이스는 이러한 프로파일과 정책을 사용하여 온보딩됩니다.

Cisco ISE는 사물 인터넷 디바이스의 서명되지 않은 분류를 수행합니다. Cisco ISE는 MUD 속성을 저장하지 않습니다. 속성은 현재 세션에서만 사용됩니다. **Context and Visibility(**상황 및 가시성**)** > **Endpoints (**엔드포인트**)** 창에서 **Endpoint Profile(**엔드포인트 프로파일**)** 필드로 사물 인터넷 디바이스를 필터링할 수 있습니다.

다음 디바이스는 Cisco ISE로 MUD 데이터 전송을 지원합니다.

- Cisco Catalyst 3850 Series Switches running Cisco IOS XE Version 16.9.1 & 16.9.2
- Cisco Catalyst Digital Building Series Switches running Cisco IOS Version 15.2(6)E2
- Cisco Industrial Ethernet 4000 Series Switches running Cisco IOS Version 15.2(6)E2
- MUD 기능이 내장된 사물 인터넷(IoT) 디바이스

Cisco ISE는 다음 프로파일링 프로토콜 및 프로파일링 프로브를 지원합니다.

- LLDP 및 Radius-TLV 127
- DHCP-옵션 161

두 필드 모두 IOS Device Sensor에서 Cisco ISE로 전송할 수 있습니다.

MUD를위한 ISE 구성

1. **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Profiler Settings(**프로파일러 설정**)**를 선택하고 **Enable profiling for MUD (MUD**용 프로파일링 활성화**)** 확인란을 선택합니다.
2. ISE에 MUD URI를 보낼 수 있는 네트워크 액세스 디바이스 추가 네트워크 디바이스를 추가하려면 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택합니다.
3. MUD-URL 연결이 작동하는지 확인합니다.
    1. **Context Visibility(**상황 가시성**)** > **Endpoints(** 엔드포인트**)**를 선택하고 ISE가 성공적으로 분류한 사물 인터넷 엔드포인트를 찾습니다. **IOT-MUD**로 시작하는 엔드포인트 프로파일 이름으로 사물 인터넷 디바이스를 필터링할 수 있습니다.
    2. 사물 인터넷 디바이스 중 한 개 디바이스의 엔드포인트 MAC 주소를 클릭하고 속성 태그를 선택합니다. 속성 목록에 mud-url이 있는지 확인합니다.
    3. **Policy(**정책**)** > **Profiling(**프로파일링**)**을 선택하고 **System Type(**시스템 유형**)**으로 **IOT Created(IOT** 생성됨**)**를 선택하여 목록을 필터링합니다.
4. 필요에 따라 새 사물 인터넷 디바이스에 대한 디버그 로깅을 구성합니다.
    1. System Logging Debug Log Configuration (시스템 로깅 디버그 로그 컨피그레이션)을 선택하고 MUD 컨피그레이션이있는 ISE 노드를 선택합니다. > >
    2. 왼쪽 메뉴에서 **Debug Log Configuration(**디버그 로그 컨피그레이션**)**을 선택한 다음 프로파일러를 선택합니다.

더 많은 사물 인터넷 디바이스가 분류됨에 따라 동일한 카테고리 또는 동일한 MUD-URL 을 갖는 동일한 그룹의 모든 디바이스가 동일한 엔드포인트 그룹으로 할당됩니다. 예를 들어, Molex 라이트가 연결되고 분류된 경우 해당 Molex 라이트에 대한 프로파일러 그룹이 생성됩니다. 동일한 유형(MUD-URL이 동일한)의 더 많은 Molex 라이트가 분류됨에 따라 동일한 분류 또는 엔드포인트 ID 그룹을 상속합니다.

ISE 및 Switch에서 MUD 트래픽 흐름 확인

1. 사물 인터넷 디바이스를 켜기 전에 포트를 연결하거나 인터페이스를 활성화합니다.
    1. ISE에서 패킷 캡처를 시작합니다.
    2. 스위치 포트에서 패킷 캡처를 시작합니다.

2. 스위치에서 다음 출력을 확인합니다.
    1. **show device-sensor cache all**
    2. **show access-session**
    3. **show radius statistics**
3. 사물 인터넷 디바이스를 켭니다.
4. 1분마다 다음을 반복합니다.
    1. **show device-sensor cache all**
    2. **show access-session**
    3. **show radius statistics**
5. 모든 디바이스가 ISE에 표시될 때까지 3 ~ 5분 동안 기다립니다.
6. ISE 및 스위치 패킷 캡쳐를 중단합니다.
7. 1분마다 다음을 반복합니다.
    1. **show device-sensor cache all**
    2. **show access-session**
    3. **show radius statistics**

프로파일러 조건

프로파일링 조건은 다른 조건과 유사한 정책 요소입니다. 그러나 인증, 권한 부여 및 게스트 조건과 달리 프로파일링 조건은 제한된 수의 속성을 기반으로 할 수 있습니다. 프로파일러 조건 페이지에는 Cisco ISE에서 사용 가능한 속성과 해당 설명이 나열됩니다.

프로파일러 조건은 다음 중 하나일 수 있습니다.

- Cisco 제공: Cisco ISE는 구축될 때 미리 정의된 프로파일링 조건을 포함하는데, 그러한 조건은 프로파일러 조건 페이지에서 Cisco 제공으로 식별됩니다. Cisco 제공 프로파일링 조건은 삭제할 수 없습니다.

  Policy(정책**) > Policy Elements(**정책 요소**) > Dictionaries(**사전**) > System(**시스템**)** 위치에 있는 시스템 프로파일러 사전에서도 Cisco 제공 조건을 찾을 수 있습니다.

  MAC 사전을 예를 들 수 있습니다. 일부 제품에서 OUI(Organizationally Unique Identifier)는 디바이스 구성을 식별하고 만들 때 우선적으로 사용하는 고유한 속성입니다. 디바이스 MAC 주소의 구성 요소인 MAC 사전에는 MACAddress 및 OUI 속성이 있습니다.

- 관리자 생성: Cisco ISE 관리자가 생성하는 프로파일러 조건 또는 복제되어 미리 정의된 프로파일링 조건은 관리자 생성으로 식별됩니다. 프로파일러 조건 창에서 프로파일러 사전을 사용하

여 DHCP, MAC, SNMP, IP, RADIUS, NetFlow, CDP, LLDP 및 NMAP 유형의 프로파일러 조건을 생성할 수 있습니다.

프로파일링 정책 수의 권장 상한은 1,000개이지만 프로파일링 정책은 최대 2,000개까지 늘릴 수 있습니다.

네트워크 스캔 작업 프로파일링

엔드포인트 스캔 작업은 엔드포인트 프로파일링 정책에서 참조될 수 있으며 네트워크 스캔 작업과 연결된 조건이 충족되는 경우 트리거되는 구성 가능한 작업입니다.

엔드포인트 스캔은 Cisco ISE 시스템에서 리소스 사용량을 제한하기 위해 엔드포인트를 스캔하는 데 사용됩니다. 네트워크 스캔 작업은 리소스를 많이 사용하는 네트워크 스캔과 달리 단일 엔드포인트를 스캔합니다. 그에 따라 전반적인 엔드포인트 분류 기능이 개선돼 엔드포인트에 대한 엔드포인트 프로파일이 수정됩니다. 엔드포인트 스캔은 한 번에 하나씩만 처리될 수 있습니다.

단일 네트워크 스캔 작업을 엔드포인트 프로파일링 정책에 연결할 수 있습니다. Cisco ISE에는 네트워크 스캔 작업에 대한 3가지 스캔 유형이 미리 정의되어 있습니다. 3가지 스캔 유형(예: OS-scan, SNMPPortsAndOS-scan 및 CommonPortsAndOS-scan)이 모두 포함되거나 하나만 포함될 수 있습니다. Cisco ISE에서 미리 정의된 네트워크 스캔 작업인 OS-scan, SNMPPortsAndOS-scan 및 CommonPortsAndOS-scans는 편집하거나 삭제할 수 없습니다. 고유한 네트워크 스캔 작업을 새로 생성할 수도 있습니다.

엔드포인트가 적절히 프로파일링된 경우 해당 엔드포인트에 대해 구성한 네트워크 스캔 작업을 사용할 수 없습니다. 예를 들어 Apple-Device를 스캔하면 스캔된 엔드포인트를 Apple 디바이스로 분류할 수 있습니다. OS-scan에 따라 엔드포인트가 실행되고 있는 운영체제가 확인되면 Apple-Device 프로파일에 더 이상 일치되지 않으며 Apple 디바이스에 대한 적절한 프로파일에 일치됩니다.

네트워크 스캔 작업 생성

엔드포인트 프로파일링 정책과 연결되어 있는 네트워크 스캔 작업에서는 엔드포인트에서 운영체제, SNMP(Simple Network Management Protocol) 포트 및 일반 포트를 스캔합니다. Cisco에서는 가장 일반적인 NMAP 스캔을 위한 네트워크 스캔 작업을 제공하지만 원하는 작업을 생성할 수도 있습니다.

새 네트워크 스캔을 생성할 때는 NMAP 프로브가 스캔하도록 할 정보의 유형을 정의합니다.

시작하기 전에

네트워크 스캔(NMAP) 프로브를 활성화해야 네트워크 스캔 작업을 트리거하는 규칙을 정의할 수 있습니다. 해당 절차는 Cisco ISE 노드별 프로브 구성에 설명되어 있습니다.

단계 **1** **Policy**(정책) > **Policy Elements**(정책 요소) > **Results**(결과) > **Profiling**(프로파일링) > **Network Scan (NMAP) Actions**(네트워크 스캔(**NMAP**) 작업)를 선택합니다. **Work Centers**(작업 센터) > **Profiler**(프로파일러) > **Policy Elements**(정책 요소) > **NMAP Scan Actions**(**NMAP** 스캔 작업).

단계 **2** **Add**(추가)를 클릭합니다.

단계 **3** 생성할 네트워크 스캔 작업의 이름과 설명을 입력합니다.

단계 **4** 엔드포인트에서 다음을 스캔하려는 경우 하나 이상의 확인란을 선택합니다.

- Scan OS(OS 스캔): 운영체제를 스캔하려는 경우 선택합니다.
- Scan SNMP Port(SNMP 포트 스캔): SNMP 포트(161, 162)를 스캔하려는 경우 선택합니다.
- Scan Common Port(일반 포트 스캔): 일반 포트를 스캔하려는 경우 선택합니다.
- Scan Custom Ports(맞춤형 포트 스캔): 맞춤형 포트를 스캔하려는 경우 선택합니다.
- Scan Include Service Version Information(스캔에 서비스 버전 정보 포함): 디바이스의 세부 설명을 포함할 수 있는 버전 정보를 스캔하려는 경우 선택합니다.
- Run SMB Discovery Script(SMB 검색 스크립트 실행): OS 및 컴퓨터 이름과 같은 정보를 검색하기 위해 SMB 포트(445 및 139)를 스캔하려는 경우 선택합니다.
- Skip NMAP Host Discovery(NMAP 호스트 검색 건너뛰기): NMAP 스캔의 초기 호스트 검색 단계를 건너뛰려는 경우 선택합니다.

  참고 Skip NMAP Host Discovery(NMAP 호스트 검색 건너뛰기) 옵션은 자동 NMAP 스캔의 경우 기본적으로 선택되지만 수동 NMAP 스캔을 실행하려면 이 옵션을 선택해야 합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

NMAP 운영체제 스캔

OS-scan(Operating System scan) 유형에서는 엔드포인트가 실행되고 있는 운영체제(및 OS 버전)를 스캔합니다. 이 스캔에서는 리소스를 많이 사용합니다.

NMAP 툴은 OS-scan에 제한이 있어 신뢰성이 낮은 결과가 생성될 수 있습니다. 예를 들어 스위치 및 라우터와 같은 네트워크 디바이스의 운영체제를 스캔할 때 NMAP OS-scan에서 해당 디바이스에 대해 잘못된 operating-system 속성을 제공할 수 있습니다. 정확도가 100%는 아니더라도 Cisco ISE에는 operating-system 속성이 표시됩니다.

규칙에서 NMAP operating-system 속성을 사용하는 엔드포인트 프로파일링 정책이 낮은 확실성 값 조건(확실성 요인 값)을 포함하도록 구성해야 합니다. NMAP:operating-system 속성을 기반으로 하여 엔드포인트 프로파일링 정책을 생성할 때마다 NMAP에서 잘못된 결과를 필터링할 수 있도록 AND 조건을 포함하는 것이 좋습니다.

다음 NMAP 명령은 스캔 OS를 엔드포인트 프로파일링 정책과 연결할 때 운영체제를 스캔합니다.

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```

다음 NMAP 명령은 서브넷을 스캔하여 출력을 nmapSubnet.log로 보냅니다.

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

표 ***97:*** 수동 서브넷 스캔용 ***NMAP*** 명령

-O	OS 탐지를 활성화합니다.

-sU	UDP를 스캔합니다.
-p <포트 범위>	지정된 포트만 스캔합니다. 예를 들면 U:161, 162와 같이 입력합니다.
oN	일반 출력을 생성합니다.
oX	XML 출력을 생성합니다.

운영체제 포트

다음 표에는 NMAP가 OS 스캔에 사용하는 TCP 포트가 나와 있습니다. 또한 NMAP는 ICMP 및 UDP 포트 51824도 사용합니다.

1	3	4	6	7	9	13	17	19
20	21	22	23	24	25	26	30	32
33	37	42	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99
100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301
306	311	340	366	389	406	407	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808
843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
1000	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040-1100
1102	1104	1105	1106	1107	1108	1110	1111	1112
1113	1114	1117	1119	1121	1122	1123	1124	1126

1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199
1201	1213	1216	1217	1218	1233	1234	1236	1244
1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720
1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972	1974	1984	1998-2010	2013	2020	2021년
2022년	2030	2033	2034	2035	2038	2040-2043	2045-2049	2065
2068	2099	2100	2103	2105-2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196
2200	2222	2251	2260	2288	2301	2323	2366	2381-2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875
2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659
3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995
3998	4000-4006	4045	4111	4125	4126	4129	4224	4242

4279	4321	4343	4443	4444	4445	4446	4449	4550
4567	4662	4848	4899	4900	4998	5000-5004	5009	5030
5033	5050	5051	5054	5060	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900-5907	5910	5911	5915	5922	5925	5950	5952	5959
5960-5963	5987-5989	5998-6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565-6567	6580	6646	6666	6667	6668	6669	6689
6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496
7512	7625	7627	7676	7741	7777	7778	7800	7911
7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080-8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654
8701	8800	8873	8888	8899	8994	9000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876
9877	9878	9898	9900	9917	9929	9943	9944	9968
9998	9999	10000	10001	10002	10003	10004	10009	10010
10012	10024	10025	10082	10180	10215	10243	10566	10616

10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774
32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443
44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389
50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

NMAP SNMP 포트 스캔

SNMPPortsAndOS-scan 유형은 엔드포인트가 실행되는 운영체제 및 OS 버전을 스캔하고 SNMP 포트(161 및 162)가 열려 있으면 SNMP 쿼리를 트리거합니다. 처음 식별되어 알 수 없음 프로파일과 일치하는 것으로 확인된 엔드포인트를 보다 효율적으로 분류하기 위해 이 스캔 유형을 사용할 수 있습니다.

다음 NMAP 명령은 스캔 SNMP 포트를 엔드포인트 프로파일링 정책과 연결할 때 SNMP 포트(UDP 161 및 162)를 스캔합니다.

nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>

표 ***98:*** 엔드포인트 ***SNMP*** 포트 스캔을 위한 ***NMAP*** 명령

-sU	UDP를 스캔합니다.

-p <포트 범위>	지정된 포트만 스캔합니다. 예를 들어 USP 포트 161 및 162를 스캔합니다.
oN	일반 출력을 생성합니다.
oX	XML 출력을 생성합니다.
IP-address	스캔하는 엔드포인트의 IP 주소입니다.

NMAP 공통 포트 스캔

CommanPortsAndOS-scan 유형은 엔드포인트가 실행 중인 운영체제(및 OS 버전) 및 공통 포트(TCP 및 UDP)를 스캔하며 SNMP 포트는 스캔하지 않습니다. 다음 NMAP 명령은 스캔 공통 포트를 엔드포인트 프로파일링 정책과 연결할 때 공통 포트를 스캔합니다. nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>

표 ***99:*** 엔드포인트 공통 포트 스캔을 위한 ***NMAP*** 명령

-sTU	TCP 연결 스캔 및 UDP 스캔 모두입니다.
-p <포트 범위>	TCP 포트(21,22,23,25,53,80,110,135,139,143, 443,445,3306,3389,8080) 및 UDP 포트 (53,67,68,123,135,137, 138,139,161,445,500,520,631,1434,1900)를 스캔합니다.
oN	일반 출력을 생성합니다.
oX	XML 출력을 생성합니다.
IP address	스캔하는 엔드포인트의 IP 주소입니다.

공통 포트

다음 표에는 NMAP가 스캔에 사용하는 공통 포트가 나와 있습니다.

표 ***100:*** 공통 포트

TCP 포트		**UDP** 포트	
포트	서비스	포트	서비스
21/tcp	ftp	53/udp	도메인
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	도메인	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns

TCP 포트		UDP 포트	
포트	서비스	포트	서비스
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

NMAP 맞춤형 포트 스캔

공용 포트 외에 맞춤형 포트를 사용(**Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Policy Elements(**정책 요소**)** > **NMAP Scan Actions(NMAP** 스캔 작업**)**또는**Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Profiling(**프로파일링**)** > **Network Scan (NMAP) Actions(**네트워크 스캔 **(NMAP)** 작업**)**)하여 자동 및 수동 NMAP 스캔 작업을 지정할 수 있습니다. NMAP 프로브는 열려 있는 지정된 맞춤형 포트를 통해 엔드포인트에서 속성을 수집합니다. 이러한 속성은 ISE Identities 페이지의 엔드포인트 속성 목록에서 업데이트됩니다(**Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**). 각 스캔 작업에 대해 최대 10개의 UDP와 10개의 TCP 포트를 지정할 수 있습니다. 공통 포트로 지정한 것과 같은 포트 번호는 사용할 수 없습니다. 자세한 내용은 McAfee ePolicy Orchestrator를 사용하여 프로파일러 정책 구성을 참조하십시오.

NMAP 서비스 버전 정보 포함 스캔

서비스 버전 정보 포함 NMAP 프로브는 디바이스에서 실행 중인 서비스에 대한 정보를 수집하여 엔드포인트를 보다 효율적으로 분류하기 위해 자동으로 스캔합니다. 서비스 버전 옵션을 공용 포트 또는 맞춤형 포트와 결합할 수 있습니다.

예:

CLI 명령: nmap -sV -p T:8083 172.21.75.217

출력:

포트	상태	서비스	버전
8083/tcp	개방형	http	McAfee ePolicy Orchestrator 에이전트 4.8.0.1500 (ePOServerName: WIN2008EPO, AgentGuid: {15D79A243BBABA0FA76C2E}

NMAP SMB 검색 스캔

그러면 NMAP SMB Discovery가 Windows 버전을 구별할 수 있으므로 엔드포인트 프로파일링을 보다 효율적으로 수행할 수 있습니다. NMAP에서 제공하는 SMB 검색 스크립트를 실행하도록 NMAP 스캔 작업을 구성할 수 있습니다.

NMAP 스캔 작업은 Windows 기본 정책 내에 통합되며, 엔드포인트가 정책 및 스캔 규칙과 일치하는 경우 엔드포인트가 스캔되고 결과를 통해 정확한 Windows 버전을 확인할 수 있습니다. 피드 서비스에서 정책이 구성되며, SMB 검색 옵션을 사용하여 사전 정의된 새 NMAP 스캔이 생성됩니다.

NMAP 스캔 작업은 Microsoft-Workstation 정책에 의해 호출되며 스캔 결과는 엔드포인트의 운영체제 속성 아래에 저장되어 Windows 정책에 활용됩니다. 서브넷의 수동 스캔에서 SMB 검색 스크립트 옵션을 찾을 수도 있습니다.

참고 SMB 검색의 경우 엔드포인트에서 Windows 파일 공유 옵션을 활성화해야 합니다.

SMB 검색 속성

엔드포인트에서 SMB 검색 스크립트가 실행되면 SMB.Operating-system과 같은 새 SMB 검색 속성이 엔드포인트에 추가됩니다. 피드 서비스에서 Windows 엔드포인트 프로파일링 정책을 업데이트할 때 이러한 속성을 고려합니다. SMB 검색 스크립트가 실행되면 SMB 검색 속성 앞에 SMB.operating-system, SMB.lanmanager, SMB.server, SMB.fqdn, SMB.domain, SMB.workgroup, SMB.cpe와 같은 SMB가 접두사로 붙습니다.

NMAP 호스트 검색 스캔 건너뛰기

모든 IP 주소의 포트를 모두 스캔하려면 시간이 많이 걸립니다. 스캔의 목적에 따라서는 활성 엔드포인트의 NMAP 호스트 검색을 건너뛸 수 있습니다.

엔드 포인트 분류 후 NMAP 스캔이 트리거되는 경우 프로파일 러는 항상 엔드 포인트의 호스트 검색을 건너 뜁니다. 그러나 Skip NMAP Host Discovery(NMAP 호스트 검색 건너뛰기)를 활성화한 후 수동 스캔 작업이 트리거되면 호스트 검색을 건너뛰게 됩니다.

NMAP 스캔 워크플로우

NMAP 스캔을 수행하기 위해 따라야 할 단계:

시작하기 전에

NMAP SMB 검색 스크립트를 실행하려면 시스템에서 파일 공유를 활성화해야 합니다. 예를 확인하려면 NMAP SMB 검색 스크립트 실행을 위해 파일 공유 활성화 항목을 참고하십시오.

단계 **1** SMB 스캔 작업 생성.

단계 **2** SMB 스캔 작업을 사용하여 프로파일러 정책 구성.

단계 **3** SMB 속성을 사용하여 새 조건 추가.

SMB 스캔 작업 생성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Profiling(**프로파일링**)** > **Network Scan (NMAP) Actions(**네트워크 스캔**(NMAP)** 작업**)**를 선택합니다.

단계 **2** **Action Name(**작업 이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **3** **Run SMB Discovery Script(SMB** 검색 스크립트 실행**)** 확인란을 선택합니다.

단계 **4** 네트워크 액세스 사용자를 생성하려면 **Add(**추가**)**를 클릭합니다.

다음에 수행할 작업

SMB 스캔 작업을 사용하여 프로파일러 정책을 구성해야 합니다.

SMB 스캔 작업을 사용하여 프로파일러 정책 구성

시작하기 전에

SMB 스캔 작업을 사용하여 엔드포인트를 스캔하려면 새 프로파일러 정책을 생성해야 합니다. 예를 들어 DHCP 클래스 식별자가 MSFT 속성을 포함하면 네트워크 작업을 수행해야 하는 규칙을 지정하여 Microsoft 워크스테이션을 스캔할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Add(**추가**)**를 선택합니다.

단계 **2** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **3** 드롭다운에서, 생성한 스캔 작업(예: SMBScanAction)을 선택합니다.

다음에 수행할 작업

SMB 속성을 사용하여 새 조건을 추가해야 합니다.

SMB 속성을 사용하여 새 조건 추가

시작하기 전에

엔드포인트 버전을 스캔하려면 새 프로파일러 정책을 생성해야 합니다. 예를 들어 Microsoft 워크스테이션 상위 정책 아래에서 Windows 7을 스캔할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Add(**추가**)**를 선택합니다.

단계 **2** **Name(**이름**)**(예: Windows-7Workstation) 및 **Description(**설명**)**을 입력합니다.

단계 **3** **Network Scan (NMAP) Action(**네트워크 스캔**(NMAP)** 작업**)** 드롭다운에서 **None(**없음**)**을 선택합니다.

단계 **4** **Parent Policy(**상위 정책**)** 드롭다운에서 Microsoft-Workstation 정책을 선택합니다.

NMAP SMB 검색 스크립트 실행을 위해 파일 공유 활성화

아래에는 NMAP SMB 검색 스크립트를 실행하기 위해 Windows OS 버전 7에서 파일 공유를 활성화하는 예가 나와 있습니다.

단계 **1** 제어판 > 네트워크 및 인터넷을 선택합니다.

단계 **2** 네트워크 및 공유 센터를 선택합니다.

단계 **3** 고급 공유 설정 변경을 선택합니다.

단계 **4** 파일 및 프린터 공유 켜기를 클릭합니다.

단계 **5** **40**비트 또는 **56**비트 암호화를 사용하는 장치에 대해 파일 공유 사용 및 비밀번호 보호 공유 켜기 옵션을 활성화합니다.

단계 **6** **Save Changes(**변경 사항 저장**)**를 클릭합니다.

단계 **7** 방화벽 설정을 구성합니다.

a) 제어판에서 시스템 및 보안 > **Windows** 방화벽 > **Windows** 방화벽에서 프로그램 허용으로 이동합니다.
b) 파일 및 프린터 공유 확인란이 선택되어 있는지 확인합니다.
c) 확인을 클릭합니다.

단계 **8** 공유 폴더를 구성합니다.

a) 대상 폴더를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.
b) 공유 탭을 클릭하고 공유를 클릭합니다.
c) 파일 공유 대화 상자에서 필요한 이름을 추가하고 공유를 클릭합니다.
d) 선택한 폴더를 공유한 후 완료를 클릭합니다.
e) 고급 공유를 클릭하고 이 폴더 공유 확인란을 선택합니다.
f) 권한을 클릭합니다.
g) 스캔 권한 대화 상자에서 **Everyone**을 선택하고 모든 권한 확인란을 선택합니다.
h) **OK(**확인**)**를 클릭합니다.

NMAP 스캔에서 서브넷 제외

NMAP 스캔을 수행하여 엔드포인트의 OS 또는 SNMP 포트를 식별할 수 있습니다.

NMAP 스캔을 수행할 때 NMAP에서 스캔하지 않아야 하는 전체 서브넷 또는 IP 범위를 제외할 수 있습니다. **NMAP Scan Subnet Exclusions(NMAP** 스캔 서브넷 제외**)** 창(**Work Centers(**작업 센터**) > Profiler(**프로파일러**) > Settings(**설정**) > NMAP Scan Subnet Exclusions(NMAP** 스캔 서브넷 제외**)**)에서 서브넷 또는 IP 범위를 구성할 수 있습니다. 이렇게 하면 네트워크의 로드를 제한하고 상당한 시간을 절약할 수 있습니다.

수동 NMAP 스캔의 경우 **Run Manual NMAP Scan(**수동 **NMAP** 스캔 실행**)** 창(**Work Centers(**작업 센터**) > Profiler(**프로파일러**) > Manual Scans(**수동 스캔**) > Manual NMAP Scan(**수동 **NMAP** 스캔**) >**

Configure NMAP Scan Subnet Exclusions(NMAP 스캔 서브넷 제외 구성**)**)을 사용하여 서브넷 또는 IP 범위를 지정할 수 있습니다.

수동 NMAP 스캔 설정

자동 NMAP 스캔에 사용할 수 있는 스캔 옵션을 사용하여 수동 NMAP 스캔(**Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Manual Scans(**수동 스캔**)** > **Manual NMAP Scan(**수동 **NMAP** 스캔**)**)을 수행할 수 있습니다. 스캔 옵션 또는 사전 정의된 스캔을 선택할 수 있습니다.

표 ***101:*** 수동 ***NMAP*** 스캔 설정

필드 이름	사용 지침
Node(노드**)**	NMAP 스캔이 실행되는 ISE 노드를 선택합니다.
Manual Scan Subnet(수동 스캔 서브넷**)**	NMAP 스캔을 실행할 엔드포인트의 서브넷 IP 주소 범위를 입력합니다.
Configure NMAP Scan Subnet Exclusions At(다음 위치에서 **NMAP** 스캔 서브넷 제외 구성**)**	**Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Settings(**설정**)** > **NMAP Scan Subnet Exclusions(NMAP** 스캔 서브넷 제외**)** 창으로 이동됩니다. 제외할 IP 주소 및 서브넷 마스크를 지정합니다. 일치하는 항목이 있으면 NMAP 스캔은 실행되지 않습니다.
NMAP Scan Subnet(NMAP 스캔 서브넷**)**	다음 중 하나를 수행할 수 있습니다. • Specify Scan Options(스캔 옵션 지정) • Select an Existing NMAP Scan(기존 NMAP 스캔 선택)
Specify Scan Options(스캔 옵션 지정**)**	필수 스캔 옵션인 OS, SNMP Port(SNMP 포트), Common Ports(공용 포트), Custom Ports(맞춤형 포트), Include Service Version Information(서비스 버전 정보 포함), Run SMB Discovery Script(SMB 검색 스크립트 실행), Skip NMAP Host Discovery(NMAP 호스트 검색 건너뛰기)를 선택합니다. 자세한 내용은 네트워크 스캔 작업 생성을 참고하십시오.
Select an Existing NMAP Scan(기존 **NMAP** 스캔 선택**)**	기본 프로파일러 NMAP 스캔 작업이 표시되는 **Existing NMAP Scan Actions(**기존 **NMAP** 스캔 작업**)** 드롭다운 목록을 표시합니다.
Reset to Default Scan Options(기본 스캔 옵션으로 재설정**)**	기본 설정으로 되돌리려면 이 옵션을 클릭합니다(모든 스캔 옵션이 선택됨).

필드 이름	사용 지침
Save as NMAP Scan Action(NMAP 스캔 작업으로 저장**)**	작업 이름과 설명을 입력합니다.

수동 **NMAP** 스캔 실행

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Manual Scans(**수동 스캔**)** > **Manual NMAP Scan(**수동 **NMAP** 스캔**)**을 선택합니다.

단계 **2** **Node(**노드**)** 드롭다운 목록에서 NMAP 스캔을 실행하려는 ISE 노드를 선택합니다.

단계 **3** **Manual Scan Subnet(**수동 스캔 서브넷**)** 텍스트 상자에서 열린 포트를 확인하려는 엔드포인트가 있는 서브넷 주소를 입력합니다.

단계 **4** 다음 중 하나를 선택합니다.

a) **Specify Scan Options(**스캔 옵션 지정**)**를 선택하고 페이지 오른쪽에서 필요한 스캔 옵션을 선택합니다. 자세한 내용은 네트워크 스캔 작업 생성 페이지를 참고하십시오.

b) **Select An Existing NMAP Scan Action(**기존 **NMAP** 스캔 작업 선택**)**을 선택하고 MCAFeeEPOOrchestratorClientScan과 같은 기본 NMAP 스캔 작업을 선택합니다.

단계 **5** **Run Scan(**스캔 실행**)**을 클릭합니다.

McAfee ePolicy Orchestrator를 사용하여 프로파일러 정책 구성

Cisco ISE 프로파일링 서비스는 McAfee ePO(McAfee ePolicy Orchestrator) 클라이언트가 엔드포인트에 있는지를 탐지할 수 있습니다. 이렇게 하면 지정된 엔드포인트가 조직에 속하는지 확인하는 데 도움이 됩니다.

프로세스와 관련된 엔터티는 다음과 같습니다.

- ISE 서버
- McAfee ePO 서버
- McAfee ePO 에이전트

Cisco ISE는 구성된 포트에서 NMAP McAfee 스크립트를 사용하여 엔드포인트에서 McAfee 에이전트가 실행되고 있는지를 확인하기 위해 기본 제공 NMAP 스캔 작업(MCAFeeEPOOrchestratorClientscan)을 제공합니다. 맞춤형 포트(예: 8082)를 사용하여 새 NMAP 스캔 옵션을 생성할 수도 있습니다. 아래 단계에 따라 McAfee ePO 소프트웨어를 사용하는 새 NMAP 스캔 작업을 구성할 수 있습니다.

단계 **1** McAfee ePo NMAP 스캔 작업 구성.

단계 **2** McAfee ePO 에이전트 구성.

단계 **3** McAfee ePO NMAP 스캔 작업을 사용하여 프로파일러 정책 구성.

McAfee ePo NMAP 스캔 작업 구성

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Policy Elements(**정책 요소**)** > **Network Scan (NMAP) Actions(**네트워크 스캔**(NMAP)** 작업**)**를 선택합니다.

단계 2 **Add(**추가**)**를 클릭합니다.

단계 3 작업 이름 및 설명을 입력합니다.

단계 4 **Scan Options(**스캔 옵션**)**에서 **Custom Ports(**맞춤형 포트**)**를 선택합니다.

단계 5 **Custom Ports(**맞춤형 포트**)** 대화 상자에서 필요한 TCP 포트를 추가합니다. McAfee ePO용으로는 기본적으로 8080 TCP 포트가 활성화됩니다.

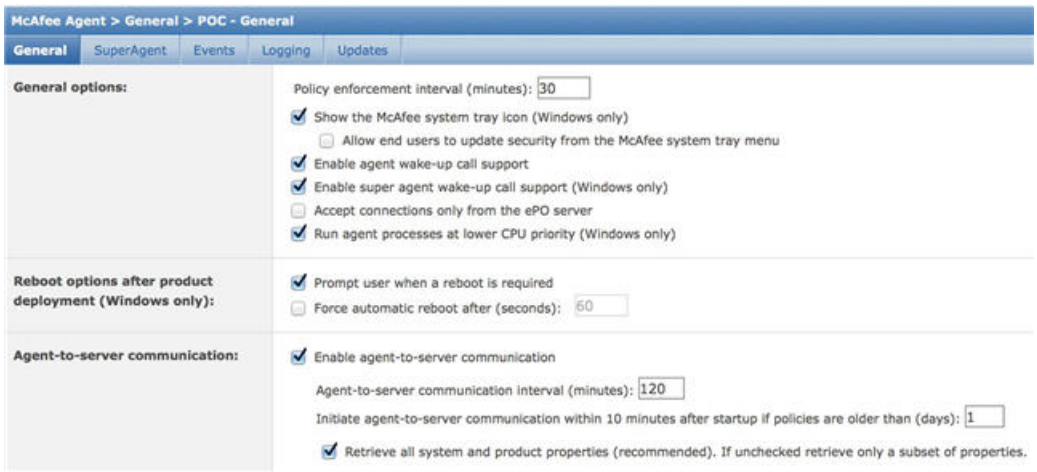
단계 6 **Include Service Version Information(**서비스 버전 정보 포함**)** 확인란을 선택합니다.

단계 7 **Submit(**제출**)**을 클릭합니다.

McAfee ePO 에이전트 구성

단계 1 McAfee ePO 서버에서 McAfee ePO 에이전트와 ISE 서버 간의 통신을 원활하게 수행하기 위한 권장 설정을 선택합니다.

그림 ***29: McAfee ePO*** 에이전트 권장 옵션



단계 2 **Accept Connections Only From The ePO Server(ePO** 서버로부터의 연결만 수락**)**이 선택 취소되어 있는지 확인합니다.

McAfee ePO NMAP 스캔 작업을 사용하여 프로파일러 정책 구성

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Add(**추가**)**를 선택합니다.

단계 2 **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **3** **Network Scan (NMAP) Action(**네트워크 스캔**(NMAP)** 작업**)** 드롭다운 목록에서 필요한 작업(예: MCAFeeEPOOrchestratorClientscan)을 선택합니다.

단계 **4** 상위 프로파일러 정책을 생성합니다(예: DHCP 클래스 식별자가 MSFT 속성을 포함하는지를 확인하는 규칙이 들어 있는 Microsoft-Workstation).

단계 **5** 엔드포인트에 McAfee ePO 에이전트가 설치되어 있는지를 확인하기 위해 상위 NMAP McAfee ePO 정책(예: Microsoft-Workstation) 내에 새 정책(예: CorporateDevice)을 생성합니다.

조건을 충족하는 엔드포인트는 기업 디바이스로 프로파일링됩니다. 정책을 사용하여 McAfee ePO 에이전트로 프로파일링된 엔드포인트를 새 VLAN으로 이동할 수 있습니다.

프로파일러 엔드포인트 사용자 맞춤화 속성

엔드포인트가 프로브에서 수집하는 속성 외에 엔드포인트에 속성을 할당하려면 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Endpoint Custom Attributes(**엔드포인트 사용자 맞춤화 속성**)**를 선택합니다. 엔드포인트 사용자 맞춤화 속성은 권한 부여 정책에서 엔드포인트를 프로파일링하는 데 사용될 수 있습니다.

최대 100개의 엔드포인트 사용자 맞춤화 속성을 생성할 수 있습니다. 지원되는 엔드포인트 사용자 맞춤화 속성 유형은 정수, 문자열, 정수(Long), 부울 및 부동 소수점입니다.

Context Directory(상황 디렉터리**)** > **Endpoints(**엔드포인트**)** > **Endpoint Classification(**엔드포인트 분류**)** 창에서 엔드포인트 사용자 맞춤화 속성의 값을 추가할 수 있습니다.

엔드포인트 사용자 맞춤화 속성의 활용 사례에는 특정 속성에 따라 디바이스를 허용 또는 차단하거나 권한 부여에 따라 특정 권한을 할당하는 것이 포함됩니다.

권한 부여 정책에서 엔드포인트 사용자 맞춤화 속성 사용

Endpoint Custom Attributes(엔드포인트 사용자 맞춤화 속성) 섹션에서는 추가 속성을 구성할 수 있습니다. 각 정의는 속성 및 유형(문자열, 정수, 부울, 부동, Long)으로 구성됩니다. 사용자 맞춤화 속성을 사용하여 디바이스를 프로파일링할 수 있습니다.

참고 엔드포인트에 사용자 맞춤화 속성을 추가하려면 Cisco ISE Advantage 라이선스가 있어야 합니다.

다음 단계에서는 엔드포인트 사용자 맞춤화 속성을 사용하여 권한 부여 정책을 생성하는 방법을 보여줍니다.

단계 **1** 엔드포인트 사용자 맞춤화 속성을 생성하고 값을 할당합니다.

a) **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Endpoint Custom Attributes(**엔드포인트 맞춤형 속성**)** 페이지를 선택합니다.

b) **Endpoint Custom Attributes(**엔드포인트 사용자 맞춤화 속성**)** 영역에서 **Attribute Name(**속성 이름**)**(예: deviceType), Data Type(데이터 유형)(예: String(문자열)) 및 Parameters(파라미터)를 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

d) **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Summary(**요약**)**를 선택합니다.

e) 맞춤형 속성 값을 할당합니다.

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

f) **Edit Endpoint(**엔드포인트 편집**)** 대화 상자의 **Custom Attribute(**맞춤형 속성**)** 영역에서 필요한 속성 값(예: deviceType = Apple-iPhone)을 입력합니다.

g) **Save(**저장**)**를 클릭합니다.

단계 **2** 맞춤형 속성 및 값을 사용하여 권한 부여 정책을 생성합니다.

a) **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택합니다.

b) Endpoints(엔드포인트) 사전에서 맞춤형 속성(예: Rule Name: Corporate Devices, Conditions:EndPoints:deviceType Contains Apple-iPhone, Permissions: then PermitAccess)을 선택하여 권한 부여 정책을 생성합니다.

c) **Save(**저장**)**를 클릭합니다.

관련 항목

프로파일러 엔드포인트 사용자 맞춤화 속성, 731 페이지

프로파일러 조건 생성

Cisco ISE의 엔드포인트 프로파일링 정책을 사용하면 네트워크에서 검색된 엔드포인트를 분류하여 특정 엔드포인트 ID 그룹에 할당할 수 있습니다. 이러한 엔드포인트 프로파일링 정책은 Cisco ISE가 엔드포인트를 분류하고 그룹화하기 위해 평가하는 프로파일링 조건으로 구성됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

단계 **1** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Profiling(**프로파일링**)** > **Add(**추가**)**를 선택합니다.

단계 **2** 엔드포인트 프로파일링 정책 설정, 733 페이지의 설명에 따라 필드의 값을 입력합니다.

단계 **3** 프로파일러 조건을 저장하려면 **Submit(**제출**)**을 클릭합니다.

단계 **4** 조건을 더 생성하려면 이 절차를 반복합니다.

엔드포인트 프로파일링 정책 규칙

라이브러리에서 이전에 생성하여 정책 요소 라이브러리에 저장한 프로파일링 조건 중 하나 이상을 선택할 수 있도록 하는 규칙을 정의할 수 있습니다. 또한 그러한 규칙에 따라 각 조건의 확실성 요인에 대한 정수 값을 연결하거나 해당 조건에 대해 예외 작업 또는 네트워크 스캔 작업을 연결할 수도

있습니다. 예외 작업 또는 네트워크 스캔 작업은 구성 가능한 작업을 트리거하는 데 사용되지만 Cisco ISE는 엔드포인트의 전반적인 분류에 따라 프로파일링 정책을 평가합니다.

OR 연산자를 사용하여 지정된 정책의 규칙을 개별적으로 평가하는 경우 각 규칙의 확실성 메트릭은 엔드포인트 프로파일을 전반적으로 특정 엔드포인트 범주와 일치시키는 데 사용됩니다. 엔드포인트 프로파일링 정책의 규칙이 일치하는 경우 네트워크에서 동적으로 검색되는 프로파일링 정책 및 일치하는 정책은 엔드포인트에 대해 동일합니다.

규칙에서 논리적으로 그룹화된 조건

엔드포인트 프로파일링 정책(프로파일)에는 단일 조건 또는 여러 단일 조건 조합이 포함되어 있으며 그러한 조건은 AND 또는 OR 연산자를 사용하여 논리적으로 결합될 수 있습니다. 이 조건을 기준으로 정책에서 지정된 규칙과 비교하여 엔드포인트를 확인, 분류 및 그룹화할 수 있습니다.

조건은 엔드포인트의 조건에 지정된 값과 비교하여 수집된 엔드포인트 속성 값을 확인하는 데 사용됩니다. 여러 속성을 매핑하는 경우 조건을 논리적으로 그룹화할 수 있습니다. 그러면 네트워크의 엔드포인트를 분류하는 데 도움이 됩니다. 규칙에서 연결되어 있는 해당 확실성 메트릭(정의한 정수 값)을 사용하여 그러한 하나 이상의 조건과 비교하여 엔드포인트를 확인할 수 있습니다. 또는 조건에 연결된 예외 작업이나 조건에 연결된 네트워크 스캔 작업을 트리거할 수 있습니다.

확실성 요인

프로파일링 정책의 최소 확실성 메트릭은 엔드포인트에 대해 일치하는 프로파일을 평가합니다. 엔드포인트 프로파일링 정책의 각 규칙에는 프로파일링 조건에 연결된 최소 확실성 메트릭(정수 값)이 있습니다. 확실성 메트릭은 엔드포인트 프로파일링 정책의 모든 유효한 규칙에 대해 추가되는 수단으로, 엔드포인트 프로파일링 정책의 각 조건이 엔드포인트의 전반적인 분류를 향상시키는 데 어떤 영향을 미치는지 측정합니다.

각 규칙의 확실성 메트릭은 엔드포인트 프로파일을 전반적으로 특정 엔드포인트 범주와 일치시키는 데 사용됩니다. 모든 유효한 규칙의 확실성 메트릭은 함께 추가되어 일치하는 확실성을 이룹니다. 이는 엔드포인트 프로파일링 정책에 정의된 최소 확실성 요인보다 높아야 합니다. 기본적으로 모든 새로운 프로파일링 정책 규칙 및 미리 정의된 프로파일링 정책에 대한 최소 확실성 요인은 10입니다.

엔드포인트 프로파일링 정책 설정

다음 표에서는 **Endpoint Policies(**엔드포인트 정책**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling Policies(**프로파일링 정책**)**입니다.

표 ***102:*** 엔드포인트 프로파일링 정책 설정

필드 이름	사용 지침
Name(이름**)**	생성하려는 엔드포인트 프로파일링 정책의 이름을 입력합니다.
Description(설명**)**	생성하려는 엔드포인트 프로파일링 정책의 설명을 입력합니다.

필드 이름	사용 지침
Policy Enabled(정책 활성화**)**	엔드포인트를 프로파일링할 때 일치하는 프로파일링 정책을 연결하기 위해 **Policy Enabled(**정책 활성화**)** 확인란은 기본적으로 선택됩니다. 이 확인란의 선택을 취소하면 엔드포인트 프로파일링 시 엔드포인트 프로파일링 정책이 제외됩니다.
Minimum Certainty Factor(최소 확실성 요인**)**	프로파일링 정책과 연결할 최소값을 입력합니다. 기본값은 10입니다.
Exception Action(예외 작업**)**	프로파일링 정책에서 규칙을 정의할 때 조건과 연결할 예외 작업을 선택합니다. 기본값은 NONE(없음)입니다. **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Profiling(**프로파일링**) > Exception Actions(**예외 작업**)**에서 예외 작업을 정의합니다.
Network Scan (NMAP) Action(네트워크 스캔 **(NMAP)** 작업**)**	필요한 경우 프로파일링 정책에서 규칙을 정의할 때 조건과 연결할 네트워크 스캔 작업을 목록에서 선택합니다. 기본값은 NONE(없음)입니다. **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Profiling(**프로파일링**) > Network Scan (NMAP) Actions(**네트워크 스캔**(NMAP)** 작업**)**에서 예외 작업을 정의합니다.
Create an Identity Group for the policy(정책에 대한 **ID** 그룹 생성**)**	엔드포인트 ID 그룹을 생성하려면 다음 옵션 중 하나를 선택합니다. • **Yes, create matching Identity Group(**예**,** 일치하는 **ID** 그룹을 생성합니다**.)** • **No, use existing Identity Group hierarchy(**아니요**,** 기존 **ID** 그룹 계층을 사용합니다**.)**

필드 이름	사용 지침
Yes, create matching Identity Group(예**,** 일치하는 **ID** 그룹을 생성합니다**.)**	기존 프로파일링 정책을 사용하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 해당 엔드포인트에 대해 일치하는 ID 그룹이 생성되며, 엔드포인트 프로파일이 기존 프로파일링 정책과 일치하면 ID 그룹은 Profiled 엔드포인트 ID 그룹의 자식이 됩니다. 예를 들어 네트워크에서 검색된 엔드포인트가 Xerox-Device 프로파일과 일치하면 엔드포인트 ID 그룹 페이지에서 Xerox-Device 엔드포인트 ID 그룹이 생성됩니다.
No, use existing Identity Group hierarchy(아니요**,** 기존 **ID** 그룹 계층을 사용합니다**.)**	프로파일링 정책 및 ID 그룹의 계층 구성을 사용하여 일치하는 부모 엔드포인트 ID 그룹에 엔드포인트를 할당하려면 이 확인란을 선택합니다. 이 옵션을 사용하는 경우 엔드포인트 프로파일링 정책 계층을 사용하여 일치하는 부모 엔드포인트 ID 그룹 중 하나와 부모 ID 그룹에 대해 연결된 엔드포인트 ID 그룹에 엔드포인트를 할당할 수 있습니다. 예를 들어 기존 프로파일과 일치하는 엔드포인트는 적절한 부모 엔드포인트 ID 그룹 아래에 그룹화됩니다. 여기서 Unknown(알 수 없음) 프로파일과 일치하는 엔드포인트는 Unknown(알 수 없음) 아래에 그룹화되고 기존 프로파일과 일치하는 엔드포인트는 프로파일이 지정된 엔드포인트 ID 그룹 아래에 그룹화됩니다. 예를 들면 다음과 같습니다. • Cisco-IP-Phone 프로파일과 일치하는 엔드포인트는 Cisco-IP-Phone 엔드포인트 ID 그룹 아래에 그룹화됩니다. • Workstation 프로파일과 일치하는 엔드포인트는 Workstation 엔드포인트 ID 그룹 아래에 그룹화됩니다. Cisco-IP-Phone 및 Workstation 엔드포인트 ID 그룹은 시스템의 Profiled 엔드포인트 ID 그룹에 연결됩니다.

필드 이름	사용 지침
Parent Policy(부모 정책**)**	새 엔드포인트 프로파일링 정책을 연결할 시스템에 정의된 부모 프로파일링 정책을 선택합니다. 자식에게 규칙과 조건을 상속할 부모 프로파일링 정책을 선택할 수 있습니다.
Associated CoA Type(연결된 **CoA** 유형**)**	엔드포인트 프로파일링 정책과 연결할 CoA 유형을 다음 중에서 하나 선택합니다. • CoA 없음 • 포트 바운스 • 재인증 • Administration(관리) > System(시스템) > Settings(설정) > Profiling(프로파일링)에 설정된 프로파일러 컨피그레이션에서 적용되는 전역 설정
Rules(규칙**)**	엔드포인트 프로파일링 정책에 정의된 하나 이상의 규칙에 따라 엔드포인트에 일치하는 프로파일링 정책이 결정됩니다. 그러면 해당 프로파일에 따라 엔드포인트를 그룹화할 수 있습니다. 규칙에서는 정책 요소 라이브러리의 프로파일링 조건을 하나 이상 사용하여 전체 분류를 위한 엔드포인트 속성 및 해당 값을 검증합니다.

필드 이름	사용 지침
Conditions(조건**)**	고정된 Conditions(조건) 오버레이를 확장하려면 더하기 [+] 기호를 클릭하고, 고정된 오버레이를 닫으려면 빼기 [-] 기호를 클릭하거나 오버레이 바깥쪽을 클릭합니다. **Select Existing Condition from Library(**라이브러리에서 기존 조건 선택**)** 또는 **Create New Condition (Advanced Option)(**새 조건 생성**(**고급 옵션**))**을 클릭합니다. **Select Existing Condition from Library(**라이브러리에서 기존 조건 선택**)**: 정책 요소 라이브러리에서 미리 정의된 Cisco 조건을 선택하여 식을 정의할 수 있습니다. **Create New Condition (Advanced Option)(**새 조건 생성**(**고급 옵션**))**: 여러 시스템 또는 사용자 맞춤화 사전에서 속성을 선택하여 식을 정의할 수 있습니다. 다음 중 하나를 프로파일링 조건과 연결할 수 있습니다. • 각 조건에 대한 확실성 요인의 정수 값 • 해당 조건에 대한 예외 작업 또는 네트워크 스캔 작업 프로파일링 조건과 연결할 다음의 미리 정의된 설정 중 하나를 선택합니다. • Certainty Factor Increases(확실성 요인 증가): 각 규칙에 대한 확실성 값을 입력합니다. 전체 분류와 관련하여 모든 일치 규칙에 대해 이 값을 추가할 수 있습니다. • Take Exception Action(예외 작업 수행): 이 엔드포인트 프로파일링 정책의 Exception Action(예외 작업) 필드에 구성되어 있는 예외 작업을 트리거합니다. • Take Network Scan Action(네트워크 스캔 작업 수행): 이 엔드포인트 프로파일링 정책의 Network Scan (NMAP) Action(네트워크 스캔 (NMAP) 작업) 필드에 구성되어 있는 네트워크 스캔 작업을 트리거합니다.

필드 이름	사용 지침
Select Existing Condition from Library(라이브러리에서 기존 조건 선택**)**	다음을 수행할 수 있습니다. • 정책 요소 라이브러리에서 사용 가능한 미리 정의된 Cisco 조건을 선택한 다음 AND 또는 OR 연산자를 사용하여 여러 조건을 추가할 수 있습니다. • Action(작업) 아이콘을 클릭하여 후속 단계에서 다음을 수행합니다. • **Add Attribute or Value(**속성 또는 값 추가**)**: 임시 속성 또는 값 쌍을 추가할 수 있습니다. • **Add Condition from Library(**라이브러리에서 조건 추가**)**: 미리 정의된 Cisco 조건을 추가할 수 있습니다. • **Duplicate(**복제**)**: 선택한 조건의 복사본을 생성합니다. • **Add Condition to Library(**라이브러리에 조건 추가**)**: 생성한 임시 속성/값 쌍을 정책 요소 라이브러리에 저장할 수 있습니다. • **Delete(**삭제**)**: 선택한 조건을 삭제합니다.

필드 이름	사용 지침
Create New Condition (Advance Option)(새 조건 생성**(**고급 옵션**))**	다음을 수행할 수 있습니다. • 식에 임시 속성/값 쌍을 추가한 다음 AND 또는 OR 연산자를 사용하여 여러 조건을 추가할 수 있습니다. • Action(작업) 아이콘을 클릭하여 후속 단계에서 다음을 수행합니다. • **Add Attribute or Value(**속성 또는 값 추가**)**: 임시 속성 또는 값 쌍을 추가할 수 있습니다. • **Add Condition from Library(**라이브러리에서 조건 추가**)**: 미리 정의된 Cisco 조건을 추가할 수 있습니다. • **Duplicate(**복제**)**: 선택한 조건의 복사본을 생성합니다. • **Add Condition to Library(**라이브러리에 조건 추가**)**: 생성한 임시 속성/값 쌍을 정책 요소 라이브러리에 저장할 수 있습니다. • **Delete(**삭제**)**: 선택한 조건을 삭제합니다. AND 또는 OR 연산자를 사용할 수 있습니다.

관련 항목

Cisco ISE 프로파일링 서비스, 688 페이지
엔드포인트 프로파일링 정책 생성, 739 페이지
UDID 속성을 사용하는 엔드포인트 상황 가시성, 776 페이지

엔드포인트 프로파일링 정책 생성

새 프로파일러 정책 페이지에서 다음 옵션을 사용하여 프로파일 엔드포인트에 대해 새 프로파일링 정책을 생성할 수 있습니다.

- Policy Enabled(정책 활성화)
- Create an Identity Group for the policy to create a matching endpoint identity group or use the endpoint identity group hierarchy(정책에 대해 ID 그룹을 생성하여 일치하는 엔드포인트 ID 그룹을 생성하거나 엔드포인트 ID 그룹 계층 사용)
- Parent Policy(부모 정책)

- Associated CoA Type(연결된 CoA 유형)

참고 **Profiling Policies(**프로파일링 정책**)** 창에서 엔드포인트 정책을 생성하도록 선택하는 경우 웹 브라우저에서 Stop(중지) 버튼을 사용하지 마십시오. Stop(중지) 버튼을 사용하는 경우 **New Profiler Policy(**새 프로파일러 정책**)** 창 로드가 중지되고, 다른 목록 페이지에 액세스할 때 해당 페이지 및 페이지 내의 메뉴가 로드되며, 목록 페이지 내의 Filter(필터) 메뉴를 제외한 모든 메뉴에서 작업을 수행할 수 없게 됩니다. 목록 페이지 내의 모든 메뉴에서 작업을 수행하려면 Cisco ISE에서 로그아웃했다가 다시 로그인해야 할 수 있습니다.

엔드포인트 프로파일링 정책을 복제하여 비슷한 특성의 프로파일링 정책을 생성할 수 있습니다. 이 경우 모든 조건을 재정의하여 새 프로파일링 정책을 생성하는 대신 기존 프로파일링 정책을 수정할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling Policies(**프로파일링 정책**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 생성하려는 새 엔드포인트 정책의 이름과 설명을 입력합니다. 엔드포인트를 프로파일링할 때 검증용으로 엔드포인트 프로파일링 정책을 포함하기 위해 **Policy Enabled(**정책 활성화**)** 확인란은 기본적으로 선택됩니다.

단계 **4** 유효한 범위(1~65,535) 내의 최소 확실성 요인 값을 입력합니다.

단계 **5** **Exception Action(**예외 작업**)** 드롭다운 목록 옆의 화살표를 클릭하여 예외 작업을 연결하거나, **Network Scan (NMAP) Action(**네트워크 스캔**(NMAP)** 작업**)** 드롭다운 목록 옆의 화살표를 클릭하여 네트워크 스캔 작업을 연결합니다.

단계 **6** **Create an Identity Group for the policy(**정책에 대한 **ID** 그룹 생성**)**에 대해 다음 옵션 중 하나를 선택합니다.

- **Yes, create matching Identity Group(**예**,** 일치하는 **ID** 그룹을 생성합니다**.)**
- **No, use existing Identity Group hierarchy(**아니요**,** 기존 **ID** 그룹 계층을 사용합니다**.)**

단계 **7** **Parent Policy(**부모 정책**)** 드롭다운 목록 옆의 화살표를 클릭하여 부모 정책을 새 엔드포인트 정책에 연결합니다.

단계 **8** **Associated CoA Type(**연결된 **CoA** 유형**)** 드롭다운 목록에서 연결할 CoA 유형을 선택합니다.

단계 **9** 규칙을 클릭하여 조건을 추가하고 각 조건에 대해 확실성 요인의 정수 값을 연결하거나, 엔드포인트의 전체 분류를 위해 해당 조건에 대한 예외 작업 또는 네트워크 스캔 작업을 연결합니다.

단계 **10** **Submit(**제출**)**을 클릭하여 엔드포인트 정책을 추가하거나 New Profiler Policy(새 프로파일러 정책) 페이지에서 **Profiler Policy List(**프로파일러 정책 목록**)** 링크를 클릭하여 Profiling Policies(프로파일링 정책) 페이지로 돌아갑니다.

엔드포인트 프로파일링 정책별 **CoA(Change of Authorization)** 컨피그레이션

Cisco ISE에서 CoA(Change of Authorization) 유형의 전역 컨피그레이션 외에, 각 엔드포인트 프로파일링 정책에 연결된 특정 CoA 유형을 실행하도록 구성할 수도 있습니다.

전역 No CoA(CoA 없음) 유형 컨피그레이션은 엔드포인트 프로파일링 정책에 구성된 각 CoA 유형을 재정의합니다. 전역 CoA 유형을 No CoA(CoA 없음) 유형이 아닌 다른 유형으로 설정하는 경우 각 엔드포인트 프로파일링 정책은 전역 CoA 컨피그레이션을 재정의할 수 있습니다.

CoA가 트리거되면 각 엔드포인트 프로파일링 정책에서 다음과 같이 실제 CoA 유형을 결정할 수 있습니다.

- General Setting(일반 설정) - 이는 전역 컨피그레이션별로 CoA를 실행하는 모든 엔드포인트 프로파일링 정책에 대한 기본 설정입니다.
- No CoA(CoA 없음) - 이 설정은 프로파일에 대한 전역 컨피그레이션을 재정의하고 CoA를 비활성화합니다.
- Port Bounce(포트 바운스) - 이 설정은 전역 포트 바운스 및 재인증 컨피그레이션 유형을 재정의하고 포트 바운스 CoA를 실행합니다.
- Reauth(재인증) - 이 설정은 전역 포트 바운스 및 재인증 컨피그레이션 유형을 재정의하고 재인증 CoA를 실행합니다.

참고 프로파일러 전역 CoA 컨피그레이션이 Port Bounce(포트 바운스)(또는 Reauth(재인증))로 설정된 경우, 모바일 디바이스에 대한 BYOD 흐름이 차단되지 않도록 정책 단위 CoA 옵션인 No CoA(CoA 없음)을 사용하여 해당 엔드포인트 프로파일링 정책을 구성해야 합니다.

모든 CoA 유형, 그리고 전역 및 엔드포인트 프로파일링 정책 설정에 따라 각각 발급되는 실제 CoA 유형에 대해 아래와 같이 결합된 컨피그레이션 요약을 참고해 주십시오.

표 ***103:*** 다양한 컨피그레이션 조합으로 발급되는 ***CoA*** 유형

전역 **CoA** 유형	정책별 기본 **CoA** 유형 집합	정책별 **No CoA(CoA 없음)** 유형	정책별 **Port Bounce(포트 바운스)** 유형	정책별 **Reauth(재인증)** 유형
No CoA(CoA 없음)	No CoA(CoA 없음)	No CoA(CoA 없음)	No CoA(CoA 없음)	CoA 없음
포트 바운스	Port Bounce(포트 바운스)	CoA 없음	포트 바운스	Re-Auth(재인증)
Reauth(재인증)	Reauth(재인증)	CoA 없음	포트 바운스	Re-Auth(재인증)

엔드포인트 프로파일링 정책 가져오기

내보내기 기능에서 생성할 수 있는 것과 같은 형식을 사용하여 XML로 된 파일에서 엔드포인트 프로파일링 정책을 가져올 수 있습니다. 부모 정책이 연결되어 있는 새로 생성한 프로파일링 정책을 가져오는 경우에는 자식 정책을 정의하기 전에 부모 정책을 정의해야 합니다.

가져오는 파일에는 엔드포인트 프로파일링 정책의 계층이 들어 있으며, 이 계층에는 부모 정책과 그 다음에 가져온 프로파일이 순서대로 포함되어 있고 정책에 정의된 규칙 및 확인 항목도 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling(**프로파일링**)** > **Profiling Policies(**프로파일링 정책**)**을 선택합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** **Browse(**찾아보기**)**를 클릭하여 이전에 내보냈으며 가져오려는 파일을 찾습니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

단계 **5** **Profiling Policies(**프로파일링 정책**)** 창으로 돌아가려면 **Profiler Policy List(**프로파일러 정책 목록**)** 링크를 클릭합니다.

엔드포인트 프로파일링 정책 내보내기

엔드포인트 프로파일링 정책을 다른 Cisco ISE 구축으로 내보낼 수 있습니다. XML 파일을 템플릿으로 사용하여 가져오려는 고유한 정책을 생성할 수도 있습니다. 또한 나중에 가져오기에 사용할 수 있도록 시스템의 기본 위치에 파일을 다운로드할 수도 있습니다.

엔드포인트 프로파일링 정책을 내보낼 때는 적절한 애플리케이션을 사용하여 profiler_policies.xml을 열거나 저장하라는 메시지가 포함된 대화 상자가 나타납니다. 이 파일은 웹 브라우저 또는 적절한 기타 애플리케이션에서 열 수 있는 XML 형식 파일입니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling(**프로파일링**)** > **Profiling Policies(**프로파일링 정책**)**를 선택합니다.

단계 **2** **Export(**내보내기**)**를 선택하고 다음 중 하나를 선택합니다.

- **Export Selected(**선택 항목 내보내기**)**: **Profiling Policies(**프로파일링 정책**)** 창에서 선택한 엔드포인트 프로파일링 정책만 내보낼 수 있습니다.
- **Export Selected with Endpoints(**엔드포인트와 함께 선택한 항목 내보내기**)**: 선택한 엔드포인트 프로파일링 정책 및 해당 정책을 사용하여 프로파일링한 엔드포인트를 내보낼 수 있습니다.
- **Export All(**모두 내보내기**)**: 기본적으로 **Profiling Policies(**프로파일링 정책**)** 창의 모든 프로파일링 정책을 내보낼 수 있습니다.

단계 **3** **OK(**확인**)**를 클릭하여 profiler_policies.xml 파일의 엔드포인트 프로파일링 정책을 내보냅니다.

미리 정의된 엔드포인트 프로파일링 정책

Cisco ISE는 구축될 때 미리 정의된 기본 프로파일링 정책을 포함하며, 계층적 구성에 따라 네트워크에서 식별된 엔드포인트를 분류하고 일치하는 엔드포인트 ID 그룹에 할당할 수 있습니다. 엔드포인트 프로파일링 정책은 계층적이므로 **Profiling Policies(**프로파일링 정책**)** 창에는 디바이스에 대한 일반(상위) 정책 및 Profiling Policies listing(프로파일링 정책 목록) 창에서 상위 정책과 연결된 하위 정책 목록이 표시될 수 있습니다.

Profiling Policies(프로파일링 정책**)** 창에는 엔드포인트 프로파일링 정책과 해당 이름, 유형, 설명 및 상태, 활성화되었는지 여부 또는 검증 대상이 아닌지 여부가 표시됩니다.

엔드포인트 프로파일링 정책 유형은 다음과 같이 분류됩니다.

- Cisco 제공: Cisco ISE에 미리 정의된 엔드포인트 프로파일링 정책은 Cisco 제공 유형으로 식별됩니다.
    - 관리자 수정: 미리 정의된 엔드포인트 프로파일링 정책을 수정하는 경우 엔드포인트 프로파일링 정책은 관리자 수정 유형으로 식별됩니다. Cisco ISE는 업그레이드 과정에서 미리 정의된 엔드포인트 프로파일링 정책에서 변경한 내용을 덮어씁니다.
- 관리자 생성: 관리자가 엔드포인트 프로파일링 정책을 생성하거나 Cisco에서 제공한 엔드포인트 프로파일링 정책을 복제하는 경우 관리자 생성 유형으로 식별됩니다.

하위 정책이 규칙 및 조건을 상속받을 수 있는 일련의 엔드포인트에 대한 일반 정책(상위)을 생성하는 것이 좋습니다. 엔드포인트를 분류해야 하는 경우 엔드포인트를 프로파일링할 때 엔드포인트 프로파일은 먼저 상위 정책과의 일치를 확인한 후 하위 정책과의 일치를 확인해야 합니다.

예를 들어 Cisco-Device는 모든 Cisco 디바이스에 대한 일반 엔드포인트 프로파일링 정책이고 Cisco 디바이스에 대한 다른 정책은 Cisco-Device의 하위 정책입니다. 엔드포인트를 Cisco-IP-Phone 7960으로 분류해야 하는 경우 이 엔드포인트의 엔드포인트 프로파일은 먼저 상위 Cisco-Device 정책과 일치시킨 다음 하위 Cisco-IP-Phone 정책 및 Cisco-IP-Phone 7960 프로파일링 정책 순으로 일치시켜야 보다 효율적인 분류가 가능합니다.

참고 Cisco ISE는 관리자 수정 정책 또는 해당 하위 정책이 여전히 Cisco Provided(Cisco 제공)으로 레이블이 지정되어 있는 경우에도 덮어쓰지 않습니다. 관리자 수정 정책이 삭제되면 이전 Cisco 제공 정책으로 돌아갑니다. 다음에 피드 업데이트가 발생하면 모든 하위 정책이 업데이트됩니다.

업그레이드 중에 덮어쓰기되는 미리 정의된 엔드포인트 프로파일링 정책

프로파일링 정책 페이지에서 기존 엔드포인트 프로파일링 정책을 편집할 수 있습니다. 미리 정의된 엔드포인트 프로파일링 정책을 수정하려면 미리 정의된 엔드포인트 프로파일의 복사본에 모든 컨피그레이션도 저장해야 합니다.

업그레이드 중에 Cisco ISE는 미리 정의된 엔드포인트 프로파일에 저장한 모든 컨피그레이션을 덮어씁니다.

엔드포인트 프로파일링 정책을 삭제할 수 없음

Profiling Policies(프로파일링 정책**)** 창에서 선택한 엔드포인트 프로파일링 정책 또는 모든 엔드포인트 프로파일링 정책을 삭제할 수 있습니다. 기본적으로는 **Profiling Policies(**프로파일링 정책**)** 창에서 모든 엔드포인트 프로파일링 정책을 삭제할 수 있습니다. **Profiling Policies(**프로파일링 정책**)** 창에서 모든 엔드포인트 프로파일링 정책을 선택하여 삭제하려고 할 때 해당 엔드포인트 프로파일링 정책이 다른 엔드포인트 프로파일링 정책이나 권한 부여 정책에 매핑된 경우 이러한 정책 중 일부가 삭제되지 않을 수 있습니다.

- Cisco에서 제공하는 엔드포인트 프로파일링 정책은 삭제할 수 없습니다.
- 엔드포인트 프로파일이 다른 엔드포인트 프로파일의 부모로 정의되어 있으면 **Profiling Policies(**프로파일링 정책**)** 창에서 부모 프로파일을 삭제할 수 없습니다. 예를 들어 Cisco-Device는 Cisco 디바이스에 대한 다른 엔드포인트 프로파일링 정책의 부모 정책입니다.
- 권한 부여 정책에 매핑되어 있는 엔드포인트 프로파일은 삭제할 수 없습니다. 예를 들어 Cisco-IP-Phone은 프로파일링된 Cisco IP 전화 권한 부여 정책에 매핑되어 있으며 Cisco IP 전화에 대한 다른 엔드포인트 프로파일링 정책의 부모 정책입니다.

Draeger 의료 디바이스용 미리 정의된 프로파일링 정책

Cisco ISE에는 Draeger 의료 디바이스용 일반 정책, Draeger-Delta 의료 디바이스용 정책 및 Draeger-M300 의료 디바이스용 정책을 포함하는 기본 엔드포인트 프로파일링 정책이 포함되어 있습니다. Draeger-Delta 및 Draeger-M300 의료 디바이스는 포트 2050 및 2150을 공유하므로 기본 Draeger 엔드포인트 프로파일링 정책을 사용할 때는 이 두 의료 디바이스를 분류할 수 없습니다.

이러한 Draeger 디바이스가 환경에서 포트 2050 및 2150을 공유하는 경우에는 해당 의료 디바이스를 구분할 수 있도록 디바이스 대상 IP 주소 확인을 위한 규칙을 기본 Draeger-Delta 및 Draeger-M300 엔드포인트 프로파일링 정책에 더 추가해야 합니다.

Cisco ISE는 Draeger 의료 디바이스용 엔드포인트 프로파일링 정책에서 사용되는 다음 프로파일링 조건을 포함합니다.

- 포트 2000을 포함하는 Draeger-Delta-PortCheck1
- 포트 2050을 포함하는 Draeger-Delta-PortCheck2
- 포트 2100을 포함하는 Draeger-Delta-PortCheck3
- 포트 2150을 포함하는 Draeger-Delta-PortCheck4
- 포트 1950을 포함하는 Draeger-M300PortCheck1
- 포트 2050을 포함하는 Draeger-M300PortCheck2
- 포트 2150을 포함하는 Draeger-M300PortCheck3

알 수 없는 엔드포인트에 대한 엔드포인트 프로파일링 정책

알 수 없는 엔드포인트는 기존 프로파일과 일치하지 않으며 Cisco ISE에서 프로파일링할 수 없는 엔드포인트입니다. 알 수 없는 프로파일은 엔드포인트에 할당되는 기본 시스템 프로파일링 정책입니다. 이 프로파일에서는 해당 엔드포인트에 대해 수집되는 속성 또는 속성 집합이 Cisco ISE의 기존 프로파일과 일치하지 않습니다.

알 수 없는 프로파일이 할당되는 시나리오는 다음과 같습니다.

- Cisco ISE에서 엔드포인트가 동적으로 검색되었는데 해당 엔드포인트에 일치하는 엔드포인트 프로파일링 정책이 없으면 엔드포인트가 알 수 없는 프로파일에 할당됩니다.
- 엔드포인트가 Cisco ISE에 정적으로 추가되었는데 정적으로 추가된 엔드포인트에 일치하는 엔드포인트 프로파일링 정책이 없으면 엔드포인트가 알 수 없는 프로파일에 할당됩니다.

  네트워크에 엔드포인트를 정적으로 추가한 경우 정적으로 추가된 엔드포인트는 Cisco ISE의 프로파일링 서비스에 의해 프로파일링되지 않습니다. 나중에 알 수 없는 프로파일을 적절한 프로파일로 변경할 수 있으며, Cisco ISE는 할당되었던 프로파일링 정책을 재할당하지 않습니다.

정적으로 추가된 엔드포인트에 대한 엔드포인트 프로파일링 정책

프로파일링 서비스는 정적으로 추가된 엔드포인트를 프로파일링하기 위해 엔드포인트에 새 MATCHEDPROFILE 속성을 추가하여 엔드포인트에 대한 프로파일을 계산합니다. 계산된 프로파일은 엔드포인트가 동적으로 프로파일링되는 경우 해당 엔드포인트의 실제 프로파일입니다. 따라서 정적으로 추가된 엔드포인트에 대해 계산된 프로파일과 동적으로 프로파일링된 엔드포인트의 일치하는 프로파일 간 불일치 여부를 확인할 수 있습니다.

정적 **IP** 디바이스에 대한 엔드포인트 프로파일링 정책

IP 주소가 정적으로 할당된 엔드포인트가 있는 경우 해당 정적 IP 디바이스에 대해 프로파일을 생성할 수 있습니다.

정적 IP 주소를 사용하는 엔드포인트를 프로파일링하려면 RADIUS 프로브나 SNMP 쿼리 및 SNMP 트랩 프로브를 활성화해야 합니다.

엔드포인트 프로파일링 정책 일치

Cisco ISE는 하나 이상의 규칙에 정의되어 있는 프로파일링 조건이 프로파일링 정책에서 충족되면 항상 평가한 정책이 아니라 엔드포인트에 대해 선택한 정책(일치한 정책)을 고려합니다. 여기서 해당 엔드포인트에 대한 정적 할당 상태는 시스템에서 false로 설정됩니다. 그러나 엔드포인트 편집 중에 정적 재할당 기능을 사용하여 시스템의 기존 프로파일링 정책에 엔드포인트를 정적으로 재할당한 후에는 해당 상태를 true로 설정할 수 있습니다.

엔드포인트의 일치한 정책에 적용되는 사항은 다음과 같습니다.

- 정적으로 할당된 엔드포인트의 경우 프로파일링 서비스는 MATCHEDPROFILE을 계산합니다.

- 정적으로 할당된 엔드포인트의 경우에는 MATCHEDPROFILE이 일치하는 엔드포인트 프로파일과 동일합니다.

프로파일링 정책에 정의되어 있는 하나 이상의 규칙을 사용하여 동적 엔드포인트에 일치하는 프로파일링 정책을 확인하고 그룹화를 위해 엔드포인트 ID 그룹을 적절하게 할당할 수 있습니다.

엔드포인트가 기존 정책에 매핑되어 있으면 프로파일링 서비스는 프로파일링 정책의 계층에서 일치하는 정책 그룹을 포함하는 가장 가까운 부모 프로파일을 검색한 다음 엔드포인트를 적절한 엔드포인트 정책에 할당합니다.

권한 부여에 사용되는 엔드포인트 프로파일링 정책

권한 부여 규칙에서 엔드포인트 프로파일링 정책을 사용할 수 있습니다. 이러한 규칙에서는 엔드포인트 프로파일링 정책에 대한 확인을 속성으로 포함하는 새 조건을 생성할 수 있습니다. 해당 속성에는 엔드포인트 프로파일링 정책의 이름이 지정됩니다. PostureApplicable, EndPointPolicy, LogicalProfile 및 BYODRegistration 속성이 포함된 엔드포인트 사전에서 엔드포인트 프로파일링 정책을 선택할 수 있습니다.

PostureApplicable의 속성 값은 운영체제에 따라 자동으로 설정됩니다. AnyConnect 지원은 해당 플랫폼에서 포스처를 수행할 수 없으므로, IOS 및 Android 디바이스에 대해 *No(*아니요*)*로 설정됩니다. 이 값은 Mac OSX 및 Windows 디바이스에 대해서는 *Yes(*예*)*로 설정됩니다.

EndPointPolicy, BYODRegistration 및 ID 그룹 조합을 포함하는 권한 부여 규칙을 정의할 수 있습니다.

논리 프로파일로 그룹화된 엔드포인트 프로파일링 정책

논리 프로파일은 Cisco에서 제공하거나 관리자가 생성한 엔드포인트 프로파일링 정책과는 무관한, 프로파일 범주 또는 연결된 프로파일이 담긴 컨테이너입니다. 엔드포인트 프로파일링 정책은 여러 논리 프로파일에 연결될 수 있습니다.

권한 부여 정책 조건의 논리 프로파일을 사용하여 프로파일 범주에 대한 전반적인 네트워크 액세스 정책을 생성할 수 있습니다. 권한 부여를 위한 단순 조건을 생성할 수 있으며, 이는 권한 부여 규칙에 포함될 수 있습니다. 권한 부여 조건에 사용할 수 있는 속성-값 쌍은 논리 프로파일(속성) 및 논리 프로파일(값)의 이름으로, 이는 엔드포인트 시스템 사전에서 찾을 수 있습니다.

예를 들어 Android, Apple iPhone 또는 Blackberry와 같은 모든 모바일 디바이스에 대한 논리 프로파일을 생성할 수 있는데, 해당 범주의 일치하는 엔드포인트 프로파일링 정책을 논리 프로파일에 할당하면 됩니다. Cisco ISE에는 IP-Phone, Cisco-IP-Phone, Nortel-IP-Phone-2000-Series 및 Avaya-IP-Phone 프로파일 등의 모든 IP Phone의 기본 논리 프로파일인 IP-Phone이 있습니다.

논리적 프로파일 생성

엔드포인트 프로파일링 정책 범주를 그룹화하는 데 사용할 수 있는 논리적 프로파일을 생성할 수 있습니다. 그러면 프로파일 또는 관련 프로파일의 전체 범주를 생성할 수 있습니다. 할당된 집합에서 엔드포인트 프로파일링 정책을 제거하여 사용 가능한 집합으로 다시 이동할 수도 있습니다. 논리적

프로파일에 대한 자세한 내용은 논리 프로파일로 그룹화된 엔드포인트 프로파일링 정책, 746 페이지를 참고하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling(**프로파일링**)** > **Logical Profiles(**논리적 프로파일**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 및 **Description(**설명**)** 텍스트 상자에 새 논리적 프로파일의 이름과 설명을 입력합니다.

단계 **4** **Available Policies(**사용 가능한 정책**)**에서 엔드포인트 프로파일링 정책을 선택하여 논리적 프로파일에 할당합니다.

단계 **5** 오른쪽 화살표를 클릭하여 선택한 엔드포인트 프로파일링 정책을 **Assigned Policies(**할당된 정책**)**로 이동합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

프로파일링 예외 작업

예외 작업은 엔드포인트 프로파일링에서 참조될 수 있으며 작업과 연결된 예외 조건이 충족되는 경우 트리거되는 단일의 구성 가능한 작업입니다.

예외 작업은 다음 유형 중 하나일 수 있습니다.

- Cisco 제공 - Cisco 제공 예외 작업은 삭제할 수 없습니다. Cisco ISE에서 엔드포인트를 프로파일링하려는 경우 Cisco ISE는 시스템에서 다음과 같은 편집 불가능한 프로파일링 예외 작업을 트리거합니다.
  - 권한 부여 변경 - 권한 부여 정책에 사용되는 엔드포인트 ID 그룹에서 엔드포인트가 추가되거나 제거될 때 프로파일링 서비스는 CoA(Change of Authorization)를 실행합니다.
  - 엔드포인트 삭제 - 엔드포인트가 시스템의 엔드포인트 페이지에서 삭제되거나 Cisco ISE 네트워크의 편집 페이지에서 알 수 없는 프로파일로 다시 할당되면, Cisco ISE에서 예외 작업이 트리거되고 CoA가 실행됩니다.
  - FirstTimeProfiled - 엔드포인트가 Cisco ISE에서 처음 프로파일링되는 경우 Cisco ISE에서 예외 작업이 트리거되고 CoA가 실행됩니다. 이 경우 엔드포인트의 프로파일이 알 수 없는 프로파일에서 기존 프로파일로 변경되지만 Cisco ISE 네트워크에서 엔드포인트가 성공적으로 인증되지 않습니다.
- 관리자 생성 - Cisco ISE에서 관리자가 생성한 프로파일링 예외 작업을 트리거합니다.

예외 작업 생성

하나 이상의 예외 규칙을 정의하여 단일 프로파일링 정책에 연결할 수 있습니다. 이와 같이 연결하는 경우 프로파일링 정책이 일치하며 Cisco ISE의 프로파일링 엔드포인트에서 하나 이상의 예외 규칙이 일치하면 예외 작업(구성 가능한 단일 작업)이 트리거됩니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Profiling(**프로파일링**)** > **Exception Actions(**예외 작업**)**를 선택합니다.

단계 2 **Add(**추가**)**를 클릭합니다.

단계 3 **Name(**이름**)** 및 **Description(**설명**)** 텍스트 상자에 예외 작업의 이름과 설명을 입력합니다.

단계 4 **CoA Action(CoA** 작업**)** 확인란을 선택합니다.

단계 5 **Policy Assignment(**정책 할당**)** 드롭다운 목록을 클릭하고 엔드포인트 정책을 선택합니다.

단계 6 **Submit(**제출**)**을 클릭합니다.

정책 및 ID 그룹을 정적으로 할당하여 엔드포인트 생성

엔드포인트 페이지에서 엔드포인트의 MAC 주소를 사용하여 새 엔드포인트를 정적으로 생성할 수 있습니다. 또한 엔드포인트 페이지에서 정적 할당용으로 엔드포인트 프로파일링 정책 및 ID 그룹을 선택할 수도 있습니다.

엔드포인트 ID 목록에는 일반 및 모바일 디바이스(MDM) 엔드포인트가 표시됩니다. 목록 페이지에는 MDM 엔드포인트에 대한 호스트 이름, 디바이스 유형, 디바이스 식별자 등의 속성에 해당하는 열이 표시됩니다. 정적 할당, 정적 그룹 할당 등의 기타 열은 기본적으로 표시되지 않습니다.

참고 이 페이지를 사용하여 MDM 엔드포인트 추가, 편집, 삭제, 가져오기 또는 내보내기를 수행할 수는 없습니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**를 선택합니다.

단계 2 **Add(**추가**)**를 클릭합니다.

단계 3 엔드포인트의 MAC 주소를 쉼표로 구분된 16진수 형식으로 입력합니다.

단계 4 **Policy Assignment(**정책 할당**)** 드롭다운 목록에서 일치하는 엔드포인트 정책을 선택하여 정적 할당 상태를 동적에서 정적으로 변경합니다.

단계 5 **Static Assignment(**정적 할당**)** 확인란을 선택하여 엔드포인트에 할당되어 있는 정적 할당 상태를 동적에서 정적으로 변경합니다.

단계 6 **Identity Group Assignment(ID** 그룹 할당**)** 드롭다운 목록에서 새로 생성하는 엔드포인트를 할당할 엔드포인트 ID 그룹을 선택합니다.

단계 7 **Static Group Assignment(**정적 그룹 할당**)** 확인란을 선택하여 엔드포인트 ID 그룹의 동적 할당을 정적으로 변경합니다.

단계 8 **Submit(**제출**)**을 클릭합니다.

CSV 파일에서 엔드포인트 가져오기

Cisco ISE 템플릿에서 생성한 CSV 파일에서 엔드포인트를 가져와 엔드포인트 세부정보로 업데이트할 수 있습니다. ISE에서 내보낸 엔드포인트는 약 75개의 속성을 포함하므로, 다른 ISE 구축으로 직접 가져올 수 없습니다. 가져올 수 없는 열이 CSV 파일에 있으면 열 목록이 포함된 메시지가 표시됩니다. 파일을 다시 가져오기 전에 지정된 열을 삭제해야 합니다.

참고 엔드포인트 사용자 맞춤화 속성을 가져오려면 올바른 데이터 유형을 사용하여 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Endpoint Custom Attributes(**엔드포인트 사용자 맞춤화 속성**)** 페이지의 CSV 파일에서와 동일한 사용자 맞춤화 속성을 만들어야합니다. 이러한 속성은 "CUSTOM."으로 시작되어 엔드포인트 속성과 차별화되어야 합니다.

가져올 수 있는 속성은 약 30개입니다. 목록에는 MACAddress, EndPointPolicy 및 IdentityGroup이 포함됩니다. 선택할 수 있는 속성은 다음과 같습니다.

설명	PortalUser	LastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress
PortalUser.Location	Device Type	host-name
PortalUser.GuestStatus	StaticAssignment	Location
PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion
PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<custom attribute name>	—	—

엔드포인트 목록이 MACAddress, EndpointPolicy, IdentityGroup <위에서 선택적 속성으로 나열된 속성 목록> 순으로 나타나도록 파일 헤더는 기본 가져오기 템플릿에 지정된 형식이어야 합니다. 다음 파일 템플릿을 생성할 수 있습니다.

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <위에서 선택적 속성으로 나열된 속성 목록>

CSV 파일에서 엔드포인트를 가져오는 경우 MAC 주소를 제외한 모든 속성 값은 선택 사항입니다. 특정 값 없이 엔드포인트를 가져오려는 경우 값을 쉼표로 구분합니다. 예를 들면 다음과 같습니다.

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser 등

단계 **1** **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Import(**가져오기**)** 를 선택합니다.
단계 **2** **Import From File(**파일에서 가져오기**)**을 클릭합니다.
단계 **3** **Browse(**찾아보기**)**를 클릭하여 이미 생성한 CSV 파일을 찾습니다.
단계 **4** **Submit(**제출**)**을 클릭합니다.

엔드포인트에 사용할 수 있는 기본 가져오기 템플릿

엔드포인트를 가져오는 데 사용할 수 있는 템플릿을 생성하여 엔드포인트를 업데이트할 수 있습니다. 기본적으로, Generate a Template(템플릿 생성) 링크를 사용하여 Microsoft Office Excel 애플리케이션에서 CSV 파일을 생성하고 파일을 로컬로 시스템에 저장할 수 있습니다. 파일은 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Import(**가져오기**)** > **Import From File(**파일에서 가져오기**)**에서 찾을 수 있습니다. Generate a Template(템플릿 생성) 링크를 사용하여 템플릿을 생성하면 Cisco ISE 서버에 Opening template.csv(template.csv 여는 중) 대화 상자가 표시됩니다. 이 대화 상자를 사용하면 기본 template.csv 파일을 열거나, template.csv 파일을 로컬로 시스템에 저장할 수 있습니다. 대화 상자에서 template.csv 파일 열기를 선택하는 경우 파일이 Microsoft Office Excel 애플리케이션에서 열립니다. 기본 template.csv 파일에는 MAC 주소, 엔드포인트 정책 및 엔드포인트 ID, 그리고 기타 선택 속성을 표시하는 헤더 행이 포함되어 있습니다.

엔드포인트의 MAC 주소, 엔드포인트 프로파일링 정책 및 엔드포인트 ID 그룹 그리고 가져오고자 하는 선택 속성값을 업데이트하고, 이를 새로운 파일명으로 저장합니다. 이 파일은 엔드포인트를 가져오는 데 사용할 수 있습니다. Generate a Template(템플릿 생성) 링크를 사용하는 경우 작성된 template.csv 파일의 헤더 행을 참고해 주십시오.

표 ***104: CSV*** 템플릿 파일

MAC	**EndPointPolicy**	**IdentityGroup**	기타 선택 속성
11:11:11:11:11:11	Android	Profiled	<Empty>/<Value>

가져오기 중에 알 수 없는 엔드포인트가 다시 프로파일링됨

가져오기에 사용되는 파일에 포함된 엔드포인트에 MAC 주소가 있으며 이러한 엔드포인트에 할당된 엔드포인트 프로파일링 정책이 알 수 없음 프로파일인 경우 해당 엔드포인트는 가져오기 중에 Cisco ISE에서 일치하는 엔드포인트 프로파일링 정책으로 즉시 다시 프로파일링됩니다. 그러나 알 수 없음 프로파일에 정적으로 할당되지는 않습니다. CSV 파일에서 엔드포인트 프로파일링 정책이 할당되어 있지 않은 엔드포인트는 알 수 없음 프로파일에 할당된 다음 일치하는 엔드포인트 프로파

일링 정책으로 다시 프로파일링됩니다. 다음 표에는 Cisco ISE가 가져오기 중에 Xerox_Device 프로파일과 일치하는 알 수 없음 프로파일을 다시 프로파일링하고 할당되지 않은 엔드포인트를 다시 프로파일링하는 방법이 나와 있습니다.

표 ***105:*** 알 수 없음 프로파일*:* 파일에서 가져오기

MAC 주소	**Cisco ISE**에서 가져오기 전에 할당된 엔드포인트 프로파일링 정책	**Cisco ISE**에서 가져오기 후에 할당되는 엔드포인트 프로파일링 정책
00:00:00:00:01:02	Unknown(알 수 없음)	Xerox-Device
00:00:00:00:01:03	Unknown(알 수 없음)	Xerox-Device
00:00:00:00:01:04	Unknown(알 수 없음)	Xerox-Device
00:00:00:00:01:05	프로파일이 할당되어 있지 않은 엔드포인트는 알 수 없음 프로파일로 할당되는 동시에 일치하는 프로파일로 다시 프로파일링됩니다.	Xerox-Device

잘못된 속성을 포함하는 엔드포인트를 가져올 수 없음

CSV 파일에 있는 엔드포인트 중 하나에 잘못된 속성이 있는 경우 엔드포인트를 가져올 수 없으며 오류 메시지가 표시됩니다.

예를 들어 가져오기에 사용하는 파일에서 엔드포인트가 잘못된 프로파일에 할당되어 있으면 Cisco ISE에 일치하는 프로파일이 없으므로 가져올 수 없습니다. CSV 파일에서 잘못된 프로파일에 할당된 엔드포인트가 가져오기되지 않는 방식은 아래 표를 참고해 주십시오.

표 ***106:*** 잘못된 프로파일*:* 파일에서 가져오기

MAC 주소	**Cisco ISE**에서 가져오기 전에 할당된 엔드포인트 프로파일링 정책	**Cisco ISE**에서 가져오기 후에 할당되는 엔드포인트 프로파일링 정책
00:00:00:00:01:02	Unknown(알 수 없음)	Xerox-Device
00:00:00:00:01:05	00:00:00:00:01:05 등의 엔드포인트가 Cisco ISE에서 사용 가능한 프로파일이 아닌 잘못된 프로파일에 할당되어 있으면 Cisco ISE에는 정책 이름이 잘못되었으며 엔드포인트를 가져오지 않는다는 경고 메시지가 표시됩니다.	Cisco ISE에 일치하는 프로파일이 없으므로 엔드포인트를 가져오지 않습니다.

LDAP 서버에서 엔드포인트 가져오기

LDAP 서버에서 엔드포인트의 MAC 주소, 연결된 프로파일 및 엔드포인트 ID 그룹을 안전하게 가져올 수 있습니다.

시작하기 전에

엔드포인트 가져오기를 시작하기 전에 LDAP 서버에 다음 항목을 설치했는지 확인합니다.

연결 설정 및 쿼리 설정을 구성해야 LDAP 서버에서 가져오기를 수행할 수 있습니다. Cisco ISE에서 연결 설정 또는 쿼리 설정이 잘못 구성되어 있으면 "LDAP 가져오기 실패:" 오류 메시지가 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트 > **Import(**가져오기**)** > **Import from LDAP(LDAP**에서 가져오기**)**를 선택합니다.

단계 **2** 연결 설정에 대한 값을 입력합니다.

단계 **3** 쿼리 설정에 대한 값을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

쉼표로 구분된 값을 사용하여 엔드포인트 내보내기

Cisco ISE 서버에서 선택한 엔드포인트 또는 모든 엔드포인트를 CSV 파일로 내보낼 수 있습니다. 이 파일에서는 엔드포인트와 약75개 속성이 해당 MAC 주소, 엔드포인트 프로파일링 정책 및 엔드포인트 ID 그룹과 함께 나열됩니다. Cisco ISE에서 생성된 사용자 맞춤화 속성도 CSV 파일로 내보내지며 다른 엔드포인트 속성과 구별할 수 있도록 "CUSTOM"이라는 접두사가 붙습니다.

참고 한 구축에서 다른 구축으로 내보낸 엔드포인트 사용자 맞춤화 속성을 가져오려면 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Endpoint Custom Attributes(**엔드포인트 사용자 맞춤화 속성**)** 창에서 동일한 사용자 맞춤화 속성을 생성하고 원래 구축에 지정된 것과 동일한 데이터 유형을 사용해야 합니다.

Export All(모두 내보내기**)**은 Cisco ISE의 모든 엔드 포인트를 내보내는 반면 **Export Selected(**선택 항목 내보내기**)**는 사용자가 선택한 엔드포인트만 내보냅니다. 기본적으로 profiler_endpoints.csv는 CSV 파일이고 CSV 파일을 여는 기본 애플리케이션은 Microsoft Office Excel입니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)**를 선택합니다.

단계 **2** **Export(**내보내기**)**를 클릭하고 다음 중 하나를 선택합니다.

- **Export Selected(**선택 항목 내보내기**)**: 엔드포인트 창에서 선택한 엔드포인트만 내보낼 수 있습니다.
- **Export All(**모두 내보내기**)**: 기본적으로 엔드포인트 창의 모든 프로파일링 엔드포인트를 내보낼 수 있습니다.

단계 **3** **OK(**확인**)**를 클릭하여 profiler_endpoints.csv 파일을 저장합니다.

식별된 엔드포인트

Cisco ISE는 네트워크에 연결하고 네트워크의 리소스를 사용하는 것으로 식별된 엔드포인트를 엔드포인트 페이지에 표시합니다. 엔드포인트는 일반적으로 유선/무선 네트워크 액세스 디바이스 및 VPN을 통해 네트워크에 연결되는 네트워크 지원 디바이스입니다. 엔드포인트는 개인용 컴퓨터, 랩탑, IP Phone, 스마트폰, 게임 콘솔, 프린터, 팩스 기기 등이 될 수 있습니다.

16진수 형식으로 표시되는 엔드포인트의 MAC 주소는 항상 고유한 엔드포인트 표시이지만, 다양한 속성 집합과 그에 연결된 값(속성-값 쌍이라고 함)으로 엔드포인트를 식별할 수 있습니다. 엔드포인트 기능, 네트워크 액세스 디바이스의 기능과 컨피그레이션, 그리고 이러한 속성을 수집하는 데 사용하는 방법(프로브)에 따라 엔드포인트에 대한 다양한 속성 집합을 수집할 수 있습니다.

동적으로 프로파일링된 엔드포인트

네트워크에서 검색된 엔드포인트는 구성된 프로파일링 엔드포인트 프로파일링 정책을 기준으로 동적으로 프로파일링될 수 있으며, 해당 프로파일에 따라 일치하는 엔드포인트 ID 그룹에 할당될 수 있습니다.

정적으로 프로파일링된 엔드포인트

MAC 주소를 사용하여 엔드포인트를 생성하고 Cisco ISE에서 엔드포인트 ID 그룹과 함께 프로파일을 연결하면 엔드포인트를 정적으로 프로파일링할 수 있습니다. Cisco ISE는 정적으로 할당된 엔드포인트에 대해 프로파일링 정책 및 ID 그룹을 다시 할당하지 않습니다.

알 수 없는 엔드포인트

엔드포인트에 대해 일치하는 프로파일링 정책이 없으면 알 수 없는 프로파일링 정책(알 수 없음)을 할당할 수 있으며 엔드포인트는 그에 따라 알 수 없음으로 프로파일링됩니다. 알 수 없음 엔드포인트 정책으로 프로파일링된 엔드포인트의 경우 해당 엔드포인트에 대해 수집된 속성 또는 속성 집합을 사용하여 프로파일을 생성해야 합니다. 프로파일과 일치하지 않는 엔드포인트는 알 수 없음 엔드포인트 ID 그룹 내에서 그룹화됩니다.

정책 서비스 노드 데이터베이스에 로컬로 저장되는 식별된 엔드포인트

Cisco ISE는 식별된 엔드포인트를 정책 서비스 노드 데이터베이스에 로컬로 씁니다. 데이터베이스에 로컬로 저장된 이러한 엔드포인트는 엔드포인트에서 중요한 속성이 변경되는 경우에만 관리 노드 데이터베이스에서 사용할 수 있으며(원격 쓰기) 다른 정책 서비스 노드 데이터베이스로 복제됩니다.

중요한 속성은 다음과 같습니다.

- ip
- EndPointPolicy

- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

Cisco ISE에서 엔드포인트 프로파일정의를 변경할 때는 모든 엔드포인트를 다시 프로파일링해야 합니다. 엔드포인트의 속성을 수집하는 정책 서비스 노드가 해당 엔드포인트를 다시 프로파일링합니다.

다른 정책 서비스 노드에서 속성이 처음 수집된 엔드포인트에 대해 정책 서비스 노드가 속성 수집을 시작하면 엔드포인트 소유권이 현재 서비스 노드로 변경됩니다. 새 정책 서비스 노드는 이전 정책 서비스 노드에서 최신 속성을 검색하며, 수집한 속성을 이미 수집된 속성에 따라 조정합니다.

엔드포인트에서 중요한 속성이 변경되면 해당 엔드포인트의 속성이 관리 노드 데이터베이스에 자동으로 저장되므로 엔드포인트에 최신 중요 변경사항이 적용됩니다. 엔드포인트를 소유하는 정책 서비스 노드를 사용할 수 없는 경우에는 소유자가 없어진 엔드포인트를 관리자 ISE 노드가 다시 프로파일링하며, 해당 엔드포인트에 대해 새 정책 서비스 노드를 구성해야 합니다.

클러스터의 정책 서비스 노드

Cisco ISE는 정책 서비스 노드 그룹을 클러스터로 사용합니다. 이를 통해 클러스터에서 둘 이상의 노드가 동일 엔드포인트에 대한 속성을 수집할 때 엔드포인트 속성을 교환할 수 있습니다. 로드 밸런서 뒤에 있는 모든 정책 서비스 노드에 대해 클러스터를 생성하는 것이 좋습니다.

현재 소유자와 다른 노드가 동일 엔드포인트에 대한 속성을 수신하는 경우, 해당 노드는 속성을 병합하고 소유권을 변경해야 하는지를 확인하기 위해 현재 소유자로부터 최신 속성을 요청하는 메시지를 클러스터를 통해 전송합니다. Cisco ISE에서 노드 그룹을 정의하지 않은 경우에는 모든 노드가 하나의 클러스터 내에 있다고 가정합니다.

Cisco ISE에서 수행되는 엔드포인트 생성 및 복제는 변경되지 않습니다. 즉, 정적 속성과 동적 속성에서 구축되는 프로파일링에 사용되는 속성의 허용 목록을 기준으로 엔드포인트에 대한 소유권 변경 여부만 결정합니다.

후속 속성 수집 시 다음 속성이 변경되면 관리 노드에서 엔드포인트가 업데이트됩니다.

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment

- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

엔드포인트를 편집하여 관리 노드에 저장하면 엔드포인트의 현재 소유자에서 속성을 검색합니다.

엔드포인트 ID 그룹 생성

Cisco ISE는 검색되는 엔드포인트를 해당하는 엔드포인트 ID 그룹으로 그룹화합니다. Cisco ISE에서는 몇 가지 시스템 정의 엔드포인트 ID 그룹이 제공됩니다. 엔드포인트 **ID** 그룹 창에서 엔드포인트 ID 그룹을 추가로 생성할 수도 있습니다. 직접 생성한 엔드포인트 ID 그룹은 편집하거나 삭제할 수 있습니다. 시스템 정의 엔드포인트 ID 그룹의 경우 설명만 편집할 수 있습니다. 그 이름은 편집하거나 삭제할 수 없습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Endpoint Identity Groups(**엔드포인트 **ID** 그룹**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 생성할 엔드포인트 ID 그룹의 **Name(**이름**)**을 입력합니다(엔드포인트 ID 그룹의 이름에 공백 제외).

단계 **4** 생성할 엔드포인트 ID 그룹에 대한 **Description(**설명**)**을 입력합니다.

단계 **5** **Parent Group(**부모 그룹**)** 드롭다운 목록을 클릭하여 새로 생성한 엔드포인트 ID 그룹을 연결할 엔드포인트 ID 그룹을 선택합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

엔드포인트 ID 그룹에서 그룹화되어 식별된 엔드포인트

Cisco ISE는 엔드포인트 프로파일링 정책에 따라 검색된 엔드포인트를 해당하는 엔드포인트 ID 그룹으로 그룹화합니다. 프로파일링 정책은 계층적이며 Cisco ISE의 엔드포인트 식별 그룹 수준에서 적용됩니다. 엔드포인트를 엔드포인트 ID 그룹으로 그룹화하고 프로파일링 정책을 엔드포인트 ID 그룹에 적용하면, 해당 엔드포인트 프로파일링 정책을 검사하여 Cisco ISE에서 엔드포인트와 엔드포인트 프로파일의 매핑을 확인할 수 있습니다.

Cisco ISE는 기본적으로 일련의 엔드포인트 ID 그룹을 생성하며, 관리자는 엔드포인트가 동적으로 또는 정적으로 할당될 수 있는 고유한 ID 그룹을 생성할 수 있습니다. 엔드포인트 ID 그룹을 생성하고 ID 그룹을 시스템에서 생성된 ID 그룹 중 하나와 연결할 수 있습니다. 또한 생성한 엔드포인트를

시스템에 존재하는 ID 그룹 중 하나에 정적으로 할당할 수 있으며, 프로파일링 서비스는 ID 그룹을 다시 할당할 수 없습니다.

엔드포인트에 대해 생성된 기본 엔드포인트 ID 그룹

Cisco ISE에서는 다음과 같은 엔드포인트 ID 그룹을 생성합니다.

- Blocked List: 이 엔드포인트 ID 그룹에는 Cisco ISE의 이 그룹에 정적으로 할당된 엔드포인트 및 디바이스 등록 포털에서 차단된 엔드포인트가 포함됩니다. Cisco ISE에서 이 그룹의 엔드포인트에 대한 네트워크 액세스를 허용하거나 거부하도록 권한 부여 프로파일을 정의할 수 있습니다.
- GuestEndpoints: 이 엔드포인트 ID 그룹에는 게스트 사용자가 사용하는 엔드포인트가 포함됩니다.
- Profiled: 이 엔드포인트 ID 그룹에는 Cisco IP 전화기 및 Cisco ISE의 워크스테이션을 제외하고 엔드포인트 프로파일링 정책과 일치하는 엔드포인트가 포함됩니다.
- RegisteredDevices: 이 엔드포인트 ID 그룹에는 직원이 디바이스 등록 포털을 통해 추가한 등록된 디바이스에 해당하는 엔드포인트가 포함됩니다. 프로파일링 서비스는 이 그룹에 할당된 디바이스를 정상적으로 프로파일링합니다. 엔드포인트는 Cisco ISE의 이 그룹에 정적으로 할당되며, 프로파일링 서비스는 해당 엔드포인트를 다른 ID 그룹에 다시 할당할 수 없습니다. 이러한 디바이스는 다른 엔드포인트와 마찬가지로 엔드포인트 목록에 표시됩니다. 디바이스 등록 포털을 통해 Cisco ISE의 Endpoints(엔드포인트) 창에 있는 엔드포인트 목록에서 추가한 디바이스는 편집, 삭제 및 차단할 수 있습니다. 디바이스 등록 포털에서 차단된 디바이스는 Blocked List 엔드포인트 ID 그룹에 할당되고, Cisco ISE에 있는 권한 부여 프로파일은 차단된 디바이스를 "Unauthorised Network Access(무단 네트워크 액세스)"라고 표시된 URL로 리디렉션합니다. 이는 차단된 디바이스에 대한 기본 포털 페이지입니다.
- Unknown: 이 엔드포인트 ID 그룹에는 Cisco ISE의 프로파일과 일치하지 않는 엔드포인트가 포함됩니다.

시스템에서 생성된 위의 엔드포인트 ID 그룹 외에 Cisco ISE에서는 프로파일링된(부모) ID 그룹에 연결되는 다음 엔드포인트 ID 그룹도 생성합니다. 부모 그룹이란 시스템에 있는 기본 ID 그룹을 의미합니다.

- Cisco-IP-Phone: 네트워크에서 프로파일링된 모든 Cisco IP 전화기가 포함된 ID 그룹입니다.
- Workstation: 네트워크에서 프로파일링된 모든 워크스테이션이 포함된 ID 그룹입니다.

일치하는 엔드포인트 프로파일링 정책에 대해 생성된 엔드포인트 ID 그룹

기존 정책과 일치하는 엔드포인트 정책이 있는 경우 프로파일링 서비스는 일치하는 엔드포인트 ID 그룹을 생성할 수 있습니다. 이 ID 그룹은 프로파일링된 엔드포인트 ID 그룹의 하위 그룹이 됩니다. 엔드포인트 정책을 생성할 때 프로파일링 정책 페이지에서 Create Matching Identity Group(일치하는 ID 그룹 생성) 확인란을 선택하여 일치하는 엔드포인트 ID 그룹을 생성할 수 있습니다. 프로파일 매핑을 제거하지 않는 한 일치하는 ID 그룹은 삭제할 수 없습니다.

엔드포인트 ID 그룹에서 정적 엔드포인트 추가

엔드포인트 ID 그룹에서 엔드포인트를 추가하거나 정적으로 추가된 엔드포인트를 제거할 수 있습니다.

엔드포인트 위젯의 엔드포인트는 특정 ID 그룹에만 추가할 수 있습니다. 특정 엔드포인트 ID 그룹에 추가하는 엔드포인트는 이전에 동적으로 그룹화되었던 엔드포인트 ID 그룹에서 이동됩니다.

엔드포인트를 최근 추가했던 엔드포인트 ID 그룹에서 제거하는 경우 해당하는 ID 그룹으로 다시 프로파일링됩니다. 엔드포인트는 시스템에서 삭제되지는 않으며 엔드포인트 ID 그룹에서만 제거됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Endpoint Identity Groups(**엔드포인트 **ID** 그룹**)**를 선택합니다.

단계 **2** 엔드포인트 ID 그룹을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** 엔드포인트 위젯에서 엔드포인트를 선택하여 엔드포인트 ID 그룹에 추가합니다.

단계 **5** 엔드포인트 ID 그룹 페이지로 돌아가려면 **Endpoint Group List(**엔드포인트 그룹 목록**)** 링크를 클릭합니다.

ID 그룹에서 추가 또는 제거된 후에 다시 프로파일링되는 동적 엔드포인트

엔드포인트 ID 그룹 할당이 정적이 아닌 경우 엔드포인트 ID 그룹에서 추가하거나 제거한 엔드포인트는 다시 프로파일링됩니다. ISE 프로파일러에서 동적으로 식별되는 엔드포인트는 적절한 엔드포인트 ID 그룹에 표시됩니다. 엔드포인트 ID 그룹에서 동적으로 추가된 엔드포인트를 제거하면 Cisco ISE에서 엔드포인트를 ID 그룹에서 성공적으로 제거했지만 엔드포인트 ID 그룹에서 다시 프로파일링된다는 메시지가 표시됩니다.

권한 부여 규칙에 사용되는 엔드포인트 ID 그룹

권한 부여 정책에서 엔드포인트 ID 그룹을 효율적으로 사용하면 검색된 엔드포인트에 대해 적절한 네트워크 액세스 권한을 제공할 수 있습니다. 예를 들어 모든 유형의 Cisco IP Phone에 대한 권한 부여 규칙은 기본적으로 Cisco ISE의 **Policy(**정책**)** > **Policy Sets(**정책 집합**)** > **Default(**기본값**)** > **Authorization Policy(**권한 부여 정책**)** 위치에서 사용 가능합니다.

엔드포인트 프로파일링 정책이 독립형 정책(다른 엔드포인트 프로파일링 정책의 부모 정책이 아님)인지 아니면 엔드포인트 프로파일링 정책의 부모 정책이 비활성화되어 있지 않은지를 확인해야 합니다.

Anycast 및 프로파일러 서비스

Anycast는 동일한 IP 주소가 둘 이상의 호스트에 할당되고 라우팅을 통해 데이터 수신에 가장 적합한 대상을 결정할 수 있는 네트워킹 기술입니다. 프로파일링 데이터(RADIUS, DHCP 릴레이, SNMP 트랩, NetFlow)에 대한 단일 대상을 제공하기 위한 로드 밸런서 활용 사례와 유사하게, Anycast에서는 여러 대상에 동일한 데이터를 전송하지 않도록 소스에 단일 IP 대상을 구성할 수 있습니다.

Anycast IP 주소는 데이터 센터 간의 리던던시(redundancy)를 지원하기 위해 실제 PSN 인터페이스 IP 주소 또는로드 밸런서 가상 IP 주소에 할당할 수 있습니다. Anycast IP 주소를 ISE 기가비트 이더넷 0 관리 인터페이스에 할당해서는 안됩니다.

Anycast에 사용되는 인터페이스는 프로파일러 프로브에서 사용하는 전용 인터페이스여야 합니다. Anycast IP 주소가 로드 밸런서 가상 IP 주소에 할당된 경우 동일한 요구 사항이 적용되지 않습니다.

Anycast를 사용할 때는 노드 장애를 자동으로 탐지하고 장애가 발생한 노드에 대한 해당 경로를 라우팅 표에서 제거해야 합니다. Anycast 대상이 링크 또는 VLAN의 유일한 호스트인 경우 장애가 발생하면 경로가 자동으로 제거될 수 있습니다.

IP Anycast를 구축할 때는 각 대상에 대한 경로 메트릭이 큰 가중치 또는 바이어스를 갖도록 해야 합니다. Anycast 대상에 대한 경로가 플랩되거나 ECMP(Equal-Cost Multi-Path Routing) 시나리오가 발생하는 경우, 지정된 서비스(RADIUS AAA, DHCP 또는 SNMP 트랩 프로파일링, HTTPS 포털)에 대한 트래픽이 각 대상에 분산되어 과도한 트래픽 및 서비스 장애(RADIUS AAA 및 HTTPS 포털)가 발생하거나 프로파일링 및 데이터베이스 복제(프로파일링 서비스)가 최적화되지 않을 수 있습니다.

IP Anycast의 주요 이점은 액세스 디바이스, 프로파일 데이터 소스 및 DNS의 구성을 크게 간소화한다는 것입니다. 또한 지정된 엔드포인트의 데이터가 단일 PSN으로만 전송되도록 하여 ISE 프로파일링을 최적화할 수 있습니다. 추가 경로 구성을 신중하게 계획하고 적절한 모니터링을 통해 관리해야 합니다. 그러나 고유한 서브 네트워크 및 IP 주소가 사용되지 않으므로 문제 해결이 어려울 수 있습니다.

프로파일러 피드 서비스

프로파일러 조건, 예외 작업 및 NMAP 스캔 작업은 Cisco 제공 항목 또는 관리자 생성 항목으로 분류됩니다(시스템 유형 속성 참고). 또한 엔드포인트 프로파일링 정책은 Cisco 제공, 관리자 생성 또는 관리자 수정 정책으로 분류됩니다. 이러한 분류는 System Type(시스템 유형) 속성에 표시됩니다.

시스템 유형 속성에 따라 프로파일러 조건, 예외 작업, NMAP 스캔 작업 및 엔드포인트 프로파일링 정책에 대해 각기 다른 작업을 수행할 수 있습니다. Cisco 제공 조건, 예외 작업 및 NMAP 스캔 작업은 편집하거나 삭제할 수 없습니다. Cisco에서 제공하는 엔드포인트 정책은 삭제할 수 없습니다. 정책을 편집할 경우 이를 관리자 수정이라고 합니다. 피드 서비스가 정책을 업데이트하면 관리자 수정 정책이 해당 정책 기반으로 하는 최신 버전의 Cisco 제공 정책으로 대체됩니다.

Cisco 피드 서버에서 신규 및 업데이트된 엔드포인트 프로파일링 정책과 MAC OUI 데이터베이스 업데이트를 검색할 수 있습니다. Cisco ISE를 구독하고 있어야 합니다. 적용된, 성공 및 실패 메시지에 대한 이메일 알림을 받을 수도 있습니다. 피드 서비스 작업에 대한 익명 정보를 Cisco에 다시 보낼 수 있습니다. 그러면 Cisco가 피드 서비스를 개선하는 데 도움이 됩니다.

OUI 데이터베이스에는 벤더에게 할당된 MAC OUI가 포함되어 있습니다. OUI 목록은 여기에서 확인할 수 있습니다. http://standards.ieee.org/develop/regauth/oui/oui.txt

Cisco ISE는 정책 및 OUI 데이터베이스 업데이트를 현지 Cisco ISE 서버 표준 시간대를 기준으로 매일 오전 1시에 다운로드합니다. Cisco ISE는 이 다운로드된 피드 서버 정책을 자동으로 적용하며 이러한 변경 사항을 이전 상태로 되돌릴 수 있도록 변경 사항 집합을 저장합니다. 마지막으로 적용한 변경 사항을 되돌리면 새로 추가된 엔드포인트 프로파일링 정책이 제거되고 업데이트된 엔드포인트 프로파일링 정책도 이전 상태로 되돌려집니다. 또한 프로파일러 피드 서비스는 자동으로 비활성화됩니다.

오프라인 모드에서 피드 서비스를 수동으로 업데이트할 수도 있습니다. ISE 구축을 Cisco 피드 서비스에 연결할 수 없는 경우에는 이 옵션을 사용하여 업데이트를 수동으로 다운로드할 수 있습니다.

참고 라이선스가 60일 기간 내에 45일 동안 컴플라이언스를 벗어나면(OOC) 피드 서비스에서 업데이트를 수행할 수 없습니다. 라이선스가 만료되었거나 사용량이 허용되는 세션 수를 초과하면 라이선스가 컴플라이언스 상태가 아닙니다.

프로파일러 피드 서비스 구성

프로파일러 피드 서비스는 Cisco 피드 서버에서 신규 및 업데이트된 엔드포인트 프로파일링 정책과 MAC OUI 데이터베이스 업데이트를 검색합니다. 피드 서비스를 사용할 수 없거나 기타 오류가 발생한 경우에는 운영 감사 보고서에 해당 내용이 보고됩니다.

피드 서비스 사용 보고서를 Cisco로 다시 보내도록 Cisco ISE를 구성할 수 있습니다. 그러면 다음 정보가 Cisco로 전송됩니다.

- Hostname: Cisco ISE 호스트 이름
- MaxCount: 총 엔드포인트 수
- ProfiledCount: 프로파일이 지정된 엔드포인트 수
- UnknownCount: 알 수 없는 엔드포인트 수
- MatchSystemProfilesCount: Cisco에서 제공한 프로파일 수
- UserCreatedProfiles: 사용자가 생성한 프로파일 수

Cisco에서 제공한 프로파일링 정책에서 CoA 유형을 변경할 수 있습니다. 피드 서비스가 해당 정책을 업데이트할 때 CoA 유형은 변경되지 않지만 해당 정책의 나머지 속성은 업데이트됩니다.

Cisco ISE 릴리스 2.7 이상에서는 정책 업데이트를 다운로드하지 않고 OUI 업데이트를 수동으로 다운로드할 수 있습니다. 일부 프로파일러 조건을 CoA 유형 이상으로 변경하도록 맞춤 설정한 경우 프로파일러 피드가 이러한 조건을 대체하지 않도록 할 수 있습니다. OUI 업데이트를 계속 원할 수 있으므로 제조업체가 디바이스를 추가할 때 프로파일러가 새 디바이스를 식별할 수 있습니다. OUI만 다운로드하는 옵션은 피드 서비스 포털에서 사용할 수 있습니다.

시작하기 전에

프로파일러 피드 서비스는 분산형 구축이나 독립형 ISE 모드에서만 Cisco ISE 관리 포털에서 구성할 수 있습니다.

관리 포털(**Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)**)에서 피드 업데이트에 대한 이메일 알림을 보내려는 경우 SMTP(Simple Mail Transfer Protocol) 서버를 설정합니다.

온라인에서 피드 서비스를 업데이트하려면 다음을 수행합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificate(**신뢰할 수 있는 인증서**)** > **Import(**가져오기**)**를 선택합니다.

단계 **2** Work Centers Profiler Feeds (작업 센터 프로파일 러 피드)를 선택합니다. > > Administration FeedService Profiler (관리 FeedService 프로파일 러) 페이지의 옵션에 액세스 할 수도 있습니다. > >

단계 **3** **Online Subscription Update(**온라인 구독 업데이트**)** 탭을 클릭합니다.

단계 **4** **Test Feed Service Connection(**피드 서비스 연결 테스트**)** 버튼을 클릭하여 Cisco 피드 서비스에 연결되어 있으며 인증서가 유효한지 확인합니다.

단계 **5** **Enable Online Subscription Update(**온라인 구독 업데이트 활성화**)** 확인란을 선택합니다.

단계 **6** 시간을 HH:MM 형식(Cisco ISE 서버의 현지 표준 시간대)으로 입력합니다. 기본적으로 Cisco ISE 피드 서비스는 매일 오전 1시에 실행되도록 예약됩니다.

단계 **7** **Notify administrator when download occurs(**다운로드 수행 시 관리자에게 알림**)** 확인란을 선택하고 **Administrator email address(**관리자 이메일 주소**)** 텍스트 상자에 이메일 주소를 입력합니다. 민감하지 않은 정보(향후 릴리스에서 보다 나은 서비스와 추가적인 기능을 제공하는 데 사용할 예정)를 Cisco ISE가 수집하도록 허용하려면 **Provide Cisco anonymous information to help improve profiling accuracy(**프로파일링 정확도 개선을 위한 익명 정보를 **Cisco**에 제공**)** 확인란을 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

단계 **9** **Update Now(**지금 업데이트**)**를 클릭합니다.

Cisco 피드 서버에 연결하여 마지막 피드 서비스 업데이트 이후 생성된 신규 및 업데이트된 프로파일이 있는지 확인하도록 Cisco ISE에 명령합니다. 그러면 시스템의 모든 엔드포인트가 다시 프로파일링되므로 시스템의 로드가 증가할 수 있습니다. 엔드포인트 프로파일링 정책이 업데이트되면 현재 Cisco ISE에 연결되어 있는 일부 엔드포인트의 권한 부여 정책이 변경될 수 있습니다.

마지막 피드 서비스 이후 생성되었으며 다운로드가 완료된 후에 활성화된 신규 및 업데이트된 프로파일을 업데이트할 때는 **Update Now(**지금 업데이트**)** 버튼이 비활성화됩니다. 프로파일러 피드 서비스의 컨피그레이션 창에서 이 창으로 돌아와야 합니다.

관련 항목

오프라인에서 프로파일러 피드 서비스 구성, 760 페이지

오프라인에서 프로파일러 피드 서비스 구성

Cisco ISE가 Cisco 피드 서버에 직접 연결할 수 없을 때는 오프라인으로 피드 서비스를 업데이트할 수 있습니다. Cisco 피드 서버에서 오프라인 업데이트 패키지를 다운로드하고 오프라인 피드 업데이트

를 사용하여 Cisco ISE에 업로드 할 수 있습니다. 또한 피드 서버에 추가된 새 정책에 대한 이메일 알림을 설정할 수도 있습니다.

오프라인으로 프로파일러 피드 서비스를 구성하려면 다음 작업을 수행합니다.

1. 오프라인 업데이트 패키지 다운로드
2. 오프라인 피드 업데이트 적용

오프라인 업데이트 패키지 다운로드

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Feeds(**피드**)**를 선택합니다.
Administration(관리**)** > **FeedService(**피드 서비스**)** > **Profiler(**프로파일러**)** 페이지에서 옵션에 액세스할 수도 있습니다.

단계 **2** **Offline Manual Update(**오프라인 수동 업데이트**)** 탭을 클릭합니다.

단계 **3** **Download Updated Profile Policies(**업데이트된 프로파일 정책 다운로드**)** 링크를 클릭합니다. 피드 서비스 파트너 포털로 리디렉션 됩니다.
브라우저에서 https://ise.cisco.com/partner/로 이동하여 피드 서비스 파트너 포털에 직접 방문할 수도 있습니다.

단계 **4** 처음 사용하는 경우 약관에 동의하십시오.
피드 서비스 관리자가 요청을 승인할 수 있도록 이메일이 트리거됩니다. 승인 시 확인 이메일이 전송됩니다.

단계 **5** Cisco.com 자격 증명을 사용하여 파트너 포털에 로그인합니다.

단계 **6** **Offline Feed(**오프라인 피드**) > Download Package(**패키지 다운로드**)**를 선택합니다.

단계 **7** **Generate Package(**패키지 생성**)**를 클릭합니다.

단계 **8** 생성된 패키지에 포함된 모든 프로파일 및 OUI를 보려면 **Click to View the Offline Update Package contents(**오프라인 업데이트 패키지 콘텐츠를 보려면 클릭**)** 링크를 클릭합니다.

- 피드 프로파일러 1 및 피드 OUI의 정책은 Cisco ISE의 모든 버전에 다운로드됩니다.
- 피드 프로파일러 2의 정책은 Cisco ISE 릴리스 1.3 이상에만 다운로드됩니다.
- 피드 프로파일러 3의 정책은 Cisco ISE 릴리스 2.1 이상에만 다운로드됩니다.

단계 **9** **Download Package(**패키지 다운로드**)**를 클릭하고 파일을 로컬 시스템에 저장합니다.
저장된 파일을 Cisco ISE 서버에 업로드하여 다운로드한 패키지에 피드 업데이트를 적용할 수 있습니다.

오프라인 피드 업데이트 적용

시작하기 전에

피드 업데이트를 적용하기 전에 오프라인 업데이트 패키지를 다운로드해야 합니다.

단계 **1** **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Feeds(**피드**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

Administration(관리) > **FeedService(피드 서비스)** > **Profiler(프로파일러)**창에서 옵션에 액세스할 수도 있습니다.

단계 **2** **Offline Manual Update(오프라인 수동 업데이트)** 탭을 클릭합니다.

단계 **3** **Browse(찾아보기)**를 클릭하고 다운로드한 프로파일러 피드 패키지를 선택합니다.

단계 **4** **Apply Update(업데이트 적용)** 탭을 클릭합니다.

프로파일 및 OUI 업데이트를 위한 이메일 알림 구성

프로파일 및 OUI 업데이트에 대한 알림을 수신하도록 이메일 주소를 구성할 수 있습니다.

단계 **1** **Download Offline Update Package(오프라인 업데이트 패키지 다운로드)** 섹션의 **1** ~ 오프라인 업데이트 패키지 다운로드를 수행하여 피드 서비스 파트너 포털로 이동합니다.

단계 **2** **Offline Feed(오프라인 피드)** > **Email Preferences(이메일 환경 설정)**를 선택합니다.

단계 **3** 공지사항을 받으려면 **Enable Notifications(공지사항 사용)** 확인란을 선택합니다.

단계 **4** **days(일 수)** 드롭 다운 목록에서 일 수를 선택하여 새 업데이트에 대한 알림을 받을 빈도를 설정합니다.

단계 **5** 이메일 주소/우편 주소를 입력하고 **Save(저장)**를 클릭합니다.

피드 업데이트 취소

이전 업데이트에서 업그레이드된 엔드포인트 프로파일링 정책을 되돌리고 이전 Profiler Feed Service 업데이트를 통해 새로 추가된 OUI와 엔드포인트 프로파일링 정책을 제거할 수 있습니다. .

엔드포인트 프로파일링 정책은 피드 서버에서 업데이트한 후 수정해도 시스템에서 변경되지 않습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(작업 센터)** > **Profiler(프로파일러)** > **Feeds(피드)**를 선택합니다.

단계 **2** **Go to Update Report Page(보고서 업데이트 페이지로 이동)**를 클릭하여 컨피그레이션 변경 감사 보고서에서 수행한 컨피그레이션 변경사항을 확인합니다.

단계 **3** **Undo Latest(최신 항목 취소)**를 클릭합니다.

프로파일러 보고서

Cisco ISE는 네트워크를 관리하는 데 사용할 수 있는 문제 해결 도구와 다양한 엔드포인트 프로파일링 관련 보고서를 제공합니다. 기록 데이터와 현재 데이터 둘 다에 대해 보고서를 생성할 수 있습니다. 보고서의 특정 부분을 드릴다운하여 추가 세부정보를 확인할 수도 있습니다. 큰 보고서의 경우에는 보고서를 예약하여 다양한 형식으로 다운로드할 수도 있습니다.

Operations(운영**) > Reports(**보고서**) > Endpoints and Users(**엔드포인트 및 사용자**)**에서 엔드포인트에 대한 다음 보고서를 실행할 수 있습니다.

- Endpoint Session History(엔드포인트 세션 기록)
- Profiled Endpoint Summary(프로파일링된 엔드포인트 요약)
- Endpoint Profile Changes(엔드포인트 프로파일 변경)
- Top Authorizations by Endpoint(엔드포인트별 상위 권한 부여)
- Registered Endpoints(등록된 엔드포인트)

엔드포인트의 비정상적인 동작 탐지

Cisco ISE는 MAC 주소의 불법 사용으로부터 네트워크를 보호합니다. Cisco ISE는 MAC 주소 스푸핑과 관련된 엔드포인트를 탐지하고 의심스러운 엔드포인트의 권한을 제한할 수 있습니다.

다음은 비정상적 동작에 대한 프로파일러 컨피그레이션 페이지의 두 가지 옵션입니다.

- 비정상적인 동작 탐지 활성화
- 비정상적인 동작 적용 활성화

비정상적인 동작 탐지를 활성화하는 경우 Cisco ISE는 데이터를 검사하고 NAS-Port-Type, DHCP 클래스 식별자 및 엔드포인트 정책과 관련된 속성의 변경 사항과 관련하여 기존 데이터와의 모순을 확인합니다. 그러한 경우 **AnomalousBehavior**라는 속성이 true로 설정된 엔드포인트에 추가되어 Visibility Context(가시성 상황) 페이지에서 엔드포인트를 필터링하고 볼 수 있습니다. 각 MAC 주소에 대한 감사 로그도 생성됩니다.

비정상적 동작 탐지가 활성화되면 Cisco ISE는 기존 엔드포인트의 다음 속성이 변경되었는지 확인합니다.

1. Port-Type(포트 유형)-엔드포인트의 액세스 방법이 변경되었는지 확인합니다. 이는 유선 Dot1x를 통해 연결된 동일한 MAC 주소가 무선 Dot1x에 사용된 경우 그리고 그 반대의 경우에만 적용됩니다.
2. DHCP Class Identifier(DHCP 클래스 식별자)-엔드포인트의 클라이언트 또는 벤더 유형이 변경되었는지 확인합니다. 이는 DHCP 클래스 식별자 속성이 특정 값으로 채워져 다른 값으로 변경된 경우에만 적용됩니다. 엔드포인트가 고정 IP로 구성된 경우 Cisco ISE에서 DHCP 클래스 식별자 속성이 비어 있습니다. 나중에 다른 디바이스가 이 엔드포인트의 MAC 주소를 스푸핑하고 DHCP를 사용하는 경우 클래스 식별자가 빈 값에서 특정 문자열로 변경됩니다. 이렇게 하면 비정상적 동작 탐지가 트리거되지 않습니다.
3. 엔드포인트 정책-중요한 프로파일 변경 사항이 있는지 확인합니다. 이는 엔드포인트의 프로파일이 "Phone(폰)" 또는 "Printer(프린터)"에서 "Workstation(워크 스테이션)"으로 변경된 경우에만 적용됩니다.

Anomalous Behavior Enforcement(비정상 동작 적용)를 활성화하는 경우 프로파일러 컨피그레이션 창에 구성된 권한 부여 규칙에 따라 의심스러운 엔드포인트를 다시 인증하는 데 사용할 수 있는 비정상 동작을 탐지하면 CoA가 실행됩니다.

비정상적인 동작이 있는 엔드포인트에 대한 권한 부여 정책 규칙 설정

Authorization Policy(권한 부여 정책) 페이지에서 해당 규칙을 설정하여 비정상적인 동작이 있는 엔드포인트에 대해 수행할 조치를 선택할 수 있습니다.

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

단계 **2** 기본 정책에 해당하는 **View(**보기**)** 열에서 화살표 아이콘 을 클릭하여 보기 설정 화면을 열고 기본 권한 부여 정책을 보고 관리합니다.

단계 **3** 행의 **Actions(**작업**)** 열에서 톱니바퀴 아이콘을 클릭한 다음 드롭 다운 목록에서 필요에 따라 삽입 또는 복제 옵션을 선택하여 새 권한 부여 규칙을 삽입합니다.
정책 집합 표에 새 행이 표시됩니다.

단계 **4** Rule Name(규칙 이름)을 입력합니다.

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

단계 **6** **Conditions Studio** 페이지에 필수 조건을 생성합니다. **Editor(**편집기**)** 섹션에서 **Click To Add an Attribute(**속성 추가 클릭**)** 텍스트 상자를 클릭하고 필요한 사전 및 속성(예: Endpoints.AnomalousBehaviorEqualsTrue)을 선택합니다.

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

단계 **7** **Use(**사용**)**를 클릭하여 비정상적인 동작이 있는 엔드포인트에 대한 권한 부여 정책 규칙 설정합니다.

단계 **8** **Done(**완료**)**을 클릭합니다.

비정상적인 동작이 있는 엔드포인트 보기

다음 옵션 중 하나를 사용하여 비정상적인 동작이 있는 엔드포인트를 볼 수 있습니다.

- **Home(**홈**)** > **Summary(**요약**)** > **Metrics(**메트릭**)**에서 Anomalous Behavior(비정상적인 동작)를 클릭합니다. 이 작업을 수행하면 창의 하단 패널에 Anomalous Behavior(비정상적인 동작) 열이 포함 된 새 탭이 열립니다.
- **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Endpoint Classification(**엔드포인트 분류**)**을 선택합니다. 창의 하단 패널에서 Anomalous Behavior(비정상적인 동작) 열을 볼 수 있습니다.
- 다음 단계에 설명된 대로 Context Visibility(상황 가시성) 창의 Authentication(인증) 보기 또는 Compromised Endpoints(침해 엔드포인트) 보기에서 Anomalous Behavior(비정상적인 동작) 열을 새로 생성할 수 있습니다.

단계 **1** **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Authentication(**인증**)** 또는 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Compromised Endpoints(**침해 엔드포인트**)**를 선택합니다.

단계 **2** 창의 하단 패널에서 설정 아이콘을 클릭하고 **Anomalous Behavior(**비정상적인 동작**)** 확인란을 선택합니다.

단계 **3** **Go(**이동**)**를 클릭합니다.
Authentication(인증) 보기 또는 Compromised Endpoints(침해 엔드포인트) 보기에서 Anomalous Behavior(비정상적인 동작) 열을 볼 수 있습니다.

클라이언트 머신의 에이전트 다운로드 문제

문제

사용자 인증 및 권한 부여 후 클라이언트 머신 브라우저에 "일치하는 정책 없음" 오류 메시지가 표시됩니다. 이 문제는 인증의 클라이언트 프로비저닝 단계 중에 사용자 세션에 적용됩니다.

가능한 원인

클라이언트 프로비저닝 정책에 필요한 설정이 없습니다.

포스처 에이전트 다운로드 문제

포스처 에이전트 설치 프로그램을 다운로드하기 위해 필요한 사항은 다음과 같습니다.

- 사용자는 에이전트를 처음 클라이언트 머신에 설치할 때 브라우저 세션에서 ActiveX 설치 프로그램을 허용해야 합니다. 클라이언트 프로비저닝 다운로드 페이지에서 이에 대한 메시지가 표시됩니다.
- 클라이언트 머신에서 인터넷에 액세스할 수 있어야 합니다.

해결 방법

- 클라이언트 프로비저닝 정책이 Cisco ISE에 있는지 확인해 주십시오. 있는 경우 정책 ID 그룹, 조건 및 정책에 정의된 에이전트 유형을 확인합니다. (또한 프로파일에 모두 기본값이 적용되어 있더라도 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)Add(**추가**)AnyConnect Posture Profile(AnyConnect** 포스처 프로파일**)**에 에어전트 프로파일이 구성되어 있는지 여부를 확인해주십시오.)
- 액세스 스위치의 포트를 바운스하여 클라이언트 머신을 다시 인증해 보십시오.

엔드포인트

이러한 창에서는 네트워크에 연결하는 엔드포인트를 구성하고 관리할 수 있습니다.

엔드포인트 설정

다음 표에서는 엔드포인트를 생성하고 엔드포인트용 정책을 할당하는 데 사용할 수 있는 **Endpoints(**엔드포인트**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**입니다.

표 ***107:*** 엔드포인트 설정

필드 이름	사용 지침
MAC Address(MAC 주소**)**	정적으로 엔드포인트를 생성하기 위한 MAC 주소를 16진수 형식으로 입력합니다. MAC 주소는 Cisco ISE가 활성화된 네트워크에 연결되어 있는 인터페이스의 디바이스 식별자입니다.
Static Assignment(정적 할당**)**	정적 할당 상태가 정적으로 설정되어 있을 때 엔드포인트 창에서 엔드포인트를 정적으로 생성하려면 이 확인란을 선택합니다. 엔드포인트의 정적 할당 상태는 정적에서 동적으로 또는 동적에서 정적으로 전환할 수 있습니다.
Policy Assignment(정책 할당**)**	(**Static Assignment(**정적 할당**)**가 선택되어 있지 않으면 기본적으로 비활성화됨) **Policy Assignment(**정책 할당**)** 드롭다운 목록에서 일치하는 엔드포인트 정책을 선택합니다. 다음 중 하나를 수행할 수 있습니다. • 일치하는 엔드포인트 정책을 선택하지 않고 기본 엔드포인트 정책인 Unknown(알 수 없음)을 사용하는 경우 엔드포인트의 동적 프로파일링을 허용하는 엔드포인트에 대해 정적 할당 상태가 동적으로 설정됩니다. • Unknown(알 수 없음) 이외의 일치하는 엔드포인트 정책을 선택하는 경우에는 해당 엔드포인트에 대해 정적 할당 상태가 정적으로 설정되며 **Static Assignment(**정적 할당**)** 확인란이 자동으로 선택됩니다.

필드 이름	사용 지침
Static Group Assignment(정적 그룹 할당**)**	엔드포인트를 ID 그룹에 정적으로 할당하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 이전에 다른 엔드포인트 ID 그룹에 동적으로 할당되었던 엔드포인트에 대해 다음 번에 엔드포인트 정책을 평가하는 동안 프로파일링 서비스가 엔드포인트 ID 그룹을 변경하지 않습니다. 이 확인란의 선택을 취소하면 정책 컨피그레이션에 따라 엔드포인트 ID 그룹이 ISE 프로파일러가 할당한 대로 동적으로 설정됩니다. Static Group Assignment(정적 그룹 할당) 옵션을 선택하지 않으면 다음 번에 엔드포인트 정책을 평가하는 동안 엔드포인트가 일치하는 ID 그룹에 자동으로 할당됩니다.

Identity Group Assignment(ID 그룹 할당**)**	엔드포인트를 할당할 엔드포인트 ID 그룹을 선택합니다.
	
	엔드포인트에 대한 엔드포인트 정책 평가 중에 **Create Matching Identity Group(**일치하는 **ID** 그룹 생성**)** 옵션을 사용하지 않으려는 경우 또는 엔드포인트를 정적으로 생성하는 경우 ID 그룹에 엔드포인트를 할당할 수 있습니다.
	
	Cisco ISE에는 시스템에서 생성된 다음과 같은 엔드포인트 ID 그룹이 포함되어 있습니다.
	• Blocked List
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

관련 항목

식별된 엔드포인트, 753 페이지
정책 및 ID 그룹을 정적으로 할당하여 엔드포인트 생성, 748 페이지

LDAP에서 엔드포인트 가져오기 설정

다음 표에서는 LDAP 서버에서 엔드포인트를 가져오는 데 사용할 수 있는 Import from LDAP(LDAP에서 가져오기) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**입니다.

표 ***108: LDAP***에서 엔드포인트 가져오기 설정

필드 이름	사용 지침
Connection Settings(연결 설정**)**	
Host(호스트**)**	LDAP 서버의 호스트 이름 또는 IP 주소를 입력합니다.
Port(포트**)**	LDAP 서버의 포트 번호를 입력합니다. LDAP 서버에서 가져오려는 경우 기본 포트인 389를 사용할 수 있으며, SSL을 통해 LDAP 서버에서 가져오려는 경우 기본 포트인 636을 사용할 수 있습니다. 참고 Cisco ISE는 구성된 모든 포트 번호를 지원합니다. 구성된 값은 LDAP 서버 연결 세부정보와 일치해야 합니다.
Enable Secure Connection(보안 연결 활성화**)**	SSL을 통해 LDAP 서버에서 가져오려면 **Enable Secure Connection(**보안 연결 활성화**)** 확인란을 선택합니다.
Root CA Certificate Name(루트 **CA** 인증서 이름**)**	신뢰할 수 있는 CA 인증서를 보려면 드롭다운 화살표를 클릭합니다. 루트 CA 인증서 이름은 LDAP 서버에 연결하는 데 필요한 신뢰할 수 있는 CA 인증서를 지칭합니다. Cisco ISE에서는 신뢰할 수 있는 CA 인증서를 추가(가져오기), 편집, 삭제 및 내보내기할 수 있습니다.
Anonymous Bind(익명 바인딩**)**	**Anonymous Bind(**익명 바인딩**)** 확인란을 활성화하거나 slapd.conf 구성 파일에서 LDAP 관리자 자격 증명을 입력해야 합니다.
Admin DN(관리자 **DN)**	slapd.conf 구성 파일에서 LDAP 관리자에 대해 구성된 DN(Distinguished Name)을 입력합니다. 관리자 DN 형식의 예제는 cn=Admin, dc=cisco.com, dc=com과 같습니다.

필드 이름	사용 지침
Password(비밀번호**)**	slapd.conf 구성 파일에서 LDAP 관리자에 대해 구성된 비밀번호를 입력합니다.
Base DN(기본 **DN)**	부모 엔트리의 고유 이름을 입력합니다. 기본 DN 형식의 예제는 dc=cisco.com, dc=com과 같습니다.
Query Settings(쿼리 설정**)**	
MAC Address objectClass(MAC 주소 **objectClass)**	MAC 주소를 가져오는 데 사용되는 쿼리 필터(예: ieee802Device)를 입력합니다.
MAC Address Attribute Name(MAC 주소 속성 이름**)**	가져오려는 반환된 속성 이름(예: macAddress)을 입력합니다.
Profile Attribute Name(프로파일 속성 이름**)**	LDAP 속성의 이름을 입력합니다. 이 속성은 LDAP 서버에 정의되어 있는 각 엔드포인트 엔트리에 대한 정책 이름을 포함합니다. **Profile Attribute Name(**프로파일 속성 이름**)** 필드를 구성할 때는 다음 사항을 고려합니다. • **Profile Attribute Name(**프로파일 속성 이름**)** 필드에서 이 LDAP 속성을 지정하지 않거나 이를 잘못 구성하는 경우에는 가져오기 작업 중에 엔드포인트가 "알 수 없음"으로 표시되며 이러한 엔드포인트는 일치하는 엔드포인트 프로파일링 정책으로 별도로 프로파일이 지정됩니다. • **Profile Attribute Name(**프로파일 속성 이름**)** 필드에서 이 LDAP 속성을 구성하면 속성 값을 검증하여 엔드포인트 정책이 Cisco ISE의 기존 정책과 일치하는지를 확인한 다음, 엔드포인트를 가져옵니다. 엔드포인트 정책이 기존 정책과 일치하지 않으면 해당 엔드포인트를 가져오지 않습니다.
Time Out(시간 초과**)**	시간을 초 단위로 입력합니다. 유효한 범위는 1초 ~ 60초입니다.

관련 항목

식별된 엔드포인트, 753 페이지
LDAP 서버에서 엔드포인트 가져오기, 752 페이지

엔드포인트 프로파일링 정책 설정

다음 표에서는 **Endpoint Policies(**엔드포인트 정책**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling Policies(**프로파일링 정책**)**입니다.

표 ***109:*** 엔드포인트 프로파일링 정책 설정

필드 이름	사용 지침
Name(이름**)**	생성하려는 엔드포인트 프로파일링 정책의 이름을 입력합니다.
Description(설명**)**	생성하려는 엔드포인트 프로파일링 정책의 설명을 입력합니다.
Policy Enabled(정책 활성화**)**	엔드포인트를 프로파일링할 때 일치하는 프로파일링 정책을 연결하기 위해 **Policy Enabled(**정책 활성화**)** 확인란은 기본적으로 선택됩니다. 이 확인란의 선택을 취소하면 엔드포인트 프로파일링 시 엔드포인트 프로파일링 정책이 제외됩니다.
Minimum Certainty Factor(최소 확실성 요인**)**	프로파일링 정책과 연결할 최소값을 입력합니다. 기본값은 10입니다.
Exception Action(예외 작업**)**	프로파일링 정책에서 규칙을 정의할 때 조건과 연결할 예외 작업을 선택합니다. 기본값은 NONE(없음)입니다. **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Profiling(**프로파일링**) > Exception Actions(**예외 작업**)**에서 예외 작업을 정의합니다.
Network Scan (NMAP) Action(네트워크 스캔 **(NMAP)** 작업**)**	필요한 경우 프로파일링 정책에서 규칙을 정의할 때 조건과 연결할 네트워크 스캔 작업을 목록에서 선택합니다. 기본값은 NONE(없음)입니다. **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Profiling(**프로파일링**) > Network Scan (NMAP) Actions(**네트워크 스캔**(NMAP)** 작업**)**에서 예외 작업을 정의합니다.

필드 이름	사용 지침
Create an Identity Group for the policy(정책에 대한 **ID** 그룹 생성**)**	엔드포인트 ID 그룹을 생성하려면 다음 옵션 중 하나를 선택합니다. • **Yes, create matching Identity Group(**예**,** 일치하는 **ID** 그룹을 생성합니다**.)** • **No, use existing Identity Group hierarchy(**아니요**,** 기존 **ID** 그룹 계층을 사용합니다**.)**
Yes, create matching Identity Group(예**,** 일치하는 **ID** 그룹을 생성합니다**.)**	기존 프로파일링 정책을 사용하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 해당 엔드포인트에 대해 일치하는 ID 그룹이 생성되며, 엔드포인트 프로파일이 기존 프로파일링 정책과 일치하면 ID 그룹은 Profiled 엔드포인트 ID 그룹의 자식이 됩니다. 예를 들어 네트워크에서 검색된 엔드포인트가 Xerox-Device 프로파일과 일치하면 엔드포인트 ID 그룹 페이지에서 Xerox-Device 엔드포인트 ID 그룹이 생성됩니다.

필드 이름	사용 지침
No, use existing Identity Group hierarchy(아니요, 기존 **ID** 그룹 계층을 사용합니다**.)**	프로파일링 정책 및 ID 그룹의 계층 구성을 사용하여 일치하는 부모 엔드포인트 ID 그룹에 엔드포인트를 할당하려면 이 확인란을 선택합니다. 이 옵션을 사용하는 경우 엔드포인트 프로파일링 정책 계층을 사용하여 일치하는 부모 엔드포인트 ID 그룹 중 하나와 부모 ID 그룹에 대해 연결된 엔드포인트 ID 그룹에 엔드포인트를 할당할 수 있습니다. 예를 들어 기존 프로파일과 일치하는 엔드포인트는 적절한 부모 엔드포인트 ID 그룹 아래에 그룹화됩니다. 여기서 Unknown(알 수 없음) 프로파일과 일치하는 엔드포인트는 Unknown(알 수 없음) 아래에 그룹화되고 기존 프로파일과 일치하는 엔드포인트는 프로파일이 지정된 엔드포인트 ID 그룹 아래에 그룹화됩니다. 예를 들면 다음과 같습니다. • Cisco-IP-Phone 프로파일과 일치하는 엔드포인트는 Cisco-IP-Phone 엔드포인트 ID 그룹 아래에 그룹화됩니다. • Workstation 프로파일과 일치하는 엔드포인트는 Workstation 엔드포인트 ID 그룹 아래에 그룹화됩니다. Cisco-IP-Phone 및 Workstation 엔드포인트 ID 그룹은 시스템의 Profiled 엔드포인트 ID 그룹에 연결됩니다.
Parent Policy(부모 정책**)**	새 엔드포인트 프로파일링 정책을 연결할 시스템에 정의된 부모 프로파일링 정책을 선택합니다. 자식에게 규칙과 조건을 상속할 부모 프로파일링 정책을 선택할 수 있습니다.

필드 이름	사용 지침
Associated CoA Type(연결된 **CoA** 유형**)**	엔드포인트 프로파일링 정책과 연결할 CoA 유형을 다음 중에서 하나 선택합니다. • CoA 없음 • 포트 바운스 • 재인증 • Administration(관리) > System(시스템) > Settings(설정) > Profiling(프로파일링)에 설정된 프로파일러 컨피그레이션에서 적용되는 전역 설정
Rules(규칙**)**	엔드포인트 프로파일링 정책에 정의된 하나 이상의 규칙에 따라 엔드포인트에 일치하는 프로파일링 정책이 결정됩니다. 그러면 해당 프로파일에 따라 엔드포인트를 그룹화할 수 있습니다. 규칙에서는 정책 요소 라이브러리의 프로파일링 조건을 하나 이상 사용하여 전체 분류를 위한 엔드포인트 속성 및 해당 값을 검증합니다.

필드 이름	사용 지침
Conditions(조건**)**	고정된 Conditions(조건) 오버레이를 확장하려면 더하기 [+] 기호를 클릭하고, 고정된 오버레이를 닫으려면 빼기 [-] 기호를 클릭하거나 오버레이 바깥쪽을 클릭합니다. **Select Existing Condition from Library(**라이브러리에서 기존 조건 선택**)** 또는 **Create New Condition (Advanced Option)(**새 조건 생성**(**고급 옵션**))**을 클릭합니다. **Select Existing Condition from Library(**라이브러리에서 기존 조건 선택**)**: 정책 요소 라이브러리에서 미리 정의된 Cisco 조건을 선택하여 식을 정의할 수 있습니다. **Create New Condition (Advanced Option)(**새 조건 생성**(**고급 옵션**))**: 여러 시스템 또는 사용자 맞춤화 사전에서 속성을 선택하여 식을 정의할 수 있습니다. 다음 중 하나를 프로파일링 조건과 연결할 수 있습니다. • 각 조건에 대한 확실성 요인의 정수 값 • 해당 조건에 대한 예외 작업 또는 네트워크 스캔 작업 프로파일링 조건과 연결할 다음의 미리 정의된 설정 중 하나를 선택합니다. • Certainty Factor Increases(확실성 요인 증가): 각 규칙에 대한 확실성 값을 입력합니다. 전체 분류와 관련하여 모든 일치 규칙에 대해 이 값을 추가할 수 있습니다. • Take Exception Action(예외 작업 수행): 이 엔드포인트 프로파일링 정책의 Exception Action(예외 작업) 필드에 구성되어 있는 예외 작업을 트리거합니다. • Take Network Scan Action(네트워크 스캔 작업 수행): 이 엔드포인트 프로파일링 정책의 Network Scan (NMAP) Action(네트워크 스캔 (NMAP) 작업) 필드에 구성되어 있는 네트워크 스캔 작업을 트리거합니다.

필드 이름	사용 지침
Select Existing Condition from Library(라이브러리에서 기존 조건 선택**)**	다음을 수행할 수 있습니다. • 정책 요소 라이브러리에서 사용 가능한 미리 정의된 Cisco 조건을 선택한 다음 AND 또는 OR 연산자를 사용하여 여러 조건을 추가할 수 있습니다. • Action(작업) 아이콘을 클릭하여 후속 단계에서 다음을 수행합니다. • **Add Attribute or Value(**속성 또는 값 추가**)**: 임시 속성 또는 값 쌍을 추가할 수 있습니다. • **Add Condition from Library(**라이브러리에서 조건 추가**)**: 미리 정의된 Cisco 조건을 추가할 수 있습니다. • **Duplicate(**복제**)**: 선택한 조건의 복사본을 생성합니다. • **Add Condition to Library(**라이브러리에 조건 추가**)**: 생성한 임시 속성/값 쌍을 정책 요소 라이브러리에 저장할 수 있습니다. • **Delete(**삭제**)**: 선택한 조건을 삭제합니다.

필드 이름	사용 지침
Create New Condition (Advance Option)(새 조건 생성**(**고급 옵션**))**	다음을 수행할 수 있습니다. • 식에 임시 속성/값 쌍을 추가한 다음 AND 또는 OR 연산자를 사용하여 여러 조건을 추가할 수 있습니다. • Action(작업) 아이콘을 클릭하여 후속 단계에서 다음을 수행합니다. • **Add Attribute or Value(**속성 또는 값 추가**)**: 임시 속성 또는 값 쌍을 추가할 수 있습니다. • **Add Condition from Library(**라이브러리에서 조건 추가**)**: 미리 정의된 Cisco 조건을 추가할 수 있습니다. • **Duplicate(**복제**)**: 선택한 조건의 복사본을 생성합니다. • **Add Condition to Library(**라이브러리에 조건 추가**)**: 생성한 임시 속성/값 쌍을 정책 요소 라이브러리에 저장할 수 있습니다. • **Delete(**삭제**)**: 선택한 조건을 삭제합니다. AND 또는 OR 연산자를 사용할 수 있습니다.

관련 항목

Cisco ISE 프로파일링 서비스, 688 페이지
엔드포인트 프로파일링 정책 생성, 739 페이지
UDID 속성을 사용하는 엔드포인트 상황 가시성, 776 페이지

UDID 속성을 사용하는 엔드포인트 상황 가시성

고유 식별자(UDID)는 특정 엔드포인트의 MAC 주소를 식별하는 엔드포인트 속성입니다. 각 엔드포인트는 여러 MAC 주소를 가질 수 있습니다. 예를 들어 유선 인터페이스용 MAC 주소 하나와 무선 인터페이스용 MAC 주소 하나를 가질 수 있습니다. AnyConnect 에이전트는 해당 엔드포인트에 대한 UDID를 생성하고 이를 엔드포인트 속성으로 저장합니다. 권한 부여 쿼리에서 UDID를 사용할 수 있습니다. 각 엔드포인트의 UDID는 일정하게 유지되며, AnyConnect 설치 또는 제거 시 변경되지 않습니다. UUID를 사용하는 경우 **Context Visibility(**상황 가시성**)** 창(**Context Visibility(**상황 가시성**) > Endpoints(**엔드포인트**) > Compliance(**규정 준수**)**에서 NIC가 여러 개인 엔드포인트에 대해 여러 항목이 아닌 하나의 항목이 표시됩니다. Mac 주소가 아닌 특정 엔드포인트에서 포스처 제어를 보장할 수 있습니다.

참고 UDID를 생성하려면 엔드포인트에 AnyConnect 4.7 이상이 있어야 합니다.

Windows 및 Macintosh 엔드포인트용 엔드포인트 스크립트 마법사

엔드포인트 스크립트 마법사를 사용하면, 연결된 엔드포인트에서 스크립트를 실행하여 조직의 요구 사항을 준수하는 관리 작업을 수행할 수 있습니다. 여기에는 더 이상 사용되지 않는 소프트웨어 제거, 프로세스 또는 애플리케이션의 시작 또는 종료, 특정 서비스의 활성화 또는 비활성화 작업이 포함됩니다.

엔드포인트 스크립트는 Windows 및 Macintosh 엔드포인트에서 엔드포인트 스크립트 마법사를 통해 실행할 수 있습니다.

시작하기 전에

- 슈퍼 관리자의 사용자 역할이 있어야 합니다.
- 관리자 권한으로 Macintosh 및 Windows 엔드포인트에 액세스할 수 있도록 Cisco ISE에 대한 로그인 자격증명을 구성합니다.

  Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **Endpoint Login Configuration(**엔드포인트 로그인 구성**)**을 선택하여 다음을 구성합니다.

  - Cisco ISE가 엔드포인트에 로그인할 수 있는 도메인 자격 증명.
  - Cisco ISE가 로컬 사용자로 엔드포인트에 로그인할 수 있는 Windows 및 Macintosh용 로컬 사용자 자격증명.

    도메인 사용자가 로컬 사용자보다 우선합니다. 두 가지를 모두 구성했으며 로컬 사용자 자격증명으로 스크립트를 실행해야 하는 경우 도메인 자격증명을 제거해야 합니다.

- Windows 엔드포인트에는 Windows PowerShell 버전 5.1 이상이 설치되어 있어야 합니다. PowerShell 원격이 반드시 활성화되어 있어야 합니다.
- Macintosh 엔드포인트에는 Bash가 설치되어 있어야 합니다.
- Windows 및 Macintosh 엔드포인트 모두 cURL 버전 7.34 이상이 설치되어 있어야 합니다.
- Windows 및 Macintosh 엔드포인트는 네트워크에 연결되어야 하며 Cisco ISE에서 활성 세션이 있어야 합니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Context Visibility Endpoints(**상황 가시성 엔드포인트**)** > **Endpoints(**엔드포인트**)**를 선택합니다.

단계 **2** 창의 오른쪽 상단에 있는 링크 아이콘을 클릭하고 드롭 다운 목록에서 **Run Endpoint Scripts(**엔드포인트 스크립트 실행**)**를 선택합니다.

로그인 자격 증명을 아직 구성하지 않은 경우 **Welcome(**시작**)** 탭에 **Endpoint Login Configuration(**엔드포인트 로그인 컨피그레이션**)** 창에 대한 링크가 포함되어 있습니다. 로그인 자격 증명이 구성된 경우에만 이 탭의 오른쪽 하단에서 **Start(**시작**)** 버튼을 클릭할 수 있습니다.

단계 **3** **Select Category(**카테고리 선택**)** 탭에서 운영체제 또는 사용 가능한 애플리케이션을 기반으로 엔드포인트를 선택할 수 있습니다. **By OS(OS** 별**)** 또는 **By Application(**애플리케이션 별**)** 라디오 버튼을 클릭하여 선택합니다. **Next(**다음**)**를 클릭하여 작업을 계속합니다.

단계 **4** **Select Endpoints(**엔드포인트 선택**)** 창에서 대시릿이 OS 유형 또는 애플리케이션에 사용 가능한 필터를 표시합니다. 대시릿에서 적용할 필터를 클릭하면 해당 필터의 모든 엔드포인트가 표에 나열됩니다.

- 선택한 필터에 대한 모든 엔드포인트를 선택하려면 표의 제목 행에 있는 확인란을 선택합니다.
- 특정 엔드포인트를 선택하려면 표에서 해당 항목의 확인란을 선택합니다. 표에서 특정 엔드포인트를 찾으려면 표 위의 **Filter(**필터**)** 버튼을 클릭하고 **Quick Filter(**빠른 필터**)**를 선택합니다. 표시된 엔드포인트를 기준으로 필터링하여 필요한 엔드포인트를 찾을 수 있습니다.

참고 **Select Categories(**카테고리 선택**)** 단계에서 **By Application(**애플리케이션 기준**)**을 선택한 경우 이 단계에서 동일한 OS 유형에 속하는 엔드포인트를 선택해야 합니다. 애플리케이션 기반 스크립트의 경우 각 OS 유형에 대한 스크립트를 생성하고 엔드포인트 스크립트 마법사에서 각 OS 유형에 대해 별도의 작업을 설정합니다.

단계 **5** 스크립트를 실행할 엔드포인트를 선택한 후 **Next(**다음**)**를 클릭합니다.

단계 **6** **Select Scripts(**스크립트 선택**)** 탭에서 **Add(**추가**)**를 클릭합니다.

단계 **7** **Add Script(**스크립트 추가**)**를 클릭하여 시스템에서 스크립트를 선택합니다. **Start Upload(**업로드 시작**)**를 클릭하여 **Select Scripts(**스크립트 선택**)** 탭에 스크립트를 추가합니다.

단계 **8** 실행할 스크립트의 확인란을 선택하고 **Next(**다음**)**를 클릭합니다.

단계 **9** **Summary(**요약**)** 탭에는 선택한 엔드포인트 및 선택한 스크립트가 표시됩니다. 여기에서 선택 항목을 검토하고 **Back(**뒤로**)**을 클릭하여 세부정보를 변경합니다. **Finish(**종료**)**를 클릭하여 스크립트 실행을 시작합니다.

이 작업의 작업 **ID**와 함께 **Endpoints Script Report(**엔드포인트 스크립트 보고서**)** 팝업 창이 표시됩니다. 이 작업의 세부정보가 포함된 창으로 리디렉션할 **Endpoint Scripts provisioning report(**엔드포인트 스크립트 프로비저닝 보고서**)**를 클릭합니다.

엔드포인트 스크립트 마법사를 통해 실행되는 작업의 보고서를 보려면 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **Endpoint Scripts Provisioning Summary(**엔드포인트 스크립트 프로비저닝 요약**)**을 선택합니다.

엔드포인트 스크립트 프로비저닝 요약 보고서

Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **Endpoint Scripts Provisioning Summary(**엔드포인트 스크립트 프로비저닝 요약**)**를 선택합니다.

엔드포인트 스크립트 프로비저닝 요약 창에는 지난 30일간 엔드포인트 스크립트 마법사를 통해 실행된 작업의 세부정보가 표시됩니다. 창 내보내기를 예약하고 이전 보고서를 추적하려면 창의 오른쪽 상단에서 **Schedule(**일정**)**을 클릭합니다.

Export To(내보내기 대상**)**를 클릭하고 드롭다운 목록에서 보고서의 CSV 또는 PDF 버전을 저장소 또는 로컬 대상에 저장하는 옵션을 선택합니다.

Endpoint Scripts Provisioning Summary(엔드 포인트 스크립트 프로비저닝 요약**)** 창에는 기본적으로 다음 열이 포함된 표가 표시됩니다.

이름 열	표시되는 정보
로그인 시간	작업 제출 타임 스탬프.
작업 **ID**	이 항목의 세부정보를 보려면 Job ID(작업 ID) 항목을 클릭합니다. 엔드포인트 스크립트 프로비저닝 세부정보가 포함된 새 탭이 열리고 타임 스탬프, 선택한 엔드포인트의 MAC 주소, 각 엔드포인트에 대한 스크립트 상태 및 프로비저닝 상태, 작업을 프로비저닝하는 PSN의 이름 및 작업 ID가 함께 표시됩니다. 참고 참고: 스크립트 실행에 대한 상세한 단계별 세부정보를 보려면 MAC 주소를 클릭합니다.
관리자 이름	작업을 제출한 관리자의 이름.
Operating System(운영체제**)**	선택한 스크립트가 실행되는 운영체제.
총/성공/실패/진행 중인 엔드포인트	• 선택한 총 엔드포인트 수. • 스크립트가 성공적으로 실행된 엔드포인트의 수. • 스크립트 실행에 실패한 엔드포인트의 수. • 스크립트가 아직 실행중인 엔드포인트의 수.
스크립트 이름	작업에 포함된 스크립트의 이름.

IF-MIB

객체	**OID**
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5

객체	OID
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

SNMPv2-MIB

객체	OID
system	1.3.6.1.2.1.1
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

IP-MIB

객체	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToPhysicalPhysAddress	1.3.6.1.2.1.4.35.1.4

CISCO-CDP-MIB

객체	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVTPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

CISCO-VTP-MIB

객체	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

CISCO-STACK-MIB

객체	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

BRIDGE-MIB

객체	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

OLD-CISCO-INTERFACE-MIB

객체	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

CISCO-LWAPP-AP-MIB

객체	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.2

객체	OID
cLApMaxNumberOfDot11Slots	1.3.6.1.4.1.9.9.513.1.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.1.8
cLApMaxNumberOfEthernetSlots	1.3.6.1.4.1.9.9.513.1.1.1.1.9
cLApPrimaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.10
cLApPrimaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.11
cLApSecondaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.12
cLApSecondaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.13
cLApTertiaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.14
cLApTertiaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.20
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
cLApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
cLApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
cLApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
cLApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
cLApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30

객체	OID
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
cLApRogueDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

CISCO-LWAPP-DOT11-CLIENT-MIB

객체	OID
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWlanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

CISCO-AUTH-FRAMEWORK-MIB

객체	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.1.5
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

EEE8021-PAE-MIB: RFC IEEE 802.1X

객체	OID
dot1xAuthAuthControlledPortStatus	1.0.8802.1.1.1.1.2.1.1.5
dot1xAuthAuthControlledPortControl	1.0.8802.1.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.1.2.4.1.9

HOST-RESOURCES-MIB

객체	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5

LLDP-MIB

객체	OID
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2

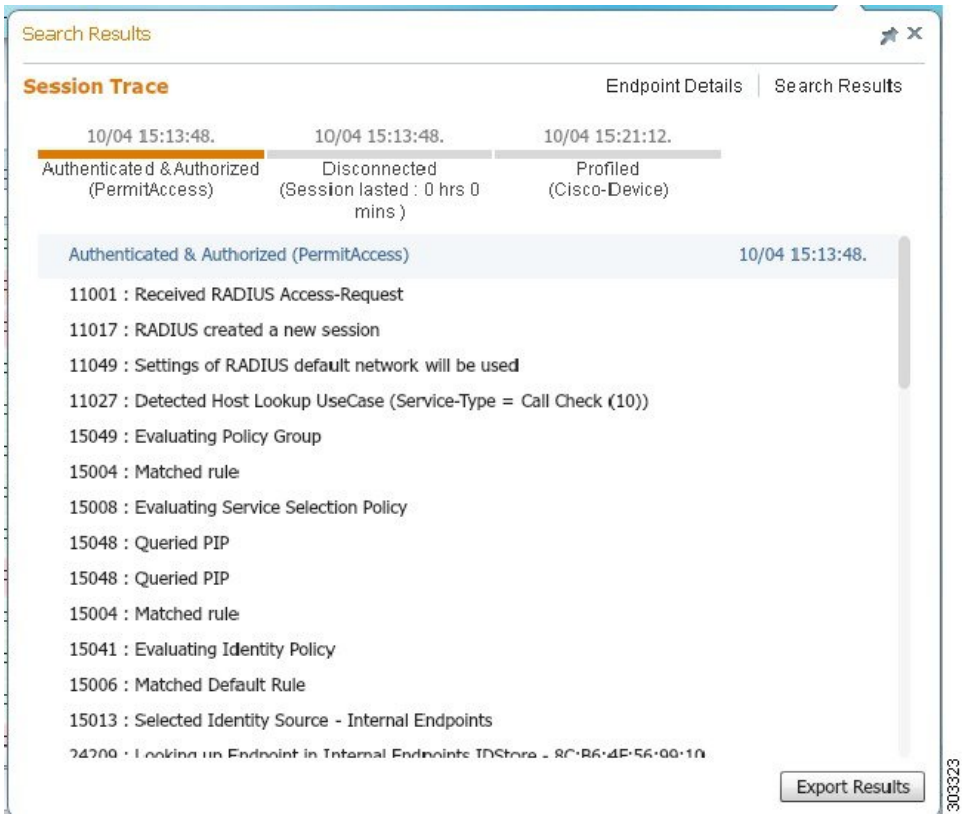
객체	**OID**
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
ldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

엔드포인트에 대한 세션 추적

Cisco ISE 홈 페이지 위쪽에 있는 글로벌 검색 상자를 사용하여 특정 엔드포인트의 세션 정보를 가져올 수 있습니다. 특정 기준으로 검색하는 경우 엔드포인트 목록이 표시됩니다. 이러한 엔드포인트 중 하나를 클릭하여 해당 엔드포인트에 대한 세션 추적 정보를 볼 수 있습니다. 다음 그림에는 엔드포인트에 대해 표시되는 세션 추적 정보의 예가 나와 있습니다.

참고 검색에 사용되는 데이터 집합은 엔드포인트 ID를 색인으로 사용합니다. 그러므로 인증이 발생할 때 인증에서 검색 결과 집합에 그러한 ID를 포함하도록 엔드포인트의 엔드포인트 ID가 반드시 있어야 합니다.

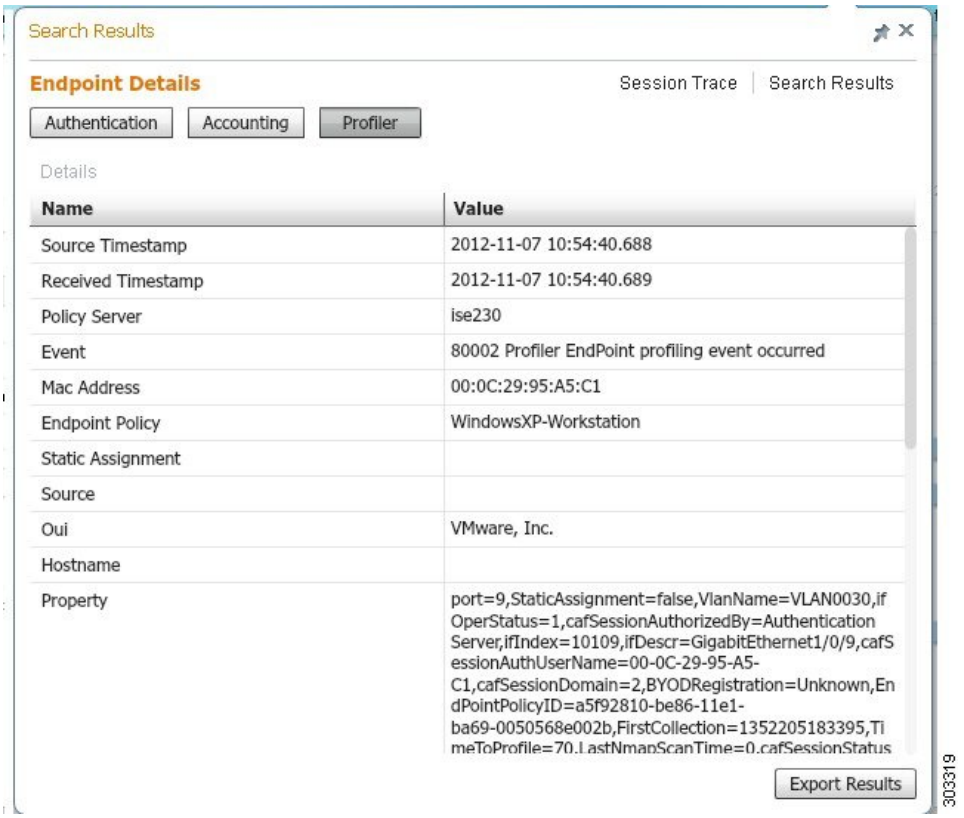
그림 ***30:*** 엔드포인트의 세션 추적



상단에 있는 클릭 가능한 타임라인을 사용하여 주요 권한 부여 전환을 볼 수 있습니다. **Export Results(**결과 내보내기**)** 옵션을 사용하여 .csv 형식으로 결과를 내보낼 수도 있습니다. 보고서는 브라우저로 다운로드됩니다.

Endpoint Details(엔드포인트 세부정보**)** 링크를 클릭하여 특정 엔드포인트에 대한 자세한 인증, 계정 관리 및 프로파일러 정보를 볼 수 있습니다. 다음 그림에는 엔드포인트에 대해 표시되는 엔드포인트 세부정보의 예가 나와 있습니다.

그림 ***31:*** 엔드포인트 세부정보



디렉토리에서 세션 제거

세션은 모니터링 및 문제 해결 노드의 세션 디렉토리에서 다음과 같이 지워집니다.

- 종료된 세션은 종료된 지 15분 후에 지워집니다.
- 인증은 있지만 계정 관리가 없는 세션은 1시간 후에 지워집니다.
- 모든 비활성 세션은 5일 이후에 지워집니다.

엔드포인트에 대한 글로벌 검색

Cisco ISE 홈 페이지 위쪽에 있는 글로벌 검색 상자를 사용하여 엔드포인트를 검색할 수 있습니다. 다음 조건을 사용하여 엔드포인트를 검색할 수 있습니다.

- 사용자 이름
- MAC 주소
- IP 주소

- 권한 부여 프로파일
- 엔드포인트 프로파일
- 실패 이유
- ID 그룹
- ID 저장소
- 네트워크 디바이스 이름
- 네트워크 디바이스 유형
- 운영체제
- 포스처 상태
- 위치
- 보안 그룹
- 사용자 유형

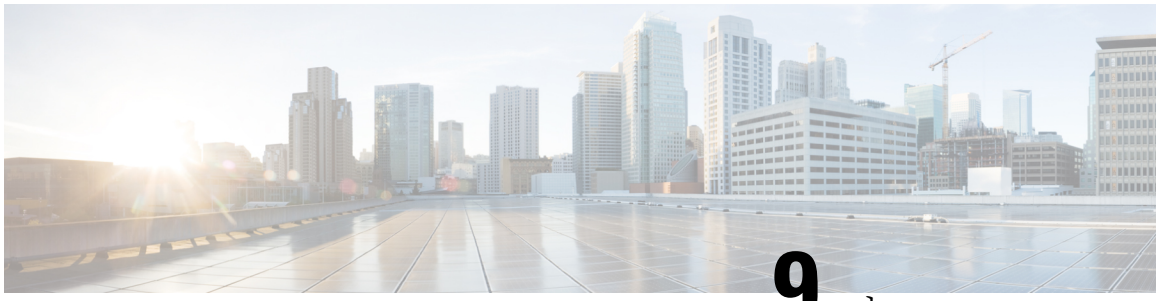
데이터를 표시하려면 Search(검색) 필드에 검색 기준으로 3자 이상을 입력해야 합니다.

참고 Cisco ISE에서 엔드포인트를 인증했거나 계정 관리 업데이트를 수신한 경우 전역 검색을 통해 엔드포인트를 찾을 수 있습니다. 수동으로 추가되었고 Cisco ISE에서 인증되지 않았거나 계정이 처리되지 않은 엔드포인트는 검색 결과에 표시되지 않습니다.

검색 결과에서는 엔드포인트의 현재 상태를 한 눈에 볼 수 있는 자세한 정보를 제공하므로 이 정보를 사용하여 문제를 해결할 수 있습니다. 검색 결과로는 상위 25개 항목만 표시됩니다. 필터를 사용하여 결과 범위를 좁히는 것이 좋습니다.

좌측 패널의 속성을 사용하여 결과를 필터링할 수 있습니다. 또한 원하는 엔드포인트를 클릭하여 다음과 같이 엔드포인트에 대한 자세한 정보를 확인할 수 있습니다.

- 세션 추적
- 인증 세부정보
- 계정 관리 세부정보
- 포스처 세부정보
- 프로파일러 세부정보
- 클라이언트 프로비저닝 세부정보
- 게스트 계정 관리 및 활동



9 장

BYOD(Bring Your Own Device)

기업 네트워크에서의 개인 디바이스(BYOD)

기업 네트워크에서 개인 디바이스를 지원하는 경우, 사용자(직원, 계약자 및 게스트) 및 해당 디바이스를 인증하고 권한을 부여하여 네트워크 서비스 및 엔터프라이즈 데이터 보호해야 합니다. Cisco ISE는 직원이 기업 네트워크에서 개인 디바이스를 안전하게 사용하도록 하는 데 필요한 도구를 제공합니다.

게스트는 게스트 포털에 로그인할 때 자신의 디바이스를 자동으로 등록할 수 있습니다. 게스트는 해당 게스트 유형에 대해 정의된 최대 제한까지 추가 디바이스를 등록할 수 있습니다. 이러한 디바이스는 포털 컨피그레이션에 따라 엔드포인트 ID 그룹에 등록됩니다.

게스트는 기본 신청자 프로비저닝(Network Setup Assistant)을 실행하거나 내 디바이스 포털에 디바이스를 추가하여 개인 디바이스를 네트워크에 추가할 수 있습니다. 운영체제에 따라, 사용할 기본 신청자 프로비저닝 마법사를 결정하는 기본 신청자 프로파일을 생성할 수 있습니다.

기본 신청자 프로파일을 모든 디바이스에 사용할 수 있는 것은 아니기 때문에 사용자는 내 디바이스 포털을 사용하여 이러한 디바이스를 수동으로 추가할 수 있습니다. 또는 이러한 디바이스를 등록하도록 BYOD 규칙을 구성할 수 있습니다.

Cisco ISE 커뮤니티 리소스

분산형 환경의 최종 사용자 디바이스 포털

Cisco ISE 최종 사용자 웹 포털에서는 관리, 정책 서비스 및 모니터링 페르소나를 사용하여 구성, 세션 지원 및 보고 기능을 제공합니다.

- **PAN(Policy Administration Node,** 정책 관리 노드**)**: 사용자, 디바이스 및 최종 사용자 포털에 적용하는 모든 구성 변경 사항은 PAN에 기록됩니다.
- **PSN(Policy Service node,** 정책 서비스 노드**)**: 네트워크 액세스, 클라이언트 프로비저닝, 게스트 서비스, 포스처 및 프로파일링을 비롯한 모든 세션 트래픽을 처리하는 PSN에서 최종 사용자 포털을 실행해야 합니다. PSN이 노드 그룹에 속해 있는 경우 노드에 장애가 발생하면 다른 노드에서 장애를 탐지하고 대기 중인 세션을 모두 재설정합니다.
- **MnT** 노드**(**모니터링 노드**)**: MnT 노드에서는 최종 사용자, 그리고 내 디바이스, 스폰서 및 게스트 포털의 디바이스 활동 관련 데이터를 수집, 집계 및 보고합니다. 기본 MnT 노드에 장애가 발생하면 보조 MnT 노드가 자동으로 기본 MnT 노드가 됩니다.

디바이스 포털용 전역 설정

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Settings(**설정**)**를 선택합니다.

BYOD 및 내 디바이스 포털에 대해 다음의 일반 설정을 구성할 수 있습니다.

- **Employee Registered Devices(**직원 등록 디바이스**)**: **Restrict employees to(**직원 제한**)**에 직원이 등록할 수 있는 최대 디바이스 수를 입력합니다. 기본적으로 이 값은 디바이스 **5**개로 설정됩니다.
- **Retry URL(**재시도 **URL)**: **Retry URL for onboarding(**온보딩용 재시도 **URL)**에 디바이스를 Cisco ISE로 다시 리디렉션하는 데 사용할 수 있는 URL을 입력합니다.

이러한 일반 설정을 구성하고 나면 회사에 대해 설정한 모든 BYOD 및 내 디바이스 포털에 해당 설정이 적용됩니다.

개인 디바이스 포털

Cisco ISE는 직원이 소유한 개인 디바이스를 지원할 수 있도록 여러 웹 기반 포털을 제공합니다. 이러한 디바이스 포털은 게스트 또는 스폰서 포털 흐름에 참여하지 않습니다.

- **Blocked List Portal(**차단 리스트 포털**)**: "차단 리스트"에 올려져 네트워크에 액세스하는 데 사용할 수 없는 개인 디바이스에 대한 정보를 제공합니다.
- **BYOD Portals(BYOD** 포털**)**: 직원이 기본 신청자 프로비저닝 기능을 사용하여 개인 디바이스를 등록하는 데 사용할 수 있습니다.
- **Certificate Provisioning Portal(**인증서 프로비저닝 포털**)**: 관리자와 직원이 BYOD 플로우를 통과할 수 없는 디바이스용으로 사용자/디바이스 인증서를 요청할 수 있습니다.
- **Client Provisioning Portals(**클라이언트 프로비저닝 포털**)**: 직원이 디바이스에서 규정 준수를 확인하는 포스처 에이전트를 다운로드하도록 합니다.
- **MDM Portals(MDM** 포털**)**: 직원이 외부 MDM(모바일 디바이스 관리) 시스템에 모바일 디바이스를 등록할 수 있도록 합니다.

- **My Devices Portals(**내 디바이스 포털**)**: 직원이 기본 신청자 프로비저닝을 지원하지 않는 개인 디바이스를 비롯한 개인 디바이스를 추가 및 등록하고 관리하는 데 사용할 수 있습니다.

Cisco ISE는 미리 정의된 일련의 기본 포털을 포함하여 Cisco ISE 서버에서 여러 디바이스 포털을 호스팅할 수 있는 기능을 제공합니다. 기본 포털 테마에는 표준 Cisco 브랜딩이 적용되어 있으며 이는 관리 포털을(**Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)**) 통해 사용자 맞춤화할 수 있습니다. 또한 조직에 따라 다른 이미지, 로고 및 CSS(Cascading Style Sheet) 파일을 업로드하여 포털을 추가로 사용자 맞춤화할 수도 있습니다.

디바이스 포털 액세스

다음과 같이 Cisco ISE GUI에서 개인 디바이스 포털에 액세스할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)**를 선택합니다.

단계 **2** 구성하려는 특정 디바이스 포털을 선택합니다.

차단 목록 포털

직원은 이 포털에 직접 액세스하지 않고 리디렉션됩니다.

직원이 자신의 개인 디바이스를 분실하거나 도난당한 경우, 내 디바이스 포털에서 해당 상태를 업데이트하고 해당 디바이스를 Blocked List(차단 목록) 엔드포인트 ID 그룹에 추가할 수 있습니다. 이렇게 하면 다른 사용자가 디바이스를 사용하여 무단으로 네트워크에 액세스하는 것을 차단할 수 있습니다. 누군가 이러한 디바이스를 사용하여 네트워크에 연결하려고 시도하면 Blocked List(차단 목록) 포털로 리디렉션되고 디바이스에서 네트워크에 대한 액세스가 거부되었다는 알림이 제공됩니다. 디바이스를 찾은 경우 직원은 디바이스를 복구(내 디바이스 포털에서)하고 디바이스를 다시 등록할 필요 없이 네트워크 액세스 권한을 다시 얻을 수 있습니다. 디바이스를 분실했는지 아니면 도난당했는지에 따라 디바이스를 네트워크에 연결하려면 추가 프로비저닝이 필요할 수 있습니다.

Blocked List(차단 목록) 포털에 대한 포트 설정(기본값은 포트 8444)을 구성할 수 있습니다. 포트 번호를 변경하는 경우 다른 최종 사용자 포털에 사용되고 있지 않은지 확인해 주십시오.

Blocked List(차단 목록) 포털 구성에 대한 자세한 내용은 차단 목록 포털 편집, 804 페이지를 참고하십시오.

인증서 프로비저닝 포털

직원은 인증서 프로비저닝 포털에 직접 액세스할 수 있습니다.

인증서 프로비저닝 포털에서 직원은 온보딩 플로우를 통과할 수 없는 디바이스에 대해 인증서를 요청할 수 있습니다. 예를 들어 point-of-sale 터미널과 같은 디바이스는 BYOD 플로우를 통과할 수 없으며 인증서를 수동으로 발급해야 합니다. 인증서 프로비저닝 포털에서는 권한이 있는 사용자 집합이 그러한 디바이스에 대해 인증서 요청을 업로드하고, 필요한 경우 키 쌍을 생성하고, 인증서를 다운로드할 수 있습니다.

직원은 이 포털에 액세스하여 단일 인증서를 요청하거나 CSV 파일을 사용하여 대량 인증서 요청을 수행할 수 있습니다.

ISE 커뮤니티 리소스

Cisco ISE 인증서 프로비저닝 포털의 기능 및 구성에 대한 자세한 내용은 ISE 2.0: 인증서 프로비저닝 포털을 참고하십시오.

BYOD(Bring Your Own Device) 포털

직원은 이 포털에 직접 액세스하지 않습니다.

기본 신청자를 사용하여 개인 디바이스를 등록하는 경우 직원은 BYOD(Bring Your Own Device) 포털로 리디렉션됩니다. 직원이 처음으로 개인 디바이스를 사용하여 네트워크에 액세스하기 위해 시도하는 경우, 수동으로 NSA(Network Setup Assistant) 마법사를 다운로드하여 실행할지 묻는 메시지를 표시한 다음 기본 신청자를 등록하고 설치하는 절차를 안내할 수 있습니다. 디바이스를 등록한 후에는 내 디바이스 포털을 사용하여 디바이스를 관리할 수 있습니다.

참고 디바이스가 AnyConnect NAM(Network Access Manager)을 사용하여 네트워크에 연결된 경우 BYOD 플로우는 지원되지 않습니다.

관련 항목

BYOD 포털 생성, 807 페이지
기업 네트워크에서의 개인 디바이스(BYOD), 791 페이지

클라이언트 프로비저닝 포털

직원은 이 포털에 직접 액세스하지 않고 리디렉션됩니다.

클라이언트 프로비저닝 시스템은 기업 네트워크에 액세스하려고 시도하는 디바이스에 대한 포스처 평가 및 교정 기능을 제공합니다. 직원이 디바이스를 사용하여 네트워크 액세스를 요청하면 이 직원을 클라이언트 프로비저닝 포털로 경로 지정하고 먼저 포스처 에이전트를 다운로드하도록 요구할 수 있습니다. 포스처 에이전트는 예를 들어 바이러스 방지 소프트웨어가 설치되었으며 해당 운영체제가 지원되는지 확인하는 방식으로 디바이스가 규정을 준수하는지 스캔합니다.

관련 항목

클라이언트 프로비저닝 포털 생성, 809 페이지

모바일 디바이스 관리 포털

직원은 이 포털에 직접 액세스하지 않고 리디렉션됩니다.

다수의 기업에서 MDM(Mobile Device Management) 시스템을 사용하여 직원의 모바일 디바이스를 관리하고 있습니다.

Cisco ISE를 사용하면 직원이 모바일 디바이스를 등록하고 기업 네트워크에 액세스하는 데 사용할 수 있는 외부 MDM 시스템을 통합할 수 있습니다. Cisco는 직원이 디바이스를 등록하고 네트워크에 연결하는 데 사용할 수 있는 외부 MDM 인터페이스를 제공합니다.

MDM 포털에서 직원은 외부 MDM 시스템에 등록할 수 있습니다.

그러면 직원은 내 디바이스 포털을 사용하여 PIN 코드를 사용한 디바이스 잠금, 디바이스를 기본 초기 설정으로 재설정, 디바이스를 등록할 때 설치한 애플리케이션 및 설정 제거 등과 같이 모바일 디바이스를 관리할 수 있습니다.

Cisco ISE에서는 모든 외부 MDM 시스템용 단일 MDM 포털 또는 각 개별 MDM 시스템용 포털을 사용할 수 있습니다.

MDM 서버를 ISE와 작동하도록 구성하는 방법에 대한 자세한 내용은 MDM 포털 생성, 811 페이지을 참고하십시오.

내 디바이스 포털

직원은 내 디바이스 포털에 직접 액세스할 수 있습니다.

네트워크 액세스가 필요한 일부 네트워크 디바이스는 기본 신청자 프로비저닝에서 지원되지 않으므로 BYOD 포털을 사용하여 등록할 수 없습니다. 그러나 직원은 운영체제가 지원되지 않거나 웹 브라우저가 없는 개인 디바이스(예: 프린터, 인터넷 라디오 및 기타 디바이스)를 내 디바이스 포털을 사용하여 추가하여 등록할 수 있습니다.

직원은 디바이스의 MAC 주소를 입력하여 새 디바이스를 추가 및 관리할 수 있습니다. 직원이 내 디바이스 포털을 사용하여 디바이스를 추가하면 Cisco ISE는 이 디바이스를 **RegisteredDevices** 엔드포인트 ID 그룹의 멤버로 엔드포인트 창(**Administration(**관리**)** > **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)**)에 추가합니다(다른 엔드포인트 ID 그룹에 이미 정적으로 할당된 경우는 제외). 디바이스는 Cisco ISE의 다른 엔드포인트처럼 프로파일링되고 네트워크 액세스를 위해 등록 프로세스를 거칩니다.

사용자가 하나의 디바이스에서 2개의 MAC 주소를 내 디바이스 포털에 입력하면 프로파일링은 두 주소가 동일한 호스트 이름을 갖는다고 판단하여 Cisco ISE에서 단일 항목으로 병합됩니다. 예를 들어 사용자가 유선 및 무선 주소로 노트북 컴퓨터를 등록합니다. 해당 디바이스에서 삭제와 같은 모든 작업이 두 주소 모두에서 수행됩니다.

포털에서 등록된 디바이스를 삭제하면 **DeviceRegistrationStatus** 및 **BYODRegistration** 속성이 각각 **NotRegistered** 및 **No**로 변경됩니다. 그러나 이러한 속성은 직원이 아닌 게스트가 자격 증명이 있는 게스트 포털의 게스트 디바이스 등록 창을 사용하여 디바이스를 등록하면 변경되지 않고 그대로 유지됩니다. 그 이유는 BYOD 속성은 직원 디바이스 등록 중에만 사용되기 때문입니다.

직원이 디바이스를 등록할 때 BYOD 포털을 사용하는지 아니면 내 디바이스 포털을 사용하는지에 관계없이 내 디바이스 포털을 사용하여 디바이스를 관리할 수 있습니다.

참고 관리자 포털이 작동 중지된 경우 내 디바이스 포털을 사용할 수 없습니다.

관련 항목

내 디바이스 포털 생성, 813 페이지

BYOD 구축 옵션 및 상태 플로우

개인 디바이스를 지원하는 BYOD 구축 플로우는 다음 요소에 따라 약간씩 다릅니다.

- 단일 또는 이중 SSID: 단일 SSID를 사용하는 경우 동일한 WLAN(Wireless Local Area Network)이 인증서 등록, 프로비저닝 및 네트워크 액세스에 사용됩니다. 이중 SSID 구축 환경에는 두 개의 SSID가 있습니다. 하나는 등록 및 프로비저닝을 제공하고, 다른 하나는 보안 네트워크 액세스를 제공합니다.
- Windows, macOS, iOS 또는 Android 디바이스: 기본 신청자 플로우는 디바이스 유형에 관계없이, 지원되는 개인 디바이스를 사용해 직원을 BYOD 포털로 리디렉션하여 디바이스 정보를 확인하는 방식으로 비슷하게 시작됩니다. 프로세스는 디바이스 유형에 따라 분기됩니다.

직원이 네트워크에 연결됨

1. Cisco ISE는 회사 Active Directory 또는 다른 회사 ID 저장소에 대해 직원의 자격 증명을 인증하고 권한 부여 정책을 제공합니다.
2. 디바이스가 BYOD 포털로 리디렉션됩니다. 디바이스의 MAC 주소 필드가 미리 구성되어 있으며 사용자가 디바이스 이름과 설명을 추가할 수 있습니다.
3. 기본 신청자는 구성되지만(MacOS, Windows, iOS, Android) 그 프로세스는 디바이스마다 다릅니다.
   - MacOS 및 Windows 디바이스: 직원이 BYOD 포털에서 **Register(**등록**)**를 클릭하여 신청자 프로비저닝 마법사(Network Setup Assistant)를 다운로드하고 설치합니다. 이 마법사는 신청자를 구성하고 EAP-TLS 기반 인증에 사용되는 인증서(필요한 경우)를 제공합니다. 발급되는 인증서는 디바이스의 MAC 주소 및 직원의 사용자 이름이 함께 내장됩니다.

     참고 Windows 디바이스의 사용자에게 관리자 권한이 없으면 Network Setup Assistant를 해당 디바이스에 다운로드할 수 없습니다. 최종 사용자에게 관리 권한을 부여할 수 없는 경우 BYOD 플로우를 사용하는 대신 GPO(Group Policy Object)를 사용하여 사용자의 디바이스에 인증서를 푸시합니다.

     참고 MacOS 10.15 버전부터는 사용자가 SPW(Supplicant Provisioning Wizard)의 다운로드를 허용해야 합니다. 사용자 디바이스에, Cisco ISE 서버로부터의 다운로드를 허용할지 거부할지 묻는 창이 표시됩니다.

   - iOS 디바이스: Cisco ISE 정책 서버는 Apple의 iOS를 사용하여 다음을 포함하여 새 프로파일을 무선으로 IOS 디바이스에 보냅니다.

- 발급되는 인증서(구성된 경우)는 디바이스의 MAC 주소 및 직원의 사용자 이름이 함께 내장됩니다.
- 802.1X 인증에 대한 EAP-TLS 사용을 강제하는 Wi-Fi 신청자 프로파일

- Android 디바이스: Cisco ISE는 직원이 Google Play에서 Cisco NSA(Network Setup Assistant)를 다운로드하도록 메시지를 표시하고 라우팅합니다. 직원은 애플리케이션을 설치한 후 NSA를 열고 설정 마법사를 시작할 수 있습니다. 이를 통해 디바이스를 구성하는 데 사용되는 신청자 컨피그레이션 및 발급된 인증서가 생성됩니다.

4. 사용자가 온보딩 플로우를 완료하면 Cisco ISE가 CoA(Change of Authorization)를 시작합니다. 이로 인해 MacOS, Windows 및 Android 디바이스가 보안 802.1X 네트워크에 다시 연결됩니다. 단일 SSID에 대해 iOS 디바이스는 자동으로 연결되지만, 이중 SSID의 경우 마법사는 iOS 사용자에게 새 네트워크에 연결할지 묻는 메시지를 표시합니다.

참고 신청자를 사용하지 않는 BYOD 플로우를 구성할 수 있습니다. Cisco ISE 커뮤니티 문서 https://supportforums.cisco.com/blog/12705471/ise-byod-registration-only-without-native-supplicant-or-certificate-provisioning을 참조하십시오.

참고 실제 Wi-Fi 네트워크가 숨겨져 있을 때만 **Enable if Target Network is Hidden(**타깃 네트워크가 숨겨진 경우 활성화**)** 확인란을 선택합니다. 그러지 않으면 단일 SSID 플로우(특히 온보딩과 연결 둘 다에 대해 동일한 Wi-Fi 네트워크 또는 SSID가 사용되는 경우)에서 특정 iOS 디바이스에 대해 Wi-Fi 네트워크 컨피그레이션이 올바르게 프로비저닝되지 않을 수 있습니다.

BYOD 세션 엔드포인트 속성

BYOD 플로우 중에 엔드포인트 속성 *BYODRegistration*의 상태가 다음 상태로 변경됩니다.

- *Unknown(*알 수 없음*)*: 디바이스가 BYOD 플로우를 진행하지 않았습니다.
- *Yes(*예*)*: 디바이스가 BYOD 플로우를 진행했으며 등록되었습니다.
- *No(*아니요*)*: 디바이스가 BYOD 플로우를 진행했지만 등록되지 않았습니다. 이는 디바이스가 삭제되었음을 의미합니다.

디바이스 등록 상태 엔드포인트 속성

디바이스 등록 중에 엔드포인트 속성 *DeviceRegistrationStatus*의 상태가 다음 상태로 변경됩니다.

- *Registered(*등록됨*)*: 디바이스가 BYOD 플로우를 진행했으며 등록되었습니다. 속성이 보류 중에서 등록됨으로 변경될 때까지 20분 정도 지연됩니다.
- *Pending(*보류 중*)*: 디바이스가 BYOD 플로우를 진행했으며 등록되었습니다. 그러나 Cisco ISE가 네트워크에서 이 디바이스를 발견하지 않았습니다.

- *Not Registered(*등록되지 않음*)*: 디바이스가 BYOD 플로우를 진행하지 않았습니다. *Not Registered(*등록되지 않음*)*는 *DeviceRegistrationStatus* 속성의 기본 상태입니다.
- *Stolen(*도난됨*)*: 사용자가 내 디바이스 포털에 로그온하여 현재 온보딩된 디바이스를 Stolen(도난됨)으로 표시합니다. 이는 다음의 경우에 발생합니다.
  - 인증서 및 프로파일을 프로비저닝하여 디바이스가 온보딩된 경우 Cisco ISE는 디바이스에 프로비저닝된 인증서를 취소하고 디바이스의 MAC 주소를 차단 목록 엔드포인트 ID 그룹에 할당합니다. 해당 디바이스는 더 이상 네트워크 액세스 권한을 갖지 않습니다.
  - 프로파일을 프로비저닝하여 디바이스가 온보딩된 경우(인증서 없음) Cisco ISE는 디바이스를 차단 목록 엔드포인트 ID 그룹에 할당합니다. 이 경우에서는 권한 부여 정책을 생성하지 않는 한, 디바이스가 계속해서 네트워크 액세스 권한을 갖게 됩니다. 예를 들어, **IF Endpoint Identity Group is Blocked List AND BYOD_is_Registered THEN DenyAccess**와 같습니다.

  관리자는 여러 디바이스에 대해 인증서 삭제 또는 취소와 같이 네트워크 액세스를 비활성화하는 작업을 수행합니다.

  사용자가 도난당한 디바이스를 복원하면 상태가 *Not Registered(*등록 안 됨*)*로 돌아갑니다. 사용자는 해당 디바이스를 삭제하고 다시 추가해야 합니다. 이렇게 하면 온보딩 프로세스가 시작됩니다.
- *Lost(*손실*)*: 사용자가 내 디바이스 포털에 로그온하고 현재 온보딩된 디바이스를 *Lost(*손실*)*로 표시합니다. 이 경우 다음 작업이 수행됩니다.
  - 디바이스가 차단 목록 ID 그룹에 할당됩니다.
  - 디바이스에 프로비저닝된 인증서는 취소되지 않습니다.
  - 디바이스 상태가 *Lost(*손실*)*로 업데이트됩니다.
  - *BYODRegistration* 상태가 *No(*아니요*)*로 업데이트됩니다.

  손실된 디바이스를 차단하기 위한 권한 부여 정책을 생성하지 않는 한, 손실된 디바이스는 계속해서 네트워크 액세스 권한을 갖게 됩니다. 차단 목록 ID 그룹 또는 *endpoint:BYODRegistration* 속성을 규칙에서 사용할 수 있습니다. 예를 들어, **IF Endpoint Identity Group is Blocked List AND EndPoints:BYODRegistrations Equals No THEN BYOD**와 같습니다. 더 세부적인 액세스를 위해 *NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST*" , *InternalUser:IdentityGroup Equals* <<*group*>>을 규칙의 IF 부분에 추가할 수도 있습니다.

직원이 등록하는 개인 디바이스의 수 제한

직원이 1~100개의 개인 디바이스를 등록하도록 허용할 수 있습니다. 직원이 개인 디바이스를 등록하는 데 사용하는 포털과는 관계없이 이 설정은 모든 포털에서 등록할 수 있는 최대 디바이스 수를 정의합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Settings(**설정**)** > **Employee Registered Devices(**직원 등록 디바이스**)**를 선택합니다.

단계 **2** **Restrict employees to(**직원의 등록 수 제한**)** 필드에 직원이 등록할 수 있는 최대 디바이스 수를 입력합니다. 기본적으로 이 값은 디바이스 **5**개로 설정됩니다.

단계 **3** **Save(**저장**)**를 클릭합니다. 설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

기본 신청자를 사용하는 디바이스 등록 지원

Cisco ISE 네트워크에서 개인 디바이스를 지원하기 위해 기본 신청자 프로파일을 생성할 수 있습니다. 사용자의 권한 부여 요건과 연결하는 프로파일을 기준으로 하여 Cisco ISE는 사용자 개인 디바이스가 네트워크에 액세스하도록 설정하는 데 필요한 신청자 프로비저닝 마법사를 제공합니다.

그러면 직원이 개인 디바이스를 사용하여 네트워크에 처음 액세스를 시도할 때 등록 및 신청자 컨피그레이션 과정이 자동으로 안내됩니다. 디바이스를 등록한 직원은 내 디바이스 포털을 사용하여 디바이스를 관리할 수 있습니다.

기본 신청자가 지원하는 운영체제

기본 신청자가 지원되는 운영체제는 다음과 같습니다.

- Android(Amazon Kindle, B&N Nook 제외)
- Mac OS X(Apple Mac 컴퓨터용)
- Apple iOS 디바이스(Apple iPhone, iPhone 및 iPad)
- Microsoft Windows 7 및 8(RT 제외), Vista 및 XP

자격 증명이 지정된 게스트 포털을 사용한 직원의 개인 디바이스 등록 허용

자격 증명이 지정된 게스트 포털을 사용하는 직원은 개인 디바이스를 등록할 수 있습니다. 직원은 BYOD 포털에서 제공하는 셀프 프로비저닝 흐름을 통해 기본 신청자를 사용하여 디바이스를 네트워크에 직접 연결할 수 있습니다. Windows, MacOS, iOS 및 Android 디바이스용 기본 신청자가 제공됩니다.

시작하기 전에

기본 신청자 프로파일을 생성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals and Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)**를 선택합니다.

단계 **2** 직원이 기본 신청자를 사용하여 디바이스를 등록하는 데 사용할 수 있도록 할 자격 증명이 지정된 게스트 포털을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 3 **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 4 **BYOD Settings(BYOD** 설정**)**에서 **Allow employees to use personal devices on the network(**네트워크에서 직원의 개인 디바이스 사용 허용**)** 확인란을 선택합니다.

단계 5 **Save(**저장**)**를 클릭합니다.

BYOD 등록과 다시 연결하기 위한 URL 제공

BYOD 포털을 사용하여 개인 디바이스를 등록하는 동안 문제가 발생한 직원이 등록 프로세스에 다시 연결하는 데 사용할 수 있는 정보를 제공할 수 있습니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Settings(**설정**)** > **Retry URL(**재시도 **URL)**을 선택합니다.

단계 2 **Retry URL for Onboarding(**온보딩용 재시도 **URL)** 필드에 디바이스를 Cisco ISE로 다시 리디렉션하는 데 사용할 URL을 입력합니다.

등록 프로세스 중에 문제가 발생하면 디바이스가 인터넷에 자동으로 다시 연결하려고 시도합니다. 이 시점에서 여기에 입력하는 URL이 디바이스를 Cisco ISE로 리디렉션하며, Cisco ISE가 온보딩 프로세스를 다시 시작합니다. 기본값은 192.0.2.123입니다.

단계 3 **Save(**저장**)**를 클릭합니다.

설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

디바이스 포털 컨피그레이션 작업

기본 포털 및 해당 기본 설정(예: 인증서, 엔드포인트 ID 그룹, ID 소스 시퀀스, 포털 테마, 이미지 및 Cisco ISE가 제공하는 기타 세부정보)을 사용할 수 있습니다. 기본 설정을 사용하지 않으려면 새 포털을 생성하거나 자신의 요구 사항에 맞게 기존 포털을 편집해야 합니다. 여러 포털을 생성하려는 경우 동일한 설정을 사용하여 포털을 복제할 수 있습니다.

새 포털을 생성하거나 기본 포털을 편집한 후에는 포털을 사용할 수 있는 권한을 부여해야 합니다. 포털을 사용할 수 있는 권한을 부여한 경우 이후의 컨피그레이션 변경 사항은 즉시 반영됩니다.

내 디바이스 포털을 사용하기 위해 권한을 부여하지 않아도 됩니다.

포털을 삭제하기로 선택한 경우에는 먼저 권한 부여 정책 규칙 및 이와 연결된 권한 부여 프로파일을 모두 삭제하거나 다른 포털을 사용하도록 수정해야 합니다.

여러 디바이스 포털 구성과 관련된 작업에 대해서는 다음 표를 참고해 주십시오.

작업	차단 목록 포털	**BYOD** 포털	클라이언트 프로비저닝 포털	**MDM** 포털	내 디바이스 포털
정책 서비스 활성화, 802 페이지	필수	필수	필수	필수	필수
디바이스 포털에 인증서 추가, 802 페이지	필수	필수	필수	필수	필수
외부 ID 소스 생성, 802 페이지	필수가 아님	필수가 아님	필수가 아님	필수가 아님	필수
ID 소스 시퀀스 생성, 803 페이지	필수가 아님	필수가 아님	필수가 아님	필수가 아님	필수
엔드포인트 ID 그룹 생성, 804 페이지	필수가 아님	필수	필수가 아님	필수	필수
차단 목록 포털 편집	필수	해당 없음	해당 없음	해당 없음	해당 없음
BYOD 포털 생성, 807 페이지	해당 없음	필수	해당 없음	해당 없음	해당 없음
클라이언트 프로비저닝 포털 생성, 809 페이지	해당 없음	해당 없음	필수	해당 없음	해당 없음
MDM 포털 생성, 811 페이지	해당 없음	해당 없음	해당 없음	필수	해당 없음
내 디바이스 포털 생성, 813 페이지	해당 없음	해당 없음	해당 없음	해당 없음	필수
권한 부여 프로파일 생성, 814 페이지	해당 없음	필수	필수	필수	필수가 아님
디바이스 포털 사용자 맞춤화, 815 페이지	선택 사항	선택 사항	선택 사항	선택 사항	선택 사항

정책 서비스 활성화

Cisco ISE 최종 사용자 포털을 지원하려면 해당 포털을 호스트하려는 노드에서 포털 정책 서비스를 활성화해야 합니다.

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

단계 **2** 노드를 클릭하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **General Settings(**일반 설정**)** 탭에서 **Policy Service(**정책 서비스**)** 토글 버튼을 활성화합니다.

단계 **4** **Enable Session Services(**세션 서비스 활성화**)** 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

디바이스 포털에 인증서 추가

기본 인증서를 사용하지 않으려는 경우 유효한 인증서를 추가하고 인증서 그룹 태그에 할당할 수 있습니다. 모든 최종 사용자 웹 포털에 사용되는 기본 인증서 그룹 태그는 **Default Portal Certificate Group(**기본 포털 인증서 그룹**)**입니다.

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

단계 **2** 시스템 인증서를 추가한 다음 포털에 사용하려는 인증서 그룹 태그에 할당합니다.

포털 생성 또는 편집 시에 이 인증서 그룹 태그를 선택할 수 있습니다.

단계 **3** **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **(**임의의 포털**)** > **Create or Edit(**생성 또는 편집**)** > **Portal Settings(**포털 설정**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **4** 새로 추가한 인증서와 연결된 특정 인증서 그룹 태그를 **Certificate Group Tag(**인증서 그룹 태그**)** 드롭다운 목록에서 선택합니다.

참고

- BYOD는 3개를 초과하는 인증서 체인을 지원하지 않습니다.
- BYOD 온보딩 중에는 iOS 디바이스용 인증서가 두 번 발급됩니다.

외부 **ID** 소스 생성

Cisco ISE는 Active Directory LDAP, RADIUS 토큰 및 RSA SecurID 서버와 같은 외부 ID 소스에 연결하여 인증 및 권한 부여를 위한 사용자 정보를 가져올 수 있습니다. 외부 ID 소스에는 인증서 기반 인증에 필요한 인증서 인증 프로파일도 포함되어 있습니다.

참고 인증된 사용자 ID를 수신하고 공유할 수 있는 패시브 ID 서비스를 사용하려면 추가 패시브 ID 서비스 제공자, 596 페이지의 내용을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **Identity Management(ID 관리)** > **External Identity Sources(외부 ID 소스)**를 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 인증서 기반 인증의 경우 **Certificate Authentication Profile(인증서 인증 프로파일)**을 선택합니다.
- 외부 ID 소스로 Active Directory에 연결하려는 경우 **Active Directory**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 Active Directory, 540 페이지를 참조하십시오.
- LDAP ID 소스를 추가하려는 경우 **LDAP**를 선택합니다. 자세한 내용은 LDAP, 640 페이지를 참조하십시오.
- RADIUS 토큰 서버를 추가하려는 경우 **RADIUS** 토큰을 선택합니다. 자세한 내용은 RADIUS 토큰 ID 소스, 665 페이지를 참조하십시오.
- RSA SecurID 서버를 추가하려는 경우 **RSA SecurID**를 선택합니다. 자세한 내용은 RSA ID 소스, 672 페이지를 참조하십시오.
- Oracle Access Manager 등의 IdP(Identity Provider)를 추가하려는 경우 **SAML Id Provider(SAML ID 제공자)**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 SAMLv2 ID 제공자, 679 페이지를 참조하십시오.
- 소셜 로그인(예: Facebook 등)을 외부 ID 소스로 추가하려면 **Social Login(소셜 로그인)**을 선택합니다. 자세한 내용은 셀프 등록 게스트의 소셜 로그인, 371 페이지을(를) 참조하십시오.

ID 소스 시퀀스 생성

시작하기 전에

Cisco ISE에서 외부 ID 소스를 구성했는지 확인합니다.

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

게스트 사용자가 로컬 WebAuth를 통해 인증하도록 허용하려면 게스트 포털 인증 소스와 ID 소스 시퀀스가 동일한 ID 저장소를 포함하도록 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **Identity Management(ID 관리)** > **Identity Source Sequences(ID 소스 시퀀스)** > **Add(추가)**를 선택합니다.

단계 **2** ID 소스 시퀀스의 이름을 입력합니다. 원하는 경우 설명을 입력할 수도 있습니다.

단계 **3** **Select Certificate Authentication Profile(인증서 인증 프로파일 선택)** 확인란을 선택하고 인증서 기반 인증용 인증서 인증 프로파일을 선택합니다.

단계 **4** ID 소스 시퀀스에 포함할 하나 이상의 데이터베이스를 **Selected List(선택됨 목록)** 필드에서 선택합니다.

단계 **5** Cisco ISE가 데이터베이스를 검색하도록 할 순서대로 **Selected List(선택됨 목록)** 필드의 데이터베이스를 다시 정렬합니다.

단계 6 **Advanced Search List(**고급 검색 목록**)** 영역에서 다음 옵션 중 하나를 선택합니다.

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError(**시퀀스의 다른 저장소에 액세스하지 않고 **AuthenticationStatus** 속성을 **ProcessError**로 설정**)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 검색을 중지하도록 하려면 이 옵션을 선택합니다.
- **Treat as if the user was not found and proceed to the next store in the sequence(**사용자를 찾지 못한 것으로 간주하여 다음 저장소로 순차 진행**)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 시퀀스에서 선택한 다른 ID 소스에서 검색을 계속하도록 하려면 이 옵션을 선택합니다.

  요청을 처리하는 동안 Cisco ISE는 이러한 ID 소스를 순서대로 검색합니다. Selected list(선택됨 목록) 필드의 ID 소스가 Cisco ISE가 검색하도록 할 순서대로 나열되어 있는지 확인합니다.

단계 7 ID 소스 시퀀스를 생성하려면 **Submit(**제출**)**을 클릭합니다. 생성된 시퀀스는 정책에서 사용할 수 있습니다.

엔드포인트 ID 그룹 생성

Cisco ISE는 검색되는 엔드포인트를 해당하는 엔드포인트 ID 그룹으로 그룹화합니다. Cisco ISE에서는 몇 가지 시스템 정의 엔드포인트 ID 그룹이 제공됩니다. 엔드포인트 **ID** 그룹 창에서 엔드포인트 ID 그룹을 추가로 생성할 수도 있습니다. 직접 생성한 엔드포인트 ID 그룹은 편집하거나 삭제할 수 있습니다. 시스템 정의 엔드포인트 ID 그룹의 경우 설명만 편집할 수 있습니다. 그 이름은 편집하거나 삭제할 수 없습니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Endpoint Identity Groups(**엔드포인트 **ID** 그룹**)**를 선택합니다.

단계 2 **Add(**추가**)**를 클릭합니다.

단계 3 생성할 엔드포인트 ID 그룹의 **Name(**이름**)**을 입력합니다(엔드포인트 ID 그룹의 이름에 공백 제외).

단계 4 생성할 엔드포인트 ID 그룹에 대한 **Description(**설명**)**을 입력합니다.

단계 5 **Parent Group(**부모 그룹**)** 드롭다운 목록을 클릭하여 새로 생성한 엔드포인트 ID 그룹을 연결할 엔드포인트 ID 그룹을 선택합니다.

단계 6 **Submit(**제출**)**을 클릭합니다.

차단 목록 포털 편집

Cisco ISE에서는 분실하거나 도난당하여 Cisco ISE에서 차단 목록에 포함되어 있는 디바이스가 회사 네트워크 액세스를 시도할 때 정보를 표시하는 단일 차단 목록 포털을 제공합니다.

기본 포털 설정을 편집하고 포털에 대해 표시되는 기본 메시지를 사용자 맞춤화하는 작업만 가능합니다. 새 차단 목록 포털을 생성하거나 기본 포털을 복제 또는 삭제할 수는 없습니다.

시작하기 전에

이 포털에 사용할 필수 인증서를 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Blocked List Portal(**차단 목록 포털**)** > **Edit(**편집**)**를 선택합니다.

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal test URL(**포털 테스트 **URL)** 링크를 클릭하여 이 포털의 URL을 표시하는 새 브라우저 탭을 엽니다. 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.

단계 **5** **Portal Settings(**포털 설정**)**를 확장합니다. 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

- **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.
- **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.

단계 **6** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭에서 권한이 없는 디바이스가 네트워크 액세스 권한을 얻으려고 할 때 포털에 표시되는 페이지 제목 및 메시지 텍스트를 사용자 맞춤화합니다.

단계 **7** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

BYOD 포털 생성

직원들이 개인 디바이스를 등록하도록 BYOD(Bring Your Own Device) 포털을 제공할 수 있습니다. 그러면 네트워크에 대한 액세스를 허용하기 전에 등록 및 supplicant 구성을 완료할 수 있습니다.

새 BYOD 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 BYOD 포털을 삭제할 수 있습니다.

Portal Behavior and Flow Settings(포털 동작 및 플로우 설정**)** 탭의 **Portal & Page Settings(**포털 및 페이지 설정**)**에 적용하는 모든 변경 사항은 디바이스 포털 플로우 다이어그램의 그래픽 플로우에 반영됩니다. 지원 정보 창과 같은 창을 활성화하면 흐름에 표시되고 직원이 해당 페이지를 포털에서 경험할 수 있습니다. 창을 비활성화하면 플로우에서 해당 창이 제거됩니다.

시작하기 전에

이 포털에 사용할 필수 인증서 및 엔드포인트 ID 그룹을 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **BYOD** > **Create(**만들기**)**를 선택합니다.

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 **5** **Portal Settings(**포털 설정**)**를 확장합니다. 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 **6** **Support Information Page Settings(**지원 정보 페이지 설정**)**를 확장합니다. 헬프 데스크에서 네트워크 액세스 문제를 해결하는 데 사용할 수 있는 정보를 직원들이 제공할 수 있도록 여기에서 필요한 정보를 업데이트합니다.

단계 **7** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 클릭합니다. 아래로 스크롤하여 **Page Customizations(**페이지 사용자 지정**)** 영역으로 이동하여 다음 최종 사용자 포털 창을 사용자 지정합니다. 왼쪽 메뉴의 **Pages(**페이지**)** 아래에 나열된 해당 옵션을 클릭하여 사용자 지정할 포털 창을 선택합니다.

- **BYOD Welcome(BYOD** 시작**)**:
  - **Device Configuration Required(**디바이스 구성 필요**)**: 디바이스가 BYOD 포털로 처음 리디렉션될 때 인증서 프로비저닝이 필요한 경우 표시될 콘텐츠를 입력합니다.

- **Certificate Needs Renewal(**인증서 갱신 필요**)**: 이전 인증서를 갱신해야 하는 경우 표시될 콘텐츠를 입력합니다.

- **BYOD Device Information(BYOD** 디바이스 정보**)**:
  - **Maximum Devices Reached(**최대 디바이스 수에 도달함**)**: 직원이 등록할 수 있는 최대 디바이스 제한에 도달하는 경우 표시될 콘텐츠를 입력합니다.
  - **Required Device Information(**필수 디바이스 정보**)**: 직원이 디바이스를 등록하는 데 필요한 디바이스 정보를 요청할 때 표시될 콘텐츠를 입력합니다.

- **BYOD Installation(BYOD** 설치**)**:
  - **Desktop Installation(**데스크톱 설치**)**: 데스크톱 디바이스에 대한 설치 정보를 제공할 때 표시될 콘텐츠를 입력합니다.
  - **iOS Installation(iOS** 설치**) -** iOS 모바일 디바이스에 대한 설치 지침을 제공할 때 표시될 콘텐츠를 입력합니다.
  - **Android Installation(iOS** 설치**)** - Android 모바일 디바이스에 대한 설치 지침을 제공할 때 표시될 콘텐츠를 입력합니다.

- **BYOD Success(BYOD** 성공**)**:
  - **Success(**성공**)**: 디바이스가 구성되어 네트워크에 자동으로 연결되면 표시될 콘텐츠를 입력합니다.
  - **Success: Manual Instructions(**성공**:** 수동 지침**)**: 디바이스가 구성되었으며 직원이 네트워크에 수동으로 연결해야 하는 경우 표시될 콘텐츠를 입력합니다.
  - **Success: Unsupported Device(**성공**:** 지원되지 않는 디바이스**)**: 지원되지 않는 디바이스가 네트워크에 연결할 수 있는 경우 표시될 콘텐츠를 입력합니다.

단계 **8** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

다음에 수행할 작업

포털을 사용하려면 권한을 부여해야 합니다. 포털 사용 권한을 부여하기 전이나 부여한 후에 포털을 사용자 맞춤화할 수도 있습니다.

인증서 프로비저닝 포털 생성

Cisco ISE에서는 온보딩 플로우를 통과할 수 없는 디바이스에 대해 인증서를 요청할 수 있는 인증서 프로비저닝 포털을 제공합니다. point-of-sale 터미널 등의 디바이스를 예로 들 수 있습니다. 단일 인증서를 요청하거나 CSV 파일을 사용하여 대량 인증서 요청을 수행할 수 있습니다.

기본 포털 설정을 편집하고 포털에 표시되는 메시지를 맞춤화할 수 있습니다. 또한 인증서 프로비저닝 포털을 생성, 복제 및 삭제할 수도 있습니다.

다음의 두 사용자 유형이 인증서 프로비저닝 포털에 액세스할 수 있습니다.

- 관리 권한이 있는 내부 또는 외부 사용자: 본인이나 다른 사용자를 위해 인증서를 생성할 수 있습니다.
- 기타 모든 사용자: 본인의 인증서만 생성할 수 있습니다.

슈퍼 관리자 또는 ERS 관리자 역할이 할당된 사용자(네트워크 액세스 사용자)는 이 포털에 액세스할 권한이 가지며 다른 사용자를 위한 인증서를 요청할 수 있습니다. 그러나 새 내부 관리 사용자를 생성하여 슈퍼 관리자 또는 ERS 관리자 역할을 할당하는 경우 해당 내부 관리 사용자에게는 이 포털에 액세스할 권한이 없습니다. 먼저 네트워크 액세스 사용자를 생성한 다음 슈퍼 관리자 또는 ERS 관리자 그룹에 해당 사용자를 추가해야 합니다. 슈퍼 관리자 또는 ERS 관리자 그룹에 추가되는 기존 네트워크 액세스 사용자에게는 이 포털에 액세스할 권한이 있습니다.

다른 사용자가 포털에 액세스하고 본인의 인증서를 생성할 수 있도록 하려면 인증서 프로비저닝 포털 설정을 구성합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Certificate Provisioning(**인증서 프로비저닝**)** > **Edit(**편집**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Portal Settings(**포털 설정**)**입니다. **Authentication Method(**인증 방법**)** 아래에서 적절한 ID 소스 또는 ID 소스 시퀀스를 선택하고 **Configure Authorized Groups(**권한이 부여된 그룹 구성**)**에서 사용자 그룹을 선택해야 합니다. 선택하는 그룹에 속한 모든 사용자는 포털에 액세스할 권한을 가지며 본인의 인증서를 생성할 수 있습니다.

시작하기 전에

이 포털에 사용할 필수 인증서를 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **CertificateProvisioning(**모바일 디바이스 관리**)** > **Create(**생성**)**를 선택합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 **5** **Portal Settings(**포털 설정**)**를 확장합니다. 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 **6** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 클릭합니다. 포털에 나타나는 페이지 제목 및 메시지 텍스트를 맞춤화합니다.

단계 **7** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

클라이언트 프로비저닝 포털 생성

직원들이 Cisco AnyConnect 포스처 구성 요소를 다운로드할 수 있는 클라이언트 프로비저닝 포털을 제공할 수 있습니다. 이 포털은 네트워크 액세스를 허용하기 전에 디바이스의 포스처 규정 준수를 확인합니다.

새 클라이언트 프로비저닝 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 클라이언트 프로비저닝 포털을 삭제할 수 있습니다.

슈퍼 관리자 또는 ERS 관리자 역할이 할당된 사용자(네트워크 액세스 사용자)는 이 포털에 액세스할 수 있습니다. 그러나 새 내부 관리 사용자를 생성하여 슈퍼 관리자 또는 ERS 관리자 역할을 할당하는 경우 해당 내부 관리 사용자에게는 이 포털에 액세스할 권한이 없습니다. 먼저 네트워크 액세스 사용자를 생성한 다음 슈퍼 관리자 또는 ERS 관리자 그룹에 해당 사용자를 추가해야 합니다. 슈퍼 관리자 또는 ERS 관리자 그룹에 추가되는 기존 네트워크 액세스 사용자에게는 이 포털에 액세스할 권한이 있습니다.

다른 사용자가 포털에 액세스하고 본인의 인증서를 생성할 수 있도록 하려면 인증서 프로비저닝 포털 설정을 구성합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Edit(**편집**)** > **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** > **Portal Settings(**포털 설정**)**입니다. **Authentication Method(**인증 방법**)** 아래에서 적절한 ID 소스 또는 ID 소스 시퀀스를 선택하고 **Configure Authorized Groups(**권한이 부여된 그룹 구성**)**에서 사용자 그룹을 선택해야 합니다. 선택하는 그룹에 속한 모든 사용자는 포털에 액세스할 권한을 가지며 본인의 인증서를 생성할 수 있습니다.

Portal Behavior and Flow Settings(포털 동작 및 플로우 설정**)** 탭의 **Portal & Page Settings(**포털 및 페이지 설정**)**에 적용하는 모든 변경 사항은 디바이스 포털 플로우 다이어그램의 그래픽 플로우에 반영됩니다. 지원 정보 창과 같은 창을 활성화하면 흐름에 표시되고 직원이 해당 페이지를 포털에서 경험할 수 있습니다. 창을 비활성화하면 플로우에서 해당 창이 제거됩니다.

시작하기 전에

이 포털에 사용할 필수 인증서 및 클라이언트 프로비저닝 정책을 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Create(**생성**)**를 선택합니다.

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

포털 이름 확인

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 **5** **Portal Settings(**포털 설정**)**를 확장합니다. 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 **6** **Support Information Page Settings(**지원 정보 페이지 설정**)**를 확장합니다. 헬프 데스크에서 네트워크 액세스 문제를 해결하는 데 사용할 수 있는 정보를 직원들이 제공할 수 있도록 여기에서 필요한 정보를 업데이트합니다.

단계 **7** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 클릭합니다. 아래로 스크롤하여 **Page Customizations(**페이지 사용자 지정**)** 영역으로 이동하여 다음 최종 사용자 포털 창을 사용자 지정합니다. 왼쪽 메뉴의 **Pages(**페이지**)** 아래에 나열된 해당 옵션을 클릭하여 사용자 지정할 포털 창을 선택합니다.

- 클라이언트 프로비저닝 포털:
  - **Agent Unknown(**에이전트 알 수 없음**)**: 에이전트를 알 수 없을 경우 표시할 내용을 입력합니다.

- **Checking**, **Scanning** and **Compliant**(확인, 스캔 및 규정 준수): 포스처 에이전트가 설치되어 디바이스가 포스처 요건을 준수하는지 확인, 스캔 및 검증할 때 표시할 내용을 입력합니다.
- **Non-compliant**(미준수): 포스처 에이전트에서 디바이스가 포스처 요건을 준수하지 않는다고 판단할 경우 표시할 내용을 입력합니다.

- 클라이언트 프로비저닝(에이전트를 찾을 수 없음):
  - **Agent Not Found**(에이전트를 찾을 수 없음): 디바이스에 포스처 에이전트가 탐지되지 않을 경우 표시할 내용을 입력합니다.
  - **Manual Installation Instructions**(수동 설치 지침): 디바이스에 Java 또는 ActiveX 소프트웨어가 설치되어 있지 않을 경우 표시할 내용과 포스처 에이전트를 수동으로 다운로드하고 설치하는 방법에 대한 지침을 입력합니다.
  - **Install, No Java/ActiveX**(설치, **Java/ActiveX** 없음): 디바이스에 Java 또는 ActiveX 소프트웨어가 설치되어 있지 않을 경우 표시할 내용과 Java 플러그인을 다운로드하고 설치하는 방법에 대한 지침을 입력합니다.
  - **Agent Installed**(에이전트 설치됨): 디바이스에 포스처 에이전트가 탐지될 경우 표시할 내용과 포스처 에이전트를 시작하는 방법에 대한 지침을 입력하여 디바이스가 포스처 요건을 준수하는지 확인합니다.

단계 **8** **Save**(저장), **Close**(닫기)를 차례로 클릭합니다.

다음에 수행할 작업

포털을 사용하려면 권한을 부여해야 합니다. 포털 사용 권한을 부여하기 전이나 부여한 후에 포털을 사용자 맞춤화할 수도 있습니다.

관련 항목

포털 권한 부여, 388 페이지
디바이스 포털 사용자 맞춤화, 815 페이지

MDM 포털 생성

직원들이 회사 네트워크에서 사용하도록 등록한 모바일 디바이스를 관리할 수 있도록 MDM(Mobile Device Management) 포털을 제공할 수 있습니다.

새 MDM 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. 모든 MDM 시스템에 대해 단일 MDM 포털을 지정할 수도 있고 각 시스템용 포털을 생성할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 MDM 포털을 삭제할 수 있습니다. 기본 포털은 타사 MDM 제공자용입니다.

새 MDM 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 MDM 포털을 삭제할 수 있습니다. 기본 포털은 타사 MDM 제공자용입니다.

Portal Behavior and Flow Settings(포털 동작 및 플로우 설정) 탭의 **Portal & Page Settings**(포털 및 페이지 설정)에 적용하는 모든 변경 사항은 디바이스 포털 플로우 다이어그램의 그래픽 플로우에 반영

됩니다. 지원 정보 창과 같은 창을 활성화하면 흐름에 표시되고 직원이 해당 페이지를 포털에서 경험할 수 있습니다. 창을 비활성화하면 플로우에서 해당 창이 제거됩니다.

시작하기 전에

이 포털에 사용할 필수 인증서 및 엔드포인트 ID 그룹을 구성했는지 확인해 주십시오.

단계 1 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Mobile Device Management(**모바일 디바이스 관리**)** > **Create, Edit or Duplicate(**생성**,** 편집 또는 복제**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 2 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 3 **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 4 **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 5 **Portal Settings(**포털 설정**)**를 확장합니다. 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 6 **Employee Mobile Device Management Settings(**직원 모바일 디바이스 관리 설정**)**를 확장합니다. 타사 MDM 제공자를 구성할 수 있도록 제공된 링크에 액세스한 다음 MDM 포털을 사용하는 직원에 대한 수락 정책 동작을 정의합니다.

단계 7 **Support Information Page Settings(**지원 정보 페이지 설정**)**를 확장합니다. 헬프 데스크에서 네트워크 액세스 문제를 해결하는 데 사용할 수 있는 정보를 직원들이 제공할 수 있도록 여기에서 필요한 정보를 업데이트합니다.

단계 8 **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭을 클릭합니다.

단계 9 디바이스 등록 프로세스를 진행하는 동안 MDM 포털에 나타나는 **Content Area(**콘텐츠 영역**)** 메시지를 사용자 지정합니다.

- **Unreachable(**연결할 수 없음**)**: 선택한 MDM 시스템에 연결할 수 없는 경우에 표시될 콘텐츠를 입력합니다.
- **Non-compliant(**미준수**)**: 등록 대상 디바이스가 MDM 시스템 요건을 준수하지 않을 때 표시될 콘텐츠를 입력합니다.
- **Continue(**계속**)**: 연결 문제 발생 시 디바이스가 네트워크 연결을 시도해야 하는 경우 표시될 콘텐츠를 입력합니다.
- **Enroll(**등록**)**: 디바이스에 MDM 에이전트가 필요하며 MDM 시스템에 디바이스를 등록해야 하는 경우 표시될 콘텐츠를 입력합니다.

단계 10 **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

다음에 수행할 작업

포털을 사용하려면 권한을 부여해야 합니다. 포털 사용 권한을 부여하기 전이나 부여한 후에 포털을 사용자 맞춤화할 수도 있습니다. 다음 항목도 참고하십시오.

- 디바이스 포털에 인증서 추가, 802 페이지
- 엔드포인트 ID 그룹 생성, 804 페이지

• 권한 부여 프로파일 생성, 814 페이지
• 디바이스 포털 사용자 맞춤화, 815 페이지

내 디바이스 포털 생성

직원들이 기본 신청자를 지원하지 않으며 BYOD(Bring Your Own Device) 포털을 사용하여 추가할 수 없는 개인 디바이스를 추가하고 등록할 수 있도록 내 디바이스 포털을 제공할 수 있습니다. 그런 다음 내 디바이스 포털을 사용하여 두 포털 중 하나를 사용해 추가된 모든 디바이스를 관리할 수 있습니다.

새 내 디바이스 포털을 생성할 수도 있고 기존 포털을 편집하거나 복제할 수도 있습니다. Cisco ISE에서 제공하는 기본 포털을 포함하여 모든 내 디바이스 포털을 삭제할 수 있습니다.

Portal Behavior and Flow Settings(포털 동작 및 플로우 설정**)** 탭의 **Portal & Page Settings(**포털 및 페이지 설정**)**에 적용하는 모든 변경 사항은 디바이스 포털 플로우 다이어그램의 그래픽 플로우에 반영됩니다. 지원 정보 창과 같은 창을 활성화하면 흐름에 표시되고 직원이 해당 페이지를 포털에서 경험할 수 있습니다. 창을 비활성화하면 플로우에서 해당 창이 제거됩니다.

시작하기 전에

이 포털에 사용할 필요한 인증서, 외부 ID 소스, ID 소스 시퀀스 및 엔드포인트 ID 그룹을 구성했는지 확인해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **My Devices(**내 디바이스**)** > **Create(**생성**)**를 선택합니다.

단계 **2** 포털의 고유한 **Portal Name(**포털 이름**)** 및 **Description(**설명**)**을 입력합니다.

여기서 사용하는 포털 이름은 다른 최종 사용자 포털에서 사용되지 않는 이름이어야 합니다.

단계 **3** **Language File(**언어 파일**)** 드롭다운 메뉴에서 포털에 사용할 언어 파일을 내보내고 가져오는 작업을 선택합니다.

단계 **4** **Portal Behavior and Flow Settings(**포털 동작 및 플로우 설정**)** 탭을 클릭합니다.

단계 **5** **Portal Settings(**포털 설정**)**를 확장하여 포트, 인증서 그룹 태그, 엔드포인트 ID 그룹 등에 대한 기본값을 업데이트하고 전체 포털에 적용되는 동작을 정의합니다.

단계 **6** **Login Page Settings(**로그인 페이지 설정**)**를 확장하여 직원 자격 증명 및 로그인 지침을 지정합니다.

단계 **7** **Acceptable Use Policy (AUP) Page Settings(AUP** 페이지 설정**)**을 확장하여 별도의 AUP 페이지를 추가하고 직원에 대한 사용 제한 정책 동작을 정의합니다.

단계 **8** **Post-Login Banner Page Settings(**로그인 후 배너 페이지 설정**)**를 확장하여 직원이 포털에 로그인한 후 추가 정보를 알립니다.

단계 **9** **Employee Change Password Settings(**직원 비밀번호 변경 설정**)**를 확장하여 직원이 비밀번호를 직접 변경하도록 허용합니다. 이 옵션은 직원이 내부 사용자 데이터베이스에 포함되어 있는 경우에만 활성화됩니다.

단계 **10** **Portal Page Customization(**포털 페이지 사용자 맞춤화**)** 탭에서 등록 및 관리 중에 내 디바이스 포털에 표시되는 다음 정보를 사용자 맞춤화합니다.

- 제목, 지침, 내용, 필드 및 버튼 레이블

- 오류 메시지 및 알림 메시지

단계 **11** **Save(**저장**)**, **Close(**닫기**)**를 차례로 클릭합니다.

다음에 수행할 작업

포털 모양을 변경하려는 경우 포털을 사용자 맞춤화할 수 있습니다.

관련 항목

디바이스 포털 사용자 맞춤화, 815 페이지
내 디바이스 포털, 795 페이지
직원이 추가한 디바이스 표시, 816 페이지

권한 부여 프로파일 생성

포털에 권한을 부여할 때는 네트워크 액세스를 위한 규칙과 네트워크 권한 부여 프로파일을 설정합니다.

시작하기 전에

포털에 권한을 부여하려면 먼저 포털을 생성해야 합니다.

단계 **1** 포털에 대해 특수 권한 부여 프로파일을 설정합니다.

단계 **2** 프로파일에 대한 권한 부여 정책 규칙을 생성합니다.

권한 부여 프로파일 생성

각 포털에서는 해당 포털용으로 특수 권한 부여 프로파일을 설정해야 합니다.

시작하기 전에

기본 포털을 사용하지 않으려는 경우에는 포털 이름을 권한 부여 프로파일과 연결할 수 있도록 먼저 포털을 생성해야 합니다.

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

단계 **2** 사용하기 위해 권한을 부여하려는 포털의 이름을 사용하여 권한 부여 프로파일을 생성합니다.

다음에 수행할 작업

새로 생성한 권한 부여 프로파일을 사용하는 포털 권한 부여 정책 규칙을 생성해야 합니다.

권한 부여 정책 규칙 생성

사용자(게스트, 스폰서, 직원)의 액세스 요청에 응답할 때 포털에서 사용하도록 할 리디렉션 URL을 구성하려면 해당 포털용 권한 부여 정책 규칙을 정의합니다.

URL 리디렉션은 포털 유형에 따라 다음 형식을 사용합니다.

ip:port: IP 주소와 포트 번호입니다.

PortalID: 고유한 포털 이름입니다.

핫스팟 게스트 포털:
https://*ip:port*/guestportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=cwa&type=drw

MDM(Mobile Device Management) 포털:
https://*ip:port*/mdmportal/gateway?sessionID=SessionIdValue&portal=*PortalID*&action=mdm

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택하여 **Standard(**표준**)** 정책 아래에 새 권한 부여 정책 규칙을 생성합니다.

단계 **2** **Conditions(**조건**)**에 대해 포털 검증에 사용할 엔드포인트 ID 그룹을 선택합니다. 예를 들어 핫스팟 게스트 포털의 경우 기본값인 **GuestEndpoints** 엔드포인트 ID 그룹을 선택하고 MDM 포털의 경우 기본값인 **RegisteredDevices** 엔드포인트 ID 그룹을 선택합니다.

참고 핫스팟 게스트 포털에서는 종료 CoA만 발급하므로 핫스팟 게스트 권한 부여 정책의 검증 조건 중 하나로 Network Access:UseCase EQUALS Guest Flow를 사용하지 마십시오. 대신 검증을 위해 엔드포인트가 속하는 ID 그룹을 일치시킵니다. 예를 들면 다음과 같습니다.

- `If GuestEndpoint + Wireless MAB then Permit Access`
- `If Wireless MAB then HotSpot Redirect`

단계 **3** **Permissions(**권한**)**에 대해 생성한 포털 권한 부여 프로파일을 선택합니다.

참고 MAC 옵션이 활성화된 사전 속성(예: RADIUS.Calling-Station-ID)을 사용하여 권한 부여 조건을 생성하는 동안 Mac 연산자(예: Mac_equals)로 다른 MAC 형식을 지원해야 합니다.

디바이스 포털 사용자 맞춤화

포털 테마를 사용자 맞춤화하고, 포털 페이지의 UI 요소를 변경하고, 사용자에게 표시되는 오류 메시지와 알림을 편집하여 포털 모양과 사용자(해당하는 게스트, 스폰서 또는 직원) 환경을 사용자 맞춤화할 수 있습니다. 포털 사용자 맞춤화에 대한 자세한 내용은 의 최종 사용자 웹 포털 사용자 맞춤화 섹션을 참조하십시오.

직원이 추가한 개인 디바이스 관리

직원이 BYOD(Bring Your Own Device) 또는 내 디바이스 포털을 사용하여 등록하는 디바이스는 **Endpoints(**엔드포인트**)** 목록에 표시됩니다. 직원은 디바이스를 삭제하여 계정에서 디바이스 연결을 끊을 수는 있지만 Cisco ISE 데이터베이스에는 해당 디바이스가 유지됩니다. 따라서 직원은 디바이스로 작업을 할 때 발생하는 오류를 해결하기 위해 관리자의 지원을 받아야 할 수 있습니다.

직원이 추가한 디바이스 표시

Endpoints(엔드포인트**)** 목록 창에 표시되는 **Portal User(**포털 사용자**)** 필드를 사용하여 특정 직원이 추가한 디바이스를 찾을 수 있습니다. 이렇게 하면 특정 사용자가 등록한 디바이스를 삭제해야 하는 경우 유용할 수 있습니다. 이 필드는 기본적으로 표시되지 않으므로 검색 전에 먼저 필드를 활성화해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**를 선택합니다.

단계 **2** dashlet 아래의 엔드포인트 목록 오른쪽 상단에서 사용 가능한 **Settings(**설정**)** 아이콘을 클릭합니다.

단계 **3** **Portal User(**포털 사용자**)** 확인란을 선택합니다. **Portal User(**포털 사용자**)** 토글 버튼을 활성화하여 정보를 엔드포인트 목록에 표시합니다.

단계 **4** **Go(**이동**)**를 클릭합니다.

단계 **5** **Filter(**필터**)** 드롭다운 목록을 클릭하고 **Quick Filter(**빠른 필터**)**를 선택합니다.

단계 **6** 해당 특정 사용자에게 할당된 엔드포인트만 표시하려면 **Portal User(**포털 사용자**)** 필드에 사용자 이름을 입력합니다.

내 디바이스 포털에 디바이스를 추가할 때의 오류

직원은 다른 직원이 이미 추가한 디바이스를 또 추가할 수 없으며 해당 디바이스는 그대로 엔드포인트 데이터베이스에 남게 됩니다.

직원이 Cisco ISE 데이터베이스에 이미 있는 디바이스를 추가하려는 경우 다음을 수행해야 합니다.

- 기본 신청자 프로비저닝이 지원되는 경우 BYOD 포털을 통해 디바이스를 추가하는 것이 좋습니다. 이렇게 하면 디바이스를 네트워크에 처음 추가할 때 생성된 등록 세부정보를 덮어쓰게 됩니다.
- 디바이스가 프린터 등의 MAB(MAC Authentication Bypass) 디바이스인 경우에는 먼저 디바이스 소유권을 확인해야 합니다. 해당하는 경우에는 관리자 포털을 사용하여 엔드포인트 데이터베이스에서 디바이스를 제거할 수 있습니다. 그러면 새 소유자가 내 디바이스 포털을 사용하여 디바이스를 정상적으로 추가할 수 있습니다.

참고 관리자 포털이 작동 중지된 경우 내 디바이스 포털을 사용할 수 없습니다.

내 디바이스 포털에서 삭제된 디바이스가 엔드포인트 데이터베이스에 남아 있음

직원이 내 디바이스 포털에서 디바이스를 삭제하는 경우 직원의 등록된 디바이스 목록에서 디바이스가 제거됩니다. 하지만 이 디바이스는 Cisco ISE 엔드포인트 데이터베이스에서 유지되며 엔드포인트 목록에 표시됩니다.

엔드포인트 창에서 디바이스를 영구적으로 삭제할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**입니다.

직원이 등록하는 개인 디바이스의 수 제한

직원이 1~100개의 개인 디바이스를 등록하도록 허용할 수 있습니다. 직원이 개인 디바이스를 등록하는 데 사용하는 포털과는 관계없이 이 설정은 모든 포털에서 등록할 수 있는 최대 디바이스 수를 정의합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Settings(**설정**)** > **Employee Registered Devices(**직원 등록 디바이스**)**를 선택합니다.

단계 **2** **Restrict employees to(**직원의 등록 수 제한**)** 필드에 직원이 등록할 수 있는 최대 디바이스 수를 입력합니다. 기본적으로 이 값은 디바이스 **5**개로 설정됩니다.

단계 **3** **Save(**저장**)**를 클릭합니다. 설정에 대한 업데이트를 저장하지 않으려면 **Reset(**재설정**)**을 클릭하여 마지막으로 저장한 값으로 되돌립니다.

내 디바이스 포털 및 엔드포인트 활동 모니터링

Cisco ISE에서는 엔드포인트 및 사용자 관리 정보와 게스트 및 스폰서 활동을 확인할 수 있는 다양한 보고서 및 로그를 제공합니다.

온디맨드 또는 예약 방식으로 이러한 보고서를 실행할 수 있습니다.

단계 **1** **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 다양한 게스트, 스폰서 및 엔드포인트 관련 보고서를 보려면 **Guest(**게스트**)** 또는 **Endpoints and Users(**엔드포인트 및 사용자**)**를 선택합니다.

단계 **3** **Filters(**필터**)** 드롭다운 목록을 사용하여 검색에 사용할 데이터를 선택합니다.

단계 **4** 데이터를 확인할 **Time Range(**시간 범위**)**를 선택합니다.
단계 **5** **Run(**실행**)**을 클릭합니다.

내 디바이스 로그인 및 감사 보고서

내 디바이스 로그인 및 감사 보고서는 다음을 추적하는 종합 보고서입니다.

- 내 디바이스 포털에서 직원이 수행하는 로그인 작업
- 내 디바이스 포털에서 직원이 수행하는 디바이스 관련 작업

이 보고서는**Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Guest(**게스트**)** > **My Devices Login and Audit(**내 디바이스 로그인 및 감사**)**에서 확인 가능합니다.

등록된 엔드포인트 보고서

등록된 엔드포인트 보고서는 직원이 등록한 모든 엔드포인트에 대한 정보를 제공합니다. 이 보고서는**Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **Registered Endpoints(**등록된 엔드포인트**)**에서 확인 가능합니다. **Identity(ID)**, **Endpoint ID(**엔드포인트 **ID)**, **Identity Group(ID** 그룹**)**, **Endpoint Profile(**엔드포인트 프로파일**)** 등의 속성을 기준으로 필터링하고 보고서를 생성할 수 있습니다.

엔드포인트 데이터베이스를 쿼리하여 **Registered Endpoints(**등록된 디바이스**)** 엔드포인트 ID 그룹에 할당된 엔드포인트를 확인할 수 있습니다. 또한 포털 사용자 속성 집합이 null이 아닌 값으로 설정된 특정 사용자에 대한 보고서를 생성할 수도 있습니다.

등록된 엔드포인트 보고서는 선택한 기간 동안 특정 사용자가 디바이스 등록 포털을 통해 등록한 엔드포인트 목록에 대한 정보를 제공합니다.

10 장

보안 유선 액세스

Cisco ISE의 네트워크 디바이스 정의

스위치 또는 라우터와 같은 네트워크 디바이스는 AAA(Authentication, Authorization, Accounting) 서비스 요청이 Cisco ISE로 전송될 때 사용되는 AAA 클라이언트입니다. Cisco ISE와 네트워크 디바이스 간의 상호 작용을 활성화하려면 Cisco ISE에서 네트워크 디바이스를 정의합니다.

프로파일링 서비스에 대해 RADIUS 또는 TACACS AAA, SNMP(Simple Network Management Protocol)용 네트워크 디바이스를 구성하여 프로파일링 엔드포인트용 Cisco Discovery Protocol 및 LLDP(Link Layer Discovery Protocol) 속성과 Cisco TrustSec 디바이스용 TrustSec 속성을 수집할 수 있습니다. Cisco ISE에 정의되지 않은 네트워크 디바이스는 Cisco ISE에서 AAA 서비스를 받을 수 없습니다.

네트워크 디바이스 정의에서는 다음을 수행합니다.

- 네트워크 디바이스에 적합한 벤더 프로파일을 선택합니다. 프로파일에는 URL 리디렉션 및 Change of Authorization용 설정과 같이 디바이스용으로 미리 정의된 컨피그레이션이 포함됩니다.
- RADIUS 인증용 RADIUS 프로토콜을 구성합니다. Cisco ISE가 네트워크 디바이스에서 RADIUS 요청을 받으면 해당 디바이스 정의를 찾아 구성된 공유 암호를 검색합니다. Cisco ISE가 디바이스 정의를 찾으면 해당 디바이스에 구성된 공유 암호를 가져와 액세스 인증을 위해 요청의 공유 암호와 일치하는지 확인합니다. 공유 암호가 일치하면 RADIUS 서버는 정책과 컨피그레이션을 기준으로 하여 요청을 추가로 처리합니다. 공유 암호가 일치하지 않으면 네트워크 디바이스에 거부 응답이 전송됩니다. 실패 이유를 제공하는 실패한 인증 보고서가 생성됩니다.

- TACACS+ 인증용 TACACS+ 프로토콜을 구성합니다. Cisco ISE는 네트워크 디바이스에서 TACACS+ 요청을 받으면 해당 디바이스 정의를 찾아 구성된 공유 암호를 검색합니다. 디바이스 정의가 발견되면 디바이스에 구성된 공유 암호를 가져와 액세스 인증을 위해 요청의 공유 암호와 일치하는지 확인합니다. 공유 암호가 일치하면 TACACS+ 서버는 정책과 컨피그레이션을 기준으로 하여 요청을 추가로 처리합니다. 일치하지 않으면 네트워크 디바이스에 거부 응답이 전송됩니다. 실패 이유를 제공하는 실패한 인증 보고서가 생성됩니다.
- 네트워크 디바이스 정의에서 프로파일링 서비스가 네트워크 디바이스 및 네트워크 디바이스에 연결된 프로파일 엔드포인트와 통신하도록 SNMP(Simple Network Management Protocol)를 구성할 수 있습니다.
- Cisco Trustsec 솔루션에 속할 수 있는 TrustSec 지원 디바이스의 요청을 처리하도록 Cisco ISE에서 Cisco TrustSec 지원 디바이스를 정의해야 합니다. Cisco TrustSec 솔루션을 지원하는 모든 스위치는 Cisco TrustSec 지원 디바이스입니다.

  Cisco TrustSec 디바이스는 IP 주소를 사용하지 않습니다. 대신 Cisco TrustSec 디바이스가 Cisco ISE와 통신할 수 있도록 다른 설정을 정의해야 합니다.

  Cisco TrustSec 지원 디바이스는 TrustSec 속성을 사용하여 Cisco ISE와 통신합니다. Nexus 7000 Series 스위치, Catalyst 6000 Series 스위치, Catalyst 4000 Series 스위치 및 Catalyst 3000 Series 스위치와 같은 Cisco TrustSec 지원 디바이스는 Cisco TrustSec 디바이스를 추가하는 동안 정의된 Trustsec 속성을 사용하여 인증됩니다.

참고 Cisco ISE에서 네트워크 디바이스를 구성할 때는 공유 암호에 백슬래시(\)를 포함하지 않는 것이 좋습니다. Cisco ISE를 업그레이드할 때 백슬래시가 공유 암호에 표시되지 않기 때문입니다. 단, Cisco ISE를 업그레이드하는 대신 재이미지화하는 경우 백슬래시가 공유 암호에 나타납니다.

Cisco ISE의 기본 네트워크 디바이스 정의

Cisco ISE는 RADIUS 및 TACACS 인증을 위한 기본 디바이스 정의를 지원합니다. Cisco ISE가 특정 IP 주소에 대한 디바이스 정의를 발견하지 못하는 경우에 사용할 수 있는 기본 네트워크 디바이스를 정의할 수 있습니다. 이 기능을 사용하면 새로 프로비저닝된 디바이스에 대한 기본 RADIUS 또는 TACACS 공유 암호 및 액세스 레벨을 정의할 수 있습니다.

참고 기본 RADIUS 및 TACACS 인증에 대해서만 기본 디바이스 정의를 추가하는 것이 좋습니다. 고급 플로우에서는 각 네트워크 디바이스에 대한 별도의 디바이스 정의를 추가해야 합니다.

Cisco ISE는 네트워크 디바이스에서 RADIUS 또는 TACACS 요청을 수신하면 해당 디바이스 정의를 찾아 네트워크 디바이스 정의에 구성된 공유 암호를 검색합니다.

RADIUS 또는 TACACS 요청이 수신되는 경우 Cisco ISE는 다음 절차를 수행합니다.

1. 요청의 IP 주소와 일치하는 특정 IP 주소를 찾습니다.
2. 범위를 조회하여 요청의 IP 주소가 지정된 범위 안에 포함되는지 확인합니다.

3. 1단계와 2단계 모두 실패하는 경우 기본 디바이스 정의(정의된 경우)를 사용하여 요청을 처리합니다.

Cisco ISE는 해당 디바이스의 디바이스 정의에 구성된 공유 암호를 가져온 다음 RADIUS 또는 TACACS 요청의 공유 암호와 일치하는지 확인하여 액세스를 인증합니다. 디바이스 정의를 찾을 수 없는 경우 Cisco ISE는 기본 네트워크 디바이스 정의에서 공유 암호를 가져와 RADIUS 또는 TACACS 요청을 처리합니다.

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 ***110:*** 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.
Description(설명**)**	디바이스에 대한 설명을 입력합니다.

필드 이름	설명
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 ***111: 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 포트를 사용하려면 **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 ***112: 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 ***113: 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 ***114:*** 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 붙여 넣어야 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 ***115: 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.

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 ***116:*** 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.
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.

Cisco ISE에서 네트워크 디바이스 추가

Cisco ISE에서 네트워크 디바이스를 추가하거나 기본 네트워크 디바이스를 사용할 수 있습니다.

Network Devices(네트워크 디바이스**)(Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**))** 창에서 네트워크 디바이스를 추가할 수도 있습니다.

시작하기 전에

추가할 네트워크 디바이스에서 AAA 기능을 활성화해야 합니다. 릴리스에 대한 *Cisco ISE* 관리자 가이드의 "통합" 장에서 "AAA 기능을 활성화하는 명령" 섹션을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)**, **Description(**설명**)** 및 **IP Address(IP** 주소**)** 필드에 해당 값을 입력합니다.

단계 **4** 드롭다운 목록에서 **Device Profile(**디바이스 프로파일**)**, **Model Name(**모델 이름**)**, **Software Version(**소프트웨어 버전**)** 및 **Network Device Group(**네트워크 디바이스 그룹**)** 필드에 필요한 값을 선택합니다.

단계 **5** (선택 사항) 인증용 RADIUS 프로토콜을 구성하려면 **RADIUS Authentication Settings(RADIUS** 인증 설정**)** 확인란을 선택합니다.

단계 **6** (선택 사항) 인증용 TACACS 프로토콜을 구성하려면 **TACACS Authentication Settings(TACACS** 인증 설정**)** 확인란을 선택합니다.

단계 **7** (선택 사항) 네트워크 디바이스에서 정보를 수집하기 위해 Cisco ISE 프로파일링 서비스용으로 SNMP를 구성하려면 **SNMP Settings(SNMP** 설정**)** 확인란을 선택합니다.

단계 **8** (선택 사항) Cisco TrustSec이 활성화된 디바이스를 구성하려면 **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)** 확인란을 선택합니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

Cisco ISE로 네트워크 디바이스 가져오기

Cisco ISE가 네트워크 디바이스와 통신하도록 하려면 Cisco ISE에서 네트워크 디바이스의 디바이스 정의를 추가해야 합니다. **Network Devices(**네트워크 디바이스**)** 창(메인 메뉴에서 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**))**을 통해 Cisco ISE로 네트워크 디바이스의 디바이스 정의를 가져옵니다.

CSV(comma-separated value) 파일을 사용하여 Cisco ISE 노드로 디바이스 정의 목록을 가져옵니다. **Network Devices(**네트워크 디바이스**)** 창에서 **Import(**가져오기**)**를 클릭하면 CSV 템플릿 파일을 사용할 수 있습니다. 해당 파일을 다운로드하고 원하는 디바이스 정의를 입력한 다음, **Import(**가져오기**)** 창을 통해 편집한 파일을 업로드합니다.

같은 리소스 유형의 가져오기를 동시에 여러 개 실행할 수는 없습니다. 예를 들어 서로 다른 두 가져오기 파일에서 네트워크 디바이스를 동시에 가져올 수는 없습니다.

디바이스 정의의 CSV 파일을 가져올 때 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 옵션을 클릭하여 새 기록을 생성하거나 기존 기록을 업데이트할 수 있습니다.

가져오기 템플릿은 Cisco ISE마다 다를 수 있습니다. 다른 Cisco ISE 릴리스에서 내보낸 네트워크 디바이스의 CSV 파일을 가져오지 마십시오. 릴리스의 CSV 템플릿 파일에 네트워크 디바이스의 세부 정보를 입력하고 해당 파일을 Cisco ISE로 가져옵니다.

참고 모든 octet의 IP 범위가 있는 네트워크 디바이스를 가져올 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** 표시되는 **Import Network Devices(**네트워크 디바이스 가져오기**)** 창에서 **Generate A Template(**템플릿 생성**)**을 클릭하여 CSV 파일을 다운로드합니다. 이 파일을 편집해서 필요한 세부정보를 포함하여 Cisco ISE로 가져올 수 있습니다.

단계 **4** **Choose File(**파일 선택**)**을 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 CSV 파일을 선택합니다.

단계 **5** (선택 사항) 필요에 따라 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 및 **Stop Import on First Error(**첫 번째 오류에서 가져오기 중지**)** 확인란을 선택합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.

파일을 모두 가져오면 Cisco ISE에 요약 메시지가 표시됩니다. 요약 메시지에는 가져오기 상태(성공 또는 실패), 발생한 오류 수(있는 경우), 파일 가져오기 프로세스에 소요된 총 처리 시간이 포함됩니다.

Cisco ISE에서 네트워크 디바이스 내보내기

Cisco ISE 노드에서 사용 가능한 네트워크 디바이스의 디바이스 정의를 CSV 파일 형식으로 내보낼 수 있습니다. 그런 다음 필요한 Cisco ISE 노드에서 디바이스 정의를 사용할 수 있도록 이 CSV 파일을 다른 Cisco ISE 노드로 가져올 수 있습니다.

참고 모든 octet의 IP 범위가 있는 네트워크 디바이스를 내보낼 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택합니다.

단계 **2** **Export(**내보내기**)**를 클릭합니다.

단계 **3** 다음 작업 중 하나를 수행하여 Cisco ISE 노드에 추가된 네트워크 디바이스에 대한 디바이스 정의를 내보냅니다.

- 내보낼 디바이스 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭하여 드롭다운 목록에서 **Export Selected(**선택 항목 내보내기**)**를 선택합니다.

- **Export(**내보내기**)**를 클릭하고 드롭다운 목록에서 **Export All(**모두 내보내기**)**을 선택하여 Cisco ISE 노드에 추가된 모든 네트워크 디바이스를 내보냅니다.

단계 **4** 두 경우 모두 디바이스 정의에 대한 CSV 파일이 시스템에 다운로드됩니다.

네트워크 디바이스 컨피그레이션 문제 해결

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고**Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Evaluate Configuration Validator(**구성 검증기 평가**)**를 선택합니다.

단계 **2** 구성을 평가할 네트워크 디바이스의 IP 주소를 **Network Device IP(**네트워크 디바이스 **IP)** 필드에 입력합니다.

단계 **3** 확인란을 선택하고 권장 템플릿과 비교할 구성 옵션 옆의 라디오 버튼을 클릭합니다.

단계 **4** **Run(**실행**)**을 클릭합니다.

단계 **5** 표시되는 **Progress Details...(**진행 세부정보**)** 영역에서 **Click Here to Enter Credentials(**여기를 클릭하여 자격 증명 입력**)**를 클릭합니다. **Credentials Window(**자격 증명 창**)** 대화 상자에서 네트워크 디바이스와의 연결을 설정하는 데 필요한 연결 매개변수 및 자격 증명을 입력하고 **Submit(**제출**)**를 클릭합니다

워크플로우를 취소하려면 **Progress Details...(**진행 세부정보...**)** 창에서 **Click Here to Cancel the Running Workflow(**여기를 클릭하여 실행 중인 워크플로우 취소**)**를 클릭합니다.

단계 **6** 분석할 인터페이스 옆의 확인란을 선택하고 **Submit(**제출**)**을 클릭합니다.

단계 **7** 구성 평가에 대한 자세한 내용을 보려면 **Show Results Summary(**결과 요약 표시**)**를 클릭합니다.

네트워크 디바이스 명령 진단 도구 실행

네트워크 디바이스 실행 명령 진단 도구를 사용하면 네트워크 디바이스에 대해 **show** 명령을 실행할 수 있습니다.

표시되는 결과는 콘솔에 표시되는 것과 동일합니다. 이 도구를 사용하면 디바이스 컨피그레이션의 모든 문제를 식별할 수 있습니다.

네트워크 디바이스의 컨피그레이션을 확인하거나 네트워크 디바이스가 구성된 방법을 확인하려면 이 도구를 활용하면 됩니다.

네트워크 디바이스 실행 명령 진단 도구에 액세스하려면 다음 탐색 경로 중 하나를 선택하십시오.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고**Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **Execute Network Device Command(**네트워크 디바이스 명령 실행**)**를 선택합니다.
- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고**Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Troubleshoot(**문제 해결**)** > **Execute Network Device Command(**네트워크 디바이스 명령 실행**)**를 선택합니다.

표시되는 **Execute Network Device Command(**네트워크 디바이스 실행 명령**)** 창에서 해당 필드에 실행할 네트워크 디바이스의 IP 주소와 show 명령을 입력합니다. **Run(**실행**)**을 클릭합니다.

Cisco ISE의 서드파티 네트워크 디바이스 지원

Cisco ISE는 네트워크 디바이스 프로파일을 사용하여 서드파티 NAD(Network Access Device)를 지원합니다. NAD 프로파일은 벤더 쪽 구현에 관계없이 간소화된 정책 컨피그레이션을 사용하여 서드파티 디바이스 기능을 정의합니다. 네트워크 디바이스 프로파일에는 다음이 포함됩니다.

- RADIUS, TACACS+, Cisco TrustSec 등 네트워크 디바이스가 지원하는 프로토콜. 네트워크 디바이스용으로 존재하는 벤더별 RADIUS 사전을 Cisco ISE로 가져올 수 있습니다.
- 디바이스가 유선 MAB 및 802.1X 등의 다양한 인증 플로우에 사용하는 속성과 값. Cisco ISE는 이러한 속성 및 값을 사용하여, 네트워크 디바이스가 사용하는 속성에 따라 디바이스에 적합한 인증 플로우를 탐지할 수 있습니다.
- 네트워크 디바이스에 있는 CoA(Change of Authorization) 기능. RADIUS 프로토콜 RFC 5176은 CoA 요청을 정의하지만 CoA 요청에 사용되는 속성은 네트워크 디바이스에 따라 달라집니다. RFC 5176을 지원하는 대부분의 Cisco 이외의 디바이스는 "푸시" 및 "연결 끊기" 기능을 지원합니다. RADIUS CoA 유형을 지원하지 않는 디바이스의 경우 Cisco ISE는 SNMP CoA도 지원합니다.
- 네트워크 디바이스가 MAB 플로우에 사용하는 속성 및 프로토콜. 여러 벤더의 네트워크 디바이스는 각기 다른 방식으로 MAB 인증을 수행합니다.
- 디바이스에서 사용하는 VLAN 및 ACL 권한. 프로파일을 저장하면 Cisco ISE는 구성된 각 권한에 대해 권한 부여 프로파일을 자동으로 생성합니다.
- URL 리디렉션 기술 정보. BYOD(Bring Your Own Device), 게스트 액세스, 포스처 서비스 등의 고급 플로우에서는 URL 리디렉션이 필요합니다. 네트워크 디바이스에서는 두 가지 유형의 URL 리디렉션(정적 및 동적)을 확인할 수 있습니다. 정적 URL 리디렉션의 경우 Cisco ISE 포털 URL을 복사하여 컨피그레이션에 붙여 넣을 수 있습니다. 동적 URL 리디렉션의 경우 Cisco ISE는 RADIUS 속성을 사용하여 리디렉션 대상 위치를 네트워크 디바이스에 알려 줍니다.

  디바이스가 동적 및 정적 URL 리디렉션을 모두 지원하지 않는 경우 Cisco ISE는 URL 리디렉션 시뮬레이션에 사용하는 인증 VLAN 컨피그레이션을 제공합니다. 인증 VLAN 컨피그레이션은 Cisco ISE에서 실행되는 DHCP 및 DNS 서비스를 기반으로 합니다.

Cisco ISE에서 네트워크 디바이스를 정의한 후 프로파일러, 게스트, BYOD, MAP, 보안 상태 등 고급 플로우와 함께 기본 인증 플로우를 활성화하는 데 사용하는 기능을 정의하기 위해 이러한 디바이스 프로파일을 구성하거나 Cisco ISE에서 제공하는 사전 구성된 디바이스 프로파일을 사용합니다.

URL 리디렉션 메커니즘 및 인증 VLAN

네트워크에서 서드파티 디바이스를 사용하며 해당 디바이스가 동적 또는 정적 URL 리디렉션을 지원하지 않는 경우, ISE는 URL 리디렉션 플로우를 시뮬레이션합니다. 이러한 디바이스에 대한 URL 리디렉션 시뮬레이션 플로우는 Cisco ISE에서 DHCP 또는 DNS 서비스를 실행하여 작동합니다.

다음은 인증 VLAN 플로우의 예입니다.

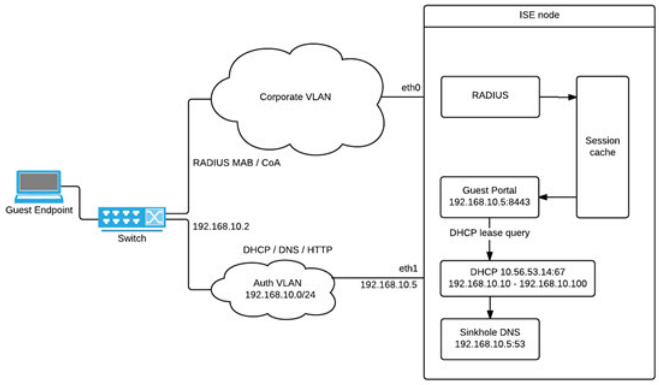
1. 게스트 엔드포인트가 NAD에 연결됩니다.
2. 네트워크 디바이스가 RADIUS 또는 MAB 요청을 Cisco ISE에 보냅니다.
3. ISE가 구성된 인증 및 권한 부여 정책을 실행하고 사용자 계정 관리 정보를 저장합니다.
4. ISE가 인증 VLAN ID를 포함하는 RADIUS 액세스-수락 메시지를 보냅니다.
5. 게스트 엔드포인트가 네트워크 액세스 권한을 수신합니다.
6. 엔드포인트가 DHCP 요청을 브로드캐스트하고 Cisco ISE DHCP 서비스에서 클라이언트 IP 주소 및 Cisco ISE DNS 싱크홀 IP 주소를 가져옵니다.
7. 게스트 엔드포인트에서 브라우저를 열고 여기에서 DNS 쿼리를 전송하고 Cisco ISE IP 주소를 수신합니다.
8. 엔드포인트 HTTP 및 HTTPS 요청이 Cisco ISE로 전송됩니다.
9. Cisco ISE가 게스트 포털 URL이 있는 HTTP 301 Moved 메시지로 응답합니다. 엔드포인트 브라우저가 게스트 포털 창으로 리디렉션됩니다.
10. 게스트 엔드포인트 사용자가 인증을 위해 로그인합니다.
11. Cisco ISE가 엔드포인트 규정 준수를 확인한 다음 NAD에 응답합니다. Cisco ISE가 CoA를 전송하고 엔드포인트에 권한을 부여하며 싱크홀을 우회합니다.
12. 게스트 사용자는 CoA를 기준으로 적절한 액세스 권한을 부여받습니다. 엔드포인트는 엔터프라이즈 DHCP에서 IP 주소를 수신합니다. 이제 게스트 사용자가 네트워크를 사용할 수 있습니다.

엔드포인트가 인증을 통과하기 전에 게스트 엔드포인트가 무단으로 네트워크에 액세스할 수 없도록 하기 위해 기업 네트워크에서 인증 VLAN을 분리할 수 있습니다. Cisco ISE 머신을 가리키도록 인증 VLAN IP 헬퍼를 구성하거나 Cisco ISE 네트워크 인터페이스 중 하나를 인증 VLAN에 연결합니다.

NAD 컨피그레이션에서 VLAN IP 헬퍼를 구성하여 여러 VLAN을 하나의 네트워크 인터페이스 카드에 연결할 수 있습니다. IP 헬퍼 구성에 대한 자세한 내용은 네트워크 디바이스의 관리 설명서에서 지침을 참고하십시오. IP 헬퍼가 있는 VLAN을 포함하는 게스트 액세스 플로우의 경우, 게스트 포털을 정의하고 MAB 권한 부여에 바인딩된 권한 부여 프로파일에서 해당 포털을 선택합니다. 게스트 포털에 관한 자세한 정보는 *Cisco ISE* 관리 가이드*:* 게스트 및 *BYOD*에서 Cisco ISE 게스트 서비스 섹션을 참조하십시오. 참고.

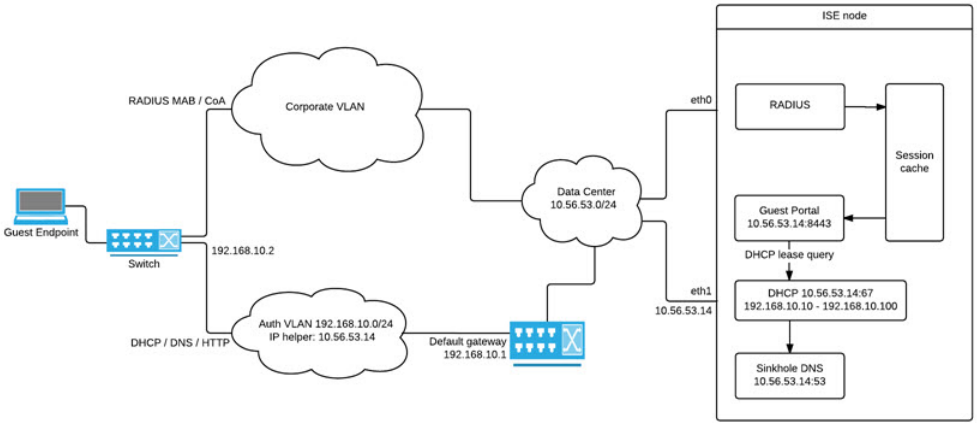
다음 다이어그램에는 인증 VLAN을 정의할 때의 기본 네트워크 설정이 나와 있습니다(인증 VLAN은 Cisco ISE 노드에 직접 연결됨).

그림 *32: Cisco ISE* 노드에 연결되는 인증 *VLAN*



다음 다이어그램에는 인증 VLAN 및 IP 헬퍼가 있는 네트워크가 나와 있습니다.

그림 *33: IP* 헬퍼를 이용해 구성된 인증 *VLAN*



CoA 유형

Cisco ISE는 RADIUS 및 SNMP CoA 유형을 모두 지원합니다. 복잡한 플로우에서 NAD가 작동하려면 RADIUS 또는 SNMP CoA 유형이 지원되어야 하지만 기본 플로우의 경우에는 이러한 유형이 반드시 지원되지 않아도 됩니다.

Cisco ISE에서 NAD를 구성할 때 네트워크 디바이스에서 지원하는 RADIUS 및 SNMP 설정을 정의하고, NAD 프로파일을 구성할 때 특정 플로우에 대해 사용할 CoA 유형을 나타냅니다. NAD용 프로토콜을 정의하는 방법에 대한 자세한 내용은 네트워크 디바이스 정의 설정, 821 페이지를 참고하십시오. Cisco ISE에서 디바이스 및 NAD 프로파일을 생성하기 전에 서드파티 공급업체에 문의하여 NAD가 지원하는 유형을 확인하십시오.

네트워크 디바이스 프로파일

Cisco ISE는 네트워크 디바이스 프로파일을 사용하여 일부 타사 NAD(Network Access Device)를 지원합니다. 이러한 프로파일은 Cisco ISE가 기본 플로우 및 게스트, BYOD, MAB, 포스처 등의 고급 플로우를 활성화하는 데 사용하는 기능을 정의합니다.

Cisco ISE에는 여러 벤더의 네트워크 디바이스용으로 사전 정의된 프로파일이 포함되어 있습니다. Cisco ISE 2.1 이상 릴리스는 다음 표에 나열된 네트워크 디바이스와 함께 테스트되었습니다.

표 ***117: Cisco ISE 2.1*** 이상 릴리즈에서 테스트한 벤더 디바이스

디바이스 유형	벤더	**CoA** 유형	**URL** 리디렉션 유형	지원 및 검증된 활용 사례				
				802.1X 및 **MAB** 플로우	**CoA**가 없는 프로파일러	**CoA**가 있는 프로파일러	포스처	게스트 및 **BYOD** 플로우
무선	Aruba 7000, InstantAP	RADIUS	정적 URL	예	예	예	예	예
	Motorola RFS 4000	RADIUS	동적 URL	예	예	예	예	예
	HP 830	RADIUS	정적 URL	예	예	예	예	예
	Ruckus ZD 1200	RADIUS	—	예	예	예	예	예
유선	HP A5500	RADIUS	ISE에서 제공하는 인증 VLAN	예	예	예	예	예
	HP 3800 및 2920(ProCurve)	RADIUS	ISE에서 제공하는 인증 VLAN	예	예	예	예	예
	Alcatel 6850	SNMP	동적 URL	예	예	예	예	예
	Brocade ICX 6610	RADIUS	ISE에서 제공하는 인증 VLAN	예	예	예	예	예
	Juniper EX3300-24p	RADIUS	ISE에서 제공하는 인증 VLAN	예	예	예	예	예

기타 타사 NAD의 경우 디바이스 속성과 기능을 식별하고 Cisco ISE에서 맞춤형 NAD 프로파일을 생성해야 합니다.	예	예	CoA 지원 필요	CoA 지원이 필요합니다. 유선 디바이스가 URL 리디렉션을 지원하지 않는 경우 Cisco ISE는 인증 VLAN을 사용합니다. 무선 디바이스는 인증 VLAN을 사용하여 테스트되지 않았습니다.

미리 정의된 프로파일이 없는 기타 타사 네트워크 디바이스의 경우 맞춤형 NAD 프로파일을 생성해야 합니다. 게스트, BYOD 및 포스처와 같은 고급 플로우의 경우 네트워크 디바이스가 CoA 이러한 플로우에 대한 지원은 NAD 기능에 따라 달라집니다. Cisco ISE에서 네트워크 디바이스 프로파일을 생성하는 데 필요한 속성에 자세한 내용은 디바이스 관리 가이드를 참조하십시오.

Cisco ISE 릴리스 2.0 이하에서 Cisco ISE 릴리스 2.1 이상으로 업그레이드하는 경우 이전 릴리스에서 비 Cisco NAD와 통신하기 위해 생성한 인증 정책 규칙 및 RADIUS 사전은 업그레이드 후에도 Cisco ISE에서 계속 작동합니다.

ISE Community Resource(ISE 커뮤니티 리소스)

타사 NAD 프로파일에 자세한 내용은 ISE 타사 NAD 프로파일 및 컨피그레이션을 참조하십시오.

Cisco ISE에서 서드파티 네트워크 디바이스 구성

Cisco ISE는 네트워크 디바이스 프로파일을 사용하여 서드 파티 NAD를 지원합니다. 이러한 프로파일은 Cisco ISE가 게스트, BYOD, MAB, 포스처 등의 플로우를 활성화하는 데 사용하는 기능을 정의합니다.

시작하기 전에

네트워크 디바이스 프로파일, 847 페이지의 내용을 참조하십시오.

단계 **1** Cisco ISE에서 서드파티 네트워크 디바이스 추가(Cisco ISE로 네트워크 디바이스 가져오기, 841 페이지 참고) 게스트, BYOD 또는 포스처 워크플로우를 구성하는 경우 CoA(Change of Authorization)가 정의되어 있으며 NAD의 URL 리디렉션 메커니즘이 관련 Cisco ISE 포털을 가리키도록 구성되어 있는지 확인합니다. URL 리디렉션을 구성하려면 포털의 랜딩 페이지에서 Cisco ISE 포털 URL을 복사합니다. Cisco ISE에서 NAD에 대한 CoA 유형 및 URL 리디렉션 구성에 대한 자세한 내용은 네트워크 디바이스 정의 설정, 821 페이지를 참고하십시오. 또한 서드파티 디바이스의 관리 설명서에 나와 있는 지침을 참고하십시오.

단계 **2** 디바이스용으로 적절한 NAD 프로파일을 ISE에서 사용할 수 있는지 확인합니다. 기존 프로파일을 확인하려면 **Administration**(관리) > **Network Resources**(네트워크 리소스) > **Network Device Profiles**(네트워크 디바이스 프로파일)를 선택합니다. Cisco ISE에 적절한 프로파일이 아직 없으면 사용자 맞춤화 프로파일을 생성합니다. 맞춤형 프로파일을 생성하는 방법에 대한 자세한 내용은 네트워크 디바이스 프로파일 생성, 849 페이지을 참고하십시오.

단계 **3** 구성하려는 NAD에 NAD 프로파일을 할당합니다. Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**. 프로파일을 할당할 디바이스를 열고 **Device Profile(**디바이스 프로파일**)**의 드롭다운 목록에서 올바른 프로파일을 선택합니다.

단계 **4** 정책 규칙을 구성할 때 VLAN 또는 ACL만 사용하거나 네트워크에 여러 벤더의 각기 다른 디바이스가 있는 경우 권한 부여 프로파일을 1단계에서 NAD 프로파일 또는 "Any(모두)"로 명시적으로 설정해야 합니다. 권한 부여 프로파일에 대해 NAD 프로파일을 설정하려면 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다. 관련 권한 부여 프로파일을 열고 **Network Device Profile(**네트워크 디바이스 프로파일**)**의 드롭다운 목록에서 관련 NAD 프로파일을 선택합니다. 또한 게스트 플로우에 대해 인증 VLAN을 사용하는 경우 게스트 포털을 정의한 다음 일반 게스트 플로우와 비슷하게 MAB 권한 부여로 바인딩되는 권한 부여 프로파일에서 해당 포털을 선택해야 합니다. 게스트 포털에 관한 자세한 내용은 *Cisco ISE* 관리 가이드*:* 게스트 및 *BYOD*에서 Cisco ISE 게스트 서비스 섹션을 참고하십시오. 참고.

네트워크 디바이스 프로파일 생성

시작하기 전에

- 대부분의 NAD에는 표준 IETF RADIUS 속성 외에 다수의 벤더별 속성을 제공하는 벤더별 RADIUS 사전이 있습니다. 네트워크 디바이스에 벤더별 RADIUS 사전이 있으면 Cisco ISE로 가져옵니다. RADIUS 사전이 필요한 지침은 서드파티 디바이스의 관리 설명서를 참고하십시오. Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘을 클릭하고(☰) **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**)** > **System(**시스템**)** > **Radius(RADIUS)** > **RADIUS Vendors(RADIUS** 벤더**)**를 선택합니다. RADIUS 사전을 가져오려면 Cisco ISE Admin Guide: Secure Wired Access의 *"RADIUS-*벤더 사전 생성*"* 항목을 확인하십시오. .
- 게스트 및 포스처와 같은 복잡한 플로우의 경우 네트워크 디바이스는 RFC 5176을 지원해야합니다.
- 네트워크 디바이스 프로파일을 생성하기 위한 필드 및 가능한 값에 대한 자세한 내용은 Cisco ISE 관리 가이드: 보안 유선 액세스의 네트워크 디바이스 프로파일 설정 섹션을 참조하십시오. .

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 표시되는 **New Network Device Profile(**새 네트워크 디바이스 프로파일**)** 창에서 네트워크 디바이스의 **Name(**이름**)** 및 **Description(**설명**)** 필드에 해당 값을 입력합니다.

단계 **4** 드롭다운 목록에서 네트워크 디바이스의 벤더를 선택합니다.

단계 **5** 아이콘 영역에서 아이콘 변경 **...** 버튼을 클릭하여 시스템의 네트워크 디바이스 아이콘을 업로드합니다.

Cisco ISE에서 제공하는 기본 아이콘을 사용하려면 아이콘 영역에서**Set To Default(**기본값으로 설정**)** 버튼을 클릭합니다.

단계 **6** **Supported Protocols(**지원되는 프로토콜**)** 영역에서 디바이스가 지원하는 프로토콜의 확인란을 선택합니다. 실제로 사용하려는 프로토콜에 대해서만 확인란을 선택합니다. 디바이스가 RADIUS 프로토콜을 지원하는 경우 **RADIUS Dictionaries(RADIUS** 사전**)** 드롭다운 목록에서 디바이스와 함께 사용할 RADIUS 사전을 선택합니다.

단계 **7** **Templates(**템플릿**)** 영역에서 다음과 같이 관련 세부정보를 입력합니다.

a) **Authentication/Authorization(**인증/권한 부여**)** 섹션을 펼쳐 플로우 유형, 속성 별칭 및 호스트 조회에 대한 디바이스의 기본 설정을 구성합니다. 표시되는 새 **Flow Type Conditions(**플로우 유형 조건**)** 영역에서 디바이스가 Wired MAB 또는 802.1X와 같은 다양한 인증 및 권한 부여 플로우에 사용하는 속성 및 값을 입력합니다. 그러면 Cisco ISE가 사용하는 속성에 따라 디바이스에 적합한 플로우 유형을 탐지할 수 있습니다. MAB에 대한 IETF 표준은 없으며, 벤더마다 Service-Type에 각기 다른 값을 사용합니다. 올바른 설정을 확인하려면 디바이스의 사용 설명서를 참고하거나 MAB 인증의 스니퍼 추적을 사용합니다. **Attribute Aliasing(**속성 별칭**)** 영역에서 정책 규칙을 간소화하기 위해 디바이스별 속성 이름을 공용 이름에 매핑합니다. 현재는 SSID(Service Set Identifier)만 정의되어 있습니다. 네트워크 디바이스에 무선 SSID 개념이 있는 경우 이를 디바이스가 사용하는 속성으로 설정합니다. Cisco ISE는 이를 정규화된 RADIUS 사전 내의 SSID라는 속성에 매핑합니다. 이렇게 하면 규칙 하나에서 SSID를 참조할 수 있으며, 기본 속성이 다르더라도 해당 규칙이 여러 디바이스에서 작동하므로 정책 규칙 컨피그레이션을 간소화할 수 있습니다. **Host Lookup(**호스트 조회**)** 영역에서 **Process Host Lookup(**프로세스 호스트 조회**)** 확인란을 선택하고 서드파티 지침에 따라 디바이스에 대해 관련 MAB 프로토콜 및 속성을 선택합니다.

b) **Permissions(**권한**)** 접힘 메뉴를 클릭해서 VLAN 및 ACL에 대한 네트워크 디바이스의 기본 설정을 구성합니다. 이러한 설정은 Cisco ISE에서 생성한 권한 부여 프로파일을 기준으로 하여 자동으로 매핑됩니다.

c) 네트워크 디바이스의 CoA 기능을 구성하려면 **CoA(Change of Authorization)** 접힘 메뉴를 클릭합니다.

d) 디바이스의 URL 리디렉션 기능을 구성하려면 **Redirect(**리디렉션**)** 섹션을 펼칩니다. URL 리디렉션은 게스트, BYOD 및 포스처 서비스에 필요합니다.

단계 **8** **Submit(**제출**)**을 클릭합니다.

관련 항목

ISE 네트워크 액세스 디바이스 프로파일을 생성하는 방법

Cisco ISE에서 네트워크 디바이스 프로파일 내보내기

Cisco ISE에 구성된 단일 또는 여러 네트워크 디바이스 프로파일을 XML 파일 형식으로 내 보냅니다. 그런 다음 XML 파일을 편집하여 새 네트워크 프로파일로 Cisco ISE 파일에 가져올 수 있습니다.

시작하기 전에

ISE 네트워크 액세스 디바이스 프로파일을 생성하는 방법을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**)**를 선택합니다.

단계 **2** 내보낼 디바이스 옆의 확인란을 선택하고 **Export Selected(**선택 항목 내보내기**)**를 선택합니다.

단계 **3** **DeviceProfiles.xml** 파일이 로컬 하드 디스크에 다운로드됩니다.

Cisco ISE로 네트워크 디바이스 프로파일 가져오기

Cisco ISE XML 구조인 XML 파일 하나를 사용하여 네트워크 디바이스 프로파일 하나 또는 여러 개를 Cisco ISE로 가져옵니다. 가져온 여러 개의 파일에서 네트워크 디바이스 프로파일을 동시에 가져올 수는 없습니다.

일반적으로는 먼저 템플릿으로 사용할 기존 프로파일을 Cisco ISE 관리자 포털에서 내보냅니다. 파일에 디바이스 프로파일 세부정보를 필요한 대로 입력하고 XML 파일로 저장합니다. 그런 다음 수정한 파일을 다시 Cisco ISE로 가져옵니다. 여러 네트워크 디바이스 프로파일로 작업하려면 하나의 XML 파일로 구성된 다수의 프로파일을 내보내고 파일을 편집한 다음, 해당 프로파일을 함께 가져와 Cisco ISE에서 여러 프로파일을 생성하면 됩니다.

네트워크 디바이스 프로파일을 가져오는 동안에는 새 기록 생성만 할 수 있습니다. 기존 프로파일을 덮어쓸 수는 없습니다. 기존 네트워크 디바이스 프로파일을 업데이트하려면 Cisco ISE에서 기존 프로파일을 내보내고 Cisco ISE에서 프로파일을 삭제한 다음, 적절하게 편집한 후 프로파일을 가져옵니다.

시작하기 전에

ISE 네트워크 액세스 디바이스 프로파일을 생성하는 방법을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**)**를 선택합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** **Choose File(**파일 선택**)**을 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 XML 파일을 선택합니다.

단계 **4** **Import(**가져오기**)**를 클릭합니다.

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 ***118: 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 ***119: 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 그룹

Cisco ISE에서는 네트워크 디바이스를 포함하는 계층적 NDG(Network Device Groups)를 생성할 수 있습니다. NDG에서는 지리적 위치, 디바이스 유형 및 네트워크의 상대적 위치(예: "액세스 레이어" 또는 "데이터 센터")와 같은 다양한 기준에 따라 네트워크 디바이스를 논리적으로 그룹화합니다.

NDG 창을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)**를 .

예를 들어 지리적 위치별로 네트워크 디바이스를 구성하려는 경우 다음과 같이 대륙, 지역 및 국가별로 디바이스를 그룹화할 수 있습니다.

- 아프리카 > 남부 > 나미비아
- 아프리카 > 남부 > 남아프리카
- 아프리카 > 남부 > 보츠와나

디바이스 유형에 따라 네트워크 디바이스를 그룹화할 수 있습니다.

- 아프리카 > 남부 > 보츠와나 > 방화벽
- 아프리카 > 남부 > 보츠와나 > 라우터
- 아프리카 > 남부 > 보츠와나 > 스위치

하나 이상의 계층적 네트워크 디바이스 그룹에 네트워크 디바이스를 할당합니다. 따라서 Cisco ISE가 특정 디바이스에 할당할 적절한 그룹을 확인하기 위해 구성된 NDG의 순서가 지정된 목록을 살펴볼 때 같은 디바이스 프로파일이 여러 디바이스 그룹에 적용되어 있음을 확인할 수 있습니다. 이 경우 Cisco ISE는 일치하는 첫 번째 디바이스 그룹을 적용합니다.

생성할 수 있는 네트워크 디바이스 그룹의 최대 수에는 제한이 없습니다. 네트워크 디바이스 그룹에 대해 최대 6개 레벨의 계층 구조(상위 그룹 포함)를 생성 할 수 있습니다.

디바이스 그룹 계층 구조는 **Tree Table(**트리 표**)** 및 **Flat Table(**플랫 표**)**의 두 가지 보기로 표시됩니다. 네트워크 디바이스 그룹 목록 위의 **Tree Table(**트리 표**)** 또는 **Flat Table(**플랫 표**)**을 클릭하여 원하는 보기로 목록을 구성합니다.

Tree Table(트리 표**)** 보기에서는 루트 노드가 트리의 맨 위에 나타나며 그 뒤에 하위 그룹이 계층 구조로 나타납니다. 각 루트 그룹의 모든 디바이스 그룹을 보려면 **Expand All(**모두 확장**)**을 클릭합니다. 루트 그룹만 목록으로 보려면 **Collapse All(**모두 축소**)**를 클릭합니다.

Flat Table(플랫 표**)** 보기에서는 각 디바이스 그룹의 계층 구조가 **Group Hierarchy(**그룹 계층 구조**)** 열에 표시됩니다.

두 보기 모두에서 각 하위 그룹에 할당된 네트워크 디바이스의 수가 해당하는 **No. of Network Devices(**네트워크 디바이스 수**)** 열에 표시됩니다. 이 숫자를 클릭하면 해당 디바이스 그룹에 할당된 모든 네트워크 디바이스가 나열된 대화 상자가 실행됩니다. 표시되는 대화 상자에는 네트워크 디바이스를 한 그룹에서 다른 그룹으로 이동할 수 있는 두 개의 버튼도 있습니다. 네트워크 그룹을 현재 그룹에서 다른 그룹으로 이동하려면 **Move Devices to Another Group(**디바이스를 다른 그룹으로 이동**)** 버튼을 클릭합니다. **Add Devices to Group(**그룹에 디바이스 추가**)** 버튼을 클릭하여 네트워크 디바이스를 선택한 네트워크 디바이스 그룹으로 이동합니다.

Network Device Groups(네트워크 디바이스 그룹**)** 창에서 네트워크 디바이스 그룹을 추가하려면 **Add(**추가**)**를 클릭합니다. **Parent Group(**상위 그룹**)** 드롭 다운 목록에서 네트워크 디바이스 그룹을 추가해야 하는 상위 그룹을 선택하거나 **Add As Root Group(**루트 그룹으로 추가**)** 옵션을 선택하여 새 네트워크 디바이스 그룹을 상위 그룹으로 추가합니다.

참고 해당 디바이스 그룹에 디바이스가 할당되어 있으면 디바이스 그룹을 삭제할 수 없습니다. 디바이스 그룹을 삭제하기 전에 모든 기존 디바이스를 다른 디바이스 그룹으로 이동해야 합니다.

루트 네트워크 디바이스 그룹

Cisco ISE에는 **All Device Types(**모든 디바이스 유형**)** 및 **All Locations(**모든 위치**)**의 두 가지 미리 정의된 루트 네트워크 디바이스 그룹이 포함되어 있습니다. 이러한 미리 정의된 네트워크 디바이스 그룹을 편집, 복제 또는 삭제할 수는 없지만 그 아래에 새 디바이스 그룹을 추가할 수는 있습니다.

이전 섹션에서 설명한 대로 루트 네트워크 디바이스 그룹(네트워크 디바이스 그룹)을 생성 한 다음 **Network Device Groups(**네트워크 디바이스 그룹**)** 창의 루트 그룹 아래에 하위 네트워크 디바이스 그룹을 생성할 수 있습니다.

정책 평가에서 Cisco ISE가 사용하는 네트워크 디바이스 속성

새 네트워크 디바이스 그룹을 생성할 때는 새 네트워크 디바이스 속성이 **System Dictionaries(**시스템 사전**)**의 **Device(**디바이스**)** 사전에 추가됩니다**(Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**))**. 그러면 추가된 디바이스 속성이 정책 정의에 사용됩니다.

Cisco ISE에서는 디바이스 유형, 위치, 모델 이름 및 네트워크 디바이스에서 실행 중인 소프트웨어 버전과 같은 디바이스 사전 속성을 기준으로 인증 및 권한 부여 정책을 구성할 수 있습니다.

Cisco ISE로 네트워크 디바이스 그룹 가져오기

CSV(comma-separated value) 파일을 사용하여 Cisco ISE 노드로 네트워크 디바이스 그룹을 가져올 수 있습니다. 서로 다른 두 가져오기 파일에서 네트워크 디바이스 그룹을 동시에 가져올 수는 없습니다.

Cisco ISE 관리자 포털에서 CSV 템플릿을 다운로드하고 해당 템플릿에 네트워크 디바이스 그룹 세부정보를 입력한 후에 템플릿을 CSV 파일로 저장합니다. 그런 다음 편집한 파일을 Cisco ISE로 가져오면 됩니다.

디바이스 그룹을 가져올 때 새 기록을 생성하거나 기존 기록을 업데이트할 수 있습니다. 디바이스 그룹을 가져올 때는 Cisco ISE가 기존 디바이스 그룹을 새 그룹으로 덮어쓰도록 할지 아니면 Cisco ISE에서 첫 번째 오류를 발견할 때 가져오기 프로세스를 중지하도록 할지를 정의할 수도 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)**를 선택합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** 대화 상자가 표시되면 **Choose File(**파일 선택**)**을 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 CSV 파일을 선택합니다.

네트워크 디바이스 그룹을 추가하는 데 필요한 CSV 템플릿 파일을 다운로드하려면 **Generate a Template(**템플릿 생성**)**을 클릭합니다.

단계 **4** 기존 네트워크 디바이스 그룹을 덮어쓰려면 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 확인란을 선택합니다.

단계 **5** **Stop Import on First Error(**첫 번째 오류에서 가져오기 중지**)** 확인란을 선택합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.

Cisco ISE에서 네트워크 디바이스 그룹 내보내기

Cisco ISE에 구성된 네트워크 디바이스 그룹을 CSV 파일 형식으로 내보낼 수 있습니다. 그런 다음 이러한 네트워크 디바이스 그룹을 다른 Cisco ISE 노드로 가져올 수 있습니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)** > **All Groups(**모든 그룹**)**를 선택합니다.

단계 **2** 네트워크 디바이스 그룹을 내보내려는 경우 다음 중 하나를 수행할 수 있습니다.

- 내보낼 디바이스 그룹 옆의 확인란을 선택하고 **Export(**내보내기**)** > **Export Selected(**선택 항목 내보내기**)**를 선택합니다.
- 정의되어 있는 모든 네트워크 디바이스 그룹을 내보내려면 **Export(**내보내기**)** > **Export All(**모두 내보내기**)**을 선택합니다.

단계 **3** CSV 파일이 로컬 하드 디스크에 다운로드됩니다.

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 ***120: 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 ***121: 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.
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.

Cisco ISE에서 템플릿 가져오기

Cisco ISE에서는 CSV 파일을 사용하여 많은 네트워크 디바이스 및 네트워크 디바이스 그룹을 가져올 수 있습니다. 템플릿은 필드의 형식을 정의하는 헤더 행을 포함합니다. 이 헤더 행을 편집해서는 안 됩니다.

네트워크 디바이스 및 네트워크 디바이스 그룹에 대한 해당 가져오기 플로우에서 **Generate a Template(**템플릿 생성**)** 링크를 사용하여 CSV 파일을 로컬 시스템에 저장할 수 있습니다.

네트워크 디바이스 가져오기 템플릿 형식

다음 표는 가져오기 네트워크 디바이스 CSV 템플릿 파일의 헤더에 있는 필드를 나열하고 그에 대한 설명을 제공합니다.

표 ***122: CSV*** 템플릿 필드 및 네트워크 디바이스에 대한 설명

필드	설명
Name:String(32)(이름**:**문자열**(32))**	(필수) 네트워크 디바이스 이름 필드입니다. 최대 길이가 32자인 영숫자 문자열입니다.
Description:String(256)(설명**:**문자열**(256))**	네트워크 디바이스에 대한 설명입니다. 최대 길이가 256자인 문자열입니다.
IP Address:Subnets(a.b.c.d/m|...)(IP 주소**:**서브넷**(a.b.c.d/m|...))**	(필수) 네트워크 디바이스의 IP 주소 및 서브넷 마스크 필드입니다. 둘 이상의 값을 파이프("|") 기호로 구분하여 포함할 수 있습니다. IPv4 및 IPv6 네트워크 디바이스(TACACS 및 RADIUS) 컨피그레이션 및 외부 RADIUS 서버 컨피그레이션에 지원됩니다. IPv4 주소를 입력할 때 범위 및 서브넷 마스크를 사용할 수 있습니다.
Model Name:String(32)(모델 이름**:**문자열**(32))**	(필수) 네트워크 디바이스 모델 이름 필드입니다. 최대 길이가 32자인 문자열입니다.
Software Version:String(32)(소프트웨어 버전**:**문자열**(32))**	(필수) 네트워크 디바이스 소프트웨어 버전 필드입니다. 최대 길이가 32자인 문자열입니다.
Network Device Groups:String(100)(네트워크 디바이스 그룹**:**문자열**(100))**	(필수) 이 필드에는 기존 네트워크 디바이스 그룹을 입력해야 합니다. 하위 그룹이지만 상위 그룹과 하위 그룹을 쉼표로 구분하여 모두 포함해야 합니다. 최대 길이가 100자인 문자열입니다. 예를 들어 *Location>All Location>US*입니다.

필드	설명
Authentication:Protocol:String(6)(인증**:**프로토콜**:** 문자열**(6))**	이 필드는 사용하고자 하는 인증 프로토콜을 나타냅니다. 유효한 값은 "RADIUS"(대/소문자 구분 안 함)뿐입니다.
Authentication:Shared Secret:String(128)(인증**:** 공유 암호**:**문자열**(128))**	(인증 프로토콜 필드에 값을 입력하는 경우 필수) 이 필드의 값은 최대 길이가 128자인 문자열입니다.
EnableKeyWrap:Boolean(true|false)(EnableKeyWrap: 부울**(true|false))**	이 필드는 네트워크 디바이스에서 지원되는 경우에만 활성화됩니다. 유효한 값은 "true" 및 "false"입니다.
EncryptionKey:String(ascii:16|hexa:32)(EncryptionKey: 문자열**(ascii:16|16**진수**:32))**	(KeyWrap을 활성화하는 경우 필수) 이 필드는 세션 암호화에 사용되는 암호화 키를 나타냅니다. ASCII 값: 길이가 16자(바이트)입니다. 16진수 값: 길이가 32자(바이트)입니다.
AuthenticationKey:String(ascii:20|hexa:40)(AuthenticationKey: 문자열**(ascii:20|16**진수**:40))**	(KeyWrap을 활성화하는 경우 필수) 이 필드는 RADIUS 메시지에 대한 키 HMAC(Hashed Message Authentication Code) 계산을 나타냅니다. ASCII 값: 길이가 20자(바이트)입니다. 16진수 값: 길이가 40자(바이트)입니다.
InputFormat:String(32)(InputFormat:문자열**(32))**	이 필드는 암호화 및 인증 키 입력 형식을 나타냅니다. ASCII 및 16진수 값이 허용됩니다.
SNMP:Version:Enumeration (|2c|3)(SNMP:버전**:** 열거**(|2c|3))**	이 필드는 프로파일러 서비스에서 사용하는 필드입니다. SNMP 프로토콜의 버전 1, 2c 또는 3입니다.
SNMP:RO Community:String(32)(SNMP:RO 커뮤니티**:**문자열**(32))**	(SNMP Version(SNMP 버전) 필드에 값을 입력하는 경우 필수) SNMP 읽기 전용 커뮤니티입니다. 이 필드는 최대 길이가 32자인 문자열을 나타냅니다.
SNMP:RW Community:String(32)(SNMP:RW 커뮤니티**:**문자열**(32))**	(SNMP Version(SNMP 버전) 필드에 값을 입력하는 경우 필수) SNMP 읽기/쓰기 커뮤니티입니다. 이 필드는 최대 길이가 32자인 문자열을 나타냅니다.
SNMP:Username:String(32)(SNMP:사용자 이름**:** 문자열**(32))**	이 필드는 최대 길이가 32자인 문자열을 나타냅니다.

필드	설명
SNMP:Security Level:Enumeration(Auth|No Auth|Priv)(SNMP:보안 레벨**:**열거**(**인증**|**인증 안 함**|**개인**))**	(SNMP 버전 3을 선택하는 경우 필수) 이 필드는 "Auth(인증)", "No Auth(인증 안 함)", "Priv(개인)" 값을 허용합니다.
SNMP:Authentication Protocol:Enumeration(MD5|SHA)(SNMP:인증 프로토콜**:**열거**(MD5|SHA))**	(SNMP 보안 레벨로 인증 또는 개인을 입력한 경우 필수) 이 필드는 "MD5" 또는 "SHA" 값을 허용합니다.
SNMP:Authentication Password:String(32)(SNMP:인증 비밀번호**:**문자열**(32))**	(SNMP 보안 레벨로 Auth(인증)를 입력한 경우 필수) 이 필드는 최대 길이가 32자인 문자열을 나타냅니다.
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)(SNMP: 프라이버시 프로토콜**:**열거 **(DES|AES128|AES192|AES256|3DES))**	(SNMP 보안 레벨로 개인을 입력한 경우 필수) 이 필드는 "DES", "AES128", "AES192", "AES256" 또는 "3DES" 값을 허용합니다.
SNMP:Privacy Password:String(32)(SNMP:프라이버시 비밀번호**:**문자열**(32))**	(SNMP 보안 레벨로 "Priv"(개인)를 입력한 경우 필수) 이 필드는 최대 길이가 32자인 문자열을 나타냅니다.
SNMP:Polling Interval:Integer:600-86400 seconds(SNMP:폴링 간격**:**정수**:600-86,400**초**)**	이 필드는 SNMP 폴링 간격 설정을 위한 필드입니다. 유효한 값은 600~86400의 정수입니다.
SNMP:Is Link Trap Query:Boolean(true|false)(SNMP:링크 트랩 쿼리 여부**:**부울**(true|false))**	SNMP 링크 트랩을 활성화 또는 비활성화하기 위한 필드입니다. 유효한 값은 "true" 또는 "false"입니다.
SNMP:Is MAC Trap Query:Boolean(true|false)(SNMP:MAC 트랩 쿼리 여부**:**부울**(true|false))**	이 필드는 SNMP MAC 트랩을 활성화 또는 비활성화하기 위한 필드입니다. 유효한 값은 "true" 또는 "false"입니다.
SNMP:Originating Policy Services Node:String(32)(SNMP:원래 정책 서비스 노드**:**문자열**(32))**	이 필드는 SNMP 데이터를 폴링하는 데 사용해야 하는 ISE 서버를 나타냅니다. 기본적으로는 자동 설정되지만 다른 값을 이 필드에 할당하여 설정을 덮어쓸 수 있습니다.
Trustsec:Device Id:String(32)(Trustsec:디바이스 **ID:**문자열**(32))**	이 필드는 Cisco Trustsec 디바이스 ID를 나타내며 최대 길이가 32자인 문자열입니다.
Trustsec:Device Password:String(256)(Trustsec: 디바이스 비밀번호**:**문자열**(256))**	(Cisco TrustSec 디바이스 ID를 입력한 경우 필수) 이 필드는 Cisco TrustSec 디바이스 비밀번호를 나타내며 최대 길이가 256자인 문자열입니다.

필드	설명
Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds(Trustsec: 환경 데이터 다운로드 간격**:**정수**:1-2,147,040,000** 초**)**	이 필드는 Cisco TrustSec 환경 데이터 다운로드 간격을 설정하는 필드입니다. 유효한 값은 1~24850의 정수입니다.
Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds(Trustsec: 피어 권한 부여 정책 다운로드 간격**:**정수**:1-2,147,040,000**초**)**	이 필드는 Cisco TrustSec 피어 권한 부여 정책 다운로드 간격을 설정하는 필드입니다. 유효한 값은 1~24850의 정수입니다.
Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds(Trustsec: 재인증 간격**:**정수**:1-2,147,040,000**초**)**	이 필드는 Cisco TrustSec 재인증 간격을 설정하는 필드입니다. 유효한 값은 1~24850의 정수입니다.
Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds(Trustsec:SGACL 목록 다운로드 간격**:**정수**:1-2,147,040,000**초**)**	이 필드는 Cisco TrustSec 보안 그룹 ACL 목록 다운로드 간격을 설정하는 필드입니다. 유효한 값은 1~24850의 정수입니다.
Trustsec:Is Other Trustsec Devices Trusted:Boolean(true|false)(Trustsec:다른 **Trustsec** 디바이스 신뢰 여부**:**부울**(true|false))**	이 필드는 Cisco TrustSec 디바이스의 신뢰 여부를 나타냅니다. 유효한 값은 "true" 또는 "false"입니다.
Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL|DISABLE_ALL)(Trustsec:Trustsec 컨피그레이션 변경사항을 이 디바이스에 알림**:**문자열**(ENABLE_ALL|DISABLE_ALL))**	이 필드는 Cisco TrustSec 디바이스의 Cisco TrustSec 컨피그레이션 변경사항을 알립니다. 유효한 값은 **ENABLE_ALL** 또는 **DISABLE_ALL**입니다.
Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true|false)(Trustsec:보안 그룹 태그 매핑 업데이트 구축 시 이 디바이스 포함**:**부울**(true|false))**	이 필드는 Cisco TrustSec 디바이스가 보안 그룹 태그에 포함되어 있는지 여부를 나타냅니다. 유효한 값은 "true" 또는 "false"입니다.
Deployment:Execution Mode Username:String(32)(구축**:**실행 모드 사용자 이름**:**문자열**(32))**	이 필드는 디바이스 컨피그레이션 편집 권한이 있는 사용자 이름을 나타냅니다. 최대 길이가 32자인 문자열입니다.
Deployment:Execution Mode Password:String(32)(구축**:**실행 모드 비밀번호**:**문자열**(32))**	이 필드는 디바이스 비밀번호를 나타내며 최대 길이가 32자인 문자열입니다.
Deployment:Enable Mode Password:String(32)(구축**:**활성화 모드 비밀번호**:**문자열**(32))**	이 필드는 컨피그레이션을 수정할 수 있는 디바이스의 비밀번호를 나타냅니다. 최대 길이가 32자인 문자열입니다.

필드	설명
Trustsec:PAC issue date:Date(Trustsec:PAC 발급 날짜**:**날짜**)**	이 필드는 Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성한 Cisco TrustSec PAC의 발급 날짜를 표시합니다.
Trustsec:PAC expiration date:Date(Trustsec:PAC 만료 날짜**:**날짜**)**	이 필드는 Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성한 Cisco TrustSec PAC의 만료 날짜를 표시합니다.
Trustsec:PAC issued by:String(Trustsec:PAC 발급자**:**문자열**)**	이 필드는 Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성한 Cisco TrustSec PAC의 발급자 이름(Cisco TrustSec 관리자)을 표시합니다. 문자열 값입니다.

네트워크 디바이스 그룹 가져오기 템플릿 형식

다음 표에서는 템플릿 헤더의 필드를 소개하고 네트워크 디바이스 그룹 CSV 파일의 필드에 대해 설명합니다.

표 ***123: CSV*** 템플릿 필드 및 네트워크 디바이스 그룹에 대한 설명

필드	설명
Name:String(100)(이름:문자열(100)):	(필수) 네트워크 디바이스 그룹 이름 필드입니다. 최대 길이가 100자인 문자열입니다. NDG의 전체 이름은 최대 100자까지 지정할 수 있습니다. 예를 들어 Global(전 세계) > Asia(아시아) 부모 그룹 아래에 하위 그룹 India(인도)를 생성하는 경우 생성하는 NDG의 전체 이름은 Global#Asia#India이며 이 전체 이름의 길이는 100자를 초과할 수 없습니다. NDG의 전체 이름 길이가 100자를 초과하면 NDG 생성이 실패합니다.
Description:String(1024)(설명:문자열(1024))	네트워크 디바이스 그룹 설명(선택 사항)입니다. 최대 길이가 1,024자인 문자열입니다.
Type:String(64)(유형:문자열(64)):	(필수) 네트워크 디바이스 그룹 유형 필드입니다. 최대 길이가 64자인 문자열입니다.
Is Root:Boolean(true|false)(루트 여부:부울(true|false)):	(필수) 특정 네트워크 디바이스 그룹이 루트 그룹인지를 결정하는 필드입니다. 유효한 값은 true 또는 false입니다.

Cisco ISE와 NAD 간의 통신을 보호하기 위한 IPsec 보안

IPsec은 IP에 보안을 제공하는 프로토콜 집합입니다. AAA, RADIUS 및 TACACS+ 프로토콜은 MD5 해싱 알고리즘을 사용합니다. 보안 강화를 위해 Cisco ISE는 IPsec 기능을 제공합니다. IPsec은 발신자를 인증하고, 전송 중에 데이터의 변경 사항을 검색하고, 전송되는 데이터를 암호화하여 보안 통신을 제공합니다.

Cisco ISE는 터널 모드와 전송 모드에서 IPsec을 지원합니다. Cisco ISE 인터페이스에서 IPsec을 활성화하고 피어를 구성하면 Cisco ISE와 NAD 간에 IPsec 터널이 생성되어 통신을 보호합니다.

사전 공유 키를 정의하거나 IPsec 인증에 X.509 인증서를 사용할 수 있습니다. IPsec은 기가비트 이더넷 1 ~ 기가비트 이더넷 5 인터페이스에서 활성화할 수 있습니다. PSN 당 하나의 Cisco ISE 인터페이스에서만 IPsec을 구성할 수 있습니다.

스마트 라이선스가 기본적으로 활성화되어 있으므로(e0/2—> eth2) 기가비트 이더넷 2에서 IPsec을 활성화 할 수 없습니다. 그러나 IP 보안을 활성화해야 하는 경우 스마트 라이선싱을 위해 다른 인터페이스를 선택해야 합니다.

참고 기가비트 이더넷 0 및 본드 0(기가비트 이더넷 0 및 기가비트 이더넷 1 인터페이스가 결합 된 경우)은 Cisco ISE CLI의 관리 인터페이스입니다. IPsec은 기가비트 이더넷 0 및 본드 0에서 지원되지 않습니다.

필수 구성 요소

- Cisco ISE Release 2.2 및 그 이상
- Cisco IOS 소프트웨어, C5921 ESR 소프트웨어 (C5921_I86-UNIVERSALK9-M): ESR 5921 컨피그레이션은 기본적으로 터널 및 전송 모드에서 IPsec을 지원합니다. Diffie-Hellman Group 14와 Group 16이 지원됩니다.

참고 C5921 ESR 소프트웨어는 Cisco ISE 릴리스 2.2 이상과 함께 번들로 제공됩니다. 이를 활성화하려면 ESR 라이선스가 필요합니다. ESR 라이선싱 정보는 Cisco 5921 Embedded Services 라우터 통합 가이드를 참조하십시오.

Cisco ISE에서 RADIUS IPsec 구성

Cisco ISE에서 RADIUS IPsec을 구성하려면 다음을 수행해야합니다.

단계 **1** Cisco ISE CLI에서 인터페이스의 IP 주소를 구성합니다.

기가비트 이더넷 1 ~ 기가비트 이더넷 5 인터페이스(본드 1 및 본드 2)는 IPsec을 지원합니다. 그러나 Cisco ISE 노드의 인터페이스 하나에서만 IPsec을 구성 할 수 있습니다.

단계 **2** IPsec 네트워크 디바이스 그룹에 직접 연결된 네트워크 디바이스를 추가합니다.

참고 RADIUS IPsec을 사용하려면 디바이스의 인터페이스를 통해 고정 경로 게이트웨이를 직접 연결해야 합니다.

a) Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 .
b) **Networks Devices(**네트워크 디바이스**)** 창에서 **Add(**추가**)**를 클릭합니다.
c) 해당 필드에 추가할 네트워크 디바이스의 이름과 IP 주소 및 서브넷을 입력합니다.
d) IPSEC 드롭다운 목록에서 **Yes(**예**)**를 선택합니다.
e) **RADIUS Authentication Settings(RADIUS** 인증 설정**)** 확인란을 선택합니다.
f) **Shared Secret(**공유 암호**)** 필드에 네트워크 디바이스에서 구성한 공유 암호 키를 입력합니다.
g) **Save(**저장**)**를 클릭합니다.

단계 **3** Cisco SMSM(Smart Software Manager)과 상호 작용할 별도의 관리 인터페이스를 추가합니다. ESR(Embedded Services Router)에 대한 정보는 Smart Software Manager Satellite를 참조하십시오. 그렇게 하려면 Cisco ISE CLI에서 다음 명령을 실행하여 해당 관리 인터페이스(기가비트 이더넷 1 ~ 5 (또는 본드 1 또는 2))를 선택합니다.

ise/admin# **license esr smart** {*interface*}

이 인터페이스는 Cisco.com에 연결하여 Cisco 온라인 라이선싱 서버에 액세스할 수 있어야합니다

단계 **4** Cisco ISE CLI에서 직접 연결된 게이트웨이에 네트워크 디바이스를 추가합니다.

ip route [*destination network(*대상 네트워크*)*] [*network mask(*네트워크 마스트*)*] **gateway** [*next-hop address(*다음 홉 주소*)*]

단계 **5** Cisco ISE 노드에서 IPsec을 활성화합니다.

a) Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **IPSec**를 선택합니다.

구축의 모든 Cisco ISE 노드가이 창에 나열됩니다.

b) IPsec을 활성화하려는 Cisco ISE 노드 옆의 확인란을 선택하고 **Enable(**활성화**)** 라디오 버튼을 클릭합니다.
c) 선택한 노드의 **IPSec** 인터페이스: 드롭 다운 목록에서 IPsec 통신에 사용할 인터페이스를 선택합니다.
d) 선택한 Cisco ISE 노드에 대해 다음 인증 유형 중 하나의 라디오 버튼을 클릭합니다.

- **Pre-shared Key(**사전 공유 키**)**: 이 옵션을 선택하는 경우 사전 공유 키를 입력하고 네트워크 디바이스에서 동일한 키를 구성해야 합니다. 사전 공유 키에는 영숫자 문자를 사용합니다. 특수 문자는 사용할 수 없습니다 네트워크 디바이스에서 사전 공유 키를 구성하는 방법에 대한 지침은 네트워크 디바이스 설명서를 참조하십시오. 사전 공유 키 컨피그레이션 출력의 예는 예: Cisco Catalyst 3850 Series 스위치의 사전 공유 키 컨피그레이션 출력, 872 페이지의 내용을 참조하십시오.

- **X.509 Certificates(X.509** 인증서**)**: 이 옵션을 선택하는 경우 Cisco ISE CLI에서 ESR 셸로 이동하여 ESR 5921용 X.509 인증서를 구성 및 설치합니다. 그런 다음 IPsec용 네트워크 디바이스를 구성합니다. 자세한 내용은 ESR-5921에서 X.509 인증서 구성 및 설치, 867 페이지 섹션을 참조하십시오.

e) **Save(**저장**)**를 클릭합니다.

참고 IPsec 컨피그레이션을 직접 수정할 수 없습니다. IPsec이 활성화된 경우 IPsec 터널 또는 인증을 수정하려면 현재 IPsec 터널을 비활성화하고 IPsec 컨피그레이션을 수정한 다음 다른 컨피그레이션으로 IPsec 터널을 다시 활성화합니다.

참고 활성화되면 IPsec이 Cisco ISE 인터페이스에서 IP 주소를 제거하고 인터페이스를 종료합니다. 사용자가 Cisco ISE CLI에서 로그인하면 인터페이스가 IP 주소 없이 종료 상태로 표시됩니다. 이 IP 주소는 ESR-5921 인터페이스에서 구성됩니다.

단계 **6** **esr** 명령을 입력하여 ESR 쉘(shell)을 시작합니다.

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

참고 FIPS 규정 준수를 위해 8자 이상의 비밀번호를 구성해야 합니다. **Enable secret level 1** 명령을 입력하여 비밀번호를 지정합니다.

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

참고 GUI에서 사용자 맞춤화된 RADIUS 포트(1645, 1646, 1812, 1813 이외)를 구성하는 경우 구성된 RADIUS 포트를 수락하려면 ESR 셸에서 다음 CLI 명령을 입력해야합니다.

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

단계 **7** IPsec 터널 및 IPsec 터널을 통한 RADIUS 인증을 확인합니다.

a) Cisco ISE에서 사용자를 추가하고 사용자를 사용자 그룹에 할당합니다(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다).

b) 다음 단계를 수행하여 Cisco ISE와 NAD 간에 IPsec 터널이 설정되었는지 확인합니다.

1. Cisco ISE와 NAD 간의 연결이 설정되었는지 테스트하려면 **ping** 명령을 사용합니다.
2. ESR 셸 또는 NAD CLI에서 다음 명령을 실행하여 연결이 활성 상태인지 확인합니다.

   show crypto isakmp sa

```
ise-esr5921#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.30.1    192.168.30.3    QM_IDLE           1001 ACTIVE
```

3. ESR 셸 또는 NAD CLI에서 다음 명령을 실행하여 터널이 설정되었는지 확인합니다.

   show crypto ipsec sa

```
ise-esr5921#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: radius, local addr 192.168.30.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.30.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (192.168.30.2/255.255.255.255/0/0)
   current_peer 192.168.30.2 port 500
     PERMIT, flags={}
    #pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52
    #pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x393783B6(959939510)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8EA0F6EE(2392913646)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 99, flow_id: SW:99, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237963/2229)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x393783B6(959939510)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 100, flow_id: SW:100, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237970/2229)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

c) 다음 방법 중 하나를 사용하여 RADIUS 인증을 확인합니다.

- 8단계 (a)에서 생성한 사용자의 자격증명을 사용하여 네트워크 디바이스에 로그인합니다. RADIUS 인증 요청이 Cisco ISE 노드로 전송됩니다. **Live Authentications(**라이브 인증**)** 창에서 세부정보를 확인합니다.
- 엔드 호스트를 네트워크 디바이스에 연결하고 802.1X 인증을 구성합니다. 8단계 (a)에서 생성한 사용자의 자격증명을 사용하여 최종 호스트에 로그인합니다. RADIUS 인증 요청이 Cisco ISE 노드로 전송됩니다. **Live Authentications(**라이브 인증**)** 창에서 세부정보를 확인합니다.

ESR-5921에서 X.509 인증서 구성 및 설치

단계 **1** **esr** 명령을 입력하여 ESR 쉘(shell)을 시작합니다.

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

참고 FIPS 규정 준수를 위해 8자 이상의 비밀번호를 구성해야 합니다. **Enable secret level 1** 명령을 입력하여 비밀번호를 지정합니다.

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

참고 GUI에서 사용자 맞춤화된 RADIUS 포트(1645, 1646, 1812, 1813 이외)를 구성하는 경우 ESR 쉘(shell)에서 다음 CLI 명령을 입력하여 구성된 RADIUS 포트를 수락해야 합니다.

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

단계 **2** 다음 명령을 사용하여 RSA 키 페어를 생성합니다.

예제:

```
crypto key generate rsa label rsa2048 exportable modulus 2048
```

단계 **3** 다음 명령을 사용하여 트러스트 포인트를 생성합니다.

예제:

```
crypto pki trustpoint trustpoint-name

enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=networkdevicename.cisco.com
revocation-check none
rsakeypair rsa2048
```

단계 **4** 다음 명령을 사용하여 인증서 서명 요청을 생성합니다.

예제:

```
crypto pki enroll rsaca-mytrustpoint

Display Certificate Request to terminal? [yes/no]: yes
```

단계 **5** 인증서 서명 요청의 출력을 텍스트 파일에 복사하고 서명을 위해 외부 CA에 제출하고 서명된 인증서 및 CA 인증서를 가져옵니다.

단계 **6** 다음 명령을 사용하여 CA(Certificate Authority) 인증서를 가져옵니다.

예제:

```
crypto pki authenticate rsaca-mytrustpoint
```

"—**BEGIN**—" 및 "—**-End**—" 줄을 포함하여 CA 인증서의 내용을 복사하여 붙여 넣습니다.

단계 **7** 다음 명령을 사용하여 서명된 인증서를 가져옵니다.

예제:

```
crypto pki import rsaca-mytrustpoint
```

"—**BEGIN**—" 및 "—**-End**—" 줄을 포함하여 서명된 인증서의 내용을 복사하여 붙여 넣습니다.

다음은 Cisco 5921 ESR에서 X.509 인증서를 구성하고 설치할 때 표시되는 출력의 예입니다.

```
ise-esr5921#show running-config
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address to
send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint rsaca-mytrustpoint
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=ise-5921.cisco.com
revocation-check none
rsakeypair rsa2048
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
```

```
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
crypto pki certificate chain rsaca-mytrustpoint
certificate 39
  30820386 3082026E A0030201 02020139 300D0609 2A864886 F70D0101 0B050030
  61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06
  03550407 0C035254 50310E30 0C060355 040A0C05 43495343 4F310C30 0A060355
  040B0C03 53544F31 19301706 03550403 0C107273 6163612E 65726368 616F2E63
  6F6D301E 170D3136 30393031 32313037 34335A17 0D313730 39303132 31303734
  335A301D 311B3019 06035504 03131269 73652D35 3932312E 63697363 6F2E636F
  6D308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
  0100EE87 CABFBA18 7E0405A8 ACAAAB23 E7CB6109 2CF98BAE 8EE93536 BF1EBBD3
  73E60BE7 F430B5AF EBF8B0C5 969B2828 A6783BB4 64E333E4 29C8744E 6E783617
  194AF1B0 7F04B4EA B89FD6EB F9C4F2DD 196DC6E0 CAA49B8B 665B6E0D 2FBC1D2F
  8E8181B9 60FAE126 D1B2E4E4 1F321A97 10C1B76A C2BB3174 361B13FA 2CB7BDFE
  22C0C33F 2792D714 C41E2237 00B1AE49 6593DCC3 A799D526 D81F9706 A71DA14E
  5ED76038 7A2C84B4 C668E35C 337BA1DC 9CA56AC2 C8E0059F 660CE39C 925310A0
  F9A21FFB 3C3C507A 20B924F7 E0125D60 6552321C 35736079 42449401 15E68DA6
  B4776DAA FB5AFDF8 59E31373 263175E3 1F14416A 24C21D69 A46173B6 96CC84FB
  5B9D0203 010001A3 818C3081 89300906 03551D13 04023000 302C0609 60864801
  86F84201 0D041F16 1D4F7065 6E53534C 2047656E 65726174 65642043 65727469
  66696361 7465301D 0603551D 0E041604 146DD31C 03690B98 330B67FA 6EDC7B20
  F99FB924 60301F06 03551D23 04183016 8014966A 0C21AF96 3E827690 423599CC
  EE8087A1 2909300E 0603551D 0F0101FF 04040302 05A0300D 06092A86 4886F70D
  01010B05 00038201 0100C0B9 D2845D97 6FFC16DB 01559659 BC1DECA6 E1A01965
  1F6CD459 E03D7ABE 91179FEB 08BF5B9B 84B62C36 236F528E E30C921C 81DA29E1
  EA3DFDC1 B0B0EEBA 14EADAEC 078576E4 D643A0EF 7D8E0880 C5FC3965 811B08C0
  5696DBF5 FADA4092 ACF549B8 2257F508 636D52AA 6CDC9596 AB43313F 6C33C9C1
  2CFDDBE3 EA9D407C 8D1B0F49 BBACD0CD 2832AC12 CD3FEFC8 501E1639 A4EFDC27
  69CA0147 971A1B2D DB2758E6 A84AFC86 4F9A4942 3D7EDBCC 7BDCC1BB 61F69B31
  BF13E39B 10AAC31C 55E73C8B C30BE516 7C506FF4 AC367D94 814A6880 EF201A6D
  CD2E1A95 7BBEC982 01CE867D 931F56E1 1EF1C457 9DC9A0BE 9DB2DC9B 19873585
  89AE82F6 A37E51D6 EECD
        quit
certificate ca 008DD3A81106B14664
  308203A2 3082028A A0030201 02020900 8DD3A811 06B14664 300D0609 2A864886
  F70D0101 05050030 61310B30 09060355 04061302 5553310B 30090603 5504080C
  024E4331 0C300A06 03550407 0C035254 50310E30 0C060355 040A0C05 43495343
  4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273 6163612E
```

```
  65726368 616F2E63 6F6D301E 170D3135 31303231 32313135 34335A17 0D323531
  30313832 31313534 335A3061 310B3009 06035504 06130255 53310B30 09060355
  04080C02 4E43310C 300A0603 5504070C 03525450 310E300C 06035504 0A0C0543
  4953434F 310C300A 06035504 0B0C0353 544F3119 30170603 5504030C 10727361
  63612E65 72636861 6F2E636F 6D308201 22300D06 092A8648 86F70D01 01010500
  0382010F 00308201 0A028201 0100CB82 2AECEE38 1BCB27B9 FA5F2FBD 8609B190
  16A6F741 5BEC18B8 8B260CAF 190EA1CE 063BC558 556DC085 6FAC5425 14AFE225
  0E9E3A12 05F3DA7E D17E03F2 7FFE92FB 38D67027 DBC5C175 EB53E96B 66C20D11
  B4C32D38 AE04385C 8FD4CB74 31A97824 CA1CAFD5 091806C3 6F9CBF8D DC42DD5B
  D985703D F3BB9ED1 7DE99614 422D765C 86AB25CD E80008C5 22049BE8 66D1CA27
  E1EB6D4F 4FD3CC18 E091BBF0 6FE0EB52 B33F231A 6D6B7190 4196C929 D22E2C42
  B9CD2BBD 24550E82 8CD8838F C41B4DAD 2FA1636A 5787BBB2 F21E4718 335B005B
  DFBE6EA7 56EBE30B D52DE85F FFAF0189 E372CBFC 44BFF235 4DA7C9EF DAAC6D0A
  A196DA5A 1B525175 C26B3581 EA4B0203 010001A3 5D305B30 1D060355 1D0E0416
  0414966A 0C21AF96 3E827690 423599CC EE8087A1 2909301F 0603551D 23041830
  16801496 6A0C21AF 963E8276 90423599 CCEE8087 A1290930 0C060355 1D130405
  30030101 FF300B06 03551D0F 04040302 02A4300D 06092A86 4886F70D 01010505
  00038201 01002334 A3F0E5D3 4D229985 67A07754 73EC52E3 05B7D05F 926CC863
  220F849B 861C36B2 EF7C3485 474D4EF0 73895879 CAE08BBB 183B7CFA A20C4354
  86C6D9DF D445DACE C252C608 236F6673 F3F3C329 474B22E8 660BF91E 41054B8D
  43B80E44 AE69C164 2C9F41A2 8284F577 21FFAB8E A6771A5E DD34EBE4 A0DC2EAD
  95702010 02964566 478DA90F 5E134643 81A5F5EA 362D0394 1F9F23D1 DEE50B07
  12938299 1AF11A36 82DAFC6A 164B2F66 8B0AB7CC 9A723EBC B50E740B 0A9270E3
  60E2ED42 7F10D1A6 F6735144 AE93BF86 3D5A0502 6811D2BD 6E694693 28DE84C5
  3747CF0A D2B8D6C9 6CBEBA0A D1137CF8 E31CBF6B 437D82DD D74A4A9F 3557B3D9
  D0BD055F 65A8
        quit
license udi pid CISCO5921-K9 sn 9XG4481W768
username lab password 0 lab
!
redundancy
!
crypto keyring MVPN-spokes
rsa-pubkey address 0.0.0.0
  address 0.0.0.0
  key-string
  quit
!
crypto isakmp policy 10
encr aes
hash sha256
group 16
!
crypto isakmp policy 20
encr aes
hash sha256
group 14
crypto isakmp profile MVPN-profile
   description LAN-to-LAN for spoke router(s) connection
   keyring MVPN-spokes
   match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
mode transport
!
crypto dynamic-map MVPN-dynmap 10
set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
interface Ethernet0/0
description e0/0->connection to external NAD
```

```
ip address 192.168.20.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
!
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
transport input none
!
end
```

다음은 Cisco Catalyst 3850 시리즈 스위치에서 X.509 인증서를 구성하고 설치할 때 표시되는 출력의 예입니다.

```
cat3850#show running-config

enable password lab
!
username lab password 0 lab
aaa new-model

!

aaa group server radius ise
server name ise-vm
deadtime 60
!
aaa authentication login default group radius local

aaa authentication enable default group radius enable

!
```

```
crypto isakmp policy 10

encr aes

hash sha256
authentication rsa-sig
group 16
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel

!

crypto ipsec profile radius-profile

!

crypto map radius 10 ipsec-isakmp
set peer 192.168.20.1
set transform-set radius

match address 100

!

interface GigabitEthernet1/0/1
no switchport
ip address 192.168.20.2 255.255.255.0

crypto map radius

!
access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
!
snmp-server community public RO
snmp-server community private RW
!
radius server rad-ise
address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

key secret
```

예: Cisco Catalyst 3850 Series 스위치의 사전 공유 키 컨피그레이션 출력

다음은 Cisco Catalyst 3850 Series 스위치에서 사전 공유 키를 구성할 때 표시되는 출력의 예입니다.

```
cat3850#show running-config

enable password lab
 !
 username lab password 0 lab
 aaa new-model
 !
 aaa group server radius ise
 server name ise-vm
 deadtime 60
 !
 aaa authentication login default group radius local
```

```
 aaa authentication enable default group radius enable

!

crypto isakmp policy 10

 encr aes

 hash sha256
 authentication pre-share
 group 16
 crypto isakmp key 123456789 address 0.0.0.0
 !
 crypto ipsec security-association lifetime seconds 86400
 !
 crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
 !
 crypto ipsec profile radius-profile
 !
 crypto map radius 10 ipsec-isakmp
 set peer 192.168.20.1
 set transform-set radius
 match address 100
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 192.168.20.2 255.255.255.0

 crypto map radius
!
 access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
 !
 snmp-server community public RO
 snmp-server community private RW
 !
 radius server rad-ise
 address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

 key secret
```

Mobile Device Manager와 Cisco ISE와 상호운용성

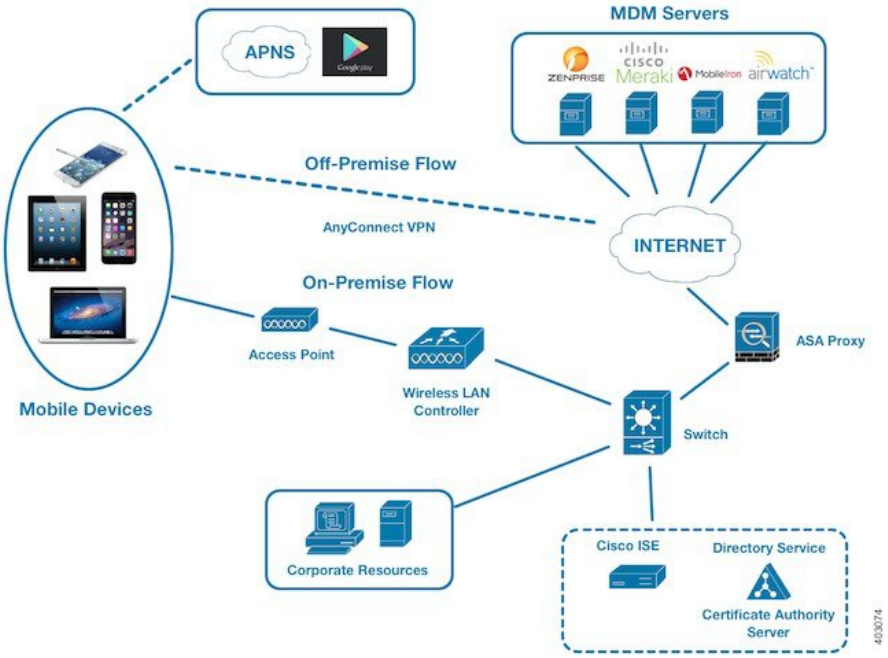
MDM(Mobile Device Management) 서버는 모바일 운영자, 서비스 제공자 및 엔터프라이즈 전반에 걸쳐 구축된 모바일 디바이스를 보호, 모니터링, 관리 및 지원합니다. MDM 서버는 구축된 환경의 모바일 디바이스에 있는 일부 애플리케이션(예: 이메일 애플리케이션)의 사용을 제어하는 정책 서버로 작동합니다. 그러나 네트워크는 ACL(액세스 제어 목록)을 기반으로 엔드포인트에 대한 세부적인 액세스를 제공할 수 있는 유일한 엔티티입니다. Cisco ISE는 MDM 서버에 필요한 디바이스 속성을 쿼리하여 그러한 디바이스에 대한 네트워크 액세스 제어를 제공하는 ACL을 생성합니다.

여러 벤더의 MDM 서버를 비롯하여 여러 활성 MDM 서버를 네트워크에서 실행할 수 있습니다. 이렇게 하면 위치 또는 디바이스 유형과 같은 디바이스 요소를 기반으로 MDM 서버마다 각기 다른 엔드포인트를 라우팅할 수 있습니다.

Cisco ISE는 또한 디바이스에서 Cisco AnyConnect 4.1 및 Cisco Adaptive Security Appliances 9.3.2 이상 버전을 사용하여 VPN을 통해 네트워크에 액세스할 수 있도록 Cisco MDM Server Info API, 버전 2를 사용하여 MDM 서버와 통합됩니다.

다음 그림에서 Cisco ISE는 시행 포인트이고 MDM 정책 서버는 정책 정보 포인트입니다. Cisco ISE는 MDM 서버에서 데이터를 가져와 완벽한 솔루션을 제공합니다.

그림 ***34: Cisco ISE***와의 ***MDM*** 상호운용성



하나 이상의 외부 MDM(Mobile Device Manager) 서버와 상호운용되도록 Cisco ISE를 구성할 수 있습니다. 이 유형의 타사 연결을 설정하면 MDM 데이터베이스에서 사용 가능한 자세한 정보를 활용할 수 있습니다. Cisco ISE에서는 REST API 호출을 사용하여 외부 MDM 서버에서 정보를 가져옵니다. Cisco ISE에서는 스위치, 액세스 라우터, 무선 액세스 포인트 및 다른 네트워크 액세스 포인트에 적절한 액세스 제어 정책을 적용합니다. 이 정책을 통해 Cisco ISE 지원 네트워크에 액세스하는 원격 디바이스를 보다 효과적으로 제어할 수 있습니다.

Cisco ISE에서 지원하는 MDM 벤더 목록은 지원되는 모바일 디바이스 관리 서버, 876 페이지를 참조하십시오.

지원되는 모바일 디바이스 관리 활용 사례

Cisco ISE는 외부 MDM 서버를 이용해 다음과 같은 기능을 수행합니다.

- 디바이스 등록 관리: 네트워크에 액세스하는 등록되지 않은 엔드포인트는 MDM 서버에서 호스팅되는 등록 페이지로 리디렉션됩니다. 디바이스 등록에는 사용자 역할, 디바이스 유형 등이 포함됩니다.
- 디바이스 교정 처리: 교정 중 제한된 액세스 권한만 엔드포인트에 부여됩니다.

- 엔드포인트 데이터 보완: Cisco ISE 프로파일링 서비스를 사용하여 수집할 수 없는 MDM 서버의 정보로 엔드포인트 데이터베이스를 업데이트합니다. Cisco ISE는 **Endpoints(**엔드포인트**)** 창에서 볼 수있는 6가지 디바이스 속성을 사용합니다. Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**를 선택합니다.

  다음은 사용 가능한 디바이스 속성의 예입니다.

- MDMImei: 99 000100 160803 3
- MDMManufacturer: Apple
- MDMModel: iPhone
- MDMOSVersion: iOS 6.0.0
- MDMPhoneNumber: 9783148806
- MDMSerialNumber: DNPGQZGUDTF9

- 4시간마다 MDM 서버를 폴링하여 디바이스 규정 준수 데이터를 확인합니다. **External MDM Servers(**외부 **MDM** 서버**)** 창에서 폴링 간격을 구성합니다. (이 창을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Network Resources(**네트워크 리소스**)** > **Network Resources(**외부 **MDM** 서버**)**를 선택합니다.
- MDM 서버를 통해 디바이스 명령 실행: Cisco ISE가 MDM 서버를 통해 사용자 디바이스에 대한 원격 작업을 발급합니다. **Endpoints(**엔드포인트**)** 창을 통해 Cisco ISE 관리 포털에서 원격 작업을 시작합니다. 이 창을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Context Visibility Endpoints(**상황 가시성 엔드포인트**)** > **Endpoints(**엔드포인트**)**를 선택합니다. MDM 서버 옆의 확인란을 선택하고 **MDM Actions(MDM** 작업**)**를 클릭합니다. 표시되는 드롭다운 목록에서 필요한 작업을 선택합니다.

벤더 **MDM** 속성

Cisco ISE에서 MDM 서버를 구성하면 Cisco ISE 시스템 사전에 **mdm**이라는 이름의 새 항목에 벤더의 속성이 추가됩니다. 다음 속성은 등록 상태에 사용되며 일반적으로 MDM 벤더에서 지원합니다.

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus
- JailBrokenStatus
- Manufacturer
- IMEI

- SerialNumber
- OsVersion
- PhoneNumber
- MDMServerName
- MDMServerReachable
- MEID
- Model
- UDID

벤더의 고유한 속성이 지원되지 않는 경우 ERS API를 사용하여 벤더별 속성을 교환할 수 있습니다. 지원되는 ERS API에 대한 자세한 내용은 벤더의 설명서를 참조합니다.

권한 부여 정책에 사용 가능한 새 MDM 사전 속성을 확인할 수 있습니다.

지원되는 모바일 디바이스 관리 서버

지원되는 MDM 서버에는 다음 벤더의 제품이 포함됩니다.

- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Cisco0 Meraki Systems Manager
- Citrix Endpoint Management(이전 명칭: Xenmobile)
- Globo
- IBM MaaS360
- JAMF Casper Suite
- Microsoft Intune(모바일 디바이스용)
- Microsoft SCCM(데스크톱 디바이스용)
- MobileIron UEM

참고 일부 MobileIron 버전은 Cisco ISE에서 작동하지 않습니다. MobileIron에서 이 문제를 인지하고 있으며 해결 방법을 마련했습니다. 자세한 내용은 MobileIron에 문의하십시오.

- Mosyle

- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE(이전 명칭: AirWatch)
- 42 Gears

ISE 커뮤니티 리소스

How To: Meraki EMM / MDM Integration with ISE

모바일 디바이스 관리 서버에서 사용하는 포트

다음 표에는 Cisco ISE와 MDM 서버가 서로 통신할 수 있도록 하려면 열어야 하는 포트가 나와 있습니다. MDM 에이전트와 서버에서 열어야 하는 포트의 목록은 MDM 벤더 설명서를 참고해 주십시오.

표 ***124: MDM*** 서버에서 사용되는 포트

MDM 서버	포트
MobileIron	443
Zenprise	443
Good	19005
Airwatch	443
Afaria	443
Fiberlink MaaS	443
Meraki	443
Microsoft Intune	80 및 443
Microsoft SCCM	80 및 443

모바일 디바이스 관리 통합 프로세스 플로우

1. 사용자가 SSID를 사용하여 디바이스를 연결합니다.
2. Cisco ISE에서 MDM 서버에 대한 API 호출을 수행합니다.
3. 이 API 호출에서는 사용자의 디바이스 목록 및 디바이스의 포스처 상태가 반환됩니다.

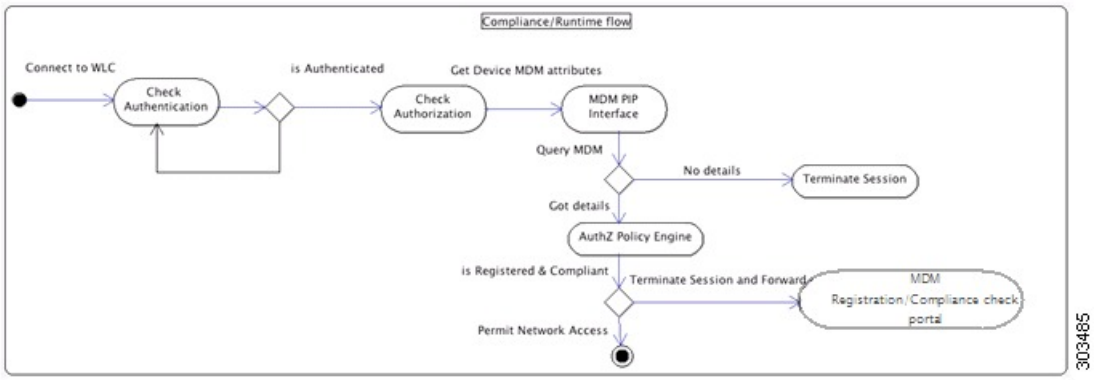
참고 입력 매개변수는 엔드포인트 디바이스의 MAC 주소입니다. 오프프레미스 Apple iOS 디바이스(VPN을 통해 Cisco ISE에 연결하는 모든 디바이스)의 경우 입력 매개변수는 UDID입니다.

4. 이 목록에 없는 사용자 디바이스는 등록되지 않은 것입니다. Cisco ISE가 Cisco ISE로의 리디렉션을 위한 권한 부여 요청을 NAD에 보냅니다. 그러면 사용자에게 MDM 서버 페이지가 표시됩니다.

참고 MDM 포털을 통해 Cisco ISE 네트워크 외부의 MDM 서버에 등록된 디바이스를 등록해야 합니다. 이는 Cisco ISE 릴리스 1.4 이상에 적용됩니다. 이전 Cisco ISE 버전에서는 Cisco ISE 지원 네트워크 외부에 등록된 디바이스가 포스처 정책을 준수하는 경우 자동으로 등록될 수 있습니다.

5. Cisco ISE가 MDM을 사용하여 디바이스를 프로비저닝하고 사용자가 디바이스를 등록할 수 있는 적절한 창을 표시합니다.
6. 사용자가 MDM 서버에서 디바이스를 등록합니다. 그러면 MDM 서버가 자동 리디렉션 또는 수동 브라우저 새로 고침을 통해 요청을 Cisco ISE로 리디렉션합니다.
7. Cisco ISE가 MDM 서버를 다시 쿼리하여 포스처 상태를 확인합니다.
8. 사용자 디바이스가 MDM 서버에 구성되어 있는 포스처(규정 준수) 정책을 준수하지 않으면 디바이스가 규정을 준수하지 않는다는 알림이 사용자에게 표시됩니다. 사용자는 디바이스가 규정을 준수하도록 필요한 조치를 취해야 합니다.
9. 사용자 디바이스가 규정을 준수하면 MDM 서버가 내부 표에서 디바이스 상태를 업데이트합니다.
10. 사용자가 지금 브라우저를 새로 고치면 제어권이 Cisco ISE로 다시 전송됩니다.
11. Cisco ISE가 4시간마다 MDM 서버를 폴링하여 규정 준수 정보를 가져오고 적절한 CoA(Change of Authorization)를 발급합니다. 폴링 간격을 구성할 수 있습니다. 또한 Cisco ISE는 MDM 서버가 사용 가능한 상태인지를 5분마다 확인합니다.

다음 그림에는 MDM 프로세스 플로우이 나와 있습니다.



참고 각 디바이스는 한 번에 하나의 MDM 서버에만 등록할 수 있습니다. 다른 벤더의 MDM 서비스에 동일한 디바이스를 등록하려는 경우에는 이전 벤더의 프로파일을 디바이스에서 제거해야 합니다. MDM 서비스는 대개 "회사 초기화" 기능을 제공합니다. 이 기능은 디바이스(전체 디바이스 아님)의 벤더 컨피그레이션만 삭제합니다. 사용자가 파일을 제거할 수도 있습니다. 예를 들어 사용자는 iOS 디바이스에서 Settings(설정) > General(일반) >Device management(디바이스 관리) 창으로 이동하여 **Remove management(**제거 관리**)**를 클릭할 수 있습니다. 또는 사용자가 ISE에서 내 디바이스 포털로 이동하여 **Corporate Wipe(**회사 초기화**)**를 클릭할 수도 있습니다.

Cisco ISE를 통한 모바일 디바이스 관리 서버 설정

Cisco ISE를 사용하여 MDM 서버를 설정하려면 다음과 같은 높은 수준의 작업을 수행해야 합니다.

단계 **1** MDM 서버 인증서를 Cisco ISE로 가져옵니다. 단, Intune의 경우에는 PAN(Policy Administration Node)의 인증서를 Azure로 가져옵니다.

단계 **2** Mobile Device Manager 정의를 생성합니다.

단계 **3** Wireless LAN Controller에서 ACL을 구성합니다.

단계 **4** 등록되지 않은 디바이스를 MDM 서버로 리디렉션하는 권한 부여 프로파일을 구성합니다.

단계 **5** 네트워크에 여러 MDM 서버가 있는 경우 각 벤더에 대해 별도의 권한 부여 프로파일을 구성합니다.

단계 **6** MDM 활용 사례용으로 권한 부여 정책 규칙을 구성합니다.

Cisco ISE로 모바일 디바이스 관리 서버 인증서 가져오기

Cisco ISE가 MDM 서버와 연결할 수 있도록 하려면 MDM 서버 인증서를 Cisco ISE 신뢰할 수 있는 인증서 저장소로 가져와야 합니다. MDDM 서버에 CA가 서명한 인증서가 있는 경우에는 루트 인증서를 Cisco ISE 신뢰할 수 있는 인증서 저장소로 가져와야 합니다.

참고 Microsoft Azure의 경우 Cisco ISE 인증서를 Azure로 가져옵니다. 모바일 디바이스 관리 서버로 Microsoft Intune을 Cisco ISE에 연결, 883 페이지의 내용을 참조하십시오.

단계 **1** MDM 서버에서 MDM 서버 인증서를 내보낸 다음 로컬 머신에 저장합니다.

단계 **2** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificate(**신뢰할 수 있는 인증서**)** > **Import(**가져오기**)**를 선택합니다.

단계 **3** **Import a new Certificate into the Certificate Store(**인증서 저장소로 새 인증서 가져오기**)** 창에서 **Choose File(**파일 선택**)**을 클릭하여 MDM 서버에서 가져온 MDM 서버 인증서를 선택합니다.

단계 4 **Friendly Name(**식별 이름**)** 필드에 인증서의 이름을 입력합니다.

단계 5 **Trust for authentication within ISE(ISE** 내의 인증 신뢰**)** 확인란을 선택합니다.

단계 6 **Submit(**제출**)**을 클릭합니다.

단계 7 **Trust Certificates(**신뢰 인증서**)** 창에 새로 추가된 MDM 서버 인증서가 나열되어 있는지 확인합니다.

다음에 수행할 작업

Cisco ISE에서 디바이스 관리 서버 정의, 880 페이지

에 전달하는 고성능 고속 어플라이언스입니다.

Cisco ISE에서 디바이스 관리 서버 정의

Cisco ISE가 필요한 서버와 통신할 수 있도록 Cisco ISE에서 모바일 및 데스크톱 디바이스 관리 서버를 정의합니다. 서버와의 통신에 사용되는 인증 유형, Cisco ISE가 디바이스 관리 서버에서 디바이스 정보를 요청하는 빈도 등을 구성할 수 있습니다.

모바일 관리 서버를 정의하려면 Cisco ISE에서 모바일 디바이스 관리 서버 정의, 880 페이지의 내용을 참조하십시오.

Microsoft SCCM(System Center Configuration Manager) 서버를 정의하려면 데스크톱 디바이스 관리자 서버에서 엔드포인트 규정 준수에 대한 구성 베이스라인 정책 선택를 참조하십시오.

Cisco ISE에서 모바일 디바이스 관리 서버 정의

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)**

단계 2 **MDM Servers(MDM** 서버**)** 창에서 를 클릭합니다.

단계 3 추가할 MDM 서버의 이름과 설명을 해당 필드에 입력합니다.

단계 4 **Server Type(**서버 유형**)** 드롭 다운 목록에서 **Mobile Device Manager(**모바일 디바이스 관리자**)**를 선택합니다.

단계 5 **Authentication Type(**인증 유형**)** 드롭다운 목록에서 **Basic(**기본**)** 또는 **OAuth - Client Credentials(OAuth -** 클라이언트 자격 증명**)**을 선택합니다.

Basic(기본**)** 인증 유형을 선택하면 다음 필드가 표시됩니다.

- **Host Name / IP Address(**호스트 이름**/IP** 주소**)**: MDM 서버의 호스트 이름 또는 IP 주소를 입력합니다.
- **Port(**포트**)**: MDM 서버에 연결할 때 사용할 포트(일반적으로 443)를 입력합니다,
- **Instance Name(**인스턴스 이름**)**: 이 MDM 서버에 인스턴스가 여러 개 있는 경우 연결하려는 인스턴스를 입력합니다.
- **Username(**사용자 이름**)**: MDM 서버에 연결하는 데 사용해야 하는 사용자 이름을 입력합니다.
- **Password(**비밀번호**)**: MDM 서버에 연결하는 데 사용할 비밀번호를 입력합니다.

- **Polling Interval(**폴링 간격**)**: Cisco ISE가 규정 준수 확인 정보를 위해 MDM 서버를 폴링할 폴링 간격을 분 단위로 입력합니다. 이 값은 MDM 서버의 폴링 간격과 동일해야 합니다. 유효 범위는 15분~1440분입니다. 기본값은 240분입니다. 네트워크의 활성 클라이언트 몇 개를 테스트할 경우 폴링 간격을 60분 미만으로 설정하는 것이 좋습니다. 활성 클라이언트가 많은 프로덕션 환경에서 이 값을 60분 미만으로 설정하면 시스템의 로드가 크게 증가하여 성능이 저하될 수 있습니다.

  폴링 간격을 0으로 설정하면 Cisco ISE는 MDM 서버와의 통신을 비활성화합니다.

- **Time Interval For Compliance Device ReAuth Query(**규정 준수 디바이스 재인증 쿼리 시간 간격**)**: 엔드포인트가 인증되거나 재인증되는 경우 Cisco ISE는 캐시를 사용하여 해당 엔드포인트에 대한 MDM 변수를 가져옵니다. 캐시된 값의 기간이 이 필드에 구성된 값보다 높은 경우 Cisco ISE는 새 디바이스 쿼리를 MDM 서버로 보내 새 값을 가져옵니다. 규정 준수 상태가 변경된 경우 Cisco ISE는 적절한 CoA를 트리거합니다.

  유효 범위는 1분~1440분입니다. 기본값은 1분입니다.

OAuth - Client Credentials(클라이언트 자격 증명**)** 인증 유형을 선택하면 다음 필드가 표시됩니다.

- **Auto Discovery(**자동 검색**)** 드롭다운 목록에서 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다.

- **Auto Discovery URL(**자동 검색 **URL)**: Microsoft Azure 관리 포털에서 *Microsoft Azure AD Graph API* 엔드포인트의 값을 입력합니다. 이 URL은 애플리케이션이 Graph API를 사용하여 Microsoft Azure AD 디렉토리 내의 디렉토리 데이터에 액세스할 수 있는 엔드포인트입니다. URL 형식은 `https://<hostname>/<tenant id>`입니다.

  예를 들어 `https://graph.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329`가 될 수 있습니다.

  이 URL을 펼친 버전은 `https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>`와 같은 형식의 속성 파일에도 있습니다.

- **Client ID(**클라이언트 **ID)**: 애플리케이션의 고유 식별자입니다. 애플리케이션이 Microsoft Azure AD Graph API, Microsoft Intune API 등 다른 애플리케이션의 데이터에 액세스하는 경우 이 속성을 사용합니다.

- **Token Issuing URL(**토큰 발급 **URL)**: 이전 단계의 *Oauth2.0 Authorization Endpoint(Oauth2.0* 권한 부여 엔드포인트*)* 값을 입력합니다. 이 엔드포인트에서 앱이 OAuth2.0을 사용하여 액세스 토큰을 얻습니다. 앱이 인증되고 나면 Microsoft Azure AD는 앱(Cisco ISE)에 액세스 토큰을 발급합니다. 그러면 앱이 Graph API 또는Intune API를 호출할 수 있습니다.

- **Token Audience(**토큰 대상**)**: 토큰의 사용 대상인 수신자 리소스로, Microsoft Intune API에 대한 알려진 공용 **(APP ID URL)**앱 **ID URL**입니다.

- **Polling Interval(**폴링 간격**)**: Cisco ISE가 규정 준수 확인 정보를 위해 MDM 서버를 폴링할 폴링 간격을 분 단위로 입력합니다. 이 값은 MDM 서버의 폴링 간격과 동일해야 합니다. 유효 범위는 15분~1440분입니다. 기본값은 240분입니다. 네트워크의 활성 클라이언트 몇 개를 테스트할 경우 폴링 간격을 60분 미만으로 설정하는 것이 좋습니다. 활성 클라이언트가 많은 프로덕션 환경에서 이 값을 60분 미만으로 설정하면 시스템의 로드가 크게 증가하여 성능이 저하될 수 있습니다.

  폴링 간격을 0으로 설정하면 Cisco ISE는 MDM 서버와의 통신을 비활성화합니다.

- **Time Interval For Compliance Device ReAuth Query(**규정 준수 디바이스 재인증 쿼리 시간 간격**)**: 엔드포인트가 인증되거나 재인증되는 경우 Cisco ISE는 캐시를 사용하여 해당 엔드포인트에 대한 MDM 변수를 가져옵니

다. 캐시된 값의 기간이 이 필드에 구성된 값보다 높은 경우 Cisco ISE는 새 디바이스 쿼리를 MDM 서버로 보내 새 값을 가져옵니다. 규정 준수 상태가 변경된 경우 Cisco ISE는 적절한 CoA를 트리거합니다.

유효 범위는 1분~1440분입니다. 기본값은 1분입니다.

단계 **6** **Status(**상태**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

단계 **7** MDM 서버가 Cisco ISE에 연결되어 있는지 확인하려면 **Test Connection(**연결 테스트**)**을 클릭합니다. **Test Connection(**테스트 연결**)**은 모든 활용 사례(베이스 라인 가져 오기, 디바이스 정보 가져 오기 등)에 대한 권한을 확인하기 위한 것이 아닙니다. 이들은 서버가 Cisco ISE에 추가될 때 검증됩니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

Microsoft Intune 및 Microsoft System Center Configuration Manager에 대한 Cisco ISE 모바일 디바이스 관리 지원

- **Microsoft Intune**: Cisco ISE는 모바일 디바이스를 관리하는 파트너 MDM 서버로 Microsoft Intune 디바이스 관리를 지원합니다.

  모바일 디바이스를 관리하는 Microsoft Intune 서버에서 Cisco ISE를 OAuth 2.0 클라이언트 애플리케이션으로 구성합니다. Cisco ISE는 Azure에서 토큰을 가져와 해당 Cisco ISE Intune 애플리케이션과 세션을 설정합니다.

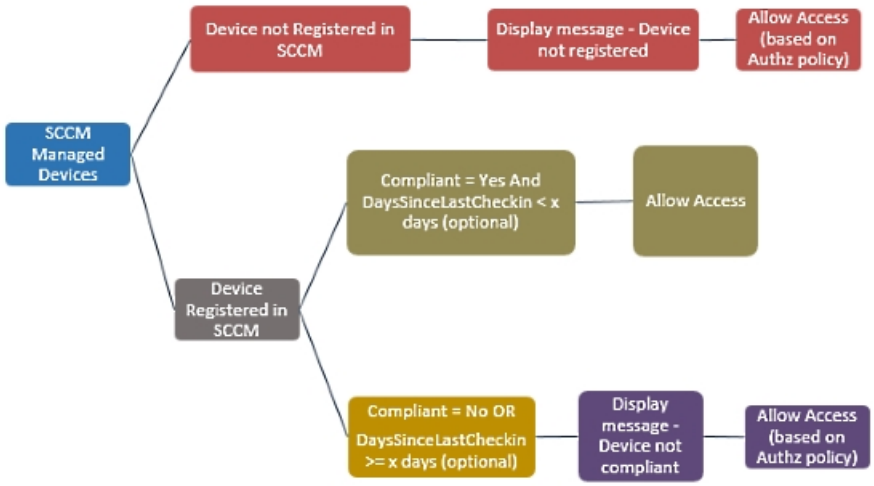
  Microsoft Intune이 클라이언트 애플리케이션과 통신하는 방법에 대한 자세한 내용은 https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx를 참고하십시오.

- 데스크톱 디바이스 관리자**(Microsoft SCCM)**: Cisco ISE는 Windows 컴퓨터를 관리하는 파트너 MDM 서버로 Microsoft SCCM(System Center Configuration Manager)을 지원합니다. ISE는 WMI를 사용하여 SCCM 서버에서 규정 준수 정보를 검색하며 해당 정보를 사용하여 사용자의 Windows 디바이스에 대한 네트워크 액세스 권한을 부여하거나 거부합니다.

Microsoft SCCM 워크플로우

Cisco ISE는 디바이스 등록 여부 및 디바이스가 등록된 경우 규정 준수 여부에 대해 Microsoft SCCM 서버에서 정보를 검색할 수 있습니다. 다음 다이어그램에는 Microsoft SCCM에서 관리하는 디바이스의 워크플로우가 나와 있습니다.

그림 ***35: SCCM*** 워크플로우



디바이스가 네트워크에 연결되고 Microsoft SCCM 정책이 일치하면 Cisco ISE는 권한 부여 정책에 지정된 SCCM 서버를 쿼리하여 규정 준수 및 마지막 로그인(체크인) 시간을 검색합니다. 이 정보를 사용해 Cisco ISE는 **Endpoint(**엔드포인트**)** 목록에서 디바이스의 규정 준수 상태 및 lastCheckinTimeStamp를 업데이트합니다.

디바이스가 규정을 준수하지 않거나 Microsoft SCCM에 등록되어 있지 않으며 권한 부여 정책에서 리디렉션 프로파일이 사용되는 경우에는 디바이스가 규정을 준수하지 않거나 Microsoft SCCM에 등록되어 있지 않다는 메시지가 사용자에게 표시됩니다. 사용자가 메시지를 확인하고 나면 Cisco ISE는 Microsoft SCCM 등록 사이트에 CoA를 실행할 수 있습니다. 권한 부여 정책과 프로파일에 따라 사용자에게 액세스 권한이 부여됩니다.

Microsoft SCCM 서버 연결 모니터링

Microsoft SCCM에 대한 폴링 간격을 구성할 수 없습니다.

Cisco ISE는 Microsoft SCCM 서버 연결을 확인하는 MDM 하트비트 작업을 실행하며 Microsoft SCCM 서버 연결이 끊기면 경보를 생성합니다. 하트비트 작업 간격은 구성할 수 없습니다.

모바일 디바이스 관리 서버로 **Microsoft Intune**을 **Cisco ISE**에 연결

단계 **1** Microsoft Azure 포털에 로그인하고 **Active Directory**를 선택합니다.

단계 **2** **New Registration(**새 등록**)**을 클릭합니다.

단계 **3** 표시되는 **Register An Application(**애플리케이션 등록**)** 창에서 **Name(**이름**)** 필드에 값을 입력합니다.

단계 **4** **Supported Account Types(**지원되는 계정 유형**)** 영역에서 **Accounts in this organizational directory only(**이 조직 디렉토리에 있는 계정만**)** 라디오 버튼을 클릭합니다.

단계 **5** **Register(**등록**)**를 클릭합니다.

단계 **6** 새로 등록된 애플리케이션의 **Overview(**개요**)** 창이 표시됩니다. 이 창이 열린 상태에서 Cisco ISE 관리 포털에 로그인합니다.

단계 **7** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System(**시스템**)** > **Certificates(**인증서**)**를 선택합니다.

단계 **8** 표시된 인증서 목록에서 기본 자가서명 서버 인증서 또는 관리자 사용을 위해 구성한 다른 인증서를 선택합니다. 원하는 인증서의 확인란을 선택합니다.

단계 **9** **Export(**내보내기**)**를 클릭합니다.

단계 **10** 표시되는 대화 상자에서 **Export Certificate Only(**인증서만 내보내기**)** 라디오 버튼을 클릭하고 **Export(**내보내기**)**를 클릭합니다.

단계 **11** 해당 인증서의 세부정보를 보려면 **View(**보기**)**를 클릭합니다. 표시된 **Certificate Hierarchy(**인증서 계층 구조**)** 대화 상자를 아래로 스크롤하여 **Fingerprints(**핑거프린트**)** 영역으로 이동합니다. 이후 단계에서 해당 값을 참조하게 됩니다.

단계 **12** Microsoft Azure Active Directory 포털의 왼쪽 메뉴 패널에서 **Certificates and Secrets(**인증서 및 암호**)**를 클릭합니다.

단계 **13** **Upload Certificate(**인증서 업로드**)**를 클릭하고 Cisco ISE에서 내보낸 인증서를 업로드합니다.

단계 **14** 인증서가 업로드되면 창에 표시되는 지문 값이 Cisco ISE 인증서의 핑거프린트 값과 일치하는지 확인합니다.

단계 **15** 왼쪽 메뉴 패널에서 **Manifest(**매니페스트**)**를 선택합니다.

단계 **16** 표시되는 콘텐츠에서 **displayName**의 값을 확인합니다. 값은 Cisco ISE 인증서에 나와 있는 공용 이름과 일치해야 합니다.

단계 **17** 왼쪽 메뉴 패널에서 **API Permissions(API** 권한**)**를 선택합니다.

단계 **18** **Add(**추가**)**를 클릭하고 다음 권한을 추가합니다.

API / Permissions name	Type	Description	Admin consent req...	Status
∨ Intune (1)				
get_device_compliance	Application	Get device state and compliance information from Micr...	Yes	Granted
∨ Microsoft Graph (6)				
DeviceManagementConfigurat	Delegated	Read Microsoft Intune Device Configuration and Policies	Yes	Granted
DeviceManagementServiceCo	Delegated	Read Microsoft Intune configuration	Yes	Granted
Directory.Read.All	Delegated	Read directory data	Yes	Granted
Directory.Read.All	Application	Read directory data	Yes	Granted
openid	Delegated	Sign users in	-	Granted
User.Read	Delegated	Sign in and read user profile	-	Granted

단계 **19** 애플리케이션의 **Overview(**개요**)** 창에서 다음 세부정보를 수집합니다.

- 애플리케이션**(**클라이언트**) ID**
- 디렉토리**(**테넌트**) ID**

단계 **20** **Overview(**개요**)** 창에서 **Endpoints(**엔드포인트**)**를 클릭하고 **Oauth 2.0 Token Endpoint (V2)(Oauth 2.0** 토큰 엔드포인트**(V2))** 필드의 값을 복사합니다.

단계 **21** PEM(체인) 형식으로 https://graph.windows.net 및 https://fef.msuc05.manage.microsoft.com/에서 인증서를 다운로드합니다. 다음 인증서를 다운로드해야 합니다.

- Microsoft IT TLS CA 1

- Baltimore CyberTrust Root
- DigiCert SHA2 Secure Server CA
- DigiCert Global Root CA

단계 **22** Cisco ISE 관리 포털에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **23** 다운로드한 4개의 인증서 각각에 대해 다음 단계를 수행합니다.

1. **Import(**가져오기**)**를 클릭합니다.
2. **Choose File(**파일 선택**)**을 클릭하고 시스템에서 다운로드한 인증서를 선택합니다.
3. 인프라 및 Cisco Services에서 인증서를 신뢰할 수 있도록 허용합니다. **Usage(**사용**)** 영역에서 **Trust for authentication within ISE(ISE** 내의 인증 신뢰**)** 및 **Trust for authentication of Cisco Services(Cisco Services**의 인증 신뢰**)** 확인란을 선택합니다.
4. **Save(**저장**)**를 클릭합니다.

단계 **24** 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)**을 선택합니다.

단계 **25** **Add(**추가**)**를 클릭합니다.

단계 **26** **Name(**이름**)** 필드에 값을 입력합니다.

단계 **27** **Authentication Type(**인증 유형**)** 드롭다운 목록에서 **OAuth – Client Credentials(OAuth -** 클라이언트 자격 증명**)**를 선택합니다.

단계 **28** 다음 필드에는 Microsoft Azure Active Directory의 Microsoft Intune 애플리케이션의 정보가 필요합니다.

1. **Auto Discovery URL(**자동 검색 **URL)** 필드에 “https://graph.windows.net/<디렉토리*(*테넌트*) ID*>”를 입력합니다.
2. **Client ID(**클라이언트 **ID)** 필드에 Microsoft Intune 애플리케이션의 애플리케이션**(**클라이언트**) ID** 값을 입력합니다.
3. **Token Issuing URL(**토큰 발급 **URL)** 필드에 **Oauth 2.0** 토큰 엔드포인트**(V2)** 값을 입력합니다.

단계 **29** **Polling Interval(**폴링 간격**)** 및 **Time Interval For Compliance Device ReAuth Query(**규정 준수 디바이스 재인증 쿼리 시간 간격**)** 필드에 원하는 값을 입력합니다.

단계 **30** **Test Connection(**연결 테스트**)**을 클릭하여 Cisco ISE에서 Microsoft 서버에 연결할 수 있는지 확인합니다.

단계 **31** 연결 테스트에 성공하면 **Status(**상태**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

단계 **32** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

Cisco ISE 관리 포털에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)**을 클릭합니다. 추가된 Microsoft Intune 서버가 표시된 **MDM Server(MDM** 서버**)** 목록에 나타나야 합니다.

Microsoft System Center Configuration Manager용 정책 집합 예

Microsoft SCCM을 지원하기 위해 다음과 같은 새로운 사전 항목을 정책에서 사용할 수 있습니다.

- **MDM.DaysSinceLastCheckin**: 사용자가 마지막으로 Microsoft SCCM에 디바이스를 체크인하거나 동기화한 이후 경과된 기간(일)입니다. 유효한 값 범위는 1일~365일입니다.
- **MDM.UserNotified**: 유효한 값은 **Y** 또는 **N**입니다. 이 값은 사용자에게 디바이스가 등록되지 않았다는 알림을 받았는지를 나타냅니다. 그런 다음 사용자는 네트워크에 대한 제한된 액세스를 허용한 뒤 등록 포털로 리디렉션하거나 네트워크에 대한 액세스를 거부할 수 있습니다.
- **MDM.ServerType**: 유효한 값은 MDM 서버용 **MDM** 및 데스크톱 디바이스 관리용 **DM**입니다.

Microsoft SCCM을 지원하는 정책 집합의 예는 다음과 같습니다.

정책 이름	**If**	**Then**
SCCM_Comp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	PermitAccess
SCCM_NonComp_Notify	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	PermitAccess
SCCM_NonComp_Days	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	SCCMRedirect

정책 이름	If	Then
SCCM_NonComp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	SCCMRedirect
SCCM_UnReg_Notify	Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	PermitAccess

Cisco ISE에 Microsoft System Center Configuration Manager 서버 구성

Cisco ISE는 WMI(Windows Management Instrumentation)를 사용하여 Microsoft SCCM 서버와 통신합니다. Microsoft SCCM을 실행 중인 Windows 서버에서 WMI를 구성합니다.

참고 Cisco ISE 통합에 사용하는 사용자 계정은 다음 중 하나여야 합니다.

- SMS 관리자 사용자 그룹의 멤버여야 합니다.
- WMI 네임스페이스에서 SMS 개체와 동일한 권한을 갖습니다.

  `root\sms\site_<sitecode>`

  여기서 *sitecode*는 Microsoft SCCM 사이트입니다.

Microsoft Active Directory 사용자가 도메인 관리자 그룹에 있을 때의 권한 설정

Windows Server 2008 R2, Windows Server 2012 및 Windows Server 2012 R2의 경우 도메인 관리자 그룹에는 기본적으로 Windows 운영체제의 특정 레지스트리 키에 대한 모든 제어 권한이 없습니다. Microsoft Active Directory 관리자는 Microsoft Active Directory 사용자에게 다음 레지스트리 키에 대한 모든 제어 권한을 부여해야 합니다.

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

다음 Microsoft Active Directory 버전의 경우에는 레지스트리를 변경할 필요가 없습니다.

- Windows 2003
- Windows 2003R2

- Windows 2008

모든 제어 권한을 부여하려면 Microsoft Active Directory 관리자가 먼저 다음과 같이 키 소유권을 얻어야 합니다.

단계 **1** 키 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **Owner(**소유자**)** 탭을 선택합니다.

단계 **2** **Permissions(**권한**)**를 클릭합니다.

단계 **3** **Advanced(**고급**)**를 클릭합니다.

도메인 관리자 그룹에 속하지 않은 **Microsoft Active Directory** 사용자에 대한 권한

Windows 2012 R2의 경우 Microsoft AD 사용자에게 다음 레지스트리 키에 대한 모든 제어 권한을 부여합니다.

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Windows PowerShell에서 다음 명령을 사용하여 레지스트리 키에 대한 전체 권한이 부여되었는지 확인합니다.

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

Microsoft AD 사용자가 도메인 관리자 그룹에는 없지만 도메인 사용자 그룹에는 있으면 다음 권한이 필요합니다.

- Cisco ISE가 도메인 컨트롤러에 연결할 수 있도록 레지스트리 키 추가
- 도메인 컨트롤러에서 DCOM을 사용하기 위한 권한, 578 페이지
- WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정, 580 페이지

이러한 권한은 다음 Microsoft AD 버전에만 필요합니다.

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012

- Windows 2012 R2
- Windows 2016

Cisco ISE가 도메인 컨트롤러에 연결할 수 있도록 레지스트리 키 추가

Cisco ISE가 도메인 사용자로 연결하여 로그인 인증 이벤트를 검색할 수 있게 하려면 도메인 컨트롤러에 일부 레지스트리 키를 수동으로 추가해야 합니다. 도메인 컨트롤러 또는 도메인의 머신에서 에이전트는 필요하지 않습니다.

다음 레지스트리 스크립트에는 추가할 키가 나와 있습니다. 이 스크립트를 복사하여 텍스트 파일에 붙여 넣고 파일을 .reg 확장자로 저장한 다음 파일을 더블 클릭하여 레지스트리를 변경합니다. 레지스트리 키를 추가하려면 사용자가 루트 키의 소유자여야 합니다.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

DllSurrogate 키의 값에는 공백이 두 개 포함되어야 합니다. 레지스트리를 수동으로 업데이트하는 경우 두 개의 공백만 포함하고 따옴표는 포함하지 않아야 합니다. 레지스트리를 수동으로 업데이트하는 동안 AppID, DllSurrogate 및 해당 값에 따옴표가 포함되지 않았는지 확인하십시오.

파일 맨 끝의 빈 줄을 포함하여 위 스크립트에 나와 있는 빈 줄은 그대로 유지합니다.

Windows 명령 프롬프트에서 다음 명령을 사용하여 레지스트리 키가 생성되었고 올바른 값을 가지고 있는지 확인합니다.

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

도메인 컨트롤러에서 **DCOM**을 사용하기 위한 권한

Cisco ISE 패시브 ID 서비스에 사용되는 Microsoft Active Directory 사용자는 도메인 컨트롤러 서버에서 DCOM을 사용할 권한이 있어야 합니다. **dcomcnfg** 명령줄 도구를 사용하여 권한을 구성하십시오.

단계 **1** 명령줄에서 **dcomcnfg** 도구를 실행합니다.

단계 **2** **Component Services(**구성 요소 서비스**)**를 펼칩니다.

단계 **3** **Computers(**컴퓨터**)** > **My Computer(**내 컴퓨터**)**를 펼칩니다.

단계 **4** 메뉴 모음에서 **Action(**작업**)**을 선택하고 **Properties(**속성**)**를 클릭한 후 **COM Security(COM** 보안**)**를 클릭합니다.

단계 **5** Cisco ISE가 액세스 및 실행에 모두 사용할 계정에 Allow(허용) 권한이 있는지 확인합니다. 해당 Microsoft Active Directory 사용자를 4개 옵션(**Access Permissions(**액세스 권한**)** 및 **Launch and Activation Permissions(**실행 및 활성화 권한**)** 모두에 대한 **Edit Limits(**제한 편집**)**와 **Edit Default(**기본값 편집**))**에 모두 추가해야 합니다.

단계 **6** **Access Permissions(**액세스 권한**)** 및 **Launch and Activation Permissions(**실행 및 활성화 권한**)** 둘 다에 대해 로컬 액세스 및 Remote Access를 모두 허용합니다.

그림 ***36:*** 액세스 권한에 대한 로컬 및 ***Remote Access***

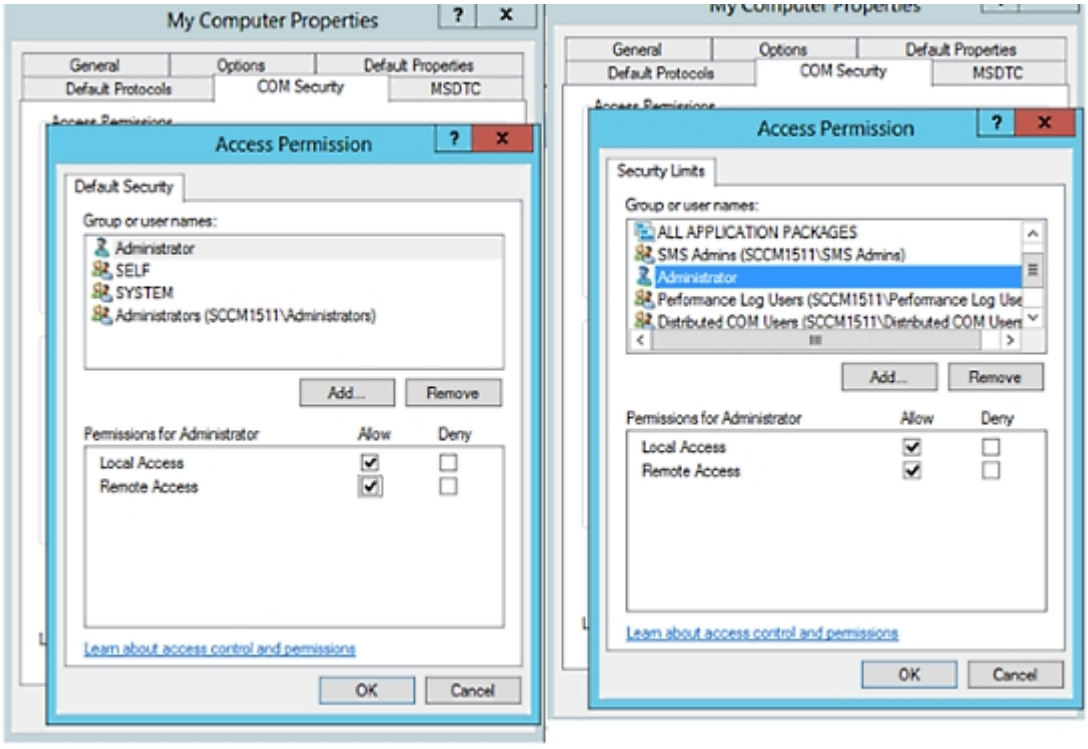
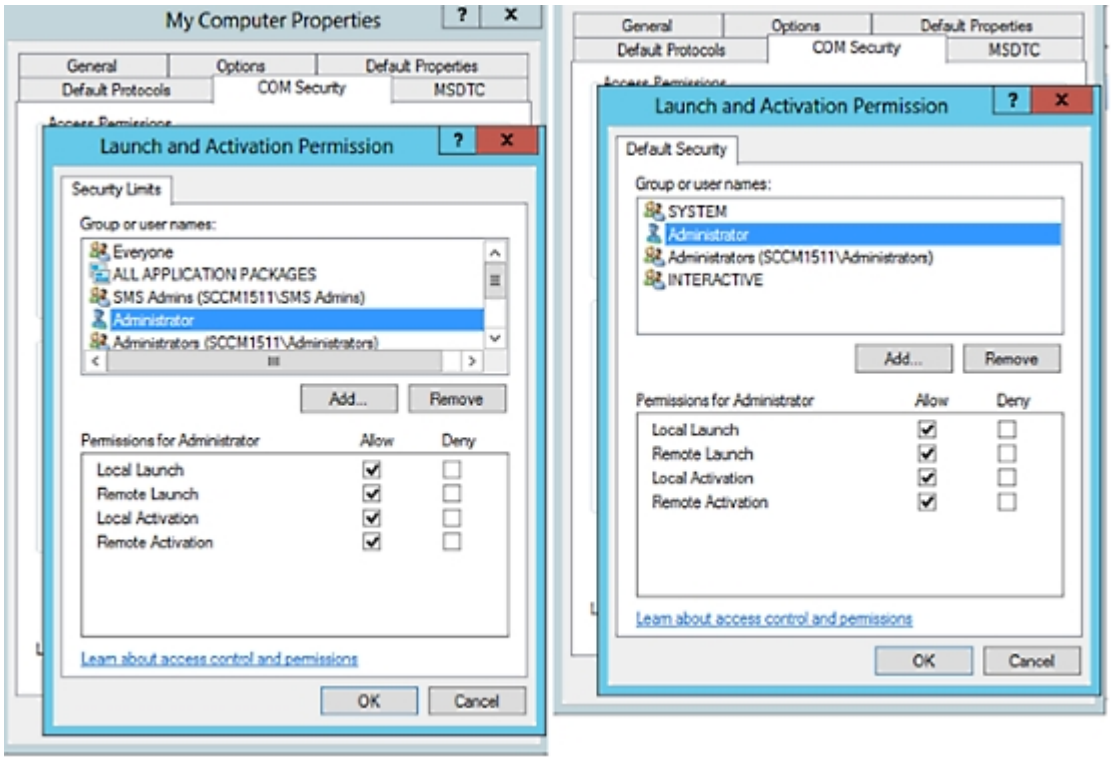


그림 *37:* 실행 및 활성화 권한에 대한 로컬 및 ***Remote Access***



WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정

기본적으로 Microsoft Active Directory 사용자에게는 방법 실행 및 원격 활성화에 대한 권한이 없습니다. wmimgmt.msc MMC 콘솔을 사용하여 액세스 권한을 부여할 수 있습니다.

단계 **1** **Start(**시작**)** > **Run(**실행**)**을 선택하고 `wmimgmt.msc`를 입력합니다.

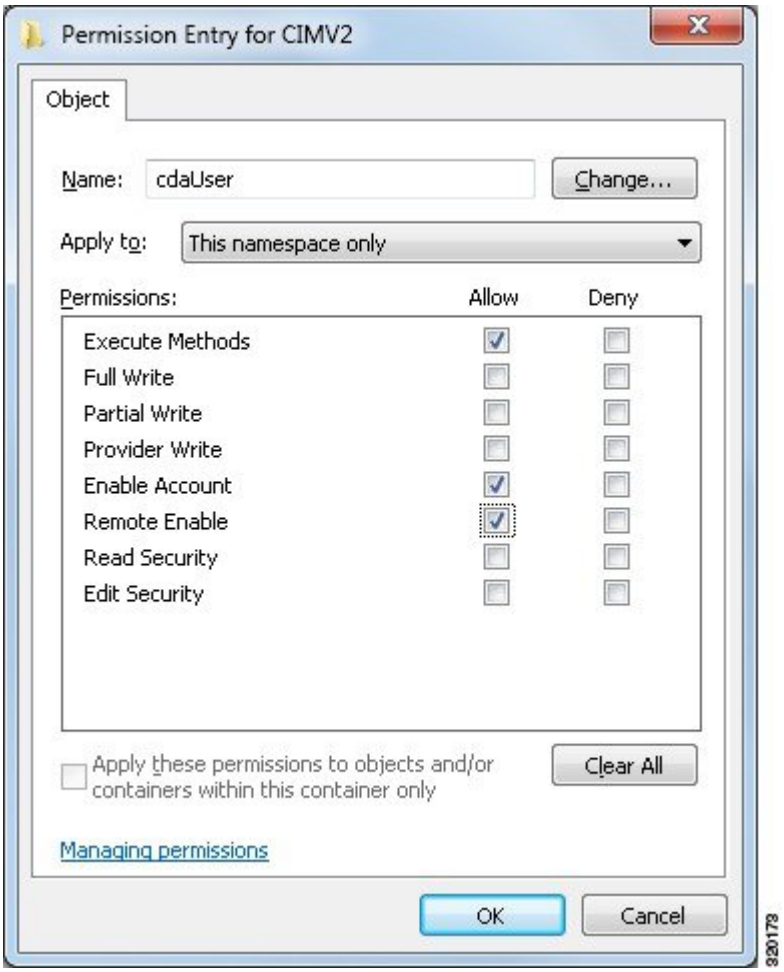
단계 **2** **WMI Control(WMI** 컨트롤**)**을 마우스 오른쪽 버튼으로 클릭하고 **Properties(**속성**)**를 클릭합니다.

단계 **3** **Security(**보안**)** 탭에서 **Root(**루트**)**를 펼치고 **CIMV2**를 선택합니다.

단계 **4** **Security(**보안**)**를 클릭합니다.

단계 **5** Active Directory 사용자를 추가하고 아래 이미지에 나와 있는 대로 필요한 권한을 구성합니다.

그림 ***38: WMI Root\CIMv2*** 이름 공간에 필요한 권한



WMI 액세스를 위한 방화벽 포트 열기

Microsoft Active Directory 도메인 컨트롤러의 방화벽 소프트웨어가 WMI에 대한 액세스를 차단할 수 있습니다. 방화벽을 끄거나, 특정 IP(Cisco ISE IP 주소)에서의 다음 포트에 대한 액세스를 허용할 수 있습니다.

- TCP 135: 일반 RPC 포트입니다. 비동기 RPC 호출을 수행하는 경우, 이 포트에서 수신 대기하는 서비스는 이 요청을 서비스하는 구성 요소에서 사용 중인 포트를 클라이언트에 알립니다.
- UDP 138: NetBIOS 데이터그램 서비스
- TCP 139: NetBIOS 세션 서비스
- TCP 445: SMB

참고 Cisco ISE는 SMB 2.0을 지원합니다.

더 많은 포트가 동적으로 할당됩니다. 또는 수동으로 구성할 수 있습니다. 대상으로 *%SystemRoot%\System32\dllhost.exe*를 추가하는 것을 권장합니다. 이 프로그램은 포트를 동적으로 관리합니다.

모든 방화벽 규칙을 특정 IP(Cisco ISE IP)에 할당할 수 있습니다.

데스크톱 디바이스 관리자 서버에서 엔드포인트 규정 준수에 대한 구성 베이스라인 정책 선택

Cisco ISE에 추가된 데스크톱 디바이스 관리자 서버(예 : Microsoft SCCM 서버)에서 사용 가능한 베이스라인 정책을 확인하고 네트워크 액세스에 대한 엔드포인트 규정 준수를 확인하는 데 사용할 특정 베이스라인 정책을 선택할 수 있습니다. 데스크톱 디바이스 관리자 서버에서 활성화되고 구축된 구성 베이스라인 정책은 Cisco ISE 관리 포털에서 확인할 수 있습니다.

참고 데스크톱 디바이스 관리 서버에서 사용자 권한을 검토하여 베이스라인 정책 및 규정 준수 정보를 Cisco ISE로 전송하는 데 필요한 보안 권한이 있는지 확인하십시오. 관리자는 데스크톱 디바이스 관리자의 **Security(**보안**) > Administrator Users(**관리자**)** 폴더에 추가해야 합니다.

Cisco ISE GUI에서 데스크톱 디바이스 관리자 서버의 베이스라인 정책을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)** > **MDM Servers(MDM** 서버**)**를 선택합니다.

Cisco ISE에 새 데스크톱 디바이스 관리자 서버 추가 및 구성 베이스라인 정책 선택

1. **MDM Servers(MDM** 서버**)** 창에서 **Add(**추가**)**를 클릭합니다.
2. **Server Type(**서버 유형**)** 드롭다운 목록에서 **Desktop Device Manager(**데스크톱 디바이스 관리자**)**를 선택합니다.
3. 다음 필드의 필수 세부 사항을 입력합니다.
   - **Host Name / IP Address(**호스트 이름**/IP** 주소**)**: Microsoft SCCM 서버의 호스트 이름 또는 IP 주소를 입력합니다.
   - **Instance Name(**인스턴스 이름**)**: Microsoft SCCM 서버에 인스턴스가 여러 개 있는 경우 연결하려는 인스턴스를 입력합니다.
   - **Username(**사용자 이름**)**: Microsoft SCCM 서버에 연결하는 데 사용해야 하는 사용자 이름을 입력합니다.
   - **Password(**비밀번호**)**: Microsoft SCCM 서버에 연결하는 데 사용해야 하는 비밀번호를 입력합니다.

- **Time Interval For Compliance Device ReAuth Query(**규정 준수 디바이스 재인증 쿼리 시간 간격**)**: 엔드포인트가 인증되거나 재인증되는 경우 Cisco ISE는 캐시를 사용하여 해당 엔드포인트에 대한 MDM 변수를 가져옵니다. 캐시된 값의 기간이 이 필드에 구성된 값보다 높은 경우 Cisco ISE는 새 디바이스 쿼리를 MDM 서버로 보내 새 값을 가져옵니다. 규정 준수 상태가 변경된 경우 Cisco ISE는 적절한 CoA를 트리거합니다.

  유효 범위는 1분~1440분입니다. 기본값은 1분입니다.

4. **Status(**상태**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

서버가 Cisco ISE에 연결되어 있는지 확인하려면 **Test Connection(**연결 테스트**)** 버튼을 클릭합니다. 이 서버에서 사용 가능한 구성 베이스라인 정책을 보려면 **Save & Continue(**저장 후 계속**)**를 클릭합니다. 베이스라인 정책의 이름 및 ID 목록이 포함된 새 창이 표시됩니다.

기존 데스크톱 디바이스 관리자 서버에서 구성 베이스라인 정책 선택

MDM Servers(MDM 서버**)** 창에서 원하는 서버의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다. 이 서버에서 사용 가능한 베이스라인 정책 목록을 보려면 **Configuration Baselines(**구성 베이스라인**)** 탭을 클릭합니다.

기본적으로 모든 베이스라인 정책이 선택됩니다. **Name(**이름**)** 옆의 확인란을 선택 취소하여 모든 베이스라인 정책을 선택 취소합니다. 해당 이름 옆의 확인란을 선택하여 필요한 베이스라인 정책을 선택합니다. **Save(**저장**)**를 클릭합니다.

엔드포인트 규정 준수는 선택한 구성 베이스라인 정책에 따라 확인됩니다.

데스크톱 디바이스 관리자 서버의 구성 베이스라인 정책에 변경 사항이 있는 경우 **Configuration Baselines(**구성 베이스라인**)** 탭에서 **Update Now(**지금 업데이트**)** 버튼을 클릭하여 Cisco ISE에서 업데이트할 변경 사항을 확인합니다.

Windows 엔드포인트에 대한 디바이스 식별자 구성

데스크톱 디바이스 관리자 서버는 특정 속성을 식별자로 사용하여 네트워크에 연결하는 엔드포인트를 확인합니다. 엔드포인트 MAC 주소가 가장 많이 사용되는 식별자입니다. 그러나 동글, 도킹 스테이션 또는 MAC 주소 임의 지정 기술을 사용하는 경우 MAC 주소가 그다지 신뢰할 수 있는 식별자가 아닙니다.

이제 호스트 이름을 식별자로 사용하도록 선택할 수 있습니다. 호스트 이름은 인증서에서 사용 가능한 CN(Common Name) 또는 SAN-DNS 속성에서 파생됩니다. 엔드포인트의 인증서 기반 인증은 호스트 이름을 사용하여 베이스라인 정책 규정 준수를 확인하는 데 필수입니다.

데스크톱 디바이스 관리자 서버의 디바이스 식별자를 구성하려면 해당 **Server Configuration(**서버 구성**)** 탭으로 이동합니다. 메인 메뉴에서 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)** > **MDM Servers(MDM** 서버**)** > **Edit(**편집**)**를 선택합니다.

Device Identifier Configurations(디바이스 식별자 구성**)** 섹션에서는 다음 식별자가 나열된 순서대로 기본적으로 활성화되어 있습니다.

1. 레거시 **MAC** 주소
2. 인증서 **- CN,** 호스트 이름

3. 인증서 - **SAN-DNS,** 호스트 이름

식별자를 선택 취소하려면 식별자에 대한 확인란을 선택 취소합니다. 속성을 끌어 서버에서 확인에 사용하는 순서를 재배열할 수 있습니다.

디바이스 식별자의 구성 확인

호스트 이름을 확인에 사용하는 경우 Cisco ISE에서 엔드포인트에 GUID가 할당됩니다. **Live Logs(**라이브 로그**)** 창(Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고**Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)** 선택)에서 GUID 항목의 세부정보를 확인합니다.

미등록 디바이스 리디렉션을 위한 권한 부여 프로파일 구성

각 외부 MDM 서버에 대해 미등록 디바이스를 리디렉션하도록 Cisco ISE에서 권한 부여 프로파일을 구성해야 합니다.

시작하기 전에

- Cisco ISE에서 MDM 서버 정의를 생성했는지 확인합니다. Cisco ISE를 MDM 서버와 정상적으로 통합해야 MDM 사전이 채워지며 MDM 사전 속성을 사용하여 권한 부여 정책을 생성할 수 있습니다.
- 미등록 디바이스 리디렉션을 위해 Wireless LAN Controller에서 ACL을 구성합니다.
- 인터넷 연결에 프록시를 사용하며 MDM 서버가 내부 네트워크에 속해 있는 경우에는 프록시-우회 목록에 MDM 서버의 이름이나 해당 IP 주소를 포함해야 합니다. 이 작업을 수행하려면 Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Proxy(**프록시**)**를 선택합니다.

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

단계 **2** 규정을 준수하지 않거나 등록되지 않은 미등록 디바이스 리디렉션을 위한 권한 부여 프로파일을 생성합니다.

단계 **3** MDM 서버 이름과 일치하는 권한 부여 프로파일의 이름을 **Name(**이름**)** 필드에 입력합니다.

단계 **4** **Access Type(**액세스 유형**)** 드롭다운 목록에서 **ACCESS_ACCEPT**를 선택합니다.

단계 **5** **Common Tasks(**일반 작업**)** 섹션에서 **Web Redirection(**웹 리디렉션**)** 확인란을 선택하고 드롭다운 목록에서 **MDM Redirect(MDM** 리디렉션**)**를 선택합니다.

단계 **6** **ACL** 드롭다운 목록에서 무선 LAN 컨트롤러에 구성한 ACL의 이름을 선택합니다.

단계 **7** **Value(**값**)** 드롭다운 목록에서 MDM 포털을 선택합니다.

단계 **8** **MDM Server(MDM** 서버**)** 드롭다운 목록에서 사용할 MDM 서버를 선택합니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

모바일 디바이스 관리 활용 사례용으로 권한 부여 정책 규칙 구성.

모바일 디바이스 관리 활용 사례용으로 권한 부여 정책 규칙 구성

MDM 컨피그레이션을 완료하려면 Cisco ISE에서 권한 부여 정책 규칙을 구성해야 합니다.

시작하기 전에

- Cisco ISE 인증서 저장소에 MDM 서버 인증서를 추가합니다.
- Cisco ISE에서 MDM 서버 정의를 생성했는지 확인합니다. Cisco ISE를 MDM 서버와 정상적으로 통합해야 MDM 사전이 채워지며 MDM 사전 속성을 사용하여 권한 부여 정책을 생성할 수 있습니다.
- 미등록 또는 규정 미준수 디바이스 리디렉션을 위해 Wireless LAN Controller에서 ACL을 구성합니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**을 선택한 다음 정책 집합을 확장하여 권한 부여 정책 규칙을 확인합니다.

단계 **2** 다음 규칙을 추가합니다.

- **MDM_Un_Registered_Non_Compliant**: MDM 서버에 아직 등록되지 않았거나 MDM 정책을 준수하지 않는 디바이스용입니다. 요청이 이 규칙과 일치하면 디바이스를 MDM 서버에 등록하는 방법에 대한 정보가 포함된 Cisco ISE MDM 창이 사용자에게 표시됩니다.

  참고 이 정책에서 **MDM.MDMServerName** 조건을 사용하지 마십시오. 이 조건을 사용하는 경우 엔드포인트가 MDM 서버에 등록된 경우에만 엔드포인트가 정책과 일치합니다.

- **PERMIT**: Cisco ISE와 MDM에 등록되어 있으며 Cisco ISE/MDM 정책을 준수하는 디바이스의 경우 Cisco ISE에 구성된 액세스 제어 정책에 따라 네트워크 액세스 권한이 부여됩니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

모바일 디바이스 관리 상호운용성을 위해 무선 **LAN** 컨트롤러에서 **ACL** 구성

미등록 디바이스 및 인증서 프로비저닝을 리디렉션하려면 권한 부여 정책에 사용할 ACL을 무선 컨트롤러에서 구성해야 합니다. ACL의 순서는 다음과 같이 지정해야 합니다.

단계 **1** 서버에서 클라이언트로의 모든 아웃바운드 트래픽을 허용합니다.

단계 **2** (선택 사항) 문제 해결용으로 클라이언트에서 서버로의 ICMP 클라이언트 인바운드 트래픽을 허용합니다.

단계 **3** 미등록/규정 미준수 디바이스에 대해 MDM 에이전트를 다운로드하고 규정 준수 확인을 진행할 수 있도록 MDM 서버 액세스를 허용합니다.

단계 **4** 웹 포털과 supplicant 및 인증서 프로비저닝 플로우에 대해 클라이언트->서버->Cisco ISE로의 모든 인바운드 트래픽을 허용합니다.

단계 **5** 이름 확인용으로 클라이언트에서 서버로의 인바운드 DNS 트래픽을 허용합니다.

단계 **6** IP 주소용으로 클라이언트에서 서버로의 인바운드 DHCP 트래픽을 허용합니다.

단계 **7** 회사 정책에 따른 Cisco ISE로의 리디렉션용으로 클라이언트->서버->회사 리소스로의 모든 인바운드 트래픽을 거부합니다.

단계 **8** (선택 사항) 나머지 트래픽을 허용합니다.

예

다음 예제에서는 미등록 디바이스를 BYOD 흐름으로 리디렉션하기 위한 ACL을 보여 줍니다. 이 예제에서 Cisco ISE IP 주소는 10.35.50.165, 내부 회사 네트워크 IP 주소는 192.168.0.0 및 172.16.0.0(리디렉션용), MDM 서버 서브넷은 204.8.168.0입니다.

그림 ***39:*** 미등록 디바이스 리디렉션용 ***ACL***

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

디바이스 초기화 또는 잠금

Cisco ISE는 분실한 디바이스를 초기화하거나 해당 디바이스에 대해 PIN 잠금을 켤 수 있습니다. **Endpoints(**엔드포인트**)** 창에서 이를 구성할 수 있습니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**를 선택합니다.

단계 **2** 초기화하거나 잠글 디바이스 옆의 확인란을 선택합니다.

단계 **3** **MDM Actions(MDM** 작업**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Full Wipe(**완전 초기화**)**: MDM 벤더에 따라 이 옵션은 회사 앱을 제거하거나 디바이스를 공장 설정으로 재설정합니다.
- **Corporate Wipe(**회사 초기화**)**: 이 옵션은 MDM 서버 정책에서 구성한 애플리케이션을 제거합니다.
- **PIN Lock(PIN** 잠금**)**: 이 옵션은 디바이스를 잠급니다.

단계 **4** **Yes(**예**)**를 클릭하여 디바이스를 초기화하거나 잠급니다.

Mobile Device Manager 보고서 보기

Cisco ISE는 MDM 서버 정의에 대한 모든 추가, 업데이트 및 삭제 사항을 기록합니다. 이러한 이벤트는 선택한 기간에 걸쳐 시스템 관리자의 모든 컨피그레이션 변경 사항을 제공하는 **Change Configuration Audit(**컨피그레이션 변경 감사**)** 보고서에서 볼 수 있습니다.

Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Audit(**감사**)** > **Change Configuration Audit(**컨피그레이션 변경 감사**)**를 선택합니다. 검토하려는 MDM 서버에 대한 **Object Type(**개체 유형**)** 및 **Object Name(**개체 이름**)** 열의 항목을 확인하고 해당 **Event(**이벤트**)** 값을 클릭하여 컨피그레이션 이벤트의 세부정보를 확인합니다.

Mobile Device 관리 로그 보기

Debug Wizard(디버그 마법사) 창을 사용하여 모바일 디바이스 관리 로그 메시지를 볼 수 있습니다. Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Debug Wizard(**디버그 마법사**)** > **Debug Log Configuration(**디버그 로그 구성**)**을 선택합니다. Cisco ISE 노드 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다. 표시되는 새 창에서 구성 요소 이름 **external-mdm** 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다. 이 구성 요소의 기본 로그 레벨은 **INFO**입니다. 해당 **Log Level(**로그 레벨**)** 드롭 다운 목록에서 **DEBUG** 또는 **TRACE**를 선택하고 **Save(**저장**)**를 클릭합니다.

11 장

세분화

정책 집합

Cisco ISE는 네트워크 액세스 정책 집합을 제공하는 정책 기반의 네트워크 액세스 제어 솔루션으로, 무선, 유선, 게스트 및 클라이언트 프로비저닝과 같은 여러 네트워크 액세스 활용 사례를 관리할 수 있도록 지원합니다. 정책 집합(네트워크 액세스 및 디바이스 관리 집합 모두)을 사용하면 동일한 집합 내의 인증 및 권한 부여 정책을 논리적으로 그룹화할 수 있습니다. 위치, 액세스 유형 및 유사 매개변수를 기반으로 하는 정책 집합처럼 영역에 따라 여러 정책 집합을 가질 수 있습니다. ISE를 설치하면 항상 기본 정책 집합인 정책 집합이 하나만 정의되며, 기본 정책 집합에는 사전 정의 및 기본 인증, 권한 부여 및 예외 정책 규칙이 포함됩니다.

정책 집합을 생성할 때 이러한 규칙(조건 및 결과로 구성됨)을 구성하여 정책 집합 레벨에서 네트워크 액세스 서비스, 인증 정책 레벨에서 ID 소스, 권한 부여 정책 레벨에서 네트워크 권한을 선택할 수 있습니다. 다양한 벤더에 대해 Cisco ISE 지원 사전의 속성을 사용하여 하나 이상의 조건을 정의할 수 있습니다. Cisco ISE를 사용하면 조건을 재사용할 수 있는 개별 정책 요소로 생성할 수 있습니다.

정책 집합별로 네트워크 디바이스와 통신하는 데 사용할 네트워크 액세스 서비스는 해당 정책 집합의 최상위 수준에 정의됩니다. 네트워크 액세스 서비스에는 다음이 포함됩니다.

- 허용된 프로토콜 - 초기 요청 및 프로토콜 협상을 처리하도록 구성된 프로토콜
- 프록시 서비스 - 외부 RADIUS 서버로 요청을 전송하여 처리

참고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)**에서 정책 집합에 대한 관련 TACACS 서버 시퀀스를 선택할 수도 있습니다. TACACS 서버 시퀀스를 사용하여 처리할 TACACS 프록시 서버 시퀀스를 구성합니다.

정책 집합은 계층적으로 구성되며, 정책 집합 표에서 볼 수 있는 정책 집합의 최상위 수준 규칙이 전체 집합에 적용되고 나머지 정책 및 예외에 대한 규칙에 앞서 일치됩니다. 그런 다음 집합의 규칙이 다음 순서로 적용됩니다.

1. 인증 정책 규칙
2. 로컬 정책 예외
3. 전역 정책 예외
4. 권한 부여 정책 규칙

참고 정책 집합 기능은 네트워크 액세스 및 디바이스 관리 정책에서 동일합니다. 이 장에서 설명하는 모든 프로세스는 Network Access(네트워크 액세스) 및 Device Administration(디바이스 관리) 작업 센터에서 작업할 때 적용할 수 있습니다. 이 장에서는 Network Access(네트워크 액세스) 작업 센터 정책 집합에 대해 구체적으로 안내합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Policy Sets(**정책 집합**)**를 선택합니다.

ISE Community Resource(ISE 커뮤니티 리소스)

WLC에서 RADIUS 결과를 사용하는 방법에 대한 자세한 내용은 WLC Called-Station-ID(RADIUS 인증 및 계정 관리 컨피그레이션)를 참조하십시오.

정책 집합 컨피그레이션 설정

다음 표에서는 인증, 예외 및 권한 부여 정책을 포함하여 정책 집합을 구성할 수 있는 **Policy Sets(**정책 집합**)** 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 네트워크 액세스 정책의 경우 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Policy Sets(**정책 집합**)**. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리 정책 집합**)**를 선택합니다.

표 ***125:*** 정책 집합 컨피그레이션 설정

필드 이름	사용 지침
Status(상태**)**	이 정책의 상태를 선택합니다. 다음 중 하나일 수 있습니다. • **Enabled(**활성화됨**)**: 이 정책 조건이 활성 상태입니다. • **Disabled(**비활성화됨**)**: 이 정책 조건이 비활성 상태이며 평가되지 않습니다. • **Monitor Only(**모니터링만**)**: 이 정책 조건이 평가되지 않습니다.
Policy Set Name(정책 집합 이름**)**	이 정책 집합에 대한 고유한 이름을 입력합니다.
Conditions(조건**)**	새 정책 행에서 더하기(+) 아이콘을 클릭하거나, 기존의 정책 행에서 편집 아이콘을 클릭해 Conditions Studio를 엽니다.
Description(설명**)**	정책에 대한 고유한 설명을 입력합니다.
허용되는 프로토콜 또는 서버 시퀀스	이미 생성한 허용되는 프로토콜을 선택하거나, (+) 기호를 클릭하여 **Create a New Allowed Protocol(**새 허용되는 프로토콜 생성**)**, **Create a New Radius Sequence(**새 **Radius** 시퀀스 생성**)** 또는 **Create a TACACS Sequence(TACACS** 시퀀스 생성**)**을 수행합니다.
Conditions(조건**)**	새 예외 행에서 더하기(+) 아이콘을 클릭하거나, 기존의 예외 행에서 편집 아이콘을 클릭하여 Conditions Studio를 엽니다.

필드 이름	사용 지침
Hits(히트**)**	Hits(히트)는 조건이 충족된 횟수를 나타내는 진단 도구입니다. 이 정보가 마지막으로 업데이트되었을 때 이 아이콘 위에 마우스를 올리면 0으로 재설정되며 업데이트 빈도를 확인할 수 있습니다.
Actions(작업**)**	작업 열에서 톱니바퀴 아이콘( )을 클릭해 다양한 작업을 보고 선택할 수 있습니다. • Insert new row above(위에 새 행 삽입): Actions(작업) 메뉴가 열린 정책의 위에 새 정책을 삽입합니다. • Insert new row below(아래에 새 행 삽입): Actions (작업) 메뉴가 열린 정책의 아래에 새 정책을 삽입합니다. • Duplicate above(위에 복제): Actions(작업) 메뉴가 열린 정책의 위에 중복 정책을 삽입합니다(원본 집합 위). • Duplicate below(아래 복제) : Actions(작업) 메뉴가 열린 정책의 아래에 중복 정책을 삽입합니다(원본 집합 아래). • Delete(삭제): 정책 집합을 삭제합니다.
View(보기**)**	화살표 아이콘을 클릭하여 특정 정책 집합의 Set(집합) 보기를 열고 그 인증, 예외 및 권한 부여 하위 정책을 봅니다.

인증 정책

각 정책 집합에는 해당 집합에 대한 인증 정책을 함께 나타내는 여러 인증 규칙이 포함될 수 있습니다. 인증 정책의 우선순위는 정책 집합 자체(정책 집합 보기 페이지의 인증 정책 영역) 내에 표시되는 정책의 순서에 따라 결정됩니다.

Cisco ISE는 정책 집합 레벨에서 구성된 설정에 따라 네트워크 액세스 서비스(허용되는 프로토콜 또는 서버 시퀀스)를 동적으로 선택하고, 그 후에 인증 및 권한 부여 정책 레벨에서 ID 소스 및 결과를 확인합니다. Cisco ISE 사전의 속성을 사용하여 조건을 하나 이상 정의할 수 있습니다. Cisco ISE에서는 라이브러리에 저장하여 다른 규칙 기반 정책에서 재사용 가능한 개별 정책 요소로 조건을 생성할 수 있습니다.

인증 정책에 따라 결정되는 ID 방법은 다음 중 하나일 수 있습니다.

- 액세스 거부 - 사용자에 대한 액세스가 거부되며 인증이 수행되지 않습니다.

- ID 데이터베이스 - 다음 중 하나일 수 있는 단일 ID 데이터베이스입니다.
  - 내부 사용자
  - 게스트 사용자
  - 내부 엔드포인트
  - Active Directory
  - LDAP(Lightweight Directory Access Protocol) 데이터베이스
  - RADIUS 토큰 서버(RSA 또는 SafeWord 서버)
  - 인증서 인증 프로파일
- ID 소스 시퀀스 - 인증에 사용되는 ID 데이터베이스 시퀀스입니다.

초기 Cisco ISE 설치 시 구현되는 기본 정책 집합에는 기본 ISE 인증 및 권한 부여 규칙이 포함됩니다. 기본 정책 집합에는 인증 및 권한 부여에 대해서 구축 당시 기본으로 내장된 유연한 규칙(기본값 아님)도 추가로 포함됩니다. 이러한 정책에 규칙을 추가할 수 있으며, 구축 당시 기본으로 내장된 규칙은 삭제 및 변경할 수 있습니다. 단, 기본 규칙과 기본 정책 집합은 삭제할 수 없습니다.

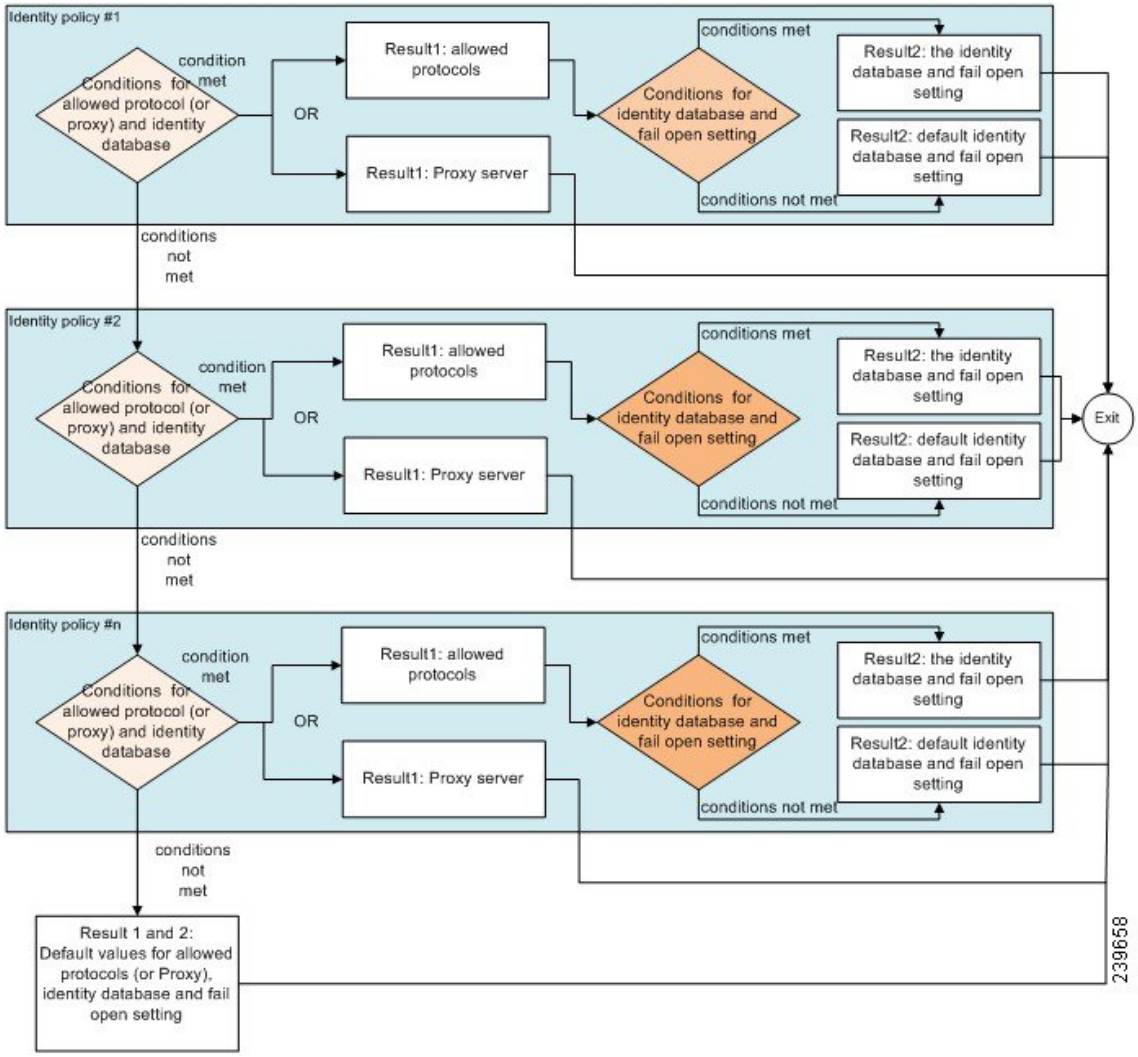
인증 정책 플로우

인증 정책에서 조건과 결과로 구성된 여러 규칙을 정의할 수 있습니다. ISE에서는 지정된 조건을 평가하고 평가 결과에 따라 해당 결과를 할당합니다. 기준과 일치하는 첫 번째 규칙에 따라 ID 데이터베이스가 선택됩니다.

여러 데이터베이스로 구성되는 ID 소스 시퀀스도 정의할 수 있습니다. Cisco ISE에서 이러한 데이터베이스를 조회하는 데 사용할 순서를 정의할 수 있습니다. Cisco ISE는 인증이 성공할 때까지 이러한 데이터베이스에 순서대로 액세스합니다. 외부 데이터베이스에 동일한 사용자의 인스턴스가 여러 개 있는 경우 인증이 실패합니다. 각 ID 소스에는 하나의 사용자 기록만 포함될 수 있습니다.

ID 소스 시퀀스마다 3개 또는 최대 4개의 데이터베이스만 사용하는 것이 좋습니다.

그림 *40:* 인증 정책 플로우



인증 실패 - 정책 결과 옵션

ID 방법을 액세스 거부로 선택하면 요청에 대한 응답으로 거부 메시지가 전송됩니다. ID 데이터베이스 또는 ID 소스 시퀀스를 선택하는 경우 인증이 성공하면 동일한 정책 집합에 구성된 권한 부여 정책으로 처리가 계속 진행됩니다. 실패하는 일부 인증은 다음과 같이 분류됩니다.

- 인증 실패 - 잘못된 자격 증명, 비활성화된 사용자 등 인증이 실패했다는 명시적 응답이 수신되었습니다. 이 경우 기본적으로 수행되는 작업은 인증 거부입니다.
- 사용자를 찾을 수 없음 - ID 데이터베이스에서 해당 사용자를 찾지 못했습니다. 이 경우 기본적으로 수행되는 작업은 인증 거부입니다.
- 프로세스 실패 - ID 데이터베이스 하나 이상에 액세스할 수 없습니다. 이 경우 기본적으로 수행되는 작업은 삭제입니다.

Cisco ISE에서는 인증 실패에 대해 다음과 같은 작업 중 하나를 구성할 수 있습니다.

- Reject(거부) - 거부 응답이 전송됩니다.
- Drop(삭제) - 응답이 전송되지 않습니다.
- Continue(계속) - Cisco ISE가 권한 부여 정책을 계속합니다.

Continue(계속) 옵션을 선택하더라도 사용 중인 프로토콜에 대한 제한으로 인해 Cisco ISE가 요청을 계속 처리할 수 없는 경우가 있을 수 있습니다. PEAP, LEAP, EAP-FAST, EAP-TLS 또는 RADIUS MSCHAP를 사용하는 인증의 경우 인증이 실패하거나 사용자를 찾을 수 없으면 요청을 계속 처리할 수 없습니다.

인증이 실패하면 PAP/ASCII 및 MAC Authentication Bypass(MAB 또는 호스트 조회)를 위한 권한 부여 정책을 계속 처리할 수 있습니다. 기타 모든 인증 프로토콜의 경우 인증이 실패하면 다음 작업이 수행됩니다.

- 인증 실패 - 거부 응답이 전송됩니다.
- 사용자 또는 호스트를 찾을 수 없음 - 거부 응답이 전송됩니다.
- 프로세스 실패 - 응답이 전송되지 않으며 요청이 삭제됩니다.

인증 정책 구성

필요에 따라 여러 인증 규칙을 구성하고 유지 관리하여 정책 집합별로 인증 정책을 정의합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

지원되는 시스템 기본값을 사용하지 않기로 선택한다면 필요한 경우 외부 ID 저장소를 구성했는지 확인합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 자산 가시성의 내부 및 외부 ID 소스 섹션을 참조하십시오. 을 참조하십시오.

단계 **1** 네트워크 액세스 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Policy Sets(**정책 집합**)**를 선택합니다. 디바이스 관리 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리자 정책 집합**)**를 선택합니다.

단계 **2** 인증 정책을 추가하거나 업데이트하려는 정책 집합의 행에서 Policy Sets(정책 집합) 표의 View(보기) 열에 있는 › 아이콘을 클릭하여 모든 정책 집합 세부정보에 액세스하고 인증 및 권한 부여 정책뿐만 아니라 정책 예외도 생성합니다.

단계 **3** 페이지의 Authentication Policy(인증 정책) 부분 옆에 있는 화살표 아이콘을 클릭하면 표의 모든 인증 정책 규칙을 확장해서 볼 수 있습니다.

단계 **4** 아무 행의 **Actions(**작업**)** 열에서 톱니바퀴 아이콘을 클릭합니다. 드롭다운 메뉴에서 필요에 따라 Insert(삽입) 또는 Duplicate(중복) 옵션을 선택하여 새 인증 정책 규칙을 삽입합니다.
Authentication Policy(인증 정책) 표에 새 행이 나타납니다.

단계 **5** **Status(**상태**)** 열에서 현재 상태 아이콘을 클릭하고 드롭다운 목록에서 필요에 따라 정책 집합의 상태를 업데이트합니다. 상태에 대한 자세한 내용은 인증 정책 컨피그레이션 설정, 906 페이지를 참조하십시오.

단계 **6** 표의 규칙에 대해 **Rule Name(**규칙 이름**)** 또는 **Description(**설명**)** 셀을 클릭하여 자유 텍스트를 필요에 따라 변경합니다.

단계 **7** 조건을 추가하거나 변경하려면 **Conditions(**조건**)** 열의 셀 위에 마우스를 가져가 아이콘을 클릭합니다. Condition Studio가 열립니다. 자세한 내용은 정책 조건, 926 페이지를 참고하십시오.

선택하는 모든 속성에 "Equals(같음)", "Not Equals(같지 않음)", "In(존재)", "Not In(존재하지 않음)", "Matches(일치함)", "Starts With(다음으로 시작)" 또는 "Not Starts With(다음으로 시작 안 함)" 연산자 옵션이 포함되지는 않습니다.

"Matches(일치함)" 연산자는 와일드카드가 아닌 정규식(REGEX)을 지원하며 사용합니다.

참고 직접 비교하려면 "같음" 연산자를 사용해야 합니다. 다중 값 속성에 "Contains(포함)" 연산자를 사용할 수 있습니다. 정규식 비교에는 "일치함" 연산자를 사용해야 합니다. "일치함" 연산자를 사용하면 정적 값과 동적 값 모두에 대해 정규식이 해석됩니다. 목록의 경우 "In(존재)" 연산자는 목록에 특정 값이 있는지 확인합니다. 단일 문자열의 경우 "In(존재)" 연산자는 문자열이 "Equals(같음)" 연산자와 동일한지를 확인합니다.

단계 **8** 확인하고 일치시킬 순서에 따라 표 내에서 정책을 정리합니다. 규칙의 순서를 변경하려면 행을 올바른 위치로 끌어다 놓습니다.

단계 **9** **Save(**저장**)**를 클릭하여 변경사항을 저장하고 구현합니다.

다음에 수행할 작업

1. 권한 부여 정책 구성

인증 정책 컨피그레이션 설정

다음 표에서는 정책 집합 창의 인증 정책 섹션에 있는 필드에 대해 설명합니다. 여기서 정책 집합의 일부를 인증 정책 하위 집합으로 구성할 수 있습니다.Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Policy Sets(**정책 집합**)**를 선택합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리 정책 집합**)**를 선택합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy Sets(**정책 집합**)** > **View(**보기**)** > **Authentication Policy(**인증 정책**)**를 선택합니다.

표 ***126:*** 인증 정책 컨피그레이션 설정

필드 이름	사용 지침
Status(상태**)**	이 정책의 상태를 선택합니다. 다음 중 하나일 수 있습니다. • **Enabled(**활성화됨**)**: 이 정책 조건이 활성 상태입니다. • **Disabled(**비활성화됨**)**: 이 정책 조건이 비활성 상태이며 평가되지 않습니다. • **Monitor Only(**모니터링만**)**: 이 정책 조건이 평가되지만 결과가 적용되지 않습니다. 라이브 로그 인증 페이지에서 이 정책 조건의 결과를 확인할 수 있습니다. 이 페이지에서는 모니터링되는 단계 및 속성이 포함된 상세 보고서를 확인할 수 있습니다. 새 정책 조건을 추가하려고 하는데 해당 조건이 올바른 결과를 제공할지 여부가 확실치 않은 경우를 예로 들어 보겠습니다. 이러한 상황에서는 모니터링되는 모드에서 정책 조건을 생성하여 결과를 확인한 다음 원하는 결과가 표시되면 조건을 활성화할 수 있습니다.
Rule Name(규칙 이름**)**	이 인증 정책의 이름을 입력합니다.
Conditions(조건**)**	새 정책 행에서 더하기(+) 아이콘을 클릭하거나, 기존의 정책 행에서 편집 아이콘을 클릭해 **Conditions Studio**를 엽니다.
Use(사용**)**	인증에 사용할 ID 소스를 선택합니다. ID 소스 시퀀스를 구성한 경우 해당 시퀀스를 선택할 수도 있습니다. 이 규칙에 정의된 ID 소스 중 요청과 일치하는 소스가 없는 경우 Cisco ISE가 사용하도록 할 기본 ID 소스를 편집할 수 있습니다.
Options(옵션**)**	인증 실패, 사용자를 찾을 수 없음 또는 프로세스 실패 이벤트에 대한 추가 작업 과정을 정의합니다. 다음 옵션 중 하나를 선택할 수 있습니다. • **Reject(**거부**)**: 거부 응답이 전송됩니다. • **Drop(**삭제**)** : 응답이 전송되지 않습니다. • **Continue(**계속**)** - Cisco ISE가 권한 부여 정책을 계속 진행합니다.

필드 이름	사용 지침
Hits(히트**)**	Hits(히트)는 조건이 충족된 횟수를 나타내는 진단 도구입니다.
Actions(작업**)**	작업 열에서 톱니바퀴 아이콘( )을 클릭해 다양한 작업을 보고 선택할 수 있습니다. • 위에 새 행 삽입: Actions(작업) 메뉴를 연 정책 위에 새 인증 정책을 삽입합니다. • 아래에 새 행 삽입: Actions(작업) 메뉴를 연 정책 아래에 새 인증 정책을 삽입합니다. • 위에서 복제: Actions(작업) 메뉴를 연 정책 위에서 원래 집합 위로 중복 인증 정책을 삽입합니다. • 아래 복제: Actions(작업) 메뉴를 연 정책 아래에서 원본 집합 밑으로 중복 인증 정책을 삽입합니다. • Delete(삭제): 정책 집합을 삭제합니다.

비밀번호 기반 인증

인증에서는 사용자 ID 확인을 위해 사용자 정보를 검사합니다. 기존 인증에서는 이름과 고정 비밀번호를 사용합니다. 이는 가장 대중적이고 간단하며 비용이 적게 드는 인증 방법입니다. 단점은 이 정보가 다른 사람에게 노출되거나 다른 사람에 의해 추측 또는 포착 가능하다는 것입니다. 암호화되지 않은 간단한 사용자 이름 및 비밀번호를 사용하는 방법은 강력한 인증 메커니즘으로 간주되지 않지만 인터넷 액세스와 같이 권한 부여 또는 권한 수준이 낮은 데 사용하기에는 충분할 수 있습니다.

암호화된 비밀번호 및 암호화 기술을 사용하는 보안 인증

네트워크에서 비밀번호 캡처 위험을 줄이려면 암호화를 사용해야 합니다. RADIUS와 같은 클라이언트 및 서버 액세스 제어 프로토콜은 네트워크 내에서 캡처되지 않도록 비밀번호를 암호화합니다. 그러나 RADIUS는 AAA(Authentication, Authorization, and Accounting) 클라이언트와 Cisco ISE 간에만 작동합니다. 그러므로 다음 예제와 같이 인증 프로세스의 이 포인트에 도달하기 전까지는 권한이 없는 사람이 일반 텍스트 비밀번호를 알아낼 수 있습니다.

- 전화선을 통해 전화를 거는 최종 사용자 클라이언트 간의 통신
- 네트워크 액세스 서버에서 종료되는 ISDN 회선
- 최종 사용자 클라이언트와 호스팅 디바이스 간의 텔넷(Telnet) 세션

보다 안전한 인증 방법에서는 CHAP(Challenge Handshake Authentication Protocol), OTP(One-Time Password) 및 고급 EAP 기반 프로토콜 내에서 사용되는 것과 같은 암호화 기술을 사용합니다. Cisco ISE는 이와 같은 다양한 인증 방법을 지원합니다.

인증 방법 및 권한 부여 권한

인증과 권한 부여 사이에는 기본적인 암시적 관계가 존재합니다. 사용자에게 부여된 권한이 많을수록 인증은 더 강력해야 합니다. Cisco ISE는 다양한 인증 방법을 제공하여 이러한 관계를 지원합니다.

인증 **Dashlet**

Cisco ISE 대시보드는 네트워크와 디바이스에서 발생하는 모든 요약 정보를 제공합니다. 인증 dashlet에서 인증 및 인증 실패에 대한 정보를 한 눈에 볼 수 있습니다.

RADIUS 인증 dashlet에서는 Cisco ISE가 처리한 인증에 대한 다음 통계 정보를 제공합니다.

- 통과한 인증, 실패한 인증 및 같은 사용자에 의한 동시 로그인 수를 포함하여 Cisco ISE가 처리한 총 RADIUS 인증 요청 수
- Cisco ISE가 처리한 실패한 총 RADIUS 인증 요청 수

TACACS+ 인증의 요약을 볼 수도 있습니다. TACACS+ 인증 dashlet에서는 디바이스 인증에 대한 통계 정보를 제공합니다.

디바이스 관리 인증에 대한 자세한 내용은 *Cisco ISE* 관리 가이드*:* 문제 해결의 TACACS 라이브 로그 섹션을 참고하십시오. 참고 RADIUS 라이브 로그 설정에 대한 자세한 내용은 *Cisco ISE* 관리 가이드*:* 문제 해결의 RADIUS 라이브 로그 섹션을 참고하십시오. 참고

ISE Community Resource(ISE 커뮤니티 리소스)

실패한 인증 및 권한 부여 문제를 해결하는 방법에 대한 자세한 내용은 How To: Troubleshoot ISE Failed Authentications & Authorizations를 참고하십시오.

인증 결과 보기

Cisco ISE에서는 실시간 인증 요약(Authentication Summary)을 확인할 수 있는 여러 가지 방법을 제공합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 네트워크 인증(RADIUS)의 경우**Operations(**작업**)** > **RADIUS** > **Live Logs(**라이브 로그**)**. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 실시간 인증 요약을 보려면 **Operations(**작업**)** > **TACACS** > **Live Logs(**라이브 로그**)**.

단계 **2** 다음과 같은 방법으로 인증 요약(Authentication Summary)을 확인할 수 있습니다.

- 마우스 커서로 상태 아이콘을 가리키면 인증의 결과와 간단한 요약을 볼 수 있습니다. 상태 세부정보가 포함된 팝업이 나타납니다.
- 목록 위쪽에 표시되는 하나 이상의 텍스트 상자에 검색 기준을 입력하고 **Enter** 키를 눌러 결과를 필터링합니다.

- 세부 보고서를 보려면 세부정보 열에서 돋보기 아이콘을 클릭합니다.

참고 인증 요약**(Authentication Summary)** 보고서 또는 대시보드에는 실패했거나 성공한 인증에 해당하는 최신 데이터가 수집되어 표시되므로, 보고서 내용이 표시될 때까지는 몇 분 정도 걸립니다.

인증 보고서 및 문제 해결 도구

인증 세부정보와 별도로 Cisco ISE는 네트워크를 효율적으로 관리하는 데 사용할 수 있는 다양한 보고서 및 문제 해결 도구를 제공합니다.

네트워크의 인증 트렌드 및 트래픽을 이해하기 위해 실행할 수 있는 보고서는 여러 가지가 있습니다. 기록 데이터와 현재 데이터 둘 다에 대해 보고서를 생성할 수 있습니다. 다음은 인증 보고서 목록입니다.

- AAA 진단
- RADIUS 계정 관리
- RADIUS 인증
- 인증 요약(Authentication Summary)

참고 Cisco Catalyst 4000 시리즈 스위치에서 IPv6 스누핑(Snooping)을 활성화해야 합니다. 그러지 않으면 IPv6 주소가 인증 세션에 매핑되지 않으며 show 출력에 표시되지 않습니다. IPv6 스누핑을 활성화하려면 다음 명령을 사용합니다.

```
vlan config <vlan-number>
 ipv6 snooping
 end
ipv6 nd raguard policy router
 device-role router
interface <access-interface>
  ipv6 nd raguard
interface <uplink-interface>
  ipv6 nd raguard attach-policy router
  end
```

권한 부여 정책

권한 부여 정책은 Cisco ISE 네트워크 권한 부여 서비스의 구성 요소입니다. 이 서비스를 사용하면 네트워크 리소스에 액세스하는 특정 사용자 및 그룹에 대한 권한 부여 정책을 정의하고 권한 부여 프로파일을 구성할 수 있습니다.

권한 부여 정책은 하나 이상의 권한 부여 프로파일을 반환할 수 있는 권한 부여 확인을 포함하는 복합 조건을 사용하여 하나 이상의 ID 그룹을 결합하는 조건부 요건을 포함할 수 있습니다. 또한 특정 ID 그룹을 사용하는 것과는 별도로 조건부 요건이 존재할 수 있습니다.

Cisco ISE에서 권한 부여 프로파일을 생성하는 경우 권한 부여 정책이 사용됩니다. 권한 부여 정책은 권한 부여 규칙으로 구성됩니다. 권한 부여 규칙에는 3가지 요소, 이름, 속성 및 권한이 있습니다. 권한 요소는 권한 부여 프로파일에 매핑됩니다.

Cisco ISE 권한 부여 프로파일

권한 부여 정책은 규칙을 특정 사용자 및 그룹 ID에 연결하여 해당 프로파일을 생성합니다. 이러한 규칙이 구성한 속성과 일치할 때마다 항상 권한을 부여하는 해당 권한 부여 프로파일이 정책에 의해 반환되며 그에 따라 네트워크 액세스 권한이 부여됩니다.

예를 들어 권한 부여 프로파일은 다음 유형으로 분류되는 일련의 권한을 포함할 수 있습니다.

- 표준 프로파일
- 예외 프로파일
- 디바이스 기반 프로파일

프로파일은 사용 가능한 벤더 사전에 저장되어 있는 리소스 집합에서 선택된 속성으로 구성되며, 특정 권한 부여 정책에 대한 조건이 일치할 때 반환됩니다. 권한 부여 정책에는 단일 네트워크 서비스 규칙에 대한 조건 매핑이 속할 수 있으므로, 여기에는 권한 목록 부여 확인도 포함될 수 있습니다.

권한 부여 확인은 반환될 권한 부여 프로파일을 따라야 합니다. 권한 부여 확인은 맞춤화 이름을 비롯한 하나 이상의 조건으로 구성됩니다. 이러한 조건은 라이브러리에 추가되어 다른 정책에 의해 재사용될 수 있습니다.

권한 부여 프로파일에 대한 권한

권한 부여 프로파일에 대한 권한 구성을 시작하기 전에 필요한 사항은 다음과 같습니다.

- 권한 부여 정책과 프로파일 간의 관계 이해
- 권한 부여 프로파일 페이지에 대해 숙지
- 정책 및 프로파일을 구성할 때 따라야 할 기본 지침 파악
- 권한 부여 프로파일에서 권한을 구성하는 요소 이해

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 권한 부여 프로파일을 사용하려면 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)**를 선택합니다. 왼쪽 메뉴에서 **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다.

네트워크의 여러 권한 부여 프로파일 유형에 대한 정책 요소 권한을 표시, 생성, 수정, 삭제, 복제 또는 검색하는 프로세스의 시작점으로 결과 탐색 창을 사용할 수 있습니다. 처음에 결과 창에는 Authentication(인증), Authorization(권한 부여), Profiling(프로파일링), Posture(포스처), Client Provisioning(클라이언트 프로비저닝) 및 Trustsec 옵션이 표시됩니다.

권한 부여 프로파일에서는 RADIUS 요청이 수락되는 경우에 반환할 속성을 선택할 수 있습니다. Cisco ISE는 일반적으로 사용되는 속성을 지원하도록 일반 작업 설정을 구성할 수 있는 메커니즘을 제공합니다. 일반 작업 속성 값을 입력해야 하며, 이는 Cisco ISE에서 기본 RADIUS 값으로 해석됩니다.

ISE 커뮤니티 리소스

802.1x 신청자(Cisco AnyConnect Mobile Security)와 인증자(스위치) 간에 MACsec(Media Access Control Security) 암호화를 구성하는 방법의 예는 Cisco AnyConnect를 사용한 MACsec 스위치-호스트 암호화 및 ISE 컨피그레이션 예를 참조하십시오.

위치 기반 권한 부여

Cisco ISE를 Cisco MSE(Mobility Services Engine)와 통합하면 물리적 위치 기반 권한 부여 기능을 도입할 수 있습니다. Cisco ISE는 MSE의 정보를 사용하여 MSE에서 보고된 대로 사용자의 실제 위치를 기반으로 각기 다른 네트워크 액세스 권한을 제공합니다.

이 기능을 통해, 사용자가 적절한 영역에 있으면 엔드포인트 위치 정보를 사용하여 네트워크 액세스 권한을 제공할 수 있습니다. 또한 엔드포인트 위치를 정책의 추가 속성으로 추가하여 디바이스 위치를 기준으로 보다 자세한 정책 권한 부여 집합을 정의할 수도 있습니다. 다음과 같은 위치 기반 속성을 사용하는 권한 부여 규칙 내에서 조건을 구성할 수 있습니다.

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

Cisco Prime Infrastructure 애플리케이션을 사용하면 위치 계층 구조(캠퍼스/건물/층 구조)를 정의하고 보안 및 비보안 영역을 구성할 수 있습니다. 위치 계층 구조를 정의한 후에는 위치 계층 구조 데이터를 MSE 서버와 동기화해야 합니다. Cisco Prime Infrastructure에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html를 참고하십시오.

MSE 인스턴스를 하나 또는 여러 개 추가하여 MSE 기반 위치 데이터를 권한 부여 프로세스에 통합할 수 있습니다. 이러한 MSE에서 위치 계층 구조 데이터를 검색하고 이 데이터를 사용하여 위치 기반 권한 부여 규칙을 구성할 수 있습니다.

엔드포인트 이동을 추적하려면 권한 부여 프로파일을 생성할 때 Track Movement(이동 추적) 확인란을 선택합니다. Cisco ISE는 5분마다 관련 MSE에서 엔드포인트 위치를 쿼리하여 위치가 변경되었는지를 확인합니다.

참고

- MSE 디바이스를 Cisco ISE에 추가할 때는 MSE 디바이스의 인증서를 ISE로 복사하여 권한 부여를 용이하게 합니다.
- 여러 사용자를 추적하면 빈번한 업데이트로 인해 성능에 영향을 줍니다. Track Movement(이동 추적) 옵션은 보안 수준이 높은 위치에 사용할 수 있습니다.
- MSE 인스턴스에서 검색된 위치 데이터를 사용하여 위치 트리를 생성합니다. 위치 트리를 사용하여 권한 부여 정책에 표시되는 위치 항목을 선택할 수 있습니다.
- Location Services(위치 서비스)를 사용하려면 Cisco ISE Advantage 라이선스가 필요합니다.

MSE 서버 추가

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Network Resources(**네트워크 리소스**) > Location Services(**위치 서비스**) > Location Servers(**위치 서버**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 서버 이름, 호스트 이름/IP 주소, 비밀번호 등의 MSE 서버 세부정보를 입력합니다.

단계 **4** 입력한 서버 세부정보를 사용하여 MSE 연결을 테스트하려면 **Test(**테스트**)**를 클릭합니다.

단계 **5** (선택 사항) **Find Location(**위치 찾기**)** 필드에 엔드포인트의 MAC 주소를 입력하고 **Find(**찾기**)**를 클릭하여 엔드포인트가 현재 이 MSE에 연결되어 있는지 확인합니다.

엔드포인트가 발견되는 경우 캠퍼스:건물:층:영역 형식으로 표시됩니다. 위치 계층 및 영역 설정에 따라 둘 이상의 엔트리가 표시되는 경우도 있습니다. 예를 들어 이름이 *Campus1*인 캠퍼스 내 건물(*building1*)의 모든 층이 비보안 영역으로 정의되어 있고 1층의 실험실 영역이 보안 영역으로 정의되어 있는 경우 실험실 영역에 엔드포인트가 있으면 다음 엔트리가 표시됩니다.

찾은 위치:

Campus1#building1#floor1#LabArea

Campus1#building1#floor1#NonSecureZone

단계 **6** **Submit(**제출**)**을 클릭합니다.

새 MSE를 추가한 후 Location Tree(위치 트리) 페이지로 이동한 다음 **Get Update(**업데이트 가져오기**)**를 클릭하여 해당 위치 계층을 검색해 위치 트리에 추가합니다. 이 트리에 필터가 정의되어 있는 경우 새 MSE 엔트리에도 이러한 필터가 적용됩니다.

위치 트리

MSE 인스턴스에서 검색된 위치 데이터를 사용하여 위치 트리를 생성합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Network Resources(**네트워크 리소스**) > Location Services(**위치 서비스**) > Location Tree(**위치 트리**)**를 선택합니다.

건물 하나에 MSE가 여러 개 있는 경우 Cisco ISE는 모든 MSE의 위치 세부정보를 수집하여 단일 트리로 표시합니다.

Location Tree(위치 트리)를 사용하여 권한 부여 정책에 표시되는 위치 항목을 선택할 수 있습니다. 또한 요건을 기반으로 특정 위치를 숨길 수 있습니다. 위치를 숨기기 전에 위치 트리를 업데이트하는 것이 좋습니다. 숨겨진 위치는 트리를 업데이트해도 숨겨진 상태로 유지됩니다.

권한 부여 규칙과 관련된 위치 항목을 수정하거나 제거한 경우 영향을 받는 규칙을 비활성화하고 이러한 위치를 Unknown(알 수 없음)으로 설정하거나 영향을 받는 각 규칙에 대해 대체 위치를 선택해야 합니다. 변경 사항을 적용하거나 업데이트를 취소하기 전에 새 트리 구조를 확인해야 합니다.

모든 MSE에서 최신 위치 계층 구조를 가져오려면 **Get Update(**업데이트 가져오기**)**를 클릭합니다. 새 트리 구조를 확인한 후 변경 사항을 적용하려면 Save(저장)를 클릭합니다.

다운로드 가능한 ACL

ACL(Access Control List, 액세스 제어 목록)은 정책 적용 포인트(예 : 스위치)에서 리소스에 적용할 수 있는 ACE(Access Control Entry)의 목록입니다. 각 ACE는 해당 개체에 대해 사용자마다 허용되는 권한(예: 읽기, 쓰기, 실행 등)을 식별합니다. 예를 들어 한 ACE로 Sales 그룹에 쓰기 권한을 허용하고 또 다른 ACE로 조직의 다른 모든 직원에게 읽기 권한을 허용하여 네트워크의 Sales 영역에 사용할 ACL을 구성할 수 있습니다. RADIUS 프로토콜을 사용하는 경우 ACL은 소스 및 대상 IP 주소, 전송 프로토콜 및 추가 매개변수를 필터링하여 권한을 부여합니다. 정적 ACL은 스위치에 있고 스위치에서 직접 구성되며 ISE GUI의 권한 부여 정책에서 적용할 수 있습니다. 다운로드 가능한 ACL(DACL)은 ISE GUI의 권한 부여 정책에서 구성, 관리 및 적용할 수 있습니다.

ISE의 네트워크 권한 부여 정책에서 DACL을 구현하려면

1. **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Downloadable ACLs(**다운로드 가능한 **ACL)**에서 기존 또는 새 DACL을 구성합니다. 자세한 내용은 다운로드 가능한 ACL에 대한 권한 구성, 914 페이지를 참고하십시오.
2. 이미 구성한 DACL을 사용하여 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization Profiles(**권한 부여 프로파일**)**에서 기존 권한 부여 프로파일을 구성합니다.
3. **Policy(**정책**)** > **Policy Sets(**정책 집합**)**에서 새 정책 집합과 기존 정책 집합을 생성 및 구성할 때 구성한 권한 부여 프로파일을 구현합니다.

다운로드 가능한 ACL에 대한 권한 구성

ISE를 사용하면 권한 부여 정책에서 DACL(Downloadable ACL)을 구성하고 구현하여 다양한 사용자 및 사용자 그룹이 네트워크에 액세스하는 방식을 제어할 수 있습니다. 기본 권한 부여 DACL은 다음 기본 프로파일을 포함하여 ISE 설치와 함께 사용할 수 있습니다.

- DENY_ALL_IPV4_TRAFFIC
- PERMIT_ALL_IPV4_TRAFFIC
- DENY_ALL_IPV6_TRAFFIC
- PERMIT_ALL_IPV6_TRAFFIC

DACL을 사용할 때는 이러한 기본값을 변경할 수 없지만, 해당 기본값을 복제하여 비슷한 DACL을 추가로 생성할 수 있습니다.

필요한 DACL을 구성했으면 해당 DACL을 네트워크의 관련 권한 부여 정책에 적용할 수 있습니다. DACL을 권한 부여 정책에 적용한 후에는 더 이상 유형을 변경하거나 ISE에서 삭제할 수 없습니다. 정책에서 이미 사용된 DACL 유형을 변경하려면 복제 DACL을 생성하여 복제본을 업데이트하거나 정책에서 DACL을 제거한 후 DACL을 업데이트하여 관련 있는 경우 다시 적용하면 됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Downloadable ACLs(**다운로드 가능한 **ACL)**.

단계 **2** **Downloadable ACL(**다운로드 가능한 **ACL)** 표 상단에서 **Add(**추가**)**를 클릭하거나 기존 DACL 중 하나를 선택하고 표 상단에서 **Duplicate(**복제**)**를 클릭합니다.

단계 **3** 다음 규칙을 고려하여 DACL에 대해 원하는 값을 입력하거나 편집합니다.

- Name(이름) 필드에 지원되는 문자는 영숫자, 하이픈(-), 점(.) 및 밑줄(_)입니다.
- IP 형식은 다음과 같이 DACL 유형을 선택할 때 설정한 IP 버전에 따라 처리됩니다.
  - 합법적인 IPv4 ACE만 검증하려면 **IPv4**를 선택합니다. 유효한 IPv4 형식을 입력해야 합니다.
  - 합법적인 IPv6 ACE만 검증하려면 **IPv6**을 선택합니다. 유효한 IPv6 형식을 입력해야 합니다.
  - 이전 릴리스에서 릴리스 2.6으로 업그레이드된 DACL의 **IP Version(IP** 버전**)** 필드에는 **Agnostic(**무관**)** 옵션이 DACL 유형으로 표시됩니다. 필요에 따라 원하는 형식을 입력합니다. **Agnostic(**무관**)**을 사용하여 Cisco에서 지원하지 않는 디바이스에 대한 DACL을 생성합니다. **Agnostic(**무관**)**을 선택하면 형식이 검증되지 않으며 DACL 구문을 확인할 수 없습니다.
- DACL의 모든 ACE에서 키워드 **Any(**일부**)**를 소스로 사용해야 합니다. DACL이 푸시되면 소스의 **Any(**일부**)**는 스위치에 연결되는 클라이언트의 IP 주소로 바뀝니다.

참고 DACL이 권한 부여 프로파일에 매핑된 경우 **IP Version(IP** 버전**)** 필드는 편집할 수 없습니다. 이 경우 **Authorization Profiles(**권한 부여 프로파일**)**에서 DACL 참조를 제거하고 IP 버전을 편집한 다음, **Authorization Profiles(**권한 부여 프로파일**)**에서 DACL을 다시 매핑합니다.

단계 **4** 필요한 경우 전체 ACE 목록 생성을 완료한 후 **Check DACL Syntax(DACL** 구문 확인**)**를 클릭하여 목록을 검증합니다. 검증 오류가 발생한 경우 이 검증은 자동으로 열리는 창에서 유효하지 않은 구문을 식별하는 특정 지침을 반환합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

Active Directory 사용자 권한 부여를 위한 머신 액세스 제한

Cisco ISE에는 Microsoft Active Directory 인증 사용자에 대해 권한 부여를 제어하는 추가 방법을 제공하는 MAR(Machine Access Restriction) 구성 요소가 포함되어 있습니다. 이 권한 부여 형식은 Cisco ISE 네트워크에 액세스하는 데 사용되는 컴퓨터의 머신 인증을 기반으로 합니다. 정상적으로 완료되는 모든 머신 인증에 대해 Cisco ISE는 RADIUS Calling-Station-ID 속성(속성 31)에서 수신된 값을 머신 인증 성공의 증거로 캐시합니다.

Cisco ISE는 Active Directory 설정 페이지의 "Time to Live" 매개변수에서 구성한 시간이 만료될 때까지 캐시의 각 Calling-Station-ID 속성을 유지합니다. 매개변수가 만료되면 Cisco ISE는 캐시에서 만료된 매개변수를 삭제합니다.

사용자가 최종 사용자 클라이언트에서 인증을 하면 Cisco ISE는 캐시를 검색해 성공한 머신 인증의 Calling-Station-ID 값을 찾은 다음 사용자 인증 요청에서 수신된 Calling-Station-ID 값을 확인합니다. Cisco ISE가 캐시에서 일치하는 사용자 인증 Calling-Station-ID 값을 찾으면 인증을 요청하는 사용자에 대해 Cisco ISE가 권한을 할당하는 방식에 다음과 같이 영향을 주게 됩니다.

- Calling-Station-ID 값이 Cisco ISE 캐시의 값과 일치하면 성공한 권한 부여에 대해 권한 부여 프로파일이 할당됩니다.
- Calling-Station-ID 값이 Cisco ISE 캐시의 값과 일치하지 않으면 머신 인증 없이 성공한 사용자 인증에 대한 권한 부여 프로파일이 할당됩니다.

권한 부여 정책 및 프로파일을 구성하기 위한 지침

권한 부여 정책 및 프로파일을 관리하는 경우 다음 지침을 따르십시오.

- 규칙 이름을 생성할 때는 다음과 같이 지원되는 문자를 사용해야 합니다.
  - 기호: 더하기(+), 하이픈(-), 밑줄 (_), 기간(.) 및 공백( )
  - 알파벳 문자: A~Z 및 a~z
  - 숫자 문자: 0~9
- ID 그룹은 기본적으로 "Any"(이 글로벌 기본값을 사용하여 모든 사용자에게 적용할 수 있음)로 설정됩니다.
- 조건을 사용하여 하나 이상의 정책 값을 설정할 수 있습니다. 그러나 조건은 선택적이며 권한 부여 정책을 생성하는 데 필요하지 않습니다. 조건을 생성하는 방법은 두 가지가 있습니다.
  - 선택한 해당 사전에서 기존 조건 또는 속성을 선택합니다.
  - 제안 값을 선택하거나 텍스트 상자를 사용하여 사용자 맞춤화 값을 입력할 수 있게 해주는 사용자 맞춤화 조건을 생성합니다.
- 조건 이름을 생성할 때는 다음과 같이 지원되는 문자를 사용해야 합니다.
  - 기호: 하이픈 (-), 밑줄 (_) 및 마침표(.)
  - 알파벳 문자: A~Z 및 a~z
  - 숫자 문자: 0~9
- 권한 부여 프로파일을 생성하거나 편집할 때 **Client Provisioning (Policy)(**클라이언트 프로비저닝**(**정책**))** 이외의 옵션으로 **Web Redirection (CWA, MDM, NSP, CPP)(**웹 리디렉션**(CWA, MDM, NSP, CPP))**을 활성화하도록 선택하면 해당 권한 부여 정책에 대해 IPv6 주소를 고정 **IP/**호스트 이름**/FQDN**으로 구성할 수 없습니다. IPv6 고정 IP/호스트 이름/FQDN이 CWA(Central Web Auth), MDM(Mobile Device Management) 리디렉션 및 NSP(Native Supplicant Protocol)에서 지원되지 않기 때문입니다.
- 정책에 사용할 권한 부여 프로파일을 선택하는 경우 권한이 중요합니다. 권한은 특정 리소스에 대한 액세스를 부여하거나 특정 작업을 수행하도록 허용할 수 있습니다. 예를 들어 사용자가 특정 ID 그룹(예: Device Admins)에 속해 있는 경우 사용자가 정의된 조건(예: 보스턴의 사이트)을 충족하면 이 사용자에게 해당 그룹과 연결된 권한이 부여됩니다(예: 네트워크 리소스 집합에 대한 액세스 또는 디바이스에 대한 특정 작업을 수행할 수 있는 권한).
- 권한 부여 조건에서 **radius** 속성 **Tunnel-Private-Group-ID**를 사용하는 경우, **EQUALS** 연산자를 사용할 때 태그와 조건의 값을 모두 언급해야합니다. 예를 들면 다음과 같습니다.

```
Tunnel-Private-Group-ID EQUALS (tag=0) 77
```

참고 Cisco ISE 1.4부터 ANC가 EPS(Endpoint Protection Services)를 대체합니다. ANC는 추가 분류 및 성능 개선을 제공합니다. 때때로 일부 ANC 작업에서는 ERS 속성을 사용하는 것이 가능할 수도 있지만 ANC 속성을 사용하는 것이 좋습니다. 예를 들어 **Session:EPSStatus=Quarantine**은 실패할 수 있습니다. **Session:ANCPolicy**를 정책의 조건으로 사용하십시오.

권한 부여 정책 구성

Policy(정책) 메뉴에서 권한 부여 정책에 대한 속성 및 구성 요소를 생성한 후 Policy Sets(정책 집합) 메뉴에서 정책 집합 내에 권한 부여 정책을 생성합니다.

시작하기 전에

이 절차를 시작하기 전에 그룹 및 조건 식별과 같은 권한 부여 정책을 생성하는 데 사용되는 여러 구성 요소를 기본적으로 파악해야 합니다.

단계 **1** 네트워크 액세스 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Policy Sets(**정책 집합**)**를 선택합니다. 디바이스 관리 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리자 정책 집합**)**를 선택합니다.

단계 **2** View(보기) 열에서 › 표시를 클릭하여 모든 정책 집합 세부정보에 액세스하고 인증 및 권한 부여 정책과 정책 예외를 생성합니다.

단계 **3** 페이지의 Authentication Policy(인증 정책) 부분 옆에 있는 화살표 아이콘을 클릭하면 인증 정책 표을 확장해서 볼 수 있습니다.

단계 **4** 아무 행의 **Actions(**작업**)** 열에서 톱니바퀴 아이콘을 클릭합니다. 드롭다운 메뉴에서 필요에 따라 Insert(삽입) 또는 Duplicate(중복) 옵션을 선택하여 새 인증 정책 규칙을 삽입합니다.
권한 부여 정책 표에 새 행이 나타납니다.

단계 **5** 정책 상태를 설정하려면 현재 **Status(**상태**)**를 클릭하고 드롭 다운 메뉴의 **Status(**상태**)** 열에서 필요한 상태를 선택합니다. 상태에 대한 자세한 내용은 권한 부여 정책 설정, 919 페이지를 참조하십시오.

단계 **6** 표의 정책에 대해선 **Rule Name(**규칙 이름**)** 셀을 클릭하여 자유 텍스트를 변경하고 고유한 규칙 이름을 생성합니다.

단계 **7** 조건을 추가하거나 변경하려면 **Conditions(**조건**)** 열의 셀 위에 마우스를 가져가 아이콘을 클릭합니다. Condition Studio가 열립니다. 자세한 내용은 정책 조건, 926 페이지를 참고하십시오.

선택하는 모든 속성에 "Equals(같음)", "Not Equals(같지 않음)", "In(존재)", "Not In(존재하지 않음)", "Matches(일치함)", "Starts With(다음으로 시작)" 또는 "Not Starts With(다음으로 시작 안 함)" 연산자 옵션이 포함되지는 않습니다.

"Matches(일치함)" 연산자는 와일드카드가 아닌 정규식(REGEX)을 지원하며 사용합니다.

참고 직접 비교하려면 "같음" 연산자를 사용해야 합니다. 다중 값 속성에 "Contains(포함)" 연산자를 사용할 수 있습니다. 정규식 비교에는 "일치함" 연산자를 사용해야 합니다. "일치함" 연산자를 사용하면 정적 값과 동적 값 모두에 대해 정규식이 해석됩니다. 목록의 경우 "In(존재)" 연산자는 목록에 특정 값이 있는지 확인합니다. 단일 문자열의 경우 "In(존재)" 연산자는 문자열이 "Equals(같음)" 연산자와 동일한지를 확인합니다.

단계 **8** 네트워크 액세스 결과 프로파일의 경우 **Results Profiles(**결과 프로파일**)** 드롭 다운 목록에서 관련 권한 부여 프로파일을 선택하거나 **Create or New Authorization Profile(**새 권한 부여 프로파일 생성**)**을 ✚를 선택하거나 클릭하고 **Add New Standard Profile(**새 표준 프로파일 추가**)** 화면이 열리면 다음 단계를 수행합니다.

a) 새 권한 부여 프로파일을 구성하는 데 필요한 값을 입력합니다. 다음에 유의해야 합니다.

- Name(이름) 필드에 입력할 수 있는 문자는 공백, ! # $ % & ' ( ) * + , - . / ; = ? @ _ {입니다.
- **Common Tasks(**일반 작업**)**에서 DACL을 입력하려면 다음과 같이 관련 **DACL Name(DACL** 이름**)** 옵션을 선택한 다음 동적 드롭 다운 목록에서 필요한 DACL을 선택합니다.
  - IPv4 DACL을 사용하려면 **DACL Name(DACL** 이름**)**을 선택합니다.
  - IPv6 DACL을 입력하려면 **IPv6 DACL Name(IPv6 DACL**이름**)**을 선택합니다.
  - 다른 DACL 구문을 입력하려면 두 옵션 중 하나를 선택합니다. 비종속 DACL은 IPv4 및 IPv6 드롭 다운 목록에 모두 표시됩니다.

    참고 **DACL Name(DACL** 이름**)**을 선택하는 경우에는 DACL 자체가 비종속적이더라도 IPv4에 대한 AVP 유형이 사용됩니다. **IPv6 DACL Name(IPv6 DACL** 이름**)**으로 DACL을 선택하는 경우에는 DACL 자체가 비종속적이어도 AVP 유형은 IPv6용입니다.

- 참고 정책에 ACL을 사용하려는 경우 디바이스가 이 기능과 호환되는지 확인합니다. 자세한 내용은 *Cisco Identity Services Engine Compatibility Guide*를 참조하십시오.

  Common Tasks(일반 작업**)**에서 ACL을 입력하려면 다음과 같이 관련 **ACL(Filter-ID)** 옵션을 선택한 다음 필드에 ACL 이름을 입력합니다.
  - IPv4 ACL을 사용하려면 **ACL(Filter-ID)**을 선택합니다.
  - IPv6 ACL을 입력하려면 **ACL IPv6(Filter-ID)**를 선택합니다.
- Airespace 디바이스에 ACL을 사용하려면 필요에 따라 **Airespace ACL Name(Airespace ACL** 이름**)** 또는 **Airespace IPv6 ACL Name(Airespace IPv6 ACL** 이름**)**을 선택하고 필드에 ACL 이름을 입력합니다.
- **Attributes Details(**속성 세부정보**)**에서 화면 하단에 동적으로 표시되는 권한 부여 프로파일 RADIUS 구문을 다시 확인할 수 있습니다.

b) 변경사항을 Cisco ISE 시스템 데이터베이스에 저장해 권한 부여 프로파일을 생성하려면 **Save(**저장**)**을 클릭합니다.

c) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택하여 Policy Sets(정책 집합) 영역 외부에서 프로파일을 생성, 관리, 편집 및 삭제합니다.

단계 **9** 네트워크 액세스 결과 보안 그룹의 경우 **Results Security Groups(**결과 보안 그룹**)** 드롭 다운 목록에서 관련 보안 그룹을 선택하거나 ➕을 클릭하고 **Create a New Security Group(**새 보안 그룹 생성**)**을 선택하여 Create New Security Group(새 보안 그룹 생성) 화면이 열리면 다음 단계를 수행합니다.

a) 새 보안 그룹의 이름과 설명(선택 사항)을 입력합니다.

b) 이 SGT를 Cisco ACI로 전파하려는 경우 **Propagate to ACI(ACI**로 전파**)** 확인란을 선택합니다. 이 SGT와 관련된 SXP 매핑은 Cisco ACI Settings(Cisco ACI 설정) 페이지에서 선택한 VPN에 속하는 경우에만 Cisco ACI로 전파됩니다.

이 옵션은 기본적으로 비활성화되어 있습니다.

c) 태그 값을 입력합니다. 태그 값은 수동으로 입력하거나 자동 생성되도록 설정할 수 있습니다. SGT의 범위를 예약할 수도 있습니다. 에서 이 범위를 구성할 수 있습니다.Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Settings(**설정**) > General TrustSec Settings(**일반 **TrustSec** 설정**)**

d) **Submit(**제출**)**을 클릭합니다.

자세한 내용은 보안 그룹 컨피그레이션, 1024 페이지를 참고하십시오.

단계 **10** TACACS+ 결과의 경우 **Results(**결과**)** 드롭 다운 목록에서 관련 명령 집합 및 셸 프로파일을 선택하거나 **Command Sets(**명령 집합**)** 또는 **Shell Profiles(**셸 프로파일**)** 열에서 ➕를 클릭하여 **Add Commands(**명령 추가**)** 화면 또는 **Add Shell Profile(**셸 프로파일 추가**)**을 각각 엽니다. **Create a New Command Set(**새 명령 집합 생성**)** 또는 **Create a New Shell Profile(**새 셸 프로파일 생성**)**을 선택하고 필드를 입력합니다.

단계 **11** 확인하고 일치시킬 순서에 따라 표 내에서 정책을 정리합니다.

단계 **12** 변경사항을 Cisco ISE 시스템 데이터베이스에 저장하고 이 새 권한 부여 정책을 생성하려면 **Save(**저장**)**를 클릭합니다.

권한 부여 정책 설정

다음 표에서는 정책 집합의 일부로 권한 부여 정책을 구성할 수 있는 **Policy Sets(**정책 집합**)** 창의 **Authorization Policy(**권한 부여 정책**)** 섹션에 대해 설명합니다. 네트워크 액세스 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > Network Access(**네트워크 액세스**) > Policy Sets(**정책 집합**)**를 선택합니다. 디바이스 관리 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > Device Administration(**디바이스 관리**) > Device Admin Policy Sets(**디바이스 관리자 정책 집합**)**를 선택합니다.

표 ***127:*** 권한 부여 정책 구성 설정

필드 이름	사용 지침
Status(상태**)**	이 정책의 상태를 선택합니다. 다음 중 하나일 수 있습니다. • **Enabled(**활성화됨**)**: 이 정책 조건이 활성 상태입니다. • **Disabled(**비활성화됨**)**: 이 정책 조건이 비활성 상태이며 평가되지 않습니다. • **Monitor Only(**모니터링만**)**: 이 정책 조건이 평가되지만 결과가 적용되지 않습니다. 라이브 로그 인증 페이지에서 이 정책 조건의 결과를 확인할 수 있습니다. 이 페이지에서는 모니터링되는 단계 및 속성이 포함된 상세 보고서를 확인할 수 있습니다. 새 정책 조건을 추가하려고 하는데 해당 조건이 올바른 결과를 제공할지 여부가 확실치 않은 경우를 예로 들어 보겠습니다. 이러한 상황에서는 모니터링되는 모드에서 정책 조건을 생성하여 결과를 확인한 다음 원하는 결과가 표시되면 조건을 활성화할 수 있습니다.
Rule Name(규칙 이름**)**	이 정책에 대한 고유한 이름을 입력합니다.
Conditions(조건**)**	새 정책 행에서 더하기(+) 아이콘을 클릭하거나, 기존의 정책 행에서 편집 아이콘을 클릭해 Conditions Studio를 엽니다.
결과 또는 프로파일	구성된 보안 그룹에 제공되는 여러 권한 레벨을 결정하는 관련 권한 부여 프로파일을 선택합니다. 관련 권한 부여 프로파일을 아직 구성하지 않은 경우 인라인으로 설정할 수 있습니다.
결과 또는 보안 그룹	특정 규칙과 관련된 사용자 그룹을 결정하는 관련 보안 그룹을 선택합니다. 관련 보안 그룹을 아직 구성하지 않은 경우 인라인으로 구성할 수 있습니다.
결과 또는 명령 집합	명령 집합은 디바이스 관리자가 실행할 수 있는 지정된 명령 목록을 적용합니다. 디바이스 관리자가 네트워크 디바이스에서 작동 명령을 실행하면 관리자가 이러한 명령을 실행할 권한이 있는지를 확인하기 위해 ISE가 쿼리됩니다. 이를 명령 권한 부여라고도 합니다.

필드 이름	사용 지침
결과 또는 쉘**(shell)** 프로파일	TACACS+ 쉘(shell) 프로파일은 디바이스 관리자의 초기 로그인 세션을 제어합니다.
Hits(히트**)**	Hits(히트)는 조건이 충족된 횟수를 나타내는 진단 도구입니다.
Actions(작업**)**	작업 열에서 톱니바퀴 아이콘( )을 클릭해 다양한 작업을 보고 선택할 수 있습니다. • Insert new row above(위에 새 행 삽입): Actions(작업) 메뉴가 열린 규칙의 위에 새 권한 부여 정책을 삽입합니다. • Insert new row below(아래에 새 행 삽입): Actions(작업) 메뉴가 열린 규칙의 아래에 새 권한 부여 정책을 삽입합니다. • Duplicate above(위에 복제): Actions(작업) 메뉴가 열린 규칙의 위에 복제 권한 부여 정책을 삽입합니다(원본 집합 위). • Duplicate below(위에 복제): Actions(작업) 메뉴가 열린 규칙의 아래에 복제 권한 부여 정책을 삽입합니다(원본 집합 아래). • Delete(삭제): 규칙을 삭제합니다.

권한 부여 프로파일 설정

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다. **Authorization Profiles(**권한 부여 프로파일**)** 창은 네트워크 액세스에 대한 속성을 정의합니다.

권한 부여 프로파일 설정

- **Name(**이름**)**: 권한 부여 프로파일의 이름을 입력합니다.
- **Description(**설명**)**: 권한 부여 프로파일에 대한 설명을 입력합니다.
- **Access Type(**액세스 유형**)**: 액세스 유형을 **ACCESS_ACCEPT** 또는 **ACCESS_REJECT** 중에서 선택합니다.
- **Service Template(**서비스 템플릿**)**:이 옵션을 활성화하면 SAnet 지원 디바이스와의 세션을 지원할 수 있습니다. Cisco ISE는 서비스 템플릿 호환 상태로 표시하는 특수 플래그를 사용하는 권한 부여 프로파일로 서비스 템플릿을 구현합니다. 서비스 템플릿은 권한 부여 프로파일이기도 하므로, SAnet 및 비 SAnet 디바이스를 모두 지원하는 단일 정책 역할을 합니다.

- **Track Move(**이동 추적**)**: Cisco MSE(Mobility Services Engine)로 사용자 위치를 추적하려면 이 옵션을 활성화합니다.

  참고 이 옵션은 Cisco ISE 성능에 영향을 줄 수 있으며, 보안 수준이 높은 위치에서만 사용할 수 있습니다.

- **Passive Identity Tracking(**패시브 **ID** 추적**)**: 정책 시행 및 사용자 추적에 패시브 ID의 Easy Connect 기능을 사용하려면 이 옵션을 활성화합니다.

공통 작업

공통 작업은 네트워크 액세스에 적용되는 특정 권한 및 작업입니다.

- **DACL Name(DACL** 이름**)**: 다운로드 가능한 ACL을 사용하려면 이 옵션을 활성화합니다. 기본값(**PERMIT_ALL_IPV4_TRAFFIC**, **PERMIT_ALL_IPV6_TRAFFIC**, **DENY_ALL_IPV4_TRAFFIC**, **DENY_ALL_IPV6_TRAFFIC**)을 사용하거나 다음 사전에서 속성을 선택할 수 있습니다.
  - 외부 ID 저장소(속성)
  - 엔드포인트
  - 내부 사용자
  - 내부 엔드포인트

  DACL을 추가하거나 기존 DACL을 편집 및 관리하는 방법에 대한 자세한 내용은 다운로드 가능한 ACL, 914 페이지를 참조하십시오.

- **ACL (Filter-ID)**: RADIUS Filter-ID 속성을 구성하려면 이 옵션을 활성화합니다. Filter-ID는 NAD에서 ACL을 지정합니다. Filter-ID를 정의하면 Cisco ISE가 파일 이름에 ".in"을 추가합니다. Filter-ID가 **Attributes Details(**속성 세부정보**)** 패널에 표시됩니다. **ACL IPv6 (Filter-ID)**는 NAD에 대한 IPv6 연결에도 동일한 방식으로 작동합니다.

- **Security Group(**보안 그룹**)**: 권한 부여에 대한 보안 그룹(SGT) 부분을 할당하려면 이 옵션을 활성화합니다.
  - Cisco ISE가 Cisco DNA 센터와 통합되지 않은 경우 Cisco ISE는 VLAN ID 1을 할당합니다.
  - Cisco ISE가 Cisco DNA 센터와 통합된 경우 Cisco DNA 센터가 Cisco ISE와 공유하는 VN(Virtual Network)을 선택하고 **Data Type(**데이터 유형**)**과 서브넷/주소 풀을 선택합니다.

  참고 보안 그룹 작업에는 보안 그룹 및 VN이 포함됩니다. 보안 그룹을 구성하는 경우 VLAN을 구성할 수 없습니다. 엔드포인트 디바이스는 하나의 가상 네트워크에만 할당할 수 있습니다.

- **VLAN**: VLAN(Virtual LAN) ID를 지정하려면 이 옵션을 활성화합니다. VLAN ID에 정수 또는 문자열 값을 입력할 수 있습니다. 이 항목의 형식은 `Tunnel-Private-Group-ID:VLANnumber`입니다.
- **Voice Domain Permission(**음성 도메인 권한**)**: 다운로드 가능한 ACL을 사용하려면 이 옵션을 활성화합니다. `cisco-av-pair`의 VSA(Vendor-Specific Attribute)가 `device-traffic-class=voice` 값과 연결됩니다. 다중 도메인 권한 부여 모드에서 네트워크 스위치가 이 VSA를 받으면 권한 부여가 완료된 후 엔드포인트가 음성 도메인에 연결됩니다.
- **Web Redirection (CWA, DRW, MDM, NSP, CPP)(**웹 리디렉션**(CWA, DRW, MDM, NSP, CPP))**: 인증 후 웹 리디렉션을 활성화하려면 이 옵션을 활성화합니다.
  - 리디렉션 유형을 선택합니다. 선택하는 웹 리디렉션 유형에 추가 옵션이 표시되며, 이러한 옵션은 아래에 설명되어 있습니다.
  - Cisco ISE가 NAD로 전송하는 리디렉션을 지원하려면 ACL을 입력합니다.

    NAD로 전송하기 위해 입력하는 ACL은 **Attributes Details(**속성 세부정보**)** 패널에 cisco-av 쌍으로 표시됩니다. 예를 들어 입력한 값이 **acl119**인 경우 이는 **Attributes Details(**속성 세부정보**)** 패널에 `cisco-av-pair = url-redirect-acl = acl119`로 반영됩니다.
  - 선택한 웹 리디렉션 유형에 대한 기타 설정을 선택합니다.

  다음 웹 리디렉션 유형 중 하나를 선택합니다.
  - **Centralized Web Auth(**중앙 웹 인증**)**: **Value(**값**)** 드롭다운에서 선택한 포털로 리디렉션됩니다.
  - **Client Provisioning (Posture)(**클라이언트 프로비저닝**(**포스처**))**: **Value(**값**)** 드롭다운에서 선택하는 클라이언트 프로비저닝 포털로 리디렉션되어 클라이언트에서 포스처를 활성화합니다.
  - **Hot Spot: Redirect(**핫스팟**:** 리디렉션**)**: **Value(**값**)** 드롭다운에서 선택한 핫스팟 포털로 리디렉션됩니다.
  - **MDM Redirect(MDM** 리디렉션**)**: 지정한 MDM 서버의 MDM 포털로 리디렉션됩니다.
  - **Native Supplicant Provisioning(**기본 신청자 프로비저닝**)**: **Value(**값**)** 드롭다운에서 선택하는 BYOD 포털로 리디렉션됩니다.

  웹 리디렉션 유형을 선택하고 필수 매개변수를 입력한 후 다음 옵션을 구성합니다.
  - **Display Certificates Renewal Message(**인증서 갱신 메시지 표시**)**: 인증서 갱신 메시지를 표시하려면 이 옵션을 활성화합니다. URL-redirect 속성 값이 변경되어 인증서가 유효한 기간(일)이 포함됩니다. 이 옵션은 중앙 웹 인증 리디렉션에만 사용됩니다.
  - **Static IP/Host Name/FQDN(**정적 **IP/**호스트 이름**/FQDN)**: 사용자를 다른 PSN으로 리디렉션하려면 이 옵션을 활성화합니다. 대상 IP 주소, 호스트 이름 또는 FQDN을 입력합니다. 해당 옵션을 구성하지 않으면 사용자가 이 요청을 수신한 정책 서비스 노드의 FQDN으로 리디렉션됩니다.

  - **Suppress Profiler CoA for endpoints in Logical Profile(**논리적 프로파일에서 엔드포인트에 대해 프로파일러 **CoA** 표시 안 함**)**: 특정 유형의 엔드포인트 디바이스에 대한 리디렉션을 취소하려면 이 옵션을 활성화합니다.

- **Auto SmartPort**: Auto SmartPort 기능을 사용하려면 이 옵션을 활성화합니다. 이벤트 이름을 입력합니다. 그러면 `auto-smart-port=event_name`값으로 VSA cisco-av-pair가 생성됩니다. 이 값은 **Attributes Details(**속성 세부정보**)** 패널에 표시됩니다.
- **Access Vulnerabilities(**액세스 취약점**)**: 권한 부여의 일부로 이 엔드포인트에서 Threat Centric NAC 취약점 평가를 실행하려면 이 옵션을 활성화합니다. 어댑터를 선택하고 스캔을 실행할 시기를 선택합니다.
- **Reauthentication(**재인증**)**: 재인증 중에 엔드포인트를 연결 상태로 유지하려면 이 옵션을 활성화합니다. **RADIUS-Request**(1)를 사용하도록 선택하여 재인증 중에 연결을 유지하도록 설정합니다. 기본 RADIUS-Request(0)는 기존 세션의 연결을 끊습니다. 비활성 타이머를 설정할 수도 있습니다.
- **MACSec Policy(MACSec** 정책**)**: MACSec 활성화 클라이언트가 Cisco ISE에 연결할 때마다 MACSec 암호화 정책을 사용하려면 이 옵션을 활성화합니다. **must-secure**, **should-secure**, **must-not-secure** 중에서 옵션을 하나 선택합니다. 예를 들어 선택한 설정이 **Attributes Details(**속성 세부정보**)** 패널에 `cisco-av-pair = linksec-policy=must-secure`로 표시됩니다.
- **NEAT**: 네트워크 간에 ID 인식을 확장하는 기능인 NEAT(Network Edge Access Topology)를 사용하려면 이 확인란을 활성화합니다. 이 확인란을 선택하면 **Attributes Details(**속성 세부정보**)** 패널에 `cisco-av-pair = device-traffic-class=switch` 값이 표시됩니다.
- **Web Authentication (Local Web Auth)(**웹 인증 **(**로컬 웹 인증**)):** 이 권한 부여 프로파일에 로컬 웹 인증을 사용하려면 이 옵션을 활성화합니다. 이 값을 사용하면 스위치가 DACL과 함께 VSA를 보내는 Cisco ISE에 의한 웹 인증에 대한 권한 부여를 인식할 수 있습니다. VSA는 `cisco-av-pair = priv-lvl=15`이고, 이는 **Attributes Details(**속성 세부정보**)** 패널에 표시됩니다.
- **Airespace ACL Name(Airespace ACL** 이름**)**: Cisco Airespace 무선 컨트롤러에 ACL 이름을 전송하려면 이 옵션을 활성화합니다. Airespace VSA는 이 ACL을 사용하여 WLC의 연결에 대해 로컬로 정의된 ACL 권한을 부여합니다. 예를 들어 **rsa-1188**을 입력하면 **Attributes Details(**속성 세부정보**)** 패널에 `Airespace-ACL-Name = rsa-1188` 로 표시됩니다.
- **ASA VPN**: ASA(Adaptive Security Appliance) VPN 그룹 정책을 할당하려면 이 옵션을 활성화합니다. 드롭다운 목록에서 VPN 그룹 정책을 선택합니다.
- **AVC Profile Name(AVC** 프로파일 이름**)**: 이 엔드포인트에서 애플리케이션 가시성을 실행하려면 이 옵션을 활성화합니다. 사용할 AVC 프로파일을 입력합니다.
- **UPN Lookup(UPN** 조회**)**: TBD

고급 속성 설정

- **Dictionaries(**사전**)**: **Dictionaries(**사전**)** 창에 사용 가능한 옵션을 표시하려면 아래쪽 화살표 아이콘을 클릭합니다. 첫 번째 필드에서 구성해야 하는 사전 및 속성을 선택합니다.

- **Attribute Values(**속성 값**)**: **Attribute Values(**속성 값**)** 창에 사용 가능한 옵션을 표시하려면 아래쪽 화살표 아이콘을 클릭합니다. 원하는 속성 그룹과 속성 값을 선택합니다. 이 값은 첫 번째 필드에서 선택한 항목과 일치합니다. 사용자가 구성한 **Advanced Attributes(**고급 속성**)** 설정은 **Attributes Details(**속성 세부정보**)** 패널에 표시됩니다.
- **Attributes Details(**속성 세부정보**)**: 이 패널에는 **Common Tasks(**일반 작업**)** 및 **Advanced Attributes(**고급 속성**)**에 대해 설정한 구성된 속성 값이 모두 표시됩니다.

  Attributes Details(속성 세부정보**)** 패널에 표시되는 값은 읽기 전용입니다.

참고 **Attributes Details(**속성 세부정보**)** 패널에 표시되는 읽기 전용 값을 수정하거나 삭제하려면 **Advanced Attributes Settings(**고급 속성 설정**)** 패널의 **Attribute Values(**속성 값**)** 필드에서 선택한 속성 또는 해당 **Common Tasks(**일반 작업**)** 필드 값을 수정하거나 삭제해야 합니다.

관련 항목

Cisco ISE 권한 부여 프로파일, 911 페이지
권한 부여 프로파일에 대한 권한, 911 페이지
미등록 디바이스 리디렉션을 위한 권한 부여 프로파일 구성, 895 페이지
권한 부여 프로파일 생성, 389 페이지

권한 부여 정책 예외

각 정책 집합 내에서 일반 권한 부여 정책뿐만 아니라 로컬 예외 규칙(각 정책 집합에 대한 Set(집합) 보기의 권한 부여 정책 로컬 예외 부분에서 정의)과 전역 예외 규칙(각 정책 집합에 대한 Set(집합) 보기의 권한 부여 정책 전역 예외 부분에서 정의)도 정의할 수 있습니다.

전역 권한 부여 예외 정책을 활성화하면 모든 정책 집합의 권한 부여 규칙 전체를 재정의하는 규칙을 정의할 수 있습니다. 전역 권한 부여 예외 정책을 구성하면 모든 정책 집합에 추가됩니다. 그런 다음 현재 구성된 정책 집합 내에서 전역 권한 부여 예외 정책을 업데이트할 수 있습니다. 전역 권한 부여 예외 정책을 업데이트할 때마다 해당 업데이트가 모든 정책 집합에 적용됩니다.

로컬 권한 부여 예외 규칙이 전역 예외 규칙을 덮어쓰게 됩니다. 권한 부여 규칙은 첫 번째 로컬 예외 규칙, 전역 예외 규칙, 권한 부여 정책의 일반 규칙순으로 처리됩니다.

권한 부여 예외 정책 규칙은 권한 부여 정책 규칙과 동일하게 구성됩니다. 권한 부여 정책에 대한 자세한 내용은 권한 부여 정책 구성, 917 페이지를 참조하십시오.

참고 Cisco ISE에서는 보안 문제를 방지하기 위해 권한 부여 정책에서 % 문자를 사용할 수 없습니다.

로컬 및 전역 예외 컨피그레이션 설정

네트워크 액세스 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Policy Sets(**정책 집합**)**를 선택합니다. 디바이스 관리 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리자 정책 집합**)**를 선택합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy Sets(**정책 집합**)** > **View(**보기**)** > **Local Exceptions Policy(**로컬 예외 정책**)** 또는 **Global Exceptions Policy(**전역 예외 정책**)**.

권한 부여 예외 설정은 권한 부여 정책 설정과 동일하며 권한 부여 정책 설정, 919 페이지에 설명되어 있습니다.

정책 조건

Cisco ISE는 규칙 기반 정책을 사용하여 네트워크 액세스를 제공합니다. 정책은 규칙 및 결과 집합이며, 규칙은 결과로 구성됩니다. Cisco ISE에서는 시스템 라이브러리에 저장하여 Conditions Studio의 다른 규칙 기반 정책에서 재사용 가능한 개별 정책 요소로 조건을 생성할 수 있습니다.

조건은 필요에 따라 연산자(같음, 같지 않음, 보다 큼 등) 및 값을 사용하거나 여러 속성, 연산자 및 복합 계층 구조를 포함하여 복잡할 수도 있고 단순할 수도 있습니다. 런타임에 Cisco ISE는 정책 조건을 평가한 다음 정책 평가에서 true 값을 반환하는지, 아니면 false 값을 반환하는지에 따라 관리자가 정의한 결과를 적용합니다.

조건을 생성하고 고유한 이름을 할당한 후에는 Conditions Studio Library에서 조건을 선택하여 다양한 규칙과 정책에서 이 조건을 여러 번 재사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
Network Conditions.MyNetworkCondition EQUALS true
```

정책 또는 다른 조건의 일부로 사용되는 조건은 Condition Studio에서 삭제할 수 없습니다.

각 조건은 정책 조건에 포함할 수 있는 개체 목록을 정의하므로 요청에 표시되는 것과 일치하는 정의 집합이 생성됩니다.

연산자 `EQUALS true`를 사용하여 네트워크 조건이 true로 평가되는지(요청에 제시된 값이 네트워크 조건 내에서 하나 이상의 항목과 일치하는지) 확인하거나 `EQUALS false`를 사용하여 네트워크 조건이 false로 평가되는지(네트워크 조건의 어느 항목과도 일치하지 않음) 확인할 수 있습니다.

또한 Cisco ISE는 정책에서 개별적으로 또는 사용자 맞춤화 조건의 구성 요소로 사용할 수 있는 미리 정의된 스마트 조건을 제공하며, 이러한 조건은 필요에 따라 업데이트하고 변경할 수 있습니다.

다음과 같은 고유한 네트워크 조건을 생성하여 네트워크에 대한 액세스를 제한할 수 있습니다.

- Endstation Network Conditions(엔드스테이션 네트워크 조건) - 연결을 시작하고 종료하는 엔드스테이션을 기준으로 합니다.

  Cisco ISE는 원격 주소 TO 필드(TACACS+ 요청인지 아니면 RADIUS 요청인지에 따라 다르게 수집)를 평가하여 해당 엔드포인트의 IP 주소, MAC 주소, CLI(Calling Line Identification), DNIS(Dialed Number Identification Service) 중 어느 것인지를 식별합니다.

  RADIUS 요청에서는 이 식별자를 속성 31(Calling-Station-Id)에서 확인할 수 있습니다.

TACACS+ 요청에서는 원격 주소에 슬래시(/)가 포함되어 있으면 슬래시 앞부분은 FROM 값으로, 슬래시 뒷부분은 TO 값으로 사용됩니다. 예를 들어 요청에 CLI/DNIS가 있는 경우 CLI는 FROM 값으로, DNIS는 TO 값으로 사용됩니다. 슬래시가 포함되지 않은 경우 전체 원격 주소가 FROM 값(IP 주소, MAC 주소 또는 CLI)으로 간주됩니다.

- Device Network Conditions(디바이스 네트워크 조건) - 요청을 처리하는 AAA 클라이언트를 기준으로 합니다.

  네트워크 디바이스는 IP 주소, 네트워크 디바이스 저장소에 정의된 디바이스 이름 또는 네트워크 디바이스 그룹으로 식별할 수 있습니다.

  RADIUS 요청에서는 속성 4(NAS-IP-Address)가 있는 경우 Cisco ISE가 이 속성에서 IP 주소를 가져오며, 속성 32(NAS-Identifier)가 있는 경우 속성 32에서 IP 주소를 가져옵니다. 그리고 이러한 속성을 찾을 수 없는 경우 수신하는 패킷에서 IP 주소를 가져옵니다.

  디바이스 사전(NDG 사전)에는 위치, 디바이스 유형 또는 NDG를 나타내는 동적으로 생성된 기타 속성과 같은 네트워크 디바이스 그룹 속성이 포함되어 있습니다. 이러한 속성에는 현재 디바이스와 관련된 그룹이 포함됩니다.

- Device Port Network Conditions(디바이스 포트 네트워크 조건) - 디바이스의 IP 주소, 이름, NDG, 포트(엔드스테이션이 연결된 디바이스의 물리적 포트)를 기준으로 합니다.

  RADIUS 요청에서는 요청에 속성 5(NAS-Port)가 있는 경우 Cisco ISE가 이 속성에서 값을 가져오며, 속성 87(NAS-Port-Id)가 있는 경우 속성 87에서 요청을 가져옵니다.

  TACACS+ 요청에서는 Cisco ISE가 모든 단계의 시작 요청 포트 필드에서 이 식별자를 가져옵니다.

이러한 고유한 조건에 대한 자세한 내용은 특수 네트워크 액세스 조건 , 946 페이지 항목을 참고하십시오.

사전 및 사전 속성

사전은 속성 및 허용되는 값으로 구성된 도메인별 카탈로그로 도메인에 대한 액세스 정책을 정의하는 데 사용할 수 있습니다. 개별 사전은 동일한 속성 유형의 모음입니다. 사전에 정의된 속성의 속성 유형은 동일하며 해당 유형은 지정된 속성의 소스 또는 상황을 나타냅니다.

속성 유형은 다음 중 하나일 수 있습니다.

- MSG_ATTR
- ENTITY_ATTR
- PIP_ATTR

속성 및 허용되는 값 외에, 사전에는 이름과 설명, 데이터 유형, 기본값 등 속성에 대한 정보가 포함되어 있습니다. 속성은 BOOLEAN, FLOAT, INTEGER, IPv4, IPv6, OCTET_STRING, STRING, UNIT32 및 UNIT64 데이터 유형 중 하나를 가질 수 있습니다.

Cisco ISE는 설치 중에 시스템 사전을 생성하며 관리자는 사용자 사전을 생성할 수 있습니다.

속성은 다른 시스템 사전에 저장됩니다. 속성은 조건을 구성하는 데 사용됩니다. 속성은 여러 조건에서 재사용 할 수 있습니다.

정책 조건을 생성할 때 유효한 속성을 재사용하려면 지원되는 속성이 포함된 사전에서 해당 속성을 선택합니다. 예를 들어 Cisco ISE는 NetworkAccess 사전에 있는 AuthenticationIdentityStore라는 속성을 제공합니다. 이 속성은 사용자 인증 과정에서 액세스한 마지막 ID 소스를 식별합니다.

- 인증 중에 단일 ID 소스가 사용되는 경우 이 속성은 인증이 성공적으로 완료된 ID 저장소의 이름을 포함합니다.
- 인증 중에 ID 소스 시퀀스가 사용되는 경우 이 속성은 마지막으로 액세스한 ID 소스의 이름을 포함합니다.

AuthenticationIdentityStore 속성과 함께 AuthenticationStatus 속성을 사용하여 사용자가 성공적으로 인증된 ID 소스를 식별하는 조건을 정의할 수 있습니다. 예를 들어 권한 부여 정책에서 LDAP 디렉토리(LDAP13)를 사용하여 사용자 인증이 이루어지는 조건을 확인하려면 재사용 가능한 다음 조건을 정의할 수 있습니다.

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

참고 AuthenticationIdentityStore는 조건 데이터를 입력하는 데 사용할 수 있는 텍스트 필드를 나타냅니다. 이 필드에 이름을 올바르게 입력하거나 복사해야 합니다. ID 소스의 이름이 변경된 경우 ID 소스 변경 사항과 일치하도록 이 조건을 수정해야 합니다.

이전에 인증된 엔드포인트 ID 그룹을 기반으로 조건을 정의할 수 있도록 Cisco ISE에서는 엔드포인트 ID 그룹 802.1X 인증 과정에서 정의된 권한 부여를 지원합니다. Cisco ISE에서 802.1X 인증을 수행하는 경우, RADIUS 요청의 "Calling-Station-ID" 필드에서 MAC 주소를 추출하고 이 값을 사용하여 디바이스의 엔드포인트 ID 그룹(endpointIDgroup 속성으로 정의됨)에 대한 세션 캐시를 조회하여 채웁니다. 이 프로세스로 권한 부여 정책 조건 생성에 사용할 수 있는 endpointIDgroup 속성을 제공할 수 있으며, 이 속성을 사용자 정보와 함께 사용하여 엔드포인트 ID 그룹 정보를 기반으로 권한 부여 정책을 정의할 수 있습니다.

엔드포인트 ID 그룹에 대한 조건은 권한 부여 정책 컨피그레이션 페이지의 ID 그룹 열에 정의될 수 있습니다. 사용자 관련 정보를 기반으로 하는 조건은 권한 부여 정책의 "기타 조건" 섹션에 정의되어야 합니다. 사용자 정보가 내부 사용자 속성을 기반으로 하는 경우 내부 사용자 사전의 ID 그룹 속성을 사용합니다. 예를 들어 "User Identity Group:Employee:US"와 같은 값을 사용하여 ID 그룹에 전체 값 경로를 입력할 수 있습니다.

네트워크 액세스 정책에 대해 지원되는 사전

Cisco ISE는 인증 및 권한 부여 정책에 대한 조건 및 규칙을 구축할 때 필요한 다양한 속성을 포함하는 다음과 같은 시스템 저장 사전을 지원합니다.

- 시스템 정의 사전
  - CERTIFICATE

- DEVICE
- RADIUS

- RADIUS 벤더 사전
  - Airespace
  - Cisco
  - Cisco-BBSM
  - Cisco-VPN3000
  - Microsoft
  - 네트워크 액세스

권한 부여 정책 유형의 경우, 조건에 구성된 확인은 반환될 인증 프로파일을 따라야 합니다.

일반적으로 확인에는 사용자 맞춤화 이름이 있는 하나 이상의 조건이 포함됩니다. 이러한 조건은 라이브러리에 추가되어 다른 정책에 의해 재사용될 수 있습니다.

다음 섹션에서는 조건 구성에 사용할 수 있는 지원되는 속성 및 사전에 대해 설명합니다.

사전에서 지원되는 속성

이 표에는 사전에서 지원되는 고정 속성이 나와 있으며 이러한 속성은 정책 조건에서 사용할 수 있습니다. 모든 유형의 조건을 생성할 때 이러한 속성 전부를 사용할 수 있는 것은 아닙니다.

예를 들어 인증 정책에서 액세스 서비스를 선택하기 위한 조건을 생성하는 경우, 네트워크 액세스 속성으로 디바이스 IP 주소, ISE 호스트 이름, 네트워크 디바이스 이름, 프로토콜 및 활용 사례만 표시됩니다.

정책 조건에서 다음 표에 나열된 속성을 사용할 수 있습니다.

사전	속성	허용되는 프로토콜 규칙 및 프록시	**ID** 규칙
디바이스	디바이스 유형(미리 정의된 네트워크 디바이스 그룹)	예	예
	디바이스 위치(미리 정의된 네트워크 디바이스 그룹)		
	기타 사용자 맞춤화 네트워크 디바이스 그룹		
	소프트웨어 버전		
	모델 이름		
RADIUS	모든 속성	예	예

사전	속성	허용되는 프로토콜 규칙 및 프록시	**ID** 규칙
네트워크 액세스	ISE 호스트 이름	예	예
	AuthenticationMethod	아니요	예
	AuthenticationStatus	아니요	아니요
	CTSDeviceID	아니요	아니요
	디바이스 IP 주소	예	예
	EapAuthentication(머신 사용자 인증 중에 사용되는 EAP 방법)	아니요	예
	EapTunnel(터널 설정에 사용되는 EAP 방법)	아니요	예
	프로토콜	예	예
	UseCase	예	예
	UserName	아니요	예
	WasMachineAuthenticated	아니요	아니요

사전	속성	허용되는 프로토콜 규칙 및 프록시	**ID** 규칙
인증서	공용 이름	아니요	예
	국가		
	이메일		
	LocationSubject		
	조직		
	조직 구성 단위		
	일련 번호		
	시/도		
	제목		
	주체 대체 이름		
	주체 대체 이름 - DNS		
	주체 대체 이름 - 이메일		
	주체 대체 이름 - 기타 이름		
	주체 일련 번호		
	발급자		
	발급자 - 공통 이름		
	발급자 - 조직		
	발급자 - 조직 구성 단위		
	발급자 - 위치		
	발급자 - 국가		
	발급자 - 이메일		
	발급자 - 일련 번호		
	발급자 - 시/도		
	발급자 - 거리 주소		
	발급자 - 도메인 구성 요소		

사전	속성	허용되는 프로토콜 규칙 및 프록시	**ID** 규칙
	발급자 - 사용자 ID		

시스템 정의 사전 및 사전 속성

Cisco ISE를 설치하는 동안에는 시스템 사전 페이지에서 확인할 수 있는 시스템 사전이 생성됩니다. 시스템 정의 사전 속성은 읽기 전용 속성입니다. 따라서 기존 시스템 정의 사전은 보기만 가능하며 시스템 사전에서 시스템 정의 값이나 속성을 생성, 편집 또는 삭제할 수는 없습니다.

시스템 정의 사전 속성은 속성을 설명하는 이름, 도메인이 이해할 수 있는 내부 이름 및 허용되는 값과 함께 표시됩니다.

Cisco ISE는 역시 시스템 정의 사전의 일부이며 IETF(Internet Engineering Task Force)에 의해 정의되는 IETF RADIUS 속성 집합에 대한 사전 기본값도 생성합니다. ID를 제외한 모든 무료 IETF RADIUS 속성 필드를 편집할 수 있습니다.

시스템 사전 및 사전 속성 표시

시스템 사전의 시스템 정의 속성은 생성, 편집 또는 삭제할 수 없습니다. 시스템 정의 속성은 보기만 가능합니다. 사전 이름과 설명을 기준으로 하는 빠른 검색을 수행하거나, 직접 정의하는 검색 규칙을 기준으로 하는 고급 검색을 수행할 수 있습니다.

단계 **1**

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**)** > **System(**시스템**)**.

단계 **3** 시스템 사전 페이지에서 시스템 사전을 선택하고 **View(**보기**)**를 클릭합니다.

단계 **4** **Dictionary Attributes(**사전 속성**)**를 클릭합니다.

단계 **5** 목록에서 시스템 사전 속성을 선택하고 **View(**보기**)**를 클릭합니다.

단계 **6** 시스템 사전 페이지로 돌아가려면 **Dictionaries(**사전**)** 링크를 클릭합니다.

사용자 맞춤화 사전 및 사전 속성

Cisco ISE에서는 사용자가 생성하는 사용자 맞춤화 사전이 사용자 사전(User Dictionary) 페이지에 표시됩니다. 생성하여 시스템에 저장한 기존 사용자 사전의 사전 이름 또는 사전 유형 값은 수정할 수 없습니다.

사용자 사전 페이지에서는 다음을 수행할 수 있습니다.

- 사용자 사전 편집 및 삭제
- 이름과 설명을 기반으로 사용자 사전 검색

- 사용자 사전의 사용자 맞춤화 사전 속성 추가, 편집 및 삭제
- NMAP 스캔 작업을 사용하여 NMAP 익스텐션 사전의 속성 삭제. NMAP Scan Actions(NMAP 스캔 작업) 페이지에서 맞춤형 포트를 추가하거나 삭제하면 해당하는 맞춤형 포트 속성이 사전에서 추가, 삭제 또는 업데이트됩니다.
- 사전 속성에 대해 허용되는 값 추가 또는 제거

사용자 맞춤화 사전 생성

사용자 맞춤화 사전을 생성, 편집 또는 삭제할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**)** > **User(**사용자**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 사용자 사전의 이름, 설명(선택 사항) 및 버전을 입력합니다.

단계 **4** 사전 속성 유형 드롭다운 목록에서 속성 유형을 선택합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

사용자 맞춤화 사전 속성 생성

사용자 사전에서 사용자 맞춤화 사전 속성을 추가, 편집 및 삭제할 수 있으며 사전 속성에 대해 허용되는 값을 추가하거나 제거할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**)** > **User(**사용자**)**.

단계 **2** 사용자 사전 페이지에서 사용자 사전을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Dictionary Attributes(**사전 속성**)**를 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** 사전 속성의 이름, 설명(선택 사항) 및 사전 속성의 내부 이름을 입력합니다.

단계 **6** 데이터 유형 드롭다운 리스트에서 데이터 유형을 선택합니다.

단계 **7** **Add(**추가**)**를 클릭하여 허용되는 값 표에서 이름과 허용되는 값을 구성하고 기본 상태를 설정합니다.

단계 **8** **Submit(**제출**)**을 클릭합니다.

RADIUS 벤더 사전

Cisco ISE에서는 RADIUS 벤더 사전 집합과 각 사전에 대한 속성 집합을 정의할 수 있습니다. 목록의 각 벤더 정의에는 벤더 이름, 벤더 ID 및 간단한 설명이 포함됩니다.

Cisco ISE는 다음 RADIUS 벤더 사전을 기본적으로 제공합니다.

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

RADIUS 프로토콜은 이러한 벤더 사전 및 권한 부여 프로파일과 정책 조건에서 사용 가능한 벤더별 속성을 지원합니다.

RADIUS 벤더 사전 생성

RADIUS 벤더 사전 생성/편집/삭제/내보내기/가져오기를 수행할 수도 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**)** > **System(**시스템**)** > **Radius** > **Radius Vendors(Radius** 벤더**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** RADIUS 벤더 사전의 이름, 설명(선택 사항) 및 RADIUS 벤더용으로 IANA(Internet Assigned Numbers Authority)에서 승인한 벤더 ID를 입력합니다.

단계 **4** 속성 값에서 가져온 바이트 수를 선택하여 벤더 속성 유형 필드 길이 드롭다운 목록에서 속성 유형을 지정합니다. 유효한 값은 1, 2, 4입니다. 기본값은 1입니다.

단계 **5** 속성 값에서 가져온 바이트 수를 선택하여 벤더 속성 크기 필드 길이 드롭다운 목록에서 속성 길이를 지정합니다. 유효한 값은 0과 1입니다. 기본값은 1입니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

RADIUS 벤더 사전 속성 생성

Cisco ISE가 지원하는 RADIUS 벤더 속성을 생성, 편집 및 삭제할 수 있습니다. 각 RADIUS 벤더 속성에는 이름, 데이터 유형, 설명 및 방향이 포함되어 있습니다. 속성의 방향은 해당 속성과 관련이 있는 항목(요청, 응답 또는 둘 다)을 지정합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**)** > **System(**시스템**)** > **Radius** > **Radius Vendors(Radius** 벤더**)** 를 선택합니다**.**

단계 **2** RADIUS 벤더 사전 목록에서 원하는 RADIUS 벤더 사전을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Dictionary Attributes(**사전 속성**)**, **Add(**추가**)**를 차례로 클릭합니다.

단계 **4** RADIUS 벤더 속성의 속성 이름과 설명(선택 사항)을 입력합니다.

단계 **5** 데이터 유형 드롭다운 목록에서 데이터 유형을 선택합니다.

단계 **6** **Enable MAC option(MAC** 옵션 활성화**)** 확인란을 선택합니다.

단계 **7** 방향 드롭다운 목록에서 RADIUS 요청에만 적용되는 방향, RADIUS 응답에만 적용되는 방향 또는 둘 다에 적용되는 방향을 선택합니다.

단계 **8** ID 필드에 벤더 속성을 입력합니다.

단계 **9** **Allow Tagging(**태그 지정 허용**)** 확인란을 선택합니다.

단계 **10** **Allow multiple instances of this attribute in a profile(**프로파일에서 이 속성의 여러 인스턴스 허용**)** 확인란을 선택합니다.

단계 **11** **Add(**추가**)**를 클릭하여 벤더 속성에 대해 허용되는 값을 허용되는 값 표에 추가합니다.

단계 **12** **Submit(**제출**)**을 클릭합니다.

HP RADIUS IETF 서비스 유형 속성

Cisco ISE에는 RADIUS IETF 서비스 유형 속성에 대해 새로운 값 두 개가 도입되었습니다. RADIUS IETF 서비스 유형 속성은 **Policy(**정책**) > Policy Elements(**정책 요소**) > Dictionaries(**사전**) > System(**시스템**) > RADIUS > IETF**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(IETF** 정책**) > Policy Elements(**정책 요소**) > Dictionaries(**사전**) > System(**시스템**) > RADIUS > IETF**에서 사용 가능합니다. 정책 조건에서 이러한 두 개의 값을 사용할 수 있습니다. 이 두 개의 값은 사용자 권한을 파악할 수 있도록 HP 디바이스용으로 특별히 설계된 것입니다.

열거 이름	열거 값
HP-Oper	252
HP-User	255

RADIUS 벤더 사전 속성 설정

이 섹션에서는 Cisco ISE에 사용되는 RADIUS 벤더 사전에 대해 설명합니다.

다음 표에서는 RADIUS 벤더에 대한 사전 속성을 구성할 수 있는 RADIUS 벤더용 Dictionary(사전) 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**)** > **System(**시스템**)** > **RADIUS** > **RADIUS Vendors(RADIUS** 벤더**)**입니다.

표 ***128: RADIUS*** 벤더 사전 속성 설정

필드 이름	사용 지침
Attribute Name(속성 이름**)**	선택한 RADIUS 벤더에 대한 벤더별 속성 이름을 입력합니다.
Description(설명**)**	벤더별 속성에 대한 선택적 설명을 입력합니다.
Internal Name(내부 이름**)**	데이터베이스 내부적으로 가리키는 벤더별 속성의 이름을 입력합니다.

필드 이름	사용 지침
Data Type(데이터 유형**)**	벤더별 속성에 대해 다음 데이터 유형 중 하나를 선택합니다. • STRING • OCTET_STRING • UNIT32 • UNIT64 • IPV4 • IPV6
Enable MAC option(MAC 옵션 활성화**)**	RADIUS 속성을 MAC 주소로 비교하려면 이 확인란을 선택합니다. 기본적으로, RADIUS 속성 calling-station-id의 경우 이 옵션은 활성화 상태로 표시되며 비활성화할 수 없습니다. RADIUS 벤더 사전 내의 다른 사전 속성(문자열 유형)의 경우 이 옵션을 활성화하거나 비활성화할 수 있습니다. 이 옵션을 활성화하면, 인증 및 권한 부여 조건을 설정하는 동안 텍스트 옵션을 선택하여 일반 문자열을 비교할지, 아니면 MAC 주소 옵션을 선택하여 MAC 주소를 비교할지 정의할 수 있습니다.
Direction(방향**)**	RADIUS 메시지에 적용되는 옵션 중 하나를 선택합니다.
ID	벤더 속성 ID를 입력합니다. 유효 범위는 0~255입니다.
Allow Tagging(태그 지정 허용**)**	RFC2868에 정의된 대로 속성의 태그 포함이 허용되는 것으로 표시하려면 이 확인란을 선택합니다. 태그는 터널링된 사용자에 대한 속성 그룹화를 허용하기 위한 것입니다. 자세한 내용은 RFC2868을 참고하십시오. 태그가 지정된 속성 지원은 지정된 터널과 관련된 모든 속성이 각 태그 필드에서 동일한 값을 포함하도록 보장하며, 각 집합에는 Tunnel-Preference 속성의 적절한 값이 지정된 인스턴스가 포함됩니다. 이 지원은 멀티벤더 네트워크 환경에서 사용할 터널 속성을 준수하므로 각기 다른 벤더에서 제조한 NAS(Network Access Server) 간의 상호운용성 문제가 발생하지 않습니다.

필드 이름	사용 지침
Allow Multiple Instances of this Attribute in a Profile(프로파일에서 이 속성의 여러 인스턴스 허용**)**	프로파일에서 이 RADIUS 벤더별 속성 인스턴스를 여러 개 사용하려면 이 확인란을 선택합니다.

관련 항목

시스템 정의 사전 및 사전 속성, 932 페이지
사용자 맞춤화 사전 및 사전 속성, 932 페이지
RADIUS 벤더 사전, 933 페이지
RADIUS 벤더 사전 생성, 934 페이지

Condition Studio 탐색

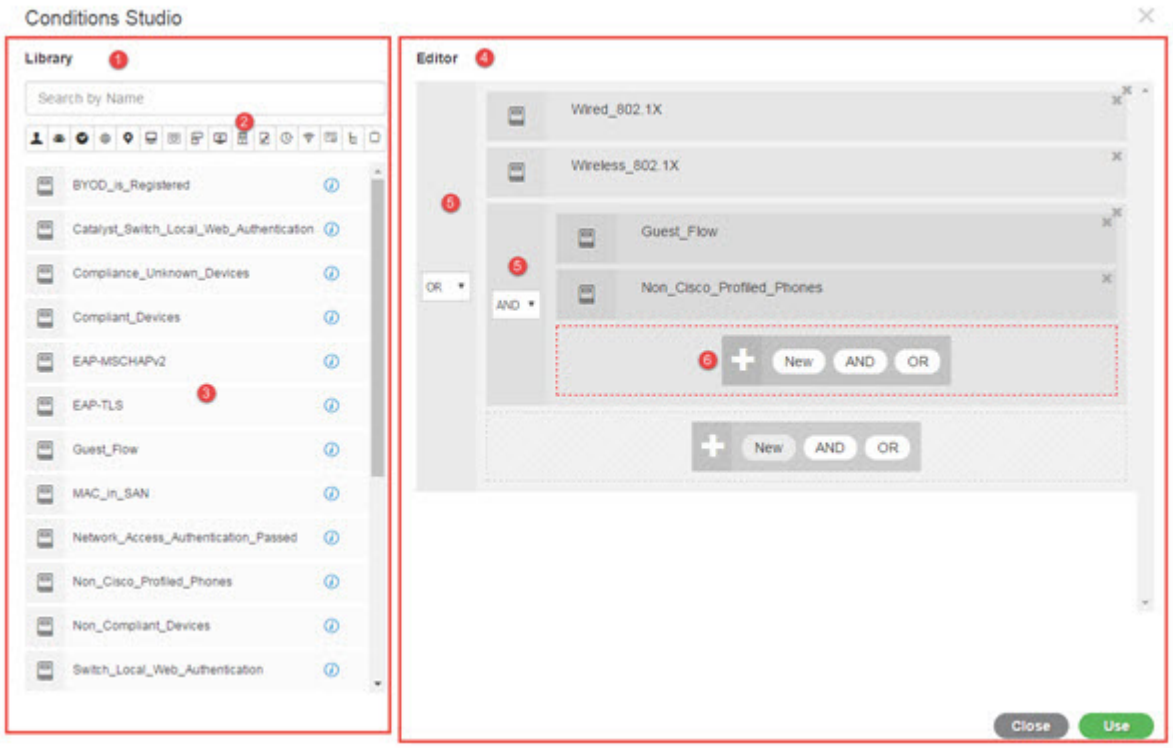
Conditions Studio를 사용하여 조건을 생성, 관리 및 재사용합니다. 조건은 둘 이상의 규칙을 포함할 수 있으며, 하나의 레벨만 포함하거나 여러 계층 레벨을 포함하는 다양한 수준의 복잡성으로 구축할 수 있습니다. Conditions Studio를 사용하여 새 조건을 생성할 경우, 이미 라이브러리에 저장한 조건 블록을 사용할 수 있으며 저장된 조건 블록을 업데이트하고 변경할 수도 있습니다. 나중에 조건을 생성 및 관리하는 동안 빠른 카테고리 필터 등을 사용하여 필요한 블록 및 속성을 쉽게 찾을 수 있습니다.

네트워크 액세스 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Policy Sets(**정책 집합**)**를 선택합니다. 디바이스 관리 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리자 정책 집합**)**를 선택합니다.

정책 집합의 특정 규칙에 이미 적용된 조건을 편집하거나 변경하려면 **Conditions(**조건**)** 열의 셀 위에 마우스를 올려 놓고  를 클릭하거나 정책 집합 표의 **Conditions(**조건**)** 열에서 ✚를 클릭하여 새로운 조건을 생성합니다. 이 새로운 조건을 동일한 정책 집합에 즉시 적용 할 수도 있고 나중에 사용하기 위해 라이브러리에 저장할 수도 있습니다.

다음 그림에는 Conditions Studio의 기본 요소가 나와 있습니다.

그림 *41: Condition Studio*



Condition Studio는 라이브러리와 편집기라는 두 가지 주요 부분으로 나뉩니다. 라이브러리는 재사용을 위해 조건 블록을 저장하는 반면 편집기에서는 저장된 블록을 편집하고 새로 생성할 수 있습니다.

다음 표에서는 Conditions Studio의 여러 부분에 대해 설명합니다.

필드	사용 지침
라이브러리	재사용을 위해 ISE 데이터베이스에서 생성되고 저장된 모든 조건 블록의 목록을 표시합니다. 이러한 조건 블록을 현재 편집된 조건의 일부로 사용하려면 라이브러리에서 편집기의 관련 레벨로 끌어다 놓은 다음 필요에 따라 연산자를 업데이트합니다. 조건이 둘 이상의 범주와 연결될 수 있으므로 라이브러리에 저장된 조건은 모두 라이브러리 아이콘  으로 표시됩니다. 라이브러리의 각 조건 옆에는 i 아이콘도 있습니다. 이 아이콘 위에 마우스를 올려 놓으면 조건의 전체 설명을 볼 수 있으며, 해당 조건이 연결된 범주를 볼 수 있으며, 라이브러리에서 조건을 완전히 삭제할 수 있습니다. 정책에서 사용되는 조건은 삭제할 수 없습니다. 라이브러리 조건을 편집기에 끌어다 놓은 다음 그 자체로 현재 편집중인 정책에 사용할 수도 있고 아니면 현재 정책에 사용하기 위한 더 복잡한 조건의 구성 요소로 사용할 수도 있으며 아니면 라이브러리에 새 조건으로 저장할 수도 있습니다. 편집기에 조건을 끌어 놓은 다음 해당 조건을 변경하고 라이브러리에 동일한 이름 또는 새 이름으로 저장할 수도 있습니다. 설치 시 사전 정의된 조건도 있습니다. 이러한 조건도 변경 및 삭제할 수 있습니다.
검색 및 필터	이름으로 조건을 검색하거나 범주별로 필터링합니다. 유사한 방식으로 편집기의 **Add to add an attribute(**속성을 클릭하여 추가**)** 필드에서 속성을 검색하고 필터링할 수도 있습니다. 툴바의 아이콘은 제목, 주소 등의 다양한 속성 범주를 나타냅니다. 아이콘을 클릭하여 특정 범주와 관련된 속성을 보고, 범주 도구 모음에서 강조 표시된 아이콘을 클릭하여 선택을 취소하여 필터를 제거합니다.
Conditions(조건) 목록	라이브러리에 있는 모든 조건의 전체 목록 또는 검색 또는 필터 결과를 기반으로 한 라이브러리의 조건 목록입니다.

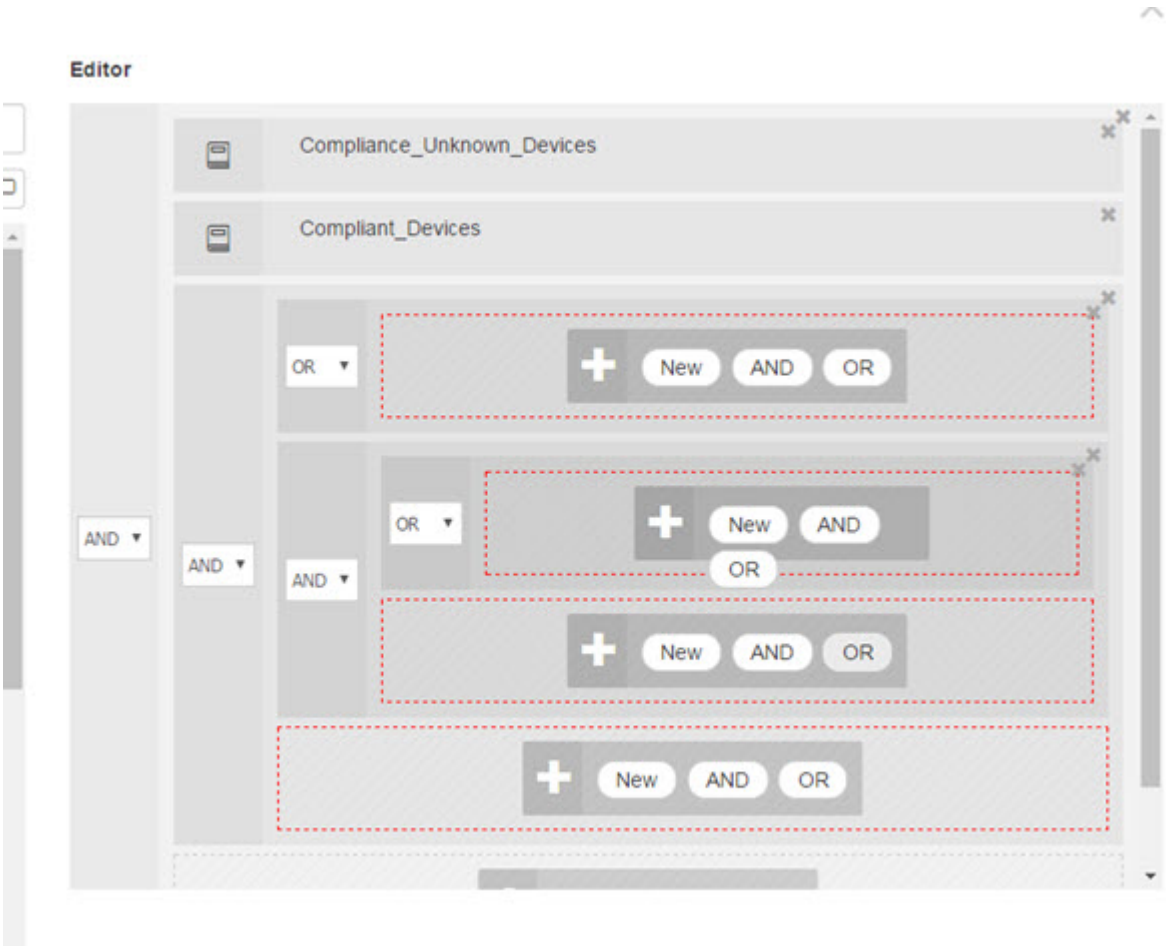
필드	사용 지침
편집기	즉시 사용할 수 있도록 새 조건을 생성하고 나중에 사용할 수 있도록 시스템 라이브러리에 저장하고, 기존 조건을 편집하여 즉시 및 향후 사용을 위해 라이브러리에 변경 사항을 저장합니다. 새 조건을 생성하기 위해 Conditions Studio를 열면 (정책 집합 표에서 더하기 기호 클릭), 첫 번째 규칙을 추가할 수 있는 빈 줄 하나만 편집기에 나타납니다. 필드가 비어 있는 편집기가 열리면 연산자 아이콘이 표시되지 않습니다.
	편집기는 다양한 가상 열과 행으로 나뉩니다. 열은 서로 다른 계층 레벨을 나타내며 각 열은 계층 구조에서의 위치에 따라 들여 쓰기됩니다. 행은 개별 규칙을 나타냅니다. 레벨 당 하나 또는 여러 개의 규칙을 생성할 수 있으며 여러 레벨을 포함할 수 있습니다. 위 이미지의 예는 작성 또는 편집되는 과정에 있는 조건을 표시하며 규칙의 계층 구조를 포함합니다. 여기서 그림의 첫 번째 레벨과 두 번째 레벨은 모두 숫자 5로 표시됩니다. 최상위 레벨의 규칙은 연산자 OR을 사용합니다. 연산자를 선택하고 계층 레벨을 만든 후에 연산자를 변경하려면 이 열에 표시되는 드롭 다운 목록에서 관련 옵션을 선택하면 됩니다. 연산자 드롭 다운 목록 외에 각 규칙에는이 열에 해당 아이콘이 있으며 이는 해당 규칙이 속하는 범주를 나타냅니다. 아이콘 위에 마우스를 올려 놓으면 툴팁에 카테고리 이름이 표시됩니다. 라이브러리에 저장하면 모든 조건 블록에 Library (라이브러리) 아이콘이 할당되고 Editor (편집기)에 표시된 범주 아이콘이 대체됩니다. 마지막으로, 규칙이 일치하는 모든 관련 항목을 제외하도록 구성된 경우 Is-Not(불일치) 표시기가 열에 나타납니다. 예를 들어, 값이 London인 위치 속성이 Is-Not(불일치)으로 설정된 경우 London의 모든 디바이스에 대한 액세스가 거부됩니다.

필드	사용 지침
	이 영역에는 조건 내에서 계층 레벨은 물론 복수의 규칙에 따라 사용 가능한 옵션이 표시됩니다. 열 또는 행 위에 마우스를 올려 놓으면 관련 작업이 나타납니다. 작업을 선택하면 해당 섹션 및 모든 하위 섹션에 적용됩니다. 예를 들어 계층 A에 5개 레벨이 있을 경우 세 번째 레벨의 규칙에서 AND를 선택하면 원래 규칙 아래에 새 계층 B가 생성되어 원래 규칙이 계층 B의 상위 규칙이 되며 계층 B는 계층 A에 속하게 됩니다. 새 조건을 새롭게 생성하기 위해 우선 Condition Studio를 열면 Editor(편집기) 영역에는 사용자가 구성할 수 있는 한 개 규칙을 위한 한 줄 그리고 관련 연산자를 선택하거나 라이브러리에서 관련 조건을 끌어다 놓기 위한 옵션이 포함됩니다. **AND** 및 **OR** 연산자 옵션을 사용하여 조건에 레벨을 추가할 수 있습니다. 옵션을 클릭한 레벨과 같은 레벨에서 새 규칙을 생성하려면 **New(**새로 만들기**)**를 선택합니다. **New(**새로 만들기**)** 옵션은 계층 구조의 최상위 레벨에서 하나 이상의 규칙을 구성한 경우에만 나타납니다.

정책 조건 구성, 편집 및 관리

Conditions Studio를 사용하여 조건을 생성, 관리 및 재사용합니다. 조건은 둘 이상의 규칙을 포함할 수 있으며, 하나의 레벨만 포함하거나 여러 계층 레벨을 포함하는 다양한 수준의 복잡성으로 구축할 수 있습니다. 다음 이미지와 같이 Conditions Studio의 편집기 측에서 조건 계층 구조를 관리합니다.

그림 *42:* 편집기—조건 계층 구조



새 조건을 생성할 경우, 이미 라이브러리에 저장한 조건 블록을 사용할 수 있으며 저장된 조건 블록을 업데이트하고 변경할 수도 있습니다. 조건을 생성 및 관리하는 동안 빠른 범주 필터 등을 사용하여 필요한 블록 및 속성을 쉽게 찾을 수 있습니다.

조건 규칙을 생성하고 관리할 때는 속성, 연산자 및 값을 사용합니다.

Cisco ISE에는 가장 일반적인 활용 사례 중 일부에 대해 사전 정의된 조건 블록이 포함되어 있습니다. 이러한 사전 정의된 조건을 요건에 맞게 편집할 수 있습니다. 즉시 사용 가능한 블록을 포함하여 재사용을 위해 저장된 조건은이 작업에 설명 된대로 Condition Studio의 라이브러리에 저장됩니다.

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

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

단계 **2** Conditions Studio에 액세스하여 새 조건을 생성하고 기존 조건 블록을 편집합니다. 그런 다음, 특정 정책 집합(및 그 관련 정책과 규칙)에 대해 구성하는 규칙의 일부로서 이러한 조건을 사용하거나 향후 사용을 위한 라이브러리에 저장하려면 다음을 따릅니다.

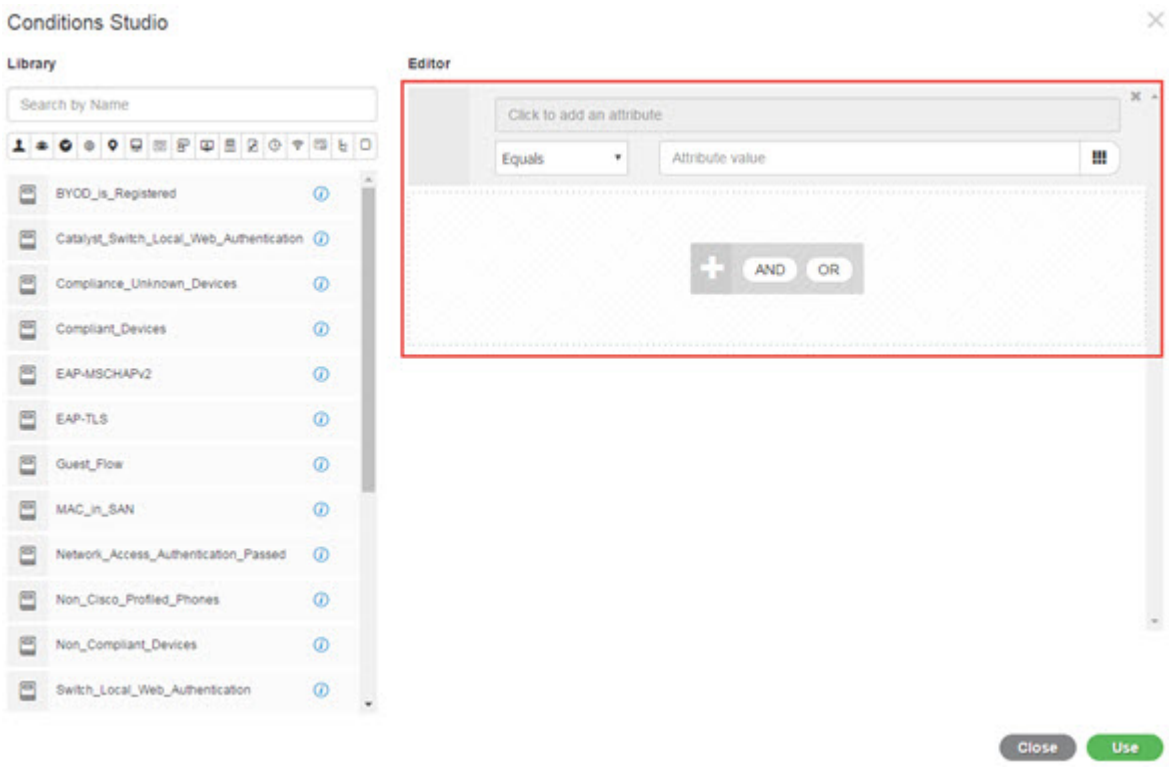
a) 기본 정책 집합 페이지의 정책 집합 표에서 **Conditions(조건)** 열의 ✚ 버튼을 클릭하여 전체 정책 집합과 관련된 조건(인증 정책 규칙의 일치 전에 확인되는 조건)을 생성합니다.

b) 또는 특정 정책 집합 행에서 › 버튼을 클릭하여 인증 및 권한 부여에 대한 모든 규칙을 포함하는 집합 보기를 볼 수 있습니다. 집합 보기에서 규칙 표의 **Conditions(조건)** 열에 있는 셀 위에 마우스를 올리고 ✚ 버튼을 클릭하여 Conditions Studio를 엽니다.

c) 정책 집합에 이미 적용된 조건을 수정하는 경우 편집 버튼을 클릭하여 Conditions Studio에 액세스합니다.

Condition Studio가 열립니다. 새 조건을 생성하기 위해 연 경우 다음 이미지와 같이 나타납니다. 정책 집합에 이미 적용된 조건을 편집하기 위해 필드를 열었을 때 필드에 대한 설명과 Conditions Studio의 예를 보려면 Condition Studio 탐색, 937 페이지을 참조하십시오.

그림 ***43: Conditions Studio***—새 조건 생성



단계 **3** 생성 또는 편집 중인 조건의 규칙으로 라이브러리의 기존 조건 블록을 사용합니다.

a) 범주 툴바에서 관련 범주를 선택하여 필터링합니다. 라이브러리에서는 선택한 범주의 속성을 포함하는 모든 블록이 표시됩니다. 둘 이상의 규칙을 포함하지만 그러한 규칙 중 하나 이상에 대해 선택한 범주의 속성을 사용하는 조건 블록도 표시됩니다. 필터가 더 추가된 경우, 특정 필터의 조건 블록 중 특정 필터 이외의 포함된 기타 필터와도 일치하는 조건 블록만 표시 결과에 포함됩니다. 예를 들어 툴바에서 Ports(포트) 범주를 선택하고 **Search by Name(**이름으로 검색**)** 필드에 "auth"를 자유 텍스트로 입력하면 이름에 "auth"가 있는 포트와 관련된 모든 블록이 표시됩니다. 범주 툴바에서 강조 표시된 아이콘을 다시 클릭하여 선택을 취소하면 해당 필터가 제거됩니다.

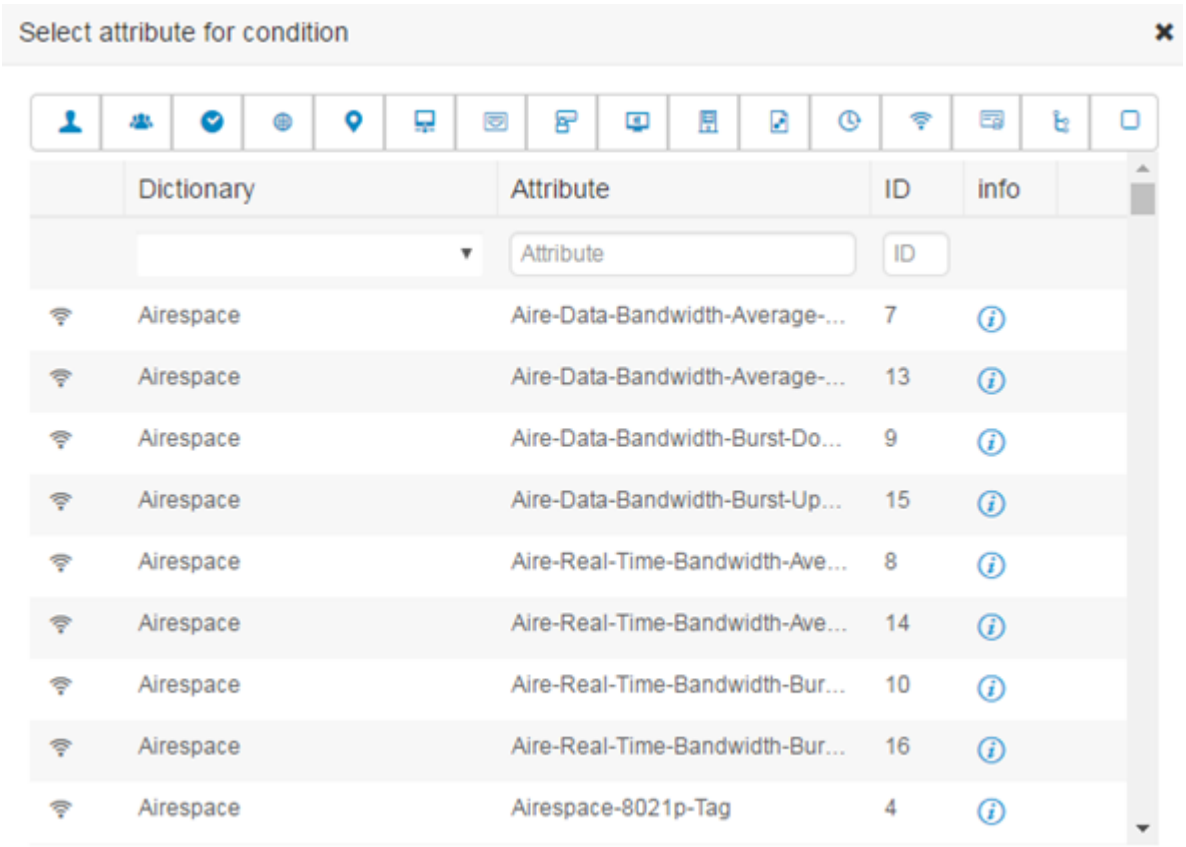
b) 자유 텍스트로 조건 블록을 검색합니다. 검색하려는 블록의 이름에 표시되는 단어 중 아무 것이든 또는 일부를 **Search by Name(**이름으로 검색**)** 자유 텍스트 필드에 입력합니다. 입력하는 동안 시스템은 실시간으로 관련 결과를 동적으로 검색합니다. 범주를 선택하지 않으면(강조 표시된 아이콘 없음) 모든 범주의 조건 블록이 결과에 포함됩니다. 범주 아이콘이 이미 선택된 경우(표시된 목록이 이미 필터링됨)에는 특정 텍스트를 사용하는 특정 범주의 블록만 표시 결과에 포함됩니다.

c) 조건 블록을 찾고 나면 편집기로 끌어서 현재 작성 중인 블록의 올바른 레벨에 놓습니다. 잘못된 위치에 놓은 경우 편집기 내에서 올바른 위치에 놓을 때까지 다시 끌어다 놓을 수 있습니다.

d) 편집기에서 블록 위에 마우스를 올리고 **Edit(**편집**)**를 클릭해 규칙을 변경하여, 현재 작업 중인 조건과 관련된 변경 사항을 적용하거나 라이브러리의 규칙을 이러한 변경 사항으로 덮어쓰거나 라이브러리에 규칙을 새 블록으로 저장할 수 있습니다.
읽기 전용인 블록은 편집기에 놓이고 나면 편집이 가능해지며 편집기의 다른 모든 사용자 맞춤화 규칙과 동일한 필드, 구조, 목록 및 작업을 갖습니다. 이 규칙을 편집하는 것과 관련하여 자세한 내용을 보려면 다음 단계를 계속 진행합니다.

단계 **4** 동일한 레벨에 새 규칙을 추가하려면 현재 레벨에 **AND(**그리고**)**, **OR(**또는**)** 또는 **Set to 'Is not'('**아님'으로 설정**)** 연산자를 선택하여 추가합니다. **Set to 'Is not'('**아님'으로 설정**)**은 개별 규칙에도 적용할 수 있습니다.

단계 **5** 속성 사전을 사용하여 규칙을 생성 및 수정합니다. **Click to add an attribute(**클릭해서 속성 추가**)** 필드를 클릭합니다. 다음 이미지와 같이 속성 선택기가 열립니다.



속성 선택기의 일부가 다음 표에 설명되어 있습니다.

필드	사용 지침
속성 카테고리 툴바	다양한 속성 범주 각각에 대한 고유한 아이콘을 포함합니다. 범주별로 보기를 필터링하려면 속성 범주 아이콘을 선택합니다. 강조 표시된 아이콘을 클릭하여 선택을 취소하면 필터가 제거됩니다.
사전	속성이 저장된 사전의 이름을 나타냅니다. 벤더 사전별로 속성을 필터링하려면 드롭다운에서 특정 사전을 선택합니다.
속성	속성의 이름을 나타냅니다. 사용 가능한 필드에 속성 이름에 대한 자유 텍스트를 입력하여 속성을 필터링합니다. 입력하는 동안 시스템은 실시간으로 관련 결과를 동적으로 검색합니다.
ID	고유한 속성 식별 번호를 나타냅니다. 사용 가능한 필드에 ID 번호를 입력하여 속성을 필터링합니다. 입력하는 동안 시스템은 실시간으로 관련 결과를 동적으로 검색합니다.
정보	관련 속성 행의 정보 아이콘에 마우스를 올리면 속성에 대한 추가 세부정보를 볼 수 있습니다.

a) 속성 선택기 검색에서 필요한 속성을 필터링하고 검색합니다. 속성 선택기의 아무 부분의 자유 텍스트를 필터링하거나 입력할 때, 활성화된 다른 필터가 없으면 선택한 필터에만 관련된 모든 속성이 결과에 포함됩니다. 둘 이상의 필터를 사용하는 경우에는 표시되는 검색 결과가 모든 필터와 일치합니다. 예를 들어 툴바에서 포트 아이콘을 클릭하고 Attribute(속성) 열에 "auth"를 입력하면 이름에 "auth"가 있는 포트 범주의 속성만 표시됩니다. 범주를 선택하면 툴바의 아이콘이 파란색으로 강조 표시되고 필터링된 목록이 표시됩니다. 범주 툴바에서 강조 표시된 아이콘을 다시 클릭하여 선택을 취소하면 필터가 제거됩니다.

b) 관련 속성을 규칙에 추가하려면 해당 속성을 선택합니다.
속성 선택기가 닫히고 선택한 속성이 **Click to add an attribute(**클릭해서 속성 추가**)** 필드에 추가됩니다.

c) **Equals(**같음**)** 드롭다운 목록에서 관련 연산자를 선택합니다.

선택하는 모든 속성에 "Equals(같음)", "Not Equals(같지 않음)", "Matches(일치함)", "Starts With(다음으로 시작)" 또는 "Not Starts With(다음으로 시작 안 함)" 연산자 옵션이 포함되는 것은 아닙니다.

"Matches(일치함)" 연산자는 와일드카드가 아닌 정규식(REGEX)을 지원하며 사용합니다.

직접 비교하려면 "같음" 연산자를 사용해야 합니다. 다중 값 속성에 "Contains(포함)" 연산자를 사용할 수 있습니다. 정규식 비교에는 "일치함" 연산자를 사용해야 합니다. "일치함" 연산자를 사용하면 정적 값과 동적 값 모두에 대해 정규식이 해석됩니다.

d) **Attribute value(**속성 값**)** 필드에서 다음 중 하나를 수행합니다.

- 필드에 자유 텍스트 값을 입력합니다.
- 목록에서 동적으로 로드되는 값을 선택합니다(관련 있는 경우 이전 단계에서 선택한 속성에 따라 다름).

- 다른 속성을 조건 규칙의 값으로 사용합니다. 이 경우 필드 옆에 있는 표 아이콘을 선택하여 속성 선택기를 연 다음 관련 속성을 검색, 필터링 및 선택합니다. 속성 선택기가 닫히고 선택한 속성이 **Attribute value(**속성 값**)** 필드에 추가됩니다.

단계 **6** 라이브러리의 규칙을 조건 블록으로 저장합니다.

a) 라이브러리에서 블록으로 저장하려는 규칙 또는 계층 구조 위에 마우스를 올립니다. 단일 조건 블록으로 저장할 수 있는 규칙 또는 규칙 그룹에 대해 **Duplicate(**복제**)** 및 **Save(**저장**)** 버튼이 나타납니다. 규칙 그룹을 블록으로 저장하려면 전체 계층 구조의 차단된 영역에서 전체 계층 구조의 맨 아래에 있는 작업 버튼을 선택합니다.

b) **Save(**저장**)**를 클릭합니다. 조건 저장 화면이 나타납니다.

c) 선택:

- Save to Existing Library Condition(기존 라이브러리 조건에 저장)—생성한 새 규칙으로 라이브러리의 기존 조건 블록을 덮어쓰려면 이 옵션을 선택한 다음 **Select from list(**목록에서 선택**)** 드롭다운 목록에서 덮어쓰려는 조건 블록을 선택합니다.
- Save as a new Library Condition(새 라이브러리 조건으로 저장)—블록의 Condition Name(조건 이름) 필드에 고유한 이름을 입력합니다.

d) 또는, **Description(**설명**)** 필드에 설명을 입력합니다. 이 설명은 라이브러리 내의 아무 조건 블록에 대한 정보 아이콘 위에 마우스를 올리면 표시되며, 이를 통해 다양한 조건 블록 및 해당 용도를 빠르게 식별할 수 있습니다.

e) **Save(**저장**)**를 클릭하여 조건 블록을 라이브러리에 저장합니다.

단계 **7** 새 하위 레벨에서 새 규칙을 생성하려면 **AND(**그리고**)** 또는 **OR(**또는**)**을 클릭하여 기존 상위 계층 구조와 현재 생성 중인 하위 계층 구조 간에 올바른 연산자를 적용합니다. 연산자를 선택한 출처 규칙 또는 계층 구조의 하위 항목으로, 선택한 연산자가 포함된 새 섹션이 편집기 계층 구조에 추가됩니다.

단계 **8** 현재 기존 레벨에서 새 규칙을 생성하려면 관련 레벨에서 **New(**새로 만들기**)**를 클릭합니다. 시작 레벨과 같은 레벨에 새 규칙에 대한 새 빈 행이 나타납니다.

단계 **9** 편집기 및 모든 하위 항목에서 조건을 제거하려면 **X**를 클릭합니다.

단계 **10** 계층 구조 내에서 특정 조건을 자동으로 복사하고 붙여 넣어 동일한 레벨에서 동일한 하위 항목을 추가로 생성하려면 **Duplicate(**복제**)**를 클릭합니다. **Duplicate(**복제**)** 버튼을 클릭하는 출처 레벨에 따라 하위 항목이 있거나 없는 개별 규칙을 복제할 수 있습니다.

단계 **11** 페이지 하단에서 **Use(**사용**)**를 클릭하여, 편집기에서 생성한 조건을 저장하고 이 조건을 정책 집합에 구현합니다.

특수 네트워크 액세스 조건

이 섹션에서는 정책 집합을 생성할 때 유용할 수 있는 고유한 조건에 대해 설명합니다. 이러한 조건은 Conditions Studio에서 생성할 수 없으므로 고유한 자체 프로세스가 있습니다.

디바이스 네트워크 조건 구성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**) > Policy Elements(**정책 요소**) > Conditions(**조건**) > Network Conditions(**네트워크 조건**) > Device Network Conditions(**디바이스 네트워크 조건**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 네트워크 조건의 이름과 설명을 입력합니다.

단계 **4** 다음 세부정보를 입력합니다.

- IP 주소 - IP 주소 또는 서브넷 목록을 라인당 하나씩 추가할 수 있습니다. IP 주소/서브넷은 IPv4 또는 IPv6 형식일 수 있습니다.
- Device Name(디바이스 이름)-디바이스 이름 목록을 한 줄에 하나씩 추가 할 수 있습니다. 네트워크 디바이스 개체에 구성된 것과 동일한 디바이스 이름을 입력해야 합니다.
- Device Groups(디바이스 그룹) - 루트 NDG, 쉼표, NDG(루트 아래에 있음) 순서로 튜플 목록을 추가합니다. 줄당 튜플(tuple)이 하나씩 있어야 합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

디바이스 포트 네트워크 조건 구성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**) > Policy Elements(**정책 요소**) > Conditions(**조건**) > Network Conditions(**네트워크 조건**) > Device Port Network Conditions(**디바이스 포트 네트워크 조건**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 네트워크 조건의 이름과 설명을 입력합니다.

단계 **4** 다음 세부정보를 입력합니다.

- IP Addresses(IP 주소) - IP 주소 또는 서브넷, 쉼표, 디바이스에서 사용되는 포트 순서로 세부정보를 입력합니다. 줄당 튜플(tuple)이 하나씩 있어야 합니다.
- Devices(디바이스) - 디바이스 이름, 쉼표, 포트 순서로 세부정보를 입력합니다. 줄당 튜플(tuple)이 하나씩 있어야 합니다. 네트워크 디바이스 개체에 구성된 것과 동일한 디바이스 이름을 입력해야 합니다.
- Device Groups(디바이스 그룹) - 루트 NDG, 쉼표, NDG(루트 아래에 있음), 포트 순서로 세부정보를 입력합니다. 줄당 튜플(tuple)이 하나씩 있어야 합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

엔드스테이션 네트워크 조건 구성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**) > Policy Elements(**정책 요소**) > Conditions(**조건**) > Network Conditions(**네트워크 조건**) > Endstation Network Conditions(**엔드 스테이션 네트워크 조건**)**

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 네트워크 조건의 이름과 설명을 입력합니다.

단계 **4** 다음 세부정보를 입력합니다.

- IP 주소 - IP 주소 또는 서브넷 목록을 라인당 하나씩 추가할 수 있습니다. IP 주소/서브넷은 IPv4 또는 IPv6 형식일 수 있습니다.
- MAC 주소 - 엔드스테이션 MAC 주소 및 대상 MAC 주소 목록을 쉼표로 구분하여 입력할 수 있습니다. 각 MAC 주소는 12자리 16진수를 포함해야 하며, nn:nn:nn:nn:nn:nn, nn-nn-nn-nn-nn-nn, nnnn.nnnn.nnnn, nnnnnnnnnnnn 형식 중 하나여야 합니다.

  엔드스테이션 MAC 또는 대상 MAC이 필요하지 않은 경우에는 토큰 "-ANY-"를 대신 사용합니다.
- CLI/DNIS - 발신자 ID(CLI) 및 발신된 ID(DNIS) 목록을 쉼표로 구분하여 추가할 수 있습니다. 발신자 ID(CLI) 또는 발신된 ID(DNIS)가 필요하지 않은 경우에는 토큰 "-ANY-"를 대신 사용하십시오.

단계 **5** **Submit(**제출**)**을 클릭합니다.

시간 및 날짜 조건 생성

정책 요소 조건 페이지에서는 시간 및 날짜 정책 요소 조건을 표시, 생성, 수정, 삭제, 복제 및 검색할 수 있습니다. 정책 요소는 관리자가 구성한 특정 시간 및 날짜 속성 설정을 기반으로 조건을 정의하는 공유 객체입니다.

시간 및 날짜 조건을 사용하면 Cisco ISE 시스템 리소스에 대한 액세스 권한을 설정하거나 속성 설정에 지정된 특정 날짜 및 시간으로 제한할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**) > Policy Elements(**정책 요소**) > Conditions(**조건**) > Common(**공통**) > Time and Date(**시간 및 날짜**) > Add(**추가**)**

단계 **2** 필드에 해당하는 값을 입력합니다.

- 표준 설정 영역에서 액세스 권한을 제공할 시간과 날짜를 지정합니다.
- 예외 영역에서 액세스 권한을 제한할 시간 및 날짜 범위를 지정합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

권한 부여 정책의 **IPv6** 조건 속성 사용

Cisco ISE는 엔드포인트에서 IPv6 트래픽을 탐지, 관리 및 보호할 수 있습니다.

IPv6가 활성화된 엔드포인트는 Cisco ISE 네트워크에 연결할 때 IPv6 네트워크를 통해 NAD(Network Access Device)와 통신합니다. NAD는 IPv6 값을 비롯한 엔드포인트의 계정 관리 및 프로파일링 정보를 IPv4 네트워크를 통해 Cisco ISE에 전달합니다. 규칙 조건에서 IPv6 속성을 사용하여 Cisco ISE에서 권한 부여 프로파일과 정책을 구성하여 IPv6가 활성화된 엔드포인트의 해당 요청을 처리하고 엔드포인트의 규정 준수를 보장할 수 있습니다.

IPv6 접두사 및 IPv6 인터페이스 값에 와일드카드 문자가 지원됩니다. 예를 들면 2001:db8:1234::/48과 같습니다.

지원하는 IPv6 주소 형식은 다음과 같습니다.

- 전체 표기법: 콜론으로 구분되는 16진수 4자리로 구성된 8개 그룹입니다. 예: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- 단축 표기법: 그룹 맨 앞의 0을 제외하며 0으로 구성된 그룹을 이어진 두 개의 콜론으로 대체합니다. 예: 2001:db8:85a3::8a2e:370:7334
- 도티드 쿼드(Dotted Quad) 표기법(IPv4 매핑 및 IPv4 호환 IPv6 주소): 예를 들어, ::ffff:192.0.2.128

지원되는 IPv6 속성에는 다음이 포함됩니다.

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address
- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

아래 표에는 지원되는 Cisco 속성-값 쌍 및 이에 상응하는 IETF 속성이 나열되어 있습니다.

Cisco 속성-값 쌍	**IETF** 속성
ipv6:addrv6=<ipv6 주소>	Framed-ipv6-Address
ipv6:stateful-ipv6-address-pool=<이름>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<이름>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 주소>	DNS-Server-IPv6-Address

RADIUS Live Logs(RADIUS 라이브 로그) 페이지, RADIUS 인증 보고서, RADIUS 계정 관리 보고서, 현재 활성 세션 보고서, RADIUS 오류 보고서, 잘못 구성된 NAS 보고서, 적응형 네트워크 제어 감사 및 잘못 구성된 신청자 보고서는 IPv6 주소를 지원합니다. RADIUS Live Logs(RADIUS 라이브 로그) 페이지 또는 이러한 보고서에서 관련 세션에 대한 세부정보를 확인할 수 있습니다. IPv4, IPv6 또는 MAC 주소를 기준으로 기록을 필터링할 수 있습니다.

참고 Android 디바이스를 IPv6가 활성화된 DHCPv6 네트워크에 연결하는 경우 Android 디바이스는 DHCP 서버에서 링크-로컬 IPv6 주소만 수신합니다. 따라서 전역 IPv6 주소는 Live Logs(라이브 로그) 및 Endpoints(엔드포인트) 페이지(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**)에 표시되지 않습니다.

다음 절차에서는 권한 부여 정책에서 IPv6 속성을 구성하는 방법을 설명합니다.

시작하기 전에

구축의 NAD가 IPv6을 사용하는 AAA를 지원하는지 확인합니다. NAD에서 IPv6에 대한 AAA 지원을 활성화하는 방법에 대한 자세한 내용은 **IPv6**에 대한 **AAA** 지원을 참고하십시오.

단계 **1** 네트워크 액세스 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Policy Sets(**정책 집합**)**를 선택합니다. 디바이스 관리 정책의 경우 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Device Admin Policy Sets(**디바이스 관리자 정책 집합**)**를 선택합니다.

단계 **2** 권한 부여 규칙을 생성합니다.

단계 **3** 권한 부여 규칙을 만들 때 Conditon Studio에서 조건을 생성합니다. Condition Studio에서 RADIUS 사전의 RADIUS IPv6 속성, 연산자 및 값을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭하여 정책 집합에 권한 부여 규칙을 저장합니다.

Policy Set(정책 집합) 프로토콜 설정

Cisco ISE에서 전역 프로토콜 설정을 정의해야 이러한 프로토콜을 사용하여 정책 집합을 생성, 저장 및 구현할 수 있습니다. 프로토콜 설정 페이지를 사용하여 EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling), EAP-TLS(Extensible Authentication Protocol-Transport Layer Security) 및 PEAP(Protected Extensible Authentication Protocol) 프로토콜에 대한 전역 옵션을 정의할 수 있습니다. 이러한 프로토콜은 네트워크의 다른 디바이스와 통신합니다.

지원되는 네트워크 액세스 정책 집합 프로토콜

아래에는 네트워크 액세스 정책 집합 정책을 정의할 때 선택할 수 있는 프로토콜 목록이 나와 있습니다.

- PAP(Password Authentication Protocol)
- PEAP(Protected Extensible Authentication Protocol)
- MS-CHAPv2(Microsoft Challenge Handshake Authentication Protocol Version 2)
- EAP-MD5(Extensible Authentication Protocol-Message Digest 5)
- EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)
- EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)
- EAP-TTLS(Extensible Authentication Protocol-Tunneled Transport Layer Security)
- PEAP-TLS(Protected Extensible Authentication Protocol-Transport Layer Security)

EAP-FAST를 프로토콜로 사용하기 위한 지침

인증 프로토콜으로 EAP-FAST를 사용할 때는 다음 지침을 따르십시오.

- 인증된 프로비저닝에 대해 EAP-FAST 클라이언트 인증서 수락이 활성화되어 있으면 EAP-FAST 내부 메서드를 활성화하는 것이 좋습니다. 인증된 프로비저닝에 대한 EAP-FAST 클라이언트 인증서 수락은 별도의 인증 방법이 아니라, 동일한 인증서 자격 증명을 사용하여 사용자를 인증하되 내부 메서드를 실행할 필요는 없는 간단한 형식의 클라이언트 인증서 인증입니다.
- 인증된 프로비저닝에 대한 클라이언트 인증서 수락은 비 PAC 전체 핸드셰이크 및 인증된 PAC 프로비저닝에서 작동합니다. 반면 비 PAC 세션 재개, 익명 PAC 프로비저닝 및 PAC 기반 인증에서는 작동하지 않습니다.
- 인증이 다른 순서로 수행되는 경우에도 ID별로 표시되는 EAP 속성(EAP 체인에서 두 번 표시됨)은 모니터링 도구의 인증 세부정보에서 사용자->머신 순서로 표시됩니다.
- EAP-FAST 권한 부여 PAC를 사용하는 경우 라이브 로그에 표시되는 EAP 인증 방법은 조회가 아닌 PEAP에서 전체 인증에 사용되는 인증 방법과 동일합니다.

- EAP 체인 모드에서 터널 PAC가 만료되면 ISE가 프로비저닝으로 폴백되며 AC가 사용자 및 머신 권한 부여 PAC를 요청합니다. 이 경우 머신 권한 부여 PAC는 프로비저닝할 수 없습니다. 이 PAC는 AC가 요청하는 경우 후속 PAC 기반 인증 대화에서 프로비저닝됩니다.
- Cisco ISE가 체인용으로, AC가 단일 모드용으로 구성되어 있으면 AC는 IdentityType TLV를 사용하여 ISE에 응답합니다. 그러나 두 번째 ID 인증은 실패합니다. 이 대화에서는 클라이언트가 체인을 수행할 수 있지만 현재는 단일 모드로 구성되어 있음을 확인할 수 있습니다.
- Cisco ISE는 AD에 대해서만 EAP-FAST 체인의 머신 및 사용자용 검색 속성과 그룹을 지원합니다. LDAP 및 내부 DB의 경우 ISE는 마지막 ID 속성만 사용합니다.

참고 High Sierra, Mojave 또는 Catalina MAC OSX 디바이스에 EAP-FAST 인증 프로토콜을 사용하는 경우 "EAP-FAST cryptobinding verification failed" 메시지가 표시될 수 있습니다. 이러한 MAC OSX 디바이스에 대해 EAP-FAST 대신 PEAP 또는 EAP-TLS를 사용하도록 허용되는 프로토콜 페이지에서 Preferred EAP Protocol(기본 EAP 프로토콜) 필드를 구성하는 것이 좋습니다.

EAP-FAST 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **EAP-FAST** > **EAP FAST Settings(EAP FAST** 설정**)**를 선택합니다.

단계 **2** EAP-FAST 프로토콜을 정의하는 데 필요한 세부정보를 입력합니다.

단계 **3** 이전에 생성한 기본 키와 PAC를 모두 취소하려면 **Revoke(**취소**)**를 클릭합니다.

단계 **4** EAP-FAST 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

EAP-FAST용 PAC 생성

Cisco ISE에서 Generate PAC(PAC 생성) 옵션을 사용하여 EAP-FAST 프로토콜용 터널 또는 머신 PAC를 생성할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)**를 선택합니다.

단계 **2** 왼쪽의 설정 탐색창에서 **Protocols(**프로토콜**)**를 클릭합니다.

단계 **3** **EAP-FAST** > **Generate PAC(PAC** 생성**)**를 선택합니다.

단계 **4** EAP-FAST 프로토콜용 머신 PAC를 생성하는 데 필요한 세부정보를 입력합니다.

단계 **5** **Generate PAC(PAC** 생성**)**를 클릭합니다.

EAP-FAST 설정

다음 표에서는 EAP-FAST, EAP-TLS 및 PEAP 프로토콜을 구성하는 데 사용할 수 있는 프로토콜 설정 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **EAP-FAST** > **EAP FAST Settings(EAP FAST** 설정**)**입니다.

표 ***129: EAP-FAST*** 설정 구성

필드 이름	사용 지침
Authority Identity Info Description(기관 **ID** 정보 설명**)**	클라이언트에 자격 증명을 보내는 Cisco ISE 노드를 설명하는 사용자가 쉽게 이해할 수 있는 문자열을 입력합니다. 클라이언트는 TLV(Type, Length, Value)에 대한 PAC(Protected Access Credentials) 정보에서 이 문자열을 검색할 수 있습니다. 기본값은 Identity Services Engine입니다.
Master Key Generation Period(마스터 키 생성 기간**)**	기본 키 생성 기간을 초, 분, 시간, 일 또는 주 단위로 지정합니다. 값은 1초에서 2,147,040,000초 사이의 양의 정수여야 합니다. 기본값은 604,800초(1주일)입니다.
Revoke all master keys and PACs(모든 마스터 키 및 **PAC** 취소**)**	모든 기본 키 및 PAC를 취소하려면 Revoke(취소)를 클릭합니다.
Enable PAC-less Session Resume(비 **PAC** 세션 재개 활성화**)**	PAC 파일 없이 EAP-FAST를 사용하려면 이 확인란을 선택합니다.
PAC-less Session Timeout(비 **PAC** 세션 시간 초과**)**	비 PAC 세션 재개 시간이 초과될 때까지의 시간을 초 단위로 입력합니다. 기본값은 7,200초입니다.

관련 항목

Policy Set(정책 집합) 프로토콜 설정, 951 페이지
EAP-FAST를 프로토콜로 사용하기 위한 지침, 951 페이지
EAP-FAST의 이점, 1002 페이지
EAP-FAST 설정 구성, 952 페이지

PAC 설정

다음 표에서는 EAP-FAST 인증용으로 보호 액세스 자격 증명을 구성하는 데 사용할 수 있는 Generate PAC(PAC 생성) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **EAP-FAST** > **Generate PAC(PAC** 생성**)**입니다.

표 ***130: EAP-FAST***용 ***PAC*** 생성 설정

필드 이름	사용 지침
Tunnel PAC(터널 **PAC)**	터널 PAC를 생성하려면 이 라디오 버튼을 클릭합니다.
Machine PAC(머신 **PAC)**	머신 PAC를 생성하려면 이 라디오 버튼을 클릭합니다.
TrustSec PAC	TrustSec PAC를 생성하려면 이 라디오 버튼을 클릭합니다.
Identity(ID)	(터널 및 머신 PAC의 경우) EAP-FAST 프로토콜에서 "내부 사용자 이름"으로 표시되는 사용자 이름 또는 머신 이름을 지정합니다. ID 문자열이 해당 사용자 이름과 일치하지 않으면 인증은 실패합니다. 이 ID는 ASA(Adaptive Security Appliance)에 정의된 호스트 이름입니다. ID 문자열은 ASA 호스트 이름과 일치해야 합니다. 그렇지 않으면 ASA가 생성된 PAC 파일을 가져올 수 없습니다. TrustSec PAC를 생성하는 경우 Identity(ID) 필드에서 TrustSec 네트워크 디바이스의 디바이스 ID를 지정하며, EAP-FAST 프로토콜에서 개시자 ID가 제공됩니다. 여기에 입력된 ID 문자열이 해당 디바이스 ID와 일치하지 않으면 인증이 실패합니다.
PAC Time to Live	(터널 및 머신 PAC의 경우) PAC의 만료 시간을 지정하는 값을 초 단위로 입력합니다. 기본값은 604,800초(1주일)입니다. 이 값은 1초에서 157,680,000초 사이의 양의 정수여야 합니다. TrustSec PAC의 경우 일, 주, 월 또는 년 단위로 값을 입력합니다. 기본값은 1년입니다. 최소값은 1일이고 최대값은 10년입니다.
Encryption Key(암호화 키**)**	암호화 키를 입력합니다. 키의 길이는 8~256자여야 합니다. 키는 대/소문자, 숫자 또는 영숫자 문자 조합을 포함할 수 있습니다.

필드 이름	사용 지침
Expiration Data(만료 데이터**)**	(TrustSec PAC에만 해당함) 만료 날짜는 PAC Time to Live를 기준으로 계산됩니다.

관련 항목

Policy Set(정책 집합) 프로토콜 설정, 951 페이지
EAP-FAST를 프로토콜로 사용하기 위한 지침, 951 페이지
EAP-FAST용 PAC 생성, 952 페이지

인증 프로토콜로 **EAP-TTLS** 사용

EAP-TTLS는 EAP-TLS 프로토콜의 기능을 확장하는 2단계 프로토콜입니다. 1단계에서는 보안 터널을 구축하고 2단계에서 사용되는 세션 키를 파생시켜 서버와 클라이언트 간에 속성 및 내부 방법 데이터를 안전하게 터널링합니다. 2단계 도중 터널링된 속성을 사용하면 다양한 메커니즘을 사용하여 추가로 인증할 수 있습니다.

Cisco ISE는 다음을 비롯한 여러 TTLS 신청자의 인증을 처리할 수 있습니다.

- Windows의 AnyConnect NAM(Network Access Manager)
- Windows 8.1 기본 신청자
- Secure W2(MultiOS에서는 JoinNow라고도 함)
- MAC OS X 기본 신청자
- IOS 기본 신청자
- Android 기반 기본 신청자
- Linux WPA 신청자

참고 암호화 바인딩이 필요한 경우 내부 방법으로 EAP-FAST를 사용해야 합니다.

EAP-TTLS 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Protocols(**프로토콜**) > EAP-TTLS**

단계 **2** EAP-TTLS Settings(EAP-TTLS 설정) 페이지에서 필요한 세부정보를 입력합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

EAP-TTLS 설정

다음 표에서는 EAP-TTLS Setting(EAP-TTLS 설정) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Protocols(**프로토콜**) > EAP-TTLS**입니다.차

표 ***131: EAP-TTLS*** 설정

필드 이름	사용 지침
Enable EAP-TTLS Session Resume(EAP-TTLS 세션 재개 활성화**)**	이 확인란을 선택하면 사용자가 EAP-TTLS의 2단계에서 정상적으로 인증되는 경우 Cisco ISE가 EAP-TTLS 인증의 1단계 중에 생성된 TLS 세션을 캐시합니다. 사용자가 다시 연결해야 하는데 원래 EAP-TTLS 세션이 시간 초과되지 않은 경우 Cisco ISE는 캐시된 TLS 세션을 사용하므로 EAP-TTLS 성능이 개선되며 AAA 서버 로드가 감소합니다. 참고 EAP-TTLS 세션을 재개할 때는 내부 방법을 건너뜁니다.
EAP-TTLS Session Timeout(EAP-TTLS 세션 시간 초과**)**	EAP-TTLS 세션이 시간 초과될 때까지의 시간을 초 단위로 지정합니다. 기본값은 7,200초입니다.

관련 항목

Policy Set(정책 집합) 프로토콜 설정, 951 페이지
인증 프로토콜로 EAP-TTLS 사용, 955 페이지
EAP-TTLS 설정 구성, 955 페이지

EAP-TLS 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Protocol(**프로토콜**) > EAP-TLS**를 선택합니다.
단계 **2** EAP-TLS 프로토콜을 정의하는 데 필요한 세부정보를 입력합니다.
단계 **3** EAP-TLS 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

EAP-TLS 설정

다음 표에서는 EAP-TLS 프로토콜 설정을 구성하는 데 사용할 수 있는 EAP-TLS Settings(EAP-TLS 설정) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **EAP-TLS**입니다.

표 ***132: EAP-TLS*** 설정

필드	사용 지침
Enable EAP-TLS Session Resume(EAP-TLS 세션 재개 활성화**)**	전체 EAP-TLS 인증을 통과한 사용자의 단축 재인증을 지원하려면 이 확인란을 선택합니다. 이 기능을 사용하는 경우 인증서를 적용하지 않고 SSL(Secure Sockets Layer) 핸드셰이크만 사용하여 사용자를 재인증할 수 있습니다. EAP-TLS 세션 재개는 EAP-TLS 세션 시간이 초과되지 않은 경우에만 작동합니다.
EAP-TLS Session Timeout(EAP-TLS 세션 시간 초과**)**	EAP-TLS 세션의 시간이 초과될 때까지의 시간을 초 단위로 지정합니다. 기본값은 7,200초입니다.
무상태 세션 재개	
Master Key Generation Period(마스터 키 생성 기간**)**	기본 키가 재생성되는 시간을 입력합니다. 이 값은 기본 키가 활성 상태로 유지되는 기간을 결정합니다. 초, 분, 시간, 일 또는 주 단위로 값을 입력할 수 있습니다.
Revoke(철회**)**	**Revoke(**철회**)**를 클릭하여 이전에 생성한 모든 기본 키와 티켓을 취소합니다. 이 옵션은 보조 노드에서 비활성화됩니다.

관련 항목

Policy Set(정책 집합) 프로토콜 설정, 951 페이지
EAP-TLS 설정 구성, 956 페이지

PEAP 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)**를 선택합니다.
단계 **2** 왼쪽의 설정 탐색창에서 **Protocols(**프로토콜**)**를 클릭합니다.
단계 **3** **PEAP**를 선택합니다.

단계 **4** 필요에 따라 세부정보를 입력하여 PEAP 프로토콜을 정의합니다.
단계 **5** PEAP 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

PEAP 설정

다음 표에서는 PEAP 프로토콜 설정을 구성하는 데 사용할 수 있는 PEAP Settings(PEAP 설정) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **PEAP**입니다.

표 ***133: PEAP*** 설정

필드 이름	사용 지침
Enable PEAP Session Resume(PEAL 세션 재개 활성화**)**	사용자가 PEAP의 2단계에서 정상적으로 인증되는 경우, Cisco ISE에서 PEAP 인증의 1단계 중에 생성된 TLS 세션을 캐시하도록 하려면 이 확인란을 선택합니다. 사용자가 다시 연결해야 하는데 원래 PEAP 세션이 시간 초과되지 않은 경우 Cisco ISE는 캐시된 TLS 세션을 사용하므로 PEAP 성능이 개선되며 AAA 서버 로드가 감소합니다. PEAP 세션 재개 기능이 작동하도록 PEAP 세션 시간 초과 값을 지정해야 합니다.
PEAP Session Timeout(PEAP 세션 시간 초과**)**	PEAP 세션 시간이 초과될 때까지의 시간을 초 단위로 지정합니다. 기본값은 7,200초입니다.
Enable Fast Reconnect(빠른 다시 연결 활성화**)**	세션 재개 기능이 활성화되어 있을 때 사용자 자격 증명을 확인하지 않고 Cisco ISE에서 PEAP 세션이 재개되도록 허용하려면 이 확인란을 선택합니다.

관련 항목

Policy Set(정책 집합) 프로토콜 설정, 951 페이지
PEAP 설정 구성, 957 페이지
PEAP를 사용하는 경우의 이점, 1000 페이지
PEAP 프로토콜용으로 지원되는 신청자, 1001 페이지
PEAP 프로토콜 흐름, 1001 페이지

RADIUS 설정 구성

인증하지 못한 클라이언트를 탐지하고 반복적으로 표시되는 인증 성공 보고를 숨기도록 RADIUS 설정을 구성할 수 있습니다.

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

단계 **2** Settings(설정) 탐색창에서 **Protocols(**프로토콜**)**를 클릭합니다.

단계 **3** **RADIUS**를 선택합니다.

단계 **4** RADIUS 설정을 정의하는 데 필요한 세부정보를 입력합니다.

단계 **5** 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

RADIUS 설정

다음 표에서는 RADIUS Settings(RADIUS 설정) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **RADIUS**입니다.

Suppress Repeated Failed Clients(반복 실패한 클라이언트 숨기기**)** 옵션을 활성화하면 인증에 반복적으로 실패한 클라이언트가 감사 로그에서 숨겨지고, 지정된 기간 동안 이러한 클라이언트의 요청이 자동으로 거부됩니다. 또한 이러한 클라이언트의 요청을 거부해야 하는 인증 실패 횟수를 지정할 수도 있습니다. 예를 들어 이 값이 5로 구성된 경우 클라이언트 인증이 5번 실패하면 해당 클라이언트에서 수신된 모든 요청이 구성된 기간 동안 거부됩니다.

참고 잘못된 비밀번호를 입력해서 인증에 실패한 경우 클라이언트가 숨겨지지 않습니다.

참고 RADIUS 실패 숨기기를 구성한 경우 RADIUS 로그 숨기기를 구성한 후에 "`5440 Endpoint Abandoned EAP Session and started a new one(5440 엔드포인트에서 EAP 세션이 종료되고 새 세션이 시작됨)`" 오류가 계속해서 발생할 수 있습니다. 자세한 내용은 다음 ISE 커뮤니티 게시물을 참조하십시오.

https://community.cisco.com/t5/network-access-control/authentication-failed-quot-5440-endpoint-abandoned-eap-session/td-p/3191944

표 ***134: RADIUS*** 설정

필드 이름	사용 지침
Suppress Repeated Failed Clients(반복 실패한 클라이언트 숨기기**)**	
Suppress Repeated Failed Clients(반복 실패한 클라이언트 숨기기**)**	같은 이유로 인증에 반복적으로 실패한 클라이언트를 숨기려면 이 확인란을 선택합니다. **Reject RADIUS Requests from Clients with Repeated Failures(**반복 실패한 클라이언트의 **RADIUS** 요청 거부**))** 옵션이 활성화된 경우 이러한 클라이언트는 감사 로그에서 숨겨지며 지정된 기간 동안 해당 클라이언트의 요청이 거부됩니다.

필드 이름	사용 지침
Detect Two Failures Within(기간 내에 **2**번의 실패 탐지**)**	시간 간격을 분 단위로 입력합니다. 이 기간 내에 클라이언트가 동일한 이유로 인증에 2번 실패하면 감사 로그에서 숨겨지며, **Reject RADIUS Requests from Clients with Repeated Failures(**반복 실패한 클라이언트의 **RADIUS** 요청 거부**)** 옵션이 활성화되어 있으면 이 클라이언트의 요청이 거부됩니다.
Report Failures Once Every(매번 실패 보고**)**	실패한 인증을 보고할 시간 간격을 분 단위로 입력합니다. 예를 들어 이 값을 15분으로 설정하면 반복적으로 인증에 실패한 클라이언트가 15분마다 한 번씩 감사 로그에 보고되므로, 초과 보고를 방지할 수 있습니다.
Reject RADIUS Requests from Clients with Repeated Failures(반복 실패한 클라이언트의 **RADIUS** 요청 거부**)**	인증에 반복적으로 실패하는 클라이언트의 RADIUS 요청을 자동으로 거부하려면 이 확인란을 선택합니다. 이 옵션을 활성화하여 Cisco ISE의 불필요한 처리를 방지하고 잠재적인 서비스 거부 공격으로부터 보호할 수 있습니다.
Failures Prior to Automatic Rejection(자동 거부 전 실패**)**	반복적으로 인증에 실패하는 클라이언트의 요청이 자동으로 거부될 때까지의 인증 실패 횟수를 입력합니다. 이러한 클라이언트에서 수신된 모든 요청은 구성된 기간(**Continue Rejecting Requests for(**요청 계속 거부**)** 필드에 지정) 동안 자동으로 거부됩니다. 간격이 만료되면 이러한 클라이언트의 인증 요청이 처리됩니다.
Continue Rejecting Requests for(요청 계속 거부**)**	반복적으로 인증에 실패한 클라이언트의 요청을 거부할 시간 간격을 분 단위로 입력합니다.
Ignore Repeated Accounting Updates Within(기간 내 반복 계정 관리 업데이트 무시**)**	이 기간 내에 반복적으로 발생하는 계정 관리 업데이트는 무시됩니다.
Suppress Successful Reports(성공적인 보고 숨기기**)**	
Suppress Repeated Successful Authentications(반복적인 인증 성공 메시지 숨기기**)**	ID 상황, 네트워크 디바이스 및 권한 부여가 변경되지 않은 지난 24시간 동안의 인증 요청 성공이 반복적으로 보고되지 않도록 하려면 이 확인란을 선택합니다.
Authentications Details(인증 세부정보**)**	
Highlight Steps Longer Than(다음보다 긴 단계 표시**)**	시간 간격을 밀리초 단위로 입력합니다. 단일 단계를 실행하는 데 지정된 임계값을 초과할 경우 인증 세부정보 창에 시계 아이콘으로 표시됩니다.

필드 이름	사용 지침
Detect High Rate of RADIUS Requests(높은 비율의 **RADIUS** 요청 탐지**)**	
Detect Steady High Rate of RADIUS Requests(꾸준히 높은 **RADIUS** 요청 탐지**)**	**Duration of RADIUS requests(RADIUS** 요청 기간**)** 및 **Total number of RADIUS requests(**총 **RADIUS** 요청 수**)** 필드에 지정된 한도를 초과한 경우 높은 RADIUS 요청 로드에 대한 경보를 생성하려면 이 확인란을 선택합니다.
Duration of RADIUS Requests(RADIUS 요청 기간**)**	RADIUS 비율을 계산하는 데 적용할 기간을 초 단위로 입력합니다. 기본값은 60초입니다. 유효 범위는 20~86400초입니다.
Total Number of RADIUS Requests(총 **RADIUS** 요청 수**)**	RADIUS 비율을 계산하는 데 적용할 요청 한도를 입력합니다. 기본값은 72000개의 요청입니다. 유효 범위는 24000~103680000개의 요청입니다.
RADIUS UDP Ports(RADIUS UDP 포트**)**	
Authentication Port(인증 포트**)**	RADIUS UDP 인증 플로우에 사용할 포트를 지정합니다. 최대 4개의 포트 번호(쉼표로 구분)를 지정할 수 있습니다. 기본값으로 포트 1812 및 포트 1645가 사용됩니다. 유효 범위는 1024~65535입니다.
Accounting Port(계정 관리 포트**)**	RADIUS UDP 계정 관리 플로우에 사용할 포트를 지정합니다. 최대 4개의 포트 번호(쉼표로 구분)를 지정할 수 있습니다. 기본값으로 포트 1813 및 포트 1646이 사용됩니다. 유효 범위는 1024~65535입니다. 참고 해당 포트가 다른 서비스에서 사용되지 않는지 확인하십시오.
RADIUS DTLS	
Authentication and Accounting Port(인증 및 계정 관리 포트**)**	RADIUS DTLS 인증 및 계정 관리 플로우에 사용할 포트를 지정합니다. 기본값으로 포트 2083이 사용됩니다. 유효 범위는 1024~65535입니다. 참고 해당 포트가 다른 서비스에서 사용되지 않는지 확인하십시오.
Idle Timeout(유휴 시간 초과**)**	네트워크 디바이스에서 패킷이 수신되지 않는 경우 Cisco ISE가 TLS 세션을 닫기 전에 대기할 시간을 초 단위로 입력합니다. 기본값은 120초입니다. 유효 범위는 60~600초입니다.

필드 이름	사용 지침
Enable RADIUS/DTLS Client Identity Verification(RADIUS/DTLS 클라이언트 **ID** 확인 활성화**)**	Cisco ISE가 DTLS 핸드셰이크 중에 RADIUS/DTLS 클라이언트의 ID를 확인하도록 하려면 이 확인란을 선택합니다. 클라이언트 ID가 유효하지 않으면 Cisco ISE에서 핸드셰이크에 실패합니다. 구성된 경우 기본 네트워크 디바이스에 대한 ID 확인을 건너뜁니다. ID 확인은 다음 순서로 수행됩니다. **1.** 클라이언트 인증서에 SAN(Subject Alternative Name) 속성이 포함된 경우 다음과 같이 진행됩니다. • SAN에 DNS 이름이 포함되어 있으면 인증서에 지정된 DNS 이름이 Cisco ISE의 네트워크 디바이스에 대해 구성된 DNS 이름과 비교됩니다. • SAN에 IP 주소가 포함되어 있고 DNS 이름이 포함되어 있지 않으면 인증서에 지정된 IP 주소가 Cisco ISE에 구성된 모든 디바이스 IP 주소와 비교됩니다. **2.** 인증서에 SAN이 포함되어 있지 않으면 주체 CN은 Cisco ISE에서 네트워크 디바이스에 대해 구성된 DNS 이름과 비교됩니다. Cisco ISE가 일치하지 않을 경우 핸드셰이크에 실패합니다.

관련 항목

Policy Set(정책 집합) 프로토콜 설정, 951 페이지
Cisco ISE의 RADIUS 프로토콜 지원, 968 페이지
RADIUS 설정 구성, 958 페이지

보안 설정 구성

보안 설정을 구성하려면 다음을 수행합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Security Settings(**보안 설정**)**.

단계 **2** Security Settings(보안 설정) 페이지에서 다음 옵션을 선택합니다.

- **Allow TLS 1.0(TLS 1.0** 허용**)**: 다음 워크플로우에서 레거시 피어와의 통신을 위해 TLS 1.0을 허용합니다.
  - Cisco ISE가 EAP 서버로 구성됨

- Cisco ISE가 HTTPS 또는 보안 LDAP 서버에서 CRL을 다운로드함
- Cisco ISE가 보안 시스템 로그 클라이언트로 구성됨
- Cisco ISE가 보안 LDAP 클라이언트로 구성됨

- **Allow TLS 1.0(TLS 1.0** 허용**)**: 다음 워크플로우에서 레거시 피어와의 통신을 위해 TLS 1.0을 허용합니다.
  - Cisco ISE가 EAP 서버로 구성됨
  - Cisco ISE가 HTTPS 또는 보안 LDAP 서버에서 CRL을 다운로드함
  - Cisco ISE가 보안 시스템 로그 클라이언트로 구성됨
  - Cisco ISE가 보안 LDAP 클라이언트로 구성됨

- **Allow SHA1 Ciphers(SHA1** 암호 허용**)**: 다음 워크플로우에서 피어와의 통신을 위해 SHA-1 암호를 허용합니다.
  - Cisco ISE가 EAP 서버로 구성됨
  - Cisco ISE가 RADIUS DTLS 서버로 구성됨
  - Cisco ISE가 RADIUS DTLS 클라이언트로 구성됨
  - Cisco ISE가 HTTPS 또는 보안 LDAP 서버에서 CRL을 다운로드함
  - Cisco ISE가 보안 시스템 로그 클라이언트로 구성됨
  - Cisco ISE가 보안 LDAP 클라이언트로 구성됨

  다음 옵션 중 하나를 선택할 수 있습니다.
  - 모든 **SHA-1** 암호 허용
  - **TLS_RSA_with_AES_128_CBC_SHA** 만 허용

  참고 보안 강화를 위해 SHA-256 또는 SHA-384 암호를 사용하는 것이 좋습니다.

- **Allow ECDHE-RSA Ciphers(ECDHE-RSA** 암호 허용**)**: 다음 워크플로우에서 피어와의 통신을 위해 ECDHE-RSA 암호를 허용합니다.
  - Cisco ISE가 EAP 서버로 구성됨
  - Cisco ISE가 RADIUS DTLS 서버로 구성됨
  - Cisco ISE가 RADIUS DTLS 클라이언트로 구성됨
  - Cisco ISE가 HTTPS 또는 보안 LDAP 서버에서 CRL을 다운로드함
  - Cisco ISE가 보안 시스템 로그 클라이언트로 구성됨
  - Cisco ISE가 보안 LDAP 클라이언트로 구성됨

- **Allow 3DES Ciphers(3DES** 암호 허용**)**: 다음 워크플로우에서 피어와의 통신을 위해 3DES 암호를 허용합니다.

- Cisco ISE가 EAP 서버로 구성됨
- Cisco ISE가 RADIUS DTLS 서버로 구성됨
- Cisco ISE가 RADIUS DTLS 클라이언트로 구성됨
- Cisco ISE가 HTTPS 또는 보안 LDAP 서버에서 CRL을 다운로드함
- Cisco ISE가 보안 시스템 로그 클라이언트로 구성됨
- Cisco ISE가 보안 LDAP 클라이언트로 구성됨

- **Accept Certificates without Validating Purpose(**용도 확인 없이 인증서 수락**)**: ISE가 EAP 또는 RADIUS DTLS 서버로 작동하는 경우 키 사용 확장에 ECDHE-ECDSA 암호용 keyAgreement 비트가 포함되어 있는지 아니면 다른 암호용 keyEncipherment 비트가 포함되어 있는지를 확인하지 않고 클라이언트 인증서를 수락합니다.
- **Allow DSS ciphers for ISE as a client(**클라이언트로 작동하는 **ISE**에 **DSS** 암호 허용**)**: Cisco ISE가 클라이언트로 작동하는 경우 다음 워크플로우에서 서버와의 통신에 DSS 암호를 허용합니다.
  - Cisco ISE가 RADIUS DTLS 클라이언트로 구성됨
  - Cisco ISE가 HTTPS 또는 보안 LDAP 서버에서 CRL을 다운로드함
  - Cisco ISE가 보안 시스템 로그 클라이언트로 구성됨
  - Cisco ISE가 보안 LDAP 클라이언트로 구성됨
- **Allow Legacy Unsafe TLS Renegotiation for ISE as a Client(**클라이언트로 작동하는 **ISE**에 안전하지 않은 레거시 **TLS** 재협상 허용**)**: 다음 워크플로우에서 안전한 TLS 재협상을 지원하지 않는 레거시 TLS 서버와의 통신을 허용합니다.
  - Cisco ISE가 HTTPS 또는 보안 LDAP 서버에서 CRL을 다운로드함
  - Cisco ISE가 보안 시스템 로그 클라이언트로 구성됨
  - Cisco ISE가 보안 LDAP 클라이언트로 구성됨

단계 **3** **Disclose invalid usernames(**잘못된 사용자 이름 공개**)**: 기본적으로 ISE에서는 잘못된 사용자 이름으로 인한 인증 실패 시 INVALID가 표시됩니다. 디버깅을 지원하기 위해 이 옵션을 사용하는 경우 ISE에서 보고서에 INVALID 대신 USERNAME이 공개(표시)됩니다. 이 옵션의 선택 여부와 관계없이 잘못된 사용자 이름이 아닌 다른 이유로 인해 인증에 실패할 경우 항상 USERNAME이 표시됩니다.

Disclose invalid usernames(잘못된 사용자 이름 공개**)**를 활성화하는 경우 **Always show invalid usernames(**항상 잘못된 사용자 이름 표시**)** 또는 **Show invalid usernames for a specific time(**특정 시간 동안 잘못된 사용자 이름 표시**)**을 선택해야 합니다. 특정 시간 동안 표시하는 옵션을 선택하는 경우 최대 1개월(43,200분)의 시간(분)을 선택합니다.

이 기능은 Active Directory, Internal Users(내부 사용자), LDAP 및 ODBC ID 소스에 대해 지원되며, RADIUS 토큰, RSA 또는 SAML 등의 다른 ID 저장소에 대해서는 지원되지 않습니다. 이러한 ID 저장소의 경우 잘못 입력한 사용자 이름은 항상 "invalid"로 보고됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

지원되는 암호 그룹

Cisco ISE는 TLS 버전 1.0, 1.1 및 1.2를 지원합니다.

Cisco ISE는 RSA 및 ECDSA 서버 인증서를 지원합니다. 다음과 같은 타원 곡선이 지원됩니다.

- secp256r1
- secp384r1
- secp521r1

다음 표에는 지원되는 암호 그룹이 나와 있습니다.

암호 그룹	**Cisco ISE**가 **EAP** 서버로 구성된 경우 **Cisco ISE**가 **RADIUS DTLS** 서버로 구성된 경우	**Cisco ISE**가 **HTTPS** 또는 보안 **LDAP** 서버에서 **CRL**을 다운로드하는 경우 **Cisco ISE**가 보안 시스템 로그 클라이언트 또는 보안 **LDAP** 클라이언트로 구성된 경우 **Cisco ISE**가 **CoA**용 **RADIUS DTLS** 클라이언트로 구성된 경우
TLS 1.0 지원	TLS 1.0이 허용되는 경우 (DTLS 서버는 DTLS 1.2 만 지원) Allow TLS 1.0(TLS 1.0 허용) 옵션은 Cisco ISE 2.3 이상에서 기본적으로 비활성화되어 있습니다. 이 옵션이 비활성화되어 있으면 TLS 기반 EAP 인증 방법(EAP-TLS, EAP-FAST / TLS) 및 802.1X 신청자에 대해 TLS 1.0이 지원되지 않습니다. TLS 1.0에서 TLS 기반 EAP 인증 방법을 사용하려면 **Security Settings(**보안 설정**)** 창에서 Allow TLS 1.0(TLS 1.0 허용) 확인란을 선택합니다. 를 선택합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **Security Settings(**보안 설정**)**.	TLS 1.0이 허용되는 경우 (DTLS 클라이언트는 DTLS 1.2 만 지원)
TLS 1.1 지원	TLS 1.1이 허용되는 경우	TLS 1.1이 허용되는 경우
ECC DSA 암호		

ECDHE-ECDSA-AES256-GCM-SHA384	예	예
ECDHE-ECDSA-AES128-GCM-SHA256	예	예
ECDHE-ECDSA-AES256-SHA384	예	예
ECDHE-ECDSA-AES128-SHA256	예	예
ECDHE-ECDSA-AES256-SHA	SHA-1이 허용되는 경우	SHA-1이 허용되는 경우
ECDHE-ECDSA-AES128-SHA	SHA-1이 허용되는 경우	SHA-1이 허용되는 경우
ECC RSA 암호		
ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA가 허용되는 경우	ECDHE-RSA가 허용되는 경우
ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA가 허용되는 경우	ECDHE-RSA가 허용되는 경우
ECDHE-RSA-AES256-SHA384	ECDHE-RSA가 허용되는 경우	ECDHE-RSA가 허용되는 경우
ECDHE-RSA-AES128-SHA256	ECDHE-RSA가 허용되는 경우	ECDHE-RSA가 허용되는 경우
ECDHE-RSA-AES256-SHA	ECDHE-RSA/SHA-1이 허용되는 경우	ECDHE-RSA/SHA-1이 허용되는 경우
ECDHE-RSA-AES128-SHA	ECDHE-RSA/SHA-1이 허용되는 경우	ECDHE-RSA/SHA-1이 허용되는 경우
DHE RSA 암호		
DHE-RSA-AES256-SHA256	아니요	예
DHE-RSA-AES128-SHA256	아니요	예
DHE-RSA-AES256-SHA	No(아니요)	SHA-1이 허용되는 경우
DHE-RSA-AES128-SHA	No(아니요)	SHA-1이 허용되는 경우
RSA 암호		
AES256-SHA256	예	예
AES128-SHA256	예	예
AES256-SHA	SHA-1이 허용되는 경우	SHA-1이 허용되는 경우
AES128-SHA	SHA-1이 허용되는 경우	SHA-1이 허용되는 경우

3DES 암호		
DES-CBC3-SHA	3DES/SHA-1이 허용되는 경우	3DES/DSS 및 SHA-1이 활성화된 경우
DSS 암호		
DHE-DSS-AES256-SHA	No(아니요)	3DES/DSS 및 SHA-1이 활성화된 경우
DHE-DSS-AES128-SHA	No(아니요)	3DES/DSS 및 SHA-1이 활성화된 경우
EDH-DSS-DES-CBC3-SHA	No(아니요)	3DES/DSS 및 SHA-1이 활성화된 경우
약한 RC4 암호		
RC4-SHA	Allowed Protocols(허용되는 프로토콜) 페이지에서 "Allow weak ciphers(약한 암호 허용)"옵션이 활성화된 경우 및 SHA-1이 허용되는 경우	No(아니요)
RC4-MD5	Allowed Protocols(허용되는 프로토콜) 페이지에서 "Allow weak ciphers(약한 암호 허용)"옵션이 활성화된 경우	No(아니요)
EAP-FAST 익명 프로비저닝의 경우에만: ADH-AES-128-SHA	예	아니요
피어 인증서 제한		
KeyUsage 검증	클라이언트 인증서에는 다음 암호에 대해 KeyUsage=Key Agreement 및 ExtendedKeyUsage=Client Authentication이 있어야 합니다. • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	

ExtendedKeyUsage 검증	클라이언트 인증서에는 다음 암호에 대해 KeyUsage=Key Encipherment 및 ExtendedKeyUsage=Client Authentication이 있어야 합니다. • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	서버 인증서에는 ExtendedKeyUsage=Server Authentication이 있어야합니다.

Cisco ISE의 RADIUS 프로토콜 지원

RADIUS는 원격 액세스 서버가 중앙 서버와 통신하여 전화 접속 사용자를 인증하고 요청한 시스템 또는 서비스에 액세스할 수 있는 권한을 부여하는 데 사용되는 클라이언트/서버 프로토콜입니다. RADIUS를 사용하여 모든 원격 서버가 공유할 수 있는 중앙 데이터베이스에서 사용자 프로파일을 유지할 수 있습니다. 이 프로토콜은 향상된 보안을 제공하므로 이 프로토콜을 사용하여 관리되는 단일 네트워크 포인트에 적용되는 정책을 설정할 수 있습니다.

또한 RADIUS는 Cisco ISE에서 원격 RADIUS 서버에 대한 요청을 프록시하는 RADIUS 클라이언트 역할을 하며, 활성 세션 중에 CoA(Change of Authorization) 활동을 제공합니다.

Cisco ISE는 RFC 2865에 따라 RADIUS 프로토콜 흐름을 지원하며 RFC 2865 및 확장에 설명된 것처럼 모든 일반 RADIUS 속성에 대한 일반적인 지원을 제공합니다. Cisco ISE는 Cisco ISE 사전에 정의된 벤더에 대해서만 벤더별 속성을 구문 분석할 수 있습니다.

RADIUS 인터페이스는 RFC 2865에 정의된 다음과 같은 속성 데이터 유형을 지원합니다.

- 텍스트(UTF(Unicode Transformation Format))
- 문자열(이진)
- 주소(IP)

- 정수
- 시간

ISE 커뮤니티 리소스

Cisco ISE에서 지원하는 네트워크 액세스 속성에 대한 자세한 내용은 ISE 네트워크 액세스 속성을 참고하십시오.

허용되는 프로토콜

다음 표에서는 인증 중에 사용할 프로토콜을 구성할 수 있는 **Allowed Protocols(**허용되는 프로토콜**)** 창의 필드에 대해 설명합니다. **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authentication(**인증**)** > **Allowed Protocols(**허용되는 프로토콜**)**입니다.

표 ***135:*** 허용되는 프로토콜

필드 이름	사용 지침
Allowed Protocols(허용되는 프로토콜**) > Authentication Bypass(**인증 우회**)**	
Process Host Lookup(프로세스 호스트 조회**)**	Cisco ISE가 호스트 조회 요청을 처리하도록 지정하려면 이 확인란을 선택합니다. RADIUS 서비스 유형이 10(통화 확인)이고 사용자 이름이 Calling-Station-ID와 같으면 PAP/CHAP 프로토콜에 대한 호스트 조회 요청이 처리됩니다. 서비스 유형이 1(프레임)이고 사용자 이름이 Calling-Station-ID와 같으면 EAP-MD5 프로토콜에 대한 호스트 조회 요청이 처리됩니다. Cisco ISE가 호스트 조회 요청을 무시하고 인증에 시스템 사용자 이름 속성의 원래 값을 사용하도록 지정하려면 이 확인란의 선택을 취소합니다. 선택을 취소하면 프로토콜(예: PAP)에 따라 메시지 처리가 수행됩니다. 참고 이 옵션을 비활성화하면 기존 MAB 인증이 실패할 수 있습니다.
Allowed Protocols(허용되는 프로토콜**) > Authentication Protocols(**인증 프로토콜**)**	
Allow PAP/ASCII(PAP/ASCII 허용**)**	이 옵션은 PAP/ASCII를 활성화합니다. PAP는 일반 텍스트 비밀번호(즉, 암호화되지 않은 비밀번호)를 사용하며 보안 레벨이 가장 낮은 인증 프로토콜입니다.

필드 이름	사용 지침
Allow CHAP(CHAP 허용**)**	이 옵션은 CHAP 인증을 활성화합니다. CHAP는 비밀번호 암호화와 함께 시도 응답 메커니즘을 사용합니다. Microsoft Active Directory에서는 CHAP가 작동하지 않습니다.
Allow MS-CHAPv1(MS-CHAPv1 허용**)**	MS-CHAPv1을 활성화하려면 이 확인란을 선택합니다.
Allow MS-CHAPv2(MS-CHAPv2 허용**)**	MS-CHAPv2를 활성화하려면 이 확인란을 선택합니다.
Allow EAP-MD5(EAP-MD5 허용**)**	EAP 기반 MD5 비밀번호 해시 인증을 활성화하려면 이 확인란을 선택합니다.

필드 이름	사용 지침
Allow EAP-TLS(EAP-TLS 허용)	

필드 이름	사용 지침
	EAP-TLS 인증 프로토콜을 활성화하고 EAP-TLS 설정을 구성하려면 이 확인란을 선택합니다. Cisco ISE에서 최종 사용자 클라이언트의 EAP ID 응답에 제공된 사용자 ID를 확인하는 방법을 지정할 수 있습니다. 사용자 ID는 최종 사용자 클라이언트가 제공하는 인증서의 정보와 비교하여 확인됩니다. Cisco ISE와 최종 사용자 클라이언트 간에 EAP-TLS 터널이 설정된 후에 이러한 비교가 이루어집니다. 참고 EAP-TLS는 인증서 기반 인증 프로토콜입니다. 인증서를 구성하는 데 필요한 단계를 완료한 후에만 EAP-TLS 인증이 발생할 수 있습니다. • **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy(**만료된 인증서 인증을 허용하여 권한 부여 정책에서 인증서 갱신 허용**)**: 사용자가 인증서를 갱신하도록 허용하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 요청을 추가로 처리하기 전에 인증서가 갱신되었는지 확인하는 권한 부여 정책 규칙을 구성할 수 있습니다. • **Enable Stateless Session Resume(**상태 비저장 세션 재개 활성화**)**: 서버에 세션 상태를 저장할 필요 없이 EAP-TLS 세션 재개를 허용하려면 이 확인란을 선택합니다. Cisco ISE는 RFC 5077에 설명된 대로 세션 티켓 확장을 지원합니다. Cisco ISE는 티켓을 생성하여 EAP-TLS 클라이언트로 전송합니다. 클라이언트는 세션을 다시 시작하기 위해 ISE에 티켓을 제공합니다. • **Proactive Session Ticket update(**선제적 세션 티켓 업데이트**)**: 세션 티켓이 업데이트되기 전에 얼마만큼의 TTL(Time To Live)이 필수로 경과해야 하는지 나타내는 값을 백분율로 입력합니다. 예를 들어 값 60을 입력하면 TTL의 60%가 만료된 후 세션 티켓이 업데이트됩니다. • **Session ticket Time to Live(**세션 티켓 **TTL(Time to Live))**: 여기에 입력하는 시간이 지나면 세션 티켓이 만료됩니다. 이 값은 세

필드 이름	사용 지침
	션 티켓이 활성 상태로 유지되는 기간을 결정합니다. 초, 분, 시간, 일 또는 주 단위로 값을 입력할 수 있습니다.
Allow LEAP(LEAP 허용**)**	LEAP(Lightweight Extensible Authentication Protocol) 인증을 활성화하려면 이 확인란을 선택합니다.

필드 이름	사용 지침
Allow PEAP(PEAP 허용**)**	

필드 이름	사용 지침

	PEAP 인증 프로토콜을 활성화하고 PEAP 설정을 구성하려면 이 확인란을 선택합니다. 기본 내부 방법은 MS-CHAPv2입니다.
	
	Allow PEAP(PEAP 허용) 확인란을 선택하면 다음 PEAP 내부 방법을 구성할 수 있습니다.
	
	• **Allow EAP-MS-CHAPv2(EAP-MS-CHAPv2 허용)**: EAP-MS-CHAPv2를 내부 방법으로 사용하려면 이 확인란을 선택합니다.
	
	  • **Allow Password Change(**비밀번호 변경 허용**)**: Cisco ISE가 비밀번호 변경을 지원하게 하려면 이 확인란을 선택합니다.
	
	  • **Retry Attempts(**재시도 횟수**)**: 로그인 실패를 반환하기 전까지 Cisco ISE가 사용자 자격 증명을 요청하는 횟수를 지정합니다. 유효한 값은 0~3입니다.
	
	• **Allow EAP-GTC(EAP-GTC** 허용**)**: EAP-GTC를 내부 방법으로 사용하려면 이 확인란을 선택합니다.
	
	  • **Allow Password Change(**비밀번호 변경 허용**)**: Cisco ISE가 비밀번호 변경을 지원하게 하려면 이 확인란을 선택합니다.
	
	  • **Retry Attempts(**재시도 횟수**)**: 로그인 실패를 반환하기 전까지 Cisco ISE가 사용자 자격 증명을 요청하는 횟수를 지정합니다. 유효 범위는 0~3입니다.
	
	• **Allow EAP-TLS(EAP-TLS** 허용**)**: EAP-TLS를 내부 방법으로 사용하려면 이 확인란을 선택합니다.
	
	  사용자가 인증서를 갱신하도록 허용하려면 **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy(**만료된 인증서 인증을 허용하여 권한 부여 정책에서 인증서 갱신 허용**)** 확인란을 선택합니다. 이 확인란을 선택하면 요청을 추가로 처리하기 전에 인증서가 갱신되었는지 확인하는 권한 부여 정책 규칙을 구성할 수 있습니다.
	
	• **Require CryptoBinding TLV(**암호화 바인딩

필드 이름	사용 지침
	TLV 필요**)**: EAP 피어와 EAP 서버 모두 PEAP 인증의 내부 및 외부 EAP 인증에 참여하게 하려면 이 확인란을 선택합니다. • **Allow PEAPv0 only for Legacy Clients(**레거시 클라이언트에만 **PEAPv0** 허용**)**: PEAP 신청자가 PEAPv0을 사용하여 협상하도록 허용하려면 이 확인란을 선택합니다. 일부 레거시 클라이언트는 EAPv1 프로토콜 표준을 따르지 않습니다. 그러한 EAP 대화가 삭제되지 않게 하려면 이 확인란을 선택합니다.

필드 이름	사용 지침
Allow EAP-FAST(EAP-FAST 허용**)**	

필드 이름	사용 지침

	EAP-FAST 인증 프로토콜을 활성화하고 EAP-FAST 설정을 구성하려면 이 확인란을 선택합니다. EAP-FAST 프로토콜은 동일한 서버에 대해 여러 내부 프로토콜을 지원합니다. 기본 내부 방법은 MS-CHAPv2입니다.
	
	Allow EAP-FAST(EAP-FAST 허용) 확인란을 선택하면 EAP-FAST를 내부 방법으로 구성할 수 있습니다.
	
	• **Allow EAP-MS-CHAPv2(EAP-MS-CHAPv2 허용)**
	  • **Allow Password Change(**비밀번호 변경 허용**)**: Cisco ISE가 비밀번호 변경을 지원하게 하려면 이 확인란을 선택합니다.
	  • **Retry Attempts(**재시도 횟수**)**: 로그인 실패를 반환하기 전까지 Cisco ISE가 사용자 자격 증명을 요청하는 횟수를 지정합니다. 유효한 값은 0~3입니다.
	
	• **Allow EAP-GTC(EAP-GTC** 허용**)**
	Allow Password Change(비밀번호 변경 허용**)**: Cisco ISE가 비밀번호 변경을 지원하게 하려면 이 확인란을 선택합니다.
	Retry Attempts(재시도 횟수**)**: 로그인 실패를 반환하기 전까지 Cisco ISE가 사용자 자격 증명을 요청하는 횟수를 지정합니다. 유효한 값은 0~3입니다.
	
	• **Use PACs(PAC** 사용**)**: EAP-FAST 클라이언트에 대한 권한 부여 PAC(보호 액세스 자격 증명)를 프로비저닝하도록 Cisco ISE를 구성하려면 이 옵션을 선택합니다. 추가 PAC 옵션이 나타납니다.
	
	• **Don't use PACs(PAC** 사용 안 함**)**: Cisco ISE가 터널 또는 머신 PAC를 발급하거나 수락하지 않고도 EAP-FAST를 사용하도록 구성하려면 이 옵션을 선택합니다. PAC에 대한 모든 요청이 무시되고 Cisco ISE는 PAC 없이 Success-TLV로 응답합니다.
	
	이 옵션을 선택하면 Cisco ISE가 머신 인증을 수행하도록 구성할 수 있습니다.

필드 이름	사용 지침
	• **Allow EAP-TLS(EAP-TLS** 허용**)**: EAP-TLS를 내부 방법으로 사용하려면 이 확인란을 선택합니다. 사용자가 인증서를 갱신하도록 허용하려면 **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy(**만료된 인증서 인증을 허용하여 권한 부여 정책에서 인증서 갱신 허용**)** 확인란을 선택합니다. 이 확인란을 선택하면 요청을 추가로 처리하기 전에 인증서가 갱신되었는지 확인하는 권한 부여 정책 규칙을 구성할 수 있습니다.

필드 이름	사용 지침
	• **Enable EAP Chaining(EAP** 체인 활성화**)**: EAP 체인을 활성화하려면 이 확인란을 선택합니다. EAP 체인은 Cisco ISE에서 EAPChainingResult 속성을 사용하여 사용자 및 머신 인증 결과의 상관관계를 지정하고 적절한 권한 부여 정책을 적용할 수 있도록 합니다. EAP 체인을 사용하려면 클라이언트 디바이스에서 EAP 체인을 지원하는 신청자가 필요합니다. 신청자에서 User and Machine Authentication(사용자 및 머신 인증) 옵션을 선택합니다. EAP 체인은 EAP-FAST 프로토콜(PAC 기반 및 PAC 제외 모드에서 모두)을 선택하는 경우에 사용할 수 있습니다. PAC 기반 인증에서는 사용자 권한 부여 PAC나 머신 권한 부여 PAC 또는 둘 모두를 사용하여 내부 방법을 건너뛸 수 있습니다. 인증서 기반 인증의 경우 EAP-FAST 프로토콜에 대해 Accept Client Certificate for Provisioning(프로비저닝할 클라이언트 인증서 수락) 옵션을 활성화(허용되는 프로토콜 서비스 내)하고 터널 내에서 사용자 인증서를 보내도록 엔드포인트(AnyConnect)가 구성된 경우, 터널 설정 중에 ISE는 인증서를 사용하여 사용자를 인증하며(내부 방법을 건너뜀) 내부 방법을 통해 머신 인증이 수행됩니다. 이러한 옵션을 구성하지 않으면 EAP-TLS가 사용자 인증을 위한 내부 방법으로 사용됩니다. EAP 체인을 활성화한 후에 권한 부여 정책을 업데이트하고 NetworkAccess:EapChainingResult 속성을 사용하여 조건을 추가하고 적절한 권한을 할당합니다.

필드 이름	사용 지침

Allow EAP-TTLS(EAP-TTLS 허용)	EAP-TTLS 프로토콜을 활성화하려면 이 확인란을 선택합니다.
	
	다음 내부 방법을 구성할 수 있습니다.
	
	• **Allow PAP/ASCII(PAP/ASCII 허용)**: PAP/ASCII를 내부 방법으로 사용하려면 이 확인란을 선택합니다. 토큰 및 OTP 기반 인증을 위해 EAP-TTLS PAP를 사용할 수 있습니다.
	
	• **Allow CHAP(CHAP허용)**: CHAP를 내부 방법으로 사용하려면 이 확인란을 선택합니다. CHAP는 비밀번호 암호화와 함께 시도 응답 메커니즘을 사용합니다. Microsoft Active Directory에서는 CHAP가 작동하지 않습니다.
	
	• **Allow MS-CHAPv1(MS-CHAPv1 허용)**: MS-CHAPv1을 내부 방법으로 사용하려면 이 확인란을 선택합니다.
	
	• **Allow MS-CHAPv2(MS-CHAPv2 허용)**: MS-CHAPv2를 내부 방법으로 사용하려면 이 확인란을 선택합니다.
	
	• **Allow EAP-MD5(EAP-MD5 허용)**: EAP-MD5를 내부 방법으로 사용하려면 이 확인란을 선택합니다.
	
	• **Allow EAP-MS-CHAPv2(EAP-MS-CHAPv2 허용)**: EAP-MS-CHAPv2를 내부 방법으로 사용하려면 이 확인란을 선택합니다.
	
	  • **Allow Password Change(**비밀번호 변경 허용**)**: Cisco ISE가 비밀번호 변경을 지원하게 하려면 이 확인란을 선택합니다.
	
	  • **Retry Attempts(**재시도 횟수**)**: 로그인 실패를 반환하기 전까지 Cisco ISE가 사용자 자격 증명을 요청하는 횟수를 지정합니다. 유효한 값은 0~3입니다.

필드 이름	사용 지침
TEAP 허용	

필드 이름	사용 지침

	TEAP(Tunnel Extensible Authentication Protocol)를 활성화하고 TEAP 설정을 구성하려면 이 확인란을 선택합니다. TEAP는 TLS(Transport Layer Security) 프로토콜을 사용해 터널을 설정하여 피어와 서버 간의 보안 통신을 활성화하는 터널 기반 EAP 방법입니다. TAP(유형-길이-값) 개체는 TEAP 터널 내에서 EAP 피어와 EAP 서버 간에 인증 관련 데이터를 전송하기 위해 사용됩니다.
	
	TEAP에 대해 다음의 내부 방법을 구성할 수 있습니다.
	
	• **Allow EAP-MS-CHAPv2(EAP-MS-CHAPv2** 허용**)**: EAP-MS-CHAPv2를 내부 방법으로 사용하려면 이 확인란을 선택합니다.
	
	  • **Allow Password Change(**비밀번호 변경 허용**)**: Cisco ISE가 비밀번호 변경을 지원하게 하려면 이 확인란을 선택합니다.
	
	  • **Retries(**재시도 횟수**)**: Cisco ISE에서 로그인 실패 메시지를 반환하기 전에 사용자가 자격 증명을 입력할 수 있도록 허용하는 횟수를 입력합니다. 유효 범위는 0~3입니다.
	
	• **Allow EAP-TLS(EAP-TLS** 허용**)**: EAP-TLS를 내부 방법으로 사용하려면 이 확인란을 선택합니다.
	
	  • **Allow Authentication of Expired Certificates to Allow Certificate Renewal in Authorization Policy(**만료된 인증서 인증을 허용하여 권한 부여 정책에서 인증서 갱신 허용**)**: 사용자가 인증서를 갱신하도록 허용하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 권한 부여 요청을 추가로 처리하기 전에 인증서가 갱신되었는지 확인하는 적절한 권한 부여 정책 규칙을 구성할 수 있습니다.
	
	• **Allow Downgrade to MSK(MSK**로 다운그레이드 허용**)**: 내부 방법이 EMSK(Extended Master Session Key)를 지원하지만 클라이언트 디바이스가 MSK(Master Session Key)만 제공하는 경우 이 확인란을 선택합니다. 참고

필드 이름	사용 지침
	로 MSK보다 EMSK가 더 안전하지만 일부 클라이언트 디바이스는 EMSK를 지원하지 않을 수 있습니다. • **Accept Client Certificate during Tunnel Establishment(**터널 설정 중 클라이언트 인증서 허용**)**: Cisco ISE가 TEAP 터널 설정 중에 클라이언트 인증서를 요청하도록 하려면 이 확인란을 선택합니다. 인증서가 제공되지 않으면 Cisco ISE는 구성된 내부 방법을 사용하여 인증합니다. • **Enable EAP Chaining(EAP** 체인 활성화**)**: EAP 체인을 활성화하려면 이 확인란을 선택합니다. EAP 체인을 사용하면 Cisco ISE가 동일한 TEAP 터널 내에서 사용자 및 머신 인증 모두에 대해 내부 방법을 실행할 수 있습니다. 이를 통해 Cisco ISE는 EAPChainingResult 속성을 사용하여 인증 결과의 상관관계를 지정하고 적절한 권한 부여 정책을 적용할 수 있습니다. EAP 체인을 활성화한 후에는 권한 부여 정책을 업데이트하고 NetworkAccess:EapChainingResult 속성을 사용하여 조건을 추가한 다음 적절한 권한을 할당합니다. 참고 EAP 체인이 활성화된 경우, 사용자 및 머신 인증을 모두 수행하려면 사용자 및 머신 인증서가 신청자에서 복사되었는지 확인합니다.

필드 이름	사용 지침
	참고 • EAP 체인이 Cisco ISE에서 활성화된 경우 Microsoft 신청자에 대해 기본 및 보조 인증 방법을 모두 구성해야 합니다. • Cisco ISE에서 EAP 체인이 비활성화된 경우 Microsoft 신청자에 대해 기본 인증 방법 만 구성해야 합니다. • 기본 인증 방법과 보조 인증 방법이 모두 None(없음)으로 구성된 경우 EAP 협상이 다음 메시지와 함께 실패할 수 있습니다. `Supplicant stopped responding to ISE(신청자가 ISE에 대한 응답을 중지함)`
Preferred EAP Protocol(기본 설정 **EAP** 프로토콜**)**	EAP-FAST, PEAP, LEAP, EAP-TLS, EAP-TTLS 및 EAP-MD5 옵션에서 기본 설정 EAP 프로토콜을 선택하려면 이 확인란을 선택합니다. 기본 설정 프로토콜을 지정하지 않으면 기본적으로 EAP-TLS가 사용됩니다.
EAP-TLS L-bit(EAP-TLS L 비트**)**	기본적으로 ISE로부터의 TLS 암호 사양 변경 메시지 및 암호화된 핸드셰이크 메시지 내 길이 포함 플래그(L 비트 플래그)를 예상하는 레거시 EAP 신청자를 지원하려면 이 확인란을 선택합니다.
Allow Weak Ciphers for EAP(EAP에 대해 약한 암호 허용**)**	이 옵션을 활성화하면 레거시 클라이언트가 약한 암호(RSA_RC4_128_SHA, RSA_RC4_128_MD5 등)를 사용하여 협상을 할 수 있습니다. 레거시 클라이언트가 약한 암호만 지원하는 경우에만 이 옵션을 활성화하는 것이 좋습니다. 이 옵션은 기본적으로 비활성화되어 있습니다. 참고 Cisco ISE는 EDH_RSA_DES_64_CBC_SHA 및 EDH_DSS_DES_64_CBC_SHA를 지원하지 않습니다.

필드 이름	사용 지침
Require Message Authenticator for all RADIUS Requests(모든 **RADIUS** 요청에 대해 메시지 인증자 필요**)**	이 옵션을 활성화하면 Cisco ISE는 RADIUS 메시지에 RADIUS 메시지 인증 자 속성이 있는지 확인합니다. 메시지 인증자 속성이 없으면 RADIUS 메시지가 삭제됩니다. 이 옵션을 활성화하면 스푸핑된 Access-Request 메시지 및 RADIUS 메시지 변조로부터 보호할 수 있습니다. RADIUS 메시지 인증자 속성은 전체 RADIUS 메시지의 MD5(Message Digest 5) 해시입니다. 참고 EAP는 기본적으로 메시지 인증자 속성을 사용하므로 이를 활성화하지 않아도 됩니다.

관련 항목

TACACS + 디바이스 관리를 위해 FIPS 및 비 FIPS 모드에서 허용되는 프로토콜 , 340 페이지
네트워크 액세스용으로 허용되는 프로토콜 정의, 995 페이지

PAC 옵션

다음 표에서는 **Allowed Protocols Services List(**허용되는 프로토콜 서비스 목록**)** 창에서 Use PACs(PAC 사용)를 선택하면 표시되는 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authentication(**인증**)** > **Allowed Protocols(**허용되는 프로토콜**)**입니다.

표 *136: PAC* 옵션

필드 이름	사용 지침
Use PAC(PAC 사용**)**	

필드 이름	사용 지침
	• Tunnel PAC Time To Live(터널 PAC Time to Live): TTL(Time to Live) 값은 PAC의 수명을 제한합니다. 수명 값과 단위를 지정합니다. 기본값은 90일입니다. 수명의 범위는 1~1,825일입니다. • Proactive PAC Update When: <n%> of PAC TTL is Left(PAC TTL이 <n%> 남았을 때 사전 PAC 업데이트): 업데이트 값을 통해 클라이언트가 유효한 PAC를 갖게 됩니다. Cisco ISE는 최초 정상 인증 이후 TTL에 의해 설정된 만료 시간 이전에 업데이트를 시작합니다. 업데이트 값은 남은 TTL 시간의 백분율입니다. 기본값은 90%입니다. • Allow Anonymous In-band PAC Provisioning(익명 대역 내 PAC 프로비저닝 허용): Cisco ISE가 클라이언트와의 보안 익명 TLS 핸드셰이크(Handshake)를 설정하고 EAP-MSCHAPv2와 함께 EAP-FAST 0단계를 사용하여 해당 핸드셰이크를 PAC에 프로비저닝하도록 하려면 이 확인란을 선택합니다. 익명 PAC 프로비저닝을 활성화하려면 내부 방법 EAP-MSCHAPv2 및 EAP-GTC를 모두 선택해야 합니다. • Allow Authenticated In-band PAC Provisioning(인증된 대역 내 PAC 프로비저닝 허용): Cisco ISE가 SSL 서버 측 인증을 사용하여 EAP-FAST의 0단계 중에 클라이언트에 PAC를 프로비저닝합니다. 이 옵션은 익명 프로비저닝보다 안전하기는 하지만, 서버 인증서 및 신뢰할 수 있는 루트 CA를 Cisco ISE에 설치해야 합니다. 이 옵션을 선택하는 경우 Cisco ISE가 PAC 프로비저닝을 정상적으로 인증한 후 액세스 수락 메시지를 클라이언트에 반환하도록 구성할 수 있습니다. • Server Returns Access Accept After Authenticated Provisioning(인증된 프로비저닝 이후 서버에서 액세스 수락 메시지 반환): Cisco ISE가 인증된 PAC 프로비저닝 이후 액세스 수락 패키지를 반환하도록 하려면 이 확인란을 선택합니다.

필드 이름	사용 지침
	• Allow Machine Authentication(머신 인증 허용): Cisco ISE가 최종 사용자 클라이언트에 머신 PAC를 프로비저닝하고 머신 자격 증명이 없는 최종 사용자 클라이언트에 대해 머신 인증을 수행하도록 하려면 이 확인란을 선택합니다. 머신 PAC는 요청 시(대역 내) 클라이언트에 프로비저닝할 수도 있고 관리자가(대역 외) 프로비저닝할 수도 있습니다. Cisco ISE가 최종 사용자 클라이언트로부터 유효한 머신 PAC를 받으면 머신 ID 세부정보가 PAC에서 추출되어 Cisco ISE 외부 ID 소스에서 확인됩니다. Cisco ISE는 머신 인증용 외부 ID 소스로 Active Directory만을 지원합니다. 이러한 세부정보가 올바르게 확인되고 나면 추가 인증이 수행되지 않습니다. 이 옵션을 선택하면 머신 PAC를 사용할 수 있는 시간 값을 입력할 수 있습니다. Cisco ISE는 만료된 머신 PAC를 받으면 최종 사용자 클라이언트로부터의 새 머신 PAC 요청을 대기하지 않고 최종 사용자 클라이언트에 새 머신 PAC를 자동으로 다시 프로비저닝합니다.

필드 이름	사용 지침
	• Enable Stateless Session Resume(스테이트리스 세션 재개 활성화): Cisco ISE가 EAP-FAST 클라이언트에 대해 권한 부여 PAC를 프로비저닝하고 EAP-FAST의 2단계(기본값 = 활성화됨)를 건너뛰도록 하려면 이 확인란을 선택합니다. 다음과 같은 경우에는 이 확인란의 선택을 취소합니다. • Cisco ISE가 EAP-FAST 클라이언트에 대한 권한 부여 PAC를 프로비저닝하지 않도록 하려는 경우 • 항상 EAP-FAST의 2단계를 수행하려는 경우 이 옵션을 선택하면 사용자 권한 부여 PAC의 권한 부여 기간을 입력할 수 있습니다. 이 기간이 지나면 PAC는 만료됩니다. Cisco ISE는 만료된 권한 부여 PAC를 받으면 2단계 EAP-FAST 인증을 수행합니다.

관련 항목

OOB TrustSec PAC, 1021 페이지
EAP-FAST용 PAC 생성, 952 페이지

RADIUS 프록시 서버 역할을 하는 Cisco ISE

Cisco ISE는 RADIUS 서버와 RADIUS 프록시 서버 모두로 작동할 수 있습니다. 프록시 서버 역할을 하는 경우 Cisco ISE는 NAS(Network Access Server)에서 인증 및 계정 관리 요청을 받고 이를 외부 RADIUS 서버로 전달합니다. Cisco ISE는 요청 결과를 수락하고 이를 NAS에 반환합니다.

Cisco ISE는 동시에 여러 외부 RADIUS 서버에 대한 프록시 서버 역할을 할 수 있습니다. RADIUS 서버 시퀀스에서 여기서 구성한 외부 RADIUS 서버를 사용할 수 있습니다. 외부 RADIUS 서버 페이지에는 Cisco ISE에서 정의한 모든 외부 RADIUS 서버가 나열됩니다. 필터 옵션을 사용하여 이름이나 설명 또는 둘 모두를 기준으로 특정 RADIUS 서버를 검색할 수 있습니다. 단순 인증 정책과 규칙 기반 인증 정책 모두에서는 RADIUS 서버 시퀀스를 사용하여 RADIUS 서버로 요청을 프록시 처리할 수 있습니다.

RADIUS 서버 시퀀스에서는 RADIUS 인증을 위해 RADIUS-Username 속성에서 도메인 이름을 제거합니다. EAP-Identity 속성을 사용하는 EAP 인증에는 이 도메인 제거가 적용되지 않습니다. RADIUS 프록시 서버는 RADIUS-Username 속성에서 사용자 이름을 가져오고 RADIUS 서버 시퀀스를 구성할 때 지정한 문자에서 해당 이름을 제거합니다. EAP 인증의 경우 RADIUS 프록시 서버는 EAP-Identity

속성에서 사용자 이름을 가져옵니다. RADIUS 서버 시퀀스를 사용하는 EAP 인증은 EAP-Identity 값과 RADIUS-Username 값이 동일한 경우에만 성공합니다.

외부 **RADIUS** 서버 구성

Cisco ISE가 외부 RADIUS 서버로 요청을 전달할 수 있도록 하려면 Cisco ISE에서 해당 외부 RADIUS 서버를 구성해야 합니다. 시간 초과 기간과 연결 시도 횟수를 정의할 수 있습니다.

시작하기 전에

- 이 섹션에서 생성하는 외부 RADIUS 서버는 단독으로는 사용할 수 없습니다. 즉, RADIUS 서버 시퀀스를 생성한 다음 이 섹션에서 생성하는 RADIUS 서버를 사용하도록 구성해야 합니다. 그러면 인증 정책에서 RADIUS 서버 시퀀스를 사용할 수 있습니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External RADIUS Servers(**외부 **RADIUS** 서버**)**를 선택합니다.

RADIUS 서버 페이지에는 Cisco ISE에 정의되어 있는 외부 RADIUS 서버의 목록이 표시됩니다.

단계 **2** 외부 RADIUS 서버를 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 **3** 필요한 대로 값을 입력합니다.

단계 **4** 외부 RADIUS 서버 컨피그레이션을 저장하려면 **Submit(**제출**)**을 클릭합니다.

RADIUS 서버 시퀀스 정의

Cisco ISE의 RADIUS 서버 시퀀스를 사용하면 NAD에서 외부 RADIUS 서버로 요청을 프록시할 수 있습니다. 그러면 요청이 처리되며 결과가 Cisco ISE로 반환되며, Cisco ISE는 응답을 NAD에 전달합니다.

RADIUS 서버 시퀀스 페이지에는 Cisco ISE에서 정의한 모든 RADIUS 서버 시퀀스가 나열됩니다. 이 페이지에서 RADIUS 서버 시퀀스를 생성, 편집 또는 복제할 수 있습니다.

시작하기 전에

- 이 절차를 시작하기 전에 프록시 서비스에 대해 기본적으로 파악해야 하며 관련 링크의 첫 번째 엔트리에 나와 있는 작업을 정상적으로 완료해야 합니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **RADIUS Server Sequences(RADIUS** 서버 시퀀스**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 필요한 대로 값을 입력합니다.

단계 4 정책에서 사용할 RADIUS 서버 시퀀스를 저장하려면 **Submit(**제출**)**을 클릭합니다.

TACACS+ 프록시 클라이언트 역할을 하는 Cisco ISE

Cisco ISE는 외부 TACACS+ 서버에 대한 프록시 클라이언트 역할을 할 수 있습니다. 프록시 클라이언트 역할을 하는 경우 Cisco ISE는 NAS(Network Access Server)에서 인증, 권한 부여 및 계정 관리 요청을 수신하여 외부 TACACS+ 서버로 전달합니다. Cisco ISE는 요청 결과를 수락하고 이를 NAS에 반환합니다.

TACACS+ External Servers(TACACS+ 외부 서버) 페이지에는 Cisco ISE에서 정의한 모든 외부 TACACS+ 서버가 나열됩니다. 필터 옵션을 사용하여 이름이나 설명 또는 둘 모두를 기준으로 특정 TACACS+ 서버를 검색할 수 있습니다.

Cisco ISE는 동시에 여러 외부 TACACS+ 서버에 대한 프록시 클라이언트 역할을 할 수 있습니다. 여러 외부 서버를 구성하려면 TACACS+ 서버 시퀀스 페이지를 사용할 수 있습니다. 자세한 내용은 TACACS+ 서버 시퀀스 설정 페이지를 참고하십시오.

외부 TACACS+ 서버 구성

Cisco ISE가 외부 TACACS 서버로 요청을 전달할 수 있도록 하려면 Cisco ISE에서 해당 외부 TACACS 서버를 구성해야 합니다. 시간 초과 기간과 연결 시도 횟수를 정의할 수 있습니다.

시작하기 전에

- 이 섹션에서 생성하는 외부 TACACS 서버를 정책에서 직접 사용할 수는 없습니다. TACACS 서버 시퀀스를 생성하고 이 섹션에서 생성하는 TACACS 서버를 사용하도록 구성해야 합니다. 그러면 정책 집합에서 TACACS 서버 시퀀스를 사용할 수 있습니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **TACACS External Servers(TACACS** 외부 서버**)**를 선택합니다.
Cisco ISE에 정의되어 있는 외부 TACACS 서버의 목록이 포함된 **TACACS External Servers(TACACS** 외부 서버**)** 페이지가 나타납니다.

단계 2 외부 TACACS 서버를 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 3 필요한 대로 값을 입력합니다.

단계 4 외부 TACACS 서버 컨피그레이션을 저장하려면 **Submit(**제출**)**을 클릭합니다.

TACACS+ 외부 서버 설정

다음 표에서는 TACACS External Servers(TACACS 외부 서버) 페이지의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이

스 관리**)** > **Network Resources(**네트워크 리소스**)** > **TACACS External Servers(TACACS** 외부 서버**)** 페이지입니다.

표 ***137: TACACS+*** 외부 서버 설정

필드	사용 지침
Name(이름)	TACACS+ 외부 서버의 이름을 입력합니다.
Description(설명)	TACACS+ 외부 서버 설정에 대한 설명을 입력합니다.
Host IP(호스트 IP)	원격 TACACS+ 외부 서버의 IP 주소(IPv4 또는 IPv6 주소)를 입력합니다.
Connection Port(연결 포트)	원격 TACACS+ 외부 서버의 포트 번호를 입력합니다. 포트 번호는 49입니다.
Timeout(시간 초과)	ISE가 외부 TACACS+ 서버로부터의 응답을 대기해야 하는 시간을 초 단위로 지정합니다. 기본값은 5초입니다. 유효한 값은 1~120입니다.
Shared Secret(공유 암호)	TACACS+ 외부 서버와의 연결을 보호하는 데 사용되는 텍스트 문자열입니다. 올바르게 구성되지 않은 경우 연결은 TACACS+ 외부 서버에 의해 거부됩니다.
Use Single Connect(단일 연결 사용)	TACACS 프로토콜은 연결에 세션을 연관시키는 두 가지 모드, 즉 Single Connect(단일 연결) 및 Non-Single Connect(비단일 연결)를 지원합니다. Single Connect(단일 연결) 모드에서는 클라이언트가 시작할 수 있는 여러 TACACS+ 세션에 대해 단일 TCP 연결을 재사용합니다. Non-Single Connect(비단일 연결)에서는 클라이언트가 시작하는 모든 TACACS+ 세션에 대해 새 TCP 연결이 열립니다. 각 세션 이후에는 TCP 연결이 닫힙니다. 트래픽이 많은 환경의 경우 Use Single Connect(단일 연결 사용) 확인란을 선택할 수 있으며 트래픽이 적은 환경의 경우에는 이 확인란의 선택을 취소할 수 있습니다.

TACACS+ 서버 시퀀스 정의

Cisco ISE의 TACACS+ 서버 시퀀스를 사용하면 NAD에서 외부 TACACS+ 서버로 요청을 프록시할 수 있습니다. 외부 TACACS+ 서버는 요청을 처리하고 결과를 Cisco ISE로 반환하며, Cisco ISE는 응답을 NAD에 전달합니다. TACACS+ Server Sequences(TACACS+ 서버 시퀀스) 페이지에는 Cisco ISE

에서 정의한 모든 TACACS+ 서버 시퀀스가 나열됩니다. 이 페이지에서 TACACS+ 서버 시퀀스를 생성, 편집 또는 복제할 수 있습니다.

시작하기 전에

- 프록시 서비스, Cisco ISE 관리자 그룹, 액세스 레벨, 권한 및 제한에 대해 기본적으로 이해하고 있어야 합니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- TACACS+ 서버 시퀀스에서 사용하려는 외부 TACACS+ 서버가 이미 정의되어 있는지 확인해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **TACACS External Server Sequence(TACACS** 외부 서버 시퀀스**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 필요한 값을 입력합니다.

단계 **4** 정책에서 사용할 TACACS+ 서버 시퀀스를 저장하려면 **Submit(**제출**)**을 클릭합니다.

TACACS+ 서버 시퀀스 설정

다음 표에서는 TACACS Server Sequence(TACACS 서버 시퀀스) 페이지의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **TACACS Server Sequence(TACACS** 서버 시퀀스**)** 페이지입니다.

표 ***138: TACACS+*** 서버 시퀀스 설정

필드	사용 지침
Name(이름)	TACACS 프록시 서버 시퀀스의 이름을 입력합니다.
Description(설명)	TACACS 프록시 서버 시퀀스에 대한 설명을 입력합니다.
서버 목록	필요한 TACACS 프록시 서버를 사용 가능 목록에서 선택합니다. 사용 가능 목록에는 TACACS External Services(TACACS 외부 서비스) 페이지에 구성된 TACACS 프록시 서버의 목록이 포함되어 있습니다.

필드	사용 지침
Logging Control(로깅 제어)	로깅 제어를 활성화하려면 선택합니다. • Local Accounting(로컬 계정 관리): 디바이스의 요청을 처리하는 서버가 계정 관리 메시지를 기록합니다. • Remote Accounting(원격 계정 관리): 디바이스의 요청을 처리하는 프록시 서버가 계정 관리 메시지를 기록합니다.
Username Stripping(사용자 이름 분리)	사용자 이름 접두사/접미사 분리: • Prefix Strip(접두사 분리): 접두사에서 사용자 이름을 분리하려면 선택합니다. 예를 들어 주체 이름이 acme\smith이고 구분 기호가 \이면 사용자 이름은 smith가 됩니다. 기본 구분 기호는 \입니다. • Suffix Strip(접미사 분리): 접미사에서 사용자 이름을 분리하려면 선택합니다. 예를 들어 주체 이름이 smith@acme.com이고 구분 기호가 @이면 사용자 이름은 smith가 됩니다. 기본 구분 기호는 @입니다.

네트워크 액세스 서비스

네트워크 액세스 서비스에는 요청에 사용되는 인증 정책 조건이 있습니다. 활용 사례별로 각기 다른 네트워크 액세스 서비스를 생성할 수 있습니다(예: 무선 802.1X, 무선 MAB 등). 네트워크 액세스 서비스를 생성하려면 허용되는 프로토콜 또는 서버 시퀀스를 구성합니다. 그런 다음 Policy Sets(정책 집합) 페이지에서 네트워크 액세스 정책에 대한 네트워크 액세스 서비스를 구성합니다.

네트워크 액세스용으로 허용되는 프로토콜 정의

허용되는 프로토콜에 따라 Cisco ISE가 네트워크 리소스에 대한 액세스 권한을 요청하는 디바이스와 통신하는 데 사용할 수 있는 프로토콜 집합이 정의됩니다. 허용되는 프로토콜 액세스 서비스는 인증 정책을 구성하기 전에 생성해야 하는 독립 엔티티이자 특정 활용 사례용으로 선택한 프로토콜이 포함되어 있는 객체입니다.

허용되는 프로토콜 서비스 페이지에는 사용자가 생성하는 허용되는 프로토콜 서비스가 모두 나열됩니다. 그리고 Cisco ISE에는 미리 정의된 기본 네트워크 액세스 서비스가 있습니다.

시작하기 전에

이 절차를 시작하기 전에 인증에 사용되는 프로토콜 서비스에 대해 기본적으로 파악해야 합니다.

- 다양한 데이터베이스에서 지원하는 인증 유형과 프로토콜을 파악하려면 이 장의 Cisco ISE 인증 정책 섹션을 검토해 주십시오.
- 네트워크에 적합한 항목을 선택할 수 있도록 각 프로토콜 서비스의 기능과 옵션을 파악하려면 PAC 옵션을 검토해 주십시오.
- 전역 프로토콜 설정을 정의했는지 확인해 주십시오.

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authentication(**인증**)** > **Allowed Protocols(**허용되는 프로토콜**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 필수 정보를 입력합니다.

단계 **4** 네트워크에 적합한 인증 프로토콜 및 옵션을 선택합니다.

단계 **5** PAC를 사용하려는 경우 적절한 항목을 선택합니다.

익명 PAC 프로비저닝을 활성화하려면 내부 방법인 EAP-MSCHAPv2 및 EAP-GTC(Extensible Authentication Protocol-Generic Token Card)를 모두 선택해야 합니다. 또한 Cisco ISE는 머신 인증용 외부 ID 소스로 Active Directory만을 지원합니다.

단계 **6** 허용되는 프로토콜 서비스를 저장하려면 **Submit(**제출**)**을 클릭합니다.

허용되는 프로토콜 서비스는 단순 및 규칙 기반 인증 정책 페이지에서 독립적인 객체로 표시됩니다. 이 객체는 다른 규칙에서 사용할 수 있습니다.

이제 단순 인증 정책 또는 규칙 기반 인증 정책을 생성할 수 있습니다.

내부 방법으로 EAP-MSCHAP를 비활성화하고 PEAP 또는 EAP-FAST에 대해 EAP-GTC 및 EAP-TLS 내부 방법을 활성화하면 ISE는 내부 방법 협상 중에 EAP-GTC 내부 방법을 시작합니다. 첫 번째 EAP-GTC 메시지가 클라이언트로 전송되기 전에 ISE는 ID 선택 정책을 실행하여 ID 저장소에서 GTC 비밀번호를 가져옵니다. 이 정책을 실행하는 동안 EAP 인증은 EAP-GTC와 동일합니다. EAP-GTC 내부 방법이 클라이언트에서 거부되어 EAP-TLS를 협상하는 경우에는 ID 저장소 정책이 다시 실행되지 않습니다. ID 저장소 정책이 EAP 인증 속성을 기준으로 하는 경우 예기치 않은 결과가 발생할 수 있습니다. 실제 EAP 인증(EAP-TLS)이 ID 정책 평가 이후에 설정되었기 때문입니다.

사용자에 대한 네트워크 액세스

네트워크 액세스를 위해 호스트는 네트워크 디바이스에 연결되고 네트워크 리소스를 사용하도록 요청합니다. 네트워크 디바이스는 새로 연결된 호스트를 식별하고, RADIUS 프로토콜을 전송 메커니즘으로 사용하여 사용자를 인증하고 권한을 부여하도록 Cisco ISE에 요청합니다.

Cisco ISE는 RADIUS 프로토콜을 통해 전송되는 프로토콜에 따라 네트워크 액세스 흐름을 지원합니다.

EAP 없는 **RADIUS** 기반 프로토콜

EAP가 포함되지 않은 RADIUS 기반 프로토콜은 다음과 같습니다.

- PAP(Password Authentication Protocol)
- CHAP
- MS-CHAPv1(Microsoft Challenge Handshake Authentication Protocol Version 1)
- MS-CHAP 버전 2(MS-CHAPv2)

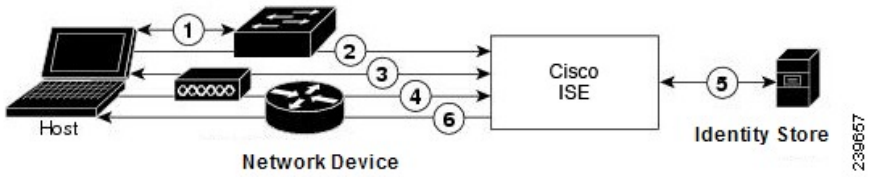
RADIUS 기반 비 EAP 인증 흐름

이 섹션에서는 EAP 인증을 수행하지 않는 RADIUS 기반 흐름에 대해 설명합니다. PAP 인증을 사용하는 RADIUS 기반 흐름은 다음과 같은 과정으로 수행됩니다.

1. 호스트가 네트워크 디바이스에 연결합니다.
2. 네트워크 디바이스가 사용 중인 특정 프로토콜(PAP, CHAP, MS-CHAPv1 또는 MS-CHAPv2)에 적합한 RADIUS 속성이 포함된 RADIUS 요청(Access-Request)을 Cisco ISE에 전송합니다.
3. Cisco ISE가 ID 저장소를 사용하여 사용자 자격 증명을 검증합니다.
4. 결정 사항을 적용할 네트워크 디바이스에 RADIUS 응답(Access-Accept 또는 Access-Reject)이 전송됩니다.

다음 그림에는 EAP를 수행하지 않는 RADIUS 기반 인증이 나와 있습니다.

그림 ***44: EAP***를 수행하지 않는 ***RADIUS*** 기반 인증



Cisco ISE에서 지원되는 비 EAP 프로토콜은 다음과 같습니다.

Password Authentication Protocol

PAP는 사용자가 양방향 핸드셰이크를 사용하여 자신의 ID를 설정하는 데 사용할 수 있는 간단한 방법을 제공합니다. PAP 비밀번호는 공유 암호로 암호화되며 복잡성이 가장 낮은 인증 프로토콜입니다. PAP는 반복되는 시행착오 공격으로부터 거의 보호 기능을 제공하지 않으므로 강력한 인증 방법이 아닙니다.

*Cisco ISE*의 *RADIUS* 기반 *PAP* 인증

Cisco ISE는 결과적으로 인증을 승인하거나 연결을 종료할 때까지 ID 저장소를 기준으로 사용자 이름 및 비밀번호 쌍을 확인합니다.

Cisco ISE에서 요건을 달리하여 서로 다른 보안 레벨을 동시에 사용할 수 있습니다. PAP는 양방향 핸드셰이킹 절차를 적용합니다. 인증이 성공할 경우 Cisco ISE는 승인을 반환합니다. 그렇지 않으면 Cisco ISE는 연결을 종료하거나 발신자에게 다른 옵션을 제공합니다.

발신자는 시도의 빈도와 시간을 전면적으로 제어합니다. 그러므로 강력한 인증 방법을 사용하는 서버에서는 PAP에 앞서 해당 방법을 제공하여 협상합니다. RFC 1334에서는 PAP를 정의합니다.

Cisco ISE는 RADIUS UserPassword 속성을 기반으로 하는 표준 RADIUS PAP 인증을 지원합니다. RADIUS PAP 인증은 모든 ID 저장소와 호환됩니다.

RADIUS PAP 인증 흐름에는 통과 및 실패한 시도 로깅이 포함됩니다.

CHAP(Challenge Handshake Authentication Protocol)

CHAP는 응답 시 단방향 암호화와 함께 시도 응답 메커니즘을 사용합니다. Cisco ISE는 CHAP를 통해 보안 레벨이 가장 높은 암호화 메커니즘에서 보안 레벨이 가장 낮은 암호화 메커니즘으로 하향식으로 협상하고 프로세스에서 전송되는 비밀번호를 보호할 수 있습니다. CHAP 비밀번호는 재사용이 가능합니다. 인증에 Cisco ISE 내부 데이터베이스를 사용하는 경우 PAP 또는 CHAP를 사용할 수 있습니다. Microsoft 사용자 데이터베이스에서는 CHAP가 작동하지 않습니다. RADIUS PAP와 달리 CHAP는 최종 사용자 클라이언트에서 AAA 클라이언트로 통신할 때 비밀번호를 암호화하는 데 더 높은 수준의 보안을 사용할 수 있습니다.

Cisco ISE는 RADIUS ChapPassword 속성을 기반으로 하는 표준 RADIUS CHAP 인증을 지원합니다. Cisco ISE는 내부 ID 저장소에 대한 RADIUS CHAP 인증만 지원합니다.

Microsoft Challenge Handshake Authentication Protocol Version 1

Cisco ISE는 RADIUS MS-CHAPv1 인증 및 비밀번호 변경 기능을 지원합니다. RADIUS MS-CHAPv1은 두 가지 버전의 비밀번호 변경 기능(Change-Password-V1 및 Change-Password-V2)을 포함합니다. Cisco ISE는 RADIUS MS-CHAP-CPW-1 속성을 기준으로 하는 Change-Password-V1을 지원하지 않으며 MS-CHAP-CPW-2 속성을 기준으로 하는 Change-Password-V2만 지원합니다. RADIUS MS-CHAPv1 인증 및 비밀번호 변경 기능이 지원되는 ID 소스는 다음과 같습니다.

- 내부 ID 저장소
- Microsoft Active Directory ID 저장소

Microsoft Challenge Handshake Authentication Protocol Version 2

RADIUS MS-CHAPv2 인증 및 비밀번호 변경 기능이 지원되는 ID 소스는 다음과 같습니다.

- 내부 ID 저장소
- Microsoft Active Directory ID 저장소

RADIUS 기반 **EAP** 프로토콜

EAP는 다양한 인증 유형을 지원하는 확장 가능한 프레임워크입니다. 이 섹션에서는 Cisco ISE에서 지원하는 EAP 방법에 대해 설명하고 다음과 같은 항목을 포함합니다.

간단한 **EAP** 방법

- EAP-Message Digest 5
- Lightweight EAP

인증에 **Cisco ISE** 서버 인증서를 사용하는 **EAP** 방법

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

위에 나열된 방법과는 별도로, 서버 및 클라이언트 인증 모두에 인증서를 사용하는 EAP 방법이 있습니다.

RADIUS 기반 EAP 인증 흐름

인증 프로세스에서 EAP가 사용될 때마다 해당 프로세스 전에 EAP 협상 단계가 수행되어 사용해야 하는 특정 EAP 방법 및 내부 방법(해당하는 경우)을 결정합니다. EAP 기반 인증은 다음과 같은 과정으로 수행됩니다.

1. 호스트가 네트워크 디바이스에 연결합니다.
2. 네트워크 디바이스가 호스트에 EAP 요청을 보냅니다.
3. 호스트가 EAP 응답으로 네트워크 디바이스에 회신을 합니다.
4. 네트워크 디바이스가 EAP-Message RADIUS 속성을 사용하여 호스트에서 받은 EAP 응답을 RADIUS Access-Request로 캡슐화한 다음 RADIUS Access-Request를 Cisco ISE로 보냅니다.
5. Cisco ISE가 RADIUS 패킷에서 EAP 응답을 추출하고 새 EAP 요청을 생성한 다음, 마찬가지로 EAP-Message RADIUS 속성을 사용하여 해당 요청을 RADIUS Access-Challenge로 캡슐화해 네트워크 디바이스로 보냅니다.
6. 네트워크 디바이스가 EAP 요청을 추출하여 호스트로 보냅니다.

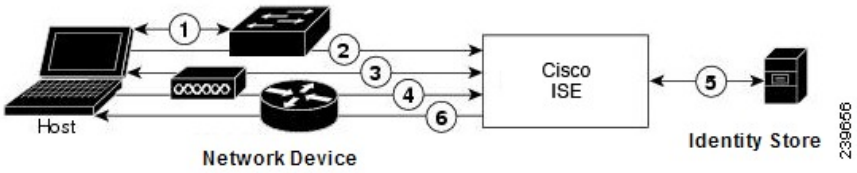
호스트와 Cisco ISE는 이러한 방식으로 EAP 메시지(RADIUS를 통해 전송되며 네트워크 디바이스를 통해 전달됨)를 간접 교환합니다. 이러한 방식으로 교환되는 최초 EAP 메시지 집합은 이후 인증을 수행하는 데 사용되는 특정 EAP 방법을 협상합니다.

그리고 이후 교환되는 EAP 메시지는 실제 인증을 수행하는 데 필요한 데이터를 전달하는 데 사용됩니다. 협상하는 특정 EAP 인증 방법에서 필요한 경우 Cisco ISE는 ID 저장소를 사용하여 사용자 자격 증명을 검증합니다.

Cisco ISE는 인증의 성공 여부를 확인하고 나면 RADIUS Access-Accept 또는 Access-Reject 메시지로 캡슐화된 EAP-Success 또는 EAP-Failure 메시지를 네트워크 디바이스로, 그리고 최종적으로는 호스트로 보냅니다.

다음 그림에는 EAP를 사용하는 RADIUS 기반 인증이 나와 있습니다.

그림 *45: EAP*를 사용하는 *RADIUS* 기반 인증



Extensible Authentication Protocol-Message Digest 5

EAP-MD5(Extensible Authentication Protocol-Message Digest 5)는 단방향 클라이언트 인증을 제공합니다. 서버는 클라이언트에게 임의 시도를 보냅니다. 클라이언트는 MD5를 사용하여 시도 및 해당 비밀번호를 암호화하여 응답에서 해당 ID를 검증합니다. 메시지 가로채기에서는 시도 및 응답을 인식할 수 있으므로 오픈 매체를 통해 사용되는 경우 EAP-MD5는 사전 공격에 취약합니다. 서버 인증이 발생하지 않기 때문에 스푸핑에도 취약합니다. Cisco ISE는 Cisco ISE 내부 ID 저장소에 대해 EAP-MD5 인증을 지원합니다. EAP-MD5 프로토콜을 사용하는 경우 호스트 조회도 지원됩니다.

Lightweight Extensible Authentication Protocol

Cisco ISE는 현재 Cisco Aironet 무선 네트워킹에만 LEAP(Lightweight Extensible Authentication Protocol)를 사용합니다. 이 옵션을 활성화하지 않으면 LEAP 인증을 수행하도록 구성된 Cisco Aironet 최종 사용자 클라이언트는 네트워크에 액세스할 수 없습니다. 모든 Cisco Aironet 최종 사용자 클라이언트가 EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)와 같이 다른 인증 프로토콜을 사용하는 경우 이 옵션을 비활성화하는 것이 좋습니다.

참고 사용자가 네트워크 디바이스 섹션에 정의된 AAA 클라이언트를 RADIUS(Cisco Aironet) 디바이스로 사용하여 네트워크에 액세스하는 경우 LEAP나 EAP-TLS 또는 둘 모두를 활성화해야 합니다. 그렇지 않으면 Cisco Aironet 사용자는 인증되지 않습니다.

Protected Extensible Authentication Protocol

PEAP(Protected Extensible Authentication Protocol)를 사용하면 상호 인증을 제공하고, 취약한 사용자 자격 증명에 대한 기밀성과 무결성을 보장하며, 수동(도청) 및 활성(메시지 가로채기) 공격으로부터 자신을 보호하고 암호화 키 관련 자료를 안전하게 생성할 수 있습니다. PEAP는 IEEE 802.1X 표준 및 RADIUS 프로토콜과 호환됩니다. Cisco ISE는 EAP-MS-CHAP(Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol), EAP-GTC(Extensible Authentication Protocol-Generic Token Card) 및 EAP-TLS 내부 방법을 사용하는 PEAP 버전 0(PEAPv0) 및 PEAP 버전 1(PEAPv1)을 지원합니다. Cisco SSC(Secure Services Client) 신청자는 Cisco ISE가 지원하는 모든 PEAPv1 내부 방법을 지원합니다.

*PEAP*를 사용하는 경우의 이점

PEAP를 사용하는 경우 다음과 같은 이점을 얻을 수 있습니다. PEAP는 널리 구현되고 광범위한 보안 검토가 이루어진 TLS를 기반으로 합니다. PEAP는 키를 파생시키지 않는 방법으로 키를 설정합니다. 터널 내에서 ID를 전송하고 내부 방법 교환 및 결과 메시지를 보호하며 단편화를 지원합니다.

PEAP 프로토콜용으로 지원되는 신청자

PEAP가 지원하는 신청자는 다음과 같습니다.

- Microsoft 내장 클라이언트 802.1X XP
- Microsoft 내장 클라이언트 802.1X Vista
- Cisco SSC(Secure Services Client) 릴리스 4.0
- Cisco SSC 릴리스 5.1
- Funk Odyssey Access Client 릴리스 4.72
- Intel 릴리스 12.4.0.0

PEAP 프로토콜 흐름

PEAP 대화는 세 부분으로 구분할 수 있습니다.

1. Cisco ISE 및 피어가 TLS 터널을 구축합니다. Cisco ISE는 인증서를 제시하고 피어는 인증서를 제시하지 않습니다. 피어와 Cisco ISE가 터널 내의 데이터를 암호화하기 위한 키를 생성합니다.
2. 내부 방법에 따라 터널 내의 흐름이 결정됩니다.
   - EAP-MS-CHAPv2 내부 방법 - EAP-MS-CHAPv2 패킷이 헤더 없이 터널 내부에서 이동합니다. 헤더의 첫 번째 바이트에는 유형 필드가 포함되어 있습니다. EAP MS CHAPv2 내부 방법은 비밀번호 변경 기능을 지원합니다. 사용자가 관리 포털을 통해 비밀번호 변경을 시도할 수 있는 횟수를 구성할 수 있습니다. 사용자 인증 시도가 이 횟수로 제한됩니다.
   - EAP-GTC 내부 방법 - PEAPv0 및 PEAPv1은 모두 EAP-GTC 내부 방법을 지원합니다. 지원되는 신청자는 EAP-GTC 내부 방법을 사용하는 PEAPv0을 지원하지 않습니다. EAP-GTC는 비밀번호 변경 기능을 지원합니다. 사용자가 관리 포털을 통해 비밀번호 변경을 시도할 수 있는 횟수를 구성할 수 있습니다. 사용자 인증 시도가 이 횟수로 제한됩니다.
   - EAP-TLS 내부 방법 - Windows 기본 제공 supplicant는 터널 설정 후의 메시지 프래그먼트화를 지원하지 않으며, 이는 EAP-TLS 내부 방법에 영향을 줍니다. Cisco ISE는 터널이 설정된 이후 외부 PEAP 메시지 단편화를 지원하지 않습니다. 터널 설정 중에는 PEAP 설명서에 지정된 대로 단편화가 작동합니다. PEAPv0에서는 EAP-TLS 패킷 헤더가 제거되고 PEAPv1에서는 EAP-TLS 패킷이 변경 없이 전송됩니다.
   - EAP-TLV(Extensible Authentication Protocol-Type, Length, Value) 확장 - EAP-TLV 패킷은 변경 없이 전송됩니다. EAP-TLV 패킷은 헤더와 함께 터널 내부에서 이동합니다.
3. 대화가 내부 방법에 도달한 경우 성공 및 실패 승인이 보호됩니다.

   클라이언트 EAP 메시지는 항상 RADIUS Access-Request 메시지에 포함되어 이동되며 서버 EAP 메시지는 항상 RADIUS Access-Challenge 메시지에 포함되어 이동됩니다. EAP-Success 메시지는 항상 RADIUS Access-Accept 메시지에 포함되어 이동됩니다. EAP-Failure 메시지는 항상 RADIUS Access-Reject 메시지에 포함되어 이동됩니다. 클라이언트 PEAP 메시지를 삭제하면 RADIUS 클라이언트 메시지가 삭제됩니다.

참고 Cisco ISE에서는 PEAPv1 통신 중에 EAP-Success 또는 EAP-Failure 메시지를 승인해야 합니다. 피어는 성공 또는 실패 메시지 수신을 승인하기 위해 빈 TLS 데이터 필드가 있는 PEAP 패킷을 다시 전송해야 합니다.

EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)

EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)는 상호 인증을 제공하고 공유 암호를 사용하여 터널을 설정하는 인증 프로토콜입니다. 터널은 비밀번호를 기반으로 하는 취약한 인증 방법을 보호하는 데 사용됩니다. PAC(Protected Access Credentials) 키라고 하는 공유 암호는 터널을 보호하는 동시에 클라이언트 및 서버를 상호 인증하는 데 사용됩니다.

*EAP-FAST*의 이점

EAP-FAST는 다른 인증 프로토콜에 비해 다음과 같은 이점을 제공합니다.

- 상호 인증 - EAP 서버는 피어 ID와 신뢰성을 확인할 수 있어야 하며, 피어는 EAP 서버의 신뢰성을 확인할 수 있어야 합니다.
- 수동 사전 공격에 대한 내성 - 대다수의 인증 프로토콜을 사용하려면 피어가 비밀번호를 일반 텍스트 또는 해시 형태로 명시적으로 EAP 서버에 제공해야 합니다.
- 메시지 가로채기 공격에 대한 내성 - 상호 인증 방식으로 보호되는 터널을 설정하는 경우 프로토콜은 공격자가 피어와 EAP 서버 사이의 통신에 정보를 주입하지 못하게 차단해야 합니다.
- MS-CHAPv2, GTC(Generic Token Card) 및 기타 인터페이스와 같은 다른 여러 비밀번호 인증 인터페이스를 지원할 수 있는 유연성 - EAP-FAST는 동일한 서버에서 여러 내부 프로토콜을 지원할 수 있는 확장 가능한 프레임워크입니다.
- 효율성 -무선 미디어를 사용하는 경우 피어는 컴퓨팅 및 성능 리소스 측면에서 제한적입니다. EAP-FAST를 사용하면 네트워크 액세스 통신에서 경량의 컴퓨팅 방식이 적용됩니다.
- 인증 서버의 사용자 단위 인증 상태 요건 최소화 - 대규모 구축에는 일반적으로 다수의 피어에 대해 인증 서버 역할을 하는 서버가 많이 있습니다. 네트워크에 액세스하는 데 사용자 이름 및 비밀번호를 사용하는 것과 같은 방식으로, 피어는 터널을 보호하기 위해 같은 공유 암호를 사용하는 것이 좋습니다. EAP-FAST는 서버가 캐시하고 관리해야 하는 사용자 단위 및 디바이스 상태를 최소화하는 동시에 피어가 하나의 강력한 공유 암호를 사용하도록 지원합니다.

EAP-FAST 흐름

EAP-FAST 프로토콜 흐름은 항상 다음 단계의 조합으로 구성됩니다.

1. 프로비저닝 단계 - EAP-FAST의 0단계입니다. 이 단계에서는 Cisco ISE와 피어 간에 공유되는 고유하고 강력한 암호(PAC)가 피어에 프로비저닝됩니다.
2. 터널 설정 단계 - 클라이언트와 서버가 PAC를 사용하여 서로 인증해 새 터널 키를 설정합니다. 이 터널 키는 대화의 나머지 부분을 보호하는 데 사용되며 메시지의 기밀성과 신뢰성을 유지합니다.
3. 인증 단계 - 터널 내에서 인증이 처리되는 단계로, 세션 키 생성 및 보호되는 방식의 종료가 수행됩니다. Cisco ISE에서는 EAP-FAST 버전 1 및 1a를 지원합니다.

Cisco 이외의 디바이스에서 MAB 활성화

Cisco 이외의 디바이스에서 MAB를 구성하려면 다음 설정을 순서대로 구성합니다.

단계 **1** 인증할 엔드포인트의 MAC 주소를 엔트포인트 데이터베이스에서 사용할 수 있는지 확인합니다. 이러한 엔드포인트는 직접 추가할 수도 있고 프로파일러 서비스에서 자동으로 프로파일링하도록 지정할 수도 있습니다.

단계 **2** Cisco 이외의 디바이스에서 사용하는 MAC 인증의 유형을 기준으로 하여 네트워크 디바이스 프로파일을 생성합니다(PAP, CHAP 또는 EAP-MD5).

a) **Administration(**관리**) > Network Resources(**네트워크 리소스**) > Network Device Profiles(**네트워크 디바이스 프로파일**)**를 선택합니다.

b) **Add(**추가**)**를 클릭합니다.

c) 네트워크 디바이스 프로파일의 이름과 설명을 입력합니다.

d) **Vendor(**벤더**)** 드롭다운 목록에서 벤더 이름을 선택합니다.

e) 디바이스가 지원하는 프로토콜의 확인란을 선택합니다. 디바이스가 RADIUS를 지원하는 경우 네트워크 디바이스에 사용할 RADIUS 사전을 선택합니다.

f) **Authentication/Authorization(**인증/권한 부여**)** 섹션을 펼쳐 플로우 유형, 속성 별칭 및 호스트 조회에 대한 디바이스의 기본 설정을 구성합니다.

g) **Host Lookup (MAB)(**호스트 조회**(MAB))** 섹션에서 다음을 수행합니다.

- 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**)** 확인란 및/또는 **Check Calling-Station-Id equals MAC Address(Calling-Station-Id**가 **MAC** 주소와 같은지 확인**)** 확인란을 선택합니다.

- Via PAP/ASCII(PAP/ASCII 사용) - Cisco ISE가 네트워크 디바이스 프로파일로부터의 PAP 요청을 호스트 조회 요청으로 탐지하도록 구성하려면 이 확인란을 선택합니다.

- Via CHAP(CHAP 사용) - Cisco ISE가 네트워크 디바이스로부터의 이 요청 유형을 호스트 조회 요청으로 탐지하도록 구성하려면 이 확인란을 선택합니다.

- Via EAP-MD5(EAP-MD5 사용) - 네트워크 디바이스 프로파일에 대해 EAP 기반 MD5 해시 인증을 활성화하려면 이 확인란을 선택합니다.

h) Permissions(권한), Change of Authorization (CoA)(CoA(Change of Authorization) 및 Redirect(리디렉션) 섹션에 필요한 세부정보를 입력하고 **Submit(**제출**)**을 클릭합니다.

맞춤형 NAD 프로파일을 생성하는 방법에 대한 자세한 내용은 Cisco Identity Services 엔진을 사용하는 네트워크 액세스 디바이스 프로파일을 참고하십시오.

단계 **3** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Network Resources(**네트워크 리소스**) > Network Devices(**네트워크 디바이스**)**를 선택합니다.

단계 **4** MAB를 활성화할 디바이스를 선택한 후 **Edit(**편집**)**를 클릭합니다.

단계 **5** Network Device(네트워크 디바이스) 페이지의 **Device Profile(**디바이스 프로파일**)** 드롭다운 목록에서 2단계에서 생성한 네트워크 디바이스 프로파일을 선택합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

참고 Cisco NAD의 경우 MAB와 웹/사용자 인증에 사용되는 Service-Type 값은 서로 다릅니다. 따라서 ISE는 Cisco NAD 사용 시 MAB를 웹 인증과 구분할 수 있습니다. Cisco 이외의 일부 NAD는 MAB 및 웹/사용자 인증 둘 다에 대해 Service-Type 속성에 같은 값을 사용하며, 이로 인해 액세스 정책에서 보안 문제가 발생할 수 있습니다. Cisco 이외의 디바이스에서 MAB를 사용하는 경우에는 네트워크 보안이 침해되지 않도록 추가 권한 부여 정책 규칙을 구성하는 것이 좋습니다. 예를 들어 프린터가 MAB를 사용하는 경우 권한 부여 정책 규칙을 ACL의 프린터 프로토콜 포트로 제한하도록 구성할 수 있습니다.

Cisco 디바이스에서 MAB 활성화

Cisco 디바이스에서 MAB를 구성하려면 다음 설정을 순서대로 구성합니다.

단계 **1** 인증할 엔드포인트의 MAC 주소를 엔트포인트 데이터베이스에서 사용할 수 있는지 확인합니다. 이러한 엔드포인트는 직접 추가할 수도 있고 프로파일러 서비스에서 자동으로 프로파일링하도록 지정할 수도 있습니다.

단계 **2** Cisco 디바이스에서 사용하는 MAC 인증의 유형을 기준으로 하여 네트워크 디바이스 프로파일을 생성합니다(PAP, CHAP 또는 EAP-MD5).

a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Network Resources(**네트워크 리소스**) > Network Device Profiles(**네트워크 디바이스 프로파일**)**를 선택합니다.

b) **Add(**추가**)**를 클릭합니다.

c) 네트워크 디바이스 프로파일의 이름과 설명을 입력합니다.

d) 디바이스가 지원하는 프로토콜의 확인란을 선택합니다. 디바이스가 RADIUS를 지원하는 경우 네트워크 디바이스에 사용할 RADIUS 사전을 선택합니다.

e) **Authentication/Authorization(**인증/권한 부여**)** 섹션을 펼쳐 플로우 유형, 속성 별칭 및 호스트 조회에 대한 디바이스의 기본 설정을 구성합니다.

f) **Host Lookup (MAB)(**호스트 조회**(MAB))** 섹션에서 다음을 수행합니다.

- Process Host Lookup(프로세스 호스트 조회) - 네트워크 디바이스 프로파일에 사용되는 호스트 조회용 프로토콜을 정의하려면 이 확인란을 선택합니다.

  디바이스 유형에 따라 사용 중인 프로토콜에 대해 **Check Password(**비밀번호 확인**)** 확인란 및/또는 **Check Calling-Station-Id equals MAC Address(Calling-Station-Id**가 **MAC** 주소와 같은지 확인**)** 확인란을 선택합니다.

- Via PAP/ASCII(PAP/ASCII 사용) - Cisco ISE가 네트워크 디바이스 프로파일로부터의 PAP 요청을 호스트 조회 요청으로 탐지하도록 구성하려면 이 확인란을 선택합니다.

- Via CHAP(CHAP 사용) - Cisco ISE가 네트워크 디바이스로부터의 이 요청 유형을 호스트 조회 요청으로 탐지하도록 구성하려면 이 확인란을 선택합니다.
- Via EAP-MD5(EAP-MD5 사용) - 네트워크 디바이스 프로파일에 대해 EAP 기반 MD5 해시 인증을 활성화하려면 이 확인란을 선택합니다.

g) Permissions(권한), Change of Authorization (CoA)(CoA(Change of Authorization) 및 Redirect(리디렉션) 섹션에 필요한 세부정보를 입력하고 **Submit(**제출**)**을 클릭합니다.

맞춤형 NAD 프로파일을 생성하는 방법에 대한 자세한 내용은 Cisco Identity Services 엔진을 사용하는 네트워크 액세스 디바이스 프로파일을 참고하십시오.

단계 **3** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Network Resources(**네트워크 리소스**) > Network Devices(**네트워크 디바이스**)**를 선택합니다.

단계 **4** MAB를 활성화할 디바이스를 선택한 후 **Edit(**편집**)**를 클릭합니다.

단계 **5** Network Device(네트워크 디바이스) 페이지의 **Device Profile(**디바이스 프로파일**)** 드롭다운 목록에서 2단계에서 생성한 네트워크 디바이스 프로파일을 선택합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

ISE Community Resource(ISE 커뮤니티 리소스)

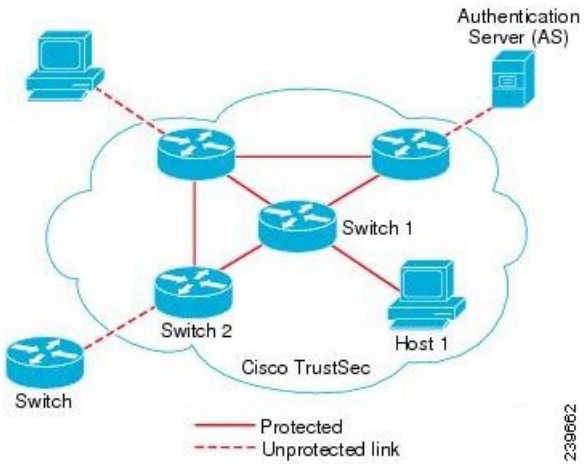
IP 전화기 인증 기능에 자세한 내용은 전화기 인증 기능을 참조하십시오.

TrustSec 아키텍처

Cisco TrustSec 솔루션은 보안 네트워크 구축을 위한 신뢰할 수 있는 네트워크 디바이스 클라우드를 설정합니다. Cisco TrustSec 클라우드의 각 디바이스는 인접 디바이스(피어)를 통해 인증됩니다. TrustSec 클라우드의 디바이스 간 통신은 암호화, 메시지 무결성 확인 및 데이터 경로 재생 보호 메커니즘 조합으로 보호됩니다. TrustSec 솔루션은 인증 중에 가져오는 디바이스 및 사용자 ID 정보를 사용하여 네트워크로 들어오는 패킷을 분류하거나 색상을 지정합니다. 이 패킷 분류는 패킷이 데이터 경로와 함께 보안 및 다른 정책 기준을 적용하기 위한 목적으로 올바르게 식별될 수 있도록, TrustSec 네트워크에 들어올 때 패킷에 태그를 지정하는 방식으로 유지 관리됩니다. SGT(Security Group Tag)라고도 하는 태그를 사용하면 Cisco ISE에서 트래픽을 필터링할 수 있도록 엔드포인트 디바이스가 SGT에 따라 작동하게 함으로써 액세스 제어 정책을 시행할 수 있습니다.

다음 그림에는 TrustSec 네트워크 클라우드의 예가 나와 있습니다.

그림 *46: TrustSec* 아키텍처



ISE 커뮤니티 리소스

Cisco TrustSec을 사용하여 네트워크 세그멘테이션을 간소화하고 보안을 개선하는 방법에 대한 자세한 내용은 Simplify Network Segmentation with Cisco TrustSec 및 Policy-Based Software Defined Segmentation and Cisco TrustSec Improve Security 백서를 참고하십시오.

Cisco TrustSec 플랫폼 지원 매트릭스의 전체 목록은 Cisco TrustSec Platform Support Matrix를 참고하십시오.

TrustSec에 사용 가능한 지원 문서의 전체 목록은 Cisco TrustSec을 참고하십시오.

TrustSec 커뮤니티 리소스의 전체 목록은 TrustSec Community를 참고하십시오.

TrustSec 구성 요소

주요 TrustSec 구성 요소는 다음과 같습니다.

- NDAC(Network Device Admission Control) - 신뢰할 수 있는 네트워크에서는 인증 중에 TrustSec 클라우드의 이더넷 스위치와 같은 각 네트워크 디바이스에 대해 피어 디바이스가 해당 자격 증명 및 신뢰 가능성을 확인합니다. NDAC는 IEEE 802.1x 포트 기반 인증을 사용하며 EAP(Extensible Authentication Protocol) 방법으로 EAP-FAST(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)를 사용합니다. MDAC 프로세스에서 인증과 권한 부여가 정상적으로 수행되면 IEEE 802.1AE 암호화를 위한 Security Association Protocol 협상이 진행됩니다.
- EAC(Endpoint Admission Control) - TrustSec 클라우드에 연결하는 엔드포인트 사용자 또는 디바이스에 대한 인증 프로세스입니다. EAC는 보통 액세스 레벨 스위치에서 진행됩니다. EAC에서 인증과 권한 부여가 정상적으로 수행되면 사용자나 디바이스에 SGT가 할당됩니다. 인증 및 권한 부여를 위한 EAC 액세스 방법은 다음과 같습니다.
  - 802.1X 포트 기반 인증
  - MAB(MAC 인증 바이패스)
  - WebAuth(웹 인증)

- SG(Security Group, 보안 그룹) - 액세스 제어 정책을 공유하는 사용자, 엔드포인트 디바이스 및 리소스의 그룹입니다. Cisco ISE의 관리자가 SG를 정의합니다. 새 사용자와 디바이스가 TrustSec 도메인에 추가되면 Cisco ISE는 이러한 새 엔티티를 적절한 보안 그룹에 할당합니다.
- SGT(Security Group Tag) - TrustSec 서비스는 고유한 16비트 보안 그룹 번호를 각 보안 그룹에 할당합니다. 이러한 번호는 TrustSec 도메인 내에서 전역적으로 적용됩니다. 스위치의 보안 그룹 수는 인증된 네트워크 엔티티의 수로 제한됩니다. 보안 그룹 번호는 수동으로 구성하지 않아도 됩니다. 보안 그룹 번호는 자동으로 생성되지만 IP-SGT 매핑용으로 SGT 범위를 예약할 수 있습니다.
- SGACL(Security Group Access Control List) - SGACL을 사용하면 할당된 SGT를 기반으로 하여 액세스 및 권한을 제어할 수 있습니다. 권한을 역할로 그룹화하면 보안 정책을 쉽게 관리할 수 있습니다. 디바이스를 추가할 때는 보안 그룹만 하나 이상 할당하면 됩니다. 그러면 디바이스가 적절한 권한을 즉시 받게됩니다. 보안 그룹을 수정하여 새 권한을 도입하거나 현재 권한을 제한할 수 있습니다.
- SXP(Security Exchange Protocol) - SXP(SGT Exchange Protocol)는 SGT/SGACL을 지원하는 하드웨어에 대한 SGT 가능 하드웨어 지원이 제공되지 않는 네트워크 디바이스로 IP-SGT 바인딩을 전파할 수 있도록 TrustSec 서비스용으로 개발된 프로토콜입니다.
- 환경 데이터 다운로드 - TrustSec 디바이스는 신뢰할 수 있는 네트워크에 처음으로 가입할 때 Cisco ISE에서 환경 데이터를 가져옵니다. 디바이스의 일부 데이터는 수동으로 구성할 수도 있습니다. 디바이스는 환경 데이터를 만료 전에 새로 고쳐야 합니다. TrustSec 디바이스는 Cisco ISE에서 다음 환경 데이터를 가져옵니다.
  - 서버 목록 - 클라이언트가 이후 RADIUS 요청(인증 및 권한 부여 둘 다)에 대해 사용할 수 있는 서버의 목록입니다.
  - 디바이스 SG - 디바이스 자체가 속하는 보안 그룹입니다.
  - 만료 시간 초과 - TrustSec 디바이스가 환경 데이터를 다운로드하거나 새로 고쳐야 하는 빈도를 제어하는 간격입니다.
- ID-포트 매핑 - 엔드포인트가 연결된 포트에서 스위치가 ID를 정의하고 이 ID를 사용하여 Cisco ISE 서버의 특정 SGT 값을 조회하는 방법입니다.

TrustSec 용어

다음 표에는 TrustSec 솔루션에서 일반적으로 사용되는 몇 가지 용어 및 TrustSec 환경에서 해당 용어의 의미가 나와 있습니다.

표 ***139: TrustSec*** 용어

용어	의미
신청자	신뢰할 수 있는 네트워크에 연결을 시도하는 디바이스입니다.

용어	의미
인증	각 디바이스를 신뢰할 수 있는 네트워크의 일부로 허용하기 전에 해당 디바이스의 ID를 확인하는 프로세스입니다.
승인	디바이스의 인증된 ID를 기준으로 하여 신뢰할 수 있는 네트워크의 리소스에 대한 액세스를 요청하는 디바이스에 대한 액세스 레벨을 결정하는 프로세스입니다.
액세스 제어	각 패킷에 할당된 SGT를 기준으로 하여 패킷당 액세스 제어를 적용하는 프로세스입니다.
보안 통신	신뢰할 수 있는 네트워크에서 각 링크를 통해 흐르는 패킷을 보호하기 위한 암호화, 무결성 및 데이터 경로 재생 보호 프로세스입니다.
TrustSec 디바이스	TrustSec 솔루션을 지원하는 Cisco Catalyst 6000 Series 또는 Cisco Nexus 7000 Series 스위치입니다.
TrustSec 가능 디바이스	TrustSec 가능 하드웨어와 소프트웨어가 포함된 TrustSec 가능 디바이스입니다. Nexus 운영체제가 포함된 Nexus 7000 Series 스위치를 예로 들 수 있습니다.
TrustSec 시드 디바이스	Cisco ISE 서버에 대해 직접 인증하는 TrustSec 디바이스입니다. 이 디바이스는 인증자이자 신청자로 작동합니다.
인그레스	Cisco TrustSec 솔루션이 활성화되어 있는 네트워크의 일부분인 TrustSec 가능 디바이스에 처음으로 도착하는 패킷은 SGT로 태그가 지정됩니다. 신뢰할 수 있는 네트워크로의 이 엔트리 포인트를 인그레스라고 합니다.
이그레스	Cisco TrustSec 솔루션이 활성화되어 있는 네트워크의 일부분인 TrustSec 가능 디바이스를 통과하는 패킷은 태그가 해제됩니다. 신뢰할 수 있는 네트워크로부터의 이 종료 포인트를 이그레스라고 합니다.

TrustSec용으로 지원되는 스위치 및 필수 구성 요소

Cisco TrustSec 솔루션을 통해 활성화되는 Cisco ISE 네트워크를 설정하려면 TrustSec 솔루션 및 기타 구성 요소를 지원하는 스위치가 필요합니다. 그리고 이러한 스위치 외에 IEEE 802.1X 프로토콜을 사용하는 ID 기반 사용자 액세스 제어를 위한 기타 구성 요소도 필요합니다. TrustSec을 지원하는 Cisco

스위치 플랫폼 및 필수 구성 요소의 전체 최신 목록은 Cisco TrustSec 활성화 인프라를 참고해 주십시오.

Cisco DNA 센터와의 통합

Cisco ISE는 Cisco DNA(Cisco Digital Network Architecture)의 핵심입니다. Cisco DNA 센터를 사용하면 네트워크를 자동화하여 비즈니스 민첩성을 제공할 수 있습니다. Cisco ISE와 Cisco DNA 센터를 통합하면 Cisco ISE에서 Cisco DNA 센터에 대한 엔드포인트 인증을 제공합니다.

Cisco DNA 센터에 Cisco ISE 연결

DNAC 사용 설명서 https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html의 Cisco DNA 센터 및 Cisco ISE 구성에 대한 요건 및 지침을 참조하십시오.

이 섹션에서는 Cisco DNA 센터의 Cisco ISE 컨피그레이션에 대한 추가 정보를 제공합니다.

- 비밀번호: Cisco DNA 센터는 Cisco ISE에 연결할 때 Cisco ISE 관리 사용자 이름과 비밀번호를 사용하여 Cisco ISE에 대한 액세스를 인증합니다. 시스템 비밀번호에 대한 자세한 내용은 *Cisco ISE* 관리 가이드*:* 시작하기의 Cisco ISE에 대한 관리 액세스 섹션을 참조하십시오.

  참고 Cisco DNA 센터 2.2.1.0 이전 버전에서는 초기 통합 단계를 수행하는 데 Cisco ISE CLI가 사용되었으므로, Cisco ISE CLI와 관리 사용자 이름 및 비밀번호가 동일해야 했습니다. Cisco DNA 센터 릴리스 2.2.1.0부터는 Cisco ISE CLI 사용이 중단되어 Cisco ISE CLI와 관리 사용자 이름 및 비밀번호가 같을 필요가 없습니다.

- API: Cisco DNA 센터는 ISE API를 호출하여 ISE의 일부를 구성합니다. Cisco ISE에서 API 액세스를 활성화하되, CSRF는 활성화하지 마십시오. 자세한 내용은 의 외부 RESTful 서비스 API 활성화 섹션을 참조하십시오.

- pxGrid: Cisco ISE는 pxGrid 컨트롤러이고, Cisco DNA 센터는 가입자입니다. Cisco ISE와 Cisco DNA 센터는 모두 SGT 및 SGACL 정보가 포함된 TrustSec(SD-Access) 콘텐츠를 모니터링합니다. Cisco ISE와 Cisco DNA 센터 간에 시스템 시계를 동기화합니다. Cisco ISE는 인증서를 사용하여 pxGrid에 연결합니다. pxGrid는 연결을 위해 Cisco DNA 센터에서 구성합니다. Cisco ISE의 pxGrid에 대한 자세한 내용은 *Cisco ISE* 관리 가이드*:* 구축의 pxGrid 노드 섹션을 참조하십시오.

  참고 Cisco ISE 2.4 이상에서는 pxGrid 2.0 및 pxGrid 1.0을 지원합니다. PxGrid 2.0은 Cisco ISE 구축 시 pxGrid 노드를 최대 4개까지 허용하지만, 현재 Cisco DNA 센터는 2개 이상의 pxGrid 노드를 지원하지 않습니다.

- Cisco ISE IP 주소: Cisco ISE PAN과 Cisco DNA 센터는 서로 직접 연결되어야 합니다. 프록시, 로드 밸런서 또는 가상 IP 주소를 통과할 수 없습니다. Cisco ISE와 Cisco DNA 센터는 서로에 대해 고정 주소를 구성합니다.

  Cisco ISE가 프록시를 사용하고 있지 않은지 확인합니다. 사용하는 경우 프록시에서 Cisco DNA 센터 IP를 제외합니다.

  다음 기능은 IPv4 및 IPv6 IP 주소를 지원합니다.

  - ERS(External RESTful Services) API
  - 관리자 REST API
  - SSH(Secure Shell) 프로토콜

- SXP: DNA 센터에는 SXP가 필요하지 않습니다. Cisco ISE를 DNA 관리 네트워크에 연결할 때 SXP를 활성화할 수 있습니다. 그러면 Cisco ISE는 TrustSec(SD-Access)에 대한 하드웨어 지원을 제공하지 않는 네트워크 디바이스와 통신할 수 있습니다.

  참고 TrustSec을 지원하도록 ISE 구축을 구성하거나 ISE가 Cisco DNA 센터와 통합된 경우 ISE 정책 서비스 노드를 SXP 전용으로 구성하지 마십시오. SXP는 TrustSec과 비 TrustSec 디바이스 간의 인터페이스입니다. TrustSec 지원 네트워크 디바이스와 통신하지 않습니다.

- Cisco ISE 연결용 인증서:
  - Cisco ISE 관리 인증서는 주체 이름 또는 SAN에 Cisco ISE IP 또는 FQDN을 포함해야 합니다.
  - ECDSA는 SSH 키, ISE SSH 액세스 또는 Cisco DNA 센터 및 Cisco ISE 연결용 인증서에는 지원되지 않습니다.
  - Cisco DNA 센터의 자가서명 인증서에는 cA:TRUE(RFC5280 section-4.2.19)가 포함된 기본 제약 조건 확장이 있어야 합니다.

참고 2.2.1.0 이전의 Cisco DNA 센터 버전에서는 SSH를 활성화해야 한다는 요건이 있었습니다. Cisco DNA 센터 릴리스 2.2.1.0부터는 SSH 사용이 중단되었으므로, SSH를 활성화할 필요가 없습니다.

TrustSec 대시보드

TrustSec 대시보드는 TrustSec 네트워크용 중앙 집중식 모니터링 툴입니다.

TrustSec 대시보드에는 다음 대시릿이 포함되어 있습니다.

- **Metrics(**메트릭**)**: 메트릭 대시릿에는 TrustSec 네트워크의 동작에 대한 통계가 표시됩니다.

- **Active SGT Sessions(**활성 **SGT** 세션**)**: 활성 SGT 세션 대시릿에는 네트워크에서 현재 활성 상태인 SGT 세션이 표시됩니다. 경보 대시릿에는 TrustSec 세션과 관련된 경보가 표시됩니다.
- **Alarms(**경보**):**
- **NAD/SGT/ACI Quick View(NAD/SGT/ACI** 간단히 보기**)**: 이 간단히 보기에는 NAD 및 SGT를 위한 TrustSec 관련 정보가 표시됩니다.
- **TrustSec Sessions/NAD Activity/ACI endpoint Activity Live Log(TrustSec** 세션**/NAD** 활동**/ACI** 엔드포인트 활동 라이브 로그**)**: 라이브 로그 대시릿에서 TrustSec 세션 링크를 클릭하여 활성 TrustSec 세션을 확인합니다. 또한 NAD에서 Cisco ISE로의 TrustSec 프로토콜 데이터 요청 및 응답과 관련한 정보도 확인할 수 있습니다.

메트릭

이 섹션에는 TrustSec 네트워크의 행동에 대한 통계가 표시됩니다. 기간(예: 지난 2시간, 지난 2일 등)과 차트 유형(예: 막대, 선형, 스플라인)을 선택할 수 있습니다.

그래프에는 최신 막대 값이 표시됩니다. 또한 이전 막대로부터의 백분율 변경 사항도 표시됩니다. 막대 값이 증가하는 경우 더하기 기호가 있는 녹색으로 표시됩니다. 막대 값이 감소하는 경우 빼기 기호가 있는 빨간색으로 표시됩니다.

그래프의 막대 위에 커서를 놓으면 값이 계산된 시간과 정확한 값이 <값:xxxx 날짜/시간: xxx> 형식으로 표시됩니다.

다음과 같은 메트릭을 확인할 수 있습니다.

SGT 세션	선택한 기간 중에 생성된 SGT 세션의 총 수가 표시됩니다. 참고 SGT 세션은 권한 부여 플로우의 일부분으로 SGT를 수신한 사용자 세션입니다.
사용 중인 SGT	선택한 기간 중에 사용된 고유 SGT의 총 수가 표시됩니다. 예를 들어 1시간 동안의 TrustSec 세션 수가 200개였는데 ISE가 권한 부여 응답에서 6가지 SGT 유형으로만 응답한 경우 그래프에는 이 시간에 대한 값이 6으로 표시됩니다.
경보	선택한 기간 중에 발생한 경보와 오류의 총 수가 표시됩니다. 오류는 빨간색으로 표시되며 경보는 노란색으로 표시됩니다.
사용 중인 NAD	선택한 기간 동안 TrustSec 인증에 참여한 고유 NAD의 수가 표시됩니다.

현재 네트워크 상태

대시보드의 가운데 섹션에는 TrustSec 네트워크의 현재 상태에 대한 정보가 표시됩니다. 페이지를 로드하면 그래프에 표시되는 값이 업데이트됩니다. Refresh Dashboard(대시보드 새로 고침) 옵션을 사용하여 이러한 값을 새로 고칠 수 있습니다.

활성 SGT 세션

이 대시릿에는 네트워크에서 현재 활성 상태인 SGT 세션이 표시됩니다. 가장 많이 사용된 상위 10개 또는 가장 적게 사용된 SGT를 확인할 수 있습니다. X축에는 SGT 사용량이 표시되고 Y축에는 SGT의 이름이 표시됩니다.

SGT에 대한 TrustSec 세션 세부정보를 확인하려면 원하는 SGT에 해당하는 바를 클릭합니다. 그러면 해당 SGT와 관련된 TrustSec 세션의 세부정보가 Live Log 대시릿에 표시됩니다.

경보

이 대시릿에는 TrustSec 세션과 관련된 경보가 표시됩니다. 다음과 같은 세부정보를 확인할 수 있습니다.

- 경보 심각도 - 경보의 심각도 레벨을 나타내는 아이콘이 표시됩니다.
  - 높음 - TrustSec 네트워크에서 장애를 나타내는 경보가 포함됩니다(예: 디바이스가 해당 PAC를 새로 고침하지 못함). 빨간색 아이콘으로 표시됩니다.
  - 중간 - 네트워크 디바이스의 잘못된 컨피그레이션을 나타내는 경고가 포함됩니다(예: 디바이스가 CoA 메시지를 수락하지 못함). 노란색으로 표시됩니다.
  - 낮음 - 네트워크 행동의 업데이트와 일반적인 정보가 포함됩니다(예: TrustSec의 컨피그레이션 변경). 파란색으로 표시됩니다.
- 경보 설명
- 이 경보 카운터를 마지막으로 재설정한 이후 경보가 발생한 횟수입니다.
- 마지막 경보 발생 시간

간단히 보기

간단히 보기 대시릿에는 NAD에 대한 TrustSec 관련 정보가 표시됩니다. SGT에 대한 TrustSec 관련 정보도 확인할 수 있습니다.

NAD 간단히 보기

세부정보를 확인하려는 TrustSec 네트워크 디바이스의 이름을 검색 상자에 입력하고 **Enter** 키를 누릅니다. 검색 상자에서는 사용자가 텍스트 상자에 입력을 할 때 드롭다운에 일치하는 디바이스 이름을 필터링하고 표시하는 자동 완성 기능이 제공됩니다.

이 대시릿에는 다음 정보가 표시됩니다.

- **NDG**: 이 네트워크 디바이스가 속하는 NDG(Network Device Group)가 나열됩니다.
- **IP Address(IP 주소)**: Live Log(라이브 로그) 대시릿에서 NAD 활동 세부정보를 보려면 이 링크를 클릭합니다.
- **Active sessions(활성 세션)**: 이 디바이스에 연결된 활성 TrustSec 세션의 수입니다.
- **PAC expiry(PAC 만료)**: PAC 만료 날짜입니다.

- **Last Policy Refresh(**마지막 정책 새로 고침**)**: 마지막으로 정책을 다운로드한 날짜입니다.
- **Last Authentication(**마지막 인증**)**: 이 디바이스에 대한 마지막 인증 보고서 타임스탬프입니다.
- **Active SGTs(**활성 **SGT)**: 이 네트워크 디바이스와 관련된 활성 세션에서 사용되는 SGT가 나열됩니다. 괄호안에 표시되는 숫자는 현재 이 SGT를 사용 중인 세션의 수를 나타냅니다. Live Log(라이브 로그) 대시릿에서 TrustSec 세션 세부정보를 보려면 SGT 링크를 클릭합니다.

Show Latest Logs(최신 로그 표시) 옵션을 사용하여 디바이스에 대한 NAD 활동 라이브 로그를 볼 수 있습니다.

SGT 간단히 보기

세부정보를 확인할 SGT의 이름을 검색 상자에 입력하고 **Enter** 키를 누릅니다.

이 대시릿에는 다음 정보가 표시됩니다.

- **Value(**값**)**: SGT 값(10진수 및 16진수 둘 다)입니다.
- **Icon(**아이콘**)**: 이 SGT에 할당된 아이콘이 표시됩니다.
- **Active sessions(**활성 세션**)**: 현재 이 SGT를 사용 중인 활성 세션의 수입니다.
- **Unique users(**고유 사용자**)**: 활성 세션에 이 SGT가 포함되어 있는 고유 사용자 이름의 수입니다.
- **Updated NADs(**업데이트 **NAD)**: 이 SGT용 정책을 다운로드한 NAD의 수입니다.

ACI 간단히 보기

이 대시릿에는 다음 정보가 표시됩니다.

- **SDA SGTs(SDA SGT)**: Cisco ISE에서 Cisco SD-Access로 전송한 SGT의 수를 나열합니다.
- **ACI EPGs(ACI EPG)**: Cisco ACI에서 Cisco ISE가 학습한 EPG 수를 나열합니다.
- **SDA Bindings(SDA** 바인딩**)**: Cisco ISE에서 Cisco SD-Access로 전송한 바인딩 수를 나열합니다.
- **ACI Bindings(ACI** 바인딩**)**: Cisco ACI에서 Cisco ISE가 확인한 바인딩 수를 나열합니다.
- **SDA VNs(SDA VN)**: Cisco SD-Access에서 Cisco ISE가 학습한 가상 네트워크의 수를 나열합니다.
- **ACI VNs(ACI VN)**: Cisco ACI에서 Cisco ISE가 학습한 가상 네트워크의 수를 나열합니다.
- **SDA Extended VNs(SDA** 확장 **VN)**: Cisco SD-Access 도메인에서 Cisco ACI 도메인으로 전송된 확장 가상 네트워크의 수를 나열합니다.
- **SDA Tenant(SDA** 테넌트**)**: Cisco SD-Access에서 Cisco ISE와 공유하는 테넌트의 이름을 표시합니다.
- **ACI Tenants(ACI** 테넌트**)**: Cisco ACI에서 Cisco SD-Access와 공유하는 테넌트 수를 나열합니다.
- **SDA Domain ID(SDA** 도메인 **ID)** : Cisco SD-Access의 도메인 ID 번호를 표시합니다.
- **ACI Domain ID(ACI** 도메인 **ID)**: Cisco ACI의 도메인 ID 번호를 표시합니다.

- **Peering State(**피어링 상태**)**: Cisco SD-Access 도메인과 Cisco ACI 도메인 간의 피어링 관계의 현재 상태를 표시합니다.

Cisco SD-Access(Cisco Software-Defined Access) 및 Cisco ACI(Cisco Application Centric Infrastructure)에 대해 자세히 알아 보려면 TrustSec-Cisco ACI 통합, 1063 페이지 및 Cisco ACI 및 Cisco SD-Access와 가상 네트워크 인식 통합, 1067 페이지를 참조하십시오.

라이브 로그

활성 TrustSec 세션(응답의 일부로 SGT가 있는 세션)을 보려면 **TrustSec Sessions(TrustSec** 세션**)** 링크를 클릭합니다.

NAD에서 Cisco ISE로의 TrustSec 프로토콜 데이터 요청 및 응답과 관련한 정보를 보려면 **NAD Activity(NAD** 활동**)** 링크를 클릭합니다.

Cisco ACI에서 Cisco ISE가 확인한 IP-SGT 정보를 보려면 **ACI endpoint Activity(ACI** 엔드 포인트**)** 활동 링크를 클릭합니다.

TrustSec 전역 설정 구성

Cisco ISE가 TrustSec 서버로 작동하고 TrustSec 서비스를 제공하도록 하려면 몇 가지 전역 TrustSec 설정을 정의해야 합니다.

시작하기 전에

- 전역 TrustSec 설정을 구성하기 전에 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **EAP-FAST** > **EAP-FAST Settings(EAP-FAST** 설정**)**를 선택하여 전역 EAP-FAST 설정을 정의했는지 확인합니다.

  기관 ID 정보 설명은 사용 중인 Cisco ISE 서버 이름으로 변경할 수 있습니다. 이 설명은 엔드포인트 클라이언트에 자격 증명을 보내는 Cisco ISE 노드를 설명하는 사용자가 쉽게 이해할 수 있는 문자열입니다. Cisco TrustSec 아키텍처의 클라이언트는 IEEE 802.1X 인증용 EAP 방법으로 EAP-FAST를 실행하는 엔드포인트이거나, NDAC(Network Device Access Control)를 수행하는 신청자 네트워크 디바이스일 수 있습니다. 클라이언트는 PAC(Protected Access Credentials) TLV(Ttype-Length-Value) 정보에서 이 문자열을 검색할 수 있습니다. 기본값은 Identity Services Engine입니다. NDAC 인증 시 Cisco ISE PAC 정보가 네트워크 디바이스에서 고유하게 식별될 수 있도록 값을 변경해야 합니다.

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **TrustSec** > **Settings(**설정**)** > **General TrustSec Settings(**일반 **TrustSec** 설정**)**

단계 **2** 필드에 값을 입력합니다. 필드에 대한 자세한 내용은 다음을 참조하십시오. 일반 TrustSec 설정, 1015 페이지

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

• TrustSec 디바이스 구성, 1020 페이지

일반 TrustSec 설정

Cisco ISE가 TrustSec 서버로 작동하고 TrustSec 서비스를 제공하도록 하려면 전역 TrustSec 설정을 정의하십시오. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Settings(**설정**) > General TrustSec Settings(**일반 **TrustSec** 설정**)**를 선택합니다.

TrustSec 구축 확인

이 옵션을 사용하면 모든 네트워크 디바이스에 최신 TrustSec 정책이 구축되어 있는지 확인할 수 있습니다. Cisco ISE와 네트워크 디바이스에 구성된 정책 간에 불일치가 있는 경우 경보는 **Work Centers(**작업 센터**) > TrustSec** 및 **Dashboard and Home(**대시보드 및 홈**) > Summary(**요약**)** 아래의 Alarms(경보) dashlet에 표시됩니다. 다음 경보가 TrustSec 대시보드에 나타납니다.

- 확인 프로세스가 시작되거나 완료될 때마다 정보 아이콘과 함께 경보가 표시됩니다.
- 새 구축 요청으로 인해 확인 프로세스가 취소된 경우 정보 아이콘과 함께 경보가 표시됩니다.
- 확인 프로세스가 오류와 함께 실패할 경우 경고 아이콘과 함께 경보가 표시됩니다. 네트워크 디바이스와의 SSH 연결을 열지 못하거나 네트워크 디바이스를 사용할 수 없거나 Cisco ISE와 네트워크 디바이스에 구성된 정책 간에 불일치가 있는 경우를 예로 들 수 있습니다.

Verify Deployment(구축 확인**)** 옵션은 아래 창에서도 사용할 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 :

- **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Security Groups(**보안 그룹**)**
- **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Security Group ACLs(**보안 그룹 **ACL)**
- **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Egress Policy(**이그레스 정책**) > Matrix(**매트릭스**)**
- **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Egress Policy(**이그레스 정책**) > Source Tree(**소스 트리**)**
- **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Egress Policy(**이그레스 정책**) > Destination Tree(**대상 트리**)**

Automatic Verification After Every Deploy(구축 완료 시마다 자동 확인**)**: Cisco ISE가 구축이 완료될 때마다 모든 네트워크 디바이스에서 업데이트를 확인하도록 하려면 이 확인란을 선택합니다. 구축 프로세스가 완료되면 **Time after Deploy Process(**구축 후 프로세스 시간**)** 필드에 지정한 시간이 지나고 확인 프로세스가 시작됩니다.

Time After Deploy Process(구축 후 프로세스 시간**)**: 구축 프로세스가 완료된 후 확인 프로세스를 시작하기 전에 Cisco ISE가 대기할 시간을 지정합니다. 유효 범위는 10~60분입니다.

대기 시간 동안 새 구축 요청이 수신되거나 다른 확인이 진행 중인 경우 현재 확인 프로세스가 취소됩니다.

Verify Now(지금 확인**)**: 확인 프로세스를 즉시 시작하려면 이 옵션을 클릭합니다.

PAC(Protected Access Credential)

- **Tunnel PAC Time to Live(**터널 **PAC Time to Live)**:

  PAC의 만료 시간을 지정합니다. 터널 PAC는 EAP-FAST 프로토콜용 터널을 생성합니다. 초, 분, 시간, 일 또는 주 단위로 시간을 지정할 수 있습니다. 기본값은 90일입니다. 유효 범위는 다음과 같습니다.

  - 1~157680000초
  - 1~2628000분
  - 1~43800시간
  - 1~1825일
  - 1~260주

- **Proactive PAC Update Will Occur After(**사전 **PAC** 업데이트 수행까지의 시간**)**: Cisco ISE는 터널 PAC TTL이 구성된 백분율만큼 남아 있으면 인증 성공 후 클라이언트에 새 PAC를 사전 제공합니다. 서버는 PAC 만료 전에 첫 번째 인증이 성공하면 터널 PAC 업데이트를 시작합니다. 이 메커니즘을 통해 유효한 PAC를 사용하여 클라이언트가 업데이트됩니다. 기본값은 10%입니다.

보안 그룹 태그 번호 지정

- **System will Assign SGT Numbers(**시스템이 **SGT** 번호 할당**)**: Cisco ISE가 모든 SGT 번호를 자동으로 생성하도록 하려면 이 옵션을 선택합니다.
- **Except Numbers in Range(**다음 범위의 번호 제외**)**: 수동 컨피그레이션용으로 SGT 번호 범위를 예약하려면 이 옵션을 선택합니다. Cisco ISE가 SGT 생성 중에 이 범위의 값을 사용하지 않습니다.
- **User Must Enter SGT Numbers Manually(**사용자가 수동으로 **SGT** 번호를 입력해야 함**)**: SGT 번호를 수동으로 정의하려면 이 옵션을 선택합니다.

APIC EPG에 대한 보안 그룹 태그 번호 지정

Security Group Tag Numbering for APIC EPGs(APIC EPG에 대한 보안 그룹 태그 번호 지정**)**: 이 확인란을 선택하고 APIC에서 학습된 EPG에 따라 생성된 SGT에 사용할 번호의 범위를 지정합니다.

자동 보안 그룹 생성

Auto Create Security Groups When Creating Authorization Rules(권한 부여 규칙 생성 시 보안 그룹 자동 생성**)**: 권한 부여 정책 규칙을 생성하는 동안 SGT를 자동으로 생성하려면 이 확인란을 선택합니다.

이 옵션을 선택하면 **Authorization Policy(**권한 부여 정책**)** 창의 상단에 "Auto Security Group Creation is On(자동 보안 그룹 생성 설정)" 메시지가 표시됩니다.

자동으로 생성된 SGT는 규칙 속성에 따라 이름이 지정됩니다.

참고 해당 권한 부여 정책 규칙을 삭제해도 자동 생성된 SGT는 삭제되지 않습니다.

기본적으로 이 옵션은 새로 설치 또는 업그레이드한 후 비활성화됩니다.

- **Automatic Naming Options(**자동 이름 지정 옵션**)**: 이 옵션을 사용하여 자동으로 생성되는 SGT에 대해 명명 규칙을 정의합니다.

  (필수) **Name Will Include(**이름에 포함할 항목**)**: 다음 옵션 중 하나를 선택합니다.

  - **Rule name(**규칙 이름**)**
  - **SGT number(SGT** 번호**)**
  - **Rule name and SGT number(**규칙 이름 및 **SGT** 번호**)**

  기본적으로 **Rule name(**규칙 이름**)** 옵션이 선택되어 있습니다.

  필요한 경우 SGT 이름에 다음 정보를 추가할 수 있습니다.

  - **Policy Set Name(**정책 집합 이름**)**(정책 집합이 활성화되어 있어야 이 옵션을 사용할 수 있음)
  - **Prefix(**접두사**)**(최대 8자)
  - **Suffix(**접미사**)**(최대 8자)

  Cisco ISE는 선택한 항목에 따라 **Example Name(**예시 이름**)** 필드에 샘플 SGT 이름을 표시합니다.

  이름이 같은 SGT가 있는 경우 ISE는 SGT 이름에 *_x*를 추가합니다. 여기서 *x*는 첫 번째 값이며 1부터 시작합니다(현재 이름에서 1이 사용되지 않는 경우). 새 이름이 32자보다 길면 Cisco ISE는 처음 32자 이후의 문자를 자릅니다.

호스트 이름의 **IP SGT** 정적 매핑

IP SGT Static Mapping of Hostnames(호스트 이름의 **IP SGT** 정적 매핑**)**: FQDN 및 호스트 이름을 사용하는 경우 Cisco ISE는 매핑을 구축하고 구축 상태를 확인하는 동안 PAN 및 PSN 노드에서 해당 IP 주소를 찾습니다. 이 옵션을 사용하여 DNS 쿼리에서 반환하는 IP 주소에 대해 생성되는 매핑 수를 지정할 수 있습니다. 다음 옵션 중 하나를 선택할 수 있습니다.

- **Create mappings for all IP addresses returned by a DNS query(DNS** 쿼리에서 반환하는 모든 **IP** 주소에 대한 매핑 생성**)**
- **Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query(DNS** 쿼리로 반환되는 첫 번째 **IPv4** 주소 및 **IPv6** 주소에 대해서만 매핑 생성**)**

네트워크 디바이스용 **TrustSec HTTP** 서비스

- **Enable HTTP Service(HTTP** 서비스 활성화**)**: HTTP를 사용하여 포트 9063을 통해 네트워크 디바이스에 TrustSec 데이터를 전송합니다.
- **Include entire response payload body in Audit(**감사에 전체 응답 페이로드 본문 포함**)**: 감사 로그에 전체 TrustSec HTTP 응답 페이로드 본문을 표시하려면 이 옵션을 활성화합니다. 이 옵션을 사용하면 성능이 크게 저하될 수 있습니다. 이 옵션을 비활성화하면 HTTP 헤더, 상태 및 인증 정보만 기록됩니다.

관련 항목

TrustSec 아키텍처, 1005 페이지
TrustSec 구성 요소, 1006 페이지
TrustSec 전역 설정 구성, 1014 페이지

TrustSec 매트릭스 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > Settings(**설정**) > TrustSec Matrix Settings(TrustSec** 매트릭스 설정**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Settings(**설정**) > TrustSec Matrix Settings(TrustSec** 매트릭스 설정**)**.

단계 **3** TrustSec Matrix Settings(TrustSec 매트릭스 설정) 페이지에서 필요한 세부정보를 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

TrustSec 매트릭스 설정

다음 표에서는 TrustSec Matrix Settings(TrustSec 매트릭스 설정) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Settings(**설정**) > TrustSec Matrix Settings(TrustSec** 매트릭스 설정**)**입니다.

표 *140: TrustSec* 매트릭스 설정 구성

필드 이름	사용 지침
Allow Multiple SGACLs(여러 **SGACL** 허용**)**	셀 하나에서 여러 SGACL을 허용하려면 이 확인란을 선택합니다. 이 옵션을 선택하지 않으면 Cisco ISE는 셀당 하나의 SGACL만 허용합니다. 기본적으로 이 옵션은 새로 설치한 후 비활성화됩니다. 업그레이드 후 Cisco ISE는 이그레스 셀을 스캔하며, 여러 SGACL이 할당된 셀이 하나 이상 식별되는 경우 관리자가 셀 하나에 여러 SGACL을 추가할 수 있습니다. 그렇지 않은 경우에는 셀당 하나의 SGACL만 허용됩니다. 참고 여러 SGACL을 비활성화하기 전에 SGACL이 하나만 포함되도록 여러 SGACL을 포함하는 셀을 편집해야 합니다.
Allow Monitoring(모니터링 허용**)**	매트릭스의 모든 셀에 대해 모니터링을 활성화하려면 이 확인란을 선택합니다. 모니터링을 비활성화하면 Monitor All(모두 모니터링) 아이콘이 흐리게 표시되며 Edit Cell(셀 편집) 대화 상자에서 Monitor(모니터) 옵션이 비활성화됩니다. 기본적으로 모니터링은 새로 설치한 후 비활성화됩니다. 참고 매트릭스 레벨에서 모니터링을 비활성화하기 전에 현재 모니터링되고 있는 셀에 대해 모니터링을 비활성화해야 합니다.
Show SGT Numbers(SGT 번호 표시**)**	매트릭스 셀에서 SGT 값(10진수 및 16진수 둘 다)을 표시하거나 숨기려면 이 옵션을 사용합니다. 기본적으로 SGT 값은 셀에 표시됩니다.
모양 설정**(Appearance Settings)**	다음 옵션을 사용할 수 있습니다. • **Custom settings(**맞춤형 설정**)**: 처음에는 기본 테마(패턴이 없는 색상)가 표시됩니다. 원하는 색상 및 패턴을 설정할 수 있습니다. • **Default settings(**기본 설정**)**: 패턴이 없는 색상에 대한 사전 정의된 목록(편집 불가)입니다. • **Accessibility settings(**접근성 설정**)**: 패턴이 있는 색상에 대한 사전 정의된 목록(편집 불가)입니다.

필드 이름	사용 지침
Color/Pattern(색상/패턴**)**	매트릭스를 보다 쉽게 읽을 수 있도록 셀 내용에 따라 매트릭스 셀에 색상과 패턴을 적용할 수 있습니다. 다음 표시 유형을 사용할 수 있습니다. • **Permit IP/Permit IP Log(IP** 허용**/IP** 로그 허용**)**: 셀 내부에 구성됩니다. • **Deny IP/Deny IP Log(IP** 거부**/IP** 로그 거부**)**: 셀 내에 구성됩니다. • **SGACLs**: 셀 내에 구성되는 SGACL에 적용됩니다. • **Permit IP/Permit IP Log(Inherited)(IP** 허용**/IP** 로그 허용**(**상속됨**))**: 기본 정책에서 가져옵니다(구성되지 않은 셀에 해당). • **Deny IP/Deny IP Log(Inherited)(IP** 거부**/IP** 로그 거부**(**상속됨**))**: 기본 정책에서 가져옵니다(구성되지 않은 셀에 해당). • **SGACLs(Inherited)(SGACL(**상속됨**))**: 기본 정책에서 가져옵니다(구성되지 않은 셀에 해당).

관련 항목

이그레스 정책, 1031 페이지
매트릭스 보기, 1032 페이지
TrustSec 매트릭스 설정 구성, 1018 페이지

TrustSec 디바이스 구성

Cisco ISE가 TrustSec이 활성화된 디바이스에서 요청을 처리할 수 있도록 하려면 Cisco ISE에서 TrustSec이 활성화된 이러한 디바이스를 정의해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Network Device(**네트워크 디바이스**)**

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Network Devices(**네트워크 디바이스**)** 섹션에서 필요한 정보를 입력합니다.

단계 **4** **Advanced Trustsec Settings(**고급 **TrustSec** 설정**)** 확인란을 선택하여 Trustsec이 활성화된 디바이스를 구성합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

OOB TrustSec PAC

모든 TrustSec 네트워크 디바이스는 EAP-FAST 프로토콜의 일부로 TrustSec PAC를 보유하고 있습니다. 또한 이는 RADIUS 공유 암호가 PAC를 통해 수행된 파라미터에서 파생되는 보안 RADIUS 프로토콜에 사용됩니다. 이러한 매개변수 중 하나인 Initiator-ID는 TrustSec 네트워크 디바이스 ID, 즉 Device ID를 포함합니다.

디바이스가 TrustSec PAC를 사용하여 식별된 경우 디바이스 ID(Cisco ISE의 해당 디바이스에 구성됨)와 PAC의 Initiator-ID가 일치하지 않을 경우 인증이 실패합니다.

일부 TrustSec 디바이스(예: Cisco 방화벽 ASA)는 EAP-FAST 프로토콜을 지원하지 않습니다. 그러므로 Cisco ISE는 EAP-FAST를 통해 TrustSec PAC와 함께 이러한 디바이스를 프로비저닝할 수 없습니다. 대신, TrustSec PAC가 Cisco ISE에서 생성되므로 수동으로 디바이스에 복사할 수 있습니다. 이를 OOB(Out Of Band) TrustSec PAC 생성이라고 합니다.

Cisco ISE에서 PAC를 생성할 때 암호화 키를 사용하여 암호화된 PAC 파일이 생성됩니다.

이 섹션에는 다음 사항을 설명합니다.

설정 화면에서 **TrustSec PAC** 생성

설정 화면에서 TrustSec PAC를 생성할 수 있습니다.

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

단계 **2** 왼쪽의 설정 탐색창에서 **Protocols(**프로토콜**)**를 클릭합니다.

단계 **3** **EAP-FAST** > **Generate PAC(PAC** 생성**)**를 선택합니다.

단계 **4** TrustSec PAC를 생성합니다.

네트워크 디바이스 화면에서 **TrustSec PAC** 생성

네트워크 디바이스 화면에서 TrustSec PAC를 생성할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Network Device(**네트워크 디바이스**)**

단계 **2** **Add(**추가**)**를 클릭합니다. 네트워크 디바이스 탐색 창의 작업 아이콘에서 **Add new device(**새 디바이스 추가**)**를 클릭할 수도 있습니다.

단계 **3** 새 디바이스를 추가하는 경우 디바이스 이름을 입력합니다.

단계 **4** **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)** 확인란을 선택하여 TrustSec 디바이스를 구성합니다.

단계 **5** **Out of Band (OOB) TrustSec PAC(OOB TrustSec PAC)** 하위 섹션에서 **Generate PAC(PAC** 생성**)**를 클릭합니다.

단계 **6** 다음 세부정보를 입력합니다.

- PAC Time to Live - 값을 일, 주, 월 또는 년 단위로 입력합니다. 기본값은 1년입니다. 최소값은 1일이고 최대값은 10년입니다.

- Encryption Key(암호화 키) - 암호화 키를 입력합니다. 키의 길이는 8~256자여야 합니다. 키는 대/소문자, 숫자 또는 영숫자 문자 조합을 포함할 수 있습니다.

  암호화 키는 생성되는 파일에서 PAC를 암호화하는 데 사용되며, 디바이스에서 PAC 파일의 암호를 해독할 때도 사용됩니다. 따라서 관리자는 나중에 사용할 수 있도록 암호화 키를 저장하는 것이 좋습니다.

  Identity(ID) 필드에서는 TrustSec 네트워크 디바이스의 디바이스 ID를 지정합니다. 여기에는 EAP-FAST 프로토콜에서 제공하는 개시자 ID가 지정됩니다. 여기서 입력하는 ID 문자열이 네트워크 디바이스 생성 페이지의 TrustSec 섹션에 정의된 디바이스 ID와 일치하지 않으면 인증은 실패합니다.

  만료 날짜는 PAC Time to Live를 기준으로 계산됩니다.

단계 **7** **Generate PAC(PAC** 생성**)**를 클릭합니다.

네트워크 디바이스 목록 화면에서 **TrustSec PAC** 생성

네트워크 디바이스 목록 화면에서 TrustSec PAC를 생성할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Network Device(**네트워크 디바이스**)**

단계 **2** **Network Devices(**네트워크 디바이스**)**를 클릭합니다.

단계 **3** TrustSec PAC를 생성할 디바이스 옆의 확인란을 선택하고 **Generate PAC(PAC** 생성**)**를 클릭합니다.

단계 **4** 필드에 세부정보를 입력합니다.

단계 **5** **Generate PAC(PAC** 생성**)**를 클릭합니다.

푸시 버튼

이그레스 정책의 Push(푸시) 옵션을 사용하는 경우 CoA 알림이 시작됩니다. 이 알림에서는 TrustSec 디바이스를 호출하여 이그레스 정책의 컨피그레이션 변경사항과 관련해 Cisco ISE의 업데이트를 즉시 요청합니다.

TrustSec AAA 서버 구성

AAA 서버 목록에서 TrustSec이 활성화된 Cisco ISE 서버 목록을 구성할 수 있습니다. TrustSec 디바이스는 이러한 서버에 대해 인증합니다. Push(푸시)를 클릭하면 이 목록의 새 서버가 TrustSec 디바이스에 다운로드됩니다. TrustSec 디바이스가 인증을 시도하면 이 목록에서 Cisco ISE 서버를 선택합니다. TrustSec 디바이스는 첫 번째 서버가 다운되었거나 사용 중인 경우 이 목록의 다른 서버에 대해 인증할 수 있습니다. 기본적으로 기본 Cisco ISE 서버는 TrustSec AAA 서버입니다. 보다 안정적인 TrustSec 환경을 위해 더 많은 Cisco ISE 서버를 구성하는 것이 좋습니다.

이 페이지에는 TrustSec AAA 서버로 구성한 구축 내의 Cisco ISE 서버가 나열됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > TrustSec AAA Servers(TrustSec AAA** 서버**)**

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 다음 설명에 따라 값을 입력합니다.

- Name(이름) - AAA 서버 목록의 Cisco ISE 서버에 할당할 이름입니다. 이 이름은 Cisco ISE 서버의 호스트 이름과 다를 수 있습니다.
- Description(설명) - 필요에 따라 설명을 입력합니다.
- IP - AAA 서버 목록에 추가할 Cisco ISE 서버의 IP 주소입니다.
- Port(포트) - TrustSec 디바이스와 서버 간의 통신이 수행되어야 하는 포트입니다. 기본값은 1,812입니다.

단계 **4** **Push(**푸시**)**를 클릭합니다.

다음에 수행할 작업

보안 그룹을 구성합니다.

TrustSec HTTPS 서버

기본적으로 Cisco ISE는 RADIUS를 사용하여 Cisco ISE와 Trustsec NAD간에 TrustSec 환경 데이터를 교환합니다. RADIUS보다 빠르고 안정적인 HTTPS를 사용하도록 Cisco ISE를 구성할 수 있습니다. Cisco ISE는 REST API를 사용하여 HTTP 전송을 구현합니다.

HTTPS 전송에는 다음이 필요합니다.

- HTTPS 서버와 TrustSec 네트워크 디바이스 간에 포트 9603이 열려 있어야 합니다.
- PSN에 연결하는 모든 네트워크 디바이스에서 HTTPS 서버의 자격 증명은 고유해야 합니다.
- Cisco 스위치는 16.12.2, 17.1.1 또는 그 이상 버전을 실행해야 합니다.

HTTPS 전송을 구성하려면 다음을 따릅니다.

1. 각 네트워크 디바이스에서 HTTP 파일 전송을 활성화해야 하며 자격 증명이 필요합니다.
2. Cisco ISE의 **General Trustsec Settings(**일반 **TrustSec** 설정**)**에서 **Trustsec REST API Service for Network Devices(**네트워크 디바이스의 **Trustsec REST API** 서비스**)**를 활성화합니다.
3. Cisco ISE에서 각 PSN의 네트워크 디바이스 정의를 편집하여 **Enable HTTP REST API(HTTP REST API** 활성화**)**를 선택하고 네트워크 디바이스의 HTTP 서버에 대한 자격 증명을 입력합니다.

4. Cisco ISE에서 **Trustsec > Components(**구성 요소**)** 아래에 이 네트워크 디바이스를 TrustSec HTTPs 서버로 추가합니다.

참고 HTTPS에 대해 하나의 노드만 구성하는 경우, HTTPS에 대해 구성되지 않은 TrustSec 서버는 TrustSec 서버 목록에 표시되지 않습니다. HTTPS에 대한 구축에서 나머지 모든 TrustSec 지원 노드를 구성해야 합니다. HTTPS에 대해 구성된 PSN이 없으면 RADIUS가 사용되며 모든 Cisco ISE는 이 TrustSec 구축의 모든 PSN 노드를 나열합니다.

컨피그레이션이 완료되면 Cisco ISE는 TrustSec 환경 데이터의 구성된 서버 목록을 **Trustsec > Network Devices(**네트워크 디바이스**)**에 반환합니다.

디버그

디버그에서 ERS를 활성화합니다. 이 설정은 모든 ERS 트래픽을 로깅합니다. 로그 파일이 오버로드되지 않도록 방지하려면 이 설정을 30분 이상 활성화된 상태로 두지 마십시오.

Trustsec > Settings(설정**) > General Trustsec Settings(**일반 **Trustsec** 설정**)**에 있는 **Trustsec REST API Service for Network Devices(**네트워크 디바이스의 **Trustsec REST API** 서비스**)** 아래에서 **Include request payload body(**요청 페이로드 본문 포함**)**를 선택하여 추가 감사 정보를 활성화할 수 있습니다.
일반 TrustSec 설정

보안 그룹 컨피그레이션

SG(Security Group) 또는 SGT(Security Group Tag)는 TrustSec 정책 컨피그레이션에 사용되는 요소입니다. SGT는 신뢰할 수 있는 네트워크 내에서 이동할 때 패킷에 연결됩니다. 이러한 패킷은 신뢰할 수 있는 네트워크(인그레스)에 진입할 때 태그가 지정되고, 신뢰할 수 있는 네트워크(이그레스)를 나갈 때 태그 해제됩니다.

SGT는 순차적으로 생성되지만, IP 대 SGT 매핑을 위한 일련의 SGT를 예약할 수 있습니다. Cisco ISE는 SGT를 생성하는 동안 예약된 번호를 건너뛸 수 있습니다.

TrustSec 서비스는 이러한 SGT를 사용하여 이그레스에서 TrustSec 정책을 시행합니다.

관리 포털의 다음 페이지에서 보안 그룹을 구성할 수 있습니다.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Security Groups(**보안 그룹**)**
- **Configure(**구성**)** > **Create New Security Group(**새 보안 그룹 생성**)**의 이그레스 정책 페이지에서 직접

여러 SGT를 업데이트한 후에 **Push**(푸시) 버튼을 클릭하여 환경 CoA 알림을 시작할 수 있습니다. 이 환경 CoA 알림은 모든 TrustSec 네트워크 디바이스로 전송되어 정책/데이터 새로 고침 요청이 시작되도록 합니다.

Cisco ISE에서 보안 그룹 관리

사전 요건

보안 그룹을 생성, 편집 또는 삭제하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

보안 그룹 추가

1. **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Security Groups(**보안 그룹**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .
2. **Add(**추가**)**를 클릭하여 새 보안 그룹을 추가합니다.
3. 새 보안 그룹의 이름과 설명(선택 사항)을 입력합니다.
4. 이 SGT를 Cisco ACI로 전파하려는 경우 **Propagate to ACI(ACI**로 전파**)** 확인란을 선택합니다. 이 SGT와 관련된 SXP 매핑은 Cisco ACI Settings(Cisco ACI 설정) 페이지에서 선택한 VPN에 속하는 경우에만 Cisco ACI로 전파됩니다.

   이 옵션은 기본적으로 비활성화되어 있습니다.
5. 태그 값을 입력합니다. 태그 값은 수동으로 입력하거나 자동 생성되도록 설정할 수 있습니다. SGT의 범위를 예약할 수도 있습니다. 에서 이 범위를 구성할 수 있습니다. General TrustSec Settings(일반 TrustSec 설정) 페이지(**Work Centers(**작업 센터**) > TrustSec > Settings(**설정**) > General TrustSec Settings(**일반 **TrustSec** 설정**)**).
6. **Save(**저장**)**를 클릭합니다.

보안 그룹 삭제

소스 또는 대상에서 아직 사용 중인 보안 그룹은 삭제할 수 없습니다. 여기에는 Cisco ISE의 기능에 매핑되는 기본 그룹이 포함됩니다.

- BYOD
- Guest
- TrustSec 디바이스
- Unknown

Cisco ISE로 보안 그룹 가져오기

CSV(comma-separated value) 파일을 사용하여 Cisco ISE 노드로 보안 그룹을 가져올 수 있습니다. 먼저 템플릿을 업데이트해야 Cisco ISE로 보안 그룹을 가져올 수 있습니다. 같은 리소스 유형의 가져오기를 동시에 실행할 수는 없습니다. 예를 들어 서로 다른 두 가져오기 파일에서 보안 그룹을 동시에 가져올 수는 없습니다.

관리 포털에서 CSV 템플릿을 다운로드하고 해당 템플릿에 보안 그룹 세부정보를 입력한 후에 템플릿을 CSV 파일로 저장할 수 있습니다. 이 CSV 파일을 Cisco ISE로 다시 가져올 수 있습니다.

보안 그룹을 가져오는 동안 Cisco ISE에서 첫 번째 오류를 발견하면 가져오기 프로세스를 중지할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Security Groups(**보안 그룹**)**를 선택합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** **Browse(**찾아보기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 CSV 파일을 선택합니다.

단계 **4** **Stop Import on First Error(**첫 번째 오류에서 가져오기 중지**)** 확인란을 선택합니다.

단계 **5** **Import(**가져오기**)**를 클릭합니다.

Cisco ISE에서 보안 그룹 내보내기

보안 그룹을 다른 Cisco ISE 노드로 가져오는 데 사용할 수 있는 CSV 파일 형식으로 Cisco ISE에 구성된 보안 그룹을 내보낼 수 있습니다.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Security Groups(**보안 그룹**)**를 선택합니다.

단계 **2** **Export(**내보내기**)**를 클릭합니다.

단계 **3** 보안 그룹을 내보내려는 경우 다음 중 하나를 수행할 수 있습니다.

- 내보낼 그룹 옆의 확인란을 선택하고 **Export(**내보내기**)** > **Export Selected(**선택 항목 내보내기**)**를 선택합니다.
- 정의되어 있는 모든 보안 그룹을 내보내려면 **Export(**내보내기**)** > **Export All(**모두 내보내기**)**을 선택합니다.

단계 **4** export.csv 파일을 로컬 하드 디스크에 저장합니다.

IP SGT 정적 매핑 추가

IP-SGT 정적 매핑을 사용하여 TrustSec 디바이스 및 SXP 도메인에 통합된 방식으로 매핑을 구축할 수 있습니다. 새 IP-SGT 정적 매핑을 생성하는 동안 이 매핑을 구축할 SXP 도메인 및 디바이스를 지정할 수 있습니다. 매핑 그룹에 IP-SGT 매핑을 연결할 수도 있습니다.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > IP SGT Static Mapping(IP SGT** 정적 매핑**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 표시되는 **New(**새로 만들기**)** 영역의 드롭다운 목록에서 **IP Address(IP** 주소**)** 또는 **Hostname(**호스트 이름**)**을 선택하고 그 옆의 필드에 해당 값을 입력합니다.

다음 단계의 **Map to SGT individually(SGT**에 개별적으로 매핑**)** 옵션에서 매핑할 SXP 도메인을 지정할 수 있습니다. 그러나 이 단계에서 **Hostname(**호스트 이름**)**을 선택하는 경우 **Send to SXP Domain(SXP** 도메인으로 전송**)** 필드

에 액세스할 수 없습니다. 다음 단계에서 SXP 도메인을 추가하려면 여기에서 **IP Address(IP** 주소**)**를 선택해야 합니다.

단계 **4** 기존 매핑 그룹을 사용하려면 **Add to a Mapping Group(**매핑 그룹에 추가**)**을 클릭하고 **Mapping Group(**매핑 그룹**)** 드롭다운 목록에서 필요한 그룹을 선택합니다.

이 IP 주소/호스트 이름을 SGT에 개별적으로 매핑하려면 **Map to SGT Individually(SGT**에 개별적으로 매핑**)**를 클릭하고 다음을 수행합니다.

- SGT 드롭다운 목록에서 SGT를 선택합니다.
- 드롭다운 목록에서 매핑에 대한 Virtual Network(가상 네트워크)를 선택합니다.
- 매핑을 구축해야 하는 SXP VPN 그룹을 선택합니다.
- 이 매핑을 구축할 디바이스를 지정합니다. 모든 TrustSec 디바이스, 선택한 네트워크 디바이스 그룹 또는 선택한 네트워크 디바이스에서 매핑을 구축할 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

IP SGT 정적 매핑 구축

매핑을 추가한 후에는 **Deploy(**구축**)** 옵션을 사용하여 타깃 네트워크 디바이스에서 매핑을 구축합니다. 매핑을 이전에 저장했더라도 이 작업을 명시적으로 수행해야 합니다. **Check Status(**상태 확인**)**를 클릭하여 디바이스의 구축 상태를 확인합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > IP SGT Static Mapping(IP SGT** 정적 매핑**)**

단계 **2** 구축할 매핑 옆의 확인란을 선택합니다. 모든 매핑을 구축하려면 맨 위의 확인란을 선택합니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다.

모든 TrustSec 디바이스가 **Deploy IP SGT Static Mapping(IP SGT** 정적 매핑 구축**)** 창에 나열됩니다.

단계 **4** 선택한 매핑을 구축해야 하는 디바이스 또는 디바이스 그룹 옆의 확인란을 선택합니다.

- 모든 디바이스를 선택하려면 맨 위의 확인란을 선택합니다.
- 필터 옵션을 사용하여 특정 디바이스를 찾습니다.
- 디바이스를 선택하지 않으면 선택한 매핑이 모든 TrustSec 디바이스에 구축됩니다.
- 새 매핑을 구축할 디바이스를 선택하면 ISE는 새 매핑의 영향을 받게 될 디바이스를 모두 선택합니다.

단계 **5** **Deploy(**구축**)**를 클릭합니다. 구축 버튼은 새 맵의 영향을 받는 모든 디바이스의 매핑을 업데이트합니다.

Deployment Status(구축 상태**)** 창에는 디바이스가 업데이트되는 순서와 오류로 인해 또는 디바이스가 연결 불가능하여 업데이트되지 않는 디바이스가 표시됩니다. 구축이 완료되면 성공적으로 업데이트 된 총 디바이스 수와 업데이트되지 않은 디바이스 수가 창에 표시됩니다.

IP SGT Static Mapping(IP SGT 정적 매핑**)** 페이지의 **Check Status(**상태 확인**)** 옵션을 사용하여 특정 디바이스의 동일한 IP 주소에 서로 다른 여러 SGT가 할당되었는지 확인합니다. 이 옵션을 사용하면 충돌하는 매핑이 있는 디바이스, 여러 SGT에 매핑된 IP 주소, 동일한 IP 주소에 할당된 여러 SGT를 찾을 수 있습니다. **Check Status(**상태 확인**)** 옵션은 디바이스 그룹, FQDN, 호스트 이름 또는 IPv6 주소가 구축에 사용되는 경우에도 사용할 수 있습니다. 이러한 매핑을 구축하기 전에, 충돌하는 매핑을 제거하거나 구축 범위를 수정해야 합니다.

IPv6 주소는 IP SGT 정적 매핑에 사용할 수 있습니다. 이러한 매핑은 SSH 또는 SXP를 사용하여 특정 네트워크 디바이스 또는 네트워크 디바이스 그룹에 전파할 수 있습니다.

FQDN 및 호스트 이름이 사용되는 경우 Cisco ISE는 매핑을 구축하고 구축 상태를 확인하는 동안 PAN 및 PSN 노드에서 해당 IP 주소를 찾습니다.

General TrustSec Settings(일반 **TrustSec** 설정**)** 창의 **IP SGT Static Mapping of Hostnames(**호스트 이름의 **IP SGT** 정적 매핑**)** 옵션을 사용하여, DNS 쿼리에서 반환하는 IP 주소에 대해 생성되는 매핑 수를 지정합니다. 다음 옵션 중 하나를 선택합니다.

- **DNS** 쿼리에서 반환하는 모든 **IP** 주소에 대한 매핑을 생성합니다.
- **DNS** 쿼리에서 반환한 첫 번째 **IPv4** 주소 및 첫 번째 **IPv6** 주소에 대해서만 매핑을 생성합니다.

Cisco ISE로 IP SGT 정적 매핑 가져오기

CSV 파일을 사용하여 IP SGT 매핑을 가져올 수 있습니다.

또한 관리 포털에서 CSV 템플릿을 다운로드하여 매핑 세부정보를 입력한 다음 해당 템플릿을 CSV 파일로 저장하여 Cisco ISE로 다시 가져올 수도 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > IP SGT Static Mapping(IP SGT** 정적 매핑**)**

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** **Browse(**찾아보기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 CSV 파일을 선택합니다.

단계 **4** **Upload(**업로드**)**를 클릭합니다.

Cisco ISE에서 IP SGT 정적 매핑 내보내기

CSV 파일 형식으로 IP SGT 매핑을 내보낼 수 있습니다. 이 파일을 사용하여 다른 Cisco ISE 노드로 이러한 매핑을 가져올 수 있습니다.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > IP SGT Static Mapping(IP SGT** 정적 매핑**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 다음 중 하나를 수행합니다.

- 내보낼 매핑 옆의 확인란을 선택하고 **Export(**내보내기**) > Selected(**선택 항목**)**를 선택합니다.
- 모든 매핑을 내보내려면 **Export(**내보내기**) > All(**모두**)**을 선택합니다.

단계 **3** mappings.csv 파일을 로컬 하드 디스크에 저장합니다.

SGT 매핑 그룹 추가

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > IP SGT Static Mapping(IP SGT** 정적 매핑**) > Manage Groups(**그룹 관리**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 매핑 그룹의 이름과 설명을 입력합니다.

단계 **4** 다음을 수행합니다.

- **SGT** 드롭다운 목록에서 SGT를 선택합니다.
- 드롭다운 목록에서 매핑에 대한 Virtual Network(가상 네트워크)를 선택합니다.
- 매핑을 구축해야 하는 SXP VPN 그룹을 선택합니다.
- 매핑을 구축할 디바이스를 지정합니다. 모든 TrustSec 디바이스, 선택한 네트워크 디바이스 그룹 또는 선택한 네트워크 디바이스에서 매핑을 구축할 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

하나의 매핑 그룹에서 다른 매핑 그룹으로 IP SGT 매핑을 이동할 수 있습니다.

매핑 및 매핑 그룹을 업데이트하거나 삭제할 수도 있습니다. 매핑 또는 그룹 매핑을 업데이트하려면 업데이트할 매핑 또는 매핑 그룹 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다. 매핑 또는 그룹 매핑을 삭제하려면 삭제할 매핑 또는 매핑 그룹 옆의 확인란을 선택하고 **Trash(**삭제**) > Selected(**선택한 항목**)**를 클릭합니다. 매핑 그룹을 삭제하면 해당 그룹 내의 IP SGT 매핑도 삭제됩니다.

Security Group Access Control List 추가

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 1 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Security Group ACLs(**보안 그룹 **ACL)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 2 **Add(**추가**)**를 클릭하여 새 보안 그룹 ACL을 생성합니다.

단계 3 다음 정보를 입력합니다.

- Name(이름) - SGACL의 이름입니다.
- Description(설명) - SGACL의 설명(선택 사항)입니다.
- IP Version(IP 버전) - 이 SGACL이 지원하는 IP 버전입니다.
  - IPv4 - IP 버전 4(IPv4)가 지원됩니다.
  - IPv6 - IP 버전 6(IPv6)이 지원됩니다.
  - Agnostic(무제한) - IPv4 및 IPv6이 모두 지원됩니다.
- Security Group ACL Content(보안 그룹 ACL 콘텐츠) - ACL(Access Control List) 명령입니다. 예를 들면 다음과 같습니다.

  permit icmp

  deny ip

  SGACL 입력 syntax(명령문)는 ISE 내에서 확인되지 않습니다. 스위치, 라우터 및 액세스 포인트에서 오류 없이 적용할 수 있도록 올바른 syntax(명령문)를 사용하고 있는지 확인하십시오. 기본 정책은 **permit IP**, **permit ip log**, **deny ip** 또는 **deny ip log**로 구성할 수 있습니다. TrustSec 네트워크 디바이스는 기본 정책을 특정 셀 정책의 끝에 연결합니다.

  다음은 가이드라인을 위한 두 가지 SGACL의 예입니다. 둘 다 최종 모두 연결 규칙을 포함합니다. 첫 번째는 최종 모두 연결 규칙을 거부하고 두 번째는 허용합니다.

  Permit_Web_SGACL

  ```
  permit tcp dst eq 80
  permit tcp dst eq 443
  deny ip
  ```

  Deny_JumpHost_Protocols

  ```
  deny tcp dst eq 23
  deny tcp dst eq 23
  deny tcp dst eq 3389
  permit ip
  ```

  다음 표에는 IOS, IOS XE 및 NS-OS 운영체제에 해당하는 SGACL 구문이 나와 있습니다.

SGACL CLI 및 **ACE**	**IOS, IOS XE** 및 **NX-OS**에서 공통되는 구문
config acl	deny, exit, no, permit
deny permit	ahp, eigrp, gre, icmp, igmp, ip, nos, ospf, pcp, pim, tcp, udp
deny tcp deny tcp src deny tcp dst	dst, log, src
deny tcp dst eq deny tcp src eq	range 0 65535
deny udp deny udp src deny udp dest	Dst, log, src
deny tcp dst eq www deny tcp src eq www	range 0 65535

참고 일부 Cisco 스위치에서는 하이픈을 사용할 수 없습니다. 따라서 `permit dst eq 32767-65535`는 유효하지 않습니다. `permit dst eq range 32767 65535`를 사용하십시오.

단계 **4** **Push(**푸시**)**를 클릭합니다.
Push(푸시) 옵션을 사용하는 경우 CoA 알림이 시작됩니다. 이 알림은 TrustSec 디바이스가 구성 변경 사항과 관련해 Cisco ISE의 업데이트를 즉시 요청하도록 지시합니다.

참고 Cisco ISE에는 Permit IP, Permit IP Log, Deny IP 및 Deny IP Log와 같은 미리 정의된 SGACL이 있습니다. 이러한 SGACL을 사용하여 GUI 또는 ERS API를 통해 TrustSec 매트릭스를 구성할 수 있습니다. 이러한 SGACL은 GUI의 Security Group ACLs(보안 그룹 ACL) 목록 페이지에 표시되지 않지만, ERS API를 사용하여 사용 가능한 SGACL을 나열하는 경우(ERS getAll 호출) 이러한 SGACL이 표시됩니다.

이그레스 정책

이그레스 표에는 소스 및 대상 SGT(예약 항목과 예약되지 않은 항목 모두)가 나열됩니다. 이 페이지에서는 이그레스 표을 필터링하여 특정 정책을 보고 이와 같은 사전 설정 필터를 저장할 수도 있습니다. 소스 SGT가 대상 SGT에 대한 연결을 시도하면 TrustSec 지원 디바이스는 이그레스 정책에 정의된 TrustSec 정책에 따라 SGACL을 적용합니다. Cisco ISE는 정책을 생성하고 프로비저닝합니다.

TrustSec 정책을 생성하는 데 필요한 기본 구성 요소인 SGT 및 SGACL을 생성한 후에는 SGACL을 소스 및 대상 SGT에 할당하여 둘 사이의 관계를 설정할 수 있습니다.

소스 SGT에서 대상 SGT로의 각 조합은 이그레스 정책에서 한 셀을 이룹니다.

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Egress Policy(**이그레스 정책**)**

이그레스 정책은 다음 3가지 방법으로 확인할 수 있습니다.

- 소스 트리 보기
- 대상 트리 보기
- 매트릭스 보기

소스 트리 보기

소스 트리 보기에는 소스 SGT의 간략한 보기와 구성된 보기가 축소된 상태로 나열됩니다. 소스 SGT를 확장하면 선택한 해당 소스 SGT와 관련된 모든 정보가 나열되는 내부 표을 확인할 수 있습니다. 이 보기에는 대상 SGT에 매핑된 소스 SGT만 표시됩니다. 특정 소스 SGT를 확장하면 이 소스 SGT에 매핑된 모든 대상 SGT와 그에 해당하는 정책(SGACL)이 표에 표시됩니다.

일부 필드 옆에는 점 3개(...)가 표시됩니다. 이 점은 셀에 정보가 더 포함되어 있음을 나타냅니다. 3개 점 위에 커서를 놓으면 간단히 보기 팝업에서 나머지 정보를 볼 수 있습니다. SGT 이름 또는 SGACL 이름 위에 커서를 놓으면 간단히 보기 팝업이 열리고 해당 특정 SGT 또는 SGACL의 내용이 표시됩니다.

대상 트리 보기

대상 트리 보기에는 대상 SGT의 간략한 보기와 구성된 보기가 축소된 상태로 나열됩니다. 대상 SGT를 확장하면 선택한 해당 대상 SGT와 관련된 모든 정보가 나열되는 내부 표을 확인할 수 있습니다. 이 보기에는 소스 SGT에 매핑된 대상 SGT만 표시됩니다. 특정 대상 SGT를 확장하면 이 대상 SGT에 매핑된 모든 소스 SGT와 그에 해당하는 정책(SGACL)이 표에 표시됩니다.

일부 필드 옆에는 점 3개(...)가 표시됩니다. 이 점은 셀에 정보가 더 포함되어 있음을 나타냅니다. 3개 점 위에 커서를 놓으면 간단히 보기 팝업에서 나머지 정보를 볼 수 있습니다. SGT 이름 또는 SGACL 이름 위에 커서를 놓으면 간단히 보기 팝업이 열리고 해당 특정 SGT 또는 SGACL의 내용이 표시됩니다.

매트릭스 보기

이그레스 정책의 매트릭스 보기는 스프레드시트와 같이 표시되며, 다음의 두 축을 포함하고 있습니다.

- 소스 축 - 세로 축에는 모든 소스 SGT가 나열됩니다.
- 대상 축 - 가로 축에는 모든 대상 SGT가 나열됩니다.

소스 SGT에서 대상 SGT로의 매핑은 셀로 표현됩니다. 데이터를 포함하는 셀은 해당하는 소스 SGT와 대상 SGT 간에 매핑이 있음을 나타냅니다. 매트릭스 보기에는 다음 두 가지 유형의 셀이 있습니다.

- 매핑된 셀 - 소스 및 대상 SGT 쌍이 순서가 지정된 SGACL 집합과 관련되어 있으며 지정된 상태가 설정되어 있는 경우입니다.
- 매핑되지 않은 셀 - 소스 및 대상 SGT 쌍이 SGACL과 관련이 없으며 지정된 상태가 설정되어 있지 않은 경우입니다.

이그레스 정책 셀에는 소스 SGT와 대상 SGT가 표시되며 최종 모두 연결 규칙이 쉼표로 구분된 SGACL 아래에 단일 목록으로 표시됩니다. 최종 모두 연결 규칙은 없음으로 설정된 경우 표시되지 않습니다. 매트릭스의 빈 셀은 매핑되지 않은 셀을 나타냅니다.

이그레스 정책 매트릭스 보기에서 매트릭스를 스크롤하여 필요한 셀 집합을 확인할 수 있습니다. 브라우저에서는 전체 매트릭스 데이터를 한 번에 로드하지 않습니다. 즉, 브라우저는 서버에 스크롤 중인 영역에 속하는 데이터를 요청합니다. 따라서 메모리 오버플로 및 성능 문제를 방지할 수 있습니다.

View(보기**)** 드롭다운 목록에서 다음 옵션을 사용하여 매트릭스 보기를 변경할 수 있습니다.

- Condensed with SGACL names(축소하고 SGACL 이름 표시) - 이 옵션을 선택하면 빈 셀이 숨겨지고 SGACL 이름이 셀에 표시됩니다.
- Condensed without SGACL names(축소하고 SGACL 이름 표시 안 함) - 이 옵션을 선택하면 빈 셀이 숨겨지고 SGACL 이름이 셀에 표시되지 않습니다. 이 보기는 매트릭스 셀을 더 많이 표시하고 색상, 패턴 및 아이콘(셀 상태)을 사용하여 셀의 콘텐츠를 구분하려는 경우 유용합니다.
- Full with SGACL names(모두 표시하고 SGACL 이름 표시) - 이 옵션을 선택하면 좌측 및 위쪽 메뉴가 숨겨지고 SGACL 이름이 셀에 표시됩니다.
- Full without SGACL names(모두 표시하고 SGACL 이름 표시 안 함) - 이 옵션을 선택하면 매트릭스가 전체 화면 모드로 표시되며 SGACL 이름이 셀에 표시되지 않습니다.

ISE에서는 맞춤형 보기를 생성하고 이름을 지정하고 저장할 수 있습니다. 맞춤형 보기를 생성하려면 **Show(**표시**) > Create Custom View(**맞춤형 보기 생성**)**를 선택합니다. 보기 기준을 업데이트하거나 사용하지 않는 보기를 삭제할 수도 있습니다.

매트릭스 보기는 소스 및 대상 보기와 동일한 GUI 요소를 포함하고 있으며 다음 요소를 추가로 포함합니다.

매트릭스 차원

매트릭스 보기의 **Dimension(**차원**)** 드롭다운에서는 매트릭스 차원을 설정할 수 있습니다.

매트릭스 가져오기/내보내기

Import(가져오기**)** 및 **Export(**내보내기**)** 버튼을 사용하면 매트릭스를 가져오거나 내보낼 수 있습니다.

맞춤형 보기 생성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Matrix View(매트릭스 보기) 페이지의 **Show(**표시**)** 드롭다운 목록에서 **Create Custom View(**맞춤형 보기 생성**)** 옵션을 선택합니다.

단계 **2** **Edit View(**보기 편집**)** 대화 상자에 다음 세부정보를 입력합니다.

- View Name(보기 이름) - 맞춤형 보기의 이름을 입력합니다.
- Source Security Groups(소스 보안 그룹) - 맞춤형 보기에 포함할 SGT를 Show(표시) 전송 상자로 이동합니다.
- Show Relevant for Destination(대상의 관련 항목 표시) - Source Security Group(소스 보안 그룹)의 Show(표시) 전송 상자에서 선택한 항목을 재정의하고 Destination Security Group(대상 보안 그룹)의 Hide(숨기기) 전송 상자에 있는 모든 엔트리를 복사하려면 이 확인란을 선택합니다. 엔트리가 200개보다 많으면 데이터가 복사되지 않으며 경고 메시지가 표시됩니다.
- Destination Security Groups(대상 보안 그룹) - 맞춤형 보기에 포함할 SGT를 Show(표시) 전송 상자로 이동합니다.
- Show Relevant for Source(소스의 관련 항목 표시) - Destination Security Group(대상 보안 그룹)의 Show(표시) 전송 상자에서 선택한 항목을 재정의하고 Source Security Group(소스 보안 그룹)의 Hide(숨기기) 전송 상자에 있는 모든 엔트리를 복사하려면 이 확인란을 선택합니다.
- Sort Matrix By(매트릭스 정렬 기준) - 다음 옵션 중 하나를 선택합니다.
  - Manual Order(수동 순서)
  - Tag Number(태그 번호)
  - SGT Name(SGT 이름)

단계 **3** **Save(**저장**)**를 클릭합니다.

매트릭스 연산

매트릭스 탐색

커서를 사용하거나 매트릭스 콘텐츠 영역을 끌거나 가로 및 세로 스크롤 막대를 사용하여 매트릭스를 탐색할 수 있습니다. 셀을 클릭하여 누른 상태로 전체 매트릭스 콘텐츠를 따라 원하는 방향으로 끌 수 있습니다. 소스 및 대상 막대가 셀을 따라 이동합니다. 매트릭스 보기에서 셀을 선택하면 셀과 해당 행(소스 SGT) 및 열(대상 SGT)이 강조 표시됩니다. 선택한 셀의 좌표(소스 SGT 및 대상 SGT)가 매트릭스 콘텐츠 영역 아래에 표시됩니다.

매트릭스에서 셀 선택

매트릭스 보기에서 셀을 선택하려면 클릭해 주십시오. 선택한 셀이 다른 색상으로 표시되고 소스 및 대상 SGT가 강조 표시됩니다. 셀을 다시 클릭하거나 다른 셀을 선택하여 셀 선택을 취소할 수 있습니다. 매트릭스 보기에서 여러 셀 선택은 허용되지 않습니다. 셀 컨피그레이션을 편집하려면 셀을 두 번 클릭합니다.

이그레스 정책에서 **SGACL** 구성

이그레스 정책 페이지에서 보안 그룹 ACL을 생성할 수 있습니다.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Egress Policy(**이그레스 정책**)**를 선택합니다.

단계 **2** Source(소스) 또는 Destination(대상) 트리 보기 페이지에서 **Configure(**구성**) > Create New Security Group ACL(**새 보안 그룹 **ACL** 생성**)**을 선택합니다.

단계 **3** 필요한 세부정보를 입력하고 **Submit(**제출**)**을 클릭합니다.

워크 프로세스 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자여야 합니다.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > Settings(**설정**) > SXP Settings(SXP** 설정**)**를 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- Single Matrix(단일 매트릭스)-TrustSec 네트워크의 모든 디바이스에 대해 하나의 정책 매트릭스만 생성하려는 경우 이 옵션을 선택합니다.
- Multiple Mtrixs(다중 매트릭스)-여러 시나리오에 대해 여러 정책 매트릭스를 생성할 수 있습니다. 이러한 매트릭스를 사용하여 서로 다른 네트워크 디바이스에 서로 다른 정책을 구축할 수 있습니다.

  참고 매트릭스는 독립적이며 각 네트워크 디바이스는 하나의 매트릭스에만 할당할 수 있습니다.

- Production and Staging Matrices with Approval Process(승인 프로세스가 포함된 프로덕션 및 스테이징 매트릭스)-워크플로우 모드를 활성화하려면 이 옵션을 선택합니다. 편집자 및 승인자 역할에 할당된 사용자를 선택합니다. 정책 관리자 및 슈퍼 관리자 그룹의 사용자만 선택할 수 있습니다. 사용자 한 명을 편집자 역할과 승인자 역할에 모두 할당할 수는 없습니다.

  편집자 및 승인자 역할에 할당된 사용자에 대해 이메일 주소가 구성되어 있는지 확인합니다. 그렇지 않은 경우 워크플로우 프로세스 관련 이메일 알림이 이러한 사용자에게 전송되지 않습니다.

  워크플로우 모드가 활성화되면 편집자로 배정된 사용자는 스테이징 매트릭스를 생성하고, 해당 스테이징 정책을 구축하고자 하는 디바이스를 선택하며 해당 스테이징 정책을 승인자에게 제출하여 승인을 받습니다. 승

인자 역할에 할당된 사용자는 스테이징 정책을 검토하고 요청을 승인하거나 거부할 수 있습니다. 스테이징 정책은 승인자가 해당 정책을 검토하고 승인해야 선택한 네트워크 디바이스에 구축할 수 있습니다.

단계 **3** DEFCON 매트릭스를 생성하려면 **Use DEFCONS(DEFCONS** 사용**)** 확인란을 선택합니다.

DEFCON 매트릭스는 네트워크 보안 침해 시 쉽게 구축할 수 있는 대기 정책 매트릭스입니다.

Critical(매우 심각), Severe(심각), Substantial(다소 심각) 및 Moderate(보통)의 심각도 레벨에 대해 DEFCON 매트릭스를 생성할 수 있습니다.

DEFCON 매트릭스가 활성화되면 해당 DEFCON 정책이 모든 TrustSec 네트워크 디바이스에 즉시 구축됩니다. Deactivate(비활성화) 옵션을 사용하여 네트워크 디바이스에서 DEFCON 정책을 제거할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

매트릭스 목록 페이지

TrustSec 정책 매트릭스 및 DEFCON 매트릭스가 Matrices Listing(매트릭스 목록) 페이지에 나열됩니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Egress Policy(**이그레스 정책**) > Matrices List(**매트릭스 목록**)**. 각 매트릭스에 할당된 디바이스 수를 볼 수도 있습니다.

참고 DEFCON 매트릭스 옵션이 비활성화된 상태에서 단일 매트릭스 모드가 활성화된 경우 Matrices Listing(매트릭스 목록) 페이지가 표시되지 않습니다.

Matrices Listing(매트릭스 목록) 페이지에서 다음을 수행할 수 있습니다.

- 새 매트릭스 추가
- 기존 매트릭스 편집
- 매트릭스 삭제
- 기존 매트릭스 복제
- 매트릭스에 NAD 할당

Assign NADs(NAD 할당) 옵션을 사용하여 매트릭스에 NAD를 할당할 수 있습니다. 방법은 다음과 같습니다.

1. Assign Network Devices(네트워크 디바이스 할당) 창에서 매트릭스에 할당할 네트워크 디바이스를 선택합니다. 필터 옵션을 사용하여 네트워크 디바이스를 선택할 수도 있습니다.
2. Matrix(매트릭스) 드롭다운 목록에서 매트릭스를 선택합니다. 모든 기존 매트릭스 및 기본 매트릭스가 이 드롭다운 목록에 나열됩니다.

디바이스를 매트릭스에 할당한 후 Push(푸시)를 클릭하여 TrustSec 구성 변경 사항을 관련 네트워크 디바이스에 알립니다.

Matrices Listing(매트릭스 목록) 페이지에서 작업하는 동안 다음 사항에 유의하십시오.

- 기본 매트릭스는 편집 또는 삭제하거나 이름을 변경할 수 없습니다.
- 새 매트릭스를 생성할 때 빈 매트릭스로 시작하거나 기존 매트릭스에서 정책을 복사할 수 있습니다.
- 매트릭스를 삭제하면 해당 매트릭스에 할당된 NAD가 기본 매트릭스로 자동 이동됩니다.
- 기존 매트릭스를 복사하면 매트릭스의 복사본이 생성되지만 디바이스는 복사된 매트릭스에 자동으로 할당되지 않습니다.
- 다중 매트릭스 모드에서는 모든 디바이스가 초기 단계에서 기본 매트릭스에 할당됩니다.
- 다중 매트릭스 모드에서는 일부 SGACL이 매트릭스 간에 공유될 수 있습니다. 이러한 경우 SGACL 내용을 변경하면 셀 중 하나에서 이 SGACL을 포함하는 모든 매트릭스에 영향을 미칩니다.
- 스테이징이 진행 중인 경우 여러 매트릭스를 활성화할 수 없습니다.
- 다중 매트릭스 모드에서 단일 매트릭스 모드로 전환하면 모든 NAD가 기본 매트릭스에 자동으로 할당됩니다.
- DEFCON 매트릭스가 현재 활성화되어 있는 경우 삭제할 수 없습니다.

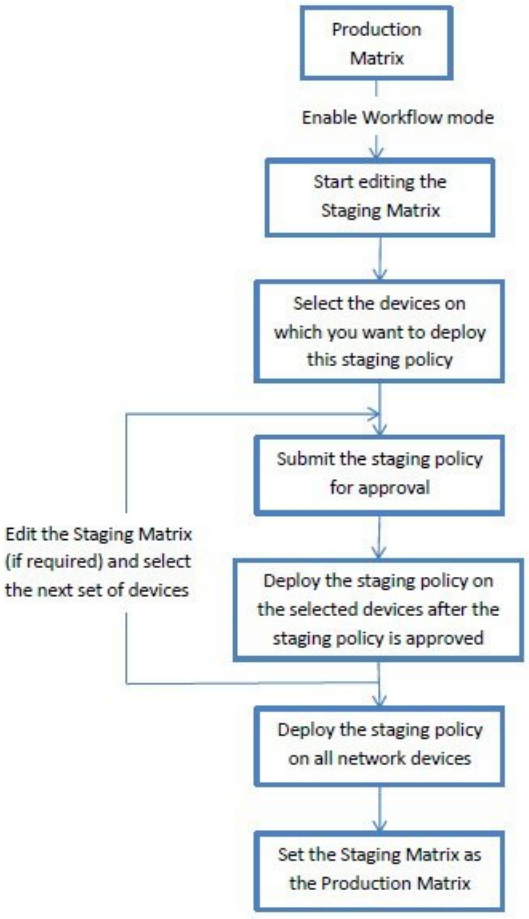
TrustSec 매트릭스 워크플로우 프로세스

Matrix Workflow(매트릭스 워크플로우) 기능을 사용하면 모든 네트워크 디바이스에서 정책을 구축하기 전에 초안 매트릭스 버전(스테이징 매트릭스라고 함)을 사용하여 제한된 디바이스 집합에서 새 정책을 테스트할 수 있습니다. 승인을 위해 스테이징 정책을 제출한 다음 정책이 승인되고 나면 선택한 네트워크 디바이스에서 스테이징 정책을 구축할 수 있습니다. 이 기능을 통해 제한된 디바이스 집합에서 새 정책을 구축하고, 해당 정책이 정상적으로 작동하는지 확인하고, 필요한 경우 정책을 변경할 수 있습니다. 계속해서 다음 디바이스 집합이나 모든 디바이스에 정책을 구축할 수 있습니다. 스테이징 정책을 모든 네트워크 디바이스에 구축할 때는 스테이징 매트릭스를 새 프로덕션 매트릭스로 설정할 수 있습니다.

워크플로우 모드를 활성화하면 편집자 역할에 할당된 사용자가 스테이징 매트릭스를 생성하고 매트릭스 셀을 편집할 수 있습니다. 스테이징 매트릭스는 TrustSec 네트워크에 현재 구축되어 있는 프로덕션 매트릭스의 복사본입니다. 편집자는 스테이징 정책을 구축할 디바이스를 선택하고 승인을 위해 승인자에게 스테이징 정책을 제출할 수 있습니다. 승인자 역할에 할당된 사용자는 스테이징 정책을 검토하고 요청을 승인하거나 거부할 수 있습니다. 스테이징 정책은 승인자가 해당 정책을 검토하고 승인해야 선택한 네트워크 디바이스에 구축할 수 있습니다.

다음 그림은 워크플로우 프로세스를 설명합니다.

그림 *47:* 매트릭스 워크플로우 프로세스



슈퍼 관리자 사용자는 **Workflow Process Settings(**워크플로우 프로세스 설정**)** 페이지에서 편집자 및 승인자 역할에 할당된 사용자를 선택할 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Settings(**설정**) > Workflow Proces(**워크플로우 프로세스**)**를 선택합니다.

선택한 디바이스에 스테이징 정책을 구축한 후에는 SGT 및 SGACL을 편집할 수 없지만 매트릭스 셀은 편집할 수 있습니다. Configuration Delta(컨피그레이션 델타) 보고서를 사용하여 프로덕션 매트릭스와 스테이징 매트릭스 간의 차이를 추적할 수 있습니다. 또한 셀의 Delta(델타) 아이콘을 클릭하여 스테이징 프로세스 중에 해당 셀에 대해 수행한 변경 사항을 확인할 수도 있습니다.

다음 표에서는 워크플로우의 여러 단계에 대해 설명합니다.

단계	설명
Staging in Edit(스테이징 편집 중)	편집자가 스테이징 매트릭스 편집을 시작하면 매트릭스가 Staging in Edit(스테이징 편집 중) 상태로 전환됩니다. 스테이징 매트릭스를 편집한 후 편집자는 새 스테이징 정책을 구축할 디바이스를 선택할 수 있습니다.
Staging Awaiting Approval(스테이징 승인 대기 중)	편집자는 매트릭스를 편집한 후 승인자가 검토하고 승인할 수 있도록 스테이징 매트릭스를 제출합니다. 승인을 위해 스테이징 매트릭스를 제출할 때 편집자는 승인자에게 전송되는 이메일에 포함할 코멘트를 추가할 수 있습니다. 승인자는 스테이징 정책을 검토하고 요청을 승인하거나 거부할 수 있습니다. 또한 승인자는 선택한 네트워크 디바이스 및 컨피그레이션 델타 보고서를 확인할 수 있습니다. 요청을 승인하거나 거부하는 동안 승인자는 편집자에게 전송되는 이메일에 포함할 코멘트를 추가할 수 있습니다. 스테이징 정책이 네트워크 디바이스에 구축되지 않은 상태이면 편집자는 승인 요청을 취소할 수 있습니다.
Deploy Approved(구축 승인됨)	승인자가 요청을 승인하면 스테이징 매트릭스는 Deploy Approved(구축 승인됨) 상태로 전환됩니다. 요청이 거부되면 매트릭스는 Staging in Edit(스테이징 편집 중) 상태로 다시 전환됩니다. 스테이징 정책을 승인자가 승인해야 편집자가 해당 스테이징 정책을 선택한 네트워크 디바이스에 구축할 수 있습니다.
Partially Deployed(부분적으로 구축됨)	스테이징 매트릭스는 선택한 디바이스에 구축되고 나면 Partially Deployed(부분적으로 구축됨) 상태로 전환됩니다. 모든 네트워크 디바이스에 스테이징 정책이 구축될 때까지 매트릭스는 Partially Deployed(부분적으로 구축됨) 단계로 유지됩니다. 이 단계에서 SGT 및 SGACL을 편집할 수는 없지만 매트릭스 셀은 편집할 수 있습니다. 최신 정책이 구축되지 않은 디바이스(동기화되지 않은 디바이스)는 Network Device Deployment(네트워크 디바이스 구축) 창에서 주황색(기울임꼴)으로 표시됩니다. 이 상태는 구축 진행률 상태 바에도 표시됩니다. 편집자는 이러한 디바이스를 선택하고 승인을 요청해 각기 다른 구축 주기에서 업데이트된 디바이스를 동기화할 수 있습니다.

단계	설명
Fully Deployed(완전히 구축됨)	모든 네트워크 디바이스에 스테이징 정책이 구축될 때까지 위의 프로세스가 반복됩니다. 모든 네트워크 디바이스에 스테이징 매트릭스가 구축되면 승인자는 스테이징 매트릭스를 프로덕션 매트릭스로 설정할 수 있습니다. 스테이징 매트릭스를 새 프로덕션 매트릭스로 설정하기 전에 프로덕션 매트릭스의 복사본을 생성하는 것이 좋습니다. 스테이징 매트릭스로 프로덕션 매트릭스를 대체하고 나면 이전 프로덕션 매트릭스 버전으로 롤백할 수 없기 때문입니다.

Workflow(워크플로우) 드롭다운 목록에 표시되는 옵션은 워크플로우 상태 및 사용자 역할(편집자 또는 승인자)에 따라 달라집니다. 아래 표에는 편집자 및 승인자에 대해 표시되는 메뉴 옵션이 나와 있습니다.

워크플로우 상태	편집자에게 표시되는 메뉴	승인자에게 표시되는 메뉴

Staging in Edit(스테이징 편집 중)	• Select network devices(네트워크 디바이스 선택)
	Network Device Deployment(네트워크 디바이스 구축) 창에서 사용 가능한 옵션은 다음과 같습니다.
	  • Request approval for selected devices(선택한 디바이스에 대한 승인 요청)
	  • Request approval for all/filtered Staging list(모든/필터링된 스테이징 목록에 대한 승인 요청)
	  • Request approval for all/filtered Production list(모든/필터링된 프로덕션 목록에 대한 승인 요청)
	  • Request approval for all/filtered devices(모든/필터링된 디바이스에 대한 승인 요청)
	• Request approval for all devices(모든 디바이스에 대한 승인 요청)
	• Discard staging(스테이징 취소)
	• View deltas(델타 보기)
		• View network devices(네트워크 디바이스 보기)
		• View deltas(델타 보기)

워크플로우 상태	편집자에게 표시되는 메뉴	승인자에게 표시되는 메뉴

Staging Awaiting Approval(스테이징 승인 대기 중)	• Cancel approval request(승인 요청 취소)
	• View network devices(네트워크 디바이스 보기)
	Network Device Deployment(네트워크 디바이스 구축) 창에서 사용 가능한 옵션은 다음과 같습니다.
	  • Cancel approval request(승인 요청 취소)
	• View deltas(델타 보기)
		• Approve deploy(구축 승인)
		• Reject deploy(구축 거부)
		• View network devices(네트워크 디바이스 보기)
		Network Device Deployment(네트워크 디바이스 구축) 창에서 사용 가능한 옵션은 다음과 같습니다.
		  • Approve deploy(구축 승인)
		  • Reject deploy(구축 거부)
		• View deltas(델타 보기)

Approved - ready to deploy(승인됨 - 구축 준비)	• 구축
	• Cancel approval request(승인 요청 취소)
	• View network devices(네트워크 디바이스 보기)
	Network Device Deployment(네트워크 디바이스 구축) 창에서 사용 가능한 옵션은 다음과 같습니다.
	  • 구축
	  • Cancel approval request(승인 요청 취소)
	• View deltas(델타 보기)
		• Reject deploy(구축 거부)
		• View network devices(네트워크 디바이스 보기)
		Network Device Deployment(네트워크 디바이스 구축) 창에서 사용 가능한 옵션은 다음과 같습니다.
		  • Reject deploy(구축 거부)
		• View deltas(델타 보기)

워크플로우 상태	편집자에게 표시되는 메뉴	승인자에게 표시되는 메뉴

Partially deployed(부분적으로 구축됨)	• Select network devices(네트워크 디바이스 선택)
	Network Device Deployment(네트워크 디바이스 구축) 창에서 사용 가능한 옵션은 다음과 같습니다.
	  • Request approval for selected devices(선택한 디바이스에 대한 승인 요청)
	  • Request approval for all/filtered Staging list(모든/필터링된 스테이징 목록에 대한 승인 요청)
	  • Request approval for all/filtered Production list(모든/필터링된 프로덕션 목록에 대한 승인 요청)
	  • Request approval for all/filtered devices(모든/필터링된 디바이스에 대한 승인 요청)
	• Request approval for all devices(모든 디바이스에 대한 승인 요청)
	• View deltas(델타 보기)
		• View network devices(네트워크 디바이스 보기)
		• View deltas(델타 보기)

워크플로우 상태	편집자에게 표시되는 메뉴	승인자에게 표시되는 메뉴

Fully deployed(완전히 구축됨)	• Select network devices(네트워크 디바이스 선택)
	Network Device Deployment(네트워크 디바이스 구축) 창에서 사용 가능한 옵션은 다음과 같습니다.
	  • Request approval for selected devices(선택한 디바이스에 대한 승인 요청)
	  • Request approval for all/filtered Staging list(모든/필터링된 스테이징 목록에 대한 승인 요청)
	  • Request approval for all/filtered Production list(모든/필터링된 프로덕션 목록에 대한 승인 요청)
	  • Request approval for all/filtered devices(모든/필터링된 디바이스에 대한 승인 요청)
	• Request approval for all devices(모든 디바이스에 대한 승인 요청)
	• View deltas(델타 보기)
		• Set as production(프로덕션으로 설정)
		• View network devices(네트워크 디바이스 보기)
		• View deltas(델타 보기)

워크플로우 옵션은 Source and Destination Tree(소스 및 대상 트리) 보기에서도 제공됩니다.

TrustSec Policy Download(TrustSec 정책 다운로드) 보고서(Work Centers[작업 센터] > TrustSec > Reports[보고서])를 사용하여 스테이징/프로덕션 정책을 다운로드한 디바이스 목록을 확인할 수 있습니다. TrustSec Policy Download(TrustSec 정책 다운로드)에는 정책(SGT/SGACL) 다운로드를 위해 네트워크 디바이스에서 전송한 요청과 ISE에서 전송한 세부정보가 나열됩니다. 워크플로우 모드가 활성화되어 있으면 프로덕션 또는 스테이징 매트릭스에 대한 요청을 필터링할 수 있습니다.

이그레스 정책 표 셀 컨피그레이션

Cisco ISE는 도구 모음에서 제공되는 다양한 옵션을 사용하여 셀을 구성할 수 있습니다. 선택한 소스 및 대상 SGT가 매핑 셀과 일치하는 경우 Cisco ISE에서는 셀 컨피그레이션이 허용되지 않습니다.

이그레스 정책 셀의 매핑 추가

정책 페이지에서 이그레스 정책에 대해 매핑 셀을 추가할 수 있습니다.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Egress Policy(**이그레스 정책**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 매트릭스 셀을 선택하려면 다음을 수행합니다.

- 매트릭스 보기에서 셀을 클릭하여 선택합니다.
- Source(소스) 및 Destination(대상) 트리 보기에서 내부 표의 행 확인란을 선택하여 해당 행을 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하여 새 매핑 셀을 추가합니다.

단계 **4** 다음에 대해 적절한 값을 선택합니다.

- Source Security Group(소스 보안 그룹)
- Destination Security Group(대상 보안 그룹)
- Status, Security Group ACLs(상태, 보안 그룹 ACL)
- Final Catch All Rule(최종 모두 연결 규칙)

단계 **5** **Save(**저장**)**를 클릭합니다.

이그레스 정책 내보내기

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Egress Policy(**이그레스 정책**) > Matrix(**매트릭스**) > Export(**내보내기**)**를 선택합니다.

단계 **2** 내보내는 파일에 SGACL이 구성되어 있지 않은 빈 셀을 포함하려면 **Include Empty Cells(**빈 셀 포함**)** 확인란을 선택합니다.

이 옵션을 활성화하면 전체 매트릭스가 내보내지며 빈 셀은 SGACL 열에서 "Empty(비어 있음)" 키워드로 표시됩니다.

참고 내보낸 파일에는 줄이 50만 개보다 많이 포함되어 있지 않아야 합니다. 그렇지 않으면 내보내기에서 장애가 발생할 수 있습니다.

단계 **3** 다음 옵션 중 하나를 선택합니다.

- Local Disk(로컬 디스크) - 로컬 드라이브로 파일을 내보내려면 이 옵션을 선택합니다.

- Repository(저장소) - 원격 저장소로 파일을 내보내려면 이 옵션을 선택합니다.

  파일을 내보내기 전에 저장소를 구성해야 합니다. 저장소를 구성하려면 **Administration(**관리**) > Maintenance(**유지 관리**) > Repository(**저장소**)**를 선택합니다. 선택한 저장소에 대해 읽기 및 쓰기 액세스 권한이 제공되는지 확인합니다.

  암호화 키를 사용하여 내보낸 파일을 암호화할 수 있습니다.

  파일 이름을 수정할 수 있습니다. 파일 이름은 50자 이내여야 합니다. 기본적으로 파일 이름에는 현재 시간이 포함되지만 원격 저장소에 동일한 파일 이름이 있는 경우 해당 파일을 덮어씁니다.

단계 **4** **Export(**내보내기**)**를 클릭합니다.

이그레스 정책 가져오기

이그레스 정책을 오프라인으로 생성한 다음 Cisco ISE로 가져올 수 있습니다. 보안 그룹 태그가 많은 경우 보안 그룹 ACL 매핑을 하나씩 생성하면 시간이 많이 걸릴 수 있습니다. 이렇게 하는 대신 이그레스 정책을 오프라인으로 생성한 다음 Cisco ISE로 가져오면 시간을 절약할 수 있습니다. 가져오기 중에 Cisco ISE는 CSV 파일의 엔트리를 이그레스 정책 매트릭스에 추가하며 데이터를 덮어쓰지는 않습니다.

다음과 같은 경우에는 이그레스 정책 가져오기가 실패합니다.

- 소스 또는 대상 SGT가 없는 경우
- SGACL이 없는 경우
- 모니터링 상태가 해당 셀에 대해 Cisco ISE에 현재 구성되어 있는 것과 다른 경우

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Egress Policy(**이그레스 정책**) > Matrix(**매트릭스**) > Import(**가져오기**)**를 선택합니다.

단계 **2** **Generate a Template(**템플릿 생성**)**을 클릭합니다.

단계 **3** 이그레스 정책 페이지에서 템플릿(CSV 파일)을 다운로드하고 CSV 파일에 다음 정보를 입력합니다.

- Source SGT(소스 SGT)
- Destination SGT(대상 SGT)
- SGACL
- Monitor status(상태 모니터링)(enabled(활성화됨), disabled(비활성화됨) 또는 monitored(모니터링됨))

단계 **4** 기존 정책을 가져오는 정책으로 덮어쓰려면 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 확인란을 선택합니다. 빈 셀(SGACL 열에서 "Empty(비어 있음)" 키워드로 표시되어 있는 셀)이 가져오는 파일에 포함되어 있으면 해당하는 매트릭스 셀의 기존 정책이 삭제됩니다.

이그레스 정책을 내보내는 동안 빈 셀을 포함하려면 **Include Empty Cells(**빈 셀 포함**)** 확인란을 선택합니다. 자세한 내용은 이그레스 정책 내보내기, 1045 페이지를 참고하십시오.

단계 **5** 가져온 파일을 검증하려면 **Validate File(**파일 검증**)**을 클릭합니다. Cisco ISE는 파일을 가져오기 전에 CSV 구조, SGT 이름, SGACL 및 파일 크기를 검증합니다.

단계 **6** Cisco ISE가 오류를 발견하는 경우 가져오기를 취소하도록 하려면 **Stop Import on First Error(**첫 번째 오류에서 가져오기 중지**)** 확인란을 선택합니다.

단계 **7** **Import(**가져오기**)**를 클릭합니다.

이그레스 정책에서 SGT 구성

이그레스 정책 페이지에서 보안 그룹을 직접 생성할 수 있습니다.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Egress Policy(**이그레스 정책**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** Source(소스) 또는 Destination(대상) 트리 보기 페이지에서 **Configure(**구성**) > Create New Security Group(**새 보안 그룹 생성**)**을 선택합니다.

단계 **3** 필요한 세부정보를 입력하고 **Submit(**제출**)**을 클릭합니다.

모니터 모드

이그레스 정책의 Monitor All(모두 모니터) 옵션을 사용하면 클릭 한 번으로 전체 이그레스 정책 컨피그레이션 상태를 모니터 모드로 변경할 수 있습니다. 모든 셀의 이그레스 정책 컨피그레이션 상태를 모니터 모드로 변경하려면 이그레스 정책 페이지에서 **Monitor All(**모두 모니터**)** 확인란을 선택합니다. Monitor All(모두 모니터) 확인란을 선택하면 컨피그레이션 상태에서 다음 변경이 수행됩니다.

- 상태가 활성화인 셀은 모니터링되는 것으로 작동하며 활성화된 것으로 표시됩니다.
- 상태가 비활성화인 셀은 영향을 받지 않습니다.
- 상태가 모니터인 셀은 모니터링 상태로 유지됩니다.

원래 컨피그레이션 상태를 복원하려면 **Monitor All(**모두 모니터**)** 확인란 선택을 취소합니다. 데이터베이스 내 셀의 실제 상태는 변경되지 않습니다. **Monitor All(**모두 모니터**)** 선택을 취소하면 이그레스 정책의 각 셀이 원래 구성 상태로 돌아갑니다.

모니터 모드의 기능

모니터 모드의 모니터링 기능을 사용하면 다음을 수행할 수 있습니다.

- 필터링되며 모니터 모드에서 모니터링되는 트래픽의 양 확인
- SGT-DGT 쌍이 모니터 모드인지 아니면 시행 모드인지를 확인하고 네트워크에서 비정상적인 패킷 삭제가 발생하는지 관찰
- SGACL 삭제가 실제로 시행 모드에 의해 시행되는지 아니면 모니터 모드에 의해 허용되는지 파악
- 모드 유형(모니터, 시행 또는 둘 다)에 따라 맞춤 보고서 생성

- NAD에 적용된 SGACL을 확인하고 불일치 사항이 있으면 표시

알 수 없는 보안 그룹

알 수 없는 보안 그룹은 미리 구성된 보안 그룹이며 수정할 수 없고 태그 값이 0인 Trustsec을 나타냅니다.

Cisco 보안 그룹 네트워크 디바이스는 소스 또는 대상의 SGT가 없는 경우 알 수 없는 SGT를 참조하는 셀을 요청합니다. 소스를 알 수 없는 경우에만 요청이 <unknown, Destination SGT> 셀에 적용됩니다. 대상을 알 수 없는 경우에만 요청이 <source SGT, unknown> 셀에 적용됩니다. 소스와 대상을 모두 알 수 없는 경우 요청은 <Unknown, Unknown> 셀에 적용됩니다.

기본 정책

기본 정책은 <ANY,ANY> 셀을 가리킵니다. 소스 SGT는 모든 대상 SGT에 매핑됩니다. 여기서 ANY SGT는 수정할 수 없으며 소스 또는 대상 SGT에 나열되지 않습니다. ANY SGT는 ANY SGT하고만 쌍을 이룰 수 있으며, 다른 SGT와는 쌍을 이룰 수 없습니다. TrustSec 네트워크 디바이스는 기본 정책을 특정 셀 정책의 끝에 연결합니다.

- 셀이 비어 있으면 기본 정책만 포함되어 있는 것입니다.
- 셀에 정책이 포함된 경우 결과 정책은 셀 특정 정책과 기본 정책의 조합으로, 기본 정책이 뒤에 옵니다.

Cisco ISE에 따라 셀 정책 및 기본 정책은 디바이스에서 두 개의 개별 정책 쿼리에 대한 응답으로 가져오는 두 가지 별도의 SGACL입니다.

기본 정책의 컨피그레이션은 다른 셀과 다릅니다.

- 상태 값은 활성화됨 또는 모니터링됨의 두 가지만 있을 수 있습니다.
- 보안 그룹 ACL은 기본 정책에 대한 선택적 필드로 비어 있을 수 있습니다.
- 최종 Catch All Rule(모든 규칙 인식)은 Permit IP(IP 허용), Deny IP(IP 거부), Permit IP(IP 허용) 로그 또는 Deny IP(IP 거부) 로그 중 하나일 수 있습니다. 기본 정책 이외의 보안 네트워크는 없으므로 여기서는 Clearly the None 옵션을 사용할 수 없습니다.

SGT 할당

디바이스 호스트 이름 또는 IP 주소를 알고 있는 경우 Cisco ISE에서는 SGT를 TrustSec 디바이스에 할당할 수 있습니다. 특정 호스트 이름 또는 IP 주소를 사용하는 디바이스가 네트워크에 가입하면 Cisco ISE에서 인증하기 전에 SGT를 할당합니다.

다음 SGT는 기본적으로 생성됩니다.

- SGT_TrustSecDevices
- SGT_NetworkServices
- SGT_Employee

- SGT_Contractor
- SGT_Guest
- SGT_ProductionUser
- SGT_Developer
- SGT_Auditor
- SGT_PointofSale
- SGT_ProductionServers
- SGT_DevelopmentServers
- SGT_TestServers
- SGT_PCIServers
- SGT_BYOD
- SGT_Quarantine

보안 그룹 태그를 엔드포인트에 매핑하도록 디바이스를 수동으로 구성해야 하는 경우가 있습니다. 보안 그룹 매핑 페이지에서 이러한 매핑을 생성할 수 있습니다. 이 작업을 수행하기 전에 SGT 범위를 예약했는지 확인해 주십시오.

ISE에서는 최대 10,000개의 IP-SGT 매핑을 생성할 수 있습니다. 그와 같은 대규모 매핑을 논리적으로 그룹화하기 위해 IP-SGT 매핑 그룹을 생성할 수 있습니다. IP-SGT 매핑의 각 그룹에는 IP 주소 목록, 매핑되는 단일 보안 그룹 및 그러한 매핑의 구축 대상인 네트워크 디바이스 또는 네트워크 디바이스 그룹이 포함되어 있습니다.

NDAC 권한 부여

SGT를 디바이스에 할당하여 TrustSec 정책을 구성할 수 있습니다. TrustSec 디바이스 ID 속성에 따라 보안 그룹을 디바이스에 할당할 수 있습니다.

NDAC 권한 부여 구성

시작하기 전에

- 정책에서 사용할 보안 그룹을 생성할 수 있는지 확인해 주십시오.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Network Device Authorization(**네트워크 디바이스 권한 부여**)**을 선택합니다.

단계 **2** 기본 규칙 행 오른쪽에서 **Action(**작업**)** 아이콘을 클릭하고 **Insert New Row Above(**위에 새 행 삽입**)**를 클릭합니다.

단계 **3** 이 규칙의 이름을 입력합니다.

단계 **4** 더하기 기호(+)를 클릭하여 정책 조건을 추가합니다.이 기호는 **Conditions(**조건**)** 옆에 있습니다.

단계 **5** **Create New Condition (Advance Option)(**새 조건 생성**(**고급 옵션**))**을 클릭하여 새 조건을 생성할 수 있습니다.

단계 **6** **Security Group(**보안 그룹**)** 드롭다운 목록에서 이 조건이 true로 평가되는 경우 할당할 SGT를 선택합니다.

단계 **7** 이 행에서 **Action(**작업**)** 아이콘을 클릭하여 디바이스 속성을 기준으로 현재 규칙 위나 아래에 규칙을 더 추가합니다. 이 프로세스를 반복하여 TrustSec 정책에 필요한 모든 규칙을 생성할 수 있습니다.  아이콘을 클릭하여 규칙을 끌어 놓기하는 방법으로 순서를 다시 지정할 수 있습니다. 기존 조건을 복제할 수도 있지만 이 경우에는 정책 이름을 변경해야 합니다.

true로 평가되는 첫 번째 규칙에 따라 평가 결과가 결정됩니다. 일치하는 규칙이 없으면 기본 규칙이 적용됩니다. 기본 규칙을 편집하여 일치하는 규칙이 없는 경우 디바이스에 적용해야 하는 SGT를 지정할 수 있습니다.

단계 **8** **Save(**저장**)**를 클릭하여 TrustSec 정책을 저장합니다.

네트워크 디바이스 정책을 구성한 후에 인증을 시도하는 TrustSec 디바이스는 자신과 피어의 SGT를 가져오며, 모든 관련 세부정보를 다운로드할 수 있습니다.

참고 기본적으로 기본 네트워크 디바이스 권한 부여 정책의 결과는 **TrustSec_Devices**로 설정됩니다.

최종 사용자 권한 부여 구성

Cisco ISE에서는 권한 부여 정책 평가의 결과로 보안 그룹을 할당할 수 있습니다. 이 옵션을 사용하면 사용자와 엔드포인트에 보안 그룹을 할당할 수 있습니다.

시작하기 전에

- 권한 부여 정책에 대한 정보를 확인해 주십시오.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > Authorization Policy(**권한 부여 정책**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 새 권한 부여 정책을 생성합니다.

단계 **3** 권한에 대해 보안 그룹을 선택합니다.

사용자나 엔드포인트에 대해 이 권한 부여 정책에 지정된 조건이 참이면 이 보안 그룹이 해당 사용자 또는 엔드포인트에 할당되며 이 사용자 또는 엔드포인트에서 전송하는 모든 데이터 패킷에 이 특정 SGT가 태그로 지정됩니다.

TrustSec 컨피그레이션 및 정책 푸시

Cisco ISE는 Cisco ISE가 TrustSec 디바이스에 TrustSec 컨피그레이션 및 정책 변경에 대한 알림을 제공하는 데 사용할 수 있는 CoA(Change of Authorization)를 지원합니다. 이를 통해 디바이스는 관련 데이터를 가져오기 위한 요청에 응답할 수 있습니다.

CoA 알림은 TrustSec 네트워크 디바이스가 환경 CoA 또는 정책 CoA를 보내도록 트리거할 수 있습니다.

기본적으로 TrustSec CoA 기능을 지원하지 않는 디바이스에 컨피그레이션 변경 사항을 푸시할 수도 있습니다.

CoA에서 지원하는 네트워크 디바이스

Cisco ISE는 다음 네트워크 디바이스에 CoA 알림을 보냅니다.

- 단일 IP 주소를 사용하는 네트워크 디바이스(서브넷은 지원되지 않음)
- TrustSec 디바이스로 구성된 네트워크 디바이스
- 지원되는 CoA인 네트워크 디바이스

여러 디바이스 집합과 상호 운용되는 여러 보조 항목이 있는 분산형 환경에 Cisco ISE가 구축된 경우 Cisco ISE 기본 노드에서 모든 네트워크 디바이스로 CoA 요청이 전송됩니다. 그러므로 Cisco ISE 기본 노드를 CoA 클라이언트로 사용하여 TrustSec 네트워크 디바이스를 구성해야 합니다.

디바이스는 CoA NAK 또는 ACK를 다시 Cisco ISE 기본 노드로 반환합니다. 그러나 네트워크 디바이스에서 발생하는 다음 TrustSec 세션은 Cisco ISE 노드로 전송됩니다. 이 노드는 네트워크 디바이스가 다른 모든 AAA 요청을 보내는 대상으로, 반드시 기본 노드일 필요는 없습니다.

CoA 미지원 디바이스에 컨피그레이션 변경사항 푸시

Nexus 네트워크 디바이스의 일부 버전과 같은 일부 플랫폼은 CoA(Change of Authorization)를 위한 Cisco ISE의 "푸시" 기능을 지원하지 않습니다. 이러한 경우 ISE는 네트워크 디바이스에 연결한 다음 해당 디바이스가 ISE에 대해 업데이트된 컨피그레이션 요청을 트리거하도록 합니다. 이를 위해 ISE는 네트워크 디바이스에 대한 SSHv2 터널을 열고 TrustSec 정책 매트릭스 새로 고침을 트리거하는 명령을 전송합니다. CoA 푸시를 지원하는 네트워크 플랫폼에서도 이 방법을 사용할 수 있습니다.

단계 **1** **Work Centers**(작업 센터) > **Device Administration**(디바이스 관리) > **Network Resources**(네트워크 리소스) > **Network Devices**(네트워크 디바이스)Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 필요한 네트워크 디바이스 옆의 확인란을 선택하고 **Edit**(편집)를 클릭합니다.

네트워크 디바이스 이름, IP 주소, RADIUS 및 TrustSec 설정이 올바르게 구성되어 있는지 확인합니다.

단계 **3** 아래쪽의 **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)**로 스크롤한 다음 **TrustSec Notifications and Updates(TrustSec** 알림 및 업데이트**)** 섹션에서 **Send configuration changes to device(**디바이스에 컨피그레이션 변경사항 보내기**)** 확인란을 선택하고 **CLI (SSH)** 라디오 버튼을 클릭합니다.

단계 **4** (선택 사항) SSH 키를 입력합니다.

단계 **5** 이 SGA 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.

단계 **6** 실행 모드에서 디바이스 컨피그레이션을 편집할 권한이 있는 사용자의 사용자 이름과 비밀번호를 입력합니다.

단계 **7** (선택 사항) 디바이스에 대해 실행 모드 비밀번호를 활성화(디바이스 컨피그레이션을 편집할 수 있음)하는 비밀번호를 입력합니다. **Show(**표시**)**를 클릭하면 이 디바이스에 대해 이미 구성된 실행 모드 비밀번호가 표시됩니다.

단계 **8** 페이지 맨 아래에서 **Submit(**제출**)**을 클릭합니다.

이제 네트워크 디바이스가 TrustSec 변경사항을 푸시하도록 구성되었습니다. Cisco ISE 정책을 변경한 후 **Push(**푸시**)**를 클릭하면 새 구성이 네트워크 디바이스에 반영됩니다.

SSH 키 검증

SSH 키를 사용하여 보안을 강화하려는 경우가 있습니다. Cisco ISE에서는 SSH 키 검증 기능을 통해 이러한 보안 강화를 지원합니다.

이 기능을 사용하려면 Cisco ISE에서 네트워크 디바이스로의 SSHv2 터널을 연 다음 네트워크 디바이스의 자체 CLI를 사용해 SSH 키를 검색합니다. 그런 후에 이 키를 복사하여 Cisco ISE에 검증용으로 붙여 넣습니다. SSH 키가 잘못된 경우 Cisco ISE는 연결을 종료합니다.

Limitation(제한**)**: 현재 Cisco ISE는 IP를 하나만 검증할 수 있으며 IP 범위나 IP 내의 서브넷을 검증할 수는 없습니다.

시작하기 전에

Cisco ISE가 안전하게 통신하도록 하려는 네트워크 디바이스용으로

- 로그인 자격 증명
- SSH 키를 검색하는 CLI 명령

이 필요합니다.

단계 **1** 네트워크 디바이스에서 다음을 수행합니다.

a) Cisco ISE가 SSH 키를 사용하여 안전하게 통신하도록 하려는 네트워크 디바이스에 로그온합니다.

b) 디바이스 CLI를 사용하여 SSH 키를 표시합니다.

예제**:**

Catalyst 디바이스용 명령은 `sho ip ssh`입니다.

c) 표시된 SSH 키를 복사합니다.

단계 **2** Cisco ISE 사용자 인터페이스에서 다음을 수행합니다.

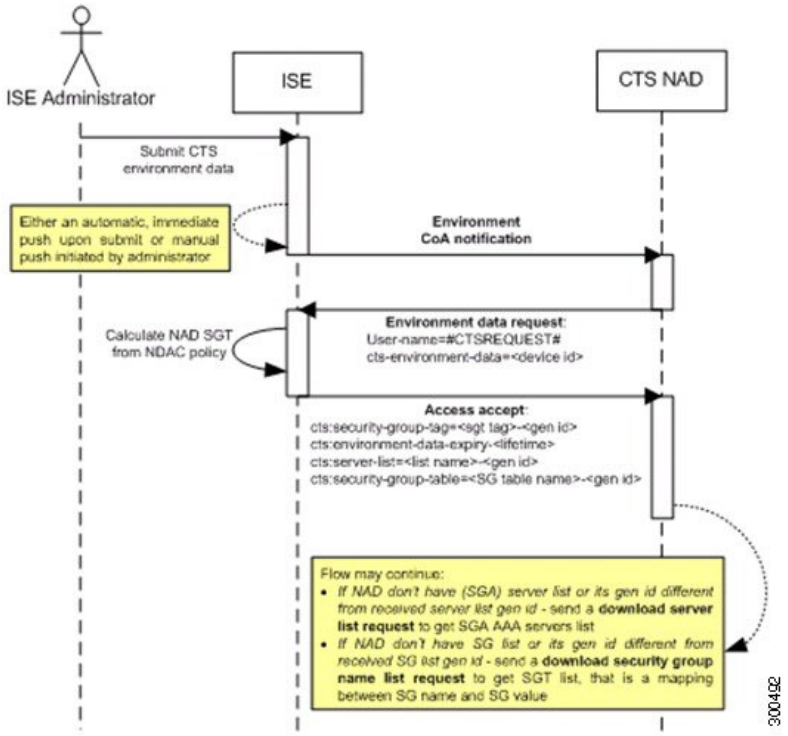
a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택하고 필요한 네트워크 디바이스의 이름, IP 주소, RADIUS 및 TrustSec 설정이 올바르게 구성되어 있는지 확인합니다.
b) 아래쪽의 **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)**로 스크롤한 다음 **TrustSec Notifications and Updates(TrustSec** 알림 및 업데이트**)** 섹션에서 **Send configuration changes to device(**디바이스에 컨피그레이션 변경사항 보내기**)** 확인란을 선택하고 **CLI (SSH)** 라디오 버튼을 클릭합니다.
c) **SSH Key(SSH** 키**)** 필드에 네트워크 디바이스에서 이전에 검색한 SSH 키를 붙여넣습니다.
d) 페이지 맨 아래에서 **Submit(**제출**)**을 클릭합니다.

이제 네트워크 디바이스가 SSH 키 검증을 사용하여 Cisco ISE와 통신합니다.

환경 **CoA** 알림 흐름

다음 그림에는 환경 CoA 알림 흐름이 나타나 있습니다.

그림 ***48:*** 환경 ***CoA*** 알림 흐름



1. Cisco ISE는 환경 CoA 알림을 TrustSec 네트워크 디바이스에 보냅니다.
2. 그러면 디바이스는 환경 데이터 요청을 반환합니다.
3. 환경 데이터 요청에 대한 응답으로 Cisco ISE는 다음을 반환합니다.

요청을 보내는 디바이스의 환경 데이터 - 여기에는 TrustSec 디바이스의 SGT(NDAC 정책에서 유추된 항목) 및 다운로드 환경 TTL이 포함됩니다.

TrustSec AAA 서버 목록의 이름 및 생성 ID.

(잠재적으로 여러 개) SGT 표의 이름 및 생성 ID - 이러한 표에는 SGT 이름과 SGT 값이 나열될 뿐 아니라 전체 SGT 목록이 들어 있습니다.

4. 디바이스에 TrustSec AAA 서버 목록이 없거나 생성 ID가 수신된 생성 ID와 다른 경우 디바이스는 AAA 서버 목록 내용을 얻기 위해 또 다른 요청을 보냅니다.
5. 응답에 나열된 SGT 표이 디바이스에 없거나 생성 ID가 수신된 생성 ID와 다른 경우 디바이스는 해당 SGT 표의 내용을 얻기 위해 또 다른 요청을 보냅니다.

환경 CoA 트리거

다음에 대해 환경 CoA가 트리거될 수 있습니다.

- 네트워크 디바이스
- 보안 그룹
- AAA 서버

네트워크 디바이스에 대해 환경 CoA 트리거

네트워크 디바이스에 대해 환경 CoA를 트리거하려면 다음 단계를 완료해 주십시오.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택합니다.

단계 2 네트워크 디바이스를 추가하거나 편집합니다.

단계 3 고급 TrustSec 설정 섹션에서 TrustSec 알림 및 업데이트 매개변수를 업데이트합니다.

환경 속성 변경 알림은 변경을 수행한 특정 TrustSec 네트워크 디바이스로만 전송됩니다.

이처럼 단일 디바이스만 영향을 받으므로 환경 CoA 알림은 제출하는 즉시 전송됩니다. 그러면 디바이스의 환경 속성이 업데이트됩니다.

보안 그룹에 대해 환경 CoA 트리거

보안 그룹에 대해 환경 CoA를 트리거하려면 다음 단계를 완료해 주십시오.

단계 1 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Security Groups(**보안 그룹**)**.

단계 2 보안 그룹 페이지에서 SGT의 이름을 변경합니다. 그러면 해당 SGT의 매핑 값 이름이 변경됩니다. 이렇게 하면 환경 변경이 트리거됩니다.

단계 **3** 여러 SGT의 이름을 변경한 후 **Push(**푸시**)** 버튼을 클릭하여 환경 CoA 알림을 시작합니다. 이 환경 CoA 알림은 모든 TrustSec 네트워크 디바이스로 전송되며 변경된 모든 SGT의 업데이트를 제공합니다.

TrustSec AAA 서버에 대해 환경 **CoA** 트리거

TrustSec AAA 서버에 대해 환경 CoA를 트리거하려면 다음 단계를 완료해 주십시오.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > TrustSec AAA Servers(TrustSec AAA** 서버**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** TrustSec AAA 서버 페이지에서 TrustSec AAA 서버의 컨피그레이션을 생성, 삭제 또는 업데이트합니다. 이렇게 하면 환경 변경이 트리거됩니다.

단계 **3** 여러 TrustSec AAA 서버를 구성한 후 **Push(**푸시**)** 버튼을 클릭하여 환경 CoA 알림을 시작합니다. 이러한 환경 CoA 알림은 모든 TrustSec 네트워크 디바이스로 전송되며, 변경된 모든 TrustSec AAA 서버의 업데이트를 제공합니다.

NDAC 정책에 대해 환경 **CoA** 트리거

NDAC 정책에 대해 환경 CoA를 트리거하려면 다음 단계를 완료해 주십시오.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > Policy(**정책**) > Network Device Authorization(**네트워크 디바이스 권한 부여**)**을 선택합니다.

NDAC 정책 페이지에서 NDAC 정책의 규칙을 생성, 삭제 또는 업데이트할 수 있습니다. 이러한 환경 변경 알림은 모든 네트워크 디바이스로 전송됩니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > TrustSec Policy(TrustSec** 정책**) > Network Device Authorization(**네트워크 디바이스 권한 부여**)**을 선택합니다.

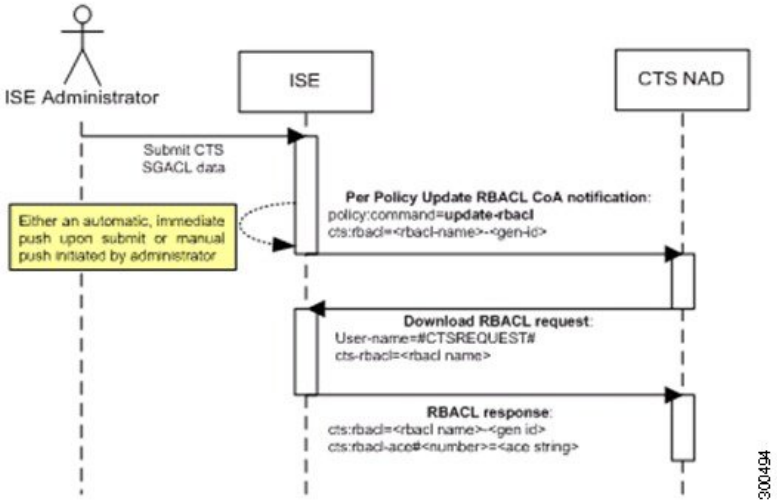
NDAC 정책 페이지에서 NDAC 정책의 규칙을 생성, 삭제 또는 업데이트할 수 있습니다. 이러한 환경 변경 알림은 모든 네트워크 디바이스로 전송됩니다.

단계 **3** NDAC 정책 페이지에서 **Push(**푸시**)** 버튼을 클릭하여 환경 CoA 알림을 시작할 수 있습니다. 이 환경 CoA 알림은 모든 TrustSec 네트워크 디바이스로 전송되며 네트워크 디바이스 소유 SGT의 업데이트를 제공합니다.

SGACL 콘텐츠 업데이트 흐름

다음 그림에는 SGACL 콘텐츠 업데이트 흐름이 나타나 있습니다.

그림 *49: SGACL* 콘텐츠 업데이트 흐름



1. Cisco ISE는 SGACL 명명된 목록 업데이트 CoA 알림을 TrustSec 네트워크 디바이스에 보냅니다. 알림에는 SGACL 이름 및 생성 ID가 포함되어 있습니다.
2. 다음 조건을 모두 충족하면 디바이스가 SGACL 데이터 요청으로 재생될 수 있습니다.

   SGACL이 디바이스에 포함된 이그레스 셀의 일부인 경우. 디바이스에 인접 디바이스 및 엔드포인트(선택한 대상 SGT의 이그레스 정책 열)의 SGT와 관련된 셀에 해당하는 이그레스 정책 데이터의 하위 집합이 포함되어 있습니다.

   CoA 알림의 생성 ID는 디바이스에서 이 SGACL용으로 보유하는 생성 ID와는 다릅니다.
3. SGACL 데이터 요청에 대한 응답에서 Cisco ISE는 SGACL(ACE)의 내용을 반환합니다.

SGACL 명명된 목록 업데이트 CoA 시작

SGACL 명명된 목록 업데이트 CoA를 트리거하려면 다음 단계를 완료해 주십시오.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > Security Group ACLs(**보안 그룹 **ACL)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** SGACL의 내용을 변경합니다. SGACL을 제출하면 SGACL의 세대 ID가 승격됩니다.

단계 **3** 여러 SGACL의 내용을 변경한 후 **Push(**푸시**)** 버튼을 클릭하여 SGACL 명명된 목록 업데이트 CoA 알림을 시작합니다. 이 알림은 모든 TrustSec 네트워크 디바이스로 전송되며, 관련 디바이스에 대한 SGACL 내용의 업데이트를 제공합니다.

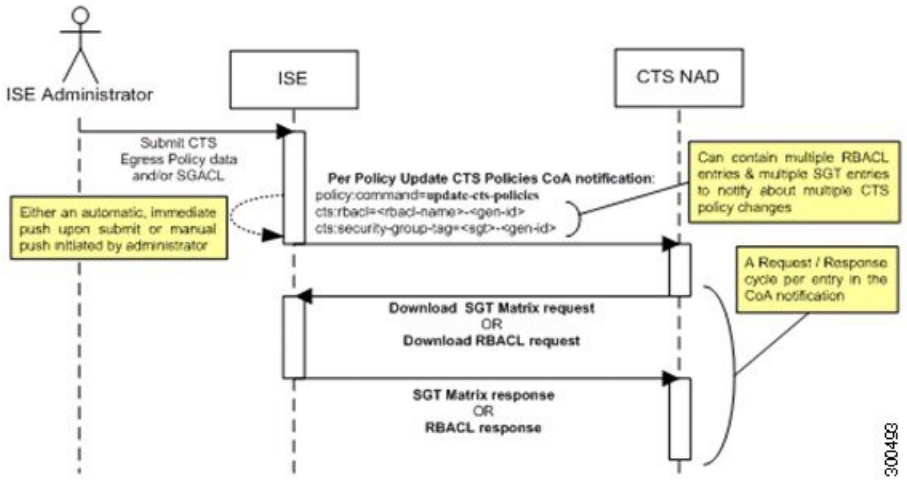
SGACL의 이름이나 IP 버전을 변경해도 세대 ID는 변경되지 않으므로 SGACL 명명된 목록 업데이트 CoA 알림을 보내지 않아도 됩니다.

그러나 이그레스 정책에서 사용 중인 SGACL의 이름이나 IP 버전을 변경하면 해당 SGACL이 포함된 셀에서 변경이 표시됩니다. 그러면 해당 셀의 대상 SGT 세대 ID가 변경됩니다.

정책 업데이트 CoA 알림 흐름

다음 그림에는 정책 CoA 알림 흐름이 나타나 있습니다.

그림 50: 정책 CoA 알림 흐름

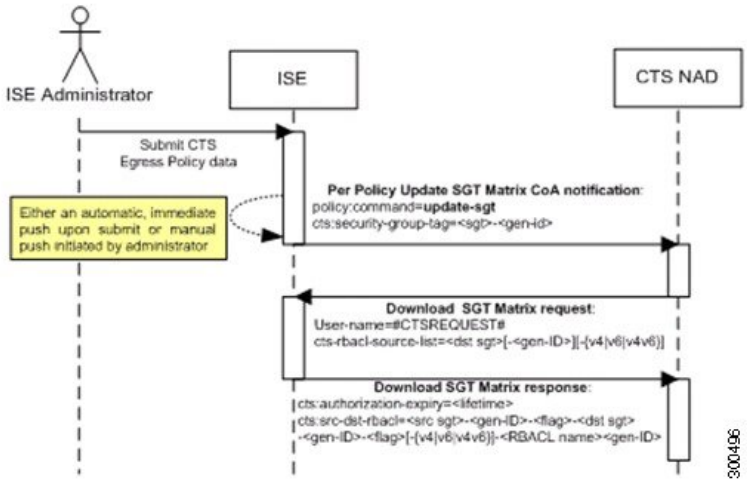


1. Cisco ISE는 업데이트 정책 CoA 알림을 TrustSec 네트워크 디바이스로 보냅니다. 알림에는 여러 SGACL 이름 및 생성 ID, 그리고 여러 SGT 값과 생성 ID가 포함될 수 있습니다.
2. 디바이스는 여러 SGACL 데이터 요청 및/또는 여러 SGT 데이터를 사용하여 재생될 수 있습니다.
3. Cisco ISE는 각 SGACL 데이터 요청 또는 SGT 데이터 요청에 대한 응답으로 관련 데이터를 반환합니다.

SGT 매트릭스 CoA 업데이트 흐름

다음 그림에는 SGT 매트릭스 CoA 업데이트 흐름이 나타나 있습니다.

그림 *51: SGT* 매트릭스 *CoA* 업데이트 흐름



1. Cisco ISE는 업데이트된 SGT 매트릭스 CoA 알림을 TrustSec 네트워크 디바이스에 보냅니다. 알림에는 SGT 값 및 생성 ID가 포함되어 있습니다.
2. 다음 조건을 모두 충족하면 디바이스가 SGT 데이터 요청으로 재생될 수 있습니다.

   SGT가 인접 디바이스 또는 엔드포인트의 SGT인 경우 디바이스는 인접 디바이스 및 엔드포인트의 SGT(대상 SGT)와 관련된 셀을 다운로드 및 보유합니다.

   CoA 알림의 생성 ID는 디바이스에서 이 SGT용으로 보유하는 생성 ID와는 다릅니다.
3. SGT 데이터 요청에 대한 응답에서 Cisco ISE는 소스 및 대상 SGT, 셀의 상태 및 이 셀에 구성된 SGACL 이름의 순서가 지정된 목록과 같은 모든 이그레스 셀의 데이터를 반환합니다.

이그레스 정책에서 **SGT** 매트릭스 업데이트 **CoA** 시작

단계 **1** **Work Centers**(작업 센터) > **TrustSec** > **TrustSec Policy**(TrustSec 정책) > **Egress Policy**(이그레스 정책)Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 이그레스 정책 페이지에서 셀의 내용(상태, SGACL)을 변경합니다.

단계 **3** 변경사항을 제출하면 해당 셀의 대상 SGT 세대 ID가 승격됩니다.

단계 **4** 여러 이그레스 셀의 내용을 변경한 후 **Push**(푸시) 버튼을 클릭하여 SGT 매트릭스 업데이트 CoA 알림을 시작합니다. 이 알림은 모든 TrustSec 네트워크 디바이스로 전송되며, 관련 디바이스에 대한 셀 내용의 업데이트를 제공합니다.

TrustSec CoA 요약

다음 표에는 TrustSec CoA를 시작해야 할 수 있는 다양한 시나리오, 각 시나리오에서 사용되는 CoA의 유형 및 관련 UI 페이지가 요약되어 있습니다.

표 *141: TrustSec CoA* 요약

UI 페이지	**CoA**를 트리거하는 작업	작업이트리거되는 방법	**CoA** 유형	전송 대상
네트워크디바이스	페이지의 TrustSec 섹션에서 환경 TTL 변경	TrustSec 네트워크 디바이스의 제출 성공	환경	특정 네트워크 디바이스
TrustSec AAA 서버	TrustSec AAA 서버에서 수행하는 변경(생성, 업데이트, 삭제, 순서 바꾸기)	TrustSec AAA 서버 목록 페이지에서 Push(푸시) 버튼을 클릭하여 누적 변경사항을 푸시할 수 있음	환경	모든 TrustSec 네트워크 디바이스
보안 그룹	SGT에서 수행하는 변경(생성, 이름 바꾸기, 삭제)	SGT 목록 페이지에서 Push(푸시) 버튼을 클릭하여 누적 변경사항을 푸시할 수 있음	환경	모든 TrustSec 네트워크 디바이스
NDAC 정책	NDAC 정책에서 수행하는 변경(생성, 업데이트, 삭제)	NDAC 정책 페이지에서 Push(푸시) 버튼을 클릭하여 누적 변경사항을 푸시할 수 있음	환경	모든 TrustSec 네트워크 디바이스
SGACL	SGACL ACE 변경	SGACL 목록 페이지에서 Push(푸시) 버튼을 클릭하여 누적 변경사항을 푸시할 수 있음	RBACL 명명된 목록 업데이트	모든 TrustSec 네트워크 디바이스
	SGACL 이름 또는 IP 버전 변경	SGT 목록 페이지의 Push(푸시) 버튼 또는 이그레스 표의 Policy Push(정책 푸시) 버튼을 클릭하여 누적 변경사항을 푸시할 수 있음	SGT 매트릭스업데이트	모든 TrustSec 네트워크 디바이스
이그레스 정책	SGT의 세대 ID를 변경하는 모든 작업	이그레스 정책 페이지에서 Push(푸시) 버튼을 클릭하여 누적 변경사항을 푸시할 수 있음	SGT 매트릭스업데이트	모든 TrustSec 네트워크 디바이스

Security Group Tag Exchange Protocol

SXP(SGT[Security Group Tag] Exchange Protocol)는 TrustSec에 하드웨어가 지원되지 않는 네트워크 장치 간에 SGT를 전파하는 데 사용됩니다. SXP는 SGT 인식 네트워크 디바이스 간에 엔드포인트 SGT를 IP 주소와 함께 전송하는 데 사용됩니다. SXP가 전송하는 데이터는 IP-SGT 매핑입니다. 엔드포인트가 속하는 SGT는 정적 또는 동적으로 할당할 수 있으며, SGT를 네트워크 정책에서 분류자로 사용할 수 있습니다.

노드에서 SXP 서비스를 활성화하려면 General Node Settings(일반 노드 설정) 페이지에서 Enable SXP Service(SXP 서비스 활성화) 확인란을 선택합니다. SXP 서비스에 사용할 인터페이스도 지정해야 합니다.

SXP는 TCP를 전송 프로토콜로 사용하여 두 개별 네트워크 디바이스 간에 SXP 연결을 설정합니다. 각 SXP 연결에는 SXP 스피커로 지정된 피어와 SXP 리스너로 지정된 피어가 하나씩 있습니다. 각 피어가 스피커와 리스너 역할을 모두 수행하는 양방향 모드로 피어를 구성할 수도 있습니다. 두 피어 중 하나가 연결을 시작할 수 있지만 매핑 정보는 항상 스피커에서 리스너로 전파됩니다.

참고 세션 바인딩은 항상 기본 SXP 도메인에서 전파됩니다.

다음 표에는 SXP 환경에서 일반적으로 사용되는 몇 가지 용어가 나와 있습니다.

IP-SGT 매핑	SXP 연결을 통해 교환되는 IP 주소에서 SGT로의 매핑입니다. 정적 매핑과 세션 매핑을 포함하여 SXP 디바이스에서 학습한 모든 매핑을 확인하려면 **Work Centers(**작업 센터**) > TrustSec > SXP > All SXP Mappings(**모든 **SXP** 매핑**)**를 선택합니다.
SXP 스피커	SXP 연결을 통해 IP-SGT 매핑을 전송하는 피어입니다.
SXP 리스너	SXP 연결을 통해 IP-SGT 매핑을 수신하는 피어입니다.

Cisco ISE에 추가된 SXP 피어 디바이스를 확인하려면 **Work Centers(**작업 센터**) > TrustSec > SXP > SXP Devices(SXP** 디바이스**)**를 선택합니다.

참고 SXP 서비스는 독립형 노드에서 실행하는 것이 좋습니다.

SXP 서비스를 사용할 때는 다음 사항에 유의하십시오.

- Cisco ISE는 같은 IP 주소를 사용하는 여러 SXP 세션 바인딩을 지원하지 않습니다.
- RADIUS 어카운팅 업데이트가 너무 자주 발생한다면(예: 몇 초 골랑 어카운팅 업데이트 6~8회), 어카운팅 업데이트 패킷이 손실되고 SXP에서 IP-SGT 바인딩을 수신하지 못할 수 있습니다.

- 이전 버전 ISE에서의 업그레이드가 끝나도 SXP가 자동으로 시작되지는 않습니다. 업그레이드가 끝나면 SXP 비밀번호를 변경하고 SXP 프로세스를 재시작해야 합니다.

SXP 디바이스 추가

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Work Centers(**작업 센터**) > TrustSec > SXP > SXP Devices(SXP** 디바이스**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 다음과 같이 디바이스 세부정보를 입력합니다.

- CSV 파일을 사용하여 SXP 디바이스를 추가하려면 **Upload from a CSV file(CSV** 파일에서 업로드**)**을 클릭합니다. CSV 파일을 찾아 선택한 다음 **Upload(**업로드**)**를 클릭합니다.

  CSV 템플릿 파일을 다운로드하여 추가할 디바이스의 세부정보를 채운 다음 CSV 파일을 업로드할 수도 있습니다.

- 각 SXP 디바이스에 대해 디바이스 세부정보를 수동으로 추가하려면 **Add Single Device(**단일 디바이스 추가**)**를 클릭합니다.

  피어 디바이스의 이름, IP 주소, SXP 역할(리스너, 스피커 또는 둘 다), 비밀번호 유형, SXP 버전 및 연결된 PSN을 입력합니다. 또한 피어 디바이스가 연결되는 SXP 도메인도 지정해야 합니다.

단계 **4** (선택 사항) **Advanced Settings(**고급 설정**)**를 클릭하고 다음 세부정보를 입력합니다.

- Minimum Acceptable Hold Timer(허용되는 최소 보류 타이머) - 스피커가 연결을 유지하기 위해 keepalive 메시지를 전송하는 시간을 초 단위로 지정합니다. 1~65534 사이의 값을 입력할 수 있습니다.
- Keep Alive Timer(keepalive 타이머) - 간격 중에 업데이트 메시지를 통해 내보내지는 다른 정보가 없을 때 스피커가 keepalive 메시지 디스패치를 트리거하는 데 사용됩니다. 0~64000 사이의 값을 입력할 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

SXP 도메인 필터 추가

정적 매핑과 세션 매핑을 포함하여 SXP 디바이스에서 학습한 모든 매핑을 확인할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > SXP > Static SXP Mappings(**정적 **SXP** 매핑**)**를 선택하면 됩니다**.**

기본적으로 네트워크 디바이스에서 학습된 세션 매핑은 기본 VPN 그룹으로만 전송됩니다. SXP 도메인 필터를 생성하여 다른 SXP 도메인(VPN)에 매핑을 전송할 수 있습니다.

IP-SGT 매핑에서 구성된 가상 네트워크를 기반으로 이 창에서 자동으로 생성된 매핑을 찾을 수 있습니다.

참고 Cisco ISE 3.0부터 네트워크 디바이스는 둘 이상의 SXP 도메인에 속할 수 있습니다.

SXP 도메인 필터를 추가하려면 다음을 수행합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > SXP > All SXP Mappings(**모든 **SXP** 매핑**)**를 선택합니다.

단계 **2** **Add SXP Domain Filter(SXP** 도메인 필터 추가**)**를 클릭합니다.

단계 **3** 다음을 수행합니다.

- 서브넷 세부정보를 입력합니다. 이 서브넷에서 IP 주소가 있는 네트워크 디바이스의 세션 매핑은 **SXP Domain(SXP** 도메인**)** 필드에서 선택한 SXP 도메인(VPN)으로 전송됩니다.
- SGT 드롭다운 목록에서 SGT를 선택합니다. 이 SGT와 관련된 세션 매핑은 **SXP Domain(SXP** 도메인**)** 필드에서 선택한 SXP 도메인으로 전송됩니다.

  서브넷 및 SGT를 모두 지정한 경우 이 필터와 일치하는 세션 매핑이 **SXP Domain(SXP** 도메인**)** 필드에서 선택한 SXP 도메인으로 전송됩니다.
- 드롭다운 목록에서 Virtual Network(가상 네트워크)를 선택합니다. 이 가상 네트워크와 관련된 세션 매핑은 **SXP Domain(SXP** 도메인**)** 필드에서 선택한 SXP 도메인으로 전송됩니다.
- 매핑을 전송해야 하는 SXP 도메인을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

SXP 도메인 필터를 업데이트하거나 삭제할 수도 있습니다. 필터를 업데이트하려면 **Manage SXP Domain Filter(SXP** 도메인 필터 관리**)**를 클릭하고 업데이트할 필터 옆의 확인란을 선택한 다음, **Edit(**편집**)**를 클릭합니다. 필터를 삭제하려면 삭제할 필터 옆의 확인란을 선택하고 **Trash(**휴지통**) > Selected(**선택한 항목**)**를 클릭합니다.

SXP 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Settings(**설정**) > SXP Settings(SXP** 설정**)**를 선택합니다.

단계 **2** SXP Settings(SXP 설정) 페이지에서 필요한 세부정보를 입력합니다.

Publish SXP Bindings on PxGrid(PxGrid에 **SXP** 바인딩 게시**)** 확인란을 선택 취소하면 네트워크 디바이스 간에 IP-SGT 매핑이 전파되지 않습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

참고 SXP 설정을 변경하면 SXP 서비스가 재시작됩니다.

TrustSec-Cisco ACI 통합

Cisco ISE에서는 Cisco ACI(Application Centric Infrastructure)의 IEPG(Internal Endpoint Group), EEPG(External Endpoint Group) 및 EP(Endpoint) 컨피그레이션을 SGT 및 SXP 매핑과 동기화할 수 있습니다.

Cisco ISE는 IEPG를 동기화하고 ISE에서 상관관계가 있는 읽기 전용 SGT를 생성하여 Cisco ACI 도메인에서 TrustSec 도메인으로 전송되는 패킷을 지원합니다. 이러한 SGT는 Cisco ACI에 구성된 엔드포인트를 매핑하고 ISE에서 상관관계가 있는 SXP 매핑을 생성합니다. 이러한 SGT는 Security Groups(보안 그룹) 페이지에 표시됩니다(Learned From[학습 위치] 필드의 값은 "Cisco ACI"). All SXP Mappings(모든 SXP 매핑) 페이지에서 SXP 매핑을 확인할 수 있습니다. 이러한 매핑은 Cisco ACI Settings(Cisco ACI 설정) 페이지에서 Policy Plane(정책 플레인) 옵션을 선택하고 Cisco ACI Settings(Cisco ACI 설정) 페이지에서 구성된 SXP 도메인에 SXP 디바이스가 속하는 경우에만 Cisco ACI에 전송됩니다.

참고 읽기 전용 SGT는 IP-SGT 매핑, 매핑 그룹 및 SXP 로컬 매핑에 사용할 수 없습니다.

보안 그룹을 추가할 때 **Propagate to ACI(ACI**로 전파**)** 옵션을 활성화하여 SGT를 Cisco ACI로 전송할지 여부를 지정할 수 있습니다. 이 옵션을 활성화하면 이 SGT와 관련된 SXP 매핑이 Cisco ACI로 전송됩니다. 단, 이는 Cisco ACI Settings(Cisco ACI 설정) 페이지에서 Policy Plane(정책 플레인) 옵션을 선택하고 Cisco ACI Settings(Cisco ACI 설정) 페이지에서 구성된 SXP 도메인에 SXP 디바이스가 속하는 경우에 한합니다.

Cisco ACI는 SGT를 동기화하고 상관관계가 있는 EEPG를 생성하여 TrustSec 도메인에서 Cisco ACI 도메인으로 전송되는 패킷을 지원합니다. Cisco ACI는 Cisco ISE에서 전달되는 SXP 매핑을 기반으로 하여 EEPG 아래에 서브넷을 생성합니다. 해당하는 SXP 매핑을 Cisco ISE에서 삭제해도 이러한 서브넷은 Cisco ACI에서 삭제되지 않습니다.

Cisco ACI에서 IEPG를 업데이트하면 Cisco ISE에서 해당 SGT 컨피그레이션이 업데이트됩니다. Cisco ISE에서 SGT를 추가하면 Cisco ACI에서 새 EEPG가 생성됩니다. SGT를 삭제하면 Cisco ACI에서 해당 EEPG가 삭제됩니다. Cisco ACI에서 엔드포인트를 업데이트하면 Cisco ISE에서 해당 SXP 매핑이 업데이트됩니다.

Cisco ACI 서버와의 연결이 끊기면 Cisco ISE는 연결이 다시 설정될 때 데이터를 다시 동기화합니다.

참고 Cisco ACI 통합 기능을 사용하려면 SXP 서비스를 활성화해야 합니다.

Cisco ISE에서 Cisco ACI로 전송된 모든 바인딩 또는 그 반대로 전송된 모든 바인딩은 **All ACI Mappings(**모든 **ACI** 매핑**)** 창에서 볼 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **TrustSec** > **ACI**. Cisco ACI에서 바인딩을 학습하면 **Learned By(**학습자**)** 열에 **ACI**가 표시되고 **PSNs involved(**관련 **PSN)** 열은 비어 있습니다. 반면 바인딩이 Cisco ISE에서 Cisco ACI로 전송되는 경우 **Learned By(**학습자**)** 열에 바인딩 유형(예: 정적, SXP 또는 세션)이 표시되고, **PSNs involved(**관련 **PSN)**의 열에는 관련 PSN의 FQDN이 표시됩니다. ACI로 전송되는 바인딩에 대한 테넌트 정보도 **VN** 열에 표시됩니다(*tenant:VN* 형식).

참고 Cisco ISE와 Cisco ACI를 성공적으로 통합하려면 서명된 인증서에 적절한 SAN 필드가 있어야 합니다. Cisco ISE는 APIC 서버에서 제공하는 인증서의 SAN 확장 속성에 지정된 값을 사용합니다.

참고 Cisco ACI와의 IPv4-SXP 바인딩만 현재 Cisco ISE에서 지원됩니다. Cisco ACI의 IPv6-SGT 바인딩은 지원되지 않습니다.

ACI 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** > **Import(**가져오기**)**.

단계 **2** Cisco ACI 인증서를 가져옵니다. 자세한 내용은 신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 177 페이지를 참고하십시오.

단계 **3** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **TrustSec** > **Settings(**설정**)** > **ACI Settings(ACI** 설정**)**.

단계 **4** **Enable ACI Integration(ACI** 통합 활성화**)** 확인란을 선택하여 Cisco ACI에서 엔드포인트를 학습하고 SXP를 사용하여 전파합니다.

단계 **5** 다음 옵션 중 하나를 선택합니다.

- 데이터 플레인/하드웨어 통합
- 정책 플레인/**API** 통합

참고 **Data Plane / Hardware Integration(**데이터 플레인/하드웨어 통합**)**을 선택하는 경우 Cisco ISE를 Cisco DNA 센터와 통합해야 합니다. **Policy Plane / API Integration(**정책 플레인/**API** 통합**)**을 선택하는 경우 활성 SXP 서비스가 없으면 SXP 전파가 불가능합니다. 이 옵션을 선택하기 전에 **Deployment(**구축**)** 창에서 SXP 서비스를 활성화합니다.

단계 **6** **Data Plane / Hardware Integration(**데이터 플레인/하드웨어 통합**)**을 선택하는 경우 다음 세부정보를 입력합니다.

- **IP address(IP** 주소**)**: Cisco ACI 서버의 IP 주소 또는 호스트 이름을 입력합니다. IP 주소 또는 호스트 이름 3개를 쉼표로 구분하여 입력할 수 있습니다.
- **Username(**사용자 이름**)**: Cisco ACI 관리 사용자의 사용자 이름을 입력합니다.
- **Password(**비밀번호**)**: Cisco ACI 관리 사용자의 비밀번호를 입력합니다.
- **Tenant name(**테넌트 이름**)**: Cisco ACI에 구성되어 있는 테넌트의 이름을 입력합니다.
- **Test Connection to ACI(ACI**에 대한 연결 테스트**)**: Cisco ACI 서버와의 연결을 확인하려면 이 버튼을 클릭합니다.
- **Renew Certificate(**인증서 갱신**)**: 도메인 관리자 새로 고침을 수행하려면 이 버튼을 클릭합니다. 인증서는 일반적으로 10년 동안 유효합니다. 인증서를 갱신하기 전에 시스템에서 성공적인 피어링을 사용할 수 있어야 합니다. 인증서 갱신 후 구축의 모든 노드 CLI에서 Cisco ISE 애플리케이션을 다시 시작해야 합니다. 대략적인 인증서 갱신 시간은 5분입니다.
- **New SGT Suffix(**새 **SGT** 접미사**)**: 이 접미사는 Cisco ACI에서 학습된 EPG를 기준으로 새로 생성되는 SGT에 추가됩니다.

  참고 EPG 이름은 32자보다 길면 잘립니다. 그러나 Security Groups(보안 그룹) 목록 페이지의 Description(설명) 필드에서 EPG의 전체 이름, 애플리케이션 프로파일 이름 및 SGT 접미사 세부정보를 확인할 수 있습니다.

- **New EPG Suffix(**새 **EPG** 접미사**)**: 이 접미사는 Cisco ISE에서 학습된 SGT를 기준으로 Cisco ACI에서 새로 생성되는 EPG에 추가됩니다.
- **Enable Data Plane(**데이터 플레인 활성화**)**: 보더 라우터에 대한 변환 표을 다운로드하려면 이 확인란을 선택합니다. 이 확인란을 선택하는 경우 다른 기존 SGT와 일치시킬 수 없는 패킷의 기본 SGT 이름을 선택해야 합니다.
  - **Default SGT name(**기본 **SGT** 이름**)**: 드롭다운 목록에서 SGT의 기본 이름을 선택합니다.
- **Enable Elements Limit(**요소 제한 활성화**)**: 이 옵션은 데이터 플레인을 활성화하는 경우에만 사용할 수 있습니다.
  - **Max number of IEPGs(IEPG** 최대 수**)**: SGT로 변환할 최대 IEPG 수를 지정합니다. IEPG는 알파벳 순서로 변환됩니다. 기본값은 1000입니다.
  - **Max number of SGTs(SGT** 최대 수**)**: IEPG로 변환할 최대 SGT 수를 지정합니다. SGT는 알파벳 순서로 변환됩니다. 기본값은 500입니다.

단계 **7** **Policy Plane / API Integration(**정책 플레인/**API** 통합**)** 옵션을 선택한 경우 다음 세부정보를 입력하십시오.

- **IP address / Host name(IP** 주소/호스트 이름**)**: Cisco ACI 서버의 IP 주소 또는 호스트 이름을 입력합니다. IP 주소 또는 호스트 이름 3개를 쉼표로 구분하여 입력할 수 있습니다.
- **Admin name(**관리자 이름**)**: Cisco ACI 관리 사용자 이름을 입력합니다.
- **Admin password(**관리자 비밀번호**)**: Cisco ACI 관리 사용자 비밀번호를 입력합니다.
- **Tenant name(**테넌트 이름**)**: Cisco ACI에 구성되어 있는 테넌트의 이름을 입력합니다.
- **L3 Route network name(L3** 경로 네트워크 이름**)**: 정책 요소 동기화를 위해 Cisco ACI에 구성되어 있는 레이어 3 경로 네트워크의 이름을 입력합니다.
- **Test Settings(**테스트 설정**)**: Cisco ACI 서버와의 연결을 확인하려면 이 버튼을 클릭합니다.
- **New SGT Suffix(**새 **SGT** 접미사**)**: 이 접미사는 Cisco ACI에서 학습된 EPG를 기준으로 새로 생성되는 SGT에 추가됩니다.
- **New EPG Suffix(**새 **EPG** 접미사**)**: 이 접미사는 Cisco ISE에서 학습된 SGT를 기준으로 Cisco ACI에서 새로 생성되는 EPG에 추가됩니다.
- **SXP Propagation(SXP** 전파**)** 영역에서 모든 SXP 도메인을 선택하거나 Cisco ACI와 매핑을 공유할 SXP 도메인을 지정할 수 있습니다.
- **Enable Data Plane(**데이터 플레인 활성화**)**: 보더 라우터에 대한 변환 표을 다운로드하려면 이 확인란을 선택합니다. 이 확인란을 선택하는 경우 다른 기존 SGT와 일치시킬 수 없는 패킷의 기본 SGT 이름을 선택해야 합니다.
  - **EEPG name for untagged packets(**태그가 없는 패킷용 **EEPG** 이름**)**: EEPG로 변환되지 않은 Cisco TrustSec 패킷은 Cisco ACI에서 이 이름으로 태그가 지정됩니다.
  - **Default SGT name(**기본 **SGT** 이름**)**: 드롭다운 목록에서 SGT의 기본 이름을 선택합니다.
- **Enable Elements Limit(**요소 제한 활성화**)**: 이 옵션은 데이터 플레인을 활성화하는 경우에만 사용할 수 있습니다.
  - **Max number of IEPGs(IEPG** 최대 수**)**: SGT로 변환할 최대 IEPG 수를 지정합니다. IEPG는 알파벳 순서로 변환됩니다. 기본값은 1000입니다.
  - **Max number of SGTs(SGT** 최대 수**)**: IEPG로 변환할 최대 SGT 수를 지정합니다. SGT는 알파벳 순서로 변환됩니다. 기본값은 500입니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

참고 ACI 통합 옵션이 활성화된 경우 EPG 및 SGT 접미사를 변경할 수 없습니다. EPG 및 SGT 접미사를 변경하려면 먼저 **Enable ACI Integration(ACI** 통합 활성화**)** 옵션을 비활성화해야 합니다.

Cisco ACI 및 Cisco SD-Access와 가상 네트워크 인식 통합

Cisco ISE 릴리스 2.7에서는 SGT 및 SXP 매핑을 IEPG(Internal Endpoint Groups), EEPG(External Endpoint Groups) 및 Cisco ACI의 엔드포인트 컨피그레이션과 동기화하는 기본 구현이 있습니다.

Cisco ISE 릴리스 3.0은 Cisco ACI 인프라를 사용하는 Cisco SD-Access(Software-Defined Access) 패브릭에 대한 향상된 정보 교환 및 도메인 간 자동화 변환을 제공하는 추가 구현을 지원합니다. 구현은 다음을 지원합니다.

- EPG 및 SGT 정보 교환 및 변환
- Cisco ACI 패브릭으로 Cisco SD-Access 가상 네트워크 확장
- Cisco SD-Access 및 Cisco ACI 패브릭 데이터 플레인 자동화
- IP-SGT 바인딩 교환
- pxGrid 및 SXP 도메인에 바인딩 전송

Cisco ISE는 RADIUS 바인딩 또는 Cisco ACI 바인딩에서 가상 네트워크 정보를 학습하고 특정 가상 네트워크에 대한 로컬 정적 매핑을 제공합니다. 가상 네트워크를 사용하여 Cisco ACI와의 IP-SGT 바인딩 공유를 조정하는 데 사용되는 SXP 필터 논리를 개선할 수 있습니다. SXP 도메인과 가상 네트워크는 Cisco ACI로 확장되는 가상 네트워크가 Cisco ACI와 IP-SGT 바인딩을 공유하는 유일한 구성이라는 점에서 밀접하게 연결되어 있습니다. 따라서 특정 SXP 도메인(SD-Access- 접두사로 표시)은 Cisco ISE에서 동등한 가상 네트워크(SXP 도메인에서 SD-Access- 접두사 제외)에 매핑됩니다.

Cisco SD-Access 경계 노드가 Cisco CI 바인딩에 대해 알 수 있도록 Cisco ACI 바인딩은 SXP 필터 논리를 통해 전송되기 전에 모든 확장된 가상 네트워크에서 생성된 것처럼 복제됩니다. 예를 들어 Cisco SD-Access 가상 네트워크 1, 가상 네트워크 2 및 가상 네트워크 3이 Cisco ACI로 확장되는 경우 원래 Cisco ACI 가상 네트워크를 사용하는 Cisco ACI의 바인딩은 SXP 필터를 통해 4번 전송됩니다. 이렇게 정확히 똑같은 바인딩이 전체 가상 네트워크 4개의 필터를 통과합니다. 필터는 특정 구축 요건에 따라 수정되고 맞춤 설정될 수 있습니다. 단, 모든 확장된 가상 네트워크에서는 항상 복제가 수행됩니다.

Cisco ISE는 가능한 경우 Cisco ACI의 IP-SGT, EPG 바인딩에 대해 학습합니다. 그러나 Cisco ISE가 Cisco ACI에서 바인딩을 학습하도록 강제할 수는 없습니다. Cisco ACI는 Cisco ISE에서 바인딩을 명시적으로 요청해야 합니다.

다음 표에는 Cisco ISE에서 IP-SGT 또는 IP-EPG 바인딩에 사용할 수 있는 소스 및 대상 조합이 나와 있습니다.

소스 도메인	대상 도메인	소스 그룹	대상 그룹	메모
Cisco ACI	SXP	Cisco ACI 가상 네트워크	SXP 도메인	Cisco ACI 가상 네트워크를 SXP 필터에서 키로 사용하여 하나 이상의 SXP 도메인과 바인딩을 공유할 수 있습니다.

Cisco ACI	pxGrid	Cisco ACI 가상 네트워크	pxGrid의 SXP 항목에 대한 VPN	Cisco ACI 가상 네트워크를 SXP 필터에서 키로 사용하여 pxGrid에서 하나 이상의 SXP VPN과 바인딩을 공유할 수 있습니다.
Cisco ACI	Cisco SD-Access 경계 노드	Cisco SD-Access 확장 가상 네트워크	SXP 도메인	Cisco ACI 바인딩은 경계 노드 가상 네트워크 정보 교환을 위해 자동으로 생성된 모든 SXP 도메인("SD-Access-"를 접두사하는 도메인)과 공유됩니다.
Cisco ISE 정적 매핑	SXP	Cisco SD-Access 가상 네트워크 또는 기존 SXP 도메인	SXP 도메인	정적 바인딩은 SXP 도메인에 직접 전송되거나(정적 매핑에서 SXP 도메인 지정) SXP 필터를 통해(가상 네트워크 정보와 함께) 전송될 수 있습니다. 가상 네트워크가 지정되지 않은 경우 SXP 필터는 가상 네트워크에 DEFAULT_VN을 사용합니다.
Cisco ISE 정적 매핑	pxGrid	Cisco SD-Access 가상 네트워크	SXP 도메인	정적 바인딩은 SXP 도메인에 직접 전송되거나(정적 매핑에서 SXP 도메인 지정) SXP 필터를 통해(가상 네트워크 정보와 함께) 전송될 수 있습니다. 가상 네트워크가 지정되지 않은 경우 SXP 필터는 가상 네트워크에 DEFAULT_VN을 사용합니다.
Cisco ISE 정적 매핑	Cisco ACI	Cisco SD-Access 가상 네트워크	Cisco SD-Access 가상 네트워크	Cisco SD-Access 가상 네트워크는 Cisco ACI(mdpExtendvirtual networkReq)로 확장되어야 하며, 바인딩은 SXP 필터의 가상 네트워크를 사용하여 가상 네트워크에 매핑된 SXP 도메인과 함께 Cisco ACI에 바인딩을 전송합니다.
SXP	pxGrid	SXP 도메인	SXP 도메인	SXP 도메인은 pxGrid의 SXP 항목에 VPN으로 표시됩니다.
SXP	Cisco ACI	SXP 도메인	Cisco SD-Access 가상 네트워크	SXP 도메인 공유가 Cisco ACI 설정에서 선택됩니다. Cisco SD-Access 가상 네트워크(가상 네트워크 등가 SXP 도메인)에서 자동으로 생성된 SXP 도메인만 공유됩니다. 가상 네트워크가 바인딩을 공유할 수 있도록 Cisco SD-Access 가상 네트워크를 Cisco ACI로 확장해야 합니다. 바인딩은 Cisco ACI가 엔드포인트 데이터를 요청하는 소비자 서비스의 일부여야 합니다.
SXP	SXP	SXP 도메인	SXP 도메인	우선순위를 지정하는 SXP 바인딩이 공유됩니다.

RADIUS 바인딩	Cisco ACI	Cisco SD-Access 가상 네트워크	Cisco SD-Access 가상 네트워크	RADIUS 바인딩은 가상 네트워크 정보와 함께 SXP 필터를 통해 전송됩니다. 바인딩에 가상 네트워크가 지정되지 않은 경우 SXP 필터는 가상 네트워크에 대해 DEFAULT_VN을 사용합니다.
RADIUS 바인딩	pxGrid	Cisco SD-Access 가상 네트워크	Cisco SD-Access 가상 네트워크	RADIUS 바인딩은 항목에 가상 네트워크 필드가 추가된 상태로 pxGrid의 세션 디렉토리 항목으로 연결됩니다.
RADIUS 바인딩	SXP	Cisco SD-Access 가상 네트워크	SXP 도메인	Cisco SD-Access 가상 네트워크를 SXP 필터에서 키로 사용하여 바인딩을 공유할 SXP 도메인을 선택할 수 있습니다.

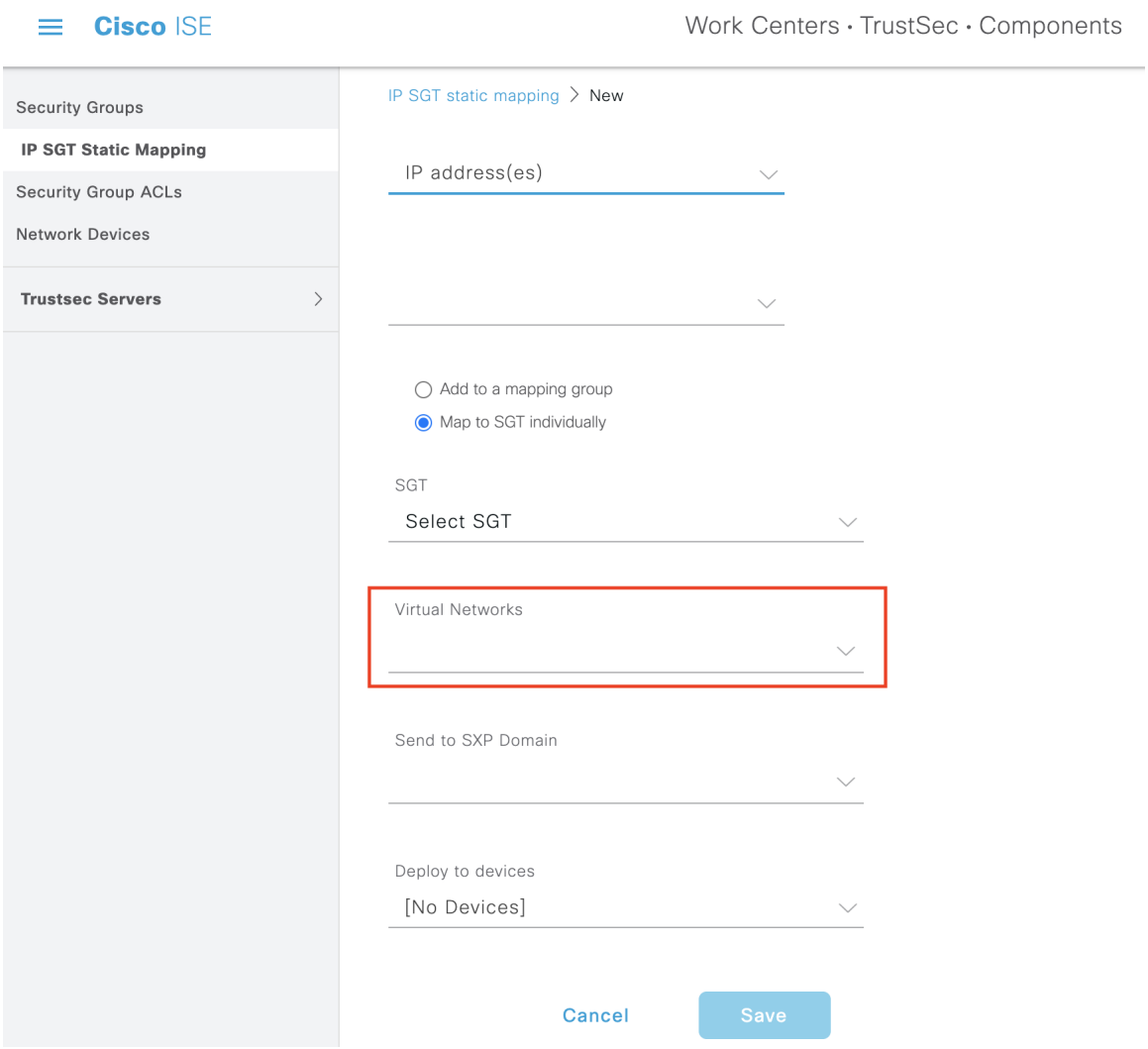
도메인 간 지원을 촉진하려면 다양한 네트워크 전환 도메인(예: IP 주소, 서브넷 마스크, 보안 그룹 태그, EPG, 가상 네트워크, VRF(가상 라우팅 및 포워딩))을 교환하고 필터링하는 기능이 있어야 합니다. 정책 도메인 또는 정책 도메인 내의 전환 도메인에서 다른 도메인으로 또는 그 반대로 교환하고 필터링할 수 있습니다. 이는 Cisco SD-Access, Cisco ACI, SD-WAN, CPC, Meraki 등의 정책 도메인에 여러 전환 도메인이 있는 경우 특히 중요합니다.

정책 도메인의 네트워크별 전환 도메인과 다른 정책 도메인에서 학습된 모든 세션 및 바인딩에 대한 도메인별 속성을 식별, 캡처 및 저장할 수 있습니다. 이는 정책 관리자가 세션 및 특정 SXP 도메인에 대한 바인딩을 필터링하는 데 사용됩니다. 또한 관리자는 하나의 전환 도메인에서 다른 전환 도메인으로 특정 바인딩만 매핑하거나 필터링하는 정책을 생성할 수 있습니다.

Cisco ISE 3.0부터는 Cisco DNA 센터에서 Cisco ISE가 학습한 모든 가상 네트워크를 통해 SXP Devices(SXP 디바이스) 창에서 자동으로 생성된 SXP 필터 및 SXP 도메인을 찾을 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > SXP > SXP Devices(SXP** 디바이스**)**를 선택합니다. 이러한 SXP 도메인은 이후 Cisco ACI와 공유되는 바인딩에서 가상 네트워크를 설정하는 데 사용됩니다.

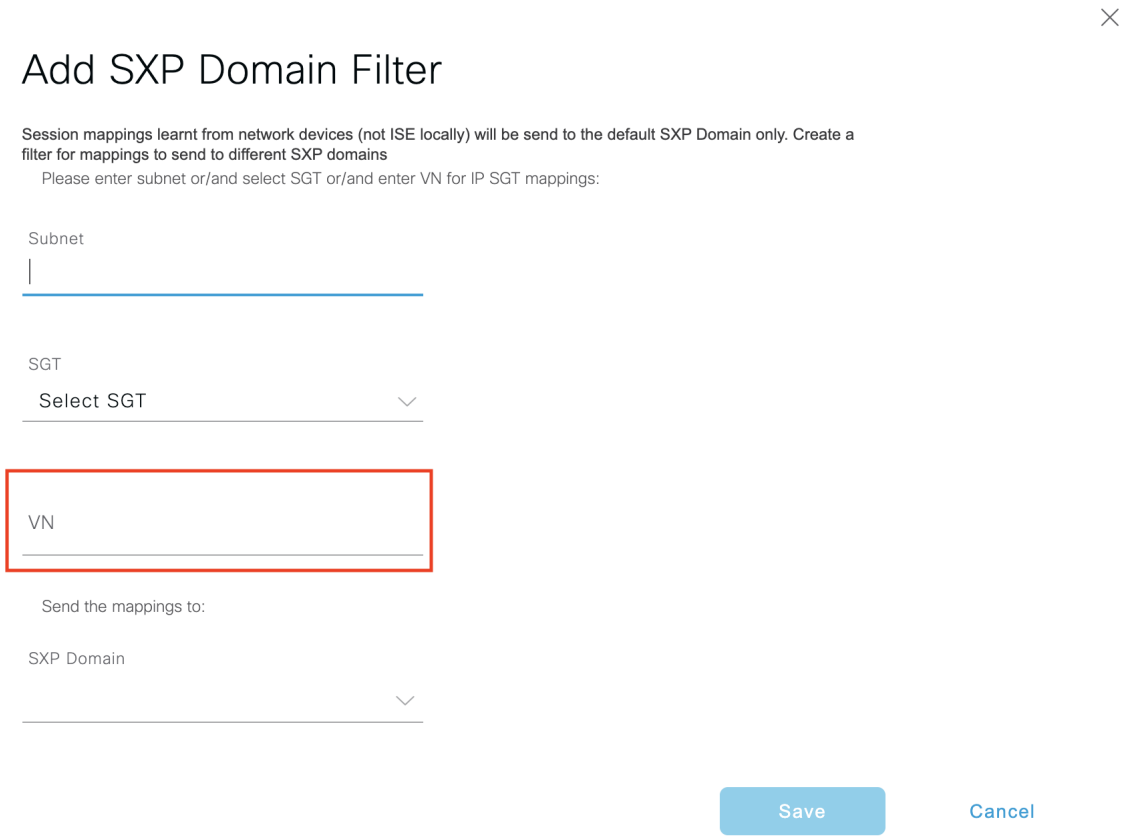
IP-SGT Static Mapping(IP-SGT 정적 매핑) 창에서 IP-SGT 정적 매핑에 가상 네트워크를 추가하고 수정할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > IP SGT Static Mapping(IP SGT** 정적 매핑**)**을 선택합니다. **Add(**추가**)**를 클릭하여 새 매핑을 추가하거나 **Edit(**편집**)**를 클릭하여 기존 매핑을 수정합니다.

그림 *52: IP SGT* 정적 매핑에 가상 네트워크 추가



또한 Cisco ISE에서 수신한 매핑이 특정 가상 네트워크에 매핑될 때 매핑을 전송할 SXP 도메인을 지정하기 위해 SXP 도메인 필터에 가상 네트워크를 포함할 수도 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > SXP > SXP Devices(SXP** 디바이스**) > All SXP Mappings(**모든 **SXP** 매핑**)**를 선택하고 **Add SXP Domain Filter(SXP** 도메인 필터 추가**)**를 클릭합니다. Cisco ACI에서 학습한 바인딩에는 원래 Cisco ACI 가상 네트워크가 있으며, 이러한 필터는 필터에 구성된 SXP 도메인으로 전송됩니다. 이 필터는 바인딩이 Cisco ACI로 전송되는 방식에도 영향을 미칩니다.

그림 ***53: SXP*** 디바이스 필터에서 가상 네트워크 정보 추가



Cisco ACI 및 Cisco SD-Access 통합을 위한 Cisco ISE 구성

이 작업은 Cisco ACI 및 Cisco SD-Access 통합을 지원하도록 Cisco ISE를 구성하는 데 도움이 됩니다.

시작하기 전에

Cisco ISE가 Cisco DNA 센터의 최신 버전과 통합되어 있는지, 사용 중인 APIC 버전이 5.1 이상인지 확인합니다.

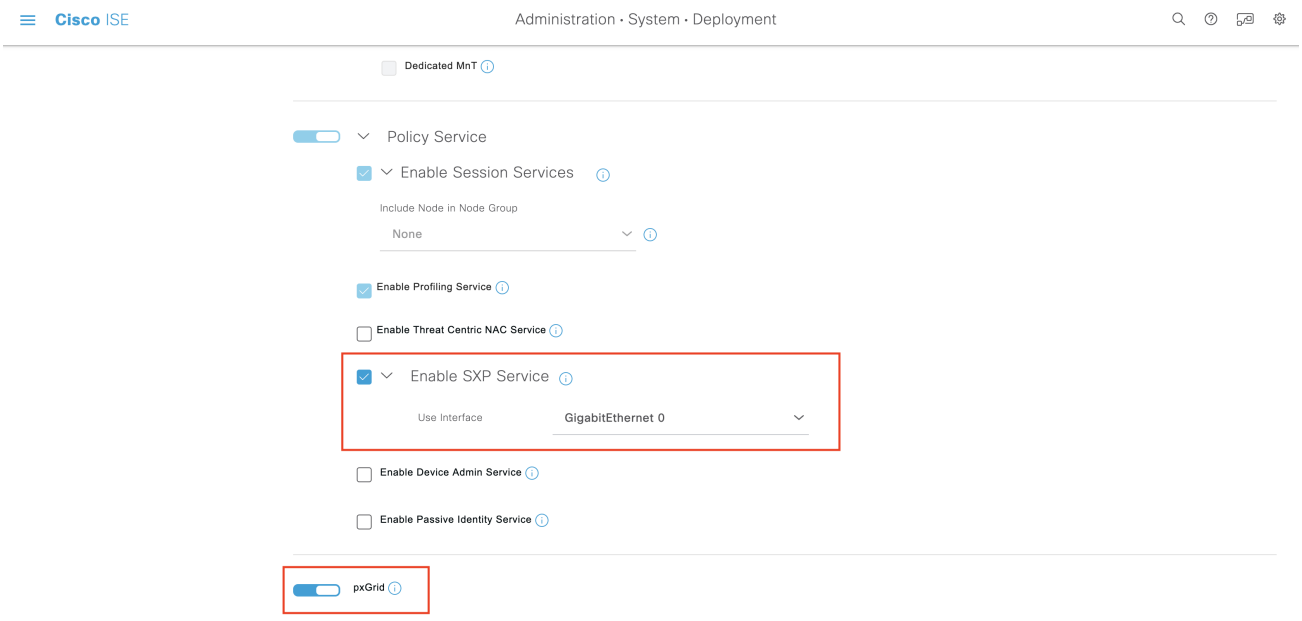
단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Deployment(구축)**를 선택합니다.

단계 **2** 노드 목록에서 SXP 및 pxGrid 서비스를 사용하도록 설정할 노드 옆의 확인란을 선택합니다.

단계 **3** 아래 그림과 같이 **Policy Service(정책 서비스)** 섹션으로 스크롤하여 pxGrid 및 SXP 서비스를 활성화합니다.

Cisco ISE에서 둘 이상의 인터페이스를 활성화한 경우 **Enable SXP Service(SXP 서비스 활성화)** 영역에서 SXP 연결을 유지할 인터페이스를 지정합니다.

그림 ***54: SXP*** 및 ***pxGrid*** 서비스 활성화



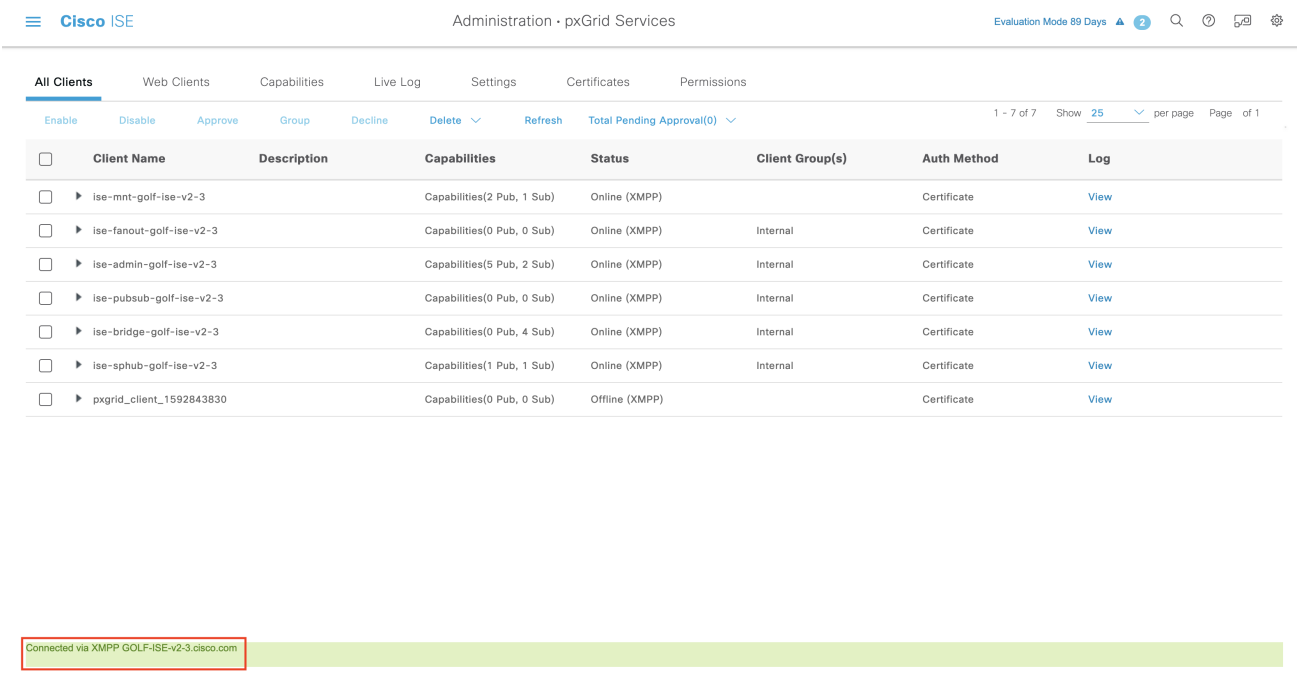
단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **All Clients(**모든 클라이언트**)**를 선택합니다.

단계 **6** pxGrid 서비스가 작동 및 실행 중인지 확인합니다.

다음 그림과 같이 연결 성공 알림은 창의 왼쪽 하단 모서리에 표시됩니다.

그림 ***55: pxGrid*** 서비스에 대한 연결 확인



단계 **7** APIC 컨트롤러 브라우저에서 APIC 인증서를 다운로드합니다. 브라우저의 주소 표시줄에서 잠금 아이콘을 클릭하여 인증서를 확인하고 PEM 파일로 다운로드합니다.

단계 **8** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **9** **Trusted Certificates(**신뢰할 수 있는 인증서**)** 창에서 다운로드한 APIC 인증서 파일을 가져옵니다.

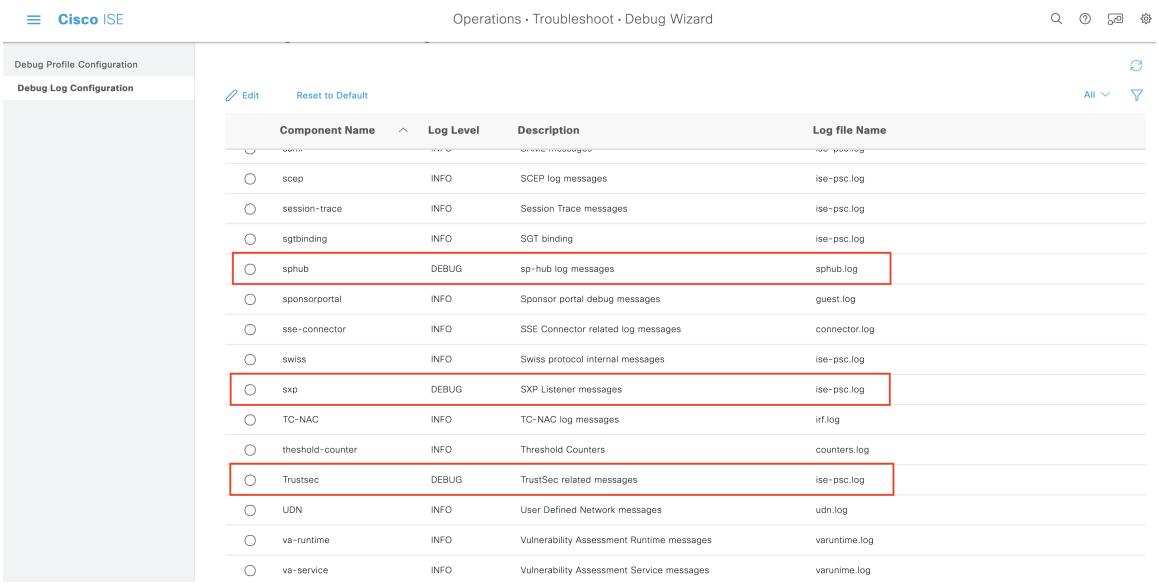
단계 **10** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centres(**작업 센터**)** > **TrustSec** > **Settings(**설정**)** > **ACI Settings(ACI** 설정**)**를 선택합니다.

단계 **11** 필요에 따라 ACI 설정을 구성합니다. 자세한 내용은 ACI 설정 구성, 1064 페이지을 참조해 주십시오.

Cisco ACI 및 Cisco SD-Access 통합 확인

Cisco ACI와 Cisco SD-Access 연결 간 자세한 정보를 확인하려면 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Debug Wizard(**디버그 마법사**)** > **Debug Log Configuration(**디버그 로그 컨피그레이션**)**을 선택합니다. SXP 및 pxGrid 서비스가 활성화된 Cisco ISE 노드를 선택하고 Edit(편집)를 클릭합니다. 다음 그림과 같이 **spbhub**, **sxp** 및 **TrustSec** 구성 요소에 대한 로그 레벨을 DEBUG로 설정합니다.

그림 ***56:*** 디버그 로그 활성화



로그는 **Dowload Logs**(로그 다운로드) 창에서 다운로드할 수 있습니다. (이 창을 보려면 메뉴 아이콘 (☰)을 클릭하고 **Operations**(운영) > **Troubleshoot**(문제 해결) > **Dowload Logs**(로그 다운로드)를 선택합니다.) **Support Bundle**(지원 번들) 탭에서 지원 번들을 다운로드하거나 **Debug Logs**(디버그 로그) 탭에서 특정 디버그 로그를 다운로드하도록 선택할 수 있습니다.

또한, Cisco ACI 관련 문제를 해결하는 데 유용한 Cisco ACI 통합에서 학습된 정보로 TrustSec 대시보드, 1010 페이지가 업데이트되었습니다.

Cisco DNA 센터에서 도메인 광고를 전송한 후에는 Cisco ISE의 **Trusted Certificates**(신뢰할 수 있는 인증서) 창과 **System Certificates**(시스템 인증서) 창에서 APIC 인증서를 APIC 도메인 관리자로부터 가져왔는지를 확인합니다.

그림 ***57: System Certificates***(시스템 인증서) 창의 ***Verify the Certificate***(인증서 확인)

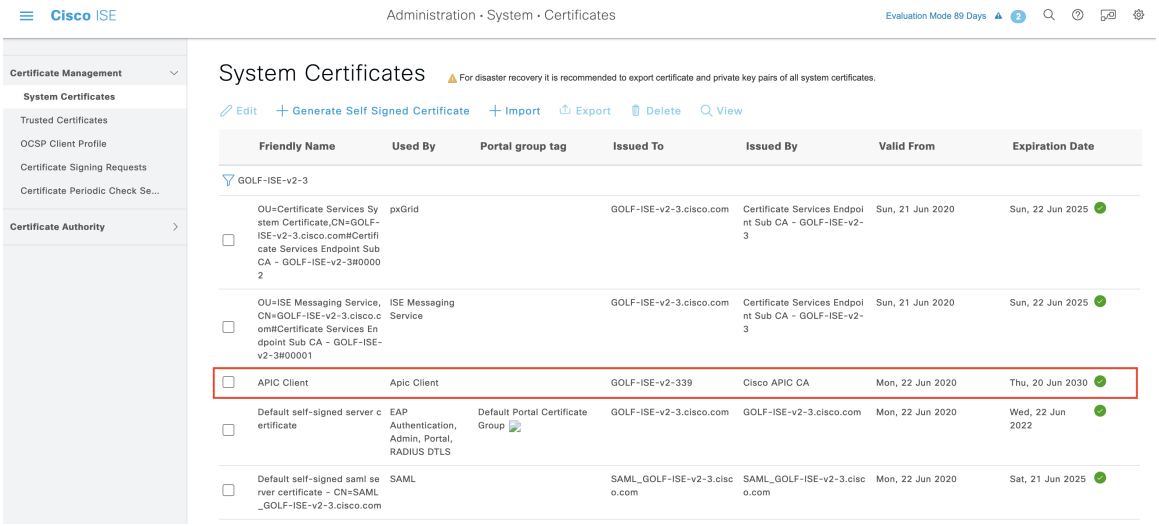
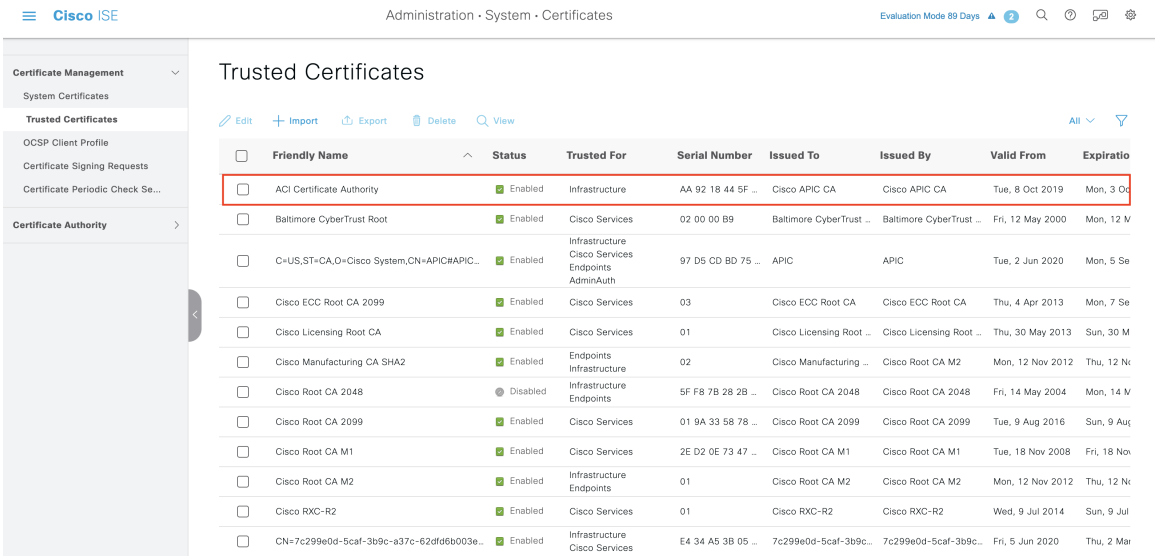


그림 *58: Trusted Certificates(*신뢰할 수 있는 인증서*)* 창의 *Verify the Certificate(*인증서 확인*)*



사용자별 상위 N개 RBACL 삭제 보고서 실행

사용자별 상위 N개 RBACL 삭제 보고서를 실행하여 특정 사용자별로 패킷 삭제 수를 기준으로 하는 정책 위반 사항을 확인할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Top N RBACL Drops by User(**사용자별 상위 **N**개 **RBACL** 삭제**)**를 클릭합니다.

단계 **3** **Filters(**필터**)** 드롭다운 메뉴에서 필요한 모니터 모드를 추가합니다.

단계 **4** 선택한 매개변수에 따라 값을 입력합니다. 시행 모드 드롭다운 목록에서 모드를 시행 Monitor(모니터) 또는 Both(모두)로 지정할 수 있습니다.

단계 **5** **Time Range(**시간 범위**)** 드롭다운 메뉴에서 보고서 데이터를 수집할 기간을 선택합니다.

단계 **6** **Run(**실행**)**을 클릭하여 특정 기간에 대해 선택한 매개변수를 사용하여 보고서를 실행합니다.

12 장

규정 준수

포스처 유형

다음 포스처 에이전트는 Cisco ISE 포스처 정책을 모니터링하고 적용합니다.

- **AnyConnect**: AnyConnect 에이전트를 구축하여 클라이언트와의 상호 작용이 필요한 Cisco ISE Posture 포스처 정책을 모니터링하고 시행합니다. AnyConnect 에이전트는 클라이언트에서 유지됩니다. Cisco ISE에서 AnyConnect를 사용하는 방법에 대한 자세한 내용은 Cisco AnyConnect Secure Mobility, 1187 페이지을 참조하십시오.

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

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

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

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

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

참고 AnyConnect Stealth 모드를 사용하려면 AnyConnect 버전 4.4 이상이 필요합니다.

Cisco ISE에서 AnyConnect Stealth를 구성하는 방법에 대한 자세한 내용은 AnyConnect 스텔스 모드 워크플로우 구성, 1154 페이지을 참조하십시오.

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

  Temporal Agent는 다음 조건을 지원하지 않습니다.

  - 서비스 조건 MAC—시스템 데몬 확인
  - 서비스 조건-MAC—데몬 또는 사용자 에이전트 검사
  - PM—최신 상태 확인
  - PM - 활성화 검사
  - DE—암호화 확인
  - **Posture Types(**포스처 유형**) Temporal Agent(**임시 에이전트**)** 및 **Compliance Module(**규정 준수 모듈**) 4.x** 이상을 사용해 포스처 정책을 구성합니다. 규정 준수 모듈을 **3.x or earlier(3.x** 이하**)** 또는 **Any Version(**모든 버전**)**으로 구성하지 마십시오.
  - Termporal Agent의 경우, **Requirements(**요건**)** 창에서 **Installation(**설치**)** 확인 유형을 포함하는 패치 관리 조건만 볼 수 있습니다.
  - Cisco ISE는 Mac OSX용 Temporal Agent에서 VLAN 제어 포스처를 지원하지 않습니다. 기존 VLAN에서 새 VLAN으로 네트워크 액세스를 변경하면 VLAN 변경 전에 사용자의 IP 주소가 해제됩니다. 사용자가 새 VLAN에 연결할 때 클라이언트는 DHCP를 통해 새 IP 주소를 가져옵니다. 새 IP 주소를 인식하려면 루트 권한이 필요하지만 Temporal Agent는 사용자 프로세스로 실행됩니다.
  - Cisco ISE는 ACL로 제어되는 포스처 환경을 지원하며 여기에서는 엔드포인트의 IP 주소의 새로고침이 필요하지 않습니다.
  - Cisco ISE에서 Temporal Agent를 구성하는 방법에 대한 자세한 내용은 Cisco 임시 에이전트 구성 워크플로우, 1159 페이지을 참조하십시오.

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

를 설치합니다. AMP 프로파일러에 대한 설명은 AMP Enabler 프로파일 설정, 1170 페이지에 제시되어 있습니다.

- **Agentless Posture(**에이전트리스 포스처**)**—에이전트리스 포스처는 클라이언트에서 얻는 포스처 정보를 제공하며 작업이 완료되면 스스로 완전히 제거됩니다. 최종 사용자 측에서 취해야 할 작업은 없습니다. Temporal Agent와 달리 Agentless Posture는 관리 사용자로 클라이언트에 연결합니다. Cisco ISE에서 에이전트리스 포스처를 사용하는 방법에 대한 자세한 내용은 에이전트리스 포스처, 1080 페이지를 참조하십시오.

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

관련 항목

AnyConnect 스텔스 모드 워크플로우 구성, 1154 페이지
Cisco 임시 에이전트 구성 워크플로우, 1159 페이지

에이전트리스 포스처

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

요구 사항

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

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

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

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

지원되는 포스처 조건

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

참고 Mac OSX에서는 서비스 조건이 지원되지 않습니다.

지원되지 않는 포스처 조건

- 교정
- 유예 기간
- 정기적 재평가
- 허용되는 사용 정책

지원되는 클라이언트 운영체제

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

Agentless Posture Process Flow

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

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

에이전트리스 포스처 컨피그레이션

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

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

5. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**에서 권한 부여 정책을 확장합니다. 다음 3가지 권한 부여 정책을 활성화하고 구성합니다.
   - **Unknown_Compliance_Redirect**: Configure conditions Network_Access_Authentication_Passed AND Compliance_Unknown_Devices with result Agentless Posture.
   - **NonCompliant_Devices_Redirect**: Configure conditions Network_Access_Authentication_Passed and Non_Compliant_Devices with result DenyAccess.
   - **Compliant_Devices_Access**: Configure conditions Network_Access_Authentication_Passed and Compliant_Devices with result PermitAccess.
6. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Settings(**설정**)** > **Endpoint Scripts(**엔드포이트 스크립트**)** > **Endpoint Login Configuration(**엔드포인트 로그인 구성**)**에서클라이언트 자격 증명을 구성하고 클라이언트에 로그인합니다. 동일한 자격증명이 엔드포인트 스크립트에서도 사용됩니다. 자세한 내용은 를 참고하십시오.<Link to Endpoint Scripts topic>>.
7. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Settings(**설정**)** > **Endpoint Scripts(**엔드포인트 스크립트**)** > **Settings(**설정**)**에서 **OS** 식별을 위한 최대 재시도 횟수와 **OS** 식별을 위한 재시도 간 지연 시간을 구성합니다. 이러한 설정에 따라 연결 문제를 얼마나 빨리 확인할 수 있는지가 결정됩니다. 예를 들어 PowerShell 포트가 열려 있지 않다는 오류는 재시도가 다 사용되지 않은 경우에로그에 표시되지 않습니다.
8. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Posture(**포스처**)** > **General Settings(**일반 설정**)**에서 에이전트리스 포스처 설정을 구성합니다. 포스처 일반 설정, 1092 페이지을(를) 참조하십시오.
9. 클라이언트가 에이전트리스 포스처에 연결되면 라이브 로그에서 확인할 수 있습니다.

디버깅 및 문제 해결

다음에 대해 디버그 로그 레벨을 활성화합니다.

- 인프라
- 클라이언트 프로비저닝
- 포스처

디버그 로그는 *ise-psc.log*에 있습니다.

에이전트리스 포스처 문제 해결은 다음에서 사용할 수 있습니다.

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

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

에이전트리스 포스처 문제 해결

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

다음 두 위치에서 에이전트리스 포스처 문제 해결에 액세스할 수 있습니다.

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

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

보고서

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

포스처 관리 설정

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

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

클라이언트 포스처 요건

포스처 요건을 생성하려면 다음을 따릅니다.

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

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

표 ***142:*** 포스처 요건

필드 이름	사용 지침
Name(이름)	요건의 이름을 입력합니다.
Operating Systems(운영체제)	운영체제를 선택합니다. 정책에 여러 운영체제를 연결하려면 더하기 [+]를 클릭합니다. 정책에서 운영체제를 제거하려면 빼기 [-]를 클릭합니다.
규정 준수 모듈**(Compliance Module)**	**Compliance Module(규정 준수 모듈)** 드롭다운 목록에서 필요한 규정 준수 모듈을 선택합니다. • 4.x 이상: 안티멀웨어, 디스크 암호화, 패치 관리 및 USB 조건을 지원합니다. • 3.x 이하: 안티바이러스, 안티스파이웨어, 디스크 암호화 및 패치 관리 조건을 지원합니다. • 모든 버전: 파일, 서비스, 레지스트리, 애플리케이션 및 복합 조건을 지원합니다. 규정 준수 모듈에 대한 자세한 내용은 규정 준수 모듈, 1103 페이지에서 참조하십시오.

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

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

관련 항목

Posture Assessment용 사용 제한 정책 구성, 1098 페이지
클라이언트 포스처 요건 생성, 1149 페이지

클라이언트용 타이머 설정

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

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

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

지정된 시간 내에 클라이언트를 교정하기 위한 교정 타이머 설정

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

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

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

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

기본값은 4분입니다. 유효 범위는 1~300분입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

클라이언트를 전환할 네트워크 전환 지연 타이머 설정

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

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

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

기본값은 3초입니다. 유효 범위는 2초~30초입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

로그인 성공 창이 자동으로 닫히도록 설정

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

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

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

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

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

단계 **4** **Save(**저장**)**를 클릭합니다.

에이전트가 아닌 디바이스의 포스처 상태 설정

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

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

시작하기 전에

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

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

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

단계 **3** **Save(**저장**)**를 클릭합니다.

포스처 임대

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

이 컨피그레이션은 포스처 평가에 AnyConnect 에이전트를 사용하는 사용자에게만 적용됩니다.

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

활용 사례 시나리오 예:

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

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

정기적 재평가

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

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

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

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

정기 재평가 구성

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

시작하기 전에

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

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

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

단계 **2** **Add(**추가**)**를 클릭합니다.

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

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

포스처 문제 해결 설정

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

표 ***143:*** 포스처 문제 해결 설정

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

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

관련 항목

포스처 문제 해결 도구, 1161 페이지

포스처 일반 설정

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

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

일반 포스처 설정

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

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

포스처 임대

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

관련 항목

포스처 관리 설정, 1084 페이지
포스처 임대, 1089 페이지

Cisco ISE에 포스처 업데이트 다운로드

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

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

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

시작하기 전에

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

포스처 업데이트 창을 사용하여 웹에서 업데이트를 동적으로 다운로드할 수 있습니다.

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

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

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

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

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

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

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

단계 **6** **Yes(**예**)**를 클릭하여 계속합니다.

Cisco ISE 오프라인 업데이트

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

클라이언트 프로비저닝 리소스를 다운로드하려면 다음 단계를 수행합니다.

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

단계 **2** 로그인 자격 증명을 입력합니다.

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

다음과 같은 오프라인 설치 패키지를 다운로드할 수 있습니다.

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

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

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

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

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

오프라인 포스처 업데이트를 다운로드하려면 다음 단계를 수행합니다.

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

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

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

단계 **4** 포스처에 대한 설정을 보려면 화살표를 클릭합니다.

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

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

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

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

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

자동으로 포스처 업데이트 다운로드

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

시작하기 전에

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

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

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

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

Cisco ISE는 초기 지연 시간이 종료된 후 업데이트 확인을 시작합니다.

단계 **4** 시간 간격을 시간 단위로 입력합니다.

Cisco ISE는 초기 지연 시간부터 지정된 간격으로 구축에 업데이트를 다운로드합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

포스처 사용 제한 정책 컨피그레이션 설정

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

표 ***144:*** 포스처 ***AUP*** 컨피그레이션 설정

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

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

관련 항목

Posture Assessment용 사용 제한 정책 구성, 1098 페이지

Posture Assessment용 사용 제한 정책 구성

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

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

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

단계 **2** **Add(**추가**)**를 클릭합니다.

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

단계 **4** **Submit(**제출**)**을 클릭합니다.

포스처 조건

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

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

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

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

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

단순 포스처 조건

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

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

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

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

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

단순 포스처 조건 생성

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

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

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

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

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** 필드에 해당하는 값을 입력합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

복합 포스처 조건

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

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

복합 포스처 조건 생성

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

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

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

단계 **2** 필드에 해당하는 값을 입력합니다.

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

단계 **4** **Submit(**제출**)**을 클릭합니다.

사전 복합 조건 설정

표 ***145:*** 사전 복합 조건 설정

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

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

관련 항목

복합 포스처 조건, 1100 페이지
복합 포스처 조건 생성, 1100 페이지

Windows 클라이언트에서 자동 업데이트를 사용할 수 있도록 사전 정의된 조건

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

미리 구성된 안티바이러스 및 안티스파이웨어 조건

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

안티바이러스 및 안티스파이웨어 지원 차트

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

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

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

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

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

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

규정 준수 모듈

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

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

규정 준수 모듈은 Cisco.com에서 이용 가능합니다.

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

표 ***146: OPSWAT API*** 버전

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

참고

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

포스처 규정 준수 확인

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

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

도구 설명에 자세한 정보가 제공됩니다.

단계 **3** 자세한 내용을 확인하려면 데이터 범주를 확장합니다.

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

자세한 실시간 보고서가 표시됩니다.

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

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

패치 관리 조건 생성

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

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

참고 Cisco ISE 및 AnyConnect의 지원되는 버전은 다음과 같습니다.

- Cisco ISE 버전 1.4 이상
- AnyConnect 버전 4.1 이상

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

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

단계 **2** **Add(**추가**)**를 클릭합니다.

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

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

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

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

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

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

단계 **9** **Submit(**제출**)**을 클릭합니다.

관련 항목

패치 관리 조건 설정, 1127 페이지
패치 관리 교정 추가, 1146 페이지

디스크 암호화 조건 생성

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

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

시작하기 전에

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

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

단계 **2** **Add(**추가**)**를 클릭합니다.

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

단계 **4** **Submit(**제출**)**을 클릭합니다.

포스처 조건 설정

이 섹션에서는 포스처에 사용되는 단순 및 복합 조건에 대해 설명합니다.

파일 조건 설정

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

표 ***147:*** 파일 조건 설정

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

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

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

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

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

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

관련 항목

단순 포스처 조건, 1099 페이지
복합 포스처 조건, 1100 페이지
포스처 조건 생성, 1157 페이지

방화벽 조건 설정

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

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

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

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

레지스트리 조건 설정

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

표 ***148:*** 레지스트리 조건 설정

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

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

관련 항목

단순 포스처 조건, 1099 페이지
복합 포스처 조건, 1100 페이지

지속적인 엔드포인트 속성 모니터링

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

애플리케이션 조건 설정

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

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

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

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

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

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

서비스 조건 설정

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

표 ***149:*** 서비스 조건 설정

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

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

관련 항목

단순 포스처 조건, 1099 페이지
복합 포스처 조건, 1100 페이지

포스처 복합 조건 설정

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

표 ***150:*** 포스처 복합 조건 설정

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

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

관련 항목

포스처 조건, 1099 페이지
복합 포스처 조건 생성, 1100 페이지

안티바이러스 조건 설정

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

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

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

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

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

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

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

베이스라인 조건

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

고급 조건**(Advance Condition)**

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

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

관련 항목

복합 포스처 조건, 1100 페이지
미리 구성된 안티바이러스 및 안티스파이웨어 조건, 1102 페이지
안티바이러스 및 안티스파이웨어 지원 차트, 1102 페이지

안티스파이웨어 복합 조건 설정

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

표 ***151:*** 안티스파이웨어 복합 조건 설정

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

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

관련 항목

복합 포스처 조건, 1100 페이지
미리 구성된 안티바이러스 및 안티스파이웨어 조건, 1102 페이지
안티바이러스 및 안티스파이웨어 지원 차트, 1102 페이지

안티 멀웨어 조건 설정

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

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

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

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

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

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

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

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

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

베이스라인 조건

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

고급 조건**(Advance Condition)**
관련 항목
복합 포스처 조건, 1100 페이지

사전 단순 조건 설정

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

표 ***152:*** 사전 단순 조건 설정

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

관련 항목
단순 포스처 조건, 1099 페이지
단순 포스처 조건 생성, 1100 페이지

사전 복합 조건 설정

표 ***153:*** 사전 복합 조건 설정

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

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

관련 항목

복합 포스처 조건, 1100 페이지
복합 포스처 조건 생성, 1100 페이지

패치 관리 조건 설정

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

표 ***154:*** 패치 관리 조건

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

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

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

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

관련 항목

패치 관리 조건 생성, 1105 페이지

디스크 암호화 조건 설정

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

표 ***155:*** 디스크 암호화 조건 설정

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

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

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

관련 항목

디스크 암호화 조건 생성, 1106 페이지

USB 조건 설정

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

USB 확인은 사전 정의된 조건이며 Windows OS만 지원합니다.

표 ***156: USB*** 조건 설정

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

관련 항목

단순 포스처 조건, 1099 페이지

하드웨어 속성 조건 설정

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

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

포스처 외부 데이터 소스 조건

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

포스처 정책 구성

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

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

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

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

참고

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

시작하기 전에

- AUP(Acceptable Use Policy)를 이해하고 있어야 합니다.
- PRA(Periodic Reassessments)에 대해 알고 있어야 합니다.
- 규정 준수 관련 알림을 보려면 AnyConnect 에이전트 4.7 이상을 사용해야 합니다. AnyConnect 에이전트 구성에 대한 자세한 내용은 AnyConnect 컨피그레이션 생성, 1188 페이지를 참조하십시오.

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

단계 **2** 드롭다운 화살표를 사용하여 새 정책을 추가합니다.

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

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

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

유효한 값은 다음과 같습니다.

- 1~30일
- 1~720시간
- 1~43200분

기본적으로 이 설정은 비활성화되어 있습니다.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

단계 **14** **Save(**저장**)**를 클릭합니다.

AnyConnect 워크플로우 구성

AnyConnect 에이전트를 구성하려면 Cisco ISE에서 다음 단계를 수행합니다.

단계 **1** AnyConnect 에이전트 프로파일을 생성합니다.

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

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

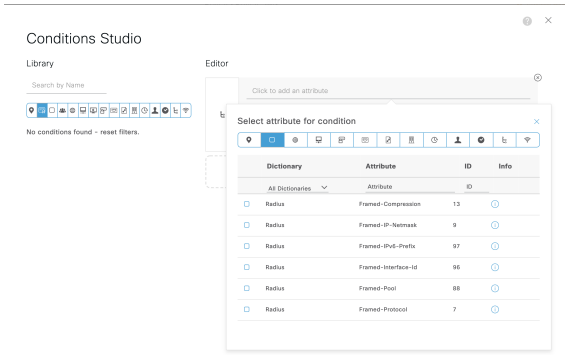
인증서 기반 조건의 사전 요건

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

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

그림 ***59: Cisco*** 프로비저닝 정책

그림 ***60: Condition Studio***



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

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

기본 포스처 정책

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

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

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

Client Posture 평가

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

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

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

Posture Assessment 옵션

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

표 ***157: Posture Assessment*** 옵션

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

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

포스처 교정 옵션

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

표 ***158:*** 포스처 교정 옵션

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

ISE 커뮤니티 리소스

Cisco ISE and SCCM integration Reference Guide

포스처를 위한 사용자 맞춤화 조건

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

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

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

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

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

포스처 엔드포인트 사용자 맞춤화 속성

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

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

엔드포인트 맞춤형 속성을 사용한 포스처 정책 생성

엔드포인트 맞춤형 속성을 사용하여 포스처 정책을 생성하려면 다음을 따릅니다.

단계 **1** 엔드포인트 맞춤형 속성을 생성합니다.

a)

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

c) **Save(**저장**)**를 클릭합니다.

단계 **2** 맞춤형 속성에 값을 할당합니다.

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

b) 맞춤형 속성 값을 할당합니다.

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

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

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

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

e) **Save(**저장**)**를 클릭합니다.

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

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

b) 필요한 정책을 생성합니다. **Other Conditions(**기타 조건**)**를 클릭하여 맞춤형 속성을 선택하고 필요한 사전을 선택합니다(예: Endpoints(엔드 포인트) > deviceType, 즉 1단계에서 생성한 맞춤형 속성 선택). 자세한 내용은 Cisco 임시 에이전트 구성 워크플로우, 1159 페이지을 참조하십시오.

c) **Save(**저장**)**를 클릭합니다.

엔드포인트 맞춤형 속성을 사용하여 클라이언트 프로비저닝 정책을 생성하려면 다음을 따릅니다.

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

사용자 맞춤화 포스처 교정 작업

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

안티스파이웨어 교정 추가

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

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

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

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

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

단계 **4** **Add(**추가**)**를 클릭합니다.

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

단계 **6** **Submit(**제출**)**을 클릭합니다.

안티바이러스 교정 추가

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

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

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

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

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

단계 **4** **Add(**추가**)**를 클릭합니다.

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

단계 **6** **Submit(**제출**)**을 클릭합니다.

파일 교정 추가

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

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

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

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

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

단계 **4** **Add(**추가**)**를 클릭합니다.

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

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

단계 **7** **Submit(**제출**)**을 클릭합니다.

프로그램 시작 교정 추가

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

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

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

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

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

단계 **4** **Add(**추가**)**를 클릭합니다.

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

단계 **6** **Submit(**제출**)**을 클릭합니다.

프로그램 시작 치료 문제 해결

문제

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

해결책

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

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

링크 교정 추가

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

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

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

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

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

단계 **4** **Add(**추가**)**를 클릭합니다.

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

단계 **6** **Submit(**제출**)**을 클릭합니다.

패치 관리 교정 추가

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

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

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

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

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

단계 **4** **Add(**추가**)**를 클릭합니다.

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

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

Windows Server Update Services 교정 추가

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

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

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

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

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

단계 **4** **Add(**추가**)**를 클릭합니다.

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

단계 **6** **Submit(**제출**)**을 클릭합니다.

Windows 업데이트 교정 추가

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

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

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

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

단계 **4** **Add(**추가**)**를 클릭합니다.

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

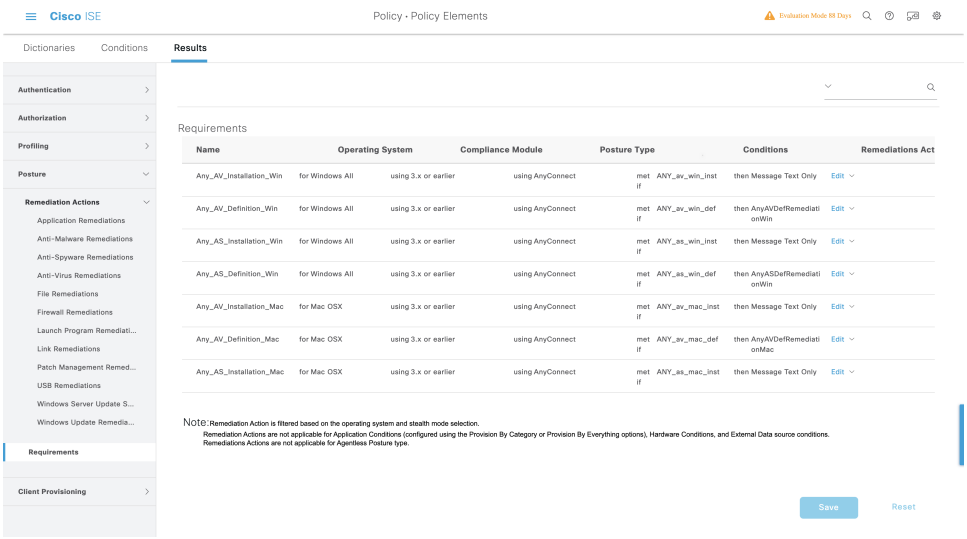
단계 **6** **Submit(**제출**)**을 클릭합니다.

Posture Assessment 요건

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

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

그림 ***61: Posture Policy*** 요건 유형



필수 요건

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

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

선택 요건

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

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

감사 요건

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

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

가시성을 위한 요구 사항

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

규정 미준수 상태로 중단된 클라이언트 시스템

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

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

클라이언트 포스처 요건 생성

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

시작하기 전에

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

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

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

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

단계 **4** **Save(**저장**)**를 클릭합니다.

Posture Reassessment 컨피그레이션 설정

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

표 ***159: Posture Reassessment*** 컨피그레이션 설정

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

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

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

관련 항목

포스처 임대, 1089 페이지
정기적 재평가, 1090 페이지
Posture Assessment 옵션, 1140 페이지
포스처 교정 옵션, 1141 페이지
포스처를 위한 사용자 맞춤화 조건, 1142 페이지
사용자 맞춤화 포스처 교정 작업, 1143 페이지
정기 재평가 구성, 1090 페이지

포스처를 위한 사용자 맞춤화 권한

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

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

알 수 없는 프로파일

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

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

규정 준수 프로파일

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

규정 미준수 프로파일

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

표준 권한 부여 정책 구성

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

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

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

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

단계 **4** 규칙 이름을 입력합니다.

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

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

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

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

단계 **8** **Save(**저장**)**를 클릭합니다.

포스처를 통한 네트워크 드라이브 매핑 모범 사례

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

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

AnyConnect 스텔스 모드 워크플로우 구성

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

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

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

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

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

단계 **5** 포스처 조건을 생성합니다(포스처 조건 생성 참조).

단계 **6** 포스처 교정을 생성합니다(포스처 교정 생성 참조).

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

단계 **8** 포스처 정책을 생성합니다(포스처 정책 생성 참조).

단계 **9** 권한 부여 프로파일을 구성합니다.

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

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

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

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

단계 **10** 권한 부여 정책을 구성합니다.

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

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

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

AnyConnect 에이전트 프로파일을 생성합니다.

시작하기 전에

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

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

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

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

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

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

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

AnyConnect 패키지용 AnyConnect 구성을 생성해야 합니다.

AnyConnect 패키지의 AnyConnect 컨피그레이션 생성

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

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

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

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

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

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

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

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

다음에 수행할 작업

Open DNS 프로파일을 업로드하여 클라이언트에 푸시해야 합니다.

Cisco ISE에서 Open DNS 프로파일 업로드

Open DNS 프로파일이 클라이언트에 푸시됩니다.

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

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

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

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

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

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

단계 7 **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

클라이언트 프로비저닝 정책을 생성해야 합니다.

클라이언트 프로비저닝 정책 생성

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

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

다음에 수행할 작업

포스처 조건을 생성해야 합니다.

포스처 조건 생성

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

단계 **2** 필요한 이름(예: filechk)을 입력합니다.

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

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

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

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

다음에 수행할 작업

포스처 교정을 생성해야 합니다.

포스처 교정 생성

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

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

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

단계 **3** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

포스처 요건을 생성해야 합니다.

스텔스 모드에서 포스처 요건 생성

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

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

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

다음에 수행할 작업

포스처 정책을 생성해야 합니다.

포스처 정책 생성

시작하기 전에

포스처 정책 요건을 확인하고 정책이 클라이언트리스 모드에서 생성되었는지 파악합니다.

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

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

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

AnyConnect 스텔스 모드 알림 활성화

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

참고 AnyConnect 4.5.0.3040 이상 버전은 스텔스 모드 알림을 지원합니다.

시작하기 전에

스텔스 모드에서 AnyConnect를 구성합니다.

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

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

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

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

Cisco 임시 에이전트 구성 워크플로우

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

단계 **1** 포스처 조건 생성

단계 **2** 포스처 요건 생성

단계 **3** 포스처 정책 생성

단계 **4** 클라이언트 프로비저닝 정책 구성

단계 **5** 권한 부여 프로파일을 구성합니다.

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

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

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

단계 **6** 권한 부여 정책을 구성합니다.

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

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

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

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

포스처 조건 생성

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

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

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

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

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

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

포스처 요건 생성

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

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

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

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

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

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

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

참고 Temporal Agent는 AnyConnect 4.x 이상에서 지원됩니다.

포스처 정책 생성

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

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

클라이언트 프로비저닝 정책 구성

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

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

Cisco Temporal Agent 다운로드 및 실행

단계 **1** SSID에 연결합니다.

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

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

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

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

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

포스처 문제 해결 도구

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

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

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

엔드포인트 로그인 자격 증명 구성

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

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

다음 탭이 표시됩니다.

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

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

엔드포인트 스크립트 설정

이 페이지에서는 엔드포인트 스크립트 및 에이전트리스 포스처에 대한 옵션을 구성합니다.

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

Cisco ISE에서 클라이언트 프로비저닝 구성

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

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

시작하기 전에

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

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

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

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

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

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

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

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

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

클라이언트 프로비저닝 리소스 정책을 구성합니다.

클라이언트 프로비저닝 리소스

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

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

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

- **Agent resources from Cisco Site(Cisco** 사이트의 에이전트 리소스**)**: 클라이언트 프로비저닝 정책에 사용하려는 AnyConnect 및 Supplicant Provisioning(신청자 프로비저닝) 마법사를 선택합니다. Cisco는 새 리소스를 추가하고 기존 리소스를 업데이트하여 이 리소스 목록을 정기적으로 업데이트합니다. 또한 모든 Cisco 리소스 및 리소스 업데이트를 자동으로 다운로드하도록 ISE를 설정할 수도 있습니다. 더 자세한 내용은 Cisco ISE에서 클라이언트 프로비저닝 구성, 1162 페이지를 참고하십시오.
- **Agent resources from local disk(**로컬 디스크의 에이전트 리소스**)**: ISE에 업로드할 PC의 리소스를 선택합니다. 로컬 머신에서 Cisco 제공 클라이언트 프로비저닝 리소스 추가, 1165 페이지를 참고하십시오.
- **AnyConnect Configuration(AnyConnect** 컨피그레이션**)**: 클라이언트 프로비저닝에 사용하려는 AnyConnect PC 클라이언트를 선택합니다. 자세한 내용은 AnyConnect 컨피그레이션 생성을 참고하십시오.
- **Native Supplicant Profile(**기본 신청자 프로파일**)**: 네트워크의 설정이 포함된 휴대폰 및 태블릿용 신청자 프로파일을 구성합니다. 자세한 내용은 기본 신청자 프로파일 생성을 참고하십시오.
- **AnyConnect ISE Posture Profile(AnyConnect ISE Posture** 프로파일**)**: 에이전트 XML 프로파일을 생성 및 배포하지 않으려는 경우 여기서 AnyConnect ISE Posture를 구성합니다. AnyConnect ISE Posture 에이전트 및 ISE 포스처 프로파일 편집기에 대한 자세한 내용은 사용자의 AnyConnect 버전에 대한 AnyConnect 관리자 설명서를 참고하십시오https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html.

클라이언트 프로비저닝 리소스를 생성한 후에는 엔드포인트에 클라이언트 프로비저닝 리소스를 적용하는 클라이언트 프로비저닝 정책을 생성합니다. 클라이언트 프로비저닝 리소스 정책 구성, 1193 페이지를 참고하십시오.

관련 항목

Cisco ISE에서 클라이언트 프로비저닝 구성, 1162 페이지
Cisco의 클라이언트 프로비저닝 리소스 추가, 1164 페이지
로컬 머신에서 Cisco 제공 클라이언트 프로비저닝 리소스 추가, 1165 페이지
로컬 머신에서 AnyConnect용으로 고객이 생성한 리소스 추가, 1166 페이지

Cisco의 클라이언트 프로비저닝 리소스 추가

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

시작하기 전에

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

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

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

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

단계 4 **Save** 버튼을 클릭합니다.

다음에 수행할 작업

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

로컬 머신에서 Cisco 제공 클라이언트 프로비저닝 리소스 추가

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

시작하기 전에

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

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

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

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

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

단계 4 **Browse(찾아보기)**를 클릭하여 Cisco ISE로 다운로드할 리소스 파일이 있는 로컬 머신의 디렉토리로 이동합니다.

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

단계 5 **Submit(제출)**을 클릭합니다.

다음에 수행할 작업

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

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

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

시작하기 전에

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

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

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

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

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

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

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

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

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

다음에 수행할 작업

AnyConnect 에이전트 프로파일을 생성합니다.

기본 신청자 프로파일 생성

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

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

시작하기 전에

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

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

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

단계 **3** 다음 내용의 설명에 따라 프로파일을 생성합니다. 기본 신청자 프로파일 설정, 1167 페이지

다음에 수행할 작업

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

기본 신청자 프로파일 설정

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

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

무선 프로파일

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

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

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

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

iOS 설정

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

유선 프로파일

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

선택적 설정 **- Windows**용

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

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

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

다른 네트워크의 **URL** 리디렉션 없는 클라이언트 프로비저닝

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

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

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

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

Dot1X EAP-TLS

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

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

Dot1X PEAP

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

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

MAB(유선 네트워크)

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

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

MAB(무선 네트워크)

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

   AnyConnect가 포스처를 수행합니다. 포스처는 무선 802.1X에만 시작됩니다.

AMP Enabler 프로파일 설정

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

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

표 ***160: AMP Enabler*** 프로파일 페이지

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

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

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

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

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

시작하기 전에

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

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

단계 **2** **Add(**추가**)** 드롭다운을 클릭합니다.

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

단계 **4** 필드에 해당하는 값을 입력합니다.

독립형 편집기를 사용하여 **AMP Enabler** 프로파일 생성

AnyConnect 독립형 편집기에서 AMP Enabler 프로파일을 생성하려면 다음 단계를 수행합니다.

시작하기 전에

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

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

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

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

단계 **2** **Add(**추가**)**를 클릭합니다.

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

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

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

단계 **6** 이름과 설명을 입력합니다.

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

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

아래 예에는 사용자 맞춤화된 제거 파일이 나와 있습니다.

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

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

일반 **AMP Enabler** 설치 오류 문제 해결

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

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

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

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

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

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

  구문이 잘못된 URL 형식을 입력하면 이 오류 메시지가 표시됩니다.

Cisco ISE의 **Chromebook** 디바이스 온보딩 지원

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

관리되지 않는 Chromebook 디바이스는 보안 네트워크로 온보딩할 수 없습니다.

Chromebook 온보딩 프로세스에서 사용되는 엔터티는 다음과 같습니다.

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

Google 관리자는 다음을 수행합니다.

- 다음 라이선스 보호:

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

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

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

ISE 관리자는 다음을 수행합니다.

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

Chromebook 사용자는 다음을 수행합니다.

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

Google Admin Console은 다음을 수행합니다.

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

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

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

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

Chromebook 온보딩 프로세스

Chromebook 온보딩 프로세스에서는 다음과 같은 일련의 단계가 포함되어 있습니다.

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

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

단계 **3** Chromebook 디바이스 초기화.

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

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

Google Admin Console에서 네트워크 및 강제 익스텐션 구성

다음 단계는 Google 관리자가 수행합니다.

단계 **1** Google Admin Console에 로그인합니다.

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

b) 필요한 사용자 이름 및 비밀번호를 입력합니다.

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

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

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

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

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

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

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

c) **Add(**추가**)**를 클릭합니다.

단계 **3** 강제 익스텐션을 생성합니다.

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

b) **User Settings(**사용자 설정**)**를 클릭합니다.

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

단계 **4** 강제 익스텐션을 설치합니다.

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

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

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

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

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

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

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

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

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

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

f) **Save(**저장**)**를 클릭합니다.

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

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

다음에 수행할 작업

Chromebook 온보딩용으로 Cisco ISE 구성

Chromebook 온보딩용으로 Cisco ISE 구성

시작하기 전에

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

아래는 권한 부여 정책의 예입니다.

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

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

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

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

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

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

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

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

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

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

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

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

b) 결과를 정의합니다.

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

Chromebook 디바이스 초기화

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

Chromebook 사용자는 다음 단계를 수행합니다.

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

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

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

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

단계 **5** 로그인하기 전에 Chromebook을 등록합니다.

다음에 수행할 작업

Google Admin Console에 Chromebook을 등록합니다.

Google Admin Console에 Chromebook 등록

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

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

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

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

단계 **4** **Done(**완료**)**을 클릭합니다.

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

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

Chromebook 등록은 일회용 프로세스입니다.

BYOD 온보딩을 위해 Chromebook을 Cisco ISE 네트워크에 연결

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

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

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

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

단계 **3** 자격증명이 있는 게스트 포털이 열립니다.

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

2. **Sign-on(**로그인**)**을 클릭합니다.

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

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

단계 **6** **Continue(**계속**)**를 클릭합니다.

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

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

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

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

Google Admin Console - Wi-Fi 네트워크 설정

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

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

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

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

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

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

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

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

Cisco ISE에서 Chromebook 디바이스 활동 모니터링

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

Chromebook 디바이스 온보딩 문제 해결

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

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

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

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

Cisco AnyConnect Secure Mobility

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

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

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

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

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

AnyConnect 컨피그레이션 생성

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

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

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

시작하기 전에

AnyConnect 구성 개체를 구성하기 전에 다음을 수행하십시오.

1. Cisco 소프트웨어 다운로드 페이지에서 AnyConnect Headend Deployment 패키지 및 규정 준수 모듈을 다운로드합니다.
2. Cisco ISE에 이러한 리소스를 업로드합니다(로컬 머신에서 Cisco 제공 클라이언트 프로비저닝 리소스 추가, 1165 페이지 참고).
3. (선택 사항) 사용자 맞춤화 및 현지화 번들을 추가합니다(로컬 머신에서 AnyConnect용으로 고객이 생성한 리소스 추가, 1166 페이지 참고).
4. AnyConnect 포스처 에이전트 프로파일을 구성합니다(포스처 에이전트 프로파일 생성, 1189 페이지 참고).

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

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

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

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

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

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

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

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

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

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

단계 **10** **Submit(**제출**)**을 클릭합니다.

포스처 에이전트 프로파일 생성

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

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

단계 **2** **Add(**추가**)**를 클릭합니다.

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

단계 **4** 프로파일의 이름을 입력합니다.

단계 **5** 다음에 대해 매개변수를 구성합니다.

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

단계 **6** **Submit(**제출**)**을 클릭합니다.

클라이언트 IP 주소 새로 고침 컨피그레이션

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

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

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

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

포스처 프로토콜 설정

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

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

지속적인 엔드포인트 속성 모니터링

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

Cisco Web Agent

Cisco Web Agent는 클라이언트 머신에 대한 임시 포스처 평가를 제공합니다.

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

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

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

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

Cisco Web Agent

Cisco Web Agent는 클라이언트 머신에 대한 임시 포스처 평가를 제공합니다.

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

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

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

클라이언트 프로비저닝 리소스 정책 구성

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

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

시작하기 전에

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

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

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

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

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

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

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

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

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

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

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

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

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

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

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

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

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

시작하기 전에

Cisco ISE에서 AnyConnect용 클라이언트 프로비저닝 리소스를 추가해야 합니다.

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

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

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

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

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

개인 디바이스의 기본 신청자 구성

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

시작하기 전에

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

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

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

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

단계 **4** 다음 항목을 지정합니다.

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

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

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

단계 **7** **Save(**저장**)**를 클릭합니다.

클라이언트 프로비저닝 보고서

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

클라이언트 프로비저닝 요청

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

신청자 프로비저닝 요청

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

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

클라이언트 프로비저닝 이벤트 로그

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

클라이언트 프로비저닝 포털의 포털 설정

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

포털 설정

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

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

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

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

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

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

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

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

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

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

로그인 페이지 설정

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

AUP(Acceptable Use Policy) 페이지 설정

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

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

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

비밀번호 변경 설정

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

클라이언트 프로비저닝 포털 언어 파일을 위한 HTML 지원

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

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

참고 이 목록은 파일 내 사전 키의 전체 목록이 아닙니다.

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

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

13 장

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, 1365 페이지 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, 1207 페이지
Cognitive Threat Analytics 어댑터 구성, 1208 페이지
CTA 어댑터를 위한 권한 부여 프로파일 구성, 1210 페이지
작업 과정 속성을 사용하여 권한 부여 정책 구성, 1210 페이지
Threat Centric NAC 서비스, 1203 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, 1206 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, 1206 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, 1206 페이지.

단계 **2** 구성하려면 다음을 따릅니다.

- Qualys 어댑터는 Qualys 어댑터 구성, 1213 페이지를 참조하십시오.
- Nexpose 어댑터는 Nexpose 어댑터 구성, 1216 페이지를 참조하십시오.
- Tenable 어댑터는 Tenable 어댑터 구성, 1219 페이지를 참조하십시오.

단계 **3** 권한 부여 프로파일 구성, 1222 페이지.

단계 **4** 취약한 엔드포인트 격리를 위한 예외 규칙 구성, 1223 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, 1207 페이지
Cognitive Threat Analytics 어댑터 구성, 1208 페이지
CTA 어댑터를 위한 권한 부여 프로파일 구성, 1210 페이지
작업 과정 속성을 사용하여 권한 부여 정책 구성, 1210 페이지
Threat Centric NAC 서비스, 1203 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 ***161:*** 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 ***162: 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 ***163: 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 ***164: 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 ***165:*** 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 붙여 넣어야 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 ***166: 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, 821 페이지

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 ***167:*** 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 ***168: 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 ***169: 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 ***170:*** 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 ***171:*** 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 ***172:*** 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 ***173: 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 ***174:*** 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 ***175:*** 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 *176: 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 ***177: 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 ***178:*** 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.

14 장

pxGrid

pxGrid 및 Cisco ISE

참고

Cisco ISE 릴리스 3.1부터 모든 pxGrid 연결은 pxGrid 2.0을 기반으로 해야 합니다. pxGrid 1.0 기반(XMPP 기반) 통합은 릴리스 3.1부터 Cisco ISE에서 작동하지 않습니다.

WebSockets를 기반으로 하는 pxGrid 버전 2.0은 Cisco ISE 릴리즈 2.4에서 소개되었습니다. 잠재적인 통합 중단을 방지하려면 다른 시스템을 pxGrid 2.0 호환 버전으로 계획 및 업그레이드하는 것이 좋습니다.

Cisco pxGrid는 양방향 any-to-any 파트너 플랫폼 통합을 허용하는 확장 가능한 개방형 SPIF(Security Product Integration Framework)입니다.

pxGrid 1.0은 레거시 XMPP(Extensible Messaging and Presence Protocol) 구현을 사용합니다. pxGrid 1.0은 유지 관리 모드이며 곧 제거됩니다. Cisco pxGrid 1.0에는 pxGrid와 호환되는 클라이언트 SDK 라이브러리(Java 또는 C)가 필요합니다.

pxGrid 2.0은 REST 및 WebSocket 인터페이스를 사용합니다. 클라이언트는 제어 메시지, 쿼리 및 애플리케이션 데이터에 REST를 사용하고 이벤트 푸시에 WebSocket을 사용합니다. pxGrid 2.0에 대한 자세한 내용은 **Welcome to Learning Cisco Platform Exchange Grid(pxGrid)**를 참고하십시오.

Cisco pxGrid는 다음 기능을 제공합니다.

- Cisco ISE 세션 디렉터리에서 다른 정책 네트워크 시스템(예: ISE Eco 시스템 파트너 시스템 및 기타 Cisco 플랫폼)과 상황에 맞는 정보를 공유합니다.
- 타사 시스템이 네트워크 또는 보안 이벤트에 대한 응답으로 사용자 및 디바이스를 격리하기 위해 적응형 네트워크 제어 작업을 호출할 수 있습니다. 태그 정의, 값 및 설명과 같은 TrustSec 정보는 TrustSec 주제를 통해 Cisco ISE에서 다른 네트워크로 전달됩니다.
- FQN(Fully Qualified Names)을 사용하는 엔드포인트 프로파일을 엔드포인트 프로파일 메타 주제를 통해 Cisco ISE에서 다른 네트워크로 전송합니다.

- 태그 및 엔드포인트 프로파일을 대량으로 다운로드합니다.
- pxGrid를 통해 SXP 바인딩(IP-SGT 매핑)을 게시하고 구독합니다. SXP 바인딩에 대한 자세한 내용은 Cisco ISE 관리 가이드의 세그멘테이션 장에 있는 보안 그룹 태그 교환 프로토콜 섹션을 참고하십시오.
- Cisco pxGrid Context-in을 사용하면 에코시스템 파트너가 Cisco ISE에 주제 정보를 게시할 수 있습니다. 이를 통해 Cisco ISE는 에코시스템에서 식별된 에셋을 기반으로 조치를 취할 수 있습니다. Cisco pxGrid Context-in에 대한 자세한 내용은 pxGrid Context-In을 참고하십시오.

참고 pxGrid 1.0은 유지 관리 모드이며 곧 사용이 중단됩니다. ISE 2.4에서 pxGrid 2.0을 도입했습니다. 파트너는 pxGrid 클라이언트 구현을 pxGrid 2.0으로 전환하는 것이 좋습니다.

pxGrid 개요

pxGrid에는 다음 구성 요소가 있습니다.

- 컨트롤러: 검색, 인증 및 권한 부여를 처리합니다.
- 제공자: 쿼리 결과를 반환하거나 게시합니다.
- Pubsub : 제공자 및 사용자에게 pxGrid 서비스를 제공합니다.
- 가입자: 권한이 부여된 가입자는 구독하는 주제에서 상황 정보 및 알림을 받습니다.

pxGrid는 다음 기능을 제공합니다.

- 검색: 서비스 이름을 기준으로 서비스 속성을 검색합니다. 제공자가 pxGrid 컨트롤러에 "Register Service(서비스 등록)"를 요청하면 플로우가 시작됩니다. 등록 후 사용자는 "Lookup Service(조회 서비스)"를 사용하여 제공자의 위치를 검색합니다.
- 인증: pxGrid 컨트롤러는 서비스에 액세스하기 위해 pxGrid 클라이언트를 인증합니다. 자격 증명은 사용자 이름과 비밀번호 또는 인증서(기본 설정)입니다.
- 권한 부여: pxGrid는 작업 요청을 받으면 pxGrid 컨트롤러를 통해 확인하여 요청에 권한을 부여합니다. pxGrid는 클라이언트를 미리 정의된 그룹에 할당합니다.

pxGrid 1.0 고가용성

pxGrid 1.0을 사용하면 pxGrid 페르소나가 활성/대기 모드로 작동하는 두 개의 노드를 구성할 수 있습니다. 고가용성 구성에서 Cisco pxGrid 서버는 PAN을 통해 노드 간에 정보를 복제합니다. PAN이 다운되면 pxGrid 서버는 클라이언트 등록 및 서브스크립션 처리를 중단합니다. pxGrid 서버를 활성화하려면 PAN을 수동으로 승격해야 합니다.

CLI 명령 **show application status ise**를 사용하여 pxGrid 프로세스를 확인할 수 있습니다. pxGrid 1.0과 관련된 프로세스는 다음과 같습니다.

- pxGrid 인프라 서비스

- pxGrid 게시자 가입자 서비스
- pxGrid 연결 관리자
- pxGrid 컨트롤러

활성 pxGrid 1.0 노드에서 이러한 프로세스는 'Running'으로 표시됩니다. 대기 pxGrid 1.0 노드에서는 Disabled로 표시됩니다. 활성 pxGrid 1.0 노드가 작동 중지되면**show logging application pxgrid.state** 대기 pxGrid 노드가 이를 탐지하고 4개의 pxGrid 프로세스를 시작합니다. 몇 분 내에 이러한 프로세스가 'Running'으로 표시되고 대기 노드는 활성 노드가 됩니다. CLI 명령 **show logging application pxgrid**를 실행하여 pxGrid가 해당 노드에서 대기 중인지 확인할 수 있습니다.

Cisco ISE는 보조 pxGrid 노드에 대한 자동 페일오버를 수행합니다. 원래 기본 pxGrid 노드를 다시 네트워크에 연결하는 경우 원래 기본 pxGrid 노드는 보조 역할로 계속 유지되며 현재 기본 노드를 종료하지 않는 한 기본 역할로 다시 승격되지 않습니다.

pxGrid 2.0의 고가용성

pxGrid 2.0 노드는 활성/활성 구성에서 작동합니다. 고가용성을 위해서는 구축에 두 개 이상의 pxGrid 노드가 있어야 합니다. 대규모 구축의 경우 확장성 및 리던던시(redundancy)를 높이기 위해 최대 4개의 노드를 포함할 수 있습니다. 모든 노드에 대해 IP 주소를 구성하여 한 노드가 작동 중지될 경우 해당 노드의 클라이언트가 작동하는 노드에 연결되도록 하는 것이 좋습니다. PAN이 작동 중지되면 pxGrid 서버는 활성화 처리를 중지합니다. pxGrid 서버를 활성화하려면 PAN을 수동으로 승격합니다. pxGrid 구축에 대한 자세한 내용은 **ISE Performance & Scale**을 참고하십시오.

모든 pxGrid 서비스 제공자 클라이언트는 7.5분 이내에 pxGrid 컨트롤러에 주기적으로 다시 등록됩니다. PAN 노드는 다시 등록되지 않는 클라이언트를 비활성 상태로 간주하고 삭제합니다. PAN 노드가 7.5분 넘게 작동 중지되었다가 다시 작동되는 경우 7.5분보다 오래된 타임스탬프 값을 가진 모든 클라이언트가 삭제됩니다. 모든 클라이언트는 pxGrid 컨트롤러에 다시 등록해야 합니다.

pxGrid 2.0 클라이언트는 pub/sub 및 쿼리에 WebSocket 및 REST 기반 API를 사용했습니다. 이러한 API는 포트 8910의 ISE 애플리케이션 서버에서 제공됩니다. **show logging application pxgrid**를 실행할 때 표시되는 pxGrid 프로세스는 pxGrid 2.0에 적용되지 않습니다.

손실 탐지

Cisco ISE 3.0에서는 pxGrid 주제에 시퀀스 ID를 추가했습니다. 전송이 중단되는 경우 가입자는 ID 시퀀스의 단절을 확인하여 이를 인식할 수 있습니다. 가입자는 주제 시퀀스 ID의 변경을 확인하고 마지막 시퀀스 번호의 날짜를 기준으로 데이터를 요청합니다. 게시자가 작동 중지되었다가 다시 시작되는 경우 주제 시퀀스가 0부터 시작합니다. 가입자는 시퀀스 0이 표시될 경우 캐시를 지우고 대량 다운로드를 시작해야 합니다. 가입자의 연결이 끊어질 경우 게시자는 시퀀스 ID를 계속 할당합니다. 가입자가 다시 연결한 후 시퀀스 ID의 단절을 확인할 경우 마지막 시퀀스 번호의 시간부터 데이터를 요청합니다. 손실 탐지는 세션 디렉터리 및 TrustSec 구성을 사용하여 작동합니다. 세션 디렉터리를 사용하는 경우 클라이언트가 손실을 탐지하면 캐시를 지우고 대량 다운로드를 시작해야 합니다.

시퀀스 ID를 사용하지 않는 기존 애플리케이션이 있는 경우 시퀀스 ID를 사용할 필요가 없습니다. 그러나 이를 사용하면 손실을 탐지하고 손실을 복구할 수 있다는 이점이 있습니다.

세션 디렉터리 세션은 알림 간격마다 비동기식으로 MnT에서 일괄 처리되고 `/topic/com.cisco.ise.session`에 게시됩니다.

TrustSec Config 보안 그룹에 대한 변경 사항은 `/topic/com.cisco.ise.config.trustsec.security.group`에 게시됩니다.

손실 탐지는 pxGrid 2.0에서만 지원되며 기본적으로 설정되어 있습니다.

손실 탐지를 사용하는 코드 예를 보려면 https://github.com/cisco-pxgrid/pxgrid-rest-ws/tree/master/java/src/main/java/com/cisco/pxgrid/samples/ise 항목을 참고하십시오.

모니터링 및 디버깅

pxGrid 노드에 대해 제공되는 로그는 다음과 같습니다.

- pxgrid.log: pxGrid 1.0 프로세스 활동
- pxgrid-server.log: pxGrid 2.0 활동 및 오류
- pxgrid-cm.log: pxGrid 1.0 연결 로그
- pxgrid-controller.log: pxGrid 1.0 제어 메시지 로그
- pxgrid-jabberd.log: pxGrid 1.0 XMPP 서버 로그
- pxgrid-pubsub.log: pxGrid 1.0 XMPP Pubsub 로그

Log(로그**)** 페이지에는 모든 pxGrid 2.0 관리 이벤트가 표시됩니다. 이벤트 정보에는 이벤트 유형 및 타임스탬프와 함께 클라이언트 및 기능 이름이 포함됩니다. **Administration(**관리**) > pxGrid Services(pxGrid** 서비스**) > Diagnostics(**진단**) > Log(**로그**)**로 이동하여 이벤트 목록을 봅니다. 로그를 지우고 목록을 다시 동기화하거나 새로 고칠 수도 있습니다.

pxGrid 요약 페이지

Summary(요약) 페이지에는 현재 pxGrid 2.0 환경의 통계가 표시됩니다.

- Current Connections(현재 연결): 컨트롤러에 대한 연결 목록
- Control Messages(제어 메시지): 인증, 권한 부여 및 서비스 검색
- REST APIs(REST API): WebSocket 또는 XMPP를 사용하여 연결된 클라이언트 수
- Pubsub Throughput(Pubsub 처리량): 클라이언트에 게시된 데이터의 양
- Clients(클라이언트): REST 또는 WebSocket으로 연결된 클라이언트
- Errors(오류): 클라이언트가 데이터 전송 재시작을 요청하도록 야기한 전송 오류의 수

pxGrid 클라이언트 관리

새 클라이언트가 pxGrid에 연결하는 경우 먼저 관리자가 이 페이지를 방문하여 클라이언트를 승인해야 클라이언트가 그리드에 사용될 수 있습니다. 그러나 **Settings(**설정**)** 페이지에서 인증서 기반 계정의 자동 승인을 활성화한 경우 수동 승인이 필요하지 않습니다.

- **Clients(**클라이언트**)**: pxGrid 1.0 및 2.0의 외부 클라이언트 계정을 나열합니다.

- **pxGrid Policy(pxGrid** 정책**)**: 클라이언트가 가입할 수 있는 사용 가능한 서비스를 나열합니다. 정책을 편집하여 해당 정책에 액세스 할 수 있는 그룹을 변경할 수 있습니다. 아직 정책이 없는 서비스에 대해 새 정책을 생성할 수도 있습니다.
- **Groups(**그룹**)**: 기본 그룹은 EPS 또는 ANC입니다. 더 많은 그룹을 추가하고 이를 사용하여 서비스에 대한 액세스를 제한할 수 있습니다.

  pxGrid 클라이언트는 REST API를 통해 사용자 이름을 전송하여 pxGrid 컨트롤러에 자체적으로 등록할 수 있습니다. pxGrid 컨트롤러는 클라이언트 등록 중에 pxGrid 클라이언트의 비밀번호를 생성합니다. 관리자는 연결 요청을 승인하거나 거부할 수 있습니다.
- **Certificates(**인증서**)**: Cisco ISE 내부 CA(Certificate Authority)를 사용하기 위해 새 인증서를 생성할 수 있습니다.

  pxGrid용 인증서를 생성하는 방법에 대한 자세한 내용은 다음을 참고하십시오.

  - Cisco pxGrid를 사용하여 인증서 구축 - Cisco ISE 2.0/2.1/2.2에 대한 자체 서명 인증서 업데이트 사용
  - Cisco pxGrid를 사용하여 인증서 구축 - Cisco ISE 2.0/2.1/2.2 업데이트와 함께 외부 CA 사용

pxGrid 정책 제어

pxGrid 클라이언트가 액세스할 수 있는 서비스에 대한 액세스를 제어하기 위해 pxGrid 권한 부여 정책을 생성할 수 있습니다. 이러한 정책은 pxGrid 클라이언트에서 사용 가능한 서비스를 제어합니다.

서로 다른 유형의 그룹을 생성하고 pxGrid 클라이언트에서 사용 가능한 서비스를 이러한 그룹에 매핑할 수 있습니다. **Client Management(**클라이언트 관리**) > Groups(**그룹**)** 창에서 **Manage Groups(**그룹 관리**)** 옵션을 사용하여 새 그룹을 추가합니다. Policies(정책) 창에서 사전 정의된 그룹(예: EPS 및 ANC)을 사용하는 사전 정의된 권한 부여 정책을 확인할 수 있습니다.

pxGrid 클라이언트에 대한 권한 부여 정책을 생성하려면 다음을 수행하십시오.

SUMMARY STEPS

1. **Administration(**관리**)**에서 **pxGrid Services(pxGrid** 서비스**) > Client Management(**클라이언트 관리**) > Policy(**정책**)**를 선택한 다음 **Add(**추가**)** 버튼을 클릭합니다.
2. **Service(**서비스**)** 드롭다운 목록에서 서비스를 선택합니다.
3. **Operation(**운영**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
4. **Groups(**그룹**)** 드롭다운 목록에서 이 서비스에 매핑할 그룹을 선택합니다.
5. **Submit(**제출**)**을 클릭합니다.

DETAILED STEPS

단계 **1** **Administration(**관리**)**에서 **pxGrid Services(pxGrid** 서비스**) > Client Management(**클라이언트 관리**) > Policy(**정책**)**를 선택한 다음 **Add(**추가**)** 버튼을 클릭합니다.

단계 **2** **Service(**서비스**)** 드롭다운 목록에서 서비스를 선택합니다.

- com.cisco.ise.radius
- come.cisco.ise.sxp
- com.cisco.ise.trustsec
- com.cisco.ise.session
- com.cisco.ise.system
- com.cisco.ise.mdm
- com.cisco.ise.config.trustsec
- com.cisco.ise.config.profiler
- com.cisco.ise.pxgrid.admin
- com.cisco.ise.config.deployment.node
- com.cisco.ise.endpoint
- com.cisco.ise.config.anc
- com.cisco.ise.dnac
- com.cisco.ise.config.upn
- com.cisco.ise.pubsub

단계 **3** **Operation(**운영**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- <ANY>
- publish
- publish /topic/com.cisco.ise.session
- publish /topic/com.cisco.ise.session.group
- publish /topic/com.cisco.ise.anc
- <CUSTOM> - 이 옵션을 선택하면 사용자 맞춤화 작업을 지정할 수 있습니다.

단계 **4** **Groups(**그룹**)** 드롭다운 목록에서 이 서비스에 매핑할 그룹을 선택합니다.

사전 정의된 그룹(예: EPS 및 ANC) 및 수동으로 추가한 그룹이 이 드롭다운 목록에 나열됩니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

pxGrid 서비스 활성화

시작하기 전에

- Cisco pxGrid 클라이언트에서 요청을 확인하려면 하나 이상의 노드에서 pxGrid 페르소나를 활성화합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)**.

단계 **2** 클라이언트 옆의 확인란을 선택하고 **Approve(**승인**)**를 클릭합니다.

단계 **3** 최신 상태를 보려면 **Refresh(**새로 고침**)**를 클릭합니다.

단계 **4** 활성화할 기능을 선택하고 **Enable(**활성화**)**을 클릭합니다.

단계 **5** 최신 상태를 보려면 **Refresh(**새로 고침**)**를 클릭합니다.

pxGrid 진단

- XMPP: **Administration (**관리**) > pxGrid Services(pxGrid** 서비스**) > Diagnostics(**진단**) > XMPP** 페이지에 pxGrid 1.0 클라이언트(외부 및 내부)가 나열됩니다. 또한 기능도 나열됩니다.
- Websocket: **Administration (**관리**) > pxGrid Services(pxGrid** 서비스**) > Diagnostics(**진단**) > Websocket** 페이지에 pxGrid 2.0 클라이언트(외부 및 내부)가 나열됩니다. 또한 사용 가능한 pxGrid 2.0 주제와 각 주제를 게시하거나 구독하는 클라이언트도 나열됩니다.
- Log: **Administration(**관리**) > pxGrid Services(pxGrid** 서비스**) > Diagnostics(**진단**) > Live Logs(**라이브 로그**)** 페이지에 관리 이벤트가 나열됩니다.
- 테스트: **Administration(**관리**) > pxGrid Services(pxGrid** 서비스**) > Diagnostics(**진단**) > Tests(**테스트**)** 페이지에서 실행되는 상태 모니터링 테스트는 클라이언트가 세션 디렉터리 서비스에 액세스할 수 있는지 확인합니다. **Start Test(**테스트 시작**)** 버튼을 클릭하면 내부 pxGrid 2.0 클라이언트가 생성됩니다. 이 클라이언트는 대량 세션 다운로드 REST API를 쿼리한 다음 세션 주제를 구독합니다. 해당 주제를 몇 분간 수신한 후 종료됩니다. 테스트가 완료되면 테스트 활동의 로그를 표시할 수 있습니다.

pxGrid 설정

- **Automatically approve new certificate-based accounts(**새 인증서 기반 계정 자동 승인**)**: 기본적으로 꺼져 있으며, pxGrid 서버에 대한 연결을 제어할 수 있습니다. 환경의 모든 클라이언트를 신뢰하는 경우에만 이 설정을 선택하십시오.
- **Allow password based account creation(**비밀번호 기반 계정 생성 허용**)**: pxGrid 클라이언트에 대해 사용자 이름/비밀번호 기반 인증을 활성화하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 pxGrid 클라이언트가 자동으로 승인되지 않습니다.

Cisco pxGrid 인증서 생성

시작하기 전에

일부 Cisco ISE 버전에는 NetscapeCertType을 사용하는 Cisco pxGrid용 인증서가 있습니다. 새 인증서를 생성하는 것이 좋습니다.

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- 기본 PAN에서 Cisco pxGrid 인증서를 생성해야 합니다.
- Cisco pxGrid 인증서가 SAN(Subject Alternative Name) 확장을 사용하는 경우, 주체 ID의 FQDN을 DNS 이름 항목으로 포함해야 합니다.
- 디지털 서명을 사용하여 인증서 템플릿을 생성하고 이를 사용하여 새 Cisco pxGrid 인증서를 생성합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **Client Management(**클라이언트 관리**)** > **Certificates(**인증서**)**.

단계 **2** **I want to(**수행할 작업**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)**: 이 옵션을 선택하면 CN(Common Name)을 입력해야 합니다.
- **Generate a single certificate without a certificate signing request(**인증서 서명 요청을 이용해 단일 인증서 생성**)**: 이 옵션을 선택하면 Certificate Signing Request(인증서 서명 요청) 세부정보를 입력해야 합니다.
- **Generate bulk certificates(**대량 인증서 생성**)**: 필수 세부정보를 포함하는 CSV 파일을 업로드할 수 있습니다.
- **Download Root Certificate Chain(**루트 인증서 체인 다운로드**)**: 루트 인증서를 다운로드하여 신뢰할 수 있는 인증서 저장소에 추가합니다. 호스트 이름 및 인증서 다운로드 형식을 지정해야 합니다.

단계 **3** **CN(Common Name)**: **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)** 옵션을 선택하는 경우에 필요합니다. pxGrid 클라이언트의 FQDN을 입력합니다.

단계 **4** **Certificate Signing Request Details(**인증서 서명 요청 세부정보**)**: **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)** 옵션을 선택하는 경우에 필요합니다. 전체 인증서 서명 요청 세부정보를 입력합니다.

단계 **5** **Description(**설명**)**: (선택 사항) 이 인증서에 대한 설명을 입력합니다.

단계 **6** **Certificate Template(**인증서 템플릿**)**: **pxGrig_Certificate_Template** 링크를 클릭하여 인증서 템플릿을 다운로드하고 요구 사항에 따라 템플릿을 편집합니다.

단계 **7** **SAN(Subject Alternative Name)**: 여러 SAN을 추가할 수 있습니다. 다음 옵션을 사용할 수 있습니다.

- **IP address(IP** 주소**)**: 인증서에 연결할 Cisco pxGrid 클라이언트의 IP 주소를 입력합니다.
- **FQDN**: pxGrid 클라이언트의 정규화된 도메인 이름을 입력합니다.

참고 **Generate Bulk Certificate(**대량 인증서 생성**)** 옵션을 선택했다면 이 필드는 표시되지 않습니다.

단계 **8** **Certificate Download Format(**인증서 다운로드 형식**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **PEM(Private Enhanced Electronic Mail)** 형식의 인증서**, PKCS8 PEM** 형식의 키**(**인증서 체인 포함**))**: 루트 인증서, 중간 CA 인증서 및 최종 엔티티 인증서는 PEM 형식으로 표시됩니다. PEM 형식 인증서는 BASE64 인코딩 ASCII 파일입니다. 각 인증서는 "--------BEGIN CERTIFICATE-----" 태그로 시작하고 "-------END CERTIFICATE----" 태그로 끝납니다. 최종 엔티티의 개인 키는 PKCS * PEM을 사용하여 저장됩니다. "-----BEGIN ENCRYPTED PRIVATE KEY----" 태그로 시작하고 "-----END ENCRYPTED PRIVATE KEY----" 태그로 끝납니다.
- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)(PKCS12** 형식**(**인증서 체인 포함**,** 인증서 체인과 모두를 위한 단일 파일**))**: 루트 CA 인증서, 중간 CA 인증서, 최종 엔티티의 인증서 및 개인 키를 단일 암호화 파일에 저장하는 이진 형식입니다.

단계 **9** **Certificate Password(**인증서 비밀번호**)**: 인증서의 비밀번호를 입력하고 다음 필드에 비밀번호를 다시 입력하여 확인합니다.

단계 **10** **Create(**생성**)**를 클릭합니다.

생성한 인증서는 Cisco ISE의 **Issued Certificates(**발급된 인증서**)** 창에 표시됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Issued Certificates(**발급된 인증서**)**입니다. 인증서는 브라우저의 다운로드 디렉터리에도 다운로드됩니다.

참고 Cisco ISE 2.4 패치 13부터는 pxGrid 서비스에 대한 인증서 요건이 더욱 엄격해졌습니다. Cisco ISE의 기본 SSC(Self-Signed Certificate, 자가서명 인증서)를 pxGrid 인증서로 사용하는 경우 Cisco ISE 2.4 패치 13 이상 버전을 적용한 후 Cisco ISE에서 해당 인증서를 거부할 수 있습니다. 해당 인증서의 이전 버전에서 **Netscape Cert Type(Netscape** 인증서 유형**)** 확장이 **SSL Server(SSL** 서버**)**로 지정되었기 때문에 실패하는 것입니다(이제 클라이언트 인증서도 필요함).

규정 미준수 인증서가 있는 클라이언트는 Cisco ISE와 통합되지 않습니다. 내부 CA에서 발급한 인증서를 사용하거나 적절한 사용 확장을 사용하여 새 인증서를 생성합니다.

- 인증서의 키 사용**(Key Usage)** 확장에는 **Digital Signature(**디지털 서명**)** 및 **Key Encipherment(**키 암호화**)** 필드가 포함되어야 합니다.
- 인증서의 **Extended Key Usage(**확장 키 사용**)** 확장에는 **Client Authentication(**클라이언트 인증**)** 및 **Server Authentication(**서버 인증**)** 필드가 포함되어야 합니다.
- **Netscape Certificate Type(Netscape** 인증서 유형**)** 확장은 필요하지 않습니다. 해당 확장을 포함하려면 확장에 **SSL Client(SSL** 클라이언트**)** 및 **SSL Server(SSL** 서버**)**를 모두 포함해야 합니다.
- 자가서명 인증서를 사용하는 경우 **Basic Constraints CA** 기본 제약 조건 **CA)** 필드를 True로 설정하고 **Key Usage(**키 사용**)** 확장에 **Key Cert Sign(**키 인증서 서명**)** 필드를 포함해야 합니다.

15 장

통합

다음 섹션에서는 Cisco ISE의 기능을 지원하기 위해 스위치 및 무선 컨트롤러에 필요한 컨피그레이션에 대해 설명합니다.

표준 웹 인증을 지원하도록 스위치 활성화

인증 시의 URL 리디렉션을 위한 프로비저닝을 포함하여 Cisco ISE에 대해 표준 웹 인증 기능을 활성화하려면 스위치 구성에 다음 명령을 포함해 주십시오.

```
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.2.3

ip http server
! Must enable HTTP/HTTPS for URL-redirection on port 80/443
ip http secure-server
```

가상 RADIUS 트랜잭션을 위한 로컬 사용자 이름 및 비밀번호 정의

스위치가 이 네트워크 세그먼트에 대한 RADIUS 서버인 경우에도 Cisco ISE 노드와 통신할 수 있게 하려면 다음 명령을 입력합니다.

```
username test-radius password 0 abcde123
```

로그 및 계정 타임스탬프 정확도 유지를 위한 NTP 서버 컨피그레이션

다음 명령을 입력하여 Cisco ISE에 설정한 것처럼 스위치에 NTP 서버를 지정합니다.

```
ntp server <IP_address>|<domain_name>
```

AAA 기능을 활성화하는 명령

802.1X 및 MAB 인증 기능을 포함하여 Cisco ISE와 스위치 간에 다양한 AAA 기능을 활성화하려면 스위치에서 다음 명령을 입력합니다.

```
aaa new-model
! Creates an 802.1X port-based authentication method list
aaa authentication dot1x default group radius
! Required for VLAN/ACL assignment
aaa authorization network default group radius
! Authentication & authorization for webauth transactions
aaa authorization auth-proxy default group radius
! Enables accounting for 802.1X and MAB authentications
```

```
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
!
aaa accounting update periodic 5

! Update AAA accounting information periodically every 5 minutes

aaa accounting system default start-stop group radius
!
```

스위치에서의 **RADIUS** 서버 컨피그레이션

다음 명령을 입력하여 RADIUS 소스 서버 역할을 하는 Cisco ISE와 상호 작용하도록 스위치를 구성합니다.

```
!
radius-server <ISE Name>

! ISE Name is the name of the ISE PSN

address ipv4 <ip address> auth-port 1812 acct-port 1813

! IP address is the address of the PSN. This example uses the standard RADIUS ports.

key <passwd>

! passwd is the secret password confiugured in Cisco ISE

exit
```

참고 인증에 Active Directory를 사용하는 RADIUS 요청에 더 긴 응답 시간을 제공하도록 3회 재시도와 함께 데드 기준 시간으로 30초를 구성하는 것이 좋습니다.

RADIUS CoA(Change of Authorization)를 활성화하는 명령

다음 명령을 입력하여 Cisco ISE에서 포스처 기능을 지원하는 RADIUS CoA 동작을 스위치가 적절하게 처리할 수 있도록 하는 설정을 지정합니다.

```
aaa server radius dynamic-author

client <ISE-IP> server-key 0 abcde123
```

참고

- Cisco ISE는 Cisco IOS 소프트웨어 기본값인 포트 1700을 사용하지만 CoA에 대해서는 RFC 기본 포트 3799를 사용합니다. 기존의 Cisco Secure ACS 5.x 고객은 기존 ACS 구현의 일부분으로 CoA를 사용 중인 경우 이 포트가 포트 3799로 이미 설정되어 있을 수 있습니다.
- 공유 암호 키는 네트워크 디바이스를 추가하는 동안 Cisco ISE에 구성한 키와 동일해야 하며 IP 주소는 PSN IP 주소여야 합니다.

디바이스 추적 및 DHCP 스누핑을 활성화하는 명령

Cisco ISE에서 선택적인 보안 기반 기능을 제공하려는 경우 다음 명령을 입력하여 스위치 포트에서 동적 ACL의 IP 교체를 위해 디바이스 추적 및 DHCP 스누핑을 활성화할 수 있습니다.

```
! Optional

ip dhcp snooping

! Required!

! Configure Device Tracking Policy!
device-tracking policy <DT_POLICY_NAME>
no protocol ndp
tracking enable

! Bind it to interface!
interface <interface_id>
device-tracking attach-policy<DT_POLICY_NAME>
```

RADIUS 계정 관리에서는 DHCP 스누핑을 활성화해도 IOS 센서에서 DHCP 속성을 Cisco ISE로 전송하지 않습니다. 이러한 경우에는 VLAN에서 DHCP 스누핑을 활성화하여 DHCP를 활성 상태로 설정해야 합니다.

VLAN에서 DHCP 스누핑을 활성화하려면 다음 명령을 사용합니다.

```
ip dhcp snooping
ip dhcp snooping vlan 1-100
```

802.1X 포트 기반 인증을 활성화하는 명령

스위치 포트에 대해 802.1X 인증을 전역적으로 설정하려면 다음 명령을 입력합니다.

```
dot1x system-auth-control
```

중요 인증에 대해 **EAP**를 활성화하는 명령

LAN을 통한 신청자 인증 요청을 지원하려면 다음 명령을 입력하여 중요 인증에 대한 EAP(액세스할 수 없는 인증 바이패스)를 활성화합니다.

```
dot1x critical eapol
```

복구 지연을 사용하여 **AAA** 요청을 제한하는 명령

중요 인증 복구 이벤트가 발생하면 다음 명령을 입력하여 Cisco ISE가 복구 후 서비스를 다시 시작할 수 있도록 밀리초 단위의 지연을 자동으로 적용하도록 스위치를 구성할 수 있습니다.

```
authentication critical recovery delay 1000
```

시행 상태에 따른 **VLAN** 정의

네트워크의 알려진 시행 상태에 따라 VLAN 이름, 번호 및 SVI(Switch Virtual Interface)를 정의하려면 다음 명령을 입력합니다. 해당 VLAN 인터페이스를 생성하여 네트워크 간에 라우팅을 활성화할 수 있습니다. 이는 엔드포인트(PC, 노트북 등)와 엔드포인트를 네트워크에 연결하는 데 사용되는 IP 폰 모두에서 동일한 네트워크 세그먼트를 통해 전달되는 여러 소스의 트래픽을 처리할 때 특히 유용할 수 있습니다.

```
vlan <VLAN_number>

name ACCESS!

vlan <VLAN_number>

name VOICE

!

interface <VLAN_number>

description ACCESS

ip address 10.1.2.3 255.255.255.0

ip helper-address <DHCP_Server_IP_address>

ip helper-address <Cisco_ISE_IP_address>

!
```

```
interface <VLAN_number>

description VOICE

ip address 10.2.3.4 255.255.255.0

ip helper-address <DHCP_Server_IP_address>
```

스위치에서의 로컬(기본) ACL(Access List) 정의

다음 명령을 입력하여 Cisco ISE가 인증 및 권한 부여를 위해 필요한 동적 ACL 업데이트를 수행할 수 있도록 이전 스위치(12.2(55)SE 이전 버전의 Cisco IOS 소프트웨어 릴리스)에서 다음 기능을 활성화합니다.

```
ip access-list extended ACL-ALLOW

 permit ip any any

!

ip access-list extended ACL-DEFAULT

  remark DHCP

  permit udp any eq bootpc any eq bootps

  remark DNS

  permit udp any any eq domain

  remark Ping

  permit icmp any any

  remark Ping

  permit icmp any any

  remark PXE / TFTP

  permit udp any any eq tftp

  remark Allow HTTP/S to ISE and WebAuth portal

permit tcp any host <Cisco_ISE_IP_address> eq www
```

```
permit tcp any host <Cisco_ISE_IP_address> eq 443

permit tcp any host <Cisco_ISE_IP_address> eq 8443

permit tcp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8905

permit udp any host <Cisco_ISE_IP_address> eq 8906

permit tcp any host <Cisco_ISE_IP_address> eq 8080

permit udp any host <Cisco_ISE_IP_address> eq 9996

remark Drop all the rest
  deny ip any any log
!
! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
```

참고 무선 컨트롤러의 컨피그레이션은 CPU 사용률을 높이고 시스템이 불안정해질 수 있는 위험을 높일 수 있습니다. 이는 IOS 문제로, Cisco ISE에 부정적인 영향을 미치지 않습니다.

802.1X 및 MAB에 대한 스위치 포트 활성화

802.1X 및 MAB에 대해 스위치 포트를 활성화하려면 다음 단계를 수행합니다.

단계 **1** 모든 액세스 스위치 포트의 인터페이스 구성 모드로 진입합니다.

interface range FastEthernet0/1-8

단계 **2** 트렁크 모드가 아닌 액세스 모드용으로 스위치 포트를 활성화합니다.

switchport mode access

단계 **3** 액세스 VLAN을 정적으로 구성합니다. 이렇게 하면 액세스 VLAN에 대한 로컬 프로비저닝을 제공하며, 개방형 모드 인증을 사용하려면 다음과 같이 구성해야 합니다.

switchport access vlan <*VLAN_number*>

단계 **4** 음성 VLAN을 정적으로 구성합니다.

switchport voice vlan <*VLAN_number*>

단계 **5** 개방형 모드 인증을 활성화합니다. 개방형 모드를 사용하면 인증이 완료되기 전에 트래픽을 데이터 및 음성 VLAN에 브리지할 수 있습니다. 프로덕션 환경에서는 무단 액세스를 방지하기 위해 포트 기반 ACL을 사용하는 것이 좋습니다.

개방형 모드 인증을 활성화하면 포트 ACL에 따라 AAA 서버 응답 전에 사전 인증 액세스도 활성화됩니다.

authentication open

단계 **6** 포트 기반 ACL을 적용하여 인증되지 않은 엔드포인트에서 액세스 VLAN에 기본적으로 브리지해야 하는 트래픽을 확인합니다. 먼저 모든 액세스를 허용하고 정책을 나중에 시행해야 하므로, 스위치 포트를 통한 모든 트래픽을 허용하기 위해 ACL-ALLOW를 적용해야 합니다. 네트워크를 완전하게 파악하고 기존의 최종 사용자 경험에는 아직 영향을 주지 않아야 하므로, 현재 모든 트래픽을 허용하는 기본 Cisco ISE 권한 부여는 이미 생성한 상태여야 합니다.

AAA 서버에서 동적 ACL을 앞에 추가하도록 ACL을 구성해야 합니다.

ip access-group ACL-ALLOW in

참고 DSBU 스위치의 Cisco IOS 소프트웨어 릴리스 12.2(55)SE 이전 버전에서는 RADIUS AAA 서버의 동적 ACL을 적용하려면 포트 ACL이 필요합니다. 기본 ACL을 포함하지 않으면 스위치가 할당된 동적 ACL을 무시합니다. Cisco IOS 소프트웨어 릴리스 12.2(55)SE에서는 기본 ACL이 자동으로 생성되어 적용됩니다.

참고 여기서는 기존 네트워크에 영향을 주지 않고 802.1X 포트 기반 인증을 활성화할 것이므로 실험의 이 부분에서는 ACL-ALLOW를 사용합니다. 이후 연습에서는 프로덕션 환경에 대해 원치 않는 트래픽을 차단하는 다른 ACL-DEFAULT를 적용할 것입니다.

단계 **7** 다중 인증 호스트 모드를 활성화합니다. 다중 인증은 기본적으로 MDA(Multi-Domain Authentication)의 상위 집합입니다. MDA에서는 데이터 도메인에 엔드포인트를 하나만 허용합니다. 다중 인증을 구성할 때는 MDA에서와 마찬가지로 음성 도메인에는 인증된 전화 하나를 포함할 수 있지만 데이터 도메인에서는 데이터 디바이스를 수에 제한 없이 인증할 수 있습니다.

같은 물리적 액세스 포트에서 음성 및 여러 엔드포인트를 허용합니다.

authentication host-mode multi-auth

참고 여러 데이터 디바이스(가상화된 디바이스 또는 허브에 연결된 물리적 디바이스)가 IP 전화기에 연결되는 경우 액세스 포트의 물리적 링크 상태 인식 성능이 저하될 수 있습니다.

단계 **8** 다음과 같은 명령으로 다양한 인증 방법 옵션을 활성화합니다.
다음과 같이 재인증을 활성화합니다.
authentication periodic
다음과 같이 RADIUS 세션 시간 초과를 통한 재인증을 활성화합니다.
authentication timer reauthenticate server
authentication event fail action next-method
데드 서버의 경우 다음과 같이 중요 인증 VLAN 방법을 구성합니다.
authentication event server dead action reinitialize vlan *<VLAN_number>*
authentication event server alive action reinitialize
다음과 같이 802.1X 및 MAB에 대한 IOS Flex-Auth 인증을 구성합니다.
authentication order dot1x mab
authentication priority dot1x mab

단계 **9** 다음과 같이 스위치 포트에서 802.1X 포트 제어를 활성화합니다.
authentication port-control auto
authentication violation restrict

단계 **10** 다음과 같이 MAB(MAC Authentication Bypass)를 활성화합니다.
mab

단계 **11** 다음과 같이 스위치 포트에서 802.1X를 활성화합니다.
dot1x pae authenticator

단계 **12** 다음과 같이 재전송 기간을 10초로 설정합니다.
dot1x timeout tx-period *10*

참고 802.1X tx-period 시간 초과는 10초로 설정해야 합니다. 결과에 대해 잘 알고 있는 경우가 아니면 이 값을 변경하지 마십시오.

단계 **13** portfast 기능을 활성화합니다.
spanning-tree portfast

ID 기반 네트워킹 서비스를 기반으로 802.1X를 활성화하는 명령

다음 예에서는 802.1X, MAB 및 웹 인증을 사용하는 순차적 인증 방법을 허용하도록 구성된 제어 정책을 보여줍니다.

```
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
```

```
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
!


policy-map type control subscriber DOT1XMAB
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
   30 authorize
  40 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x retries 2 retry-time 0 priority 10
!
```

다음 예에서는 MAB, 802.1X 및 웹 인증을 사용하는 순차적 인증 방법을 허용하도록 구성된 제어 정책을 보여줍니다.

```
policy-map type control subscriber MABDOT1X
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using mab priority 20
   20 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class ALL_FAILED do-until-failure
   10 authentication-restart 60
 event authentication-success match-all
  10 class DOT1X do-until-failure
   10 terminate mab
 event agent-found match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
```

인터페이스에서 서비스 정책 적용:

```
interface GigabitEthernet1/0/4
 switchport mode access
 device-tracking attach-policy pol1
 ip access-group sample in
 authentication timer reauthenticate server
 access-session port-control auto
 mab
```

```
dot1x pae authenticator
dot1x timeout tx-period 10
dot1x timeout auth-period 10
spanning-tree portfast
service-policy type control subscriber DOT1XMAB
```

EPM 로깅을 활성화하는 명령

Cisco ISE 기능에 대해 사용 가능한 문제 해결 및 기록을 지원하려면 스위치에서 표준 로깅 기능을 설정합니다.

epm logging

SNMP 트랩을 활성화하는 명령

스위치가 이 네트워크 세그먼트에서 적절한 VLAN을 통해 Cisco ISE로부터 전송되는 SNMP 트랩을 수신할 수 있는지 확인합니다.

snmp-server community public RO

snmp-server trap-source *<VLAN_number>*

프로파일링을 위해 SNMP v3 쿼리를 활성화하는 명령

다음 명령을 사용하여 Cisco ISE 프로파일링 서비스를 지원하기 위해 SNMP v3 폴링이 올바르게 수행되도록 하려면 스위치를 구성합니다. 그 전에는 **SNMP Settings(SNMP** 설정**)** 창의 Cisco ISE GUI에서 SNMP 설정을 구성합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Add | Edit(**추가 | 편집**)** > **SNMP Settings(SNMP** 설정**)**입니다.

Snmp-server user *<name> <group>* **v3 auth md5** *<string>* **priv des** *<string>*

snmp-server group *<group>* **v3 priv**

snmp-server group *<group>* **v3 priv context***vlan-1*

참고 각 상황 정보에 대해 **snmp-server group** *<group>* **v3 priv context** *vlan-1* 명령을 구성해야 합니다. **snmp show context** 명령은 모든 상황 정보를 나열합니다.

연결 문제가 없는데 SNMP 요청 시간이 초과되는 경우에는 시간 초과 값을 늘릴 수 있습니다.

프로파일러가 수집하도록 할 **MAC** 알림 트랩을 활성화하는 명령

Cisco ISE 프로파일러 기능이 네트워크 엔드포인트에서 정보를 수집할 수 있도록 적절한 MAC 알림 트랩을 전송하려면 스위치를 구성합니다.

```
mac address-table notification change

mac address-table notification mac-move

snmp trap mac-notification change added

snmp trap mac-notification change removed
```

스위치에서의 **RADIUS** 유휴 시간 초과 컨피그레이션

스위치에서 RADIUS 유휴 시간 초과를 구성하려면 다음 명령을 사용합니다.

```
Switch(config-if)# authentication timer inactivity
```

여기서 *inactivity*는 클라이언트 활동이 권한이 부여되지 않은 활동으로 간주될 때까지의 비활성 간격(초)입니다.

Cisco ISE에서는 세션 비활성 타이머가 적용되어야 하는 모든 권한 부여 정책에 대해 이 옵션을 활성화할 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다.

iOS 신청자 프로비저닝을 위한 무선 **LAN** 컨트롤러 컨피그레이션

단일 **SSID**용

Apple iOS 기반 디바이스(iPhone 또는 iPad)가 동일한 무선 액세스 포인트에서 SSID 간을 전환할 수 있도록 지원하려면 **FAST SSID change** 기능을 활성화하도록 무선 컨트롤러를 구성해야 합니다. 이 기능을 사용하면 iOS 기반 디바이스가 SSID 간을 보다 빠르게 전환할 수 있습니다.

듀얼 **SSID BYOD**용

이중 SSID BYOD를 지원하려면 고속 SSID를 활성화해야 합니다. 고속 SSID 변환이 활성화되면 무선 컨트롤러를 통해 클라이언트가 SSID 사이를 빠르게 이동할 수 있습니다. 고속 SSID가 활성화되면 클

라이언트 항목이 지워지지 않고 지연이 적용되지 않습니다. Cisco Wireless Controller에서 고속 SSID를 구성하는 방법에 대한 자세한 내용은 Cisco Wireless Controller 컨피그레이션 가이드를 참조하십시오.

무선 컨트롤러 구성 예

```
WLC (config)# FAST SSID change
```

일부 Apple iOS 기반 디바이스에서는 무선 네트워크에 연결을 시도하는 동안 다음 오류 메시지가 표시될 수 있습니다.

```
Could not scan for Wireless Networks.(무선 네트워크를 스캔할 수 없습니다.)
```

이 오류 메시지는 디바이스 인증에 영향을 주지 않으므로 무시해도 됩니다.

모바일 디바이스 관리 상호운용성을 위해 무선 LAN 컨트롤러에서 ACL 구성

미등록 디바이스 및 인증서 프로비저닝을 리디렉션하려면 권한 부여 정책에 사용할 ACL을 무선 컨트롤러에서 구성해야 합니다. ACL의 순서는 다음과 같이 지정해야 합니다.

단계 **1** 서버에서 클라이언트로의 모든 아웃바운드 트래픽을 허용합니다.

단계 **2** (선택 사항) 문제 해결용으로 클라이언트에서 서버로의 ICMP 클라이언트 인바운드 트래픽을 허용합니다.

단계 **3** 미등록/규정 미준수 디바이스에 대해 MDM 에이전트를 다운로드하고 규정 준수 확인을 진행할 수 있도록 MDM 서버 액세스를 허용합니다.

단계 **4** 웹 포털과 supplicant 및 인증서 프로비저닝 플로우에 대해 클라이언트->서버->Cisco ISE로의 모든 인바운드 트래픽을 허용합니다.

단계 **5** 이름 확인용으로 클라이언트에서 서버로의 인바운드 DNS 트래픽을 허용합니다.

단계 **6** IP 주소용으로 클라이언트에서 서버로의 인바운드 DHCP 트래픽을 허용합니다.

단계 **7** 회사 정책에 따른 Cisco ISE로의 리디렉션용으로 클라이언트->서버->회사 리소스로의 모든 인바운드 트래픽을 거부합니다.

단계 **8** (선택 사항) 나머지 트래픽을 허용합니다.

예

다음 예제에서는 미등록 디바이스를 BYOD 흐름으로 리디렉션하기 위한 ACL을 보여 줍니다. 이 예제에서 Cisco ISE IP 주소는 10.35.50.165, 내부 회사 네트워크 IP 주소는 192.168.0.0 및 172.16.0.0(리디렉션용), MDM 서버 서브넷은 204.8.168.0입니다.

그림 ***62:*** 미등록 디바이스 리디렉션용 ***ACL***

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

16 장

문제 해결

Cisco ISE에서 서비스 모니터링 및 문제 해결

모니터링 및 문제 해결(MnT) 서비스는 모든 Cisco ISE 런타임 서비스에 사용할 수 있는 포괄적인 ID 솔루션입니다. **Operations(**운영**)** 메뉴에는 다음 구성 요소가 포함되어 있으며 기본 PAN(Policy Administration Node)에서만 볼 수 있습니다. **Operations(**운영**)** 메뉴는 기본 모니터링 노드에 표시되지 않습니다.

- 모니터링: 네트워크에 대한 액세스 활동의 상태를 나타내는 의미 있는 데이터를 실시간으로 표시합니다. 이 정보는 쉽게 해석할 수 있으며 작동 조건에 영향을 미칠 수 있습니다.
- 문제 해결: 네트워크의 액세스 문제를 해결하기 위한 상황별 지침을 제공합니다. 이를 통해 관리자가 사용자의 문제를 해결하고 시기 적절하게 해결 방법을 제공할 수 있습니다.

- 보고: 관리자가 트렌드를 분석하고 시스템 성능 및 네트워크 활동을 모니터링하는 데 사용할 수 있는 표준 보고서 카탈로그를 제공합니다. 다양한 방법으로 보고서를 맞춤화하고 나중에 사용하기 위해 저장할 수 있습니다. 모든 보고서(**Health Summary(**상태 요약 보고서**)** 제외)에서 와일드카드와 여러 값을 사용하여 **Identity(ID)**, **Endpoint ID(**엔드포인트 **ID)** 및 **ISE Node(ISE** 노드**)** 필드에 대해 기록을 검색할 수 있습니다.

ISE Community Resource(ISE 커뮤니티 리소스)

문제 해결 TechNote의 전체 목록은 ISE Troubleshooting TechNotes를 참고하십시오.

Cisco ISE에서 TAC 지원 케이스 열기

Cisco ISE에서 케이스를 제기하여 구축 문제에 대한 지원을 요청하십시오. Cisco ISE 포털의 TAC 지원 케이스 기능을 사용하면, 문제가 발생한 특정 노드에 대한 지원 사례를 쉽게 제기할 수 있습니다. 제시된 양식을 통해 제공하는 정보와 함께 노드의 일련 번호 및 사용중인 Cisco ISE 버전과 같은 정보도 Cisco TAC로 전송됩니다.

참고 이 기능은 Cisco ISE 릴리스 3.0 패치 1 이상에서 사용할 수 있습니다.

단계 **1** Cisco ISE 포털의 홈 창에서 오른쪽 상단 모서리에 있는 물음표 아이콘을 클릭합니다.

단계 **2** 표시되는 인터랙티브 도움말 메뉴에서 **Resources(**리소스**)**를 클릭하고 드롭 다운 목록에서 **TAC Support Cases(TAC** 지원 케이스**)**를 선택합니다.

단계 **3** 표시되는 새 창에서 cisco.com 자격증명을 사용하여 로그인합니다. 기능에 액세스할 수 없다는 오류 메시지가 표시되면 고객 지원에 문의하여 Cisco ISE 계약의 약관을 검토하십시오.

단계 **4** 로그인하면 **Cases(**케이스**)** 창이 표시됩니다. **Open A Case(**케이스 열기**)**를 클릭합니다.

단계 **5** **Open Case(**케이스 열기**)** 양식에서

1. 드롭 다운 목록에서 케이스를 열 최대 4 개의 노드를 선택합니다. 기본 PAN 및 MnT 노드가 기본적으로 선택됩니다.
2. **Title(**제목**)** 및 **Description(**설명**)** 필드에 문제의 세부정보를 입력합니다.
3. **Contract ID(**계약 **ID)** 및 **Product Name(**제품 이름**)** 필드에 필수 정보를 입력합니다.
4. (선택 사항) 다음에 대한 값을 선택합니다.
    1. **Tech(**기술**)** : Cisco ISE 릴리스 드롭 다운 목록에서 선택합니다. 여기서 **Cisco Identity Services Engine-2.6**은 릴리스 2.6 이상을 나타냅니다.
    2. **Sub Tech(**하위 기술**)**: Cisco ISE 기능의 드롭 다운 목록에서 문제 영역을 선택합니다.
    3. **Problem Code(**문제 코드**)**: 드롭 다운 목록에서 해당 값을 선택합니다.

다음에 수행할 작업

이를 통해 Cisco TAC는 문제의 세부정보를 수신하고 문제를 조사 및 해결하기 위해 연락을 드릴 것입니다. 여기서 생성되는 케이스는 기본적으로 심각도 레벨 3입니다. 심각도가 더 높은 케이스(1 및 2)의 경우 Cisco TAC에 문의하여 케이스를 엽니다.

TAC Support Cases(TAC 지원 케이스**)** 창에서 케이스 세부정보를 확인합니다. 표시된 케이스 목록에서 검토할 케이스의 확인란을 선택합니다. 케이스 세부정보 및 이 케이스에 대한 TAC의 업데이트가 포함된 메모 목록을 보려면 **View Case(**케이스 보기**)**를 클릭합니다. 케이스에 나만의 메모를 추가하려면 **Add Notes(**메모 추가**)**를 클릭합니다.

케이스를 닫으려면 **Close Case(**케이스 닫기**)** 버튼을 클릭합니다. 케이스를 닫을 때 그 사유를 제시해야 합니다.

상태 확인

Cisco ISE 릴리스 3.0에는 Cisco ISE 구축의 모든 노드를 진단하는 온디맨드 상태 확인 옵션이 도입되었습니다. 작업 전에 모든 노드에서 상태 확인을 실행하면 다운타임을 줄이고 중요한 문제를 식별하여 Cisco ISE 시스템의 전반적인 기능을 개선할 수 있습니다. 상태 확인은 구성 요소의 작동 상태를 알려주고 Cisco ISE 구성 요소가 손상된 경우 즉시 문제 해결 권장 사항을 안내합니다.

표 ***179:*** 상태 확인 구축

구축 유형	설명
플랫폼 지원 확인	이렇게 하면 구축에서 지원되는 플랫폼을 확인합니다. 34xx 및 기타 지원되지 않는 플랫폼 세부 정보를 확인하고 시스템에 최소 12 코어 CPU, 300GB 하드 디스크, 16GB 메모리가 있는지 확인합니다.
구축 검증	동기화 또는 진행 중인 구축 노드의 상태를 확인할 수 있습니다.
DNS 확인 가능성	호스트 이름 및 IP 주소의 정방향 및 역방향 조회를 확인합니다.
신뢰 저장소 인증서 검증	신뢰 저장소 인증서가 유효하거나 만료되었는지를 나타냅니다.
시스템 인증서 검증	각 노드에 대한 시스템 인증서 검증을 확인합니다.
디스크 공간 확인	플랫폼 지원 확인에 있는 하드 디스크를 확인합니다. 그리고 추가 업그레이드 절차를 위해 디스크의 사용 가능한 공간을 확인합니다.
NTP 연결성 및 시간 소스 확인	시스템에 구성된 NTP 및 시간 소스가 NTP 서버에서 오는지 확인합니다.

구축 유형	설명
로드 평균 확인	지정된 간격으로 시스템의 로드를 자주 확인합니다. 빈도는 1분, 5분 및 15분 간격입니다.
MDM 검증	구성된 MDM 서버와 PSN 서버 간의 연결을 확인합니다.
라이선스 검증	스마트 라이선스가 구성되어 있고 유효한지 확인합니다. 스마트 라이선스가 구성되지 않고 유효한 사용자인 경우, 라이선스를 구성하고 검증하도록 요청하는 경고가 표시됩니다.
서비스 또는 프로세스 실패	서비스 또는 애플리케이션이 실행 중이거나 장애가 발생한 상태를 나타냅니다.
I/O 대역폭 성능 확인	디스크 읽기 쓰기 속도를 확인합니다.

참고 구축 옆의 숫자는 노드의 수와 상태 확인 세부 사항을 나타냅니다. 예를 들어, 구축에 0/2가 있는 경우 0은 실패/진행/완료 상태의 노드 수를 나타내며 2는 구축의 노드 수를 나타냅니다.

참고 상태 확인 중에 노드가 15분 동안 응답을 반환하지 않으면 해당 노드에 대한 상태 확인 시간이 초과하게 됩니다.

상태 확인 시작

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Health Checks(**상태 확인**)**.

단계 **2** **Start health checks(**상태 확인 시작**)**를 클릭합니다.

정보 팝업 창에 다음 메시지가 표시됩니다.

상태 확인이 트리거되었습니다.

단계 **3** **Ok(**확인**)**를 클릭하여 상태를 확인합니다.

단계 **4** **Health Checks(**상태 확인**)** 창에서 각 구성 요소의 상태를 볼 수 있습니다. 다음 색상은 Cisco ISE 구성 요소의 상태를 나타냅니다.

색상	상태	작업
빨간색	좋지 않음	상자에서 제공되는 문제 해결 권장 사항을 보려면 드롭 다운 옵션을 클릭합니다. 문제를 해결하고 새로 고침 아이콘을 클릭합니다.
주황색	좋음 참고 구성 요소의 상태가 작업을 수행하기에 적합합니다. 그러나 향후 일부 기능에 영향을 미칠 수 있는 문제가 있습니다.	상자에서 제공되는 문제 해결 권장 사항을 보려면 드롭 다운 옵션을 클릭합니다.
녹색	좋음	추가 작업은 필요하지 않습니다.
파란색	좋음	정보 아이콘을 클릭하여 기능에 대한 중요 정보를 확인합니다.

단계 **5** **Download Reports(**보고서 다운로드**)**를 클릭합니다.

HealthChecksReport.json 파일은 Cisco ISE 구축의 자세한 상태 정보와 함께 로컬 시스템에 저장됩니다.

상태 확인이 트리거된 후 상태는 다음 3시간 동안 **Health Check(**상태 확인**)** 창에 유지됩니다. **Health Checks(**상태 확인**)** 창이 새로 고쳐지거나 만료될 때까지 상태 확인을 실행할 수 없습니다.

네트워크 권한 프레임워크 이벤트 플로우 프로세스

NPF(Network Privilege Framework) 인증 및 권한 부여 이벤트 플로우에서는 다음 표에서 설명하는 프로세스가 적용됩니다.

프로세스 단계	설명
1	NAD(Network Access Device)는 일반 권한 부여 또는 플렉스 권한 부여를 수행합니다.
2	웹 권한 부여를 통해 알 수 없는 에이전트없는 ID가 프로파일링됩니다.
3	RADIUS 서버가 ID를 인증하고 권한을 부여합니다.
4	포트에서 ID에 대해 권한 부여가 프로비저닝됩니다.

프로세스 단계	설명
5	권한이 부여되지 않은 엔드포인트 트래픽이 삭제됩니다.

모니터링 및 문제 해결 기능에 대한 사용자 역할 및 권한

모니터링 및 문제 해결 기능은 기본 사용자 역할과 연결됩니다. 수행할 수 있는 작업은 할당된 사용자 역할과 직접적으로 관련됩니다.

각 사용자 역할에 대해 설정된 권한 및 제한에 대한 자세한 내용은 *Cisco ISE* 관리자 가이드의 "Cisco ISE 관리 가이드: 개요" 장에서 "Cisco ISE 관리자 그룹" 섹션을 참고하십시오.

참고 Cisco TAC의 감독 없이 루트 쉘(shell)을 사용하여 Cisco ISE에 액세스하는 것은 지원되지 않으며 Cisco는 그로 인해 발생할 수 있는 서비스 중단에 대해 책임을 지지 않습니다.

모니터링 데이터베이스에 저장된 데이터

Cisco ISE 모니터링 서비스는 특수 모니터링 데이터베이스에 데이터를 수집하고 저장합니다. 네트워크 기능을 모니터링하는 데 사용되는 데이터 비율과 양에 따라 모니터링 전용 노드가 필요할 수 있습니다. Cisco ISE 네트워크가 정책 서비스 노드 또는 네트워크 디바이스에서 많은 양의 로깅 데이터를 수집하는 경우 모니터링 전용 Cisco ISE 노드를 사용하는 것이 좋습니다.

모니터링 데이터베이스에 저장된 정보를 관리하려면 데이터베이스에 대한 전체 백업과 증분 백업을 수행합니다. 여기에는 원치 않는 데이터를 비우기한 다음 데이터베이스를 복구하는 과정도 포함됩니다.

Cisco ISE 텔레메트리

텔레메트리는 네트워크의 시스템 및 디바이스를 모니터링하여 제품 사용 방식에 대한 피드백을 Cisco에 제공합니다. Cisco는 이 정보를 사용하여 제품을 개선합니다.

텔레메트리는 기본적으로 활성화됩니다. 이 기능을 비활성화하려면,

1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Network Success Diagnostics(**네트워크 성공 진단**)** > **Telemetry(**텔레메트리**)**
2. **Enable Telemetry(**텔레메트리 비활성화**)** 확인란을 선택 취소하면 텔레메트리가 비활성화됩니다.

   - **Cisco** 계정: 텔레메트리에서 이메일을 받을 수 있도록 Cisco 계정을 입력합니다. 또한 사용자에게 영향을 미칠 수 있는 심각한 문제를 발견할 경우 이 ID를 사용하여 연락을 취할 수도 있습니다.

- 전송 게이트웨이: Cisco ISE와 Cisco의 외부 텔레메트리 서버 간에 프록시를 사용하여 추가 보안을 제공할 수 있습니다. 이 경우 해당 확인란을 선택하고 프록시 서버의 FQDN을 입력합니다. 텔레메트리에는 프록시가 필요하지 않습니다.

  Cisco는 전송 게이트웨이용 소프트웨어를 제공합니다. Cisco.com에서 다운로드할 수 있습니다. 이 소프트웨어는 Linux 서버에서 실행됩니다. RHEL 서버에서 전송 게이트웨이 소프트웨어를 구축하는 방법에 대한 자세한 내용은 Smart Call Home Deployment Guide를 참조하십시오. 이 Cisco 소프트웨어를 사용하는 경우 URL 값은 **<FQDN of proxyserver>/Transportgateway/services/DeviceRequestHandler**입니다. 이 게이트웨이를 사용하여 스마트 라이선싱 서버에 연결할 수도 있습니다. 전송 게이트웨이 버전 3.5부터는 포트를 변경할 수 없지만 FQDN 대신 IP 주소를 입력할 수 있습니다.

텔레메트리가 수집하는 정보

텔레메트리는 Cisco에 다음과 같은 정보를 전송합니다.

노드:

각 **PAN(Policy Administration Node)**의 경우

- 현재 포스처 엔드포인트 수
- 현재 pxGrid 클라이언트 수
- 현재 MDM에서 관리하는 엔드포인트 수
- 현재 게스트 사용자 수
- 해당 텔레메트리 기록의 시작 및 종료 날짜
- FIPS 상태

각 **PSN(Policy Service Node)**의 경우

- 프로파일러 프로브 수
- 노드 서비스 유형
- 사용된 패시브 ID

모든 노드의 경우

- 총 및 활성 NAD
- CPU 코어 수
- VM 지원 디스크 공간
- VM 메모리 및 CPU 설정
- 시스템 이름
- 일련 번호

- VID 및 PID
- 업타임
- 마지막 CLI 로그인

MnT 노드 수

pxGrid 노드 수

라이선스

- 라이선스 만료 여부
- 사용 가능한 Cisco ISE Essentials 라이선스 수, 사용된 최대 수
- 사용 가능한 Cisco ISE Advantage 라이선스 수, 사용된 최대 수
- 사용 가능한 Cisco ISE Premium 라이선스 수, 사용된 최대 수
- 소형, 중형 및 대형 VM 라이선스 수
- 평가판 라이선스 사용 여부
- 스마트 어카운트 이름
- TACACS 디바이스 수
- 만료 날짜, 남은 일수, 라이선스 기간
- 서비스 유형, 기본 및 보조 UDI

포스처

- 비활성 정책 수
- 마지막 포스처 피드 업데이트
- 활성 정책 수
- 포스처 피드 업데이트

게스트 사용자

- 해당 날짜에 인증된 최대 게스트 수
- 해당 날짜의 최대 활성 게스트 수
- 해당 날짜의 최대 BYOD 사용자 수
- 인증된 게스트의 외부 ID 정보

NAD(Network Access Devices)

- 권한 부여: 활성화된 ACL, VLAN, 정책 규모
- NDG 맵 및 NAD 계층 구조

- 인증:
  - RADIUS, RSA ID, LDAP, ODBC 및 Active Directory ID 저장소 수
  - 관리자가 아닌 로컬 사용자 수
  - NDG 맵 및 NAD 맵
  - 정책 라인 수

권한 부여, 활성 VLAN, 정책 수, 활성화된 ACL 수:

- 상태, VID, PT
- 평균 로드, 메모리 사용률
- PAP, MnT, pxGrid 및 PIC 노드 수
- 이름, 프로파일 이름, 프로파일 ID

NAD 프로파일

각 NAD 프로파일:

- 이름 및 ID
- Cisco 디바이스
- TACACS 지원
- RADIUS 지원
- TrustSec 지원
- 기본 프로파일

프로파일러

- 마지막 피드 업데이트 날짜
- 자동 업데이트 활성화 여부
- 프로파일링된 엔드포인트, 엔드포인트 유형, 알 수 없는 엔드포인트, 알 수 없는 백분율 및 총 엔드포인트 수
- 맞춤형 프로파일 수
- 일련 번호, 범위, 엔드포인트 유형, 맞춤형 프로파일

MDM(Mobile Device Management)

- MDM 노드 목록
- 날짜 범위의 경우 현재 MDM 엔드포인트 수, 현재 게스트 사용자 수, 현재 포스처 사용자 수
- pxGrid 클라이언트 수

- 노드 수

Cisco ISE 프로세스를 모니터링하는 SNMP 트랩

Cisco ISE의 일반 SNMP 트랩

SNMP 트랩을 사용하면 Cisco ISE의 상태를 모니터링할 수 있습니다. Cisco ISE 서버에 액세스하지 않고 Cisco ISE를 모니터링하려는 경우 Cisco ISE에서 MIB 브라우저를 SNMP 호스트로 구성할 수 있습니다. 그런 다음 MIB 브라우저에서 Cisco ISE의 상태를 모니터링할 수 있습니다.

snmp-server host 및 **snmp-server trap** 명령에 대한 자세한 내용은 Cisco Identity Services Engine CLI 참조 가이드를 참고하십시오.

Cisco ISE는 SNMPv1, SNMPv2c 및 SNMPv3을 지원합니다.

CLI에서 SNMP 호스트를 구성하는 경우 Cisco ISE는 다음과 같은 일반 시스템 트랩을 전송합니다.

- Cold start: 디바이스를 재부팅할 때.
- Linkup: 이더넷 인터페이스가 작동중일 때.
- Linkdown: 이더넷 인터페이스가 중단되어 있을 때.
- Authentication failure: 커뮤니티 문자열이 일치하지 않을 때.

다음 표에는 Cisco ISE에서 기본적으로 생성되는 일반 SNMP 트랩이 나와 있습니다.

OID	설명	트랩 예
.1.3.6.1.4.1.8072.4.0.3 \n NET-SNMP-AGENT-MIB::nsNotifyRestart	에이전트가 재시작되었음을 나타냅니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.4.1.8072.4.0.2 \n NET-SNMP-AGENT-MIB::nsNotifyShutdown	에이전트가 종료되는 중임을 나타냅니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix

OID	설명	트랩 예
.1.3.6.1.6.3.1.1.5.4 \n IF-MIB::linkUp	에이전트 역할을 수행하는 SNMP 엔티티가 통신 링크 중 하나에 대한 ifOperStatus 개체가 다운 상태를 유지하고 (notPresent 상태가 아닌) 다른 상태로 전환된 것을 탐지했음을 나타냅니다. 이 다른 상태는 ifOperStatus의 포함된 값으로 표시됩니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.12 = INTEGER: 12 IF-MIB::ifAdminStatus.12 = INTEGER: up(1) IF-MIB::ifOperStatus.12 = INTEGER: up(1) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

OID	설명	트랩 예
.1.3.6.1.6.3.1.1.5.3 \n IF-MIB::linkDown	에이전트 역할을 수행하는 SNMP 엔티티가 통신 링크 중 하나에 대한 ifOperStatus 개체가 (notPresent 상태가 아닌) 다른 상태에서 다운 상태로 전환되려는 것을 탐지했음을 나타냅니다. 이 다른 상태는 ifOperStatus의 포함된 값으로 표시됩니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifAdminStatus.5 = INTEGER: up(1) IF-MIB::ifOperStatus.5 = INTEGER: down(2) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.1 \n SNMPv2-MIB::coldStart	알림 생성자 애플리케이션을 지원하는 SNMP 엔티티가 자체적으로 다시 초기화되고 해당 컨피그레이션이 변경되었을 수 있음을 나타냅니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8) 0:00:00.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

Cisco ISE의 프로세스 모니터링 SNMP 트랩

Cisco ISE CLI에서 SNMP 호스트를 구성하는 경우 Cisco ISE에서는 Cisco ISE 프로세스 상태에 대한 hrSWRunName 트랩을 SNMP 관리자로 전송할 수 있습니다. Cisco ISE는 cron 작업을 사용하여 이러한 트랩을 트리거합니다. 크론 작업은 Monit에서 Cisco ISE 프로세스 상태를 검색합니다. CLI에서 **SNMP** 서버 호스트 명령을 구성하고 나면 cron 작업이 5분마다 실행되어 Cisco ISE를 모니터링합니다.

참고 관리자가 ISE 프로세스를 수동으로 중지하면 해당 프로세스에 대한 모니터링도 중지되며 SNMP 관리자로 트랩이 전송되지 않습니다. 프로세스가 실수로 종료되어 자동으로 복구되지 않는 경우에만 프로세스 중지 SNMP 트랩이 SNMP 관리자에게 전송됩니다.

다음은 Cisco ISE의 프로세스 모니터링 SNMP 트랩에 대한 전체 목록입니다.

OID	설명	트랩 예
.1.3.6.1.2.1.25.4.2.1.2 \n HOST-RESOURCES-MIB::hrSWRunName	제조업체, 수정 버전 및 일반적으로 알려진 이름을 포함하여 실행중인 소프트웨어에 대한 텍스트 설명입니다. 이 소프트웨어가 로컬로 설치된 경우 해당 hrSWInstalledName에 사용된 것과 동일한 문자열이어야 합니다. 고려되는 서비스는 app-server, rsyslog, redis-server, ad-connector, mnt-collector, mnt-processor, ca-server est-server 및 elasticsearch입니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (63692139) 7 days, 8:55:21.39 SNMPv2-MIB::snmpTrapOID.0 = OID: HOSTRESOURCES- MIB::hrSWRunName HOSTRESOURCES- MIB::hrSWRunName = STRING: "redis-server:Running"

Cisco ISE는 구성된 SNMP 서버로 다음 상태에 대한 트랩을 전송합니다.

- Process Start(프로세스 시작)(monitored[모니터링됨] 상태)
- Process Stop(프로세스 중지)(not monitored[모니터링되지 않음] 상태)
- Execution Failed(실행 장애): 프로세스 상태가 "Monitored(모니터링됨)"에서 "Execution Failed(실행 장애)"로 변경되면 트랩이 전송됩니다.

- Does not exists(없음): 프로세스 상태가 "Monitored(모니터링됨)"에서 "Does Not Exists(없음)"로 변경되면 트랩이 전송됩니다.

SNMP 서버에서는 각 객체에 대해 고유 객체 ID(OID)가 생성되며 특정 값이 이 OID에 할당됩니다. SNMP 서버의 OID 값으로 객체를 찾을 수 있습니다. 실행 중인 트랩의 OID 값은 *"running(실행 중)"*이며 not monitored(모니터링되지 않음), does not exist(없음) 및 execution failed(실행 장애) 트랩의 OID 값은 *"stopped(중지됨)"*입니다.

Cisco ISE는 HOST-RESOURCES MIB에 속하는 hrSWRunName의 OID를 사용하여 트랩을 전송하고 이 OID 값을 < *PROCESS NAME* > - <*PROCESS STATUS* >로, 예를 들면 "실행 시간 - 실행"으로 설정합니다.

Cisco ISE가 SNMP 서버로 SNMP 트랩을 보내지 않도록 하려면 Cisco ISE CLI에서 SNMP 컨피그레이션을 제거합니다. 이 작업은 SNMP 관리자로부터의 SNMP 트랩 전송 및 폴링을 중지합니다.

Cisco ISE의 디스크 사용률 **SNMP** 트랩

Cisco ISE 파티션이 그 디스크 사용률 임계값에 도달하고 구성된 여유 공간이 모두 사용되면 디스크 사용률 트랩이 전송됩니다.

다음은 Cisco ISE에서 구성할 수 있는 디스크 사용 SNMP 트랩의 전체 목록입니다.

OID	설명	트랩 예
.1.3.6.1.4.1.2021.9.1.9 \n UCD-SNMP-MIB::dskPercent	디스크에서 사용된 공간의 백분율.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198297) 13 days, 16:19:42.97 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPercent UCD-SNMP-MIB::dskPercent = INTEGER: 13
.1.3.6.1.4.1.2021.9.1.2 \n UCD-SNMP-MIB::dskPath	디스크가 마운트된 경로. dskPath는 ISE admin 명령의 출력에서 모든 마운트 포인트에 대한 트랩을 전송할 수 있습니다**show disks**.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198304) 13 days, 16:19:43.04 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPath UCD-SNMP-MIB::dskPath = STRING: /opt

Cisco ISE 경보

경보는 네트워크의 위험 조건에 대해 알리며 경보 dashlet에 표시됩니다. 또한 데이터 제거 이벤트와 같은 시스템 활동에 대한 정보도 제공합니다. 시스템 활동에 대한 알림을 어떤 식으로 받으려는지 구성할 수 있습니다. 아니면 경보를 완전히 비활성화할 수도 있습니다. 특정 경보에 대한 임계값도 구성할 수 있습니다.

대부분의 경보에는 일정이 연결되어 있지 않으며 이벤트가 발생한 직후에 경보가 전송됩니다. 특정한 시점에 보존되는 경보 수는 최신 경보를 기준으로 15,000개입니다.

이벤트가 다시 발생하는 경우 약 1시간 동안 동일한 경보가 표시되지 않습니다. 이벤트가 다시 발생하는 기간 동안에는 트리거에 따라 경보가 다시 표시되려면 약 1시간이 소요될 수 있습니다.

다음 표에는 모든 Cisco ISE 경보, 설명 및 해당 해결 방법이 나와 있습니다.

표 ***180: Cisco ISE*** 경보

경보 이름	경보 설명	경보 해결 방법
관리 및 운영 관리 감사		
구축 업그레이드 장애	ISE 노드에서 업그레이드에 장애가 발생했습니다.	장애가 발생한 노드의 ADE.log에서 업그레이드 실패 이유와 정정 작업을 확인해 주십시오.
업그레이드 번들 다운로드 장애	ISE 노드에서 업그레이드 번들 다운로드에 장애가 발생했습니다.	장애가 발생한 노드의 ADE.log에서 업그레이드 실패 이유와 정정 작업을 확인해 주십시오.
SXP 연결 장애	SXP 연결에 장애가 발생했습니다.	SXP 서비스가 실행 중인지 확인해 주십시오. 피어의 호환성을 확인해 주십시오.
모든 디바이스에 적용된 Cisco 프로파일	네트워크 디바이스 프로파일은 MAB, Dot1X, CoA, 웹 리디렉션 등 네트워크 액세스 디바이스의 기능을 정의합니다. ISE 2.0 업그레이드의 일부분으로 기본 Cisco 네트워크 디바이스 프로파일이 모든 네트워크 디바이스에 적용되었습니다.	적절한 프로파일을 할당하려면 Cisco 제품이 아닌 네트워크 디바이스의 컨피그레이션을 편집하는 것이 좋습니다.
CRL에서 취소된 인증서를 발견하여 보안 LDAP 연결이 다시 연결됨	CRL 확인 결과 LDAP 연결에 사용된 인증서가 취소되었습니다.	CRL 컨피그레이션이 유효한지 확인해 주십시오. LDAP 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 LDAP 서버에 설치해 주십시오.
OCSP에서 취소된 인증서를 발견하여 보안 LDAP 연결이 다시 연결됨	OCSP 확인 결과 LDAP 연결에 사용된 인증서가 취소되었습니다.	OCSP 컨피그레이션이 유효한지 확인해 주십시오. LDAP 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 LDAP 서버에 설치해 주십시오.

경보 이름	경보 설명	경보 해결 방법
CRL에서 취소된 인증서를 발견하여 보안 시스템 로그 연결이 다시 연결됨	CRL 확인 결과 시스템 로그 연결에 사용된 인증서가 취소되었습니다.	CRL 컨피그레이션이 유효한지 확인해 주십시오. 시스템 로그 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 시스템 로그 서버에 설치해 주십시오.
OCSP에서 취소된 인증서를 발견하여 보안 시스템 로그 연결이 다시 연결됨	OCSP 확인 결과 시스템 로그 연결에 사용된 인증서가 취소되었습니다.	OCSP 컨피그레이션이 유효한지 확인해 주십시오. 시스템 로그 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 시스템 로그 서버에 설치해 주십시오.
관리자 계정 잠금/비활성화	비밀번호 만료 또는 잘못된 로그인 시도로 인해 관리자 계정이 잠기거나 비활성화되었습니다. 자세한 내용은 관리자 비밀번호 정책을 참고해 주십시오.	관리자 비밀번호는 다른 관리자가 GUI 또는 CLI를 사용하여 재설정할 수 있습니다.
ERS에서 더 이상 사용되지 않는 URL을 식별함	ERS에서 더 이상 사용되지 않는 URL을 식별함	요청 URL이 더 이상 사용되지 않으므로 해당 URL을 사용하지 않는 것이 좋습니다.
ERS에서 오래된 URL을 식별함	ERS에서 오래된 URL을 식별함	요청한 URL이 오래되었으므로 최신 URL을 사용하는 것이 좋습니다. 이 URL는 향후 릴리스에서 제거되지 않습니다.
ERS 요청 content-type 헤더가 오래됨	ERS 요청 content-type 헤더가 오래되었습니다.	요청 content-type 헤더에 나와 있는 요청 리소스 버전이 오래되었습니다. 이는 리소스 스키마가 수정되었음을 의미합니다. 하나 이상의 속성이 추가되었거나 제거되었을 수 있습니다. 오래된 스키마 문제를 해결하기 위해 ERS 엔진은 기본값을 사용합니다.
ERS XML 입력에서 XSS 또는 삽입 공격이 의심됨	ERS XML 입력에서 XSS 또는 삽입 공격이 의심됩니다.	xml 입력을 검토하십시오.

경보 이름	경보 설명	경보 해결 방법
백업 실패	ISE 백업 작업이 실패했습니다.	Cisco ISE와 저장소 사이의 네트워크 연결을 확인해 주십시오. 다음 사항을 확인해 주십시오. • 저장소에 사용되는 자격 증명이 올바릅니다. • 저장소에 충분한 디스크 공간이 있습니다. • 저장소 사용자에게 쓰기 권한이 있습니다.
CA 서버 작동 중지됨	CA 서버가 작동 중지되었습니다.	CA 서비스가 CA 서버에서 작동되어 실행 중인지 확인해 주십시오.
CA 서버 작동	CA 서버가 작동합니다.	관리자에게 CA 서버가 작동하고 있음을 알리는 알림입니다.
인증서 만료	이 인증서가 곧 만료됩니다. 인증서가 만료되면 Cisco ISE가 클라이언트와의 보안 통신을 설정하지 못할 수 있습니다.	인증서를 바꾸십시오. 신뢰 인증서의 경우 발급 CA(Certificate Authority)에 문의해 주십시오. CA 서명 로컬 인증서의 경우 CSR을 생성하고 CA에 새 인증서를 생성해 달라고 요청해 주십시오. 자체 서명된 로컬 인증서의 경우 Cisco ISE를 사용하여 만료 날짜를 연장해 주십시오. 더 이상 사용되지 않는 경우 인증서를 삭제할 수 있습니다.
인증서 취소됨	관리자가 내부 CA에 의해 엔드포인트로 발급된 인증서를 취소했습니다.	처음부터 새 인증서로 프로비저닝될 때까지 BYOD 흐름을 진행해 주십시오.
인증서 프로비저닝 초기화 오류	인증서 프로비저닝 초기화에 실패했습니다.	주체에서 동일한 CN(CommonName) 속성 값을 가진 여러 인증서가 발견되었습니다. 인증서 체인을 작성할 수 없습니다. SCEP 서버의 인증서를 비롯하여 시스템의 모든 인증서를 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
인증서 복제 실패	보조 노드에 대한 인증서 복제에 실패했습니다.	보조 노드의 인증서가 유효하지 않거나 다른 영구적인 오류 조건이 있습니다. 보조 노드에 기존의 충돌하는 인증서가 있는지 확인해 주십시오. 충돌하는 인증서가 있는 경우, 보조 노드에서 기존 인증서를 삭제하고 기본 노드에서 새 인증서를 내보내고 인증서를 삭제한 다음 가져와 복제를 다시 시도하도록 해 주십시오.
인증서 복제 일시적 실패	보조 노드에 대한 인증서 복제가 일시적으로 실패했습니다.	네트워크 중단과 같은 일시적 상태로 인해 인증서가 보조 노드로 복제되지 않았습니다. 복제가 성공할 때까지 재시도됩니다.
인증서 만료됨	이 인증서가 만료되었습니다. Cisco ISE가 클라이언트와의 보안 통신을 설정하지 못할 수 있습니다. 노드 간 통신에도 영향을 미칠 수 있습니다.	인증서를 바꾸십시오. 신뢰 인증서의 경우 발급 CA(Certificate Authority)에 문의해 주십시오. CA 서명 로컬 인증서의 경우 CSR을 생성하고 CA에 새 인증서를 생성해 달라고 요청해 주십시오. 자체 서명된 로컬 인증서의 경우 Cisco ISE를 사용하여 만료 날짜를 연장해 주십시오. 더 이상 사용되지 않는 경우 인증서를 삭제할 수 있습니다.
인증서 요청 전달 실패	인증서 요청 전달에 실패했습니다.	들어오는 인증 요청이 발신자의 속성과 일치하는지 확인해 주십시오.
컨피그레이션 변경됨	Cisco ISE 컨피그레이션이 업데이트되었습니다. 이 경보는 사용자 및 엔드포인트에서 컨피그레이션이 변경된 경우에는 트리거되지 않습니다.	컨피그레이션 변경이 예상되는지 확인해 주십시오.
CRL 검색 실패	서버에서 CRL을 검색할 수 없습니다. 이는 지정된 CRL을 사용할 수 없는 경우에 발생할 수 있습니다.	다운로드 URL이 올바르고 서비스에 사용할 수 있는지 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
DNS 확인 실패	노드에서 DNS 확인에 실패했습니다.	**ip name-server** 명령으로 구성한 DNS 서버에 연결할 수 있는지 확인해 주십시오. **DNS Resolution failed for CNAME <hostname of the node>** 에 해당하는 경보를 받는 경우 각 ISE 노드의 A 기록와 함께 CNAME RR을 생성해야 합니다.
펌웨어 업데이트 필요	이 호스트에서 펌웨어를 업데이트해야 합니다.	펌웨어 업데이트를 받으려면 Cisco TAC에 문의하십시오.
불충분한 가상 머신 리소스	이 호스트에서 CPU, RAM, 디스크 공간 또는 IOPS와 같은 VM(Virtual Machine) 리소스가 충분하지 않습니다.	Cisco ISE 하드웨어 설치 설명서에 명시된 VM 호스트에 대한 최소 요건을 확인해 주십시오.
NTP 서비스 실패	이 노드에서 NTP 서비스 작동이 중지되었습니다.	이는 NTP 서버와 Cisco ISE 노드 사이의 시간 차이가 크기 때문에 (1,000초 이상) 발생할 수 있습니다. NTP 서버가 적절히 작동 중인지 확인하고 **ntp server <servername>** CLI 명령을 사용하여 NTP 서비스를 다시 시작하여 시간 격차 문제를 해결해 주십시오.
NTP 동기화 실패	이 노드에 구성된 모든 NTP 서버에 연결할 수 없습니다.	문제를 해결하려면 CLI에서 **show ntp** 명령을 실행해 주십시오. Cisco ISE에서 NTP 서버에 연결할 수 있는지 확인해 주십시오. NTP 인증이 구성된 경우 키 ID와 값이 서버의 값과 일치하는지 확인해 주십시오.
예약된 컨피그레이션 백업 없음	Cisco ISE 컨피그레이션 백업이 예약되지 않았습니다.	컨피그레이션 백업에 대한 일정을 생성해 주십시오.
작업 DB 제거 실패	작업 데이터베이스에서 오래된 데이터를 제거할 수 없습니다. 이는 MnT 노드가 사용 중인 경우 발생합니다.	데이터 비우기 감사 보고서에서 used_space가 threshold_space보다 작은지 확인해 주십시오. CLI를 사용하여 MnT 노드에 로그인하고 제거 작업을 수동으로 수행해 주십시오.

경보 이름	경보 설명	경보 해결 방법
프로파일러 SNMP 요청 실패	SNMP 요청 시간이 초과되었거나 SNMP 커뮤니티 또는 사용자 인증 데이터가 잘못되었는지 확인해 주십시오.	SNMP가 NAD에서 실행되고 있는지 확인하고 Cisco ISE의 SNMP 컨피그레이션이 NAD와 일치하는지 확인해 주십시오.
복제 실패	보조 노드에서 복제된 메시지를 사용하지 못했습니다.	Cisco ISE GUI에 로그인하고 구축 페이지에서 수동 동기화를 수행해 주십시오. 영향을 받는 Cisco ISE 노드를 등록 취소했다가 다시 등록해 주십시오.
복원 실패	Cisco ISE 복원 작업에 실패했습니다.	Cisco ISE와 저장소 사이의 네트워크 연결을 확인해주십시오. 저장소에 사용된 자격 증명이 올바른지 확인해 주십시오. 백업 파일이 손상되지 않았는지 확인해 주십시오. CLI에서 **reset-config** 명령을 실행하고 마지막으로 알려진 안전한 백업을 복원해 주십시오.
패치 실패	서버에서 패치 프로세스가 실패했습니다.	서버에서 패치 프로세스를 다시 실행해 주십시오.
패치 성공	서버에서 패치 프로세스가 성공했습니다.	-
외부 MDM 서버 API 버전 불일치	외부 MDM 서버 API 버전이 Cisco ISE에서 구성한 버전과 일치하지 않습니다.	MDM 서버 API 버전이 Cisco ISE에서 구성한 버전과 일치하는지 확인해 주십시오. 필요한 경우 Cisco ISE MDM 서버 컨피그레이션을 업데이트해 주십시오.
외부 MDM 서버 연결 실패	외부 MDM 서버에 대한 연결에 실패했습니다.	MDM 서버가 작동하며 Cisco ISE-MDM API 서비스가 MDM 서버에서 실행되고 있는지 확인해 주십시오.
외부 MDM 서버 응답 오류	외부 MDM 서버 응답 오류입니다.	MDM 서버에서 Cisco ISE-MDM API 서비스가 제대로 실행되고 있는지 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
복제 중지됨	ISE 노드가 PAN에서 컨피그레이션 데이터를 복제할 수 없습니다.	Cisco ISE GUI에 로그인하여 구축 페이지에서 수동 동기화를 수행하거나, 필수 필드를 사용하여 영향을 받는 ISE 노드를 등록 취소했다가 다시 등록해 주십시오.
엔드포인트 인증서 만료됨	엔드포인트 인증서가 일별 예약 작업에서 만료된 상태로 표시되었습니다.	새 엔드포인트 인증서를 받으려면 엔드포인트 디바이스를 다시 등록해 주십시오.
엔드포인트 인증서 제거됨	일별 예약 작업에서 만료된 엔드포인트 인증서가 제거되었습니다.	필요 조치가 없습니다. 이는 관리자가 시작한 정리 작업입니다.
엔드포인트 제거 활동	엔드포인트에서 지난 24시간 동안의 활동을 제거합니다. 이 경보는 야간에 트리거됩니다.	**Operations(**작업**)** > **Reports(**보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **Endpoint Purge Activities(**엔드포인트 제거 활동**)**를 선택해 제거 활동을 검토해 주십시오.
느린 복제 오류	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.
느린 복제 정보	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.
느린 복제 경고	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.
PAN 자동 페일오버 - 페일오버 실패	보조 관리 노드로의 프로모션 요청이 실패했습니다.	추가 작업에 대해서는 경보 세부 정보를 참고해 주십시오.
PAN 자동 페일오버 - 페일오버 트리거됨	기본 역할에 대한 보조 관리 노드의 페일오버가 성공적으로 트리거되었습니다.	보조 PAN 프로모션이 완료될 때까지 기다렸다가 이전의 기본 PAN을 작동해 주십시오.
PAN 자동 페일오버 - 상태 검사 비활성	PAN이 지정된 모니터링 노드로부터 상태 검사 모니터링 요청을 받지 못했습니다.	보고된 모니터링 노드가 작동 중지되었거나 동기화가 중단되었는지 확인하고 필요한 경우 수동 동기화를 트리거해 주십시오.

경보 이름	경보 설명	경보 해결 방법
PAN 자동 페일오버 - 유효하지 않은 상태 검사	자동 페일오버에 대해 유효하지 않은 상태 검사 모니터링 요청이 수신되었습니다.	상태 검사 모니터링 노드의 동기화가 중단되었는지 확인하고 필요한 경우 수동 동기화를 트리거해 주십시오.
PAN 자동 페일오버 - 기본 관리 노드 작동 중지	기본 관리 노드가 작동 중지되었거나 모니터링 노드에서 연결할 수 없습니다.	PAN을 작동시키거나 페일오버가 발생할 때까지 기다리십시오.
PAN 자동 페일오버 - 페일오버 시도 거부됨	보조 관리 노드가 상태 검사 모니터 노드에 의해 생성된 프로모션 요청을 거부했습니다.	추가 작업에 대해서는 경보 세부정보를 참고해 주십시오.
EST 서비스 중단	EST 서비스가 중단되었습니다.	CA 및 EST 서비스가 실행 중이고 인증서 서비스 엔드포인트 하위 CA 인증서 체인이 완전한지 확인하십시오.
EST 서비스 작동 중	EST 서비스가 작동 중입니다.	관리자에게 EST 서비스가 작동하고 있음을 알리는 알림입니다.
Smart Call Home 통신 실패	Smart Call Home 메시지가 성공적으로 전송되지 않았습니다.	Cisco ISE와 Cisco 시스템 사이의 네트워크 연결을 확인해 주십시오.
원격 분석 통신 장애	원격 분석 메시지가 성공적으로 전송되지 않았습니다.	Cisco ISE와 Cisco 시스템 사이의 네트워크 연결을 확인해 주십시오.
어댑터에 연결할 수 없음	Cisco ISE가 어댑터에 연결할 수 없습니다.	어댑터 로그를 확인해 장애 관련 세부정보를 확인하십시오.
어댑터 오류	어댑터에 오류가 발생했습니다.	경보 설명을 확인하십시오.
어댑터 연결 실패	어댑터가 소스 서버에 연결할 수 없습니다.	소스 서버에 연결할 수 있는지 확인하십시오.
오류 때문에 어댑터 중지됨	어댑터에 오류가 발생하여 바람직한 상태에 있지 않습니다.	어댑터 구성이 올바르고 소스 서버에 연결할 수 있는지 확인합니다. 어댑터 로그를 참조해 오류 관련 세부정보를 확인하십시오.
서비스 구성 요소 오류	서비스 구성 요소에 오류가 발생했습니다.	경보 설명을 확인하십시오.
서비스 구성 요소 정보	서비스 구성 요소가 알림을 전송했습니다.	없음

경보 이름	경보 설명	경보 해결 방법
ISE 서비스		
과도한 TACACS 인증 시도	ISE 정책 서비스 노드에서 예상되는 TACACS 인증 비율보다 더 높은 인증 시도가 발생했습니다.	• 네트워크 디바이스에서 재인증 타이머를 확인해 주십시오. • ISE 인프라의 네트워크 연결을 확인해 주십시오.
과도한 TACACS 인증 시도 장애	ISE 정책 서비스 노드에서 장애가 발생한 TACACS 인증의 예상 비율보다 더 높은 인증 시도 장애가 발생했습니다.	• 인증 단계를 확인하여 근본 원인을 파악해 주십시오. • ISE/NAD 컨피그레이션에서 ID 및 암호 불일치를 확인해 주십시오.
MSE 위치 서버에 다시 액세스할 수 있음	MSE 위치 서버에 다시 액세스할 수 있습니다.	없음
MSE 위치 서버에 액세스할 수 없습니다.	MSE 위치 서버가 액세스할 수 없거나 다운된 상태입니다.	MSE 위치 서버가 작동 및 실행 중이며 ISE 노드에서 액세스 가능한지 확인해 주십시오.
AD Connector를 다시 시작해야 함	AD Connector가 예기치 않게 중지되었으므로 다시 시작해야 합니다.	이 문제가 계속되면 Cisco TAC에 지원을 요청해 주십시오.
Active Directory 포리스트를 사용할 수 없음	Active Directory 포리스트 글로벌 카탈로그를 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 속성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
인증 도메인을 사용할 수 없음	인증 도메인을 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 속성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
ISE 인증 비활성	Cisco ISE 정책 서비스 노드가 네트워크 디바이스에서 인증 요청을 받지 않습니다.	• ISE/NAD 컨피그레이션을 확인해 주십시오. • ISE/NAD 인프라의 네트워크 연결을 확인해 주십시오.
ID 매핑. 인증 비활성	ID 매핑 서비스에서 최근 15분간 사용자 인증 이벤트를 수집하지 않았습니다.	사용자 인증이 필요한 시점이라면(예: 근무 시간) Active Directory 도메인 컨트롤러에 대한 연결을 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
CoA 실패	네트워크 디바이스가 Cisco ISE 정책 서비스 노드에서 실행한 CoA(Change of Authorization) 요청을 거부했습니다.	네트워크 디바이스가 Cisco ISE에서 CoA를 허용하도록 구성되었는지 확인해 주십시오. 유효한 세션에 대해 CoA가 실행되었는지 확인해 주십시오.
구성된 네임서버 작동 중지됨	구성된 네임서버가 작동 중지되었거나 사용 불가능합니다.	DNS 컨피그레이션 및 네트워크 연결을 확인해 주십시오.
신청자가 응답을 중지함	Cisco ISE가 120초 전에 클라이언트에 마지막 메시지를 보냈지만 클라이언트로부터 응답이 없습니다.	• 신청자가 Cisco ISE와 완전한 EAP 대화를 수행하도록 올바르게 구성되었는지 확인해 주십시오. • NAS가 신청자와 EAP 메시지를 전송하도록 올바르게 구성되었는지 확인해 주십시오. • EAP 대화를 위한 신청자 또는 NAS의 시간 제한이 짧지 않은지 확인해 주십시오.
과도한 인증 시도	Cisco ISE 정책 서비스 노드에서 예상되는 인증 비율보다 더 높은 인증 시도가 발생했습니다.	네트워크 디바이스에서 재인증 타이머를 확인해 주십시오. Cisco ISE 인프라의 네트워크 연결을 확인해 주십시오. 임계값을 충족하는 경우 과도한 인증 시도 및 과도한 실패 시도 경보가 트리거됩니다. 설명 열 옆에 표시되는 숫자는 최근 15분간 Cisco ISE에 대해 인증이 완료되었거나 실패한 총 인증 수입니다.

경보 이름	경보 설명	경보 해결 방법
과도한 실패 시도	Cisco ISE 정책 서비스 노드에서 예상되는 실패한 인증 비율보다 더 높은 인증 시도가 발생했습니다.	인증 단계를 확인하여 근본 원인을 파악해 주십시오. Cisco ISE/NAD 컨피그레이션에서 ID 및 암호 불일치가 있는지 확인해 주십시오. 임계값을 충족하는 경우 과도한 인증 시도 및 과도한 실패 시도 경보가 트리거됩니다. 설명 열 옆에 표시되는 숫자는 최근 15분간 Cisco ISE에 대해 인증이 완료되었거나 실패한 총 인증 수입니다.
AD: 머신 TGT 새로 고침 실패	ISE 서버 TGT(Ticket Granting Ticket) 새로 고침에 실패했습니다. TGT는 AD 연결 및 서비스에 사용됩니다.	ISE 머신 계정이 있으며 유효한지 확인해 주십시오. 또한 가능한 클럭 오차, 복제, Kerberos 컨피그레이션 또는 네트워크 오류가 있는지 아니면 두 오류가 모두 있는지도 확인해 주십시오.
AD: ISE 계정 비밀번호 업데이트 실패	ISE 서버에서 AD 머신 계정 비밀번호를 업데이트하지 못했습니다.	ISE 머신 계정 비밀번호가 변경되지 않았는지, 그리고 머신 계정이 비활성화되었거나 제한되어 있지 않은지 확인해 주십시오. KDC에 대한 연결을 확인해 주십시오.
가입한 도메인 사용 불가능	가입한 도메인을 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 속성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
ID 저장소 사용 불가능	Cisco ISE 정책 서비스 노드를 구성한 ID 저장소에 연결할 수 없습니다.	Cisco ISE와 ID 저장소 사이의 네트워크 연결을 확인해 주십시오.
잘못 구성된 네트워크 디바이스 탐지	Cisco ISE가 NAS에서 너무 많은 RADIUS 계정 관리 정보를 탐지했습니다. 이 경보는 기본적으로 비활성화되어 있습니다. 이 경보를 활성화하려면 경보 활성화 및 구성을 참조하십시오.	NAS에서 너무 많은 중복 RADIUS 계정 관리 정보가 ISE로 전송되었습니다. 정확한 계정 관리 빈도로 NAS를 구성해 주십시오.

경보 이름	경보 설명	경보 해결 방법
잘못 구성된 신청자 탐지	Cisco ISE가 네트워크에서 잘못 구성된 신청자를 탐지했습니다. 이 경보는 기본적으로 비활성화되어 있습니다. 이 경보를 활성화하려면 경보 활성화 및 구성을 참조하십시오.	신청자의 컨피그레이션이 올바른지 확인해 주십시오.
계정 관리 시작 없음	Cisco ISE 정책 서비스 노드가 세션에 권한을 부여했지만 네트워크 디바이스로부터 계정 관리 시작을 받지 못했습니다.	네트워크 디바이스에 RADIUS 계정 관리가 구성되어 있는지 확인해 주십시오. 네트워크 디바이스 컨피그레이션에서 로컬 권한 부여를 확인해 주십시오.
알 수 없는 NAD	Cisco ISE 정책 서비스 노드가 Cisco ISE에 구성되어 있지 않은 네트워크 디바이스에서 인증 요청을 받았습니다.	네트워크 디바이스가 정식 요청인지 확인한 다음 컨피그레이션에 추가해 주십시오. 암호가 일치하는지 확인해 주십시오.
SGACL 삭제	SGACL(Secure Group Access) 삭제가 발생했습니다. 이는 SGACL 정책 위반으로 인해 Trustsec 지원 디바이스에서 패킷이 삭제되는 경우에 발생합니다.	RBACL 삭제 요약 보고서를 실행하고 SGACL 삭제를 발생시킨 소스를 검토합니다. CoA를 잘못된 소스에 실행하여 세션에 다시 권한을 부여하거나 세션 연결을 끊으십시오.
RADIUS 요청 삭제됨	NAD의 인증/계정 관리 요청이 자동으로 버려집니다. 이는 알 수 없는 NAD, 공유 암호 불일치 또는 RFC에 따른 유효하지 않은 패킷 콘텐츠로 인해 발생할 수 있습니다. 이 경보는 기본적으로 비활성화되어 있습니다. 이 경보를 활성화하려면 경보 활성화 및 구성을 참조하십시오.	Cisco ISE에서 NAD/AAA 클라이언트의 컨피그레이션이 유효한지 확인해 주십시오. NAD/AAA 클라이언트 및 Cisco ISE의 공유 암호가 일치하는지 확인해 주십시오. AAA 클라이언트 및 네트워크 디바이스에 하드웨어 문제 또는 RADIUS 호환성 문제가 없는지 확인해 주십시오. 또한 디바이스를 Cisco ISE에 연결하는 네트워크에 하드웨어 문제가 없는지 확인해 주십시오.
EAP 세션 할당 실패	EAP 세션 제한에 도달했으므로 RADIUS 요청이 삭제되었습니다. 이 상태는 너무 많은 병렬 EAP 인증 요청으로 인해 발생할 수 있습니다.	몇 초간 기다렸다가 새 EAP 세션에서 다른 RADIUS 요청을 호출해 주십시오. 계속 시스템 오버로드가 발생하는 경우 ISE 서버를 다시 시작해 주십시오.

경보 이름	경보 설명	경보 해결 방법
RADIUS 상황 할당 실패	시스템 오버로드로 인해 RADIUS 요청이 삭제되었습니다. 이 상태는 너무 많은 병렬 인증 요청으로 인해 발생할 수 있습니다.	몇 초간 기다렸다가 새 RADIUS 요청을 호출해 주십시오. 계속 시스템 오버로드가 발생하는 경우 ISE 서버를 다시 시작해 주십시오.
AD: ISE 머신 계정에 그룹을 가져오는 데 필요한 권한이 없습니다.	Cisco ISE 머신 계정에 그룹을 가져오는 데 필요한 권한이 없습니다.	Cisco ISE 머신 계정에 Active Directory에서 사용자 그룹을 가져올 권한이 있는지 확인합니다.
시스템 상태		
높은 디스크 I/O 사용률	Cisco ISE 시스템의 디스크 I/O사용률이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
높은 디스크 공간 사용률	Cisco ISE 시스템의 디스크 공간 사용률이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.

경보 이름	경보 설명	경보 해결 방법
높은 로드 평균	Cisco ISE 시스템의 로드 평균이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오. 기본 및 보조 MNT 노드의 오전 2시 타임 스탬프에 대해 높은 로드 평균 경보가 표시되는 경우, 해당 시간에 DBMS 통계가 실행되는 것 때문에 CPU 사용량이 높을 수 있습니다. DBMS 통계가 완료되면 CPU 사용량이 정상으로 돌아옵니다. 매주 일요일 오전 1시에 주간 유지 관리 작업으로 인해 높은 로드 평균 경보가 트리거됩니다. 이 유지 관리 작업은 1GB 이상의 공간을 차지하는 모든 인덱스를 재구축합니다. 이 경보는 무시해도 됩니다.
높은 메모리 사용률	Cisco ISE 시스템의 메모리 사용률이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
높은 작업 DB 사용률	Cisco ISE 모니터링 노드의 시스템 로그 데이터 볼륨이 예상보다 많습니다.	작업 데이터에 대한 컨피그레이션 제거 창을 확인하고 줄이십시오.
높은 인증 레이턴시	Cisco ISE 시스템의 인증 레이턴시가 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
상태 사용 불가능	모니터링 노드가 Cisco ISE 노드에서 상태를 받지 못했습니다.	Cisco ISE 노드가 준비되어 실행 중이며 모니터링 노드와 통신할 수 있는지 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
프로세스 작동 중지	Cisco ISE 프로세스 중 하나가 실행되고 있지 않습니다.	Cisco ISE 애플리케이션을 다시 시작해 주십시오.
프로파일러 큐 크기 제한에 도달함	ISE 프로파일러 큐 크기 제한에 도달했습니다. 큐 크기 제한에 도달한 후 수신된 이벤트는 삭제됩니다.	시스템에 충분한 리소스가 있는지 확인하고 엔드포인트 속성 필터이 활성화되어 있는지 확인해 주십시오.
OCSP 트랜잭션 임계값에 도달함	OCSP 트랜잭션 임계값에 도달했습니다. 이 경보는 내부 OCSP 서비스에서 많은 양의 트래픽이 발생하는 경우에 트리거됩니다.	시스템의 리소스가 충분한지 확인해 주십시오.
라이선싱		
라이선스가 곧 만료됨	Cisco ISE 노드에 설치된 라이선스가 만료될 예정입니다.	Cisco ISE의 라이선싱 창에서 라이선스 사용 현황을 확인해 주십시오.
라이선스 만료됨	Cisco ISE 노드에 설치된 라이선스가 만료되었습니다.	새 라이선스를 구입하려면 Cisco 계정 팀에 문의해 주십시오.
라이선스 위반	Cisco ISE 노드에서 허용되는 라이선스 수가 초과되었거나 곧 초과됨을 탐지했습니다.	추가 라이선스를 구입하려면 Cisco 계정 팀에 문의해 주십시오.
스마트 라이선싱 인증 만료	스마트 라이선싱 인증이 만료되었습니다.	**Cisco ISE** 라이선스 관리 창을 참조해 스마트 라이선싱 등록을 수동으로 갱신하거나 Cisco Smart Software Manager의 네트워크 연결을 확인하십시오. 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선스 인증 갱신 실패	Cisco Smart Software Manager를 이용한 인증 갱신에 실패했습니다.	**Cisco ISE** 라이선스 관리 창을 참조하여, **Licenses(**라이선스**)** 표에 있는 **Refresh(**새로고침**)** 버튼을 이용해 Cisco Smart Software Manager로 인증을 수동으로 갱신하십시오. 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 인증 갱신 성공	Cisco Smart Software Manager를 이용한 인증 갱신에 성공했습니다.	Cisco Smart Software Manager를 이용한 Cisco ISE 인증 갱신이 성공했음을 알리는 알림입니다.

경보 이름	경보 설명	경보 해결 방법
스마트 라이선싱 통신 장애	Cisco Smart Software Manager를 이용한 Cisco ISE 통신에 장애가 발생했습니다.	Cisco Smart Software Manager와의 네트워크 연결을 확인하십시오. Cisco Smart Software Manager에 로그인하거나, 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 통신 복원	Cisco Smart Software Manager를 이용한 Cisco ISE 통신이 복원되었습니다.	Cisco Smart Software Manager와의 네트워크 연결이 복원되었음을 알리는 알림입니다.
스마트 라이선싱 등록 취소 실패	Cisco Smart Software Manager를 이용한 Cisco ISE 등록 취소에 실패했습니다.	자세한 내용은 **Cisco ISE License Administration(Cisco ISE** 라이선스 관리**)** 창을 참조하십시오. Cisco Smart Software Manager에 로그인하거나, 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 등록 취소 성공	Cisco Smart Software Manager를 이용한 Cisco ISE 등록 취소에 성공했습니다.	Cisco Smart Software Manager를 이용한 Cisco ISE 등록 취소에 성공했음을 알리는 알림입니다.
스마트 라이선싱 비활성화	스마트 라이선스가 Cisco ISE에서 비활성화되어 기존 라이선스를 사용하고 있습니다.	스마트 라이선싱을 다시 활성화하는 방법은 **License Administration(**라이선스 관리**)** 창을 참조하십시오. Cisco ISE에서 스마트 라이선싱을 사용하는 방법을 알고 싶다면 Cisco ISE 관리 가이드를 참조하거나 Cisco 파트너에게 문의하십시오.
스마트 라이선싱 평가 기간 만료	스마트 라이선싱 평가 기간이 만료되었습니다.	Cisco Smart Software Manager를 이용해 Cisco ISE를 등록하는 방법은 **Cisco ISE License Administration(Cisco ISE** 라이선스 관리**)** 창을 참조하십시오.
스마트 라이선스 HA 역할 변경	스마트 라이선스를 사용하는 동안 고가용성 역할 변경이 발생했습니다.	Cisco ISE의 HA 역할이 변경되었음을 알리는 알림입니다.

경보 이름	경보 설명	경보 해결 방법
스마트 라이선싱 Id 인증서 만료	스마트 라이선싱 인증서가 만료되었습니다.	**Cisco ISE** 라이선스 관리 창을 참조해 스마트 라이선싱 등록을 수동으로 갱신하십시오. 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 Id 인증서 갱신 실패	Cisco Smart Software Manager를 이용한 스마트 라이선싱 등록 갱신에 실패했습니다.	**Cisco ISE** 라이선스 관리 창을 참조해 스마트 라이선싱 등록을 수동으로 갱신하십시오. 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 Id 인증서 갱신 성공	Cisco Smart Software Manager를 이용한 스마트 라이선싱 등록 갱신에 성공했습니다.	Cisco Smart Software Manager를 등록 갱신에 성공했음을 알리는 알림입니다.
스마트 라이선싱 잘못된 요청	잘못된 요청이 Cisco Smart Software Manager에 전달되었습니다.	자세한 내용은 **Cisco ISE License Administration(Cisco ISE** 라이선스 관리**)** 창을 참조하십시오. Cisco Smart Software Manager에 로그인하거나, 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 규정 위반	Cisco ISE 라이선스가 규정을 준수하지 않습니다.	자세한 내용은 **ISE License Administration(Cisco ISE** 라이선스 관리**)** 창을 참조하십시오. 새 라이선스를 구입하려면 파트너나 Cisco 계정 팀에 문의해 주십시오.
스마트 라이선싱 등록 실패	Cisco Smart Software Manager를 이용한 Cisco ISE 등록에 실패했습니다.	자세한 내용은 **ISE License Administration(Cisco ISE** 라이선스 관리**)** 창을 참조하십시오. Cisco Smart Software Manager에 로그인하거나, 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 등록 성공	Cisco Smart Software Manager를 이용한 Cisco ISE 등록에 성공했습니다.	Cisco Smart Software Manager를 이용한 Cisco ISE 등록에 성공했음을 알리는 알림입니다.
시스템 오류		

경보 이름	경보 설명	경보 해결 방법
로그 수집 오류	Cisco ISE 모니터링 컬렉터 프로세스가 정책 서비스 노드에서 생성된 감사 로그를 유지할 수 없습니다.	이는 정책 서비스 노드의 실제 기능에는 영향을 미치지 않습니다. 추가적인 해결 방법은 Cisco TAC에 문의해 주십시오.
예약된 보고서 내보내기 실패	내보낸 보고서(CSV 파일)를 구성한 저장소에 복사할 수 없습니다.	구성한 저장소를 확인해 주십시오. 저장소가 삭제되었으면 다시 추가해 주십시오. 저장소를 사용할 수 없거나 저장소에 연결할 수 없는 경우 저장소를 유효한 저장소로 다시 구성해 주십시오.
TrustSec		
알 수 없는 SGT가 프로비저닝됨	알 수 없는 SGT가 프로비저닝되었습니다.	ISE가 권한 부여 플로우 과정에서 알 수 없는 SGT를 프로비저닝했습니다. 알 수 없는 SGT를 알려진 플로우의 일부로 할당해서는 안 됩니다.
일부 TrustSec 네트워크 디바이스에 최신 ISE IP-SGT 매핑 컨피그레이션이 없음	일부 TrustSec 네트워크 디바이스에 최신 ISE IP-SGT 매핑 컨피그레이션이 없습니다.	ISE가 다른 IP-SGT 매핑 집합이 포함된 일부 네트워크 디바이스를 식별했습니다. **IP-SGT** 매핑 구축 옵션을 사용하여 디바이스를 업데이트해 주십시오.
TrustSec SSH 연결 장애	TrustSec SSH 연결에 실패했습니다.	ISE가 네트워크 디바이스에 대한 SSH 연결을 설정하지 못했습니다. **Network Device(**네트워크 디바이스**)** 창의 네트워크 디바이스 SSH 자격 증명이 네트워크 디바이스에 구성되어 있는 자격 증명과 비슷한지 확인해 주십시오. ISE(IP 주소)와의 네트워크 디바이스 사용 SSH 연결을 확인해 주십시오.
TrustSec에서 ISE가 1.0 이외의 TLS 버전에서 작동하도록 설정되었음을 식별함	TrustSec에서 식별된 ISE가 1.0 이외의 TLS 버전과 작동하도록 설정되었습니다.	TrustSec는 TLS 버전 1.0만 지원합니다.

경보 이름	경보 설명	경보 해결 방법
Trustsec PAC 검증 장애	Trustsec PAC 검증에 실패했습니다.	ISE가 네트워크 디바이스에서 전송한 PAC를 검증할 수 없습니다. **Network Device(**네트워크 디바이스**)** 창 및 디바이스 CLI에서 TrustSec 디바이스 자격 증명을 확인해 주십시오. 디바이스가 ISE 서버에 의해 프로비저닝된 유효한 PAC를 사용하는지 확인해 주십시오.
Trustsec 환경 데이터 다운로드 실패	Trustsec 환경 데이터 다운로드에 실패했습니다.	Cisco ISE에서 불법적인 환경 데이터 요청을 수신했습니다. 다음을 확인합니다. • PAC가 요청에 존재하며 유효합니다. • 모든 속성이 요청에 존재합니다.
TrustSec CoA 메시지 무시	TrustSec CoA 메시지가 무시되었습니다.	Cisco ISE에서 TrustSec CoA 메시지를 전송했지만 응답을 받지 못했습니다. 네트워크 디바이스가 CoA를 지원하는지 확인합니다. 디바이스 컨피그레이션을 확인합니다.
TrustSec 기본 이그레스 정책 수정	TrustSec 기본 이그레스 정책이 수정되었습니다.	TrustSec 기본 이그레스 정책 셀이 수정되었습니다. 보안 정책과 일치하는지 확인하십시오.

참고 사용자 또는 엔드포인트를 Cisco ISE에 추가하는 경우에는 경보가 트리거되지 않습니다.

경보 설정

다음 표에서는 **Alarm Settings(**경보 설정**)** 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Alarm Settings(**경보 설정**)** > **Alarm Configuration(**경보 컨피그레이션**)** > **Add(**추가**)**)

필드 이름	설명
경보 유형	경보 유형

필드 이름	설명
경보 이름	경보의 이름입니다.
Description(설명**)**	경보에 대한 설명입니다.
제안 작업	경보가 트리거될 때 수행할 작업입니다.
Status(상태**)**	경보 규칙을 활성화하거나 비활성화합니다.
심각도	경보의 심각도 레벨을 선택합니다. 유효한 옵션은 다음과 같습니다. • Critical (위험) : 심각한 오류 상태를 나타냅니다. • Warning(경고): 정상적이기는 하지만 중요한 상태를 나타냅니다. 기본 상태입니다. • Info(정보) - 이 옵션은 정보 메시지를 나타냅니다.
시스템 로그 메시지 보내기	Cisco ISE가 생성하는 각 시스템 경보에 대해 시스템 로그 메시지를 보냅니다.
쉼표로 구분하여 여러 이메일 입력	이메일 주소 또는 ISE 관리자 이름 또는 둘 다의 목록입니다.
이메일 메모**(0 ~ 4,000**자**)**	시스템 경보와 연결하려는 맞춤형 텍스트 메시지.

맞춤형 경보 추가

Cisco ISE에는 높은 메모리 사용률 및 구성 변경과 같은 12가지 기본 경보 유형이 포함되어 있습니다. Cisco에서 정의한 시스템 경보는 **Alarms Settings(**경보 설정**)** 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Alarm Settings(**경보 설정**)**)에 나열됩니다. 시스템 경보만 편집할 수 있습니다.

기존 시스템 경보 외에도 기존 경보 유형에서 사용자 맞춤화 경보를 추가, 수정 또는 삭제할 수 있습니다.

경보 유형별로 최대 5개의 경보를 생성할 수 있습니다. 총 경보 수는 200개로 제한됩니다.

Alarm Settings(경보 설정**)** 창의 **Alarm Configuration(**경보 구성**)** 탭에서 **Conditions(**조건**)** 열에는 4가지 경보, 즉 High Authentication Latency(높은 인증 레이턴시), High Disk I/O Utilization(높은 디스크 I/O 사용률), High Disk Space Utilization(높은 디스크 공간 사용률) 및 High Memory Utilization(높은 메모리 공간 사용률)에 대한 세부정보가 표시됩니다 이러한 각 경보에는 구성 가능한 임계값이 있습니다. 그러나 임계값이 구성된 경우에도 **Conditions(**조건**)** 열에 세부정보가 표시되지 않을 수 있습니다. 이 경우 경보의 관련 임계값 필드를 다시 편집하여 **Conditions(**조건**)** 열의 세부정보를 확인합니다.

경보를 추가하려면 다음을 수행합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Alarm Settings(**경보 설정**)**

단계 **2** **Alarm Configuration(**경보 구성**)** 탭 아래에서 **Add(**추가**)**를 클릭합니다.

단계 **3** 필요한 세부정보를 입력합니다. 자세한 내용은 경보 설정 섹션을 참고하십시오.

경보 유형(High Memory Utilization(높은 메모리 사용률), Excessive RADIUS Authentication Attempts(과도한 RADIUS 인증 시도), Excessive TACACS Authentication Attempts(과도한 TACACS 인증 시도) 등)에 따라 **Alarm Configuration(**경보 구성**)** 창에 추가 속성이 표시됩니다. 예를 들어 구성 변경 경보에 대해서는 **Object Name(**개체 이름**)**, **Object Type(**개체 유형**)** 및 **Admin Name(**관리자 이름**)** 필드가 표시됩니다. 각기 기준이 다른 동일 경보의 여러 인스턴스를 추가할 수 있습니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

Cisco ISE 경보 알림 및 임계값

Cisco ISE 경보를 활성화 또는 비활성화하고 위험 조건에 대한 알림을 받도록 경보 알림 동작을 구성할 수 있습니다. 특정 경보의 경우 과도한 실패 시도 경보에 대한 최대 실패 시도 횟수 또는 높은 디스크 사용률 경보에 대한 최대 디스크 사용률과 같은 임계값을 구성할 수 있습니다.

경보 단위로 알림 설정을 구성할 수 있습니다. 각 경보(시스템 정의 경보와 사용자 맞춤화 경보 둘 다)에 대해 알림을 받아야 하는 사용자의 이메일 ID를 입력할 수 있습니다.

참고 경보 규칙 레벨에 지정되어 있는 수신자 이메일 주소는 전역 수신자 이메일 주소 설정을 재정의합니다.

경보 활성화 및 구성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Alarm Settings(**경보 설정**)**

단계 **2** 기본 경보 목록에서 경보를 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Enable(**활성화**)** 또는 **Disable(**비활성화**)**을 선택합니다.

단계 **4** 해당하는 경우 경보 임계값을 구성합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

모니터링을 위한 **Cisco ISE** 경보

Cisco ISE는 위험 시스템 조건이 발생할 때마다 항상 알림을 보내는 시스템 경보를 제공합니다. Cisco ISE에서 생성된 경보는 경보 dashlet에 표시됩니다. 이러한 알림은 자동으로 경보 dashlet에 표시됩니다.

경보 dashlet에는 최근 경보 목록이 표시되며 여기서 경보 세부정보를 보기 위한 경보를 선택할 수 있습니다. 관리자는 또한 이메일 및 시스템 로그 메시지를 통해 경보 알림을 받을 수도 있습니다.

모니터링 경보 보기

단계 **1** Cisco ISE **Dashboard(**대시보드**)**로 이동합니다.

단계 **2** **Alarms(**경보**)** dashlet에서 원하는 경보를 클릭합니다. 경보 세부정보 및 제안 작업이 포함된 새 윈도우가 열립니다.

단계 **3** 경보를 새로 고침하려면 **Refresh(**새로 고침**)**를 클릭합니다.

단계 **4** 경보를 확인하여 경보를 읽은 것으로 표시하면 경보 카운터(경보가 생성된 횟수)가 감소합니다. 타임스탬프 옆에 있는 확인란을 선택하여 확인할 경보를 선택할 수 있습니다.

현재 창에 표시된 모든 경보를 읽은 것으로 표시하려면 **Acknowledge(**확인**)** 드롭다운 목록에서 **Acknowledge Selected(**선택한 경보 확인**)**를 선택합니다. 기본적으로 이 창에는 100개의 행이 표시됩니다. **Rows/Page(**행/페이지**)** 드롭다운 목록에서 원하는 값을 선택하여 표시할 다른 행 수를 선택할 수 있습니다.

현재 창에 표시되어 있는지 여부와 관계없이 모든 경보를 읽은 것으로 표시하려면 **Acknowledge(**확인**)** 드롭다운 목록에서 **Acknowledge All(**모두 확인**)**을 선택합니다.

참고 제목 행에서 **Time Stamp(**타임스탬프**)** 근처에 있는 확인란을 선택하면 창에 표시되는 모든 경보가 선택됩니다. 그러나 선택한 경보 중 하나 이상에 대한 확인란의 선택을 취소하면 모든 기능 선택이 취소됩니다. 이제 **Time Stamp(**타임스탬프**)** 근처의 확인란이 선택되지 않은 것을 확인할 수 있습니다.

단계 **5** 선택한 경보에 해당하는 **Details(**세부정보**)** 링크를 클릭합니다. 선택한 경보에 해당하는 세부정보가 포함된 새 창이 열립니다.

참고 페르소나를 변경하기 전에 생성된 경보에 해당하는 **Details(**세부정보**)** 링크에는 데이터가 표시되지 않습니다.

로그 수집

모니터링 서비스는 로그 및 컨피그레이션 데이터를 수집하고 데이터를 저장한 다음 처리하여 보고서와 경보를 생성합니다. 구축 서버에서 수집된 로그 세부정보를 볼 수 있습니다.

경보 시스템 로그 컬렉션 위치

경보 알림을 시스템 로그 메시지로 보내도록 모니터링 기능을 구성하는 경우 알림을 받을 시스템 로그 대상이 필요합니다. 경보 시스템 로그 대상은 경보 시스템 로그 메시지가 전송되는 대상입니다.

참고 Cisco ISE 모니터링을 위해서는 로깅 소스 인터페이스 컨피그레이션에서 NAS(Network Access Server) IP 주소를 사용해야 합니다. Cisco ISE 모니터링에 사용할 스위치를 구성해야 합니다.

또한 시스템 로그 메시지를 받을 수 있는 시스템 로그 서버로 시스템이 구성되어 있어야 합니다. 경보 시스템 로그 대상을 생성, 편집 및 삭제할 수 있습니다.

원격 로깅 대상을 경보 대상으로 구성하려면 이 절차를 수행합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Remote Logging Targets(**원격 로깅 대상**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **New Logging Target(**새 로깅 대상**)** 창에서 로깅 대상에 대한 필수 세부정보를 제출하고 **Include Alarms for this Target(**이 대상에 대한 경보 포함**)** 확인란을 선택합니다.

RADIUS 라이브 로그

다음 표에서는 최근 RADIUS 인증이 표시되는 Live Logs(RADIUS 라이브 로그) 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**입니다. 기본 PAN에서만 RADIUS 라이브 로그를 볼 수 있습니다.

표 ***181: RADIUS*** 라이브 로그

필드 이름	설명
Time(시간**)**	모니터링 및 문제 해결 수집 에이전트가 로그를 수신한 시간을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Status(상태**)**	인증 성공 여부를 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다. 인증이 통과한 경우 녹색으로 표시되고, 인증이 실패한 경우 빨간색으로 표시됩니다.

필드 이름	설명
Details(세부정보**)**	Details(세부정보) 열 아래의 아이콘을 클릭하면 새 브라우저 창에서 **Authentication Detail Report(**인증 세부정보 보고서**)**가 열립니다. 이 보고서는 인증 및 관련 속성, 인증 플로우에 대한 정보를 제공합니다. **Authentication Details(**인증 세부정보**)** 상자에서 **Response Time(**응답 시간**)**은 Cisco ISE가 인증 플로우를 처리하는 데 걸리는 총 시간입니다. 예를 들어 인증이 3개의 왕복 메시지로 구성되어 있고 첫 메시지는 300ms, 그 다음 메시지는 150ms, 마지막 메시지는 100ms의 처리 시간이 소요된 경우 **Response Time(**응답 시간**)**은 300 + 150 + 100 = 550ms입니다. 참고 48시간 넘게 활성 상태인 엔드포인트의 세부정보는 볼 수 없습니다. 48시간 넘게 활성 상태인 엔드포인트의 **Details(**세부정보**)** 아이콘을 클릭하면 다음 메시지가 포함된 페이지가 표시될 수 있습니다. `No Data available for this record(이 기록에 데이터가 없습니다). Either the data is purged or authentication for this session record happened a week ago(데이터가 삭제되었거나이 세션 기록에 대한 인증이 일주일 전에 발생했습니다). Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session('PassiveID' 또는 'PassiveID Visibility' 세션인 경우에는 ISE가 아닌 세션에 대한 인증 세부정보만 포함됩니다).`
Repeat Count(반복 횟수**)**	지난 24시간 동안 ID, 네트워크 디바이스 및 권한 부여가 변경되지 않고 인증 요청이 반복된 횟수를 표시합니다.

필드 이름	설명
ID	인증과 연결된 로그인한 사용자 이름을 표시합니다. ID 저장소에 사용자 이름이 없는 경우 INVALID로 표시됩니다. 인증이 다른 이유로 인해 실패하는 경우 USERNAME으로 표시됩니다. 참고 이는 사용자에게만 적용되며, MAC 주소에는 적용되지 않습니다. 디버깅을 지원하기 위해 Cisco ISE가 잘못된 사용자 이름을 표시하도록 할 수 있습니다. 이렇게 하려면 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Security Settings(**보안 설정**)**에서 **Disclose Invalid Usernames(**잘못된 사용자 이름 공개**)** 확인란을 선택합니다. 또한 **Disclose Invalid Usernames(**잘못된 사용자 이름 공개**)** 옵션이 시간 초과되도록 구성하여 이 옵션을 수동으로 해제할 필요가 없게 할 수 있습니다.
Endpoint ID(엔드포인트 **ID)**	엔드포인트의 고유한 식별자(일반적으로는 MAC 또는 IP 주소)를 표시합니다.
Endpoint Profile(엔드포인트 프로파일**)**	iPhone, Android, MacBook, Xbox 등으로 프로파일이 지정된 엔드포인트 유형을 표시합니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.
Authorization Policy(권한 부여 정책**)**	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.
Authorization Profiles(권한 부여 프로파일**)**	인증에 사용된 권한 부여 프로파일을 표시합니다.
IP Address(IP 주소**)**	엔드포인트 디바이스의 IP 주소를 표시합니다.
Network Device(네트워크 디바이스**)**	네트워크 액세스 디바이스의 IP 주소를 표시합니다.
Device Port(디바이스 포트**)**	엔드포인트가 연결되어 있는 포트 번호를 표시합니다.
Identity Group(ID 그룹**)**	로그가 생성된 대상인 사용자나 엔드포인트에 할당되는 ID 그룹을 표시합니다.
Posture Status(포스처 상태**)**	포스처 검증의 상태 및 인증에 대한 세부정보를 표시합니다.

필드 이름	설명
Server(서버**)**	로그가 생성된 정책 서비스를 나타냅니다.
MDM Server Name(MDM 서버 이름**)**	MDM 서버의 이름을 표시합니다.
Event(이벤트**)**	이벤트 상태를 표시합니다.
Failure Reason(실패 이유**)**	인증이 실패한 경우 자세한 실패 이유를 표시합니다.
Auth Method(인증 방법**)**	MS-CHAPv2(Microsoft Challenge Handshake Authentication Protocol Version 2), IEE 802.1x 또는 dot1x 등과 같이 RADIUS 프로토콜에서 사용하는 인증 방법을 표시합니다.
Authentication Protocol(인증 프로토콜**)**	PEAP(Protected Extensible Authentication Protocol), EAP(Extensible Authentication Protocol) 등 사용되는 인증 프로토콜을 표시합니다.
Security Group(보안 그룹**)**	인증 로그로 식별된 그룹을 표시합니다.
Session ID(세션 **ID)**	세션 ID를 표시합니다.

참고 **RADIUS Live Logs(RADIUS** 라이브 로그**)** 및 **TACACS+ Live Logs(TACACS+** 라이브 로그**)** 창에는 각 정책 권한 부여 규칙의 첫 번째 속성에 대한 "Queried PIP" 항목이 표시됩니다. 권한 부여 규칙 내의 모든 속성이 이전 규칙에 대해 이미 쿼리된 사전과 관련된 경우 추가 "Queried PIP" 항목이 표시되지 않습니다.

RADIUS **Live Logs(**라이브 로그**)** 창에서는 다음을 수행할 수 있습니다.

- 데이터를 CSV 또는 PDF 형식으로 내보냅니다.
- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 사용자 맞춤화 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.
- 열 값을 정렬합니다.

참고 모든 사용자 맞춤 설정은 사용자 기본 설정으로 저장됩니다.

TACACS 라이브 로그

다음 표에서는 TACACS+ AAA 세부정보가 표시되는 TACACS Live Logs(TACACS 라이브 로그) 페이지의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(운영)** > **RADIUS** > **Live Logs(라이브 로그)**입니다. 기본 PAN에서만 TACACS 라이브 로그를 볼 수 있습니다.

표 ***182: TACACS*** 라이브 로그

필드 이름	사용 지침
생성 시간	특정 이벤트가 트리거된 시간을 기준으로 시스템 로그 생성 시간을 표시합니다.
Logged Time(기록된 시간**)**	모니터링 노드에서 시스템 로그를 처리하고 저장한 시간을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Status(상태**)**	인증 성공 여부를 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다. 인증이 통과한 경우 녹색으로 표시되고, 인증이 실패한 경우 빨간색으로 표시됩니다.
Details(세부정보**)**	돋보기를 클릭하면 표시되는 보고서를 드릴다운하여 선택한 인증 시나리오에 대한 추가 세부정보를 확인할 수 있습니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Session Key(세션 키**)**	ISE가 네트워크 디바이스에 반환하는 세션 키(EAP 성공 또는 EAP 장애 메시지에서 확인 가능)를 표시합니다.
Username(사용자 이름**)**	디바이스 관리자의 사용자 이름을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Type(유형**)**	두 가지 유형인 Authentication(인증)과 Authorization(권한 부여)으로 구성됩니다. 인증, 권한 부여 또는 둘 다에서 통과했거나 장애가 발생한 사용자 이름을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.
권한 부여 정책	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.

필드 이름	사용 지침
ISE Node(ISE 노드**)**	액세스 요청이 처리되는 ISE 노드의 이름을 표시합니다.
Network Device Name(네트워크 디바이스 이름**)**	네트워크 디바이스의 이름을 표시합니다.
Network Device IP(네트워크 디바이스 **IP)**	액세스 요청이 처리되는 네트워크 디바이스의 IP 주소를 표시합니다.
네트워크 디바이스 그룹	네트워크 디바이스가 속한 해당 네트워크 디바이스 그룹의 이름을 표시합니다.
디바이스 유형	다른 네트워크 디바이스의 액세스 요청을 처리하는 데 사용되는 디바이스 유형 정책을 표시합니다.
Location(위치**)**	네트워크 디바이스의 액세스 요청을 처리하는 데 사용되는 위치 기반 정책을 표시합니다.
Device Port(디바이스 포트**)**	액세스 요청을 수행하는 디바이스 포트 번호를 표시합니다.
Failure Reason(실패 이유**)**	네트워크 디바이스에서 수행한 액세스 요청을 거부하는 이유를 표시합니다.
Remote Address(원격 주소**)**	최종 무선국을 고유하게 식별하는 IP 주소, MAC 주소 또는 기타 문자열을 표시합니다.
Matched Command Set(일치하는 명령 집합**)**	MatchedCommandSet 속성 값이 있으면 표시하고, MatchedCommandSet 속성 값이 비어 있거나 속성 자체가 시스템 로그에 없으면 빈 값을 표시합니다.
Shell Profile(셸 프로파일**)**	네트워크 디바이스에서 명령을 실행하기 위해 디바이스 관리자에게 부여된 권한을 표시합니다.

TACACS Live Logs(TACACS 라이브 로그) 페이지에서는 다음을 수행할 수 있습니다.

- 데이터를 csv 또는 pdf 형식으로 내보냅니다.
- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 맞춤형 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.
- 열 값을 정렬합니다.

참고 모든 사용자 맞춤 설정은 사용자 기본 설정으로 저장됩니다.

라이브 인증

Live Authentications(라이브 인증**)** 창에서 발생하는 최근 RADIUS 인증을 모니터링할 수 있습니다. 이 창에는 지난 24시간 동안의 상위 10개 RADIUS 인증이 표시됩니다. 이 섹션에서는 **Live Authentications(**라이브 인증**)** 창의 기능에 대해 설명합니다.

Live Authentications(라이브 인증**)** 창에는 발생하는 인증 이벤트에 해당하는 라이브 인증 항목이 표시됩니다. 이 창에는 인증 항목 외에 이벤트에 해당하는 라이브 세션 항목도 표시됩니다. 원하는 세션을 드릴다운하여 세션에 해당하는 상세 보고서를 볼 수도 있습니다.

Live Authentications(라이브 인증**)** 창에는 최근 RADIUS 인증이 발생한 순서에 따라 테이블 형식으로 표시됩니다. **Live Authentications(**라이브 인증**)** 창 하단에 표시되는 마지막 업데이트에는 서버 날짜, 시간 및 표준 시간대가 표시됩니다.

참고 액세스 요청 패킷의 비밀번호 속성이 비어 있는 경우 오류 메시지가 트리거되고 액세스 요청이 실패합니다.

단일 엔드포인트 인증이 성공한 경우 두 항목이 **Live Authentications(**라이브 인증**)** 창에 표시됩니다. 하나는 인증 기록에 해당하고 다른 하나는 세션 기록(세션 라이브 보기에서 가져옴)에 해당합니다. 이후에 디바이스에서 또 다른 인증이 성공적으로 수행되면 세션 기록에 해당하는 반복 카운터가 증가합니다. **Live Authentications(**라이브 인증**)** 창에 나타나는 반복 카운터에는 숨겨진 중복 RADIUS 인증 성공 메시지의 수가 표시됩니다.

기본적으로 표시되는 라이브 인증 데이터 범주를 참고하십시오. 이러한 항목은 최근 RADIUS 인증 섹션에 설명되어 있습니다.

모든 열을 표시하거나 선택한 데이터 열만 표시할 수 있습니다. 표시할 열을 선택한 후에는 선택 사항을 저장할 수 있습니다.

라이브 인증 모니터링

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**

단계 **2** **Refresh(**새로 고침**)** 드롭다운 목록에서 시간 간격을 선택하여 데이터 새로 고침 속도를 변경합니다.

단계 **3** **Refresh(**새로 고침**)** 아이콘을 클릭하여 데이터를 수동으로 업데이트합니다.

단계 **4** **Show(**표시**)** 드롭다운 목록의 옵션을 선택하여 표시되는 기록 수를 변경합니다.

단계 **5** **Within(**시간 범위**)** 드롭다운 목록에서 옵션을 선택하여 시간 간격을 지정합니다.

단계 **6** **Add or Remove Columns(**열 추가 또는 제거**)**를 클릭하고 드롭다운 목록에서 옵션을 선택하여 표시되는 열을 변경합니다.

단계 **7** 드롭다운 목록 맨 아래에서 **Save(**저장**)**를 클릭하여 수정 사항을 저장합니다.

단계 **8** **Show Live Sessions(**라이브 세션 표시**)**를 클릭하여 라이브 RADIUS 세션을 확인합니다.

라이브 세션에 대해 동적 CoA(Change of Authorization) 기능을 사용하면 활성 RADIUS 세션을 동적으로 제어할 수 있습니다. NAD(Network Access Device)에 대해 재인증 또는 연결 끊기 요청을 보낼 수 있습니다.

Live Authentications(라이브 인증) 페이지에서 데이터 필터링

Live Authentications(라이브 인증) 페이지의 필터를 사용하면 필요한 정보를 필터링하고 네트워크 인증 문제를 빠르게 해결할 수 있습니다. Authentication(인증)(라이브 로그) 페이지에서 기록을 필터링하여 원하는 기록만 볼 수 있습니다. 인증 로그에는 다양한 세부정보가 포함되어 있으며, 특정 사용자나 위치로부터의 인증을 필터링하면 데이터를 빠르게 스캔할 수 있습니다. Live Authentications(라이브 인증) 페이지의 필드에서 사용할 수 있는 다양한 연산자를 통해 검색 조건에 따라 기록을 필터링할 수 있습니다.

- 'abc': 'abc' 포함
- '!abc': 'abc' 미포함
- '{}': 비어 있음
- '!{}': 비어 있지 않음
- 'abc*': 'abc'로 시작됨
- '*abc': 'abc'로 끝남
- '\!', '*', '\{', '\\' : Esc

Escape(이스케이프) 옵션을 사용하면 필터로 사용되는 특수 문자를 비롯한 특수 문자로 텍스트를 필터링할 수 있습니다. 특수 문자 앞에는 백슬래시(\)를 접두사로 추가해야 합니다. 예를 들어 ID가 "Employee!"인 사용자의 인증 기록을 확인하려면 **Identity Filter(ID** 필터**)** 필드에 "Employee\!"를 입력합니다. 이 예제에서 Cisco ISE는 느낌표(!)를 특수 문자가 아닌 리터럴 문자로 간주합니다.

또한 **Status(**상태**)** 필드에서 통과한 인증 기록, 실패한 인증, 라이브 세션 등만 필터링할 수도 있습니다. 녹색 확인 표시를 클릭하면 이전에 통과한 모든 인증이 필터링됩니다. 빨간색 십자 표시를 클릭하면 실패한 모든 인증이 필터링됩니다. 파란색 i 아이콘을 클릭하면 모든 라이브 세션이 필터링됩니다. 이러한 옵션의 조합을 표시하도록 선택할 수도 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**

단계 **2** 라이브 인증 표시 페이지에서 원하는 필드를 기준으로 데이터를 필터링합니다.

통과/실패한 인증이나 라이브 인증을 기준으로 결과를 필터링할 수 있습니다.

RADIUS 라이브 세션

다음 표에서는 라이브 인증을 표시하는, RADIUS **Live Sessions(**라이브 세션**)** 창의 필드를 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 RADIUS 라이브 세션의 Primary PAN(기본 PAN)에서만 볼 수 있습니다.

표 ***183: RADIUS*** 라이브 세션

필드 이름	설명
Initiated(시작됨**)**	세션이 시작된 타임스탬프를 표시합니다.
Updated(업데이트됨**)**	변경으로 인해 세션이 마지막으로 업데이트된 타임스탬프를 표시합니다.
Account Session Time(계정 세션 시간**)**	사용자 세션의 시간 범위를 초 단위로 표시합니다.
Session Status(세션 상태**)**	엔드포인트 디바이스의 현재 상태를 표시합니다.
Action(CoA 작업**)**	**Actions(**작업**)** 아이콘을 클릭하여 활성 RADIUS 세션을 다시 인증하거나 활성 RADIUS 세션의 연결을 끊습니다.
Repeat Count(반복 횟수**)**	사용자 또는 엔드포인트를 재인증하는 횟수를 표시합니다.
Endpoint ID(엔드포인트 **ID)**	엔드포인트의 고유한 식별자(일반적으로는 MAC 또는 IP 주소)를 표시합니다.
ID	엔드포인트 디바이스의 사용자 이름을 표시합니다.
IP Address(IP 주소**)**	엔드포인트 디바이스의 IP 주소를 표시합니다.
Audit Session ID(감사 세션 **ID)**	고유 세션 ID를 표시합니다.
Account Session ID(계정 세션 **ID)**	네트워크 디바이스에서 제공하는 고유 ID를 표시합니다.
Endpoint Profile(엔드포인트 프로파일**)**	디바이스에 대한 엔드포인트 프로파일을 표시합니다.
Posture Status(포스처 상태**)**	포스처 검증의 상태 및 인증에 대한 세부정보를 표시합니다.
Security Group(보안 그룹**)**	인증 로그로 식별된 그룹을 표시합니다.
Server(서버**)**	로그가 생성된 정책 서비스 노드를 나타냅니다.

필드 이름	설명
Auth Method(인증 방법**)**	PAP(Password Authentication Protocol), CHAP(Challenge Handshake Authentication Protocol), IEE 802.1x 또는 dot1x 등과 같이 RADIUS 프로토콜에서 사용하는 인증 방법을 표시합니다.
Authentication Protocol(인증 프로토콜**)**	PEAP(Protected Extensible Authentication Protocol), EAP(Extensible Authentication Protocol) 등 사용되는 인증 프로토콜을 표시합니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.
권한 부여 정책	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.
Authorization Profiles(권한 부여 프로파일**)**	인증에 사용된 권한 부여 프로파일을 표시합니다.
NAS IP Address(NAS IP 주소**)**	네트워크 디바이스의 IP 주소를 표시합니다.
Device Port(디바이스 포트**)**	네트워크 디바이스에 연결된 포트를 표시합니다.
PRA Action(PRA 작업**)**	네트워크에서 클라이언트가 규정 준수를 위해 올바르게 포스처된 후 클라이언트에 대해 수행되는 정기적 재평가 작업을 표시합니다.
ANC Status(ANC 상태**)**	디바이스의 적응형 네트워크 제어 상태를 Quarantine(격리), Unquarantine(격리 해제) 또는 Shutdown(종료)으로 표시합니다.
WLC Roam(WLC 로밍**)**	로밍 중에 엔드포인트가 WLC 간에 전달되었음을 추적하는 데 사용되는 부울(Y/N)을 표시합니다. cisco-av-pair=nas-update의 값은 Y 또는 N입니다. 참고 Cisco ISE는 WLC의 nas-update=true 속성을 사용하여 세션이 로밍 상태인지 여부를 식별합니다. 원래 WLC가 nas-update=true인 계정 관리 중지 속성을 전송하는 경우 재인증을 방지하기 위해 ISE에서 세션이 삭제되지 않습니다. 로밍이 실패하는 경우 ISE는 5일 동안 활동이 없으면 세션을 지웁니다.
Packets In(수신 패킷**)**	수신된 패킷 수를 표시합니다.
Packets Out(전송 패킷**)**	전송된 패킷 수를 표시합니다.
Bytes In(수신 바이트**)**	수신된 바이트 수를 표시합니다.

필드 이름	설명
Bytes Out(전송 바이트**)**	전송된 바이트 수를 표시합니다.
Session Source(세션 소스**)**	RADIUS 세션인지 아니면 패시브 ID 세션인지를 나타냅니다.
User Domain Name(사용자 도메인 이름**)**	사용자의 등록된 DNS 이름을 표시합니다.
Host Domain Name(호스트 도메인 이름**)**	호스트의 등록된 DNS 이름을 표시합니다.
User NetBIOS Name(사용자 **NetBIOS** 이름**)**	사용자의 NetBIOS 이름을 표시합니다.
Host NetBIOS Name(호스트 **NetBIOS** 이름**)**	호스트의 NetBIOS 이름을 표시합니다.
라이선스 유형	사용하는 라이선스 유형을 표시합니다.
라이선스 세부정보	라이선스 세부정보를 표시합니다.

필드 이름	설명
Provider(사업자**)**	엔드포인트 이벤트는 다양한 시스템 로그 소스에서 학습됩니다. 이러한 시스템 로그 소스를 제공자라고 합니다. • WMI(Windows Management Instrumentation)—WMI는 운영체제, 장치, 애플리케이션 및 서비스 관련 관리 정보에 액세스하기 위한 공통 인터페이스와 개체 모델을 제공하는 Windows 서비스입니다. • 에이전트: 클라이언트나 다른 프로그램을 대신하여 클라이언트에서 실행되는 프로그램입니다. • 시스템 로그: 클라이언트가 메시지를 전송하는 로깅 서버입니다. • REST: 클라이언트가 터미널 서버를 통해 인증됩니다. 이 시스템 로그 소스에 대한 TS Agent ID(TS 에이전트 ID), Source Port Start(소스 포트 시작), Source Port End(소스 포트 끝), Source First Port(소스 최초 포트) 값이 표시됩니다. • Span: 네트워크 정보가 span 프로브를 사용해 검색됩니다. • DHCP: DHCP 이벤트입니다. • 엔드포인트 참고 엔드포인트 세션에서 서로 다른 제공자에서 발생한 두 이벤트를 파악하면, 제공자는 라이브 세션 페이지에 쉼표로 구분된 값으로 표시됩니다.
MAC 주소**(MAC Address)**	클라이언트의 MAC 주소를 표시합니다.
엔드포인트 확인 시간	엔드포인트 프로브가 엔드포인트를 마지막으로 확인한 시간을 표시합니다.

필드 이름	설명
Endpoint Check Result(엔드포인트 확인 결과**)**	엔드포인트 프로브의 결과를 표시합니다. 가능한 값은 다음과 같습니다. • 연결 불가 • 사용자 로그아웃 • 활성 사용자
Source Port Start(소스 포트 시작**)**	(값은 REST 제공자에 대해서만 표시됨) 포트 범위의 첫 번째 포트 번호를 표시합니다.
Source Port End(소스 포트 종료**)**	(값은 REST 제공자에 대해서만 표시됨) 포트 범위의 마지막 포트 번호를 표시합니다.
Source First Port(소스 첫 번째 포트**)**	(값은 REST 제공자에 대해서만 표시됨) 터미널 서버 에이전트가 할당한 첫 번째 포트를 표시합니다. 터미널 서버는 모뎀이나 네트워크 인터페이스 없이도 여러 엔드포인트가 연결될 수 있고 여러 엔드포인트와 LAN 네트워크 간의 연결을 촉진하는 서버 또는 네트워크 디바이스를 말합니다. 여러 엔드포인트가 같은 IP 주소를 이용하는 것처럼 보이기 때문에 특정 사용자의 IP 주소를 식별하기가 어렵습니다. 따라서 특정 사용자를 식별하기 위해 각 사용자에 포트 범위를 할당하는 터미널 서버 에이전트가 서버에 설치됩니다. 이렇게 하면 IP 주소-포트-사용자 매핑을 만들 수 있습니다.
TS 에이전트 **ID**	(값은 REST 제공자에 대해서만 표시됨) 엔드포인트에 설치된 터미널 서버 에이전트의 고유 ID를 표시합니다.
AD User Resolved Identities(AD 사용자가 확인한 **ID)**	(값은 AD 사용자에 대해서만 표시됨) 일치하는 잠재적 계정을 표시합니다.
AD User Resolved DNs(AD 사용자가 확인한 **DN)**	(값은 AD 사용자에 대해서만 폿시됨) AD 사용자의 Distinguished Name(고유 이름) 을 표시합니다 (예: CN=chris,CN=Users,DC=R1,DC=com).

요약 내보내기

지난 7일 동안 모든 사용자가 내보낸 보고서의 세부정보를 상태와 함께 볼 수 있습니다. 내보내기 요약에는 수동 보고서와 예약 보고서가 모두 포함됩니다. 내보내기 요약 페이지는 2분마다 자동으로

새로 고쳐집니다. 내보내기 요약 페이지를 수동으로 새로 고치려면 새로 고침 아이콘을 클릭하십시오.

슈퍼 관리자는 진행 중이거나 대기열에 있는 내보내기를 취소할 수 있습니다. 다른 사용자는 본인이 시작한 내보내기 프로세스만 취소할 수 있습니다.

기본적으로는 특정 시점에 보고서를 3번만 수동으로 내보낼 수 있으며, 수동으로 트리거된 나머지 보고서는 대기열에 추가됩니다. 예약된 보고서 내보내기에는 이러한 제한이 없습니다.

참고 대기열에 있는 모든 보고서가 다시 예약되며, 진행 중이거나 취소 중인 상태의 보고서는 Cisco ISE 서버가 재시작되면 실패로 표시됩니다.

참고 기본 MnT 노드가 다운되면 예약된 보고서 내보내기 작업이 보조 MnT 노드에서 실행됩니다.

다음 표에서는 Export Summary(요약 내보내기) 페이지의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Export Summary(**요약 내보내기**)**입니다.

표 ***184:*** 요약 내보내기

필드 이름	설명
Report Exported(내보낸 보고서**)**	보고서의 이름을 표시합니다.
Exported By(내보낸 사람**)**	내보내기 프로세스를 시작한 사용자의 역할을 표시합니다.
Scheduled(예약됨**)**	보고서 내보내기가 예약된 내보내기인지 표시합니다.
Triggered On(트리거됨**)**	내보내기 프로세스가 시스템에서 트리거된 시간을 표시합니다.
Repository(저장소**)**	내보낸 데이터를 저장할 저장소 이름을 표시합니다.
Filter Parameters(필터 파라미터**)**	보고서를 내보내는 동안 선택한 필터 파라미터를 표시합니다.

필드 이름	설명
Status(상태**)**	내보낸 보고서의 상태를 표시합니다. 다음 중 하나일 수 있습니다. • 대기열에 있음 • 진행 중 • 완료됨 • 취소 중 • 취소됨 • 실패 • 건너뜀 참고 실패 상태에는 실패 이유가 표시됩니다. 건너뜀 상태는 기본 MnT 노드가 다운되어 예약된 보고서 내보내기를 건너뛰었음을 나타냅니다.

Export Summary(내보내기 요약) 페이지에서 다음을 수행할 수 있습니다.

- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 맞춤형 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.

인증 요약(Authentication Summary) 보고서

인증 요청과 관련된 속성에 따른 특정 사용자, 디바이스 또는 검색 기준에 대한 네트워크 액세스 문제를 해결할 수 있습니다. 이를 위해서는 인증 요약 보고서를 실행합니다.

네트워크 액세스 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Device Administration(**디바이스 관리**)** > **Authentication Summary Report(**인증 요약 보고서**)**.

단계 **2** 보고서에서 오류 사유를 필터링합니다.

단계 **3** 네트워크 액세스 문제를 해결하려면 보고서의 오류 사유별 인증 섹션 내 데이터를 검토합니다.

참고 인증 요약(Authentication Summary) 보고서에는 실패했거나 성공한 인증에 해당하는 최신 데이터가 수집되어 표시되므로, 보고서 내용이 표시될 때까지는 몇 분 정도 걸립니다.

구축 및 지원 정보에 대한 **Cisco Support Diagnostics**

개요

Cisco Support Diagnostics Connector는 Cisco TAC(Technical Assistance Center) 및 Cisco 지원 엔지니어가 기본 관리 노드에서 구축 정보를 가져올 수 있도록 지원하는 새로운 기능입니다. TAC는 커넥터를 통해 구축의 특정 노드에 대한 지원 정보를 가져올 수 있게 됩니다. 이 데이터를 사용하면 문제를 보다 신속하고 효과적으로 해결할 수 있습니다.

Cisco ISE 관리 포털을 통해 Cisco Support Diagnostics Connector를 활성화할 수 있습니다. 이 기능을 사용하면 SSE(Security Services Exchange) 클라우드 포털을 활용하여 구축의 기본 정책 관리 노드와 Cisco Support Diagnostics를 양방향으로 연결할 수 있습니다.

사전 요건

- Cisco Support Diagnostics를 활성화하거나 비활성화하려면 슈퍼 관리자 또는 시스템 관리자 역할이 필요합니다.

Cisco Support Diagnostics Connector 구성

Cisco Support Diagnostics 기능을 활성화하려면 다음 단계를 수행합니다.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Network Success Diagnostics(**네트워크 성공 진단**)** > **Cisco Support Diagnostics** > **Cisco Support Diagnostics Setting(Cisco Support Diagnostics** 설정**)**으로 이동합니다.
- 이 기능은 기본적으로 비활성화되어 있습니다. 비활성화된 경우 **Enable Cisco Support Diagnostics(Cisco Support Diagnostics** 활성화**)** 확인란을 선택하여 Cisco Support Diagnostics를 활성화합니다.

Cisco Support Diagnostics 양방향 연결 확인

Cisco ISE가 Cisco Support Diagnostics에 성공적으로 등록되었는지와 Security Services Exchange 포털을 통해 양방향 연결이 설정되었는지 확인하려면 다음 단계를 수행합니다.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Audit(**감사**)** > **Change Configuration Audit(**컨피그레이션 변경 감사**)**으로 이동합니다.
- 다음과 같이 이벤트 보고서를 확인합니다.
  1. Cisco Support Diagnostics가 활성화됩니다.
  2. ISE 서버가 Cisco Support Diagnostics에 등록되었습니다.
  3. ISE SSE 서비스가 Cisco Support Diagnostics에 등록되었습니다.
  4. Cisco Support Diagnostics 양방향 연결이 활성화됩니다.

- Operations Audit(운영 감사) 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Audit(**감사**)** > **Operations Audit(**운영 감사**)**)으로 이동하여 Cisco Support Diagnostics에 구성된 활성화, 비활성화, 등록, 미등록, 기입, 미기입 서비스에 대한 세부정보를 확인해도 됩니다.

문제 해결 정보

Cisco Support Diagnostics 양방향 연결이 끊긴 것으로 표시되면 다음을 확인합니다.

- 스마트 라이선싱: 스마트 라이선싱을 비활성화하면 Cisco Support Diagnostics가 자동으로 비활성화됩니다. 스마트 라이선싱을 재활성화하여 커넥터를 활성화합니다.
- **Security Services Exchange** 클라우드에 대한 연결: Cisco Support Diagnostics가 활성화된 경우 Cisco ISE는 Security Services Exchange 포털로 설정된 영구 연결을 지속적으로 확인합니다. 이 연결이 끊어진 것으로 확인되면 "Alarms: The Cisco Support Diagnostics bi-directional connectivity is broken.(경보: Cisco Support Diagnostics 양방향 연결이 끊겼습니다.)" 경보가 트리거됩니다. 이전에 제공된 컨피그레이션 단계를 사용하여 기능을 다시 활성화하십시오.
-

관련 정보

관리자는 ERS API를 사용하여 다음과 같은 특정 작업을 수행할 수 있습니다.

- 특정 노드에서 지원 정보를 트리거합니다.
- 트리거된 지원 번들의 상태를 가져옵니다.
- 지원 번들을 다운로드합니다.
- 구축 정보를 가져옵니다.

사용 및 기타 정보는 ERS SDK 페이지를 참조하십시오.

진단 문제 해결 도구

진단 도구를 사용하면 Cisco ISE 네트워크를 진단하여 문제를 해결하고 문제 해결 방법에 대한 자세한 지침을 제공할 수 있습니다. 이러한 도구를 사용하여 인증 문제를 해결하고 Trustsec 디바이스를 포함하여 네트워크에 있는 네트워크 디바이스의 컨피그레이션을 평가할 수 있습니다.

RADIUS 인증 문제 해결 도구

이 도구를 사용하면 예기치 않은 인증 결과가 있는 경우 문제 해결을 위해 RADIUS 인증 또는 Active Directory 관련 RADIUS 인증을 검색하고 선택할 수 있습니다. 인증을 통과할 것으로 기대했지만 실패했을 경우 또는 사용자나 머신에서 특정 권한 수준을 가질 것을 예상했지만 사용자나 머신에 해당 권한이 없는 경우 이 도구를 사용하십시오.

- 문제 해결을 위해 사용자 이름, 엔드포인트 ID, NAS(Network Access Service) IP 주소 및 인증 실패 이유를 기준으로 RADIUS 인증을 검색하면 Cisco ISE에는 시스템(현재) 날짜의 인증만 표시됩니다.
- 문제 해결을 위해 NAS 포트를 기준으로 RADIUS 인증을 검색하면 Cisco ISE에는 지난달의 시작부터 현재 날짜까지 모든 NAS 포트 값이 표시됩니다.

참고 NAS IP 주소 및 엔드포인트 ID 필드를 기준으로 RADIUS 인증을 검색하면 검색은 먼저 작업 데이터베이스에서 수행된 다음 컨피그레이션 데이터베이스에서 수행됩니다.

예기치 않은 **RADIUS** 인증 결과 관련 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **RADIUS Authentication Troubleshooting(RADIUS** 인증 문제 해결**)**

단계 **2** 필요에 따라 필드에서 검색 기준을 지정합니다.

단계 **3** **Search(**검색**)**를 클릭하여 검색 기준과 일치하는 RADIUS 인증을 표시합니다.

AD 관련 인증을 검색하는 경우 구축에 Active Directory 서버가 구성되어 있지 않으면 'AD가 구성되어 있지 않음' 메시지가 표시됩니다.

단계 **4** 표에서 RADIUS 인증 기록을 선택하고 **Troubleshoot(**문제 해결**)**을 클릭합니다.

AD 관련 인증 문제를 해결해야 하는 경우 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory** > **AD node(AD** 노드**)** 아래의 진단 도구에 액세스합니다.

단계 **5** **User Input Required(**사용자 입력 필요**)**를 클릭하고 필드의 내용을 필요한 대로 수정한 후에 **Submit(**제출**)**을 클릭합니다.

단계 **6** **Done(**완료**)**을 클릭합니다.

단계 **7** 문제 해결이 완료된 후 **Show Results Summary(**결과 요약 표시**)**를 클릭합니다.

단계 **8** 진단 내용, 문제 해결을 위한 단계 및 문제 해결 요약을 확인하려면 **Done(**완료**)**을 클릭합니다.

네트워크 디바이스 명령 진단 도구 실행

네트워크 디바이스 실행 명령 진단 도구를 사용하면 네트워크 디바이스에 대해 **show** 명령을 실행할 수 있습니다.

표시되는 결과는 콘솔에 표시되는 것과 동일합니다. 이 도구를 사용하면 디바이스 컨피그레이션의 모든 문제를 식별할 수 있습니다.

네트워크 디바이스의 컨피그레이션을 확인하거나 네트워크 디바이스가 구성된 방법을 확인하려면 이 도구를 활용하면 됩니다.

네트워크 디바이스 실행 명령 진단 도구에 액세스하려면 다음 탐색 경로 중 하나를 선택하십시오.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고**Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **Execute Network Device Command(**네트워크 디바이스 명령 실행**)**를 선택합니다.
- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고**Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Troubleshoot(**문제 해결**)** > **Execute Network Device Command(**네트워크 디바이스 명령 실행**)**를 선택합니다.

표시되는 **Execute Network Device Command(**네트워크 디바이스 실행 명령**)** 창에서 해당 필드에 실행할 네트워크 디바이스의 IP 주소와 show 명령을 입력합니다. **Run(**실행**)**을 클릭합니다.

구성 확인을 위해 **Cisco IOS** 표시 명령 실행

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Execute Network Device Command(**네트워크 디바이스 명령 실행**)**.

단계 **2** 해당 필드에 정보를 입력합니다.

단계 **3** **Run(**실행**)**을 클릭하여 지정한 네트워크 디바이스에서 명령을 실행합니다.

단계 **4** **User Input Required(**사용자 입력 필요**)**를 클릭하고 필드의 내용을 필요한 대로 수정합니다.

단계 **5** **Submit(**제출**)**을 클릭하여 네트워크 디바이스에서 명령을 실행하고 출력을 확인합니다.

컨피그레이션 검증기 평가 도구

이 진단 도구를 사용하여 네트워크 디바이스의 컨피그레이션을 평가하고 컨피그레이션 문제를 모두 식별할 수 있습니다. Expert Troubleshooter는 디바이스의 컨피그레이션을 표준 컨피그레이션과 비교합니다.

에이전트리스 포스처 문제 해결

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

다음 두 위치에서 에이전트리스 포스처 문제 해결에 액세스할 수 있습니다.

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

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

보고서

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

네트워크 디바이스 컨피그레이션 문제 해결

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고**Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Evaluate Configuration Validator(**구성 검증기 평가**)**를 선택합니다.

단계 **2** 구성을 평가할 네트워크 디바이스의 IP 주소를 **Network Device IP(**네트워크 디바이스 **IP)** 필드에 입력합니다.

단계 **3** 확인란을 선택하고 권장 템플릿과 비교할 구성 옵션 옆의 라디오 버튼을 클릭합니다.

단계 **4** **Run(**실행**)**을 클릭합니다.

단계 **5** 표시되는 **Progress Details...(**진행 세부정보**)** 영역에서 **Click Here to Enter Credentials(**여기를 클릭하여 자격 증명 입력**)**를 클릭합니다. **Credentials Window(**자격 증명 창**)** 대화 상자에서 네트워크 디바이스와의 연결을 설정하는 데 필요한 연결 매개변수 및 자격 증명을 입력하고 **Submit(**제출**)**를 클릭합니다

워크플로우를 취소하려면 **Progress Details...(**진행 세부정보**...)** 창에서 **Click Here to Cancel the Running Workflow(**여기를 클릭하여 실행 중인 워크플로우 취소**)**를 클릭합니다.

단계 **6** 분석할 인터페이스 옆의 확인란을 선택하고 **Submit(**제출**)**을 클릭합니다.

단계 **7** 구성 평가에 대한 자세한 내용을 보려면 **Show Results Summary(**결과 요약 표시**)**를 클릭합니다.

엔드포인트 포스처 장애 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Posture Troubleshooting(**포스처 문제 해결**)**을 선택합니다.

단계 **2** 해당 필드에 정보를 입력합니다.

단계 **3** **Search(**검색**)**를 클릭합니다.

단계 **4** 이벤트에 대한 설명을 찾고 해결책을 확인하려면 목록에서 이벤트를 선택하고 **Troubleshoot(**문제 해결**)**을 클릭합니다.

세션 추적 테스트 케이스

이 툴을 사용하면 정책 플로우를 예측 가능한 방식으로 테스트하여 실제 트래픽을 실제 디바이스에서 생성할 필요 없이 정책이 구성된 방식을 확인하고 검증할 수 있습니다.

테스트 사례에 사용할 속성 및 해당 값의 목록을 구성할 수 있습니다. 이러한 세부정보는 정책의 런타임 호출을 시뮬레이션하기 위해 정책 시스템과의 상호 작용을 수행하는 데 사용됩니다.

사전을 사용하여 속성을 구성할 수 있습니다. 단순 RADIUS 인증에 적용 가능한 모든 사전이 **Attributes(**속성**)** 필드에 나열됩니다.

참고 단순 RADIUS 인증에 대해서만 테스트 케이스를 구성할 수 있습니다.

세션 추적 테스트 케이스 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Troubleshoot(**문제 해결**) > Diagnostic Tools(**진단 도구**) > General Tools(**일반 도구**) > Session Trace Test Cases(**세션 추적 테스트 케이스**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Test Details(**테스트 세부정보**)** 탭에서 테스트 케이스의 이름과 설명을 입력합니다.

단계 **4** 사전 정의된 테스트 케이스 중 하나를 선택하거나 필수 속성 및 해당 값을 구성합니다. 다음과 같은 미리 정의된 테스트 케이스를 사용할 수 있습니다.

- 기본 인증 액세스
- 프로파일링된 Cisco 폰
- 호환되는 디바이스 액세스
- Wi-Fi 게스트(리디렉션)
- Wi-Fi 게스트(액세스)

미리 정의된 테스트 케이스를 선택하면 Cisco ISE가 테스트 케이스의 관련 속성을 자동으로 채웁니다. 이러한 속성에 기본값을 사용하거나 표시된 옵션에서 원하는 값을 선택할 수 있습니다. 테스트 케이스에 사용자 맞춤화 속성을 더 추가할 수도 있습니다.

테스트 케이스에 추가하는 속성 및 값은 Text(텍스트) 필드에 나열됩니다(Custom Attributes(사용자 맞춤화 속성) 필드 아래). Text(텍스트) 필드에서 콘텐츠를 편집하면 Cisco ISE에서 업데이트된 콘텐츠의 유효성과 syntax(명령문)를 확인합니다.

Test Details(테스트 세부정보) 페이지 하단에서 모든 속성의 요약을 볼 수 있습니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

Cisco ISE는 테스트 세부정보를 저장하기 전에 속성 및 해당 값을 검증하고 오류가 있는 경우 이를 표시합니다.

단계 **6** **Test Visualizer(**시각화 테스트**)** 탭에서 이 테스트 케이스를 실행할 노드를 선택합니다.

참고 정책 서비스 페르소나가 있는 노드만 **ISE Node(ISE** 노드**)** 드롭다운 목록에 표시됩니다.

User Groups/Attributes(사용자 그룹/속성**)**를 클릭하여 외부 ID 저장소에서 사용자의 그룹 및 속성을 검색합니다.

단계 **7** **Execute(**실행**)**를 클릭합니다.

Cisco ISE는 테스트 케이스를 실행하고 테스트 케이스의 단계별 결과를 표 형식으로 나타냅니다. 정책 단계, 일치 규칙 및 결과 개체가 표시됩니다. 각 단계의 세부정보를 보려면 녹색 아이콘을 클릭합니다.

단계 **8** 이전 테스트 실행의 결과를 보려면 **Previous Test Executions(**이전 테스트 실행**)** 탭을 클릭합니다. 또한 두 개의 테스트 케이스를 선택하고 비교할 수 있습니다. Cisco ISE는 각 테스트 케이스의 속성에 대한 비교 보기를 표 형식으로 표시합니다.

RADIUS Live Logs(RADIUS 라이브 로그) 페이지에서 세션 추적 테스트 케이스 툴을 시작할 수 있습니다. Live Logs(라이브 로그) 페이지에서 항목을 선택하고 Actions(작업) 아이콘(Details(세부정보) 열)을 클릭하여 세션 추적 테스트 케이스 툴을 시작할 수 있습니다. Cisco ISE는 해당 로그 항목에서 관련 속성 및 해당 값을 추출합니다. 필요한 경우 이러한 속성 및 값을 수정하고 테스트 케이스를 실행할 수 있습니다.

고급 문제 해결을 위한 기술 지원 터널

Cisco ISE는 Cisco IronPort Tunnel 인프라를 사용하여 Cisco 기술 지원 엔지니어가 ISE 서버에 연결해 시스템의 문제를 해결할 수 있는 보안 터널을 생성합니다. Cisco ISE는 SSH를 사용하여 터널을 통한 보안 연결을 생성합니다.

관리자는 터널 액세스를 제어할 수 있습니다. 즉, 지원 엔지니어에게 액세스 권한을 부여할 시기와 기간을 선택할 수 있습니다. Cisco 고객 지원에서는 사용자 개입 없이 터널을 설정할 수 없습니다. 서비스 로그인에 대한 알림이 수신됩니다. 언제든지 터널 연결을 비활성화할 수 있습니다. 기본적으로 기술 지원 터널은 72시간 동안 열려 있습니다. 기본적으로 기술 지원 터널은 72시간 동안 열려 있지만 모든 문제해결 작업이 완료되면 관리자나 지원 엔지니어가 터널을 닫는 것이 좋습니다. 필요한 경우 터널 오픈 기간을 72시간보다 길게 연장하도록 선택할 수 있습니다.

tech support-tunnel enable 명령을 사용하여 터널 연결을 시작합니다.

tech support-tunnel status 명령은 연결 상태를 표시합니다. 이 명령은 연결 설정 여부, 인증 장애 발생 여부 또는 서버에 연결할 수 없는지 여부에 대한 정보를 제공합니다. 터널 서버에 연결할 수는 있지만 ISE가 인증을 할 수 없으면 ISE는 30분 동안 5분마다 다시 인증을 시도하며 그 후에는 터널이 비활성화됩니다.

tech support-tunnel disable 명령을 사용하여 터널 연결을 비활성화할 수 있습니다. 이 명령을 실행하면 지원 엔지니어가 현재 로그인되어 있어도 기존 터널의 연결이 끊깁니다.

ISE 서버에서 터널 연결을 이미 설정한 경우에는 생성된 SSH 키를 ISE 서버에서 사용할 수 있습니다. 나중에 지원 터널을 활성화하려고 하면 이전에 생성되었던 SSH 키를 재사용할지를 묻는 메시지가 표시됩니다. 같은 키를 사용하거나 새 키를 생성하도록 선택할 수 있습니다. 또한 **tech support-tunnel resetkey** 명령을 사용하여 키를 수동으로 재설정할 수도 있습니다. 터널 연결이 활성화되어 있을 때 이 명령을 실행하면 연결을 먼저 비활성화하라는 메시지가 표시됩니다. 기존 연결을 비활성화하지 않고 계속 사용하도록 선택하면 기존 연결이 비활성화된 후에 키가 재설정됩니다. 연결을 비활성화하도록 선택하면 터널 연결이 끊기고 키가 즉시 재설정됩니다.

터널 연결을 설정한 후에는 **tech support-tunnel extend** 명령을 사용하여 연결을 연장할 수 있습니다.

tech support-tunnel 명령의 사용 지침은 CCisco Identity Services Engine CLI Reference Guide를 참고하십시오.

기술 지원 터널 설정

Cisco ISE CLI(Command Line Interface)를 통해 보안 터널을 설정할 수 있습니다.

단계 **1** Cisco ISE CLI에서 다음 명령을 입력합니다.

tech support-tunnel enable

시스템에서 터널의 비밀번호와 별칭을 입력하라는 메시지를 표시합니다.

단계 **2** 비밀번호를 입력합니다.

단계 **3** (선택 사항) 터널의 별칭을 입력합니다.

시스템에서 SSH 키를 생성하고 비밀번호, 디바이스 일련 번호 및 SSH 키를 표시합니다. 지원 엔지니어가 시스템에 연결할 수 있도록 이 정보를 Cisco 고객 지원에 전달해야 합니다.

단계 **4** 비밀번호, 디바이스 일련 번호 및 SSH 키를 복사하여 Cisco 고객 지원에 전송합니다.

이제 지원 엔지니어가 ISE 서버에 안전하게 연결할 수 있습니다. 서비스 로그인에 대한 정기 알림이 수신됩니다.

들어오는 트래픽을 검증하는 **TCP** 덤프 유틸리티

TCP 덤프 유틸리티는 패킷을 스니핑합니다. 이 패킷을 사용하여 예상 패킷이 노드에 도달했는지 확인할 수 있습니다. 예를 들어 보고서에 들어오는 인증 또는 로그인이 나타나 있지 않은 경우 들어오는 트래픽이 없거나 들어오는 트래픽이 Cisco ISE에 도달되지 않는다는 의심이 있을 수 있습니다. 이 경우 이 도구를 실행하여 검증할 수 있습니다.

네트워크 문제를 해결하는 데 도움이 되도록 TCP 덤프 옵션을 구성한 다음 네트워크 트래픽에서 데이터를 수집할 수 있습니다.

TCP 덤프를 사용하여 네트워크 트래픽 모니터링

TCP Dump(TCP 덤프) 페이지에는 생성한 TCP 덤프 프로세스 파일이 나열됩니다. 다양한 용도로 다른 파일을 생성하고 필요에 따라 실행한 다음, 필요하지 않은 경우 삭제할 수 있습니다.

크기, 파일 수 및 프로세스 실행 기간을 지정하여 수집되는 데이터를 제어할 수 있습니다. 프로세스가 제한 시간 전에 완료되고 최대 크기보다 작은 파일 둘 이상을 활성화한 경우 프로세스가 계속 진행되고 다른 덤프 파일이 생성됩니다.

결합된 인터페이스를 포함하여 더 많은 인터페이스에서 TCP 덤프를 실행할 수 있습니다.

사람이 읽을 수 있는 형식은 더 이상 옵션으로 제공되지 않으며, 덤프 파일은 항상 원시 형식입니다.

저장소에 대한 IPv6 연결을 지원합니다.

시작하기 전에

TCP Dump(TCP 덤프) 페이지의 Network Interface(네트워크 인터페이스) 드롭다운 목록에는 IPv4 또는 IPv6 주소가 구성되어 있는 NIC(Network Interface Cards)만 표시됩니다. 기본적으로 VMware에서는 모든 NIC가 연결되어 있으므로 모든 NIC에 IPv6 주소가 있으며 네트워크 인터페이스 드롭다운 목록에 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **TCP Dump(TCP** 덤프**)**.

단계 **2** TCP 덤프 유틸리티의 소스로 **Host Name(**호스트 이름**)**을 선택합니다.

단계 **3** 드롭다운 목록에서 모니터링할 네트워크 인터페이스를 선택합니다.

단계 **4** Filter(필터) 필드에 필터링할 부울 식을 입력합니다.

다음과 같은 표준 tcpdump 필터 식이 지원됩니다.

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 및 not 10.77.122.119

단계 **5** 이 TCP 덤프 프로세스의 파일 이름을 입력합니다.

단계 **6** TCP 덤프 로그 파일을 저장할 저장소를 선택합니다.

단계 **7** **File Size(**파일 크기**)** - 최대 파일 크기를 선택합니다.

덤프가 이 파일 크기를 초과하면 새 파일이 열려 덤프를 계속합니다. 덤프가 새 파일을 계속 사용할 수 있는 횟수는 **Limit to(**다음으로 제한**)** 설정을 기준으로 제한됩니다.

단계 **8** **Limit to(**다음으로 제한**)** - 덤프가 확장할 수 있는 파일의 수를 제한합니다.

단계 **9** **Time Limit(**시간 제한**)** - 종료 전에 덤프가 실행되는 기간을 구성합니다.

단계 **10** 라디오 버튼을 클릭해 On(켜기) 또는 Off(끄기)로 설정하여 Promiscuous Mode(무차별 모드)를 설정합니다. 기본값은 On(켜기)입니다.

무차별 모드는 네트워크 인터페이스가 시스템 CPU로 모든 트래픽을 전달하는 기본 패킷 스니핑 모드입니다. 이 모드는 On(켜기)으로 설정해 두는 것이 좋습니다.

참고 Cisco ISE는 1500MTU(점보 프레임)보다 큰 프레임을 지원하지 않습니다.

TCP 덤프 파일 저장

시작하기 전에

TCP 덤프를 사용하여 네트워크 트래픽 모니터링 섹션의 설명에 따라 작업을 정상적으로 완료한 상태여야 합니다.

참고 Cisco ISE CLI를 통해 TCP Dump에 액세스할 수도 있습니다. 자세한 내용은 *Cisco Identity Services Engine CLI Reference Guide*를 참고해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **TCP Dump(TCP** 덤프**)**.

단계 **2** **Format(**형식**)** 드롭다운 목록에서 옵션을 선택합니다. **Human Readable(**사람이 읽을 수 있음**)**이 기본값입니다.

단계 **3** **Download(**다운로드**)**를 클릭하고 원하는 위치로 이동한 후에 **Save(**저장**)**를 클릭합니다.

단계 **4** 이전 덤프 파일을 먼저 저장하지 않고 제거하려면 **Delete(**삭제**)**를 클릭합니다.

엔드포인트 또는 사용자의 예기치 않은 SGACL 비교

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **TrustSec Tools(TrustSec** 도구**)** > **Egress (SGACL) Policy(**이그레스**(SGACL)** 정책**)**.

단계 **2** SGACL 정책을 비교할 TrustSec 디바이스의 네트워크 디바이스 IP 주소를 입력합니다.

단계 **3** **Run(**실행**)**을 클릭합니다.

단계 **4** **User Input Required(**사용자 입력 필요**)**를 클릭하고 필드의 내용을 필요한 대로 수정합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** **Show Results Summary(**결과 요약 표시**)**를 클릭하여 진단 및 제안 해결 단계를 확인합니다.

이그레스 정책 진단 흐름

이그레스 정책 진단 도구는 비교를 위해 다음 표에서 설명하는 프로세스를 사용합니다.

프로세스 단계	설명
1	사용자가 입력한 IP 주소에 디바이스를 연결하고 각 소스 및 대상 SGT 페어에 대해 ACL(Access Control List, 액세스 제어 목록)을 가져옵니다.
2	Cisco ISE에 구성되어 있는 이그레스 정책을 확인하고 각 소스 및 대상 SGT 쌍에 대해 ACL을 가져옵니다.
3	Cisco ISE에서 가져온 SGACL 정책과 네트워크 디바이스에서 가져온 SGACL 정책을 비교합니다.
4	SGACL이 일치하지 않으면 소스 및 대상 SGT 쌍을 표시합니다. 또한 일치하는 엔트리도 추가 정보로 표시합니다.

SXP-IP 매핑을 사용하여 **TrustSec**이 활성화된 네트워크의 연결 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **Trustsec Tools(TrustSec** 도구**)** > **SXP-IP Mappings(SXP-IP** 매핑**)**.

단계 **2** 네트워크 디바이스의 IP 주소를 입력합니다.

단계 **3** **Select(**선택**)**를 클릭합니다.

단계 **4** **Run(**실행**)**, **User Input Required(**사용자 입력 필요**)**를 차례로 클릭하고 필요한 필드를 수정합니다.

Expert Troubleshooter가 네트워크 디바이스에서 TrustSec SXP 연결을 검색하며, 피어 SXP 디바이스를 선택하라는 메시지가 다시 표시됩니다.

단계 **5** **User Input Required(**사용자 입력 필요**)**를 클릭하고 필요한 정보를 입력합니다.

단계 **6** SXP 매핑을 비교할 피어 SXP 디바이스의 확인란을 선택하고 일반 연결 매개변수를 입력합니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

단계 **8** **Show Results Summary(**결과 요약 표시**)**를 클릭하여 진단 및 해결 단계를 확인합니다.

IP-SGT 매핑을 사용하여 **TrustSec**이 활성화된 네트워크의 연결 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **TrustSec Tools(TrustSec** 도구**)** > **IP User SGT(IP** 사용자 **SGT)**를 선택합니다.

단계 **2** 필요에 따라 필드에 정보를 입력합니다.

단계 **3** **Run(**실행**)**을 클릭합니다.

추가 입력을 요청하는 메시지가 표시됩니다.

단계 **4** **User Input Required(**사용자 입력 필요**)**를 클릭하고 필드의 내용을 필요한 대로 수정합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** **Show Results Summary(**결과 요약 표시**)**를 클릭하여 진단 및 해결 단계를 확인합니다.

디바이스 **SGT** 도구

Trustsec 솔루션에서 활성화된 디바이스의 경우 각 네트워크 디바이스는 RADIUS 인증을 통해 SGT 값이 할당됩니다. 디바이스 SGT 진단 도구는 네트워크 디바이스(관리자가 제공하는 IP 주소 사용)에 연결하여 네트워크 디바이스 SGT 값을 얻습니다. 그런 다음 RADIUS 인증 기록에서 가장 최근에 할당된 SGT 값을 확인합니다. 마지막으로 디바이스-SGT 쌍이 테이블 형식으로 표시되며 SGT 값이 동일한지, 아니면 다른지 나타냅니다.

디바이스 **SGT** 매핑을 비교하여 **TrustSec**이 활성화된 네트워크의 연결 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **TrustSec Tools(TrustSec** 도구**)** > **Device SGT(**디바이스 **SGT)**

단계 **2** 필요에 따라 필드에 정보를 입력합니다.

텔넷의 기본 포트 번호는 23이고 SSH의 기본 포트 번호는 22입니다.

단계 **3** **Run(**실행**)**을 클릭합니다.

단계 **4** **Show Results Summary(**결과 요약 표시**)**를 클릭하여 디바이스 SGT 비교 결과를 확인합니다.

추가 문제 해결 정보 얻기

Cisco ISE에서는 관리 포털에서 지원 및 문제 해결 정보를 다운로드할 수 있습니다. 지원 번들을 사용하면 Cisco TAC(Technical Assistance Center)가 Cisco ISE의 문제 해결을 위한 진단 정보를 준비할 수 있습니다.

참고 TAC용 고급 문제 해결 정보를 제공하는 지원 번들과 디버그 로그는 해석하기가 어렵습니다. Cisco ISE에서 제공하는 다양한 보고서 및 문제 해결 도구를 사용하여 네트워크에서 발생하는 문제를 진단하고 해결할 수 있습니다.

Cisco ISE 지원 번들

지원 번들에 포함시킬 로그를 구성할 수 있습니다. 예를 들어 디버그 로그에 포함되도록 특정 서비스의 로그를 구성할 수 있습니다. 날짜를 기준으로 로그를 필터링할 수도 있습니다.

다운로드할 수 있는 로그는 다음과 같이 분류될 수 있습니다.

- 전체 구성 데이터베이스: 사람이 읽을 수 있는 XML 형식의 Cisco ISE 구성 데이터베이스를 포함합니다. 문제를 해결할 때 이 데이터베이스 구성을 다른 Cisco ISE 노드로 가져와 시나리오를 다시 생성할 수 있습니다.
- 디버그 로그: 부트스트랩, 애플리케이션 구성, 런타임, 구축, PKI(Public Key Infrastructure) 정보와 모니터링 및 보고 로그를 캡처합니다.

  디버그 로그는 특정 Cisco ISE 구성 요소에 대한 문제 해결 정보를 제공합니다. 디버그 로그를 사용하려면 11장, "로깅"을 참고해 주십시오. 디버그 로그를 사용하지 않으면 모든 정보 메시지(INFO)가 지원 번들에 포함됩니다. 자세한 내용은 Cisco ISE 디버그 로그, 1366 페이지를 참고하십시오.
- 로컬 로그: Cisco ISE에서 실행되는 다양한 프로세스의 시스템 로그 메시지를 포함합니다.
- 코어 파일: 크래시의 원인을 식별하는 데 도움이 되는 중요한 정보를 포함합니다. 이 로그는 애플리케이션이 크래시될 때 생성되며 힙 덤프를 포함합니다.
- 모니터링 및 보고 로그: 알림 및 보고서에 대한 정보를 포함합니다.
- 시스템 로그: Cisco ADE(Application Deployment Engine) 관련 정보를 포함합니다.
- 정책 구성: Cisco ISE에서 사람이 읽을 수 있는 형식으로 구성된 정책을 포함합니다.

Cisco ISE CLI에서 **backup-logs** 명령을 사용하여 이러한 로그를 다운로드할 수 있습니다. 자세한 내용은 *Cisco Identity Services Engine CLI Reference Guide*를 참고해 주십시오.

참고 인라인 포스처 노드의 경우 관리 포털에서 지원 번들을 다운로드할 수 없습니다. Cisco ISE CLI에서 **backup-logs** 명령을 사용해야 합니다.

관리 포털에서 이러한 로그를 다운로드하도록 선택하는 경우 다음과 같이 해 주십시오.

- 디버그 로그 또는 시스템 로그 등의 로그 유형에 따라 로그 하위 집합만 다운로드합니다.
- 선택한 로그 유형에 대한 마지막 *n* 번호 파일만 다운로드합니다. 이 옵션을 사용하면 지원 번들의 크기와 다운로드에 소요되는 시간을 제어할 수 있습니다.

모니터링 로그는 모니터링, 보고 및 문제 해결 기능에 대한 정보를 제공합니다. 로그 다운로드에 대한 자세한 내용은 Cisco ISE 로그 파일 다운로드, 1365 페이지를 참고하십시오.

지원 번들

지원 번들을 단순 tar.gpg 파일로 로컬 컴퓨터에 다운로드할 수 있습니다. 지원 번들은 ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg 형식으로 날짜 및 타임스탬프를 사용하여 이름이 지정됩니다. 브라우저에서 지원 번들을 적절한 위치에 저장하도록 메시지를 표시합니다. 지원 번들 콘텐츠를 추출하여 README.TXT 파일을 볼 수 있습니다. 이 파일에는 지원 번들의 콘텐츠와 함께 지원 번들에 포함되어 있는 ISE 데이터베이스의 콘텐츠를 가져오는 방법이 설명되어 있습니다.

Cisco ISE 로그 파일 다운로드

네트워크에서 문제를 해결하는 동안 자세한 정보를 확인하기 위해 Cisco ISE 로그 파일을 다운로드할 수 있습니다.

설치 및 업그레이드 문제를 해결하기 위해 ADE-OS가 포함된 시스템 로그 및 기타 로그 파일을 다운로드할 수도 있습니다.

지원 번들을 다운로드하는 동안 암호화 키를 수동으로 입력하는 대신 이제 암호화를 위한 공개 키를 사용하도록 선택할 수 있습니다. 이 옵션을 선택하면 지원 번들 암호화 및 암호 해독에 Cisco PKI가 사용됩니다. Cisco TAC에서 공개 키와 개인 키를 유지 관리합니다. Cisco ISE는 공개 키를 사용하여 지원 번들을 암호화합니다. Cisco TAC는 개인 키를 사용하여 지원 번들을 암호 해독할 수 있습니다. 문제 해결을 위해 Cisco TAC에 지원 번들을 제공하려면 이 옵션을 사용합니다. 문제를 온프레미스(구내 장비)에서 문제 해결하려는 경우에는 공유 키 암호화를 사용합니다.

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자 권한이 있어야 합니다.
- 디버그 로그 및 디버그 로그 레벨을 구성해야 합니다.

단계 **1** **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)** > **Appliance node list(**어플라이언스 노드 목록**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)** > **Appliance node list(**어플라이언스 노드 목록**)**.

단계 **3** 지원 번들을 다운로드할 노드를 클릭합니다.

단계 **4** **Support Bundle(**지원 번들**)** 탭에서 지원 번들에 입력할 매개변수를 선택합니다.

모든 로그를 포함하는 경우 지원 번들이 매우 커지며 다운로드 시간이 오래 걸립니다. 다운로드 프로세스를 최적화하려면 최근 *n*개 파일만 다운로드하도록 선택합니다.

단계 **5** 지원 번들을 생성할 시작 및 종료 날짜를 입력합니다.

단계 **6** 다음 중 하나를 선택합니다.

- Public Key Encryption(공개 키 암호화): 문제 해결을 위해 Cisco TAC에 지원 번들을 제공하려면 이 옵션을 선택합니다.

- Shared Key Encryption(공유 키 암호화): 온프레미스에서 로컬로 문제를 해결하려는 경우 이 옵션을 선택합니다. 이 옵션을 선택하는 경우 지원 번들의 암호화 키를 입력해야 합니다.

단계 **7** 지원 번들용 암호화 키를 입력하고 한 번 더 입력합니다.

단계 **8** **Create Support Bundle(**지원 번들 생성**)**을 클릭합니다.

단계 **9** **Download(**다운로드**)**를 클릭하여 새로 생성한 지원 번들을 다운로드합니다.

지원 번들은 애플리케이션 브라우저를 실행 중인 클라이언트 시스템에 다운로드되는 tar.gpg 파일입니다.

다음에 수행할 작업

특정 구성 요소에 대한 디버그 로그를 다운로드합니다.

Cisco ISE 디버그 로그

디버그 로그는 다양한 Cisco ISE 구성 요소에 대한 문제 해결 정보를 제공합니다. 디버그 로그에는 최근 30일 내에 생성된 위험 및 경고 경보와 함께 최근 7일 내에 생성된 정보 경보가 포함됩니다. 문제를 보고하는 동안 이러한 디버그 로그를 사용하고 문제 진단 및 확인을 위해 해당 로그를 보낼지 묻는 메시지가 표시될 수 있습니다.

참고 디버그 로그의 모니터링 등 로드가 많은 디버그 로그를 활성화하면 높은 로드에 대한 경보가 생성될 수 있습니다.

디버그 로그 가져오기

단계 **1** 디버그 로그를 가져올 구성 요소를 구성합니다.

단계 **2** 디버그 로그를 다운로드합니다.

Cisco ISE 구성 요소 및 해당 디버그 로그

표 ***185:*** 구성 요소 및 해당 디버그 로그

구성 요소	디버그 로그
Active Directory	ad_agent.log
Cache Tracker	tracking.log
EDF(Entity Definition Framework)	edf.log
JMS	ise-psc.log
License	ise-psc.log

구성 요소	디버그 로그
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
client	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
게스트 액세스 관리자	guest.log
게스트 액세스	guest.log
MyDevices	guest.log
포털	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log

구성 요소	디버그 로그
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

기능별 디버그 마법사 설정

디버그 마법사에는 Cisco ISE 노드의 문제를 해결하는 데 사용할 수 있는 디버그 템플릿이 포함되어 있습니다. 디버그 프로파일 및 디버그 로그를 구성 할 수 있습니다.

Debug Profile Configuration(디버그 프로파일 컨피그레이션**)** 창에서 템플릿 내부의 개별 구성 요소에 대한 디버그 로그 심각도 레벨을 구성할 수 있습니다.

Debug Profile Configuration(디버그 프로파일 컨피그레이션**)** 창에서 디버그 로그의 심각도 레벨을 구성할 수 있습니다. 디버그 로그에서는 부트스트랩, 애플리케이션 컨피그레이션, 런타임, 구축, 모니터링, 보고 및 PKI(Public Key Infrastructure) 정보를 캡처합니다.

참고

- 노드별 로그 레벨은 디버그 마법사 프로파일보다 우선합니다.
- 동일한 구성 요소를 편집하는 여러 프로파일을 활성화할 때는 추적의 우선 순위가 가장 높은 경우에 로그 레벨이 높을수록 우선 순위가 높습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Debug Wizard(**디버그 마법사**)** > **Debug Profile Configuration(**디버그 프로파일 컨피그레이션**)**에서 디버그 프로파일을 구성할 수 있습니다.

단계 **2** 새 프로파일을 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 **3** 새 프로파일의 **Name(**이름**)**과 **Description(**설명**)**을 입력합니다.
프로파일에 포함할 구성 요소 옆의 확인란을 선택하고 각 구성 요소에 대해 해당하는 **Log Level(**로그 레벨**)**을 설정합니다.

단계 **4** **Save(**저장**)**를 클릭하여 프로파일을 저장합니다.

단계 **5** ISE 노드를 즉시 활성화하려면 **Enable(**활성화**)**을 클릭합니다. 그렇지 않은 경우 **Do it Later(**나중에**)**를 클릭합니다.

단계 **6** **Enable(**활성화**)**을 클릭하는 경우, 프로파일을 활성화하려는 ISE 노드 옆의 확인란을 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Debug Wizard(**디버그 마법사**)** > **Debug Profile Configuration(**디버그 프로파일 컨피그레이션**)**에서 디버그 로그를 구성할 수 있습니다.

단계 **9** 라디오 버튼을 클릭하여 노드를 선택합니다.

단계 **10** 라디오 버튼을 클릭하여 구성 요소를 선택하고 **Edit(**편집**)**를 클릭하여 구성 요소의 **Component Name(**구성 요소 이름**)**, **Log Level(**로그 레벨**)**, **Description(**설명**)** 및 **Log File Name(**로그 파일 이름**)**을 변경합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

디버그 로그 다운로드

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)** > **Appliance node list(**어플라이언스 노드 목록**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)** > **Appliance node list(**어플라이언스 노드 목록**)**.

단계 **3** Appliance node(어플라이언스 노드) 목록에서 디버그 로그를 다운로드할 노드를 클릭합니다.

단계 **4** **Debug Logs(**디버그 로그**)** 탭을 클릭합니다.

디버그 로그 유형 및 디버그 로그의 목록이 표시됩니다. 이 목록은 디버그 로그 컨피그레이션을 기반으로 합니다.

단계 **5** 다운로드하려는 로그 파일을 클릭하여 클라이언트 브라우저를 실행 중인 시스템에 저장합니다.

필요에 따라 이 프로세스를 반복하여 다른 로그 파일을 다운로드할 수 있습니다. **Debug Logs(**디버그 로그**)** 창에서 다운로드할 수 있는 추가 디버그 로그는 다음과 같습니다.

- isebootstrap.log: 부트스트래핑 로그 메시지를 제공합니다.
- monit.log: Watchdog 메시지를 제공합니다.
- pki.log: 타사 암호화 라이브러리 로그를 제공합니다.

- iseLocalStore.log: 로컬 저장소 파일에 대한 로그를 제공합니다.
- ad_agent.log: Microsoft Active Directory 타사 라이브러리 로그를 제공합니다.
- catalina.log: 타사 로그를 제공합니다.