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 ***1:*** 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.

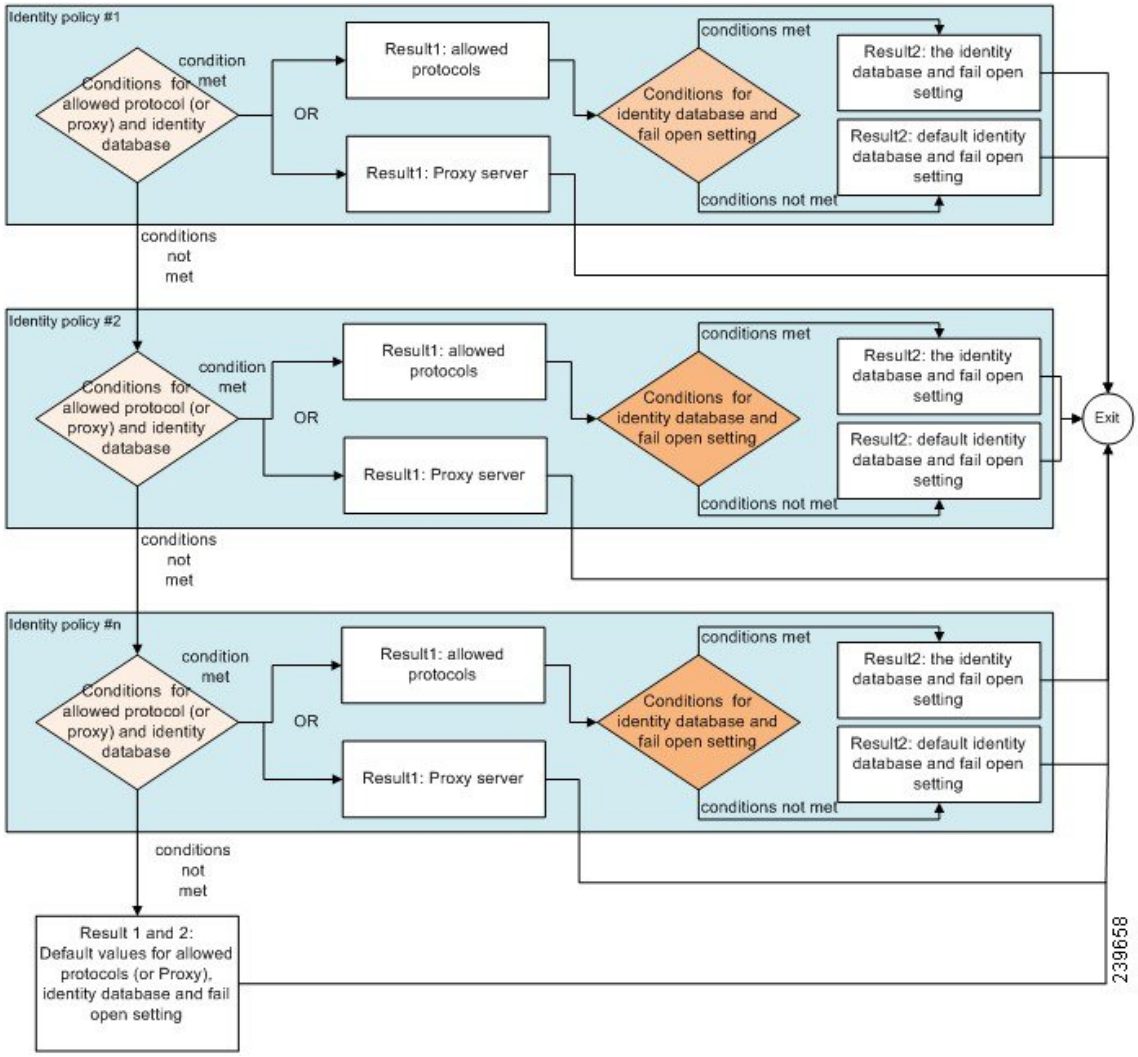
인증 정책 플로우

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 *1:* 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, 8 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, 28 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 *2:* 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, 16 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, 21 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, 28 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, 126 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 *3:* 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, 16 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, 13 페이지
권한 부여 프로파일에 대한 권한, 13 페이지
미등록 디바이스 리디렉션을 위한 권한 부여 프로파일 구성
권한 부여 프로파일 생성

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, 19 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, 21 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 , 48 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 ***4: 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, 34 페이지
사용자 맞춤화 사전 및 사전 속성, 34 페이지
RADIUS 벤더 사전, 35 페이지
RADIUS 벤더 사전 생성, 36 페이지

Condition Studio 탐색

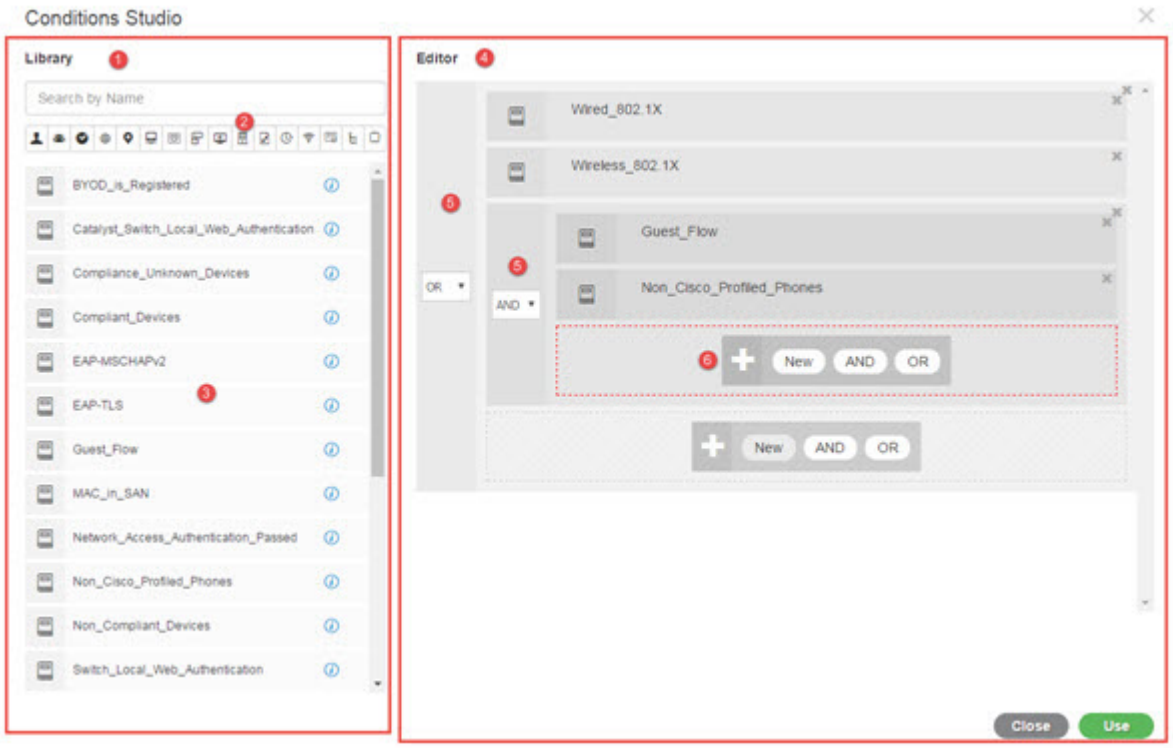
Conditions Studio를 사용하여 조건을 생성, 관리 및 재사용합니다. 조건은 둘 이상의 규칙을 포함할 수 있으며, 하나의 레벨만 포함하거나 여러 계층 레벨을 포함하는 다양한 수준의 복잡성으로 구축할 수 있습니다. Conditions Studio를 사용하여 새 조건을 생성할 경우, 이미 라이브러리에 저장한 조건 블록을 사용할 수 있으며 저장된 조건 블록을 업데이트하고 변경할 수도 있습니다. 나중에 조건을 생성 및 관리하는 동안 빠른 카테고리 필터 등을 사용하여 필요한 블록 및 속성을 쉽게 찾을 수 있습니다.

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 ***2: 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.

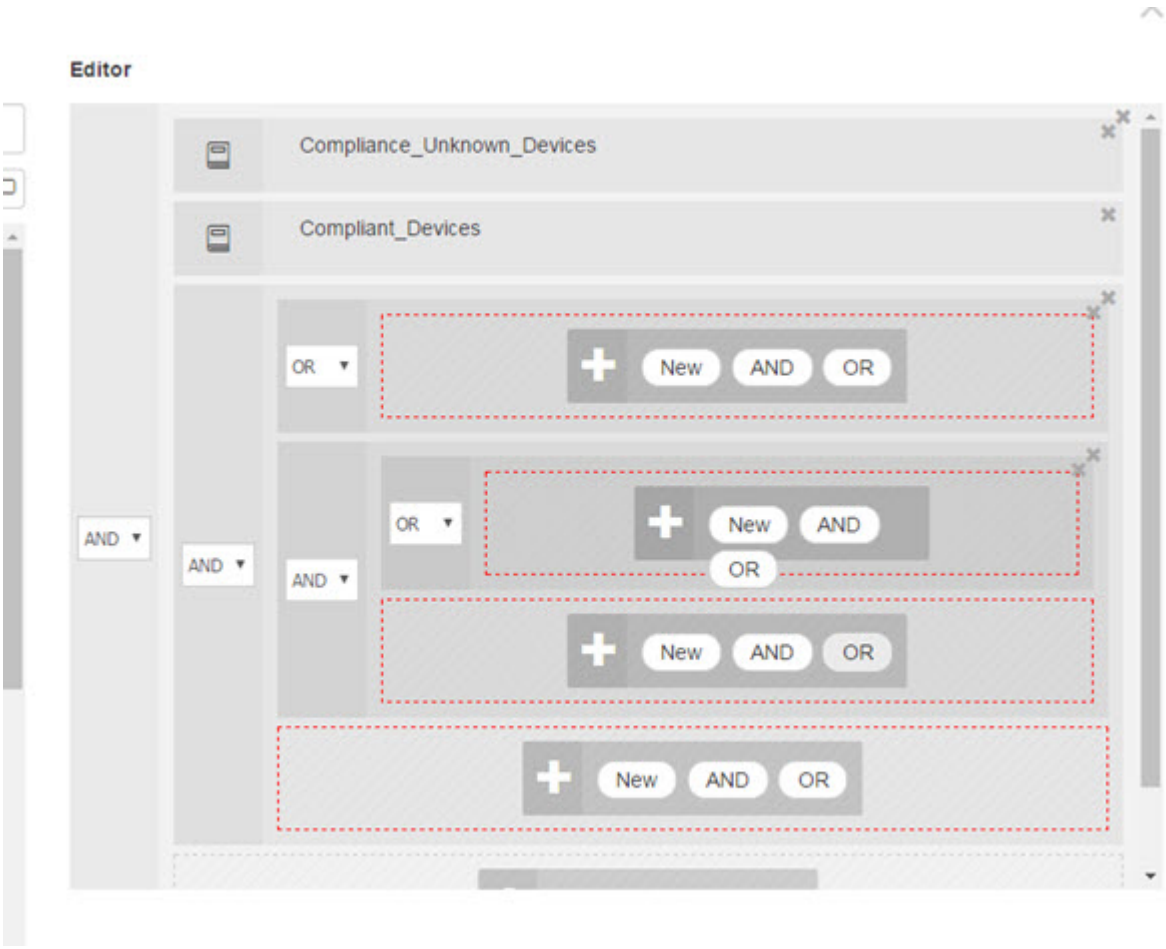
필드	사용 지침
편집기	즉시 사용할 수 있도록 새 조건을 생성하고 나중에 사용할 수 있도록 시스템 라이브러리에 저장하고, 기존 조건을 편집하여 즉시 및 향후 사용을 위해 라이브러리에 변경 사항을 저장합니다. 새 조건을 생성하기 위해 Conditions Studio를 열면 (정책 집합 표에서 더하기 기호 클릭), 첫 번째 규칙을 추가할 수 있는 빈 줄 하나만 편집기에 나타납니다. 필드가 비어 있는 편집기가 열리면 연산자 아이콘이 표시되지 않습니다.
	편집기는 다양한 가상 열과 행으로 나뉩니다. 열은 서로 다른 계층 레벨을 나타내며 각 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 **3:** 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.

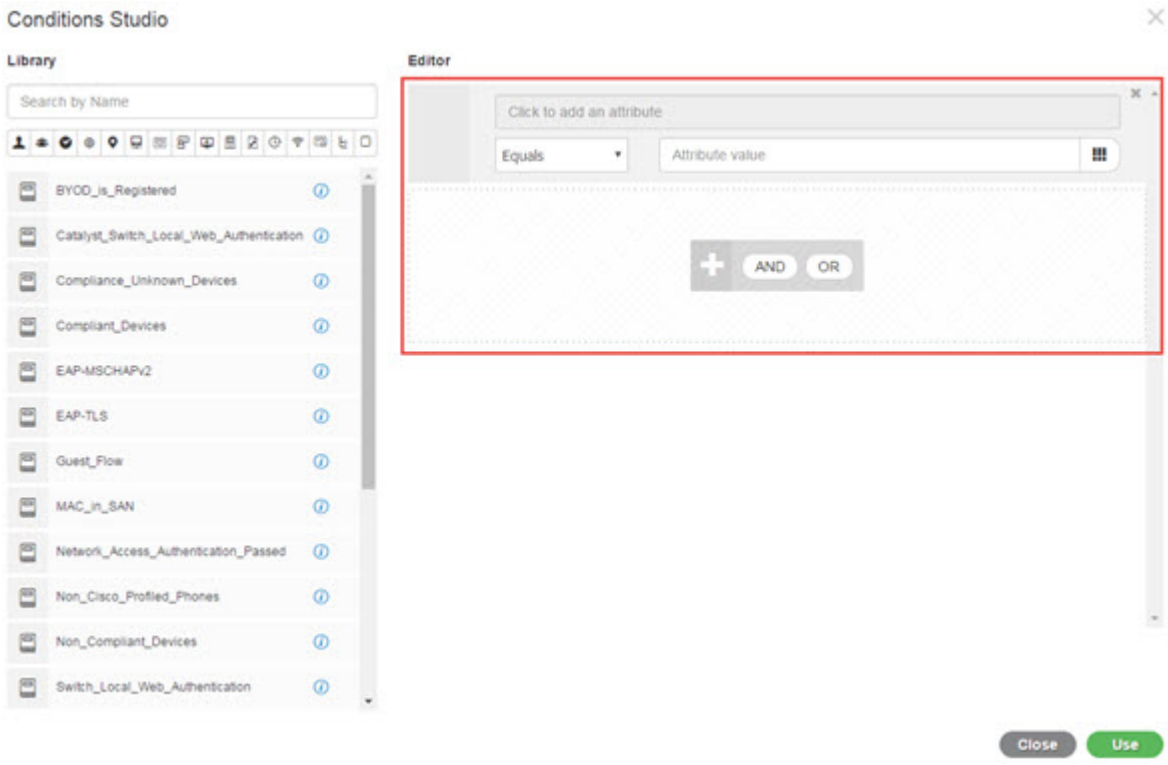
a) 기본 정책 집합 페이지의 정책 집합 표에서 **Conditions(조건)** 열의 ✚ 버튼을 클릭하여 전체 정책 집합과 관련된 조건(인증 정책 규칙의 일치 전에 확인되는 조건)을 생성합니다.

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  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, 39 페이지을 참조하십시오.

그림 ***4: 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.

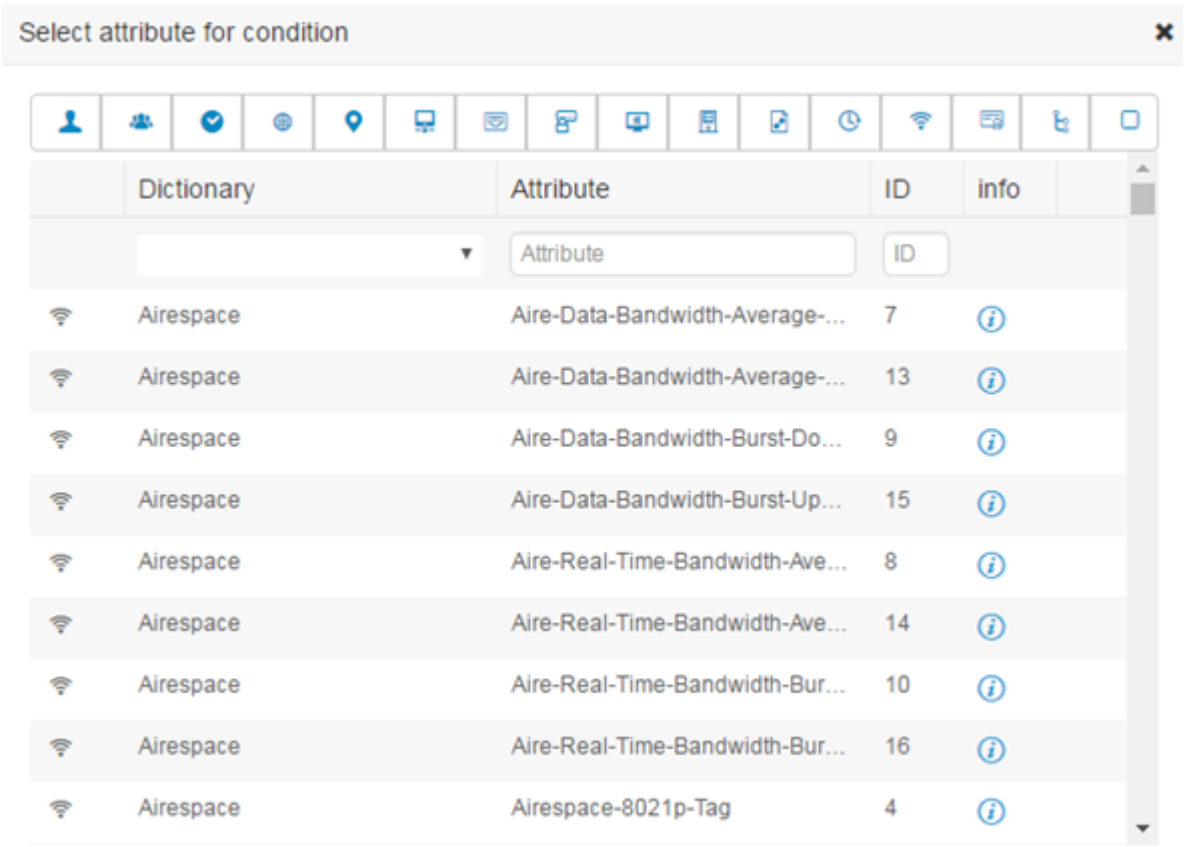
b) 자유 텍스트로 조건 블록을 검색합니다. 검색하려는 블록의 이름에 표시되는 단어 중 아무 것이든 또는 일부를 **Search by Name(**이름으로 검색**)** 자유 텍스트 필드에 입력합니다. 입력하는 동안 시스템은 실시간으로 관련 결과를 동적으로 검색합니다. 범주를 선택하지 않으면(강조 표시된 아이콘 없음) 모든 범주의 조건 블록이 결과에 포함됩니다. 범주 아이콘이 이미 선택된 경우(표시된 목록이 이미 필터링됨)에는 특정 텍스트를 사용하는 특정 범주의 블록만 표시 결과에 포함됩니다.

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 ***5: 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, 53 페이지
EAP-FAST를 프로토콜로 사용하기 위한 지침, 53 페이지
EAP-FAST의 이점, 104 페이지
EAP-FAST 설정 구성, 54 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 ***6: 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, 53 페이지
EAP-FAST를 프로토콜로 사용하기 위한 지침, 53 페이지
EAP-FAST용 PAC 생성, 54 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 ***7: 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, 53 페이지
인증 프로토콜로 EAP-TTLS 사용, 57 페이지
EAP-TTLS 설정 구성, 57 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 ***8: 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, 53 페이지
EAP-TLS 설정 구성, 58 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 ***9: 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, 53 페이지
PEAP 설정 구성, 59 페이지
PEAP를 사용하는 경우의 이점, 102 페이지
PEAP 프로토콜용으로 지원되는 신청자, 103 페이지
PEAP 프로토콜 흐름, 103 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 ***10: 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, 53 페이지
Cisco ISE의 RADIUS 프로토콜 지원, 70 페이지
RADIUS 설정 구성, 60 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 ***11:*** 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 PAC 나 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
네트워크 액세스용으로 허용되는 프로토콜 정의, 97 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 *12: 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, 123 페이지
EAP-FAST용 PAC 생성, 54 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 ***13: 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 ***14: 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)

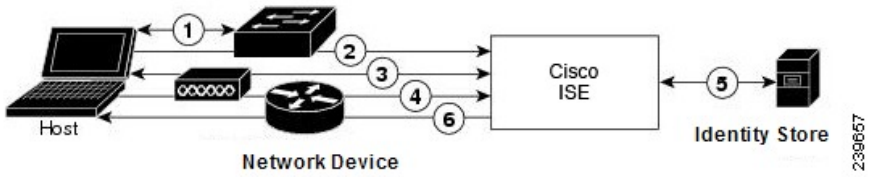
RADIUS 기반 비 EAP 인증 흐름

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 ***5: 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.

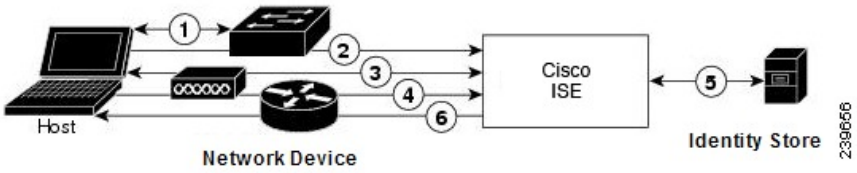
호스트와 Cisco ISE는 이러한 방식으로 EAP 메시지(RADIUS를 통해 전송되며 네트워크 디바이스를 통해 전달됨)를 간접 교환합니다. 이러한 방식으로 교환되는 최초 EAP 메시지 집합은 이후 인증을 수행하는 데 사용되는 특정 EAP 방법을 협상합니다.

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 ***6: 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.

PEAP를 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)

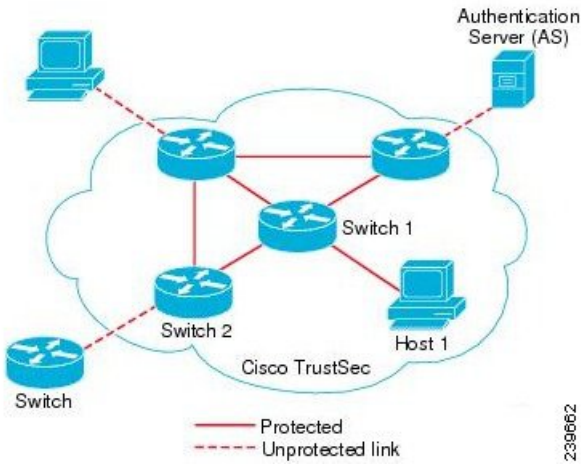
IP 전화기 인증 기능에 자세한 내용은 전화기 인증 기능을 참조하십시오.

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 *7: 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 ***15: 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, 165 페이지 및 Cisco ACI 및 Cisco SD-Access와 가상 네트워크 인식 통합, 169 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, 117 페이지

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- TrustSec 디바이스 구성, 122 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, 107 페이지
TrustSec 구성 요소, 108 페이지
TrustSec 전역 설정 구성, 116 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 *16: 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, 133 페이지
매트릭스 보기, 134 페이지
TrustSec 매트릭스 설정 구성, 120 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.

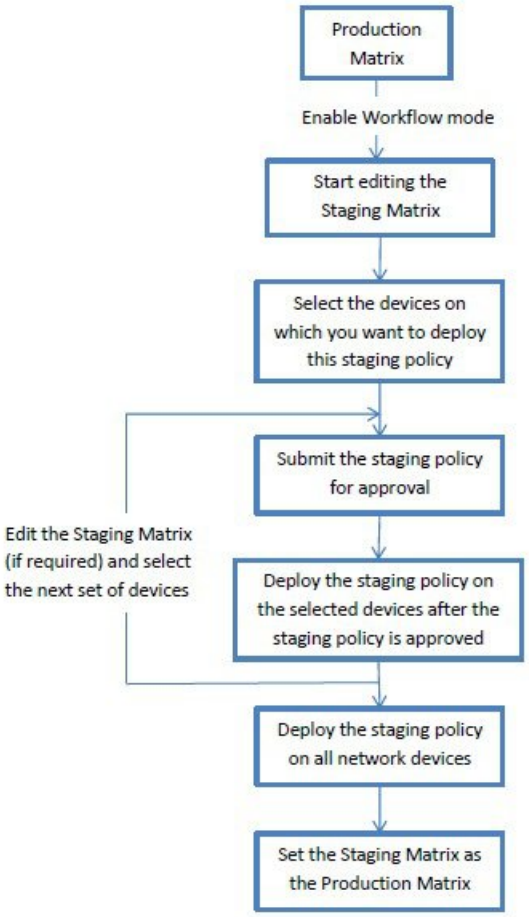
TrustSec 매트릭스 워크플로우 프로세스

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 *8:* 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, 147 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.

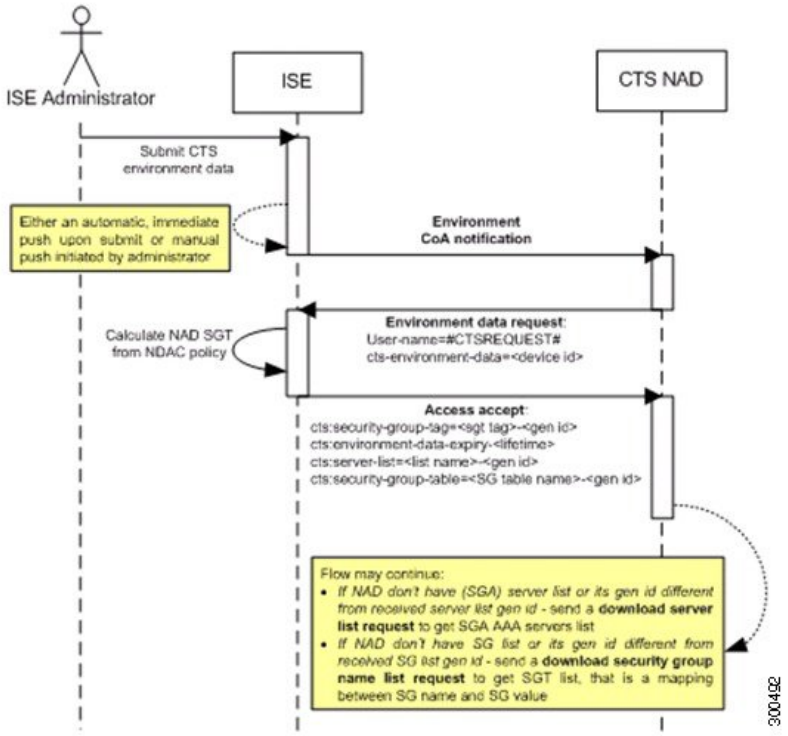
a) Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택하고 필요한 네트워크 디바이스의 이름, IP 주소, RADIUS 및 TrustSec 설정이 올바르게 구성되어 있는지 확인합니다.
b) 아래쪽의 **Advanced TrustSec Settings(**고급 **TrustSec** 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 ***9:*** 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.

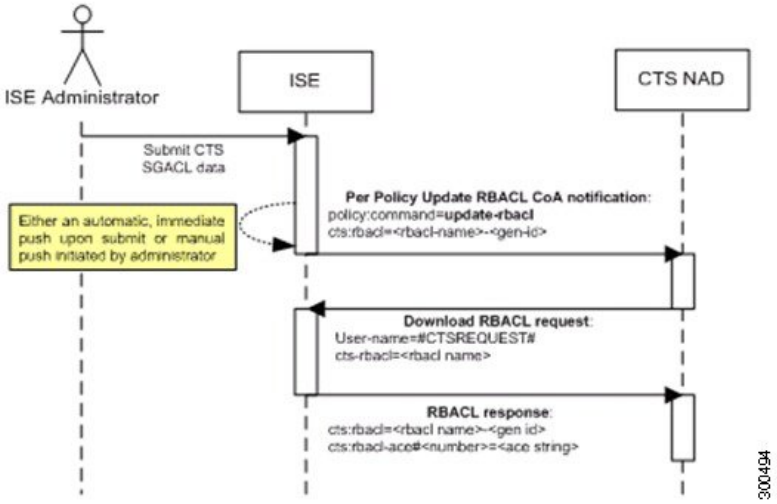
NDAC 정책 페이지에서 NDAC 정책의 규칙을 생성, 삭제 또는 업데이트할 수 있습니다. 이러한 환경 변경 알림은 모든 네트워크 디바이스로 전송됩니다.

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 *10: 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.

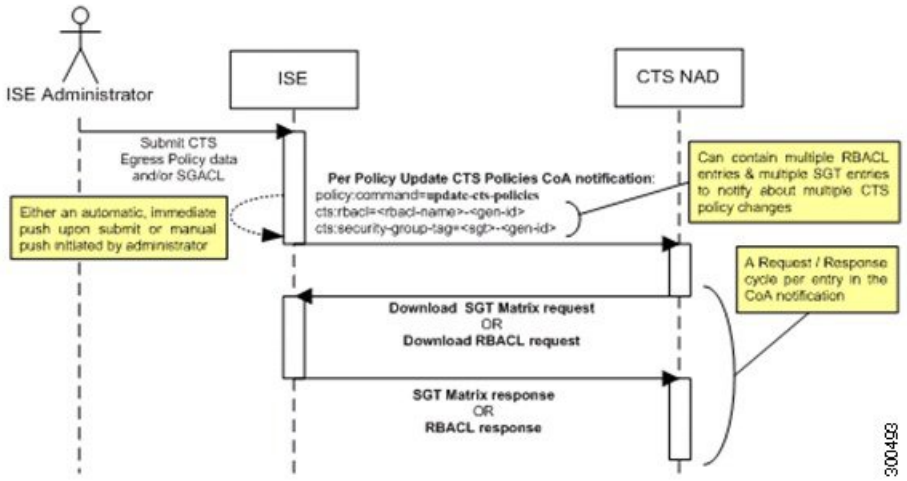
SGACL의 이름이나 IP 버전을 변경해도 세대 ID는 변경되지 않으므로 SGACL 명명된 목록 업데이트 CoA 알림을 보내지 않아도 됩니다.

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 *11:* 정책 *CoA* 알림 흐름

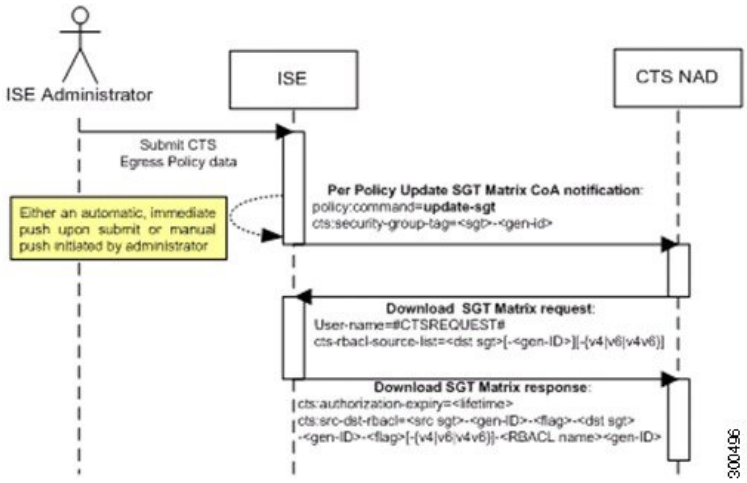


1. Cisco ISE는 업데이트 정책 CoA 알림을 TrustSec 네트워크 디바이스로 보냅니다. 알림에는 여러 SGACL 이름 및 생성 ID, 그리고 여러 SGT 값과 생성 ID가 포함될 수 있습니다.
2. 디바이스는 여러 SGACL 데이터 요청 및/또는 여러 SGT 데이터를 사용하여 재생될 수 있습니다.
3. Cisco ISE는 각 SGACL 데이터 요청 또는 SGT 데이터 요청에 대한 응답으로 관련 데이터를 반환합니다.

SGT 매트릭스 CoA 업데이트 흐름

다음 그림에는 SGT 매트릭스 CoA 업데이트 흐름이 나타나 있습니다.

그림 *12: 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 *17: 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 가져오기를 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.

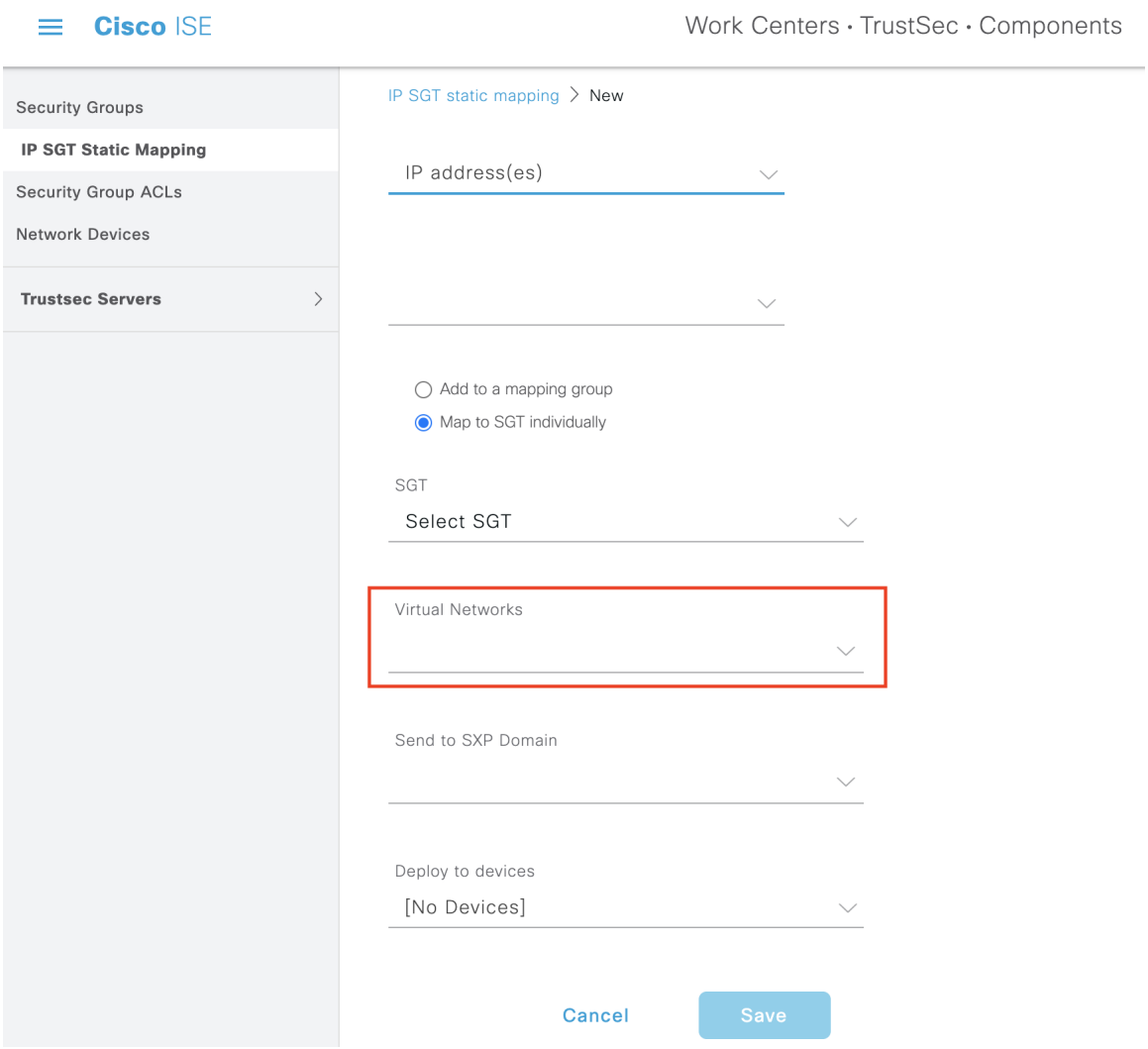
도메인 간 지원을 촉진하려면 다양한 네트워크 전환 도메인(예: IP 주소, 서브넷 마스크, 보안 그룹 태그, EPG, 가상 네트워크, VRF(가상 라우팅 및 포워딩))을 교환하고 필터링하는 기능이 있어야 합니다. 정책 도메인 또는 정책 도메인 내의 전환 도메인에서 다른 도메인으로 또는 그 반대로 교환하고 필터링할 수 있습니다. 이는 Cisco SD-Access, Cisco ACI, SD-WAN, CPC, Meraki 등의 정책 도메인에 여러 전환 도메인이 있는 경우 특히 중요합니다.

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.

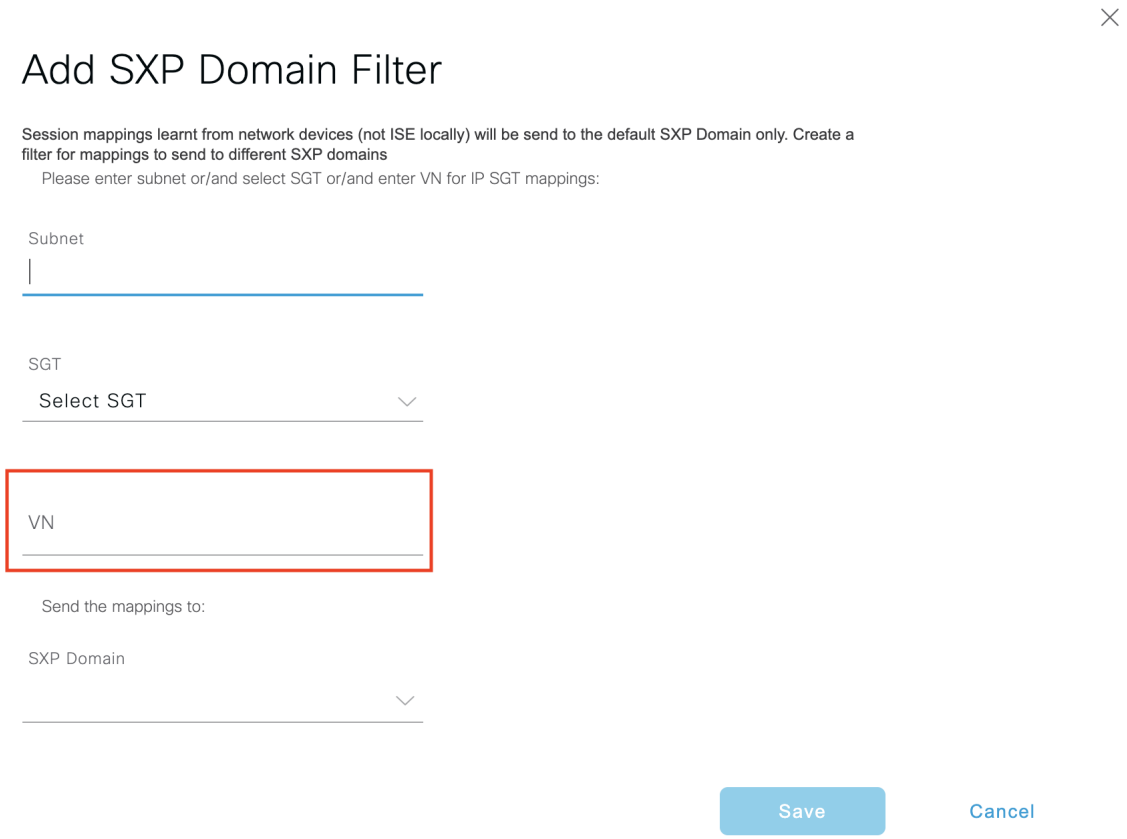
IP-SGT Static Mapping(IP-SGT 정적 매핑) 창에서 IP-SGT 정적 매핑에 가상 네트워크를 추가하고 수정할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > TrustSec > Components(**구성 요소**) > IP SGT Static Mapping(IP SGT** 정적 매핑**)**을 선택합니다. **Add(**추가**)**를 클릭하여 새 매핑을 추가하거나 **Edit(**편집**)**를 클릭하여 기존 매핑을 수정합니다.

그림 *13: 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 ***14: 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.

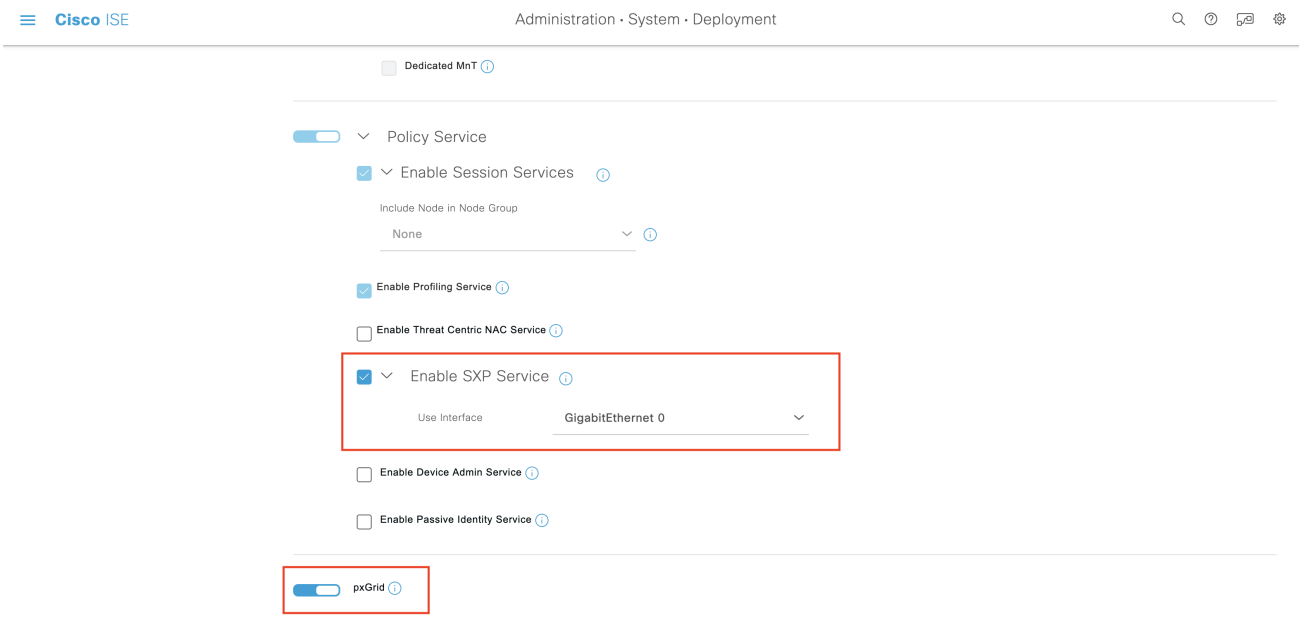
단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Deployment(구축)**를 선택합니다.

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 ***15: SXP*** 및 ***pxGrid*** 서비스 활성화



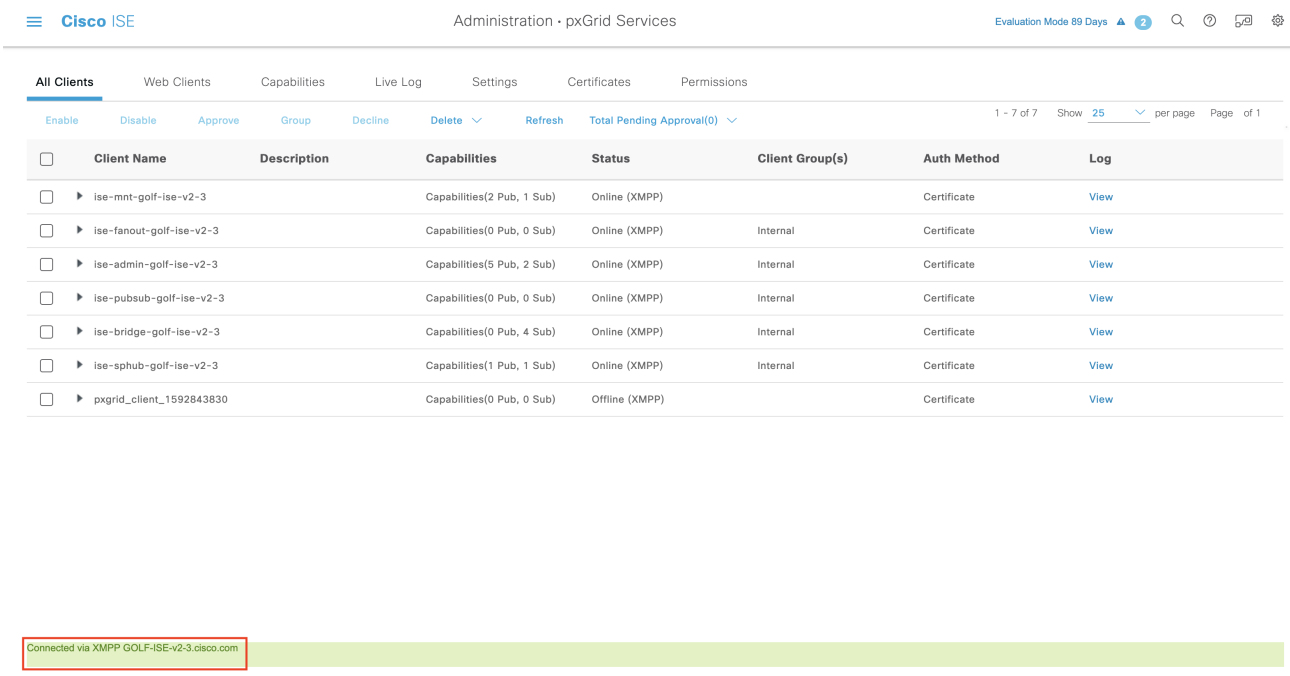
단계 **4** **Save(**저장**)**를 클릭합니다.

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 ***16: 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.

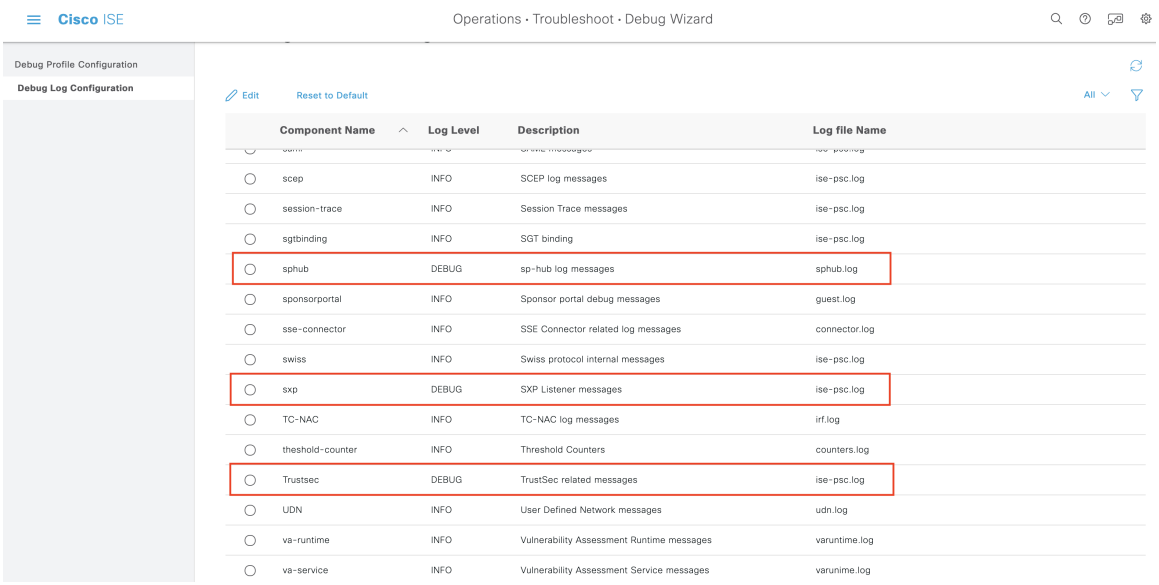
단계 **10** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centres(**작업 센터**)** > **TrustSec** > **Settings(**설정**)** > **ACI Settings(ACI** 설정**)**를 선택합니다.

단계 **11** 필요에 따라 ACI 설정을 구성합니다. 자세한 내용은 ACI 설정 구성, 166 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 ***17:*** 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, 112 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 ***18: System Certificates(***시스템 인증서***)*** 창의 ***Verify the Certificate(***인증서 확인***)***

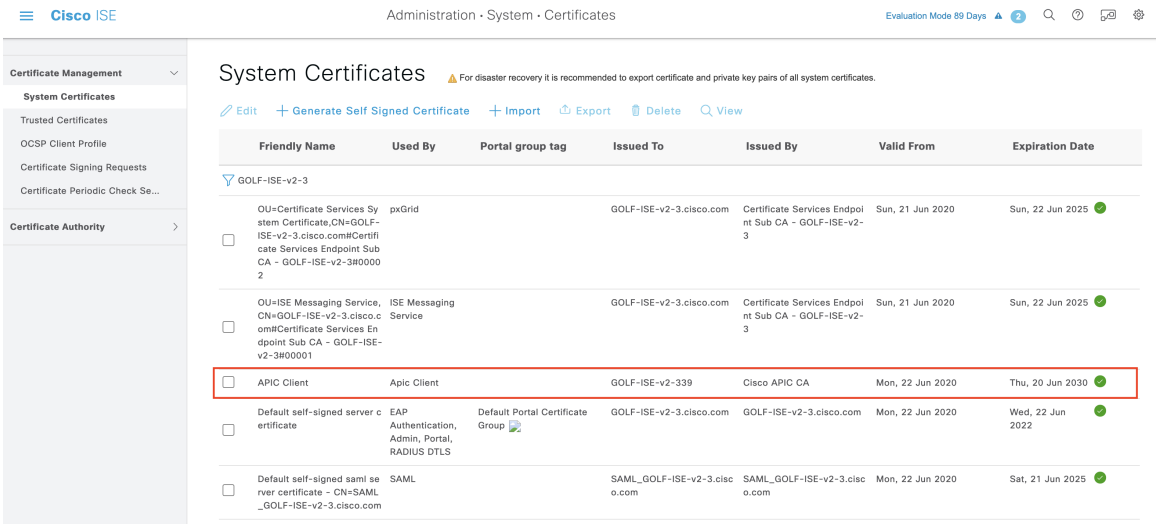
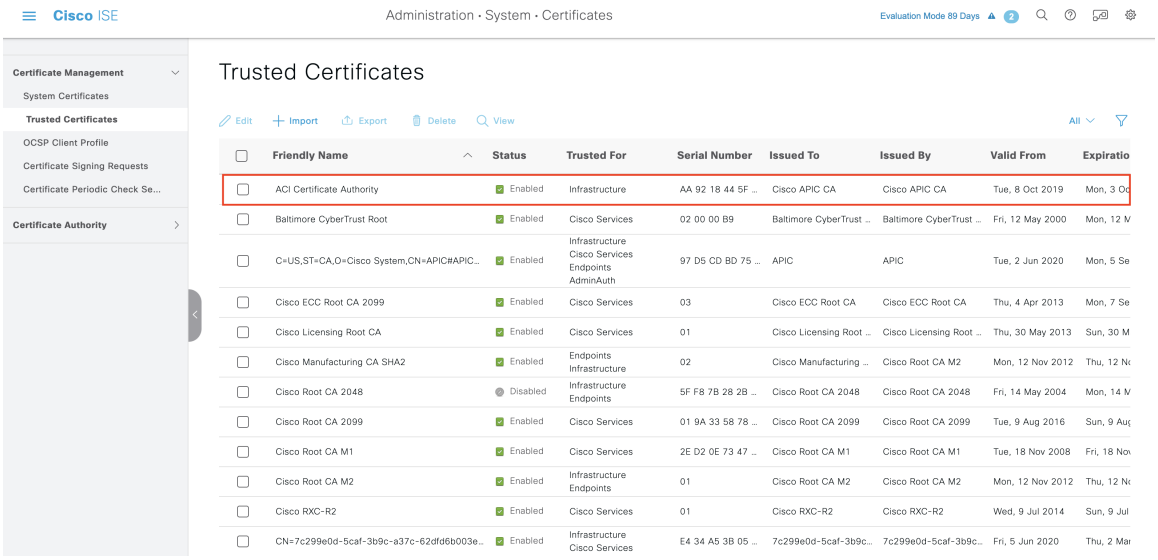


그림 ***19: Trusted Certificates(***신뢰할 수 있는 인증서***)*** 창의 ***Verify the Certificate(***인증서 확인***)***



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.