기본 설정

관리 포털

그림 ***1: Cisco ISE*** 관리 포털

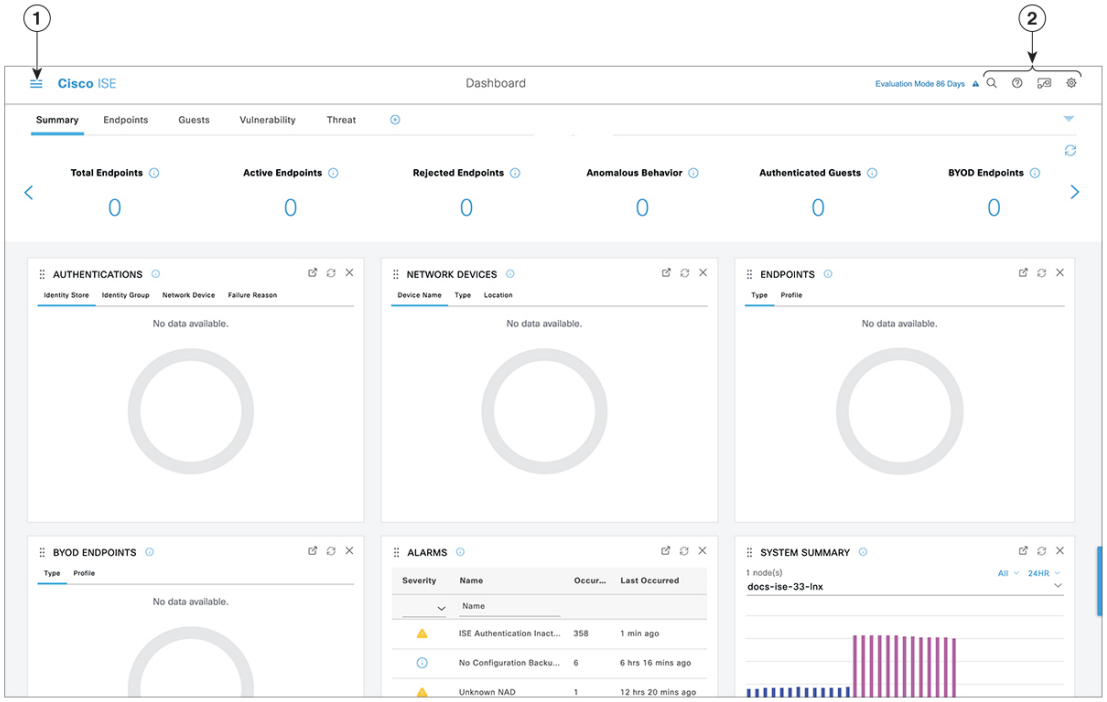
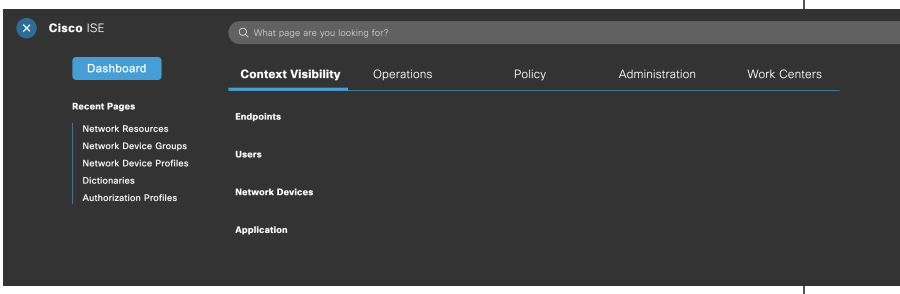


표 ***1: Cisco ISE*** 관리 포털의 구성 요소

1	메뉴 아이콘	다음 메뉴가 있는 슬라이드식 창에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭합니다. 슬라이드식 메뉴 창에는 필요한 창을 찾을 수 있는 검색 창도 포함되어 있습니다. 홈 페이지의 **Dashboard(**대시보드**)**를 클릭합니다. 그림 ***2: Cisco ISE*** 주 메뉴  • **Context Visibility(**상황 가시성**)**: 상황 가시성 창에는 엔드포인트, 사용자 및 NAD(Network Access Device)에 대한 정보가 표시됩니다. 상황 가시성 정보는 등록한 라이선스에 따라 기능, 애플리케이션, BYOD(Bring Your Own Device) 및 기타 범주별로 구분됩니다. 상황 가시성 창은 중앙 데이터베이스를 사용하며 데이터베이스 표, 캐시 및 버퍼에서 정보를 수집합니다. 따라서 상황 가시성 dashlet 및 목록의 콘텐츠가 빠르게 업데이트됩니다. 상황 가시성 창은 상단의 dashlet과 하단의 정보 목록으로 구성되어 있습니다. 목록에서 열 속성을 수정하여 데이터를 필터링하면 dashlet이 새로 고침되어 변경된 콘텐츠가 보여집니다. • **Policy(**정책**)**: 정책 창은 인증, 권한 부여, 프로파일링, 포스처 및 클라이언트 프로비저닝 영역에서 네트워크 보안을 관리할 수 있는 도구를 포함합니다. • **Administration(**관리**)**: 관리 창은 Cisco ISE 노드, 라이선스, 인증서, 네트워크 디바이스, 사용자, 엔드포인트 및 게스트 서비스를 관리할 수 있는 도구를 포함합니다.

2	오른쪽 상단 메뉴 아이콘	

-

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

-

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

-

  다음 옵션에 액세스하려면 이 아이콘을 클릭합니다.

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

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

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

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

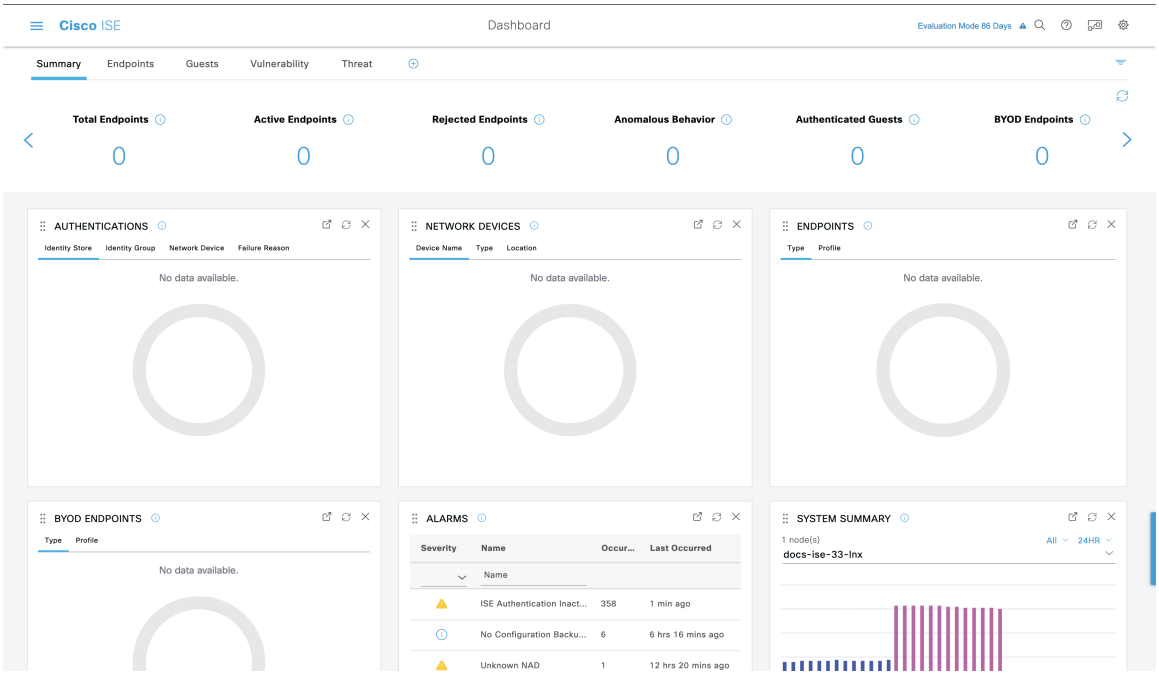
  - **Run Endpoint Scripts(**엔드포인트 스크립트 실행**)**: 연결된

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

Cisco ISE 홈 대시보드

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

그림 ***3: Cisco ISE*** 홈 대시보드



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

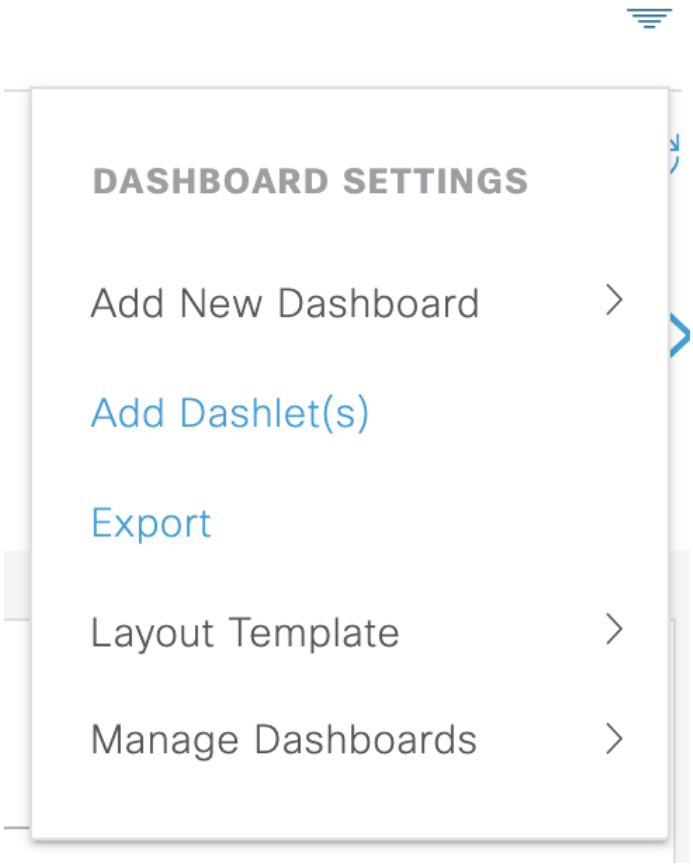
- **Summary(**요약**)**: 이 대시보드에는 선형 메트릭 dashlet, 원형 차트 dashlet 및 목록 dashlet이 포함됩니다. 메트릭 dashlet은 구성할 수 없습니다. 기본적으로 이 대시보드에는 **Status(**상태**) Endpoints(**엔드포인트**)**, **Endpoint Categories(**엔드포인트 범주**)** 및 **Network Devices(**네트워크 디바이스**)** dashlet이 포함됩니다.

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

홈 대시보드 구성

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

그림 ***4:*** 대시보드 사용자 맞춤화



드롭다운 목록에 다음과 같은 옵션이 표시됩니다.

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

상황 가시성 보기

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

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

기본 PAN에서만 상황 가시성 데이터를 볼 수 있습니다.

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

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

- **Endpoints(**엔드포인트**)**: 디바이스 유형, 규정 준수 상태, 인증 유형, 하드웨어 인벤토리 등에 따라 표시할 엔드포인트를 필터링합니다. 자세한 내용은 하드웨어 대시보드, 12 페이지의 내용을 참조하십시오.

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

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

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

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

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

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

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

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

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

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

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

dashlet에서 원형 그래프의 섹션을 클릭하여 해당 dashlet에서 필터링된 데이터가 포함된 새 창을 표시합니다. 이 새 창에서 보기에서 표시되는 데이터 필터링, 16 페이지에 설명된 대로 표시된 데이터를 계속 필터링할 수 있습니다.

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

관련 항목

하드웨어 대시보드, 12 페이지

상황 가시성의 속성

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

운영체제

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

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

포털 이름

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

포털 사용자의 경우

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

애플리케이션 대시보드

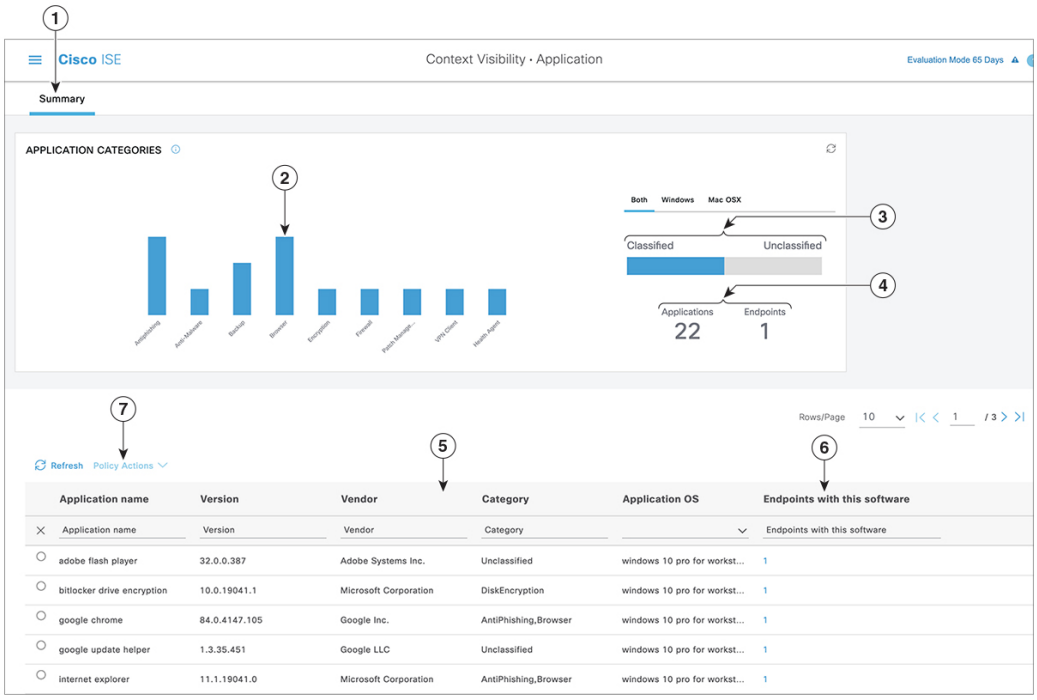


표 *2:* 애플리케이션 대시보드에 대한 설명

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

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

하드웨어 대시보드

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

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

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

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

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

참고

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

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

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

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

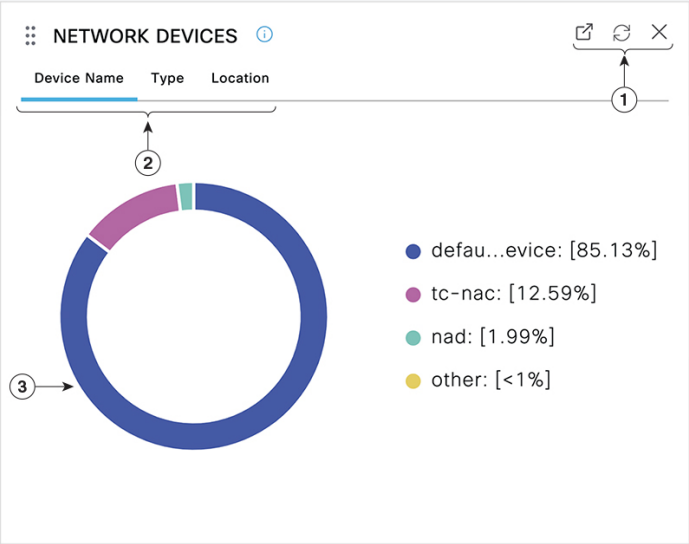
엔드포인트에 해당하는 **Attached Devices(**연결된 디바이스**)** 열의 번호를 클릭하면 현재 엔드포인트에 연결된 USB 디바이스의 이름, 범주, 제조업체, 유형, 제품 ID 및 벤더 ID를 볼 수 있습니다.

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

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

Dashlet

다음 이미지는 dashlet의 예입니다.



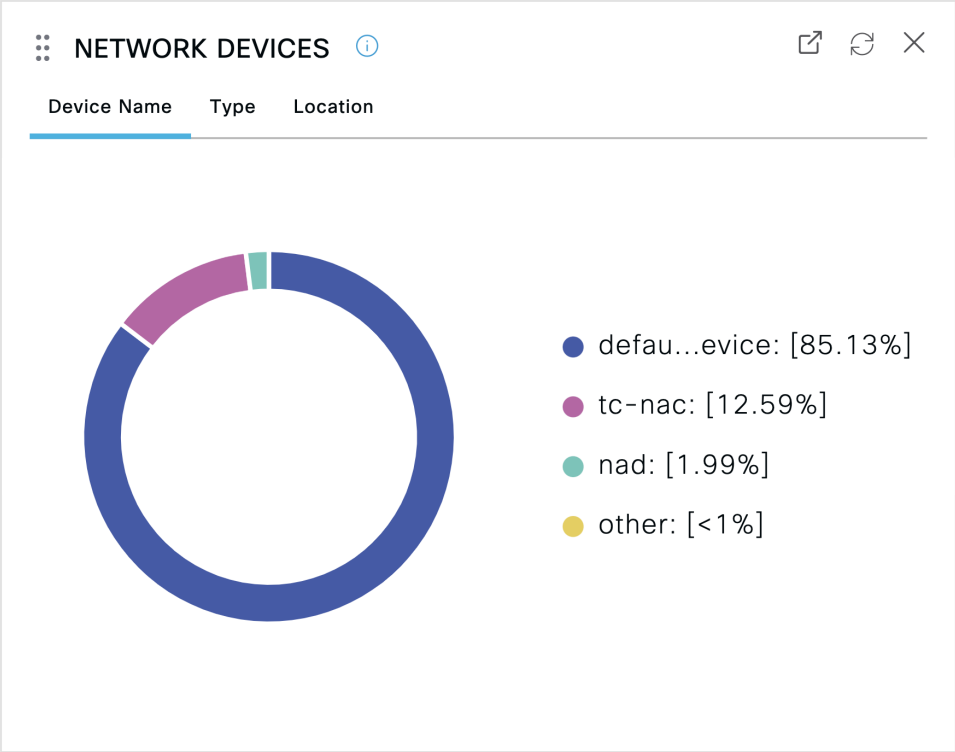
1. 열린 새 창 아이콘을 클릭하면 새 브라우저 창에서 이 dashlet이 열립니다. 파이 차트가 새로 고쳐집니다. 이 dashlet을 삭제하려면 **X**를 클릭합니다. 이 옵션은 홈 페이지에서만 사용할 수 있습니다. 화면 오른쪽 상단의 기어 기호를 사용하면 상황 가시성 창에서 dashlet이 삭제됩니다.
2. 일부 dashlet은 데이터 범주가 서로 다릅니다. 해당 데이터 집합이 포함된 원형 차트를 보려면 범주를 클릭합니다.
3. 원형 차트에는 선택한 데이터가 표시됩니다. 원 세그먼트 중 하나를 클릭하면 해당 원 세그먼트를 기준으로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

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

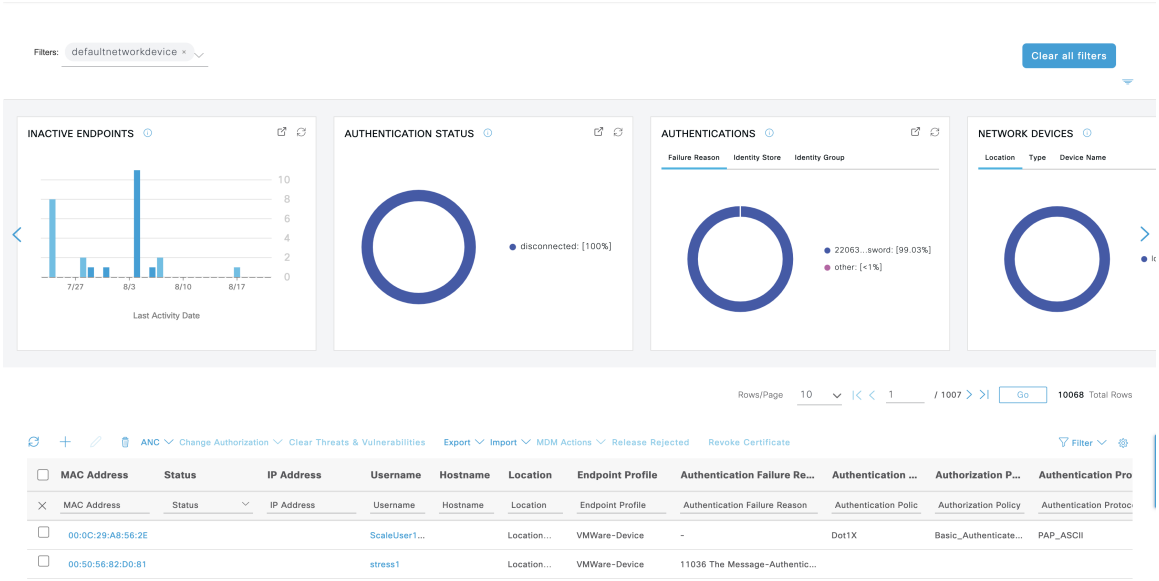
Context Visibility(상황 가시성) 창에서 원도표의 섹션을 클릭하면 표시되는 데이터는 필터링되지만 상황은 변경되지 않습니다. 필터링된 데이터를 동일한 브라우저 창에서 볼 수 있습니다.

보기에서 표시되는 데이터 필터링

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



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



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

맞춤형 필터를 저장합니다.

사용자 맞춤화 필터 생성

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

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

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

단계 **3** 조건을 더 추가하려면 **+**를 클릭합니다.

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

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

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

고급 필터를 사용하여 조건별로 데이터 필터링

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

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

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

단계 **3** 조건을 더 추가하려면 +를 클릭합니다.

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

빠른 필터를 사용하여 필드 속성을 기준으로 데이터 필터링

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

단계 **1** **Filter(**필터**)**를 클릭하고 드롭다운 목록에서 **Quick Filter(**빠른 필터**)**를 선택합니다.

단계 **2** 속성 필드 중 하나 이상에 검색 기준을 입력하면 지정한 속성과 일치하는 엔트리가 자동으로 표시됩니다.

Dashlet 보기의 엔드포인트 작업

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

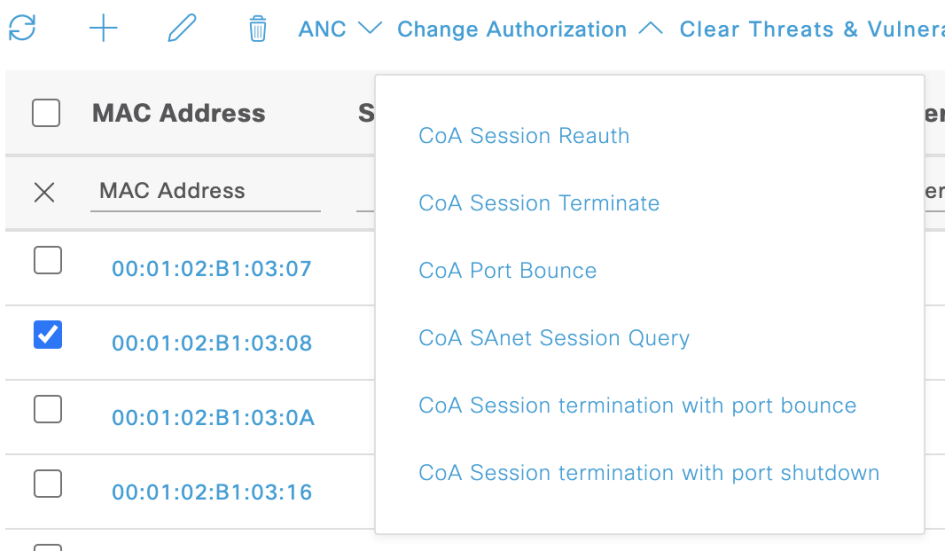
- **Adaptive Network Control Actions(**적응형 네트워크 제어 작업**)**

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

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

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

그림 *5: Dashlet* 보기의 엔드포인트 작업



- **MDM** 작업

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

Cisco ISE 대시보드

Cisco ISE 대시보드 또는 홈 페이지(**Menu(**메뉴**)** 아이콘(☰)을 클릭하고 대시보드를 선택)는 Cisco ISE 관리 포털에 로그인한 후에 표시되는 랜딩 페이지입니다. 대시보드는 창 위쪽에 메트릭 측정기가 표시되고 아래에는 dashlet이 구성된 중앙 집중식 관리 콘솔입니다. 기본 대시보드는 **Summary(**요약**)**, **Endpoints(**엔드포인트**)**, **Guests(**게스트**)**, **Vulnerability(**취약점**)** 및 **Threat(**위협**)**입니다. Cisco ISE 홈 대시보드, 6 페이지를 참조하십시오.

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

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

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

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

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

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

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

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

참고 기본 대시보드는 이름을 바꾸거나 삭제할 수 없습니다.

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

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

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

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

Cisco ISE 국제화 및 현지화

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

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

지원되는 언어

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

표 *3:* 지원되는 언어 및 로캘

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

최종 사용자 웹 포털 현지화

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

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

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

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

UTF-8 문자 데이터 입력 지원

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

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

UTF-8 인증서 인증

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

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

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

UTF-8 정책 및 Posture Assessment

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

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

신청자에게 전송되는 메시지에 대한 UTF-8 지원

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

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

보고서 및 경보 **UTF-8** 지원

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

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

포털의 **UTF-8** 문자 지원

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

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

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

표 ***4:*** 관리 포털 ***UTF-8*** 문자 필드

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

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

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

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

Cisco ISE 사용자 인터페이스 외부에서 UTF-8 지원

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

디버그 로그 및 CLI 관련 UTF-8 지원

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

Cisco Secure ACS 마이그레이션 UTF-8 지원

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

UTF-8 값 가져오기 및 내보내기 지원

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

REST에 대한 UTF-8 지원

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

ID 저장소 권한 부여 데이터에 대한 UTF-8 지원

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

MAC 주소 정규화

Cisco ISE는 다음 형식으로 입력되는 MAC 주소의 정규화를 지원합니다.

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

다음 Cisco ISE 창에서는 전체 또는 부분 MAC 주소를 제공합니다.

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

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

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

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

REST API는 전체 MAC 주소의 정규화도 지원합니다.

옥텟의 유효 범위는 0~9, a~f 또는 A~F입니다.

Cisco ISE 구축 업그레이드

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

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

관리자 액세스 콘솔

다음 단계에서는 관리 포털에 로그인하는 방법을 설명합니다.

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

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

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

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

관리자 로그인 브라우저 지원

Cisco ISE 관리 포털은 다음의 HTTPS 사용 가능 브라우저를 지원합니다.

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

ISE 커뮤니티 리소스

Adblock Plus 사용 시 ISE 페이지가 완전히 로드되지 않는 경우

실패한 로그인 시도 이후에 관리자 잠금

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

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

Cisco ISE의 프록시 설정 구성

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

프록시 설정은 다음 Cisco ISE 기능에 영향을 줍니다.

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

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

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

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

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

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

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

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

단계 **6** **Save(**저장**)**를 클릭합니다.

관리 포털에서 사용하는 포트

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

Cisco ISE 애플리케이션 프로그래밍 인터페이스 게이트웨이 설정

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

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

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

단계 **1** 기본 PAN에 로그인합니다.

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

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

단계 **4** **Enable(**활성화**)**을 클릭합니다.

문제 해결

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

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

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

확인

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

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

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

외부 **RESTful** 서비스 애플리케이션 프로그래밍 인터페이스 활성화

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

단계 **5** **Save(**저장**)**를 클릭합니다.

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

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

관련 항목

외부 RESTful 서비스 소프트웨어 개발 키트 , 36 페이지

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

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

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

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

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

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

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

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

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

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

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

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

단계 **10** **Save(**저장**)**를 클릭합니다.

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

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

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

외부 **RESTful** 서비스 소프트웨어 개발 키트

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

SDK는 다음 구성 요소로 구성됩니다.

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

시스템 시간 및 네트워크 시간 프로토콜 서버 설정 지정

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

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

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

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

시작하기 전에

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

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

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

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

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

a) **Add(**추가**)**를 클릭합니다.

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

c) **OK(**확인**)**를 클릭합니다.

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

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

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

단계 **5** **Save(**저장**)**를 클릭합니다.

시스템 표준 시간대 변경

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

clock timezone *timezone*

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

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

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

알림을 지원하도록 SMTP 서버 구성

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

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

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

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

표 ***5:*** 이메일을 전송하는 ***Cisco ISE*** 노드

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

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

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

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

대화형 도움말

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

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

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

보안 잠금 해제 클라이언트 메커니즘 활성화

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

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

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

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

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

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

```
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
1
Generating Challenge.....................................
Challenge String (Please copy everything between the asterisk lines exclusively):
********************************************************************************
GLCX7gAAQEBAAQAAAAPAgAFAAAAAAMACImJxgubOhitBAAQiUwv+XeD3pnJ4HLnJy3OXQLABAAADhAGAANUUUHAAZJUUVfQlQIAANUUUACcJIDU2NGQ3NjgwLTFmZmEtOWI0ZS0wZjY1LTdlZDllMGQlM2UzNQo=
********************************************************************************
Starting background timer of 15mins
1. Generate Challenge Token Request
2. Enter Challenge Response for Root Access
3. Show History
4. Exit
Enter CLI Option:
```

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

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

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

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

참고 응답 서명 확인에 성공하면 권한 있는 액세스가 활성화됩니다.

다음에 수행할 작업

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

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

옵션 **3**을 선택하여 루트 액세스 세션의 기록을 확인합니다.

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

FIPS(연방 정보 처리 표준) 모드 지원

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

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

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

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

FIPS 모드를 활성화하는 경우 영향을 받는 기능은 다음과 같습니다.

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

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

FIPS 모드를 활성화하는 경우:

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

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

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

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

Cisco ISE에서 연방 정보 처리 표준 모드 활성화

Cisco ISE에서 FIPS 모드를 활성화하려면

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

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

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

다음에 수행할 작업

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

- 셀프 서명 인증서 생성, 67 페이지.
- 인증서 서명 요청을 생성하고 인증 기관에 제출, 88 페이지.
- 네트워크 디바이스 정의 설정에서 RADIUS 인증 설정을 구성합니다.

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

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

시작하기 전에

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

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

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

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

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

단계 **2** 지침에 따라 인증서 인증 프로파일을 구성합니다.

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

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

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

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

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

단계 **5** 외부 관리자 그룹에 대한 RBAC 권한을 할당할 관리자 권한 부여 정책을 구성합니다.

주의 외부 슈퍼 관리자 그룹을 생성하여 Active Directory 그룹에 매핑하고, 슈퍼 관리자 권한(메뉴 액세스 및 데이터 액세스)으로 관리자 권한 부여 정책을 구성한 후에 해당 Active Directory 그룹에서 사용자를 한 명 이상 생성하는 것이 좋습니다. 이 매핑을 사용하는 경우 **Client Certificate-Based Authentication(**클라이언트 인증서 기반 인증**)**을 활성화하면 외부 관리자 한 명 이상이 슈퍼 관리자 권한을 가지게 됩니다. 이렇게 하지 않으면 Cisco ISE 관리자가 관리 포털에서 중요한 기능을 사용하지 못하게 될 수도 있습니다.

단계 **6** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Store(**인증서 저장소**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** 인증 기관 인증서를 Cisco ISE 인증서 신뢰 저장소로 가져옵니다.

클라이언트 인증서 신뢰 체인의 인증 기관 인증서를 Cisco ISE 인증서 저장소에 저장하지 않으면 Cisco ISE는 클라이언트 인증서를 수락하지 않습니다. 적절한 인증 기관 인증서를 Cisco ISE 인증서 저장소로 가져와야 합니다.

a) **Import(**가져 오기**)**를 클릭하고 **Certificate File(**인증서 파일**)** 영역에서 **Choose File(**파일 선택**)**을 클릭합니다.
b) **Trust for client authentication and Syslog(**클라이언트 인증 및 시스템 로그용으로 신뢰**)** 확인란을 선택합니다.
c) **Submit(**제출**)**을 클릭합니다.

인증서를 가져오고 나면 구축의 모든 노드를 재시작하라는 메시지가 표시됩니다. 모든 인증서를 가져올 때까지 재시작을 연기할 수 있습니다. 그러나 모든 인증서를 가져온 후에는 계속 진행하기 전에 Cisco ISE를 재시작해야 합니다.

단계 **7** 취소 상태 확인용으로 인증 기관 인증서를 구성합니다.

a) **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **OSCP Client Profile(OSCP** 클라이언트 프로파일**)**.
b) **Add(**추가**)**를 클릭합니다.
c) OCSP 서버의 이름, 설명(선택 사항) 및 서버의 URL을 해당 필드에 입력합니다.
d) **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Store(**인증서 저장소**)**.
e) 클라이언트 인증서에 서명을 할 수 있는 각 CA 인증서에 대해 해당 CA의 취소 상태 확인을 수행할 방법을 지정합니다. 목록에서 인증 기관 인증서를 선택하고 Edit(편집)를 클릭합니다. 편집 페이지에서 OCSP 또는 CRL(인증서 해지 목록) 검증 또는 둘 다를 선택합니다. OCSP를 선택하는 경우 해당 인증 기관에 사용할 OCSP 서비스를 선택합니다. CRL을 선택하는 경우에는 CRL 배포 URL 및 기타 컨피그레이션 파라미터를 지정합니다.

단계 **8** 클라이언트 인증서 기반 인증을 활성화합니다. **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)**을 선택합니다.

a) **Authentication Method(**인증 방법**)** 탭에서 **Client Certificate Based(**클라이언트 인증서 기반**)** 라디오 버튼을 클릭합니다.
b) 이전에 구성한 인증서 인증 프로파일을 **Certificate Authentication Profile(**인증서 인증 프로파일**)** 드롭다운 목록에서 선택합니다.
c) **Identity Source(ID** 소스**)** 드롭 다운 목록에서 Active Directory 인스턴스 이름을 선택합니다.
d) **Save(**저장**)**를 클릭합니다.

여기서 패스워드 기반 인증을 클라이언트 인증서 기반 인증으로 전환합니다. 이전에 구성한 인증서 인증 프로파일에 따라 관리자 인증서를 인증하는 방법이 결정됩니다. 외부 ID 소스(이 예에서는 Active Directory)를 사용하여 관리자에게 권한을 부여합니다.

인증서 인증 프로파일의 보안 주체 이름 속성을 사용하여 Active Directory의 관리자를 조회합니다.

지원되는 **CAC(Common Access Card)** 표준

Cisco ISE는 CAC(Common Access Card) 인증 디바이스를 사용하여 자신을 인증하는 미국 정부 사용자를 지원합니다. CAC는 특정 직원을 식별하는 X.509 클라이언트 인증서 집합이 포함된 전자 칩을 사용하는 ID 배지입니다. CAC를 통해 액세스하려면 카드를 삽입하고 PIN을 입력할 수 있는 카드 판독기가 필요합니다. 그러면 카드에 있는 인증서가 Windows 인증서 저장소로 전송되어 Cisco ISE를 실행하는 로컬 브라우저 같은 애플리케이션에서 사용할 수 있게 됩니다.

Cisco ISE의 **CAC(Common Access Card)** 작업

Cisco ISE 인증이 클라이언트 인증서를 통해서만 발생하도록 관리 포털을 구성할 수 있습니다. 사용자 ID 또는 비밀번호가 필요한 자격 증명 기반 인증은 허용되지 않습니다. 클라이언트 인증서 기반 인증에서 CAC(Common Access Card) 카드를 삽입하고 PIN을 입력한 다음 Cisco ISE 관리 포털 URL을 브라우저 주소 필드에 입력합니다. 브라우저는 인증서를 Cisco ISE에 전달하며, Cisco ISE는 인증서 내용을 기반으로 로그인 세션을 인증하고 권한을 부여합니다. 이 프로세스에 성공한 경우 Cisco ISE 모니터링 및 문제 해결 홈 페이지가 표시되고 적절한 RBAC 권한이 부여됩니다.

Diffie-Hellman 알고리즘을 사용하여 **SSH** 키 교환 보호

Diffie-Hellman-Group14-SHA1 SSH 키 교환만 허용하도록 Cisco ISE를 구성할 수 있습니다. Cisco ISE CLI 구성 모드에서 다음 명령을 입력합니다.

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

예를 들면 다음과 같습니다.

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

보안 시스템 로그를 전송하도록 Cisco ISE 구성

시작하기 전에

Cisco ISE가 Cisco ISE 노드 간에, 그리고 모니터링 노드에 TLS로 보호되는 보안 시스템 로그만 전송하도록 구성하려면 다음 작업을 수행합니다.

- 구축의 모든 Cisco ISE 노드가 적절한 서버 인증서를 사용하여 구성되어 있는지 확인해 주십시오.
- 기본 네트워크 액세스 인증 정책이 모든 SSL 프로토콜 버전을 허용하지 않도록 합니다.
- 구축의 모든 노드가 기본 PAN에 등록되어 있는지 확인합니다. 또한 구축 환경에 있는 하나 이상의 노드가 보안 시스템 로그 수신기(TLS 서버)로 작동하도록 모니터링 페르소나가 활성화되어 있는지 확인합니다.
- 시스템 로그에 지원되는 RFC 표준을 확인합니다. 사용 중인 Cisco ISE 릴리스에 대한 Cisco Identity Services Engine 네트워크 구성 요소 호환성을 참고하십시오.

단계 **1** 보안 시스템 로그 원격 로깅 대상을 구성합니다.

단계 **2** 보안 시스템 로그 원격 로깅 대상으로 감사 가능한 이벤트를 보내도록 로깅 범주를 활성화합니다.

단계 **3** TCP 시스템 로그 및 UDP 시스템 로그 컬렉터를 비활성화합니다. TLS로 보호되는 시스템 로그 컬렉터만 활성화해야 합니다.

참고 Cisco ISE Release 2.6 이상 릴리스에서는 UDP 시스템 로그를 MnT 노드로 전달하기 위해 Cisco ISE 메시징 서비스를 사용하도록 설정할 경우 TLS로 보호되는 UDP 시스템 로그가 포함됩니다.

보안 시스템 로그 원격 로깅 대상 구성

Cisco ISE 시스템 로그는 다양한 용도로 사용할 수 있도록 로그 컬렉터에 의해 수집되어 저장됩니다. 보안 시스템 로그 대상을 구성하려면 모니터링 페르소나가 활성화되어있는 Cisco ISE 노드를 로그 컬렉터로 선택합니다.

단계 **1** Cisco ISE 관리 포털에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Logging(로깅)** > **Remote Logging Targets(원격 로깅 대상)**을 선택합니다.

단계 **3** **Add(추가)**를 클릭합니다.

단계 **4** 보안 시스템 로그 서버의 이름을 입력합니다.

단계 **5** **Target Type(대상 유형)** 드롭다운 목록에서 **Secure Syslog(보안 시스템 로그)**를 선택합니다.

단계 **6** **Status(상태)** 드롭다운 목록에서 **Enabled(활성화됨)**를 선택합니다.

단계 **7** **Host / IP Address(**호스트/**IP** 주소**)** 필드에서 구축의 Cisco ISE 모니터링 노드 호스트 이름 또는 IP 주소를 입력합니다.

단계 **8** **Port(**포트**)** 필드에서 포트 번호를 *6514*로 입력합니다. 보안 시스템 로그 수신기는 TCP 포트 6514에서 수신 대기합니다.

단계 **9** **Facility Code(**기능 코드**)** 드롭다운 목록에서 시스템 로그 기능 코드를 선택합니다. 기본값은 **LOCAL6**입니다.

단계 **10** 다음 확인란을 선택하여 해당 컨피그레이션을 활성화합니다.

a) **Include Alarms For This Target(**이 대상에 대한 경보 포함**)**

b) **Comply to RFC 3164(RFC 3164** 준수**)**

c) **Enable Server Identity Check(**서버 **ID** 확인 활성화**)**

단계 **11** **Buffer Messages When Server Down(**서버가 다운되면 메시지 버퍼링**)** 확인란을 선택합니다. 이 옵션을 선택하면 Cisco ISE는 보안 시스템 로그 수신기에 연결할 수 없는 경우 로그를 저장하고, 보안 시스템 로그 수신기를 주기적으로 확인하며, 보안 시스템 로그 수신기가 작동하면 로그를 전달합니다.

a) **Buffer Size (MB)(**버퍼 크기**(MB))** 필드에 버퍼 크기를 입력합니다.

b) Cisco ISE가 보안 시스템 로그 수신기를 정기적으로 확인하도록 하려면 **Reconnect Time (Sec)(**다시 연결 시간 초과**(**초**))** 필드에서 다시 연결 시간 초과 값을 입력합니다. 시간 초과 값은 초 단위로 구성됩니다.

단계 **12** **Select CA Certificate(CA** 인증서 선택**)** 드롭다운 목록에서 Cisco ISE가 보안 시스템 로그 서버에 제공해야 하는 CA 인증서를 선택합니다.

단계 **13** 보안 시스템 로그를 구성할 때 **Ignore Server Certificate validation(**서버 인증서 검증 무시**)** 확인란이 선택되지 않았는지 확인합니다.

단계 **14** **Submit(**제출**)**을 클릭합니다.

원격 로깅 대상 설정

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

표 ***6:*** 원격 로깅 대상 설정

필드 이름	사용 지침
Name(이름**)**	새 시스템 로그 대상의 이름을 입력합니다.
Target Type(대상 유형**)**	드롭다운 목록에서 대상 유형을 선택합니다. 기본값은 **UDP** 시스템 로그입니다.
Description(설명**)**	새 대상의 간략한 설명을 입력합니다.
IP Address(IP 주소**)**	로그를 저장할 대상 머신의 IP 주소 또는 호스트 이름을 입력합니다. Cisco ISE는 로깅에 IPv4 및 IPv6 형식을 지원합니다.

필드 이름	사용 지침
Port(포트**)**	대상 머신의 포트 번호를 입력합니다.
Facility Code(시설 코드**)**	드롭다운 목록에서 로깅에 사용할 시스템 로그 시설 코드를 선택합니다. 유효한 옵션은 Local0~Local7입니다.
Maximum Length(최대 길이**)**	원격 로그 대상 메시지의 최대 길이를 입력합니다. 유효한 값은 200~1024바이트입니다.
Buffer Message When Server Down(서버 다운 시 메시지 버퍼링**)**	이 확인란은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **TCP** 시스템 로그 또는 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. TCP 시스템 로그 대상 및 보안 시스템 로그 대상을 사용할 수 없을 때 Cisco ISE가 시스템 로그 메시지를 버퍼링하도록 하려면 이 확인란을 선택합니다. Cisco ISE는 대상에 연결을 재개할 때 대상에 대한 메시지 전송을 다시 시도합니다. 연결이 재개되면 메시지는 가장 오래된 것부터 시작하여 최신순으로 전송됩니다. 버퍼링된 메시지는 항상 새 메시지보다 먼저 전송됩니다. 버퍼가 가득 차면 오래된 메시지는 폐기됩니다.
Buffer Size (MB)(버퍼 크기**(MB))**	각 대상의 버퍼 크기를 설정합니다. 기본적으로 버퍼 크기는 100MB로 설정됩니다. 버퍼 크기를 변경하면 버퍼가 지워지며 특정 대상에 대해 기존에 버퍼링된 모든 메시지는 손실됩니다.
Reconnect Timeout (Sec)(다시 연결 시간 초과**(**초**))**	서버가 다운되었을 때 TCP 및 보안 시스템 로그를 폐기할 때까지 저장할 시간을 초 단위로 입력합니다.
Select CA Certificate(CA 인증서 선택**)**	이 드롭다운 목록은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. 드롭다운 목록에서 클라이언트 인증서를 선택합니다.
Ignore Server Certificate Validation(서버 인증서 검증 무시**)**	이 확인란은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. Cisco ISE가 서버 인증서 인증을 무시하고 모든 시스템 로그 서버를 수락하도록 하려면 이 확인란을 선택합니다.

보안 시스템 로그 대상으로 감사 가능 이벤트를 전송하기 위한 로깅 범주 활성화

감사 가능 이벤트를 보안 시스템 로그 대상으로 보내려면 Cisco ISE에 대해 로깅 범주를 활성화해야 합니다.

단계 **1** Cisco ISE 관리 포털에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**을 선택합니다.

단계 **2** **Administrative and Operational Audit(**관리 및 운영 감사**)** 로깅 범주 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Log Severity Level(**로그 심각도 레벨**)** 드롭다운 목록에서 **WARN**을 선택합니다.

단계 **4** **Targets(**대상**)** 영역에서 앞서 생성한 보안 시스템 로그 원격 로깅 대상을 **Selected(**선택된**)** 영역으로 이동합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 이 절차를 반복하여 다음 로깅 범주를 활성화합니다. 이 두 로깅 범주 모두 기본 로그 심각도 레벨로 **INFO**를 가지며 수정할 수 없습니다.

- **AAA** 감사.
- **Posture and Client Provisioning Audit(**포스처 및 클라이언트 프로비저닝 감사**)**.

로깅 범주 구성

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

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

표 ***7:*** 로깅 범주 설정

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

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

TCP 시스템 로그 및 UDP 시스템 로그 컬렉터 비활성화

Cisco ISE가 노드 간에 보안 시스템 로그만 전송하도록 하려는 경우 TCP 및 UDP 시스템 로그 컬렉터를 비활성화하고 보안 시스템 로그 컬렉터만 활성화하십시오.

참고 Cisco ISE Release 2.6 이상 릴리스에서는 UDP 시스템 로그를 MnT 노드로 전달하기 위해 Cisco ISE 메시징 서비스를 사용하도록 설정할 경우 TLS로 보호되는 UDP 시스템 로그가 포함됩니다. Cisco ISE 메시징 서비스의 시스템 로그의 내용을 참조하십시오.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Remote Logging Targets(**원격 로깅 대상**)**를 선택합니다.

단계 **2** TCP 또는 UDP 시스템 로그 컬렉터 옆의 라디오 버튼을 클릭합니다.

단계 **3** **Edit(**편집**)**를 클릭합니다.

단계 **4** **Status(**상태**)** 드롭다운 목록에서 **Disabled(**비활성화됨**)**를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 이 절차를 반복하여 모든 TCP 또는 UDP 시스템 로그 컬렉터를 비활성화합니다.

기본 보안 시스템 로그 컬렉터

Cisco ISE는 MnT 노드에 대한 기본 보안 시스템 로그 컬렉터를 제공합니다. 기본적으로 로깅 범주는 이러한 기본 보안 시스템 로그 컬렉터에 매핑되지 않습니다. 기본 보안 시스템 로그 컬렉터의 이름은 다음과 같습니다.

- 기본 MnT node: SecureSyslogCollector
- 보조 MnT node: SecureSyslogCollector2

이 정보는 **Remote Logging Targets(**원격 로그인 대상**)** 창에서 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로그인**)** > **Remote Logging Targets(**원격 로그인 대상**)**을 선택합니다 에서 확인할 수 있습니다. 기본 시스템 로그 컬렉터는 삭제할 수 없으며 기본 시스템 로그 컬렉터에 대해서는 다음 필드를 업데이트할 수 없습니다.

- **Name(**이름**)**
- **Target Type(**대상 유형**)**
- **IP /** 호스트 주소
- **Port(**포트**)**

Cisco ISE를 새로 설치할 때 **Default Self-signed Server Certificate(**기본 자체 서명 서버 인증서**)**라는 이름의 인증서가 신뢰할 수 있는 인증서 저장소에 추가됩니다. 이 인증서는 **Trust for Client authentication and Syslog(**클라이언트 인증 및 시스템 로그에 대한 신뢰**)** 사용으로 표시되어 있으므로 안전한 시스템 로그 사용에 적용할 수 있습니다. 구축을 구성하거나 인증서를 업데이트하는 동안 보안 시스템 로그 대상에 관련 인증서를 할당해야 합니다.

Cisco ISE 업그레이드 중에 포트 6514의 MnT 노드를 가리키는 기존 보안 시스템 로그 대상이 있는 경우 대상의 이름과 컨피그레이션이 유지됩니다. 업그레이드 후에는 이러한 시스템 로그 대상을 삭제할 수 없으며 다음 필드를 편집할 수 없습니다.

- **Name(**이름**)**
- **Target Type(**대상 유형**)**
- **IP /** 호스트 주소
- **Port(**포트**)**

업그레이드 시점에 이러한 대상이 없는 경우 인증서 설치 없이 기본 보안 시스템 로그 대상이 신규 설치 시나리오와 유사하게 생성됩니다. 이러한 시스템 로그 대상에 관련 인증서를 할당할 수 있습니다. 인증서에 매핑되지 않은 보안 시스템 로그 대상을 로깅 범주에 매핑하려고 하면 Cisco ISE는 다음 메시지를 표시합니다.

Please configure the certificate for *log_target_name*

오프라인 유지 관리

유지 관리 기간이 1시간 미만인 경우 Cisco ISE 노드를 오프라인으로 전환하고 유지 관리 작업을 수행합니다. 노드를 다시 온라인 상태로 전환하면 PAN 노드는 유지 관리 기간 동안 발생한 모든 변경 사항을 자동으로 동기화합니다. 변경 사항이 자동으로 동기화되지 않으면 PAN과 수동으로 동기화할 수 있습니다.

유지 관리 기간이 1시간을 초과하는 경우 유지 관리 시 노드를 등록 취소하고 노드를 다시 구축에 추가할 때 재등록합니다.

활동이 적은 기간에 유지 관리를 예약하는 것이 좋습니다.

참고

1. 큐에 1,000,000개가 넘는 메시지가 포함되어 있거나 Cisco ISE 노드가 6시간 이상 오프라인 상태인 경우 데이터 복제 문제가 발생할 수 있습니다.
2. 기본 MnT 노드에서 유지 관리를 수행하는 경우 유지 관리 활동을 수행하기 전에 MnT 노드의 운영 백업을 수행하는 것이 좋습니다.

엔드포인트 로그인 자격 증명 구성

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

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

다음 탭이 표시됩니다.

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

Cisco ISE에서의 인증서 관리

인증서는 개인, 서버, 회사 또는 다른 엔터티를 식별하고 해당 엔터티를 공용 키에 연결하는 전자 문서입니다. 자가서명 인증서는 해당 생성자가 서명합니다. 인증서는 자가 서명하거나 외부 CA(Certificate Authority)가 디지털 서명할 수 있습니다. CA 서명 디지털 인증서는 업계 표준으로 자가서명 인증서보다 보안성이 더 높은 것으로 간주됩니다.

인증서는 네트워크에서 보안 액세스를 제공하기 위해 사용됩니다. 인증서는 엔드포인트에 대한 Cisco ISE 노드를 식별하고 엔드포인트와 Cisco ISE 노드 간 통신을 보호합니다.

Cisco ISE는 다음 용도로 인증서를 사용합니다.

- Cisco ISE 노드 간의 통신.
- Cisco ISE와 시스템 로그 및 피드 서버와 같은 외부 서버 간의 통신.
- Cisco ISE와 최종 사용자 포털(예: 게스트, 스폰서 및 BYOD 포털) 간의 통신.

관리 포털을 사용하여 구축 환경의 모든 노드에 대한 인증서를 관리할 수 있습니다.

Cisco ISE에서 보안 액세스를 위한 인증서 구성

Cisco ISE는 PKI(Public Key Infrastructure)를 사용하여 엔드포인트 및 관리자 모두와의 보안 통신은 물론 다중 노드 구축 환경에서 Cisco ISE 노드 간 보안 통신을 제공합니다. PKI는 X.509 디지털 인증서를 사용하여 메시지의 암호화 및 암호 해독을 위한 공용 키를 전송하고 사용자 및 디바이스를 나타내는 다른 인증서의 신뢰성을 확인합니다. Cisco ISE 관리 포털을 통해 두 가지 X.509 인증서 범주를 관리할 수 있습니다.

- 시스템 인증서: 이는 클라이언트 애플리케이션에 대한 Cisco ISE 노드를 식별하는 서버 인증서입니다. 각 Cisco ISE 노드는 고유한 시스템 인증서를 가지고 있으며 각 인증서는 해당 개인 키와 함께 노드에 저장됩니다.
- 신뢰할 수 있는 인증서: 이는 사용자 및 디바이스로부터 받은 공개 키에 대한 신뢰 관계를 설정하는 데 사용되는 CA 인증서입니다. 신뢰할 수 있는 인증서 저장소에는 엔터프라이즈 네트워크에 모바일 디바이스를 등록할 수 있게 해주는 SCEP(Simple Certificate Enrollment Protocol)를 통해 배포된 인증서가 포함되어 있습니다. 신뢰할 수 있는 인증서는 기본 PAN에서 관리되며 Cisco ISE 구축 환경의 다른 모든 노드로 자동 복제됩니다.

분산형 구축 환경에서는 인증서를 PAN의 CTL(Certificate Trust List)로만 가져올 수 있습니다. 인증서는 보조 노드로 복제됩니다.

Cisco ISE의 인증서 인증이 인증서 기반 확인 기능의 소소한 차이에 따른 영향을 받지 않게 하려면 네트워크에 구축된 모든 Cisco ISE 노드에 대해 소문자 호스트 이름을 사용해 주십시오.

인증서 사용

Cisco ISE로 인증서를 가져오는 경우 인증서를 사용할 용도를 지정해야 합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**시스템 관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**) Import(**가져오기**)**를 클릭합니다.

다음 용도 중 하나 이상을 선택합니다.

- **Admin(**관리**)**: 노드 간 통신 및 관리 포털 인증에 사용됩니다.
- **EAP Authentication(EAP** 인증**)**: TLS 기반 EAP 인증에 사용됩니다.
- **RADIUS DTLS**: RADIUS DTLS 서버 인증에 사용됩니다.
- **Portal(**포털**)**: 모든 Cisco ISE 최종 사용자 포털과의 통신에 사용됩니다.
- **SAML**: SAML 응답이 올바른 ID 제공자로부터 수신되고 있는지 확인하는 데 사용됩니다.
- **pxGrid**: pxGrid 컨트롤러와의 통신에 사용됩니다.

각 노드의 다양한 인증서를 관리 포털(관리자 사용), pxGrid 컨트롤(pxGrid 사용) 및 TLS 기반 EAP 인증(EAP 인증 사용)과 통신할 수 있도록 연결할 수 있습니다. 그러나 각 노드에서 이러한 용도로 하나의 인증서만 연결할 수 있습니다.

구축에서 웹 포털 요청을 처리할 수 있는 PSN이 여러 개 있는 경우 Cisco ISE에는 포털 통신에 사용할 인증서를 식별할 수 있는 고유 식별자가 필요합니다. 포털에서 사용하도록 지정된 인증서를 추가하거나 가져오는 경우 인증서 그룹 태그를 정의하고 이를 구축의 각 노드에 있는 해당 인증서와 연결해야 합니다. 이 인증서 그룹 태그를 해당 최종 사용자 포털(게스트, 스폰서 및 개인 디바이스 포털)에 연결해야 합니다. 이 인증서 그룹 태그는 Cisco ISE가 이러한 각 포털과 통신할 때 사용해야 하는 인증서를 식별하도록 도와주는 고유 식별자입니다. 포털마다 각 노드의 인증서를 하나씩만 지정할 수 있습니다.

참고 EAP-TLS 클라이언트 인증서에는 다음 암호에 대해 KeyUsage=Key Agreement 및 ExtendedKeyUsage=Client Authentication이 있어야 합니다.

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

EAP-TLS 클라이언트 인증서에는 다음 암호에 대해 KeyUsage=Key Encipherment 및 ExtendedKeyUsage=Client Authentication이 있어야 합니다.

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

Cisco ISE에서의 인증서 일치

구축에서 Cisco ISE 노드를 설정할 때 노드는 서로 통신합니다. 시스템은 각 Cisco ISE 노드의 FQDN이 일치하는지 확인합니다(예: ise1.cisco.com 및 ise2.cisco.com 또는 와일드카드 인증서를 사용하는 경우 *.cisco.com). 또한 외부 머신에서 Cisco ISE 서버에 인증서를 제공할 경우 Cisco ISE 서버의 인증서와 비교하여 인증을 위해 제공되는 외부 인증서를 확인하거나 일치시킵니다. 두 인증서가 일치하면 인증이 성공합니다.

Cisco 의 경우 노드 간(2개가 있는 경우), 그리고 Cisco 와 pxGrid 간에 일치가 수행됩니다.

Cisco ISE에서는 다음과 같이 일치하는 주체 이름을 확인합니다.

1. Cisco ISE에서 인증서의 대체 주체 이름 확장을 확인합니다. 대체 주체 이름에 하나 이상의 DNS 이름이 있는 경우 DNS 이름 중 하나를 Cisco ISE 노드의 FQDN과 일치시켜야 합니다. 와일드카드 인증서를 사용하는 경우 와일드카드 도메인 이름을 Cisco ISE 노드 FQDN의 도메인과 일치시켜야 합니다.
2. 대체 주체 이름에 DNS 이름이 없거나 대체 주체 이름이 완전히 누락된 경우 인증서의 **Subject(**주체**)** 필드에 있는 공용 이름 또는 인증서의 **Subject(**주체**)** 필드에 있는 와일드카드 도메인을 노드의 FQDN과 일치시켜야 합니다.
3. 일치 항목이 발견되지 않으면 인증서가 거부됩니다.

참고 Cisco ISE로 가져온 X.509 인증서는 PEM(Privacy-Enhanced Mail) 또는 식별 부호화 규칙 형식이어야 합니다. 인증서 체인(시스템 인증서와 여기에 서명하는 신뢰 인증서 시퀀스)이 포함된 파일은 특정 제한 사항에 따라 가져올 수 있습니다.

X.509 인증서의 유효성

X.509 인증서는 특정 날짜까지 유효합니다. 시스템 인증서가 만료되면 해당 인증서를 사용하는 Cisco ISE 기능이 영향을 받게 됩니다. Cisco ISE에서는 만료 날짜까지 남은 기간이 90일 미만이면 시스템 인증서의 보류 중인 만료에 대한 알림을 표시합니다. 이 알림은 다음과 같은 여러 가지 방법으로 표시됩니다.

- **System Certificates(**시스템 인증서**)** 창에 색상이 지정된 만료 상태 아이콘이 나타납니다. 이 창을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificate Management(**시스템 관리**)** > **Certificates(**시스템 인증서**)**를 선택합니다.
- Cisco ISE 시스템 진단 보고서에 만료 메시지가 나타납니다. 이 창을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Diagnostics(**진단**)** > **System Diagnostics(**시스템 진단**)**를 선택합니다.
- 만료 전 90일, 60일, 그리고 30일 시점에 만료 경보가 생성됩니다. 만료 전 30일부터는 매일 만료 경보가 생성됩니다.

만료되는 인증서가 셀프 서명 인증서인 경우에는 인증서를 편집하여 만료 날짜를 연장할 수 있습니다. 인증 기관이 서명한 인증서의 경우에는 만료 전에 충분한 여유를 두고 인증 기관으로부터 교체 인증서를 받아야 합니다.

Cisco ISE에서 공개 키 인프라 활성화

PKI는 보안 통신을 수행할 수 있도록 하고 디지털 서명을 사용 중인 사용자의 신원을 확인하는 암호화 기술입니다.

단계 **1** 구축의 각 노드에서 다음을 위해 시스템 인증서를 구성합니다.

- EAP-TLS와 같은 TLS 지원 인증 프로토콜
- 관리 포털 인증
- 브라우저 및 REST 클라이언트에서 Cisco ISE 웹 포털에 액세스할 수 있도록 허용
- pxGrid 컨트롤러에 대한 액세스 허용

기본적으로 Cisco ISE 노드는 EAP 인증과 관리 포털, 최종 사용자 포털 및 pxGrid 컨트롤러 액세스에 사용되는 SSC(자가서명 인증서)와 함께 미리 설치됩니다. 일반적인 엔터프라이즈 환경에서 이 자가서명 인증서는 신뢰할 수 있는 CA가 서명한 서버 인증서로 교체됩니다.

단계 **2** 사용자와의 신뢰 관계를 설정하는 데 필요한 CA 인증서 및 Cisco ISE에 제공할 디바이스 인증서를 신뢰할 수 있는 인증서 저장소에 저장합니다.

루트 CA 인증서 하나와 중간 CA 인증서 하나 이상으로 구성된 인증서 체인을 사용하여 사용자 또는 디바이스 인증서의 신뢰성을 검증하려면 다음을 수행하십시오.

- 루트 CA에 대해 관련 신뢰 옵션을 활성화합니다.

  Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** >**Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다. 이 창에서 루트 CA 인증서의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다. **Usage(**사용**)** 영역의 **Trusted For(**신뢰 대상**)** 영역에서 필요한 확인란을 선택합니다.

- 루트 CA에 대해 신뢰 옵션을 활성화하지 않으려면 전체 CA 서명 인증서 체인을 신뢰할 수 있는 인증서 저장소로 가져옵니다.

노드 간 통신의 경우에는 Cisco ISE 구축에 포함된 각 노드의 관리자 시스템 인증서를 검증하는 신뢰 인증서를 신뢰할 수 있는 인증서 저장소에 저장해야 합니다. 기본 자가서명 인증서를 노드 간 통신에 사용하려는 경우에는 각 Cisco ISE 노드의 System Certificates(시스템 인증서) 페이지에서 이 인증서를 내보낸 다음 신뢰할 수 있는 인증서 저장소로 가져옵니다. 자가서명 인증서를 CA에서 서명한 인증서로 교체하는 경우에는 적절한 루트 CA 및 중간 CA 인증서만 신뢰할 수 있는 인증서 저장소에 저장하면 됩니다. 이 단계를 완료할 때까지는 Cisco ISE 구축에서 노드를 등록할 수 없습니다.

구축의 클라이언트와 PSN 간 통신을 보호하기 위해 자가서명 인증서를 사용하는 경우 BYOD 사용자가 한 위치에서 다른 위치로 이동하면 EAP-TLS 사용자 인증이 실패합니다. 몇 개의 PSN 간에 서비스를 받아야 하는 인증 요청

의 경우에는 외부에서 서명한 CA 인증서를 사용하여 클라이언트와 PSN 간의 통신을 보호하거나 외부 CA가 서명한 와일드카드 인증서를 사용해야 합니다.

참고 독립형 Cisco ISE 노드 또는 PAN에서 백업을 가져온 후 구축의 노드 하나 이상에서 인증서 컨피그레이션을 변경하는 경우에는 다른 백업을 가져와서 데이터를 복원해야 합니다. 이렇게 하지 않는 경우 이전 백업을 사용하여 데이터를 복원하려고 하면 노드 간의 통신이 실패할 수 있습니다.

와일드카드 인증서

와일드카드 인증서는 와일드카드 표기법(별표 및 도메인 이름 앞의 마침표)을 사용하므로 조직의 여러 호스트 간에 인증서를 공유할 수 있습니다. 예를 들어 인증서 주체의 **CN** 값은 aaa.ise.local과 같은 일반 호스트 이름이고, SAN 필드에는 동일한 일반 호스트 이름과 함께 DNS.1=aaa.ise.local 및 DNS.2=*.ise.local과 같은 와일드카드 표기법이 포함된다고 가정합니다.

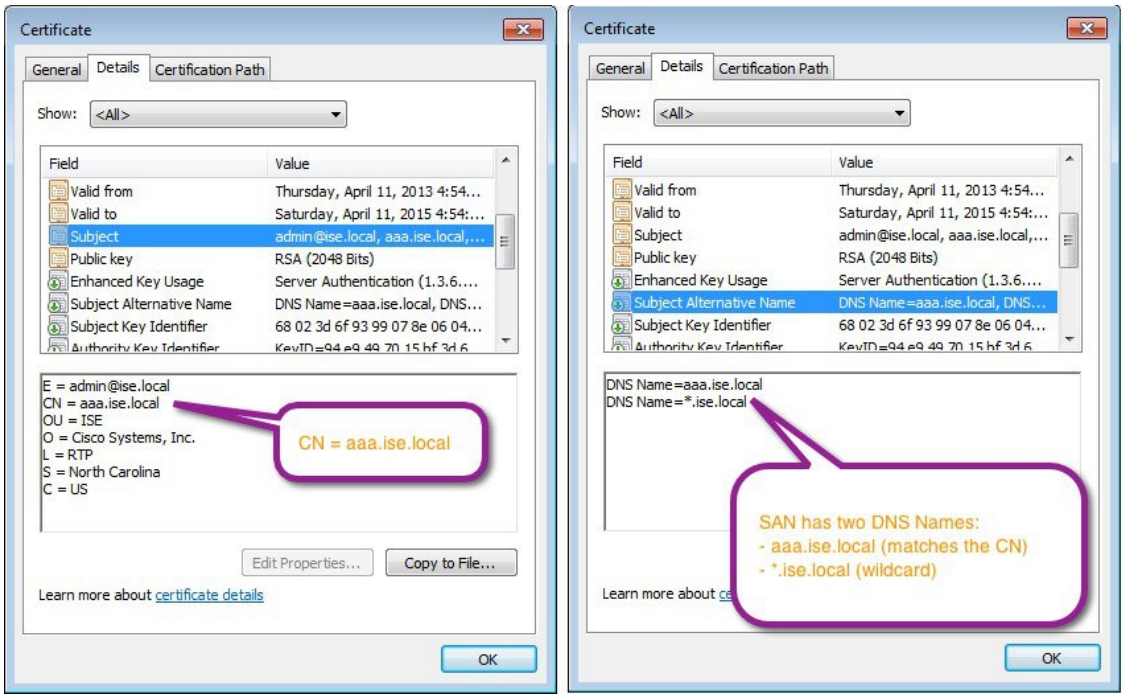
*.ise.local을 사용하도록 와일드카드 인증서를 구성하는 경우 동일한 인증서를 사용하여 DNS 이름이과 같이 ".ise.local"로 끝나는 다른 모든 호스트를 보호할 수 있습니다.:

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

와일드카드 인증서는 일반 인증서와 동일한 방법으로 통신을 보호하며 요청은 동일한 검증 방법을 사용하여 처리됩니다.

다음 그림에는 웹사이트를 보호하는 데 사용되는 와일드카드 인증서의 예가 나와 있습니다.

그림 *6:* 와일드카드 인증서 예



Cisco ISE의 와일드카드 인증서 지원

Cisco ISE는 와일드카드 인증서를 지원합니다. 이전 릴리스에서 Cisco ISE는 HTTPS용으로 활성화된 모든 인증서를 확인하여 CN 필드가 호스트의 FQDN과 정확하게 일치하는지를 확인했습니다. 이 필드가 일치하지 않으면 인증서를 HTTPS 통신에 사용할 수 없었습니다.

이전 릴리스에서 Cisco ISE는 해당 CN 값을 사용하여 url-redirect A-V 쌍 문자열의 변수를 교체했습니다. 모든 CWA(Centralized Web Authentication), 온보딩, 포스처 리디렉션 등에 대해 CN 값이 사용되었습니다.

Cisco ISE는 ISE 노드의 호스트 이름을 CN으로 사용합니다.

HTTPS 및 Extensible Authentication Protocol 통신용 와일드카드 인증서

SSL 또는 TLS 터널링을 이용하는 EAP 프로토콜 및 관리용 Cisco ISE(웹 기반 서비스)에서 와일드카드 서버 인증서를 사용할 수 있습니다. 와일드카드 인증서를 사용하는 경우에는 각 Cisco ISE 노드에 대해 고유한 인증서를 생성하지 않아도 됩니다. 또한 인증서 경고가 표시되지 않도록 하기 위해 여러 FQDN 값을 SAN 필드에 입력할 필요도 없습니다. SAN 필드에 별표(*)를 사용하면 구축의 여러 노드 간에 단일 인증서를 공유할 수 있으며, 인증서 이름 불일치 경고가 표시되지 않습니다. 그러나 와일드카드 인증서를 사용하는 방식은 각 Cisco ISE 노드에 고유한 서버 인증서를 할당하는 방식보다 보안성이 낮은 것으로 간주됩니다.

공개 와일드카드 인증서를 게스트 포털에 할당하고 루트 CA 인증서가 포함된 하위 CA를 가져오는 경우 Cisco ISE 서비스가 재시작될 때까지 인증서 체인이 전송되지 않습니다.

참고 와일드카드 인증서를 사용하는 경우에는 보안 향상을 위해 도메인 공간을 분할하는 것이 좋습니다. 예를 들어 *.example.com 대신 *.amer.example.com으로 도메인을 분할할 수 있습니다. 도메인을 분할하지 않으면 심각한 보안 문제가 발생할 수 있습니다.

와일드카드 인증서에서는 도메인 이름 앞에 별표(*)와 기간이 사용됩니다. 인증서 주체 이름의 공용 이름 값은 aaa.ise.local과 같은 일반 호스트 이름이고 SAN 필드에 *.ise.local과 같은 와일드카드 문자를 사용하는 경우를 예로 들 수 있습니다. Cisco ISE는 와일드카드 문자(*)가 표시되는 식별자의 맨 왼쪽 문자인 와일드카드 인증서를 지원합니다. *.example.com 또는 *.ind.example.com 등을 예로 들 수 있습니다. Cisco ISE는 표시되는 식별자가 와일드카드 문자와 함께 다른 문자를 포함하는 인증서를 지원하지 않습니다. abc*.example.com, a*b.example.com, *abc.example.com 등을 예로 들 수 있습니다.

URL 리디렉션의 인증된 도메인 이름

중앙 웹 인증, 디바이스 등록 웹 인증, 기본 신청자 프로비저닝, 모바일 디바이스 관리, 클라이언트 프로비저닝 및 포스처 서비스용으로 권한 부여 프로파일 리디렉션이 수행됩니다. Cisco ISE가 권한 부여 프로파일 리디렉션을 구축할 때 결과로 생성된 cisco-av-pair에는 다음과 유사한 문자열이 포함됩니다.

url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa와 같은 문자열이 포함됩니다.

이 요청을 처리할 때 Cisco ISE는 이 문자열의 일부 키워드를 실제 값으로 대체합니다. 예를 들어 SessionIdValue는 요청의 실제 세션 ID로 바뀝니다. eth0 인터페이스의 경우 Cisco ISE는 URL의 IP를 Cisco ISE 노드의 FQDN으로 바꿉니다. eth0가 아닌 인터페이스의 경우 Cisco ISE는 URL의 IP 주소를 사용합니다. eth1~eth3 인터페이스에 대해 호스트 별칭(이름)을 할당할 수 있습니다. Cisco ISE는 URL 리디렉션 중에 IP 주소를 이러한 별칭으로 대체할 수 있습니다.

이렇게 하려는 경우 Cisco ISE CLI ISE /admin(config)# 프롬프트의 컨피그레이션 모드에서 **ip host** 명령을 사용하면 됩니다.

ip host *IP_address host-alias FQDN-string*

여기서 *IP_address*는 네트워크 인터페이스의 IP 주소(eth1, eth2 또는 eth3)이고 *host-alias*는 네트워크 인터페이스에 할당하는 이름입니다. *FQDN-string*은 네트워크 인터페이스의 인증된 도메인 이름입니다. 이 명령을 사용하여 *host-alias* 또는 *FQDN-string* 중 하나 또는 둘 다를 네트워크 인터페이스에 할당할 수 있습니다.

ip host 명령을 사용하는 예는 ip host a.b.c.d sales sales.amerxyz.com과 같습니다.

eth0이 아닌 인터페이스에 호스트 별칭을 할당한 후에는 **application start ise** 명령을 사용하여 Cisco ISE에서 애플리케이션 서비스를 재시작해야 합니다.

네트워크 인터페이스와 호스트 별칭의 연결을 제거하려면 이 명령의 **no** 형식을 사용합니다.

no ip host *IP_address host-alias FQDN-string*

호스트 별칭 정의를 보려면 **show running-config** 명령을 사용합니다.

*FQDN-string*을 제공하는 경우 Cisco ISE는 URL의 IP 주소를 FQDN으로 바꿉니다. 호스트 별칭만 제공하는 경우 Cisco ISE는 호스트 별칭을 구성된 IP 도메인 이름과 결합하여 완전한 FQDN을 만든 다음 URL의 IP 주소를 FQDN으로 바꿉니다. 네트워크 인터페이스를 호스트 별칭에 매핑하지 않으면 Cisco ISE는 URL에 포함된 네트워크 인터페이스의 IP 주소를 사용합니다.

클라이언트 프로비저닝이나 기본 신청자 또는 게스트 플로우용으로 eth0이 아닌 인터페이스를 사용할 때는 PSN 인증서의 SAN 필드에서 eth0이 아닌 인터페이스의 IP 주소 또는 호스트 별칭을 적절하게 구성해야 합니다.

와일드카드 인증서를 사용하는 경우의 이점

- 비용 절감: 서드 파티 CA에서 서명한 인증서는 비용이 많이 들며 특히 서버 수가 증가할수록 비용이 큽니다. 와일드카드 인증서는 Cisco ISE 구축의 여러 노드에서 사용할 수 있습니다.
- 운영 효율성: 와일드카드 인증서를 사용하면 모든 PSN이 EAP 및 웹 서비스에 대해 동일한 인증서를 공유할 수 있습니다. 막대한 비용 절감 효과를 거둘 수 있을 뿐 아니라, 인증서를 한 번 생성하여 모든 PSN에 적용하는 방식으로 인증서 관리 작업도 간소화할 수 있습니다.
- 인증 오류 감소: 와일드카드 인증서는 클라이언트가 프로파일에 신뢰할 수 있는 인증서를 저장하지만 서명 루트를 신뢰할 수 있는 iOS 키 체인을 따르지 않는 Apple iOS 디바이스에서 발생하는 문제를 해결해 줍니다. PSN과 처음 통신하는 iOS 클라이언트는 신뢰할 수 있는 CA가 인증서에 서명한 경우에도 PSN 인증서를 명시적으로 신뢰하지 않습니다. 와일드카드 인증서를 사용하면 인증서가 모든 PSN에서 동일하게 유지되므로 사용자가 인증서를 수락하기만 하면 여러 PSN에 대한 이후의 인증은 오류 또는 메시지 없이 진행됩니다.
- 신청자 컨피그레이션 간소화: 예를 들어 PEAP-MSCHAPv2 및 신뢰할 수 있는 서버 인증서가 있는 Microsoft Windows 신청자에서는 각 서버 인증서를 신뢰하도록 지정해야 합니다. 아니면 클라이언트가 다른 PSN을 사용하여 연결할 때 사용자에게 각 PSN 인증서를 신뢰하는지 묻는 메시지가 표시될 수 있습니다. 와일드카드 인증서를 사용하면 각 PSN의 개별 인증서가 아니라 단일 서버 인증서를 신뢰할 수 있습니다.
- 와일드카드 인증서를 사용하면 메시지 수를 줄이고 원활한 연결을 진행할 수 있으므로 사용자 환경을 개선할 수 있습니다.

와일드카드 인증서를 사용하는 경우의 단점

다음은 와일드카드 인증서 사용과 관련된 몇 가지 보안 고려 사항입니다.

- 감사 기능 손실 및 미거부
- 개인 키의 노출 증가
- 일반적이지 않거나 관리자가 이해할 수 없음

와일드카드 인증서는 각 Cisco ISE 노드의 고유 서버 인증서보다 보안성이 낮은 것으로 간주됩니다. 그러나 보안 위험 문제보다 비용 및 다른 운영 관련 이점이 훨씬 큽니다.

Cisco Adaptive Security Appliance와 같은 보안 디바이스도 와일드카드 인증서를 지원합니다.

와일드카드 인증서를 구축할 때에는 주의해야 합니다. 예를 들어 *.company.local을 사용하여 인증서를 생성하는 경우 공격자가 개인 키를 복구할 수 있으면 공격자는 company.local 도메인의 서버를 스푸핑할 수 있습니다. 그러므로 이러한 종류의 문제를 방지하려면 도메인 공간을 분할하는 것이 좋습니다.

이러한 문제를 해결하고 사용 범위를 제한하려면 조직의 특정 하위 도메인을 보호하도록 와일드카드 인증서를 사용할 수 있습니다. 와일드카드를 지정하려는 공통 이름의 하위 도메인 영역에 별표(*)를 추가합니다.

예를 들어 *.ise.company.local에 대한 와일드카드 인증서를 구성하는 경우 다음과 같이 DNS 이름이 ".ise.company.local"로 끝나는 다른 모든 호스트를 해당 인증서를 사용하여 보호할 수 있습니다.

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

와일드카드 인증서 호환성

와일드카드 인증서는 일반적으로 인증서 주체의 CN(Common Name)으로 나열되는 와일드카드를 사용하여 생성됩니다. Cisco ISE에서는 이러한 생성 유형을 지원합니다. 그러나 모든 엔드포인트 신청자가 인증서 주체의 와일드카드 문자를 지원하는 것은 아닙니다.

테스트를 거친 모든 Microsoft 기본 신청자(현재 중단된 Windows Mobile 포함)는 인증서 주체에서 와일드카드 문자를 지원하지 않습니다.

Subject(주체) 필드에서 와일드카드 문자 사용을 허용할 수 있는 Cisco AnyConnect NAM(Network Access Manager) 등의 다른 신청자를 사용할 수 있습니다.

또한 인증서의 주체 대체 이름에 특정 하위 도메인을 포함하여 호환되지 않는 디바이스에서 사용 가능한 DigiCert의 Wildcard Plus와 같은 특수 와일드카드 인증서를 사용할 수도 있습니다.

Microsoft 신청자 제한으로 인해 와일드카드 인증서를 사용할 수 없다고 생각할 수도 있지만, Microsoft 기본 신청자를 포함하여 보안 액세스용으로 테스트된 모든 디바이스에서 사용할 수 있는 와일드카드 인증서를 생성하는 대체 방법이 있습니다.

이러한 인증서를 생성하려면 주체에 와일드카드 문자를 사용하는 대신 SAN(Subject Alterative Name) 필드에 와일드카드 문자를 사용해야 합니다. SAN 필드에서 도메인 이름(DNS 이름) 확인용 확장을 유지 관리할 수 있습니다. 자세한 내용은 RFC 6125 및 2128을 참고해 주십시오.

인증서 계층 구조

관리 포털에서 모든 엔드포인트, 시스템 및 신뢰할 수 있는 인증서의 인증서 계층 구조 또는 인증서 신뢰 체인을 확인할 수 있습니다. 인증서 계층 구조에는 인증서, 모든 중간 CA 인증서 및 루트 인증서가 포함됩니다. 예를 들어 관리 포털에서 시스템 인증서를 보도록 선택하면 해당 시스템 인증서의 세부정보가 표시됩니다. 인증서 계층 구조는 인증서의 상단에 나타납니다. 계층 구조에서 인증서를 클릭하면 해당 세부정보를 볼 수 있습니다. 셀프 서명 인증서에는 계층 구조 또는 신뢰 체인이 없습니다.

인증서 목록 창의 **Status(**상태**)** 열에는 다음 아이콘 중 하나가 표시됩니다.

- 녹색 아이콘: 유효한 인증서(유효한 신뢰 체인)를 나타냅니다.
- 빨간색 아이콘: 오류(예: 신뢰 인증서가 누락되었거나 만료됨)를 나타냅니다.
- 노란색 아이콘: 인증서가 곧 만료된다고 경고하며 갱신하라는 메시지가 표시됩니다.

시스템 인증서

Cisco ISE 시스템 인증서는 구축의 다른 노드 및 클라이언트 애플리케이션에 대해 Cisco ISE 노드를 식별하는 서버 인증서입니다. 시스템 인증서는 다음과 같이 사용됩니다.

- Cisco ISE 구축에서 노드 간 통신에 사용됩니다. 이러한 인증서의 **Usage(**사용**)** 영역에서 **Admin(**관리**)** 확인란을 선택합니다.
- 브라우저 및 Cisco ISE 웹 포털에 연결되는 REST 클라이언트에 사용됩니다. 이러한 인증서의 **Usage(**사용**)** 영역에서 **Portal(**포털**)** 확인란을 선택합니다.
- PEAP 및 EAP-FAST와 함께 외부 TLS 터널을 형성하는 데 사용됩니다. **Usage(**사용**)** 영역에서 EAP-TLS, PEAP 및 EAP-FAST와의 상호 인증을 위한 **EAP Authentication(EAP** 인증**)** 확인란을 선택합니다.
- RADIUS DTLS 서버 인증에 사용됩니다.
- SAML IdP(Identity Provider)와 통신하는 데 사용됩니다. 이러한 인증서의 **Usage(**사용**)** 영역에서 **SAML** 확인란을 선택합니다. SAML 옵션을 선택하는 경우 다른 서비스에 이 인증서를 사용할 수 없습니다.
- pxGrid 컨트롤러와의 통신에 사용됩니다. 이러한 인증서의 **Usage(**사용**)** 영역에서 **pxGrid** 확인란을 선택합니다.

Cisco ISE 구축의 각 노드에 유효한 시스템 인증서를 설치합니다. 기본적으로 설치 중에 Cisco ISE 노드에 자체 서명 인증서 2개와 내부 Cisco ISE CA에서 서명 1개가 생성됩니다.

- EAP, 관리자, 포털, RADIUS DTLS (키 크기는 2048이며 1년 동안 유효함)
- SAML IdP와의 통신을 보호하는 데 사용할 수 있는 자체 서명 SAML 서버 인증서(키 크기는 2048이며 1년 동안 유효함)
- pxGrid 클라이언트와의 통신을 보호하는 데 사용할 수 있는 내부 Cisco ISE CA 서명 서버 인증서(키 크기가 4096이고 1년 동안 유효함).

구축을 설정하고 보조 노드를 등록하면 pxGrid 컨트롤러용으로 지정된 인증서가 기본 노드의 CA에서 서명한 인증서로 자동 교체됩니다. 따라서 모든 pxGrid 인증서는 동일한 PKI 신뢰 계층 구조의 일부가 됩니다.

참고 가져온 와일드카드 시스템 인증서를 다른 노드(노드 간 통신을 위해)로 내보내는 경우 인증서 및 개인 키를 내보내고 암호화 비밀번호를 지정해야 합니다. 가져오는 동안 인증서, 개인 키 및 암호화 비밀번호가 필요합니다.

참고 릴리스에 대해 지원되는 키 및 암호 정보를 찾으려면 Cisco Identity Services Engine Network Component Compatibility의 해당 버전을 확인하십시오.

보안을 향상하기 위해 셀프 서명 인증서는 CA 서명 인증서로 대체하는 것이 좋습니다. CA 서명 인증서를 가져오려면 다음을 수행해야 합니다.

1. 인증서 서명 요청을 생성하고 인증 기관에 제출, 88 페이지
2. 신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 81 페이지
3. 인증서 서명 요청에 대한 CA 서명 인증서 바인딩, 89 페이지

ISE 커뮤니티 리소스

방법: ISE 서버 측 인증서 구현

Certificate Renewal on Cisco Identity Services Engine Configuration Guide

시스템 인증서 보기

System Certificate(시스템 인증서**)** 창에는 Cisco ISE에 추가된 모든 시스템 인증서가 나열됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다.

단계 **2** 다음 열이 **System Certificates(**시스템 인증서**)** 창에 표시됩니다.

- **Friendly Name(**식별 이름**)**: 인증서의 이름입니다.
- **Usage(**사용**)**: 이 인증서가 사용되는 서비스입니다.
- **Portal group tag(**포털 그룹 태그**)**: 포털에서 사용하도록 지정된 인증서에만 해당되며, 이 필드가 포털에 사용해야 하는 인증서를 지정합니다.
- **Issued To(**발급 대상**)**: 인증서 주체의 공용 이름입니다.
- **Issued By(**발급자**)**: 인증서 발급자의 공용 이름입니다.
- **Valid From(**유효 기간 시작**)**: 인증서가 생성된 날짜이며, "Not Before" 인증서 속성이라고도 합니다.
- **Valid To (Expiration)(**만료 날짜**)**: 인증서의 만료 날짜이며, "Not After" 인증서 속성이라고도 합니다. 만료 날짜 옆에 다음 아이콘이 표시됩니다.
  - 녹색 아이콘: 만료 날짜까지 남은 기간이 90일 이상입니다.
  - 파란색 아이콘: 90일 이내에 만료됩니다.
  - 노란색 아이콘: 60일 이내에 만료됩니다.

- 주황색 아이콘: 30일 이내에 만료됩니다.
- 빨간색 아이콘: 만료되었습니다.

시스템 인증서 가져오기

관리 포털에서 Cisco ISE 노드의 시스템 인증서를 가져올 수 있습니다.

참고 기본 PAN 노드에서 관리 역할 인증서의 인증서를 변경하면 다른 모든 노드에서 서비스가 재시작됩니다. 시스템은 기본 PAN이 재시작되고 나면 노드를 한 번에 한 개씩 재시작합니다.

시작하기 전에

- 클라이언트 브라우저를 실행 중인 시스템에 시스템 인증서 및 개인 키 파일이 있는지 확인합니다.
- 가져오는 시스템 인증서에 외부 CA가 서명을 한 경우 관련 루트 및 중간 CA 인증서를 신뢰할 수 있는 인증서 저장소(**Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**)로 가져옵니다.
- 가져오는 시스템 인증서에 CA 플래그가 true로 설정된 기본 제한 확장명이 포함되어 있으면 키 사용 확장이 있는지 확인하고, keyEncipherment 비트나 keyAgreement 중 하나 또는 두 비트가 모두 설정되어 있는지 확인합니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1**

단계 **2** **Import(**가져오기**)**를 클릭합니다.
Import Server Certificate(서버 인증서 가져오기**)** 창이 표시됩니다.

단계 **3** 가져올 인증서에 대한 값을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

시스템 인증서 가져오기 설정

다음 표에서는 서버 인증서를 가져오는 데 사용할 수 있는 **Import System Certificate(**시스템 인증서 가져오기**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**입니다. **Import(**가져오기**)**를 클릭합니다.

표 *8:* 시스템 인증서 가져오기 설정

필드 이름	설명
Select Node(노드 선택**)**	(필수) 드롭다운 목록에서 시스템 인증서를 가져올 Cisco ISE 노드를 선택합니다.
Certificate File(인증서 파일**)**	(필수) **Choose File(**파일 선택**)**을 클릭하고 로컬 시스템에서 인증서 파일을 선택합니다.
Private Key File(개인 키 파일**)**	(필수) **Choose File(**파일 선택**)**을 클릭하고 로컬 시스템에서 개인 키 파일을 선택합니다.
Password(비밀번호**)**	(필수) 개인 키 파일의 암호를 해독하기 위한 비밀번호를 입력합니다.
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다. 이름을 지정하지 않으면 Cisco ISE는 다음 형식으로 이름을 자동으로 생성합니다. <common name> # <issuer> # <nnnnn>에서 <nnnnn>은 고유한 5자리 숫자입니다.
Allow Wildcard Certificates(와일드카드 인증서 허용**)**	와일드카드 인증서를 가져오려면 이 확인란을 선택합니다. 와일드카드 인증서에서는 와일드카드 표기법(도메인 이름 앞에 별표와 기간)이 사용됩니다. 와일드카드 인증서는 조직의 여러 호스트에서 공유됩니다. 이 확인란을 선택하는 경우 Cisco ISE는 구축의 기타 모든 노드로 이 인증서를 가져옵니다.
Validate Certificate Extensions(인증서 확장명 검증**)**	Cisco ISE가 인증서 확장명을 검증하도록 지정하려면 이 확인란을 선택합니다. 이 확인란을 선택하는 경우 가져오는 인증서에 CA 플래그가 true로 설정된 기본 제한 확장명이 포함되어 있으면 키 사용 확장이 있는지 확인합니다. keyEncipherment 비트나 keyAgreement 비트 중 하나 또는 둘 모두 설정되어야 합니다.

필드 이름	설명
Usage(사용)	이 시스템 인증서를 사용할 서비스를 선택합니다. • **Admin(관리)**: 구축의 Cisco ISE 노드 간 통신 및 관리 포털과의 통신을 보호하는 데 사용되는 서버 인증서입니다. 참고 기본 PAN에서 관리자 역할 인증서의 인증서를 변경하면 다른 모든 Cisco ISE 노드에서 서비스가 재시작됩니다. • **EAP Authentication(EAP 인증)**: SSL 또는 TLS 터널링용 EAP 프로토콜을 사용하는 인증에 사용되는 서버 인증서입니다. • **RADIUS DTLS**: RADIUS DTLS 인증에 사용되는 서버 인증서입니다. • **pxGrid**: pxGrid 클라이언트와 서버 간의 통신을 보호하기 위한 클라이언트 및 서버 인증서입니다. • **ISE Messaging Service(ISE 메시징 서비스)**: 내장 UDP 시스템 로그 수집 대상(LogCollector 및 LogCollector2)에 대해 MnT WAN 지속성을 지원하는 **Syslog Over Cisco ISE Messaging(Cisco ISE 메시징을 통한 시스템 로그)**에서 사용됩니다. • **SAML**: SAML ID 제공자와의 통신을 보호하는 데 사용되는 서버 인증서입니다. SAML에 사용하도록 지정된 인증서는 관리, EAP 인증 등의 기타 서비스에는 사용할 수 없습니다. • **Portal(포털)**: 모든 Cisco ISE 웹 포털과의 통신을 보호하는 데 사용되는 서버 인증서입니다.

관련 항목

시스템 인증서, 63 페이지
시스템 인증서 보기, 64 페이지
시스템 인증서 가져오기, 65 페이지

셀프 서명 인증서 생성

SSC(자가서명 인증서)를 생성하여 새 로컬 인증서를 추가할 수 있습니다. Cisco에서는 내부 테스트 및 평가에 필요한 SSC(자가서명 인증서)만 사용하기를 권장합니다. 생산 환경에서 Cisco ISE를 구축하려는 경우에는 생산 네트워크 전체에서 보다 균일하게 수락될 수 있도록 가능하면 항상 CA 서명 인증서를 사용하십시오.

참고 SSC(자가서명 인증서)를 사용 중일 때 Cisco ISE 노드의 호스트 이름을 변경해야 하는 경우에는 Cisco ISE 노드의 관리 포털에 로그인하여 이전 호스트 이름이 지정된 SSC(자가서명 인증서)를 삭제한 다음 새 SSC(자가서명 인증서)를 생성해야 합니다. 이렇게 하지 않으면 Cisco ISE는 이전 호스트 이름이 지정된 SSC(자가서명 인증서)를 계속 사용합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

셀프 서명 인증서 설정

다음 표에서는 셀프 서명 인증서 생성 창의 필드에 대해 설명합니다. 이 창에서는 노드 간 통신, EAP-TLS 인증, Cisco ISE 웹 포털용 시스템 인증서를 생성하고 pxGrid 컨트롤러와 통신할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**입니다. 셀프 서명 인증서 생성을 클릭합니다.

표 ***9:*** 셀프 서명 인증서 설정

필드 이름	사용 지침
Select Node(노드 선택**)**	(필수) 시스템 인증서를 생성할 노드입니다.
Common Name(공통 이름**) (CN)**	(SAN을 지정하지 않는 경우 필수) 기본적으로 일반 이름은 셀프 서명 인증서를 생성하는 Cisco ISE 노드의 FQDN입니다.
Organizational Unit(OU)(조직 단위**)**	조직 단위의 이름입니다. Engineering 등을 예로 들 수 있습니다.
Organization(O)(조직**)**	조직의 이름입니다. Cisco 등을 예로 들 수 있습니다.
City (L)(L(구/군/시**))**	(약어로 표기하지 않음) 구/군/시의 이름입니다. San Jose 등을 예로 들 수 있습니다.
State(ST)(시/도**)**	(약어로 표기하지 않음) 시/도의 이름입니다. California 등을 예로 들 수 있습니다.
Country(C)(국가**)**	국가의 이름입니다. 2자리 ISO 국가 코드를 입력해야 합니다. US 등을 예로 들 수 있습니다.
SAN(Subject Alternative Name)	인증서와 연결된 IP 주소, DNS 이름 또는 URI(Uniform Resource Identifier)
Key Type(키 유형**)**	공개 키(RSA 또는 ECDSA)를 생성하는 데 사용할 알고리즘입니다.

필드 이름	사용 지침
Key Length(키 길이**)**	공개 키의 비트 크기입니다. RSA를 위한 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • 512 • 1024 • 2048 • 4096 ECDSA를 위한 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • 256 • 384 참고 RSA 및 ECDSA 공개 키는 동일한 보안 레벨에서 키 길이가 다를 수 있습니다. 공용 CA 서명 인증서를 가져오거나 FIPS 호환 정책 관리 시스템으로 Cisco ISE를 구축하려면 2048을 선택합니다.
Digest to Sign With(서명에 사용할 다이제스트**)**	드롭다운 목록에서 다음 해싱 알고리즘 중 하나를 선택합니다. • SHA-1 • SHA-256
인증서 정책	인증서가 준수해야 하는 인증서 정책 OID 또는 OID 목록을 입력합니다. 쉼표나 공백을 사용하여 OID를 구분합니다.
Expiration TTL(만료 **TTL)**	인증서가 만료될 때까지의 기간(일)을 지정합니다. 드롭다운 목록에서 필요한 값을 선택합니다.
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다. 이름을 지정하지 않으면 Cisco ISE가 <common name> # <issuer> # <nnnnn> 형식으로 이름을 자동 생성합니다. 여기서 <nnnnn>은 고유한 5자리 숫자입니다.
Allow Wildcard Certificates(와일드카드 인증서 허용**)**	셀프 서명 와일드카드 인증서를 생성하려면 이 확인란을 선택합니다. 와일드카드 인증서는 와일드카드 표기법(별표 및 도메인 이름 앞의 마침표)을 사용하므로 조직의 여러 호스트 간에 인증서를 공유할 수 있습니다.

필드 이름	사용 지침
Usage(사용)	이 시스템 인증서를 사용할 서비스를 선택합니다. • **Admin(관리)**: 구축의 Cisco ISE 노드 간 통신 및 관리 포털과의 통신을 보호하는 데 사용되는 서버 인증서입니다. • **EAP Authentication(EAP 인증)**: SSL 또는 TLS 터널링용 EAP 프로토콜을 사용하는 인증에 사용되는 서버 인증서입니다. • **RADIUS DTLS**: RADIUS DTLS 인증에 사용되는 서버 인증서입니다. • **pxGrid**: pxGrid 클라이언트와 서버 간의 통신을 보호하기 위한 클라이언트 및 서버 인증서입니다. • **SAML**: SAML ID 제공자와의 통신을 보호하는 데 사용되는 서버 인증서입니다. SAML에 사용하도록 지정된 인증서는 관리, EAP 인증 등의 기타 서비스에는 사용할 수 없습니다. • **Portal(포털)**: 모든 Cisco ISE 웹 포털과의 통신을 보호하는 데 사용되는 서버 인증서입니다.

관련 항목

시스템 인증서, 63 페이지
시스템 인증서 보기, 64 페이지
셀프 서명 인증서 생성, 67 페이지

시스템 인증서 편집

이 창을 사용하여 시스템 인증서를 편집하고 셀프 서명 인증서를 갱신할 수 있습니다. 와일드카드 인증서를 편집하면 변경사항이 구축의 모든 노드로 복제됩니다. 와일드카드 인증서를 삭제하면 구축의 모든 노드에서 해당 와일드카드 인증서가 제거됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** 선택Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Certificates(인증서)** > **System Certificates(시스템 인증서)**를 선택합니다.

단계 **2** 편집할 인증서 옆의 확인란을 선택하고 **Edit(편집)**를 클릭합니다.

단계 **3** 셀프 서명 인증서를 갱신하려면 **Renewal Period(갱신 기간)** 확인란을 선택하고 만료 TTL(Time to Live)를 일, 주, 월 또는 연도 단위로 입력합니다. 드롭다운 목록에서 필요한 값을 를 선택합니다.

단계 **4** **Save(저장)**를 클릭합니다.

Admin(관리**)** 확인란을 선택하면 Cisco ISE 노드의 애플리케이션 서버가 다시 시작됩니다. 또한 Cisco ISE 노드가 구축의 PAN인 경우에는 구축 내 기타 모든 노드의 애플리케이션 서버도 다시 시작됩니다. 시스템은 기본 PAN이 재시작되고 나면 노드를 한 번에 한 개씩 재시작합니다.

참고 Chrome 65 이상을 사용하여 Cisco ISE를 시작하면 URL이 성공적으로 리디렉션되어도 브라우저에서 BYOD 포털 또는 게스트 포털이 시작되지 않을 수 있습니다. 이는 모든 인증서에 주체 대체 이름 필드를 요구하는 Google의 새로운 보안 기능 때문입니다. Cisco ISE 릴리스 2.4 이상의 경우 Subject Alternative Name(주체 대체 이름) 필드를 입력해야 합니다.

Chrome 65 이상에서 실행하려면 다음 단계를 수행합니다.

1. Subject Alternative Name(주체 대체 이름) 필드를 입력해 Cisco ISE GUI에서 새 자체 서명 인증서를 생성합니다. DNS 및 IP 주소를 모두 입력해야 합니다.

2. Cisco ISE 서비스가 다시 시작됩니다.

3. Chrome 브라우저에서 포털을 리디렉션합니다.

4. 브라우저에서 View Certificate(인증서보기)>Details(세부정보)>Copy the certificate by selecting base-64 encoded(base-64 인코딩을 선택하여 인증서 복사)를 실행합니다.

5. 신뢰할 수 있는 경로에 인증서를 설치합니다.

6. Chrome 브라우저를 닫고 포털 리디렉션을 시도합니다.

참고 운영체제 Win RS4 또는 RS5에서 브라우저 Firefox 64 이상 릴리스에 대해 무선 BYOD 설정을 구성할 때 인증서 예외를 추가하지 못할 수 있습니다. 이 동작은 Firefox 64 이상 릴리스를 새로 설치하는 경우에 예상되며, 이전 버전에서 Firefox 64 이상으로 업그레이드하는 경우에는 발생하지 않습니다. 이 경우 다음과 같은 단계를 통해 인증서 예외를 추가할 수 있습니다.

1. BYOD 플로우 단일 또는 이중 PEAP 또는 TLS를 구성합니다.
2. Windows ALL 옵션을 사용해 CP 정책을 구성합니다.
3. 엔드 클라이언트 Windows RS4 또는 Windows RS5에서 Dot1.x 또는 MAB SSID를 연결합니다.
4. 게스트 또는 BYOD 포털로의 리디렉션을 위해 FF64 브라우저에 1.1.1.1을 입력합니다.
5. **Add Exception(**예외 추가**)** > **Unable to add certificate(**인증서 추가 불가능**)**을 클릭한 다음 플로우를 진행합니다.

이를 해결하는 방법으로, Firefox 64용 인증서를 수동으로 추가합니다. Firefox 64 브라우저에서 **Options(**옵션**)** > **Privacy & Settings(**개인 정보 및 설정**)** > **View Certificates(**인증서 보기**)** > **Servers(**서버**)** > **Add Exception(**예외 추가**)**을 선택합니다.

시스템 인증서 삭제

더 이상 사용하지 않는 시스템 인증서는 삭제할 수 있습니다.

시스템 인증서 저장소에서 한 번에 여러 인증서를 삭제할 수는 있지만, 이 경우 관리 및 EAP 인증에 사용할 수 있는 인증서가 하나 이상 있어야 합니다. 또한 관리, EAP 인증, 포털 또는 pxGrid 컨트롤러에 사용되는 인증서는 삭제할 수 없습니다. 단, 서비스를 비활성화하는 경우 pxGrid 인증서는 삭제할 수 있습니다.

와일드카드 인증서를 삭제하도록 선택하는 경우에는 구축의 모든 Cisco ISE 노드에서 인증서가 제거됩니다.

단계 **1** 선택Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다.

단계 **2** 삭제할 인증서 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

경고 메시지가 표시됩니다.

단계 **3** **Yes(**예**)**를 클릭하여 인증서를 삭제합니다.

시스템 인증서 내보내기

시스템 인증서 또는 인증서와 그 연결된 개인 키를 내보낼 수 있습니다. 인증서 및 해당 개인 키를 백업용으로 내보내는 경우 나중에 필요하면 인증서와 키를 다시 가져올 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** 선택Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **3** 인증서만 내보낼지 아니면 인증서 및 연결된 개인 키를 내보낼지를 선택합니다.

팁 인증서와 연결된 개인 키의 값이 노출될 수 있으므로 개인 키는 내보내지 않는 것이 좋습니다. 노드 간 통신용으로 와일드카드 시스템 인증서를 다른 Cisco ISE 노드로 가져오기 위해 내보내는 등의 경우와 같이 개인 키를 내보내야 하는 경우에는 개인 키용 암호화 비밀번호를 지정합니다. 개인 키의 암호를 해독하려면 이 인증서를 다른 Cisco ISE 노드로 가져오는 동안 이 비밀번호를 지정해야 합니다.

단계 **4** 개인 키를 내보내도록 선택한 경우 비밀번호를 입력합니다. 비밀번호는 8자 이상이어야 합니다.

단계 **5** **Export(**내보내기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 파일 시스템에 인증서를 저장합니다.

인증서만 내보내는 경우에는 PEM 형식으로 인증서가 저장됩니다. 인증서와 개인 키를 모두 내보내는 경우에는 PEM 형식 인증서와 암호화된 개인 키 파일을 포함하는 .zip 파일로 인증서가 내보내집니다.

신뢰할 수 있는 인증서 저장소

신뢰할 수 있는 인증서 저장소에는 신뢰 및 SCEP(Simple Certificate Enrollment Protocol)에 사용되는 X.509 인증서가 포함되어 있습니다.

신뢰할 수 있는 인증서 저장소의 인증서는 기본 PAN에서 관리되고 Cisco ISE 구축의 각 노드에 복제됩니다. Cisco ISE는 와일드카드 인증서를 지원합니다.

Cisco ISE는 다음과 같은 용도로 신뢰할 수 있는 인증서를 사용합니다.

- 인증서 기반 관리자 인증을 사용하여 ISE-PIC관리 포털에 액세스하는 Cisco ISE 관리자 및 엔드포인트에서 인증을 위해 사용하는 클라이언트 인증서 확인
- 구축에 있는 Cisco ISE 노드 간의 통신 보호 활성화. 신뢰할 수 있는 인증서 저장소는 구축의 각 노드에 있는 시스템 인증서와의 신뢰 관계를 설정하는 데 필요한 CA 인증서 체인을 포함해야 합니다.
  - 셀프 서명 인증서는 시스템 인증서에 사용되고 각 노드의 셀프 서명 인증서는 PAN의 신뢰할 수 있는 인증서 저장소에 위치해야 합니다.
  - CA 서명 인증서가 시스템 인증서로 사용되는 경우 CA 루트 인증서와 함께 신뢰 체인의 중간 인증서는 PAN의 신뢰할 수 있는 인증서 저장소에 위치해야 합니다.
- 보안 LDAP 인증을 활성화하려면 SSL을 통해 액세스하는 LDAP ID 소스를 정의할 때는 인증서 저장소의 인증서를 선택해야 합니다.
- 개인 디바이스 포털을 사용하여 네트워크에 등록할 수 있도록 개인 디바이스에 배포. Cisco ISE는 개인 디바이스 등록을 지원하기 위해 PSN에 SCEP를 구현합니다. 등록 디바이스는 SCEP 프로토콜을 사용하여 PSN에서 클라이언트 인증서를 요청할 수 있습니다. PSN에는 중개자 역할을 하는 RA(Registration Authority)가 포함되어 있습니다. RA는 등록 디바이스로부터 요청을 받고 검증한 다음 요청을 외부 CA 또는 내부 Cisco ISE CA로 전달하는데, 이 CA에서 클라이언트 인증서를 발급합니다. CA는 인증서를 다시 RA로 보내고 RA에서 디바이스로 인증서를 반환합니다.

  Cisco ISE에 사용되는 각 SCEP CA는 SCEP RA 프로파일로 정의됩니다. SCEP RA 프로파일이 생성되면 다음 두 개의 인증서가 자동으로 신뢰할 수 있는 인증서 저장소에 추가됩니다.

  - CA 인증서(셀프 서명 인증서)
  - CA가 서명한 RA 인증서(인증서 요청 에이전트 인증서)

  SCEP 프로토콜 요건에 따라 RA에서 이러한 두 인증서를 등록 디바이스에 제공해야 합니다. 신뢰할 수 있는 인증서 저장소에서 이러한 두 인증서를 대체하면 해당 노드의 RA에 사용되도록 인증서가 모든 PSN 노드로 복제됩니다.

참고 SCEP RA 프로파일이 제거되면 연결된 CA 체인도 신뢰할 수 있는 인증서 저장소에서 제거됩니다. 그러나 보안 시스템 로그, LDAP, 시스템 또는 신뢰 인증서에서 동일한 인증서를 참조하는 경우 SCEP 프로파일만 삭제됩니다.

참고

- Cisco ISE로 가져온 X.509 인증서는 PEM(Privacy-Enhanced Mail) 또는 DER(Distinguished Encoding Rule) 형식이어야 합니다. 인증서 체인, 시스템 인증서와 여기에 서명하는 신뢰 인증서 시퀀스를 포함하는 파일은 특정 제한 사항에 따라 가져올 수 있습니다.
- 공개 와일드카드 인증서를 게스트 포털에 할당하고 루트 CA 인증서가 포함된 하위 CA를 가져오는 경우 Cisco ISE 서비스가 재시작될 때까지 인증서 체인이 전송되지 않습니다.

ISE 커뮤니티 리소스

ISE 2.0에 타사 CA 인증서 설치

신뢰할 수 있는 인증서 저장소의 인증서

신뢰할 수 있는 인증서 저장소는 신뢰할 수 있는 인증서, 즉 Manufacturing 인증서, 루트 인증서, 및 다른 신뢰할 수 있는 인증서로 미리 채워져 있습니다. 루트 인증서(Cisco 루트 CA)는 Manufacturing (Cisco CA Manufacturing) 인증서에 서명합니다. 이 인증서는 기본적으로 비활성화되어 있습니다. 구축에서 Cisco IP Phone을 엔드포인트로 사용하는 경우 이러한 두 인증서를 활성화해야 IP Phone에 대한 Cisco 서명 클라이언트 인증서를 인증할 수 있습니다.

신뢰할 수 있는 인증서 목록

다음 표에서는 관리 노드에 추가된 신뢰할 수 있는 인증서 목록이 표시되는 **Trusted Certificates(**신뢰할 수 있는 인증서**)** 창의 열에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**입니다.

표 ***10:*** 신뢰할 수 있는 인증서 창의 열

필드 이름	사용 지침
Friendly Name(식별 이름**)**	인증서의 이름을 표시합니다.
Status(상태**)**	이 열에는 **Enabled(**활성화됨**)** 또는 **Disabled(**비활성화됨**)**가 표시됩니다. 인증서가 비활성화되면 Cisco ISE가 신뢰를 설정하는 데 인증서를 사용하지 않습니다.
Trusted for(신뢰 대상**)**	인증서를 사용하는 다음 서비스를 하나 이상 표시합니다. • **Infrastructure(**인프라**)** • **Cisco Services(**시스코 서비스**)** • **Endpoints(**엔드포인트**)**

필드 이름	사용 지침
Issued To(발급 대상**)**	인증서 주체의 CN(Common Name)을 표시합니다.
Issued By(발급자**)**	인증서 발급자의 CN(Common Name)을 표시합니다.
Valid From(유효 기간 시작**)**	인증서가 발급된 날짜와 시간을 표시합니다. 이 값은 "Not Before" 인증서 속성이라고도 합니다.
Expiration Date(만료일**)**	인증서가 만료되는 날짜와 시간을 표시합니다. 이 값은 "Not After" 인증서 속성이라고도 합니다.
Expiration Status(만료 상태**)**	인증서 만료의 상태에 대한 정보를 제공합니다. 이 열에는 정보 메시지의 범주와 5개 아이콘이 표시됩니다. • 녹색: 만료일까지 남은 기간이 90일 이상입니다. • 파란색: 90일 이내에 만료됩니다. • 노란색: 60일 이내에 만료됩니다. • 주황색: 30일 이내에 만료됩니다. • 빨간색: 만료되었습니다.

관련 항목

신뢰할 수 있는 인증서 저장소, 73 페이지
신뢰할 수 있는 인증서 보기, 76 페이지
신뢰할 수 있는 인증서 저장소의 상태 변경, 77 페이지
신뢰할 수 있는 인증서 저장소에 인증서 추가, 77 페이지

신뢰할 수 있는 인증서 명명 제한

CTL의 신뢰할 수 있는 인증서는 이름 제한 확장명을 포함할 수 있습니다. 이 확장명은 인증서 체인 내 후속 인증서의 모든 주체 이름 및 대체 주체 이름 필드 값에 대한 네임스페이스를 정의합니다. Cisco ISE는 루트 인증서에 지정된 제한을 확인하지 않습니다.

Cisco ISE에서 지원되는 이름 제한은 다음과 같습니다.

- 디렉토리 이름

  Subject(주체) 또는 Subject Alternative Name(대체 주체 이름) 필드에서 디렉토리 이름 접두사를 디렉토리 이름 제한으로 사용해야 합니다. 예를 들면 다음과 같습니다.

  - 올바른 주체 접두사:

    CA 인증서 이름 제한: Permitted: O=Cisco

    클라이언트 인증서 주체: O=Cisco,CN=Salomon

- 잘못된 주체 접두사:

  CA 인증서 이름 제한: Permitted: O=Cisco

  클라이언트 인증서 주체: CN=Salomon,O=Cisco

- DNS
- 이메일
- URI(URI 제한은 http://, https://, ftp:// 또는 ldap://와 같은 URI 접두사로 시작되어야 함)

Cisco ISE는 다음 이름 제약 조건을 지원하지 않습니다.

- IP 주소
- 기타 이름

신뢰할 수 있는 인증서에 지원되지 않는 제약 조건이 있고 확인 중인 인증서에 적절한 필드가 없는 경우 Cisco ISE는 지원되지 않는 제약 조건을 확인할 수 없으므로 인증서를 거부합니다.

신뢰할 수 있는 인증서 내의 이름 제한 정의 예제는 다음과 같습니다.

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.abcde.at
                  email:.abcde.be
                  email:.abcde.bg
                  email:.abcde.by
                  DNS:.dir
                  DirName: DC = dir, DC = emea
                  DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
                  DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
                  DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
                  DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100
                  URI:.dir
                  IP:172.23.0.171/255.255.255.255
                Excluded:
                  DNS:.dir
                  URI:.dir
```

위의 정의와 일치하는 허용되는 클라이언트 인증서 주체는 다음과 같습니다.

```
           Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

신뢰할 수 있는 인증서 보기

Trusted Certificates(신뢰할 수 있는 인증서**)** 창에는 Cisco ISE에서 사용 가능한 신뢰할 수 있는 인증서가 모두 나열됩니다. 신뢰할 수 있는 인증서를 보려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** 모든 인증서를 보려면 메뉴 아이콘(☰)을 클릭합니다. 그런 다음**Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다. Trusted Certificates(신뢰할 수 있는 인증서) 창이 표시되고 신뢰할 수 있는 인증서가 모두 나열됩니다.

단계 **2** 신뢰할 수 있는 인증서의 확인란을 선택하고 **Edit(**편집**)**, **View(**보기**)**, **Export(**내보내기**)** 또는 **Delete(**삭제**)**를 클릭하여 필요한 작업을 수행합니다.

신뢰할 수 있는 인증서 저장소의 상태 변경

Cisco ISE가 신뢰를 설정하는 데 인증서를 사용할 수 있도록 인증서의 상태를 활성화해야 합니다. 인증서는 신뢰할 수 있는 인증서 저장소로 가져올 때 자동으로 활성화됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **3** 활성화하거나 비활성화할 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** **Status(**상태**)** 드롭다운 목록에서 상태를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

신뢰할 수 있는 인증서 저장소에 인증서 추가

신뢰할 수 있는 인증서 저장소 창에서 Cisco ISE에 CA 인증서를 추가할 수 있습니다.

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- 브라우저를 실행 중인 컴퓨터의 파일 시스템에 추가하고자 하는 인증서가 있어야 합니다. 인증서는 PEM 또는 DER 형식이어야 합니다.
- 관리자 또는 EAP 인증용으로 인증서를 사용하려는 경우 인증서에 기본 제한을 정의하고 CA 플래그를 true로 설정합니다.

신뢰할 수 있는 인증서 편집

신뢰할 수 있는 인증서 저장소에 추가한 인증서는 **Edit(**편집**)** 옵션을 사용하여 추가로 편집할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** 선택Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2** 편집할 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** (선택 사항) **Friendly Name(**식별 이름**)** 필드에 인증서의 이름을 입력합니다. 식별 이름을 지정하지 않으면 기본 이름이 다음 형식으로 생성됩니다.

common-name#issuer#nnnnn

단계 **4** **Trusted For(**신뢰 대상**)** 영역에서 필요한 확인란을 선택하여 인증서 사용을 정의합니다.

단계 **5** (선택 사항) **Description(**설명**)** 필드에 인증서 설명을 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

신뢰할 수 있는 인증서 설정

다음 표에서는 신뢰할 수 있는 인증서의 **Edit(**편집**)** 창에 있는 필드에 대해 설명합니다. 이 창에서 CA 인증서 속성을 편집합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**입니다. 편집할 신뢰할 수 있는 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

표 ***11:*** 신뢰할 수 있는 인증서 편집 설정

필드 이름	사용 지침
인증서 발급자	
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다. 선택적 필드로, 식별 이름을 입력하지 않으면 기본 이름이 다음 형식으로 생성됩니다. *common-name # issuer # nnnnn*
Status(상태**)**	드롭다운 목록에서 **Enabled(**활성화됨**)** 또는 **Disabled(**비활성화됨**)**를 선택합니다. 인증서가 비활성화되면 Cisco ISE가 신뢰를 설정하는 데 인증서를 사용하지 않습니다.
Description(설명**)**	(선택 사항) 설명을 입력합니다.
사용	
Trust for authentication within ISE(ISE 내의 인증 신뢰**)**	이 인증서가 다른 Cisco ISE 노드 또는 LDAP 서버의 서버 인증서를 확인하도록 하려면 이 확인란을 선택합니다.

필드 이름	사용 지침
Trust for client authentication and Syslog(클라이언트 인증 및 시스템 로그 신뢰**)**	(Trust for authentication within **ISE**(ISE 내의 인증 신뢰) 확인란을 선택하는 경우에만 해당함) 다음 용도로 이 인증서를 사용하려는 경우 확인란을 선택합니다. • EAP 프로토콜을 사용하여 Cisco ISE에 연결하는 엔드포인트 인증 • 시스템 로그 서버 신뢰
Trust for authentication of Cisco Services(Cisco 서비스의 인증 신뢰**)**	피드 서비스와 같은 외부 Cisco 서비스를 신뢰하는 데 이 인증서를 사용하려는 경우 이 확인란을 선택합니다.
Certificate Status Validation(인증서 상태 검증**)**	Cisco ISE는 특정 CA가 발급한 클라이언트 또는 서버 인증서의 취소 상태를 확인하는 두 가지 방법을 지원합니다. 첫 번째 방법은 OCSP(Online Certificate Status Protocol)를 사용하여 인증서를 검증하는 것입니다. 이 경우 CA가 유지 관리하는 OCSP 서비스에 요청을 하게 됩니다. 두 번째 방법은 CA에서 Cisco ISE로 다운로드할 수 있는 CRL과 대조하여 인증서를 검증하는 것입니다. 이 두 방법은 모두 활성화할 수 있으며 이 경우 OCSP가 먼저 사용됩니다. 상태를 확인할 수 없는 경우에만 CRL이 사용됩니다.
Validate Against OCSP Service(OCSP 서비스와 대조하여 검증**)**	OCSP 서비스와 대조하여 인증서를 검증하려면 확인란을 선택합니다. 먼저 OCSP 서비스를 생성해야 이 확인란을 선택할 수 있습니다.
Reject the request if OCSP returns UNKNOWN status(OCSP에서 **UNKNOWN** 상태를 반환하는 경우 요청 거부**)**	OCSP 서비스에서 인증서 상태를 확인할 수 없는 경우 요청을 거부하려면 확인란을 선택합니다. 이 확인란을 선택하면 OCSP 서비스에서 알 수 없는 상태 값을 반환하는 경우 Cisco ISE가 현재 평가 중인 클라이언트 또는 서버 인증서를 거부합니다.
Reject the request if OCSP Responder is unreachable(OCSP 응답자에 연결할 수 없는 경우 요청 거부**)**	OCSP 응답자에 연결할 수 없는 경우 Cisco ISE가 요청을 거부하도록 하려면 이 확인란을 선택합니다.
Download CRL(CRL 다운로드**)**	Cisco ISE가 CRL을 다운로드하도록 하려면 확인란을 선택합니다.

필드 이름	사용 지침
CRL Distribution URL(CRL 배포 **URL)**	CA에서 CRL를 다운로드할 URL을 입력합니다. 인증 기관 인증서에 URL이 지정되어 있으면 이 필드는 자동으로 채워집니다. URL은 " http", "https" 또는 "ldap"로 시작해야 합니다.
Retrieve CRL(CRL 검색**)**	CRL은 자동으로 다운로드할 수도 있고 정기적으로 다운로드할 수도 있습니다. 이 필드에서 다운로드 간의 시간 간격을 구성합니다.
If download failed, wait(다운로드 실패 시 대기**)**	Cisco ISE가 다시 CRL 다운로드를 시도할 때까지 대기할 시간 간격을 구성합니다.
Bypass CRL Verification if CRL is not Received(CRL이 수신되지 않으면 **CRL** 확인 바이패스**)**	CRL이 수신되기 전에 클라이언트 요청을 수락하려면 이 확인란을 선택합니다. 이 확인란의 선택을 취소하면 선택한 CA가 서명을 한 인증서를 사용하는 모든 클라이언트 요청은 Cisco ISE가 CRL 파일을 받을 때까지 거부됩니다.
Ignore that CRL is not yet valid or expired(CRL 이 아직 유효하지 않거나 만료된 경우 시작일/만료 날짜 무시**)**	Cisco ISE가 시작일과 만료 날짜를 무시하고 아직 활성화되지 않았거나 만료된 CRL을 계속 사용하도록 하고, CRL의 내용에 따라 EAP-TLS 인증을 허용하거나 거부하도록 하려면 이 확인란을 선택합니다. Cisco ISE가 CRL 파일에서 Effective Date(유효 날짜) 필드의 시작일과 Next Update(다음 업데이트) 필드의 만료 날짜를 확인하도록 하려면 이 확인란의 선택을 취소합니다. CRL이 아직 활성화되지 않았거나 만료된 경우에는 이 CA가 서명을 한 인증서를 사용하는 모든 인증은 거부됩니다.

관련 항목

신뢰할 수 있는 인증서 저장소, 73 페이지
신뢰할 수 있는 인증서 편집, 77 페이지

신뢰할 수 있는 인증서 삭제

더 이상 필요하지 않은 신뢰할 수 있는 인증서는 삭제할 수 있습니다. 그러나 Cisco ISE 내부 CA 인증서를 삭제해서는 안 됩니다. Cisco ISE 내부 CA 인증서는 전체 구축에 대해 Cisco ISE 루트 인증서 체인을 교체할 때만 삭제할 수 있습니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2** 삭제할 인증서 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

경고 메시지가 표시됩니다. Cisco ISE 내부 CA 인증서를 삭제하려면 다음 옵션 중 하나를 클릭합니다.

- **Delete(**삭제**)**: Cisco ISE 내부 CA 인증서를 삭제합니다. 이 경우 Cisco ISE 내부 CA가 서명한 모든 엔드포인트 인증서는 무효화되며 엔드포인트가 네트워크에 가입할 수 없게 됩니다. 엔드포인트가 네트워크에 다시 가입할 수 있게 하려면 신뢰할 수 있는 인증서 저장소에 동일한 Cisco ISE 내부 CA 인증서를 가져옵니다.
- **Delete & Revoke(**삭제 및 취소**)**: Cisco ISE 내부 CA 인증서를 삭제 및 취소합니다. 이 경우 Cisco ISE 내부 CA가 서명한 모든 엔드포인트 인증서는 무효화되며 엔드포인트가 네트워크에 연결할 수 없게 됩니다. 이 작업은 취소할 수 없으며, 전체 구축에 대해 Cisco ISE 루트 인증서 체인을 교체해야 합니다.

단계 **3** **Yes(**예**)**를 클릭하여 인증서를 삭제합니다.

신뢰할 수 있는 인증서 저장소에서 인증서 내보내기

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

참고 내부 CA에서 인증서를 내보내는 경우 해당 내보내기를 사용하여 백업에서 복원하려는 경우 CLI 명령 `application configure ise`를 사용해야 합니다. Cisco ISE CA 인증서 및 키 내보내기, 118 페이지의 내용을 참조하십시오.

단계 **1** 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2**

단계 **3** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다. 인증서는 한 번에 하나씩만 내보낼 수 있습니다.

단계 **4** 선택한 인증서가 PEM 형식으로 클라이언트 브라우저를 실행중인 파일 시스템에 다운로드됩니다.

신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기

루트 CA 및 중간 CA 인증서를 가져오는 동안 신뢰할 수 있는 CA 인증서를 사용할 서비스를 지정할 수 있습니다.

시작하기 전에

인증서 서명 요청에 서명하고 디지털 서명 CA 인증서를 반환한 CA의 루트 인증서와 기타 중간 인증서가 있어야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2**

단계 **3** **Import(**가져오기**)**를 클릭합니다.

단계 **4** 표시되는 **Import a new Certificate into the Certificate Store(**인증서 저장소에 새 인증서 가져오기**)** 창에서 **Choose File(**파일 선택**)**을 클릭하여 CA에서 서명하고 반환한 루트 CA 인증서를 선택합니다.

단계 **5** 식별 이름을 입력합니다.

식별 이름을 입력하지 않으면 Cisco ISE는 *common-name#issuer#nnnnn* 형식의 이름을 이 필드에 자동으로 채웁니다. 여기서 *nnnnn*은 고유한 번호입니다. 추후 인증서를 편집하여 식별 이름을 변경할 수 있습니다.

단계 **6** 이 신뢰할 수 있는 인증서를 사용할 서비스 옆의 확인란을 선택합니다.

단계 **7** (선택 사항) **Description(**설명**)** 필드에 인증서 설명을 입력합니다.

단계 **8** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

해당하는 경우 신뢰할 수 있는 인증서 저장소로 중간 CA 인증서를 가져옵니다.

신뢰할 수 있는 인증서 가져오기 설정

다음 표에서는 Cisco ISE에 CA 인증서를 추가하는 데 사용할 수 있는 Trusted Certificate Import(신뢰할 수 있는 인증서 가져오기) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** > **Import(**가져오기**)** 입니다.

표 ***12:*** 신뢰할 수 있는 인증서 가져오기 설정

필드 이름	설명
Certificate File(인증서 파일**)**	브라우저를 실행 중인 컴퓨터에서 인증서 파일을 선택하려면 **Browse(**찾아보기**)**를 클릭합니다.
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다. 이름을 지정하지 않으면 Cisco ISE에서 <common name>#<issuer>#<nnnnn> 형식으로 이름을 자동 생성합니다. 여기서 <nnnnn>은 고유한 5자리 숫자입니다.
Trust for authentication within ISE(ISE 내의 인증 신뢰**)**	다른 ISE 노드 또는 LDAP 서버의 서버 인증서를 확인하는 데 이 인증서를 사용하려는 경우 확인란을 선택합니다.

필드 이름	설명
Trust for client authentication and Syslog(클라이언트 인증 및 시스템 로그 신뢰**)**	(Trust for authentication within ISE(ISE 내의 인증 신뢰) 확인란을 선택하는 경우에만 해당함) 다음 용도로 이 인증서를 사용하려는 경우 확인란을 선택합니다. • EAP 프로토콜을 사용하여 ISE에 연결하는 엔드포인트 인증 • 시스템 로그 서버 신뢰
Trust for authentication of Cisco Services(Cisco 서비스의 인증 신뢰**)**	피드 서비스와 같은 외부 Cisco 서비스를 신뢰하는 데 이 인증서를 사용하려는 경우 이 확인란을 선택합니다.
Validate Certificate Extensions(인증서 확장명 검증**)**	(Trust for client authentication(클라이언트 인증 신뢰) 및 Enable Validation of Certificate Extensions(인증서 확장명 검증 활성화) 옵션을 둘 다 선택하는 경우에만 해당함) "keyUsage" 확장명이 있고 "keyCertSign" 비트가 설정되어 있으며 CA 플래그가 true로 설정된 기본 제한 확장명이 있는지 확인합니다.
Description(설명**)**	필요에 따라 설명을 입력합니다.

관련 항목

신뢰할 수 있는 인증서 저장소, 73 페이지
인증서 체인 가져오기, 83 페이지
신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 81 페이지

인증서 체인 가져오기

인증서 저장소에서 수신한 인증서 체인이 들어 있는 단일 파일에서 여러 인증서를 가져올 수 있습니다. 파일의 모든 인증서는 PEM 형식이어야 하며, 인증서는 다음 순서로 정렬되어야 합니다.

- 파일의 마지막 인증서는 CA에서 발급된 클라이언트 또는 서버 인증서여야 합니다.
- 이전의 모든 인증서는 루트 CA 인증서이자 발급된 인증서의 서명 체인에 있는 중간 CA 인증서여야 합니다.

2단계 프로세스로 인증서 체인 가져오기:

1. Cisco ISE 관리 포털의 신뢰할 수 있는 인증서 저장소로 인증서 체인 파일을 가져옵니다. 이 작업은 마지막 인증서를 제외한 파일의 모든 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다.
2. CA 서명 인증서 바인딩 작업을 사용하여 인증서 체인 파일을 가져옵니다. 이 작업은 파일에서 마지막 인증서를 로컬 인증서로 가져옵니다.

Cisco ISE 노드 간 통신용으로 신뢰할 수 있는 인증서 설치

구축을 설정할 때는 보조 노드를 등록하기 전에 보조 노드의 관리 인증서를 검증하는 데 사용되는 적절한 CA 인증서를 PAN의 CTL에 입력해야 합니다. PAN의 CTL에 인증서를 입력하는 절차는 시나리오마다 다릅니다.

- 보조 노드가 CA 서명 인증서를 사용하여 Cisco ISE 관리 포털과 통신하는 경우 보조 노드의 CA 서명 인증서, 관련 중간 인증서(있는 경우) 및 보조 노드 인증서에 서명을 한 CA의 루트 CA 인증서를 PAN의 CTL로 가져와야 합니다.
- 보조 노드가 SSC(자가서명 인증서)를 사용하여 Cisco ISE 관리 포털과 통신하는 경우에는 보조 노드의 해당 인증서를 PAN의 CTL로 가져올 수 있습니다.

참고

- 등록된 보조 노드에서 관리 인증서를 변경하는 경우에는 보조 노드 관리 인증서를 검증하는 데 사용할 수 있는 적절한 CA 인증서를 얻은 다음 PAN의 CTL로 가져와야 합니다.
- 구축의 클라이언트와 PSN 간 통신을 보호하기 위해 SSC(자가서명 인증서)를 사용하는 경우 BYOD 사용자가 한 위치에서 다른 위치로 이동하면 EAP-TLS 사용자 인증이 실패합니다. 몇 개의 PSN 간에 서비스를 받아야 하는 인증 요청의 경우에는 외부에서 서명한 CA 인증서로 클라이언트와 PSN 간의 통신을 보호하거나 외부 CA가 서명한 와일드카드 인증서를 사용해야 합니다.

외부 CA가 발급한 인증서에 기본 제한이 정의되어 있으며 CA 플래그가 true로 설정되어 있는지 확인합니다. 노드 간 통신을 위해 CA 서명 인증서를 설치하려면 다음 단계를 수행합니다. 이러한 작업에 대한 자세한 내용은 *Cisco ISE* 관리자 가이드의 "기본 설정" 장을 참조하십시오.

단계 **1** CSR(Certificate Signing Request)을 생성하고 CSR을 인증 기관에 제출합니다.

단계 **2** 신뢰할 수 있는 인증서 저장소로 루트 인증서를 가져옵니다.

단계 **3** CSR에 CA 서명 인증서를 바인딩합니다.

Cisco ISE의 기본 신뢰할 수 있는 인증서

Cisco ISE의 신뢰할 수 있는 인증서 저장소(**Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**)에는 기본적으로 사용 가능한 일부 인증서가 포함되어 있습니다. 이러한 인증서는 보안 요구 사항을 충족하기 위해 저장소로 자동으로 가져옵니다. 그러나 이 모두를 사용해야 하는 것은 아닙니다. 아래 표에서 달리 언급되지 않는 한, 이미 사용 가능한 인증서 대신 원하는 인증서를 사용할 수 있습니다.

표 *13:*

신뢰할 수 있는 인증서 이름	**Serial Number**(일련 번호)	인증서의 목적	인증서가 포함된 **Cisco ISE** 릴리스
Baltimore CyberTrust Root CA	02 00 00 B9	이 인증서는 일부 지역에서 cisco.com이 사용하는 CA 체인의 루트 CA 인증서로 사용할 수 있습니다. 인증서는 https://s3.amazonaws.com에서 호스팅될 때 ISE 2.4 Posture / CP 업데이트 XML 파일에도 사용되었습니다.	릴리스 2.4 이상.
DST Root CA X3 Certificate Authority	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	이 인증서는 cisco.com에서 사용하는 CA 체인의 루트 CA 인증서 역할을 할 수 있습니다.	릴리스 2.4 이상.
Thawte Primary Root CA	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	이 인증서는 루트 CA 역할을 할 수 있습니다. cisco.com 및 perfigo.com에서 사용하는 CA 체인용 인증서입니다.	릴리스 2.4 이상.
VeriSign Class 3 Public Primary Certification Authority	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	이 인증서는 VeriSign Class 3 Secure Server CA-G3의 루트 CA 인증서 역할을 합니다. Cisco ISE에서 프로파일러 피드 서비스를 구성할 때 이 인증서를 사용해야 합니다.	릴리스 2.4 이상.
VeriSign Class 3 Secure Server CA - G3	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	이는 2020년 2월 7일에 만료되는 중간 CA 인증서입니다. 이 인증서는 갱신할 필요가 없습니다. 아래 작업에 따라 인증서를 제거 할 수 있습니다.	릴리스 2.4 이상.

신뢰할 수 있는 인증서 이름	**Serial Number**(일련 번호)	인증서의 목적	인증서가 포함된 **Cisco ISE** 릴리스
Cisco CA Manufacturing	6A 69 67 B3 00 00 00 00 00 03	이 인증서는 Cisco ISE에 연결하는 특정 Cisco 디바이스에서 사용할 수 있습니다. 이 인증서는 기본적으로 비활성화되어 있습니다.	릴리스 2.4 및 2.6.
Cisco Manufacturing CA SHA2	02	이 인증서는 CA 체인에서 관리자 인증, 엔드포인트 인증 및 구축 인프라 흐름에 사용할 수 있습니다.	릴리스 2.4 이상.
Cisco Root CA 2048	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	이 인증서는 Cisco ISE에 연결하는 특정 Cisco 디바이스에서 사용할 수 있습니다. 이 인증서는 기본적으로 비활성화되어 있습니다.	릴리스 2.4 이상.
Cisco Root CA M2	01	이 인증서는 CA 체인에서 관리자 인증, 엔드포인트 인증 및 구축 인프라 흐름에 사용할 수 있습니다.	릴리스 2.4 이상.
DigiCert Root CA	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	Facebook으로 게스트 로그인을 사용하는 플로우에 이 인증서를 사용해야 합니다.	릴리스 2.4 이상.
DigiCert SHA2 High Assurance Server CA	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	Facebook으로 게스트 로그인을 사용하는 플로우에 이 인증서를 사용해야 합니다.	릴리스 2.4 이상.
HydrantID SSL ICA G2	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	Cisco 서비스에 대해 신뢰됩니다.	릴리스 2.4 및 2.6.
QuoVadis Root CA 2	05 09	프로파일러, 포스처 및 클라이언트 프로비저닝 플로우에서 이 인증서를 사용해야 합니다.	릴리스 2.4 이상.

신뢰할 수 있는 인증서 이름	**Serial Number(**일련 번호**)**	인증서의 목적	인증서가 포함된 **Cisco ISE** 릴리스
Cisco ECC Root CA	01	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6.
Cisco Licensing Root CA	01	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상
Cisco Root CA 2099	01 9A 33 58 78 CE 16 C1 C1	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상
Cisco Root CA M1	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상
Cisco RXC-R2	01	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상
DigiCert Global Root CA	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상
Cisco ECC Root CA 2099	03	이 인증서는 Cisco ISE에서 사용되는 Cisco Trust 루트 저장소 번들의 일부입니다.	릴리스 2.6 이상

Cisco ISE에서 신뢰할 수 있는 기본 인증서 제거

- Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.
- 필요한 경우 다시 가져올 수 있도록 삭제할 인증서를 내보내고 저장합니다.

  내보낼 인증서 확인란을 선택하고 위의 메뉴 모음에서 **Export(**내보내기**)**를 클릭합니다. 키 체인이 시스템에 다운로드됩니다.

- 인증서를 삭제합니다. 삭제할 인증서 확인란을 선택하고 위의 메뉴 모음에서 **Delete(**삭제**)**를 클릭합니다. CA 체인, 보안 시스템 로그 또는 보안 LDAP에서 인증서를 사용 중인 경우 해당 인증서를 삭제할 수 없습니다.
- CA 체인, 보안 시스템 로그 및 그 일부인 시스템 로그에서 인증서를 제거하기 위래 필요한 컨피그레이션을 변경합니다. 그런 다음 인증서를 삭제합니다.
- 인증서를 삭제한 후 관련 서비스(인증서의 목적 참조)가 정상적으로 작동하는지 확인합니다.

인증서 서명 요청

서명된 인증서를 발급하는 CA의 경우 인증서 서명 요청을 생성하고 CA에 제출해야 합니다.

생성한 인증서 서명 요청 목록은 **Certificate Signing Requests(**인증서 서명 요청**)** 창에서 확인할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다. CA에서 서명을 받으려면 인증서 서명 요청을 내보낸 다음, 인증서를 CA로 보내야 합니다. CA는 인증서에 서명하고 반환합니다.

Cisco ISE 관리 포털을 통해 중앙에서 인증서를 관리할 수 있습니다. 구축의 모든 노드에 사용할 인증서 서명 요청을 생성하고 내보낼 수 있습니다. 그런 다음 인증서 서명 요청을 CA에 제출하고, CA에서 CA 서명 인증서를 받고, CA에서 반환된 루트 및 중간 CA 인증서를 신뢰할 수 있는 인증서 저장소로 가져온 다음, CA 서명 인증서를 인증서 서명 요청에 바인딩해야 합니다.

인증서 서명 요청을 생성하고 인증 기관에 제출

CSR(Certificate Signing Request)을 생성하여 구축의 노드용으로 CA에서 서명한 인증서를 가져올 수 있습니다. 구축의 특정 노드 또는 구축의 모든 노드에 대해 CSR을 생성할 수 있습니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

단계 **2** **Generate Certificate Signing Requests(CSR)(**인증서 서명 요청 생성**)** 클릭하여 인증서 서명 요청을 생성합니다.

단계 **3** 인증서 서명 요청 생성에 대한 값 입력 표시된 창의 각 필드에 대한 자세한 내용은 인증서 서명 요청 설정을 참조하십시오.

단계 **4** 서명 요청 확인란을 선택하고 **Export(**내보내기**)**를 클릭하여 인증서 서명 요청을 다운로드합니다.

단계 **5** **"-----BEGIN CERTIFICATE REQUEST-----"**부터 **"-----END CERTIFICATE REQUEST-----"**까지의 모든 텍스트를 복사합니다."

단계 **6** CSR의 내용을 선택한 CA의 인증서 요청에 붙여 넣습니다.

단계 **7** 서명된 인증서를 다운로드합니다.

일부 CA의 경우 서명된 인증서를 이메일로 전송할 수 있습니다. 서명된 인증서는 zip 파일 형식이며 새로 발급된 인증서와 CA의 공개 서명 인증서가 들어 있습니다. 이러한 인증서를 Cisco ISE 신뢰할 수 있는 인증서 저장소에 추가

해야 합니다. 디지털 서명된 CA 인증서, 루트 CA 인증서 및 기타 중간 CA 인증서(해당하는 경우)가 클라이언트 브라우저를 실행 중인 로컬 시스템에 다운로드됩니다.

인증서 서명 요청에 대한 CA 서명 인증서 바인딩

CA가 디지털 서명된 인증서를 반환하고 나면 해당 인증서를 CSR(Certificate Signing Request)에 바인딩해야 합니다. 관리 포털에서 구축의 모든 노드에 대해 바인딩 작업을 수행할 수 있습니다.

시작하기 전에

- 디지털 서명된 인증서와 CA가 반환한 관련 루트 중간 CA 인증서가 있어야 합니다.
- 관련 루트 및 중간 CA 인증서를 신뢰할 수 있는 인증서 저장소(**Menu(**메뉴**)** 아이콨(☰) 클릭 후 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** 선택)로 가져옵니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

CA 서명 인증서에 바인딩해야 하는 인증서 서명 요청 옆의 확인란을 선택합니다.

단계 **2** **Bind Certificate(**인증서 바인딩**)**를 클릭합니다.

단계 **3** **Bind CA Signed Certificate(CA** 서명 인증서 바인딩**)** 창에서 **Choose File(**파일 선택**)**을 클릭하여 CA 서명 인증서를 선택합니다.

단계 **4** **Friendly Name(**식별 이름**)** 필드에 값을 입력합니다.

단계 **5** Cisco ISE가 인증서 확장명을 검증하도록 하려면 **Validation of Certificate Extensions(**인증서 확장명 검증**)** 확인란을 선택합니다.

Validation of Certificate Extensions(인증서 확장명 검증**)** 옵션을 활성화하는 경우 가져오는 인증서에 CA 플래그가 true로 설정된 기본 제한 확장명이 포함되어 있으면 키 사용 확장이 있는지 확인하고, keyEncipherment 비트나 keyAgreement 중 하나 또는 두 비트가 모두 설정되어 있는지도 확인합니다.

참고 Cisco ISE는 EAP-TLS 클라이언트 인증서가 있어야 디지털 서명 키 사용 확장명을 보유할 수 있습니다.

단계 **6** (선택 사항) **Usage(**사용**)** 영역에서 이 인증서를 사용할 서비스를 확인합니다.

인증서 서명 요청을 생성하는 중에 **Usage(**사용**)** 옵션을 활성화한 경우 이 정보는 자동으로 채워집니다. 나중에 인증서를 편집하여 사용을 지정할 수도 있습니다.

기본 PAN에서 **Admin(**관리자**)** 사용 인증서를 변경하면 다른 모든 노드에서 서비스가 재시작됩니다. 시스템은 기본 PAN이 재시작한 뒤에 노드를 한 번에 한 개씩 재시작합니다.

단계 **7** CA 서명 인증서에 인증서 서명 요청을 바인딩하려면 **Submit(**제출**)**을 클릭합니다.

이 인증서가 Cisco ISE 노드 간 통신 사용에 대해 표시되어 있는 경우 Cisco ISE 노드의 애플리케이션 서버가 다시 시작됩니다.

구축에서 다른 노드에 대해 이 프로세스를 반복하여 인증서 서명 요청을 CA 서명 인증서와 바인딩할 수 있습니다.

다음에 수행할 작업

신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 81 페이지

인증서 서명 요청 내보내기

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **3** 인증서 서명 요청이 로컬 파일 시스템에 다운로드됩니다.

인증서 서명 요청 설정

Cisco ISE에서는 관리 포털에서 단일 요청으로 구축의 모든 노드에 대한 인증서 서명 요청을 생성할 수 있습니다. 또한 필요에 따라 구축의 단일 노드 또는 여러 모든 노드에 대한 인증서 서명 요청도 생성할 수 있습니다. 여러 노드에 대한 인증서 서명 요청을 생성하도록 선택하는 경우 ISE는 인증서 주체의 CN= 필드에서 특정 노드의 FQDN(Fully Qualified Domain Name)을 자동으로 대체합니다. 인증서의 SAN(Subject Alternative Name) 필드에 항목을 포함하도록 선택하는 경우 다른 SAN 속성과 함께 ISE 노드의 FQDN을 입력해야 합니다. 구축의 모든 노드에 대해 인증서 서명 요청을 생성하도록 선택하는 경우 Allow Wildcard Certificates(와일드카드 인증서 허용) 확인란을 선택하고 SAN 필드(DNS 이름)에 와일드카드 FQDN 표기법(예: *.amer.example.com)을 입력합니다. EAP 인증에 인증서를 사용하려는 경우 CN= 필드에 와일드카드 값을 입력하지 마십시오.

와일드카드 인증서를 사용하는 경우에는 각 Cisco ISE 노드에 대해 고유한 인증서를 더 이상 생성하지 않아도 됩니다. 또한 인증서 경고가 표시되지 않도록 하기 위해 여러 FQDN 값을 SAN 필드에 입력할 필요도 없습니다. SAN 필드에 별표(*)를 사용하면 구축의 여러 모든 노드에 걸쳐 단일 인증서를 공유할 수 있으며, 인증서 이름 불일치 경고가 표시되지 않습니다. 그러나 와일드카드 인증서를 사용하는 방식은 각 Cisco ISE 노드용으로 고유한 서버 인증서를 할당하는 방식보다 보안성이 낮은 것으로 간주됩니다.

다음 표에서는 인증서 서명 요청 창의 필드에 대해 설명합니다. 이 창은 CA(Certificate Authority)에 의해 서명될 수 있는 인증서 서명 요청을 생성하는 데 사용할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Signing Request(**인증서 서명 요청**)** 입니다.

표 ***14:*** 인증서 서명 요청 설정

필드	사용 지침
Certificate(s) will be used for(인증서 사용 대상**)**	

필드	사용 지침
	인증서를 사용할 서비스를 선택합니다. **Cisco ISE ID** 인증서 • **Multi-Use(**다용도**)**: 여러 서비스(관리, EAP-TLS 인증, pxGrid 및 포털)에 사용됩니다. 다용도 인증서는 클라이언트 및 서버 키 사용을 모두 지원합니다. 서명 CA의 인증서 템플릿은 컴퓨터 또는 머신 인증서 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 및 TLS 웹 클라이언트 인증(1.3.6.1.5.5.7.3.2) • **Admin(**관리**)**: 구축의 ISE 노드 간 통신 및 관리 포털과의 통신을 보호하기 위한 서버 인증에 사용됩니다. 서명 CA의 인증서 템플릿은 웹 서버 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) • **EAP Authentication(EAP** 인증**)**: 서버 인증에 사용됩니다. 서명 CA의 인증서 템플릿은 컴퓨터 또는 머신 인증서 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 참고 EAP-TLS 클라이언트 인증서에는 디지털 서명 키를 사용해야 합니다. • **RADIUS DTLS**: RADIUS DTLS 서버 인증에 사용됩니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) • **ISE Messaging Service(ISE** 메시징 서비스**)**: Syslog Over Cisco ISE Messaging(Cisco ISE 메시징을 통한 시스템 로그) 기능에서 사용되며, 구축 당시 기본으로 내장된 UDP 시스템 로그 수집 대상(LogCollector 및 LogCollector2)에 대해 MnT WAN 존속성을 활성화합니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) • **Portal(**포털**)**: 모든 ISE 웹 포털과의 통신을 보호하기 위한 서버 인증에 사

필드	사용 지침
	용됩니다. 서명 CA의 인증서 템플릿은 컴퓨터 또는 머신 인증서 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) • **pxGrid**: pxGrid 클라이언트와 서버 간의 통신을 보호하기 위해 클라이언트 및 서버 인증에 사용됩니다. 서명 CA의 인증서 템플릿은 컴퓨터 또는 머신 인증서 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 및 TLS 웹 클라이언트 인증(1.3.6.1.5.5.7.3.2) • **SAML**: SAML IdP(Identity Provider)와의 통신을 보호하는 데 사용되는 서버 인증서입니다. SAML에 사용하도록 지정된 인증서는 관리, EAP, 인증 등의 기타 서비스에는 사용할 수 없습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 참고 Extended Key Usage(확장 키 사용) 속성의 모든 용도 개체 식별자에 대해 2.5.29.37.0 값을 포함하는 인증서를 사용하지 않는 것이 좋습니다. Extended Key Usage(확장 키 사용) 속성에서 모든 용도 개체 식별자에 대해 2.5.29.37.0 값을 포함하는 인증서를 사용하는 경우 인증서가 유효하지 않은 것으로 간주되고, 다음 오류 메시지가 표시됩니다. `source=local ; type=fatal ; message="unsupported certificate"` **Cisco ISE** 인증 기관 인증서

필드	사용 지침

	• **ISE Root CA(ISE** 루트 **CA)**: (내부 CA 서비스에만 해당함) 기본 PAN의 루트 CA 및 PSN의 하위 CA를 비롯하여 전체 내부 CA 인증서 체인을 재생성하는 데 사용됩니다.
	• **ISE Intermediate CA(ISE** 중간 **CA)**: (ISE가 외부 PKI의 중간 CA로 작동하는 경우 내부 CA 서비스에만 해당함) 기본 PAN의 중간 CA 인증서 및 PSN의 하위 CA 인증서를 생성하는 데 사용됩니다. 서명 CA의 인증서 템플릿은 하위 인증 기관이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다.
	  • 기본 제한: 위험, 인증 기관 여부
	  • 키 사용: 인증서 서명, 디지털 서명
	  • 확장 키 사용: OCSP 서명(1.3.6.1.5.5.7.3.9)
	• **Renew ISE OCSP Responder Certificates(ISE OCSP** 응답자 인증서 갱신**)**: (내부 CA 서비스에만 해당함) 전체 구축에 대한 ISE OCSP 응답자 인증서를 갱신하는 데 사용되며, 인증서 서명 요청과는 다릅니다. 보안을 위해 ISE OCSP 응답자 인증서는 6개월에 한 번씩 갱신하는 것이 좋습니다.

Allow Wildcard Certificates(와일드카드 인증서 허용**)**	인증서의 SAN 필드에서 CN 및/또는 DNS 이름에 와일드카드 문자(*)를 사용하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 구축의 모든 노드가 자동으로 선택됩니다. 맨 왼쪽 레이블 위치에 별표(*) 와일드카드 문자를 사용해야 합니다. 와일드카드 인증서를 사용하는 경우에는 보안 향상을 위해 도메인 공간을 분할하는 것이 좋습니다. 예를 들어 *.example.com 대신 *.amer.example.com으로 도메인을 분할할 수 있습니다. 도메인을 분할하지 않으면 심각한 보안 문제가 발생할 수 있습니다.
Generate CSRs for these Nodes(이 노드에 대해 **CSR** 생성**)**	인증서를 생성할 노드 옆에 있는 확인란을 선택합니다. 구축의 선택 노드에 대해 CSR을 생성하려면 Allow Wildcard Certificates(와일드카드 인증서 허용) 옵션의 선택을 취소해야 합니다.
Common Name(CN)(공용 이름**)**	기본적으로 공용 이름은 인증서 서명 요청을 생성하는 ISE 노드의 FQDN입니다. $FQDN$은 ISE 노드의 FQDN을 나타냅니다. 구축의 여러 노드에 대해 인증서 서명 요청을 생성하는 경우 인증서 서명 요청의 Common Name(공통 이름) 필드가 해당 ISE 노드의 FQDNdmfh 대체됩니다.
Organizational Unit(OU)(조직 단위**)**	조직 단위의 이름입니다. Engineering 등을 예로 들 수 있습니다.
Organization(O)(조직**)**	조직의 이름입니다. Cisco 등을 예로 들 수 있습니다.
City(L)(구/군/시**)**	(약어로 표기하지 않음) 구/군/시의 이름입니다. San Jose 등을 예로 들 수 있습니다.

필드	사용 지침
State(ST)(시/도**)**	(약어로 표기하지 않음) 시/도의 이름입니다. California 등을 예로 들 수 있습니다.
Country(C)(국가**)**	국가의 이름입니다. 2자리 ISO 국가 코드를 입력해야 합니다. US 등을 예로 들 수 있습니다.
SAN(Subject Alternative Name)	IP 주소, DNS 이름, URI(Uniform Resource Identifier) 또는 인증서와 연결된 디렉토리 이름 • **DNS** 이름: DNS 이름을 선택하는 경우 ISE 노드의 정규화된 도메인 이름을 입력합니다. Allow Wildcard Certificates(와일드카드 인증서 허용) 옵션을 활성화한 경우 와일드카드 표기법(별표 및 도메인 이름 앞의 마침표)을 지정합니다. 예: *.amer.example.com • **IP** 주소: 인증서와 연결할 ISE 노드의 IP 주소입니다. • **Uniform Resource Identifier**: 인증서와 연결할 URI입니다. • 디렉토리 이름: RFC 2253에 따라 정의된 DN(Distinguished Name)의 문자열 표현입니다. 쉼표(,)를 사용하여 DN을 구분합니다. "dnQualifier" RDN의 경우 쉼표를 이스케이프하고 구분 기호로 백슬래시와 쉼표, 즉 "\,"를 사용합니다. 예: CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL
Key Type(키 유형**)**	공개 키를 생성하는 데 사용할 알고리즘을 RSA 또는 ECDSA로 지정합니다.
Key Length(키 길이**)**	공개 키의 비트 크기를 지정합니다. RSA에는 다음 옵션을 사용할 수 있습니다. • 512 • 1024 • 2048 • 4096 ECDSA에는 다음 옵션을 사용할 수 있습니다. • 256 • 384 참고 RSA 및 ECDSA 공개 키는 동일한 보안 레벨에서 키 길이가 다를 수 있습니다. 공용 CA 서명 인증서를 가져오거나 하려면 2048 이상을 선택합니다.

필드	사용 지침
Digest to Sign With(서명에 사용할 다이제스트**)**	SHA-1 또는 SHA-256 해싱 알고리즘 중 하나를 선택합니다.
인증서 정책	인증서가 준수해야 하는 인증서 정책 OID 또는 OID 목록을 입력합니다. 쉼표나 공백을 사용하여 OID를 구분합니다.

관련 항목

인증서 서명 요청, 88 페이지
인증서 서명 요청을 생성하고 인증 기관에 제출, 88 페이지
인증서 서명 요청에 대한 CA 서명 인증서 바인딩, 89 페이지

포털 사용을 위한 인증서 설정

구축에서 웹 포털 요청을 처리할 수 있는 PSN이 여러 개 있는 경우 Cisco ISE에는 포털 통신에 사용할 인증서를 식별할 수 있는 고유 식별자가 필요합니다. 포털에서 사용하도록 지정된 인증서를 추가하거나 가져오는 경우 인증서 그룹 태그를 정의하고 이를 구축의 각 노드에 있는 해당 인증서와 연결해야 합니다. 이 인증서 그룹 태그를 해당 최종 사용자 포털(게스트, 스폰서 및 개인 디바이스 포털)에 연결해야 합니다. 이 인증서 그룹 태그는 Cisco ISE가 이러한 각 포털과 통신할 때 사용해야 하는 인증서를 식별하도록 도와주는 고유 식별자입니다. 포털마다 각 노드의 인증서를 하나씩만 지정할 수 있습니다.

참고 Cisco ISE는 TCP 포트 8443(또는 포털 사용을 위해 구성한 포트)에서 포털 인증서를 제공합니다.

단계 **1** 인증서 서명 요청을 생성하고 인증 기관에 제출, 88 페이지.

이미 정의한 인증서 그룹 태그를 선택하거나 포털용으로 새 태그를 생성해야 합니다. 예를 들어 mydevicesportal과 같은 태그를 생성할 수 있습니다.

단계 **2** 신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 81 페이지.

단계 **3** 인증서 서명 요청에 대한 CA 서명 인증서 바인딩, 89 페이지.

CA 서명 인증서에 기본 포털 인증서 그룹 태그 재할당

기본적으로 모든 Cisco ISE 포털은 셀프 서명 인증서를 사용합니다. 포털에 CA 서명 인증서를 사용하려는 경우 CA 서명 인증서에 기본 포털 인증서 그룹 태그를 할당할 수 있습니다. 기존의 CA 서명 인증서를 사용할 수도 있고, CSR을 생성하여 포털에서 사용할 새 CA 서명 인증서를 얻을 수도 있습니다. 인증서 간에 포털 그룹 태그를 재할당할 수 있습니다.

참고 기존 인증서를 편집할 때 해당 인증서에 연결되어 있는 포털 태그(게스트)를 이미 사용 중인 포털이 있으면 기본 포털 인증서 그룹 태그 또는 기타 포털 그룹 태그를 이 인증서에 재할당할 수 없습니다. 시스템에는 "게스트" 포털 태그를 사용하는 포털 목록이 나열됩니다.

다음 절차에서는 CA 서명 인증서에 기본 포털 인증서 그룹 태그를 재할당하는 방법을 설명합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다.

기본 포털 인증서 그룹 태그 옆의 i 아이콘을 마우스로 가리키면 해당 태그를 사용하는 포털 목록을 확인할 수 있습니다. 이 태그가 할당된 포털 인증서가 있는 구축 내 ISE 노드도 확인할 수 있습니다.

단계 **2** 포털에 사용할 CA 서명 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

포털에서 사용하고 있지 않은 CA 서명 인증서를 선택해야 합니다.

단계 **3** **Usage(**사용**)** 영역에서 **Portal(**포털**)** 확인란을 선택하고 기본 포털 인증서 그룹 태그를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

경고 메시지가 표시됩니다.

단계 **5** **Yes(**예**)**를 클릭하여 기본 포털 인증서 그룹 태그를 CA 서명 인증서에 재할당합니다.

노드 등록 전에 포털 인증서 태그 연결

구축의 모든 포털에 대해 "기본 포털 인증서 그룹" 태그를 사용하는 경우에는 새 ISE 노드를 등록하기 전에 관련 CA 서명 인증서를 가져오고 서비스로 "Portal(포털)"을 선택한 다음 "기본 포털 인증서 그룹" 태그를 이 인증서와 연결해야 합니다.

구축에 새 노드를 추가하면 기본 셀프 서명 인증서가 "기본 포털 인증서 그룹" 태그와 연결되며 이 태그를 사용하도록 포털이 구성됩니다.

새 노드를 등록한 후에는 인증서 그룹 태그 연결을 변경할 수 없습니다. 그러므로 구축에 노드를 등록하기 전에 다음을 수행해야 합니다.

단계 **1** 셀프 서명된 인증서를 생성하고 서비스로 "Portal(포털)"을 선택한 후 tempportaltag 등의 다른 인증서 그룹 태그를 할당합니다.

단계 **2** 새로 생성한 인증서 그룹 태그(tempportaltag)를 사용하도록 포털 컨피그레이션을 변경합니다.

단계 **3** 기본 셀프 서명 인증서를 편집하여 Portal(포털) 역할을 제거합니다.

이 옵션을 사용하는 경우 기본 셀프 서명 인증서와의 "기본 포털 인증서 그룹" 태그 연결이 제거됩니다.

단계 **4** 다음 중 하나를 수행합니다.

옵션	설명
Generate a CSR(CSR 생성)	CSR 생성 시: **1.** 이 인증서를 사용할 서비스로 "Portal(포털)"을 선택하고 "기본 포털 인증서 그룹" 태그를 연결합니다. **2.** CA에 CSR을 보내고 서명된 인증서를 가져옵니다. **3.** 인증서에 서명을 한 CA의 루트 및 기타 중간 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다. **4.** CA 서명 인증서를 CSR에 바인딩합니다.
Import the private key and the CA-signed certificate(개인 키 및 CA 서명 인증서 가져오기)	CA 서명 인증서를 가져올 때는 다음을 수행합니다. **1.** 이 인증서를 사용할 서비스로 "Portal(포털)"을 선택하고 "기본 포털 인증서 그룹" 태그를 연결합니다. **2.** 인증서에 서명을 한 CA의 루트 및 기타 중간 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다.
기존 CA 서명 인증서를 편집합니다.	기존 CA 서명 인증서를 편집할 때는 다음을 수행합니다. 이 인증서를 사용할 서비스로 "Portal(포털)"을 선택하고 "기본 포털 인증서 그룹" 태그를 연결합니다.

단계 **5** 구축에 ISE 노드를 등록합니다.
구축의 포털 컨피그레이션이 "기본 포털 인증서 그룹" 태그로 구성되고 포털이 새 노드에서 "기본 포털 인증서 그룹" 태그와 연결된 CA 서명 인증서를 사용하도록 구성됩니다.

사용자 및 엔드포인트 인증서 갱신

기본적으로 Cisco ISE는 인증서가 만료된 디바이스에서 발생하는 요청을 거부합니다. 그러나 이 기본 동작을 변경하여 그러한 요청을 처리하고 사용자에게 인증서를 갱신할지 묻는 메시지를 표시하도록 ISE를 구성할 수 있습니다.

사용자가 인증서를 갱신하도록 허용하는 경우 요청을 추가로 처리하기 전에 인증서가 갱신되었는지 확인하는 권한 부여 정책 규칙을 구성하는 것이 좋습니다. 인증서가 만료된 디바이스에서 오는 요청을 처리하면 잠재적 보안 위협이 발생할 수 있습니다. 따라서 조직의 보안이 손상되지 않도록 적절한 권한 부여 프로파일 및 규칙을 구성해야 합니다.

일부 디바이스에서는 인증서가 만료되기 전과 후에 인증서를 갱신할 수 있습니다. 그러나 Windows 디바이스에서는 인증서가 만료되기 전에만 갱신할 수 있습니다. Apple iOS, Mac OSX 및 Android 디바이스에서는 인증서가 만료되기 전과 후에 인증서를 갱신할 수 있습니다.

인증서 갱신을 위해 정책 조건에 사용되는 사전 속성

Cisco ISE 인증서 사전에는 정책 조건에 사용되는 다음과 같은 속성이 있습니다. 사용자는 그러한 정책 조건을 통해 인증서를 갱신할 수 있습니다.

- Days to Expiry(만료될 때까지 남은 일 수): 이 속성은 인증서가 유효한 기간(일)을 제공합니다. 이 속성을 사용하여 권한 부여 정책에 사용할 수 있는 조건을 생성할 수 있습니다. 이 속성은 0~15 범위의 값을 사용할 수 있습니다. 값 0은 인증서가 이미 만료되었음을 나타냅니다. 값 1은 인증서가 만료되기까지 1일이 채 남지 않았음을 나타냅니다.
- Is Expired(만료됨): 이 부울 속성은 인증서가 만료되었는지 여부를 나타냅니다. 인증서 만료가 다가오는 경우 인증서가 만료되기 전에만 인증서 갱신을 허용하려면, 권한 부여 정책 조건에서 이 속성을 사용합니다.

인증서 갱신을 위한 권한 부여 정책 조건

권한 부여 정책에서 CertRenewalRequired 단순 조건(기본적으로 사용 가능)을 사용하여 Cisco ISE에서 요청을 추가로 처리하기에 앞서 인증서(만료됨 또는 만료 예정)가 갱신되었는지 확인할 수 있습니다.

인증서 갱신을 위해 **CWA** 리디렉션

사용자 인증서가 만료되기 전에 취소되면 Cisco ISE가 CA에서 게시한 CRL을 확인하고 인증 요청을 거부합니다. 취소된 인증서가 만료된 경우 CA는 CRL에 이 인증서를 게시하지 않을 수 있습니다. 이 시나리오에서 Cisco ISE는 취소된 인증서를 갱신할 수 있습니다. 이런 문제를 방지하려면 인증서를 갱신하기 전에 전체 인증을 위해 요청이 CWA(Centralized Web Authentication)로 리디렉션되는지 확인해 주십시오. 사용자를 CWA로 리디렉션하려면 권한 부여 프로파일을 생성해야 합니다.

사용자가 인증서를 갱신할 수 있도록 **Cisco ISE** 구성

사용자가 인증서를 갱신할 수 있도록 Cisco ISE를 구성하려면 이 절차에 나와 있는 작업을 완료해야 합니다.

시작하기 전에

CWA 요청을 리디렉션하도록 WLC에서 제한된 액세스 ACL을 구성합니다.

단계 **1** 허용되는 프로토콜 컨피그레이션 업데이트, 100 페이지
단계 **2** CWA 리디렉션용 권한 부여 정책 프로파일 생성, 100 페이지
단계 **3** 인증서 갱신용 권한 부여 정책 규칙 생성, 101 페이지
단계 **4** 게스트 포털에서 BYOD 설정 활성화, 102 페이지

허용되는 프로토콜 컨피그레이션 업데이트

단계 **1** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authentication(**인증**)** > **Allowed Protocols(**허용되는 프로토콜**)** > **Default Network Access(**기본 네트워크 액세스**)**를 선택합니다.

단계 **2** EAP-TLS 프로토콜 아래에서 **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy(**만료된 인증서 인증을 허용하여 권한 부여 정책에서 인증서 갱신 허용**)** 확인란을 선택하고 PEAP 및 EAP-FAST 프로토콜용 EAP-TLS 내부 메서드를 선택합니다.

그러면 EAP-TLS를 사용하는 요청이 NSP 플로우를 통과하게 됩니다.

PEAP 및 EAP-FAST 프로토콜의 경우 Cisco ISE가 요청을 처리하도록 Cisco AnyConnect를 수동으로 구성해야 합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

CWA 리디렉션용 권한 부여 정책 프로파일 생성, 100 페이지

CWA 리디렉션용 권한 부여 정책 프로파일 생성

시작하기 전에

WLC에서 제한된 액세스 ACL을 구성했는지 확인합니다.

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

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 권한 부여 프로파일의 이름을 입력합니다. 예를 들어 CertRenewal_CWA와 같이 입력합니다.

단계 **4** 일반 작업 영역에서 **Web Redirection (CWA, DRW, MDM, NSP, CPP)(**웹 리디렉션**(CWA, DRW, MDM, NSP, CPP))** 확인란을 선택합니다.

단계 **5** 드롭다운 목록에서 **Centralized Web Auth(**중앙 웹 인증**)**를 선택하고 제한된 액세스 ACL을 선택합니다.

단계 **6** **Display Certificates Renewal Message(**인증서 갱신 메시지 표시**)** 확인란을 선택합니다.

URL-redirect 속성 값이 변경되어 인증서가 유효한 기간(일)이 포함됩니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

참고 Cisco ISE 1.2에서 무선 디바이스용으로 다음과 같은 DRW(Device Registration WebAuth) 정책을 구성한 경우:

- 조건 = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) 및 프로파일 = Wireless-drw-redirect가 포함된 DRW-Redirect 정책
- 조건 = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) 및 프로파일 = Wireless-Permit이 포함된 DRW-Allow 정책

ISE 1.3 이상 버전으로 업그레이드한 후 DRW-Allow 정책 조건을 다음과 같이 업데이트해야 합니다.

- 조건 = (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow) 및 프로파일 = Wireless-Permit

다음에 수행할 작업

인증서 갱신용 권한 부여 정책 규칙 생성, 101 페이지

인증서 갱신용 권한 부여 정책 규칙 생성

시작하기 전에

중앙 웹 인증 리디렉션용 권한 부여 프로파일을 생성했는지 확인합니다.

Administration(관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Policy Settings(**정책 집합**)**에서 정책 집합을 활성화합니다.

단계 **1** **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Policy Sets(**정책 집합**)**를 선택합니다.

단계 **2** **Create Above(**위에 생성**)**를 클릭합니다.

단계 **3** 새 규칙의 이름을 입력합니다.

단계 **4** 다음의 단순 조건 및 결과를 선택합니다.

CertRenewalRequired=True인 경우 권한에 대해 앞에서 생성한 권한 부여 프로파일(CertRenewal_CWA)을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

참고 Cisco ISE에서는 한 번에 최대 50개의 권한 부여 정책을 로드할 수 있으며, 다음 정책 집합을 로드하는 데 약 10초가 지연됩니다.

참고 생성된 정책 목록에서 특정 권한 부여 정책을 검색하는 경우 검색 창에 제공된 정책 이름이 아래 정책 목록에서 강조 표시되지만 필터링되지는 않습니다.

다음에 수행할 작업

인증서가 만료된 디바이스를 사용하여 회사 네트워크에 액세스할 때는 **Renew(**갱신**)**를 클릭하여 디바이스를 재구성합니다.

게스트 포털에서 **BYOD** 설정 활성화

사용자가 개인 디바이스 인증서를 갱신할 수 있도록 하려면 선택한 게스트 포털에서 BYOD 설정을 활성화해야 합니다.

단계 **1** **Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals and Components(**포털 및 구성 요소**)** > **Guest Portals(**게스트 포털**)**를 선택합니다.

a) 선택한 CWA 포털을 고르고 **Edit(**편집**)**를 클릭합니다.

단계 **2** BYOD Settings(BYOD 설정)에서 **Allow employees to use personal devices on the network(**네트워크에서 직원의 개인 디바이스 사용 허용**)** 확인란을 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

Apple iOS 디바이스용 인증서 갱신 실패

ISE를 사용하여 Apple iOS 디바이스에서 엔드포인트 인증서를 갱신하는 경우 "Profiled Failed to Install(프로파일링 설치 실패)" 오류 메시지가 표시될 수 있습니다. 이 오류 메시지는 만료 예정이거나 만료된 네트워크 프로파일이 동일한 PSN(Policy Service Node)에서, 또는 다른 PSN에서 갱신 처리에 사용되는 것과 다른 관리 HTTPS 인증서로 서명된 경우에 나타납니다.

문제 해결을 위해서는 일반적으로 UCC(Unified Communications Certificate)라고 하는 다중 도메인 SSL 인증서, 또는 구축의 모든 PSN에서 관리 HTTPS에 대해 와일드카드 인증서를 사용해 주십시오.

인증서 정기 확인 설정

Cisco ISE는 CRL(Certificate Revocation List)을 정기적으로 확인합니다. 이 창에서는 자동으로 다운로드되는 CRL에 대해 진행 중인 세션을 확인하도록 Cisco ISE를 구성할 수 있습니다. 매일 OCSP 또는 CRL 확인을 시작해야 하는 시간과 Cisco ISE가 OCSP 서버 또는 CRL을 다시 확인할 때까지 대기하는 시간 간격을 시간 단위로 지정할 수 있습니다.

다음 표에서는 인증서(OCSP 또는 CRL)의 상태를 확인할 시간 간격을 지정할 수 있는 Certificate Periodic Check Settings(인증서 정기 확인 설정) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Periodic Check Settings(**인증서 정기 확인 설정**)**입니다.

표 ***15:*** 인증서 정기 확인 설정

필드 이름	사용 지침
Certificate Check Settings(인증서 확인 설정**)**	

필드 이름	사용 지침
Check ongoing sessions against automatically retrieved CRL(자동으로 검색된 **CRL**에 대해 진행 중인 세션 확인**)**	Cisco ISE가 자동으로 다운로드되는 CRL에 대해 진행 중인 세션을 확인하도록 지정하려면 이 확인란을 선택합니다.
CRL/OCSP Periodic Certificate Checks(CRL/OCSP 정기 인증서 확인**)**	
First check at(첫 확인 시간**)**	매일 CRL 또는 OCSP 확인을 시작할 시간을 지정합니다. 00:00~23:59시간 사이의 값을 입력합니다.
Check every(확인 간격**)**	Cisco ISE가 CRL 또는 OCSP 서버를 다시 확인할 때까지 대기하는 시간 간격을 시간 단위로 지정합니다.

관련 항목

OCSP 서비스, 139 페이지
OCSP 클라이언트 프로파일 추가, 141 페이지

Cisco ISE CA 서비스

인증서는 자체 서명되거나 외부 CA(Certificate Authority)에 의해 디지털 서명될 수 있습니다. Cisco ISE Internal Certificate Authority(ISE CA)는 엔드포인트에 대한 디지털 인증서를 발급하고 중앙 집중식 콘솔에서 관리하므로 직원이 회사 네트워크에서 개인 디바이스를 사용할 수 있습니다. CA 서명 디지털 인증서는 업계 표준으로 보안성이 더 높은 것으로 간주됩니다. 기본 PAN은 루트 CA입니다. PSN(Policy Service Nodes)은 기본 PAN(SCEP RA)에 대한 하위 CA입니다. ISE CA는 다음과 같은 기능을 제공합니다.

- Certificate Issuance: 네트워크에 연결되는 엔드포인트에 대한 CSR(Certificate Signing Requests)을 검증하고 서명합니다.
- Key Management: 키와 인증서를 생성하고 PAN 및 PSN 노드에서 모두 안전하게 저장합니다.
- Certificate Storage: 사용자 및 디바이스에 발급된 인증서를 저장합니다.
- Support OCSP(Online Certificate Status Protocol): 인증서의 유효성을 확인하도록 OCSP 응답자를 제공합니다.

기본 관리 노드에서 CA 서비스가 비활성화된 경우에도 보조 관리 노드의 CLI에서 실행 중인 것으로 간주됩니다. CA 서비스는 비활성화된 상태로 표시하는 것이 가장 좋습니다. 이는 알려진 Cisco ISE 문제입니다.

Cisco ISE 인증서 핑거프린트

인증서 핑거프린트 프로세스는 신뢰할 수 있는 인증서와 일치하도록 인증서 즉시 발급 핑거프린트 SHA256을 평가하는 데 사용됩니다. 이렇게 하면 여러 CA가 서로 다른 도메인을 지원하도록 보안 메커니즘이 적용되며 802.1x 프로토콜용으로 신뢰할 수 있는 CA를 잠글 수도 있습니다.

정책 조건에서 인증서를 업데이트하기 전에 발급자 핑거프린트 SHA-256 인증서가 Cisco ISE 구축에 추가되었는지 확인하십시오.

참고 신뢰할 수 있는 인증서가 정책으로 구성된 후에는 인증서를 삭제할 수 없습니다. 다음 메시지가 **Trusted Certificates(**신뢰할 수 있는 인증서**)** 창의 **This Trusted Certificate Refered by Policy Sets(**정책 집합에서 참조하는 신뢰할 수 있는 인증서**)**에 표시됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

인증서가 정책에서 사용되므로 인증서를 삭제할 수 없습니다. 인증서를 삭제하려면 먼저 정책 조건을 수정하십시오.

Cisco ISE용 인증서 핑거프린트를 구성하려면 아래 단계를 순서대로 수행합니다.

1. 내부 사용자를 생성합니다. 자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드, 릴리스 *3.0*의 "자산 가시성" 장에서 "사용자 추가" 섹션을 참조하십시오.
2. 네트워크 디바이스를 추가합니다. 자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드, 릴리스 *3.0*의 "기본 설정" 장에서 "Cisco ISE에서 네트워크 디바이스 추가" 섹션을 참조하십시오.
3. **External Certificates(**외부 인증서**)**에서 외부 CA를 가져옵니다. 자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드, 릴리스 *3.0*의 "기본 설정" 장에서 "시스템 인증서 가져오기" 섹션을 참조하십시오.

   SCEP 프로토콜을 사용하여 발급자 핑거프린트 SHA-256 인증서를 가져올 수도 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authorit(**인증 기관**)** > **External CA Settings(**외부 **CA** 설정**)**를 선택합니다. 표시되는 **Add SCEP RA Profile(SCEP RA** 프로파일 추가**)** 창에서 **Add(**추가**)**를 클릭합니다. **Name(**이름**)** 필드에 인증서 이름을 입력합니다. **URL** 필드에 CA 서버 URL을 입력합니다. **Test Connection(**테스트 연결**)**을 클릭합니다.
4. SHA-256 핑거프린트로 정책 생성
5. SHA-256 핑거프린트를 사용하여 인증 정책 생성 및 매핑
6. 권한 부여 정책 생성.
7. PRRT 로그 확인

SHA-256 핑거프린트로 정책 생성

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

단계 2 표시되는 **Policy Set(정책 집합)** 창에서 **Settings(설정)**를 클릭하고 드롭다운 목록에서 **Insert a new row(새 행 삽입)**를 선택합니다.

단계 3 **New Policy Name(새 정책 이름)** 필드에 이름을 입력합니다.

단계 4 이 정책에 대한 설명을 입력합니다.

단계 5 **Conditions(조건)** 열 아래에서 새 **Policy Set Name(정책 집합 이름)** 옆의 **Add(추가)(+)** 아이콘을 클릭합니다.

단계 6 표시되는 **Condition Studio** 창에서 **Click to Add Attribute(속성을 추가하려면 클릭)** 필드를 클릭합니다.

단계 7 **All Dictionary(모든 사전)** 드롭다운 목록에서 **Network Access-Protocol(네트워크 액세스-프로토콜)**(**Dictionary-Attribute(사전-속성)**) 조합을 선택합니다.

단계 8 논리 조건을 작성하기 위해 **Equals(같음)** 연산자를 선택합니다.

단계 9 **Choose from List or Type(목록 또는 유형 선택)** 드롭다운 목록에서 **RADIUS**를 선택합니다.

단계 10 **Use(사용)**를 클릭합니다.

단계 11 표시되는 **Policy Set(정책 집합)** 창의 **Allowed Protocols/Server Sequence(허용되는 프로토콜/서버 시퀀스)** 드롭다운 목록에서 **Default Network Access(기본 네트워크 액세스)**를 선택합니다.

단계 12 **Save(저장)**를 클릭합니다.

SHA-256 핑거프린트를 사용하여 인증 정책 생성 및 매핑

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

단계 2 **Authentication Policy(인증 정책)**를 클릭합니다.

단계 3 Settings(설정) 아이콘을 클릭하고 **Insert a new row(새 행 삽입)**를 선택합니다.

단계 4 **Authentication Rule Name(인증 규칙 이름)** 창에서 이름을 입력합니다.

단계 5 규칙 이름 옆에 있는 **Add(추가)(+)** 아이콘을 클릭합니다.

단계 6 표시되는 **Condition Studio** 창에서 **Click to add Attributes(클릭하여 속성 추가)** 필드를 클릭합니다.

단계 7 **All Dictionary(모든 사전)** 드롭다운 목록에서 **CERTIFICATE-Issuer- Fingerprint SHA-256**(**Dictionary-Attribute**) 조합을 선택합니다.

단계 8 논리 조건을 작성하기 위해 **Equals(같음)** 연산자를 선택합니다.

단계 9 **Choose from List or Type(목록 또는 유형에서 선택)** 드롭다운 목록에서 **Cisco Manufacturing CA SHA2 fingerprint sha256**을 선택합니다.

단계 10 **Use(사용)**를 클릭합니다.

단계 11 표시되는 **Policy Set(정책 집합)** 창의 **Allowed Protocols/Server Sequence(허용되는 프로토콜/서버 시퀀스)** 드롭다운 목록에서 **Preloaded_Certificate_Profile**을 선택합니다.

단계 12 **Save(저장)**를 클릭합니다.

권한 부여 정책 생성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Set(**정책 집합**)** > **Default(**기본값**)**를 선택합니다.

단계 **2** **Authorization Policy(**권한 부여 정책**)**을 클릭합니다.

단계 **3** 설정 아이콘을 클릭하고 드롭 다운 목록에서 **Insert a new row(**새 행 삽입**)**를 선택합니다.

단계 **4** **Authorization Rule Name(**권한 부여 규칙 이름**)** 창에서 이름을 입력합니다.

단계 **5** 규칙 이름 옆에 있는 **Add(**추가**)**(+) 아이콘을 클릭합니다.

단계 **6** 표시되는 **Condition Studio** 창에서 **Click to add Attributes(**클릭하여 속성 추가**)** 필드를 클릭합니다.

단계 **7** **All Dictionary(**모든 사전**)** 드롭다운 목록에서 **CERTIFICATE-Issuer- Fingerprint SHA-256(Dictionary-Attribute)** 조합을 선택합니다.

단계 **8** 논리 조건을 작성하기 위해 **Equals(**같음**)** 연산자를 선택합니다.

단계 **9** 목록 또는 유형 드롭 다운 목록에서 **Cisco Root CA 2099** 핑거프린트 **sha**를 선택합니다.

단계 **10** **Use(**사용**)**를 클릭합니다.

단계 **11** 표시되는 **Policy Set(**정책 집합**)** 창의 **Allowed Protocols/Server Sequence(**허용되는 프로토콜/서버 시퀀스**)** 드롭다운 목록에서 **PermitAccess(**액세스 허용**)**를 선택합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

PRRT 로그 확인

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operation(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**.

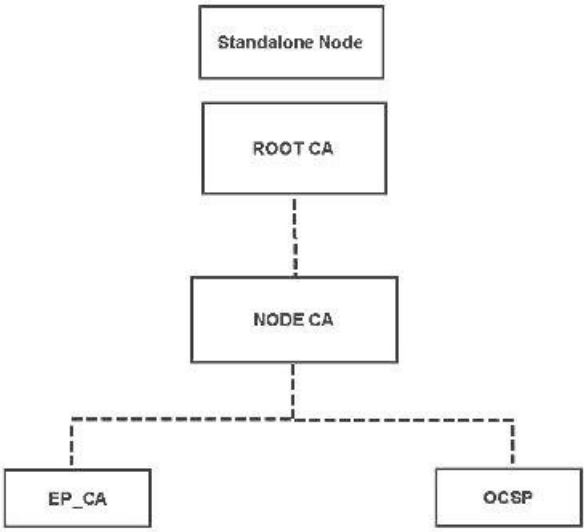
단계 **2** 표시되는 **Live Logs(**라이브 로그**)** 창에서 최신 로그 세부정보를 클릭합니다.

단계 **3** 표시되는 **Authentication Details(**인증 세부정보**)** 창에서 **Issuer- Fingerprint SHA-256(**발급자- 핑거프린트 **SHA-256)** 열의 SHA-256 값을 확인하여 **Issuer- Fingerprint SHA-256(**발급자- 핑거프린트 **SHA-256)** 인증서가 성공적으로 추가 및 검증되었는지 확인합니다.

관리 및 정책 서비스 노드에 프로비저닝된 **ISE CA** 인증서

설치 후 Cisco ISE 노드에는 엔드포인트용 인증서를 관리할 수 있도록 루트 CA 인증서와 노드 CA 인증서가 프로비저닝됩니다.

그림 ***7:*** 독립형 노드에 프로비저닝된 ***ISE CA*** 인증서

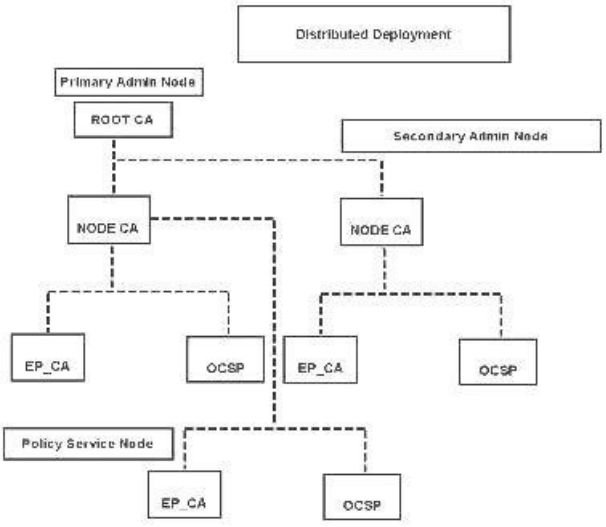


구축을 설정할 때는 PAN(Primary Administration Node)으로 지정하는 노드가 루트 CA가 됩니다. PAN에는 루트 CA 인증서 및 루트 CA가 서명한 노드 CA 인증서가 있습니다.

보조 관리 노드를 PAN에 등록하면 노드 CA 인증서가 생성되며, 기본 관리 노드의 루트 CA가 이 인증서에 서명합니다.

PAN에 등록하는 모든 PSN(Policy Service Node)에는 PAN의 노드 CA가 서명한 OCSP 인증서 및 엔드포인트 CA가 프로비저닝됩니다. PSN(Policy Service Node)은 PAN의 하위 CA입니다. ISE CA를 사용할 때는 PSN의 엔드포인트 CA가 네트워크에 액세스하는 엔드포인트에 대해 인증서를 발급합니다.

그림 ***8:*** 구축의 관리 및 정책 서비스 노드에 프로비저닝된 ***ISE CA*** 인증서



CA와 Cisco ISE의 상호운용성을 위한 요구 사항

CA 서버와 Cisco ISE를 함께 사용할 때는 다음 요구 사항이 충족되어야 합니다.

- 키 크기는 1024, 2048 또는 그 이상이어야 합니다. CA 서버에서 키 크기는 인증서 템플릿을 사용하여 정의됩니다. Cisco ISE에서 서플리컨트 프로파일을 사용하여 키 크기를 정의할 수 있습니다.
- 키를 사용하면 확장 프로그램에서 서명 및 암호화가 지원됩니다.
- SCEP 프로토콜을 통해 GetCACapabilities를 사용하면 암호화 알고리즘과 요청 해시가 지원됩니다. RSA 및 SHA1을 사용하는 것이 권장됩니다.
- OCSP(Online Certificate Status Protocol)가 지원됩니다. 이 프로토콜은 BYOD에서 직접적으로 사용되지는 않지만, 인증 철회 시 OCSP 서버처럼 작동하는 CA가 사용될 수 있습니다.

  참고 Cisco ISE는 PEAP, EAP-TLS 등의 표준 EAP 인증을 위해 EJBCA(Enterprise Java Beans Certificate Authority)를 지원합니다. 프록시 SCEP에 대한 EJBCA 지원을 활성화하려면 EJBCA에서 **System(**시스템**) > Basic Configurations(**기본 컨피그레이션**)**에 있는 **Enable End Entity Profile Limitations(**종료 엔터티 프로파일 제한 활성화**)** 옵션을 비활성화해야합니다.

- 엔터프라이즈 PKI를 사용하여 Apple iOS 디바이스용 인증서를 발급하는 경우 SCEP 템플릿에서 키 사용을 구성하고 **Key Encipherment(**키 암호화**)** 옵션을 활성화해야 합니다.

  Microsoft CA를 사용하는 경우 인증서 템플릿에서 키 사용 확장을 편집합니다. **Encryption(**암호화**)** 영역에서 **Allow Key Exchange only with Key Encryption (Key encipherment)(**키 암호화를 사용하여 키 교환만 허용**(**키 암호화**))** 라디오 버튼을 클릭하고 **Allow Encryption of User Data(**사용자 데이터 암호화 허용**)** 확인란을 선택합니다.

- Cisco ISE는 EAP-TLS 인증을 위한 신뢰할 수 있는 인증서 및 엔드포인트 인증서에 대해 RSASSA-PSS 알고리즘 사용을 지원합니다. 인증서를 볼 때 서명 알고리즘은 알고리즘 이름 대신 1.2.840.113549.1.1.10으로 나열됩니다.

참고 BYOD 플로우에 Cisco ISE 내부 CA를 사용하는 경우 외부 CA에서 RSASSA-PSS 알고리즘을 통해 관리자 인증서에 서명해서는 안 됩니다. Cisco ISE 내부 CA는 해당 알고리즘을 사용하여 서명된 관리자 인증서를 확인할 수 없으며, 요청이 실패합니다.

인증서 기반 인증을 위한 클라이언트 인증서 요건

Cisco ISE를 통한 인증서 기반 인증의 경우 클라이언트 인증서가 다음 요건을 충족해야 합니다.

표 ***16: RSA*** 및 ***ECC***에 대한 클라이언트 인증서 요건

RSA

지원되는 키 크기	1024, 2048 및 4096 비트	
지원되는 SHA(Secure Hash Algorithms)	SHA-1 및 SHA-2(SHA-256 포함)	
ECC [1] [2]		
지원되는 커브 유형	P-192, P-256, P-384 및 P-521	
지원되는 SHA(Secure Hash Algorithm)	SHA-256	
클라이언트 머신 운영체제 및 지원되는 커브 유형		
Windows	8 이상	P-256, P-384 및 P-521
Android	4.4 이상 참고 Android 6.0에서 ECC 인증서를 지원하려면 2016년 5월 패치가 필요합니다.	모든 커브 유형(P-192 커브 유형을 지원하지 않는 Androidv6.0 제외)

[1] Windows 7 및 Apple iOS는 기본적으로 EAP-TLS 인증에 대해 ECC를 지원하지 않습니다.
[2] Cisco ISE의 이 릴리스에서는 MAC OS X 디바이스에서 ECC 인증서 사용을 지원하지 않습니다.

ISE CA 체인 재생성

Cisco ISE CA 체인을 재생성하면 루트 CA, 노드 CA 및 엔드포인트 CA 인증서를 포함한 모든 인증서가 재생성됩니다. PAN 또는 PSN의 도메인 이름이나 호스트 이름을 변경할 때는 ISE CA 체인을 재생성해야 합니다. 이전 릴리스에서 릴리스 2.0 이상으로 업그레이드할 때는 2개의 루트 계층 구조에서 단일 루트 계층 구조로 이동하도록 ISE CA 체인을 재생성하는 것이 좋습니다.

루트 CA이든 중간 CA 인증서이든 시스템 인증서를 재생성하면 ISE 메시징 서비스가 재시작되어 새 인증서 체인이 로드됩니다. ISE 메시징 서비스를 다시 사용할 수 있을 때까지 감사 로그가 손실됩니다.

참고 구축에서 Cisco ISE 내부 CA를 교체할 때마다 ISE 메시징 서비스도 업데이트해야 전체 인증서 체인을 검색할 수 있습니다.

Cisco ISE 내부 CA 체인을 재생성할 경우, 체인에 있는 모든 인증서의 **Valid From(**유효 기간 시작**)** 필드에 재생성 1일 전의 날짜가 표시됩니다.

Elliptical Curve Cryptography 인증서 지원

Cisco ISE CA 서비스는 ECC(Elliptical Curve Cryptography) 알고리즘을 기반으로 하는 인증서를 지원합니다. ECC는 훨씬 작은 키 크기를 사용하는 경우에도 다른 암호화 알고리즘보다 더 우수한 보안 및 성능을 제공합니다.

다음 표에서는 ECC 및 RSA의 키 크기와 보안 수준을 비교합니다.

ECC 키 크기**(**비트**)**	**RSA** 키 크기**(**비트**)**
160	1024
224	2048
256	3072
384	7680
521	15360

키 크기가 더 작기 때문에 암호화가 더 빠릅니다.

Cisco ISE는 다음과 같은 ECC 커브 유형을 지원합니다. 커브 유형 또는 키 크기가 클수록 보안이 우수합니다.

- P-192
- P-256
- P-384
- P-521

ISE는 인증서의 EC 부분에서 명시적 매개변수를 지원하지 않습니다. 명시적 매개변수를 사용하여 인증서를 가져오려고 하면 Validation of certificate failed: Only named ECParameters(인증서 검증 실패: 명명된 EC 매개변수만 지원됨)라는 오류가 표시됩니다.

Cisco ISE CA 서비스는 BYOD 플로우를 통해 연결하는 디바이스용 ECC 인증서를 지원합니다. 인증서 프로비저닝 포털에서 ECC 인증서를 생성할 수도 있습니다.

참고 다음 표에는 ECC를 사용할 수 있는 운영체제 및 버전이 지원되는 커브 유형과 함께 나와 있습니다. 디바이스가 지원되는 운영체제를 실행하고 있지 않거나 지원되는 버전에서 실행되고 있지 않은 경우에는 RSA 기반 인증서를 대신 사용할 수 있습니다.

Operating System(운영 체제**)**	지원되는 버전	지원되는 커브 유형
Windows	8 이상	P-256, P-384 및 P-521
Android	4.4 이상 참고 Android 6.0에서 ECC 인증서를 지원하려면 2016년 5월 패치가 필요합니다.	모든 커브 유형(Android 6.0은 P-192 커브 유형을 지원하지 않으므로 제외).

Windows 7 및 Apple iOS는 기본적으로 EAP-TLS를 통한 인증에 ECC를 지원하지 않습니다. Cisco ISE의 이 릴리스에서는 MAC OS X 디바이스에서 ECC 인증서 사용을 지원하지 않습니다.

EST(Enrollment over Secure Transport) 프로토콜을 사용하는 BYOD 플로우가 정상적으로 작동하지 않으면 다음 사항을 확인하십시오.

- 인증서 서비스 엔드포인트 하위 CA 인증서 체인이 완료 되었습니다. 인증서 체인이 완료되었는지 확인하려면 다음을 수행합니다.
  1. **Administration(**관리**) > System(**시스템**) > Certificates(**인증서**) > Certificate Authority(**인증 기관**) > Certificate Authority Certificates(**인증 기관 인증서**)**를 선택합니다.
  2. 확인할 인증서 옆의 확인란을 선택하고 **View(**보기**)**를 클릭합니다.
- CA 및 EST 서비스가 작동되어 실행 중인지 확인합니다. 서비스가 실행되지 않으면 **Administration(**관리**) > System(**시스템**) > Certificates(**인증서**) > Certificate Authority(**인증 기관**) > Internal CA Settings(**내부 **CA** 설정**)**로 이동하여 CA 서비스를 활성화합니다.
- 2.0 이전의 ISE 버전에서 Cisco ISE 2.x로 업그레이드한 경우 업그레이드 후에 ISE 루트 CA 인증서 체인을 교체합니다. 방법은 다음과 같습니다.
  1. **Administration(**관리**) > System(**시스템**) > Certificates(**인증서**) > Certificate Management(**인증서 관리**) > Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.
  2. **Generate Certificate Signing Requests (CSR)(CSR** 생성**)**를 클릭합니다.
  3. Choose ISE Root CA from one or more Certificates(하나 이상의 인증서에서 ISE 루트 CA 선택)는 드롭다운 목록에 사용됩니다.
  4. **Replace ISE Root CA Certificate Chain(ISE** 루트 **CA** 인증서 체인 교체**)**을 클릭합니다.

참고 이 Cisco ISE 릴리스에서는 EST 클라이언트가 Cisco ISE 내에 있는 EST 서버에 대해 직접 인증하는 것을 지원하지 않습니다.

Android 또는 Windows 엔드포인트를 온보딩하는 동안 ECC 기반 인증서에 대한 요청이 있는 경우 ISE는 EST 플로우를 트리거합니다.

Cisco ISE 인증 기관 인증서

CA(인증기관) 인증서 페이지에는 내부 Cisco ISE CA와 관련된 모든 인증서가 나열됩니다. 이전 릴리스에서 이러한 CA 인증서는 Trusted Certificates(신뢰할 수 있는 인증서) 저장소에서 제공되었지만 이제는 CA Certificates(CA 인증서) 페이지로 이동되었습니다. 이러한 인증서는 이 페이지에 노드별로 나열됩니다. 노드를 펼쳐서 해당 특정 노드의 모든 ISE CA 인증서를 확인할 수 있습니다. 기본 및 보조 관리 노드에는 루트 CA, 노드 CA, 하위 CA 및 OCSP 응답자 인증서가 있습니다. 구축의 다른 노드에는 엔드포인트 하위 CA 및 OCSP 인증서가 있습니다.

Cisco ISE CA 서비스를 활성화하면 이러한 인증서가 생성되어 모든 노드에 자동으로 설치됩니다. 또한 전체 ISE 루트 CA 체인을 교체하면 이러한 인증서가 재생성되어 모든 노드에 자동으로 설치됩니다. 수동 개입이 필요하지 않습니다.

Cisco ISE CA 인증서는 **Certificate Services** <***Endpoint Sub CA/Node CA/Root CA/OCSP Responder***>-<*node_hostname*>#*certificate_number* 명명 규칙을 따릅니다.

CA 인증서 페이지에서 Cisco ISE CA 인증서의 편집, 가져오기, 내보내기, 삭제 및 보기가 가능합니다.

Cisco ISE CA 인증서 편집

Cisco ISE CA 인증서 저장소에 인증서를 추가한 뒤에는 설정 편집을 사용하여 추가로 편집할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Authority Certificates(**인증 기관 인증서**)**를 선택합니다. .

단계 **2** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 를 선택합니다.

단계 **3** 편집할 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** 편집 가능한 필드를 필요한 대로 수정합니다. 필드에 대한 설명은 신뢰할 수 있는 인증서 설정을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭하여 인증서 저장소에 대한 변경사항을 저장합니다.

Cisco ISE CA 인증서 내보내기

Cisco ISE 루트 CA 및 노드 CA 인증서를 내보내려면 다음을 수행합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 1 **Administration**(관리) > **System**(시스템) > **Certificates**(인증서) > **Certificate Authority**(인증 기관) > **Certificate Authority Certificates**(인증 기관 인증서)를 선택합니다.

단계 2 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 3 내보낼 인증서 옆의 확인란을 선택하고 **Export**(내보내기)를 클릭합니다. 인증서는 한 번에 하나씩만 내보낼 수 있습니다.

단계 4 클라이언트 브라우저를 실행 중인 파일 시스템에 프라이버시가 강화된 메일 파일을 저장합니다.

Cisco ISE CA 인증서 가져오기

엔드포인트가 다른 의 Cisco ISE CA에서 발급한 인증서를 사용하여 네트워크에 인증하려고 하는 경우에는 해당 구축의 Cisco ISE 루트 CA, 노드 CA 및 엔드포인트 하위 CA 인증서를 Cisco ISE 신뢰할 수 있는 인증서 저장소로 가져와야 합니다.

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- 엔드포인트 인증서가 서명된 구축에서 ISE 루트 CA, 노드 CA 및 엔드포인트 하위 CA 인증서를 내보낸 다음 브라우저를 실행 중인 컴퓨터의 파일 시스템에 저장합니다.

단계 1 엔드포인트가 인증되는 구축의 관리 포털에 로그인합니다.

단계 2 **Administration**(관리) > **System**(시스템) > **Certificates**(인증서) > **Trusted Certificates**(신뢰할 수 있는 인증서)를 선택합니다.

단계 3

단계 4 **Import**(가져오기)를 클릭합니다.

단계 5 필요한 대로 필드 값을 구성합니다. 자세한 내용은 신뢰할 수 있는 인증서 가져오기 설정을 참조하십시오.

클라이언트 인증서 기반 인증이 활성화되어 있으면 Cisco ISE는 구축의 각 노드에서 애플리케이션 서버를 다시 시작합니다. 이때 PAN에서 애플리케이션 서버부터 시작한 다음 각 추가 노드의 애플리케이션 서버를 하나씩 시작합니다.

인증서 템플릿

인증서 템플릿은 해당 템플릿을 기준으로 CA(Certificate Authority)에서 발급한 모든 인증서에 일반적인 속성을 포함합니다. 인증서 템플릿은 사용해야 하는 주체, SAN(Subject Alternative Name), 키 크기, SCEP RA 프로파일, 인증서의 유효 기간, 그리고 클라이언트 또는 서버 인증이나 두 인증에 모두 인증서를 사용해야 하는지 여부를 지정하는 EKU(Extended Key Usage: 확장 키 사용)를 정의합니다. 내

부 Cisco ISE CA(ISE CA)는 인증서 템플릿을 사용하여 해당 템플릿을 기준으로 인증서를 발급합니다.

Cisco ISE에서는 다음과 같은 ISE CA용 기본 인증서 템플릿이 제공됩니다. 필요한 경우 추가 인증서 템플릿을 생성할 수 있습니다. 기본 인증서 템플릿은 다음과 같습니다.

- CA_SERVICE_Certificate_Template - ISE CA(Certificate Authority)를 사용하는 기타 네트워크 서비스용입니다. 예를 들어 ASA VPN 사용자를 위한 인증서를 발급하도록 ISE를 구성하는 동안 이 인증서 템플릿을 사용합니다. 이 인증서 템플릿에서는 유효 기간만 수정할 수 있습니다.
- EAP_Authentication_Certificate_Template - EAP 인증용입니다.
- pxGrid_Certificate_Template - Certificate Provisioning Portal(인증서 프로비저닝 포털)에서 인증서를 생성하는 동안 pxGrid 컨트롤러에 사용됩니다.

인증서 템플릿 이름 익스텐션

Cisco ISE 내부 CA에는 엔드포인트 인증서를 생성하는 데 사용된 인증서 템플릿을 나타내는 익스텐션이 포함되어 있습니다. 내부 CA에서 발급한 모든 엔드포인트 인증서에는 인증서 템플릿 이름 익스텐션이 포함됩니다. 이 익스텐션은 해당 엔드포인트 인증서를 생성하는 데 사용된 인증서 템플릿을 나타냅니다. 익스텐션 ID는 1.3.6.1.4.1.9.21.2.5입니다. 권한 부여 정책 조건에서 CERTIFICATE: Template Name(인증서: 템플릿 이름) 속성을 사용하여 평가 결과에 따라 적절한 액세스 권한을 할당할 수 있습니다.

권한 부여 정책 조건에서 인증서 템플릿 이름 사용

권한 부여 정책 규칙에서 인증서 템플릿 이름 익스텐션을 사용할 수 있습니다.

단계 **1** **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택하고 기본 정책 집합을 확장하여 권한 부여 정책 규칙을 확인합니다.

단계 **2** 새 규칙을 추가하거나 기존 규칙을 편집합니다. 이 예에서는 Compliant_Device_Access 규칙 편집에 대해 설명합니다.

a) Compliant_Device_Access 규칙을 편집합니다.
b) **Add Attribute/Value(**속성/값 추가**)**를 선택합니다.
c) Dictionaries(사전)에서 **CERTIFICATE: Template Name(**인증서**:** 템플릿 이름**)** 속성과 **Equals(**같음**)** 연산자를 선택합니다.
d) 인증서 템플릿 이름의 값을 입력합니다. 예를 들어 EAP_Authentication_Certificate_Template을 입력합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

---

pxGrid 컨트롤러용 **Cisco ISE CA** 인증서 구축

Cisco ISE CA는 pxGrid 컨트롤러가 인증서 프로비저닝 포털에서 인증서를 생성하도록 인증서 템플릿을 제공합니다.

시작하기 전에

pxGrid 클라이언트용 CSR(Certificate Signing Request)을 생성하고 CSR의 내용을 클립보드에 복사합니다.

단계 **1** 네트워크 액세스 사용자 계정을 생성(Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자) > Add(추가))합니다.

사용자가 할당된 사용자 그룹을 적어 둡니다.

단계 **2** 인증서 프로비저닝 포털 설정을 편집(Administration(관리) > Device Portal Management(디바이스 포털 관리) > Certificate Provisioning(인증서 프로비저닝))합니다.

a) 인증서 프로비저닝 포털을 선택하고 **Edit(**편집**)**를 클릭합니다.

b) **Portal Settings(**포털 설정**)** 드롭다운 목록을 클릭합니다. 권한 부여된 그룹 구성의 사용 가능 목록에서 네트워크 액세스 사용자가 속하는 사용자 그룹을 선택하고 선택됨 목록으로 이동합니다.

c) **Certificate Provisioning Portal Settings(**인증서 프로비저닝 포털 설정**)** 드롭다운 목록을 클릭합니다. pxGrid_Certificate_Template을 선택합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 게스트 및 *BYOD*의 인증서 프로비저닝 포털 포털 설정 섹션을 참고하십시오.

d) 포털 설정을 저장합니다.

단계 **3** 인증서 프로비저닝 포털을 시작합니다. Portal Test URL(포털 테스트 URL) 링크를 클릭합니다.

a) 1단계에서 생성한 사용자 계정을 사용하여 인증서 프로비저닝 포털에 로그인합니다.

b) AUP를 수락하고 **Continue(**계속**)**를 클릭합니다.

c) **I want to(**수행할 작업**)** 드롭다운 목록에서 **Generate a single certificate (with certificate signing request)(**인증서 서명 요청을 사용하여 단일 인증서 생성**)**를 선택합니다.

d) Certificate Signing Request Details(인증서 서명 요청 세부정보) 필드에 클립보드의 CSR 내용을 붙여 넣습니다.

e) **Certificate Download Format(**인증서 다운로드 형식**)** 드롭다운 목록에서 **PKCS8 format(PKCS8** 형식**)**을 선택합니다.

참고 PKCS12 형식을 선택하는 경우 단일 인증서 파일을 별도의 인증서 및 키 파일로 변환해야 합니다. 인증서 및 키 파일은 이진 DER로 인코딩되거나 PEM 형식이어야만 Cisco ISE로 가져올 수 있습니다.

f) **Choose Certificate Template(**인증서 템플릿 선택**)** 드롭다운 목록에서 **pxGrid_Certificate_Template**을 선택합니다.

g) 인증서 비밀번호를 입력합니다.

h) **Generate(**생성**)**를 클릭합니다.

인증서가 생성됩니다.

i) 인증서를 내보냅니다.

인증서가 인증서 체인과 함께 내보내기됩니다.

단계 **4** pxGrid 클라이언트의 신뢰할 수 있는 인증서 저장소로 Cisco ISE CA 체인을 가져옵니다.

Simple Certificate Enrollment Protocol 프로파일

사용자가 네트워크에 등록할 수 있는 다양한 모바일 디바이스에 대한 인증서 프로비저닝 기능을 활성화하기 위해, Cisco ISE에서는 Cisco ISE가 여러 CA 위치를 가리키도록 하나 이상의 SCEP(Simple Certificate Enrollment Protocol) CA(Certificate Authority) 프로파일(Cisco ISE 외부 CA 설정이라고 함)을 구성할 수 있습니다. 여러 프로파일을 허용하는 경우의 이점은 고가용성을 보장하고 지정한 CA 위치 전체에서 로드 밸런싱을 수행할 수 있다는 것입니다. 특정 SCEP CA에 대한 요청이 3번 연속으로 응답이 없는 경우 Cisco ISE는 특정 서버가 사용 불가능하다고 선언하고 로드 및 응답 시간이 다음으로 가장 낮은 것으로 알려진 CA로 자동으로 전환합니다. 그런 다음 서버가 다시 온라인으로 복구되면 주기적 폴링을 시작합니다.

Cisco ISE와 상호 운용되도록 Microsoft SCEP 서버를 설정하는 방법에 대한 자세한 내용은

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf

를 참고해 주십시오.

Issued Certificates(발급된 인증서)

관리 포털은 내부 ISE CA에서 엔드포인트에 발급한 모든 인증서가 나열됩니다(Administration(관리) > System(시스템) > Certificates(인증서) > Endpoint Certificates(엔드포인트 인증서)). Issued Certificates(발급된 인증서) 페이지에서는 인증서 상태를 한 눈에 볼 수 있습니다. 인증서가 취소된 경우 상태 열 위에 마우스를 놓으면 취소 이유를 확인할 수 있습니다. Certificate Template(인증서 템플릿) 열 위에 마우스를 놓으면 인증서의키 유형, 키 크기 또는 커브 유형, 주체, SAN(Subject Alternative Name) 및 유효성과 같은 추가 세부정보를 볼 수 있습니다. 엔드포인트 인증서를 클릭하여 인증서를 볼 수 있습니다.

ISE CA에서 발급한 모든 인증서(BYOD 플로우를 통해 자동으로 프로비저닝된 인증서 및 인증서 프로비저닝 포털에서 가져온 인증서)는 Endpoint Certificates(엔드포인트 인증서) 페이지에 나열됩니다. 이 페이지에서 이러한 인증서를 관리할 수 있습니다.

예를 들어 user7에게 발급된 인증서를 보려면 Friendly Name(식별 이름) 필드 아래 표시되는 텍스트 상자에 user7을 입력합니다. 그러면 Cisco ISE에서 이 사용자에게 발급한 모든 인증서가 표시됩니다. 필터를 취소하려면 텍스트 상자에서 검색어를 제거합니다. 또한 고급 필터 옵션을 사용하여 다양한 검색 기준에 따라 기록을 볼 수도 있습니다.

이 엔드포인트 인증서 페이지에는 필요한 경우 엔드포인트 인증서를 취소할 수 있는 옵션도 제공됩니다.

인증서 관리 개요 페이지에는 구축 환경의 각 PSN 노드에서 발급된 총 엔드포인트 인증서 수가 표시됩니다. 노드별로 취소된 총 인증서 수와 실패한 총 인증서 수도 확인할 수 있습니다. 이 페이지에서 특정한 속성에 따라 데이터를 필터링할 수 있습니다.

발급 및 취소된 인증서

다음 표에서는 Overview of Issued and Revoked Certificates(발급 및 취소된 인증서 개요) 창의 필드에 대해 설명합니다. 구축의 PSN 노드는 엔드포인트에 인증서를 발급합니다. 이 창에서는 구축의 각 PSN 노드에서 발급한 엔드포인트 인증서 관련 정보를 제공합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **System(시스템)** > **Certificates(인증서)** > **Overview(개요)**입니다.

표 *17:* 발급 및 취소된 인증서

필드	사용 지침
Node Name(노드 이름**)**	인증서를 발급한 PSN(Policy Service Node)의 이름입니다.
Certificates Issued(발급된 인증서**)**	PSN 노드에서 발급한 엔드포인트 인증서의 수입니다.
Certificates Revoked(취소된 인증서**)**	취소된 엔드포인트 인증서의 수입니다(PSN 노드에서 발급한 인증서).
Certificates Requests(인증서 요청**)**	PSN 노드에서 처리한 인증서 기반 인증 요청 수입니다.
Certificates Failed(인증서 실패**)**	PSN 노드에서 처리한 인증 요청 중 실패한 인증 요청 수입니다.

관련 항목

Issued Certificates(발급된 인증서), 116 페이지
사용자 및 엔드포인트 인증서 갱신, 98 페이지
개인 디바이스 인증에 인증서를 사용하도록 Cisco ISE 구성, 120 페이지
사용자가 인증서를 갱신할 수 있도록 Cisco ISE 구성, 99 페이지
엔드포인트 인증서 취소, 138 페이지

Cisco ISE CA 인증서 및 키의 백업 및 복구

Cisco ISE CA 인증서 및 키를 안전하게 백업해야 PAN 장애 발생 시 외부 PKI의 루트 CA 또는 중간 CA로 작동하도록 보조 관리 노드를 승격시키려는 경우 보조 관리 노드에서 다시 복구할 수 있습니다. Cisco ISE 컨피그레이션 백업에는 CA 인증서 및 키가 포함되지 않습니다. 대신 CLI(Command Line Interface)를 사용하여 CA 인증서 및 키를 저장소로 내보냈다가 가져와야 합니다. **application configure ise** 명령에는 이제 CA 인증서 및 키를 백업하고 복원할 수 있는 Export(내보내기) 및 Import(가져오기) 옵션이 포함되어 있습니다.

신뢰할 수 있는 인증서 저장소의 다음 인증서가 보조 관리 노드에서 복원됩니다.

- Cisco ISE 루트 CA 인증서
- Cisco ISE 하위 CA 인증서
- Cisco ISE 엔드포인트 RA 인증서
- Cisco ISE OCSP Responder 인증서

다음과 같은 경우에 Cisco ISE CA 인증서 및 키를 백업하고 복원해야 합니다.

- 구축 환경에 보조 관리 노드가 있는 경우
- 전체 Cisco ISE CA 루트 체인을 바꾸는 경우

- 외부 PKI의 하위 CA 역할을 하도록 Cisco ISE 루트 CA를 구성하는 경우
- 릴리스 1.2에서 이후 릴리스로 업그레이드하는 경우
- 컨피그레이션 백업에서 데이터를 복원하는 경우 (이 경우에는 먼저 Cisco ISE CA 루트 체인을 다시 생성한 다음, ISE CA 인증서 및 키를 백업하고 복원해야 합니다.)

참고 구축에서 Cisco ISE 내부 CA를 교체할 때마다 ISE 메시징 서비스도 업데이트해야 전체 인증서 체인을 검색할 수 있습니다.

Cisco ISE CA 인증서 및 키 내보내기

PAN에서 CA 인증서 및 키를 내보내야 보조 관리 노드에서 해당 인증서와 키를 가져올 수 있습니다. 이 옵션을 사용하는 경우 PAN이 다운되면 보조 관리 노드가 엔드포인트에 대해 인증서를 발급하고 관리할 수 있으며, 이 경우 보조 관리 노드를 PAN으로 승격합니다.

시작하기 전에

CA 인증서와 키를 저장할 저장소를 생성했는지 확인합니다.

단계 **1** Cisco ISE CLI에서 **application configure ise** 명령을 입력합니다.

단계 **2** 7을 입력하여 인증서와 키를 내보냅니다.

단계 **3** 저장소 이름을 입력합니다.

단계 **4** 암호화 키를 입력합니다.

내보내진 인증서 목록 및 주체, 발급자, 일련 번호가 포함된 성공 메시지가 나타납니다.

예제**:**

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x621867df-568341cd-944cc77f-c9820765

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

Cisco ISE CA 인증서 및 키 가져오기

보조 관리 노드를 등록한 후에는 PAN에서 CA 인증서와 키를 내보낸 다음 보조 관리 노드로 가져와야 합니다.

단계 **1** Cisco ISE CLI의 **application configure ise** 명령을 입력합니다.

단계 **2** CA 인증서와 키를 가져오려면 8을 입력합니다.

단계 **3** 저장소 이름을 입력합니다.

단계 **4** 가져올 파일의 이름을 입력합니다. 파일 이름은 **ise_ca_key_pairs_of_<vm hostname>** 형식이 되어야 합니다.

단계 **5** 파일 암호를 해독할 암호화 키를 입력합니다.

성공 메시지가 나타납니다.

예제**:**

```
The following 4 CA key pairs were imported:
        Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

        Subject:CN=Cisco ISE Endpoint CA of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

        Subject:CN=Cisco ISE Endpoint RA of ise-vm1
        Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
        Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

        Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
        Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
        Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
```

참고 내 보낸 키 파일의 암호화는 Cisco ISE 릴리스 2.6에 도입되었습니다. Cisco ISE 릴리스 2.4 이하 버전에서 키를 내보내고 Cisco ISE 릴리스 2.6 이상 버전에서 키를 가져오면 성공하지 못합니다.

기본 PAN 및 PSN에서 루트 CA 및 하위 CA 생성

구축을 설정할 때 Cisco ISE는 Cisco ISE CA 서비스용으로 기본 PAN에 루트 CA를 생성하고 PSN에 하위 CA 인증서를 생성합니다. 그러나 기본 PAN 또는 PSN의 도메인 이름이나 호스트 이름을 변경할 때는 기본 PAN에서 루트 CA를, PSN에서 하위 CA를 각각 재생성해야 합니다.

PSN에서 호스트 이름을 변경하려는 경우에는 기본 PAN과 PSN에서 각각 루트 CA와 하위 CA를 재생성하는 대신 호스트 이름을 변경하기 전에 PSN 등록을 취소했다가 변경 후 다시 등록할 수 있습니다. 그러면 새 하위 인증서가 PSN에 자동으로 프로비저닝됩니다.

단계 1 를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**.

단계 2 **Generate Certificate Signing Requests (CSR)(CSR** 생성**)**를 클릭합니다.

단계 3 **Certificate(s) will be used for(**인증서 사용 대상**)** 드롭다운 목록에서 ISE Root CA(ISE 루트 CA)를 선택합니다.

단계 4 **Replace ISE Root CA Certificate chain(ISE** 루트 **CA** 인증서 체인 교체**)**을 클릭합니다.

루트 CA 및 하위 CA 인증서가 구축의 모든 노드에 대해 생성됩니다.

외부 PKI의 하위 CA로 Cisco ISE 루트 CA 구성

기본 PAN의 루트 CA가 외부 PKI의 하위 CA로 작동하도록 하려면 ISE 중간 CA 인증서 서명 요청을 생성하여 외부 CA로 보낸 다음 루트 및 CA 서명 인증서를 받습니다. 그런 다음 루트 CA 인증서는 신뢰할 수 있는 인증서 저장소로 가져오고 CA 서명 인증서는 CSR에 바인딩합니다. 이 경우 외부 CA는 루트 CA이고 기본 PAN은 외부 CA의 하위 CA이며 PSN은 기본 PAN의 하위 CA입니다.

단계 1 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

단계 2 **Generate Certificate Signing Requests (CSR)(CSR** 생성**)**를 클릭합니다.

단계 3 **Certificate(s) will be used for(**인증서 사용 대상**)** 드롭다운 목록에서 ISE Intermediate CA(ISE 중간 CA)를 선택합니다.

단계 4 **Generate(**생성**)**를 클릭합니다.

단계 5 CSR을 내보내 외부 CA로 보낸 다음 CA 서명 인증서를 받습니다.

단계 6 외부 CA의 루트 CA 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다.

단계 7 CA 서명 인증서를 CSR에 바인딩합니다.

다음에 수행할 작업

구축에 보조 PAN이 있는 경우 기본 PAN에서 Cisco ISE CA 인증서와 키의 백업을 가져온 다음 보조 PAN에서 복원합니다. 그러면 서버 및 루트 인증서가 보조 PAN에 자동으로 복제됩니다. 그러면 관리 노드 장애 시 보조 PAN이 외부 PKI의 하위 CA로 작동할 수 있습니다.

개인 디바이스 인증에 인증서를 사용하도록 Cisco ISE 구성

네트워크에 연결하는 엔드포인트(개인 디바이스)용 인증서를 발급하고 관리하도록 Cisco ISE를 구성할 수 있습니다. 내부 Cisco ISE CA 서비스를 사용하여 엔드포인트에서 CSR(Certificate Signing Request)에 서명을 하거나 CSR을 외부 CA에 전달할 수 있습니다.

시작하기 전에

- 기본 PAN에서 Cisco ISE CA 인증서와 키의 백업을 받아 재해 복구용으로 안전한 위치에 저장합니다.

단계 **1** 직원 사용자 그룹에 사용자 추가, 121 페이지

내부 ID 저장소 또는 Microsoft Active Directory 등의 외부 ID 저장소에 사용자를 추가할 수 있습니다.

단계 **2** TLS 기반 인증용 인증서 인증 프로파일 생성, 122 페이지

단계 **3** TLS 기반 인증용 인증서 ID 소스 시퀀스 생성, 122 페이지

단계 **4** 클라이언트 프로비저닝 정책을 생성합니다.

a) 인증 기관 설정 구성, 123 페이지
b) CA 템플릿 생성, 124 페이지
c) 클라이언트 프로비저닝 정책에서 사용할 기본 신청자 프로파일 생성, 126 페이지
d) Cisco 사이트에서 Windows 및 MAC OS X 운영체제용 에이전트 리소스 다운로드, 127 페이지
e) Apple iOS, Android 및 MACOSX 디바이스용 클라이언트 프로비저닝 정책 규칙 생성, 128 페이지

단계 **5** TLS 기반 인증용 Dot1X 인증 정책 규칙 구성, 128 페이지

단계 **6** TLS 기반 인증용 인증 정책 규칙을 구성합니다.

a) 중앙 웹 인증 및 신청자 프로비저닝 흐름용 권한 부여 프로파일 생성, 129 페이지
b) 권한 부여 정책 규칙 생성, 130 페이지

ECDHE-RSA 기반 인증서를 사용하는 경우 개인 디바이스에서 무선 SSID에 연결하는 동안 비밀번호를 다시 입력하라는 프롬프트가 표시됩니다.

직원 사용자 그룹에 사용자 추가

다음 절차에서는 Cisco ISE ID 저장소의 직원 사용자 그룹에 사용자를 추가하는 방법을 설명합니다. 외부 ID 저장소를 사용하는 경우에는 사용자를 추가할 수 있는 직원 사용자 그룹이 있는지 확인해 주십시오.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 사용자 세부정보를 입력합니다.

단계 **4** **Passwords(**비밀번호**)** 섹션에서 **Login Password(**로그인 비밀번호**)** 및 TACACS+ **Enable Password(**활성화 비밀번호**)**를 선택하여 네트워크 디바이스에 대한 액세스 레벨을 설정합니다.

단계 **5** 사용자 그룹 드롭다운 목록에서 Employee(직원)를 선택합니다.

직원 사용자 그룹에 속하는 모든 사용자는 동일한 권한 집합을 공유합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

TLS 기반 인증용 인증서 인증 프로파일 생성, 122 페이지

TLS 기반 인증용 인증서 인증 프로파일 생성

인증서를 사용하여 네트워크에 연결하는 엔드포인트를 인증하려면 Cisco ISE에서 인증서 인증 프로파일을 정의하거나 기본 프로파일인 Preloaded_Certificate_Profile을 편집해야 합니다. 인증서 인증 프로파일에는 보안 주체 사용자 이름으로 사용해야 하는 인증서 필드가 포함됩니다. 예를 들어 Common Name(일반 이름) 필드에 사용자 이름이 포함되어 있으면 보안 주체 사용자 이름이 주체 - 일반 이름인 인증서 인증 프로파일을 정의할 수 있으며 이 이름을 ID 저장소에 대해 확인할 수 있습니다.

단계 1 **Administration(관리)** > **Identity Management(ID 관리)** > **External Identity Sources(외부 ID 소스)** > **Certificate Authentication Profile(인증서 인증 프로파일)**을 선택합니다.

단계 2 인증서 인증 프로파일의 이름을 입력합니다. 예를 들어 CAP 등을 입력할 수 있습니다.

단계 3 주체 - 일반 이름을 **Principal Username X509 Attribute(보안 주체 사용자 이름 X509 속성)**로 선택합니다.

단계 4 **Save(저장)**를 클릭합니다.

다음에 수행할 작업

TLS 기반 인증용 인증서 ID 소스 시퀀스 생성, 122 페이지

TLS 기반 인증용 인증서 ID 소스 시퀀스 생성

인증서 인증 프로파일을 생성한 후에는 Cisco ISE가 인증서에서 속성을 가져온 다음 ID 소스 시퀀스에서 정의한 ID 소스와 해당 속성이 일치하는지를 확인할 수 있도록 ID 소스 시퀀스에 해당 프로파일을 추가해야 합니다.

시작하기 전에

다음 작업을 완료했는지 확인합니다.

- 직원 사용자 그룹에 사용자 추가
- 인증서 기반 인증용 인증서 인증 프로파일 생성

단계 1 **Administration(관리)** > **Identity Management(ID 관리)** > **Identity Source Sequences(ID 소스 시퀀스)**를 선택합니다.

단계 2 **Add(추가)**를 클릭합니다.

단계 3 ID 소스 시퀀스의 이름을 입력합니다. 예를 들어 Dot1X와 같이 입력할 수 있습니다.

단계 4 **Select Certificate Authentication Profile(인증서 인증 프로파일 선택)** 확인란을 선택하고 이전에 생성한 인증서 인증 프로파일(CAP)을 선택합니다.

단계 5 사용자 정보가 포함된 ID 소스를 인증 검색 목록 영역의 **Selected(선택됨)** 목록 상자로 이동합니다.

ID 소스를 더 추가할 수 있으며, 그러면 Cisco ISE는 일치하는 항목을 찾을 때까지 이러한 데이터 저장소를 순차적으로 검색합니다.

단계 **6** **Treat as if the user was not found and proceed to the next store in the sequence(**사용자를 찾지 못한 것으로 간주하여 다음 저장소로 순차 진행**)** 라디오 버튼을 클릭합니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

인증 기관 설정 구성, 123 페이지

인증 기관 설정 구성

외부 CA를 사용하여 CSR에 서명을 하려는 경우 외부 CA 설정을 구성해야 합니다. Cisco ISE의 이전 릴리스에서는 외부 CA 설정의 명칭이 SCEP RA 프로파일이었습니다. Cisco ISE CA를 사용하는 경우에는 CA 설정을 명시적으로 구성할 필요가 없습니다. Administration(관리) > System(시스템) > Certificates(인증서) > Internal CA Settings(내부 CA 설정)에서 내부 CA 설정을 검토할 수 있습니다.

사용자 디바이스가 수신한 검증된 인증서는 다음 표에서 설명하는 것처럼 디바이스에 상주하게 됩니다.

표 ***18:*** 디바이스 인증서 위치

디바이스	인증서 저장 위치	액세스 방법
iPhone/iPad	표준 인증서 저장소	Settings(설정) > General(일반) > Profile(프로파일)
Android	암호화된 인증서 저장소	최종 사용자에게 표시되지 않습니다. 참고 Settings(설정) > Location & Security(위치 및 보안) > Clear Storage(저장소 지우기)를 사용하면 인증서를 제거할 수 있습니다.
Windows	표준 인증서 저장소	**/cmd** 프롬프트에서 mmc.exe를 시작하거나 인증서 스냅인에서 확인합니다.
Mac	표준 인증서 저장소	Application(애플리케이션) > Utilities(유틸리티) > Keychain Access(키 체인 액세스)

시작하기 전에

외부 CA(Certificate Authority)를 사용하여 CSR(Certificate Signing Request)에 서명을 하려는 경우에는 외부 CA의 URL이 있어야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **External CA Settings(**외부 **CA** 설정**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 외부 CA 설정의 이름을 입력합니다. EXTERNAL_SCEP 등을 예로 들 수 있습니다.

단계 **4** URL 텍스트 상자에 외부 CA 서버 URL을 입력합니다.

Test Connection(연결 테스트**)**을 클릭하여 외부 CA에 연결할 수 있는지 확인합니다. 추가 CA 서버 URL을 입력하려면 + 버튼을 클릭합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

CA 템플릿 생성, 124 페이지

CA 템플릿 생성

인증서 템플릿은 내부 또는 외부 CA에 대해 사용해야 하는 SCEP RA 프로파일, 키 유형, 키 크기 또는 커브 유형,주체, SAN(Subject Alternative Name), 인증서의 유효 기간 및 확장 키 사용을 정의합니다. 이 예제에서는 내부 Cisco ISE CA를 사용한다고 가정합니다. 외부 CA 템플릿의 경우 유효 기간은 외부 CA에 의해 결정되며 지정할 수 없습니다.

새 CA 템플릿을 생성할 수도 있고 기본 인증서 템플릿인 EAP_Authentication_Certificate_Template을 편집할 수도 있습니다.

기본적으로 Cisco ISE에서는 다음 CA 템플릿을 사용할 수 있습니다.

- CA_SERVICE_Certificate_Template - ISE CA를 사용하는 기타 네트워크 서비스용입니다. 예를 들어 ASA VPN 사용자를 위한 인증서를 발급하도록 ISE를 구성하는 동안 이 인증서 템플릿을 사용합니다.
- EAP_Authentication_Certificate_Template - EAP 인증용입니다.
- pxGrid_Certificate_Template—Certificate Provisioning Portal(인증서 프로비저닝 포털)에서 인증서를 생성하는 동안 pxGrid 컨트롤러에 사용됩니다.

참고 ECC 키 유형을 사용하는 인증서 템플릿은 내부 Cisco ISE CA에서만 사용할 수 있습니다.

시작하기 전에

CA 설정을 구성했는지 확인합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **CA Service(CA** 서비스**)** > **Internal CA Certificate Template(**내부 **CA** 인증서 템플릿**)**을 선택합니다.

단계 **2** 내부 CA 템플릿의 이름을 입력합니다. 예를 들어 Internal_CA_Template과 같이 입력할 수 있습니다.

단계 **3** (선택 사항) Organizational Unit(조직 단위), Organization(조직), City(구/군/시), State(시/도) 및 Country(국가) 필드에 값을 입력합니다.

UTF-8 문자는 인증서 템플릿 필드(조직 단위, 조직, 구/군/시, 시/도 및 국가)에서 지원되지 않습니다. 인증서 템플릿에 UTF-8 문자를 사용하면 인증서 프로비저닝이 실패합니다.

인증서를 생성하는 내부 사용자의 사용자 이름이 인증서의 공용 이름으로 사용됩니다. Cisco ISE 내부 CA는 Common Name(공용 이름) 필드에서 "+" 또는 "*" 문자를 지원하지 않습니다. 사용자 이름에는 특수 문자 "+" 또는 "*"가 포함되어 있지 않아야 합니다.

단계 **4** 인증서의 유효 기간과 SAN(Subject Alternative Name)을 지정합니다.

단계 **5** 키 유형을 지정합니다. RSA 또는 ECC를 선택합니다.

다음 표에는 ECC를 지원하는 운영체제 및 버전과 지원되는 커브 유형이 나열되어 있습니다. 디바이스가 지원되는 운영체제를 실행하고 있지 않거나 지원되는 버전에서 실행되고 있지 않은 경우에는 RSA 기반 인증서를 대신 사용할 수 있습니다.

Operating System(운영체제**)**	지원되는 버전	지원되는 커브 유형
Windows	8 이상	P-256, P-384 및 P-521
Android	4.4 이상 참고 Android 6.0에서 ECC 인증서를 지원하려면 2016년 5월 패치가 필요합니다.	모든 커브 유형(Android 6.0은 P-192 커브 유형을 지원하지 않으므로 제외).

Windows 7 및 Apple iOS는 기본적으로 EAP-TLS 인증에 ECC를 지원하지 않습니다. Cisco ISE의 이 릴리스에서는 MAC OS X 디바이스에서 ECC 인증서 사용을 지원하지 않습니다.

네트워크의 디바이스가 지원되지 않는 운영체제(Windows 7, MAC OS X 또는 Apple iOS)를 실행하는 경우에는 키 유형으로 RSA를 선택하는 것이 좋습니다.

단계 **6** (RSA 키 유형을 선택하는 경우에 해당함) 키 크기를 지정합니다. 1024 이상의 키 크기를 선택해야 합니다.

단계 **7** (ECC 키 유형을 선택하는 경우에만 해당함) 커브 유형을 지정합니다. 기본 값은 P-384 입니다.

단계 **8** ISE Internal CA를 SCEP RA 프로파일로 선택합니다.

단계 **9** 유효 기간을 일 단위로 입력합니다. 기본값은 730일입니다. 유효 범위는 1~730입니다.

단계 **10** 확장 키 사용을 지정합니다. 클라이언트 인증에 인증서를 사용하려면 **Client Authentication(**클라이언트 인증**)** 확인란을 선택합니다. 서버 인증에 인증서를 사용하려면 **Server Authentication(**서버 인증**)** 확인란을 선택합니다.

단계 **11** **Submit(**제출**)**을 클릭합니다.

내부 CA 인증서 템플릿이 생성되어 클라이언트 프로비저닝 정책에 사용됩니다.

다음에 수행할 작업

클라이언트 프로비저닝 정책에서 사용할 기본 신청자 프로파일 생성, 126 페이지

내부 CA 설정

다음 표에서는 내부 CA 설정 창의 필드에 대해 설명합니다. 이 창에서 내부 CA 설정을 확인하고 내부 CA 서비스를 비활성화할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Internal CA Settings(**내부 **CA** 설정**)**입니다.

표 *19:* 내부 *CA* 설정

필드 이름	사용 지침
Disable Certificate Authority(인증 기관 비활성화**)**	내부 CA 서비스를 비활성화하려면 이 버튼을 클릭합니다.
Host Name(호스트 이름**)**	CA 서비스를 실행 중인 Cisco ISE 노드의 호스트 이름입니다.
Personas(역할 분담**)**	CA 서비스를 실행 중인 노드에서 활성화된 Cisco ISE 노드 페르소나입니다. Administration(관리), Policy Service(정책 서비스) 등을 예로 들 수 있습니다.
Role(s)(역할**)**	CA 서비스를 실행 중인 Cisco ISE 노드에 지정된 역할입니다. Standalone(독립형), Primary(기본), Secondary(보조) 등을 예로 들 수 있습니다.
CA, EST & OCSP Responder Status(CA, EST 및 **OCSP** 응답기 상태**)**	Enabled(활성화됨) 또는 Disabled(비활성화됨)입니다.
OCSP Responder URL(OCSP 응답기 **URL)**	OCSP 서버에 액세스하는 Cisco ISE 노드의 URL입니다.
SCEP URL	SCEP 서버에 액세스하는 Cisco ISE 노드의 URL입니다.

관련 항목

Cisco ISE CA 서비스, 103 페이지
개인 디바이스 인증에 인증서를 사용하도록 Cisco ISE 구성, 120 페이지

클라이언트 프로비저닝 정책에서 사용할 기본 신청자 프로파일 생성

사용자가 회사 네트워크에서 개인 디바이스를 사용할 수 있도록 기본 신청자 프로파일을 생성할 수 있습니다. Cisco ISE는 각 운영체제에 대해 서로 다른 정책 규칙을 사용합니다. 각 클라이언트 프로비

저닝 정책 규칙에는 기본 신청자 프로파일이 포함되어 있으며, 이 프로파일은 각 운영체제에 대해 사용할 프로비저닝 마법사를 지정합니다.

시작하기 전에

- Cisco ISE에서 CA 인증서 템플릿을 구성합니다.
- TCP 포트 8905 및 UDP 포트 8905를 열어 클라이언트 에이전트 및 supplicant 프로비저닝 마법사 설치를 활성화합니다. 포트 사용에 대한 자세한 내용은 *Cisco Identity Services Engine* 하드웨어 설치 설명서에서 "Cisco ISE 어플라이언스 포트 참조" 부록을 참고하십시오.

단계 **1** **Policy**(정책) > **Policy Elements**(정책 요소) > **Results**(결과) > **Client Provisioning**(클라이언트 프로비저닝) > **Resources**(리소스)를 선택합니다.

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

단계 **3** 기본 신청자 프로파일의 이름을 입력합니다. 예를 들어 EAP_TLS_INTERNAL과 같이 입력할 수 있습니다.

단계 **4** **Operating System**(운영체제) 드롭다운 목록에서 ALL(모두)을 선택합니다.

참고 MAC OS 버전 10.10 사용자는 듀얼 SSID PEAP 플로우용으로 프로비저닝된 SSID에 수동으로 연결해야 합니다.

단계 **5** **Wired**(유선) 또는 **Wireless**(무선) 확인란을 선택합니다.

단계 **6** **Allowed Protocol**(허용되는 프로토콜) 드롭다운 목록에서 TLS를 선택합니다.

단계 **7** 앞에서 생성한 CA 인증서 템플릿을 선택합니다.

단계 **8** **Submit**(제출)을 클릭합니다.

다음에 수행할 작업

Cisco 사이트에서 Windows 및 MAC OS X 운영체제용 에이전트 리소스 다운로드, 127 페이지

Cisco 사이트에서 Windows 및 MAC OS X 운영체제용 에이전트 리소스 다운로드

Windows 및 MAC OS X 운영체제의 경우에는 Cisco 사이트에서 원격 리소스를 다운로드해야 합니다.

시작하기 전에

네트워크의 프록시 설정이 올바르게 구성되어 있는지 확인하여 Cisco ISE에 클라이언트 프로비저닝 리소스를 다운로드하기 위한 적절한 원격 위치에 액세스할 수 있는지 확인합니다.

단계 **1** **Policy**(정책) > **Policy Elements**(정책 요소) > **Resources**(리소스) > **Client Provisioning**(클라이언트 프로비저닝) > **Resources**(리소스)를 선택합니다.

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

단계 **3** **Windows** 및 **MAC OS X** 패키지 옆의 확인란을 선택합니다. 최신 버전을 포함해야 합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

Apple iOS, Android 및 MACOSX 디바이스용 클라이언트 프로비저닝 정책 규칙 생성, 128 페이지

Apple iOS, Android 및 MACOSX 디바이스용 클라이언트 프로비저닝 정책 규칙 생성

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

에이전트 규정 준수 모듈을 다운로드할 때는 항상 시스템에서 사용 가능한 기존 모듈(있는 경우)을 덮어씁니다.

직원이 iOS, Android 및 MACOSX 디바이스를 사용할 수 있도록 하려면 클라이언트 프로비저닝 정책 페이지에서 이러한 각 디바이스에 대해 정책 규칙을 생성해야 합니다.

시작하기 전에

클라이언트 프로비저닝 정책 페이지에서 필수 기본 신청자 프로파일을 구성하고 필수 에이전트를 다운로드해야 합니다.

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

단계 **2** Apple iOS, Android 및 MACOSX 디바이스용 클라이언트 프로비저닝 정책 규칙을 생성합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

TLS 기반 인증용 Dot1X 인증 정책 규칙 구성, 128 페이지

TLS 기반 인증용 Dot1X 인증 정책 규칙 구성

이 작업에서는 TLS 기반 인증에 대해 Dot1X 인증 정책 규칙을 업데이트하는 방법을 보여줍니다.

시작하기 전에

TLS 기반 인증용으로 인증서 인증 프로파일을 생성했는지 확인합니다.

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

단계 **2** **View(**보기**)** 열에서 화살표 › 아이콘을 클릭하여 Set view(보기 설정) 화면을 열어 인증 정책을 보고, 관리하고, 업데이트합니다.

기본 규칙 기반 인증 정책에는 Dot1X 인증용 규칙이 포함되어 있습니다.

단계 **3** Dot1X 인증 정책 규칙의 조건을 편집하려면 **Conditions(**조건**)** 열의 셀 위에 마우스를 올려놓고 아이콘을 클릭합니다. Condition Studio가 열립니다.

단계 **4** Dot1X 정책 규칙의 **Actions(**작업**)** 열에서 톱니바퀴 아이콘을 클릭한 다음, 드롭다운 메뉴에서 필요에 따라 Insert(삽입) 또는 Duplicate(중복) 옵션을 선택하여 새 정책 집합을 삽입합니다.
정책 집합 표에 새 행이 표시됩니다.

단계 **5** 규칙의 이름을 입력합니다. 예를 들어 eap-tls와 같이 입력할 수 있습니다.

단계 **6** **Conditions(**조건**)** 열에서 (+) 기호를 클릭합니다.

단계 **7** **Conditions Studio** 페이지에 필수 조건을 생성합니다. **Editor(**편집기**)** 섹션에서 **Click To Add an Attribute(**클릭하여 속성 추가**)** 텍스트 상자를 클릭하고 필요한 사전 및 속성(예: Network Access:UserName Equals User1)을 선택합니다.

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

단계 **8** **Use**를 클릭합니다.

단계 **9** 기본 규칙은 그대로 유지합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

중앙 웹 인증 및 신청자 프로비저닝 흐름용 권한 부여 프로파일 생성, 129 페이지

중앙 웹 인증 및 신청자 프로비저닝 흐름용 권한 부여 프로파일 생성

인증서 기반 인증이 성공한 후 사용자에게 부여해야 하는 액세스 권한을 결정하려면 권한 부여 프로파일을 정의해야 합니다.

시작하기 전에

WLC(Wireless LAN Controller)에서 필요한 ACL(Access Control Lists)을 구성했는지 확인합니다. WLC에서 ACL을 생성하는 방법에 대한 자세한 내용은 *TrustSec* 사용 방법 설명서*:* 구별된 액세스를 위해 인증서 사용을 참고해 주십시오.

이 예제에서는 WLC에서 다음 ACL을 생성했다고 가정합니다.

- NSP-ACL - 기본 신청자 프로비저닝용
- BLACKHOLE - 차단 목록에 포함된 디바이스에 대한 액세스 제한용
- NSP-ACL-Google - Android 디바이스 프로비저닝용

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

단계 **2** **Add(**추가**)**를 클릭하여 새 권한 부여 프로파일을 생성합니다.

단계 **3** 권한 부여 프로파일의 이름을 입력합니다.

단계 **4** **Access Type(**액세스 유형**)** 드롭다운 목록에서 ACCESS_ACCEPT를 선택합니다.

단계 **5** **Add(**추가**)**를 클릭하여 중앙 웹 인증용 권한 부여 프로파일, Google Play용 중앙 웹 인증, 기본 신청자 프로비저닝 및 Google용 기본 신청자 프로비저닝을 추가합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

권한 부여 정책 규칙 생성, 130 페이지

권한 부여 정책 규칙 생성

Cisco ISE는 권한 부여 정책 규칙을 평가하여 정책 규칙에 지정된 권한 부여 프로파일을 기준으로 사용자에게 네트워크 리소스 액세스 권한을 부여합니다.

시작하기 전에

필요한 권한 부여 프로파일을 생성했는지 확인합니다.

단계 **1** **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택하고 정책 집합을 확장하여 권한 부여 정책 규칙을 확인합니다.

단계 **2** 기본 규칙 위에 추가 정책 규칙을 삽입합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

CA 서비스 정책 참조

이 섹션에서는 Cisco ISE CA 서비스를 활성화하기 전에 먼저 생성해야 하는 권한 부여 및 클라이언트 프로비저닝 정책 규칙에 대한 참조 정보를 제공합니다.

인증서 서비스용 클라이언트 프로비저닝 정책 규칙

이 섹션에는 Cisco ISE 인증서 서비스를 사용하는 동안 생성해야 하는 클라이언트 프로비저닝 정책 규칙이 나와 있습니다. 다음 표에는 세부정보가 나와 있습니다.

규칙 이름	**ID** 그룹	운영체제	기타 조건	결과
iOS	모든	모든 Apple iOS	조건	EAP_TLS_INTERNAL(이전에 생성한 기본 신청자 프로파일). 외부 CA를 사용하는 경우 외부 CA에 대해 생성한 기본 신청자 프로파일을 선택합니다.

규칙 이름	ID 그룹	운영체제	기타 조건	결과
Android	모든	Android	조건	EAP_TLS_INTERNAL(이전에 생성한 기본 신청자 프로파일). 외부 CA를 사용하는 경우 외부 CA에 대해 생성한 기본 신청자 프로파일을 선택합니다.
MACOSX	모든	MACOSX	조건	Native Supplicant Configuration(기본 신청자 컨피그레이션)에서 다음을 지정합니다. 1. Config Wizard(컨피그레이션 마법사): Cisco 사이트에서 다운로드한 MACOSX 신청자 마법사를 선택합니다. 2. Wizard Profile(마법사 프로파일): 이전에 생성한 EAP_TLS_INTERNAL 기본 신청자 프로파일을 선택합니다. 외부 CA를 사용하는 경우 외부 CA에 대해 생성한 기본 신청자 프로파일을 선택합니다.

인증서 서비스용 권한 부여 프로파일

이 섹션에는 Cisco ISE에서 인증서 기반 인증을 활성화하기 위해 생성해야 하는 권한 부여 프로파일이 나와 있습니다. WLC(Wireless LAN Controller)에서 이미 ACL(NSP-ACL 및 NSP-ACL-Google)을 생성한 상태여야 합니다.

- CWA - 이 프로파일은 중앙 웹 인증 흐름을 진행하는 디바이스에 사용됩니다. **Web Authentication(**웹 인증**)** 확인란을 선택하고 드롭다운 목록에서 Centralized(중앙 집중식)를 선택하고 ACL 텍스트 상자에 NSP-ACL을 입력합니다.
- CWA_GooglePlay - 이 프로파일은 중앙 웹 인증 흐름을 진행하는 디바이스에 사용됩니다. 이 프로파일은 Android 디바이스가 Google Play 스토어에 액세스하고 Cisco Network Setup Assistant를 다운로드하도록 합니다. **Web Authentication(**웹 인증**)** 확인란을 선택하고 드롭다운 목록에서 Centralized(중앙 집중식)를 선택하고 ACL-Google 텍스트 상자에 NSP-ACL을 입력합니다.
- NSP - 이 프로파일은 신청자 프로비저닝 흐름을 진행하는, Android 이외의 디바이스에 사용됩니다. **Web Authentication(**웹 인증**)** 확인란을 선택하고 드롭다운 목록에서 Supplicant Provisioning(신청자 프로비저닝)을 선택하고 ACL 텍스트 상자에 NSP-ACL을 입력합니다.
- NSP-Google - 이 프로파일은 신청자 프로비저닝 흐름을 진행하는, Android 이외의 디바이스에 사용됩니다. **Web Authentication(**웹 인증**)** 확인란을 선택하고 드롭다운 목록에서 Supplicant Provisioning(신청자 프로비저닝)을 선택하고 ACL 텍스트 상자에 NSP-ACL-Google을 입력합니다.

기본 Blackhole_Wireless_Access 권한 부여 프로파일을 검토합니다. 필수적인 고급 속성 설정은 다음과 같습니다.

- Cisco:cisco-av-pair = url-redirect=https://*ip*:*port*/blockedlistportal/gateway?portal=*PortalID*
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

인증서 서비스용 권한 부여 정책 규칙

이 섹션에는 Cisco ISE CA 서비스를 활성화하는 동안 생성해야 하는 권한 부여 정책 규칙이 나와 있습니다.

- 기업 자산 - 이 규칙은 802.1X 및 MSCHAPV2 프로토콜을 사용하여 회사 무선 SSID에 연결되는 회사 디바이스에 사용됩니다.
- Android_SingleSSID - 이 규칙은 Google Play 스토어에 액세스하여 프로비저닝용 Cisco Network Setup Assistant를 다운로드하는 Android 디바이스에 사용됩니다. 이 규칙은 단일 SSID 설정과 관련이 있습니다.
- Android_DualSSID - 이 규칙은 Google Play 스토어에 액세스하여 프로비저닝용 Cisco Network Setup Assistant를 다운로드하는 Android 디바이스에 사용됩니다. 이 규칙은 이중 SSID 설정과 관련이 있습니다.
- CWA - 이 규칙은 중앙 웹 인증 흐름을 진행하는 디바이스에 사용됩니다.
- NSP - 이 규칙은 EAP-TLS 인증에 인증서를 사용하여 기본 신청자 프로비저닝 흐름을 진행하는 디바이스에 사용됩니다.
- EAP-TLS - 이 규칙은 신청자 프로비저닝 흐름을 완료하고 인증서로 프로비저닝된 디바이스에 사용됩니다. 네트워크에 대한 액세스가 부여됩니다.

다음 표에는 Cisco ISE CA 서비스에 대한 권한 부여 정책 규칙을 구성하면서 선택해야 하는 속성 및 값이 나와 있습니다. 이 예에서는 Cisco ISE에서 해당 권한 부여 프로파일을 구성했다고 가정합니다.

규칙 이름	조건	권한(적용될 권한 부여 프로파일)
기업 자산	Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	PermitAccess
Android_SingleSSID	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	NSP_Google
Android_DualSSID	(Wireless_MAB AND Session:Device-OS EQUALS Android)	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	NSP
EAP-TLS	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI	PermitAccess

ASA VPN 사용자에 대한 ISE CA의 인증서 발급

ISE CA는 ASA VPN을 통해 연결하는 클라이언트 머신에 인증서를 발급합니다. 이 기능을 사용하면 ASA VPN을 통해 연결하는 엔드 디바이스에 인증서를 자동으로 프로비저닝할 수 있습니다.

Cisco ISE는 인증서를 클라이언트 머신에 등록하고 프로비저닝하기 위해 SCEP(Simple Certificate Enrollment Protocol)를 사용합니다. AnyConnect 클라이언트는 HTTPS 연결을 통해 ASA에 SCEP 요청을 보냅니다. ASA는 Cisco ISE와 ASA 간에 설정된 HTTP 연결을 통해 Cisco ISE로 요청을 릴레이하기 전에 요청을 평가하고 정책을 시행합니다. Cisco ISE CA의 응답은 클라이언트로 다시 릴레이됩니다. ASA는 SCEP 메시지의 내용을 읽을 수 없으며 Cisco ISE CA에 대한 프록시로 작동합니다. Cisco ISE CA는 클라이언트에서 SCEP 메시지를 암호 해독하고 응답을 암호화된 형식으로 보냅니다.

ISE CA SCEP URL은 http://<*ISE CA* 서버의 *IP* 주소 또는 *FQDN*>:9090/auth/caservice/pkiclient.exe입니다. ISE 노드의 FQDN을 사용하는 경우 ASA에 연결된 DNS 서버가 FQDN을 확인할 수 있어야 합니다.

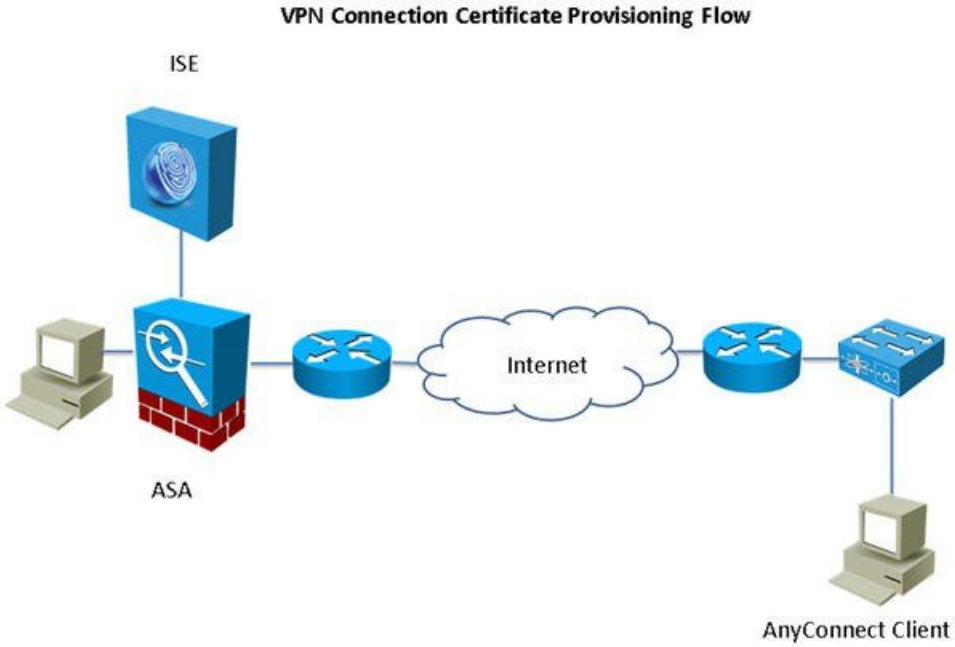
AnyConnect 클라이언트 프로파일에서 만료 전에 인증서 갱신을 구성할 수 있습니다. 인증서가 이미 만료된 경우 갱신 플로우는 새 등록과 비슷합니다.

지원되는 버전은 다음과 같습니다.

- 소프트웨어 버전 8.x를 실행하는 Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco AnyConnect VPN 버전 2.4 이상

VPN 연결 인증서 프로비저닝 플로우

그림 *9: ASA VPN* 사용자를 위한 인증서 프로비저닝



1. 사용자가 VPN 연결을 시작합니다.
2. AnyConnect 클라이언트는 클라이언트 머신을 스캔하고 고유한 디바이스 식별자(예: IMEI)와 같은 속성을 ASA에 전송합니다.
3. ASA는 클라이언트에서 인증서 기반 인증을 요청합니다. 인증서가 없으므로 인증에서 장애가 발생합니다.
4. ASA는 계속해서 사용자 이름/비밀번호를 사용하여 기본 사용자 인증(AAA)을 진행하고 정보를 인증 서버(ISE)에 전달합니다.
    1. 인증에서 장애가 발생하면 연결이 즉시 종료됩니다.
    2. 인증에 통과하면 제한적 액세스 권한이 부여됩니다. aaa.cisco.sceprequired 속성을 사용하여 인증서를 요청하는 클라이언트 머신에 대해 DAP(Dynamic Access Policy)를 구성할 수 있습니다. 이 속성의 값을 "true"로 설정하고 ACL 및 웹 ACL을 적용할 수 있습니다.
5. 관련 정책과 ACL이 적용된 후 VPN 연결이 설정됩니다. AAA 인증이 성공하고 VPN 연결이 설정되어야 클라이언트가 SCEP용 키 생성을 시작합니다.
6. 클라이언트가 SCEP 등록을 시작하고 HTTP를 통해 SCEP 요청을 ASA로 보냅니다.
7. ASA는 요청의 세션 정보를 조회하여 세션 등록이 허용되면 요청을 ISE CA로 릴레이합니다.
8. ASA가 ISE CA의 응답을 클라이언트로 다시 릴레이합니다.

9. 등록에 성공하면 클라이언트는 구성 가능한 메시지를 사용자에게 제공하고 VPN 세션과의 연결을 끊습니다.
10. 사용자는 인증서를 사용하여 다시 인증할 수 있으며, 그러면 정상 VPN 연결이 설정됩니다.

ASA VPN 사용자에게 인증서를 발급하도록 Cisco ISE CA 구성

ASA VPN 사용자에게 인증서를 프로비저닝하려면 Cisco ISE 및 ASA에서 다음 컨피그레이션을 수행해야 합니다.

시작하기 전에

- Cisco ISE 내부 또는 외부 ID 소스에 VPN 사용자 계정이 있는지 확인합니다.
- ASA 및 Cisco ISE 정책 서비스 노드가 동일한 NTP 서버를 사용하여 동기화되는지 확인합니다.

단계 **1** Cisco ISE에서 ASA를 네트워크 액세스 디바이스로 정의합니다. ASA를 네트워크 디바이스로 추가하는 방법에 대한 자세한 내용은 Cisco ISE에서 네트워크 디바이스 추가, 135 페이지을 참고하십시오.

단계 **2** ASA에서 그룹 정책 구성, 136 페이지.

단계 **3** SCEP 등록용 AnyConnect 연결 프로파일 구성, 136 페이지.

단계 **4** ASDM에서 VPN 클라이언트 프로파일 구성, 137 페이지.

단계 **5** ASA로 Cisco ISE CA 인증서 가져오기.

Cisco ISE에서 네트워크 디바이스 추가

Cisco ISE에서 네트워크 디바이스를 추가하거나 기본 네트워크 디바이스를 사용할 수 있습니다.

Network Devices(네트워크 디바이스)(**Work Centers**(작업 센터) > **Device Administration**(디바이스 관리) > **Network Resources**(네트워크 리소스) > **Network Devices**(네트워크 디바이스)) 창에서 네트워크 디바이스를 추가할 수도 있습니다.

시작하기 전에

추가할 네트워크 디바이스에서 AAA 기능을 활성화해야 합니다. 릴리스에 대한 *Cisco ISE* 관리자 가이드의 "통합" 장에서 "AAA 기능을 활성화하는 명령" 섹션을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration**(관리) > **Network Resources**(네트워크 리소스) > **Network Devices**(네트워크 디바이스)를 선택합니다.

단계 **2** **Add**(추가)를 클릭합니다.

단계 **3** **Name**(이름), **Description**(설명) 및 **IP Address**(IP 주소) 필드에 해당 값을 입력합니다.

단계 **4** 드롭다운 목록에서 **Device Profile**(디바이스 프로파일), **Model Name**(모델 이름), **Software Version**(소프트웨어 버전) 및 **Network Device Group**(네트워크 디바이스 그룹) 필드에 필요한 값을 선택합니다.

단계 **5** (선택 사항) 인증용 RADIUS 프로토콜을 구성하려면 **RADIUS Authentication Settings(RADIUS** 인증 설정**)** 확인란을 선택합니다.

단계 **6** (선택 사항) 인증용 TACACS 프로토콜을 구성하려면 **TACACS Authentication Settings(TACACS** 인증 설정**)** 확인란을 선택합니다.

단계 **7** (선택 사항) 네트워크 디바이스에서 정보를 수집하기 위해 Cisco ISE 프로파일링 서비스용으로 SNMP를 구성하려면 **SNMP Settings(SNMP** 설정**)** 확인란을 선택합니다.

단계 **8** (선택 사항) Cisco TrustSec이 활성화된 디바이스를 구성하려면 **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)** 확인란을 선택합니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

ASA에서 그룹 정책 구성

AnyConnect가 SCEP 등록 요청을 전달하도록 할 ISE CA URL을 정의하려면 ASA에서 그룹 정책을 구성합니다.

단계 **1** Cisco ASA ASDM에 로그인합니다.

단계 **2** 좌측의 Remote Access VPN(원격 액세스 VPN) 탐색창에서 **Group Policies(**그룹 정책**)**를 클릭합니다.

단계 **3** 그룹 정책을 생성하려면 **Add(**추가**)**를 클릭합니다.

단계 **4** 그룹 정책의 이름을 입력합니다. ISE_CA_SCEP를 예로 들 수 있습니다.

단계 **5** SCEP forwarding URL(SCEP 전달 URL) 필드에서 **Inherit(**상속**)** 확인란 선택을 취소하고 포트 번호와 함께 ISE SCEP URL을 입력합니다.

ISE 노드의 FQDN을 사용하는 경우 ASA에 연결된 DNS 서버가 ISE 노드의 FQDN을 확인할 수 있어야 합니다.

예제**:**

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe

단계 **6** 그룹 정책을 저장하려면 **OK(**확인**)**를 클릭합니다.

SCEP 등록용 **AnyConnect** 연결 프로파일 구성

ISE CA 서버, 인증 방법 및 ISE CA SCEP URL을 지정하려면 ASA에서 AnyConnect 연결 프로파일을 구성합니다.

단계 **1** Cisco ASA ASDM에 로그인합니다.

단계 **2** 좌측의 Remote Access VPN(원격 액세스 VPN) 탐색창에서 **AnyConnect Connection Profiles(AnyConnect** 연결 프로파일**)**를 클릭합니다.

단계 **3** 연결 프로파일을 생성하려면 **Add(**추가**)**를 클릭합니다.

단계 **4** 연결 프로파일의 이름을 입력합니다. 예를 들어 Get-Group과 같이 입력합니다.

단계 **5** (선택 사항) Aliases(별칭) 필드에 연결 프로파일의 설명을 입력합니다. 예를 들어 SCEP-Call-ASA와 같이 입력합니다.

단계 **6** Authentication(인증) 영역에서 다음을 지정합니다.

- Method(방법) - **Both(**둘 다**)** 라디오 버튼을 클릭합니다.
- AAA Server Group(AAA 서버 그룹) - **Manage(**관리**)**를 클릭하고 ISE 서버를 선택합니다.

단계 **7** Client Address Assignment(클라이언트 주소 할당) 영역에서, 사용할 DHCP 서버 및 클라이언트 주소 풀을 선택합니다.

단계 **8** Default Group Policy(기본 그룹 정책) 영역에서 **Manage(**관리**)**를 클릭하고 ISE SCEP URL 및 포트 번호로 생성한 그룹 정책을 선택합니다.

예제**:**

ISE_CA_SCEP를 예로 들 수 있습니다.

단계 **9** **Advanced(**고급**)** > **General(**일반**)**을 선택하고 이 연결 프로파일에 대해 **Enable Simple Certificate Enrollment Protocol(Simple Certificate Enrollment Protocol** 활성화**)** 확인란을 선택합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.
AnyConnect 연결 프로파일이 생성되었습니다.

다음에 수행할 작업

ASDM에서 VPN 클라이언트 프로파일 구성

SCEP 등록을 위해 AnyConnect에서 VPN 클라이언트 프로파일을 구성합니다.

단계 **1** Cisco ASA ASDM에 로그인합니다.

단계 **2** 좌측의 Remote Access VPN(원격 액세스 VPN) 탐색창에서 **AnyConnect Client Profile(AnyConnect** 클라이언트 프로파일**)**을 클릭합니다.

단계 **3** 사용할 클라이언트 프로파일을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** 좌측의 Profile(프로파일) 탐색창에서 **Certificate Enrollment(**인증서 등록**)**를 클릭합니다.

단계 **5** **Certificate Enrollment(**인증서 등록**)** 확인란을 선택합니다.

단계 **6** 다음 필드에 값을 입력합니다.

- Certificate Expiration Threshold(인증서 만료 임계값) - AnyConnect에서 사용자에게 인증서가 만료될 예정임을 경고하는 인증서 만료 전 남은 날짜 수입니다(SCEP가 활성화되어 있으면 지원되지 않음). 기본값은 영(0)(표시된 경고 없음)입니다. 값의 범위는 영(0)부터 180일까지입니다.
- Automatic SCEP Host(자동 SCEP 호스트) - SCEP 인증서 검색이 구성되어 있는 ASA의 호스트 이름과 연결 프로파일(터널 그룹)을 입력합니다. ASA의 FQDN(Fully Qualified Domain Name, 정규화된 도메인 이름) 또는 연결 프로파일 이름을 입력합니다. 예를 들어 호스트 이름인 asa.cisco.com과 연결 프로파일 이름인 Cert_Group을 입력합니다.
- CA URL - SCEP CA 서버를 식별합니다. ISE 서버의 FQDN 또는 IP 주소를 입력합니다. 예를 들어 http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe와 같이 입력합니다.

단계 **7** 클라이언트가 인증서의 콘텐츠를 요청하는 방법을 정의하는 Certificate Contents(인증서 콘텐츠)의 값을 입력합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.
AnyConnect 클라이언트 프로파일이 생성되었습니다. 자세한 내용은 해당 AnyConnect 버전의 Cisco AnyConnect Secure Mobility 클라이언트를 참고하십시오.

ASA로 **Cisco ISE CA** 인증서 가져오기

Cisco ISE 내부 CA 인증서를 ASA로 가져옵니다.

시작하기 전에

Cisco ISE 내부 CA 인증서를 내보냅니다. **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Authority Certificates(**인증 기관 인증서**)**를 선택합니다. **Certificate Services Node CA(**인증서 서비스 노드 **CA)** 및 **Certificate Services Root CA(**인증서 서비스 루트 **CA)** 인증서 옆의 확인란을 선택하여 해당 인증서를 한 번에 하나씩 내보냅니다.

단계 **1** Cisco ASA ASDM에 로그인합니다.

단계 **2** 왼쪽의 Remote Access VPN(원격 액세스 VPN) 탐색창에서 **Certificate Management(**인증서 관리**)** > **CA Certificates(CA** 인증서**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭한 다음 Cisco ISE 내부 CA 인증서를 선택하여 ASA로 가져옵니다.

엔드포인트 인증서 취소

직원의 개인 디바이스로 발급된 인증서를 취소해야 하는 경우 엔드포인트 인증서 페이지에서 해당 인증서를 취소할 수 있습니다. 예를 들어 직원 디바이스가 도난당하거나 분실된 경우 Cisco ISE 관리 포털에 로그인한 다음 엔드포인트 인증서 페이지에서 해당 디바이스에 발급된 인증서를 취소할 수 있습니다. 식별 이름, 디바이스 고유 ID 또는 일련 번호를 기준으로 이 페이지에서 데이터를 필터링할 수 있습니다.

PSN(하위 CA)이 노출된 경우에는 엔드포인트 인증서 페이지에서 Issued By(발급자) 필드를 기준으로 필터링하여 해당 PSN에서 발급한 모든 인증서를 취소할 수 있습니다.

직원에게 발급된 인증서를 취소할 때 해당 인증서를 사용하여 인증된 활성화된 세션이 있으면 해당 세션이 즉시 종료됩니다. 인증서를 취소하면 권한이 부여되지 않은 사용자가 인증서 취소 즉시 리소스에 액세스할 수 없게 됩니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Issued Certificates(**발급된 인증서**)**를 선택합니다.

단계 **2** 취소할 엔드포인트 인증서 옆의 확인란을 선택하고 **Revoke(**취소**)**를 클릭합니다.
식별 이름 및 디바이스 유형을 기준으로 인증서를 검색할 수 있습니다.

단계 **3** 인증서 취소 사유를 입력합니다.

단계 **4** **Yes(**예**)**를 클릭합니다.

OCSP 서비스

OCSP(Online Certificate Status Protocol)는 x.509 디지털 인증서의 상태를 확인하는 데 사용되는 프로토콜입니다. CRL(Certificate Revocation List) 대신 사용 가능한 이 프로토콜은 CRL 처리로 인해 발생하는 문제를 해결합니다.

Cisco ISE에는 HTTP를 통해 OCSP 서버와 통신하여 인증에서 인증서의 상태를 검증하는 기능이 있습니다. Cisco ISE에 구성되어 있는 모든 CA(Certificate Authority) 인증서에서 참조할 수 있는 재사용 가능한 컨피그레이션 객체에서 OCSP 컨피그레이션을 구성합니다.

CA별로 CRL 및/또는 OCSP 확인을 구성할 수 있습니다. CRL과 OCSP를 모두 선택하면 Cisco ISE는 OCSP를 통해 먼저 확인을 수행합니다. 기본 및 보조 OCSP 서버에서 모두 통신 문제가 탐지되거나 지정된 인증서에 대해 알 수 없는 상태가 반환되면 Cisco ISE는 CRL을 확인하도록 전환됩니다.

Cisco ISE CA Service Online Certificate Status Protocol 응답자

Cisco ISE CA OCSP 응답자는 OCSP 클라이언트와 통신하는 서버입니다. Cisco ISE CA용 OCSP 클라이언트에는 내부 Cisco ISE OCSP 클라이언트 및 ASA(Adaptive Security Appliance)의 OCSP 클라이언트가 있습니다. OCSP 클라이언트는 RFC 2560, 5019에 정의된 OCSP 요청/응답 구조를 사용하여 OCSP 응답자와 통신해야 합니다.

Cisco ISE CA는 OCSP 응답자에 인증서를 발급합니다. OCSP 응답자는 포트 2560에서 모든 들어오는 요청을 수신 대기합니다. 이 포트는 OCSP 트래픽만 허용하도록 구성되어 있습니다.

OCSP 응답자는 RFC 2560, 5019에 정의된 구조를 따르는 요청을 수락합니다. OCSP 요청에서는 Nonce 확장이 지원됩니다. OCSP 응답자는 인증서 상태를 확보하여 OCSP 응답을 생성하고 서명합니다. 최대 기간인 24시간 동안 클라이언트에서 OCSP 응답을 캐시할 수 있지만 OCSP 응답자에서 OCSP 응답은 캐시되지 않습니다. OCSP 클라이언트는 OCSP 응답의 서명을 검증해야 합니다.

PAN의 셀프 서명된 CA 인증서(또는 ISE가 외부 CA의 중간 CA로 작동하는 경우 중간 CA 인증서)는 OCSP 응답자 인증서를 발급합니다. PAN의 이 CA 인증서는 PAN 및 PSN에서 OCSP 인증서를 발급합니다. 이 셀프 서명된 CA 인증서는 전체 구축의 루트 인증서이기도 합니다. 구축 전체의 모든 OCSP 인증서는 이러한 인증서를 사용하여 서명된 응답을 검증하기 위해 ISE의 신뢰할 수 있는 인증서 저장소에 배치됩니다.

OCSP 인증서 상태 값

OCSP 서비스는 지정된 인증서 요청에 대해 다음 값을 반환합니다.

- 정상 - 상태 질의에 대한 긍정적 응답을 나타냅니다. 이는 인증서가 취소되지 않았으며 상태가 다음 시간 간격(Time to Live) 값까지만 정상이라는 것을 의미합니다.
- 취소됨 - 인증서가 취소되었습니다.

- 알 수 없음 - 인증서 상태를 알 수 없습니다. 이 OCSP 응답자의 CA에 의해 인증서가 발급되지 않은 경우 OCSP 서비스에서 이 값을 반환합니다.
- 오류 - OCSP 요청에 대한 응답이 수신되지 않았습니다.

OCSP 고가용성

Cisco ISE는 CA당 최대 2대의 OCSP 서버를 구성할 수 있으며, 이러한 서버를 각각 기본 및 보조 OCSP 서버라고 합니다. 각 OCSP 서버 컨피그레이션에는 다음 매개변수가 포함됩니다.

- URL - OCSP 서버 URL입니다.
- Nonce - 요청에서 전송되는 난수입니다. 이 옵션을 사용하는 경우 재생 공격에서 이전 통신을 사용할 수 없습니다.
- Validate response - Cisco ISE는 OCSP 서버에서 수신되는 응답 서명을 검증합니다.

Cisco ISE는 기본 OCSP 서버와 통신할 때 시간 초과(5초)이 발생하면 보조 OCSP 서버로 전환합니다.

Cisco ISE는 구성 가능한 시간 동안 보조 OCSP 서버를 사용한 후 기본 서버 사용을 다시 시도합니다.

OCSP 실패

3가지 일반 OCSP 실패 시나리오는 다음과 같습니다.

- 실패한 OCSP 캐시 또는 OCSP 클라이언트 측(Cisco ISE) 장애
- 실패한 OCSP 응답자 시나리오. 예를 들어 다음과 같습니다.

  첫 번째 기본 OCSP 응답자가 응답하지 않고 보조 OCSP 응답자가 Cisco ISE OCSP 요청에 응답함

  Cisco ISE OCSP 요청에서 수신되지 않은 응답 또는 오류

  OCSP 응답자가 Cisco ISE OCSP 요청에 대한 응답을 또는 제공하지 않거나 OCSP 응답 상태를 실패한 상태로 반환할 수 있습니다. OCSP 응답 상태 값은 다음과 같습니다.

  - tryLater
  - signRequired
  - unauthorized
  - internalError
  - malformedRequest

    OCSP 요청에는 여러 가지 날짜 및 시간 검사, 서명 유효성 검사 등이 있습니다. 자세한 내용은 *RFC 2560 X.509* 인터넷 공개 키 인프라 *OCSP(Online Certificate Status Protocol)*를 참고하십시오. 여기에서는 오류 상태를 포함한 모든 가능한 상태를 설명합니다.

- 실패한 OCSP 보고서

OCSP 클라이언트 프로파일 추가

OCSP 클라이언트 프로파일 페이지를 사용하여 Cisco ISE에 새 OCSP 클라이언트 프로파일을 추가할 수 있습니다.

시작하기 전에

CA(Certificate Authority)가 비표준 포트(80 또는 443 이외의 포트)에서 OCSP 서비스를 실행 중인 경우 Cisco ISE와 해당 포트의 CA 간에 통신을 허용하도록 스위치에서 ACL을 구성해야 합니다. 예를 들면 다음과 같습니다.

permit tcp <*source ip*> <*destination ip*> **eq** <*OCSP port number*>

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **OCSP Client Profile(OSCP** 클라이언트 프로파일**)**을 선택합니다 .

단계 **2** 값을 입력하여 OCSP 클라이언트 프로파일을 추가합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

OCSP 클라이언트 프로파일 설정

다음 표에서는 OCSP 클라이언트 프로파일을 구성하는 데 사용할 수 있는 OSCP Client Profile(OCSP 클라이언트 프로파일) 페이지의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **OCSP Client Profile(OCSP** 클라이언트 프로파일**)**입니다.

표 ***20: OCSP*** 클라이언트 프로파일 설정

필드 이름	사용 지침
Name(이름**)**	OCSP 클라이언트 프로파일의 이름입니다.
Description(설명**)**	필요에 따라 설명을 입력합니다.
OCSP 응답자 구성	
Enable Secondary Server(보조 서버 활성화**)**	고가용성을 위해 보조 OCSP 서버를 활성화하려면 이 확인란을 선택합니다.
Always Access Primary Server First(항상 기본 서버에 먼저 액세스**)**	보조 서버로 이동하기 전에 기본 서버를 확인하려면 이 옵션을 사용합니다. 이전에 기본 서버를 확인한 결과 응답하지 않았더라도 Cisco ISE는 보조 서버로 이동하기 전에 기본 서버로의 요청 전송을 시도합니다.

필드 이름	사용 지침
Fallback to Primary Server After Interval *n* Minutes(n분 간격 이후 기본 서버로 대체**)**	Cisco ISE가 보조 서버로 이동했다가 기본 서버로 다시 대체하도록 하려면 이 옵션을 사용합니다. 이 경우 다른 요청은 모두 건너뛰며 텍스트 상자에서 구성하는 시간 동안 보조 서버가 사용됩니다. 사용할 수 있는 시간 범위는 1~999분입니다.
Primary and Secondary Servers(기본 서버 및 보조 서버**)**	
URL	기본 및/또는 보조 OCSP 서버의 URL을 입력합니다.
Enable Nonce Extension Support(nonce 확장 지원 활성화**)**	OCSP 요청의 일부분으로 nonce를 전송하도록 구성할 수 있습니다. nonce에는 OCSP 요청의 의사 난수가 포함됩니다. 이 옵션을 사용하는 경우 응답에서 수신된 숫자가 요청에 포함된 숫자와 동일한지를 확인합니다. 이 옵션을 사용하는 경우 재생 공격에서 이전 통신을 사용할 수 없습니다.
Validate Response Signature(응답 서명 검증**)**	OCSP 응답자는 다음 인증서 중 하나를 사용하여 응답을 표시합니다. • CA 인증서 • CA 인증서와 다른 인증서 Cisco ISE가 응답 서명을 검증하도록 하려면 OCSP 응답자가 인증서와 함께 응답을 보내야 합니다. 그렇지 않으면 응답 확인이 실패하며 인증서의 상태를 신뢰할 수 없습니다. RFC에 따르면 OCSP는 서로 다른 여러 인증서를 사용하여 응답에 서명을 할 수 있습니다. 단, OCSP는 Cisco ISE가 검증할 수 있도록 응답에 서명을 하는데 사용한 인증서를 보내야 합니다. OCSP가 Cisco ISE에 구성되어 있지 않은 다른 인증서로 응답에 서명을 하는 경우에는 응답 확인이 실패합니다.
Use OCSP URLs specified in Authority Information Access (AIA)(AIA(Authority Information Access)에 지정된 **OCSP URL** 사용**)**	Authority Information Access 익스텐션에 지정된 OCSP URL을 사용하려면 라디오 버튼을 클릭합니다.
응답 캐시	

필드 이름	사용 지침
Cache Entry Time To Live *n* Minutes(캐시 엔트리 **Time To Live n**분**)**	캐시 엔트리가 만료될 때까지의 시간을 분 단위로 입력합니다. OCSP 서버의 각 응답은 nextUpdate 값을 포함합니다. 서버에서 다음 번에 인증서 상태를 업데이트하면 이 값이 표시됩니다. OCSP 응답을 캐시할 때는 두 값, 즉 컨피그레이션의 값과 응답의 값을 비교하며 이 두 값 중 더 작은 기간에 대해 응답이 캐시됩니다. nextUpdate 값이 0이면 응답은 캐시되지 않습니다. Cisco ISE는 구성된 시간 동안 OCSP 응답을 캐시합니다. 캐시는 복제되거나 영구적으로 저장되지 않으므로 Cisco ISE를 재시작하면 캐시가 지워집니다. OCSP 캐시는 OCSP 응답을 유지 관리하는 데 사용되며, 다음과 같은 이유로도 사용됩니다. • 이미 알려진 인증서에 대한 OCSP 서버의 네트워크 트래픽 및 로드 감소 • 이미 알려진 인증서 상태를 캐시하여 Cisco ISE의 성능 개선 기본적으로 캐시는 내부 CA OCSP 클라이언트 프로파일에 대해 2분으로 설정됩니다. 엔드포인트가 첫 번째 인증 후 2분 이내에 두 번째 인증을 수행하는 경우 OCSP 캐시가 사용되고 OCSP 응답자가 쿼리되지 않습니다. 엔드포인트 인증서가 캐시 기간 내에 취소된 경우 이전 OCSP 상태인 Good이 사용되며 인증이 성공합니다. 캐시를 0분으로 설정하면 응답이 캐시되지 않습니다. 이 옵션을 사용하면 보안이 개선되지만 인증 성능은 저하됩니다.
Clear Cache(캐시 지우기**)**	OCSP 서비스에 연결된 모든 인증 기관의 엔트리를 지우려면 **Clear Cache(**캐시 지우기**)**를 클릭합니다. 구축에서 **Clear Cache(**캐시 지우기**)**는 모든 노드와 상호 작용하여 작업을 수행합니다. 이러한 메커니즘은 구축의 모든 노드를 업데이트합니다.

관련 항목

OCSP 서비스, 139 페이지
Cisco ISE CA Service Online Certificate Status Protocol 응답자, 139 페이지
OCSP 인증서 상태 값, 139 페이지
OCSP 고가용성, 140 페이지
OCSP 실패, 140 페이지
OCSP 통계 카운터, 143 페이지
OCSP 클라이언트 프로파일 추가, 141 페이지

OCSP 통계 카운터

Cisco ISE는 OCSP 카운터를 사용하여 OCSP 서버의 데이터와 상태를 기록하고 모니터링합니다. 5분마다 로깅됩니다. Cisco ISE는 시스템 로그 메시지를 모니터링 노드로 보내며, 이 메시지는 로컬 저장

소에 보존됩니다. 로컬 저장소에는 지난 5분 동안의 데이터가 포함되어 있습니다. Cisco ISE가 시스템 로그 메시지를 보내고 나면 다음 간격에 대해 카운터가 다시 계산됩니다. 즉, 5분이 지나면 새로운 5분 시간 간격이 다시 시작됩니다.

다음 표에는 OCSP 시스템 로그 메시지와 해당 설명이 나와 있습니다.

표 ***21: OCSP*** 시스템 로그 메시지

메시지	설명
OCSPPrimaryNotResponsiveCount	응답하지 않는 기본 요청의 수
OCSPSecondaryNotResponsiveCount	응답하지 않는 보조 요청의 수
OCSPPrimaryCertsGoodCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '정상' 인증서의 수
OCSPSecondaryCertsGoodCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '정상' 상태의 수
OCSPPrimaryCertsRevokedCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '취소된' 상태의 수
OCSPSecondaryCertsRevokedCount	보조 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '취소된' 상태의 수
OCSPPrimaryCertsUnknownCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '알 수 없는' 상태의 수
OCSPSecondaryCertsUnknownCount	보조 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '알 수 없는' 상태의 수
OCSPPrimaryCertsFoundCount	기본 원본의 캐시에서 발견된 인증서의 수
OCSPSecondaryCertsFoundCount	보조 원본의 캐시에서 발견된 인증서의 수
ClearCacheInvokedCount	간격 이후 일반 캐시가 트리거된 횟수
OCSPCertsCleanedUpCount	간격 이후 정리된 캐시된 엔트리의 수
NumOfCertsFoundInCache	캐시에서 이행된 요청의 수
OCSPCacheCertsCount	OCSP 캐시에서 발견된 인증서의 수

관리자 액세스 정책 구성

RBAC 정책은 if-then 형식으로 표현됩니다. 여기서 "if"는 RBAC 관리자 그룹 값이고 "then"은 RBAC 권한 값입니다.

RBAC 정책 창(**Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authorization(**권한 부여**)** > **RBAC Policy(RBAC** 정책**)** 선택)에는 기본 정책 목록이 포함되어 있습니다. 이러한 기본 정책은 편집하거나 삭제할 수 없습니다. 그러나 읽기 전용 관리 정책에 대한 데이터 액세스 권한은 편집할 수 있습니다. 또한 RBAC 정책 페이지에서는 직장 전용 관리자 그룹에 대해 사용자 맞춤화 RBAC 정책을 생성하여 개인 설정된 관리자 그룹에 적용할 수 있습니다.

제한된 메뉴 액세스를 할당할 경우 관리자가 데이터 액세스 권한을 통해 지정된 메뉴를 사용하는 데 필요한 데이터에 액세스할 수 있는지 확인하십시오. 예를 들어, MyDevices 포털에 대한 메뉴 액세스는 제공하지만 엔드포인트 ID 그룹에 대한 데이터 액세스는 허용하지 않는 경우 해당 관리자는 포털을 수정할 수 없습니다.

참고 관리자는 엔드포인트 MAC 주소를 읽기 전용 액세스 권한이 있는 엔드포인트 ID 그룹에서 전체 액세스 권한이 있는 엔드포인트 ID 그룹으로 이동할 수 있습니다. 다른 방법으로는 불가능합니다.

시작하기 전에

- RBAC(Role-Based Access Control) 정책을 정의하려는 모든 관리자 그룹을 생성합니다.
- 이러한 관리자 그룹이 개별 관리 사용자에게 매핑되어 있는지 확인합니다.
- 메뉴 액세스 및 데이터 액세스 권한과 같은 RBAC 권한을 구성했는지 확인합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Authorization(**권한 부여**)** > **RBAC Policy(RBAC** 정책**)**를 선택합니다.

RBAC 정책 페이지에는 기본 관리자 그룹에 대해 즉시 사용 가능한 미리 정의된 정책이 포함되어 있습니다. 이러한 기본 정책은 편집하거나 삭제할 수 없습니다. 그러나 기본 읽기 전용 관리 정책에 대한 데이터 액세스 권한을 편집할 수 있습니다.

단계 **2** 기본 RBAC 정책 규칙 옆의 **Actions(**작업**)**를 클릭합니다.

여기서 새 RBAC 정책을 삽입하고 기존 RBAC 정책을 복제/삭제할 수 있습니다.

단계 **3** **Insert new policy(**새 정책 삽입**)**를 클릭합니다.

단계 **4** Rule Name(규칙 이름), RBAC Group(s)(RBAC 그룹) 및 Permissions(권한) 필드에 값을 입력합니다.

RBAC 정책을 생성할 때는 여러 메뉴 액세스 및 데이터 액세스 권한을 선택할 수 없습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

관리자 액세스 설정

Cisco ISE를 사용하면 관리자 계정에 대한 일부 규칙을 정의하여 보안을 개선할 수 있습니다. 관리 인터페이스에 대한 액세스를 제한하여 관리자가 강력한 비밀번호를 사용하거나 비밀번호를 정기적으로 변경하는 등의 작업을 하도록 강제할 수 있습니다. Cisco ISE의 관리자 계정 설정에서 정의하는 비밀번호 정책은 모든 관리자 계정에 적용됩니다.

Cisco ISE는 UTF-8 문자를 포함하는 관리자 비밀번호를 지원합니다.

동시 관리 세션 및 로그인 배너의 최대 수 구성

관리자에게 관리 웹 또는 CLI 인터페이스에 액세스하는 사용자를 알려 주는 동시 관리 GUI 또는 CLI(SSH) 세션 및 로그인 배너의 최대 수를 구성할 수 있습니다. 관리자 로그인 전과 후에 표시되는 로그인 배너를 구성할 수 있습니다. 이러한 로그인 배너는 기본적으로 비활성화됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration**(관리) > **System**(시스템) > **Admin Access**(관리자 액세스) > **Settings**(설정) > **Access**(액세스) > **Session**(세션)을 선택합니다.

단계 **2** GUI 및 CLI 인터페이스를 통해 허용하려는 동시 관리 세션의 최대 수를 입력합니다. 동시 관리 GUI 세션의 유효 범위는 1~20입니다. 동시 관리 CLI 세션의 유효 범위는 1~10입니다.

단계 **3** 관리자 로그인 전에 Cisco ISE가 메시지를 표시하도록 하려면 **Pre-login banner**(로그인 전 배너) 확인란을 선택하고 텍스트 상자에 메시지를 입력합니다.

단계 **4** 관리자 로그인 후에 Cisco ISE가 메시지를 표시하도록 하려면 **Post-login banner**(로그인 후 배너) 확인란을 선택하고 텍스트 상자에 메시지를 입력합니다.

단계 **5** **Save**(저장)를 클릭합니다.

관련 항목

선택한 IP 주소에서 Cisco ISE로의 관리 액세스 허용, 146 페이지

선택한 IP 주소에서 Cisco ISE로의 관리 액세스 허용

Cisco ISE에서는 관리자가 Cisco ISE 관리 인터페이스에 액세스할 수 있는 IP 주소 목록을 구성할 수 있습니다.

관리자 액세스 제어 설정은 관리, 정책 서비스 또는 모니터링 페르소나가 지정된 Cisco ISE 노드에만 적용 가능합니다. 이러한 제한은 기본 노드에서 보조 노드로 복제됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Settings(**설정**)** > **Access(**액세스**)** > **IP Access(IP** 주소**)**를 선택합니다.

단계 **2** **Allow only listed IP address to connect(**연결하도록 나열된 **IP** 주소만 허용**)** 라디오 버튼을 클릭합니다.

참고 포트 161(SNMP)에 대한 연결은 관리 액세스에 사용됩니다. 그러나 IP 액세스 제한이 구성된 경우, snmpwalk가 수행되는 출처 노드를 관리 액세스용으로 구성하지 않으면 snmpwalk는 실패합니다.

단계 **3** **Configure IP List for Access Restriction(**액세스 제한용 **IP** 목록 구성**)** 영역에서 **Add(**추가**)**를 클릭합니다.

단계 **4** **Add IP CIDR(IP CIDR** 추가**)** 대화 상자에서 **IP address(IP** 주소**)** 필드에 IP 주소를 CIDR(Classless Interdomain Routing) 형식으로 입력합니다.

참고 이 IP 주소는 IPv4 또는 IPv6 주소일 수 있습니다. 하나의 ISE 노드에 대해 여러 IPv6 주소를 구성할 수 있습니다.

단계 **5** **Netmask in CIDR format(CIDR**의 네트워크 마스크 형식**)** 필드에 서브넷 마스크를 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다. 단계 4~7을 반복하여 이 목록에 IP 주소 범위를 더 추가합니다.

단계 **7** **Save(**저장**)**를 클릭하여 변경사항을 저장합니다.

단계 **8** **Reset(**재설정**)**을 클릭하여 **IP Access(IP** 액세스**)** 창을 새로 고칩니다.

Cisco ISE의 MnT 섹션에 대한 액세스 허용

Cisco ISE에서는 관리자가 Cisco ISE의 Mnt 섹션에 액세스할 수 있는 노드의 목록을 구성할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE 홈페이지에서 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Access(**액세스**)**를 선택합니다.

단계 **2** **Mnt Access(Mnt** 액세스**)** 탭을 클릭합니다.

단계 **3** 구축 내에서 또는 구축 외부에서 시스템 로그를 MnT로 전송하도록 노드 또는 엔티티를 허용하려면 **Allow any IP address to connect to MnT(MnT**에 연결할 모든 **IP** 주소 허용**)** 라디오 버튼을 클릭합니다. 구축 내 노드 또는 엔티티만 시스템 로그를 MnT로 전송하도록 허용하려면 **Allow any IP address to connect to MnT (**구축 내의 노드만 **MnT** 에 연결 허용**)** 라디오 버튼을 클릭합니다.

참고 ISE 2.6 P2 이상 버전의 경우 Use ISE Messaging Service for UDP Syslogs delivery to MnT(UDP Syslogs를 Mnt로 전송하기 위해서 ISE 메시지 서비스만 사용)이 기본적으로 켜져 있습니다. 그러면 구축 외부의 다른 엔티티에서 오는 시스템 로그가 허용되지 않습니다.

관리자 계정의 비밀번호 정책 구성

Cisco ISE에서는 보안을 강화하기 위해 관리자 계정용 비밀번호 정책을 생성할 수도 있습니다. 비밀번호 기반 또는 클라이언트 인증서 기반 관리자 인증을 원하는지 정의할 수 있습니다. 여기에서 정의하는 비밀번호 정책은 Cisco ISE의 모든 관리자 계정에 적용됩니다.

참고

- 내부 관리자 사용자에 대한 이메일 알림은 root@host로 전송됩니다. 이메일 주소를 구성 할 수 없으며 많은 SMTP 서버가 이 이메일을 거부합니다.

  이메일 주소를 변경할 수 있는 개선된 오픈 결함 CSCui5583을 따릅니다.

- Cisco ISE는 UTF-8 문자를 포함하는 관리자 비밀번호를 지원합니다.

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- 구축에서 활성화되어 있는 경우 자동 페일오버 구성을 끕니다. 관리 노드에 대한 자동 페일오버 지원의 내용을 참조하십시오.

  인증 방법을 변경하면 애플리케이션 서버 프로세스가 다시 시작됩니다. 이러한 서비스가 다시 시작되는 동안 작업이 지연될 수 있습니다. 서비스가 다시 시작될 때의 이러한 지연으로 인해 보조 관리 노드의 자동 페일오버가 시작될 수 있습니다.

단계 **1** Cisco ISE GUI 메뉴에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭한 뒤**Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)**를 선택합니다.

단계 **2** 다음 인증 방법 중 하나의 라디오 버튼을 클릭합니다.

- **Password Based(**비밀번호 기반**)**: 관리자 로그인에 표준 사용자 ID 및 비밀번호 자격 증명을 사용하려면 이 옵션을 선택합니다. **Identity Source** 드롭다운 목록에서 **Internal(**내부**)** 또는 **External(**외부**)**을 선택합니다.

  참고 LDAP 등의 외부 ID 소스를 구성했으며 관리자에게 액세스 권한을 부여하기 위한 인증 소스로 해당 소스를 사용하려는 경우에는 ID 소스 목록 상자에서 해당 특정 ID 소스를 선택해야 합니다.

- **Client Certificate Based(**클라이언트 인증서 기반**)**: 인증서 기반 정책을 지정하려면 이 옵션을 선택합니다. **Certificate Authentication Profile(**인증서 인증 프로파일**)** 드롭다운 목록에서 기존 인증 프로파일을 선택합니다. **Identity Source(ID** 소스**)** 드롭다운 목록에서 필요한 값을 선택합니다.

단계 **3** **Password Policy(**비밀번호 정책**)** 탭을 클릭하고 Cisco ISE GUI 및 CLI 비밀번호 요구 사항을 구성하는 데 필요한 값을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭하여 관리자 비밀번호 정책을 저장합니다.

참고 로그인 시 외부 ID 저장소를 사용하여 관리자를 인증하는 경우, 관리자 프로파일에 적용되는 비밀번호 정책에 대해 이 설정이 구성되어 있더라도 외부 ID 저장소는 관리자의 사용자 이름과 비밀번호를 계속 검증합니다.

관련 항목

관리자 비밀번호 정책 설정
관리자 계정의 계정 비활성화 정책 구성, 149 페이지
관리자 계정에 대한 잠금 또는 일시 중단 설정 구성, 149 페이지

관리자 계정의 계정 비활성화 정책 구성

Cisco ISE에서는 구성된 연속 기간(일) 동안 관리자 계정이 인증되지 않은 경우 해당 관리자 계정을 비활성화할 수 있습니다.

단계 **1** Cisco ISE GUI 메뉴에서 **Menu**(메뉴) 아이콘(☰)을 클릭한 뒤 **Administration**(관리) > **System**(시스템) > **Admin Access**(관리자 액세스) > **Authentication**(인증) > **Account Disable Policy**(계정 비활성화 정책)를 선택합니다.

단계 **2** **Disable account after *n* days of inactivity**(n일 동안 비활성 상태였던 계정 비활성화) 확인란을 선택하고 해당 필드에 기간(일)을 입력합니다.

이 옵션을 사용하면 구성된 지정된 기간(일) 동안 관리자 계정이 비활성 상태인 경우 해당 관리자 계정을 비활성화할 수 있습니다. 그러나 **Inactive Account Never Disabled**(비활성화된 적 없는 계정 비활성화) 옵션(**Administration**(관리) > **System**(시스템) > **Admin Access**(관리 액세스) > **Administrators**(관리자) > **Admin Users**(관리 사용자) 창에서 사용 가능)을 사용하여 이 계정 비활성화 정책에서 개별 관리자 계정을 제외할 수 있습니다.

단계 **3** 관리자에 대한 전역 계정 비활성화 정책을 구성하려면 **Save**(저장)를 클릭합니다.

관리자 계정에 대한 잠금 또는 일시 중단 설정 구성

Cisco ISE에서는 실패한 로그인 시도 횟수가 지정된 횟수보다 많은 관리자 계정(비밀번호 기반 내부 관리자 계정 및 인증서 기반 관리자 계정 포함)을 잠그거나 일시 중지할 수 있습니다.

단계 **1** Cisco ISE GUI 메뉴에서 **Menu**(메뉴) 아이콘(☰)을 클릭한 뒤 **Administration**(관리) > **System**(시스템) > **Admin Access**(관리자 액세스) > **Authentication**(인증) > **Lock/Suspend Settings**(설정 잠금/일시 중지)를 선택합니다.

단계 **2** **Suspend or Lock Account With Incorrect Login Attempts**(잘못된 로그인 시도 시 계정 잠금 또는 일시 중지) 확인란을 선택하고 몇 번의 시도가 실패한 후 조치를 취할지 입력합니다. 유효 범위는 3~20입니다. 다음 중 하나의 옵션에 해당하는 라디오 버튼을 클릭합니다.

- **Suspend Account For *n* Minutes**(n분 동안 계정 일시 중지): 지정된 잘못된 로그인 시도 횟수를 초과하는 계정을 일시 중지하려면 이 옵션을 선택합니다. 유효 범위는 15~1440입니다.
- **Lock Account**(계정 잠금): 지정된 잘못된 로그인 시도 횟수를 초과하는 계정을 잠그려면 이 옵션을 선택합니다.

최종 사용자에게 헬프데스크에 문의하여 계정 잠금을 해제하도록 요청하는 등의 사용자 맞춤화 이메일 교정 메시지를 입력할 수 있습니다.

참고 Cisco ISE 릴리스 2.3 이하에서는 **Lock/Suspend Settings(**설정 잠금/일시 중지**)**은 **Password Policy(**비밀번호 정책**)** 탭(**Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Authentication(**인증**)** > **Password Policy(**비밀번호 정책**)**에서 사용할 수 있습니다.

관리자에 대한 세션 시간 초과 구성

Cisco ISE에서는 관리 GUI 세션이 비활성 상태로 계속 연결되어 있을 수 있는 시간을 결정할 수 있습니다. Cisco ISE가 관리자를 로그아웃 처리할 때까지의 시간을 분 단위로 지정할 수 있습니다. 세션 시간이 초과되고 나면 관리자는 다시 로그인해야 Cisco ISE 관리 포털에 액세스할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Session(**세션**)** > **Session Timeout(**세션 시간 초과**)**을 선택합니다.

단계 **2** 작업을 수행하지 않는 경우 관리자가 로그아웃될 때까지 Cisco ISE가 대기하도록 할 시간을 분 단위로 입력합니다. 기본값은 60분입니다. 유효 범위는 6분~100분입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

활성 관리 세션 종료

Cisco ISE는 필요한 경우 언제든지 세션을 선택하여 종료할 수 있도록 모든 활성 관리 세션을 표시합니다. 동시 관리 GUI 세션의 최대 수는 20개입니다. GUI 세션의 최대 수에 도달하면 슈퍼 관리자 그룹에 속하는 관리자가 로그인하여 일부 세션을 종료할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Settings(**설정**)** > **Session(**세션**)** > **Session Info(**세션 정보**)**를 선택합니다.

단계 **2** 종료할 세션 ID 옆의 확인란을 선택하고 **Invalidate(**무효화**)**를 클릭합니다.

관리자 이름 변경

Cisco ISE에서는 Cisco ISE GUI를 통해 사용자 이름을 변경할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE 관리 포털에 로그인합니다.

단계 **2** Cisco ISE GUI의 오른쪽 상단에서 기어 아이콘 ()을 클릭하고 드롭다운 목록에서 **Account Settings(**계정 설정**)**를 선택합니다.

단계 **3** 표시되는 **Admin User(**관리 사용자**)** 대화 상자에 새 사용자 이름을 입력합니다.

단계 **4** 변경할 계정에 대한 기타 세부정보를 편집합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

관리자 액세스 설정

이 섹션에서는 관리자용 액세스 설정을 구성할 수 있습니다.

관리자 비밀번호 정책 설정

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

표 ***22:*** 관리자 비밀번호 정책 설정

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

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

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

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

관련 항목

Cisco ISE 관리자
새 관리자 생성

세션 시간 초과 및 세션 정보 설정

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

표 ***23:*** 세션 시간 초과 및 세션 정보 설정

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

관련 항목

관리자 액세스 설정, 146 페이지
관리자에 대한 세션 시간 초과 구성, 150 페이지
활성 관리 세션 종료, 150 페이지