pxGrid

pxGrid 및 Cisco ISE

참고

Cisco ISE 릴리스 3.1부터 모든 pxGrid 연결은 pxGrid 2.0을 기반으로 해야 합니다. pxGrid 1.0 기반(XMPP 기반) 통합은 릴리스 3.1부터 Cisco ISE에서 작동하지 않습니다.

WebSockets를 기반으로 하는 pxGrid 버전 2.0은 Cisco ISE 릴리즈 2.4에서 소개되었습니다. 잠재적인 통합 중단을 방지하려면 다른 시스템을 pxGrid 2.0 호환 버전으로 계획 및 업그레이드하는 것이 좋습니다.

Cisco pxGrid는 양방향 any-to-any 파트너 플랫폼 통합을 허용하는 확장 가능한 개방형 SPIF(Security Product Integration Framework)입니다.

pxGrid 1.0은 레거시 XMPP(Extensible Messaging and Presence Protocol) 구현을 사용합니다. pxGrid 1.0은 유지 관리 모드이며 곧 제거됩니다. Cisco pxGrid 1.0에는 pxGrid와 호환되는 클라이언트 SDK 라이브러리(Java 또는 C)가 필요합니다.

pxGrid 2.0은 REST 및 WebSocket 인터페이스를 사용합니다. 클라이언트는 제어 메시지, 쿼리 및 애플리케이션 데이터에 REST를 사용하고 이벤트 푸시에 WebSocket을 사용합니다. pxGrid 2.0에 대한 자세한 내용은 **Welcome to Learning Cisco Platform Exchange Grid(pxGrid)**를 참고하십시오.

Cisco pxGrid는 다음 기능을 제공합니다.

- Cisco ISE 세션 디렉터리에서 다른 정책 네트워크 시스템(예: ISE Eco 시스템 파트너 시스템 및 기타 Cisco 플랫폼)과 상황에 맞는 정보를 공유합니다.
- 타사 시스템이 네트워크 또는 보안 이벤트에 대한 응답으로 사용자 및 디바이스를 격리하기 위해 적응형 네트워크 제어 작업을 호출할 수 있습니다. 태그 정의, 값 및 설명과 같은 TrustSec 정보는 TrustSec 주제를 통해 Cisco ISE에서 다른 네트워크로 전달됩니다.
- FQN(Fully Qualified Names)을 사용하는 엔드포인트 프로파일을 엔드포인트 프로파일 메타 주제를 통해 Cisco ISE에서 다른 네트워크로 전송합니다.

- 태그 및 엔드포인트 프로파일을 대량으로 다운로드합니다.
- pxGrid를 통해 SXP 바인딩(IP-SGT 매핑)을 게시하고 구독합니다. SXP 바인딩에 대한 자세한 내용은 Cisco ISE 관리 가이드의 세그멘테이션 장에 있는 보안 그룹 태그 교환 프로토콜 섹션을 참고하십시오.
- Cisco pxGrid Context-in을 사용하면 에코시스템 파트너가 Cisco ISE에 주제 정보를 게시할 수 있습니다. 이를 통해 Cisco ISE는 에코시스템에서 식별된 에셋을 기반으로 조치를 취할 수 있습니다. Cisco pxGrid Context-in에 대한 자세한 내용은 pxGrid Context-In을 참고하십시오.

참고 pxGrid 1.0은 유지 관리 모드이며 곧 사용이 중단됩니다. ISE 2.4에서 pxGrid 2.0을 도입했습니다. 파트너는 pxGrid 클라이언트 구현을 pxGrid 2.0으로 전환하는 것이 좋습니다.

pxGrid 개요

pxGrid에는 다음 구성 요소가 있습니다.

- 컨트롤러: 검색, 인증 및 권한 부여를 처리합니다.
- 제공자: 쿼리 결과를 반환하거나 게시합니다.
- Pubsub : 제공자 및 사용자에게 pxGrid 서비스를 제공합니다.
- 가입자: 권한이 부여된 가입자는 구독하는 주제에서 상황 정보 및 알림을 받습니다.

pxGrid는 다음 기능을 제공합니다.

- 검색: 서비스 이름을 기준으로 서비스 속성을 검색합니다. 제공자가 pxGrid 컨트롤러에 "Register Service(서비스 등록)"를 요청하면 플로우가 시작됩니다. 등록 후 사용자는 "Lookup Service(조회 서비스)"를 사용하여 제공자의 위치를 검색합니다.
- 인증: pxGrid 컨트롤러는 서비스에 액세스하기 위해 pxGrid 클라이언트를 인증합니다. 자격 증명은 사용자 이름과 비밀번호 또는 인증서(기본 설정)입니다.
- 권한 부여: pxGrid는 작업 요청을 받으면 pxGrid 컨트롤러를 통해 확인하여 요청에 권한을 부여합니다. pxGrid는 클라이언트를 미리 정의된 그룹에 할당합니다.

pxGrid 1.0 고가용성

pxGrid 1.0을 사용하면 pxGrid 페르소나가 활성/대기 모드로 작동하는 두 개의 노드를 구성할 수 있습니다. 고가용성 구성에서 Cisco pxGrid 서버는 PAN을 통해 노드 간에 정보를 복제합니다. PAN이 다운되면 pxGrid 서버는 클라이언트 등록 및 서브스크립션 처리를 중단합니다. pxGrid 서버를 활성화하려면 PAN을 수동으로 승격해야 합니다.

CLI 명령 **show application status ise**를 사용하여 pxGrid 프로세스를 확인할 수 있습니다. pxGrid 1.0과 관련된 프로세스는 다음과 같습니다.

- pxGrid 인프라 서비스

- pxGrid 게시자 가입자 서비스
- pxGrid 연결 관리자
- pxGrid 컨트롤러

활성 pxGrid 1.0 노드에서 이러한 프로세스는 'Running'으로 표시됩니다. 대기 pxGrid 1.0 노드에서는 Disabled로 표시됩니다. 활성 pxGrid 1.0 노드가 작동 중지되면**show logging application pxgrid.state** 대기 pxGrid 노드가 이를 탐지하고 4개의 pxGrid 프로세스를 시작합니다. 몇 분 내에 이러한 프로세스가 'Running'으로 표시되고 대기 노드는 활성 노드가 됩니다. CLI 명령 **show logging application pxgrid**를 실행하여 pxGrid가 해당 노드에서 대기 중인지 확인할 수 있습니다.

Cisco ISE는 보조 pxGrid 노드에 대한 자동 페일오버를 수행합니다. 원래 기본 pxGrid 노드를 다시 네트워크에 연결하는 경우 원래 기본 pxGrid 노드는 보조 역할로 계속 유지되며 현재 기본 노드를 종료하지 않는 한 기본 역할로 다시 승격되지 않습니다.

pxGrid 2.0의 고가용성

pxGrid 2.0 노드는 활성/활성 구성에서 작동합니다. 고가용성을 위해서는 구축에 두 개 이상의 pxGrid 노드가 있어야 합니다. 대규모 구축의 경우 확장성 및 리던던시(redundancy)를 높이기 위해 최대 4개의 노드를 포함할 수 있습니다. 모든 노드에 대해 IP 주소를 구성하여 한 노드가 작동 중지될 경우 해당 노드의 클라이언트가 작동하는 노드에 연결되도록 하는 것이 좋습니다. PAN이 작동 중지되면 pxGrid 서버는 활성화 처리를 중지합니다. pxGrid 서버를 활성화하려면 PAN을 수동으로 승격합니다. pxGrid 구축에 대한 자세한 내용은 **ISE Performance & Scale**을 참고하십시오.

모든 pxGrid 서비스 제공자 클라이언트는 7.5분 이내에 pxGrid 컨트롤러에 주기적으로 다시 등록됩니다. PAN 노드는 다시 등록되지 않는 클라이언트를 비활성 상태로 간주하고 삭제합니다. PAN 노드가 7.5분 넘게 작동 중지되었다가 다시 작동되는 경우 7.5분보다 오래된 타임스탬프 값을 가진 모든 클라이언트가 삭제됩니다. 모든 클라이언트는 pxGrid 컨트롤러에 다시 등록해야 합니다.

pxGrid 2.0 클라이언트는 pub/sub 및 쿼리에 WebSocket 및 REST 기반 API를 사용했습니다. 이러한 API는 포트 8910의 ISE 애플리케이션 서버에서 제공됩니다. **show logging application pxgrid**를 실행할 때 표시되는 pxGrid 프로세스는 pxGrid 2.0에 적용되지 않습니다.

손실 탐지

Cisco ISE 3.0에서는 pxGrid 주제에 시퀀스 ID를 추가했습니다. 전송이 중단되는 경우 가입자는 ID 시퀀스의 단절을 확인하여 이를 인식할 수 있습니다. 가입자는 주제 시퀀스 ID의 변경을 확인하고 마지막 시퀀스 번호의 날짜를 기준으로 데이터를 요청합니다. 게시자가 작동 중지되었다가 다시 시작되는 경우 주제 시퀀스가 0부터 시작합니다. 가입자는 시퀀스 0이 표시될 경우 캐시를 지우고 대량 다운로드를 시작해야 합니다. 가입자의 연결이 끊어질 경우 게시자는 시퀀스 ID를 계속 할당합니다. 가입자가 다시 연결한 후 시퀀스 ID의 단절을 확인할 경우 마지막 시퀀스 번호의 시간부터 데이터를 요청합니다. 손실 탐지는 세션 디렉터리 및 TrustSec 구성을 사용하여 작동합니다. 세션 디렉터리를 사용하는 경우 클라이언트가 손실을 탐지하면 캐시를 지우고 대량 다운로드를 시작해야 합니다.

시퀀스 ID를 사용하지 않는 기존 애플리케이션이 있는 경우 시퀀스 ID를 사용할 필요가 없습니다. 그러나 이를 사용하면 손실을 탐지하고 손실을 복구할 수 있다는 이점이 있습니다.

세션 디렉터리 세션은 알림 간격마다 비동기식으로 MnT에서 일괄 처리되고 `/topic/com.cisco.ise.session`에 게시됩니다.

TrustSec Config 보안 그룹에 대한 변경 사항은 `/topic/com.cisco.ise.config.trustsec.security.group`에 게시됩니다.

손실 탐지는 pxGrid 2.0에서만 지원되며 기본적으로 설정되어 있습니다.

손실 탐지를 사용하는 코드 예를 보려면 https://github.com/cisco-pxgrid/pxgrid-rest-ws/tree/master/java/src/main/java/com/cisco/pxgrid/samples/ise 항목을 참고하십시오.

모니터링 및 디버깅

pxGrid 노드에 대해 제공되는 로그는 다음과 같습니다.

- pxgrid.log: pxGrid 1.0 프로세스 활동
- pxgrid-server.log: pxGrid 2.0 활동 및 오류
- pxgrid-cm.log: pxGrid 1.0 연결 로그
- pxgrid-controller.log: pxGrid 1.0 제어 메시지 로그
- pxgrid-jabberd.log: pxGrid 1.0 XMPP 서버 로그
- pxgrid-pubsub.log: pxGrid 1.0 XMPP Pubsub 로그

Log(로그**)** 페이지에는 모든 pxGrid 2.0 관리 이벤트가 표시됩니다. 이벤트 정보에는 이벤트 유형 및 타임스탬프와 함께 클라이언트 및 기능 이름이 포함됩니다. **Administration(**관리**) > pxGrid Services(pxGrid** 서비스**) > Diagnostics(**진단**) > Log(**로그**)**로 이동하여 이벤트 목록을 봅니다. 로그를 지우고 목록을 다시 동기화하거나 새로 고칠 수도 있습니다.

pxGrid 요약 페이지

Summary(요약) 페이지에는 현재 pxGrid 2.0 환경의 통계가 표시됩니다.

- Current Connections(현재 연결): 컨트롤러에 대한 연결 목록
- Control Messages(제어 메시지): 인증, 권한 부여 및 서비스 검색
- REST APIs(REST API): WebSocket 또는 XMPP를 사용하여 연결된 클라이언트 수
- Pubsub Throughput(Pubsub 처리량): 클라이언트에 게시된 데이터의 양
- Clients(클라이언트): REST 또는 WebSocket으로 연결된 클라이언트
- Errors(오류): 클라이언트가 데이터 전송 재시작을 요청하도록 야기한 전송 오류의 수

pxGrid 클라이언트 관리

새 클라이언트가 pxGrid에 연결하는 경우 먼저 관리자가 이 페이지를 방문하여 클라이언트를 승인해야 클라이언트가 그리드에 사용될 수 있습니다. 그러나 **Settings(**설정**)** 페이지에서 인증서 기반 계정의 자동 승인을 활성화한 경우 수동 승인이 필요하지 않습니다.

- **Clients(**클라이언트**)**: pxGrid 1.0 및 2.0의 외부 클라이언트 계정을 나열합니다.

- **pxGrid Policy(pxGrid** 정책**)**: 클라이언트가 가입할 수 있는 사용 가능한 서비스를 나열합니다. 정책을 편집하여 해당 정책에 액세스 할 수 있는 그룹을 변경할 수 있습니다. 아직 정책이 없는 서비스에 대해 새 정책을 생성할 수도 있습니다.
- **Groups(**그룹**)**: 기본 그룹은 EPS 또는 ANC입니다. 더 많은 그룹을 추가하고 이를 사용하여 서비스에 대한 액세스를 제한할 수 있습니다.

  pxGrid 클라이언트는 REST API를 통해 사용자 이름을 전송하여 pxGrid 컨트롤러에 자체적으로 등록할 수 있습니다. pxGrid 컨트롤러는 클라이언트 등록 중에 pxGrid 클라이언트의 비밀번호를 생성합니다. 관리자는 연결 요청을 승인하거나 거부할 수 있습니다.
- **Certificates(**인증서**)**: Cisco ISE 내부 CA(Certificate Authority)를 사용하기 위해 새 인증서를 생성할 수 있습니다.

  pxGrid용 인증서를 생성하는 방법에 대한 자세한 내용은 다음을 참고하십시오.

  - Cisco pxGrid를 사용하여 인증서 구축 - Cisco ISE 2.0/2.1/2.2에 대한 자체 서명 인증서 업데이트 사용
  - Cisco pxGrid를 사용하여 인증서 구축 - Cisco ISE 2.0/2.1/2.2 업데이트와 함께 외부 CA 사용

pxGrid 정책 제어

pxGrid 클라이언트가 액세스할 수 있는 서비스에 대한 액세스를 제어하기 위해 pxGrid 권한 부여 정책을 생성할 수 있습니다. 이러한 정책은 pxGrid 클라이언트에서 사용 가능한 서비스를 제어합니다.

서로 다른 유형의 그룹을 생성하고 pxGrid 클라이언트에서 사용 가능한 서비스를 이러한 그룹에 매핑할 수 있습니다. **Client Management(**클라이언트 관리**) > Groups(**그룹**)** 창에서 **Manage Groups(**그룹 관리**)** 옵션을 사용하여 새 그룹을 추가합니다. Policies(정책) 창에서 사전 정의된 그룹(예: EPS 및 ANC)을 사용하는 사전 정의된 권한 부여 정책을 확인할 수 있습니다.

pxGrid 클라이언트에 대한 권한 부여 정책을 생성하려면 다음을 수행하십시오.

SUMMARY STEPS

1. **Administration(**관리**)**에서 **pxGrid Services(pxGrid** 서비스**) > Client Management(**클라이언트 관리**) > Policy(**정책**)**를 선택한 다음 **Add(**추가**)** 버튼을 클릭합니다.
2. **Service(**서비스**)** 드롭다운 목록에서 서비스를 선택합니다.
3. **Operation(**운영**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
4. **Groups(**그룹**)** 드롭다운 목록에서 이 서비스에 매핑할 그룹을 선택합니다.
5. **Submit(**제출**)**을 클릭합니다.

DETAILED STEPS

단계 **1** **Administration(**관리**)**에서 **pxGrid Services(pxGrid** 서비스**) > Client Management(**클라이언트 관리**) > Policy(**정책**)**를 선택한 다음 **Add(**추가**)** 버튼을 클릭합니다.

단계 **2** **Service(**서비스**)** 드롭다운 목록에서 서비스를 선택합니다.

- com.cisco.ise.radius
- come.cisco.ise.sxp
- com.cisco.ise.trustsec
- com.cisco.ise.session
- com.cisco.ise.system
- com.cisco.ise.mdm
- com.cisco.ise.config.trustsec
- com.cisco.ise.config.profiler
- com.cisco.ise.pxgrid.admin
- com.cisco.ise.config.deployment.node
- com.cisco.ise.endpoint
- com.cisco.ise.config.anc
- com.cisco.ise.dnac
- com.cisco.ise.config.upn
- com.cisco.ise.pubsub

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

- <ANY>
- publish
- publish /topic/com.cisco.ise.session
- publish /topic/com.cisco.ise.session.group
- publish /topic/com.cisco.ise.anc
- <CUSTOM> - 이 옵션을 선택하면 사용자 맞춤화 작업을 지정할 수 있습니다.

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

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

단계 **5** **Submit(**제출**)**을 클릭합니다.

pxGrid 서비스 활성화

시작하기 전에

- Cisco pxGrid 클라이언트에서 요청을 확인하려면 하나 이상의 노드에서 pxGrid 페르소나를 활성화합니다.

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

단계 **2** 클라이언트 옆의 확인란을 선택하고 **Approve(**승인**)**를 클릭합니다.

단계 **3** 최신 상태를 보려면 **Refresh(**새로 고침**)**를 클릭합니다.

단계 **4** 활성화할 기능을 선택하고 **Enable(**활성화**)**을 클릭합니다.

단계 **5** 최신 상태를 보려면 **Refresh(**새로 고침**)**를 클릭합니다.

pxGrid 진단

- XMPP: **Administration (**관리**) > pxGrid Services(pxGrid** 서비스**) > Diagnostics(**진단**) > XMPP** 페이지에 pxGrid 1.0 클라이언트(외부 및 내부)가 나열됩니다. 또한 기능도 나열됩니다.
- Websocket: **Administration (**관리**) > pxGrid Services(pxGrid** 서비스**) > Diagnostics(**진단**) > Websocket** 페이지에 pxGrid 2.0 클라이언트(외부 및 내부)가 나열됩니다. 또한 사용 가능한 pxGrid 2.0 주제와 각 주제를 게시하거나 구독하는 클라이언트도 나열됩니다.
- Log: **Administration(**관리**) > pxGrid Services(pxGrid** 서비스**) > Diagnostics(**진단**) > Live Logs(**라이브 로그**)** 페이지에 관리 이벤트가 나열됩니다.
- 테스트: **Administration(**관리**) > pxGrid Services(pxGrid** 서비스**) > Diagnostics(**진단**) > Tests(**테스트**)** 페이지에서 실행되는 상태 모니터링 테스트는 클라이언트가 세션 디렉터리 서비스에 액세스할 수 있는지 확인합니다. **Start Test(**테스트 시작**)** 버튼을 클릭하면 내부 pxGrid 2.0 클라이언트가 생성됩니다. 이 클라이언트는 대량 세션 다운로드 REST API를 쿼리한 다음 세션 주제를 구독합니다. 해당 주제를 몇 분간 수신한 후 종료됩니다. 테스트가 완료되면 테스트 활동의 로그를 표시할 수 있습니다.

pxGrid 설정

- **Automatically approve new certificate-based accounts(**새 인증서 기반 계정 자동 승인**)**: 기본적으로 꺼져 있으며, pxGrid 서버에 대한 연결을 제어할 수 있습니다. 환경의 모든 클라이언트를 신뢰하는 경우에만 이 설정을 선택하십시오.
- **Allow password based account creation(**비밀번호 기반 계정 생성 허용**)**: pxGrid 클라이언트에 대해 사용자 이름/비밀번호 기반 인증을 활성화하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 pxGrid 클라이언트가 자동으로 승인되지 않습니다.

Cisco pxGrid 인증서 생성

시작하기 전에

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

단계 **10** **Create(**생성**)**를 클릭합니다.

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

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

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

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