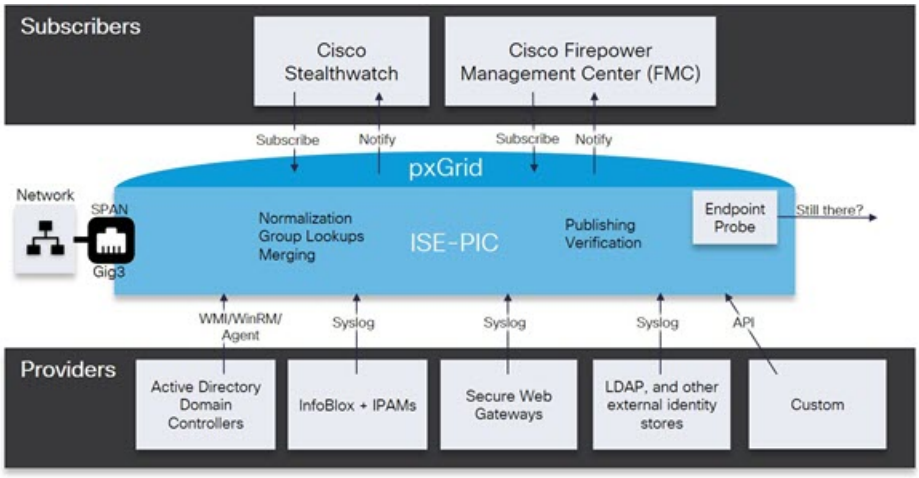
Subscribers(가입자)

ISE-PIC사용Cisco pxGrid 서비스를 사용하여 다양한 제공자로부터 수집하여 Cisco ISE-PIC 세션 디렉토리가 저장한 인증된 사용자 ID를 Cisco Stealthwatch나 Cisco FMC(Firepower Management Center) 같은 다른 네트워크 시스템으로 전달합니다.

다음 그림에서 pxGrid 노드는 외부 제공자로부터 사용자 ID를 수집합니다. 이러한 ID는 구문 분석, 매핑 및 형식화됩니다. pxGrid는 형식화된 사용자 ID를 가져와서 ISE-PIC 가입자에게 전송합니다.

그림 ***1: ISE-PIC Flow***



Cisco ISE-PIC에 연결된 가입자는 등록해야 pxGrid 서비스를 사용할 수 있습니다. 가입자는 고유한 이름과 인증서 기반 상호 인증을 사용하여 pxGrid에 로그인할 수 있습니다. 유효한 인증서를 전송하면, Cisco pxGrid 가입자는 자동으로 ISE-PIC에 의해 승인됩니다.

가입자는 pxGrid 서버 호스트 이름 또는 IP 주소에 연결할 수 있습니다. Cisco에서는 불필요한 오류를 방지하기 위해, 특히 DNS 쿼리가 올바르게 작동할 수 있도록 호스트 이름 사용을 권장합니다. 기능은 가입자가 게시 및 구독할 수 있도록 pxGrid에 생성되는 정보 토픽 또는 채널입니다. Cisco ISE-PIC에서는 SessionDirectory 및 IdentityGroup만 지원됩니다. 기능 정보는 **Capabilities(**기능**)** 탭의 **Subscribers(**가입자**)**로 이동하여 게시자로부터 게시, 직접 쿼리 또는 대량 다운로드 쿼리를 통해 사용할 수 있습니다.

가입자가 ISE-PIC에서 정보를 수신하게 하려면 다음 작업을 수행해야 합니다.

1. 선택 사항으로, 가입자 측에서 인증서를 생성합니다.
2. ISE-PIC에서 가입자를 위한 pxGrid 인증서 생성, 2 페이지 작업을 수행합니다.
3. 가입자 활성화, 3 페이지에 전달하는 고성능 고속 어플라이언스입니다. 가입자가 ISE-PIC에서 사용자 ID를 수신하게 하려면 이 단계를 수행하거나 승인을 자동으로 활성화해야 합니다. 가입자 설정 구성, 4 페이지의 내용을 참조하십시오.

가입자를 위한 pxGrid 인증서 생성

시작하기 전에

설치 시 ISE-PIC에서는 기본 ISE-PIC 노드에서 디지털 서명한 pxGrid 서비스용 자체 서명 인증서를 자동으로 생성합니다. 이후에는 pxGrid 가입자용 인증서를 생성하여 pxGrid와 가입자 간의 상호 신뢰를 보장하고, 궁극적으로는 사용자 ID가 ISE-PIC에서 가입자로 전달됩니다.

단계 **1** **Subscribers(**가입자**)**를 선택하고 **Certificates(**인증서**)** 탭으로 이동합니다.

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

- **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**):** 이 옵션을 선택하면 CN(Common Name)을 입력해야 합니다. Common Name(일반 이름) 필드에 pxGrid FQDN을 입력합니다(pxGrid는 접두사로 추가됩니다). (예: www.pxgrid-ise.ise.net) 와일드 카드를 사용할 수도 있습니다. (예: *. ise.net)
- **Generate a single certificate with a certificate signing request(**인증서 서명 요청을 사용하여 단일 인증서 생성**)**: 이 옵션을 선택하면 인증서 서명 요청 세부 정보를 입력해야 합니다.
- **Generate bulk certificates(**대량 인증서 생성**)**: 필수 세부 사항을 포함하는 CSV 파일을 업로드할 수 있습니다.
- **Download Root Certificate Chain(**루트 인증서 체인 다운로드**)**: ISE 공용 루트 인증서를 다운로드하여 pxGrid 클라이언트의 신뢰할 수 있는 인증서 저장소에 추가합니다. ISE pxGrid 노드는 새로 서명한 pxGrid 클라이언트 인증서만 신뢰하며 반대의 경우도 마찬가지라, 외부 인증 기관을 이용하지 않아도 됩니다.

단계 **3** (선택 사항) 이 인증서에 대한 설명을 입력합니다.

단계 **4** 이 인증서가 기반으로 하는 pxGrid 인증서 템플릿을 보거나 수정합니다. 인증서 템플릿은 해당 템플릿을 기준으로 CA(Certificate Authority)에서 발급한 모든 인증서에 일반적인 속성을 포함합니다. 인증서 템플릿은 사용해야 하는 주체, SAN(Subject Alternative Name), 키 크기, SCEP RA 프로파일, 인증서의 유효 기간, 그리고 클라이언트 또는 서버 인증이나 두 인증에 모두 인증서를 사용해야 하는지 여부를 지정하는 EKU(Extended Key Usage: 확장 키 사용)를 정의합니다. 내부 Cisco ISE CA(ISE CA)는 인증서 템플릿을 사용하여 해당 템플릿을 기준으로 인증서를 발급합니다. PxGrid의 경우 Passive Identity(패시브 ID) 서비스를 사용할 때는 pxGrid 인증서 템플릿만 사용할 수 있으며, 이

템플릿에서는 Subject(주체) 정보만 수정할 수 있습니다. 이 템플릿을 수정하려면 다음을 선택합니다. **Certificates(**인증서**)** > **Certificate Templates(**인증서 템플릿**)Administration(**관리**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Templates(**인증서 템플릿**)**.

단계 **5** SAN(대체 주체 이름)을 지정합니다. 여러 SAN을 추가해도 됩니다. 다음 옵션을 사용할 수 있습니다.

- **FQDN**: ISE 노드의 정규화된 도메인 이름을 입력합니다. (예: www.isepic.ise.net) FQDN에 와일드 카드를 사용할 수도 있습니다. (예: *. ise.net)

  pxGrid FQDN을 입력할 수 있는 FQDN용 추가 회선을 추가할 수 있습니다. Common Name(일반 이름) 필드에 사용한 FQDN과 동일해야 합니다.

- **IP address(IP** 주소**)**: 인증서에 연결할 ISE 노드의 IP 주소를 입력합니다. 가입자가 FQDN 대신 IP 주소를 사용한다면 이 정보를 반드시 입력해야 합니다.

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

단계 **6** **Certificate Download Format(**인증서 다운로드 형식**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)(PEM(Private Enhanced Electronic Mail)** 형식의 인증서**, PKCS8 PEM** 형식의 키**(**인증서 체인 포함**))**: 루트 인증서, 중간 CA 인증서 및 최종 엔티티 인증서는 PEM 형식으로 표시됩니다. PEM 형식 인증서는 BASE64 인코딩 ASCII 파일입니다. 각 인증서는 "--------BEGIN CERTIFICATE-----" 태그로 시작하고 "-------END CERTIFICATE----" 태그로 끝납니다. 최종 엔티티의 개인 키는 PKCS * PEM을 사용하여 저장됩니다. "-----BEGIN ENCRYPTED PRIVATE KEY----" 태그로 시작하고 "-----END ENCRYPTED PRIVATE KEY----" 태그로 끝납니다.

- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)(PKCS12** 형식**(**인증서 체인 포함**,** 인증서 체인과 모두를 위한 단일 파일**))**: 루트 CA 인증서, 중간 CA 인증서, 최종 엔티티의 인증서 및 개인 키를 단일 암호화 파일에 저장하는 이진 형식입니다.

단계 **7** 인증서 비밀번호를 입력합니다.

단계 **8** **Create(**생성**)**를 클릭합니다.

가입자 활성화

가입자가 Cisco ISEISE-PIC에서 사용자 ID를 수신하려면 이 작업을 수행하거나 승인을 자동으로 활성화해야 합니다. 가입자 설정 구성, 4 페이지의 내용을 참조하십시오.

단계 **1** 다음 메뉴를 선택합니다. **Subscribers(**가입자**)** 그런 다음 **Clients(**클라이언트**)** 탭이 표시되는지 확인합니다.

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

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

Live Logs(라이브 로그)에서 가입자 이벤트 보기

Live Logs(라이브 로그) 페이지에는 모든 가입자 이벤트가 표시됩니다. 이벤트 정보에는 이벤트 유형 및 타임스탬프와 함께 가입자 및 기능 이름이 포함됩니다.

이벤트 목록을 확인하려면 **Subscribers(**가입자**)** 로 이동하고 **Live Log(**라이브 로그**)** 탭을 선택합니다. 로그를 지우고 목록을 다시 동기화하거나 새로 고칠 수도 있습니다.

가입자 설정 구성

단계 **1** **Subscribers(**가입자**)**를 선택하고 **Settings(**설정**)** 탭을 선택합니다.

단계 **2** 요건에 따라 다음 옵션을 선택합니다.

- Automatically Approve New Accounts(새 계정 자동 승인)—새 pxGrid 클라이언트의 연결 요청을 자동으로 승인하려면 이 확인란을 선택합니다.
- Allow Password Based Account Creation(암호 기반 계정 생성 허용)—pxGrid 클라이언트에 대해 사용자 이름/암호 기반 인증을 활성화하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 pxGrid 클라이언트를 자동으로 승인할 수 없습니다.

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

단계 **3** **Save(**저장**)**를 클릭합니다.