Cisco에서 인증서 관리 ISE-PIC

인증서는 개인, 서버, 회사 또는 다른 엔터티를 식별하고 엔터티를 공용 키에 연결하는 전자 문서입니다. PKI(Public Key Infrastructure)는 보안 통신을 수행할 수 있도록 하고 디지털 서명을 사용 중인 사용자의 신원을 확인하는 암호화 기술입니다. 인증서는 네트워크에서 보안 액세스를 제공하기 위해 사용됩니다. 인증서는 자체 서명되거나 외부 CA(Certificate Authority)에 의해 디지털 서명될 수 있습니다. 자체 서명된 인증서는 자체 생성자가 서명합니다. CA 서명 디지털 인증서는 업계 표준이며 더 안전한 것으로 간주됩니다. ISE-PIC는 pxGrid 가입자의 pxGrid 인증서에 디지털 서명을 하는 pxGrid의 외부 CA 역할을 할 수 있습니다.

Cisco ISE-PIC는 노드 간 통신 (각 노드가 서로 통신하기 위해 다른 노드에 인증서를 제공함) 및 pxGrid (ISE-PIC 및 pxGrid가 서로에게 인증서를 제공함)와 통신하는 데 인증서를 사용합니다. 이러한 두 가지 목적을 위해 노드 당 하나의 인증서를 생성할 수 있습니다. 인증서는 pxGrid에 대한 Cisco ISE 노드를 식별하고 pxGrid와 Cisco ISE 노드 간 통신을 보호합니다.

설치시 ISE-PIC는 각 ISE-PIC 노드에 대해 자체 서명된 인증서(설치 중에 관리자가 기본 노드에서 자동으로 보조 노드에 대해 생성된 인증서를 수락하라는 메시지가 표시됨) 및 기본 ISE-PIC 노드에서 디지털 서명한 pxGrid 서비스에 대한 인증서를 자동으로 생성합니다. 이후에는 pxGrid 가입자용 인증서를 생성하여 pxGrid와 가입자 간의 상호 신뢰를 보장하고, 궁극적으로는 사용자 ID가 ISE-PIC에서 가입자로 전달됩니다. ISE-PIC의 인증서 메뉴를 사용하여 인증서를 보고, 추가 ISE-PIC 인증서를 생성하고, 몇 가지 고급 작업을 수행할 수 있습니다.

참고 관리자는 엔터프라이즈 인증서를 사용할 수 있지만, ISE-PIC는 가입자에 대한 pxGrid 인증서 발급에 내부 권한을 사용하도록 기본적으로 설계되었습니다.

Cisco ISE-PIC에서 인증서 매칭

구축에서 Cisco ISE-PIC 노드를 설정할 때 이 두 노드는 서로 통신합니다. 시스템은 각 ISE-PIC 노드의 FQDN이 일치하는지 확인합니다(예: ise1.cisco.com 및 ise2.cisco.com 또는 와일드 카드 인증서를 사용하는 경우 *.cisco.com). 또한 외부 시스템이 ISE-PIC 서버에 인증서를 제공하면 인증을 위해 제공되는 외부 인증서가 ISE-PIC 서버의 인증서와 비교하여 확인됩니다. 두 인증서가 일치하면 인증이 성공합니다.

Cisco ISE-PIC에서는 다음과 같이 일치하는 주체 이름을 확인합니다.

1. Cisco ISE-PIC에서 인증서의 SAN(Subject Alternative Name) 확장을 확인합니다. SAN에 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. SAN에 DNS 이름이 없거나 SAN이 완전히 누락된 경우, 인증서의 Subject(주체) 필드에 있는 CN(Common Name) 또는 인증서의 Subject(주체) 필드에 있는 와일드카드 도메인을 노드의 FQDN과 일치시켜야 합니다.
3. 일치 항목이 발견되지 않으면 인증서가 거부됩니다.

와일드카드 인증서

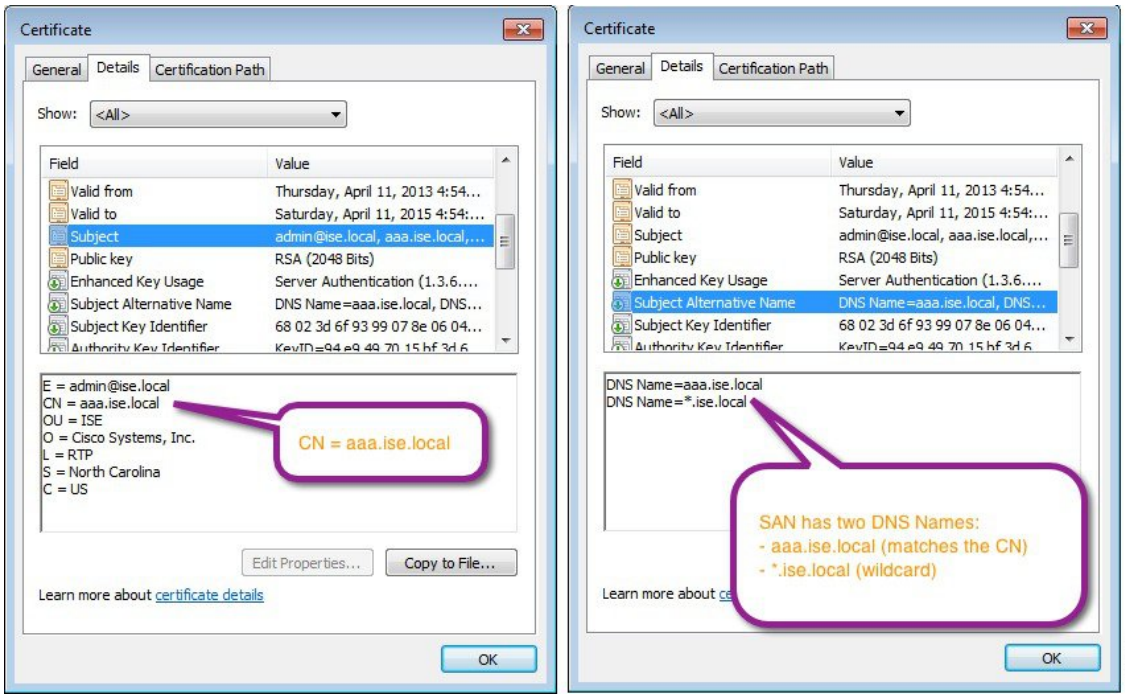
와일드카드 인증서는 와일드카드 표기법(별표 및 도메인 이름 앞의 마침표)을 사용하므로 조직의 여러 호스트 간에 인증서를 공유할 수 있습니다. 예를 들어 인증서 주체의 CN 값은 aaa.ise.local과 같은 일반 호스트 이름이고, SAN 필드에는 동일한 일반 호스트 이름과 함께 DNS.1=aaa.ise.local 및 DNS.2=*.ise.local과 같은 와일드카드 표기법이 포함된다고 가정합니다.

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

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

다음 그림에는 웹 사이트를 보호하는 데 사용되는 와일드카드 인증서의 예가 나와 있습니다.

그림 *1:* 와일드카드 인증서 예



SAN 필드에 별표(*)를 사용하면 단일 인증서를 두 노드와 공유할 수 있으며(두 노드를 설치한 경우) 인증서 이름 불일치 경고가 표시되지 않습니다. 그러나 와일드카드 인증서를 사용하는 방식은 각 Cisco ISE 노드용으로 고유한 서버 인증서를 각각 할당하는 방식보다 보안성이 낮은 것으로 간주됩니다.

참고 FQDN의 일부 예는 전체 ISE 설치에서 가져온 것이므로 ISE-PIC 설치와 관련된 주소와 다를 수 있습니다.

와일드카드 인증서를 사용하는 경우의 이점

- 비용 절감. 타사 인증 기관이 서명하는 인증서는 비용이 많이 드는데 서버 수가 증가할수록 더욱 그렇습니다. 와일드카드 인증서는 Cisco ISE 구축의 여러 노드에서 사용할 수 있습니다.
- 운영 효율성. 와일드카드 인증서를 사용하면 모든 PSN(Policy Service Node) EAP 및 웹 서비스에서 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 인증 기관이 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 서버 인증서 신뢰가 활성화되어 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 인증서와 관련된 몇 가지 보안 고려 사항입니다.

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

와일드카드 인증서는 SE 노드 기준의 고유 서버 인증서보다 보안성이 낮은 것으로 간주됩니다. 그러나 보안 위험 문제보다 비용 및 다른 작동 요소의 이점이 훨씬 큽니다.

ASA와 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(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.

의ISE-PIC 인증서 계층 구조

ISE-PIC에서 모든 인증서의 인증서 계층 구조 또는 인증서 신뢰 체인을 확인할 수 있습니다. 인증서 계층 구조에는 인증서, 모든 중간 CA(Certificate Authority) 인증서 및 루트 인증서가 포함됩니다. 예를 들어 ISE-PIC에서 시스템 인증서를 보도록 선택하면 기본적으로 해당 시스템 인증서의 세부사항이 표시됩니다. 인증서 계층은 인증서의 상단에 나타납니다. 계층 구조에서 인증서를 클릭하면 해당 세부사항을 볼 수 있습니다. 셀프 서명 인증서에는 계층 구조 또는 신뢰 체인이 없습니다.

인증서 목록 페이지의 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-PIC 시스템 인증서는 구축의 다른 노드 및 클라이언트 애플리케이션에 대해 Cisco ISE-PIC 노드를 식별하는 서버 인증서입니다. 시스템 인증서에 액세스하려면 **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다. 시스템 인증서는 다음과 같이 사용됩니다.

- Cisco ISE-PIC 구축에서 노드 간 통신에 사용됩니다. Usage(사용) 필드에서 이러한 인증서에 대한 Admin(관리) 옵션을 선택합니다.
- pxGrid 컨트롤러와의 통신에 사용됩니다. Usage(사용) 필드에서 이러한 인증서에 대한 pxGrid 옵션을 선택합니다.

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

- 관리 및 pxGrid용으로 지정된 자체 서명 서버 인증서(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 릴리스에 대해 지원되는 키 및 암호 정보를 찾으려면 Cisco Identity Services Engine 네트워크 구성 요소 호환성 설명서의 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 CSR 제출, 18 페이지
2. 신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 15 페이지
3. CSR에 CA 서명 인증서 바인딩, 18 페이지

시스템 인증서 보기

시스템 인증서 페이지에는 Cisco ISE-PIC에 추가된 모든 시스템 인증서가 나열됩니다.

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

시스템 인증서 페이지가 표시되고 로컬 인증서에 대해 다음 정보가 제공됩니다.

- 식별 이름 - 인증서의 이름입니다.
- 사용 대상 - 이 인증서가 사용되는 서비스입니다.
- 포털 그룹 태그 - 포털에서 사용하도록 지정된 인증서에만 해당되며, 포털에 사용해야 하는 인증서를 지정합니다.
- 발급 대상 - 인증서 주체의 일반 이름입니다.
- 발급자 - 인증서 발급자의 일반 이름입니다.
- 유효 기간 시작 - 인증서가 생성된 날짜이며 Not Before 인증서 특성이라고도 합니다.
- 만료 날짜 - 인증서의 만료 날짜이며 Not After 인증서 특성이라고도 합니다. 인증서가 만료되는 시기를 나타냅니다. 여기에는 5개 범주가 연결된 아이콘과 함께 표시됩니다.

- 만료 날짜까지 남은 기간이 90일을 초과함(녹색 아이콘)
- 90일 이내에 만료됨(파란색 아이콘)
- 60일 이내에 만료됨(노란색 아이콘)
- 30일 이내에 만료됨(주황색 아이콘)
- 만료됨(빨간색 아이콘)

단계 **2** 인증서를 선택하고 보기 를 선택하여 인증서 세부 사항을 표시합니다.

시스템 인증서 가져오기

관리 포털에서 Cisco ISE-PIC 노드의 시스템 인증서를 가져올 수 있습니다.

참고 기본 PAN에서 관리 역할 인증서의 인증서를 변경하면 다른 모든 노드에서 서비스가 재시작됩니다. PAN(Primary Administration Node)에서 다시 시작이 완료된 후 한 번에 한 노드씩 시스템이 다시 시작됩니다.

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(**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.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

단계 **2** **Import(**가져오기**)**를 클릭합니다.
Import Server Certificate(서버 인증서 가져오기) 화면이 열립니다.

단계 **3** 가져올 인증서에 대한 값을 입력합니다.

단계 **4** 제출을 클릭합니다.

셀프 서명 인증서 생성

셀프 서명 인증서를 생성하여 새 로컬 인증서를 추가할 수 있습니다. 내부 테스트 및 평가에 필요한 셀프 서명 인증서만 사용하는 것이 좋습니다. 생산 환경에서 Cisco ISE-PIC를 구축하려는 경우에는 생산 네트워크 전체에서 보다 동일하게 수락될 수 있도록 가능하면 항상 CA 서명 인증서를 사용해야 합니다.

참고 셀프 서명 인증서를 사용 중일 때 Cisco ISE-PIC 노드의 호스트 이름을 변경해야 하는 경우에는 Cisco ISE-PIC 노드의 에 로그인하여 이전 호스트 이름이 지정된 셀프 서명 인증서를 삭제한 다음 새 셀프 서명 인증서를 생성해야 합니다. 이렇게 하지 않으면 Cisco ISE-PIC는 이전 호스트 이름이 지정된 셀프 서명 인증서를 계속 사용합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

단계 **2** **Generate Self Signed Certificate(**셀프 서명 인증서 생성**)**를 클릭하고 셀프 서명 인증서 생성 페이지에서 세부사항을 입력합니다.

단계 **3** 셀프 서명 와일드카드 인증서, 즉 주체 이름의 일반 이름 및/또는 주체 대체 이름의 DNS 이름에 별표(*)가 포함된 인증서를 생성하려면 **Allow Wildcard Certificates(**와일드카드 인증서 허용**)** 확인란을 선택합니다. 예를 들어 SAN에 할당되는 DNS 이름이 *.amer.cisco.com일 수 있습니다.

단계 **4** 이 인증서를 사용하려는 서비스를 기준으로 **Usage(**사용**)** 영역의 확인란을 선택합니다.

단계 **5** **Submit(**제출**)**을 클릭하여 인증서를 생성합니다.

보조 노드를 다시 시작하려면 CLI에서 다음 명령을 지정된 순서로 입력합니다.

a) **application stop ise**
b) **application start ise**

시스템 인증서 편집

이 페이지를 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.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **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**)** 체크 박스를 선택하고 만료 TTL(Time to Live)를 일, 주, 월 또는 연도 단위로 입력합니다.

단계 **4** **Save**(저장)를 클릭하여 변경 사항을 저장합니다.

Admin(관리**)** 확인란을 선택하면 Cisco ISE-PIC 노드의 애플리케이션 서버가 다시 시작됩니다.

참고 Chrome 65 이상을 사용하여 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. 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 ISE GUI에서 새 자체 서명 인증서를 생성합니다. DNS 및 IP 주소를 모두 입력해야 합니다.

2. 이제 ISE 서비스가 다시 시작됩니다.

3. Chrome 브라우저에서 포털을 리디렉션합니다.

4. 브라우저에서 View Certificate(인증서보기)>Details(세부 사항)>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 운영 체제 Win RS4 또는 RS5에서 브라우저 Firefox 64 이상에 대해 무선 BYOD 설정을 구성할 때 인증서 예외를 추가하지 못할 수 있습니다. 이 동작은 Firefox 64 이상을 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/이중 PEAP 또는 TLS를 구성합니다.

2. Windows ALL 옵션을 사용해 CP 정책을 구성합니다.

3. 엔드 클라이언트 Windows RS4/RS5에서 Dot1.x/MAB SSID를 연결합니다.

4. 게스트/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 해결하려면 옵션 > 프라이버시 및 설정 > 인증서 보기 > 서버 > 예외 추가로 이동하여 Firefox 64용 인증서를 수동으로 추가해야 합니다.

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 인증에 사용할 수 있는 인증서가 하나 이상 있어야 합니다. 또한 관리 또는 pxGrid 컨트롤러에 사용되는 인증서는 삭제할 수 없습니다. 단, 서비스를 비활성화하는 경우 pxGrid 인증서는 삭제할 수 있습니다.

와일드카드 인증서를 삭제하도록 선택하는 경우에는 구축의 모든 노드에서 인증서가 제거됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **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

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

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

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 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-PIC 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 프라이버시 향상 메일 형식으로 인증서가 저장됩니다. 인증서와 개인 키를 모두 내보내는 경우에는 프라이버시 향상 메일 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.

X.509 인증서는 특정 날짜까지만 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.

- 시스템 인증서 페이지에 색상이 지정된 만료 상태 아이콘이 나타납니다.
- Cisco ISE 시스템 진단 보고서에 만료 메시지가 나타납니다.
- 만료 전 90일과 60일, 그리고 마지막 30일 동안에는 매일 만료 경보가 생성됩니다.

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

Cisco ISE는 다음과 같은 용도로 신뢰할 수 있는 인증서를 사용합니다.

- 인증서 기반 관리자 인증을 사용하여 ISE-PIC에 액세스하는 Cisco ISE 관리자 및 엔드포인트에서 인증을 위해 사용하는 클라이언트 인증서 확인
- 구축에 있는 Cisco ISE-PIC 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.

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 시퀀스)이 포함된 파일은 특정 제한 사항에 따라 가져올 수 있습니다.
- 공개 와일드카드 인증서를 게스트 포털에 할당하고 루트 CA 인증서가 포함된 하위 CA를 가져오는 경우 ISE 서비스가 재시작될 때까지 인증서 체인이 전송되지 않습니다.

설치시 신뢰할 수 있는 인증서 저장소가 자동으로 생성된 신뢰할 수 있는 인증서로 채워집니다. 루트 인증서(Cisco 루트 CA)는 Manufacturing (Cisco CA Manufacturing) 인증서에 서명합니다.

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 주체 대체 이름 필드 값에 대한 네임스페이스를 정의합니다. Cisco ISE는 루트 인증서에 지정된 제한을 확인하지 않습니다.

지원되는 이름 제한은 다음과 같습니다.

- 디렉토리 이름

  주체/SAN의 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)

지원되지 않는 이름 제한은 다음과 같습니다.

- IP 주소
- 기타 이름

Cisco ISE는 지원되지 않는 제한을 확인할 수 없으므로, 신뢰할 수 있는 인증서에 포함된 제한이 지원되지 않으며 확인 중인 인증서에 적절한 필드가 포함되어 있지 않으면 해당 인증서는 거부됩니다.

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 저장소 인증서 보기

신뢰할 수 있는 인증서 페이지에는 Cisco ISE-PIC에 추가된 모든 신뢰할 수 있는 인증서가 나열됩니다.

모든 인증서를 보려면 Choose(선택) **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다. 신뢰할 수 있는 인증서 페이지가 표시되고 신뢰할 수 있는 인증서가 모두 나열됩니다.

신뢰할 수 있는 인증서 저장소의 상태 변경

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

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**.

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

단계 **3** 상태를 변경합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

신뢰할 수 있는 인증서 저장소에 인증서 추가

인증서 저장소 페이지에서 Cisco ISE-PIC에 CA 인증서를 추가할 수 있습니다.

시작하기 전에

- 브라우저를 실행 중인 컴퓨터의 파일 시스템에 인증서 저장소 인증서가 있는지 확인합니다. 인증서는 PEM 또는 DER 형식이어야 합니다.
- 관리자 또는 EAP 인증용으로 인증서를 사용하려는 경우 인증서에 기본 제한이 정의되어 있으며 CA 플래그가 true로 설정되어 있는지 확인합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** 필요한 대로 필드 값을 구성합니다.

EAP 인증 또는 인증 기반 관리자 인증용으로 인증서 체인의 하위 CA 인증서를 사용하려는 경우 인증서 체인에서 루트 CA까지의 모든 인증서를 가져오는 동안 **Trust for client authentication and Syslog(**클라이언트 인증 및 **Syslog** 신뢰**)** 확인란이 선택되어 있어야 합니다. Cisco ISE 2.6 패치 1 이상에서 동일한 주체 이름을 가진 CA 인증서를 둘 이상 가져올 수 있습니다. 인증서 기반 관리자 인증의 경우 신뢰할 수 있는 인증서를 추가 할 때 **Trust for certificate based admin authentication(**인증서 기반 관리자 인증 신뢰**)** 확인란을 선택합니다. 저장소에 주체 이름이 동일한 다른 인증서가 있고 **Trust for certificate based admin authentication(**인증서 기반 관리자 인증에 대한 신뢰**)** 확인란이 활성화되어 있으면 신뢰할 수 있는 저장소의 인증서에 대한 **Trust for certificate based admin authentication(**인증서 기반 관리자 인증에 대한 신뢰**)** 옵션을 수정할 수 없습니다.

인증 유형을 비밀번호 기반 인증에서 인증서 기반 인증으로 변경하면 Cisco ISE-PIC는 구축의 각 노드에서 애플리케이션 서버를 재시작합니다. 이때 PAN.

신뢰할 수 있는 인증서 편집

신뢰할 수 있는 인증서 저장소에 추가한 인증서는 설정 편집을 사용하여 추가로 편집할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

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

단계 **3** 편집 가능한 필드를 필요한 대로 수정합니다.

단계 **4** **Save(**저장**)**를 클릭하여 인증서 저장소에 대한 변경사항을 저장합니다.

신뢰할 수 있는 인증서 삭제

더 이상 필요하지 않은 신뢰할 수 있는 인증서는 삭제할 수 있습니다. 그러나 ISE-PIC 내부 CA(Certificate Authority) 인증서는 삭제하면 안 됩니다. ISE-PIC 내부 CA 인증서는 전체 구축에 대해 ISE-PIC 루트 인증서 체인을 교체할 때만 삭제할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

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

경고 메시지가 표시됩니다. ISE-PIC 내부 CA 인증서를 삭제하도록 선택한 경우 다음을 클릭합니다.

- **Delete(**삭제**)** - ISE-PIC 내부 CA 인증서를 삭제합니다. 이 경우 ISE-PIC 내부 CA가 서명한 모든 엔드포인트 인증서는 무효화되며 엔드포인트가 네트워크에 연결할 수 없게 됩니다. 엔드포인트가 네트워크에 다시 연결할 수 있도록 하려면 같은 ISE-PIC 내부 CA 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다.
- **Delete & Revoke(**삭제 및 취소**)** - ISE-PIC 내부 CA 인증서를 삭제 및 취소합니다. 이 경우 ISE-PIC 내부 CA가 서명한 모든 엔드포인트 인증서는 무효화되며 엔드포인트가 네트워크에 연결할 수 없게 됩니다. 이 작업은 취소할 수 없으며, 전체 구축에 대해 ISE-PIC 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. 자세한 내용은 Cisco ISE CA 인증서 및 키 내보내기, 31 페이지를 참조하십시오.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다. 인증서는 한 번에 하나씩만 내보낼 수 있습니다.

단계 **3** 클라이언트 브라우저를 실행 중인 파일 시스템에 프라이버시가 강화된 메일 파일을 저장합니다.

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

CSR에 서명을 했으며 디지털 서명 CA 인증서를 반환한 인증 기관의 루트 인증서 및 기타 중간 인증서가 있어야 합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** 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 **4** **Friendly Name**을 입력합니다.

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

단계 **5** 이 신뢰할 수 있는 인증서를 사용할 서비스 옆의 확인란을 선택합니다.

단계 **6** (선택 사항) **Description(**설명**)** 필드에 인증서 설명을 입력합니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

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

인증서 체인 가져오기

인증서 저장소에서 수신한 인증서 체인이 들어 있는 단일 파일에서 여러 인증서를 가져올 수 있습니다. 파일의 모든 인증서는 PEM(Privacy-Enhanced Mail) 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. 관리 포털의 신뢰할 수 있는 인증서 저장소로 인증서 체인 파일을 가져옵니다. 이 작업은 마지막 인증서를 제외한 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.

신뢰할 수 있는 인증서 가져오기 설정

다음 표에서는 Cisco ISE-PIC에 CA(Certificate Authority) 인증서를 추가하는 데 사용할 수 있는 신뢰할 수 있는 인증서 가져오기 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** > **Import**가져오기.

표 *1:* 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 ISE-PIC는 <common name> 형식으로 이름을 자동으로 생성합니다.#<issuer>#<nnnnn>, 여기서 <nnnnn>은 고유한 5자리 숫자입니다.
Trust for authentication within ISE(ISE 내의 인증 신뢰**)**	다른 ISE-PIC 노드 또는 LDAP 서버의 서버 인증서를 확인하는 데 이 인증서를 사용하려면 확인란을 선택합니다.

필드 이름	설명
Trust for client authentication and Syslog(클라이언트 인증 및 **Syslog** 신뢰**)**	(Trust for authentication within ISE-PIC(ISE 내의 인증 신뢰) 확인란을 선택하는 경우에만 해당함) 다음 용도로 이 인증서를 사용하려는 경우 확인란을 선택합니다. • EAP 프로토콜을 사용하여 ISE-PIC에 연결하는 엔드포인트 인증 • Syslog 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, 10 페이지
인증서 체인 가져오기, 16 페이지
신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 15 페이지

인증서 서명 요청

서명된 인증서를 발급하는 CA(Certificate Authority)의 경우 CSR(Certificate Signing Request)을 생성하고 CA에 제출해야 합니다.

생성한 CSR(Certificate Signing Requests) 목록은 인증서 서명 요청 페이지에서 사용할 수 있습니다. CA(Certificate Authority)에서 서명을 받으려면 CSR을 내보낸 다음 인증서를 CA로 보내야 합니다. CA는 인증서에 서명한 다음 반환합니다.

관리 포털을 통해 중앙에서 인증서를 관리할 수 있습니다. 구축 환경의 모든 노드에 사용할 CSR을 생성하고 내보낼 수 있습니다. 그런 다음 CSR을 CA에 제출하고, CA에서 CA 서명 인증서를 받고, CA에서 반환된 루트 및 중간 CA 인증서를 신뢰할 수 있는 인증서 저장소로 가져온 다음 CA 서명 인증서를 CSR에 바인딩해야 합니다.

인증서 서명 요청을 생성하고 인증 기관에 CSR 제출

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

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

단계 2 CSR 생성을 위한 값을 입력합니다. 각 필드에 대한 자세한 내용은 인증서 서명 요청 설정을 참조하십시오.

단계 3 **Generate(**생성**)**를 클릭하여 CSR을 생성합니다.

CSR이 생성됩니다.

단계 4 **Export(**내보내기**)**를 클릭하여 메모장에서 CSR을 엽니다.

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-PIC 신뢰할 수 있는 인증서 저장소에 추가해야 합니다. 디지털 서명된 CA 인증서, 루트 CA 인증서 및 기타 중간 CA 인증서(해당하는 경우)가 클라이언트 브라우저를 실행 중인 로컬 시스템에 다운로드됩니다.

CSR에 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(**Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서)로 가져옵니다. .

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

CSR을 CA 서명 인증서에 바인딩할 노드 옆의 확인란을 선택합니다.

단계 2 **Bind(**바인딩**)**를 클릭합니다.

단계 3 **Browse(**찾아보기**)**를 클릭하여 CA 서명 인증서를 선택합니다.

단계 4 인증서의 식별 이름을 지정합니다.

단계 **5** Cisco **ISE**가 인증서 확장명을 검증하도록 하려면 ISE-PIC 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 ISE는 EAP-TLS 클라이언트 인증서가 있어야 디지털 서명 키 사용 확장명을 보유할 수 있습니다.

단계 **6** 사용 영역에서 이 인증서를 사용할 서비스를 확인합니다.

CSR을 생성하는 중에 Usage(사용) 옵션을 활성화한 경우 이 정보는 자동으로 채워집니다. 인증서를 바인딩할 때 사용을 지정하지 않으려면 Usage(사용) 옵션을 선택 취소해 주십시오. 나중에 인증서를 편집하여 사용을 지정할 수 있습니다.

참고 기본 PAN에서 관리 역할 인증서의 인증서를 변경하면 다른 모든 노드에서 서비스가 재시작됩니다.

기본 PAN에서 관리 역할 인증서의 인증서를 변경하면 다른 모든 노드에서 서비스가 재시작됩니다. PAN(Primary Administration Node)에서 다시 시작이 완료된 후 한 번에 한 노드씩 시스템이 다시 시작됩니다.

단계 **7** **Submit(**제출**)**을 클릭하여 CA 서명 인증서를 바인딩합니다.

Cisco ISE-PIC 노드 간 통신에 이 인증서를 사용하도록 선택한 경우에는 Cisco ISE-PIC 노드의 애플리케이션 서버가 다시 시작됩니다.

이 프로세스를 반복하여 다른 노드에서 CSR을 CA 서명 인증서와 바인딩합니다.

다음에 수행할 작업

신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 15 페이지

인증서 서명 요청 내보내기

이 페이지를 사용하여 인증서 서명 요청을 내보낼 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)** 다.

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

단계 **3** **OK(**확인**)**를 클릭하여 클라이언트 브라우저를 실행 중인 파일 시스템에 파일을 저장합니다.

인증서 서명 요청 설정

Cisco ISE-PIC에서는 관리 포털에서 단일 요청으로 구축의 노드에 대한 CSR을 생성할 수 있습니다. 또한 선택적으로 구축의 단일 노드 또는 노드에 대한 CSR도 생성할 수 있습니다. 여러 노드에 대한 CSR을 생성하도록 선택하는 경우 ISE는 인증서 주체의 CN= 필드에서 특정 노드의 FQDN(Fully Qualified Domain Name)을 자동으로 대체합니다. 인증서의 SAN(대체 주체 이름) 필드에 항목을 포함

하도록 선택하는 경우 다른 SAN 특성과 함께 ISE-PIC 노드의 FQDN을 입력해야 합니다. 구축의 노드에 대해 CSR을 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-PIC 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 노드 에 걸쳐 단일 인증서를 공유할 수 있으며, 인증서 이름 불일치 경고가 표시되지 않습니다. 그러나 와일드카드 인증서를 사용하는 방식은 각 Cisco ISE-PIC 노드용으로 고유한 서버 인증서를 할당하는 방식보다 보안성이 낮은 것으로 간주됩니다.

다음 표에서는 CSR(Certificate Signing Request) 페이지의 필드에 대해 설명합니다. 이 페이지는 CA(Certificate Authority)에 의해 서명될 수 있는 CSR을 생성하는 데 사용할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Signing Requests(**인증서 서명 요청**)**.

표 *2:* 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)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-PIC 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) • **ISE Messaging Service(ISE** 메시징 서비스**)**: Cisco ISE 메시징을 통한 시스템 로그 기능에서 사용되며, 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) • **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) Extended Key

필드	사용 지침

	참고 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
	• **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)**: (ISE-PIC가 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, Certificate Authority
	  • 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-PIC OCSP 응답자 인증서를 갱신하는 데 사용됩니다(및 인증서 서명 요청이 아님). 보안을 위해 ISE-PIC 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.

필드	사용 지침
Common Name(공통 이름**) (CN)**	기본적으로 공통 이름은 CSR을 생성하는 ISE-PIC 노드의 FQDN입니다. $FQDN$은 ISE-PIC 노드의 FQDN을 나타냅니다. 구축의 여러 노드에 대해 CSR을 생성하는 경우 CSR의 Common Name(공통 이름) 필드가 해당 ISE 노드의 FQDNdmfh 대체됩니다.
Organizational Unit (OU)(OU(조직 단위**))**	조직 단위의 이름입니다. Engineering 등을 예로 들 수 있습니다.
Organization (O)(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)(ST(시/도**))**	(약어로 표기하지 않음) 시/도의 이름입니다. California 등을 예로 들 수 있습니다.
Country(국가**) (C)**	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-PIC 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-PIC 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
키 유형	공개 키를 생성하는 데 사용할 알고리즘을 RSA 또는 ECDSA로 지정합니다.

필드	사용 지침
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 FIPS 호환 정책 관리 시스템으로 Cisco ISE-PIC를 구축하려면 2048 이상을 선택합니다.
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.

Cisco ISE CA 서비스

인증서는 자체 서명되거나 외부 CA(Certificate Authority)에 의해 디지털 서명될 수 있습니다. ISE-PIC는 pxGrid 인증서에 디지털 서명을 하는 pxGrid의 외부 인증서 기관(CA) 역할을 할 수 있습니다. CA 서명 디지털 인증서는 업계 표준으로 보안성이 더 높은 것으로 간주됩니다. ISE-PIC CA는 다음과 같은 기능을 제공합니다.

- Certificate Issuance: 네트워크에 연결되는 엔드포인트에 대한 CSR(Certificate Signing Requests)을 검증하고 서명합니다.
- Key Management: 키와 인증서를.
- 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 비활성화 된 상태로 표시하는 것이 가장 좋습니다. 이는 알려진 Cisco ISE 문제입니다.

Elliptical Curve Cryptography 인증서 지원

Cisco ISE-PIC 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 테이블에서는 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 ISE-PIC는 다음과 같은 ECC 커브 유형을 지원합니다. 커브 유형 또는 키 크기가 클수록 보안이 우수합니다.

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

ISE-PIC는 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.

인증서 프로비저닝 포털에서 ECC 인증서를 생성할 수 있습니다.

Cisco ISE-PIC Certificate Authority 인증서

CA(인증기관) 인증서 페이지에는 내부 Cisco ISE-PIC CA와 관련된 모든 인증서가 나열됩니다. 이러한 인증서는 이 페이지에 노드별로 나열됩니다. 노드를 펼쳐서 해당 특정 노드의 모든 ISE-PIC 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-PIC CA 서비스를 활성화하면 이러한 인증서가 생성되어 모든 노드에 자동으로 설치됩니다. 또한 전체 ISE-PIC 루트 CA 체인을 교체하면 이러한 인증서가 재생성되어 모든 노드에 자동으로 설치됩니다. 수동 개입이 필요하지 않습니다.

Cisco ISE-PIC 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-PIC CA 인증서의 편집, 가져오기, 내보내기, 삭제 및 보기가 가능합니다.

Cisco ISE-PIC CA 인증서 편집

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

단계 **1**

단계 **2** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Authority Certificates(**인증 기관 인증서**)**.

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

단계 **4** 편집 가능한 필드를 필요한 대로 수정합니다. 필드에 대한 설명은 인증서 설정 편집을 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** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Authority Certificates(**인증 기관 인증서**)**.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다. 인증서는 한 번에 하나씩만 내보낼 수 있습니다.

단계 **3** 클라이언트 브라우저를 실행 중인 파일 시스템에 프라이버시가 강화된 메일 파일을 저장합니다.

Cisco ISE-PIC CA 인증서 가져오기

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

시작하기 전에

- 엔드포인트 인증서가 서명된 구축에서 ISE-PIC 루트 CA, 노드 CA 및 엔드포인트 하위 CA 인증서를 내보낸 다음 브라우저를 실행 중인 컴퓨터의 파일 시스템에 저장합니다.

단계 **1**

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

단계 **3** **Import(**가져오기**)**를 클릭합니다.

단계 **4** 필요한 대로 필드 값을 구성합니다. 자세한 내용은 신뢰할 수 있는 인증서 가져오기 설정을 참조하십시오.

클라이언트 인증서 기반 인증이 활성화되어 있으면 Cisco ISE-PIC는 구축의 각 노드에서 애플리케이션 서버를 다시 시작합니다. 이때 PAN에서 애플리케이션 서버부터 시작한 다음 .

인증서 설정 편집

다음 표에서는 CA(Certificate Authority) 인증서 특성을 편집하는 데 사용할 수 있는 인증서 저장소 인증서 편집 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** > **Certificate(**인증서**)** > **Edit(**편집**)**.

표 ***3:*** 인증서 저장소 편집 설정

필드 이름	사용 지침
인증서 발급자	
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다.
상태	Enabled(활성화됨) 또는 Disabled(비활성화됨)를 선택합니다. Disabled(비활성화됨)를 선택하면 ISE가 신뢰를 설정하는 데 인증서를 사용하지 않습니다.
설명	필요에 따라 설명을 입력합니다.
사용	
Trust for authentication within ISE(ISE 내의 인증 신뢰**)**	이 인증서가 다른 ISE 노드 또는 LDAP 서버의 서버 인증서를 확인하도록 하려면 확인란을 선택합니다.

필드 이름	사용 지침
Trust for client authentication and Syslog(클라이언트 인증 및 **Syslog** 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 • Syslog 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**)**	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 ISE로 다운로드할 수 있는 CRL(Certificate Revocation List)과 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**)**	OCSP에서 인증서 상태를 확인할 수 없는 경우 요청을 거부하려면 확인란을 선택합니다. 이 확인란을 선택하면 OCSP 서비스에서 알 수 없는 상태 값을 반환하면 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 ISE가 요청을 거부하도록 하려면 체크 박스를 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 체크 박스를 선택합니다. Cisco ISE가 CRL 파일에서 Effective Date(유효 날짜) 필드의 시작일과 Next Update(다음 업데이트) 필드의 만료 날짜를 확인하도록 하려면 이 체크 박스의 선택을 취소합니다. CRL이 아직 활성화되지 않았거나 만료된 경우에는 이 CA가 서명을 한 인증서를 사용하는 모든 인증은 거부됩니다.

관련 항목

신뢰할 수 있는 인증서 저장소, 10 페이지
신뢰할 수 있는 인증서 편집, 14 페이지

Cisco ISE-PIC CA 인증서 및 키 백업 및 복원

Cisco ISE-PIC 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 복원할 수 있습니다. Cisco ISE-PIC 컨피그레이션 백업에는 CA 인증서 및 키가 포함되지 않습니다. 대신 CLI(Command Line Interface)를 사용하여 CA 인증서 및 키를 리포지토리로 내보냈다가 가져와야 합니다. 제공 **application configure ise** 명령에는 이제 CA 인증서 및 키를 백업하고 복원할 수 있는 export 및 import 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-PIC CA 루트 체인을 바꾸는 경우
- 외부 PKI의 하위 CA 역할을 하도록 Cisco ISE-PIC 루트 CA를 구성하는 경우
- 컨피그레이션 백업에서 데이터를 복원하는 경우. 이 경우에는 먼저 Cisco ISE-PIC 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 리포지토리를 생성했는지 확인합니다.

단계 **1** 입력 **application configure ise** 명령을 사용하여 CPU 및 메모리 크기를 확인할 수 있습니다.

단계 **2** 입력 7 그런 다음 인증서와 키를 내보냅니다.

단계 **3** 리포지토리 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-PIC CA 인증서 및 키 가져오기

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

단계 **1** 입력 **application configure ise** 을 Cisco ISE-PIC CLI에서 입력합니다.

단계 **2** 입력 8 그런 다음 CA 인증서와 키를 가져옵니다.

단계 **3** 리포지토리 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... ISE Certificate Authority 서비스 시작 중... ISE CA 키 가져오기가 완료되었습니다.
```

기본 PAN 및 PSN에서

구축을 설정할 때 Cisco ISE-PIC는 Cisco ISE CA 서비스용으로 노드. 그러나 노드의 또는 PSN의 도메인 이름이나 호스트 이름을 변경할 때는 기본 PAN에서 루트 CA를, PSN에서 하위 CA를 각각 재생성해야 합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **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.

다음에 수행할 작업

구축에 보조 PAN이 있는 경우 기본 PAN에서 Cisco ISE-PIC CA 인증서와 키의 백업을 가져온 다음 보조 PAN에서 복원합니다. 그러면 기본 PAN 장애 시 보조 PAN이 루트 CA로 작동할 수 있으며, 이 경우 보조 PAN을 기본 PAN으로 승격합니다.

외부 PKI의 하위 CA로 Cisco ISE-PIC 루트 CA 구성

기본 PAN의 루트 CA가 외부 PKI의 하위 CA로 작동하도록 하려면 ISE-PIC 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 노드은 외부 CA의 하위 CA이며 PSN은 노드의 하위 CA입니다.

단계 1 **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.

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 타임아웃(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** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **OCSP Client Profile(OCSP** 클라이언트 프로파일**)**.

단계 **2** 값을 입력하여 OCSP 클라이언트 프로파일을 추가합니다.

단계 **3** 제출을 클릭합니다.

OCSP 통계 카운터

Cisco ISE는 OCSP 카운터를 사용하여 OCSP 서버의 데이터와 상태를 기록하고 모니터링합니다. 5분마다 기록됩니다. Cisco ISE는 syslog 메시지를 모니터링 노드로 보내며, 이 메시지는 로컬 저장소에 보존됩니다. 로컬 저장소에는 지난 5분 동안의 데이터가 포함되어 있습니다. Cisco ISE가 syslog 메시지를 보내고 나면 다음 간격에 대해 카운터가 다시 계산됩니다. 즉, 5분이 지나면 새로운 5분 시간 간격이 다시 시작됩니다.

다음 표에는 OCSP syslog 메시지와 해당 설명이 나와 있습니다.

표 ***4: OCSP syslog*** 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