인증서

인증서 요구 사항 및 사전 요건

지원되는 도메인

모든

사용자 역할

관리자

네트워크 관리자

Secure Firewall Threat Defense VPN 인증서 가이드라인 및 제한 사항

- PKI 등록 개체가 연결된 후 디바이스에 설치되면 인증서 등록 프로세스가 즉시 시작됩니다. 이 프로세스는 자체 서명 및 SCEP 등록 유형의 경우 자동으로 진행되므로, 관리자의 추가 작업이 필요하지 않습니다. 수동 인증서 등록에는 관리자의 작업이 필요합니다.

- 인증서 등록이 완료되면 디바이스에 인증서 등록 개체와 이름이 동일한 트러스트 포인트가 존재하게 됩니다. 이 트러스트 포인트를 VPN 인증 방법의 컨피그레이션에서 사용하십시오.
- threat defense 디바이스는 Microsoft CA 서비스, Cisco Adaptive Security Appliance 및 Cisco IOS Router에서 제공하는 CA 서비스를 사용한 인증서 등록을 지원합니다.
- threat defense 디바이스는 CA(Certificate Authority)로 구성할 수 없습니다.

인증서 관리 도메인 및 디바이스에 대한 지침

- 인증서 등록은 하위 또는 상위 도메인에서 수행할 수 있습니다.
- 상위 도메인에서 등록이 완료되면 동일한 도메인에 인증서 등록 개체가 포함되어야 합니다. 디바이스의 트러스트 포인트가 하위 도메인에 오버라이드된 경우, 오버라이드된 값이 디바이스에 구축됩니다.
- 리프 도메인의 디바이스에 인증서 등록이 완료되면 상위 도메인 및 다른 하위 도메인에 표시됩니다. 추가 인증서를 추가할 수 있습니다.
- 리프 도메인을 삭제하면 포함된 디바이스의 인증서 등록이 자동으로 제거됩니다.
- 디바이스에 한 도메인의 인증서가 등록되면 다른 도메인에서도 등록이 허용됩니다. 인증서가 다른 도메인에 추가될 수 있습니다.
- 한 도메인에서 디바이스를 이동하면 인증서도 이동됩니다. 디바이스에서 등록을 제거하면 알림을 받게 됩니다.

Threat Defense 인증서 매핑

디지털 인증서의 소개는 PKI 인프라 및 디지털 인증서을 참조하십시오.

관리되는 디바이스에서 인증서를 가져오고 등록하는 데 사용되는 개체에 대한 설명은 인증서 등록 개체을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Certificates(**인증서**)**을(를) 선택합니다.

이 화면에 나열된 각 디바이스에 대해 다음 열을 볼 수 있습니다.

- **Name(**이름**)** - 이미 관련된 트러스트 포인트가 있는 디바이스를 나열합니다. 연결된 트러스트 포인트 목록을 보려면 디바이스를 확장합니다.
- **Domain(**도메인**)** - 특정 도메인에 등록된 인증서가 표시됩니다.
- **Enrollment Type(**등록 유형**)** - 트러스트 포인트에 사용된 등록 유형을 표시합니다.
- **Status(**상태**)** - **CA** 인증서 및 **ID** 인증서의 상태를 제공합니다. 인증서 내용이 사용 가능일 때 돋보기를 클릭하여 볼 수 있습니다.

CA 인증서 정보를 볼 때 CA 인증서를 발급한 모든 인증 기관의 계층 구조를 볼 수 있습니다.

등록이 실패한 경우 오류 메시지를 보려면 상태를 클릭합니다.

- 인증서에서 약한 암호 사용을 활성화하려면 오른쪽에서 **Enable weak-crypto(**약한 암호화 활성화**)**를 클릭합니다. 토글 버튼을 클릭하면 약한 암호를 활성화하기 전에 확인하라는 경고가 표시됩니다. 약한 암호를 활성화하려면 **Yes(**예**)**를 클릭합니다.

  참고 약한 암호 사용으로 인해 인증서 등록이 실패하면 약한 암호화를 활성화하라는 메시지가 표시됩니다. 약한 암호화를 사용해야 하는 경우 약한 암호를 활성화하도록 선택할 수 있습니다.

- 추가 열에는 다음 작업을 수행하는 아이콘이 나열됩니다.
  - **Export Certificate(**인증서 내보내기**)** - 인증서의 복사본을 내보내고 다운로드하려면 클릭합니다. PKCS12(전체 인증서 체인) 또는 PEM(ID 인증서 전용) 형식을 내보내도록 선택할 수 있습니다.

    나중에 파일을 가져오려면 PKCS12 인증서 형식을 내보내려면 암호를 제공해야 합니다.
  - **Re-enroll certificate(**인증서 다시 등록**)** - 기존 인증서를 다시 등록합니다.
  - **Refresh certificate status(**인증서 상태 새로 고침**)** - 인증서를 새로 고쳐 Firepower Threat Defense 디바이스 인증서 상태를 Firepower Management Center와 동기화합니다.
  - **Delete certificate(**인증서 삭제**)** - 트러스트 포인트에 대한 모든 연결된 인증서를 삭제합니다.

단계 **2** 디바이스에 등록된 개체를 연결하고 설치하려면 **(+)** 추가를 선택합니다.

인증서 등록 개체가 연결된 후 디바이스에 설치되면 인증 등록 프로세스가 즉시 시작됩니다. 이 프로세스는 자체 서명 및 SCEP 등록 유형의 경우 자동으로 진행되므로, 관리자의 추가 작업이 필요하지 않습니다. 수동 인증서 등록에는 관리자의 추가 작업이 필요합니다.

참고 디바이스의 인증서 등록은 사용자 인터페이스를 차단하지 않으며 등록 프로세스는 백그라운드에서 실행되므로 사용자가 다른 디바이스에서 동시에 인증서 등록을 수행할 수 있습니다. 이런 병렬 작업의 진행 상황은 동일한 사용자 인터페이스에서 모니터링할 수 있습니다. 해당 아이콘은 인증서 등록 상태를 표시합니다.

관련 항목

자체 서명 등록을 사용한 인증서 설치 , 5 페이지
SCEP 등록을 사용한 인증서 설치, 7 페이지
수동 등록을 사용한 인증서 설치, 8 페이지
PKCS12 파일을 사용하여 인증서 설치, 9 페이지

CA 번들 자동 업데이트

CLI 명령을 통해 CA 인증서를 자동으로 업데이트하도록 관리 센터를 설정할 수 있습니다. 기본적으로 CA 인증서는 버전 7.0.5를 설치하거나 버전으로 업그레이드할 때 자동으로 업데이트됩니다.

참고 IPv6 전용 구축에서는 일부 Cisco 서버가 IPv6을 지원하지 않기 때문에 CA 인증서의 자동 업데이트가 실패할 수 있습니다. 이 경우 **configure cert-update run-now force** 명령을 사용하여 CA 인증서를 강제로 업데이트합니다.

프로시저

단계 **1** SSH를 사용하여 FMC CLI에 로그인하거나(가상인 경우) VM 콘솔을 엽니다.

단계 **2** 로컬 시스템의 CA 인증서가 최신 버전인지 확인할 수 있습니다.

configure cert-update test

이 명령은 로컬 시스템의 CA 번들을 Cisco 서버의 최신 CA 번들과 비교합니다. CA 번들이 최신 버전이면 연결 확인이 실행되지 않으며 테스트 결과가 아래와 같이 표시됩니다.

예제:

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

CA 번들이 최신 상태가 아닌 경우 다운로드한 CA 번들에서 연결 확인이 실행되고 테스트 결과가 표시됩니다.

예제:

연결 확인이 실패하는 경우:

```
> configure cert-update test
Test failed, not able to fully connect.
```

예제:

연결 확인이 성공하거나 CA 번들이 이미 최신 상태인 경우:

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

단계 **3** (선택 사항) CA 번들을 즉시 업데이트하려면 다음을 수행합니다.

configure cert-update run-now

예제:

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

이 명령을 실행하면 Cisco 서버의 CA 인증서에서 SSL 연결이 확인됩니다. Cisco 서버 중 하나라도 SSL 연결 확인에 실패하면 프로세스가 종료됩니다.

예제:

```
> configure cert-update run-now
Certs failed some connection checks.
```

연결 실패에도 불구하고 업데이트를 계속 진행하려면 **force** 키워드를 사용합니다.

예제:

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

단계 **4** CA 번들을 자동으로 업데이트하지 않으려면 구성을 비활성화합니다.

configure cert-update auto-update disable

예제:

```
> configure cert-update auto-update disable
Autoupdate is disabled
```

단계 **5** CA 번들의 자동 업데이트를 다시 활성화하려면 다음을 수행합니다.

configure cert-update auto-update enable

예제:

```
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

CA 인증서에서 자동 업데이트를 활성화하면 시스템에서 정의한 시간에 업데이트 프로세스가 매일 실행됩니다.

단계 **6** (선택 사항) CA 인증서의 자동 업데이트 상태를 확인합니다.

show cert-update

예제:

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

자체 서명 등록을 사용한 인증서 설치

프로시저

단계 **1** 장치 > 인증서 화면에서 새 인증서 추가 대화 상자를 열려면 추가를 선택합니다.

단계 **2** 디바이스 드롭다운 목록에서 디바이스를 선택합니다.

단계 **3** 다음 방법 중 하나로 인증서 등록 객체를 이 디바이스와 연결합니다.

- 드롭다운 목록에서 자체 서명 인증서 유형의 인증서 등록 개체를 선택합니다.
- 새 인증서 등록 개체를 추가하려면 **(+)**을 클릭합니다. 인증서 등록 개체 추가를 참조하십시오.

단계 **4** 추가를 누르면 자체 서명된 자동 등록 프로세스가 시작됩니다.

자체 서명된 등록 유형의 트러스트 포인트의 경우 **CA** 인증서 상태가 항상 표시되며 관리되는 디바이스는 자체 CA로 작동하여 자체 ID를 생성하는 CA 인증서가 필요하지 않습니다.

디바이스가 자체 서명된 ID 인증서를 생성하면 **ID** 인증서는 InProgress에서 Available 상태로 변경됩니다.

단계 **5** 이 장치에 대해 생성된 자체 서명된 ID 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

등록이 완료되면 디바이스에 동일한 이름의 트러스트 포인트가 인증서 등록 개체로 존재하게 됩니다. 설정 시 사이트 간 원격 VPN 인증 방법으로 이 트러스트 포인트를 사용하십시오.

EST 등록을 사용한 인증서 설치

시작하기 전에

참고 EST 등록을 사용할 경우 매니지드 디바이스와 CA 서버 간에 직접 연결이 설정됩니다. 등록 프로세스를 시작하기 전에 디바이스가 CA 서버에 연결되었는지 확인하십시오.

참고 EST의 인증서 만료시 디바이스를 자동 등록하는 기능은 지원되지 않습니다.

프로시저

단계 **1** **Devices > Certificates(**디바이스 > 인증서**)** 화면에서 **Add New Certificate(**새 인증서 추가**)** 대화 상자를 열려면 **Add(**추가**)**를 선택합니다.

단계 **2** 디바이스 드롭다운 목록에서 디바이스를 선택합니다.

단계 **3** 다음 방법 중 하나로 인증서 등록 객체를 이 디바이스와 연결합니다.

- **Cert Enrollment(**인증서 등록**)** 드롭다운 목록에서 EST 인증서 등록 개체를 선택합니다.
- **(+)**를 클릭하고 새 인증서 등록 개체를 추가하려면 인증서 등록 개체 추가을 참조하십시오.

단계 **4** **Add(**추가**)**를 클릭하여 디바이스에 인증서를 등록합니다.

ID 인증서는 디바이스가 특정 CA에서 EST를 사용해 ID 인증서를 가져오므로 `InProgress`에서 `Available` 상태로 변경됩니다. 경우에 따라 ID 인증서를 가져오기 위해 수동 갱신이 필요할 수 있습니다.

단계 **5** 이 장치에 생성되고 설치된 ID 인증서를 보려면 돋보기를 클릭합니다.

SCEP 등록을 사용한 인증서 설치

시작하기 전에

참고 SCEP 등록을 사용할 경우 매니지드 디바이스와 CA 서버 간에 직접 연결이 설정됩니다. 등록 프로세스를 시작하기 전에 디바이스가 CA 서버에 연결되었는지 확인하십시오.

프로시저

단계 **1** 장치 > 인증서 화면에서 새 인증서 추가 대화 상자를 열려면 추가를 선택합니다.

단계 **2** 디바이스 드롭다운 목록에서 디바이스를 선택합니다.

단계 **3** 다음 방법 중 하나로 인증서 등록 객체를 이 디바이스와 연결합니다.

- 드롭다운 목록에서 SCEP 유형의 인증서 등록 개체를 선택합니다.
- 새 인증서 등록 개체를 추가하려면 **(+)**을 클릭합니다. 인증서 등록 개체 추가를 참조하십시오.

단계 **4** **Add(**추가**)**를 누르면 자동 등록 프로세스가 시작됩니다.

SCEP 등록 유형 트러스트 포인트의 경우 CA 서버에서 CA 인증서를 가져와 디바이스에 설치하므로 **CA** 인증서 상태가 InProgress에서 Available로 전환됩니다.

Identity Certificate(ID 인증서**)**는 디바이스가 특정 CA에서 SCEP를 사용해 ID 인증서를 가져오므로 `InProgress`에서 `Available` 상태로 변경됩니다. 경우에 따라 ID 인증서를 가져오기 위해 수동 갱신이 필요할 수 있습니다.

단계 **5** 이 장치에 생성되고 설치된 ID 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

등록이 완료되면 디바이스에 동일한 이름의 트러스트 포인트가 인증서 등록 개체로 존재하게 됩니다. 설정 시 사이트 간 원격 VPN 인증 방법으로 이 트러스트 포인트를 사용하십시오.

EST 등록을 사용한 인증서 설치

시작하기 전에

참고 EST 등록을 사용할 경우 매니지드 디바이스와 CA 서버 간에 직접 연결이 설정됩니다. 등록 프로세스를 시작하기 전에 디바이스가 CA 서버에 연결되었는지 확인하십시오.

참고 EST의 인증서 만료시 디바이스를 자동 등록하는 기능은 지원되지 않습니다.

프로시저

단계 **1** **Devices** > **Certificates(**디바이스 > 인증서**)** 화면에서 **Add New Certificate(**새 인증서 추가**)** 대화 상자를 열려면 **Add(**추가**)**를 선택합니다.

단계 **2** 디바이스 드롭다운 목록에서 디바이스를 선택합니다.

단계 **3** 다음 방법 중 하나로 인증서 등록 객체를 이 디바이스와 연결합니다.

- **Cert Enrollment(**인증서 등록**)** 드롭다운 목록에서 EST 인증서 등록 개체를 선택합니다.
- **(+)**를 클릭하고 새 인증서 등록 개체를 추가하려면 인증서 등록 개체 추가을 참조하십시오.

단계 **4** **Add(**추가**)**를 클릭하여 디바이스에 인증서를 등록합니다.

ID 인증서는 디바이스가 특정 CA에서 EST를 사용해 ID 인증서를 가져오므로 `InProgress`에서 `Available` 상태로 변경됩니다. 경우에 따라 ID 인증서를 가져오기 위해 수동 갱신이 필요할 수 있습니다.

단계 **5** 이 장치에 생성되고 설치된 ID 인증서를 보려면 돋보기를 클릭합니다.

수동 등록을 사용한 인증서 설치

프로시저

단계 **1** 장치 > 인증서 화면에서 새 인증서 추가 대화 상자를 열려면 추가를 선택합니다.

단계 **2** 디바이스 드롭다운 목록에서 디바이스를 선택합니다.

단계 **3** 다음 방법 중 하나로 인증서 등록 객체를 이 디바이스와 연결합니다.

- 드롭다운 목록에서 수동 유형의 인증서 등록 개체를 선택합니다.

- 새 인증서 등록 개체를 추가하려면 **(+)**을 클릭합니다. 인증서 등록 개체 추가를 참조하십시오.

단계 **4** 추가를 누르면 등록 프로세스가 시작됩니다.

단계 **5** ID 인증서를 가져오기 위해 PKI CA 서버에서 적절한 작업을 실행합니다.

a) CSR을 보고 복사하려면 **Identity Certificate(ID** 인증서**)** 경고를 클릭합니다.

b) CRS을 사용해 ID 인증서를 가져오기 위해 PKI CA 서버에서 적절한 작업을 실행합니다.

이러한 작업은 Secure Firewall Management Center 또는 관리되는 디바이스와는 완전히 별개입니다. 완료되면 관리되는 디바이스에 대한 ID 인증서가 생성됩니다. 파일에 저장할 수 있습니다.

c) 수동 프로세스를 완료하려면 가져온 ID 인증서를 관리되는 디바이스에 설치합니다.

Secure Firewall Management Center 대화 상자로 돌아가 **ID** 인증서 검색을 선택하여 ID 인증서 파일을 선택합니다.

단계 **6** ID 인증서를 가져오려면 가져오기를 선택합니다.

가져오기가 완료되면 ID 인증서 상태는 `Available`이 됩니다.

단계 **7** 장치에 대한 **ID** 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

등록이 완료되면 디바이스에 동일한 이름의 트러스트 포인트가 인증서 등록 개체로 존재하게 됩니다. 설정 시 사이트 간 원격 VPN 인증 방법으로 이 트러스트 포인트를 사용하십시오.

PKCS12 파일을 사용하여 인증서 설치

프로시저

단계 **1** 장치 > 인증서 화면에서 새 인증서 추가 대화 상자를 열려면 추가를 선택합니다.

단계 **2** 디바이스 드롭다운 목록에서 사전 구성된 관리되는 디바이스를 선택합니다.

단계 **3** 다음 방법 중 하나로 인증서 등록 객체를 이 디바이스와 연결합니다.

- 드롭다운 목록에서 PKCS 유형의 인증서 등록 개체를 선택합니다.
- **(+)**를 클릭하고 새 인증서 등록 개체를 추가하려면 인증서 등록 개체 추가을 참조하십시오.

단계 **4** 추가를 누릅니다.

CA 인증서 및 ID 인증서 상태는 PKCS12 파일이 디바이스에 설치됨에 따라 `In Progress`(진행 중)에서 `Available`(사용 가능)으로 전환됩니다.

참고 PKCS12 파일을 처음 업로드할 때 파일은 CertEnrollment 개체의 일부러 Firepower Management Center에 저장됩니다. 잘못된 암호 또는 실패한 구축으로 등록이 실패하는 경우 파일을 다시 업로드하지 않고 PKCS12 인증서 등록을 다시 시도합니다. PKCS12 파일 크기는 24K를 초과하지 않아야 합니다.

단계 **5** 사용 가능 상태에서 장치에 대한 ID 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

관리되는 디바이스의 인증서(트러스트 포인트)는 PKCS#12 파일과 동일합니다. VPN 인증 설정에서 이 인증서를 사용합니다.

Threat Defense 인증서 문제 해결

인증서 등록 환경의 차이로 인해 문제가 발생했는지 여부는 Secure Firewall Threat Defense VPN 인증서 가이드라인 및 제한 사항, 1 페이지을 참조하십시오. 다음을 확인합니다.

- 디바이스에서 CA 서버에 대한 경로가 있는지 확인합니다.

  CA 서버의 호스트 이름이 등록 개체에 지정된 경우 Flex Config를 사용해 서버에 적절히 연결하는 DNS를 구성합니다. CA 서버의 IP 주소를 사용해도 됩니다.

- Microsoft 2012 CA 서버를 사용하는 경우 관리되는 디바이스에서 기본 IPsec 템플릿을 허용하지 않으므로 변경해야 합니다.

  작업 템플릿을 구성하려면 MS CA 설명서를 참조하여 다음 단계를 따르십시오.

  1. IPsec(오프라인 요청) 템플릿을 복제합니다.
  2. **Extensions(**확장**) > Application policies(**애플리케이션 정책**)**에서 *IP security IKE intermediate(IP* 보안 *IKE* 중급*)* 대신 *IP security end system(IP* 보안 최종 시스템*)*을 선택합니다.
  3. 권한 및 템플릿 이름을 설정합니다.
  4. 새 템플릿을 추가하고 새 템플릿 이름을 반영하기 위해 레지스트리 설정을 변경합니다.

- management center에서 threat defense 디바이스와 관련된 다음 상태 알림을 받을 수 있습니다.

  ```
  코드 - F0853; 설명 - 기본 키 링의 인증서가 유효하지 않습니다. 이유: 만료됨
  ```

  이 경우 다음 명령을 사용하여 CLISH CLI에서 기본 인증서를 다시 생성합니다.

  ```
  > system support regenerate-security-keyring default
  ```