인증서

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다. 다음 주제에서는 인증서를 생성하고 관리하는 방법에 대해 설명합니다.

인증서 정보

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. 디지털 인증서는 사용자 또는 디바이스의 공개 키 사본 하나도 포함합니다. 인증서는 HTTPS 및 LDAPS와 같은 SSL(Secure Socket Layer), TLS(Transport Layer) 및 DTLS(Datagram TLS) 연결에 사용됩니다.

다음과 같은 인증서 유형을 생성할 수 있습니다.

- 내부 인증서 — 내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명 인증서를 생성할 수도 있습니다.
- 내부 CA(Certificate Authority) 인증서 — 내부 CA 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다. 이러한 인증서는 OpenSSL 툴킷을 사용하여 직접 생성하거나 인증 기관에서 받을 수 있습니다. 자체 서명된 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다.
- 신뢰할 수 있는 CA(Certificate Authority) 인증서 — 신뢰할 수 있는 CA 인증서는 다른 인증서에 서명하는 데 사용됩니다. 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.

CA(인증 증명)는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 컨텍스트에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다. CA는 VeriSign과 같이 신뢰받는 서드파티

이거나, 조직 내에서 설정한 전용 (내부) CA일 수 있습니다. CA는 인증서 요청을 관리하고 디지털 인증서를 발급하는 기능을 담당합니다. 자세한 내용은 공개 키 암호화, 2 페이지를 참고하십시오.

공개 키 암호화

RSA 암호화 시스템과 같은 공개 키 암호 방식에서는 각 사용자가 공개 키와 개인 키로 구성된 키 쌍을 갖습니다. 키는 상호 보완적 역할을 하는데, 둘 중 하나의 키로 암호화된 것은 다른 하나의 키를 사용하여 해독할 수 있습니다.

간단하게 설명하자면, 개인 키를 사용하여 데이터를 암호화할 때 서명이 생성됩니다. 이 서명이 데이터에 첨부되어 수신자에게 전송됩니다. 수신자는 발신자의 공개 키를 데이터에 적용합니다. 데이터와 함께 보내진 서명이 공개 키를 데이터에 적용한 결과와 일치하면 메시지가 유효한 것으로 확인됩니다.

이 프로세스에서는 수신자가 발신자의 공개 키 사본을 가지고 있어야 하며 이 키가 발신자를 가장하는 누군가가 아닌 발신자 본인의 것이어야 합니다.

발신자의 공개 키를 취득하는 것은 대개 외부에서 이루어지거나 설치 시 수행되는 어떤 작업을 통해 이루어집니다. 예를 들어, 대부분의 웹 브라우저는 기본적으로 여러 CA의 루트 인증서가 구성되어 있습니다.

openssl.org, Wikipedia 또는 기타 출처를 통해 디지털 인증서와 공개 키 암호화에 대해 자세히 알아볼 수 있습니다. SSL/TLS 암호화에 대해 숙지하면 디바이스에 대한 보안 연결을 쉽게 설정할 수 있습니다.

기능에 사용되는 인증서 유형

각 기능에 대해 적절한 유형의 인증서를 생성해야 합니다. 인증서가 필요한 기능은 다음과 같습니다.

ID 정책**(**캡티브 포털**) -** 내부 인증서

(선택 사항). 캡티브 포털은 ID 정책에 사용됩니다. 사용자는 신원을 증명하고 IP 주소를 사용자 이름과 연결하기 위해 디바이스에 인증할 때 이 인증서를 수락해야 합니다. 인증서를 제공하지 않으면 디바이스는 자동으로 생성된 인증서를 사용합니다.

ID 영역**(ID** 정책 및 원격 액세스 **VPN) -** 신뢰할 수 있는 **CA** 인증서

(선택 사항). 디렉터리 서버에 암호화된 연결을 사용하는 경우 디렉터리 서버 인증을 수행하려면 인증서를 허용해야 합니다. 사용자는 ID 및 원격 액세스 VPN 정책에 따라 메시지가 표시되면 인증을 해야 합니다. 디렉터리 서버에 대해 암호화를 사용하지 않는 경우에는 인증서가 필요하지 않습니다.

관리 웹 서버**(**관리 액세스 시스템 설정**)** — 내부 인증서

(선택 사항.) Device Manager는 웹 기반 애플리케이션으로, 웹 서버에서 실행됩니다. 브라우저에서 유효한 것으로 승인한 인증서를 업로드하면 신뢰할 수 없는 기관 경고를 피할 수 있습니다.

원격 액세스 **VPN -** 내부 인증서

(필수) 내부 인증서는 Secure Client가 디바이스에 대해 연결을 생성할 때 AnyConnect 클라이언트에 대해 디바이스 ID를 설정하는 외부 인터페이스용입니다. 클라이언트는 이 인증서를 허용해야 합니다.

Site-to-Site VPN - 내부 및 신뢰할 수 있는 **CA** 인증서

사이트 대 사이트 VPN 연결에 인증서 인증을 사용하는 경우 연결에서 로컬 피어 인증에 사용하는 내부 ID 인증서를 선택해야 합니다. 이 인증서가 VPN 연결 정의의 일부는 아니지만, 시스템에서 피어를 인증할 수 있도록 로컬 및 원격 피어 ID 인증서에 서명하는 데 사용한 신뢰할 수 있는 CA 인증서도 업로드해야 합니다.

SSL 암호 해독 정책 — 내부**,** 내부 **CA** 및 신뢰할 수 있는 **CA** 인증서 및 인증서 그룹

(필수) SSL 암호 해독 정책은 다음 목적을 위해 인증서를 사용합니다.

- 내부 인증서는 알려진 키 암호 해독 규칙에 사용됩니다.
- 내부 CA 인증서는 클라이언트와 threat defense 디바이스 사이에 세션을 생성할 때 암호 해독 재서명 규칙에 사용됩니다.
- 신뢰할 수 있는 CA 인증서는 threat defense 디바이스와 서버 사이에 세션을 생성할 때 암호 해독 재서명 규칙에 간접적으로 사용됩니다. 신뢰할 수 있는 CA 인증서는 서버 인증서의 서명 기관을 확인하는 데 사용됩니다. 이러한 인증서를 직접 구성하거나 정책 설정의 인증서 그룹에서 구성할 수 있습니다. 시스템에는 CTA(Cisco-Trusted-Authorities)에서 수집된 신뢰할 수 있는 CA 인증서가 많이 포함되어 있으므로 추가 인증서를 업로드할 필요가 없을 수도 있습니다.

예: **OpenSSL**을 사용하여 내부 인증서 생성

다음 예에서는 OpenSSL 명령을 사용하여 내부 서버 인증서를 생성합니다. OpenSSL은 openssl.org에서 다운로드할 수 있습니다. 구체적인 정보는 OpenSSL 설명서를 참조하십시오. 이 예에서 사용되는 명령은 변경될 수 있으며 사용하려는 옵션이 아닌 다른 옵션이 제공될 수도 있습니다.

이 절차에서는 threat defense에 업로드할 인증서를 얻는 방법을 대략 파악할 수 있습니다.

참고 여기에 표시되어 있는 OpenSSL 명령은 예로만 제공됩니다. 파라미터는 보안 요건에 맞게 조정하십시오.

프로시저

단계 **1** 키를 생성합니다.

```
openssl genrsa -out server.key 4096
```

단계 **2** CSR(인증서 서명 요청)을 생성합니다.

```
openssl req -new -key server.key -out server.csr
```

단계 **3** 키와 CSR을 사용하여 셀프 서명한 인증서를 생성합니다.

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

device manager는 암호화된 키를 지원하지 않으므로, 셀프 서명한 인증서를 생성할 때는 Return 키를 눌러 생성 과정에서 비밀번호를 입력하라는 메시지를 건너뜁니다.

단계 **4** device manager에서 내부 인증서 개체를 생성할 때 적절한 필드에 파일을 업로드합니다.

파일 내용을 복사하여 붙여 넣을 수도 있습니다. 샘플 명령은 다음 파일을 생성합니다.

- server.crt - 내용을 서버 인증서 필드에 업로드하거나 붙여 넣습니다.
- server.key - 내용을 인증서 키 필드에 업로드하거나 붙여 넣습니다. 키를 생성할 때 비밀번호를 입력한 경우에는 다음 명령을 사용하여 암호 해독할 수 있습니다. 출력은 stdout으로 전송되며, 여기서 출력 내용을 복사할 수 있습니다.

  ```
  openssl rsa -in server.key -check
  ```

인증서 구성

Threat Defense는 PEM 또는 DER 형식의 X509 인증서를 지원합니다. 필요한 경우 OpenSSL을 사용하여 인증서를 생성하거나, 신뢰할 수 있는 인증 증명에서 인증서를 받거나, 자체 서명 인증서를 생성합니다.

인증서에 대한 자세한 내용은 인증서 정보, 1 페이지를 참조하십시오.

각 기능에 사용되는 유형에 대한 자세한 내용은 기능에 사용되는 인증서 유형, 2 페이지를 참고하십시오.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 새 인증서 생성 링크를 클릭하여 인증서 속성을 수정하면서 인증서 개체를 생성할 수도 있습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Certificates(**인증서**)**를 차례로 선택합니다.

시스템에는 다음과 같은 사전 정의된 인증서가 제공되며 이러한 인증서는 있는 그대로 사용하거나 대체할 수 있습니다.

- DefaultInternalCertificate
- DefaultWebserverCertificate
- NGFW-Default-InternalCA

시스템에는 서드파티 인증 증명에서 제공되는 수많은 신뢰할 수 있는 CA 인증서도 포함됩니다. 이러한 인증서는 Decrypt Re-Sign(암호 해독 재서명) 작업을 위한 SSL 암호 해독 정책에서 사용됩니다. CTA(Cisco-Trusted-Authorities) 그룹은 이러한 인증서를 모두 포함하며 SSL 암호 해독 정책에서 사용하는 기본 그룹입니다.

사전 정의된 검색 필터를 클릭하여 목록을 **System-defined(**시스템 정의**)** 또는 **User-defined(**사용자 정의**)** 인증서로 제한할 수 있습니다. 또한 **Weak Key(**약한 키**)** 필터를 사용하여 키가 권장 최소 길이보다 짧은 인증서를 찾을 수 있습니다. 이러한 인증서는 더 긴 키가 있는 인증서로 교체하는 것이 좋습니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 인증서 개체를 생성하려면 **+** 메뉴에서 인증서 유형에 맞는 명령을 사용합니다.
- 새 인증서 그룹을 생성하려면 을 클릭하고 **Add Certificate Group(**인증서 그룹 추가**)**을 선택합니다.
- 인증서 또는 그룹을 보거나 수정하려면 인증서의 수정 아이콘( ) 또는 보기 아이콘( )을 클릭합니다.
- 참조되지 않는 인증서 또는 그룹을 삭제하려면 해당 인증서의 휴지통 아이콘( )을 클릭합니다.

인증서 생성 또는 수정에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 내부 및 내부 CA 인증서 업로드, 5 페이지
- 자체 서명 내부 및 내부 CA 인증서 생성, 7 페이지
- 신뢰할 수 있는 CA 인증서 업로드, 9 페이지
- 신뢰할 수 있는 CA 인증서 그룹 구성, 10 페이지

내부 및 내부 CA 인증서 업로드

내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다.

내부 CA 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다.

OpenSSL 툴킷을 사용하여 이러한 인증서를 직접 생성하거나 인증 증명에서 가져온 후, 다음 절차를 사용하여 업로드할 수 있습니다. 키 생성의 예를 보려면 예: OpenSSL을 사용하여 내부 인증서 생성, 3 페이지를 참조하십시오.

자체 서명된 내부 ID 및 내부 CA 인증서를 생성할 수도 있습니다. 자체 서명된 내부 CA 인증서를 구성할 경우, CA는 디바이스 자체에서 실행됩니다. 자체 서명 인증서를 만드는 방법에 대한 내용은 자체 서명 내부 및 내부 CA 인증서 생성, 7 페이지를 참조하십시오.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 기능에 사용되는 인증서 유형, 2 페이지를 참조하십시오.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Certificates(**인증서**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **+** > **Add Internal Certificate(**내부 인증서 추가**)**를 클릭한 다음 **Upload Certificate and Key(**인증서 및 키 업로드**)**를 클릭합니다.
- **+** > **Add Internal CA Certificate(**내부 **CA** 인증서 추가**)**를 클릭한 다음 **Upload Certificate and Key(**인증서 및 키 업로드**)**를 클릭합니다.
- 인증서를 수정하거나 보려면 정보 아이콘( )을 클릭합니다. 대화 상자에는 인증서 주체, 발급자, 유효 기간 범위가 표시됩니다. 새 인증서 및 키를 업로드하려면 Replace Certificate(인증서 교체)를 클릭합니다. 대화 상자에서 인증서 및 키를 붙여넣을 수도 있습니다.

단계 **3** 인증서의 **Name(**이름**)**을 입력합니다.

이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** **Upload Certificate(**인증서 업로드**)** 또는 **Replace Certificate(**인증서 교체**)**(수정 시)를 클릭하고 인증서 파일(예: *.crt)을 선택합니다. 허용된 파일 확장명은 .pem, .cert, .cer, .crt, and .der입니다. 또는 인증서를 붙여넣습니다.

인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다.

붙여넣는 인증서는 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함해야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

단계 **5** **Upload Key(**키 업로드**)** 또는 **Replace Key(**키 교체**)**(수정 시)를 클릭하고 인증서 파일(예: *.key)을 선택합니다. 파일 확장명은 .key여야 합니다. 또는 인증서의 키를 붙여넣습니다.

키는 암호화할 수 없으며, RSA 키여야 합니다.

예를 들면 다음과 같습니다.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQClSu1BknrMjzw/5FZ9YgdMLDUGJlbYgkjN7mVrkjyLQx2TYsem
r8iTiKB6iyTKbuS4iPeyEYkNF5FglCqKWEdmthNZkBhOsPs1A8e60r5mImeDrtw+
Cc0O5cSfnlTAw5CgcGkcxTCaGIZmXMkzwGlfYmzbJDeazfSmvys76A8I8wIDAQAB
AoGAUVDgEX8vXE0m9cOubPZ54pZo64KW/OJzUKP0TwxdLqGw/h39XFpkEXiIgmDL
(...5 lines removed...)
DSWvzekRDH83dmP66+MIbWePhbhty+D1OxbiuVuHV0/ZhxOhCG8tig3R8QJBAJmj
fId05+1dNI4tGbWv6hHh/H/dTP2STlZ3jERMZd29fjIRuJ9jpFC2lIDjvs8YGeAe
0YHkfSOULJn8/jOCf6kCQQDIJiHfGF/31Dk/8/5MGrg+3zau6oKXiuv6db8Rh+7l
MUOx09tvbBUy9REJq1YJWTKpeKD+E0QL+FX0bqvz4tHA
-----END RSA PRIVATE KEY-----
```

단계 **6** **OK(**확인**)**를 클릭합니다.

키 크기가 생성된 자체 서명 인증서에 대해 허용되는 최소 크기보다 작으면 인증서가 권장 최소 요구 사항을 충족하지 않는다는 경고가 표시됩니다. 인증서를 계속 업로드하려면 **Proceed(**진행**)**를 클릭합니다. 하지만 더 강력한 새 인증서를 생성하는 것이 좋습니다.

자체 서명 내부 및 내부 **CA** 인증서 생성

내부 ID 인증서는 특정 시스템 또는 호스트용 인증서입니다.

내부 CA 인증서는 시스템에서 다른 인증서를 서명하는 데 사용할 수 있는 인증서입니다. 이러한 인증서는 CA 인증서에는 활성화되지만 ID 인증서에는 비활성화되는 기본 제약 조건 확장 및 CA 플래그와 관련된 내부 ID 인증서와 다릅니다.

자체 서명 내부 ID 및 내부 CA 인증서를 생성할 수 있으며, 즉 디바이스 자체에서 인증서를 서명합니다. 자체 서명 내부 CA 인증서를 구성할 경우, CA는 디바이스에서 실행됩니다. 시스템에서는 인증서 및 키를 모두 생성합니다.

OpenSSL을 사용하여 이러한 인증서를 생성하거나, 신뢰할 수 있는 CA에서 인증서를 가져오고 업로드할 수 있습니다. 자세한 내용은 내부 및 내부 CA 인증서 업로드, 5 페이지를 참고하십시오.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 기능에 사용되는 인증서 유형, 2 페이지를 참조하십시오.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Certificates(**인증서**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **+** > **Add Internal Certificate(**내부 인증서 추가**)**를 클릭한 다음 **Self-Signed Certificate(**자체 서명 인증서**)**를 클릭합니다.
- **+** > **Add Internal CA Certificate(**내부 **CA** 인증서 추가**)**를 클릭한 다음 **Self-Signed Certificate(**자체 서명 인증서**)**를 클릭합니다.

참고 인증서를 수정하거나 보려면 정보 아이콘()을 클릭합니다. 대화 상자에는 인증서 주체, 발급자, 유효 기간 범위가 표시됩니다. 새 인증서 및 키를 업로드하려면 **Replace Certificate(**인증서 교체**)**를 클릭합니다. 인증서를 교체할 경우, 다음 단계에 설명된 자체 서명 특성을 다시 실행할 수 없습니다. 그 대신, 내부 및 내부 CA 인증서 업로드, 5 페이지에 설명된 대로 새 인증서를 붙여넣거나 업로드해야 합니다. 나머지 단계는 새로운 자체 서명 인증서에만 적용됩니다.

단계 **3** 인증서의 **Name(**이름**)**을 입력합니다.

이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** 인증서 주체와 발급자 정보에 다음 중 한 가지 이상의 정보를 구성합니다.

- **Country(**국가**)**(C) — 인증서에 포함할 두 글자로 된 ISO 3166 국가 코드입니다. 예를 들어 미국의 국가 코드는 US입니다. 드롭다운 목록에서 국가 코드를 선택합니다.
- **State or Province(**주/도**)**(ST) — 인증서에 포함할 주/도입니다.
- **Locality or City(**구/군/시**)**(L) — 인증서에 포함할 구/군/시(예: 도시 이름)입니다.
- **Organization(**조직**)**(O) — 인증서에 포함할 조직 또는 회사 이름입니다.
- **Organizational Unit(Department)(**조직 단위**(**부서**))**(OU) — 인증서에 포함할 조직 단위의 이름(예: 부서 이름)입니다.
- **Common Name(**공용 이름**)**(CN) — 인증서에 포함할 X.500 공용 이름입니다. 이는 디바이스, 웹사이트 또는 다른 문자열의 이름일 수 있습니다. 일반적으로 연결에 성공하려면 이 요소가 필요합니다. 예를 들어 원격 액세스 VPN에 사용되는 내부 인증서에는 CN을 포함해야 합니다.
- **Key Type(**키 유형**)** - 이 인증서에 대해 생성할 키 유형: RSA, ECDSA(Elliptic Curve Digital Signature Algorithm) 또는 EDDSA(Edward-curve Digital Signature Algorithm).
- **Key Size(**키 크기**)** - 생성할 키의 크기. 일반적으로 키가 길수록 더 안전합니다. 그러나 모듈러스 크기가 큰 키는 생성 및 교환 프로세스에 더 오랜 시간이 걸립니다. 허용되는 크기는 키 유형에 따라 다릅니다.
  - RSA 키는 2048, 3072 또는 4096비트일 수 있습니다.
  - ECDSA 키는 256, 384 또는 521비트일 수 있습니다.

    EDDSA 키는 256비트일 수 있습니다.
- **Validity Period(**유효 기간**)** - 인증서가 유효한 것으로 간주되는 기간입니다. 기본값은 만료일 설정 방법과 무관하게 오늘을 기준으로 825일입니다. 기본값으로 돌아가려면 **Set default(**기본값으로 설정**)**를 클릭합니다. 다음 방법 중 하나를 사용하여 기간을 설정할 수 있습니다. 만료되기 전에 인증서를 교체하십시오.
  - **By Date(**날짜 기준**) - Expiration Date(**만료 날짜**)**를 클릭하고 인증서가 유효한 것으로 간주되는 마지막 날을 선택합니다.

- **By Number of Days(**일 수 기준**)** - 오늘을 시작으로 인증서가 유효한 것으로 간주되는 기간(일)을 입력합니다. 수를 입력한 후 **By Date(**날짜 기준**)**을 클릭하면 계산된 만료 날짜가 표시됩니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

신뢰할 수 있는 CA 인증서 업로드

신뢰할 수 있는 CA(Certificate Authority) 인증서는 다른 인증서에 서명하는 데 사용되며, 자체 서명되며 루트 인증서라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서는 하위 인증서라고 합니다.

이러한 인증서를 사용하는 기능에 대한 자세한 내용은 기능에 사용되는 인증서 유형, 2 페이지를 참조하십시오.

외부 인증 기관으로부터 신뢰할 수 있는 CA 인증을 획득하거나, OpenSSL 도구 등 자체 내부 CA를 사용하여 CA 인증을 생성하십시오. 그런 다음, 아래 절차를 사용하여 인증서를 업로드합니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Certificates(**인증서**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **+** > **Add Trusted CA Certificate(**신뢰받는 **CA** 인증서 추가**)**를 클릭합니다.
- 인증서를 수정하려면 인증서의 수정 아이콘()을 클릭합니다.

단계 **3** 인증서의 **Name(**이름**)**을 입력합니다.

이름은 컨피그레이션에서 개체 이름으로만 사용되며 인증서 자체에 포함되지는 않습니다.

단계 **4** 인증서 업로드 또는 인증서 교체(수정 시)를 클릭하고 신뢰할 수 있는 CA 인증서 파일(예: *.pem)을 선택합니다. 허용된 파일 확장명은 .pem, .cert, .cer, .crt, and .der입니다. 또는 신뢰할 수 있는 CA 인증서를 붙여넣습니다.

인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.

인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다.

붙여넣는 인증서는 BEGIN CERTIFICATE 및 END CERTIFICATE 줄을 포함해야 합니다. 예를 들면 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
```

```
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

단계 **5** 인증서 사용을 제한하려면 **Validation Usage(**검증 사용**)**를 설정합니다.

일부 기능을 사용하면 특정 인증서에 대해 연결을 검증할 수 있는지 여부를 선택할 수 있습니다. 이러한 기능이 인증서를 유효하게 사용할 수 있음을 인증서에 표시해야 하며, 그렇지 않은 경우 연결이 거부됩니다.

이러한 옵션에 포함되지 않은 기능은 명시적 사용 허용 없이 이 인증서에 대해 검증할 수 있습니다. 예를 들어 SSL 암호 해독 정책 및 device manager을 호스팅하는 웹 서버는 Validation Usage(검증 사용) 옵션을 무시합니다. 이 필드에서 옵션을 선택하면 **show running-config** 명령을 사용하여 표시되는 실행 중인 구성에 인증서가 다운로드됩니다.

이러한 옵션의 기본 목적은 특정 인증서에 대해 검증될 수 있으므로 VPN 연결이 설정되지 않도록 하는 것입니다.

- **SSL Server(SSL** 서버**)** - 원격 SSL 서버에서 인증서를 검증합니다. 동적 DNS에 사용합니다.
- **SSL Client(SSL** 클라이언트**)** - 수신 원격 액세스 VPN 연결 인증서를 검증합니다.
- **IPsec Client(IPsec** 클라이언트**)** - 수신 IPsec 사이트 간 VPN 연결 인증서를 검증합니다.
- **Other(**기타**)** - Snort 검사 엔진에서 관리하지 않는 LDAPS 등의 기능을 검증합니다. 특정 기능에 문제가 있는 경우에만 이 옵션을 선택하십시오. **Other(**기타**)**는 다른 모든 옵션과 상호 배타적입니다. 다른 옵션을 선택하려면 먼저 **Other(**기타**)**를 선택 취소해야 하고, **Other(**기타**)**를 선택하려면 먼저 모든 옵션을 선택 취소해야 합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

신뢰할 수 있는 **CA** 인증서 그룹 구성

SSL 암호 해독 정책 설정에서 외부의 신뢰할 수 있는 CA 인증서 그룹을 사용하여 SSL 암호 해독 정책에서 신뢰해야 하는 인증서를 지정합니다. 엔드 유저가 인증서 발급자의 인증서가 신뢰할 수 있는 인증서에 속하지 않은 사이트에 연결을 시도하면 해당 유저에게 인증서를 신뢰하라는 메시지가 표시됩니다. 따라서 신뢰할 수 있는 목록에 인증서가 없는 경우 엔드 유저는 불편하지만 액세스 제어 규칙으로 수행할 수 있는 연결 자체가 차단되지는 않습니다.

기본 그룹은 CTA(Cisco-Trusted-Authorities)입니다. 다음과 같은 경우에만 고유한 그룹을 생성해야 합니다.

- 기본 그룹에 없는 인증서를 신뢰하고자 합니다. 그러면 SSL 암호 해독 정책 설정에서 기본 그룹과 새 그룹을 모두 선택합니다.

- 기본 그룹보다 제한된 인증서 목록을 신뢰하고자 합니다. 그러면 델타 뿐 아니라 신뢰할 수 있는 인증서의 전체 목록이 포함된 그룹을 생성하고 이를 SSL 암호 해독 정책 설정에서 단독 그룹으로 선택합니다.

시작하기 전에

시스템에 아직 없는 경우 그룹에 추가할 신뢰할 수 있는 CA 인증서를 모두 업로드합니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Certificates(**인증서**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 인증서 그룹을 생성하려면 을 클릭하고 **Add Certificate Group(**인증서 그룹 추가**)**을 선택합니다.
- 인증서 그룹을 수정하려면 해당 그룹의 수정 아이콘( )을 클릭합니다.

단계 **3** 인증서 그룹의 **Name(**이름**)**을 입력하고 필요한 경우 설명을 입력합니다.

단계 **4** **+**를 클릭하여 그룹에 인증서를 추가합니다.

그룹에 필요한 모든 인증서를 추가합니다. **Create New Trusted CA Certificate(**새 신뢰할 수 있는 **CA** 인증서 생성**)**를 클릭하여 그룹을 구축하는 동안 새 인증서를 업로드할 수 있습니다.

그룹에 인증서가 더 이상 필요하지 않은 경우 인증서의 X 아이콘(오른쪽)을 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.