# ASA의 Unified Mobility Advantage 서버 인증서 문제

## 목차



## 소개

이 문서에서는 ASA(Adaptive Security Appliance)와 Cisco CUMA(Unified Mobility Advantage) 서버 간에 자체 서명 인증서를 교환하는 방법과 그 반대의 방법을 설명합니다. 또한 인증서를 가져오는 동안 발생하는 일반적인 문제를 해결하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 5500 시리즈
- Cisco Unified Mobility Advantage Server 7

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

## 구축 시나리오

**Cisco Mobility Advantage** 솔루션에서 사용하는 **TLS 프록시**에 대한 두 가지 구축 시나리오가 있습니다.

**참고:** 두 시나리오에서는 클라이언트가 인터넷에서 연결됩니다.

1. Adaptive Security Appliance는 방화벽 및 TLS 프록시의 역할을 모두 수행합니다.
2. Adaptive Security Appliance는 TLS 프록시로만 작동합니다.

두 시나리오에서 모두 **Cisco UMA 서버 인증서** 및 **키 쌍을 PKCS-12** 형식으로 내보내고 Adaptive Security Appliance로 가져와야 합니다. 인증서는 Cisco UMA 클라이언트와의 핸드셰이크 중에 사용됩니다.

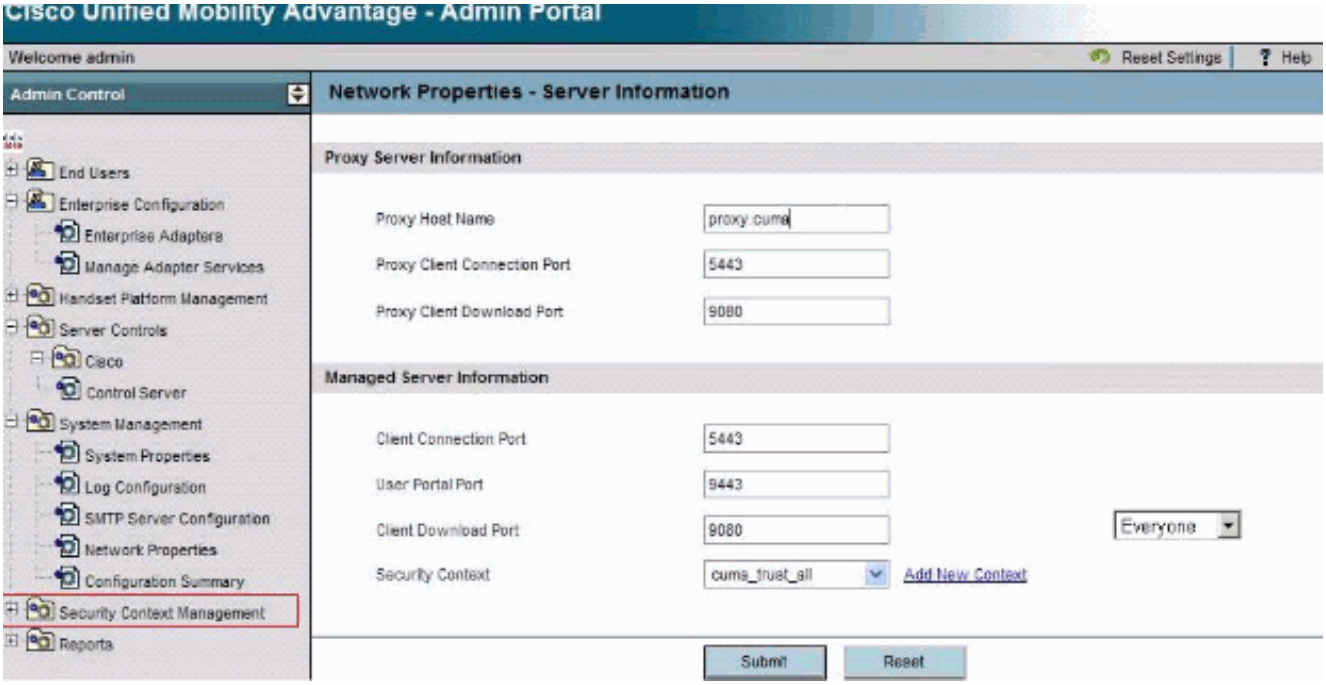
Adaptive Security Appliance 신뢰 저장소에 Cisco UMA 서버 자체 서명 인증서를 설치하려면 Adaptive Security Appliance 프록시와 Cisco UMA 서버 간의 핸드셰이크 중에 Cisco UMA 서버를 인증해야 합니다.

## Cisco UMA 서버 자체 서명 인증서 설치

### CUMA 서버에서 수행할 작업

이러한 단계는 CUMA 서버에서 수행해야 합니다. 다음 단계를 수행하면 CUMA에서 자체 서명 인증서를 생성하여 ASA와 CN=portal.aipc.com을 교환합니다. ASA 트러스트 저장소에 설치해야 합니다. 다음 단계를 완료하십시오.

1. CUMA 서버에서 자체 서명 인증서를 만듭니다.Cisco Unified Mobility Advantage 관리 포털에 로그인합니다.Security Context **Management** 옆에 있는**[+]**를 선택합니다
   .




**보안 컨텍스트를 선택합니다**.컨텍스트 **추가를 선택합니다**.다음 정보를 입력합니다.

```
Do you want to create/upload a new certificate? create
Context Name "cuma"
Description "cuma"
Trust Policy "Trusted Certificates"
Client Authentication Policy "none"
Client Password "changeme"
Server Name cuma.ciscodom.com
Department Name "vsec"
Company Name "cisco"
City "san jose"
State "ca"
Country "US"
```

2. Cisco Unified Mobility Advantage에서 자체 서명 인증서를 다운로드합니다. 작업을 수행하려면 다음 단계를 완료하십시오.Security Context **Management** 옆에 있는**[+]**를 선택합니다.**보안 컨텍스트를 선택합니다**.다운로드할 인증서가 있는 보안 컨텍스트 옆에 있는 Manage Context를 선택합니다.Download **Certificate를 선택합니다**.**참고:** 인증서가 체인이고 연결된 루트 또는 중간 인증서가 있는 경우 체인의 첫 번째 인증서만 다운로드됩니다. 자체 서명 인증서에 충분합니다.파일을 저장합니다.
3. 다음 단계는 Cisco Unified Mobility Advantage의 자체 서명 인증서를 ASA에 추가하는 것입니다. ASA에서 다음 단계를 완료합니다.텍스트 편집기에서 Cisco Unified Mobility Advantage의 자체 서명 인증서를 엽니다.Cisco Adaptive Security Appliance 트러스트 저장소로 인증서를 가져옵니다.

```
cuma-asa(config)# crypto ca trustpoint cuma-server-id-cert
cuma-asa(config-ca-trustpoint)# enrollment terminal
cuma-asa(config-ca-trustpoint)# crypto ca authenticate
cuma-server-id-cert
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

----BEGIN CERTIFICATE----
** paste the contents from wordpad **
----END CERTIFICATE----
```

4. CUMA 서버에서 ASA 자체 서명 인증서를 내보냅니다. Cisco Adaptive Security Appliance의 인증서를 요구하려면 Cisco Unified Mobility Advantage를 구성해야 합니다. 필요한 자체 서명 인증서를 제공하려면 다음 단계를 완료하십시오. 이러한 단계는 ASA에서 수행해야 합니다.새 키 쌍을 생성합니다.

```
cuma-asa(config)# crypto key generate rsa label asa-id-key mod 1024
```

```
INFO: The name for the keys will be: asa-id-key

Keypair generation process begin. Please wait...
```

새 신뢰 지점을 추가합니다.

```
cuma-asa(config)# crypto ca trustpoint asa-self-signed-id-cert

cuma-asa(config-ca-trustpoint)# keypair asa-id-key

cuma-asa(config-ca-trustpoint)# enrollment self
```

신뢰 지점 등록:

```
cuma-asa(config-ca-trustpoint)# crypto ca enroll asa-self-signed-id-cert
% The fully-qualified domain name in the certificate will be:
cuma-asa.cisco.com
% Include the device serial number in the subject name? [yes/no]: n
Generate Self-Signed Certificate? [yes/no]: y
```

인증서를 텍스트 파일로 내보냅니다.

```
cuma-asa(config)# crypto ca export asa-self-signed-id-cert
identity-certificate
The PEM encoded identity certificate follows:

-----BEGIN CERTIFICATE-----

Certificate data omitted

-----END CERTIFICATE-----
```

5. 이전 출력을 텍스트 파일에 복사하고 CUMA 서버 트러스트 저장소에 추가하고 다음 절차를 사용합니다.Security Context **Management** 옆에 있는**[+]**를 선택합니다.**보안 컨텍스트를 선택합니다**.서명된 인증서**를** 가져올 보안 컨텍스트 옆에 있는 Manage Context를 선택합니다 .Trusted **Certificates**(신뢰할 수 있는 인증서) 표시줄에서 Import(가져오기)를 선택합니다.인증서 텍스트를 붙여넣습니다.인증서 이름을 지정합니다.가져오기를 **선택합니다**.**참고:** 원격 대상 컨피그레이션의 경우 일반 전화기로 전화를 걸어 휴대폰 벨소리가 동시에 울릴지 확인합니다. 그러면 모바일 연결이 작동하고 원격 대상 구성에 문제가 없음을 확인할 수 있습니다.

# CUMA 인증서 요청을 다른 인증 기관에 추가하는 동안 문제가 발생했습니다.

## 문제 1

CUMC/CUMA 솔루션이 신뢰할 수 있는 인증서와 함께 작동하는 경우 도움이 되는 많은 데모/프로토타입 설치 프로그램을 자체 서명하거나 *다른 인증 기관에서* 가져옵니다. Verisign 인증서는 비싸며 이러한 인증서를 가져오는 데 시간이 오래 걸립니다. 솔루션에서 다른 CA의 자체 서명 인증서 및 인증서를 지원하는 것이 좋습니다.

지원되는 현재 인증서는 GeoTrust 및 Verisign입니다. Cisco 버그 ID CSCta62971에 설명되어 있습니다(등록된 고객만 해당).

# 오류: 연결할 수 없음

사용자 포털 페이지(예: `https://<host>:8443`) `Unable to connect` error 메시지가 나타납니다.

## 솔루션

이 문제는 Cisco 버그 ID CSCsm26730(등록된 고객만 해당)에 설명되어 있습니다. 사용자 포털 페이지에 액세스하려면 다음 해결 방법을 완료합니다.

이 문제의 원인은 달러 문자이므로 관리 대상 서버의 **server.xml 파일**에 달러 문자가 하나 이상 있는 달러 문자를 이스케이프합니다. 예를 들어, /opt/cuma/jboss-4.0.1sp1/server/cuma/deploy/jbossweb-tomcat50.sar/server.xml을 편집합니다.

줄: **keystorePass="pa$word"** maxSpareThreads="15"

$$문자를 $$ . keystorePass=**"pa$$word"maxSpareThreads=**"15" 같습니다.

# CUMA 관리 포털의 일부 페이지에 액세스할 수 없습니다.

다음 페이지는 CUMA 관리 **포털**에서 볼 수 없습니다.

- 사용자 활성화/비활성화
- 검색/유지 보수

사용자가 왼쪽 메뉴에 있는 위의 두 페이지 중 하나를 클릭하면 브라우저가 페이지를 로드하고 있음을 나타내는 것처럼 보이지만 아무 일도 발생하지 않습니다(브라우저에 있던 이전 페이지만 표시됨).

## 솔루션

사용자 페이지와 관련된 이 문제를 해결하려면 Active Directory에 사용되는 포트를 **3268**로 변경하고 CUMA를 다시 시작합니다.

# 관련 정보

- ASA-CUMA 프록시 단계별 구성
- 모든 ASR5000 v1 소개
- Cisco Unified Mobility Advantage 업그레이드
- 음성 기술 지원
- 음성 및 통합 커뮤니케이션 제품 지원
- 기술 지원 및 문서 – Cisco Systems