# CVOS 시스템의 SAN 인증서에서 여러 주소 구성

## 목차



## 소개

이 문서에서는 Cisco VOS 환경에 VVB(Virtual Voice Browser)와 같은 Publisher - Subscriber 아키텍처 모델이 없는 경우 SAN(Subject Alternative Name) 인증서 필드에 여러 주소가 포함되도록 Cisco VOS(Voice Operating System) 시스템을 설정하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CA 서명 인증서
- 자체 서명 인증서
- Cisco VOS CLI

### 사용되는 구성 요소

- VVB
- Cisco VOS 시스템 관리 - 인증서 관리
- Cisco VOS CLI

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

컨피그레이션은 Cisco VOS 명령줄 인터페이스를 통해 수행됩니다. 이렇게 하면 조직이 보안 통신

채널을 통해 호스트 이름 또는 FQDN(Fully Qualified Domain Name)으로 웹 페이지를 사용하고 탐색하는 데 도움이 됩니다. 따라서 브라우저는 신뢰할 수 없는 HTTP 연결을 보고하지 않습니다.

# 구성

이 컨피그레이션을 시도하기 전에 이러한 서비스가 작동 중인지 확인하십시오.

- Cisco Tomcat 서비스
- Cisco 인증서 변경 알림
- Cisco 인증서 만료 모니터

## 설정

1단계. 자격 증명을 사용하여 VVB OS CLI에 로그인합니다.

2단계. CSR을 생성하기 전에 먼저 인증서 정보를 설정해야 합니다.

- 실행 set web-security 명령을 실행합니다.

```
set web-security <orgunit> <orgname> <locality> <state> [country] [alternatehostname1,alternatehostname
```

예를 들면 다음과 같습니다. set web-security tac cisco bangalore karnataka IN vvbpri,vvbpri.raducce.com 이 그림에 표시된 것과 같습니다.

```
admin:set web-security tac cisco bangalore karnataka IN vvbpri,vvbpri.raducce.com
```

Set web-security 명령

다음으로, 다음 질문에 답하라는 메시지가 표시됩니다. Yes/No 이 그림에서 볼 수 있습니다.

```
WARNING: This operation creates self-signed certificate for web access (tomcat) with the updated organizational information.  However, certificates for other components (ipse
c, CallManager, CAPF, etc.) still contain the original information. You may need to re-generate these self-signed certificates to update them.

Regenerating web security certificates please wait ...

WARNING: This operation will overwrite any CA signed certificate previously imported for  tomcat
Proceed with regeneration (yes|no)?
```

set web-security 명령 실행

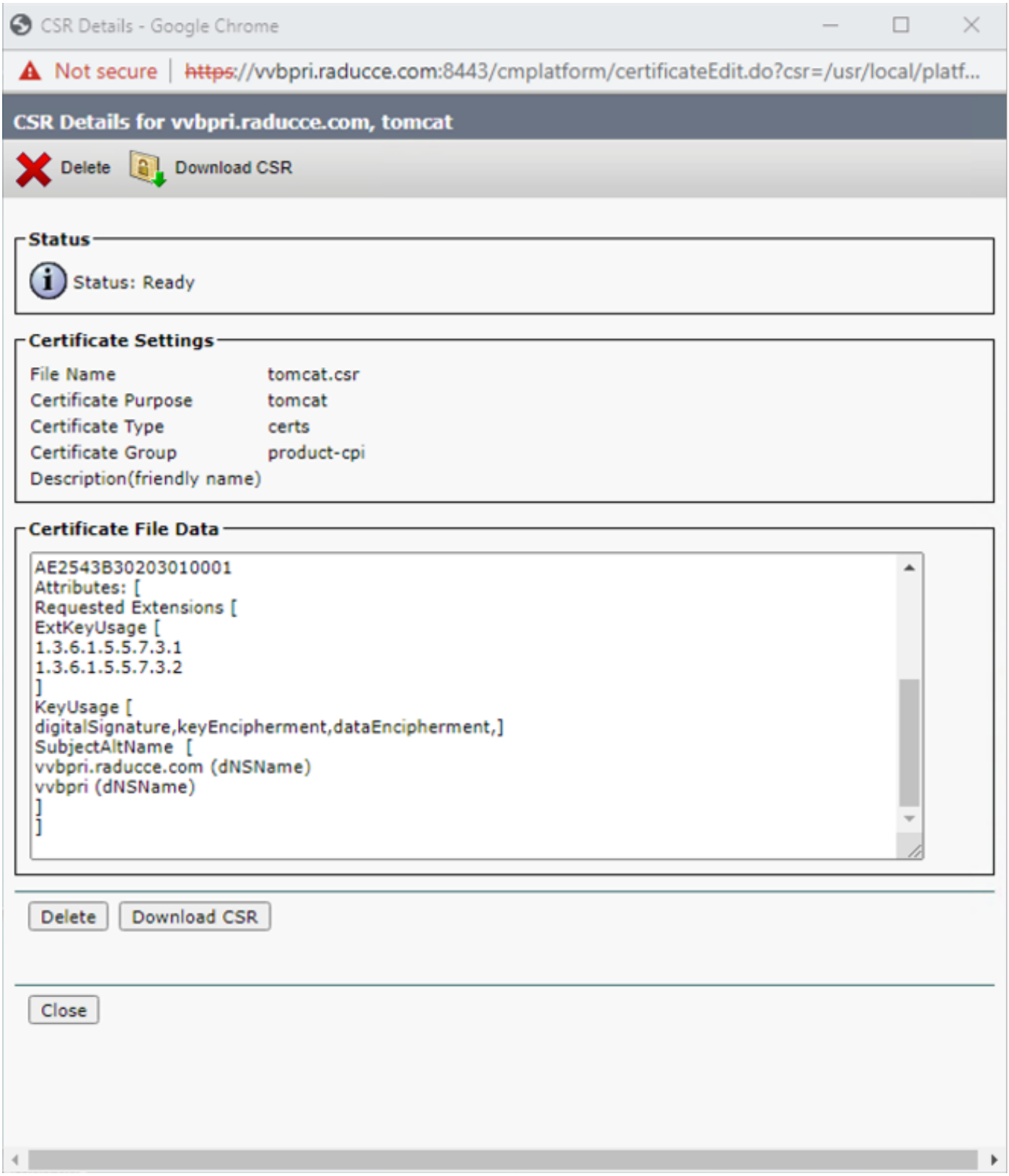
- 입력 사항 Yes
- Cisco VOS 노드에서 Cisco Tomcat 서비스를 다시 시작합니다.

```
utils service restart Cisco Tomcat
```

3단계. CLI를 통해 Tomcat CSR(Certificate Signing Request)을 생성합니다. 명령 set csr gen tomcat

vos CLI 인터페이스에서 Tomcat 인증서를 생성합니다.

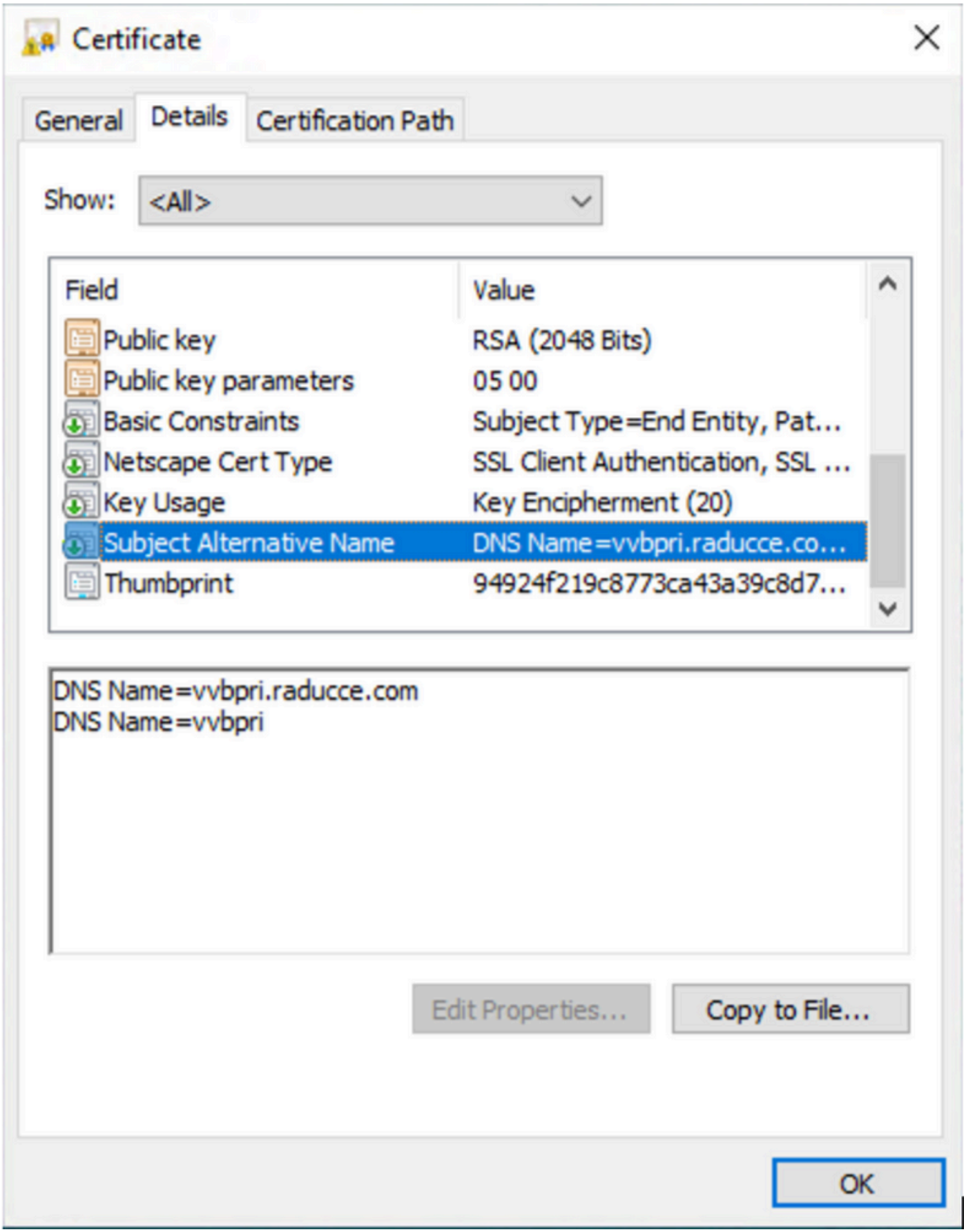
4단계. VVB OS ADMIN Certificate(VVB OS 관리 인증서) 관리 페이지에서 Tomcat CSR 인증서가 생성되는지 확인합니다. 다음을 클릭합니다. Download CSR 이 이미지에 표시된 옵션입니다.




Tomcat CSR 인증서

5단계. CA 팀에 CSR 인증서를 제공하고 CA에서 서명한 인증서를 가져옵니다.

6단계. 이 그림에서 SAN의 CA where-in에서 서명한 인증서는 앞서 설명한 명령에서 구성한 여러 주소를 표시합니다.




Tomcat CA 서명 인증서

# 다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1. 에 로그인합니다 VOS Portal URL 페이지에서 LOCK SAN certificate(SAN 인증서) 필드에서 정의된 주소를 확인합니다.
2. SAN 필드에 정의된 주소를 사용하고 보안 HTTP 통신을 확인합니다.

# 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

CLI 액세스에서 이러한 인증서 관리 로그를 수집하고 Cisco TAC에서 케이스를 엽니다. file get activelog platform/log/cert*

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.