

# SAN は Finesse のサードパーティ署名入り認証 証における発行します

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題： SAN は Finesse のサードパーティ署名入り認証における発行します](#)

[解決策](#)

## 概要

この資料はアプリケーションサーバ証明書がエラーメッセージ「CSR SAN および証明書 SAN とロードしない一致する」問題を記述したものです。

著者： Anuj Bhatia、Cisco TAC エンジニア。

## 前提条件

### 要件

以下についての知識をお持ちの上でこの文書をお読みになることを推奨します。

- 証明書は音声オペレーティングシステム (VOS) プラットフォームの要求 (CSR) 生成プロセスに署名しました
- VOS プラットフォームの認証局 (CA) 署名入り認証をアップロードするプロセス

### 使用するコンポーネント

この資料に記載されている情報は Cisco Finesse 11.0(1) に以上に基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

## 問題： SAN は Finesse のサードパーティ署名入り認証 における発行します

サーバに関しては CA 署名入り認証第一歩を使用することは CSR を生成することです。それはデフォルトでサブジェクト代替名 (SAN) フィールドがサーバのドメイン名とデータ入力される生成する CSR ページから作成されます。

**Generate Certificate Signing Request**

Generate Close

**Status**

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

**Generate Certificate Signing Request**

Certificate Purpose\* tomcat

Distribution\* finessea.ora.com

Common Name\* finessea.ora.com

**Subject Alternate Names (SANs)**

Parent Domain ora.com

Key Length\* 2048

Hash Algorithm\* SHA256

Generate Close

CSR 生成がこの形式で CSR の SAN 示された後

DNS Name=ora.com ( dNSName )

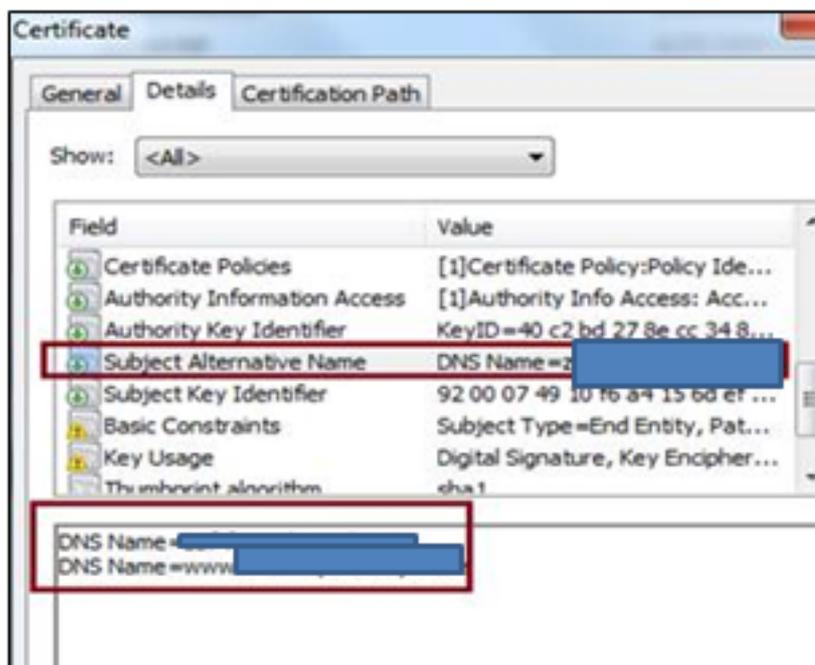
DNS Name=finessea.ora.com ( dNSName )

それらは CSR から組合わせを誤るアプリケーション 証明書一般にこれらの SAN 名前が含まれていると同時にサードパーティ CA がこの CSR からの証明書 チェーンを作成する時。

DNS Name= finessea.ora.com

DNS Name=www. finessea.ora.com

GoDaddy CA によって提供されるアプリケーション 証明書はイメージで示されています:



SAN のこのミスマッチは Tomcat 信頼ストアのアプリケーション 証明書のロードを妨げ、生成しますエラー「CSR SAN および証明書 SAN を一致する」

注: 問題は VOS plafom に、Cisco Live データ、Cisco Unified Intelligence Center ( CUIC ) 先祖などのようなこのオペレーティング システムで動作するすべてのコンタクト

センター 製品に適合です

## 解決策

問題にアプローチする 2 つの方法があります:

- 顧客は CA 権限と相談、CSR の現在として SAN の証明書 チェーンを得るように要求できます。
- より容易なオプションは CSR を生成するとき SAN フィールドは空白を保存することです。

**Status**

 Warning: Generating a new CSR for a specific certificate type will overwrite the exist

---

**Generate Certificate Signing Request**

Certificate Purpose\*

Distribution\*

Common Name\*

**Subject Alternate Names (SANs)**

Parent Domain

Key Length\*

Hash Algorithm\*

それに CSR の SAN 情報でデータがありません。CA 権限がアップロードの間に証明書 チェーンをそれ popualtes 情報提供するが、とき、システムは allows インストールされるべき証明書 フィールドを無視します。