Contents

Introduction

This document describes the problem where application server certificate fails to load with the error message "CSR SAN and Certificate SAN does not match".

Contributed by Anuj Bhatia, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics

- Certificate Signed Request (CSR) generation process on Voice Operating System (VOS) platform
- Process to upload Certificate Authority (CA) signed certificate on VOS platform

Components Used

The information in this document is based on the Cisco Finesse 11.0(1) and above.

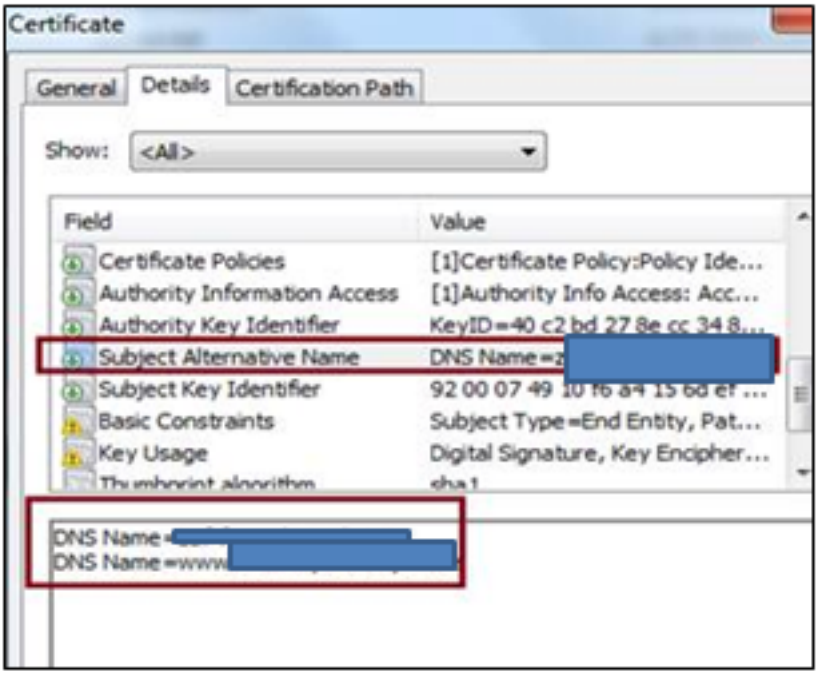
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problem: SANs issue with a Third Party Signed Certificate in Finesse

For the server to use CA signed certificates first step is to generate a CSR. It is created from the Generate CSR page where by default Subject Alternate Names (SANs) field is populated with the domain name of the server.

After CSR generation the SANs in CSR are presented in this format
DNS Name=ora.com (dNSName)
DNS Name=finessea.ora.com (dNSName)

When the third party CA creates a certificate chain from this CSR as they commonly include these SANs name in the application certificate which mismatches from the CSR.
DNS Name= finessea.ora.com
DNS Name=www. finessea.ora.com
The application certificate provided by GoDaddy CA is shown in the image:



This mismatch of SANs hinders the loading of application certificate in the tomcat trust store and generates the error "CSR SAN and Certificate SAN does not match"

> **Note**: The problem is on VOS plaform and is applicable to all the Contact Center products running on this operating system such as Cisco Live Data, Cisco Unified Intelligence Center (CUIC) etc.

Solution

There are two ways to approach the issue:

- Customer can consult with the CA authority and can request to get the certificate chain with the SANs as present in the CSR.
- Easier option is to keep the SANs field blank when generating the CSR.

It has no data in the SANs information of CSR. When CA authority provides the certificate chain it popualtes the information but during the upload, system ignores the field which allowes the certificate to be installed.