Configure Multiple Addresses in SAN Certificate in CVOS Systems

Contents

Introduction

This document describes how to set up a Cisco Voice Operating System (VOS) system to have multiple addresses in Subject Alternative Name (SAN) certificate field when the Cisco VOS environment does not have a Publisher â€“ Subscriber architecture model for example Virtual Voice Browser (VVB).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CA-signed certificates
- Self-Signed certificates
- Cisco VOS CLI

Components Used

- VVB
- Cisco VOS System Administration - Certificate Management
- Cisco VOS CLI

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, ensure that you understand the potential impact of any command.

Background Information

The configuration is carried through the Cisco VOS command line interface. This helps the organisation to use and browse the webpages either with the hostname or Fully Qualified Domain Name (FQDN) through the secure communication channel. Thereby, the browser does not report an untrusted HTTP connection.

Configure

Before you attempt this configuration, ensure these services are up and functional;

- Cisco Tomcat service
- Cisco Certificate Change Notification
- Cisco Certificate Expiry Monitor

Configurations

Step 1. Login to VVB OS CLI with credentials.

Step 2. You need to first set the Certificate information prior to the generation of CSR.

- Execute the `set web-security` command on the VVB CLI interface.

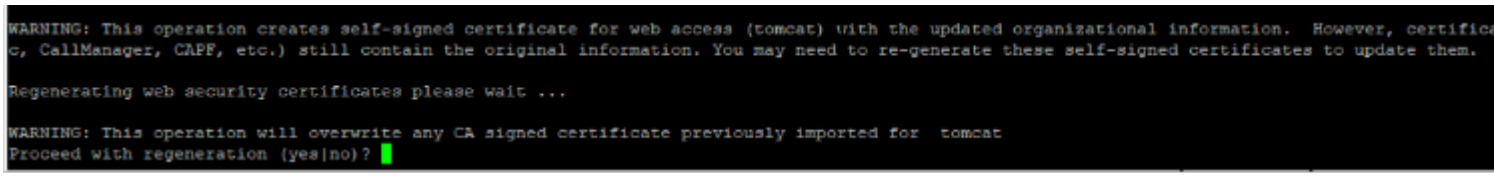
```
set web-security <orgunit> <orgname> <locality> <state> [country] [alternatehostname1,alternatehostname2
```

For example, `set web-security tac cisco bangalore karnataka IN vvbpri,vvbpri.raducce.com` as shown in this image.

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

Set web-security command

Next, it prompts you to answer with Yes/No as demonstrated in this image.



set web-security command execution

- Enter Yes
- Restart the Cisco Tomcat service on the Cisco VOS node.

```
utils service restart Cisco Tomcat
```

Step 3. Generate Tomcat certificate signing request (CSR) via CLI. The command set csr gen tomcat generates a Tomcat certificate from the VOS CLI interface.

Step 4. Check on the VVB OS ADMIN Certificate management page, a Tomcat CSR certificate is generated. Click on the Download CSR option as shown in this image.