

Configurar vários endereços no certificado SAN em sistemas CVOS

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar um sistema Cisco Voice Operating System (VOS) para ter vários endereços no campo de certificado Subject Alternative Name (SAN) quando o ambiente Cisco VOS não tem um modelo de arquitetura Publisher - Subscriber, por exemplo, Virtual Voice Browser (VVB).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Certificados assinados pela CA
- Certificados autoassinados
- CLI do Cisco VOS

Componentes Utilizados

- VVB
- Administração do sistema Cisco VOS - Gerenciamento de certificados
- CLI do Cisco VOS

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A configuração é realizada através da interface de linha de comando do Cisco VOS. Isso ajuda a organização a usar e navegar nas páginas da Web com o nome do host ou o Nome de domínio totalmente qualificado (FQDN) através do canal de comunicação seguro. Assim, o navegador não relata uma conexão HTTP não confiável.

Configurar

Antes de tentar essa configuração, verifique se esses serviços estão ativos e funcionais;

- Serviço Cisco Tomcat
- Notificação de alteração de certificado da Cisco
- Monitor de expiração de certificado da Cisco

Configurações

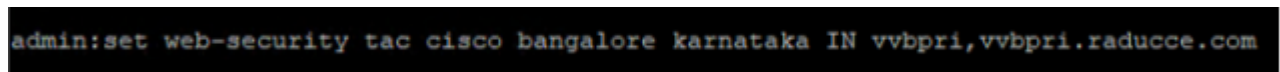
Etapa 1. Faça login na CLI do VVB OS com credenciais.

Etapa 2. Você precisa primeiro definir as informações do certificado antes da geração do CSR.

- Execute o comando `set web-security` na interface CLI do VVB.

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

Por exemplo, `set web-security tac cisco bangalore karnataka IN vvbpri,vvbpri.raducce.com` como mostrado nesta imagem.



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

Comando Set web-security

Em seguida, ele solicita que você responda com Yes/No como demonstrado nesta imagem.

```
WARNING: This operation creates self-signed certificate for web access (tomcat) with the updated organizational information. However, certificates (e.g., 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]? █
```

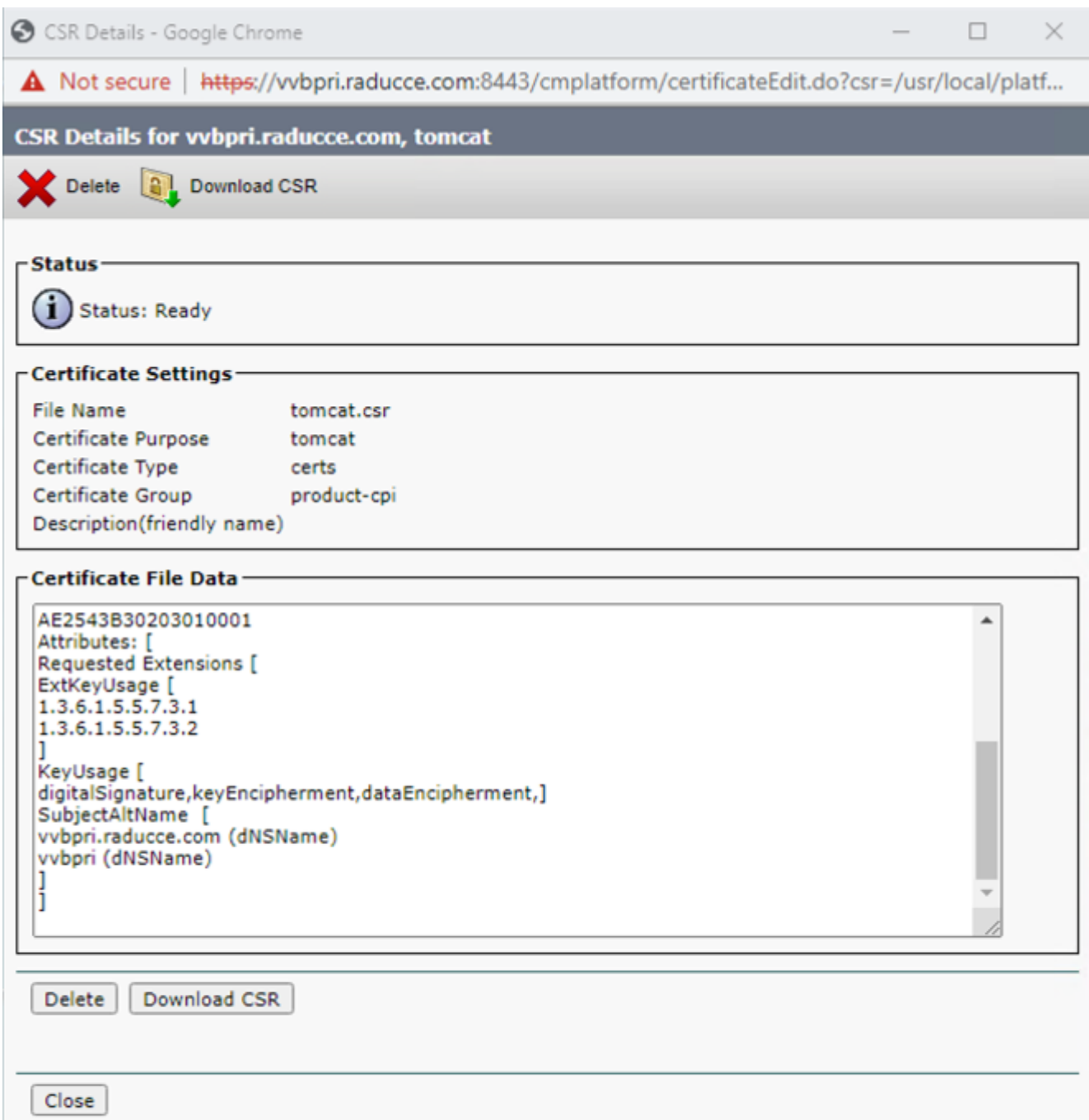
set web-security command execution

- Enter Yes
- Reinicie o serviço Cisco Tomcat no nó do Cisco VOS.

utils service restart Cisco Tomcat

Etapa 3. Gerar solicitação de assinatura de certificado (CSR) do Tomcat via CLI. O comando `set csr gen tomcat` gera um certificado Tomcat da interface CLI do VOS.

Etapa 4. Verifique na página de gerenciamento do certificado VVB OS ADMIN se um certificado Tomcat CSR foi gerado. Clique no botão `Download CSR` como mostrado nesta imagem.



Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.