# Entender o certificado da Web para vManage

## Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Certificados usados no Cisco SD-WAN](#)
[Certificado da Web](#)
[Certificado do controlador](#)
[Entender o certificado da Web para vManage](#)
[Mensagem "A conexão não é privada" no vManage](#)
[Informações proativas](#)
[Certificado registrado no nome incorreto do site](#)
[Informações Relacionadas](#)

## Introduction

Este documento descreve a diferença entre o certificado da Web e o certificado do controlador na solução Cisco SD-WAN. Este documento também explica em detalhes o certificado da Web e esclarece o uso entre esses dois tipos de certificados.

## Prerequisites

### Requirements

Conhecimento básico da Public Key Infrastructure (PKI).

### Componentes Utilizados

- Cisco vManage network management system (NMS) versão 20.4.1
- Google Chrome versão 94.0

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Certificados usados no Cisco SD-WAN

Há dois tipos de certificados usados nas soluções Cisco SD-WAN, Certificados de Controlador e Certificados da Web.

### Certificado da Web

Usado para acesso à Web para o vManage. Por padrão, a Cisco instala um certificado autoassinado. Um certificado autoassinado é um certificado SSL (Secure Sockets Layer) assinado por seu próprio criador.

No entanto, a Cisco recomenda seu próprio certificado de servidor Web. Isso ocorre principalmente nos casos em que as empresas de rede podem ter firewalls com restrições de acesso à Web.
A Cisco não fornece certificados da Web públicos emitidos pela autoridade de certificação (CA).

> Para obter mais informações sobre como gerar o certificado Web vManage, consulte os guias: Gerar certificado do servidor Web e Como gerar certificado Web com assinatura automática para vManage

### Certificado do controlador

Usado para criar conexões de controle entre os controladores, ou seja, vManage, vBonds, vSmarts.

Observe que esses certificados são críticos para todo o plano de controle de estrutura de SDWAN e devem ser mantidos válidos o tempo todo.

> Para obter mais informações sobre certificados de controladora, consulte o guia: Assinatura automática de certificado através da Cisco Systems

## Entender o certificado da Web para vManage

O protocolo HTTPS (Hypertext Transfer Protocol Secure) é um protocolo de comunicação da Internet que protege a integridade e a confidencialidade dos dados entre o computador do usuário e o site, neste caso a GUI do vManage. Os usuários esperam uma conexão segura e privada ao acessar o vManage.

Para obter uma conexão segura e privada, você deve obter um certificado de segurança. O certificado é emitido por uma autoridade de certificação (AC), que toma medidas para verificar se o domínio vManage pertence efetivamente à sua organização.

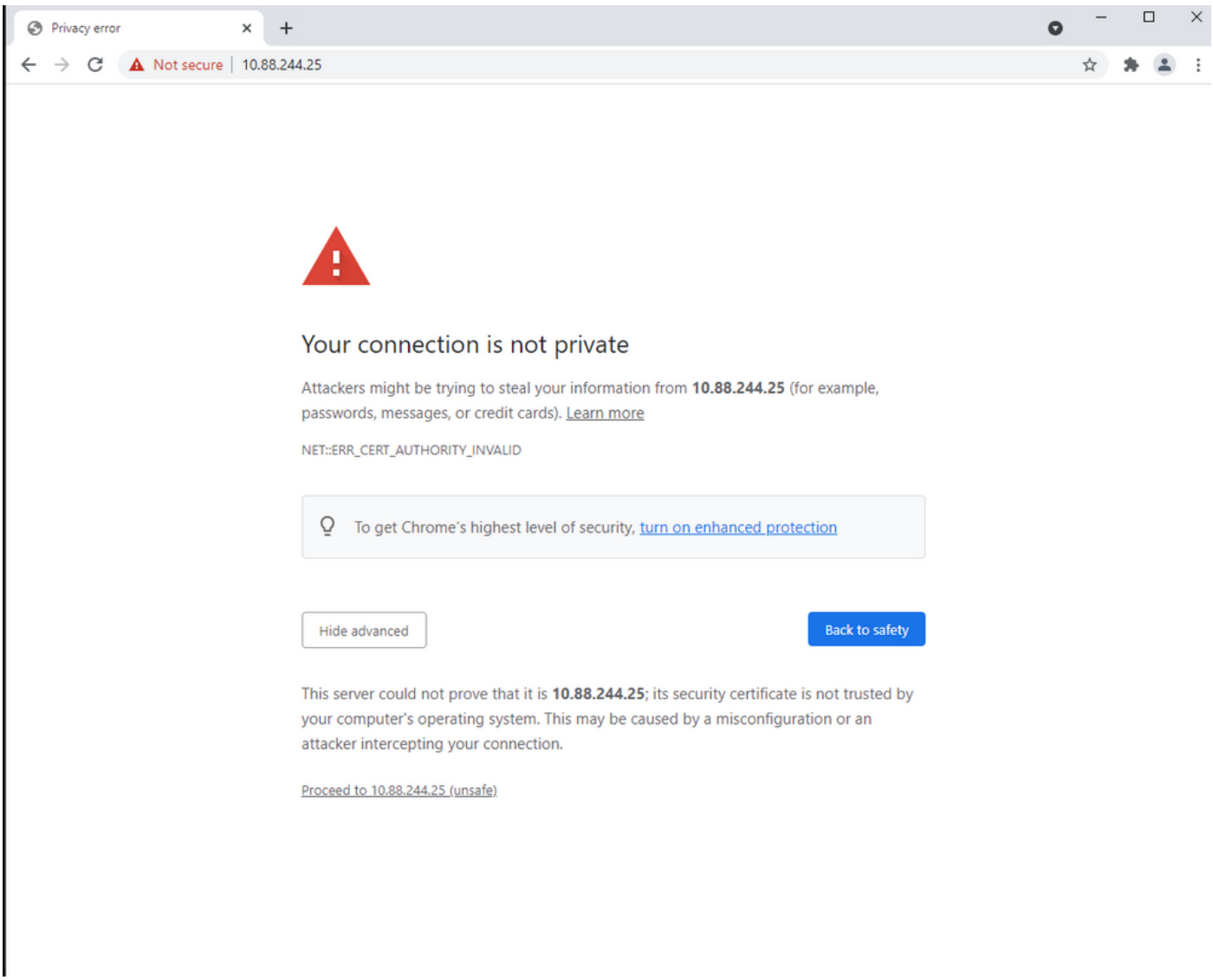
Quando um usuário acessa o vManage, o PC do usuário executa uma conexão HTTPS e um túnel seguro é estabelecido entre o servidor vManage e o computador com os certificados SSL instalados para autenticação. A autenticação do certificado SSL é executada no computador do usuário em relação ao banco de dados de CAs raiz válidas instaladas no dispositivo. Geralmente, o computador já instalou várias CAs, como Google, GoDaddy, Enterprise CA (se este for o caso) e mais entidades públicas. Portanto, se a solicitação de assinatura de certificado (CSR) for assinada por Goddady (apenas um exemplo), ela é confiável.

### Mensagem "A conexão não é privada" no vManage

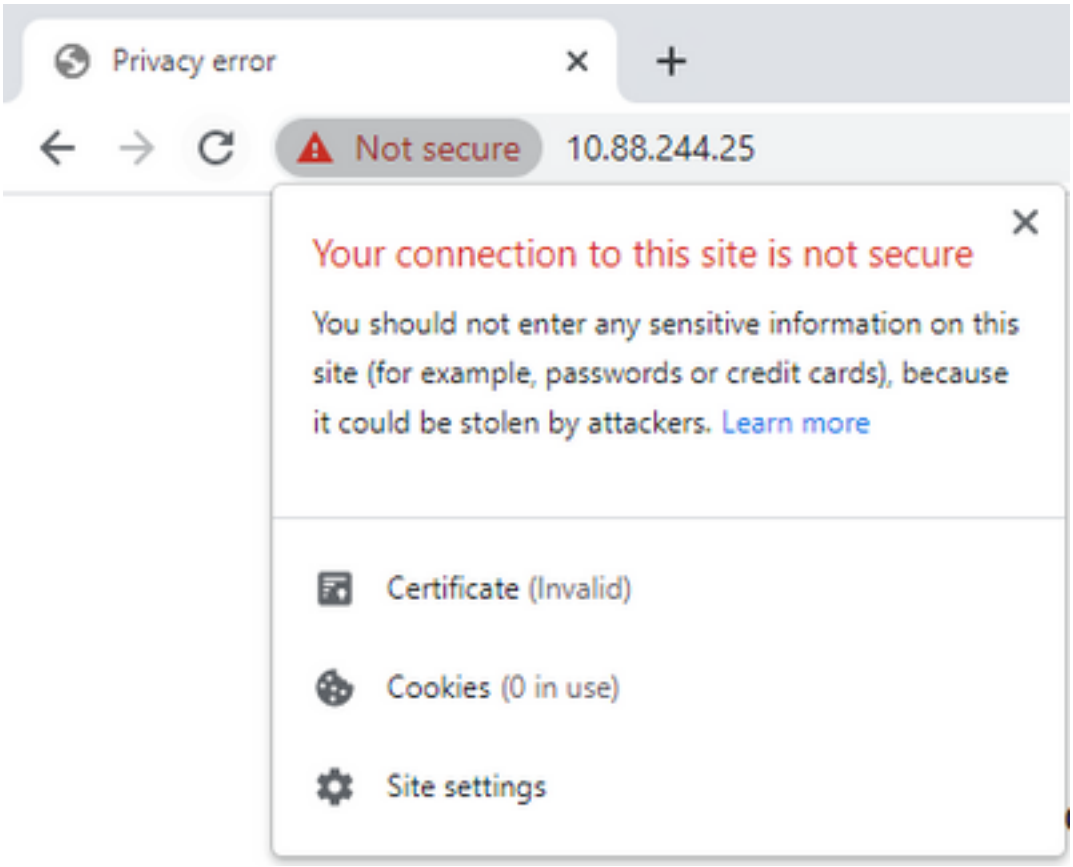
O certificado autoassinado do vManage não está assinado por uma AC. Ele foi assinado pelo mesmo vManage e nem pela CA pública nem privada, portanto, não é confiável para um cliente de PC. Por isso, o navegador exibe uma conexão de erro não segura/de privacidade para o URL

do vManage.

Exemplo do erro de alteração com o certificado autoassinado padrão pelo navegador Google Chrome, como mostrado na imagem.




**Note: Clique na opção exibir informações do site, o certificado é exibido como inválido.**




# Informações proativas

## Certificado registrado no nome incorreto do site

Certifique-se de que o certificado Web foi obtido para todos os nomes de host servidos pelo site. Por exemplo, se o certificado só abranger domínio fictício www.vManage-example-test.com, um visitante que carrega o site com o vManage-example-test.com (sem www. prefixo) e se for obtém um certificado assinado por uma AC pública, é fidedigno, mas recebe outro erro com um erro de incompatibilidade de nome de certificado.

> **Observação:** um erro de incompatibilidade de nome comum ocorre quando o nome comum do certificado SSL/TLS não corresponde ao domínio ou à barra de endereços no navegador.

# Informações Relacionadas

- Decodificador CSR
- Gerar uma solicitação de assinatura de certificado
- Suporte Técnico e Documentação - Cisco Systems