

Understand the Web Certificate For vManage

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Certificates Used on Cisco SD-WAN](#)

[Web Certificate](#)

[Controller Certificate](#)

[Understand Web Certificate for vManage](#)

["Connection Is Not private" Message on vManage](#)

[Proactive information](#)

[Certificate Registered to the Incorrect Website Name](#)

[Related Information](#)

Introduction

This document describes the difference between the Web Certificate and the Controller Certificates on the Cisco SD-WAN solution. This document also explains in detail the Web Certificate and clarifies the use between these two types of certificates.

Prerequisites

Requirements

Basic knowledge of Public Key Infrastructure (PKI).

Components Used

- Cisco vManage network management system (NMS) version 20.4.1
- Google Chrome version 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. If your network is live, ensure that you understand the potential impact of any command.

Certificates Used on Cisco SD-WAN

There are two types of certificates used in Cisco SD-WAN solutions, Controller Certificates & Web Certificates.

Web Certificate

Used for web access to the vManage. Cisco installs a self-signed certificate by default. A Self-signed certificate is a Secure Sockets Layer (SSL) certificate that is signed by its own creator.

However, Cisco recommends their own web server certificate. This is especially for cases, where network enterprises can have firewalls with web access restrictions.

Cisco does not provide public web certificates issued by Certificate Authority (CA).

For more information on how to generate the vManage Web certificate, please refer to the guides: [Generate Web Server Certificate](#) and [How To Generate Self-Signed Web Certificate For vManage](#)

Controller Certificate

Used to build control connections between the controllers i.e. vManage, vBonds, vSmarts.

Note that these certificates are critical for the entire SDWAN fabric control plane and must be kept valid at all times.

For more controller certificates information, please refer to the guide: [Automated certificate signing through Cisco Systems](#)

Understand Web Certificate for vManage

Hypertext Transfer Protocol Secure (HTTPS) is an internet communication protocol that protects the integrity and confidentiality of data between the user's computer and the website in this case the vManage GUI. Users expect a secure and private connection when they access the vManage.

To achieve a secure and private connection, you must obtain a security certificate. The certificate is issued by a certificate authority (CA), which takes steps to verify that your vManage domain actually belongs to your organization.

When a user accesses the vManage, the user PC performs an HTTPS connection and a secure tunnel is established between the vManage server and the computer with the SSL certificates installed for authentication. The authentication of the SSL certificate is performed on the user computer against the database of valid root CAs installed on the device. Usually, the computer has already installed multiples CA like, Google, GoDaddy, Enterprise CA (if this is the case), and more public entities. Therefore, if the Certificate Signing Request (CSR) is signed by Goddady (just an example) it is trusted.


"Connection Is Not private" Message on vManage

The vManage self-signed certificate is not signed by a CA. It has been signed by the same vManage and neither by the public nor private CA, therefore it is not trusted for a PC client. That is the reason, the browser displays a not secure/privacy error connection for the vManage URL.

Example for the vMange error with the default self-signed certificate by the Google Chrome browser as shown in the image.

Privacy error x +

← → ↻ Not secure | 10.88.244.25 ☆ ⚙️ 👤 ⋮



Your connection is not private

Attackers might be trying to steal your information from **10.88.244.25** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

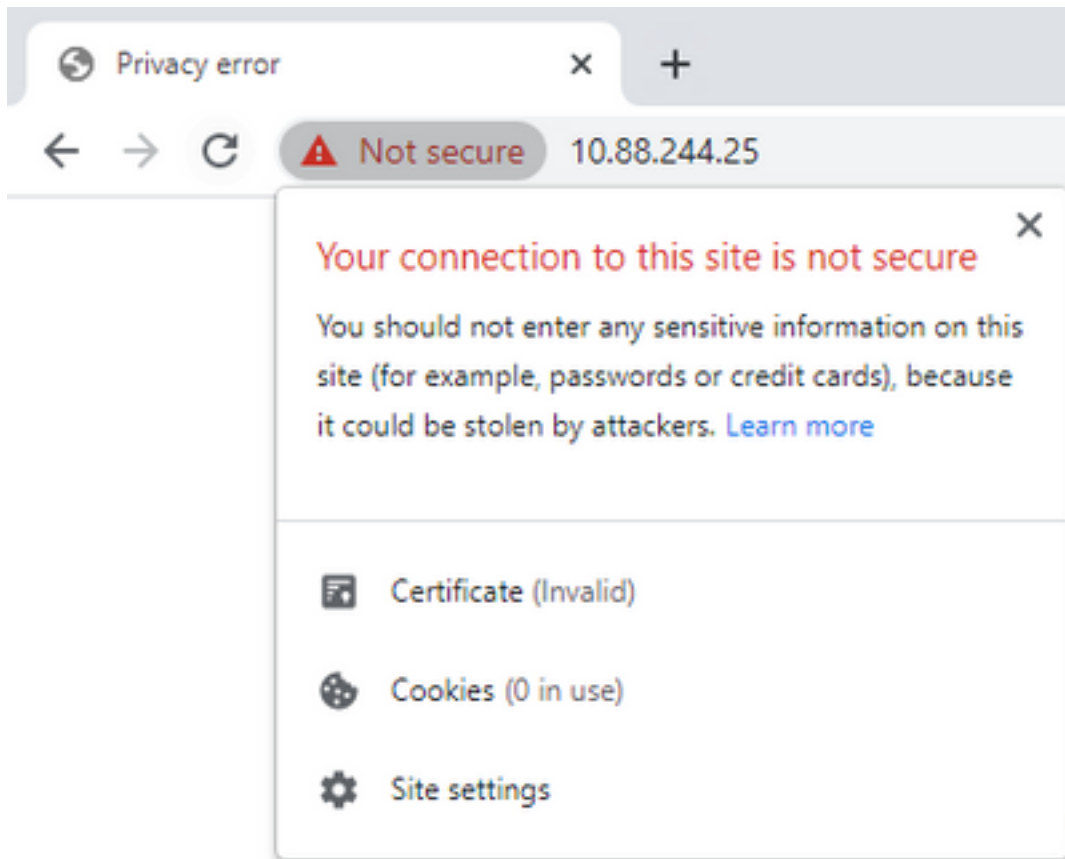
💡 To get Chrome's highest level of security, [turn on enhanced protection](#)

Hide advanced Back to safety

This server could not prove that it is **10.88.244.25**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 10.88.244.25 \(unsafe\)](#)

Note: Click on the view site information option, the certificate is displayed as invalid.



Proactive information

Certificate Registered to the Incorrect Website Name

Ensure that the web certificate has been obtained for all hostnames that your site serves. For example, if your certificate only covers fictional domain `www.vManage-example-test.com`, a visitor who loads the site with the `vManage-example-test.com` (without the `www.` prefix), and if it gets a signed certificate by a Public CA, it is trusted but it gets another error with a certificate name mismatch error.

Note: A common name mismatch error occurs when the common name of the SSL/TLS Certificate does not match the domain or address bar in the browser.

Related Information

- [CSR Decoder](#)
- [Generate a Certificate Signing Request](#)
- [Technical Support & Documentation - Cisco Systems](#)