# Informazioni sul certificato Web per vManage

## Sommario



## Introduzione

Questo documento descrive la differenza tra il certificato Web e i certificati del controller sulla soluzione Cisco SD-WAN. Il presente documento illustra inoltre in dettaglio il certificato Web e ne chiarisce l'utilizzo.

## Prerequisiti

### Requisiti

Conoscenze base dell'infrastruttura a chiave pubblica (PKI).

### Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Certificati utilizzati su Cisco SD-WAN

Nelle soluzioni Cisco SD-WAN sono utilizzati due tipi di certificati, Certificati controller e Certificati Web.

### Certificato Web

Utilizzato per l'accesso Web a vManage. Per impostazione predefinita, Cisco installa un certificato autofirmato. Un certificato autofirmato è un certificato SSL (Secure Sockets Layer) firmato dal proprio creatore.

Tuttavia, Cisco consiglia il proprio certificato di server Web. Ciò è particolarmente utile nei casi in cui le aziende di rete possono disporre di firewall con restrizioni di accesso al Web.
Cisco non fornisce certificati Web pubblici rilasciati da CA (Certification Authority).

> Per ulteriori informazioni su come generare il certificato Web vManage, consultare le guide: Generate Web Server Certificate e How To Generate Self-Signed Web Certificate For vManage

### Certificato controller

Utilizzato per creare connessioni di controllo tra i controller, ad esempio vManage, vBonds, vSmarts.

Si noti che questi certificati sono fondamentali per l'intero control plane dell'infrastruttura SDWAN e devono essere sempre validi.

> Per ulteriori informazioni sui certificati dei controller, consultare la guida: Firma automatica dei certificati tramite Cisco Systems

## Informazioni sul certificato Web per vManage

HTTPS (Hypertext Transfer Protocol Secure) è un protocollo di comunicazione Internet che protegge l'integrità e la riservatezza dei dati tra il computer dell'utente e il sito Web, in questo caso l'interfaccia grafica di vManage. Gli utenti si aspettano una connessione protetta e privata quando accedono a vManage.

Per ottenere una connessione protetta e privata, è necessario ottenere un certificato di protezione. Il certificato viene rilasciato da un'Autorità di certificazione (CA), che esegue le operazioni necessarie per verificare che il dominio vManage appartenga effettivamente all'organizzazione.

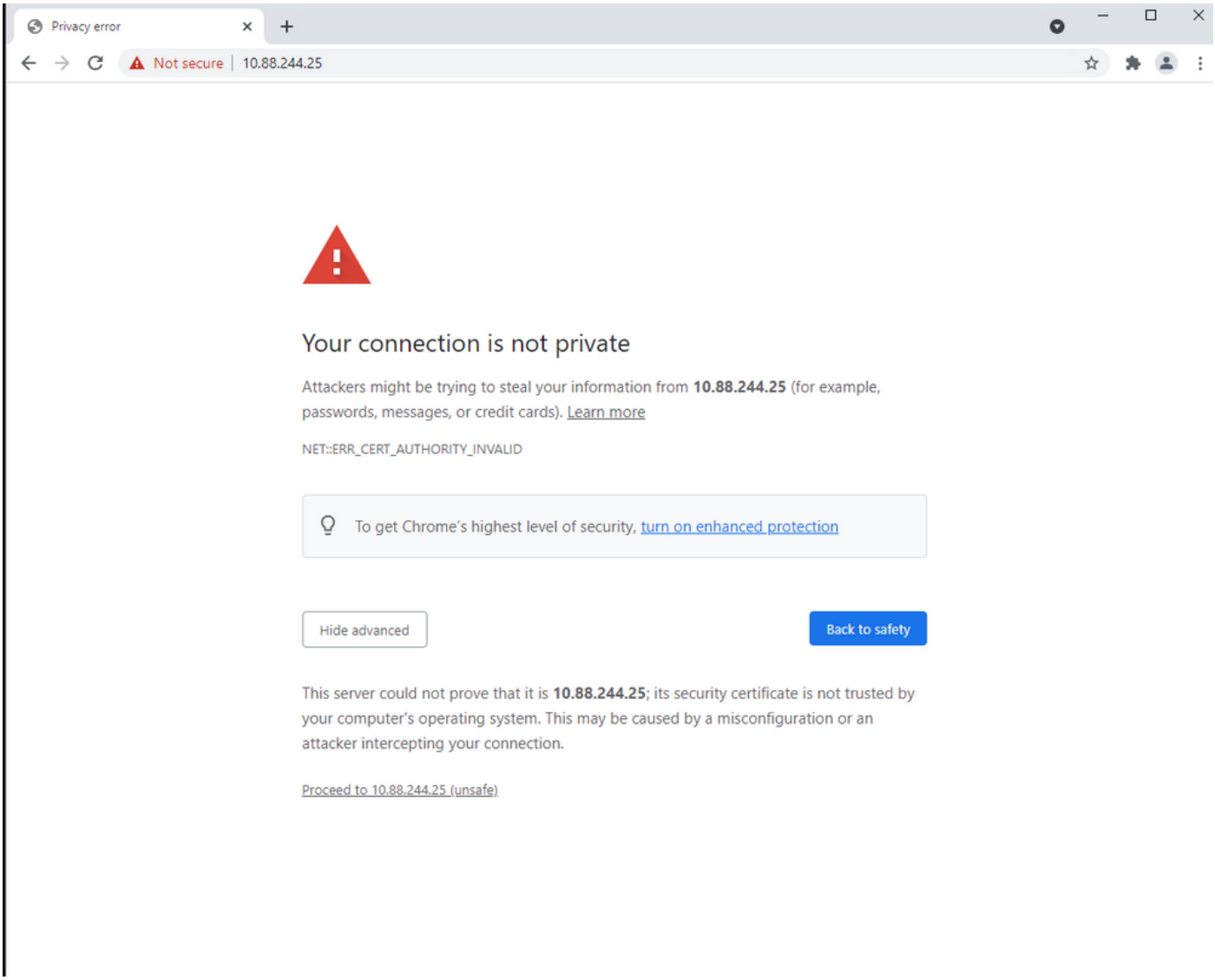
Quando un utente accede a vManage, il PC dell'utente esegue una connessione HTTPS e viene stabilito un tunnel sicuro tra il server vManage e il computer con i certificati SSL installati per l'autenticazione. L'autenticazione del certificato SSL viene eseguita nel computer dell'utente in base al database delle CA radice valide installate nel dispositivo. Di solito, il computer ha già installato più CA come Google, GoDaddy, Enterprise CA (se è il caso), e più enti pubblici. Pertanto, se la richiesta di firma del certificato (CSR) è firmata da Goddady (solo un esempio), è attendibile.

### Messaggio "Connessione non privata" su vManage

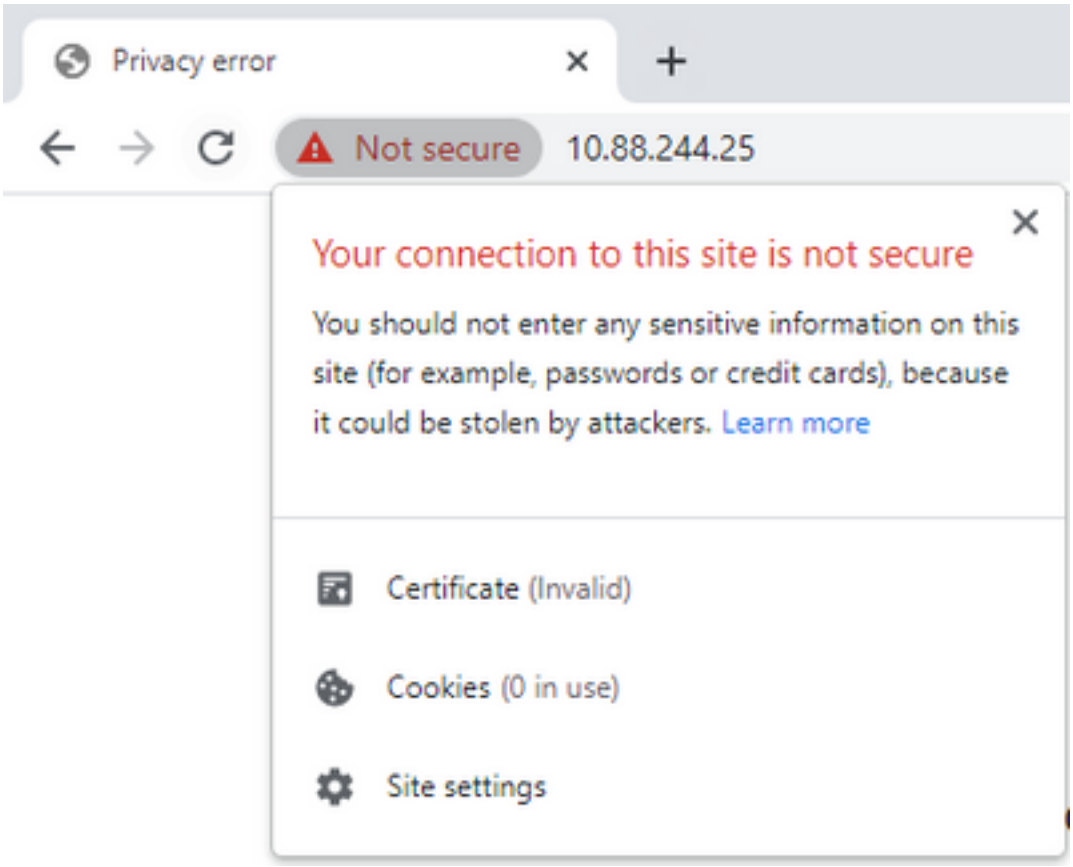
Il certificato autofirmato vManage non è firmato da una CA. È stato firmato dallo stesso vManage

e non dall'autorità di certificazione pubblica né privata, pertanto non è attendibile per un client PC. Per questo motivo, nel browser viene visualizzata una connessione non protetta/errore di privacy per l'URL vManage.

Esempio di errore vManage con il certificato autofirmato predefinito dal browser Google Chrome, come mostrato nell'immagine.




**Nota: Fare clic sull'opzione Visualizza informazioni sito. Il certificato verrà visualizzato come non valido.**




# Informazioni proattive

## Certificato registrato con il nome del sito Web non corretto

Verificare che il certificato Web sia stato ottenuto per tutti i nomi host serviti dal sito. Ad esempio, se il certificato copre solo il dominio fittizio www.vManage-example-test.com, un visitatore che carica il sito con il test vManage-example-example.com (senza www. prefisso) e se ottiene un certificato firmato da una CA pubblica, è attendibile ma ottiene un altro errore con un errore di mancata corrispondenza del nome del certificato.

> **Nota:** un errore di mancata corrispondenza del nome comune si verifica quando il nome comune del certificato SSL/TLS non corrisponde al dominio o alla barra degli indirizzi nel browser.

# Informazioni correlate

- Decoder CSR
- Genera una richiesta di firma del certificato
- Documentazione e supporto tecnico – Cisco Systems