CSM - Come installare i certificati SSL di terze parti per l'accesso GUI

Sommario

Introduzione

Cisco Security Manager (CSM) consente di utilizzare i certificati di sicurezza emessi da autorità di certificazione (CA, Certification Authority) di terze parti. Questi certificati possono essere utilizzati quando il criterio organizzativo impedisce l'utilizzo di certificati autofirmati CSM o richiede ai sistemi di utilizzare un certificato ottenuto da una particolare CA.

TLS/SSL utilizza questi certificati per la comunicazione tra il server CSM e il browser client. In questo documento viene descritto come generare una richiesta di firma di certificato (CSR) in CSM e come installare i certificati di identità e CA radice nello stesso CSM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza dell'architettura dei certificati SSL.
- Conoscenze base di Cisco Security Manager.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Security Manager versione 4.11 e successive.

Creazione di CSR dall'interfaccia utente

In questa sezione viene descritto come generare un CSR.

Passaggio 1. Eseguire la home page di Cisco Security Manager e selezionare **Amministrazione server > Server > Sicurezza > Gestione server singolo > Impostazione certificato.**

Passaggio 2. Inserire i valori richiesti per i campi descritti nella tabella seguente:

Campo	Note sull'utilizzo
Nome paese	Codice paese a due caratteri.
Provincia	Codice provincia o stato a due caratteri o nome completo della provincia.
Località	Codice di due caratteri della città o del paese o nome completo della città o del paese.
Nome organizzazione	Nome completo dell'organizzazione o abbreviazione.
Nome unità organizzativa	Nome completo o abbreviazione del reparto.
Nome server	Nome DNS, indirizzo IP o nome host del computer. Immettere il nome del server con un nome di dominio corretto e risolvibile. Viene visualizzato nel certificato (autofirmato o rilasciato da terze parti). Non specificare l'hos locale o 127.0.0.1.
Indirizzo e-mail	Indirizzo di posta elettronica a cui inviare il messaggio.

Passaggio 3. Fare clic su **Applica** per creare il CSR.

Il processo genera i seguenti file:

- server.key: chiave privata del server.
- server.crt: certificato autofirmato del server.
- server.pk8 - Chiave privata del server in formato PKCS#8.
- server.csr: file CSR (Certificate Signing Request).

Nota: questo è il percorso dei file generati.
~CSCOpx\MDC\Apache\conf\ssl\chain.cer
~CSCOpx\MDC\Apache\conf\ssl\server.crt
~CSCOpx\MDC\Apache\conf\ssl\server.csr
~CSCOpx\MDC\Apache\conf\ssl\server.pk8
~CSCOpx\MDC\Apache\conf\ssl\server.key

Nota: se il certificato è autofirmato, non è possibile modificare queste informazioni.

Caricamento del certificato di identità nel server CSM

In questa sezione viene descritto come caricare il certificato di identità fornito dalla CA al server CSM

1. Trovare lo script utility SSL disponibile in questa posizione

```
NMSROOT\MDC\Apache
```

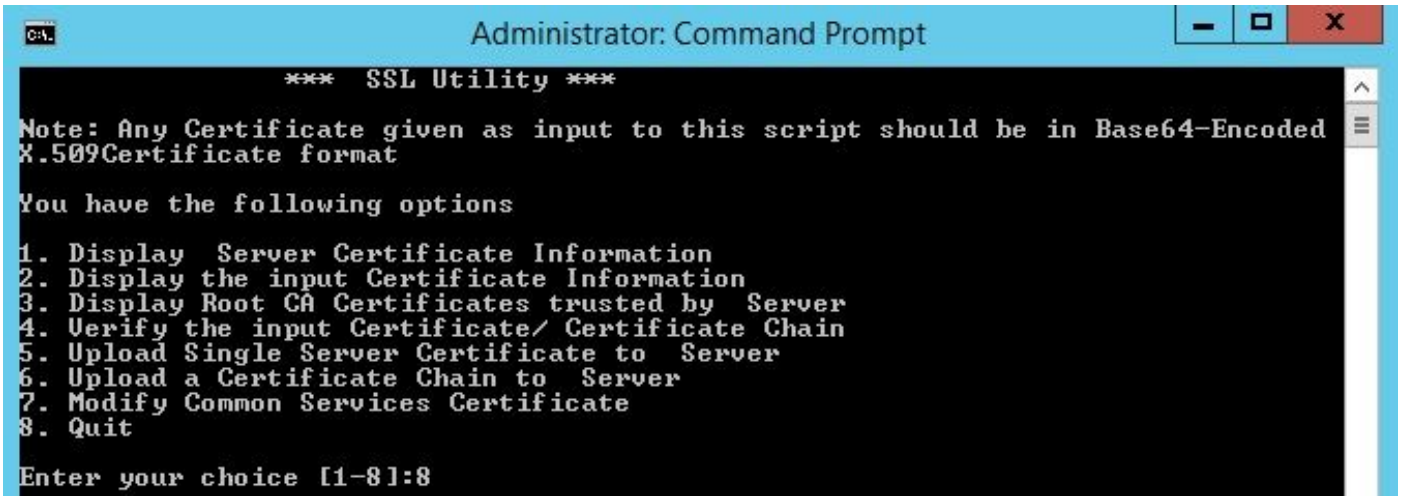
Nota: NMSROOT deve essere sostituito dalla directory in cui è installato CSM.

Questa utilità dispone delle seguenti opzioni.

Numero	Opzione	Cosa fa...
1	Visualizza informazioni certificato server	• Visualizza i dettagli del certificato del server CSM. Per i certificati rilasciati da terze parti, questa opzione visualizza i detta del certificato del server, gli eventuali certificati intermedi e il certificato CA radice.
2	Visualizza le informazioni sul certificato di input	• Verifica se il certificato è valido. Questa opzione accetta un certificato come input e: • Verifica se il certificato è in formato X.509 codificato. • Visualizza l'oggetto del certificato e i dettagli del certificato di rilasc • Verifica se il certificato è valido nel server.
3	Visualizza certificati CA radice attendibili per il server	Genera un elenco di tutti i certificati CA radice.
4	Verificare il certificato di input o la catena di certificati	Verifica se è possibile caricare il certificato server rilasciato da CA di te parti. Quando si sceglie questa opzione, l'utilità: • Verifica se il certificato è in formato Certificato X.509 con codifica Base64. • Verifica se il certificato è valido nel server • Verifica se la chiave privata del server e il certificato del server di i corrispondono. • Verifica se il certificato server può essere tracciato sul certificato C radice richiesto con cui è stato firmato. • Costruisce la catena di certificati, se vengono fornite anche le cate

		intermedie, e verifica se la catena termina con il certificato CA rad appropriato. Al termine della verifica, verrà richiesto di caricare i certificati nel serve CSM. Viene visualizzato un errore: • Se i certificati di input non sono nel formato richiesto • Se la data del certificato non è valida o se il certificato è già scadu • Se non è stato possibile verificare il certificato del server o eseguir traccia di un certificato CA radice. • Se uno dei certificati intermedi non è stato fornito come input. • Se la chiave privata del server è mancante o se non è possibile verificare il certificato del server in fase di caricamento con la chia privata del server. Per risolvere questi problemi, è necessario contattare la CA che ha em i certificati prima di caricare i certificati in CSM.
5	Carica certificato server singolo nel server	Ènecessario verificare i certificati utilizzando l'opzione 4 prima di selezionare questa opzione. Selezionare questa opzione solo se non sono presenti certificati interm ed è presente solo il certificato del server firmato da un certificato CA r visibile. Se la CA radice non è considerata attendibile da CSM, non selezionar questa opzione. In questi casi, è necessario ottenere un certificato CA radice utilizzato firmare il certificato dalla CA e caricare entrambi i certificati utilizzando l'opzione 6. Quando si seleziona questa opzione e si specifica il percorso del certif l'utility: • Verifica se il certificato è in formato certificato X.509 con codifica Base64. • Visualizza l'oggetto del certificato e i dettagli del certificato di rilasc • Verifica se il certificato è valido nel server. • Verifica se la chiave privata del server e il certificato del server di i corrispondono. • Verifica se è possibile tracciare il certificato del server sul certificat radice richiesto utilizzato per la firma. Al termine della verifica, l'utility carica il certificato sul server CiscoWor Viene visualizzato un errore: • Se i certificati di input non sono nel formato richiesto • Se la data del certificato non è valida o se il certificato è già scadu • Se non è stato possibile verificare il certificato del server o eseguir traccia di un certificato CA radice. • Se la chiave privata del server è mancante o se non è possibile verificare il certificato del server in fase di caricamento con la chia privata del server. Per risolvere questi problemi, è necessario contattare la CA che ha em i certificati prima di caricare di nuovo i certificati in CSM.
6	Carica catena di certificati nel server	Ènecessario verificare i certificati utilizzando l'opzione 4 prima di selezionare questa opzione. Selezionare questa opzione se si sta caricando una catena di certificat si carica anche il certificato CA radice, è necessario includerlo tra i cer

		della catena. Quando si seleziona questa opzione e si specifica il percorso dei certif la utility: • Verifica se il certificato è in formato Certificato X.509 con codifica Base64. • Visualizza l'oggetto del certificato e i dettagli del certificato di rilasc • Verifica se il certificato è valido nel server • Verifica se la chiave privata e il certificato del server corrispondon • Verifica se il certificato server può essere tracciato sul certificato C radice utilizzato per la firma. • Costruisce la catena di certificati, se sono specificate catene intermedie, e verifica se la catena termina con il certificato CA rad appropriato. Al termine della verifica, il certificato del server viene caricato nel serve CiscoWorks. Tutti i certificati intermedi e il certificato CA radice vengono caricati e c nell'archivio di attendibilità CSM. Viene visualizzato un errore: • Se i certificati di input non sono nel formato richiesto. • Se la data del certificato non è valida o se il certificato è già scadu • Se non è stato possibile verificare il certificato del server o eseguir traccia di un certificato CA radice. • Se uno dei certificati intermedi non è stato fornito come input. • Se la chiave privata del server è mancante o se non è possibile verificare il certificato del server in fase di caricamento con la chia privata del server. Per risolvere questi problemi, è necessario contattare la CA che ha em i certificati prima di caricare di nuovo i certificati in CiscoWorks.
7	Modifica certificato servizi comuni	Questa opzione consente di modificare la voce Nome host nel certifica servizi comuni. Èpossibile immettere un nome host alternativo se si desidera modifica voce del nome host esistente.



2. Utilizzare l'**opzione 1** per ottenere una copia del certificato corrente e salvarla per riferimento futuro.

3. Arrestare CSM Daemon Manager utilizzando questo comando al prompt dei comandi di

Windows prima di avviare il processo di caricamento dei certificati.

```
net stop crmdmgtd
```

> **Nota**: i servizi CSM non sono disponibili utilizzando questo comando. Verificare che non vi siano distribuzioni attive durante questa procedura.

4. Aprire di nuovo l'utilità SSL. È possibile aprire questa utilità dal prompt dei comandi passando al percorso indicato in precedenza e utilizzando questo comando.

```
perl SSLUtil.pl
```

5. Selezionare l'**opzione 4**. **Verificare il certificato/catena di certificati di input.**

6. Immettere il percorso dei certificati (certificato server e certificato intermedio).

> **Nota**: lo script verifica se il certificato del server è valido. Al termine della verifica, la utility visualizza le opzioni. Se lo script riporta errori durante la convalida e la verifica, la utility SSL visualizza le istruzioni per correggere gli errori. Seguire le istruzioni per risolvere questi problemi, quindi provare a utilizzare la stessa opzione un'altra volta.

7. Selezionare una delle due opzioni successive.

Selezionare l'**opzione 5** se è presente un solo certificato da caricare, ovvero se il certificato del server è firmato da un certificato CA radice.

O

Selezionare l'**opzione 6** se è presente una catena di certificati da caricare, ovvero se sono presenti un certificato server e un certificato intermedio.

> **Nota**: CiscoWorks non consente di procedere con il caricamento se CSM Daemon Manager non è stato arrestato. La utility visualizza un messaggio di avviso se vengono rilevate mancate corrispondenze dei nomi host nel certificato del server da caricare, ma è possibile continuare il caricamento.

8. Inserire questi dettagli obbligatori.

- Posizione del certificato
- Ubicazione degli eventuali certificati intermedi.

L'utilità SSL carica i certificati se tutti i dettagli sono corretti e i certificati soddisfano i requisiti CSM per i certificati di protezione.

9. Riavviare CSM Daemon Manager per rendere effettiva la nuova modifica e abilitare i servizi CSM.

```
net start crmdmgtd
```

Nota: attendere 10 minuti complessivi per riavviare tutti i servizi CSM.

Passaggio 10. Verificare che il CSM utilizzi il certificato di identità installato.

Nota: non dimenticare di installare i certificati CA radice e intermedio nel PC o nel server da cui viene stabilita la connessione SSL al CSM.