CSM - Como instalar certificados SSL de terceiros para acesso à GUI

Contents

Introduction

O Cisco Security Manager (CSM) oferece uma opção para usar certificados de segurança emitidos por autoridades de certificação (CAs) de terceiros. Esses certificados podem ser usados quando a política organizacional impede o uso de certificados autoassinados CSM ou exige que os sistemas usem um certificado obtido de uma CA específica.

O TLS/SSL usa esses certificados para comunicação entre o servidor CSM e o navegador do cliente. Este documento descreve as etapas para gerar uma Solicitação de Assinatura de Certificado (CSR - Certificate Signing Request) no CSM e como instalar a identidade e os certificados CA raiz na mesma.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da arquitetura de certificados SSL.
- Conhecimento básico do Cisco Security Manager.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Security Manager versão 4.11 e posterior.

Criação de CSR a partir da interface do usuário

Esta seção descreve como gerar um CSR.

Etapa 1. Execute a página inicial do Cisco Security Manager e selecione **Server Administration > Server > Security > Single-Server Management > Certificate Setup.**

Etapa 2. Insira os valores necessários para os campos descritos nesta tabela:

Campo	Notas de uso
Nome do país	Código de país de dois caracteres.
Estado ou Província	Código de estado ou província de dois caracteres ou nome completo do estado ou provín
Localidade	Código de cidade ou cidade de dois caracteres ou o nome completo da cidade ou cidade.
Nome da organização	Preencha o nome da sua organização ou uma abreviação.
Nome da unidade da organização	Preencha o nome do seu departamento ou uma abreviação.
Nome do servidor	Nome DNS, endereço IP ou nome de host do computador. Digite o nome do servidor com um nome de domínio apropriado e que possa ser resolvid é exibido no certificado (com assinatura automática ou emitido por terceiros). Host lo 127.0.0.1 não deve ser fornecido.
Endereço de e-mail	Endereço de correio eletrônico para o qual o correio tem de ser enviado.

Etapa 3. Clique em **Apply** para criar o CSR.

O processo gera os seguintes arquivos:

- server.key — Chave privada do servidor.
- server.crt — certificado autoassinado do servidor.

- server.pk8 — A chave privada do servidor no formato PKCS#8.
- server.csr — Arquivo CSR (Certificate Signing Request).

Observação: este é o caminho para os arquivos gerados.
~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 o certificado for um certificado autoassinado, não poderá modificar estas informações.

Carregamento do certificado de identidade no servidor CSM

Esta seção descreve como carregar o certificado de identidade fornecido pela CA para o servidor CSM

Etapa 1 Localizar o script do utilitário SSL disponível neste local

```
NMSROOT\MDC\Apache
```

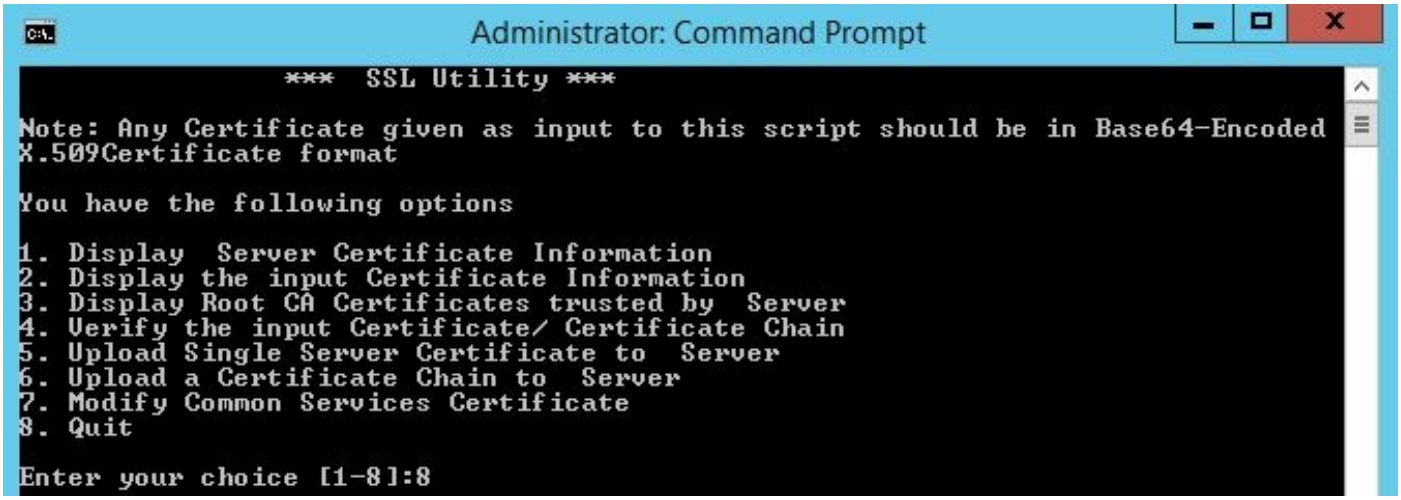
Observação: o NMSROOT deve ser substituído pelo diretório onde o CSM está instalado.

Este utilitário tem estas opções.

Número	Opção	O que faz...
1	Exibir informações do certificado do Servidor	• Exibe os detalhes do certificado do servidor CSM. Para certificados emitidos por terceiros, esta opção exibe os detalhes certificado do servidor, os certificados intermediários, se houver, e o certificado CA raiz.
2	Exibir as informações do certificado de entrada	• Verifica se o certificado é válido. Esta opção aceita um certificado como entrada e: • Verifica se o certificado está no formato de certificado X.509 codif • Exibe o assunto do certificado e os detalhes do certificado de emi • Verifica se o certificado é válido no servidor.
3	Exibir certificados CA raiz confiáveis pelo servidor	Gera uma lista de todos os certificados CA raiz.
4	Verificar o certificado de entrada ou a cadeia de certificados	Verifica se o certificado do servidor emitido por CAs de terceiros pode carregado. Ao escolher esta opção, o utilitário: • Verifica se o certificado está no formato X.509Certificado Codifica Base64. • Verifica se o certificado é válido no servidor • Verifica se a chave privada do servidor e o certificado do servidor entrada correspondem. • Verifica se o certificado do servidor pode ser rastreado até o certif

		CA raiz necessário usando o qual ele foi assinado. • Constrói a cadeia de certificados, se as cadeias intermediárias tar forem fornecidas, e verifica se a cadeia termina com o certificado raiz apropriado. Depois que a verificação for concluída com êxito, você será solicitado carregar os certificados no servidor CSM. O utilitário exibe um erro: • Se os certificados de entrada não estiverem no formato exigido • Se a data do certificado não for válida ou se o certificado já tiver expirado. • Se o certificado do servidor não puder ser verificado ou rastreado um certificado CA raiz. • Se algum dos certificados intermediários não foi fornecido como in • Se a chave privada do servidor estiver ausente ou se o certificado servidor que está sendo carregado não puder ser verificado com a chave privada do servidor. Você deve entrar em contato com a CA que emitiu os certificados para corrigir esses problemas antes de carregar os certificados no CSM. Você deve verificar os certificados usando a opção 4 antes de selecio essa opção.
5	Carregar certificado de servidor único para o servidor	Selecione esta opção, somente se não houver certificados intermediár se houver apenas o certificado do servidor assinado por um certificado raiz proeminente. Se a CA raiz não for confiável pelo CSM, não selecione essa opção. Nesses casos, você deve obter um certificado CA raiz usado para ass certificado da CA e carregar ambos os certificados usando a opção 6. Quando você seleciona essa opção e fornece o local do certificado, o utilitário: • Verifica se o certificado está no formato de certificado X.509 codif em Base64. • Exibe o assunto do certificado e os detalhes do certificado de emi • Verifica se o certificado é válido no servidor. • Verifica se a chave privada do servidor e o certificado do servidor entrada correspondem. • Verifica se o certificado do servidor pode ser rastreado até o certif CA raiz necessário que foi usado para assinatura. Após a conclusão com êxito da verificação, o utilitário carrega o certifi no CiscoWorks Server. O utilitário exibe um erro: • Se os certificados de entrada não estiverem no formato exigido • Se a data do certificado não for válida ou se o certificado já tiver expirado. • Se o certificado do servidor não puder ser verificado ou rastreado um certificado CA raiz. • Se a chave privada do servidor estiver ausente ou se o certificado servidor que está sendo carregado não puder ser verificado com a chave privada do servidor. Você deve entrar em contato com a CA que emitiu os certificados para corrigir esses problemas antes de carregar os certificados no CSM novamente.

		Você deve verificar os certificados usando a opção 4 antes de selecio essa opção. Selecione esta opção se estiver carregando uma cadeia de certificado você também estiver carregando o certificado de CA raiz, deverá inclu como um dos certificados na cadeia. Ao selecionar essa opção e fornecer o local dos certificados, o utilitári • Verifica se o certificado está no formato X.509 Codificado Base64 • Exibe o assunto do certificado e os detalhes do certificado de emi • Verifica se o certificado é válido no servidor • Verifica se a chave privada do servidor e o certificado do servidor correspondem. • Verifica se o certificado do servidor pode ser rastreado até o certif CA raiz usado para assinatura. • Constrói a cadeia de certificados, se forem fornecidas cadeias intermediárias e verifica se a cadeia termina com o certificado CA apropriado.
6	Carregar uma cadeia de certificados para o servidor	Após a conclusão com êxito da verificação, o certificado do servidor é carregado no CiscoWorks Server. Todos os certificados intermediários e o certificado CA raiz são carreg e copiados para o CSM TrustStore. O utilitário exibe um erro: • Se os certificados de entrada não estiverem no formato exigido. • Se a data do certificado não for válida ou se o certificado já tiver expirado. • Se o certificado do servidor não puder ser verificado ou rastreado um certificado CA raiz. • Se algum dos certificados intermédios não foi indicado como inpu • Se a chave privada do servidor estiver ausente ou se o certificado servidor que está sendo carregado não puder ser verificado com a chave privada do servidor. Você deve entrar em contato com a CA que emitiu os certificados para corrigir esses problemas antes de carregar os certificados no CiscoWo novamente.
7	Modificar certificado de serviços comuns	Esta opção permite modificar a entrada do Nome do Host no Certifica Serviços Comuns. Você pode inserir um nome de host alternativo se desejar alterar a en de nome de host existente.



Etapa 2 Use a **Opção 1** para obter uma cópia do certificado atual e salvá-lo para referência futura.

Etapa 3 Parar o Gerenciador de daemon do CSM usando esse comando no Prompt de Comando do Windows antes de iniciar o processo de carregamento do certificado.

```
net stop crmdmgtd
```

> **Observação**: os serviços CSM ficam inativos usando este comando. Verifique se não há implantações ativas durante este procedimento.

Etapa 4 Abrir o Utilitário SSL mais uma vez. Esse utilitário pode ser aberto usando o prompt de comando navegando até o caminho mencionado anteriormente e usando esse comando.

```
perl SSLUtil.pl
```

Etapa 5 Selecione a **Opção 4**. **Verifique a cadeia de certificado/certificado de entrada.**

Etapa 6 Inserir o local dos certificados (certificado do servidor e certificado intermediário).

> **Observação**: o script verifica se o certificado do servidor é válido. Após a conclusão da verificação, o utilitário exibe as opções. Se o script relatar erros durante validação e verificação, o Utilitário SSL exibirá instruções para corrigir esses erros. Siga as instruções para corrigir esses problemas e tente a mesma opção mais uma vez.

Etapa 7 Selecione uma das duas opções a seguir.

Selecione a **Opção 5** se houver apenas um certificado para carregar, ou seja, se o certificado do servidor for assinado por um certificado CA raiz.

OU

Selecione a **Opção 6** se houver uma cadeia de certificados para carregar, ou seja, se houver um certificado de servidor e um certificado intermediário.

> **Observação**: o CiscoWorks não permite prosseguir com o upload se o CSM Daemon Manager não tiver sido interrompido. O utilitário exibe uma mensagem de aviso se houver incompatibilidades de nome de host detectadas no certificado do servidor sendo carregado, mas o carregamento pode ser continuado.

Etapa 8 Insira os detalhes necessários**.**

- Localização do certificado
- Localização dos certificados intermédios, se aplicável.

O Utilitário SSL carrega os certificados se todos os detalhes estiverem corretos e os certificados atenderem aos requisitos do CSM para certificados de segurança.

Etapa 9 Reinicie o CSM Daemon Manager para que a nova alteração entre em vigor e habilite os serviços CSM.

```
net start crmdmgtd
```

> **Observação**: aguarde um total de 10 minutos para que todos os serviços CSM sejam reiniciados.

Etapa 10 Confirme se o CSM está usando o certificado de identidade instalado.

> **Observação**: não se esqueça de instalar os certificados CA raiz e intermediários no PC ou servidor de onde a conexão SSL está sendo estabelecida para o CSM.