CS - Como instalar Certificados da terceira SSL para o acesso de GUI

Índice

Introdução

O Cisco Security Manager (CS) fornece uma opção para usar os Certificados da Segurança emitidos pelas autoridades de certificação da terceira (CA). Estes Certificados podem ser usados quando a política organizacional impede de usar certificados auto-assinados CS ou exige sistemas usar um certificado obtido de CA particular.

TLS/SSL usa estes Certificados para uma comunicação entre o server CS e o navegador cliente. Este documento descreve as etapas para gerar uma solicitação de assinatura de certificado (CSR) no CS e como instalar a identidade e os certificados CA raiz no mesmos.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da arquitetura dos Certificados SSL.
- Conhecimento básico do Cisco Security Manager.

Componentes Utilizados

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

- Versão 4.11 e mais recente do Cisco Security Manager.

Criação CSR da interface do utilizador

Esta seção descreve como gerar um CSR.

Etapa 1. Execute o Home Page do Cisco Security Manager e selecione o **> segurança da administração de servidor > do server > o Gerenciamento do servidor único > a instalação do certificado.**

Etapa 2. Incorpore os valores exigidos para os campos descritos nesta tabela:

Campo	Notas de uso
Nome do país	Código de país de dois caráteres.
Estado ou província	Código do estado ou da província de dois caráteres ou o nome completo do estado ou província.
Localidade	Código da cidade ou da cidade de dois caráteres ou o nome completo da cidade ou da ci
Nome de organização	Termine o nome de sua organização ou de uma abreviatura.
Nome da unidade da organização	Termine o nome de seu departamento ou de uma abreviatura.
Nome do servidor	Nome de DNS, endereço IP ou nome do host do computador. Dê entrada com o nome do servidor com um Domain Name apropriado e solucionável. indicado em seu certificado (se auto-assinado ou terceira parte emitido). O host loc 127.0.0.1 não devem ser dados.
Endereço email	Endereço email a que o correio tem que ser enviado.

Etapa 3. O clique **aplica-se** para criar o CSR.

O processo gerencie os seguintes arquivos:

- server.key — A chave privada do server.
- server.crt — O certificado auto-assinado do server.

- server.pk8 — A chave privada do server no formato PKCS#8.
- server.csr — Arquivo da solicitação de assinatura de certificado (CSR).

Note: Este é o trajeto para os arquivos gerados.
~CSCOpx \ CDM \ Apache \ conf \ SSL \ chain.cer
~CSCOpx \ CDM \ Apache \ conf \ SSL \ server.crt
~CSCOpx \ CDM \ Apache \ conf \ SSL \ server.csr
~CSCOpx\MDC\Apache\conf\ssl\server.pk8
~CSCOpx \ CDM \ Apache \ conf \ SSL \ server.key

Note: Se o certificado é um certificado auto-assinado, a seguir você não pode alterar esta informação.

Transferência de arquivo pela rede do certificado de identidade no server CS

Esta seção descreve como transferir arquivos pela rede o certificado de identidade fornecido por CA ao server CS

Etapa 1 Encontre o script utilitário SSL disponível neste lugar

```
NMSROOT\MDC\Apache
```

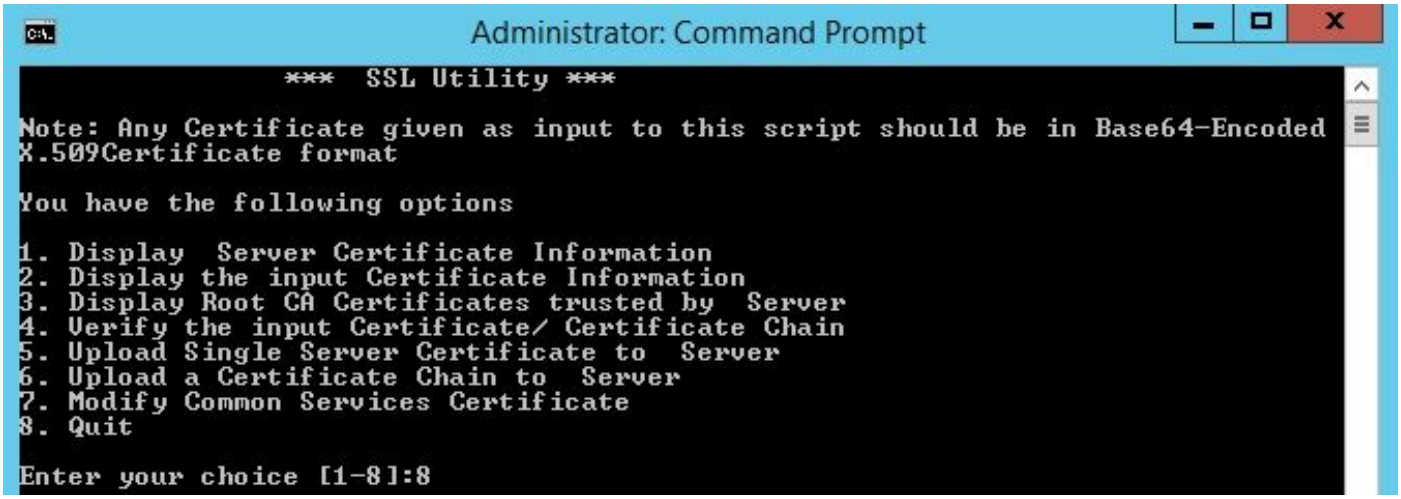
Note: O NMSROOT deve ser substituído pelo diretório onde o CS é instalado.

Esta utilidade tem estas opções.

Número	Opção	O que faz…
1	Informação do certificado de servidor do indicador	• Indica os detalhes certificados do server CS. Para a terceira parte emitida os Certificados, esta opção indicam os detalhes do certificado de servidor, dos Certificados intermediários, eventualmente, e do certificado CA raiz.
2	Indique a informação do certificado da entrada	• Verifica se o certificado é válido. Esta opção aceita um certificado como uma entrada e: • Verifica se o certificado está no formato do certificado X.509 codificado. • Indica o assunto do certificado e os detalhes do certificado de em • Verifica se o certificado é válido no server.
3	Certificados CA raiz do indicador confiados pelo server	Gerencie uma lista de todos os certificados CA raiz.
4	Verifique o certificado ou o certificate chain da entrada	Verifica se o certificado de servidor emitido pela terceira parte CA, po transferido arquivos pela rede. Quando você escolher esta opção, a utilidade: • Verifica se o certificado está em Base64 codificou o formato X.509Certificate. • Verifica se o certificado é válido no server

		• Verifica se o certificado de servidor da chave privada e da entrad server combina. • Verifica se o certificado de servidor pode ser seguido à utilização exigida do certificado CA raiz que esteve assinado. • Constrói o certificate chain, se as correntes intermediárias são da igualmente, e verifica se a corrente termina com o certificado CA apropriado. Depois que a verificação é terminada com sucesso, você está alertad transferir arquivos pela rede os Certificados ao server CS. A utilidade indica um erro: • Se os Certificados da entrada não são formato dentro exigido • Se a data do certificado é inválida ou se o certificado tem expirad • Se o certificado de servidor não poderia ser verificado ou seguido certificado CA raiz. • Se alguns dos Certificados intermediários não foram dados como entrada. • Se a chave privada do server falta ou se o certificado de servidor está sendo transferido arquivos pela rede não poderia ser verifica com a chave privada do server. Você deve contactar CA que emitiu os Certificados para corrigir estes problemas antes que você transfira arquivos pela rede os Certificados CS. Você deve verificar os Certificados usando a opção 4 antes que você selecione esta opção. Selecione esta opção, simplesmente se não há nenhum Certificados intermediário e há somente o certificado de servidor assinado por um certificado CA raiz proeminente. Se a CA raiz não é uma confiada pelo CS, não selecione esta opção. Nesses casos, você deve obter um certificado CA raiz usado assinan certificado de CA e transferir arquivos pela rede ambos os Certificado usando a opção 6. Quando você selecionar esta opção, e fornecer o lugar do certificado, utilidade: • Verifica se o certificado está em Base64 codificou o formato do certificado X.509. • Indica o assunto do certificado e os detalhes do certificado de em
5	Certificado de servidor único da transferência de arquivo pela rede ao server	• Verifica se o certificado é válido no server. • Verifica se o certificado de servidor da chave privada e da entrad server combina. • Verifica se o certificado de servidor pode ser seguido ao certificad raiz exigido que foi usado assinando. Depois que a verificação é terminada com sucesso, a utilidade transfe arquivos pela rede o certificado ao servidor ciscoworks. A utilidade indica um erro: • Se os Certificados da entrada não são formato dentro exigido • Se a data do certificado é inválida ou se o certificado tem expirad • Se o certificado de servidor não poderia ser verificado ou seguido certificado CA raiz. • Se a chave privada do server falta ou se o certificado de servidor

		está sendo transferido arquivos pela rede não poderia ser verifica com a chave privada do server. Você deve contactar CA que emitiu os Certificados para corrigir estes problemas antes que você transfira arquivos pela rede os Certificados CS outra vez. Você deve verificar os Certificados usando a opção 4 antes que você selecione esta opção. Selecione esta opção, se você está transferindo arquivos pela rede u certificate chain. Se você igualmente está transferindo arquivos pela r certificado CA raiz igualmente, você deve inclui-lo como um dos Certificados na corrente. Quando você selecionar esta opção e fornecer o lugar dos Certificado utilidade: • Verifica se o certificado está em Base64 codificou o formato do certificado X.509. • Indica o assunto do certificado e os detalhes do certificado de em • Verifica se o certificado é válido no server • Verifica se a chave privada do server e o certificado de servidor combinam. • Verifica se o certificado de servidor pode ser seguido ao certificad raiz que foi usado assinando. • Constrói o certificate chain, se as correntes intermediárias são da verifica se a corrente termina com o certificado CA raiz apropriad
6	Transfira arquivos pela rede um certificate chain ao server	Depois que a verificação é terminada com sucesso, o certificado de servidor está transferido arquivos pela rede ao servidor ciscoworks. Todos os Certificados intermediários e o certificado CA raiz são transferidos arquivos pela rede e copiados ao CS TrustStore. A utilidade indica um erro: • Se os Certificados da entrada não são formato dentro exigido. • Se a data do certificado é inválida ou se o certificado tem expirad • Se o certificado de servidor não poderia ser verificado ou seguido certificado CA raiz. • Se alguns dos Certificados intermediários não foram dados como entrada. • Se a chave privada do server falta ou se o certificado de servidor está sendo transferido arquivos pela rede não poderia ser verifica com a chave privada do server. Você deve contactar CA que emitiu os Certificados para corrigir estes problemas antes que você transfira arquivos pela rede os Certificados CiscoWorks outra vez.
7	Altere o certificado comum dos serviços	Esta opção permite que você altere a entrada de nome de host no certificado comum dos serviços. Você pode entrar em um hostname alternativo se você deseja mudar entrada de nome de host existente.



Etapa 2 Use a opção 1 para obter uma cópia do certificado atual e para salvar a para a referência futura.

Etapa 3 Pare o daemon manager CS que usa este comando no comando prompt de Windows antes de começar o processo da transferência de arquivo pela rede do certificado.

```
net stop crmdmgtd
```

> Note: Os serviços CS vão abaixo de usar este comando. Certifique-se que não há nenhuma disposições ativa durante este procedimento.

Etapa 4 Abra a utilidade SSL mais uma vez. Esta utilidade pode ser aberta usando o comando prompt navegando ao trajeto previamente mencionado e usando este comando.

```
perl SSLUtil.pl
```

A opção seleta 4. da etapa 5 verifica o certificate chain do certificado da entrada.

A etapa 6 entra no lugar dos Certificados (certificado de servidor e certificado do intermediário).

> Note: O script verifica se o certificado de servidor é válido. Depois que a verificação está completa, a utilidade indica as opções. Se os erros dos relatórios do script durante a validação e a verificação, as instruções de indicadores de serviço público SSL para corrigir estes erros. Siga as instruções para corrigir aqueles problemas e para tentar então o mesmo opção um mais tempo.

A etapa 7 seleciona algumas das duas opções seguintes.

Selecione a opção 5 se há somente um certificado a transferir arquivos pela rede, isso é se o certificado de servidor é assinado por um certificado CA raiz.

> OU

Selecione a opção 6 se há um certificate chain a transferir arquivos pela rede, isso é se há um certificado de servidor e um certificado do intermediário.

Note: Os CiscoWorks não reservam continuar com a transferência de arquivo pela rede se o daemon manager CS não foi parado. A utilidade indica um mensagem de advertência se há umas más combinações do hostname detectadas no certificado de servidor que está sendo transferido arquivos pela rede, mas a transferência de arquivo pela rede pode ser continuada.

Etapa 8 Incorpore estes detalhes exigidos.

- Lugar do certificado
- Lugar de Certificados intermediários, se exister.

A utilidade SSL transfere arquivos pela rede os Certificados se todos os detalhes estão corretos e os Certificados cumprem exigências CS para Certificados da Segurança.

Reinício da **etapa 9 o** daemon manager CS para que a mudança nova tome o efeito e permitam serviços CS.

```
net start crmdmgtd
```

Note: Espere para um macacão dos minutos 10 para que todos os serviços CS sejam reiniciados.

A etapa 10 confirma o CS está usando o certificado de identidade instalado.

Note: Não esqueça instalar os certificados de CA da raiz e do intermediário no PC ou o server de onde a conexão SSL stablished ao CS.