

Apoio chave do bit IEA 2048 para o CSR no exemplo de configuração IEA

Índice

[Introdução](#)

[Configurar](#)

[Gerencia um certificado](#)

[Importe um certificado](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como gerar o apoio chave de 2048 bit para a solicitação de assinatura de certificado (CSR) no dispositivo da criptografia de Cisco IronPort (IEA).

Configurar

A maioria das autoridades de certificação (CA) indicaram um pedido explícito para ter todos os CSR gerados com um par de chaves de bit do comprimento 2048. À revelia, a versão 6.5 IEA usa um comprimento chave de 1024 bit para a geração de par chave. A fim forçar o IEA a gerar um par de chaves do comprimento 2048, use o comando do keytool como descrito aqui.

Gerencia um certificado

1. Entre ao IEA CLI
2. No menu principal, datilografe x a fim deixar cair no shell.
3. Mude ao usuário de raiz:

```
$ su -
```

4. Execute o keytool a fim criar um keystore novo:

```
# /usr/local/postx/server/jre/bin/keytool -genkey -alias <server alias>
-keyalg RSA -keysize 2048 -keystore <name the new keystore>
  *alias should be what the server is known as externally when customers
log into the device
  *When prompted for password use a easily remembered password
  *Enter in all requested information when prompted for the certificate
request, make special note of the next question:
  --- What is your first and last name?
[Unknown]: server1.example.com
```

*For this question enter in the fully qualified domain name of the system

*The name of the newkeystore should be in the format <name>.keystore where name should include the current date

Example: enterpriseks20130108.keystore

```
root@ies360 ~
# /usr/local/postx/server/jre/bin/keytool -genkey -alias stevesiea.cisco.com -keyalg RSA -keysize 2048 -keystore /usr/local/p
ostx/server/conf/2013_05_13.keystore
Enter keystore password: password
What is your first and last name?
[Unknown]: stevesiea.cisco.com
What is the name of your organizational unit?
[Unknown]: TAC
What is the name of your organization?
[Unknown]: Cisco
What is the name of your City or Locality?
[Unknown]: Morrisville
What is the name of your State or Province?
[Unknown]: NC
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=stevesiea.cisco.com, OU=TAC, C=Cisco, L=Morrisville, ST=NC, C=US correct?
[no]: yes

Enter key password for <stevesiea.cisco.com>
(RETURN if same as keystore password):

root@ies360 ~
#
```

5. Execute o keytool a fim criar um arquivo CSR:

```
# /usr/local/postx/server/jre/bin/keytool -certreq -keyalg RSA -alias <server alias>
-file <servername>.csr -keystore <name of the new keystore>
```

```
root@ies360 ~
# /usr/local/postx/server/jre/bin/keytool -certreq -keyalg RSA -alias stevesiea.cisco.com -file /home/admin/stevesiea.csr -ke
yystore /usr/local/postx/server/conf/2013_05_13.keystore
Enter keystore password: password

root@ies360 ~
#
```

6. Forneça o arquivo CSR ao Certificate Authority a fim gerar um certificado. Assegure-se de que você o submeta como uma requisição de assinatura de Certificate do servidor da Web Apache.
7. Depois que você recebe o arquivo de .cer de CA, continue às próximas etapas.

Importe um certificado

Nota: A senha usada quando você gerencie o CSR **deve** combinar a senha do keystore para que estes procedimentos trabalhem. Se o CSR era fora-caixa criada, a senha entrada **deve** combinar a senha do keystore para que estes procedimentos trabalhem.

Você deve acorrentar o certificado corretamente

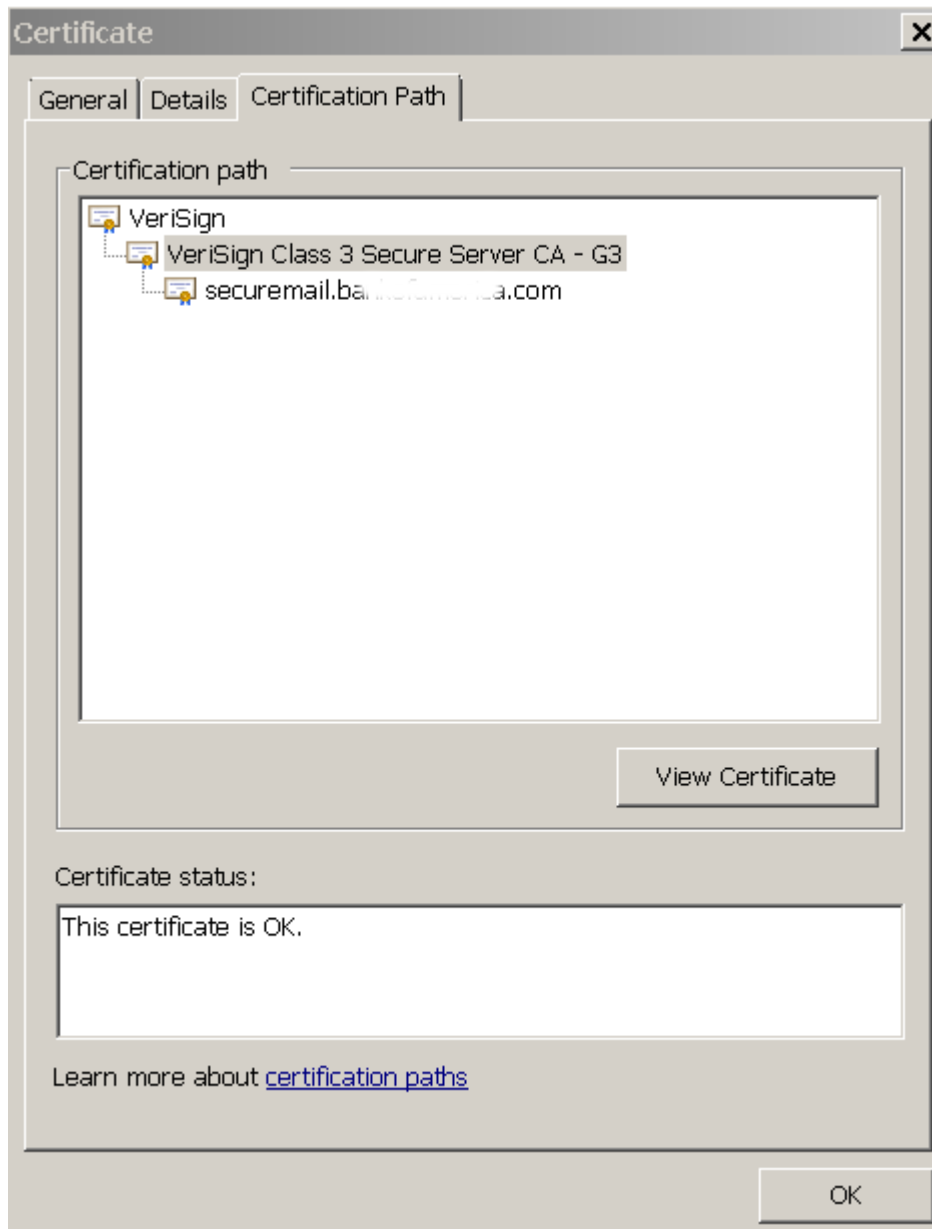
1. Cada certificado de CA deve ser extraído do arquivo CER recebido de CA e fundido então junto em um editor de texto.

Nota: Este é o mais fácil feito de uma máquina de Microsoft Windows. Outros sistemas operacionais funcionam mas são mais difíceis de extrair.

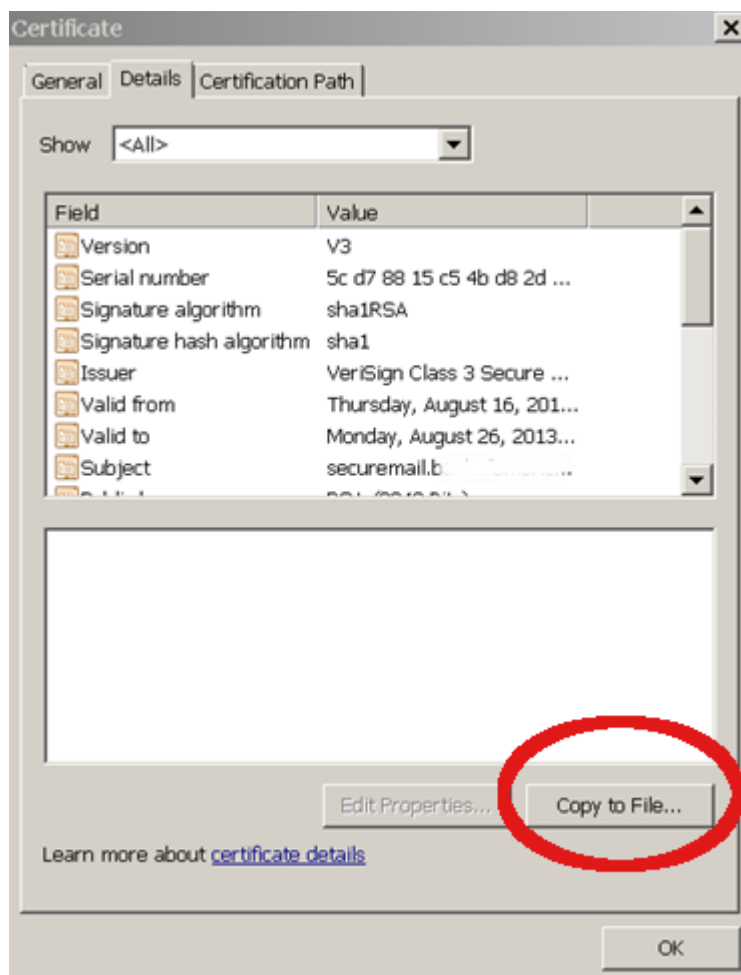
Os Certificados devem ser acorrentados nesta ordem: 1.Domain 2. 3.Root intermediário

Fazer duplo clique a fim abrir o arquivo certificado (arquivo .CER), e clique então a aba do

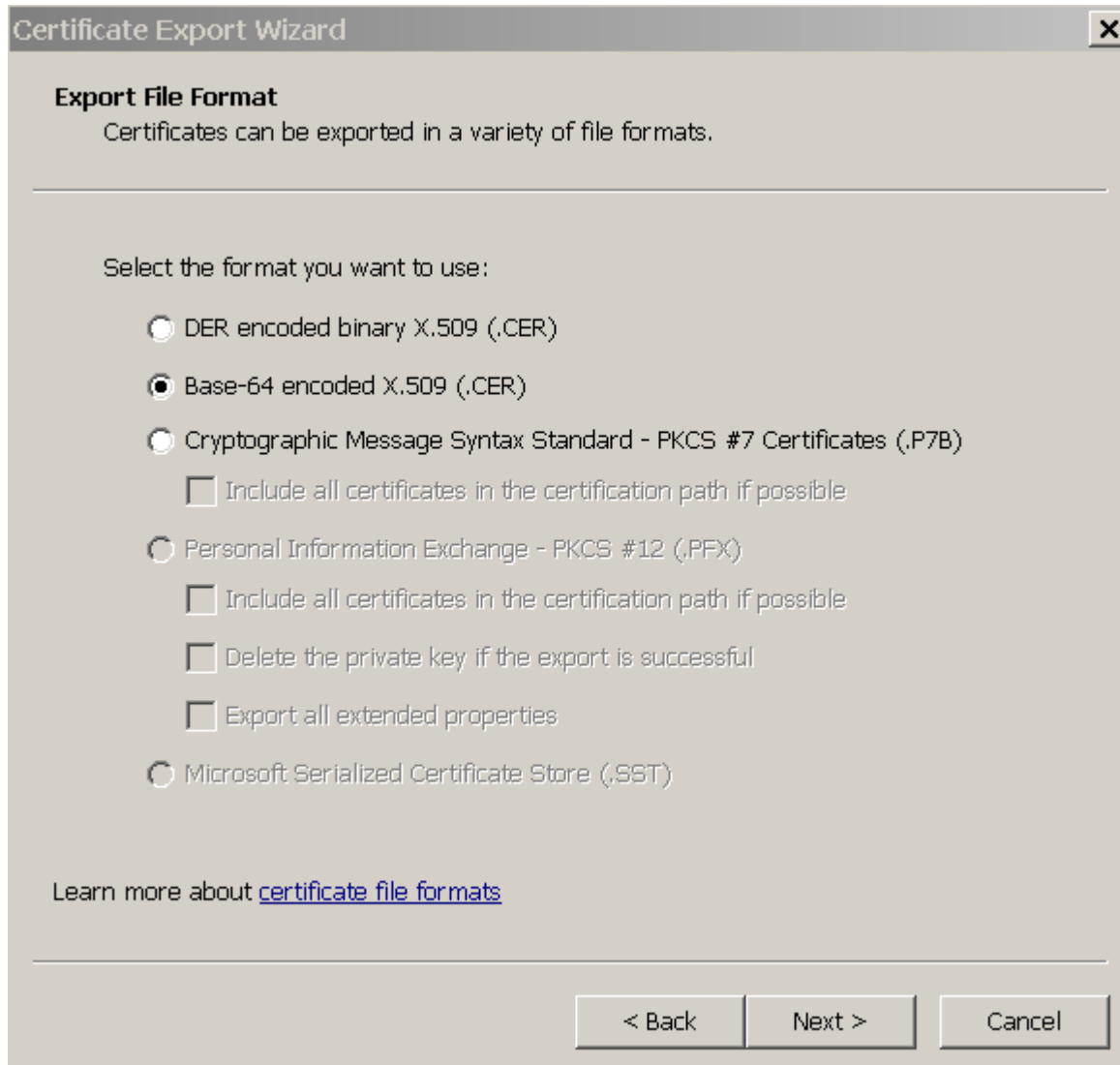
caminho de certificação:



Comece com o de nível médio do caminho de certificação, clique a aba dos **detalhes**, clique a **cópia para arquivar**, e nomeie-a então **1.CER**.

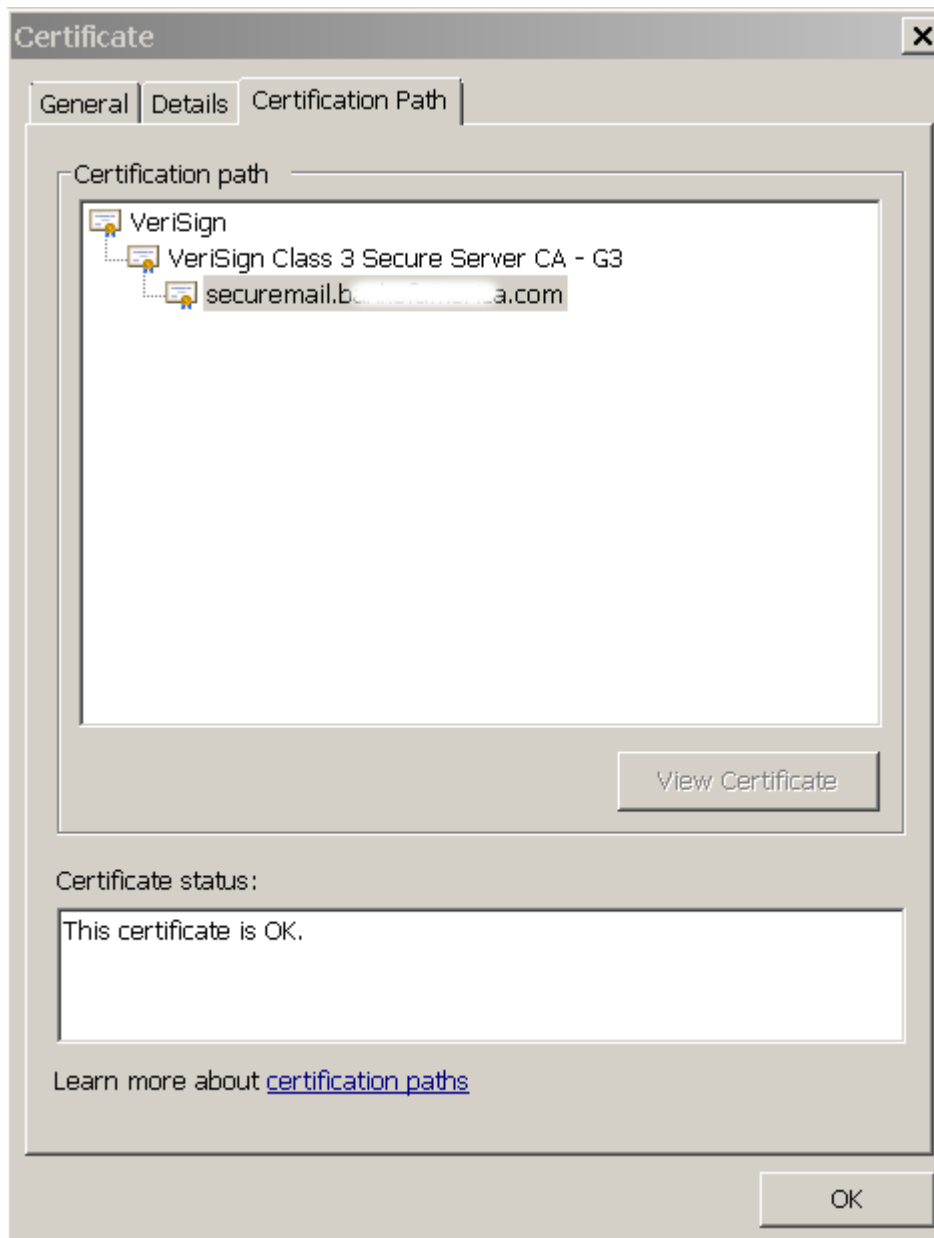


Selecione **Base-64** codificou X.509(.CER).



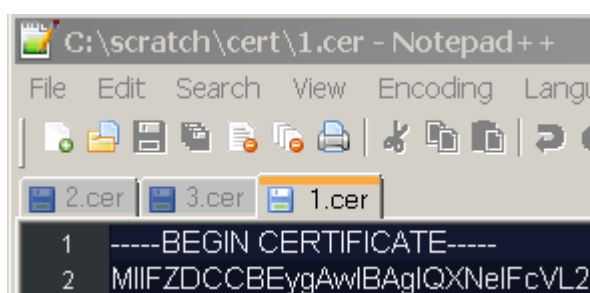
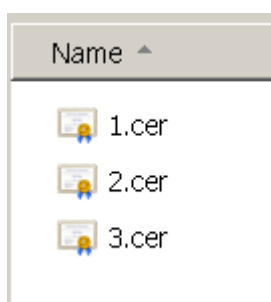
Repita para o nível superior CA, e nomeie-o **2.CER**.

Repita para o certificado de servidor, e nomeie-o **3.CER**.



Use um editor de texto

(**não** bloco de notas, mas trabalhos notepad++ bem) a fim abrir todos os três arquivos **X.CER** e combiná-los em ordem (1 na parte superior, e 3 na parte inferior):



Nota: Não deve haver nenhuma linha vazia entre Certificados e nenhuma linha vazia na parte inferior.

Salvar como <servername>.CER.

Transfira arquivos pela rede o arquivo <servername>.CER ao IEA em /home/admin/<servername.cer> com FTP ou SCP.

Copie /home/admin/ <servername.cer> a /usr/local/postx/server/conf:

```
root@iea360 /home/admin
# cp /home/admin/stevesiea.cer /usr/local/postx/server/conf

root@iea360 /home/admin
#
```

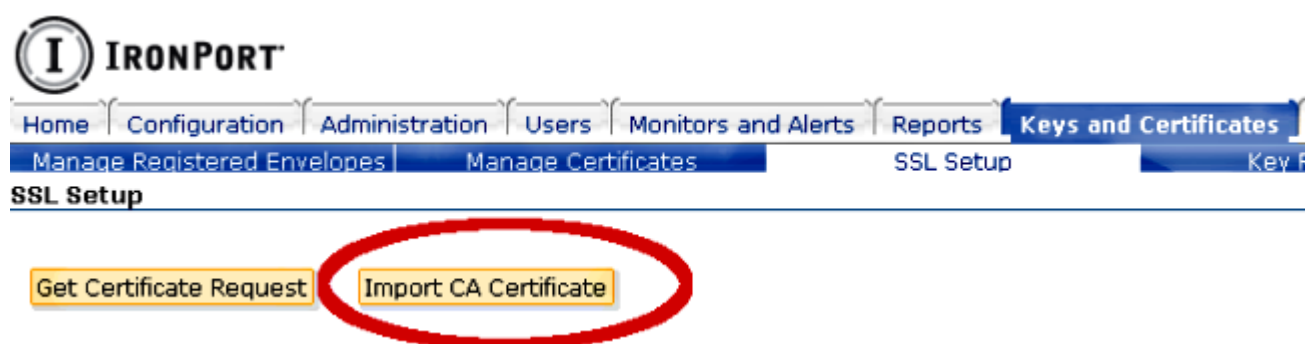
2. Use o IEA GUI a fim importar o certificado [chaves e Certificados | SSL Setup].

Nota: Keystore = [Install Directory] /conf/enterprisenamestore.keystore ou o nome atual de seu arquivo do keystore.

Certificado = /usr/local/postx/server/conf/NEWCERT.CER.

Verifique a confiança CA Certs.

Clique o certificado de importação



3. (Opcional -- Se um keystore novo deve ser criado). Do IEA GUI, diga o IEA para usar o keystore novo:

Escolha a configuração | Servidor de Web e proxys | Servidor da Web | Ouvintes da conexão | HTTPS

Datilografe dentro o trajeto ao arquivo novo do keystore:

Exemplo: `#{postx.home}/conf/2013_5_13.keystore`

The screenshot shows the IronPort configuration interface. The 'Keystore File' field is highlighted with a red oval. The value entered is `#{postx.home}/conf/keystore`. Other visible configuration items include 'Connection Listener Name' (HTTPS), 'Accept Count' (100), 'Maximum Threads' (150), 'Minimum Spare Threads' (5), 'Maximum Spare Threads' (15), 'Keep-Alive Requests' (100), 'Maximum HTTP Header Size (bytes)' (4096), 'Maximum HTTP POST Size (bytes)' (104857600), 'Socket Receive Buffer Size (bytes)' (25188), 'Socket Send Buffer Size (bytes)' (65536), 'HTTP Server Header' (unknown), 'SSL Protocol' (TLS), and 'SSL Algorithm' (SunX509).

4. Distribua mudanças e reinicie o adaptador S TP.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.