Soporte dominante del bit IEA 2048 para el CSR en el ejemplo de configuración IEA

Contenido

Introducción

Este documento describe cómo generar el soporte dominante de 2048 bits para el pedido de firma de certificado (CSR) en el dispositivo del cifrado de Cisco IronPort (IEA).

Configurar

La mayor parte de las autoridades de certificación (CA) han expuesto una petición explícita para tener todos los CSR generados con un par clave de bit de la longitud 2048. Por abandono, la versión 6.5 IEA utiliza la longitud de clave de 1024 bits para la generación de par clave. Para forzar el IEA a generar un par clave de la longitud 2048, utilice el comando del keytool según lo descrito aquí.

Genere un certificado

1. Inicie sesión al IEA CLI

2. En el menú principal, teclee **x** para caer en el shell.

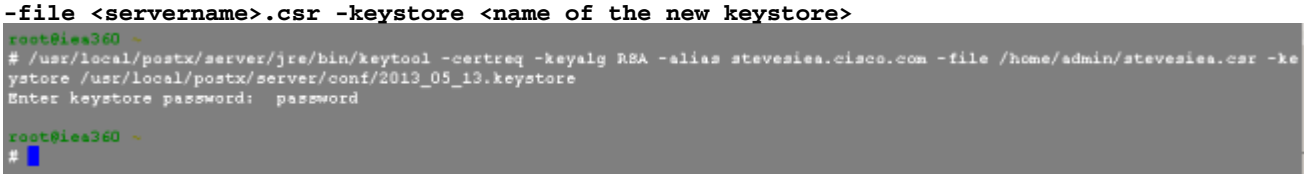
3. Cambie al usuario raíz:
```
$ su -
```

4. Ejecute el keytool para crear un nuevo keystore:
```
    # /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
```

5. Ejecute el keytool para crear un archivo CSR:

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



6. Proporcione el archivo CSR al Certificate Authority para generar un certificado. Asegúrese que usted lo someta como servidor Web Apache solicitud de firma de Certficate.
7. Después de que usted reciba el archivo de .cer de CA, proceda a los siguientes pasos.

Importe un certificado

Nota: La contraseña usada cuando usted genera el CSR **debe** hacer juego la contraseña del keystore para que estos procedimientos trabajen. Si el CSR era apagado-cuadro creado, la contraseña entrada **debe** hacer juego la contraseña del keystore para que estos procedimientos trabajen.

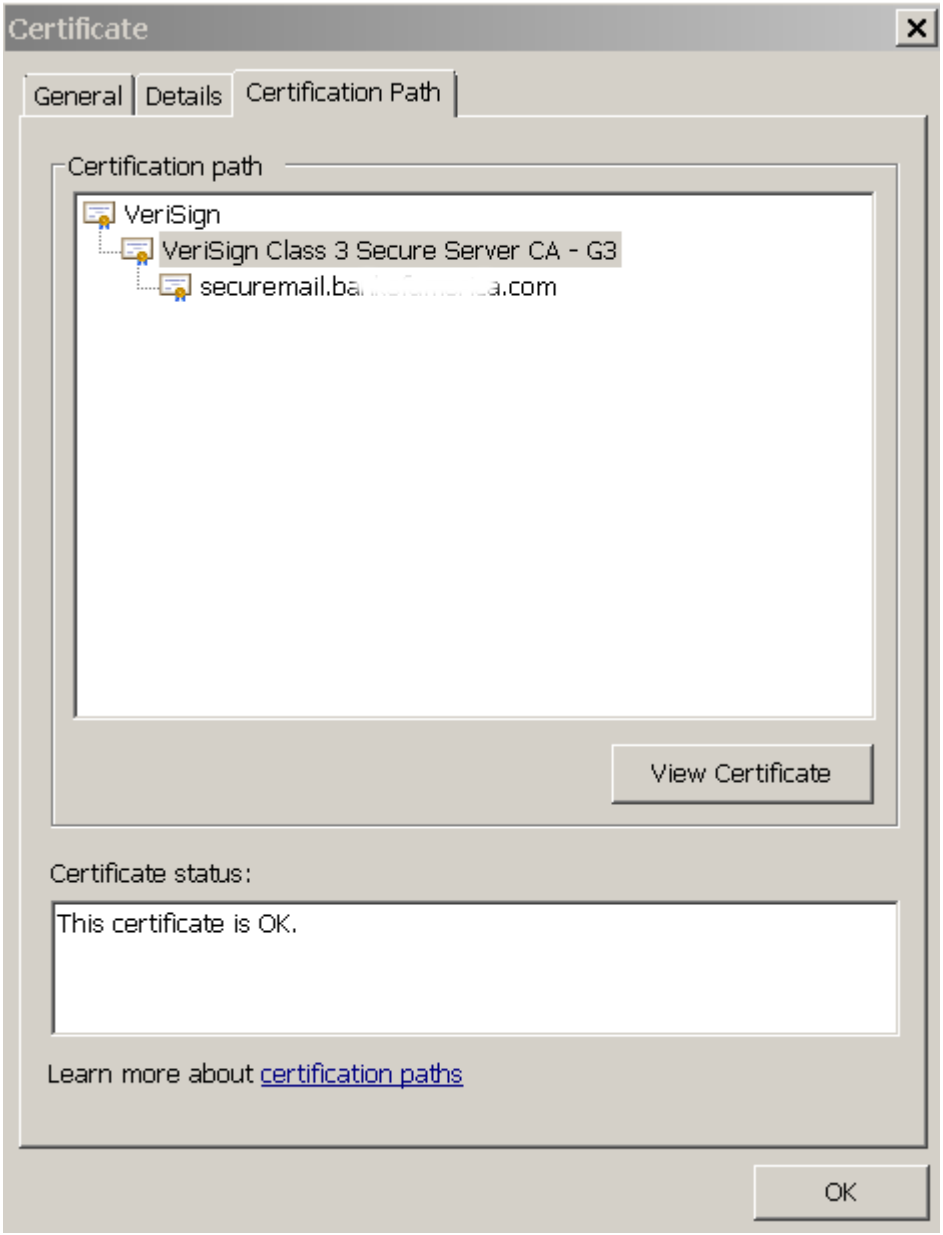
Usted debe encadenar el certificado correctamente

1. Cada certificado de CA se debe extraer del archivo CER recibido de CA y después combinado junto en un editor de textos.

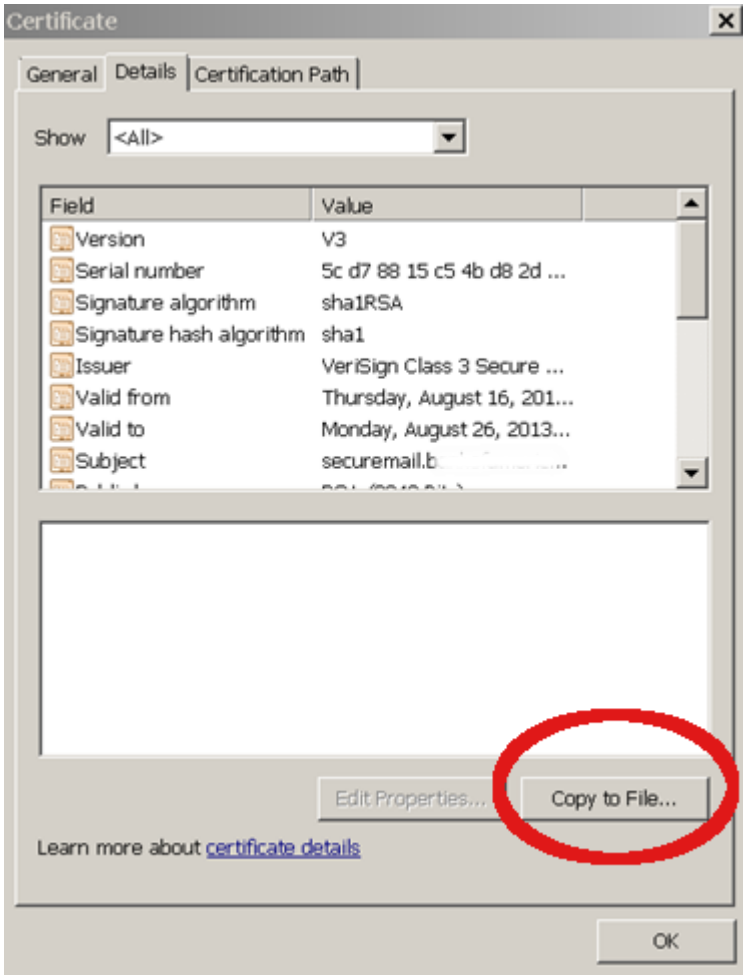
   Nota: Esto es la más fácil hecha de una máquina de Microsoft Windows. Otros sistemas operativos funcionan pero son más difíciles de extraer.

   Los Certificados se deben encadenar en esta orden: 1.Domain 2. 3.Root intermedio

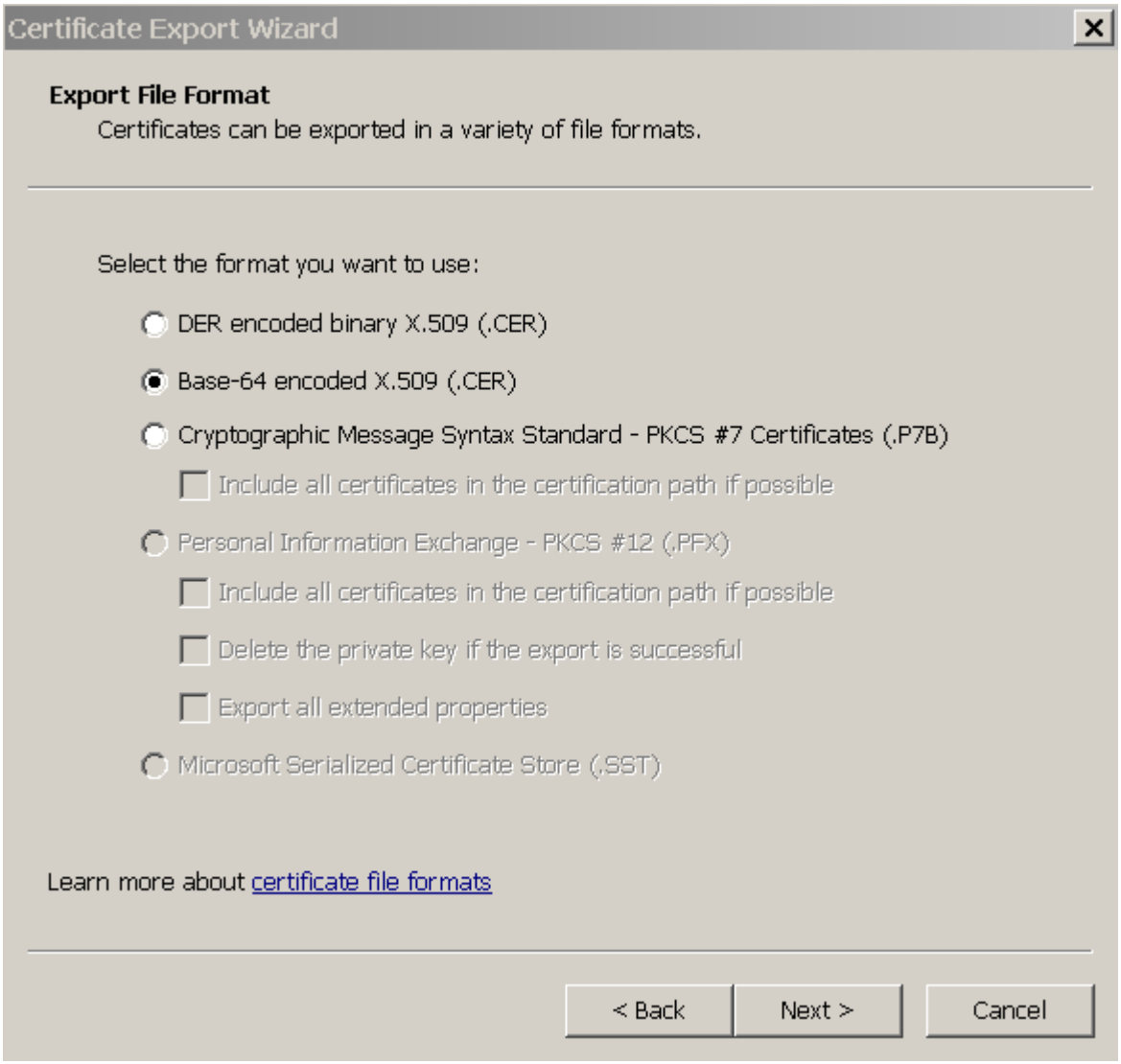
Haga doble clic para abrir el archivo de certificado (archivo .CER), y después haga clic la lengueta del **trayecto de certificación**:



Comience con el de nivel medio del trayecto de certificación, haga clic la lengueta de los **detalles**, haga clic la **copia para clasifiar**, y después nómbrela **1.CER**.

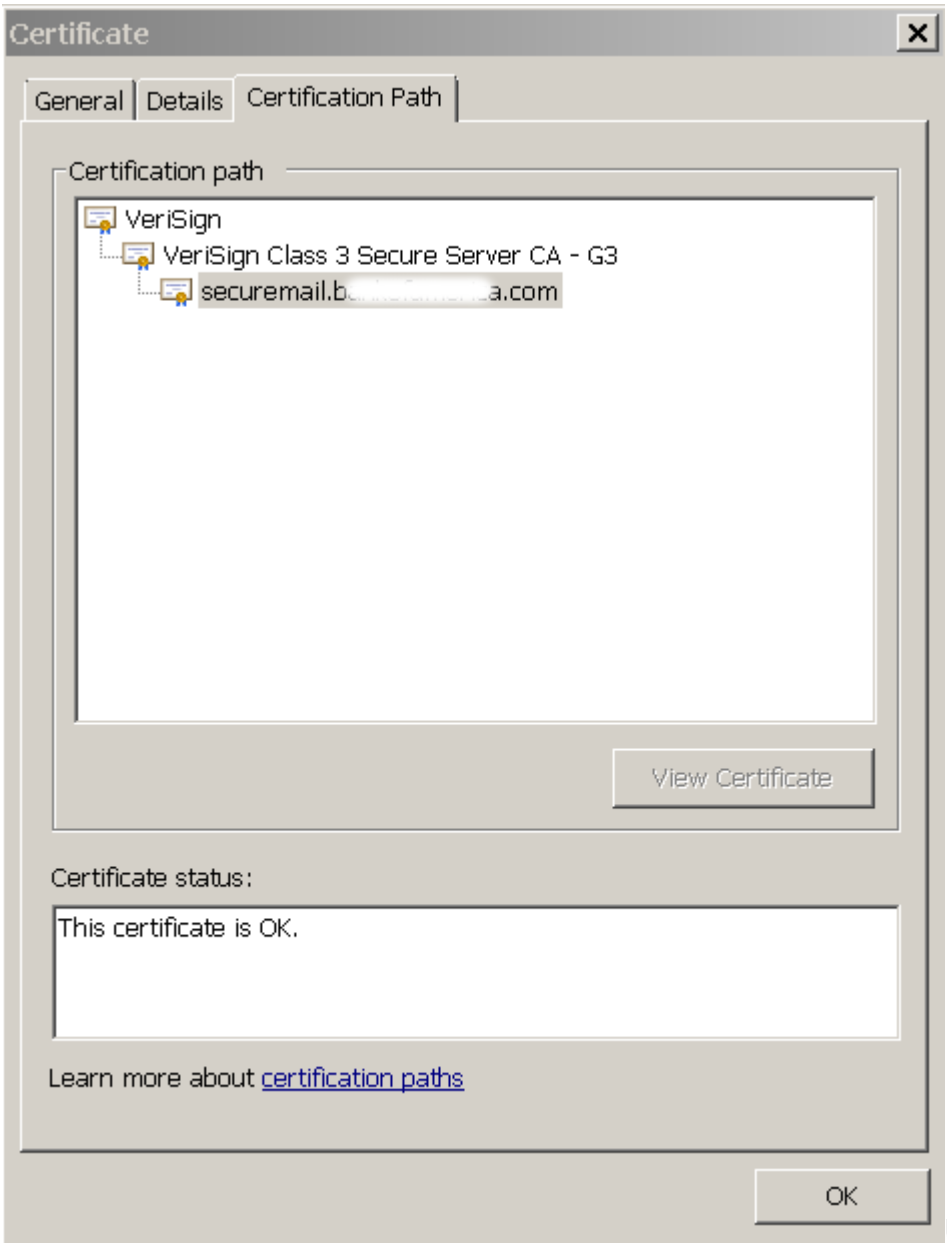


Seleccione el **base 64 codificó X.509(.CER)**.

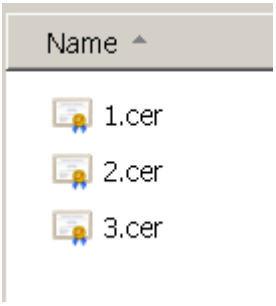


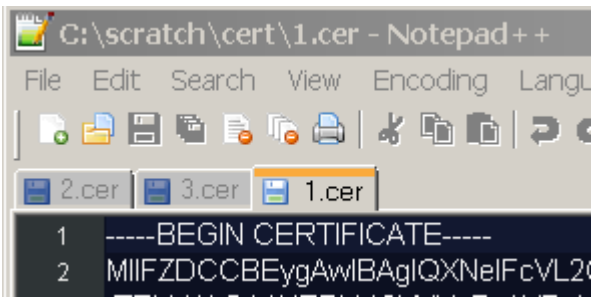
Relance para el nivel superior CA, y nómbrelo **2.CER**.

Relance para el certificado de servidor, y **nómbrelo 3.CER**.



Utilice un editor de textos (**no** libreta, pero los trabajos notepad++ bien) para abrir los tres archivos **X.CER** y combinarlos en la orden (1 en el top, y 3 en la parte inferior):





Nota: No debe haber líneas vacías entre los Certificados y ninguna línea vacía en la parte inferior.

Salve como **<servername>.CER**.

Cargue el archivo **<servername>.CER al** IEA en **/home/admin/ <servername.cer>** con el FTP o 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. Utilice el IEA GUI para importar el certificado [las claves y los Certificados | SSL puesto].

   Nota: Keystore = **[Install Directory] /conf/enterprisenamestore.keystore o el** nombre actual de su archivo del keystore.

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

   Confianza CA Certs del control.

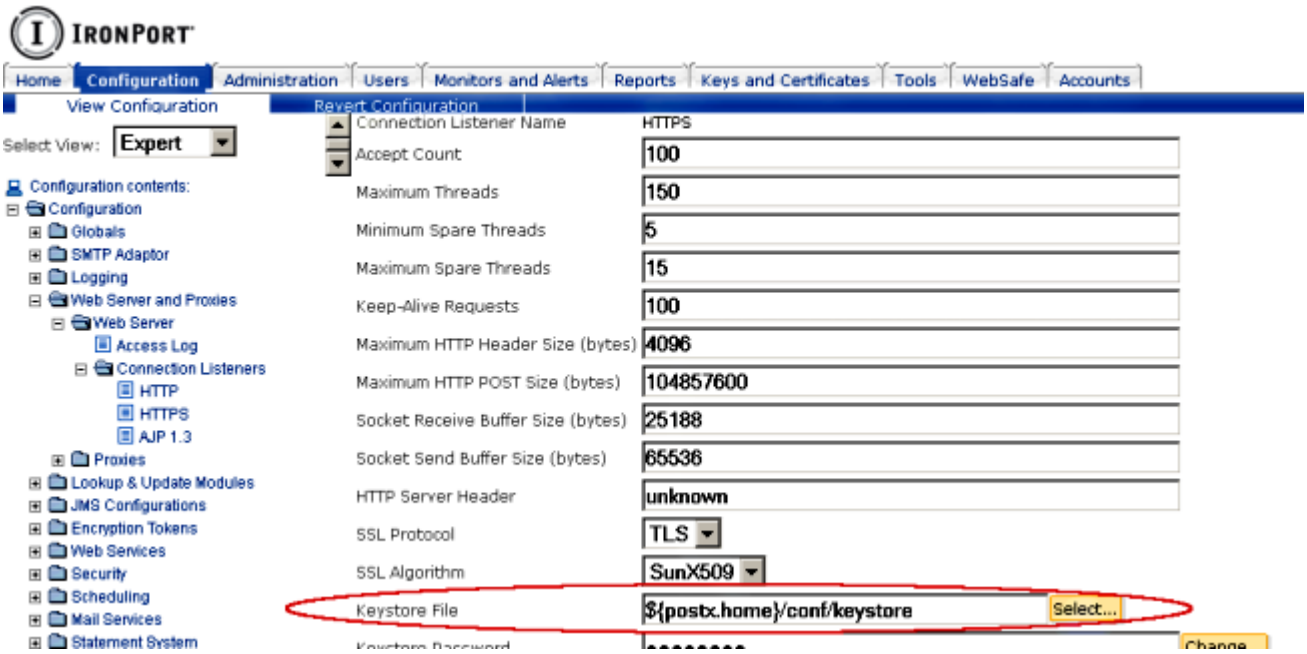
   Tecleo **Import Certificate (Importar certificado)**

3. (Opcional -- Si un nuevo keystore se debe crear). Del IEA GUI, diga el IEA utilizar el nuevo keystore:

   Elija la configuración | Servidor Web y proxys | Servidor Web | Módulos de escucha de la conexión | HTTPS

   Teclee adentro la trayectoria al nuevo archivo del keystore:

Ejemplo: ${postx.home}/conf/2013_5_13.keystore



4. Despliegue los cambios y recomience el adaptador S TP.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.