



## Como generar CSR en Zimbra e instalar SSL

### Creación de CSR Zimbra

Iniciar sesión como root

Ajuste el siguiente comando para que coincida con su información:

**`/opt/zimbra/bin/zmcertmgr createcsr comm -new"/C = UY/ST = Montevideo/L = Montevideo/O=Abitab S.A/OU=TI/CN = sudominio.com"`** donde:

C = Código de país (e.j., UY)

ST = Estado/Provincia

L = Ciudad

O = Nombre de organización (COMO FIGURA EN DGI)

OU = Departamento (e.j., TI)

CN = Common Name (mail.dominio.com, \*.dominio.com)

Si desea incluir más de un nombre en el CSR, puede agregar `-subjectAltNames` al final del comando. Ejemplo:

**`/opt /zimbra /bin/zmcertmgr createcsr comm -new "/C = UY/ST = Montevideo/L = Montevideo/O=Abitab S.A/OU=TI/CN = sudominio.com" -subjectAltNames "www.dominio.com, dominio.dominio.com"`**

La ejecución de este comando generará la CSR en la siguiente ubicación:

**`/opt/zimbra/ssl/zimbra/commercial/commercial.csr`**

Utilizará la CSR para realizar el pedido del certificado (seleccione "Other" como el software del servidor al realizar su pedido).

### Instalación de SSL Zimbra

Una vez que reciba el correo que contiene los archivos del certificado, descargue todos los PEM mediante el botón [**Save plain**].

[Get binary](#) [Get plain](#)

**Certificate chain**

Subject	Abitab SSL Domain Validated
Issuer DN	Certum Global Services CA SHA2
Serial number	101d422255e1fe41886660c480177611
Valid from	August 22, 2018 9:09:52 AM
Expire date	May 2, 2027 9:09:52 AM

[Save binary](#) [Save plain](#)

Subject	Certum Global Services CA SHA2
Issuer DN	Certum Trusted Network CA
Serial number	d04b8fe5dd5bd221e7c74cf6468b3146
Valid from	September 11, 2014 2:00:00 PM
Expire date	June 9, 2027 12:46:39 PM

[Save binary](#) [Save plain](#)

Subject	Certum Trusted Network CA
Issuer DN	Certum CA
Serial number	939285400165715f947f288f6c99b28
Valid from	October 22, 2008 2:07:37 PM
Expire date	June 10, 2027 12:46:39 PM

[Save binary](#) [Save plain](#)

Subject	Certum CA
Issuer DN	Certum CA
Serial number	010020
Valid from	June 11, 2002 12:46:39 PM
Expire date	June 11, 2027 12:46:39 PM

[Save binary](#) [Save plain](#)

Ahora mediante un programa de edición de texto (Bloc de notas, Word) abra cada uno de los archivos y copie todo su contenido en un nuevo documento en blanco, respetando el orden de la cadena (**First Intermediate, Second Intermediate, Third Intermediate y Root**).

Asegúrese de incluir etiquetas **BEGIN CERTIFICATE y END CERTIFICATE** al copiar, el resultado final se debería ver así:

```
-----BEGIN CERTIFICATE-----
```

(First Intermediate certificate: Abitab SSL Domain Validated)

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

(Second Intermediate certificate: Certum Organization Validation CA SHA2)

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

(Third Intermediate certificate: Certum Trusted Network CA)

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

(Root certificate: Certum CA)

```
-----END CERTIFICATE-----
```

Guarde el archivo combinado como `commercial_ca.crt` en el siguiente directorio:

**`/opt/zimbra/ssl/zimbra/commercial/`**

Luego lleve su certificado de servidor (`su_dominio.cer`) y cópielo en el archivo guardado `commercial.crt` en el siguiente directorio:

**`/opt/zimbra/ssl/zimbra/commercial/`**

Ejecute el siguiente comando para validar la cadena de certificados: **`/opt/zimbra/openssl/bin/openssl verify -CAfile commercial_ca.crt su_dominio.cer`**

Una vez que se valida la cadena de certificados, puede ejecutar el siguiente comando para habilitar el nuevo certificado para su uso: **`/opt/zimbra/bin/zmcertmgr deploycert comm commercial.crt commercial_ca.crt`**.