

Configuración correcta de Let's Encrypt en Webmin con

Problema común tras instalación de Webmin

Webmin puede venir con certificados SSL preconfigurados (autofirmados) que interfieren con la configuración correcta de Let's Encrypt, causando errores como:

```
Unable to change the --key-type of this certificate because --reuse-key is set
```

Diagnóstico inicial

1. Verificar certificados existentes

```
certbot certificates
```

2. Identificar conflictos en Webmin

- Ir a **Webmin Configuration → SSL Encryption**
- Verificar si hay certificados autofirmados que no se pueden eliminar desde la interfaz

Solución paso a paso

Paso 1: Limpieza desde línea de comandos

Si existe un certificado conflictivo, eliminarlo completamente:

```
# Listar certificados actuales
certbot certificates
```

```
# Eliminar certificado problemático (reemplazar con tu dominio)
certbot delete --cert-name tu-dominio.com
```

Importante: Certbot preguntará confirmación. Responder ☐ para continuar.

Paso 2: Configuración en Webmin

1. Ir a **Webmin Configuration → SSL Encryption**
2. Seleccionar **"Let's Encrypt certificate"**
3. **Método de validación crítico:** Seleccionar **"Certbot built-in webserver"**
 - Esta opción es más robusta
 - Evita conflictos de directorio
 - Maneja automáticamente puertos 80/443
4. Introducir tu dominio
5. Hacer click en **"Request Certificate"**

Paso 3: Verificación

```
# Verificar que el certificado se creó correctamente
certbot certificates

# Verificar que Webmin está usando el certificado correcto
systemctl status webmin
```

¿Por qué "Certbot built-in webserver"?

Ventajas sobre "Other webserver document directory":

- **Sin conflictos de directorio:** No depende de configuraciones de Apache/Nginx
- **Control total:** Certbot maneja temporalmente los puertos necesarios
- **Más limpio:** Evita interferencias con otros servicios web
- **Mayor éxito:** Funciona incluso cuando hay configuraciones SSL complejas

Desventajas:

- **Downtime mínimo:** Detiene temporalmente el servicio web (segundos)

- **Puertos requeridos:** Necesita acceso libre a puertos 80 y 443

Configuración de renovación automática

Months between automatic renewal 2

Renovación manual

```
# Forzar renovación (si faltan menos de 30 días)
certbot renew --force-renewal

# Renovación específica de un dominio
certbot certonly --standalone -d tu-dominio.com --force-renewal
```

Mejores prácticas

Antes de solicitar certificado:

1. **DNS configurado:** Asegurar que el dominio apunta al servidor
2. **Firewall:** Puertos 80 y 443 abiertos
3. **Limpieza:** Eliminar certificados conflictivos

Configuración recomendada:

- **Método:** Certbot built-in webserver
- **Renovación:** Automática (certbot.timer)
- **Monitoreo:** Verificar expiración mensualmente

Comandos de verificación regular:

```
# Estado general
certbot certificates

# Próximas renovaciones
certbot renew --dry-run
```

```
# Logs de renovación
```

```
tail -f /var/log/letsencrypt/letsencrypt.log
```

Última actualización: Septiembre 2025

Testeado en: Webmin 2.x, Ubuntu/Debian

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Revision #1

Created 2025-09-03 17:34:15 UTC by Abkrim

Updated 2025-09-03 17:39:45 UTC by Abkrim