

Generación de Certificado para IIS

Se requiere generar un certificado con una algoritmos de SHA256 y una llave de 512 bits, para evitar que el IIS se vea afectado en la entrega de los archivos debido a la validación del certificado, en escenarios de SSL.

Prerequisitos

- **OpenSSL**, este viene incluido en OSX o se puede descargar para Microsoft.

Datos del Certificado

- Password para PFX: **w0rk1ng**
- Longitud de la Llave: **512**
- Algoritmo: **RSA**

- Country Name: **MX**
- State or Province Name: **CDMX**
- Locality Name: **CDMX**
- Organization Name: **ISAT Telecomunicaciones**
- Organizational Unit Name: **Desarrollo**
- Common Name: **ISAT**
- Email Address: **isat@isat.com.mx**

Generar Llave (isat_key.pem)

```
$ openssl genrsa -out isat_key.pem
```

```
$ openssl genrsa -out isat_key.pem
Generating RSA private key, 512 bit long modulus
.....++++++
...++++++
e is 65537 (0x10001)
```

Crear el SelfSigned Certified

```
$ openssl req -new -x509 -days 5000 -key isat_key.pem -out isat_cert.pem
```

Ejemplo:

```
$ openssl req -new -x509 -days 5000 -key isat_key.pem -out isat_cert.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:CDMX
Locality Name (eg, city) []:CDMX
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ISAT Telecomunicacion
Organizational Unit Name (eg, section) []:Desarrollo
Common Name (e.g. server FQDN or YOUR name) []:ISAT
Email Address []:isat@isat.com.mx
```

Generar el archivo pfx

```
openssl pkcs12 -export -out certificate.pfx -inkey isat_key.pem -in isat_cert.pe
```

Importante: Se requiere utilizar el Password para PFX, especificado al inicio del documeto.

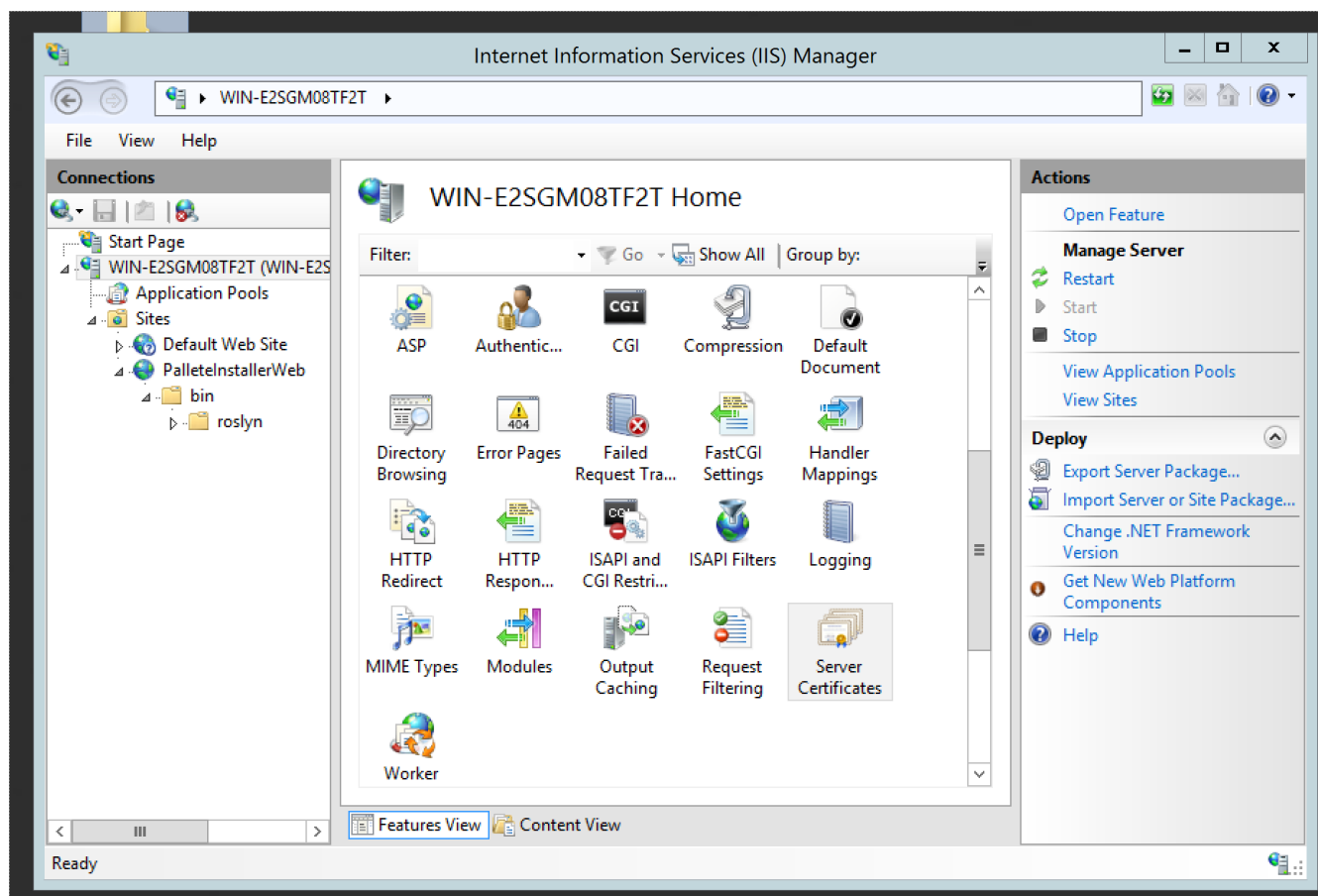
Ejemplo:

```
$ openssl pkcs12 -export -out certificate.pfx -inkey isat_key.pem -in isat_cert.
Enter Export Password:
Verifying - Enter Export Password:

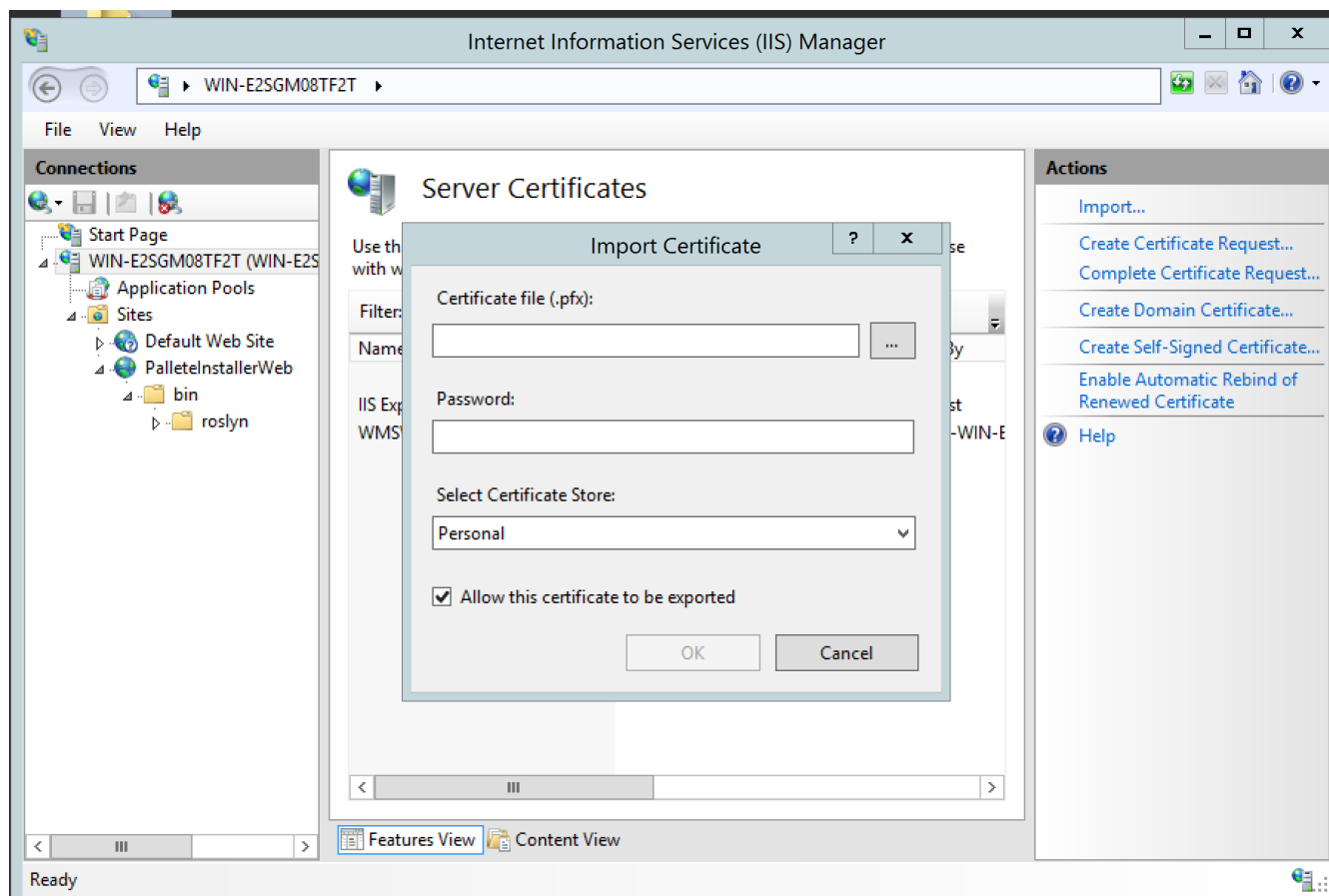
$ ls
certificate.pfx    isat.pem    isat_cert.pem    isat_key.pem
```

Importarlo en IIS

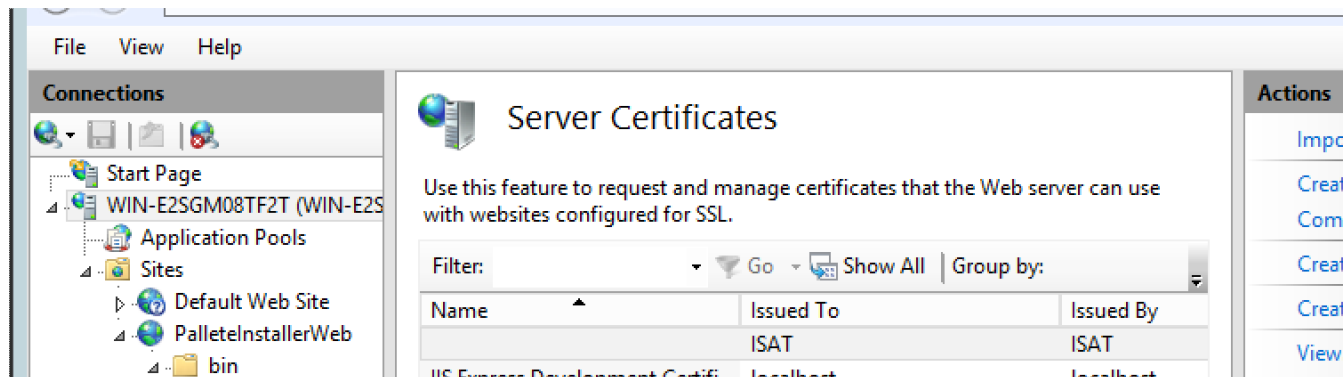
Abrir IIS y entrar a la sección de Certificados:



Utilizar la opción **Import** de la sección **Actions**

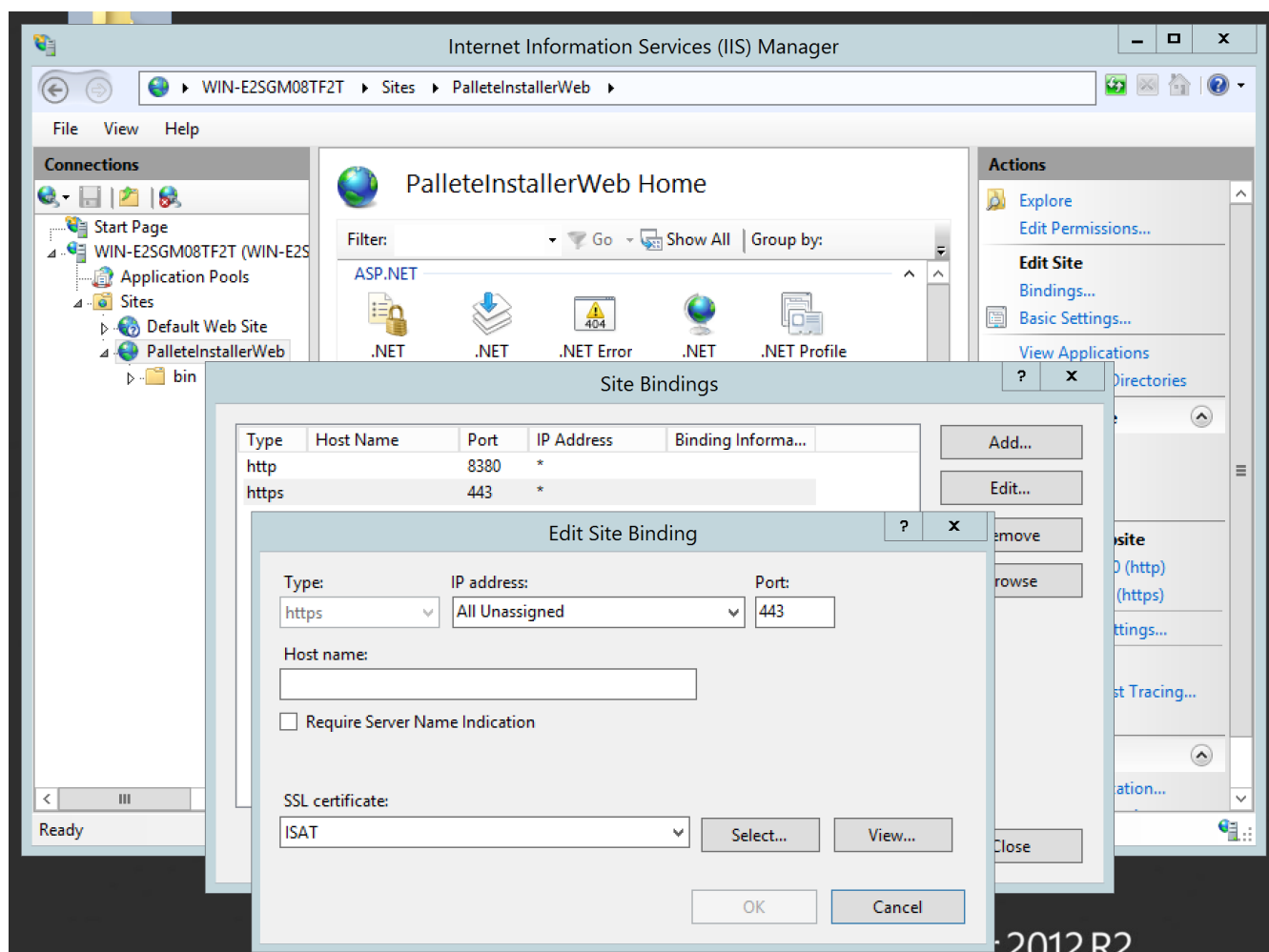


Seleccione el archivo **.pfx** e introduzca el Password para PFX, especificado al inicio del documento, y seleccione el grupo **Personal**.



Asigne el certificado al sitio web deseado, utilizando la opción de **Bindings**, propia del sitio web a modificar.

Una vez abierta la ventana de **Edit Site Bindings** seleccione el certificado de la lista de seleccion **SSL Certificate**:



La asignación del certificado ha terminado.

