SSL□□□

- openssl□□□□□
- IIS Crypto□□

openssl□□□□□

□□□□

□□Linux□openssl□□□□cer□□crt

```
openssl x509 -in server.cer -out server2.crt -inform DER
```

crt□□cer(DER□□)

```
openssl x509 -in server.crt -out server.cer -outform DER
```

□crt□key□□□pfx□ca

```
openssl pkcs12 -export -in server.crt -inkey server.key -out server.pfx -certfile ca.crt -password pass:123456
```

pfx□□□pem

```
openssl pkcs12 -in server.pfx -out server.pem -nodes -password pass:123456
```

pem□□crt

```
openssl x509 in server.pem -out server.crt
```

pem□□key

```
openssl rsa -in server.pem -out server.key
```

pfx□□crt□ca

```
openssl pkcs12 -in server.pfx -nokeys -out server2.crt -nodes -password pass:123456
```

pfx□□key

```
openssl pkcs12 -in server.pfx -nocerts -out server2.key -nodes -password pass:123456
```

crt □□ p7b

```
openssl crl2pkcs7 -nocrl -certfile server.crt -out server.p7b -certfile ca.crt
```

pfx□□jks

```
keytool -importkeystore -srckeystore server.pfx -destkeystore server.jks -srcstoretype PKCS12 -deststoretype jks -s
```

jks□pfx

```
keytool -importkeystore -srckeystore server.jks -destkeystore server2.pfx -srcstoretype jks -deststoretype PKCS12
```

□□3□□□□□□□□hash□□□□□□□

```
openssl pkey -in server.key -pubout -outform pem | sha256sum
openssl x509 -in server.crt -pubkey -noout -outform pem | sha256sum
openssl req -in server.csr -pubkey -noout -outform pem | sha256sum
```

□□crt

```
openssl x509 -in server.crt -text -noout
```

□□□□

```
openssl verify server.crt
```

□□key

```
openssl rsa -in server.key -text -noout
```

□□key

```
openssl rsa -noout -text -check -in server.key
```

□□ server.pfx

```
openssl pkcs12 -info -in server.pfx
```

□□ server.jks

```
keytool -v -list -storetype jks -keystore server.jks -storepass 123456
```

□□:cer□□IIS□□□crt□□apache□nginx□□□

□□□□

cert□cr certificate□□

windows□□□□:cer pfx p7b□cer□der□□(□□□)□base64□□(plain text)

apache□nginx□□pem□crt

java□□jks□pfx

pem□□.crt□.key

□□□□□BEGIN CERTIFICATE□□□□END CERTIFICATE

□□□□□BEGIN RSA PRIVATE KEY□□□□END RSA PRIVATE KEY

□□□□:

https://ssorc.tw/7142/openssl-command-line-convert-file-for-pem-der-p7b-pfx-cer/

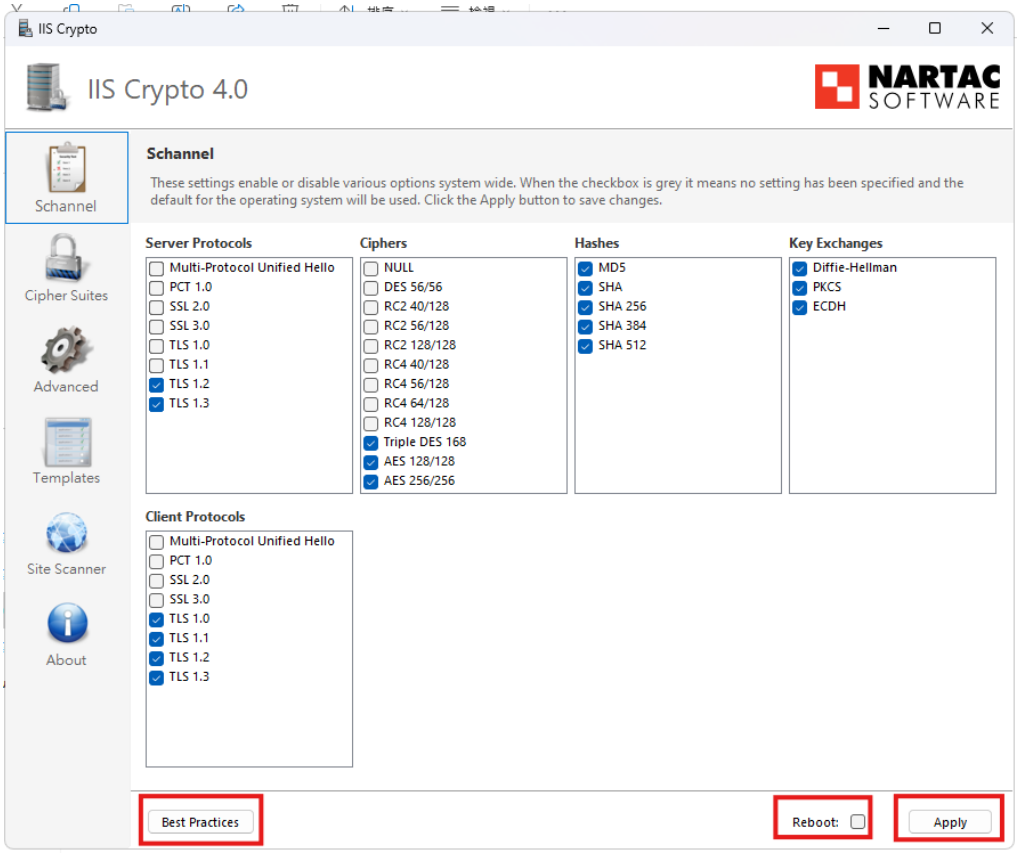
IIS Crypto□□

□□□□□□□□□□□□SSL□□□□□□□□□□□□□□□□□□□□□□server 2012□Win8□□□Windows□□□

□□□□:https://www.nartac.com/Products/IISCrypto/Download

□□□□□□□□□□□□□□□□□Windows□□□□□□□□

□□□Best Practices□□□□□□□□□□□□□□□□□□□□



□□:

1.□□□□□□□□□□OS□Client□□□(Server Protocols)□□□□□□□□(Client Protocols)□□□□□□□□□

2.□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]
```

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]

"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]

"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]

"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]

"DisabledByDefault"=dword:00000000