MARQUIS NEXT

SSL Certificates

Table of Contents

Introduction

You should approach online security in the same way that you would approach physical security for your business. Not only does it make you feel safer, but it also protects people who visit your place of business, or website. But most importantly, it secures your data.

This guide will de-mystify the technology involved used in Marquis Next and give you the information you need create a self-signed certificate or acquire a signed certificate.

What Is an SSL Certificate?

An SSL certificate is a digital computer file (or small piece of code) that has two specific functions:

1. **Authentication and Verification:** The SSL certificate has information about the authenticity of certain details regarding the identity of a person, business or website, which it will display to visitors on your website when they click on the browser's padlock symbol or trust mark. The vetting criteria used by Certificate Authorities to determine if an SSL certificate should be issued is most stringent with an Extended Validation (EV) SSL certificate; making it the most trusted SSL certificate available.
2. **Data Encryption:** The SSL certificate also enables encryption, which means that the sensitive information exchanged via the website cannot be intercepted and read by anyone other than the intended recipient.

In the same way that an identity document or passport may only be issued by the country's government officials, an SSL certificate is most reliable when issued by a trusted Certificate Authority (CA). The CA must follow very strict rules and policies about who may or may not receive an SSL certificate. When you have a valid SSL certificate from a trusted CA, there is a higher degree of trust by your customers, clients or partners.

How Does SSL Encryption Work?

In the same way that you lock and unlock doors using a key, encryption makes use of keys to lock and unlock your information. Unless you have the right key, you will not be able to "open" the information

Each SSL session consists of two keys

- The public key is used to encrypt (scramble) the information.
- The private key is used to decrypt (un-scramble) the information and restore it to its original format so that it can be read.

The SSL 'Greeting'

Every SSL certificate that is issued for a CA-verified entity is issued for a specific server and website domain (website address). When a person uses their browser to navigate to the address of a website with an SSL certificate, an SSL handshake (greeting) occurs between the browser and server. Information is requested from the server – which is then made visible to the person in their browser window. You will notice changes to indicate that a secure session has been initiated – for example, a trust mark will appear in the browser. If you click on the trust mark, you will see additional information such as the validity period of the SSL certificate, the domain secured, the type of SSL certificate, and the issuing CA. All of this means that a secure link is established for that session, with a unique session key, and secure communications can begin.

Certificate Singing Request (CSR)

A certificate signing request (CSR) is one of the first steps towards getting your own SSL Certificate. Generated on the same server you plan to install the certificate on, the CSR contains information (e.g. common name, organization, country) the Certificate Authority (CA) will use to create your certificate. It also contains the public key that will be included in your certificate and is signed with the corresponding private key. We'll go into more details on the roles of these keys below.

What Information Is Included in a CSR?

The CA will use the data from the CSR to build your SSL Certificate. The key pieces of information include the following.

Information about your business and the website you're trying to equip with SSL, including:

Common Name (CN) (e.g. *.example.com www.example.com mail.example.com)	The fully qualified domain name (FQDN) of your server.
Organization (O)	The legal name of your organization. Do not abbreviate and include any suffixes, such as Inc., Corp., or LLC. For EV and OV SSL Certificates, this information is verified by the CA and included in the certificate.
Organizational Unit (OU)	The division of your organization handling the certificate.
City/Locality (L)	The city where your organization is located. This shouldn't be abbreviated.
State/County/Region (S)	The state/region where your organization is located. This shouldn't be abbreviated.
Country (C)	The two-letter code for the country where your organization is located.
Email Address	An email address used to contact your organization.

The public key that will be included in the certificate. SSL uses public-key, or asymmetric, cryptography to encrypt transmitted data during an SSL session. The public key is used to encrypt and the corresponding private key is used to decrypt.

Information about the key type and length. The most common key size is RSA 2048, but some CAs support larger key sizes (e.g. RSA 4096+) or ECC keys.

What Does a CSR Look Like?

The CSR itself is usually created in a Base-64 based PEM format. You can open the CSR file using a simple text editor and it will look like the sample below. You must include the header and footer (-----BEGIN NEW CERTIFICATE REQUEST-----) when pasting the CSR.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDVDCCAr0CAQAweTEeMBwGA1UEAxMVd3d3Lmpvc2VwaGNoYXBtYW4uY29tMQ8w
DQYDVQQLEwZEZXNpZ24xFjAUBgNVBAoTDUpvc2VwaENoYXBtYW4xEjAQBgNVBAcT
CU1haWRzdG9uZTENMAsGA1UECBMES2VudDELMAkGA1UEBhMCR0IwgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMIGJAoGBAOEFDpnOKRabQhDa5asDxYPnG0c/neW18e8apjOk
1yuGRk+3GD7YQvuhBVS1x6wkw1D2RnmnZgN1nNUK0cRK7sIvOyCh1+jgD7u46mLk
81j+b4YSEmYZGPLIuclyocPDm0hXayjCUqWt7z6LMIKpLym8gayEZzz9Gn97PsbP
kVFBAgMBAAGgggGZMBoGCisGAQQBgjcNAgMxDBYKNS4xLjI2MDAuMjB7BgorBgEE
AYI3AgEOMW0wazAOBgNVHQ8BAf8EBAMCBPAwRAYJKoZIhvcNAQkPBDcwNTAOBggq
hkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCAMAcGBSsOAwIHMAoGCCqGSIb3DQMH
MBMGA1UdJQQMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQICMYHuMIHrAgEBHloA
TQBpAGMAcgBvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMA
cgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABlAHIDgYkAk0kf
HSkr4jsEVya3mgUoyaYMO456ECNZr4Cb+WhPgexfjOO5qwOG1oDOTaKycrkc5pG+
IPBQnq+4cotT8hWJQwpc+qGb8xUETpxCokhrhN5079vFXq/5dsHkmtOTwkSqSnz9
yruVoxYeDQ8jI3KG3HTgxwFto8oZnm+E+Y4oshUAAAAAAAAAADANBgkqhkiG9w0B
AQUFAAOBgQAuAxetLzgfjBdWpjpixeVYZXuPZ+6jvZNL/9hOw7Fk5pVVXWdr8csJ
6JUW8QdH9KB6ZlM4yg8Df+vat1/DG6GuD2hiIR7fQ0NtPFBQmbrSm+TTBo95lwP+
ZSZTusPFTLKaqValdnS9Uw+6Vq7/I4ouDA8QBIuaTFtPOp+8wEGBHQ==
-----END NEW CERTIFICATE REQUEST-----
```

Generating an IIS SSL Certificate Signing Request (CSR) using Microsoft IIS Manager

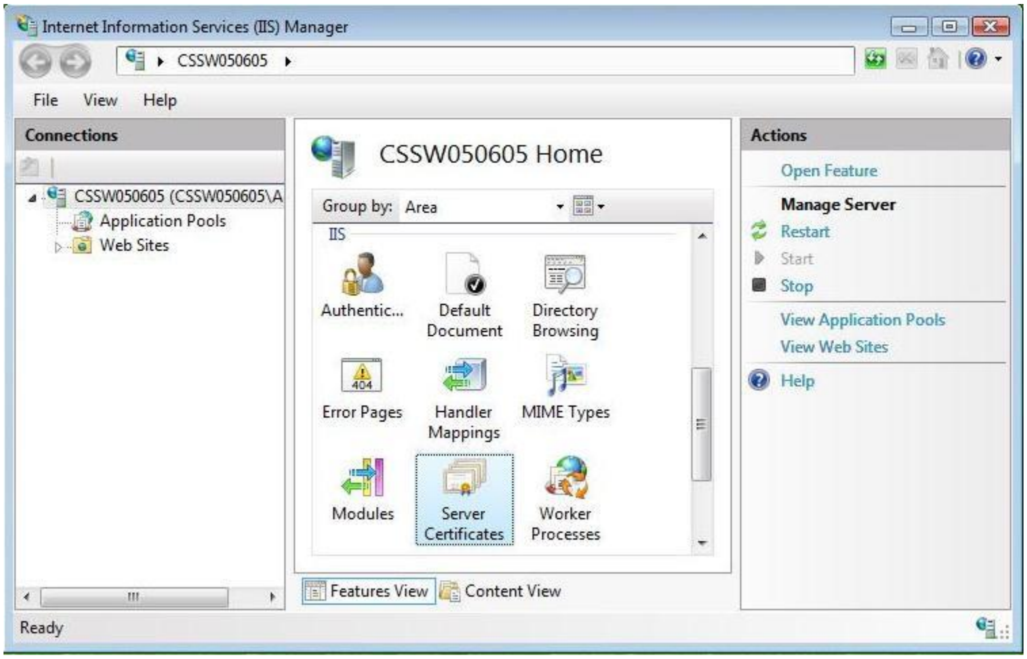
Click Start.

Select Administrative Tools.

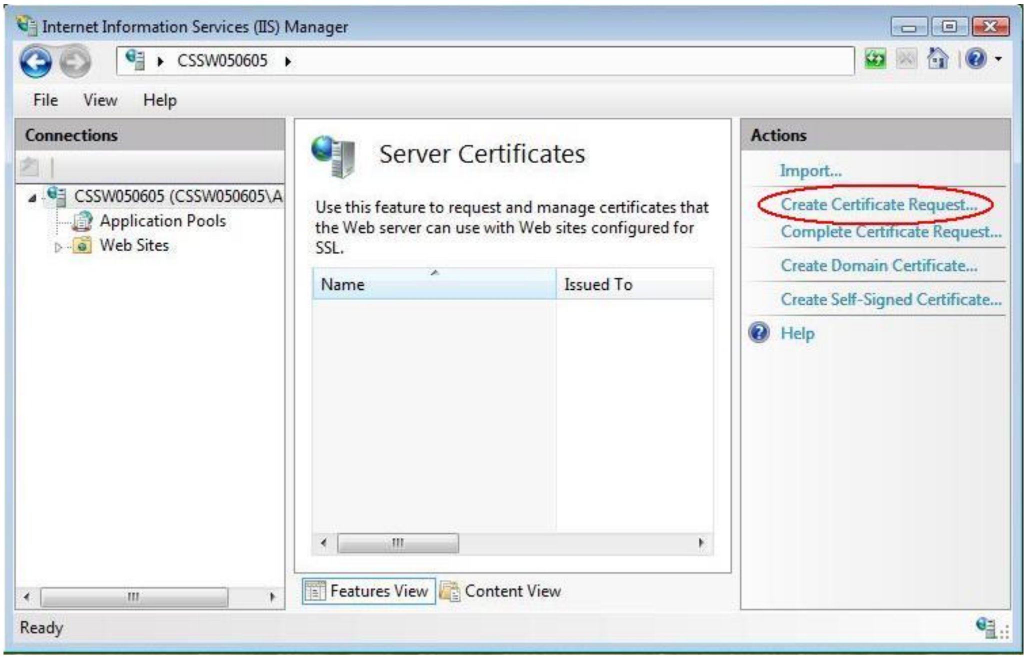
Start Internet Services Manager.

Click Server Name.

From the center menu, double-click the "Server Certificates" button in the "Security" section.

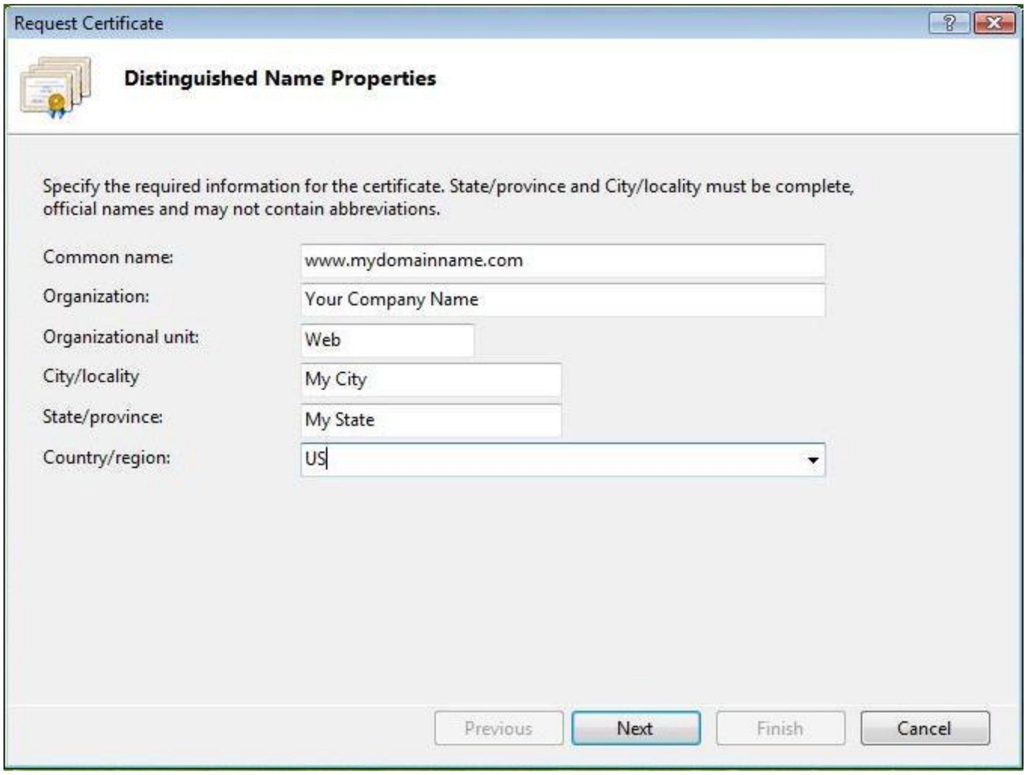


Select "Actions" menu (on the right), click on "**Create Certificate Request.**"



Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

This will open the Request Certificate wizard.



Specify the required information for the certificate. State/province and City/locality must be complete, official names and may not contain abbreviations.

Common name: www.mydomainname.com
Organization: Your Company Name
Organizational unit: Web
City/locality: My City
State/province: My State
Country/region: US

In the "Distinguished Name Properties" window, enter the information as follows:

The Common Name field should be the Fully Qualified Domain Name (FQDN) or the web address for which you plan to use your IIS SSL Certificate. You will need to ensure that the common name submitted in the CSR is the correct domain name / FQDN that you intend to use the certificate for. For Wildcard

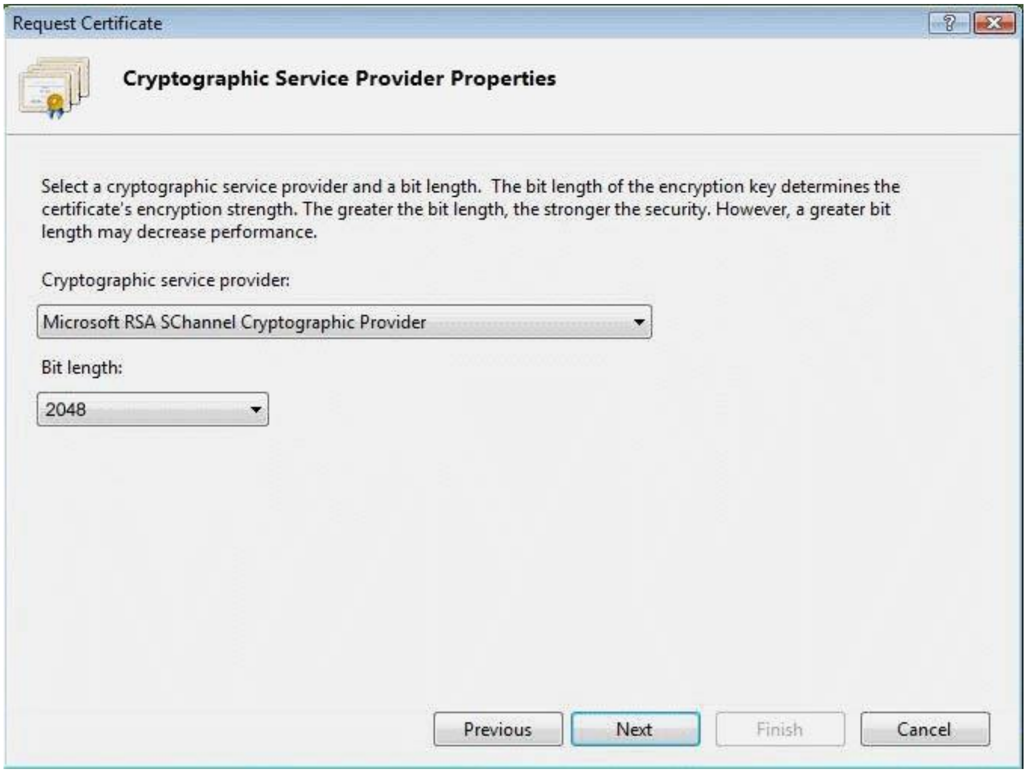
SSL certificates the common name should contain at least one asterisks (*) e.g. *.comodo.com,*.instantssl.com, etc

Enter Organization and Organization Unit, these are your company name and department respectively.

Enter your City/locality, State/province and Country/region.

Click Next.

In the "Cryptographic Service Provider Properties" window, leave both settings at their defaults (Microsoft RSA SChannel and 2048) and then Click **Next**.



Request Certificate

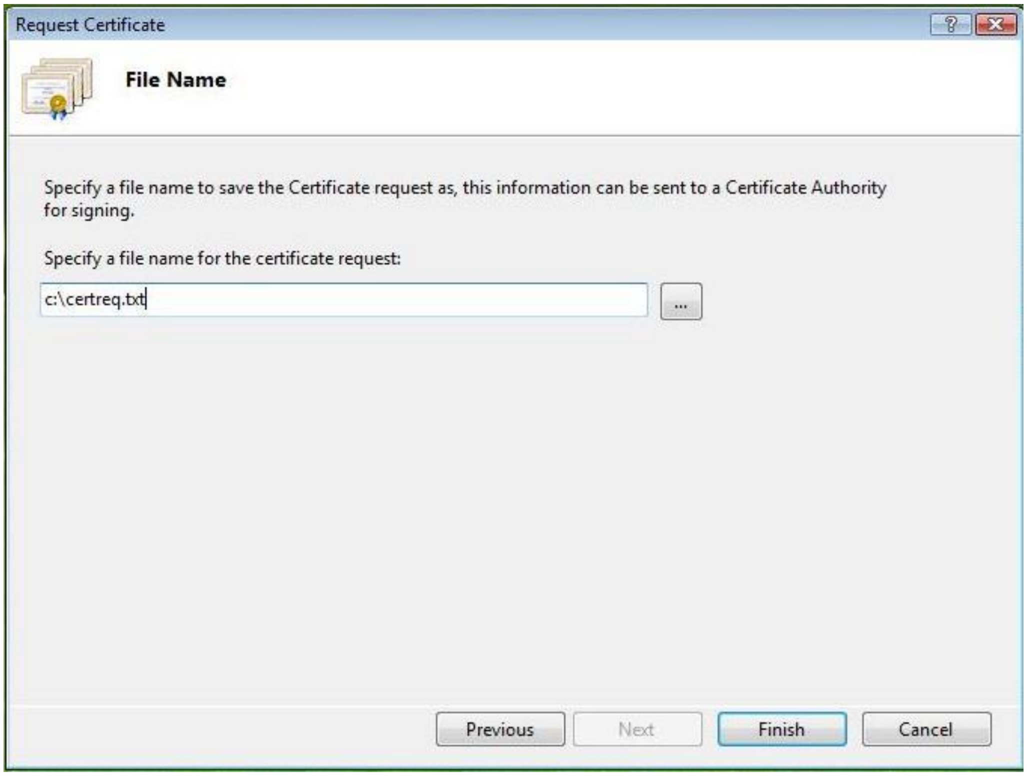
Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 2048

Enter a filename and location to save your CSR. You will need this CSR to enroll for your IIS SSL Certificate.



Request Certificate

File Name

Specify a file name to save the Certificate request as, this information can be sent to a Certificate Authority for signing.

Specify a file name for the certificate request:

c:\certreq.txt

Click Finish.

Your new CSR is now contained within the file **c:\certreq.txt**

When you make your application, make sure you include the CSR in its entirety into the appropriate section of the enrollment form - including
-----BEGIN CERTIFICATE REQUEST-----to-----END CERTIFICATE REQUEST-----

Click Next

Confirm your details in the enrollment form and Finish.

Install an SSL Certificate in Microsoft IIS

Launch the Server Manager.

From Tools, select Internet Information Services (IIS) Manager.

In the Connections panel on the left, click the server name for which you want to generate the CSR.

In the middle panel, scroll to the bottom, and then double-click Server Certificates.

In the Actions panel on the right, click Complete Certificate Request....

Do the following to install the certificate, and then click OK:

File name containing the certificate authority's response — Click ..., locate the .crt file on your computer, and then click Open.

Friendly name — Enter a unique name to identify the SSL certificate. For wildcard SSL certificates, make sure your friendly name matches your common name (such as _*.coolexample.com_).

Select a certificate store for the new certificate — Select Personal.

In the Connections panel on the left, select the name of the server on which you installed the certificate.

Click + to expand Sites, and then select the site you want to secure with the SSL certificate. (This process is called binding.)

In the Actions panel on the right, click Bindings....

Click Add....

Do the following to configure the settings, and then click OK:

Field	What to do...
Type	Select **https**.
IP address	Select **All Unassigned**, or select the IP address of the site.
Port	Type **443** (Marquis Next) or **19443** (Marquis Id)
SSL Certificate	Select the SSL certificate you just installed.

In the Actions panel on the right, click Restart to complete the installation process.