Server software page

Certificate Signing Request (CSR) Generation

Software

Apache (mod_SSL and OpenSSL)

To generate your CSR, you will need to log in to your server and use the OpenSSL software to generate a CSR and private key.

- Log in to your server, and enter the following command:
  ```
  OpenSSL req -nodes -newkey rsa:2048 -keyout myserver.key -out server.csr
  ```
- This will generate two files: a CSR called "server.csr" and a 2048-bit private key called ""myserver.key.""

You will be prompted to enter some information for your CSR:

- Country Name (2 letter code) [AU]: GB
- State or Province Name (full name) [some state]: Yorks
- Locality Name (e.g., city) []: York
- Organization Name (e.g., company) [Internet Widgits Pty Ltd]: MyCompany Ltd
- Organizational Unit Name (e.g., section) []: IT
- Common Name (e.g., YOUR name) []: mysubdomain.mydomain.com
- Email Address []:

Please enter the following "extra" attributes to be sent with your certificate request:

- A challenge password []:
- An optional company name []:
- The Common Name (CN) field, where you should enter the fully-qualified domain name of the website you require the certificate for.

Note, for wildcard certificates, the CN should be in the format: *.mydomain.com

- Your CSR is now generated.
- Open the "server.csr" file with a text editor and copy the contents, then paste them into the enrollment form when requested.

Notes:
The "myserver.key" file should be kept secure (e.g., readable only by root on Linux systems).

Removing the "-nodes" option from the OpenSSL command will request a password and encrypt the private key. This can increase security, but note that the password will be required each time Apache is restarted.

Extended validation (EV) certificates require a minimum of a 1024-bit keysize if valid before 2011, and 2048-bit if they are valid into 2011. We recommend 2048-bit keysize as a minimum for all certificates.

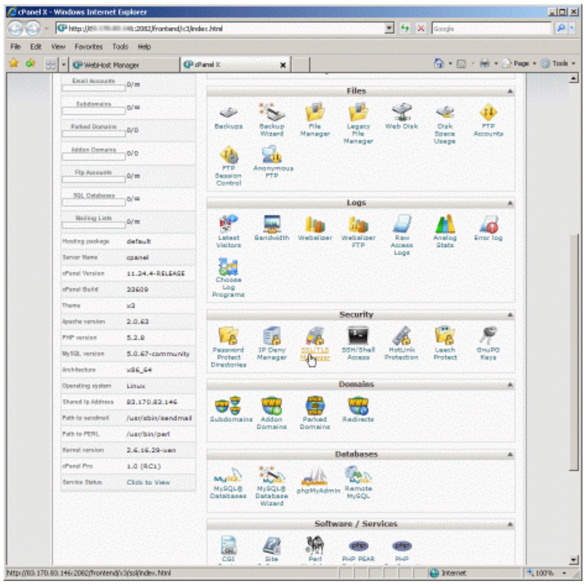
The two-letter CN field must be the ISO-3166 standard country code. Please note that "GB" is correct for Great Britain, not "UK." A complete list can be found here: http://www.iso.org/iso/country_codes.htm.

cPanel and WHM

To generate your CSR, you will need to login to your cPanel or WHM account. Both cPanel (the end-user control panel) and WHM (the administrator panel) have slightly different ways to request certificates and generate CSRs.

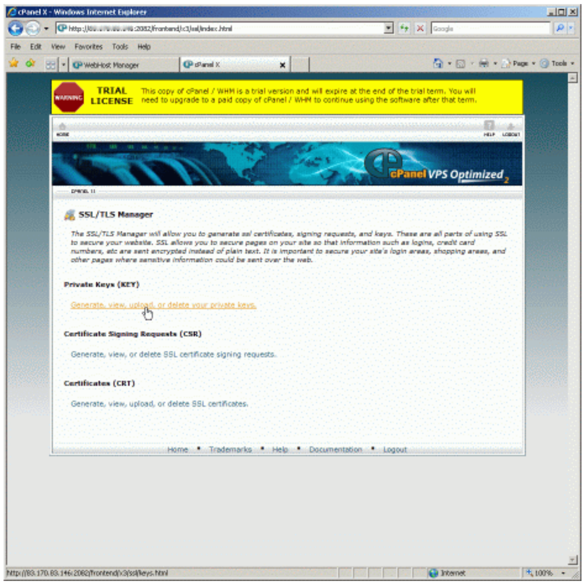
cPanel

- Login to cPanel.
- Under the "Security" menu, click the "SSL/TLS Manager."



Email Accounts	0/∞
Subdomains	0/∞
Parked Domains	0/0
Addon Domains	0/0
Ftp Accounts	0/∞
SQL Databases	0/∞
Mailing Lists	0/∞
Hosting package	default
Server Name	cpanel
cPanel Version	11.24.4-RELEASE
cPanel Build	33609
Theme	x3
Apache version	2.0.63
PHP version	5.2.9
MySQL version	5.0.67-community
Architecture	x86_64
Operating system	Linux
Shared Ip Address	83.170.83.146
Path to sendmail	/usr/sbin/sendmail
Path to PERL	/usr/bin/perl
Kernel version	2.6.16.29-xen
cPanel Pro	1.0 (RC1)
Service Status	Click to View

- The first step is to create a private key by clicking the "Generate..." link.


cPanel X - Windows Internet Explorer
File Edit View Favorites Tools Help
WebHost Manager
cPanel X
Page
Tools
HOME
HELP
LOGOUT
cPanel VPS Optimized 2
Home • Trademarks • Help • Documentation • Logout
http://83.170.83.146:2082/frontend/x3/ssl/keys.html
Internet
100%

TRIAL LICENSE This copy of cPanel / WHM is a trial version and will expire at the end of the trial term. You will need to upgrade to a paid copy of cPanel / WHM to continue using the software after that term.

SSL/TLS Manager

The SSL/TLS Manager will allow you to generate ssl certificates, signing requests, and keys. These are all parts of using SSL to secure your website. SSL allows you to secure pages on your site so that information such as logins, credit card numbers, etc are sent encrypted instead of plain text. It is important to secure your site's login areas, shopping areas, and other pages where sensitive information could be sent over the web.

Private Keys (KEY)

Generate, view, upload, or delete your private keys.

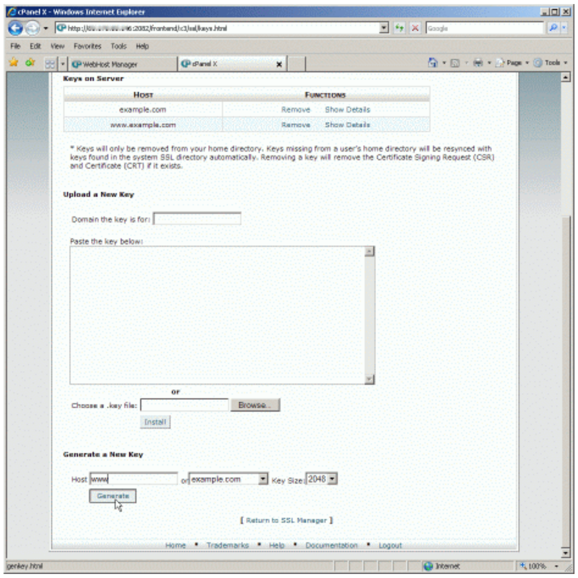
Certificate Signing Requests (CSR)

Generate, view, or delete SSL certificate signing requests.

Certificates (CRT)

Generate, view, upload, or delete SSL certificates.

- Scroll to the bottom section "Generate a New Key" and enter your information. We advise to use at least a 2048-bit key, which is the minimum for EV certificates. Click "Generate."


cPanel X - Windows Internet Explorer
File Edit View Favorites Tools Help
WebHost Manager
cPanel X
Page
Tools
Browse...
Install
Generate
[Return to SSL Manager]
Home • Trademarks • Help • Documentation • Logout
genkey.html
Internet
100%

Keys on Server

Host	Functions
example.com	Remove Show Details
www.example.com	Remove Show Details

* Keys will only be removed from your home directory. Keys missing from a user's home directory will be resynced with keys found in the system SSL directory automatically. Removing a key will remove the Certificate Signing Request (CSR) and Certificate (CRT) if it exists.

Upload a New Key

Domain the key is for:

Paste the key below:

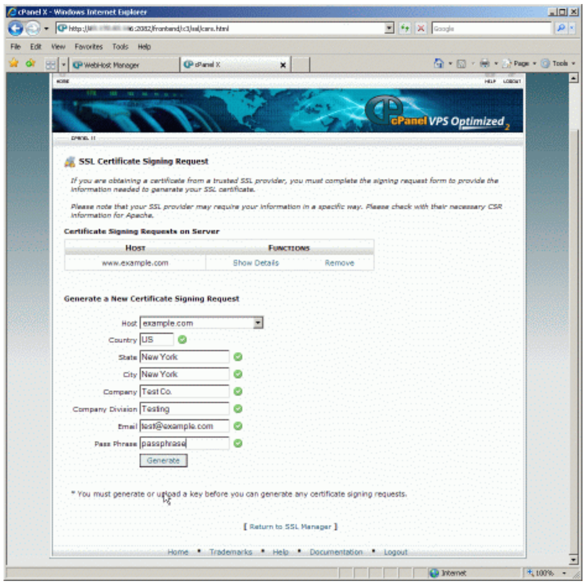
or

Choose a .key file:

Generate a New Key

Host www or example.com Key Size: 2048

- You will be shown the private key and its information. Click the link at the bottom to return to the "SSL/TLS Manager."
- In the "SSL/TLS Manager," click the "Generate..." link under "Certificate Signing Requests."
- Fill out your information in the "Generate a New Certificate Signing Request" form. Click "Generate."



SSL Certificate Signing Request

If you are obtaining a certificate from a trusted SSL provider, you must complete the signing request form to provide the information needed to generate your SSL certificate.

Please note that your SSL provider may require your information in a specific way. Please check with their necessary CSR information for Apache.

Certificate Signing Requests on Server

Host	Functions	
www.example.com	Show Details	Remove

Generate a New Certificate Signing Request

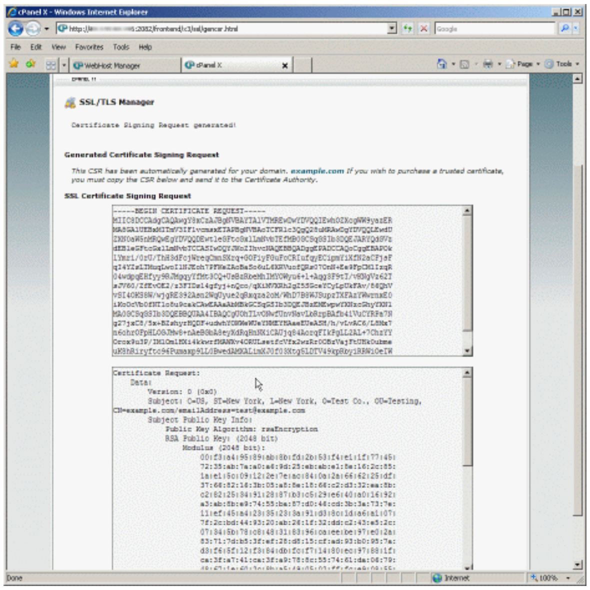
Host	example.com
Country	US
State	New York
City	New York
Company	Test Co.
Company Division	Testing
Email	test@example.com
Pass Phrase	passphrase

* You must generate or upload a key before you can generate any certificate signing requests.

[Return to SSL Manager]

cPanel X - Windows Internet Explorer
File Edit View Favorites Tools Help
WebHost Manager
cPanel X
Page
Tools
cPanel VPS Optimized 2
Generate
Home • Trademarks • Help • Documentation • Logout
Internet
100%

- You will be shown the CSR and its associated information. Copy the contents of the CSR and paste it into the enrollment form when requested.



SSL/TLS Manager

Certificate Signing Request generated!

Generated Certificate Signing Request

This CSR has been automatically generated for your domain. **example.com** *If you wish to purchase a trusted certificate, you must copy the CSR below and send it to the Certificate Authority.*

SSL Certificate Signing Request

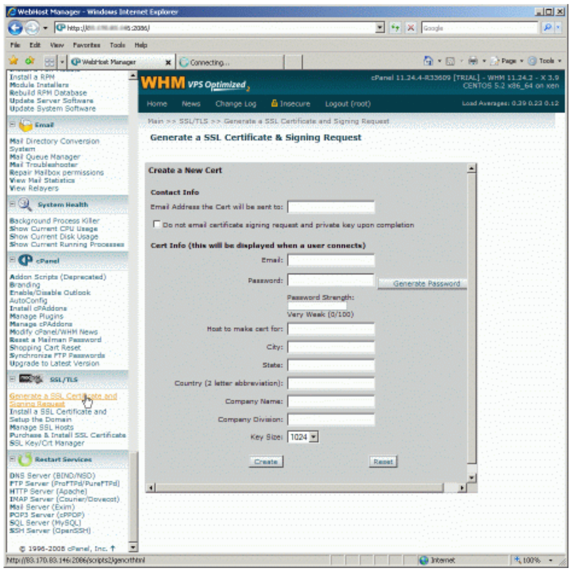
```
-----BEGIN CERTIFICATE REQUEST-----
MIIC8DCCAdgCAQAwgY8xCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhOZXcgWW9yazER
MA8GA1UEBxMITmV3IFlvcmsxETAPBgNVBAoTCFRlc3QgQ28uMRAwDgYDVQQLEwdU
ZXN0aW5nMRQwEgYDVQQDEwtleGFtcGxlLmNvbTEfMB0GCSqGSIb3DQEJARYQdGVz
dEBleGFtcGxlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPOk
lYmrl/0rU/ThH3dFcjWreqCmnSKrq+GOP1yF0uFoCRIufqyEC1pmY1XfN2aCFjsF
qI4YZslTMuqLwoIlNJEoh7PFWsZAcBa5c6uL6XRVuofQRs07OrN+Ee9FpCMlIzqR
04wdpqEHfyy9BJMgqyYfMt3CQ+UsBzRbeMhIMYOWyu6+l+Agg8F9tI/v80gVz62T
sJV60/ZfEvOE2/z3FIDsl4gfyj+nQco/qKiMVXRh2gZ55GcsYCyLpUkFAv/86QhV
vSI4OHS8W/wjgRE392Aen2WqUyue2qRmqza2oM/WhD7B8WJSupzIXFAzYWwrnxE0
iKoDcVb0fNTlc8u9cakCAwEAAaAbMBkGCSqGSIb3DQEJBzEMEwpwYXNzcGhyYXNl
MA0GCSqGSIb3DQEBBQUAA4IBAQCgUOhTLvONwfUnvNavLo8rpBAfb41VuCYRPa7N
g27jxC8/5x+BZshyrMQDF+udwhYORWeWJeYHMEYMAaeEUeA5M/h/vLvAC6/L8MxT
n6ohr0FpHLOGJMw8+nAeB0bA8eyXdRqHnNXiCAUjq84AorqFIkFgLL2Al+7ChzYY
Crox9u3P/IMlOmlMXi4kkwrfMANKv4ORULsetfcVfx2wzRr0CBsVajFtUNk0ubme
uH8hBiryftc96Pumaxp9LL/BwedAMXALimXJ0f03Xtg6LDTV49kpBby1RBW1OeIW
```

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=New York, L=New York, O=Test Co., OU=Testing,
CN=example.com/emailAddress=test@example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:f3:a4:95:89:ab:8b:fd:2b:53:f4:e1:1f:77:45:
                    72:35:ab:7a:a0:a6:9d:25:eb:ab:e1:8e:16:2c:85:
                    1a:e1:5c:09:12:2e:7e:ac:84:0a:2a:66:62:25:df:
                    37:66:82:16:3b:05:a8:8e:18:66:c2:d3:32:ea:8b:
                    c2:82:25:34:91:28:87:b3:c5:29:e6:40:a0:16:92:
                    a3:ab:5b:e9:74:55:ba:87:d0:46:cd:3b:3a:73:7e:
                    11:ef:45:a4:23:35:23:3a:91:d3:8c:1d:a6:a1:07:
                    7f:2c:bd:44:93:20:ab:26:1f:32:dd:c2:43:e5:2c:
                    07:34:5b:78:c8:48:31:83:96:ca:ee:be:97:e0:2a:
                    83:71:7d:b5:3f:ef:28:d8:15:cf:ad:93:b0:95:7a:
                    d3:f6:5f:12:f3:84:db:fc:f7:14:80:ec:97:88:1f:
                    ca:3f:a7:41:ca:3f:a9:78:8c:55:74:61:da:06:79:
```

cPanel X - Windows Internet Explorer
File Edit View Favorites Tools Help
WebHost Manager
cPanel X
Page
Tools
Done
Internet
100%

WHM

- Log in to WHM.
- From the menu, navigate to the "SSL/TLS" section and click "Generate a SSL Certificate and Signing Request."


WebHost Manager - Windows Internet Explorer
WHM VPS Optimized
cPanel 11.24.4-R33609 [TRIAL] - WHM 11.24.2 - X 3.9
CENTOS 5.2 x86_64 on xen
Home
News
Change Log
Insecure
Logout (root)
SSL/TLS
Generate a SSL Certificate and Signing Request

Main >> SSL/TLS >> Generate a SSL Certificate and Signing Request

Generate a SSL Certificate & Signing Request

Create a New Cert

Contact Info

Email Address the Cert will be sent to:

□ Do not email certificate signing request and private key upon completion

Cert Info (this will be displayed when a user connects)

Email:

Password: Generate Password

Password Strength:
Very Weak (0/100)

Host to make cert for:

City:

State:

Country (2 letter abbreviation):

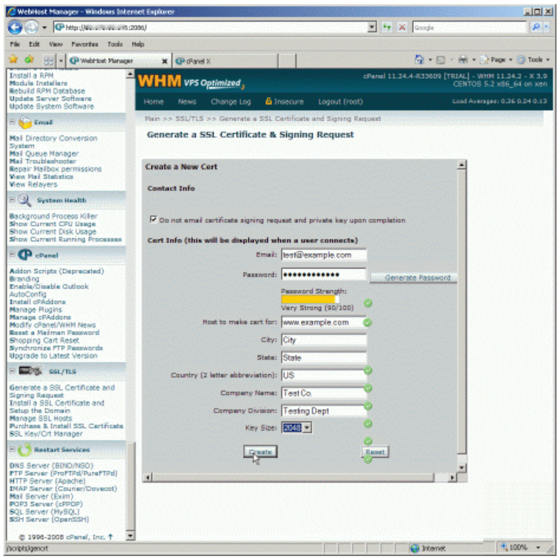
Company Name:

Company Division:

Key Size: 1024

Create Reset

- Fill out the form. Enter the name of the site you want a certificate for in “Host to make cert for.”
  Note, for wildcard certificates, the CN should be in the format: *.mydomain.com.
- We advise to use at least a 2048-bit key, which is the minimum for EV certificates. Click “Create.”


WebHost Manager - Windows Internet Explorer
WHM VPS Optimized
cPanel 11.24.4-R33609 [TRIAL] - WHM 11.24.2 - X 3.9
CENTOS 5.2 x86_64 on xen
Home
News
Change Log
Insecure
Logout (root)
SSL/TLS
Generate a SSL Certificate and Signing Request

Main >> SSL/TLS >> Generate a SSL Certificate and Signing Request

Generate a SSL Certificate & Signing Request

Create a New Cert

Contact Info

☑ Do not email certificate signing request and private key upon completion

Cert Info (this will be displayed when a user connects)

Email: test@example.com

Password: ●●●●●●●●●●●● Generate Password

Password Strength:
Very Strong (90/100)

Host to make cert for: www.example.com

City: City

State: State

Country (2 letter abbreviation): US

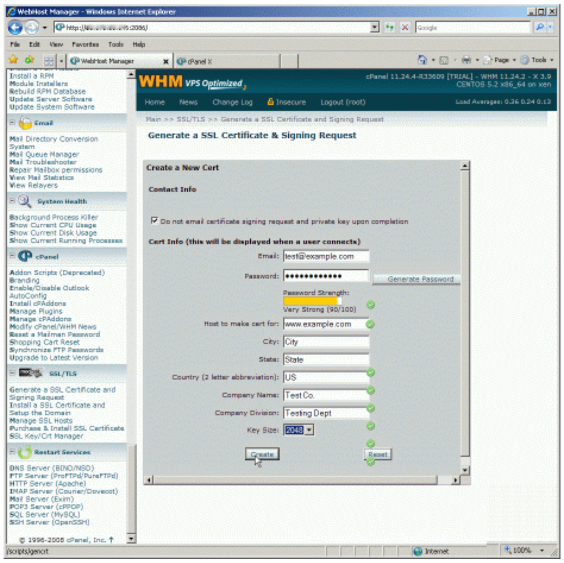
Company Name: Test Co.

Company Division: Testing Dept

Key Size: 2048

Create Reset

- Fill out the form. Enter the name of the site in “Host to make cert for.”


WebHost Manager - Windows Internet Explorer
WHM VPS Optimized
cPanel 11.24.4-R33609 [TRIAL] - WHM 11.24.2 - X 3.9
CENTOS 5.2 x86_64 on xen
Home
News
Change Log
Insecure
Logout (root)
Load Averages: 0.36 0.24 0.12
Main >> SSL/TLS >> Generate a SSL Certificate and Signing Request
Generate a Password
Create
Reset

Generate a SSL Certificate & Signing Request

Create a New Cert

Contact Info

☑ Do not email certificate signing request and private key upon completion

Cert Info (this will be displayed when a user connects)

Email: test@example.com

Password: ●●●●●●●●●●●●●

Password Strength: Very Strong (90/100)

Host to make cert for: www.example.com

City: City

State: State

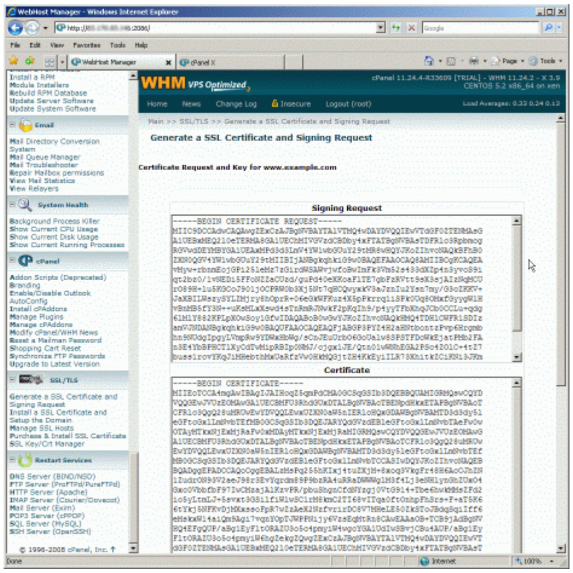
Country (2 letter abbreviation): US

Company Name: Test Co.

Company Division: Testing Dept

Key Size: 2048

- Finally, you will be presented with the CSR (labelled "Signing Request"), the private key, and a temporary self-signed certificate.
- Copy contents of the CSR and paste it into the enrollment form when requested.


WebHost Manager - Windows Internet Explorer
WHM VPS Optimized
cPanel 11.24.4-R33609 [TRIAL] - WHM 11.24.2 - X 3.9
CENTOS 5.2 x86_64 on xen
Home
News
Change Log
Insecure
Logout (root)
Load Averages: 0.33 0.24 0.12
Main >> SSL/TLS >> Generate a SSL Certificate and Signing Request

Generate a SSL Certificate and Signing Request

Certificate Request and Key for www.example.com

Signing Request

```
-----BEGIN CERTIFICATE REQUEST-----
[illegible]
```

Certificate

```
-----BEGIN CERTIFICATE-----
[illegible]
```

Microsoft Exchange 2007

CSR generation on Microsoft Exchange 2007 uses a cmdlet accessed via the Exchange Management Shell (EMS). To access the EMS, go to the Start menu > Programs > Microsoft Exchange Server 2007 and choose “Exchange Management Shell.”

- Once EMS is open, enter the following command:

    -
      ```
      New-ExchangeCertificate -GenerateRequest -KeySize 2048 -SubjectName "C=US, O=Example Company, L=City, ST=State, CN=exchange.example.com" -DomainName exampletwo.com, examplethree.com -Path c:\exchange.example.com.req -PrivateKeyExportable:$true
      ```
        - GenerateRequest: This is the command flag to create a new CSR.
        - KeySize: This controls the size of your private key. We recommend at least 2048 bit.
        - SubjectName: This sets the Subject of your CSR. “C” is country, in the ISO-3166 two-letter standard (note “GB” for Great Britain, US for USA, etc.). “O” is organisation. “L” is locality. “ST” is state or province. “CN” is common name, or your primary FQDN for the server.
        - DomainName: This allows you to specify additional domain names, as most Exchange 2007 installations require the certificate to secure more than one FQDN.
        - Path: This specifies where to place the CSR.
        - PrivateKeyExportable: This sets that the private key being generated is exportable, and will allow you to backup and/or move the private key later.
- Open the CSR file (specified above with the “-Path” flag) with a text-editor, copy the contents and paste them into the enrollment form when requested.

Notes:
Instead of specifying all the domains within the command, there are two additional flags that can be specified: “-IncludeAcceptedDomains” and “-IncludeAutoDiscover.” Using these instead of the “-DomainName” flag will automatically add the autodiscover Fully Qualified Domain Names (FQDNs), as well as all of the domains Exchange is configured to accept.

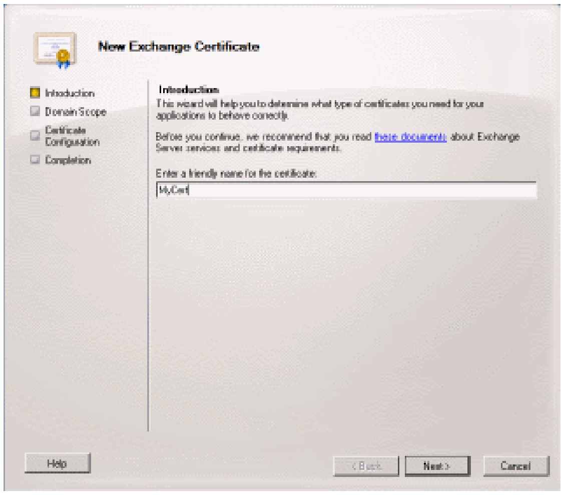
The Microsoft TechNet article for this command is available here:
http://technet.microsoft.com/en-us/library/aa998327(EXCHG.80).aspx.

Microsoft Exchange 2010

CSR generation on Microsoft Exchange 2010 can be done via either the GUI or via a cmdlet accessed via the Exchange Management Shell (EMS). Choose either option from below.

GUI

- Start the Exchange Management Console by going to Start > Programs > Microsoft Exchange 2010 > "Exchange Management Console."
- Click the link for "Manage Databases."
- Select "Server Configuration" and choose "New Exchange Certificate" from the actions. This will begin the wizard.
- Enter a name for the certificate; this name is for your own reference.



Introduction

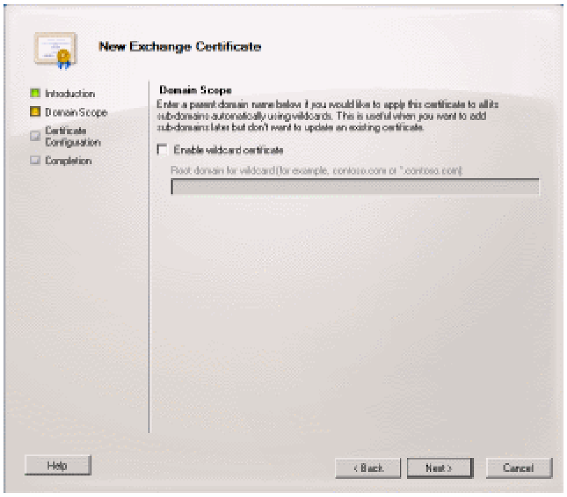
This wizard will help you to determine what type of certificates you need for your applications to behave correctly.

Before you continue, we recommend that you read these documents about Exchange Server services and certificate requirements.

Enter a friendly name for the certificate:

MyCert

- Here you have the option to enable a wildcard; only choose this if you are ordering a single wildcard certificate. In this case, skip the next step.



New Exchange Certificate

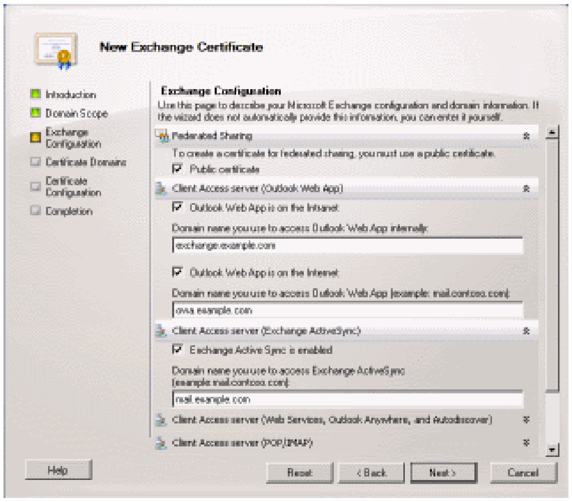
Domain Scope

Enter a parent domain name below if you would like to apply this certificate to all its sub-domains automatically using wildcards. This is useful when you want to add sub-domains later but don't want to update an existing certificate.

□ Enable wildcard certificate

Root domain for wildcard (for example, contoso.com or *.contoso.com)

- Now you must select the services you require the certificate for, and enter the appropriate FQDNs. As a general rule, you should enter all the names through which your Exchange 2010 server is accessed.



New Exchange Certificate

Exchange Configuration

Use this page to describe your Microsoft Exchange configuration and domain information. If the wizard does not automatically provide this information, you can enter it yourself.

Federated Sharing

To create a certificate for federated sharing, you must use a public certificate.

☑ Public certificate

Client Access server (Outlook Web App)

☑ Outlook Web App is on the Intranet

Domain name you use to access Outlook Web App internally:

exchange.example.com

☑ Outlook Web App is on the Internet

Domain name you use to access Outlook Web App (example: mail.contoso.com):

owa.example.com

Client Access server (Exchange ActiveSync)

☑ Exchange Active Sync is enabled

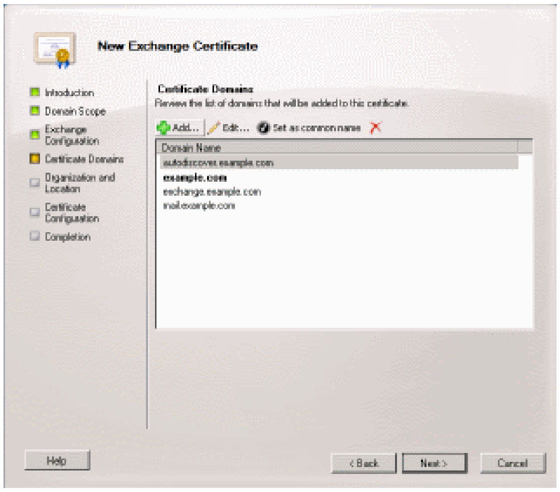
Domain name you use to access Exchange ActiveSync (example: mail.contoso.com):

mail.example.com

Client Access server (Web Services, Outlook Anywhere, and Autodiscover)

Client Access server (POP/IMAP)

- Review and confirm the list of domains and FQDNs to be added to the certificate.



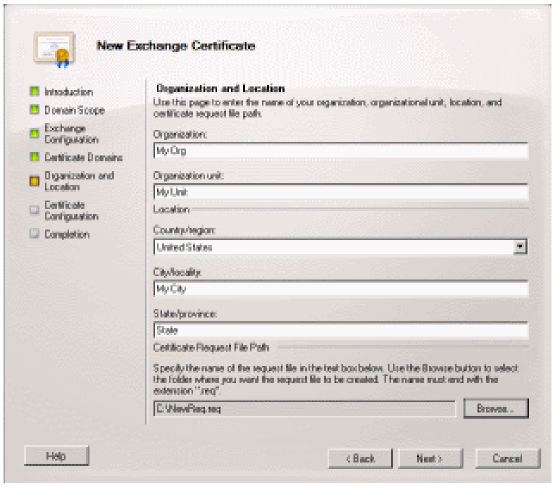
New Exchange Certificate

Certificate Domains

Review the list of domains that will be added to this certificate.

Domain Name
autodiscover.example.com
example.com
exchange.example.com
mail.example.com

- Now enter the information for your organization. You must also select a location for the CSR file to be written to.



New Exchange Certificate

Organization and Location

Use this page to enter the name of your organization, organizational unit, location, and certificate request file path.

Organization: My Org

Organization unit: My Unit

Location

Country/region: United States

City/locality: My City

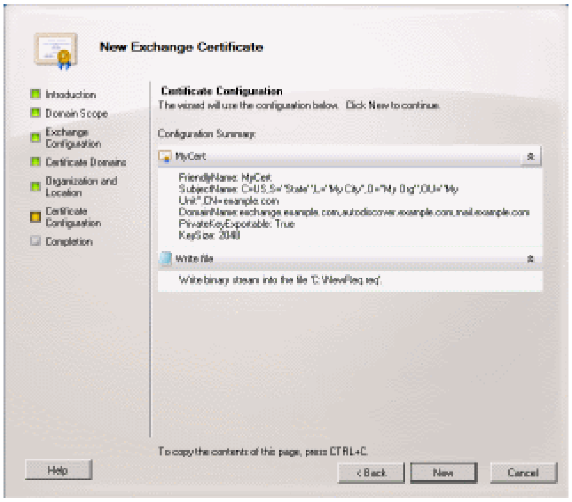
State/province: State

Certificate Request File Path

Specify the name of the request file in the text box below. Use the Browse button to select the folder where you want the request file to be created. The name must end with the extension ".req".

C:\NewReq.req

- Review the summary of the CSR generation, and the CSR file will be saved.



Certificate Configuration

The wizard will use the configuration below. Click New to continue.

Configuration Summary:

MyCert

FriendlyName: MyCert
SubjectName: C=US,S="State",L="My City",O="My Org",OU="My Unit",CN=example.com
DomainName: exchange.example.com,autodiscover.example.com,mail.example.com
PrivateKeyExportable: True
KeySize: 2048

Write file

Write binary stream into the file 'C:\NewReq.req'.

To copy the contents of this page, press CTRL+C.

- Open the CSR file (specified above) with a text-editor and copy and paste the contents into the enrollment form when requested.

cmdlet

- Open the EMS by Start menu > Programs > Microsoft Exchange Server 2007 and choose "Exchange Management Shell". The command you need to enter looks like this:
    - New-ExchangeCertificate -GenerateRequest -KeySize 2048 -SubjectName "C=US, O=Example Company, L=City, ST=State, CN=exchange.example.com" -DomainName exampletwo.com, examplethree.com -Path c:\exchange.example.com.req -PrivateKeyExportable:$true
        - GenerateRequest: This is the command flag to create a new CSR.
        - KeySize: This controls the size of your private key. We recommend at least 2048 bit.
        - SubjectName: This sets the Subject of your CSR. "C" is country, in the ISO-3166 two-letter standard (note "GB" for Great Britain, US for USA etc.). "O" is organisation. "L" is locality. "ST" is state or province. "CN" is common name, or your primary FQDN for the server.
        - DomainName: This allows you to specify additional domain names, as most Exchange 2007 installations require the certificate to secure more than one FQDN.
        - Path: This specifies where to place the CSR.
        - PrivateKeyExportable: This sets that the private key being generated is exportable, and will allow you to backup or move the private key later.
- Open the CSR file (specified above with the "-Path" flag) with a text-editor, copy the contents then paste them into the enrollment form when requested.

Notes:

Instead of specifying all the domains within the command, there are two additional flags that can be specified: “-IncludeAcceptedDomains” and “-IncludeAutoDiscover.” Using these instead of the “-DomainName” flag will automatically add the autodiscover FQDN, as well as all of the domains that Exchange is configured to accept.

The Microsoft TechNet article for this command is available here: http://technet.microsoft.com/en-us/library/aa998327(EXCHG.80).aspx.

F5 BigIP

To generate your CSR, use the instructions based on your version of the BigIP software.

F5 BigIP version 9 and later

- Open and log into the BigIP web interface.
- Under the “Local Traffic” menu, select “SSL Certificates,” then click “Create.”
- Under “General Properties,” you can give the certificate a name to identify it on the device. We suggest using the FQDN you are requesting the certificate for.
- Fill out the “Certificate Properties” form:
  - Issuer: Certificate Authority.
  - Common Name: Your FQDN, for example: www.example.com.
  - Your CSR is now generated. Open the “certreq.txt” file with a text-editor, copy the contents, then paste them into the enrollment form when requested.

F5 BigIP version 4.x

- Log in to the device as “root.” Execute the following command:
  #/usr/local/bin/genconf
  You will need to enter all of your company information, like name, address, etc.
- Now execute the command:
  #/usr/local/bin/genkey www.yourdomain.com
  Replace “www.yourdomain.com” with the FQDN you require the certificate for. This will generate the CSR.
- The CSR will be saved in a file at the location:
  /config/bigconfig/ssl.csr/www.yourdomain.com.csr
  Copy and paste the contents into the enrollment form when requesting a certificate.

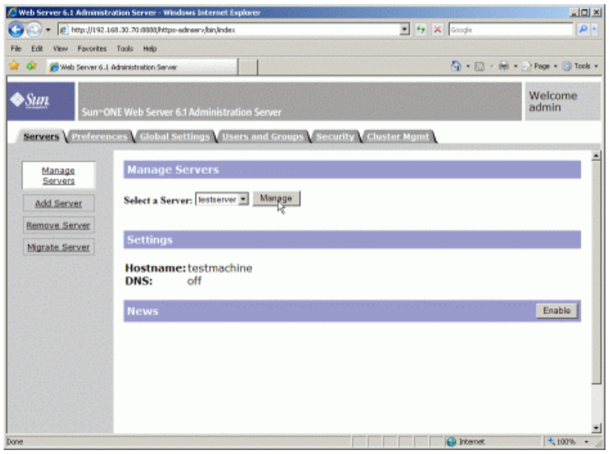
IBM HTTP Server

- First, you must create a new key database. Start the “IKEYMAN” software either by running the command “IKEYMAN” or loading the GUI version.
- Select “Key Database File” from the main menu and choose “New.”
- Choose and enter a new key database name. Click “OK.”
- Now enter and confirm a password for the key database. Please take care to remember the password you enter.
- Now we need to use the new key database to create a CSR. Start IKEYMAN again, select “Key Database File” and choose “Open.”
- Now enter the password from Step 4 and click “OK.”
- Select “Create” from the main menu, and choose “New Certificate Request.”
- A form will appear, and all the fields require completion. Click “OK” when completed. Notes on some of the fields are:
    - Key Label: simply a descriptive label for the CSR.
    - Keysize: we suggest the keysize be as large as possible, preferably 2048 bit.
    - Common Name: where you should enter the fully qualified domain name of the website you require the certificate for.
        - Note, for wildcard certificates, the Common Name should be in the format: *.mydomain.com
    - Country: the ISO-3166 two-letter country code for the country. “US” for the USA, “GB” for Great Britain, etc.
    - Certificate Request Filename: the path and filename for the CSR.
- Open the CSR file with a text-editor, copy the contents, then paste into the enrollment form when requested.

iPlanet 4.x /SunONE 6.x

To generate your CSR, you need to log in to the administrative web-interface of your iPlanet/SunONE server. This is usually at: http://<yourserver>:8888/

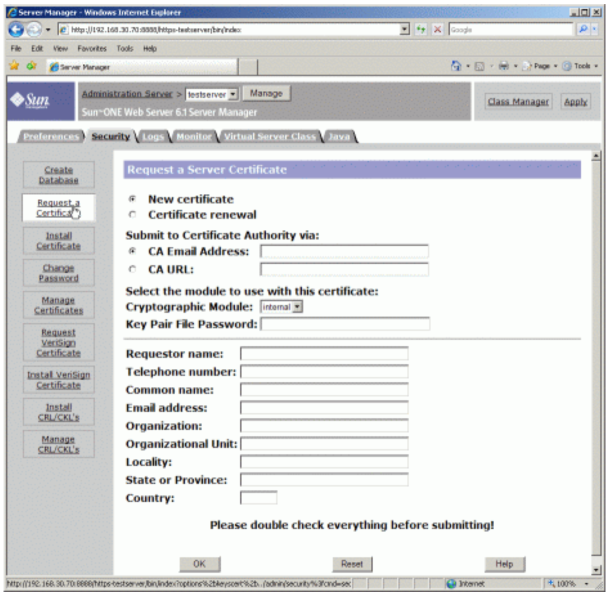
- Log into the iPlanet/SunONE administation interface. Select the server instance you require the certificate for and click “Manage.”


Web Server 6.1 Administration Server - Windows Internet Explorer
http://192.168.30.70:8888/https-admserv/bin/index
File Edit View Favorites Tools Help
Web Server 6.1 Administration Server
Sun
Sun-ONE Web Server 6.1 Administration Server
Welcome admin
Servers
Preferences
Global Settings
Users and Groups
Security
Cluster Mgmt
Manage Servers
Add Server
Remove Server
Migrate Server
Manage Servers
Manage
Settings
News
Enable
Done
Internet
100%

Select a Server: testserver

Hostname: testmachine
DNS: off

- Click the “Security” tab at the top of the page, then on the left, click the link for “Request a Certificate.”


Server Manager - Windows Internet Explorer
http://192.168.30.70:8888/https-testserver/bin/index
File Edit View Favorites Tools Help
Server Manager
Sun
Administration Server > testserver
Manage
Sun-ONE Web Server 6.1 Server Manager
Class Manager
Apply
Preferences
Security
Logs
Monitor
Virtual Server Class
Java
Create Database
Request a Certificate
Install Certificate
Change Password
Manage Certificates
Request VeriSign Certificate
Install VeriSign Certificate
Install CRL/CKL's
Manage CRL/CKL's
Request a Server Certificate
OK
Reset
Help
Internet
100%

● New certificate
○ Certificate renewal

Submit to Certificate Authority via:
● CA Email Address:
○ CA URL:

Select the module to use with this certificate:
Cryptographic Module: internal
Key Pair File Password:

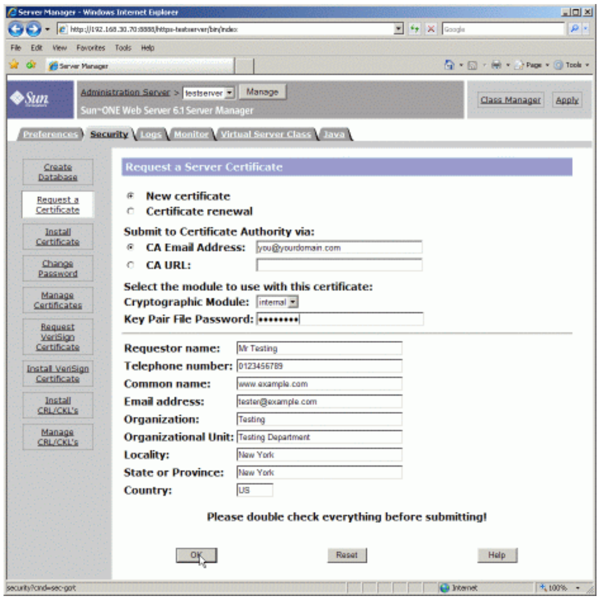
Requestor name:
Telephone number:
Common name:
Email address:
Organization:
Organizational Unit:
Locality:
State or Province:
Country:

Please double check everything before submitting!

- Fill your information into the form. Set the option for “Submit to Certificate Authority via:” to “CA Email Address” and **enter your own email address**.

  The “Common Name” is where you should enter the fully qualified domain name of the website you require the certificate for.

  Note, for wildcard certificates, the Common Name should be in the format: *.mydomain.com



Request a Server Certificate

● New certificate
○ Certificate renewal

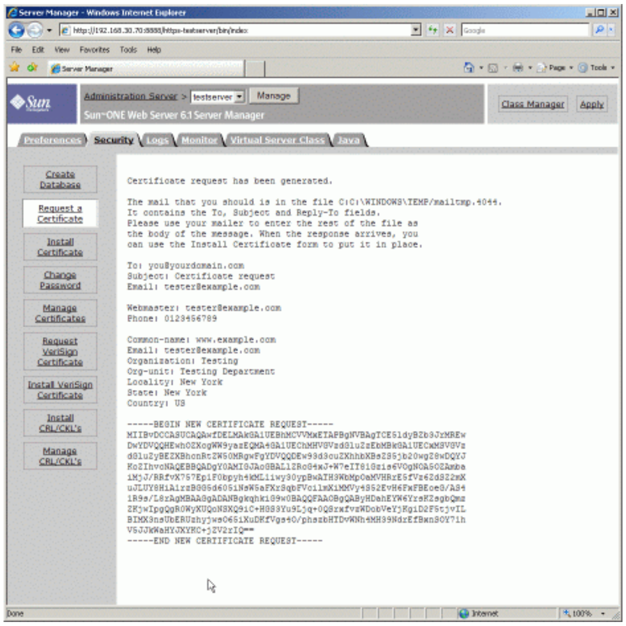
Submit to Certificate Authority via:
● CA Email Address: you@yourdomain.com
○ CA URL:

Select the module to use with this certificate:
Cryptographic Module: internal
Key Pair File Password: ••••••••

Requestor name: Mr Testing
Telephone number: 0123456789
Common name: www.example.com
Email address: tester@example.com
Organization: Testing
Organizational Unit: Testing Department
Locality: New York
State or Province: New York
Country: US

Please double check everything before submitting!

- After you have clicked "OK," you will be presented with a summary of the information, and the CSR. You can now copy and paste the contents of the CSR into the enrollment form when requested. Be sure to include the whole CSR, including the -----BEGIN NEW CERTIFICATE REQUEST----- line and the -----END NEW CERTIFICATE REQUEST----- line.



```
Certificate request has been generated.

The mail that you should is in the file C:C:\WINDOWS\TEMP/mailtmp.4044.
It contains the To, Subject and Reply-To fields.
Please use your mailer to enter the rest of the file as
the body of the message. When the response arrives, you
can use the Install Certificate form to put it in place.

To: you@yourdomain.com
Subject: Certificate request
Email: tester@example.com

Webmaster: tester@example.com
Phone: 0123456789

Common-name: www.example.com
Email: tester@example.com
Organization: Testing
Org-unit: Testing Department
Locality: New York
State: New York
Country: US

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBvDCCASUCAQAwfDELMAkGA1UEBhMCVVMxETAPBgNVBAgTCE5ldyBZb3JrMREw
DwYDVQQHEwhOZXogWW9yazEQMA4GA1UEChMHVGVzdGluZzEbMBkGA1UECxMSVGVz
dGluZyBEZXBhcnRtZW50MRgwFgYDVQQDEw93d3cuZXhhbXBsZS5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBALlZRo84xJ+W7eIT81Gzis6VOgNOA5OZAmba
iMjJ/RRfvX757Ep1F0bpyh4kML1iwy30ypBwATH3WbMpOaMVHRrE5fVz62d822mX
uJLUY8HiA1rzBG85d605iNsW5aFXrSqbFVoilmXiMMVy4852EvH6FxFBEoe3/A84
1R9s/L8rAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAByHDahEYW6YrsKZsgbQmz
ZKjwIpgQgR0WyXUQoNSXQ91C+H883Yu9Ljq+0Q8rxfvzWDobVeYjKgiD2F5tjvIL
BIMX3nsUbERUzhyjws066iXuDKfVgs40/phszbHIDvWNh4MH39NdrEfBxn8OY71h
V5JJkWaHYJXYKC+j2V2rIQ==
-----END NEW CERTIFICATE REQUEST-----
```

Java-based Webservers

To generate your CSR, log in to the server and open a command prompt or shell, and use the following instructions:

- Generate a new keystore and key with the following command:
  ```
  keytool -genkey -keyalg RSA -alias server -keystore my_keystore.jks
  ```
  Replace the file “my_keystore.jks” with the filename and path you wish to locate the keystore. The alias “server” can be changed to the site or server name if needed.

  For Tomcat, change the “-alias server” to “-alias tomcat.”

- You may be prompted for some information:
  ```
  Enter keystore password:
  What is your first and last name?
  What is the name of your organizational unit? **This is your CN**
  What is the name of your organization?
  What is the name of your city or locality?
  What is the name of your state or province?
  What is the two-letter country code for this unit?
  ```
  The “first and last name” actually means the fully-qualified domain name for your site, e.g., www.mydomain.com.

Note, for wildcard certificates, the Common Name should be in the format: .mydomain.com.

Please take care to remember the password you enter.

- Now generate the CSR using the key and keystore you have just created:
  ```
  keytool -certreq -alias server -file csr.txt -keystore my_keystore.jks
  ```

  Ensure that the alias and keystore have the same name and filename as in Step 1.

  You will be prompted to enter the password again. If successful, the file “csr.txt” will be created. Open this file with a text editor, copy the contents, then paste them into the enrollment form when requested.

Notes:
If you do not enter an alias with the “-alias” command flag, the default alias will be used, “mykey.”

Microsoft IIS 4.x

To generate your CSR, you will need to log in to your server and use the following instructions:

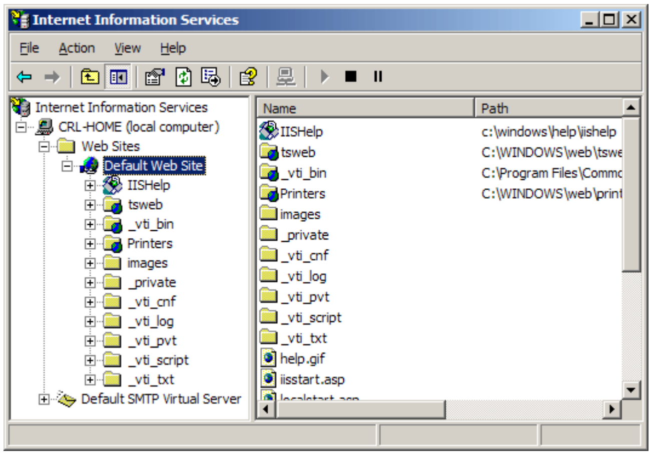
- Open the Microsoft Management Console.
- Expand the “Internet Information Server” and then expand your server name.
- Open the “Properties” of the website you require the CSR for. Do this by right-clicking on the website.
- Open “Directory Security.”
- Under the “Secure Communications” area, choose “Key Manager” and select “Create a New Key.”
- Fill out your information. The following characters are not allowed: ! @ # $ % ^ * ( ) ~ ? > < & / \
- Click “Next” until you complete the process. Answer “Yes” to saving any changes.
- Open the CSR file that was created with a text-editor (usually notepad). Copy the contents of the file, from:
  -----BEGIN CERTIFICATE REQUEST-----
  ...to...
  -----END CERTIFICATE REQUEST-----
  Paste this information into the enrollment form when requested.

Microsoft IIS 5.x& 6.x

To generate your CSR, you will need to log in to your server and use the following instructions.

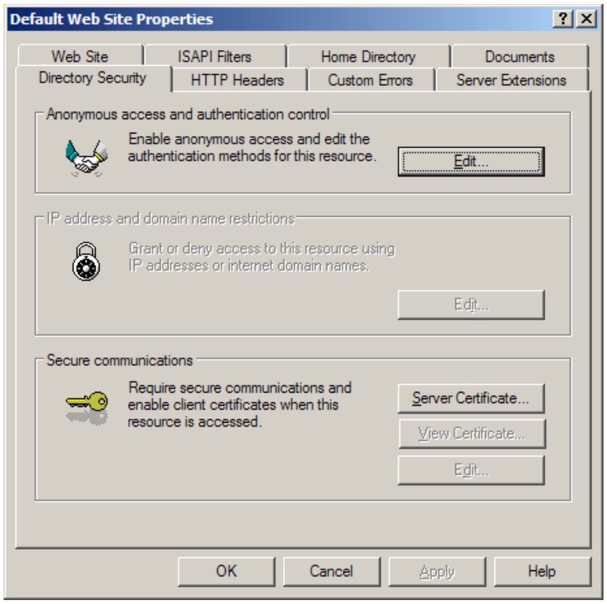
If you are generating a CSR to renew a certificate, or a CSR for a site that has an existing certificate, please see the notes at the end of this guide.

- Log in to the server. Go to “Control Panel” > “Administrative Tools” and double-click “Internet Services Manager.”



Name	Path
IISHelp	c:\windows\help\iishelp
tsweb	C:\WINDOWS\web\tswe
_vti_bin	C:\Program Files\Commc
Printers	C:\WINDOWS\web\print
images	
_private	
_vti_cnf	
_vti_log	
_vti_pvt	
_vti_script	
_vti_txt	
help.gif	
iisstart.asp	

- Right-click on the website you require the CSR for and choose “Properties.” Select the “Directory Security” tab.

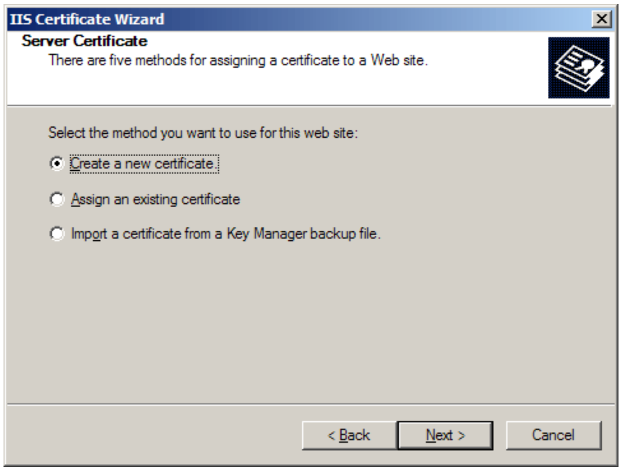


Enable anonymous access and edit the authentication methods for this resource.

Grant or deny access to this resource using IP addresses or internet domain names.

Require secure communications and enable client certificates when this resource is accessed.

- Click the “Server Certificate” button. A wizard will start. Choose the option to “Create a new certificate.” Click “Next.”



IIS Certificate Wizard

Server Certificate

There are five methods for assigning a certificate to a Web site.

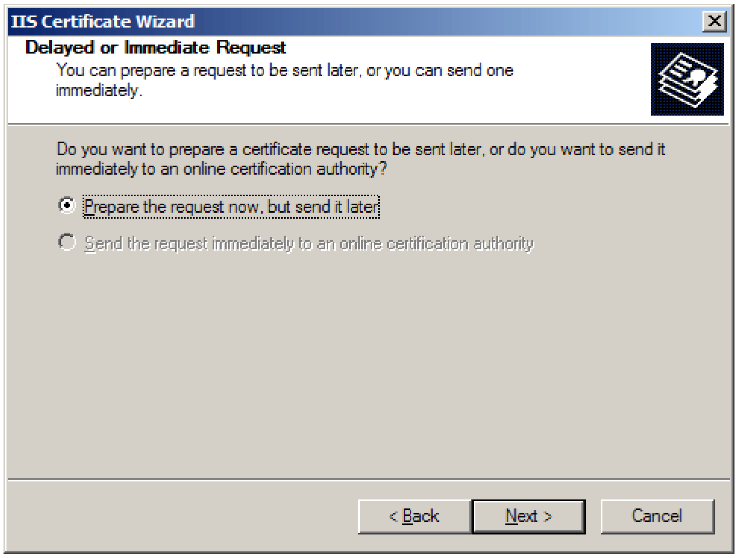
Select the method you want to use for this web site:

● Create a new certificate

○ Assign an existing certificate

○ Import a certificate from a Key Manager backup file.

- Click “Prepare the request now, but send it later.” Click “Next.”



IIS Certificate Wizard

Delayed or Immediate Request

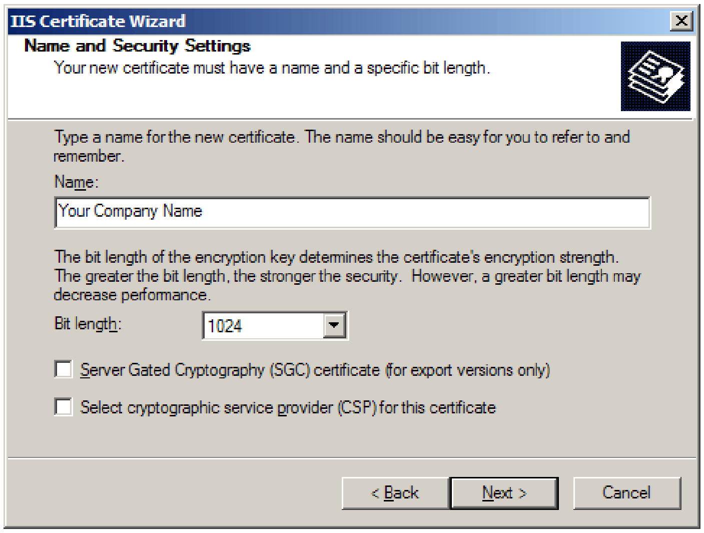
You can prepare a request to be sent later, or you can send one immediately.

Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

● Prepare the request now, but send it later

○ Send the request immediately to an online certification authority

- Enter your information. The “Name” here refers to a friendly name for the certificate, and is not your domain. The other options can be left at their defaults. Click “Next.”



IIS Certificate Wizard

Name and Security Settings

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Name: Your Company Name

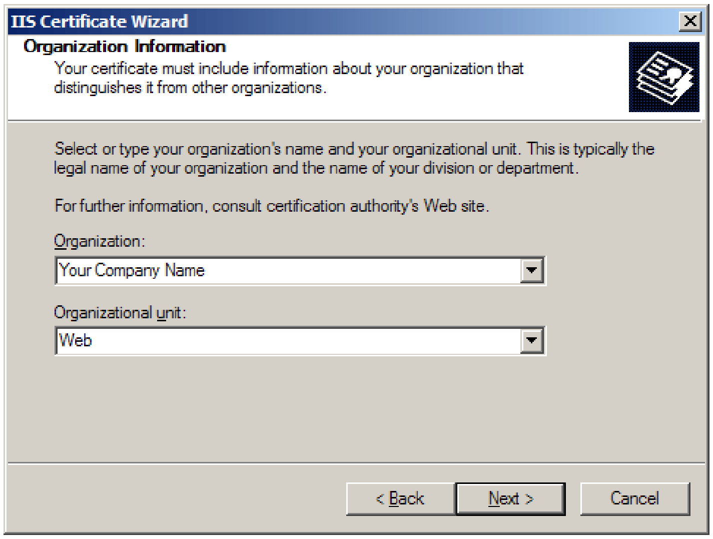
The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length: 1024

□ Server Gated Cryptography (SGC) certificate (for export versions only)

□ Select cryptographic service provider (CSP) for this certificate

- Enter your organization and organizational unit information. Click "Next."



IIS Certificate Wizard

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

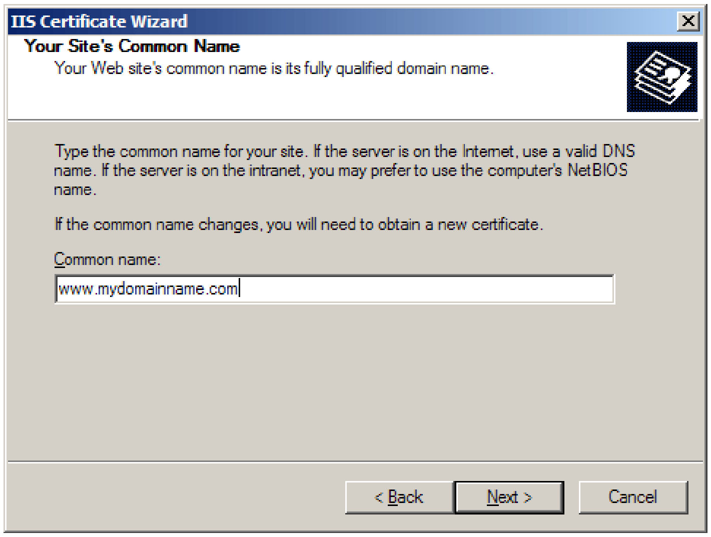
Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization: Your Company Name

Organizational unit: Web

- Enter the fully qualified domain name of the website you require the certificate for. For wildcard certificates, enter in the format *.mydomain.com. Click "Next."



IIS Certificate Wizard

Your Site's Common Name

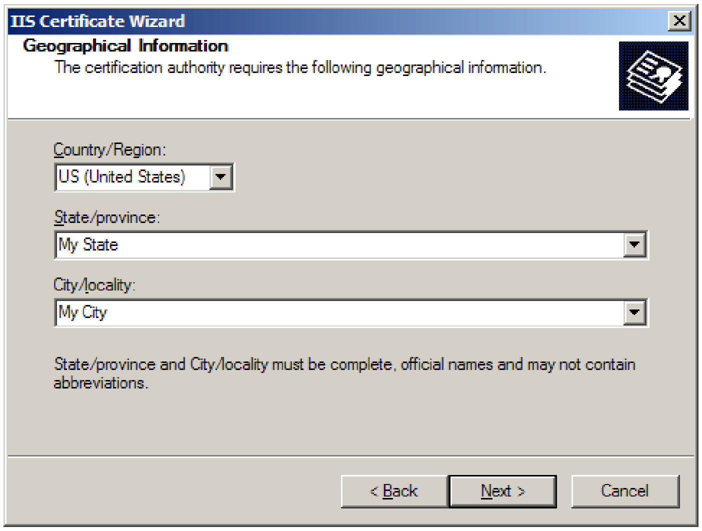
Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name: www.mydomainname.com

- Enter your location information. Click “Next.”



IIS Certificate Wizard

Geographical Information

The certification authority requires the following geographical information.

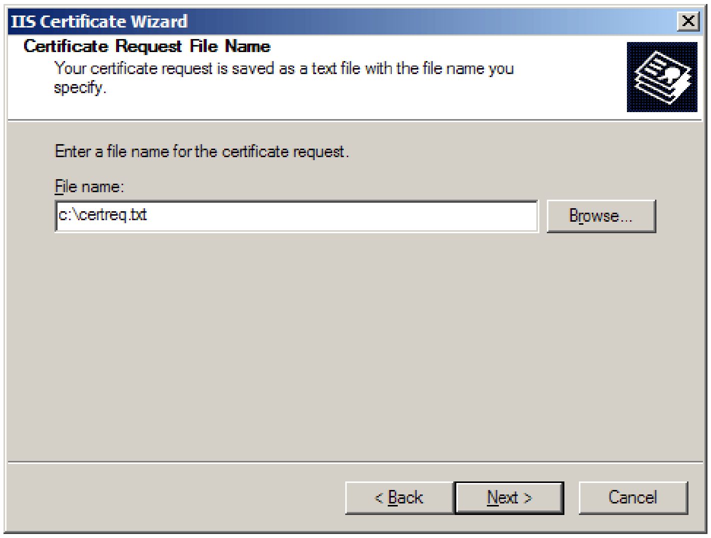
Country/Region: US (United States)

State/province: My State

City/locality: My City

State/province and City/locality must be complete, official names and may not contain abbreviations.

- Choose a path and filename to save the CSR. Click “Next.”



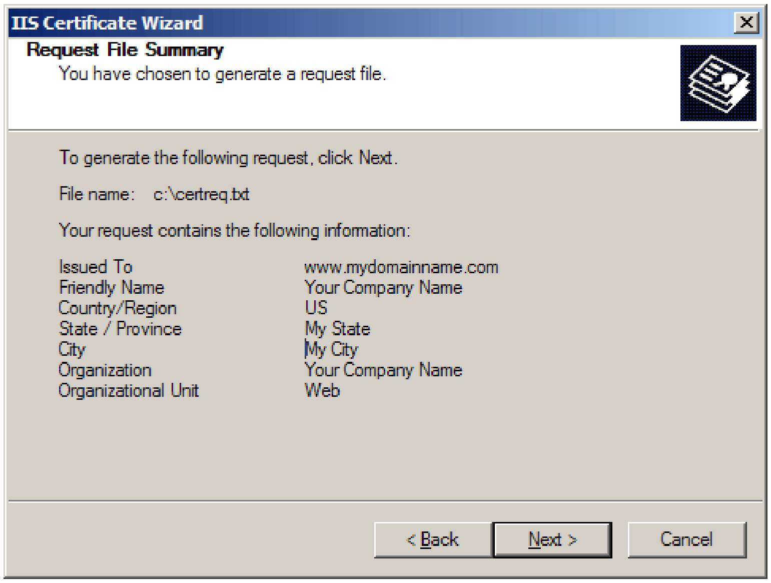
Certificate Request File Name

Your certificate request is saved as a text file with the file name you specify.

Enter a file name for the certificate request.

File name: c:\certreq.txt

- Review the information. Click "Next."



Request File Summary

You have chosen to generate a request file.

To generate the following request, click Next.

File name: c:\certreq.txt

Your request contains the following information:

Issued To	www.mydomainname.com
Friendly Name	Your Company Name
Country/Region	US
State / Province	My State
City	My City
Organization	Your Company Name
Organizational Unit	Web

- Your CSR is now generated. Open the "certreq.txt" file with a text-editor, copy the contents, then paste them into the enrollment form when requested.

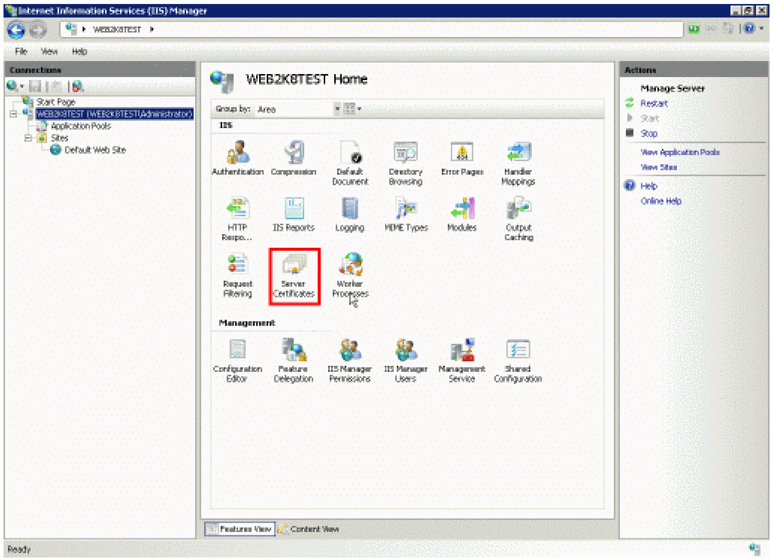
Notes:
If you are generating CSR for a renewal of a certificate, Step 3 should have an option to renew the certificate and generate a new CSR. Select this and follow the wizard through to create a renewal CSR for the certificate.

The CSR generation process will create a “Pending Request” on the website. DO NOT remove this pending request. It will be completed once you receive and install the certificate. Removing the Pending Request before you have installed your certificate will render the certificate useless, and you will need to repeat the whole CSR generation process again, and re-submit the CSR to us.

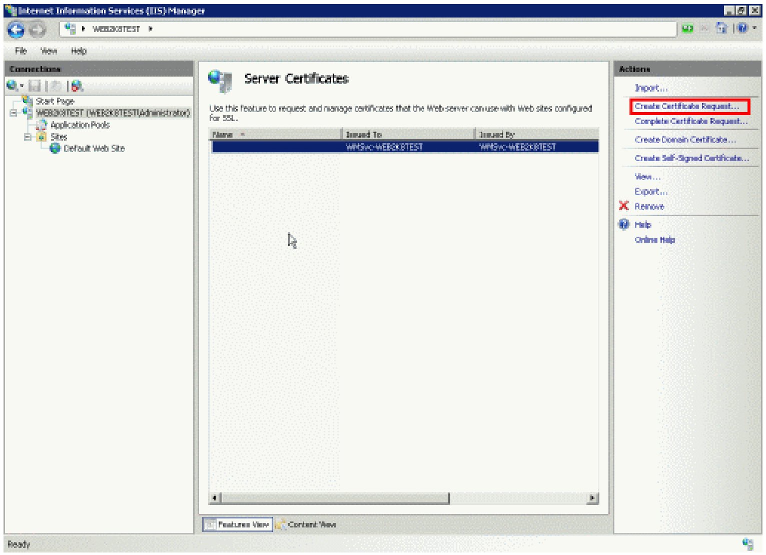
Microsoft IIS 7.x

To generate your CSR, you will need to log in to your server and use the following instructions:

- Click the Start menu > Administrative Tools > Internet Information Services (IIS) Manager.
- Click the server name.
- In the menu, click the “Server Certificates” button in the “Security” section.



- On the right-hand-side, click the “Create Certificate Request...” Action. This will begin the Request Certificate Wizard.

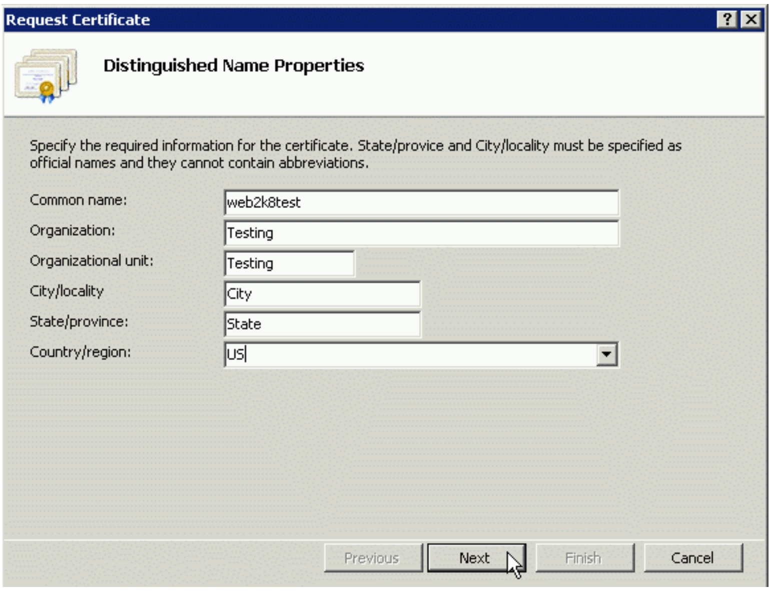


Internet Information Services (IIS) Manager
WEB2K8TEST
File
View
Help
Connections
Start Page
WEB2K8TEST (WEB2K8TEST\Administrator)
Application Pools
Sites
Default Web Site
Server Certificates
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Help
Online Help
Features View
Content View
Ready

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

Name	Issued To	Issued By
	WMSvc-WEB2K8TEST	WMSvc-WEB2K8TEST

- Fill out your information. The CN is where you should enter the fully qualified domain name of the website you require the certificate for. For wildcard certificates, this is in the format *.mydomain.com. Click “Next.”

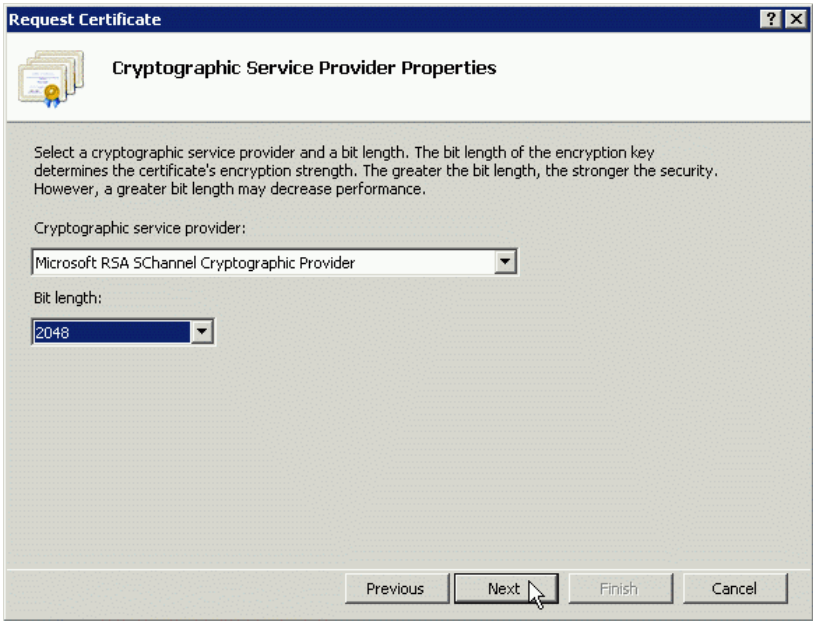


Distinguished Name Properties

Specify the required information for the certificate. State/provice and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	web2k8test
Organization:	Testing
Organizational unit:	Testing
City/locality	City
State/province:	State
Country/region:	US

- Leave the “cryptographic service provider” as default. The “bit length” can be changed, we recommend a minimum of 1024-bit, and 2048-bit where possible. Click “Next.”



Request Certificate

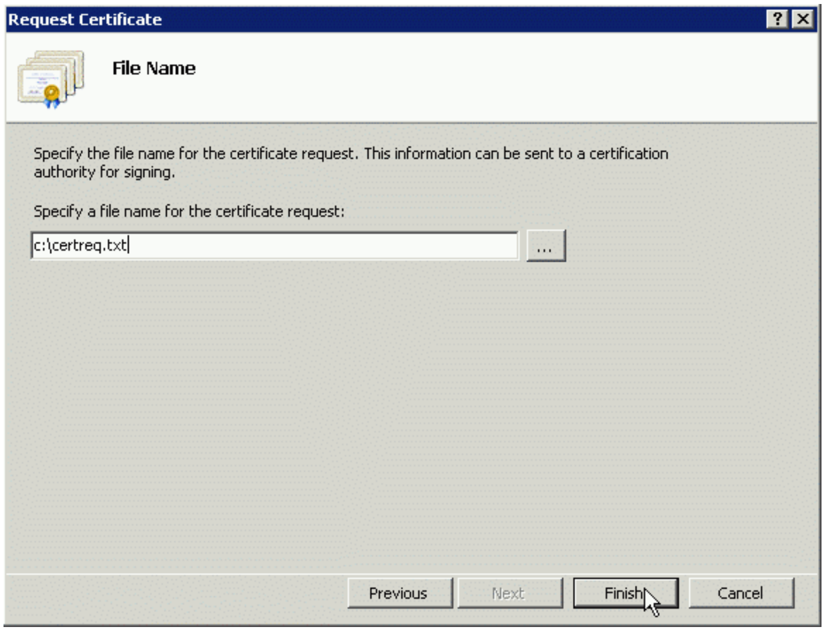
Cryptographic Service Provider Properties

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

- Choose a path and filename to save the CSR. Click "Finish."



Request Certificate

File Name

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request: c:\certreq.txt

- Your CSR is now generated. Open the "certreq.txt" file with a text-editor, copy the contents, then paste them into the enrollment form when requested.

Notes:

EV certificates require a minimum of a 1024-bit keysize if valid before 2011, and 2048-bit if they are valid into 2011. We recommend a 2048-bit keysize as minimum for all certificates.

Oracle (using Oracle Wallet Manager)

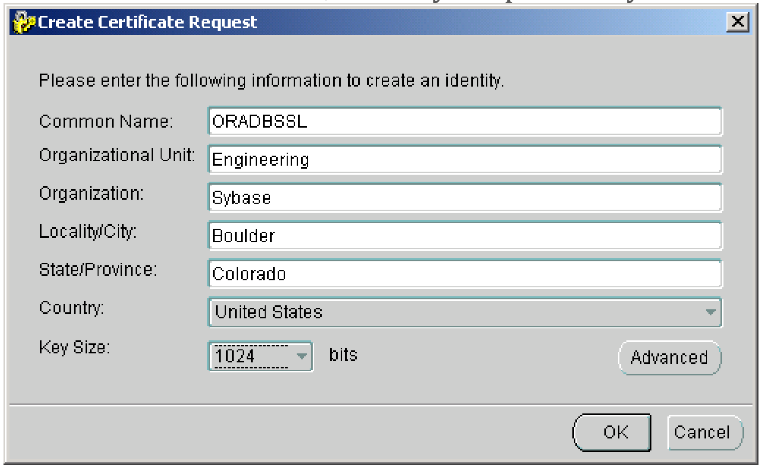
To generate your CSR, start the Oracle Wallet Manager program.

- Select “Operations” from the main menu. Choose the option “Create Certificate Request.”
- You will be presented with a form, complete the information.

  The CN is where you should enter the fully qualified domain name of the website you require the certificate for. Note that Oracle Wallet Manager does not currently support wildcard certificates.

  Set the keysize to at least 1024 bit, preferably 2048 if possible.

  Do not click the “Advanced” button, unless you specifically have been instructed to.



Create Certificate Request

Please enter the following information to create an identity.

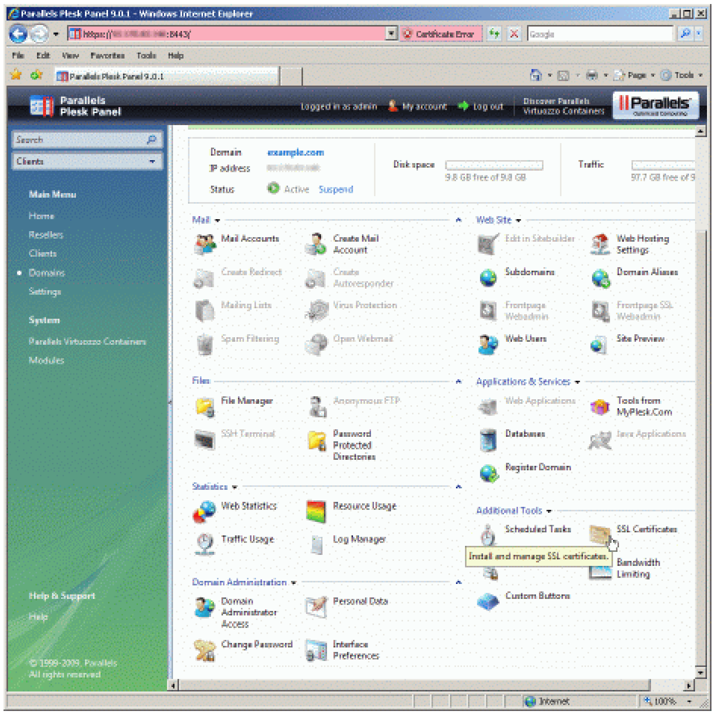
Common Name:	ORADBSSL
Organizational Unit:	Engineering
Organization:	Sybase
Locality/City:	Boulder
State/Province:	Colorado
Country:	United States
Key Size:	1024 bits

- Click “OK” to create the request, and “OK” again to return to the menu.
- Select “Operations” from the main menu again, and choose the “Export Certificate Request” option.
- Choose a path and filename to save the CSR. Click “OK.”
- Locate the CSR file in the path you just chose. Open with a text-editor, copy the contents, then paste them into the enrollment form when requested.

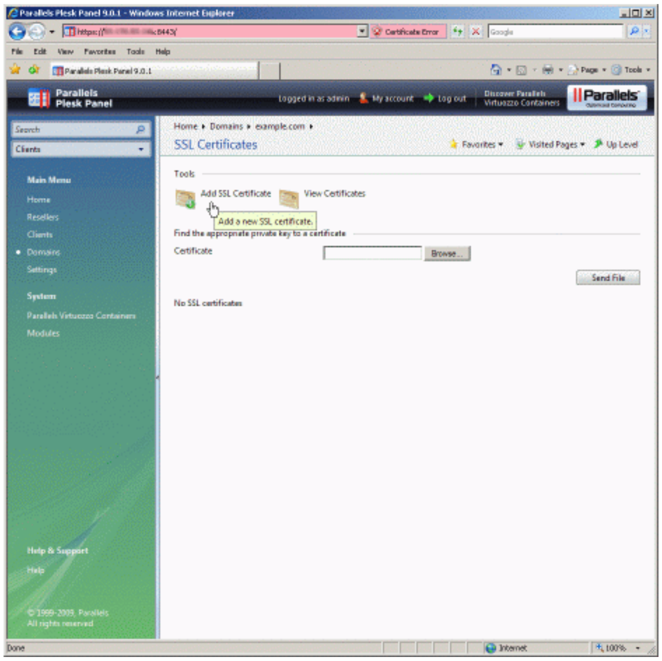
Plesk

To generate your CSR, you will need to log in to your Plesk account. The screenshots are from the latest Plesk release (v9), but the instructions apply to versions 7-9.

- Log in to Plesk. Click on "Domains" on the left, then click the domain you wish to request the certificate for. Click the "SSL Certificates" icon.



- Click the "Add SSL Certificate" icon.



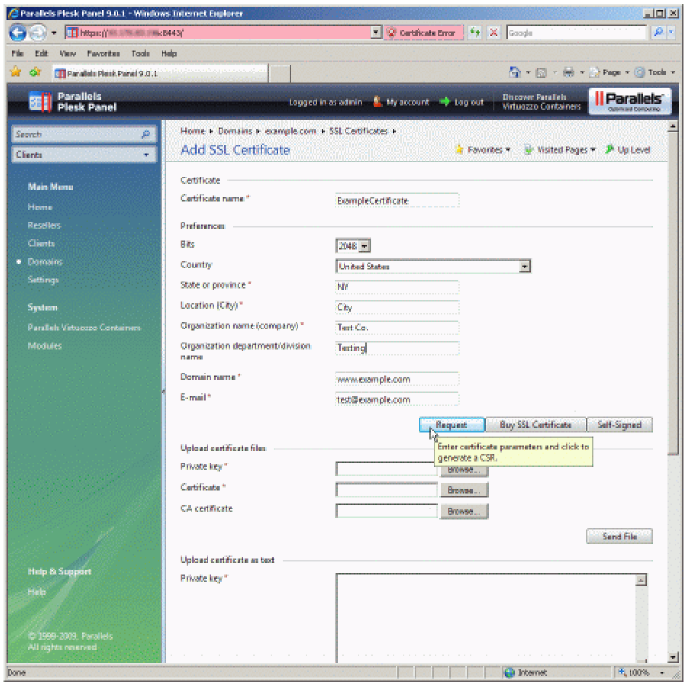
Add a new SSL certificate.

Find the appropriate private key to a certificate

Certificate

No SSL certificates

- Fill out your information in the form. Note, for wildcard certificates, the domain name field should be in the format: *.mydomain.com.



Certificate

Certificate name *	ExampleCertificate

Preferences

Bits	2048
Country	United States
State or province *	NY
Location (City) *	City
Organization name (company) *	Test Co.
Organization department/division name	Testing
Domain name *	www.example.com
E-mail *	test@example.com

Enter certificate parameters and click to generate a CSR.

Upload certificate files

Private key *

Certificate *

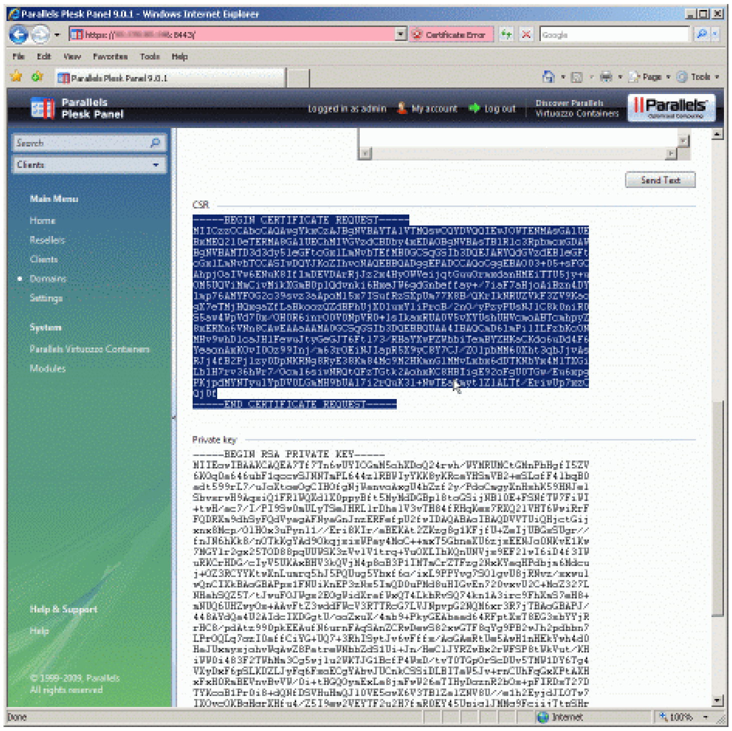
CA certificate

Upload certificate as text

Private key *

- We advise to use at least a 2048-bit key, which is the minimum for EV certificates.

- Click the “Request” button.
- You will be returned to the “SSL Certificates” section. Click the name of the certificate in the list.
- Scroll down to the section labelled “CSR.” Highlight the whole CSR as shown in the screenshot, and then you can copy and paste the CSR into the web enrollment form.



CSR

```
-----BEGIN CERTIFICATE REQUEST-----
[illegible]
-----END CERTIFICATE REQUEST-----
```

Private key

```
-----BEGIN RSA PRIVATE KEY-----
[illegible]
```

- Your CSR is now generated.