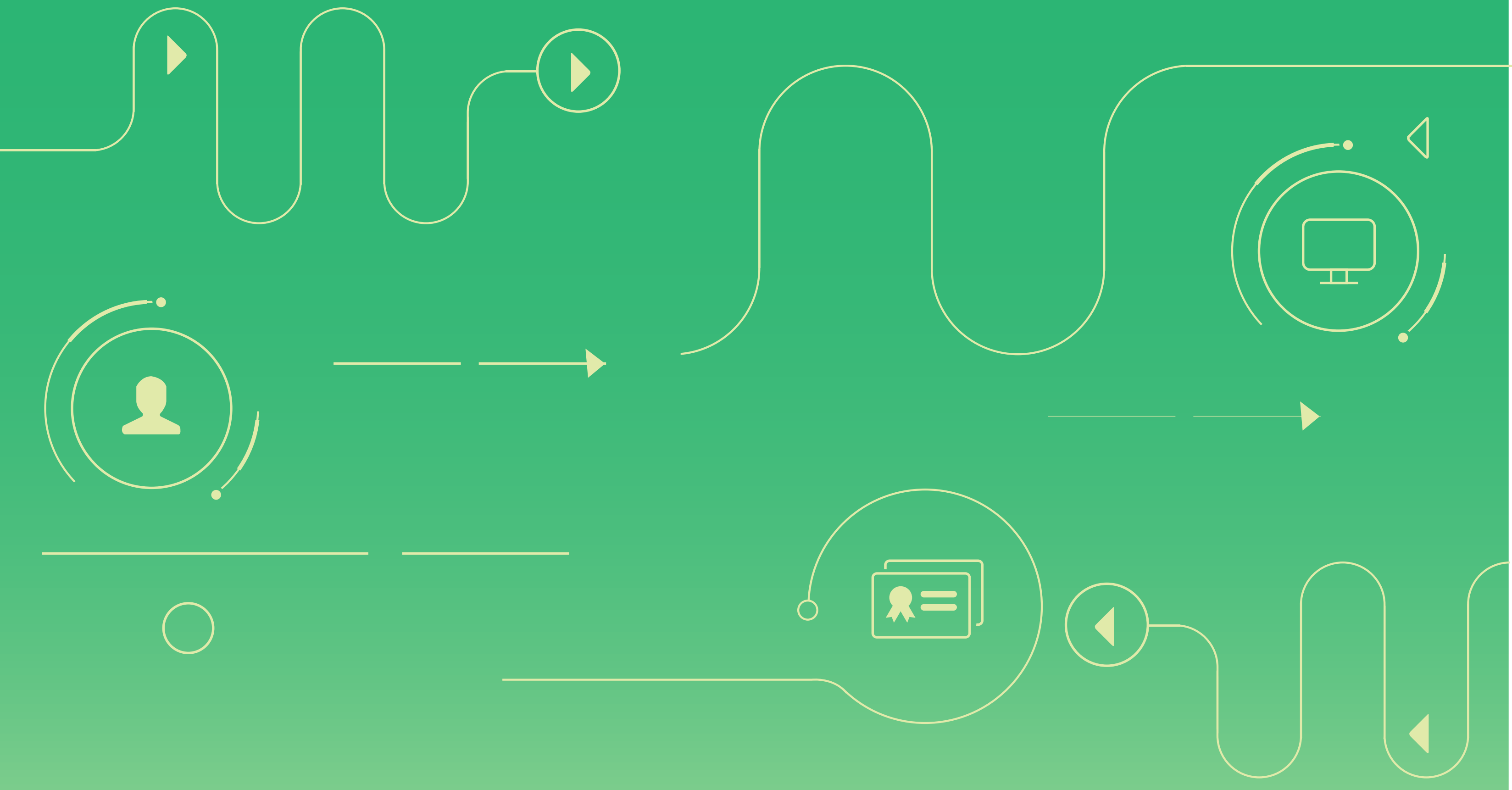
ManageEngine
Key Manager Plus

Installing SSL Certificates in Microsoft Internet Information Services(IIS)



www.keymanagerplus.com

Article purpose

This article provides step-by-step instructions for installing SSL certificates in Microsoft Internet Information services (IIS) using Key Manager Plus.

If you are an organization dealing with a large number of web applications, deploying SSL certificates for your websites and managing them might be one of your top concerns. Let's go over on how to simplify the process of deploying and managing SSL certificates for your websites using Key Manager Plus.

Deploying existing SSL certificates to IIS

If you have already purchased SSL certificates, follow the steps below to deploy them in Internet Information Services (IIS) and manage them using Key Manager Plus.

Step 1: Add your certificate to Key Manager Plus repository

To deploy and manage certificates in IIS, you initially have to add your certificates to KeyManager Plus certificate repository. To do that,

- Navigate to **SSL > Certificates** tab
- Click **Add**
- In the **Add Certificate** window that opens, provide the path and click **Add**
- The certificate gets added to Key Manager Plus certificate repository and you can view it from the **SSL > Certificates** tab

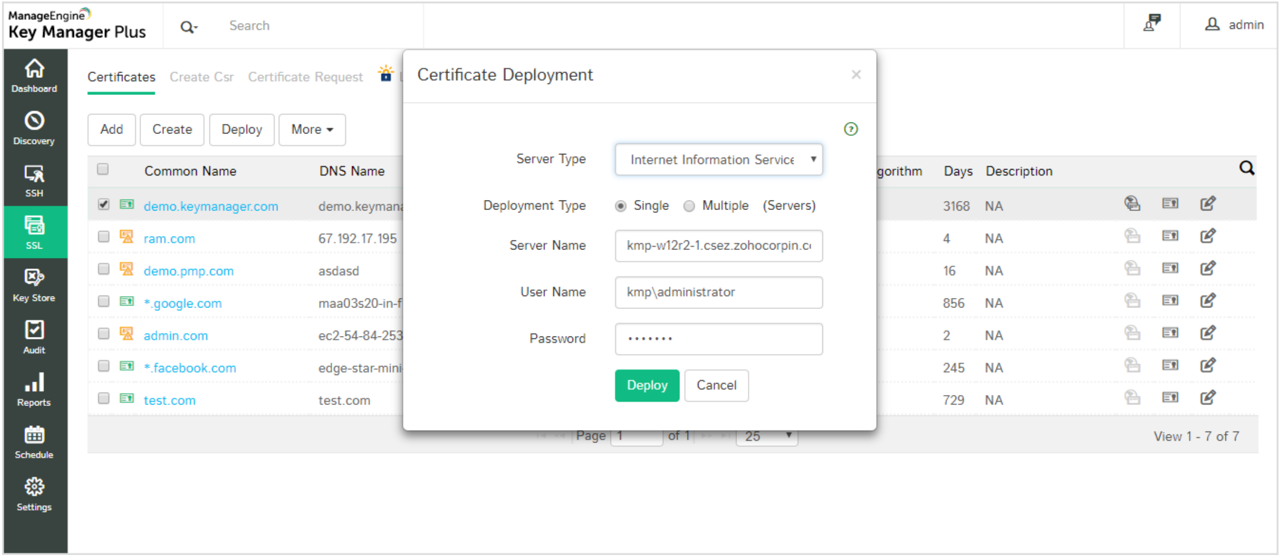
Step 2: Deploy the certificate to Internet Information Services (IIS)

After adding the certificate to the centralized repository, you have to deploy it to your Windows server. This can directly be done from the Key Manager Plus interface.

To deploy the certificate to IIS,

- Navigate to **SSL --> Certificates** tab
- Select the required certificate and click **Deploy**
- In the **Certificate Deployment** window that opens, choose the server type as **Internet Information services (IIS)**
- Choose the deployment type as **single** or **multiple** as per your need Select the required certificate and click **Deploy**
- For single deployment, provide the required details: **Server name**, **user name**, password.
- For certificate deployment on multiple servers, upload a .csv file comprising the following details:
  Server name, user name, password
- After providing the details, click **Deploy**
- The certificate is deployed in **Server Certificates** of the specified server(s)

(Note: By default, the common name is taken as the certificate file name).



Certificate Deployment

Server Type: Internet Information Service

Deployment Type: ● Single ○ Multiple (Servers)

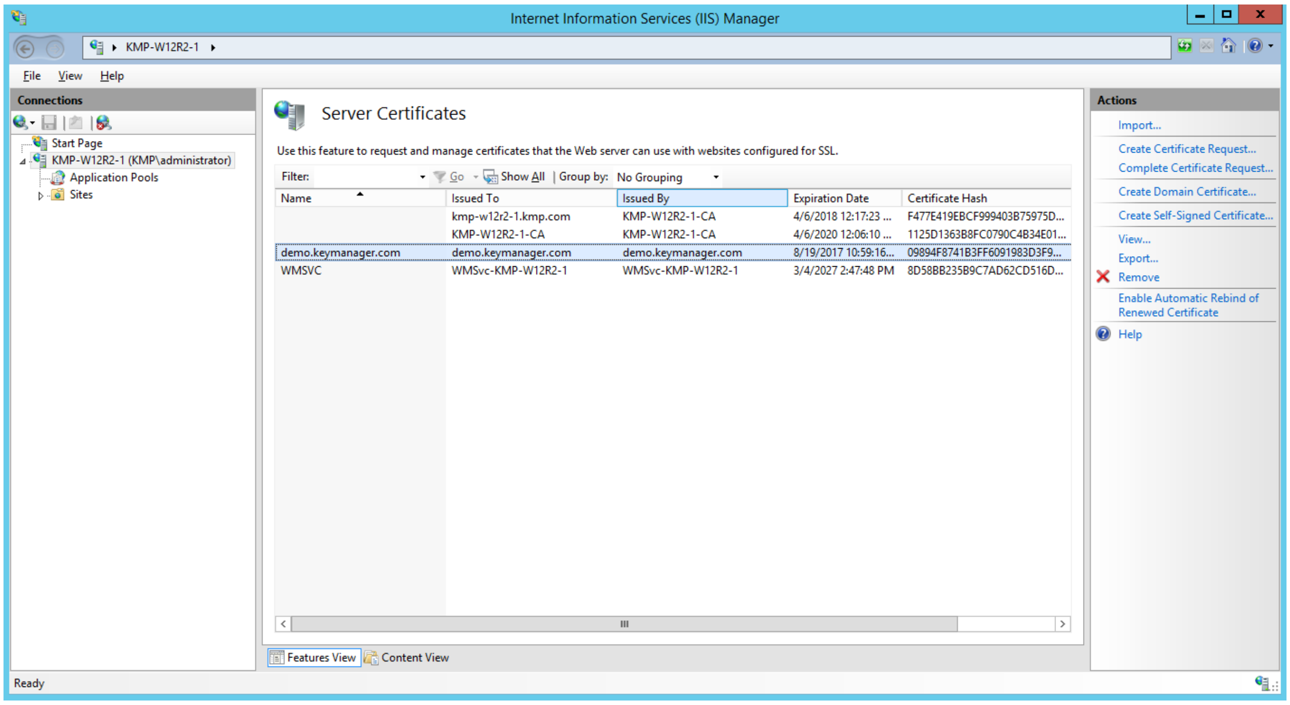
Server Name: kmp-w12r2-1.csez.zohocorpin.c

User Name: kmp\administrator

Password: •••••••

Deploy Cancel

	Common Name	DNS Name	gorithm	Days	Description
☑	demo.keymanager.com	demo.keymana		3168	NA
□	ram.com	67.192.17.195		4	NA
□	demo.pmp.com	asdasd		16	NA
□	*.google.com	maa03s20-in-f		856	NA
□	admin.com	ec2-54-84-253		2	NA
□	*.facebook.com	edge-star-mini		245	NA
□	test.com	test.com		729	NA



Internet Information Services (IIS) Manager
KMP-W12R2-1
File
View
Help
Connections
Start Page
KMP-W12R2-1 (KMP\administrator)
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready

Server Certificates

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

Filter: Go Show All | Group by: No Grouping

Name	Issued To	Issued By	Expiration Date	Certificate Hash
	kmp-w12r2-1.kmp.com	KMP-W12R2-1-CA	4/6/2018 12:17:23 ...	F477E419EBCF999403B75975D...
	KMP-W12R2-1-CA	KMP-W12R2-1-CA	4/6/2020 12:06:10 ...	1125D1363B8FC0790C4B34E01...
demo.keymanager.com	demo.keymanager.com	demo.keymanager.com	8/19/2017 10:59:16...	09894F8741B3FF6091983D3F9...
WMSVC	WMSvc-KMP-W12R2-1	WMSvc-KMP-W12R2-1	3/4/2027 2:47:48 PM	8D58BB235B9C7AD62CD516D...

Step 3: Bind the certificate to your website

Once the certificate is installed on the required server(s), you have to bind the certificate with your website. To do this,

- Navigate to the domain server
- Open the Internet Information Services (IIS) manager

(In the Windows **start** menu, click **Administrative Tools --> Internet Information Services (IIS) manager**)

- In IIS manager, under connections, expand your server name, then expand **Sites**, and then select the site that you want to secure with the SSL certificate
- In the **Actions** pane, under **edit sites** click **Bindings**
- In the **Site Binding** window that opens, click **Add**
- Enter the following information in the **Add Site Binding** window

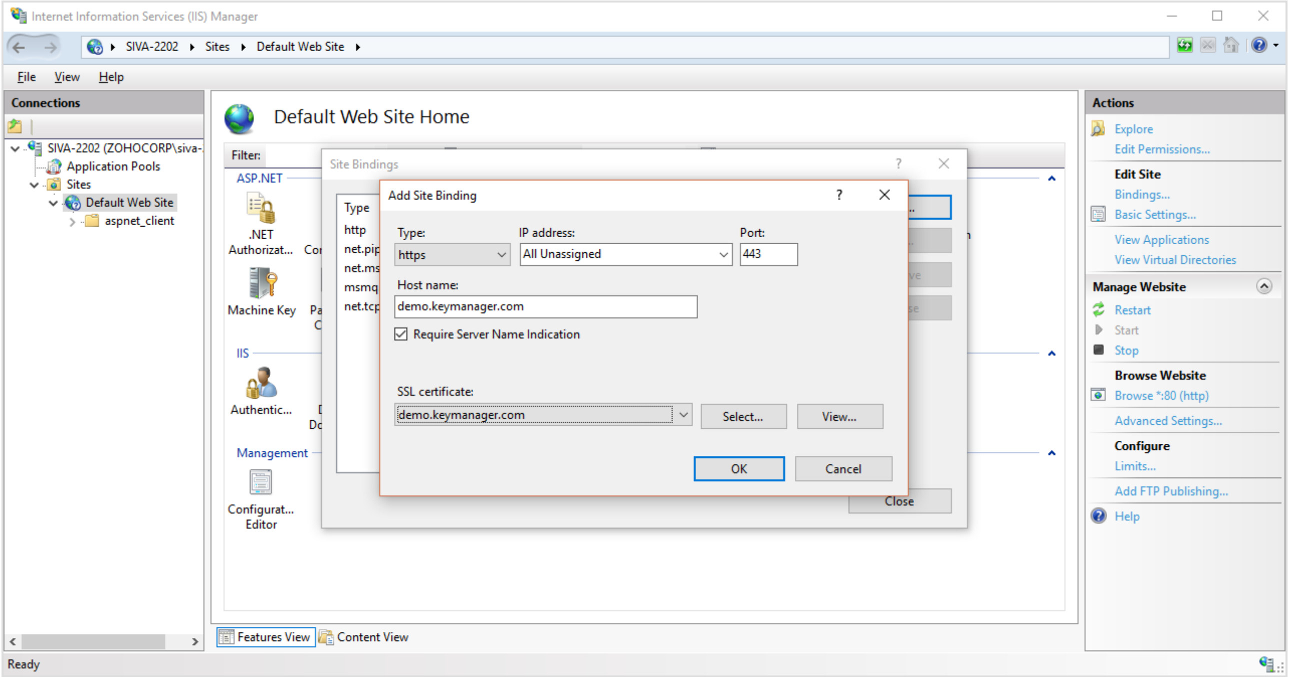
  1**. Type**: In the drop-down list, select **https**.

  2. **IP address**: In the drop-down list, select **All unassigned**. If your server has multiple IP addresses, select the one that applies.

  3. **Port**: Enter 443, unless you are using a non-standard port for SSL traffic.

  4. **SSL certificate**: In the drop-down list, select the name of the certificate that you just installed.

  5. After filling in the details, click **OK**



Type: https

IP address: All Unassigned

Port: 443

Host name: demo.keymanager.com

☑ Require Server Name Indication

SSL certificate: demo.keymanager.com

There you go, your domain is now SSL secured!

Step 4: Manage certificate expiry and notification

After deploying your certificates in IIS, you can manage, monitor, audit and track them for expiry from Key Manager Plus interface.

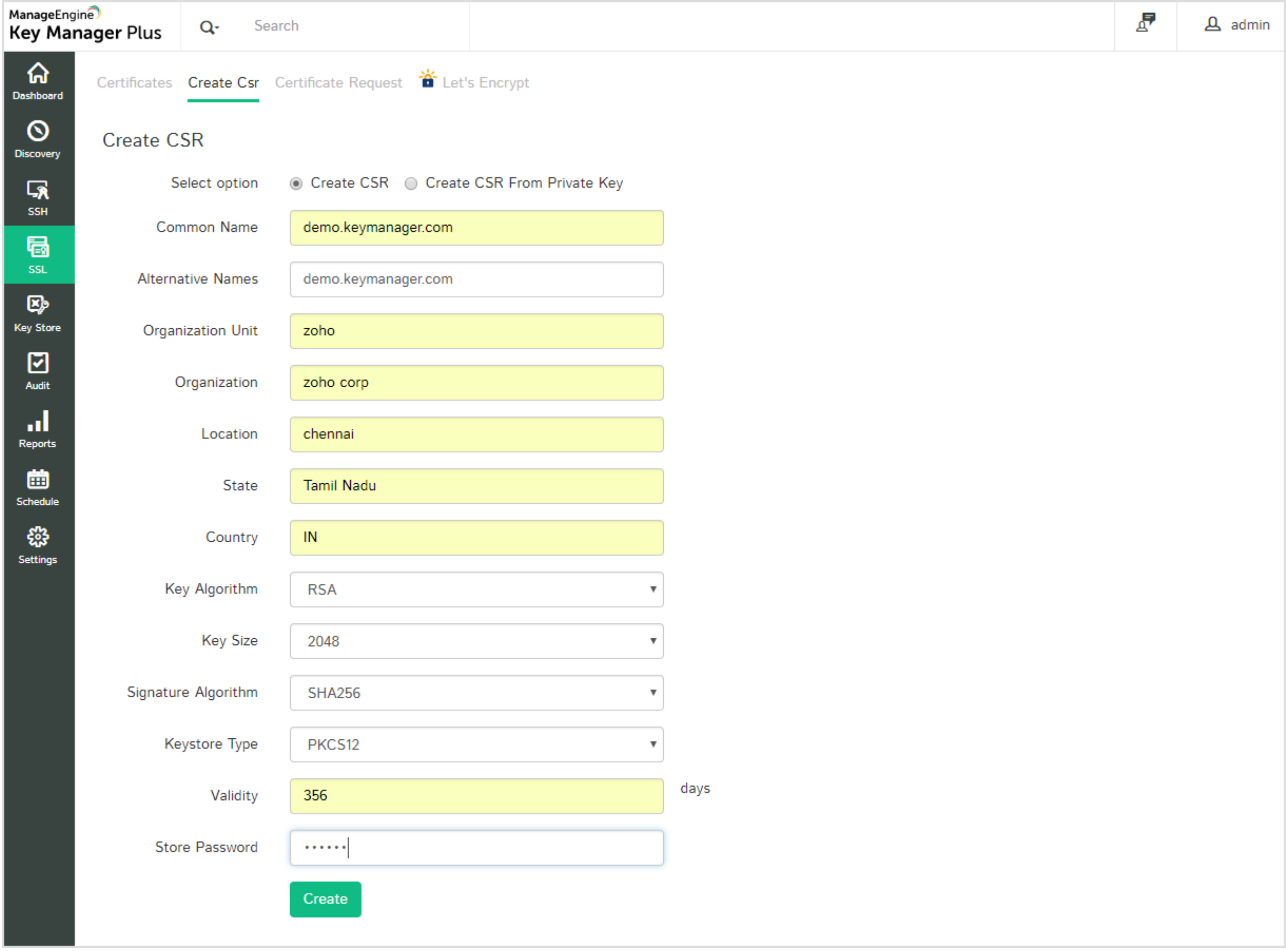
Click here to try your hand at Key Manager Plus live demo

Acquiring Microsoft CA signed certificates and deploying them to IIS

Follow the steps below to request for certificates from Microsoft CA, deploy and manage them in Internet Information Services (IIS) using Key Manager Plus.

Step 1: Generate Certificate Signing Request (CSR)

The first step is generating a Certificate Signing Request (CSR), which is more like a blue print for the certificate you are going to purchase.



Create CSR

Select option	● Create CSR ○ Create CSR From Private Key
Common Name	demo.keymanager.com
Alternative Names	demo.keymanager.com
Organization Unit	zoho
Organization	zoho corp
Location	chennai
State	Tamil Nadu
Country	IN
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	SHA256
Keystore Type	PKCS12
Validity	356 days
Store Password	••••••

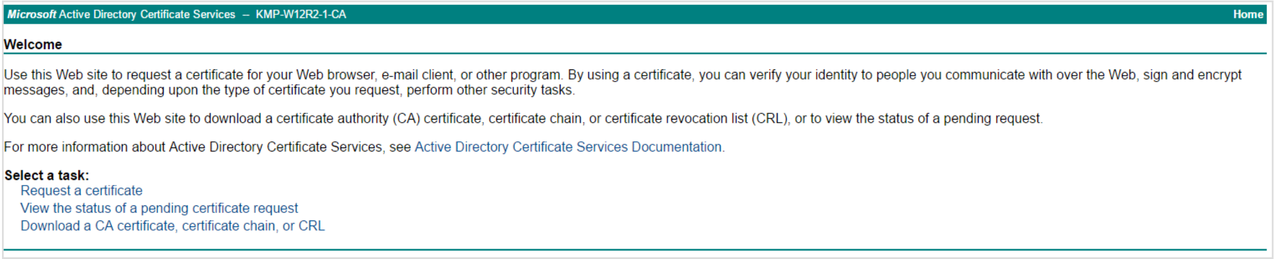
To generate CSR using Key Manager Plus,

- Login to Key Manager Plus and navigate to **SSL-->Create Csr**
- Click **Create**
- In the **Create CSR** form that opens, fill in the required details and click **Create**
- The **CSR** is saved and you can view it from the **SSL-->Create Cs**r tab

Step 2: Request for certificate from Microsoft Certificate Services

After generating CSR, the next step is requesting for certificates from Microsoft Certificate Services. To do this,

- Open Microsoft Active Directory Certificate Services on your server
- In the window that opens, click Request a certificate



Microsoft Active Directory Certificate Services -- KMP-W12R2-1-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

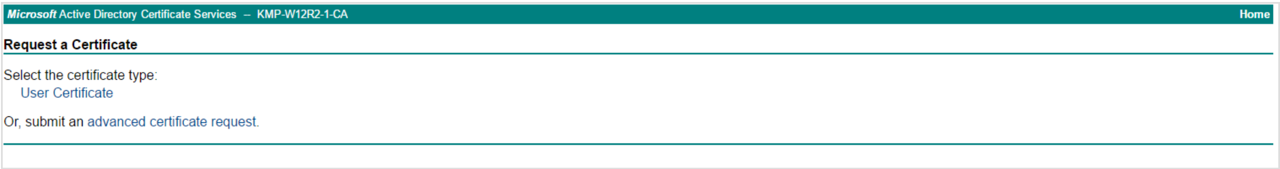
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

- Choose the certificate type as advanced certificate request



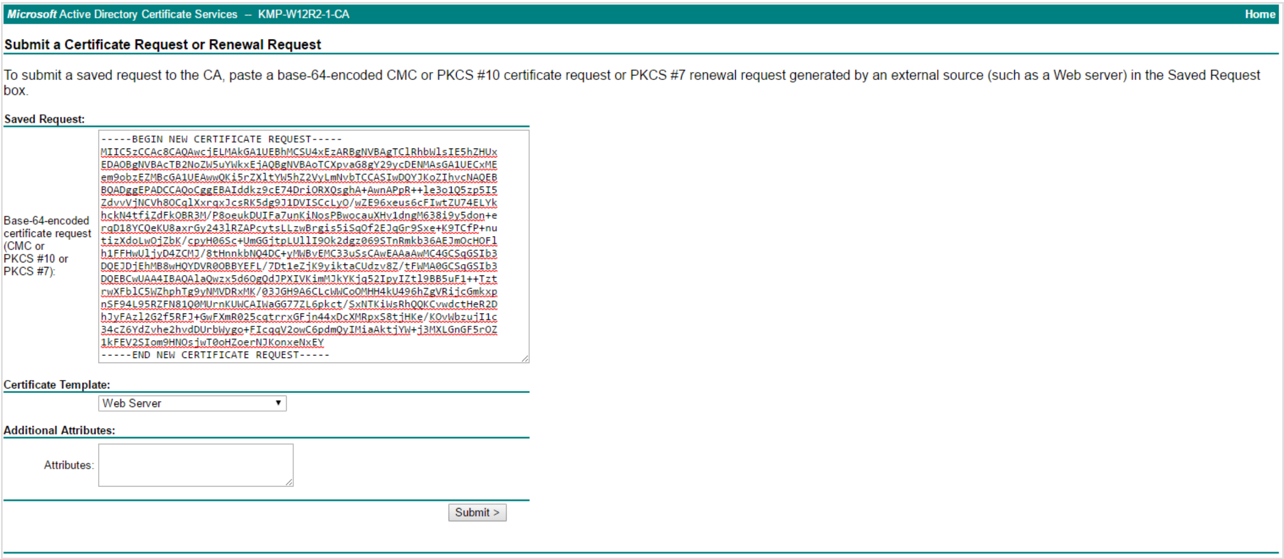
Microsoft Active Directory Certificate Services -- KMP-W12R2-1-CA

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

- You will be redirected to a certificate request window, where you have to paste the CSR generated earlier, and choose the certificate template as web server



Microsoft Active Directory Certificate Services -- KMP-W12R2-1-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC5zCCAc8CAQAwcjELMAkGA1UEBhMCSU4xEzARBgNVBAgTClRhbWlsIE5hZHUx
EDAOBgNVBAcTB2NoZW5uYWkxEjAQBgNVBAoTCXpvaG8gY29ycDENMAsGA1UECxME
em9obzEZMBcGA1UEAwwQKi5rZXltYW5hZ2VyLmNvbTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAIddkz9cE74DriORXQsghA+AwnAPpR++le3o1Q5zp5I5
ZdvvVjNCVh8OCqlXxrqxJcsRK5dg9J1DVISCcLyO/wZE96xeus6cFIwtZU74ELYk
hckN4tfiZdFkOBR3M/P8oeukDUIFa7unKiNosPBwocauXHv1dngM638i9y5don+e
rqD18YCQeKU8axrGy243lRZAPcytsLLzwBrgis5iSqOf2EJqGr9Sxe+K9TCfP+nu
tizXdoLwOjZbK/cpyH06Sc+UmGGjtpLUllI9Ok2dgz069STnRmkb36AEJmOcHOFl
h1FFHwUljyD4ZCMJ/8tHnnkbNQ4DC+yMWBvEMC33uSsCAwEAAaAwMC4GCSqGSIb3
DQEJDjEhMB8wHQYDVR0OBBYEFL/7Dt1eZjK9yiktaCUdzv8Z/tFWMA0GCSqGSIb3
DQEBCwUAA4IBAQAlaQwzx5d6OgQdJPXIVKimMJkYKjq52IpyIZtl9BB5uF1++Tzt
rwXFblC5WZhphTg9yNMVDRxMK/03JGH9A6CLcWWCoOMHH4kU496hZgVRijcGmkxp
nSF94L95RZFN81Q0MUrnKUWCAIWaGG77ZL6pkct/SxNTKiWsRhQQKCvwdctHeR2D
hJyFAzl2G2f5RFJ+GwFXmR025cqtrrxGFjn44xDcXMRpxS8tjHKe/KOvWbzujI1c
34cZ6YdZvhe2hvdDUrbWygo+FIcqqV2owC6pdmQyIMiaAktjYW+j3MXLGnGF5rOZ
1kFEV2SIom9HNOsjwT0oHZoerNJKonxeNxEY
-----END NEW CERTIFICATE REQUEST-----
```

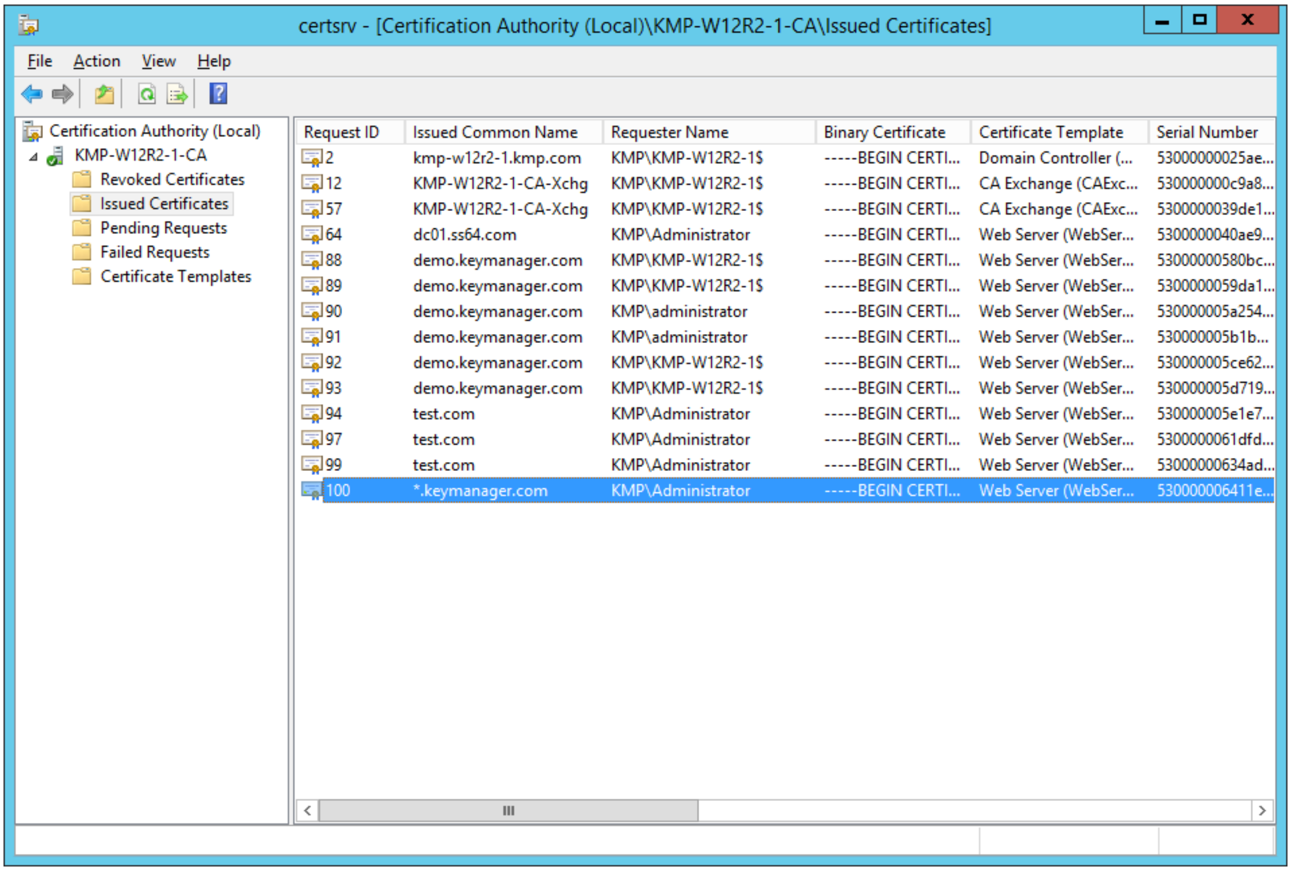
Certificate Template:

Web Server ▼

Additional Attributes:

Attributes:

- The certificate is issued and is present in **Issued Certificates** of **Local CA**



Request ID	Issued Common Name	Requester Name	Binary Certificate	Certificate Template	Serial Number
2	kmp-w12r2-1.kmp.com	KMP\KMP-W12R2-1$	-----BEGIN CERTI...	Domain Controller (...	5300000025ae...
12	KMP-W12R2-1-CA-Xchg	KMP\KMP-W12R2-1$	-----BEGIN CERTI...	CA Exchange (CAExc...	530000000c9a8...
57	KMP-W12R2-1-CA-Xchg	KMP\KMP-W12R2-1$	-----BEGIN CERTI...	CA Exchange (CAExc...	530000039de1...
64	dc01.ss64.com	KMP\Administrator	-----BEGIN CERTI...	Web Server (WebSer...	530000040ae9...
88	demo.keymanager.com	KMP\KMP-W12R2-1$	-----BEGIN CERTI...	Web Server (WebSer...	5300000580bc...
89	demo.keymanager.com	KMP\KMP-W12R2-1$	-----BEGIN CERTI...	Web Server (WebSer...	530000059da1...
90	demo.keymanager.com	KMP\administrator	-----BEGIN CERTI...	Web Server (WebSer...	53000005a254...
91	demo.keymanager.com	KMP\administrator	-----BEGIN CERTI...	Web Server (WebSer...	530000005b1b...
92	demo.keymanager.com	KMP\KMP-W12R2-1$	-----BEGIN CERTI...	Web Server (WebSer...	530000005ce62...
93	demo.keymanager.com	KMP\KMP-W12R2-1$	-----BEGIN CERTI...	Web Server (WebSer...	530000005d719...
94	test.com	KMP\Administrator	-----BEGIN CERTI...	Web Server (WebSer...	530000005e1e7...
97	test.com	KMP\Administrator	-----BEGIN CERTI...	Web Server (WebSer...	5300000061dfd...
99	test.com	KMP\Administrator	-----BEGIN CERTI...	Web Server (WebSer...	5300000634ad...
100	*.keymanager.com	KMP\Administrator	-----BEGIN CERTI...	Web Server (WebSer...	53000006411e...

Step 3: Add the certificate to Key Manager Plus repository

After the certificate has been issued by MS Certificate Authority, you have to import the certificate to Key Manager Plus repository. To do this,

- Navigate to **Discovery --> MS Certificate Store**
- Select the type as **Local Certificate Authority**
- Specify the server name, user name and password of the machine in which the certificate is present
- Click **Discover**
- The certificates issued by **Microsoft Certificate Authority** are discovered and imported into Key Manager Plus certificate repository, which can be viewed from **SSL --> Certificates** tab

  Then follow the steps 2,3 and 4 as mentioned in the previous case to deploy the certificate to your domain server using Key Manager Plus and bind it to the respective website.

Acquiring trusted third party SSL certificates and deploying them to IIS

Step 1: Generate Certificate Signing Request (CSR)

Follow the same procedure as in the previous case

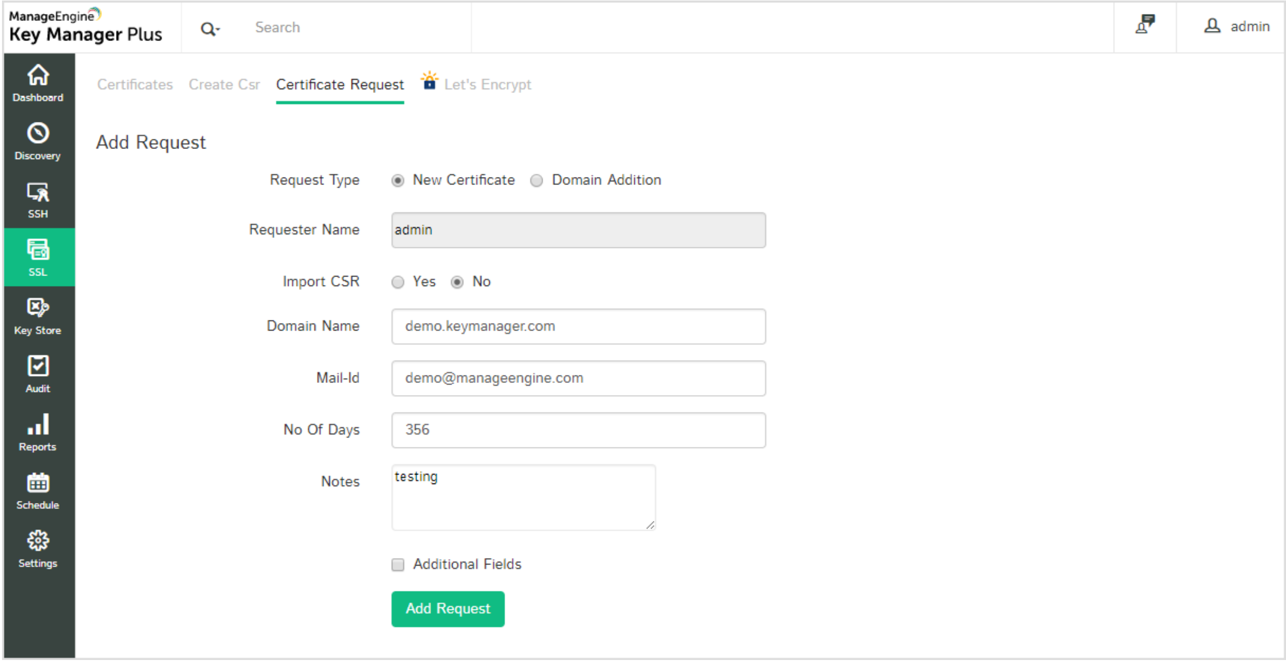
Step 2: Request for certificate from third party CA

After generating CSR, the next step is requesting for certificates from third party CA. This request is usually submitted to the organization administrator or helpdesk, from where it's taken forward to the required Certificate Authority. To raise requests for certificates from Key Manager Plus,

- Navigate **to SSL --> Certificate Request**
- Click on **Add request**
- Select the type of request – **New certificate** or **domain addition**.

  1. New Certificate – Attach a CSR to your request (optional) and a domain name for the new certificate.

  2. Add domain – Enter the name of the new domain and select a parent domain from the certificates added to the Key Manager Plus repository.
- Enter the mail addresses to which you would like to send the request and specify the certificate the validity period. These email addresses can be that of an administrator, an intermediary who handles certificate requests, or even that of your help desk software to raise the certificate request as a ticket.
  For eg., admin@keymanagerplus.com, help-desk@manageengine.com.
- Click **Additional fields** to add additional information such as device name and IP address
- Click the **Add Request** button to add it to the list of requests in the **Certificate Request tab** and to send the same to the specified email addresses.



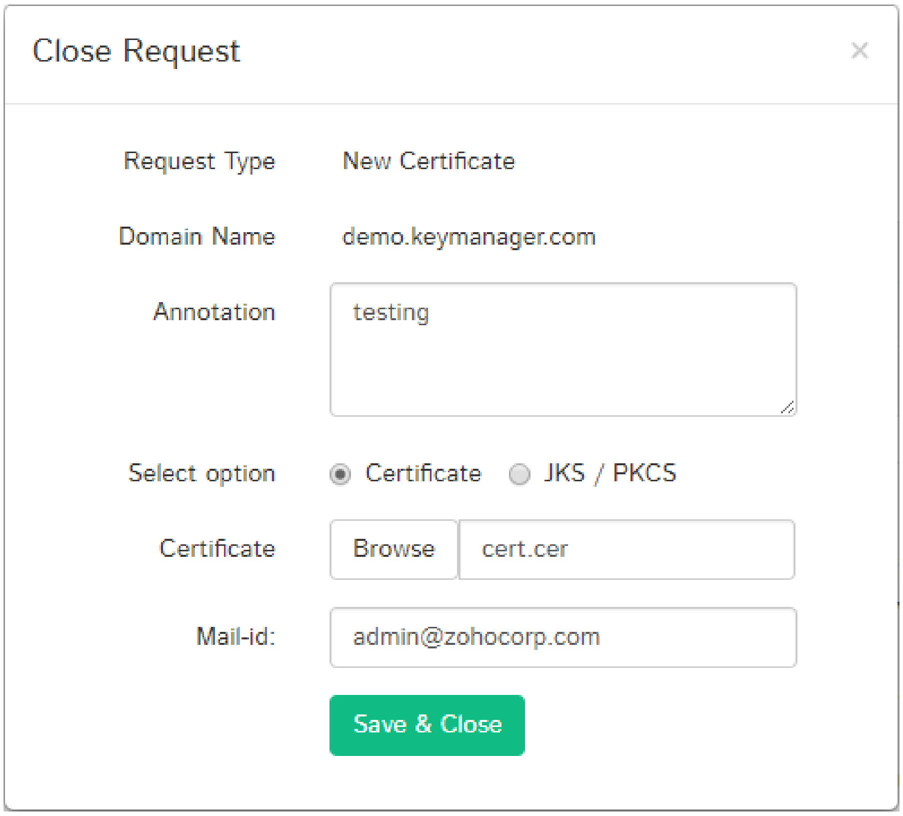
Add Request

Request Type	● New Certificate ○ Domain Addition
Requester Name	admin
Import CSR	○ Yes ● No
Domain Name	demo.keymanager.com
Mail-Id	demo@manageengine.com
No Of Days	356
Notes	testing
	□ Additional Fields
	Add Request

Step 3: Add the certificate to Key Manager Plus repository

The next step is adding the certificate (that has been purchased from external CA through the above certificate request process) to Key Manager Plus centralized certificate repository.

- Navigate to **SSL --> Certificate** Request
- You can see that the request you have raised earlier is in the '**Open**' state. Now click Open and in the pop up that opens, attach the certificate obtained from the third party CA, an annotation if you want and click **Save & Close**.
- The request is closed and at the same time, the certificate is added to the centralized certificate repository
- You can view the certificate by navigating to **SSL --> Certificates** tab
- To keep track of the requests, email is sent to users who raise and close the certificate requests



Close Request

Request Type: New Certificate

Domain Name: demo.keymanager.com

Annotation: testing

Select option: ● Certificate ○ JKS / PKCS

Certificate: cert.cer

Mail-id: admin@zohocorp.com

Then again, follow steps 2,3 and 4 under the first case to deploy the certificate to your domain server using Key Manager Plus and bind it to the respective website.

Go ahead, and give the trial version of Key Manager Plus a shot and write to us for any assistance to keymanagerplus-support@manageengine.com. Click here to download Key Manager Plus.