



- On the screen that appears, give your domain entry a name.  
This will result in a dns record of [myname].[mydomain].[com/net/org]  
Example: mybridge.lockt.com

Enter the IP Address of the bridge

New Host

Name (uses parent domain name if blank):  
mybridge

Fully qualified domain name (FQDN):  
mybridge.lockt.com.

IP address:  
11.22.33.44

Create associated pointer (PTR) record

Allow any authenticated user to update DNS records with the same owner name

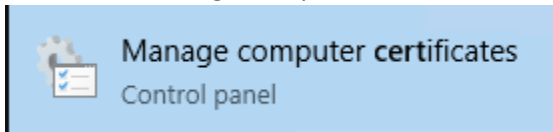
Add Host Cancel

- Click **Add Host**
- You now have a DNS entry created and can access your bridge using:  
https://[mydomain]  
Example: <https://mybridge.lockt.com>

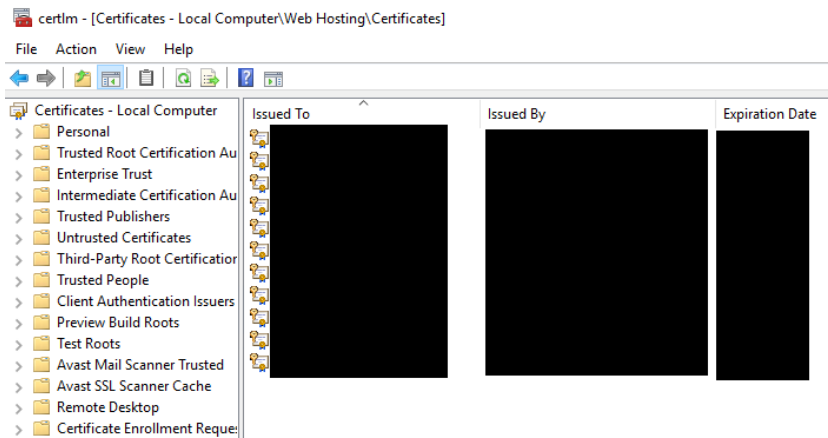
## Exporting your Certificate

To import your certificate into your bridge, you will need a PFX file containing the certificate and private key. The following instructions are for configuring Certificate by exporting it from Microsoft Windows Server certificate store.

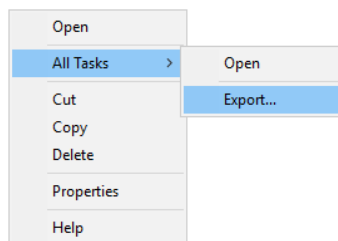
1. Log into the server that contains the certificate for the domain you want to use with your bridge
2. Locate and Manage Computer Certificates



3. In the window that appears, click on the folder containing the certificate you wish to export. Certificates are generally stored in either the **Personal** or **Web Hosting** folders.



4. Right Click on your certificate and select **All Tasks > Export**



5. The Welcome to the Certificate Export Screen will appear. Click **Next**
6. When prompted, select, **“Yes, export the private key”** and Click Next

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

- Yes, export the private key
- No, do not export the private key

- On the Export File Format Screen, select **Personal Information Exchange PKCS #12** and Select these Options and then click Next

### Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
  - Include all certificates in the certification path if possible
  - Delete the private key if the export is successful
  - Export all extended properties
  - Enable certificate privacy
- Microsoft Serialized Certificate Store (.SST)

- On the Security screen, select **Password**. Then, enter a complex password, and select Encryption of **AES256-SHA256** and Click NExt

### Security

To maintain security, you must protect the private key to a security principal or by using a password.

Group or user names (recommended)

Add

Remove

Password:

Confirm password:

Encryption:

- On the File to Export screen, select a place to export your certificate file. It will be exported with a file extension of .PFX. Click Next.

### File to Export

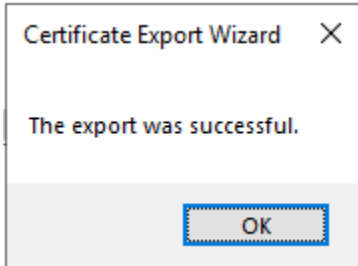
Specify the name of the file you want to export

File name:

C:\Cert\_Export\mycert.pfx

Browse...

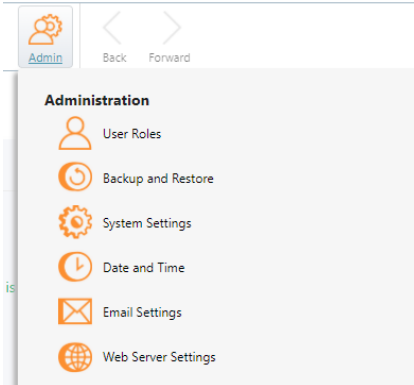
10. You will be taken to the Completing the Certificate Export Wizard window summarizing the activities. Click the Finish button, and you will receive the message that the export was successful.



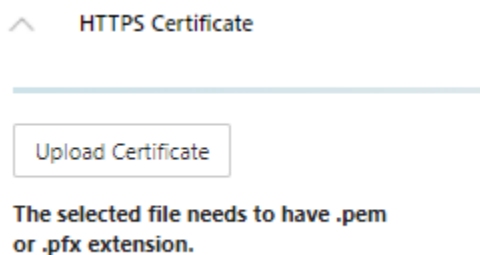
## Importing Your Certificate into Lockt

**Please Note: Do not load an SSL Certificate without first configuring and confirming DNS settings function properly. Doing so may result in the bridge being inaccessible.**

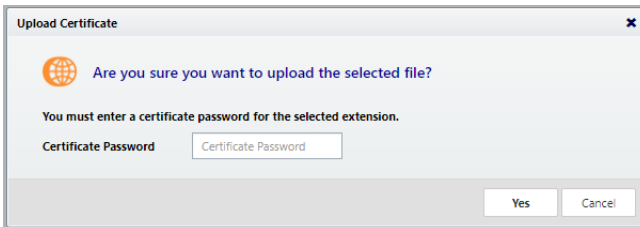
1. Log into Lockt
2. Click Admin > Web Server Settings



3. On the Web Server Settings page, you will see a button to Upload Certificate. Click Upload Certificate.



4. Locate and select the PFX certificate file containing the Certificate and Private Key. Click Open.
5. A window will appear asking you for the password to the certificate. Enter the password and Click Yes



6. Your certificate is now loaded.  
You should be able to access your bridge on your custom DNS name, and your web browser should now indicate the site is fully secure with the lock icon next to the url in your browser:

