IceWarp Unified Communications

The IceWarp SSL Certificate Process

Printed on 4 October, 2010

Contents

CHAPTER 1

The IceWarp SSL Certificate Process

Icewarp is well aware of the complexities that SSL certificate generation and installation provide to administrators and because of this we created this guide to walk you through creating your CSR, choosing the proper IceWarp SSL certificate, and finally installing the signed certificate. All of this can be done without doing most of the necessary steps required by most other vendor's, no merging of intermediate certificates, or worrying whether or not you have the proper root certificate. The guess work is done for you so the whole process is as clear and simple as possible.

In This Chapter

Choosing the Proper Certificate Type

Before generating your CSR you will want to decide what type of certificate suits your specific needs. You will have the option from the following certificate types:

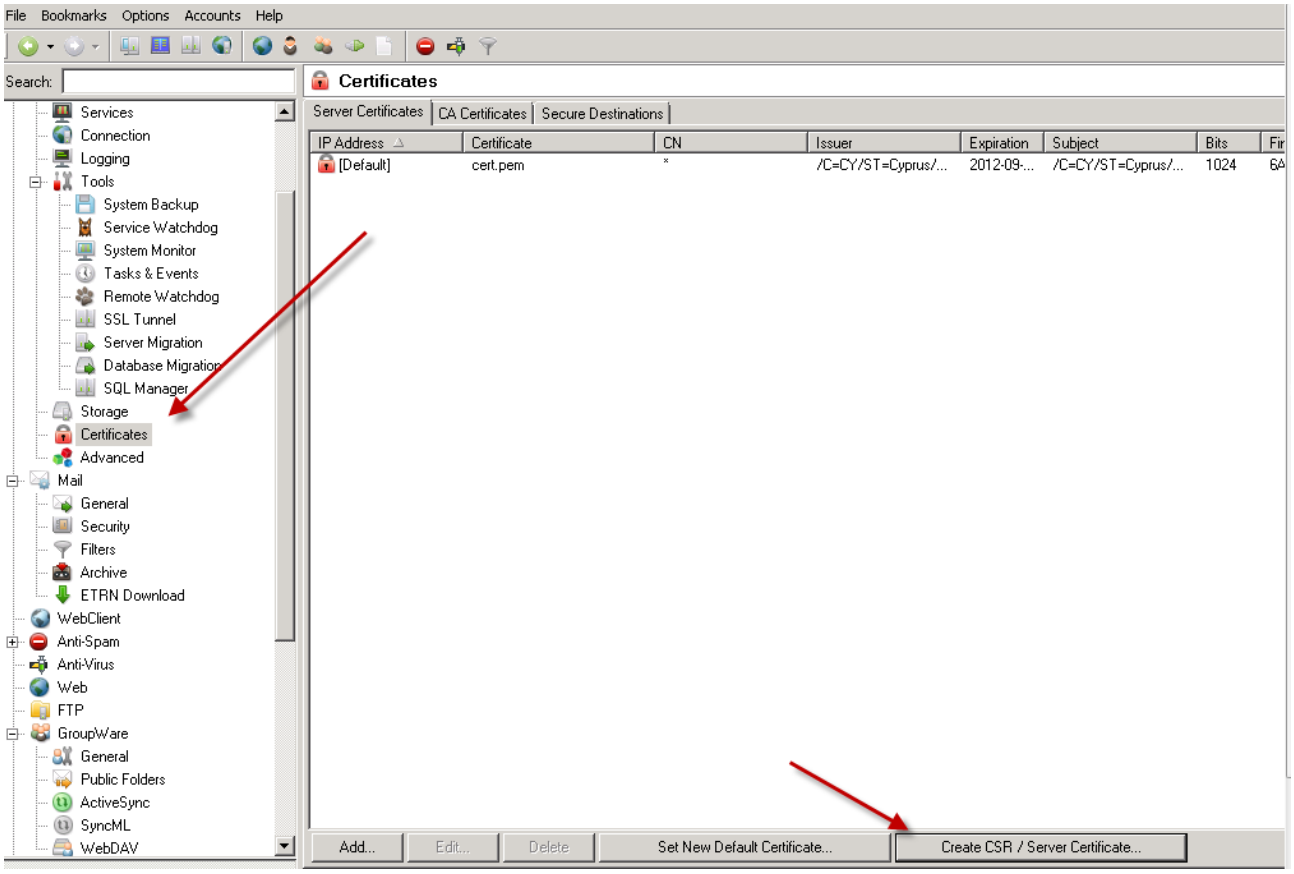
- **Personal Identification (ID)** – This certificate is for personal use and will allow the individual to encrypt their email with any recipient that has the public certificate given by the sender. In order to send encrypted mail the recipient of the message must have the sender's certificate installed so the message can be decrypted.
- **Domain Validation (DV)** – This is the standard SSL certificate used and will allow a company to secure communication for a domain. There are additional options for this type of certificate so a single domain can be secured or a wild card certificate can be issued to provide all sub domains under the primary domain coverage.
  - **Single** – This option will create a certificate for a single domain, eg. Mail.domain.com or domain.com. When choosing this certificate you must know the exact domain name you wish to apply this certificate to. If your hostname is mail.domain.com and the certificate is issued for this domain but you access webmail using "webmail.domain.com" then this would not be covered by the certificate.
  - **Wildcard** – The wildcard certificate will allow you to cover all sub domains relating to the primary domain. For example, if you have domain.com as your primary domain and also want to have mail.domain.com and webmail.domain.com covered under one certificate then choosing a wildcard is the best route.
- **Organizational Validation (OV)** – The organizational certificates go a step further in verifying the identity of the company purchasing the certificate and therefore instead of only showing the domain name on the certificate it will also show the company name in the site seal providing an extra level of security and comfort for the visitors. The same as the Domain Validation certificates there are two options for a single cert and a wildcard certificate, these act in the same manner as described above. This type of certificate requires a higher level of vetting than the domain validation certificate.
- **Extended Validation (EV)** – Extended validation certificates increase the vetting required and thus provide the ultimate level of security to visitors of your site as they will see the "Green Site Seal" and know it is a trust worthy site. The vetting process is much more intense and because of this an EV certificate can only be issued for a maximum term of two years before the certificate is revoked and the process starts again. Below is what you will see in your browser when navigating to an EV protected site.

Creating your CSR (Certificate Signing Request)

In order to generate your SSL certificate to protect your data and communicate securely you first need to generate the CSR. The certificate will be generated based on the information outlined in the CSR. It is very important you ensure the data listed in the CSR is valid and correct so you will have no problems when applying your certificate.

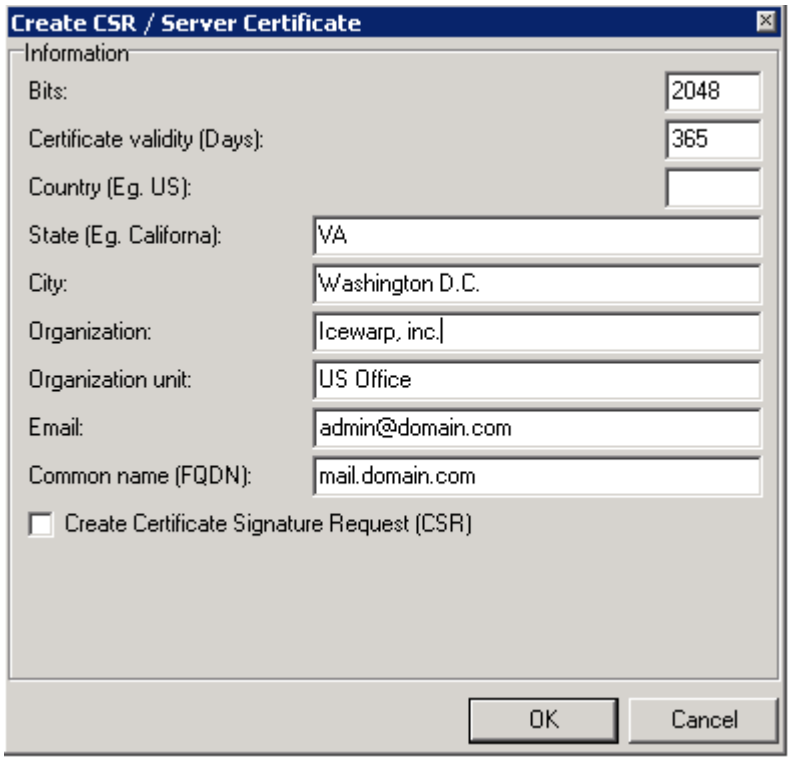
The CSR can be generated using the IceWarp Unified Communications Server with the directions below.

- You first must open the Administration Console directly on the server and navigate to the [Tools, Certificates, Server Certificates] tab.



- Once here you will also see the [Create CSR/Server Certificate] button, press this.

- The certificate creation window will open. You will need to have the required information in order to generate the CSR properly. Each field is explained further below and whether it is a required field.



Bits (***Required***) – What level of encryption will be used for this certificate

Certificate Validity (***Required***) – How long the certificate will be valid

Country (***Optional***) – Use the two letter country code where the office resides

State (***Optional***) – The two letter state code where the company is located

City (***Optional***) – The city where the company is located

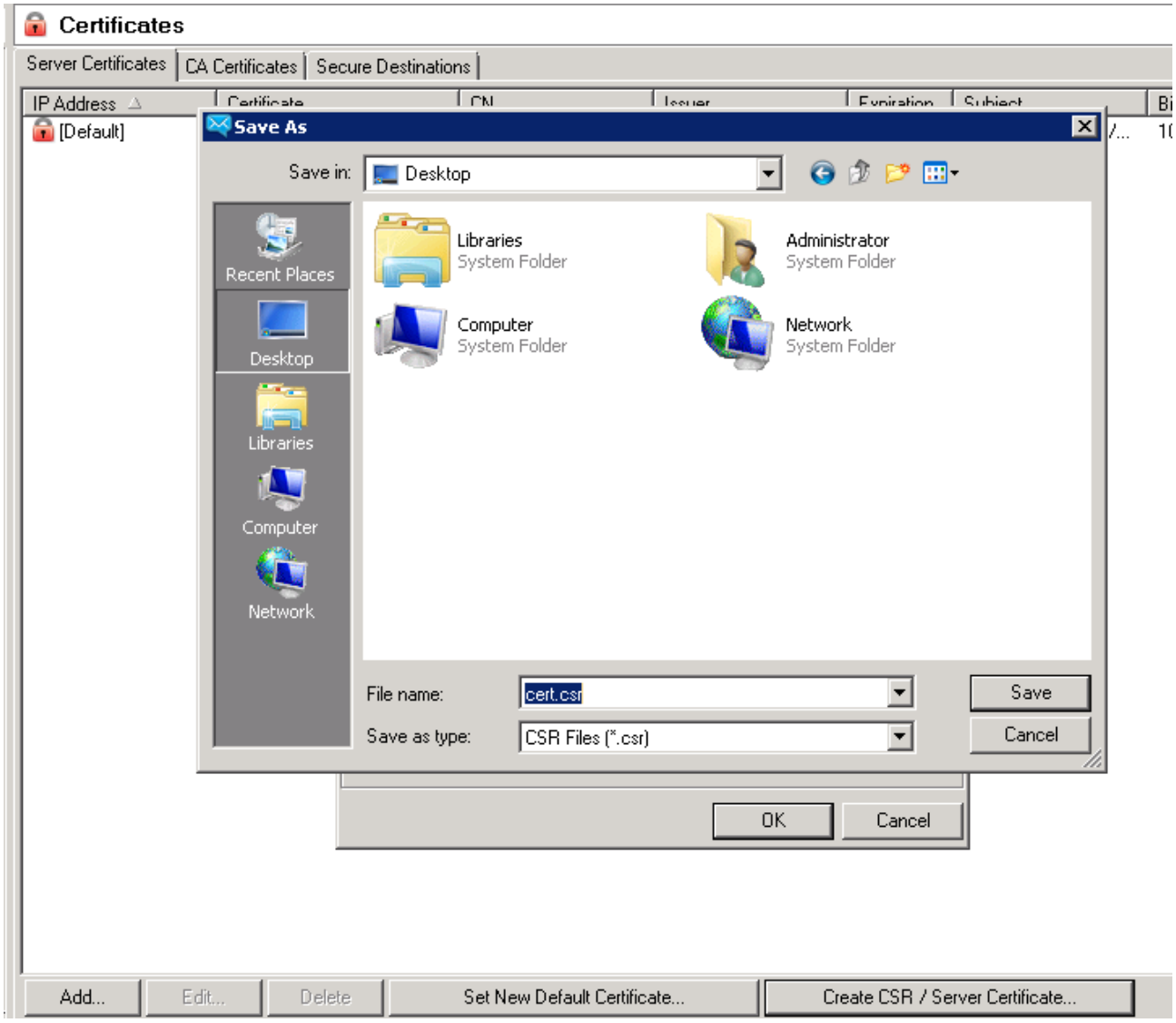
Organization (***Optional***) – The company name

Organizational Unit (***Optional***) – If you have multiple offices it can be good to specify the business unit to keep track of the certificates.

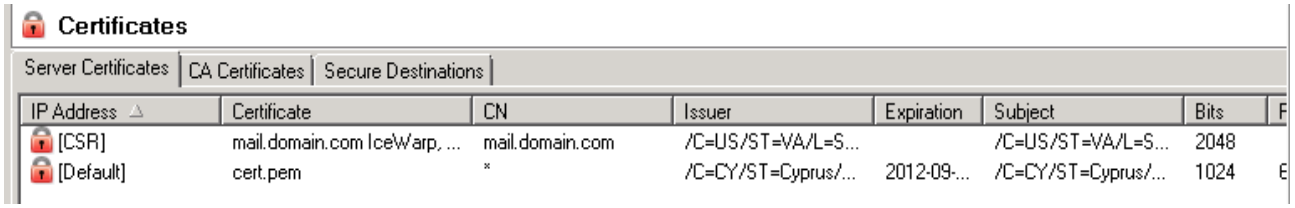
Email (***Optional***) – Normally this is the administrative contact of the company

Common Name (***Required***) – You need to enter the domain name you are wanting to the certificate generated for. If you want to have all services that use the hostname of mail.domain.com covered for SSL then make sure the Common Name is mail.domain.com, if only specifying domain.com then "mail" would not work unless the certificate is a wildcard. If you wish to create a wildcard certificate then use the format of *.domain.com as the common name.

- Lastly you will need to place a check in the box labeled “Create Certificate Signature Request” (CSR). Once you check this box and click “OK” the CSR will be created and you will be prompted to save this to a location of your choosing.

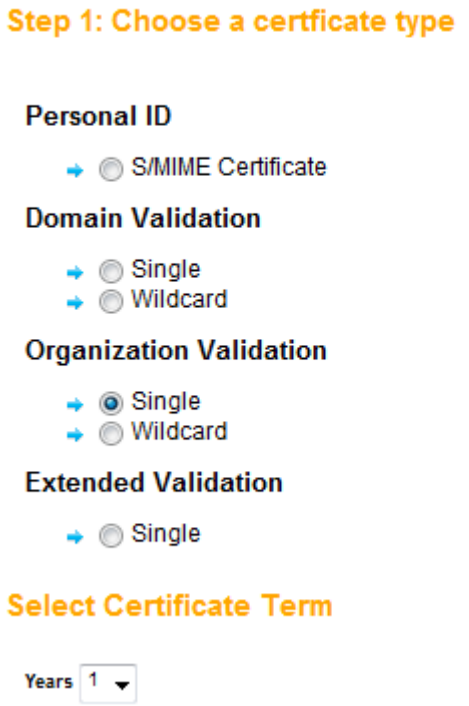


- Now that you have saved your certificate you will see the CSR entered under your [Certificates, Server Certificates] tab.



Purchasing your IceWarp SSL Certificate

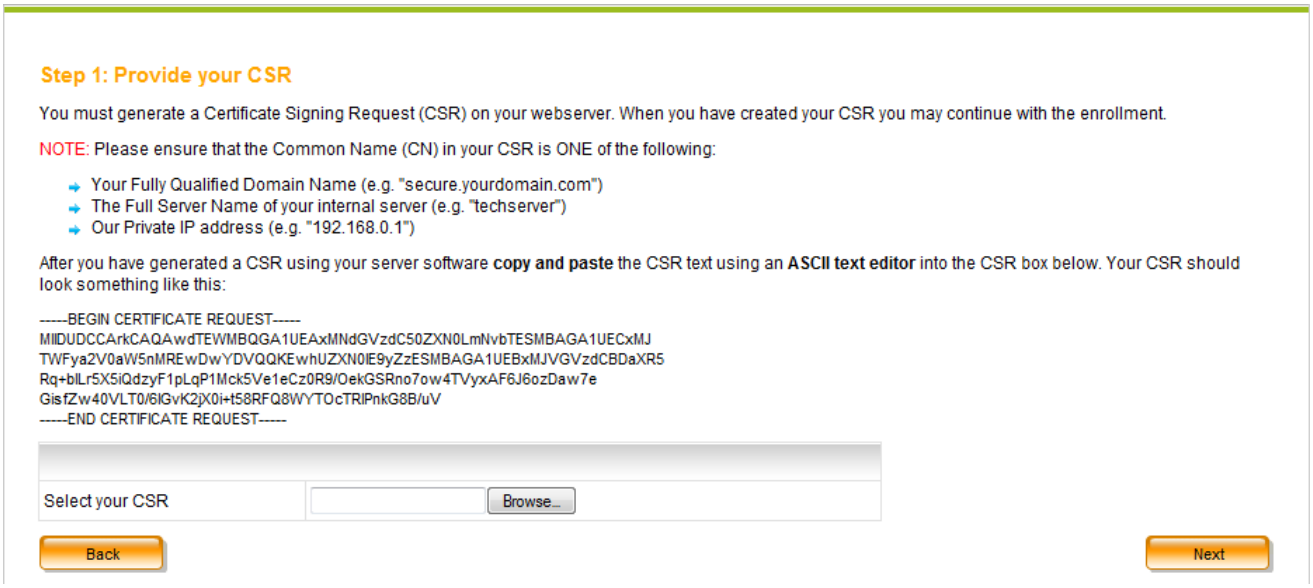
Now that you have the CSR you are ready to start the purchase process of the certificate. You will want to first decide on what type of SSL certificate is right for you. Once you enter the purchase screen you will see the different choices you have. We will explain the differences of each certificate so you know which suits your needs best.



Purchasing your IceWarp SSL Certificate – Continued

Step 1: Now that you have decided what type of certificate you wish to purchase you can proceed with the order. Once you choose the certificate option you can then choose the life cycle of the certificate. Any DV or OV certificate has a maximum life cycle of five years while a EV certificate has two years and a personal certificate only one year.

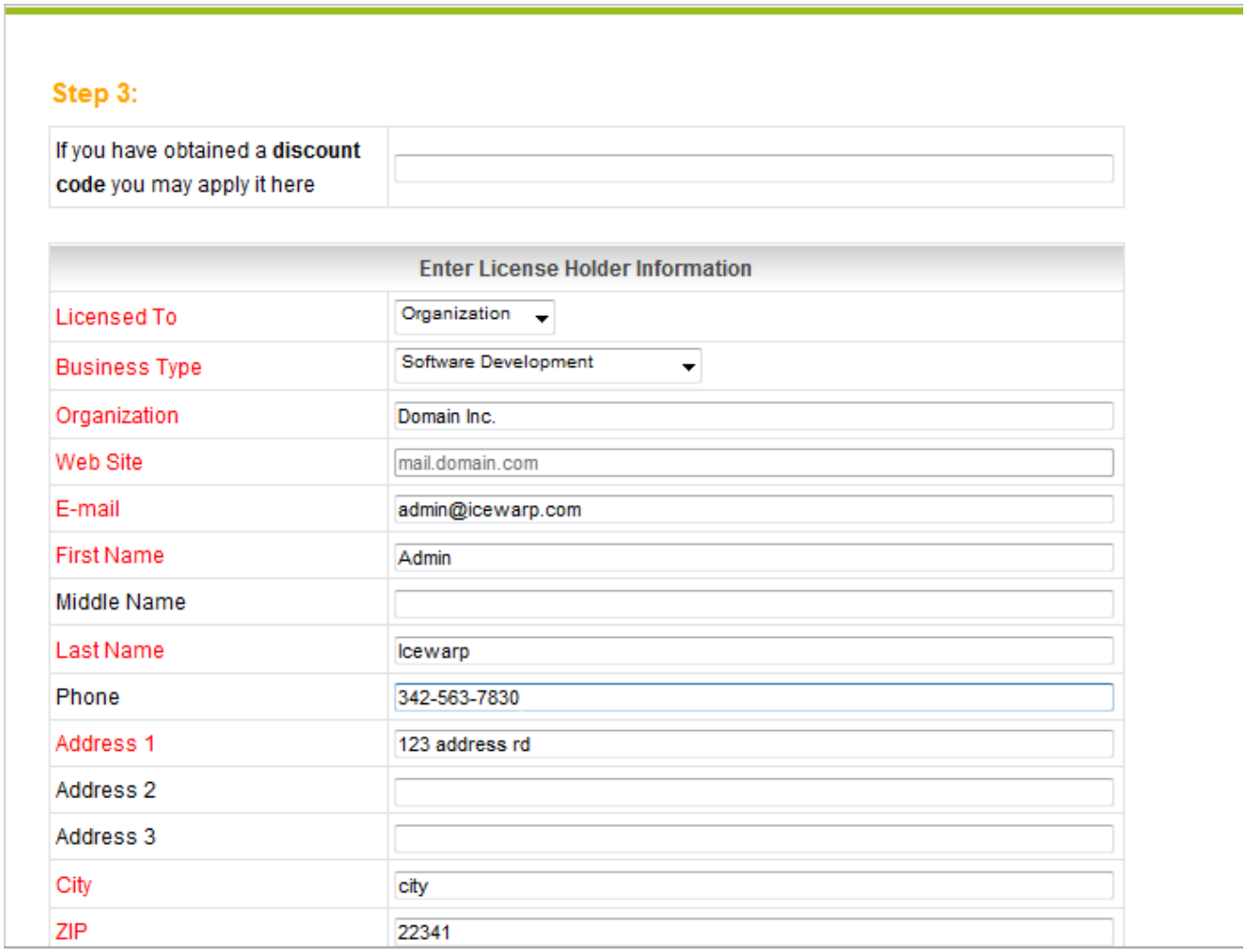
With this chosen you can press [Next] to move on to the next stage of the order.



You will need to upload the CSR file created earlier to proceed. If you have not yet generated the CSR please refer back to the beginning of the document for those directions.

Step 2: After uploading the certificate file you will be asked to pick the email address to send the certificate correspondence to. It will pull the "WHOIS" contact and also display any alternative addresses. The account you choose must be live and able to receive mail in order to process the certificate.

Step 3: Once proceeding to step 3 you will enter the company and contact information. You will be required to enter a challenge password to retrieve the certificate once it has been generated. Be sure to write this password down as you will not be able to collect the certificate without this challenge password.



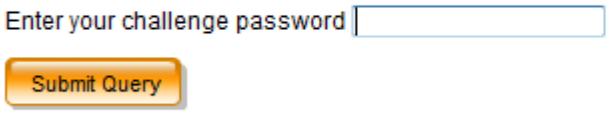
Step 4: This will be a summary view so you can verify all of the specified information and the cost of the certificate being purchased. Ensure all of this is correct before proceeding with placing the order.

Step 5: You will see confirmation of the order being placed. If you chose to pay by check then the details for this will be outlined here as well.

You will now receive the purchase confirmation emails and validation email that will require you to use the validation code inside the email and go to the website specified to validate the certificate; this will need to be done before the certificate can be processed. Once the certificate is generated and ready for collection you will receive a final email with the directions for downloading the certificate. We will now proceed to installing the certificate after you have collected it.

Collecting and Installing Your Certificate

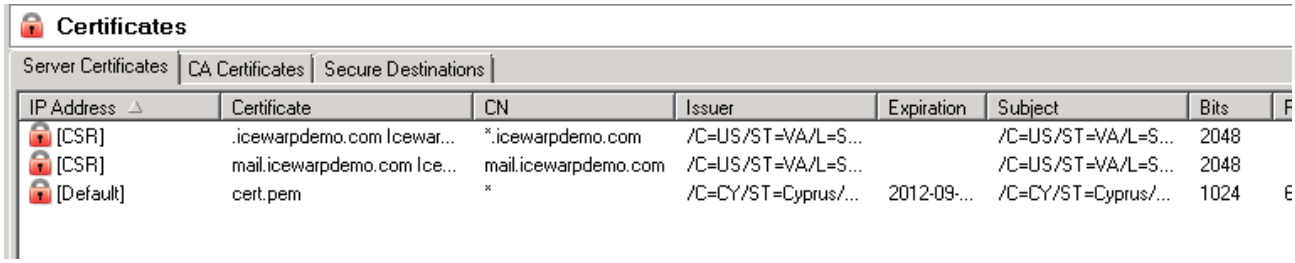
Once you have received the confirmation email telling you the certificate is ready you can download the certificate. You will be prompted to enter your challenge password that you set during the ordering process.



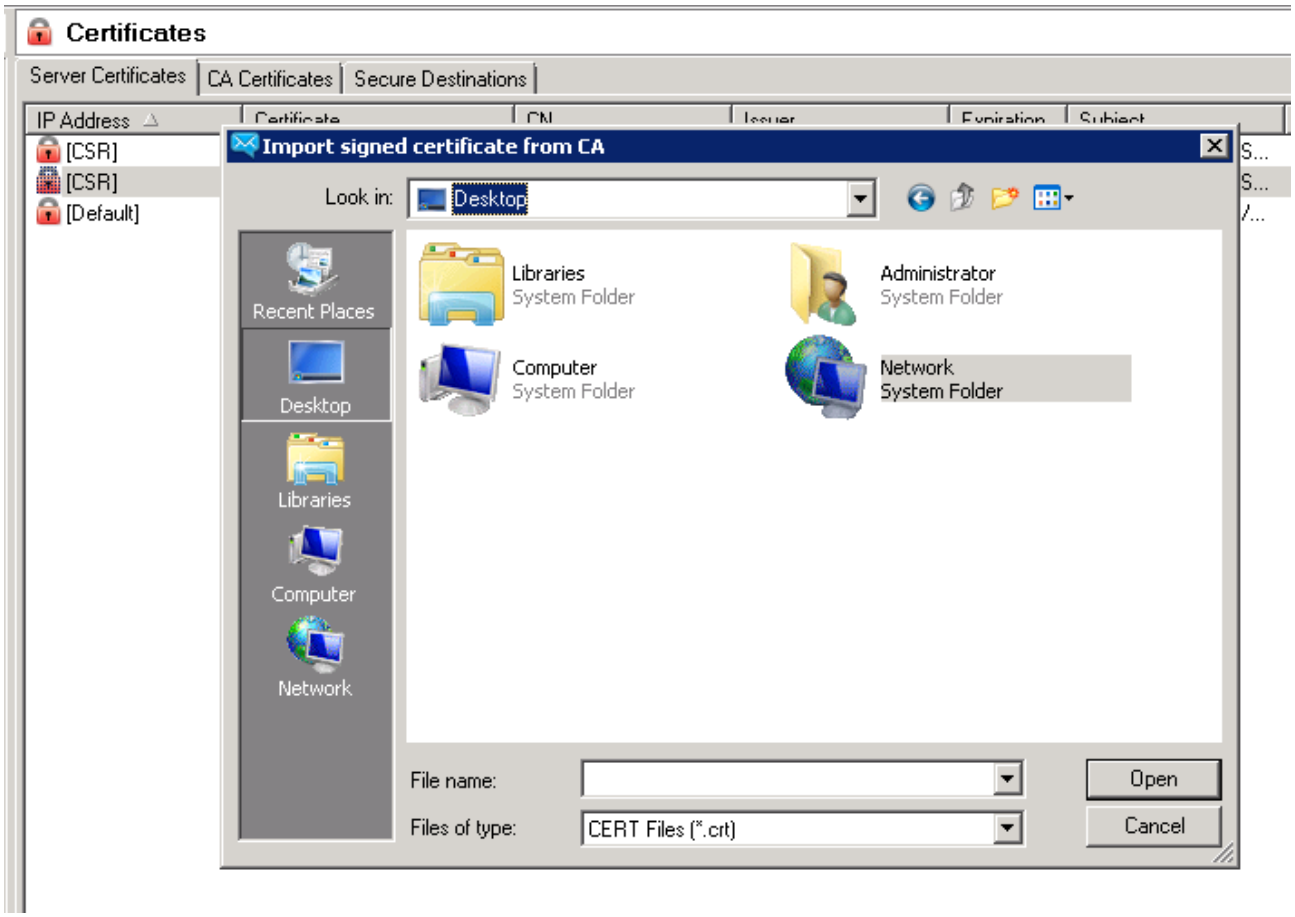
After you have entered the proper challenge password you can download the certificate and begin the installation process.

IceWarp has made the installation process for the certificate very user friendly and automated so there will no longer be any merging or combining of certificates to create a .pem file. This will be done for you using the following directions.

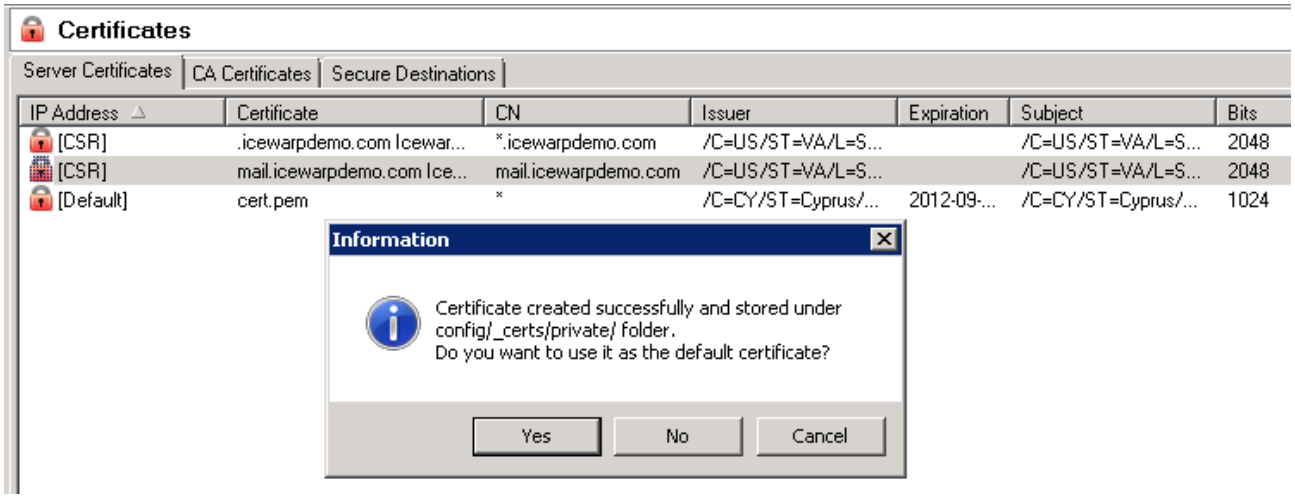
- Connect to the server and open the administration console then navigate to the [Certificates, Server Certificates] tab.



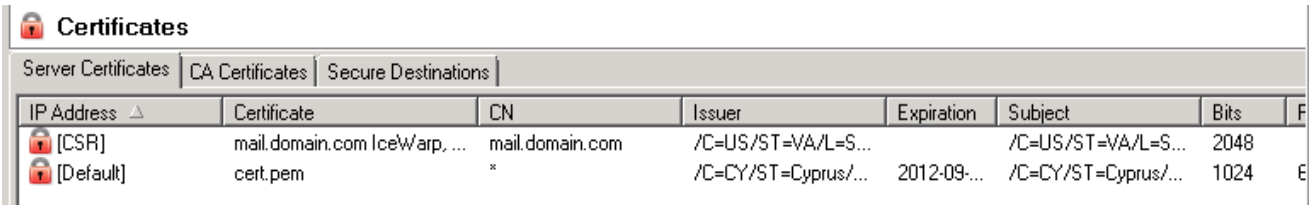
- You will see the entry for the CSR you created earlier. Double Click this CSR entry and you will be prompted to upload the signed certificate file with a .crt extension.



- The server will now automatically combine the private key with the signed certificate and add the certificate entry into the server.



If you wish for the certificate to be the default certificate for the server you can choose this after the import. You will now see the CSR entry removed if choosing for the certificate to be default you will now see the cert.pem default entry updated with your newly imported certificate.

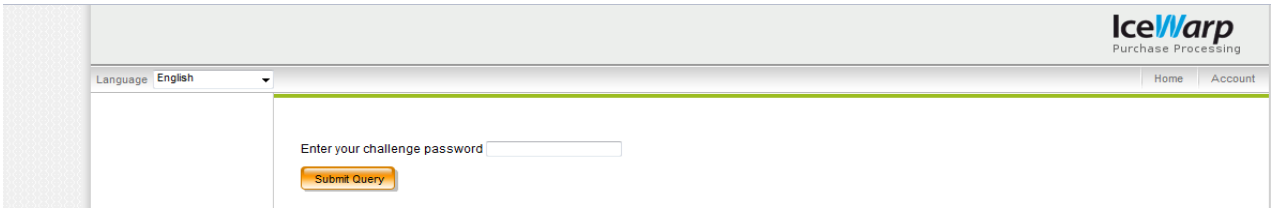


To finish the installation process and apply the certificate to all services you will want to restart the IceWarp services. Once they restart you will be able to utilize the SSL ports for each service depending on the type of certificate generated and the common name used.

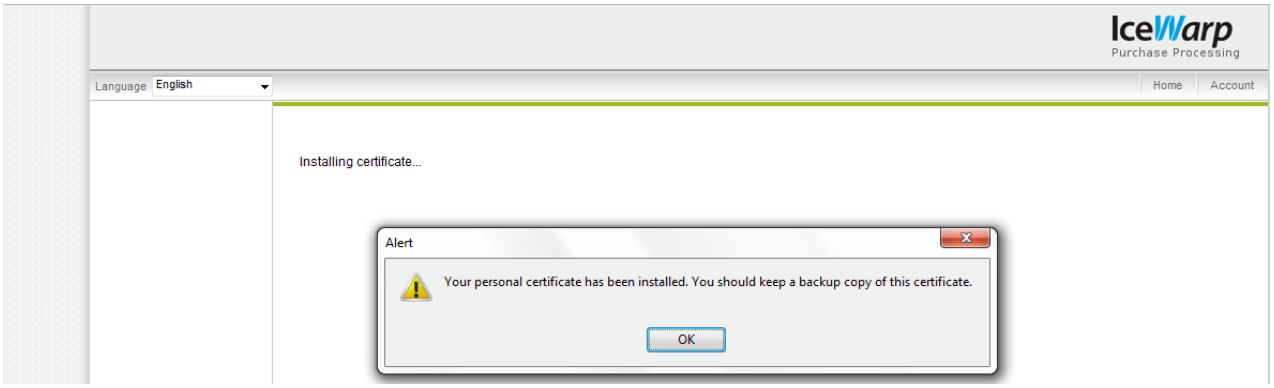
Installing Personal Certificates

The installation of the personal certificate is only a few steps and we will go over these here.

- By this point you should have already received the email alerting you that your certificate is ready to be installed. Once you click on the hyperlink you will be redirected to a secure page and told to enter your challenge password.



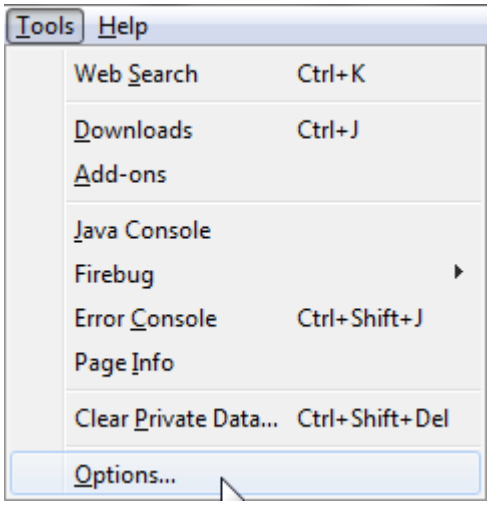
- The certificate will now be automatically installed into the browser you are using.



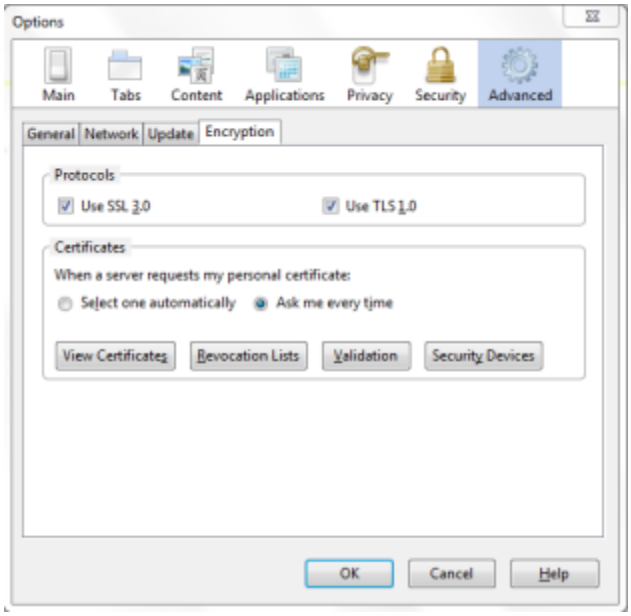
- The certificate now needs to be retrieved from the browser so you can then import this into other email clients, webmail, etc. This will differ depending on the browser being used. We will demonstrate how to retrieve these certificates in Mozilla Firefox 3.x and Internet Explorer 8.

Mozilla Firefox 3.x

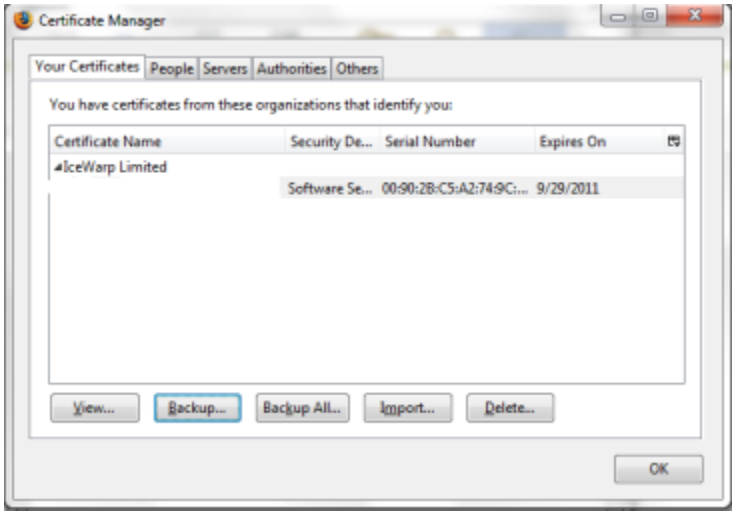
- Open Firefox and go to [Tools, Options]



- Now move to the [Advanced] tab. Here you will see the option “View Certificates”, click this.

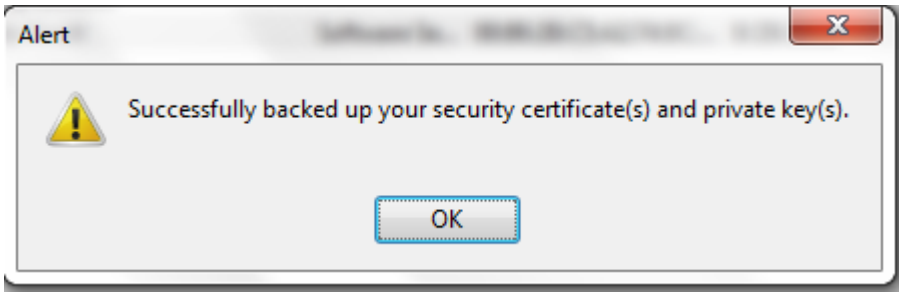


- You will now be in the certificate manager for the browser. You will then want to look for the certificate with the name of "Icewarp Limited" and then highlight this. When the certificate entry is highlighted you will see the option now to "Backup", press this.



- You will now be asked to save the certificate, choose the destination you wish to store the certificate. It will save the certificate in the PKCS12 format so please leave it set to this.
- Once you choose to save the certificate you will be prompted to create a password for this backup file. You must specify a password in order to save the file and then use it later when importing into email clients.

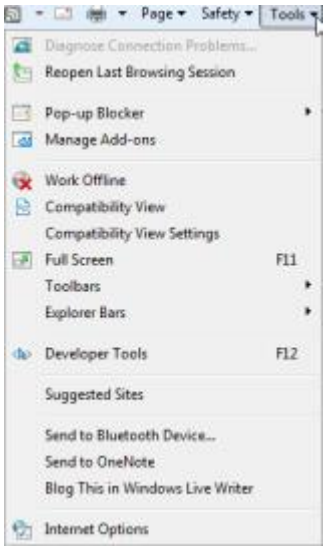
- If everything is correct you will then see the message telling you that the certificate and the private keys have been exported.



- You are now complete with the process using Mozilla and can now use this certificate on most email clients and the Icewarp Webclient.

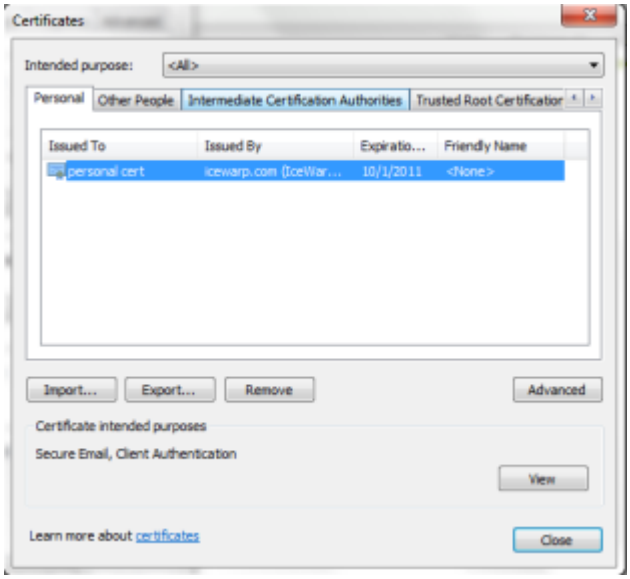
Internet Explorer 8

- Open up Internet Explorer and go to [Tools, Internet Options]

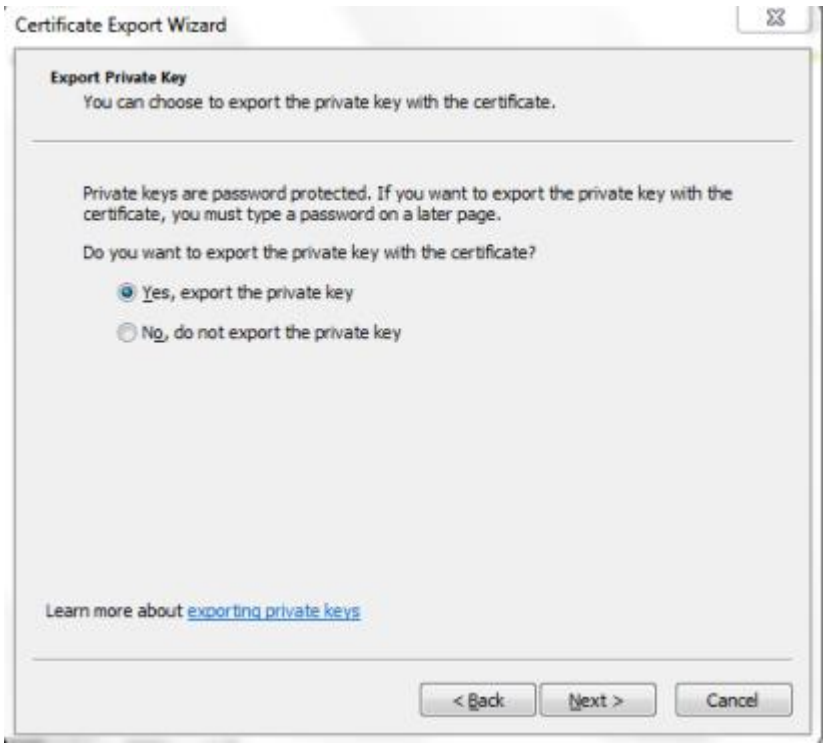


- Now move to the [Content] tab and click on the [Certificates] option.

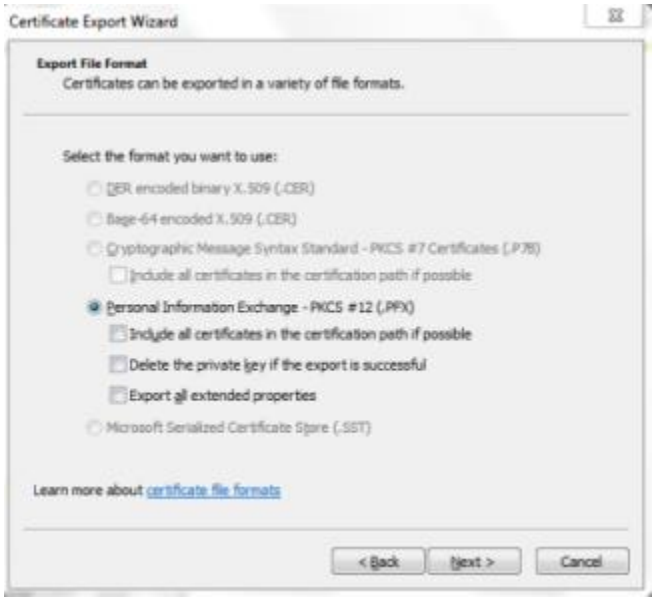
- You should now see the certificate issued to you by “Icewarp.com (Icewarp SMIME Certification Authority)”. Once you highlight this you then choose to “Export” the certificate.



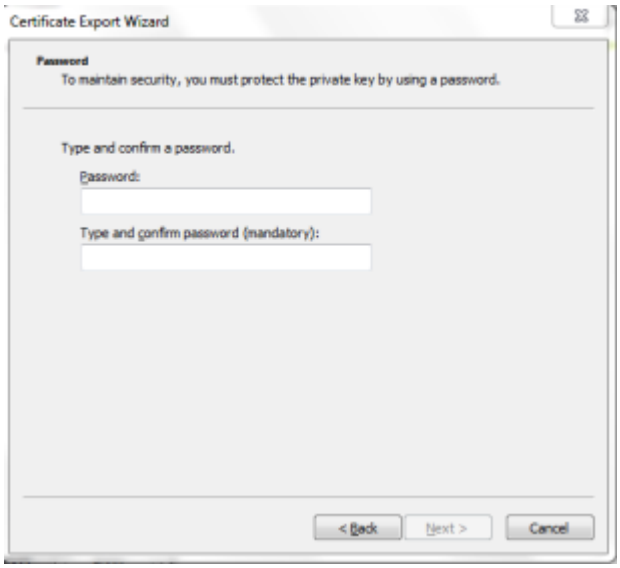
- You will then enter the “Certificate Export Wizard”, just click “Next” to proceed to the next page. Once here you will be asked what you want to export. You have the choice between exporting the certificate with or without the “Private Key”, you will always want to export the certificate with the private key so choose the first option.



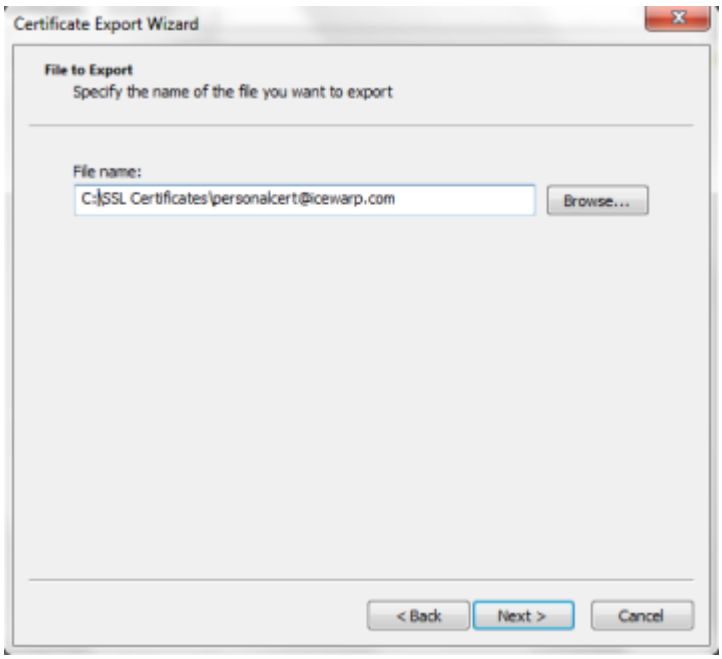
- You will now be presented options for the format to export the certificate in and other options to export with. You will be exporting the certificate in the PKCS12 (.PFX) format. You will not be exporting with any other options so leave all three choices blank.



- You will now be prompted to specify a password to protect this file. You must choose a password before you can export the certificate. You should write this password down in the event you need to reinstall the certificate in another location or client.



- Lastly, you will be prompted for the file name and where to export the certificate to. You do not need to specify the file extension as it will already save in the .pfx format when saving so just browse to the location you wish to save the certificate to and choose the file name.

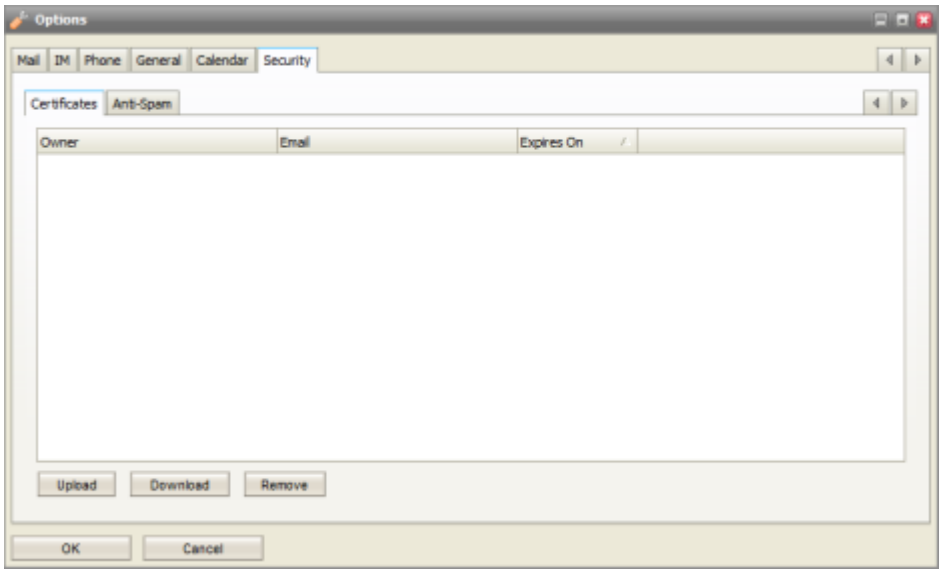


- The wizard will now give you a summary of where the certificate is being saved, what format, and whether or not you are exporting the private key. If this information is correct then click “Finish” and if saved then you will see the notification stating the “The Export Was Successful”. You are now ready to import and use the certificate.

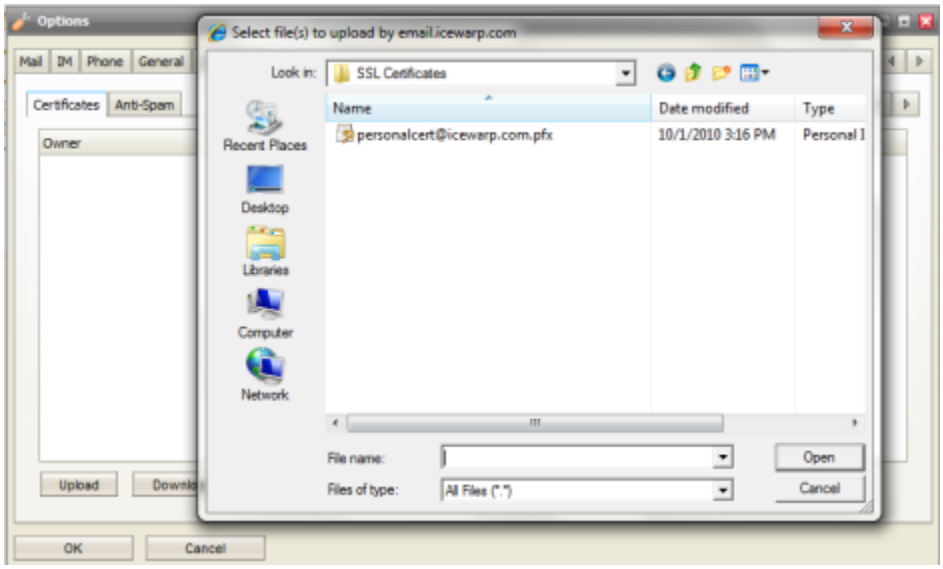
Importing Your Certificate into the IceWarp WebClient

Now that you have the certificate downloaded you can upload this into the Webclient and start using it immediately. We are only showing the steps to import the certificate into the Icewarp Webclient as there are many tutorials and resources showing how to do this for Outlook and other Email Clients.

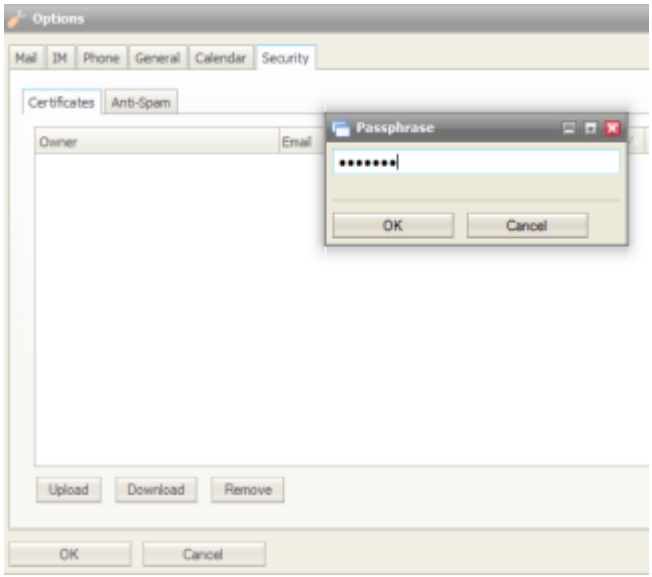
- You first need to open a browser and login to your Icewarp Webclient account. Once there go to the [Tools, Options, Security] tab.



- Now click the "Upload" button so you can upload your certificate. Just browse to the location of your certificate.



- You will now be prompted to enter the password you specified when exporting the certificate. Enter the password and click “OK”



- As long as the password was correct the certificate will be imported and you will now see this listed in the Webclient.

You are now ready to sign your email being sent from the Webclient. By signing your email you are sending your public key for this certificate to all recipients. If you and any recipient exchange keys then you will be able to encrypt all mail being sent between you. You can only encrypt mail to recipients who have your public key so the message can be decrypted and read.

Summary

Following the steps outlined in this guide you should have easily created your CSR, chosen the right certificate for your needs, ordered this certificate, and finally installed the server or personal certificate. From this point forward all communication can be secured and encrypted to prevent any eavesdropping.

If you have any problems or questions about this please contact mailto:support@icewarp.com.