Installing an SSL certificate on the InfoVaultz Cloud Appliance

This document reviews the prerequisites and installation of an SSL certificate for the InfoVaultz Cloud Appliance.

Please note that the installation of the SSL certificate will require an interruption in service as well as port forwarding rules to be edited to point to port :443 instead of port :80. Any users who are using the InfoVaultz will be required to redirect to port :443 in their apps and will be required to use https:// prefix

About SSL Certificates

A SSL certificate is a way to encrypt a site's information and create a more secure connection. Additionally, the certificate can show the virtual private server's identification information to site visitors. Certificate Authorities can issue SSL certificates that verify the server's details while a self-signed certificate has no 3rd party corroboration.

There are two different methodologies to activate SSL service on the InfoVaultz:

- Self-Signed SSL
- 3rd party Certificate Authority (Ensure that when purchasing certificates for the InfoVaultz that they are specifically generated for an apache2 instance)

Self-Signed SSL certificate instructions:

Login to the InfoVaultz using SSH and type:

```
sudo a2enmod ssl

sudo service apache2 restart
```

Create a new certificate by typing the command:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/apache.key -out /etc
/ssl/apache.crt
```

With this command, we will be both creating the self-signed SSL certificate and the server key that protects it, and placing both of them into the new directory.

This command will prompt terminal to display a lists of fields that need to be filled in.

The most important line is "Common Name". Enter your official domain name here or, if you don't have one yet, your site's IP address.

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:NYC
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Awesome Inc
Organizational Unit Name (eg, section) []:Dept of Merriment
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:webmaster@awesomeinc.com
```

Now we have all of the required components of the finished certificate. The next thing to do is to set up the virtual hosts to display the new certificate.

Open up the SSL config file:

```
sudo nano /etc/apache2/sites-available/default
```

You should make the following changes.

Change the port on the virtual host to 443, the default SSL port:

```
<VirtualHost *:443>
```

Add a line with your server name right below the Server Admin email:

```
ServerName example.com:443
```

Replace example.com with your DNS approved domain name or server IP address (it should be the same as the common name on the certificate).

Add in the following three lines to the end of your virtual host configuration, and make sure that they match the extensions below:

```
SSLEngine on

SSLCertificateFile /etc/ssl/apache.crt

SSLCertificateKeyFile /etc/ssl/apache.key
```

Save and Exit out of the file.

Before the website that will come on the 443 port can be activated, we need to enable that Virtual Host:

```
sudo a2ensite default
```

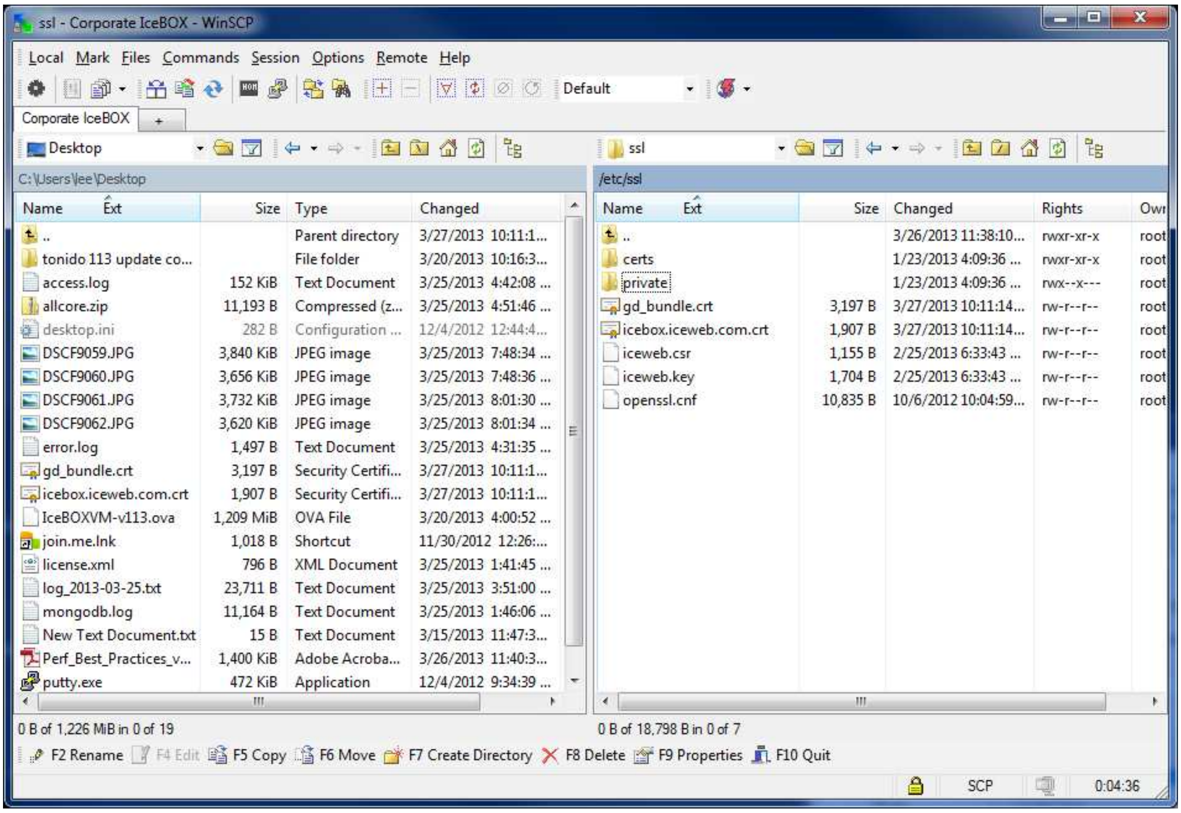
You are all set. Restarting your Apache server will reload it with all of your changes in place.

```
sudo service apache2 reload
```

In your browser, type **https://youraddress**, and you will be able to see the new certificate.

3rd party Certificate Authority instructions:

Ensure that when purchasing certificates for the InfoVaultz that they are specifically generated for an apache2 instance. Copy certificates purchased from domain registrar into /etc/ssl using WinSCP (Secure Copy Protocol) or the like:



C:\Users\lee\Desktop

Name	Ext	Size	Type	Changed
..			Parent directory	3/27/2013 10:11:1...
tonido 113 update co...			File folder	3/20/2013 10:16:3...
access.log		152 KiB	Text Document	3/25/2013 4:42:08 ...
allcore.zip		11,193 B	Compressed (z...	3/25/2013 4:51:46 ...
desktop.ini		282 B	Configuration ...	12/4/2012 12:44:4...
DSCF9059.JPG		3,840 KiB	JPEG image	3/25/2013 7:48:34 ...
DSCF9060.JPG		3,656 KiB	JPEG image	3/25/2013 7:48:36 ...
DSCF9061.JPG		3,732 KiB	JPEG image	3/25/2013 8:01:30 ...
DSCF9062.JPG		3,620 KiB	JPEG image	3/25/2013 8:01:34 ...
error.log		1,497 B	Text Document	3/25/2013 4:31:35 ...
gd_bundle.crt		3,197 B	Security Certifi...	3/27/2013 10:11:1...
icebox.iceweb.com.crt		1,907 B	Security Certifi...	3/27/2013 10:11:1...
IceBOXVM-v113.ova		1,209 MiB	OVA File	3/20/2013 4:00:52 ...
join.me.lnk		1,018 B	Shortcut	11/30/2012 12:26:...
license.xml		796 B	XML Document	3/25/2013 1:41:45 ...
log_2013-03-25.txt		23,711 B	Text Document	3/25/2013 3:51:00 ...
mongodb.log		11,164 B	Text Document	3/25/2013 1:46:06 ...
New Text Document.txt		15 B	Text Document	3/15/2013 11:47:3...
Perf_Best_Practices_v...		1,400 KiB	Adobe Acroba...	3/26/2013 11:40:3...
putty.exe		472 KiB	Application	12/4/2012 9:34:39 ...

0 B of 1,226 MiB in 0 of 19

/etc/ssl

Name	Ext	Size	Changed	Rights	Owi
..			3/26/2013 11:38:10...	rwxr-xr-x	root
certs			1/23/2013 4:09:36 ...	rwxr-xr-x	root
private			1/23/2013 4:09:36 ...	rwx--x---	root
gd_bundle.crt		3,197 B	3/27/2013 10:11:14...	rw-r--r--	root
icebox.iceweb.com.crt		1,907 B	3/27/2013 10:11:14...	rw-r--r--	root
iceweb.csr		1,155 B	2/25/2013 6:33:43 ...	rw-r--r--	root
iceweb.key		1,704 B	2/25/2013 6:33:43 ...	rw-r--r--	root
openssl.cnf		10,835 B	10/6/2012 10:04:59...	rw-r--r--	root

0 B of 18,798 B in 0 of 7

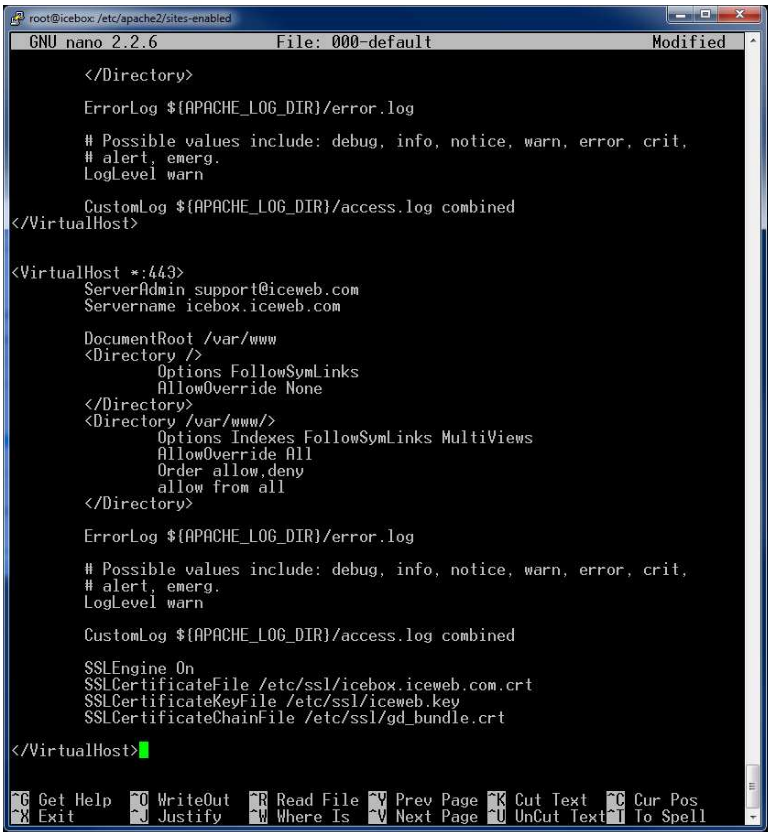
Edit the /etc/apache2/sites-enabled/000-default file by adding the following lines to the file below its current contents:

```
<VirtualHost *:443>
        ServerAdmin support@iceweb.com
        Servername <FQDN goes here>

        DocumentRoot /var/www
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride All
                Order allow,deny
                allow from all
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log

        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn

        CustomLog ${APACHE_LOG_DIR}/access.log combined

        SSLEngine On
        SSLCertificateFile /etc/ssl/InfoVaultz.com.crt
        SSLCertificateKeyFile /etc/ssl/InfoVaultz.key
        SSLCertificateChainFile /etc/ssl/InfoVaultz_bundle.crt


</VirtualHost>
```

Once added edit the bottom section of the added text to reflect the proper file names:

```
       SSLCertificateFile /etc/ssl/InfoVaultz.com.crt
        SSLCertificateKeyFile /etc/ssl/InfoVaultz.key
        SSLCertificateChainFile /etc/ssl/InfoVaultz_bundle.crt
```

This will change depending on filenames of the SSL certificate file, key file, and chain file.



```
  GNU nano 2.2.6              File: 000-default                       Modified

        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log

        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn

        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>


<VirtualHost *:443>
        ServerAdmin support@iceweb.com
        Servername icebox.iceweb.com

        DocumentRoot /var/www
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride All
                Order allow,deny
                allow from all
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log

        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn

        CustomLog ${APACHE_LOG_DIR}/access.log combined

        SSLEngine On
        SSLCertificateFile /etc/ssl/icebox.iceweb.com.crt
        SSLCertificateKeyFile /etc/ssl/iceweb.key
        SSLCertificateChainFile /etc/ssl/gd_bundle.crt

</VirtualHost>
```

Before the website that will come on the 443 port can be activated, we need to enable that Virtual Host:

```
sudo a2ensite default
```

You are all set. Restarting your Apache server will reload it with all of your changes in place.

```
sudo service apache2 reload
```

In your browser, type **https://youraddress**, and you will be able to see the new certificate.