Create a new certificate for a vSphere HTML5 Web Client Fling

This document explains list of steps required to:

i) Generate a VMCA (VMware Certificate Authority) issued SSL certificate specific for vSphere Client (HTML5),
ii) Create a solution user in VECS (VMware Endpoint Certificate Store) for the vSphere Client (HTML5)
iii) Connect the vSphere Client (HTML5) to PSC (Platform Services Controller).

NOTE:

- Tested on v1.12 (4059162) of the fling, should work on any versions above 1.12.
- These commands are tested for 6.0 GA, U1, U2 and 6.5 vCenter. Tested on both VCSA (both embedded and external PSC) and Windows VC (only embedded PSC)
- Replace these strings with appropriate values in the commands:
  IP_ADDRESS_OF_HTML5_APPLIANCE, PSC_NODE_PASSWORD, PSC_HOSTNAME/FQDN, VC_IP_ADDRESS
- Location where the commands have to be run is shown in the [] before the command:
  - `[h5client-appliance] to be run the HTML5 web client appliance.`
  - `[psc] to be run on the PSC node for external PSC`
  - `[VC] to be run on the VC node, applicable in case of embedded PSC as VC and PSC sit in the same node`

Instructions:

I. Deploy the vSphere HTML5 web client appliance and power on the VM. Set the hostname for the vSphere HTML5 web client appliance by running below command from a SSH connection to the appliance. Using h5client-01a as a sample hostname in the document.

```
[h5client-appliance]# hostname h5client-01a
```

II. On ControlCenter (or your DHCP server), create the DNS record for the new appliance. Using `'controlcenter.corp.local, corp.local'` as examples, please change as appropriate :

```
PS> Add-DnsServerResourceRecordA --ComputerName 'controlcenter.corp.local' --ZoneName 'corp.local' --name 'h5client-01a' --IPv4Address <IP_ADDRESS_OF_HTML5_APPLIANCE> --CreatePtr
```

Alternatively, if you access your vSphere HTML5 web client from a single (or small subset) of machines, you can add entry to the hosts file of those machines.

For VCSA with Embedded PSC appliance

1. **SSH to the VC node and run below commands**

Aliases to save typing

```
[VC]# alias vecs-cli='/usr/lib/vmware-vmafd/bin/vecs-cli'
[VC]# alias dir-cli='/usr/lib/vmware-vmafd/bin/dir-cli'
[VC]# alias certool='/usr/lib/vmware-vmca/bin/certool'
```

NOTE: If you want to user your own certificates or any other 3rd party generated certificates rather than using VMCA to issue new certificates for the vSphere HTML5 web client fling, you can skip steps 2, 3 & 4 below and go to step 5.

2. Create the new VMCA-issued certificate on the PSC

If you want to see what the current store looks like

```
[VC]# vecs-cli entry list --store vsphere-webclient
```

Log in as root, make a directory to hold the new certificate and key, generate the keys

```
[VC]# mkdir h5
[VC]# cd h5
[VC]# certool --genkey --privkey=h5.key --pubkey=h5.pubkey
```

3. **Copy and update the certool.cfg template**

```
[VC]# cp /usr/lib/vmware-vmca/share/config/certool.cfg .
```

```
[VC]# vecs-cli entry getcert --store vsphere-webclient --alias vsphere-webclient --
output webclient.cer
[VC]# certool --viewcert --cert webclient.cer | grep Subject:

  Subject: CN=vsphere-webclient, DC=vsphere, DC=local, C=US, OU=mID-baf7a6b1-023f-
426d-bb20-4d02d81515ec
```

NOTE: Copy the OU id above and enter it for the field “OrgUnit” in the certool.cfg below. I am not sure if it makes any difference, but it doesn't hurt, either. I got that using the following commands

MODIFY certool.cfg TO LOOK LIKE THIS

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = h5-client
Organization = VMware
OrgUnit = mID-baf7a6b1-023f-426d-bb20-4d02d81515ec
State = California
Locality = Palo Alto
IPAddress = <IP_ADDRESS_OF_HTML5_APPLIANCE>
Email = administrator@corp.local
Hostname = h5client-01a.corp.local
```

4. **Using the key and the config file, generate the certificate**

```
[VC]# certool --gencert --privkey=h5.key --cert=h5.crt
[VC]# certool --viewcert --cert=h5.crt
```

5. **Create a new service/solution user**

NOTE: If you are using your own custom certificates or 3rd party generated certificates, and have skipped steps 2, 3 and 4 above, then you need to replace `h5.crt` in the below command with the respective crt file name.

Create a new service "h5-webclient" on the PSC

```
[VC]# dir-cli service create --name h5-webclient --cert h5.crt --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
```

This solution user account needs godly powers: *ActAsUsers, Administrators, SolutionUsers, LicenseService.Administrators* (the last one might get inherited by virtue of Administrators membership)

```
[VC]# dir-cli group modify --name Administrators --add h5-webclient --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
```

```
[VC]# dir-cli group modify --name ActAsUsers --add h5-webclient --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
[VC]# dir-cli group modify --name SolutionUsers --add h5-webclient --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
[VC]# dir-cli group modify --name LicenseService.Administrators --add h5-webclient --
login administrator@vsphere.local --password <PSC_NODE_PASSWORD>
```

6. **Create a new store and import the new cert+key**
   Change the names h5-webclient as appropriate for your environment in all the comments below.

```
[VC]# vecs-cli store create --name h5-webclient
[VC]# vecs-cli entry create --store h5-webclient --alias vsphere-webclient --cert
h5.crt --key h5.key
```

7. **View the new store**

```
[VC]# vecs-cli entry list --store h5-webclient
```

8. **Grant permissions to the new store**

Check the current one to see what permissions we need to add to the new one

```
[VC]# vecs-cli store get-permissions --name vsphere-webclient
```

Duplicate these onto the h5-webclient store. Run these commands in the **PSC** node.

```
[VC]# vecs-cli store permission --name h5-webclient --user perfcharts --grant read
[VC]# vecs-cli store permission --name h5-webclient --user vapiEndpoint --grant read
```

Need to create a user in the local OS on PSC

```
[VC]# useradd h5-client -G dialout,video,cis
```

Grant the new user permission to the new store

```
[VC]# vecs-cli store permission --name h5-webclient --user h5-client --grant read
```

EXAMPLE OUTPUTS

```
 [VC]# vecs-cli store get-permissions --name vsphere-webclient
PERMISSIONS FOR STORE: [vsphere-webclient]
OWNER : root
USER ACCESS
perfcharts read
vsphere-client read
vapiEndpoint read
```

```
[VC]# vecs-cli store get-permissions –name h5-webclient
PERMISSIONS FOR STORE: [h5-webclient]
OWNER : root
USER ACCESS
h5-client read
vapiEndpoint read
perfcharts read
```

Kick the certificate services on the PSC, just in case

```
[VC]# vecs-cli force-refresh
```

9. **On the h5client-01a appliance**

Configure hostname, IP, root password, add SSH key

Ensure you can ping the PSC by name

```
[h5client-appliance]# ping -c 2 <PSC_HOSTNAME/FQDN>
```

10. **BEFORE DOING ANYTHING ELSE**
    Edit the script used to pull the certificates from the VCSA onto the h5client appliance:

```
[h5client-appliance]# vi /usr/lib/vmware-client-configui/scripts/local_sso.sh
```

Change the line NGC_STORE line to look like this (points to the new store):

```
NGC_STORE="h5-webclient"
```

(this ensures that the configuration pulls the correct certificate and key)

11. Configure the h5client appliance to communicate with PSC_FQDN:

```
[h5client-appliance]# /etc/init.d/configui configure --start no --user root --vc <PSC_HOSTNAME/FQDN> --ntp <NTP_SERVER>
```

12. Stop the client service (should not be running with --start=no in the previous command)

```
[h5client-appliance]# /etc/init.d/vsphere-client stop
```

13. Hack the vi config/ds.properties to point at the correct keyStore

```
[h5client-appliance]# vi /etc/vmware/vsphere-client/config/ds.properties
```

Change the *keyStoreName* from "vsphere-webclient" to "h5-webclient" ... do **NOT** change the *keyAlias*

The file should look something like this:

```
service.homeLdu = 0bc19327-1944-4f71-b269-93c97f5a0e54
solutionUser.keyAlias = vsphere-webclient
solutionUser.keyStoreName = h5-webclient
```

The *homeLdu* appears to be the ID of the local domain on the VCSA. If you need it, you can find it in this file on the VCSA:

```
[VC]# vi /etc/vmware/install-defaults/vmdir.ldu-guid
```

14. Start the service... it takes a few minutes to run

```
[h5client-appliance]# /etc/init.d/vsphere-client start
```

Try to access the client from ControlCenter at

https://h5client-01a.corp.local/ui/

For VCSA with external PSC appliance

1. **SSH to the PSC node and run below commands**

Have separate SSH connections to both PSC and VC node, and create these aliases in both the nodes.

Aliases to save typing

```
[psc/VC]# alias vecs-cli='/usr/lib/vmware-vmafd/bin/vecs-cli'
[psc/VC]# alias dir-cli='/usr/lib/vmware-vmafd/bin/dir-cli'
[psc/VC]# alias certool='/usr/lib/vmware-vmca/bin/certool'
```

NOTE: If you want to user your own certificates or any other 3rd party generated certificates rather than using VMCA to issue new certificates for the vSphere HTML5 web client fling, you can skip steps 2, 3 & 4 below and go to step 5.

2. Create the new VMCA-issued certificate on the PSC

If you want to see what the current store looks like, then run below command in **VC (NOT PSC)**, as vsphere-webclient solution user is stored in the VECS residing in the VC node.

```
[VC]# vecs-cli entry list --store vsphere-webclient
```

Log in as root, make a directory to hold the new certificate and key, generate the keys

```
[psc]# mkdir h5
[psc]# cd h5
[psc]# certool --genkey --privkey=h5.key --pubkey=h5.pubkey
```

3. **Copy and update the certool.cfg template**

```
[psc]# cp /usr/lib/vmware-vmca/share/config/certool.cfg .
```

*** vsphere-webclient solution user is stored in the VECS residing in the VC node, so you should run below command from the **VC** (**NOT PSC**)

```
[VC]# vecs-cli entry getcert --store vsphere-webclient --alias vsphere-webclient --
output webclient.cer
[VC]# certool --viewcert --cert webclient.cer | grep Subject:

  Subject: CN=vsphere-webclient, DC=vsphere, DC=local, C=US, OU=mID-baf7a6b1-023f-
426d-bb20-4d02d81515ec
```

NOTE: Copy the OU id above and enter it for the field “OrgUnit” in the certool.cfg below. I am not sure if it makes any difference, but it doesn't hurt, either. I got that using the following commands

MODIFY certool.cfg TO LOOK LIKE THIS

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = h5-client
Organization = VMware
OrgUnit = mID-baf7a6b1-023f-426d-bb20-4d02d81515ec
State = California
Locality = Palo Alto
IPAddress = <IP_ADDRESS_OF_HTML5_APPLIANCE>
Email = administrator@corp.local
Hostname = h5client-01a.corp.local
```

4. **Using the key and the config file, generate the certificate**

```
[psc]# certool --gencert --privkey=h5.key --cert=h5.crt
[psc]# certool --viewcert --cert=h5.crt
```

5. **Create a new service/solution user**

NOTE: If you are using your own custom certificates or 3rd party generated certificates, and have skipped steps 2, 3 and 4 above, then you need to replace `h5.crt` in the below command with the respective crt file name.

Create a new service "h5-webclient" on the PSC

```
[psc]# dir-cli service create --name h5-webclient --cert h5.crt --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
```

This solution user account needs godly powers: *ActAsUsers, Administrators, SolutionUsers, LicenseService.Administrators* (the last one might get inherited by virtue of Administrators membership)

```
[psc]# dir-cli group modify --name Administrators --add h5-webclient --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
[psc]# dir-cli group modify --name ActAsUsers --add h5-webclient --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
[psc]# dir-cli group modify --name SolutionUsers --add h5-webclient --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
[psc]# dir-cli group modify --name LicenseService.Administrators --add h5-webclient -
-login administrator@vsphere.local --password <PSC_NODE_PASSWORD>
```

6. **Create a new store and import the new cert+key**
   Change the names h5-webclient as appropriate for your environment in all the comments below.

```
[psc]# vecs-cli store create --name h5-webclient
[psc]# vecs-cli entry create --store h5-webclient --alias vsphere-webclient --cert
h5.crt --key h5.key
```

7. **View the new store**

```
[psc]# vecs-cli entry list --store h5-webclient
```

8. **Grant permissions to the new store**

Check the current one to see what permissions we need to add to the new one by running below command from the **VC (NOT PSC)** since vsphere-webclient solution user is stored in VECS of VC.

```
[psc/VC]# vecs-cli store get-permissions --name vsphere-webclient
```

Duplicate these onto the h5-webclient store. Run these commands in the **PSC** node.

```
[psc]# vecs-cli store permission --name h5-webclient --user vmware-perfcharts --grant
read
[psc]# vecs-cli store permission --name h5-webclient --user vapiEndpoint --grant read
vecs-cli store permission --name h5-webclient --user vspherewebclientsvc --grant read
```

When you run above commands, if you get errors like – *"vecs-cli failed. Error 1332: Operation failed with error ERROR_NONE_MAPPED (1332)",* ignore them. This means, you don't need to map these roles from PSC. Continue with next steps.

Need to create a user in the local OS on PSC

```
[psc]# useradd h5-client -G dialout,video,cis
```

Grant the new user permission to the new store

```
[psc]# vecs-cli store permission --name h5-webclient --user h5-client --grant read
```

EXAMPLE OUTPUTS

*** For **external PSC**, you need to run below command from the **VC (NOT PSC)**

```
[psc/VC]# vecs-cli store get-permissions --name vsphere-webclient
PERMISSIONS FOR STORE: [vsphere-webclient]
OWNER : root
USER ACCESS
perfcharts read
vsphere-client read
vapiEndpoint read
```

```
[psc]# vecs-cli store get-permissions –name h5-webclient
PERMISSIONS FOR STORE: [h5-webclient]
OWNER : root
USER ACCESS
h5-client read
vapiEndpoint read
perfcharts read
```

Kick the certificate services on the PSC, just in case

```
[psc]# vecs-cli force-refresh
```

9. **Configure files in PSC for HTML5 client to use the same SSO as that of the web client**
   Run below commands to copy few necessary files from VC to PSC to make the configure command work

   ```
   [psc]# mkdir -p /etc/vmware/vsphere-client/cmCatalog
   [psc]# mkdir -p /etc/vmware/vsphere-client/config
   ```

```
[psc]# scp -rp root@<VC_IP_ADDRESS>:/etc/vmware/vsphere-client/cmCatalog/*
/etc/vmware/vsphere-client/cmCatalog/
[psc]# scp -rp root@<VC_IP_ADDRESS>:/etc/vmware/vsphere-client/config/*
/etc/vmware/vsphere-client/config/
```

10. **On the h5client-01a appliance**

Configure hostname, IP, root password, add SSH key

Ensure you can ping the PSC by name

```
[h5client-appliance]# ping -c 2 <PSC_HOSTNAME/FQDN>
```

11. **BEFORE DOING ANYTHING ELSE**
    Edit the script used to pull the certificates from the VCSA onto the h5client appliance:

```
[h5client-appliance]# vi /usr/lib/vmware-client-configui/scripts/local_sso.sh
```

Change the line NGC_STORE line to look like this (points to the new store):

```
NGC_STORE="h5-webclient"
```

(this ensures that the configuration pulls the correct certificate and key)

12. Configure the h5client appliance to communicate with PSC_FQDN:

```
[h5client-appliance]# /etc/init.d/configui configure --start no --user root --vc
<PSC_HOSTNAME/FQDN> --ntp <NTP_SERVER>
```

13. Stop the client service (should not be running with --start=no in the previous command)

```
[h5client-appliance]# /etc/init.d/vsphere-client stop
```

14. Hack the vi config/ds.properties to point at the correct keyStore

```
[h5client-appliance]# vi /etc/vmware/vsphere-client/config/ds.properties
```

Change the *keyStoreName* from "vsphere-webclient" to "h5-webclient" ... do **NOT** change the *keyAlias*

The file should look something like this:

```
service.homeLdu = 0bc19327-1944-4f71-b269-93c97f5a0e54
solutionUser.keyAlias = vsphere-webclient
solutionUser.keyStoreName = h5-webclient
```

The *homeLdu* appears to be the ID of the local domain on the VCSA. If you need it, you can find it in this file on the VCSA:
Run below command from the **VC** node

```
[psc/VC]# vi /etc/vmware/install-defaults/vmdir.ldu-guid
```

15. Start the service... it takes a few minutes to run

```
[h5client-appliance]# /etc/init.d/vsphere-client start
```

Try to access the client from ControlCenter at

https://h5client-01a.corp.local/ui/

For windows VC with Embedded PSC

1. **Connect to windows VC (For remote connections, you can use RDP/Powershell etc.,)** and open command prompt in administration mode

Aliases to save typing

```
[VC]# doskey vecs-cli="c:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe" $*
[VC]# doskey dir-cli="c:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe" $*
[VC]# doskey certool="c:\Program Files\VMware\vCenter Server\vmcad\certool.exe" $*
```

NOTE: If you want to user your own certificates or any other 3rd party generated certificates rather than using VMCA to issue new certificates for the vSphere HTML5 web client fling, you can skip steps 2, 3 & 4 below and go to step 5.

2. Create the new VMCA-issued certificate on the PSC

If you want to see what the current store looks like

```
[VC]# vecs-cli entry list --store vsphere-webclient
```

Log in as root, make a directory to hold the new certificate and key, generate the keys

```
[VC]# mkdir h5
[VC]# cd h5
[VC]# certool --genkey --privkey=h5.key --pubkey=h5.pubkey
```

3. **Copy and update the certool.cfg template**

```
[VC]# cp /usr/lib/vmware-vmca/share/config/certool.cfg .
```

```
[VC]# vecs-cli entry getcert --store vsphere-webclient --alias vsphere-webclient --
output webclient.cer
[VC]# certool --viewcert --cert webclient.cer
```

Look for OU for the Subject: CN=vsphere-webclient in the output

```
Subject: CN=vsphere-webclient, DC=vsphere, DC=local, C=US, OU=mID-baf7a6b1-023f-426d-
bb20-4d02d81515ec
```

NOTE: Copy the OU id above and enter it for the field “OrgUnit” in the certool.cfg below. I am not sure if it makes any difference, but it doesn't hurt, either. I got that using the following commands

MODIFY certool.cfg TO LOOK LIKE THIS

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = h5-client
Organization = VMware
OrgUnit = mID-baf7a6b1-023f-426d-bb20-4d02d81515ec
State = California
Locality = Palo Alto
IPAddress = <IP_ADDRESS_OF_HTML5_APPLIANCE>
Email = administrator@corp.local
Hostname = h5client-01a.corp.local
```

4. **Using the key and the config file, generate the certificate**

```
[VC]# certool --gencert --privkey=h5.key --cert=h5.crt
[VC]# certool --viewcert --cert=h5.crt
```

5. **Create a new service/solution user**

NOTE: If you are using your own custom certificates or 3rd party generated certificates, and have skipped steps 2, 3 and 4 above, then you need to replace `h5.crt` in the below command with the respective crt file name.

Create a new service "h5-webclient" on the PSC

```
[VC]# dir-cli service create --name h5-webclient --cert h5.crt --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
```

This solution user account needs godly powers: *ActAsUsers, Administrators, SolutionUsers, LicenseService.Administrators* (the last one might get inherited by virtue of Administrators membership)

```
[VC]# dir-cli group modify --name Administrators --add h5-webclient --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
```

```
[VC]# dir-cli group modify --name ActAsUsers --add h5-webclient --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
[VC]# dir-cli group modify --name SolutionUsers --add h5-webclient --login
administrator@vsphere.local --password <PSC_NODE_PASSWORD>
[VC]# dir-cli group modify --name LicenseService.Administrators --add h5-webclient --
login administrator@vsphere.local --password <PSC_NODE_PASSWORD>
```

6. **Create a new store and import the new cert+key**
   Change the names h5-webclient as appropriate for your environment in all the comments below.

```
[VC]# vecs-cli store create --name h5-webclient
[VC]# vecs-cli entry create --store h5-webclient --alias vsphere-webclient --cert
h5.crt --key h5.key
```

7. **View the new store**

```
[VC]# vecs-cli entry list --store h5-webclient
```

8. **Grant permissions to the new store**

Check the current one to see what permissions we need to add to the new one

```
[VC]# vecs-cli store get-permissions --name vsphere-webclient
```

Duplicate these onto the h5-webclient store. Run these commands in the **PSC** node.

```
[VC]# vecs-cli store permission --name h5-webclient --user perfcharts --grant read
[VC]# vecs-cli store permission --name h5-webclient --user vapiEndpoint --grant read
```

Need to create a user in the local OS on PSC. Go to Control Panel, User Accounts, Manage Accounts and add a new user called h5-client with the password same as PSC login password

Grant the new user permission to the new store

```
[VC]# vecs-cli store permission --name h5-webclient --user h5-client --grant read
```

EXAMPLE OUTPUTS

```
 [VC]# vecs-cli store get-permissions --name vsphere-webclient
```

```
PERMISSIONS FOR STORE: [vsphere-webclient]
OWNER : root
USER ACCESS
perfcharts read
vsphere-client read
vapiEndpoint read
```

```
[VC]# vecs-cli store get-permissions –name h5-webclient
PERMISSIONS FOR STORE: [h5-webclient]
OWNER : root
USER ACCESS
h5-client read
vapiEndpoint read
perfcharts read
```

Kick the certificate services on the PSC, just in case

```
[VC]# vecs-cli force-refresh
```

9. Generate the configure files for the HTML5 client appliance
   From the windows VC, follow below steps to generate the necessary files to configure the appliance. These are same steps which you would run if you are configuring windows VC for the HTML5 appliance with default certificates.
   a. Download service-configure.bat from the fling website
   b. Edit service-configure.bat and replace the value for NGC_STORE from vsphere-webclient to h5-webclient
   c. Run service-configure.bat from the command prompt opened with administrative rights
   d. Following files will be generated after the command successfully completes:
      ```
      i) store.jks
      ii) ds.properties
      iii) webclient.properties
      ```
   e. SSH as root into the H5 client appliance VM (Note: password is demova)
      ```
      mkdir /etc/vmware/vsphere-client/
      mkdir /etc/vmware/vsphere-client/config
      mkdir /etc/vmware/vsphere-client/vsphere-client/
      mkdir /etc/vmware/vsphere-client/vsphereFeatures
      ```
   f. Copy the files to H5 client virtual appliance at the following locations:

      ```
      i) /etc/vmware/vsphere-client/store.jks
      ii) /etc/vmware/vsphere-client/config/ds.properties
      iii) /etc/vmware/vsphere-client/vsphere-client/webclient.properties
      ```

      If you want to set an NTP server - Add NTP servers using the following command, where

NTP servers are comma separated, e.g., 0.pool.ntp.org,1.pool.ntp.org,2.pool.ntp.org,3.pool.ntp.org

10. **On the h5client-01a appliance**

Configure hostname, IP, root password, add SSH key

Ensure you can ping the PSC by name

```
[h5client-appliance]# ping -c 2 <PSC_HOSTNAME/FQDN>
```

11. Stop the client service if it is already running

```
[h5client-appliance]# /etc/init.d/vsphere-client stop
```

12. Hack the vi config/ds.properties to point at the correct keyStore

```
[h5client-appliance]# vi /etc/vmware/vsphere-client/config/ds.properties
```

Change the *keyStoreName* from "vsphere-webclient" to "h5-webclient" ... do **NOT** change the *keyAlias*

The file should look something like this:

```
service.homeLdu = 0bc19327-1944-4f71-b269-93c97f5a0e54
solutionUser.keyAlias = vsphere-webclient
solutionUser.keyStoreName = h5-webclient
```

13. Start the service... it takes a few minutes to run

```
[h5client-appliance]# /etc/init.d/configui post_configure
[h5client-appliance]# /etc/init.d/vsphere-client start
```

Try to access the client from ControlCenter at

https://h5client-01a.corp.local/ui/

For windows VC with external windows PSC

There are still some issues making this combination work, so steps are not listed at this time. If you can generate the certificates for this mode, do let us know.

Notes

i) For what it is worth, it looks like, the NgcSolutionUser.class here */usr/lib/vmware-vsphere-client/server/work/deployer/s/global/28/0/vim-services-6.1.0.jar/com/vmware/vise/vim/security/sso/impl/NgcSolutionUser.class* is hardcoded to use the "vsphere-webclient" alias name, so the alias in the store.jks keystore must have that value or the whole thing falls apart.

ii) If you are using PSC from 6.0 U2 (and above) release, then you can look at the certificates by logging in to PSC UI (https://<psc-ip>/psc) and navigating to certificates in the left navigator. You can import your certificates from PSC UI if you face issue with command line.

iii) **Cleanup steps:** In case you want to remove/delete the HTML5 client appliance and the respective certificates from the VECS store, follow below steps:

a. Power off the HTML5 web client appliance and delete the VM

b. To clean-up VECS store and corresponding certificates generated for the vSphere HTML5 web client, run below commands from PSC:

```
[psc]# alias vecs-cli='/usr/lib/vmware-vmafd/bin/vecs-cli'
[psc]# alias dir-cli='/usr/lib/vmware-vmafd/bin/dir-cli'
[psc]# alias certool='/usr/lib/vmware-vmca/bin/certool'
[psc]# vecs-cli entry delete --store h5-webclient --alis vsphere-webclient
[psc]# vecs-cli store delete --name h5-webclient
[psc]# dir-cli service delete --name h5-webclient
[psc]# userdel h5-client
[psc]# rm –fr /root/h5/
```

Reference

https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID-DB55A84F-8405-49AB-89B5-04FE3A5CD03C.html

To use custom certificates for Fling Appliance Management UI (FAMI UI) running at port 5490:

Thanks to fling users who have created below steps to replace the certificates of FAMI UI with custom certs.

- Log into the HTML5 appliance as root
- Look up the keystore location and password in your config file
- grep keystore.jks /etc/vmware/vsphere-client/vsphere-client/webclient.properties
- Set some handy variables based on that info
  PASS='<your password here>'
  STORE='/etc/vmware/vsphere-client/store.jks'
  SERVER=html5-lab
- Combine the certificate with any intermediate and root signing cert into one file
  cat ${SERVER}_cmu_edu_cert.cer > cert_chain.cer
  echo >> cert_chain.cer
  cat ${SERVER}_cmu_edu_interm.cer >> cert_chain.cer
- Bundle up the private key and certificate into a PKCS12 file (fix the filenames in the variables)
  CER=cert_chain.cer
  KEY=${SERVER}.key
  openssl pkcs12 -export -in $CER -inkey $KEY -name '1' -out store.p12 -password "pass:$PASS"
- Backup the keystore, just in case
  cp -pn $STORE $STORE.orig
- Stop the servers
  /etc/init.d/vsphere-client stop
  /etc/init.d/configui stop
- Import the certs and key into the keystore
  keytool -importkeystore -srckeystore store.p12 -srcstoretype PKCS12 -srcstorepass $PASS -destkeystore $STORE -deststorepass $PASS
  rm store.p12
- Replace the configui self-signed cert
  mv -n /usr/lib/vmware-client-configui/src/server/cert/configui-cert.pem{,.orig}
  mv -n /usr/lib/vmware-client-configui/src/server/cert/configui-key.pem{,.orig}
  cp $CER /usr/lib/vmware-client-configui/src/server/cert/configui-cert.pem
  cp $KEY /usr/lib/vmware-client-configui/src/server/cert/configui-key.pem
- Start the servers
  /etc/init.d/vsphere-client start
  /etc/init.d/configui start