View CAC Instructions:

Find a workstation that has all the DOD certificates on it. Export all the DOD certificates including the DOD ROOT CA 2 and DOD ROOT CA 3. (For SIPR this will be different. You will have to look at the certificate on the CAC to be used.)

You can look at the certificate by opening mmc, click add remove snap-ins, click certificates, personal. Open the certificates that are on the CAC there. It should say what CA it was signed by and the ROOT CA that authorized it.

STEP1 extract the ROOT CA and trusted certificate authorities for all certs that users will use.

Click Start, RUN, MMC, click add / remove snap-ins, click certificates, click computer (use local computer).

Find the certificates that they are using for CAC login (NIPR is DOD ROOT CA2, DOD ROOT CA3, CA-11 through CA-29). Right click the certificate and click export. Save it to a folder you will remember later.

STEP2

In order for CAC login to work for that user you need to import the ROOT CA and the certificate authority's certificate into a keystore file. (you extracted this from STEP1)

From the C:\Program Files\VMware\VMware View\Server\jre\bin directory run keytool

```
keytool -import -alias <typesomethinghere> -file (this is where you specify a certificate you exported) -keystore dhdw.key
```

Example:

```
keytool -import -alias DODROOTCA2 -file DODROOTCA.cer -keystore dhdw.key
```

Repeat this step for all the certificates that you exported. this will be a minimum of two certs. The ROOT CA and the issuing certificate authority for the users card.

STEP3 CAC ENABLE VIEW USING YOUR FILE

Create a file called locked.properties in the c:\Program Files\VMware\VMware View\Server\sslgateway\conf directory.

The file should have this in it:

```
trustKeyfile=dhdw.key

trustStoretype=JKS

useCertAuth=true
```

Restart the vmware view server. You're done! You have to copy that file you created to each and every View Connection Broker and View Security Server for it to work. This whole thing is contingent on the domain being cac enabled already.

Typically the windows 7 workstation needs to have all the DOD root certificates installed and the Active Client software including all Active client patches. This is usually the reason CAC login fails. They will also need Desktop Validator configured to validate the certificates.