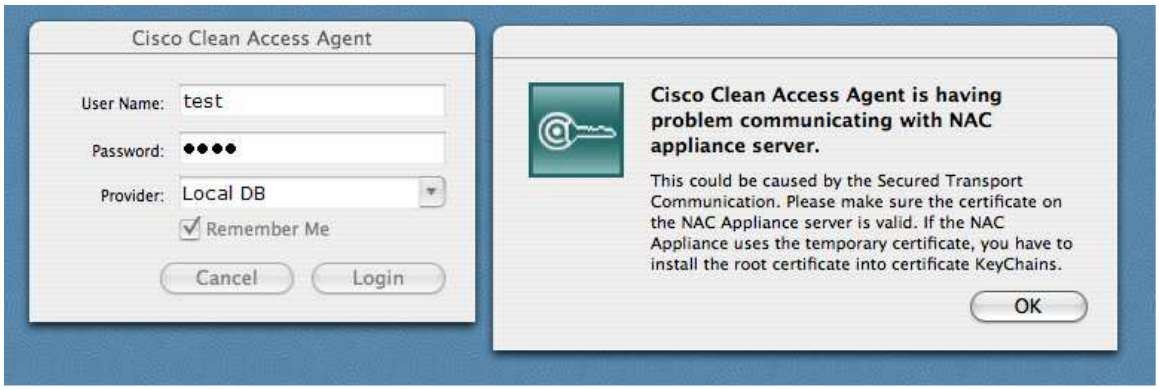
Getting CCA Mac Agent to Successfully Communicate with Clean Access Server

Symptoms: When logging in to CCA 4.1.x with a Mac Agent, you may receive an error like the one pictured below.



Root Causes: The certificate on the CAS has to be issued to a fully qualified domain or host name in order to be validated in Mac OS-X, and the client needs to have a proper root certificate.

Options for creating a cert based on FQDN:

1) *Use a self signed certificate from the CAS*. Generate this by browsing to the CAM, manage the CAS you are connecting into ("Device Management" > "CCA Servers" > "Manage", and select "Network" > "Certs". Make sure this cert is generated to a hostname that is resolvable by clients (either add the hostname to your DNS server, or we can edit hosts files on test computers. Also, the hostname that is used should match the hostname found under the "Network" > "DNS" page. Then reboot the CAS to apply the settings.

Attached to this email, I have included the root certificate to use if you are using self-signed certificates.

Note: In the later section when we import this root cert into the Mac cert store, it will show up in the store as "www.perfigo.com".

2) *Export a CSR and bring it to an internal CA*. First, follow the steps above to generate a self signed cert based on the hostname. The CSR we create will be based on the hostname in the self-signed cert. After that, browse to the same place on the CAS, "Network" > "Certs", and drop the dropdown box to the export option. Here, export the CSR and the private key, and save them in an appropriate place.

Now we need to take the CSR to your internal CA. If you are using Microsoft, it is located at http://<hostname>/certsrv where <hostname> is a name or address of your CA

server. Once there we request a certificate, select advanced request on the next page, and then request a cert based on a PKCS #10 cert request. Here we can paste in the CSR contents, and select “Web Server” from the template dropdown box.

It will create the cert and let you download it in a DER format or Base 64 format. We want the Base 64 format.

Now, return to the homepage of the cert server, and select “Download a CA certificate”. Change the encoding method to Base 64 and select “Download CA Certificate”. This will be the root certificate.

Return to the page on the CAS under “Network” > “Certs”, and dropdown the box to “Import”. Here we will import three things. We import the Private Key file we exported before (make sure the dropdown is set to private key when you select upload), the root (CA) cert from your internal CA (make sure Root/Intermediate cert is selected in the dropdown when you select upload), and the cert we created (make sure CA-signed PEM-encoded X509 cert is selected underneath). If all three were successful, then select “Verify and install uploaded certificates”. Once that completes, reboot the CAS. You will need to also make sure the CA Root certificate is on the MAC. That is explained in another selection below.

3) *Export a CSR and send it to a third party cert issuer (Thawte, Verisign, GoDaddy).* First, follow the steps in number 1 to generate a self signed cert based on the hostname. The CSR we create will be based on the hostname in the self-signed cert. After that, browse to the same place on the CAS, “Network” > “Certs”, and drop the dropdown box to the export option. Here, export the CSR and the private key, and save them in an appropriate place.

Send the CSR to your CA of choice. They will send you back a certificate. Browse back to where you exported the CSR, and drop the box down to “Import”. We import the Private Key file we exported before (make sure the dropdown is set to private key when you select upload) and the cert the third party company created (make sure CA-signed PEM-encoded X509 cert is selected underneath). Note that you should not need to import a root cert for these, because the CAS has the roots built in. If both were successful, then select “Verify and install uploaded certificates”. Once that completes, reboot the CAS.

The root cert should already be in the MAC client for most third party vendors. You can verify that by following the instructions in the next section.

Placing the Root Certificate in the proper place on the MAC client:

If you were using a self-signed cert or one signed from internal CA, you will need to import that root cert into your Mac client. First, if the cert is not on the Mac, move the root certificate onto the Mac by emailing it over or using a USB key. To access the Mac certificate store, open “Finder”. Select “Go” > “Applications” > “Utilities”, and open

“Keychain Access”. Click on “X.509 Anchors”. Make sure that the small lock icon in the window is unlocked, and if it isn’t click on it and enter your credentials to unlock it.

Now select the “File” menu, and the “Import” option. Browse and select the root certificate. Now it should appear in the ‘X509 Anchors” right hand pane with all the other root certs. Scroll down and select it. On the top of that pane it will show the details of the cert. It should have a green checkbox and a message that says “This certificate is valid”. If it has a red “x” and says something different, double click on the cert, scroll to the bottom, expand “Trust Settings”, and after “When using this certificate”, change the box to say “Always Trust”.

Ensuring that the MAC client can resolve the name of the CAS:

Now that your cert is installed, make sure the Mac can resolve the IP address of the CAS. If you added the CAS name into your DNS server, when you ping the name from the Mac terminal, it should resolve and attempt to ping the IP address. If not then you have not added the CAS properly to your DNS server.

If you are doing this in a test environment, then we can temporarily add the DNS entry to a “hosts” file on your MAC client so that you do not have to add anything to a production DNS server. Note that for this procedure you will need “root” access to your Mac. The instructions to enable the root account on a Mac should be available from a google search.

To do this, open a terminal on the Mac. It will show a unix prompt. Enter “su” and type in the root password to login as root. Now enter “cd /etc”. Open the hosts file by typing “vi hosts”. There should be a few lines in the host file such as:

127.0.0.1 localhost

We want to add a new line. Move the cursor to the bottom of the file (end of the last line of text and hit “o”. It should move the cursor to a new line. Type in the IP of the CAS, then a tab, then the name (that we defined on the CAS and issued the cert to), ie:

10.10.10.10 caserver

Hit enter to exit text editing mode, then type “:wq” to save and quit. Once back at the command line, try to ping the name to see if it resolves to the address.

Once the MAC can resolve that name to the proper address, try to log in to the CCA Agent. Note that you may need to re-download the agent from the GUI login for the settings to take affect. You should be able to login successfully.