CONSTELLA GROUP ℠
*Enhancing Human Health*

CONSTELLA FUTURES

Opening IQCare on a server and client machine

1. IQCare can work on either standalone machine or in a network setup
2. For a standalone machine a full installation of all components is required
3. For computers accessing IQCare via the network no specialised installation is required. The client machine only needs an up to date Operating system and webbrowser.
4. The following user privileges need to be set on both server machine and the client machines (computers accessing IQCare via a network). Follow all steps below

5. To open IQCare using the Sever machine open a web browser and type in
http://localhost/IQCare/frmLogin.aspx

- To open IQCare from a client machine type in the following

http://**ipaddess of server machine**/IQCare/frmlogin.aspx i.e.

http://172.23.190.175/IQCare/frmlogin.aspx

6. Security issues to consider over wireless network
    o Ensure that the network administrator has enabled at the least WEP encryption on the wireless LAN, WPA encryption is preferred if available. This will prevent eavesdropping (listening to data traffic) and unauthorized access to IQCare.
    o Ensure that the SSID (or access point name) of the wireless network is not advertised or broadcast by any of the wireless access points on the network to help prevent unauthorised access.
7. Security issues to consider over cable network
    o See 8 and 9.
8. In both models above (wireless and cable), ensure that the server's firewall is set to only accept connections from trusted computers, and not the entire network. Ro do this, on the server, go to your network connections and find the connection that is sharing the services (wireless or LAN), then click it with the right button and go to properties. Under properties, go to Advanced and Settings under windows firewall. The firewall should be on. On the exceptions tab, find the IIS exception rule (port 80 or IIS application), double click it and click "Change Scope" to specify the trusted environment. The default setting allows access from anywhere, it is recommended that you specify either my network (subnet only) if all computers on the LAN are trusted, or Custom List (recommended). With custom list, you specify the IP addresses of trusted computers on the LAN to allow access from them alone. Note for wireless networks, it is recommended you use the latter option as the "my network (subnet) only" option could include people outside the building in range of wireless signal. See below for screenshot.
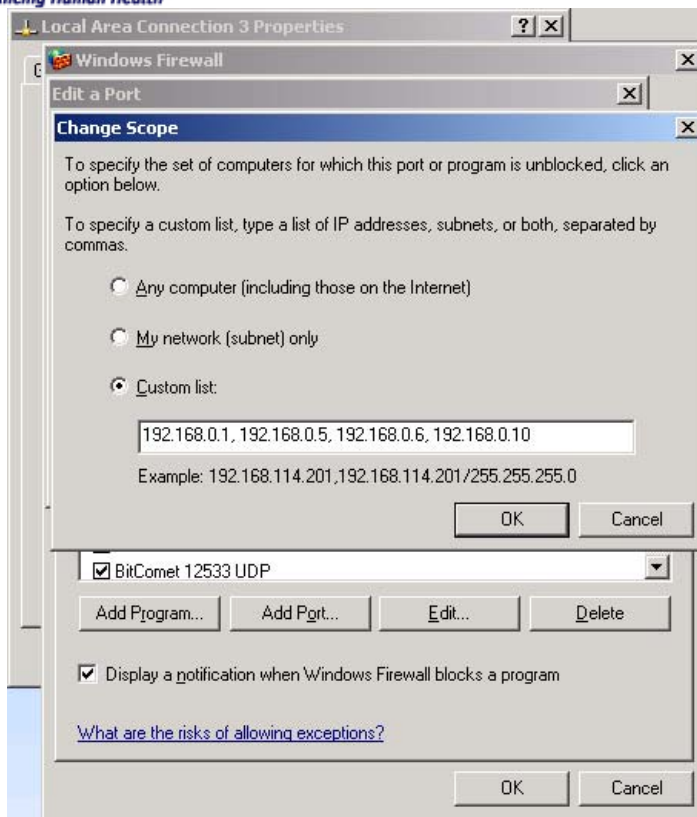
9. For networks with a domain logins (cable and wireless), access to IQCare can and should be controlled with the use of a domain group account under IIS. To do this, get the administrator to create an active directory group called IQCare. Add users who should have rights to access IQCare on the server to the IQCare group. In IIS under the IQCare virtual folder, directory security tab, click the edit button to assign "Integrated windows authentication" access (and not anonymous access as is the default). Then find the IQCare folder on the server's hard drive using windows explorer (usually C:\INETPUB\WWWROOT\IQCARE). Under the security tab for the folder properties, add the IQCare group, give it read access, click advanced and check the "Replace permission entries on all child objects…" before clicking OK. Then restart IIS for the changes to take effect. With this change, only users who are members of the IQCare group will be able to access IQCare across the LAN. This should be done in addition to no 8 above.

Note that the ideal setup will have us serve IQCare in a secure (SSL) environment from IIS. This will provide encryption from client to server irrespective of the medium the data travels on. This will be investigated for future.

Steps to setup user privileges for Network/Stand-alone machines.

Below steps are need to be done only on the Server Machine in case of Network setting. In case of stand-alone all the steps need to be followed on as the same machine will also be a server.

1. Move into the folder options of the system. Click on "View" Tab. Check for the option of "Use Simple File Sharing", this should be unchecked.
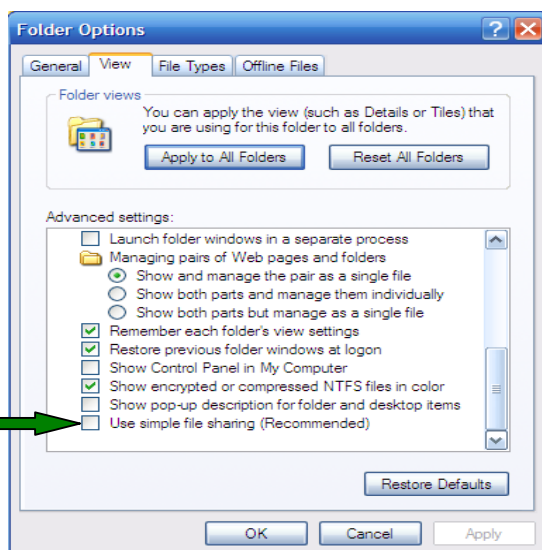

2. Check for the "Inetpub" folder in "C:". Move into the properties of "Inetpub" folder by right clicking on it.
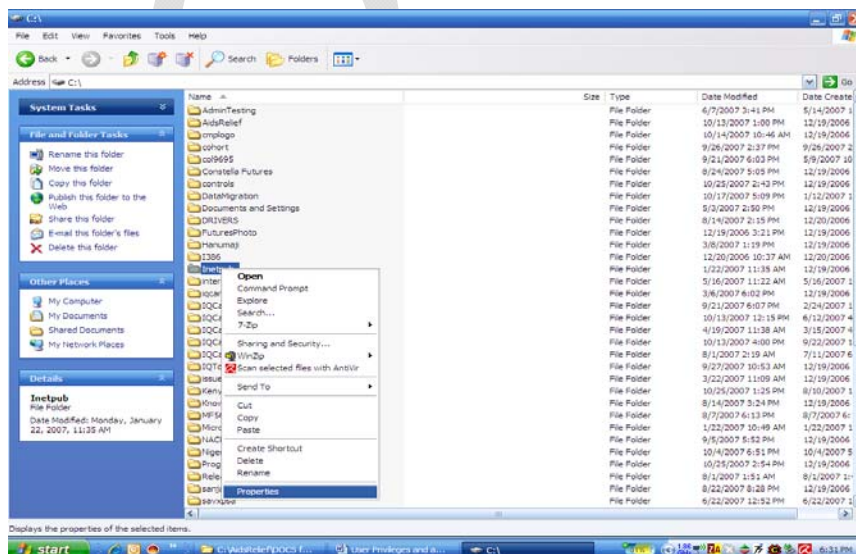
3. On the property page of "Inetpub" folder move into the "Security Tab". Check weather "Everyone" and "Internet User (IUSR_SystemName) of the System is appearing on the "Group or user names" sub window. If in-case any one of the them are missing, Press the Add button below the "Group or user names" sub window
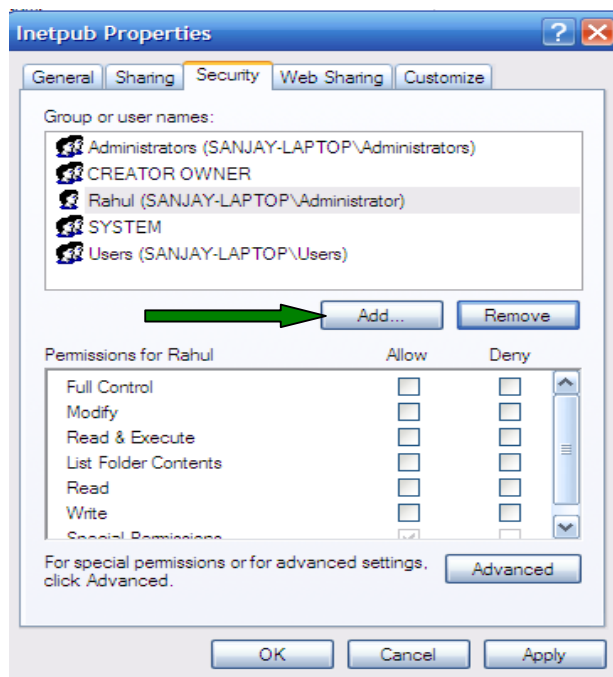

4. After clicking Add button, User will get the screen for the adding the user and user groups to the security tab of the "Inetpub" folder. Now click on the Advance button to get the options of adding user and groups.
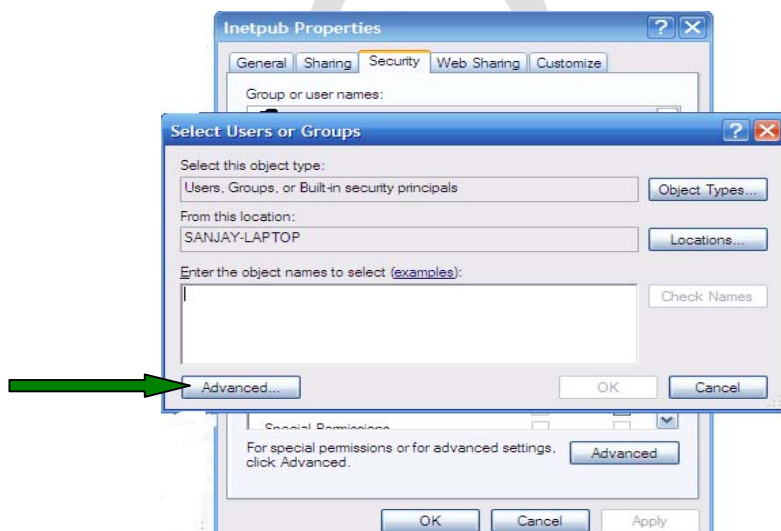
5. After clicking "Advance" button, user will see a search screen for adding users and user groups. Click on find now to get the entire list of the users and groups. Select "Everyone" and "IUSR_ xxx" from the list and click "OK" Button
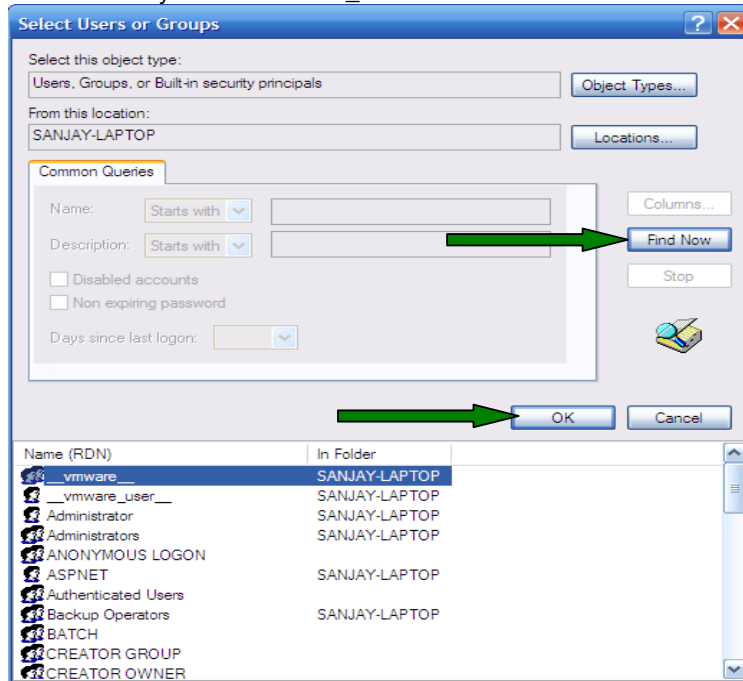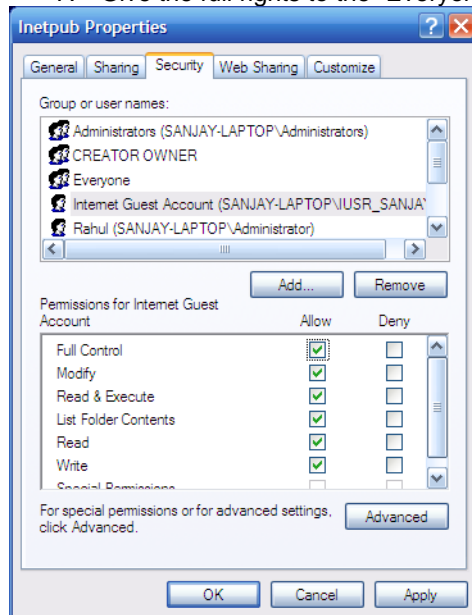

6. After clicking "OK" button, user will see the "Everyone" and Internet user in the "Select Users or Group" window. Click on "OK" button to get it in the main property window of the "Inetpub" folder.
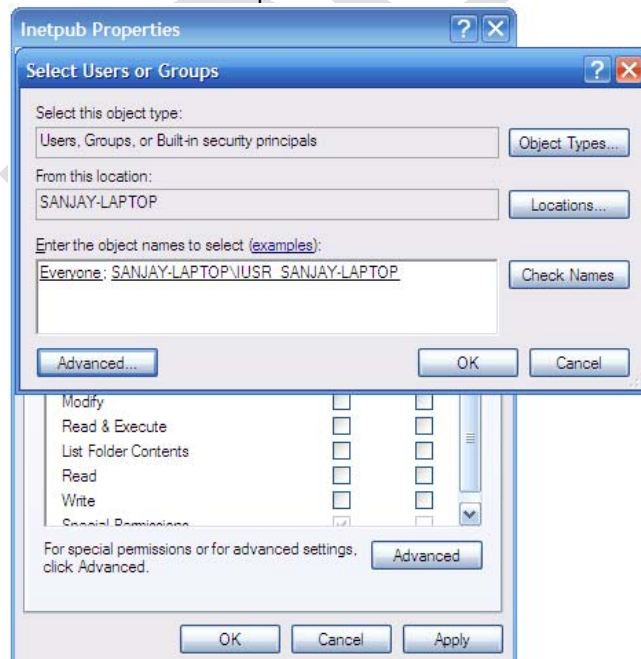
7. Give the full rights to the "Everyone" and Internet User on "Inetpub" folder.

8. Same steps needs to be followed for granting authentication on "C:\Inetpub\WWWRoot" folder.

After going through all these steps, users connected on the network or on the standalone will have rights to make changes to the "IQCare" Application.

For networked machines, one more step needs to be followed to make IQCare available to all the users: Open up the windows firewall and add a port "80" for IIS Server. This will help server's IIS to be visible to all machines available on the network.
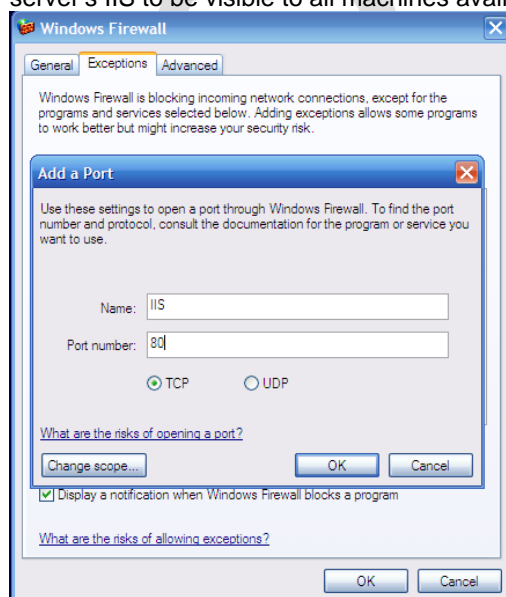
Important Steps after Migration

Below are some of the steps that are required to be taken soon after the migration of Careware data in IQCare.

- Make sure that a proper facility name is provided with County, LPTF and Satellite Number. As these things were not mandatory in the Careware system, migration may have incomplete data. Please also choose the Backup drive to make sure that the system takes backup in the designated position. Detailed steps for doing this:
  - Click on the Administration Tab
  - Click on the Facility Setup Tab
  - Ensure that all the required information is filled in.

- Soon after the setting up the Facility setup in the application, move into the Custom Fields Administration to edit any one of the field without making changes to it. This will enable the View responsible for showing up Custom Fields results in Custom Reports. Detailed steps for doing the same:
  - Click on Administration Tab
  - Click on Configure Custom Fields
  - Click on any of the Change buttons at the bottom of the page
  - Click on the Edit Custom Fields button

Important steps to be taken after Migration/New Setup

- After setting up the system, set the user authentication/access rights. This can be done in two phases. First step involves creation of User Group in User Group Administration of the system (Data Group). Second steps involves, actual creation of users in the application under the "Data" Group.
  Steps for doing the same are:

  - Click on the Administration Tab.
  - Click on User Group Administration.
  - Click on Add button to add a group.
  - Name newly added group as "Data".
  - Provide the proper authentication rights (Check all accept the User Administration and User Group Administration)
  - Click Save button to create the group and close the screen.
  - Click on the Administration Tab
  - Click on the Tab User Administration
  - Click on Add
  - Add a User (the name of the data staff at the LPTF)
  - Ensure that you add them to the "Data" group previously created
  - Give them a password (make this password the name of the LPTF)
  - Click on Save button to create the new User.
  - In the "Password" option of the application, change the password of the admin to the Universal Password. Don't tell anyone at the LPTF that you have done this. This will allows the CF field staff to access the application in case of users lost their password.