ASSUMPTION: The person who installs the operating system, creates accounts, and shares the information, is the de facto system administrator for RESA. Ultimately responsible for knowing who has access to the machines and for what purpose. It should also be noted that the system administrator is the sole person that can circumvent any security settings. I.e. Security settings and protocols are only effective if the system administrator (and other users with access to privileged accounts) don’t circumvent them. General rules:

* Don’t create permanent passwords that do not meet requirements. Usually:
  + 16 characters
  + At least 2 upper case
  + At least 2 lower case
  + At least 2 special character
  + At least 2 numeric
* Limit usage of shared/common accounts
* Know who has each individual account
* Require individual account holders to set their own password

The following changes can be implemented to reduce the use of shared accounts and passwords. This is a working document as of the date at the top of the page.

1. **LIMIT the permissions to directories and files.**

A more restrictive change may be available, but will require adding to the packages installed with the operating system and is not warranted at this time. As ROOT:

* 1. cd /opt/resa
  2. chmod 750 -R \*
  3. cd /opt/resa/resa\_build/game
  4. chmod 770 NWISS\_DB

**NOTE: After recovering to a checkpoint, check the permission of NWISS\_DB and reset if needed.**

* 1. chmod 770 DTED.AA
  2. cd /opt/resa/resa\_build/coretools/library/map
  3. chmod 770 pt\*.dat

NOTE: if workstations have issue, try changing all of /opt/resa/resa\_build/coretools/library/map to 770

1. **Implement individual controller workstations.** 
   1. **Overview**
      1. This will be different than before and will require a paper log be kept as to who has been assigned each login. For a remote site, a designated person can be given the list of available logins for assignment.
      2. For each workstation that will be in use, e.g. STA11, create multiple logins one for EACH controller. At the CIT it was assumed that only 2 controllers per a station would be needed and were labeled **d** and **n** for day shift and night shift. (e.g.sta 41d and sta41n). Each account will be created on the designated workstation machine AND on each alpha machine.
      3. As before, a resa account is not required on the workstation machines.
   2. **On each workstation machine**
      1. Use ROOT account and create file **/etc/profile.d/resastation.sh**

The contents of this will be the one line:

alias resaprod=’ssh -X -l $USER alpha1’

NOTE: the use of $USER allows this line to work for all user logins.

NOTE: if desired also add a second or third alias line to connect to a different alpha e.g.

alias resatest=’ssh -X -l $USER alpha2’

* + 1. Use the system > administrator > users and groups dialogue to create each account (e.g. for the workstation hosting station 11, these are sta11d, sta11n)
       1. Be sure to note the initial password assigned
       2. Use the User Properties on each account, Password Info tab
       3. ENABLE password expiration
       4. Days before change required 45 (or duration of exercise)
       5. Days before account inactive can also be set to 45. The workstation controller accounts should expire when no longer needed.
       6. Check “force password change on next login”

OPTIONAL! Assign passwords to each account that meet 16 character and complexity needs. E.g. yamaJAPAN2018!@# or tailored for each operator yama@JAPAN18\_14D, yama@JAPAN18\_14N. This is not as secure an approach as requiring each user to set their own 16 character password, but it does lesson the burden of resetting passwords if it is forgotten.

* 1. **On each Alpha machine**
     1. Use the system > administrator > users and groups dialogue to create account(s) with same exact name and initial password as the workstation logins created above. Use the same settings as above **including** the mandatory login change. Add this account to group resa.
     2. Edit the .bashrc for the account to have

source /opt/resa/resa\_build/resabashrc

gwar

sta11s

exit

NOTES:

* + - * The accounts sta11d and sta11n would both call sta11s
      * Replace sta11s with the appropriate login information.
      * If desired you could replace sta11s with vsta 11 c as=4 config=cciox
      * sta11s can be a combination of gwar and vsta command (removing need for gwar in the .bashrc account). E.g.

alias sta11s=”gwar; vsta 11 b as=4 config=cciox”

* + 1. Edit the resabashrc file to have an alias for sta11s as already (if using this option)
  1. **RESULTS of doing the above.** 
     1. Each user will have a unique login. Upon initial login to the workstation, the user will need to set a password. The current requirements are 16 characters with at least 1 upper, 1 lower, 1 digit, and 1 special.
     2. Upon connecting to the alpha machines, the user will also have to set password.
     3. Multiple operators will have access to each station account (sta10, sta11, sta14…), but they will make the connection via unique logins. Which means that the user’s login history can be tracked.
     4. A known few, will have the ability to reset logins if necessary (i.e. Kon Shin and 1-2 others will have root password)

1. **LOGIN History.**

To see who is logged in or who has been logged in, as root:

* To check direct login history (i.e. where the user logged directly into the local machine)
  + type ‘last’ on the command line.

prompt> **last**

* + This will show all of the information. For a single user add the user

prompt> **last sta11**

* + Alternatively look at the data file directly (do not edit the file):

/var/log/wtmp.1

e.g. **less /var/log/wtmp.1**

* To check ssh connections (those connections coming from a workstation)
  + Look at the data file directly (do not edit the file):

/var/log/secure

e.g. **less /var/log/secure**