Setting SoloBug Permissions on Linux

If you use SoloBug on Linux, you may want to set permissions for editing the SoloBug executable or adding files to the SoloBug_In folder in the TestTrack database directory. By default, /usr/bin/SoloBug is owned by root and cannot be accessed by other users.

We recommend using group security to manage these items. For example, the default group for regular users is 'staff'. To restrict SoloBug access to only a few users, you can create a new group specifically for SoloBug and any users added to that group.

To restrict access to the SoloBug executable:

1. Create a private SoloBug group
   ```
   # /usr/sbin/groupadd -g [new group id] solobug
   ```
2. Set permissions on the SoloBug executable
   ```
   # chmod 775 /usr/bin/SoloBug
   # chgrp solobug /usr/bin/SoloBug
   ```
3. Modify users to have a supplemental group of SoloBug
   ```
   # /usr/sbin/usermod -G [solobug group id] [username]
   ```

To provide full access to the SoloBug executable:

1. Set full permissions on the SoloBug executable
   ```
   # chmod 777 /usr/bin/SoloBug
   ```

To restrict access to the SoloBug_In folder:

1. Set permissions on the SoloBug_In folder
   ```
   # chmod 775 [path to TestTrack project]/SoloBug_In
   # chgrp solobug [path to TestTrack project]/SoloBug_In
   ```

To provide full access to the SoloBug_In folder:

1. Set full permissions on the SoloBug_In folder
   ```
   # chmod 777 [path to TestTrack project]/SoloBug_In
   ```

Article ID: 577
Last updated: 24 May, 2017
Revision: 3
Helix ALM (formerly TestTrack) -> SoloBug -> Setting SoloBug Permissions on Linux
http://www.seapine.com/knowledgebase/index.php?View=entry&EntryID=577