

GG Admin's Quick Guide for Adding Users



Revision Date

August 19, 2016

Purpose

The Admin Tool Guide's *Adding Users* section contains detailed steps for adding new users to GRIN-Global, including information on setting security permissions. This document summarizes the basic considerations needed when establishing new UserIDs as well as general security considerations.

The primary focus in this document is on adding users to the Curator Tool, since GRIN-Global Public Website (PW) users can self register. They can also change their password on the Public Website.

However, the section "*Assigning a Web Login for Internal (Genebank) Users*" in this document explains how to grant special privileges to Curator Tool users for the Public Website. This is an option that the administrator can do so that the genebank's internal staff can use the Public Website to access reports designed only for internal users, as well as several options listed under the Tools menu. (**Tools** is not visible to the public, the "external" users.)

Table of Contents

Overview	3
Adding New GG Users	3
Sites and Site Codes	4
Assigning a Web Login for Internal (Genebank) Users	4
Security	6
Error Messages	6
Establishing Groups and Permissions	7

Overview

User accounts must be established for all Curator Tool users by the GG administrator. Public Website users can self register at the GRIN-Global website. The GG administrator can also assign additional Public Website privileges for the internal genbank users.

Adding New GG Users

Refer to the Admin Tool Guide for complete “how-to” directions on setting up new users. Some key points to remember when adding users:

Action	Description
Select the Enabled checkbox	Indicates that the user will be allowed to login to the Curator Tool
Select the Active checkbox	Indicates the UserID is associated with an active cooperator – any data created or modified by this user will be tagged by his CooperatorID
Select a language for the user	The language setting determines what column headings, button text, etc. the user will see displayed in the Curator Tool
Assign the same Site Code	Site Codes are used to organize users by sites. This is a required field. Users in the same site can see each other’s tabs and lists in the CT. (Users can see lists of other users by selecting the Show All checkbox in the List Panel.) For more details about sites, see Sites and Site Codes .
Add user to the CT Users group	If the user will be using the Curator Tool, he needs to be added to the CT Users group. (By default, a new user is added only to the All Users group – the user has no CT permissions at that point)
Assign All Access permission to the user (if the user needs unlimited access)	Gives universal Create/Read/Update/Delete rights. The Administrators group has this permission as does the Administrator UserID. (Alternatively, you may decide to set up other Groups (see the next row in this table) with narrower permissions and not assign All Access to every user.)
Add user to other groups as needed	Groups will have specific permissions which meet an organization’s very unique needs. Groups are essentially templates for establishing permissions, so that each user does not need to be set up individually, but rather can be assigned to appropriate groups.

Sites and Site Codes

(Site Codes are a different kind of code as compared to the Codes described in the [Codes and Code Groups](#) section.). An organization using GRIN-Global can establish Site Codes for various reasons. The sites may be separate physical locations such as in the U.S., where “COR” is the site code for the Corvallis, Oregon genebank and “W6” is the code for the Western Regional Plant Introduction Station in Pullman, Washington.

A site code could be set up as the (virtual) site for special purposes, for example the “black box” storage of certain collections that are not routinely distributed.

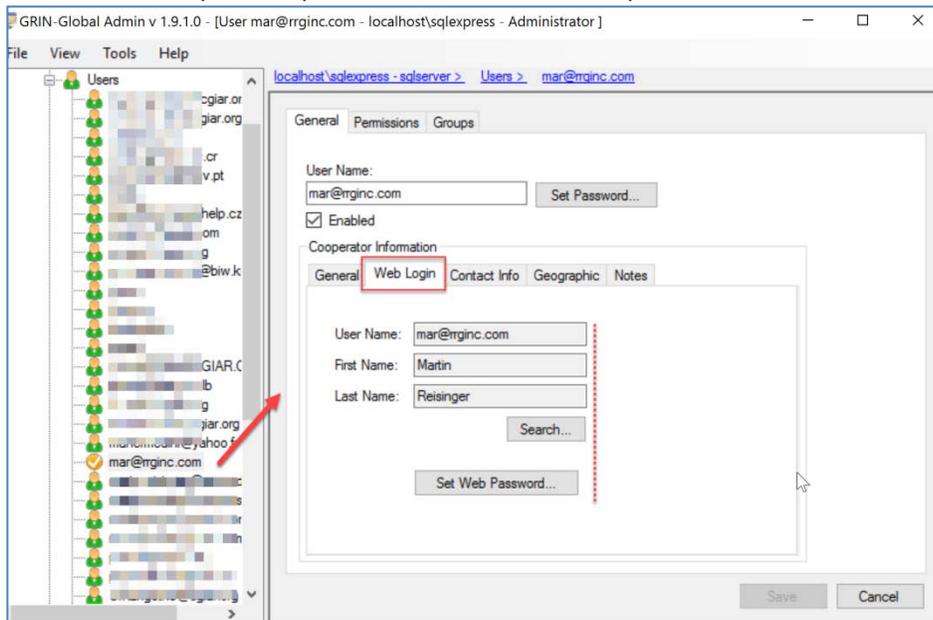
A site could also be set up for a specific crop or even for specific germplasm types. For example, if your genebank has two sets of procedures that vary, depending on the germplasm type, such as In-vitro and seeds, it may be helpful to create one site for the in-vitro, and the second for seeds.

Sites Example:

Get Site	Source Descriptor	Get Inventory Action	Get Sys Dataview Field Lang	Get Sys Table Field Lang	Accession Inventory Name	Site		
Site ID	Site Short Name	Site Long Name	Organization Abbreviation	Is Internal?	Is Distribution Site?	Type	FAO Institute Number	
2	BRW	Natl. Gemplasm Repository - Brownwood	BRW	Y	Y	Clonal maintenance site	USA133	
30	CLO	Clover collection	CLO	Y	Y	Seed maintenance site	USA134	
3	COR	Natl. Gemplasm Repository - Corvallis	COR	Y	Y	Seed and clonal maintenance site	USA026	
1	COT	Cotton Collection	COT	Y	Y	Seed maintenance site	USA049	
4	DAV	Natl. Gemplasm Repository - Davis	DAV	Y	Y	Clonal maintenance site	USA028	
10	DBMU	Database Management Unit	DBMU	Y	N	Seed maintenance site	USA126	
33	DLEG	Desert Legume Program	DLEG	Y	Y	Seed maintenance site	USA971	

Assigning a Web Login for Internal (Genebank) Users

The Public Website was designed for users who need to search for accessions and perhaps order them, typically external general users, researchers, breeders, etc. Genebank staff will also use the Public Website to search for accessions and display descriptors information, taxonomy, etc. Over time the Public Website has been modified to include additional features which are only appropriate to internal users, that is, users working in the genebank. When a CT user’s User Name is configured with a Web Login, that user can then access on the Public Website special reports and the Tools menu option.



The GG Administrator can complete this screen after the user has created her Public Website account, or can create it when creating or modifying the Curator Tool account.

Before the CT user has logged in:



After she has logged in:



At the National Plant Germplasm System, these are the reports currently available when logged in:



Reports available to the public users:



Security

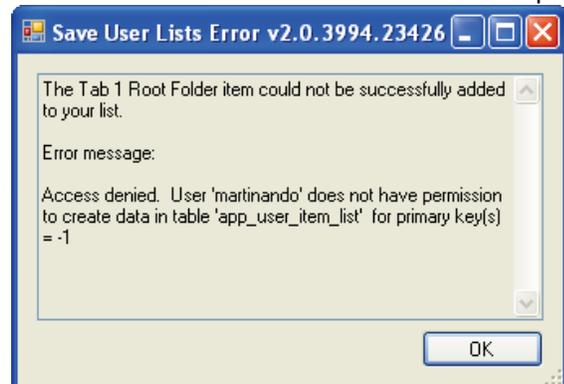
In general terms, there are three security alternatives to be considered:

1. Disable security entirely
2. Have an intermediate level of security centered around parent and child tables or related dataviews
3. Very strict security, as controlled as possible, where security is set at the record level based on specified criteria

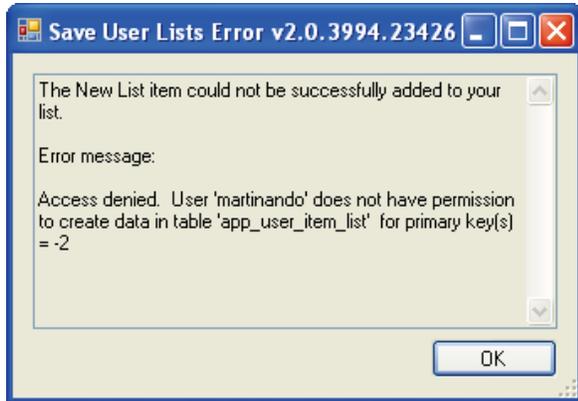
Usually most organizations opt for the second and third alternatives. The basic CT user account can read and write records, but then the sites and record owners determine in what dataviews edits are allowed. There are two security concepts to be considered: ownership and permissions. These are explained in detail in both the Curator Tool User Guide and the Admin Tool Guide.

Error Messages

If security is enabled (the default situation), users not added to the **CT Users** Group will receive several error messages when they log on. The following message displays when a user logs in to the Curator Tool and the user was not added to the CT Users Group:



The following error message will immediately be displayed as well, again for the same reason:

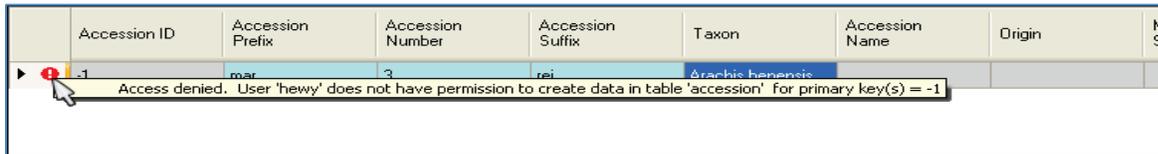


To correct this situation and to avoid the error messages, add the user to the **CT Users** group.

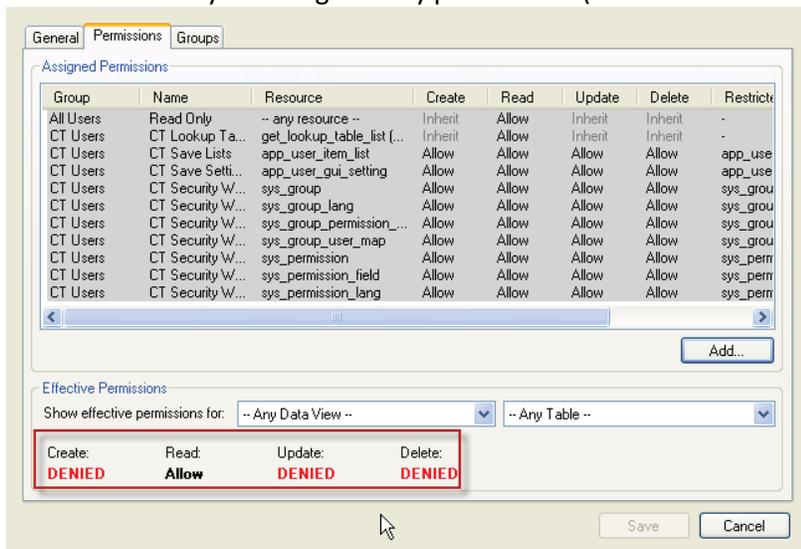
Establishing Groups and Permissions

Even when users are included in the **CT Users** group, they still will not be able to save new records. This section explains why an organization will want to establish other Groups and Permissions beyond the **All Users** and **CT User** groups that come installed with GRIN-Global.

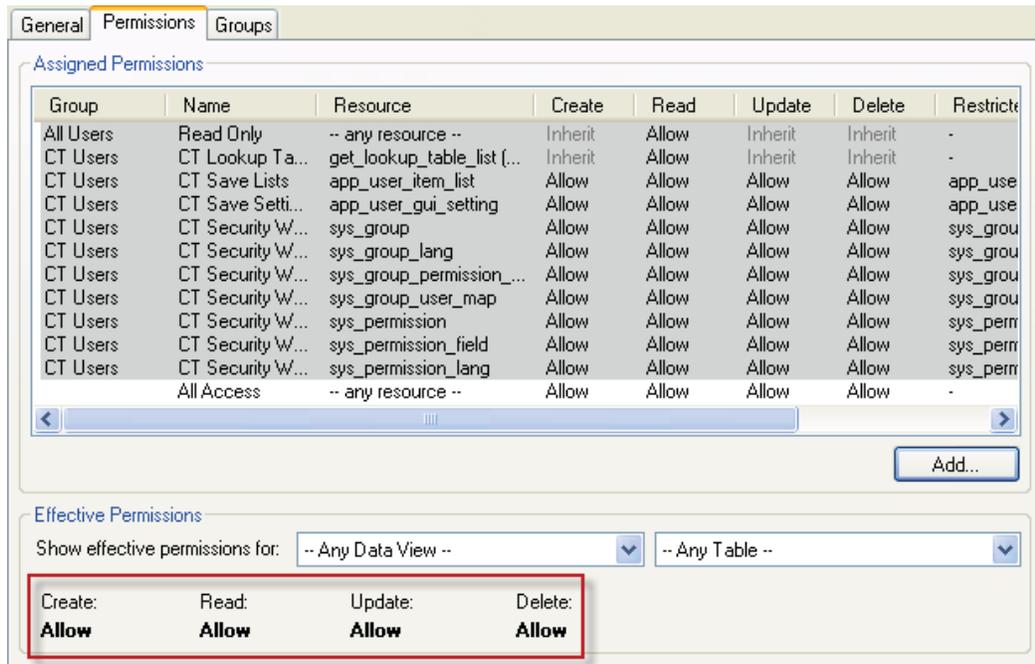
For example, a message similar to the following will be displayed after a failed Save action:



This user has not yet been given any permissions (other than “Read”) to the Accession (or any) table:

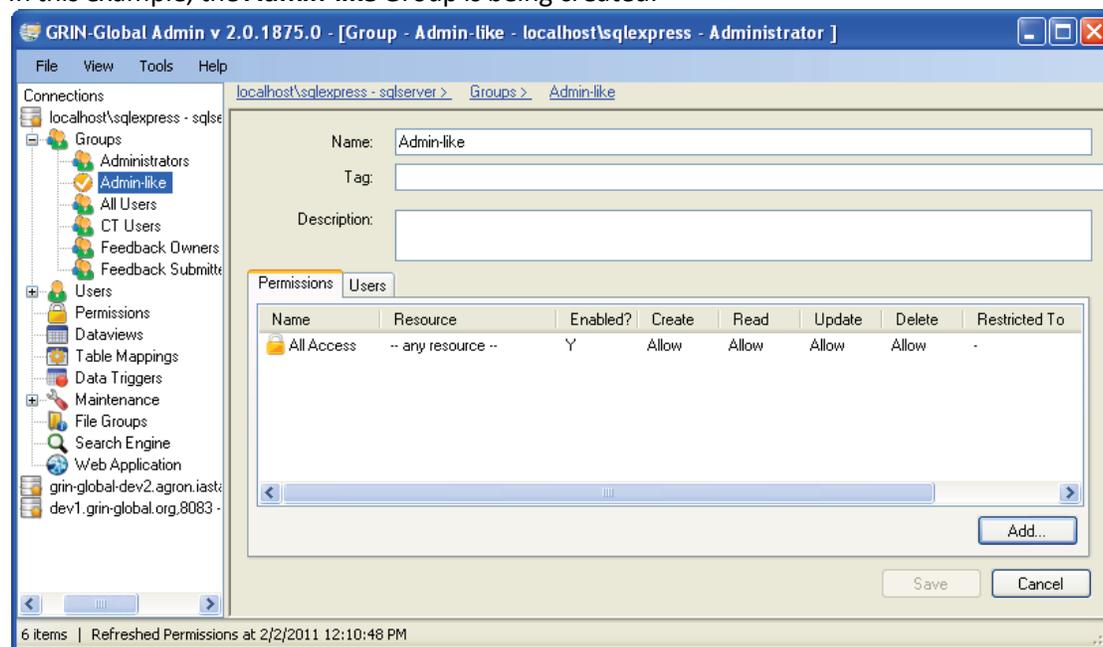


There are two quick methods for remedying this. One fix would be to add the user to the **Administrators** group; a second method would be to grant the **All Access** (to any resource) permission to the user as shown below:



However, a better solution would be to create a new group, modeled after the **Administrators** group, and then add users to that group. The advantages of doing this rather than simply adding users to the **Administrators** group are you keep the “true” Administrator permissions separate from other users.

In this example, the **Admin-like** Group is being created:



Any users then included in this group would initially have full data access as do administrators. Later, this group's permissions can be edited if necessary, for example to restrict access to certain data. The "true" administrators would not be impacted.

Also, groups or permissions can be established for certain categories of workers. For instance, an organization might want to establish that users who handle germplasm orders cannot modify accession records. Because of the flexibility with permissions, this can easily be accomplished.