## GG Admin’s Guide for Adding Users & Permissions Overview



Revision Date

October 31, 2016

Purpose

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 and on the security in the Curator Tool, which has two components: ownership and permissions.

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

[GG Admin’s Guide for Adding Users & Permissions Overview 1](#_Toc465701929)

[Overview 3](#_Toc465701930)

[Adding New GG Users 3](#_Toc465701931)

[Sites and Site Codes 4](#_Toc465701932)

[Curator Tool Users in the Same Site 5](#_Toc465701933)

[Super Users in a Site 5](#_Toc465701934)

[Assigning a Web Login for Internal (Genebank) Users 5](#_Toc465701935)

[Security 7](#_Toc465701936)

[Error Messages 7](#_Toc465701937)

[Establishing Groups and Permissions 8](#_Toc465701938)

[Appendix 11](#_Toc465701939)

[SQL for Establishing Site “Super Users” 11](#_Toc465701940)

#### 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 genebank 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 usedto 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](#sites).   C:\Users\MartyR\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\8PP0LLVL\site at 2016-10-31_15-35-59.jpg |
| 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

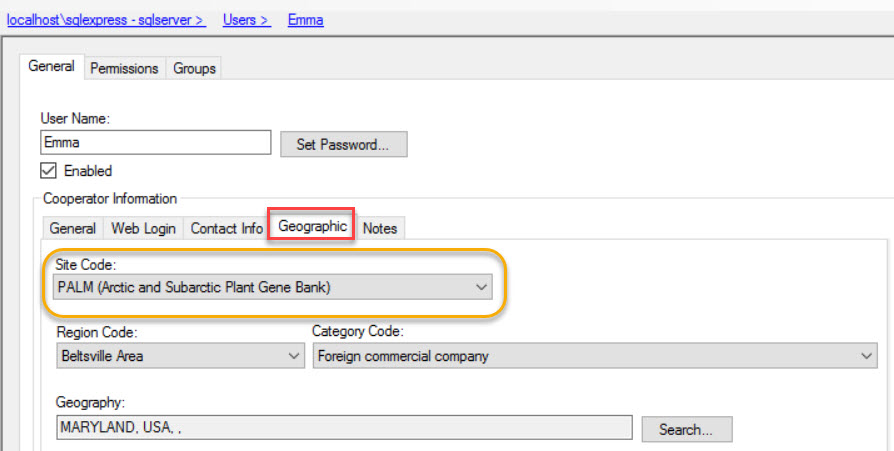
|  |  |
| --- | --- |
|  | The word “codes” being used to describe Site Codes is different from the Codes described in the [*Codes and Code Groups*](#code_groups) section. |

An organization using GRIN-Global can establish Sites for various reasons. The National Plant Germplasm System (NPGS) is comprised of multiple locations across the United States, so it was natural for the system to be subdivided into sites. “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.

Sites Example:  

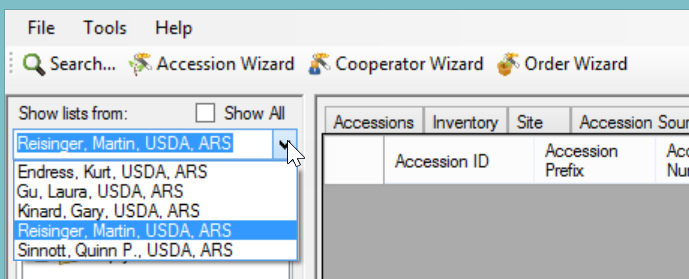

Besides physical locations, site codes can be set up for special purposes. For example, you could use a site for the “black box” storage of certain collections that are not routinely distributed. A site could also be set up for a specific crop or even for specific germplasm types. For example, if your 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.

###### Screen in AT When Adding s New User:



Users in different sites are not precluded from anything at the other sites, but there are some advantages of segmenting an organization into sites.

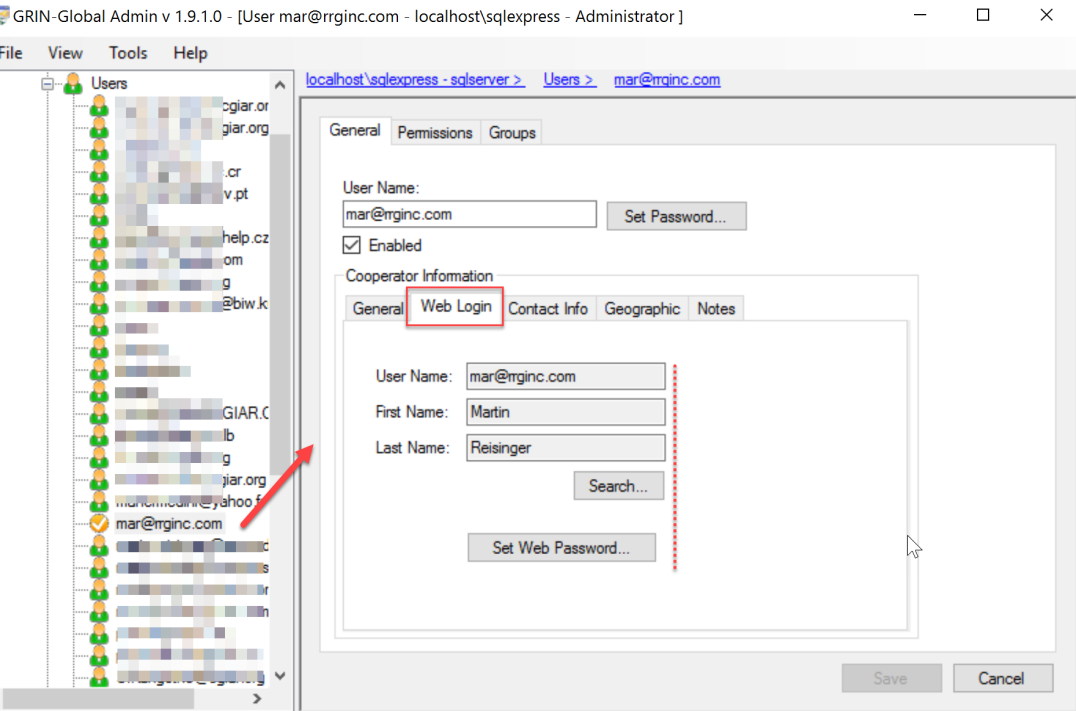
##### Curator Tool Users in the Same Site

The Curator Tool is designed to automatically display lists from users in the same site:   


##### Super Users in a Site

A site may want to extend global permissions privileges to specific users so that they can read, update, or delete any records that are associated with their site. In the appendix, in the section [*SQL for Establishing Site “Super Users,”*](#sql_for_site_super_users) directions are included for running a SQL script to set up site groups. Ownership and permission privileges are discussed later in this document.

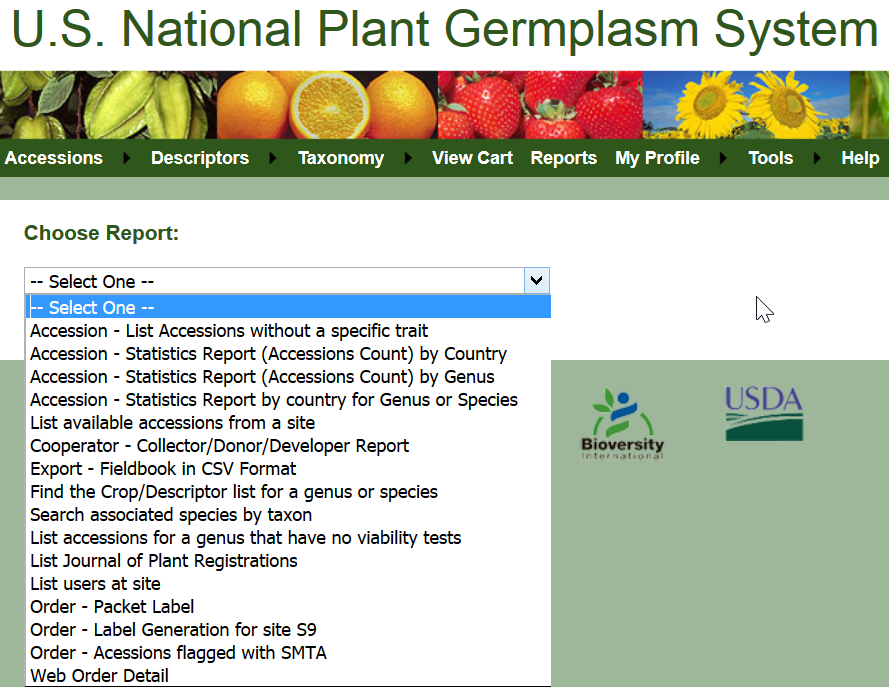
#### Assigning a Web Login for Internal (Genebank) Users

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:  

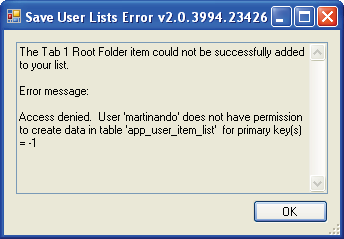

#### Security

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

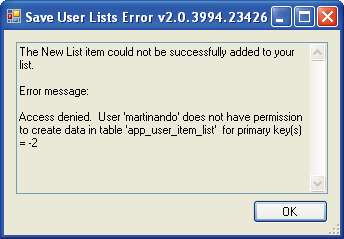
1. Disable security entirely
2. Have an intermediate level of security centered around parent and child tables or related dataviews
3. Very strict security, as controlled as possible, where security is set at the record level based on specified criteria (possible; but not typically done

Usually most organizations opt for the second alternative. 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 the 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:

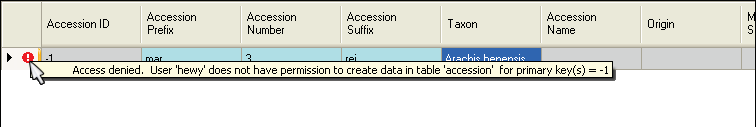


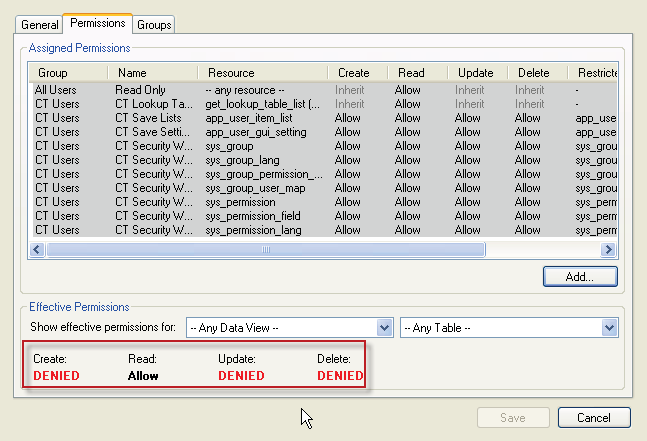
To correct this situation and to avoid the error messages, add the user to the **CT Users** group.

#### Establishing Groups and Permissions

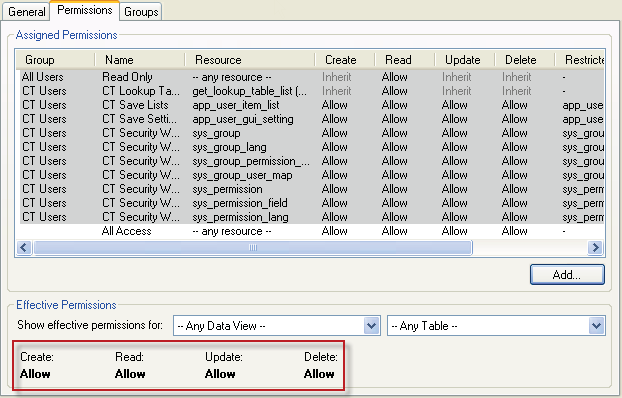
Even when users are included in the **CT Users** group, they still will not be able to save new records. This section explains why an organization will want to establish other Groups and Permissions beyond the **All Users** and **CT User** groups that come installed with GRIN-Global.

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

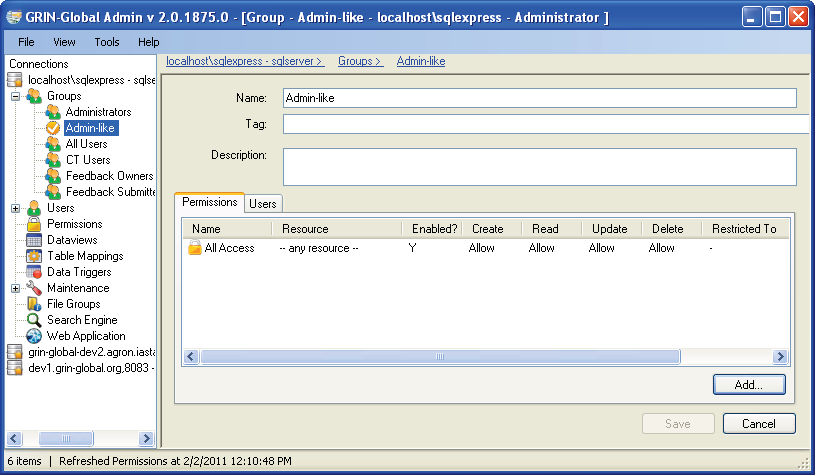


This user has not yet been given any permissions (other than “Read”) to the Accession (or any) table:  


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.

### Appendix

#### SQL for Establishing Site “Super Users”

The following SQL could be run by a GRIN-Global administrator to establish users in a site who would have full permission for all accessions within the same site code. The SQL creates empty groups, one for each site, linked to a permission that gives the members all rights to any records created by anyone at the site.

It creates a management group for each site as the name MANAGE\_SITE\_WHATEVER implies. In order to use this capability. after running the script, in the Admin Tool find the group and add users to it. For example, the group may be listed as MANAGE\_SITE\_NC7.

This script:

* Creates groups and permissions for managing site records
* Members of the group will be able to update and delete all records in any table owned by users at a particular site
* This SQL creates a group for each site in the site table

Remember that appropriate users will need to be added to the group separately by using the Admin Tool

-- fill in missing permission tags

UPDATE sp

SET sp.permission\_tag = REPLACE(spl.title,' ','\_')

FROM sys\_permission sp

JOIN sys\_permission\_lang spl ON sp.sys\_permission\_id = spl.sys\_permission\_id AND spl.sys\_lang\_id = 1

WHERE sp.permission\_tag IS NULL AND sp.owned\_by IN (1,48)

-- make system permissions owned by administrator

UPDATE sys\_permission

SET owned\_by = 48

WHERE owned\_by = 1

-- make system groups owned by administrator

UPDATE sys\_group

SET owned\_by = 48

WHERE owned\_by = 1

-- make create permission

INSERT INTO sys\_permission

SELECT null, null, 'CREATE\_ALL', 'Y', 'A', 'I', 'I', 'I', GETUTCDATE(), 48, null, null, GETUTCDATE(), 48

-- link create permission to ALLUSERS

INSERT INTO sys\_group\_permission\_map

SELECT

    (SELECT sys\_group\_id FROM sys\_group WHERE group\_tag = 'ALLUSERS'),

    (SELECT sys\_permission\_id FROM sys\_permission WHERE permission\_tag = 'CREATE\_ALL'),

    GETUTCDATE(), 48, null, null, GETUTCDATE(), 48

-- lang title and description for create permission

INSERT INTO sys\_permission\_lang

SELECT

    (SELECT sys\_permission\_id FROM sys\_permission WHERE permission\_tag = 'CREATE\_ALL'),

       1, 'CREATE\_ALL', 'Allow users to create rows in all tables',

    GETUTCDATE(), 48, null, null, GETUTCDATE(), 48

-- create site management groups

INSERT INTO sys\_group

SELECT 'MANAGE\_SITE\_'+s.site\_short\_name, 'Y', GETUTCDATE(), 48, NULL, NULL, GETUTCDATE(), 48

  FROM site s

-- create site management permissions

INSERT INTO sys\_permission

SELECT null, null, 'MANAGE\_SITE\_'+s.site\_short\_name, 'Y', 'I', 'I', 'A', 'A', GETUTCDATE(), 48, NULL, NULL, GETUTCDATE(), 48

  FROM site s

-- create site management permission field rows

INSERT INTO sys\_permission\_field

SELECT

    (SELECT sys\_permission\_id FROM sys\_permission WHERE permission\_tag = 'MANAGE\_SITE\_'+s.site\_short\_name),

       NULL,

       (SELECT MIN(sys\_table\_field\_id) from sys\_table\_field where field\_name = 'site\_id'),

       'INTEGER', '=', CONCAT(s.site\_id, ''),

       NULL,NULL,NULL,NULL,

       'current',

    GETUTCDATE(), 48, NULL, NULL, GETUTCDATE(), 48

         FROM site s

-- link site management groups and permissions

INSERT INTO sys\_group\_permission\_map

SELECT

    (SELECT sys\_group\_id FROM sys\_group WHERE group\_tag = 'MANAGE\_SITE\_'+s.site\_short\_name),

    (SELECT sys\_permission\_id FROM sys\_permission WHERE permission\_tag = 'MANAGE\_SITE\_'+s.site\_short\_name),

    GETUTCDATE(), 48, NULL, NULL, GETUTCDATE(), 48

  FROM site s