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

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:

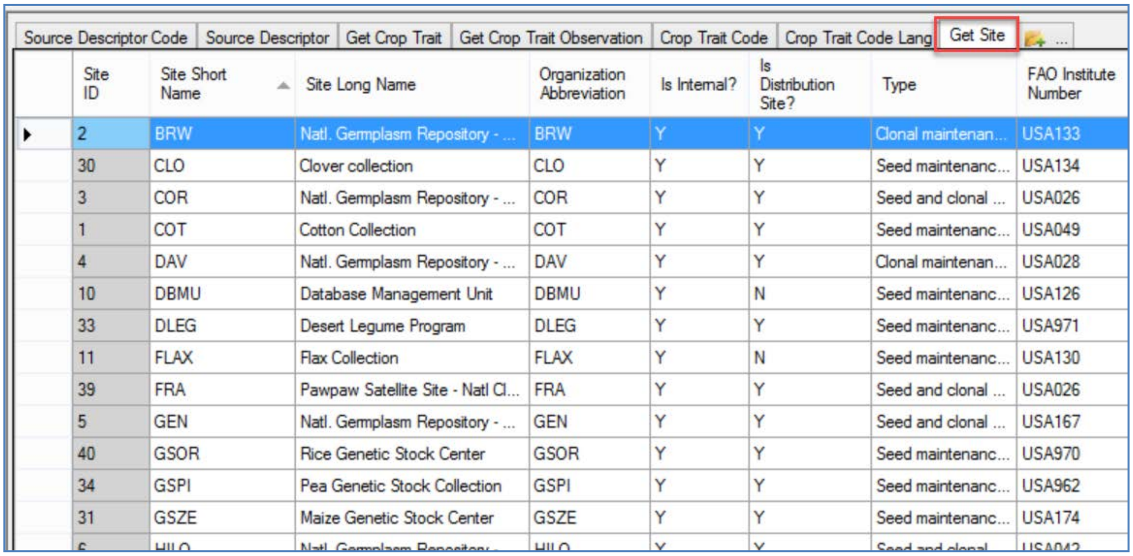
Action	Description
Select the **Enabled** checkbox	Indicates that the user will be allowed to login to the Curator Tool
Select the **Active** checkbox	Indicates the **UserID** is associated with an active cooperator – any data created or modified by this user will be tagged by his **CooperatorID**
Select 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 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

Note The word “codes” being used to describe Site Codes is different from the Codes described in the *Codes and 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.

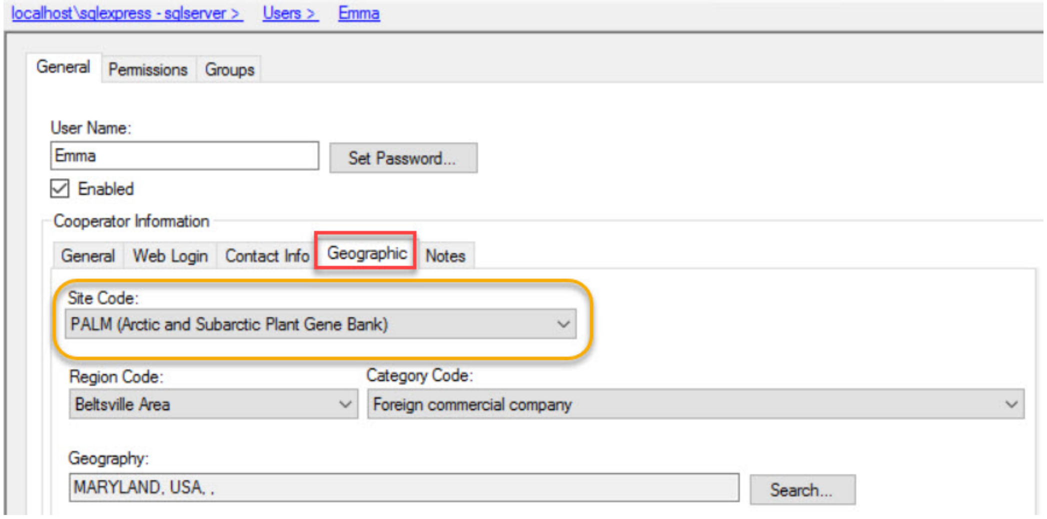
Sites Example:



Site ID	Site Short Name	Site Long Name	Organization Abbreviation	Is Internal?	Is Distribution Site?	Type	FAO Institute Number
2	BRW	Natl. Germplasm Repository - ...	BRW	Y	Y	Clonal maintenan...	USA133
30	CLO	Clover collection	CLO	Y	Y	Seed maintenanc...	USA134
3	COR	Natl. Germplasm Repository - ...	COR	Y	Y	Seed and clonal ...	USA026
1	COT	Cotton Collection	COT	Y	Y	Seed maintenanc...	USA049
4	DAV	Natl. Germplasm Repository - ...	DAV	Y	Y	Clonal maintenan...	USA028
10	DBMU	Database Management Unit	DBMU	Y	N	Seed maintenanc...	USA126
33	DLEG	Desert Legume Program	DLEG	Y	Y	Seed maintenanc...	USA971
11	FLAX	Flax Collection	FLAX	Y	N	Seed maintenanc...	USA130
39	FRA	Pawpaw Satellite Site - Natl Cl...	FRA	Y	Y	Seed and clonal ...	USA026
5	GEN	Natl. Germplasm Repository - ...	GEN	Y	Y	Seed and clonal ...	USA167
40	GSOR	Rice Genetic Stock Center	GSOR	Y	Y	Seed maintenanc...	USA970
34	GSPI	Pea Genetic Stock Collection	GSPI	Y	Y	Seed maintenanc...	USA962
31	GSZE	Maize Genetic Stock Center	GSZE	Y	Y	Seed maintenanc...	USA174
6	HILO	Natl. Germplasm Repository - ...	HILO	Y	Y	Seed and clonal ...	USA042

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:



User Name: Emma

☑ Enabled

Site Code: PALM (Arctic and Subarctic Plant Gene Bank)

Region Code: Beltsville Area

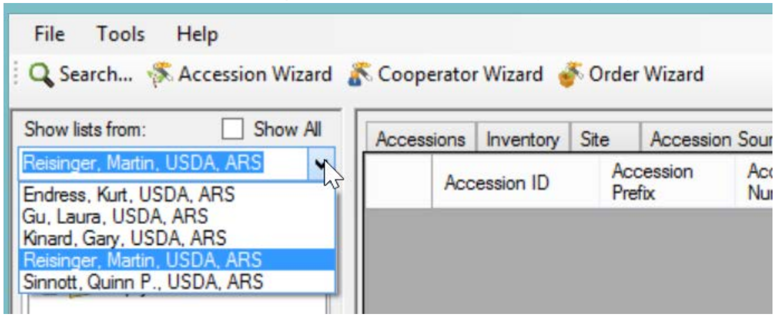
Category Code: Foreign commercial company

Geography: MARYLAND, USA, ,

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:



Show lists from: ☐ Show All

Reisinger, Martin, USDA, ARS

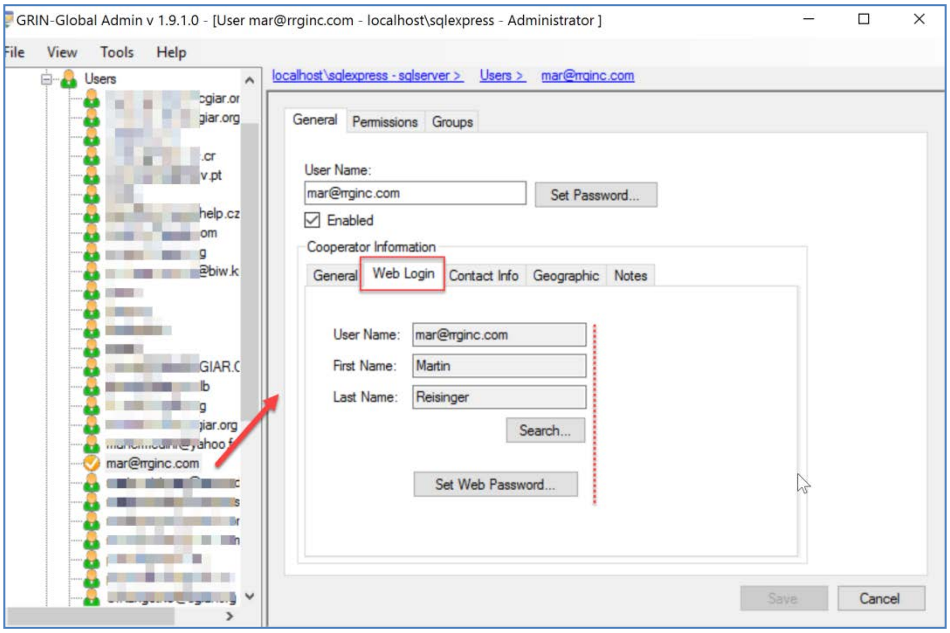
Endress, Kurt, USDA, ARS
Gu, Laura, USDA, ARS
Kinard, Gary, USDA, ARS
Reisinger, Martin, USDA, ARS
Sinnott, Quinn P., USDA, ARS

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,"* 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.



GRIN-Global Admin v 1.9.1.0 - [User mar@rrginc.com - localhost\sqlexpress - Administrator]

localhost\sqlexpress - sqlserver > Users > mar@rrginc.com

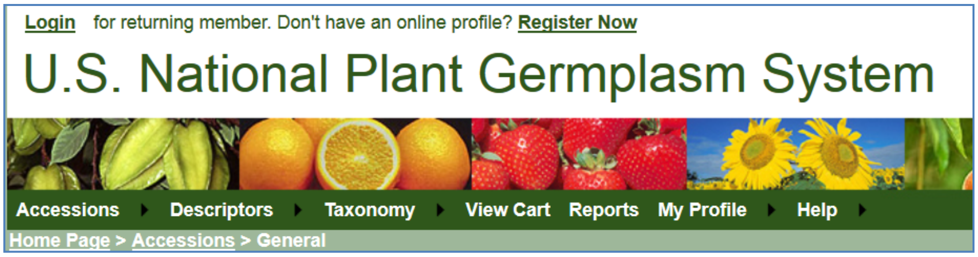
User Name: mar@rrginc.com

☑ Enabled

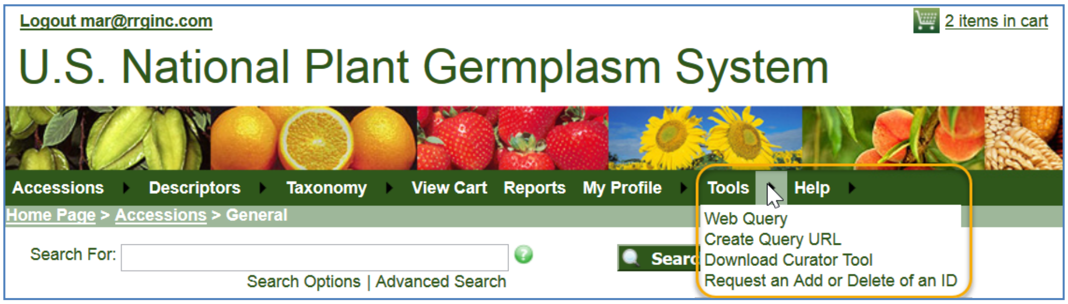
User Name: mar@rrginc.com
First Name: Martin
Last Name: Reisinger

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.

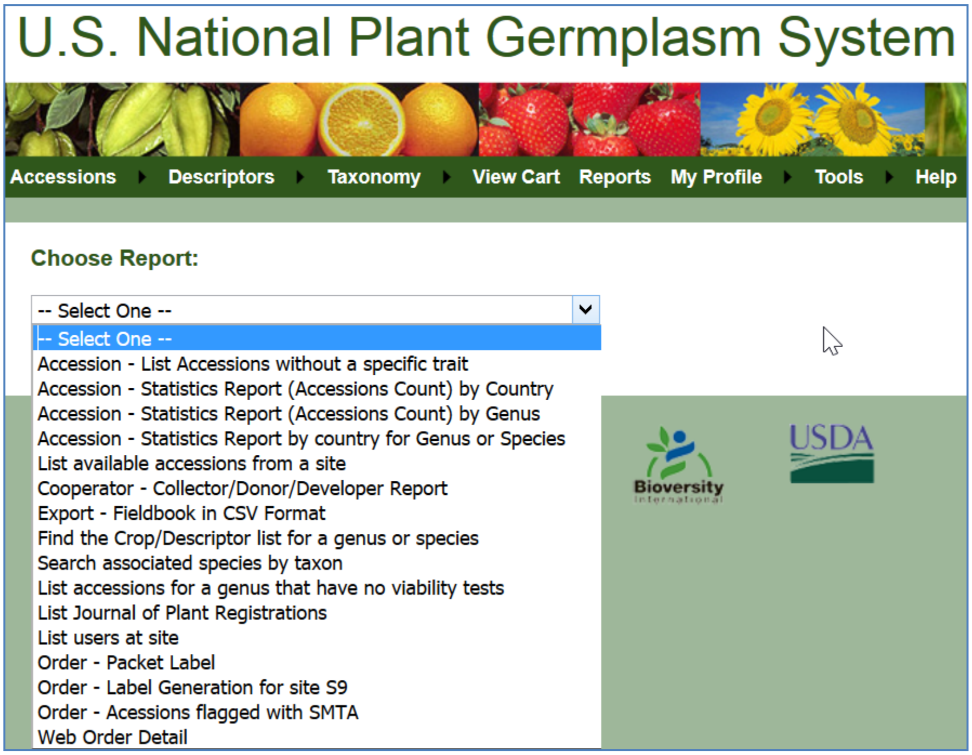
Before the CT user has logged in:


Login for returning member. Don't have an online profile? Register Now
U.S. National Plant Germplasm System
Accessions
Descriptors
Taxonomy
View Cart
Reports
My Profile
Help
Home Page > Accessions > General

After she has logged in:



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

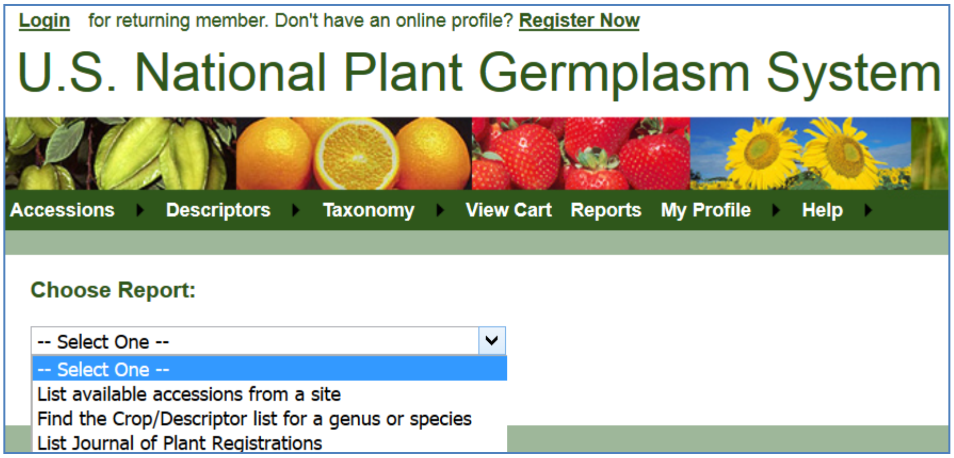


Choose Report:

-- Select One --

-- Select One --
Accession - List Accessions without a specific trait
Accession - Statistics Report (Accessions Count) by Country
Accession - Statistics Report (Accessions Count) by Genus
Accession - Statistics Report by country for Genus or Species
List available accessions from a site
Cooperator - Collector/Donor/Developer Report
Export - Fieldbook in CSV Format
Find the Crop/Descriptor list for a genus or species
Search associated species by taxon
List accessions for a genus that have no viability tests
List Journal of Plant Registrations
List users at site
Order - Packet Label
Order - Label Generation for site S9
Order - Acessions flagged with SMTA
Web Order Detail

Reports available to the public users:


Login for returning member. Don't have an online profile? Register Now
U.S. National Plant Germplasm System
Accessions
Descriptors
Taxonomy
View Cart
Reports
My Profile
Help
Choose Report:
-- Select One --
-- Select One --
List available accessions from a site
Find the Crop/Descriptor list for a genus or species
List Journal of Plant Registrations

Security

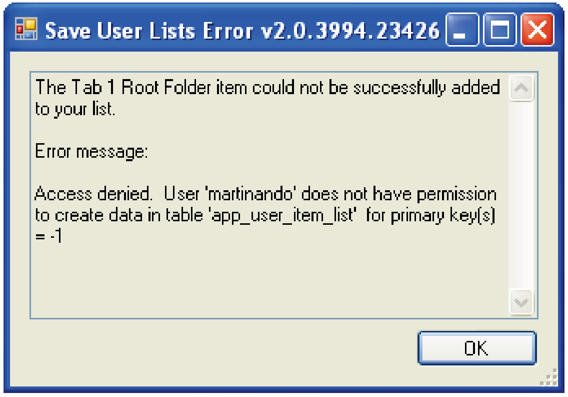
In general terms, there are three security alternatives to be considered:

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:

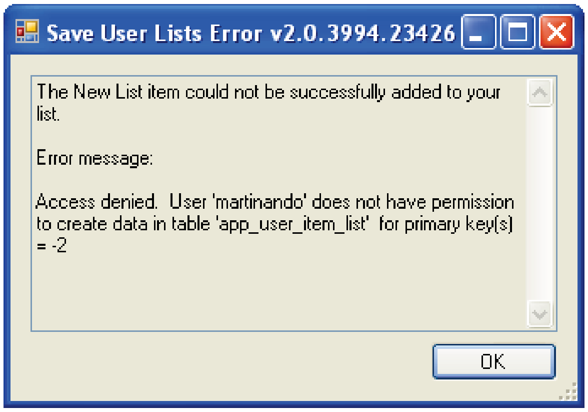


The Tab 1 Root Folder item could not be successfully added to your list.

Error message:

Access denied. User 'martinando' does not have permission to create data in table 'app_user_item_list' for primary key(s) = -1

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



The New List item could not be successfully added to your list.

Error message:

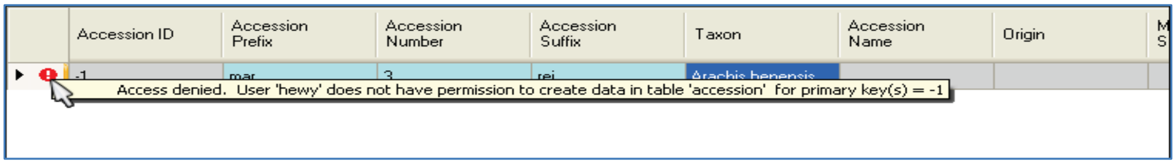
Access denied. User 'martinando' does not have permission to create data in table 'app_user_item_list' for primary key(s) = -2

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.

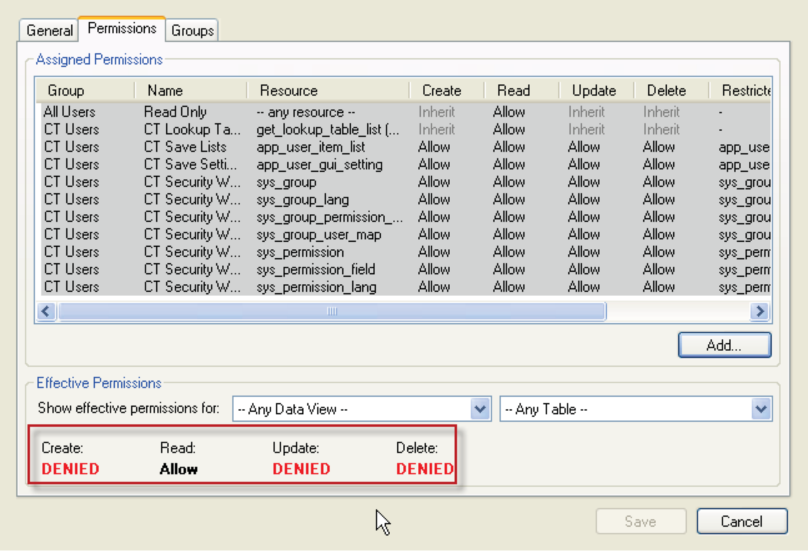
For example, a message similar to the following will be displayed after a failed Save action:



	Accession ID	Accession Prefix	Accession Number	Accession Suffix	Taxon	Accession Name	Origin	M S
▶	-1	mar	3	rei	Arachis henensis			

Access denied. User 'hewy' does not have permission to create data in table 'accession' for primary key(s) = -1

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

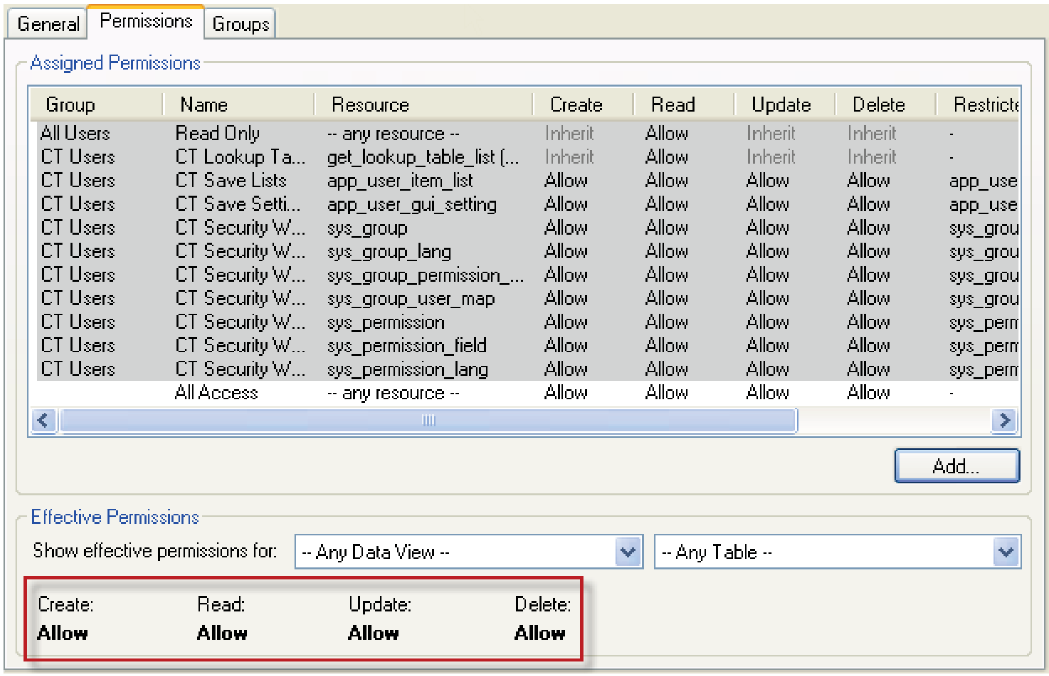


Group	Name	Resource	Create	Read	Update	Delete	Restricte
All Users	Read Only	-- any resource --	Inherit	Allow	Inherit	Inherit	-
CT Users	CT Lookup Ta...	get_lookup_table_list (...	Inherit	Allow	Inherit	Inherit	-
CT Users	CT Save Lists	app_user_item_list	Allow	Allow	Allow	Allow	app_use
CT Users	CT Save Setti...	app_user_gui_setting	Allow	Allow	Allow	Allow	app_use
CT Users	CT Security W...	sys_group	Allow	Allow	Allow	Allow	sys_grou
CT Users	CT Security W...	sys_group_lang	Allow	Allow	Allow	Allow	sys_grou
CT Users	CT Security W...	sys_group_permission_...	Allow	Allow	Allow	Allow	sys_grou
CT Users	CT Security W...	sys_group_user_map	Allow	Allow	Allow	Allow	sys_grou
CT Users	CT Security W...	sys_permission	Allow	Allow	Allow	Allow	sys_perm
CT Users	CT Security W...	sys_permission_field	Allow	Allow	Allow	Allow	sys_perm
CT Users	CT Security W...	sys_permission_lang	Allow	Allow	Allow	Allow	sys_perm

Show effective permissions for: -- Any Data View -- -- Any Table --

Create:	Read:	Update:	Delete:
DENIED	Allow	DENIED	DENIED

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:



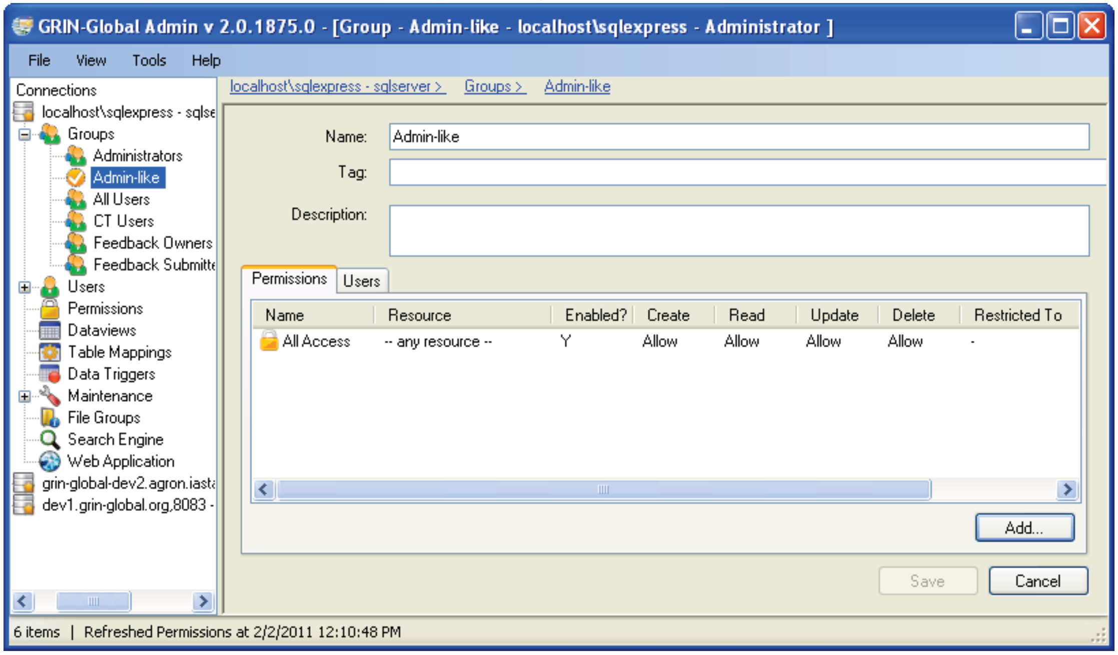
Group	Name	Resource	Create	Read	Update	Delete	Restricte
All Users	Read Only	-- any resource --	Inherit	Allow	Inherit	Inherit	-
CT Users	CT Lookup Ta...	get_lookup_table_list (...	Inherit	Allow	Inherit	Inherit	-
CT Users	CT Save Lists	app_user_item_list	Allow	Allow	Allow	Allow	app_use
CT Users	CT Save Setti...	app_user_gui_setting	Allow	Allow	Allow	Allow	app_use
CT Users	CT Security W...	sys_group	Allow	Allow	Allow	Allow	sys_grou
CT Users	CT Security W...	sys_group_lang	Allow	Allow	Allow	Allow	sys_grou
CT Users	CT Security W...	sys_group_permission_...	Allow	Allow	Allow	Allow	sys_grou
CT Users	CT Security W...	sys_group_user_map	Allow	Allow	Allow	Allow	sys_grou
CT Users	CT Security W...	sys_permission	Allow	Allow	Allow	Allow	sys_perm
CT Users	CT Security W...	sys_permission_field	Allow	Allow	Allow	Allow	sys_perm
CT Users	CT Security W...	sys_permission_lang	Allow	Allow	Allow	Allow	sys_perm
	All Access	-- any resource --	Allow	Allow	Allow	Allow	-

Show effective permissions for: -- Any Data View -- -- Any Table --

Create:	Read:	Update:	Delete:
Allow	**Allow**	**Allow**	**Allow**

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:


GRIN-Global Admin v 2.0.1875.0 - [Group - Admin-like - localhost\sqlexpress - Administrator]

Name: Admin-like

Tag:

Description:

Name	Resource	Enabled?	Create	Read	Update	Delete	Restricted To
All Access	-- any resource --	Y	Allow	Allow	Allow	Allow	-

6 items | Refreshed Permissions at 2/2/2011 12:10:48 PM

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
```