Database Mapper User Permissions

Last Modified on 06 October 2021

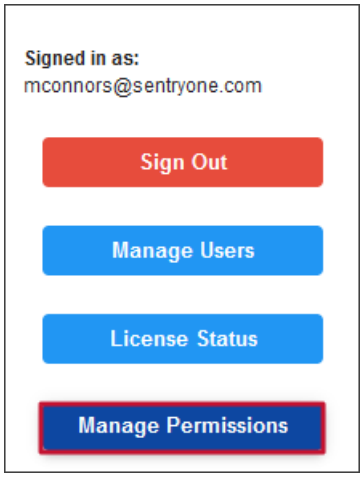
📢 **Update:** SentryOne Document is now SolarWinds Database Mapper (DMR). See the Database Mapper product page to learn more about features and licensing. Want to explore Database Mapper? An interactive demo environment is available without any signup requirements.

Introduction

Database Mapper permissions may be set at the **user** or **group** level. Users are not required to belong to a group and they may be assigned to multiple groups. A *DEFAULT* **user** exists as a catch-all and initially has all permissions granted. See the sections below for accessing and customizing the permissions for your organization.

Accessing Permissions

1. Select the **Profile** button from the top navigation menu.
2. Select the **Manage Permissions** button from the options.



Permissions

Values

Granted

Represented by a blue checkbox. When the permissions box is checked, then the permission is granted.

Denied

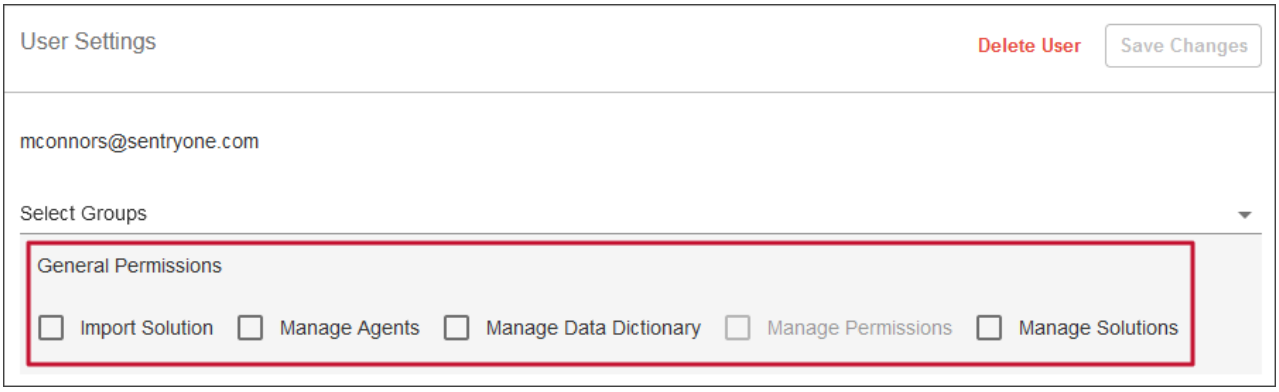
Represented by an X in an orange square. When the permissions box is x'd out, then the permission is denied.

Unset

Represented by an empty square. When the permission box is empty, then the permission is unset.

General Permissions

These are system-level permissions that are applied at the user or user group level. General permissions are not tied to specific solutions. They provide access to top-level functionality for the Organization.



Import Solution

Grants the ability to import a solution from DOC xPress.

Manage Agents

Grants the ability to install and configure remote agents.

If **denied**, the user:

- Can view the list of remote agents.
- Cannot perform **Edit Description**, **Change Pool Assignment**, **Delete** actions on the remote agents.
- Cannot perform **Create**, **Edit**, or **Delete** actions on the remote agent pools.
- Cannot perform **Change Pool Assignment** action for solutions or solution items.
- Cannot install a remote agent using their account.

> **Note:** Changing pool assignments requires a combination of **Manage Solutions** and **Solution Access**.

Manage Data Dictionary

Grants the ability to configure the Data Dictionary.

If **denied**, the user:

- Can view the **Categories**, **Global Entries**, **Value Lists**, and **Grid View** pages for Data Dictionary.
- Cannot perform actions to **Create**, **Edit**, or **Delete** any **Categories**, **Global Entries**, or **Value Lists**.

Note: This permission does not control the ability to **edit** Data Dictionary values for a solution. See **Data Dictionary Edit** under the Securable Permissions section for available controls.

Manage Permissions

Grants the ability to access the **Permissions** page and edit permissions for the organization.

Note: The **Manage Permissions** option for the current user is disabled to prevent a user from removing their own ability to manage permissions. Since permissions can be inherited from other places, like **Groups** or via the *DEFAULT* user where that checkbox won't be disabled, proposed changes will be validated and the changes will be rejected if they would result in the current user losing their **Manage Permissions** access.

Manage Solutions

Grants the ability to **Add**, **Edit** or **Delete** solutions via the **Solution Configuration Tool** and the ability to manage which **Agent Pool** is assigned for a solution.

Note: Changing pool assignments requires a combination of **Manage Solutions** and **Solution Access**.

Securable Permissions

Securable permissions are those that that apply to specific objects (the *securables*) within the organization. In Database Mapper, this relates to restricting permissions on a per solution basis.

Securable permissions can be set:

- At the **Organization** level, which then inherit down to all solutions.
- At the **Solution** level, which overrides the permission set at **Organization** level

Note: The minimum permission required to be able to view a solution, is **Solution Access**. The extra permissions listed grant additional rights on the solution.

Data Dictionary Edit

Data Dictionary Edit grants the ability to edit the data dictionary values for a solution via the **Documentation** page or the **Data Dictionary Grid View** page. If **denied**, the data dictionary values are read-only.

Export

Export grants the ability to request an export. If **denied**, the **Export** button on the **Solutions** page is disabled.

Manage Endpoint Aliases

Manage Endpoint Aliases grants the ability to configure endpoints aliases for the solution. If **denied**, the **Manage Endpoint Aliases** button on the **Solutions** page and **Lineage** page is disabled.

Snapshot Request

Snapshow Request grants the ability to take a snapshot for the solution. If **denied**, the **Configure Snapshot** button on the **Solutions** page is disabled

Solution Access

Solution Access grants the ability to see the solution in the **Solution Configuration Tool** and **Database Mapper**. This is the minimum permission required to view the solution.

> ℹ **Note:** When you add a solution via the **Configuration Tool**, the current user adding the solution will be explicitly assigned full permissions to that solution at their user level. If you're already in **Database Mapper** when you add the solution and the solution appears with the snapshot button disabled, refreshing the page should pick up the updated permissions.

Order of Precedence

Permissions are checked in order of precedence starting at the most specific level (the user) then proceeding to the most general level as follows:

1. User level permissions for the specific user. If none exist, then
2. User group level permissions for specific user groups to which the user belongs. If none exist, then
3. User level permissions for the *DEFAULT* user. If none exist, then
4. User group level permissions for the *DEFAULT* user for the groups to which the *DEFAULT* user belongs.

Adding Users

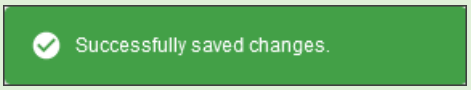
> ℹ **Note:**
>
> - Users will be added to the list automatically the first time they access the Database Mapper site. They will inherit the *DEFAULT* permissions.
>   - The **Add** option allows you to add users with specific permissions before they access the site. If they have already accessed the site, follow the instructions for editing a user if you want to modify their permissions from the default.
> - Regarding access:

- **Database Mapper Cloud**: This does not add a user to the organization. Users must already exist in the organization to access Database Mapper. Use Manage Users to add or remove users.
- **Database Mapper Software**: This does not grant access to Database Mapper. If someone is on the same domain as Database Mapper and can access the web server, then they can access the site by default.

To manually add a user's permissions:

1. Select the **Add** option under the **Users** section.
2. Enter a **User Id**.
    - **Note:** For **Database Mapper Cloud**, this is the user's associated email address that matches the one used in Organization Settings. For **Database Mapper Software**, this is the user's associated Windows account (e.g. *DOMAIN**username*).
3. Enter permission choices or leave as-is to accept the *DEFAULT* user permissions.
4. Select the **Save Changes** option.

Success: You have added a user with the associated permissions.

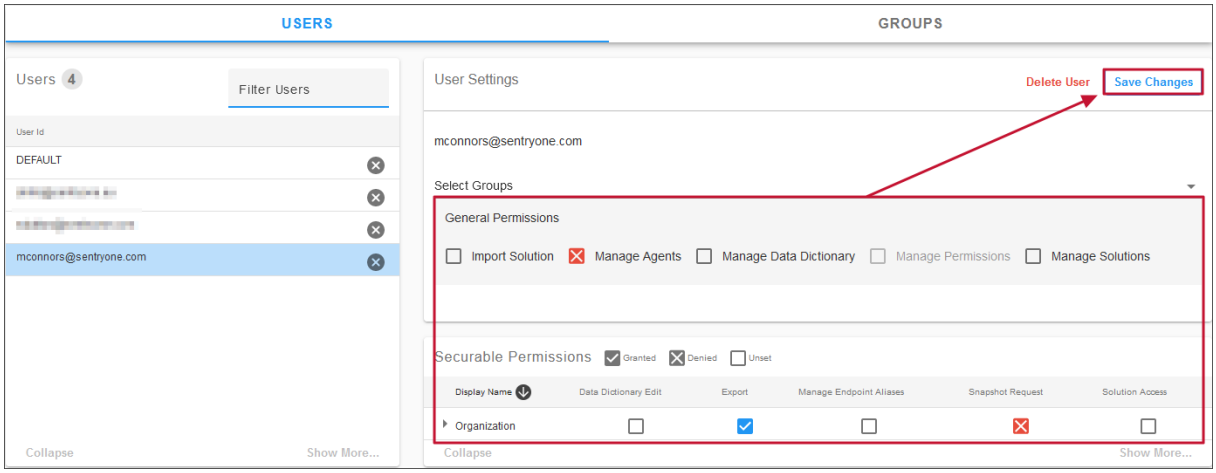


Editing User Permissions

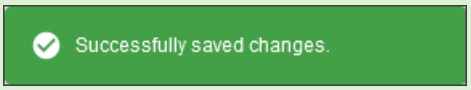
The **Permissions** page is in **Edit** mode by default.

To change permissions:

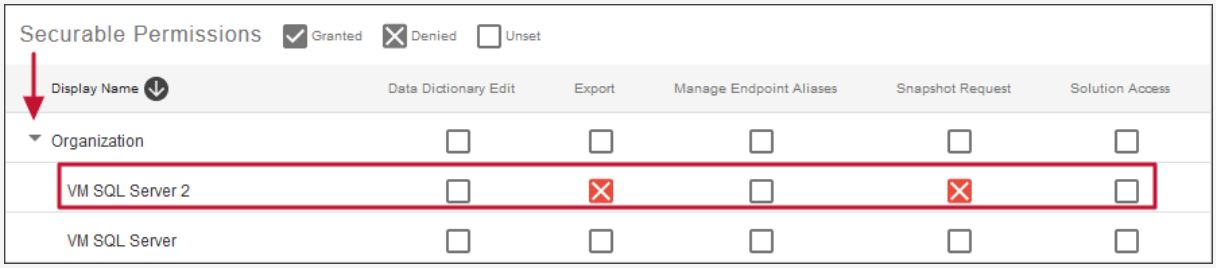
1. Select a user from the **User Id** list.
2. Edit General Permissions and Securable Permissions as needed.
3. Select the **Save Changes** button (which is enabled when changes exist to save).



Success: You have updated the permissions for a user.



Note: Expand the **Organization** list to set permissions at the **Solution** level instead of the **Organization** level.



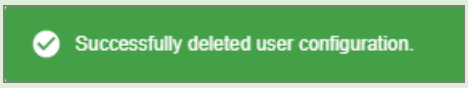
Deleting User Configurations

Note:

- Once a user is in the list for permissions, they cannot be fully deleted from the permissions page.
  - Use the available permissions to control their access to Database Mapper.
  - To remove access:
    - **Database Mapper Cloud**: This does not delete a user from the organization. Use Manage Users within Organization Settings to block their access.
    - **Database Mapper Software**: If someone is on the same domain as Database Mapper and can access the web server, then they can access the site by default. Use your Windows security policies to block access.

1. Select the ⊗ next to a user name (or the **Delete User Configuration** option under **User Settings**) to delete configured permissions for a user.
2. A confirmation popup message will display with the text "*Are you sure you want to delete the permissions for [USER]? This will reset them to have the DEFAULT user permissions.*" Select **OK** to reset the configured permissions for the user.

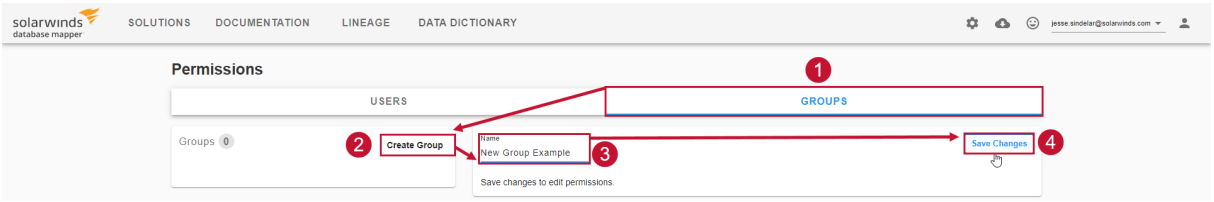
🏆 **Success:** You have reset the user permissions.



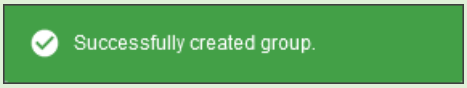
Creating User Groups

To create a new user group:

1. Select **Groups** on the **Permissions** page.
2. Select **Create Group** text.
3. Select the **Name** text, then enter a name for the **Group**.
4. Select the **Create Group** button.



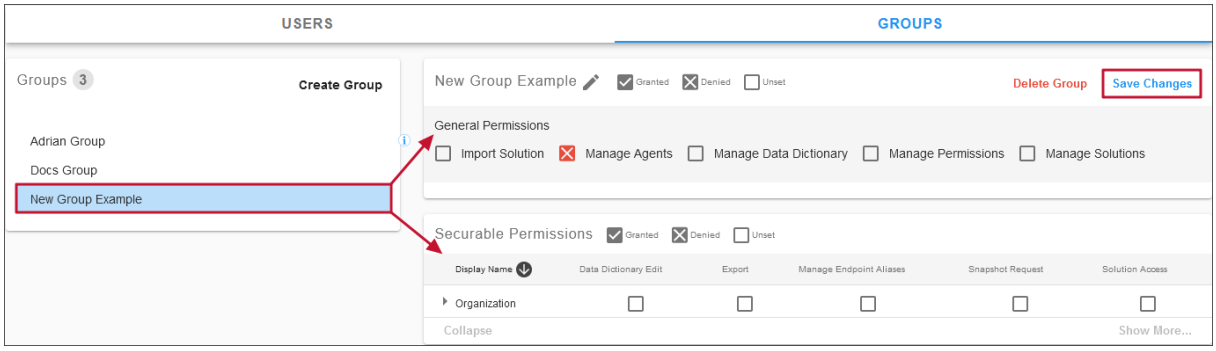
🏆 **Success:** You have created a user group.



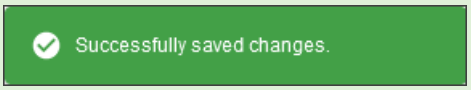
Editing Users Groups

The **Permissions** page is in **Edit** mode by default.

1. Select the user group from the **Groups** list.
2. Make changes to **General Permissions** and **Securable Permissions**.
3. Select the **Save Changes** button.



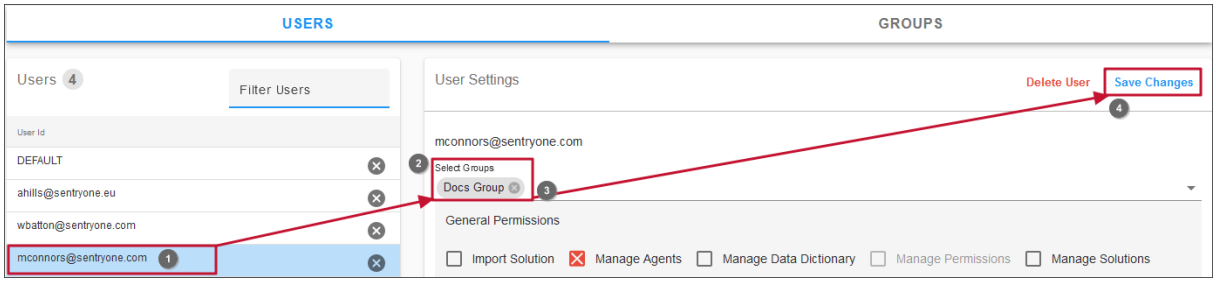
Success: You have updated the permissions for a user group.



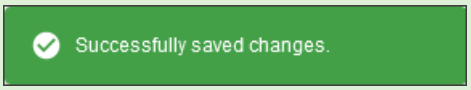
Adding Users to Groups

To add a user to a user group:

1. Select the user from the **User Id** list.
2. Select the **Select Groups** text.
3. Select a **Group** from the **Select Groups** drop-down list.
4. Select the **Save Changes** button.

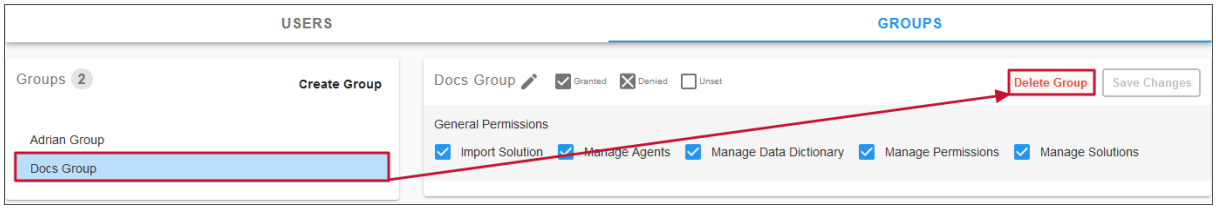


Success: You have added a user to a group.



Deleting User Groups

1. Select the user group from the **Groups** list.
2. Select the **Delete Group** text.



3. Select **OK** on the **Are you sure you want to delete [Group Name]?** confirmation window.

Success: You have deleted a user group.