Security Setup

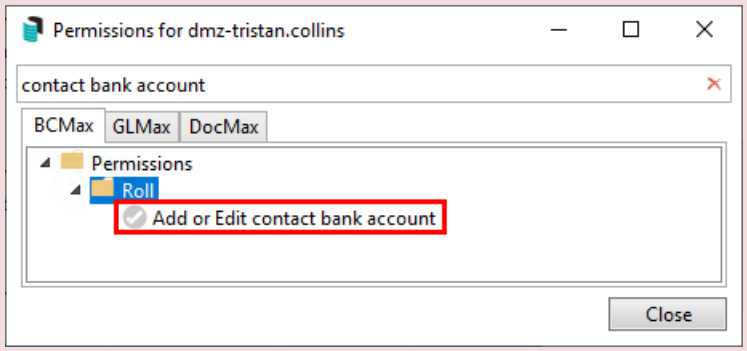
Last Modified on 30/09/2024 3:32 pm AEST

The instructions in this article relate to ***Security Setup.*** The icon may be located on your *StrataMax Desktop* or found using the *StrataMax Search*.

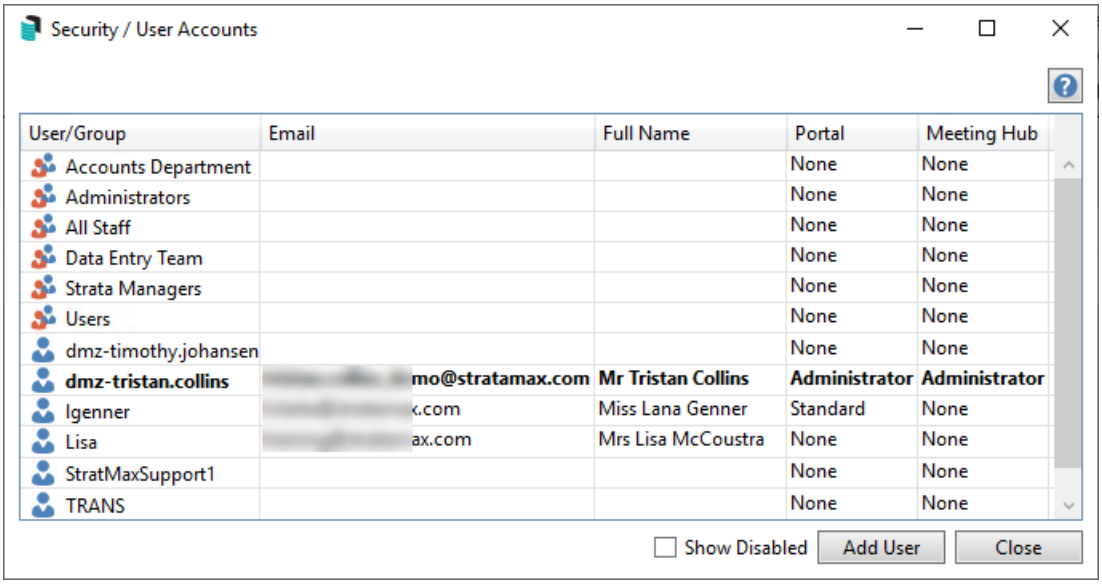
Security in StrataMax has been designed to mimic the Microsoft Windows security model - with *Groups* and *Users*, and inherited permission. Permissions determine the access to menus or functions, and can be applied to *Users,* to *Groups,* or to a specific building. Only *Users* that are in the *Administrators* group or have 'Allow' access to the *Administration* permissions can access ***Security Setup.***

Security Setup is also where access to the *StrataMax Portal* or ***Meeting Hub*** is set up, and where the details for each *User* are determined.

Due to the increased incidents of hacking and invoice fraud we would like to highlight a very important StrataMax permission that every business should review and implement; 'Add and edit contact bank account'. This is in order to limit the staff that are involved in this particular task, and should be incorporated into your own in office processes for manual independent verification of account and BSB changes. See this *Email Invoice Fraud Article* for important information around this topic.



Security Setup | Overview

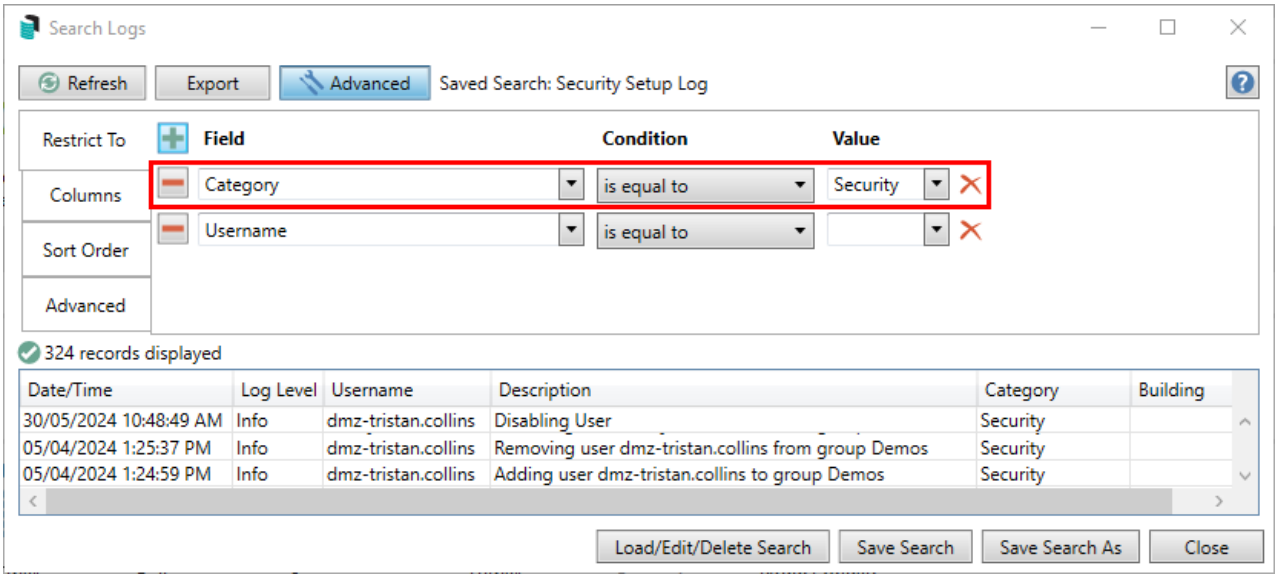


When ***Security Setup*** is opened, a list of the current *Users* and *Groups* appears:

- This icon  represents an individual *User*.
- This icon  represents a *Group*, which contains *Users*.
- This icon  represents a *User* that has been disabled, and will be visible in the list if the 'Show Disabled' box is ticked.
- The 'Email' column states the user's e-mail address, which is used for the user's StrataMax account, including access to the *StrataMax Portal* and ***Meeting Hub***.
- The 'Full Name' column is used to identify the user in the event the *Username* is generic or ambiguous like 'User 1' for example.
- The 'Portal' column indicates the level of access the *User* has in the *StrataMax Portal*; this can be 'None', 'User', or 'Administrator'.
- The 'Meeting Hub' column indicates the level of access the *User* has in ***Meeting Hub***; this can be 'None', 'User', or 'Administrator'.
- The 'Show Disabled' box can be ticked to display disabled *Users*, identified by a  icon.
- The *Add User* button provides the ability to create a new StrataMax User. To learn how to create a new user, see *Creating a new StrataMax User Account*.

Security Setup | Log

To check who has made any changes to ***Security Setup,*** have a look in the Log Viewer. In here you can review any changes that have been made to any *Users* and *Groups*.
Upon opening the ***Log Viewer***, change the 'Value' drop-down for the 'Category' field to 'Security' and click the *Refresh* button in the top left to display items. You can also change the filters, for example you can change the 'Date/Time' value to *Specific Dates* (tick the box), or choose a period from the drop-down menu. See the *Log Viewer article* for more info.

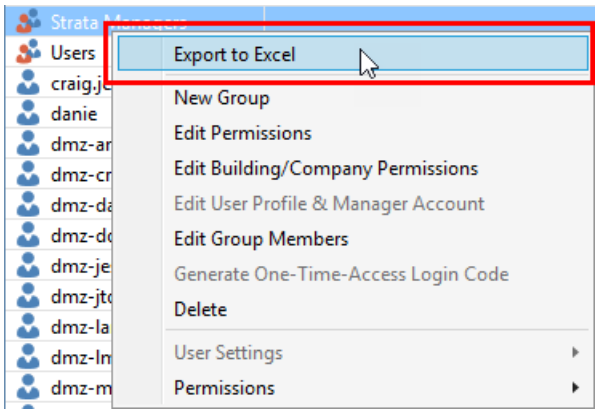


Security Setup | Export to Excel

There is a function to export all the security information available in StrataMax to an Excel worksheet. The sheet contains multiple tabs with each tab breaking down which users have access to menus in StrataMax, DocMax, and GLMax, as well as which features for each, and which buildings. It also details the permissions for each *Group*.

This sheet is extremely useful when reviewing and configuring permissions for staff members in order to ensure they have the appropriate access to the menus and functions they need to perform their role.

To do this, simply right-click on any *User* or *Group* and in the context menu select 'Export to Excel'.



Security Permissions Explained

In order for permissions to be more manageable, the StrataMax security model is based on a hierarchy system, which allows for *inherited* permissions. Essentially this means that certain permissions "trump" others. The examples below have been given to explain this better and are presented in a *lowest to highest* order:

Users may need to close StrataMax by right clicking on the StrataMax icon in the Windows System Tray (bottom right of screen) and selecting Exit and reopen for new permissions to take affect.

Inherit (Lowest Level)

Inherit is represented by no icon in ***Security Setup***, and it has lowest authority on a permission. This means:

- When a permission on a user is set to *inherit*, the system will observe the group permission to determine access.
- When *inherit* is used in a work group, the system will observe the group member's individual permission to determine access.
- When the user and the group have a permission set to *inherit*, then the system will not grant any access to that menu or function.

Allow

Gives the *User* or *Group* access to the function or menu.

Deny (Highest Level)

- Does not allow the *User* or *Group* to access the process or menu.
- Deny is the highest.
- Also refer to the supporting information and examples for setup of security.

Hierarchy Examples

Example 1

John is part of the 'Accounts Receivable' *Group*. Within this *Group,* access to ***GLMax*** has been set to 'Inherit' (a blank value). John's individual *User* permission has been set to 'Allow'. As 'Allow' is a higher value, John will have access to ***GLMax***. All other users in the 'Accounts Receivable' *Group* will not have access to ***GLMax***.

	Lowest →		Highest
	Inherit	Allow	Deny
John (user)		X	
Accounts Receivable (user group)	X		

Example 2

John is part of 'Accounts Receivable' *Group*. Within this *Group*, access to ***TaskMax*** has been set to 'Inherit'. John's individual *User* permission has been set to 'Deny', which is prioritised by the system because John's individual user is set to 'Deny', he will not have access to ***TaskMax***.

	Lowest →		Highest
	Inherit	Allow	Deny
John (user)			X
Accounts Receivable (user group)	X		

Example 3

If John belongs to two or more groups, access to processes and menus will be determined from the highest value per the hierarchy system. For example if the 'Accountants Receivable' *Group* has set ***GLMax*** to 'Inherit' and the 'Accountant' *Group* is set to 'Allow' John will be have access to ***GLMax*** as this is the highest value in the hierarchy.

	Lowest →		Highest
	Inherit	Allow	Deny
John (user)		X	
Accounts Receivable (user group)	X		
Accountant		X	

Example 4

John will have no access if the permission setting for both the *Group* he is in, and his individual setting has been set to 'Inherit'.

	Lowest		Highest
	Inherit	Allow	Deny
John (user)	X		
Accounts Receivable (user group)	X		

StrataMax Groups

By default, there are two *Groups* in StrataMax; one called 'Administrators' and the other called 'Users'.

Users can also belong to more than one *Group,* however, the permissions for each *Group* should be compared as to not cause any conflict in permissions, resulting in unwanted access to certain menus and functions.

When adding or removing a *User* to or from a *Group*, it can alter their access to menus and functions. Which ones will depend on how that *Group's* permissions have been configured and how the *User*'s permissions are set. It will also affect:

- Visibility of StrataMax desktop icons: See *Creating a New Desktop Group* for more info.
- ***Dashboard*** icons.
- Visibility of *DocMax Work Queues* and *Saved Searches*.

'Users' Group

By default, each new users is added to the 'Users' *Group,* which is pre-configured with permissions to allow access to the all the basic menus and functions of StrataMax including ***GLMax*** and ***DocMax***. You should review and configure this *Group* as early as possible to ensure the right staff have the appropriate access.

'Administrators' Group

Any user belonging to this group will have full control in ***Security Setup*** and full permissions throughout StrataMax including ***GLMax*** and ***DocMax***. You should review and configure this *Group* as early as possible to ensure the right staff have the appropriate access.

It is not recommended to change the permissions for the 'Administrators' *Group*. Instead, you should remove any necessary *Users* from the *Group,* then create a new *Group* with the appropriate permissions.

Be aware that users in the 'Administrators' *Group* should be added to other *Groups* with care to prevent any conflicts in permissions, resulting in restricted access to menus and functions. For example, if adding a member to another *Group* to grant them access to a specific *DocMax Work Queue*, or group of *Dashboard Items*.

Create New Group

Setting up different *Groups* with differing permissions allows for greater control over which menus and functions are available to staff members, third/external parties, roles, or teams. For example, a new *Group* could be created for third party users, like auditors or search agents where only access to specific *Saved Searches* in ***DocMax*** are allowed.

1. Search or select ***Security Setup***.
2. Right-click any *Group* or *User* and select 'New Group' .
3. The 'Edit Security Group' window will appear, where you must:
    - Enter the *Group Name*. For example 'Accounts Payable' or 'Account Managers', etc.
    - Add the required members by ticking the box next to each *User* in the list and click the *Save* button.
4. You can then edit the permissions for this group to specify the access the members have to various menus and functions in StrataMax. See the '*Edit Permissions*' section for more info.

External Parties/Users Group

When external parties need access to certain areas of StrataMax or ***DocMax*** (most commonly *Saved Searches* to be able to see certain documents in ***DocMax***), it is recommended that a new group is created with specific permissions.

Before settings up a security group for external users, you will first need to contact your IT tech/consultant to set up usernames with passwords, and e-mail addresses for them on your StrataMax server (in Windows), if the external party is logging in remotely. The usernames should be easily identifiable, generic usernames such as 'extuser01' or similar, so that they can be used again and again by different companies - then you just need to ask your IT tech/consultant to reset the password once the current external user no longer should have access.

Once you receive the usernames and passwords from your IT tech/consultant, you'll need to follow the below steps as a StrataMax Administrator on a different PC or different remote desktop session. You will need to log into your StrataMax server with those credentials and test access to StrataMax, after you've sent them up with an account.

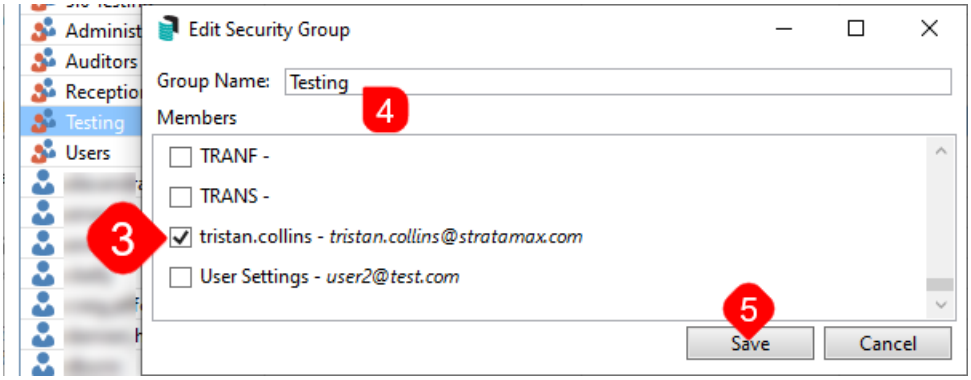
1. Search or select ***Security Setup***, and right-click any *Group* or *User* and select 'New Group'.
2. The 'Edit Security Group' window will appear, where you must:
    - Enter the *Group Name*. For example, 'External Parties', 'External Users', 'Auditors', or 'Search Agents', etc.
    - Add the external users by ticking the box next to each *User* in the list.
3. Click *Save* to close the 'Edit Security Group' window.
4. Now you will need to edit the permissions, making sure to only grant the 'Allow' permission for specific menus and/or features that you want external users to have access to. See the '*Edit Permissions*' section for more info.

Edit Group Members

This sub-menu is only available when right-clicking *Group*.

1. Search or select ***Security Setup***.
2. Right-click any *Group* and select 'Edit Group Members'.

3. The 'Edit Security Group' window will appear.
4. Add or remove the required members by ticking or unticking the box next to each *User* in the list.
5. You can also change the name of the *Group* by typing a new name into the 'Group Name:' field a the top.
6. Click *Save* to close the 'Edit Security Group' window.



StrataMax Users

This section details what *Users* are in StrataMax, how they are created, and how the permissions can be changed.

Create New Users

StrataMax Security Administrators have the ability to create a new user for new staff members who need to access StrataMax. Refer to our *Accessing StrataMax* article for more details.

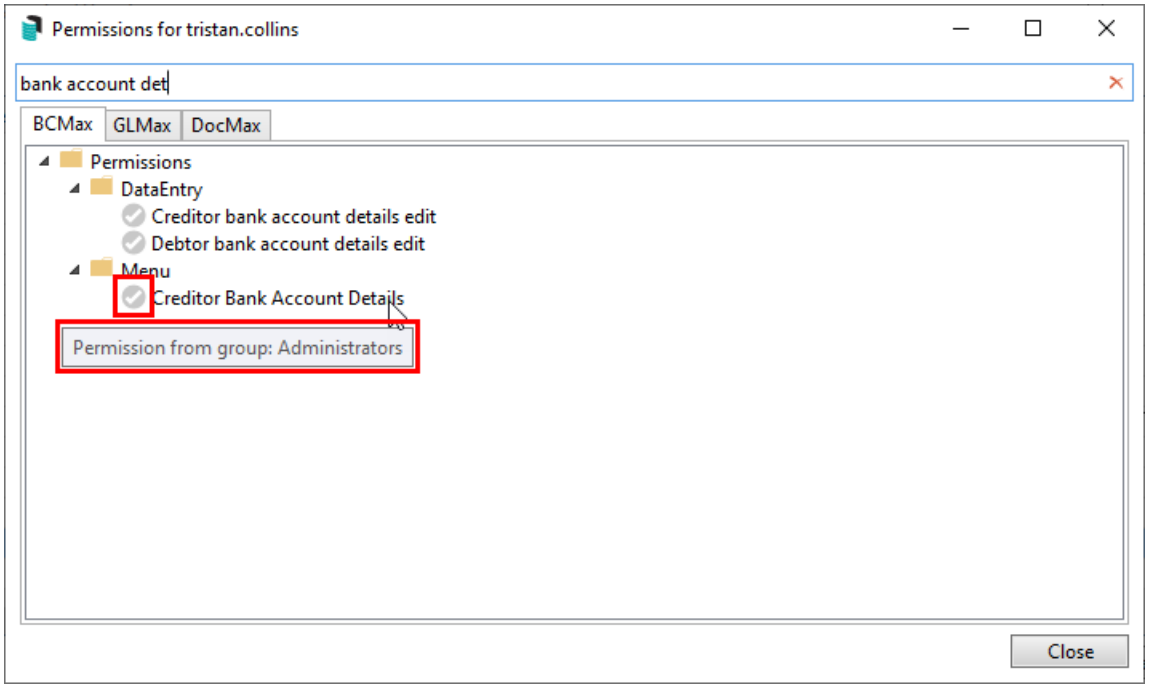
New *Users* are automatically added to the 'Users' *Group,* but they can also be added to other *Groups* and have their permissions set.

Edit User / Group Permissions

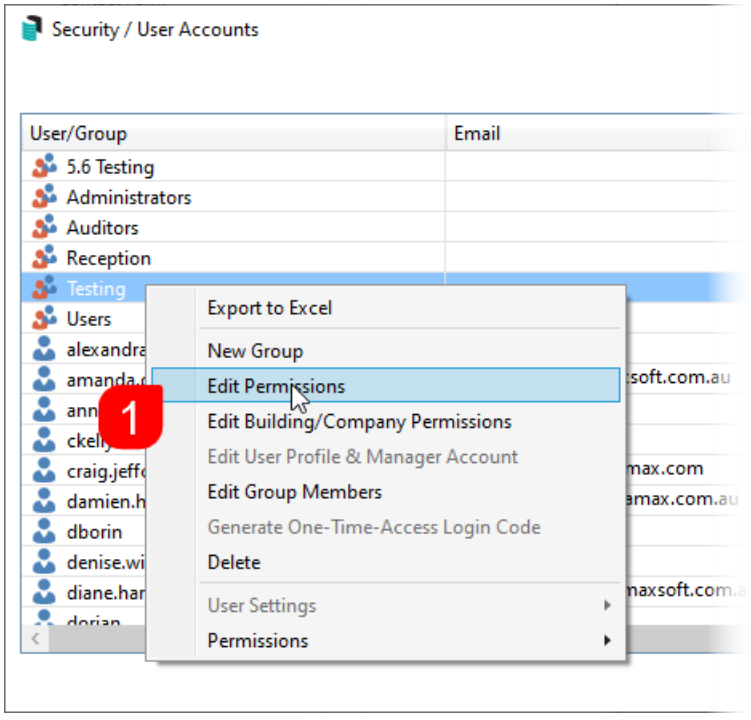
By configuring different *Groups* with appropriate permissions, you have greater control over which menus and functions are available to staff members, third/external parties, roles, or teams.

- It is recommended to start by configuring the permissions for each *User* with all menus and functions as 'Inherit'.
- Then in the *Group,* configure all the required permissions for menus and functions.
- If there are specific members of the *Group* that require access to other menus or functions that are otherwise restricted for this *Group*, these individual *Users* can have their own permissions set accordingly or be added to another *Group* that has access to those menus and functions.

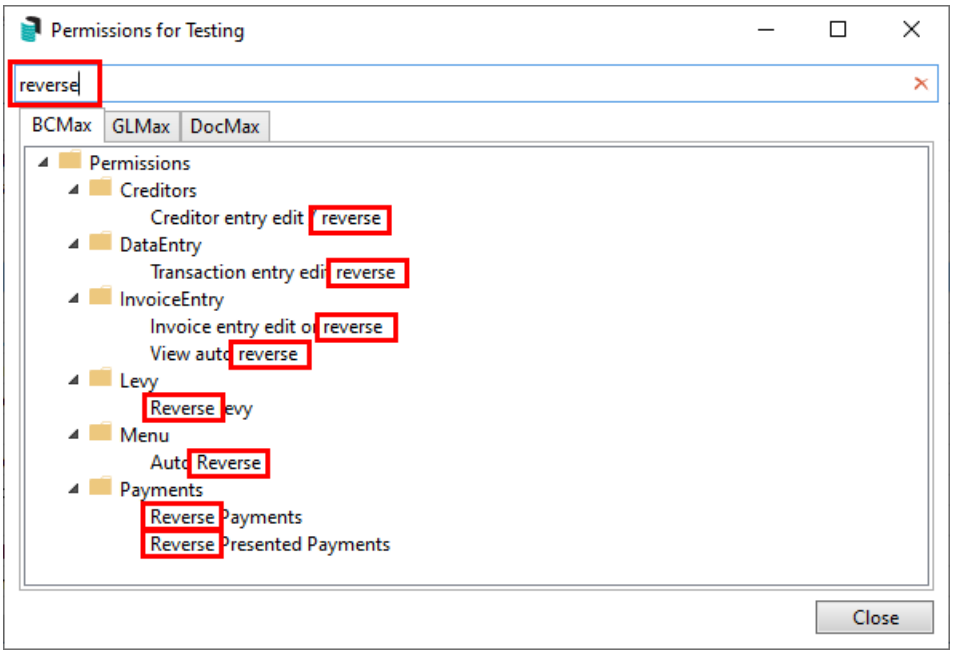
When changing permissions for a *User* or *Group*, if the permission's icon is in colour, it has been set in the *User* or *Group* you are checking.
However, when changing the permissions for an individual *User*, if the icon is grey, the permission has been inherited from a *Group*. To find out which *Group*, hover your mouse cursor over the permission.



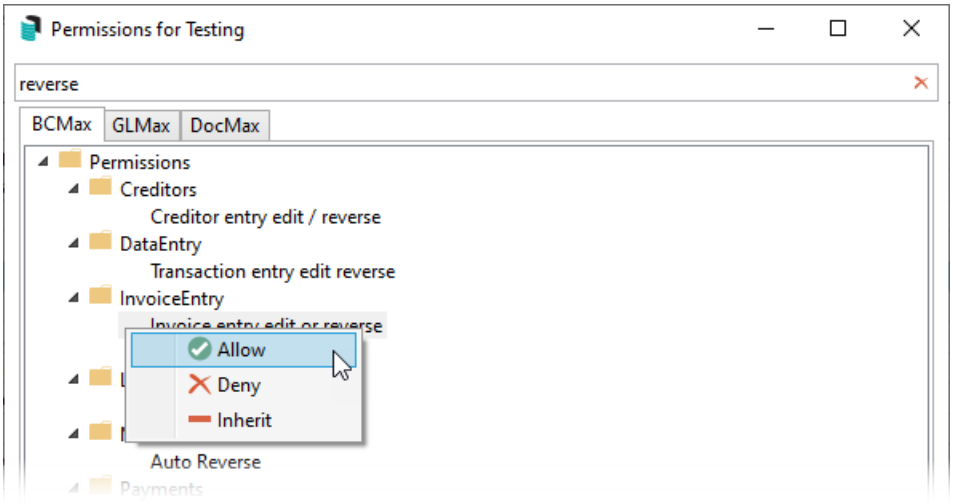
1. Right-click any *Group* and select 'Edit Permissions'.



2. In the *Permissions* window, select the required tab: *BCMax, GLMax, DocMax*. Each tab has its own list of permissions.
3. To locate the required permission, you can:
    - Expand each folder by clicking the little plus to the left of the folder.
    - Type part of the permission's name in the bottom-left field and click the *Filter* button. For example 'reverse'.



4. Once you have located the required permission, right-click it and set to *Inherit*, *Allow* or *Deny*.
    - See *Security Permissions Explained* for more info on each permission.

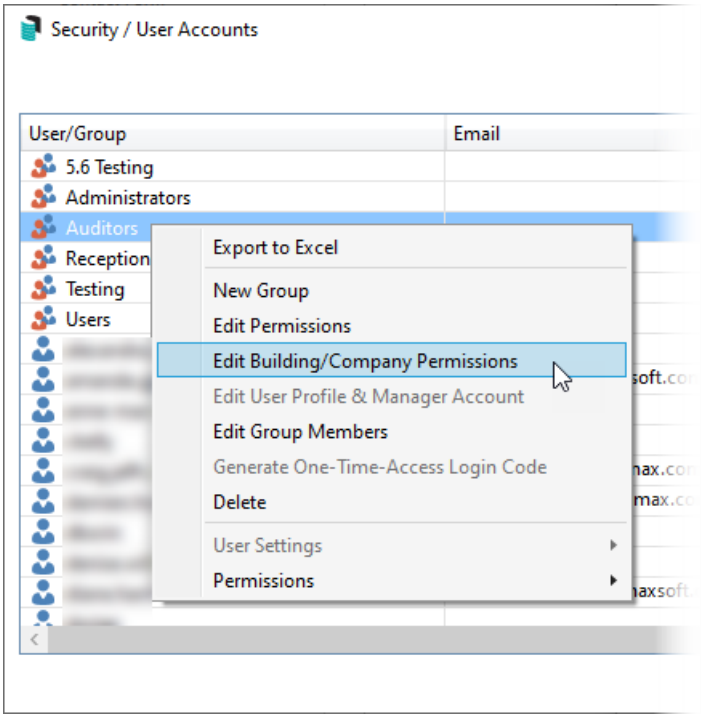


Edit Building/Company Permissions

This allows you to give permission to particular buildings in StrataMax or a company in ***GLMax***. Click on either the *BCMax* or *GLMax* tab.

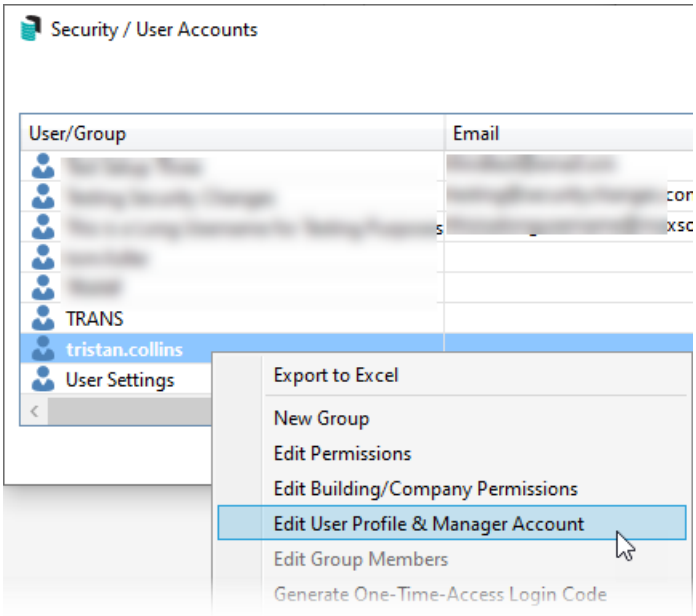
There is a *GLMax* permission setting in StrataMax to grant users access to *GLMax*, this is found in the *BCMax*

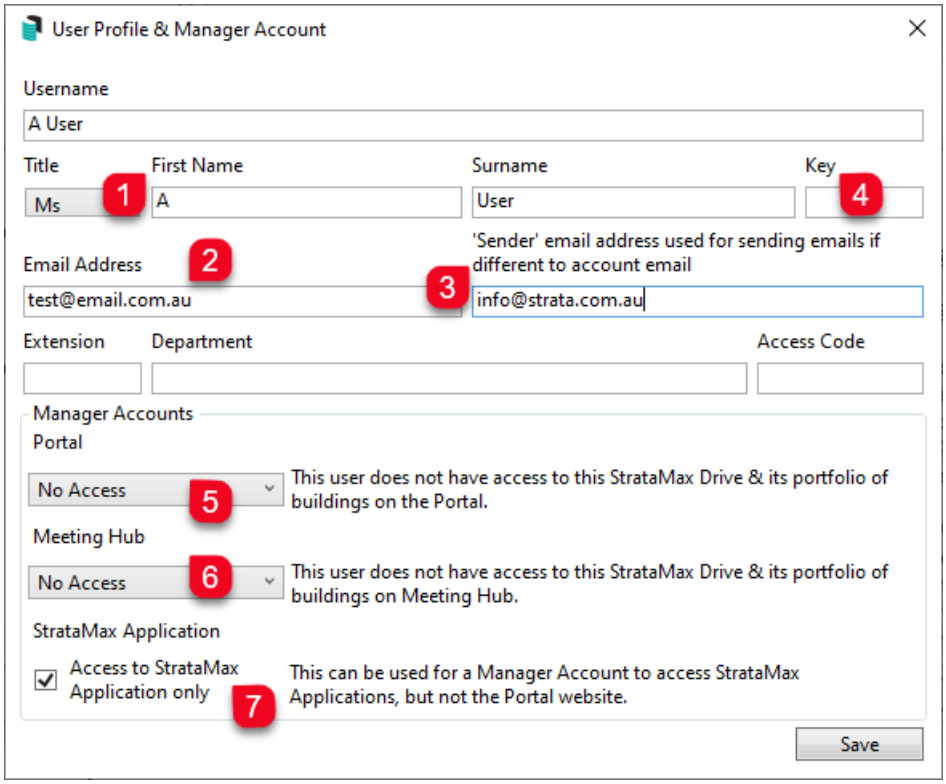
tab under the 'System' section and the permission is called 'Access to GLMax'. The 'Company Permission' is whether this company is accessible to the user or user group.



Edit User Profile & Manager Account

You can use this sub-menu to grant users to access the ***StrataMax Portal*** and the ***Meeting Hub***, and populate the 'Key' field in order to add this user as an *Operator* in ***TRMax*****.** This is also where you can configure a 'Sender' Email Address for sending emails from StrataMax.





1. When configuring this screen for the first time for a new user, the contents in the *First Name* and *Surname* fields will be combined and copied to the *Sender Name* field in ***Communications***, under *Options* > *Communications Setup*.
2. When configuring this screen for the first time for a new user, the *Email Address* field will be copied to the *Email Address* field in ***Communications***, under *Options* > *Communications Setup*.
3. If you would prefer to use a different "sender" address, then you can type it into this field. This field is also synced with the *Email Address* field in ***Communications***, under *Options* > *Communications Setup*, so if you update it there, it will display here.
4. The *Key* field is used to add the user as an *Operator* in ***TRMax***.
5. The *Portal* drop-down menu is to provide access to and set the appropriate access level on the StrataMax Portal. See *StrataMax Portal | Getting Access*.
6. The *Meeting Hub* drop-down menu is to provide access to and set the appropriate access level in Meeting Hub. See *Set Up Access to Meeting Hub*.
7. If the *Access to StrataMax Application only* box is ticked, no StrataMax Portal access will be granted. This setting is for users such as search agents, auditors, accountants as they do not require StrataMax Portal access.

Add User

StrataMax security administrators can create a new user for new staff members who need to access StrataMax. Refer to our *Accessing StrataMax* article for more details.

Delete Users/Groups

This option will allow you to delete a *User* or a *Group*. When the user is deleted, it will no longer be visible in drop-down lists or pick lists in StrataMax, including DocMax. However, the user will still be visible in reports and logs throughout StrataMax.

Deleting a group does not also delete the members of that group. It simply removes any permission that were in effect for that group.

1. Select the *User* or *Group*.
2. Right-click and select 'Delete'.

Copy User Settings

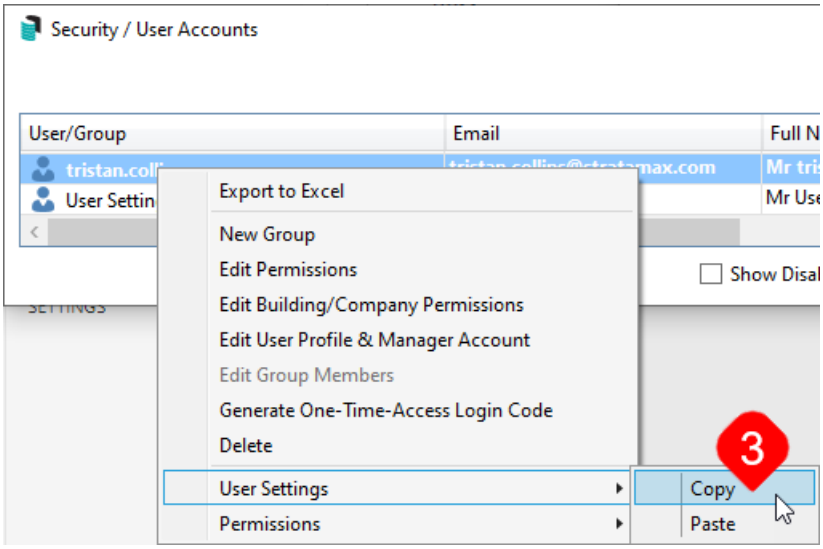
Use this option to replicate the *User* settings from one user to another, and across drives if you have multiple drives in your StrataMax. This tool allows the management of user settings when taking on new staff or to ensure existing staff have the same configuration setup across departments, with exception of the ***Communication*** *settings*.

> This feature will allow settings to be replicated to other users and across drives.

All configuration settings that show 'User Setting' are in:

- BCMax
- GLMax
- TaskMax
- TRMax
- DocMax

1. Search or select ***Security Setup***.
2. Right-click the user whose settings need to be copied.
3. Hover the mouse cursor over *User Settings* and click *Copy*.



4. Right-click the user who needs the settings applied to them, hover the mouse cursor over *User Settings* and click *Paste*.
5. Click *Yes* to confirm to override this user's settings.
    - The settings will be copied to the selected User, and an entry will be written to the StrataMax log to show any user that has had settings replaced.