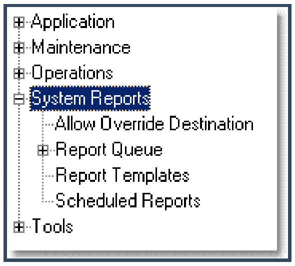
SWS - Forms in the Maintenance Menu - Permissions

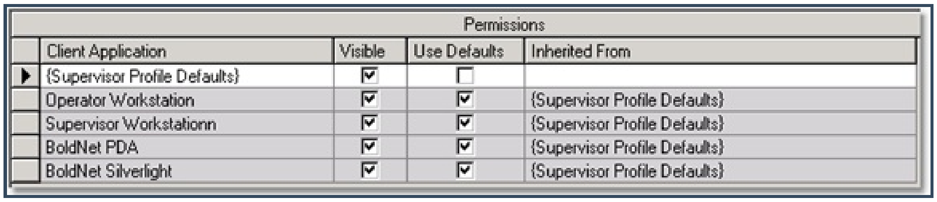
Last Modified on 08/07/2024 4:06 pm EDT

1. You want to change "System Reports" within the Supervisor Permissions Profile. You go into Edit mode, select the Supervisor Profile, and highlight System Reports:



```
⊞ Application
⊞ Maintenance
⊞ Operations
⊟ System Reports
      Allow Override Destination
    ⊞ Report Queue
      Report Templates
      Scheduled Reports
⊞ Tools
```

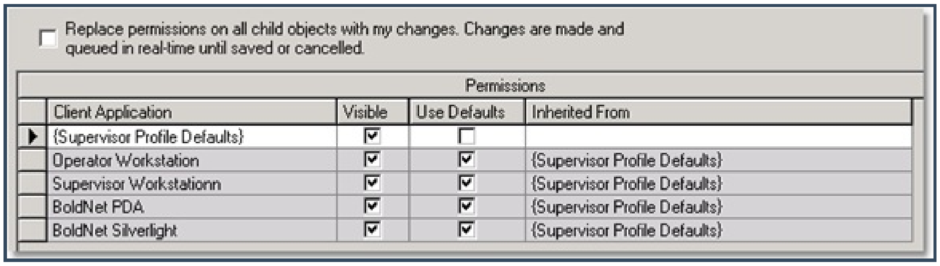
2. By default, the following permissions are set as follows:



Permissions

	Client Application	Visible	Use Defaults	Inherited From
▶	{Supervisor Profile Defaults}	☑	□	
	Operator Workstation	☑	☑	{Supervisor Profile Defaults}
	Supervisor Workstationn	☑	☑	{Supervisor Profile Defaults}
	BoldNet PDA	☑	☑	{Supervisor Profile Defaults}
	BoldNet Silverlight	☑	☑	{Supervisor Profile Defaults}

3. You want "Supervisor Profile Defaults" and every item under it (Allow Override Destination, Report Queue, etc.) to lose the ability to view the items. So you check the "Replace permissions on all child objects..." option and then select the top "Visible" checkbox which then removes the checkboxes on all of its child objects:

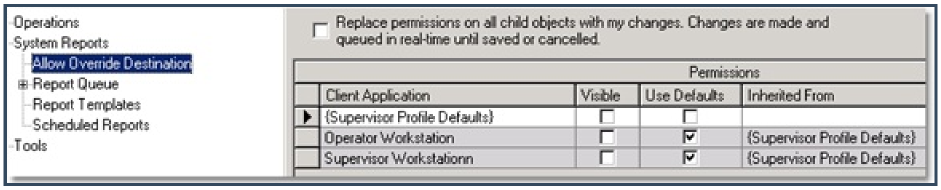


□ Replace permissions on all child objects with my changes. Changes are made and queued in real-time until saved or cancelled.

Permissions

	Client Application	Visible	Use Defaults	Inherited From
▶	{Supervisor Profile Defaults}	☑	□	
	Operator Workstation	☑	☑	{Supervisor Profile Defaults}
	Supervisor Workstationn	☑	☑	{Supervisor Profile Defaults}
	BoldNet PDA	☑	☑	{Supervisor Profile Defaults}
	BoldNet Silverlight	☑	☑	{Supervisor Profile Defaults}

4. When you drill down into System Reports you will see now that all of its child items have lost the visibility setting as well:



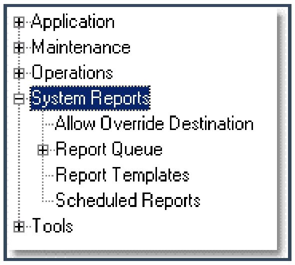
```
Operations
System Reports
    Allow Override Destination
  ⊞ Report Queue
    Report Templates
    Scheduled Reports
Tools
```

□ Replace permissions on all child objects with my changes. Changes are made and queued in real-time until saved or cancelled.

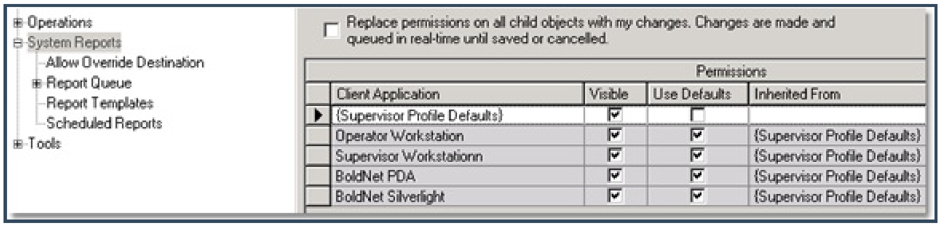
Permissions

	Client Application	Visible	Use Defaults	Inherited From
▶	{Supervisor Profile Defaults}	□	□	
	Operator Workstation	□	☑	{Supervisor Profile Defaults}
	Supervisor Workstationn	□	☑	{Supervisor Profile Defaults}

5. Next, you only want to change Visible capability for the Supervisor and Operator Workstations at the top "System Report" level only, leaving all child objects without this permission. Select "System Reports" again:



6. Then, in the Permissions table unselect the "Replace permissions on all child objects..." option then select the top "Visible" checkbox. Now only this top level has the Visible option enabled:

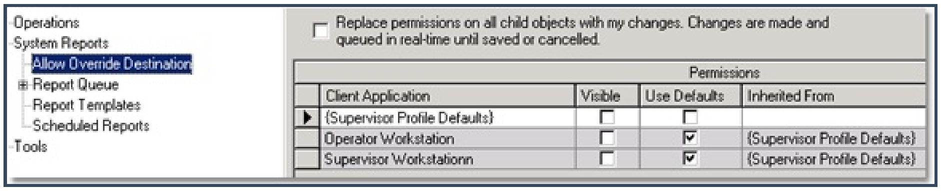


□ Replace permissions on all child objects with my changes. Changes are made and queued in real-time until saved or cancelled.

Permissions

Client Application	Visible	Use Defaults	Inherited From
{Supervisor Profile Defaults}	☑	□	
Operator Workstation	☑	☑	{Supervisor Profile Defaults}
Supervisor Workstationn	☑	☑	{Supervisor Profile Defaults}
BoldNet PDA	☑	☑	{Supervisor Profile Defaults}
BoldNet Silverlight	☑	☑	{Supervisor Profile Defaults}

7. Upon drilling down, you will find that all of its child objects have retained their setting:

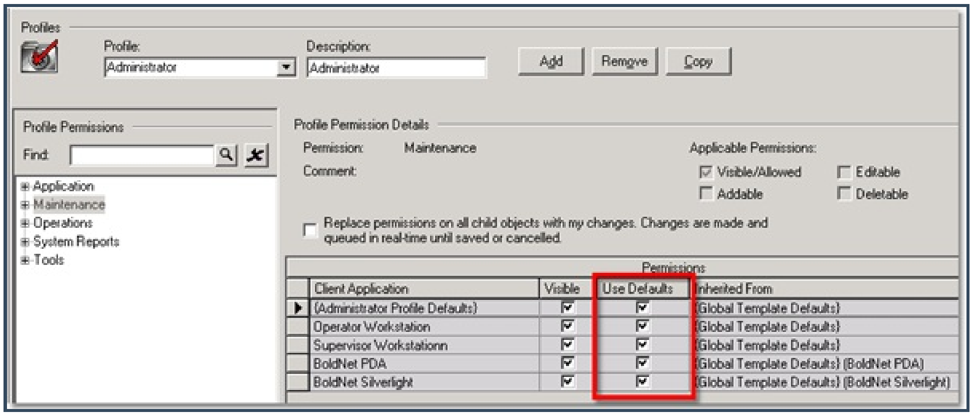


□ Replace permissions on all child objects with my changes. Changes are made and queued in real-time until saved or cancelled.

Permissions

Client Application	Visible	Use Defaults	Inherited From
{Supervisor Profile Defaults}	□	□	
Operator Workstation	□	☑	{Supervisor Profile Defaults}
Supervisor Workstationn	□	☑	{Supervisor Profile Defaults}

SWS 1.6.1 and later gives you the option to revert settings to a higher level setting. It is the "Use Defaults" setting, as follows:



Profile: Administrator

Description: Administrator

Find:

Permission: Maintenance

Comment:

Applicable Permissions:

☑ Visible/Allowed □ Editable

□ Addable □ Deletable

□ Replace permissions on all child objects with my changes. Changes are made and queued in real-time until saved or cancelled.

Permissions

Client Application	Visible	Use Defaults	Inherited From
{Administrator Profile Defaults}	☑	☑	{Global Template Defaults}
Operator Workstation	☑	☑	{Global Template Defaults}
Supervisor Workstationn	☑	☑	{Global Template Defaults}
BoldNet PDA	☑	☑	{Global Template Defaults} (BoldNet PDA)
BoldNet Silverlight	☑	☑	{Global Template Defaults} (BoldNet Silverlight)

"Use Defaults" uses hierarchy and inheritance in two (2) ways as follows:

8. When "Use Defaults" is selected in the first line of the Permissions table (for example in the picture above this would be "Template Profile Defaults") it will revert to the Profile level above itself - in this case it will revert to the Global Template Defaults.
9. Any items below the first line are considered child items, so clicking the "Use Defaults" checkbox on any of these child items will make them inherit permission from that top item. In the example above, Operator Workstation and all items below it are child items of the {Template Profile Defaults} item.

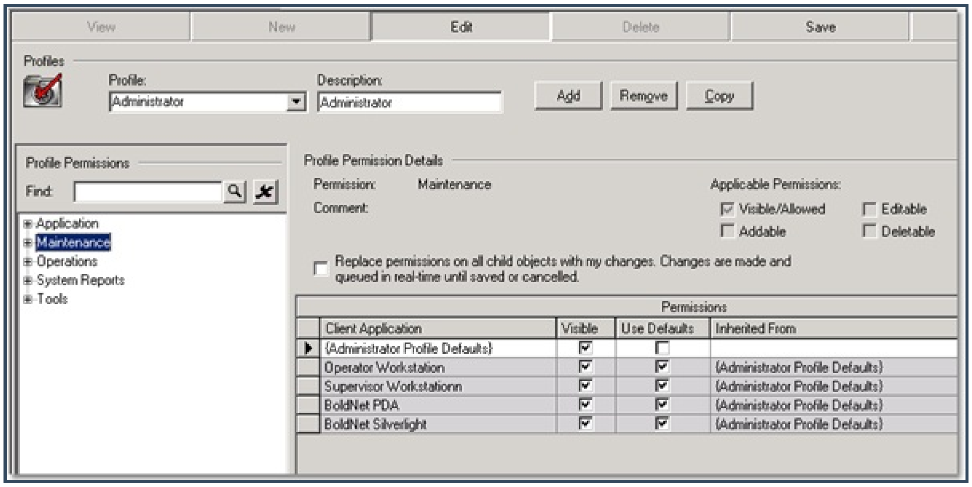
Note: The Global Template is the highest level template so if you are editing the Global Template, there is nothing higher to inherit so the "Use Defaults" checkbox is irrelevant.

Note: The "Replace permissions on all child objects..." checkbox will function as described in the previous section.

Example

Open Permissions Profiles and perform the following:

1. Highlight "Maintenance" on the left and change the drop-down Profile menu to "Administrator".



Profile: Administrator

Description: Administrator

Profile Permission Details

Permission: Maintenance

Comment:

Applicable Permissions:

☑ Visible/Allowed ☐ Editable

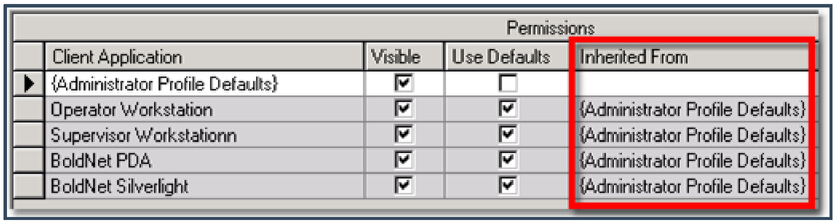
☐ Addable ☐ Deletable

☐ Replace permissions on all child objects with my changes. Changes are made and queued in real-time until saved or cancelled.

Permissions

	Client Application	Visible	Use Defaults	Inherited From
▶	{Administrator Profile Defaults}	☑	☐	
	Operator Workstation	☑	☑	{Administrator Profile Defaults}
	Supervisor Workstationn	☑	☑	{Administrator Profile Defaults}
	BoldNet PDA	☑	☑	{Administrator Profile Defaults}
	BoldNet Silverlight	☑	☑	{Administrator Profile Defaults}

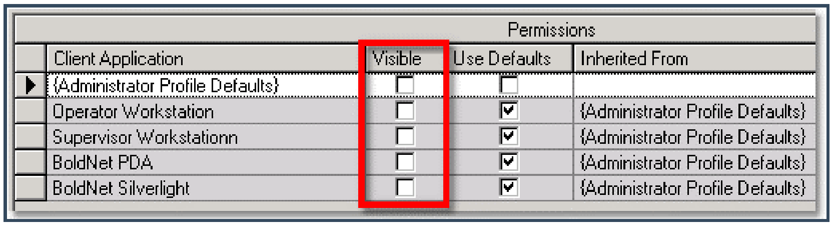
2. Then click Edit at the top.
3. Note that the "Inherited From" column gets its settings from the Administrator Profile (since this is the profile you have selected from the Profile drop-down menu):



Permissions

	Client Application	Visible	Use Defaults	Inherited From
▶	{Administrator Profile Defaults}	☑	☐	
	Operator Workstation	☑	☑	{Administrator Profile Defaults}
	Supervisor Workstationn	☑	☑	{Administrator Profile Defaults}
	BoldNet PDA	☑	☑	{Administrator Profile Defaults}
	BoldNet Silverlight	☑	☑	{Administrator Profile Defaults}

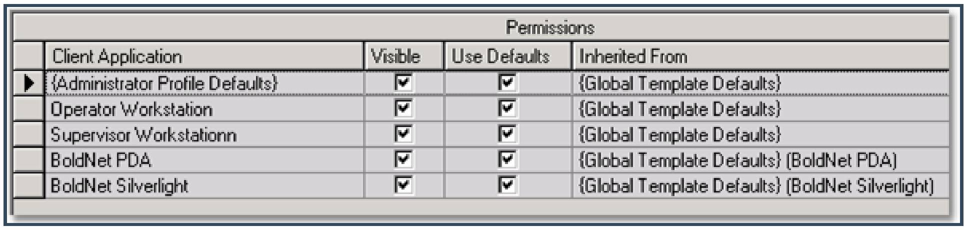
If you were to unselect the visible column on the top {Administrator Profile Defaults} line, all items that have the "Use Defaults" selected will lose the visible checkbox as well:



Permissions

	Client Application	Visible	Use Defaults	Inherited From
▶	{Administrator Profile Defaults}	☐	☐	
	Operator Workstation	☐	☑	{Administrator Profile Defaults}
	Supervisor Workstationn	☐	☑	{Administrator Profile Defaults}
	BoldNet PDA	☐	☑	{Administrator Profile Defaults}
	BoldNet Silverlight	☐	☑	{Administrator Profile Defaults}

Additionally, if you were to then select the "Use Defaults" checkbox from just the top "Administrator Profile..." line, every line below it would receive the same [Global Template] settings as follows:



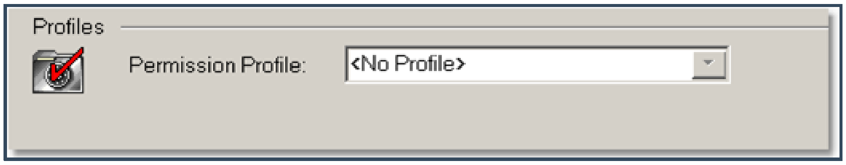
Permissions

Client Application	Visible	Use Defaults	Inherited From
{Administrator Profile Defaults}	☑	☑	{Global Template Defaults}
Operator Workstation	☑	☑	{Global Template Defaults}
Supervisor Workstationn	☑	☑	{Global Template Defaults}
BoldNet PDA	☑	☑	{Global Template Defaults} (BoldNet PDA)
BoldNet Silverlight	☑	☑	{Global Template Defaults} (BoldNet Silverlight)

On the other hand if you were to uncheck the "Use Defaults" column for any of the objects, they would lose the inheritance from the parent object and retain their own setting regardless of how their respective parent objects are configured going forward.

SWS 1.6.1 and later deals with user account and group permissions in a new way as well. To view some of these differences click on the Maintenance Menu -> Users Groups.

You will find that the "Permissions Profile" properties has been simplified, containing only one setting for an Operator Profile:

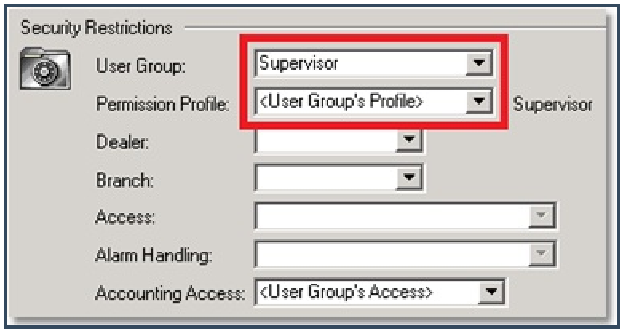


Profiles

Permission Profile: <No Profile>

Previous Manitou versions had an Operator and Supervisor Profile integrated into this section.

Like User Groups, the Users form (Maintenance Menu -> Users) previously had Operator and Supervisor Profile selection combo boxes. This has been reduced to a single Permission Profile option and moved to "Security Restrictions" within the Users form:



Security Restrictions

User Group: Supervisor

Permission Profile: <User Group's Profile> Supervisor

Dealer:

Branch:

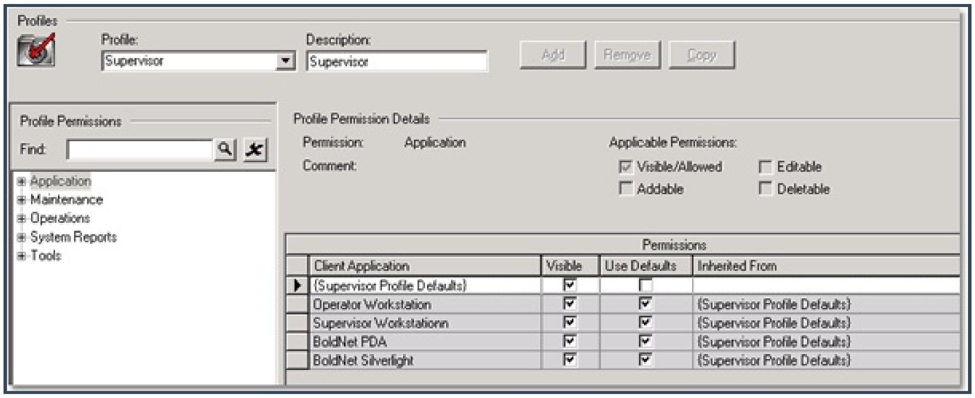
Access:

Alarm Handling:

Accounting Access: <User Group's Access>

By default, when creating a user, the group association will default to the "User Group's Profile" setting. This means that the user will inherit all of the permissions settings as seen in the prior Editing Permissions section. For instance, a user assigned to the "Supervisor" User group will receive the "User Group's Profile" setting by default.

Following is an example of the Supervisor Permissions profile:



Profiles

Profile: Supervisor

Description: Supervisor

Profile Permissions

Find:

Profile Permission Details

Permission: Application

Comment:

Applicable Permissions:

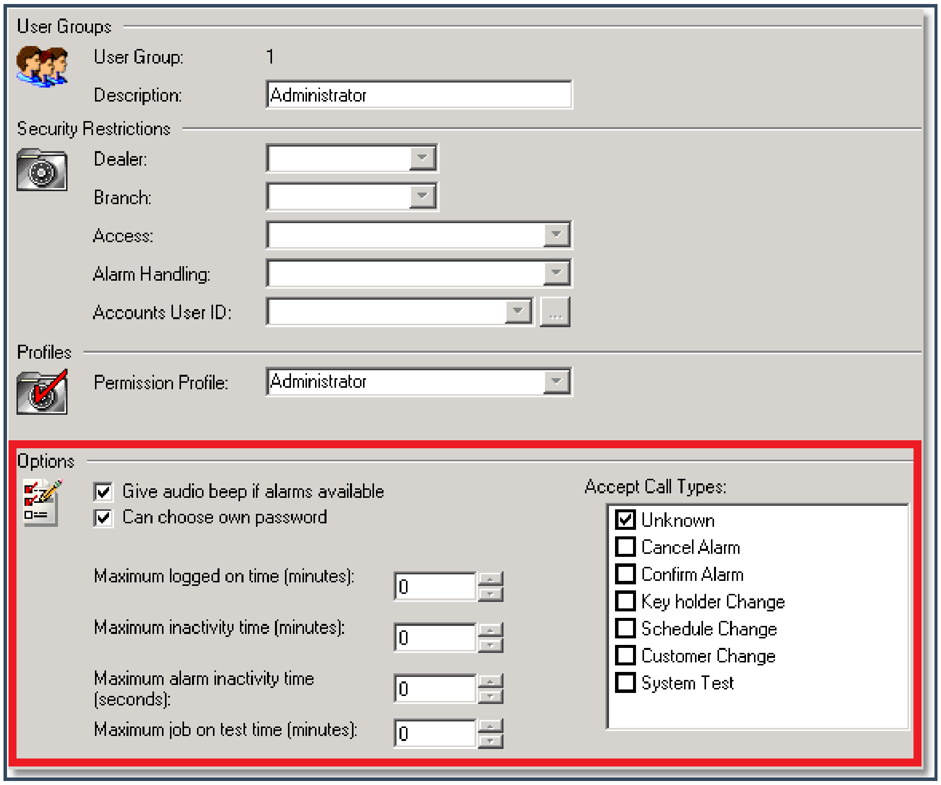
☑ Visible/Allowed ☐ Editable
☐ Addable ☐ Deletable

Permissions

Client Application	Visible	Use Defaults	Inherited From
{Supervisor Profile Defaults}	☑	☐	
Operator Workstation	☑	☑	{Supervisor Profile Defaults}
Supervisor Workstationn	☑	☑	{Supervisor Profile Defaults}
BoldNet PDA	☑	☑	{Supervisor Profile Defaults}
BoldNet Silverlight	☑	☑	{Supervisor Profile Defaults}

There are a couple of reasons one may want to create a user account that has a different User Group and Permission Profile assignment.

1. This provides an extra layer of customization, giving Manitou users even more flexibility with user rights assignments and permissions.
2. There is an additional set of options that can be assigned to user groups (Maximum logged on time, inactivity time, the Call Types they are allowed to receive, etc.) that are not available in the Permissions Profiles settings. Following is an example of the additional options available to the "Administrator" User Group:



User Groups

User Group: 1

Description: Administrator

Security Restrictions

Dealer:

Branch:

Access:

Alarm Handling:

Accounts User ID:

Profiles

Permission Profile: Administrator

Options

☑ Give audio beep if alarms available
☑ Can choose own password

Maximum logged on time (minutes): 0

Maximum inactivity time (minutes): 0

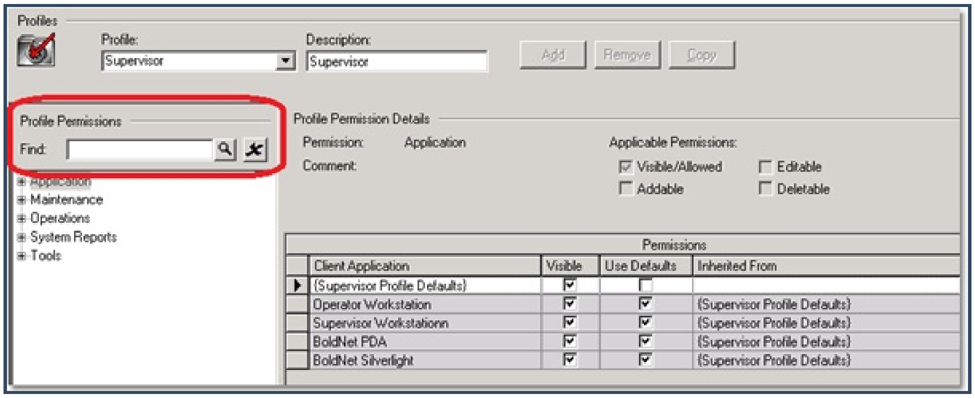
Maximum alarm inactivity time (seconds): 0

Maximum job on test time (minutes): 0

Accept Call Types:

☑ Unknown
☐ Cancel Alarm
☐ Confirm Alarm
☐ Key holder Change
☐ Schedule Change
☐ Customer Change
☐ System Test

When trying to find a permission, it may be helpful to use the search field, as follows:



Profile: Supervisor

Description: Supervisor

Profile Permissions

Find:

- ⊞ Application
- ⊞ Maintenance
- ⊞ Operations
- ⊞ System Reports
- ⊞ Tools

Profile Permission Details

Permission: Application

Comment:

Applicable Permissions:

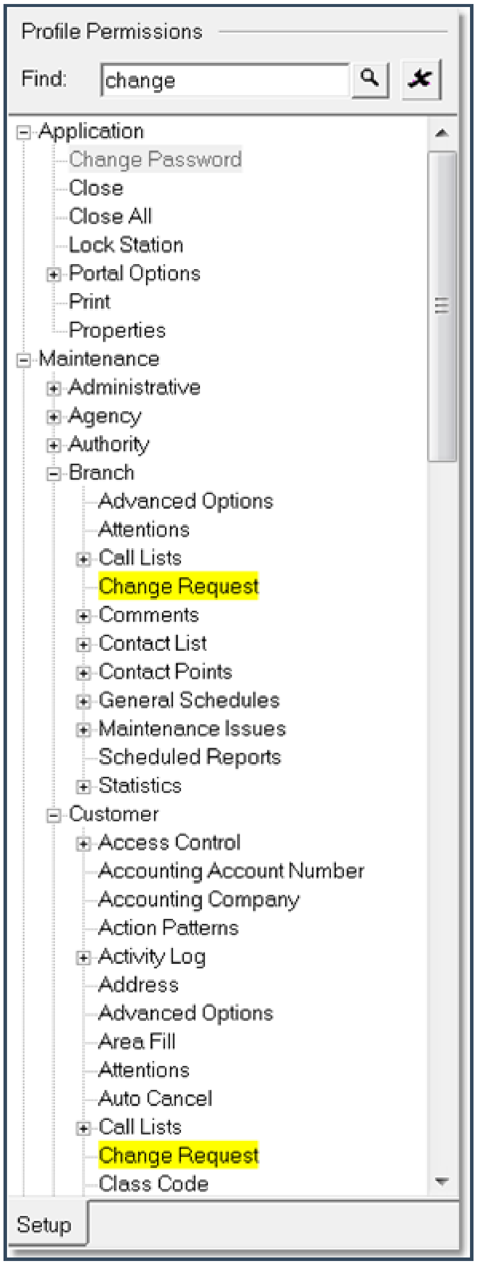
☑ Visible/Allowed ☐ Editable

☐ Addable ☐ Deletable

Permissions

	Client Application	Visible	Use Defaults	Inherited From
▶	{Supervisor Profile Defaults}	☑	☐	
	Operator Workstation	☑	☑	{Supervisor Profile Defaults}
	Supervisor Workstationn	☑	☑	{Supervisor Profile Defaults}
	BoldNet PDA	☑	☑	{Supervisor Profile Defaults}
	BoldNet Silverlight	☑	☑	{Supervisor Profile Defaults}

To perform a search, type a word such as "change", then press Enter on your keyboard or click the magnifying glass (🔍) icon next to the search field. Then Manitou will find all instances related to the word "change" and highlights them in yellow, as follows:



Find: change

Be sure to scroll down as there may be additional results, deeper in the list. The search function will also find partial matches. For instance, if you search for the word "work" it will also find words like "Network".

To clear the search field and start again, simply click the X icon (✗) located next to the magnifying glass icon. It may be helpful to know that you do not need to be in edit mode to find search terms.

Operators

A Central Station may choose for Operators to only handle alarms, and therefore do not need access to the Maintenance menu in the Client Workstation for data entry. Thus, the Administrator in the Supervisor Workstation will set the Permissions for an Operator to disable all menu functions, including customer data entry, Reports, File menu options, and Tools to disabled or hidden. Under the Operations functions, all alarm handling permissions would be enabled.

Data Entry

Likewise, a Central Station may wish to enable specific users to only handle data entry, such as entering new customer information or maintaining customer records. Once the User Group is set up, the Administrator may choose to give access to only the Maintenance menu and withhold access to any other menus in the Client Workstation, such as alarm handling.

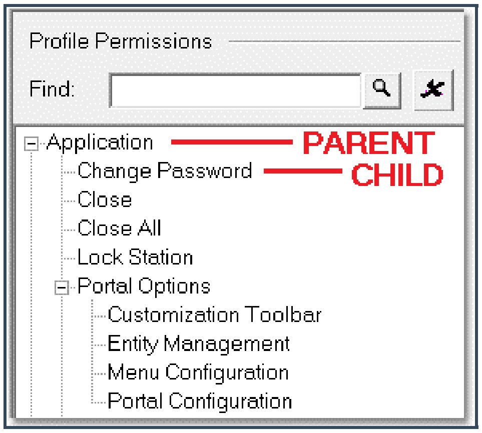
Trainee

Sometimes, a Central Station may choose to set up a "Trainee" User Group for new Operators learning to use Manitou. The permissions for a Trainee may be limited to customer maintenance, scheduling reports, and small tasks such as putting an account out of service before learning to handle alarms. Therefore, restrictions may be put on alarm handling, including canceling alarms from the alarm queue, pre-cancels, or alarm tracking, but enabling options such as scheduling reports or editing customer records. Additionally, Administrators may wish to first set the Trainee User Group to "View Only," and create a View Only profile in Permissions. Administrators may then set all functions to viewing only, where access may be visible, but not enabled for the Trainee. This would allow the new Trainee to become familiar with Manitou without having the ability to utilize any Manitou functions.

Permissions have been enhanced significantly in Manitou 1.6 affecting the entire suite: Manitou Server, Manitou Clients and BoldNet. Following is a brief overview.

Note: The differences in 1.6 are enhanced and different enough from previous versions of Manitou, that they warrant special attention. If not understood properly one could encounter unexpected results and in a worst case scenario give way to safety or security risks. So please take extra care when reading this section.

Terminology Note: The following hierarchal structure will be used to edit Permission Profiles:



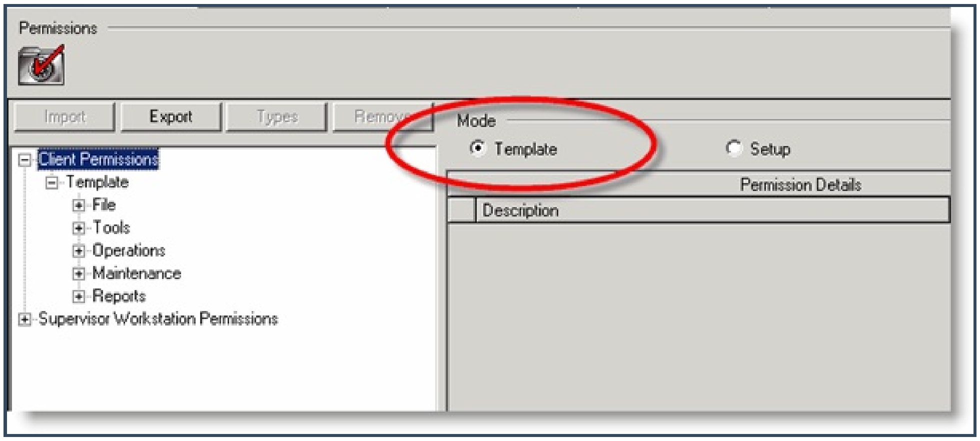
The top-level nodes will be referred to as "Parents" whereas the items below these top nodes will be referred to as "Children". In the picture above, "Change Password" is a Child of the Parent "Application".

Child objects can also be parents. For instance, in the picture above, the "Portal Options" object has a few child objects including "Customization Toolbar".

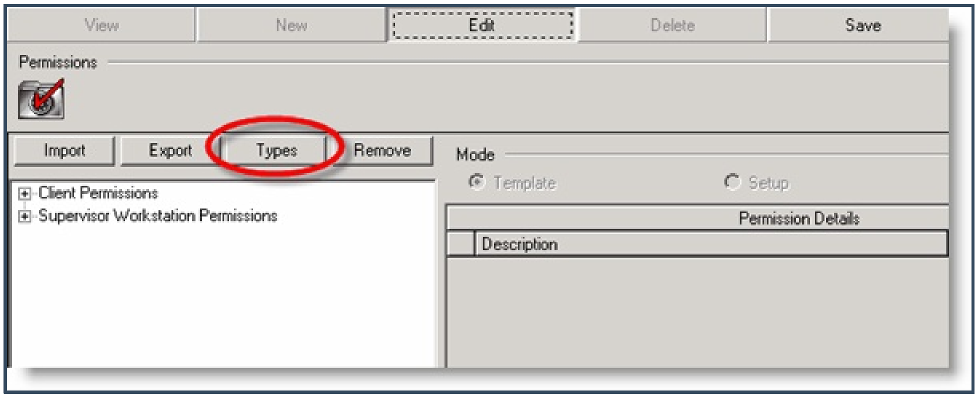
Note: These terms and concepts regarding hierarchy must be understood in order to grasp the further intricacies of Manitou 1.6 permission settings.

Should a new User Group need to be created, the first step is to create a new Profile type in Permissions.

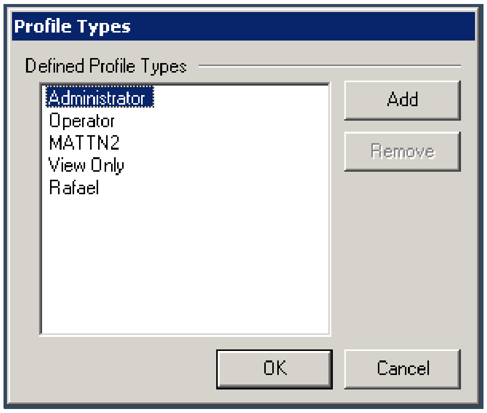
1. Open the Permissions form by first clicking on the Maintenance menu.
2. Select Setup.
3. Select Permissions.
4. Click on the Template mode.



5. Click on the Edit button to put the screen into Edit mode.
6. Click on the Types button located above the Permissions templates list.



7. A Profile Types box will appear. Click Add to add a new Profile Type:

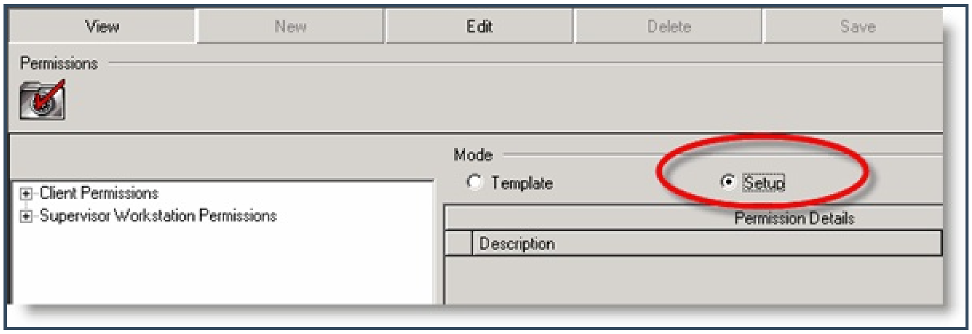


8. Enter the new Profile name.
9. Click OK. The new profile type has been created. However, the new User Group requires additional creation in the

10. First, log out of the Supervisor Workstation and log back in for the new changes to take place. This will enable the new Profile type to be listed in the User Groups section.
11. Click on the Maintenance menu.
12. Select User Groups.
13. Click on the Edit button to put the screen into edit mode.
14. Click Add.
15. Enter the description of the new User Group.
16. Click OK.
17. Under the Profile Name drop-down menu, select the newly created profile.
18. Enter the appropriate settings for the User Group.
19. Click Save.

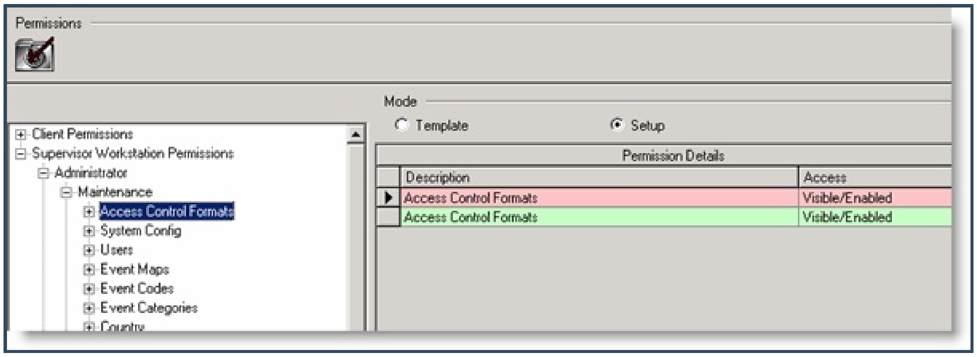
After the User Groups and Profiles have been set up, the permissions for each User Group must now be applied.

1. Set the Permissions screen to Setup mode.



Mode: ○ Template ● Setup

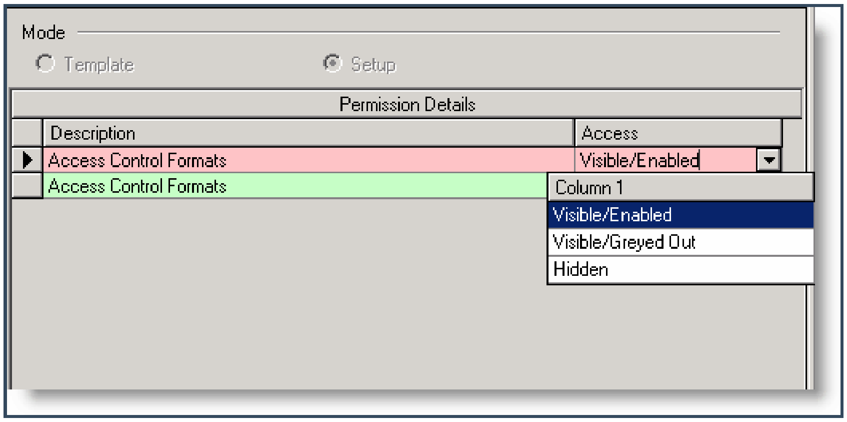
2. Click the Edit button to put the screen into Edit mode.
3. Expand the Supervisor Workstation permissions tree by clicking on "Supervisor Workstation Permissions" in the Templates list.
4. Select the Profile type that should be adjusted, and expand the Profile type. For example, under Supervisor Workstation Permissions, expand Administrator or Operator.
5. Under the Permission Details section of the screen, Permissions options will appear. If the option appears in green, it may be edited. If the option appears in red, it may not be edited.



Mode: ○ Template ● Setup

Description	Access
Access Control Formats	Visible/Enabled
Access Control Formats	Visible/Enabled

6. Continue expanding the Permissions tree until the menu to be edited is found.
7. Once the desired menu is found, locate the Access column in the Permissions Details portion of the screen.
8. Click in the Access column of the appropriate menu function to bring up a downward-pointing arrow.
9. Click on the arrow to display the Access options:


Mode

○ Template ● Setup

Permission Details

Description	Access
Access Control Formats	Visible/Enabled
Access Control Formats	

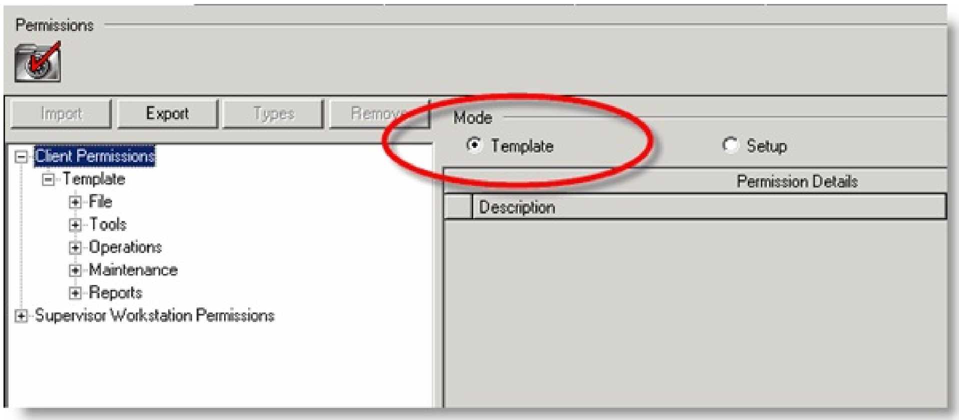
10. Select from the following Access options:

- Visible/Enabled - This menu function will be visible to this User Group and may be used by the User Group.
- Visible/Greyed Out - This menu function will be visible but not enabled (greyed out) and cannot be used by the User Group.
- Hidden - This menu function is hidden and will not be displayed or enabled to the User Group.

11. Once the Access options have been set, click Save.

Additionally, Manitou provides templates for setting up basic client and Supervisor permissions. These templates can be exported and imported. The permissions templates are normally imported upon the initial setup. The removal of old templates deletes all settings. When a new template is imported, all permissions will require resetting the permission restrictions for all the User Groups.

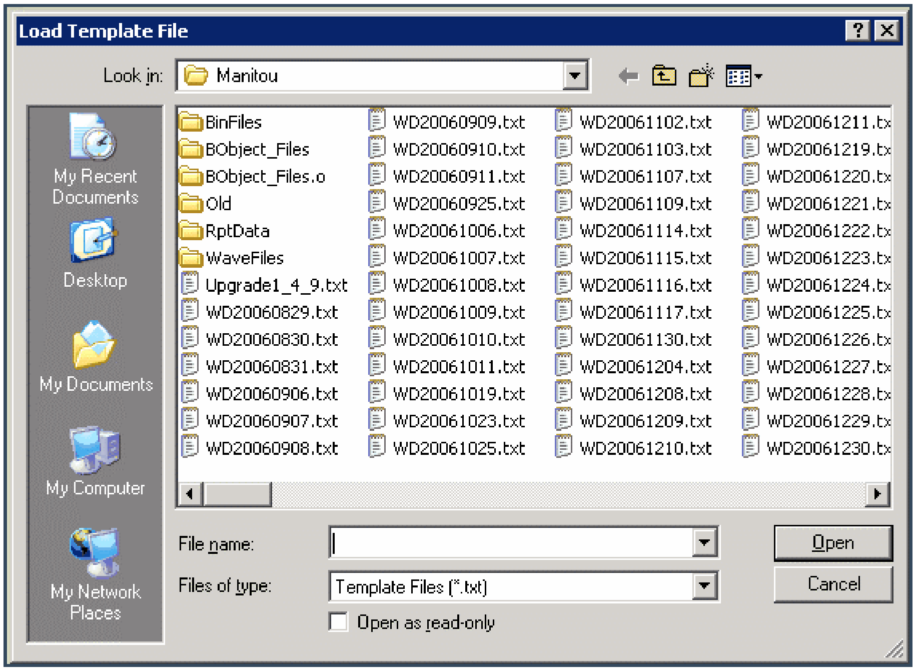
1. Bring up the Permissions screen by first clicking on the Maintenance menu.
2. Select Setup.
3. Select Permissions. The screen will default load in Setup mode.
4. Select Templates from the Mode settings.



Mode

● Template ○ Setup

5. Click the Edit button to put the screen into Edit mode.
6. Click on the Import button located above the Templates list. A Load Template File list will appear:



Look in: Manitou

File name:

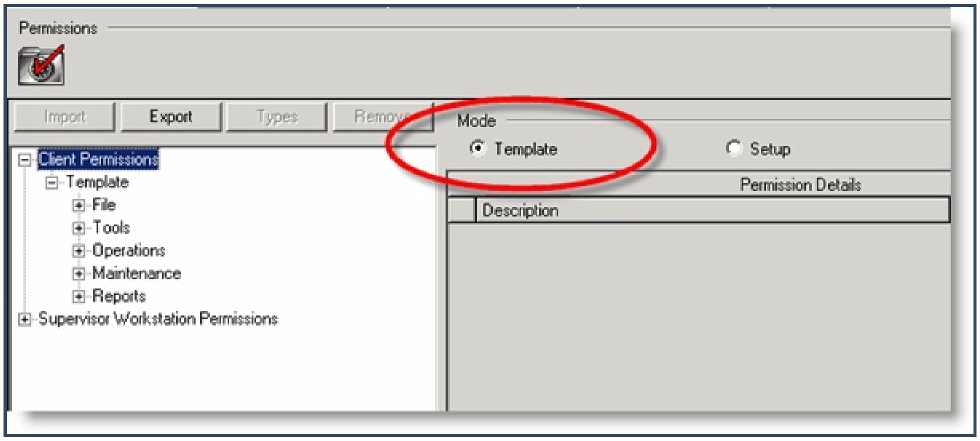
Files of type: Template Files (*.txt)

☐ Open as read-only

7. Select either Profile_0_0.txt or Profile_0_1.txt.
8. Click Open. The Template is now imported.
9. Click Save.

Bring up the Permissions screen by first clicking on the Maintenance menu.

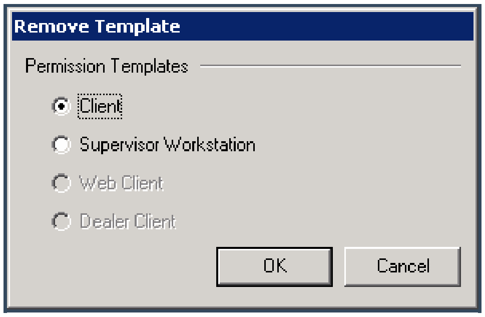
1. Select Setup.
2. Select Permissions. The screen will default load in Setup mode.
3. Select Templates from the Mode settings.



Mode

● Template ○ Setup

4. Click the Edit button to put the screen into Edit mode.
5. Select the template to be removed from the templates list.
6. Click the Remove button. A Remove Template box will appear:



Remove Template

Permission Templates

● Client
○ Supervisor Workstation
○ Web Client
○ Dealer Client

7. Users may opt to remove the template from either the Client (Operator) Workstation or the Supervisor Workstation. Select either the Client Workstation or the Supervisor Workstation. If the template must be removed from both Workstations, repeat the removal process to remove the template from the second Workstation.
8. Click OK.
9. Click Save.