

MemberLink® – Permission Levels Guide

Revised August, 2018

Overview

MemberLink supports the nine permission levels. Each of these includes their own built-in security that dictates what role a person plays in regard to control after logging into one of the **MemberLink** modules. This includes whether they can update the Bulletin Board; upload documents; create, change, or delete contact records; change permission levels, and much more.

Presented in the following list are the nine permission levels, along with a description of each one. Shown first is the highest access and authority level; the lowest level is last in this list that follows.

Permission Levels

1. Master Administrator (known as MasterAdmin)

MemberLink supports only one Master Administrator (MasterAdmin) per church. It can be someone at your church, or you can ask CAA to handle the MasterAdmin duties for you in your **MemberLink** system.

The MasterAdmin “Username” and “Password” are defined (and stored) in your system Configuration File. **There is no contact record in your database that identifies any person as the MasterAdmin.** The MasterAdmin is more of a “role” than a person, a “super user” above all the other roles and permission levels. MasterAdmin will not show as a selection option in the permission level menu list. It can only be assigned in the Configuration File.

Note: All other permission levels may be assigned only to existing contact records in your **MemberLink** database. In other words, levels two through nine described later in this document can only be granted via the Profile screen for a person in your system’s database.

The MasterAdmin may login only to the Administrator (Admin) module. The MasterAdmin cannot login to the Member Portal module because there is no “MasterAdmin role” in the Member Portal module.

The MasterAdmin has full access and authority to perform all functions and operations afforded in the Admin module.

The MasterAdmin is the only person that can do the following:

- View or update the system’s Configuration File or even see the “Main Configure” option on the screen. Therefore the MasterAdmin is the only person that will see or be able to update the MasterAdmin “Username” or “Password” as well as other controls in the Configuration File.
- Assign a permission level of “SysAdmin” on a user Profile screen. No other permission level may grant SysAdmin permission to anyone else.
- Turn on the ContributionLink Manager Checkbox on a user Profile screen. Therefore the only users with access to ContributionLink (to post donations, update giving records, print contribution statements, etc.) are those specifically granted that access by the MasterAdmin.

Warning: Only someone that understands the impact of each change should apply system Configuration File updates. An incorrect setting can disable the entire **MemberLink** system. It also can possibly corrupt the church’s database of contact records, doing such damage that **CAA** cannot restore system operation.

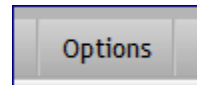
If you elect to take advantage of this service, a **CAA** representative will perform the Configuration File updates for your church at no cost. **CAA** will assist in establishing the initial configuration for you; then you can choose to make future changes yourself (MasterAdmin) or ask **CAA** to do it for you.

2. System Administrator (known as SysAdmin)

The MasterAdmin and SysAdmin permission levels are nearly identical in capability. More MasterAdmin capabilities are mentioned in this section.

As you start with **MemberLink**, you will have one MasterAdmin person but no SysAdmin people. The MasterAdmin is the only person that can create a SysAdmin. The MasterAdmin can create as many SysAdmin users as your church needs in that role. The MasterAdmin can make himself or herself a SysAdmin in their own contact record in the database if desired.

A SysAdmin can login to either the Administrative module or the Member Portal module. A SysAdmin has only slightly less access and authority than the fully empowered MasterAdmin.



On the “Operations Bar” in **MemberLink**, the Options tab appears only to the MasterAdmin, SysAdmin, and Admin permission levels. None of the other permission levels will see the Options tab. However, SysAdmin and Admin permission levels will not be able to view all the configuration options on the Options screen that the MasterAdmin can see and perform.

When the MasterAdmin or a SysAdmin creates Groups, those Groups are visible to all other permission levels. When an Administrator (and all lower levels) create Groups, assignments must be made to make those Groups visible or not visible to other users.

The MasterAdmin and SysAdmin users can view the “Manager Checkboxes” on the Profile screen and can turn them on or off. The one exception is that only the MasterAdmin can designate who can access the Contributions area of the system (by turning on or off the ContributionLink Manager Checkbox). The SysAdmin and other levels cannot give ContributionLink access to anyone.

The MasterAdmin and SysAdmin users can view the “Manage Searches” button on the Search screen for deleting saved searches.

Also, the MasterAdmin can include “Username” and “Password” in the data Export to a spreadsheet... as can the SysAdmin... but none of the other permission levels can Export these two pieces of data about a person.

3. Administrator

An Administrator (Admin) can login to either the Administrator module or the Member Portal module. This person has full access and authority to perform all functions and operations afforded in each module, with some notable exceptions.

Things an Admin permission level user cannot do in the Admin module:

- Cannot view the Configuration File or update it.
- On the Options screen, cannot see or do all of the options and configuration updates – some are only available to the MasterAdmin or SysAdmin permission levels as described above.
- Cannot view or update the Profile record of anyone designated as a SysAdmin. Thus an Admin (and all lower levels of permissions) cannot see the “Username” or “Password” assigned to a SysAdmin (and of course not the MasterAdmin either).
- Cannot upgrade the permission level of any user to that of SysAdmin.
- Cannot create universally visible Groups.
- Cannot manipulate the Manager Checkboxes.
- Cannot delete saved Search templates
- Cannot include the “Username” and “Password” data in Exports to .CSV file spreadsheets.

4. Associate Administrator

An Associate Administrator (AssocAdmin) can login to either the Administrator module or the Member Portal module. They have access and authority to perform many functions and operations afforded in each module, but there are some exceptions. This level of capability is less than the level of capability of an Admin permission level.

Things an AssocAdmin permission level user cannot do in the Admin module:

- Cannot perform the functions unique to the MasterAdmin or SysAdmin permission levels such as Configuration File updates, anything on the Options screen, or creating universally visible groups.
- Cannot view or update the Profile record of any SysAdmin person

Note: but can view and update the Profile data for all other contact records (people) and can create new Profiles (add new people to the contact database).

- Cannot view or update “Username” or “Password” on the Profile screen of any person.
- Cannot do any of these (unless the applicable Manager Checkbox is turned on in the AssocAdmin’s Profile screen:
 - Access the ContributionLink module
 - Access the Bulletin Board to do updates
 - Be a Group Manager
 - Be an Attendance Manager
 - Be a Care Group Leader
 - Perform Global Changes
 - Access Child CheckinLink module
- Cannot create, change, or delete custom data fields.

- Cannot delete saved Search templates.
- Cannot delete (remove) any contact records from the database.

Note: the MasterAdmin can designate any AssocAdmin to have access to ContributionLink, by turning on the CheckinLink Manager Checkbox, so that such people can do that type of work while not being able to do the other things this level is blocked from doing in **MemberLink**.

5. Assistant Administrator

An Assistant Administrator (AssistAdmin) can login to either the Administrator module or the Member Portal module. They have “limited” access and authority to perform functions and operations afforded in each module, but there are lots of exceptions. This level of capability is less than the level of capability of an AssocAdmin or any of the permission levels described above.

Things an AssocAdmin permission level user cannot do in the Admin module:

- Cannot perform the functions unique to the MasterAdmin or SysAdmin permission levels such as Configuration File updates, anything on the Options screen, or creating universally visible groups.
- Cannot view or update the Profile record of any person. The only data they see about a person is what is shown on the Contact tab screen’s Display Panel.

Note: but they can create new Profiles (add new people to the contact database).

- Cannot do any of these (unless the applicable Manager Checkbox is turned on in the AssocAdmin Profile screen:
 - Access the ContributionLink module
 - Access the Bulletin Board to do updates
 - Be a Group Manager
 - Be an Attendance Manager
 - Be a Care Group Leader
 - Perform Global Changes
 - Access Child CheckinLink module
- Cannot create, change, or delete custom data fields.

- Cannot export data to a spreadsheet.
- Cannot delete saved Search templates.
- Cannot delete (remove) any contact records from the database.

Note: the MasterAdmin can designate any AsstAdmin to have access to ContributionLink, by turning on the ContributionLink Manager Checkbox, so that such people can do that type of work while not being able to do the other things this level is blocked from doing in **MemberLink**.

6. Staff

No specific use right now.

Staff is simply a special category of Regular User. If you want to give any Regular Users a special designation, you can use either the Staff or the Special User permission levels.

Staff cannot login to the Administrator module. In the Member Portal module, Staff has the same privileges as a Regular User. See the description of Regular User below.

7. Special User

No specific use right now.

Special User is simply a special category of Regular User. If you want to give any Regular Users a special designation, you can use either the Staff or the Special User permission level.

Special Users cannot login to the Administrator module. In the Member Portal module, Special Users have the same privileges as a Regular User. See the description of Regular User below.

8.Regular User

Regular Users can login to the Member Portal module. They have access to perform many of the functions and operations afforded in the Member module, such as the following:

- Updating some of their own profile data
- Using the prayer wall for interactive prayer requests and topic discussions
- Answering surveys (questionnaires)
- Downloading documents from the shared area
- Viewing the photo/contact directory
- And more.

Regular Users can be granted (from their Profile screen in the Administrator module) some special privileges. These will appear at the top of their Profile screen in the Member Portal module, or in the Navigation Panel of that screen.

For example, you can grant a regular user the capability of emailing groups or reviewing group attendance data. You might do this for a teacher or class recordkeeper without giving them permission to login to the Administrator module.

Regular Users cannot login to the Administrator module.

9. Guest

CAA has created a special permission level that serves only one purpose. If you want to create a generic login to the Member Portal module, with a generic “Username” and generic “Password”, you can use the Guest permission level. People will be able to login to your Member Portal module, view your Bulletin Board information, and use the Photo/Contact Directory – but do nothing else.

Guest permission level is restricted from updating a Profile, from posting on the Prayer Wall, from answering Surveys or Questionnaires, and from Downloading any material.

This feature enables you to create a dummy contact record in the Administrator module and give it the Guest permission level. There can be only one such record, and any attempt to create two contact records with Guest permission level will give you an error.

In the dummy Guest record, you could give it a Username=Guest and a Password=Password; and a Firstname=Church and a Lastname=Guest. Another combination might be Username=Guest, Password=Guest, Firstname=Guest, and Lastname=Login. The point is, each church can create their own combination and then give the dummy Guest record “Username” and “Password” to anyone and everyone you want to enable logging into your Member Portal to use the Photo/Contact Directory without having to create a contact database record for each of them.

Some churches may have people they do not want updating their own Profile or posting on the Prayer Wall; some churches may want to give a login to people who are not members but want access to the Photo/Contact Directory anyway. Whatever the case, you can use Permission Level = Guest with a dummy record to do that.

Guest Users cannot login to the Administrator module.