Member Management Guide

©2018 Arbitration Forums, Inc.

All rights reserved. No part of this work may be reproduced in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the written permission of Arbitration Forums, Inc.

While every precaution has been taken in the preparation of this document, Arbitration Forums, Inc. assumes no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall Arbitration Forums, Inc. be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Published: June 2018

Revised: March 2019
# Table of Contents

Member Management Guide .................................................................................................. 2

I. Introduction .......................................................................................................................... 4
   About AF’s Member Management Guide ........................................................................... 4

II. Getting Started..................................................................................................................... 4
   Initial (One-Time) Setup Functions .................................................................................. 4
   Ongoing Maintenance Functions ..................................................................................... 5
   Business Units and Users Overview ............................................................................... 5
   Business Units .................................................................................................................. 6
   Multiple Business Units Example ................................................................................. 6
   Single Business Unit Example ....................................................................................... 6
   User Accounts .................................................................................................................. 6
   Individual and Group Privileges ..................................................................................... 7
   Individual Privileges ....................................................................................................... 7
   Group Privileges ............................................................................................................. 7

III. Business Unit Maintenance .............................................................................................. 8
   Add Business Unit .......................................................................................................... 8
   Edit Business Unit .......................................................................................................... 10

IV. User Maintenance ........................................................................................................... 11
   Add User .......................................................................................................................... 11
   Assign User Business Units ............................................................................................ 16
   Assign User Privileges .................................................................................................... 17
   Search User ..................................................................................................................... 20
   Edit User .......................................................................................................................... 24
   Multi-User Edit .................................................................................................................. 26
   List of Users (Export Feature) ....................................................................................... 31
   Advanced Search ........................................................................................................... 31
   Modify User Password ..................................................................................................... 32

V. Create a New Privilege Group .......................................................................................... 34
I. Introduction

About AF’s Member Management Guide
This Member Management Guide was developed to help you manage business units and users, and specify company preferences related to your company’s participation in AF’s programs. It contains information on how to establish and maintain business units and add and edit individual user accounts.

The topics below can help you get started using the Guide quickly. In just a few minutes, you will have an understanding of each topic. Click a topic below to learn more!

   Business Units and Users Overview
   Add Business Unit
   Add User

II. Getting Started
The following subsections outline the one-time Security Administration setup functions as well as the ongoing maintenance that will be performed by the Security Administrator.

Initial (One-Time) Setup Functions
The following steps represent the initial actions taken by both the participating company and AF to establish a Security Administrator. These represent steps that occur once during the initial setup of a company within AF’s online system.

1. Designate Security Administrator – An authorized person, often the same person authorized by a company to sign the arbitration agreement, designates someone to serve as the company’s Security Administrator. Multiple Security Administrators may be designated by the company. Each will need to be aware of and understand his or her role and responsibilities.

2. Complete and submit the Security Administrator Profile Form – The Security Administrator(s) must complete a Security Administrator Profile Form and return it to AF for processing. This form captures the basic information AF needs to create the Security Administrator account.

3. Create Security Administrator account – AF creates the Security Administrator account(s) and sends an email to the Security Administrator(s) that contains a link the Security Administrator will use to access AF’s website and establish a password.

4. Create Business Units, Users, and other Security Administrators – For companies new to AF’s website, the Security Administrator begins the setup process by creating business units to which individual user accounts will be assigned at the time they are
created. Business units are discussed in detail in the Business Unit section of this guide. The Security Administrator can also designate other Security Administrators for the company, if needed. Each Security Administrator can add and modify all business units and users.

**Ongoing Maintenance Functions**
The following steps represent the ongoing maintenance functions that will be handled by the Security Administrator. These represent recurring activities that could occur with some regularity depending on the company.

Security Administrator maintenance functions include:

- **Creating Business Units** – The initial business unit will be created by AF at the time the initial Security Administrator account is created. All business units created after that point will be created by the Security Administrator(s). For more information on business units, see Business Units and Users Overview.

- **Modifying and Maintaining Business Units** – Updates to any Business Unit will be made by Security Administrator(s). In the case of a large company with numerous Business Units, it is recommended that the Business Unit contact be the Security Administrator. For more information on modifying business units, see Edit Business Unit.

- **Creating User Accounts** – The addition of new users will be the responsibility of the Security Administrator(s). For more information on creating a user, see Add User.

- **Assigning and Maintaining Individual and Group Privileges** – Privileges may need to be changed over time based on the activity of the user or company. The Security Administrator(s) will make any privilege updates that may be needed. For more information on privileges, see Individual and Group Privileges.

- **Creating and Maintaining Users on Integrated Login (if applicable)** – If integrated login is used, the Security Administrator will maintain the user-related logins that occur on the company side.

- **Administering User Password Modification Process** – The Security Administrator(s) will be the primary contact for users who have password-related difficulties. For more information on password administration, see Modify User Password.

- **Inactivating Users** – Maintaining user accounts is an important security responsibility of the Security Administrator(s). When a user should no longer have access to AF’s website, the Security Administrator(s) must make that account inactive to prevent unauthorized use/access. For more information on inactivating a user, see Edit User.

**Business Units and Users Overview**
In AF’s website, the concepts of business units and users are linked because every user must belong to a business unit.
• A **business unit** is simply a group of users who share the need to access specific areas within AF’s website or who have some other similarities that allow them to be grouped together.

• A **user** is an individual who has an account that allows him or her to gain access to a secure computer system and particular resources within that system.

Typically, the Security Administrator creates the user account, which consists of information about the user such as login and access privileges. The access privileges define what a user can do on AF’s website.

### Business Units

Participating companies are diverse in size and organizational structure. As such, AF’s website security model is designed to meet a wide variety of needs. The security model provides a framework for organizing your users into business units and, as such, at least one business unit must exist for each company.

#### Multiple Business Units Example

Large companies may choose to organize their offices by region and locality. For example, ABC Mutual has four regional offices in the United States. Each office is responsible for claims within its region. Based on the number of individual user accounts the company will need to establish, the Security Administrator could create four business units and designate a Security Administrator for each who will manage the individual user accounts within that business unit.

#### Single Business Unit Example

Smaller companies, or those with centralized operations and/or a low number of individual user accounts, may opt to use the initial business unit created by AF and add/manage all user accounts within this sole business unit.

These represent only two examples of how a company might divide the administration of its users into business units. The number of Security Administrators and business units will vary depending upon the company’s needs, and how the company chooses to configure its user accounts is within its discretion.

### User Accounts

There are two categories of user accounts, and each has specific privileges associated with it:

• **Administrator** – May add and modify business units and users for his or her company. Regardless of the business unit to which they’re assigned, Administrators can control business units and users for the entire company. Administrators also can select and generate reports related to their company’s participation in AF’s programs.
• **User** – May work with E-Subro Hub demands and/or arbitration cases as well as edit some of his or her own account profile information such as his or her name and email address.

**Individual and Group Privileges**

AF’s website provides the ability to assign privileges in one of two ways:

- **Individual privileges** allow the greatest flexibility when assigning actionable items, but they also require the highest level of administration and maintenance.
- **Group privileges** provide a method to easily assign the most common sets of privileges without the extra work required when making assignments on an individual basis.

**Individual Privileges**

The assignment of privileges on an individual basis, while an acceptable method, is neither the primary method used by most companies nor the method recommended by AF due to the long-term administrative effort that would be required to maintain the privileges in this manner. Rather, this type of assignment is typically used to supplement one or more sets of group privileges.

Individual privileges are assigned by choosing the desired privilege from a list of all available privileges and making the assignment.

For more information on assigning privileges, see [Add User](#).

**Group Privileges**

The assignment of privileges on a group basis is the method AF recommends for this activity. Group privileges ease the long-term administrative burden associated with maintaining a user. AF provides several pre-defined groups that contain the privileges most commonly used together.
Group privileges are assigned in the same manner as individual privileges by choosing the desired group and making the assignment.

For more information on assigning privilege groups, see Add User.

III. Business Unit Maintenance

Business unit and user maintenance may only be completed after logging into AF’s website. The following procedures are based on the Security Administrator being logged on.

Add Business Unit

AF creates the initial default business unit at the time the initial Security Administrator account is created.

To add a business unit:

1. Select Administration > Business Unit Maint.
2. Click **Add New Business Unit** to go to the Add Business Unit screen. 

   **Note:** To avoid duplication of business units, AF recommends searching the list of available business units before creating a new one.

   ![Add Business Unit Screen]

3. Enter the requested information in the appropriate fields and select **Save**. 

   **Note:** AF recommends that the contact information for the business unit be the Security Administrator assigned to that unit. This provides AF with direction for use in supporting the end user. In addition, Password Change Interval options of 30, 60, and 90 days are available to allow companies to adhere to their own password security policy if less than AF’s maximum of 90 days.

   ![Edit Business Unit Screen]
4. A success message will be displayed. Click **Back to Business Unit List**.

To add additional business units, simply repeat the steps above to add as many business units as needed.

**Edit Business Unit**

To edit a business unit:

1. Select **Administration > Business Unit Maint.**

2. Select **Edit** located on the row associated with the desired business unit.
3. Make any desired changes and click **Save**.

4. A success message will be displayed. Click **Back to Business Unit List**.

**IV. User Maintenance**

**Add User**

To create a user:

1. Select **Administration > New Member Management**.
2. To create a new user, select **Users**, which can be found on the left side of the page.

Next, select **New User**.

**Note:** To avoid duplication of users, AF recommends searching for the user by entering a last name and clicking **List Users** prior to creating a new user.
3. Add the information noted below (1–9) for the individual being added.

<table>
<thead>
<tr>
<th>1</th>
<th>Default Business Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Login ID</td>
</tr>
<tr>
<td>3</td>
<td>New Password</td>
</tr>
<tr>
<td>4</td>
<td>Confirm Password</td>
</tr>
<tr>
<td>5</td>
<td>Challenge Question</td>
</tr>
<tr>
<td>6</td>
<td>Challenge Answer</td>
</tr>
<tr>
<td>7</td>
<td>Email</td>
</tr>
<tr>
<td>8</td>
<td>First Name</td>
</tr>
<tr>
<td>9</td>
<td>Last Name</td>
</tr>
</tbody>
</table>

**Company**
- BETA INSURANCE CO (04514)

**Login ID**
- Please include the code in the login, e.g., login ID 04514. Login ID cannot be more than 20 characters long.
- A Login ID is required.

**Account Type**
- Standard User
- Auto Login
- Send Email Confirmation

**Require IP Address Validation**
- Yes
- No

**New Password**
- Password must be at least 8 characters long, with uppercase and lowercase letters.

**Required Password Change Upon Next Login**
- Yes
- No

**Is the user active?**
- Yes
- No

**Email**

**First Name**

**Last Name**

**Phone**

**Comment**
- Comments will be added to the changelog for the user.
The following is a brief explanation of the User Info fields:

<table>
<thead>
<tr>
<th>Steps</th>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Business Unit</td>
<td>From the drop-down menu, select the desired business unit to which the new user should be added.</td>
</tr>
<tr>
<td>2</td>
<td>Login ID</td>
<td>Enter a name that will enable AF’s website to identify and address the individual for whom the ID is being created. If a duplicate ID is entered, the system will reset it. AF recommends using the individual’s company network ID (the name he/she used in your company’s email) along with your AF company code, separated by a period. For example, user.88881. Using this naming convention will avoid a login ID conflict with a person working for another company with the same name.</td>
</tr>
<tr>
<td>3 &amp; 4</td>
<td>New Password and Confirm Password</td>
<td>The AF system will send each user an email containing his or her login ID and a link to create a password when you select Yes in the send email confirmation field. Note: You must select the button, so the user receives an email to create a password. Passwords must be at least 8 characters long with uppercase and lowercase letters. Once a password is entered, confirm it by entering it again under “Confirm Password.” The system will default to “Require Password Change Upon Next Login.”</td>
</tr>
<tr>
<td>5</td>
<td>Challenge Question</td>
<td>Select a question from the drop-down box. AF’s website will ask the user one of the selected questions to generate a new password if the user loses or forgets his or her original password. As Security Administrator, you can coordinate this question and answer with the user or pick one of the general questions (e.g., what is your company code?). After the Administrator enters a user, the user can change his or her name, password, and the challenge question and answer.</td>
</tr>
<tr>
<td>6</td>
<td>Challenge Answer</td>
<td>Enter the answer to the challenge question in this field. AF’s website will compare the answer given by the user to the answer entered here. It is important for the user to remember this answer.</td>
</tr>
<tr>
<td>7</td>
<td>Email</td>
<td>Enter the user’s company email address.</td>
</tr>
<tr>
<td>8</td>
<td>First Name</td>
<td>Enter the user’s first name.</td>
</tr>
<tr>
<td>9</td>
<td>Last Name</td>
<td>Enter the user’s last name.</td>
</tr>
</tbody>
</table>
4. Once all information has been entered, click **Save**.

5. The next step is the assignment of privileges, which can be done on an individual or group basis. Privileges are assigned from either the **Privilege Groups** tab or the **Privileges** tab. In either tab, select the box next to the desired item. The privilege will be automatically moved from the **All Privileges** column to the **Assigned Privileges** column.

6. To add additional users, select **New User** and follow the steps under **Section IV. User Maintenance**.
Assign User Business Units
To assign additional business units to an existing user:

1. Select Administration > New Member Management.

2. Select Users from the main page. Enter user’s last name in the search field. Choose the specific user by clicking on his or her name.

3. Use the drop-down menu under Default Business Unit and Non Default Business Units to select additional business units specific to the user.
Assign User Privileges
The next step is the assignment of privileges, which can be done on an individual or group basis. Privileges are assigned from either the Privilege Groups tab or the Privileges tab. In either tab, select the box next to the desired item. This will automatically save that item to the Assigned Privileges tab.

To assign Privilege Groups to an existing user:

1. Select Administration > New Member Management.

![My Arfile](image)
2. Enter user’s last name in the search field.

3. Search the desired user from the list below:

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>Email</th>
<th>Login ID</th>
<th>Business Unit</th>
<th>Account Type</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>D313</td>
<td>D313</td>
<td><a href="mailto:test@test.org">test@test.org</a></td>
<td>D313</td>
<td>Accelerated Recovery Services, Inc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP</td>
<td>Support</td>
<td><a href="mailto:test@test.org">test@test.org</a></td>
<td>apsupport D413</td>
<td>Subrogation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP DI SYSTEM</td>
<td>04113</td>
<td><a href="mailto:test@test.org">test@test.org</a></td>
<td>apsystem 04113</td>
<td>AP Test Business Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANFAC</td>
<td>TEST1N</td>
<td><a href="mailto:test@test.org">test@test.org</a></td>
<td>anfac 0413</td>
<td>Subrogation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aaron</td>
<td>Rodgers</td>
<td><a href="mailto:test@test.org">test@test.org</a></td>
<td>arrodgers D0413</td>
<td>AP Test Business Unit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. Select user by clicking on his or her name.

5. Select Privilege Groups tab.
6. Selecting a privilege under All Privilege Groups automatically saves it to Assigned Privilege Groups.

7. Select Save to save and exit user’s profile.
8. Click the **Assigned Privileges** tab to see a list of the privileges currently assigned to the user.

*Note: This tab displays all assigned privileges regardless of whether they were assigned via a group assignment or an individual assignment.*
2. Select Users.

3. Enter user name in the field below.
4. Once user is found, simply click on his or her name.

5. From this screen, edits can be made. See Edit User for more information on this topic.
Shortcut: To find a user quickly, select Administration > New Member Management.

Select the Find Your Users tile. This takes you directly to the search field under the Users tab.
Edit User
To edit an existing user:

1. Select **Administration > New Member Management**.

2. Select **Users** and search for the user you want to edit.

3. Click on the user’s name, which brings you directly to the edit screen.
4. Edits can be made from either the **Account** or **User Profile Tab**.
   Make any desired edits and select **Save**.

**Shortcut:** Edit users with ease by taking this shortcut.

Select **Administration** > **New Member Management**.
From the website, click on the **Edit Users with Ease** tile and follow the steps provided under **Edit User**.

**Multi-User Edit**
This feature allows Security Administrators to edit multiple users at one time.

Select **Administration> New Member Management**.
From the **Users** tab, select users you wish to edit. Do this by selecting each desired user.

When selecting multiple users, another tab will appear called **Multi Edit**. Select that tab to edit multiple users at one time.

From this page, you can change users’ passwords. Do this by selecting **Account Settings**.
Multi Edit also allows you to change **Privilege Groups** for users.

To make a change, select **Add**, **No Change**, or **Remove**. This will change the account of all selected users at once.

Once changes have been made, select **Review changes**.
Once your changes have been reviewed, select **Submit changes**.

**Shortcut:** To edit multiple users directly, go to **Administration>New Member Management**.
From the webpage, click on the **Multi-user Edit** tile and follow the steps provided under **Multi-user Edit**.

Multi-user Edit

You can now select multiple users and perform bulk operations on them, from adding/removing a privilege to a group of users, to requiring a password change for the next login.
List of Users (Export Feature)
This feature gives System Administrators the ability to export a list of users based on the search criteria entered. The list is formatted as an Excel spreadsheet.

Advanced Search
The Advanced Search tab allows users to search using more detailed information.

Go to Users and select Advanced Search.

From this tab, you can search for a variety of information, e.g., users who are currently active and assigned to specific business units or account types. You can also search for “arbitrators only.”
Modify User Password
The following provides the steps used to modify the password of an existing user on AF’s website. For an overview of users, see Business Units and Users Overview.

To modify the password of an existing user:

1. Select Administration > New Member Management from the My Arbfile section of AF’s website.

2. Select Users and search for user’s name.

3. Click on the user’s name, which brings you directly to the edit screen.
4. On the **Account** tab, click **Modify Password**.

5. New fields will appear to enter a **New Password** and to **Confirm Password**.

6. Enter the information and confirm the **Email** field is accurate.

7. Confirm the **Send Email confirmation** field is selected.
8. Click **Save Changes** to send the user an email with a link to create a new password. 
   *Note: If a user’s password has not expired, AF recommends that he or she be directed to modify his or her own password by either editing the user profile or using the **Forgot Password** link on the home page.*

---

**V. Create a New Privilege Group**

**Creating a New Privilege Group** allows System Administrators to create a new privilege group for specific users with various tasks. For example, a user who is assigned to the **Customer User Group Privilege** may also need privileges to run reports. Instead of allowing all users within that specific privilege group to have access to reports, the System Administrator can create a new privilege group. Once the new group is created, the System Administrator can add specific privileges within the group without granting access to ALL users assigned to that original group privilege.

1. To create a new privilege group, select **Administration > New Member Management**.
2. Select **Privilege Groups**.

3. A list of group privileges will appear. To see what privileges are assigned to specific privilege groups, select the group name.
4. **All Privileges** will appear on the screen.

5. To Create a New Privilege Group, select **Create a New Privilege Group**.

6. Enter a **Group Name**, and then select **Privileges** within that group. To assign privileges, simply select the box next to **All Privileges**. This will automatically assign the privilege as seen under **Assigned Privileges**.
7. Save your selections.
8. Go to **Privilege Groups** to see your newly added Privilege Group.

9. To add this Privilege Group to specific users, go back to the **User Tab** and search for each user’s name.

10. Select the specific user by clicking on his or her name.
11. Select **Privilege Groups** and assign this privilege to specific users.

**Shortcut to Create a New Privilege Group:**

To create a unique group of users who need specific privileges, select **Administration > New Member Management.**
Then click the **Create Privilege Groups** tile.

Select **Create a New Privilege Group** and follow the step outlined above.