Security Administrator Guide

©2017 Arbitration Forums, Inc.

All rights reserved. No parts 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: July 2016, May 2017, September 2017
# Table of Contents

Security Administrator Guide ................................................................. 2

I. Introduction ................................................................................................. 4
   About AF’s Security Administrator Guide ............................................... 4

II. Getting Started............................................................................................ 4
   Initial (One-Time) Setup Functions .......................................................... 4
   Ongoing Maintenance Functions .............................................................. 5
   Business Units and Users Overview ......................................................... 6
   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 ..................................................................... 17
   Assign User Privileges ............................................................................ 18
   Edit User .................................................................................................. 20
   Modify User Password – System-Generated Password Only ....................... 21
I. Introduction

About AF’s Security Administrator Guide

This Security Administrator 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 needed by AF 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
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. For more information on Integrated Login, please see [Integrated Login](#).

- **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 regions 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 privileges, 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.
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. Also, 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.

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 are 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 > User Maintenance**.
2. The User Maintenance List screen for your organization will be displayed. By default, All Business Units is selected for the Show Users for Business Unit field. Since a user must belong to a business unit, this selection must be changed to add a new user. Change this selection by clicking Change to the right of the entry.

**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. All existing business units will be displayed in the popup window. Select the desired business unit to which the new user should be added by clicking Select next to the appropriate business unit name.

**Note:** If numerous business units exist, specific units can be located by entering all or part of the unit’s name and clicking Search Business Units. To undo a previous selection, click Select All Business Units.

4. The User Maintenance List will be displayed with the selected business unit displayed. Click Add New User to proceed.
5. Add the information noted below (1-10) for the individual being added.
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>
</table>
| 1     | Login ID   | 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 uses 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.  
Note: Login IDs are case-sensitive. |
| 2     | System-Generated Password | 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 press the button, so the user receives an email to create a password. |
|       | Require Password Change Upon Next Login | This field requires the user to change his or her password the next time a login is attempted. |
|       | Grace Logins Used | This field is the current state of the password.  
- Password Not Expired (default selection)  
- 1 Grace Login Used  
- 2 Grace Logins Used  
- Password expired; no grace logins left  
**Note:** No changes are recommended when adding a new user. |
<p>| 3     | Email      | Enter the user’s email address where AF can send information related to the user’s account. |
| 4, 5, | First Name, Last Name and Phone | Enter the user’s first and last names, and telephone number in the appropriate fields. |
| and 6 | Is this account active? | The default answer is Yes, which means the user has access privileges on AF’s website. Select No, and the user account is inactive with no access privileges to AF’s website. |
| 7     | Challenge Question | 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. |</p>
<table>
<thead>
<tr>
<th></th>
<th>Challenge Answer</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Send E-Mail confirmation</td>
<td>The default answer is Yes. When the system-generated password is selected, this field must have Yes selected for the user to receive an email with the link to create a password.</td>
</tr>
<tr>
<td>9</td>
<td>Require IP Address Validation (OPTIONAL)</td>
<td>Companies configured for IP address filter will have this field visible. The default answer is Yes. Change the selection to No if the user is allowed to access AF’s website from a non-dedicated IP address, i.e., from home or other locations without first making a network connection (VPN, CITRIX, VMware, etc.).</td>
</tr>
</tbody>
</table>
|   | Service Account Type | The field is un-editable and the default answer is Not a Service Account. The service account types are:  
• AFClient  
• Auto Login  
• Data Integration  
• System  
Contact support@arbfile.org if you wish to create a service account. |
|   | Last Modified | This is a system-generated field used to display the date and user associated with the last modification of this user account. |

6. Once all information has been entered, click **Save Changes**. A success message will appear at the top of the page.
7. The next step is the assignment of privileges, which can be done on an individual or group basis. Privileges are assigned from either the **Set Groups** tab or the **Set Privileges** tab. In either tab, Select the box next to the desired item and move that item to the Assigned list by clicking the arrow that points to that table. Once moved, the selection is saved automatically.

**Note:** Every user should have, at minimum, the “Customer User” group assignment.
8. To add additional users, navigate back to the User Info tab and click Back to User Listing.

Assign User Business Units
To assign additional business units to an existing User:

1. Select Administration > User Maintenance.

2. The User Maintenance List screen for your organization will be displayed. By default, All Business Units is selected for the Show Users for Business Unit field. The Login ID and Last Name fields are also blank. Any of these fields can be used to locate a specific user by entering the desired values and clicking List Users.

3. Select Edit on the row associated with the desired user.

4. Select the Set Business Units tab.

5. If the user is to belong to more than one business unit, click the Assign new Business Unit link.
6. Click **Select** to choose the business unit to add to the current user’s profile. If needed, the search function can be used to narrow the list of business units.

7. The business unit will be added to the user’s profile where edits can be made regarding which business unit is default, whether this user is a supervisor of this business unit, and if a business unit should be removed from this user. Make the appropriate edits and click **Save Changes**, as needed.

**Assign User Privileges**

To assign privileges to an existing User:
1. Select **Administration > User Maintenance**.

2. The User Maintenance List screen for your organization will be displayed. By default, All Business Units is selected for the Show Users for Business unit field. The Login ID and Last Name fields are also blank. Any of these fields can be used to locate a specific user by entering the desired values and clicking **List Users**.

3. Select **Edit** on the row associated with the desired user.

4. The next step is the assignment of privileges, which can be done on an individual or group basis. Privileges are assigned from either the **Set Groups** tab or the **Set Privileges** tab. In either tab, check the box next to the desired item and move that item to the Assigned list by clicking the arrow that points to that table. Once moved, the selection is saved automatically.
5. Click the **User 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.

---

**Edit User**

To edit an existing user:

1. Select **Administration > User Maintenance**.

2. The User Maintenance List screen for your organization will be displayed. By default, All Business Units is selected for the Show Users for Business Unit field. The Login ID and Last Name fields are also blank. Any of these fields can be used to locate a specific user by entering the desired values and clicking **List Users**.
3. Click the **Edit** button on the row associated with the desired user.

4. Make any desired edits and click **Save Changes**.

5. **Note:** Edits made to group or individual privileges, on those respective tabs, are automatically saved.

### Modify User Password – System-Generated Password Only

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 > User Maintenance** from the My Arbfile section of AF’s website.

2. The User Maintenance List screen for your organization will be displayed. By default, All Business Units is selected for the Show Users for Business Unit field. The Login ID...
and Last Name fields are also blank. Any of these fields can be used to locate a specific user by entering the desired values and clicking **List Users**.

3. **Click the Edit button** on the row associated with the desired user.

4. **On the User Info tab**, click **Modify Password**.

5. **Click System-Generated Password**.
6. Confirm the **Email** field is accurate.

7. Confirm the **Send Email confirmation** field has Yes.

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.