User Management

https://campus.barracuda.com/doc/79466725/

These instructions describe how to add new administrators to the system and how to manage them. In the user settings, you can also enforce policies like forced password expiration and multi-factor authorization.

- Note that these are administrators who will use Security Awareness Training, not individuals in Address Books who will receive campaign materials. Individuals in Address Books are not users of Security Awareness Training.
- If you do not see the **System > User Manager** utility, contact Barracuda Support for assistance.

To add users to your Security Awareness Training account:

1. Navigate to **System > User Manager**.
2. Click **New**.
3. In the **User** field, enter a unique name for the user – usually, this is the user's email address. Click **Save**.
4. When the page refreshes, enter basic **Identification** information for the user:
   - **User** – The unique name you just chose. You can change it here, if needed.
   - **Full Name** – The complete, first and last, name of the user.
   - **Title** – The job title for this user.
   - **Email** – The email address for the user.
   - **Manager Name** – The name of the person to whom this user reports.
   - **Manager Email Address** – The email address for this user's manager.
   - **UID** – A unique identifier created by the system.
   - **Notes** – Anything important to say about the user, including name pronunciation and their preferences.
5. In the **Authentication** section, specify the following information:
   - **Active** – Confirm that this check box is selected to enable the user to access Security Awareness Training.
   - **Force Password Expire** – Select this check box to force the user to change their password after a number of failed login attempts.
   - **Failed Password Attempt Lock** – If this check box is selected, the user account is currently locked. The user has been sent an email, requiring them to change their password.

     Rather than your creating a new password for a new user, allow the user to make their own password by following the instructions in Resetting Your Password.
   - **New Password** – Optional. See note above.
     Enter a base password for the user. Type it again in the next field. Note that passwords must:
     - contain at least 8 characters.

        - contain at least one numeric digit 0-9.
        - contain both upper and lower case letters.
        - not be common variations of words in a dictionary.
        - not be reused.
        - change every 60 days.
        - contain 100 characters or fewer.
    - **Authorization Type** – Select either **Standard User** or **Single Sign On User**. If neither option appears, leave this field blank.
    - **Multi-Factor Enabled** – Select this check box to require an authentication method, in addition to a password, to authenticate this user.

      Using multi-factor authentication increases security and is strongly recommended.

    - **Multi-Factor Method** – If you enabled multi-factor authentication, select the secondary authentication method here:
        - **Email** – User receives an authentication code via email. They must enter this code to authenticate into Security Awareness Training.
        - **SMS** – User receives an authentication code via text. They must enter this code to authenticate into Security Awareness Training.
        - **Voice** – User receives a phone call and must press a specific button to authenticate into Security Awareness Training.

        - **Multi-Factor Phone #** – Based on the Multi-Factor Method you just selected, specify the corresponding email, phone number, or mobile phone number for contacting the user. Punctuation is not required in phone numbers. If the phone number is international, be sure to include the country code prefix with the plus (+) sign.
          Note that the title of this field does not change. Just match your entry type with the Multi-Factor Method you select in the field above (i.e., enter an email address for email authentication, regardless of the field label).

In the **Group Membership** section, click **Select** to associate this user with one or more groups, each of which has associated permissions.Click the preview icon  to see which users are already members of a certain group.

Consider your data integrity when granting permissions. All users can view almost all data, so consider which users need permissions to alter or delete data. For example, not every user needs to be able to delete Address Books or delete Campaigns.

Settings for most new administrative users – Select all options *except* any **Document Folders** and **Single Sign-on – Can Manage All**.

Settings include:

- Address Book - Can Delete Any Address Book – Allowed to delete Address Books. All users can add and edit Address Books.
- API - Can Edit All – Allowed to edit APIs. All users can view and use APIs.
- Approvals - Can Approval All – Can approve all campaigns. Other users cannot approve campaigns.
- Campaign Administrator – Can manage and take any action on all Campaigns and Address

Books. Essentially full administrative privileges, except Client User administration. There must be at least one Campaign Administrator in your organization.
    - Client User Administrator - Can Manage All Client Users – Can add new users to the instance and can assign permissions to these users. Do not assign if you do not want this user to be able to create new user accounts.
    - Content Center – Admin only group.
    - Default Reminder Group – Receives all reminders.
    - Document Folder – Your individual folder rights. This depends on your settings.
    - Document Library - Can Download Files – The user can download files from the document library.
    - Document Library - Can Upload Files – The user can upload files from the document library.
    - Document Manager - Can Manage All Folders and All Files – The user can manage the folders, add, edit and delete the folders themselves.
    - Domain Authorization - Can Edit All – The user can set ignore on the domain authorization page.
    - Email Campaign - Can Copy All – Specific right to copy email campaigns.
    - Email Campaign - Can Delete All – Specific right to delete email campaigns.
    - Email Campaign - Can Edit All – Specific right to add and edit campaigns.
    - Email Campaign Results - Can View All – Can view campaign rights. Effectively, a read only access to system.
    - **Everyone** – All Users Must Be In This Group
    - Incident Response Dashboard - Can Manage All – Can view and update the disposition and notes in the Incident Response Dashboard.
    - LDAP Config - Can Edit All – Can configure the LDAP integration configuration used to connect to your LDAP and active directory (AD).
    - Outlook Plugin - Can Manage All – Can add, edit, and delete button configurations. The button is used to report emails to the Incident Response Dashboard.
    - Phone IVR - Can Edit All – Can add, edit and delete Voice applications.
    - Questionnaire Templates - Can Manage All – Can add, edit, and delete Training Templates and LMS Templates. Note that this is not permission to edit the training content itself.
    - Questionnaires - Take Survey – Can preview training courses.
    - SFTP Config - Can Edit All – Can edit the secure FTP configuration. This is an alternate method to automatically import address books via a CSV file that is hosted on a SFTP server.
    - Single Sign On - Can Manage All – Can add, edit, and delete Single Sign On (SSO) configurations.
    - Slideshows - Can Manage All – Can review training content when it is being developed or previewed by the administrative user.
    - Training Results - Can View All – Can view training results.
6. In the **Preferences** section, specify the following information:
    - **Email Enabled** – Select to enable notifications for this user via email.
    - **Pop-Up Hints Enabled** – Select to enable Security Awareness Training pop-up hints for this user.
    - **Max Display Rows** – The maximum number of rows to show on a page in Security Awareness Training.

    - **Time Zone** – Select the time zone for this user.
    - **Time Format** – Select the preferred format for date and time for this user.
7. The **History** section displays the following read-only information:
    - **Add Date** – Date the user was added.
    - **Last Password Change Date** – Date the user's password was most recently changed.
    - **Last Session Date** – Last date the user logged into Security Awareness Training.
8. Click **Save**. The administrative user is now added to the system.

The new administrative user is now ready to log into the system. Note that the first time this user logs in, they will need to change their password.

Notifications

You can configure the system to send Security Awareness Training notifications to this new administrative user. The user must be Active (see above). For details, refer to Notification Settings.

Figures

1. previewIcon.png