Global Settings

https://campus.barracuda.com/doc/13208/

Navigate to **System > Global Settings** to specify the settings described in this article. Settings are described in order of appearance on the **Global Settings** page. Use the shortcuts in the left navigation panel on the **Global Settings** page or scroll down to the setting you want to specify.

Login Message

Customize the message users see when they log into Security Awareness Training.

1. Enter the message you want users to see when they log into Security Awareness Training.
2. Click **Save**.

DLP Activator

If your organization uses DLP (Data Loss Prevention) you might want to mark all Security Awareness Training emails with a customized string for reasons including:

- preventing your users from forwarding Security Awareness Training emails outside of your organization
- enabling your support organization to more easily identify Security Awareness Training emails, so they can address questions

To append the DLP Activation String to all emails and smart attachments:

1. Set the DLP Activator to **Enabled**.
2. Specify the string you want to add to all outbound Security Awareness Training emails. The string can contain only letters and numbers, and *cannot* contain spaces.
3. Click **Save**.

Security Awareness Training appends your custom text string to emails and smart attachments, formatted in tiny (0.1 pixel) white text, which is invisible on a white background.

Custom Headers

You can add up to four custom X-Headers to all of your outbound email messages for your

organization's use, such as enabling your support organization to more easily identify Security Awareness Training emails.

To append custom X-Headers to all of your outbound email messages:

1. Enter a **Name** and **Value** for an X-Header string.
2. Repeat for up to four Name-Value pairs.
3. Click **Save**.

Advanced Domain

Customer Awareness Domain

If you are using your organization's own domain for training campaigns, enter it here. Refer to Using Your Own Domains for background and instructions on setting up your own Customer Awareness Domain.

To specify your own Customer Awareness Domain for campaigns:

1. Enter the full domain and subdomain you created in Using Your Own Domains – usually in the format `securityawareness.yourcompany.com`.
2. Click **Save**.

Global Host Domain for Email Images

Optionally select a domain to host all email images, excluding inline images. This enables you to add this single domain to your Allow list, even if your campaigns use many different email and web domains. Note that images on the landing page will still be served from the landing page domain.

To specify the Global Host Domain for Email Images:

1. Select a domain from the menu.
2. Click **Save**.
3. *Outside of Security Awareness Training*: Add the domain you chose in Step 1 to your organization's Allow list.

Approvals

Require *all* campaigns to be approved before they can go live. Note that this setting affects all campaigns; you can also set this requirement per individual campaign.

1. Select the **Campaign Approval Required** checkbox.
2. Click **Save**.

Grant permissions for specific users to approve campaigns in User Management.

Outbound Sleep Time

The system sends out campaign messages at random intervals to prevent suspicion. The outbound sleep time is the maximum time, in seconds, between each outgoing email the system sends.

Levelized Campaigns

Set the default starting level for Program Calendar Terms, only used with Levelized Campaigns.
To learn about Levelized Campaigns, contact Barracuda Networks Support.

User Log Purge

With GDPR requirements, companies are now required to automatically purge user activity from their systems. This enhancement addresses one of those requirements by allowing the Security Awareness Training system to automatically purge administrative user activity logs.

The default purge period is two years.

To change the purge period:

1. Set the **User Log Purge Unit** to either **Month** or **Year**.
2. Select the number of months or years to retain records before purging.
3. Click **Save**.

The latest purge results are displayed at the bottom of the **User Log Purge** section.

The purge process is run at least once a day.

User Security Settings

All of the settings in this section concern user security and are all optional.

1. Adjust the settings for the following fields or select **Disabled**, as needed:
   - **Minimum Password Age** – Passwords younger than this value cannot be changed.
   - **Maximum Password Age –** Passwords older than this value must be changed. By default, this value is **3 months**, or 90 days.
   - **Disable Password Expiration for Accounts Using MFA** – Users with multi-factor authentication (MFA) do not have to change their password. By default, this check box is selected.
   - **Maximum Session Length** – Session lengths longer than this value will expire automatically.
   - **Maximum API Key Expiration** – API keys older than that age are considered to be expired. If an otherwise valid POST command occurs, but the API key is expired, the command cannot be executed.
   - **Maximum User Inactivity Period** – Users who do not log into Security Awareness Training for that length of time are automatically deactivated. If needed, reactivate accounts on the User Management page. Select from **30**, **60**, **90**, **180**, or **365** days. By default, this value is **Disabled**.
   - **Maximum User Session Inactivity** – Users who are idle for a specified amount of time are automatically logged off the system. Select from **15**, **30**, or **60 minutes**; **2**, **3**, **6**, or **10 hours**.
   - **Login IP Filter** – If you only want users to be able to log in from specific IP addresses, select **Enable Login IP Filter** and specify the values in the filter space below. Enter one or more IP values, separated by commas or line breaks. Only IPv4 addresses and Class C IPv4 blocks are supported. For IPv4 blocks, enter an asterisk for the last octet value (e.g., 192.168.1.*).

     Caution: Entering an invalid or incorrect **Login IP Filter** *will lock you out of your own account*. Check your entry carefully, before clicking **Save**.
2. Click **Save**.

Data Retention Configuration

For data privacy and/or storage reasons, you can optionally choose to automatically delete your campaign and results data after a certain retention period. An email notification is sent to the address(es) you specify. If you choose to automatically delete your data, consider backing up your data in case you need it after it is deleted from Security Awareness Training system.

Note that Barracuda will not be able to restore your data after it has been deleted in this manner.

By default, this setting is **Disabled**.

To set up Data Retention Configuration:

1. Specify the following settings:
    - **Retention Period** – Specify how many years you want to save your data, after which it will be permanently deleted. Choose between **1-7 years**. Time period is measured from the Campaign Cutoff Date. Data retention deletion checks occur on the first day of each month. If data is older than the age you select, data is also deleted on the first day of the month.
    - **Retention Notification Weeks** – Specify the time frame before the deletion you want to receive a notification email. Choices are **1 week**, **2 weeks**, and **3 weeks**.
    - **Retention Notification Email** – Specify one or more email addresses to receive advanced email notification of the automatic data purging. Separate multiple email addresses with commas.
2. Note the informational fields:
    1. **Last Notification Sent** – Date the system last notified you of a pending deletion.
    2. **Last Deletion Date** – Date the system last deleted data.
    3. **Next Deletion Date** – Date the system will check if any data is ready to delete – always on the first of the next month. If any data is older than the age you select, data will also be deleted on this date.
3. Click **Save**.

The email notification provides you sufficient time to change or disable the data retention configuration, so your data is not purged without your permission. You can increase your Retention Period to a larger number, but you cannot combine time periods to increase the Retention Period past 7 years.

Activity Filter

Select whether you want to explicitly block certain entities, like ISPs or IP addresses.

To set up Activity Filter configuration:

1. Select **Block** as the filter type to prevent activity from one or more specified entities.
2. Specify one or more filters. Select one of the following choices for blocking based on these criteria. Be sure to read the General Filtering Guidelines section below.
    - **by IP Address** – Filter based on a single IP or a range of IPs.
        - Only IPv4 and Class C IPv4 blocks are supported.
        - To specify an IPv4 block, enter the first three octets and end with an asterisks. For example, 192.168.1.*.
    - **by IP Country** – Filter based on the country in which the IP is registered.
    - **by IP Organization** – Filter based on a specific organization name.
    - **by ISP** – Filter based on an Internet Service Provider (ISP).

        - Use the full name or use a wildcard for a larger filter. For example, *Acme Networks* or *Acme**.
    - **by Machine Click Score** – Filter based on an integer score, showing how likely it is that a click was made by a machine, rather than by a human.
      Enter an integer. No wildcards. Scores of 3 and above are most likely clicks made by a machine. For more information on Machine Click Score, refer to Address Book Utility.
      Activities are *blocked* if the score is *greater than or equal to* the value entered.
    - **by OS type** – Filter based on operating system name.
3. To specify additional filters, click the plus button to create a new row. Then repeat step 2.
   For example, if you want to block by more than one IP country, create a new row for each IP country you want to block.
   If needed, click the minus button to remove a filter.
4. Click **Save**.

General Filtering Guidelines

- Only specify one value per field. If you want to block by two different IP Countries, create two different filters, one for each country.
- Use asterisks (*) as wildcards, where permitted. For example, use the full name or use a wildcard for a larger filter. For example, use Acme Networks or Acme*, as described above.