Users & Security Guide

3/22/2016 Blackbaud NetCommunity 7.0 Users & Security US

UserSec-2016

Contents

Users & Security

In *Users & security*, you manage user records, assign security, and import constituent information exported from other Blackbaud products to create website users. Security in the program is determined by roles, task groups, and security assignments. Create roles to group users together. Create task groups to establish feature permissions in the program. Use security assignments to associate roles and task groups to apply security throughout the program.

Show Me: Watch an overview of security in Blackbaud NetCommunity.

Security Overview

The security model for the program allows you to create a structure that is as simple or complex as needed. Security components include users, roles, task groups, and security assignments. These components answer the security questions of who, what, and where.

Tip: It is important to maintain security because it protects your website, promotes consistency, and helps prevent errors.

Users

The user record authenticates a website user's identity. User records are created manually by a Supervisor or automatically when a user signs up for a website through the User Login, Personal Page Manager, or Fundraiser parts. For more information, see Users on page 8.

Roles

Roles are user records grouped together manually or by query. Roles can also include other roles. For more information, see Roles on page 14.

Task groups

Task groups assign feature permissions for administrative tasks. These permissions include the features accessible from the menu bar, such as *Site explorer* and *Administration*. For example, a Supervisor creates a task group called Content Authors and selects full rights for pages, images, and templates. For more information, see Task Groups on page 21.

Note: Task groups do not determine *who* has task rights. Task groups simply organize rights to associate with a role in *Security assignments*. Task groups are *not* directly connected to user records or roles.

In addition to the administrative security in *Task groups*, you can assign view, edit, delete, and change security rights for users and roles for your website. You can assign rights for individual parts, pages, templates, and images on the Targeting & Security tab. For example, on a Documents part, you can assign view rights to the Board Members role so they can review the minutes from the previous Board meeting. For more information, see the *Parts Guide*.

Security assignments

Create security assignments to associate roles and task groups to apply security to a site. If you host one website, all security assignments apply to the default site. If you host multiple websites, security assignments apply to specific sites. Security assignments are crucial to the integrity of your database when you host multiple sites. For more information, see Security Assignments on page 29.

Show Me: Watch an overview of security in Blackbaud NetCommunity.

Security Examples

Review this information for low, medium, and high security scenarios and how to implement them in *Users & security*.

- **Low security scenario**: Your Board Members require view permissions only for Board Member specific site pages. They should not have rights to create, edit, or delete content.

  To establish this low-level security, in *Roles*, create a role to group Board Members. You can do this by selecting a query or by including the individual members on the Members tab. Do not associate the role with a task group because Board Members should not be granted permissions for administrative tasks. Because there is not a role and task group association, there is not a security assignment for the role.

Note: Task groups assign feature permissions for administrative tasks. To provide view rights for Board Members on your website, assign the **View** permission to the role on the Targeting & Security tab for the applicable pages, parts, and images. For more information, see the *Parts Guide*.

- **Medium security scenario**: Your Development Staff requires unique permissions for content author rights to specific site pages.

  To establish this medium-level security, in *Roles*, create a role to group Development Staff members. You can do this by selecting a query or by including the individual members on the Members tab. In *Task groups*, select the following site task rights under **Website security**.

  Under **Page tasks**, select **Can create new Pages** and **Has access to Pages in Site Explorer**.

  Under **Part tasks**, select **Can create new Parts** and **Has access to the Part Gallery**.

  Under **Image tasks**, select **Can upload Images** and **Has access to Image Library**.

  In *Security assignments*, associate the role and task group and assign it to the development site.

Note: Task groups assign feature permissions for administrative tasks. To provide security for the Development Staff from your website, assign the **View** and **Edit** permission to the role on the Targeting & Security tab for the applicable pages, parts, and images. For more information, see the *Parts Guide*.

- **High security scenario**: Your Web Designer requires unique permissions for rights to edit pages, templates, and layouts. However, they cannot access *Workflows* and *Merchant accounts*.

  To establish this high-level security, in *Roles*, include individual Web Designer users in a role.

  Under **Page tasks**, select **Has all Page related rights**.

  Under **Template tasks**, select **Has all Template related rights**.

  Under **Layout tasks**, select **Has all Layout related rights**.

  In *Security assignments*, associate the role and task group and assign it to your default site.

Note: To provide security for the Web Designers from your website, you can assign all permissions to the role on the Targeting & Security tab for the applicable pages, parts, and images. For more information, see the *Parts Guide*.

For more information about *Roles*, see Roles on page 14.

For more information about *Task groups*, see Task Groups on page 21.

For more information about *Security assignments*, see Security Assignments on page 29.

Users

In *Users*, you can add and manage users accounts for your website. User records contain basic biographical and user login information. When a user signs up for your website through the User Login, Personal Page Manager, or Fundraiser parts, the program automatically creates a user record.

Note: Only users with Supervisor rights can view and manage *Users*.

To search for a user, use the fields in *Users* to filter by name, login, or role. To narrow the search to users linked to records in another Blackbaud program or to users not linked to any records, use the **Linked to** field. If you select **Deleted**, the search includes deleted users.

Your database always includes a Supervisor record. You can edit this record, but you cannot delete it.

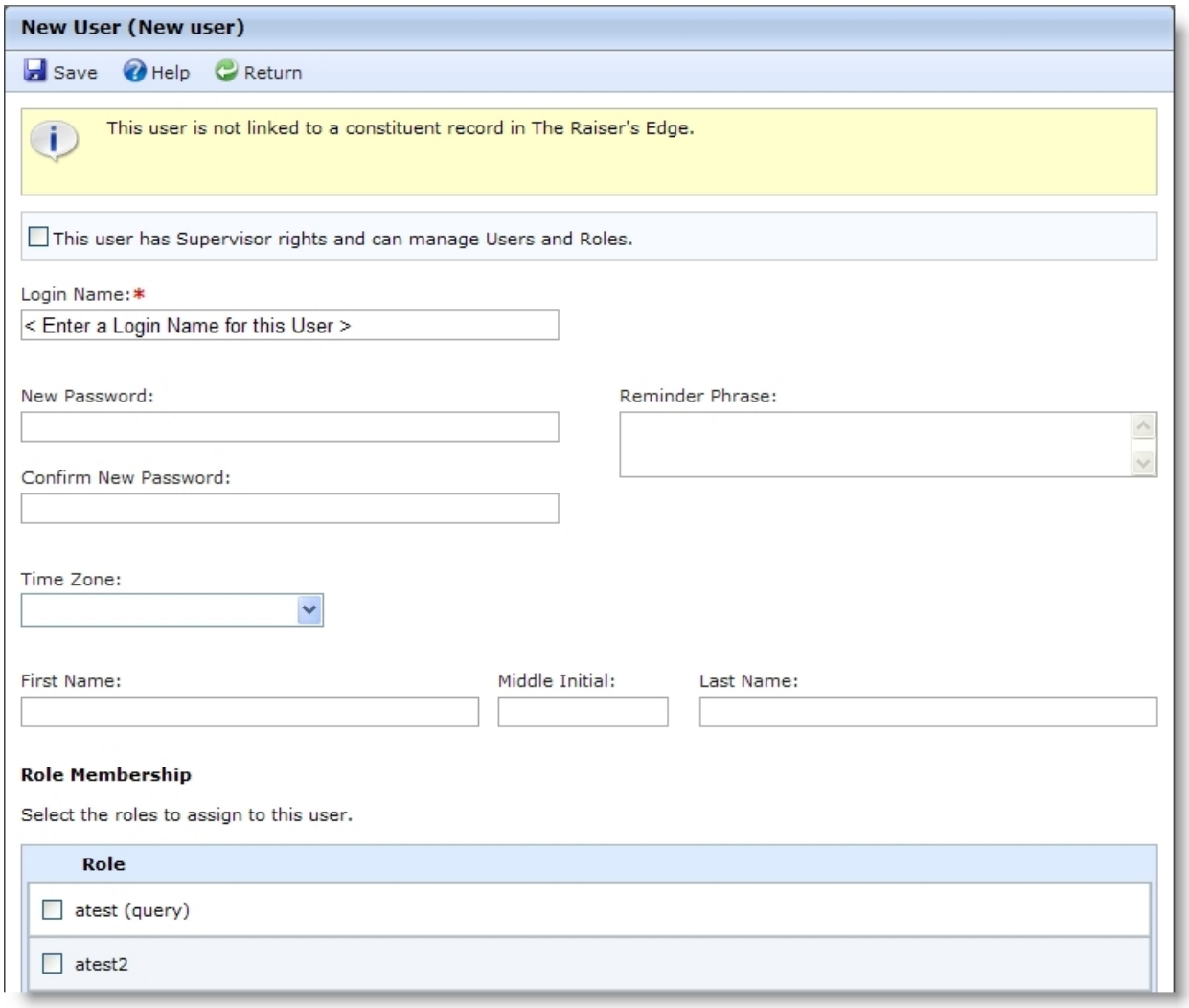
To view or edit a user's constituent record, select the user in the grid and click **Click here to view this constituent**. If this does not appear, a constituent record does not exist for the user in The Raiser's Edge.

In *Users*, you assign users to roles. To create a role, see Roles on page 14.

Show Me: Watch an overview of security in Blackbaud NetCommunity.

Create a user

1. In *Users & security*, click **Users**. *Users* appears.
2. Click **New user**. The New user page appears.



3. To enable the user to access all areas of the program, including the ability to set security rights for others, select **This user has Supervisor rights and can manage Users and Roles**.

   Users with Supervisor rights manage *Users*, *Roles*, *Task groups*, *Security assignments*, *Merchant accounts*, *Code tables*, and *User imports*. When this checkbox is not selected, the user cannot view these areas. In addition, Supervisor users are logged out of the program automatically when it is idle for more than 15 minutes. To avoid this, select the **Remember me** checkbox when you log into the program.
4. In the **Login Name** field, enter a login name for the user. The user name must be unique.
5. In the **New Password** field, enter the password for the user.

Note: If you select **Require complex passwords** in *Sites & settings* or if you intend to grant the user Supervisor rights, enter a complex password. This password must contain at least eight characters, including at least one upper-case and lower-case letter, and either a special character or a number.

6. In the **Confirm New Password** field, re-enter the password.

   When you create a user, the **Reminder Phrase** field is disabled.

7. In the **Time Zone** field, select the user's time zone. For example, if the user is in New York, select America/New York (EST) GMT-5:00.

Note: The program uses Coordinated Universal Time (UTC) as its time standard. Time zones are expressed as offsets from the UTC. This enables the program to retain time and date information and display it accurately in multiple time zones.

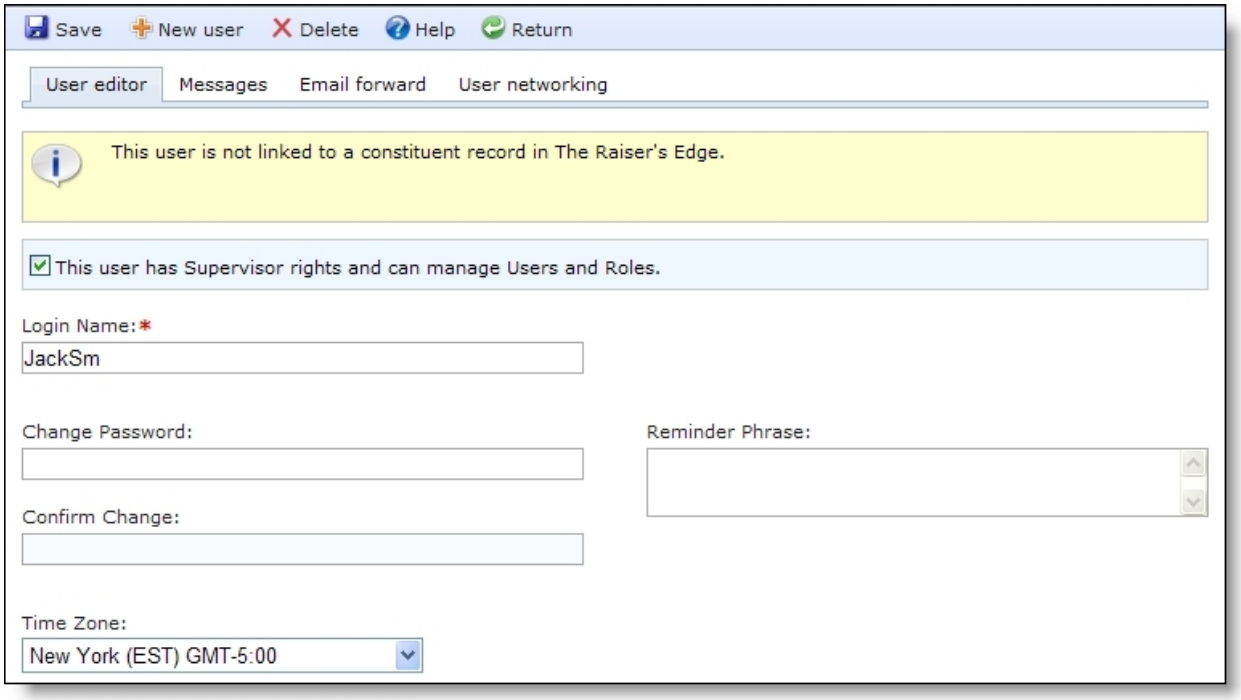
   The time and dates the user sees on your site pages and email use the time zone you selected here or the default time zone selected from *Sites & settings*.

8. In the **First Name**, **Middle Initial**, and **Last name** fields, enter the user's name.
9. In the **Role Membership** grid, select the roles to assign to user. Roles act as security for sections of the program and the website. When you assign task rights to roles, users in the roles are granted access.
10. Click **Save**. You return to *Users*.

    To edit the user rights, select the user and click **Click here to edit this user**. The User Editor page appears. On the User Editor tab, the information you entered in this procedure appears. Additional tabs also appear. For information about these tabs, see View and edit a user on page 10.

View and edit a user

1. From *Users & security*, click **Users**. *Users* appears.
2. Select the user and click **Click here to edit this user**. The User editor page appears.
3. On the User editor tab, information appears from when the user was created. For more information about these fields, refer toCreate a user on page 8.



Tip: If you select **Allow team captains to manually add new team members** or **Add non-anonymous attendees to registrant's during event registration** on a Fundraiser part, "<Enter a Login Name for this User>" may appear in the **Login Name** field. In *Users*, "[user account not activated]" appears in the **Login** column. This indicates the user is a member of a team but has not registered for the Fundraiser on your website. For more information, refer to the *Team Fundraising Guide*.

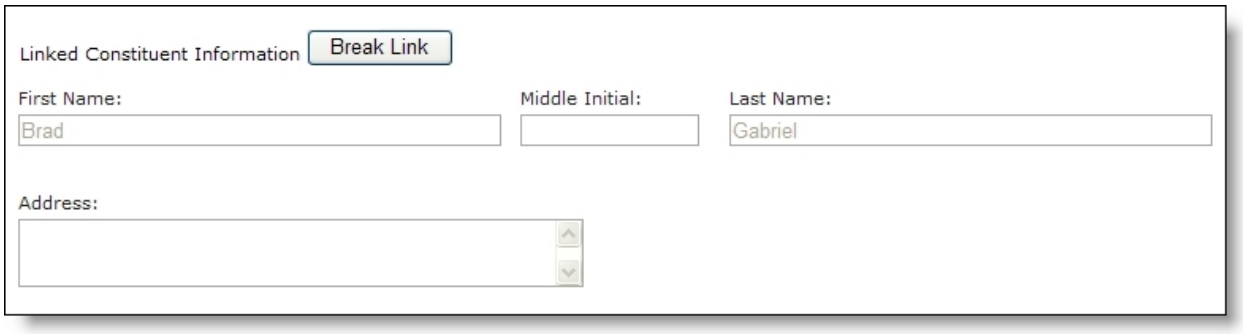
If the user has been deleted, a message appears above the login name. For information about how to restore a user, refer to Restore a deleted user on page 14.

If the user's account has been locked, a message appears above the login name. To allow the user to access the account, click **Unlock**.

4. To enable the user to access all areas of the program and set security rights for others, select **This user has Supervisor rights and can manage Users and Roles**.
5. In the **Login Name**, **Change Password**, **Reminder Phrase**, and **Time Zone** fields, review the information entered when you created the user or the website user created the account.
6. To change the password, enter the new password in the **Change Password** and **Confirm Change** fields. In the **Reminder Phrase** box, enter a phrase or question to help remind the user of the password.

Note: If you select **Require complex passwords** in *Sites & settings* or if a user has Supervisor rights, you must enter a complex password. The password must contain at least eight characters, including at least one upper-case and lower-case letter, and either a special character or a number.

7. If the user is linked to an offline constituent record, **Linked Constituent Information** appears above the name fields, along with address information. You cannot edit these fields.



To break the link between the user record and the constituent record, such as if you link the user to the wrong constituent, click **Break Link**. If you want to generate a new sign-up transaction to link to a different constituent record, you must delete the user record and then restore it. For more information, refer to Restore a deleted user on page 14.

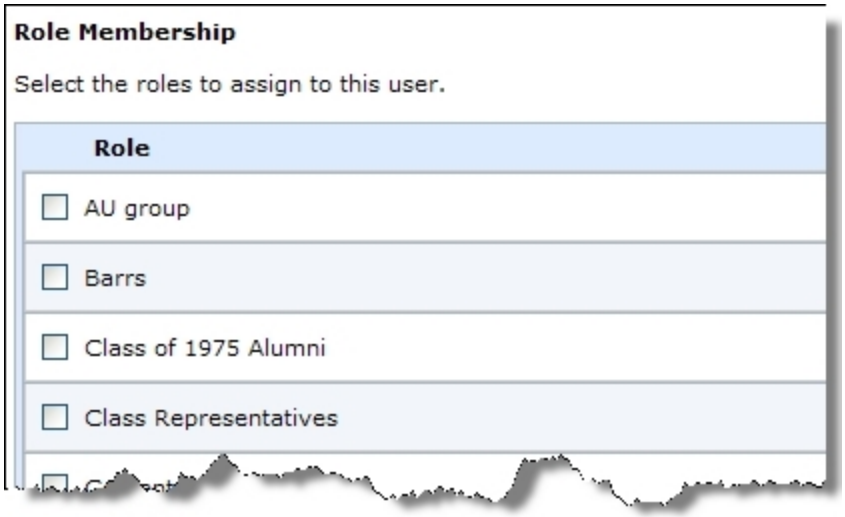
8. If the user has a personal page dashboard, the **Fundraiser Participation** or **Personal Pages** grid appears. In the **Fundraiser** or **Personal Page Manager** column, the dashboard name appears.

- To access the dashboard, in the **Page** column, click **Visit**.
- To copy a URL link to a user with Administrator rights, in the **Dashboard** column, click **Administer**. Users with Administrator rights for the part can edit the dashboard. The URL link bypasses the login for the dashboard user so the Administrator can access the page.
- For a Personal Page Manager dashboard, to remove the dashboard for the user, click **Delete**.
- For a Fundraiser dashboard, in the **Performance Units** column, adjust the user's performance. If the user completed the fundraiser, select the checkbox in the **Performance Completed** column.

9. In the **Query-Based Membership Last Refreshed On** field, the date when the query was last refreshed appears. To refresh the query, click **Refresh Now**. When you refresh the query, the user is granted the additional rights assigned to the role.

   If the user is in multiple query-based roles, all queries refresh to include the user.

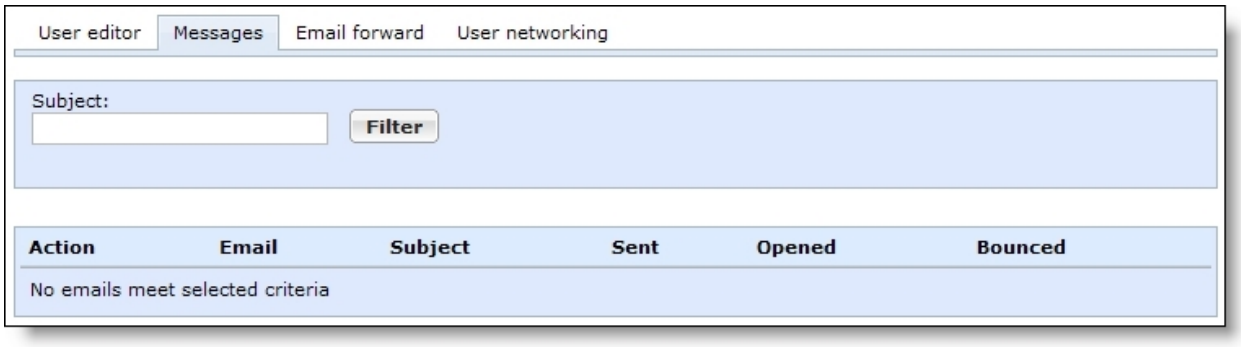
10. In the **Role Membership** grid, select the roles to assign to the user. When you associate roles and task groups to assign security, users in the role receive that security access. For more information, refer to Security Assignments on page 29.



11. To refresh the query the user is in, click **Refresh Now**. When you refresh the query, the user is granted the additional rights assigned to the role. If the user is in multiple query-based roles, all queries refresh to include the user.

Note: If **Refresh Now** does not appear, the user is not linked to an offline record. Therefore the user cannot be refreshed for a query-based role.

12. To view a list of email messages sent to the user, select the Messages tab.



Note: Users who select the global opt-out checkbox on the website still receive requested notifications and acknowledgement email messages.

13. To set up email forwarding for the user, select the Email Forward tab. If a website user sets up an email forwarding address, select this tab to view or change the information.

    This tab shares email forwarding data with the Email Forwarding Form part. A website user who accesses the Email Forwarding Form from a page on your website can change the addresses you enter on the Email Forward tab.

14. To enable email forwarding, select **Enabled**.
15. In the **Incoming Email Address** field, enter the email address the user set up for forwarding, such as MUAlumni_1981.

    Your email domain appears after the field. If you have multiple domains, select the domain to use.

16. In the **Forwarding Address** field, enter the user's original email address.

    If the user's address changes, enter the new address here. This way, other users are never aware of the change and continue to use the email forwarding address. If a user changes the address, this field updates the information automatically.

17. To view user networking information about the user, select the User Networking tab. If the user has a user networking account on your website, information about the account appears.

The tab displays the user's profile image and display name, when the user created and last updated the user networking account, and the URL to the user's account profile page. If you enable ranking on the User Networking Manager part, the user's rank also appears. If a user changes the user networking profile image or display name, the program updates this tab with the new information.

18. Click **Return**. You return to *Users*.

Restore a deleted user

1. In *Users*, select **Deleted** and click **Filter**. The grid displays all deleted users.
2. Select the user and click **Click here to edit this user**. The User editor page appears. Above the user's login name, a message notes that the user is deleted.

3. To restore the record:
   - If the user was linked to an offline constituent record, click **undelete**. The program restores the user and the link to the constituent record and removes the deleted user message.
   - If the user was not previously linked to an offline constituent record, click **undelete and generate a sign-up transaction**. The program restores the user, generates a pending sign-up transaction, and removes the deleted user message. When you process the sign-up transaction, you can link the user to a constituent record.
4. Click **Return**. You return to *Users*.

Roles

Roles are user records grouped together individually, by a query, or by including existing roles in a role.

- To group user records individually, you can assign the user to a role from the user record or you can include the user when you create or edit a role.
- To select a query for a role, create the query in another Blackbaud product. When you create a role, you select the query to include in the group.
- Similar to user records, you include an existing role for a role from the role's Members tab. For example, you have an Intranet site for your organization. You have roles that exist for "Development Staff," "Event Staff," "Membership Staff," and "Web Designers." You can create role called "Our Staff" to group these existing roles into one role to support Intranet security.

Note: Only users with Supervisor rights can view and manage *Roles*.

After a new website user is accepted in a download transaction, the user has anonymous rights and is referred to as a "provisional" user. To grant access to secure web pages, you include the user in a role that is associated with a task group that has the applicable permissions. To update the role to include the new user, you need to refresh the role. You can do this in two ways.

- You can manually refresh the role so the user has additional access to secure web pages rights immediately.
- You can wait for the next standard refresh to process.

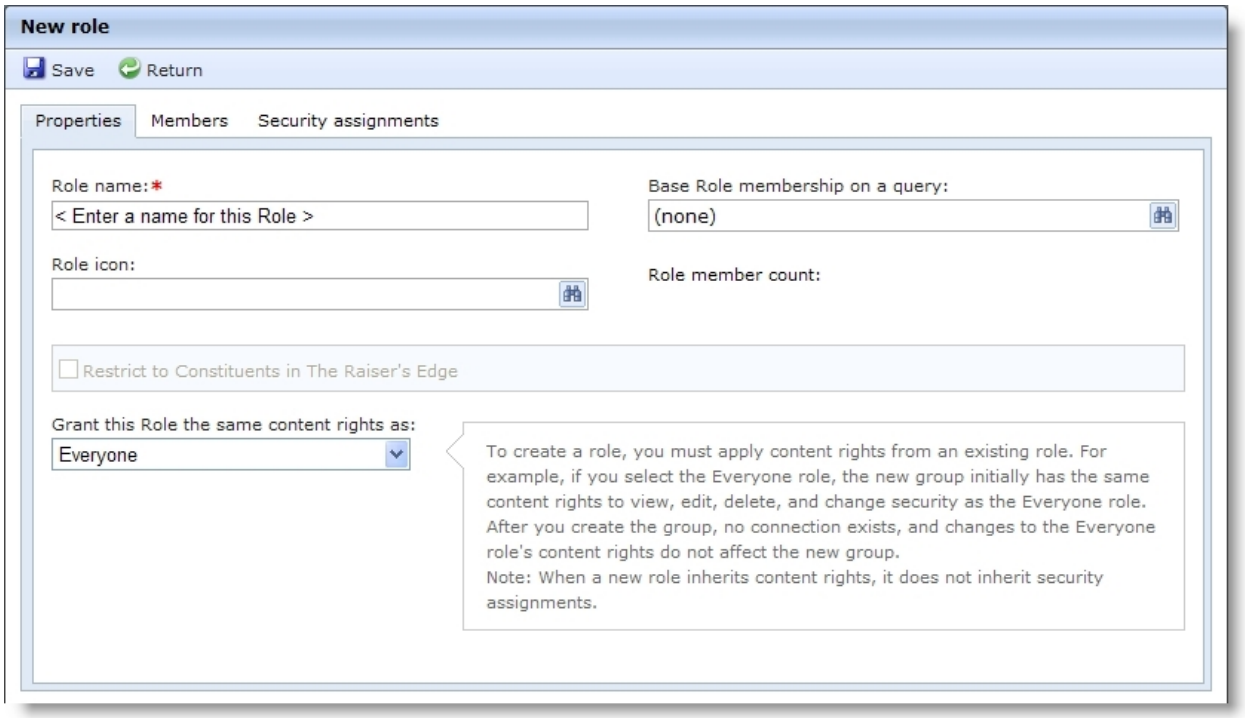
For more information, see Role Refresh on page 19.

Note: In *Roles*, you include user records in groups. In *Task groups*, you create task rights for feature permissions. In *Security assignments*, you associate roles and task groups to assign security for a site. For information about *Task groups* and *Security assignments*, see Task Groups on page 21 and Security Assignments on page 29.

Show Me: Watch an overview of security in Blackbaud NetCommunity.

Create a role

1. In *Users & security*, click **Roles**. *Roles* appears.
2. Click **New role**. The New role page appears.



3. On the Properties tab, in the **Role** field, enter a name for the group such as "Class of 1989 Content Author," "Gold Member," or "Class of 1989 Administrator."
4. To associate an image with the role, click the binoculars in the **Role icon** field. The Select Image from Image Library screen appears. For information about how to select an image, see the *Program Basics Guide*.

   When you associate an image with a role, you can use the **Role Block** merge field on a Profile Display web page to display the role image on a user's profile. If a user is in multiple roles with images, all images display on the web page. Images can provide a visual about the role. For example, an image with a notepad and pen can indicate the role includes content authors. For information about the Profile Display part, see the *Parts Guide*.
5. Assign users to the role.
   - To automatically assign users to the role now, click the binoculars in the **Base Role membership on a query** field. A search screen appears to select the query of users to include.

Note: When you create a query in another Blackbaud program, you may need to refresh Blackbaud NetCommunity for it to appear as a selection. To refresh, select **View**, **Refresh** in the menu bar.

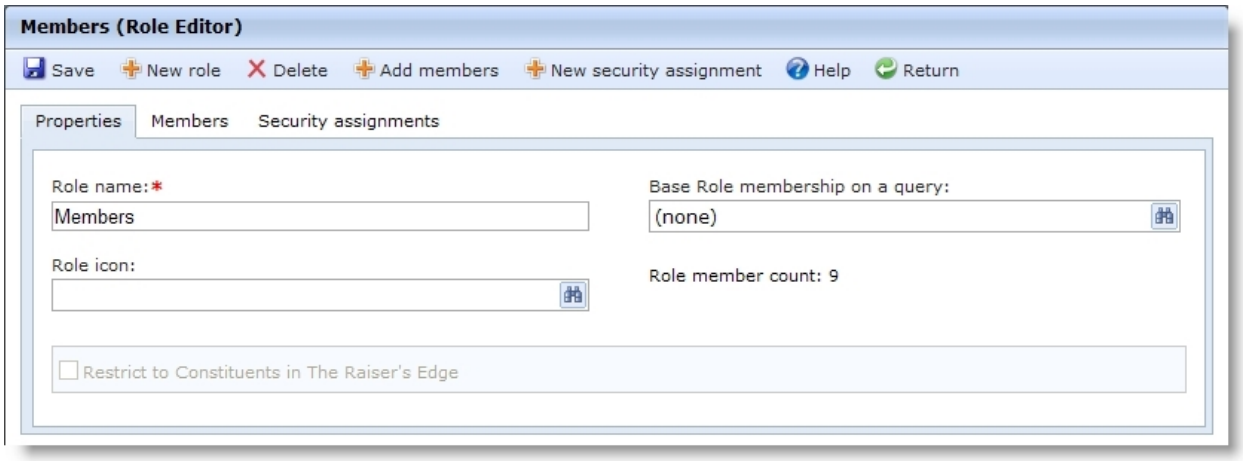
   - To assign users individually to the role later, in the **Base role membership on a query** field, leave the default "(none)."
6. In the **Grant this role the same content rights as** field, select an existing role to assign the same content rights for the new role.
7. Click **Save**. You return to *Roles*.

   After you save the role, you can modify the Members and Security assignments tabs. For information, see Edit a role on page 17.

Edit a role

When you edit a role, you can edit its properties, add users, roles, and it with a task group to assign security.

1. In *Users & security*, click **Roles**. *Roles* appears.
2. Select a role and click **Click here to edit this Role**. The Role Editor page appears.



3. On the Properties tab, edit the fields as necessary. For information, see Create a role on page 15.
4. If the role includes a query in the **Base Role membership on a query** field, you can refresh the role. To do this, click **Refresh Now**. After the refresh, the new member count appears in the **Role member count** field, and the date and time of the refresh appears in the **Role last refreshed on** field.

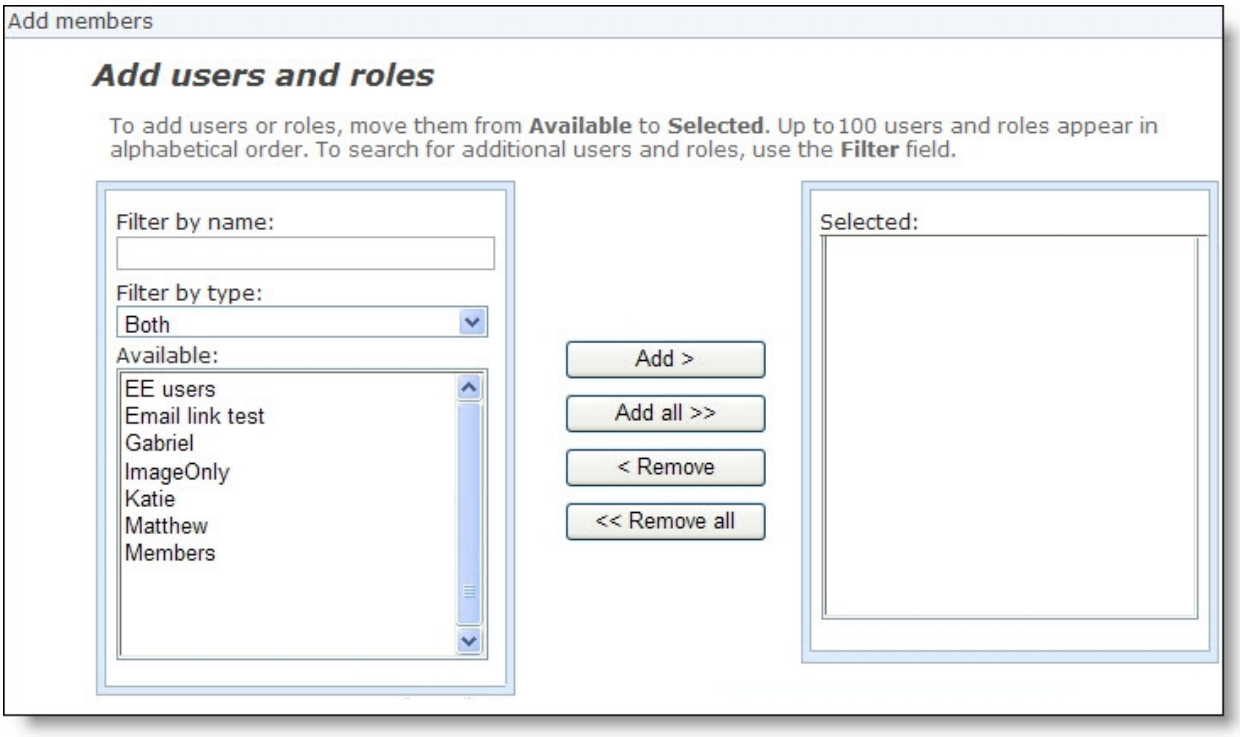
Tip: To view the contents of the log file for the refresh, return *Roles*. Click **Role refresh**. The Role Refresh page appears. This page displays a log file from the last refresh. For more information about this screen, see Refresh all query-based roles in the database on page 20.

5. Select the Members tab.

Note: The grid displays 50 users and roles in alphabetical order. To search for additional users or roles, use the filter fields. The grid only displays users and roles that you add directly to this role. It does not display users or roles that are included through another role.

   a. To include users and roles, click **Add members**. The Add members screen appears.

Tip: To improve efficiency, you can include roles in the role. For example, you have an Intranet site for your organization. You have roles that exist for "Development Staff," "Event Staff," "Membership Staff," and "Web Designers." You can create role called "Our Staff" to group these existing roles into one role to support Intranet security.



b. In the **Filter** field, enter the first letter of the user or role to include.

Note: The **Available** box displays 30 users and roles in alphabetical order. Use the **Filter** field to find additional users and roles that do not appear in the box.

c. Locate the user or role, and click **Add**. The user appears in the **Selected** box.

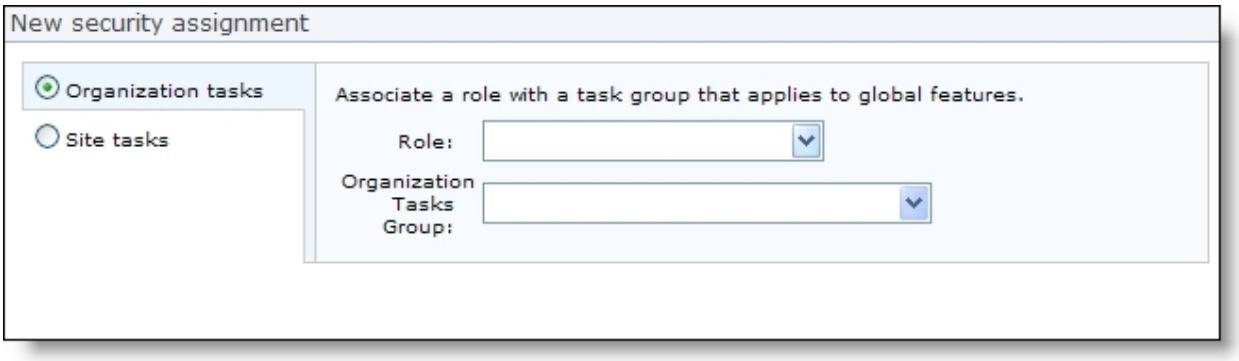
   To select multiple users or roles, press **SHIFT** while you select the multiple users, and then click **Add**. The users appear in the **Selected** box.

d. To return to the Members tab, click **OK**.

6. Select the Security assignments tab. The grid displays the existing security assignments for the role, along with the task group, site, and child sites information.

Note: To apply security in the program, you associate a role and task group for a site in *Security assignments*. You can create these assignments for roles on the Security assignments tab. This allows you to modify the task rights for the role. For example, to grant rights to *Pages & templates* for the Content Authors Charleston Chapter role, go to the Security assignments tab and create a security assignment that associates the role with a task group that provides rights to *Pages & templates*.

- To edit a security assignment, select it and click **Click here to select this security assignment**. For information, see Edit a security assignment on page 31.
- To create an assignment, click **New security assignment**. The New security assignment screen appears.



For information about how to create a security assignment, see Create a security assignment on page 29.

Click **Save** and you return to the Security assignments tab. The security assignment appears in the grid.

7. Click **Save**. You return to *Roles*.

Role Refresh

New website members are not part of queries in other Blackbaud programs until you download them to the program from Blackbaud NetCommunity. New members are initially granted anonymous access rights and referred to as "provisional" members. By default, roles are not assigned to these members but you can assign roles through the User Login part. It is important to decide the content to present to provisional members. Without a role, provisional members view the same content as the Everyone role. These users have the same access as anonymous on your website.

After another Blackbaud program accepts a newly registered user in a download transaction, the program includes the user in queries. The role needs to be refreshed to include the user. You can do this manually to provide access to secure web pages immediately, or you can wait for the next standard role refresh to process.

Standard Role Refresh

The program refreshes roles every 24 hours after a member's last login. If no other Blackbaud program accepts the member in a download transaction since the last login, there is no role to refresh. After another Blackbaud program accepts the member in a download transaction, the role refreshes upon the next login, and the program sets the 24 hour interval to that date and time.

You can edit the standard role refresh settings as necessary. For information, see the *Administration Guide*.

Manual Role Refresh

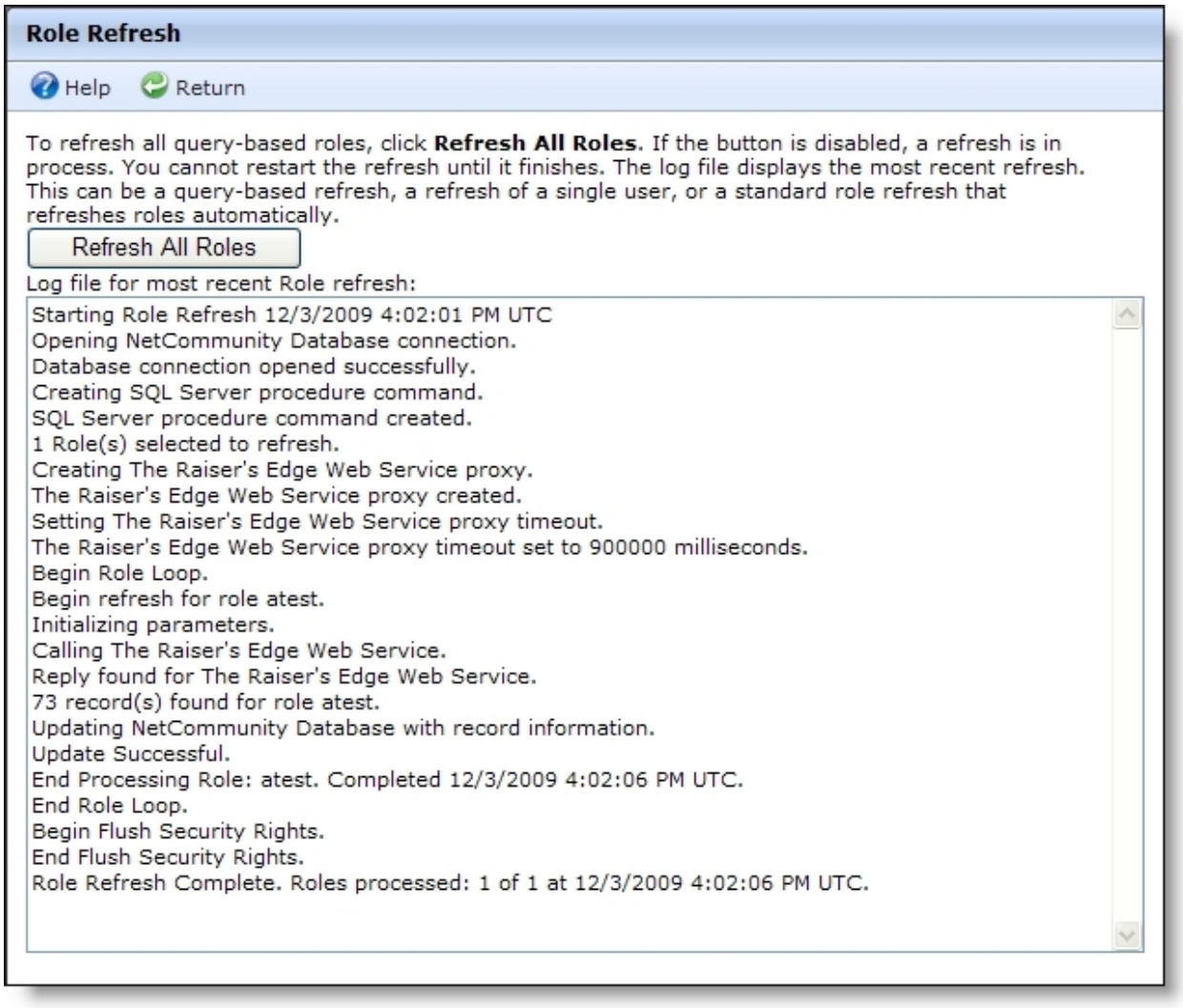
A Supervisor can manually refresh users and roles. For information about how to refresh a user, see View and edit a user on page 10. For information about how to manually refresh individual roles, see

Edit a role on page 17. For information about how to manually refresh all query-based roles in the database, see the procedure in this section.

Refresh all query-based roles in the database

To manually refresh all query-based roles in your database, review this procedure. To manually refresh an individual query-based role, see Edit a role on page 17.

1. In *Users & security*, click **Roles**. *Roles* appears.
2. Click **Role refresh**. The Role Refresh page appears.



This screen displays a log file from the previous role refresh processed in the program. This includes a refresh of all roles on this screen, a manually refresh of a single user, or the standard role refresh that refreshes roles automatically. For more information, see Role Refresh on page 19.

3. To refresh all query-based roles, click **Refresh All Roles**. The refresh begins. Depending on your environment and the number of roles in the database, this may take several minutes.

When the refresh is complete, "Role Refresh Complete" appears in the last line of the log.

Tip: The log file is view only. The file is stored in your database unless you designate another location in *Sites & settings*. For more information, see Role Refresh on page 19.

4. Click **Return**. You return to *Roles*.

Task Groups

In *Task groups*, you create and edit task groups for feature permissions for administrative tasks. These permissions include the features accessible from the menu bar, such as *Site explorer* and *Administration*. Task groups do not determine *who* has task rights. Task groups simply organize rights to associate with a role in *Security assignments*. You associate task groups with roles so users can perform tasks on the website. For example:

- The Web Designer may create web pages from start to finish and needs assistance from co-workers. You can associate the Web Designer role with a task group that has security rights to all areas of the program.
- The Director of Special Events may update last year's golf tournament web page with this year's information. You can associate the Event Managers role with a task group that has security rights to create and edit parts. This allows the Director to update the Event Registration Form part with this year's information.

It is important to remember that task groups are *not* directly connected to user records or roles.

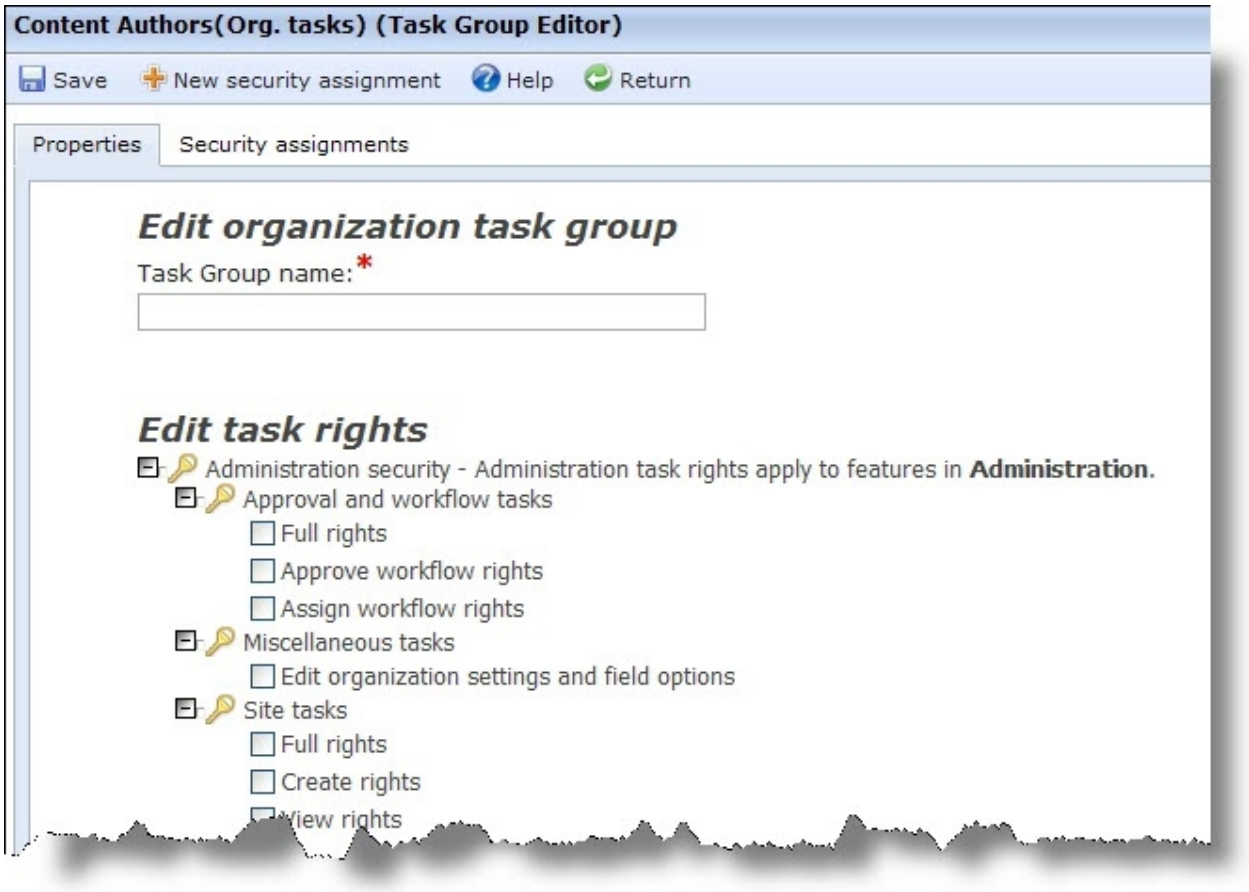
Note: In *Roles*, you include user records in groups. In *Task groups*, you organize related rights for feature permissions. In *Security assignments*, you associate roles and task groups to apply security for a site. For information about *Roles* and *Security assignments*, see Roles on page 14 and Security Assignments on page 29.

Show Me: Watch an overview of security in Blackbaud NetCommunity.

Edit a task group

When you edit a task group, you can edit the properties for the task group and you can associate a role with the task group to assign security.

1. In *Users & security*, click **Task groups**. *Tasks groups* appears.
2. Select a task group and click **Click here to edit this task group**. The Task Group Editor page appears.



3. On the Properties tab, in the **Task group name** field, edit the task group name as necessary.
4. Under **Edit task rights**, select the feature permissions for administrative tasks to include. These permissions include the features accessible from the menu bar, such as *Site explorer* and *Administration*.

Note: The available feature permissions depend on the task group type you select. For example, organization task groups appear for miscellaneous tasks and site task groups appear for website tasks. For detailed information about the checkboxes on these screens, see Task Group Rights Details on page 23.

It is important to remember this grants permissions to the users and roles associated with this task group in *Security assignments*.

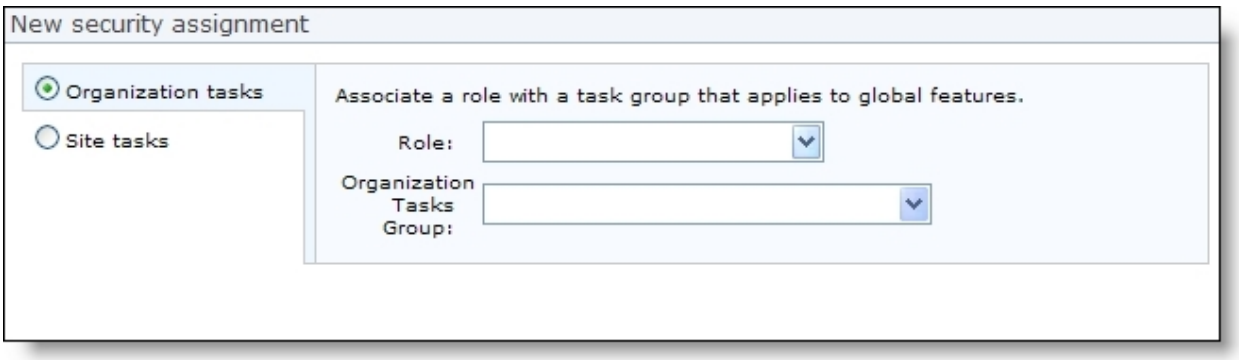
In addition to these rights, you assign view, edit, delete, and change security rights for users and roles for your website on the Targeting & Security tab for individual parts, pages, templates, and images. For example, on a Documents part, you can assign view rights to the Board Members role so they can review the minutes from the previous Board meeting. For more information, see the *Parts Guide*.

5. Select the Security assignments tab. The grid displays the existing security assignments for the task group, along with the role, site, and child sites information.

Note: To apply security in the program, you associate a role and task group for a site in *Security assignments*. You can create these assignments for roles on the Security assignments tab. This

allows you to modify the task rights for the role. For example, to grant rights to *Pages & templates* for the Content Authors task group, go to the Security assignments tab and create a security assignment to associate the task group with a role that needs rights to Pages & security.

- To edit an assignment, select it and click **Click here to select this security assignment**. For information, see Edit a security assignment on page 31.
- To create an assignment, click **New security assignment**. The New security assignment screen appears.



For information about how to create a security assignment, see Create a security assignment on page 29.

Click **Save** and you return to the Security assignments tab. The security assignment appears in the grid.

6. Click **Save**. You return to *Task groups*.

Task Group Rights Details

In *Task groups*, most feature permission areas are broken into three levels. Generally, these are **Full rights**, **Create rights**, and **View rights**. **Full rights** grants create, edit, and delete rights, as well as rights to view and edit information other users create. **Create rights** grants rights to create content and edit rights for content the user created. View rights grants view-only rights to the applicable section of the program, but not rights to create or edit information.

Other task right details include:

- Every feature permission grants rights to Help.
- For security changes to take effect, users must log out and log back into the program.
- When rights are removed from a role, users in the role retain the previous rights for existing content. For example, a user creates a web page. Later, create rights for pages are removed for the role the user is in. The user can no longer create pages, but can edit or delete the page previously created.
- You can also use Targeting & security tabs to grant rights. These tabs allow you to grant rights for individual parts, pages, templates, and images rather than for entire feature areas. For example, if members of a role only need full rights for select parts, you shouldn't assign full rights to parts in Task groups because this gives them full rights to all parts. Instead, you can use the Targeting & security tabs on the parts that this role manages to grant full rights for just those parts.

Review the following sections for details about the checkboxes on the Edit organization task group and Edit site task groups screens.

Organization Task Rights Details

Organization task rights apply globally to your entire website.

Approval and Workflow Tasks

Any rights selected under **Approval and workflow tasks** provide view rights to *Workflows* in *Administration*.

Full rights grants view rights to Workflows in *Administration* and *Approvals* in *Site explorer*. When you select this checkbox, you include rights for **Approve workflow rights** and **Assign workflow rights**.

Approve workflow rights grants rights to view *Approvals* in *Site explorer*. To actually view and manage content, the user must also have full rights to part tasks.

Assign workflow rights grants rights to manage workflows and to create workflow notifications. These rights only apply to notifications in *Workflows*. They do not apply to notifications in *Email*.

For more information about these rights, see the *Website Design Guide*.

Miscellaneous Tasks

Edit organization settings and rights grants rights to change settings in *Sites & settings* and field options in *Administration*.

Sites Tasks

Full rights grants rights to add, edit, and delete sites, as well as rights to view and edit sites other users create.

Create rights grants rights to add and edit sites. It also grants view-only rights to sites other users create.

View rights grants rights to view *Sites & settings* in *Administration*.

Site Task Rights Details

Site task rights apply to an individual site.

Page Tasks

Any rights selected under **Page tasks** provides view rights to *Pages & templates*. These rights also control if a user can add, edit, and delete folders

Full rights grants rights to create, edit, and delete pages, as well as rights to view and edit pages other users create. In addition, this applies the same rights to friendly URLs.

Create rights grants rights to create pages and edit pages a user created. To grant rights to pages other users create, assign permissions on the Targeting & Security tab for the page. This set of rights also applies to friendly URLs.

View rights grants rights to view *Pages & templates* and *Friendly URLs* in Site explorer.

Part Tasks

When a user has part rights, but does not have rights to page and template tasks, the user cannot view *Pages & templates* and *Friendly URLs*.

Full rights grants rights to create, edit, and delete parts, as well as rights to view and edit parts other users create.

Create rights grants rights to create parts and edit parts a user owns. To grant rights to parts other users create, assign permissions on the Targeting & Security tab for the part.

View rights grants rights to view *Parts* in Site explorer.

After you select these rights, you can apply the rights to all parts or individual parts. To apply the rights to all parts, select **All parts**. To apply the rights to a select number of content management parts, select **Content management parts** and select the checkbox beside each applicable part that appears. To view a list of every part type in Blackbaud NetCommunity, select **Individual parts**. To apply the rights, select the checkbox beside each applicable part in the list.

Image Tasks

Users with access to *Image library* have the ability to add, edit, and delete image folders.

Full rights grants rights to add, edit, and delete images, as well as rights to view and edit images other users create.

Upload rights grants rights to create, edit, and delete images, but only grants rights to view images uploaded by other users. Users can view options to edit and delete images uploaded by other users. However, if a user attempts to do this an access denied message appears.

View rights grants rights to view *Image library* in *Site explorer*.

Template Tasks

Any rights selected under **Template tasks** provide view rights to *Pages & templates*. Any user with access to *Pages & templates* can add, edit, and delete folders.

Full rights grants rights to add, edit, and delete templates, as well as rights to view and edit templates other users create.

Create rights grants rights to create templates and edit templates a user created. To grant rights to templates other users create, assign permissions on the Targeting & Security tab for the template.

View rights grants rights to view *Parts* in Site explorer.

Layout Tasks

Any rights selected under **Layout tasks** provide view rights to *Layouts* and *Style sheets*.

Full rights is required to view, edit or delete layouts and style sheets. In additions this grants create rights for layouts and style sheets, as well as rights to view and edit layouts and style sheets other users create.

Create rights grants rights to create and edit layouts and style sheets. However, users cannot view, edit or delete layouts and style sheets created by other users.

View rights grants rights to view *Layouts* and *Style sheets* in *Site explorer*.

File Tasks

Users with access to *Files* have the ability to add, edit, and delete file folders.

Full rights grants rights to add, approve, edit, and delete files, as well as rights to view and edit files other users create.

Approve rights grants rights to approve files uploaded by other users.

Upload rights grants rights to add, edit, and delete files.

View rights grants rights to view *Files* in *Site explorer*.

Profile Tasks

Full rights grants rights to approve photos and see private data. When you select this, you also assign rights for **Approve photo rights** and **View private data rights**.

Approve photo rights grants rights to view unapproved images and to approve images. To actually do this, users must also have full rights to image tasks. If they do not, unapproved images do not appear.

View private data rights grants rights to view directory results and profile displays without the private field filter. Any offline information on the constituent record appears online, even if it is marked private.

Email Tasks

Send rights grants rights to send email messages, eCampaign messages, and newsletter issues. You can send test email messages, eCampaign messages, and newsletter issues without send rights.

List Tasks

Any rights selected under **List tasks** provide view rights to *Lists* in *Email*.

Full rights grants rights to create, edit, and delete lists, as well as rights to view and edit lists other users create.

Create rights grants rights to add, edit, and delete lists. It also grants view-only rights to lists other users create.

View rights grants rights to view *Lists* in *Email*. This does not include rights to view statistics, recipients, or usage of existing lists

Email Template Tasks

Any rights selected under **Email template tasks** provide view rights to *Templates*, *Newsletters*, and *Acknowledgements* in *Email*.

Full rights grants rights to add, edit, and delete all email templates, as well as rights to view and edit email templates other users create. **Full rights** also grants rights to modify the acknowledgement default and to view acknowledgement reports in *Acknowledgements*.

Create rights grants rights to create and copy email templates. It also grants view-only rights to templates other users create. In addition, this grants rights to create newsletters, but does not provide the ability to create or send new issues of newsletters.

View rights grants rights to view the list of templates, newsletters and acknowledgements. This does not grant rights to add, edit, and delete email templates or view reports on templates, newsletters, and acknowledgements. However, the icon for reports still appears.

Email Messages, Invalid Accounts, and Notification Tasks

Full rights grants rights to add, edit, and delete email messages and notifications, as well as rights to view and edit messages and notifications other users create. It also grants rights to send email messages, eCampaign messages, and newsletter issues. For invalid accounts, this grants rights to edit, export, and mark accounts as valid.

Create rights grants rights to create email messages and to view reports for sent messages created by that user. This also provides edit and delete rights for messages by the user. For invalid accounts, this grants rights to view and export accounts. For notifications, this grants create, edit, and delete rights for the user for notifications they create. Use this task right to grant rights to notifications for the Fundraiser part.

View rights provide view-only access to messages, invalid accounts, and notifications. This does not grant rights to view email message reports. For invalid accounts, this also grants rights to export accounts.

Scheduled Email Tasks

Any rights selected under **Scheduled email tasks** provide view rights to *Scheduled emails*.

Full rights grants rights to add, edit, and delete all scheduled emails, as well as rights to view and edit scheduled emails other users create.

Create rights grants rights to create schedules and edit and delete schedules a user created. It grants view-only rights to schedules other users create.

View rights grants rights to view the list of scheduled emails. This does not grant rights to add, edit, and delete scheduled emails.

Campaign Tasks

Any rights selected under **Campaign tasks** provide view rights to *Campaigns* in *Email*. Any user with access to *Campaigns* can also add, edit, and delete folders.

Full rights grants rights to create, edit and delete all email campaigns, as well as view, edit, and delete rights for campaigns other users create. Assign **Full rights** to allow users, other than Supervisors, to add and edit appeals for email campaigns.

Create rights grants rights to create email campaigns. It also grants view-only rights to campaigns other users create. After you create a campaign, users cannot add appeals. This does not provide edit and delete rights for campaigns. To provide these rights, assign **Edit** and **Delete** rights on the Targeting & Security tab for the campaign.

View rights grants rights to view *Campaigns* in *Email*. This does not grant rights to access appeals associated with the campaigns.

eCard Tasks

Any rights selected under **eCard tasks** provide view rights to *eCard templates* in *Email*. Users with access to *eCard templates* can also add, edit, and delete folders.

Full rights grants rights to create, edit, and delete eCard templates, as well as view, edit, and delete rights for eCard templates other users create.

Create rights only grants rights to create eCard templates. This does not grant rights to delete or edit eCards.

View rights grants rights to view *eCard templates* in *Email*.

Form Tasks

Full rights grants rights to create and manage online forms, as well as rights to view and edit forms that other users create. Also grants rights to the Data tab to manage the data that website users submit.

Create, view, and edit rights grants rights to add, edit, and view online forms.

View and edit rights for Forms grants rights to edit and view online forms. It also grants view-only rights to forms that other users create.

View rights for Data tab only grants rights to the Data tab to manage the data that website users submit, but does not include rights to access the forms themselves.

Merchant Accounts Tasks

Use merchant account rights applies site security for the **Merchant account** field on parts and forms. When you select this and a user clicks the drop down for the field, he only views the merchant accounts for the sites he has rights to.

Security Assignments

In *Security assignments*, you associate roles and task groups to apply security to a site. This informs the program *who* is granted *what* rights and *where* the security applies. For example, you can associate an Events Team role with an Events Team task group for the Charleston site.

When you only host one website, you associate roles and task groups to apply security, but all security assignments apply to the default site.

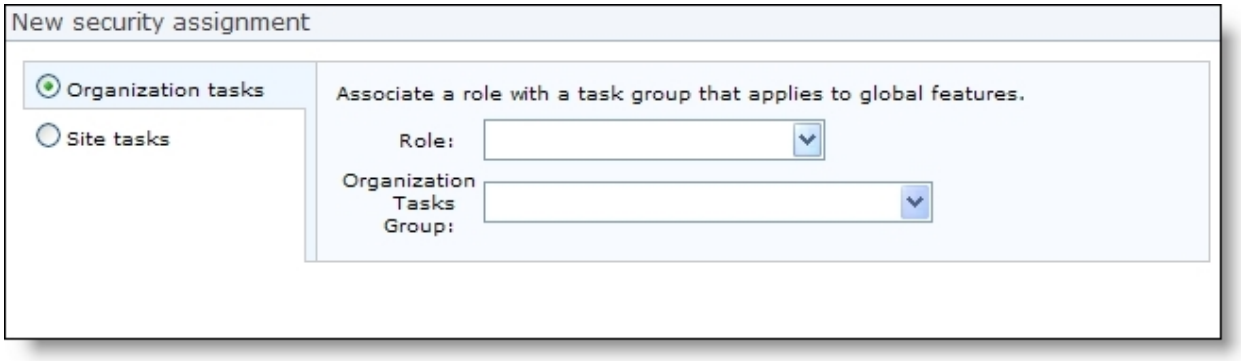
When you host multiple websites, you associate roles and task groups and apply the assignments to sites. You can apply security assignments to default, parent, or child sites. When you apply an assignment to a parent site, you can select whether its child sites inherit the security.

Note: Only users with Supervisor rights can view and manage *Security assignments*.

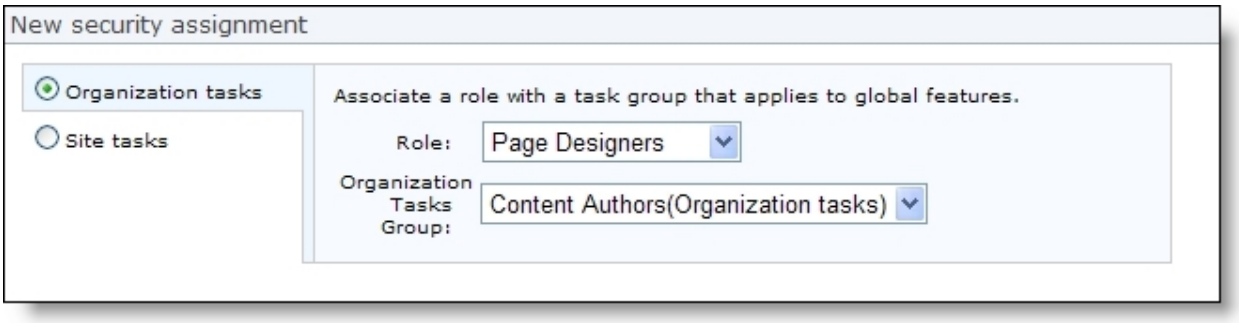
Show Me: Watch an overview of security in Blackbaud NetCommunity.

Create a security assignment

1. In *Users & security*, click **Security assignments**. *Security assignments* appears.
2. Click **New security assignment**. The New security assignment screen appears.



3. To create a security assignment that applies globally to your entire website, select **Organization tasks assignment**.
   a. In the **Role** field, select the role to associate with the organization task group.
   b. In the **Organization Tasks Group** field, select the task group with the global task rights to apply to the role.

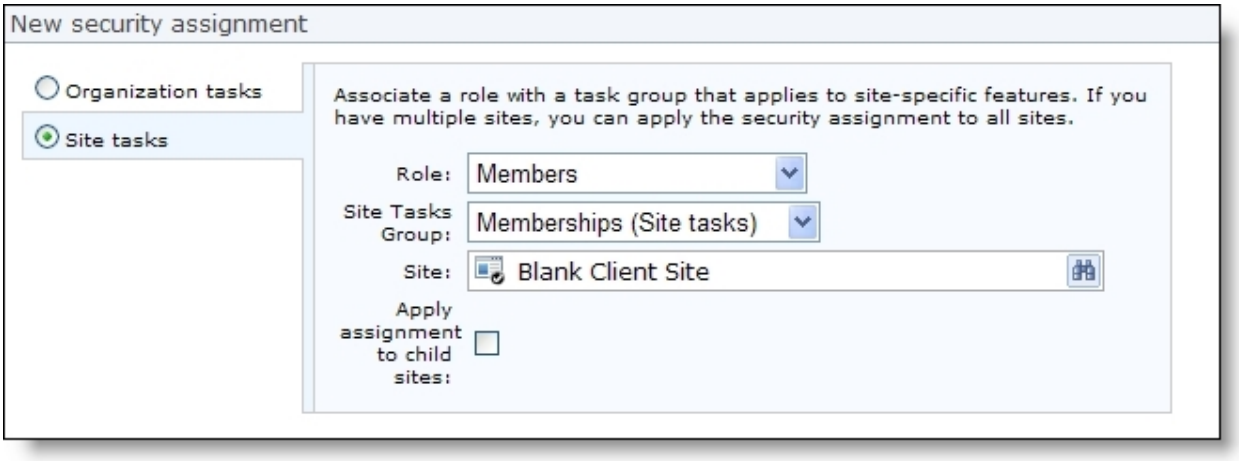


Tip: For overview information about security, see Security Overview on page 5. For information about global task rights, see Organization Task Rights Details on page 24.

c. Click **Save** and you return to *Security assignments*. The new security assignment appears in the grid.

Note: For information about sites, see the *Administration Guide*.

4. To create a security assignment that applies to an individual site, select **Site tasks assignment**.
   a. In the **Role** field, select the role to associate with the site task group.
   b. In the **Site Tasks Group** field, select the task group with the individual site task rights to apply to the role.
   c. In the **Site** field, select the site where the security assignment applies. You can select a default, parent, or child site.

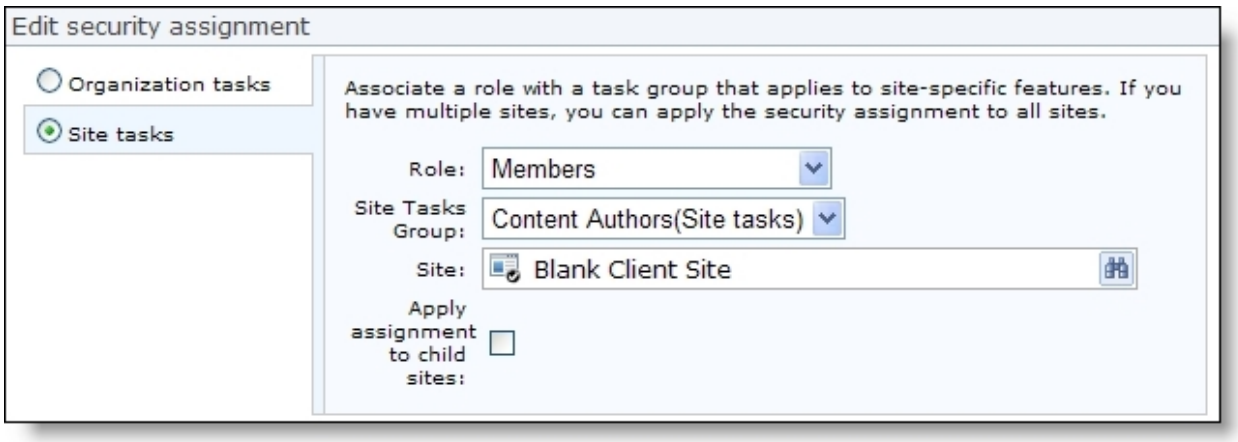


Tip: For overview information about security, see Security Overview on page 5. For information about site task rights, see Site Task Rights Details on page 24.

   d. If the security assignment is for a parent site and its child sites should inherit the assignments, select **Apply assignment to child sites**.
   e. Click Save. You return to *Security assignments*. The security assignment appears in the grid.

Edit a security assignment

1. In *Users & security*, click **Security assignments**. *Security assignments* appears.
2. Select the security assignment and click **Click here to edit this security assignment**. The Edit security assignment screen appears.



3. Make changes as necessary. The items on this screen are the same as the New security assignment screen. For information, see Create a security assignment on page 29.

   To edit a role for a security assignment, see Edit a role on page 17. To edit a task group for a security assignment, see Edit a task group on page 21.
4. Click **Save**. You return to *Security assignments*.

User Imports

With *User imports*, you can import constituent information exported from The Raiser's Edge to create website users. In *User imports*, you select the file to import and whether to schedule the import for a later date. We recommend only Administrators or users with Supervisor rights access *User imports*.

Note: The import file must be a comma-separated values (*.csv) file, and its first row must contain the field names. To import the user information correctly, each record in the import file must contain the user's first and last name, email address, and System Record ID.

Warning: The ID required for the import file is the System Record ID, not the Constituent ID or Import ID.

Warning: Before you import users into your database, we strongly recommend you back up your database and verify the import file contains correct information. After the program processes the user import, you cannot undo the import or globally delete the imported user information from your database.

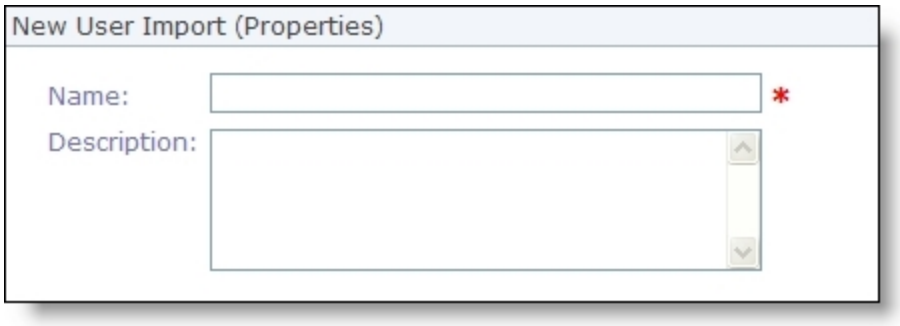
On the Settings tab in *Sites & settings*, you can set how often the program runs the process to import

user information. For information about how to configure the user import process, see the *Administration Guide*.

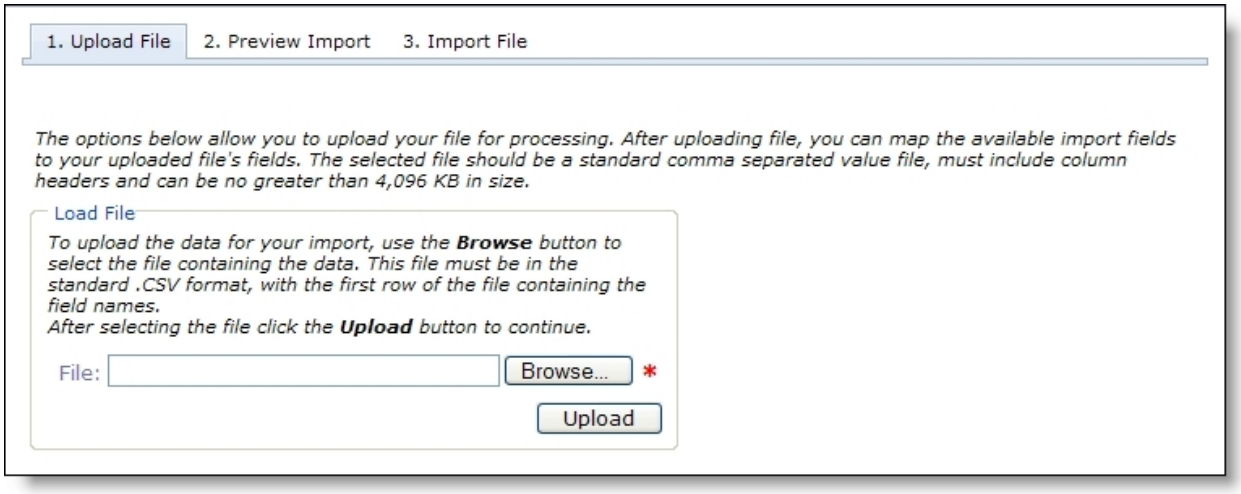
If you selected the **Require complex passwords** checkbox in *Sites & settings*, the passwords assigned to records you import must also meet the complexity requirements.

Create a user import

1. From *Users & security*, click **User imports**. *User imports* appears.
2. Click **New user import**. The Properties screen appears.



3. In the **Name** field, enter a name for the user import so users can quickly identify the information in *User imports*.
4. In the **Description** field, enter any additional information to identify the user import, such as an explanation of the users imported.
5. Click **Next**. The User Import Wizard page appears.
6. Select the Upload File tab.



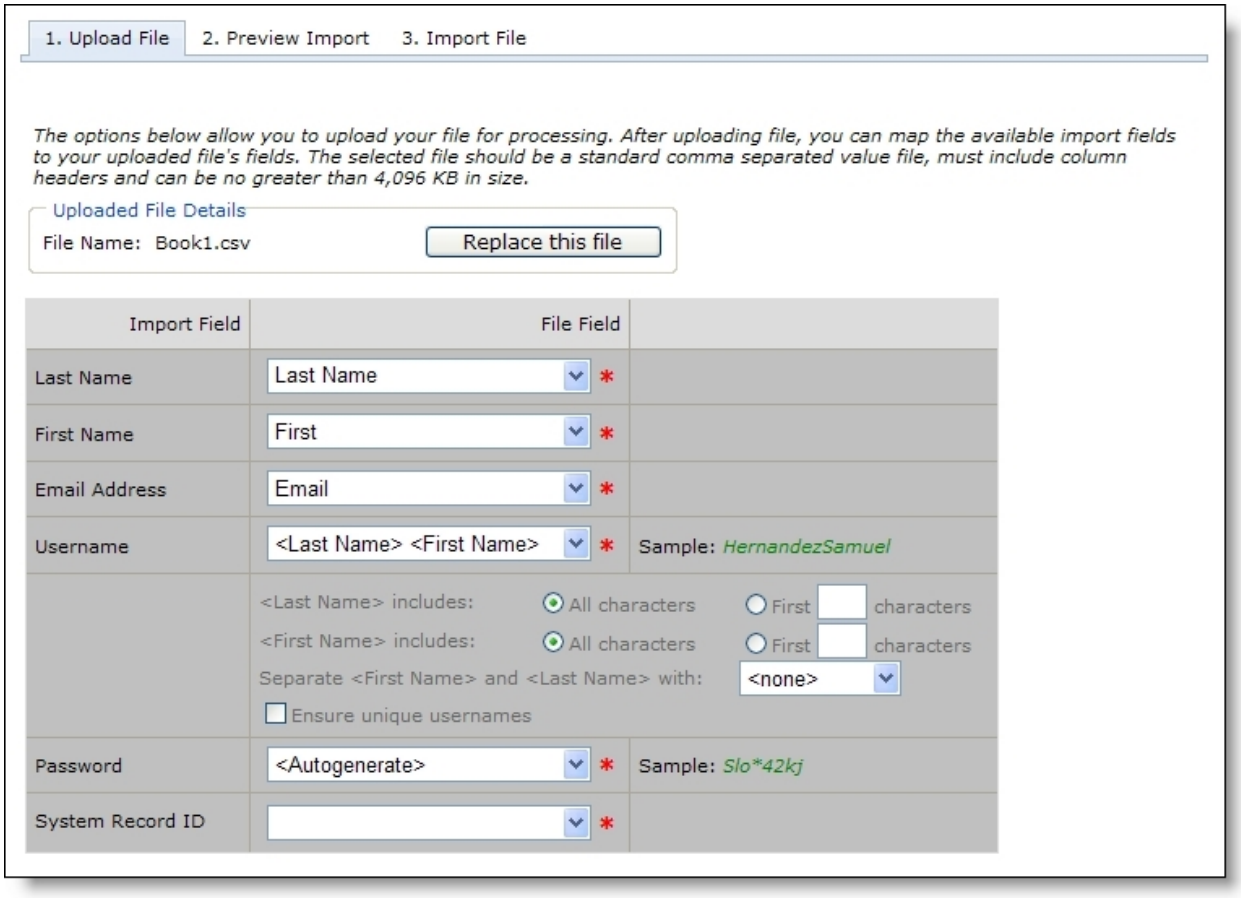
7. In the **Load File** frame, in the **File** field, enter the path to the *.csv file to import. To map to the location of the import file, click **Browse** and use the Choose File screen.

Note: At a minimum, the imported *.csv file must contain the constituent's first and last name, email address, and system record ID, and its first row must contain the field names. You can export a *.csv file of this constituent information from The Raiser's Edge. For information about how to export data

from The Raiser's Edge, see *The Raiser's Edge Query and Export Guide* or the Export section of the help file in The Raiser's Edge.

Warning: The ID required for the import file is the System Record ID, not the Constituent ID or Import ID.

8. Click **Upload**. The **Uploaded File Details** frame and field mapping grid appear.



Note: Under **Uploaded File Details**, the **File Name** field displays the selected import file. To import a different file, click **Replace this file**. The **Load File** frame appears.

9. In the field mapping grid, the **Import Field** column displays the fields required to import users into the program. For each import field, in the **File Field** column, select the field of the import file to import information from.

Note: When you upload an import file, the program automatically attempts to match field names in the import file with the fields required to import to users into the program. You can adjust the automatically mapped fields as necessary.

   a. In the **Last name** and **First Name** fields, select the field names in the import file that contains the last and first name of each user.

b. In the **Email Address** field, select the field name in the import file that contains the email address for each user.

c. In the **Username** field, select the field name in the import file that contains the user name for each user or, to automatically generate user names, select the format to use for the user names, such as "<Last name> <First Name>."

   If you select a user name format, specify how the user name appears. In the **<Last name> includes** and **<First Name> includes** fields, select whether to use all characters in the name or only the first specific number of characters. In the **Separate <First Name> and <Last name> with** field, select the character to separate the first and last names in the user name. You can select to display a space, a period, a dash, or an underscore, or you can select to display no separation. Next to the **Username** field, the **Sample** field displays how user names appear with the selected format.

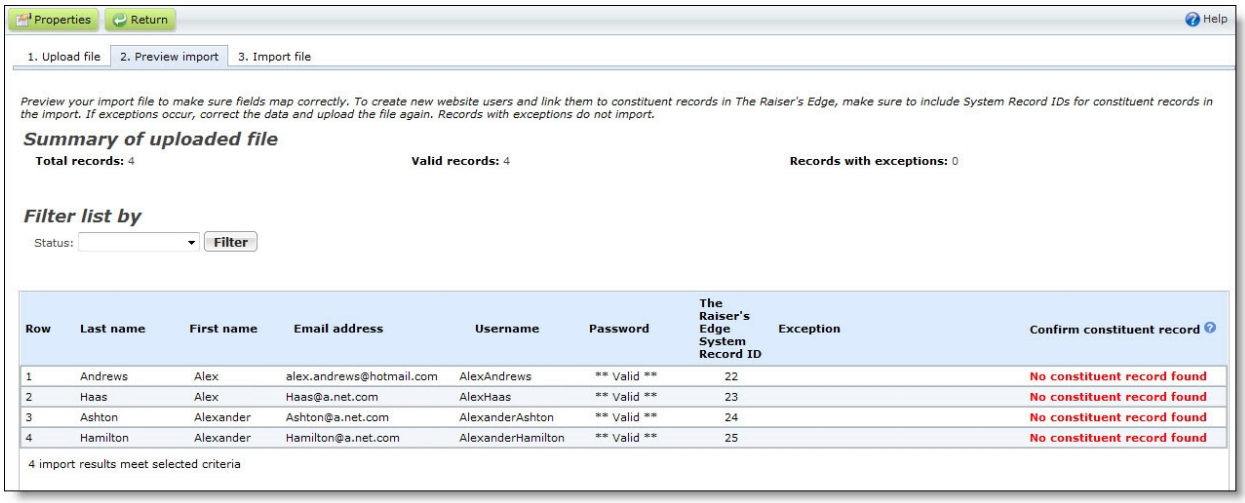
d. To prevent duplicate user names, select **Ensure unique usernames**. When you select this checkbox, the program adds a number to the end of any user name that already exists in the program or is included elsewhere in the import file.

e. In the **Password** field, select the field name in the import file that contains the password for each user or, to automatically generate passwords, select "<Autogenerate>."

f. In the **The Raiser's Edge System Record ID** field, select the field name in the import file that contains the system record ID for each user.

Tip: If an invalid ID is processed in *User imports*, the user appears as a new user when you download sign-up requests in The Raiser's Edge. For more information about sign-up requests, see the *Blackbaud NetCommunity & The Raiser's Edge Integration Guide*.

10. Select the Preview Import tab or click **Next**.



Note: If you exit the User Import Wizard page after you upload an import file but before you add the import to the queue, you can return to the user import from *User imports*. The **Status** column for the import is blank. For information about how to view a user import, see View the tabs of a user import on page 36.

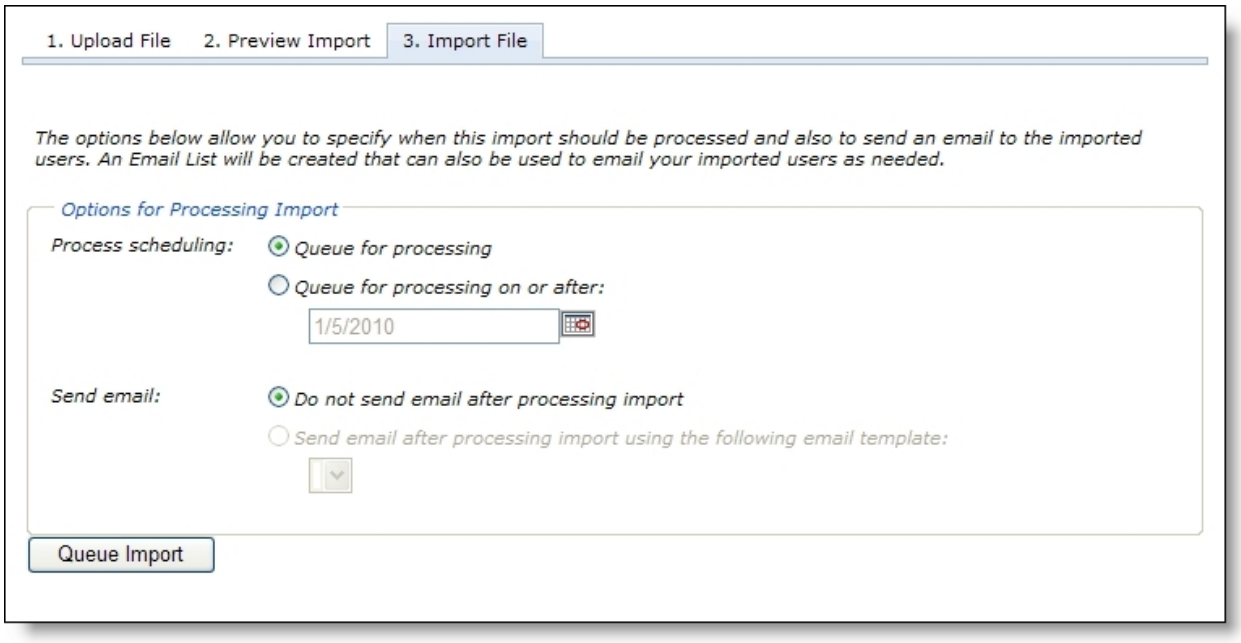
11. Under **Summary of Uploaded File**, view the total number of records included in the import file and how many of those records are valid and how many contain exceptions.
12. Under **Filter List By**, enter the exception status of the records to view. You can select to view all valid records, all exceptions, or all with a specific exception status. To view all records in the import file, regardless of exception status, leave the **Status** field blank. For information about the exception status, see User Import Exception Reasons on page 39.
13. Click **Go**. In the grid, records in the import file that match the entered filter criteria appear. Make sure the fields are mapped correctly.

    In the **Exception reason** column, view the cause for any exceptions in your import file, such as "This record is already linked to a Blackbaud NetCommunity user." For more information about user import exceptions and their causes, see User Import Exception Reasons on page 39.

    If the constituent record does not match the constituent in the **Last name** and **First name** columns or if **No constituent record found** appears, return to the Upload file tab and make sure you select System Record ID in **The Raiser's Edge System Record ID** field, not the constituent ID or the import ID.

Note: The grid can display up to 50 records at a time. If you import more than 50 records, click **Prev** or **Next** to page through the results, or select the page number to view.

14. Select the Import File tab or click **Next**.



15. Under **Options for Processing Import**, in the **Process scheduling** field, select when to process the user import.
    - To add the user import to the queue immediately when you click **Queue Import**, select **Queue for processing**.

- To add the user import to the queue at a later date when you click **Queue Import**, select **Queue for processing on or after** and, in the field, click the calendar and select the date to add the process to the queue.

16. For **Send email**, select whether to automatically send an email to the new users added during the import.
    - To not automatically send an email to the new users, select **Do not send email after processing import**.
    - To automatically send an email to the new users, select **Send email after processing import using the following email template**. TYou can select any template with a data source of Registered Users. For more information about email templates, see the *Email Guide*.

Note: Regardless of your selection for **Send email**, when the program imports the user information, it automatically creates a email list that contains the new users added during the import. The email list is associated with the site you are logged in to when you run the import process. You can use it to send future email to these users. For information about email lists, see the *Email Guide*.

17. Click **Queue Import**. You return to *User imports*.
    - If, under **Options for Processing Import**, you select **Queue for processing**, the program imports the user information during the next scheduled user import process, as specified on the Settings tab in *Sites & settings*.
    - If, under **Options for Processing Import**, you select **Queue for processing on or after**, the program imports the user information on or after the selected date, in accordance with the user import process settings selected on the Settings tab in *Sites & settings*.

Note: For information about the user import process settings on the Settings tab in *Sites & settings*, see the *Administration Guide*.

View the tabs of a user import

1. From *Users & security*, click **User imports**. *User imports* appears.
2. Under **Filter List By**, enter the criteria of the user import to view. You can enter the import's name or status. For information about the import status, see User Import Status on page 38.
3. Click **Go**. In the grid, user imports that match the entered filter criteria appear.

Note: The grid can display up to 50 results at a time. If you have more than 50 results, click **Prev** or **Next** to page through the results, or select the page number to view.

4. Next to the user import to view, click **Click here to edit this import**. The User Import Wizard page appears.
5. If the **Status** column for the user import is blank or "Queued," the User Import Wizard page includes the Upload File, Preview Import, and Import File tabs. For information about how to complete these tabs, see Create a user import on page 32.

Note: You cannot change a user import with a status of "Queued." To adjust a user import with a status of "Queued," such as to correct any exceptions, you must first cancel the user import. For information about how to cancel a user import, see Cancel a queued user import on page 37.

If the **Status** column for the user import is "Imported" or "Exceptions," the User Import Wizard page includes the Status and Results tabs.

- On the Status tab, view details about the current status of the import, such as the date, time, and duration of the import; how many records the import contained and how many records imported successfully and how many did not; and whether the program sent email to the imported users.

If the user import contains exceptions, click **Download Exceptions** to create a *.csv file of the exceptions. The *.csv file includes a column to explain the reason for each exception. For more information about user import exceptions and their causes, see User Import Exception Reasons on page 39.

- On the Results tab, view the user information that imported correctly and any exceptions. If information does not import correctly, the Results tab displays the reason for the exception.

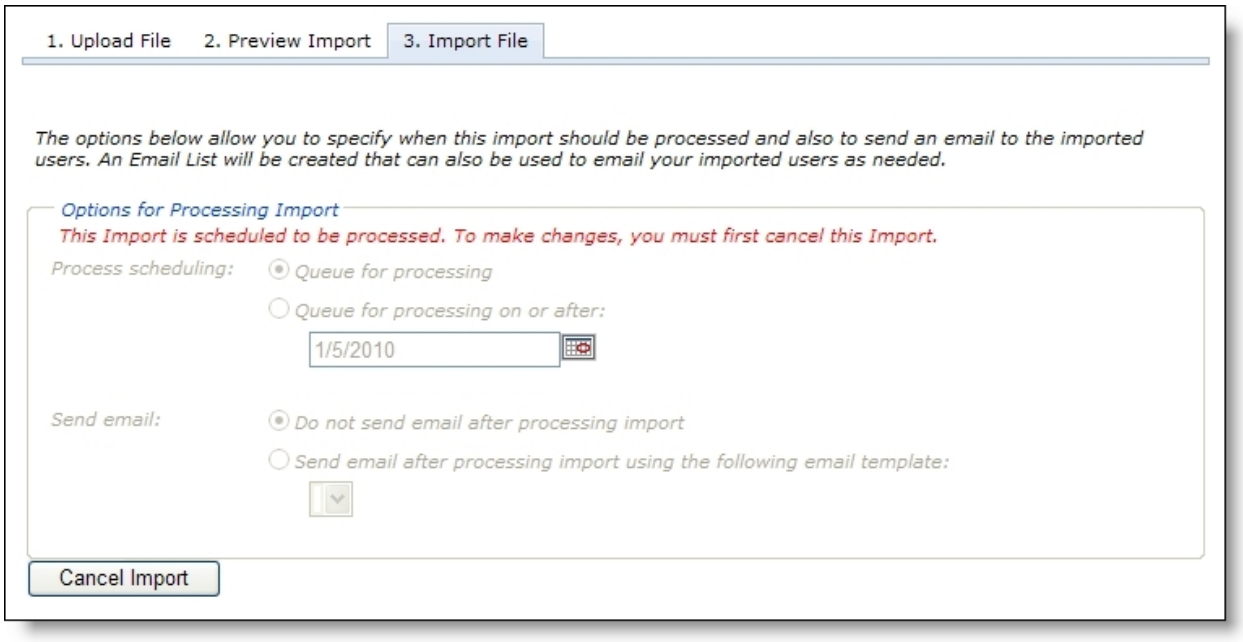
Note: To view the properties of the user import, click **Properties** on the action bar. The user import Properties screen appears. You can adjust the name or description of the user import as required.

6. Click **Return**. You return to *User imports*.

Cancel a queued user import

You cannot change a user import with a status of "Queued." To adjust a user import with a status of "Queued," such as to correct any exceptions, you must first cancel the user import.

1. From *Users & security*, click **User imports**. *User imports* appears.
2. Under **Filter List By**, enter the name of the user import to cancel, or in the **Status** field, select "Queued."
3. Click **Go**. In the grid, user imports that match the entered filter criteria appear.
4. Next to the user import to cancel, click **Click here to edit this User Import**. The User Import Wizard page appears.
5. Select the Import File tab.



6. Click **Cancel Import**. The user import is removed from the queue and the **Queue Import** button appears.
7. Adjust the user import as required. For information about how to create a user import, see Create a user import on page 32.
8. Click **Return**. You return to *User imports*.

Delete a user import

1. From *Users & security*, click **User imports**. *User imports* appears.
2. Under **Filter List By**, enter the criteria of the user import to delete. You can enter the import's name or status. For information about the import status, see User Import Status on page 38.
3. Click **Go**. In the grid, user imports that match the entered filter criteria appear.

Note: The grid can display up to 50 results at a time. If you have more than 50 results, click **Prev** or **Next** to page through the results, or select the page number to view.

4. Next to the user import to view, click **Click here to delete this User Import**. A message appears to confirm the deletion of the user import.
5. Click **OK**. You return to *User imports*. The grid no longer displays the user import.

User Import Status

After you create a user import, you can view its current status in *User imports*. The **Status** column displays the status of each user import. Under **Filter List By**, you can also select the status of the user imports to view in *User imports*.

- "Imported" – The program imported the user information and successfully added the new users.

- "Queued" – The user import is in the queue to be imported. When you create a user import, you specify whether to import the users during the next scheduled import process or at a future date.
- "Exceptions" – The program attempted to import the user information but failed, such as if all records contained errors, or the import file contained no valid records.
- No status – If the **Status** column is blank for a user import, the import is created but not yet in the queue.

User Import Exception Reasons

After you create a user import, you can view its exceptions, or records that do not import correctly, in *User imports*. You can also view the reason for each exception.

- Before you add the import to the queue, you can view its exceptions on the Preview Import tab of the User Import Wizard page. Under **Summary of Uploaded File**, the **Records with exceptions** field displays how many exceptions the import file contains. In the grid, the **Exception reason** column explains why each exception will not import.
- After you add the import to the queue, you can view its exceptions on the Status tab of the User Import Wizard page. In the **Status** frame, the **Exceptions** field displays how many exceptions the import file contains. To view a *.csv file of the exceptions, click **Download Exceptions**. The *.csv file includes the user information that did not import and a column to explain the reason for each exception.

Exceptions can occur for multiple reasons.

- "Required field missing" – The import file does not contain one or more required fields.
- "Invalid field value" – The email address or System Record ID in the import file is invalid or in an invalid format.
- "This record is already linked to a Blackbaud NetCommunity user" – The constituent imported from The Raiser's Edge is already linked to a user in Blackbaud NetCommunity.
- "This login is in use" – The user name specified or generated in the user import already exists in the program.

Before you add the user import to the queue, you can upload a corrected import file or adjust the field matching to resolve the exceptions. If you import a file that includes exceptions, the program imports only the valid records and ignores the exceptions.