Administration Guide

11/03/2021Blackbaud NetCommunity 7.1 Administration US

Contents

Administration

In *Administration*, you manage settings for your website. For example, in *Merchant accounts*, you add merchant account information to allow parts to process payments. And in *Field options*, you set privacy settings for profile information. We recommend that only website administrators or those with Supervisor rights access *Administration*.

Sites & Settings

In *Sites & settings*, you select whether to host multiple websites. You also select the global organization tasks and settings that apply to all your websites. And you select site-specific tasks and settings for each website that you host.

> ***Warning:*** We strongly recommend that you only assign full Supervisor rights for *Sites & settings* to a select group of users. General users should not access this section of the program because changes can affect multiple web pages and sites. Only users knowledgeable in all areas of website creation and publishing should perform tasks in *Sites & settings*.

Single Site

When you host a single website, all tasks and settings apply to the website. If you add additional sites, the organization tasks and settings still apply to all sites, but you select site-specific tasks and settings for each new site.

Organization Tasks and Settings — Single Site

In *Workflows, Code tables, Merchant accounts,* and *Field options*, you apply global organization tasks to your entire website. To access these options, select the top-level item in the *Sites & settings* treeview. This top-level item most likely displays your organization's name. The Tasks tab appears.
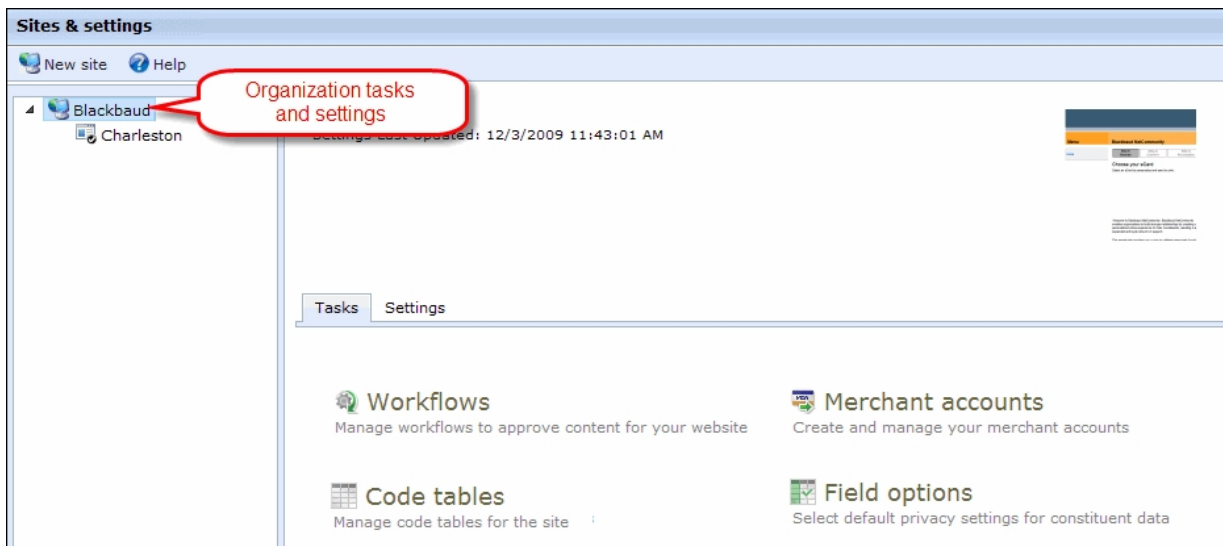
For information about these areas, see Workflows on page 78, Code Tables on page 92, Merchant Accounts on page 83, and Field Options on page 90.

To access organization settings such as web services, caching, and service scheduling, select the Settings tab.
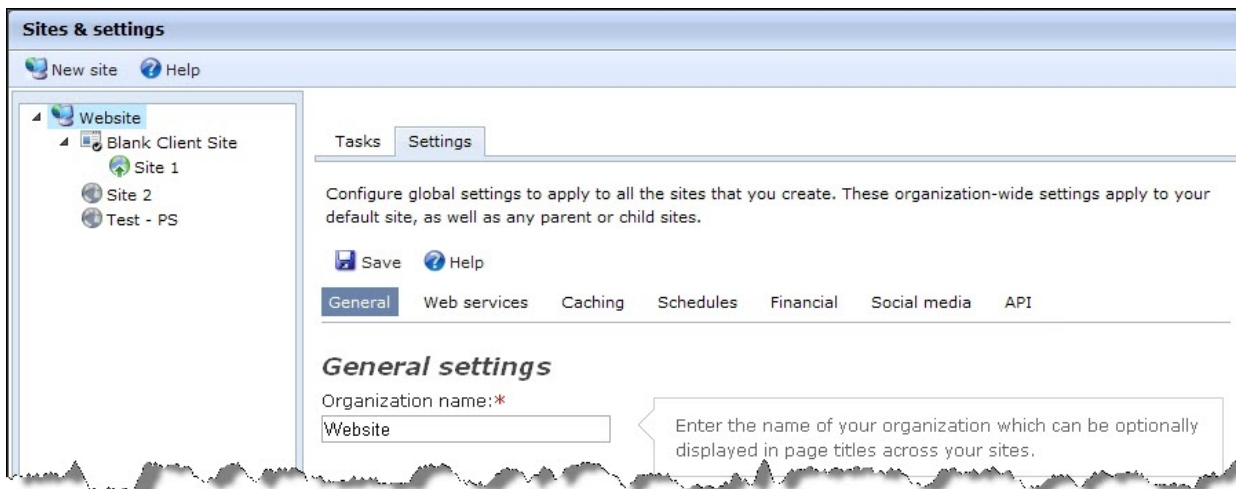
For information about organization settings, see Organization Settings on page 32.

Default Site — Single Site

To select site-specific settings when you host a single website, select the default site in the *Sites & settings* treeview. On the Tasks tab, you design your site from sections such as *Pages & templates*, *Parts*, and *Friendly URLs*.

Note: After you create an item on the Tasks tab, you can access it from the corresponding section in *Site explorer*. For example, after you create a Donation Form part on the Tasks tab, you can access it by clicking **Site explorer**, **Parts** in the menu bar.

For information about the website design tasks on the Tasks tab, see the *Website Design Guide*.

On the Settings tab, you select site-specific settings such as languages to support, registration and login options, and whether to use reCAPTCHA for payments.

For information about site-specific settings, see Site Settings on page 58.

On the Targeting & security tab, you assign security rights for the site's users and roles. For example, you can grant edit rights to allow a role to edit site settings. On the Site contents tab, you view data about the default website site such as the number of images, pages, and parts.

Multiple Sites

When you host multiple sites, you select global organization tasks and settings that apply to all sites, as well as site-specific tasks and settings for each default, parent, and child site. Your website always includes a default site, and you can create an unlimited number of additional sites. You can create any combination of parent and child sites, and the program does not limit the hierarchy structure. For example, you can create multiple parent and child sites, and child sites can be parent sites to additional child sites.
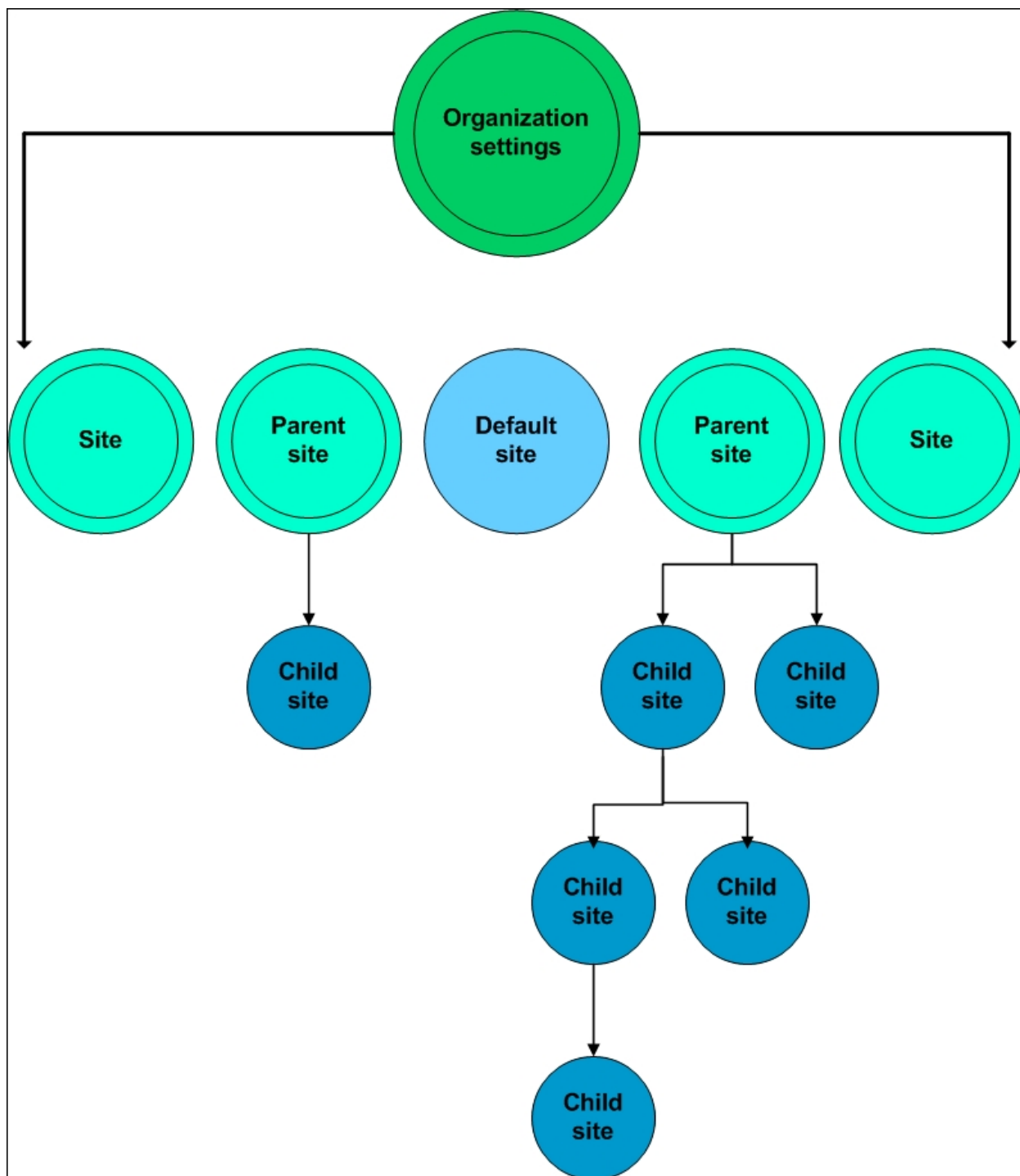
Multiple sites can benefit your organization in several ways. You can create sites for intranets, chapters, affiliates, and large campaigns, and you can customize their content, appearance, and security for targeted audiences. You can also hide sites that should not appear on the Internet and archive old sites.

For more information about organization settings and default, parent, and child sites, review the information in this section.

Organization Tasks and Settings — Multiple Sites

In *Workflows, Code tables, Merchant accounts, and Field options*, you apply global organization tasks to your entire website. To access these options, select the top-level item in the *Sites & settings* treeview. This top-level item most likely displays your organization's name. The Tasks tab appears.
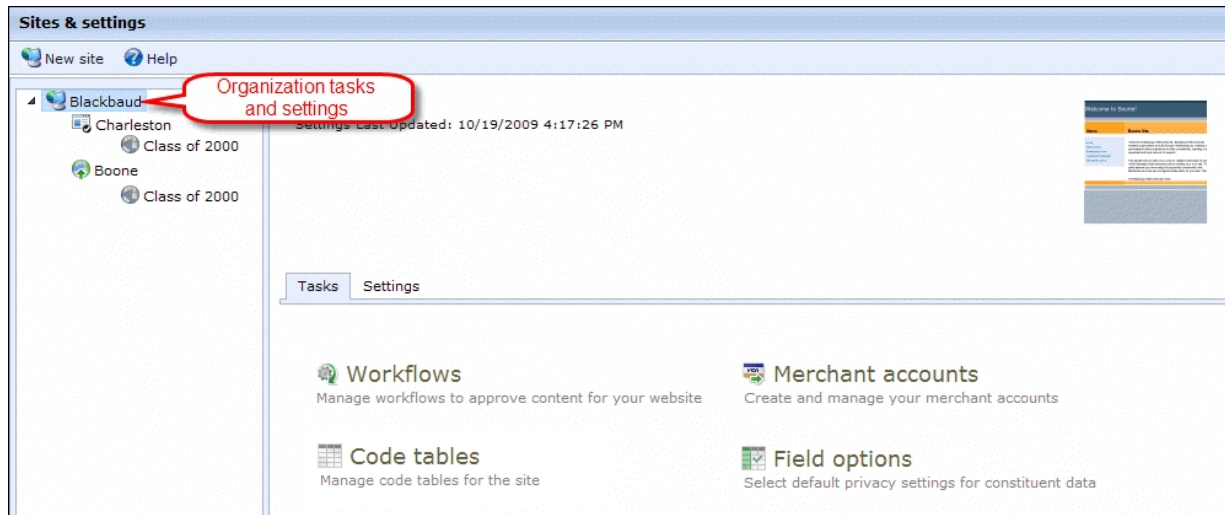
These options are not site-specific. They apply to all default, parent, and child sites. For example, the code tables and merchant accounts that you configure are available on all sites. For information about these areas, see Workflows on page 78, Code Tables on page 92, Merchant Accounts on page 83, and Field Options on page 90.

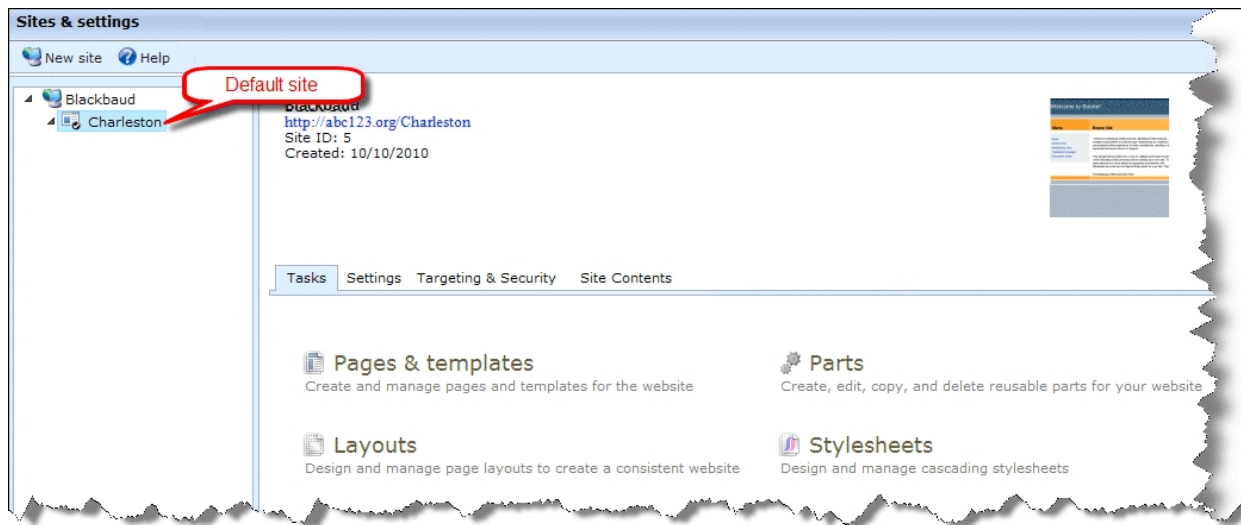> **Note:** Settings in *Email* and *Users & security* also apply globally to all sites. To access these areas, select **Email** and **Users & security** in the menu. For more information, see the *Email Guide* and the *Users & Security Guide*.

To access organization settings, such as web services, caching, and service scheduling, select the Settings tab for the top-level item in the *Sites & settings* treeview.
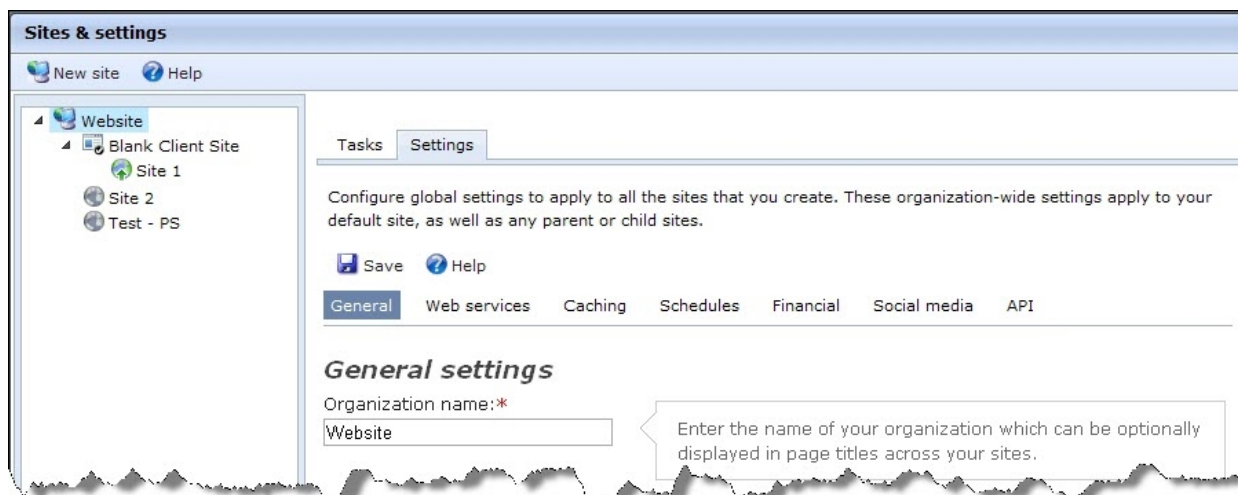
For more information about organization settings, see Organization Settings on page 32.

Default Site — Multiple Sites

When you host multiple websites, the default site is your primary site. You design the default website and select its settings just like other sites. The only difference is that the program redirects users to the default site when they click URLs and it cannot determine where to navigate to. For example, if users click links to archived sites, the home page of your default site appears. The default site receives all unresolvable URLs that the program cannot render.

Note: The default site can be a parent site, child site, or both. This means the default site can be a parent site with child sites and also the child site of a parent site.

To manage your default site, select it in the *Sites & settings* treeview. You can identify it by the unique default site icon. On the Tasks tab, you design your site from sections such as *Pages & templates*, *Parts*, and *Friendly URLs*.

Note: After you create an item on the Tasks tab, you can access it from the corresponding section in *Site explorer*. For example, after you create a Donation Form part on the Tasks tab, you can access it by clicking **Site explorer**, **Parts** in the menu bar.

For information about the website design tasks on the Tasks tab, see the *Website Design Guide*.

On the Settings tab, you select site-specific settings such as languages to support, registration and login options, and whether to use reCAPTCHA for payments.
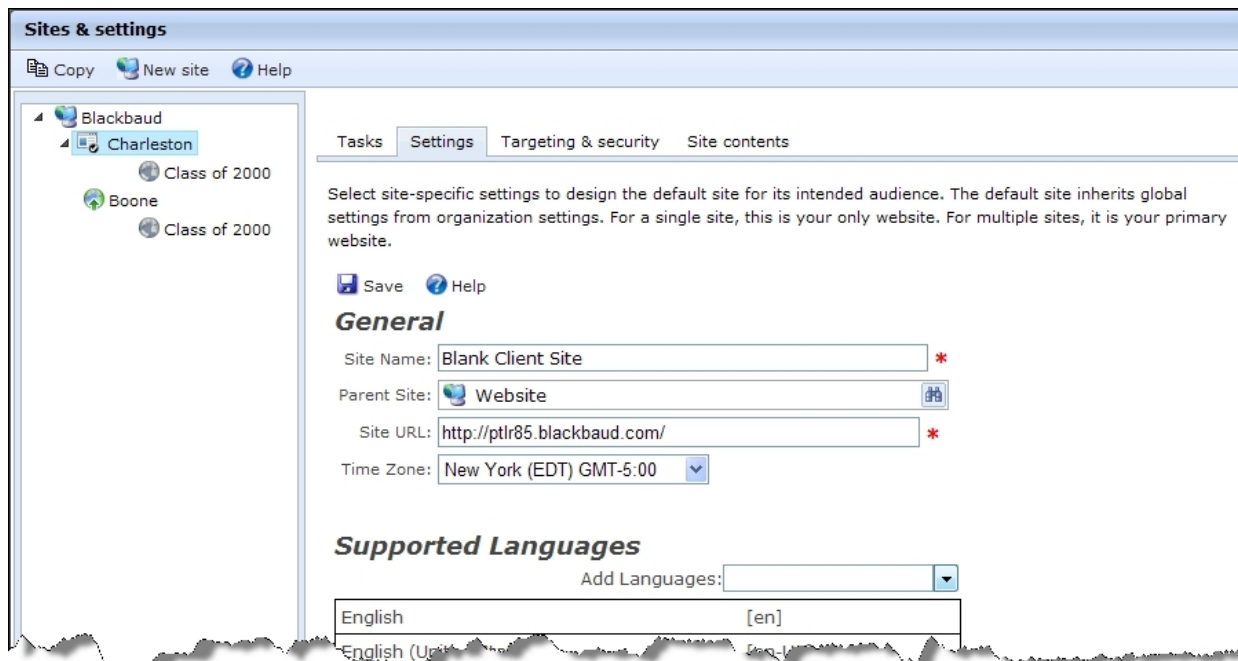
For information about default site settings, see Site Settings on page 58.

On the Targeting & security tab, you assign security rights for the site's users and roles. For example, you can grant edit rights to allow a role to edit site settings. On the Site contents tab, you view data about the default website site such as the number of images, pages, and parts.

Parent Site — Multiple Sites

You manage parent sites the same way as the default site. Select the parent site in the *Sites & settings* treeview. On the Tasks tab, you design your site from sections such as *Pages & templates*, *Parts*, and *Friendly URLs*. On the Settings tab, you select site-specific settings such as languages to support, registration and login options, and whether to use reCAPTCHA for payments.
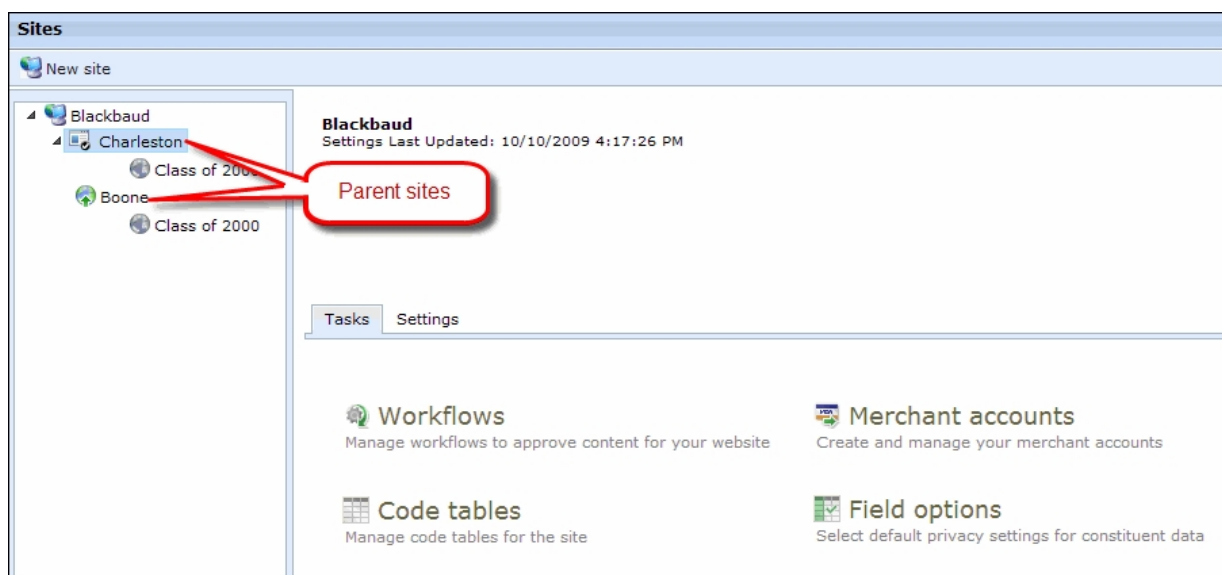
For information about how to create a site, see Manage a Parent or Child Site on page 15.

Child Site - Multiple Sites

A parent site can contain child sites. You manage child sites the same way as default and parent sites. Select the child site in the *Sites & settings* treeview. On the Tasks tab, you design your site from sections such as *Pages & templates*, *Parts*, and *Friendly URLs*. On the Settings tab, you select site-specific settings such as languages to support, registration and login options, and whether to use reCAPTCHA for payments.
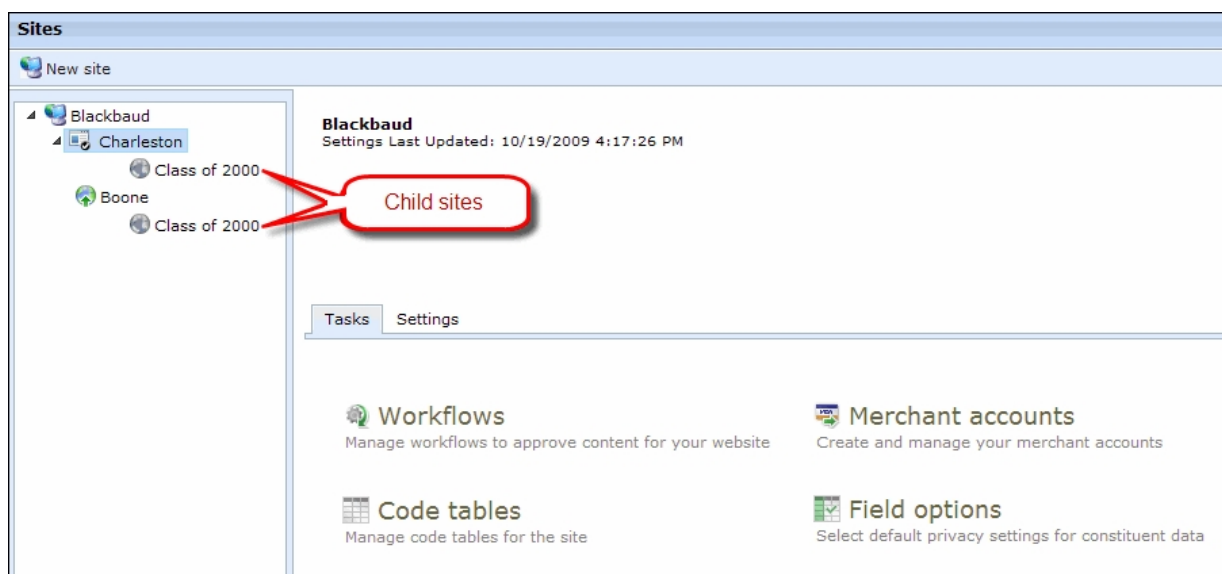
For information about how to create a site, see Manage a Parent or Child Site on page 15.

Note: You can select for child sites to inherit security assignments from parent sites. You can also edit the inherited security settings for a child site. For more information, see the *Users & Security Guide.*

Manage a Parent or Child Site

Review this section to learn about the procedures for parent and child sites.

Warning: We strongly recommend that you only assign full Supervisor rights for *Sites & settings* to a select group of users. General users should not access this section of the program because changes can affect multiple web pages and sites. Only users knowledgeable in all areas of website creation and publishing should perform tasks in *Sites & settings*.

> **Create a parent or child site**

Multiple sites can benefit your organization in several ways. You can create sites for intranets, chapters, affiliates, and large campaigns, and you can customize the content, appearance, and security for targeted audiences. You can create an unlimited number of sites at any level in a hierarchy.

1. From *Administration*, click **Sites & settings**. *Sites & settings* appears.

2. Select the default site or parent site in the treeview and click **New site**. The Create New Site page appears.

Create New Site

| 💾 Save | ❓ Help | 🔄 Return |

Create new site

You can create an unlimited number of sites. You can create any combination of parent and child sites at any level in the hierarchy.

New site name:*

Enter a name to appear in the **Sites** treeview.

Parent site:

Blank Client Site

Select the parent site. By default, the program uses the site you selected in the **Sites** treeview.

New site URL:*

Enter a URL and click **Validate**. The program confirms that the domain maps to the installation.

Validate

3. In the **New site name** field, enter a name to identify the site in the program. The name only appears in the *Sites & settings* treeview. Website users do not view it.

4. In the **Parent site** field, select the parent site.

5. In the **New site URL** field, enter your site URL.

6. To verify the URL, click **Validate**. The program confirms this domain maps to the location of your program installation. When it does not, a message appears to inform you the URL is not valid. If this occurs, check your Domain Name System (DNS) configuration.

    You can enter URLs such as http://www.example.org or http://www.example.org/cambridge. To enter a subdomain URL such as http://www.cambridge.example.org, you must configure the subdomain outside of the program. For more information, contact your System Administrator.

7. Click **Save**. You return to *Sites & settings* and the site appears in the *Sites & settings* treeview.

> Edit a site

You edit the site name, parent, and URL for a site in site settings. For more information, see General site settings on page 58.

1. In the *Sites & settings* treeview, select the site to edit. The Tasks tab appears.
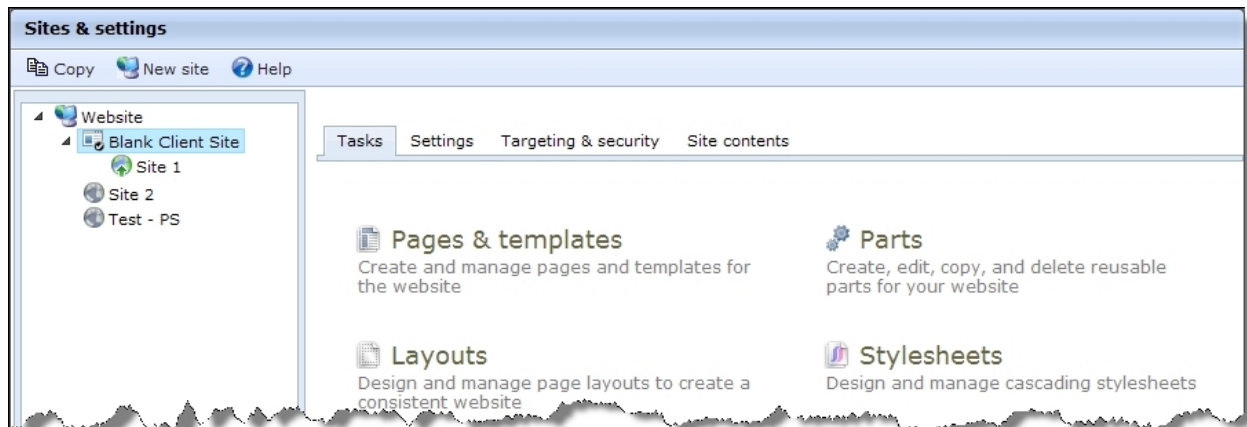
2. On the Tasks tab, edit tasks for website design as necessary. You can edit pages, templates, layouts, forms, friendly URLs, parts, style sheets, images, and approvals. For more information, see the *Website Design Guide*.

3. On the Settings tab, edit site-specific settings such as languages to support, registration and login options, and whether to use reCAPTCHA for payments.

Note: To change a site URL, enter a new one in the **Site URL** field. If a message appears that informs you the URL is not valid, check your Domain Name System (DNS) configuration. For more information about the **Site URL** field, see.

4. On the Targeting & security tab, assign security rights for the site's users and roles. For example, you can grant edit rights to allow a role to edit site settings.

For more information about the Targeting & security tab, see the *Parts Guide*.

5. On the Site contents tab, view data about the site such as the number of images, pages, and parts.
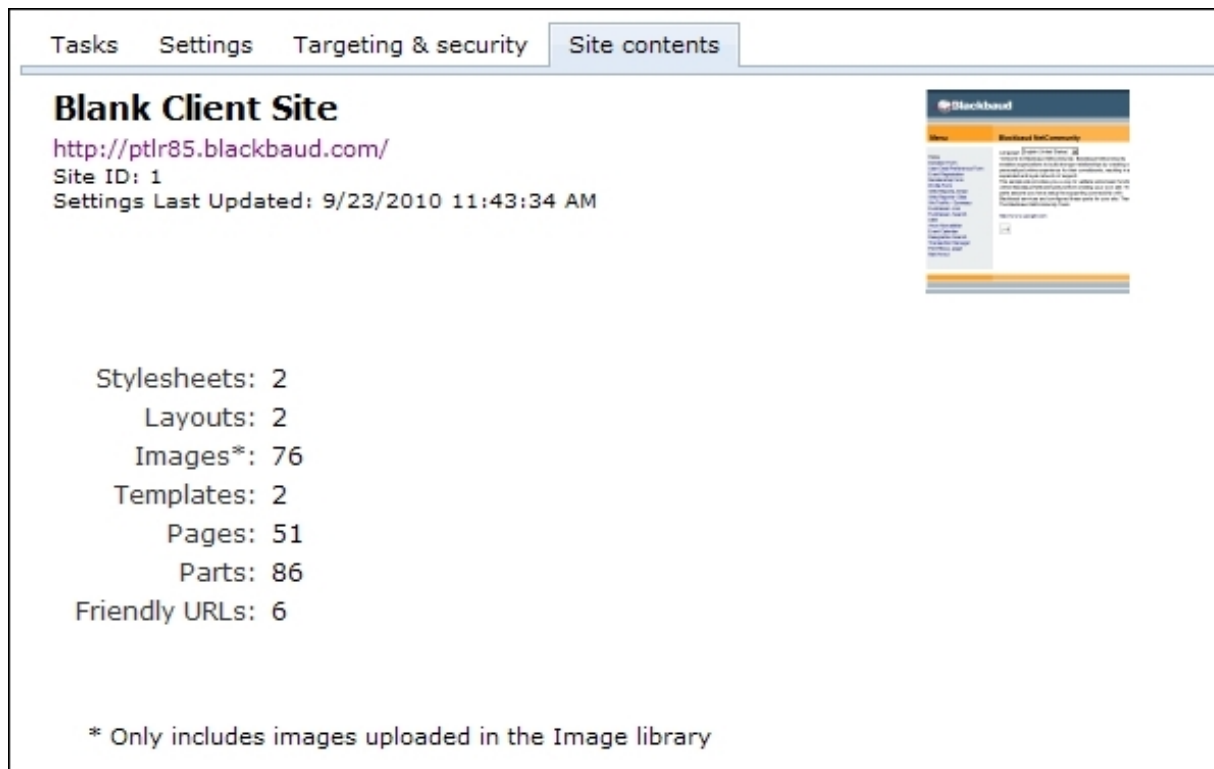
6. To edit another site in *Sites & settings*, you can select it in the *Sites & settings* treeview.

Select a default site

The program requires a default site. When you host one site, the default site is your only website. When you host multiple websites, you select a default site to serve as your main website. The default site receives all unresolvable URLs that the program cannot render. For example, when users click links to archived sites, the home page of your default site appears.

1. In the *Sites & settings* treeview, select a site.

2. Click **Make default**.

Note: Only users with Supervisor rights can designate the default site.

The default site can be a parent site, child site, or both.
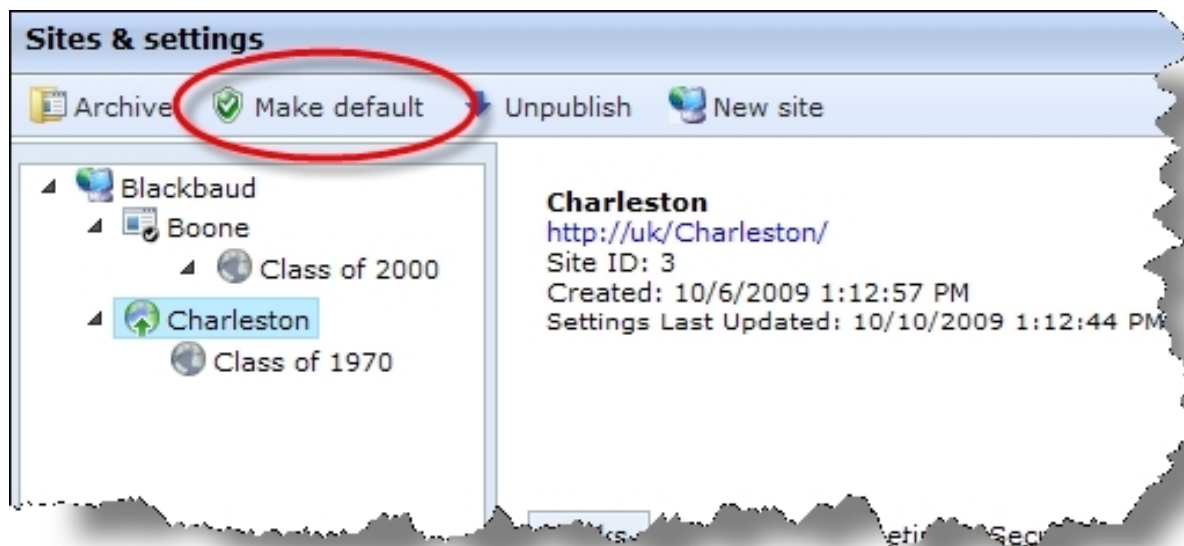
Tip: The **Make default** button does not appear if the site is not published. You must publish the site to select it as the default site. For more information, see Publish a site on page 19.

The default site icon identifies the default site in the *Sites & settings* treeview and no longer appears for the previous default site.

> **Publish a site**

Before you publish a site, it must contain an authorization failed page, home page, and privacy page. For more information, see Page settings on page 61.

1. In the *Sites & settings* treeview, select a site.

2. Click **Publish**.
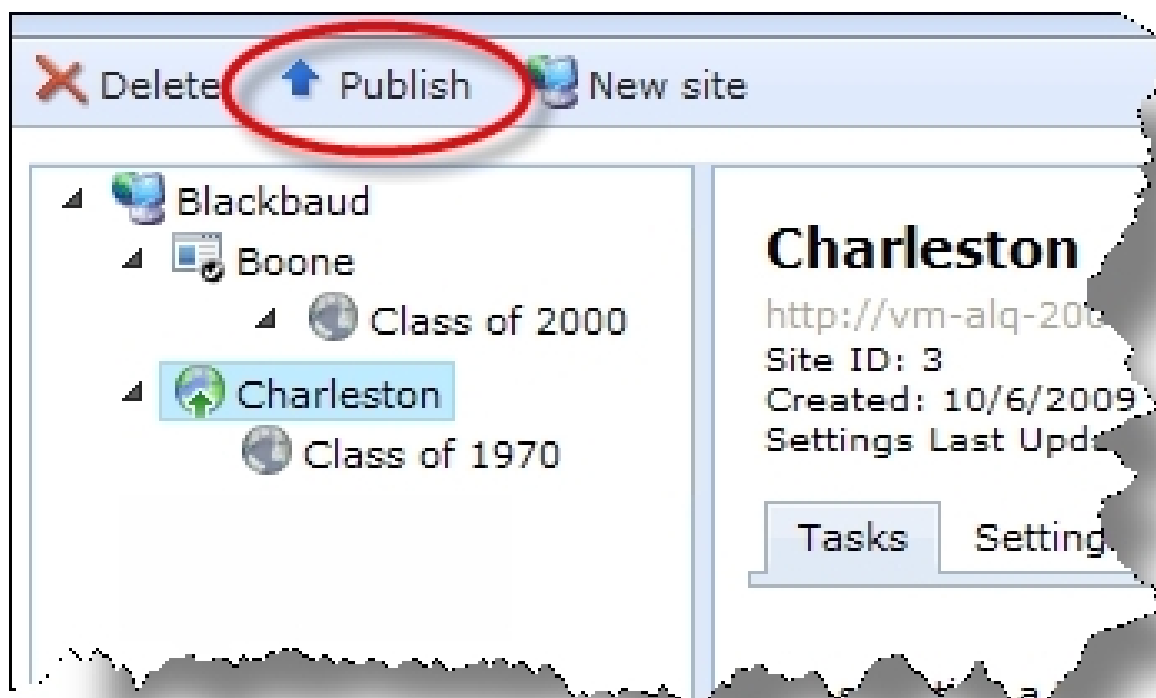
The publish process begins. After it completes, you can access the website.

Tip: You cannot create a site with the same URL as a published or unpublished site.

Note: You can unpublish or archive a site to limit access to Supervisor users and registered users with administrative rights. For more information, see Unpublish a Site on page 21 or Archive a Site on page 21.

Go to Site

To quickly navigate to a site, click **Go to site**.
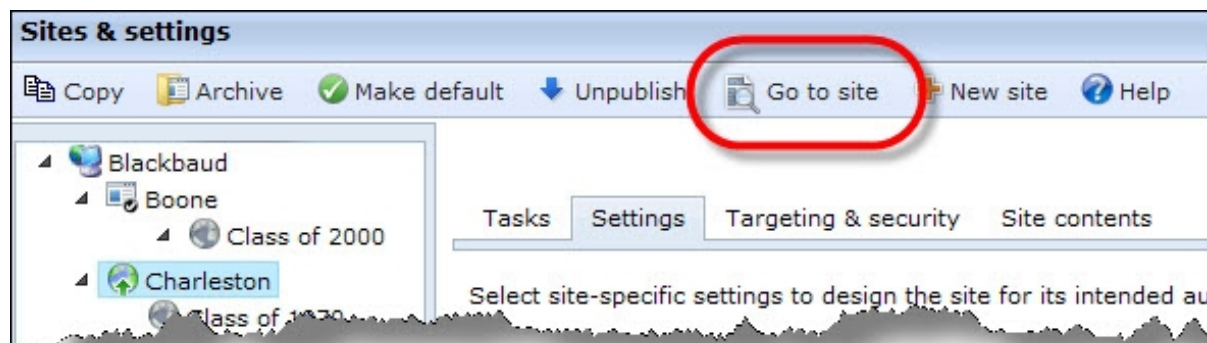
To create content such as a part or email for an individual site, highlight the site in the treeview and click **Go to site**. You will automatically log in to the site.

Unpublish a Site

The **Unpublish** button appears for published sites. If you unpublish a site, only Supervisor users and registered users with administrative rights can access the site. You can unpublish a site to hide it from users while you make updates. When you unpublish a site, you cannot create a site with the same URL.

Archive a Site

To remove a site from the Internet but retain it in the database, you can archive it. You can access an archived site from the *Sites & settings* treeview, but you cannot edit it.

Only Supervisor users and users with Edit site rights can archive a site. After you archive a site, only Supervisor users and registered users with administrative rights can access it through the URL.

The **Archive** button appears for a site under these conditions:

- The site is not the default site.
- You are not currently working in the site. To verify your current site, check the URL or the breadcrumbs beneath the menu bar.
- You have rights to delete the site.

To archive a parent or child site, select it in the *Sites & settings* treeview and click **Archive**. If you archive a parent site, you also archive its child sites.

A **Restore** button appears for archived sites. Supervisor users and users with Edit site rights can use this button to activate the archived site. You must publish the site again for it to appear on the Internet. For information, see Publish a site on page 19.

Tip: You cannot create another site using the same URL as a published, unpublished, or archived site.

Copy a Site

When you create a site, you can base it on an existing site to save time on tasks such as web design and part configuration. This creates a site with existing layouts, templates, and settings that you can update as necessary, which is useful for recurring events and programs such as walk-a-thons or campaigns.

Note: You can copy any site in the database, including the default site and any parent or child site.

When you copy a site, you select one of four options to determine the content to copy. The program copies parts in one of three ways. Some parts are automatically shared between the original site and the new site, and select parts are shared when you use an option to share them from a template with other sites. Other parts are duplicated to create separate parts for the new site.

Tip: If you do not want to copy an entire site, you can move content, such as parts and layouts, from their current site to another site. For example, to move a Donation Form part, select another site in the **Assign to site** field on the Properties tab for the part.

> **Copy a site**

1. In the *Sites & settings* treeview, select a site.

2. Click **Copy**. The Copy Site page appears.
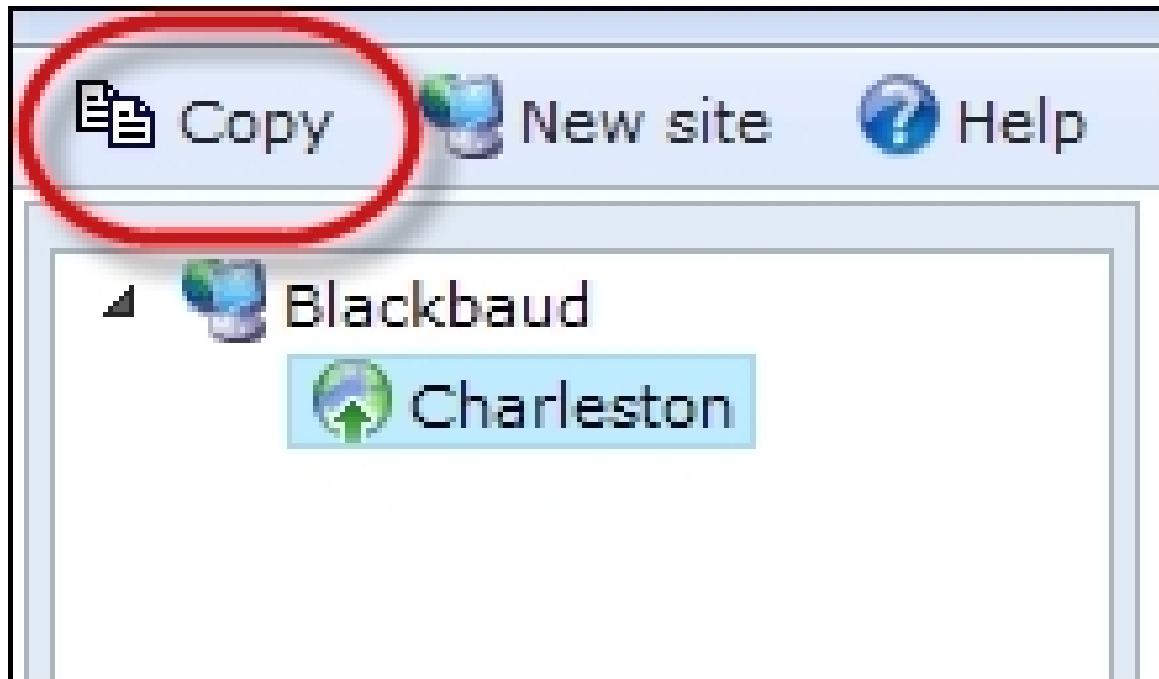
3. Under **Copy site**, enter settings such as the site name. For information about these options, see Create a parent or child site on page 15.

4. Under **Select content to copy**, select the content to copy for the new site.

Tip: The program copies all site settings from the original site to the new site. You can edit the site settings as necessary. For example, you can adjust site tracking settings so Google *Analytics* tracks only the new site. For information about settings, see Settings on page 31.

- **All** — To copy the entire content and design, select **All**. The option provides details such as the number of images, pages, and parts to copy.

- **Templates** — To copy templates for pages, email, and eCards, select **Templates**. This does not copy the pages, friendly URLs, email messages, or eCards that use the templates.

Note: The **All** and **Templates** options copy parts. Some parts are shared between the original site and the new site, while other parts are duplicated to create separate parts for the new site.

- **Layouts** — To copy only style sheets, layouts, and images, select **Layouts**.

Note: The **All**, **Templates**, and **Layouts** options copy images from *Image library* but not images uploaded by website users such as profile images on the User Networking part.

- **Settings only** — To copy only site settings, select **Settings only**.

5. To copy security settings, select **Copy security settings**. This copies the original site's security permissions from the Targeting & security tab, as well as security assignments. It also copies security permissions from the Targeting & security tabs on parts and pages.

   For information about the Targeting & security tab, see the *Parts Guide*. For information about security assignments, see the *Users & Security Guide*.

6. To create the new site, click **Copy site**. A process page appears. After the process, "Complete" appears.

Note: To undo the copy and remove the new site, click **Undo copy** on the process page. The program removes the site and all duplicated content from the database. Shared content remains in the database for the original site.

7. To update the new site's settings, click **Go to site settings**. The Settings tab appears. For information about site settings, see Site Settings on page 58.

   The new site does not appear on the Internet. For information about how to publish it, see Publish a site on page 19.

Duplicate Parts

When you copy a site and its parts, the parts copy in one of three ways. Some parts are automatically shared between the original site and the new site, and select parts are shared when you use an option to share them from a template with other sites. Other parts are duplicated to create separate parts for the new site.

The following parts are duplicated when you copy a site and its parts. The "*" indicates parts that do not include website user data. For example, the Discussion Group part is duplicated but its posts are not.

Note: Parts that are not in the list are shared between the original or template site and the new site . For information about shared parts, seeShared Parts on page 25. For information about shared template parts, see Shared Template Parts on page 26.

- Anonymous Newsletter Subscription
- Change User ID/Password
- *Content Comparison

- Directory
- *Discussion Group
- *Documents
- Donation Form
- eCards
- Email Forwarding Form
- *Event Calendar
- *Event Calendar Group
- *Event Calendar Highlights
- Event Registration Form
- Flash Player
- Frame
- Giving Search
- Language Selector
- Membership Form
- Menu
- Navigation Buttons
- News Reader
- Page Sharing
- Payment
- Payment 2.0
- Payment Summary
- *Poll
- Profile Display
- Profile Form
- Quick Search
- Search
- *Survey
- Tag Display
- Targeted Content
- Transaction Manager
- User Email Preferences Form
- User Interests Form
- User Link Module
- User Login

- User Photos Form
- *Weblog

Shared Parts

When you copy a site and its parts, the parts copy in one of three ways. Some parts are automatically shared between the original site and the new site, and select parts are shared when you use an option to share them from a template with other sites. Other parts are duplicated to create separate parts for the new site.

The following parts are automatically shared when you copy a site and its parts.

Note: Parts that are not in the list are shared between the template site and the new site, or are duplicated to create separate parts for the new site. For information about shared template parts, seeShared Template Parts on page 26. For information about duplicate parts, seeDuplicate Parts on page 23.

- Alumni Class Notes
- Chapter Links
- Chapter Manager
- Chapter Page Element
- Form Display
- Fundraiser
- Fundraiser Dashboard
- Fundraiser Page Element
- Giving History
- Job Board
- Menu (Deprecated)
- My Friends
- Payment Summary 2.0
- Personal Notes
- Personal Page Element
- Personal Page Manager
- Report (Email)
- Report (Fundraiser)
- Report (Web Traffic)
- Scrolling Donor Display
- Suggested Content
- User Education Profile Form
- User Networking Manager

Shared Template Parts

When you copy a site and its parts, the parts copy in one of three ways. Some parts are automatically shared between the original site and the new site, and select parts are shared when you use an option to share them from a template with other sites. Other parts are duplicated to create separate parts for the new site.

The following parts are shared when you share them from a template with other sites.

> **Note:** Parts that are not in the list are shared between the original site and the new site, or are duplicated to create separate parts for the new site. For information about shared parts, seeShared Parts on page 25For information about duplicate parts, seeDuplicate Parts on page 23.

- Formatted Text and Images
- Formatted Text and Images (secured)
- Slideshow
- Unformatted Text

> **Note:** If you do not select the option to share a part, it is duplicated to create a separate part when you copy the site.

Multi-Factor Authentication

To help you maintain security, you can use multi-factor authentication (MFA) during login. In order to enable MFA, you must complete the following admin tasks.

MFA Configuration has its own Tab within **Sites & Settings**, **Settings** at the Organization level. This setting is system-wide; it cannot be enabled/disabled for specific users.

- Email templates must be configured for MFA code emails for each instance of a User Login part and at the organization level.

- Email templates must be configured for MFA address change emails for each instance of a User Login part and at the organization level.

- **Blackbaud NetCommunity** requires the Fundraiser and Form Display parts to have these Emails configured.
- In the Administration MFA section, if you have parts that need email templates configured, you can select **Open incomplete parts list** to see a list of all those parts.

Note: You can only save or activate the MFA checkbox once all the Email template/incomplete part requirements have been completed.

- Labels and messages on the MFA popups are customizable from the Language tab of the User Login part editor

Note: For login.aspx, labels and messages have default text and are not customizable.

Login Experience

When you enter your username and password into the User Login part on a page for the first time after you have enabled MFA, a popup is presented which provides a one-time opportunity to add or update the email address which is associated with your user account and where you wish to receive your MFA code.

Select **Send Code** to receive a multi-factor authentication code via email.

The following are details about the security code:

- The code is valid for 10 minutes--this time limit is non configurable.
- The code locks out after five security code requests have been entered incorrectly--this number is non configurable.
- Resend requests count as a failed login attempt.

  Note: Resend requests invalidate any prior codes.

- The lockout duration originates from Sites & Settings, Registration and login options, Account lockout duration. Admins can configure this, and it must be at least ten minutes.
- The code is required after manual logout, when the session expires, and on each different browser and device.

If you do not have an email address on file, you will be prompted to enter one. When the user chooses to update their email address, a new popup is displayed providing the ability to change their email address. For added security, an email is sent to their old email address alerting them of this address update. Subsequently, the email address the user has selected for MFA cannot be changed via the MFA popup and must be changed through the Change Username/Password part or by contacting your organization's admin.

User Login Part

The User Login Part includes a link to **MFA Code Email**, which allows you to access and edit the MFA code email template. You can also use the new **Change Email Address Email** option.

In addition, the Language tab on the User Login part includes a category for "Multi-factor authentication." This allows you to customize verification popups and data entry validations.

User List

When MFA has been enabled, the user list displays a filterable column showing the Email Verification Status of the Users account linked email. When you verify email addresses, fraud prevention is improved and the ability to protect sender reputation increases.
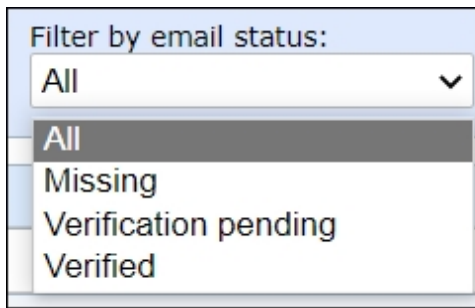
Settings

There are two types of settings in *Sites & settings*: organization settings and site settings.

Organization settings are global settings that apply to all sites you host. To access organization settings, select the Settings tab from the top-level item in the *Sites & settings* treeview.
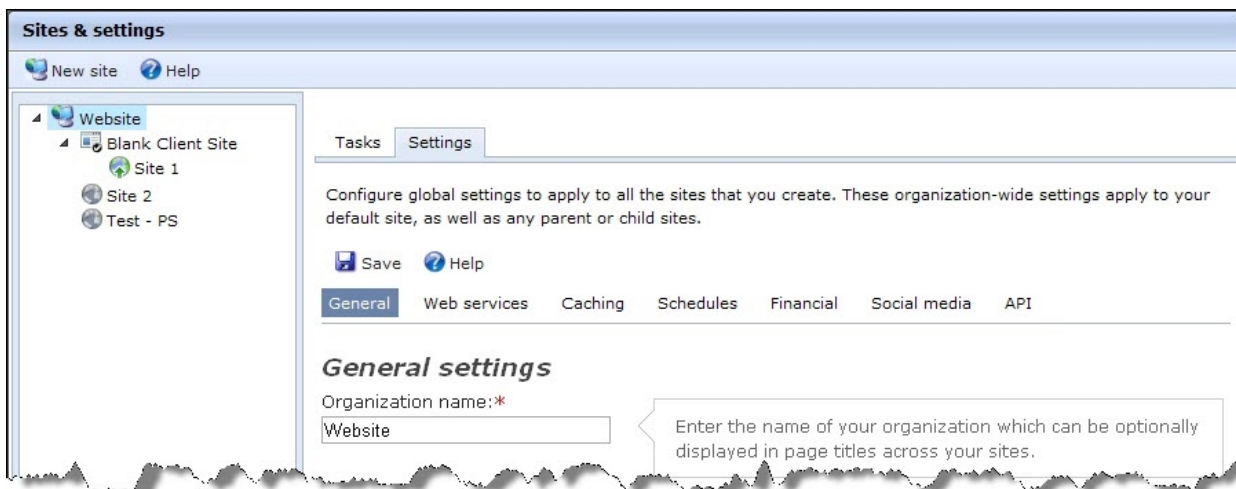
Site settings are site-specific settings that apply to default, parent, or child sites. To access site settings, select the Settings tab from a default, parent, or child site in the *Sites & settings* treeview.
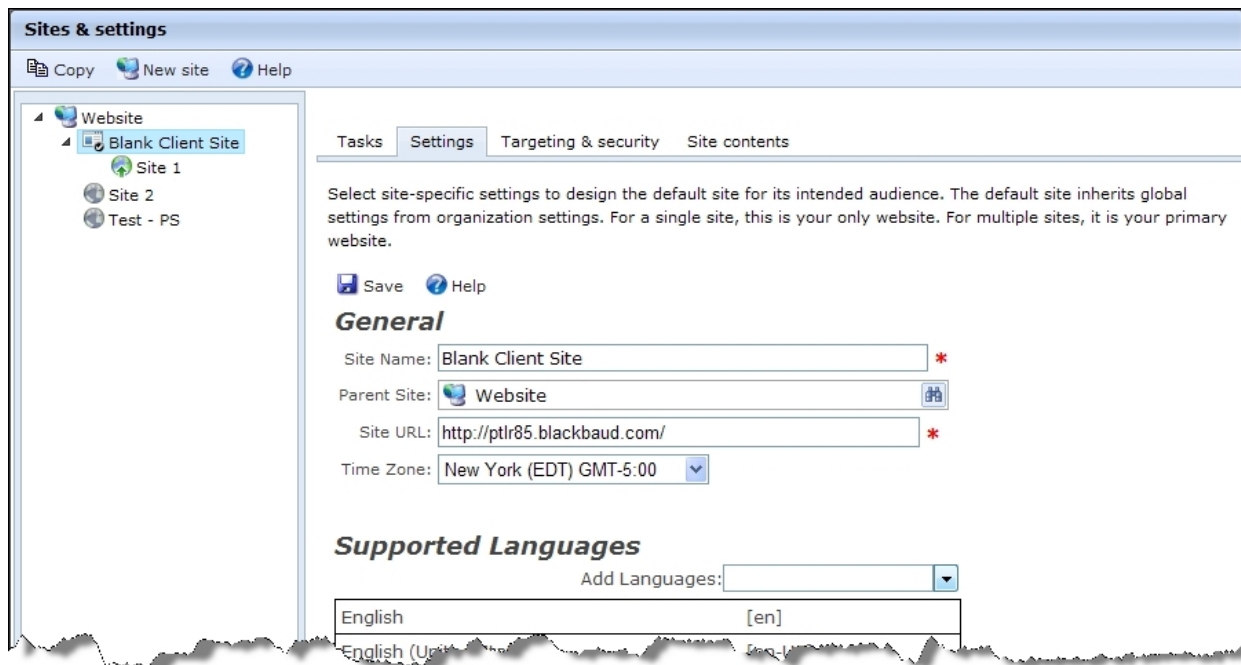
Organization Settings

Organization settings are global settings that apply to all sites you host. These settings include web services, caching, and service scheduling. All default, parent, and child sites inherit organization settings.

> *Warning:* We strongly recommend you assign full Administrator rights to only a select number of users for organization settings. General users should not have access to these settings because any change can affect multiple websites and web pages.

General

Under **General**, enter global settings for your organization such as spell check settings and integration options. For example, you can select an HTML tag to define line breaks in content and whether to require Secure Sockets Layer for pages.

> **General organization settings**

1. In the **Organization name** field, enter the name of your organization.

2. When users log in to your website, the program refreshes their roles. To allow users to leave the site and log in again without role refreshes, enter a role update interval in the **Update user role** field. During this interval, the program does not refresh roles when users log in again. To disable this option, enter "-1."

Tip: We recommend you enter "-1" to disable the option and mange role refreshes with the role refresh interval instead. You set the role refresh interval under **Role refresh** on the Service schedules tab.The **Update user role** option can impact performance when the site refreshes roles for each user on each login, or on each login after the specified interval. The performance impact depends on the number of users who log in and query-based roles the site refreshes. For information about the role refresh interval, seeSchedules on page 45.

3. To save the settings, click **Save**.

Email settings

To use this setting, you must send email messages to query-based email lists that use constituents as the data source. You create the queries in The Raiser's Edge and then create email lists based on them in *Lists*. For information about email lists, see the *Email Guide*.

1. To autofill forms with constituent data when users click links in email messages, select **Use email links to autofill forms**.

The setting autofills forms with biographical details such as name, title, primary address, phone number, and email address. When you include links to forms in query-based emails, the program pulls data from constituent records even when users are not logged in to your website.

The setting applies to forms that you create with Donation Form, Email Forwarding Form, Event Registration Form, Event Registration Form (Classic), Membership Form, User Email Preferences Form, and User Login parts. It does not apply to forms that require users to log in because email links do not bypass login requirements.

> **Warning:** If a recipient forwards a query-based email and someone else follows a link from the email message to a web form, the original recipient's biographical details autofill the form.

2. To send emails to each constituent when multiple records include the same email addresses, select **Send a unique email to each constituent who shares the same email address**. Typically, you select this option when you want constituents such as couples or parents and children who share email addresses to each receive copies of messages. If the emails include merge fields, the messages for each recipient are unique and populate each constituent's information.

> ☑ Send a unique email to each constituent who shares the same email address
>
> When multiple constituents share the same email address, select this checkbox if you want each constituent to receive emails to that address. If the email includes merge fields, the message for each recipient is unique and populates with that constituent's information. When you do not select the checkbox, only one copy of the email is sent to the address, and any merge fields populate with information for the constituent whose record has been in The Raiser's Edge the longest.

To send single copies of emails when multiple constituent records include the same email addresses, clear the checkbox. When you send single copies of messages, any merge fields populate with information for constituents whose records have been in the database the longest.

> **Note:** If you use multiple lists to identify email recipients, the program does not always select the constituent records that have been in the database the longest. In those instances, the merge fields populate with the information for the selected constituents.

3. To save the settings, click **Save**.

HTML editors settings

1. In the **Tag line for breaks** field, select an HTML tag to define line breaks in content created in the HTML editor. For example, if styles are applied to paragraph tags in your existing HTML content, select the paragraph tag to indicate line breaks. You can use the <p>, <div>, or <br> tags.

HTML editors

Tag for line breaks:

P	▾

Select an HTML tag for line breaks in the content that you create with the HTML editor.

Spell check language:

US	▾

Select the language dictionary to use with the spell check.

Words to ignore:

NetCommunity; my site; you

Enter words or phrases to include in the spell check dictionary. For example, enter your organization's name and other common words or phrases to allow on your site.

Words to correct:

Blackbaud

Enter words or phrases to remove from the spell check dictionary of safe words.

More rules for spell check:
- ☑ Ignore words capitalized and in all UPPERCASE
- ☐ Ignore words with any UPPERCASE letters
- ☑ Ignore Internet and file addresses
- ☑ Ignore words that contain numbers
- ☑ Ignore HTML

Safe HTML tags:
- ☑ APPLET
- ☑ BUTTON
- ☑ EMBED
- ☑ IFRAME
- ☑ INPUT
- ☑ NOSCRIPT

Select HTML elements that website users can access in HTML editors. The list includes potentially hazardous tags.

2. In the **Spell check language** field, select a language dictionary for spell check.

3. In the **Words to ignore** field, enter common words or phrases such as your organization's name to include in the language dictionary. Spell check ignores these words.

4. In the **Words to correct** field, enter words or phrases to remove from the dictionary. Spell check highlights these words as incorrect.

5. Under **More rules for spell check**, select the types of words for spell check to ignore.

- To ignore words if the first letter is uppercase or if all letters are uppercase, select **Ignore words capitalized and in all UPPERCASE**. This setting allows spell check to ignore proper nouns and acronyms.
- To ignore words that contain any uppercase letters, select **Ignore words with any UPPERCASE letters**.
- To ignore website addresses and filenames, select **Ignore Internet and file addresses**.
- To ignore words that contain numerals, select **Ignore words that contain numbers**.
- To ignore HTML code, select **Ignore HTML**. This setting allows spell check to ignore strings of code entered in the HTML editor.

6. Under **Safe HTML tags**, a list of potentially hazardous HTML elements appears. Select the HTML elements to allow in HTML editors on your website and in RSS feeds through the News Reader part. By default, all elements are included. To exclude an element, clear its checkbox.

   Warning: If you do not select **SCRIPT**, in addition to all <script> tags, the program marks all HTML event attributes, such as onmouseover, and all href attributes that contain the string javascript: as unsafe.

7. To save the settings, click **Save**.

Attributes settings

1. Under **Attributes**, select the active attributes from The Raiser's Edge to make available on the website. You can use attributes in multiple places in Blackbaud NetCommunity, such as email messages and profile pages.

Tip: If you recently added a new attribute in The Raiser's Edge and it does not appear under **Attributes**, click **Refresh code tables** in *Code tables*. This updates code tables from The Raiser's Edge in Blackbaud NetCommunity. For more information about how to update code tables, seeCode Tables on page 92

Attributes

Select the attributes to make available for parts on your website. For **Interests attribute**, select the corresponding constituent attribute to use. Attributes integrate from *The Raiser's Edge*.

Constituent attributes:

- ☑ # of Family Members
- ☑ Availability
- ☑ Business Hours
- ☑ Closing Codes

Participant attributes:

- ☐ Special Requests
- ☐ Dietary Preference
- ☐ Source
- ☐ Partner Request

Education attributes:

- ☑ Athletics
- ☑ Clubs
- ☑ Reason Left?
- ☑ Dorms/Housing

Interests attribute:

Closing Codes ▾

2. In the **Interests attribute** field, select the attribute that tracks the interests of your constituents. On the User Interests Form part, users can specify interests for you to download to your database. You can then group users in email lists based on their interests and target mailings or particular web pages to the users.

Note: You can use one-per-record attributes with types of Date, Text, Number, Currency, and Yes/No in the program. Table type attributes are available without being marked as one per record. Fuzzy Date and Constituent Name type attributes are not available.

3. To save the settings, click **Save**.

❯ Permissions for organization profiles settings

1. Under **Permissions for organization profiles**, select the relationship types that you allow to edit organization profiles. Website users with these relationships to an organization can edit its profile.

2. To save the settings, click **Save**.

❯ Countries settings

1. Under **Countries**, select the countries to include as options on your website. Users can select these countries in the **Country** fields on donation forms, profile update forms, and other areas.

2. To save the settings, click **Save**.

❯ Titles settings

1. Under **Titles**, select the titles to include as options on your website. Users can select these titles in the **Title** fields on donation forms, profile forms, and other areas.

2. To save the settings, click **Save**.

❯ Addressee and salutation merge fields settings

1. To expose the **Addressee** and **Salutation** merge fields in *Email* and on the Directory, Profile Display, and Profile Form parts, select **Enable merge fields**. These fields pull data from the Addressees/Salutations tab in The Raiser's Edge. For information about addressees and salutations, see the The Raiser's Edge *Constituent Data Entry Guide*.

Warning: The **Addressee** and **Salutation** merge fields do not inherit privacy settings from other fields, so these fields can expose data that you want to hide. For example, if you set the **First Name** field as private in *Field options* but not the **Addressee** field, the program displays first names when the addressees include this information.

2. In the **Addressee** field, select the addressee type for the **Addressee** merge field.

3. In the **Salutation** field, select the salutation type for the **Salutation** merge field.

   If you select **Enable merge fields** but do not select an addressee or salutation type, the program uses the primary addressee and salutation types from The Raiser's Edge. If you do not set primary addressee and salutation types, the program uses full names.

4. To save the settings, click **Save**.

Phone type mapping settings

1. Under **Phone type mapping**, map phone types from Blackbaud NetCommunity to The Raiser's Edge. Under **The Raiser's Edge phone type**, phone types in The Raiser's Edge appear. Under **Blackbaud NetCommunity phone type**, select the corresponding phone types.

Note: The **Blackbaud NetCommunity phone type** column includes phone types from the Bio 1 tab on constituent records in The Raiser's Edge, except Business which is from constituent primary business records.

2. In addition to the default phone types in The Raiser's Edge, you can map five additional phone types. Under **Blackbaud NetCommunity phone type**, select the additional phone types. Under **Caption**, enter labels for the types in The Raiser's Edge.

Note: When you send messages from **Email**, **Messages**, individuals in a "Constituents" data source list must have an email address that matches the type selected in the **Email address type** field on the template or message, an email address marked as primary in The Raiser's Edge, or an email address with the same phone type that is mapped to **Email** under **Phone type mapping**. If the constituent's record does not have an email address that matches any of these types, the individual does not receive the message.

Warning: To avoid email delivery errors, do not change the mapping for the Email address type after you set it. If you change the Email address type after you map it for the website profile, click **Refresh code tables** in Code Tables on page 92.

3. To save the settings, click **Save**.

Web Services

Under **Web services**, establish global service settings for the program, integration, customizations, and QAS address service.

> The Raiser's Edge web service settings

Under **The Raiser's Edge settings**, enter information about the web service that allows the website to communicate with The Raiser's Edge database.

1. In the **URL** field, enter the location of the web service.

The Raiser's Edge settings

Enter the web service URL and your login credentials to allow *Blackbaud NetCommunity* to communicate with your *The Raiser's Edge* database.

URL:

http://vm-ec-us08/RE7Service/MasterService.asmx

User: Password:

ShelbyPortal   ●●●●●●●●●●●●●

Database number:

50

2. In the **User** and **Password** fields, enter the login credentials to connect to the web service.

3. In the **Database number** field, enter the database number for the web service from the registry.

4. To save the settings, click **Save**.

> Blackbaud core components settings

Under **Blackbaud core components**, enter information about the Blackbaud core components that you must install on the web server.

1. In the **URL** field, enter the location of the Blackbaud core components. The core components include all files and configuration settings required to integrate the website and its database, as well as the services required by your website.

Blackbaud core components

Enter the URL where you installed the Blackbaud core components on the web server and the ID for your website's database. Blackbaud core components include files and configuration settings to integrate the website and its database.

URL:

http://localhost/bbappfx/AppFxWebService.asmx

Database ID:

BBInfinity

Credentials for bbAppFx web service:

◉ Default credentials   To use credentials from the *Blackbaud NetCommunity* application pool to connect to
○ Specific user   the bbAppFx web service, select this option.

2. In the **Database ID** field, enter the ID for your website's database.

3. Under **Credentials for bbAppFx web service**, select whether to connect to the bbAppFx web service with default credentials from the application pool or with credentials for a particular *Windows* user account.

Tip: If you use basic authentication, select **Specific user** and enter credentials for a *Windows* user account. If you use Windows authentication, you can use default credentials from the application pool or use a *Windows* user account.

4. To save the settings, click **Save**.

Blackbaud services settings

Under **Blackbaud services**, enter information about Blackbaud-hosted services such as email servers. The program uses this information to communicate with the hosted service.

1. The **Host name** field displays the name of your Blackbaud host.

Blackbaud services

Enter your login credentials for Blackbaud-hosted services such as email servers. The program uses the credentials to communicate with your hosted services.

Host name:

ncsrvtest.bbhosttest.com   ☐ Use "https" to connect

User: Password:

DemoUser   ●●●●●●●●●●●●●●

Warning: Do not edit the **Host name** field unless Blackbaud Support instructs you to. If you change the host name, you may not be able to process donations or communicate with constituents.

2. To access hosted services via HTTPS, select **Use "https" to connect**. Always select this checkbox unless Blackbaud Support tells you otherwise.

3. In the **User** and **Password** fields, enter the login credentials provided by your Blackbaud account manager. If you do not have this information, send an email to solutions@blackbaud.com.

4. To save the settings, click **Save**.

Blackbaud Payment Service settings

Under **Blackbaud Payment Service**, enter the *Blackbaud Payment Service* login credentials provided by your Blackbaud account manager. To help you comply with the Payment Card Industry Data Security Standards (PCI DSS), the program uses the *Blackbaud Payment Service* to securely store credit card and merchant account information.

1. In the **User** and **Password** fields, enter the Blackbaud *Payment Service* login credentials provided by Blackbaud. If you do not have this information, contact Customer Support from Blackbaud's website.

Blackbaud Payment Service

To help you comply with the Payment Card Industry Data Security Standards (PCI DSS), **Blackbaud NetCommunity** uses the *Blackbaud Payment Service* to securely store credit card and merchant account information. For information about the *Blackbaud Payment Service*, click here. Enter your login credentials to allow the website to communicate with the service.

User:

laurapay

Password:

••••••••••••••

2. To save the settings, click **Save**.

Note: For more information about how the program helps your organization comply with PCI DSS, as well as additional steps to secure sensitive cardholder information, see the *Payment Application Data Security Standards (PA DSS) Implementation Guide.*

Custom service settings

Under **Custom service**, enter information about any custom service that you use for custom parts.

1. In the **URL** field, enter the location of the custom service.

Custom service

If you use a custom service for your custom parts, enter the web service URL and login credentials to allow **Blackbaud NetCommunity** to communicate with the service.

URL:

http://ptlr02/bbAppFx/BBNCSvc/MasterService.asmx

User:

ShelbyPortal

Password:

••••••••••••••

Database number:

1

2. In the **User** and **Password** fields, enter the login credentials to connect to the custom service.

3. In the **Database number** field, enter the database number for the custom service from the registry.

4. To save the settings, click **Save**.

QAS address service settings

Under **QAS address service**, enter information about the *QAS* address service that allows United Kingdom users to quickly and accurately enter addresses. After you set up this option, a **Find address** link appears beside the **Postcode** field on parts that process addresses. When users enter postcodes and click the link, a **Select Address** field lists addresses for the postcode. Users can select addresses to autofill the remaining address fields.

1. In the **URL** field, enter the *QAS* URL to integrate with the address service.

QAS address service

You can integrate with the QAS address service to allow users in the United Kingdom to search for addresses based on postcodes. This allows them to select addresses quickly and improves accuracy. Enter the address service URL and your login credentials to allow **Blackbaud NetCommunity** to communicate with the service. For information about the QAS, click here.

URL:

User: Password:

2. In the **User** and **Password** fields, enter your *QAS* credentials.

3. To save the settings, click **Save**.

   To confirm the integration, visit a web page on your site that processes United Kingdom addresses. For example, visit a page that includes the Donation Form part. When integration is successful, a **Find address** link appears beside the **Postcode** field.

Caching

Under **Cache settings**, define how long to store items. To minimize repeated access to the database and web services, the program can store recently accessed items in a cache. If the program does not retrieve an item from the cache within the set time limit, it is removed from the cache.

❯ Cache settings

1. Enter how many minutes to store items placed in the cache while the program is running. If another cache setting applies to an item, that setting overwrites this value.

Cache settings

The program uses data caching to minimize repeated access to the database and web services. Enter how long to store items in cache.

Application:

[20]   minutes

> Enter how long to store information for *NetCommunity*. Settings for specific types of data can also be set below.

Code tables:

[20]   minutes

> Enter how long to store code tables from *The Raiser's Edge*.

News reader:

[60]   minutes

> Enter how long to store Really Simple Syndication (RSS) for a News Reader part.

News feed:

[60]   minutes

> Enter how long to store RSS content for a Weblog part.

Note: If you do not define cache settings, the program cache uses the .NET default of 20 minutes.

2. In the **Application** field, enter how long to store objects, content, and settings that the web service retrieves from the database.

3. In the **Code tables** field, enter how long to store code tables and table entries that the web service retrieves from the database.

4. In the **News reader** field, enter how long to store Really Simple Syndication (RSS) or Atom content retrieved for the News Reader part.

5. In the **News feed** field, enter how long to store RSS content created by the Weblog part.

6. To save the settings, click **Save**.

Schedules

Under **Schedules**, establish schedules for services such as email jobs, email lists, and role refreshes.

> **Email settings**

1. Under **Email jobs**, select how often to run the process to send email messages.

Tip: If you are in a different time zone than your web server, select times based on your web server's time zone. The program does not use your organization's default time zone or the local time zone of the user who sets the schedule.

- To not run the process, select **Never**.

- To send email at regular intervals, select **Every [ ] (minutes)** and enter the interval between instances of the process.

- To send email once a day, select **Daily at** and select the time to run the process.

2. To save the settings, click **Save**.

Note: The program does not use this schedule to send acknowledgment emails that are automatically generated when website users complete actions such as submitting forms. The program only uses this schedule to send alerts, email messages, and staff notifications. For information about messages and staff notifications, refer to the *Email Guide*. For information about email alerts, refer to the *Forms Guide*.

> **List acquisition and refresh settings**

1. Under **List acquisition and refresh**, select how often to run the process to acquire and refresh the email lists.

- To not run the process, select **Never**.

- To acquire and refresh email lists at regular intervals, select **Every [ ] (minutes)** and enter the interval between instances of the process.

- To acquire and refresh email lists once a day, select **Daily at** and select the time to run the process.

    Tip: If you are in a different time zone than your web server, select times based on your web server's time zone. The program does not use your organization's default time zone or the local time zone of the user who sets the schedule.

2. To save the settings, click **Save**.

> **Role refresh settings**

1. Under **Role refresh**, select how often to run the role refresh process.

    Note: When you configure standard role refresh, the program caches the information rather than load it by a SQL call on every login. For more information, see the *Users & Security Guide*.

- To not run the process, select **Never**.

- To refresh roles at regular intervals, select **Every [ ] (hours)** and enter the interval between instances of the process.

- To refresh roles once a day, select **Daily at** and select the time to run the process.

    Tip: If you are in a different time zone than your web server, select times based on your web server's time zone. The program does not use your organization's default time zone or the local time zone of the user who sets the schedule.

2. To save the settings, click **Save**.

    Note: By default, a member role refreshes every 24 hours after the member's last login. If your organization does not download the member to the database as part of a download transaction after the last login, there is no role to refresh. After you download the member, the role refreshes during the next login and the 24-hour interval is set to that date and time.

> **Fundraiser synchronization settings**

1. Under **Fundraiser synchronization**, select how often to run the synchronization process that merges data from the database with Fund solicitor information on the Fundraiser part.

    Note: To apply this setting to a Fundraiser part, you must select its **Synchronize** checkbox.

- To not run the process, select **Never**.
- To synchronize the Fundraiser part at regular intervals, select **Every [ ] (hours)** and enter the interval between instances of the process.
- To synchronize the Fundraiser part once a day, select **Daily at** and select the time to run the process.

Tip: If you are in a different time zone than your web server, select times based on your web server's time zone. The program does not use your organization's default time zone or the local time zone of the user who sets the schedule.

2.   To save the settings, click **Save**.

Integration service settings

Under **The Raiser's Edge Integration service**, you view the number of records to update in The Raiser's Edge, and you can select to refresh them. You can also determine how often to run the integration process to send information to the The Raiser's Edge database.

1.   Beside **Number of records to update**, the number of records to update in The Raiser's Edge appears as a hyperlink. When you select it, a screen appears that lists each record type that is updated by this process. The number of records to update for each type also appears, along with the type's last integration date.

   To refresh the records to make sure the process integrates the latest data from Blackbaud NetCommunity to The Raiser's Edge, click the **Refresh** icon. When the refresh completes, the date and time update to reflect the refresh.

2.   Under **Frequency**, select how often to run the integration process to send information to the database.

- To prevent the process from running, select **Never**.

- To send information to the database at regular intervals, enter the number of records to process each time and enter the interval in minutes in the **[ ] records every [ ] (minutes)** fields.

- To send information daily, enter the number of records to send during each process and enter the time in the **[ ] records daily at [ ][ ][ ]** fields.

Tip: If you are in a different time zone than your web server, select times based on your web server's time zone. The program does not use your organization's default time zone or the local time zone of the user who sets the schedule.

3. To save the settings, click **Save**.

User import settings

1. Under **User imports**, select how often to run the process to import user information from the database.

- To not run the process, select **Never**.

- To import user information at regular intervals, select **Every [ ] (hours)** and enter the interval between instances of the process.

- To import user information once a day, select **Daily at** and select the time to run the process.

Tip: If you are in a different time zone than your web server, select times based on your web server's time zone. The program does not use your organization's default time zone or the local time zone of the user who sets the schedule.

2. To save the settings, click **Save**.

Secure payment page template update

To help you comply with the Payment Card Industry Data Security Standard (PCI DSS), some parts use secure payment pages on a Blackbaud server to process credit card billing information and payment information. Use this setting to update your secure payment pages with the latest design and property changes you make for style sheets, layouts, templates, and pages. If you do not use this setting, the program holds your changes in a queue and pushes them to the secure payment page within one hour. For more information about secure payment pages, see the *Parts Guide*.

1. Under **Secure payment template update**, to manually update secure payment pages so they include the latest template changes for desktop browsers and mobile devices, click **Update templates**.

The update begins and the button disables. After it completes, the button enables again.

Note: You cannot select to update a secure payment page for a specific part. When you click **Update templates**, secure payment pages update for almost all Payment 2.0 parts. The program does not send updates to the Blackbaud secure payment server for Payment 2.0 and Event Registration pages that do not accept credit cards.

2. To replace your organization's template for the secure payment page with a generic template, clear **Enable secure payment template updates**. The **Update templates** button disables so you cannot apply your template to the page.

   It is unlikely you want to use the generic template because it does not match the rest of your website. However, Flash, JavaScript, and externally hosted content does not upload to the secure payment page for PCI DSS compliance. If your page, template, or layout includes this content and the absence of it heavily impacts the appearance of your secure payment page, you may want to use the generic template. You can also use the generic template if you need to temporarily revert your template updates to the page. When you are ready to use your template again, select **Enable secure payment template updates** and click **Update templates**.

3. To save the setting, click **Save**.

> **Delete email permanently**

In *Email*, when you select to delete an email message or newsletter issue, it removes from the user interface, but the data remains in the back end of the database. To improve performance and permanently delete this email, schedule the options on this setting. If you do not want to delete these messages, select **Never** for both options.

Note: To prevent the possibility of anyone scheduling this setting, your System Administrator can use the ShowEmailDelete web.config setting to remove it from the Schedules tab. By default, the setting is <add key="ShowEmailDelete" value="True"/>. To remove it from the tab, enter False.

1. Under **Automatically delete email older than**, you can select to delete messages and newsletters based on whether the email is beyond a certain number of days, months, or years.

   If you do not want to permanently delete these email based on age, select **Never**.

To delete email older than a certain age, select the second option. In the field beside it, enter the number of days, months, or years to delete email, and then select an option in the drop down. For example, to delete email older than two years, enter "2" in the field and select Years.

Note: When you use this setting, the program calculates the age based on the email sent date. The process then deletes the applicable email from *Email* before deleting it from the back end of the database. If you leave the default as **Never**, the program only removes email from the back end of the database.

2. Under **Business process frequency**, you select how often to run the business process.

If you do not want to permanently delete these messages, select **Never**.

To establish a frequency for the program to permanently delete email messages and newsletter issues, select **Every [ ] day(s) at [ ]:[ ][ ]** and enter the number of days and time to run this delete process in the fields.

Delete email permanently

In *Email*, when you select to delete an email message or newsletter issue, it no longer appears in the user interface, but the data remains in the database. To improve performance and permanently delete these messages from the database, schedule the options for this setting. If you do not want to delete these messages, select **Never** for both options.

To run the process as efficiently as possible, we recommend you schedule this to run after hours when users are less likely to access *Blackbaud NetCommunity* and *Raiser's Edge*.

Automatically delete emails older than:
⦿ Never
◯ [   ] [Days ▾]

Last run: Never

Business process frequency:
⦿ Never
◯ Every [   ] day(s) at [1 ▾]:[00 ▾] [AM ▾]

Options:
Do not allow for process to run more than [30] minutes

3. Under **Options**, enter the number of minutes to allow the process to run in the **Do not allow for process to run more than [ ] minutes** field.

Depending on the volume of email you need to permanently delete, the process can exceed the amount of time you enter in this field. When this occurs, the process pauses and starts again according to the interval you scheduled in the **Every [ ] day(s) at [ ]:[ ][ ]** fields.

For example, you need to run this process for the first time. Due to the high volume of email to initially delete, you can schedule it to run every night (1 day) at 1 AM for 300 minutes (5 hours). The process runs longer than 300 minutes so it pauses until the next night at 1 AM. At that time, it starts again for the next 300 minutes.

If the process pauses according to your schedule and the number of minutes you allow it to process, **Did not finish** appears in the **Last run** information box on the right.

Note: To run the process as efficiently as possible, we recommend you schedule it to run after hours when users are less likely to access Blackbaud NetCommunity and The Raiser's Edge.

Before you permanently delete email using this process, email messages and newsletter issues on a constituent record in The Raiser's Edge appear with a link in the **Email Received** grid on the NetCommunity tab. You can click this link to open the message in Blackbaud NetCommunity. After you run this process, the link disables because you can no longer open it in Blackbaud NetCommunity. Also, if a recipient opens an email after it has been deleted permanently, submits a donation from one, or

clicks links in it, the **Opened**, **Donated**, and **Links clicked** fields do not update to reflect this information. The data that appeared in these fields when it was deleted from your database remains in place. For historical purposes, the other data, such as **Email name** and **Date sent**, also remain on the constituent record.

Financial

Under **Financial**, establish settings for eReceipts.

❯ Donation eReceipts settings

Under **Donation eReceipts**, set up a unique receipt stack for donations through your website. You can use eReceipts to include links to *.pdf files of donor receipts with acknowledgment emails.

1. In the **Receipt stack** field, enter a unique identifier such as "Online" for the receipt stack. When the program generates eReceipts, it includes the identifier as a prefix to receipt numbers. You can enter up to 60 characters.

Tip: The receipt stack you create in Blackbaud NetCommunity is not associated with receipt stacks in The Raiser's Edge; it is an independent identifier. However, you cannot save a receipt stack in Blackbaud NetCommunity that exists in The Raiser's Edge. The Blackbaud NetCommunity receipt stack must be unique.

2. In the **Initial sequence number** field, enter the first available receipt number in the receipt stack for donations through the website.

3. To save the settings, click **Save**.

Social Media

You can integrate your website with *Janrain*, a third-party authentication service to manage multiple logins for your Blackbaud NetCommunity and social network websites, such as *Facebook* and *Twitter*. When you configure this integration and users register on your website, they can select to create a unique login for your site or they can use existing login credentials from a social network website.

To allow website users to use existing social network logins, you must:

- Create a social media application so your website can integrate with the social media authentication service. Settings for the application are global. If you have more than one website, the application applies to all sites.

- On the *Janrain* website, configure the application and select the social networks to support on your login pages.

- On User Login parts, enable the social media login and select the display of the icons on login pages.

After you create and configure social media login, users view social network icons on login pages.

When a website user uses social network credentials to register for your website, the user is also logged into their social network account. Your registration page appears and the first name, last name, and email address automatically default in the fields on the page. When the user completes the page and submits the data, the program automatically creates a user record in Blackbaud NetCommunity to store the first name, last name, email address, and a link to the user's social network page. The user record includes an automatically generated user name (SocialWeb_xxx) and password (Sweb_xxx), where xxx is a random generated number. The default role assigned to new registrants applies to the user.

Note: On the login page, social media registrants cannot use the Blackbaud NetCommunity forgotten username and password functionality. Instead, users must access the social media site's forgotten password functionality to retrieve their credentials. Also, social media registrants cannot use a Blackbaud NetCommunity profile update to update a social network profile. The changes must be made separately on the social network website.

After a website user registers for your website by using social network credentials, the program remembers the social network account so users can log in again the same way.

When a user logs out of your site, the connection to the social network remains active until the user signs out of the account from the social network site.

The table below lists fields from the social media authentication service that may be sent to The Raiser's Edge. Profile data sent to The Raiser's Edge depends on whether users allow social network providers to share their information.

Social media field	Field sent to The Raiser's Edge
displayName	First name
preferredUsername	Last name
email	Email

Note: Email maps to the primary email address. If email is not available, it does not appear in The Raiser's Edge.

Create Social Media Application and Configure Janrain Settings

Create a social media application to enable the website to use the *Janrain* social media authentication and sharing service to integrate with social network providers such as *Google*. Website users can then use social network login credentials on your website login page.

When you host multiple sites and create a social media application, it applies to all sites. You must specify a domain for the application and provide the email address to use for communication with the authentication service. The *rpxnow.com* domain is available for you to use for your application or you can use your organization's domain. After you create the application, you receive an email from *Janrain*. The email contains a link for you to access your *Janrain* account and select the social networks to provide on your login pages.

Note: We recommend you use the *Janrain* help documentation for the most up to date *Janrain* procedures.

❯ Create social media application and configure Janrain settings

1. Under **Social media**, select **Create social media application**. Additional fields appear.

2. In the **Domain** field, enter the fully qualified domain for the social media application. For example, you might enter signin.yoursite.com. To qualify a domain, you must create a CNAME (canonical name) record and an A record (referred to as the @) to map to *Janrain's* domain and IP address. We recommend you contact *Janrain* for detailed configuration information.

Note: Blackbaud provides a standard preconfigured domain, *rpxnow*, that you can use for free. You may want to use this domain if your organization does not have its own domain configured with *Janrain*. To use the *rpxnow* domain, enter it in this format: name.rpxnow.com, where "name" is the name you want to assign to the social media application. For example, the domain for a Blackbaud NetCommunity for ABC Organization may be "abcorganization.rpxnow.com."

Tip: Registering domain names and creating CNAMEs and A records requires advanced knowledge of the DNS (Domain Name System). If you do not have this knowledge or experience, contact the appropriate system administrator at your organization for assistance.

3. In the **Email** field, enter the email address to use for communication from the social media authentication service about your account.

4. Click **Create**. The application creates and you receive an email from the authentication service. The email provides a link to your *Janrain* account so you can configure it.

5. To save the settings, click **Save**.

Note: After you save the social media application, use **Clear Settings** with caution. When you clear settings, the **Domain** and **Email** fields remove, but the social media application does not delete from *Janrain*. If you create a new social media application, you cannot use the same domain again. To delete the *Janrain* account, you must do so on *Janrain's* website.

6. Open the email from *Janrain* and click the link to access your account. On the *Janrain* website, you identify website domains and select the social networks to display on Blackbaud NetCommunity login pages. For information about *Janrain* settings, see *Janrain's* help file.

    After you complete these steps in *Janrain*, you can enable the social media application on User Login parts. For more information, see .

❯ Update social media application configuration

After you configure a social media application, you can make changes as necessary. For example, you can disable the social media application. When you do this, social media disables for all sites, and website users cannot view social media icons on login pages.

1. Under **Social media**, the **Enable social media authentication** field is selected, and the **Domain** and **Email** fields are disabled. To remove the application, clear the checkbox.

Note: After you save the social media application, use **Clear Settings** with caution. When you clear settings, the **Domain** and **Email** fields remove, but the social media application does not delete from *Janrain*. If you create a new social media application, you cannot use the same domain again. To delete the *Janrain* account, you must do so on *Janrain's* website.

2. To adjust *Janrain* settings, click the link beside **To configure your application click here**. A page appears so you can sign in to the authentication service and configure the social media application with the login used when the application was originally created. For information about *Janrain* settings, see *Janrain's* help file.

3. To save the settings, click **Save**.

❯ Enable social website login on a User Login part

On a User Login part, enable social media login and select the display for social network icons on the login page.

1. In *Parts*, open the User Login part to enable social media on the login web page.

    For information about how to create or edit a part, as well as the tabs on the Edit Part screen, see the *Parts Guide*.

2. On the Design tab, under **Social website login**, select **Enable social website login**. Additional options appear.

a. In the **Sign in text** field, enter the text to display for standard and social network login options.

b. In the **Social website sign in text** field, enter the text to display above the social site icons.

c. Under **Display options**, specify where to place the social site icons relative to the standard login fields.

3. Click **Save**. You return to *Parts*.

API

Under **API**, you can enter keys and other API information to allow Blackbaud NetCommunity to access data from an external system such as websites and online applications.

> **Single sign on**

When you integrate your website with another site, it can use the single sign on private key so that users who are logged in to your site do not need to enter different logins when they access the external site through links on your Blackbaud NetCommunity site. Users can click unique links from a Blackbaud NetCommunity page to access secured non-Blackbaud NetCommunity pages without entering user name and password information for the non-Blackbaud NetCommunity pages.

1. Uder **Single Sign On**, enter a private key that an external system can use to decrypt user IDs that it accesses through the GetUserID.ashx endpoint in the Blackbaud NetCommunity API. The external system can use the user IDs so that users who are logged in to your site do not need to enter different logins to access the external site through links on your Blackbaud NetCommunity site.

Single Sign On

Enter a private key that an external system can use to decrypt user IDs that it accesses through the GetUserID.ashx endpoint in the **Blackbaud NetCommunity** API. The external system can use the user IDs so that users who are logged in to your site do not need to enter different logins to access the external site through links on your **Blackbaud NetCommunity** site.

GetUserId.ashx private key:

To determine user IDs, the external system accesses the GetUserID.ashx endpoint with a return URL in the query string. The endpoint redirects website users to the return URL and uses several query string parameters to securely determine their user IDs.

2. To save the settings, click **Save**.

> LinkedIn

Note: Due to *LinkedIn* API changes, the LinkedIn Group Join part has been deprecated and no longer works on your website. If the part exists on any of your websites, we recommend you remove it as soon as possible.

Site Settings

When you host one website, site settings only apply to your default site. When you host multiple websites, you apply site settings to each default, parent, and child site.

> General site settings

Under **General**, establish default, parent, or child settings for an individual website.

1. In the **Site name** field, enter a name for the site. In the **Parent site** field, select a parent site to inherit global settings.

2. In the **Time zone** field, select your organization's default time zone. For example, if your organization is located in New York, select "New York (EST) GMT-5:00."

   The time and dates the user sees on your site pages and email in the program use the time zone specified on the User Profile Form part. If the user does not specify a time zone on the User Profile Form part, the time zone selected in the **Time zone** field appears as the default. The program uses Coordinated Universal Time (UTC) as its time standard, and time zones are expressed as offsets from the UTC. This allows the program to retain time and date information and display it accurately in multiple time zones.

   If you do not select a default time zone in the **Time zone** field, the program uses the date and time zone from the web server.

3. In the **Favicon image (.ico)** field, click **Browse** and select an .ico image file. A favicon image is a small icon that represents your website and appears in browser address bars and locations where users save your website URL, such as browser favorite lists. We recommend you upload a 16x16 or 32X32 pixel image for maximum display quality. If you select an image with a different file type or size, or if the file does not convert correctly to .ico, the file may not render correctly in all browsers.

   Note: The image file size must be 50KB or less.

4. In the **Primary site URL** field, enter the URL for a new site or change it for an existing site. You must enter the URL with a protocol such as "http://www.example.org". If a message appears that informs you it is not valid, check your Domain Name System (DNS) configuration.

> **Warning:** When "/netcommunity/" appears in your URL by default, you can remove it but you must uninstall and reinstall the program to do so. Additional technical steps are also required. For more information, refer to this Knowledgebase solution.

5. In the **Add URL** field, click **Add** to include URLs that you want to redirect to your primary site URL. For example, you can include URLs with typos or an abbreviation for your organization so that users who mistype the primary URL still reach your site.

> **Note:** When Blackbaud hosts your website and you need to add primary site URL redirects for a new Blackbaud NetCommunity domain, contact Customer Support on Blackbaud's website.

> **There are several important items to remember about alternate site URLs.**
> - You must register the domain URLs with a registrar in order for the redirects to render your primary URL. If you do not, the redirects do not work.
> - These URLs are 301 redirects that maintain search engine rankings for the primary site.
> - You can enter the URL with or without a protocol, such as "http://".
> - The program validates each URL to make sure it is unique in Blackbaud NetCommunity. When you include a URL that already exists in the database, you cannot save it in the grid.
> - It is important to remember the difference between these redirects and redirects you add in *Administration*, *URL redirects*. In this grid, you enter website redirects for the primary website URL. One redirect can reroute a group of URLs. For example, you add http://yoursite.org to redirect to the primary URL, http://www.yoursite.org. This redirects all http://yoursite.org URL requests, such as http://yoursite.org/donate and http://yoursite.org/aboutus, to the primary URL. In *URL redirects*, you add page URL redirects to reroute traffic to another page. For example, you add http://yoursite.com/donate to redirect to http://www.yoursite.com/donate. This only redirects the donation page. Be aware these page URL redirects override the redirects you add in this grid. For more information about page redirects, seeURL Redirects on page 93

6. To save the settings, click **Save**.

Language settings

1. Under **Supported languages**, select the languages to support on your website. For example, if your website audience includes Spanish and French-Canadian users, in the **Add languages** field, select **Español (Mexico)** and **français (Canada)**.

In the **Default language** field, select the default language for the website. If a website visitor's browser has a country code that is not supported, the site renders in the default language.

Note: The languages you support appear in multiple areas of the program. Supported languages appear in the **Target language** field on a part's Properties tab. They appear in the **Language** field on the Language tab. They also appear in the **Language** field that appears on a web page when you use the Language Selector part.

After you select the languages to support, you can create international pages for your website. For more information, see the *Parts Guide*.

2. Under **International**, you can select **Require postcode for UK addresses** to make the **Postcode** field required when a website donor selects United Kingdom in the **Country** field of a donation form.

3. To save the settings, click **Save**.

> **Page settings**

Under **Pages**, set up how the title bar of your web pages appears and select the default pages to appear for your website users, such as for your home page or when a login fails.

1. Under **Site page titles**, select the text to appear in the title bar of the web pages.

- To display your organization's name in the browser title bar, select **Show organization name**.
- To display the site name in the browser title bar, select **Show site name**.
- To display the title from the web page's properties in *Pages & templates*, select **Show browser title**. For more information, see the *Website Design Guide*.

Note: When you select all three options, your organization's name, site name, and page browser title all appear in the browser title bar. If you do not select an option, "Blackbaud NetCommunity" appears.

2. In the **Authorization failed page** field, select the web page from *Pages & templates* to automatically appear when a user's attempt to log in fails.

3. In the **Home page** field, select the default web page from *Pages & templates* to automatically appear as your website's Home page.

4. In the **Privacy page** field, select the web page from *Pages & templates* that includes your organization's privacy statement. In each email you send, you must include a link to a page on your website that contains the privacy statement.

Note: The program requires that you enable cookies on your browser. As a best practice, we recommend you note this in your privacy statement, in addition to any security issues.

5. In the **Error page** field, select a web page from *Pages & templates* to appear if errors occur. For example, if there is an internal problem that generates a 500 error, users view the page you select instead of the generic one from the website's server.

    The page can include a custom message with information to help identify the causes of errors. To provide error details in the message, use error merge fields in a Formatted Text and Images part. For information about the Formatted Text and Images part, see the *Parts Guide*.

Note: The program includes default behavior that prevents unresolvable page link errors from appearing. In those instances, the program redirects users to the default site's home page. However, when users attempt to access unresolvable links to files, for example www.abc.org/file/123.pdf, the custom error page you select appears. For information about default sites, see .

6. To save the settings, click **Save**.

❯ Registration and login options settings

Under **Registration and login options**, set up how your website users register and log in. For example, you can set a minimum character length for passwords on your website and configure the program to temporarily lock an account after a set number of failed login attempts.

1. In the **Member login page** field, select the web page from *Pages & templates* to automatically appear as your website's login page.

Warning: When you have multiple websites, make sure you select the login page for the same site as this setting. For example, you select **Registration and login options** for Site B. In the **Member login page** field, make sure you select the login page for Site B. If you select the login page for Site A, users do not have access to Site B.

2. Select **Require complex passwords** to apply additional password security. A complex password must contain at least eight characters, including one upper-case and one lower-case letter, and either a special character or a number.

   When you select **Require complex passwords**, the **Password minimum length** field and **Passwords are case-sensitive** checkbox are disabled.

Note: Users with Supervisor rights must always enter a complex password.

Note: To help you comply with the Payment Card Industry Data Security Standard (PCI DSS), users with Supervisor rights must change their passwords at least every 90 days. 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 in to the program. In addition, new passwords cannot match one of the last four passwords entered by the user.

3. In the **Password minimum length** field, enter the minimum number of characters to allow for passwords. To not require a password and allow users to register and log in with only a user name, enter "0."

Note: If you enter "0" in the **Password minimum length** field, when you click **Save**, the field's background color changes to red. This visual reminder indicates that users do not need to enter a password to access your website.

4. To make passwords case-sensitive, select **Passwords are case-sensitive**. This checkbox applies only to new members.

5. In the **Lock account after attempts** field, enter the number of attempts to allow the user to log in correctly. For example, to lock an account after three failed attempts, enter "3."

   To keep an account available regardless of the number of failed attempts, enter "0."

Note: You can unlock a user's account in *Users & Security*. For more information, see the *Users & Security Guide.*

6. In the **Account lockout duration** field, enter how long, in minutes, the program should lock an account after its user reaches the failed login attempt limit.

   To keep an account available regardless of the number of failed attempts, enter "0."

7. Under **Email opt-in**, select **Opt in new users to receive email messages** to set a default for new users to accept email messages from your organization. You can place a User Email Preferences Form part on your website to allow users to change the default. This setting does not affect notifications or acknowledgements.

Note: In some cases, legal restrictions may prohibit you from sending email messages to users by default. To require website users to opt in to receive email messages, clear **Opt in new users to receive email messages** and create a User Email Preferences Form part for users to subscribe to email messages. For information about the User Email Preferences Form part, see the *Parts Guide.*

Note: When you import offline users, the email setting associated with those users overwrites the online default setting.

8. To save the settings, click **Save**.

> User image options settings

Under **User image options**, configure the settings of the *Image library* the website user accesses. For example, you can select whether to require approval for images your users upload to the website and set a maximum file size for user images.

1. To require approval of all images that the user uploads to *Image library*, select **Require approval for all images uploaded by users**. By default, this checkbox is selected.

User image options

☑ Require approval for all images uploaded by users

Maximum number of images allowed per user: `0` *(enter zero for no limit)*

Maximum image size: `0` KB *(enter zero for no limit)*

Default image folder: 📁 Images 🔍

Default profile image folder: 📁 Images 🔍

Note: When you select **Require approval for all images uploaded by users**, the program saves images that the website user uploads as unapproved. Until an Administrator approves an image, it appears only for the user who loads it. To other users, an unapproved image appears as the standard "Photo Not Available" graphic.

2. In the **Maximum number of images allowed per user** field, enter the maximum number of personal images a website user can upload to *Image library*. Users upload personal images on the User Photos Form part. You can view these in *Image library* by selecting "Personal" in the **Type of image** field on the Search tab.

    To allow website users to upload an unlimited number of images, enter "0."

3. In the **Maximum image size** field, enter the maximum file size in kilobytes for images that website users upload to *Image library*.

    To use the default file size limit of 4 megabytes from the web.config file, enter "0." To upload files larger than 4 MB, you must edit the web.config file.

4. In the **Default image folder** field, select the default folder images upload to in *Image library*.

5. In the **Default profile image folder** field, select the default folder profile images upload to in *Image library*. A website user uploads a profile image on their profile page. You can view these in *Image library* by selecting "Profile" in the **Type of image** field on the Search tab.

    For information about *Image library*, see the *Website Design Guide*.

6. To save the settings, click **Save**.

❯ Site tracking settings

Google *Universal Analytics* is a service that generates detailed statistics about a website's traffic and measures conversions. When you sign up for an account with the service, you create a property for the website you want to monitor and receive a script for the service to track the website's performance. In Blackbaud NetCommunity, you enable site tracking and enter the script. The program automatically adds the script you enter to each page of your website.

1. To set up your website for traffic measurement, select **Enable site tracking**.

2. In the **Site tracking script** box, enter the script from Google *Universal Analytics* to track traffic on your website. To provide a more informative URL to capture traffic measurements on web pages, enter the variable BBNCAnalyticsURL in the script.

Note: For procedures and recommendations about how to configure visitor tracking, goals, and E-Commerce for Google *Universal Analytics*, refer to Configure Blackbaud NetCommunity for Google Universal Analytics on page 66.

> When you enable site tracking on your website, the program generates URL information that Google *Universal Analytics* uses to identify your web pages. These URLs are associated with your web page URLs and passed through the back end to Google *Universal Analytics*.

Note: Parts that contain multiple steps generate additional URL information so you can track website users as they navigate through the steps. For information about these URLs, see Site Tracking URL Information for Google Universal Analytics Goals on page 68.

3. To save the settings, click **Save**.

Configure Blackbaud NetCommunity for Google Universal Analytics

When you sign up for an account with Google *Universal Analytics*, you create a property for the website you want to monitor and receive a script for the service to track the website's performance. To use the service with Blackbaud NetCommunity, enable site tracking for each site you host and provide the script from the service. The program automatically adds the script you enter to each page of your website.

Note: If you host multiple websites, you can create a property for each because you enable site tracking for them separately.

This section provides information to help you configure site search tracking, goals, and E-commerce with Google *Universal Analytics*. Although the program supports the previous Google *Analytics* version of the service, we recommend you upgrade to *Universal Analytics* to use the latest features. For information about how to upgrade to *Universal Analytics*, refer to Google Universal Analytics.

❯ Configure visitor tracking for Google Universal Analytics

If you use Google *Universal Analytics* reports to track website user behavior such as search patterns, you can add code to the script you receive from Google *Universal Analytics* to monitor whether users

are logged into the website or visiting when they perform searches. Add the code to the script you entered when you enabled tracking in Blackbaud NetCommunity so the program includes the additional tracking requirements on each page of your website.

Note: Search metrics are pulled from the Search and Quick Search parts in Blackbaud NetCommunity.

1. From your Google *Universal Analytics* account, create a custom dimension to track logged in users for the property that corresponds to your Blackbaud NetCommunity website. A custom dimension is a way to send custom data to Google *Universal Analytics* so you can view the information in reports. For detailed information about custom dimensions, refer to the Google *Universal Analytics* help documentation.

2. Open Blackbaud NetCommunity. On the Administration page, select **Sites & settings**.

3. Select the site to configure and then select the Settings tab.

4. In the **Site Tracking Script** box, add this section of code to the Google *Universal Analytics* script you entered when you enabled site tracking for the website. Add the code below the information in the field before </script>. For information about how to enable site tracking, see .

Note: When you enter the code, use the name you entered for your custom dimension for <replace with custom dimension name>.

```
if (LOGGEDIN) {

    ga('set', '<replace with custom dimension name>', LOGGEDIN);

} else {

    ga('set', '<replace with custom dimension name>', 'Visitor');

}
```

The combined script should look similar to the one below. Your version should include the account ID provided by Google *Universal Analytics* in place of UA-XXXXXXXX-Y. Also, if you are testing your website locally, replace ga('create', 'UA-XXXXXX-Y', 'auto'); with ga('create', 'UA-XXXXXX-Y', {'cookieDomain': 'none'});.

```
<script type="text/javascript">

    (function (i, s, o, g, r, a, m) {

        i['GoogleAnalyticsObject'] = r; i[r] = i[r] || function () {

            (i[r].q = i[r].q || []).push(arguments)

        }, i[r].l = 1 * new Date(); a = s.createElement(o),

        m = s.getElementsByTagName(o)[0]; a.async = 1; a.src = g;
m.parentNode.insertBefore(a, m)

    })(window, document, 'script', '//www.google-
analytics.com/analytics.js', 'ga');

    ga('create', 'UA-XXXXXXXX-Y', 'auto');
```

```
     ga('send', 'pageview');

  if (LOGGEDIN) {

     ga('set', '<replace with custom dimension name>', LOGGEDIN);

  } else {

     ga('set', '<replace with custom dimension name>', 'Visitor');

  }

  </script>
```

5. To save the settings, click **Save**.

Site Tracking URL Information for Google Universal Analytics Goals

To use certain types of Google *Universal Analytics* conversion tracking tools such as destination goals and funnels, you must enter URL information from Blackbaud NetCommunitywhen you configure them. The program generates these URLs when you enable site tracking on your website and passes them through the back end to Google *Universal Analytics*. The site tracking URLs include the website URL and page name. For example, http://www.yourdomain.org/Page.aspx&part_[part ID]&pagename&pid= [page ID].

The following information provides the URL information for parts that contain multiple steps a website user navigates through on your website. For example, the Donation Form part may generate http://www.yourdomain.org/Page.aspx&DonationStep_[part ID]=DonationStep_ Acknowledgement&pagename=My+Donation+Form&pid=[page ID].

> *Note:* For information about how to configure conversion tracking tools, refer to the Google *Universal Analytics* help documentation.

*   **Donation Form**: Generates an associated URL that contains "DonationStep_Checkout" or "DonationStep_Acknowledgement." A URL that contains "DonationStep_Acknowledgement" indicates a completed donation. If your website contains multiple Donation Form parts, you can identify an individual part when "DonationStep_[part ID]" appears before the part step information in the URL. For example, "DonationStep_[part ID]=DonationStep_Acknowledgement."

> *Note:* To use the examples in this section, replace "[part ID]" and "[page ID]" with the actual number for the part ID and page ID. To obtain a part ID, open the part. On the Properties tab, the ID appears in the **Part ID** field. To obtain a page ID, select the page in *Pages & templates*. On the Properties tab, the ID appears in the **Page ID** row.

Associated URL example for a donation web page:
http://www.yourdomain.org/Page.aspx&DonationStep_[part ID]=DonationStep_ Checkout&pagename=My+Donation+Form&pid=[page ID]

- **eCard**: Generates an associated URL that contains "pnlStepConfirm," "pnlStepPersonalize," "pnlStepPreview," "pnlStepCaptcha," "pnlStepFinish," or "pnlStepDonation." A URL that contains "pnlStepDonation" indicates a completed eCard. If your website contains multiple eCard parts, you can identify an individual part when "eCardStep_[part ID]" appears before the part step information in the URL. For example, "eCardStep_[part ID]=pnlStepPreview."

Associated URL for an eCard web page: http://www.yourdomain.org/Page.aspx&eCardStep=[part ID]=pnlStepPersonalize&pagename=eCards&pid=[page ID]
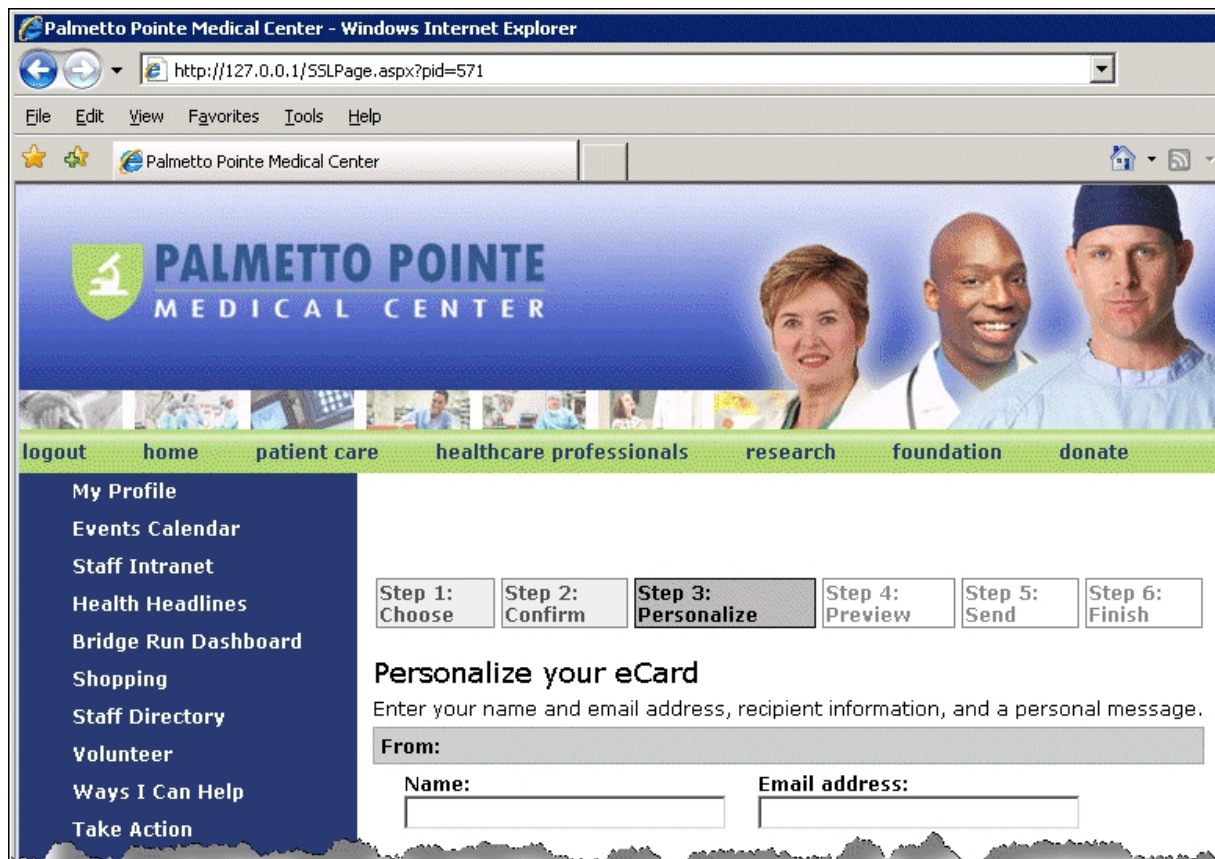
- **Event Registration Form**: Generates an associated URL that contains "Event," "Prices," "Attendees," "RegisterNow," or "Acknowledgement." A URL that contains "Acknowledgement" indicates a completed event registration. If your website contains multiple Event Registration Form parts, you can identify an individual part when "EventStep_[part ID]" appears before the part step information in the URL. For example, "EventStep_[part ID]=Prices."

Associated URL for an event registration web page:
http://www.yourdomain.org/Page.aspx&EventStep_[part
ID]=Attendees&pagename=Event+Registration&pid=[page ID]
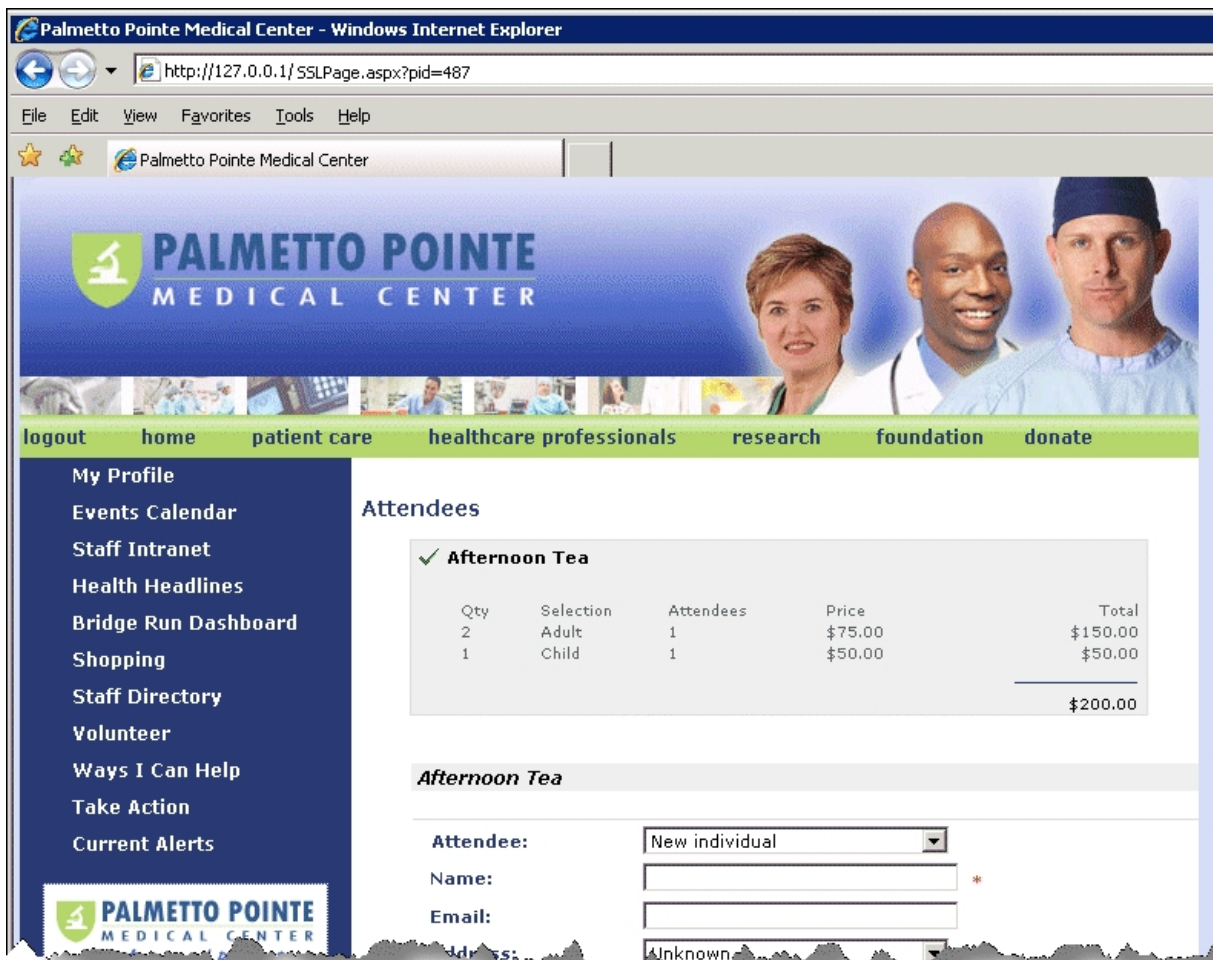
- **Membership Form**: Generates an associated URL that contains "Current," "Transaction," "Cards," "Pay," or "Acknowledgement." A URL that contains "Acknowledgement" indicates a completed membership transaction. If your website contains multiple Membership Form parts, you can identify an individual part when "MembershipStep_[part ID]" appears before the part step information in the URL. For example, "MembershipStep_[part ID]=Transaction."

Associated URL for a membership web page:
http://www.yourdomain.org/Page.aspx&MembershipStep_[part ID]=Transaction&pagename=Membership+Programs&pid=[page ID]

› Configure E-Commerce tracking for Google Universal Analytics

If you use Google *Universal Analytics* reports to track E-Commerce conversions,you must configure Blackbaud NetCommunity to provide the service with purchase information. You can track and report on revenue transactions made on pages that contain these part types: Donation Form, Membership Form, Event Registration Form, and Payment 2.0.

First you add code to the script you receive from Google *Universal Analytics* to monitor whether users complete E-Commerce purchases. Add the code to the script you entered when you enabled tracking in Blackbaud NetCommunity so the program includes the additional tracking requirements on each page of your website. Next, use an Unformatted Text part to add another script to pages that include transaction part types. The additional script is necessary because transactions are processed separately from the website by a secure payment processing service. The script receives transaction information from the processing service during the confirmation step and forwards the purchase details to Google *Universal Analytics*.

1. Open Blackbaud NetCommunity. On the Administration page, select **Sites & settings**.

2. Select the site to configure and then select the Settings tab.

3. In the **Site Tracking Script** box, add this section of code to the Google *Universal Analytics* script you entered when you enabled site tracking for the website. Add the code below the information in the field before </script>. For information about how to enable site tracking, see <u>Site tracking settings on page 65</u>.

```
ga('require', 'ecommerce');
```

The combined script should look similar to the one below. Your version should include the account ID provided by Google *Universal Analytics* in place of UA-XXXXXXXX-Y. Also, if you are testing your website locally, replace ga('create', 'UA-XXXXXX-Y', 'auto'); with ga('create', 'UA-XXXXXX-Y', {'cookieDomain': 'none'});.

```
<script type="text/javascript">

    (function (i, s, o, g, r, a, m) {

        i['GoogleAnalyticsObject'] = r; i[r] = i[r] || function () {

            (i[r].q = i[r].q || []).push(arguments)

        }, i[r].l = 1 * new Date(); a = s.createElement(o),

        m = s.getElementsByTagName(o)[0]; a.async = 1; a.src = g;
m.parentNode.insertBefore(a, m)

    })(window, document, 'script', '//www.google-
analytics.com/analytics.js', 'ga');

    ga('create', 'UA-XXXXXXXX-Y', 'auto');

    ga('send', 'pageview');

    ga('require', 'ecommerce');

</script>
```

4. Open Blackbaud NetCommunity. From *Parts*, create a new Unformatted Text part. For information about how to create an Unformatted Text part, refer to the *Parts Guide*.

5. In the box, enter the script below and then click **Save**.

```
<script type="text/javascript">

    BLACKBAUD.netcommunity.api.DonationConfirmation.add(function
(data) {

        if (data.TransTotal) {

            ga('ecommerce:addTransaction', {

                'id': data.TransID,

                'affiliation': '',

                'revenue': data.TransTotal,

                'shipping': '',
```

```
            'tax': ''

        });

        for (var i = 0; i < data.Items.length; i++) {

            ga('ecommerce:addItem', {

                'id': data.Items[i].ID,

                'name': data.Items[i].Name,

                'sku': data.Items[i].SKU,

                'category': data.Items[i].Name,

                'price': data.Items[i].Price,

                'quantity': data.Items[i].Quantity

            });

        }

        ga('ecommerce:send');

        ga('ecommerce:clear');

    }

    });

</script>
```

Warning: This code applies to standard Blackbaud NetCommunity transactions. If your site processes custom transaction data, please contact Blackbaud Professional Services or a developer who is familiar with the Google Universal Analytics API to configure the E-Commerce code. This code is also provided as an example from Google *Universal Analytics* and may not be the most recent version. To ensure that you have the correct code, refer to Google Universal Analytics.

6. Select **Show advanced options**.

7. In the **Placement in HTML** field, select "At the end of the <body> tag."

8. Place the Unformatted Text part on any page that includes one of these part types: Donation Form, Membership Form, Event Registration Form, and Payment 2.0. The script you entered in the Unformatted Text part sends tracking information to Google *Universal Analytics* about transactions made on those pages. The tracking information includes:

Data ID in Google Analytics	Description of data type
data.TransTotal	Total dollar amount for the transaction.

Data ID in Google Analytics	Description of data type
data.TransID	Identifies the transaction.
data.Items	Items included in the transaction. If the transaction contains multiple items (for example, a transaction from a Payment 2.0 part may include several purchased items), the items are identified as data.Item[0], data.Item[1], data.Item[2], etc.
data.Items.ID:	Associates an item with a transaction. This is the same value as the TransID.
data.Items.SKU	Unique SKU used to track the price and quantity of an item.
data.Items.Name	Human readable name for an item.
data.Items.Price	Price of an item.
data.Items.Quantity	Number of items purchased of the same type.

> reCAPTCHA settings

To help prevent automated abuse of your website, the program uses a completely automated public turing test to tell computers and humans apart (CAPTCHA). With CAPTCHA functionality, the program can ensure a user is not an automated program to generate spam or phish for payment information. To verify the website user is a person, the website program displays a checkbox labeled "I'm not a robot." To send an email message through the website, such as through an eCards part, the user must click the checkbox. Under **reCAPTCHA**, you can select whether to also use CAPTCHA on all parts that process credit card or direct debit payments, such as the Donation Form and Event Registration Form parts.

Note: In cases where the program cannot confidently predict whether a user is a human or an abusive agent, it will display an additional test to confirm the user is valid. For example, the CAPTCHA may display multiple images and ask the user to identify which images match a particular description.

1. Under **reCAPTCHA**, enter the public and private keys you receive when you sign up for *reCAPTCHA*. The program uses this information to access your installation of *reCAPTCHA*. For additional security, the program masks the entry in the **Private key** field.

reCAPTCHA provides free CAPTCHA functionality for your website. For accessibility, *reCAPTCHA* also provides an audio CAPTCHA for visually impaired website users. To use CAPTCHA functionality on your website, you must install *reCAPTCHA* and configure the installation. To obtain **reCAPTCHA**, go to http://www.google.com/recaptcha. When you sign up for *reCAPTCHA*, you receive the public and private keys.

2. Select where to use *reCAPTCHA* on your website.

    • By default, the program selects **Non-donation eCards**. You cannot clear this option because these parts leave your website vulnerable to automated abuse without CAPTCHA. If you create eCard parts before you install reCAPTCHA and enter the private and public keys, a warning message appears.

    • To use CAPTCHA on parts that process payments for users who did not log in to your website and users who log in but are not yet linked to constituent records in your database, select **Anonymous and provisional users when processing a payment**.

    • To use CAPTCHA on parts that process payments for users who log in to your website and are linked to constituent records in your database, select **Non-provisional authenticated users when processing a payment**.

    • To use CAPTCHA on the new user registration form, select **New user registrations**.

Note: The *reCAPTCHA* usage options you select control all Blackbaud NetCommunity parts except those using the Blackbaud Secure Payments form, which is controlled by the settings on each applicable part.

3. To save the settings, click **Save**.

Single sign-on authentication settings

If your website contains web pages that integrate with software programs other than Blackbaud NetCommunity, you can use single sign-on so users do not have to enter different logins on the Blackbaud NetCommunity pages. With incoming single sign-on, users click a unique link from a non-Blackbaud NetCommunity page to access Blackbaud NetCommunity secured pages without entering user name and password information. Under **Enable single sign-on authentication**, select whether to enable single sign-on authentication to allow users transparent access to secured pages. When you do this, single sign-on systems for non-Blackbaud NetCommunity pages authenticate users with a shared key and time algorithm in a querystring, such as &u=Supervisor&t=151256232434&m=282FE2ECF98F5FFEDAAB12A38F3A3D54.

1. To enable single sign-on for your website, select **Enable single sign-on authentication**. When you select this checkbox, the grid enables.

Note: Integration of your website with a third-party single sign-on system requires additional custom programming. For information about the code necessary to integrate with a single sign-on system, consult your single sign-on system provider.

Single Sign-on Authentication

☑ Enable Single Sign-on Authentication

To add an SSO entry enter the data in the row above and click "Add New" at the bottom right.

	Description	Shared Key	UserName Querystring	Time Querystring	MD5 Hash Querystring	Expiration (seconds)	Include IP	Require SSL	
Edit	Default	5CCCE206-5609-448	u	t	m	300	☑	☑	
			u	t	m	300	☐	☐	Add New

2. In the grid, enter the information to use with the single sign-on system.

Warning: With incoming single sign-on, users can log in to a non-Blackbaud NetCommunity page and gain access to a Blackbaud NetCommunity page but they cannot log in to a Blackbaud NetCommunity page and gain access to a non-Blackbaud NetCommunity page. To set up outgoing single sign-on to allow users to navigate from Blackbaud NetCommunity to a third-party site without entering their credentials for the third-party site, see API on page 57.

a. Under **Description**, enter a unique name to identify the single sign-on instance.

b. Under **Shared key**, enter a string value key used by the single sign-on system to access your website. We recommend a combination of letters and numbers.

c. The Querystring columns contain the three variable parameters that other single sign-on systems pass via the URL.

Under **UserName querystring** enter the plain text variable that identifies the user name in the querystring generated by the single sign-on system.

Under **Time querystring** enter the variable that indicates the timestamp in the querystring generated by the single sign-on system. The timestamp is in epochtime when the URL was created. Epochtime is the number of seconds since January 1, 1970.

Under **MD5 hash querystring** enter the variable that indicates the MD5 hash value in the query string generated by the single sign-on system.

Note: The single sign-on system uses this information to generate a message digest (MD5) algorithm hash value in a querystring for security. If you select **Include IP**, the MD5 hash value has a format of "shared key + user name + client IP + time," where the client IP is the IP address of the website user. If you do not select **Include IP**, the MD5 hash value has a format of "shared key + user name + time."

d. In the **Expiration (seconds)** column, enter for how long after the timestamp generated in the querystring the user has transparent access to the web page. By default, the single sign-on authentication expires after 300 seconds (5 minutes).

e. If the single sign-on system uses the client IP address as additional security, select the checkbox in the **Include IP** column. This optional feature provides additional security by ensuring that the single sign-on link is only valid for a specific user's IP address.

f. To require encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for additional security, select the checkbox in the **Require encryption** column. When you select this, pages require URLs that begin with "https."

g.   If you maintain multiple third-party web pages on your site, click **Add New** to add additional single sign-on entries. For security purposes, we recommend a separate entry for each third-party integration.

3.   To edit an existing single sign-on entry, click **Edit** and update the information as necessary.

4.   To delete an existing single sign-on entry, click **Delete**. At the message to confirm the deletion of the row, click **Yes**.

5.   To save the settings, click **Save**.

Workflows

In *Workflows*, you create and manage the content approval workflows for Formatted Text and Images and Formatted Text and Images (Secured) parts on your website. With a workflow, users in specific roles must approve the content of a part before it appears on your website. When you create a workflow, you select whether it is the default workflow for the selected part type and designate users who can approve content. To access *Workflows*, from *Administration*, click **Workflows**.

Note: When you design a Formatted Text and Images or Formatted Text and Images (Secured) part, you select its workflow on the Content Approval tab. On the Content Approval tab, you also select the approval status for the part: "Draft" or "Ready for Approval." To display the content on your website, users with approval rights can select an approval status of "Publish." For more information about the Content Approval tab, see the *Parts Guide*.

> ### Create a workflow

When you create a workflow, you assign approval rights to users by role. Before you create a workflow, you must associate roles and task rights in *Security assignments* for users to approve content. For example, you can assign users to approval roles based on the type on the content of the parts they review. You can also select whether a role has all workflow related rights or only limited rights. For more information, see the *Users & Security Guide*.

1.   From *Administration*, click **Workflows**. *Workflows* appears.

2.   Click **New workflow**. The New Workflow screen appears.

New Workflow

| Properties | Notifications |

Name: [   ] *

Description:
[   ]

Part Type: [Formatted Text and Images ▼]

Default for this Part Type: ☐

Approval Roles:

Role	Can Approve
Members	☐
Content Authors	☐
Everyone	☐
Content Authors	☐
Participant	☐
Site Administrators	☐

3. In the **Name** field, enter a unique name for your workflow so users with rights to manage workflows can quickly identify the workflow in *Workflows* and when they create Formatted Text and Images parts.

4. In the **Description** box, enter more information to help identify the workflow, such as an explanation of when to apply this workflow to a part.

5. In the **Part Type** field, select whether the workflow applies to a Formatted Text and Images part or a Formatted Text and Images (Secured) part.

6. To make the workflow the default for the selected part type, select **Default for this Part Type**. When you select this checkbox, the workflow appears with an asterisk (*) when users select the workflow for parts of the type selected in the **Part Type** field.

7. In the **Approval Roles** grid, assign Can Approve security rights for each role. To designate the approval role to a user's role, select its checkbox.

8. Click **Save**. You return to *Workflows*.

Note: After you save a new workflow, we recommend you assign its part approval notifications. Part approval notifications alert the users who create or approve a part that uses the workflow when the approval status changes. To assign notifications to a workflow, you can edit the workflow or notification. For more information about notifications, see the *Email Guide*.

❯ Edit a workflow

1. From *Administration*, click **Workflows**. *Workflows* appears.

2. In the **Filter by Name** field, enter the complete or partial name of the workflow to edit.

3. Click **Filter**. The grid displays all workflows that meet the name criteria entered.

4. Under **Action**, click **Click here to edit this workflow**. The workflow appears.

5. To adjust the properties of the workflow, select the Properties tab. On this tab, adjust the name or description of the workflow, its selected part type, whether it's the default for the selected part type, and the users designated as the approval role.

6. To view or manage the notifications used with the workflow, select the Notifications tab. On the tab, the grid displays the part approval notifications in your database.

In the grid, the **Active for this Workflow** column indicates whether the workflow uses a notification. To edit a notification, such as to apply it to the workflow, click **Edit**. The notification appears. Under **Workflows**, select the workflows that use the notification. To return to the workflow, click **Save**.

To add a notification to the database, such as to create it for the workflow, click **Create New Notification**. The Select Notification Type screen appears so you can select the type of notification to create.

Warning: To create notifications for a workflow in Mozilla *Firefox*, you must first disable the pop-up window block. In *Firefox*, select **Tools**, **Options** from the menu bar. On the Options screen, select the Content tab and click **Exceptions** next to the **Block pop-up windows** checkbox. On the Allowed Sites screen, enter the addresses of the websites to allow pop-up windows and click **Close**. To return to the Notifications tab, click **OK**.

To customize the notifications based on the part and its approval status, add merge fields. To display the list of available merge fields, click **Merge fields** on the Insert tab in the toolbar. To expand the list, click the plus sign next to **General**. For information about the merge fields that appear when you design a notification for a workflow, see Part Approval Notification Merge Fields on page 83.

For information about how to edit and create notifications, see the Notifications section of the *Email Guide*.

7. To view the parts that are under construction or require approval in the workflow, select the Approvals tab. On this tab, the grid displays all parts that use the workflow and are not yet published on the website. In the grid, view the name, approval status, and most recent update activity of each part. For information about the approval status, see Workflow Approval Status on page 82.

- To adjust the approval status of a part, such as to approve and publish its content on your website, click **Click here to set the approval status for this version** in the **Action** column. The part appears and opens to the Content Approval tab.

  For information about how to adjust the approval status from the Content Approval tab, see the *Parts Guide*.

- To send an email message to the person who most recently updated the approval status of the part, such as to discuss a Pending part with its author before you approve the content, click **Click here to send email** in the **Status Updated By** column.

Note: You can also view the parts that are under construction or require approval in a workflow from *Approvals*. In *Approvals*, you can view all draft and pending parts for all workflows or for a specific workflow. You can also access a draft or pending part, such as to adjust its approval status. For more information about *Approvals*, see the Approvals chapter of the *Website Design Guide*.

8. Click **Save**. You return to *Workflows*.

Workflow Approval Status

Workflows provide an approval process for the parts program users create for your website. With a workflow, users in the approval role must review and approve the content on all new and revised Formatted Text and Images and Formatted Text and Images (Secured) parts before they appear on your website. You can view the approval status of a part from its Content Approval tab. On the Approvals tab of a workflow, you can view the parts associated with the workflow and their approval statuses.

Note: In *Approvals*, you can view and access all parts with an approval status of "Draft" or "Pending."

- **Draft** – An approval status of "Draft" indicates that a content author created the part but did not yet submit it for approval, such as when the user has not yet finished its design. "Draft" is the default approval status for newly created or updated Formatted Text and Images or Formatted Text and Images (Secured) parts.

- **Pending** – An approval status of "Pending" indicates that a content author designed the part and selected an approval status of "Ready for Approval" on the Content Approval tab of the part, but a user with Content Approval rights has not yet approved its content. If you create a Part Approval – Ready for Approval notification for the workflow, users with Content Approval rights receive a notification to alert them when the content author adjusts the status to "Ready for Approval."

- **Published** – An approval status of "Published" indicates that a user with Content Approval rights reviewed and approved the part, and its content appears on your website. To publish a part's content on the website, the user with Content Approval rights selects an approval status of "Publish" on the Content Approval tab of the part. If you create a Part Approval – Published notification for the workflow, the content author receives a notification when the user with Content Approval rights adjusts the status to "Published."

- **Rejected** – An approval status of "Rejected" indicates that a user with Content Approval rights reviewed the part but did not approve its content. When a user rejects a part, the program generates a new version of the part with an approval status of "Draft." If you create a Part Approval – Rejected notification for the workflow, the content author receives a notification when the user with Content Approval rights adjusts the status to "Rejected."

- **Archived** – An approval status of "Archived" indicates that a user revised a published part. When a content author updates a published part, the program automatically creates an archived copy of the original version and assigns it a status of "Archived." From the Content Approval tab of a part, users with Content Approval rights can restore its content to an earlier, archived version.

Part Approval Notification Merge Fields

When you design part approval notifications in *Notifications*, use merge fields to customize the notification sent with information specific to the part and its approval status. To display the list of available merge fields, click **Merge fields** on the Insert tab in the toolbar of the Email Template tab. To expand a list, click the plus sign next to **General**. The merge fields specific to workflows and part approval appear.

- **Part Name** – To display the name of the part that the notification applies to, add this merge field. For example, add "Part: <Part Name>."

- **Status** – To display the current status of the part, add this merge field. For example, add "Part <Part Name> now has a status of <Status>."

- **Status Updated By** – To display the name of the content author or user with Content Approval rights who updated the status of the part and generated the notification, add this merge field. For example, add "<Status Updated By> updated the status of part <Part Name> to <Status>."

- **Approvals Gallery Hyperlink** – To include a link to *Approvals* so the recipient can quickly view or update the part as necessary, add this merge field. For example, add "To view part <Part Name> and its content: <Approvals Gallery Hyperlink>."

Merchant Accounts

In *Merchant Accounts*, you set up merchant accounts to process payments through parts and forms. On each part or form that processes payments, you select a merchant account.

Note: Only users with Supervisor rights can view, create, and manage *Merchant accounts*. When you host multiple sites, you can create a merchant account for an individual site. For more information, seeMerchant Account Security on page 84.

To view the parts and forms that use merchant accounts, select the Merchant accounts usage tab. To access parts and forms, go to *Site explorer*.

To process credit card transactions, the program supports merchant accounts from multiple credit card processors available through the *Blackbaud Payment Service*, including *Blackbaud Merchant Services*, Authorize.Net; BeanStream; International Automated Transactions Service (IATS); Moneris Solutions; Payflow Pro, owned by PayPal (formerly Verisign); and Verus Card Services, owned by Sage Payment Solutions.

Warning: PayPal has acquired Verisign. If your organization has a Verisign account, PayPal may contact you to convert to a Payflow Pro account. To ensure the program continues to manage your credit card transactions smoothly, please contact Blackbaud support when you convert to Payflow Pro.

Merchant Account Security

Only users with Supervisor rights can view, create, and manage *Merchant accounts*. When you host multiple sites, you can create merchant accounts for individual sites. To do this, log in to the site and create the merchant account. For more information, see Go to Site on page 20.

To apply site security to a merchant account, select the task right **Use merchant account rights** for site task groups associated with the site. This right provides users with the ability to select merchant accounts for parts and forms. A Supervisor user can select an account from any site for parts and forms.

Note: To use a merchant account for more than one site or all sites, make sure this task right is selected for the site the merchant account was created in.

For information about task rights, task groups, and security assignments, see the *Users & Security Guide*.

❯ Configure a merchant account

1. In *Administration*, click Merchant Accounts. *Merchant Accounts* appears.

2. Select the Merchant accounts tab.

3. Click **New merchant account**. The New Merchant Account screen appears.

New Merchant Account (New merchant account)

💾 Save   ❓ Help   ↻ Return

Merchant Account Details

Name: PayPal Payflow Pro   *

☐ Merchant account is inactive

Process mode: Live

Description: PayPal account for US transactions

Gateway Account Details

Gateway: Payflow Pro

Currency:

Gateway ID: *

Password: *

Confirm Password: *

AVS Level: Full

CSC Level: Full

☐ Use 3DS processing

Supported Credit Cards:

Enable	Card	Processor
☑	American Express	American Express Brighton
☑	Diner's Club	Global Payments Central
☑	Discover	EDS Aurora
☑	JCB	EDS Aurora
☑	Mastercard	EDS Aurora
☑	Visa	EDS Aurora

Additional Fields:

Field	Value	
Partner	Blackbaud	*
User		

4. Under **Merchant Account Details**, in the **Name** field, enter a unique name for the merchant account.

Note: To support multiple currencies, you must add a merchant account for each currency you process. To differentiate between accounts, we recommend you include the currency type in the name of the merchant account, such as "IATS account for Canadian dollars."

5. To set up the merchant account but not make it available for use on a donation part, select **Merchant account is inactive**.

6. In the **Process mode** field, select whether to use the merchant account to process transactions or for another purpose.

   • To use the merchant account to process transactions, select "Live."

   • To use the merchant account to test the connection with the gateway, if the gateway selected for the merchant account supports a test mode, select "Test."

Note: For details about credit card test and demo information, see Credit Card Information for Demo and Test Mode on page 89.

   • To use the merchant account for internal use only and not send data to the gateway, select "Demo."

7. In the **Description** field, enter a description to help identify the merchant account. For example, explain the types of donation parts to use the merchant account.

   When you host multiple sites and edit a merchant account, the **Assign to site** field appears so you can move an account from its current site to another site. If the account is in use on the source site, it continues to be on that site. However, the account is now associated with the target site and its security.

8. Under **Gateway Account Details**, in the **Gateway** field, select the credit card gateway to use with the merchant account.

9. In the **Currency** field, select the currency to use with the merchant account.

Note: To support multiple currencies, add a merchant account for each currency you process. Your merchant account settings are the same, except for the information you enter in the **Currency**, **Name**, and **Description** fields.

10. When you set up an account with the gateway, you receive a vendor login ID and password. In the **Gateway ID** field, enter your vendor ID.

11. In the **Password** and **Confirm Password** fields, enter your password. Regardless of the characters you enter, only bullets appear in these fields.

12. In the **AVS Level** field, select whether to use the Address Verification Service (AVS) with the merchant account and at what level. For example, you may select to use AVS to process Card Not Present transactions.

Note: The AVS is fraud protection that verifies customer billing addresses submitted through online payment transactions. With AVS, the gateway issues a transaction to authorize the payment. In response, the gateway receives information about the payment, including whether the numeric portion of the street address and Zip code are correct. Depending on the AVS level selected for the merchant account, the gateway uses this information to determine whether to accept the payment. The program performs this service only when the selected gateway supports AVS for the country of the transaction. For information about AVS support, contact your gateway.

- Full: To accept transactions only when both the street address and Zip code match, select this option.

- Medium: To accept transactions when either the street address or Zip code match, select this option. We recommend you select this option.

- Light: To deny transactions only when neither the street address nor the Zip code match, select this option. This level may accept transactions when either the street address or Zip code returns no response, regardless of whether the other criteria matches.

- None: To perform no address verification, select this option.

    For more information about how the program uses AVS to protect your account from fraudulent credit card activity, see Address Verification Service (AVS) on page 88.

13. If the gateway checks the Card Security Code (CSC) to protect against fraud, the **CSC Level** field is enabled. Select whether to use CSC checks. The Card Security Code, or Card Verification Value (CVV2), appears only on the credit card and not on receipts or statements.

    - To perform no CSC check, select "None."
    - To accept transactions only when the CSC matches, select "Full."
    - To decline transactions only when the CSC does not match, select "Light."

    For more information about how the program uses a CSC check to protect your account from fraudulent credit card activity, see Card Security Code (CSC) Check on page 88.

14. To indicate whether to use Three-Domain Secure (3DS) authentication for Card Not Present transactions when using a payment processer that supports 3DS, select **Use 3DS processing**.

Tip: Developed by major credit card providers, 3DS authentication is an additional security layer for online transactions. 3DS requires a cardholder to register the credit card through the card issuer's website and specify credentials used to verify online transactions. Examples of 3DS authentication include *Verified by Visa* and *MasterCard SecureCode*.

15. Under **Supported Credit Cards**, the credit cards that the selected gateway can process appear. Select the checkboxes for the types of credit cards available for transactions on your website. For each credit card type you select, in the **Processor** column, select the credit card processor to handle transactions of the card type.

Note: Credit card processors vary in support for AVS and CSC. Before you activate your website, check with the gateway for the latest information. For information about whether and how processors use a CSC check to protect your account from fraudulent credit card activity, see Card Security Code (CSC) Check on page 88.

16. If the selected gateway requires additional information, the **Additional Fields** grid appears. In the Value column, enter the information required by the gateway. For example, Payflow Pro requires a **Partner** field so you can enter your organization's Payflow Pro partner.

17. Click **Save**. You return to *Merchant Accounts*. To ensure the secure processing of credit card transactions, the program automatically sends your merchant account information to the *Blackbaud Payment Service*.

Address Verification Service (AVS)

When you set up a Moneris or PayPal merchant account in *Administration*, you select the level of its Address Verification Service (AVS). AVS is fraud protection to verify customer billing addresses submitted through online payment transactions. If you select "Full," "Medium," or "Light," the program uses AVS to process transactions through your merchant account.

With AVS, the gateway issues a transaction to authorize the payment. An authorization transaction only puts a hold on the credit card account for the transaction amount. No charges are applied to the card. If the program does not post a follow-up transaction within a few hours, the authorization transaction expires.

In response to the authorization transaction, Moneris or PayPal returns information about the payment, including whether the bank supports AVS and whether two AVS fields – AVSADDR (numeric portion of the street address) and AVSZIP (Zip code) – are correct. Depending on the AVS level selected for the merchant account, the program uses this information to determine whether to accept the payment transaction.

Note: The program performs this service only when the selected gateway supports AVS for the country of the transaction. For information about this AVS support, contact your gateway.

- Full: To accept transactions only when both the street address and Zip code match, select this option.

- Medium: To accept transactions when either the street address or Zip code match, select this option. We recommend you select this option.

- Light: To deny transactions only when neither the street address nor the Zip code match, select this option. This level may accept transactions when either the street address or Zip code returns no response, regardless of whether the other criteria matches.

- None: To perform no address verification, select this option.

Depending on whether the transaction passes AVS, the program then uses the PNREF value received from the authorization transaction to issue a follow-up transaction.

- If the transaction passes AVS, the program issues a "Delayed Capture" transaction. The delayed capture transaction issues the charge against the credit card.

- If the transaction fails AVS, the program issues a "Void" transaction. The void transaction removes the hold from the credit card, but does not issue a charge against the card.

Tip: If only authorization (AUTH) transactions appear for a specific date in reports, rerun the reports for that date. In the Select Reports Filters section of the Custom Report Template, select at least "Authorization," "Delayed Capture," and "Void" as transaction types. We recommend you also include both "Approvals" and "Declines." In the output field list, include "AVS Street Match" and "AVS ZIP Match."

Card Security Code (CSC) Check

When you set up a Moneris or PayPal merchant account in *Administration*, you select the level of its Card Security Code (CSC) check. CSC is fraud protection to verify the card security code, called the

Card Verification Value (CVV2). The CSC appears only on the credit card itself, and not on receipts or statements. If you select "Full" or "Light," the program use a CSC check to process transactions through your merchant account.

When you set up a PayPal merchant account, you also select the types of credit cards available for transactions on your website through your Internet merchant account and the processor to handle transactions of each credit card type. Regardless of the CSC setting on your merchant account, not all processors support CSC checks for all credit card types. Depending on the processor you select, PayPal may not be able to perform a CSC check for all transactions.

Note: None of the processors available in the program support CSC checks on JCB, Diner's Card, CarteB, Enroute, or Switch/Solo credit cards.

- American Express supports CSC checks on only American Express credit cards.

- EDS and Norwest do not support CSC checks on any credit card types.

- FDMS Nashville supports CSC checks on only MasterCard and Visa credit cards.

- FDMS South and PaymenTech support CSC checks on only American Express, MasterCard, and Visa credit cards.

- Nova and Global Central support CSC checks on only Discover, MasterCard, and Visa credit cards.

- Vital, Global East, FDMS North, and Wells Fargo support CSC checks on American Express, Discover, MasterCard, and Visa credit cards.

Credit Card Information for Demo and Test Mode

To use a merchant account to test the connection with the gateway, you select "Test" in the **Process mode** field when you configure the merchant account. To use the merchant account for internal use only and not send data to the gateway, you select "Demo."

Review the following table for credit card information to use in Test and Demo modes. The table includes credit card type and credit card numbers. You can enter any future date for the expiration dates and any three-digit number for Card Security Codes (CSC).

Note: All credit card numbers work in Demo mode. However, a subset of these credit card numbers do not work in Test mode for the gateways that support them. The credit cards that do not work are not known because gateway support varies.

Credit card type	Credit card number
American Express	378282246310005
American Express	371449635398431
American Express	378734493671000
American Express	373599005095005
Diners Club	30569309025904

Credit card type	Credit card number
Diners Club	38520000023237
Diners Club	36462462742008
Discover	6011111111111117
Discover	6011000990139424
JCB	3530111333300000
JCB	3566002020360505
MasterCard	5555555555554444
MasterCard	5105105105105100
MasterCard	5454545454545454
Visa	4111111111111111
Visa	4012888888881881
Visa	4222222222222
Visa	4242424242424242
enRoute	201400000000009
Laser	630495060000000000
Maestro	6759015050123445
Solo	6334960300099354
Solo	6334900000000005
Switch	4911001999992348
Visa Electron	4917300000000008
Visa Electron	4508750000000009

Field Options

In *Field Options*, you can set default privacy settings for profile fields. Privacy settings determine the profile fields that are visible to other members of the community. If a field is public, all website users can view it. If a field is private, only the individual website user can view it.

Warning: We recommend only website administrators or users with Supervisor rights access *Field options*.

Users can set privacy settings for their profile information in the Profile Form part. The user's settings overwrite the default privacy settings in *Field options*. For example, Home Phone may be marked

Public By Default in *Field options*, but users can make their phone numbers private on the Profile Form part.

> ### Set privacy defaults for profile fields

1. From *Administration*, click **Field options**. *Field options* appears and lists the profile fields.

2. By default, all fields are public. To make a profile field private by default, clear its checkbox in the **Public by Default** column.

Warning: After you process users and they visit the profile form, the program locks in your current default privacy settings. It is important to carefully consider your decision for each field because you cannot manually or globally change a privacy setting for existing profiles. You can still change privacy settings for profile fields on the Field options screen, but future changes do not affect existing profiles.

3. Click **Save**.

Custom Parts

In *Administration*, *Custom parts*, you can create a new custom content part type or link to an existing framework part type. After you create or link to the part type, it is available for selection in *Parts*.

Note: Custom parts offer additional flexibility, but come with additional complexity. If you host your own website, we strongly recommend only developers knowledgeable in all areas of customizations design them. This includes writing HTML and JavaScript code. Users without this expertise should not design these parts. If Blackbaud hosts your website, customizations can only be completed by Blackbaud or one of our designated partners. For more information, please contact your Blackbaud Account Executive.

To create a custom content part type, click **New content part**. A custom content part uses JavaScript and HTML to create the part editor and define how to display the part on a web page. You can use custom content parts to create customizations such as slideshows, tabbed content, RSS Feed readers, accordion content, pop-up boxes, and callout boxes.

To link to an existing framework part type, click **New framework part**. To build custom framework parts for your website, you should understand Blackbaud NetCommunity from a site designer's perspective and have a working technical knowledge of ASP.NET. The content for custom framework parts can come from a variety of sources and can be as simple as text or HTML stored in the Blackbaud NetCommunity database, or it can be data from the back office such as constituent giving history. For example, you can use a custom framework part to create a custom individual search form or a custom pledge form for Blackbaud NetCommunity.

| Custom parts				
➕ New content part ➕ New framework part				
Manage your custom parts by specifying the display and edit user controls for your custom parts.				
Filter by name: [ ] [Filter]				
Action	Name	Require SSL	Description	Type
✏ ✕	Main slideshow	No	Slideshow rotating pics for home page	Content
✏ ✕	News widget	No	Recent news posts	Content
2 custom parts meet selected criteria				

Code Tables

Code tables in this program are similar to those in other Blackbaud programs. In *Code tables*, you can manage a table for event categories. These code table entries are available under **Event Category** on the Event Calendar part.

You can also manage a code table for site tags. This code table contains keywords, or tags, that you can assign to parts to improve site navigation. You can select the tags in this code table on the Tags tab of the Part Editor screen. If you update a table entry, the change cascades to all pages that include a part with this tag. For example, if a Donation Form part with an "Arts" tag is included on two pages with Tag Display parts and you change "Arts" to "Visual Arts" in the site tags code table, "Visual Arts" automatically appears in the tag display for both donation pages.

Tip: Only users with Supervisor rights can view and manage *Code tables*.

> **Manage code tables**
> 1. From *Administration*, click **Code tables**. *Code tables* appears.
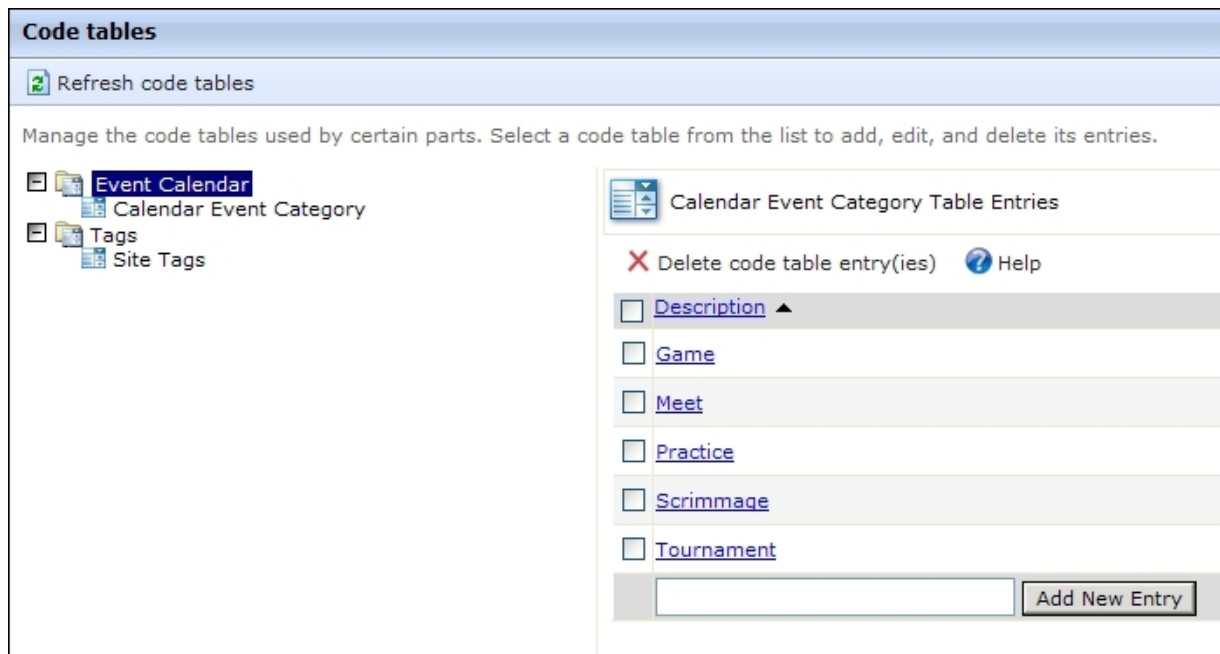
2. To update code tables from The Raiser's Edge, click **Refresh code tables**. For example, to integrate a new table or update an existing one after you add code table entries in The Raiser's Edge, click this button.

Note: The event categories code table under **Event Calendar** and the site tags code table under **Tagging** are both website specific. These code tables are not from The Raiser's Edge. In the event categories code table, you enter event categories to select on the Event Calendar part. In the site tags code table, you enter tags to assign to parts on your website to improve site navigation.

3. In the tree-view list, select a code table. In the grid, its code table entries appear.

4. To add a code table entry, enter text in the field below the grid and click **Add New Entry**. The entry appears in the grid.

5. To edit an entry, click it and update the text.

6. To delete an entry, select its checkbox and click **Delete code table entry(ies)**.

Note: Changes to tags in the Site Tags code table automatically appear throughout the program. For example, if you change an "Arts" tag to "Visual Arts," the tag appears as "Visual Arts" in tag displays as well as on the Tags tab on the Edit Part screen. If you delete a code table entry, the program removes the tag from all parts.

7. After you make your changes, you can leave *Code tables*. The program automatically saves your changes.

URL Redirects

In *URL redirects*, you can create 301 redirects to reroute traffic when website users try to access old URLs.

Tip: You add URLs that you want to redirect to your primary site URL in *Sites & settings*. For example, you can include URLs with typos or an abbreviation for your organization so that users who mistype the primary URL still reach your site. For more information about these URL redirects, see General site settings on page 58.

301 redirects are a search engine-friendly way to redirect users without losing search engine rankings for web pages. When website users attempt to access the original URLs, the program reroutes them to the new target URLs that you enter in *URL redirects*. The new target URLs allow you to preserve page ranks and maintain back links for the original URLs.

If you change URLs as part of a site redesign or other changes on your website, you can use redirects to reroute traffic from old URLs to the new URLs.

Likewise, if you migrate to Blackbaud NetCommunity from an existing website with a domain that you own, you can also create 301 redirects to route traffic from the pages of your old site to the pages of your new Blackbaud NetCommunity website.

Note: To route traffic from your old website, you must point the domain for the old website at Blackbaud NetCommunity. For example, if www.oldsite.org and www.newsite.org are both being run through Blackbaud NetCommunity, then you can set up redirects from www.oldsite.org to www.newsite.org. If www.oldsite.org is hosted somewhere else on a different server and does not run through Blackbaud NetCommunity, you cannot create redirects because incoming requests are not routed through Blackbaud NetCommunity.

> **Create a URL redirect**

1. From *Administration*, click **URL redirects**. *URL redirects* appears.
2. Click **New redirect**. The New redirect screen appears.

3. In the **Redirect this page** field, enter the original URL that you want to reroute to another URL. Be sure to enter the full URL, including a protocol such as "http://" at the start.

Note: When you migrate to Blackbaud NetCommunity from an existing website with a domain that you own, you can create redirects to route traffic from the pages of your old site to the pages of your new Blackbaud NetCommunity website. However, you must point the domain for the old website at Blackbaud NetCommunity. If the domain does not run through Blackbaud NetCommunity, you cannot create redirects because incoming requests are not routed through Blackbaud NetCommunity.

4. Under **To this page**, select whether to reroute users to another page on your website or to a page on an external site. For a page on your site, click the binoculars and select a page. For a page on another site, enter the URL.

5. Click **Save**. You return to *URL redirects*. When website users attempt to access the original URL, the program redirects them to the new target URL.

Export URL redirects to a CSV file

1. From *Administration*, click **URL redirects**. *URL redirects* appears.

2. Click **Export CSV**. A file download screen appears. Click **Save** to select a location to save a Microsoft *Excel* spreadsheet with your list of URL redirects or click **Open** to view the spreadsheet.

Import URL redirects

1. From *Administration*, click **URL redirects**. *URL redirects* appears.

2. Click **Import CSV**. The Import CSV screen appears.

Warning: The file you import must follow the proper format for *URL redirects*. The program ignores the first row in the spreadsheet because it is reserved for headers. Also, your CSV file must place the original URL in the first column and the redirect target URL in the second column.

3. Under **Import options**, select whether to add the import to your existing redirects or to replace the existing list with the import.

4. Under **Import CSV** file, click Browse to select the import file.

Tip: When you create your import file, remember to enter full URLs, including protocols such as "http://" at the start.

5. Click **Save**. You return to URL redirects and the gallery is updated with the imported redirects.