blackbaud™ Target Analytics®

Manage Application Users Pre-SSO

Last Updated: 08/05/2016 for ResearchPoint 4.91

Contents

Application Users in ResearchPoint

In this guide, learn about the tasks associated with managing application users in ***ResearchPoint***.

How to Log in to ResearchPoint

Your administrator contact should receive an email from Blackbaud with your organization's administrative login and password information.

- **URL** – Log into your hosted ***ResearchPoint*** database from the latest version of your preferred Internet browser. Replace ##### with your organization's site ID.

  Example:

  https://login.blackbaudondemand.com?SiteID=#####

  or

  https://login.blackbaudondemand.com?SiteID=#####RP

- **User Name** – The Administrator login begins with "ProspectMgr" and is appended with your site ID. Your organization sets up all other user names in ***ResearchPoint***.

  Tip: If you are the administrator and do not have an email address associated with your user name yet, contact ***ResearchPont*** Customer Support for assistance.

- **Password** – Forget your password? Use the password reset link in ResearchPoint.

ResearchPoint User Roles

To establish user security and limit access to only job-specific functions within the program, users are assigned to system roles. The program includes a set of standard system roles that should meet the needs of your organization.

Note: The tasks assigned to the standard system roles are pre-configured and cannot be changed. If a user needs additional privileges that a single system role alone will not provide, you can assign the user to multiple roles.

Prospect Research – This is the main role in ResearchPoint. Assign prospect research to individuals who perform prospect research tasks. For example, the most important task of a prospect researcher is to confirm and reject results from a WealthPoint screen. If you have an individual who performs part-time research, such as a development officer, assign them this role.

Prospect Research Manager – Assign this administrator role to individuals who need the greatest level of access to functionality. This role builds on the prospect research role. To assign someone prospect research manager rights, you should also give them the prospect research role. Prospect research managers can add new users to the system and control user access.

Development Officer (View Only) – As a view-only role, assign these rights to development officers who need to view ResearchPoint data. View-only enables development officers to search and review prospects and print prospect research reports. However, these users cannot add, edit, or delete content.

Development Officer (Advanced Rights) – This role builds on the Development Officer - View Only role. Assign both these roles to users who need more than view-only rights, but not as much as a prospect researcher. Advanced Rights enables development officers to screen records and access a limited amount of add and edit rights, in addition to the view-only rights.

Email Services Administrator and Email Services User – A system role that comes with the program, but not necessary for you to use.

System Role Tips

From *Administration*, you can access the System Roles page. The system roles page enables you to review and perform some helpful tasks for each user role in ***ResearchPoint***.

From the System Roles page, click a system role to open the system role record.

Tip #1: In the left task bar, under **Reports**, click **System role**. The System Role report displays information about the system role, this includes the assigned users, groups, and tasks, as well as the permissions and security set for the role.

Tip #2: On the Code Tables tab, you can specify whether users in the system role can add entries to a table "on the fly," edit existing entries, or delete entries.

Tip #3: On the Users tab, if you added a new application user record but did not assign them to a system role from their application user record, you can add users to the system role here.

Tip #4: On the Batch Types tab, you can specify whether a system role has administrative privileges for specific batch types.

When you grant administrative permissions to a system role for a batch type, you specify that users in that role can create templates and perform all other functions associated with that batch type, including reviewing and validating submitted batches, approving batches, and committing approved batches to the database.

Prospect Research Manager

This role grants administrative tasks not included in the Prospect Research role. To assign someone prospect research manager rights, you need to also give them the prospect research role. It is especially useful for larger organizations. This role enables users to add new users, manage code tables, and access additional configuration settings.

Task name	Task description	Functional area
Application user search	Search for and view application user records.	Administration
Application users	View the list of application users.	Administration
Attribute categories	Provides a user interface for managing attribute categories.	Administration
Business processes	View the list of business process runs.	Administration
Business process ownership	View and edit business process owners.	Administration
Code tables	View the list of code tables and table entries.	Administration
Constituent group types	Add, edit and delete constituent group types.	Prospects
Countries and states	Configure system countries and states.	Administration
Educational catalog	Create and manage the academic catalog and educational institutions.	Administration
Email alerts	Configure and manage email alert settings.	Administration
Enable/disable phone formatting	Enables or disables phone number formatting on add and edit forms.	Administration
First names	Modify first names table.	Prospects
Global changes	Create and manage global change instances.	Administration
Mapping	This task is used to configure mapping.	Administration
Notifications	Provides a user interface for managing notifications.	Administration
Organizational units	Manage the Active Directory organizational units associated with the system.	Administration
Queue	Allows for managing queue business processes.	Administration
The Raiser's Edge integration	Configure the settings for integration with The Raiser's Edge.	Prospects
Reason codes	Displays the page to manage reason codes.	Prospects
Relationship types	Provides an interface for managing relationship types.	Prospects
System roles	Manage system level permissions.	Administration

Task name	Task description	Functional area
Title code defaults	Modify title code defaults.	Prospects
Match settings (admin)	Set constituent match settings.	Administration
Match settings (batch/import)	Set constituent match settings.	Batch and Import

Prospect Research

The main system role, this role grants users access to features used to determine prospect qualifications. Rights include but are not limited to adding, editing, and managing constituent records; searching for Wealth Information; importing and exporting data; and using advanced features such as Mapping and Prospect Analysis dashboards.

Task name	Task description	Functional area
Add a group	Add a new group constituent.	Prospects
Add a household	Add a new household constituent.	Prospects
Add a prospect research request	Add a new prospect research request.	Prospects
Add an individual	Add a new individual constituent.	Prospects
Add an organization	Add a new organization constituent.	Prospects
Ad-hoc query search	Search for an ad-hoc query and view the results.	Analysis
Batch entry	Manage batches through all stages of the batch workflow.	Administration
Community	Launch browser and participate in ResearchPoint Community blogs, user forums, and Idea Bank.	Prospects
Constituent density map	Create a heat map of selected constituent addresses to help determine the location of most prospects.	Mapping
Constituent search	Search for and view constituent records.	Prospects
Export	Create and manage exports of query results.	Administration
Import	Create and manage imports into batch.	Administration
Manage research groups	Create, populate and view research groups.	Prospects
Mapping	Interactively map records based on their geographical locations.	Prospects
My prospect research page	View my prospect research area.	Prospects
Organization search	Search for and view organization constituent records.	Prospects
Prospect analysis	Analyze and segment prospects based on data modeling.	Prospects
Prospect Quick Search	Search for new prospects using partial information.	Prospects
Query	Create and manage queries.	Analysis
Search The Raiser's Edge	Search for a Raiser's Edge constituent to add or link.	Prospects
Wealth and ratings data	Configure WealthPoint searches and ratings.	Prospects

Task name	Task description	Functional area
Wealth capacity formula management	Manage wealth capacity formulas.	Prospects
Match settings (batch/import)	Set constituent match settings.	Batch and Import

Development Officer

Generally a view-only role, this role enables users to review the data in the system but not enter any changes to the data. The Development Officer can run constituent searches, view data, print prospect profiles, and execute some general queries.

Task name	Task description	Functional area
Add a prospect research request	Add a new prospect research request.	Prospects
Ad-hoc query search	Search for an ad-hoc query and view the results.	Analysis
Community	Launch browser and participate in ResearchPoint Community blogs, user forums, and Idea Bank.	Prospects
Constituent search	Search for and view constituent records.	Prospects
My fundraiser page	View my major giving area.	Prospects
Organization search	Search for and view organization constituent records.	Prospects
Product news	Launch browser to read about ResearchPoint product news, release notes, and The Prospector.	Prospects
Prospect analysis	Analyze and segment prospects based on data modeling.	Prospects
Query	Create and manage queries.	Analysis

Development Officer - Advanced Rights

Generally a view-only role, this role allows users to review the data in the system, but not enter any changes to the data. The Development Officer can run constituent searches, view data, print prospect profiles, and execute some general queries. In addition, the advanced role allows access to search and review prospects, and access research lists, research groups, and the individual screen.

Task name	Task description	Functional area
Add a prospect research request	Add a new prospect research request.	Prospects
Run prospect search	Search all existing ResearchPoint prospects; integrate the Raiser's Edge database; and the external Target Analytics database. Role does not allow user to add or modify data.	Prospects
View Research Lists	View only	Prospects
Ad-hoc query search	Search for an ad-hoc query and view the results.	Analysis
Community	Launch browser and participate in ResearchPoint Community blogs, user forums, and Idea Bank.	Prospects
Constituent search	Search for and view constituent records.	Prospects
My fundraiser page	View my major giving area.	Prospects
Organization search	Search for and view organization constituent records.	Prospects
Prospect analysis	Analyze and segment prospects based on data modeling.	Prospects
Query	Create and manage queries.	Analysis

Search for and Open Application User Records

After you add new application users, if your organization has many user records, it can far easier to search for and open an application user record than to scroll.

How to find and open an application user record

1. From *Administration*, click **Security**. The Security page appears.
2. Click **Application user search**. The Application User Search screen appears.

   Note: Because your application and database exist in a hosted environment, the results grid on the Application User Search screen may list a number of Blackbaud users who are system administrators.

   These users help clients setup and implement applications in our hosted environment.
3. Enter the search criteria to use to find the user record, such as login name or display name.
4. To return only system administrators in the search results, select **Is system administrator**. To match the search criteria exactly as entered, select **Match all criteria exactly**.

   If the user is linked to a constituent, you can also search by constituent name. To do so, enter the name in the **Constituent name** field.
5. Click **Search**. The program searches the database for the application user.
6. In the **Results** grid, all users that match your search criteria appear.

   Note: If your search returns more than 100 users, only the first 100 appear in the grid.
7. Click the row of the user record to open. The application user record appears.

Add New Users to ResearchPoint

Prospect Research Managers can add new users to **ResearchPoint** and manage other users' access to the database.

As you begin to use ResearchPoint, it's important to review program roles and create user names for each individual in your organization who needs to complete research or view research results. When you add users, we recommend you create a unique user name for each individual instead of sharing login information.

Benefits of Adding Unique Users

- For database security, it's easier to disable a single user than make adjustments when an individual separates from your organization.
- From Prospects, under Configuration, click Wealth and ratings data to track who performed WealthPoint screens.
- When you create queries to track and report on prospect data research, include the Added by

user name and Changed by user name fields to verify who worked on a specific record.

- On the Biographical Information tab of a prospect's wealth and ratings record, you can track and report on the history of changes to a prospect's record.
- You can assign users to a research list, prospect research request, batches, and more!
- If you integrate with The Raiser's Edge, separate user names enable you to link to Raiser's Edge users for greater efficiency and security.

How to Add Users

1. As your organization's ***ResearchPoint*** administrator or assigned Prospect Research Manager, log in to ***ResearchPoint***.
2. From *Administration*, under **Configuration**, click **Organizational Units**. The Domain Users page appears.

   Tip: If you manage many users, we recommend you add the Domain Users page link to your shortcuts.

3. Click **Add**.
4. Create a new username and password for the user.
   - The system automatically appends your Blackbaud site ID to the end of the user names you create.
   - Usernames, including the appended Site ID, must be less than 20 characters.
   - The password must meet the minimum security requirements.
5. Enter a description for the new user. We recommend you enter the role type you plan to assign to the user.
6. Click **Save**. You return to the Domain Users page. Before you add another user, we recommend you first assign security permissions to the user you created. If you do not, this new user will not have access to perform any tasks in ***ResearchPoint***.
7. To open the user's ***ResearchPoint*** record, click the name.
8. On the System Roles tab, click **Add**.
9. In the System role field, click the magnifying glass to search for and select a system role.

   For more information about which system role to assign, review the Manage Application Users guide.

10. Click **Save**. You return to the user's ***ResearchPoint*** record.
11. If you need to assign another role, on the System Roles tab, repeat steps 7 to 9.
12. To enable email alert settings, on the Email Preferences tab click **Edit** to enter the email address.
13. If this new user is a fundraiser at your organization, under **Tasks**, click **Edit link to constituent**. In order to access fundraiser tasks in ***ResearchPoint***, each fundraiser user needs to be linked to a constituent.
14. Select **[username] is linked to** and click the magnifying glass to search for and select the constituent name.
15. Click **Save**.
16. To enable password reset, at the top of the user's ***ResearchPoint*** record, click **Application**

Users. The Application Users page appears.

17. To access the application user's action bar, click the down arrows next to the new username.
18. Click **Edit email address**.
19. Enter the email address for the user. Now, the user can reset his or her own password.
20. Click **Save**.
21. To add another new user, return to the Domain Users page (see step 1).

    After you add a user, you can access the user's ResearchPoint record from two places — the Domain Users page, or from Administration, Security, click Application Users.

Email Addresses for Application Users

For application users, there are two important places you can add email addresses.

- You can add email addresses so your users can reset their own passwords.
- You can add email addresses so your users can receive application alerts. You can also disable email alert types for those users who may not need all the alerts.

Tip: When you add an email address for password reset, it is NOT shared with the email address for the alerts. You will need to set up both to use each of these features.

Add an application user email address for password reset

1. From *Administration*, click **Security**.
2. Click **Application users**.
3. Click the double arrows in the row for application user.
4. Click **Edit email address**. Enter the application user's email address where she wants to receive password reset instructions.
5. Click **Save**.

Add an application user email address for email alerts

1. From *Administration*, click **Security**.
2. Click **Application users**.
3. To open the application user record, in the row for application user, click the display name link.
4. Select the Email Preferences tab.
5. Click **Edit**. Enter the application user's email address where she wants to receive application email alerts.
6. Click **Save**.
7. To disable email alert types that a user does not need, click the double arrows for the email alert type row and click **Disable**.

Password Recommendations

When you create new application users, you create a temporary password so the user can access the program. To maintain security, you should instruct your new users to change their password when they log in. All user passwords must meet the following complexity requirements:

- A password cannot be the same or overly similar to a previously used password.
- Passwords must be at least eight characters in length.
- Passwords must contain at least three of the following four character types: uppercase letters (ABC), lowercase letters (abc), numbers (123), or symbol characters (!@#).

Note: If a user attempts to log in using an incorrect password five times within a 30 minute period of time, their account will be locked and must be unlocked by a System Role Administrator.

How to change your own password

1. In the upper right corner of ***ResearchPoint***, click the **Welcome** menu.
2. Select **Change password**. The Change password screen appears.
3. In the **Old password** field, enter your current password.
4. In the **New password** and **Confirm password** fields, enter a new password that meets the following complexity requirements:
    - A password cannot be the same or overly similar to a previously used password.
    - Passwords must be at least eight characters in length.
    - Passwords must contain at least three of the following four character types: uppercase letters (ABC), lowercase letters (abc), numbers (123), or symbol characters (!@#).
5. Click **Save**.

How to reset a user password as an administrator

1. From *Administration*, under **Configuration**, click **Organizational units**. The Domain Users screen appears.
2. Under **Users**, click the double arrows for the user with the password to reset and click **Reset password**. The Reset password screen appears.
3. Enter and confirm the new password.
4. Click **Save**. You return to the Domain Users page.
5. Provide the user with the temporary password and instruct them to log in with it and immediately change the temporary password to a secure password only they know.

Unlock User Accounts

If a user attempts to log in using an incorrect password five times within a 30 minute period of time, the account is locked. Once locked, a System Role Administrator must edit the user account and clear the **Account is locked** checkbox before the user can log in again.

Unlock a user account

1. From *Administration*, under **Configuration**, click **Organizational units**. The Domain Users page appears.
2. Under **Users**, click the double arrows for the user with the locked account.
3. On the action bar, click **Edit**. The Properties screen appears.
4. Clear **Account is locked out**.
5. Click **Save**. You return to the Domain Users page.

   The account is now unlocked and the user can attempt to log in again.

Remove Application Users from ResearchPoint

If a user leaves your organization, has had their password compromised, or poses some other security risk, you can disable their account. When you disable a user account, the user can no longer log into the application. If needed, you can enable their account again so they can log into the application.

Also, we recommend you disable users to remove them from ***ResearchPoint*** instead of deleting. When you disable, you remove the user's ability to log in to ***ResearchPoint*** but you maintain a history of the user's actions in the application.

Disable a user account

1. From *Administration*, under **Configuration**, click **Organizational units**. The Domain Users page appears.
2. Under **Users**, click the double arrows for the user account you want to disable.
3. On the action bar, click **Edit**. The Properties screen appears.
4. Select **Account is disabled**.
5. Click **Save**. You return to the Domain Users page. The user account is now disabled.

Note: To enable the user account again, click **Edit**, clear the **Account is disabled** checkbox, and click **Save**.

Link an Application User to a Constituent Record

If one of your prospect research users is also a fundraiser, you need to link the application user record to a constituent record in ResearchPoint.

This enables your application users to see information relevant to their fundraiser tasks. For example, in *Prospects*, under **Prospect Research**, the users can then access their **My fundraiser page**.

Add link to a constituent

1. From *Administration*, click **Security**.
2. Click **Application user search** and search for your application user.
3. Select the row of the application user you want to link. The application user record opens.
4. Under **Tasks**, click **Edit link to constituent**.
5. Select [Application user name] **is linked to** and then search for and select the constituent record to link.
6. Click **Save**. You return to the application user record.

> ***Tip:*** You can also add a link between a constituent and an application user from the prospect's wealth and ratings record. On the Biographical Information tab, **Personal Info**, click **Edit link to user**.

Add fundraiser constituency to a constituent record

After you link your application user to a constituent record in ***ResearchPoint*** but before you assign prospect research tasks to fundraisers, you need to assign the fundraiser constituency to the constituent record.

1. From the Home page, search your saved prospects for your constituent and open the record.
2. Select the Affiliations tab.
3. In the **Constituencies** section, click **Add** and select **Fundraiser**.

   Your application user is now ready to perform research request tasks.

ResearchPoint 4.91 Manage Application Users Pre-SSO US

©2016 Blackbaud, Inc. This publication, or any part thereof, may not be reproduced or transmitted in any form or by any means, electronic, or mechanical, including photocopying, recording, storage in an information retrieval system, or otherwise, without the prior written permission of Blackbaud, Inc.

The information in this manual has been carefully checked and is believed to be accurate. Blackbaud, Inc., assumes no responsibility for any inaccuracies, errors, or omissions in this manual. In no event will Blackbaud, Inc., be liable for direct, indirect, special, incidental, or consequential damages resulting from any defect or omission in this manual, even if advised of the possibility of damages.

In the interest of continuing product development, Blackbaud, Inc., reserves the right to make improvements in this manual and the products it describes at any time, without notice or obligation.

All Blackbaud product names appearing herein are trademarks or registered trademarks of Blackbaud, Inc.

All other products and company names mentioned herein are trademarks of their respective holder.