Bill Connors CFRE
Consulting and Training on Raiser's Edge®

Adding and Inactivating Users in Raiser's Edge NXT

Updated March 29, 2021, and believed accurate for the software as of this date.

This document is written for Raiser's Edge NXT organizations. It can easily be adapted for organization still using Raiser's Edge version 7.

Raiser's Edge version 7 and Raiser's Edge NXT organizations are in a variety of hosting environments. The environment dictates the exact security procedures, and there are too many variations to create a single checklist that will make perfect sense for everyone. Furthermore, procedures for Blackbaud Hosting that is not on Azure are currently changing for some clients and will be for others over 2021. If you are unclear what environment you are in, how that affects your security requirements, and how to apply that environment to the checklists below, see Bill's Security webinar presentation and/or slides for March 30, 2021. They can be found at https://billconnors.com/resources.

This document is a checklist with some tips, not a how-to, so consult Blackbaud resources such as documentation, training, and the knowledgebase for how-to questions that arise. (or contact Bill for consulting and training)

You might also wish to cross-reference the slides and presentations from Bill's 2021 webinar series on Security in partnership with Blackbaud which can be found at https://billconnors.com/resources.

They/them/theirs is used in this document in the singular for gender neutrality. This document also uses "correct" Raiser's Edge terminology. If you are confused about what is being referred to, see "Raiser's Edge NXT: What's Called What" on the same website page listed above.

Important Consideration: Changes to the Database Manager

The following checklists are for a database manager who likely has Supervisor and Admin rights and is setting up a user who does not need that level of rights. The process has additional steps and considerations if it is the database manager who is coming or going. Some of those considerations to think through before implementing the following checklists:

phone 415.861.5454 email bill@billconnors.com web billconnors.com address 584 Castro Street, #320, San Francisco, CA 94114

1. Blackbaud.com requires an "Organization admin" for your organization. This helps manage your relationship with Blackbaud, such as setting an invoice contact, among other things, and manage your organization's Blackbaud.com account, such as setting single sign-on. This is accessed from the "hamburger menu" (three lines) in the upper left of Blackbaud.com by choosing Admin. Blackbaud.com also allows for an Environment Admin, and Raiser's Edge NXT allows for a Solution admin. (for an explanation of these various admin types, see https://kb.blackbaud.com/knowledgebase/articles/Article/192031)
    a. If your database manager is leaving, you need to give someone access to these areas of the software before you inactivate the database manager's Blackbaud.com account.
    b. When your new database manager starts, likely they need to be given access to these areas.
    c. You may legitimately have more than one person with Admin access here beyond your RE database manager, such as the Financial Edge NXT admin and IT. Those with such access should coordinate their work to ensure efforts are not duplicated and areas needing attention are not assumed to be someone else's responsibility.

2. Usually only the RE database manager has Supervisor and Admin rights in RE. Do not inactivate this user's account and rights before giving those rights to someone to hold and exercise until they can be passed on to the next database manager.

If the only person with these rights is no longer with the organization and no current staff member has these rights, contact Blackbaud Support for assistance getting a new user assigned to these rights.

Adding a New User

When you have a new staff person who will use Raiser's Edge NXT, complete the following tasks.

1. Find out from the hiring manager the following information in advance:
    a. The new user's preferred name, first or nick, and last name
    b. Their new title/position at your organization
    c. Their email address
    d. Their stated Raiser's Edge knowledge and experience
    e. Their expected roles and responsibilities, both in general in their position as well as with Raiser's Edge.

2. Schedule a first appointment with the new user for 60 minutes, either in the onboarding schedule the hiring manager is preparing or directly with the new staff person.

3. If the user will be a database view user, work with IT to ensure Citrix is installed on the new user's computer or you will have sufficient security rights on the computer to do so yourself.

4. If the user will be a web view user and sending and receiving emails that should be stored as actions in RE, work with IT to install the Blackbaud or a third-party add-on on the user's computer to allow your email program (i.e., Outlook or Gmail) to communicate with RE for this purpose. (available here: https://app.blackbaud.com/marketplace/)

5. In the database view, add the user as a constituent. Pay attention to the following areas:
    a. Mark the constituent as a solicitor so you can link the user's constituent record to the user account.
    b. Use the Business button on the Bio 1 tab to link the constituent to your organization's constituent record and complete the other fields.
    c. Give the constituent a "Staff"-type Constituent Code. The Date From should be the day they started.
    d. Complete other fields your organization requires for new constituents and staff records.

6. Globally add the user as a solicitor/fundraiser to their assigned constituents, if appropriate.

7. In Administration, Security, find or create a group right for the user. Remember these important points:
    a. *Don't just pick an existing, easy user group to throw the user into. Be thoughtful, not fast. The single most important responsibility you have is protecting the institution's data and constituent privacy while enabling your team to fully do their jobs in a modern fundraising shop.*
    b. Consider putting the new user into their own security group, the rights of which will grow over time as the user gets training. There's nothing wrong with a group with only one user: security is too important.
    c. Do not give the user more rights than their immediate training will prepare them.
    d. Do not put the user in more than one security group.
    e. See Bill's 2021 webinar series on Security for more ideas (website listed on page 1).

8. Still in the database view in Administration, Security, create a user account for the user.
    a. Use full first or nickname and last name with a space between them.
    b. Put the user's title in the Description field.
    c. In most cases, link the user to their constituent record.
    d. Put them in the one security group to which they belong.
    e. Provide a password that meets the Blackbaud requirements.
        i. If you are on Blackbaud Hosting and not on Azure, and you still use blackbaudhosting.com to get to the database view, and the user will need to use the database view, you will need to remember and share this password with the user. Do not otherwise record this password anywhere.
        ii. Otherwise, you do not need to remember this password and should not.

f. Do not turn on Windows Authentication (if you are still using blackbaudhosting.com it is better security if you do not use it, otherwise this will be taken care of for you in a later step).
g. Give the user the appropriate default User Options.

9. If the user will be using the database view and should have settings similar to those of an existing or previous user who has not been deleted, use the option for Copy User Settings on the Plug-Ins page to copy the User Options, Home Page, and Dashboard pages.

10. If the user should have access to Online Express, set up the user and security group in Online Express to have the rights they need.

11. (1) If you use Blackbaud Hosting and do not use Azure, (2) and you have not yet been changed in 2021 so you can only access the database view through the web view and you still use blackbaudhosting.com, (3) and the user will use the database view, add the user in Blackbaud Hosting User Administration (otherwise skip this step).
    a. Create the user account.
        i. Remember the logon name and password to give to the user, but do not store it anywhere permanently.
        ii. Set up the account to require the user to change it upon their first login.
    b. Remember to put the user in the appropriate hosting security group as well.

12. Think through and prepare for the training plan the user needs based on what you know about them. Time should be allocated in the new staff person's first week and month(s) for proper training. A quick hour together is not sufficient training. Create a schedule, along with the new user's manager, which reflects the speed and depth at which the new staff person needs to be using Raiser's Edge. All users need:
    a. Generic RE training about how to use the system relevant to their role
    b. Training specific to how your organization uses your copy of RE: *you* or a colleague need to deliver this, Blackbaud and written material are not sufficient.

13. Set up the user in the web view just before you meet with them. Do not do it too far in advance because users often lose the invite emails, don't remember their passwords, or they might get in before you've given them the direction they need.
    a. *Review the web view security roles you are likely to need for this user and be as thoughtful with the web view roles as you were with the database view group.* Add and edit as needed for this user.
    b. Send a personal email to the user from your email account giving them a heads up about the invitation email they'll be getting from Blackbaud to join Blackbaud.com and the RE NXT web view. Ensure they know it's not spam and it's not optional – they need to do that setup.

i. Also tell them the password requirements and remind them they need to remember the password, using the tools your IT staff or consultant recommend, as this is their only way into the web view and you have no ability to reset it or retrieve it for them.

c. Add and invite this user to the web view
   i. Enter their name properly (watch spelling, casing, spacing – be consistent and professional)
   ii. Enter their email address correctly, of course
   iii. Carefully assign them to roles
   iv. And finally, make sure you link them to the database view account you created above. Do not click Create and create a duplicate account for them. Link!

14. Meet with your new user in a 60-minute meeting
   a. Welcome them, learn about them, introduce yourself to them
   b. Introduce them to the importance of the data you are about to give them access to. Especially emphasize the data is on the internet and all the risks, as well as opportunities, that poses. Ensure your user understands your organization policies and procedures for security, computer use, data use, personal smart phone use, etc.
   c. Reiterate that there are no circumstances ever, no exception, that they should ever share any of these login names and passwords with anyone: not you, not a co-worker, not a manager, not a temp, not a volunteer, not an intern, not a friend or family member, not Blackbaud, not IT – no one.
   d. Help them get into the web view.
   e. Help them turn on two-factor authentication in their Blackbaud.com account; emphasize they are not to turn it off no matter how annoying they find it (we agree, it is! but it's the best security).
   f. If you're on Blackbaud Hosting with blackbaudhosting.com and the user will need to use the database view, share the following 4 pieces of information with them confidentially and help them get in (if both conditions don't apply, skip this step).
      i. Blackbaud Hosting logon name
      ii. Blackbaud hosting password – ensure they change it, memorize it, and only store it in an IT-approved manner. They should not share it with you.
      iii. Their database view login name
      iv. Their database view password. As soon as they log in, have them go to Edit, Change Password and change their password and again, memorize it and only store in it an IT-approved way. It also should not be shared with you.
   g. Provide a brief orientation to get started.
   h. Present them with their initial training plan, their specific continuing education plan, and your ongoing continuing education plan for all users.
      i. This might involve introducing them to Blackbaud's Training Central.

ii. Consider the numerous video options available via Blackbaud Training and Customer Success as well.
iii. Make a plan to show teach them how the email add-on works.

i. Give them any needed initial cheat sheets.
j. Show them where your organization's RE policy and procedure documentation is located on the network or web and documents they might need to consult, if any, to learn and do their work correctly.
k. And while you want to avoid overwhelming the new user, should you show them the Blackbaud Community and how they can benefit from that?

15. After the meeting, schedule for yourself all needed follow-up items with your new user to ensure
    a. They get the training they need
    b. Their security rights grow as their training increases.

Inactivating a Former User

When you have a staff person who uses Raiser's Edge NXT leave your organization, complete the following tasks immediately: do not allow someone who no longer works for your organization to have access to your data and database online.

When a staff person who has been using Raiser's Edge at your organization leaves, do not begin by deleting their user account in Security. Follow these steps in order first.

1. Using the database view, identify all incomplete actions for the user. Reassign, mark as complete, or delete the actions as appropriate. Check each of the following fields for the user's activity:
    a. Action solicitor/fundraiser
    b. Action user
    c. Action added by

2. Identify all open solicitor/fundraiser assignments for the user/constituent and re-assign them.

3. Deactivate the user as a solicitor. When you do so, RE will prompt you to add a date as the Date To for the person's open solicitor assignments.

4. Update Business and Constituent Code information in the user's constituent record to reflect that they are now a former employee. Update other fields as appropriate for the person as well.

5. In the database view in Administration, Security: Rename the user to First Name Last Name Title (as much as will fit) and save (for example: Martha Hernandez, VP Development). This

makes the name more meaningful for other users when they see it long after this user has left the organization. Save this change.

6. Do not delete the user account if this user has User Options, a Home Page, and a Dashboard page that would be difficult to re-create and are worth saving for the next user in the departing user's position. Save the user account until the new user begins so you can use the option in Plug-Ins to copy the old user's settings, but change the password on the account so it cannot be used inappropriately.

7. If you don't have this situation, you now have two options to consider for the user account:

    a. Delete the user from Security. The user's name and work will remain in the database after the user name has been deleted. Leaving the user name in the database presents a small security risk of access through that account. Deleting users removes none of the work the person has done, such as queries and reports, and does not remove the person's name from Properties, such as Added by and Last Changed by in constituent and gift records. The only known downside to deleting a user is that it is no longer possible to write a query with criteria of 'Added by' or 'Last changed by' and select that user's name.

    b. OR, my preferred option: Leave the user set to "Selected group rights" but with no group in the "Member of" column. Due to the inability to query on deleted users' names, some database administrators prefer to leave the user name in the system. If you take this approach, it is recommended you also:

        i. Change the user's password so the account cannot be accessed (remember the password long enough to change it, but afterwards it is no longer needed)
        ii. Add "zz" to the beginning of the user name to sort the user name to the bottom of the list of users so your "inactive" users are sorted to the bottom, leaving your active list of users clearly at the top.

8. If the user was in a security group unique for that person, consider deleting the security group since it's no longer in use.

9. If your organization uses Blackbaud Hosting via the blackbaudhosting.com domain, outside of Blackbaud.com, disable that user account for the user. (e.g., you're on "Boston" and have not yet had the change in 2021 from the separate website to only Blackbaud.com)

10. In web view Security, inactivate the user account if they have entirely left the organization. If they are still with the organization and using another Blackbaud product, coordinate with that product's admin what you should do with this user's Blackbaud.com account.

11. Review all queries, reports, mailings, and exports the user created without giving access rights to others to re-assign them as necessary. This may involve re-saving the parameters using Save As if the user set up security on the parameters to allow only themself access to them or just changing the Execute and Modify options to allow other users access.

See anything missing? Let Bill know for future updates of this document: bill@billconnors.com