Security Guide

03/17/2015 Blackbaud Direct Marketing 4.0 Security US

Security-2014

Contents

Security

Security in the program is determined by system roles and site security. System roles determine the features, tasks, queries, and more to which your users have access, while sites can partition records and limit access. In addition, there are audit tables which track changes and deletions made to your data, along with the user who made the change.

If you have established Active Directory user/group schemes, you can leverage that infrastructure when you establish your application users and system roles. You can manage your users without the need to duplicate your *Windows* network directory. For more information, see Assign Groups of Active Directory Users to a System Role on page 22.

Fundamentals of Security

The security model for the system is multi-dimensional and allows you to create a structure which is as simple or complex as needed. There are several components of security, including users, system roles, and sites.

Application users

These are smallest units in the security structure. An application user represents each individual with access to the system. Each application user is associated with a network domain and a user name. The application uses Windows Authentication for secure user access. However, if the application runs on a server outside your domain, users enter their credentials manually.

System roles

System roles determine the features and tasks users can access. By creating system roles that match the roles in your organization, you can customize the program so your users see only the features that they need.

Audit tables

In addition to security, there are audit tables which track changes made to your data, along with the user who made the change. You can review the audit tables and, if a user makes an unwanted change to a record, you may decide to revoke certain security permissions for the user to prevent future mishaps.

Application Users

You can manage your application users from one central location in the program. Application users are the individual users of your system. Access to data is based on the permissions of the system role(s) to which the application user is assigned.

In addition, you can access the Application Users page to view a list of all users you have added to the system. You can double-click a user in the list to view their user record. On the individual user record, you can see all system roles assigned to the user and edit the user to link them to a constituent.

Search for Users

After you add an application user, you can use the Application User Search page at any time to find the user by criteria such as login name or whether the user is a system administrator. If the user is linked to a constituent, you can search by constituent name.

Search for 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.
3. Enter the search criteria to use to find the user record, such as login name or display name.

   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**.
4. Click **Search**. The program searches the database for the application user.
5. 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.
6. Click the row of the user record to open. The application user record appears.

Application User Records

From the Application Users page or the Users tab of a system role record, when you select a user and click **Go to**, the application user record for that user appears. The application user record contains information about all the items to which the user has access, a combination of the items included in all the roles to which the user belongs.

View a user record

1. From *Administration*, click **Security**. The Security page appears.
2. Click **Application users**. The Application User page appears.
3. In the grid, click the name of the user to view. The user record appears. Each record includes a System Roles tab that shows each role the user is assigned to and a Tasks tab that displays each task the user can access.

Note: Because your application and database exist in a hosted environment, the grid on the Application User page may list a number of Blackbaud users who are system administrators. These users help clients setup and implement applications in our hosted environment.

4. To return to the Application users page, close the record.

Add an Application User

When you add application users to the system, you specify the domain name and the user name.

Note: The information on the application user record is view only. In order to edit the permissions, you must add or modify the system roles to which the user belongs. However, you can grant or revoke system administrator rights from the application user record.

Add an application user

1. From *Administration*, click **Security**. The Security page appears.
2. Click **Application users**. The Application Users page appears.
3. Click **Add**. The Add application users screen appears.

Warning: Although you can select an existing application user on the Add application users screen and assign new settings, this does not change the existing application user's settings. All modifications to existing users must be done through the Edit application user screen, accessed by selecting the user you want to edit and clicking **Edit** on the Application Users page.

4. Enter the domain and user name for each user to add.
5. To link the user to a content management system (CMS) user, select **Add linked CMS user**. This checkbox appears when you use ***Blackbaud Internet Solutions***.

   The **CMS user** column appears for you to link to an existing user or create a new one. To do this, click the binoculars.

   a. To link to an existing CMS user, enter first name, last name, or user name information and click **Search**. The Constituent CMS User Search screen appears.

   b. To map to a new CMS user, click **Add**. The Add CMS User screen appears.

   c. To grant the new user rights to *Users* and *Roles* in ***Blackbaud Internet Solutions***, select the checkbox. Next, enter login credentials for the new user and the additional information you want to include such as **Email address** and **Last name**.

      When you grant rights to *Users* and *Roles*, ***Blackbaud Internet Solutions*** tasks such as *Email* and *Users & security* appear when the user clicks *Web*.

Tip: To honor CRM rights for linked users in ***Blackbaud Internet Solutions***, select **Enable CRM security for linked CMS users** in ***Blackbaud Internet Solutions*** *Administration*. For example, if you select this checkbox and a user has CRM rights to the Annual Fund designation only, then that user can only access the Annual Fund designation in ***Blackbaud Internet Solutions***.

   d. To return to the Add application users screen, click **Save**.

6. Click **Save**. You return to the application user page. Permissions and system access for the user are established when you add the user to a system role. For more information, see Assign Users to a System Role on page 21.

Edit Users

You can edit an application user to link the user to a constituent record or to assign a site to the application user.

Note: The information on the application user record is view only. In order to edit the permissions, you must add or modify the system roles to which the user belongs.

If a user has an individual constituent record in the database as a fundraiser, linking to the constituent record enables the user to see information relevant to his activities. For example, in *Prospects*, the user can access his "My Fundraiser Page."

Edit an application user

1. From an application user's record, click **Edit application user** under **Tasks**. The Edit application user screen appears.
2. Under **Constituent link**, select whether the user is linked to a constituent record. If you select **Application user is linked to**, search for and select the constituent record to link the user to.
3. When you use ***Blackbaud Internet Solutions***, the **CMS link** frame appears. To link to a content management system (CMS) user, select **Link to CMS user** and search for the user. For more information, see Add an application user on page 4.

Tip: To honor CRM rights for linked users in ***Blackbaud Internet Solutions***, select **Enable CRM security for linked CMS users** in ***Blackbaud Internet Solutions*** *Administration*. For example, if you select this checkbox and a user has CRM rights to the Annual Fund designation only, then that user can only access the Annual Fund designation in ***Blackbaud Internet Solutions***.

4. Click **Save**. You return to the application user record.

Delete Users

From the Application Users page, you can delete the user from the program. From an application user's record, click **Delete application user** under **Tasks**.

Delete a user

1. From *Administration*, click **Security**. The Security page appears.
2. Under **Configuration**, click **Organizational unit**. The organizational unit page for your organization appears.
3. Under **Users**, select a user account and click **Delete**. A confirmation message appears.
4. Click **Yes** to continue. The user account is removed from the system and you return to the organizational unit record.

Grant/Revoke Users Administrator Rights

From the application users page, you can grant or revoke administrator rights for a user. From an application user's record, click **Grant system administrator** or **Revoke system administrator** under **Tasks**.

Run the Program as a Selected User

From the Application Users page, an administrator can specify to run the program as the selected user. The System Administrator does not need to know that user's password.

To test the roles they create, System Administrators can use the **Run as another user** option, available from the

Welcome menu, to mimic the user experience of any given user. The System Administrator does not need to know that user's password. System Administrators can assign a user to a system role they create, then log in as that user to determine if the features and other items they configured for the role display as intended.

The System Administrator can alter data when running as another user and the audit table will reflect that the mimicked user made those changes.

Run the application as another user

1. Log in to the application with system administrator rights and, on the menu bar, click **Welcome** and select **Run as another user** . The Run as user screen appears.
2. Enter the domain and user name to log in with, such as "SERVERNAME\ValerieS."
3. Click **OK**. The login screen appears with a "Running as user..." ribbon at the top to indicate you will run the application as the selected user.
4. Select your login credentials to run the application.

Note: If the application does not run in your domain, you must enter your application user name (including the domain) and password. For example, you must enter these credentials if the application is hosted on a server outside your domain.

5. Click **OK**. Another instance of the application opens, and you are logged in as the selected user.

Organizational Units

If you have established Active Directory organizational units, you can use them to add application users. On the Organizational Units page, you can view and manage the Active Directory organizational units associated with the program. To access the Organizational Units page, from *Administration*, click **Organizational units** under **Configuration**.

The **Organizational units** grid displays the Active Directory organizational units added to the program. For each unit, you can view its name, user group, and Lightweight Directory Access Protocol (LDAP) path.

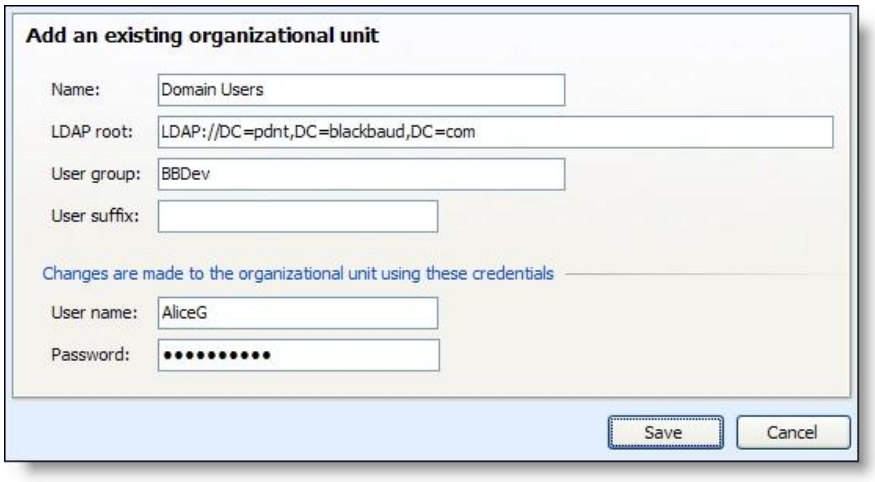
To view the users in an organizational unit, select the unit in the grid and click **Go to organizational unit**. The record of the organizational unit appears. For information about the record, see Organizational Unit Record on page 9.

From the grid, you can also manage the organizational units associated with the program.

Note: For additional information on how to assign and synchronize Active Directory groups to system roles, see Assign Groups of Active Directory Users to a System Role on page 22.

Add an Active Directory organizational unit

1. From *Administration*, click **Organizational units** under **Configuration**.
2. On the Organizational Units page, click **Add**. The Add an existing organizational unit screen appears.



3. In the **Name** field, enter a unique name to identify the organizational unit.
4. In the **LDAP root** field, enter the root LDAP path to the Active Directory organizational unit.
5. In the **User group** and **User suffix** fields, enter the group and suffix used to identify the users in the Active Directory organizational unit.
6. Under **Changes are made to the organizational unit using these credentials**, enter the user name and password of the user account that manages the Active Directory organizational unit.
7. Click **Save**. You return to the Organizational Units page. In the **Organizational units** grid, the new organizational unit appears.

Edit an organizational unit

1. On the Organizational Units page, select the unit and click **Edit**. The Edit an organizational unit screen appears.

Note: When you edit an organizational unit, you can edit only its name, LDAP root path, and user group or suffix. To edit the login credentials of the user account that manages the Active Directory organizational unit, click **Update credentials** on the action bar.

2. Adjust the information as necessary.
3. Click **Save**. You return to the Organizational Units page.

Update the credentials for an organizational unit

Update the user account credentials only if you receive notification that the credentials for the user account on the server has changed. Otherwise, the adjustment of these credentials may prevent access to the organizational unit in the Active Directory on the server.

1. On the Organizational Units page, select the unit and click **Update credentials**. The Update the credentials for the organizational unit screen appears.
2. Adjust the user name or password as necessary.
3. Click **Save**. You return to the Organizational Units page.

Remove an organizational unit

1. On the Organizational Units page, select the unit and click **Remove**. A confirmation message appears.

2. Click **Yes**. You return to the Organizational Units page. In the grid, the selected unit no longer appears.

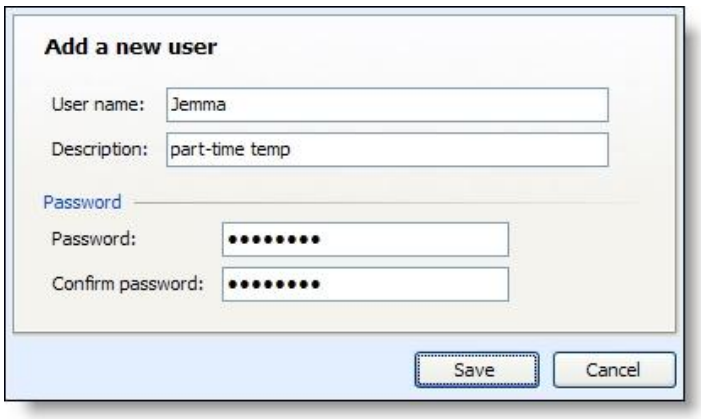
Organizational Unit Record

Each Active Directory organizational unit added to the program has a record. On the record, the Users grid displays the users associated with the organizational unit. In the grid, you can view the name and description of each user. To access the record of an organizational unit, select the unit on the Organizational Units page and click **Go to organizational unit** of the **Organizational units** grid.

From the organizational unit record, you can also manage the users associated with the unit.

Add a user to an organizational unit

1. From an organizational unit, click **Add**. The Add a new user screen appears.



2. In the **User name** and **Description** fields, enter the name and description used to identify the user.
3. In the **Password** and **Confirm password** fields, enter the password the user uses to access the organizational unit.
4. Click **Save**. You return to the organizational unit record. In the **Users** grid, the new user appears.

Edit a user of an organizational unit

When you edit a user of an organizational unit, you can edit the description of the user and select whether the user's password expires or whether the account is disabled or locked out.

1. From an organizational unit, select the user and click **Edit**. The Properties screen appears.
2. In the **Description** field, edit the description for the user as necessary.
3. To not require the user to change the password periodically, mark **Password never expires**.
4. To disable the user account, mark **Account is disabled**.
5. If a user has three or more failed login attempts, the **Account is locked out** checkbox is enabled and is marked automatically. To unlock the user's account, clear the checkbox.
6. Click **Save**. You return to the organizational unit record.

Delete a user from an organizational unit

1. From an organizational unit, select the user and click **Delete**. A confirmation message appears.
2. Click **Yes**. You return to the organizational unit record. In the grid, the selected user no longer appears.

Reset the password of a user in an organizational unit

Users of an Active Directory organizational unit can change their own passwords. If a user forgets a password, you can enter a new password for the user from the organizational unit record.

1. From an organizational unit, select the user with the password to reset and click **Reset password**. The Reset password screen appears.
2. Enter and confirm the new password.
3. Click **Save**. You return to the organizational unit record.

Application Users Page

From the Application Users page, you can view records for your users and grant users administrative rights.

Manage System Roles of an Application User

Security in the program is determined by system roles and record level access. System roles determine the features, tasks, queries, and more to which users can access, while record level security determines the specific records they can access. When you assign the system roles to users based on their jobs and responsibilities, the users see only the tasks and features required to perform their specific roles. You can also specify that users in specific roles access only specific subsets of your records. To view the system roles assigned to an application user, select the System Roles tab on the application user record.

Under **System Roles**, the system roles of the user appear. For each role, you can view whether its applicable record level access. The **Synchronized** column indicates whether the system role was assigned to the user through the Groups tab on the record of the system role and synchronized through an Active Directory group. To view additional information about a system role, such as its assigned tasks and groups, select it in the grid and click **Go to role** on the action bar. The record of the system role appears.

Tip: System administrators can assign system roles to a user and then log in as that user to determine whether the features and items configured for the user's roles appear as intended. For information, see Run the Program as a Selected User on page 6.

Depending on your system role, you can also add and manage the system roles of the application user.

Add System Roles to a User

From the System Roles tab of an application user record, you can assign applicable system roles to the user. When you assign the system roles to a user based on his or her job and responsibilities, the user sees only the tasks and features required to perform his or her specific roles. When you assign a system role to a user, you can also select the record level access for the user within the role.

Add a system role to a user

1. Access the record of the application user to which to assign a system role. For information about how to access a user record, see Search for Users on page 3.
2. Select the System Roles tab.
3. Under **System Roles**, click **Add**. The Add system role screen appears.
4. Search for and select the system role to assign the user.

5. Click **Save**. You return to the System Roles tab.

Edit a System Role for a User

From the System Roles tab of an application user record, you can edit the system roles assigned to the user. For example, you can edit the record level access assigned the user within a role.

Edit a system role for a user

1. Access the record of the application user for which to edit a system role. For information about how to access a user record, see Search for Users on page 3.
2. On the System Roles tab, select the role and click **Edit**. The Edit system role screen appears. The items on this screen are the same as the Add system role screen. For information about the items on this screen, see Add System Roles to a User on page 10.
3. Edit the information as necessary.
4. Click **Save**. You return to the System Roles tab.

Remove a System Role from a User

From the System Roles tab of an application user record, you can remove a system role from the user.

Under **System Roles**, select the role to remove and click **Remove**.

View CMS Roles Associated with an Application User

From the selected application user's page (from Application Users page, select the application user you want to view and click **Go to <application user name>**), select the CMS roles tab. Under **CMS manually added roles**, click **Add** to include the user in a ***Blackbaud Internet Solutions*** role. The Add CMS role screen appears for you to search for the role. To remove a CMS role for the user, select the role to remove and click **Remove**.

Under **CMS roles from query**, you can view a list of query based roles for the user.

Tip: This tab appears when an application user is linked to a content management system (CMS) user. For information about CMS roles, see the ***Blackbaud Internet Solutions*** *Users & Security Guide*.

View Business Processes Owned by an Application User

From the selected application user's page (from Application Users page, select the application user you want to view and click **Go to <application user name>**), select the Business Process Ownership tab.

All business processes that the application user owns display. An application user becomes a business process owner in one of two ways: an application user creates a business process or an administrator assigns business process ownership to an application user.

The tab also lists details such as process name and type, security folder, and creation date. To filter by process type, select a process in the **Process type** field.

After you enter filter criteria, click **Apply**. Business processes that match your criteria appear in the grid. To view all business processes, click **Reset**.

From this tab, you can also change the owner of a business process. You may find it necessary to edit a business process owner, for example, when a change in staff occurs at your organization. You can edit business process ownership in several ways:

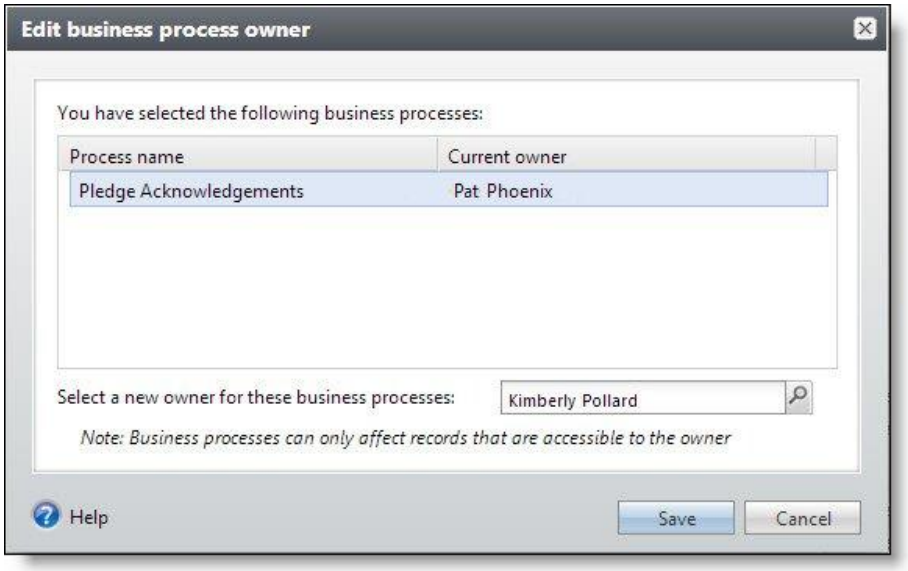
- To edit the owner for a single business process, select the business process in the grid and click **Edit owner** under the business process.
- To edit the owner for multiple business processes at one time, select each process and click **Edit owner** on the action bar.
- To edit the owner for all business processes at one time, select the checkbox next to the column names at the top of the grid, and click **Edit owner** on the action bar.

View and edit business process owner

1. From an application user's page (from Application Users page, select the application user you want to view and click **Go to <application user name>**), select the Business Process Ownership tab.
2. To edit the owner for a single business process, select a process in the grid and click **Edit owner** under the business process.

   To edit multiple processes at one time, select each process and click **Edit owner** on the action bar. Or, to edit all processes at one time, select the checkbox next to the column names at the top of the grid, and click **Edit owner** on the action bar.

   The Edit business process owner screen appears.



3. The business processes you previously selected appear in the grid. In the **Select a new owner for these business processes** field, click the search button and use the Application User Search screen to search for a different owner.

Warning: The new business owner you select is applied to all business processes that display on the Edit screen. A business process may have only one owner at a time. Note that security permissions for the business process owner may determine which records are processed when a business process runs.

4. After you select an application user as the new business process owner, click **Save**. You return to the Business Processes tab.

   The business processes are now associated with a new owner and no longer display in the grid.

View Tasks Associated with an Application User

From the selected application user's page (from Application Users page, select the application user you want to view and click **Go to <application user name>**), select the Tasks tab. All tasks to which this user has rights display.

View Features Associated with an Application User

From the selected application user's page (from Application Users page, select the application user you want to view and click **Go to <application user name>**), select the Features tab. All features to which this user has rights display.

View Code Tables Associated with an Application User

From the selected application user's page (from Application Users page, select the application user you want to view and click **Go to <application user name>**), select the Code tables tab. All code tables to which this user has rights display.

View Batch Types Associated with an Application User

From the selected application user's page (from Application Users page, select the application user you want to view and click **Go to <application user name>**), select the Batch types tab. All batch types to which this user has rights display.

View KPIs Associated with an Application User

From the selected application user's page (from Application Users page, select the application user you want to view and click **Go to <application user name>**), select the KPIs tab. All KPIs to which this user has rights display.

System Roles

Security in the program is determined by system roles and record level access. System roles determine the features, tasks, queries, and more to which your users have access while record level security determines the specific records they can access. When you create system roles that match the roles in your organization, you can customize the program so your users see only the features they need to complete the tasks associated with their role. You can also specify that users in specific roles have access to only specific subsets of your records.

The program supports integrated *Windows* security; this ensures that usernames and passwords do not have to be managed in the application and enabling a single-sign-on experience for your users. Additionally, you can synchronize the list of users in a system role with an Active Directory group (or groups) defined through *Windows* security.

System Role Security General Rules

If the standard roles included with the system do not meet your needs, you can add new roles that better reflect the work flow within your organization. If you add new system roles, you should review these general rules and keep them in mind as you proceed.

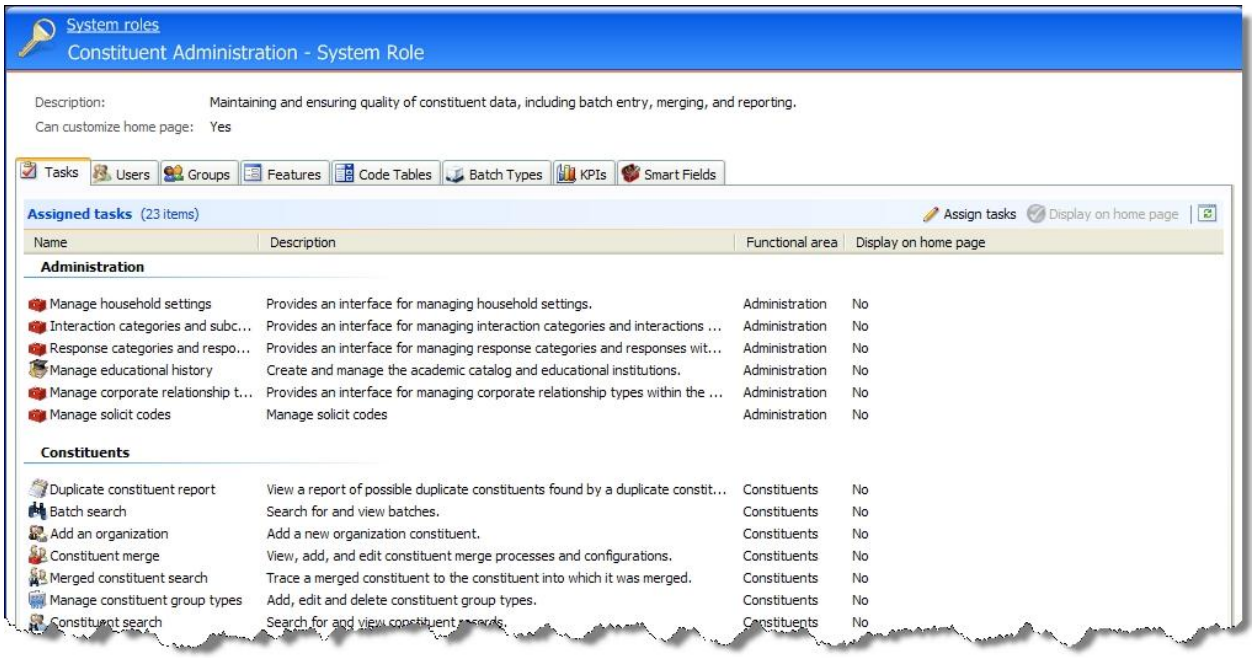
- You should set up your system roles in layers. Create the most basic, lowest level layer first. Build up from there, but for higher levels of access and permissions, don't include the permissions in the lower levels. Simply include the application users in the system role for the higher level layer as well as in the system role for the lower level layer. The user will get access for the items in each roles. This way, when a new feature is added, you can make the change in the lowest level needed only. Users in that role and above will gain access.
- Deny always take precedence over grant or unspecified rights.
- If a user belongs to multiple roles and one is granted access to a feature while another is denied access, the user does not have access to that feature. If one role has access and the other is unspecified, the user does have access.
- Tasks are really navigational elements, so they are not secured in the same way as actual feature permissions. If no features within a particular task are granted for a role, then even if that task is specifically granted to the role, it will not be visible (and directly accessible) to the users in that role.
- Tasks can either be granted or not specified. There is no deny option for tasks.
- When you grant permissions for ad-hoc queries to a role, you must grant rights to the root query view for the feature in the tree view. The user will not be able to create new ad-hoc queries without access to the root query view, such as constituents or mailings.
- Because dashboards are driven by datalists, when a dashboard feature is granted for a role, the datalists that populate that dashboard are implicitly granted. Therefore when you grant rights to a dashboard, it is not necessary to also grant rights to the datalist(s) used by the dashboard.

Manage System Roles

The System Roles page provides a central location to manage all facets of your system roles. To access the System Roles page, from *Administration*, click **Security** and then click **System roles**.

System Role Records

The system role record enables you to configure all the items and features to which a role has access.



Add System Roles

To add a system role enter a name and description for it. After you add the system role, you can add users and groups to it, as well as define the items to which users assigned to this role will have access. For example, you may want to add roles such as “Constituent Data Entry Personnel” and “Constituent Administrators” for which you will later configure access rights.

For roles that are similar, consider copying an existing role as a starting point. For more information, see Copy System Roles on page 18.

Add a system role

1. From *Administration*, click **Security** and then click **System roles**.
2. From the System Roles page, click **Add**. The Add system role screen appears.
3. Enter a name for the role, such as Marketing Coordinators.
4. You can provide a description to make the role easier to identify on the Manage System Roles page.
5. If the new role is similar to another role, you can mark the checkbox and select a role. You can also copy the users from the existing role to the new role.
6. Click **Save**. You can now configure the role.

Edit System Roles

You can edit the name and description of a role at any time. To edit a system role, select the role and click **Edit**.

Delete System Roles

When you delete a system role it does not remove any application users from the program, but if a user is associated with only one role and that role is deleted, the user will not have access to any items in the program. To delete a system role, select the system role and click **Delete**.

System Role Report

The System Role Report displays information about the system role, this includes the assigned users, groups, tasks, and KPI instances, as well as the permissions and security set for the role.

To run the System Role Report, go to a system role and click **System role report** under **Reports**.

Copy System Roles

To add system roles, you can copy another role to use as a template. You can also copy the assigned users of the other role to the new role. For example, you may want to copy roles such as “Constituent Data Entry Personnel” to use to use as the basis for a “Constituent Administrators” role.

Copy a system role

1. From the System Roles page, select a system role and click **Copy**. The Add system role screen appears, along with a “Copy from” system role.
2. Enter a name and description for the new role.
3. If you want to copy users from a system role to a new role, mark the checkbox.
4. Click **Save**. You can now configure the new role.

Export System Roles

When you export a role definition as an XML file, all information about the role is included except for users and groups. You may want to export a role if you are planning to create a new role that will have similar settings as an existing role. Rather than manually specifying all the settings in the new role, you can export the existing one, import it as the basis for the new role, then adjust the settings as necessary.

Warning: When you export an existing role, the Name and ID elements in the XML file will be that of the existing role. Before you import the XML file, change the Name and ID to that of the new role. If you leave the existing Name and ID, when you import the role, it will overwrite the existing role rather than creating a new one.

Export a system role definition

1. From the System Roles page, select the role that you want to create an export definition for and click **Export role definition**. The Save as screen appears.
2. Browse to the directory where you want to save the file and enter a file name.
3. Click **Save**.

Import System Roles

If you create a new role that will use many of the same settings as another role, you can create an export definition of the role, make the necessary changes to it, and import the definition to create a new role.

Warning: When you export an existing role, the Name and ID elements in the XML file will be that of the existing role. Before you import the XML file, change the Name and ID to that of the new role. If you leave the existing Name and ID, when you import the role, it will overwrite the existing role rather than creating a new one.

Import a system role definition

1. From the System Roles page, click **Import role definition** under **Tasks**. The Import System Role definition screen appears.
2. Browse to the XML file you want to import as a role definition.
3. Click **Save**. The role is imported. The name specified in the XML import file now appears in the list of roles on the system roles page.

Define Home Page Permissions for Roles

From a system role, you can easily specify whether or not users in that role can customize their home pages.

What users actually see on their home pages depends on several factors. The first time users in a given role log in, they will see a certain set of tasks on the home page. These are tasks you specify to display on the home page for the role when you set up that role.

For more information, see Assign Tasks to a System Role on page 20.

If you deny the role the ability to customize home pages, all users in the role will always see the same set of tasks on their home pages. If you grant the role the ability to customize home pages, users in the role have control over what appears on their individual home pages. They can include additional items and delete the default tasks you specified to display for the role.

Define home page permissions for a system role

1. From a system role record, click **Define home page permissions** under **Tasks**. The Define home page permissions screen appears.
2. Mark an option to specify rights to the home page for this role—whether to grant or deny users the ability to customize their home pages or whether to not set home page permissions for the role.
   - If you mark to grant the ability, users in this role can modify their home pages unless they belong to another role that denies this permission.
   - When you mark to deny the ability, users cannot modify home pages even if they belong to another role where rights are granted.
   - When you mark the option to not specify, users in this role cannot customize their home pages unless they also belong to another role which grants permission to do so.
3. Click **Save**. You return to the system role record.

Assign Tasks to a System Role

When configuring a role, you specify the tasks to which the role has access. For example, while “Marketing Coordinator” and “Marketing Manager” roles both center around managing direct marketing, their requirements and job duties differ greatly—difference that needs to be reflected in the tasks to which each role has access.

Because tasks are simply navigational elements, they are not secured in the same way as actual feature permissions. If no features within a particular task are granted for a role, then even if that task is specifically granted to the role, it will not be visible (and directly accessible) to the users in that role. Tasks can either be granted or not specified. There is no deny option for tasks.

For more information, see Relationship Between Tasks and Features on page 20.

Note: System Administrators can assign a user to a system role they create, then log in as that user to determine if the features and other items they configured for the role display as intended. For more information, see the *Administration Guide*.

Assign a task to a system role

1. From a system role, select the Tasks tab.
2. Click **Assign tasks**. The Assign Tasks screen appears.
3. Select a functional area and mark the checkbox for a task to grant access to that task for users assigned to this system role.

   When you grant access to a task and click **Display on home page**, the task appears on the Home page of all users assigned to the role. However, if the role grants users rights to customize the Home page (and they are not assigned to any other role that denies those rights), users can remove tasks if they want to.

   Any tasks to which a user has access, but that have not been selected to display on the Home page are still available to the user through the functional area.
4. Click **Save** and return to the Tasks tab.

Relationship Between Tasks and Features

If no features within a particular functional area task are granted for a role, then even if that task is specifically granted to the role, it will not be visible (and directly accessible) to the users in that role. At least one feature applicable to the functional area must be granted for that task to appear in the functional area for a user assigned to the role.

Additionally, when you grant certain tasks, it grants the minimum underlying features necessary for a user to actually complete the task. The rules governing this behavior are:

Task Type	Feature Granted
Go To page	Page expression form for that page (if any)
Show Form	That form + post action Go To page expression
Launch Business Process	The business process
Record operation	The record operation

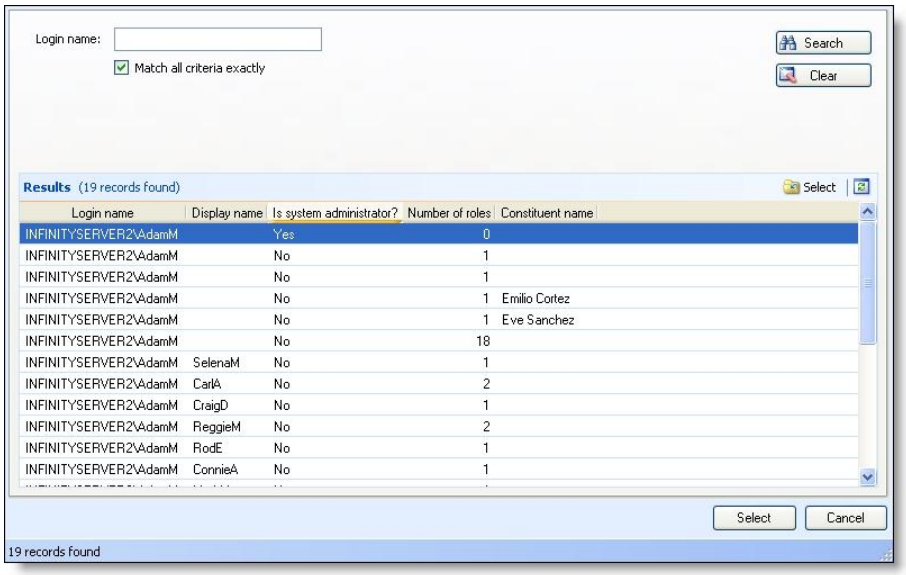
Assign Users to a System Role

On the Users tab of a system role record, you can assign individual users to the role.

Note: System Administrators can assign a user to a system role they create, then log in as that user to determine if the features and other items they configured for the role display as intended. For more information, see Run the Program as a Selected User on page 6.

Assign an existing user to a system role

1. From a system role, select the Users tab. The Users tab contains a list of users assigned to this system role.
2. On the Users tab, click **Add**. The search screen appears.



3. Enter the login name of the user you want to add to the role and click **Search**.
4. Select the user from the results grid and click **Select**.
5. You return to the Users tab of the system role record. Users entered this way appear in the list with the **Synchronized** column unmarked, indicating that they were not added via an Active Directory group. Synchronization is performed when Active Directory groups are added as users so that membership in the group is always in sync with users in the application, so it is not applicable for users added individually.

   Entering all your users in this way can be time-consuming when you have many users. The Groups tab enables Active Directory support for these situations.

Edit Users in a System Role

You can edit system role users to update the constituent security and site access for the user.

Note: System Administrators can assign a user to a system role they create, then log in as that user to determine if the features and other items they configured for the role display as intended. For more information, see the Administration Guide.

Edit a user in a system role

1. From a system role record, select the Users tab.
2. Select the user you want to edit and click **Edit**. The Edit system role user screen appears.
3. You can make the necessary changes to the user in the role.
4. Click **Save**. The system role user changes will be in effect the next time the user logs in.

Remove Individual Users from a System Role

Users are assigned to system roles that provide access only to the tasks and areas of the application needed to successfully complete their specific job responsibilities. As a user's job responsibilities change, you can adjust the system roles they are assigned to. You can also remove a user from a system role when the job responsibilities no longer match the access granted by the assigned roles.

When you remove users from a system role, it does not remove them as application users and does not affect their membership in other roles to which they may belong.

Remove an individual user from a system role

1. From a system role record, select the Users tab.
2. Select the user you want to remove from the role and click **Remove**. A confirmation message appears.
3. Click **Yes**. The system role user changes will be in effect the next time the user logs in.

Go to User

From the Users tab of a system role record, when you select a user name, you can view the record of that user including the system roles to which they belong and tasks, features, and other functions to which they have access. The information on the Application user tabs is based on the permissions established for the system roles the user belongs to and is view only.

Assign Groups of Active Directory Users to a System Role

If you have established Active Directory user/group schemes, you can leverage that infrastructure when you establish access to your system roles. You can manage your users without the need to duplicate your *Windows* network directory.

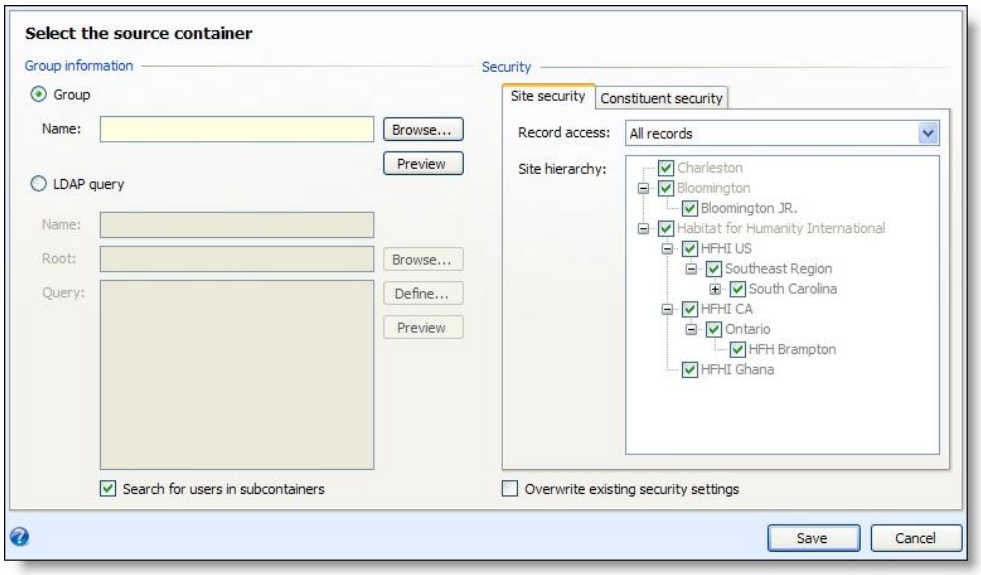
Note: An Active Directory user can be assigned to multiple roles.

You can assign multiple users to a system role either by adding an Active Directory group or via a LDAP (Lightweight Directory Access Protocol) query. LDAP is an Internet protocol that programs use to look up information from a server.

The Groups tab of a system role record contains a list of Active Directory groups and LDAP queries that have already been assigned to the role.

Assign an Active Directory group to a system role

1. From a system role, select the Groups tab. The Groups tab contains a list of Active Directory groups and LDAP queries that have been added to the role.
2. On the Groups tab, click **Add**. The Select the source container screen appears.



3. To add an Active Directory group, mark the **Group** option and click **Browse**. The Windows Select Group screen appears.

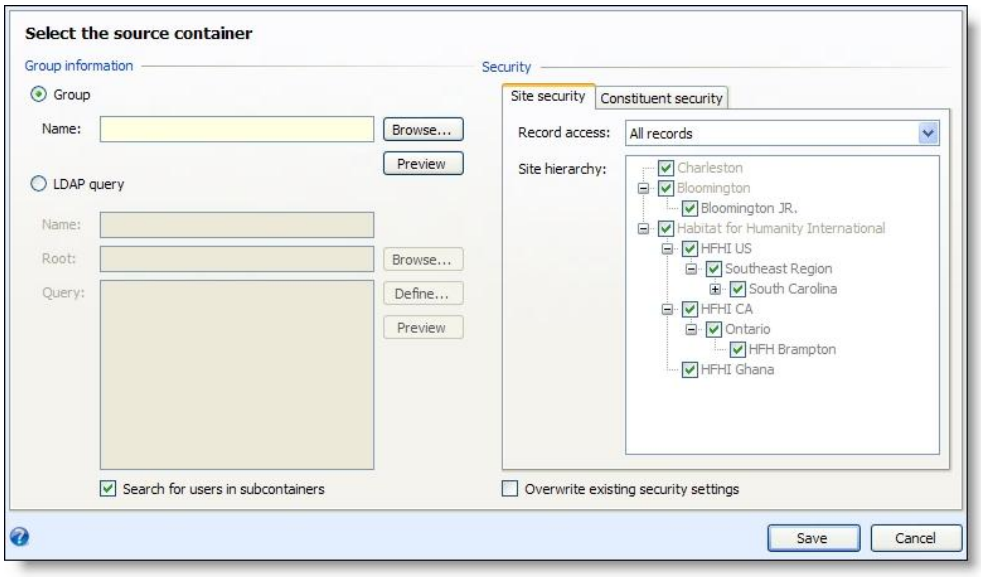
   For more information about the items on this screen, click the question mark on the screen title bar and drag it over an item.

Tip: You can display a list of users in the selected group by clicking the **Preview** button

4. Select the group you want to add to the role and click **OK**.
5. Mark the **Search for users in subcontainers** checkbox to include users in any groups within the group you specified. If you unmark the checkbox, the program returns only those users found explicitly within the specified group.
6. Click **OK** to save the user. You return to the Users tab of the System Role record. The saved Active Directory group now appears in the list on the Groups tab, but none of the users in that Active Directory group appear on the Users tab yet because synchronization has yet to take place with *Windows*. Once synchronization occurs, users in the Active Directory group appear on the Users tab, with a checkmark in the **Synchronized** column. For more information, see Synchronize Users in Windows and Blackbaud Groups on page 25.

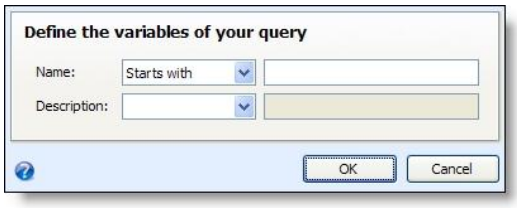
Assign a group to a system role using an LDAP query

1. From a system role, select the Groups tab. The Groups tab contains a list of Active Directory groups and LDAP queries that have already been assigned to the role.
2. On the Groups tab, click **Add**. The Select the source container screen appears.



3. Select **LDAP Query**.
4. Mark the **Search for users in subcontainers** checkbox to search for users in any groups found within your query. If you leave the checkbox unmarked, only those users found explicitly within the query results are returned.
5. Enter a name for the LDAP query.
6. To specify where the program should begin the search, click **Browse** and select the desired location within your organization's Active Directory structure. When you select a location, it appears in the **Root** field.

   Setting this "starting point" can greatly improve the performance of your LDAP query.
7. In the **Query** field, you can manually type in a valid LDAP query. If you are not familiar with LDAP syntax you can use a wizard to build a simple query.
   a. Click **Define**. The LDAP query wizard appears.



   b. Enter the information describing the users you are looking for.
   c. Click **OK** to save the query and return to the Select source container screen. The query you created with the wizard appears in the proper syntax in the **Query** field.
8. You can click **Preview** to view a list of users found by your query.
9. Click **Save** to assign the users included in your query to the selected system role. The saved LDAP query now appears in the list on the Groups tab, but none of the users in that LDAP query appear on the Users tab yet because synchronization has yet to take place with *Windows*. Once synchronization occurs, users in the LDAP query results appear on the Users tab, with a checkmark in the **Synchronized** column. For more information, see Synchronize Users in Windows and Blackbaud Groups on page 25.

Edit User Groups

You can edit the group properties or LDAP query that defines a group.

Edit a user group

1. From a system role, select the Groups tab.
2. Select a group and click **Edit**. The Select the source container screen appears. Make changes as necessary. For more information, see Assign Groups of Active Directory Users to a System Role on page 22.
3. Click **Save**. You return to the Groups tab.

Delete User Groups

When you delete a user group it does not initially remove any users from a role. However, because the group no longer exists in the role, when you click **Synchronize** or run the Role Sync utility, the users in the deleted group are automatically removed as users from the role.

Delete a user group

1. From a the system role, select the Groups tab.
2. Select the group to remove and click **Delete**. A confirmation message appears.
3. Click **Yes**.

Synchronize Users in Windows and Blackbaud Groups

When you click **Synchronize** on the Groups tab, the program gathers a complete list of users in all specified groups and LDAP query results. The role is then updated by adding the users who are not currently assigned to the role and removing users who were previously synchronized but who are not currently in the query results or part of the specified Active Directory group.

Note: Even though you can manually remove a synchronized user, the user is re-added during synchronization if nothing else changes about the user's membership in the list of Active Directory groups and LDAP queries defined for the system role.

This process can be automated with the RoleSync.exe utility (available in the AdminUtils folder of your program installation) which is a simple command line application that can be used from all common administrative tools (batch files, wscript, at command, etc.). You can use the *Windows* Scheduled Task Wizard to schedule regular synchronizations via the RoleSync utility.

Assign Feature Permissions to a System Role

When establishing security for features, deny always take precedence over any other setting. So if a user belongs to multiple roles and in any one of those roles Feature A is denied, that user will not have access to Feature A, even if access to that feature is granted in another role to which the user belongs. If in one of the user's roles Feature B is granted, but in another role Feature B is not specified, the user will have access to Feature B.

- Deny overrules everything else.

- Grant overrules no setting.
- If a feature is not specified in any role to which a user belongs, the user will not have access to it.

There is a close relationship between setting permissions for features and tasks because tasks are mainly navigation elements to maneuver among features. For more information, see Relationship Between Tasks and Features on page 20.

When you grant permissions for ad-hoc queries to a role, you must grant rights to the root query view for the feature in the tree view. The user will not be able to create new ad-hoc queries without access to the root query view, such as constituents or mailings. For more information, see Query View Permissions in Features on page 27.

Grants to a business process only permits the user to launch the business process (or the pre-process edit screen if one exists). In most cases, granting the business process is what makes the **Start process** button visible to a user.

Because dashboards are driven by datalists, when a dashboard is granted for a role, the datalists that populate that dashboard are implicitly granted. The implicit granting of datalists for use with dashboards is similar to the following example. If a user has rights to a screen that employs a drop-down list, the user is implicitly granted rights to the datalist that populates the drop-down. When you grant rights to a dashboard, it is not necessary to also grant the datalist(s) used by the dashboard.

Note: Granting rights to features that implicitly grant rights to associated features does not result in those associated features showing as granted in the feature tree.

Even if any datalists used by a dashboard are expressly denied, the denial has no affect on the ability of the user to access the dashboard. However, denying the datalist prevents it from being accessible by the members of the role in other areas of the program.

Not every feature requires that you set “Grant” or “Deny” rights for a given role. You can choose to not set a permission for a feature in a role, in effect saying that role will not be used to determine access to that feature. Any users in that role who need access to the feature will have to be granted permission to it through another role to which they belong.

System Administrators can assign a user to a system role they create, then log in as that user to determine if the features and other items they configured for the role display as intended. For more information, see the Administration Guide.

You can also use a security setting in the Web.Config file to troubleshoot feature permissions for system roles. In the Web.Config file, change the ShowFeaturesEvenIfNoRights setting to “True.” In the program, users can now see links, buttons, and lists even if they don’t have rights. If users click options that they don’t have rights to, “access denied” messages appear. If their system roles should have rights, you can update the feature permissions. We recommend you only change the ShowFeaturesEvenIfNoRights setting in test environments.

Assign feature permissions to a system role

1. From a system role, select the Features tab. Any features that have already been permissioned for this role appear on the tab.
2. Click **Assign Feature Permissions**. The Assign feature permissions screen appears.
3. Select the feature area. The specific features for the feature area are displayed.
4. Right-click on the individual features for which you want to specify permissions for this role and click **Grant** or **Deny**.
5. At the top of the screen you can **Grant All**, **Deny All**, or **Clear All** permissions for every feature in a selected folder.
6. You can select a filter to limit the features displayed.

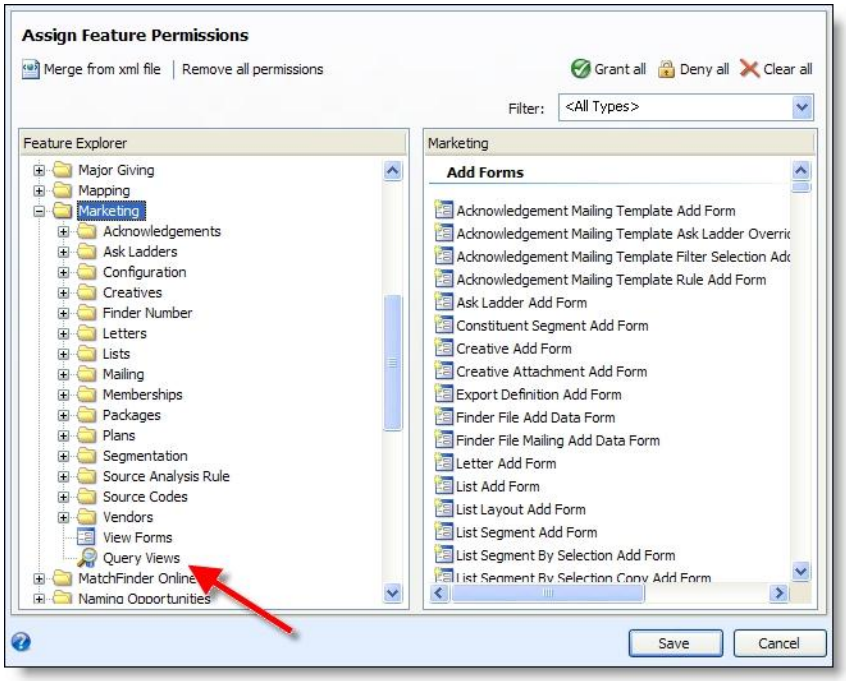
7. You can clear all grant and deny feature permissions for the features in the role by clicking **Remove all permissions**.
8. When you select **Merge from xml file** you can browse to a saved XML file you may have exported from another role and merge the feature permission settings from that file into the settings for this role.

Warning: If there are any discrepancies between existing feature permissions and those brought in from the XML file, the settings in the XML file will overwrite the existing settings. For example, if an existing setting grants rights to a feature and the XML file denies rights, the feature will be denied after merging.

9. Click **Save**. You return to the Features tab where your selections appear.

Query View Permissions in Features

All queries are based on a source view. Source views determine the child views and field categories available to include in a query. The record type on which a query is based determines in which features the query is available and how it is used in the program.



Also, users are not able to access any saved queries that use fields from query views to which they have not been granted rights. Any denied queries do not appear for that user when the user logs into the program.

For a system role, you can specify constituent security to limit access to certain constituents. Constituent security applies to queries and query results. A user without rights to security Group A will not see information pertaining to Group A constituents in query results. Queries that contain constituent records to which the user does not have access in the results will still appear in the Ad-hoc Query List for a user (if that user has rights, through a role, to the appropriate query views), but the user will not be able to see the restricted records in the results.

Export Feature Permission Settings

You can export the feature permission settings you establish for a role to an XML file. This is similar to an export of a system role definition, but enables you to later import only feature settings rather than an entire role definition.

Importing feature settings can be useful if you are creating a new role that will have similar permissions as an existing role and want to import the settings as a starting point rather than specifying all the feature permission settings in the new role manually.

Export feature permission settings to XML

1. From a system role, select the Features tab.
2. Click **Export to xml**. The Save as screen appears.
3. Browse to the directory where you want to save the file and enter a name.
4. Click **Save**. To import these settings into another role, open the new role, select the Features tab, and click **Assign feature permissions**. Click **Merge from xml file** and browse to the file you saved during the feature permission export.

Assign Code Table Permissions to a System Role

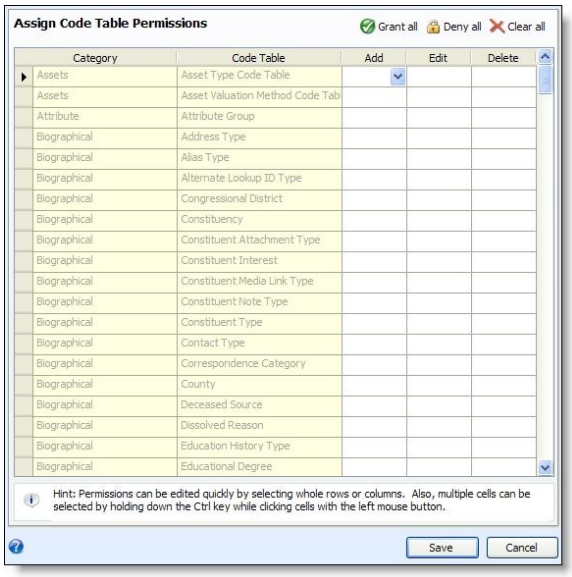
When you assign code table permissions, you specify whether users in the system role can add entries to a table "on the fly," edit existing entries, or delete entries. For example, when you add or edit a constituent record, users with add or edit rights to the **Title** table can press **F7** or click the name of the **Title** field to access a screen where they can edit the existing code table entries for it or add new ones.

Access to the table itself is determined by whether or not the role has access to the feature(s) where the table appears.

Note: System Administrators can assign a user to a system role they create, then log in as that user to determine if the features and other items they configured for the role display as intended. For more information, see the Administration Guide.

Assign code table permissions to a system role

1. From a system role, select the Code Tables tab. Any code tables that have already been permissioned for this role appear on the tab.
2. Click **Assign Code Table Permissions**. The Edit code table permissions screen appears.



3. Specify whether rights are granted or denied to add, edit, or delete entries for specific tables.
4. Click **Save**. You return to the Code Tables tab where your selections appear.

Assign code table entry permissions

Access to constituent documentation—notes, links, and attachments—can be secured by the type of documentation. From the Code Tables tab of a system role, you can deny access to a selected types of note, links, and attachments. For example, you may have an executive note type for top-level or confidential information. You could deny access to this type of note to all roles except for the executives. Documentation types that have been denied for a role will not display on the constituent records for users in that role.

1. From a system role, select the Code Tables tab.
2. In the **Code table entry permissions** grid, click **Assign permissions**. The Assign code table entry permissions screen appears.
3. You can select the items to deny permission for. Select the items and click **Deny all**.
4. Click **Save** to return to the Code Tables tab. Users for the system role will not have access to items with these code table entries.

Assign Batch Type Permissions to a System Role

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.

As with other types of permissions in the program, batch administrative permissions are intertwined with feature permissions. Even when a role is granted administrative privileges to a type of batch on the Batch Types tab, in order for users to actually do anything with those privileges, the role must be granted access to the appropriate features under the **Batch** node on the Assign Feature Permissions screen. For example, even with administrative

rights granted for a batch type, a role must be granted access to the Batch Template Add form in order to create new batch templates of that type.

Security granted on the Batch Types tab gives users of a role rights to do anything with any batch template of that type, and any batch instances built from any of these templates (with the appropriate feature permissions).

Note: System Administrators can assign a user to a system role they create, then log in as that user to determine if the features and other items they configured for the role display as intended. For more information, see the Administration Guide.

Assign batch type administrative permissions to a system role

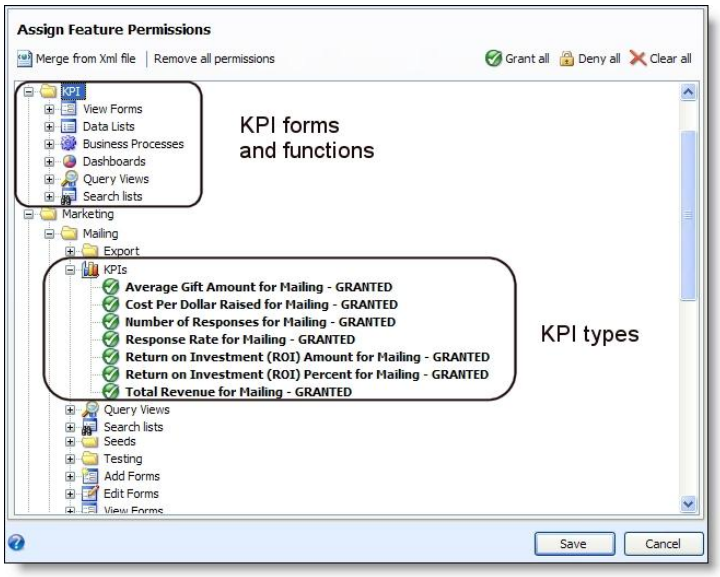
1. From a system role, select the Batch Types tab. Any batches that have already been permissioned for this role appear on the tab.
2. Click **Assign administrative permissions**. The Administer Batch Types screen appears.
3. Right-click on the individual batch types for which you want to specify permissions for this role and click **Grant** or **Deny**. Click **Clear** to remove permissions for a selected batch type.
4. You can click **Clear All** to remove permissions for every batch type.
5. Click **Save**. You return to the Batch Types tab where your selections appear.

Assign Key Performance Indicator Instance Permissions to a System Role

On the Features tab of a system role, you can specify whether a role has access to a Key Performance Indicator (KPI) type. KPI types represent the different kinds of KPIs you can create. When you grant this access, the users in the role have access to every KPI instance of that type. KPI instances are the actual individual KPIs you have created. For example, there are KPI types to help measure the effectiveness of an appeal. You might have three KPI instances of this type, with each measuring a different appeal.

To increase the granularity of KPI security, you can turn off access to the KPI type on the Features tab and, on the KPIs tab of a system role, select the specific instances of a KPI type to which a role has access.

For example, on the screen below, users in this role would have access to all instances created for the KPI types with permission granted, no matter what instances were specified on the KPIs tab. Instances specified on the KPIs tab would affect the other types, since they are not explicitly permissioned on the Features tab. The actual functions that can be performed on a KPI (editing the parameters or updating the KPI value for example) are determined by your settings in the KPI forms and functions section.



Note: System Administrators can assign a user to a system role they create, then log in as that user to determine if the features and other items they configured for the role display as intended. For more information, see the Administration Guide.

Assign permissions for a KPI instance to a system role

1. From a system role, select the KPIs tab. Any key performance indicators that have already been permissioned for this role appear on the tab.
2. Click **Assign KPI instances**. The Edit assigned KPI instances screen appears.
3. All KPI type templates appear on the left grouped under feature areas. When you select a type, any instances defined with that template appear on the right.
4. Mark the checkbox by any instance on the right to grant rights to that instance for the role.

Note: If the role has full access to the KPI type in Features, they will be able to access every instance of that type no matter what the settings are on the Edit assigned KPI instances screen. The settings on this screen are applicable only when full rights to the type are not granted.

5. Click **Save**. You return to the KPIs tab where your selections appear.

Assign Smart Field Permissions to a System Role

On the Features tab of a system role, you can specify whether a role has access to smart fields on various types of records. When you grant this access, the users in the role have access to the Smart fields tab on those records. To increase the granularity of smart field security, on the Smart Fields tab, you can select the specific instances of each type of smart field to which a role has access. To configure smart fields, you must grant permission on the Tasks and Features tabs.

Assign Attribute Category Permissions to a System Role

On the Features tab of a system role, you can specify whether a role can access attributes on various types of records. When you grant access, users in the role can view the Attributes tab on those records. To further define attribute security for a system role, select the Attribute Categories tab on the record of the role.

Under **Attribute category permissions**, you can select whether to grant or deny users in the role access to each attribute category configured for your organization. To allow users to configure attribute categories, you must grant permission on the Tasks and Feature tabs.

Tip: To determine if features and items configured for a system role appear as intended, system administrators can assign a user to the role and then log in as that user. For information about how to log in as another user, see the Administration Guide.

Assign Permissions to System Roles

On the Permissions tab, you can grant rights to related pieces of functionality. Permissions are collections of tasks and features that are necessary to perform actions such as adding a constituent. They can include access to items such as forms, lists, queries, and other items as necessary.

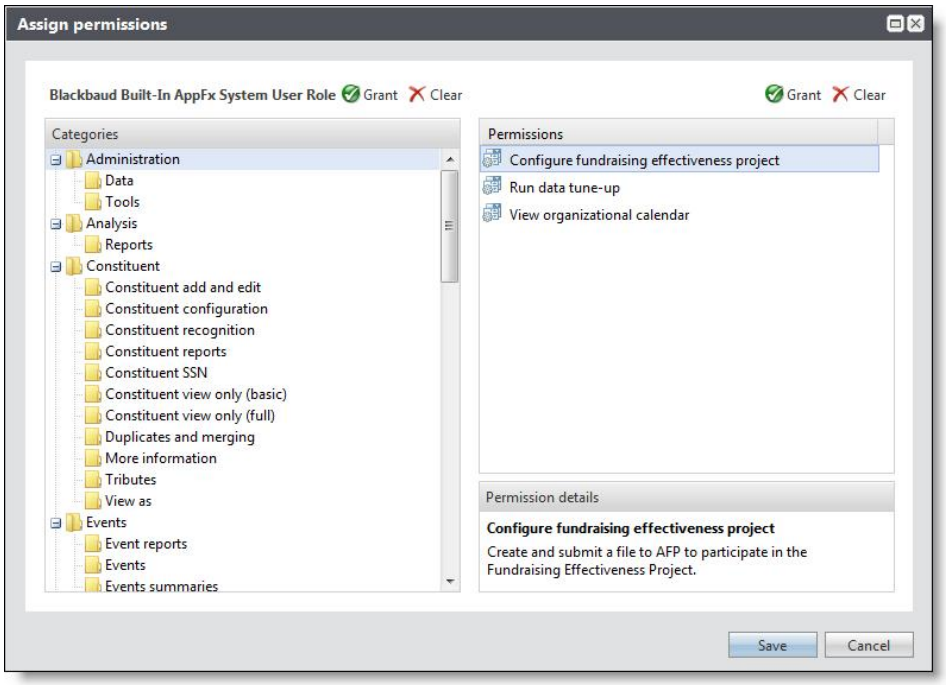
Permissions allow you to simultaneously grant rights to a multiple tasks and features instead of granting rights to individual forms, lists, and other items one at a time on the Tasks and Features tabs. They are designed to allow you to easily assign rights to related tasks that groups of users are likely to need.

Permissions are grouped into categories based on functional areas in the program such as *Administration* and *Events*, and you can grant rights to entire categories as well as to individual permissions.

After you assign permissions to a system role, you can access them through the Permissions tab to view the tasks and features included with the permission. On the permission record, the Features tab lists the forms, tasks, reports, and other items that are included with the permission. The System Roles tab lists all the system roles that the permission is assigned to.

Assign permissions to a system role

1. From a system role, select the Permissions tab. All permissions assigned to the role appear in the grid.
2. Click **Assign permissions**. The Assign Permissions screen appears.



3. Under **Categories**, a hierarchy of permissions appear in folders that are organized based on functional areas in the program. When you select a folder, individual permissions appear under **Permissions**, and when you select a permission, a description appears under **Permission details**.

   - To grant rights to all permissions in a folder, select it and click **Grant** above **Categories**.

   Note: When you grant rights to an entire folder, related permissions in other folders may also be granted.

   - To grant rights to a particular permission, select it and click **Grant** above **Permissions**.

4. Click **Save**. You return to the Permissions tab where your selections appear.