

Security Guide

03/01/2016 Blackbaud CRM 4.0 Security 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.

Security-2016

Contents



SECURITY	1
Fundamentals of Security	1
APPLICATION USERS	3
Search for Users	4
Application User Records	4
Add an Application User	4
Edit Users	6
Delete Users	7
Edit the Link Between a User and Constituent Record	7
Link an Application User to a Constituent Record	7
Grant/Revoke Users Administrator Rights	7
Run the Program as a Selected User	7
Organizational Units	8
Organizational Unit Record	10
Application Users Page	11
Manage System Roles of an Application User	11
Add System Roles to a User	11
Edit a System Role for a User	12
Remove a System Role from a User	12
View CMS Roles Associated with an Application User	13
View Business Processes Owned by an Application User	13
View Tasks Associated with an Application User	14
View Features Associated with an Application User	14
View Code Tables Associated with an Application User	15
View Batch Types Associated with an Application User	15
View KPIs Associated with an Application User	15
SYSTEM ROLES	17
System Role Security General Rules	17
Manage System Roles	18
System Role Records	18
Add System Roles	19
Edit System Roles	19
Delete System Roles	20
System Role Report	20
Copy System Roles	20
Export System Roles	20
Import System Roles	21

Define Home Page Permissions for Roles	21
Assign Tasks to a System Role	22
Relationship Between Tasks and Features	22
Assign Users to a System Role	23
Edit Users in a System Role	25
Remove Individual Users from a System Role	25
Go to User	26
Assign Groups of Active Directory Users to a System Role	26
Edit User Groups	28
Delete User Groups	28
Synchronize Users in Windows and Blackbaud Groups	29
Assign Feature Permissions to a System Role	29
Query View Permissions in Features	30
Export Feature Permission Settings	31
Assign Code Table Permissions to a System Role	32
Assign Batch Type Permissions to a System Role	33
Assign Key Performance Indicator Instance Permissions to a System Role	33
Assign Smart Field Permissions to a System Role	35
Assign Attribute Category Permissions to a System Role	35
Assign Permissions to System Roles	35
SITES AND SITE SECURITY	37
How Site Security Works	37
Account Systems	37
Acknowledgements	37
Address Processing Options	38
Batch	38
Benefit Catalog Items	38
Business Processes	39
Campaigns and Appeals	39
Code Table Entries	39
Constituent Documentation	39
Constituents	39
Constituent Mail Preferences	40
Site Options on Appeals	40
Correspondence	40
Designations and Fundraising Purposes	40
Direct Marketing	40
Donor Challenges	40
Events	41
Export	41
Giving Level Programs	41

Global Change	41
Grant Funding Plans	42
Import	42
Interactions	42
KPI Instances	42
Membership Programs	42
Merchant Accounts	42
Multicurrency	43
Name Formats	43
Opportunity Amount Ranges	43
Pledge Reminders	43
Prospect Plans	43
Prospect Research Requests	43
Queries and Selections	44
Query View Security	44
Queue	44
Receipts	45
Recognition Programs	45
Records with Multiple Sites	45
Records with No Site Assigned	45
Research Groups	45
Revenue and Recognition Credits	45
Smart Fields	46
Solicit Codes	46
Stewardship Plan Templates	46
Stewardship Plans	46
Tributes	47
Users and Sites	47
Volunteer Jobs	47
Filter Data by Site	47
Manage Sites	48
Add Sites	48
Edit Sites	49
Delete Sites	49
Edit Site Hierarchy	50
Site Search	50
Site Search Screen	51
Assign Sites to Records	52
CONSTITUENT SECURITY GROUPS	55
Configure Constituent Security Groups	55
Add Constituent Security Groups	55

Apply Security Groups to Groups of Constituents Via a Process	56
Assign Constituents Process Status and History	57
Job Schedule	58
Create a New Job Schedule	58
Create Job Screen	58
Edit an Existing Job Schedule	60
Delete an Existing Job Schedule	60
Generate WSF	60
Apply Security Groups to Individual Constituents	61
Edit Constituent Security Groups	61
Delete Constituent Security Groups	62
Security Group Record	62
Apply Constituent Security to a User in a System Role	62
Constituent Security Group Example	63
Relationship Between Feature and Constituent Level Security	63
 AUDIT TABLES	 65
Enable Audit Table	65
Audit Report	65
Disable Audit Table	68
Purge Audit Table	68
Dependencies on Audit Tables	68
Smart Field Dependencies on Audit Tables	68
Constituents Dependencies on Audit Tables	70
Revenue Dependencies on Audit Tables	71
Marketing and Communications Dependencies on Audit Tables	72

Security

Fundamentals of Security 1

Security in the program is determined by system roles, site security, and constituent group security. System roles determine the features, tasks, queries, and more to which your users have access, while sites can partition records and limit access. With constituent security groups, you can restrict access to specific groups of constituent records. 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 [Organizational Unit Record](#) on page 10 and [Assign Groups of Active Directory Users to a System Role](#) on page 26.

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

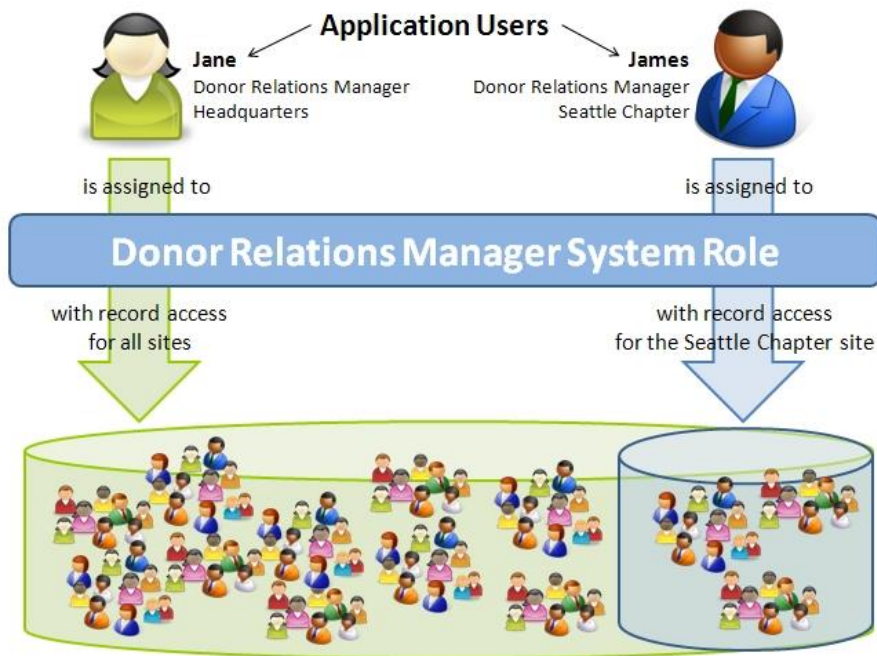
These are smallest units in the security structure. An application user represents each individual with access to the system. Each application user is associated with a network domain and a user name. The application uses Windows Authentication for secure user access. However, if the application runs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

Sites

An organization with one location or office might not use site functionality, whereas other organizations may have many sites. With sites, you have the ability to manage a complex and multi-tiered hierarchy of offices, chapters, or affiliates. A national organization with regional offices might establish site security with a headquarters site and regional sites beneath it in a hierarchy. A university may have one central university foundation with separate offices representing the different colleges beneath it. These organizations need a more complex way to set up system security and assign different rights and permissions to users in the different offices.



Constituent security groups

There is also a separate layer of security that can be used, constituent security groups. With security groups you can limit access to a specific group of constituent records. For example, your organization may interact with celebrities and therefore have constituent records for them in your system. If you want to limit access to those records for privacy, you could create a constituent security group for them. For most users, when you associate them with a system role, you would set constituent security to limit record access to only records with no security group assigned. For the few users who should have access to the celebrities' constituent records, you would set constituent security to include all records or to include that particular constituent security group.

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

Search for Users	4
Application User Records	4
Organizational Units	8
Organizational Unit Record	10
Application Users Page	11
Manage System Roles of an Application User	11
View CMS Roles Associated with an Application User	13
View Business Processes Owned by an Application User	13
View Tasks Associated with an Application User	14
View Features Associated with an Application User	14
View Code Tables Associated with an Application User	15
View Batch Types Associated with an Application User	15
View KPIs Associated with an Application User	15

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.

Application users can be associated with one primary, or default, site. However, access to data is based on the site (or sites) selected when the application user is assigned to a system role. For more information about sites and system roles, see *Sites and Site Security* on page 37 and *System Roles* on page 17.

After you add users to the system, you must assign them to system roles to determine what areas of the system they can access. You can also adjust their roles, edit the user's link to a constituent record, and send a password reset link.

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's name, 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.

You can also associate a site with the user. This is the default site for the user, so it will appear by default on records secured by site that the user adds. This site is also used to define “My site” and “My site’s branch” in filters. The user’s access to data is based on how site and constituent security permissions are established on the

system roles to which the user belongs. For more information, see *Sites and Site Security* on page 37 and *Constituent Security Groups* on page 55.

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.

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.”

► 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. In the **Site** column, select the site at your organization to assign each user. This is the default site for the user, so it will appear by default on records secured by site that the user adds. This site is also used to define “My site” and “My site’s branch” in filters. The user’s access to data is based on how site and constituent security permissions are established on the system roles to which the user belongs. For information, see *Sites and Site Security* on page 37 and *Constituent Security Groups* on page 55.
6. 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.

Add CMS User

This user has Supervisor rights and can manage Users and Roles.

Login name:

New password:

Confirm new password:

Email address:

First name:

Last name:

Save Cancel

- 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**.
7. 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 23.

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. In the **Site** field, edit the primary site of the user as necessary. This is the default site for the user, so it will appear by default on records secured by site that the user adds. This site is also used to define “My site” and “My site’s branch” in filters. The user’s access to data is based on how site and constituent security permissions are established on the system roles to which the user belongs. For information, see *Sites and Site Security* on page 37 and *Constituent Security Groups* on page 55.
4. 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 5.

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**.

5. 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.

Edit the Link Between a User and Constituent Record

If an application user also has a constituent record, from the Application User page, you can link the two records.

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."

Link an Application User to a Constituent Record

1. From an application user's record, click **Edit link to constituent** under **Tasks**.
The Edit application user screen appears.
2. 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. Click **Save**. You return to the application user 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 10.

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 26.

► **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.

Add an existing organizational unit

Name:

LDAP root:

User group:

User suffix:

Changes are made to the organizational unit using these credentials

User name:

Password:

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.

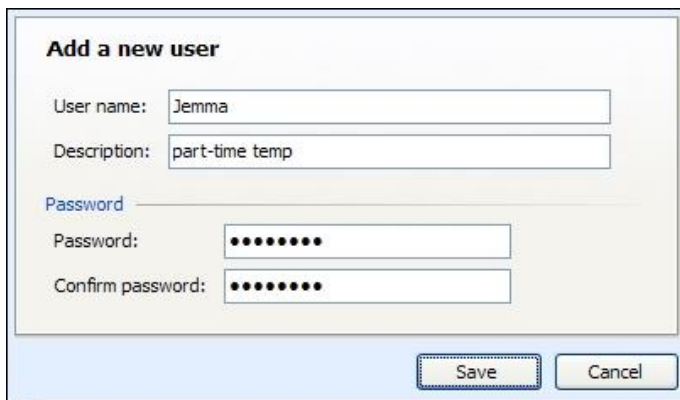
Organizational Unit Record

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, grant users administrative rights, and edit the primary site associated with the user or the link between the user and a constituent record.

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 7.

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

Warning: While you can manage system roles from a user record, we recommend you assign users to a system role from the record of the role. For information about how to assign users to a role, see [Assign Users to a System Role](#) on page 23.

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.

Warning: While you can assign system roles from a user record, we recommend you assign users to a system role from the record of the role. For information about how to assign users to a role, see [Assign Users to a System Role](#) on page 23.

► 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 4.
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. On the Site security tab, select the record access for the user within the role based on site security. You can assign access to all records, records with no site assigned, records for specific sites, or records accessible within a branch of the site hierarchy. For information about site security, see [Sites and Site Security](#) on page 37.
6. On the Constituent security tab, select the record access for the user within the role based on constituent security groups. You can assign access to all records, records with no security group assigned, or records for specific security groups. For information about security groups, see [Constituent Security Groups](#) on page 55.
7. 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.

Warning: While you can manage system roles from a user record, we recommend you edit the user assignment of a system role from the role record. For information about how to edit the user assignment, see [Edit Users in a System Role](#) on page 25.

► 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 4.
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 11.
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.

Warning: While you can manage system roles from a user record, we recommend you remove the user from a system role through the role record. For information about how to edit the user assignment, see [Remove Individual Users from a System Role](#) on page 25.

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:

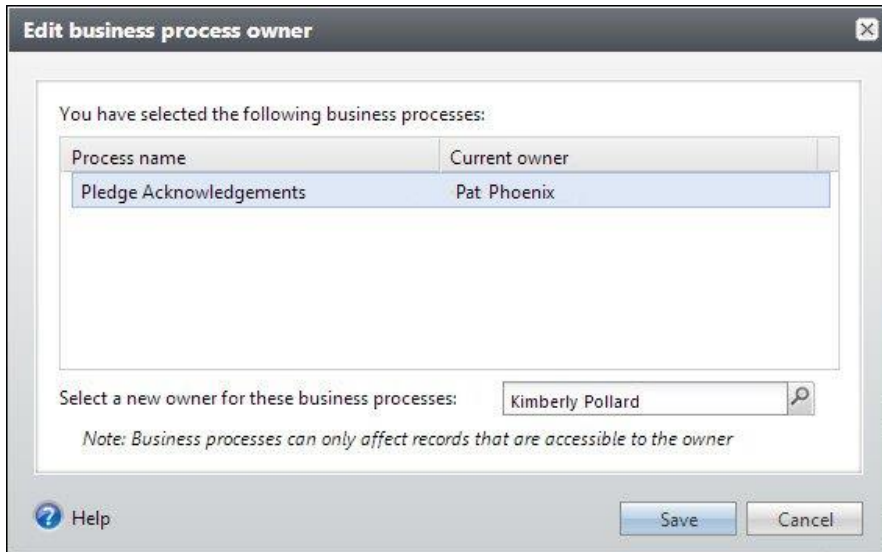
- To edit the owner for a single business process, select the business process in the grid and click **Edit owner** under the business process.
- To edit the owner for multiple business processes at one time, select each process and click **Edit owner** on the action bar.
- To edit the owner for all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

System Role Security General Rules	17
Manage System Roles	18
Assign Tasks to a System Role	22
Assign Users to a System Role	23
Assign Groups of Active Directory Users to a System Role	26
Assign Feature Permissions to a System Role	29
Assign Code Table Permissions to a System Role	32
Assign Batch Type Permissions to a System Role	33
Assign Key Performance Indicator Instance Permissions to a System Role	33
Assign Smart Field Permissions to a System Role	35
Assign Attribute Category Permissions to a System Role	35
Assign Permissions to System Roles	35

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.
- Constituent security groups can be used to limit access to certain constituents for a role. For example, you could create a "Major Donors" constituent group and limit access to that group to only selected roles. Similarly, sites can be used to limit access to certain record types such as events and appeals.

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.

System roles
Constituent Administration - System Role

Description: Maintaining and ensuring quality of constituent data, including batch entry, merging, and reporting.
Can customize home page: Yes

Tasks Users Groups Features Code Tables Batch Types KPIs Smart Fields

Assigned tasks (23 items) Assign tasks Display on home page

Name	Description	Functional area	Display on home page
Administration			
Manage household settings	Provides an interface for managing household settings.	Administration	No
Interaction categories and subc...	Provides an interface for managing interaction categories and interactions ...	Administration	No
Response categories and respo...	Provides an interface for managing response categories and responses wit...	Administration	No
Manage educational history	Create and manage the academic catalog and educational institutions.	Administration	No
Manage corporate relationship t...	Provides an interface for managing corporate relationship types within the ...	Administration	No
Manage solicit codes	Manage solicit codes	Administration	No
Constituents			
Duplicate constituent report	View a report of possible duplicate constituents found by a duplicate consti...	Constituents	No
Batch search	Search for and view batches.	Constituents	No
Add an organization	Add a new organization constituent.	Constituents	No
Constituent merge	View, add, and edit constituent merge processes and configurations.	Constituents	No
Merged constituent search	Trace a merged constituent to the constituent into which it was merged.	Constituents	No
Manage constituent group types	Add, edit and delete constituent group types.	Constituents	No
Constituent search	Search for and view constituent records.	Constituents	No

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 20.

► 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 22.

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 “Constituent Data Entry Personnel” and “Constituent Administrators” roles both center around your constituents, their requirements and job duties differ greatly—a difference that needs to be reflected in the tasks to which each role has access.

Note: You can add tasks to functional areas and the home page. However, the *Events*, *Prospects*, and *Membership* areas are actually pages in *Blackbaud CRM*. While you cannot assign tasks to pages, pages can have actions. For more information about actions, see the *Page Designer Guide*.

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 22.

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.

Note: *Events*, *Membership*, and *Prospects* are built as pages, not functional areas. While you cannot assign tasks to pages, pages can have actions. For more information about adding actions to pages, see the *Page Designer Guide*.

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 Ex. Search for constituents	Page expression form for that page (if any) Ex. Constituent Page Expression Data View Form
Show Form Ex. Add an Individual	That form + post action Go to page expression Ex. Individual Add Form + Constituent Page Expression Data View Form
Launch Business Process	The business process
Record operation Ex. A custom task could be implemented to “Delete Constituent.”	The record operation The feature associated with a Delete Constituent task is Delete Constituent (the Record operation).

Assign Users to a System Role

Users may have a site specified on their application user records, which is the primary or default site associated with them. On the Users tab of a system role record, you can assign individual users to the role. When you add users to a system role, you can determine which sites they can access as part of the system role, as well any constituent security for the user in this role. The site on the application user and its associated constituent record are usually the same. For more information, see [Application Users on page 3](#) and [Sites and Site Security on page 37](#).

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 7](#).

► 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.

Search screen showing results for 19 records found. The search criteria are: Login name: [] and Match all criteria exactly [checked].

Login name	Display name	Is system administrator?	Number of roles	Constituent name
INFINITYSERVER2\AdamM		Yes	0	
INFINITYSERVER2\AdamM		No	1	
INFINITYSERVER2\AdamM		No	1	
INFINITYSERVER2\AdamM		No	1	Emilio Cortez
INFINITYSERVER2\AdamM		No	1	Eve Sanchez
INFINITYSERVER2\AdamM		No	18	
INFINITYSERVER2\AdamM	Selenam	No	1	
INFINITYSERVER2\AdamM	CarlA	No	2	
INFINITYSERVER2\AdamM	CraigD	No	1	
INFINITYSERVER2\AdamM	ReggieM	No	2	
INFINITYSERVER2\AdamM	RodE	No	1	
INFINITYSERVER2\AdamM	ConnieA	No	1	

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.

► Assign a user to a system role

1. From *Administration*, click **Security**. The Security page appears.
2. Click **System roles**. The System Roles page appears.
3. To assign users, click the role name. The system role record appears.
4. Select the Users tab. The Users tab contains a list of users assigned to this system role.
5. On the Users tab, click **Add**. The Add system role user screen appears.

6. In the **Application user** field, search for the user.
7. On the Site security tab, select the type of record access for the user. You can optionally specify individual sites within the hierarchy. A user can be assigned access in this role to all records, to records with no site assigned, to records for specific sites, or to records accessible within a branch of the site hierarchy. For more information, see Sites and Site Security on page 37.
8. On the Constituent security tab, select the type of record access based on constituent security groups for this user. For more information, see Constituent Security Groups on page 55.
9. Click **Save**. The user is now assigned to the system role with the record access specified. Repeat this process as needed to assign additional users to system roles.

Note: Changes do not take effect immediately. For changes to take effect, you must log out, close your browser, and log back in.

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.
 - On the Site security tab, edit the type of record access for the user. You can optionally specify individual sites within the hierarchy. A user can be assigned access in this role to all records, to records with no site assigned, to records for specific sites, or to records accessible within a branch of the site hierarchy. For more information, see Sites and Site Security on page 37.
 - On the Constituent security tab, edit the type of record access based on constituent security groups for this user.
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.

► 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.

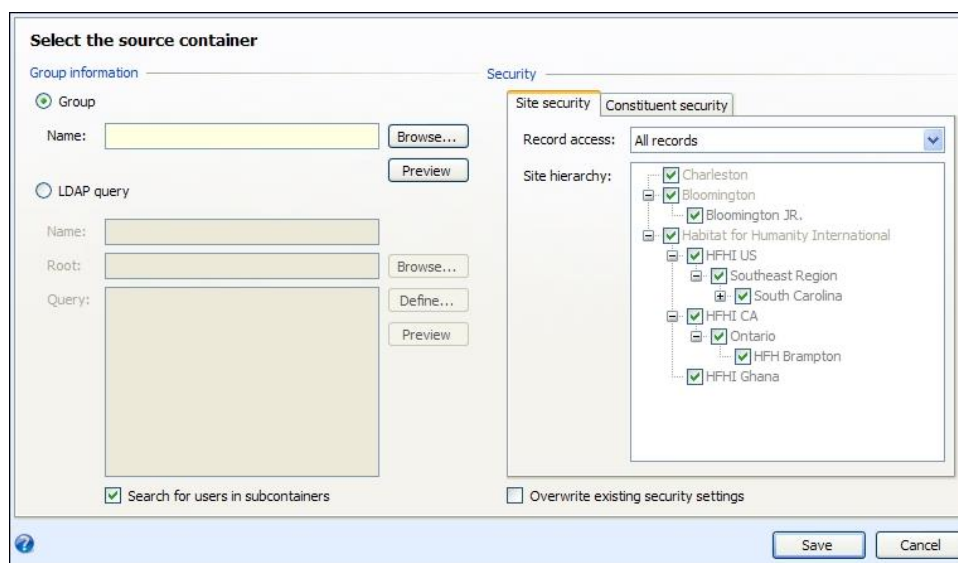
For more information about the items on this screen, click the question mark on the screen title bar and drag it over an item.

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 29.

► Assign a group to a system role using an LDAP query

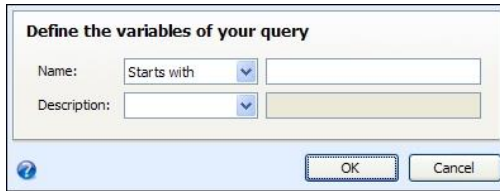
1. From a system role, select the Groups tab. The Groups tab contains a list of Active Directory groups and LDAP queries that have already been assigned to the role.
2. On the Groups tab, click **Add**. The Select the source container screen appears.



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 29.

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 26.
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 22.

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 30.

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 effect 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.

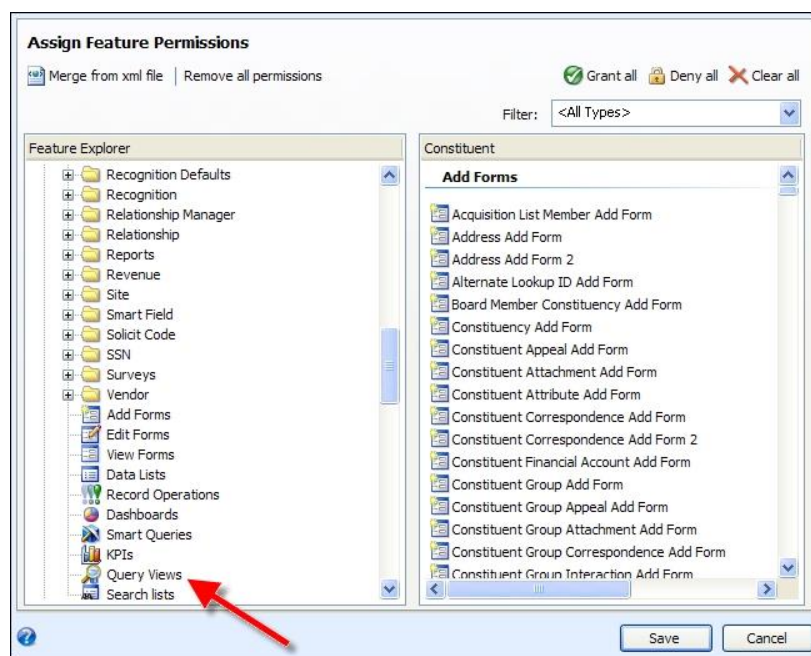
Warning: If there are any discrepancies between existing feature permissions and those brought in from the XML file, the settings in the XML file will overwrite the existing settings. For example, if an existing setting grants rights to a feature and the XML file denies rights, the feature will be denied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

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.



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

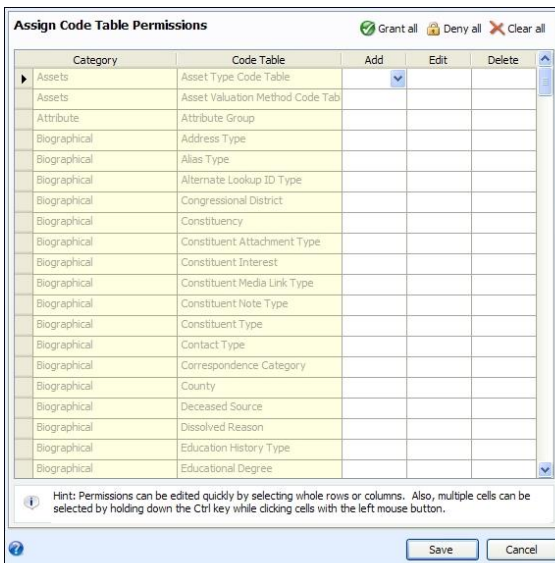
When you assign code table permissions, you specify whether users in the system role can add entries to a table “on the fly,” edit existing entries, or delete entries. For example, when you add or edit a constituent record, users with add or edit rights to the **Title** table can press **F7** or click 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

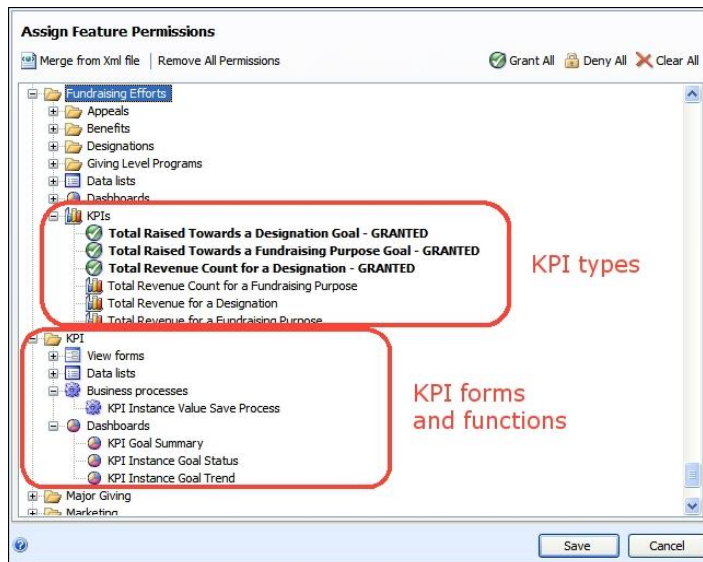
1. From a system role, select the Batch Types tab. Any batches that have already been permissioned for this role appear on the tab.
2. Click **Assign administrative permissions**. The Administer Batch Types screen appears.
3. Right-click on the individual batch types for which you want to specify permissions 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.

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 11.

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.

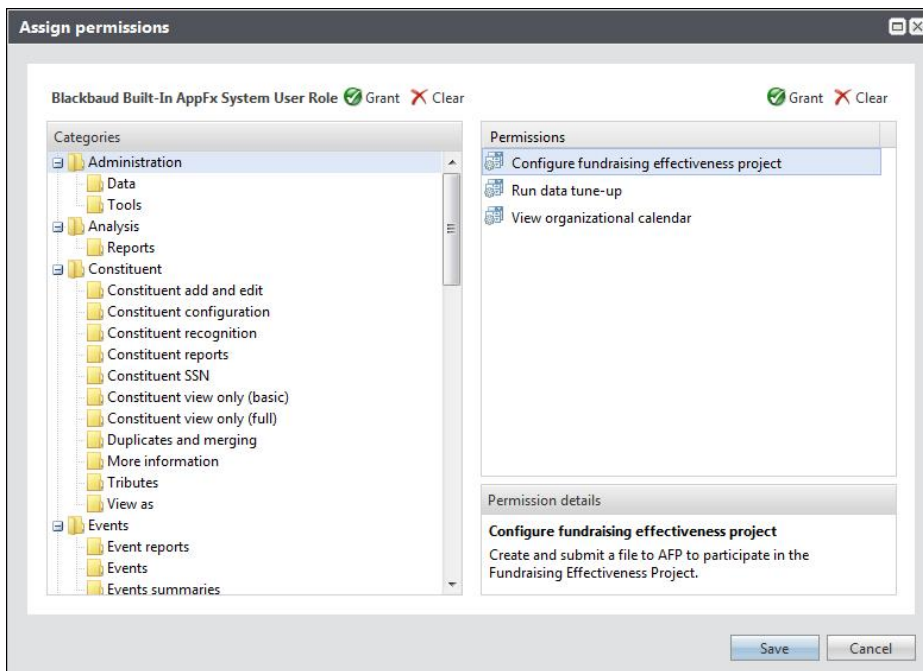
Permissions allow you to simultaneously grant rights to a multiple tasks and features instead of granting rights to individual forms, lists, and other items one at a time on the Tasks and Features tabs. They are designed to allow you to easily assign rights to related tasks that groups of users are likely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

Sites and Site Security

How Site Security Works	37
Filter Data by Site	47
Manage Sites	48
Assign Sites to Records	52

With sites, you have the ability to manage a complex and multi-tiered hierarchy of offices, chapters, or affiliates. A national organization with regional offices might establish a headquarters site with regional sites beneath it in a hierarchy. A university may have one central university foundation with separate offices representing the different colleges beneath it. These organizations need a more complex way to set up system security and assign different rights and permissions to users in different offices. Smaller or less complex organizations, such as an organization with only one office, might not need to use sites.

How Site Security Works

Site security allows you to secure data in your system based on the site with which it is associated. When a special events coordinator for the law school, for example, is searching for events, that user does not need to see (and probably does not want to see) every event for every department or college in the university.

This level of site security has two primary benefits. First, access to sensitive data can be restricted. A large, multi-site organization can ensure that each chapter or affiliate has access to its constituents and revenue information, but not access to information which belongs to another site. Second, site security offers a way to manage data so that users have access to only the data that is pertinent to them. Users do not have to search through a list of hundreds of records to find the ones for their site.

Account Systems

Each site in your organization should be associated with one general ledger account system. Your organization can configure and work with multiple general ledger account systems when site security is implemented and you have rights to work with multiple account systems.

Acknowledgements

Revenue and tribute acknowledgement letters can be associated with one or more sites, in order to allow users from different sites to create and use them.

You can restrict the following acknowledgement processes by site:

- Assign letters process
- Revenue acknowledgement process

- Tribute acknowledgement process
- Planned gift acknowledgement process
- Planned gift assign letters process

When you select a site, only users associated with the site can access the process. To allow users of all sites to access the process, select “All sites.”

Address Processing Options

The rules or address processing options an organization establishes to use when contacting constituents or supporters may be mandated at the top level of the organization or may be left up to individual sites within the organization. Address processing options can therefore be associated with all sites (by assigning no site to the record) or may be associated with one specific site.

When you add address processing options in *Communications*, you can assign site security to make each option available to all or selected sites. Users with limited site permissions may still view and select address processing formats assigned to all sites. However, only system administrators or users with access to all records or records with no site assigned can add, edit, or delete these formats. A system administrator or other user with the appropriate permissions can assign record access to a system role user in *Administration*. For information about how to assign site security to system roles, see *Assign Users to a System Role* on page 23.

Batch

Batch numbering schemes and batch workflows are system-wide and are not associated with sites. Batch templates, however, can be associated with all sites or a single, specific site. Batches inherit their site based on the site of the batch template. Users with access to site A for a system role will be able to work with batches and batch templates for site A only. Users with access to all sites for a system role will be able to work with all batches and batch templates.

Uncommitted batches are visible to batch workflow step owners and to users with batch type and site permissions. Committed batches are visible to previous workflow step owners and to users with batch type and site permissions.

To ensure a batch owner has access to the batch once it is committed, click **Update status** to change owners instead of **Edit properties**. When you change owners through **Edit properties**, batch ownership history is not tracked.

Note: Access to batch must be established based on task and feature permissions for the user’s system role. Batch types available are based on the batch type permissions for the user’s system role.

You can restrict the Multiple batch commit process by site. On the Commit Multiple Batches page, click **Add**. When you select a site, only users associated with the site can access the Multiple batch commit process. To allow users of all sites to access the process, select “All sites.”

When new constituents are created through Constituent Batch and Constituent Update Batch, if the **Site** field is not included in a batch or the **Site** field is included but is left blank, any site security the batch owner has at the time the batch is committed will be applied to the new constituents. If the batch owner has access to Site A and Site B, when the batch is committed, the new constituent records will be associated with Site A and Site B.

Benefit Catalog Items

When you set up Benefit catalog items, you can associate the items with one or more sites in your organization.

Business Processes

Business processes include generating receipts, acknowledgements, pledge reminders, and mailings. You can restrict some business processes to a specific site. On the business process form, select the site that will use the process. Select “All sites” if there is no site restriction.

Note: Users can select from sites they have access to or select “All sites.”

All other business processes run based on the site access of the person who created them. For example, if a user for site A creates a receipt business process and generates receipts, only revenue associated with site A is included. Note that if a constituent is assigned to site B, but gives to site A (as identified by the designation), that revenue is receipted and acknowledged by someone with rights to site A, not site B.

If a selection is created from a business process, it inherits the site from the user who created the business process. For example, if a user for site A adds an appeal mailing process and creates a selection of the results, the selection inherits the site from the creator of the process and is available to other users with access to site A selections.

Campaigns and Appeals

Campaigns can be associated with one or more sites, in order to allow multiple sites to collaborate with fundraising. Appeals can be associated with all sites or with a single, specific site. So while different sites might collaborate on a campaign, appeals will typically apply to just one site or, potentially, to all sites. Revenue associated with the campaign or appeal is associated with the site of the designation selected.

Code Table Entries

Different sites at your organization may have separate and unique code table entries—ones that should be available to one or more sites only. Therefore code table entries for code tables managed in *Administration* can be assigned to one or more sites so that different chapters or affiliates can use them. For example, a site without access to a particular code table entry for the code table “Attribute Group” will not see the code table entry in the **Group** field when they add or edit attribute categories.

Note: Code tables entries that are not managed in *Administration* are not filtered using site security.

Constituent Documentation

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 selected types of note, links, and attachments. For example, you may have an executive note type for top-level or confidential information and could deny access to this type of note to all roles except for the executives.

Users in system roles which have been denied access to a documentation type will not be able to view or add documentation of that type for a constituent.

Constituents

Constituents can be assigned to one or more sites. Users without access to a specific site will not be able to access constituents with that site. For example, donors to a regional chapter may be assigned to that site, so that

other chapters cannot see or access those records. Sites applied to a constituent record are also applied to other views of those constituents, such as volunteer and prospect views; however, the site of the event is applied to the event registrant view.

When new constituents are created through Constituent Batch and Constituent Update Batch, if the **Site** field is not included in a batch or the **Site** field is included but is left blank, any site security the batch owner has at the time the batch is committed will be applied to the new constituents. If the batch owner has access to Site A and Site B, when the batch is committed, the new constituent records will be associated with Site A and Site B.

There is an additional layer of security for constituent records: constituent security groups. For more information, see Constituent Security Groups on page 55.

Constituent Mail Preferences

The **Mail preferences** section of the Preferences tab includes a **Sites** filter, allowing users to filter content displayed in the **Mail preferences** grid based on selected site information. In addition, a **Sites** column displays on the grid.

Site Options on Appeals

For constituent mail preferences, a **Site** column displays on the **Appeals** section of the Appeals tab. Site information also displays in the **Details** pane of the Appeals tab.

Correspondence

Different sites may track and categorize correspondence in different ways. Correspondence codes can be associated with sites so that different chapters or affiliates can manage their own correspondence effectively.

Designations and Fundraising Purposes

Fundraising purposes can be associated with a site. The associated designation inherits the site from the purpose. Revenue associated with the designation is associated with that site.

Direct Marketing

An organization's direct marketing efforts may be coordinated across all sites of the organization. Components of the efforts may therefore be shared across the entire organization (associated with all sites by assigning no site to the record) or may be associated with one, specific site. Each marketing feature that includes site security, such as creatives, packages, source codes, and marketing efforts can be used across the organization or may be set up to be used by a specific site.

Donor Challenges

Donor challenges can be associated with a site. The challenge is available to users for that site. Only revenue for the same site is eligible for the donor challenge. For example, if a challenge is for site A, revenue for only site A is available to be encumbered and matched for the donor challenge. If a challenge is for your entire organization, you do not need to associate it with a specific site.

You can restrict the Update donor challenge process by site. On the Update donor challenge process page, click **Add**. When you select a site, only users associated with the site can access the Update donor challenge process. To allow users of all sites to access the process, select “All sites.”

Events

Events can be associated with one or more sites, in order to allow multiple sites to collaborate on the event. Event registration revenue is associated with the site of the event. When you add an event registration revenue and associate it with the outstanding event registration commitment, the revenue is tied to the event’s site.

Export

You can restrict the export process by site. On the Export page, click **Add**. When you select a site, only users associated with the site can access the export process. To allow users of all sites to access the process, select “All sites.”

Giving Level Programs

When you set up Giving level programs, you can associate the programs with one or more sites in your organization.

Global Change

When you create a global change process, you assign permissions to limit which users can globally update records in your system. From the Add global change screen, you can restrict access to a specific site. If the process is available to users associated with any site, select “All sites.” To further limit access to the process, click **Assign permissions** and select which roles to grant or deny access to the selected global change process. If you do not properly secure each global change, a user who does not have the proper permissions can apply a system-wide change to your organization’s records.

Note: To limit access to global change processes, you can grant permission to run each process to selected sites and user roles. For information about how to assign permissions, see System Roles on page 17.

When you create a process that assigns or removes a site on selected records, such as the “Add constituent site” global change, the sites to which you as the owner have access appear in the Constituent site field on the Add global change screen. Unlike the **Site** field that restricts access to the process, in this field you select the site to add, change, or remove from records.

Users with permission to edit the global change can select any site the process owner has access to from the **Constituent site** field, regardless of the permissions assigned to the user. For example, an administrator with access to all sites creates a “Delete constituent site” global change process and restricts access to users at Site A. When a Site A user edits the process, all sites appear in the **Constituent site** field list. This user can select to delete any site, not just “Site A,” from records in the selection because the process owner has access to all sites.

Note: Site security permissions do not affect which records the global change process updates.

Only the user who creates the global change process or a system administrator can assign permissions to limit which users can access the process. You cannot delete a user who owns a global change process.

Grant Funding Plans

The way different sites manage their grant funding plans may vary. Therefore funding plans can be assigned to a site so that different chapters or affiliates can best manage their plans. Funding requests for the plan are secured by the site, if any, associated with the funding plan.

Import

You can restrict the Import process by site. On the Import page, select **Add an import process** under **Tasks**. When you select a site, only users associated with the site can access the import process. To allow users of all sites to access the process, select “All sites.”

Interactions

Interactions can be associated with one or more sites, so individuals from different sites can collaborate. Pending interactions with a major donor, for example, might need to be accessible from several fundraisers in several different sites.

KPI Instances

Fundraising KPI instances can be associated with one or more sites at your organization.

To enable site filtering, from the Site filtering tab on a KPI instance screen, select **Site filter enabled**. In the **Site** grid, select sites to associate with a KPI instance. The sites you select here in combination with user security setup determine the KPI instances a user can view.

Warning: If a user can add or edit smart fields but does not have rights to all sites, **Site filter enabled** is selected by default and the entire checkbox is disabled. The **Site** grid is enabled and contains only those sites available to a user.

Note: Not all sites appear as selections in the **Sites** grid. Available sites are determined by permissions and sites assigned to a user’s system role. Only those sites assigned to a user through a system role that is associated with the smart field add or edit permission appear as selections in the grid.

When you associate a site with a KPI instance, a filter is created so that only users with rights to sites you select can view the associated KPI instances on the KPI Instances pages and dashboard.

Membership Programs

Membership programs may be shared across the entire organization (associated with all sites) or may be unique to one, specific site.

Merchant Accounts

You can restrict the use of merchant accounts by site. From *Revenue*, click **Blackbaud Payment Services merchant accounts** under **Configuration**. When you add a merchant account, you can select the site or sites that use the merchant account.

When users select a merchant account, such as for a payment or for a credit card processing process, they are restricted only to the account for which they have site access.

Multicurrency

You can restrict the Revalue foreign-denominated commitments process by site. On the Revalue Foreign-Denominated Commitments page, click **Add**. When you select a site, only users associated with the site can access the process. To allow users of all sites to access the process, select “All sites.”

Name Formats

Name format options can be assigned to a site so that different chapters or affiliates can best meet their name format requirements, as the addressee and salutation needs may vary from site to site. The name format options are available to use for mailings, for example, by the site specified.

When you add name format options in *Constituents*, you can assign site security to make each option available to all or selected sites. Users with limited site permissions may still view and select name formats assigned to all sites. However, only system administrators or users with access to all records or records with no site assigned can add, edit, or delete these name formats. A system administrator or other user with the appropriate permissions can assign record access to a system role user in *Administration*. For information about how to assign site security to system roles, see *Assign Users to a System Role* on page 23.

Opportunity Amount Ranges

When you set up Opportunity amount ranges in **Major Giving Setup** the ranges you establish can be associated with one or more sites in your organization.

Pledge Reminders

You can restrict the reminder process by site. On the Reminders page, click **Add** on the Reminders tab. When you select a site, only users associated with the site can access the reminder process. To allow users of all sites to access the process, select “All sites.”

Prospect Plans

Prospect plans can be associated with one or more sites, in order to allow fundraisers from different sites to collaborate on cultivation of the prospect. Items associated with the prospect plan, such as opportunities, plan steps, and interactions, inherit the site of the plan. Users with access to a prospect plan will also have access to the opportunities, plan steps, and interactions for the prospect plan.

When you add a planned gift to a prospect plan, the planned gift inherits the site associated with the plan, but you can associate it with additional sites. When you add revenue for a planned gift, the revenue inherits the site from the designation, if different from the site of the planned gift or prospect plan.

Prospect Research Requests

Prospect research requests can be associated with one or more sites. When you add a prospect research request and restrict it to one or more sites, only users from those sites can see the request. Users can add constituents of

any site to research requests regardless of the site on the constituent record. To add a research request, from *Prospects* click **Add a prospect research request**.

Queries and Selections

Ad-hoc and smart queries can be associated with all sites or a single, specific site. Users with access to site A for a system role can only work with queries for site A. Users with access to all sites for a system role will be able to work with all queries. If a query is created by someone with no site permissions, all users regardless of site permissions will be able to access the query.

Data in query results is limited to those records the user has rights to access. Saved queries run with the site access of the user who runs the query, not the user who created the query.

Note: Access to *Query* must be established based on task and feature permissions for the user's system role. Query type and smart query definitions available are based on the query view feature permissions for the user's system role. The user must also have rights to the top level record type for the query view or smart query definition.

Selections are created from queries or by business processes. Selections inherit the site from the business processes or queries which created them. If the query from which the selection was created is accessible to only one site, the selection will be available to just that site. If a selection accessible by all sites is used by a user with access to only one site, the output will be based on the site the user can access.

Query View Security

With query view security, you can secure child nodes in query to restrict access to data based on site security and security groups. For example, John is a prospect manager for the business school (site A). He creates a prospect plan for Robert Hernandez, a potential major donor. Joan, a prospect manager for the law school (site B) is also interested in cultivating Robert Hernandez. If the prospect plans are associated with their respective sites, then John cannot see Joan's prospect plan when he looks at Robert Hernandez's prospect record. With the query view security enabled for the prospect child node, John also cannot see Joan's prospect plan in a constituent query that includes prospect and prospect plan information. If query view security is not enabled for the prospect child node, John could see Joan's prospect plan in the query results, but still could not view the plan itself on the prospect page.

Note: When you enable child query view security, additional security checks are performed when queries are run, which may increase the time it takes a query to process.

From *Administration*, click **Security** then click **Query view security** to enable security for a child query view. On the Query View Security page, select the child query view you want to secure and click **Enable security** on the action bar.

To disable security for a child query view, select it and click **Disable security** on the action bar.

Queue

You can restrict the queue process by site. On the Queue page, click **Add**. When you select a site, only users associated with the site can access the queue process. To allow users of all sites to access the process, select "All sites."

Receipts

You can restrict the receipt process by site. On the Receipts page, click **Add** in the Receipts tab. When you select a site, only users associated with the site can access the receipt process. To allow users of all sites to access the process, select “All sites.”

Recognition Programs

Recognition programs can be associated with all sites or a single, specific site. Revenue for the recognition program is associated with the site of the designation. If the revenue designation does not match the site of the recognition program, it is not counted in that program.

Records with Multiple Sites

Some records can be associated with one or more sites; these items are ones that would likely be shared between multiple sites, such as constituents, campaigns, and events. A user with access to any one of the sites can access the record; however, information on the record is restricted based on the user’s site access. For example, multiple users from different sites may be able to access the same constituent record; however, a user from site A can see only the constituent’s revenue for site A, if revenue access is also limited to site A.

Other items can be assigned to one specific site or to all sites; these items are ones that would either apply to everyone or would be unique to one site, such as solicit codes or batch templates.

Records with No Site Assigned

If a record has no site assigned, it can be accessed by users in a role with record access set to all records or to records with no site assigned.

Research Groups

Research groups can be associated with one or more sites. When you add a research group and restrict it to one or more sites, only users from those sites can see or use the group. Users can add constituents of any site to research groups regardless of the site on the constituent record. To access the Research Groups page, from *Prospects* select **Manage research groups**.

Revenue and Recognition Credits

Revenue and recognition credit is associated with the site of the designation. Revenue and recognition credit views for a constituent will display only the revenue items for the sites the user can access, based on the system role. If a revenue transaction is split between multiple designations, a user with site access to only one of the designations will still see the whole transaction. Likewise, for cumulative giving totals, the entire amount is counted even if a user has site access to only of the split designations.

If revenue is associated with an item from another site, revenue designation always takes precedence. For example, planned gifts can be associated with a site. If the planned gift revenue is associated with a designation from a different site, the revenue is associated with the designation’s site, not the planned gift’s site.

Event registration revenue is associated with the site of the event. When you add an event registration revenue and associate it with the outstanding event registration commitment, the revenue is tied to the event's site.

Recognition for naming opportunities inherit the site of the designation, if associated with revenue. If the naming opportunity recognition is associated only with a prospect plan opportunity (and not revenue), it inherits the site of the prospect plan. If it is associated with both a plan opportunity and revenue, the revenue designation takes precedence.

Smart Fields

Smart fields can be associated with one or more sites at your organization. To associate sites with smart fields, select **Site filter enabled** on the Site filtering tab of a smart field add or edit screen. You can then select sites to associate with the smart field.

If a user can add or edit smart fields but does not have rights to all sites, **Site filter enabled** is selected by default and the entire checkbox is disabled. The **Site** grid is enabled and contains only those sites available to a user. Not all sites appear as selections in the **Site** grid. Available sites are determined by permissions and sites assigned to a user's system role. Only those sites assigned to a user through a system role that is associated with the smart field add or edit permission appear as selections in the grid.

The sites you select in combination with user security setup determine the smart fields a user can view on constituent records, sponsorship child records, and sponsorship project records. When you associate a site with a smart field, a filter is created so that only users with rights to sites you select can view the associated smart fields on the Smart Fields page.

When you are ready to process a smart field from the Smart Fields page, note that site filtering does not affect which smart fields are included or excluded in the smart field process.

Solicit Codes

The way different sites solicit their constituents and use solicit codes may vary. Therefore solicit codes can be assigned to a site so that different chapters or affiliates can best manage their solicitations.

Stewardship Plan Templates

Stewardship plan templates can be associated with one or more sites, in order to allow fundraisers from different sites to build and use the templates. The site of the stewardship plan template does not impact the site of the stewardship plan.

Stewardship Plans

Stewardship plans can be associated with one or more sites, in order to allow fundraisers from different sites to collaborate on the stewardship of a constituent. Users with access to a stewardship plan will also have access to the details and plan steps for the stewardship plan. Plans also display additional information about the constituent, such as interests and the fundraising purposes of prior giving. If a user has access to the plan, but not to certain fundraising purposes, for example, the user will not see those purposes on the plan.

Tributes

Tributes can be associated with one or more sites, in order to help organizations manage a large volume of tributes. When you associate a site with a tribute, the association is used for filtering purposes only and does not limit user access to tributes based on security. On the Tributes page, you can use the **Sites** filter to view tributes associated with specific sites.

Users and Sites

Each application user in the program is typically assigned to a site; however system access for the user is restricted to the site security applied to that user in a system role. When a user is assigned to a system role, you can specify the site security to apply to the user in the role. The site on the system role assignment is used as the default site when the user adds records that have a site field.

However, for constituent records, the record may have more than one site or no sites associated with it depending on the security rights of the user adding the record. This is based on the system role assignment that grants the user rights to create the record. If the role granting the user permission to add the record has more than one site assigned, or the user is granted permission to add the record by multiple roles associated with different sites, then the resulting record will be associated with all sites that the user has access to. If any role granting the user permission to add the record does not have sites assigned, then the resulting record will have no sites assigned, even if the user also has access to specific sites.

The site field on the application user record is used as the default filter when the user views data in the system. This default site is helpful when users have access to multiple sites, as they switch between viewing data by “My site” compared to viewing all of the data to which they have access. For more information, see [Filter Data by Site](#) on page 47.

Volunteer Jobs

Different sites at your organization may have separate and unique volunteer jobs—ones that should not be available to other sites. Therefore volunteer jobs can be assigned to a site so that different chapters or affiliates can best manage their jobs.

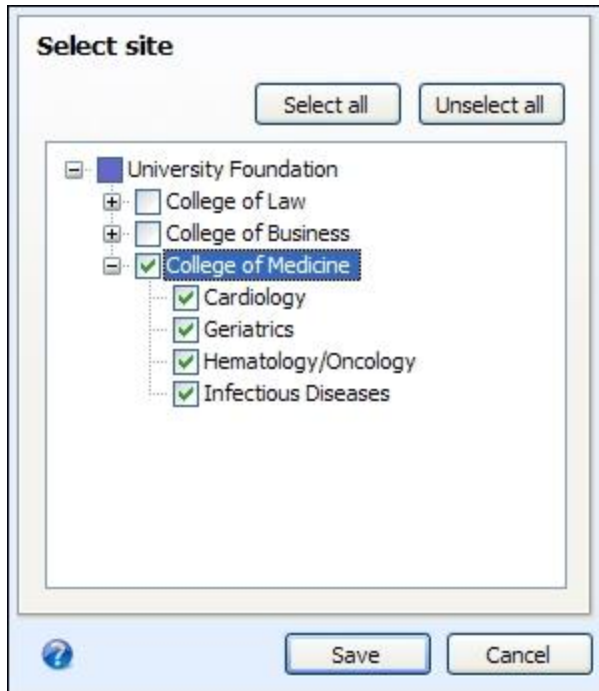
Filter Data by Site

Information you view is secured by site. If you have access to data in more than one site, you can filter the information by site.



When you select to view information for “All sites,” you will see data for all the sites you can access. When you select to view information for “My site,” you will see data associated only with the default site associated with your application user record. You can also select to view information for “My site’s branch,” which includes your site, your site’s children sites, and your site’s parent sites. When you filter based on “Selected sites,” you can choose which of the sites you can access to include.

Note: If you have access to data in multiple sites and have feature permissions to a datalist in one site but not another, data items from the site without datalist permission will not appear when you view the datalist.



Manage Sites

From *Administration*, click **Sites** under **Configuration**. On the Sites page you can view all your existing sites and add new ones. Sites in a hierarchy indicate the parent/child relationship between sites. A user with access to a parent site will inherit access for any child sites.

Once sites are created, you can implement site security by associating records with a site and by setting site permissions when you add users to system roles. For more information, see *Assign Sites to Records* on page 52 and *Assign Users to a System Role* on page 23.

Add Sites

You can add a site to the hierarchy for your organization or for another site at your organization. Adding a site consists of providing a name and optional information, such as a short name, site ID, and description. After you add a site, you can then enter it on records that include the **Site** field.

► Add a site

1. From *Administration*, click **Sites** under **Configuration**. The Sites page appears.
2. To add a site to another site at your organization, select the site to which to add the site in the grid. On the action bar, click **Add** and select **Add site to selected**. The Add site to site screen appears.

To add a site for your organization, on the action bar, click **Add** and select **Add site**. The Add site screen appears.

Add a site

Name:

Site type: ▼

Short name:

Site ID:

Acronym:

Description:

Save Cancel

3. Enter a unique name to help identify the new site.
4. In the **Site type** field, select a site type to further identify the site. The **Site type** field is optional and corresponds to the **Site type** field on the Site Search screen.

To add a site type code, you can enter text directly in this field. When you move to another field, you are prompted to add the type code as a new entry. You can also enter new site type codes from the Code Tables page in *Administration*.

5. The **Short name**, **Site ID**, **Acronym**, and **Description** fields are also optional and help further identify the site. Select or enter additional information in these fields.

The fields on the Add a site screen are the same as the Site Search screen. We recommend you be as specific and consistent as possible when adding a site to help in your search efforts at a later time.

6. Click **Save**. You return to the Sites page.

Edit Sites

You can edit site information, if necessary. The edited information appears on all records associated with the site.

► Edit a site

1. From *Administration*, click **Sites** under **Configuration**. The Sites page appears.
2. Select a site and click **Edit**. The Edit site screen appears.
3. You can edit the site information as needed.
4. When you are finished, click **Save**. You return to the Sites page. The updated information appears on any record associated with the site.

Delete Sites

You can delete a site, if necessary. The site you delete is removed from all records associated with the site.

► Delete a site

1. From *Administration*, click **Sites** under **Configuration**. The Sites page appears.
2. Select a site and click **Delete**. A confirmation message appears.
3. Click **Yes**. You return to the Sites page. The deleted site is removed from any record associated with the site.

Edit Site Hierarchy

When you have multiple sites, you can create a hierarchy to show the relationships between them.

► Edit site hierarchy

1. From *Administration*, click **Sites** under **Configuration**. The Sites page appears.
2. On the Sites page, click **Edit site hierarchy**. The Edit site hierarchy screen appears.
3. Use the arrows to move sites around in the hierarchy.
4. When you are finished, click **Save**. You return to the Sites page.

Site Search

After you add a site to the database, you can use the Site Search screen to access the site. When you search for a site, you can make the search broad or specific, depending on the criteria you select.

► Search for a site

1. From any screen where the **Site** field appears, click the binoculars next to the **Site** field. The Site Search screen appears.

Site ID:

Name:

Short name:

Acronym:

Site type:

Search

Clear

Results

Site ID	Name	Short name	Acronym	Site type	Site path
---------	------	------------	---------	-----------	-----------

Help

2. Enter the search criteria to use, such as name and site type.
3. Click **Search**. The program searches the database for sites that match the search criteria entered. In the **Results** grid, the sites that match the criteria appear. Depending on the search criteria you enter, the search may return one site or many.
4. In the **Results** grid, select the site record to open and click **Select** on the action bar. The site record opens.

Site Search Screen

The table below explains the items on the Site Search screen. For information about how to access this screen, see [Add Sites](#) on page 48.

Screen Item	Description
Site ID	Enter the primary identifier used for the site. You can enter the entire ID or only the beginning digits. For example, if you enter “1”, all site IDs that begin with the number 1 appear.
Name	Enter the name of the site to find. You can enter an entire name or only the beginning letters. Site names are not case-sensitive.
Short name	Enter a shorter name of the site to find.
Acronym	Enter the acronym of the site to find.
Site type	Select the site type of the site to find. This field corresponds to the Type code field on the Add a site screen.

Assign Sites to Records

You assign a site to a record by specifying it in the **Site** field. As soon as you associate a site with a record, that record will be unavailable to users who do not have rights to records associated with the site. However, any user currently logged in when the change is made can still access the record within the duration of the cache specified in the program’s Web.Config file. Logged in users will be unable to access the record as soon as the cache duration passes, or if they log out and log back into the program.

An application user can be associated with a site. This is the default site for the user, so it will appear by default on records secured by site that the user adds. The application user’s site is also used to define “My site” and “My site’s branch” in filters. The user’s access to data is based on how site and constituent security permissions are established on the system roles to which the user belongs.

► Assign a site to a record

1. Add or open the record to which you want to assign a site. When adding or editing a record that can be assigned to a site, a **Site** field is available.

The screenshot shows the 'Add an event' form with the following fields and values:

- General:**
 - Name: Starlight Concert
 - Description: (empty)
 - Main event: (empty)
 - Category: (dropdown menu)
 - Site: (dropdown menu with an asterisk icon)
- Details:**
 - Start date: 10/10/2009
 - Start time: 8:00 PM
 - End date: 10/10/2009
 - End time: 11:00 PM
 - Capacity: 250
 - Location information:
 - Location: Central Gardens
 - Contact: (empty)
 - Appeal: (empty)

At the bottom of the form, there is a 'Show copy options' checkbox and 'Save' and 'Cancel' buttons.

Note: For constituents, you can add or edit site information from the Security tab.

2. Select the site you want to associate with the record. Records that can be associated with more than one site have a **Site** grid, instead of a **Site** field.
3. Click **Save**.

Constituent Security Groups

Configure Constituent Security Groups	55
Apply Constituent Security to a User in a System Role	62

Constituent security groups enable you to “partition” constituents and restrict access to them. For example, your organization may interact with celebrities and therefore have constituent records for them in your system. If you want to limit access to those records for privacy, you could create a constituent security group for them. For most users, when you associate them with a system role, you would set constituent security to limit record access to only records with no security group assigned. For the few users who should have access to the celebrities’ constituent records, you would set constituent security to include all records or to include that particular constituent security group.

A single feature can also apply to more than one type of record level security. For a user to access the record, that user must have rights to all “pieces” of record level security, both site AND constituent security group. For example, a registrant for an event could belong to a constituent group and the event containing the registrant record could be assigned to a site, so that both types of security would apply to the registrant.

Configure Constituent Security Groups

From *Administration*, click **Security**. On the Security page, click **Constituent security**. You can create constituent security groups on the Security Groups tab. After you add a constituent security group, on the Assign Security Groups tab, you can add a process that specifies which constituents belong to a group. You can schedule this process so that the group is regularly updated as constituents’ statuses change and as new constituents are entered into the program.

You can then access a system role and apply it to a specific constituent security group.

Add Constituent Security Groups

Adding a constituent security group consists of providing a name and optionally a description. After you add a group, you can then configure a process to specify which constituents belong to the group.

► Add a constituent security group

1. From *Administration*, click **Security**. The Security page appears.
2. On the Security page, click **Constituent security**. The Constituent Security page appears.
3. On the Security Groups tab, click **Add**. The Add constituent security group screen appears.
4. Enter a name and description for the group.

5. Click **Save** to save the group and return to the Security Groups tab.

Apply Security Groups to Groups of Constituents Via a Process

When you assign a group to constituents, you use a selection that includes the criteria you want constituents to meet in order to be included in the security group. You can also edit the process if necessary.

► Assign a security group to constituents

1. From *Administration*, click **Security**. The Security page appears.
2. On the Security page, click **Constituent security**. The Constituent Security page appears.
3. On the Assign Security Groups tab, click **Add**. The Add assign constituent security group process screen appears.

Add assign constituent security group process

Name:

Description:

Input

Selection of constituents to process:

Assign

Group:

Selection of constituents to assign attribute to:

(those that do not meet this criteria will have the group removed if it existed)

Results

Create output selection

Selection name:

Overwrite existing selection

4. Enter a name and description for the process.
5. Under **Input**, you can optionally filter the potential pool of constituents from which your group will be formed. If you leave the field blank, all your constituents will be analyzed to see if they meet the criteria you later specify for inclusion in the group. If you specify a selection, only constituents in that selection will be available for potential inclusion in the group.
6. Under **Assign**, select the constituent security group to which these constituents will be assigned.
7. In the **Selection of constituents to assign attribute to** field, specify the selection that contains the criteria on which you want to base membership in this group. If you did not specify an **Input** selection, all your constituents will be analyzed to see if they meet the criteria of the selection you specify here, and those that do will be included in the group. If you did specify an **Input** selection, only the constituents meeting the criteria of the input selection are available to be analyzed by the selection you specify here.
8. Under **Output**, specify whether you want to create an output selection. This may be useful in other processes or analyses. Each time you run the process, if you want the new selection to overwrite the one created that last time the process was run, you can overwrite the existing selection.
9. Enter a name for the selection created from this process.
10. Click **Save** to save your settings and return to the Security Groups tab.

► Edit a constituent security group process

On the Assign Security Groups tab in Constituent Security, you can edit security group processes as needed.

1. From *Administration*, click **Security**. The Security page appears.
2. On the Security page, click **Constituent security**. The Constituent Security page appears.
3. On the Assign Security Groups tab, select a process and click **Edit**. For more information about the items on the screen, see *Assign a security group to constituents on page 56*
4. Click **Save** and the process is saved with your changes. You return to the Assign Security Groups tab.

► Delete a constituent security group process

On the Assign Security Groups tab in Constituent Security, you can delete security group processes when they are no longer needed.

1. From *Administration*, click **Security**. The Security page appears.
2. On the Security page, click **Constituent security**. The Constituent Security page appears.
3. On the Assign Security Groups tab, select a process and click **Delete**. A confirmation message appears.
4. Click **Yes** and the process is removed. You return to the Assign Security Groups tab.

Assign Constituents Process Status and History

From the Assign Security Groups tab, you can run a security group process to automatically assign constituents to security groups. You can also access detailed status and history information about the process.

► Start an Assign Constituent Process

1. From the Assign Security Groups tab, select a process and click **Start process**.
2. The process runs and assigns constituents to security groups.
3. The Process Status page appears with detailed information about the most recent instance the process was run, including any exceptions that may have occurred, as well as a history of the times the process was run.

► View Assign Constituent Process status

1. From the Assign Security Groups tab, select a process and click **Go to process**.
2. The Process Status page appears with detailed information about the most recent instance the process was run, including any exceptions that may have occurred, as well as a history of the times the process was run.

► Delete Assign Constituent Process history

1. On the Process Status page for an Assign Security Group process, select the History tab.
2. Select an item in the grid and click **Delete**. A confirmation message appears.
3. Click **Yes** to delete the item.

Job Schedule

You can arrange to process constituent security groups automatically, even during off-hours, from the Job Schedule tab.

Using *SQL Server Agent* jobs, the program automatically processes constituent security groups, and it executes the changes on a recurring basis, following the instructions you set. Scheduling jobs involves defining the condition or conditions that cause the job to begin running.

Create a New Job Schedule

When you create a job schedule for a selected constituent security group, the program automatically executes the constituent security group process at a frequency you determine.

► Create a job schedule

1. From the constituent security group process record for which you want to schedule a job, select the Job Schedule tab.
2. Click **Add**. The Create Job screen appears.
3. In the **Job name** field, enter a descriptive name for the scheduled process.
4. You can suspend the scheduled process by unchecking the **Enabled** checkbox. To make the process active, mark the **Enabled** checkbox. The default is checked.
5. In the **Schedule Type** field, select the desired frequency on which the scheduled process should run.

Note: For a detailed explanation of each field and option included on the Create Job screen, see *Create Job Screen* on page 58.

6. Click **Save** to save the job schedule.

Create Job Screen

You access the Create Job screen by clicking **Add** on the Job Schedule tab of the constituent security group process record.

Screen Item	Description
Job name	Enter the name of the job schedule.
Schedule type	<p>Selections for job frequency include:</p> <ul style="list-style-type: none"> -One time: The scheduled process runs once, on the date and time specified in the One-time occurrence field. -Daily: The scheduled process runs on a daily basis. In the Frequency section, specify the number of days to lapse between each run of the job. In the Daily frequency section, specify a time for the process to run or specify that the process run repeatedly during a specific period of time. In the Duration section, specify the date that your process begins. If you want the process to run over a specific period of time, specify an optional End date or keep the default of No end date. -Weekly: The scheduled process runs on a weekly basis. In the Frequency section specify the number of weeks to lapse before the process runs, in addition to the day of the week for it

Screen Item	Description
	<p>to run. In the Daily frequency section, set a specific time for the process to run, or specify that the process run repeatedly during a specific period of time. In the Duration section, specify the date that your process begins. If you want the process to run over a specific period of time, specify an optional End date or keep the default of No end date.</p> <p>-Monthly: The scheduled process runs on a monthly basis. In the Frequency section, specify the number of months to lapse before the process runs, in addition to the day of the month for it to run. In the Daily frequency section, specify a specific time for the process to run or specify that the process run repeatedly during a specific period of time. In the Duration section, specify the date that your process begins. If you want the process to run over a specific period of time, specify an optional End date or keep the default of No end date.</p> <p>-Start when SQL Server Agent service starts: The scheduled job process runs when the <i>SQL Server Agent service</i> starts. This is useful if you use the <i>SQL Server Agent service</i> for other tasks.</p> <p>-Start when the computer becomes idle: The job runs when enough resources are available on the server. This is determined by the idle condition defined in the <i>SQL Server Agent</i> properties on the server.</p>
Enabled	To suspend the scheduled process, unmark this checkbox. To make the process active, mark Enabled . By default, this checkbox is marked.
Date	Appears when you select One time in the Schedule type field. Use the date format mm/dd/yyyy, or click the drop down arrow to select from a calendar.
Time	Appears when you select One time in the Schedule type field. Enter the date of the one-time occurrence.
Occurs every [] month(s)	Enabled when you select Daily, Weekly, or Monthly in the Schedule type field.
Days of the week	Appears when you select Weekly in the Schedule type field. Mark the checkbox beside the day of the week to run the job. You can select one or multiple days.
Day [] of the month	Appears when you select Monthly in the Schedule type field.
The [] [] of the month	Appears when you select Monthly in the Schedule type field. In the first field select First, Second, Third, Fourth, or Last. In the second field select a day of the week or Day, Weekday, or Weekend day. For example, to run a process the last Friday of every month, select Last in the first field and Friday in the second field.
Occurs once at []	Enabled when you select Daily, Weekly, or Monthly in the Schedule type field.
Occurs every [] []	Enabled when you select Daily, Weekly, or Monthly in the Schedule type field. To move the number by one, click the up and down arrow in the first field. In the second field, select Minutes or Hour. For example, to run this process in the morning and afternoon every day at work, enter 4 in the first field and select Hours in the second field.
Starting at and Ending at	Enabled when you select Occurs every [] [] . Using the example in the previous row, enter 8:00:00AM in the Start at field and 5:00:00PM in the Ending at field.
Start	Enter the date for the job schedule to begin to process. Use the date format mm/dd/yyyy,

Screen Item	Description
date	or click the arrow to select from a calendar.
End date	Enter the date for the job schedule to end. For example, enter an end-of-year date. Use the date format mm/dd/yyyy, or click the arrow to select from a calendar. This option is disabled when No end date is selected.
No end date	If your job schedule does not have an end date, mark this option.

Edit an Existing Job Schedule

You can change any existing constituent security group process job schedule.

► Edit an existing job schedule

1. From the constituent security group process record for which you want to edit a scheduled job, select the Job Schedule tab.
2. Click **Edit**. The Edit Job screen appears.
3. Make any necessary changes.

Note: For a detailed explanation of each field and option included on the Edit Schedule screen, see [Create Job Screen](#) on page 58.

4. Click **Save** to save the changes.

Delete an Existing Job Schedule

You can easily remove any existing constituent security group process job schedule from your system.

► Delete an existing job schedule

1. From the constituent security group process record for which you want to delete a scheduled job, select the Job Schedule tab.
2. Select the scheduled job you want to delete.
3. Click **Delete**. A confirmation message appears.
4. Click **Yes** to delete the job.

Generate WSF

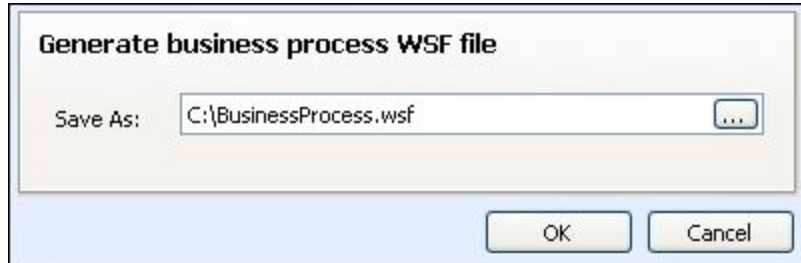
A Windows Scripting File (.wsf) is an executable script file format for *Windows* that can incorporate JScript (.js) or VBScript (.vbs) routines and include XML elements. On the Constituent Security Group process page, you can use either JScript or VBScript language to generate a .wsf file of the process to use with another application. You can use Windows Task Scheduler to schedule tasks to run the exported Windows Scripting File through the other application at a time that is most convenient to your organization.

Note: This is typically completed by the IT Administrator at your organization.

You can generate a Windows Scripting File for a process from its status page. From the explorer bar, click **Generate WSF** under **Tasks**.

► Generate a Windows Scripting File

1. Go to the process that requires a Windows Scripting File.
2. Under **Tasks**, click **Generate WSF**. The Generate business process WSF file screen appears.



3. In the **Save As** field, enter the path and file name for the WSF file. To browse for a location to save the file, click the ellipsis. The Save As screen appears.
4. Click **OK**. The program saves the WSF file.

Apply Security Groups to Individual Constituents

From a constituent record, administrators can assign that constituent to a security group. Constituent security groups can be associated with system roles to “partition” constituents so that different roles have access to different constituents.

As soon as you associate any constituent security group with a constituent record, that constituent will be unavailable to users who do not have rights to records associated with the group. However, any user currently logged in when the change is made will still be able to access the constituent record within the duration of the cache specified in the program’s Web.Config file. Logged in users will be unable to access the record as soon as the cache duration passes, or if they log out and log back into the program.

► Assign a security group to an individual constituent

1. From a constituent record, select the Security tab.
2. Click **Assign security group**. The Assign security group screen appears.
3. Specify the security group to which you want this constituent to belong.
4. Click **Save** to save the assignment and return to the constituent record.

► Remove a security group from an individual constituent

1. From a constituent record, select the Security tab.
2. Select a group in the grid and click **Remove security group**. A confirmation message appears.
3. Click **Yes** to remove the security group.

Edit Constituent Security Groups

You can change the name and description of an existing security group.

► Edit a constituent security group

1. From *Administration*, click **Security**. The Security page appears.
2. On the Security page, click **Constituent security**. The Constituent Security page appears.
3. On the Security Groups tab, select a group and click **Edit**. The Edit constituent security group screen appears.
4. You can edit the group's name and description.
5. Click **Save** and return to the Constituent Security screen.

Delete Constituent Security Groups

Security groups can be deleted from the program even if constituents belong to that group. Upon deletion, the security group setting is removed from each constituent's record.

From *Administration*, click **Security**. On the Security page, click **Constituent security**. The Constituent Security page appears. On the Security Groups tab, select the group to remove and click **Delete**.

Security Group Record

On a Security Group page, you can view all the system roles to which it is assigned. When you assign an application user to a role, you can specify the constituent group security to use. For more information, see [Apply Constituent Security to a User in a System Role](#) on page 62

Apply Constituent Security to a User in a System Role

Constituent security groups enable you to “partition” constituents by assigning them to groups that can have different permissions specified for them in different roles. For example, one role may not have access to constituents belonging to a “Major Donors” group, while another role does.

You set constituent security group access when you assign a user to a system role, so that different users in the same role can have different access.

A single feature can also apply to more than one type of record level security. For a user to access the record, that user must have rights to all “pieces” of record level security, both site AND constituent security group. For example, a registrant for an event could belong to a constituent group and the event containing the registrant record could be assigned to a site, so that both types of security would apply to the registrant.

► Assign a security group to a user in a system role

1. Open the system role and select the user on the Users tab to which you want to assign an accounting element security group.
2. Click **Edit**. The Edit system role user screen appears.
3. On the Accounting element security tab, you can determine the record access for the user in the role.
 - **All records** - The user can access all accounting element records in features to which he has granted rights. This is the default setting.

- **Allow use of records in selected groups** - The user has access only to those records that belong to the selected groups.
- **Allow use of all records except those in selected groups** - The user can access all records which are not part of the selected security groups.

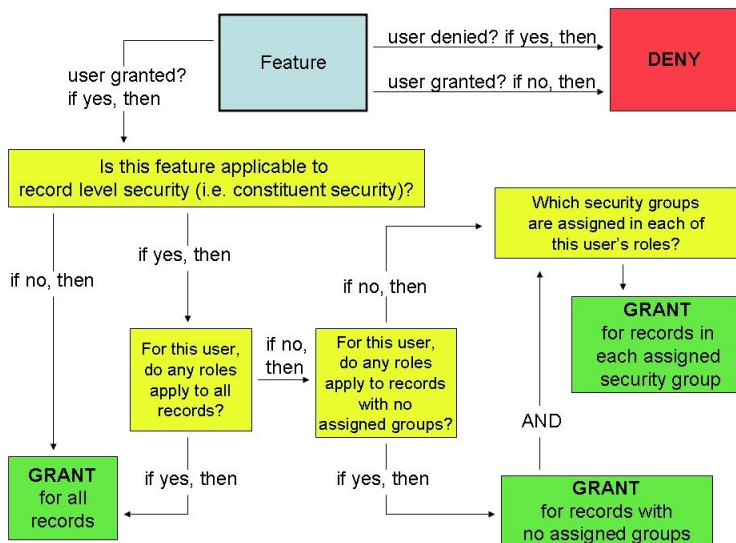
4. Click **Save** and return to the system role.

Constituent Security Group Example

Robert Hernandez is famous and belongs to a “Celebrities” constituent security group. Regular data entry users might not have access to constituents in the “Celebrities” group to help protect the constituents’ privacy. However, managers at the organization should have access to constituents in the group. What the user could do with that record would be determined by the feature permissions of the role(s) to which the user belongs.

Relationship Between Feature and Constituent Level Security

The relationship between feature and constituent level security in system roles is described below.



Things to keep in mind:

- Users permissions for constituent site security are determined when the user is assigned to a system role. Users in the same role can have different constituent security permissions.
- The default role setting for constituent security is for “All records” unless otherwise specified.
- If a user belongs to multiple roles, and each of those roles has access to different security groups, the user will have access to constituents in the union of all specified security groups.
- A single constituent record can belong to multiple security groups.
- Security groups can be deleted from the program, even if constituents belong to that group. Upon deletion, that security group setting is removed from each constituent record that belonged to the group.
- Constituent security applies to queries (root query views only) and query results. A user without rights to security Group A will not see information pertaining to Group A constituents in query results. Queries with results containing constituent records to which the user does not have access will still appear in the Ad-hoc

Query List for a user (if that user belongs to a role with rights to the appropriate query views), but the user will not be able to see these records in the results.

- Search screens do not consider constituent security when displaying results, so a user may potentially see constituents listed to which he does not have access. These records cannot be opened from the Search screen by the user.

Audit Tables

Enable Audit Table	65
Audit Report	65
Disable Audit Table	68
Purge Audit Table	68
Dependencies on Audit Tables	68

The audit tables track changes and deletions made to your data at the database level. When enabled, updates and deletions to every type of record are tracked by the database and stored separately for faster querying and reporting. From the Audit Tables page, you can quickly produce reports that list exactly which fields were changed, along with who made the change, and when it was made.

By default, audit tables are disabled, with the exception of tables that support features like the Constituent History and the Revenue History. You should determine which tables you want to audit and explicitly enable auditing for those tables. [Click here to view the tables with audit enabled by default.](#)

Note: You can create a “Table Statistics” ad-hoc query to show you the size of tables, including audit tables, in your database. You can use this information to help determine when to purge certain audit tables to free up disk space. You can also set up a “Delete audit data” global change process. The process can be configured to purge audit table data from over a certain period of time ago, such as audit table data from more than three years ago.

Enable Audit Table

If a database table is disabled and not maintaining audit data, you can enable it at anytime and resume the audit functionality.

From the Audit Tables page, select the table for which you want to collect and maintain audit data and click **Enable auditing**. The green check mark in the **Auditing enabled** column appears and the **Enable auditing** button changes to **Disable auditing**.

There is also a “Enable or disable audit tables” global change process you can use to help enable or disable auditing for multiple tables at one time.

Audit Report

From **Audit tables** in *Administration*, you can monitor all changes made to every type of record in the database:

- To a specific constituent record (or records)
- To specific gift record (or records)

- By a specific user, group of users, or process
- On a specific day (or date range)
- To a specific field (or fields)

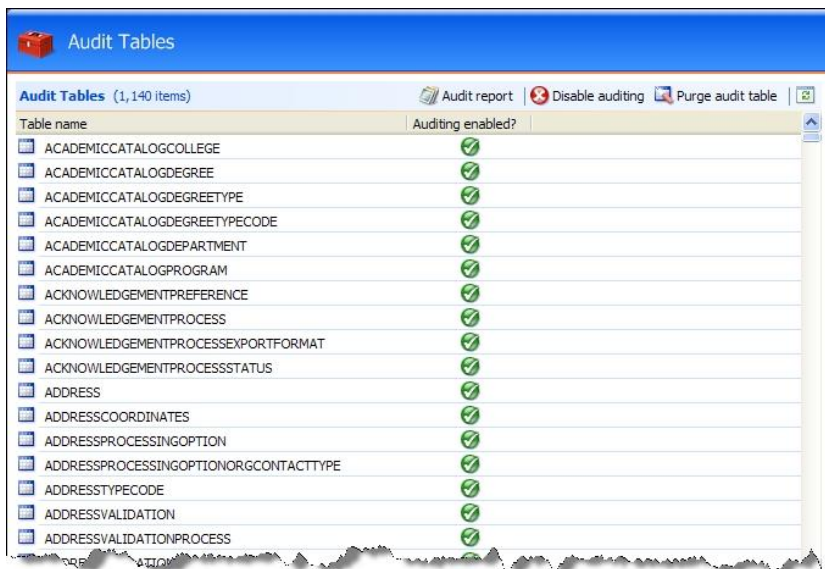
In addition, you can easily view any combination of the above. For example, the program can quickly list the last five changes made to a specific record.

Because audit trails are supported at the database level, all changes made are subject to the audit process, even those made outside the program. So not only are changes made through the program interface included but changes made via direct database access by database administrators are also included. This ensures that the audit trail content is always completely accurate and up to date.

Note: New database entities and custom database fields created through the program automatically inherit the audit functionality.

► Generate an audit report

1. From *Administration*, click **Audit tables**. The Audit Tables screen appears.



All database tables included in the program display in the **Table name** column of the grid. This includes any customized tables your organization may have added. The **Auditing enabled?** column displays a green check mark next to all enabled tables; no check mark appears if the table is disabled.

2. Select the table for which you want to view an audit report and click **Audit report**. The Table Audit Report appears.

Audit Recent Changes

Table Name: Maximum rows per table:

Start Date: NULL End Date: NULL

User: Application:

Include Inserts?: Include Deletes?:

Table Audit Report

Start date: Maximum rows per table: 25
 End date:
 User: (any user) Application: (any application)
 Include inserts: No Include deletes: Yes
 Include updates: Yes

Date	Action	User	Application
CONSTITUENT			
3/3/2009 5:25:32 AM	Update	BBNTBuildUser	.Net.SqlClient Data Provider
3/3/2009 5:25:32 AM	Update	BBNTBuildUser	.Net.SqlClient Data Provider
3/3/2009 5:15:05 AM	Update	BBNTBuildUser	RE CRM Conversion
3/3/2009 5:15:05 AM	Update	BBNTBuildUser	RE CRM Conversion

3. Once the report is generated, you can modify the output to better meet your specific needs.
 - In the **Table name** field, you can select a different database table for which to view audit information.
 - In the **Start date** field, if you want to view audit information from a specific start date, unmark the **NULL** checkbox and enter the start date you want to use.
 - In the **End date** field, if you want to view audit information up to a specific end date, unmark the **NULL** checkbox and enter the end date you want to use.
 - In the **User field**, you can select a specific database user name and view only changes made by that user.
 - Next to **Include inserts?**, mark **True** if you want to view new information entered; mark **False** if you want to view only edited information.
 - Next to **Include deletes?**, mark **True** if you want to view deleted information; mark **False** if you do not want deleted information included in the report.
 - In the **Maximum rows per table** field, enter the number of rows to which you want to limit your report. Regardless of the number of rows selected, all information is included in the report. Any information exceeding the row limit set is included on a new page.
 - In the **Application** field, select the database application for which you want to view audit information.
 - Next to **Include updates?** mark **True** if you want to view edited information; mark **False** if you do not want edited information included in the report.
4. After you enter any parameter changes for the report, click **View report** to generate an updated view.

Disable Audit Table

If for any reason you do not want audit data maintained for a specific table, you can disable the audit functionality for the selected table.

From the Audit Tables page, select the table for which you no longer want to collect and maintain audit data and click **Disable auditing**. The green check mark in the **Auditing enabled** column disappears and the **Disable auditing** button changes to **Enable auditing**.

Purge Audit Table

Over time, as more changes and deletions occur, the audit data store grows, but the program is optimally configured into distinct database files which can reside apart from the main database. However, should it become necessary due to a lack of disk space, you can purge the audit data store, erasing the audit trail.

Note: You can create a “Table Statistics” ad-hoc query to show you the size of tables, including audit tables, in your database. You can use this information to help determine when to purge certain audit tables to free up disk space. You can also set up a “Delete audit data” global change process. The process can be configured to purge audit table data from over a certain period of time ago, such as audit table data from more than three years ago.

Each table defined in the program has an associated audit table mirroring the source table structure. As changes and deletions occur to the source table, a trigger handles writing information to the associated audit table. In addition, each table defined in the program has an associated audit view, which provides user-friendly formatted data.

From the Audit Tables page, select the table for which you want to purge data and click **Purge audit table**. The table is purged and you return to the Audit Tables page.

Dependencies on Audit Tables

When the program processes certain features of the program, such as smart fields and reports, it is important to understand that these features may not process correctly when dependent audit tables are disabled. Parameters determine when a feature is dependent on an audit table.

Smart Field Dependencies on Audit Tables

Specific smart fields are dependent on the following audit tables:

- CONSTITUENTAPPEAL
- FINANCIALTRANSACTION
- MEMBERSHIP
- MEMBERSHIPTRANSACTION
- RECOGNITIONCREDIT

- REVENUERECOGNITION
- REVENUE_EXT
- SPONSORSHIP

The table below breaks down each field and its dependent table.

Smart Fields	Dependent Audit Tables
Constituent\Appeal\Constituent appeal count	CONSTITUENTAPPEAL
Constituent\Appeal\Constituent appeal years	CONSTITUENTAPPEAL
Constituent\Appeal\Last constituent appeal name	CONSTITUENTAPPEAL
Constituent\Recognition Credits\Constituent recognition credit amounts	FINANCIALTRANSACTION RECOGNITIONCREDIT REVENUERECOGNITION REVENUE_EXT
Constituent\Recognition Credits\Constituent recognition credit dates	FINANCIALTRANSACTION RECOGNITIONCREDIT REVENUERECOGNITION REVENUE_EXT
Constituent\Revenue\Constituent annual revenue renewer	FINANCIALTRANSACTION
Constituent\Revenue\Constituent largest revenue date	FINANCIALTRANSACTION
Constituent\Revenue\Constituent revenue amounts	FINANCIALTRANSACTION
Constituent\Revenue\Constituent revenue counts	FINANCIALTRANSACTION
Constituent\Revenue\Constituent revenue dates	FINANCIALTRANSACTION
Constituent\Revenue\Constituent revenue giving years	FINANCIALTRANSACTION
Constituent\Revenue\Constituent revenue application	FINANCIALTRANSACTION REVENUERECOGNITION REVENUE_EXT
Constituent\Revenue\Constituent revenue application amounts	FINANCIALTRANSACTION REVENUERECOGNITION REVENUE_EXT
Constituent\Revenue\Constituent revenue application annual renewer	FINANCIALTRANSACTION REVENUERECOGNITION REVENUE_EXT
Constituent\Revenue\Constituent revenue application counts	FINANCIALTRANSACTION REVENUERECOGNITION REVENUE_EXT
Constituent\Revenue\Constituent revenue application dates	FINANCIALTRANSACTION REVENUERECOGNITION REVENUE_EXT

Smart Fields	Dependent Audit Tables
Marketing\Constituent Lifetime gifts on file	FINANCIALTRANSACTION REVENUE_EXT
Marketing\Constituent Lifetime giving	FINANCIALTRANSACTION REVENUE_EXT
Marketing\Constituent Loyalty	FINANCIALTRANSACTION REVENUE_EXT
Marketing\Constituent Single gift consecutive year donors	FINANCIALTRANSACTION REVENUE_EXT
Marketing\Years on file	FINANCIALTRANSACTION REVENUE_EXT
Membership\Membership expiration	MEMBERSHIP MEMBERSHIPTRANSACTION
Sponsorship\Sponsor active sponsorship count	SPONSORSHIP
Sponsorship\Sponsorship child active sponsor count	SPONSORSHIP
Sponsorship\Sponsorship project active sponsor count	SPONSORSHIP

Constituents Dependencies on Audit Tables

Specific *Constituents* features are dependent on the following audit tables:

- ADDRESS
- ADDRESSVALIDATIONUPDATE
- APPUSER
- CONSTITUENT
- DECEASEDCONSTITUENT
- EMAILADDRESS
- ORGANIZATIONDATA
- PHONE

The table below breaks down each field and its dependent table.

Constituents Feature	Dependent Audit Tables
Constituent data review	ADDRESS ADDRESSVALIDATIONUPDATE EMAILADDRESS PHONE
Constituent history	ADDRESS ADDRESSVALIDATIONUPDATE APPUSER

Constituents Feature	Dependent Audit Tables
	CONSTITUENT DECEASEDCONSTITUENT ORGANIZATIONDATA

Revenue Dependencies on Audit Tables

Specific *Revenue* features are dependent on the following audit tables:

- FINANCIALTRANSACTION
- FINANCIALTRANSACTIONLINEITEM
- FUNDINGREQUEST
- JOURNALENTY
- JOURNALENTY_EXT
- PAYMENTORIGINALAMOUNT
- PLANNEDGIFT
- PLANNEDGIFTADDITION
- PLEDGEORIGINALAMOUNT
- REVENUEBENEFIT_EXT
- REVENUECATEGORY
- REVENUERECOGNITION
- REVENUESCHEDULE
- REVENUESPLITBUSINESSUNIT
- REVENUESPLITCAMPAIGN
- REVENUESPLITOTHER
- REVENUESPLIT_EXT
- REVENUE_EXT

The table below breaks down each field and its dependent table.

Revenue Feature	Dependent Audit Tables
Funding request history	FUNDINGREQUEST

Revenue Feature	Dependent Audit Tables
Planned gift addition history	PLANNEDGIFTADDITION
Planned gift history	PLANNEDGIFT
Revenue history	FINANCIALTRANSACTION FINANCIALTRANSACTIONLINEITEM JOURNALENTY JOURNALENTY_EXT PAYMENTORIGINALAMOUNT PLEDGEORIGINALAMOUNT REVENUEBENEFIT_EXT REVENUECATEGORY REVENUERECOGNITION REVENUESCHEDULE REVENUESPLITBUSINESSUNIT REVENUESPLITCAMPAIGN REVENUESPLITOTHER REVENUESPLIT_EXT REVENUE_EXT

Marketing and Communications Dependencies on Audit Tables

Specific *Marketing and Communications* features are dependent on the following audit tables:

- MKTSEGMENTATIONFILTERSEGMENTATION
- MKTSEGMENTATIONFILTERSELECTION
- REVENUELETTER
- REVENUELETTERMARKETING
- REVENUERECEIPT
- REVENUERECEIPTMARKETING

The table below breaks down each field and its dependent table.

Marketing and Communications Feature	Dependent Audit Tables
Appeal mailing activate edit screen	MKTSEGMENTATIONFILTERSEGMENTATION MKTSEGMENTATIONFILTERSELECTION REVENUELETTER REVENUELETTERMARKETING REVENUERECEIPT REVENUERECEIPTMARKETING
Appeal mailing processes	MKTSEGMENTATIONFILTERSEGMENTATION MKTSEGMENTATIONFILTERSELECTION
Communication efforts query view	MKTSEGMENTATIONFILTERSEGMENTATION MKTSEGMENTATIONFILTERSELECTION

Marketing and Communications Feature	Dependent Audit Tables
Marketing acknowledgement export process	MKTSEGMENTATIONFILTERSEGMENTATION MKTSEGMENTATIONFILTERSELECTION
Marketing effort export process	MKTSEGMENTATIONFILTERSEGMENTATION MKTSEGMENTATIONFILTERSELECTION
Marketing effort page expression view screen	MKTSEGMENTATIONFILTERSEGMENTATION MKTSEGMENTATIONFILTERSELECTION REVENUELETTER REVENUELETTERMARKETING REVENUERECEIPT REVENUERECEIPTMARKETING
Marketing effort selection briefs report	MKTSEGMENTATIONFILTERSEGMENTATION MKTSEGMENTATIONFILTERSELECTION
Membership renewal effort export process	MKTSEGMENTATIONFILTERSEGMENTATION MKTSEGMENTATIONFILTERSELECTION
Segmentation report	MKTSEGMENTATIONFILTERSEGMENTATION MKTSEGMENTATIONFILTERSELECTION
Sponsorship effort export process	MKTSEGMENTATIONFILTERSEGMENTATION MKTSEGMENTATIONFILTERSELECTION

