ProgressBook StudentInformation Security Guide

ProgressBook. **Student**Information

Ohio

ProgressBook StudentInformation Security Guide

(This document is current for v18.1.0 or later.)

Change Log

The following Change Log explains by Product Version, Heading, Page, and Reason where changes in the *ProgressBook StudentInformation Security Guide* have been made.

Product Version	Heading	Page	Reason
18.1.0	*"Sitemap Access"*	*12*	Updated section to exclude resource permissions.
18.1.0	*"Resource Permissions"*	*20*	Added new section with new **Notifications** tab.

Table of Contents

Security Overview

Security defines access to the various features in the StudentInformation system. The security administration pages use a number of concepts similar to modern network operating systems. This section focuses on concepts and background information needed to understand and use the Security system.

Base Concepts

Determining the Access. Roles are used or created to define access to specific nodes or branches of the site map. This is covered in more detail in the Site Map Hierarchy section below.

Giving Users Access. Users are given access to StudentInformation by being granted one or more role/school combinations. The role defines the access while school defines where that access is given. These role/school combinations can be assigned directly to the user account or can be applied to the user account through their membership in one or more groups with direct or inherited role/school assignments.

Open – Shut – Clear. Each node access (i.e. Create, Read, Update, Delete) in StudentInformation can have one of the following settings: Open, Shut, Clear. Open means the user is granted access. Shut means the user is denied access. Clear means neither an Open or Shut has been assigned to the menu item. When one school/role assigns an Open to the menu item and a second school/role assigns a Shut to that menu item, the shut will take precedence. A Shut always takes precedence over an Open. Each node defined in the role has the security options of Create, Read, Update, and Delete though for several items.

Group Hierarchy

Groups can be members of other groups thus making a hierarchy of groups. While this is a very powerful feature, it should be used sparingly and only in situations where this is determined to be time saving or the complexity lends itself to solve the security configuration need.

In a group hierarchy, any security applied to the parent group is inherited by the members of that group and also members of any child (or grandchild, great-grandchild, etc.) groups. Note that security applied to a child group does not flow up to the members of the parent group.

School Hierarchy

Access in StudentInformation is specified on a school basis. Schools within StudentInformation are organized in a hierarchical fashion. For instance, District A has elementary school buildings E, F, G, and H; middle school buildings M and N; and high school building Z. The following hierarchy could be setup in StudentInformation to represent these buildings.

District A

- Elementary Buildings
  - Building E
  - Building F
  - Building G
  - Building H
- Middle School Buildings
  - Building M
  - Building N
- Building Z (high school)

Assume that a user needs access to the Student List menu item for all schools in the district. While you could grant this user access to Student List for buildings E, F, G, H, M, N and Z; the easier approach would be to grant access to Student List for District A. Granting access at to District A rather than each individual building would give the user access to building I if it was added to the district at a later time.

Site Map Hierarchy

Navigation and security in StudentInformation is based on the hierarchical site map. In looking at the sample site map clip-it shown below, the menu item "Contact" is available by selecting "SIS" from the main menu then selecting "Student". Security is configured by either adding or denying access to any of the nodes on the site map. Access is propagated down the site map. For instance, if access is granted to Student, then the user would have access to the Student node as well as each of the nodes below it (i.e. Contact, Medical, Misc. Data, and Notes). Also, in order to get to the Student node, access to the SIS node is implied.

SIS

- Student
  - Contact
  - Medical
  - Misc. Data
  - Notes
- School
  - Counselors
  - Free Lockers
- Registration

Denying access to a particular node takes precedence over granting access to it. Assume access was denied to school and access was granted to "Free Lockers." The denying of access to school blocks access to the School node and each of the nodes below it (including Free Lockers).

Understanding the Security Module

This section focuses on terminology used in the Security system.

Default Domain

The domain value is used to create and house Windows user accounts at the DA-Site where StudentInformation is run. All accounts are created in the default domain unless your district or school has established a trust between your Windows server and the server at the DA-Site maintaining the Windows user accounts.

Domain

A Windows user account is used to access StudentInformation. The domain value indicates which Windows domain the user account is located in. For installations with trusts to district servers, several domain values may be available to select from.

Group

A group is a collection of users and other groups. Groups can be used for collection purposes, assignment of job functions, and/or assignment of security access.

Job Function

Job functions are recognized jobs in the educational environment. For example, the current list of job functions include: All, Teacher, Principal, Superintendent, Secretary, Media Specialist, EMIS Coordinator, Technology Coordinator, Curriculum Coordinator, Bus Driver, Cafeteria Worker, Counselor, and Nurse. Job functions can be applied to groups which in turn determine what the users that comprise that group can see in the StudentInformation Portal. Job functions can also be applied to the staff school assignments which determine the list of staff members in several drop-down lists of staff members.

Node

One menu item on the site map. A node includes information describing the page heading, the name in the navigation, what type of access the node provides, and the type of node.

Operator

The operator is the person using the StudentInformation security administration pages. Most likely that is you since you are reading this information. Other references to the person using the StudentInformation security administration pages include the Security Administrator or the Super User.

Role

A role is a collection of nodes with the corresponding security permissions. Roles are usually associated with a specific task, set of tasks, or type of position in the school. For example, one role, "Take Attendance", would allow users assigned the role to access the page used to enter attendance information. Another role, "Run Reports" would allow the users to run the various reports in the StudentInformation application. Yet another role, "Guidance Counselor" would define all the areas of StudentInformation that the guidance counselor for this school should have access to.

Permissions on the nodes within a role are Open, Shut, or Clear. Each of these permissions can be set for Create, Read, Update, and Delete access. Open means the role allows that action to be taken. Shut indicates that the role does not allow any of the assigned users access to that option. Clear means that the role does not define whether access is granted or denied.

Roles are either pre-defined roles (included as part of the StudentInformation software package – StudentInformation State Support recommends they not be used) or local roles. While both roles are available for use in StudentInformation, only the local roles can be created, modified, and removed.

Role Scope

Role scope is the schools assigned to be able to use this role. When a school is assigned to a role, the role scope includes the assigned schools and any of their children. The role scope also includes the administrative school but does not include any children of the administrative school unless those schools are assigned.

School

A school is any educational entity referenced in StudentInformation. Schools are organized into a hierarchy.

In StudentInformation, the following additional references to schools are made:

- **Administrative School** –The administrative school defines the recognized owner of the item which the administrative school is being applied. For instance, in the portal administration pages, the administrative school of an announcement indicates what school a user must have access to in order to edit or remove that announcement. Items such as users, groups, and roles also have administrative schools associated with them.

- **Context School** – Used in the maintenance of groups. The context school of a group indicates the school to which the group's job functions apply.
- **Default School** – The default school is the school that is designated as the working school when the user logs into StudentInformation. Default school can be set or changed when changing your working school.
- **Selected Schools** – The list of schools the user has selected to be the currently active schools. The selected school determines what schools appear in the EZ Query portion of the application and also what content is displayed in the portal. Selected schools can either be saved for the current session or can be saved permanently.
- **Working School** – The working school is the current school that the user is working in. The working school name is listed in the upper right hand corner of StudentInformation.

Site Map

The site map is a hierarchical listing of nodes. The site map is the basis for the StudentInformation navigational system.

Staff Impersonation

Staff impersonation is the ability in StudentInformation for a user to be able to do tasks as if they were the staff member that they are impersonating. For each staff member that a user impersonates, zero or more staff user permissions can be applied. Users can also impersonate all staff members in the school if so specified. This option is mostly used by administrative staff.

Staff Member

A staff member represents one district employee. A user can be assigned to one staff member per district.

Staff User Permission

A staff user permission is a designation of what the user impersonating a staff member can do. For example, the current list of staff user permissions include: Full, Fee Collect, EZ Query, Attendance, and Marks.

User

A user represents one login account to the StudentInformation system. Users have an administrative school which indicates which school can manage the user.

Vendor

If your district uses ProgressBook VendorLink, a vendor is set up in StudentInformation as a user. You must assign the roles and schools to define the information the vendor application can access in StudentInformation.

Special Note concerning Security, EZ Query, and the Teacher Menu

The EZ Query and Teacher Menu modules have specialized security functionality based on Staff Member settings and job functions. See the *ProgressBook StudentInformation EZ Query Guide* and *ProgressBook StudentInformation Teacher Menu Guide* for additional information.

Security Maintenance

Role Maintenance

Navigation: StudentInformation – Management – Security – View Roles

Roles are used to define which of the StudentInformation features a user can access. Role management is the process of creating, changing, and removing roles as well as defining the access the role will have to each of the nodes on the site map. Role assignment involves assigning users to a role/school combination.

> ***Note:*** *A user may be assigned multiple roles. If two roles conflict regarding a node, any role that denies access to that node takes precedence over a role that grants access to that node. Denial of access to a node also takes precedence over default access (neither granted nor denied) to that node.*

Find Roles

Navigation: StudentInformation – Management – Security – View Roles

Click **Add New Role** to add a new role.

- **School** – Choose the school of the group(s) to filter from the drop-down list. This will limit your search based on the administrative school of the role.
- **Role Name** – The name of the role(s) to filter. See *"Find Users"* for an explanation and examples of the use of wildcards in filters.

Click **Search** to list the roles that match the criteria selected to which you have access.

In addition to matching the search filters, users must have an administrative school that you as the operator have security access to for the page where the search takes place.

- **School** – Administrative school of role.
- **Role Name** – Descriptive name of role.
- 🖉 – View/edit Details about a specific role.
- 🗑 – Delete role

Remove Roles

Navigation: StudentInformation – Management – Security – View Roles

> *Note: As of the 8.1.0 release, deleting a role now also removes that role from any user who was assigned that role.*

Click 🗑 to delete the school name/role.

- **Ok** – Delete the specified role.
- **Cancel** – Do not delete the specified role.

Create/Update Roles

Navigation: StudentInformation – Management – Security – View Roles – Add/Edit Roles

Click **Add New Role** to add a new role.

- **Role Name** (required) – Enter the name of the new role (be as descriptive as possible).
- **Administrative School** (required) – Choose the administrative school from the drop-down list. This designates what schools can edit the role.

  Note: The role/administrative school combination must be unique (no other role can have the same combination).

- **Available** – The available buildings and districts that can be assigned to be within the scope of this role.
- **Assigned** – The schools assigned to be able to use this role.
- **Save** – Save new role and proceed with setting Sitemap Access.
- **Save and New** – Save new role and return to this page to enter another new role.

- **Edit Sitemap Access** – Set sitemap access for this role (see *"Sitemap Access"*).

Sitemap Access

Navigation: StudentInformation – Management – Security – View Roles – Add New Role button or View Details icon – Sitemap Access button

This screen is accessed by first selecting or creating a role, then clicking **Edit Sitemap Access** on that role's maintenance screen.

Click ✏ to view details of this role, or click **Add New Role** to create a role.

Click **Edit Sitemap Access** to view and set sitemap access for this role.

Clicking **Edit Sitemap Access** brings up the StudentInformation sitemap with the four access settings (**Display**, **Add**, **Change**, **Delete**) in front of each node. The sitemap displays hierarchically. Access for a node can be toggled between Open, Shut, and Clear by clicking on the space or icon to the right of each access setting name.

- Open ● – The user with this role can use the option in StudentInformation.
- Shut ✕ – The user with the role is denied access to this option in StudentInformation.
- Clear (blank) – Access is neither allowed nor restricted to this node.

The nodes can be expanded and collapsed using the ⊞ and ⊟ buttons to the left of the folders.

- **Save Access** – Save the Sitemap Access for this role.
- **Cancel** – Do not save the Sitemap Access for this role.

In the following example, this role has Display access to all of SIS, except they do not have Delete access to SIS-Registration and SIS-Student. They also are denied all access to SIS-Attendance – except they have Display, Add, Change, and Delete access to the Daily Attendance Completion List, if they can reach it from some other path (such as through a direct Portal Link).

Extra System Permissions

The **Extra System Permissions** node lets the Security Administrator set specific permissions for individual actions, rather than screens, for certain elements of StudentInformation.

- **Update past on calendar dates wizard** – Opening the **Display** access of this Extra Permission setting lets this role edit past dates using the Calendar Dates Wizard. This is needed for any user not marked as **Is Privileged** who will edit past dates using the Calendar Dates Wizard.

- **Course History Default Settings** – Opening the **Display** access of this Extra Permission setting lets the role set the default Course History display settings for the Building.

Extra System Permissions – Portal

- **Portal – Document** – Opening this Extra Permission setting lets the role display, add, change, or delete items from the **Portal** screen **Documents** section. If you want a user to have access to the **Portal** or **Home** screen, you must assign the user at least Display access to the Portal.

- **Portal – Link** – Opening this Extra Permission setting lets the role view, display, change, or delete items from the **Portal** screen **Quick Links** section.

- **Portal – Html Document** – Opening this Extra Permission setting lets the role display, add, change, or delete items from the **Portal** screen **Headlines!** section.

- **Portal – Event** – Opening this Extra Permission setting lets the role display, add, change, or delete items from the **Portal** screen **Upcoming Events** section.

- **Portal – Announcement** – Opening this Extra Permission setting lets the role display, add, change, or delete items from the **Portal** screen **Announcements** section.

Extra System Permissions – EMIS

- **EMIS – Free and Reduced Lunch Status** – Opening the **Display** access of this Extra Permission setting lets the role view and edit the **Free and Reduced/Lunch Status** on the **Edit Student Profile** screen **FD-Attributes** tab. It also lets the role view and edit the

Free/Reduced Lunch Status on the **Student Profile Bulk Update** screen **FS-Standing & FD-Attributes-Effective Date** tab. It also displays the **Free/Reduced Lunch Status** when using the Student Registration Wizard.

> *Note: If you grant a user access to view the Free/Reduced Lunch Status, the user can also edit the status. The Free/Reduced Lunch Status security options provide all or nothing access for the user.*

- **EMIS – Override "Closed" on Situation History –** Opening the **Display** access of this Extra Permission setting lets the role update EMIS Situation History in closed EMIS Reporting Periods. Please note that EMIS Situation History is only used before FY09 (08-09).

- **EMIS – View/Update State Student ID** – Opening the **Display** access of this Extra Permission setting lets the role view or update the **State Student ID (SSID)** on the **Edit Student Profile** screen **Private** tab (editing the **Private** tab also requires the Edit Student Profile/SIS Student Search extra permission). Access must be given to this Extra Permission Setting to access the State Student ID on the following screens:
  - **EZ Query – Reports – SIS Student Search**
  - **EZ Query – EZ Students – Shared Student Data (JVS/Home)**
  - **EZ Query – EZ Students – EMIS Demographic**
  - **EZ Query – Reports – Download Class List**

- **EMIS – Edit Student Profile/SIS Student Search** – In the 08-09 school year and forward, opening the **Display** access of this Extra Permission setting lets the role view or update information on the **FS-Standing**, **FS-Attendance**, **FD-Attributes**, **FN-Attributes**, or **Private** tabs. In school years prior to 08-09, this setting lets the role view or update information on the **EMIS 1**, **EMIS 2**, **EMIS 3**, **Preschool**, or **Private** tabs (the **Custom** tab also requires an additional permission, described below). This Extra System Permission is also required to access the **Field Selection** tab **EMIS** subtab on the **SIS Student Search** screen.

  > *Note: If you grant a user access to view the EMIS tabs on the **Edit Student Profile** screen, the user can also edit the EMIS tabs on the **Edit Student Profile** screen. These security options provide all or nothing access for the user.*

Extra System Permissions – SIS

- **SIS – Daily Attendance Extended Permissions** – Opening this Extra Permission setting lets the role display, add, change, or delete existing absence records through the **Daily Attendance** screen on the **Teacher Menu**.

- **SIS – Period Attendance Extended Permissions** – This Extra Permission is not used by StudentInformation and will be removed in a future release.

- **SIS – Custom Profile Data** – Opening this Extra Permission setting lets the role display, add, change, or delete information on the **Edit Student Profile** screen **Custom** tab.

- **SIS – Enrollment Alerts** – Opening this Extra Permission setting lets the role display, add, change, and delete **Enrollment Alerts** from the **Portal** screen.

- **SIS – Assign Course Conflicts** – Opening this Extra Permission setting lets the role assign courses for a student that cause conflicts with that student's schedule.

- **SIS – Overfill Course Sections** – Opening this Extra Permission setting lets the role add assignments to course sections that would create an overfill.

- **SIS – Marks Cutoff Date** – Opening this Extra Permission setting lets the role edit or update the **Student Exception Credit** screen and the **Marks Cutoff Date** on the **Reporting Terms Maintenance** screen.

- **SIS – Delete All Family Groups** – Opening this Extra Permission setting lets the role display the **Remove existing groups in the district** check box on the **General** tab of the **Family Groups Wizard**.

- **SIS – Reassign Student Number** – Opening this Extra Permission setting lets the role reassign the student number on the **Edit Student Profile** screen **General** tab and select or de-select the **Auto-Assign Student Number** check box.

- **SIS – School – District Contact Code Mapping** – Opening this Extra Permission setting lets the role display the **District Codes** column on the **Contact Type Codes Maintenance** screen.

- **SIS – Add User – As Vendor** – Opening this Extra Permission setting lets the role select the **Is Vendor** check box on the **View User** screen of the **Security** menu.

SIS – Student – Edit Profile Node

In **Security – View Roles – Edit Sitemap Access**, the following Edit Profile nodes display under **SIS – Student – Edit Profile FY09**, **Edit Profile FY08**, **Edit Profile FY15**, and **Edit Student Profile**. If you have any roles with special security on **Edit Profile** (such as green dot or red X), you need to ensure all instances of the Edit Profile node are updated accordingly.

The Edit Profile Router controls access to all variations of the profile, so if you deny access to the Edit Profile Router, the user is not able to access any profile screen. You can set security on these nodes separately if needed.

VendorLink Permissions

The VendorLink node contains permissions to the methods a vendor application needs to access information in StudentInformation. The only available access setting you can define is Execute.

To enable access to a method for this role, click the space to the right of the Execute access setting until the Allow Access icon displays. To deny access to a method, click the space again until the Deny Access icon displays.

> **Note:** If you allow or deny access to the parent folder for a group of methods, the permission is applied to all of the methods unless you deny or allow access to a specific method. For example, in the following figure, the role allows access to all of the methods in the Students folder except GetStudentPersonal(s) – Medical Alerts and GetStudentSchoolEnrollment.

Resource Permissions

Navigation: StudentInformation – Management – Security – View Roles – Add New Role button or View Details icon – Edit Resource Permissions button

This screen is accessed by first selecting or creating a role, then clicking **Edit Resource Permissions** on that role's maintenance screen.

Click ✏ to view details of this role, or click **Add New Role** to create a role.

Click **Edit Resource Permissions** to view and set resource permissions for this role.

Clicking **Edit Resource Permissions** displays two tabs: **Reports** and **Notifications**. The **Reports** tab lets you modify view and update permissions for ad hoc reports, and the **Notifications** tab lets you modify view access for notifications.

Reports tab

This tab displays the StudentInformation resource permissions with the two access settings (**View**, **Update**) in front of each node. The resources display alphabetically within each level of the hierarchy. Access for a node can be toggled between Open, Shut, and Clear by clicking the space or icon to the right of each access setting name. You can also see hierarchical access for items that are not expanded (Open below, Shut below).

- Open ☑ – Indicates that the user with this role can access this resource and any other resource nested below this node in StudentInformation.

- Open below ☑ – Indicates that the user with this role can access at least one resource nested below this node in StudentInformation.

- Shut ✖ – Indicates that the user with the role cannot access this resource and any other resource below under this node in StudentInformation.

- Shut below ✖ – Indicates that the user with the role cannot access at least one resource nested below this node in StudentInformation.

- Clear ✓ ✖ – Indicates that the access is neither allowed nor restricted to this node.

The nodes can be expanded and collapsed using ▶ and ▼ to the left of the nodes.

Once you have configured the report permissions for this role, click **Save Permissions**.

In the above example, this role has **View** access to the **Assessment** and **Attendance** report types. This role has **Update** access to the **Assessment** Report Type but is denied **Update** access to the **Attendance** report type.

Notifications tab

The tab displays the notification resource permissions with the **View** access settings in front of each node. The notification resources display alphabetically within each level of the hierarchy. Access for a node can be toggled between Open, Shut, and Clear by clicking the space or icon to the right of each access setting name. You can also see hierarchical access for items that are not expanded (Open below, Shut below). For more information on notifications, see the *ProgressBook StudentInformation Notifications Guide*.

- Open ✓ – Indicates that the user with this role can subscribe to this notification rule or all notification rules nested below this notification category in StudentInformation.

- Open below ✓ – Indicates that the user with this role can subscribe to at least one notification rule nested below this notification category in StudentInformation.

- Shut ✗ – Indicates that the user with the role cannot subscribe to this notification rule or cannot subscribe any notification rules nested below this notification category in StudentInformation.

- Shut below ✗ – Indicates that the user with the role cannot subscribe to at least one rule nested below this notification category in StudentInformation.

- Clear ✓ ✗ – Indicates that the access is neither allowed nor restricted to this node.

The nodes can be expanded and collapsed using ▶ and ▼ to the left of the nodes.

Once you have enabled or disabled access to particular notification categories and/or rules for this role, click **Save Permissions**.

In the above example, this role has full notification access to the **Contacts**, **Medical**, and **VirtualClassroom** categories and all notifications within them. In the **Discipline** category, they only have access to **Discipline Referral** notifications but not **Discipline Incident** notifications.

> *Note: Users must still have the proper configurations in order to receive notifications (see the* ProgressBook StudentInformation Notifications Guide*).*

Display Role Access

Navigation: StudentInformation – Management – Security – Display Role Access

The Display Role Access screen is a read-only screen that displays the Sitemap access (see *"Sitemap Access"*) for a selected role.

- **School** – Select the appropriate school from the drop-down list.
- **Role** – Select the role for which you want to display the sitemap access from the drop-down list.
- **Show Selected Role** – Select this radio button to only show access for the role selected from the previous drop-down lists.
- **Show All Fixed Roles** (only available to ITC users with the "Is Privileged" check box marked on their user record) – Select this radio button to show access for all fixed roles.

Nodes will only display items which have defined access settings. Open (🟢) indicates that the user of the role can use the option in StudentInformation. Shut (❌) indicates that the user of the role is denied access to this option in StudentInformation. Clear (blank) or not listed indicates that access is neither allowed nor restricted to this node.

Assign Roles

Navigation: StudentInformation – Management – Security – Assign Role to Users

The Assign Role to Users option allows the operator to assign a role/school combination to one or more users at a time.

- **School** (required) – Select the school to which you want to assign the user(s).
- **Role** (required) – Select the role to which you want to assign the user(s).
- **Last Name** – The Last Name of the StudentInformation user(s) to filter.
- **First Name** – The First Name of the StudentInformation user(s) to filter.
- **Email Address** – The Email Address of the StudentInformation user(s) to filter.
- **Username** – The username of the StudentInformation user(s) to filter.
- **Domain** – Choose the Domain of the StudentInformation user(s) to filter from the drop-down list.
- **Administrative School** – Choose the administrative school of the StudentInformation user(s) to filter from the drop-down list.
- **Default School** – Choose the default school of the StudentInformation user(s) to filter from the drop-down list.

Click **Search** to list the StudentInformation users that match the criteria selected and that you have access to. See *"Find Roles"* for all of the filter and wildcard options.

- • **Available** – Users available based on the filter criteria.
- • **Assigned** – Move selected user(s) from Available to Assigned. The Assigned user(s) will be assigned the school/role defined at the top of the screen.
- • **Save Assigned Users** – Save the Assigned user(s) to the specified school/role.

The "Users Assigned Role at a Higher Level" grid shows what users have already been assigned this role at a higher level. For example, user SmithN is assigned role "Truant Reports" for Anytown Local Schools. When the operator pulls up Anytown High School (part of Anytown Local Schools) and role "Truant Reports," they will see user SmithN in the "Users Assigned Role at a Higher Level" grid.

Group Maintenance

Navigation: StudentInformation – Management – Security – View Groups

A group is a collection of users. Groups can be used for collection purposes, assignment of job functions, and/or assignment of security access. This section of the manual discusses how to find existing groups and make alterations to them or how to add new groups to StudentInformation.

> *Note: Although StudentInformation does allow sub-groups (groups within groups) please note that this functionality has not been thoroughly tested and is very seldom used. We do not recommend using this functionality unless you have done thorough testing. Also, please note that the Copy Security portion of the go-live process does NOT support sub-groups. If any district (in Live or Play) uses sub-groups, it will cause any subsequent use of Copy Security on future go-lives to fail. Sub-groups should NOT be used until all districts have been converted to StudentInformation and then only with detailed testing.*

Find Groups

Navigation: StudentInformation – Management – Security – View Groups

- **Add New Group** – Add a new group.
- **School** – Choose the school of the group(s) to filter from the drop-down list. This will limit your search based on the administrative school of the group.
- **Group Name** – The Name of the group(s) to filter. See *"Find Users"* for an explanation and examples of the use of wildcards in filters.

Click **Search** to list the groups that match the criteria selected and that you have access to.

In addition to matching the search filters, users must have an administrative school that you as the operator have security access to for the page where the search takes place.

- **Group Name** – Descriptive Name of group
- **School** – Administrative school of group
- 🖉 – View/Edit Details about a specific group
- 🗑 – Delete group

Remove Groups

Navigation: StudentInformation – Management – Security – View Groups

Click 🗑 to delete a specific group.

- **Ok** – Delete the specified group.
- **Cancel** – Do not delete the specified group.

Create/Update Groups

Navigation: StudentInformation – Management – Security – View Groups – Group tab

Click **Add New Group** to add a new group.

This page has standard add record, edit record, and delete record controls.

Records on this page are not deleted, but are inactivated instead. For information on reactivating records, see the *ProgressBook StudentInformation Getting Started Guide.*

Add/Edit Groups

- **Group Name** (required) – Enter the name of the new group (be as descriptive as possible).

- **Administrative School** (required) – Choose the administrative school from the drop-down list.

- **Context School** (required) – Choose the context school from the drop-down list.

- **Job Functions** (optional) – Check the appropriate Job Function(s) from the check boxes. Job Functions are optional and do not need to be specified.

The context school drop-down list and Job Function check boxes work together. The job functions indicate what job functions this group of users represent and the context school indicates the school to which those job functions apply. Job Function and context school determine what items on the Portal screen are visible to this group. Portal items have defined "Intended Audience" school and Job Function fields, and only roles with the appropriate context school and Job Function will see those items on their Portal page.

- **Save Group** – Save new group and apply additional settings to the new group. The group/administrative school combination must be unique (no other group can have the same combination) for the save to be successful.

- **Save and New** – Save new group and return to this page to enter another new group.

- **Return To View Groups Page** – Return to Management – Security – View Groups.

Assigning School/Roles

Navigation: StudentInformation – Management – Security – View Groups – Group Roles tab

Click ✏ to view/edit a specific group.

Click **Group Roles**.

- **School** (required) – Choose the administrative school from the drop-down list.
- **Role** (required) – Choose the role from the drop-down list. These will be both pre-defined roles that are a part of StudentInformation and roles that have been added by your school.
- **Add** – Add this school/role combination to this group. School/role combinations must be unique – you will receive a "not successful" message if you try to re-add a school/role combination.

> **The role was NOT successfully added to the group**

In the grid at the bottom of the tab is a listing of school/role combinations that have been assigned to this user. Click on 🗑 to delete a specific school/role combination from this group.

• **Return To View Groups Page** – Return to Management – Security – View Groups

Assign Groups

Navigation: StudentInformation – Management – Security – View Groups – Group Assigned Groups tab

Groups can be members of other groups forming a group hierarchy.

Click ✎ to view/edit a specific group.

Click on the **Group Assigned Groups** tab.

Filter List of Available Groups

Choose the school or group that you wish to filter by. Click **Search** to execute the filter and populate the **Available** box in the **Save Assigned Groups** section.

Save Assigned Groups

Groups that have already been assigned to this group will be in the **Assigned** box. Groups that are available but have not been assigned to this group will be in the **Available** box. Move groups from the **Available** to the **Assigned** box (and vice versa) as needed.

Click **Save** to save assigned groups. Once assigned, this group is now a member of the Assigned Groups.

Click **Return To View Groups Page** to return to Management – Security – View Groups.

View Group Members

Navigation: StudentInformation – Management – Security – View Groups – Group Members tab

Click ✏ to view/edit a specific group.

Click on the **Group Members** tab.

Lists the users and/or groups who are members of the selected group.

- **Type** – User or group
- **Group Name** – If group, name of group.
- **Last and First Name** – If user, last name and first name of user.
- **School** – Administrative school of user or group.
- **Username** – User Name
- **Domain** – Domain of user or group
- **Return To View Groups Page** – Return to Management – Security – View Groups.

View Group Members Of

Navigation: StudentInformation – Management – Security – View Groups – Member Of tab

Click ✎ to view/edit a specific group.

Click on the **Member Of** tab.

Lists the groups of which the selected group is a member.

- **Name** – Name of group
- **School** – Administrative school of group

- **Return To View Groups Page** – Return to Management – Security – View Groups

User Maintenance

A user account is necessary for users to access StudentInformation. The following sections describe how to create new and modify existing users in StudentInformation. StudentInformation user accounts must link to a CentralAdmin user account.

You can add new and edit existing users from the View Users screen located in the following path: StudentInformation > Management > Security > View Users.

Find Users

Several places in the Security module, a user needs to be searched for and selected. Most notably is the View Users option on the Security menu. Users can be found using any combination of the provided filters.

- **Add New User** – Add a new StudentInformation user.
- **Last Name** – The Last Name of the StudentInformation user(s) to filter.
- **First Name** – The First Name of the StudentInformation user(s) to filter.
- **Email Address** – The Email Address of the StudentInformation user(s) to filter.
- **Username** – The Username of the StudentInformation user(s) to filter.
- **Domain** – Choose the Domain of the StudentInformation user(s) to filter from the drop-down list.
- **Administrative School** – Choose the administrative school of the StudentInformation user(s) to filter from the drop-down list.
- **Default School** – Choose the default school of the StudentInformation user(s) to filter from the drop-down list.

Click **Search** to list the StudentInformation users that match the criteria selected and to which you have access.

The filters find any matches that contain the filter string unless you place a wildcard in the value to be filtered. For instance, searching for chris is the same as searching for *chris*. The * means that anything (including nothing) can come before chris and anything (including nothing) can come after chris. The search is not case sensitive. Here are some matches for the search string chris.

Chris, Christopher, mcchristopher, HS_Christoff, OttoChris

Searching for chris* means the matching entries must start with chris and end with anything (including nothing). The following are matches from the first example.

Chris, Christopher

If the search string is *chris, then the matching entries must end with chris. The following are matches from the first example.

Chris, OttoChris

Using a combination of several filters will further refine your search and more narrowly limit the number of users returned.

In addition to matching the search filters, users must have an administrative school that you as the operator have security access to for the page where the search takes place.

- **Sorting** – You may sort by any column (Domain, Username, First Name, Last Name, Email, Administrative School, Default School) in ascending or descending order by clicking on the column header.

- ✏ – View details about a specific StudentInformation user.

This page has standard add record, edit record, and delete record controls.

Records on this page are not deleted, but are inactivated instead. For information on reactivating records, see the *ProgressBook StudentInformation Getting Started Guide.*

Create Users

1. On the **View Users** screen, click **Add New User**.

   The **Add/Edit User** screen displays.

2. In the **Username** field, enter the user name you want to assign to the user. This is the name the user enters to log in to StudentInformation.

3. If you want to assign the user additional security permissions, select the **Is Privileged** check box.

   Note: The Is Privileged check box only displays for users with this check box selected in their own user account. Only assign this privilege to technology center personnel.

4. In the **First Name** field, enter the user's first name.

5. In the **Last Name** field, enter the user's last name.

6. In the **Employee Number** field, enter the user's employee number (numeric characters only).

7. In the **Domain** drop-down list, select the domain in which the user's account exists.

   Note: Once the user record is saved, you cannot change the user's domain. If you need to change the user's domain at a later time, contact your technology center.

8. In the **Email Address** field, enter the user's email address.

   Note: Ensure you enter the correct and unique email address for the user as this is the account to which his/her StudentInformation password is emailed.

9. Ensure the **Is Active** check box is selected to create an active StudentInformation account. If this option is not selected, the user account is not active, and the user is unable to log in to StudentInformation.

    Note: This option is selected by default when you create a new user.

10. In the **Administrative School** drop-down list, select the user's administrative school.

11. In the **Default School** drop-down list, select the school or school district that is in context by default when the user logs in to StudentInformation.

12. In the **Account Selection** drop-down list, select one of the following options:

    *   **Search By Username** – Enables you to link the StudentInformation user account to an existing CentralAdmin user account. This option is only available if the Staff: Link to Staff resource activity is assigned to your CentralAdmin user account.

    *   **Create New Central User** – Enables you to create a new CentralAdmin user. This option is only available if the Staff: Create Account & Profile resource activity is assigned to your CentralAdmin user account.

        *Note: The **Account Selection** drop-down list does not display for users not assigned the Staff: Link to Staff or Staff: Create Account & Profile resource activity in CentralAdmin.*

        Note: In the DASL.config, if you set BypassActiveDirectory to True, StudentInformation does not create a user in Active Directory or in CentralAdmin. You must create the user directly in ActiveDirectory, then within CentralAdmin, and then use StudentInformation to link a new staff member to the one you created in CentralAdmin.

13. If you selected **Search By Username** in the **Account Selection** drop-down list, perform the following steps. Otherwise, proceed to *step 14*.

    a. In the **Search (by Username)** field, enter the user's CentralAdmin user name, and then click **Go**.

        The CentralAdmin user account that matches the user name you entered displays in a grid below the **Search (by Username)** field.

    b. Select the check box in the row of the CentralAdmin user account you want to link to the StudentInformation user.

    c. Click **Save User**.

The user is linked to the selected CentralAdmin user account. Information about the linked CentralAdmin user account displays on the **Add/Edit User** screen.

14. If you selected Create New Central User, click **Save User**. To save the current StudentInformation user and create a new user, click **Save and New**.

   The following message displays: "The selected User was successfully updated."

   If your user account is assigned the appropriate access in CentralAdmin, both the StudentInformation and CentralAdmin user accounts are created, and the CentralAdmin account is linked to the StudentInformation account.

Edit Users

1. On the **View Users** screen, enter the search criteria to locate the user you want to edit, and then click **Search**.

   The users who match the criteria you entered display in the grid.

2. Click the edit icon in the row of the user you want to edit.

The **Add/Edit User** screen displays with the information for the selected user.

3. You can you perform any of the following tasks:

    • Modify whether or not the user has special privileges by selecting or de-selecting the **Is Privileged** check box.

    *Note: The **Is Privileged** check box only displays for users with this check box selected in their own user account. Only assign this privilege to technology center personnel.*

    • Modify the user's first name in the **First Name** field

    • Modify the user's last name in the **Last Name** field

    • Modify the user's employee number in the **Employee Number** field (numeric characters only)

    • Modify the user's email address in the **Email Address** field

    • Modify whether or not the user's account is active by selecting or de-selecting the **Is Active** check box

    • Modify the user's administrative school in the **Administrative School** drop-down list

    • Modify the user's default school in the **Default School** drop-down list

    • Modify the CentralAdmin user account linked to this StudentInformation user account by clicking the **edit icon** next to the linked CentralAdmin user account information. See *step 13* in *"Create Users."*

    Note: The edit icon does not display in the linked CentralAdmin user account information area for users not assigned the Staff: Link to Staff resource activity in CentralAdmin.

4. Click **Save**.

    The following message displays: "The selected User was successfully updated."

    The StudentInformation user account is updated.

Assign Roles

You can assign the roles and schools to which you want a user to have access on the User Roles tab on the Add/Edit User screen located in the following path: StudentInformation > Management > Security > View Users > User Roles Tab.

> *Note: To assign role/school combinations to a large number of users, use the Assign Role to User option on the Security menu.*

1. On the **View Users** screen, locate the user to which you want to assign roles. See *"Find Users."*

   The users who match the entered search criteria display in the grid at the bottom of the View Users screen.

2. Click the **edit icon** in the row of the user to which you want to assign roles.

   The Add/Edit User screen displays with the information for the selected user.

3. Click the **User Roles** tab.

4. In the **School** drop-down list, select the school or district to which you want to assign access.

5. In the **Role** drop-down list, select the role you want to assign to the user, and then click **Add**.

   The role assignment displays in the grid.

   Note: *If you try to add a role/school combination that already exists, a message displays indicating that adding the role was not successful.*

6. To add additional roles, repeat *step 4* and *step 5*.

7. When you are done assigning roles, click **Return To View Users Page** to return to the blank **View Users** screen.

Staff Member Impersonations

Navigation: StudentInformation – Management – Security – View Users – Staff Member Impersonations tab

Click the **edit icon** to view/edit a specific user.

Click the **Staff Member Impersonations** tab to view and edit Staff Member Impersonations for this StudentInformation user. Staff impersonation is the ability in StudentInformation for a user to be able to do tasks as if they were the staff member that they are impersonating. Users can also impersonate all staff members in the school if so specified.

In the grid at the bottom of the tab is a listing of school/school year/staff combinations that have been assigned to this user. Click 🗑 to remove a specific Staff Member Impersonation assignment.

Click **Add** to add staff impersonation entries for the selected user.

The school and school year is pre-selected based on the current working school and school year. The school will be a district if a district is in context. District impersonations trickle down to the buildings and enable building impersonations for the school year, staff, and permissions selected. The list of staff members is based on the school district associated with the pre-selected school. Select any of the staff permissions that you wish to set for this school/school year/staff combination. If you try to add a combination that already exists, you will receive a message that indicates that the Add was not successful.

Available Permissions include: Full (all permissions), Fee Collect, EZ Query, Attendance, Marks, and Medical.

- **Fee Collect** – Users with Fee Collect impersonations may collect full fee payments using the Teacher Menu.
- **EZ Query** – Users with EZ Query impersonations may view students in EZ Query.
- **Attendance** – Users with Attendance impersonation may take attendance using the Teacher Menu.
- **Marks** – Users with Marks impersonations may enter marks using the Teacher Menu.
- **Medical** – Users with Medical impersonations may view private medical information using the Teacher Menu.
- **Save** – Click to save the selected Staff Member – Selected Permissions combination. It will appear on the grid as shown in the previous screen shot.

Impersonations are school year specific. To change the selected school/school year, use the **Change Working School** screen that is accessed by clicking on the working school in the upper right hand corner of the StudentInformation screen.

> ⚠️ **Caution:** *As of StudentInformation v10.2.0, Staff Member Impersonations are now copied from year to year as part of the School Year Initialization process. Once Staff Member Impersonations are entered for a user, they will be carried on to following years as part of School Year Initialization.*

- **Return To View Users Page** – Return to Management – Security – View Users

Assign User Groups

Navigation: StudentInformation – Management – Security – View Users – User Groups tab

Click the **edit icon** to view/edit a specific user.

Click the **User Groups** tab to view and edit User Groups for this StudentInformation user.

Filter List of Available Groups

Choose the school or group that you wish to filter by. Click **Search** to execute the filter and populate the **Available** box in the **Save Assigned Groups** section.

Save Assigned Groups

Groups that have already been assigned to this user will be in the **Assigned** box. Groups that are available but have not been assigned to this user will be in the **Available** box. Move groups from the **Available** to the **Assigned** box (and vice versa) as needed.

Click **Save** to save assigned groups. Once assigned, this user is now a member of this group.

Click **Return To View Users Page** to return to Management – Security – View Users.

View Group Memberships

Navigation: StudentInformation – Management – Security – View Users – View Group Memberships tab

Click **edit icon** to view/edit a specific user.

Click on the **Group Memberships** tab.

The **Group Memberships** tab lists all the groups of which this user is a direct or indirect member.

- **Name/School** – Name of the group/school combination that this user is a member of.
- **Return To View Users Page** – Return to Management – Security – View Users.

Reset Password

Navigation: StudentInformation – Management – Security – View Users – Reset Password tab

The Reset Password option gives the operator the ability to reset the password of the selected user.

Click the **edit icon** to view/edit a specific user.

Click the **Reset Password** tab.

Click **Reset Password** to reset the displayed user's password. You will receive a message "The User Password was successfully reset." The new password is reset and will be immediately emailed to the email address on the StudentInformation user's account.

If the user's domain is not the same as the default domain, the following message is displayed and the **Reset Password** button is not available.

This indicates that the user account is on a server local to the user and the user should use the local password change or reset mechanisms for this account.

System administrators can set a variable in the Web.config file to enable or disable the ability of users to reset their password. With Forms Authentication enabled, setting ScreenAccessibility to true allows the Reset Password button to be displayed and allows passwords to be reset. Setting ScreenAccessibility to false prevents the Reset Password button from being displayed, disabling the ability to reset passwords.

For schools that want to have specific people in their buildings or district to be able to reset passwords but not alter the user accounts in any other way, they can grant access to only the Reset Password node. This will only make the **Reset Password** tab available to the person they wish to assist in resetting passwords.

Click **Return To View Users Page** to return to View Users screen and not reset the password.

Caution: *StudentInformation (and DSL) passwords expire after 120 days, and must have a minimum of 4 characters. After the expiration time, you must change your StudentInformation password. StudentInformation does not retain a history of previous passwords, nor does StudentInformation require "complex" passwords consisting of at least 1 number, at least one capital letter, and at least one lower-case letter, though these types of passwords are more secure, and should be chosen by users.*

Delete Users

1. On the **View Users** screen, locate the user you want to delete. See *"Find Users."*

   The **View Users** screen displays with the users who match your search criteria

2. Click the delete icon in the row of the vendor you want to delete.

The following message displays, "Are you sure you want to delete the following User? [User's First and Last Name] – [User Name]?"

3. Click **OK** on the deletion confirmation message.

The user is deleted.

Vendor Maintenance

To enable vendors to access information in StudentInformation, the vendor must exist in StudentInformation as a user and link to a vendor in CentralAdmin. Some vendors are loaded into StudentInformation by default. You must assign the VendorLink roles to the school to which you want the vendor to have access.

You can create, find, and modify vendors from the **View Users** screen located in the following path: StudentInformation > Management > Security > View Users.

Create Vendors

When you create a vendor in StudentInformation, you must create a corresponding vendor in CentralAdmin. Only users assigned the Vendor Admin role in CentralAdmin can create vendors in CentralAdmin.

1. On the **View Users** screen, click **Add New User**.

2. On the **Add/Edit User** screen, select the **Is Vendor** check box.

*Note: The **Is Vendor** check box only displays if your role has security access to add a user as a vendor. See "Extra System Permissions – SIS."*

The **Add/Edit User** screen displays the **Vendor** and **Vendor Roles** tabs, which contain fields for vendor information.

3. In the **Vendor Name** field, enter the vendor's name.

4. Ensure the **Is Active** check box is selected to create an active StudentInformation vendor. If this option is not selected, the vendor is not active, and the vendor is unable to access information in StudentInformation.

   Note: This option is selected by default when you create a new vendor.

5. To link the vendor to a vendor in CentralAdmin, select the **Link to Central** check box.

6. Click **Save**.

   If you selected the **Link to Central** check box, and your user account in CentralAdmin is assigned the Vendor Admin role in CentralAdmin, the **Create Vendor** screen in CentralAdmin displays. On the **Create Vendor** screen, you can create the vendor in CentralAdmin. For more information, see the *ProgressBook CentralAdmin User Guide*.

The following message displays to indicate that the vendor is successfully added to StudentInformation: "The new User was successfully added." If the vendor is linked to CentralAdmin, the **Security – Vendor** screen displays.

4. Proceed to *"Assign Roles to Vendor"* to assign roles to the vendor.

Find Vendors

To find a vendor, on the **View Users** screen, enter all or part of the vendor's name in the **Last Name** or **User Name** field, and then click **Search**. You can also use a wild card search (*). Both vendors and users that match your entered search criteria display.

Edit Vendors

1. On the **View Users** screen, enter the search criteria to locate the vendor you want to edit, and then click **Search**. Refer to *"Find Vendors."*

   The vendors and users that match your entered criteria display.

2. Click the **edit icon** in the row of the vendor you want to edit.

   The Add/Edit User screen displays with the information for the selected vendor.

3. You can assign roles to the vendor. See *"Assign Roles to Vendor."*

Assign Roles to Vendor

Roles define the information to which a vendor has access. By default, StudentInformation contains a role for each of the currently approved vendors. You can create a new or edit an existing role for a vendor if you want to modify the information a vendor can access. For more information about defining roles for VendorLink, see asdasdavendorlinke permissions

You must assign the appropriate role and school to the default vendors and the vendors you manually create in StudentInformation.

1. Access the existing vendor, as described in *"Edit Vendors,"* or create a new vendor, as described in *"Create Vendors."*

   The Add/Edit User screen displays with the information for the selected vendor.

2. On the **Vendor** tab on the Add/Edit User screen, click the **Vendor Roles** tab.

3. In the **School** drop-down list, select the school to which you want to assign the vendor access.

4. In the **Role** drop-down list, select the appropriate role for the vendor, and then click **Add**.

   The role assignment displays in the grid at the bottom of the tab.

5. To assign additional roles to the vendor, repeat *step 3* and *step 4*.

6. When you are done assigning roles, click **Return To View Users Page** to return to the blank **View Users** screen.

Remove Roles from Vendor

1. Access the existing vendor, as described in *"Edit Vendors."*

2. On the **Vendor** tab on the Add/Edit User screen, click the **Vendor Roles** tab.

3. Click the **delete icon** in the row of the role assignment you want to delete.

   The selected role assignment is removed.

Delete Vendors

1. On the **View Users** screen, locate the vendor you want to delete. See *"Find Vendors."*

   The **View Users** screen displays with the vendors and users that match the search criteria.

2. Click the **delete icon** in the row of the vendor you want to delete.

    The following message displays, "Are you sure you want to delete the following User? [Name of Vendor] – [Name of Vendor]?"

3. Click **OK** on the deletion confirmation message.

    The vendor is deleted.

Staff Member Maintenance

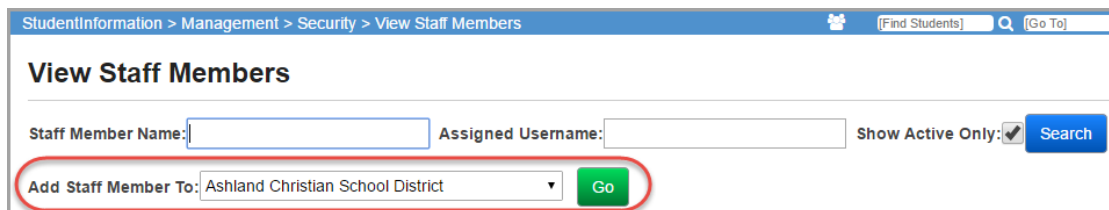**Navigation: StudentInformation – Management – Security – View Staff Members**

You can manage staff members in the following ways:

*   *"Add Staff Members"*
*   *"Edit Staff Members"*
*   *"View/Edit Staff Member Schools"*
*   *"View/Edit Staff Member Associations"*

Add Staff Members

Navigation: StudentInformation – Management – Security – View Staff Members

1. On the **View Staff Members** screen, in the **Add Staff Member To** drop-down list, select the district to which you want to add a staff member.

2. Click **Go**.

3. On the **Security – Staff Member** screen, enter the following required information about the staff member:

*   **Staff Code** – Four character code that uniquely identifies this staff member
*   **First Name**
*   **Last Name**
*   **Social Security Number**

- **State Staff ID** – Unique state-generated ID; can be up to nine numbers in length (or two letters followed by seven numbers). Also known as the credential ID and used for pre-identification exports, student subject records, program records for contracted staff, and ODE's D3A2 initiative

  Note: *A value of nine 9s can be used to indicate a post-secondary enrollment teacher. If the **State Staff ID** field is filled in, the value is used in place of the staff member's social security number.*

  Note: *Either **State Staff ID** <u>or</u> **Social Security Number** is required.*

4. Optional: Enter information in any of the following optional fields:

   - **Name Prefix** – Mr., Mrs., Ms., Dr.
   - **Middle Name**
   - **Last Name Suffix** – Jr., Sr., III, etc.
   - **Email Address** – Staff member's home email address

     Note: *The school email address is entered on the user record. (See "Create Users.")*

   - **Telephone** – Staff member's home phone
   - **Telephone Is Unlisted** – Select if the home phone number is unlisted
   - **Start Date** – Date the staff member started working in this district
   - **Stop Date** – Date the staff member stopped working in this district
   - **Primary School ID**
   - **Is Active** – Selected by default, the staff member is active and can be used on scheduling records; deselect if the staff member is no longer active in this district and cannot be used on scheduling records

- **Comments** – Any additional comments about this staff member

5. Enter the staff member's home address information (**Address**, **Address 2**, **City**, **State**, **Zip**) manually, or use the auto-complete and validate functionality as follows:

   Note: Address validation only works if ***Bypass Address Standardization*** *is de-selected.*

   a. In the **Address** field, start typing the street number and name.

   As you type, suggested addresses display in a drop-down list.

   b. Click the correct address in the list to select it.

The system validates the selected address. If the address is valid, the **Zip Code** field populates, and the ☑ icon changes to ✅ (green).

Address:	6770 W Snowville Rd
City:	Brecksville
Zip:	44141-3212 ✅

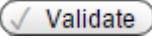If the ☑ icon in the **Zip Code** field does not change to ✅ (green), the address is invalid. To manually validate the address:

i. Hover over ☑ until it changes to (✓ **Validate**).

ii. Click (✓ **Validate**).

Address:	6770 W Snowville Rd
City:	Rocky River
Zip:	(✓ Validate)
Telephone:	Address not valid. Click to validate.
Start Date:	📅

iii. In the **ADDRESS NOT VALID** window, click the address to confirm that it is correct.

Address:	**ADDRESS NOT VALID**	X
City:		
Zip:	Click here to change your address	
Telephone:	Click here to certify the address is correct	
Start Date:	(6770 W Snowville Rd Rocky River OH)	
Primary School Id:		

*Note: When you confirm the address, the **Bypass Address Standardization** check box is automatically selected.*

6. Click **Save**. Or, to continue adding staff members, click **Save and New**.

Edit Staff Members

Navigation: StudentInformation – Management – Security – View Staff Members

1. On the **View Staff Members** screen, search for the staff member you want to edit by entering all or part of the **Staff Member Name** and/or the **Assigned User Name**.

2. Click **Search**.

A list of staff members matching your search criteria displays.

3. In the row of the staff member you want to edit, click ✎ .

*Note: To delete the staff member, click 🗑 , and then click **OK** on the delete confirmation message.*

4. On the **Security – Staff Member** screen, make any needed changes, and click **Save**. (For information about this screen, see *"Add Staff Members."*)

View/Edit Staff Member Schools

Navigation: StudentInformation – Management – Security – View Staff Members – Staff Member Schools tab

The View/Edit Staff Member Schools defines what assignments this staff member has for the various school and school years.

Click ✏ to view/edit details of a specific Staff Member.

Click the **Staff Member Schools** tab.

Click 🗑 to delete (inactivate) a current school/school year/job function record.

Click ✏ to edit a staff member's a specific school/school year/job function record.

Click **Add** to add a new staff member's school/school year/job function record. You will receive the screen below.

- **School** (required) – Choose the school from the drop-down list.
- **School Year** (required) – Choose the school year from the drop-down list.
- **Allow Staff Member to view all Students in EZ Query** (optional) – IMPORTANT! Currently this check box only affects student access when using EZ Query SIS Student Search and Upcoming Birthdays. Eventually other EZ Query pages will use this check box functionality.
  - If selected, the user will have access to all students in EZ Query SIS Student Search and Upcoming Birthdays in the school and school year selected, with or without Impersonations, regardless of their Job Function.
  - If de-selected and there is no Job Function or a Job Function other than Teacher or Counselor, the user will have access to all students in EZ Query SIS Student Search and Upcoming Birthdays in the school and school year selected, with or without Impersonations.
  - If de-selected and the Job Function = Teacher, the user will only have access to students in EZ Query SIS Student Search and Upcoming Birthdays in the school and school year selected that are assigned to course sections that the user teaches. If Impersonations are used, then the user will also inherit the Impersonation access.
  - If de-selected and the Job Function = Counselor, the user will only have access to students in EZ Query SIS Student Search and Upcoming Birthdays in the school and school year selected that are assigned to the user in a counselor role. If Impersonations are used, then the user will also inherit the Impersonation access.
- **Is Active** (optional) – Check if this school/school year combination is Active.
- **Selected Job Functions** – Select the Job Function(s) that apply to this Staff Member by moving them from the Available Job Functions side of the dual select box to the Selected Job Functions side. Job Functions control how a staff member functions in StudentInformation. Three Job Functions currently have special functionality in StudentInformation.
  - **Counselor** – A staff member must have a job function of Counselor before they display in the Counselor Maintenance or Counselor drop-down lists.
  - **Teacher** – A staff member must have a job function of Teacher before they display in the Teacher drop-down lists for that specific school.
  - **Superintendent** – A staff member must have a job function of Superintendent before they display on the custom transcript or custom report cards (with the proper keyword) as the Superintendent of the district.

    ⚠ *Caution: Job Functions also play a role in ProgressBook. StudentInformation Staff Members with job functions of All, Teacher, Principal, Secretary, Cafeteria Worker, and/or Counselor will be added to the ProgressBook Staff table for the specified school.*

- **Save** − Saves the current job role selections.

- **Cancel** – Cancel the current selection.
- **Return To View Staff Members Page** – Return to Management – Security – View Staff Members.
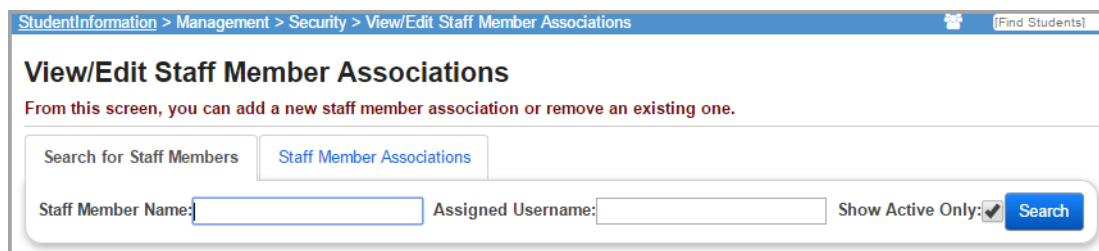
View/Edit Staff Member Associations

Navigation: StudentInformation – Management – Security – View/Edit Staff Member Associations

Each district should create one staff member record for each member of their staff. Most schools and districts will also provide each of their staff members with a user account to access StudentInformation. The intent of the View/Edit Staff Member Associations page is to associate a user account with a Staff Member. Once such an association is created, the user account will have access to perform any task as that staff member that they have been given access to on the site map.
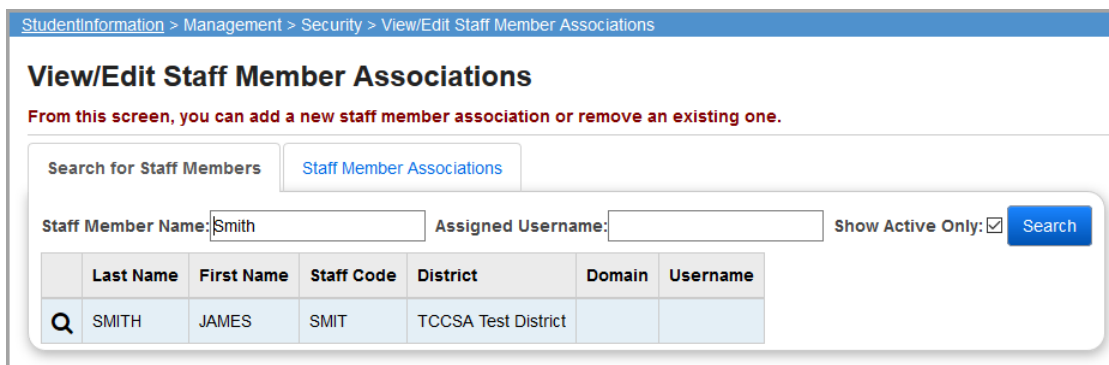
Staff Member Associations tie a login account (username) to a staff record (to which the school then attaches their course sections and those course sections' students. When a user is deleted, Staff Member Associations are removed for that user.

> **Note:** A user will only see students that they have access to when using certain functions in EZ Query and the Teacher Menu. Access to a student is accomplished through Staff Member Associations or Impersonations (see *"Staff Member Impersonations"*).

1. Use the filters to find the specific Staff Member. Click **Search** to execute the filter.

2. Click 🔍 to select the Staff Member you wish to associate.

If the Staff Member is already associated with a user, you will receive the message below. Click **Remove Staff Member Association** to remove the existing association. After confirmation, you will be returned to the View/Edit Staff Member Associations Screen.

3. Use the filters to find the specific user. See *"User Maintenance."*

A user account is necessary for users to access StudentInformation. The following sections describe how to create new and modify existing users in StudentInformation. StudentInformation user accounts must link to a CentralAdmin user account.

You can add new and edit existing users from the **View Users** screen located in the following path: **StudentInformation > Management > Security > View Users**.

See *"Find Users"* for more information on the filter criteria.

4. Click **Search** to execute the filters and search for a user.

3. Click 🔍 to assign the user to the Staff Member Selected.

4. Click **Ok** to assign the specified user to the Staff Member.

The following confirmation message displays.

Security Reports

Staff Listing (STAFF)

The Staff Listing (STAFF) report allows you to display and sort staff members by job function and staff code.

> *Note: Running this report at the district level will only display staff members who have district access. It will not display all staff members at the district. Running this report at the building level will only display staff members for that specific building. Staff members with no job function, will display on the STAFF report with a job function of "Not Specified."*

- **Job Function** (option) – Choose one or more job functions – which are defined for each staff member.
- **Sorting Options** (optional) – Choose one or more sort options for your report.
- **Delivery Method** (required) – See the Batch/Report Management documentation for further details.
- **Email Address** (auto populated from your StudentInformation profile)
- **Description** (optional) – If entered, displays on the **Batch/Report Management** screen.

- **Submit** – Click to submit this report to the Batch/Report Management application. Please see the Batch/Report Management documentation for further details.

REPORT: SI - REPO STAF				ASHLAND HIGH SCHOOL				RUN AT 9:36 AM 8/11/2017		
SCHOOLYEAR: 2016-2017				STAFF LISTINGS				PAGE 1 OF 2		
STAFF NAME	STAFF CODE	STATE STAFF ID	JOB FUNCTION	ADDRESS	ADDRESS LINE 2	City	STATE	ZipCode	Telephone
Mrs. Christine ▓▓▓	▓▓▓	▓▓▓	Teacher						
ERIC ▓▓▓	▓▓▓	▓▓▓	Teacher						
KELLY ▓▓▓	▓▓▓	▓▓▓	Teacher						
To Be Announced	▓▓▓		Teacher						
LYNAE ▓▓▓	▓▓▓	▓▓▓	Teacher						
JANEL ▓▓▓	▓▓▓		Teacher						
KATHERINE ▓▓▓	▓▓▓	▓▓▓	Teacher						
CHARLES ▓▓▓	▓▓▓	▓▓▓	Teacher						
MARTHA ▓▓▓	▓▓▓	▓▓▓	Teacher						
MELISSA ▓▓▓	▓▓▓	▓▓▓	Teacher				OH		
Nichole ▓▓▓	▓▓▓	▓▓▓	Teacher				OH		
JESSICA ▓▓▓	▓▓▓		Teacher, Counselor				OH		

Implementing StudentInformation Security

Suggested Practices

The following items are suggested practices for using the StudentInformation Security system.

Step 1 – Determine Type Security Management

Determine what type of security management your district wants to utilize: centralized, decentralized, or a combination.

- **ITC Controlled** – All security administration is done at the ITC level by ITC staff.
- **Centralized** – All security administration is done at the district level by a centralized and usually small number of people.
- **Decentralized** – Moves the security administration to the building level.
- **Combination** – Some of the security administration takes place at the district level (centralized) while certain other tasks take place at the building level (decentralized).

Step 2 – Determine Type of Staff Members and Access

Determine what types of staff members you have, and the type of access you want them to have in StudentInformation. This information will help you determine what roles to use/create and what groups to create and configure. Some questions to assist you this area include:

1. Will teachers (substitute also secretary, principal, guidance counselor) at all the buildings in the district have the same access to StudentInformation or will access vary by building?

2. Will each of these groups of people have the same access in all buildings (whether they teach in that building or not) or only in the building(s) in which they work?

3. What special supplemental jobs or tasks do staff members have that will require additional access in StudentInformation?

Step 3 – Review and Create Roles

At this point, you should review the list of pre-defined roles and determine which of these roles you intend to use and for which population of users. More information on predefined roles is available in the next section of the manual. Are the pre-defined roles sufficient to provide the necessary access to StudentInformation or are there gaps that will require you to create your own roles for specific types of staff members or additional staff tasks?

With this information, you can create the roles that you will need for your school and/or district. As you create these roles, use names that define the access you are granting. If in a centralized model, define the administrative school as the district and do not set any working schools. In a decentralized model, each building would create their own roles using their building as the administrative school. In a combination model, the district staff would create some roles for use by district staff only, while other roles where the working school includes the buildings that will be assigning this role.

Step 4 – Create Groups (as needed)

Step 5 – Assign Role/School Combinations to Groups (as needed)

and/or

Step 6 – Assign Role/School Combinations to Users (as needed)

There are two ways to proceed from this point. You can begin assigning role/school combinations to users or you can create a group of users then assign the role/school combinations to the group of users. Assigning role/school combinations to users works well if you have a lot of staff members with different needs, thus not allowing for more than one user per group. Creating a group and assigning the role/school combinations to the group works much better if you have many users that need the same access. For example, if you are in a small school where there is only one guidance counselor and 20 teachers, you may want to assign the needed roles directly to the guidance counselor's account while creating a group for the teachers and assigning the role/school combination to the group for the teachers.

Step 7 – Create User Accounts

Step 8 – Put Users in Groups (as needed)

Once you have your group access configured and user created, the final step is to put the users into the appropriate groups.

ESC StudentInformation Account Management

ESC staff members frequently serve multiple schools. Here are some options on setting up ESC staff members in StudentInformation.

If the ESC and the served schools are both on StudentInformation:

This method gives the ESC staff member a single StudentInformation user account with access to multiple school districts and buildings.

- The ESC staff member is set up in StudentInformation at the ESC with a StudentInformation user name and password.
- The served school who wants the ESC staff member to have access to their StudentInformation data sets up a specific group/role with the privileges that will give the ESC staff member the access they need to specific StudentInformation screens and specific buildings in that served school district.
- ITC StudentInformation support can then be notified of the name of the applicable group/role and ITC StudentInformation support can go to the served school and assign the ESC staff member to that group/role. The served school cannot do this because normally they won't have access to that ESC staff member in StudentInformation.

If the ESC is not on StudentInformation, but the served schools are on StudentInformation:

This method gives the ESC staff member a StudentInformation account for each school they serve. However, it works around the need for unique email addresses for each StudentInformation user account.

- The ESC staff member is set up in StudentInformation at each served school and will have a separate StudentInformation user name for each served school.

- The ESC staff member's email address can be used when creating the first StudentInformation user account.

- When creating subsequent StudentInformation user accounts, a unique email address will be required. To work around this issue, a "+1", "+2", etc. can be added to the email address before the domain name. For example, chris+1@noacsc.org and chris+2@noacsc.org will both be sent to chris@noacsc.org.

Pre-Defined Roles

StudentInformation State Support recommends Pre-Defined Roles not be used at this time.