Security Administrator Guide

Release 2019

June 2018

SISSAG-010104

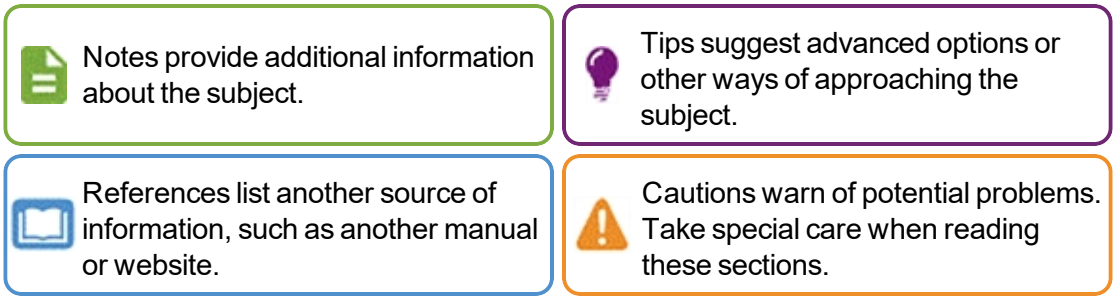
About This Manual

Edupoint Educational Systems, LLC. develops software with multiple release dates for the software and related documentation. The documentation is released in multiple volumes to meet this commitment.

This document serves as a reference for Edupoint's recommendations and Best Practices for Synergy processes. Due to the complex nature and myriad configurations possible within the Synergy software, it is not feasible to include every possible scenario within this guide.

Conventions Used in This Manual

- **Bold** indicates user interactions such as a button or field on the screen.
- *Italics* indicate the option to select or text to enter.
- Notes, Tips, References, and Cautions appear in the margin to provide additional information.



Before You Begin

Before installing any of the Edupoint family of software products, be sure to review the system requirements and make sure the district's computer hardware and software meet the minimum requirements.

Software and Document History

Document Version	Release Date	Software Release	Description
1.0	Oct 2015	10	Initial release of this document
-	Oct 2015	10.01	No changes required
-	Nov 2015	10.02	No changes required
-	Apr 2016	10.03	No changes required
2.0	Jul 2016	10.04	Updated
3.0	Dec 2016	10.05	• Added PAD Security Guidelines • Added Security Definition Guidelines • Added Business Objects Overview
-	May 2017	2018	No changes required

Document Version	Release Date	Software Release	Description
4.0	Oct 2017	–	Updated screenshots and captions for quality and consistency
5.0	Dec 2017	2018.01	• Added Setting Screen-Level Security in Admin Configuration • Added Setting Field-Level Security in Admin Configuration • Added *Update My Records Only* option to Customizing User Group Rights and Customizing User Rights • Added **Delete All Rows** permission in Setting Global Screen Rights, Setting User Access, and Setting User Group Access • Added Setting Document Security • Added Hiding Synergy Options
-	Jun 2018	2019	No changes required

Table of Contents

Chapter 1: Overview

Overview of Synergy SIS Security

There are four areas of security:

- PAD Security – Determines which users can view or update specific Synergy SIS screens.
- Business Object Security – Determines which individual fields users can edit on Synergy SISscreens.
- Organization and Year Security – Determines which users can view or edit data for schools and school years.
- User and User Group Security – Handles security settings for individual users or for user groups.

This guide outlines PAD security and Business Object security to define user access to specific areas with Synergy SIS, including TeacherVUE and Grade Book.

For more details on Organization/Year and User/User Group security, see the *Synergy SIS – System Administrator Guide.*

You can export and import security settings with the Generic Conversion Tool. For more details, see the *Synergy Data Conversion Guide*.

Implementation Considerations

What are the default user security settings?

Use one of two methods in setting Global Access rights:

- Give all users access to read/write all screens and fields, then specify security through user groups.
- Forbid access to all users, then specify security through user groups.

If forbidding access to all users, make certain the Admin user/user group has read/write access to everything. Otherwise, you can lock the admin user out of the system.

Use the first option if users should have access to view or update most screens. If only select users view or update data, use the second option.

What user groups need to be created?

Edupoint recommends setting security for user groups as much as possible to simplify the security setup. Synergy SIS security rights always move from most restrictive to least restrictive. Therefore, if a user belongs to two user groups with different settings for the same field, the user maintains the least restrictive access. For example, if one group has view rights but the other group has update rights, the user maintains update rights.

The order of security inheritance is:

1. Global
2. Public
3. User Group
4. User

> For more information on creating user groups, see the *Synergy SIS – System Administrator Guide*.

A typical district has three types of user groups:

- Organization-based – Groups that have access to view or update information for specific organizations in the district. For example, staff for a specific school with update access for only their school.
- Role-based – Groups that have access to view or update information based on their role at the district or school. For example, principals generally have security roles that do not change.
- Security-based – Groups that have access to view or update specific information based on security rights. For example, a group of users with the ability to update student addresses.

User groups sort alphabetically, so you should create a naming scheme to keep similar groups together. The below list contains sample user group names.

Organization-Based	Role-Based	Security-Based
Org – School Name – Update	Role – Principal	Sec – Discipline – Update
Org – School Name – View	Role – Secretary	Sec – Discipline – View
Org – District Name – Update	Role – District Administrator	Sec – Attendance – Update
Org – District Name – View	Role – Information Technology	Sec – Attendance – View
	Role – Nurse	Sec – Grades – Update
	Role – Office Clerk	Sec – Grades – View
	Role – Attendance Clerk	Sec – TXP – Admin
	Role – Teacher	Sec – TXP – User

Edupoint recommends creating all user groups before modifying security settings.

How should security be configured?

Set up security settings in the following order:

1. Screen Security
2. Business Object Security
3. Property Security

If a user group does not have access to a screen, you do not need to configure security for the business objects and properties in that screen for that user group. However, if using security to control access to a business object, you control access wherever it appears. Many business objects appear on multiple screens.

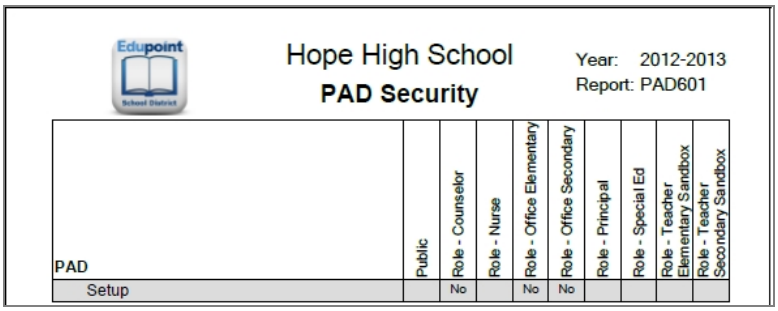
For a basic list of business objects to secure, see Business Objects Overview.

The PAD Security screen determines which screens and reports display in the Navigation Tree for each user group. In addition, the PAD Security governs certain items not in the PAD Tree, such as GBSecurity and Non PAD.

For more information on the items controlled by the PAD Security screen, see Setting Global Screen Rights.

What security settings should each user group have?

After defining user groups, determine the security settings for each user group. The Security module reports can display security settings associated with all user groups for both PAD screens and business objects. For example, the PAD601 – PAD Security report shows whether a group has been assigned access or inherited access to a screen.



Hope High School
PAD Security
Year: 2012-2013
Report: PAD601

PAD	Public	Role - Counselor	Role - Nurse	Role - Office Elementary	Role - Office Secondary	Role - Principal	Role - Special Ed	Role - Teacher Elementary Sandbox	Role - Teacher Secondary Sandbox
Setup		No		No	No				

PAD601 PAD Security Report

PAD Security Screen

PAD Security Guidelines

General

- Review available options in the Menu list before setting security for each screen. For instance, you can allow school office staff to **Edit Staff Data** on the Staff screen, but not run the **Mass Assign Badge Number** process.
- Review screens and tabs for confidential information before assigning View Only permissions. For example, most users should not access the **Private** tab of the Health screen.

- Use caution when securing items that do not have a unique PAD tree icon, such as the **User Preferences > Report Interface** screen. Securing these items may have a negative impact on functionality system wide.

View-Only

- Allows users to view all fields on a screen and disables buttons, Menu items, and certain links.
- Do not set at the node level on the PAD Tree.
- Allows access to less complicated screens or to allow users to look up information. For example, Health Office personnel can access the Student Classes screen to locate students for medication requests.

Public Users

- Leave a node level blank if the majority of User Groups can access the screens under a node.
- Set a node to deny public access before granting access to a specific user group to determine if the group has access when diagnosing an account issue.

TeacherVUE

- Set TeacherVUE accounts to have specific access to all required screens, even with Public access enabled.
- Set navigation groups to display all screen and report icons.
- TeacherVUE user groups must have specific access to the **Grade Book** node if this node denies Public access to avoid issues.
- Use the Grade Book Security screen to configure access to screens, links, buttons and features within Grade Book.
- Do not secure the **TeacherVUE Views** Node. Secure individual screens as needed.

Non-PAD Nodes

- Do not directly secure the **Non-PAD** node. Items available to secure under the Non-PAD node display as details for specific screens and require individual security.

Cautions

- Use caution when setting security on the **Security** node, PAD Security and Security Definition screens. Do not set Public access to *None* without first granting access to an admin user.
- Sign in using an account set up with specific user groups after assigning security to ensure that settings have the desired effect.
- Assign access to System module, Data and Maintenance screen to only a few specific individuals and not an entire user group.

- Assign access to Menu items **Save as Report** and **Allow Results to be Edited** on the the Query screen to a few individuals and not an entire user group.

Security Definition Guidelines

General

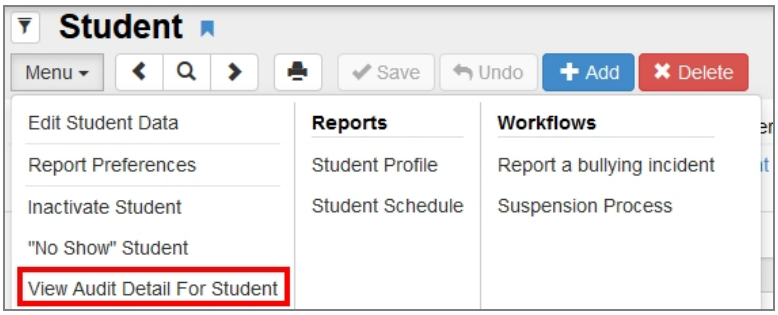
- Review all fields on screens set to *View Only* to avoid privacy concerns. For example, the SSN field on the Staff screen should not display for all users.
- Use **Security Def** to secure fields as *View* when allowing users to run reports or update only specific fields on a screen.
- Sign in using an account set up with specific user groups and click all **Show Detail** buttons to determine the need for additional security.
- Use caution when setting a BO as *None*. This might cause screens to not load or reports to fail if the loading process calls the BO.

Chapter 2: Auditing

Auditing Overview

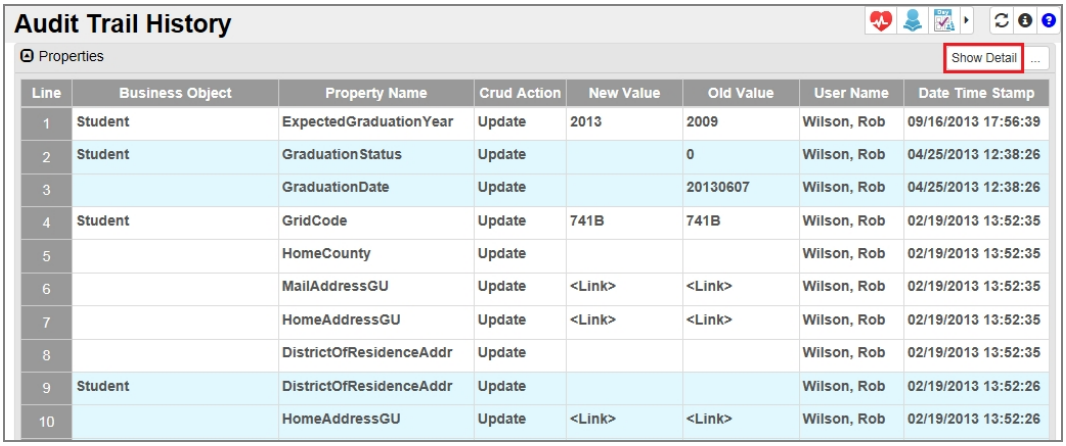
Auditing in Synergy SIS logs any changes made to the data in the screens. Enable auditing on all screens and business objects, or assign a specific type of auditing to each business object, such as a phone number.

After you enable auditing, the system generates a log of all changes to a record for any screen. To access the log from any screen, select **View Audit Detail** under the **Menu**.



Student Screen

- The Audit Trail History screen lists the **Business Object** and the modified **Property Name**.
- The **Crud Action** column lists whether the change is an addition, an update, or a deletion.
- The **Old Value** column displays the previous value, and the **New Value** column displays the current value.
- The **User Name** column shows the name of who changed the data.
- The **Date Time Stamp** shows the time of the change.

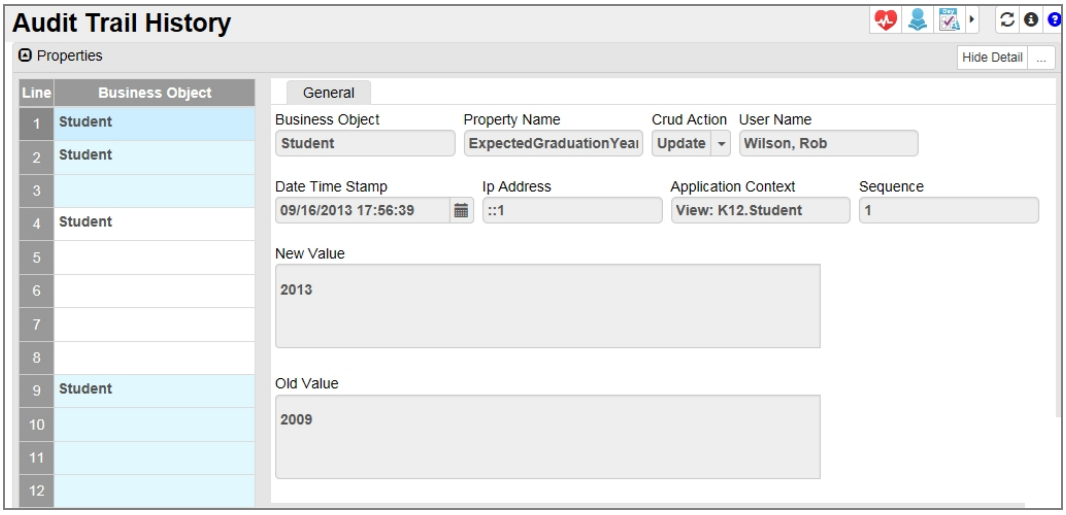


Line	Business Object	Property Name	Crud Action	New Value	Old Value	User Name	Date Time Stamp
1	Student	ExpectedGraduationYear	Update	2013	2009	Wilson, Rob	09/16/2013 17:56:39
2	Student	GraduationStatus	Update		0	Wilson, Rob	04/25/2013 12:38:26
3		GraduationDate	Update		20130607	Wilson, Rob	04/25/2013 12:38:26
4	Student	GridCode	Update	741B	741B	Wilson, Rob	02/19/2013 13:52:35
5		HomeCounty	Update			Wilson, Rob	02/19/2013 13:52:35
6		MailAddressGU	Update	<Link>	<Link>	Wilson, Rob	02/19/2013 13:52:35
7		HomeAddressGU	Update	<Link>	<Link>	Wilson, Rob	02/19/2013 13:52:35
8		DistrictOfResidenceAddr	Update			Wilson, Rob	02/19/2013 13:52:35
9	Student	DistrictOfResidenceAddr	Update			Wilson, Rob	02/19/2013 13:52:26
10		HomeAddressGU	Update	<Link>	<Link>	Wilson, Rob	02/19/2013 13:52:26

Audit Trail History Screen

- Click **Show Detail** to view additional information about each change.
- The **IP Address** field shows which computer made the change.
- The **Application Context** field shows the screen where the user made the change.

- The **Sequence** number indicates if the business object was the primary business object for the screen (*1*) or a business object linked to the primary business object (*2*).

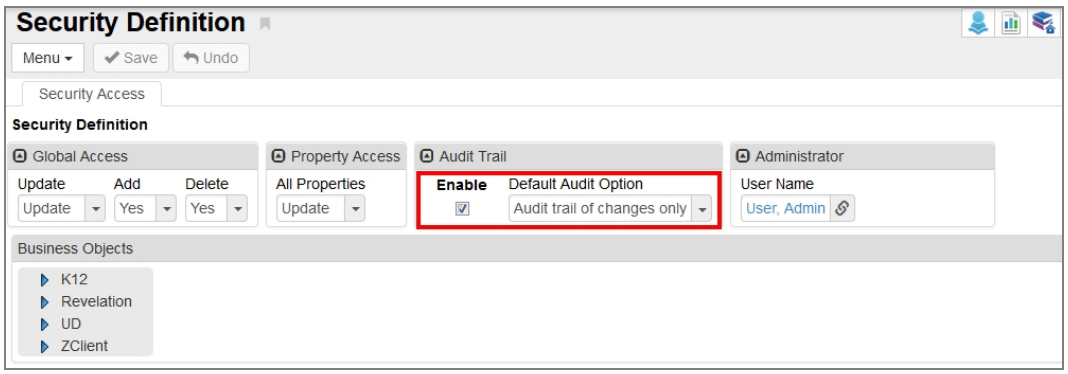


Audit Trail History Screen, Properties Detail

System-Wide Auditing

Synergy SIS has screen auditing disabled by default. Enable this through the Security Definition screen.

1. Navigate to **Synergy SIS > System > Security > Security Definition**.
2. Select **Enable** in the Audit Trail section.
3. Select the **Default Audit Option.**
    - *Full audit trail* – Logs all additions, updates, and deletions
    - *Audit trail of changes only* – Logs updates to existing data
    - *No audit trail* – Does not log changes. You can set still set auditing for individual business objects



Security Definition Screen

4. Click **Save**.

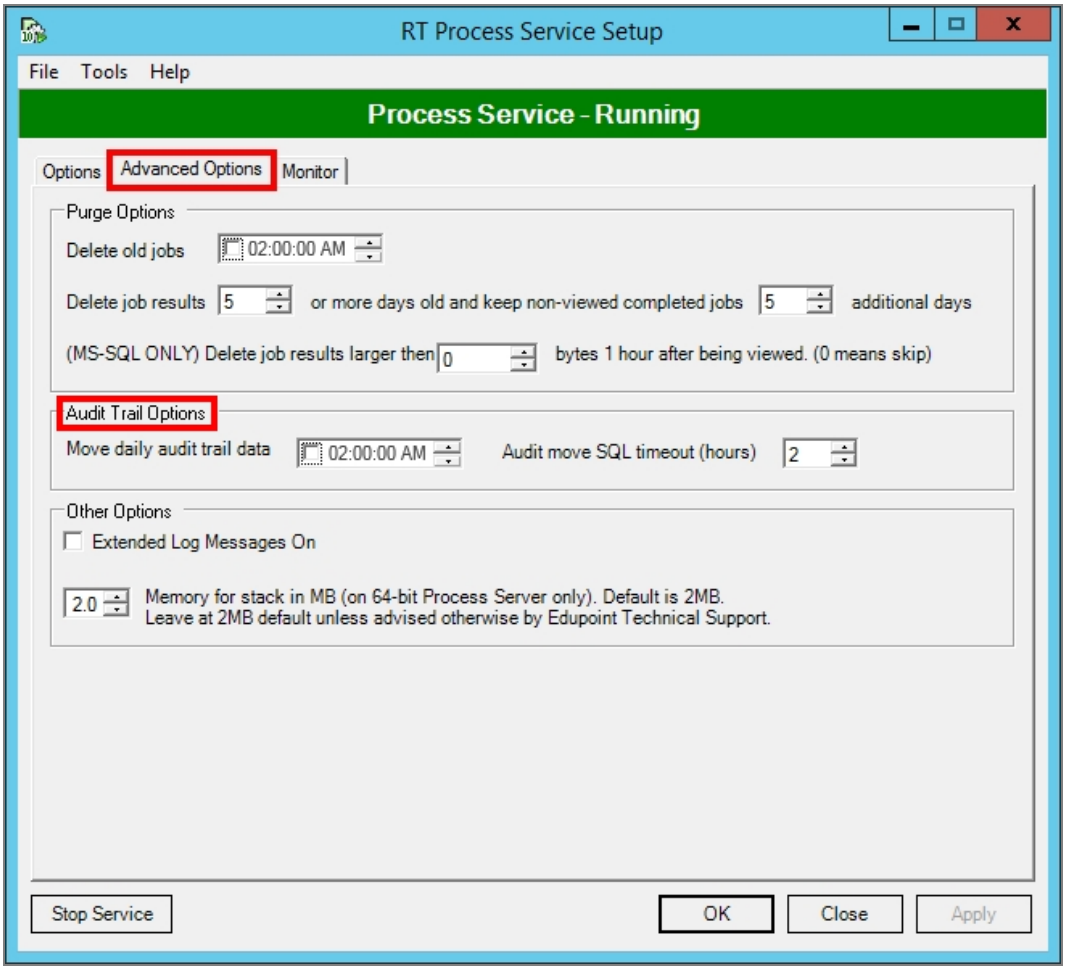
> Choosing *Full audit trail* can increase the size of the database dramatically and lead to decreased performance. Clear these tables annually to reduce database size by deleting all data in the **REV_AUDIT_TRAIL** and **REV_AUDIT_TRAIL_PROP** tables. Back up the data in these tables before deleting.

Improving Audit Trail Performance

The system stores audit trail data in current even and odd tables that maintain daily data. Move this data to historical tables using a nightly process to improve database performance.

> Configure only one process server to move audit trail records.

1. Open **RTProcessConfig.exe** from a process server.
2. Select the **Advanced Options** tab.
3. Enter the **Move daily audit trail data time** under Audit Trail Options.
4. Enter the **Audit move SQL timeout (hours)**, between 1-18 hours.



RT Process Service Setup Screen

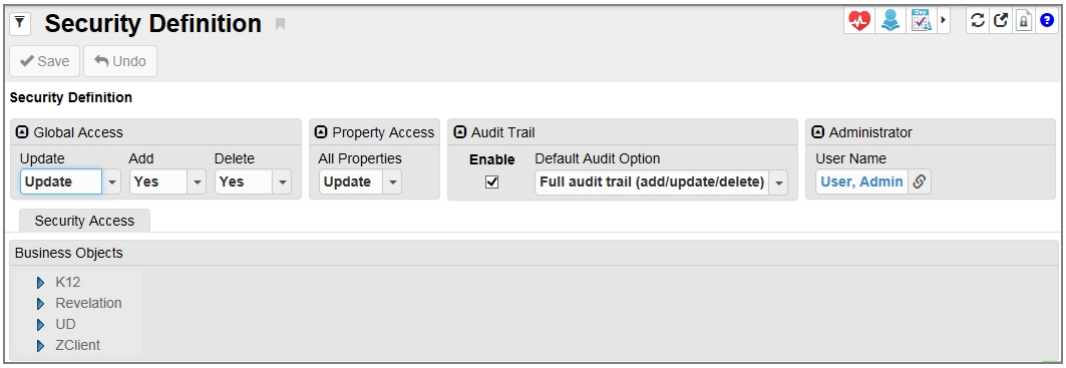
5. Click **Apply**.
6. Click **OK**.

Business Object Auditing

To reduce the size of the audit logs, disable or enable auditing for specific business objects.

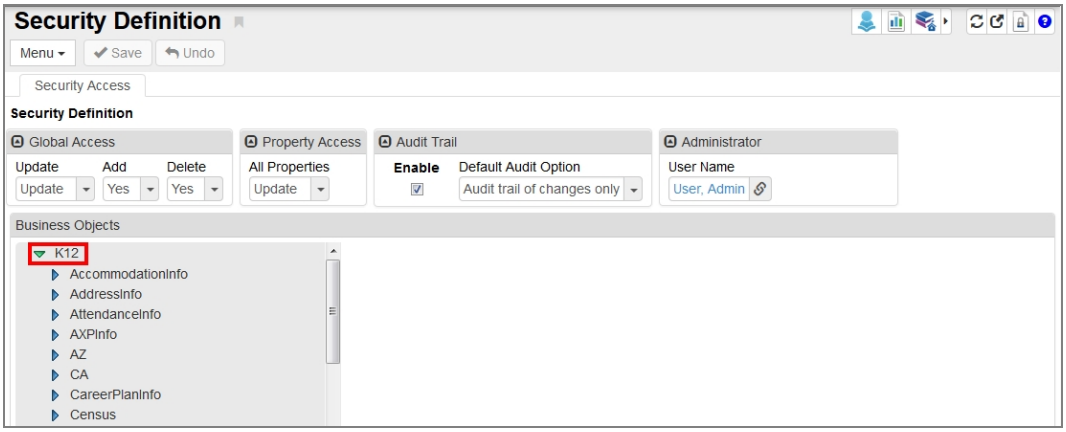
> See Business Object Group Auditing to configure auditing for a defined group of business objects.

1. Navigate to **Synergy SIS > System > Security > Security Definition**.



Security Definition Screen

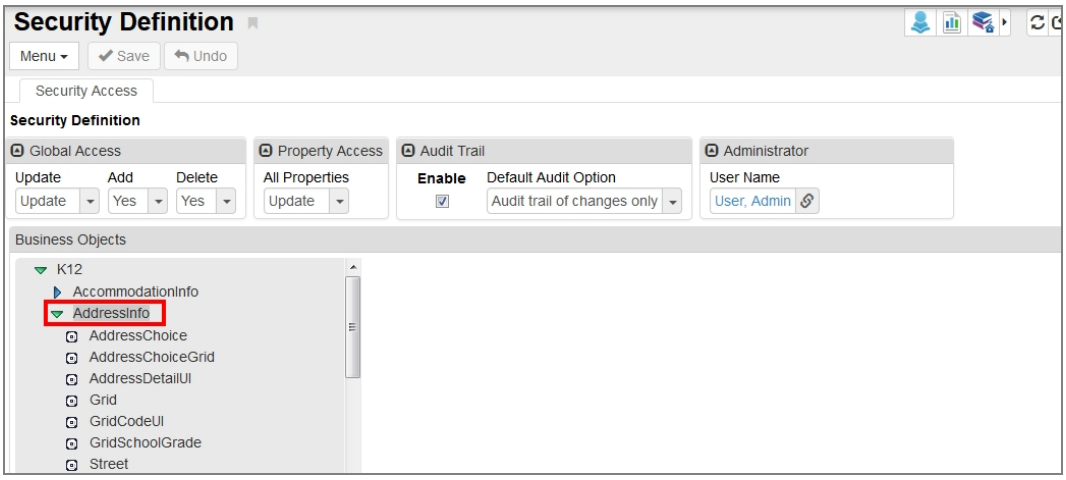
2. Select a primary namespace to expand it and list all secondary namespaces.
   - The **K12** namespace contains most Synergy business objects.
   - The **Revelation** namespace holds the system-wide business objects, including attributes such as phone numbers.
   - The **UD** namespace holds user-defined namespaces and only shows business objects for districts with customized screens .
   - The **ZClient** namespace lists customized business objects for specific districts.



Security Definition Screen

3. Select a secondary namespace to list the business objects.

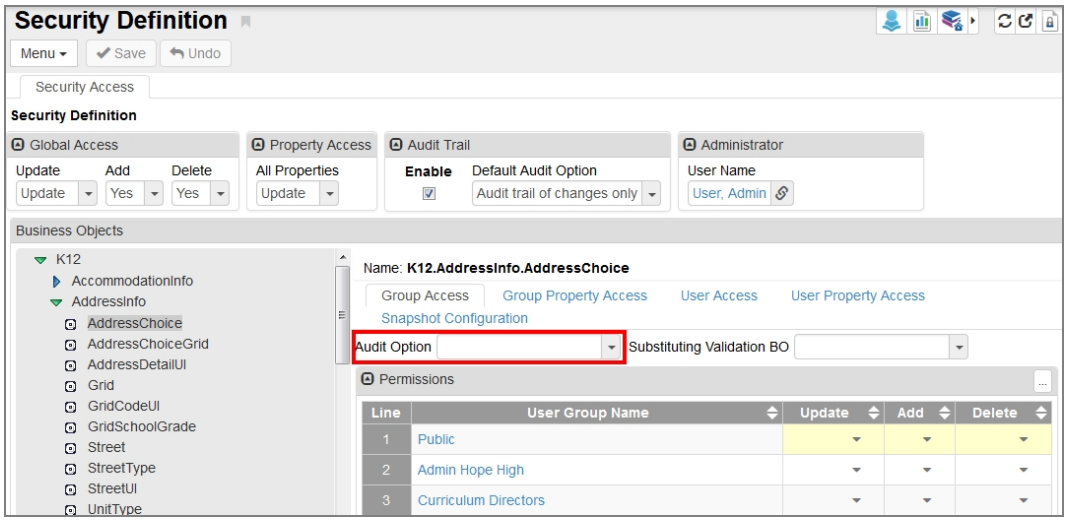
4. Select a business object to view detail.



Security Definition Screen

5. Select the **Audit Option**.

   - *Full audit trail* – Logs all additions, updates, and deletions
   - *Audit trail of changes only* – Logs updates to existing data
   - *No audit trail* – Does not log changes. You can set still set auditing for individual business objects.



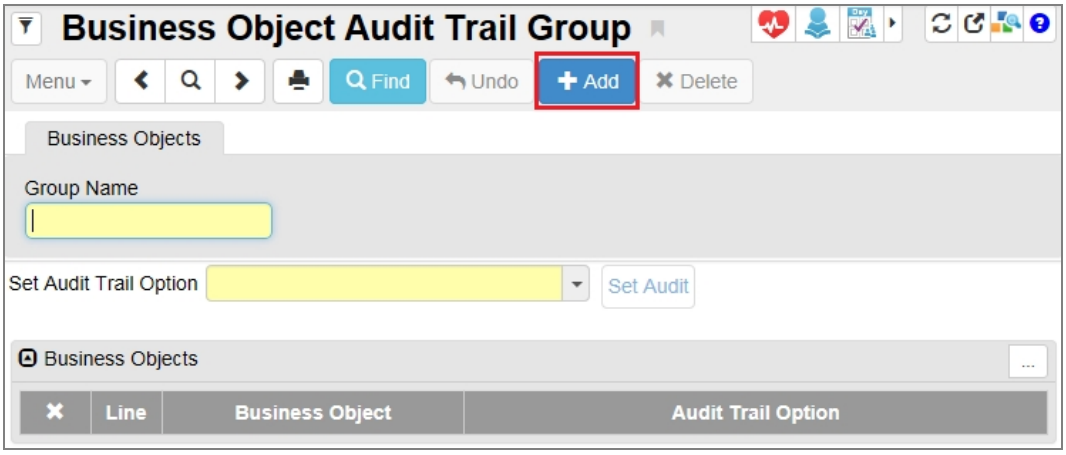
Security Definition Screen, Business Objects Detail

6. Click **Save**.

Business Object Group Auditing

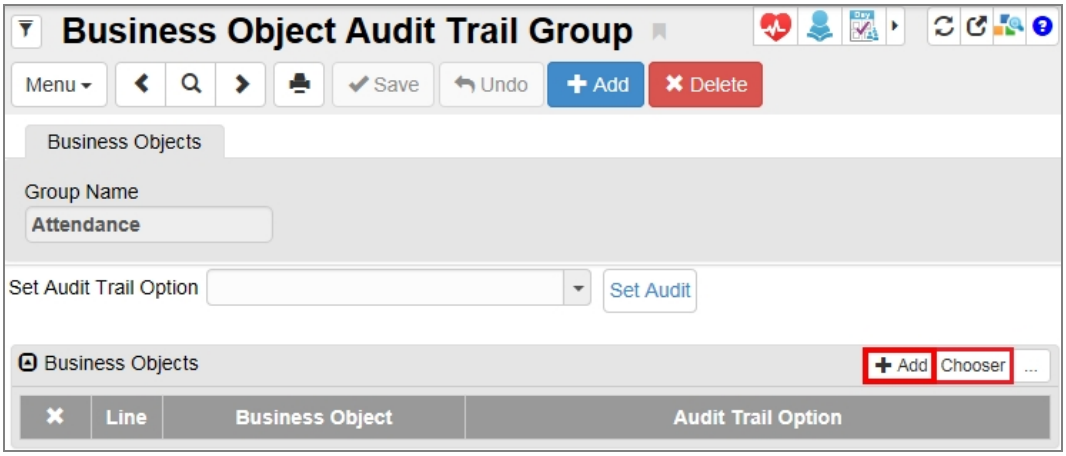
The Business Object Audit Trail Group screen enables you to group related business objects and update the audit trail properties for all of the objects at once.

1. Navigate to **Synergy SIS > System > Security > Business Object Audit Trail Group**.
2. Click **Add**. A new window opens.



Business Object Audit Trail Group Screen

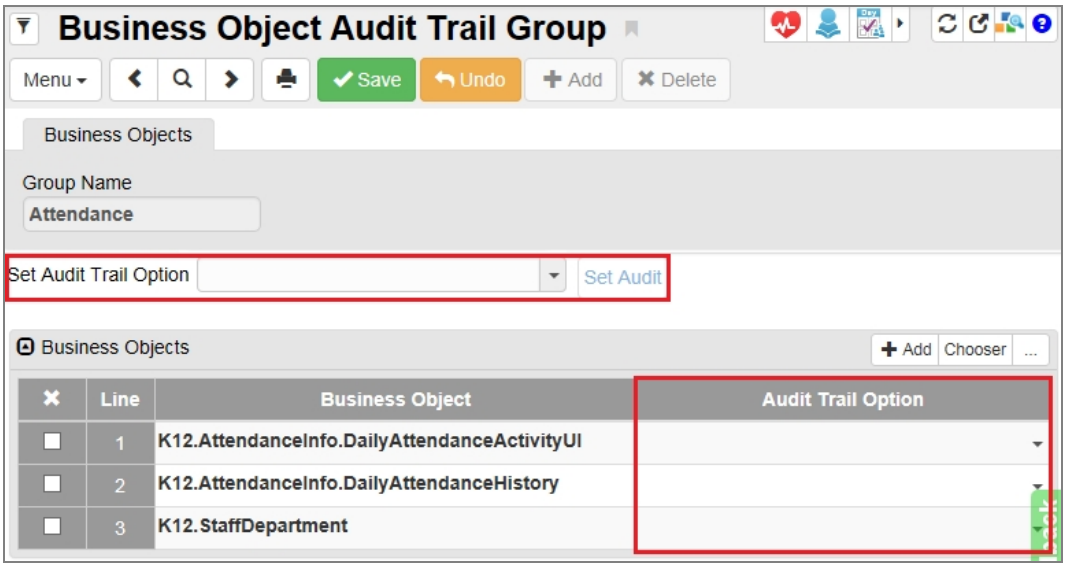
3. Enter the **Group Name** and click **Save**.
4. Click **Add** or **Chooser** to add items to the Business Objects section.



Business Object Audit Trail Group Screen

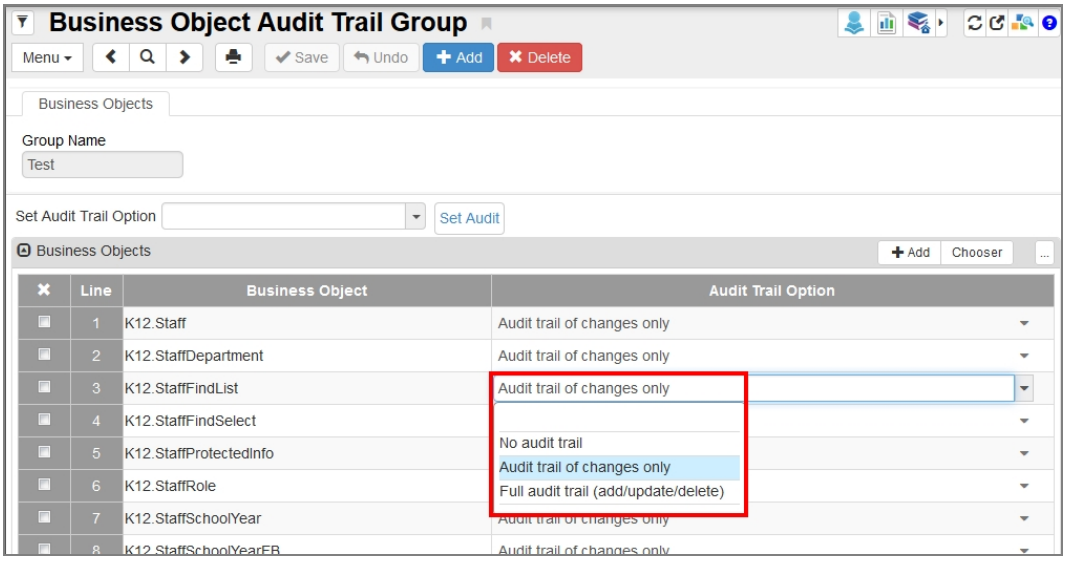
5. Click **Save**.
6. Select the **Set Audit Trail Option**.

7. Click **Set Audit**. All business objects update to this setting.



Business Object Audit Trail Group Screen

8. Select the **Audit Trail Option** column to change individual business objects.



Business Object Audit Trail Group Screen

9. Click **Save**.

Special Audit Queries

Some Synergy screens do not appear on the audit trail report, as the audit trail report shows changes for primary objects on the screen and not the objects inside a section. For example, the Schedule module, the Student Classes screen audit trail shows changes made to student information, but no changes to the Current Class Schedule section.

Synergy allows you to log changes through custom queries for screens that do not appear in the Audit Detail Report. Use the custom queries below on the Query screen, or create your own.

See the *Synergy SIS – Query and Reporting Guide* for more information about queries.

Enrollment Audit Trail

```
K12.Student R0, K12.EnrollmentInfo.StudentSchoolYear R1,
Revelation.OrganizationInfo.RevOrganizationYear R2
(OrganizationYearGU,R1.OrganizationYearGU,Inner),
Revelation.Security.AuditTrail R4 (IdentityGU,R1.StudentSchoolYearGU,Inner),
Revelation.OrganizationInfo.RevOrganization R3
(OrganizationGU,R2.OrganizationGU,Inner),
Revelation.Security.AuditTrailProperties R5, Revelation.UserInfo.RevUser R6
(UserID,R4.AddIDStamp,Inner)
COLS R0.SisNumber, R0.FormattedName, R3.OrganizationName, R4.AddDateTimeStamp,
R4.IpAddress, R4.CrudAction (,'Action'), R4.ApplicationContext (,'Screen
used'), R6.FormattedName, R5.PropertyName, R5.OldValue, R5.NewValue,
R4.AuditTrailGU (,,Hide)
If R5.PropertyName <> 'OrganizationYearGU' And ((R5.OldValue <>R5.NewValue) Or
(R5.OldValue = And R5.NewValue Not =) Or (R5.OldValue Not = And R5.NewValue
=))
Sort R0.FormattedName, R0.SisNumber, R3.OrganizationName, R4.AddDateTimeStamp,
R4.AuditTrailGU, R5.PropertyName
```

Class schedule audit trail showing deleted classes by student

```
K12.Student R0, K12.EnrollmentInfo.StudentSchoolYear R1,
Revelation.Security.AuditTrail R4
(ParentIdentityGU,R1.StudentSchoolYearGU,Inner),
Revelation.Security.AuditTrailProperties R5, Revelation.UserInfo.RevUser R6
(UserID,R4.AddIDStamp,Inner), K12.ScheduleInfo.Section R3
(SectionGU,R5.OldValue,Inner)
COLS R0.FormattedName, R3.SectionID, R4.AddDateTimeStamp, R4.IpAddress,
R4.CrudAction (,'Action'), R4.ApplicationContext (,'Screen used'),
R6.FormattedName
If R4.BOName ='StudentClass' And R4.CrudAction ='D' And R5.PropertyName
='SectionGU'
```

Class schedule audit trail showing deleted classes by section

```
K12.ScheduleInfo.Section R0, Revelation.Security.AuditTrail R4
(ParentIdentityGU,R0.SectionGU,Inner),
Revelation.Security.AuditTrailProperties R5, Revelation.UserInfo.RevUser R6
(UserID,R4.AddIDStamp,Inner), K12.EnrollmentInfo.StudentSchoolYear R2
(StudentSchoolYearGU,R5.OldValue,Inner), K12.Student R3
(StudentGU,R2.StudentGU,Inner)
COLS R0.SectionID, R3.FormattedName, R4.AddDateTimeStamp, R4.IpAddress,
R4.CrudAction (,'Action'), R4.ApplicationContext (,'Screen used'),
R6.FormattedName
If R4.BOName ='ClassStudent' And R4.CrudAction ='D' And R5.PropertyName
='StudentSchoolYearGU'
```

Custom reports built using SIREN software can also use MSSQL query language. The below query is a sample audit report using MSSQL query. For more information about SIREN reports, see the *SIREN Report Designers Guide*.

User group membership audit trail using MS SQL

```
select per.LAST_NAME+', '+per.FIRST_NAME "User",usr.LOGIN_NAME UserID,
   chgper.LAST_NAME+', '+chgper.FIRST_NAME ChangeUser,aud.ADD_DATE_TIME_STAMP
AuditDateTime,
   case aud.CRUD_ACTION when 'I' then 'Add' else 'Delete' end "Action",
   grp.USERGROUP_NAME UserGroupAddedDeleted
from REV_USER usr
inner join REV_PERSON per on (per.PERSON_GU = usr.USER_GU)
inner join REV_AUDIT_TRAIL aud on (aud.PARENT_IDENTITY_GU = usr.USER_GU)
inner join REV_PERSON chgper on (chgper.PERSON_GU = aud.ADD_ID_STAMP)
inner join REV_AUDIT_TRAIL_PROP prp on (prp.AUDIT_TRAIL_GU = aud.AUDIT_TRAIL_
GU)
inner join REV_USERGROUP grp on (prp.PROPERTY_NAME = 'UsergroupGU' and
grp.USERGROUP_GU =
case when aud.CRUD_ACTION = 'D' then convert(uniqueidentifier,prp.OLD_VALUE)
else convert(uniqueidentifier,prp.NEW_VALUE) end)
where aud.CRUD_ACTION in ('I','D')
order by per.LAST_NAME,per.FIRST_NAME,usr.LOGIN_NAME,aud.ADD_DATE_TIME_STAMP,
aud.ACTION_ID,aud.SEQUENCE,aud.AUDIT_TRAIL_GU
```

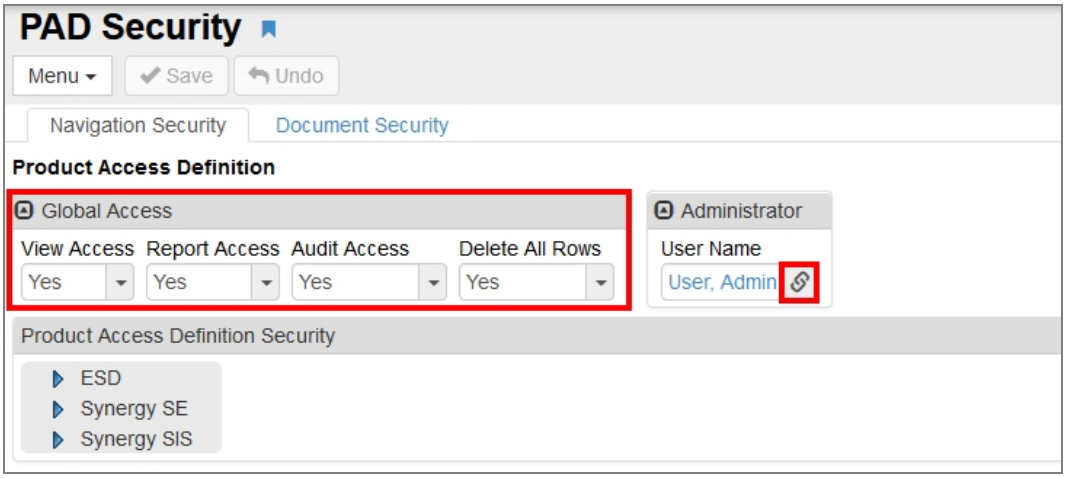
Chapter 3: Screen-Level Security

Setting Global Screen Rights

Set global screen rights and set a user as the main system administrator through the Pad Security screen.

> If forbidding access to all users, make certain the Admin user/user group has read/write access to everything. Otherwise, you can lock the admin user out of the system.

1. Navigate to **Synergy SIS > System > Security > PAD Security**.
2. Set the Global Access settings.
3. Select one of the following in the **View Access** field:
   - *Yes* – Gives everyone the ability to update data in all screens
   - *View Only* – Gives everyone the ability to see but not update the data in the screens
   - *No* – Denies everyone access
4. Select *Yes* for **Report Access** to grant everyone access to all reports in the system, or *No* to deny everyone access to all reports.
5. Select *Yes* for **Audit Access** to grant everyone access to the **Audit Detail Report** for each screen, or *No* to deny everyone access to the Audit Detail Reports.
6. Select *Yes* for **Delete All Rows** to grant everyone access to delete all the rows in a grid, or *No* to deny everyone access.



PAD Security Screen

7. Click the link icon next to **User Name** in the Administrator section to select a different administrator user. The Find: Rev User screen appears.

> This user is the same as the administrator set on the Security Definition screen. You can change this information on either screen.

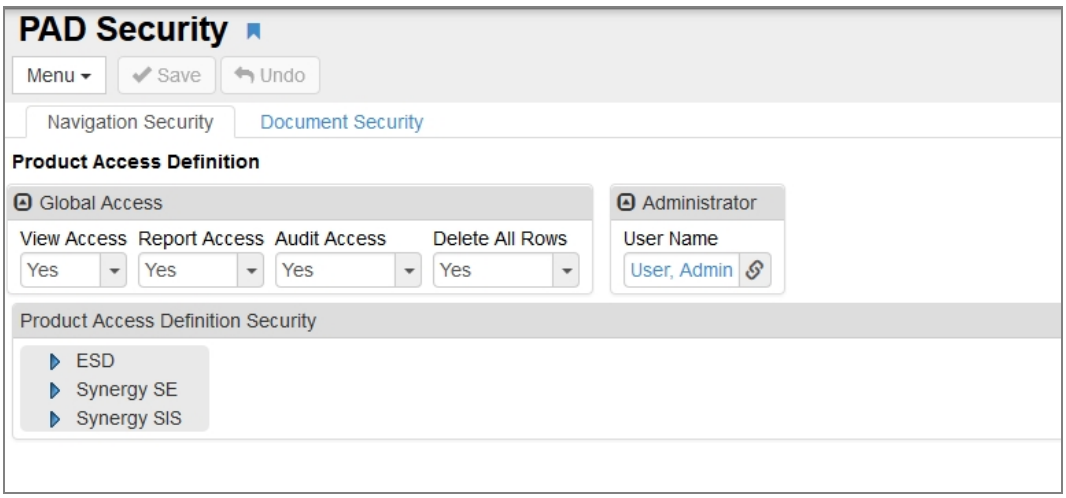
8. Find and select the user to add.
9. Click **Save**.

Setting User Group Access

After setting global access, customize access rights to user groups on the Pad Security screen at any level from the module, screen, or report. Synergy organizes screen security in layers. If you customize user group access to a module, the same access rights apply to all screens and reports in that module.

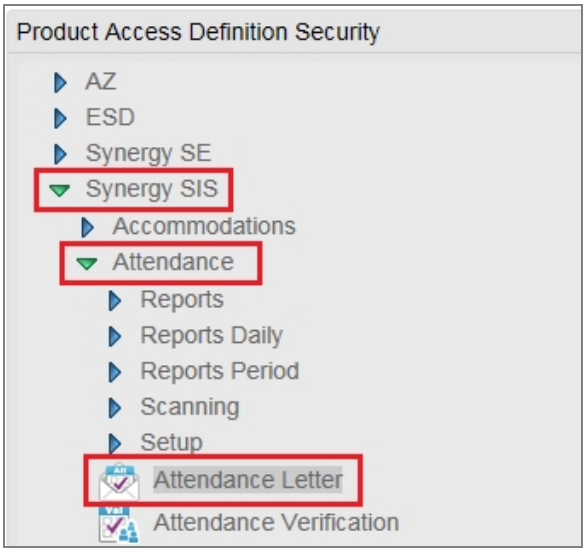
> For more information on creating user groups, see the *Synergy SIS – System Administrator Guide*.

1. Navigate to **Synergy SIS > System > Security > PAD Security**.



PAD Security Screen

2. Click a module to expand it and locate the screen or report to modify.

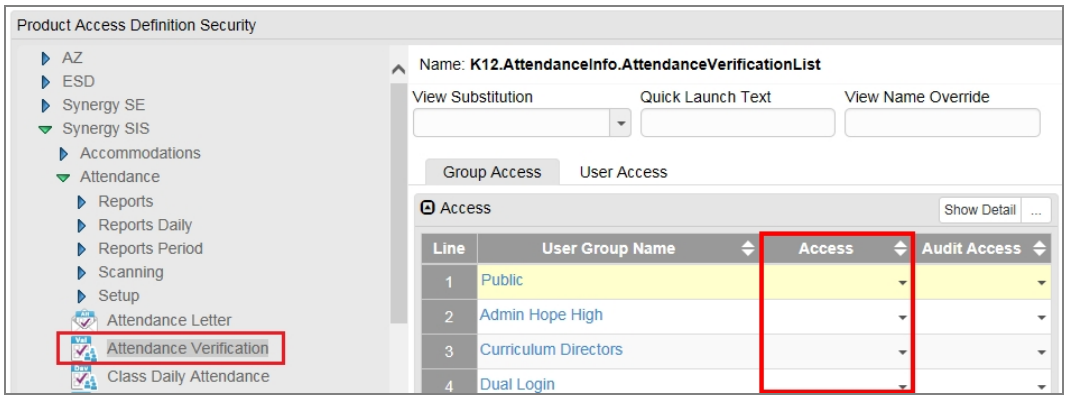


PAD Security Screen

3. Click the module name to view and set security detail.

4. Select the **Access** for each group.
    - *Yes* – Grants update rights
    - *View Only* – Grants read-only rights
    - *No* – Denies all access

> The **Public** group is the default access for all groups. If you set Public to *No* for any module or screen, you must set the admin user group or admin to *Yes* to ensure you do not lock everyone out of the module.

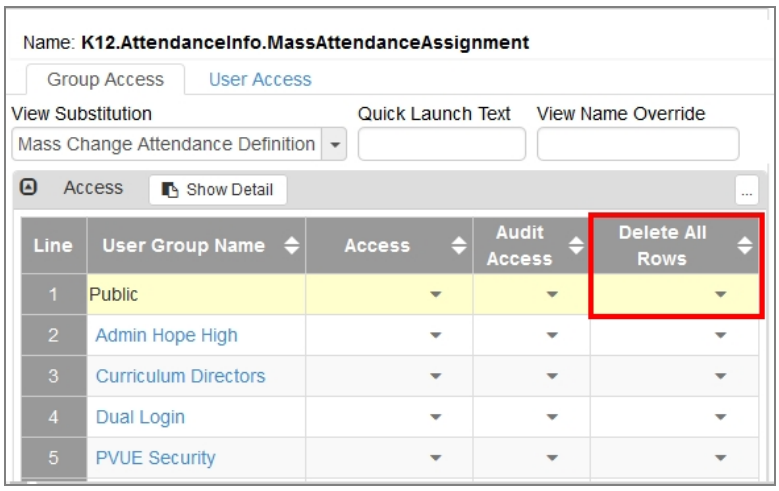


PAD Security Screen, PAD Security Details

5. To control access to the Audit Detail Report for the screen, select *Yes* or *No* for each group in the **Audit Access** field.

6. Click **Save**.

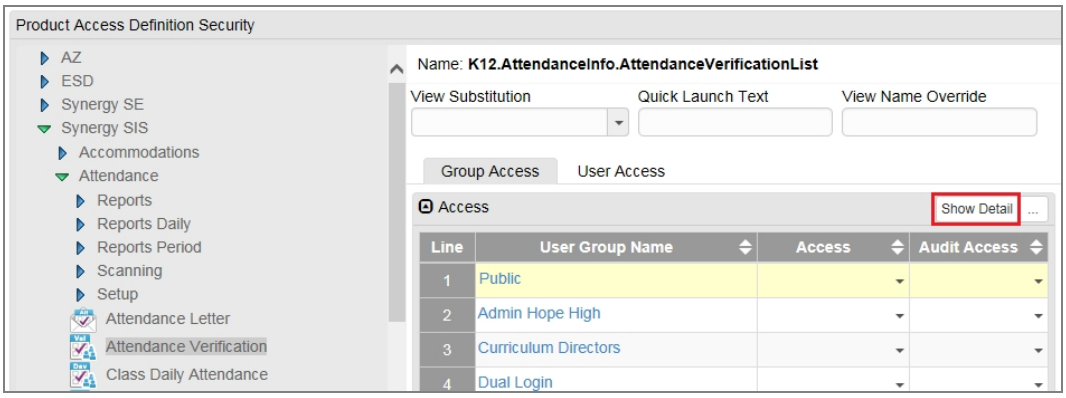
Screens that contain grids also display a column titled **Delete All Rows**. You can set the permission for specific user groups to delete all items in a grid.



PAD Security Screen

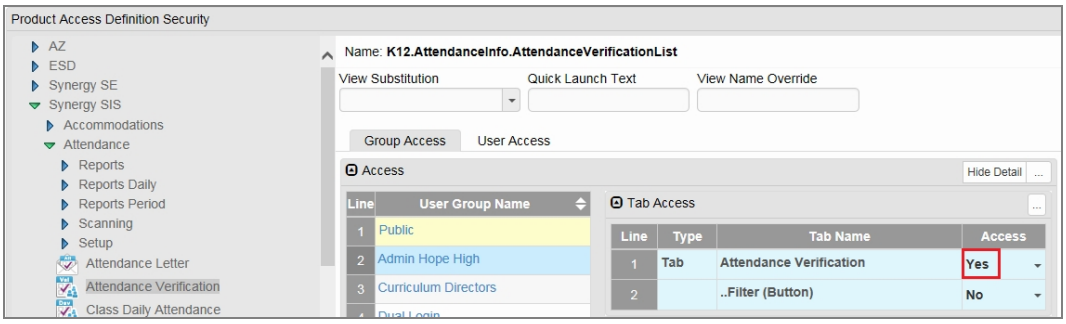
The **View Substitution**, **Quick Launch Text**, and **View Name** Override fields allow each district to customize the screen. For more information, see the *Synergy SIS – System Administrator Guide*.

7. Click **Show Detail** in the Access section to set user group access to specific screen items.



PAD Security Screen, PAD Security Details

8. Select the **Access** rights for the group for each item.



PAD Security Screen, PAD Security Details

9. Click **Save**.

The System module, Announcements property contains the **Home** screen and the **Announcement Tree** screen. If users cannot access these screens, they do not see the home page of Synergy SIS or any system announcements.

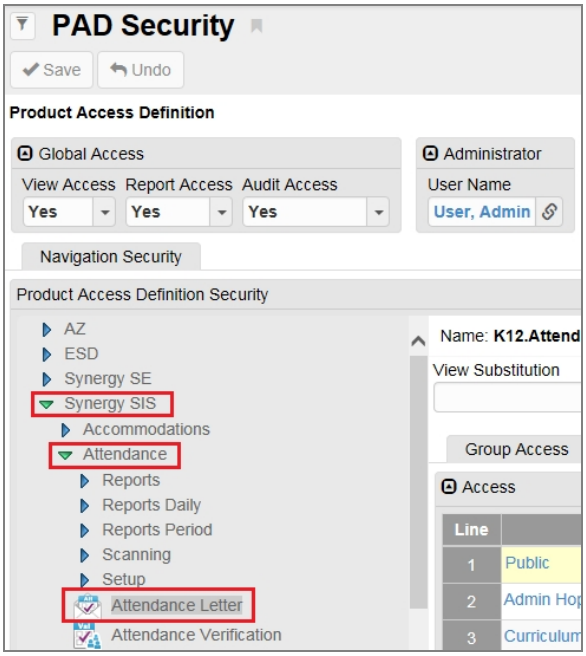
You should also be careful when securing the following items:

- System module, Job Queue screen, Job Queue Viewer property – Enables users to reprint reports
- Grade Book screen, GBSecurity property– Controls access to the buttons in Grade Book
- Non PAD – Controls several areas across the system

Setting User Access

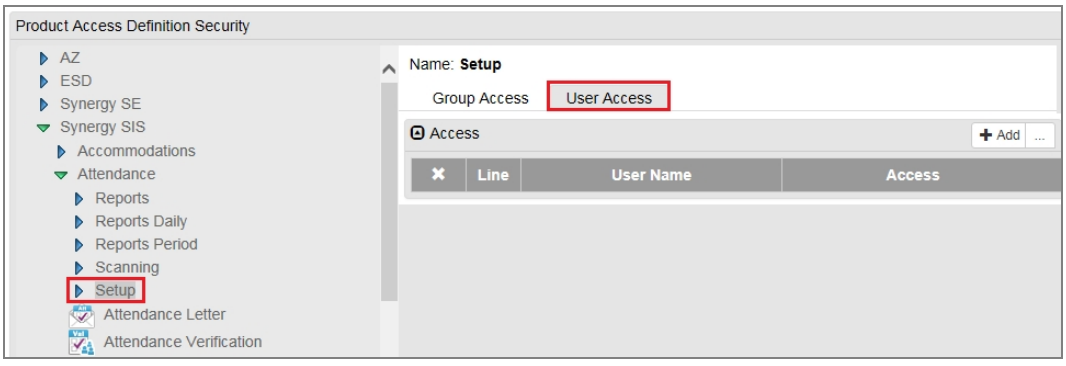
Customize screen access for specific users on the Pad Security screen. If you customize user access to a module, the same access rights apply to all screens and reports in that module.

1. Navigate to **Synergy SIS > System > Security > PAD Security**.
2. Click a module to expand it and locate the screen or report to modify.



PAD Security Screen

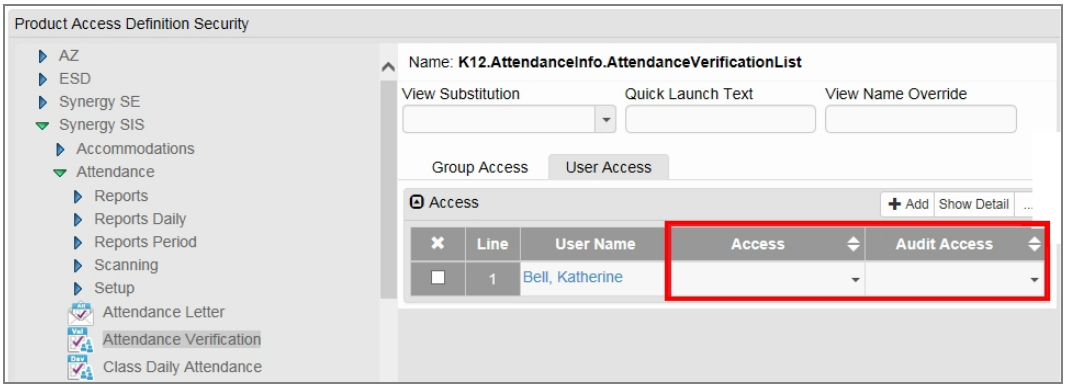
3. Select the module name to view and set security detail.
4. Select the **User Access** tab.



PAD Security Details, User Access Tab

5. Click **Add** to locate the user to modify.

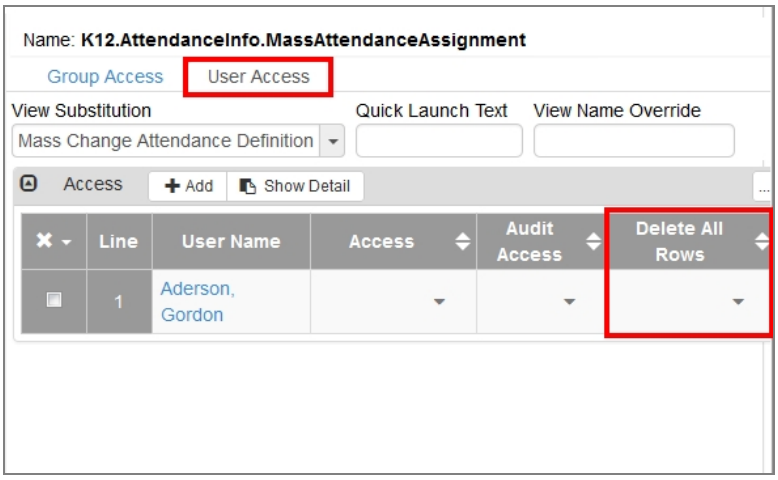
6. Select the **Access** for the module:
   - *Yes* – Grants update rights
   - *View Only* – Grants read-only rights
   - *No* – Denies all access
7. To control access to the Audit Detail Report for the screen, select *Yes* or *No* for each user in the **Audit Access** field.



PAD Security Details, User Access Tab

8. Click **Save**.

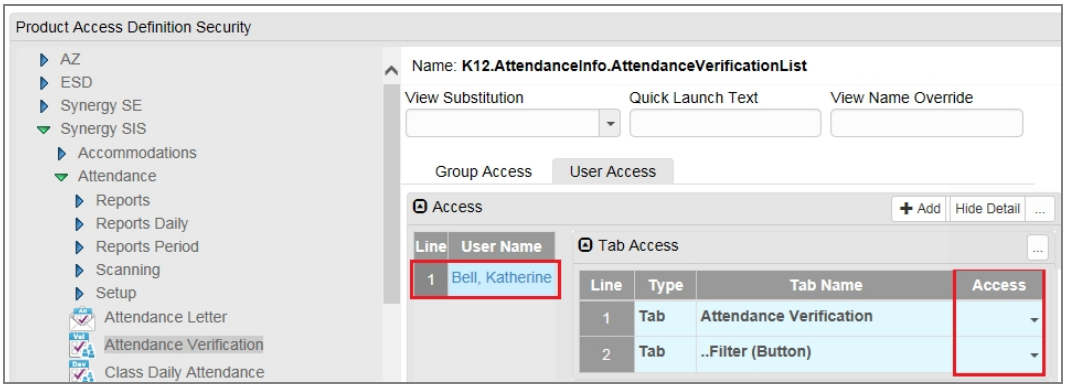
Screens that contain grids also display a column titled **Delete All Rows**. You can set the permission for individual users to delete all items in a grid.



PAD Security Screen

9. Click **Show Detail** in the **Access** section to set user access to specific screen items.

10. Select the **Access** rights for the group for each item.



PAD Security Details, User Access Tab

11. Click **Save**.

Setting Screen-Level Security in Admin Configuration

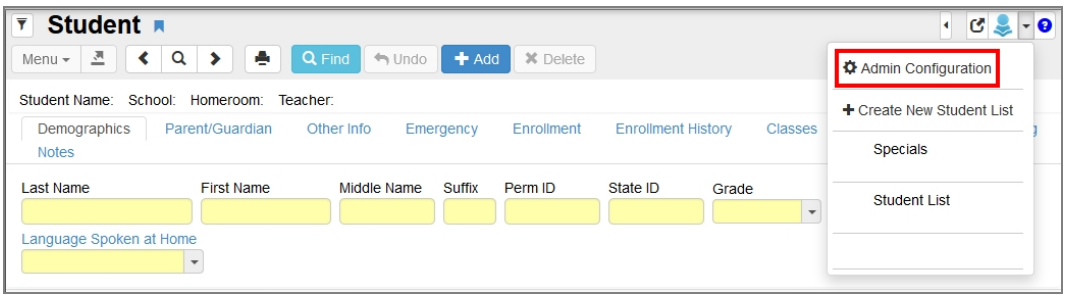
Admin Configuration allows you to configure screen security for multiple users or user groups. These changes only affect the screen currently in view.

> To access Admin Configuration, you must have *Update* permissions to the Security Definition and Property Override screens.
>
> You cannot access Admin Configuration through a pop-in window (Ex. Student Add Screen) or any report interface.

The following example uses the Student screen.

1. Navigate to **Synergy SIS > Student > Student**.
2. Click the arrow in top right corner.
3. Select **Admin Configuration**. The Admin Configuration screen appears.

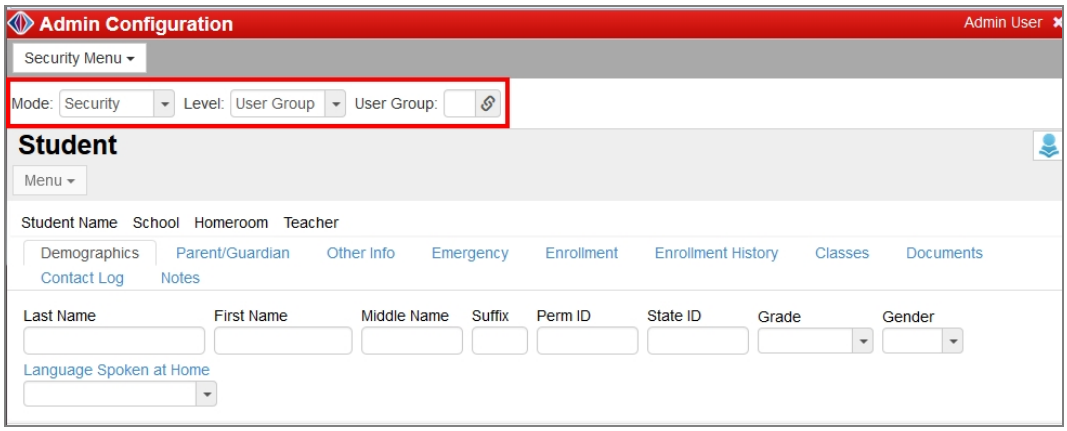
> The default **Mode** is *View / Property Override*. For more information on this mode, see the *Synergy SIS – System Administrator Guide*.



Student Screen

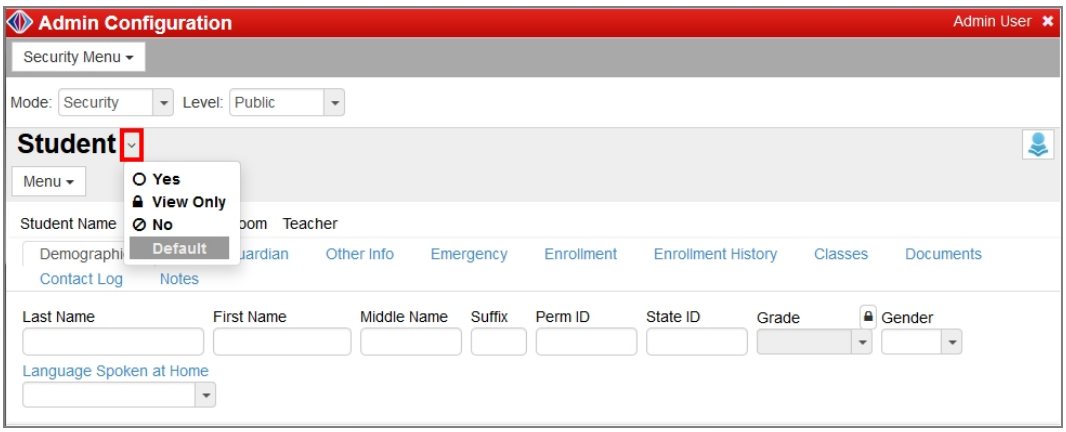
4. Select *Security* for the **Mode**.

5. Select the **Level**:
    - *Public* – Sets screen access for all users
    - *User Group* – Sets screen access for a specific user group. The **User Group** search field appears once selected.
    - *User* – Sets screen access for a specific user. The **User** search field appears once selected.



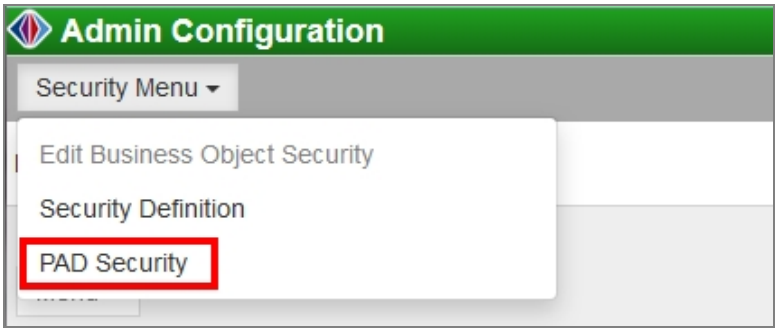
Admin Configuration Screen

6. Click the arrow next to the Student title.
7. Select the security option:
    - *Yes* – Gives everyone the ability to update data in all screens
    - *View Only* – Gives everyone read-only access to the data in the screens
    - *No* – Denies everyone access
    - *Default* – Follows Global Security settings



An icon displays next to the screen name to indicate the security change. You may need to refresh the original Synergy SIS screen after modifying values in Admin Configuration to view updates.

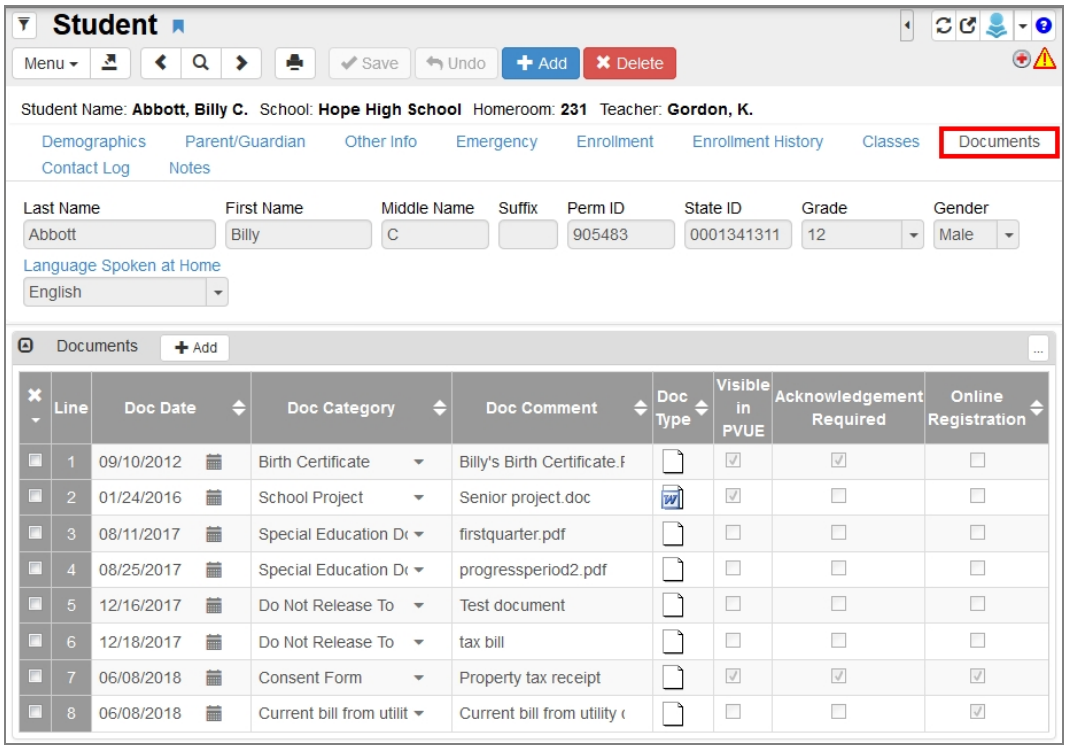
You can also select *PAD Security* from the **Security Menu** to open the PAD Security screen in a new window.



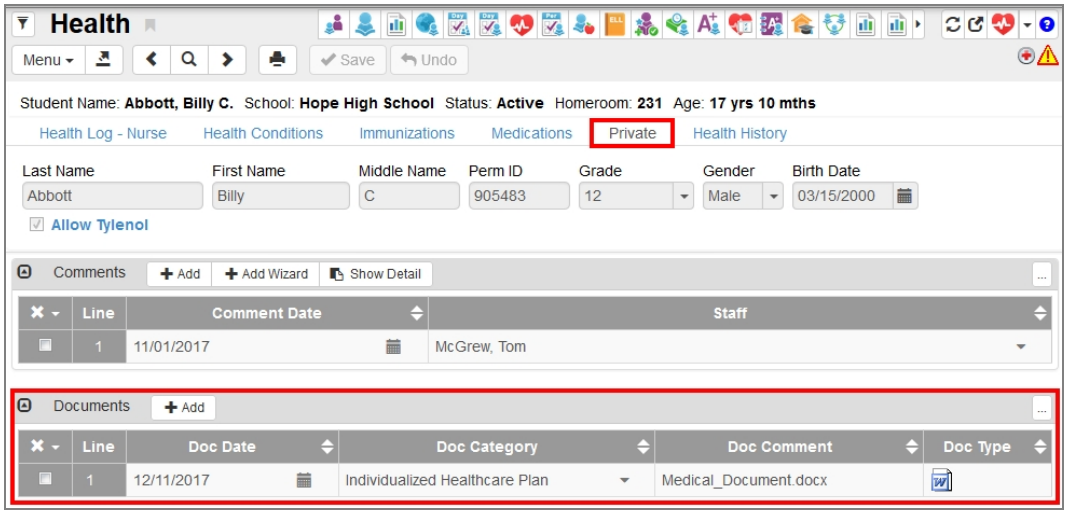
Admin Configuration Screen

Setting Document Security

You can apply security to the document categories based on the screen access that users have using the **Document Security** tab in PAD Security. This security sets the access to documents on the **Documents** tab of the **Synergy SIS > Student > Student** screen and the **Private** tab of the **Synergy SIS > Health > Health** screen.

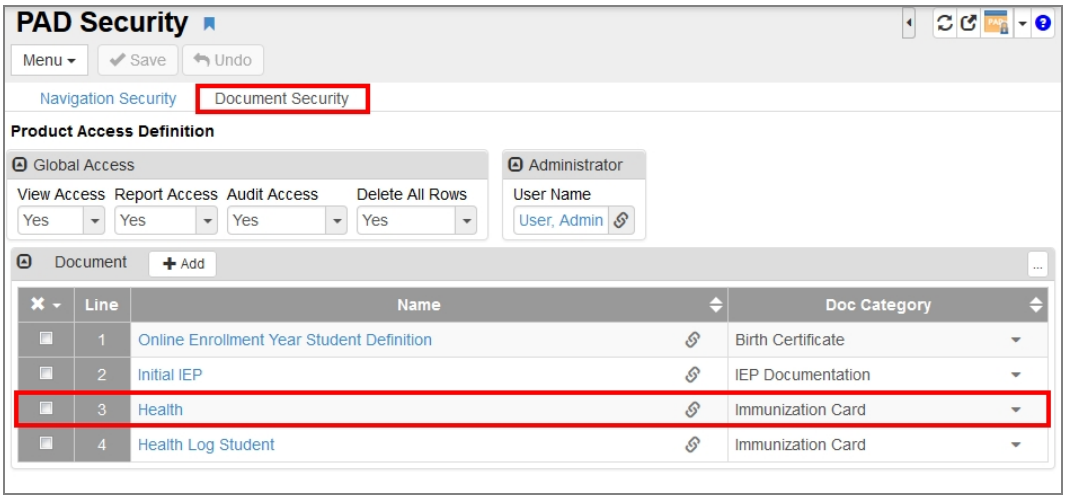


Student Screen, Documents Tab



Health Screen, Private Tab

1. Navigate to **Synergy SIS > System > Security > PAD Security**.
2. Select the **Document Security** tab.
3. Click **Add**. A new row appears.
4. Click the **Name** field to find and select a screen to apply security rights for.
5. Select the **Doc Category** those users have access to. The following example allows users with *View* or *Update* access to the Health screen to see documents with a **Doc Category** of *Immunization Card*.



PAD Security Screen, Document Security Tab

6. Repeat the steps to include additional Doc Categories.

> If a **Doc Category** is not listed in the Document section, all users can assign and view documents of that category.

7. Click **Save**.

Chapter 4: Field-Level Security

Business Objects Overview

Field-level security defines whether users can view and update business objects and the properties, or fields, of business objects. The following list contains a basic overview of business objects to secure.

Namespace	BO	Note
K12		
K12	School	
K12	Staff	
K12	StaffSchoolYear	
K12	Student	
K12	StudentPhoneNumber	
K12.AttendanceInfo		
K12.AttendanceInfo	StudentAttendancePeriod	Mirror to Period AttendanceGRID
K12.AttendanceInfo	PeriodAttendanceGRID	
K12.AttendanceInfo	StudentDailyAttendance	Mirror to Student AttendanceDetailUI
K12.AttendanceInfo	StudentAttendanceDetailUI	
K12.AttendanceInfo	StudentAttendancePeriod	Audit Needed for ATD415 to work
K12.AttendanceInfo	StudentDailyAttendance	Audit Needed for ATD415 to work
K12.ConferenceInfo		
K12.ConferenceInfo	StudentConference	
K12.CourseHistoryInfo		
K12.CourseHistoryInfo	StudentCourseHistory	
K12.CourseHistoryInfo	SchoolAttendedHistory	
K12.CourseInfo		
K12.CourseInfo	Course	
K12.CourseInfo	CourseMN	
K12.CourseInfo	CourseCoReq	
K12.CourseInfo	CoursePreReq	
K12.CourseInfo	CourseOverride	
K12.CourseInfo	CoursePreReqGroup	
K12.CourseInfo	CourseAltCode	
K12.CourseInfo	CourseAltFunding	
K12.CourseInfo	CourseLevel	

Namespace	BO	Note
K12.CourseInfo	CourseTechnicalCourse	
K12.CourseInfo	SchoolCourse	
K12.CourseInfo	CourseSchool	
K12.DisciplineInfo		
K12.DisciplineInfo	SchoolIncident	
K12.DisciplineInfo	StudentIncidentDiscipline	
K12.DisciplineInfo	StudentIncidentDisposition	
K12.EmergencyInfo		
K12.EmergencyInfo	Emergency	
K12.EnrollmentInfo **NOTE: The following BOs should use the same settings for all User Groups**		
K12.EnrollmentInfo	StudentEnrollment	
K12.EnrollmentInfo	StudentEnrollmentActivity	
K12.EnrollmentInfo	StudentSchoolYear	
K12.EnrollmentInfo	StudentSOREnrollment	
K12.GradeInfo		
K12.GradeInfo	StudentSchoolYearGrade	
K12.GradeInfo	StudentSchoolYearGradePeriod	
K12.GradeInfo	StudentSchoolYearGradePeriodComment	
K12.GradeInfo	StudentSchoolYearGradePeriodMark	
K12.HealthInfo		
K12.HealthInfo	HealthAudio	
K12.HealthInfo	HealthClinicalCodes	
K12.HealthInfo	HealthConditions	
K12.HealthInfo	HealthIncident	
K12.HealthInfo	HealthScreenActivity	
K12.HealthInfo	HealthScreenAudio	
K12.HealthInfo	HealthScreenCurrent	
K12.HealthInfo	HealthScreenDental	
K12.HealthInfo	HealthScreenGen	
K12.HealthInfo	HealthScreenTB	
K12.HealthInfo	HealthScreenVision	
K12.HealthInfo	HealthYearAudio	
K12.HealthInfo	HeathScreenScol	

Namespace	BO	Note
K12.HealthInfo	OtherClinicalCodes	
K12.HealthInfo	StudentClinicalCodes	
K12.HealthInfo	StudentImmunization	
K12.HealthInfo	StudentMedication	
K12.HealthInfo	StudentVaccination	
K12.ParentGuardianInfo		
K12.ParentGuardianInfo	Parent	
K12.ParentGuardianInfo	ParentStudent	
K12.ParentGuardianInfo	StudentParent	
K12.ProgramInfo		
K12.ProgramInfo	ChildProgParticipation	
K12.ProgramInfo	ELL	
K12.ProgramInfo	ELLAssessment	
K12.ProgramInfo	ELLAssessmentTest	
K12.ProgramInfo	ELLComment	
K12.ProgramInfo	ELLHistory	
K12.ProgramInfo	ELLWaiver	
K12.ProgramInfo	SpecialEdStudentNeeds	
K12.ProgramInfo	StudentFRM	
K12.ProgramInfo	StudentGATE	
K12.ProgramInfo	StudentNeedsPrograms	
K12.ProgramInfo	StudentNeedsProgramsGRID	Use PAD Security to turn off Add Student Need button
K12.ScheduleInfo		
K12.ScheduleInfo	ClassStudent	
K12.ScheduleInfo	Section	
K12.ScheduleInfo	StudentClass	
K12.ScheduleInfo	StudentClassGrid	Set Delete to No to prevent deleting classes
K12.ScheduleInfo. MassScheduleInfo		
K12.ScheduleInfo. MassScheduleInfo	SchedSection	
K12.ScheduleInfo. MassScheduleInfo	StudentScheduleRequest	

Namespace	BO	Note
K12.Setup		
K12.Setup	SchoolNonDistrict	Limits who can add non-district schools
K12.TestInfo		
K12.TestInfo	StudentTest	
K12.TestInfo	StudentTestObjective	
K12.TestInfo	StudentTestPart	
K12.TestInfo	StudentTestPartScore	
K12.TestInfo	StudentTestWaiver	
K12.PXP		
K12.PXP	ParentExperience	
K12.PXP	StudentExperience	
Revelation.OrganizationInfo		
Revelation.OrganizationInfo	RevOrganization	
Revelation.OrganizationInfo	RevYearOrganization	
Revelation **NOTE: The following BOs should have Auditing enabled**		
Revelation	RevAddress	
Revelation	RevPerson	
Revelation	RevPersonPhone	Always secure
Revelation	RevPersonSecondaryEthnic	Always secure
Revelation	Query.RevQuery	Set Editable Results to None for Public access
K12.SpecialEd		
K12.SpecialEd	Student	
K12.SpecialEd.IEP	IEPInfo	
K12.SpecialEd.Document	StudentDocument	
K12.SpecialEd.Document	DocumentGridProcess	
K12.SpecialEd.Document	DocumentGridHistory	
K12.SpecialEd.AZ	ProcessDocsUI	

Setting Global Field Rights

The Security Definition screen defines if users can view or modify data within a screen. This also includes the ability to add and delete records. Set these rights at the business object level instead of the screen level. While each screen can contain more than one business object, multiple screens can use the same business object. For example, if you customize the update rights for the Student business object, this impacts every screen that uses student information.

The Security chapter of the Synergy SIS Administrator Guide for each module discusses which business objects control each part of a screen. For example, the *Synergy SIS – Student Management Administrator Guide* describes the business objects that control the Student screen.

In addition, you define rights at the properties level. The properties of each business object are generally the fields shown on the screen, such as the **City** field on the Student screen. Many business objects contain hidden properties that link data but are not visible.

Set global field rights and set a user as the main system administrator through the Security Definition screen.

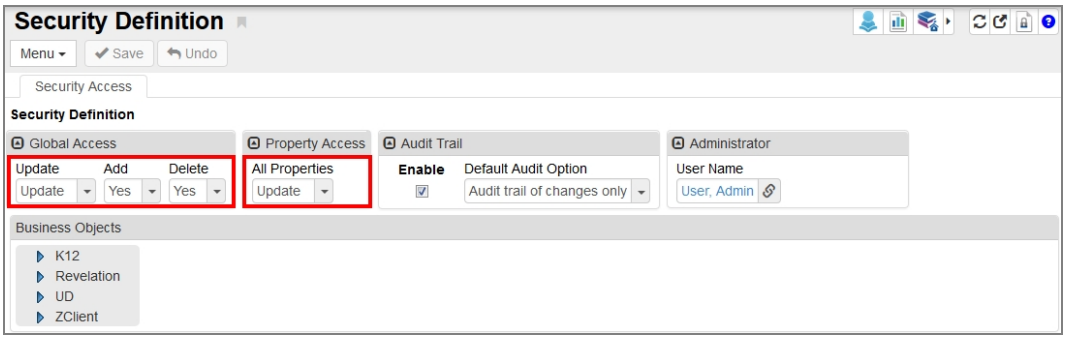
If forbidding access to all users, make certain the Admin user/user group has read/write access to everything. Otherwise, you can lock the admin user out of the system.

1. Navigate to **Synergy SIS > System > Security > Security Definition**.
2. Select one of the following in the **Update** field:
   - *Update* – Gives everyone the ability to update data in all screens.
   - *View* – Gives everyone read-only access to the data
   - *None* – Denies everyone access

Edupoint recommends using *None* only when setting individual business object rights and not for Global Access.

3. Select the **Add** value: *Yes* or *No*.
4. Select the **Delete** value for the business object: *Yes* or *No*.

5. Select the **Property Access** option for **All Properties**.

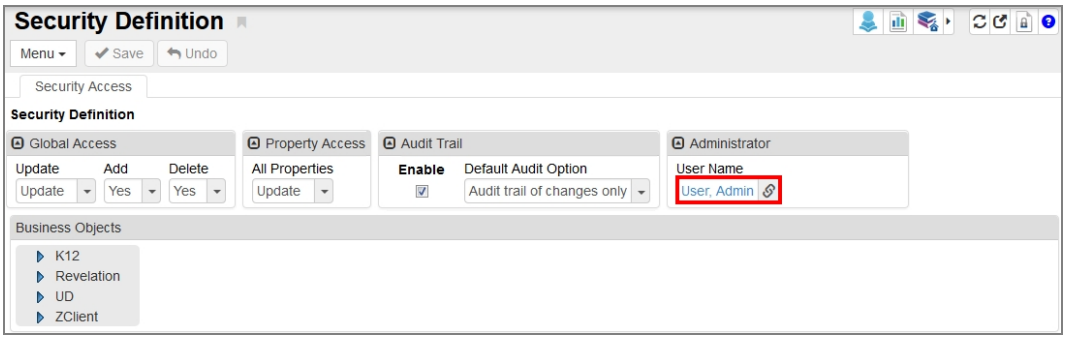


Security Definition Screen

6. Click the link icon next to **User Name** in the Administrator section to select a different administrator user. The Find: Rev User screen appears.

> This user is the same as the administrator set on the PAD Security screen. You can change this information on either screen.

7. Find and select the user to add.



Security Definition Screen

8. Click **Save**.

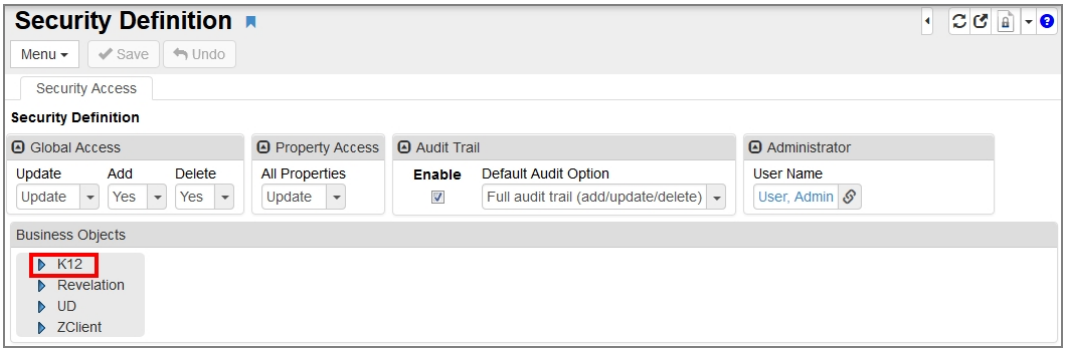
Customizing User Group Rights

After setting up global field rights, you customize security by assigning rights to user groups for specific business objects. Setting user group security is more efficient than setting individual user rights, and you set exceptions for certain users within a group.

Define the rights for both the overall business objects and for each individual property of the business object.

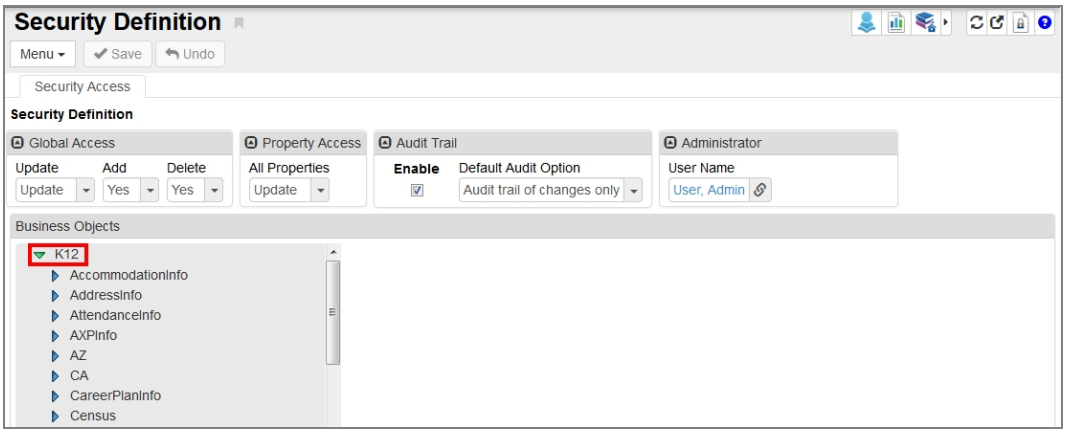
> These rights work in conjunction with the rights assigned in PAD Security for the screen. If you set the screen in PAD Security to *View Only* for a user group or user, the update rights in Security Definition do not override this setting to change a field. However, if you set the screen in PAD Security to *Update*, the rights in Security Definition can override this to set the properties or business objects to *View Only*. Therefore, to give rights to a group to update only a specific property, first give the group update access to the screen, then set all properties except that one to *View Only*.

1. Navigate to **Synergy SIS > System > Security > Security Definition**.



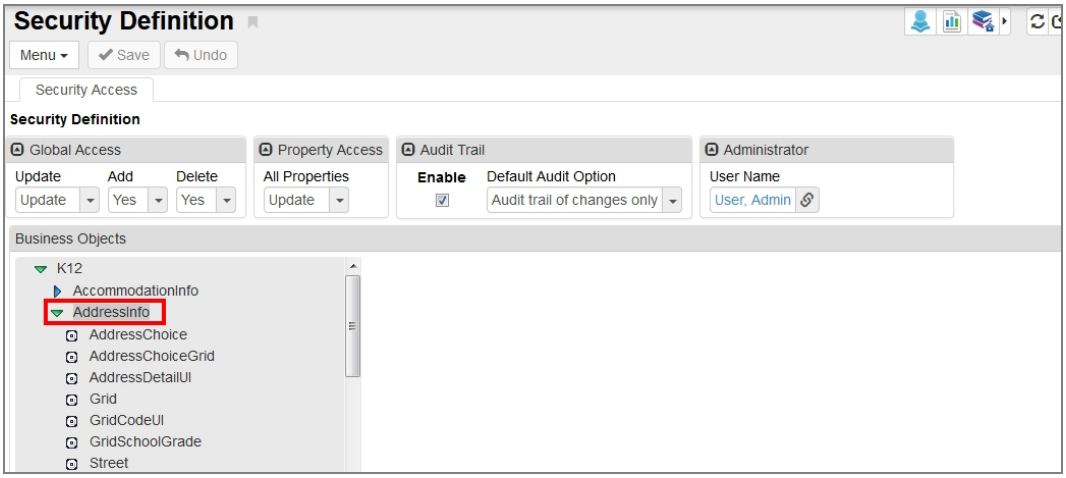
Security Definition Screen

2. Select a primary namespace to expand it and list all secondary namespaces.
   - The **K12** namespace contains most Synergy business objects.
   - The **Revelation** namespace holds the system-wide business objects, including attributes such as phone numbers.
   - The **UD** namespace holds user-defined namespaces and only shows business objects for districts with customized screens .
   - The **ZClient** namespace lists customized business objects for specific districts.



Security Definition Screen

3. Select a secondary namespace to list the business objects.



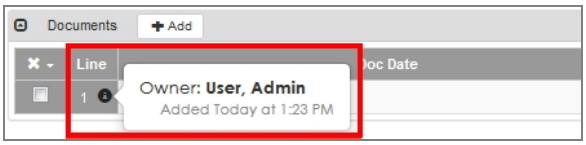
Security Definition Screen

4. Select a business object to view detail.

> For information about **Substituting Validation BO** and customizing the Synergy SIS interface, see the *Synergy SIS – System Administrator Guide*.

5. Select one of the following in the **Update** field:
   - *None* – Denies the user group access to the object
   - *Update* – Grants the user group the ability to update or delete records
   - *Update My Records Only* – Users can only update or delete records they originally entered. All other records are read-only.

     - Grids not tied to a direct business object (also called Unbound Grids) do not obey this security method. For example, you cannot secure user records on the Immunization Dosage Data grid on the **Immunization** tab of the **Synergy SIS > Health > Health** screen.
     - When enabled on a grid business object, an icon displays when hovering over a record that the user did not create. This icon displays the name of the user that created the record and when the record was added.

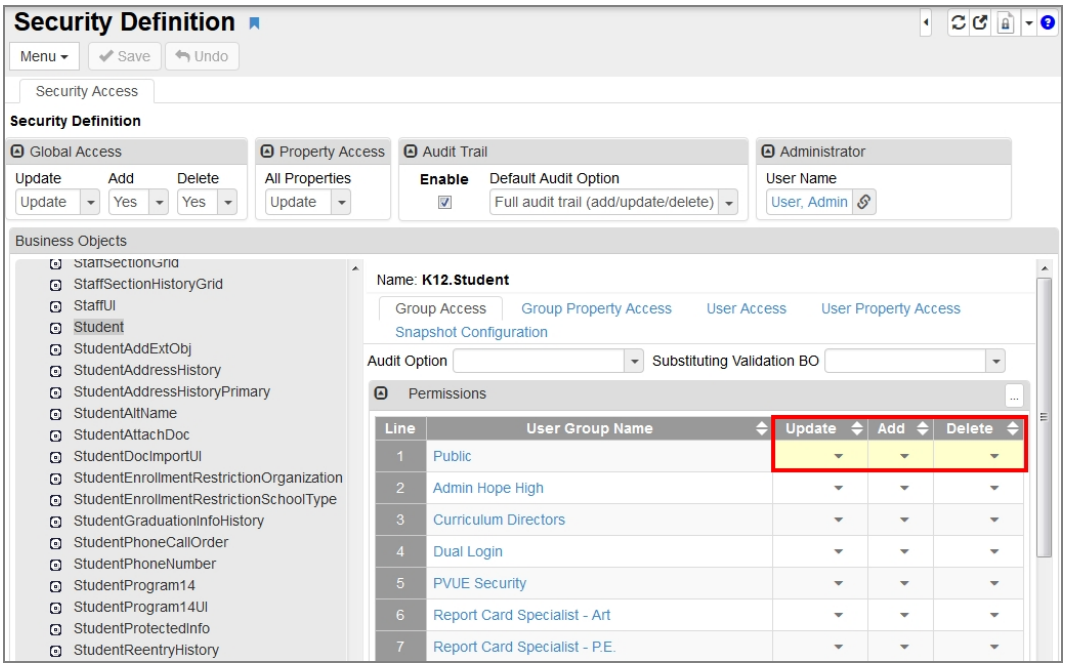
     

     Update My Records Only Option

   - *View* – Gives the user group read-only access to the object
6. Select *Yes* in the **Add** field to allow the user group to add records, or *No* to prevent users from adding records.
7. Select *Yes* in the **Delete** field to allow the user group to delete records, or *No* to prevent users from deleting records.

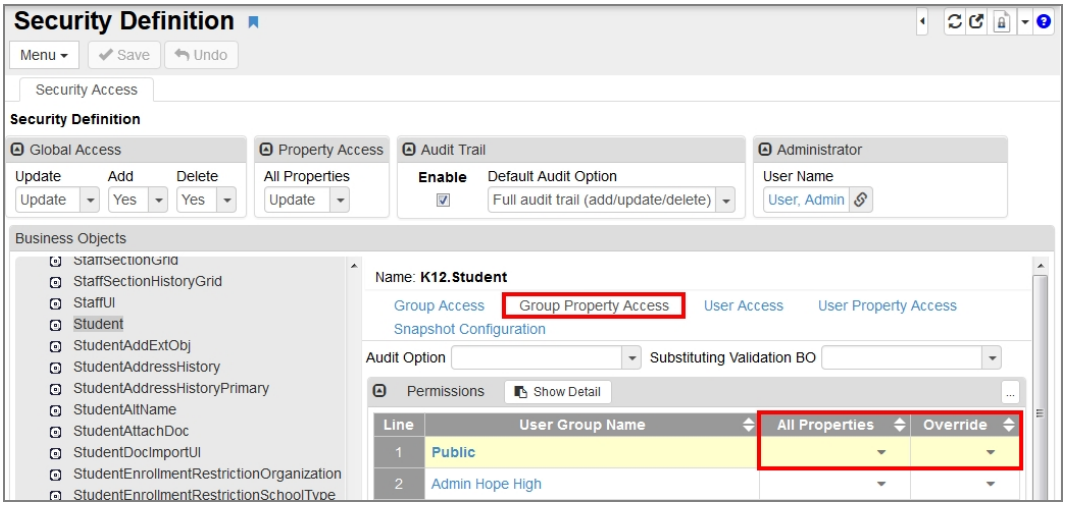
   The **Public** group is the default access for all groups. If you set Public to *No* for any business object, you must set the admin user group or admin to *Yes* to ensure you do not lock everyone out of the module.

8. Set any additional group settings.



Business Objects Details, Group Property Access Tab

9. Click **Save**. User groups with assigned custom rights display at the top of the list, followed by the groups with blank rights.
10. Select the **Group Property Access** tab to set the rights to individual properties of the selected business object.
11. Select the **All Properties** field to set the default rights for all user groups.
12. To use the value in the All Properties column to override any individual property rights set, select *Yes* in the **Override** column.

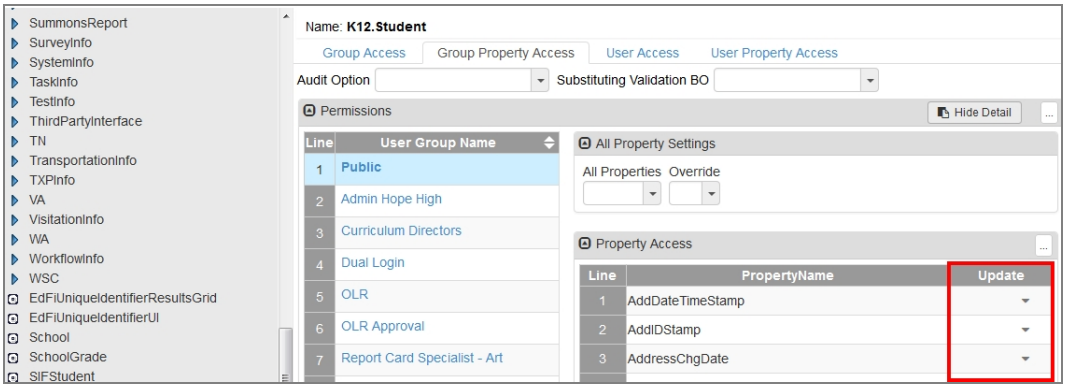


Business Objects Details, Group Property Access Tab

13. Set any additional group settings.
14. Click **Save**.
15. Click **Show Detail** to set specific rights for individual properties.

16. Select the **Update** option to set the update rights for each property.

> If the **Update** field is blank for any property, it inherits the setting for All Properties, or it uses the rights set for the entire business property.



Business Objects Details, Group Property Access Tab

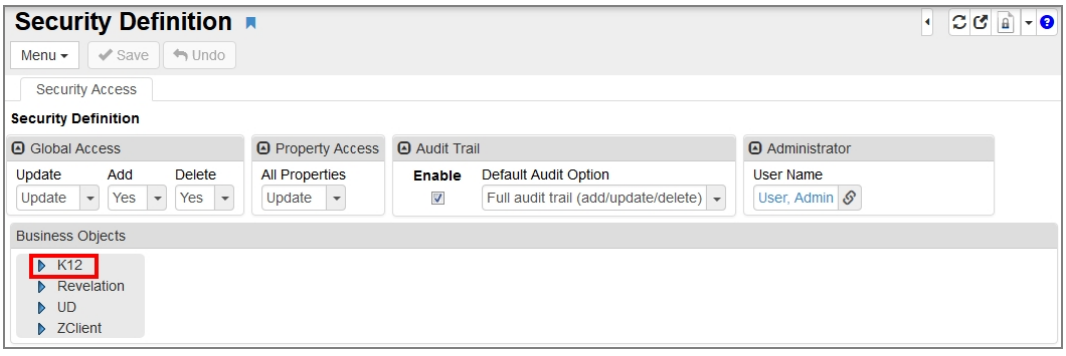
17. Click **Save**.

Customizing User Rights

Customize field access for specific users on the Security Definition screen.

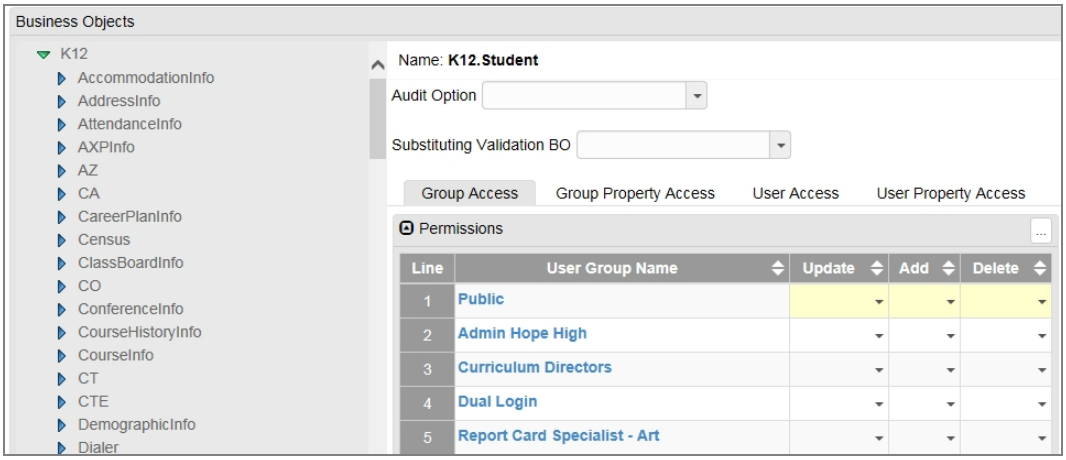
> If you set the screen in PAD Security to *View Only* for a user group or user, the update rights in Security Definition do not override this setting to change a field.

1. Navigate to **Synergy SIS > System > Security > Security Definition**.



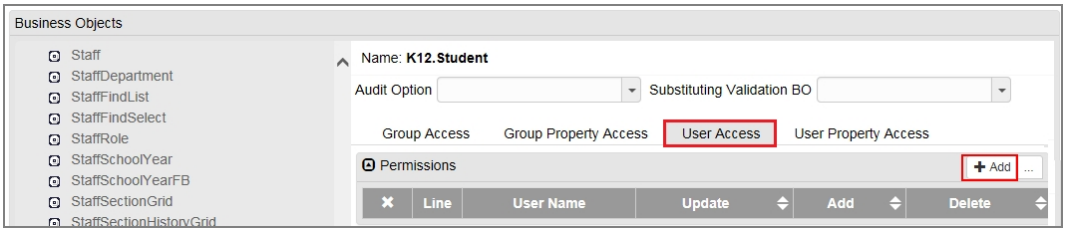
Security Definition Screen

2. Select a primary namespace to expand it and list all secondary namespaces.
   - The **K12** namespace contains most Synergy business objects.
   - The **Revelation** namespace holds the system-wide business objects, including attributes such as phone numbers.
   - The **UD** namespace holds user-defined namespaces and only shows business objects for districts with customized screens .
   - The **ZClient** namespace lists customized business objects for specific districts.
3. Select a secondary namespace to list the business objects.
4. Select a business object to view detail.



Security Definition Screen, Business Objects Details

5. Select the **User Access** tab.
6. Click **Add**. The **Find: RevUser** screen opens.



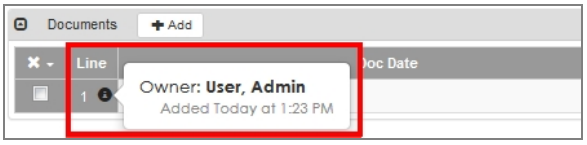
Business Objects Details, User Access Tab

7. Locate the user to modify, then click **Select**.

8. Select one of the following in the **Update** field:
   - *None* – Denies the user access to the object
   - *Update* – Grants the user the ability to update or delete records
   - *Update My Records Only* – Users can only update or delete records they originally entered. All other records are read-only.

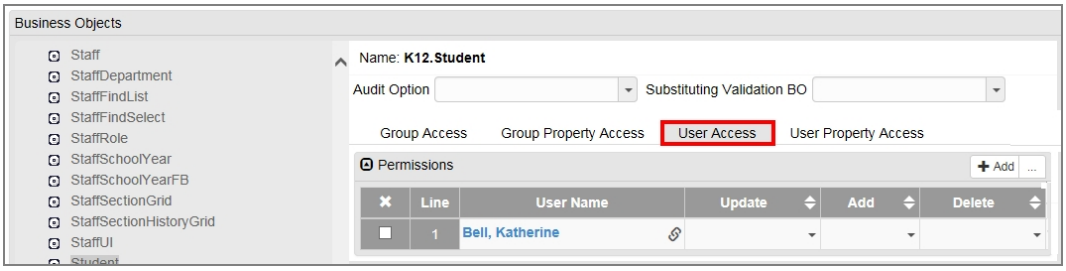
     Grids not tied to a direct business object (also called Unbound Grids) do not obey this security method. For example, you cannot secure user records on the Immunization Dosage Data grid on the **Immunization** tab of **Synergy SIS > Health > Health**.

     When enabled on a grid business object, an icon displays when hovering over a record that the user did not create. This icon displays the name of the user that created the record and when the record was added.

     Update My Records Only Option

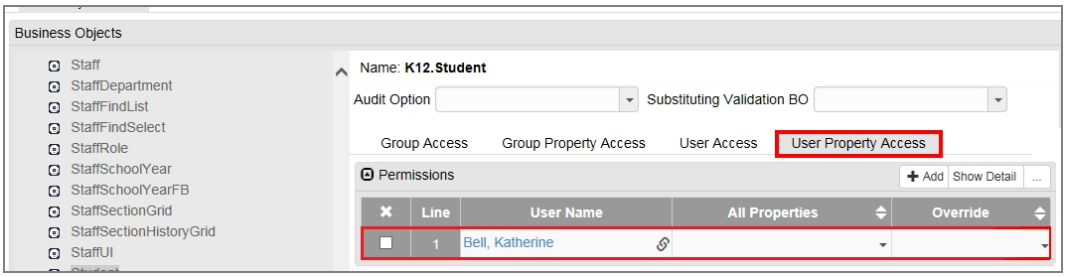
   - *View* – Gives the user group read-only access to the object
9. Select *Yes* in the **Add** field to allow the user to add records, or *No* to prevent the user from adding records.
10. Select *Yes* in the **Delete** field to allow the user to delete records, or *No* to prevent the user from deleting records.



Business Objects Details, User Access Tab

11. Click **Save**.
12. Select the **User Property Access** tab to set the rights to individual properties for the selected business object.
13. Select the **All Properties** field to set the default rights for the user.

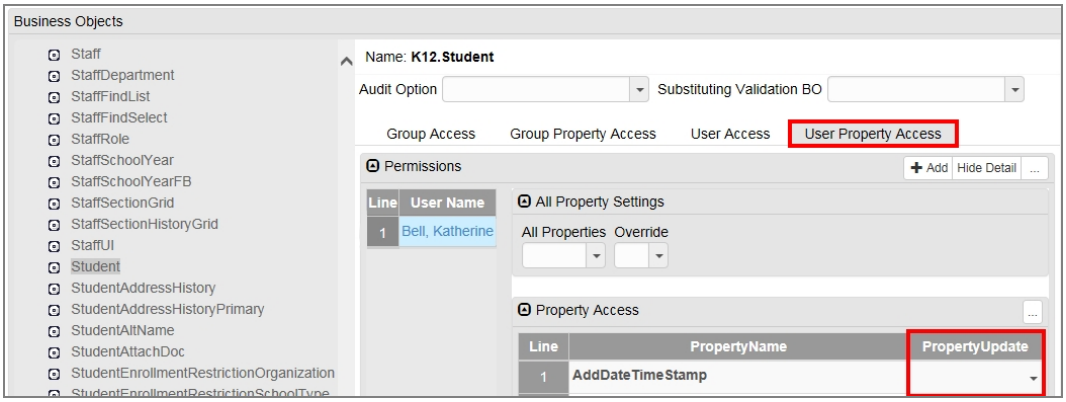
14. To use the value in the All Properties column to override any individual property rights set, select *Yes* in the **Override** column.



Business Objects Details, User Property Access Tab

15. Click **Save**.
16. Click **Show Detail** to set specific rights for individual properties.
17. Select the **Update** option to set the update rights for each property.

> If the **Update** field is blank for any property, it inherits the setting for All Properties, or it uses the rights set for the entire business property.



Business Objects Details, User Property Access Tab

18. Click **Save**.

Hiding Synergy Options

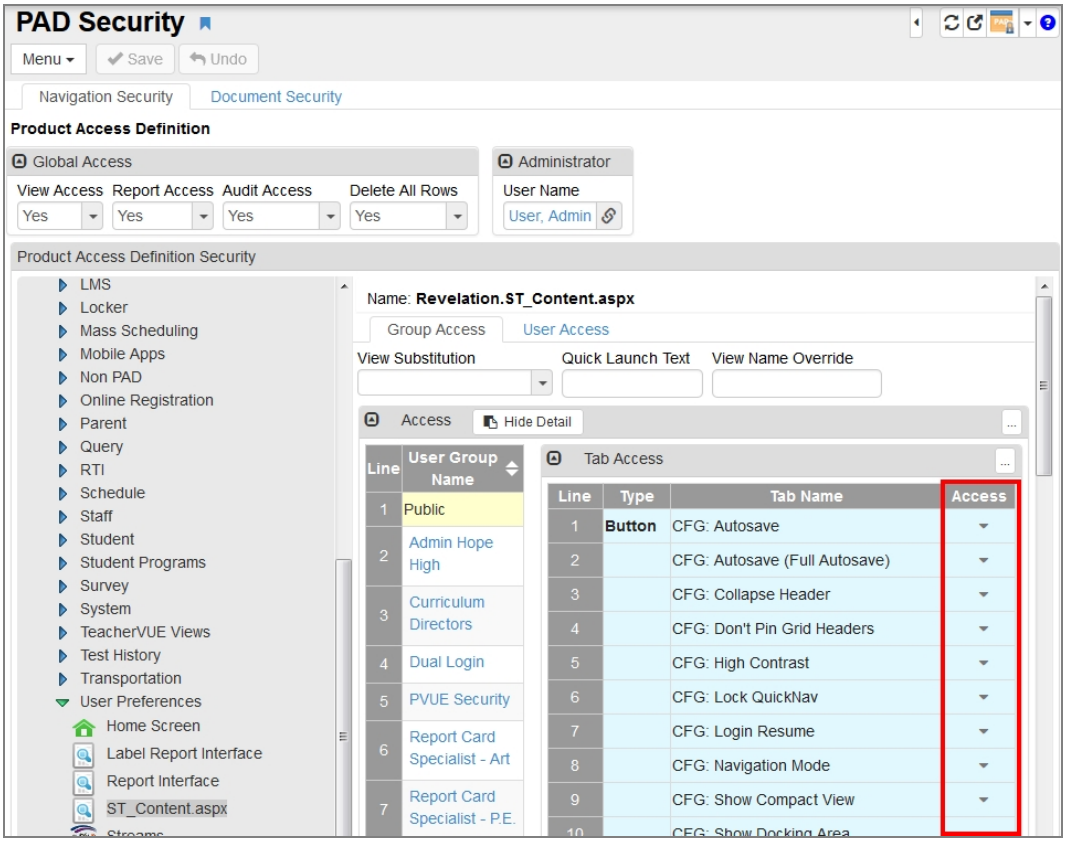
You can change the menu items that display as available for user groups or users in the Synergy Options menu in PAD Security.

Hiding Synergy Options for User Groups

1. Navigate to **Synergy SIS > System > Security > PAD Security**.
2. Navigate to **Synergy SIS > User Preferences > ST_Content.aspx** in the Product Access Definition Security tree.
3. Select the user group to modify and click **Show Detail**.

4. Select *No* in the **Access** column for any property to hide.

> The *NAV: Synergy Actions* property controls access to the Synergy Actions functionality. For more information, see the *Synergy SIS – Student Management Adminsitrator Guide*.



PAD Security Screen, PAD Security Details, Access Details

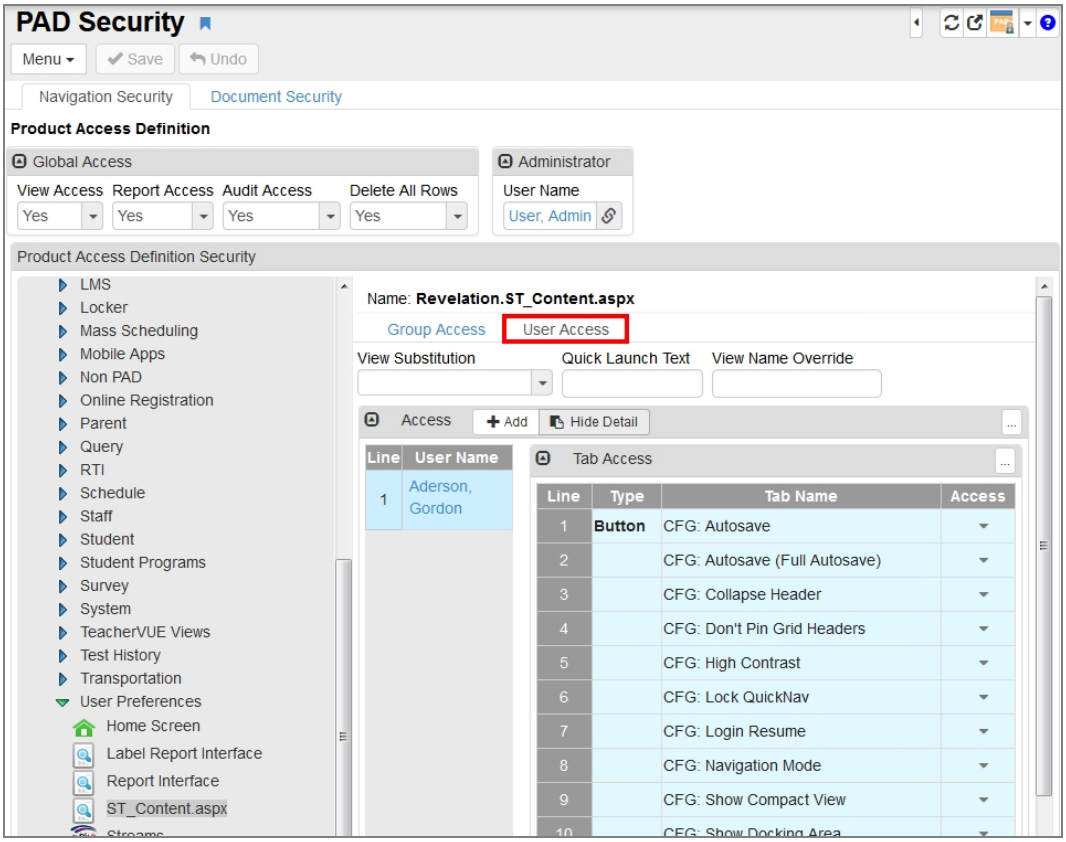
5. Click **Save**.

Hiding Synergy Options for Users

1. Navigate to **Synergy SIS > System > Security > PAD Security**.
2. Navigate to **Synergy SIS > User Preferences > ST_Content.aspx** in the Product Access Definition Security tree.
3. Select the **User Access** tab.
4. Click **Add** to find and select a user to modify.
5. Click **Show Detail**.

6. Select *No* in the **Access** column for any property to hide.

> The **NAV: Synergy Actions** property controls access to the Synergy Actions functionality. For more information, see the *Synergy SIS – Student Management Adminsitrator Guide*.



PAD Security Screen, PAD Security Details, User Access Tab, Access Details

7. Click **Save**.

Setting Field-Level Security in Admin Configuration

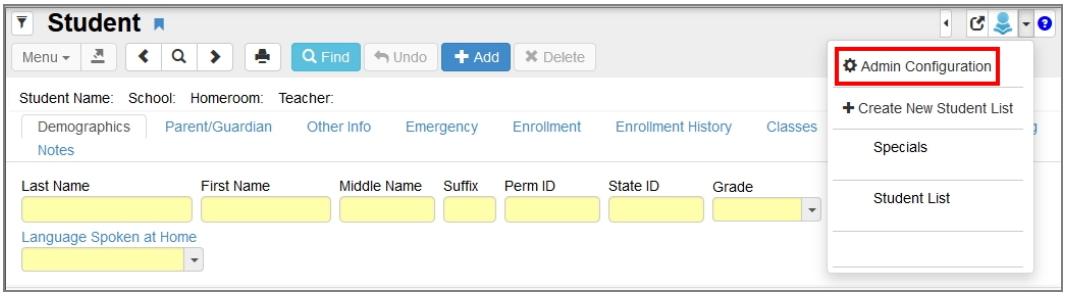
Admin Configuration allows you to configure business object security for multiple users or user groups. Security Mode allows you to directly edit security for any field on a screen. You can select the users or user groups that these changes effect.

> In order to access Admin Configuration, you must have *Update* permissions to the Security Definition and Property Override screens.
>
> You cannot access Admin Configuration through a pop-in window (Ex. Student Add Screen) or any report interface.

The following example uses the Student screen.

1. Navigate to **Synergy SIS > Student > Student**.
2. Click the arrow in top right corner.
3. Select **Admin Configuration**. The Admin Configuration screen appears.

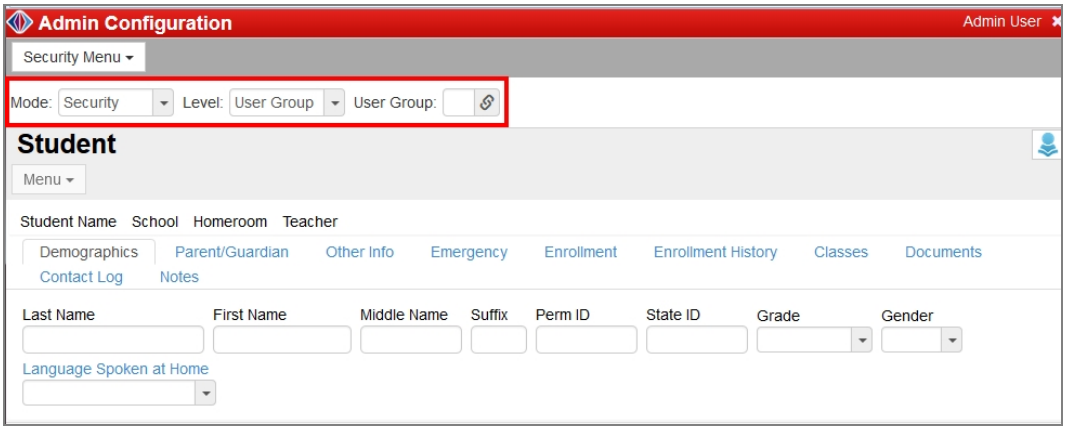
> The default **Mode** is *View / Property Override*. For more information on this mode, see the *Synergy SIS – System Administrator Guide*.



Student Screen

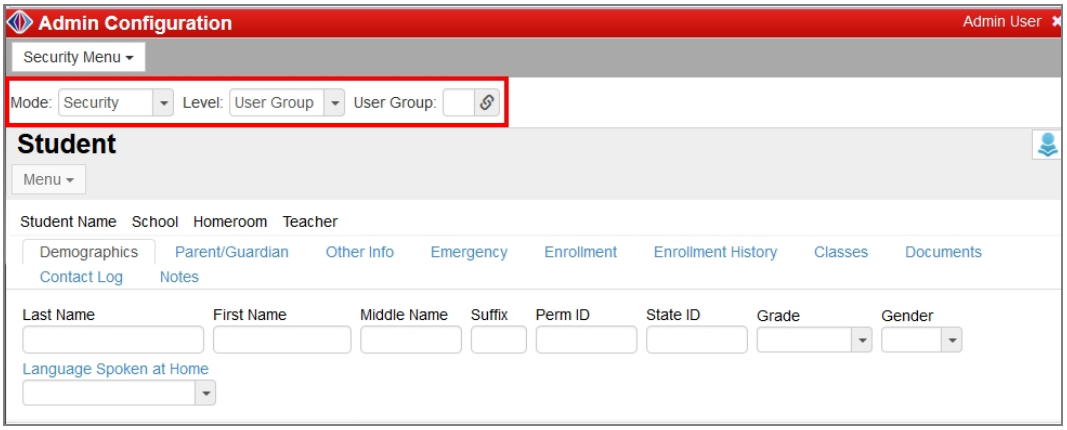
4. Select *Security* for the **Mode**.

5. Select the **Level**:
   - *Public* – Sets field access for all users
   - *User Group* – Sets field access for a specific user group. The **User Group** search field appears once selected.
   - *User* – Sets field access for a specific user. The **User** search field appears once selected.



Admin Configuration Screen

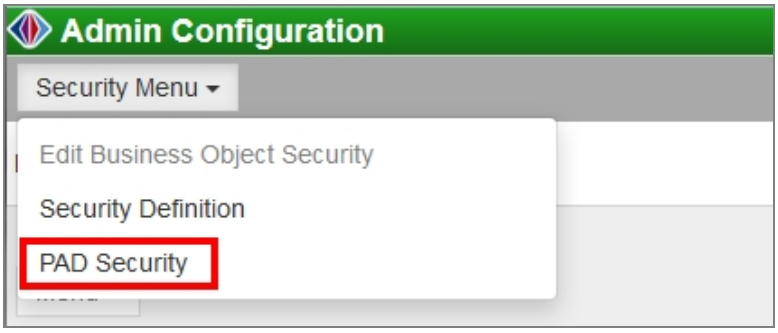
6. Click the arrow next to a field.
7. Select the security option:
   - *None* – Users have no access to the field.
   - *Update* – Users have Add, Edit, and Delete access to the field.
   - *View* – Users can only view the field.
   - *Default* – The field follows security based on the Global security settings.



Admin Configuration Screen

An icon displays next to the field to indicate the security change. You may need to refresh the original Synergy SIS screen after modifying values in Admin Configuration to view updates.

You can also select *Security Definition* from the **Security Menu** to open the Security Definition screen in a new window.



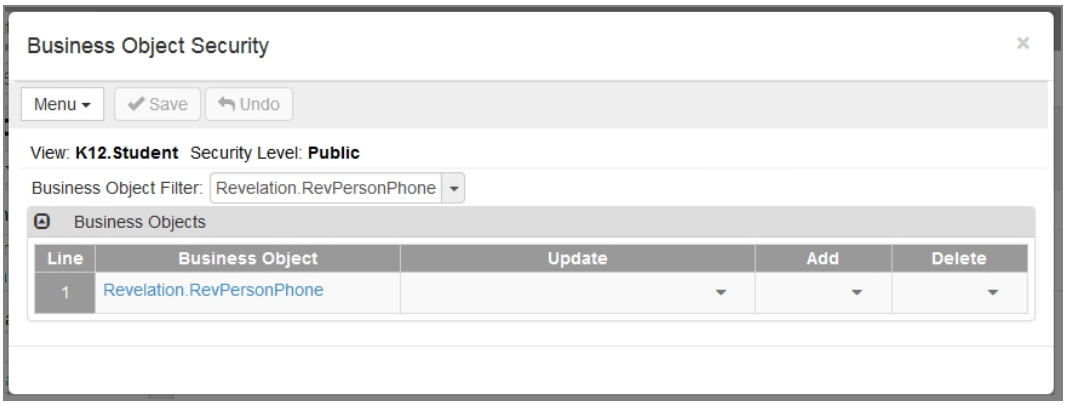
Admin Configuration Screen

Setting Grid Security

1. Click the **Grid Object Security** icon next to a grid. The Business Object Security screen opens.

Admin Configuration Screen

2. Select the **Update** value: *None*, *View*, *Update*, or *Update My Records Only*.
3. Select the **Add** value: *Yes* or *No*.
4. Select the **Delete** value for the business object: *Yes* or *No*.



Admin Configuration Screen

5. Click **Save**.

Setting Security for Multiple Fields on a Screen

You can view all the business objects associated with the screen and make changes to them at once.

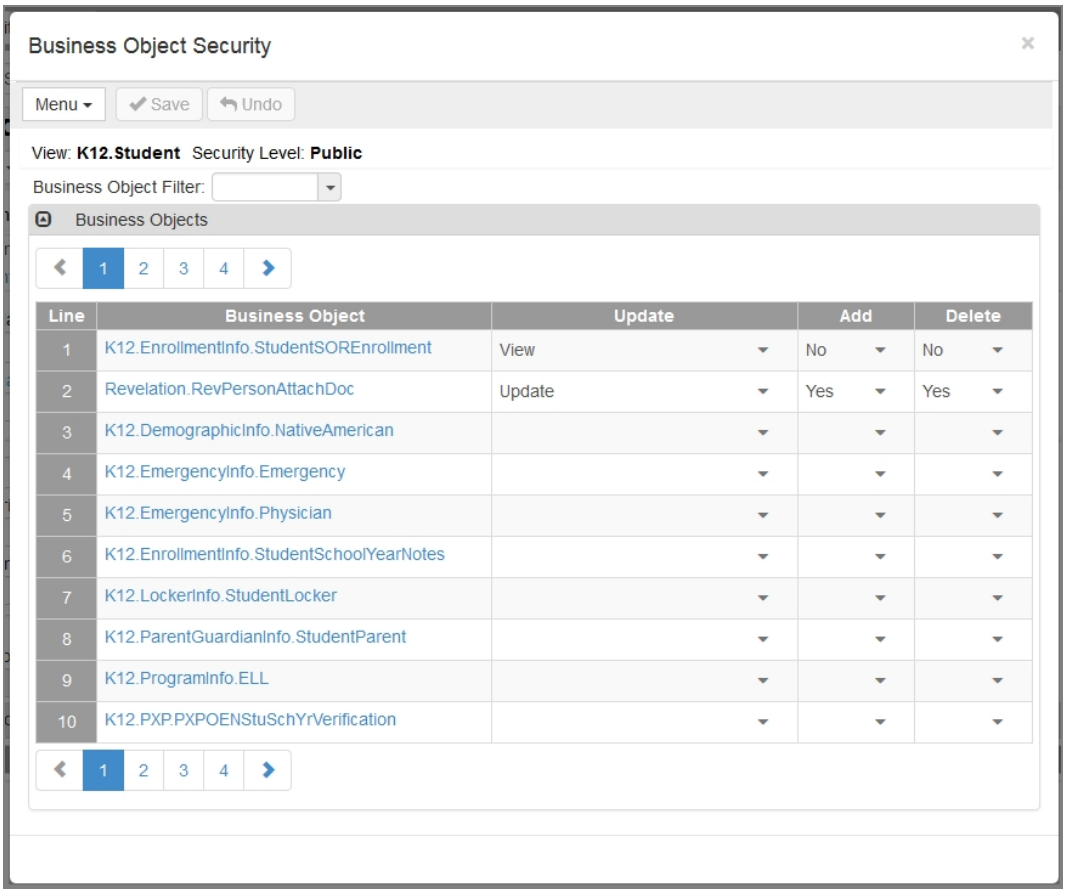
> Settings apply to the security level, user, or user group chosen on the main Admin Configuration screen.
>
> Use the **Business Object Filter** to only view a specific object.

1. Select *Edit Business Object Security* from the **Security Menu**. The Business Object Security screen appears.

Admin Configuration Screen

2. Select the **Update** value for an item: *None*, *View*, *Update*, or *Update My Records Only*.
3. Select the **Add** value for the business object: *Yes* or *No*.

4. Select the **Delete** value for the business object: *Yes* or *No*.



Business Object Security Screen

5. Click **Save**.

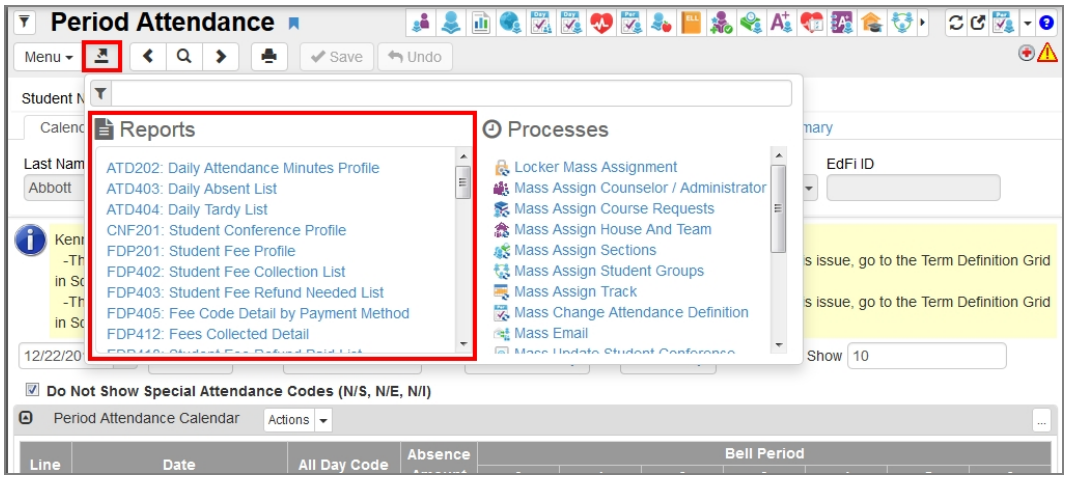
Chapter 5: Reports

Reports Overview

Four types of reports display in the PAD tree.

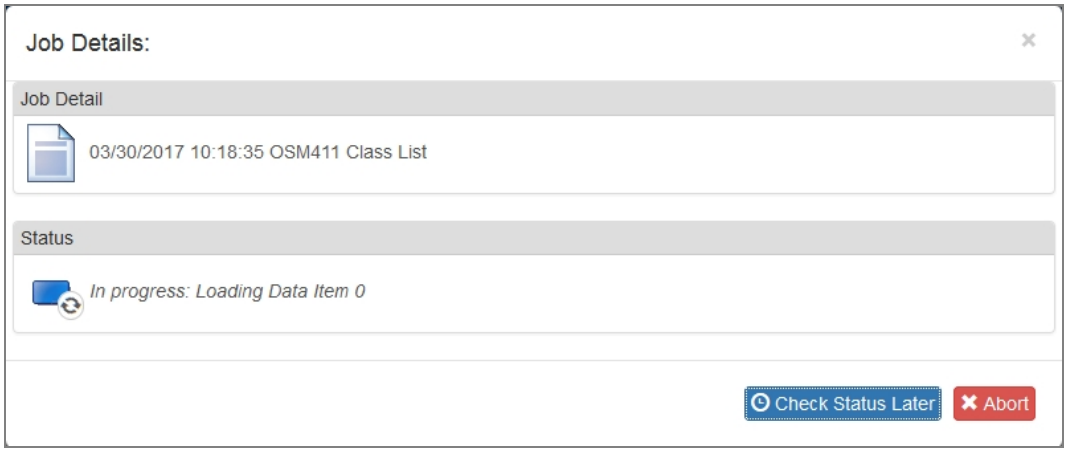
- **Individual** – 200-level reports are Individual reports. These print information for a single student per page and can be printed for multiple students at once.
- **List** – 400-level reports are List reports. These show details for multiple values, such as students or teachers, on one page.
- **Summary** – 600-level reports are Summary reports. These provide numerical totals for each category specified.
- **Extracts** – 800-level reports are Extract reports. These export information from Synergy SIS into a text file that can be used to import data into another program.

You can also run reports from any Synergy screen that focuses to a student or from Find results at **Synergy SIS > Student > Student** using the **Actions** icon. Synergy Actions includes most reports that have a Student section in the **Sort/Output** tab. The following example shows the reports available to run for a student at **Synergy SIS > Attendance > Period Attendance**.



Period Attendance Screen

The Job Details screen shows the Job Detail and Status during processing. Any processing errors show in the Status section. When the report completes, the Job Details screen closes and a PDF file of the report opens.



Job Details Screen

Reports use the current focus to pull data unless specified otherwise in report options. You can run report information at the district, organization, or school level. Options selected on the **Sort/Output** tab and your organization focus settings determine if inactive students display in reports.

> This section covers only the customizations specific to the reports used for this guide. See the *Synergy SIS – Query and Reporting Guide* to view information on additional report options.

PAD601 – PAD Security

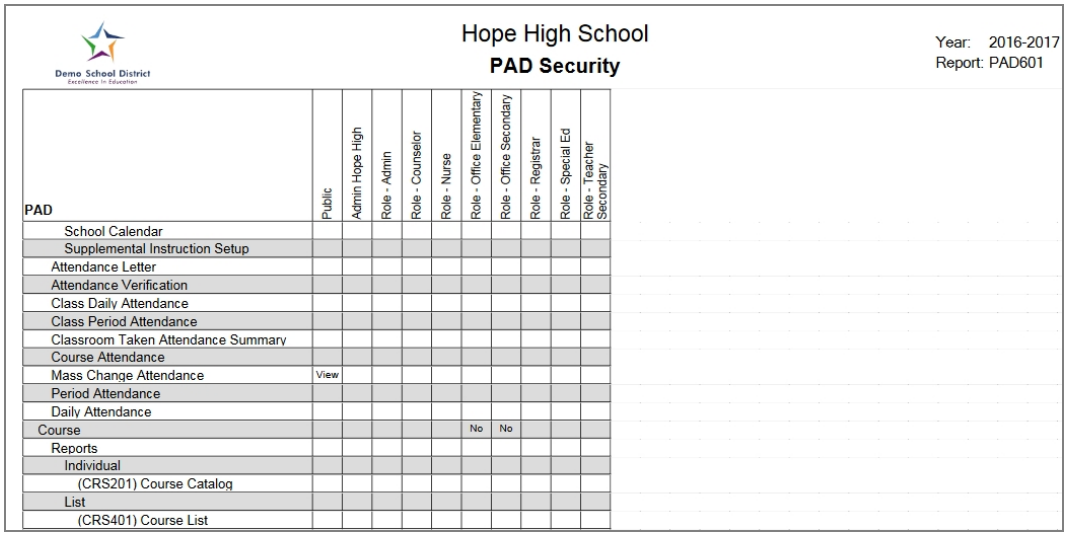
Synergy SIS > System > Security > Reports > Summary

The PAD Security report prints PAD Security detail by user group and screen/report.

PAD601 – PAD Security Report Interface Screen

Report Options:

- **User Group** – Select the user group to print results for
- **PAD Location** – Select the PAD Location to filter results for
- **Show menu, tab, and button details** – Select to include menu, tab, and button details from PAD Security

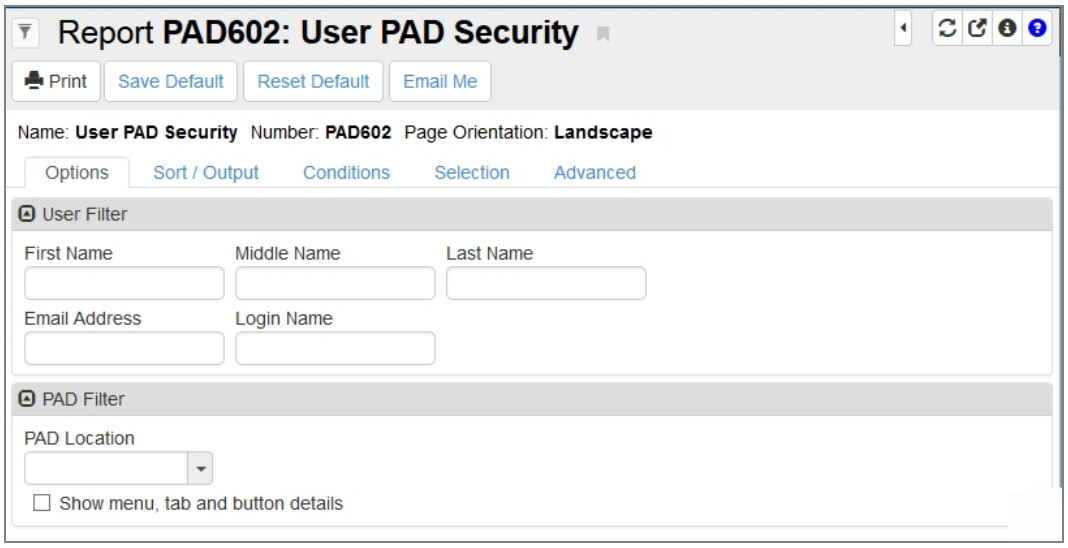


PAD601 PAD Security Report Output

PAD602 – User PAD Security

Synergy SIS > System > Security > Reports > Summary

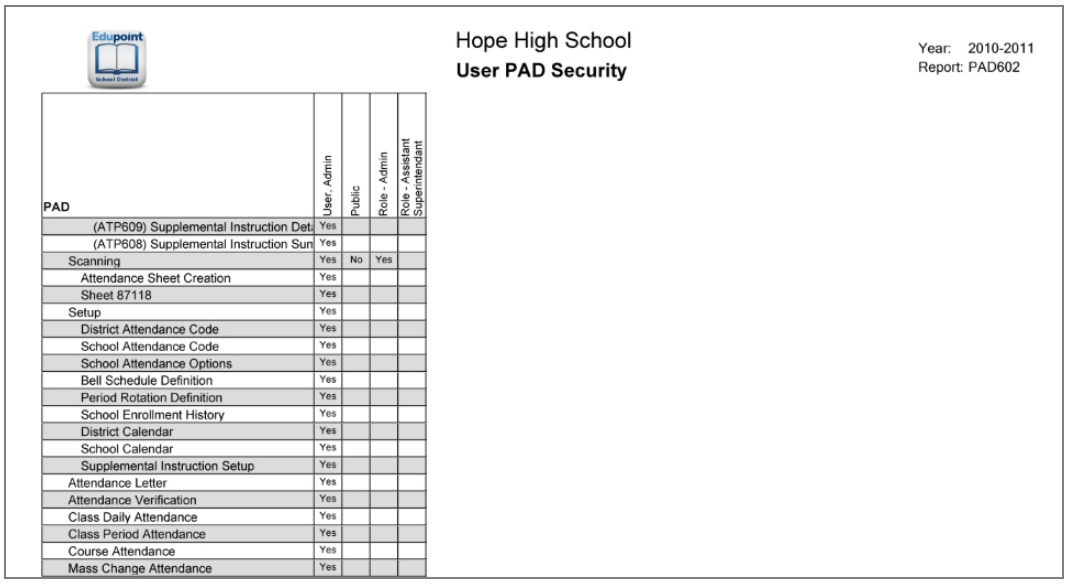
The User PAD Security report prints PAD Security detail by user.



PAD602 – User PAD Security Report Interface Screen

Report Options:

- User Filter – Select the user information to print results for
- **PAD Location** – Select the PAD Location to filter results for
- **Show menu, tab, and button details** – Select to include menu, tab, and button details from PAD Security



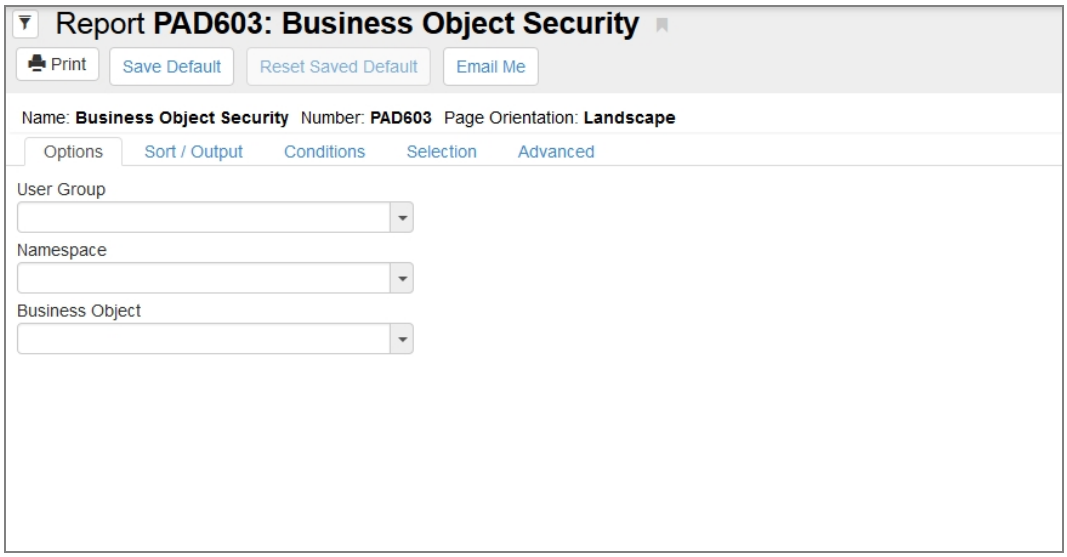
PAD	User: Admin	Public	Role - Admin	Role - Assistant Superintendant
(ATP609) Supplemental Instruction Det	Yes			
(ATP608) Supplemental Instruction Sun	Yes			
Scanning	Yes	No	Yes	
Attendance Sheet Creation	Yes			
Sheet 87118	Yes			
Setup	Yes			
District Attendance Code	Yes			
School Attendance Code	Yes			
School Attendance Options	Yes			
Bell Schedule Definition	Yes			
Period Rotation Definition	Yes			
School Enrollment History	Yes			
District Calendar	Yes			
School Calendar	Yes			
Supplemental Instruction Setup	Yes			
Attendance Letter	Yes			
Attendance Verification	Yes			
Class Daily Attendance	Yes			
Class Period Attendance	Yes			
Course Attendance	Yes			
Mass Change Attendance	Yes			

PAD602 User PAD Security Report

PAD603 – Business Object Security

Synergy SIS > System > Security > Reports > Summary

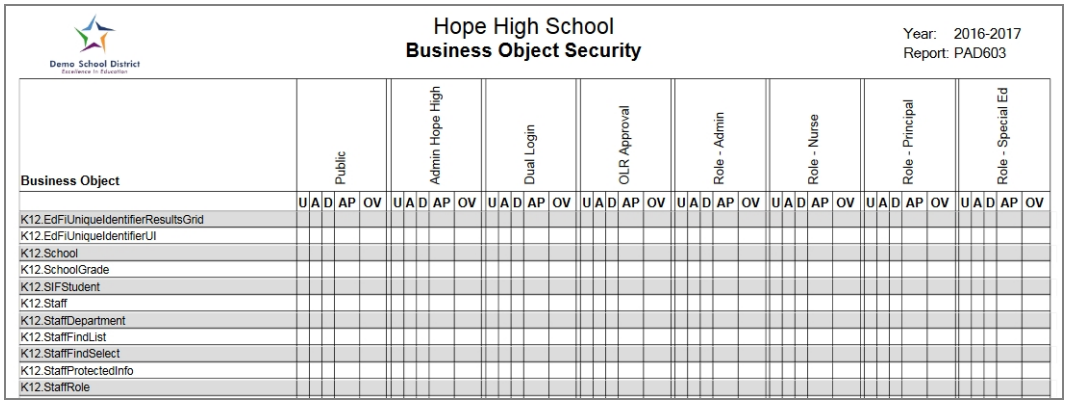
The Business Object Security report prints security detail by business object and user group.



PAD603 – Business Object Security Report Interface

Report Options:

- **User Group** – Select the user group to print results for
- **Namespace** – Select the specific namespace to filter the report for
- **Business Object** – Select the specific business object to filter the report for



Hope High School
Business Object Security

Year: 2016-2017
Report: PAD603

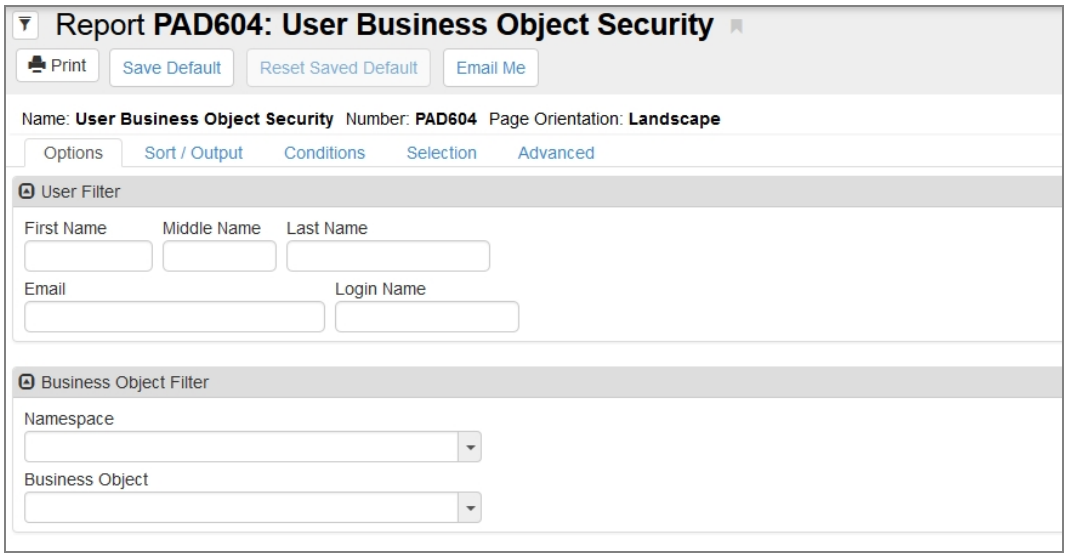
Business Object	Public					Admin Hope High					Dual Login					OLR Approval					Role - Admin					Role - Nurse					Role - Principal					Role - Special Ed				
	U	A	D	AP	OV	U	A	D	AP	OV	U	A	D	AP	OV	U	A	D	AP	OV	U	A	D	AP	OV	U	A	D	AP	OV	U	A	D	AP	OV	U	A	D	AP	OV
K12.EdFiUniqueIdentifierResultsGrid																																							
K12.EdFiUniqueIdentifierUI																																							
K12.School																																							
K12.SchoolGrade																																							
K12.SIFStudent																																							
K12.Staff																																							
K12.StaffDepartment																																							
K12.StaffFindList																																							
K12.StaffFindSelect																																							
K12.StaffProtectedInfo																																							
K12.StaffRole																																							

PAD603 Business Object Security Report

PAD604 – User Business Object Security

Synergy SIS > System > Security > Reports > Summary

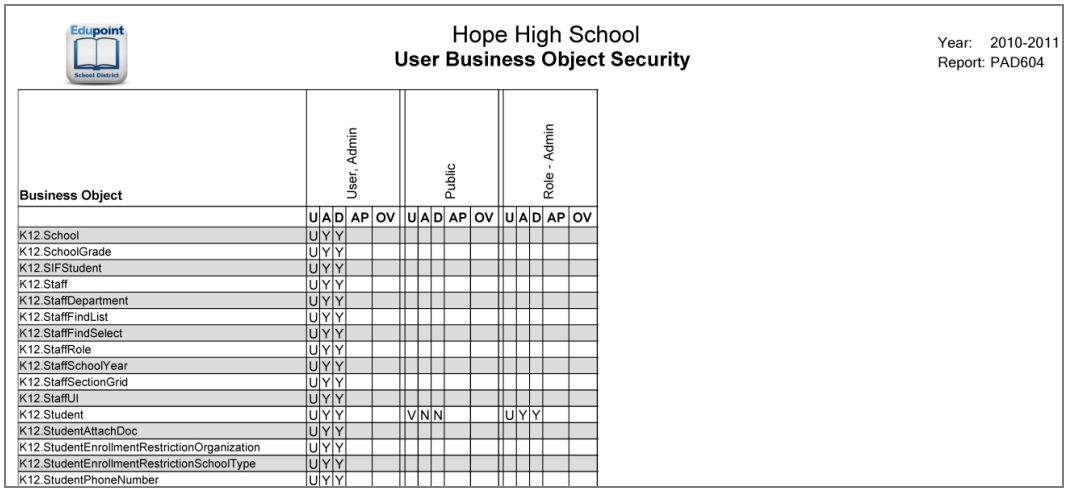
The User Business Object Security report prints security detail by business object and user.



PAD604 – Business Object Security Report Interface

Report Options:

- User Filter – Select the user information to print results for
- **Namespace** – Select the specific namespace to filter the report for
- **Business Object** – Select the specific business object to filter the report for



Hope High School
User Business Object Security

Year: 2010-2011
Report: PAD604

Business Object	User, Admin					Public					Role - Admin				
	U	A	D	AP	OV	U	A	D	AP	OV	U	A	D	AP	OV
K12.School	U	Y	Y												
K12.SchoolGrade	U	Y	Y												
K12.SIFStudent	U	Y	Y												
K12.Staff	U	Y	Y												
K12.StaffDepartment	U	Y	Y												
K12.StaffFindList	U	Y	Y												
K12.StaffFindSelect	U	Y	Y												
K12.StaffRole	U	Y	Y												
K12.StaffSchoolYear	U	Y	Y												
K12.StaffSectionGrid	U	Y	Y												
K12.StaffUI	U	Y	Y												
K12.Student	U	Y	Y			V	N	N			U	Y	Y		
K12.StudentAttachDoc	U	Y	Y												
K12.StudentEnrollmentRestrictionOrganization	U	Y	Y												
K12.StudentEnrollmentRestrictionSchoolType	U	Y	Y												
K12.StudentPhoneNumber	U	Y	Y												

Business Object Security Report