Synergy™

Student Information System

Synergy SIS©

Security
Administrator Guide

Edupoint™

Edupoint Educational Systems, LLC
1955 South Val Vista Road, Ste 210
Mesa, AZ 85204
Phone (877) 899-9111
Fax (800) 338-7646

Volume 01, Edition 01, Revision 03 **April 2013**

Document Number: SISSCAG-010102

First Edition, February 2010
First Edition, Second Revision, July 2011
First Edition, Third Revision, April 2013

This edition applies to Synergy SIS™ Student Information System software and all subsequent releases and modifications until indicated with new editions or revisions.

Edupoint’s Synergy SIS Student Information System software and any form of supporting documentation are proprietary and confidential. Unauthorized reproduction or distribution of the software and any form of supporting documentation is strictly prohibited and may result in severe civil and criminal penalties.

Information in this document is provided in connection with Edupoint Educational Systems products. No license to any intellectual property rights is granted by this document.

The screens, procedural steps, and sample reports in this manual may be slightly different from the actual software due to modifications in the software based on state requirements and/or school district customization.

The data in this document may include the names of individuals, schools, school districts, companies, brands, and products. Any similarities to actual names and data are entirely coincidental.

TABLE OF CONTENTS

ABOUT THIS GUIDE

Document History

Date	Volume	Edition	Revision	Content
February 2010	1	1	1	Initial release of this document
July 2011	1	1	2	Updated for changes in the June 2011 release
April 2013	1	1	3	Updated for changes in the March 2013 release of Synergy SIS 8.0.

CONVENTIONS USED IN THIS GUIDE

Bold Text

Bold Text - Indicates a button or menu or other text on the screen to click, or text to type.

💡

Tip – Suggests advanced techniques or alternative ways of approaching the subject.

📝

Note – Provides additional information or expands on the topic at hand.

ℹ

Reference – Refers to another source of information, such as another manual or website

CAUTION!

Caution – Warns of potential problems. Take special care when reading these sections.

BEFORE YOU BEGIN

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

> **Caution:** The Edupoint family of software does not support the use of pop-up blockers or third-party toolbars in the browser used to access Synergy SIS. Please disable any pop-up blockers and extra toolbars before logging in to any Edupoint product.

Chapter One: OVERVIEW

This chapter covers:

- ► Overview of Synergy SIS security
- ► Implementation considerations

OVERVIEW OF Synergy SIS SECURITY

This guide describes how to customize security throughout Synergy SIS. Chapter Five describes reports that list the current security configuration and shows how to customize and print them.

Security can be broken down into four areas:

- Screen-Level Security (also known as PAD Security)
- Field-Level Security (also known as Business Object Security)
- Organization and Year Security
- The **Security Settings** tab in the **User** and **User Group** screens

Screen-level security addresses which users in Synergy SIS are allowed to update or see the data in a particular screen. Field-level security specifies where users can update or screen specific data within a screen. This security is applied across all organizations and years within Synergy SIS. These security settings are outlined in this guide, and are defined using the PAD Security screen and the Security Definition screen.

The Organization and Year security sets which users can see and/or update data for a specific school, and which school years can be updated and viewed. The Security Settings define user access to specific areas with Synergy SIS, including the Discipline and Conference data, the TeacherVUE software, and the Grade Book software. These settings are covered in the *Synergy SIS – System Administrator Guide* and are defined in the **User** and **User Group** screens.

Security settings described in this guide can be exported from, and imported into, Synergy SIS with the Generic Conversion Tool. For details, see the *Synergy Data Conversion Guide*.

IMPLEMENTATION CONSIDERATIONS

When setting up the Synergy SIS security, the following issues need to be considered:

What is the default security assigned to everyone in the system before customization?

The first step in configuring the rights to each screen is to set the default, or Global Access, rights to be used throughout the system. Two approaches can be taken. The first approach is to give everyone access to update everything, and then specify by user group what that group cannot access or update. The second approach is to forbid access to everyone, and then specify what each user group can access and/or update.

> **Caution:** If selecting the second approach and forbidding access to everyone initially, be sure to set the Admin user or the user group to which the Admin user belongs with access to everything. Otherwise, even the Admin user could be completely locked out of the system.

If most users will have access to view or update most screens, the first approach would be easier to implement. If only select users will be viewing or updating the data, the second approach would be quicker to set up.

What user groups need to be created?

When setting up security, the users can be grouped to make it easier to apply security settings across several users at one time. If a particular user has unique security needs, security settings can be configured at the individual user level as well, but it is recommended to use the 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 on the same field, the user will be granted the least restrictive access. For example, if one group has View rights but the other group has Update rights, the user will have Update rights.

The order in which security settings are applied is:

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

Therefore, user-based settings override user group settings and so on.

The instructions on how to set up user groups can be found in the *Synergy SIS – System Administrator Guide*. Generally, a district has three types of user groups:

- Organization-based groups – these groups are set up to govern the access to view or update the information of specific organizations in the district. An example of an organization-based group is a group that has Update access to a specific school.
- Role-based groups – these groups are based on the position the users in the group have in the district. An example of a role-based group is a group for Principals. These types of groups are helpful if each person generally has only one role in the district and the security rights for the roles do not change.
- Security-based groups – these groups are configured around the security rights assigned to the group. An example of a security-based group is a group that has the security right to update student addresses.

When naming the user groups, remember that they are sorted alphabetically, so it is helpful to create a naming scheme that keeps like groups together. Sample user group names include:

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

User groups should be created before the security settings are modified.

In what order should security be configured?

Security settings generally should be set up in the following order:

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

In general, if a user group does not have access to a screen, there is no need to configure security for the business objects and properties in that screen for that user group.

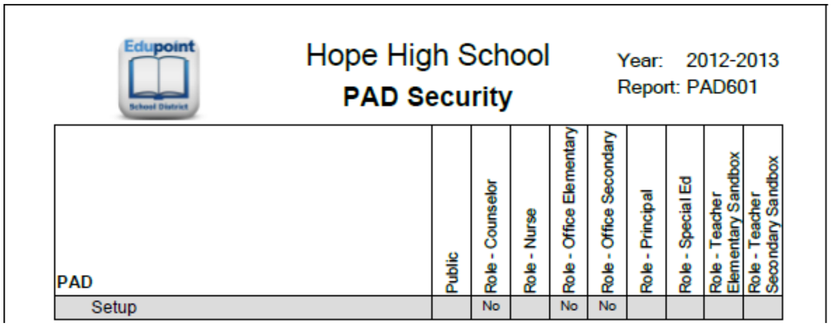
On the other hand, if you control access to a business object – allowing or disallowing access to it for some group – you are controlling access to it wherever it appears. Many business objects appear on multiple screens.

The **PAD Security** screen determines what screens and reports are shown in the Navigation Tree, or PAD Tree, for each user group. How to set PAD security is covered in Chapter Three. In addition, the **PAD Security** governs certain items not in the PAD Tree, such as **GBSecurity** and **Non PAD**; see the Caution on page 31.

What security settings need to be configured for each user group?

Once the user groups have been defined, the last step is to determine what the settings should be for each user group. It is recommended that these settings be documented on paper first before the settings are modified in Synergy SIS.

The reports described in Chapter Five can serve as a worksheet for this purpose. For example, the PAD601 – PAD Security report shows whether a group's access to something in the PAD Tree is assigned explicitly or inherited. A blank cell indicates inheritance.



Hope High School

PAD Security

Year: 2012-2013

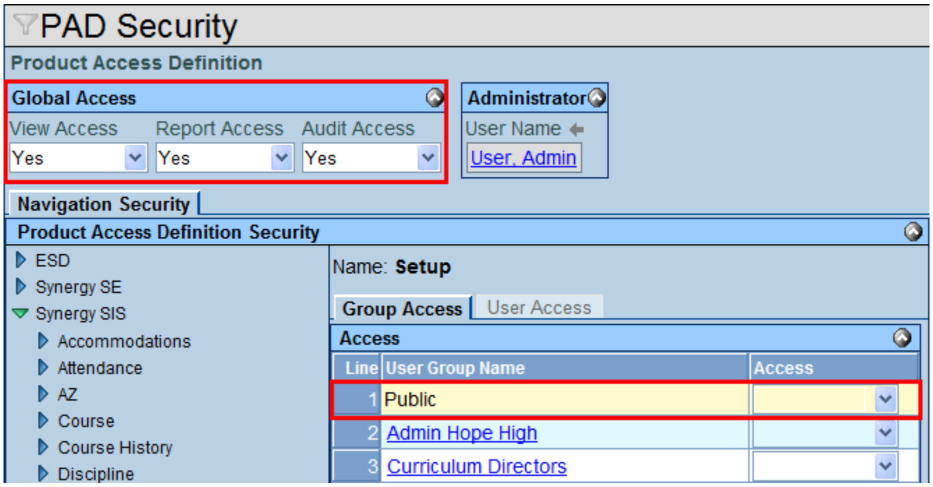
Report: PAD601

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				

Figure 1.1 – PAD Security Report

As mentioned on page 9, the order of inheritance is

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



PAD Security

Product Access Definition

Global Access

View Access	Report Access	Audit Access
Yes	Yes	Yes

Administrator

User Name: User, Admin

Navigation Security

Product Access Definition Security

Name: **Setup**

Group Access | User Access

Access

Line	User Group Name	Access
1	Public	
2	Admin Hope High	
3	Curriculum Directors	

Figure 1.2 – PAD Security Screen, Global and Public Settings

See Chapter Three for details.

Chapter Two: AUDITING

This chapter covers:

- ► What is auditing?
- ► How to configure system-wide auditing
- ► How to specify auditing for a business object
- ► How to specify auditing for a group of business objects
- ► Sample queries to review audit logs

WHAT IS AUDITING?

Auditing in Synergy SIS logs any changes to the data in the screens. The auditing may be enabled on all screens and business objects throughout Synergy SIS, or each business object may be assigned a specific type of auditing. A business object in Synergy SIS is a specific part of a screen, such as Phone Number grid.

Once auditing is enabled, a log of all changes to a record is available in any screen. To access the log from any screen:

1. Locate the record to audit using either the Scroll buttons or Find mode.
2. Click the **Menu** button at the top of the screen, and select **View Audit Detail**. The Audit Trail History screen opens.

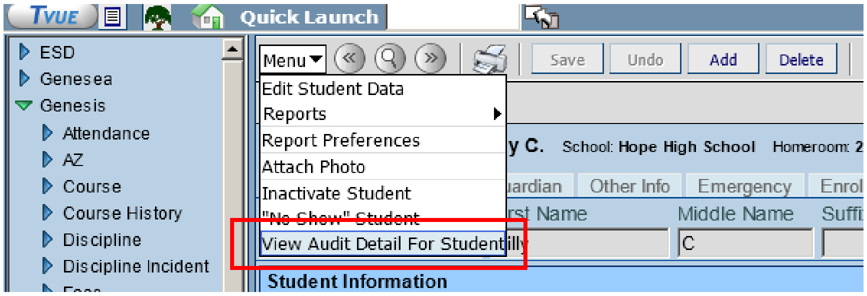
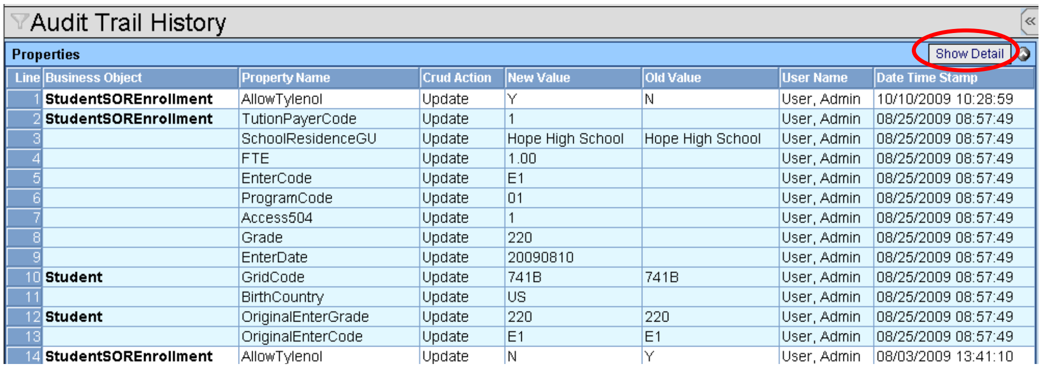


Figure 2.1 – Accessing the Audit Detail

3. This screen lists the specific **Business Object** that was changed and the field, or **Property Name**, that was modified. For each change, it lists whether the data was added, updated, or deleted in the **Crud Action** column. The previous value is shown in the **Old Value** column, and the current value is listed in the **New Value** column. The **User Name** column shows the name of who changed the data, and the **Date Time Stamp** lists when the change was made.

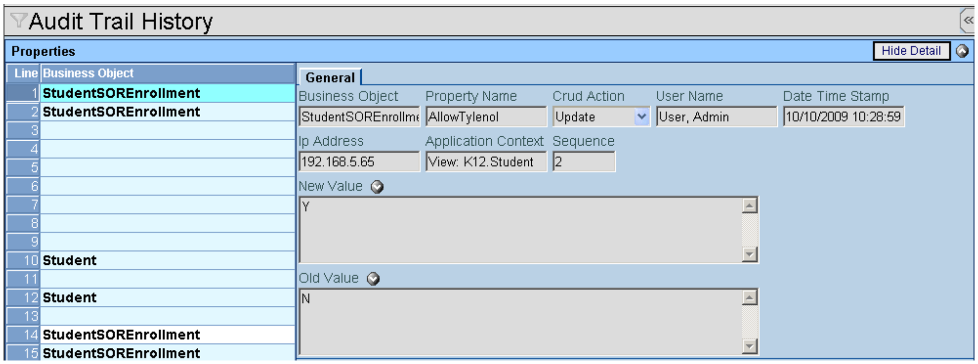


Line	Business Object	Property Name	Crud Action	New Value	Old Value	User Name	Date Time Stamp
1	**StudentSOREnrollment**	AllowTylenol	Update	Y	N	User, Admin	10/10/2009 10:28:59
2	**StudentSOREnrollment**	TutionPayerCode	Update	1		User, Admin	08/25/2009 08:57:49
3		SchoolResidenceGU	Update	Hope High School	Hope High School	User, Admin	08/25/2009 08:57:49
4		FTE	Update	1.00		User, Admin	08/25/2009 08:57:49
5		EnterCode	Update	E1		User, Admin	08/25/2009 08:57:49
6		ProgramCode	Update	01		User, Admin	08/25/2009 08:57:49
7		Access504	Update	1		User, Admin	08/25/2009 08:57:49
8		Grade	Update	220		User, Admin	08/25/2009 08:57:49
9		EnterDate	Update	20090810		User, Admin	08/25/2009 08:57:49
10	**Student**	GridCode	Update	741B	741B	User, Admin	08/25/2009 08:57:49
11		BirthCountry	Update	US		User, Admin	08/25/2009 08:57:49
12	**Student**	OriginalEnterGrade	Update	220	220	User, Admin	08/25/2009 08:57:49
13		OriginalEnterCode	Update	E1	E1	User, Admin	08/25/2009 08:57:49
14	**StudentSOREnrollment**	AllowTylenol	Update	N	Y	User, Admin	08/03/2009 13:41:10

Figure 2.2 – Audit Trail History Screen

4. To view additional information about each change, click the **Show Detail** button.

5. The detail screen appears on the right side of the screen. To select which record to view, click the **Line** number of the **Business Object** on the left. The business object currently shown is highlighted.



Audit Trail History

Properties

Hide Detail

Line	Business Object
1	StudentSOREnrollment
2	StudentSOREnrollment
3	
4	
5	
6	
7	
8	
9	
10	Student
11	
12	Student
13	
14	StudentSOREnrollment
15	StudentSOREnrollment

General

Business Object	Property Name	Crud Action	User Name	Date Time Stamp
StudentSOREnrollme	AllowTylenol	Update	User, Admin	10/10/2009 10:28:59

Ip Address	Application Context	Sequence
192.168.5.65	View: K12.Student	2

New Value: Y

Old Value: N

Figure 2.3 – Audit Trail History Screen, Detail Screen

6. Additional information shown in the detail screen is the **IP Address** of the computer from where the changes was made, the name of the screen used to make the change in the **Application Context** field, and the **Sequence** number. The Sequence number indicates if the business object was the primary business object for the screen (a 1) or a business object linked to the primary business object (a 2).

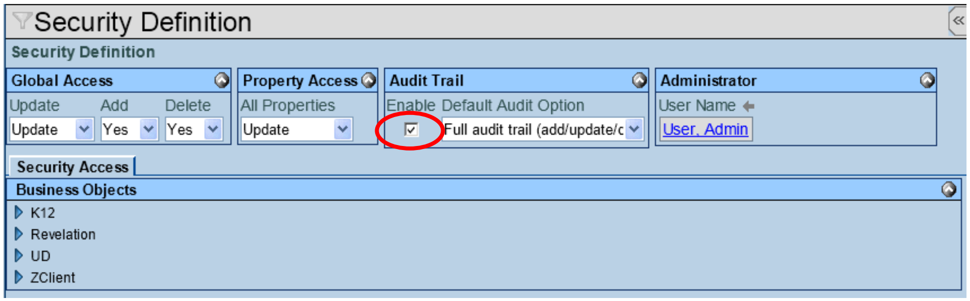
7. To return to the main screen, click the **Hide Detail** button.

SYSTEM-WIDE AUDITING

When Synergy SIS is first installed, auditing is turned off. This is controlled in the **Security Definition** screen. To enable auditing on all screens:

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

2. Check the **Enable** box in the **Audit Trail** section.



Security Definition

Security Definition

Global Access

Update	Add	Delete
Update	Yes	Yes

Property Access

All Properties: Update

Audit Trail

Enable	Default Audit Option
☑	Full audit trail (add/update/c

Administrator

User Name: User, Admin

Security Access

Business Objects

- K12
- Revelation
- UD
- ZClient

Figure 2.4 – Security Definition Screen

3. Select the **Default Audit Option** to be used for all business objects. It can be set to a **Full audit trail**, which logs all additions, updates, and deletions; **Audit trail of changes only**, which logs updates to existing data; or **No audit trail**, which does not log anything. **No audit trail** is helpful if only a few business objects will be audited; those can be enabled as described in the next section.

4. Click the **Save** button at the top of the screen.

Caution: Setting a **Full audit trail** of every business object can increase the size of the database dramatically, particularly for large districts. This can lead to decreased performance. It may be helpful to clear these tables annually to reduce database size. Be sure to back up the data in these tables before deleting. To clear the audit logs, delete all data in the REV_AUDIT_TRAIL and REV_AUDIT_TRAIL_PROP tables. All data must be removed from both tables, or errors can occur.

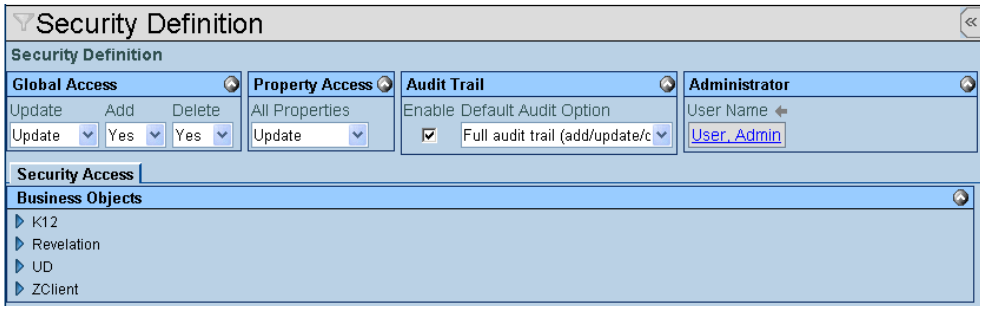
BUSINESS OBJECT AUDITING

To reduce the size of the audit logs, the district may choose to disable or enable auditing on specific business objects.

You can also configure auditing for a defined group of business objects. See *Business Object Group Auditing* on page 18.

To specify the audit option for a business object:

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

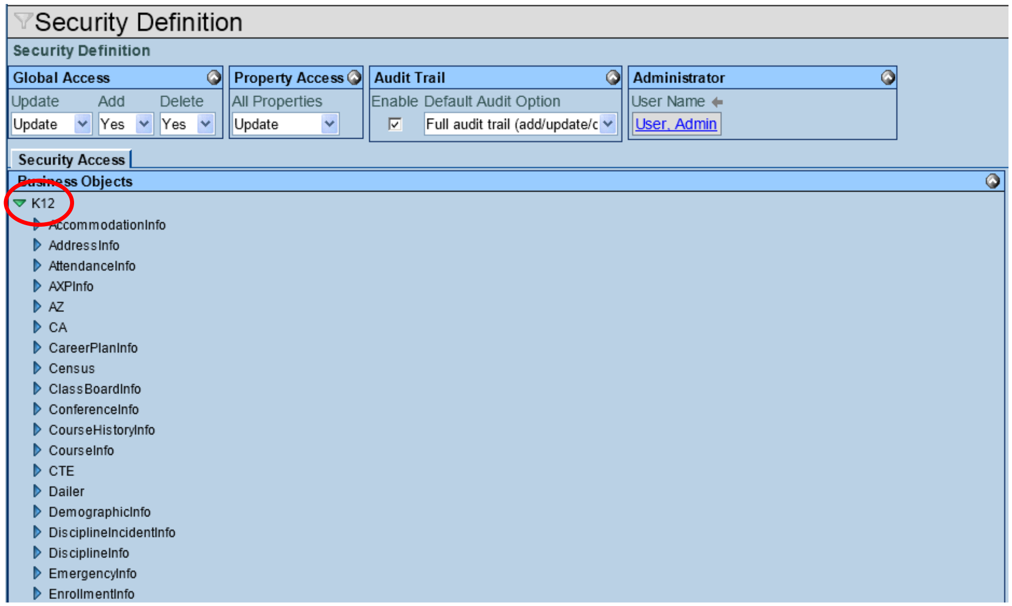


Update	Update
Add	Yes
Delete	Yes
All Properties	Update
Enable	☑
Default Audit Option	Full audit trail (add/update/c
User Name	User, Admin

- K12
- Revelation
- UD
- ZClient

Figure 2.5 – Security Definition Screen

2. Click a primary namespace to expand it and list the secondary namespaces. Most business objects are in the **K12** namespace. The **Revelation** namespace holds the system-wide business objects, including attributes like phone numbers. The **UD** namespace holds user-defined namespaces, and shows business objects for districts with customized screens only. The **ZClient** namespace lists customized business objects for specific districts.



Security Definition

Security Definition

Global Access			Property Access	Audit Trail		Administrator
Update	Add	Delete	All Properties	Enable	Default Audit Option	User Name
Update	Yes	Yes	Update	☑	Full audit trail (add/update/c	User, Admin

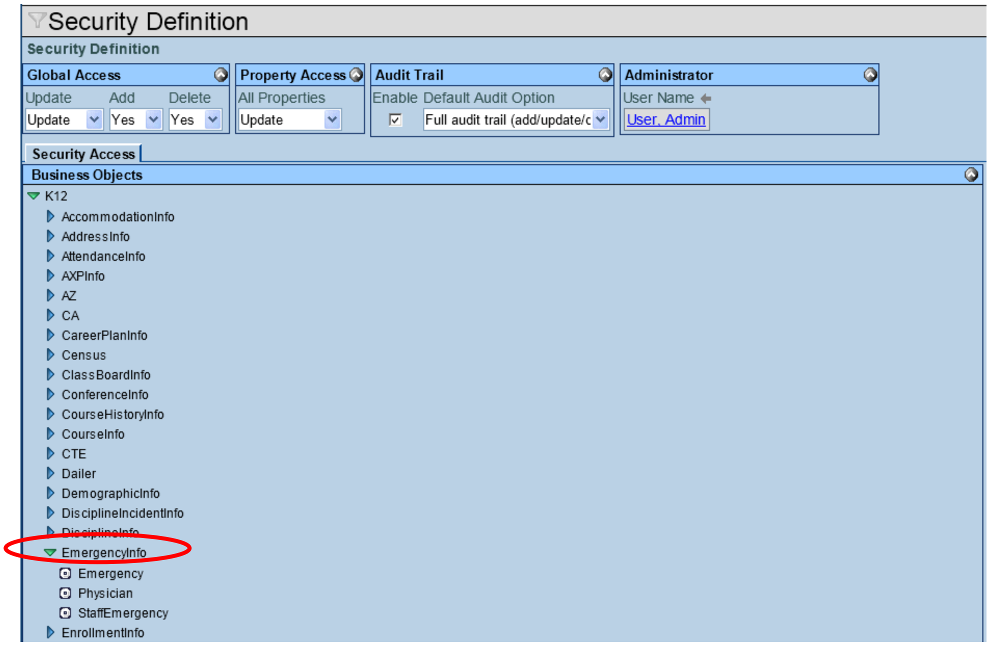
Security Access

Business Objects

K12
- AccommodationInfo
- AddressInfo
- AttendanceInfo
- AXPInfo
- AZ
- CA
- CareerPlanInfo
- Census
- ClassBoardInfo
- ConferenceInfo
- CourseHistoryInfo
- CourseInfo
- CTE
- Dailer
- DemographicInfo
- DisciplineIncidentInfo
- DisciplineInfo
- EmergencyInfo
- EnrollmentInfo

Figure 2.6 – Security Definition Screen, K12 Namespace Expanded

3. Click a secondary namespace to list the business objects in the namespace.



Security Definition

Security Definition

Global Access			Property Access	Audit Trail		Administrator
Update	Add	Delete	All Properties	Enable	Default Audit Option	User Name
Update	Yes	Yes	Update	☑	Full audit trail (add/update/c	User, Admin

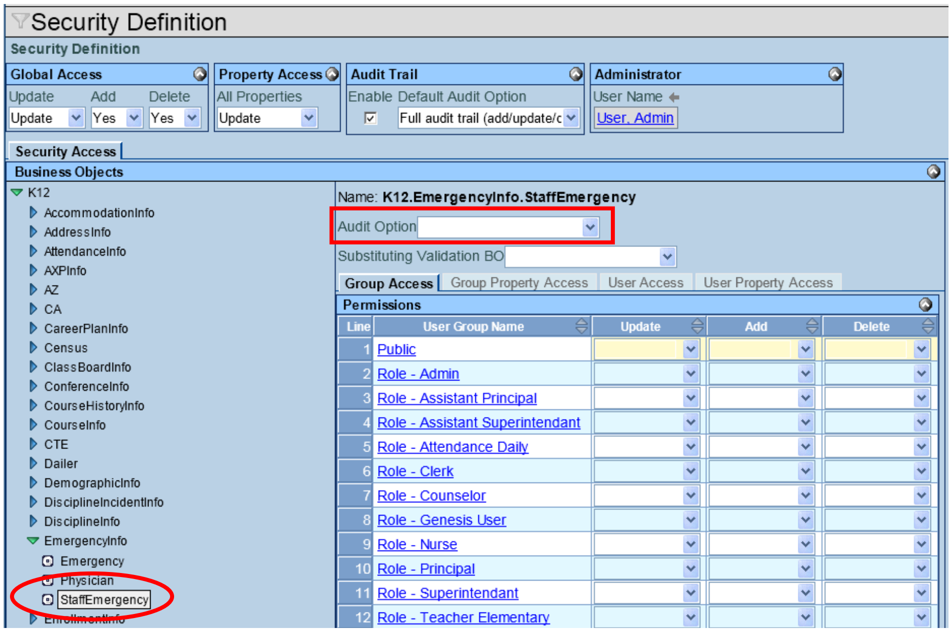
Security Access

Business Objects

K12
- AccommodationInfo
- AddressInfo
- AttendanceInfo
- AXPInfo
- AZ
- CA
- CareerPlanInfo
- Census
- ClassBoardInfo
- ConferenceInfo
- CourseHistoryInfo
- CourseInfo
- CTE
- Dailer
- DemographicInfo
- DisciplineIncidentInfo
- DisciplineInfo
- EmergencyInfo
  - Emergency
  - Physician
  - StaffEmergency
- EnrollmentInfo

Figure 2.7 – Security Definition Screen, Secondary Namespace Expanded

4. Click the business object to be adjusted.



Global Access: Update: Update; Add: Yes; Delete: Yes

Property Access: All Properties: Update

Audit Trail: Enable ☑; Default Audit Option: Full audit trail (add/update/c

Administrator: User Name: User, Admin

Business Objects: K12 – AccommodationInfo, AddressInfo, AttendanceInfo, AXPInfo, AZ, CA, CareerPlanInfo, Census, ClassBoardInfo, ConferenceInfo, CourseHistoryInfo, CourseInfo, CTE, Dailer, DemographicInfo, DisciplineIncidentInfo, DisciplineInfo, EmergencyInfo (Emergency, Physician, StaffEmergency), EnrollmentInfo

Name: K12.EmergencyInfo.StaffEmergency

Audit Option

Substituting Validation BO

Line	User Group Name	Update	Add	Delete
1	Public			
2	Role - Admin			
3	Role - Assistant Principal			
4	Role - Assistant Superintendant			
5	Role - Attendance Daily			
6	Role - Clerk			
7	Role - Counselor			
8	Role - Genesis User			
9	Role - Nurse			
10	Role - Principal			
11	Role - Superintendant			
12	Role - Teacher Elementary			

Figure 2.8 – Security Definition Screen, Business Object Selected

5. Select the **Audit Option** to be used for the business object. It can be set to a **Full audit trail**, which logs all additions, updates, and deletions; **Audit trail of changes only**, which logs updates to existing data; or **No audit trail**, which does not log anything.
6. Click the **Save** button at the top of the screen.

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.

To create a business object group and specify its audit option:

1. Go to **Synergy SIS > System > Security > Business Object Audit Trail Group**.
2. Click the **Add** button at the top of the screen.

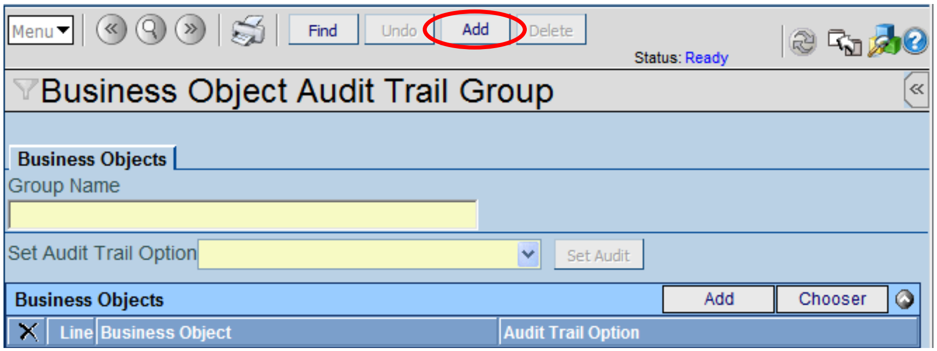
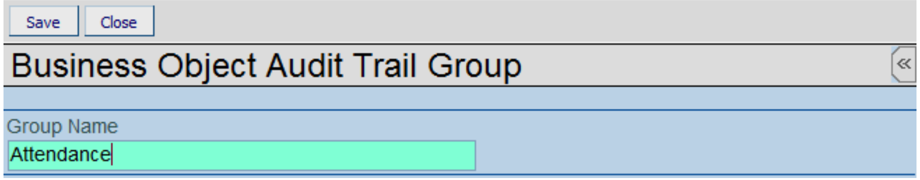


Figure 2.9 – Business Object Audit Trail Group Screen

3. Enter a name for the group in the **Group Name** field, and click the **Save** button at the top of the screen.

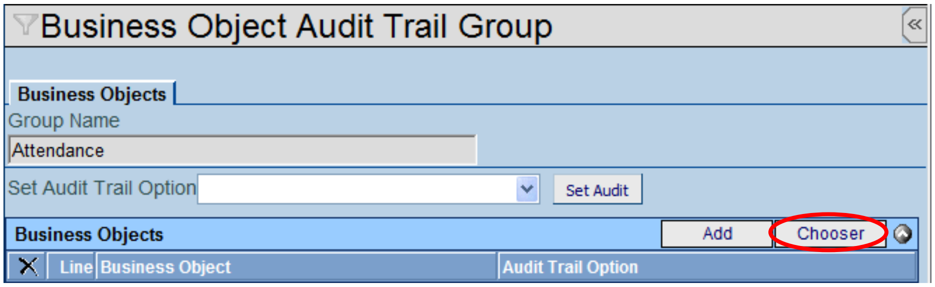


Group Name: Attendance

Figure 2.10 – Adding a Business Object Audit Trail Group

4. Find and select objects for the group using the **Chooser** button, as described in steps 5-8 or the **Add** button, as described in steps 9-12. With the **Add** button, you can add objects one at a time only.

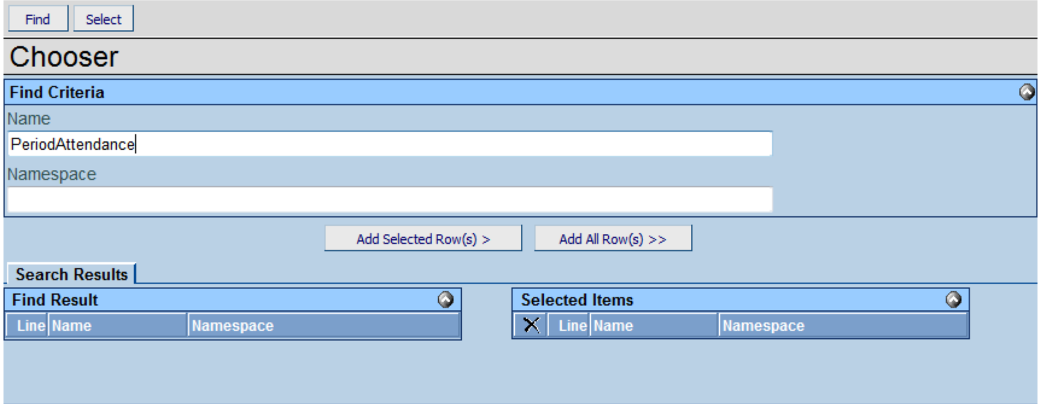
5. In the **Business Objects** grid, click the **Chooser** button.



Group Name: Attendance

Figure 2.11 – Business Object Audit Trail Group Screen, Chooser Button

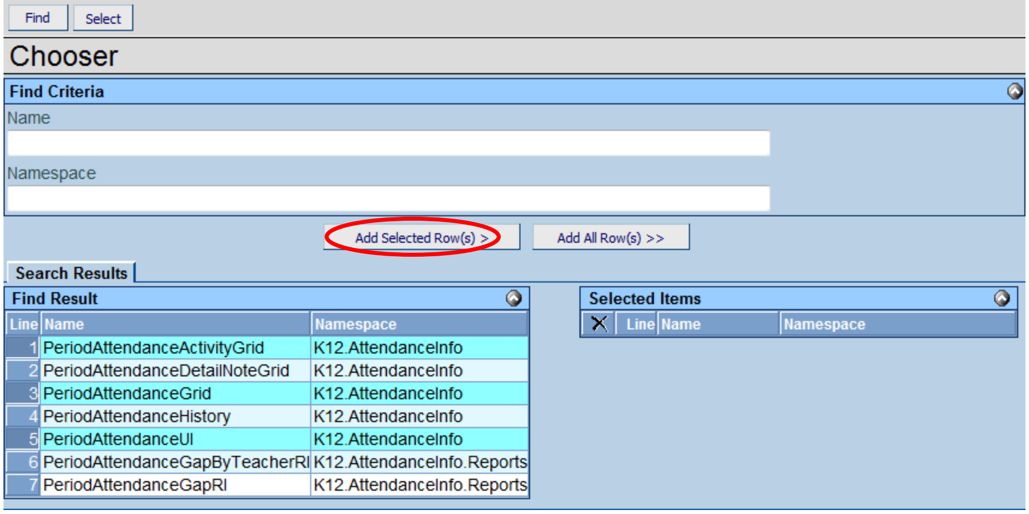
6. In the **Chooser** screen, enter all or part of a business object **Name** or a **Namespace** to search for the desired objects, and click the **Find** button.



Name: PeriodAttendance

Figure 2.12 – Chooser Screen

7. In the **Find Result** grid, click objects or Ctrl-click multiple objects to add to the group, and click the **Add Selected Row(s)** button.



Chooser

Find Criteria

Name

Namespace

Find Result

Line	Name	Namespace
1	PeriodAttendanceActivityGrid	K12.AttendanceInfo
2	PeriodAttendanceDetailNoteGrid	K12.AttendanceInfo
3	PeriodAttendanceGrid	K12.AttendanceInfo
4	PeriodAttendanceHistory	K12.AttendanceInfo
5	PeriodAttendanceUI	K12.AttendanceInfo
6	PeriodAttendanceGapByTeacherRI	K12.AttendanceInfo.Reports
7	PeriodAttendanceGapRI	K12.AttendanceInfo.Reports

Selected Items

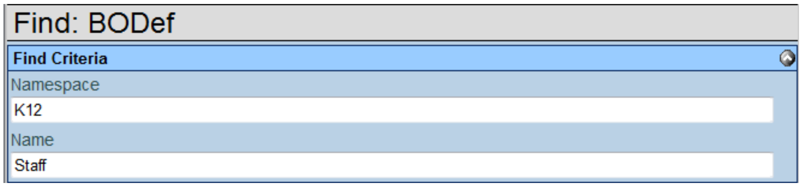
✕	Line	Name	Namespace

Figure 2.13 – Chooser Screen, Selecting Objects

8. Click the **Select** button at the top of the screen, and skip to step 13 if you have selected all desired objects.

9. In the **Business Objects** grid, click the **Add** button.

10. In the **Find: BODef** screen, enter all, part, or none of the **Namespace** and **Name** of the desired object.



Find: BODef

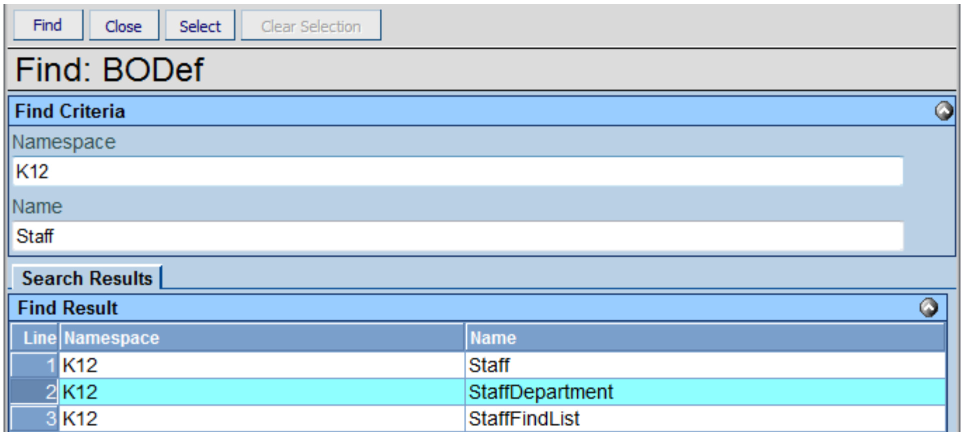
Find Criteria

Namespace: K12

Name: Staff

Figure 2.14 – Find: BODef Screen

11. In the **Find Result** grid, click the desired object.



Find: BODef

Find Criteria

Namespace: K12

Name: Staff

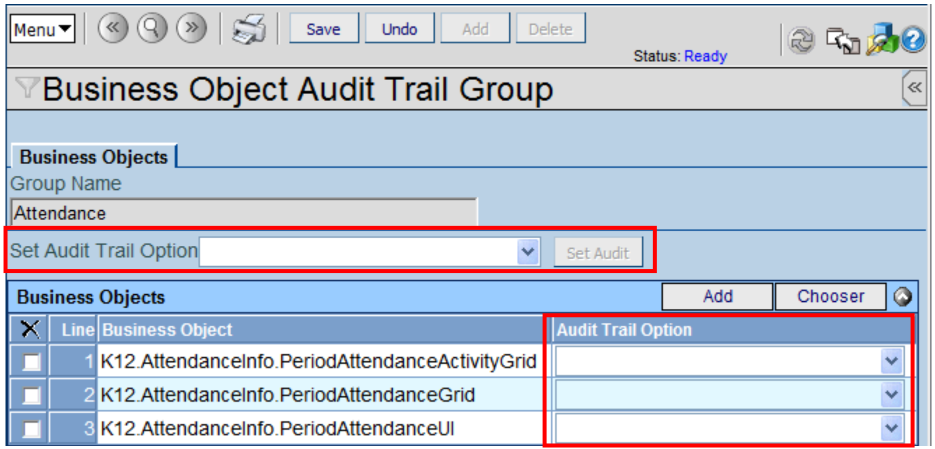
Find Result

Line	Namespace	Name
1	K12	Staff
2	K12	StaffDepartment
3	K12	StaffFindList

Figure 2.15 – Find: BODef Screen, Selecting an Object

12. Click the **Select** button at the top of the screen.

13. Optionally, use the **Set Audit Trail Option** field to set the option for all business objects in the group, and click the **Set Audit** button. This sets the values, for all objects, in the **Audit Trail Option** column.



Business Object Audit Trail Group

Group Name: Attendance

Set Audit Trail Option:

Business Objects

☒	Line	Business Object	Audit Trail Option
□	1	K12.AttendanceInfo.PeriodAttendanceActivityGrid	
□	2	K12.AttendanceInfo.PeriodAttendanceGrid	
□	3	K12.AttendanceInfo.PeriodAttendanceUI	

Figure 2.16 – Business Object Audit Trail Group Screen, Selecting Options

14. In the **Audit Trail Option** column, adjust the option for individual objects as desired.

15. Click the **Save** button at the top of the screen.

SPECIAL AUDIT QUERIES

While most screens show an audit trail, some areas are inaccessible to the audit trail report, as the audit trail report shows the changes for the primary objects in the screen and not the objects in a grid. For example, the audit trail for a student's schedule shows information about the student but not the schedule.

Although these logs are not displayed in the Audit Detail Report, the changes are logged and can be accessed via a custom query. To access some commonly used audit trails using the **Query** screen, enter the queries listed below. For more about queries, see the *Synergy SIS – Query & Reporting Guide*.

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 the SIREN software can also use the MS SQL query language. Below is a sample audit report using a Microsoft SQL query. For more information about SIREN reports, please 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 Three:
SCREEN-LEVEL SECURITY

This chapter covers:

- ► How to setup the system-wide access to views
- ► How to customize screen access by user group
- ► How to customize screen access by individual user

The screen-level security determines what screens and reports are shown in the Navigation Tree, or PAD Tree, for each user, and what data can be updated.

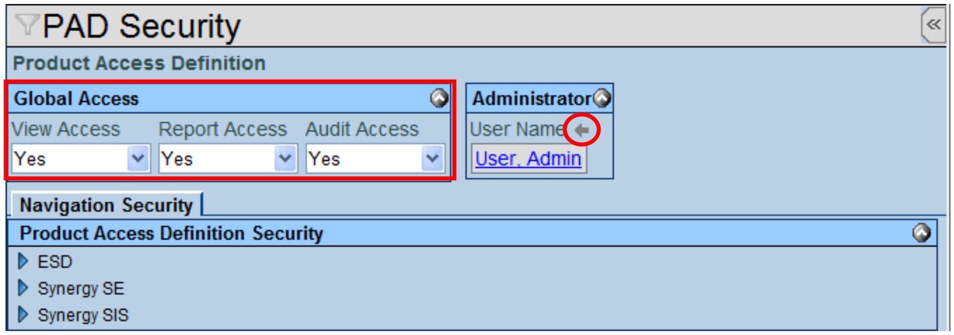
SETTING SYSTEM-WIDE ACCESS RIGHTS

The first step in configuring the rights to each screen is to set the default, or Global Access, rights to be used throughout the system. There are two approaches that can be taken. The first approach is to give everyone access to everything, and then specify by user group what screens that group cannot access or update. The second approach is to forbid access to everyone, and then specify what screens each user group can access or update.

> **Caution:** If selecting the second approach and forbidding access to everyone initially, be sure to set the Admin user or the user group to which the Admin user belongs with access to everything. Otherwise, even the Admin user could be completely locked out of the system!!

To set the system-wide access and update rights:

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



PAD Security

Product Access Definition

Global Access

View Access: Yes
Report Access: Yes
Audit Access: Yes

Administrator

User Name: User, Admin

Navigation Security

Product Access Definition Security

Figure 3.1 – PAD Security Screen

2. In the **View Access** list, click one of the following:
   - **Yes** to grant everyone the ability to update data in all screens
   - **View Only** to give everyone the ability to see but not update the data in the screens
   - **No** to deny everyone access
3. In the **Report Access** list, click **Yes** to grant everyone access to all reports in the system, or **No** to deny everyone access to all reports.
4. In the **Audit Access** list, click **Yes** to grant everyone access to the Audit Detail Report for each screen, or **No** to deny everyone access to the Audit Detail Reports.
5. To select a different **User Name** as the main administrator account:
   - Click the gray arrow in the **Administrator** section. This is the same as the Administrator set in the **Security Definition** screen, and this information can be changed in either screen.

- In the **Find: Rev User** screen, enter all or part of the **Last Name** and/or **First Name** of the user, and click the **Find** button.

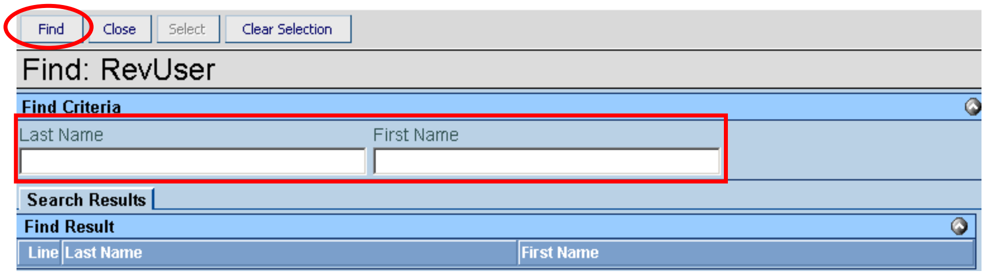
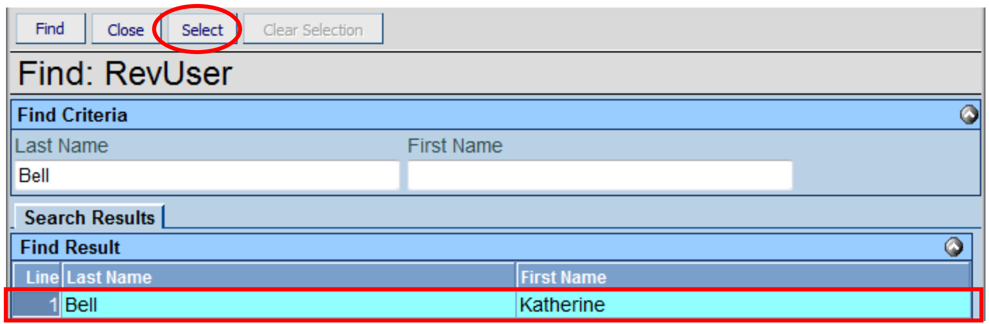


Figure 3.2 – Find: RevUser Screen

- In the **Find Result** grid, click the user, and click the **Select** button.



Last Name: Bell
First Name:

Line	Last Name	First Name
1	Bell	Katherine

Figure 3.3 – Find RevUser Screen, Selecting

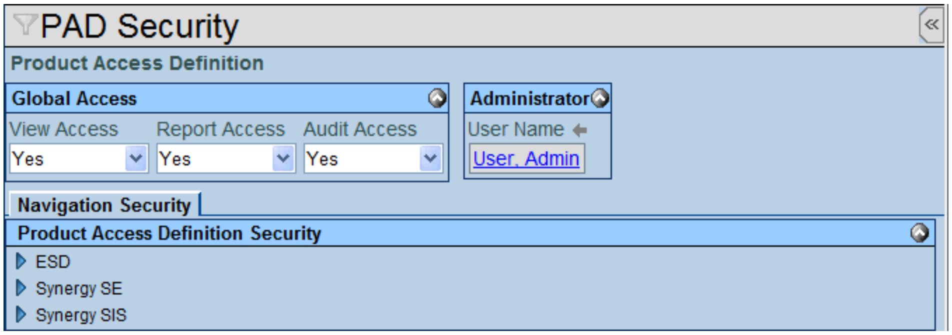
6. Click the **Save** button at the top of the screen.

Setting User Group Access

After the overall access has been set, the access can further be customized by granting or forbidding access or update rights to user groups. An outline of how user groups can be structured is in Chapter One. Setting access by user group is preferable over setting access by individual user, as it is easier to maintain. If there are exceptions for certain users, this can be set up as described in the next section.

Access can be customized at any level from the module, screen, or report. If a module's access is customized, the customization also applies to modules, screens, and reports in that module. To define access for user groups:

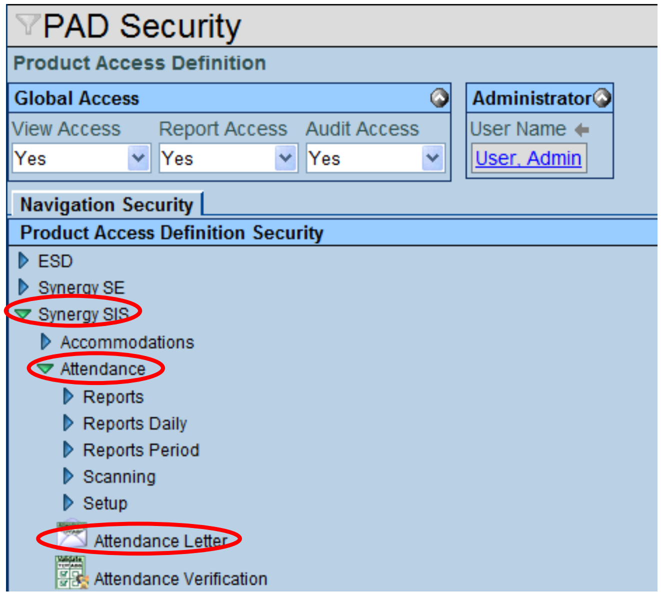
1. Go to **Synergy SIS > System > Security > PAD Security**.



View Access: Yes
Report Access: Yes
Audit Access: Yes
User Name: User, Admin

Figure 3.4 – PAD Security Screen

2. To expand a module, click its name. Continue clicking until the target module, screen, or report interface is displayed, and click the target.



PAD Security

Product Access Definition

Global Access

View Access	Report Access	Audit Access
Yes	Yes	Yes

Administrator

User Name: User, Admin

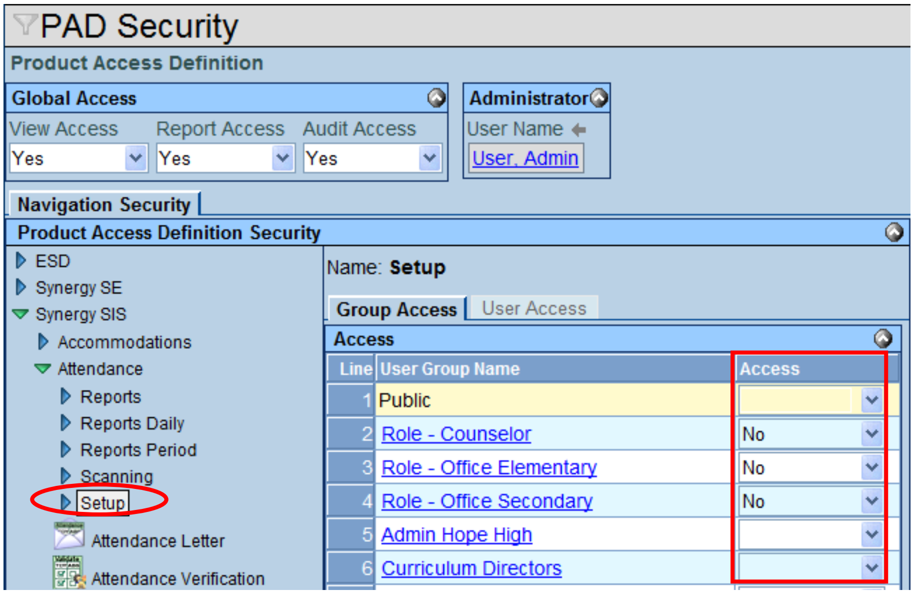
Navigation Security

Product Access Definition Security

- ESD
- Synergy SE
- Synergy SIS
  - Accommodations
  - Attendance
    - Reports
    - Reports Daily
    - Reports Period
    - Scanning
    - Setup
  - Attendance Letter
  - Attendance Verification

Figure 3.5 – PAD Security Screen, Expanded List

3. To set the access for an entire module, including the modules, screens, or reports within it, click the name of the module.



PAD Security

Product Access Definition

Global Access

View Access	Report Access	Audit Access
Yes	Yes	Yes

Administrator

User Name: User, Admin

Navigation Security

Product Access Definition Security

- ESD
- Synergy SE
- Synergy SIS
  - Accommodations
  - Attendance
    - Reports
    - Reports Daily
    - Reports Period
    - Scanning
    - Setup
  - Attendance Letter
  - Attendance Verification

Name: **Setup**

Group Access | User Access

Access

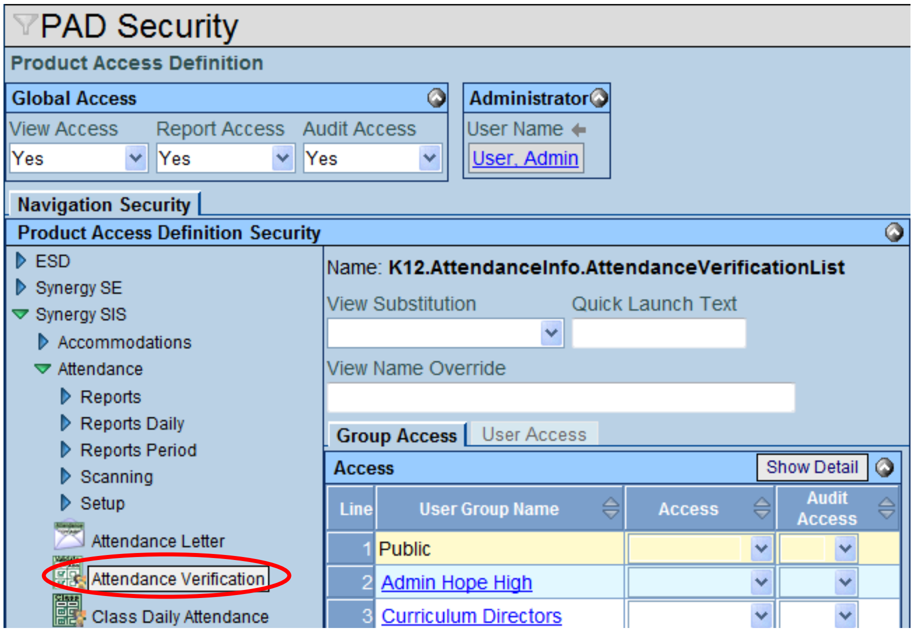
Line	User Group Name	Access
1	Public	
2	Role - Counselor	No
3	Role - Office Elementary	No
4	Role - Office Secondary	No
5	Admin Hope High	
6	Curriculum Directors	

Figure 3.6 – PAD Security Screen, Setting Module Security

4. Select the **Access** for each group. **Yes** grants update rights for the group, **View Only** gives rights to see the data, and **No** denies access. The **Public** group is the default access for all groups. If **Public** is set to **No** for any module or screen, be sure to set **Yes** for the Admin user group or the Admin User, or everyone could be locked out of the module.

5. Click the **Save** button at the top of the screen.

6. To set security for a screen or report, click the screen or report.



PAD Security

Product Access Definition

Global Access

View Access	Report Access	Audit Access
Yes	Yes	Yes

Administrator

User Name: User, Admin

Product Access Definition Security

Name: **K12.AttendanceInfo.AttendanceVerificationList**

View Substitution

Quick Launch Text

View Name Override

Group Access | User Access

Access

Line	User Group Name	Access	Audit Access
1	Public		
2	Admin Hope High		
3	Curriculum Directors		

Figure 3.7 – PAD Security Screen, Setting Screen or Report Security

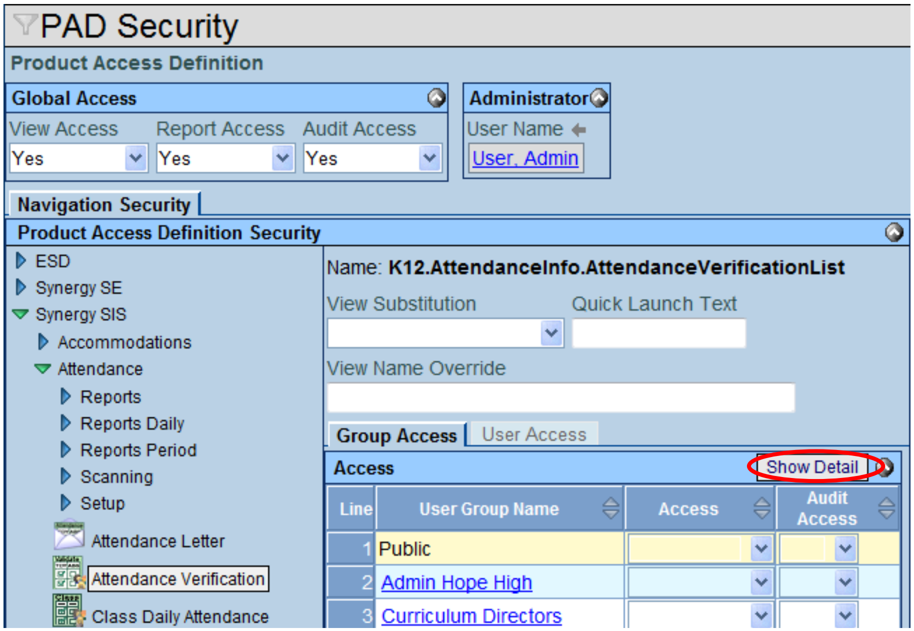
7. Select the **Access** for each group. **Yes** grants update rights for the group, **View Only** gives rights to see the data, and **No** denies access. The **Public** group is the default access for all groups. If **Public** is set to **No** for any screen, be sure to set **Yes** for the Admin user group or the Admin User, or everyone could be locked out of the screen.

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

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

10. Click the **Save** button at the top of the screen.

11. To set the access for the **Menu** button at the top of the screen, any tabs on the screen, and any buttons on the screen, click the **Show Detail** button.



View Access: Yes
Report Access: Yes
Audit Access: Yes
User Name: User, Admin

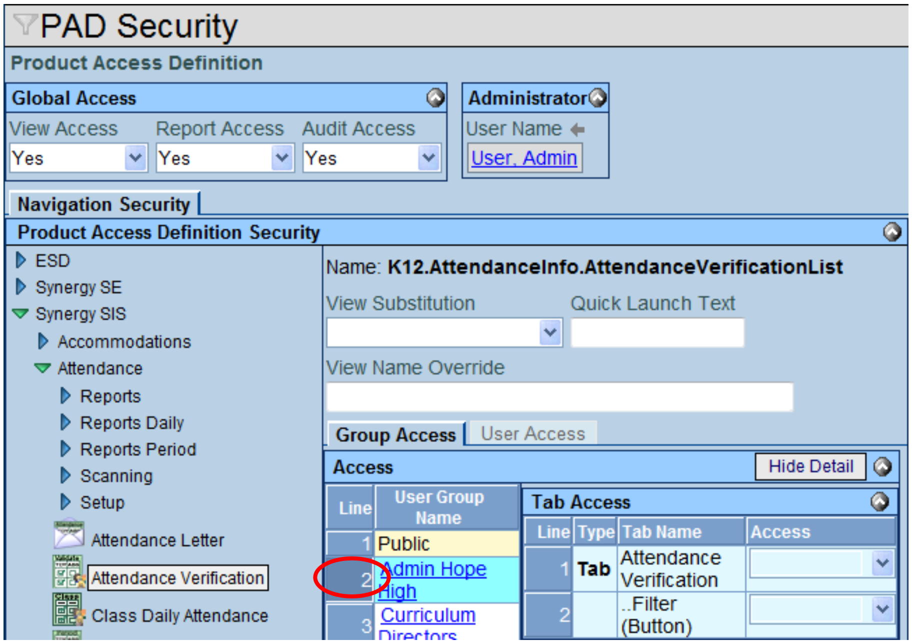
Name: **K12.AttendanceInfo.AttendanceVerificationList**

View Substitution
Quick Launch Text
View Name Override

Line	User Group Name	Access	Audit Access
1	Public		
2	Admin Hope High		
3	Curriculum Directors		

Figure 3.8 – PAD Security Screen, Group Access Detail

12. To set the access to an object for a user group, click the **Line** number of the user group.



View Access: Yes
Report Access: Yes
Audit Access: Yes
User Name: User, Admin

Name: **K12.AttendanceInfo.AttendanceVerificationList**

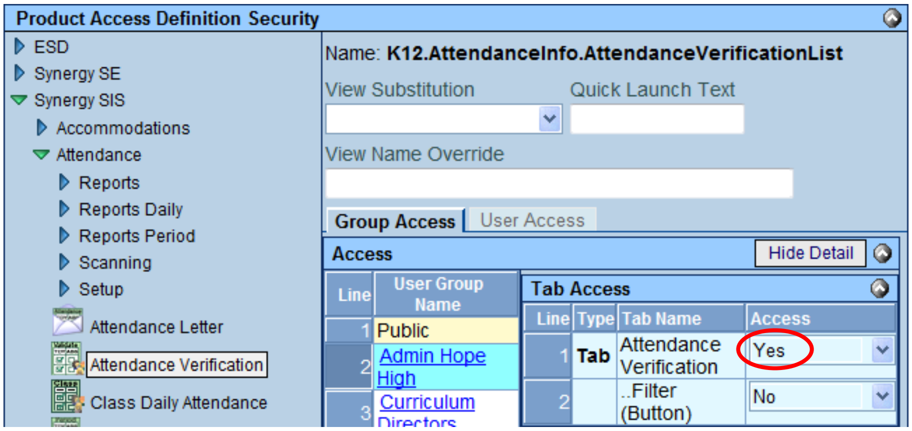
View Substitution
Quick Launch Text
View Name Override

Line	User Group Name
1	Public
2	Admin Hope High
3	Curriculum Directors

Line	Type	Tab Name	Access
1	Tab	Attendance Verification	
2		..Filter (Button)	

Figure 3.9 – PAD Security Screen, Group Access Detail

13. Select the **Access** rights for the group.



Product Access Definition Security

Name: **K12.AttendanceInfo.AttendanceVerificationList**

View Substitution

Quick Launch Text

View Name Override

Line	User Group Name
1	Public
2	Admin Hope High
3	Curriculum Directors

Tab Access

Line	Type	Tab Name	Access
1	Tab	Attendance Verification	Yes
2		..Filter (Button)	No

Figure 3.10 – PAD Security Screen, Group Access Detail

14. Click the **Save** button at the top of the screen.

15. To close the detail screen, click the **Hide Detail** button.

Caution: If **Public** is to be set to **No** for any module or screen, be sure to set **Yes** for the Admin user group or the Admin User before setting the **Public** rights. Take particular care with the **System** and **Security** modules. If these modules are set to **No** for **Public** before setting the Admin user with **Yes** access to these modules, everyone could be locked out of making changes to security.

Also, take care in locking the entire **System** module. The **Announcements** module in that module contains the **Home Screen** screen and the **Announcement Tree** screen. If users are prevented from accessing these screens, they will not see the home page of Synergy SIS and will not see any system announcements.

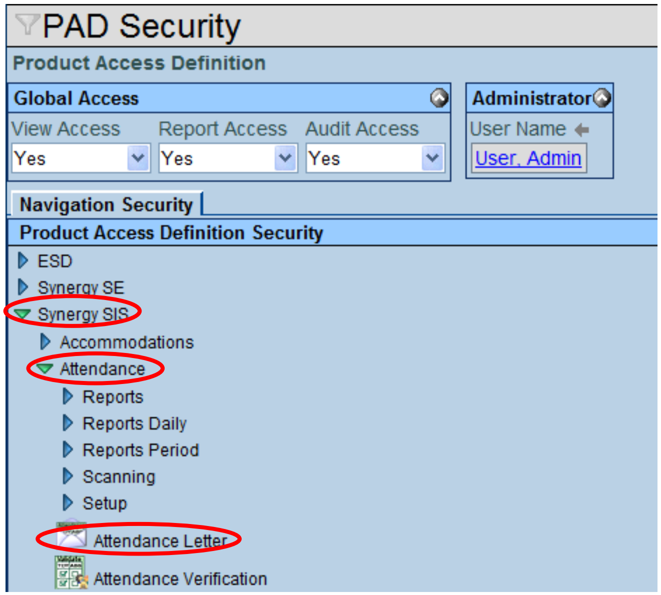
Other screens to be aware of include

- **Synergy SIS > System > Job Queue > Job Queue Viewer**, which enables users to reprint reports
- **Synergy SIS > Grade Book > GBSecurity**, which controls access to the buttons in Grade Book
- **Synergy SIS > Non PAD**, which controls several areas across the system.

SETTING USER ACCESS

Occasionally, it may be necessary to grant access rights to a specific user, apart from user groups. Access can be customized at any level from the module to the screen or report, just as with user group access. If a module's access is customized, the customization also controls any modules, screens, and reports in that module. To customize access for a user:

1. Go to **Synergy SIS > System > Security > PAD Security**.
2. To expand a module, click its name. Continue clicking until the target module, screen, or report interface is displayed, and click the target.



PAD Security

Product Access Definition

Global Access

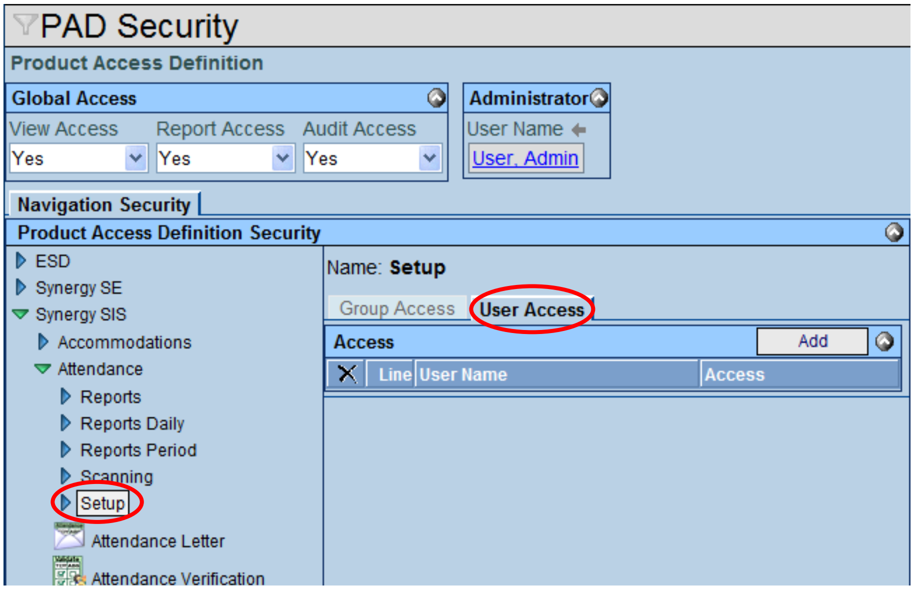
View Access: Yes
Report Access: Yes
Audit Access: Yes

Administrator

User Name: User, Admin

Figure 3.11 – PAD Security Screen, Expanded List

3. To set individual access for an entire module, including the modules, screens, or reports within it, click the name of the module, and click the **User Access** tab.



PAD Security

Product Access Definition

Global Access

View Access: Yes
Report Access: Yes
Audit Access: Yes

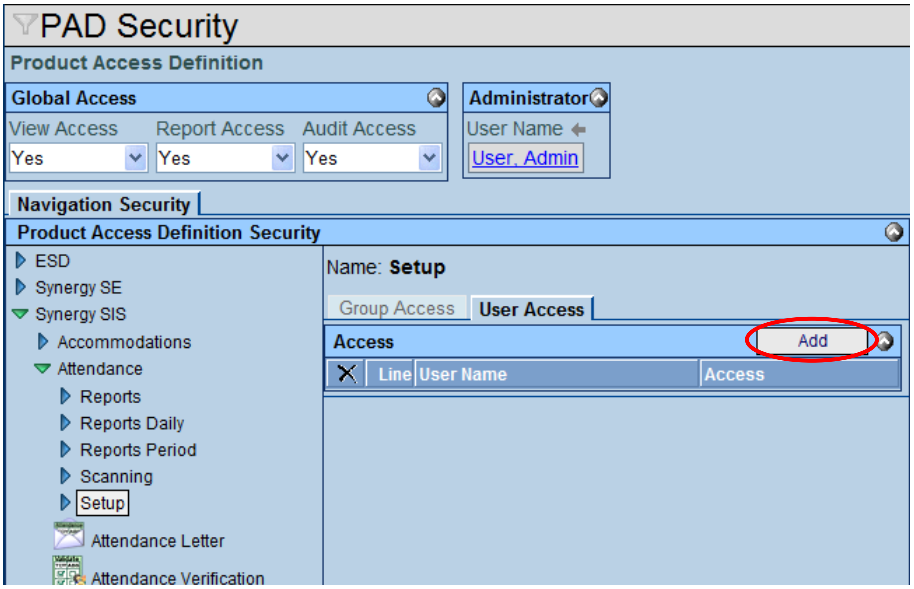
Administrator

User Name: User, Admin

Name: **Setup**

Figure 3.12 – PAD Security Screen, Setting Module Security

4. To select the user to set access for, click the **Add** button.



View Access	Report Access	Audit Access
Yes	Yes	Yes

User Name: User, Admin

Name: Setup

Line	User Name	Access

Figure 3.13 – PAD Security Screen, User Access Tab

5. In the **Find: Rev User** screen, enter all or part of the **Last Name** and/or **First Name** of the user, and click the **Find** button.

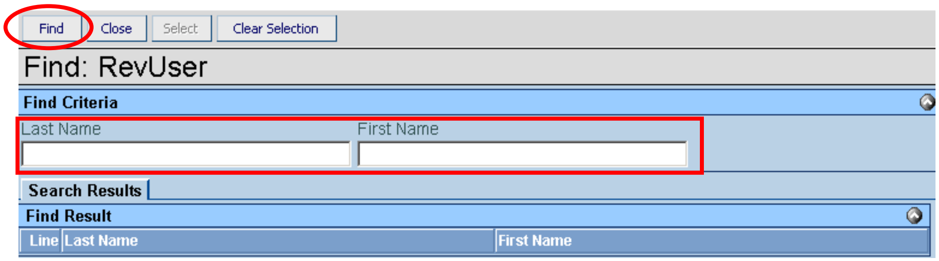
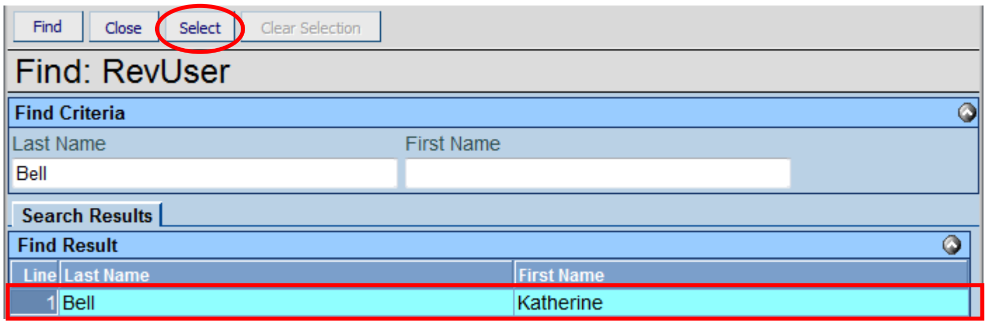


Figure 3.14 – Find: RevUser Screen

6. In the **Find Result** grid, click the user, and click the **Select** button.



Last Name: Bell

First Name:

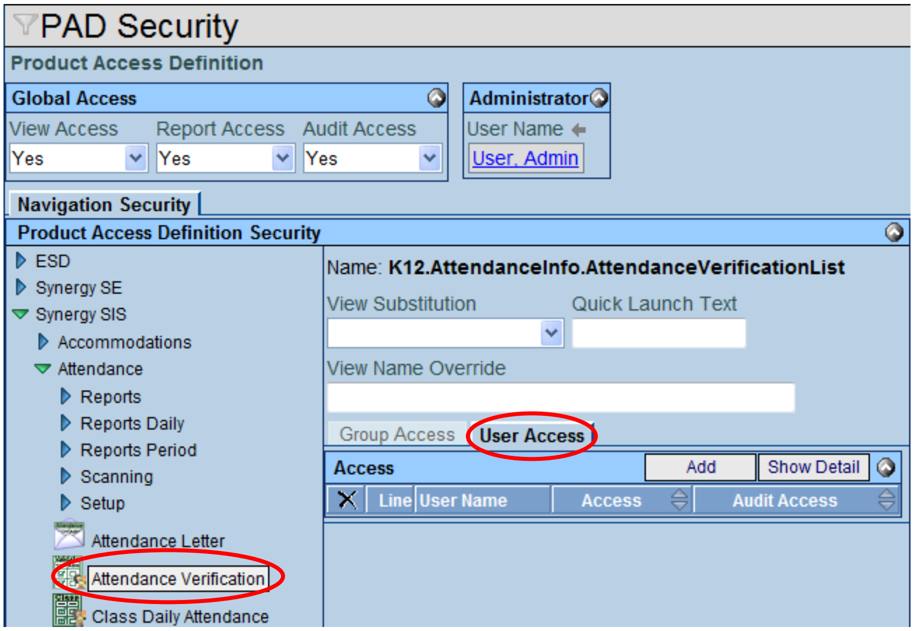
Line	Last Name	First Name
1	Bell	Katherine

Figure 3.15 – Find RevUser Screen, Selecting

7. Select the **Access** for the module. **Yes** grants update rights, **View Only** gives read-only access, and **No** denies access.

8. Click the **Save** button at the top of the screen.

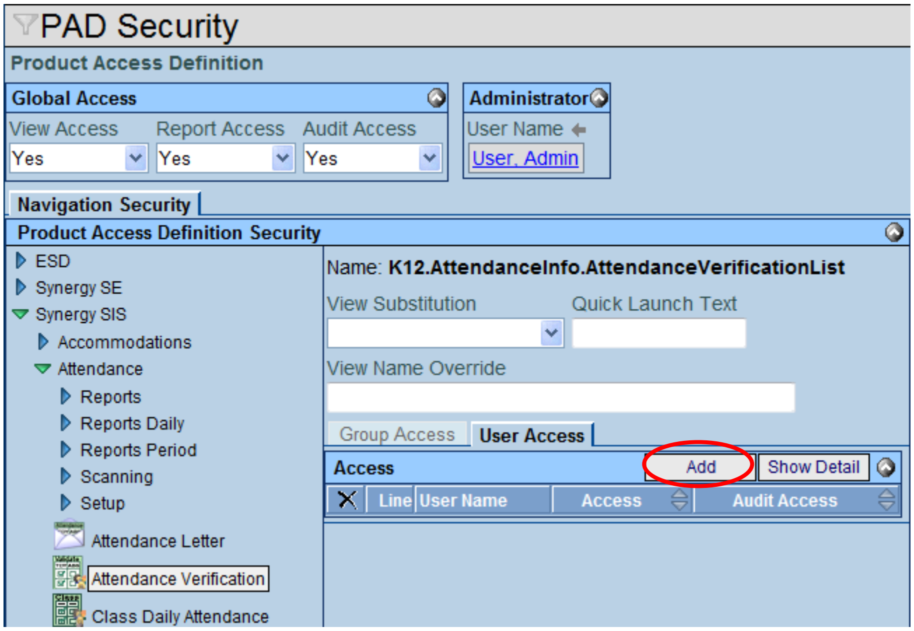
9. To set security on a screen or report, click the screen or report, and click the **User Access** tab.



View Access: Yes
Report Access: Yes
Audit Access: Yes
User Name: User, Admin
Name: **K12.AttendanceInfo.AttendanceVerificationList**

Figure 3.16 – PAD Security Screen, Setting Screen or Report Security

10. To select the user to set access for, click the **Add** button.



View Access: Yes
Report Access: Yes
Audit Access: Yes
User Name: User, Admin
Name: **K12.AttendanceInfo.AttendanceVerificationList**

Figure 3.17 – PAD Security Screen, Setting Screen Access, User Access Tab

11. In the **Find: Rev User** screen, enter all or part of the **Last Name** and/or **First Name** of the user, and click the **Find** button.

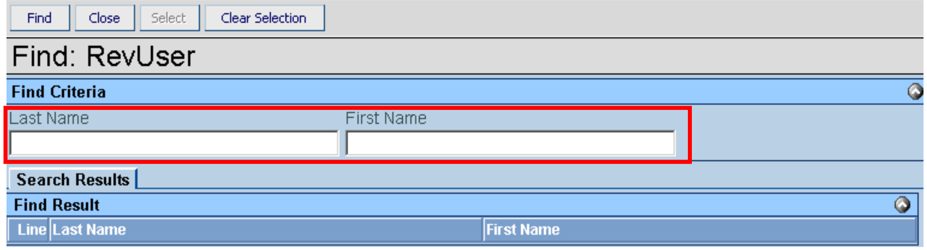
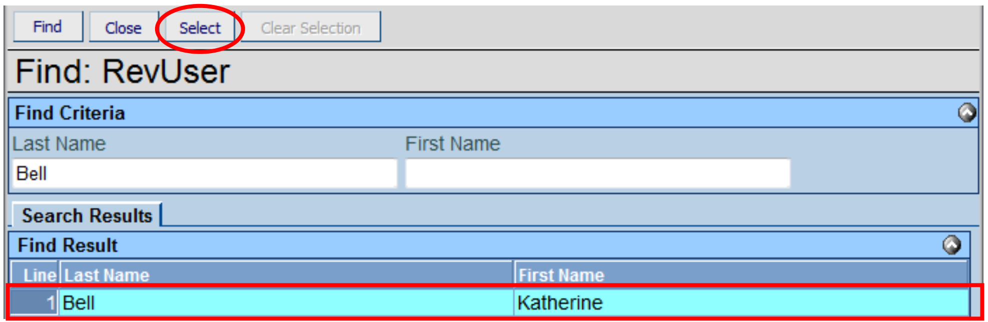


Figure 3.18 – Find: RevUser Screen

12. In the **Find Result** grid, click the user, and click the **Select** button.

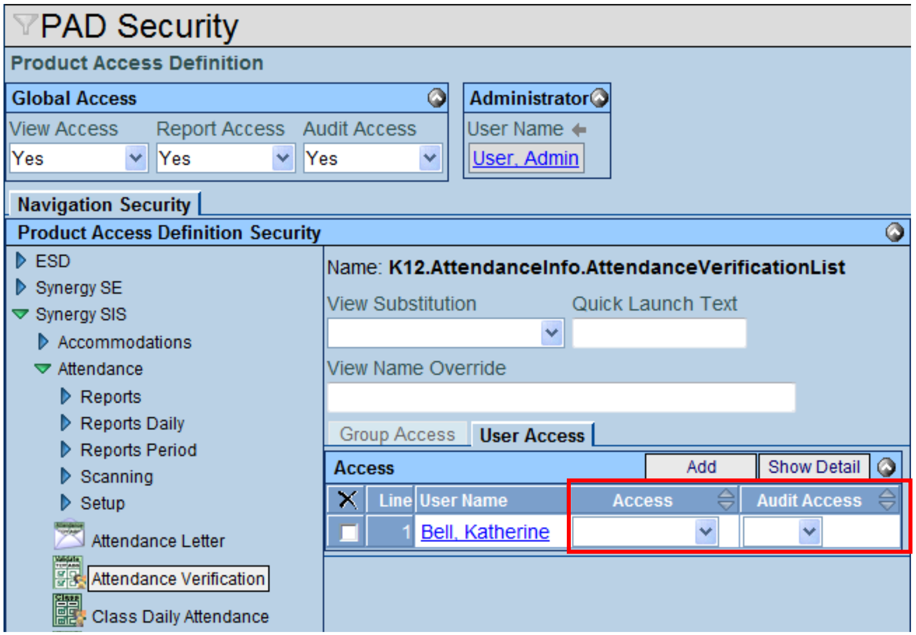


Last Name: Bell
First Name:

Line	Last Name	First Name
1	Bell	Katherine

Figure 3.19 – Find: RevUser Screen, Selecting

13. Select the **Access** and **Audit Access** (access to the Audit Detail Report) for the user.



View Access: Yes
Report Access: Yes
Audit Access: Yes
User Name: User, Admin

Name: **K12.AttendanceInfo.AttendanceVerificationList**
View Substitution:
Quick Launch Text:
View Name Override:

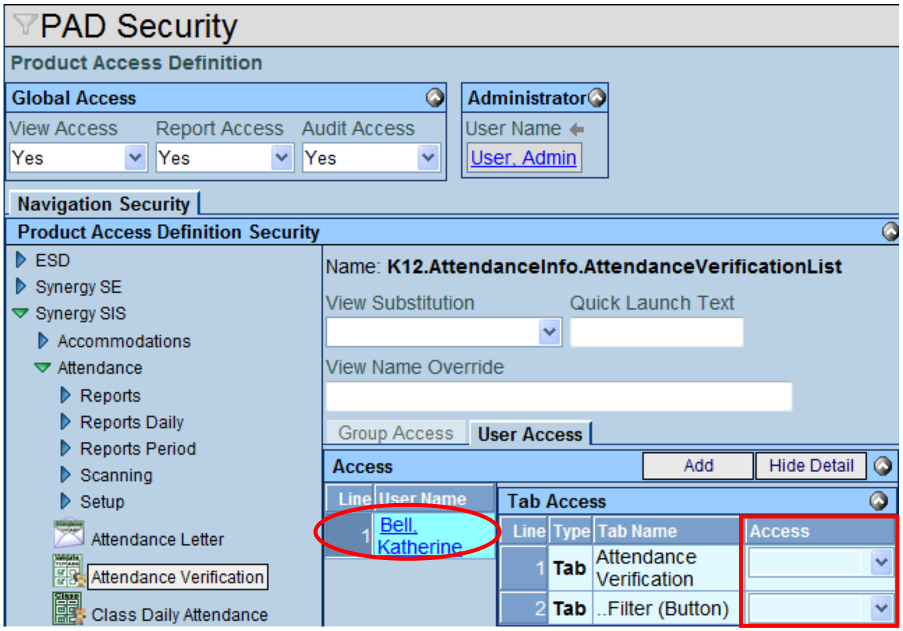
	Line	User Name	Access	Audit Access
□	1	Bell, Katherine		

Figure 3.20 – PAD Security Screen, Setting Screen or Report Security

14. Click the **Save** button at the top of the screen.

15. To set the access for the **Menu** button at the top of the screen, any tabs on the screen, and any buttons on the screen, click the **Show Detail** button.

16. Click the user, and select an **Access** option for each object.



View Access	Report Access	Audit Access
Yes	Yes	Yes

User Name: User, Admin

Name: K12.AttendanceInfo.AttendanceVerificationList

Line	User Name
1	Bell, Katherine

Line	Type	Tab Name	Access
1	Tab	Attendance Verification	
2	Tab	..Filter (Button)	

Figure 3.21 – PAD Security Screen, Screen Access, User Access Tab, Detail

17. Click the **Save** button at the top of the screen.

18. To close the detail screen, click the **Hide Detail** button.

Chapter Four:
FIELD-LEVEL SECURITY

This chapter covers:

- ► How to setup the system-wide field-level rights
- ► How to customize field-level rights by user group
- ► How to customize field-level rights by individual user

Field-level security defines whether users can view and update business objects and the properties, or fields, of business objects.

SETTING SYSTEM-WIDE FIELD-LEVEL RIGHTS

The rights in the **Security Definition** screen set whether a user can change the data in a screen or only view the data. These rights also specify whether the user can add and delete records. These rights are set at the business object level instead of the screen level. Each screen may contain one or more business objects, but business objects may be used in multiple screens. For example, if the update rights for the Student business object are customized, this impacts every screen that uses student information.

To see which business objects control each part of a screen, see the Security chapter in the administrator guide that explains the setup of that screen. For example, the business objects that control the **Student** screen are described in the *Synergy SIS – Student Information Administrator Guide*.

In addition, rights can be configured at the Properties level. The properties of each business object are generally the fields shown on the screen. An example of a property is the **City** field on the **Student** screen. In addition, many business objects contain hidden properties that link data but are not displayed.

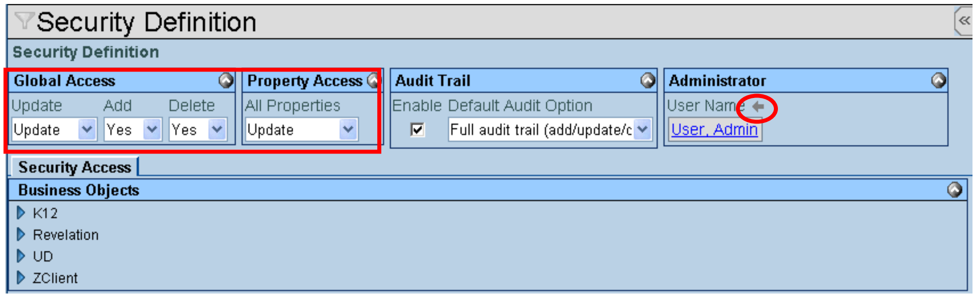
Caution: These rights work in conjunction with the rights assigned in **PAD Security** for the screen. If the screen in **PAD Security** is set to view only for the given user group or user, the rights in **Security Definition** do not override this setting and change a field to update rights. However, if the screen in **PAD Security** is set to update, the rights in **Security Definition** can override this to set the properties or business objects to view only. Therefore, to set a group to update one particular property, first give the group update access to the screen, then all properties except that one to view only.

The first step in configuring the update rights is to set the default, or Global Access, rights to be used throughout the system. Two approaches can be taken. The first is to give everyone update rights to everything, and then specify by user group what business objects that group cannot update. The second approach is to give everyone view only rights, and then specify what business objects each user group can update.

Caution: If selecting the second approach and preventing everyone from updating the data initially, be sure to set the Admin user or the user group to which the Admin user belongs with update access to everything before setting the Global Access rights. Otherwise, even the Admin user could be completely locked out of the system.

To set the system-wide update, add and delete rights:

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



Security Definition

Security Definition

Global Access

Update	Add	Delete
Update	Yes	Yes

Property Access

All Properties: Update

Audit Trail

Enable	Default Audit Option
☑	Full audit trail (add/update/c

Administrator

User Name: User, Admin

Security Access

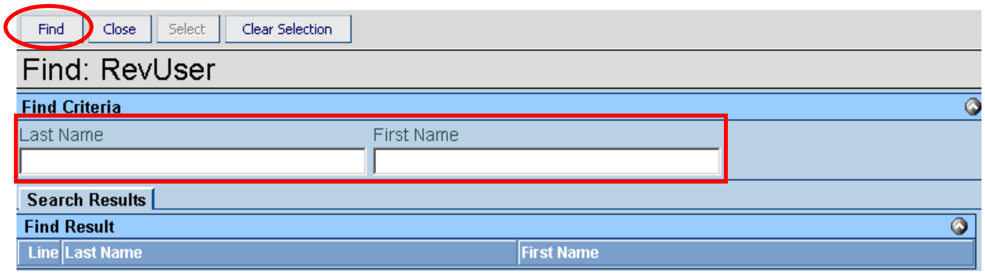
Business Objects

- K12
- Revelation
- UD
- ZClient

Figure 4.1 – Security Definition Screen

2. Select **Update**, **View**, or **None** in the **Update** list to set the overall update rights for everyone. **None** should probably be used only for setting individual business object rights and not at the Global Access level.
3. In the **Add** list, select **Yes** to allow everyone to add records, or **No** to prevent users from adding records.
4. In the **Delete** list, select **Yes** to allow everyone to delete records, or **No** to prevent users from deleting records.
5. Select **Update**, **View**, or **None** in the **All Properties** list to set the overall update rights for everyone for all the properties. **None** should probably be used only for setting individual property rights and not at the Global Access level.
6. **Enable** logging, if desired, and select the **Default Audit Option** to be used for all business objects. It can be set to a **Full audit trail**, which logs all additions, updates, and deletions; **Audit trail of changes only**, which logs updates to existing data; or **No audit trail**, which does not log anything.
7. Designate an **Administrator** user.

   - Click the gray arrow in the **Administrator** section. This is the same as the Administrator set in the **Security Definition** screen, and this information can be changed in either screen.
   - In the **Find: Rev User** screen, enter all or part of the **Last Name** and/or **First Name** of the user, and click the **Find** button.



Find: RevUser

Find Criteria

Last Name

First Name

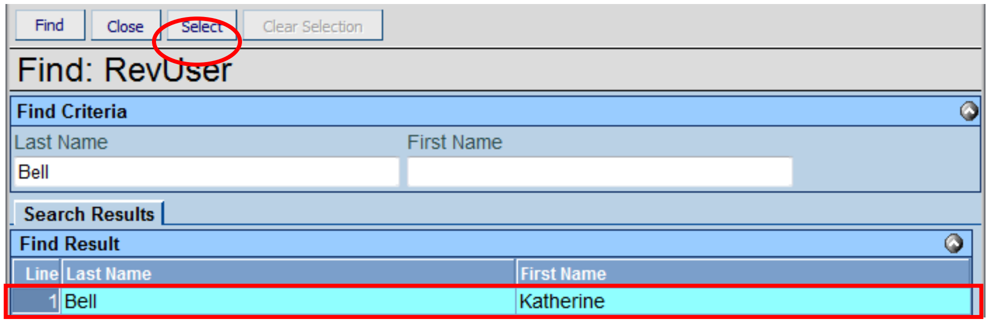
Search Results

Find Result

Line	Last Name	First Name

Figure 4.2 – Find: RevUser Screen

- In the **Find Result** grid, click the user, and click the **Select** button.



Find: RevUser

Find Criteria

Last Name: Bell

First Name:

Find Result

Line	Last Name	First Name
1	Bell	Katherine

Figure 4.3 – Find RevUser Screen, Selecting

8. Click the **Save** button at the top of the screen.

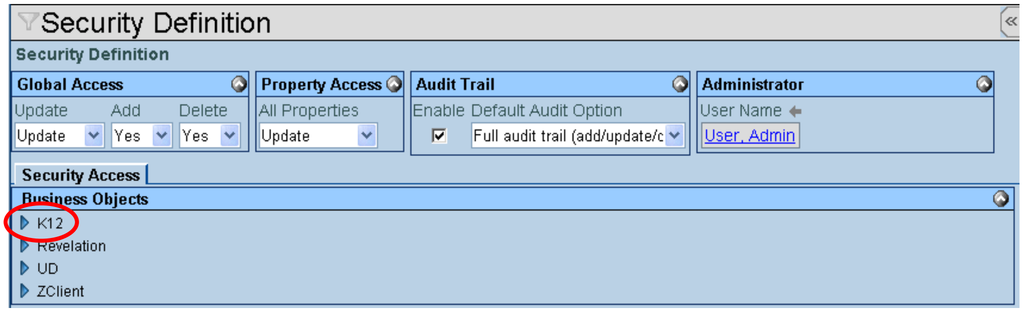
CUSTOMIZING USER GROUP RIGHTS

After the overall update rights have been set, the rights can further be customized by specifying rights for specific business objects for user groups. An outline of how user groups can be structured is found in Chapter One of this guide. Setting rights by user group is preferable over setting rights by individual user, as it is easier to maintain and setup. However, if there are exceptions for certain users this can be setup as outlined in the next section of this chapter.

The rights can be defined for both the overall business objects and for each individual property of the business object. Remember, only Screen Only rights can override the PAD Security rights within a screen. Update rights will not override Screen Only in PAD Security.

To define the rights for user groups to a business object or properties of a business object:

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



Security Definition

Security Definition

Global Access: Update: Update; Add: Yes; Delete: Yes

Property Access: All Properties: Update

Audit Trail: Enable Default Audit Option ☑ Full audit trail (add/update/c

Administrator: User Name: User, Admin

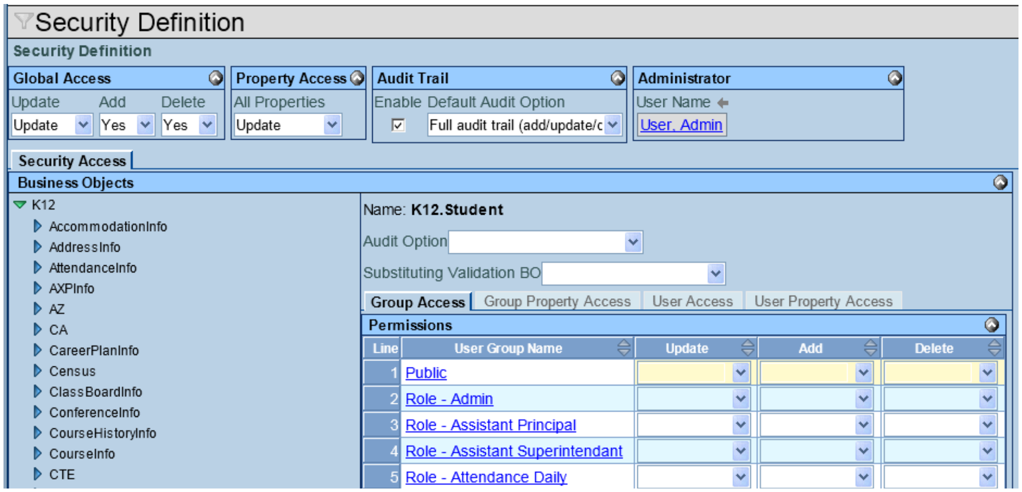
Business Objects

- K12
- Revelation
- UD
- ZClient

Figure 4.4 – Security Definition Screen

2. To find a business object, click the primary namespace that contains the business object. Most of the business objects are in the **K12** namespace. The **Revelation** namespace holds the system-wide business objects, such as phone number. The **UD** namespace holds user-defined namespaces, and shows business objects for districts with customized screens only. The **ZClient** namespace lists business objects for specific districts with customized needs.

3. Continue expanding namespaces, if necessary, by clicking them until the desired business property is shown.
4. Click the business property for which to set the access rights. For example, the K12.Student business property controls the rights for most of the **Demographics** tab and the **Other Info** tab of the **Student** screen.



Security Definition

Security Definition

Global Access: Update: Update; Add: Yes; Delete: Yes

Property Access: All Properties: Update

Audit Trail: Enable Default Audit Option: ☑ Full audit trail (add/update/c

Administrator: User Name: User, Admin

Security Access

Business Objects

- K12
  - AccommodationInfo
  - AddressInfo
  - AttendanceInfo
  - AXPInfo
  - AZ
  - CA
  - CareerPlanInfo
  - Census
  - ClassBoardInfo
  - ConferenceInfo
  - CourseHistoryInfo
  - CourseInfo
  - CTE

Name: K12.Student

Audit Option

Substituting Validation BO

Group Access | Group Property Access | User Access | User Property Access

Permissions

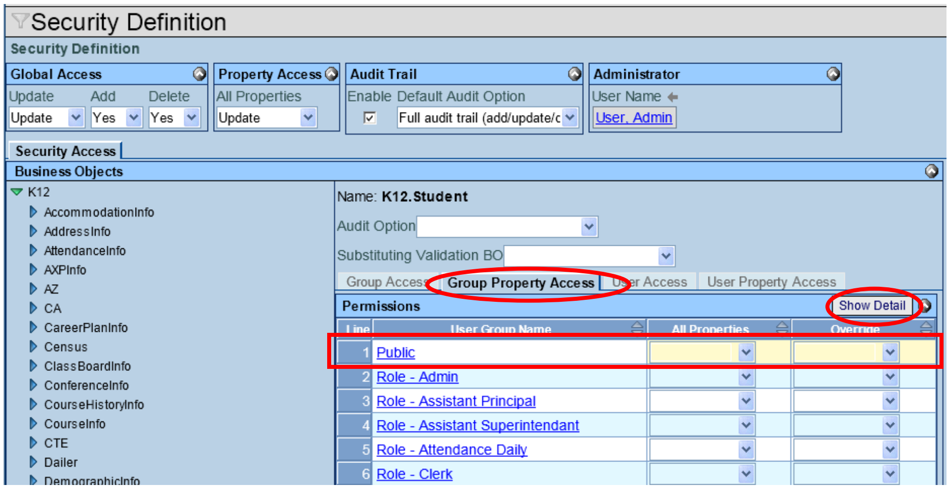
Line	User Group Name	Update	Add	Delete
1	Public			
2	Role - Admin			
3	Role - Assistant Principal			
4	Role - Assistant Superintendant			
5	Role - Attendance Daily			

Figure 4.5 – Security Definition Screen, Group Access Tab

5. For information about customizing a business property's **Audit Option**, see to Chapter Two.
6. For information about **Substituting Validation BO** and customizing the Synergy SIS interface, see the *Synergy SIS – System Administrator Guide*.
7. To set the default update rights for all groups, select a value in the **Update** column for the **Public** role.
8. In the **Add** list, select **Yes** to allow all groups to add records, or **No** to prevent users from adding records.
9. In the **Delete** list, select **Yes** to allow all groups to delete records, or **No** to prevent users from deleting records.
10. Set the **Update**, **Add**, and **Delete** rights for other user groups, as desired. User groups that do not have their own rights specified have the **Public** rights.
11. Click the **Save** button at the top of the screen. User groups that have been assigned custom rights are then listed at the top of the user groups list, followed by the groups with blank rights.

Caution: If setting **Update** for the **Public** role to **View** or **None**, first be sure to set the Admin user or the user group to which the Admin user belongs with update access to everything. Otherwise, even the Admin user could be completely locked out of the system!.

12. To set the rights to individual properties of the selected business object, click the **Group Property Access** tab.



Update	Add	Delete
Update	Yes	Yes

All Properties: Update

Enable: ☑ Default Audit Option: Full audit trail (add/update/c

User Name: User, Admin

Name: **K12.Student**

Audit Option:

Substituting Validation BO:

Line	User Group Name	All Properties	Override
1	Public		
2	Role - Admin		
3	Role - Assistant Principal		
4	Role - Assistant Superintendant		
5	Role - Attendance Daily		
6	Role - Clerk		

Figure 4.6 – Security Definition Screen, Group Property Access Tab

13. Use the **Public** role and the **All Properties** list to set the default rights for all user groups.

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

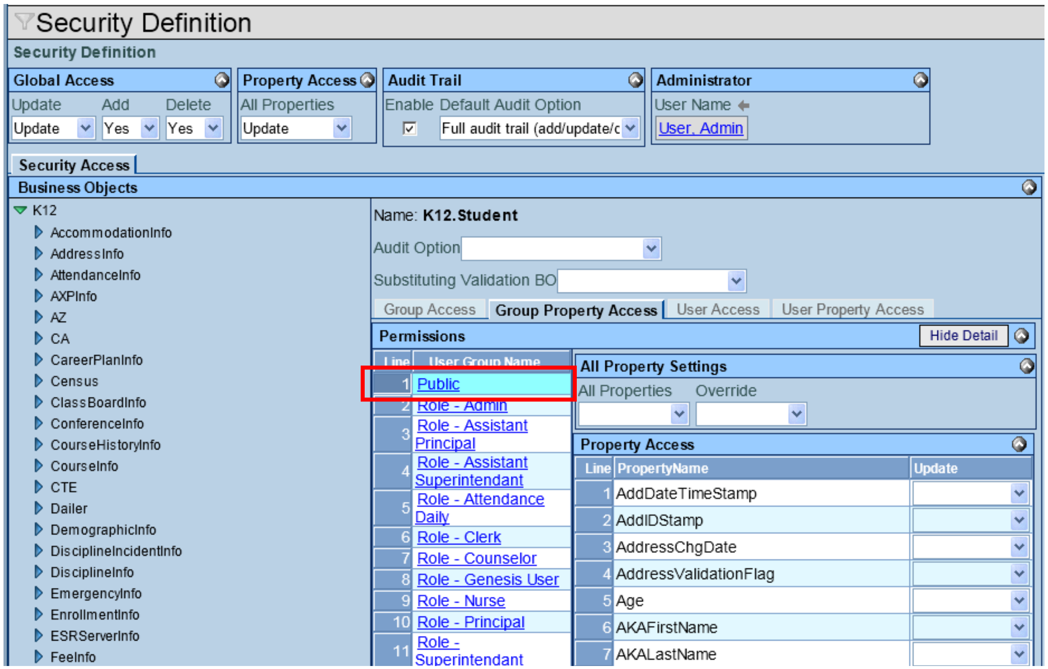
15. Set the rights for other user groups, as desired. User groups that do not have their own rights specified have the **Public** rights.

> **Caution:** If setting **All Properties** for the **Public** role to **View** or **None**, first be sure to set the Admin user or the user group to which the Admin user belongs with update access to everything. Otherwise, even the Admin user could be completely locked out of the system.

16. Click the **Save** button at the top of the screen. User groups that have been assigned custom rights are then listed at the top of the user groups list, followed by the groups listed with blank rights.

17. To set specific rights for individual properties, click the **Show Detail** button. The list of properties in the business object appears on the right.

18. To select a user group to modify, click the **Line** number of the **User Group Name** on the left.



Security Definition

Security Definition

Global Access

Update	Add	Delete
Update	Yes	Yes

Property Access

All Properties: Update

Audit Trail

Enable: ☑ Default Audit Option: Full audit trail (add/update/c

Administrator

User Name: User, Admin

Security Access

Business Objects

- K12
  - AccommodationInfo
  - AddressInfo
  - AttendanceInfo
  - AXPInfo
  - AZ
  - CA
  - CareerPlanInfo
  - Census
  - ClassBoardInfo
  - ConferenceInfo
  - CourseHistoryInfo
  - CourseInfo
  - CTE
  - Dailer
  - DemographicInfo
  - DisciplineIncidentInfo
  - DisciplineInfo
  - EmergencyInfo
  - EnrollmentInfo
  - ESRServerInfo
  - FeeInfo

Name: K12.Student

Audit Option

Substituting Validation BO

Group Access | Group Property Access | User Access | User Property Access

Permissions

Line	User Group Name
1	Public
2	Role - Admin
3	Role - Assistant Principal
4	Role - Assistant Superintendant
5	Role - Attendance Daily
6	Role - Clerk
7	Role - Counselor
8	Role - Genesis User
9	Role - Nurse
10	Role - Principal
11	Role - Superintendant

All Property Settings

All Properties Override

Property Access

Line	PropertyName	Update
1	AddDateTimeStamp	
2	AddIDStamp	
3	AddressChgDate	
4	AddressValidationFlag	
5	Age	
6	AKAFirstName	
7	AKALastName	

Figure 4.7 – Security Definition Screen, Group Property Access Tab, Detail Screen

19. Select **Update**, **View**, or **None** in the **Update** list to set the update rights for each property that needs to be customized.

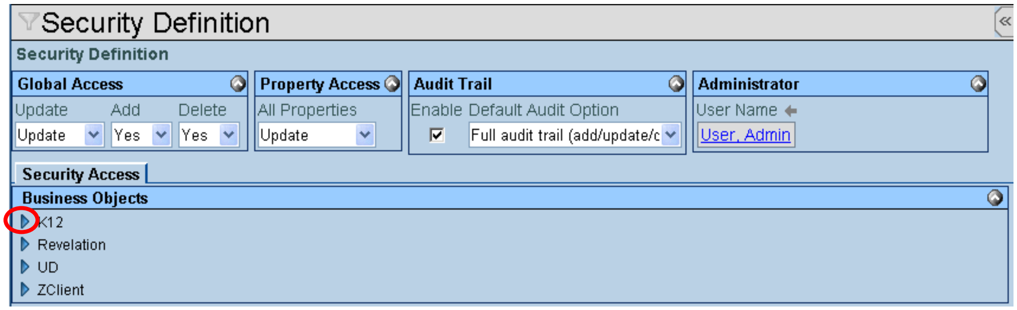
20. If the **Update** field is left blank for any property, it inherits the setting for **All Properties** if that has been set, or it uses the rights set for the entire business property. Click the **Hide Detail** button to return to the main screen.

21. Click the **Save** button at the top of the screen.

CUSTOMIZING USER RIGHTS

Occasionally, it may be necessary to grant rights to a specific user apart from user groups. These rights override user group rights. Only **View only** rights override the **PAD Security** rights within a screen. Update rights do not override **View only** in **PAD Security**. To define the rights for an individual user to a business object or properties of a business object:

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



Security Definition

Security Definition

Global Access: Update: Update; Add: Yes; Delete: Yes

Property Access: All Properties: Update

Audit Trail: Enable Default Audit Option: ☑ Full audit trail (add/update/c

Administrator: User Name: User, Admin

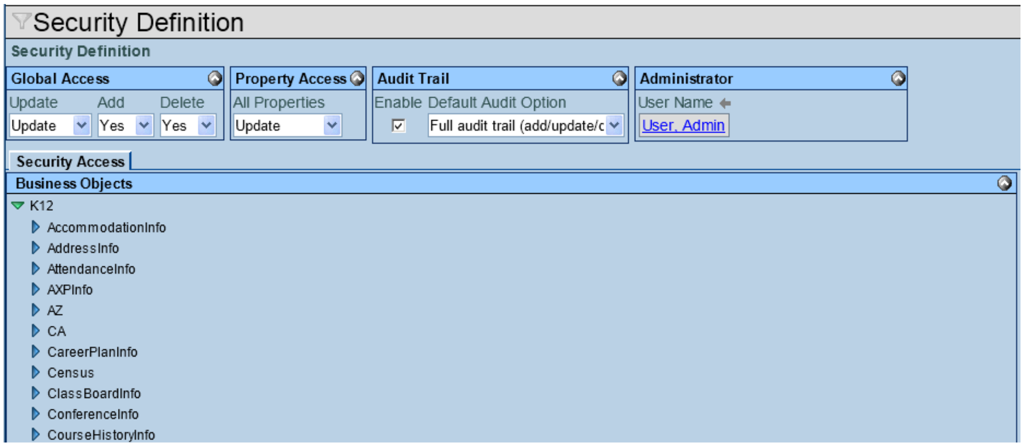
Security Access

Business Objects

Figure 4.8 – Security Definition Screen

2. To find a business object, click the primary namespace that contains the business object. Most of the business objects are in the **K12** namespace. The **Revelation** namespace holds the system-wide business objects, such as phone number. The **UD** namespace holds user-defined namespaces, and shows business objects for districts with customized screens only. The **ZClient** namespace lists business objects for specific districts with customized needs.

3. Continue expanding namespaces, if necessary, by clicking them until the desired business property is shown.



Security Definition

Security Definition

Global Access: Update: Update; Add: Yes; Delete: Yes

Property Access: All Properties: Update

Audit Trail: Enable Default Audit Option: ☑ Full audit trail (add/update/c

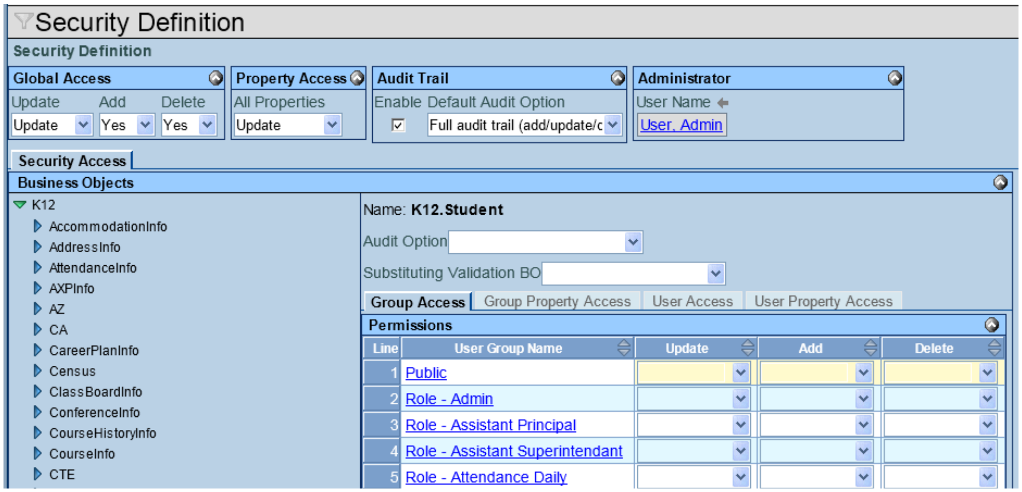
Administrator: User Name: User, Admin

Security Access

Business Objects

Figure 4.9 – Security Definition Screen, Locating Business Properties

4. Click the business property for which to set the access rights. For example, the K12.Student business property controls the rights for most of the **Demographics** tab and the **Other Info** tab of the **Student** screen.



Security Definition

Security Definition

Global Access			Property Access	Audit Trail		Administrator
Update	Add	Delete	All Properties	Enable	Default Audit Option	User Name
Update	Yes	Yes	Update	☑	Full audit trail (add/update/c	User, Admin

Security Access

Business Objects

- K12
  - AccommodationInfo
  - AddressInfo
  - AttendanceInfo
  - AXPInfo
  - AZ
  - CA
  - CareerPlanInfo
  - Census
  - ClassBoardInfo
  - ConferenceInfo
  - CourseHistoryInfo
  - CourseInfo
  - CTE

Name: **K12.Student**

Audit Option

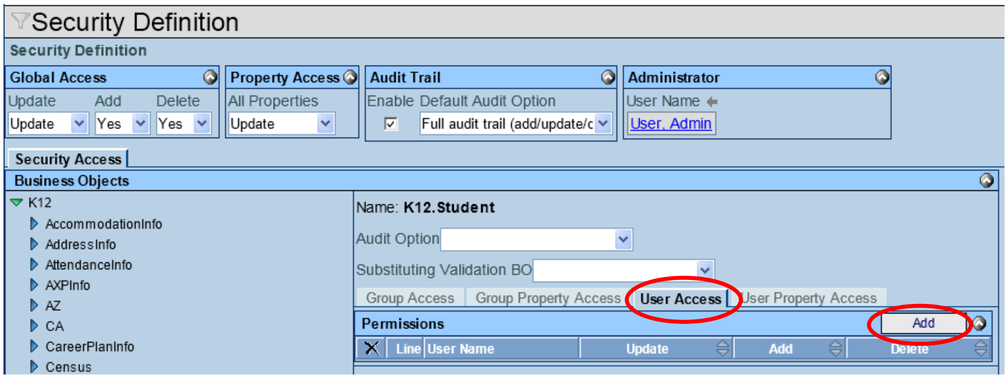
Substituting Validation BO

Permissions

Line	User Group Name	Update	Add	Delete
1	Public			
2	Role - Admin			
3	Role - Assistant Principal			
4	Role - Assistant Superintendant			
5	Role - Attendance Daily			

Figure 4.10 – Security Definition Screen, Group Access Tab

5. Click the **User Access** tab to set the update rights for a specific user.



Security Definition

Security Definition

Global Access			Property Access	Audit Trail		Administrator
Update	Add	Delete	All Properties	Enable	Default Audit Option	User Name
Update	Yes	Yes	Update	☑	Full audit trail (add/update/c	User, Admin

Security Access

Business Objects

- K12
  - AccommodationInfo
  - AddressInfo
  - AttendanceInfo
  - AXPInfo
  - AZ
  - CA
  - CareerPlanInfo
  - Census

Name: **K12.Student**

Audit Option

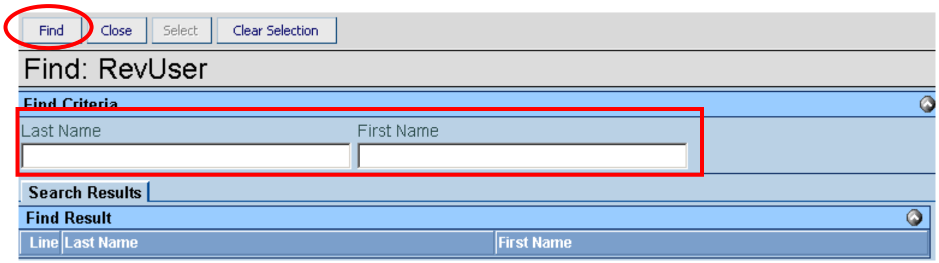
Substituting Validation BO

Line	User Name	Update	Add	Delete

Figure 4.11 – Security Definition Screen, User Access Tab

6. Select the user for which to customize update rights by clicking on the **Add** button. The **Find: RevUser** screen opens.

7. Enter all or part of the **Last Name** and/or **First Name** of the user, and click the **Find** button.



Find: RevUser

Find Criteria

Last Name

First Name

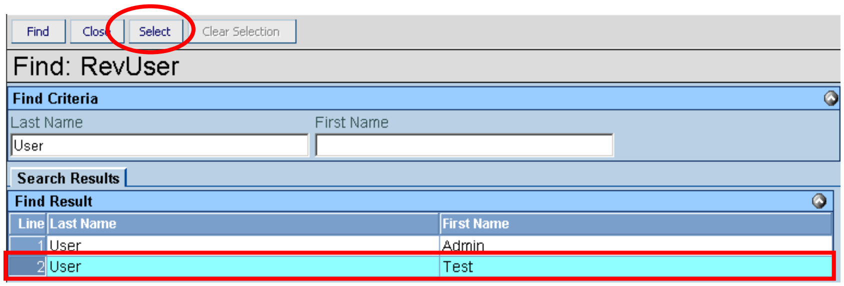
Search Results

Find Result

Line	Last Name	First Name

Figure 4.12 – Find RevUser Screen

8. In the **Find Result** grid, click the user, and click the **Select** button.



Find: RevUser

Last Name: User

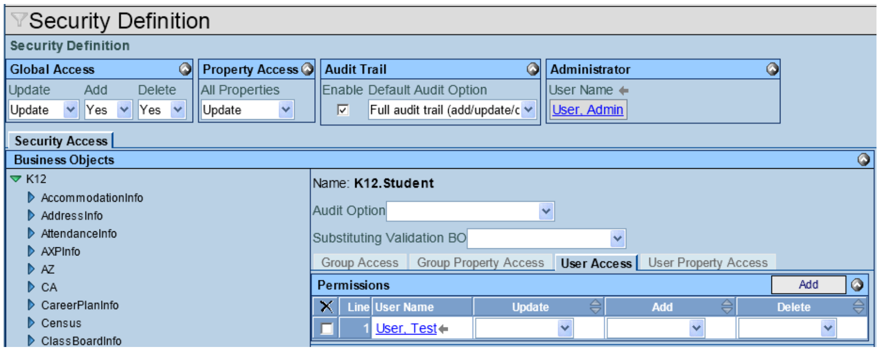
First Name:

Line	Last Name	First Name
1	User	Admin
2	User	Test

Figure 4.13 – Find RevUser Screen, Selecting

9. Click the **Select** button to add the user.

10. Select **Update**, **View**, or **None** in the **Update** list to set the update rights for the user.



Global Access: Update: Update; Add: Yes; Delete: Yes

Property Access: All Properties: Update

Audit Trail: Enable Default Audit Option ☑ Full audit trail (add/update/c

Administrator: User Name: User, Admin

Name: K12.Student

Audit Option:

Substituting Validation BO:

☒	Line	User Name	Update	Add	Delete
□	1	User, Test			

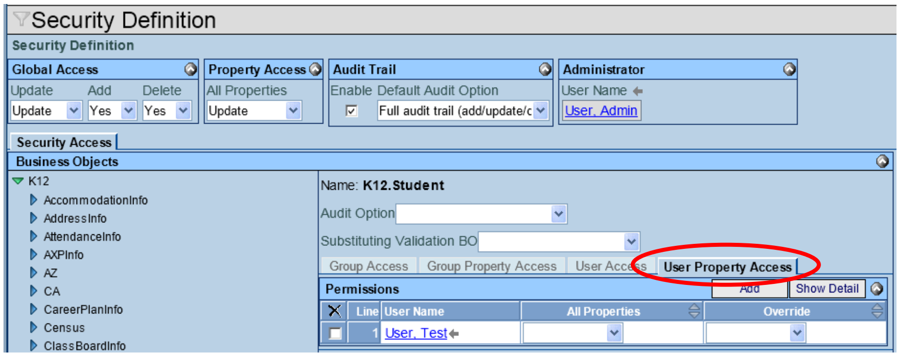
Figure 4.14 – Security Definition Screen, User Access Tab, User Added

11. In the **Add** list, select **Yes** to allow the user to add records, or **No** to prevent the user from adding records.

12. In the **Delete** list, select **Yes** to allow the user to delete records, or **No** to prevent the user from deleting records.

13. Click the **Save** button at the top of the screen.

14. To set the rights to individual properties of the selected business object, click the **User Property Access** tab. Users added on the **User Access** tab are also listed here.



Global Access: Update: Update; Add: Yes; Delete: Yes

Property Access: All Properties: Update

Audit Trail: Enable Default Audit Option ☑ Full audit trail (add/update/c

Administrator: User Name: User, Admin

Name: K12.Student

Audit Option:

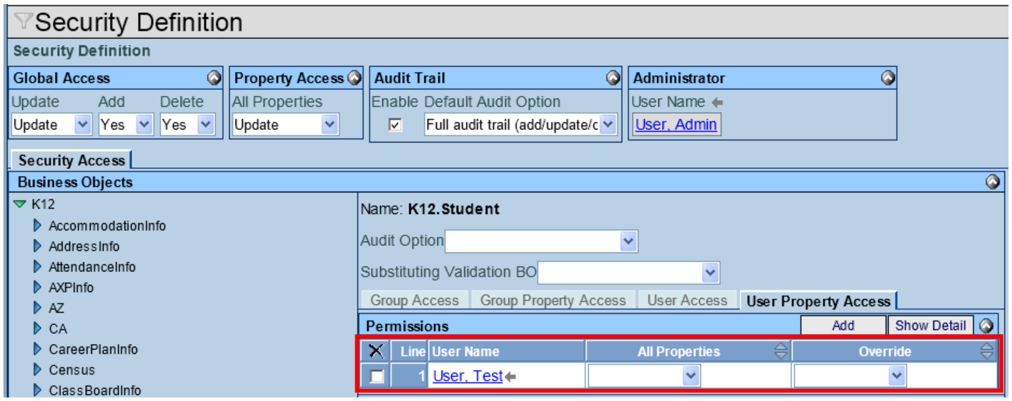
Substituting Validation BO:

☒	Line	User Name	All Properties	Override
□	1	User, Test		

Figure 4.15 – Security Definition Screen, User Property Access Tab

15. To add a user, click the **Add** button, and on the **Find: RevUser** screen, find and select the user.

16. In the **Permissions** grid on the **User Property Access** tab, set the update rights for individual properties in the **All Properties** list.



Security Definition

Security Definition

Global Access: Update: Update; Add: Yes; Delete: Yes

Property Access: All Properties: Update

Audit Trail: Enable ☑ Default Audit Option: Full audit trail (add/update/c

Administrator: User Name: User, Admin

Security Access

Business Objects

- K12
  - AccommodationInfo
  - AddressInfo
  - AttendanceInfo
  - AXPInfo
  - AZ
  - CA
  - CareerPlanInfo
  - Census
  - ClassBoardInfo

Name: K12.Student

Audit Option

Substituting Validation BO

☒	Line	User Name	All Properties	Override
□	1	User, Test		

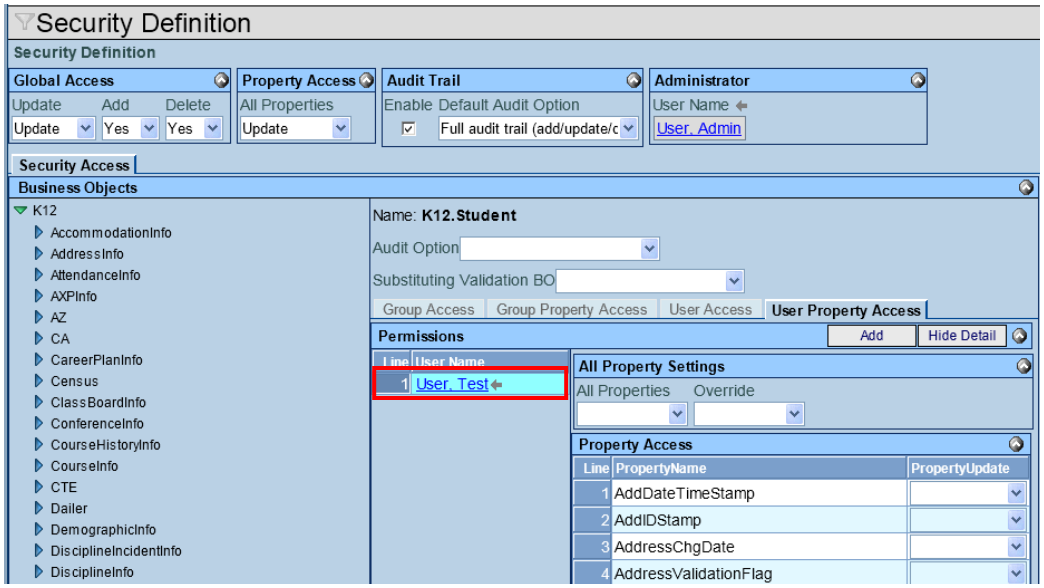
Figure 4.16 – Security Definition Screen, User Property Access Tab, User Added

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

18. Click the **Save** button at the top of the screen.

19. To set specific rights for individual properties, click the **Show Detail** button. The list of each property in the business object appears on the right.

20. To select which user to modify, click the **Line** number of the **User Name** on the left.



Security Definition

Security Definition

Global Access: Update: Update; Add: Yes; Delete: Yes

Property Access: All Properties: Update

Audit Trail: Enable ☑ Default Audit Option: Full audit trail (add/update/c

Administrator: User Name: User, Admin

Security Access

Business Objects

- K12
  - AccommodationInfo
  - AddressInfo
  - AttendanceInfo
  - AXPInfo
  - AZ
  - CA
  - CareerPlanInfo
  - Census
  - ClassBoardInfo
  - ConferenceInfo
  - CourseHistoryInfo
  - CourseInfo
  - CTE
  - Dailer
  - DemographicInfo
  - DisciplineIncidentInfo
  - DisciplineInfo

Name: K12.Student

Audit Option

Substituting Validation BO

Line	User Name
1	User, Test

All Property Settings

All Properties Override

Property Access

Line	PropertyName	PropertyUpdate
1	AddDateTimeStamp	
2	AddIDStamp	
3	AddressChgDate	
4	AddressValidationFlag	

Figure 4.17 – Security Definition Screen, User Property Access Tab, Detail Screen

21. Select **Update**, **View**, or **None** in the **Update** list to set the update rights for each property that needs to be customized.

22. If the **Update** field is left blank for any property, it inherits the setting for **All Properties** if that has been set, or it uses the rights set for the entire business property. Click the **Hide Detail** button to return to the main screen.

23. Click the **Save** button at the top of the screen.

Chapter Five:
REPORTS

This chapter covers:

- ► How to customize security reports
- ► Available security reports

In **Synergy SIS > System > Security > Reports > Summary** are four reports that show staff and user data. This chapter covers only the customizations specific to each of the reports used in Security. Additional options available on the other tabs are explained in the *Synergy SIS – Query & Reporting Guide*.

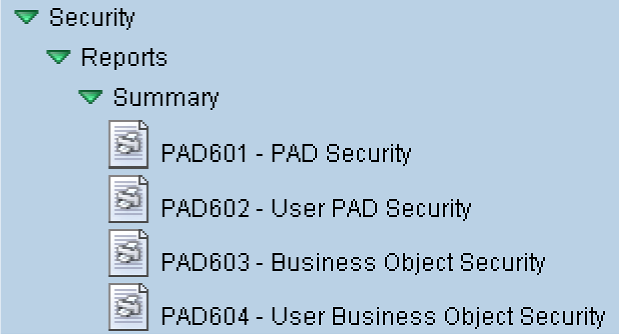
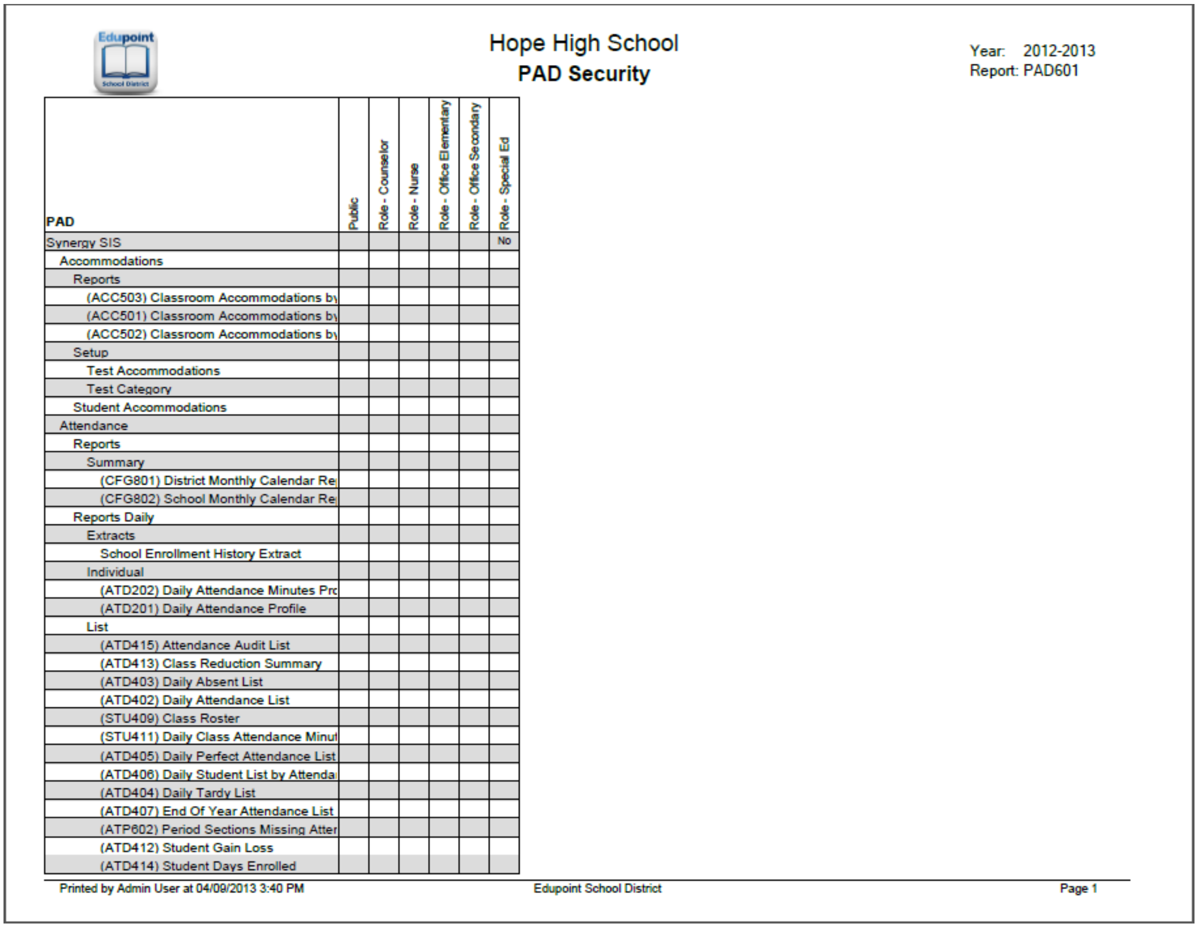

Security
Reports
Summary
PAD601 - PAD Security
PAD602 - User PAD Security
PAD603 - Business Object Security
PAD604 - User Business Object Security

Figure 5.1 – Security Reports

PAD601 – PAD SECURITY

The PAD Security report lists the screens in the district-specific folder (shown at the top of the PAD tree), Synergy SE, and Synergy SIS. It can also list the tabs, menu button, and other buttons on the screen. For each object, it displays the security assigned to each user group in the system. If blank, no security has been set, and the group inherits the rights from either the Public group (if set), or the global settings. If **No**, the group does not have access to the specified object. If **View**, the group has read-only access to the specified object. If **Yes**, the group has update access to the specified object.



Hope High School

PAD Security

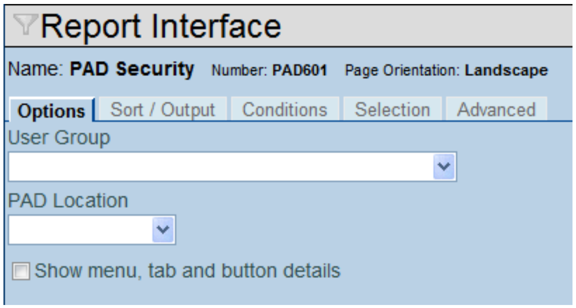
Year: 2012-2013
Report: PAD601

PAD	Public	Role - Counselor	Role - Nurse	Role - Office Elementary	Role - Office Secondary	Role - Special Ed
Synergy SIS						No
Accommodations						
Reports						
(ACC503) Classroom Accommodations by						
(ACC501) Classroom Accommodations by						
(ACC502) Classroom Accommodations by						
Setup						
Test Accommodations						
Test Category						
Student Accommodations						
Attendance						
Reports						
Summary						
(CFG801) District Monthly Calendar Re						
(CFG802) School Monthly Calendar Re						
Reports Daily						
Extracts						
School Enrollment History Extract						
Individual						
(ATD202) Daily Attendance Minutes Pro						
(ATD201) Daily Attendance Profile						
List						
(ATD415) Attendance Audit List						
(ATD413) Class Reduction Summary						
(ATD403) Daily Absent List						
(ATD402) Daily Attendance List						
(STU409) Class Roster						
(STU411) Daily Class Attendance Minut						
(ATD405) Daily Perfect Attendance List						
(ATD406) Daily Student List by Attenda						
(ATD404) Daily Tardy List						
(ATD407) End Of Year Attendance List						
(ATP602) Period Sections Missing Atten						
(ATD412) Student Gain Loss						
(ATD414) Student Days Enrolled						

Printed by Admin User at 04/09/2013 3:40 PM Edupoint School District Page 1

Figure 5.2 – PAD Security Report

The report can be customized using the following options:



Report Interface

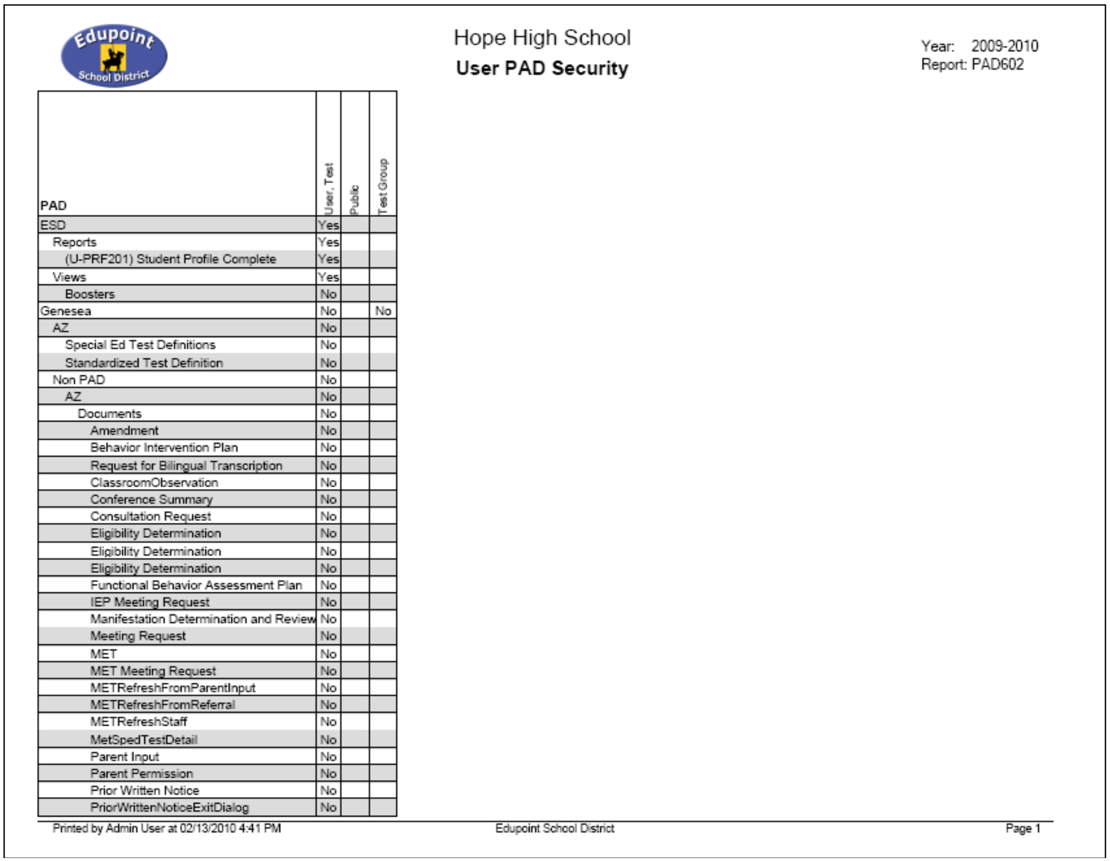
Name: **PAD Security** Number: **PAD601** Page Orientation: **Landscape**

Figure 5.3 – PAD Security Report Interface

- You can print the report for a specific **User Group**. If this field is left blank, all groups that have security settings selected are included.
- You can print the report for a specific group of screens by selecting an option in the **PAD Location** list. If this field is left blank, all screens are printed.
- To show the security assigned for the **Menu** buttons at the tops of screens, the tabs on the screens, and the buttons on the screens, check the **Show menu, tab and button details** box.

PAD602 – USER PAD SECURITY

The User PAD Security report lists the screens in the district-specific folder (shown at the top of the PAD tree), Synergy SE, and Synergy SIS. It can also list the **Menu** button, tabs, and other buttons on the screen. For each object, it displays the security assigned to the user or users selected, and the user groups to which the users belong. If blank, no security has been set and the group inherits the rights from either the Public group (if set), or the global settings. If **No**, the group does not have access to the specified object. If **View**, the group has screen-only access to the specified object. If **Yes**, the group has update access to the specified object.



Hope High School

User PAD Security

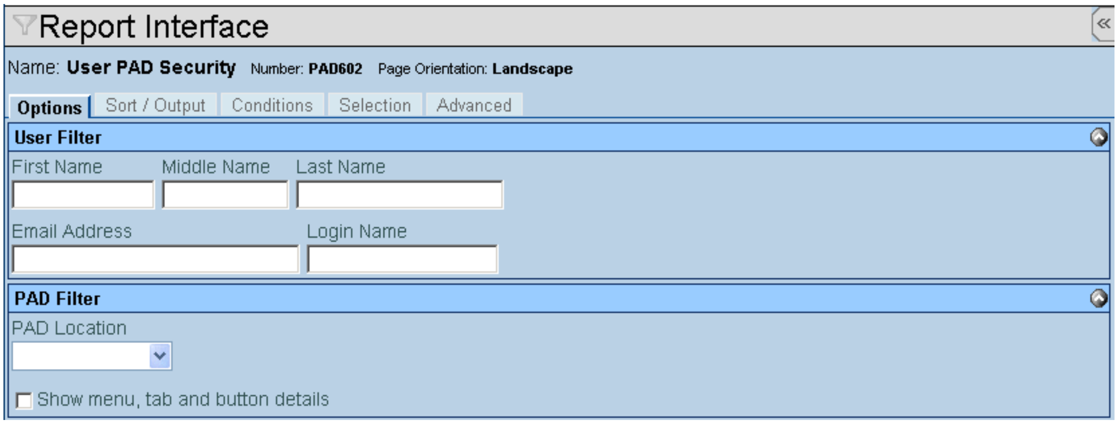
Year: 2009-2010
Report: PAD602

PAD	User, Test	Public	Test Group
ESD	Yes		
Reports	Yes		
(U-PRF201) Student Profile Complete	Yes		
Views	Yes		
Boosters	No		
Genesea	No		No
AZ	No		
Special Ed Test Definitions	No		
Standardized Test Definition	No		
Non PAD	No		
AZ	No		
Documents	No		
Amendment	No		
Behavior Intervention Plan	No		
Request for Bilingual Transcription	No		
ClassroomObservation	No		
Conference Summary	No		
Consultation Request	No		
Eligibility Determination	No		
Eligibility Determination	No		
Eligibility Determination	No		
Functional Behavior Assessment Plan	No		
IEP Meeting Request	No		
Manifestation Determination and Review	No		
Meeting Request	No		
MET	No		
MET Meeting Request	No		
METRefreshFromParentInput	No		
METRefreshFromReferral	No		
METRefreshStaff	No		
MetSpedTestDetail	No		
Parent Input	No		
Parent Permission	No		
Prior Written Notice	No		
PriorWrittenNoticeExitDialog	No		

Printed by Admin User at 02/13/2010 4:41 PM Edupoint School District Page 1

Figure 5.4 – User PAD Security Report

The report can be customized using the following options:



Report Interface

Name: **User PAD Security** Number: **PAD602** Page Orientation: **Landscape**

□ Show menu, tab and button details

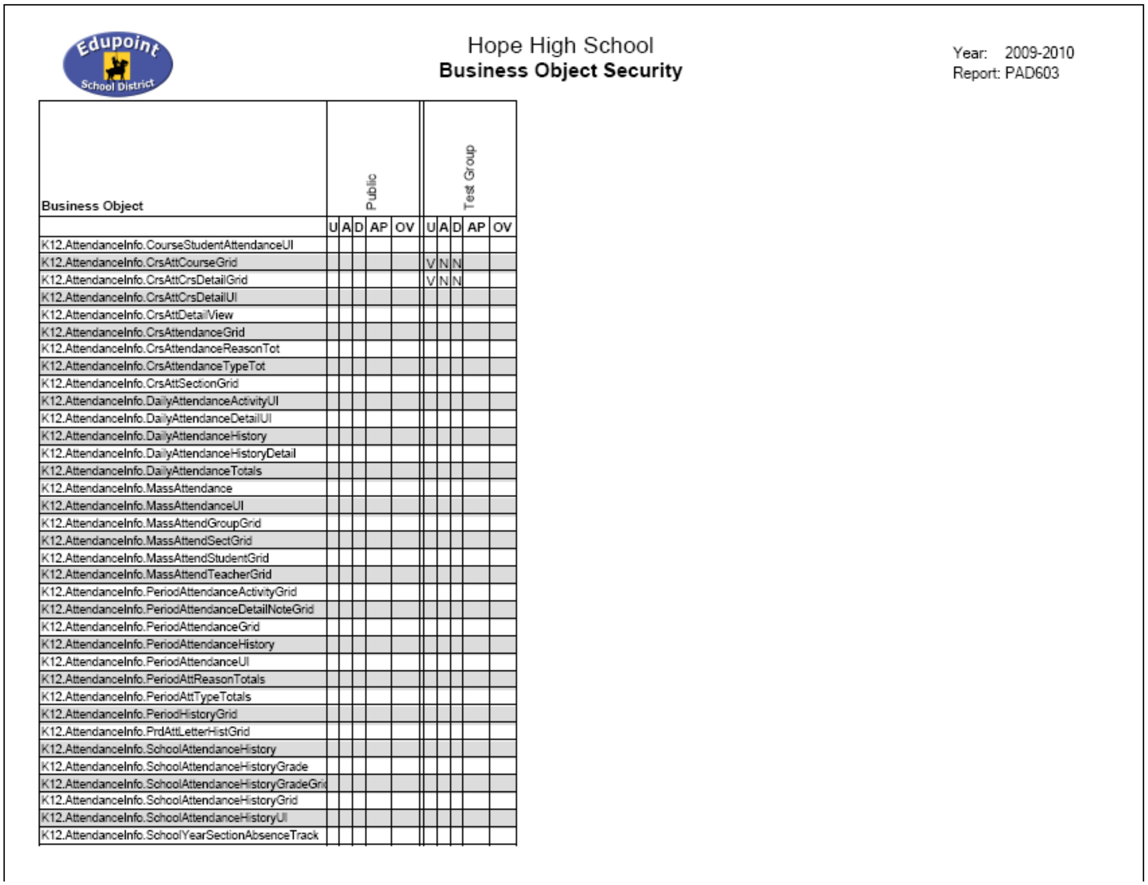
Figure 5.5 – User PAD Security Report Interface

- You can print the report for a specific user or group of users by entering the **First Name**, **Middle Name**, **Last Name**, **Email Address**, and/or **Login Name**.
- You can print the report for a specific group of screens by selecting an option in the **PAD Location** list. If this field is left blank, all screens are printed.
- To show the security assigned for the **Menu** buttons at the tops of screens, the tabs on the screens, and the buttons on the screens, check the **Show menu, tab and button details** box.

PAD603 – BUSINESS OBJECT SECURITY

The Business Object Security report lists the business objects in the system and shows the security set on the objects for each user group that has custom security set. The columns and their values:

- **U** (Update) shows **V** for view only, **N** for no access, or **U** for update.
- **A** (Add) and **D** (Delete) show **Y** for yes or **N** for no, indicating whether the user group can add or delete records.
- **AP** (All Properties) shows whether all properties (fields) of the indicated business object have been set to **V** for view only, **N** for no access, or **U** for update.
- **OV** (Override Properties) shows whether the access rights set for the group override the access rights set for individual properties.



Edupoint
School District

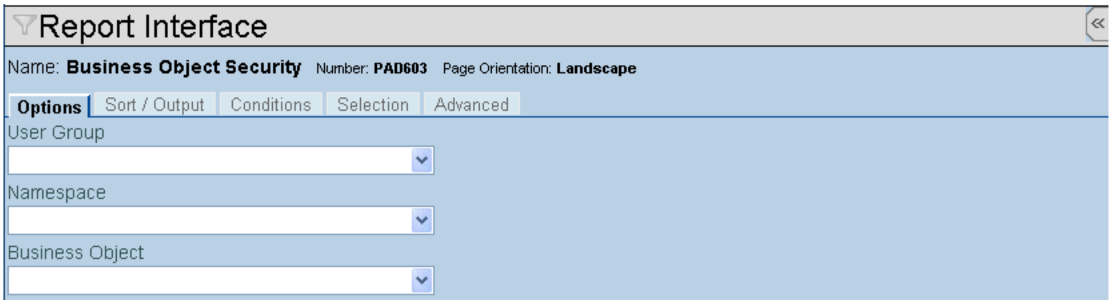
Hope High School
Business Object Security

Year: 2009-2010
Report: PAD603

Business Object	Public					Test Group				
	U	A	D	AP	OV	U	A	D	AP	OV
K12.AttendanceInfo.CourseStudentAttendanceUI										
K12.AttendanceInfo.CrsAttCourseGrid						V	N	N		
K12.AttendanceInfo.CrsAttCrsDetailGrid						V	N	N		
K12.AttendanceInfo.CrsAttCrsDetailUI										
K12.AttendanceInfo.CrsAttDetailView										
K12.AttendanceInfo.CrsAttendanceGrid										
K12.AttendanceInfo.CrsAttendanceReasonTot										
K12.AttendanceInfo.CrsAttendanceTypeTot										
K12.AttendanceInfo.CrsAttSectionGrid										
K12.AttendanceInfo.DailyAttendanceActivityUI										
K12.AttendanceInfo.DailyAttendanceDetailUI										
K12.AttendanceInfo.DailyAttendanceHistory										
K12.AttendanceInfo.DailyAttendanceHistoryDetail										
K12.AttendanceInfo.DailyAttendanceTotals										
K12.AttendanceInfo.MassAttendance										
K12.AttendanceInfo.MassAttendanceUI										
K12.AttendanceInfo.MassAttendGroupGrid										
K12.AttendanceInfo.MassAttendSectGrid										
K12.AttendanceInfo.MassAttendStudentGrid										
K12.AttendanceInfo.MassAttendTeacherGrid										
K12.AttendanceInfo.PeriodAttendanceActivityGrid										
K12.AttendanceInfo.PeriodAttendanceDetailNoteGrid										
K12.AttendanceInfo.PeriodAttendanceGrid										
K12.AttendanceInfo.PeriodAttendanceHistory										
K12.AttendanceInfo.PeriodAttendanceUI										
K12.AttendanceInfo.PeriodAttReasonTotals										
K12.AttendanceInfo.PeriodAttTypeTotals										
K12.AttendanceInfo.PeriodHistoryGrid										
K12.AttendanceInfo.PrdAttLetterHistGrid										
K12.AttendanceInfo.SchoolAttendanceHistory										
K12.AttendanceInfo.SchoolAttendanceHistoryGrade										
K12.AttendanceInfo.SchoolAttendanceHistoryGradeGri										
K12.AttendanceInfo.SchoolAttendanceHistoryGrid										
K12.AttendanceInfo.SchoolAttendanceHistoryUI										
K12.AttendanceInfo.SchoolYearSectionAbsenceTrack										

Figure 5.6 – Business Object Security Report

The report can be customized using the following options:



Report Interface

Name: **Business Object Security** Number: **PAD603** Page Orientation: **Landscape**

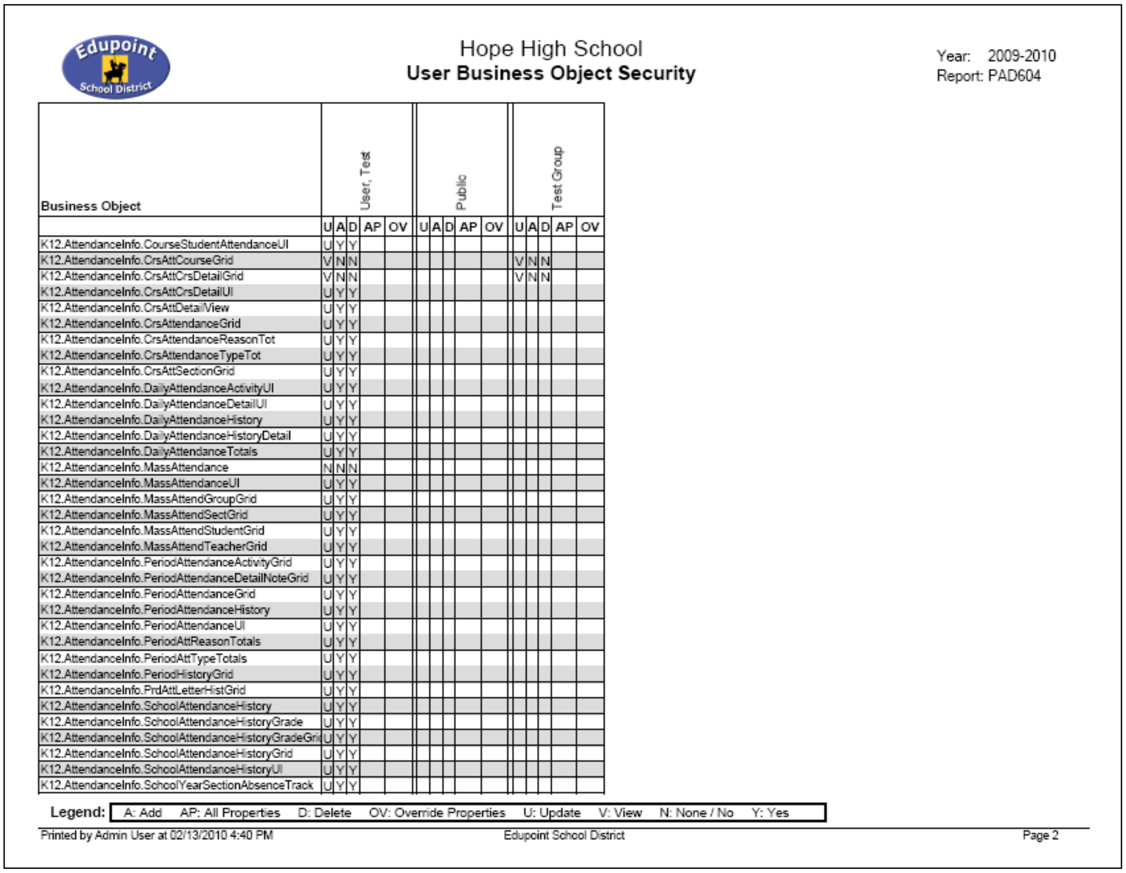
Figure 5.7 – Business Object Security Report Interface

- You can print the report for a specific **User Group**. If this field is left blank, all groups that have security settings selected are included.
- To limit the business objects displayed in the report, you can select the **Namespace** of the objects to be included.
- You can include a specific **Business Object**.

PAD604 – USER BUSINESS OBJECT SECURITY

The Business Object Security report lists the business objects in the system and shows the security set on the objects for specified users and the user groups to which they belong. The columns and their values:

- **U** (Update) shows **V** for view only, **N** for no access, or **U** for update.
- **A** (Add) and **D** (Delete) show **Y** for yes or **N** for no, indicating whether the user group can add or delete records.
- **AP** (All Properties) shows whether all properties (fields) of the indicated business object have been set to **V** for view only, **N** for no access, or **U** for update.
- **OV** (Override Properties) shows whether the access rights set for the group override the access rights set for individual properties.



Hope High School
User Business Object Security

Year: 2009-2010
Report: PAD604

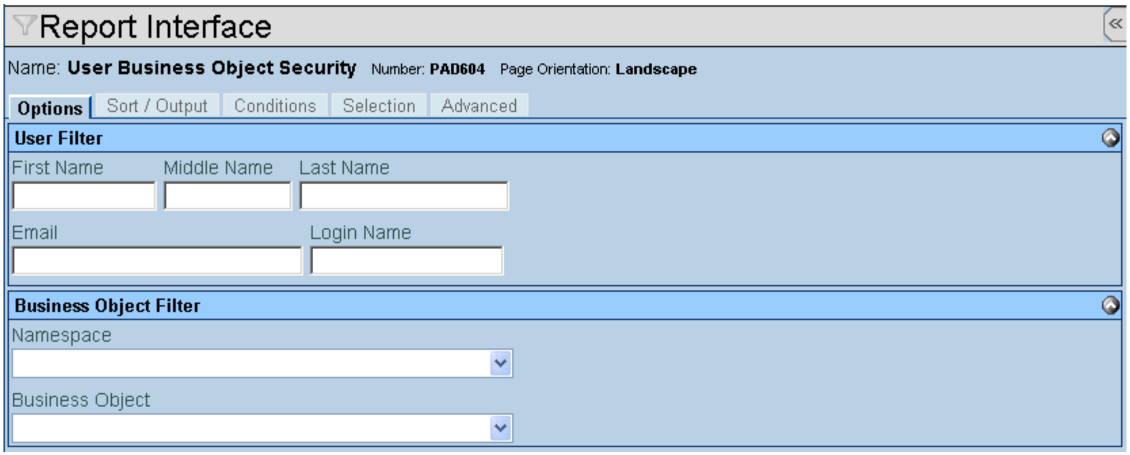
Business Object	User, Test					Public					Test Group				
	U	A	D	AP	OV	U	A	D	AP	OV	U	A	D	AP	OV
K12.AttendanceInfo.CourseStudentAttendanceUI	U	Y	Y												
K12.AttendanceInfo.CrsAttCourseGrid	V	N	N								V	N	N		
K12.AttendanceInfo.CrsAttCrsDetailGrid	V	N	N								V	N	N		
K12.AttendanceInfo.CrsAttCrsDetailUI	U	Y	Y												
K12.AttendanceInfo.CrsAttDetailView	U	Y	Y												
K12.AttendanceInfo.CrsAttendanceGrid	U	Y	Y												
K12.AttendanceInfo.CrsAttendanceReasonTot	U	Y	Y												
K12.AttendanceInfo.CrsAttendanceTypeTot	U	Y	Y												
K12.AttendanceInfo.CrsAttSectionGrid	U	Y	Y												
K12.AttendanceInfo.DailyAttendanceActivityUI	U	Y	Y												
K12.AttendanceInfo.DailyAttendanceDetailUI	U	Y	Y												
K12.AttendanceInfo.DailyAttendanceHistory	U	Y	Y												
K12.AttendanceInfo.DailyAttendanceHistoryDetail	U	Y	Y												
K12.AttendanceInfo.DailyAttendanceTotals	U	Y	Y												
K12.AttendanceInfo.MassAttendance	N	N	N												
K12.AttendanceInfo.MassAttendanceUI	U	Y	Y												
K12.AttendanceInfo.MassAttendGroupGrid	U	Y	Y												
K12.AttendanceInfo.MassAttendSectGrid	U	Y	Y												
K12.AttendanceInfo.MassAttendStudentGrid	U	Y	Y												
K12.AttendanceInfo.MassAttendTeacherGrid	U	Y	Y												
K12.AttendanceInfo.PeriodAttendanceActivityGrid	U	Y	Y												
K12.AttendanceInfo.PeriodAttendanceDetailNoteGrid	U	Y	Y												
K12.AttendanceInfo.PeriodAttendanceGrid	U	Y	Y												
K12.AttendanceInfo.PeriodAttendanceHistory	U	Y	Y												
K12.AttendanceInfo.PeriodAttendanceUI	U	Y	Y												
K12.AttendanceInfo.PeriodAttReasonTotals	U	Y	Y												
K12.AttendanceInfo.PeriodAttTypeTotals	U	Y	Y												
K12.AttendanceInfo.PeriodHistoryGrid	U	Y	Y												
K12.AttendanceInfo.PrdAttLetterHistGrid	U	Y	Y												
K12.AttendanceInfo.SchoolAttendanceHistory	U	Y	Y												
K12.AttendanceInfo.SchoolAttendanceHistoryGrade	U	Y	Y												
K12.AttendanceInfo.SchoolAttendanceHistoryGradeGri	U	Y	Y												
K12.AttendanceInfo.SchoolAttendanceHistoryGrid	U	Y	Y												
K12.AttendanceInfo.SchoolAttendanceHistoryUI	U	Y	Y												
K12.AttendanceInfo.SchoolYearSectionAbsenceTrack	U	Y	Y												

Legend: A: Add AP: All Properties D: Delete OV: Override Properties U: Update V: View N: None / No Y: Yes

Printed by Admin User at 02/13/2010 4:40 PM Edupoint School District Page 2

Figure 5.8 – User Business Object Security Report

The report can be customized using the following options:



Report Interface

Name: **User Business Object Security** Number: **PAD604** Page Orientation: **Landscape**

Figure 5.9 – User Business Object Security Report Interface

- You can print the report for one or more specific users by entering the **First Name**, **Middle Name**, **Last Name**, **Email** address, and/or **Login Name**.
- To limit the business objects displayed in the report, select the **Namespace** of the objects to be displayed. To show the security for a specific **Business Object** in the namespace, select the object.

INDEX OF SCREENS